Systemwalker Desktop Keeper V14g

運用ガイド　管理者編

Windows

B1WD-2774-02Z0(00)
2010年10月

まえがき

本書の目的

本書は、以下の製品を使用するために必要な設定方法および操作方法について説明しています。

- Systemwalker Desktop Keeper V14g(14.1.0)

本書は、Windows版を対象としています。

本書の読者

本書は、Systemwalker Desktop Keeperを使用して情報漏洩対策システムを構築/運用する方を対象に書かれています。
また、本書を読むためには、以下の知識が必要です。

- パーソナルコンピュータに関する一般的な知識
- Microsoft® Windowsに関する一般的な知識
- インターネットに関する一般的な知識
- Citrix XenApp™に関する一般的な知識(Citrix XenApp監視機能を使用する場合)

本書の構成

本書は、1章～8章および付録Aから構成されています。

第1章 運用をはじめる前に

運用全体のながれと、機能ごとの留意事項を説明します。

第2章 運用環境を整える

ポリシーの考え方、運用環境の整備を説明します。

第3章 管理コンソールでポリシーを設定する

管理コンソールでポリシーを変更する方法を説明します。

第4章 クライアント(CT)操作の傾向をみる

状況画面またはログアナライザでログの特異点をつかむ方法を説明します。

第5章 ログビューアでクライアント(CT)での操作を監査する

ログの参照方法を説明します。

第6章 監査資料を作成する

監査資料の作成方法を説明します。

第7章 運用環境を変更する

運用環境の変更方法を説明します。

第8章 設定できるポリシー

Systemwalker Desktop Keeperで設定できるポリシーを説明します。

付録A 集計目的一覧

ログアナライザで設定されている各集計目的について説明します。

付録B 複合機と連携して情報を可視化する

複合機からの情報を利用してレポートを作成・出力する方法を説明します。

本書の位置づけ

Systemwalker Desktop Keeperのマニュアルにおける本書の位置づけは、以下のとおりです。

マニュアル名称	内容
Systemwalker Desktop Keeper 解説書	Systemwalker Desktop Keeperの概要および動作環境について説明します。
Systemwalker Desktop Keeper 導入ガイド	Systemwalker Desktop Keeperの導入設定および保守/管理方法について説明します。
Systemwalker Desktop Keeper 運用ガイド 管理者編(本書)	Systemwalker Desktop Keeperの運用方法について説明します。
Systemwalker Desktop Keeper 運用ガイド クライアント編(注)	Systemwalker Desktop Keeperの持出しユーティリティの機能概要や操作方法について説明します。
Systemwalker Desktop Keeperリファレンスマニュアル	Systemwalker Desktop Keeperで使用するコマンド、ファイル、メッセージ、およびポート番号について説明します。

注) Systemwalker Desktop Keeper 運用ガイド クライアント編は、持出しユーティリティのヘルプから参照できます。

Systemwalker技術情報ホームページでは、最新のマニュアルやトラブルシューティングガイド、Systemwalkerの使用方法などを公開しています。最初に、Systemwalker技術情報ホームページを参照することをお勧めします。

URL:http://systemwalker.fujitsu.com/jp/man/

ユーザー名:DTK_V14g

パスワード:green

本書の表記について

本書では、説明のために、以下に示す名称、記号および略称を使用しています。

コマンドで使用する記号について

コマンドで使用している記号について以下に説明します。

記号の意味

記 号	意 味
[ ]	この記号で囲まれた項目を省略できることを示します。
|	この記号を区切りとして並べられた項目の中から、どれか1つを選択することを示します。

マニュアルの記号について

マニュアルでは以下の記号を使用しています。

注意

特に注意が必要な事項を説明しています。

ポイント

知っておくと便利な情報を説明しています。

略称について

本書では、以下のように製品表示名を略して表記しています。

製品表示名	略称
Systemwalker Desktop Keeper Base Edition V12.0L10	BEV12.0L10
Systemwalker Desktop Keeper Base Edition V12.0L20	BEV12.0L20
Systemwalker Desktop Keeper Base Edition V13.0.0	BEV13.0.0
Systemwalker Desktop Keeper Base Edition V13.2.0	BEV13.2.0
Systemwalker Desktop Keeper Base Edition V13.3.0	BEV13.3.0
Systemwalker Desktop Keeper Standard Edition V12.0L20	SEV12.0L20
Systemwalker Desktop Keeper Standard Edition V13.0.0	SEV13.0.0
Systemwalker Desktop Keeper Standard Edition V13.2.0、 Systemwalker Desktop Keeper Standard Edition V13.2.1	SEV13.2.0
Systemwalker Desktop Keeper Standard Edition V13.3.0	SEV13.3.0
Systemwalker Desktop Keeper V14g (V14.0.0)	V14.0.0
Systemwalker Desktop Keeper V14g (V14.0.1)	V14.0.1
Systemwalker Desktop Keeper V14g (V14.1.0)	V14.1.0
Microsoft® Internet Explorer® 6.0 Windows® Internet Explorer® 7 Windows® Internet Explorer® 8	Internet Explorer®

本書では、以下のようにオペレーティングシステム名を略して表記しています。

オペレーティングシステム名	略称
Microsoft® Windows Server® 2008 Foundation、 Microsoft® Windows Server® 2008 Standard、 Microsoft® Windows Server® 2008 Enterprise、 Microsoft® Windows Server® 2008 Standard without Hyper-V™、 Microsoft® Windows Server® 2008 Enterprise without Hyper-V™、 Microsoft® Windows Server® 2008 R2 Foundation、 Microsoft® Windows Server® 2008 R2 Standard、 Microsoft® Windows Server® 2008 R2 Enterprise	Windows Server® 2008(※)
Microsoft® Windows Server® 2003, Standard Edition、 Microsoft® Windows Server® 2003, Enterprise Edition、 Microsoft® Windows Server® 2003 R2, Standard Edition、 Microsoft® Windows Server® 2003 R2, Enterprise Edition、 Microsoft® Windows Server® 2003, Standard x64 Edition、 Microsoft® Windows Server® 2003, Enterprise x64 Edition、 Microsoft® Windows Server® 2003 R2, Standard x64 Edition、 Microsoft® Windows Server® 2003 R2, Enterprise x64 Edition	Windows Server® 2003(※)
Microsoft® Windows® 2000 Professional operating system、 Microsoft® Windows® 2000 Server operating system、 Microsoft® Windows® 2000 Advanced Server operating system	Windows® 2000
Microsoft® Windows® XP Professional、 Microsoft® Windows® XP Home Edition	Windows® XP(※)
Windows Vista® Home Basic、 Windows Vista® Home Premium、 Windows Vista® Business、	Windows Vista®(※)

オペレーティングシステム名	略称
Windows Vista® Enterprise、 Windows Vista® Ultimate	
Windows® 7 Ultimate、 Windows® 7 Enterprise、 Windows® 7 Professional、 Windows® 7 Home Premium	Windows® 7(※)
Microsoft® Windows® Millennium Edition	Windows® ME
Microsoft® Windows® 98 Second Edition	Windows® 98
Microsoft® Windows® 95 operating system	Windows® 95
Microsoft® Windows Server® 2008 Foundation、 Microsoft® Windows Server® 2008 Standard、 Microsoft® Windows Server® 2008 Enterprise、 Microsoft® Windows Server® 2008 Standard without Hyper-V™、 Microsoft® Windows Server® 2008 Enterprise without Hyper-V™、 Microsoft® Windows Server® 2008 R2 Foundation、 Microsoft® Windows Server® 2008 R2 Standard、 Microsoft® Windows Server® 2008 R2 Enterprise Microsoft® Windows Server® 2003, Standard Edition、 Microsoft® Windows Server® 2003, Enterprise Edition、 Microsoft® Windows Server® 2003 R2, Standard Edition、 Microsoft® Windows Server® 2003 R2, Enterprise Edition、 Microsoft® Windows Server® 2003, Standard x64 Edition、 Microsoft® Windows Server® 2003, Enterprise x64 Edition、 Microsoft® Windows Server® 2003 R2, Standard x64 Edition、 Microsoft® Windows Server® 2003 R2, Enterprise x64 Edition、 Microsoft® Windows® 2000 Professional operating system、 Microsoft® Windows® 2000 Server operating system、 Microsoft® Windows® 2000 Advanced Server operating system、 Microsoft® Windows® XP Professional、 Microsoft® Windows® XP Home Edition、 Windows Vista® Home Basic、 Windows Vista® Home Premium、 Windows Vista® Business、 Windows Vista® Enterprise、 Windows Vista® Ultimate、 Windows® 7 Ultimate、 Windows® 7 Enterprise、 Windows® 7 Professional、 Windows® 7 Home Premium、 Microsoft® Windows® Millennium Edition、 Microsoft® Windows® 98 Second Edition	Windows

※) コマンドやファイルの格納場所など、特に64ビット版の場合を区別して記述する場合は、略称として以下のように表記します。

- Windows ServerR 2008 64ビット版
- Windows ServerR 2008 R2
- Windows ServerR 2003 x64 Edition
- Windows ServerR 2003 R2 x64 Edition
- Windows® XP 64ビット版
- Windows Vista® 64ビット版

- Windows® 7 64ビット版

オペレーティングシステム固有の操作について

本書では、オペレーティングシステム固有の操作(ローカルエリア接続の操作など)については、代表例として、Windows Server® 2003での場合を記述しています。
Windows Server® 2003以外での操作については、各オペレーティングシステムの操作方法に従ってください。

輸出管理規制について

当社ドキュメントには、外国為替および外国貿易管理法に基づく特定技術が含まれていることがあります。特定技術が含まれている場合は、当該ドキュメントを輸出または非居住者に提供するとき、同法に基づく許可が必要となります。

商標について

Microsoft、Windows、Windows NT、Windows Vista、およびWindows Serverまたはその他のマイクロソフト製品の名称および製品名は、米国Microsoft Corporationの米国およびその他の国における商標または登録商標です。

Citrix、Xen、Citrix XenApp、Citrix XenServerおよびCitrix Presentation Serverは、Citrix Systems, Inc.の米国あるいはその他の国における登録商標または商標です。

その他の製品名は、各社の商標または登録商標です。

Microsoft Corporationのガイドラインに従って画面写真を使用しています。

平成22年 10月

改版履歴
平成22年 10月 初版

Copyright 2005 - 2010 FUJITSU LIMITED

目　次

第1章 運用をはじめる前に....1
1.1 運用の流れ....1
1.2 機能に関する留意事項....2
1.2.1 機能全般....2
1.2.2 ユーザーポリシーの一元管理について....9
1.2.3 管理(統合管理)サーバへのクライアント(CT)の導入について....9
1.2.4 Windows Vista® 64ビット版、Windows® 7 64ビット版、Windows Server® 2008 64ビット版、Windows Server® 2008 R2について....10
1.2.5 持出しユーティリティ....10
1.2.6 暗号ファイルのメールソフトへの自動添付について....14
1.2.7 USBデバイス個体識別機能について....15
1.2.8 Systemwalker Desktop Rights Masterとの混在運用について....15
1.2.9 ファイル持出し禁止....15
1.2.10 印刷禁止....17
1.2.11 ログオン禁止....17
1.2.12 アプリケーション起動禁止....17
1.2.13 メール添付禁止....17
1.2.14 URLアクセス禁止....20
1.2.15 FTPサーバ接続禁止....20
1.2.16 Webダウンロード禁止....21
1.2.17 ログ全体....21
1.2.18 ファイル持出しログ....21
1.2.19 印刷操作ログ....22
1.2.20 ウィンドウタイトル取得ログ....24
1.2.21 メール送信ログ....24
1.2.22 コマンドプロンプト操作ログ....25
1.2.23 デバイス構成変更ログ....26
1.2.24 PrintScreenキー操作ログ....26
1.2.25 Citrix XenApp上での操作ログについて....26
1.2.26 Web操作ログ....27
1.2.27 FTP操作ログ....27
1.2.28 ファイル操作ログ....28
1.2.29 ログオン/ログオフログ....30
1.2.30 画面キャプチャ....30
1.2.31 クライアント(CT)の調査用ログの採取について....31
1.2.32 ログビューアでのファイル追跡機能について....31

第2章 運用環境を整える....32
2.1 運用環境を整えるときに考慮すること....32
2.1.1 ポリシーとは....32
2.1.2 ポリシー適用のしくみ....41
2.2 運用環境を整える流れ....49
2.3 管理コンソールを起動する....52
2.4 ポリシーの初期値を設定する....62
2.4.1 端末初期設定をおこなう....62
2.4.1.1 [各種ログスイッチ]タブの設定....63
2.4.1.2 [ファイル持出し禁止]タブの設定....66
2.4.1.3 [印刷禁止]タブの設定....73
2.4.1.4 [ログオン禁止]タブの設定....74
2.4.1.5 [アプリケーション起動禁止]タブの設定....76
2.4.1.6 [ファイル操作プロセス]タブの設定....78
2.4.1.7 [ファイル操作拡張子]タブの設定....82
2.4.1.8 [メール送信]タブの設定....83
2.4.1.9 [ログフィルタ条件]タブの設定....86
2.4.1.10 [画面キャプチャ条件]タブの設定....88

2.4.1.11 [エコ監視設定]タブの設定....90
2.4.1.12 [URLアクセス禁止]タブの設定....91
2.4.1.13 [FTPサーバ接続禁止]タブの設定....92
2.4.1.14 [Webダウンロード禁止]タブの設定....93
2.4.1.15 [その他設定]タブの設定....94
2.4.2 端末動作設定をおこなう....96
2.5 構成情報ツリーを作成する....101
2.5.1 Active Directoryから情報を取り込む....101
2.5.2 Systemwalker Desktop Patrolから情報を取り込む....108
2.5.3 管理コンソールで作成する....117
2.6 部門管理者を割り当てる....124
2.6.1 管理コンソールで部門管理者情報を出力する....130
2.7 Active Directoryでログオンスクリプトを設定する....131
2.8 ログを集計するための準備をする....139
2.8.1 状況画面を利用するための準備をする....139
2.8.2 ログアナライザを利用するための準備をする....144
2.8.2.1 ログの転送をスケジュールする....144
2.8.2.1.1 管理サーバでログ取得期間を設定する....145
2.8.2.1.2 管理サーバで転送スケジュールを設定する....146
2.8.2.1.3 ログアナライザサーバのデータベースにログを格納する....156
2.8.2.2 集計条件/レポート出力条件を設定する....168
2.8.2.2.1 ランキング表示数を設定する....171
2.8.2.2.2 絞込条件を設定する....172
2.8.2.2.3 集計対象から除外する項目を設定する....174
2.8.2.2.4 その他の条件を設定する....176
2.8.2.2.5 ログアナライザサーバを選択する....179

第3章 管理コンソールでポリシーを設定する....181
3.1 CT情報/ユーザー情報を検索する....181
3.2 グループポリシーを変更する....187
3.2.1 CTグループポリシーを変更する....188
3.2.2 ユーザーグループポリシーを変更する....190
3.3 CT/ユーザーをグループに割り当てる....193
3.3.1 CTを追加/移動/削除する....193
3.3.2 ユーザーを登録する....196
3.3.3 ユーザーを更新/移動/削除する....199
3.4 CTポリシー/ユーザーポリシーを変更する....201
3.4.1 CTポリシーを変更する....201
3.4.2 ユーザーポリシーを変更する....205
3.5 CT情報/ユーザー情報を出力する....208
3.6 クライアント(CT)を制御する....213
3.6.1 クライアント(CT)のサービスを制御する....213
3.6.2 クライアント(CT)のプロセスを制御する....215

第4章 クライアント(CT)操作の傾向をみる....219
4.1 状況画面で傾向を見る....220
4.1.1 状況画面を表示する....220
4.1.2 ログの集計結果を確認する....223
4.2 ログアナライザで傾向をみる....226
4.2.1 ログアナライザを起動する....226
4.2.2 情報漏洩のリスクを診断する....230
4.2.2.1 操作別集計結果を表示する....231
4.2.2.2 違反操作ワーストランキングを表示する....235
4.2.2.3 過去の日付けを特定して集計結果を表示する....235
4.2.3 目的別に集計する....235

第5章 ログビューアでクライアント(CT)での操作を監査する....242
5.1 ログビューアを起動する....242

5.2 ログを参照する....250
5.2.1 [CT操作ログ]画面で参照する....254
5.2.2 [設定変更ログ]画面で参照する....267
5.3 ファイル操作を追跡する....272
5.4 ログビューアでCT情報を検索する....280

第6章 監査資料を作成する....284
6.1 レポート出力ツールの活用方法....284
6.2 レポート出力ツールを起動する....286
6.3 情報漏洩分析レポート....287
6.3.1 情報漏洩分析レポートを出力する....287
6.3.2 情報漏洩分析レポートの内容....292
6.4 端末利用分析レポート....298
6.4.1 端末利用分析レポートを出力する....298
6.4.2 端末利用分析レポートの内容....301
6.5 違反操作分析レポート....302
6.5.1 違反操作分析レポートを出力する....302
6.5.2 違反操作分析レポートの内容....305
6.6 総合分析レポート....306
6.6.1 総合分析レポートを出力する....306
6.6.2 総合分析レポートの内容....308
6.7 印刷量監査レポート....312
6.7.1 印刷量監査レポートを出力する....313
6.7.2 印刷量監査レポートの内容....316
6.8 レポート出力スケジュールを設定する....324

第7章 運用環境を変更する....330
7.1 構成情報の取り込み方を変更する....330
7.2 ユーザー情報の管理方法を変更する....332
7.3 システム構成を2階層から3階層へ変更する....334
7.4 3階層のシステム構成で管理サーバを追加/削除する....340
7.5 指定したUSBデバイスだけにファイルを持ち出す....345
7.6 ログの保存期間を変更する....355
7.7 CT環境を変更する....356
7.7.1 接続先の管理サーバ/統合管理サーバを変更する....356
7.7.2 クライアント(CT)の動作設定を変更する....361
7.8 管理コンソール環境を変更する....365
7.9 管理サーバ環境を変更する....367
7.9.1 サーバ設定ツールを起動する....367
7.9.2 初期管理者のパスワードを変更する....370
7.9.3 管理者通知を変更する....370
7.9.4 管理サーバ/統合管理サーバのIPアドレス/コンピュータ名の変更に伴ってシステム環境を変更する....371
7.9.5 管理サーバの通信情報を変更する....394
7.9.6 保存先フォルダを変更する....396
7.9.7 管理サーバ/統合管理サーバの移行に伴ってログアナライザ設定を移行する....396
7.10 管理サーバのデータベースを再構築する....397
7.11 ログアナライザサーバ環境を変更する....403
7.11.1 ログアナライザサーバを移行する....403
7.11.2 ログアナライザサーバのIPアドレス/ポート番号を変更する....404

第8章 設定できるポリシー....406
8.1 禁止機能のポリシーの設定....406
8.1.1 ファイル持出し禁止....406
8.1.2 ファイル読み込み禁止....409
8.1.3 印刷禁止....410
8.1.4 ログオン禁止....412
8.1.5 アプリケーション起動禁止....414
8.1.6 メール添付禁止....416

8.1.7 PrintScreenキー禁止 418
8.1.8 URLアクセス禁止 420
8.1.9 FTPサーバ接続禁止 422
8.1.10 Webダウンロード禁止 424
8.2 記録機能のポリシーの設定 426
8.2.1 アプリケーション起動ログ 429
8.2.2 アプリケーション終了ログ 429
8.2.3 アプリケーション起動禁止ログ 430
8.2.4 ウィンドウタイトル取得ログ 431
8.2.5 メール送信ログ 433
8.2.6 メール送信中止ログ 435
8.2.7 メール添付禁止ログ 436
8.2.8 コマンドプロンプト操作ログ 437
8.2.9 デバイス構成変更ログ 438
8.2.10 印刷操作ログ 440
8.2.11 印刷禁止ログ 441
8.2.12 ログオン禁止ログ 442
8.2.13 ファイル持出しログ 443
8.2.14 PrintScreenキー操作ログ 445
8.2.15 PrintScreenキー禁止ログ 446
8.2.16 Web操作ログ 447
8.2.17 Web操作禁止ログ 448
8.2.18 FTP操作ログ 449
8.2.19 FTP操作禁止ログ 450
8.2.20 ファイル操作ログ 451
8.2.21 ログオン/ログオフログ 456
8.2.22 連携アプリケーションログ 460
8.2.23 設定変更ログ 461

付録A 集計目的一覧 462

付録B 複合機と連携して情報を可視化する 467
B.1 運用パターン 467
B.2 動作環境 467
B.3 制限事項・注意事項 468
B.4 導入 468
B.5 使用方法 468
B.5.1 用紙代・CO2排出量の算出に必要な係数を設定する 468
B.5.2 複合機の用紙使用状況レポートを出力する 468
B.5.3 複合機の用紙使用状況レポートの内容 472

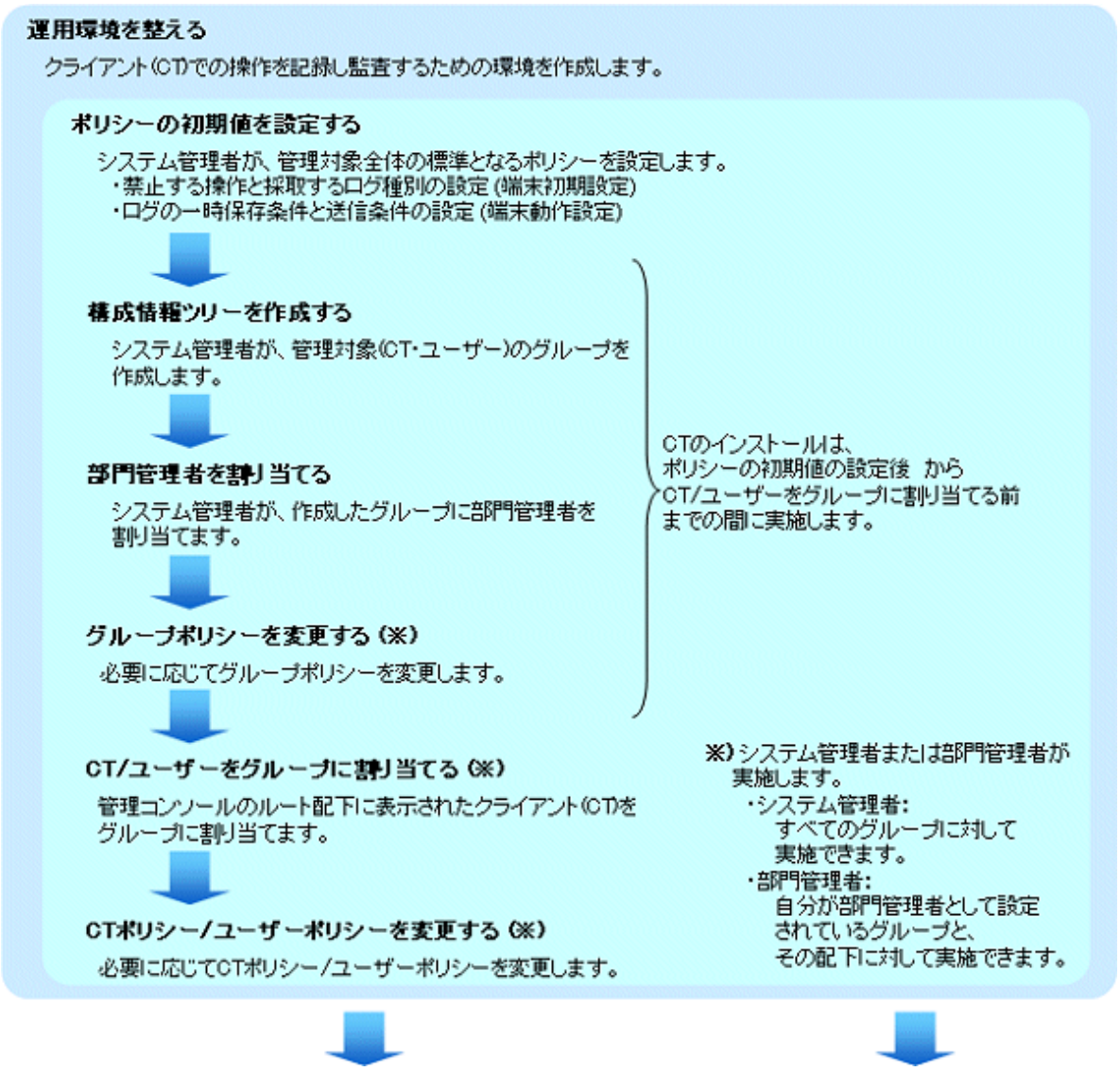
索引 477

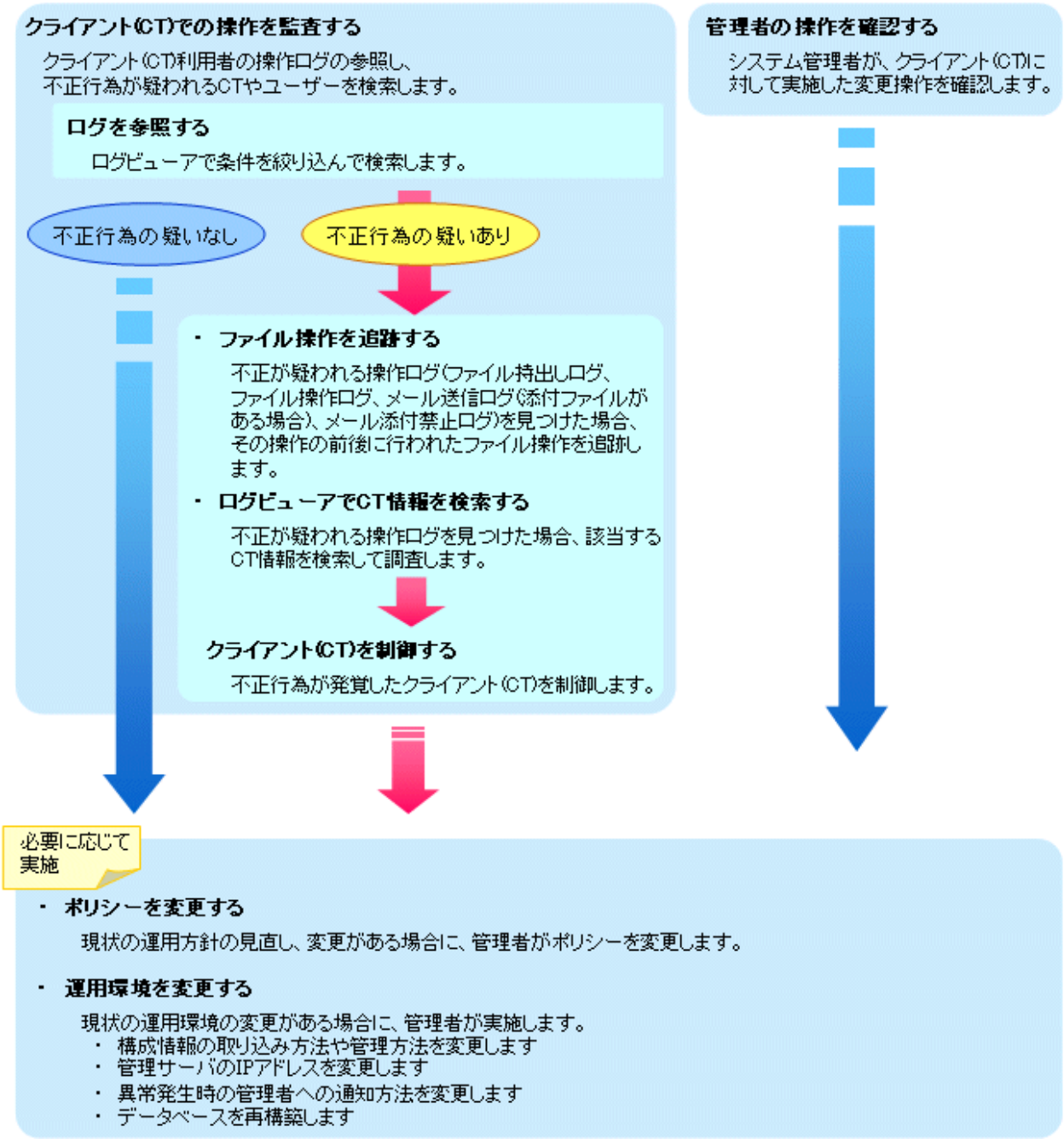
第1章 運用をはじめる前に

本章では、システム管理者、部門管理者、およびクライアント(CT)利用者の操作概要を、Systemwalker Desktop Keeperの運用の流れに沿って説明します。

1.1 運用の流れ

運用全体の流れを以下に示します。





1.2 機能に関する留意事項

1.2.1 機能全般

- 内臓ディスクでもOSがリムーバブルドライブと判断した場合、ローカルドライブではなくリムーバブルドライブとしてログが採取され、抑止動作も行われます。
- Windows Server® 2008でマルチログオン利用時の場合、メール送信時あて先確認画面、メール添付禁止画面は表示されません。このとき、メール送信時の動作は以下のようになります。

  ー あて先が除外ドメインのアドレスのみのメールについては従来からメッセージを表示せずに送信するため、変更ありません。

ー あて先に除外ドメイン以外のアドレスが含まれるメールについては、メール添付禁止の判定を実施します。メール添付禁止の判定結果によって、以下の動作となります。

- 禁止ファイルが添付されていた場合、メール添付禁止画面を表示せずに送信を中止します。
- 禁止ファイルが添付されていない場合、あて先確認画面を表示せずにそのまま送信します。

・ Windows® XPの「ユーザーの簡易切り替え」、Windows Server® 2003のマルチログオン利用時は、Systemwalker Desktop Keeperが導入されていても、禁止機能や記録機能は動作しません。

Windows Vista®、Windows Server® 2008またはWindows® 7の場合は、複数のユーザーが同時に使用しているときのポリシー状態は、以下のとおりです。

機能		有効になるポリシー
ログ (記録機能)	アプリケーション起動/終了	ユーザーポリシーで動作
	ウィンドウタイトル取得	ユーザーポリシーで動作
	メール送信	CTポリシーで動作
	メール送信中止	CTポリシーで動作
	コマンドプロンプト操作	ユーザーポリシーで動作
	デバイス構成変更	ユーザーポリシーで動作
	印刷操作	ユーザーポリシーで動作
	ファイル持出し	ユーザーポリシーで動作
	PrintScreenキー操作	ユーザーポリシーで動作
	Web操作	ユーザーポリシーで動作
	FTP操作	ユーザーポリシーで動作
	ファイル操作	CTポリシーで動作
	ログオン/ログオフ	CTポリシーで動作
	連携アプリケーション	ユーザーポリシーで動作
禁止機能	アプリケーション起動禁止	ユーザーポリシーで動作
	印刷禁止	ユーザーポリシーで動作
	PrintScreenキー禁止	ユーザーポリシーで動作
	ログオン禁止	CTポリシーで動作
	メール添付禁止	CTポリシーで動作
	ファイル持出し禁止	CTポリシーで動作
	ファイル読み込み禁止	CTポリシーで動作
	URLアクセス禁止	ユーザーポリシーで動作
	FTPサーバ接続禁止	ユーザーポリシーで動作
	Webダウンロード禁止	ユーザーポリシーで動作

・ Windows® 2000、Windows® XP、Windows Server® 2003の場合、クライアント(CT)は、ターミナルサービス、リモートデスクトップ、TS Remote APPについては、対応していません。
ただし、Citrix XenApp 監視ではターミナルサービス、リモートデスクトップに対応しています。

・ クライアント(CT)のOSがWindows Vista®、Windows Server® 2008またはWindows® 7で、コマンドプロンプトや持出しユーティリティを管理者として実行した場合、「要求されたリソースは使用中です」のメッセージが出力され、起動できない場合があります。この場合は、しばらくたってから起動するようにしてください。

・ Webコンソール使用中は、ブラウザの[戻る]ボタンを使用しないでください。使用すると、エラーや正常に表示できない可能性があります。

・ 同じユーザーIDでWindowsに同時にログオンできる設定を行わないでください。ログが区別できなくなります。

Systemwalker Desktop Keeperで扱う文字コードについて

Systemwalker Desktop Keeperで扱える文字コードは、以下の2種類です。これら以外の文字コードは、「?」に変換されます。

・ SJIS

正しく表示されます。

・ UNICODE

正しく表示できる場合と、「?」やエスケープした表現(具体的には、“ꪪ”という表現で、AAAA部分は4ケタまたは5ケタの16進コードです)に変換される場合とがあります。

CTにおけるUNICODE文字の対応

クライアント(CT)で採取された操作ログ、禁止ログにUNICODE文字が含まれていた場合、全角1文字のUNICODE文字が、エスケープ化された表現(具体的には、“ꪪ”という表現で、AAAA部分は4ケタまたは5ケタの16進コードです)に変換して記録されます。そのため、ログとして記録可能な文字数が短くなります。 エスケープ化された表現で記録した文字は、ログビューアでは、UNICODE文字として表示されます。

なお、記録するログについて、エスケープ化された表現で記録する項目と、UNICODE文字を?のまま記録する項目があります。

採取されるログの種類		記録されている項目	ログの記録パターン
共通	－	ユーザー名	A
	－	ドメイン名	A
操作ログ	アプリケーション起動ログ	アプリケーション名	B
	アプリケーション終了ログ	アプリケーション名	B
	ウィンドウタイトル取得ログ (URLを含みます)	ウィンドウタイトル名	A
		アプリケーション名	B
		URL情報	A
	メール送信ログ	全体	A
	メール送信中止ログ	メールアドレス	A
		メールのタイトル	A
		送信元アドレス	A
		送信先アドレス(To、Cc、Bccの情報)	A
		添付ファイル名	A
	デバイス構成変更ログ	ドライブレター ドライブの種別	－
		ボリューム名	B
		デバイス名	B
		内部シリアル番号	B
	印刷操作ログ	ドキュメント名	A
		プリンタ名	A
	ファイル持出しログ		×
	PrintScreenキー操作ログ		－

採取されるログの種類		記録されている項目	ログの記録パターン
	Web操作ログ	Webページを表示したアプリケーション名	B
		アクセス先のURL文字列	－
		ファイル名	A
	FTP操作ログ	FTPクライアントプログラム名	B
		FTPサーバのIPアドレス	－
		ファイル名	A
	ファイル操作ログ	ファイル名	A
		アプリケーション名	B
	ログオン/ログオフログ		－
	連携アプリケーションログ	全体	B
	コマンドプロンプト操作ログ	実体ログ	B
	設定変更ログ		B
禁止ログ	アプリケーション起動禁止ログ	アプリケーション名	×
	メール添付禁止ログ	ファイル名	A
		アプリケーション名	A
	印刷禁止ログ	ファイル名	A
		アプリケーション名	A
	ログオン禁止ログ	ユーザー名	A
	PrintScreenキー禁止ログ		－
	Web操作禁止ログ	Webページを表示したアプリケーション名	B
		アクセス先のURL文字列	－
	FTP操作禁止ログ	FTPクライアントプログラム名	B
		FTPサーバのIPアドレス	－

Windows Vista®、Windows Server® 2008、Windows® 7以外のOSでログにUNICODE文字が含まれる場合、表と異なるパターンでログが記録される場合があります。

A：UNICODE文字をエスケープした表現に変換して記録します。
B：UNICODE文字を「?」記号で記録します。
－：文字の記録はありません。
×：UNICODE文字は入力できません。このため、UNICODE文字を含む該当項目の禁止や、ログの採取はできません(ポリシーとして設定できません)

Windows® 2000、Windows® XP、またはWindows Server® 2003のクライアント(CT)で採取された操作ログ、禁止ログにUNICODE文字が含まれていた場合、?に変換して記録されます。?に変換して記録された文字は、ログビューアはそのまま?で表示します。

持出しユーティリティの操作では、UNICODE文字の入力、表示はできません。
持出しユーティリティの持ち出し元のファイルまたはフォルダの指定で、持ち出すファイルまたはフォルダの上位階層のフォルダ名にUNICODE文字が含まれる場合、持ち出し元ファイルまたはフォルダとして指定できません。

管理コンソールにおけるUNICODE文字の対応

管理コンソールでの操作は、UNICODE文字の入力、表示はできません。

管理コンソールで、クライアント(CT)のプロセス情報取得時に、プロセス名にUNICODE文字が含まれていた場合、その文字は「?」記号に変換されます。「?」記号で表示されたプロセス名を選択してプロセス停止操作を行った場合、それらがUNICODE文字で表示された場合に異なるプロセス名であったとしても、管理コンソール画面上で同じ名前として表示されているプロセスは、すべて停止します。

管理コンソール([端末初期設定]画面)での設定項目(タブ名)	項目	UNICODE文字の扱い
ファイル持出し禁止		―
印刷禁止	印刷許可アプリケーションEXE名	×
	PrintScreenキー無効化	―
ログオン禁止		―
アプリケーション起動禁止	起動禁止アプリケーションEXE名	×
ファイル操作プロセス	プロセスEXE名	×
	フォルダ名 (ファイル操作ログ取得除外フォルダ)	× エスケープ化した文字を指定しても、除外動作は有効にはなりません。
ファイル操作拡張子	拡張子名	×
メール送信	拡張子名	× ただし、エスケープ化した文字を指定した場合は、UNICODE文字が含まれる拡張子を禁止できます。
	ドメイン名	× エスケープ化した文字を指定してもUNICODEとは認識しません。
ログフィルタ条件	重複ログフィルタ設定	A 同じプロセスで同じウィンドウタイトルのログかどうかは、エスケープ化した文字で比較されます。
	キーワード	A UNICODE文字の指定はできません。 ただし、ウィンドウタイトルの比較は、エスケープ化した文字が使用されているウィンドウタイトル名で実施します。
	プロセスEXE名	×
画面キャプチャ条件	キーワード	A UNICODE文字の指定はできません。 ただし、ウィンドウタイトルの比較は、エスケープ化した文字が使用されているウィンドウタイトル名で実施します。
	プロセスEXE名	×
エコ監視設定		―
URLアクセス禁止	URL文字列	× エスケープ化した文字を指定してもUNICODEとは認識しません。
FTPサーバ接続禁止		―

管理コンソール([端末初期設定]画面)での設定項目(タブ名)	項目	UNICODE文字の扱い
Webダウンロード禁止	URL文字列	× エスケープ化した文字を指定してもUNICODEとは認識しません。
その他設定		―

A:UNICODE文字をエスケープ化した表現に変換して表示します。
B:UNICODE文字を「?」記号で表示します。
―:画面から文字を入力してポリシーを設定する項目はないため、影響ありません。
×:UNICODE文字は入力できません。このため、UNICODE文字を含む該当項目の禁止や、ログの採取はできません(ポリシーとして設定できません)。

ログビューアにおけるUNICODE文字の対応

ログビューアでの操作は、UNICODE文字の入力はできません。

採取したログを表示する場合の、UNICODE文字の対応について以下に示します。

「記録されている項目」とは、ログビューアのログ一覧の[内容]欄に表示される項目を意味しています。

採取されるログの種類		記録されている項目	UNICODE文字の扱い	
			CSVファイル	Webコンソール
共通	―	ユーザー名	A	C
	―	ドメイン名	A	C
操作ログ	アプリケーション起動ログ	アプリケーション名	B	B
	アプリケーション終了ログ	アプリケーション名	B	B
	ウィンドウタイトル取得ログ(URLを含みます)	ウィンドウタイトル名	A	C
		アプリケーション名	B	B
		URL情報	A	C
	メール送信ログ	全体	A	C
	メール送信中止ログ	メールアドレス	A	C
		メールのタイトル	A	C
		送信元アドレス	A	C
		送信先アドレス(To、Cc、Bccの情報)	A	C
		添付ファイル名	A	C
	デバイス構成変更ログ	ドライブレター ドライブの種別	―	―
		ボリューム名	B	B
		デバイス名	B	B
		内部シリアル番号	B	B
	印刷操作ログ	ドキュメント名	A	C
		プリンタ名	A	C
	ファイル持出しログ		×	×
	PrintScreenキー操作ログ		―	―

採取されるログの種類		記録されている項目	UNICODE文字の扱い	
			CSVファイル	Webコンソール
	Web操作ログ	Webページを表示したアプリケーション名	B	B
		アクセス先のURL文字列	×	×
		ファイル名	A	C
	FTP操作ログ	FTPクライアントプログラム名	B	B
		FTPサーバのIPアドレス	×	×
		ファイル名	A	C
	ファイル操作ログ	ファイル名	A	C
		アプリケーション名	B	B
	ログオン/ログオフログ		―	―
	連携アプリケーションログ	全体	B	B
	コマンドプロンプト操作ログ	実体ログ	B	B
	設定変更ログ		B	B
禁止ログ	アプリケーション起動禁止ログ	アプリケーション名	×	×
	メール添付禁止ログ	ファイル名	A	C
		アプリケーション名	A	C
	印刷禁止ログ	ファイル名	A	C
		アプリケーション名	A	C
	ログオン禁止ログ	ユーザー名	A	C
	PrintScreenキー禁止ログ		―	―
	Web操作禁止ログ	Webページを表示したアプリケーション名	B	B
		アクセス先のURL文字列	×	×
	FTP操作禁止ログ	FTPクライアントプログラム名	B	B
		FTPサーバのIPアドレス	×	×

A：UNICODE文字をエスケープした表現に変換して表示します。
B：UNICODE文字を「?」記号で表示します。
C：UNICODE文字で表示します。
―：該当する項目には固定値が表示されます。
×：UNICODE文字は扱えません。
「ファイル持出しログ」については、UNICODE文字を含むファイルの、持出し画面への登録はできません。
「アプリケーション起動禁止ログ」については、UNICODE文字を含むアプリケーション名は禁止できないため、ログは採取できません。

Webでログビューアを参照するPCのOSによって、状況が異なります。

Windows® 2000の場合：

UNICODE文字が表示されない場合があります。

Windows® XP、Windows Server® 2003の場合:

UNICODE文字をJIS2004フォントで表示する場合またはJIS2004固有の文字を表示する場合、マイクロソフト社のホームページからJIS2004対応フォントパッケージをインストールする必要があります。インストールしていない場合は、正常にUNICODE文字が表示されません。
その他のOSではインストールの必要はありません。

その他のツールにおけるUNICODDE文字の対応

- サーバ設定ツールなどのサーバ系のツールや、Systemwalker Desktop Keeperが提供するコマンドでは、UNICODE文字の入力、表示はできません。
- Active Directory連携コマンドでは、UNICODE文字を含むユーザーや組織情報は、取り込みません。
- Systemwalker Desktop Patrol構成情報取り込みコマンド、管理コンソールのDesktop Patrol連携機能では、UNICODE文字を含むデータファイルを使用できません。

Windowsへのログオン時のユーザー名にUNICODE文字が含まれる場合

- 以下に示す管理サーバのツールやコマンドを実行すると、管理者権限がないと判断されるため、起動できません。
  - 運用環境保守ウィザード(環境構築・削除)
  - 運用環境保守ウィザード(情報表示・再構築)
  - サーバ設定ツール
  - バックアップツール
  - リストアツール
  - Active Directoryとの連携コマンド
  - Systemwalker Desktop Patrol構成情報取り込みコマンド
  - 旧版データベースの変換コマンド
  - データ移行コマンド
- ファイル操作ログ取得除外フォルダとして指定する[インターネット一時ファイルのフォルダ]および[Tempフォルダ]は有効とならず、ファイル操作ログが採取されます。
- ユーザーポリシーは、UNICODE文字に対応していないため、ユーザーポリシーが適用されていない状態でクライアント(CT)が動作します。
- 持出しユーティリティを使用してCD/DVDメディアへの暗号化持ち出しは、できません。

1.2.2 ユーザーポリシーの一元管理について

統合管理サーバと管理サーバ間で、ネットワークの不具合などにより通信できない場合に、管理コンソールを管理サーバに接続して各種設定を行ったとしても、統合管理サーバと管理サーバ間の通信が再開したときには、管理サーバに設定した内容は、統合管理サーバでの設定で上書きされます。

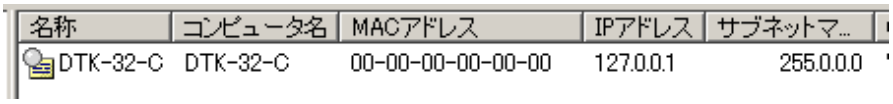
管理コンソールなどの管理ユーザーも統合管理サーバで一元管理されます。

1.2.3 管理(統合管理)サーバへのクライアント(CT)の導入について

- 持出し禁止設定で、ドライブ種別が「固定」のハードディスクに対する持出し禁止ポリシーを設定しても持出し禁止されません。これは誤って管理(統合管理)サーバの固定ハードディスクに持出し禁止設定し、管理(統合管理)サーバが正常に動作しなくなるのを予防するためです。

・ ログオン禁止設定が有効となりません。これは誤って管理(統合管理)サーバにログオン禁止を設定し、管理(統合管理)サーバが正常に動作しなくなるのを予防するためです。

・ 管理(統合管理)サーバにクライアント(CT)を導入した場合、そのクライアント(CT)は管理コンソールではMACアドレスが00-00-00-00-00-00、IPアドレスが127.0.0.1、サブネットマスクは255.0.0.0と表示されます。



・ 保守コマンドを入力した場合に、以下のどちらかのメッセージが表示される場合がありますが、異常ではありません。

　－「NBT リモート キャッシュ ネーム テーブルを正常に削除し、事前に読み込みました。」

　－「Successful purge and preload of the NBT Remote Cache Name Table.」

1.2.4 Windows Vista® 64ビット版、Windows® 7 64ビット版、Windows Server® 2008 64ビット版、Windows Server® 2008 R2について

・ 管理コンソールの[プロセス一覧取得/制御]機能において、クライアント(CT)がWindows Vista® 64ビット版、Windows® 7 64ビット版、Windows Server® 2008 64ビット版、Windows Server® 2008 R2の場合は、64ビットアプリケーションのプロセス一覧を参照する事はできません。また、プロセスを終了させる事もできません。

1.2.5 持出しユーティリティ

ファイル持出しについて

・ 持出しユーティリティでファイルを持ち出す場合、以下のディスク空き容量が、システムのテンポラリのあるドライブ(通常は起動ドライブ)に必要です。

持出し先ドライブ		原本保管しない場合		原本保管する場合(注1)	
		通常(平文)持出しするとき	暗号化持出しするとき	通常(平文)持出しするとき	暗号化持出しするとき
CD/DVD		実際に持ち出すファイル容量の1.5倍以上	実際に持ち出すファイル容量の3倍以上	実際に持ち出すファイル容量の2.5倍以上	実際に持ち出すファイル容量の4倍以上
CD/DVD以外	システムドライブではない場合(注2)	必要ありません	実際に持ち出すファイル容量の1.5倍以上	実際に持ち出すファイルと同じ容量	実際に持ち出すファイル容量の2.5倍以上
	システムドライブの場合	実際に持ち出すファイルと同じ容量	実際に持ち出すファイル容量の2.5倍以上	実際に持ち出すファイル容量の2倍以上	実際に持ち出すファイル容量の3.5倍以上

注1) 原本保管する場合、上記の表で説明した容量に加えて、原本ファイルの大きさ分の容量が、クライアント(CT)のログフォルダに必要です。

注2) 以下の条件をすべて満たしているドライブを指します。

　－ CD/DVDドライブ以外

　－ Windowsのシステムが入っているドライブ(一般的にはCドライブ)以外

・ 持出しユーティリティでファイルを持ち出す場合、起動ドライブの空き容量の推奨値は、通常(平文)持ち出し時には1GB以上、暗号化持ち出し時には2GB以上です。

CD-R/RWメディアまたはDVD-R/RWメディアへのファイル持出しについて

- UNICODE固有文字(SJISに変換できない文字)が含まれるユーザー名でログインしている場合、CDまたはDVDメディアへの暗号化持ち出しは行えません。
- 持出しユーティリティで、CD-R/RWまたはDVD-R/RWへファイルを持ち出せるOSは、以下のとおりです。ただし、使用するCD-R/RW機器またはDVD-R/RW機器がサポート対象としているOSに限ります。

  【CD-R/RWへのファイル持出し】

  - Windows® 7 Ultimate
  - Windows® 7 Enterprise
  - Windows® 7 Professional
  - Windows® 7 Home Premium
  - Microsoft® Windows® XP Professional(ServicePack2以降)
  - Microsoft® Windows® XP Home Edition(ServicePack2以降)
  - Microsoft® Windows Vista® Home Basic
  - Microsoft® Windows Vista® Home Premium
  - Microsoft® Windows Vista® Business
  - Microsoft® Windows Vista® Enterprise
  - Microsoft® Windows Vista® Ultimate

  Windows® XPの場合、セーフモードで起動したときは、CDメディアへの持出しおよび消去は行えません。

  【DVD-R/RWへのファイル持出し】

  - Windows® 7 Ultimate
  - Windows® 7 Enterprise
  - Windows® 7 Professional
  - Windows® 7 Home Premium
  - Microsoft® Windows Vista® Home Basic
  - Microsoft® Windows Vista® Home Premium
  - Microsoft® Windows Vista® Business
  - Microsoft® Windows Vista® Enterprise
  - Microsoft® Windows Vista® Ultimate
- CD-R/RWメディアまたはDVD-R/RWメディアへのファイル持出し機能を使用する場合、事前にPCと使用するCD-R/RW機器やDVD-R/RW機器、およびメディアを使用して動作検証を行った上で運用してください。
- CD/DVD持出し機能を使用する場合、ライティングソフト、パケットライトソフトがインストールされていると、持出しユーティリティでのCD/DVD書き込み機能が正常に動作しない可能性があります。持出しユーティリティでCD-R/RWまたはDVD-R/RWへ持ち出しを行う場合は、導入済みのライティングソフト、パケットライトソフトはアンインストールしてください。
- 持出しユーティリティからCD/DVD書き込みを行う場合、省電力機能に対応していないため、常に電源オンの設定にしてください。システムスタンバイ、スリープ、休止状態になると、メディアが使用不可能になるなどの問題が発生する可能性があります。また、休止状態にした場合、書き込み完了メッセージが表示されますが、実際にはメディアへの書き込みは正常に行われていない場合があります。
- CD/DVDデバイスを初めてPCに接続し、そのPCから接続したCD/DVDデバイスのCD-R/RWメディアまたはDVD-R/RWメディアへのファイル持出し機能を使用する場合は、一度OSを再起動してCD-R/RWメディアまたはDVD-R/RWメディアへのファイル持出し機能を使用してください。再起動しない場合はCD-R/RWメディアまたはDVD-R/RWメディアへの書き込みが正常に動作しない場合があります。

ー 持出しユーティリティからの新規CD書き込み機能は、ストリーム書き込み方式でのCD書き込み機能を提供します(CDFS(Joliet方式)でのセッションアットワンス書き込み)。

【書き込めるファイル】

- ファイル名:最大64文字(半角・全角とも1文字)(拡張子を含む)
- ディレクトリ名:最大64文字(半角・全角とも1文字)(拡張子を含む)
- フルパス長:最大240バイト(フォルダの区切り文字は1バイト、ファイル・フォルダ名は1文字2バイトとしてカウント。ドライブレターは1文字2バイトでカウント(例:C:は4バイト))

ー 持出しユーティリティからのCD/DVD持出し機能は、ボリュームラベルを含む一切の情報が記録されていないブランクメディアだけ対象とします。

【ブランクメディアの定義】

- 購入直後の未フォーマットのCD-R、CD-RW、DVD-R、DVD-RWメディア
- 一度書き込みを行い、持出しユーティリティによりCD-RW/DVD-RW消去を行ったCD-RWメディアまたはDVD-RWメディア

ー 以下のメディアにはファイル持出しができません。

- パケットライト書き込みのために、ディスクをUDFフォーマットした場合(中にファイルがない場合を含む)
- ストリーミング書き込みのために、ディスクをCDFSフォーマットした場合(中にファイルがない場合を含む)

ー 持出しユーティリティでのCD/DVD持出し機能が対象とするドライブの種別・接続方式・メディアは、以下のとおりです。

- ドライブ接続方式
  ATAPI、USB 1.1/2.0、IEEE1394
- メディア
  CD-R/RW(700MBまでサポート)、DVD-R/RW(4.7GBまでサポート)

メディア別の、持出しユーティリティでの使用可否、持出し禁止可否については、以下のとおりです。

持出しユーティリティでの操作/機能		CD-R	CD-RW	DVD-R	DVD-RW	DVD-R DL (注1)	DVD+R	DVD +RW	DVD+R DL (注2)	DVD +RAM (注3)
書き込み	Windows® XP(注4)	○	○	×	×	×	×	×	×	×
	Windows Vista®	○	○	○	○	×	×	×	×	×
	Windows® 7	○	○	○	○	×	×	×	×	×
消去	Windows® XP(注4)	×	○	×	×	×	×	×	×	×
	Windows Vista®	×	○	×	○	×	×	×	×	×
	Windows® 7	×	○	×	○	×	×	×	×	×
持出し禁止		○	○	○	○	○	○	○	○	○

○:可能です。
×:不可能です。
注1) DVD-R Dual Layerのことです。
注2) DVD+R Dual Layerのことです。
注3) リムーバブルディスクとして認識される場合を除きます。
注4) 64ビット版には対応していません。

ー Blu-ray、HD DVDへの対応はしていません。

ー Windows® XPの場合、CD持出し機能を使用するためには、IMAPIサービス(IMAP CD-Burning COM Service)がシステムにインストールされ、サービスの状態が“無効”以外になっている必要があります。

ー 書き込みの際、メディアに対してボリュームラベルを指定できます。ボリュームラベルには、A～Z、0～9、_(アンダースコア)を使用でき、最大16文字を指定できます。

- 持出しユーティリティからのCD/DVD持出し機能は、クローズ処理を行いません(ただし、DVD-Rの場合はクローズされます)。したがって、そのメディアに対してCD/DVD書き込み禁止を行っていないPCからエクスプローラ、ライティングソフトを使用して追記できます。ただし、ファイル持出しユーティリティからは、一切の情報が記録されていないメディアに対する書き込みしかサポートしないため、追記はできません。また、未クローズ状態のため、クローズ済みのメディアしか扱えないユニットでは読み込みできません。
- 持出しユーティリティからのCD/DVD持出し機能は、持ち出し元のファイルサイズ合計が、持ち出し先のメディアの容量を超えた場合、書き込みは行えません(マルチボリュームに対応していません)。
- 本機能によって書き込むことができるデータサイズは、書き込むメディア、書き込むファイル数、フォルダ構成によって異なります。
- 書き込みするファイルが複数存在する場合、フォルダ構成やファイル名などの情報の領域が必要になるため、メディアで許容されている最大書き込み可能なサイズまで書き込めない場合があります。
- 持出しユーティリティからCD/DVD持出しを行う場合、ユーザーのテンポラリ領域にワークファイルを書き込みます。ユーザーのテンポラリ領域は、起動ドライブから変更しないでください。
- ライティングソフトから書き込み中に、ポリシーが変更された(CD/DVDへの書き込みを不可にする)場合、媒体不良などになる可能性があります。
- 消去には、クイック消去と完全消去の2種類があります。クイック消去はPMA(Program Memory Area)とTOC(Table Of Contents)領域だけを消去し、完全消去はすべての領域を完全に消去します。
- 持出しユーティリティでのファイル操作ログは取得できません。
- ライティングソフトによっては、禁止中の書き込み動作が、一見正常に書き込み終了したように見えることがあります(ただし、ディスクへの書き込みは行われていません)。
- クライアント(CT)のインストーラにてOSがWindows® XPの場合、IMAPIサービス(IMAPI CD-Burning COM Service)が無効以外になっていた場合、「手動」に変更します(クライアント(CT)のアンインストーラでは、IMAPIサービス(IMAPI CD-Burning COM Service)の設定を変更しません)。
- 持出しユーティリティのCD/DVD持出し機能を利用してCD/DVD書き込みを行う場合、使用しているPCに対応したCD/DVDドライブユニット、メディアを使用してください。
- 持出しユーティリティで大量のファイルを持ち出す場合、持出しログが出力されるのに時間を要することがあります(目安:1万件の持ち出しで10分程度)。
- 書き込みの速度は、ドライブユニットとメディアでサポートされている倍速のうち遅い方の速度になります。
- CD-R/RWメディアまたはDVD-R/RWメディアの記録面に指紋や汚れ、ほこり、傷などがつくと、データの書き込み、消去が正常に行えなくなる場合があります。
- 書き込みでクローズ処理が行われているメディアは、メディアタイプがCDメディアの場合CD-ROMと表示され、DVDメディアの場合DVD-ROMとして表示されます。
- 消去できないメディアで、かつ、すでに書き込みされている場合、メディア消去画面で表示されるDISK全体容量が、正しく表示されないことがあります。

暗号ファイルの作成について

復号可能期限は、2037/12/31までサポートしています。復号可能期限が2037/12/31を超える暗号ファイルは、作成することができません。

暗号ファイルの復号について

- ファイルを復号するPCのテンポラリフォルダが書き込み禁止の場合、暗号ファイルを復号することはできません。
- 復号前に暗号ファイルをコピーした場合、コピーした暗号ファイルもオリジナルファイルと同様に復号できます。オリジナルファイルと同回数のパスワード試行が可能です。また、復号可能日数内であれば、復号できます。
  また、パスワード試行が5回可能な暗号ファイルを3回失敗した状態でコピーした場合、コピーしたファイルの失敗回数は、オリジナルファイルの失敗回数(3回)が引き継がれます。

オリジナルファイルの復号時に、パスワード試行回数に達したり、復号可能日数を超えたりしたために削除された場合でも、コピーしたファイルは削除されません。コピーしたファイルは、復号時に、パスワード試行回数に達したり、復号可能日数を超えたりした場合に削除されます。

- 暗号ファイルを削除できない媒体(CD/DVD、ライトプロテクトされたフロッピーディスクやUSBメモリなど)に暗号ファイルを持ち出した場合は、復号時に、パスワード試行回数に達したり、復号可能日数を超えたりしても削除されません。この場合、メッセージは表示されずに復号プログラムが終了します。
- 復号可能日数は、ポリシーで指定した日数をもとに、暗号ファイル作成時にクライアント(CT)で計算した日付が設定されます。
  復号可能であるかどうかは、復号時に使用するクライアント(CT)の日付から判断します。クライアント(CT)の日付が正しくない場合は、復号できない場合があります。
- 暗号化ファイルの削除機能が有効になるのは、ファイルに対して削除可能な状態(削除権限があるなど)にある場合だけです。メールに自己復号型暗号ファイルを添付した場合も同様です。
- パスワードの試行回数は、自己復号ファイルが書き込みできない状態にある場合、正しく動作しません。
- 持出しユーティリティで暗号化したファイルを復号する場合、復号する環境では、環境変数で設定したドライブを書き込み可能な状態にしておいてください。環境変数で設定したドライブが、書き込みできない状態の場合、復号処理を行えません。

1.2.6 暗号ファイルのメールソフトへの自動添付について

- 本機能は、「持出しユーティリティを使用して自己復号型暗号ファイルを作成し、メールに添付する」操作を自動化したものです。
  自動添付される暗号ファイルは、持出しユーティリティで作成する自己複号型暗号ファイルと同じ形式のファイルです。
- 暗号ファイルの作成および復号に関する留意事項は、「持出しユーティリティ」の暗号ファイルと同じです。
- 暗号ファイルは、ログオンユーザーの一時フォルダ(テンポラリフォルダ)配下の、暗号処理ごとに作成されたフォルダ内に配置されます。暗号処理ごとに作成されるフォルダで個別管理されるため、同名の暗号化ファイルがある場合でも、上書きされることはありません。

```
C:¥Documents and Settings¥＜ユーザー名＞¥Local Settings(または¥AppData¥Local)¥Temp¥fsw01ej8¥〈暗号処理ごとに作成される暗号フォルダ〉 ・・
```

- 環境変数TMP、TEMP、USERPROFILEが存在しない場合、または環境変数TMP、TEMP、USERPROFILEが指定しているフォルダがシステムフォルダの場合は、本機能は使用できません。
- 暗号ファイルは、ログオンユーザーが再度ログオンしたときに、削除されます。
  したがって、暗号化後、ログオンしている間にメールを送信する必要があります。
- 本機能は、メールソフトがMAPI(Messaging Application Program Interface)に対応している必要があります。
- 暗号ファイルが自動添付されるメールソフトは標準メールソフトとなります。標準のメールソフトが設定されていないPCでは、本機能を使用できません。
- 暗号ファイルの自動添付が可能なOSは以下のとおりです。
  Windows Vista® 64ビット版、Windows Server® 2008 64ビット版、Windows Server® 2008 R2、Windows® 7 64ビット版では、32bit互換モードで動作します。
  - Microsoft® Windows® XP Professional(ServicePack2以降)
  - Microsoft® Windows® XP Home Edition(ServicePack2以降)
  - Microsoft® Windows Server® 2003, Standard Edition
  - Microsoft® Windows Server® 2003 R2, Standard Edition
  - Microsoft® Windows Server® 2003, Enterprise Edition
  - Microsoft® Windows Server® 2003 R2, Enterprise Edition
  - Microsoft® Windows Vista® Home Basic
  - Microsoft® Windows Vista® Home Premium
  - Microsoft® Windows Vista® Business

- Microsoft® Windows Vista® Enterprise
- Microsoft® Windows Vista® Ultimate
- Windows® 7 Ultimate
- Windows® 7 Enterprise
- Windows® 7 Professional
- Windows® 7 Home Premium
- Microsoft® Windows Server® 2008 Standard
- Microsoft® Windows Server® 2008 Enterprise
- Microsoft® Windows Server® 2008 Standard without Hyper-V(TM)
- Microsoft® Windows Server® 2008 Enterprise without Hyper-V(TM)
- Microsoft® Windows Server® 2008 R2 Standard
- Microsoft® Windows Server® 2008 R2 Enterprise

1.2.7 USBデバイス個体識別機能について

・ USBデバイス個体識別機能を使用する場合、事前に使用するUSBデバイスを用いて動作検証を行った上で運用してください。

・ USBデバイス個体識別機能を使用する場合、USB接続の内蔵フロッピーディスクドライブも登録する必要があります。また、USB接続ではないフロッピーディスクドライブは個体識別ができないため、登録することができません。

・ 管理コンソールの[ファイル持出し禁止]タブにて、読み込み禁止、持出し禁止を一切設定しない場合、エクスプローラなどに対するUSBデバイス個体識別機能は動作しません。

  具体的には、[ファイル持出し禁止 - USBデバイス個体識別機能 - 詳細設定]画面の[使用可能USBデバイス一覧]に登録しているUSBデバイスの[アクセス設定]にて、[読み込み専用]、[読み書きともファイル持出しユーティリティに限定]、[書き込みはファイル持出しユーティリティに限定]を設定しても、エクスプローラなどからの読み込み、持ち出しは禁止されません。ファイル持出しユーティリティは、設定されたとおりの動作となります。

1.2.8 Systemwalker Desktop Rights Masterとの混在運用について

・ Systemwalker Desktop Rights Masterと混在運用時、クライアント(CT)においてSystemwalker Desktop Rights Masterの仮想ドライブ割り当て処理に伴い、構成変更ログが採取される場合があります。

・ ファイル持出し禁止機能を使用する場合、[持出し禁止]で禁止ドライブをドライブレターにより指定するのではなく、「ドライブ種別指定」で禁止を行ってください。

1.2.9 ファイル持出し禁止

メディア共通の留意点

・ ネットワークドライブへの持出し禁止および読み込み禁止はできません。

・ クライアント(CT)をインストールしたときに設定したログ格納先が、Cドライブ以外の場合、そのドライブを持出し禁止設定しないでください。

・ 持出し禁止の対象となるデバイスは、固定ハードディスク、フロッピーディスク、MO、メモリストレージ、CD/DVD、取り外し可能なハードディスク(USB、IEEE1394、PCMCIA接続など)、およびOSがリムーバブルと認識するものです。

・ 読み込み禁止の対象となるデバイスは、フロッピーディスク、MO、メモリストレージ、取り外し可能なハードディスク(USB、IEEE1394、PCMCIA接続など)、およびOSがリムーバブルと認識するものです。

・ 持出し禁止を設定したドライブは、読み取り専用となります。

・ 持出し禁止を設定したドライブに、フォルダのコピーを行った場合、フォルダだけ複写されることがあります。ただし、ファイルは複写されません。

・ 持出し禁止を設定したドライブは、エクスプローラからのフォーマットはできません(持出しユーティリティを使用してのフォーマットは可能です)。

CD/DVDメディアの留意点

・ 本製品はクライアント(CT)にライティングソフトと同様のドライバを持っているため、他のライティングソフト、パケットライトソフトと同居すると、他のライティングソフト、パケットライトソフトが予期しない動作をする場合があります。ライティングソフト、パケットライトソフトを通常利用される場合は、事前の動作検証をお勧めします。

・ ライティングソフトによっては、持出し禁止ができない場合があります。

ー 書き込みに関する要求を直接バスのドライバ(IDE/USB等)に対して行っているライティングソフト(例:Drag’on Dropなど)

この場合、アプリケーション起動禁止に該当ライティングソフトのプロセス名を登録することで、ライティングソフトの起動を禁止してください。(例:Drag’on Dropの場合はDragDropと指定)

・ CD/DVD持出し禁止の対象とするドライブの種別・接続方式・メディア・持出し禁止できることを確認済みのライティングソフトは、以下のとおりです。

ー ドライブ接続方式

ATAPI、USB 1.1/2.0
IEEE1394

ー メディア

CD-R/RW
DVD-R/RW
DVD-R Dual Layer
DVD+R/RW
DVD+R Dual Layer
DVD-RAM (※リムーバブルディスクとして認識される場合を除く)

ー ライティングソフト

B's Recorder GOLD 9
Win CDR 9
Record Now! Version 7
Easy Media Creator 8
Nero 7
エクスプローラ CD書き込み

・ DVD-RAMがセットされたドライブを、OSがリムーバブルディスクとして認識する場合があります。その場合は、リムーバブルディスクの禁止も行う必要があります。

・ Blu-ray、HD-DVDへの対応はしていません。(書き込み禁止中にBlu-ray/HD-DVD機器への書き込みを行った場合、書き込みを行った媒体が破壊される可能性があります。)

・ Windowsのセキュリティポリシーである「CD-ROMへのアクセスをローカルログオンユーザーだけに制限する」の設定は「無効」にしてください。「CD-ROMへのアクセスをローカルログオンユーザーだけに制限する」の設定が「有効」になっている場合、Systemwalker Desktop Keeperは、CD/DVDドライブの制御ができなくなります。このため、CD/DVDへ持出し禁止設定を行っていても、ライティングソフトなどで書き込めることがあります。

ロック機能がついたUSBデバイスへの持出しについて

ロック機能がついたUSBデバイスに対して持出し禁止および読み込み禁止を設定した場合、USBデバイスのロック動作、ロック解除動作、または取り外し動作が失敗する場合があります。その際は、再度ロック動作、ロック解除動作、または取り外し動作を行ってください。

また、読み込み禁止設定時、以下のロック機能付きUSBデバイスはロックが解除されないため、使用できません(持出しユーティリティからも使用できません)。

- 2つのドライブと認識し、両方ともリムーバブルのドライブ種別で、一方が読み込みだけのアクセスが可能で、他方が認証するまではデバイスがイジェクトされているように見えるデバイス(※)

1.2.10 印刷禁止

- 実行中のプロセスをSystemwalker Desktop Keeperが監視しており、WindowsのAPIである「StartDocA()」、「StartDocW()」が発行されると、関数を置き換えて印刷できなくします。フックによる監視ができない製品、「StartDocA()」、「StartDocW()」が使用されない製品の場合は、印刷禁止ができません。
- 印刷禁止ポリシーを設定した場合は、エクスプローラの右クリックメニューの[印刷]はグレーアウトされます。印刷許可アプリケーションで印刷を行う場合は、アプリケーションを起動してから印刷処理を行ってください。
- 以下の場合は印刷禁止ができません。
  - ー ActiveXやCOMインターフェースを使用して印刷処理を行っている場合
  - ー ラベルプリンタのような、印刷ドライバがCOMポートやプリンタポートに直接データを出力している場合(Windows API、スプールを経由しない印刷の場合)
  - ー Windows規約外で作成されたアプリケーションの印刷(フリーソフトの一部)
- Microsoft® Wordが印刷禁止されている場合、1度の印刷で同じログが2つ採取されます。
- Windows Vista®、Windows Server® 2008、Windows® 7でUAC(ユーザーアカウントコントロール)を無効化している場合、印刷禁止を行うことができない場合があります。また、エクスプローラの右クリックメニューの[印刷]はグレーアウトされません。
- 印刷監視動作において、「設定した印刷ページ数に達した時の動作」で、印刷を禁止する設定ページ数を超えた時の禁止動作が有効になるまで1分程度かかります。この間は、設定を越えても印刷できてしまうことがあります。

1.2.11 ログオン禁止

- シャットダウンを指定したログオン禁止ユーザーがログオンした場合、すでにログオン済みのユーザーがいると、シャットダウンは行わずにログアウトを行います。また、ログオン禁止ログにもログアウトを行ったことを記録します。

1.2.12 アプリケーション起動禁止

- 以下の場合はアプリケーション起動禁止が行えます。
  - ー Windowsのアプリケーション画面を持つ場合
- クライアント(CT)でコマンドプロンプトの起動を禁止する場合は、以下のアプリケーションを登録する必要があります。
  - ー cmd.exe
  - ー fsw41ej1.exe

1.2.13 メール添付禁止

メール添付禁止機能では、禁止対象のファイルをメールに添付して送信または保存しようとした場合の、メール内容(メール本文および添付ファイル)の保存・参照はできません。

V12.0L20～V13.0.0互換方式の場合

- メール添付禁止では、禁止対象となるファイルをメールに添付して、送信または保存（下書きフォルダへの保存）することを禁止できます。

- 対象となるメールソフトは、以下のとおりです。ほかのメールソフトでは動作保証していません。

  ー Microsoft® Outlook® Express 6.0

  ー Microsoft® Outlook® 2000

  ー Microsoft® Outlook® 2002

  ー Microsoft® Outlook® 2003

- 禁止対象ファイルと禁止対象外ファイルをメールに添付して送信する場合、禁止対象ファイルだけ禁止されます。メール本文および禁止対象外ファイルは送信されます。

- 禁止対象となるファイルをメールに添付して、送信または保存した場合、メールソフトによっては、禁止対象のファイルを空ファイルに置き換えるときがあります。その空ファイルを開くなどの操作を行ったとき、メールソフトやOSによって、処理が失敗したことを示すエラーメッセージが表示されることがあります。

- 受信したメールに禁止対象とするファイルが含まれている場合、そのメール自体を添付ファイルとして送信するときは、メール添付禁止はできません。
  たとえば、以下の場合です。

  1. システム管理者が「xls」の拡張子を持つファイルだけを添付禁止の対象とする
  2. クライアント(CT)で「xls」の拡張子を持つファイルが添付されたメールを受信する
  3. クライアント(CT)でその受信したメール自体をデスクトップに保存する
  4. クライアント(CT)のデスクトップに保存したファイル(禁止対象のファイルが含まれている)をメールに添付して送信する
  5. 添付したメールの拡張子が「xls」に該当しない場合は、メール添付禁止されない

- 受信したメールに禁止対象とするファイルが含まれている場合、そのメールを転送するときは、メール添付禁止できません。

- 受信したメールに禁止対象とするファイルが含まれている場合、そのメールを開くときに、禁止メッセージが表示される場合があります。表示された場合は、[OK]ボタンをクリックしてください。

  【例】
  HTMLメールにスタイルシートを使用している場合

- メール添付禁止のポリシーを[禁止する(指定拡張子のみ禁止)]または[禁止する(暗号化ファイルのみ許可)]にして、Microsoft® Officeアプリケーションの[送信]メニューからメールソフトを起動した場合、エラーメッセージが表示されメールソフトを起動できません。なお、メール添付禁止の対象ではないメールソフトも同様です。

- メール添付禁止のポリシーを[禁止する(指定拡張子のみ禁止)]または[禁止する(暗号化ファイルのみ許可)]にした場合、エクスプローラの右クリックメニューの[送る]から選択できる[メール受信者]は、表示されなくなります。なお、メール添付禁止の対象ではないメールソフトも同様です。

- メールソフトの機能([予定表]・[連絡先]・[仕事])で禁止対象ファイルを保存するとき、メール添付禁止機能が動作するため、禁止対象ファイルを保存できません。

- メール添付禁止のポリシーを[指定拡張子のみ禁止する]または[暗号化ファイル以外禁止する]にして、対象となるメールソフトで初めてアカウントを作成するとき、アカウント設定時にメール添付禁止に関するメッセージが表示されることがあります。ただし、アカウント設定には影響ありません。

- メールソフト、添付ファイルの種類、および操作方法によっては、禁止画面が表示されないことがあります。ただし、送信は禁止されます。

- 以下のメールソフト使用時に禁止画面が表示された場合、実際に添付したファイル名に「連番」または「(連番)」が追加されることがあります。また、採取されるログも禁止画面と同じファイル名となります。(例:添付した禁止対象のファイル名が「顧客情報.xls」の場合、禁止画面に「顧客情報1.xls」または「顧客情報(1).xls」が表示されることがある)
  また、添付ファイル名に記号(「&」「+」「=」「,」「[」「]」)を用いた場合、禁止画面および採取されたログのファイル名の記号(「&」「+」「=」「,」「[」「]」)が削除される場合があります。

  ー Microsoft® Outlook® 2000

  ー Microsoft® Outlook® 2002

  ー Microsoft® Outlook® 2003

- Windows® XPのクライアント(CT)にメール添付禁止のポリシーが適用されている場合、スタートメニュー(クラシック表示ではない場合)を選択したときに表示される左側の領域のショートカット(インターネットと電子メール)は表示されなくなります。ただし、メール添付禁止のポリシーが適用された直後は、左側の領域のショートカット(インターネットと電子メール)は表示されていますが、電子メールを選択するとインターネットのプロパティが表示されます。
- Windows® XPのクライアント(CT)でOutLook Expressの添付ファイル選択ダイアログ(メニューの[挿入]-[添付ファイル]、ツールバーの「添付」を選択した場合)の初期表示フォルダをネットワークフォルダに設定しないでください。設定されている場合、OutLook Expressが正常に動作しません。マイドキュメントをネットワークフォルダへリダイレクトしている場合などは、メール添付禁止（V13.2.0方式(ポート監視方式)の場合）を使用してください。
- 以下のメールソフト使用時に、禁止対象の添付ファイルをドラッグ&ドロップで保存する場合、OSのエラーメッセージ(「例:「ハンドルが無効です。」、「指定されたファイルが見つかりません。」)が表示され、添付ファイルの保存ができません。
  - Microsoft® Outlook® 2000
  - Microsoft® Outlook® 2002
  - Microsoft® Outlook® 2003
- 電子メールの規定メールソフトの設定は、Internet Explorer®のインターネットオプションで行ってください。

V13.2.0方式(ポート監視方式)の場合

- 添付ファイルの中に1つでも、添付禁止対象のファイルがある場合、メール(メール本文と、すべての添付ファイル)は送信できません。
- メール添付禁止を行う設定で、Microsoft® Outlook® 2003、Microsoft® Outlook® 2007のアカウントを作成しようとした場合、Systemwalker Desktop Keeperのメッセージ（D1F3-ERR001）が出力され、アカウントが作成されない場合があります。この場合はメール添付禁止の設定を解除して、アカウントを作成してください。
- メール添付禁止を行う設定の場合、条件によっては、送信したメールの本文が文字化けを起こす場合があります。下記条件がすべて満たされた場合に、Shift JISの範囲外の文字はエスケープ化した表現(具体的には、“ꪪ”という表現で、AAAA部分は4ケタまたは5ケタの16進コードです)に変換される場合があります。この場合、添付ファイルの形式をBASE64にしてください。
  - 禁止される条件のファイルを添付したとき
  - ファイルの添付形式がUUENCODEやBINHEXなどの、本文に添付される形式のとき
  - メールの本文にShift JISの範囲外の文字を使用しているとき
- クライアント(CT)のOSがWindows® 2000で、ウイルスバスター2007またはウイルスバスター2008がインストールされている環境で、メール添付禁止を行う場合、以下の設定が必要です。この設定を行わない場合は、メール添付禁止されない場合があります。
  1. ウイルスバスター2007またはウイルスバスター2008の画面の[不正侵入対策/ネットワーク管理]を選択し、パーソナルファイアウォールの[設定]ボタンをクリックします。
  2. [例外ルール(プロトコル)]タブをクリックします。
  3. [メール送信(SMTP)]を選択し[マスメール送信（SMTP)]より上に表示されるように、画面左の矢印ボタンを使用して移動させます。
  4. [OK]ボタンをクリックします。
- メール添付禁止の設定で、暗号化ファイル以外を禁止する設定の場合、S/MIME形式で暗号化されたメールを送信することができません。
- UNICODE形式でファイルを添付した場合、実際には添付していない添付ファイル(ファイル名：AttXXXXX.XXX (Xは数字または英字))が添付される場合があります。その時、メール送信ログを取得する設定にしていた場合、実際には添付していない添付ファイル名がログとして採取されます。また、メール添付禁止を行う設定で、AttXXXXX.XXX が許可されたファイルでない場合、メールが添付禁止されて送信できません。
- メールヘッダ中にfilenameパラメーターがないエンコード形式で、拡張子を指定してメール添付を禁止(あるいは許可)する場合、指定した拡張子を持つファイルのメール添付禁止が、ポリシーどおりに動作しない場合があります。
  - Outlookで.msgファイル(Outlookメッセージファイル)を添付し、送信した場合

ー Becky!で「元メールを添付して転送」の操作で、元メールにある添付ファイルを送信した場合

- メール添付禁止を行うポリシーの場合、送信するメールの文字が、JIS:ISO-2022-JP、UTF-7、UTF-8、US-ASCII以外の形式でエンコードされているときは、メールを送信できません。また、このとき、ポリシーが設定されていても、メール添付禁止機能は動作しません。
- Outlookで.msgファイル(Outlookメッセージファイル)を添付し、送信した場合、メール送信時宛先確認画面、またはメール添付禁止画面にて、msgファイルが「Unknown_File」として表示されます。
- SJISに対応する字形を持たないUNICODE文字(JIS2004を含みます)が送信者、件名、あて先、添付ファイル名に使用されていた場合、メール送信時宛先確認画面、メール添付禁止画面に表示される文字列がHTMLエスケープ形式で表示されたり、"?"で表示されたりする場合があります。

1.2.14 URLアクセス禁止

- Windows® 2000では、本機能は動作しません。
- 本機能は、Internet Explorer®以外のWebブラウザでは、動作しません。
- 本機能は、Windows® Internet Explorer® 7以上で動作します。
- 禁止機能が動作するのは、Internet Explorer®のウィンドウがアクティブになっているときです。
- 禁止されたURLへアクセスしても、そのときの画面はキャプチャしません。
- URLアクセス禁止ポリシーが適用されたとき、すでに、Webブラウザで禁止サイトが表示されていた場合は、その表示されている禁止サイトは、閉じられます。
- Webページに1つだけタブが表示されている場合、禁止されたURLへアクセスしたときは、Internet Explorer®が強制終了されます。
  Webページに複数のタブが表示されている場合、禁止されたURLへアクセスしたタブだけ、強制的に閉じられます。
- 表示中のWebページのフレーム内に禁止サイトが含まれる場合、禁止機能は動作しません。
- ウィンドウタイトル取得ログの採取が有効なときに禁止サイトにアクセスした場合、ウィンドウタイトル取得ログの備考欄にURLが記録されない場合があります。

1.2.15 FTPサーバ接続禁止

- Windows® 2000では、本機能は動作しません。
- 64ビット系OSでは、FTP.EXEの接続禁止を行うことはできません。
- Internet Explorer®を使用したFTP接続操作を禁止する場合は、URLアクセス禁止機能で実施してください。
- FTPクライアントの接続先通信ポートが「21」に設定されているFTP通信だけ、禁止できます。
- コマンドプロンプトから起動されるFTPクライアントの場合は、Windows FTP.EXE だけ、本機能の対象となります。
- セキュアFTP(FTPS, SFTPなどの暗号通信を行うFTPプロトコル)は、本機能の対象とはなりません。
- FTPサーバ接続禁止ポリシーが適用されたとき、すでに、FTPサーバへの接続が行われていた場合は、サーバへの接続が強制遮断されます。
- 以下の場合は、キャッシュ内容を表示して操作を継続し、フォルダ間の移動やファイル転送開始時にFTPサーバへの接続が行われたタイミングで、FTPサーバ接続禁止機能が動作します。

  ー FTPフォルダビューが有効な状態で、エクスプローラに対して、FTP接続禁止機能を適用した場合

  ー キャッシュ上に以前に接続した内容が保存されている場合

1.2.16 Webダウンロード禁止

- Windows® 2000では、本機能は動作しません。
- 本機能は、Windows® Internet Explorer® 7以上で動作します。
- Webページ独自の機能(ActiveXなどによるダウンロード)によってファイルのダウンロードが行われた場合は、禁止できません。
- Internet Explorer®で直接ファイルを開いた場合や実行した場合、禁止機能は動作しません。
- Internet Explorer®で表示中のWebページの構成部品(ボタンやロゴなど)を画像として保存した場合、禁止機能は動作しません。
- Internet Explorer®で表示中のWebページ全体をファイル保存した場合、禁止機能は動作しません。
- Webブラウザ起動時のポリシーが有効となります。ポリシーが変更された場合、すでにWebブラウザが起動していたときは、起動中のWebブラウザは変更前のポリシーで動作します。

1.2.17 ログ全体

- Windowsへのログオン時に入力するユーザー名にUNICODE文字を使用した場合、一部の文字はエスケープ化されます。エスケープ化後の表現が40バイトを超えた場合、41バイト目以降はログに格納されません。
- だれもログオンしていない場合に取得された操作ログは、ユーザー名が“SYSTEM”、ドメイン名が“自コンピュータ名”で記録されます。
- ユーザー名が“SYSTEM”と記録されている場合は、ドメイン名は必ず“自コンピュータ名”で記録されます。
- ログオン直後の数秒間は、ログオンユーザーによる操作であっても、ログのユーザー名に“SYSTEM”として記録されることがあります。
- PC起動、PC終了、PC休止、PC復帰のログについては、必ずユーザー名は“SYSTEM”、ドメイン名は“自コンピュータ名”で記録されます。
- Windows Vista®、Windows Server® 2008、Windows® 7でログオンユーザーが複数の場合、メール送信ログおよびメール添付禁止ログは、必ずユーザー名は“SYSTEM”、ドメイン名は“自コンピュータ名”で記録されます。
- Windows Vista®、Windows Server® 2008、Windows® 7の場合、ファイル操作ログのユーザー名が“SYSTEM”、ドメイン名が“NT AUTHORITY”で記録されることがあります。
- ログ情報を記録中にクライアント(CT)を強制電源断などで停止した場合は、ログ情報が記録されない場合があります。

1.2.18 ファイル持出しログ

- ファイル持出しログは、「持出しユーティリティ」を使用した場合だけ取得されます。エクスプローラなど「持出しユーティリティ」以外でファイルを持ち出した場合（または持ち出しが禁止された場合）はファイル持出しログが取得されません。

原本保管について

- 持ち出すデータがフォルダの場合、原本ファイルとしてはファイルだけ保管し、フォルダ構成は保管しません。
- 原本ファイルは、持ち出したファイルのファイル属性は継承しません。
- 原本保管を指定している場合は、Windowsのファイル暗号化機能(EFS)の対象ファイルを持ち出すことができません。
- 管理サーバの原本保管データが格納されているフォルダは、標準で“System”権限以外のユーザーはアクセスできないように設定されています。原本保管したデータ自体は暗号化されていないので、アクセス権限の変更やバックアップ後のデータ管理には注意してください。

1.2.19 印刷操作ログ

- Windows Vista®、Windows Server® 2008、Windows® 7でWindowsプリントサーバとして定義されているサーバに接続された共有プリンタから印刷を行う場合、Windows Vista®、Windows Server® 2008、Windows® 7の名前解決がフルDNS名で解決されるよう設定されている必要があります。フルDNS名での名前解決ができない場合、印刷操作ログは取得されません。
- Windows Vista®、Windows Server® 2008、Windows® 7でWindowsプリントサーバとして定義されているサーバに接続された共有プリンタから印刷を行う場合、Windows Vista®、Windows Server® 2008、Windows® 7側で定義されているネットワークプリンタのプロパティで、[クライアントコンピュータで印刷ジョブのレンダリングをする] がオンになっている場合、1回の印刷操作で2つのログが記録されるときがあります。2つのうち、1つのログは印刷を行ったPCの名前がプリントサーバの名前になります。
- プリンタサーバがWindows® 95、Windows® 98およびWindows® MEの場合(V12のクライアント(CT))、そのプリンタサーバ経由で印刷されるクライアント(CT)の印刷操作ログは採取できません。
- [印刷監視方式の設定]が[ローカルプリンタでの印刷のみを監視する]の場合、以下の条件のときは、印刷操作ログを取得できません。
  - ー パターン1
    - クライアント(CT)をインストールしていないプリンタサーバ経由で印刷するとき
  - ー パターン2

    以下の条件をすべて満たすときです。
    - クライアント(CT)をインストールしているプリンタサーバ経由で印刷するとき
    - プリンタサーバがクライアント(CT)と別のサブネットに設置されているとき
  - ー パターン3

    以下の条件をすべて満たすときです。
    - クライアント(CT)をインストールしているプリンタサーバ経由で印刷するとき
    - クライアント(CT)が複数のNICを使用しているとき
    - プリンタからクライアント(CT)に通知されるジョブ作成元マシン情報が、クライアント(CT)の管理サーバとは別のセグメントのIPアドレスであるとき
  - ー パターン4

    以下の条件をすべて満たすときです。
    - クライアント(CT)をインストールしているプリンタサーバ経由で印刷するとき
    - プリンタからクライアント(CT)に通知されるジョブ作成元マシン情報が、クライアント(CT)のIPV6のIPアドレスであるとき
- 印刷操作ログを取得するためには、ポート139番を開けておく必要があります。パーソナルファイアウォールを使用している場合は、クライアント(CT)のインストール時にポート139番が開いていることを確認してください。また、運用途中でパーソナルファイアウォールを導入または設定変更した場合は、ポート139番が開いていることを確認してください。なお、以下のOSの場合、クライアント(CT)のインストール時にWindowsファイアウォールに対して自動でポート139番が開けられます。
  - ー Windows® 7
  - ー Windows Vista®
  - ー Windows® XP
  - ー Windows Server® 2003
  - ー Windows Server® 2008
- ネットワークプリンタへの印刷で印刷操作ログを採取するためには、コントロールパネルのネットワーク接続のプロパティで、[Microsoftネットワーク用ファイルとプリンタ共有]のチェックボックスがチェックされている必要があります。LANカードが複数枚ある場合、ネットワーク経由で印刷を行うLANカードはすべてチェックしてください。

- クライアント(CT)のインストール時に[ローカルプリンタでの印刷のみを監視する]を選択した場合、以下について留意してください。
  - ー プリンタサーバとなるクライアント(CT)では、OSにログオンしておく必要があります。ログオンしておかないと、ほかのクライアント(CT)からの印刷依頼を検知することができないので、印刷操作ログを採取することができません。
  - ー ログビューアで印刷操作ログを参照すると、[ドメイン名]の欄には、印刷を行ったコンピュータ名の情報が表示されます。
- プリンタの負荷が高い場合や、印刷の直後にクライアント(CT)でシャットダウンまたはログオフを実施した場合、以下のようにログが採取されるときがあります。
  - ー 印刷ファイル名が[ローカルダウンレベルドキュメント]
  - ー 印刷ファイルの総ページ数が[不明]または総ページとは異なるページ数
- 印刷の直後にクライアント(CT)で電源を切断した場合、またはブルースクリーンになった場合、ログは採取されません。
- ネットワークに接続しているプリンタで印刷が行われた場合、印刷ファイルの総ページ数が[不明]または総ページとは異なるページ数として採取されるときがあります。
- 1ファイルのページ数が多い場合、複数の印刷操作ログとして採取される場合があります。その場合、ファイル名は同一となり、ページ数が分割されます。
  たとえば、「ファイルA 100ページ」として採取されるログが、「ファイルA 4ページ」、「ファイルA 90ページ」、および「ファイルA 6ページ」のように3つに分割されて採取されます。
- 短時間に多量のファイルを印刷した場合(例:部数を指定した印刷、複数ファイルを選択した印刷など)、部数ごとのログが採取されない場合や、採取されたログのページ数が正しくない場合があります。
- ログビューアに表示されるページ数が少なくなる場合があります。ページ数はプリンタスプールに通知された情報を採取しており、ページ数が多いファイルを印刷した場合、実際より少ないページ数がプリンタスプールに通知されることがあるためです。
- 印刷したアプリケーションにより、ログビューアに表示される印刷ファイル名が空欄になる場合があります。
  印刷操作ログはプリンタスプールに通知された情報を採取しており、アプリケーションによっては印刷ファイル名がプリンタスプールに通知されないためです。
- 部数指定の印刷を行った場合、アプリケーションにより、ログビューアには、1回の印刷操作ログとして表示される場合があります。
  印刷操作ログはプリンタスプールに通知された情報を採取しており、アプリケーションによっては、部数印刷を1回の印刷としてプリンタスプールに通知するためです。
- クライアント(CT)のインストール時に[この端末で設定されている全てのプリンタでの印刷を監視する(推奨)]を選択した場合、そのクライアント(CT)からネットワークプリンタ経由で印刷を行うときに、プリンタサーバとなるマシンがサーバOS以外であると、接続数に上限が発生します。上限を超えるとクライアント(CT)以外のほかのマシンからも印刷できなくなります。なお、上限はOSごとに異なり、セッションの数となります。
- プリンタの登録で、同じプリンタが重複して定義されている場合、以下のように1回の印刷操作で2つの印刷操作ログが採取されることがあります。
  - ー 正常で同じ内容のログが2つ
  - ー 正常なログと印刷ファイル名が[リモートダウンレベルドキュメント]、ページ数が[不明]のログ
- プリンタサーバに[ローカルプリンタでの印刷のみを監視する]を選択してクライアント(CT)がインストールされている場合、印刷が行われたクライアント(CT)で使用中のユーザー名をプリンタサーバにも登録しておく必要があります。登録されていない場合は、印刷ログのユーザー名が以下のように出力されるときがあります。
  - ー 印刷が行われたクライアント(CT)で使用中のユーザー名にユーザー権限しか設定されていない場合、ログの[ユーザー名]が[Guest]として採取されるときがあります。
  - ー 印刷時にプリンタサーバに対してログオン要求があり、Administratorにてログオンした場合、ログの[ユーザー名]が[Administrator]として採取されるときがあります。
- 紙に印刷を行わないドキュメントライタ(Microsoft Office Document Inage Writerや、Adobe PDFなど)の動作が、印刷ログとして記録されることがあります。

1.2.20 ウィンドウタイトル取得ログ

- 「アプリケーションのウィンドウタイトル名」および「アドレスバーに表示されるURL情報」が前回取得した時点と同じ場合には、ウィンドウタイトル取得ログは採取されません。

  ー Internet Explorer®、エクスプローラの場合は、ウィンドウタイトルとアドレスバーに表示されるURL情報が前回取得した時点と同じ場合は採取しません。

  ー その他のアプリケーションの場合は、ウィンドウタイトルが前回取得した時点と同じ場合は採取しません。

- ウィンドウタイトルログの重複ログフィルタは、最大100件までのウィンドウタイトルログの重複を管理します。100件以上のウィンドウタイトルログが発生した場合、100件のログのうち、最も古いウィンドウタイトルログを管理から外し、新しいウィンドウタイトルログを管理します。

- PCの電源を入れ直すと、重複ログフィルタのチェックは最初から行うことになります。

1.2.21 メール送信ログ

- メール送信ログの採取に関して、Systemwalker Desktop Keeperは、SMTP（クライアント(CT)インストール時に指定したポート番号）を監視します。つまり、メールの送信にSMTPプロトコルを使用するメールソフトが対象となります。複数のメールソフトを使用している場合、それぞれのSMTPのポート番号設定は、同一のポート番号を指定してください。

- SMTP以外のプロトコルを使用するWebメールやグループウェアなどは、メール送信ログが採取されません。

- Outlookの電子メールアカウントで使用するサーバの種類が“Microsoft Exchange Server”になっている場合は、SMTPプロトコルでないため、メール送信ログが採取されません。

- パーソナルファイアウォールなどで、インストール時に指定したポート番号が閉じられている場合は、メール送信ログが採取されません。

- 送信するメールは、JIS:ISO-2022-JP、UTF-7、UTF-8、US-ASCIIのどれかの形式でエンコードされている必要があります。メール送信ログを取得するポリシーの場合、JIS:ISO-2022-JP、UTF-7、UTF-8、US-ASCII以外の形式でエンコードされたメールは送信されず、メール送信ログを取得するポリシーが設定されていても、ログは記録されません。

- Microsoft® Outlook® 2003、Microsoft® Outlook® 2007の場合で、UNICODE文字を含むメールを送信した場合、「送信メッセージのエンコード方法を自動で決定する」を設定していると、文字設定を日本語(JIS)にしていても、簡体字中国語(GB2312)に変換されて送信されます。したがって、Microsoft® Outlook® 2003、Microsoft® Outlook® 2007では、「送信メッセージのエンコード方法を自動で決定する」を設定しないでください。

- メールソフトが「RFC2183」に準拠した仕様になっていない場合、正しくログが採取されない場合があります。(例:添付ファイル名が採取されない)

- メール送信ログで採取されるすべての情報は2048バイトまでです。2048バイトを超える場合は、以下の順番で情報が削除され、2048バイト以内になるまで続けられます。
  このため、メール送信ログの一部が削除された場合は、ログビューアにおいて、メール送信ログが関係したファイル追跡ができない場合があります。

  1. 送信元アドレスが削除されますが、100バイトまでは残されます。ただし、100バイト目が全角文字の1バイト目であったときは、99バイトまで残されます。
  2. 送信先アドレス(Bcc)が削除されますが、500バイトまでは残されます。ただし、500バイト目が全角文字の1バイト目であったときは、499バイトまで残されます。
  3. 送信先アドレス(Cc)が削除されますが、500バイトまでは残されます。ただし、500バイト目が全角文字の1バイト目であったときは、499バイトまで残されます。
  4. 送信先アドレス(To)が削除されますが、500バイトまでは残されます。ただし、500バイト目が全角文字の1バイト目であったときは、499バイトまで残されます。
  5. メールのタイトルが削除されますが、100バイトまでは残されます。ただし、100バイト目が全角文字の1バイト目であったときは、99バイトまで残されます。
  6. 添付ファイル名が削除されますが、300バイトまでは残されます。ただし、300バイト目が全角文字の1バイト目であったときは、299バイトまで残されます。

- 送信先アドレス(Bcc)は、アドレス部分だけログとして採取されます。メールソフトで添付される名前は採取されません。
- 新規にLANデバイスを装着し、LANドライバのインストールが行われた場合は、クライアント(CT)を再起動したあとにメール送信ログを採取できるようになります。
- 送信先アドレス(To、Cc、Bcc)に「,」や「;」が含まれている場合、メールソフトによっては「,」や「;」の部分でアドレスが分割されてログが採取されるときがあります。
- 送信先アドレス(To)と(Bcc)、(cc)と(Bcc)が同じアドレスの場合、(Bcc)のアドレスが採取されません。

メール内容の参照について

- メール内容(本文、添付ファイル含むすべて)は、MIMEエンコード後のものが、参照用ファイルとしてサーバに保管されます。したがって、ファイルサイズはMIMEでエンコードされた後のサイズで判断されます。メール内容のファイルサイズが50MBを超える場合は、保管されません(メール送信ログ自体は取得されます)。
  メール内容のファイルはバックアップツール対象外のため、定期的に退避することをお勧めします。
- メール内容参照用に管理サーバに保管したファイルは、他の原本保管ファイルと同様、バックアップツール、バックアップコマンドでのバックアップ対象外です。

メール送信時のあて先確認について

- メール送信時に確認対象となるメールアドレスは、すべてのあて先(TO、CC、BCC)です。FROMは対象外です。
- 利用者がメールソフトから除外ドメイン以外のアドレスにメールを送信しようとして、送信を中止した場合でも、メールソフトはメールの送信を完了しているため、該当メールは送信済みと見なされてしまいます。
- 本機能をメールサーバで動作させると、中継したメールの送信でメッセージが表示される場合があります。メッセージが表示されたままではメールの送信が完了していないため、メールが滞留してしまう可能性があります。メールサーバでは、本機能を使用しないでください。
- 警告メッセージが表示されている間は、メールの送信が完了しません。メッセージが表示された状態で長時間放置していた場合、メール送信が失敗する場合があります。
- 管理サーバと同じコンピュータにインストールされているCTで、本機能を動作させる場合、管理者通知のメール送信時にアドレスがチェックされ、警告メッセージが表示される可能性があります。メッセージが表示されている間は、メールの送信が完了しないため、管理者通知のあて先を除外ドメインのアドレスに設定してください。
- 本機能は、システムが自動で送信しているメールに対してもチェックを行い、警告メッセージを表示します。メッセージが表示されている間、メールが送信されないため、そのようなメール送信についてはあて先を除外ドメインのアドレスに設定してください。

1.2.22 コマンドプロンプト操作ログ

- コマンドプロンプト操作ログは[スタート]メニューから[プログラム]－[アクセサリ]－[コマンドプロンプト]で起動された場合だけ採取されます。「cmd.exe」や「command.com」を直接起動した場合、コマンドプロンプト操作ログは採取されません。
  また、コマンドプロンプト内でのIME(Input Method Editor)は、Microsoft社のIMEだけをサポートします。
  ただし、以下の場合、[スタート]メニューからコマンドプロンプトを起動しても、コマンドプロンプト操作ログは採取されません。

  － バッチファイル内の処理内容

  － 「start」コマンドの操作

  － 独自のコンソール出力を使用しているアプリケーションの出力結果(例:「telnet」、「doskey」、「debug」など)
- 出力結果の多いコマンドを実行した場合、採取されたコマンドプロンプト操作ログをログビューアで確認すると、ログの行がずれて表示されるときがあります。
- 1つのコマンドの実行あたり、出力結果が300行を超えた場合、最後の300行だけログを採取します。

- コマンドプロンプト操作ログは、「exit」コマンドまたは「×」ボタンによりコマンドプロンプトのウィンドウが閉じられたあとに、統合管理サーバまたは管理サーバに採取されます。そのため、クライアント(CT)を使用しているユーザーがコマンドプロンプトのウィンドウを閉じない場合、コマンドプロンプト操作ログは、採取されません。
- コマンドプロンプトのプロパティ(画面バッファのサイズやウィンドウのサイズなど)を変更した場合(コマンドによってプロパティを変更した場合も含む)、以下の状態になるときがあります。

  ー 変更した設定が有効にならない

  ー 画面の表示が乱れる

  ー ログの一部が採取されない

  また、変更したプロパティは、クライアント(CT)の次回起動時には有効になりません。
- コマンドプロンプト操作ログが採取されるとき、入力されたコマンドの直後に、実行した日付と時刻が挿入されます。そのため、ログビューアで参照すると、コマンドプロンプト上にはなかった日付と時刻が表示されます。
  ただし、コマンドの出力が終了する前に次のコマンドを入力されるなど、タイミングによっては、入力されたコマンドの直後に、実行した日付と時刻が挿入されないときがあります。また、出力結果が多い場合など、日付と時刻が途中に挿入されるときがあります。

  コマンドプロンプトでの表示例

```
C:¥Documents and Settings¥Administrator>dir

ドライブ C のボリューム ラベルがありません。

ボリューム シリアル番号は EC12-57D0 です
```

  ログビューアでの表示例

```
C:¥Documents and Settings¥Administrator>dir

                                --[2005/05/27 13:40:19]--

ドライブ C のボリューム ラベルがありません。

ボリューム シリアル番号は EC12-57D0 です
```

- コマンド入力により画面が再表示されるコマンドは、1回のコマンド入力でログが2回採取されます。(例:「append」コマンド)

1.2.23 デバイス構成変更ログ

Windows Vista®、Windows Server® 2008、Windows® 7でUACが有効な場合、一般ユーザーが管理者に昇格してネットワークドライブに接続したときのデバイス構成変更ログは採取されません。

記録対象となるデバイスは、Windowsにドライブ(A～Zドライブ)が割り当てられたものが対象です。

仮想環境では、ローカルデバイスにCD/DVD等をマウントした際のデバイス構成変更ログは採取されません。

1.2.24 PrintScreenキー操作ログ

PrintScreenキーにより、画面のハードコピーを採取するソフトウェアがインストールされている場合、PrintScreenキー操作ログを取得できない場合があります。

1.2.25 Citrix XenApp上での操作ログについて

FATクライアントからCitrix XenAppの公開デスクトップ上でPrintScreenキー操作を行った場合、Citrix XenAppクライアントの設定によって、採取されるPrintScreenキー操作のログが、FATクライアント側のログとして採取される場合とCitrix XenApp側のログとして採取される場合とがあります。

Windows Server® 2008の場合

- 公開アプリケーションの起動・終了ログは、Citrix XenApp のクライアント側のログとして採取されます。(Systemwalker Desktop KeeperのCTがインストールされている必要があります。)
  その際、実行したアプリケーション名ではなく、Citrix XenAppクライアントのプロセス名の起動・終了ログとして採取されます。
- 公開アプリケーションのウィンドウタイトルログは、Citrix XenApp のクライアント側のログとして採取されます。(Systemwalker Desktop KeeperのCTがインストールされている必要があります。)公開アプリケーションにログフィルタ条件や画面キャプチャ条件を設定する場合は、Citrix XenApp のクライアント側にインストールされているCTのポリシーを設定する必要があります。その際、設定するプロセスは、Citrix XenAppクライアントのプロセスを(WFICA32.exe)設定する必要があります。Citrix XenAppクライアントのプロセス名については、Citrix XenAppクライアントのバージョン等によって異なる可能性があります。
  また、公開アプリケーションでInternet Exploreを実行した場合、URLは取得されません。
- 公開アプリケーションから、Citrix XenApp のクライアント側にインストールされているプリンタで行った印刷操作は、Citrix XenApp のサーバ上の操作ログではなく、Citrix XenApp のクライアント側のログとして採取される場合があります。(Systemwalker Desktop KeeperのCTがインストールされている必要があります。)その際、ドキュメント名はCitrix ICA Remote Job、ページ数は不明で採取される場合があります。また、仮想プリンタで印刷を行った場合、仮想プリンタによっては印刷操作ログが採取されない場合があります。
- 公開アプリケーションから、Citrix XenApp のサーバ側にインストールされているプリンタで印刷した場合、印刷操作ログは採取されません。

Windows Server® 2008 64ビット版、Windows Server® 2008 R2の場合

- コマンドプロンプトログは取得されません。

1.2.26 Web操作ログ

- Windows® 2000では、本機能は動作しません。
- 本機能は、Windows® Internet Explorer® 7以上で動作します。
- HTTPプロトコルを使用したダウンロードのログを取得します。
- ActiveXやプラグインによるダウンロードによって、ファイルのダウンロードが行われた場合は、ログを取得できません。
- Internet Explorer®で直接ファイルを開いた場合や実行した場合、ログは取得されません。
- Internet Explorer®で表示中のWebページの構成部品(ボタンやロゴなど)を画像として保存した場合、ログは取得されません。
- Internet Explorer®で表示中のWebページ全体をファイル保存した場合、ログは取得されません。
- Webブラウザ起動時のポリシーが有効となります。ポリシーが変更された場合、すでにWebブラウザが起動していたときは、起動中のWebブラウザは変更前のポリシーで動作します。
- Web操作ログは、Webダウンロード操作が行われたときにログを採取します。したがって、ダウンロードが行われている間に異常が発生したり、ユーザーにより処理がキャンセルされた場合でも、ログは採取されます。
- Internet Explorer®でFTPサイトに接続した場合のダウンロード操作は、Web操作ログとして取得されます。

1.2.27 FTP操作ログ

- FTPクライアントの接続先サーバの通信ポートとして「21」が設定されているFTP通信のログだけ、記録します。
- Windows® 2000では、本機能は動作しません。
- 64ビット系OSでは、FTP.EXEのログは取得されません。
- コマンドプロンプトから起動されるFTPクライアントの場合は、Windows FTP.EXE だけ、本機能の対象となります。
- セキュアFTP(FTPS, SFTPなどの暗号通信を行うFTPプロトコル)、Webブラウザのプラグインや ActiveXを使用したFTP転送は、本機能の対象とはなりません。
- FTP操作ログで取得されるファイル名は、FTPサーバ上のファイル名です。ファイルパスは取得されません。

- エクスプローラでFTPダウンロード操作を行った場合、ファイル名がURLエンコードされる場合があります。この場合、ログはURLエンコード文字列のまま、記録されます。
- FTP操作ログは、FTPファイルのアップロードまたはダウンロード操作が行われたときに、ログを採取します。したがって、ファイルの転送中に異常が発生したり、ユーザーにより転送がキャンセルされた場合でも、ログは記録されます。
- Internet Explorer®を使用したFTP転送は、Web操作ログ(Webダウンロード)として取得されます。
- FTPクライアント起動中にポリシーが変更された場合、起動中のFTPクライアントは、変更前のポリシーで動作します。
- エクスプローラを使用する場合、FTPフォルダビューの有効/無効により、以下の動作となります。
  - ー FTPフォルダビューが有効な場合
    アップロード・ダウンロード操作ログが取得されます。ファイルパスは取得されません。ファイル名だけ取得されます。
  - ー FTPフォルダビューが無効な場合
    アップロード操作はできません。ダウンロード操作ログが取得されます。ファイルパスは取得されません。ファイル名だけ取得されます。

1.2.28 ファイル操作ログ

- 圧縮ツール(ZIP、LZH、マイクロソフト社から提供されているツールなど)による圧縮・解凍の操作ログは採取されません。
- Internet Explorer®、またはWindowsのエクスプローラに機能を追加するアプリケーションの操作ログは、採取されません。
- OSがWindows Vista®、Windows Server® 2008、Windows® 7でUACで権限昇格を許可し操作を続行した場合、アプリ名(ログビューアの[ログ一覧]の[内容]に表示されます)はアプリケーション名ではなく、「dllhost.exe」としてログが採取されます。
- [ファイルを開く]ダイアログで表示されているファイルがある場合、ファイルをオープンしていなくても、参照ログが取得される場合があります。
- ファイルサイズが大きいファイルをコピーすると、ファイル操作ログが大量に採取される場合があります。
- 以下の場合、ファイルサイズが正常に取得できないときがあります。
  - ー 30秒に満たない短い時間の間に、ファイルの移動や改名を繰り返したり、追加・削除を行ったり、操作後のファイルが存在するデバイスを取り外したりした場合
  - ー ログオフやシャットダウンの直前にファイル操作を行った場合

実際の操作と採取される操作ログが異なる場合があります

- ー 以下のソフトウェアやコマンドの場合、操作ログは、“8.2.20 ファイル操作ログ”で説明されているように採取されます。
  - エクスプローラ
  - メモ帳
  - ワードパッド
  - Microsoft® Word(2000、2002、2003、2007、および2010の場合)
  - Microsoft® Excel(2000、2002、2003、2007、および2010の場合)
  - Microsoft® PowerPoint®(2000、2002、2003、2007、および2010の場合)
  - コマンドプロンプト中のコマンド(COPY、XCOPY、MOVE、DEL、ERASE、RD、REN、MD)

  ただし、以下の点に注意してください。
  - Microsoft® Wordによる「更新」操作(新規保存および上書保存)は[作成]としてログが採取される
  - エクスプローラやXCOPYのように[ファイル操作プロセス]タブで[参照以外を取得]として登録してあるプロセスは、[参照]のログは採取されない
  - 上記のソフトウェアやコマンドの場合でも、“8.2.20 ファイル操作ログ”に示す以外に余分なログが採取されることがある

- 上記以外のソフトウェアやコマンドの場合には、実際の操作と異なる操作ログが採取されることがある(たとえば、「複写」や「移動」のログが採取できず、[参照]、[作成]、[削除]、または[変名]としてログが採取される)
- コマンドプロンプトで、リダイレクト処理(> または >>)およびMDコマンドを使用した場合、ログが出力されない

― DVDやCDに、ローカルドライブにあるデータをライティングソフトで書き込む場合、DVDやCDに対するアクセス情報が採取できないため[参照]としてログが採取されます。[複写]としては採取されません。

― テープ装置への出力、RS-232C などのクロスケーブルによる通信、IrDA(赤外線装置)経由での操作などは、接続先のドライブ情報が取得できないため、ローカルドライブ側だけの情報を採取して、操作ログが作成されます。

― サイズの大きなファイルを移動する場合(目安としては、1つのファイルの移動が上書き確認時の利用者操作を含めて30秒以上かかる場合)、ログが[複写]と移動元の[削除]の2つに分かれる場合があります。

― moveコマンドを使用して、同一ドライブ内で上書き移動した場合、上書き確認のプロンプトを30秒以上表示して、そのあとに上書きの操作を行うと、ログは[移動]ではなく[変名]となります。また、ほかのコマンドでも、上書き確認のプロンプトを表示したままの場合は、異なるログが採取される場合があります。

― COPYコマンド(XCOPYコマンド)で「COPY A.TXT+B.TXT C.TXT」や「COPY *.TXT C.TXT」として実行した場合のログは、正常に採取できません。この場合、「C.TXT」の[作成]としてログが採取されます。

― 採取されるログの[ファイル名]、[ファイル名先]、または[ファイル名元]の情報は259バイトまで採取されます。

― コマンドプロンプトでのファイル操作で存在しないパスを指定した場合、処理は失敗しますが、ログは採取されることがあります。

― 確認画面が表示される操作(例:上書き複写)を行った場合に、その操作を取り消したときもファイル操作ログが採取されることがあります。

― Windows Vista®、Windows Server® 2008、Windows® 7において、確認画面が表示される操作(上書き複写、上書き移動)を行った場合に、ログ種別に「複写」または「移動」として記録されないことがあります。(複写先ファイルまたは移動先ファイルの更新ログ、移動元の削除ログが採取されます。)

多くの[参照]ログが採取される場合があります

― 操作ログを採取する場合、[ファイル操作プロセス]タブでログ採取対象とするプロセスを登録します。このとき、[拡張子による選択]で[全拡張子を取得]とした場合、そのプロセス(アプリケーション)でアクセスするすべてのファイルの情報を採取します。これらのファイルの中には、データファイルのほかに、実行モジュールや一時作業用としてアクセスするファイル、たとえば、拡張子が「exe」、「dll」、「ini」、「tmp」、「lnk」、または「inf」などのファイルも含まれ、これらの操作ログも採取されます。

操作ログが採取できない場合があります

― 音楽CDを再生する場合、操作ログは採取できません。

ネットワークドライブ関連のファイル操作ログについて

― ネットワークドライブ関連のファイル操作は、クライアント(CT)からネットワーク上にあるSystemwalker Desktop Keeperのクライアント(CT)で動作対象としているOSに対して行われた、ファイルやフォルダの操作がログ採取の対象となります。

― ネットワークドライブ関連のファイル操作ログは、UNC表記またはUNC表記のマシン名の部分がIPアドレスで表示されます。ただし、以下の場合は、採取されるログの[ファイル名先]の情報は、ファイル名またはフォルダ名のフルパスで表示されます。

- ネットワークドライブにドライブレターの割り当てを行い、割り当てたドライブレターから変名の操作を行った
- ネットワークドライブにドライブレターの割り当てを行い、割り当てたドライブレター内で移動の操作を行った
- ネットワークドライブとして割り当てたドライブレターに対して、割り当てたドライブレターと同じネットワークドライブに直接アクセスしたフォルダから移動の操作を行った

― ネットワークドライブとして割り当てたドライブレターと、割り当てたドライブレターと同じネットワークドライブに直接アクセスしたフォルダ間での移動の操作は、“8.2.20 ファイル操作ログ”で示す表と、以下の部分が異なってログが採取されます。

- [フォルダ操作]-[フォルダ配下のファイルに対するログ]-[同じドライブ内]で、[×]の代わりに[変名]ログとして採取される

- [フォルダ操作]-[フォルダに対するログ]-[同じドライブ内]で、[変名]、[(変名)]、および[(削除)]の代わりに[作成]、[削除]、および[(削除)]ログとして採取される

[ファイル操作ログ取得除外フォルダの設定]について

- ファイル操作ログ取得除外フォルダの設定で、内臓ディスクでもOSがリムーバブルドライブと判断するドライブを設定した場合、除外対象となりません。
- 除外フォルダを有効にしていても、除外しないフォルダとの関連操作については、ログを取得します。
- 除外フォルダ配下のすべてのフォルダ、サブフォルダ、ファイルが対象です。
- システム環境変数のTEMP、TMPの設定値を変更した場合、変更後の設定値は次回のOS起動後から有効になります。OSを再起動する前は、変更前の値で動作します。
- ユーザー環境変数のTEMP、TMPの設定値を変更した場合、変更後の設定値は次回のログオン後から有効になります。ログオンをしなおす前は、変更前の値で動作します。
- システム環境変数、ユーザー環境変数のTEMP、TMPの設定値に、“¥”や“¥¥”など、¥記号だけを設定した場合、その設定は無効です。
  “¥”はそのプログラムが動作しているときのカレントドライブのルートを示しますが、固定とできないため、除外対象としません。
  また、“¥¥”などはUNC表記のネットワークパスの始まりを示しますが、“¥¥”だけでは意味をなさないため、その場合の除外対象とはしません。
- システム環境変数のTEMP、TMPや、インターネット一時ファイルのフォルダを除外指定とした場合、そのフォルダ名が260バイト以上のパスのときは、そのフォルダは除外対象とせず、ファイル操作ログは採取されます。
  ただし、260バイトちょうどの長さで260バイト目が¥記号の場合は、設定が有効となります。
- 除外対象のパスの中にUNICODE固有の文字が存在する場合、その文字は「?」記号に置き換えて比較動作をします。そのため、ファイル操作ログで同じ場所にUNICODE固有文字があるログはすべて除外動作を行います。
  たとえば、Windowsへのログオン時のユーザー名にUNICODE固有文字が含まれている場合は、同じようにUNICODE固有文字が含まれている他ユーザー名のTEMP、TMPフォルダへのアクセスについても除外する動作を行います。
- Windows Vista®、Windows Server® 2008、Windows® 7において、除外対象のパスの中にUNICODE固有の文字が存在する場合、除外対象とはなりません。

1.2.29 ログオン/ログオフログ

- ログオフログ、PC終了ログ、PC休止ログは、サーバへの即時送信は行いません。いったんクライアント(CT)のローカルディスクに保存された後、管理サーバに送信されます。このため、ログビューアで検索できるまで、時間的にずれる場合があります。
- PCの電源を強制的に切断した場合、ログオフログ、PC終了ログは、次回のクライアント(CT)起動時に作成されます。このため、ログビューアで検索できるまで、時間がかかる場合があります。
- ログオフを行った瞬間にPCの電源を強制切断した場合、そのユーザーのログオフログが2件作成される場合があります。
- Windows Vista®、Windows® 7の場合は、PCの電源切断時にログオンしていた全員のユーザーについて、ログオフログを記録します。

1.2.30 画面キャプチャ

- クライアント(CT)におけるログファイルの格納先のフォルダがあるドライブの空き容量が50MBを下回った場合には画面キャプチャは採取されません。
- 専用のグラフィックボード上で動作するゲーム画面や、ビデオ編集ソフトなど、ハードウエアで直接画面を表示、編集している場合は画面キャプチャできない場合があります。

1.2.31 クライアント(CT)の調査用ログの採取について

クライアント(CT)の調査用ログ(トレースログ)を採取する場合、ファイル操作ログを取得するポリシーを設定していると、トレースのファイル操作ログが大量に取得される場合があります。

1.2.32 ログビューアでのファイル追跡機能について

- バックトレース、フォーワードトレースともに、最大検索件数は1000件です。それ以上の件数があった場合は、超えた時点で検索中止し、検索できた1000件を画面表示します。
- ファイルを「名前を付けて保存」を行った場合、ファイル操作ログでは“作成”と記録され、ログ上では、保存する元となったファイルとの関係は出力されません。そのため、この場合、ファイル追跡は行えません。
- 「持出しユーティリティ」をファイル操作ログの取得対象としている場合、追跡画面には、ファイル持出しのログと、ファイル操作のログの両方が、重複して表示されます。
- 空白を含むファイル名を指定することはできません。空白は、キーワードの区切りとして扱うことから、分けたキーワードのどれか1つでも含まれるレコードを検索します。
- ウィンドウタイトルログはファイル追跡の検索対象ではありません。
- 各ログの、プロセス名(例えば、エクスプローラでファイル操作ログを取得したときの“Explorer.exe”のこと)については、ファイル追跡の検索対象ではありません。
- ファイル操作プロセスの設定で“全て取得する”以外の設定にした場合、ファイル追跡機能で正しくファイルの追跡が行えなくなる場合があります。

第2章 運用環境を整える

本章では、Systemwalker Desktop Keeperの運用方法について説明します。

システム管理者や部門管理者が、クライアント(CT)利用者の操作を監査するために、どのように環境を整備したらよいか、採取された操作ログをどのように検索したらよいか、運用中に設定を変更するにはどのような操作が必要かを説明します。

クライアント(CT)での操作を記録し、監査するための、環境作りについて説明します。

2.1 運用環境を整えるときに考慮すること

クライアント(CT)での操作を禁止したり操作ログを採取したりして、その記録を参照できるように運用環境を整えるとき、以下の3項目を運用方針として決定し、決定内容をSystemwalker Desktop Keeperに設定しなければなりません。

PC使用時に許可する操作、許可しない(禁止する)操作、ログを採取する操作を決定します

決定内容は、[端末初期設定]としてGUIで設定します。

保存されたログをどのようにサーバに送信するかを決定します

決定内容は、[端末動作設定]としてGUIで設定します。

PCや、PCの利用者(ユーザー)を、どんなグループで管理するかを決定します

管理するグループは、構成情報ツリーとして設定します。

2.1.1 ポリシーとは

ポリシーとは

ポリシーとは、システムの運用方針に沿って決定した約束事です。
PC使用時に許可する操作と許可しない(禁止する)操作、および、どの操作のログを採取するかが定められている情報です。

ポリシーで設定できること

Systemwalker Desktop Keeperでは、ポリシーとして「禁止する操作」と「ログを採取する操作」を設定できます。

禁止する操作を設定する

禁止する操作には、以下の種類があります。これらは、システム管理者または部門管理者が、管理コンソールで設定します。

- ファイル持出し禁止

  ポリシーとしてファイル持出し禁止を設定すると、クライアント(CT)がインストールされているPCのドライブ、リムーバブルまたはDVD/CDへのファイルやフォルダの持ち出しを、条件付きで禁止できます。
  設定条件によっては、禁止されたドライブなどへ、「持出しユーティリティ」を使用して、ファイルやフォルダを持ち出すことができます。持ち出すときには、暗号化することもできます。
  「持出しユーティリティ」については、“Systemwalker Desktop Keeper 運用ガイド クライアント編”を参照してください。

- 読み込み禁止

  クライアント(CT)がインストールされているPCのリムーバブルドライブからのデータ読み込みを禁止できます。

- 印刷禁止

  ポリシーとして印刷禁止を設定すると、クライアント(CT)がインストールされているPCでは、指定したアプリケーション以外の印刷を禁止できます。

ー PrintScreenキー禁止

ポリシーとしてPrintScreenキー禁止を設定すると、クライアント(CT)がインストールされているPCでは、キーボードのPrintScreenキーを使用した画面のハードコピーの採取を禁止できます。このとき、どんな画面のバードコピーを採取しようとしたかが明らかになるように、画面キャプチャを採取することもできます。

ー ログオン禁止

ポリシーとしてログオン禁止を設定すると、クライアント(CT)がインストールされているPCからログオンするときに、設定したグループに所属しているユーザー名でのログオンを禁止できます。禁止設定が可能なグループは以下のとおりです。

- Administrators
- Backup Operators
- Debugger Users
- Power Users
- Guests
- Replicator
- Users
- Domain Admins
- Domain Guests
- Domain Users
- Enterprise Admins
- Group Policy Creator Owners

ー アプリケーション起動禁止

ポリシーとしてアプリケーション起動禁止を設定すると、クライアント(CT)がインストールされているPCでは、指定したアプリケーションの起動を禁止できます。

ー メール添付禁止

ポリシーとしてメール添付禁止を設定すると、クライアント(CT)がインストールされているPCから、禁止対象となるファイルをメールに添付して、送信または保存することを禁止できます。
ただし、ポート監視方式(添付ファイルを送信するときに利用するメールソフトが、SMTPプロトコルを使用するタイプのもの)の場合は、保存の禁止はできません。
禁止対象として指定できるファイルは、暗号化していないファイル、または指定した拡張子のファイルです。
また、添付ファイルの中に1つでも、添付禁止対象のファイルがある場合、メール(メール本文と、すべての添付ファイル)は送信できません。

ー URLアクセス禁止

ポリシーとしてURLアクセス禁止を設定すると、クライアント(CT)がインストールされているPCでは、許可されていないURLへのアクセスを禁止できます。

ー FTPサーバ接続禁止

ポリシーとしてFTPサーバ接続禁止を設定すると、クライアント(CT)がインストールされているPCでは、指定したFTPサーバ以外への接続を禁止できます。

ー Webダウンロード禁止

ポリシーとしてWebダウンロード禁止を設定すると、クライアント(CT)がインストールされているPCでは、指定したWebサイト以外からのダウンロードを禁止できます。

ログを採取する操作を設定する

ポリシーとして、どの操作に対してログを採取するかを設定します。採取できる操作ログは以下のとおりです。ポリシーは、システム管理者または部門管理者が、管理コンソールで設定します。

- アプリケーション起動ログ
- アプリケーション終了ログ
- アプリケーション起動禁止ログ
- ウィンドウタイトル取得ログ
- メール送信ログ
- メール送信中止ログ
- メール添付禁止ログ
- コマンドプロンプト操作ログ
- デバイス構成変更ログ
- 印刷操作ログ
- 印刷禁止ログ
- ログオン禁止ログ
- ファイル持出しログ
- PrintScreenキー操作ログ
- PrintScreenキー禁止ログ
- Web操作ログ
- Web操作禁止ログ
- FTP操作ログ
- FTP操作禁止ログ
- ファイル操作ログ
- ログオン/ログオフログ
- 連携アプリケーションログ
- 画面キャプチャ

ポリシーの設定対象

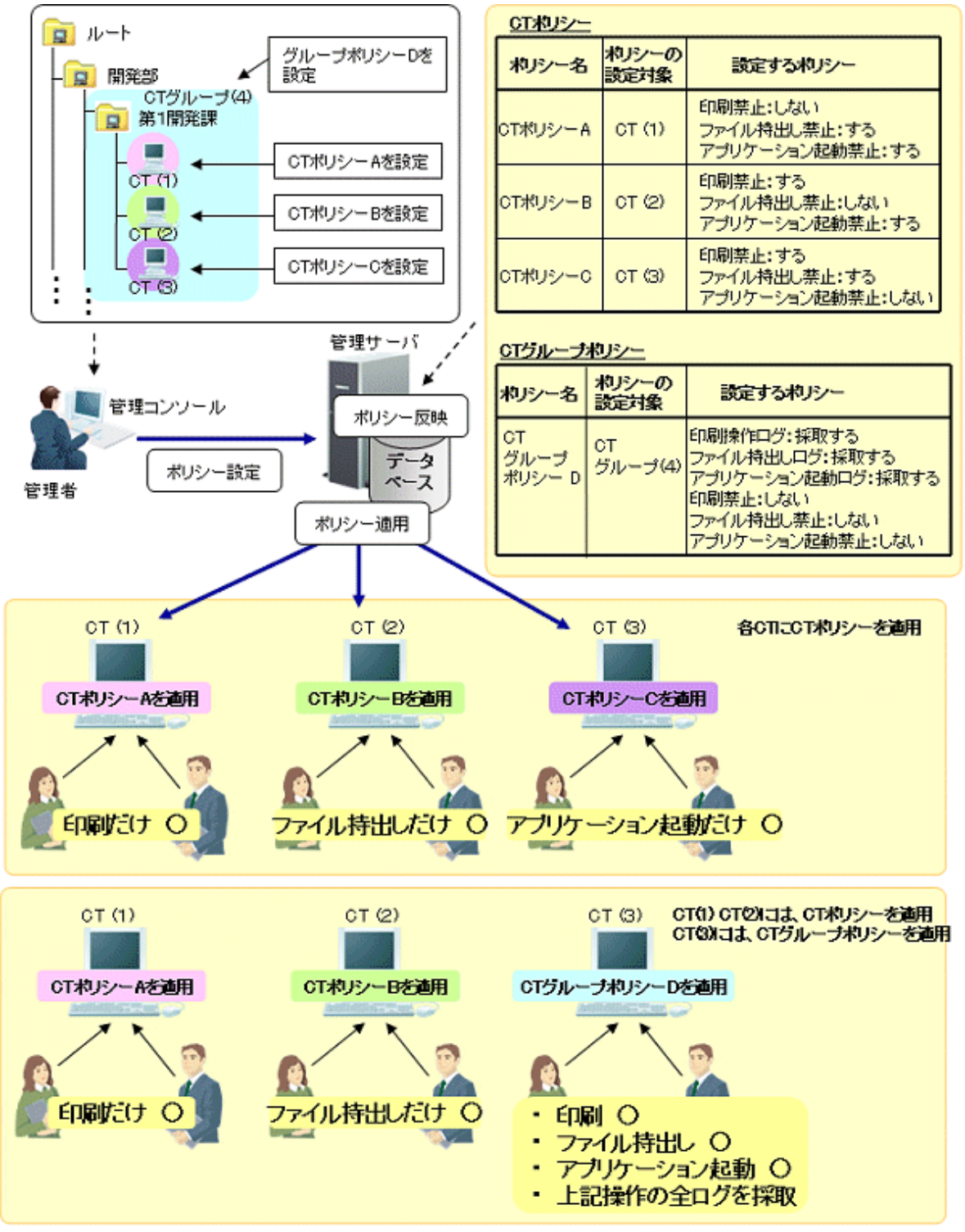
定義したポリシーを、何に対して設定するかによって、ポリシーの名称が異なります。

ポリシーを「クライアント(CT)」に対して設定する場合、「CTポリシー」といいます。
ポリシーを「ユーザー」に対して設定する場合、「ユーザーポリシー」といいます。

クライアント(CT)に対して設定する

クライアント(CT)に対して設定するポリシーを、CTポリシーといいます。クライアント(CT)の操作時に、CTポリシーが有効になっている場合、どのユーザーが操作しても、クライアント(CT)に設定されているポリシーに従って、禁止操作やログ採取が実施されます。クライアント(CT)ごとに異なるポリシーを設定できます。

また、部門ごとにクライアント(CT)をグループ化したり、使用目的が同じクライアント(CT)をグループ化したりして、そのグループに対して設定するポリシーをCTグループポリシーといいます。グループごとに異なる内容のポリシーを設定できます。



上記イメージ図では、管理コンソールからクライアント(CT)とCTグループに対して、以下の設定を行っています。

クライアント(CT)ごとに以下のポリシーを設定します。

ー CT(1)は、印刷だけできます。

印刷禁止:しない
ファイル持出し禁止:する
アプリケーション起動禁止:する

－ CT(2)は、ファイル持出しだけできます。

印刷禁止：する
ファイル持出し禁止：しない
アプリケーション起動禁止：する

－ CT(3)は、アプリケーション起動だけできます。

印刷禁止：する
ファイル持出し禁止：する
アプリケーション起動禁止：しない

クライアント(CT)をグループ化し、グループポリシーとして、“印刷、ファイル持出し、アプリケーション起動を許可”し、“すべてのログを採取”するように設定します。

各クライアント(CT)には、次回起動時または即時にCTポリシーが適用されます。ポリシーが適用されると、適用されたポリシーに従って動作します。

【各CTにCTポリシーを適用した場合】

－ CT(1)は、誰が操作しても、印刷だけできます。

－ CT(2)は、誰が操作しても、ファイル持出しだけできます。

－ CT(3)は、誰が操作しても、アプリケーション起動だけできます。

【CT(1)、CT(2)にはCTポリシーを適用し、CT(3)にはCTグループポリシーを適用した場合】

－ CT(1)は、誰が操作しても、印刷だけできます。

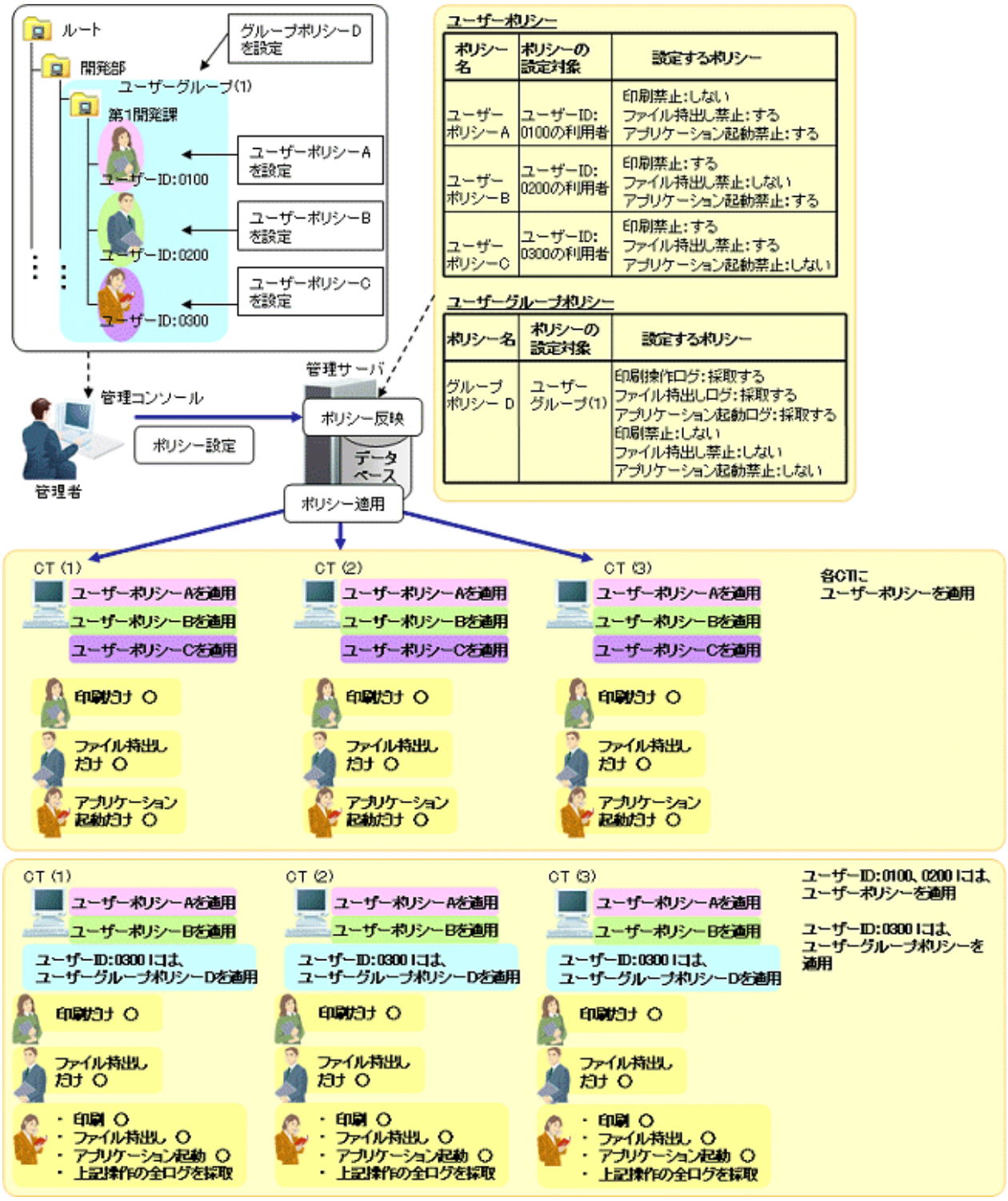
－ CT(2)は、誰が操作しても、ファイル持出しだけできます。

－ CT(3)は、誰が操作しても、印刷、ファイル持出し、アプリケーション起動ができ、各操作のログが採取されます。

ユーザーに対して設定する

クライアント(CT)がインストールされたPCで、Windowsへのログオン時に入力するユーザー名に対して設定するポリシーを、ユーザーポリシーといいます。クライアント(CT)の操作時に、ユーザーポリシーが有効になっている場合、どのPCから操作しても、ログオンしたユーザー名に設定されているポリシーに従って、禁止操作やログ採取が実施されます。ユーザー名ごとに異なるポリシーを設定できます。

また、部門ごとにユーザーをグループ化したり、作業内容が同じユーザーをグループ化したりして、そのグループに対して設定するポリシーをユーザーグループポリシーといいます。グループごとに異なる内容のポリシーを設定できます。



上記イメージ図では、管理コンソールからユーザーとユーザーグループに対して、以下の設定を行っています。

ユーザーごとに以下のポリシーを設定します。

ー　ユーザー名:0100のユーザーは、印刷だけできます。

印刷禁止:しない
ファイル持出し禁止:する
アプリケーション起動禁止:する

ー ユーザー名:0200のユーザーは、ファイル持出しだけできます。

印刷禁止:する
ファイル持出し禁止:しない
アプリケーション起動禁止:する

ー ユーザー名:0300のユーザーは、アプリケーション起動だけできます。

印刷禁止:する
ファイル持出し禁止:する
アプリケーション起動禁止:しない

ユーザーをグループ化し、グループポリシーとして、“印刷、ファイル持出し、アプリケーション起動を許可”し、“すべてのログを採取”するように設定します。

各ユーザー名でWindowsにログオンすると、ユーザーポリシーが適用されます。ポリシーが適用されると、ログオンしたクライアント(CT)のCTポリシーに関係なく、ユーザーポリシーに従って動作します。

【各CTにユーザーポリシーを適用した場合】

ー どのクライアント(CT)でログインしても、そのユーザーが可能な操作は決まっています。

ユーザー名:0100のユーザーは、印刷だけできます。
ユーザー名:0200のユーザーは、ファイル持出しだけできます。
ユーザー名:0300のユーザーは、アプリケーション起動だけできます。

【ユーザー名:0100、ユーザー名:0200にはユーザーポリシーを適用し、ユーザー名:0300にはユーザーグループポリシーを適用した場合】

ー どのクライアント(CT)でログインしても、そのユーザーが可能な操作は決まっています。

ユーザー名:0100のユーザーは、印刷だけできます。
ユーザー名:0200のユーザーは、ファイル持出しだけできます。
ユーザー名:0300のユーザーは、印刷、ファイル持出し、アプリケーション起動ができ、各操作のログが採取されます。

CTポリシー/ユーザーポリシーと設定可能な項目

CTポリシーとユーザーポリシーで、設定できる項目が異なります。以下に、設定可能な項目の一覧を示します。

設定項目		CTポリシー	ユーザーポリシー
禁止機能	ファイル持出し禁止	○	○
	読み込み禁止	○	○
	印刷禁止	○	○
	PrintScreenキー禁止	○	○
	ログオン禁止	○	― (注)
	アプリケーション起動禁止	○	○
	メール添付禁止	○	○
	URLアクセス禁止	○	○
	FTPサーバ接続禁止	○	○
	Webダウンロード禁止	○	○
記録機能	アプリケーション起動ログ	○	○
	アプリケーション終了ログ	○	○
	アプリケーション起動禁止ログ	○	○
	ウィンドウタイトル取得ログ	○	○
	メール送信ログ	○	○

設定項目		CTポリシー	ユーザーポリシー
	メール送信中止ログ	○	○
	メール添付禁止ログ	○	○
	コマンドプロンプト操作ログ	○	○
	デバイス構成変更ログ	○	○
	印刷操作ログ	○	○
	印刷禁止ログ	○	○
	ログオン禁止ログ	○	― (注)
	ファイル持出しログ	○	○
	PrintScreenキー操作ログ	○	○
	PrintScreenキー禁止ログ	○	○
	Web操作ログ	○	○
	Web操作禁止ログ	○	○
	FTP操作ログ	○	○
	FTP操作禁止ログ	○	○
	ファイル操作ログ	○	― (注)
	ログオン/ログオフログ	○	― (注)
	連携アプリケーションログ	○	― (注)
	画面キャプチャ	○	○

○:設定できます。
―:設定できません。

注) クライアント(CT)操作時にユーザーポリシーが有効になる運用の場合、ユーザーポリシーとして設定できない項目に対しては、操作しているクライアント(CT)のCTポリシーの設定値が有効になります。

運用形態と、有効になる禁止操作/採取されるログ

CTポリシーやユーザーポリシーが設定され、クライアント(CT)に反映されると、クライアント(CT)での操作禁止やログ採取ができるようになりますが、運用形態によって、有効になる禁止操作と採取されるログが異なります。
以下に、有効になる項目の一覧を示します。

また、使用している環境によって、機能が制限される場合があります。詳細は、“1.2 機能に関する留意事項”を参照してください。

運用形態		Systemwalker Desktop Keeperのクライアント(CT)の操作を記録する場合			Citrix XenApp Server上の操作を記録する場合 (注1)
OSの起動モード		通常モードで起動(OS起動後 Windowsに ログオン) する場合	セーフモード または ネットワークが使える セーフモードで起動する場合 (注3)		通常モードで起動 (OS起動後 Windows にログオン)する 場合
			Windows Vista® Windows® 7 Windows Server® 2008	Windows® 2000 Windows® XP Windows Server® 2003	
禁	ファイル持出し禁止	○	○	○	―

運用形態		Systemwalker Desktop Keeperのクライアント(CT)の操作を記録する場合			Citrix XenApp Server上の操作を記録する場合 (注1)
OSの起動モード		通常モードで起動(OS起動後 Windowsにログオン)する場合	セーフモード または ネットワークが使える セーフモードで起動する場合 (注3)		通常モードで起動 (OS起動後 Windows にログオン)する場合
			Windows Vista® Windows® 7 Windows Server® 2008	Windows® 2000 Windows® XP Windows Server® 2003	
止機能	印刷禁止	○	—	—	—
	PrintScreenキー禁止	○	○	○	—
	ログオン禁止	○	○	○	—
	アプリケーション起動禁止	○	○	○	—
	メール添付禁止	○	—	○	—
	URLアクセス禁止	○	○	○	—
	FTPサーバ接続禁止	○	○	○	—
	Webダウンロード禁止	○	○	○	—
記録機能	アプリケーション起動ログ	○	○	○	○
	アプリケーション終了ログ	○	○	○	○
	アプリケーション起動禁止ログ	○	○	○	—
	ウィンドウタイトル取得ログ	○	○	○	○
	ウィンドウタイトル取得ログ (URL付き)	○	○	○	○
	メール送信ログ	○	—	○	—
	メール送信中止ログ	○	○	○	—
	メール添付禁止ログ	○	—	○	—
	コマンドプロンプト操作ログ	○(注4)	○	○	○
	デバイス構成変更ログ	○	○	○	—
	印刷操作ログ	○	—	—	○
	印刷禁止ログ	○	—	—	—
	ログオン禁止ログ	○	○	○	—
	ファイル持出しログ	○	○	○	—
	PrintScreenキー操作ログ	○	○	○	○
	PrintScreenキー禁止ログ	○	○	○	—
	Web操作ログ	○	○	○	—
	Web操作禁止ログ	○	○	○	—
	FTP操作ログ	○	○	○	—
	FTP操作禁止ログ	○	○	○	—
	ファイル操作ログ	○	○	○	○

運用形態		Systemwalker Desktop Keeperのクライアント(CT)の操作を記録する場合			Citrix XenApp Server上の操作を記録する場合 (注1)
OSの起動モード		通常モードで起動(OS起動後 Windowsにログオン) する場合	セーフモード または ネットワークが使える セーフモードで起動する場合 (注3)		通常モードで起動 (OS起動後 Windows にログオン)する 場合
			Windows Vista® Windows® 7 Windows Server® 2008	Windows® 2000 Windows® XP Windows Server® 2003	
	ログオン/ログオフログ	○	○(注2)	○(注2)	○(注2)
	連携アプリケーションログ	○	○	○	—
	画面キャプチャ	○	○	○	—

○:有効です。
—:無効です。

注1) Citrix XenApp 監視に設定されるポリシーは、CTポリシーです。ユーザーポリシーは設定されません。
注2) PC休止ログ、PC復帰ログは、採取されません。
注3) セーフモードまたはネットワークが使えるセーフモードで起動した場合は、CTポリシーだけの動作となります。ユーザーポリシーは適用されません。
注4) Windows Server® 2008 64ビット版、Windows Server® 2008 R2では、禁止およびログの採取はできません。

2.1.2 ポリシー適用のしくみ

ポリシーが反映されるタイミング

クライアント(CT)が管理サーバと接続すると、クライアント(CT)は、管理サーバからポリシーを獲得します。

管理コンソールで更新されたCTポリシーは、即時に、またはクライアント(CT)の次回起動時に反映されます。

更新されたユーザーポリシーは、即時に、または統合管理サーバまたは管理サーバに登録されたユーザー名を持つユーザーの次回ログオン時に反映されます。
ユーザーポリシーが即時に反映されるのは、サーバに登録されたユーザー名でログオン中に、ユーザーポリシーの更新とCTポリシーの即時更新が行われた場合です。CTポリシーの即時更新と同時にユーザーポリシーも即時反映されます。

ポリシーの遷移

システム管理者(部門管理者)やクライアント(CT)利用者が、どのような操作をしたときに、どのポリシーが有効になるかは、場合によって異なります。
操作内容と有効になるポリシーの関係を説明します。

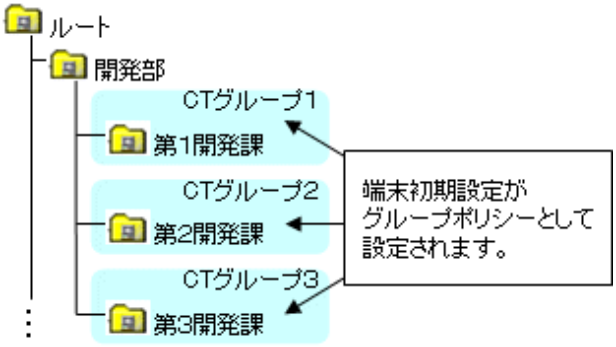
設定されているポリシーを確認する場合は、管理コンソールを起動してください。
CTポリシーは、CTグループツリーで、確認したいクライアント(CT)が属するCTグループを選択後、CTリストからクライアント(CT)を選択するとポリシー一覧に表示されます。
ユーザーポリシーは、[ユーザー設定]メニューから[ユーザーポリシー設定]を選択して表示される画面で、確認したいユーザーが属するユーザーグループを選択後、ユーザーリストからユーザーを選択すると、ポリシー一覧に表示されます。

CTグループポリシーとCTポリシーの関係

1. グループを作成します。

   グループポリシーとして、端末初期設定の値が設定されます。

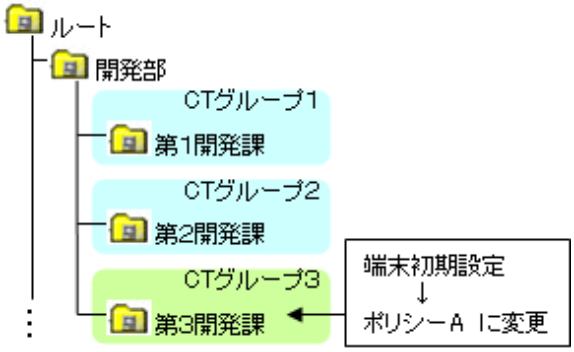
ただし、3階層の構成の場合で、統合管理サーバに接続した管理コンソールから統合管理サーバ配下の管理サーバにCTグループを作成したときは、そのCTグループには、統合管理サーバで設定したポリシーが設定されます。



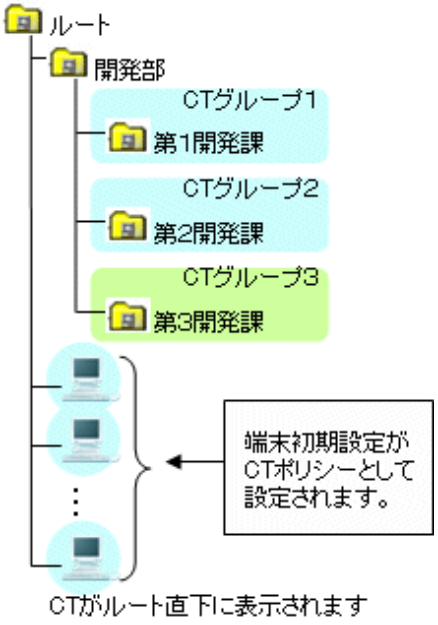
2. 必要に応じて、グループポリシーを変更します。

   以下のようにグループポリシーを変更します。

   - 「CTグループ3」のグループポリシーを「端末初期設定値」から「ポリシーA」に変更

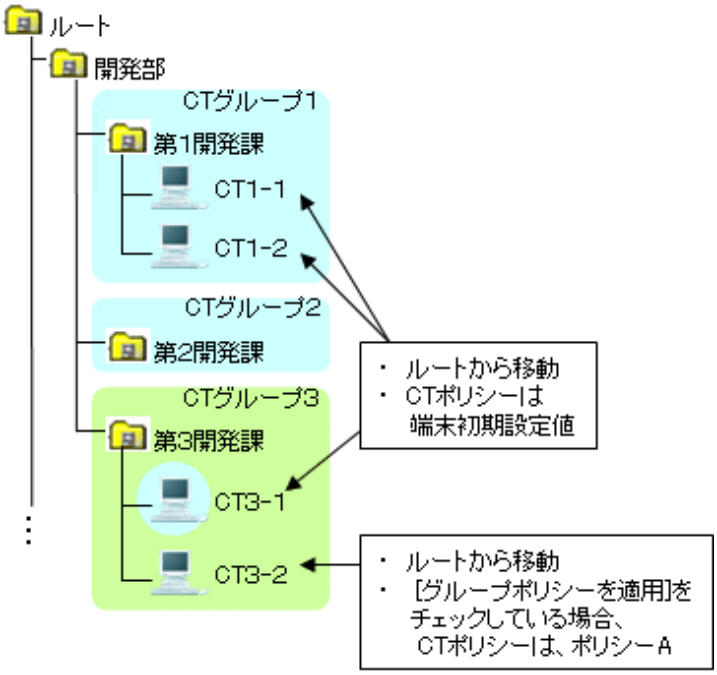


3. CTがインストールされ、クライアント(CT)と管理サーバが通信すると、CTポリシーとして、端末初期設定の値が設定されます。



4. クライアント(CT)を各グループに移動します。

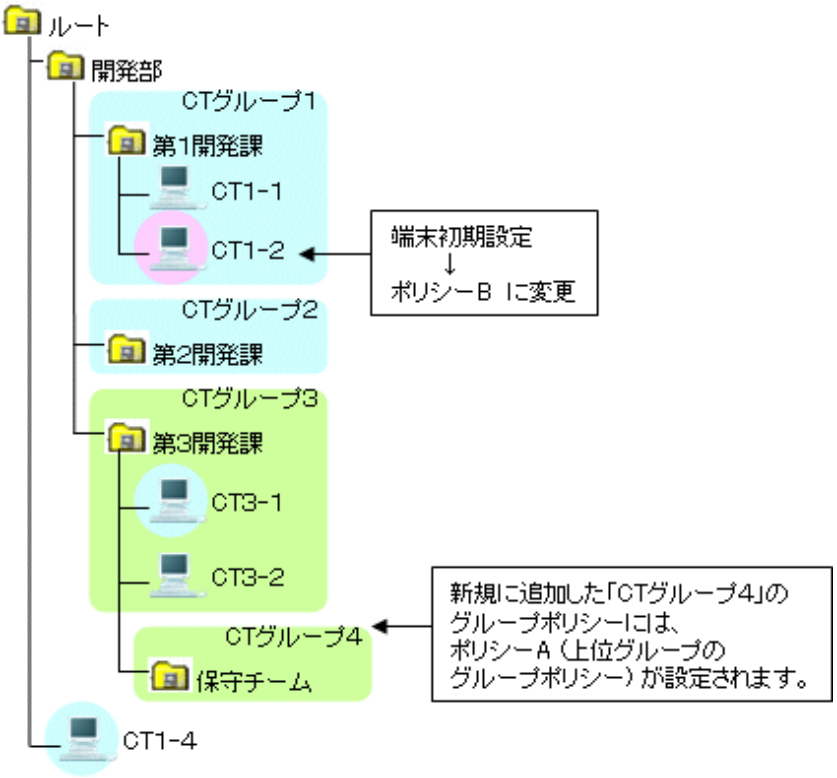
   ルートからそのまま移動したクライアント(CT)のCTポリシーには、端末初期設定の値が設定されています。
   「グループポリシーを適用」をチェックしているクライアント(CT)のポリシーには、移動先のグループポリシーが設定されます。



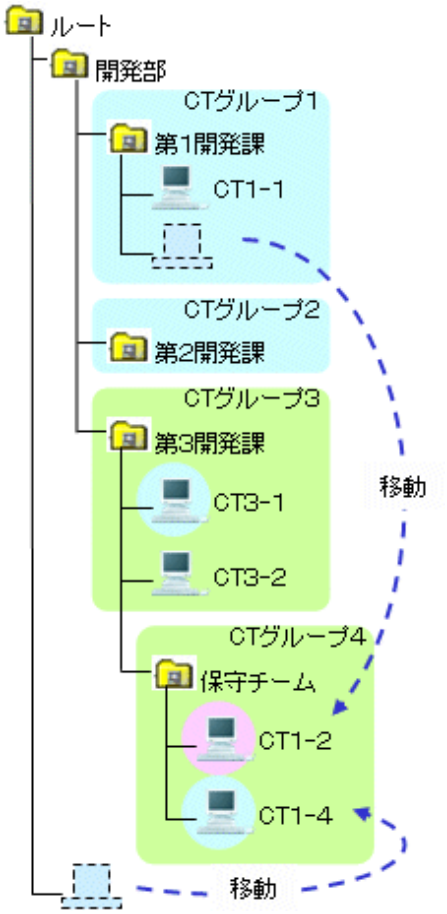
5. サブグループを新規作成します。

   新規作成したサブグループのグループポリシーには、上位グループのグループポリシーが設定されます。

   また、「CT1-2」のCTポリシーを変更し、「端末初期設定値」から「ポリシーB」に変更します。

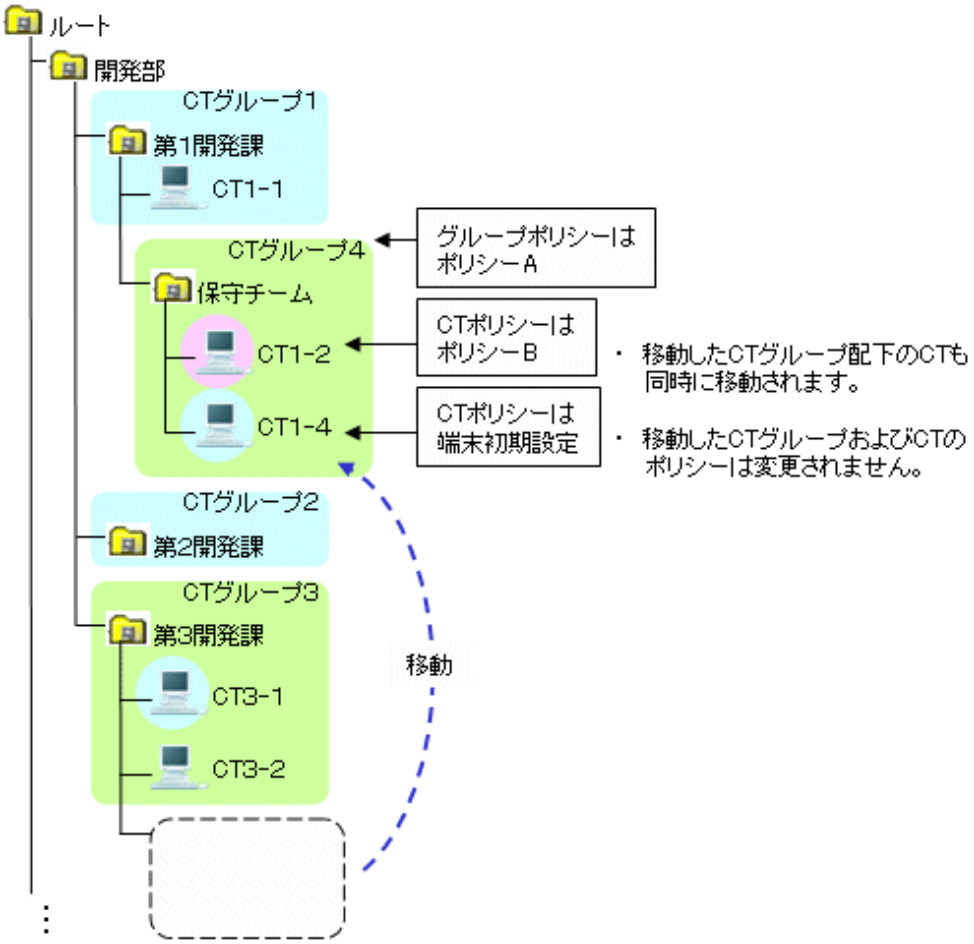


6. CTを移動します。


ルート
開発部
CTグループ1
第1開発課
CT1-1
CTグループ2
第2開発課
CTグループ3
第3開発課
CT3-1
CT3-2
移動
CTグループ4
保守チーム
CT1-2
CT1-4
移動

7. CTグループを移動します。

   CTグループを移動すると、配下のCTも同時に移動されます。
   移動したCTグループおよびCTのポリシーは、変更されません(移動前のポリシーのままです)。



8. ルート直下に存在するCTは、[グループポリシーを適用する]をチェックして、そのCTのポリシーを即時更新しても、CTポリシーが適用されます。[グループポリシーを適用する]の設定は、無効になります。

ユーザーグループポリシーとユーザーポリシーの関係

ユーザーグループポリシーとユーザーポリシーの関係は、“CTグループポリシーとCTポリシーの関係”で説明したポリシーの遷移と同じです。

クライアント(CT)操作と有効になるポリシー

CTポリシーとユーザーポリシーの両方で運用する場合、クライアント(CT)操作時に有効になるポリシーについて説明します。

ユーザーポリシーの適用は、Windowsへのログオン時に入力するユーザー名を元に、統合管理サーバまたは管理サーバにユーザー情報(ユーザー名)が登録されているか確認した結果で判断されます。
この場合、ドメイン認証の状態に関係なくWindowsへのログオン時に入力するユーザー名だけでチェックします。そのため、ドメイン認証されていないユーザー名の場合でも、統合管理サーバまたは管理サーバに登録されているユーザー情報(ユーザー名)と一致すれば、一致したユーザー情報(ユーザー名)のユーザーポリシーが適用されます。

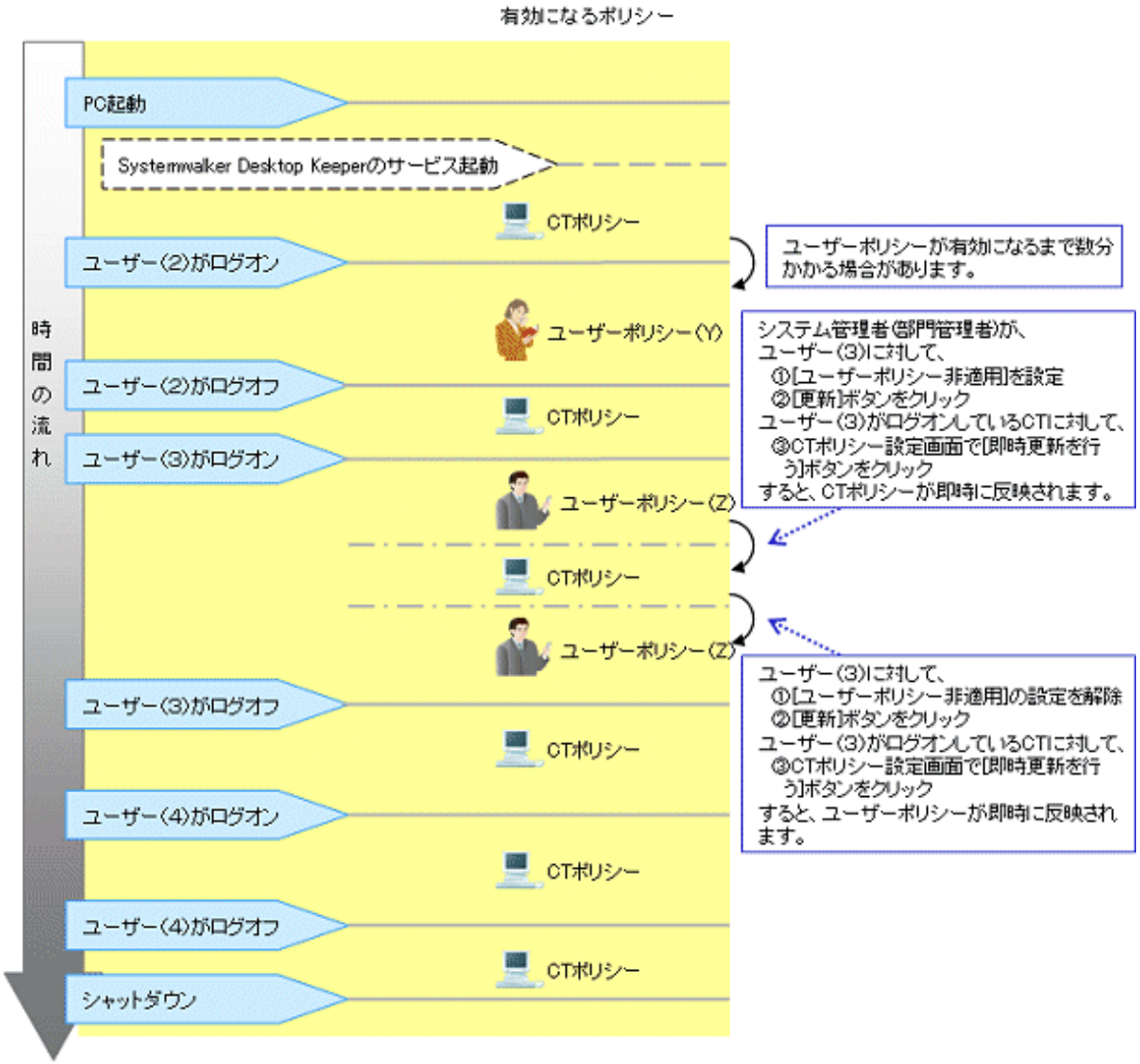
「ユーザー(1)」～「ユーザー(5)」までの5人のうち、3人を管理サーバに登録します。
ユーザーの登録後、「ユーザー(1)」～「ユーザー(3)」のユーザーポリシーを、以下のように設定したとします。

ユーザー名	ユーザーポリシー
ユーザー(1)	ポリシーX

ユーザー名	ユーザーポリシー
ユーザー(2)	ポリシーY
ユーザー(3)	ポリシーZ

ユーザー(4)およびユーザー(5)は、未登録です。

クライアント(CT)と管理サーバが、終始オンラインの場合



1. クライアント(CT)を起動します。

   Systemwalker Desktop Keeperのサービスが起動されると、CTポリシーが有効になります。(PCの起動直後は、Systemwalker Desktop Keeperのサービスが起動するまで、CTポリシーの設定が有効になりません。)

2. ユーザー(2)がクライアント(CT)にログオンします。

   ユーザーポリシー(ポリシーY)が有効になります。
   Windowsへのログオン直後は、ユーザーポリシーが適用されるまでに時間がかかる(2～3分)ことがあります。ユーザーポリシーが適用されるまでは、CTポリシーが有効です。

3. ユーザー(2)がログオフします。

   CTポリシーが有効になります。

4. ユーザー(3)がクライアント(CT)にログオンします。

   ユーザーポリシー(ポリシーZ)が有効になります。

   a) システム管理者(部門管理者)が、[ユーザーポリシー設定]画面で、ユーザー(3)に対して、[ユーザーポリシー非適用]を設定後、[更新]ボタンをクリックします。

   b) その後、ユーザー(3)がログオンしているCTに対して、CTポリシー設定画面で[即時更新を行う]ボタンをクリックします。
   →CTポリシーが即時反映されます。

   c) システム管理者(部門管理者)が、[ユーザーポリシー設定]画面で、ユーザー(3)に対して、[ユーザーポリシー非適用]の設定を解除し、[更新]ボタンをクリックします。

   d) その後、ユーザー(3)がログオンしているCTに対して、CTポリシー設定画面で[即時更新を行う]ボタンをクリックします。
   →ユーザーポリシー(ポリシーZ)が即時反映されます。

5. ユーザー(3)がログオフします。

   CTポリシーが有効になります。

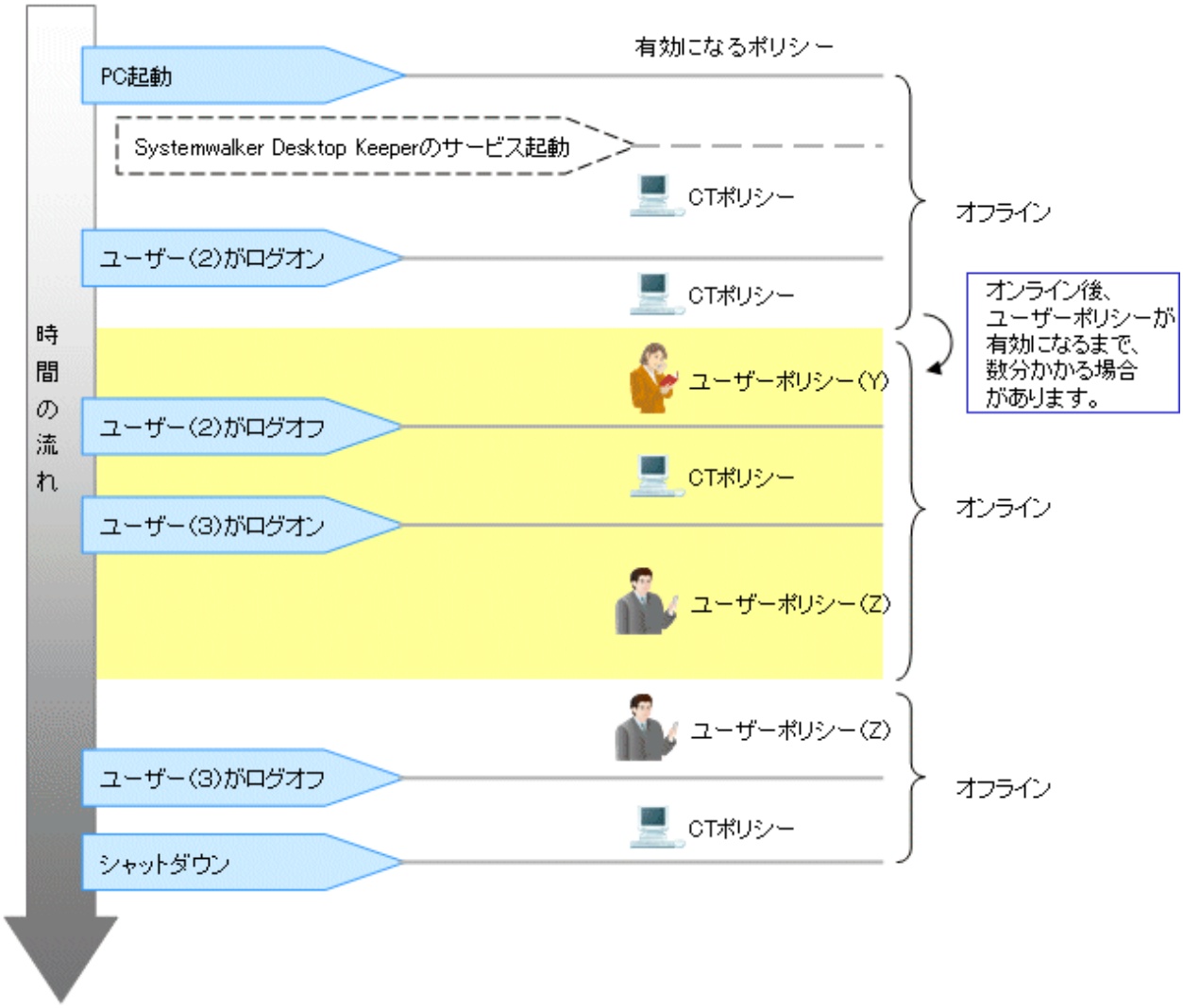
6. ユーザー(4)がクライアント(CT)にログオンします。

   CTポリシーが有効です。
   ユーザー登録されていないユーザーがログオンした場合は、CTポリシーで動作します。

7. ユーザー(4)がログオフします。

   CTポリシーが有効です。

クライアント(CT)と管理サーバが、終始オンラインではない場合



1. オフライン時に、クライアント(CT)を起動します。

   Systemwalker Desktop Keeperのサービスが起動されると、CTポリシーが有効になります。(PCの起動直後は、Systemwalker Desktop Keeperのサービスが起動するまで、CTポリシーの設定が有効になりません。)

2. ユーザー(2)がクライアント(CT)にログオンします。

   オフライン時、クライアント(CT)は、管理サーバからユーザー情報を入手できないため、CTポリシーが有効になります。

   ログオン中にオンラインになった場合は、ユーザーポリシー(ポリシーY)が有効になります。オンライン直後は、ユーザーポリシーが適用されるまでに時間がかかる(2～3分)ことがあります。

3. ユーザー(2)がログオフします。

   CTポリシーが有効になります。

4. ユーザー(3)がクライアント(CT)にログオンします。

   ユーザーポリシー(ポリシーZ)が有効になります。

   ログオン中にオフラインになった場合は、ユーザーポリシーが継続して有効になります。

5. ユーザー(3)がログオフします。

   CTポリシーが有効になります。

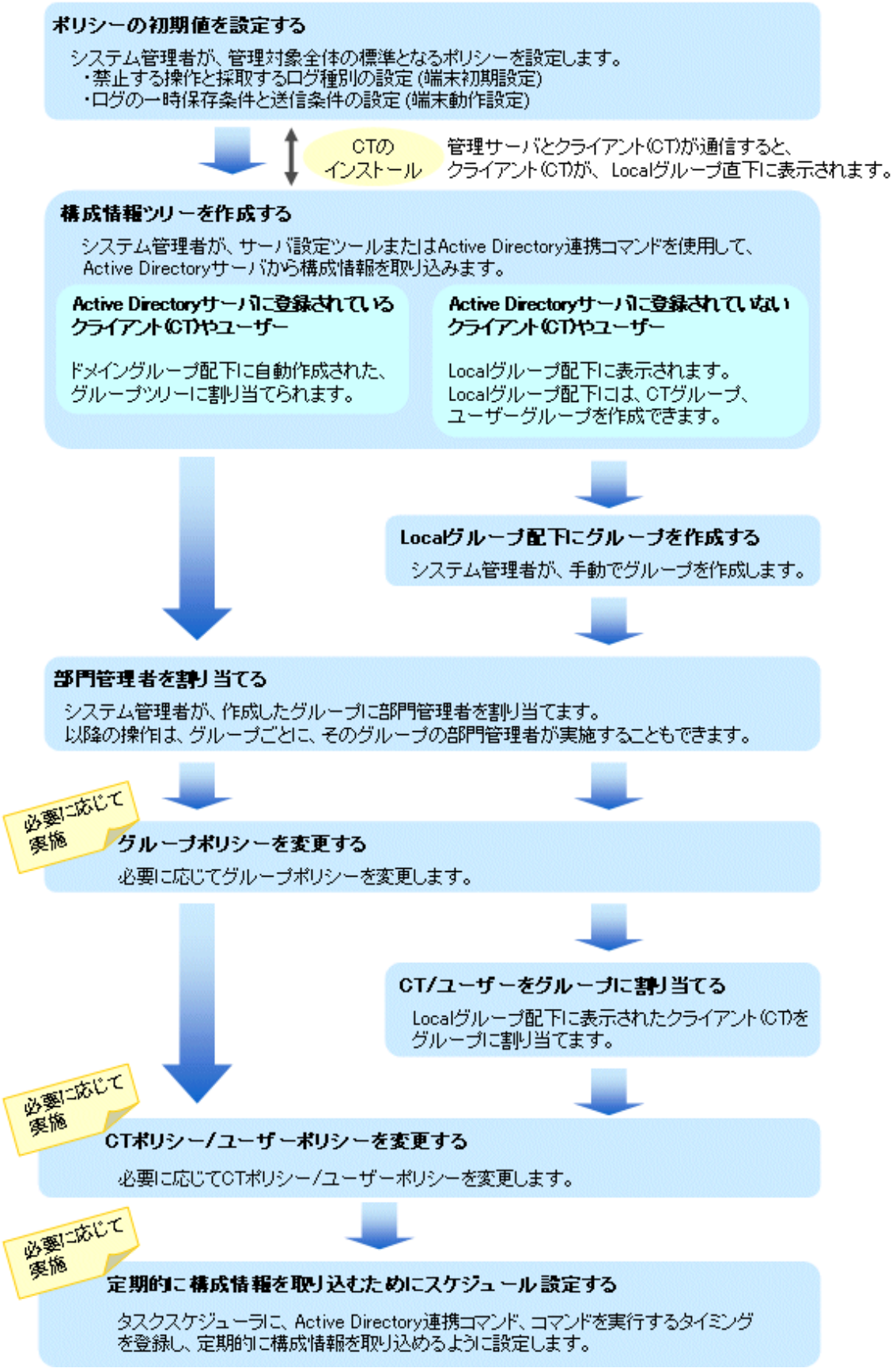
2.2 運用環境を整える流れ

Systemwalker Desktop Keeperの導入直後から、クライアント(CT)での操作を監査できるまでに実施する作業の流れを、以下に示します。

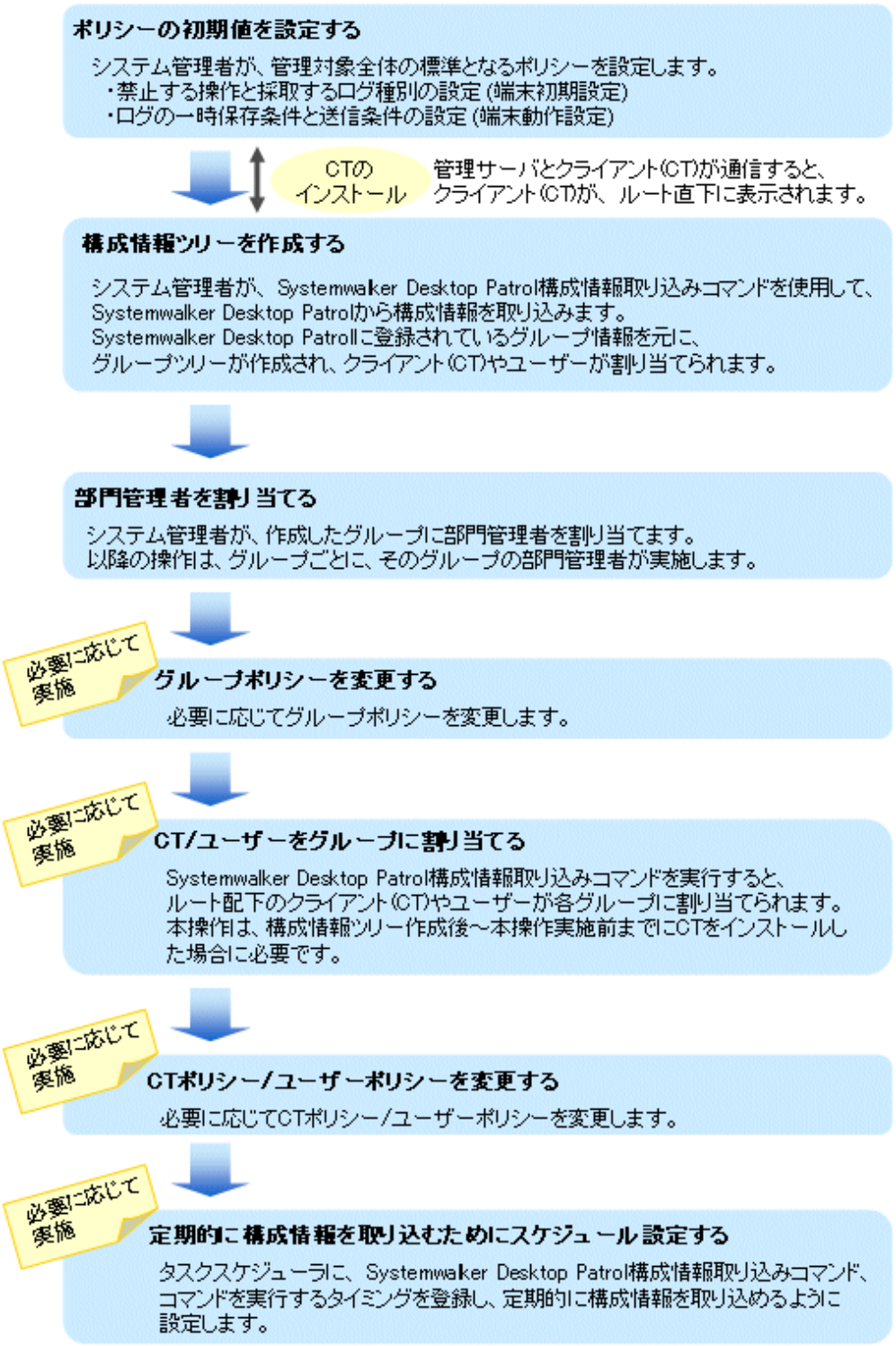
構成情報ツリーの作成方法によって、流れが異なります。

- Active Directoryから構成情報を取り込む場合
- Systemwalker Desktop Patrolから構成情報を取り込む場合
- 管理コンソールで構成情報を作成する場合

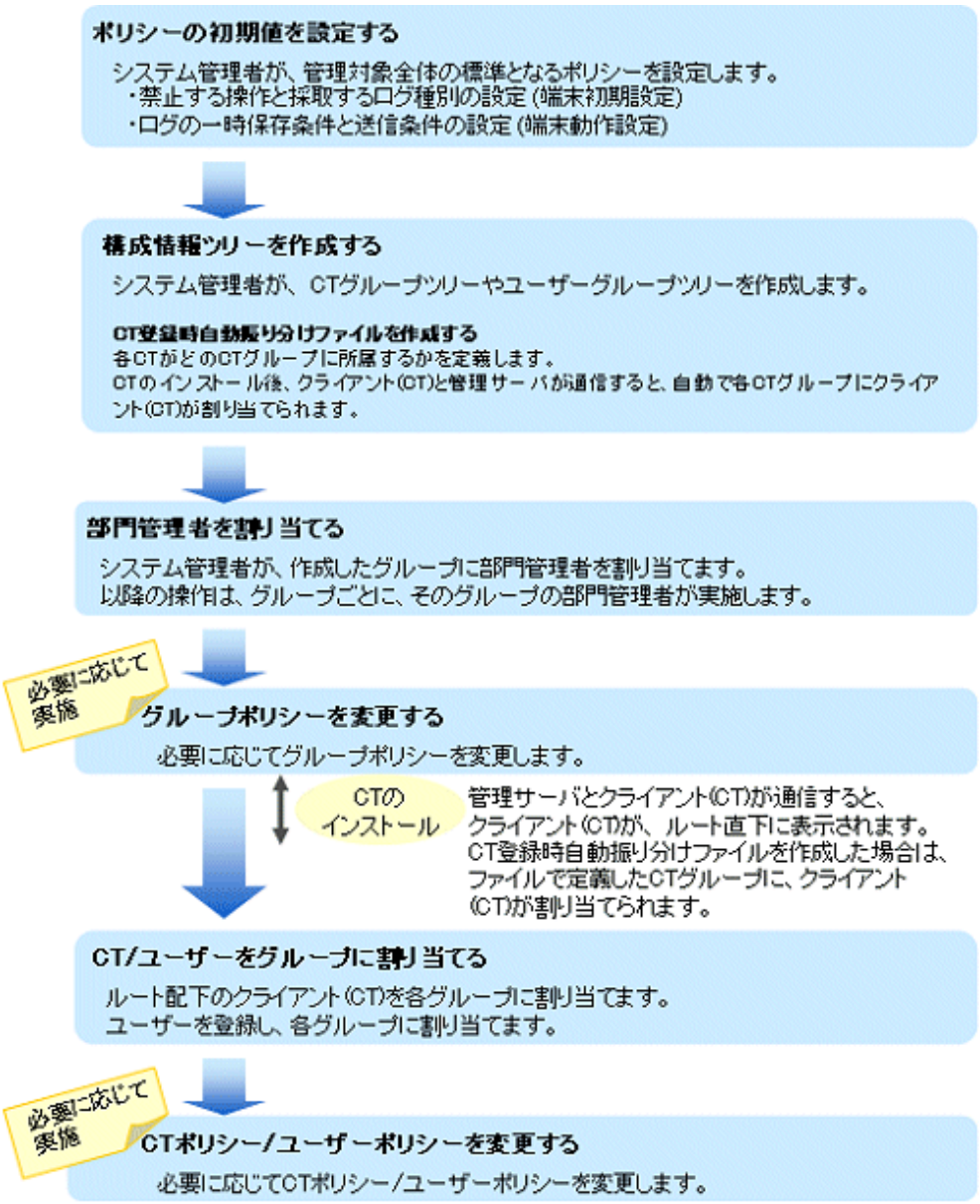
Active Directoryから構成情報を取り込む場合



Systemwalker Desktop Patrolから構成情報を取り込む場合



管理コンソールで構成情報を作成する場合



2.3 管理コンソールを起動する

管理コンソールを起動する

注意

ポリシーの不正な変更を防止するために

管理コンソール起動後に、管理コンソールをインストールしたPCから離れる場合は、不正なポリシーの設定変更を防止するため、管理コンソールを終了してください。

管理コンソールの起動時間を速くするために

管理対象のCT台数が多い場合(目安として2000台以上)、管理コンソールの起動時間が遅くなります。管理コンソールの[起動時の最新情報取得]の設定を[統合管理サーバから取得]に設定することで、遅くならないように回避できます。
この設定は、管理コンソールを統合管理サーバに接続したときに有効になります。

1. 管理コンソールをインストールしたPCの[スタート]メニューから[プログラム]-[Systemwalker Desktop Keeper]-[管理コンソール]-[管理コンソール]を選択します。

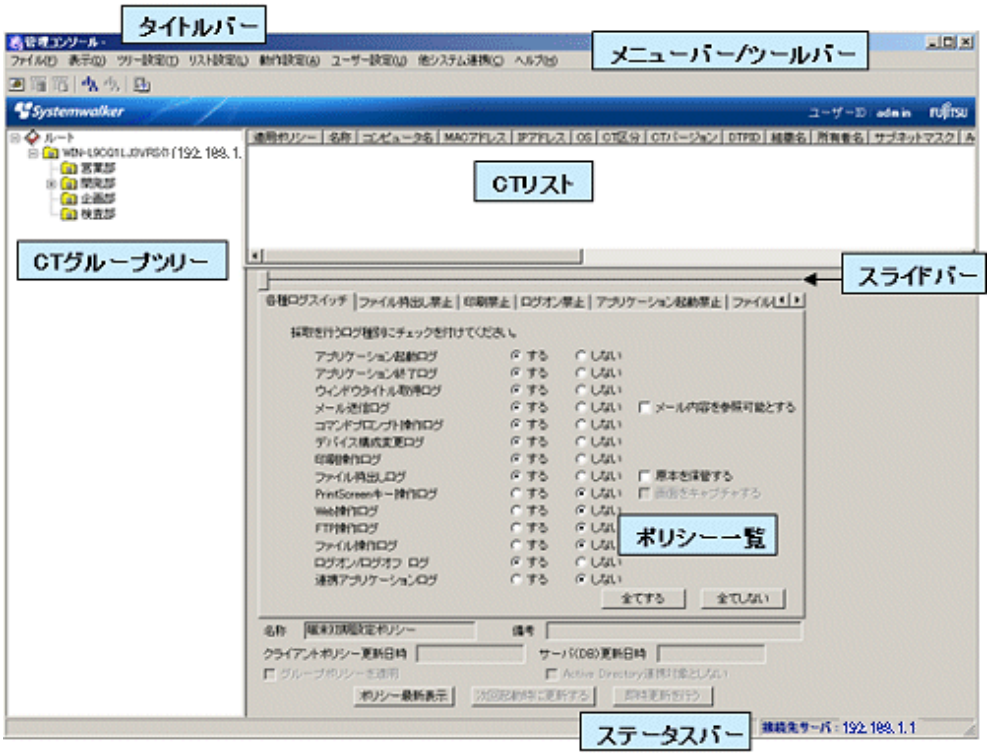
   →[Systemwalker Desktop Keeper 管理コンソール]画面が表示されます。

2. 以下の情報を入力し、[OK]ボタンをクリックします。
   システム管理者と部門管理者とで、ログイン方法に違いはありません。

   - **[接続先サーバ名]:**接続する管理(統合管理)サーバの、IPアドレスまたはコンピュータ名を選択します。
   - **[ユーザーID]:**サーバ設定ツールの[管理者情報設定]画面で設定した[ユーザーID]です。
   - **[パスワード]:**サーバ設定ツールの[管理者情報設定]画面で設定した[パスワード]です。

     パスワードは定期的に変更することを推奨します。変更方法は、“管理コンソール起動時のパスワードを変更する”を参照してください。

→[管理コンソール]画面が表示されます。
画面やメニューバーに表示される情報は、システム管理者がログオンする場合と部門管理者がログオンする場合とで異なります。



画面の表示内容

[管理コンソール]画面の各部の名称を説明します。

CTグループツリー

Active Directory連携によって取り込まれたCTグループ情報や、作成したCTグループが表示されます。

最新のCTグループツリーの情報を確認する場合は、[ツリー設定]メニューから[ツリー最新表示(全サーバ)]を選択します。
[ツリー設定]メニューから[ツリー全展開]を選択すると、すべてのCTグループが表示されます。
[ツリー設定]メニューから[ツリー全縮小]を選択すると、ルート直下(サーバ表示時はサーバ直下、ドメイン表示時はドメイン直下)のCTグループだけ表示します。
CTグループを選択した時点で、CTグループ単位に設定されているCTポリシーは最新表示されます。

CTグループツリーに表示されるサーバ名は、サーバ設定ツールの[サーバ情報設定]画面の[コンピュータ名]で設定した値が表示されます。

CTグループツリーのアイコンについて

管理コンソールにログオンする人や、Active Directory連携の実施状況によって、CTグループツリーに表示されるアイコンが異なります。

以下に、各アイコンが表示される条件を説明します。

管理コンソールにログオンする人	Active Directory連携の状況	表示されるアイコン	アイコンの意味
システム管理者	Active Directory連携を行っている場合		部門管理者が設定されているグループを示します。
			部門管理者が設定されていないグループを示します。

管理コンソールにログオンする人	Active Directory連携の状況	表示されるアイコン	アイコンの意味
	Active Directory連携を行っていない場合、またはActive Directory連携時のlocalグループの場合		部門管理者が設定されているグループを示します。
			部門管理者が設定されていないグループを示します。
	—		「削除したCT」グループを示します。
部門管理者	Active Directory連携を行っている場合		自分が部門管理者として設定されているグループを示します。
			自分が部門管理者として設定されていないグループを示します。
			配下のサブグループに、自分が部門管理者として設定されているCTグループが存在するグループを示します。
	Active Directory連携を行っていない場合、またはActive Directory連携時のlocalグループの場合		自分が部門管理者として設定されているグループを示します。
			自分が部門管理者として設定されていないグループを示します。
			配下のサブグループに、自分が部門管理者として設定されているCTグループが存在するグループを示します。

CTリスト

CTがインストールされているPCが表示されます。CTリストに表示される項目は、以下のとおりです。

項目名	説明
[適用ポリシー]	クライアント(CT)に適用されているポリシーが表示されます。 ・ [CT]:CTポリシーが設定されていることを示します。 ・ [グループ]:CTグループポリシーが設定されていることを示します。
[名称]	クライアント(CT)に付けることができる名称で、初期値はコンピュータ名です。変更する場合は、“CTポリシーを変更する”を参照し、管理コンソールのCTポリシー設定画面で実施してください。クライアント(CT)インストール後にクライアント(CT)のコンピュータ名を変更しても、名称は変更されません。
[コンピュータ名]	クライアント(CT)のコンピュータ名です。
[MACアドレス]	クライアント(CT)のMACアドレスです。
[IPアドレス]	クライアント(CT)のIPアドレスです。
[OS]	クライアント(CT)のOS名です。
[CT区分]	クライアント(CT)がStandard Editionの場合だけ[SE]と表示されます。
[CTバージョン]	インストールされているSystemwalker Desktop Keeperのクライアント(CT)のバージョンです。なお、製品のバージョン/エディションとの対応は、“Systemwalker Desktop Keeper リファレンスマニュアル”の“CTバージョン”を参照してください。
[DTPID]	Systemwalker Desktop Patrolのクライアント(CT)の「ユーザーID(+)PC名」です。 Systemwalker Desktop Keeperのクライアント(CT)およびSystemwalker Desktop Patrolのクライアント(CT)が同一のマシンにインストールされている場合に表示されます。

項目名	説明
[組織名]	クライアント(CT)のOSに設定されている組織名です。
[所有者名]	クライアント(CT)のOSに設定されている所有者名です。
[サブネットマスク]	クライアント(CT)のネットワークで設定されているサブネットマスクです。
[Active Directory連携]	クライアント(CT)が、Active Directory連携によって情報を取り込んでいるかどうかが表示されます。 ・ Active Directory連携によって情報を取り込んでいるクライアント(CT)の場合: (空欄) ・ Active Directory連携以外の方法で情報を取り込んでいるクライアント(CT)の場合: [非対象]と表示されます。
[ネットワーク参加状況]	クライアント(CT)のネットワーク参加状況が表示されます。 ・ [ドメイン]: ドメインに所属している場合に表示されます。 ・ [ワークグループ]: ドメインに所属していない場合に表示されます。
[所属ドメイン名]	クライアント(CT)が所属しているドメイン名が表示されます。 [ネットワーク参加状況]が[ワークグループ]の場合は、ワークグループ名が表示されます。
[最終ログオン日時]	クライアント(CT)は起動時に統合管理サーバまたは管理サーバと通信します。その通信でサーバがクライアント(CT)に実施した以下の処理の最終日時です。 ・ CTポリシー送信 ・ ユーザーポリシー送信
[クライアントポリシー更新日時]	管理サーバまたは統合管理サーバが、クライアント(CT)にCTポリシーを送信した最終日時です。 以下の場合に表示または更新されます。 ・ CTリストに追加されたクライアント(CT)が再起動されて、統合管理サーバまたは管理サーバとの通信が開始されたとき ・ 管理コンソールの[即時更新を行う]ボタンをクリックして、クライアント(CT)に対してCTポリシーが反映されたとき
[サーバ(DB)更新日時]	管理サーバまたは統合管理サーバがクライアント(CT)のポリシーを更新し、データベースに反映した最終日時です(即時更新も含みます)。
[備考]	クライアント(CT)のポリシー反映時に入力した情報です。 変更する場合は、“CTポリシーを変更する”を参照してください。
[DTPバージョン]	PCにインストールされている、Systemwalker Desktop Patrol CTのバージョンです。
[トレース状態]	クライアント(CT)でのトレース採取の設定内容です。 ・ [概要]:クライアント(CT)のトレースを概要レベルで採取します。 ・ [詳細]:クライアント(CT)のトレースを詳細レベルで採取します。 ・ 空欄:クライアント(CT)のトレースを採取しません、またはクライアント(CT)がV12.0の場合です。

最新のCTリストの情報を確認するには、以下の操作を行います。

- CT単位に確認する場合

  CTリストでCTを選択します。このとき、CTポリシーも最新表示されます。

- 全CTに対して情報を最新にする場合

  [ツリー設定]メニューから[ツリー最新表示(全サーバ)]を選択します。

- 選択している管理サーバ配下の全CTに対して情報を最新にする場合

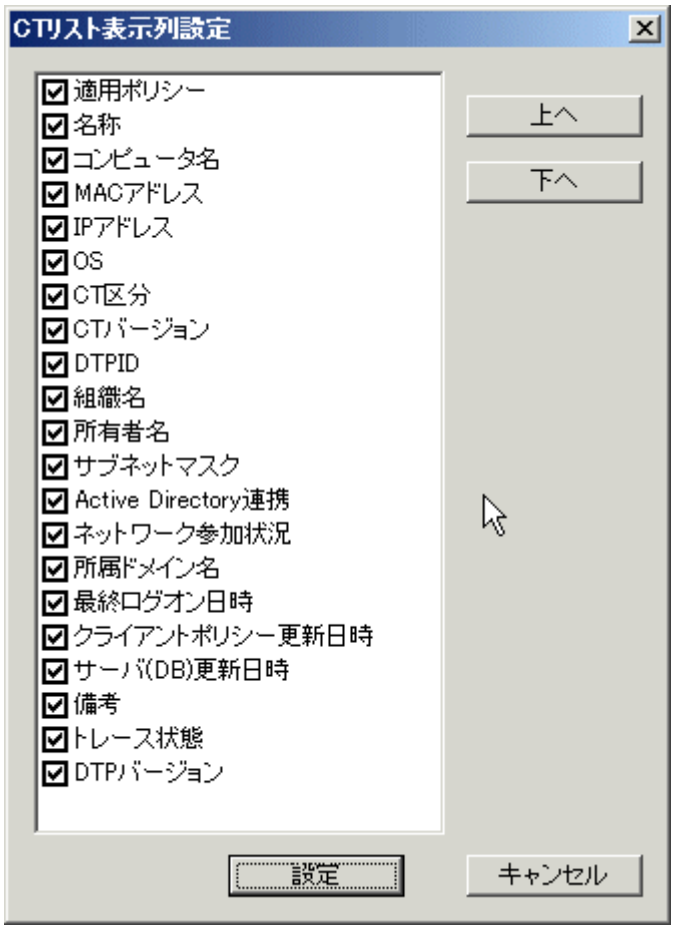
  [ツリー設定]メニューから[ツリー最新表示(選択中サーバ)]を選択します。

CTリストに表示されている項目は、表示する項目や表示の順序を変更することができます。手順は、以下のとおりです。

表示される項目と順序を変更する場合

1. [管理コンソール]画面を起動します。
2. [リスト設定]メニューから[CTリスト表示列設定]を選択します。

   →[CTリスト表示列設定]画面が表示されます。



3. CTリストに表示するチェックボックスをチェックします。
4. CTリストの表示順序を変更する項目を選択し、[上へ]ボタンまたは[下へ]ボタンをクリックします。
5. すべての操作が完了したら、[設定]ボタンをクリックします。

   →CTリストの表示項目が変更されます。

表示される順序を一時的に変更する場合

管理コンソールのCTリスト上で、CTリストの項目をドラッグ＆ドロップで移動します。管理コンソールの次回起動時には、移動する前の表示順に戻ります。

スライドバー

ポリシー一覧の各タブの画面を切り替えます。
スライドバーをドラッグすると、各画面が次々と切り替わります。ドラッグを止めた付近のタブの画面が表示されます。
スライドバーをクリックすると、各画面が1つずつ切り替わります。

ポリシー一覧

設定されているポリシーが表示されます。
設定内容の詳細は、“2.4.1 端末初期設定をおこなう”を参照してください。

ステータスバー

管理コンソール起動時に指定した接続先サーバ名が表示されます。

タイトルバー

選択しているCTまたはCTグループの、グループ名と階層が表示されます。

メニューバー/ツールバー

[管理コンソール]画面のメニューバーおよびツールバーについて説明します。

メニューバー		ツールバー	機能概要
[ファイル]	[CT/CTグループ検索]	－	クライアント(CT)/CTグループ検索画面を表示します。
	[CTグループ作成]	－	CTグループ作成画面を表示します。
	[CTグループ削除]	－	CTグループ削除画面を表示します。 選択したCTグループ内にクライアント(CT)またはCTグループが存在している場合は、このメニューを選択できません。
	[CTグループ部門管理者設定]	－	部門管理者登録画面を表示します。なお、部門管理者がログオンしている場合は、このメニューを選択できません。
	[CT情報CSV出力]	－	[CT情報CSV出力ファイル指定]画面を表示します。
	[CTグループ情報CSV出力]	－	[CTグループ情報CSV出力ファイル指定]画面を表示します。
	[CTグループ部門管理者情報CSV取り込み]	－	[CTグループ部門管理者情報CSV取り込みファイル指定]画面を表示します。
	[CTグループ部門管理者情報CSV出力]	－	[CTグループ部門管理者情報CSV出力ファイル指定]画面を表示します。
	[リモート資料採取]	－	選択したクライアント(CT)の、障害調査用の資料を採取します。
	[CTデバッグトレース]	－	選択したクライアント(CT)のトレースログの採取条件を設定します。
	[配下CTのIPアドレス出力]	－	選択したCTグループ配下(サブグループ配下を含みます)のクライアント(CT)のIPアドレスが記載されたファイルを出力します。
	[パスワード変更]	－	管理コンソール起動時のパスワードを変更します。

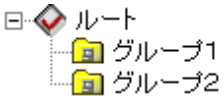
メニューバー			ツールバー	機能概要
	[終了]		－	管理コンソールを終了します。
[表示]	[端末情報参照/設定]			ポリシー参照/設定画面を表示します。
	[サービス一覧取得/制御]			サービス一覧取得/制御画面を表示します。
	[プロセス一覧取得/制御]			プロセス一覧取得/制御画面を表示します。
[ツリー設定]	[ツリー最新表示(全サーバ)]			統合管理サーバ配下の全サーバについて、CTグループツリーの階層状態の最新情報を表示します。
	[ツリー最新表示(選択中サーバ)]		－	統合管理サーバに接続している管理コンソールのCTグループツリーで、現在選択しているサーバについて、CTグループツリーの階層状態の最新情報を表示します。 選択できるサーバは、1台だけです。
	[ツリー全展開]		－	すべてのCTグループを表示します。
	[ツリー全縮小]		－	ルート直下（サーバ表示時はサーバ直下、ドメイン表示時はドメイン直下）のCTグループだけ表示します。
	[空のグループは表示しない]		－	配下にクライアント(CT)やCTグループが登録されていないCTグループを表示しません。
	[CTグループ構成反映]			CTグループツリーの階層状態を保存します。
	[サーバ表示]		－	接続している管理サーバをツリー上に表示します。 Active Directory連携時は常にサーバが表示されますので、[サーバ表示]のチェックをはずすことはできません。
	[「削除したCT」グループを表示]		－	構成情報ツリーに、「削除したCT」グループを表示します。 [サーバ表示]をチェックしている場合に、表示されます。 Active Directory連携時は、Localグループの直下に、最後のグループとして表示されます。 Active Directory連携していない場合は、サーバ直下に、最後のグループとして表示されます。
[リスト設定]	[CTリスト表示列設定]		－	CTリスト表示列設定画面を表示します。
[動作設定]	[端末初期設定]		－	端末初期設定画面を表示します。
	[端末動作設定]		－	端末における動作設定を表示します。
	[USBデバイス登録]		－	USBデバイス登録画面を表示します。 3階層のシステム構成で、統合管理サーバ以外の管理サーバに接続した管理コンソールでは、このメニューを選択できません。
	[起動時の最新情報取得]	[下位管理サーバから取得]	－	統合管理サーバに接続している管理コンソールの起動時に、下位管理サーバから最新の構成情報を取得して、画面に表示します。
		[統合管理サーバから取得]	－	統合管理サーバに接続している管理コンソールの起動時に、下位管理サーバへのデータ照会とデー

メニューバー			ツールバー	機能概要
				タの同期を行いません。現在の統合管理サーバに保存されている情報を、画面に表示します。
	[デバッグトレース]	[しない]	－	階層化サービス/サーバサービス/管理者メール通知機能のトレースを採取しません。
		[概要]	－	階層化サービス/サーバサービス/管理者メール通知機能のトレースを概要モードで採取します。
		[詳細]	－	階層化サービス/サーバサービス/管理者メール通知機能のトレースを詳細モードで採取します。
	[管理コンソールトレース]	[しない]	－	管理コンソールのトレースを採取しません。
		[概要]	－	管理コンソールのトレースを概要モードで採取します。
		[詳細]	－	管理コンソールのトレースを詳細モードで採取します。
[ユーザー設定]	[ユーザーポリシー設定]		－	ユーザーポリシー設定画面を表示します。
[他システム連携]	[Systemwalker Desktop Patrol 連携]	[構成反映取り込み]	－	構成情報取り込み画面を表示します。 部門管理者がログオンしている場合、または、Active Directory連携している場合は、選択できません。
		[構成反映出力]	－	構成情報出力画面を表示します。 部門管理者がログオンしている場合、または、Active Directory連携している場合は、選択できません。
[ヘルプ]	[オンラインヘルプ]			オンラインマニュアルを表示します。
	[バージョン情報]		－	著作権情報およびバージョン情報を表示します。

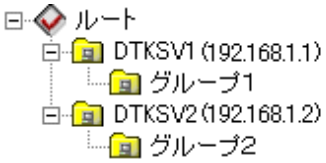
サーバ表示

統合管理サーバに接続している管理コンソールにおいて[ツリー設定]の[サーバ表示]にチェックすると接続している統合管理サーバ、および管理サーバのコンピュータ名、IPアドレスが表示され、CTグループはサーバごとに表示されます。
Active Directory連携時は常にサーバが表示されますので、[サーバ表示]のチェックをはずすことはできません。

【[サーバ表示]チェックなし(Active Directory連携なしの場合)】



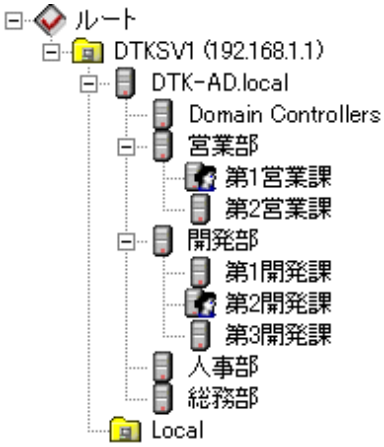
【[サーバ表示]チェックあり(Active Directory連携なしの場合)】



ドメイン表示

Active Directory連携時には、サーバ表示と合わせてドメイン名も常に表示されます。非表示には変更できません。

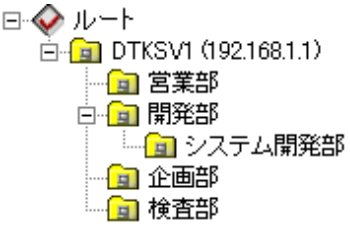
【Active Directory連携時のドメイン表示例】



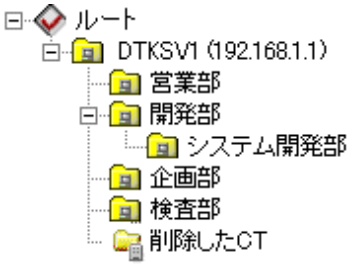
「削除したCT」グループを表示

管理コンソールの[ツリー設定]の[サーバ表示]にチェックをつけた後、[ツリー設定]の[「削除したCT」グループを表示]にチェックすると、「削除したCT」グループが表示されます([サーバ表示]にチェックがついていないときは、[「削除したCT」グループを表示]をチェックできません)。
以下は、Active Directory連携していないときの例です。
Active Directory連携時は、Localグループの直下に表示されます。

【[「削除したCT」グループを表示]チェックなし】



【[「削除したCT」グループを表示]チェックあり】

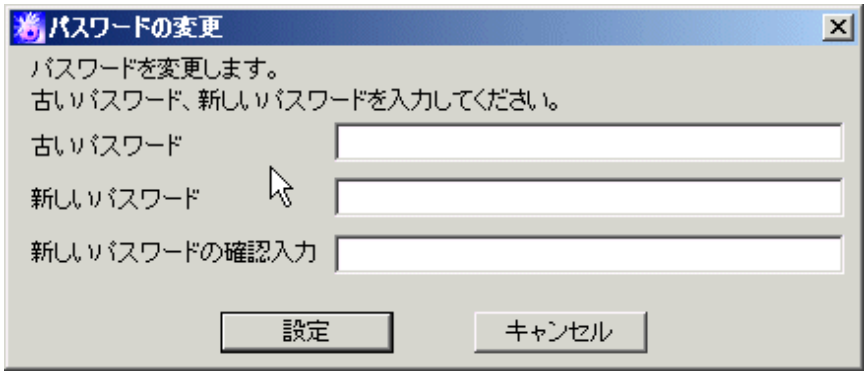


管理コンソール起動時のパスワードを変更する

1. 管理コンソールを起動します。

2. [ファイル]メニューから[パスワード変更]を選択します。

   →[パスワードの変更]画面が表示されます。



3. 以下の情報を入力し、[設定]ボタンをクリックします。

   - **[古いパスワード]**:これまで使用していたパスワードを入力します。
   - **[新しいパスワード]**:新しいパスワードを、1～32文字の半角英数字または半角の記号で入力します。
     ただし、「&」、「¥」、「:」、「?」、「”」、「~」、「^」、「’」、「<」、「>」、「|」、および空白は使用できません。また、大文字、小文字は区別されます。
   - **[新しいパスワードの確認入力]**:新しいパスワードを再入力します。

4. 確認画面が表示されますので、[OK]ボタンをクリックします。

   →パスワードが変更されます。

2.4 ポリシーの初期値を設定する

システムの運用方針に沿った、管理対象全体の標準的なポリシーを、初期値として設定します。

2.4.1 端末初期設定をおこなう

端末初期設定では、クライアント(CT)での操作を禁止する条件、および採取するログを設定します。

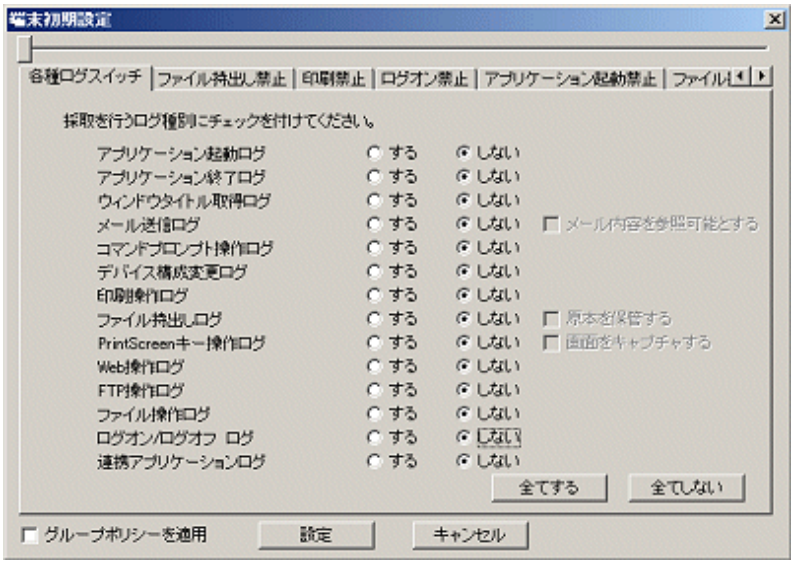
3階層のシステム構成の場合は、各管理サーバで端末初期設定を行ってください(統合管理サーバで端末初期設定を行っても、管理サーバには反映されません)。

以下に手順を示します。

1. [管理コンソール]を起動します。

2. [動作設定]メニューから[端末初期設定]を選択します。

   →[端末初期設定]画面が表示されます。



項目名	説明
[グループポリシーを適用]	CTの新規登録時またはユーザーの新規作成時に、CTポリシーまたはユーザーポリシーとして、所属するグループのグループポリシーを適用するかどうかを設定します。 チェックする場合: 所属するグループのグループポリシーが適用されます。 チェックしない場合**(初期値)**: 所属するグループのグループポリシーは適用されません。 CTまたはユーザーが、ルート直下に存在する場合は、この設定は無効です。

3. 各タブでポリシーを設定し、[設定]ボタンをクリックします。

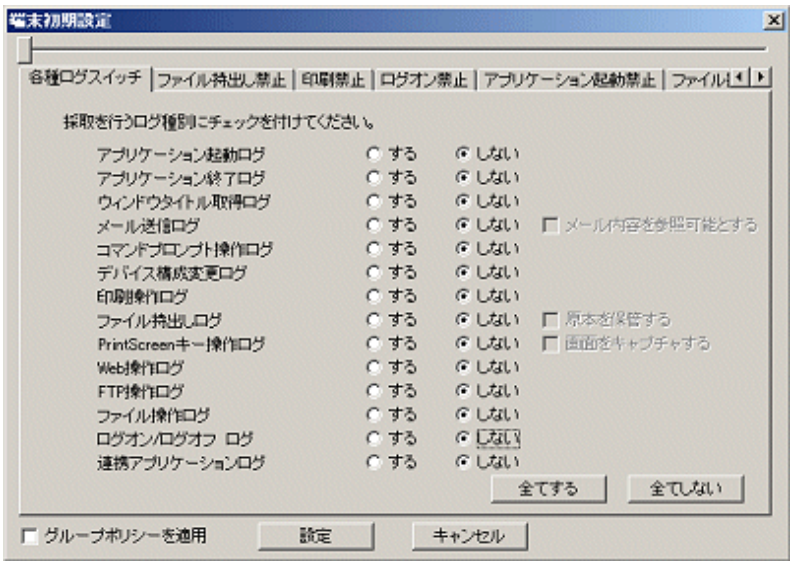
すでに設定されている端末初期設定値を変更した場合(バージョンアップ/エディションアップによって追加されたポリシー項目を設定したとき、または、運用中に端末初期設定値を変更したとき)は、[設定]ボタンをクリックしたあとで、CTへのポリシーの反映操作が必要です。
ポリシーの反映操作については、“CTポリシーを変更する”または“3.4.2 ユーザーポリシーを変更する”を参照してください。

以下に、各タブでの設定内容を説明します。

2.4.1.1 [各種ログスイッチ]タブの設定

[各種ログスイッチ]タブでは、各種ログを採取するかしないかを設定します。[する]を設定すると、クライアント(CT)での操作ログが採取されます。

[各種ログスイッチ]タブでの設定内容を説明します。



項目名	説明
[アプリケーション起動ログ]	アプリケーション起動ログが採取されます。 **初期値:**[しない]が選択されています。
[アプリケーション終了ログ]	アプリケーション終了ログが採取されます。 **初期値:**[しない]が選択されています。
[ウィンドウタイトル取得ログ]	ウィンドウを持つアプリケーション起動時のウィンドウタイトルのログが採取されます。 **初期値:**[しない]が選択されています。
[メール送信ログ]	メール送信ログが採取されます。 **初期値:**[しない]が選択されています。
[メール内容を参照可能とする]	[メール送信ログ]が[する]の場合に設定できます。 チェックする場合: メール送信ログまたはメール送信中止ログが採取された場合に、送信したメールの内容や添付ファイルが保存されます。 権限を与えられた管理者は、送信したメールの内容と添付ファイルの内容を参照できます。 チェックしない場合**(初期値)**: 送信したメールの内容や添付ファイルは保存されません。したがって、送信したメールの内容と添付ファイルの内容を参照できません。
[コマンドプロンプト操作ログ]	コマンドプロンプトで入力されたコマンドおよびコマンド結果のログが採取されます。 **初期値:**[しない]が選択されています。
[デバイス構成変更ログ]	デバイス構成の変更ログが採取されます。 **初期値:**[しない]が選択されています。
[印刷操作ログ]	印刷の操作ログが採取されます。 **初期値:**[しない]が選択されています。 [する]を選択した場合は、以下のタブの項目が入力できるようになります。 ・ [エコ監視設定]タブ
[ファイル持出しログ]	持出しユーティリティを使用してファイルの持ち出しを行ったときのログが採取されます。 **初期値:**[しない]が選択されています。
[原本を保管する]	[ファイル持出しログ]が[する]の場合に設定できます。

項目名	説明
	チェックする場合: 持出しユーティリティを使用してファイルの持ち出しを行ったファイルを原本として保管します。 チェックしない場合**(初期値)**: 持出しユーティリティを使用してファイルの持ち出しを行ったファイルを原本として保管しません。
[PrintScreenキー操作ログ]	PrintScreenキーの操作ログが採取されます。 [印刷禁止]タブの[PrintScreenキー無効化]が[しない]と設定されている場合に設定できます。 **初期値:**[しない]が選択されています。
[画面をキャプチャする]	[PrintScreenキー操作ログ]が[する] の場合に設定できます。 チェックする場合: PrintScreenキーの操作ログが記録された時点の画面キャプチャを記録します。 チェックしない場合**(初期値)**: PrintScreenキーの操作ログが記録された時点の画面キャプチャを記録しません。
[Web操作ログ]	以下のログが採取されます。 ・ Webダウンロードログ **初期値:**[しない]が選択されています。
[FTP操作ログ]	以下のログが採取されます。 ・ FTPアップロードログ ・ FTPダウンロードログ **初期値:**[しない]が選択されています。
[ファイル操作ログ]	ファイル操作ログが採取されます。 **初期値:**[しない]が選択されています。 [する]を選択した場合は、以下のタブの項目が入力できるようになります。 ・ [ファイル操作プロセス]タブ ・ [ファイル操作拡張子]タブ
[ログオン/ログオフ ログ]	以下のログが採取されます。 ・ ログオンログ ・ ログオフログ ・ PC起動ログ ・ PC終了ログ ・ PC休止ログ ・ PC復帰ログ **初期値:**[しない]が選択されています。
[連携アプリケーションログ]	連携するアプリケーションのログが採取されます。 **初期値:**[しない]が選択されています。
[全てする]	すべてのログについて、採取[する]が選択されます。
[全てしない]	すべてのログについて、採取[しない]が選択されます。

注意

[印刷操作ログ]の設定について

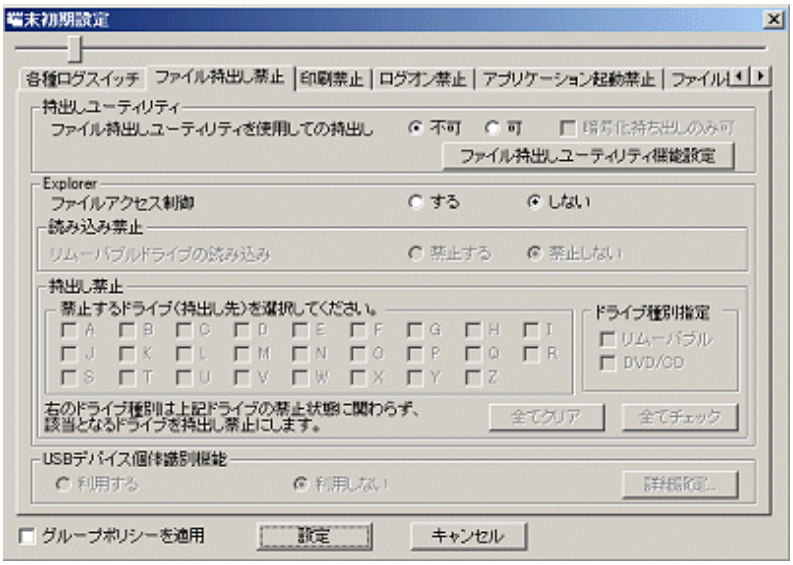
クライアント(CT)インストール時に[ローカルプリンタでの印刷のみを監視する]を選択している場合、プリンタサーバと同じ統合管理サーバまたは管理サーバ配下にあるクライアント(CT)での印刷操作が、プリンタサーバをとおして行われることを想定しています。(プリンタサーバにもクライアント(CT)がインストールされている必要があります)
この場合、印刷操作ログはプリンタサーバから採取されるので、プリンタサーバではないクライアント(CT)では、[印刷操作ログ]を[する]にしても印刷操作ログは採取されません。プリンタサーバでの[印刷操作ログ]を[する]にすると印刷操作ログが採取されます。

2.4.1.2 [ファイル持出し禁止]タブの設定

[ファイル持出し禁止]タブでは、クライアント(CT)がインストールされているPCのドライブ、リムーバブルディスク、またはDVD/CDへのファイルやフォルダの持ち出しを禁止する条件や、読み込み禁止を設定します。
読み込み禁止は、Explorer利用時には有効ですが、持出しユーティリティ利用時には有効になりません。

また、管理者によって使用を許可されたUSBデバイスに限定した持出しのための条件を設定します。

[ファイル持出し禁止]タブでの設定内容を説明します。



[持出しユーティリティ]

項目名		説明
[ファイル持出しユーティリティを使用しての持出し]	[不可] **(初期値)**	ファイル持出しユーティリティは使用できません。
	[可]	ファイル持出しユーティリティを使用できます。 持出し禁止ドライブに対しても、ファイル持出しユーティリティを使用すれば、持出しできます。
	[暗号化持ち出しのみ可]	チェックする場合: ファイル持出しユーティリティで暗号化した場合だけ、持ち出すことができます。 チェックしない場合: ファイル持出しユーティリティを使用すれば、暗号化の有無に関係なく持ち出すことができます。
[ファイル持出しユーティリティ機能設定]		[ファイル持出しユーティリティ機能設定]画面が表示されます。 (ファイル持出しユーティリティ使用時の条件を設定します。)

[Explorer]

エクスプローラなどから操作する場合の制御を設定します。

項目名			説明
[ファイルアクセス制御]		[する]	[読み込み禁止]と[持出し禁止]が設定できるようになります。
		[しない] **(初期値)**	リムーバブルドライブの読み込みや、ファイルの持ち出しを自由に行えます(Systemwalker Desktop Keeperを導入していない場合と同じように、ファイルにアクセスできます)。 本項目を選択した場合、[読み込み禁止]、[持出し禁止]は設定できません。
[読み込み禁止]			リムーバブルドライブの読み込み禁止を設定します。
	[リムーバブルドライブの読み込み]	[禁止する]	リムーバブルドライブの読み込みを禁止します。 [ドライブ種別指定]の[リムーバブル]は、自動的にチェックされます。 リムーバブルドライブの読み込み禁止については、“8.1.2 ファイル読み込み禁止”を参照してください。
		[禁止しない] **(初期値)**	リムーバブルドライブの読み込みを禁止しません。
[持出し禁止]			持出し禁止対象を設定します。
	禁止を行うドライブ(持出し先)の選択		持出し禁止の対象とするドライブをチェックします。 **初期値:**すべてチェックされていません。 禁止対象となるのは、以下の条件をすべてみたすドライブです。 以下の条件以外のもの(赤外線通信など)またはCドライブは、禁止の対象ではありません。 ・ PCにドライブレターとして認識されたドライブ ・ ネットワークドライブではないドライブ Fドライブにリムーバブルディスクが設定されている場合、[リムーバブル]をチェックしていない(禁止対象としない)ときでも、[F]がチェックされている(禁止対象とする)ときには、Fドライブは禁止対象として設定されます。
	[ドライブ種別指定]	[リムーバブル]	ドライブレターとして認識される以下への持ち出しを禁止します。 **初期値:**チェックされていません。 ・ フロッピーディスク ・ 外付けハードディスク(USB、IEEE1394、PCMCIA接続など取り外し可能なハードディスクの場合) ・ MO ・ USBメモリ ・ コンパクトフラッシュメモリ
		[DVD/CD]	DVD/CDへの持ち出しを禁止します。 **初期値:**チェックされていません。
	[全てクリア]		禁止を行うドライブ(持出し先)の設定と[ドライブ種別指定]の設定に対して、チェックをすべてはずします。
	[全てチェック]		禁止を行うドライブ(持出し先)の設定と[ドライブ種別指定]の設定に対して、すべてにチェックします。

注意

ログファイルの格納先のドライブは、設定しないでください

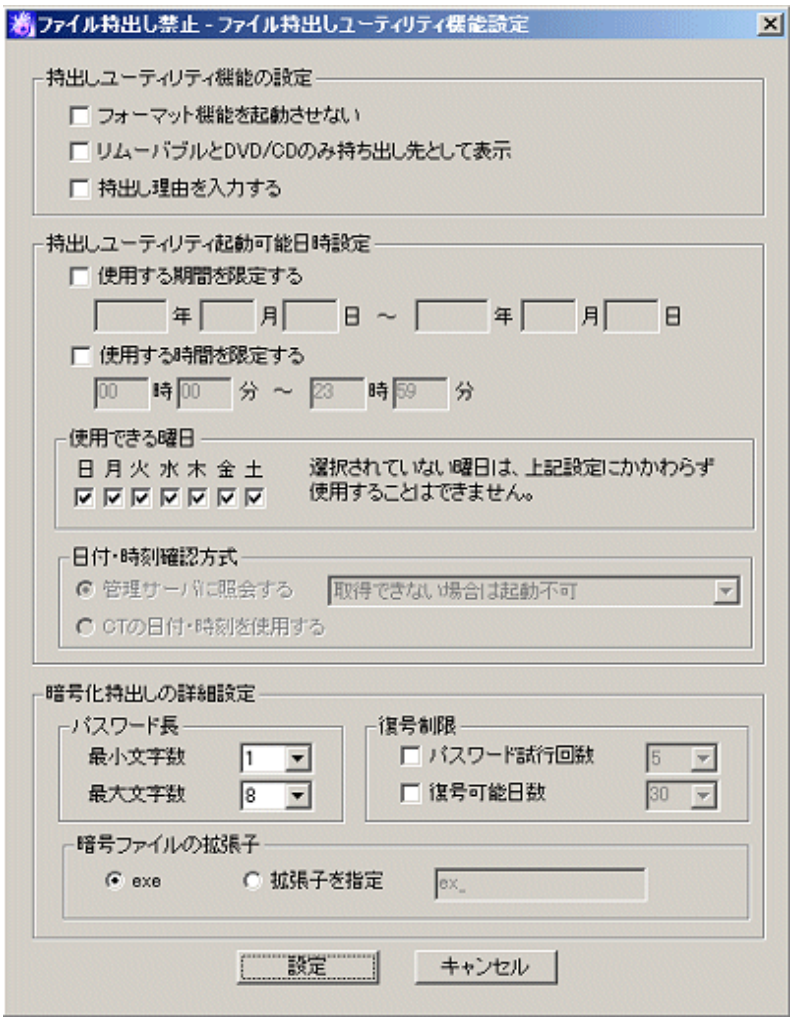
クライアント(CT)インストール時に設定したログファイルの格納先のドライブを禁止対象とすると、クライアント(CT)からログが採取できなくなります。

[USBデバイス個体識別機能]

項目名	説明
[利用する]	持出しユーティリティを使用してファイルやフォルダを持出す場合、管理コンソールの[USBデバイス登録]画面で登録したUSBデバイスのうち、管理者が指定したUSBデバイスへだけ、持ち出すことができます。 また、Explorerなど(持出しユーティリティ以外)を使用しての書き込みや読み込みが禁止されている場合でも、管理コンソールの[USBデバイス登録]画面で登録したUSBデバイスのうち、管理者が指定したUSBデバイスへだけ、持ち出すことができます。
[利用しない] **(初期値)**	持出しユーティリティを使用してファイルやフォルダを持出す場合、[持出しユーティリティ]で設定したポリシーに従います。 また、Explorerなど(持出しユーティリティ以外)を使用しての書き込みや読み込みは、[Explorer]で設定したポリシーに従います。
[詳細設定]	[ファイル持出し禁止 - USBデバイス個体識別機能 - 詳細設定]画面が表示されます。 (管理者が使用を許可したUSBデバイスのアクセス条件や、使用を許可するUSBデバイスの追加・削除を設定します。)

[ファイル持出しユーティリティ機能設定]画面

ファイル持出しユーティリティ使用時の条件を設定します。



[持出しユーティリティ機能の設定]

項目名	説明
[フォーマット機能を起動させない]	チェックする場合: [ファイル]メニューを選択したとき、以下は表示されません。ドライブや、CD-RW/DVD-RW内のデータを削除できません。 ・ [ドライブのフォーマット] ・ [CD-RW/DVD-RW消去] チェックしない場合**(初期値)**: ドライブや、CD-RW/DVD-RW内のデータを削除できます。
[リムーバブルとDVD/CDのみ持ち出し先として表示]	チェックする場合: ファイルを持ち出すとき、持ち出し先としてリムーバブルとCD/DVDドライブだけ表示されます。 チェックしない場合**(初期値)**: ファイルを持ち出すとき、すべての持ち出し先が表示されます。
[持出し理由を入力する]	チェックする場合: [ファイル持出しユーティリティ]画面に、持出し理由入力欄が表示されます。ファイルを持ち出すときは、必ず持出し理由を入力しなければなりません。 持出し理由はCT/ユーザーごとに最大10件保存されます。次回の持出し時に、プルダウンメニューから過去の入力情報を選択できます。 チェックしない場合**(初期値)**: [ファイル持出しユーティリティ]画面に、持出し理由入力欄は表示されません。

[持出しユーティリティ起動可能日時設定]

項目名		説明
[使用する期間を限定する]		チェックする場合: 起動可能な期間を設定します。設定した期間だけ、持出しユーティリティを使用できます。 入力値の範囲は以下のとおりです。 ・ 2000年1月1日～2037年12月31日 チェックしない場合**(初期値)**: 持出しユーティリティを常に使用できます。
[使用する時間を限定する]		チェックする場合: 起動可能な時間を設定します。設定した時間帯だけ、持出しユーティリティを使用できます。 チェックしない場合**(初期値)**: 24時間使用できます。
[使用できる曜日]		起動可能な曜日を設定します。 **初期値:**すべてにチェックがついています。
[日付・時刻確認方式]	[管理サーバに照会する] **(初期値)**	持出しユーティリティの起動可能な日付・時刻は、管理サーバの日付・時刻を基準にします。 また、オフライン時または管理サーバからの応答がない場合の動作を設定します。 ・ [取得できない場合はCTの日付・時刻を使用する]: 持出しユーティリティの起動可能な日付・時刻は、CTの日付・時刻を使用します。

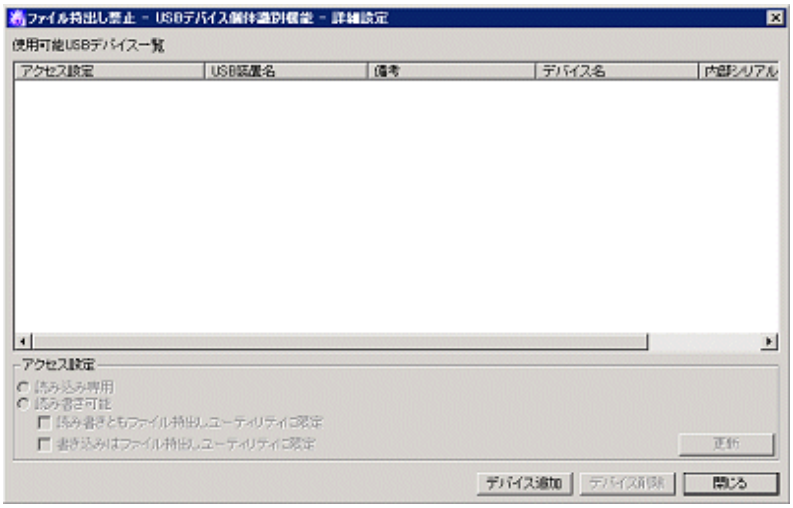
項目名		説明
		・ [取得できない場合は起動不可] **(初期値)**: 持出しユーティリティを起動できません。
	[CTの日付・時刻を使用する]	持出しユーティリティの起動可能な日付・時刻は、CTの日付・時刻を基準にします。

[暗号化持出しの詳細設定]

項目名		説明
[パスワード長]	[最小文字数]	暗号化してファイルを持ち出す場合、パスワードの最小文字数を設定します。 1～128まで設定できます。**初期値:**1です。
	[最大文字数]	暗号化してファイルを持ち出す場合、パスワードの最大文字数を設定します。 1～128まで設定できます。**初期値:**8です。
[復号制限]	[パスワード試行回数]	チェックする場合: パスワードの試行回数を設定します。 1～5の範囲で設定できます(初期表示は、5です)。 復号時のパスワード入力を、設定された回数失敗した場合は、暗号化ファイルが削除されます。 ただし、暗号化ファイルを以下の媒体に持ち出している場合は、暗号化ファイルは削除されません。 ・ CD/DVD ・ ライトプロテクトされたフロッピーディスクやUSBメモリ チェックしない場合**(初期値)**: パスワードの試行回数は無制限で、暗号化ファイルは削除されません。
	[復号可能日数]	チェックする場合: 暗号化ファイルを復号できる期間(日数)を設定します。日数は、暗号化した日を含みます。 1～999の範囲で設定できます(初期表示は、30です)。 設定された日数を超えているにもかかわらず復号操作を実施した場合は、暗号化ファイルが削除されます。 ただし、暗号化ファイルを以下の媒体に持ち出している場合は、暗号化ファイルは削除されません。 ・ CD/DVD ・ ライトプロテクトされたフロッピーディスクやUSBメモリ チェックしない場合**(初期値)**: 復号可能期間は無期限で、暗号化ファイルは削除されません。
[暗号ファイルの拡張子]	[exe] **(初期値)**	暗号ファイルの拡張子として自動的に“exe”が付与されます。 [暗号ファイル設定]画面の[暗号ファイル名]と、暗号化後のファイル名の関係を以下に示します。 ・ 暗号ファイル名に「暗号」を指定→作成されるファイル名「暗号.exe」 ・ 暗号ファイル名に「暗号.txt」を指定→作成されるファイル名「暗号.txt.exe」 ・ 暗号ファイル名に「暗号.exe」を指定→作成されるファイル名「暗号.exe」 ・ 暗号ファイル名に「暗号.ex_」を指定→作成されるファイル名「暗号.ex_.exe」 暗号ファイルは、ファイル持出しユーティリティの暗号ファイル専用アイコンで表示されます。
	[拡張子を指定]	暗号ファイルの拡張子を設定します。 16バイト(. は除きます)以内の半角英数字と記号を使用できます。ただし、以下の

項目名		説明
		記号は使用できません。 「.」、「¥」、「/」、「:」、「*」、「?」、「“」、「<」、「>」、「|」 “zip”、“lzh”など、圧縮ファイルの拡張子を設定しても、圧縮はされません。 **初期値:**“ex_”です。 [暗号ファイル設定]画面の[暗号ファイル名]と、暗号化後のファイル名の関係を以下に示します。 指定された拡張子は、“ex_”であるとします。 ・ 暗号ファイル名に「暗号」を指定→作成されるファイル名「暗号.ex_」 ・ 暗号ファイル名に「暗号.txt」を指定→作成されるファイル名「暗号.txt.ex_」 ・ 暗号ファイル名に「暗号.exe」を指定→作成されるファイル名「暗号.exe.ex_」 ・ 暗号ファイル名に「暗号.ex_」を指定→作成されるファイル名「暗号.ex_」 暗号ファイルは、ファイルとの関連付けがされている拡張子を指定した場合は、関連付けられているファイルのアイコンで表示されます。
[設定]		設定内容が一時保存されます(データベースには、まだ反映されません)。
[キャンセル]		設定内容は保存されずに、画面が閉じます。

[ファイル持出し禁止 - USBデバイス個体識別機能 - 詳細設定]画面



項目名		説明
[使用可能USBデバイス一覧]		管理者が使用を許可したUSBデバイスが表示されます。 アクセス条件を設定・変更する場合や、使用許可を取りやめる場合は、該当するUSBデバイスの行を選択します。
[アクセス設定]		使用を許可されたUSBデバイスにアクセス条件を設定します。
	[読み込み専用] **(初期値)**	[使用可能USBデバイス一覧]で選択したUSBデバイスは、読み込みだけできます。
	[読み書き可能]	[使用可能USBデバイス一覧]で選択したUSBデバイスは、読み込みと書き込みができます。 [読み書きともファイル持出しユーティリティに限定]と[書き込みはファイル持出しユーティリティに限定]のチェックボックスは、どちらか一方のみ選択できます。 どちらのチェックボックスも選択しなかった場合、登録したUSBは、持出し

項目名	説明
	ユーティリティやExplorerなど(持出しユーティリティ以外)から使用(読み書き)できます。
[読み書きともファイル持出しユーティリティに限定]	チェックする場合: 読み書き(ファイルの持出し)は、持出しユーティリティを使用した場合だけ可能です。 Explorerなど(持出しユーティリティ以外)を使用しての読み込みや書き込みは行えません。
[書き込みはファイル持出しユーティリティに限定]	チェックする場合: 書き込み(ファイルの持出し)は、持出しユーティリティを使用した場合だけ可能です。 読み込みは、どのようなツールを使用しても可能です。
[更新]	設定した内容を[使用可能USBデバイス一覧]に表示します。
[デバイス追加]	[ファイル持出し禁止 - USBデバイス個体識別機能の詳細設定 - USBデバイス選択]画面が表示され、使用を許可するUSBデバイスを追加できます。 30件まで追加できます。
[デバイス削除]	[使用可能USBデバイス一覧]で選択したUSBデバイスの使用許可を取りやめます。[使用可能USBデバイス一覧]から削除されます。
[閉じる]	画面を閉じます。

使用を許可したUSBデバイスにアクセス条件を設定(変更)する場合

1. [使用可能USBデバイス一覧]で、該当するUSBデバイスの行を選択します。
2. [アクセス設定]で条件を設定します。
3. [更新]ボタンをクリックします。

USBデバイスの使用許可を取りやめる場合

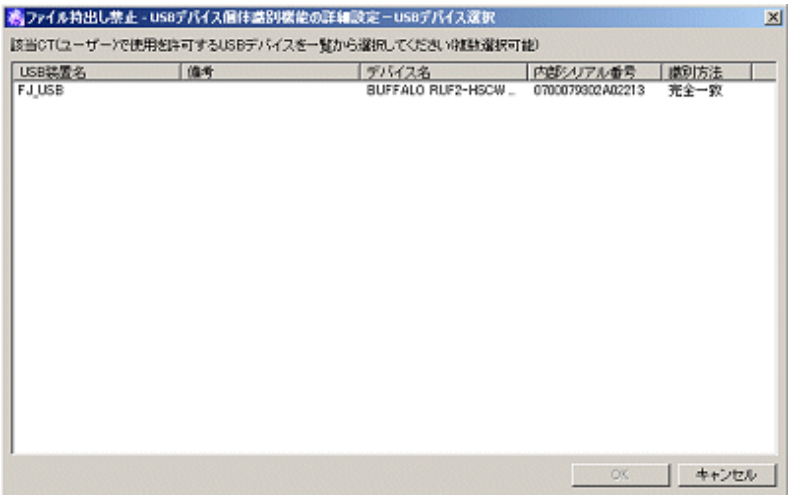
1. [使用可能USBデバイス一覧]で、該当するUSBデバイスの行を選択します。
2. [デバイス削除]ボタンをクリックします。

使用を許可するUSBデバイスを追加する場合

[デバイス追加]ボタンをクリックします。

[ファイル持出し禁止 - USBデバイス個体識別機能の詳細設定 - USBデバイス選択]画面

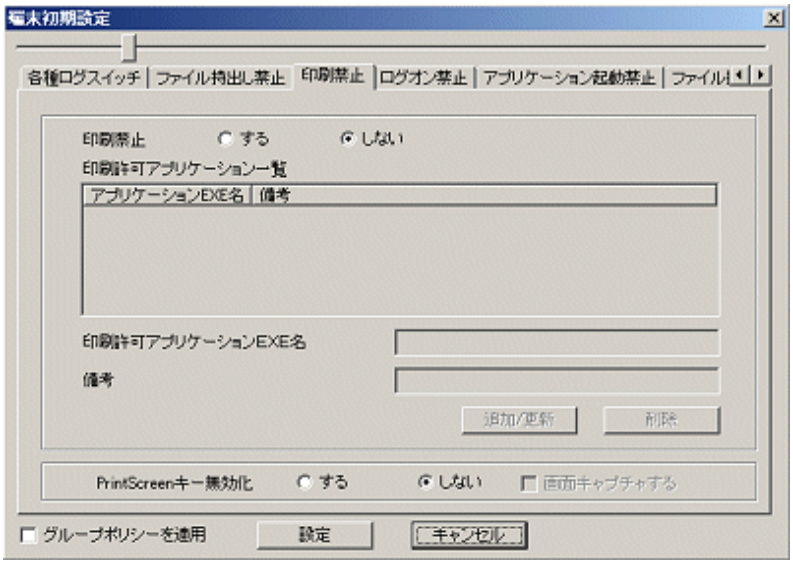
管理コンソールの[USBデバイス登録]画面で登録した内容が表示されています。
使用を許可するUSBデバイスの行を選択し、[OK]ボタンをクリックすると、[ファイル持出し禁止 - USBデバイス個体識別機能 - 詳細設定]画面の[使用可能USBデバイス一覧]に、該当USBデバイスが追加されます。



2.4.1.3　[印刷禁止]タブの設定

[印刷禁止]タブでは、クライアント(CT)がインストールされているPCでの印刷を禁止する条件(印刷を許可するアプリケーションの指定)、およびPrintScreenキーによる画面のハードコピー採取の禁止を設定します。

[印刷禁止]タブでの設定内容を説明します。



[印刷禁止]

項目名		説明
[印刷禁止]	[する]	[印刷許可アプリケーション一覧]に表示された[アプリケーションEXE名]以外のアプリケーションによる印刷が禁止されます。
	[しない] **(初期値)**	印刷は禁止されません。
[印刷許可アプリケーション一覧]		設定した[印刷許可アプリケーションEXE名]が表示されます。 **初期値:**何も指定されていません。
[印刷許可アプリケーションEXE名]		印刷を許可するアプリケーションのEXE名を拡張子も含めて入力します。 (指定例:Microsoft® Excelの場合はEXCEL.EXE) 半角で254文字(全角で127文字)まで入力できます。(英文字は大文字、小文字の区別をしません)

項目名	説明
	ただし、以下の記号を使用するとエラーとなります。 「¥」「/」「:」「*」「?」「"」「<」「>」「|」 **初期値:**何も指定されていません。
[備考]	アプリケーションの名前やメモ情報などを入力します。 半角で128文字(全角で64文字)まで入力できます。 **初期値:**何も指定されていません。
[追加/更新]	印刷を許可するアプリケーションEXE名が追加されます。 追加できる件数は100件までです。 [印刷許可アプリケーション一覧]で選択した行の[備考]を変更した場合、情報が更新されます([印刷許可アプリケーションEXE名]は更新できません)。
[削除]	[印刷許可アプリケーション一覧]で選択した行が削除されます。

[PrintScreenキー禁止]

項目名		説明
[PrintScreenキー無効化]		[各種ログスイッチ]タブの[PrintScreenキー操作ログ]が[しない]と設定されている場合に設定できます。
	[する]	PrintScreenキーの使用が禁止されます。 PrintScreenキーを押しても、画面のハードコピーは採取されません。
	[しない] **(初期値)**	PrintScreenキーの使用は禁止されません。
[画面キャプチャする]		[PrintScreenキー無効化]が[する]の場合に設定できます。 チェックする場合: PrintScreenキーの使用を禁止しているときに、PrintScreenキーが押された時点の画面キャプチャを記録します。 [PrintScreenキー無効化]を[しない]と設定した場合には、自動的に、チェックなしに変更されます。 チェックしない場合**(初期値)**: PrintScreenキーの使用を禁止しているときに、PrintScreenキーが押されても、画面キャプチャを記録しません。

【印刷許可アプリケーションEXE名を追加する場合】
上記の設定項目を入力し、[追加/更新]ボタンをクリックします。
追加できる件数は100件までです。

【既存情報を更新する場合】
[印刷許可アプリケーション一覧]から更新する行を選択し、[備考]の情報を修正して、[追加/更新]ボタンをクリックします。
[印刷許可アプリケーションEXE名]は更新できません。

【情報を削除する場合】
[印刷許可アプリケーション一覧]から削除する行を選択し、[削除]ボタンをクリックします。

2.4.1.4 [ログオン禁止]タブの設定

[ログオン禁止]タブでは、ログオンを禁止するグループを設定します。[ログオン禁止]を設定すると、クライアント(CT)がインストールされているPCからログオンするとき、設定したグループに所属しているユーザー名でのログオンを禁止できます。

ログオン禁止設定が可能なグループは以下のとおりです。

- Administrators
- Backup Operators
- Debugger Users

- Power Users
- Guests
- Replicator
- Users
- Domain Admins
- Domain Guests
- Domain Users
- Enterprise Admins
- Group Policy Creator Owners

また、1つのユーザー名が複数のグループに所属している場合、以下の条件をすべて満たすときは、ログオン禁止の対象となります。

- WindowsのPCにログオンするときに入力するユーザー名が複数のグループに属している
- 属している複数のグループの内、どれか1つのグループに対してログオン禁止が設定されている

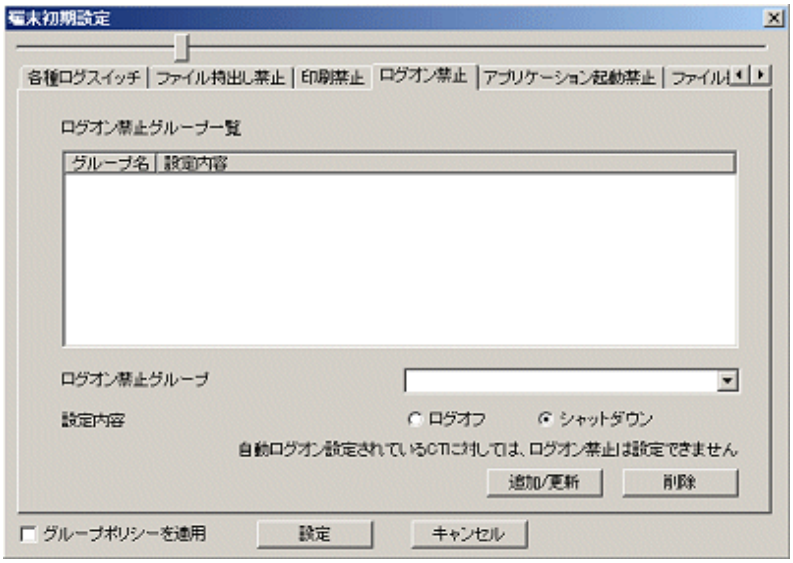
注意

Windows® XPでのシステム管理者ユーザーの作成について

Microsoft® Windows® XP Home Editionの場合、システム管理者ユーザーの作成時に自動的にAdministratorsグループとUsersグループに属したユーザー名が作成されます。Systemwalker Desktop Keeperで設定されているポリシーが、AdministratorsグループとUsersグループのどちらか一方でも禁止設定されている場合は、ログオンを禁止します。

設定内容は、CTポリシーとして動作します。
PCにログオンしているユーザーが1人の場合は、[ログオン禁止]タブで設定した内容で禁止されます。
同一PCにログオンしているユーザーが2人以上の場合は、[ログオン禁止]タブでの設定に関係なく、ログオフされます。

[ログオン禁止]タブでの設定内容を説明します。



項目名	説明
[ログオン禁止グループ一覧]	設定したログオン禁止グループが表示されます。 **初期値:**何も指定されていません。

項目名	説明
[ログオン禁止グループ]	ログオンを禁止するグループをプルダウンメニューから選択します。 各グループの詳細は、Windowsのマニュアルを参照してください。 **初期値:**何も指定されていません。
[設定内容]	禁止の対象となるグループでログオンした場合の、クライアント(CT)での対処を指定します。 ・ [ログオフ] 強制的にログオフします。 Windows Server® 2008、Windows Server® 2003、またはWindows® 2000 Serverの場合、User権限のユーザーに使用させたくない場合は、[ログオフ]を設定してください。 ・ [シャットダウン]**(初期値)** 強制的にシャットダウンします。 ただし、Windows Server® 2008、Windows Server® 2003、またはWindows® 2000 Serverでは、User権限でシャットダウンできません。 クライアント(CT)でログオン禁止が検出されてからログオフまたはシャットダウンされるまでの時間は“端末動作設定”で設定できます。“端末動作設定”については、“2.4.2 端末動作設定をおこなう”を参照してください。
[追加/更新]	ログオンを禁止するグループ名と、ログオンしたときの対処が追加されます。 [ログオン禁止グループ一覧]で選択した行の[設定内容]を変更した場合、情報が更新されます([ログオン禁止グループ]は更新できません)。
[削除]	[ログオン禁止グループ一覧]で選択した行が削除されます。

【ログオン禁止グループを追加する場合】
上記の設定項目を入力し、[追加/更新]ボタンをクリックします。

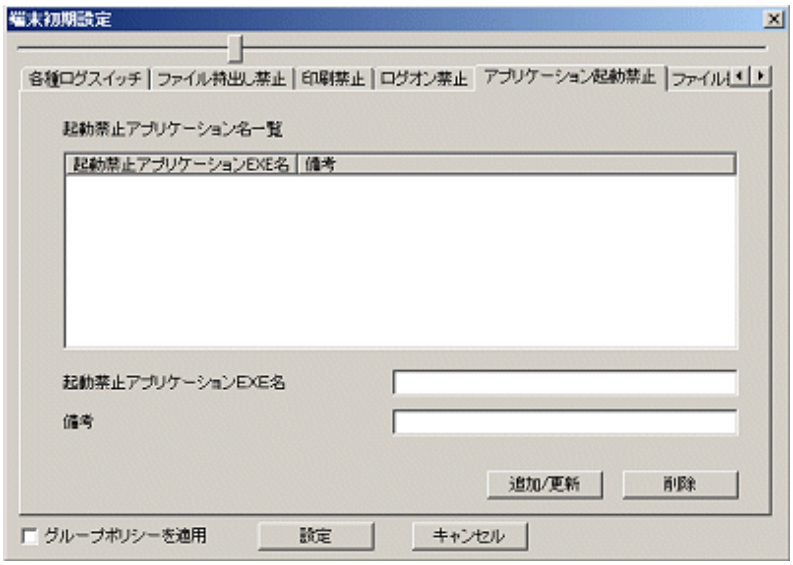
【既存情報を更新する場合】
[ログオン禁止グループ一覧]から更新する行を選択し、[設定内容]の情報を修正して、[追加/更新]ボタンをクリックします。
[グループ名]は更新できません。

【情報を削除する場合】
[ログオン禁止グループ一覧]から削除する行を選択し、[削除]ボタンをクリックします。

2.4.1.5 [アプリケーション起動禁止]タブの設定

[アプリケーション起動禁止]タブでは、クライアント(CT)がインストールされているPCで起動を禁止するアプリケーション名を設定します。

[アプリケーション起動禁止]タブでの設定内容を説明します。



項目名	説明
[起動禁止アプリケーション名一覧]	設定した起動禁止アプリケーションEXE名が表示されます。 **初期値:**何も指定されていません。
[起動禁止アプリケーションEXE名]	起動禁止するアプリケーションのEXE名を拡張子も含めて入力します。 (指定例:Microsoft® Excelの場合はEXCEL.EXE) 半角で254文字(全角で127文字)まで入力できます。 (英文字は大文字、小文字の区別をしません) ただし、以下の記号を使用するとエラーとなります。 「¥」「/」「:」「*」「?」「"」「<」「>」「|」 **初期値:**何も指定されていません。
[備考]	アプリケーションの名前やメモ情報などを入力します。 半角で128文字(全角で64文字)まで入力できます。 **初期値:**何も指定されていません。
[追加/更新]	起動を禁止するアプリケーションEXE名が追加されます。 追加できる件数は100件までです。 [起動禁止アプリケーション名一覧]で選択した行の[備考]を変更した場合、情報が更新されます([起動禁止アプリケーションEXE名]は更新できません)。
[削除]	[起動禁止アプリケーション名一覧]で選択した行が削除されます。

【起動禁止アプリケーションEXE名を追加する場合】
上記の設定項目を入力し、[追加/更新]ボタンをクリックします。
追加できる件数は100件までです。

【既存情報を更新する場合】
[起動禁止アプリケーション名一覧]から更新する行を選択し、[備考]の情報を修正して、[追加/更新]ボタンをクリックします。
[起動禁止アプリケーションEXE名]は更新できません。

【情報を削除する場合】
[起動禁止アプリケーション名一覧]から削除する行を選択し、[削除]ボタンをクリックします。

2.4.1.6　[ファイル操作プロセス]タブの設定

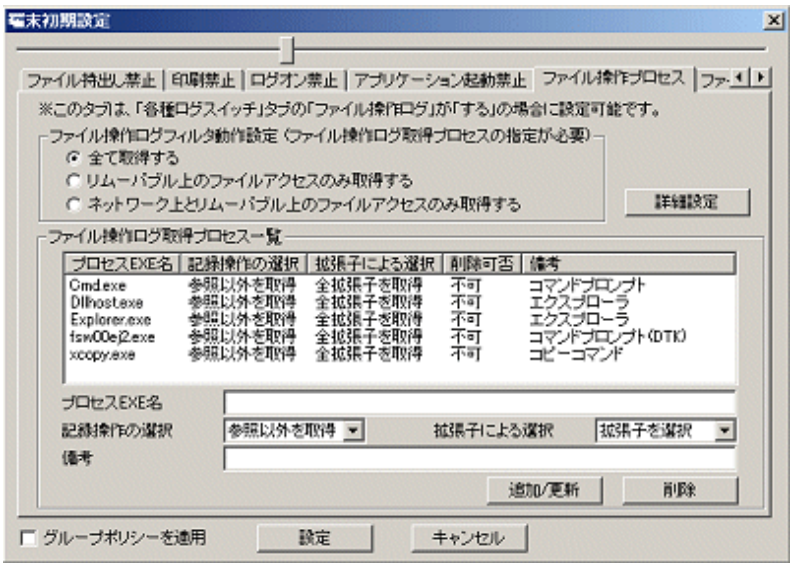
[ファイル操作プロセス]タブでは、取得するファイル操作ログのフィルタ条件を設定します。どこに存在するファイルにアクセスしたときにログを採取するか、どのプロセスが起動されているときにログを採取するかを設定します。ファイル操作ログを目的に応じて絞り込んで採取できるので、採取後の検索効率が向上します。

[ファイル操作プロセス]タブでの設定項目は、[各種ログスイッチ]タブの[ファイル操作ログ]で[する]を選択した場合に設定できます。

注意

ディスクアクセスが多いソフトウェアは登録しないでください

大量のファイル操作ログが出力され、データベース領域が枯渇する場合がありますので、ウイルスチェックソフトウェアやディスクチェック・修復ソフトウェアなど、ディスクに多くのアクセスを行うソフトウェアは、登録しないでください。
また、OS関係のソフトウェアについても、多くの操作ログを出力する場合があるため、テスト機で性能やOS動作の確認を行ったあとに、登録するようにしてください。



[ファイル操作ログ取得プロセス一覧]に表示される初期値

プロセスEXE名	記録操作の選択	拡張子による選択	削除可否	備考
[cmd.exe]	[参照以外を取得]	[全拡張子を取得]	[不可]	[コマンドプロンプト]
[explorer.exe]	[参照以外を取得]	[全拡張子を取得]	[不可]	[エクスプローラ]
[fsw00ej2.exe]	[参照以外を取得]	[全拡張子を取得]	[不可]	[コマンドプロンプト(DTK)]
[xcopy.exe]	[参照以外を取得]	[全拡張子を取得]	[不可]	[コピーコマンド]
[dllhost.exe]	[参照以外を取得]	[全拡張子を取得]	[不可]	[エクスプローラ]

[ファイル操作ログフィルタ動作設定]

項目名		説明
[ファイル操作ログフィルタ動作設定]		ファイル/フォルダ操作ログの採取対象とするドライブ種別を選択します。
	[全て取得する] **(初期値)**	すべてのドライブの操作を記録します。
	[リムーバブル上のファイルアクセスのみ取得する]	ドライブの種別がリムーバブルディスクのドライブに対する操作を記録します。

項目名	説明
[ネットワーク上とリムーバブル上のファイルアクセスのみ取得する]	ドライブの種別がネットワークとリムーバブルディスクのドライブに対する操作を記録します。
[詳細設定]	[ファイル操作プロセス一詳細設定]画面が表示されます。 ファイル操作ログを取得しないフォルダを設定します。 ([各種ログスイッチ]タブの[ファイル操作ログ]で[しない]を選択した場合は、選択できません。)

[ファイル操作ログ取得プロセス一覧]

項目名	説明
[ファイル操作ログ取得プロセス一覧]	ファイル操作ログ取得時のプロセスや条件が一覧表示されます。 **初期値:** "[ファイル操作ログ取得プロセス一覧]に表示される初期値"に示す情報が表示されます。
[プロセスEXE名]	ファイルやフォルダ操作ログ採取の対象とするプロセスのEXE名を入力します。 半角で254文字まで入力できます。 (英文字は大文字、小文字の区別をしません) また、プロセスの拡張子には「.com」または「.exe」が入力できます。ただし、全角文字や以下の記号を使用するとエラーとなります。 「¥」「/」「:」「*」「?」「"」「<」「>」「|」 **初期値:** 何も指定されていません。
[記録操作の選択]	ログとして記録する操作を選択します。 ・ [全て取得] ファイルやフォルダに対するすべての操作を記録します。 ・ [参照以外を取得]**(初期値)** ファイルやフォルダに対する参照以外の操作を記録します。 ・ [取得しない] ファイルやフォルダに対するすべての操作を記録しません。
[拡張子による選択]	ログとして記録するファイル名の拡張子を選択します。 ・ [全拡張子を取得] そのプロセス(アプリケーション)でアクセスするすべてのファイル(拡張子)に対して、ファイル操作ログを採取する場合に選択します。 これらのファイルの中には、データファイルのほかに、以下の拡張子で表示される、実行モジュールや一時作業用としてアクセスするファイルも含まれます。 ― exe ― dll ― ini ― tmp ― lnk ― inf ・ [拡張子を選択] **(初期値)** 必要なファイル操作ログだけを採取する場合に選択します。 [ファイル操作拡張子]タブで入力した拡張子に対する操作を記録します。 ※エクスプローラのようにファイルやフォルダを操作するプロセス(アプリケーション)を登録し、[全拡張子を取得]を選択した場合、多くの[参照]ログが採取されます。 したがって、データファイルなどの必要な操作ログだけを採取する場合は、[拡張子を選択]を選択することを推奨します。

項目名	説明
[備考]	プロセスの名前やメモ情報などを入力します。 半角で128文字(全角で64文字)まで入力できます。 **初期値:** 何も指定されていません。
[追加/更新]	入力した情報を一覧に追加します。 登録できる件数は、システムであらかじめ設定されているプロセス数と合わせて、30件までです。 または、変更した情報を設定します。
[削除]	[ファイル操作ログ取得プロセス一覧]で選択した情報を削除します。

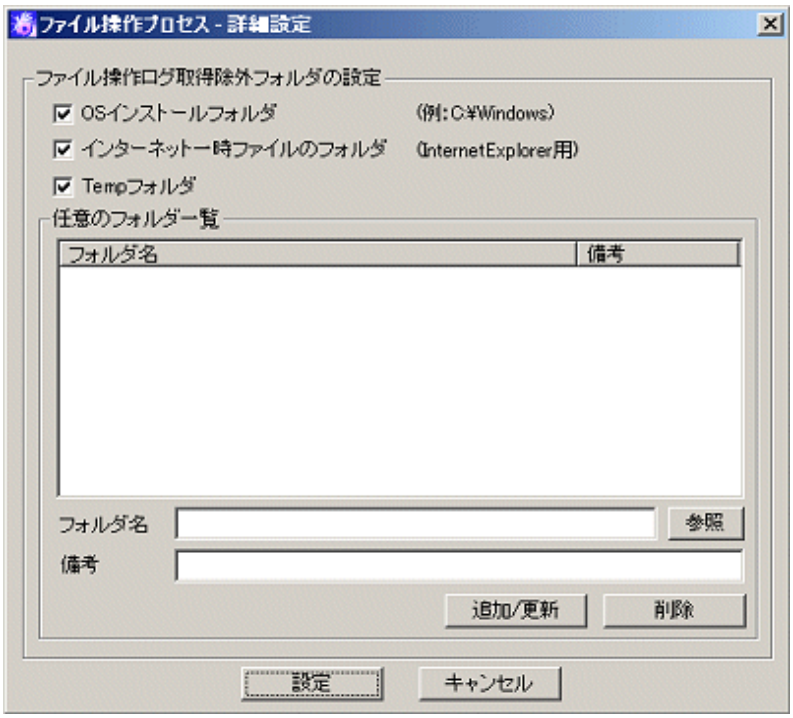
【プロセスを追加する場合】
上記の設定項目を入力し、[追加/更新]ボタンをクリックします。
登録できる件数は、システムであらかじめ設定されているプロセス数と合わせて、30件までです。

【既存情報を更新する場合】
[ファイル操作ログ取得プロセス一覧]から更新する行を選択し、以下の情報を修正して、[追加/更新]ボタンをクリックします。
[プロセスEXE名]は更新できません。また、[削除可否]:[不可]の行を、[記録操作の選択]:[全て取得]にすることはできません。

- [記録操作の選択]
- [拡張子による選択]
- [備考]

【情報を削除する場合】
[ファイル操作ログ取得プロセス一覧]から削除する行を選択し、[削除]ボタンをクリックします。
ただし、[削除可否]:[不可]の行は、削除できません。

[ファイル操作プロセスー詳細設定]画面



[ファイル操作ログ取得除外フォルダの設定]

項目名	説明
[OSインストールフォルダ]	OSインストールフォルダ上のファイルにアクセスしても、操作ログを取得しない場合にチェックします。 チェックした場合、OSインストールフォルダ配下にあるフォルダ、サブフォルダでのファイル操作ログも除外対象となります。 **初期値:**チェックがついています。(※)
[インターネット一時ファイルのフォルダ]	インターネット一時ファイルのフォルダ上のファイルにアクセスしても、操作ログを取得しない場合にチェックします。 **初期値:**チェックがついています。(※)
[Tempフォルダ]	以下のフォルダ上のファイルにアクセスしても、操作ログを取得しない場合にチェックします。 ・ ユーザー環境変数 TEMP、TMPで指定しているフォルダ ・ システム環境変数 TEMP、TMPで指定しているフォルダ **初期値:**チェックがついています。(※)
[任意のフォルダ一覧]	ファイル操作ログの取得を除外する固定ディスクのフォルダを、設定・削除できます。
[フォルダ名]	ファイル操作ログの取得を除外する、固定ディスクのフォルダを、フルパスで指定します。254バイト以内で指定できます。 大文字/小文字は区別しません。 フォルダ名は、100件まで登録できます。 ドライブ名＋コロン(:)の後に「¥」または「/」を付けて、フォルダを指定します。 ドライブ名だけの指定もできます(「D:」など)。ドライブ名だけを指定した場合は、Dドライブ配下のファイルに対するファイル操作ログは、取得されません。 本画面で設定したドライブが、クライアント(CT)ではネットワークドライブやリムーバブルドライブである場合、ファイル操作ログの取得除外フォルダとはなりません。 【例】 本画面で「D:¥temp」を除外フォルダに指定した場合 ・「クライアント(CT) A」のDドライブが固定ディスクのとき 取得除外フォルダとなります。 D:¥tempフォルダ内のファイルを削除してもファイル操作ログは取得されません。 ・「クライアント(CT) B」のDドライブがUSBメモリを使用できるリムーバブルドライブのとき 取得除外フォルダにはなりません。 D:¥tempフォルダ内のファイルを削除するとファイル操作ログが取得されます。 同一のフォルダ名は、複数登録することはできません(「D:¥aaa」と「D:¥aaa¥bbb」は同時に登録できます)。 拡張子付きのフォルダと、拡張子がないフォルダは区別します(「d:¥data」を除外フォルダに指定する場合、「d:¥data.tmp」は除外フォルダになりません。「d:¥data.tmp」も除外フォルダとするためには、「d:¥data.tmp」を登録してください)。 **初期値:**何も指定されていません。
[備考]	メモ情報などを入力します。 半角で128文字(全角で64文字)まで入力できます。 **初期値:**何も指定されていません。
[参照]	操作している管理コンソールがインストールされているPCのフォルダ構成を参照できます。 操作している管理コンソールがインストールされているPCと異なるフォルダ構成のクライアント(CT)に除外フォルダを設定する場合は、[フォルダ名]にフルパスを直接入力してください。

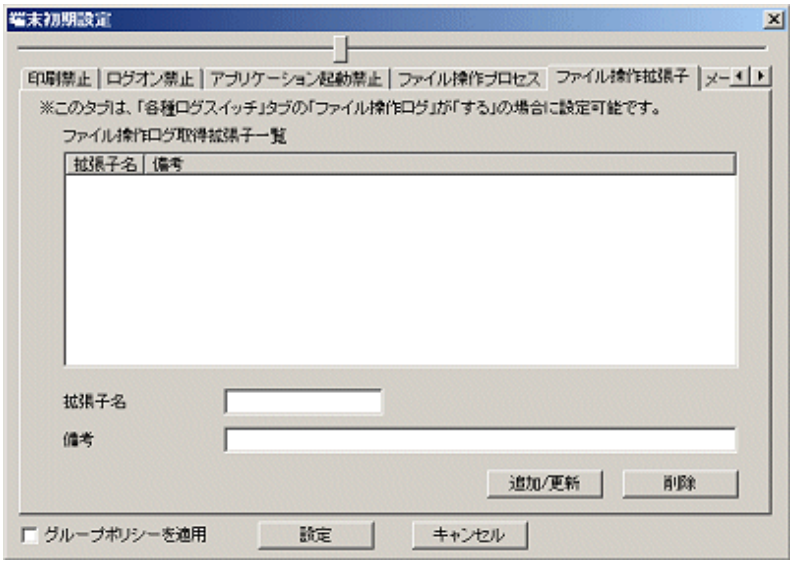
項目名		説明
	[追加/更新]	ファイル操作ログの取得を除外するフォルダを、一覧に追加します。または、すでに登録されているフォルダの備考を更新します(フォルダ名は更新できません)。
	[削除]	ファイル操作ログの取得を除外するフォルダを、一覧から削除します。 [任意のフォルダ一覧]で該当するフォルダ行を選択し、[削除]ボタンをクリックします。
[設定]		入力した内容を確定し、[ファイル操作プロセス]タブに戻ります。
[キャンセル]		設定した情報を保存せずに画面を閉じます。

※) Systemwalker Desktop Keeper V13.2.1以前からバージョンアップした場合は、すべてチェックされていません。

2.4.1.7 [ファイル操作拡張子]タブの設定

[ファイル操作拡張子]タブでは、[ファイル操作プロセス]タブで設定したプロセスでアクセスするファイル(拡張子)に対して、ファイル操作ログを採取する場合に、その拡張子名を設定します。

[ファイル操作拡張子]タブでの設定項目は、[各種ログスイッチ]タブの[ファイル操作ログ]で[する]を選択した場合に設定できます。



項目名	説明
[ファイル操作ログ取得拡張子一覧]	すでに登録されている、ファイル操作ログを取得するファイルの拡張子が表示されます。 拡張子の登録件数が0件の場合、[ファイル操作プロセス]タブで登録されているプロセスの[拡張子による選択]において[拡張子を選択]が設定されていても、そのプロセスのログは採取されません。 **初期値:**何も指定されていません。
[拡張子名]	ファイルやフォルダ操作ログ採取の対象とする拡張子名を入力します。拡張子の「.」(ドット)は入力する必要はありません。(入力できません) 半角で16文字まで入力できます(英文字は大文字、小文字の区別をしません)。 以下の記号を使用するとエラーとなります。 「¥」「/」「:」「*」「?」「"」「<」「>」「|」 ワイルドカード(*)を使用する場合は、拡張子名の先頭1文字、または末尾1文字に、*記号を付けて入力します。 ・ 前方一致を指定する場合: 「拡張子名*」を入力します。【例】xl* ・ 後方一致を指定する場合: 「*拡張子名」を入力します。【例】*ls

項目名	説明
	上記以外の位置へは、ワイルドカード(*)を入力できません。 また、ワイルドカード(*)だけの入力もできません。必ず、文字と組み合わせて入力してください。 **初期値:**何も指定されていません。
[備考]	拡張子の名前やメモ情報などを入力します。 半角で128文字(全角で64文字)まで入力できます。 **初期値:**何も指定されていません。
[追加/更新]	入力した情報を一覧に追加します。 登録できる件数は、20件までです。 または、変更した情報を設定します。
[削除]	[ファイル操作ログ取得プロセス一覧]で選択した情報を削除します。

【拡張子名を追加する場合】
上記の設定項目を入力し、[追加/更新]ボタンをクリックします。
登録できる件数は、20件までです。

【既存情報を更新する場合】
[ファイル操作ログ取得拡張子一覧]から更新する行を選択し、[備考]の情報を修正して、[追加/更新]ボタンをクリックします。
[拡張子名]は更新できません。

【情報を削除する場合】
[ファイル操作ログ取得拡張子一覧]から削除する行を選択し、[削除]ボタンをクリックします。

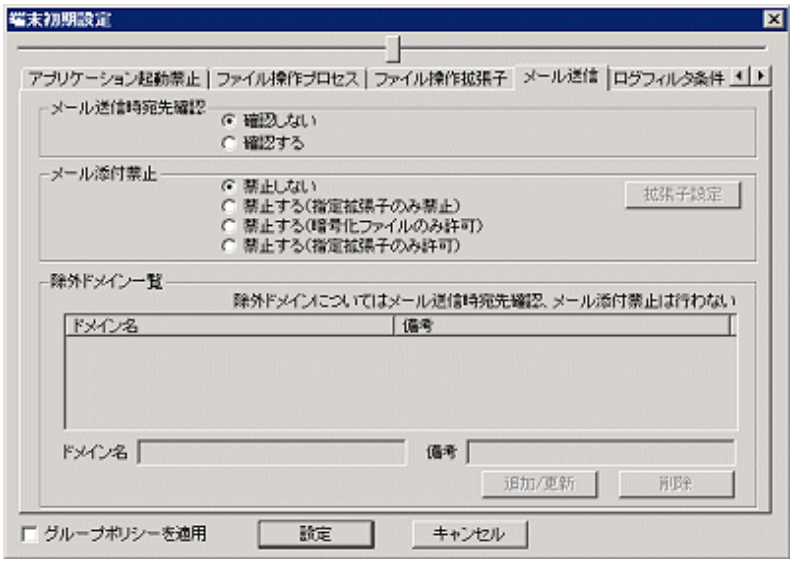
2.4.1.8 [メール送信]タブの設定

[メール送信]タブでは、以下を設定します。

- メールへのファイル添付の許可または禁止
- メール送信時のあて先確認の実施の有無
- 添付禁止、宛先確認の除外ドメインの設定

設定条件に応じて、メール送信時にあて先を確認するメッセージを表示できます。また、許可されたファイルまたは禁止されたファイルをメールに添付して送信することを、許可または禁止できます。

[メール送信]タブでの設定内容を説明します。



[メール送信時宛先確認]

本項目は、[各種ログスイッチ]タブでの[メール送信ログ]の取得ポリシーに関係なく設定できます。

項目名	説明
[確認しない] **(初期値)**	メール送信時のあて先に関係なく、警告メッセージは表示しません。
[確認する]	ユーザーが[除外ドメイン一覧]に設定されているドメイン以外へメールを送信しようとした場合、警告メッセージを表示します。 ユーザーは、警告メッセージ画面で、警告対象となったドメインのメールアドレスが正しいことを確認し、チェックをつけた場合だけ、メールを送信できます。

[メール添付禁止]

本項目は、[各種ログスイッチ]タブでの[メール送信ログ]の取得ポリシーに関係なく設定できます。
また、添付ファイルの中に1つでも、添付禁止対象のファイルがある場合、メール(メール本文と、すべての添付ファイル)は送信できません。

項目名	説明
[禁止しない] **(初期値)**	ファイルを添付して送信または保存することを禁止しません。
[禁止する(指定拡張子のみ禁止)]	指定した拡張子のファイルを添付して送信または保存することを禁止します。 対象となるメールソフトを説明します。 ・ ポート監視方式の場合:SMTPプロトコルを使用するメールソフトです。 ・ V12.0L20～V13.0.0互換方式の場合:以下のメールソフトです。 － Microsoft® Outlook® Express 5.5 － Microsoft® Outlook® Express 6.0 － Microsoft® Outlook® 2000 － Microsoft® Outlook® 2002 － Microsoft® Outlook® 2003
[禁止する(暗号化ファイルのみ許可)]	以下の製品により暗号化されたファイルだけ、メールに添付して送信または保存することを許可します。 ・ Systemwalker Desktop Keeperのすべてのバージョンにより暗号化されたファイル ・ Systemwalker Desktop Encryption V12.0L10/L20、V13.0.0により暗号化されたファイル ・ SecureBOX V2.0の自己復号ファイル ・ Systemwalker Desktop Rights Master V13.0.0、V13.2.0により暗号化されたファイル ・ FENCE-PRO V5/V6により暗号化されたファイル
[禁止する(指定拡張子のみ許可)]	指定した拡張子のファイルだけ、メールに添付して送信または保存することを許可します。 本指定が有効になるのは、以下の条件をすべて満たす場合です。 ・ ポリシー設定先のクライアント(CT)がV14.0.0以降のとき ・ クライアント(CT)の[メール制御方式の設定]が、[ポート監視方式]のとき クライアント(CT)がV13.3.0以前の場合や、[V12.0L20～V13.0.0互換方式]の場合は、添付を許可する拡張子を指定しても無効になり、すべてのファイルのメール添付が許可されます。
[拡張子設定]	[メール送信 ― メール添付禁止拡張子設定]画面が表示されます。 (メール添付を許可または禁止するファイルの拡張子名を設定します。)

[除外ドメイン一覧]

項目名	説明
[除外ドメイン一覧]	一覧に表示されているドメインへのメール送信に関しては、あて先確認を行いません。また、添付ファイルの禁止も行いません。
[ドメイン名]	メール送信を許可するドメイン名を入力します。 半角で254文字まで入力できます(英文字は大文字、小文字の区別をしません)。 以下の記号を使用するとエラーとなります。 「`」、「~」、「!」、「@」、「#」、「$」、「^」、「&」、「*」、「(」、「)」「=」、「+」、「[」、「]」、「{」、「}」、「¥」、「|」、「;」、「:」、「'」、「"」、「,」、「<」、「>」、「/」、「?」、「%」 **初期値:**何も指定されていません。
[備考]	ドメイン名に関するメモ情報などを入力します。 半角で128文字(全角で64文字)まで入力できます。 **初期値:**何も指定されていません。
[追加/更新]	メール送信を許可するドメイン名が追加されます。 追加できる件数は100件までです。 [除外ドメイン一覧]で選択した行の[備考]を変更した場合、情報が更新されます([ドメイン名]は更新できません)。
[削除]	[除外ドメイン一覧]で選択した行が削除されます。

[メール送信 — メール添付禁止拡張子設定]画面

メール添付を許可または禁止するファイルの拡張子名を設定します。

[拡張子一覧]

項目名	説明
[拡張子一覧]	メール添付を許可または禁止するファイルの拡張子名が、一覧表示されます。 **初期値:**何も指定されていません。
[拡張子名]	添付を許可または禁止するファイルの拡張子名を入力します。拡張子の「.」(ドット)は入力する必要はありません。(入力できません) 半角で16文字まで入力できます(英文字は大文字、小文字の区別をしません)。 以下の記号を使用するとエラーとなります。 「¥」「/」「:」「*」「?」「"」「<」「>」「|」 **初期値:**何も指定されていません。

項目名	説明
[備考]	拡張子の名前やメモ情報などを入力します。 半角で128文字(全角で64文字)まで入力できます。 **初期値:**何も指定されていません。
[追加/更新]	添付を許可または禁止するファイルの拡張子名が追加されます。 追加できる件数は100件までです。 [拡張子一覧]で選択した行の[備考]を変更した場合、情報が更新されます([拡張子名]は更新できません)。
[削除]	[拡張子一覧]で選択した行が削除されます。
[OK]	入力した内容を確定し、[メール送信]タブに戻ります。
[キャンセル]	設定した情報を保存せずに画面を閉じます。

2.4.1.9 [ログフィルタ条件]タブの設定

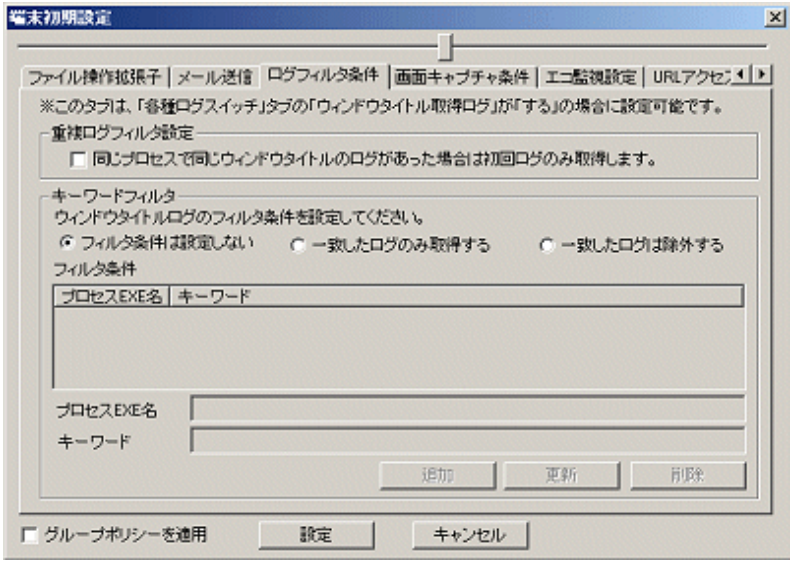
[ログフィルタ条件]タブでは、ウィンドウタイトル取得ログを採取する条件を設定します。
ウィンドウタイトル取得ログは、PC上の全操作を記録するため大量に採取され、重複したログが多数存在します。このため、ログを重複して採取しないための、フィルタリング条件を設定します。

ログフィルタ条件の指定には、2とおりあります。両方の条件を指定することも可能です。

- 重複ログフィルタ設定:
  同じプロセスで同じウィンドウタイトルログがあった場合は、初回のログだけ取得します。
- キーワードフィルタ:
  プロセス名とキーワードを指定することで、設定したプロセス名で設定したキーワードを含む、ウィンドウタイトルログを採取または除外します。

[ログフィルタ条件]タブは、[各種ログスイッチ]タブの[ウィンドウタイトル取得ログ]で[する]が選択されている場合に設定できます。

[ログフィルタ条件]タブでの設定内容を説明します。



[重複ログフィルタ設定]

項目名	説明
[重複ログフィルタ設定]	重複したログの取得方法を選択します。

項目名	説明
	・ チェックする場合: 同じプロセスで同じウィンドウタイトルのログがあった場合は初回のログだけ取得します。 ・ チェックしない場合**(初期値)**: すべてのウィンドウタイトル取得ログを採取します。

[キーワードフィルタ]

項目名	説明
[フィルタ条件は設定しない] **(初期値)**	プロセス名またはキーワードによるウインドタイトルログのフィルタを行いません。
[一致したログのみ取得する]	フィルタ条件で指定したプロセスまたは、ウィンドウタイトルがフィルタ条件で指定したキーワードと部分一致したログだけ取得します。
[一致したログは除外する]	フィルタ条件で指定したプロセスまたは、ウィンドウタイトルがフィルタ条件で指定したキーワードと部分一致したログだけ取得しません。
[フィルタ条件]	設定した条件が一覧表示されます。 **初期値:**何も指定されていません。
[プロセスEXE名]	ウィンドウタイトル取得ログを採取するプロセスのEXE名を入力します。 ウィンドウタイトルログのフィルタ条件で[一致したログは除外する]を選択した場合は、ウィンドウタイトル取得ログを採取しないプロセス名を指定します。 半角で254文字(全角で127文字)まで入力できます。 (英文字は大文字、小文字の区別をしません) プロセスの拡張子には「.com」または「.exe」が入力できます。 以下の記号を使用するとエラーとなります。 「¥」「/」「:」「*」「?」「"」「<」「>」「|」 [プロセスEXE名]を空白に設定した場合は全プロセスが対象になります。 **初期値:**何も指定されていません。
[キーワード]	ウィンドウタイトル取得ログを採取するキーワードを入力します(ウィンドウタイトルにここで指定したキーワードが含まれる(部分一致)/含まれない(部分一致)場合にウィンドウタイトルログを取得します)。 ウィンドウタイトルログのフィルタ条件で[一致したログは除外する]を選択した場合は、ウィンドウタイトル取得ログを採取しないキーワードを指定します。 【例】 ・ 名前を付けて保存 ・ 印刷 半角で254文字(全角で127文字)まで入力できます。 (英文字は大文字、小文字の区別をしません) [キーワード]を指定しない場合は、[プロセスEXE名]で指定したプロセスのすべてのウィンドウタイトル取得ログが採取(または除外)されます。 **初期値:**何も指定されていません。
[追加]	[フィルタ条件]に条件を追加します。 登録できる件数は30件までです。
[更新]	[フィルタ条件]で選択した行の情報を変更した場合、情報が更新されます。
[削除]	[フィルタ条件]で選択した行の情報を削除します。

[フィルタ条件]に[プロセスEXE名]と[キーワード]の両方を指定した場合は、AND条件として設定されます。
また、[プロセスEXE名]と[キーワード]の組み合わせからなる各行は、OR条件として設定されます。

【条件を追加する場合】
上記の設定項目を入力し、[追加]ボタンをクリックします。
登録できる件数は、30件までです。

【既存情報を更新する場合】
[フィルタ条件]から更新する行を選択し、情報を修正して、[更新]ボタンをクリックします。

【情報を削除する場合】
[フィルタ条件]から削除する行を選択し、[削除]ボタンをクリックします。

2.4.1.10 [画面キャプチャ条件]タブの設定

[画面キャプチャ条件]タブでは、画面キャプチャを取得する条件を設定します。
[ログフィルタ条件]タブで設定した条件に合致した、ウィンドウタイトル取得ログが採取された場合、同時に、その画面も採取するときに、本タブで条件を設定します。

[画面キャプチャ条件]タブは、[各種ログスイッチ]タブの[ウィンドウタイトル取得ログ]で[する]が選択されている場合に設定できます。

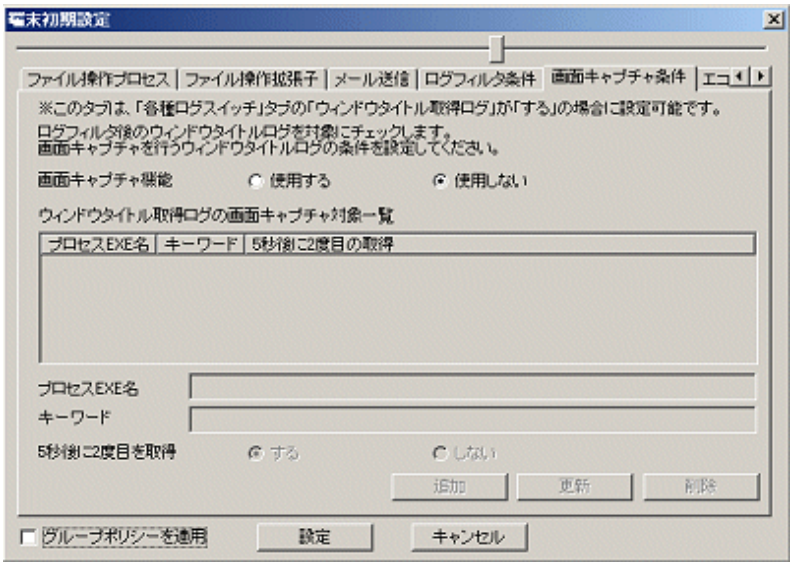
画面キャプチャに関する設定は、[端末動作設定]画面(設定項目:[付帯データ条件設定])でも行います。詳細は、“2.4.2 端末動作設定をおこなう”を参照してください。

注意

画面キャプチャデータは、定期的にバックアップまたは削除してください

画面キャプチャ条件によってはサーバ(端末動作設定の設定によってはクライアント(CT))に画面キャプチャデータが大量に蓄積され、ディスク容量が枯渇する可能性があります。このため定期的な容量確認とバックアップおよび削除を行ってください。

[画面キャプチャ条件]タブでの設定内容を説明します。



項目名	説明
[画面キャプチャ機能]	画面キャプチャを取得するかどうかを選択します。 ・ [使用する] 画面キャプチャを取得します。 ・ [使用しない] **(初期値)** 画面キャプチャを取得しません。

項目名	説明
[ウィンドウタイトル取得ログの画面キャプチャ対象一覧]	画面キャプチャを取得する条件が一覧表示されます。 **初期値:**何も指定されていません。
[プロセスEXE名]	画面キャプチャを行うプロセスのEXE名を入力します。 半角で254文字(全角で127文字)まで入力できます(英文字は大文字、小文字の区別をしません)。 プロセスの拡張子には「.com」または「.exe」が入力できます。 ただし、以下の記号を使用するとエラーとなります。 「¥」「/」「:」「*」「?」「"」「<」「>」「|」 プロセスEXE名を空白に設定した場合は全プロセスが対象になります。 **初期値:**何も指定されていません。
[キーワード]	画面キャプチャを取得するキーワードを入力します(ウィンドウタイトルにここで指定したキーワードが含まれる(部分一致)場合に画面キャプチャを取得します)。 【例】 ・ 名前を付けて保存 ・ 印刷 半角で254文字(全角で127文字)まで入力できます(英文字は大文字、小文字の区別をしません)。 [プロセスEXE名]でプロセスのEXE名を入力した場合は、必ず[キーワード]を入力してください。 **初期値:**何も指定されていません。
[5秒後に2度目を取得]	画面キャプチャを取得した後、5秒後に2度目の取得を行うかどうかを設定します。 画面キャプチャを連続して取得し、操作の状況をさらに把握したい場合は、[する]を選択してください。 ・ [する] 2度目の画面キャプチャを5秒後に取得します。 ・ [しない] 初回だけ画面キャプチャを取得します。 [する]を選択している場合、5秒後に2度目の画面キャプチャが採取されます。しかし、1度目と2度目の5秒間に、画面キャプチャを採取する条件に合致した新たな画面が存在しても、この画面キャプチャは採取されません。ただし、最初の画面の2度目のキャプチャは実行されますので、ログビューアのログ一覧では、[付帯]に画面キャプチャを2度取得したことを意味する“2”が表示されます。
[追加]	[画面キャプチャ機能]で[使用する]を選択した場合、画面キャプチャ取得条件を、一覧に追加します。 登録できる件数は10件までです。
[更新]	[ウィンドウタイトル取得ログの画面キャプチャ対象一覧]で選択した行の情報を変更した場合、情報が更新されます。
[削除]	[ウィンドウタイトル取得ログの画面キャプチャ対象一覧]で選択した行の情報を削除します。

[ウィンドウタイトル取得ログの画面キャプチャ対象一覧]に[プロセスEXE名]と[キーワード]の両方を指定した場合は、AND条件として設定されます。
また、[プロセスEXE名]と[キーワード]の組み合わせからなる各行は、OR条件として設定されます。

[画面キャプチャ条件]タブでの設定内容と[ログフィルタ条件]タブでの設定内容は、AND条件として設定されます。したがって、画面キャプチャを取得するポリシーを設定しているにもかかわらず画面キャプチャを取得できない場合は、ログフィルタ条件が設定されていないことが考えられます。

【条件を追加する場合】
上記の設定項目を入力し、[追加]ボタンをクリックします。
登録できる件数は、10件までです。

【既存情報を更新する場合】
[ウィンドウタイトル取得ログの画面キャプチャ対象一覧]から更新する行を選択し、情報を修正して、[更新]ボタンをクリックします。

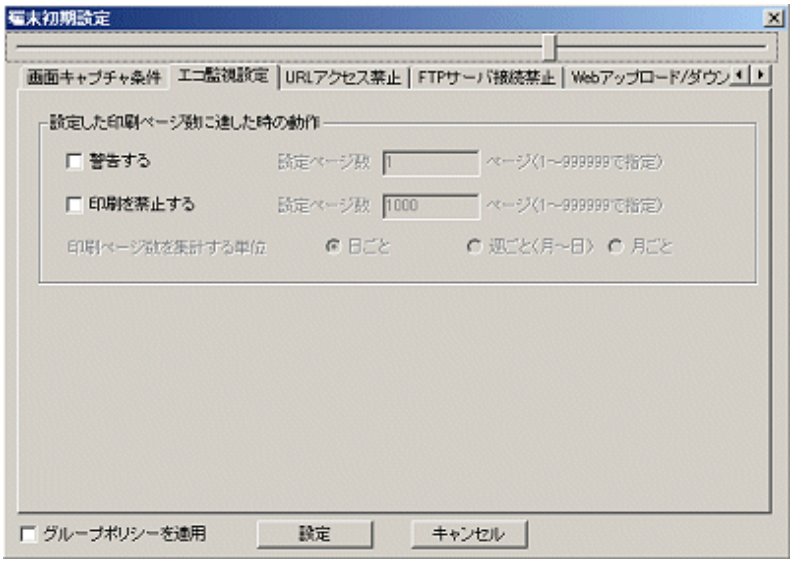
【情報を削除する場合】
[ウィンドウタイトル取得ログの画面キャプチャ対象一覧]から削除する行を選択し、[削除]ボタンをクリックします。

2.4.1.11 [エコ監視設定]タブの設定

印刷ページ数を監視することによって、紙への無駄な印刷を削減したい場合に、[エコ監視設定]タブで条件を設定します。
本機能は、CTインストール時の[印刷監視方式の設定]で、[この端末で設定されている全てのプリンタでの印刷を監視する(推奨)]を選択した場合に有効です。
監視条件は、[各種ログスイッチ]タブの[印刷操作ログ]で[する]が選択されている場合に設定できます。

設定ページ数に達した場合に印刷を禁止するときは、クライアント(CT)利用者に警告メッセージを表示したり、印刷を禁止したりできます。同時に、印刷禁止ログに違反として記録されます。

[エコ監視設定]タブでの設定内容は、CTポリシーとして扱われます。



[設定した印刷ページ数に達した時の動作]

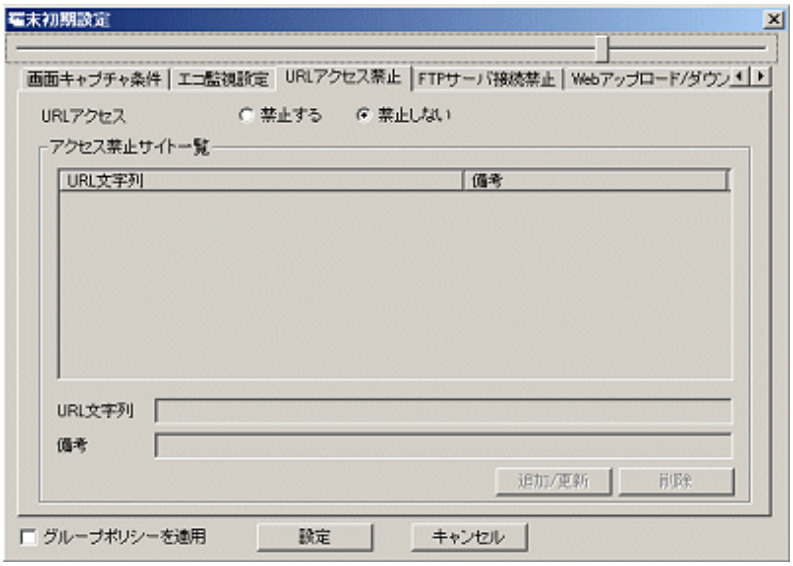
項目名	説明
[警告する](※)	・ チェックする場合: 設定した印刷ページ数に達した場合に、警告メッセージを表示します。 印刷操作ログとして記録されます。 紙に印刷を行わないドキュメントライタ(Microsoft Office Document Inage Writerや、Adobe PDFなど)の動作が、印刷ページ数にカウントされることがあります。 ー [設定ページ数]:メッセージを表示する契機となるページ数を、1～999999の範囲で設定します。初期値は、1です。 ・ チェックしない場合**(初期値)**: 印刷ページ数はカウントしますが、メッセージは表示しません。
[印刷を禁止する](※)	・ チェックする場合: 設定した印刷ページ数に達した場合に、印刷を禁止します。[印刷禁止]タブで指定した印刷許可アプリケーションの場合でも、印刷できません。また、ドキュメントライタ(Microsoft Office Document Image Writerや、Adobe PDFなど)への印刷もできません。

項目名		説明
		印刷禁止ログに違反として記録されます。 本項目をチェックした場合、[警告する]も自動的にチェックされます。 印刷開始時に、印刷済みのページが禁止の値に達していた場合、その印刷は実行されません(印刷禁止のメッセージが表示されます)。印刷途中に禁止のページ数に達した場合は、その印刷は中断されません。次の印刷から禁止されます。 管理者通知設定を行っている場合は、管理者にメール通知します。また、イベントログに記録されます。 ー [設定ページ数]:印刷を禁止する契機となるページ数を、1～999999の範囲で設定します。初期値は、1000です。 ・ チェックしない場合**(初期値)**: 印刷ページ数はカウントしますが、印刷を禁止しません。
[印刷ページ数を集計する単位]	[日ごと] **(初期値)**	24時間の範囲で印刷ページ数を監視します。 PCの時計の日付の「日」が変わると、印刷ページ数を0にリセットします。
	[週ごと(月～日)]	1週間の範囲で印刷ページ数を監視します。 PCの時計の日付が「月曜日の午前0時」で、印刷ページ数を0にリセットします。
	[月ごと]	1月の範囲で印刷ページ数を監視します。 PCの時計の日付の「月」が変わると、印刷ページ数を0にリセットします。

※) [警告する]と[印刷を禁止する]の両方をチェックする場合は、
[警告する]ときの設定ページ数≦[印刷を禁止する]ときの設定ページ数
となるように入力してください。

2.4.1.12 [URLアクセス禁止]タブの設定

[URLアクセス禁止]タブでは、アクセスを禁止するURLを設定します。

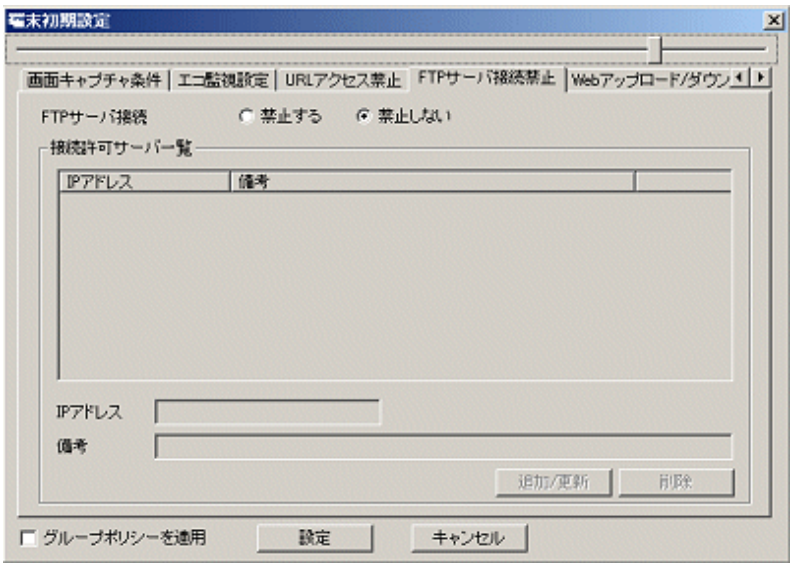


項目名		説明
[URLアクセス]	[禁止する]	[アクセス禁止サイト一覧]で指定したURLへのアクセスを禁止します。
	[禁止しない] **(初期値)**	どのURLに対しても、アクセスできます。
[アクセス禁止サイト一覧]		アクセスを禁止するURLと、そのURLに関するメモが表示されます。 **初期値:**何も表示されていません。

項目名	説明
[URL文字列]	[URLアクセス]を[禁止する]場合は、アクセスを禁止するURLの、ドメイン名部分に含まれる文字列を入力します。 入力した文字列を含むサイトは、すべてアクセスが禁止されます。 【例】[URL文字列]にfujitsu.comを設定した場合、以下のどちらも禁止されます。 http://jp.**fujitsu.com** http://www.soft.**fujitsu.com**/dt/desktopkeeper/ 半角で254バイト以内の英数字と記号(※)が入力できます(英文字は大文字、小文字の区別をしません)。 ※) URLとして有効な文字種は、以下のとおりです。 「'」「.」「-」「*」「)」「(」「_」「:」「%」「+」 日本語ドメイン名は使用できません。 100件まで登録できます。 **初期値:** 何も指定されていません。
[備考]	アクセスを禁止するURLのメモ情報などを入力します。 半角で128バイト(全角で64文字)まで入力できます。 **初期値:** 何も指定されていません。
[追加/更新]	アクセスを禁止するURLが追加されます。 追加できる件数は100件までです。 [アクセス禁止サイト一覧]で選択した行の[備考]を変更した場合、情報が更新されます([URL文字列]は更新できません)。
[削除]	[アクセス禁止サイト一覧]で選択した行が削除されます。

2.4.1.13 [FTPサーバ接続禁止]タブの設定

[FTPサーバ接続禁止]タブでは、管理者が許可したFTPサーバ以外への接続の禁止を設定します。
Internet Explorer®からFTPサーバへの接続操作を禁止する場合は、[URLアクセス禁止]タブで設定してください。

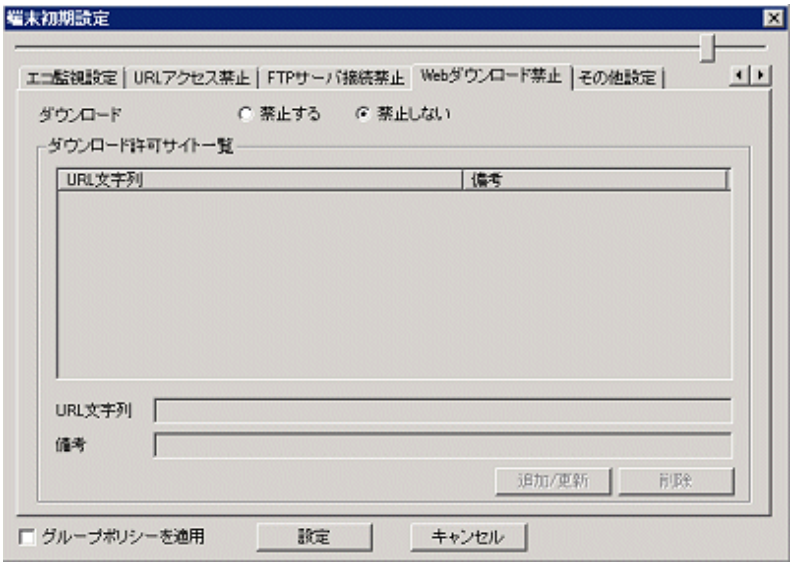


項目名		説明
[FTPサーバ接続]	[禁止する]	[接続許可サーバー覧]で指定したサーバ以外への接続を禁止します。
	[禁止しない] **(初期値)**	どのFTPサーバに対しても接続できます。

項目名	説明
[接続許可サーバー一覧]	接続を許可するサーバのIPアドレス、接続先サーバに関するメモが表示されます。 **初期値:** 何も表示されていません。
[IPアドレス]	接続先サーバのIPアドレス(IPV4形式)を入力します。 100件まで登録できます。 **初期値:** 何も表示されていません。
[備考]	接続を許可するサーバのメモ情報などを入力します。 半角で128文字(全角で64文字)まで入力できます。 **初期値:** 何も指定されていません。
[追加/更新]	接続を許可するサーバが追加されます。 追加できる件数は100件までです。 [接続許可サーバー一覧]で選択した行の[備考]を変更した場合、情報が更新されます([IPアドレス]、[接続先ポート]は更新できません)。
[削除]	[接続許可サーバー一覧]で選択した行が削除されます。

2.4.1.14 [Webダウンロード禁止]タブの設定

[Webダウンロード禁止]タブでは、管理者が許可したWebサイト以外からのダウンロードの禁止を設定します。



項目名		説明
[ダウンロード]	[禁止する]	[ダウンロード許可サイト一覧]で指定したWebサイト以外からのダウンロードを禁止します。
	[禁止しない] **(初期値)**	どのWebサイトからもダウンロードできます。
[ダウンロード許可サイト一覧]		ダウンロードを許可するWebサイトのURLと、そのURLに関するメモが表示されます。 **初期値:** 何も表示されていません。
[URL文字列]		ダウンロードを許可するWebサイトのURLを入力します。 入力した文字列を含むサイトは、すべてダウンロードが許可されます。 【例】[URL文字列]にfujitsu.comを設定した場合、以下のどちらも許可されます。 http://jp.**fujitsu.com** http://www.soft.**fujitsu.com**/dt/desktopkeeper/

項目名	説明
	半角で254バイト以内の英数字と記号(※)が入力できます(英文字は大文字、小文字の区別をしません)。 ※) URLとして有効な文字種は、以下のとおりです。 「'」「.」「-」「)」「(」「_」「:」「/」「%」「+」 日本語ドメイン名は使用できません。 100件まで登録できます。 **初期値:** 何も指定されていません。
[備考]	ダウンロードを許可するURLのメモ情報などを入力します。 半角で128バイト(全角で64文字)まで入力できます。 **初期値:** 何も指定されていません。
[追加/更新]	ダウンロードを許可するURLが追加されます。 追加できる件数は100件までです。 [ダウンロード許可サイト一覧]で選択した行の[備考]を変更した場合、情報が更新されます([URL文字列]は更新できません)。
[削除]	[ダウンロード許可サイト一覧]で選択した行が削除されます。

2.4.1.15 [その他設定]タブの設定

[その他設定]タブでは、クライアント(CT)で生成されるログを管理サーバに送信する方法を設定します。送信されるのは、操作ログ、禁止ログ、および付帯データです。

Citrix XenAppと連携する場合は、[その他設定]タブの項目を設定する必要はありません。必ず[操作ログを一定時間まとめてから送信する]が選択されたものとしてポリシーが設定されます(ただし、1度に送信するログ数や送信間隔の設定は、[端末動作設定]画面で設定してください)。

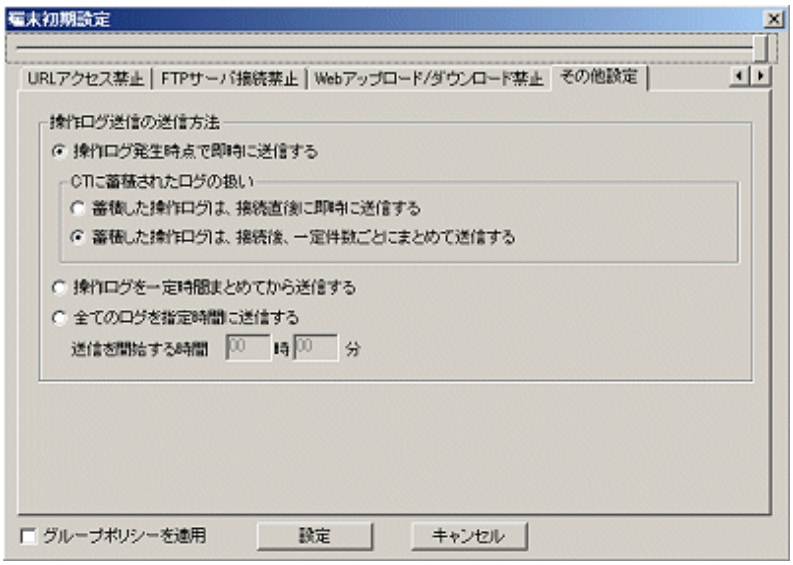
注意

コマンドプロンプト操作ログのサーバへの送信について

コマンドプロンプト操作ログは、常に、採取後即時送信されます(本設定の影響を受けません)。

以下に示す状況ごとに、送信方法を設定します。

- 常時、クライアント(CT)がサーバとネットワーク接続されているとき
- モバイル運用などでクライアント(CT)に蓄積されたログを、サーバとのネットワーク接続時に送信するとき



[操作ログ送信の送信方法]

項目名			説明
[操作ログ発生時点で即時に送信する] **(初期値)**			ログを、発生時に即時にサーバに送信します。
	[CTに蓄積されたログの扱い]		モバイル運用などでクライアント(CT)に蓄積されたログを、サーバとのネットワーク接続時に送信する方法を設定します。
		[蓄積した操作ログは、接続直後に即時に送信する]	ネットワーク非接続の環境からネットワーク接続環境に変わった時点(管理サーバ、統合管理サーバと通信開始時)で、即時にクライアント(CT)からサーバに、蓄積されたログを送信します。
		[蓄積した操作ログは、接続後、一定件数ごとにまとめて送信する] **(初期値)**	ネットワーク非接続の環境からネットワーク接続環境に変わった時点(管理サーバと通信開始時)で、一定件数ごとに、クライアント(CT)からサーバに、蓄積されたログを送信します。 1度に送信するログ数や送信間隔の設定は、[端末動作設定]画面で行います。詳細は、“2.4.2 端末動作設定をおこなう”を参照してください。
[操作ログを一定時間まとめてから送信する]			ログを一定時間蓄積してから、サーバに送信します。 1度に送信するログ数や送信間隔の設定は、[端末動作設定]画面で行います。詳細は、“2.4.2 端末動作設定をおこなう”を参照してください。
[全てのログを指定時間に送信する]			ログを、指定した時間に、サーバに送信します。 ログの[送信を開始する時間]を必ず設定します。 【ログ送信終了にかかる時間について】 目安を以下に示します。クライアント(CT)の台数や1台あたりのログ件数と、送信所要時間は、おおむね比例します。 例1 ・ クライアント(CT)台数:1000台 ・ 1台あたりのログ件数:1000件 ・ ログ送信に要する時間:最大で約15分 例2 ・ クライアント(CT)台数:2000台 ・ 1台あたりのログ件数:1000件 ・ ログ送信に要する時間:最大で約30分

項目名	説明
	1度に送信するログ数や送信間隔の設定は、[端末動作設定]画面で行います。詳細は、“2.4.2 端末動作設定をおこなう”を参照してください。

2.4.2 端末動作設定をおこなう

クライアント(CT)の動作設定(付帯データの条件設定や、ログの送信方法の設定)を行います。この設定は、システム管理者だけが実施できます。

クライアント(CT)の動作設定は、管理サーバ、統合管理サーバ単位に、設定することが可能です。設定値は、クライアント(CT)が、起動時に管理サーバ、統合管理サーバから取得します。またCTポリシーの即時更新時にもクライアント(CT)の動作設定の値が更新されます。

3階層の構成において、端末動作設定の設定値を初期値から変更する場合は、Active Directory連携の有無やユーザーポリシーの一元管理の有無にかかわらず、すべての管理サーバ（統合管理サーバにもCTが接続されている場合は、統合管理サーバでも）で再設定する必要があります。

注意

クライアント(CT)の動作設定が、クライアント(CT)に反映されるタイミング

クライアント(CT)の動作設定が、クライアント(CT)に反映されるタイミングは以下のとおりです。

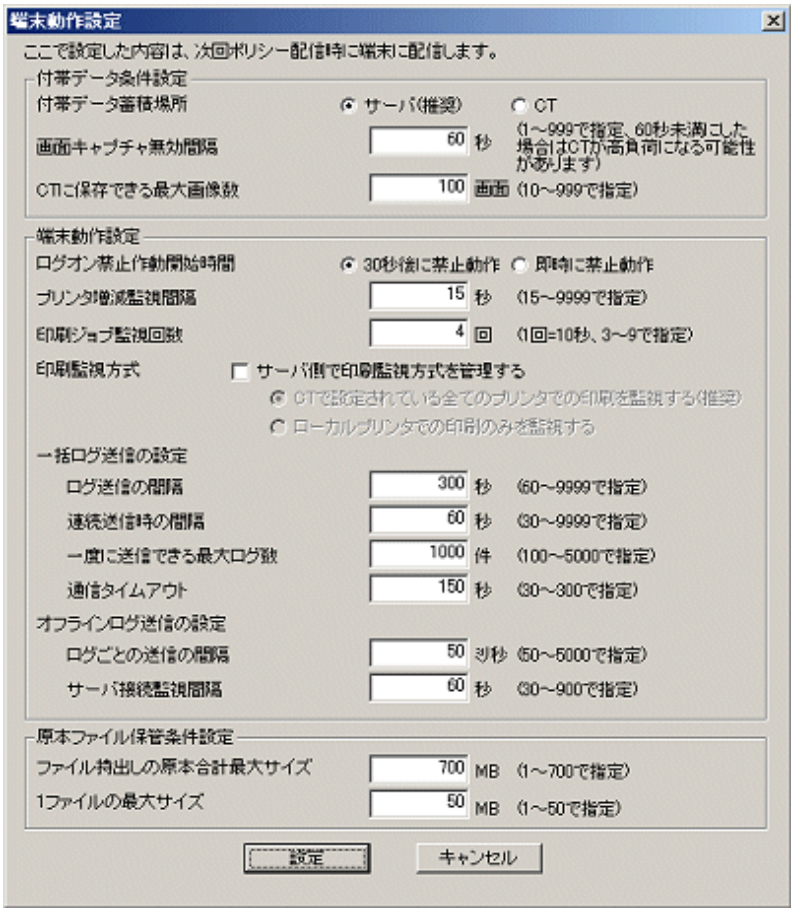
- クライアント(CT)の動作設定を行い、クライアント(CT)にCTポリシーの即時更新を行った場合は、次回のクライアント(CT)の再起動で反映します。
- クライアント(CT)の動作設定を行い、クライアント(CT)にCTポリシーの即時更新を行わない場合は、次々回のクライアント(CT)の再起動で反映します。

設定手順は、以下のとおりです。

1. [管理コンソール]を起動します。

2. [動作設定]メニューから[端末動作設定]を選択します。

→[端末動作設定]画面が表示されます。



3. 以下の情報を入力し、[設定]ボタンをクリックします。

[付帯データ条件設定]

項目名	説明
[付帯データ蓄積場所]	付帯データ(画面キャプチャデータ、ファイル持出しにおける原本保管ファイル)の蓄積場所を指定します。 ・ [サーバ(推奨)] 付帯データを管理サーバに蓄積します。 ・ [CT] 付帯データをクライアント(CT)に蓄積します。管理サーバには転送しません。 クライアント(CT)のログファイルの格納フォルダ配下のSaveフォルダに保存されます。 格納された付帯データの管理機能はありません。したがって、システム管理者が定期的に蓄積されたデータを確認する必要があります。付帯データ蓄積場所は、SYSTEM権限で保護されています。確認する場合は、格納フォルダのセキュリティ設定にデータを参照するユーザーを追加してください。 画面キャプチャデータの場合、ファイル名は“CAP-(36文字のCTID)-YYYYMMDDHHMMSS-04-02-00-AAAAAA-B.png”でAAAAAAは任意の数字です。Bは1または2で、1は最初に取得した画面キャプチャ画像、2は5秒後に取得した画面キャプチャ画像を意味します。 ファイル持出しにおける原本保管ファイルの場合、ファイル名は“CAB-(36文字のCTID)-YYYYMMDDHHMMSS-11-00-00-AAAAAA-1.(原本ファイルの拡張子)”でAAAAAAは任意の数字です。 初期値は[サーバ(推奨)]です。

項目名	説明
[画面キャプチャ無効間隔]	クライアント(CT)側の高負荷を防止するため、画面キャプチャ取得後、次の画面キャプチャ取得までの間隔を指定します。 初期値(推奨値)は「60」です。最小値は「1」、最大値は「999」です。 この値の間に次の画面キャプチャ条件を満たしても、画面キャプチャは採取されません。(ウィンドウタイトルログにおける、画面キャプチャ採取時の動作です。PrintScreenキー操作、および、PrintScreenキー禁止時の画面キャプチャ採取時はこの設定は有効とはならず、連続して採取可能です。)
[CTに保存できる最大画像数]	クライアント(CT)に保存できる最大画面キャプチャデータ数を指定します。初期値(推奨値)は「100」です。最小値は「10」、最大値は「999」です。 ウィンドウタイトルログにおける、画面キャプチャ採取時、および、PrintScreenキー操作やPrintScreenキー禁止時の画面キャプチャ採取時で共に有効となる設定です。 クライアント(CT)に保存する画面キャプチャデータ数が[CTに保存できる最大画像数]で指定した値を超えた場合、古い画像から削除されます。画面キャプチャデータがクライアント(CT)に多く保存される可能性がある場合は、必要に応じて[CTに保存できる最大画像数]を変更してください。

[端末動作設定]

項目名	説明
[ログオン禁止作動開始時間]	クライアント(CT)でログオン禁止が検出されてログオフまたはシャットダウンされるまでの間隔を選択します ・ [30秒後に禁止動作] ログオン禁止が検出されてから30秒後にログオフまたはシャットダウンします。 ・ [即時に禁止動作] ログオン禁止が検出されてから即時にログオフまたはシャットダウンします。 初期値は、[30秒後に禁止動作]です。
[プリンタ増減監視間隔]	クライアント(CT)側でのプリンタ増減監視間隔(秒)を指定します。 初期値(推奨値)は「15」です。最小値は「15」、最大値は「9999」です。 この値を増やすことでプリンタ増減を監視する間隔が長くなり、クライアント(CT)やネットワークの負荷が少なくなりますが、プリンタを新規に追加し、そのプリンタに印刷した場合の印刷ログが採取されない可能性が高くなります。特に問題がない限り、推奨値で設定してください。
[印刷ジョブ監視回数]	クライアント(CT)で印刷が行われた後に行われる印刷ジョブ監視の回数を指定します。初期値(推奨値)は「4」です。最小値は「3」、最大値は「9」です。(監視間隔は10秒です) 採取した印刷ログのドキュメント名や総ページ数が正しくない場合は、この値を増やしてください。
[印刷監視方式]	クライアント(CT)での印刷方式を選択します。 ・ [サーバ側で印刷監視方式を管理する]チェックなし 印刷方式は、管理サーバ、統合管理サーバ側での設定変更が有効となりません。 ・ [サーバ側で印刷監視方式を管理する]チェックあり 印刷方式は、管理サーバ、統合管理サーバ側での設定変更が有効となります。 ー [CTで設定されている全てのプリンタでの印刷を監視する(推奨)] 印刷方式は「CTで設定されている全てのプリンタの印刷を監視する(推奨)」となります。 ー [ローカルプリンタでの印刷のみを監視する] 印刷方式は「ローカルプリンタでの印刷のみ監視する」となります。

項目名		説明
		初期値は[サーバ側で印刷方式を管理する]チェックなしです。
[一括ログ送信の設定]	[ログ送信の間隔]	一括ログ送信を指定した場合、ログ送信間隔(秒)を指定します。 初期値(推奨値)は「300」です。最小値は「60」、最大値は「9999」です。 [ログ送信の間隔]の設定は、CTポリシーの[その他設定]タブで、以下のどちらかが設定されている場合に有効です。 ・ [操作ログ発生時点で即時に送信する]と[蓄積した操作ログは、接続後、一定件数ごとにまとめて送信する]が選択されている場合 ・ [操作ログを一定時間まとめてから送信する]と[蓄積した操作ログは、接続後、一定件数ごとにまとめて送信する]が選択されている場合
	[連続送信時の間隔]	一括ログ送信を指定した場合、ログ送信から次回のログ送信までの間隔(秒)を指定します。 初期値(推奨値)は「60」です。最小値は「30」、最大値は「9999」です。 [連続送信時の間隔]の設定は、CTポリシーの[その他設定]タブで、以下のどちらかが設定されている場合に有効です。 ・ [操作ログ発生時点で即時に送信する]と[蓄積した操作ログは、接続後、一定件数ごとにまとめて送信する]が選択されている場合 ・ [操作ログを一定時間まとめてから送信する]と[蓄積した操作ログは、接続後、一定件数ごとにまとめて送信する]が選択されている場合
	[一度に送信できる最大ログ数]	一括ログ送信を指定した場合、一度に送信する最大ログ数を指定します。 初期値(推奨値)は「1000」です。最小値は「100」、最大値は「5000」です。 [一度に送信できる最大ログ数]の設定は、CTポリシーの[その他設定]タブで、以下のどちらかが設定されている場合に有効です。 ・ [操作ログ発生時点で即時に送信する]と[蓄積した操作ログは、接続後、一定件数ごとにまとめて送信する]が選択されている場合 ・ [操作ログを一定時間まとめてから送信する]と[蓄積した操作ログは、接続後、一定件数ごとにまとめて送信する]が選択されている場合
	[通信タイムアウト]	一括ログ送信を指定した場合、管理サーバとの通信タイムアウト値(秒)を指定します。 初期値(推奨値)は「150」です。最小値は「30」、最大値は「300」です。 設定した値以内で通信が確立できなかった場合は、次回のログ送信時に再度ログを送信します。 [通信タイムアウト]の設定は、CTポリシーの[その他設定]タブで、以下のどちらかが設定されている場合に有効です。 ・ [操作ログ発生時点で即時に送信する]と[蓄積した操作ログは、接続後、一定件数ごとにまとめて送信する]が選択されている場合 ・ [操作ログを一定時間まとめてから送信する]と[蓄積した操作ログは、接続後、一定件数ごとにまとめて送信する]が選択されている場合
[オフラインログ送信の設定]	[ログごとの送信の間隔]	即時にログ送信を指定した場合、ログごとの送信間隔(ミリ秒)を指定します。 初期値(推奨値)は「50」です。最小値は「50」、最大値は「5000」です。 [ログごとの送信の間隔]の設定は、CTポリシーの[その他設定]タブで、以下のどちらかが設定されている場合に有効です。 ・ [操作ログ発生時点で即時に送信する]と[蓄積した操作ログは、接続直後に即時に送信する]が選択されている場合 ・ [操作ログ発生時点で即時に送信する]と[蓄積した操作ログは、接続後、一定件数ごとにまとめて送信する]が選択されている場合

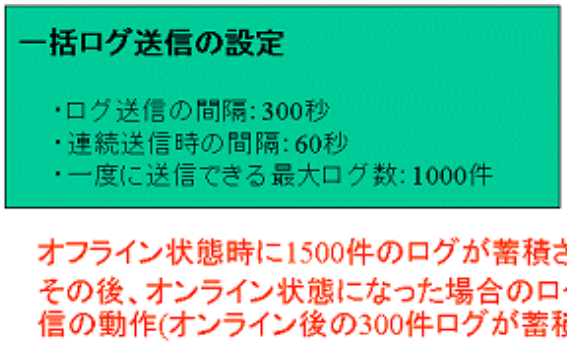
項目名		説明
	[サーバ接続監視間隔]	即時にログ送信を指定した場合、管理サーバとの通信確認間隔(秒)を指定します。 初期値(推奨値)は「60」です。最小値は「30」、最大値は「900」です。 [サーバ接続監視間隔]の設定は、CTポリシーの[その他設定]タブで、以下のどちらかが設定されている場合に有効です。 ・ [操作ログ発生時点で即時に送信する]と[蓄積した操作ログは、接続直後に即時に送信する]が選択されている場合 ・ [操作ログ発生時点で即時に送信する]と[蓄積した操作ログは、接続後、一定件数ごとにまとめて送信する]が選択されている場合

注意

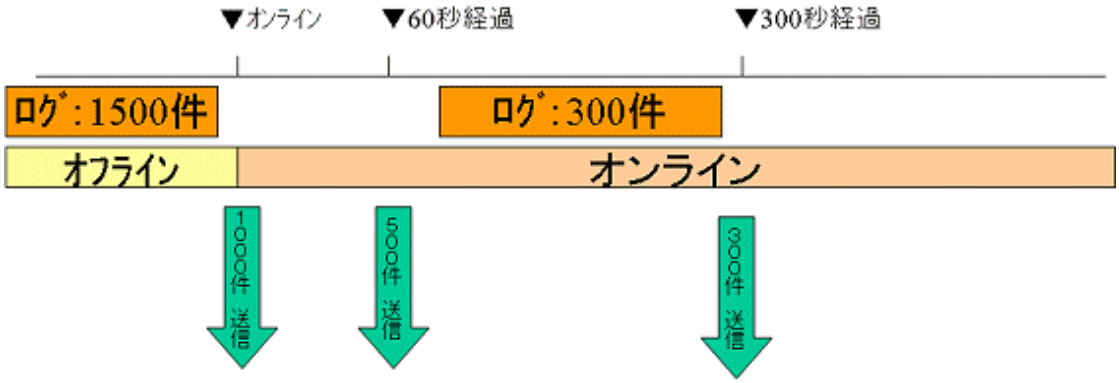
コマンドプロンプト操作ログのサーバへの送信について

コマンドプロンプト操作ログは、常に、採取後即時送信されます(本設定の影響を受けません)。

一括ログ送信の設定について、以下に説明します。



オフライン状態時に1500件のログが蓄積され、その後、オンライン状態になった場合のログ送信の動作(オンライン後の300件ログが蓄積)



オフラインからオンラインになった場合、蓄積されていた1500件のログのうち、まず1000件が送信されます。しかし、まだ500件残っているため、これらのログは、連続送信時の間隔で設定した60秒後に送信されます。
実際には、オンライン直後から新たなログが蓄積され続けています。その件数が300件だとした場合、500件送信してから300秒後に、これらの蓄積され続けているログが送信されます。

[原本ファイル保管条件設定]

項目名	説明
[ファイル持出しの原本合計最大サイズ]	クライアント(CT)に保存できるファイル持出しでの原本保管ファイルの合計最大サイズを指定します。この設定値以上の原本保管ファイルの保存はできません。 初期値は最大値です。 最小値は「1」(MB)、最大値は「700」(MB)です。
[1ファイルの最大サイズ]	原本ファイル保管時の1ファイル当たりの最大サイズを指定します。この設定値以上の原本保管ファイルの保存はできません。 初期値は最大値です。 最小値は「1」(MB)、最大値は「50」(MB)です。

セーフモードまたはネットワークが使えるセーフモードで採取されたログ

セーフモードまたはネットワークが使えるセーフモードで採取されたログは、次回の通常モードでの起動時に管理サーバに送信されます。

2.5 構成情報ツリーを作成する

管理対象全体の標準的なポリシーの設定後は、クライアント(CT)やユーザーをグループ化して管理するためのグループツリー(構成情報ツリー)を作成します。

構成情報ツリーの作成方法には、以下の3とおりがあります。

- Active Directoryから情報を取り込む
- Systemwalker Desktop Patrolから情報を取り込む
- 管理コンソールで作成する

2.5.1 Active Directoryから情報を取り込む

Active Directoryサーバから構成情報(CTグループ情報、CT情報、ユーザーグループ情報、ユーザー情報)を取り込んで、Systemwalker Desktop Keeperの構成情報ツリーを作成する方法を説明します。

Systemwalker Desktop KeeperがActive Directoryサーバから構成情報を取り込めるのは、Windows® 2000 Server、Windows Server® 2003、Windows Server® 2008でのActive Directory構築環境がネイティブモードの場合だけです。(ネイティブモードとは、Windows® 2000 Server以降で構築されるActive Directoryの標準動作モードです。)Windows NT® Serverで構築されるNT互換モードには対応しません。

構成情報を取り込めるActive Directoryサーバは、1サーバ(1ドメイン)だけです。Active Directory側でドメインの信頼関係を設定していてもその情報は取り込まず、Systemwalker Desktop Keeperが直接連携するサーバだけのデータを取り込みます。

Active Directoryサーバから構成情報を取り込むためには、連携対象のクライアントにSystemwalker Desktop KeeperのCTがインストールされている必要があります。また、サーバ設定ツールで、以下の情報が設定されている必要があります。

- システム設定
  Active Directoryサーバとのデータ連携時の条件を設定します。
- Active Directory連携設定
  Active Directoryサーバのコンピュータ名やドメイン名を設定します。
- サーバ情報設定
  統合管理サーバまたは管理サーバの情報を設定します。

構成情報の取り込み方法には、用途によって以下の2種類があります。

- サーバ設定ツールを使用する
  構成情報に変更が生じた契機で、システム管理者が、取り込みと更新を実行します。
- Active Directory連携コマンドを使用する
  タスクスケジューラにコマンドを登録して、定期的に取り込みと更新を実行します。

注意

Active Directory連携コマンドで、UNICODE 固有文字が含まれている情報を取り込む場合について

OU名、ユーザー名(UserPrincipalName)にUNICODE固有文字が含まれている場合、以下のように、Systemwalker Desktop Keeperのバージョンによって動作が異なります。

- V13.2.0の場合:
  該当文字を半角の「?」記号に変換して、Systemwalker Desktop Keeperのグループ、ユーザー情報として取り込みます。
- V13.3.0以降の場合:
  該当するOU名、ユーザー名(UserPrincipalName)は取り込みません。

このため、V13.2.0からV13.3.0以降に移行した場合、最初のActive Directory連携コマンドの実施により、すでに取り込まれているUNICODE固有文字を含むOU名およびユーザー名(「?」を含むOU名、ユーザー名)は、Systemwalker Desktop Keeperから削除されます。

ただし、Active Directoryのユーザー情報のうち、Systemwalker Desktop Keeperに取り込んでいる「使用者名(日本語名など)」、「従業員番号」、「役職名」、「部署名」、「部署コード」は、UNICODE固有文字を含んでいても、「?」記号に置換して取り込みます。

Active Directoryサーバの組織情報をもとに、ドメイングループ配下にグループが自動作成されるため、管理コンソールでCTグループツリーやユーザーグループツリーを作成する必要はありません。
ただし、Active Directory連携時でも、Localグループ配下にはグループを作成できます。LocalグループはActive Directoryとは連携しないので、配下の情報は、Active Directory連携を行っても変更されることはありません。Localグループ配下には、以下を登録できます。

- Active Directoryに登録されていないCT
- ユーザー(Active Directoryサーバに登録済のユーザーも登録できます)

Active Directoryサーバから構成情報を取り込む運用中に、Active Directory側でOU、ユーザー、コンピュータを削除すると、連携動作の実施後にはSystemwalker Desktop Keeper側の対応するグループ(CTグループ/ユーザーグループ)、ユーザー情報も無条件に削除されます。CTは、ルート直下のLocalグループ配下に配置されます。

また、Active Directory側でユーザーのアカウントを無効に変更した後にActive Directory連携を実施した場合は、Systemwalker Desktop Keeper側のユーザー情報(ユーザーポリシー)は削除されます。

3階層のシステム構成の場合、統合管理サーバでActive Directory連携を実行したときは、各管理サーバでもActive Directory連携が実行されます。
また、3階層のシステム構成では、Active Directory連携時のユーザーポリシーの管理方法は、統合管理サーバでの一元管理です。

ポイント

Citrix XenApp クライアントでの操作ログを効率よく検索するために

Citrix XenApp Server(TM)と連携して運用する場合、Citrix XenApp Serverを複数設置している環境にCitrix XenApp クライアントからログオンするとき、Citrix XenApp クライアントによって負荷分散されます。このため、どのCitrix XenApp Serverに接続されるか分かりません。したがって、操作ログを参照したり、検索したりする場合、すべてのCitrix XenApp Serverで採取されたログを参照しなければなりません。
検索を効率よく行うために、複数のCitrix XenApp Serverを、1つのCTグループとしてまとめ、そのグループ配下だけを検索すればよいように設定することを推奨します。
そのためには、Active Directoryに組織構造(OU)情報として、Citrix XenApp Serverを登録してください。

サーバ設定ツールを使用する

サーバ設定ツールを使用した取り込み手順を、以下に説明します。

Active Directoryサーバから取り込むユーザー情報の中に、以下の情報が含まれている場合、そのユーザー情報は取り込みません。

- 「ユーザー ログオン名(UserPrincipalName)」の@より前の文字列が、0バイト、または41バイト以上の場合

1. [設定]メニューの[Active Directory連携実施]を選択します。
   →連携を実行する確認画面が表示されます。

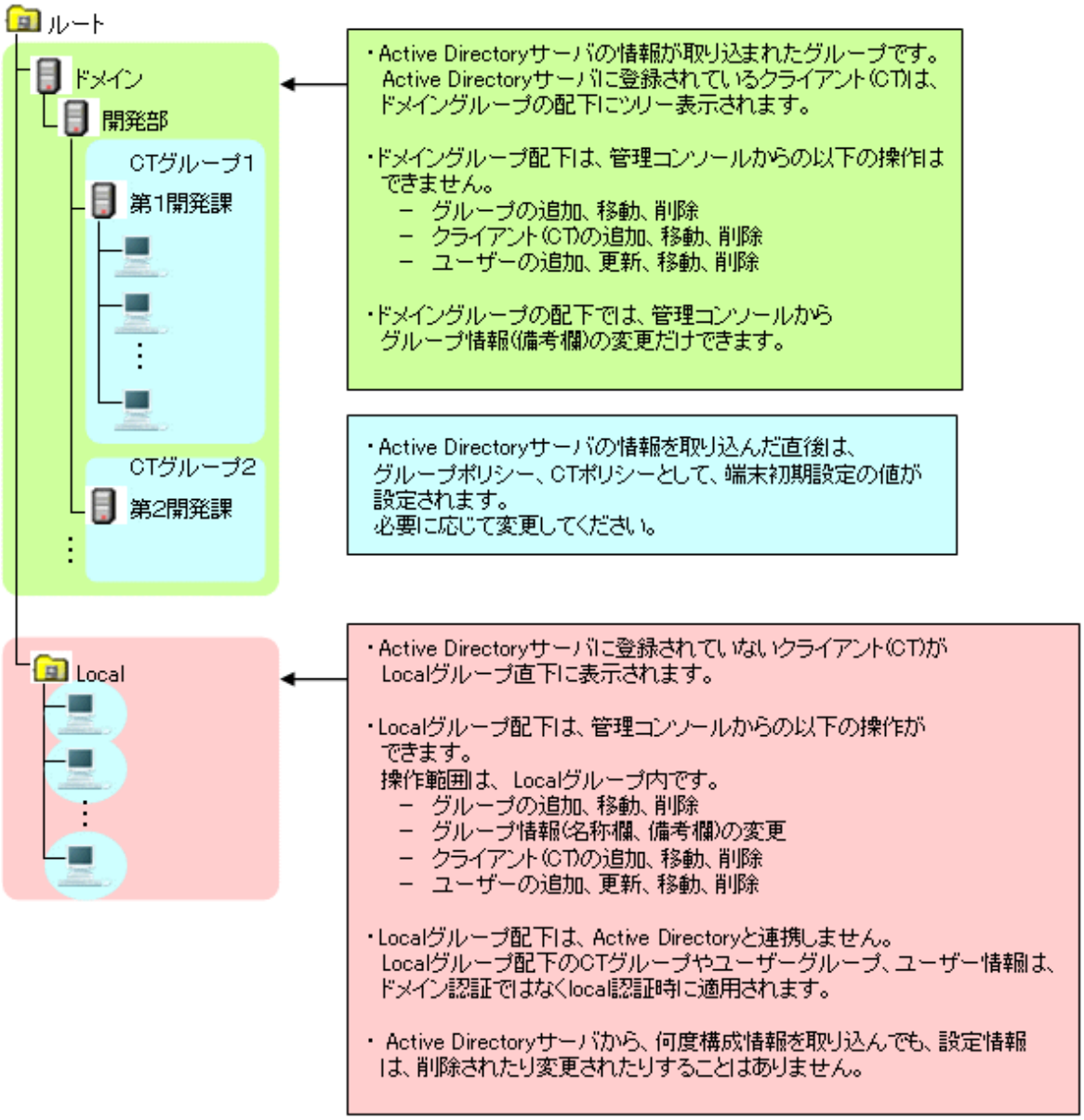
```
[STSY-SEL014] Active Directoryと通信を開始します。
Active Directory側よりユーザー情報、コンピュータ情報、階層構成情報を取得し、データベースを更新します。
処理に時間がかかる場合があります。通信を開始してよろしいですか？

                              [はい]          [いいえ]
```

2. Active Directory連携を実行する場合は、[はい]ボタンをクリックします。
   →Active Directoryからのデータ取り込み中を示すメッセージが表示されます。
   →データの取り込みが終了すると、終了メッセージが表示されます。
3. [OK]ボタンをクリックします。

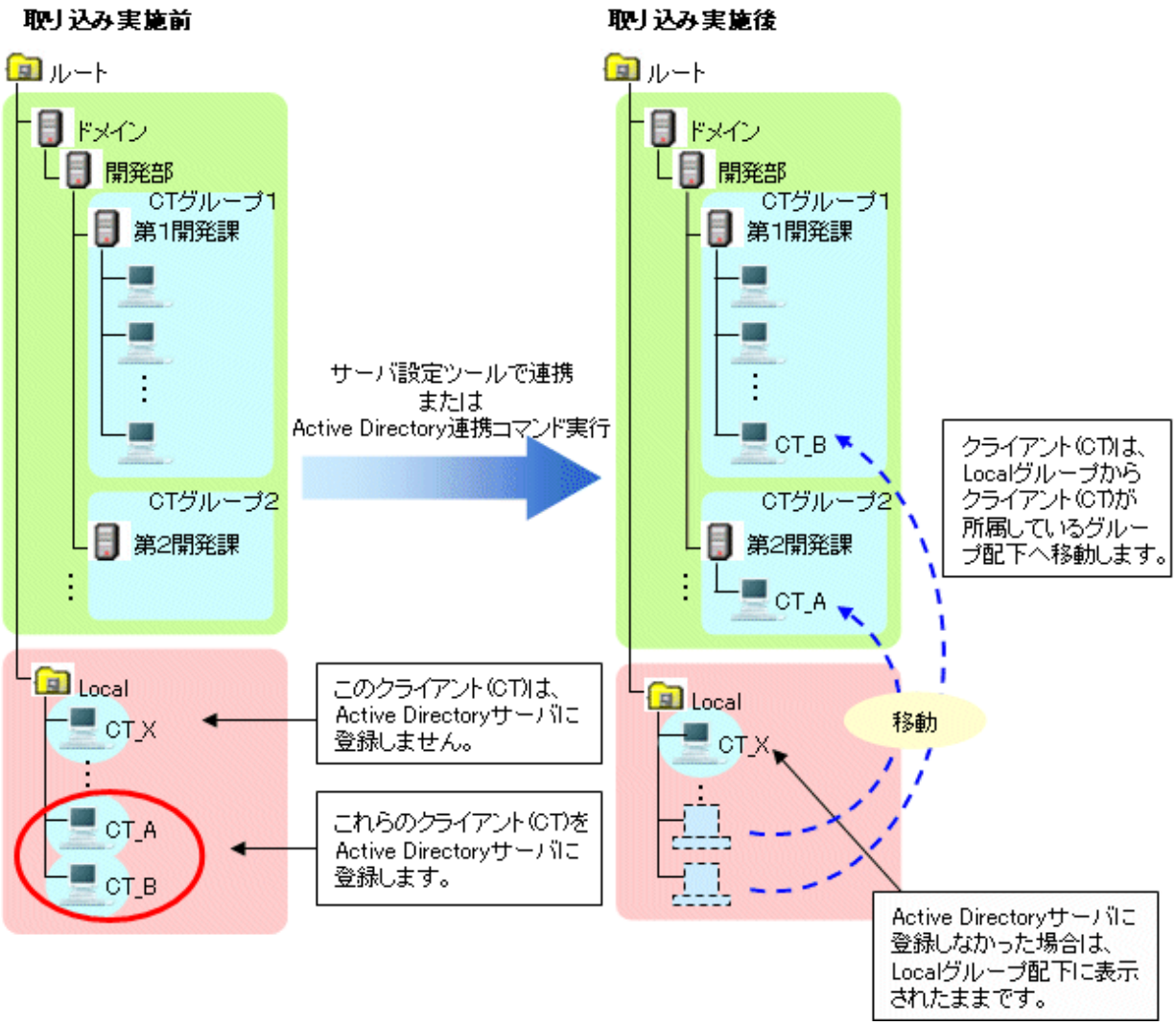
構成情報ツリーの表示

構成情報の取り込み直後は、管理コンソールを起動すると、以下のように構成情報ツリーが表示されます。



Localグループ配下に表示されているクライアント(CT)をActive Directoryサーバに登録した後、Systemwalker Desktop KeeperでActive Directory連携を実行すると、登録されたクライアント(CT)はグループ配下に移動します。

また、Active Directory連携を行い、ドメイングループで管理しているクライアント(CT)を管理コンソール上から削除する場合は、CTポリシー設定画面で、削除するクライアント(CT)を選択して[Active Directory連携対象としない]と設定した後、Active Directory連携を実施してください。その結果、クライアント(CT)はLocalグループ配下に移動しますので、その後、手動で、CT情報を削除してください。



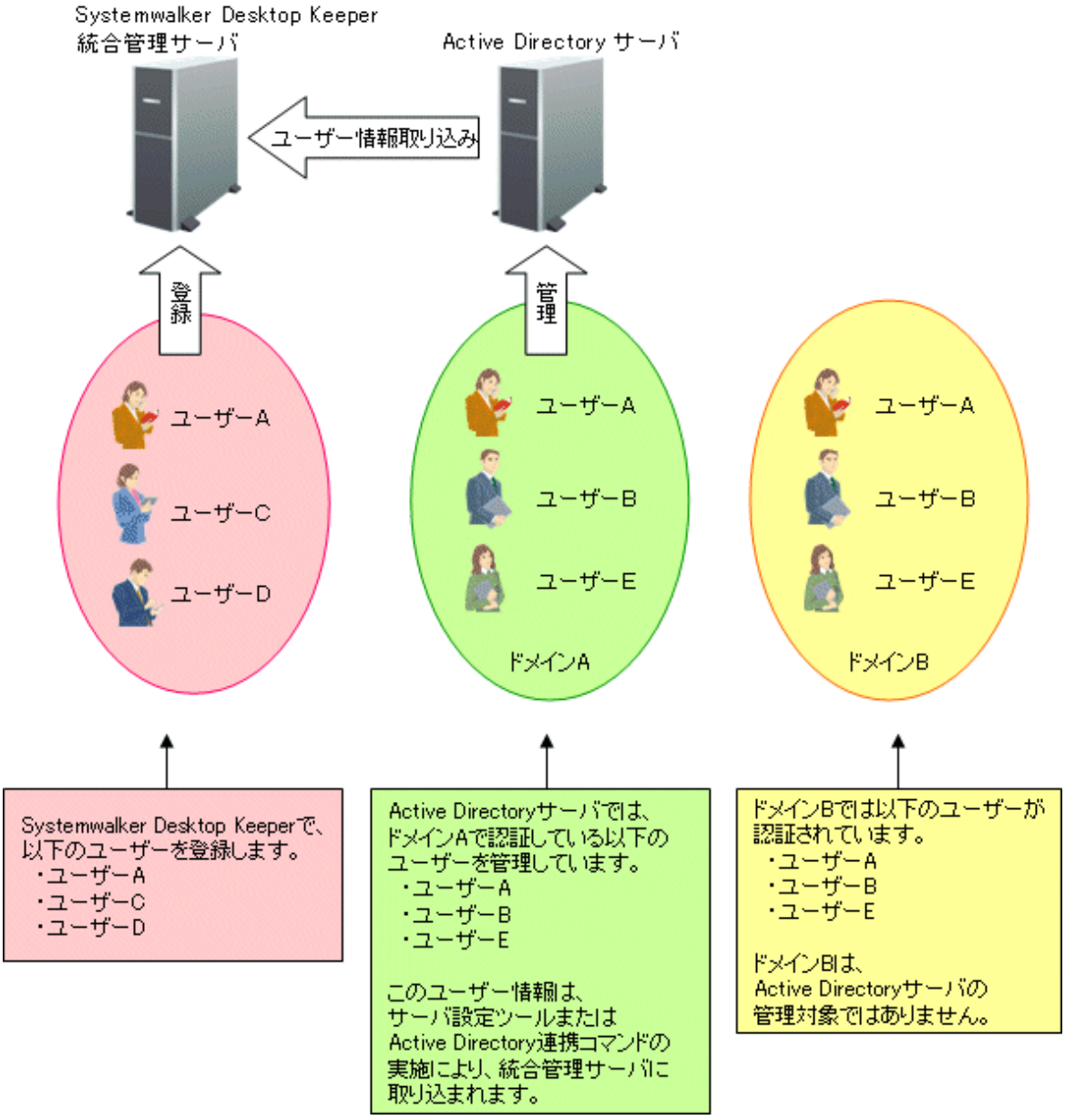
クライアント(CT)が新規に追加された場合も、まずLocalグループ配下に表示されます。このクライアント(CT)がActive Directoryサーバに登録された後、Systemwalker Desktop KeeperでActive Directory連携を実行すると、クライアント(CT)は、Localグループからクライアント(CT)が所属しているグループ配下へ移動します。

クライアント(CT)でのログイン先と適用されるポリシー

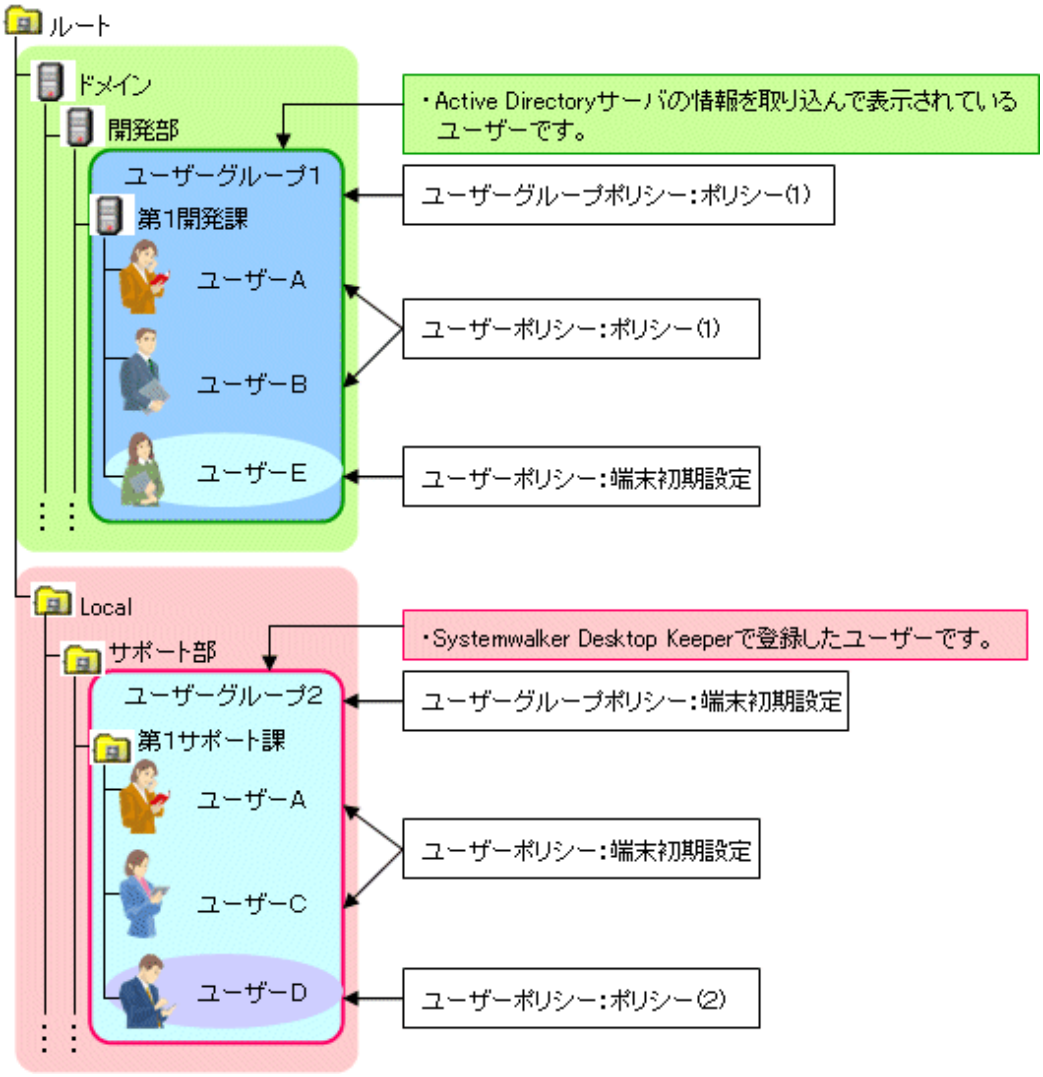
Active Directoryサーバから構成情報を取り込む運用では、ユーザーが自動的に作成されるため、ユーザーポリシーも使用します。
初回のActive Directory連携直後は、作成されたユーザーのユーザーポリシーには、端末初期設定の値が設定されます。ユーザーポリシーは、必要に応じて変更できます。
2回目以降のActive Directory連携を行った直後は、新規に追加されたユーザーのユーザーポリシーには、所属するユーザーグループ(OU)のグループポリシーが設定されます。

クライアント(CT)から、localにログインするか、連携しているドメインにログインするかによって、適用されるポリシーが異なります。クライアント(CT)でのログイン先と適用されるポリシーについて、説明します。

以下の環境で運用されているとします。



Active Directory連携を実施すると、Systemwalker Desktop Keeperの管理コンソールには、以下のように表示されます。



― Active Directory連携で指定したドメインにログインした場合
→ドメインのユーザーポリシーが適用されます。

上記の例では、ユーザーA、B、Eが、以下のドメインのユーザーポリシーで操作できます。

- ユーザーA：ポリシー(1)
- ユーザーB：ポリシー(1)
- ユーザーE：端末初期設定

― ローカルコンピュータにログインした場合(Localにも同名のユーザーがある場合)
→Localのユーザーポリシーが適用されます。

上記の例では、ユーザーAが、端末初期設定のユーザーポリシーで操作できます。

― ローカルコンピュータにログインした場合(Localには同名のユーザーがない場合)
→CTポリシーが適用されます。

上記の例では、ユーザーB、Eが、CTポリシーで操作できます。

― Active Directory連携で指定していないドメインにログインした場合(Localに同名のユーザーがある場合)
→Localのユーザーポリシーが適用されます。

上記の例では、ユーザーAがドメインBにログインした場合で、端末初期設定のユーザーポリシーで操作できます。

ー Active Directory連携で指定していないドメインにログインした場合(Localには同名のユーザーがない場合)
→CTポリシーが適用されます。

上記の例では、ユーザーB、EがドメインBにログインした場合で、CTポリシーで操作できます。

Active Directory連携コマンドを使用する

Active Directory連携コマンドを使用した取り込み手順を、以下に説明します。

コマンド実行前に“Active Directory連携組織単位対象リスト”を設定しておくと、連携対象とする組織を限定して取り込むことができます。本リストは、指定された場所に格納します(コマンドのオプションに指定する必要はありません)。

Active Directory連携コマンドの詳細は、“Systemwalker Desktop Keeper リファレンスマニュアル”の“DTKADCON.EXE(Active Directoryとの連携)”を参照してください。

1. 管理サーバに、ローカルPCのAdministratorsグループ、またはDomain Adminsグループに所属するユーザー名でログオンします。
2. タスクスケジューラを起動し、以下を登録します。
   ー Active Directory連携コマンド
   ー コマンドを実行するタイミング(日付、時間帯など)

   バックアップツール、リストアツール、およびバックアップコマンドが起動しない時間帯を指定します。
   また、管理コンソールおよびログビューア利用者の少ない時間帯を指定します。
3. タスクスケジューラが正常動作するか確認します。

コマンド実行による、管理コンソールでの構成情報ツリーの遷移は、“サーバ設定ツールを使用する”の“構成情報ツリーの表示”と同じです。

2.5.2 Systemwalker Desktop Patrolから情報を取り込む

Systemwalker Desktop Patrolの構成情報を取り込んで、Systemwalker Desktop Keeperの構成情報ツリーを作成する方法を説明します。

Systemwalker Desktop Patrolとの連携では、Systemwalker Desktop Patrolで管理している構成情報を基準とします。まずSystemwalker Desktop Patrolから情報を取り込み、それに対して、Systemwalker Desktop Keeper固有の情報をツリーに反映して管理します。

Systemwalker Desktop Patrolからの構成情報の取り込みは、Systemwalker Desktop Patrolの環境が完全に構築されてからSystemwalker Desktop Keeperを導入し、CTのインストールが完了した後、実施します。

Systemwalker Desktop Patrol構成情報取り込みコマンドを使用する

Systemwalker Desktop Patrol構成情報取り込みコマンドを使用して、構成情報を取り込む方法を説明します。

初回の構成情報取り込み時は、グループを新規に作成し、すべての構成情報を取り込みます。
2回目以降の取り込み時は、前回からの差分だけ取り込みます。

Systemwalker Desktop Patrol構成情報取り込みコマンドの実行中は、管理コンソールおよびログビューアからの操作は行えません。
構成情報取り込みの開始、終了の情報は、イベントログに出力されます。

初回の構成情報の取り込み方は、以下の方法を選択できます。

- 管理者が手動でコマンドを実行して取り込む。
- タスクスケジューラにコマンドを登録して、管理コンソールやログビューアの使用者がいない時間に実行する。

2回目以降の構成情報の取り込み方は、以下の方法を選択できます。

- システム構成に変更が生じたときだけ、情報を取り込む。

・ タスクスケジューラにコマンドを登録して、定期的に更新する。

取り込み手順

1. Systemwalker Desktop Patrolで構成情報を出力する

取り込み情報が記録されている構成情報ファイル(CSVファイル)を、Systemwalker Desktop Patrolで準備します。
この構成情報ファイルには、CTのグループ情報、およびCTがどこに所属するか(位置情報)が記録されています。
構成情報の出力方法は、Systemwalker Desktop Patrolのマニュアルを参照してください。

※ 作成した構成情報ファイルは、編集しないでください。

2. 構成情報ファイルをコピーする

Systemwalker Desktop Patrolで作成した構成情報ファイルを、Systemwalker Desktop Keeperの管理サーバにコピーします。
3階層のシステム構成で、統合管理サーバの直下に管理しているクライアント(CT)が存在する場合は、統合管理サーバにも、構成情報ファイルをコピーします。

3. Systemwalker Desktop Patrol構成情報取り込みコマンドを実行する

【コマンドの実行場所】

構成情報ファイルをコピーしたサーバで、コマンドを実行します。
ただし、実行順序については、3階層のシステム構成で、統合管理サーバに構成情報ファイルをコピーした場合は、管理サーバでコマンドを実行してから、統合管理サーバでコマンドを実行してください。

【コマンドを手動で実行する場合】

1. コマンドを実行するサーバに、ローカルPCのAdministratorsグループ、またはDomain Adminsグループに所属するユーザー名でログオンします。
2. 以下が動作していないことを確認します。

   ・バックアップツール
   ・バックアップコマンド
   ・リストアツール
   ・Active Directoryとの連携コマンド
3. コマンドプロンプトを起動します。
4. Systemwalker Desktop Patrol構成情報取り込みコマンドを実行します。
   コマンド実行時のディレクトリを意識する必要はありません。
   コマンドの実行結果情報をすべて参照する場合は、コマンドのオプションに実行ログファイルを指定します。
   Systemwalker Desktop Patrol構成情報取り込みコマンドの実行例は、“Systemwalker Desktop Keeper リファレンスマニュアル”の“DTKIMPDP.EXE(Systemwalker Desktop Patrol構成情報取り込み)”を参照してください。
5. 実行結果を画面で確認します。
   または、環境変数の%ERRORLEVEL%の値を取得して確認します。
   %ERRORLEVEL%の値は、Systemwalker Desktop Patrol構成情報取り込みコマンドの復帰値です。値とその意味については、“Systemwalker Desktop Keeper リファレンスマニュアル”の“DTKIMPDP.EXE(Systemwalker Desktop Patrol構成情報取り込み)”を参照してください。

【タスクスケジューラにコマンドを登録して実行する場合】

1. コマンドを実行するサーバに、ローカルPCのAdministratorsグループ、またはDomain Adminsグループに所属するユーザー名でログオンします。
2. タスクスケジューラを起動し、以下を登録します。

   ・Systemwalker Desktop Patrol構成情報取り込みコマンド

   コマンドのオプションに実行ログファイルを指定します。
   3階層の管理サーバの場合は、コマンドのオプションにリトライ回数を設定します(統合管理サーバと、データの整合性を確認する処理が動作している場合もあるため)。
   1リトライあたりの待ち合わせ時間は、60秒です。リトライ回数は10程度を指定します(最大10分間待ち合わせを行います)。

オプションの指定方法は、“Systemwalker Desktop Keeper リファレンスマニュアル”の“Systemwalker Desktop Patrol構成情報取り込みコマンド”を参照してください。

・コマンドを実行するタイミング(日付、時間帯など)

バックアップツール、リストアツール、およびバックアップコマンドが起動しない時間帯を指定します。
また、管理コンソールおよびログビューア利用者の少ない時間帯を指定します。

3. タスクスケジューラに表示されるジョブの実行結果を確認します。
4. コマンド終了後、実行ログファイルを参照し、正常終了していることを確認します(実行ログは追記されています)。

【コマンド実行後の状態】

- グループが作成された場合

  ルート配下にグループが作成された場合は、グループポリシーとして端末初期設定の値が設定されます。
  既存のグループの配下にグループが作成された場合は、親グループのグループポリシーが設定されます。

- グループが更新された場合

  グループ名称の更新や、グループの階層位置の移動があっても、グループポリシーや部門管理者の登録情報は引き継がれます。

- グループが削除された場合

  削除されたグループのグループポリシーや、部門管理者情報も同時に削除されます。
  削除グループ配下に、構成情報取り込み後にSystemwalker Desktop Keeperで作成したグループ、クライアント(CT)、またはユーザーが存在していた場合は、これらはルート配下に移動します。

- グループ配下にクライアント(CT)が存在しない場合

  グループだけが表示されます。不要な場合は、管理コンソールの[ツリー設定]メニューから[空のグループは表示しない]を選択してください。

- CTの移動について

  構成情報取り込み後、構成情報ファイルの内容に合わせてCTが移動します。

  構成情報ファイルにデータがないCTについては、移動しません(ルート直下に表示されたままです)。

  構成情報ファイルによりクライアント(CT)を移動できるのは、Systemwalker Desktop Patrol、Systemwalker Desktop KeeperともにV13.0.0以降のCTを導入しているPCの場合です。

4. 必要に応じて構成情報ツリーを変更する

Systemwalker Desktop Keeperでの管理情報に合わせて、管理コンソールでグループの作成、変名、移動、削除などを行います。

システム管理者および部門管理者は、取り込まれたグループに対して、グループ名の更新、移動、削除、グループポリシーの設定、および部門管理者の設定(システム管理者だけ可)ができます。部門管理者の割り当てについては、“2.6 部門管理者を割り当てる”を参照してください。

Systemwalker Desktop Keeperの管理コンソールで実施したグループ名の更新、移動、削除については、次回の構成情報取り込みによって無効となり、再度取り込んだ構成情報に修正されます。
グループポリシーや部門管理者の登録情報は、再取り込み後も引き継がれます。
グループを削除した場合は、次回の構成情報取り込みによって該当グループが再び取り込まれても、グループポリシーと部門管理者情報は削除されていますので、再設定が必要です。

また、システム管理者および部門管理者は、取り込まれたグループの配下に、新規にグループの作成、更新、および削除ができます。
取り込まれたグループの配下に作成したグループは、次回の構成情報取り込み時に上位グループが存在しなかった場合、ルート直下に移動します。

クライアント(CT)についても、グループと同様の操作を実施できます。

次回以降、継続的にSystemwalker Desktop Patrolと連携して構成情報を取り込み、Systemwalker Desktop PatrolとSystemwalker Desktop Keeperのフォルダ構成を同期して運用する場合は、以下の作業を実施してください。
Systemwalker Desktop Keeperだけで運用するグループに対しては、以降の作業は不要です。

1. 管理コンソールでの変更情報をSystemwalker Desktop Patrolに反映する

   管理コンソールで実施したグループ名の更新、移動、削除については、次回の構成情報取り込みによって無効になるため、“4. 必要に応じて構成情報ツリーを変更する”で実施した変更内容を、Systemwalker Desktop Patrolに手動で反映します。

2. Systemwalker Desktop Keeperの管理コンソールで作成したグループを削除します。削除方法は、“削除する”を参照してください。

3. Systemwalker Desktop Patrolで構成情報を出力し、Systemwalker Desktop Keeperに取り込む

   Systemwalker Desktop Keeperでの変更内容が反映された構成情報ファイルを利用して、“1. Systemwalker Desktop Patrolで構成情報を出力する”から“4. 必要に応じて構成情報ツリーを変更する”を繰り返して運用します。

参考

【Systemwalker Desktop Patrol構成情報取り込み対応ファイルを使用するには】

Systemwalker Desktop Patrolからの構成情報取り込み時に、ユーザーグループツリーも作成する場合に必要なファイルです。

本ファイルでは、PC(コンピュータ名)とユーザー名の対応情報を設定します。
Systemwalker Desktop Patrol構成情報取り込み対応ファイルの作成方法は、“Systemwalker Desktop Keeper リファレンスマニュアル”の“Systemwalker Desktop Patrol構成情報取り込み対応ファイル”を参照してください。

使用するファイルと、ファイルを格納するサーバの関係は以下のとおりです。

ー 2階層のシステム構成の場合
管理サーバに、対応ファイルと構成情報ファイルを格納します。

ー 3階層のシステム構成の場合

- ユーザー情報を一元管理する場合

  対応ファイル:統合管理サーバに格納します(ユーザー情報の取り込みは、統合管理サーバで実施するためです)。

  構成情報ファイル:統合管理サーバと管理サーバに格納します(統合管理サーバ直下に管理するクライアント(CT)が存在しなくても、統合管理サーバにも格納する必要があります)。

- ユーザー情報を各管理サーバで管理する場合

  対応ファイル:管理サーバに格納します(ユーザー情報の取り込みは、各管理サーバで実施するためです)。

  構成情報ファイル:管理サーバに格納します。ただし、統合管理サーバ直下に管理するクライアント(CT)が存在する場合は、統合管理サーバにも格納します。

Systemwalker Desktop Patrol構成情報取り込みコマンドの実行時は、/U /Fオプションを付けて実行してください。詳細は、“Systemwalker Desktop Keeper リファレンスマニュアル”の“DTKIMPDP.EXE(Systemwalker Desktop Patrol構成情報取り込み)”を参照してください。

【廃棄フォルダ情報ファイルを使用するには】

Systemwalker Desktop Patrolからの構成情報取り込み時に、Systemwalker Desktop Patrol側で廃棄処理されたPC情報を構成情報ツリーに反映する場合に必要なファイルです。
廃棄フォルダ情報ファイルの作成方法は、“Systemwalker Desktop Keeper リファレンスマニュアル”の“廃棄フォルダ情報ファイル”を参照してください。

Systemwalker Desktop Patrol構成情報取り込みコマンドの実行前に、以下の作業が完了している必要があります。

ー 削除されたCTのためのグループ作成

Systemwalker Desktop Patrolで削除されたPCを、Systemwalker Desktop Keeperの構成情報ツリーにグルーピングして表示するために、Systemwalker Desktop Keeperの構成情報ツリー上に、削除されたPC専用のグループを作成します。
グループ名は一意である必要があります。

Systemwalker Desktop Patrol構成情報取り込みコマンドのオプションにここで作成したグループ名を指定して実行すると、削除されたPCが、Systemwalker Desktop Keeperの構成情報ツリーのグループ配下に表示されます。

ー 廃棄フォルダ情報ファイルの作成

本ファイルは、Systemwalker Desktop Patrolで廃棄処理されたPC情報を、差分取り込み時にSystemwalker Desktop Keeperの構成情報ツリーに表示する場合に作成します。
Systemwalker Desktop Patrolで廃棄処理されたPCと、そのPCが所属するグループを設定します。
廃棄フォルダ情報ファイルの作成方法は、“Systemwalker Desktop Keeper リファレンスマニュアル”の“廃棄フォルダ情報ファイル”を参照してください。

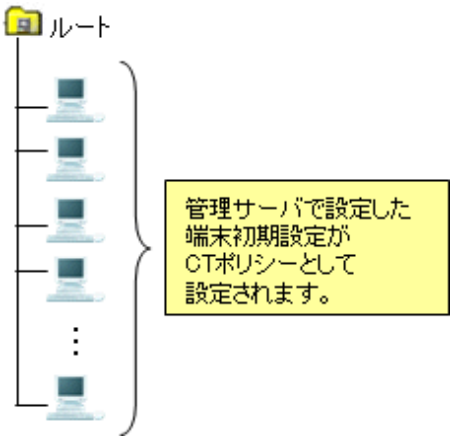
廃棄フォルダ情報ファイルは、管理サーバに格納します。ただし、統合管理サーバ直下に管理するクライアント(CT)が存在する場合は、統合管理サーバにも格納します。

Systemwalker Desktop Patrol構成情報取り込みコマンドの実行時は、/Eオプションを付けて実行してください。詳細は、“Systemwalker Desktop Keeper リファレンスマニュアル”の“DTKIMPDP.EXE（Systemwalker Desktop Patrol構成情報取り込み）”を参照してください。

構成情報ツリーでの表示

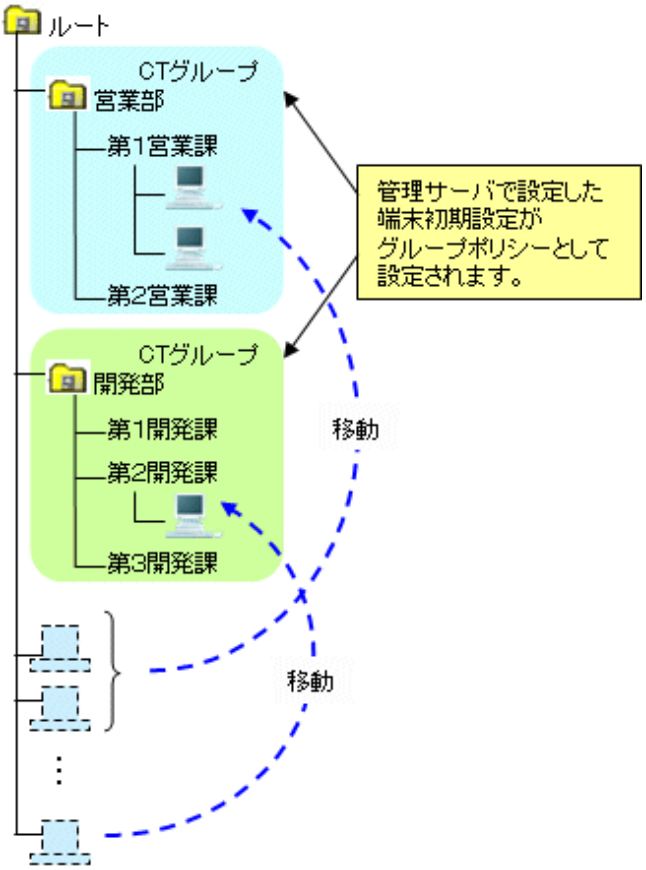
1. Systemwalker Desktop KeeperのCTをインストールします。

   →管理サーバとクライアント(CT)が通信すると、ルート配下にクライアント(CT)が表示されます。
   このとき、クライアント(CT)には、端末初期設定がCTポリシーとして設定されます。



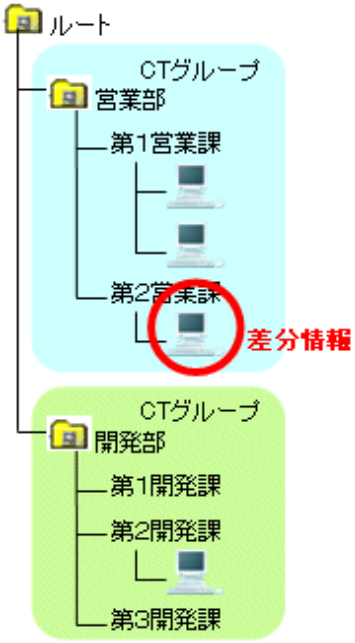
2. Systemwalker Desktop Patrol構成情報取り込みコマンドを実行します(初回取り込み)。

   →クライアント(CT)がツリーに割り当てられます。



3. Systemwalker Desktop Patrol構成情報取り込みコマンドを実行します(2回目以降の取り込み)。

   →差分が発生した情報だけを取り込みます。



管理コンソールの[他システム連携]を使用する

管理コンソールのメニューから、構成情報を取り込む方法を説明します。

注意

[他システム連携]を利用した構成情報の取り込みは、使用方法が限定されます

【使用できる条件が限られます】

管理コンソールの[他システム連携]は、新規に構成情報を取り込む場合で、初回の取り込みにしか使用できません。

【Systemwalker Desktop Patrol構成情報取り込みコマンドと併用しないでください】

管理コンソールの[他システム連携]を使用して構成情報を作成後、Systemwalker Desktop Patrol構成情報取り込みコマンドを使用した場合、[他システム連携]で取り込んだ構成情報が残されたまま、新たに構成情報を取り込んでグループを追加作成します。
このため、情報が重複し、管理しにくくなりますので、併用しないでください。

【[他システム連携]で取り込んだ既存の管理情報は削除されます】

管理コンソールの[他システム連携]を使用して、2回目以降の構成情報を取り込むと、[他システム連携]によって取り込まれた既存のすべての管理情報(グループ情報、ポリシー、部門管理者など)が削除され、Systemwalker Desktop Patrolの情報で新規に構築されます。
したがって、取り込み後は、グループポリシーや部門管理者を再設定しなければなりません。

3階層のシステム構成の場合は、統合管理サーバに接続されている管理コンソールで、構成情報を取り込んでください。この場合、統合管理サーバ、下位の管理サーバ共、すべて、同じグループ構成となります。

構成情報の取り込み時に、以下のいずれかの条件を満たすクライアント(CT)は、ルート配下に表示されます。これ以外のクライアント(CT)は、構成情報にしたがって各グループ配下に表示されます。

- Systemwalker Desktop KeeperのCTのバージョンがV12である
- クライアント(CT)にSystemwalker Desktop Patrolが導入されていない

構成情報の取り込み後は、グループポリシーとして、端末初期設定の値が設定されます。3階層のシステム構成の場合は、各管理サーバ配下のCTグループのポリシーには、その管理サーバの端末初期設定の値が設定されます。

CTグループ情報とCT情報を対応させて取り込むためには、Systemwalker Desktop Keeperの管理コンソール画面のCTリストで、取り込み対象のPCの[DTPID]に情報が表示されている必要があります。([DTPID]に情報が取り込まれるのは、対象PCにSystemwalker Desktop KeeperとSystemwalker Desktop Patrolを導入後の、次回のWindowsを起動したあとです。)
取り込み対象のPCの[DTPID]に情報が表示されていない状態で、Systemwalker Desktop Patrolの構成情報を取り込んだ場合は、CTグループ情報は取り込まれません。クライアント(CT)は、ルート直下に登録されます。

クライアント(CT)が1台も登録されていないCTグループは、取り込み対象になりません。

「削除したCT」グループに所属するクライアント(CT)は、連携対象外です。

Systemwalker Desktop Patrolでのグループ名が半角40文字を超えている場合は、先頭から半角40文字分までをグループ名称としてSystemwalker Desktop Keeperに取り込みます。

以下に取り込み手順を説明します。

1. Systemwalker Desktop Patrolで構成情報を出力します。

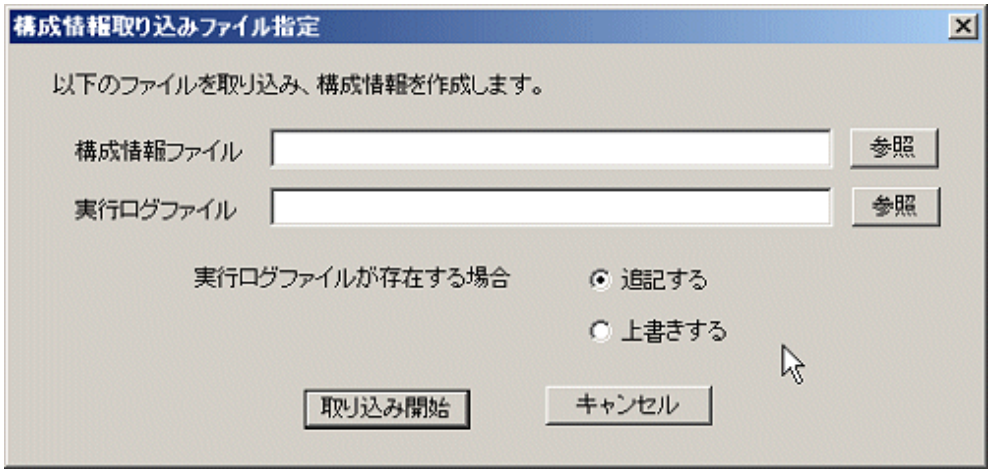
   方法についてはSystemwalker Desktop Patrolのマニュアルを参照してください。

   ※ 作成した構成情報ファイルは、編集しないでください。

2. [管理コンソール]画面を起動します。

3. [他システム連携]メニューから[Systemwalker Desktop Patrol連携]-[構成情報取り込み]を選択します。

   →[構成情報取り込みファイル指定]画面が表示されます。



4. 以下の情報を入力したあとに、[取り込み開始]ボタンをクリックします。

項目名	説明
[構成情報ファイル]	取り込むファイルを指定します。指定方法は、以下のとおりです。 ・ フルパスでファイル名を入力する 取り込むファイルまでのパスをフルパスで入力します。 ・ [参照]ボタンから選択する [取り込みファイルの指定]画面が表示されるので、取り込むファイルを選択し[開く]ボタンをクリックします。 指定できるフルパスの長さは、半角で218文字まで入力できます。ただし、以下の記号はファイル名として使用できません。 使用できない記号:「¥」「/」「:」「*」「?」「"」「<」「>」「|」
[実行ログファイル]	取り込み実行結果を出力するファイルを指定します。拡張子は自動で付与されないため、”KEKKA.TXT“のように後から判別しやすい拡張子を指定してください。指定方法は、以下のとおりです。 ・ フルパスでファイル名を入力する 入力欄に出力する実行ログファイルまでのパスをフルパスで入力します。 ・ [参照]ボタンから入力する [出力ファイルの指定]画面が表示されるので、出力する構成情報ファイルの場所を選択し、ファイル名を入力したあとに、[開く]ボタンをクリックします。 指定できるフルパスの長さは、半角で218文字まで入力できます。ただし、以下の記号はファイル名として使用できません。 使用できない記号:「¥」「/」「:」「*」「?」「"」「<」「>」「|」
[実行ログファイルが存在する場合]	実行ログファイルが[実行ログファイル]で指定した場所に存在する場合の処理を選択します。 ・ [追記する] 前回の実行ログの後に追記します。 ・ [上書きする] 前回の実行ログを上書きします。

Systemwalker Desktop Patrolへ構成情報を出力することもできます

【出力条件】

以下の条件をすべて満たす場合に、Systemwalker Desktop Keeperの構成情報を、構成情報ファイルに出力できます。

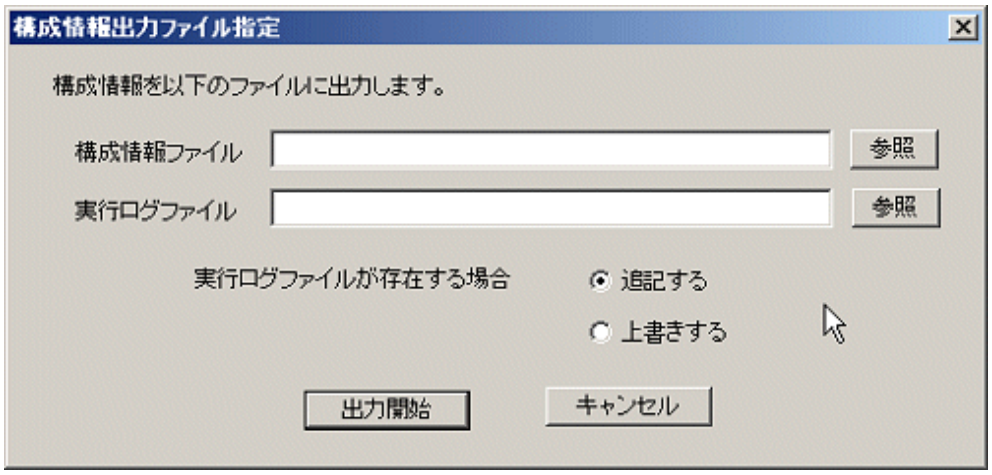
－ Systemwalker Desktop Keeperのクライアント(CT)のバージョンが、V13.0.0以降の場合

－ 管理コンソールのCTリストの[DTPID]に情報がある場合

「削除したCT」グループに所属するクライアント(CT)は、連携対象外です。

以下に、情報を出力する手順を説明します。

1. [管理コンソール]画面を起動します。
2. [他システム連携]メニューから[Systemwalker Desktop Patrol連携]-[構成情報出力]を選択します。
   →[構成情報出力ファイル指定]画面が表示されます。



3. 以下の情報を入力したあとに、[出力開始]ボタンをクリックします。

項目名	説明
[構成情報ファイル]	構成情報を出力するファイルの保存先を指定します。 構成情報出力先に同じ名前のファイルが存在していた場合は出力できません。 拡張子は自動で付与されないため、“FILEA.CSV”のように判別しやすい拡張子を指定してください。指定方法は、以下のとおりです。 ・ フルパスでファイル名を入力する 出力する構成情報ファイルまでのパスをフルパスで入力します。 ・ [参照]ボタンから選択する [出力ファイルの指定]画面が表示されるので、出力する構成情報ファイルの場所を選択し、ファイル名を入力したあとに、[開く]ボタンをクリックします。 指定できるフルパスの長さは、半角で218文字まで入力できます。ただし、以下の記号はファイル名として使用できません。 使用できない記号:「¥」「/」「:」「*」「?」「"」「<」「>」「|」
[実行ログファイル]	取り込み実行結果を出力するファイルを指定します。拡張子は自動で付与されないため、“KEKKA.LOG”のように判別しやすい拡張子を指定してください。指定方法は、以下のとおりです。 ・ フルパスでファイル名を入力する 入力欄に出力する実行ログファイルまでのパスをフルパスで入力します。 ・ [参照]ボタンから入力する [出力ファイルの指定]画面が表示されるので、出力する構成情報ファイルの場所を選択し、ファイル名を入力したあとに、[開く]ボタンをクリックします。

項目名	説明
	指定できるフルパスの長さは、半角で218文字まで入力できます。ただし、以下の記号はファイル名として使用できません。 使用できない記号:「¥」「/」「:」「*」「?」「"」「<」「>」「|」
[実行ログファイルが存在する場合]	実行ログファイルが[実行ログファイル]で指定した場所に存在する場合の処理を選択します。 ・ [追記する] 前回の実行ログの後に追記します。 ・ [上書きする] 前回の実行ログを上書きします。

4. Systemwalker Desktop Patrolで構成情報を取り込みます。

   取り込み方法についてはSystemwalker Desktop Patrolのマニュアルを参照してください。

2.5.3 管理コンソールで作成する

3階層のシステム構成の場合、構成情報ツリーを管理コンソールで手動で作成するときは、各管理サーバで実施してください。

CTグループを作成する

ポイント

Citrix XenApp クライアントでの操作ログを効率よく検索するために

Citrix XenApp Server(TM)と連携して運用する場合、Citrix XenApp Serverを複数設置している環境にCitrix XenApp クライアントからログオンするとき、Citrix XenApp クライアントによって負荷分散されます。このため、どのCitrix XenApp Serverに接続されるか分かりません。したがって、操作ログを参照したり、検索したりする場合、すべてのCitrix XenApp Serverで採取されたログを参照しなければなりません。
検索を効率よく行うために、複数のCitrix XenApp Serverを、1つのCTグループとしてまとめ、そのグループ配下だけを検索すればよいように設定することを推奨します。
そのためには、管理コンソールでCTグループとしてCitrix XenApp Serverを設定してください。

CTグループツリーに表示するCTグループの構築について説明します。

作成する

CTグループツリーの表示がグレーアウトされ、グループを作成できない場合は、[ツリー設定]メニューで[空のグループは表示しない]が設定されています。この設定を解除してください。

CTグループを作成すると、CTグループ配下のCTにCTポリシーを一括で設定できます。

CTグループは、グループ名に使用されている文字コードの昇順で表示されます。

CTグループを作成する手順は、以下のとおりです。

1. [管理コンソール]画面を起動します。
2. CTグループツリーから、グループを作成する上位のグループを選択します。

3. [ファイル]メニューから[CTグループ作成]を選択します。

   →[CTグループ作成]画面が表示されます。

4. 以下の情報を入力し、[追加]ボタンをクリックします。

   - [サーバ名]
   - [グループ名]

     半角で40文字(全角で20文字)までの英数字、漢字、ひらがな、およびカタカナが入力できます。

   →CTグループツリーに追加したグループが表示されます。

5. [ツリー設定]メニューから[CTグループ構成反映]を選択します。

   →作成したCTグループがデータベースに反映されます。

   [CTグループ構成反映]を実行しない場合、[ポリシー最新表示]、[次回起動時に更新する]、および[即時更新を行う]ボタンがグレーアウトされた状態になり、[CTグループ構成反映]を促すメッセージが表示されます。

   作成したCTグループがデータベースに反映された直後は、このCTグループのポリシーは、必ず以下のように設定されます。必要に応じてポリシーの変更を行ってください。ポリシーの変更については、“3.2.1 CTグループポリシーを変更する”を参照してください。

   - ルート配下にCTグループを作成した場合

     CTグループを作成した統合管理サーバまたは管理サーバ上の[端末初期設定]画面で設定されたポリシーが反映されます。

   - ほかのグループ配下にCTグループを作成した場合

     作成したCTグループの上位のCTグループに設定されているポリシーが反映されます。

移動する

CTグループツリーに作成されているCTグループは、同一サーバ配下であれば、ほかのCTグループ配下に移動したり、サーバの直下に移動したりできます。

CTグループポリシーは、グループを移動しても変更されません。また、CTグループを移動する場合、グループに登録されているCTも同時に移動されますが、CTに設定されているポリシーは変更されません(移動する前と変わりません)。

CTグループに部門管理者が設定されている場合は、CTグループを移動すると、部門管理者も移動します。

CTグループを移動する手順は、以下のとおりです。

1. [管理コンソール]を起動します。
2. CTグループツリーから移動するCTグループを選択します。

   →選択したCTグループが反転表示されます。

3. 同一サーバ配下の移動先CTグループに、移動するCTグループをドラッグ&ドロップで移動します。

   →CTグループが移動されます。

4. [ツリー設定]メニューから[CTグループ構成反映]を選択します。

   →移動したCTグループがデータベースに反映されます。

   [CTグループ構成反映]を実行しない場合、[ポリシー最新表示]、[次回起動時に更新する]、および[即時更新を行う]ボタンがグレーアウトされた状態になり、[CTグループ構成反映]を促すメッセージが表示されます。

削除する

削除するCTグループ配下に、CTグループまたはCTがある場合は削除できません。あらかじめ、配下のCTグループまたはCTをすべて削除してください。CTの削除方法は、“CTを削除する”を参照してください。

CTグループを削除する手順は、以下のとおりです。

1. [管理コンソール]画面を起動します。
2. CTグループツリーから削除するCTグループを選択します。
3. [ファイル]メニューから[CTグループ削除]を選択します。

   →削除確認画面が表示されます。

4. [OK]ボタンをクリックします。

   →選択したCTグループが削除されます。

5. [ツリー設定]メニューから[CTグループ構成反映]を選択します。

   →「削除したCT」グループがデータベースに反映されます。

   [CTグループ構成反映]を実行しない場合、[ポリシー最新表示]、[次回起動時に更新する]、および[即時更新を行う]ボタンがグレーアウトされた状態になり、[CTグループ構成反映]を促すメッセージが表示されます。

グループ情報を変更する

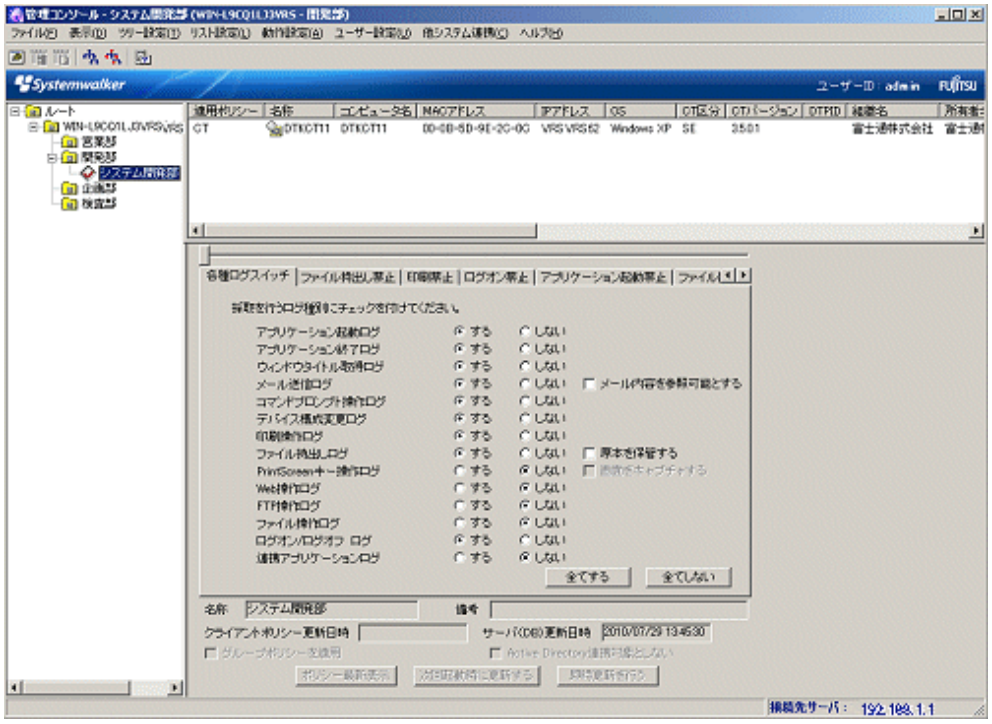
CTグループツリーに作成されているCTグループの名称、または備考を変更する方法について説明します。

手順は、以下のとおりです。

1. [管理コンソール]画面を起動します。

2. CTグループツリーから情報を変更するCTグループを選択します。

   →選択したCTグループが反転表示されます。



3. 以下の情報を入力し、[次回起動時に更新する]ボタンまたは[即時更新を行う]ボタンをクリックします。

   - [名称]:変更後のCTグループの名称を入力します。
     半角で40文字(全角で20文字)までの英数字、漢字、ひらがな、またはカタカナが入力できます。
   - [備考]:CTグループに関する備考を入力します。
     半角で128文字(全角で63文字)までの英数字、漢字、ひらがな、またはカタカナが入力できます。

4. [ツリー設定]メニューから[ツリー最新表示]を選択します。

   →選択したCTグループの名称が変更されます。

   [ツリー設定]メニューの[ツリー最新表示]がグレーアウトされている場合は、CTグループの作成、移動、削除のあと、構成反映が実施されていない可能性があります。この場合、[ツリー設定]メニューから[CTグループ構成反映]を選択し、構成反映を実施してください。

CT登録時自動振り分けファイルを作成する

CTのインストール後、クライアント(CT)と管理サーバが通信すると、クライアント(CT)が管理サーバに登録されます。このとき、クライアント(CT)は、すべてルート直下に配置されます。
CT登録時自動振り分けファイルを利用した場合、クライアント(CT)と管理サーバが通信すると、自動で各CTグループにクライアント(CT)を割り当てることができます。

手順は、以下のとおりです。

1. CTグループ情報を出力します。
   詳細は、“CTグループ情報を出力する”を参照してください。
2. CTグループ情報を出力したCSVファイルを「DTKCTEntry.csv」に変名します。
3. CT登録時自動振り分けファイル(DTKCTEntry.csv)を作成し、管理サーバに保存します。
   CT登録時自動振り分けファイルの詳細は、“Systemwalker Desktop Keeper リファレンスマニュアル”の“CT登録時自動振り分けファイル”を参照してください。

   格納場所

Windows Server® 2008以外の場合

```
[OSインストールドライブ]¥Documents and Settings¥All Users¥Application Data¥Fujitsu¥Systemwalker Desktop Keeper
```

Windows Server® 2008の場合

```
[OSインストールドライブ]¥ProgramData¥Fujitsu¥Systemwalker Desktop Keeper
```

→CTインストール後、クライアント(CT)が管理サーバと通信すると、CT登録時自動振り分けファイルの指定に従って、クライアント(CT)がCTグループに割り当てられます。

CT登録時自動振り分けファイルの内容に誤りがある場合、サーバサービスのトレースファイル(fsw21sj0.log)にエラーが表示されます。このとき、クライアント(CT)は、すべてルート直下に配置されます。

ユーザーグループを作成する

ユーザーグループツリーに表示するユーザーグループの構築について説明します。

ポイント

ユーザーポリシーを一元管理している場合は、統合管理サーバから操作してください

ユーザーポリシーを一元管理する運用を行っている場合は、統合管理サーバでユーザーグループを作成、移動、削除してください。

作成する

ユーザーグループツリーの表示がグレーアウトされ、グループを作成できない場合は、[ツリー設定]メニューで[空のグループは表示しない]が設定されています。この設定を解除してください。

ユーザーグループは、1つ1つ作成します。CSVファイルを利用して複数のユーザーグループをまとめて作成することはできません。

ユーザーグループを作成すると、ユーザーグループ配下のユーザーに、ユーザーポリシーを一括で設定できます。

ユーザーグループを作成する手順は以下のとおりです。

1. [管理コンソール]を起動します。

2. [ユーザー設定]メニューから、[ユーザーポリシー設定]を選択します。

   →[ユーザーポリシー設定]画面が表示されます。

3. ユーザーグループツリーから、グループを作成する上位のグループを選択します。
4. [ファイル]メニューから[ユーザーグループ作成]を選択します。

   →[ユーザーグループ作成]画面が表示されます。

5. 以下の情報を入力し、[追加]ボタンをクリックします。

   [グループ名]:半角で40文字(全角で20文字)までの英数字、漢字、ひらがな、およびカタカナが入力できます。

   →構成反映を促すメッセージが出力されます。

6. [OK]ボタンをクリックします。

   →ユーザーグループツリーに追加したグループが表示されます。

7. [ツリー設定]メニューから[ユーザーグループ構成反映]を選択します。

   →作成したユーザーグループがデータベースに反映されます。

   [ユーザーグループ構成反映]を実行しない場合、[ユーザーポリシー設定]画面を閉じたときに、[ユーザーグループ構成反映]を促すメッセージが表示されます。

   作成したユーザーグループがデータベースに反映された直後は、このユーザーグループのポリシーは、必ず以下のように設定されます。必要に応じてポリシーの変更を行ってください。ポリシーの変更については、“3.2.2 ユーザーグループポリシーを変更する”を参照してください。

- ルート配下にユーザーグループを作成した場合

  ユーザーグループを作成した統合管理サーバまたは管理サーバ上の[端末初期設定]画面で設定されたポリシーが反映されます。

- ほかのグループ配下にユーザーグループを作成した場合

  作成したユーザーグループの上位のユーザーグループに設定されているポリシーが反映されます。

移動する

ユーザーグループツリーに作成されているユーザーグループを、同一サーバ配下にある、ほかのユーザーグループ配下に移動する方法を説明します。

ユーザーグループポリシーは、グループを移動しても変更されません。また、ユーザーグループを移動する場合、グループに登録されているユーザーも同時に移動されますが、ユーザーポリシーは変更されません(移動する前と変わりません)。

ユーザーグループに部門管理者が設定されている場合は、ユーザーグループを移動すると、部門管理者も移動します。

ユーザーグループを移動する手順は、以下のとおりです。

1. [ユーザーポリシー設定]画面を起動します。
2. ユーザーグループツリーから移動するユーザーグループを選択します。

   →選択したユーザーグループが反転表示されます。
3. 同一サーバ配下の移動先ユーザーグループに、移動するユーザーグループをドラッグ&ドロップで移動します。

   →構成反映を促すメッセージが出力されます。
4. [OK]ボタンをクリックします。

   →ユーザーグループが移動されます。
5. [ツリー設定]メニューから[ユーザーグループ構成反映]を選択します。

   →移動したユーザーグループがデータベースに反映されます。

   [ユーザーグループ構成反映]を実行しない場合、[ユーザーポリシー設定]画面を閉じたときに、[ユーザーグループ構成反映]を促すメッセージが表示されます。

削除する

ユーザーグループツリーに作成されているユーザーグループを削除する方法について説明します。

削除するユーザーグループ配下に、ユーザーグループまたはユーザーが存在する場合は削除できません。あらかじめ、配下のユーザーグループまたはユーザーをすべて削除してください。ユーザーの削除については、“ユーザーを削除する”を参照してください。

ユーザーグループを削除する手順は、以下のとおりです。

1. [ユーザーポリシー設定]画面を起動します。
2. ユーザーグループツリーから削除するユーザーグループを選択します。
3. [ファイル]メニューから[ユーザーグループ削除]を選択します。

   →削除確認画面が表示されます。
4. [OK]ボタンをクリックします。

   →選択したユーザーグループが削除されます。
5. [ツリー設定]メニューから[ユーザーグループ構成反映]を選択します。

   →削除したユーザーグループがデータベースに反映されます。

   [ユーザーグループ構成反映]を実行しない場合、[ユーザーポリシー設定]画面を閉じたときに、[ユーザーグループ構成反映]を促すメッセージが表示されます。

グループ情報を変更する

ユーザーグループツリーに作成されているユーザーグループの名称、または備考を変更する方法について説明します。

手順は、以下のとおりです。

1. [ユーザーポリシー設定]画面を起動します。
2. ユーザーグループツリーから情報を変更するユーザーグループを選択します。

   →選択したユーザーグループが反転表示されます。
3. 以下の情報を入力し、[更新]ボタンをクリックします。

   - [グループ名]:変更後のユーザーグループのグループ名を入力します。
     半角で40文字(全角で20文字)までの英数字、漢字、ひらがな、およびカタカナが入力できます。
   - [備考]:ユーザーグループに関する備考を入力します。
     半角で128文字(全角で63文字)までの英数字、漢字、ひらがな、およびカタカナが入力できます。
4. [ツリー設定]メニューから[ツリー最新表示]を選択します。

   →選択したユーザーグループの名称が変更されます。

   [ツリー設定]メニューの[ツリー最新表示]がグレーアウトされている場合は、ユーザーグループの作成、移動、削除のあと、構成反映が実施されていない可能性があります。この場合、[ツリー設定]メニューから[ユーザーグループ構成反映]を選択し、構成反映を実施してください。

2.6 部門管理者を割り当てる

部門管理者を配置する運用の場合、構成情報ツリーの作成後に、グループに部門管理者を割り当てます。(部門管理者のリストは、Systemwalker Desktop Keeper導入時に、すでにサーバ設定ツールで登録されています。)
運用開始後、新規に部門管理者をサーバ設定ツールで登録して、割り当てることもできます。
登録方法は、“Systemwalker Desktop Keeper 導入ガイド”の“管理者情報を設定する”を参照してください。

部門管理者の割り当ては、システム管理者だけが実行できます。

部門管理者を設定したCTグループ(ユーザーグループ)配下のサブグループにも、自動的に同じ部門管理者が設定されます。
部門管理者を設定したグループでは、その部門管理者を確認(表示)できますが、サブグループで部門管理者を確認しようとしても、表示されません。
部門管理者は、自分が部門管理者として設定されたグループとその配下のグループのCT/ユーザーに対して、グループの作成、ポリシーの設定、ユーザーの登録などができます。部門管理者が実行できる操作と範囲については、“Systemwalker Desktop Keeper 導入ガイド”の“管理者種別ごとの使用可能な機能”を参照してください。

ユーザーグループだけに部門管理者を設定し、CTグループには設定しない場合、その部門管理者は、ログを参照できません。これは、ログビューアに表示されるグループツリーは、CTグループツリーであり、ログの参照はCTごとに行われるためです。したがって、ログを参照できるように、CTグループにも部門管理者を設定してください。

構成情報ツリーの以下の場所に表示されているクライアント(CT)に対しては、部門管理者を設定できません(以下の場所にグループを作成すれば、そのグループに部門管理者を設定できます)。したがって、以下の場所に表示されているクライアント(CT)の移動や削除は、システム管理者だけが実行できます。

- ルート直下
- ドメイングループ直下
- Localグループ直下

3階層のシステム構成の場合、部門管理者をどのサーバで設定するかは、[サーバ設定ツール]の[システム設定]画面での設定によって異なります。

Active Directory連携を行う場合	Active Directory連携を行わない場合	
	ユーザー情報を統合管理サーバで一元管理する場合	ユーザー情報を管理サーバごとに管理する場合(V13.0以前と互換)
統合管理サーバで設定を行います。(注)	統合管理サーバで設定を行います。(注)	各管理サーバで設定を行います。 統合管理サーバの情報は、各管理サーバへ更新されません。

注) 統合管理サーバが障害などで使用できない場合は、管理サーバで設定することもできます。しかし、以下のタイミングで、管理サーバでの設定内容は、統合管理サーバの最新情報で上書きされます。

- SWLevelControlService・SWServerService再起動時
- Active Directory連携時
- サーバ設定ツールで「管理者情報設定」を更新した場合
- 統合管理サーバに接続した管理コンソールで部門管理者設定を行った場合(ただし、設定を行った部門だけ更新されます。)

ポイント

Citrix XenApp クライアントでの操作ログを効率よく検索するために

Citrix XenApp Server管理者が設定されている場合は、Citrix XenApp Serverをまとめたグループの部門管理者になることで、Citrix XenApp Server上のすべての操作を監視できます。
また、自部門配下に、Citrix XenApp Serverのグループと、CTグループが存在する場合は、両方のグループの部門管理者となることで、Citrix XenApp クライアントとクライアント(CT)の両方で操作された内容を把握できます。

部門管理者の割り当て方法は、以下の2とおりがあります。

- GUIを使用して割り当てる

- CSVファイルを使用して一括割り当てする

  実行するには、管理コンソールに対して[CSVファイル取り込み]権限を持っていることが必要です。権限の設定は、サーバ設定ツールの[管理者情報設定]画面の[詳細権限]で行います。

  事前に、割り当てる部門管理者情報のCSVファイルを作成しておく必要があります。
  まず、管理コンソールで部門管理者情報をCSV出力し、CSVファイルのフォーマットを入手します。そのファイルに、割り当てる部門管理者を追記します。

  同じCTグループ(ユーザグループ)に対して、複数の部門管理者を割り当てる場合は、対象のグループのレコードをコピーして、部門管理者ログオンIDを記述してください。

  【作成例】
  以下の2行目以降の太字部分(5番目の項目である「部門管理者ログオンID」)が、CSVファイルに追記する情報です。

  "深さ","グループID","グループ名","処理フラグ","部門管理者ログオンID","部門管理者ユーザー名","アクセス権","詳細権限－管理コンソール1","詳細権限－管理コンソール2","詳細権限－管理コンソール3","詳細権限－管理コンソール4","詳細権限－管理コンソール5","詳細権限－管理コンソール6","詳細権限－管理コンソール7","詳細権限－管理コンソール8","詳細権限－ログビューア1","詳細権限－ログビューア2","詳細権限－ログビューア3","詳細権限－ログビューア4","詳細権限－ログビューア5","詳細権限－ログビューア6","詳細権限－ログビューア7","詳細権限－ログビューア8","備考"
  "1","8F10E643-2E93-4c5d-820E-D4A3322130A7","企画部"," ","**森山**"," "," "," "," "," "," "," "," "," "," "," "," "," "," "," "," "," "," "," "
  "2","7F9CB48C-DA30-45d7-9E86-08E95994AF1C","企画部"," ","**林**"," "," "," "," "," "," "," "," "," "," "," "," "," "," "," "," "," "," "," "
  "2","7F9CB48C-DA30-45d7-9E86-08E95994AF1D","企画部"," "

  CSVファイルの詳細は、"Systemwalker Desktop Keeper リファレンスマニュアル"の"ファイルリファレンス"の"部門管理者情報"を参照してください。

また、CSVファイルに登録する部門管理者には、部門管理者としての権限を設定しておく必要があります。権限は、サーバ設定ツールの[管理者情報設定]画面で設定します。詳細は、“Systemwalker Desktop Keeper 導入ガイド”の“管理者情報を設定する”を参照してください。

GUIを使用して割り当てる

GUIを使用して部門管理者を割り当てる方法を説明します。

CTグループに部門管理者を割り当てる

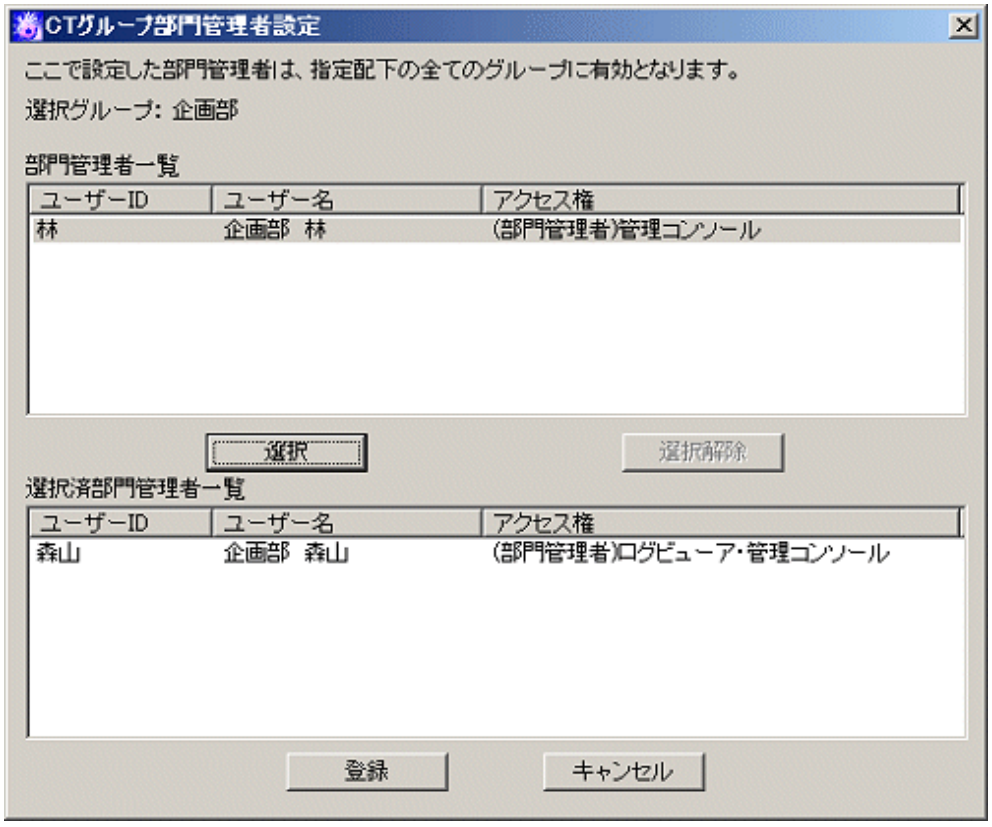
1. [管理コンソール]を起動します。

   ログオン時は、管理者のユーザーIDとパスワードを使用します。

2. CTグループツリーから部門管理者を設定するCTグループを選択します。

3. [ファイル]メニューから[CTグループ部門管理者設定]を選択します。

   →[CTグループ部門管理者設定]画面が表示されます。



4. [部門管理者一覧]から設定する部門管理者を選択し、[選択]ボタンをクリックします。

   →[選択済部門管理者一覧]に選択した部門管理者が表示されます。

5. [登録]ボタンをクリックします。

   →確認画面が表示されます。

6. [OK]ボタンをクリックします。

ユーザーグループに部門管理者を割り当てる

1. [管理コンソール]を起動します。

   ログオン時は、システム管理者のユーザーIDとパスワードを使用します。

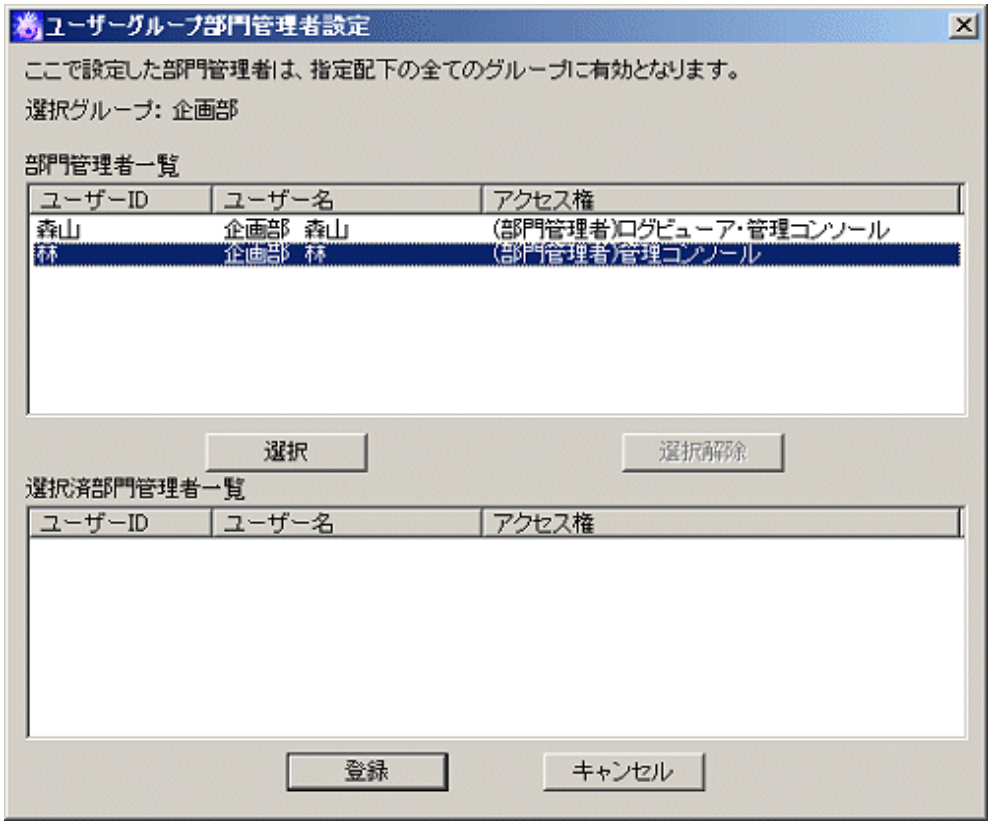
2. [ユーザー設定]メニューから[ユーザーポリシー設定]を選択します。

   →[ユーザーポリシー設定]画面が表示されます。

3. ユーザーグループツリーから部門管理者を設定するユーザーグループを選択します。

4. [ファイル]メニューから[ユーザーグループ部門管理者設定]を選択します。

   →[ユーザーグループ部門管理者設定]画面が表示されます。



5. [部門管理者一覧]から設定する部門管理者を選択し、[選択]ボタンをクリックします。

   →[選択済部門管理者一覧]に選択した部門管理者が表示されます。

6. [登録]ボタンをクリックします。

   →確認画面が表示されます。

7. [OK]ボタンをクリックします。

CSVファイルを使用して一括割り当てする

CSVファイルを使用して部門管理者を一括で割り当てる方法を説明します。

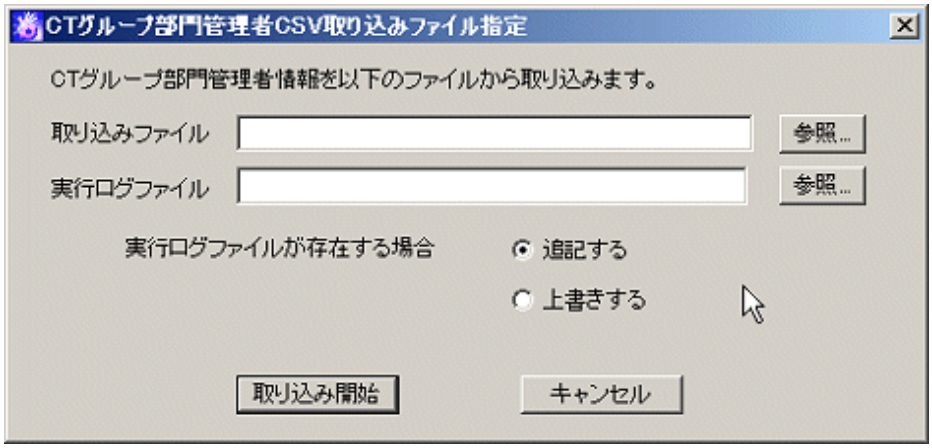
CTグループに部門管理者を割り当てる

1. [管理コンソール]を起動します。

   ログオン時は、システム管理者のユーザーIDとパスワードを使用します。

2. [ファイル]メニューから[CTグループ部門管理者情報CSV取り込み]を選択します。

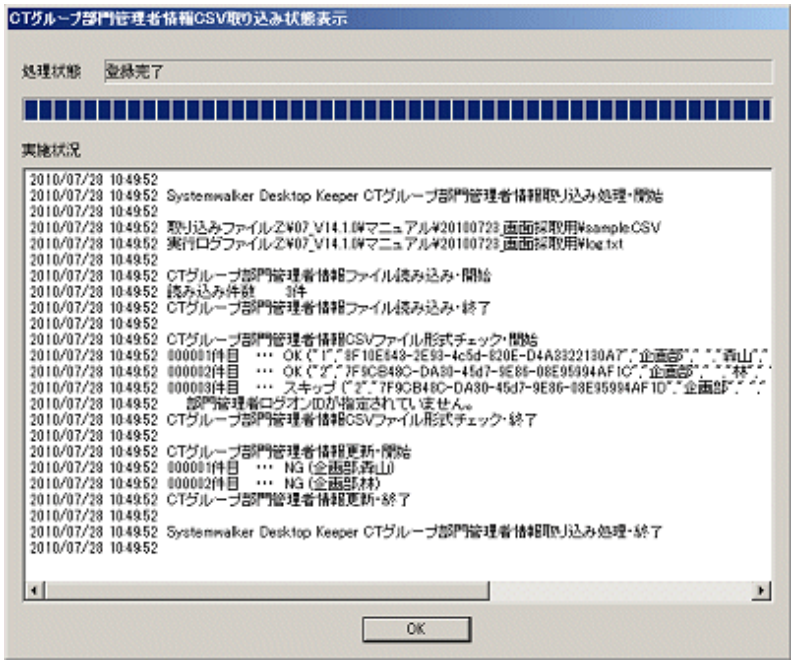
   →[CTグループ部門管理者CSV取り込みファイル指定]画面が表示されます。



   - **[取り込みファイル]**(必須):部門管理者情報が定義されているCSVファイルを、フルパスで指定します。
   - **[実行ログファイル]**(必須):実行結果を保存するファイルを、フルパスで指定します。
   - **[実行ログファイルが存在する場合]**:既存の実行ログファイルが存在する場合は必ず設定してください。
     [追記する]:既存の実行ログファイルに追記する場合に選択します。
     [上書きする]:既存の実行ログファイルに上書きする場合に選択します。

3. 上記の情報を設定し、[取り込み開始]ボタンをクリックします。

   →[CTグループ部門管理者情報CSV取り込み状態表示]画面が表示されます。



4. 部門管理者情報がデータベースに登録されると、[処理状態]に「登録完了」と表示されます。[OK]ボタンをクリックします。

ユーザーグループに部門管理者を割り当てる

1. [管理コンソール]を起動します。

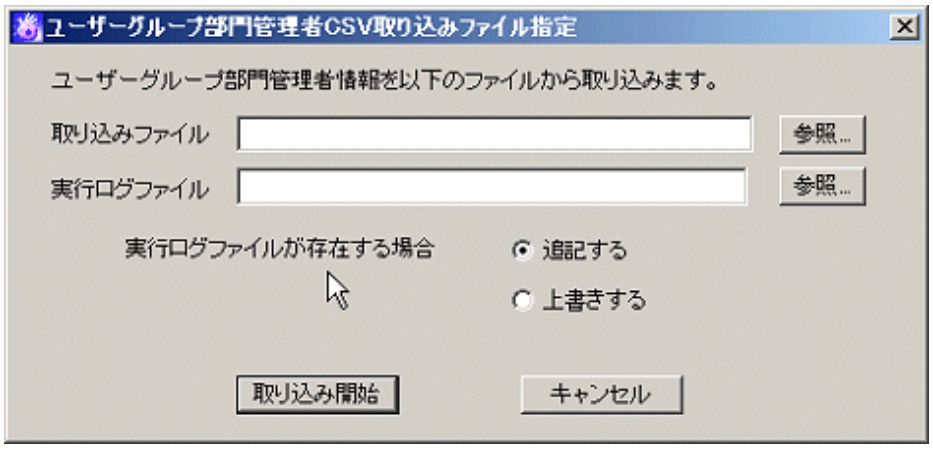
   ログオン時は、システム管理者のユーザーIDとパスワードを使用します。

2. [ユーザー設定]メニューから[ユーザーポリシー設定]を選択します。

   →[ユーザーポリシー設定]画面が表示されます。

3. [ファイル]メニューから[ユーザーグループ部門管理者情報CSV取り込み]を選択します。

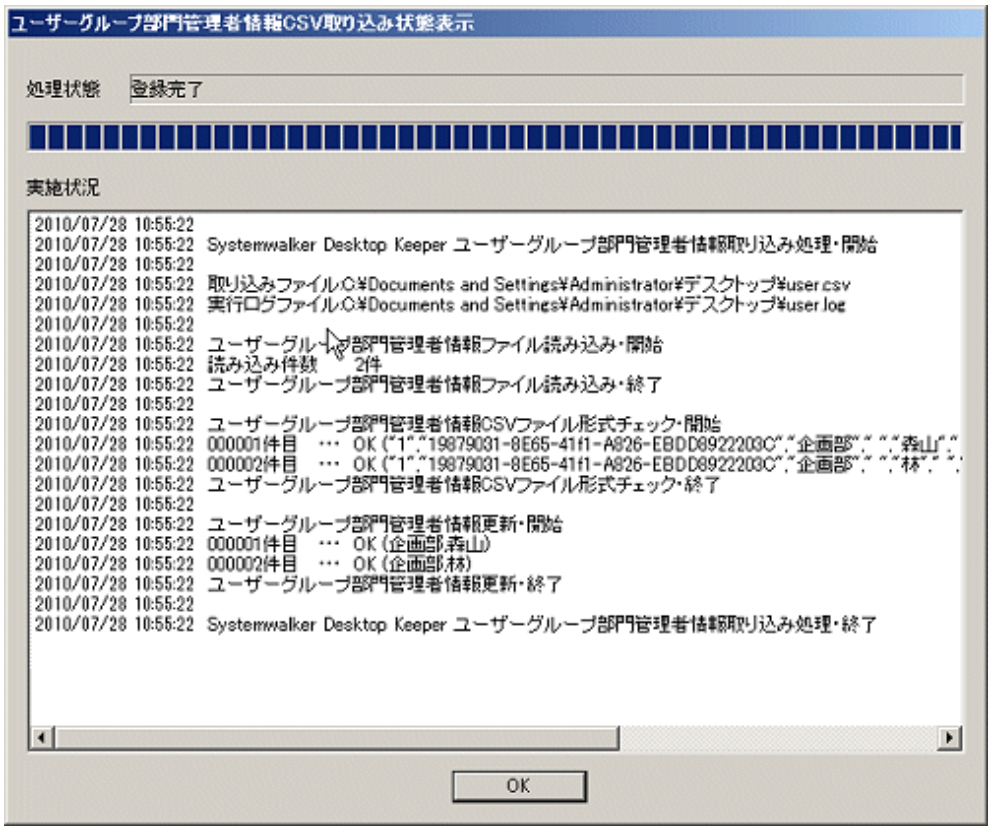
   →[ユーザーグループ部門管理者CSV取り込みファイル指定]画面が表示されます。



- **[取り込みファイル]**(必須):部門管理者情報が定義されているCSVファイルを、フルパスで指定します。
- **[実行ログファイル]**(必須):実行結果を保存するファイルを、フルパスで指定します。
- **[実行ログファイルが存在する場合]**:既存の実行ログファイルが存在する場合は必ず設定してください。
  [追記する]:既存の実行ログファイルに追記する場合に選択します。
  [上書きする]:既存の実行ログファイルに上書きする場合に選択します。

4. 上記の情報を設定し、[取り込み開始]ボタンをクリックします。

   →[ユーザーグループ部門管理者情報CSV取り込み状態表示]画面が表示されます。



5. 部門管理者情報がデータベースに登録されると、[処理状態]に「登録完了」と表示されます。[OK]ボタンをクリックします。

2.6.1 管理コンソールで部門管理者情報を出力する

部門管理者情報をCSVファイルに出力する方法を説明します。

実行できる人

部門管理者情報のCSVファイル出力は、システム管理者と部門管理者が実行できます。
実行するには、管理コンソールに対して[CSVファイル取り込み]権限を持っていることが必要です。権限の設定は、システム管理者が、サーバ設定ツールの[管理者情報設定]画面の[詳細権限]で行います。

出力できる範囲

システム管理者が実行する場合は、管理サーバ配下の全グループの部門管理者情報を出力できます。部門管理者が設定されていないグループについては、[グループID]と[グループ名]が出力されます。

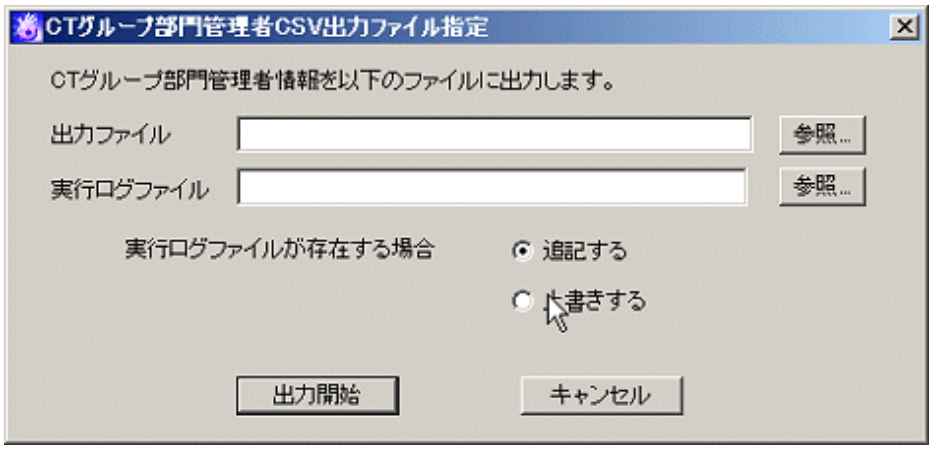
部門管理者が実行する場合は、自らが部門管理者となっているグループと、その配下のグループの全情報を出力できます。自部門以外のグループについては、[グループID]と[グループ名]だけ出力されます。

出力内容の詳細は、“Systemwalker Desktop Keeper リファレンスマニュアル”の“ファイルリファレンス”の“部門管理者情報”を参照してください。

CTグループの部門管理者情報を出力する

1. [管理コンソール]を起動します。
2. [ファイル]メニューから[CTグループ部門管理者情報CSV出力]を選択します。

   →[CTグループ部門管理者CSV出力ファイル指定]画面が表示されます。



- **[出力ファイル]**(必須):部門管理者情報を出力するCSVファイルを、フルパスで指定します。

  半角で218文字まで入力できます。ただし、以下の記号はファイル名として使用できません。
  使用できない記号:「¥」「/」「:」「*」「?」「"」「<」「>」「|」

- **[実行ログファイル]**(必須):実行結果を保存するファイルを、フルパスで指定します。

  半角で218文字まで入力できます。ただし、以下の記号はファイル名として使用できません。
  使用できない記号:「¥」「/」「:」「*」「?」「"」「<」「>」「|」

- **[実行ログファイルが存在する場合]**:既存の実行ログファイルが存在する場合は必ず設定してください。
  [追記する]:既存の実行ログファイルに追記する場合に選択します。
  [上書きする]:既存の実行ログファイルに上書きする場合に選択します。

3. 上記の情報を設定し、[出力開始]ボタンをクリックします。

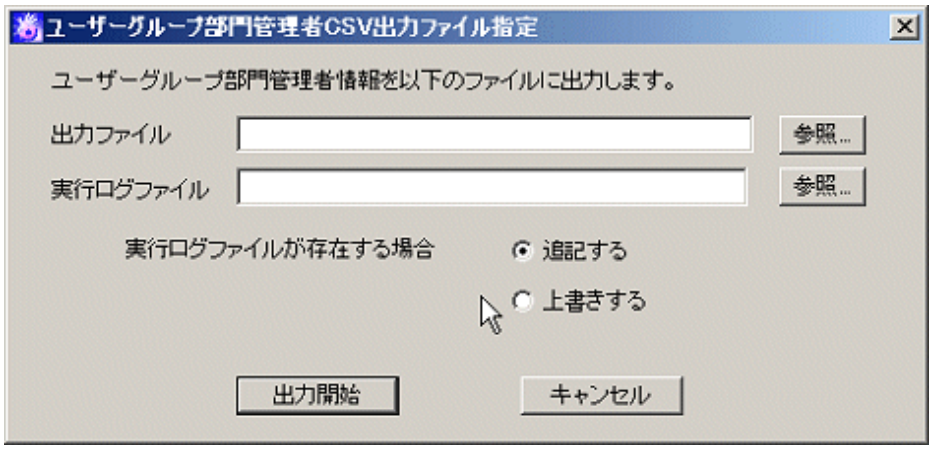
4. 出力が完了すると、メッセージが表示されます。[OK]ボタンをクリックします。

ユーザーグループの部門管理者情報を出力する

1. [管理コンソール]を起動します。
2. [ユーザー設定]メニューから[ユーザーポリシー設定]を選択します。

   →[ユーザーポリシー設定]画面が表示されます。
3. [ファイル]メニューから[ユーザーグループ部門管理者情報CSV出力]を選択します。

   →[ユーザーグループ部門管理者CSV出力ファイル指定]画面が表示されます。



- **[出力ファイル]**(必須):部門管理者情報を出力するCSVファイルを、フルパスで指定します。

  半角で218文字まで入力できます。ただし、以下の記号はファイル名として使用できません。
  使用できない記号:「¥」「/」「:」「*」「?」「"」「<」「>」「|」

- **[実行ログファイル]**(必須):実行結果を保存するファイルを、フルパスで指定します。

  半角で218文字まで入力できます。ただし、以下の記号はファイル名として使用できません。
  使用できない記号:「¥」「/」「:」「*」「?」「"」「<」「>」「|」

- **[実行ログファイルが存在する場合]**:既存の実行ログファイルが存在する場合は必ず設定してください。
  [追記する]:既存の実行ログファイルに追記する場合に選択します。
  [上書きする]:既存の実行ログファイルに上書きする場合に選択します。

4. 上記の情報を設定し、[出力開始]ボタンをクリックします。
5. 出力が完了すると、メッセージが表示されます。[OK]ボタンをクリックします。

2.7 Active Directoryでログオンスクリプトを設定する

Windows Server® 2003にインストールされたCitrix XenApp Server上の操作を記録する場合、公開アプリケーションの以下のログを採取するときは、Active Directoryでログオンスクリプトを設定する必要があります。
Windows Server® 2008の場合は、ログオンスクリプトを設定する必要はありません。

- アプリケーション起動ログ
- アプリケーション終了ログ
- 印刷操作ログ
- ウィンドウタイトル取得ログ

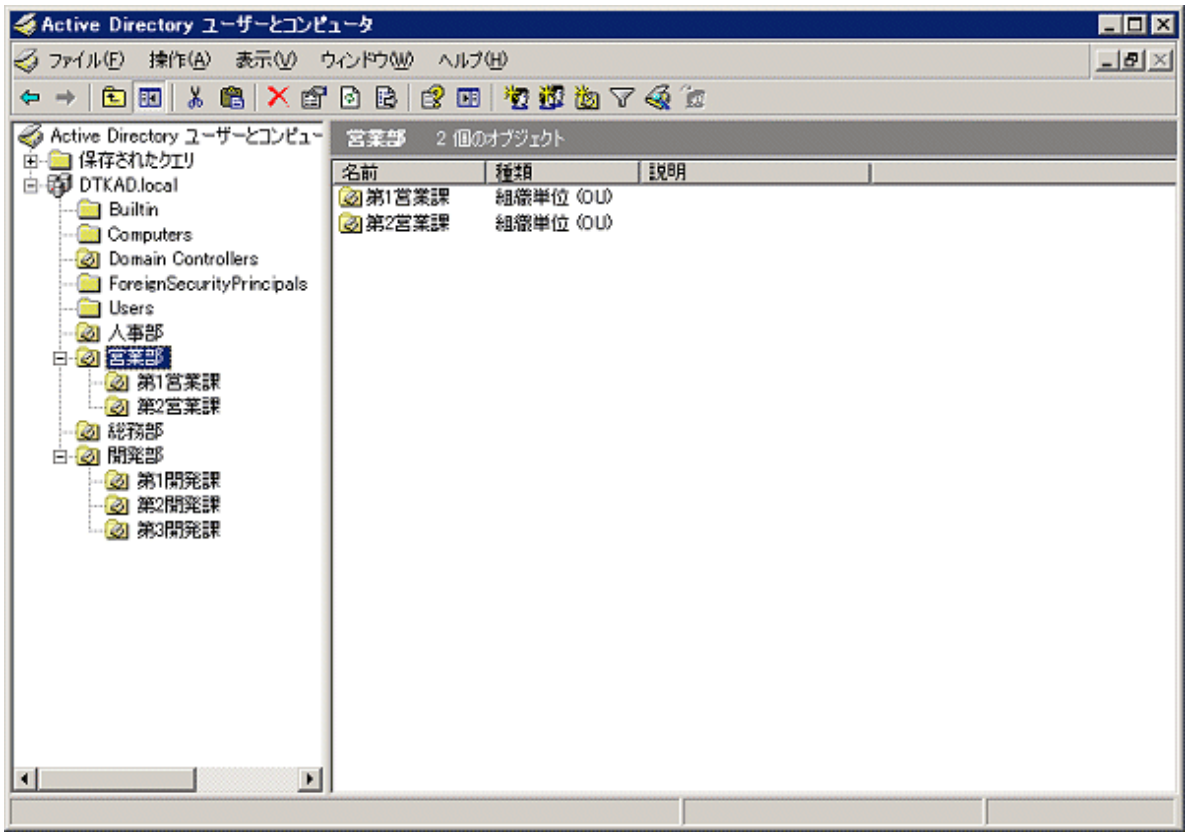
・ PrintScreenキー操作ログ

公開アプリケーション起動前の操作

公開アプリケーションを起動する前に、Active Directoryでログオンスクリプトを設定します。

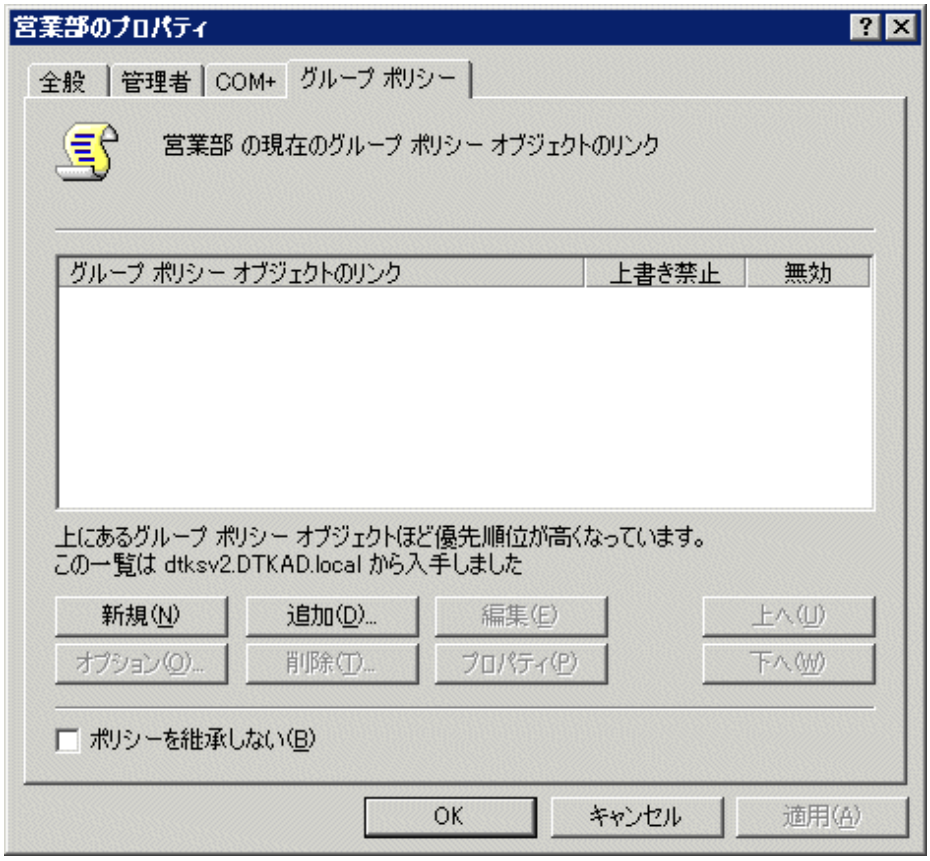
以下に設定手順を示します。

1. Active Directoryサーバの[スタート]メニューから[管理ツール]-[Active Directory ユーザーとコンピュータ]を選択します。
   →以下の画面が出力されます。

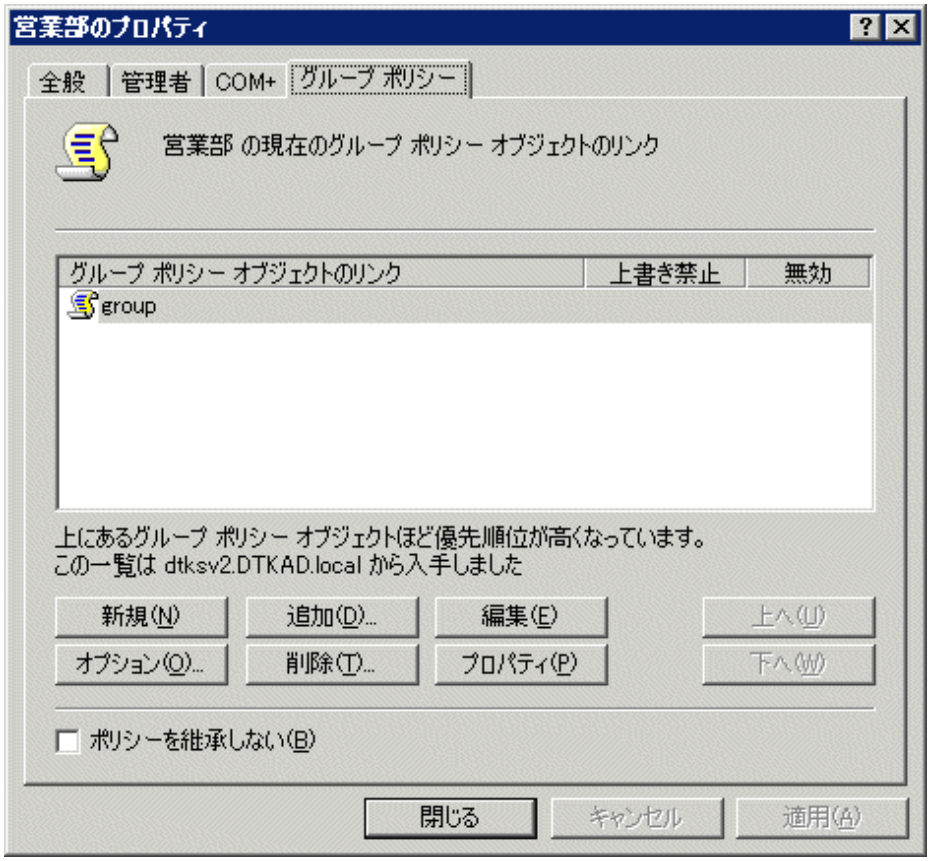


2. [Active Directory ユーザーとコンピュータ]画面のツリーで、Citrix XenApp Serverにログオンするユーザーが所属する組織(OU)やグループを選択し、右クリックメニューで[プロパティ]を選択します。

   →以下の画面が出力されます。

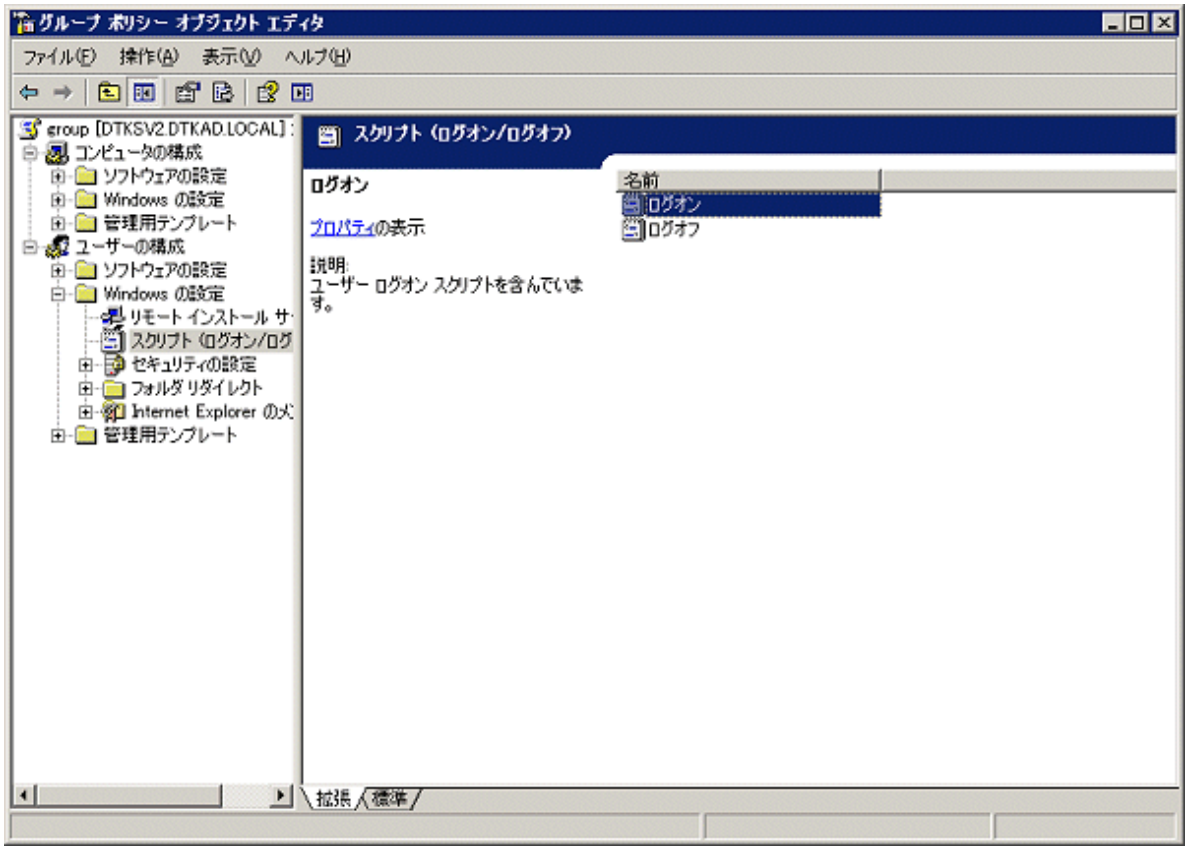


3. [グループポリシー]タブを選択後、[新規]ボタンをクリックし、任意の名前に変更します。



4. [編集]ボタンをクリックします。

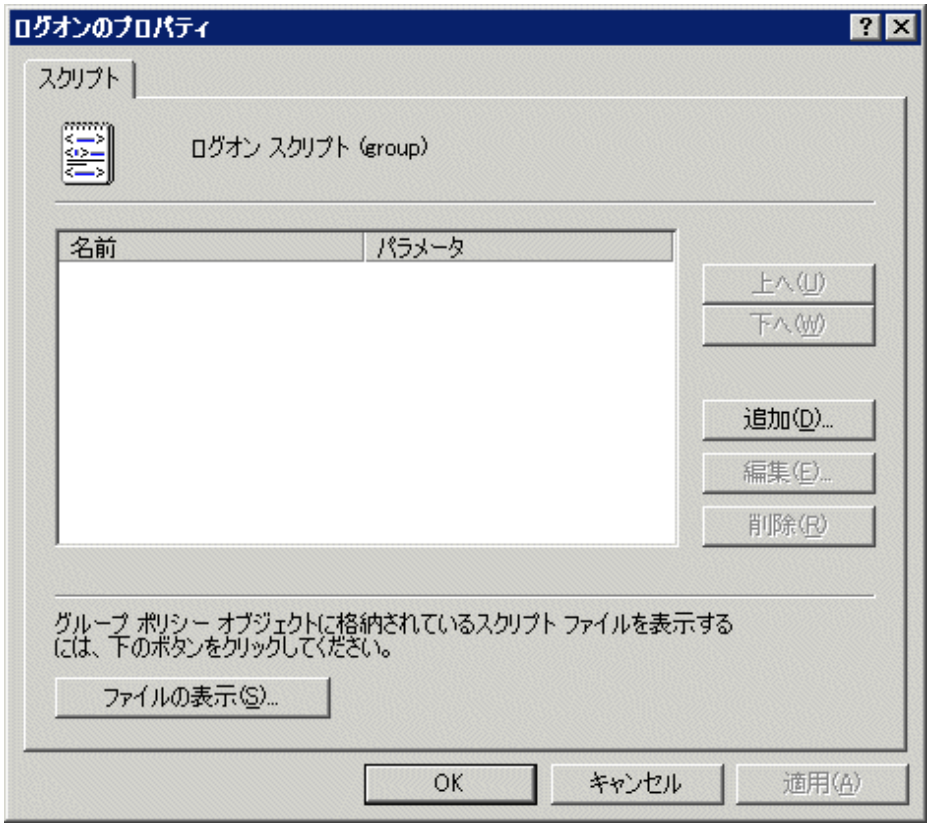
   →以下の画面が出力されます。



5. 画面のツリーで、[ユーザーの構成]-[Windowsの設定]-[スクリプト(ログオン/ログオフ)]を選択します。

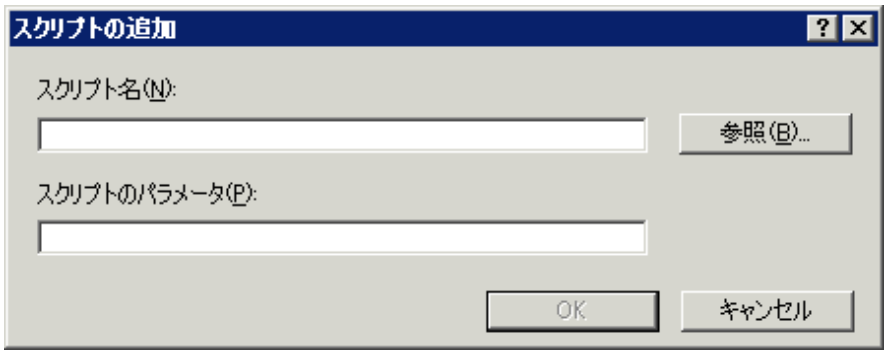
6. 右側のリストから[ログオン]を選択し、[プロパティ]を選択します。

   →[ログオンのプロパティ]画面が出力されます。



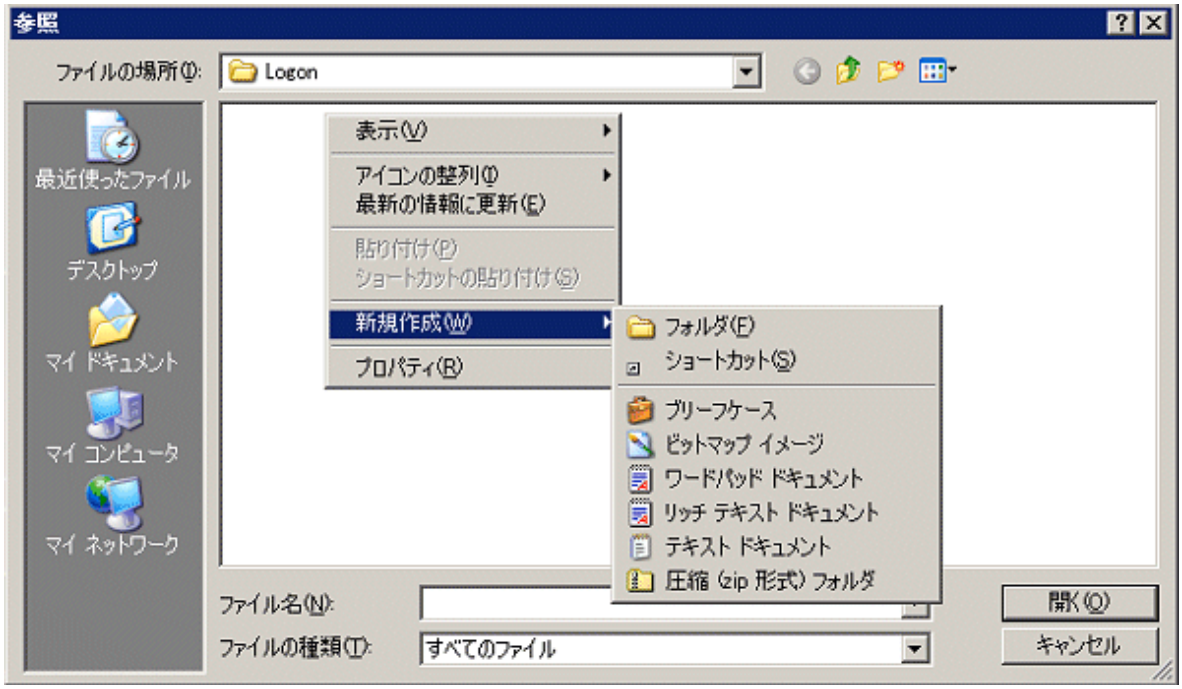
7. [追加]ボタンをクリックします。

   →[スクリプトの追加]画面が出力されます。



8. [参照]ボタンをクリックします。

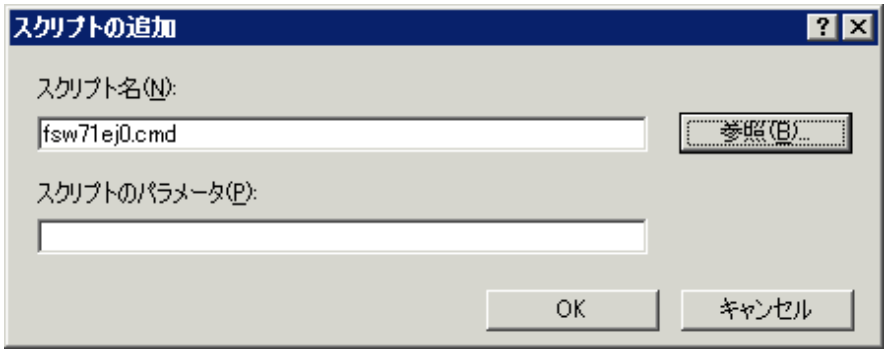
   →以下の画面が出力されます。



9. 右クリックし、[新規作成]-[テキストドキュメント]を選択します。

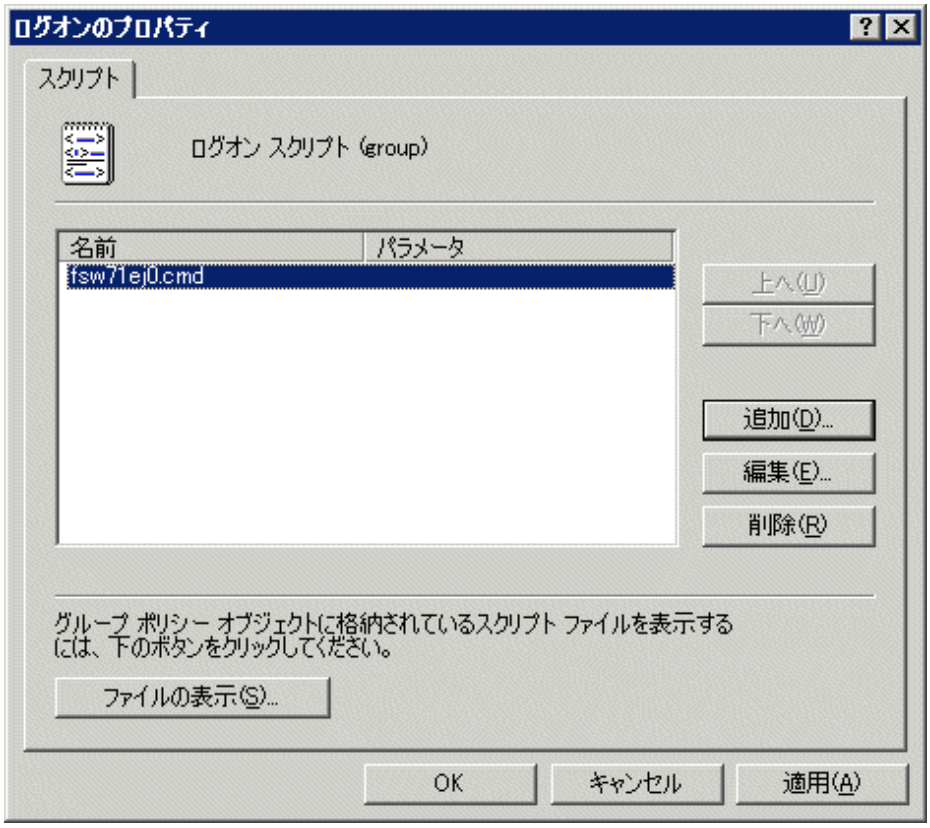
10. ファイル名を“fsw71ej0.cmd”に変更し、[開く]ボタンをクリックします。

    →[スクリプトの追加]画面が出力されます。



11. [OK]ボタンをクリックします。

    →[ログオンのプロパティ]画面が出力されます。



12. [ファイルの表示]ボタンをクリックし、“fsw71ej0.cmd”を編集します。
    以下のコマンドを記述します。

    ー fsw71ej0.exe

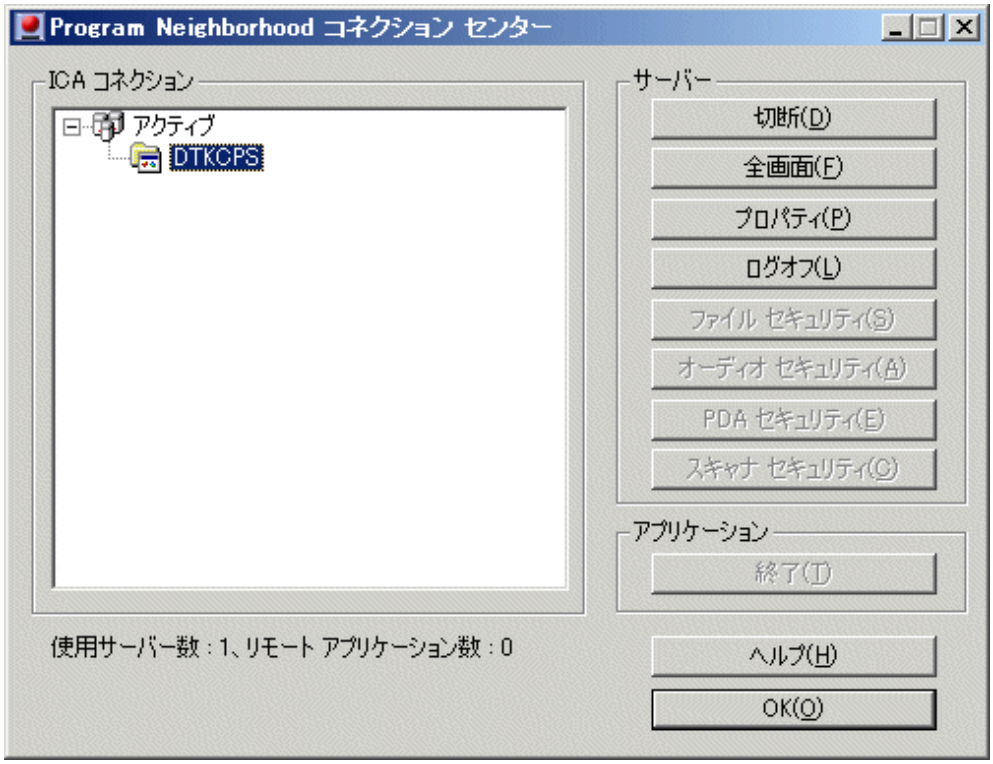
13. [適用]ボタン、[OK]ボタンをクリックします。

公開アプリケーション終了後の操作

Active Directoryでログオンスクリプトを設定した場合は、公開アプリケーションを終了しても、登録したコマンドは終了しません。
Program Neighborhoodコネクションセンター、またはCitrix コネクションセンターを使用してログオフしてください。

1. タスクトレイで[Program Neighborhood コネクションセンター]、または[Citrix コネクションセンター]を右クリックし、[コネクションセンターを開く]を選択します。

2. アクティブになっているCitrix XenApp Serverを選択し、[ログオフ]ボタンをクリックします。



2.8 ログを集計するための準備をする

状況画面またはログアナライザを使用してログの集計結果を確認する場合、表示項目、しきい値などの条件を前もって定義しておく必要があります。

注意

Webコンソールの起動に関する注意

Webコンソールは同一PC上で複数起動しないでください。

2.8.1 状況画面を利用するための準備をする

集計条件の設定方法を説明します。

集計条件の設定は、システム管理者だけが実施できます。

運用中に集計条件を変更した場合、変更後の条件が反映されるのは、次回の集計時です。そのため、次回の集計までの間は、画面上には古い条件で検出したPC台数や詳細グラフの情報が表示されます。

3階層のシステム構成の場合、システム全体の状況を把握するときは、統合管理サーバで集計条件を設定してください。配下の管理サーバ単位で状況を把握するときは、各管理サーバで集計条件を設定してください。

1. 以下のいずれかの方法で、Webコンソールを起動します。

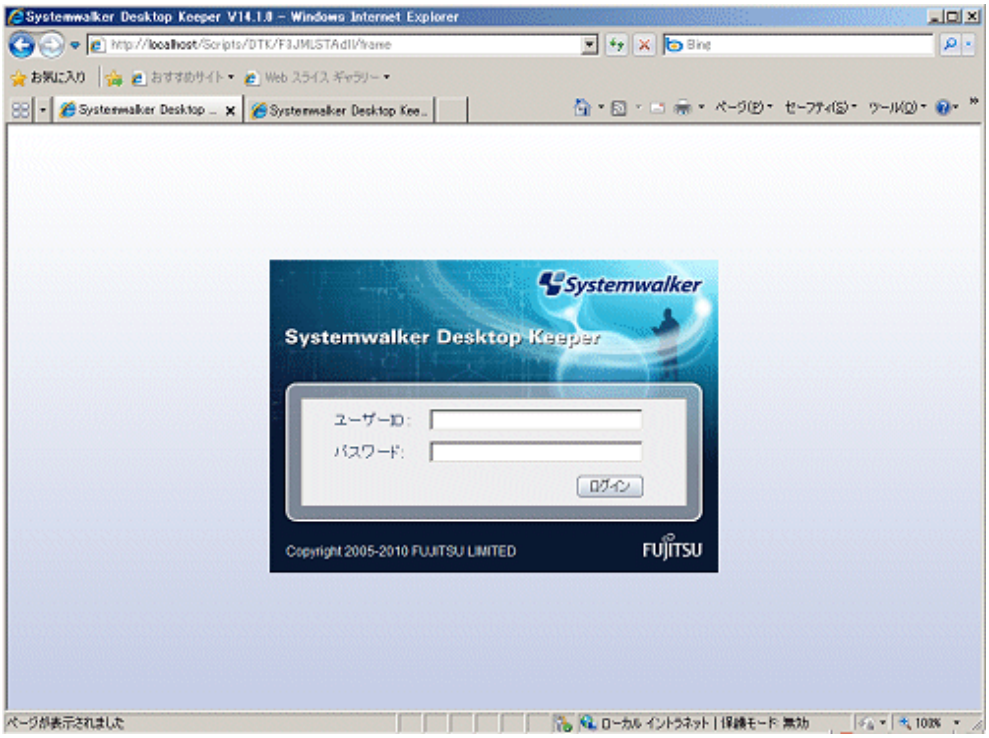
   2階層のシステム構成の場合：管理サーバに接続してください。

- 管理サーバの[スタート]メニューから[プログラム]-[Systemwalker Desktop Keeper]-[サーバ]-[Desktop Keeper メインメニュー]を選択します。
- ブラウザのアドレスに“http://管理サーバのホスト名またはIPアドレス/DTK/index.html”と指定します。
  IISのポート番号に変更があった場合は、以下のように指定します。
  http://IPアドレス:ポート番号/DTK/index.html

3階層のシステム構成の場合:管理(統合管理)サーバそれぞれに接続してください。

- 管理(統合管理)サーバの[スタート]メニューから[プログラム]-[Systemwalker Desktop Keeper]-[サーバ]-[Desktop Keeper メインメニュー]を選択します。
- ブラウザのアドレスに“http://管理(統合管理)サーバのホスト名またはIPアドレス/DTK/index.html”と指定します。
  IISのポート番号に変更があった場合は、以下のように指定します。
  http://IPアドレス:ポート番号/DTK/index.html

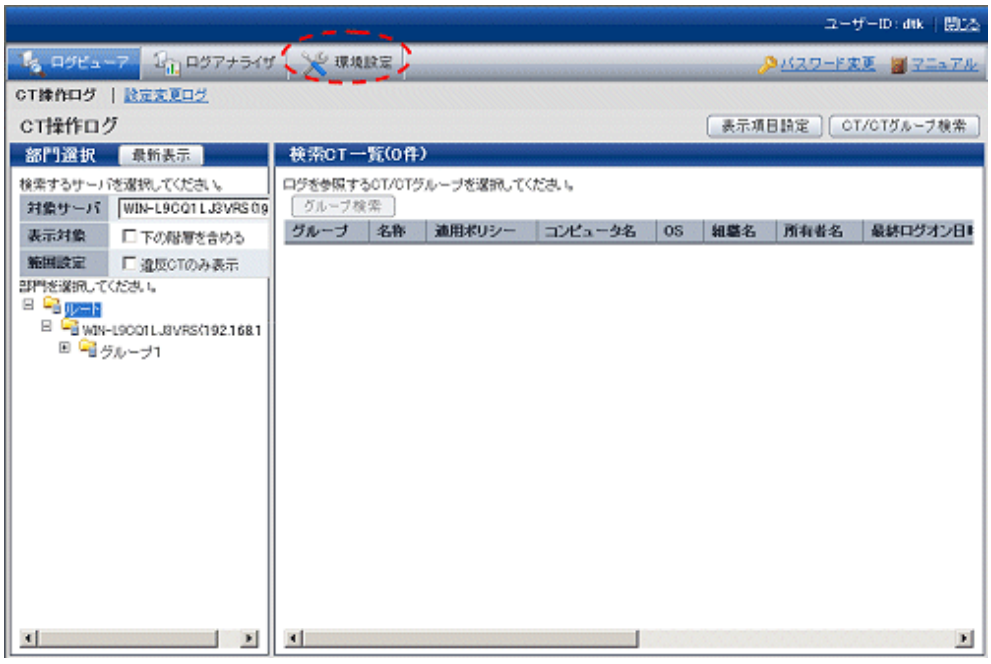
→[ログイン]画面が表示されます。



2. 以下の情報を入力し、[ログイン]ボタンをクリックします。
   - **[ユーザーID]:**サーバ設定ツールの[管理者情報設定]画面で設定した[ユーザーID]です。
   - **[パスワード]:**サーバ設定ツールの[管理者情報設定]画面で設定した[パスワード]です。
     パスワードは定期的に変更することを推奨します。変更方法は、“パスワードを変更する”を参照してください。

→状況画面が表示されます。

3. グローバルナビゲーションの[ログ管理]をクリックします。
→ログビューアが起動され、[CT操作ログ]画面が表示されます。



4. グローバルナビゲーションの[環境設定]をクリックします。
→[オプション]画面が表示されます。

5. 以下の情報を設定し、[適用]ボタンをクリックします。

集計に要する処理時間について

集計に要する処理時間は、以下の要因に影響を受けます。

- ハードウェアスペック(CPU、メモリ、ディスク性能など)
- 運用環境(ネットワーク状態、他のアプリケーション動作状況など)
- 管理サーバ台数(3階層構成における統合管理サーバの場合)
- 集計条件(監査項目数や監査期間(*)など)
- CT台数
- データベースに格納されているログ量

また上記の運用環境が同等の条件であっても集計結果の以下の要因によっても処理時間は変わります。

- 集計条件に合致するCT台数(*)
- 集計条件に合致するログ量(*)

(*)印の項目が特に影響の大きい要因です。

以下は処理時間の一例です(参考値であり、ハードウェア環境やデータにより大きく変化します)。
実際の処理時間は環境やデータの条件により数分から数時間までかかる場合があります。
ハードウェアはいずれもCPU:Core2Duo 2.4GHz メモリ:3GB の場合です。

- CT数100台(うち集計条件に合致が100台)、ログ量63万件(うち集計条件に合致が21万件)、監査期間31日で、約150秒。
- CT数500台(うち集計条件に合致が500台)、ログ量63万件(うち集計条件に合致が21万件)、監査期間31日で、約430秒。

項目名	説明
[集計スケジュール]	集計処理を開始する時刻を設定します。 ・ 時:0～23の範囲で、1時間単位で選択可能です。 ・ 分:0～59の範囲で、1分単位で選択可能です。

項目名	説明
	初期値:1時0分 注意 **集計スケジュールの設定では以下の点を考慮してください** ・集計処理には負荷がかかります。業務負荷がかからない時間帯(夜半など)に行うようにしてください。 ・集計処理中に構成情報や環境設定の変更を行わないでください。集計結果が正しく表示されない可能性があります。 ・集計処理には階層化サービスが起動している必要があります。階層化サービスを停止する操作(バックアップ・リストアや、データ転送など)の処理と重ならないよう注意してください。
[グラフ色の割合(%)]	状況画面に表示する棒グラフの色を変えるしきい値を設定します。 黄色の割合と赤色の割合を、ボタンで選択して変更できます。10%単位で変更できます。 **初期値:**黄色棒グラフのしきい値が20%以内 赤色棒グラフのしきい値が80%以上
[Desktop PatrolのURL]	Systemwalker Desktop Patrolの資産管理情報を表示する場合に設定します。 半角の英数字、「.」「:」を指定することができます。 **初期値:**なにも表示されていません。
[ファイルを持出したPC] (条件はすべてAND条件として集計されます)	
[項目の説明]	集計項目の説明です。
[項目の集計]	集計結果を状況画面に表示する/しないを設定します。 **初期値:**[する]が選択されています。
[集計期間の設定]	異常PCの集計期間(X日前から集計日まで)を設定します。 1～31日の範囲で、1日単位で選択可能です。 **初期値:**7日
[外部記憶媒体種別の設定]	外部記憶媒体のドライブ種別を、リムーバブル、CD/DVD、ネットワークから選択します。 複数選択可能です。最低1つは選択してください。 **初期値:**[リムーバブル]が選択されています。
[時間外に利用したPC] (条件はすべてAND条件として集計されます)	
[項目の説明]	集計項目の説明です。
[項目の集計]	集計する/しないを設定します。 集計しないを選択した場合は、状況画面に表示されません。 **初期値:**[する]が選択されています。
[集計期間の設定]	異常PCの集計期間(X日前から集計日まで)を設定します。 1～31日の範囲で、1日単位で選択可能です。 **初期値:**7日
[時間外の設定]	「時間外」とする時間帯を定義します。 ・曜日:時間外を設定する曜日を選択します。最低1つは選択してください。 ・時間:時間外の時間を選択します。 0～23の範囲で、1時間単位で指定可能です。 時間を指定しない場合は、「-」を設定します。 **初期値:**

<table>
<tr><th colspan="2">項目名</th><th>説明</th></tr>
<tr><td></td><td></td><td>・ パターン1(平日想定)
　ー 曜日:月、火、水、木、金
　ー 時間:00時00分～8時59分、17時00分～23時59分
・ パターン2(土日想定)
　ー 曜日:土、日
　ー 時間:指定なし

 例
指定例1
土日に利用されているPCを集計する場合
・時間:指定しない
・曜日:土、日をチェックします
指定例2
平日の業務時間外に利用されているPCを集計する場合
・時間:00時00分～8時59分 または、 17時00分～23時59分
・曜日:月、火、水、木、金をチェックします

同一時間帯が設定されている場合でも、重複して集計されることはありません。
【例】
00時00分～6時59分または、00時00分～6時59分
と設定し、上記の時間帯にPCが1台利用されている場合、集計結果は1となります。</td></tr>
<tr><td colspan="3">[禁止されたUSBデバイスを利用したPC]
[禁止されたユーザーIDを利用したPC]
[禁止されたアプリケーションを利用したPC]
[禁止された印刷を行ったPC]
[禁止されたメール添付を行ったPC]
(条件はすべてAND条件として集計されます)</td></tr>
<tr><td></td><td>[項目の説明]</td><td>集計項目の説明です。</td></tr>
<tr><td></td><td>[項目の集計]</td><td>集計結果を状況画面に表示する/しないを設定します。
初期値:[する]が選択されています。</td></tr>
<tr><td></td><td>[集計期間の設定]</td><td>異常PCの集計期間(X日前から集計日まで)を設定します。
1～31日の範囲で、1日単位で選択可能です。
初期値:7日</td></tr>
</table>

2.8.2 ログアナライザを利用するための準備をする

2.8.2.1 ログの転送をスケジュールする

管理サーバからログアナライザサーバへのログの転送は、夜間など、クライアント(CT)の利用者が少ない時間帯に実施します。定期的に実施できるように、OSのタスク機能を利用します。

2.8.2.1.1　管理サーバでログ取得期間を設定する

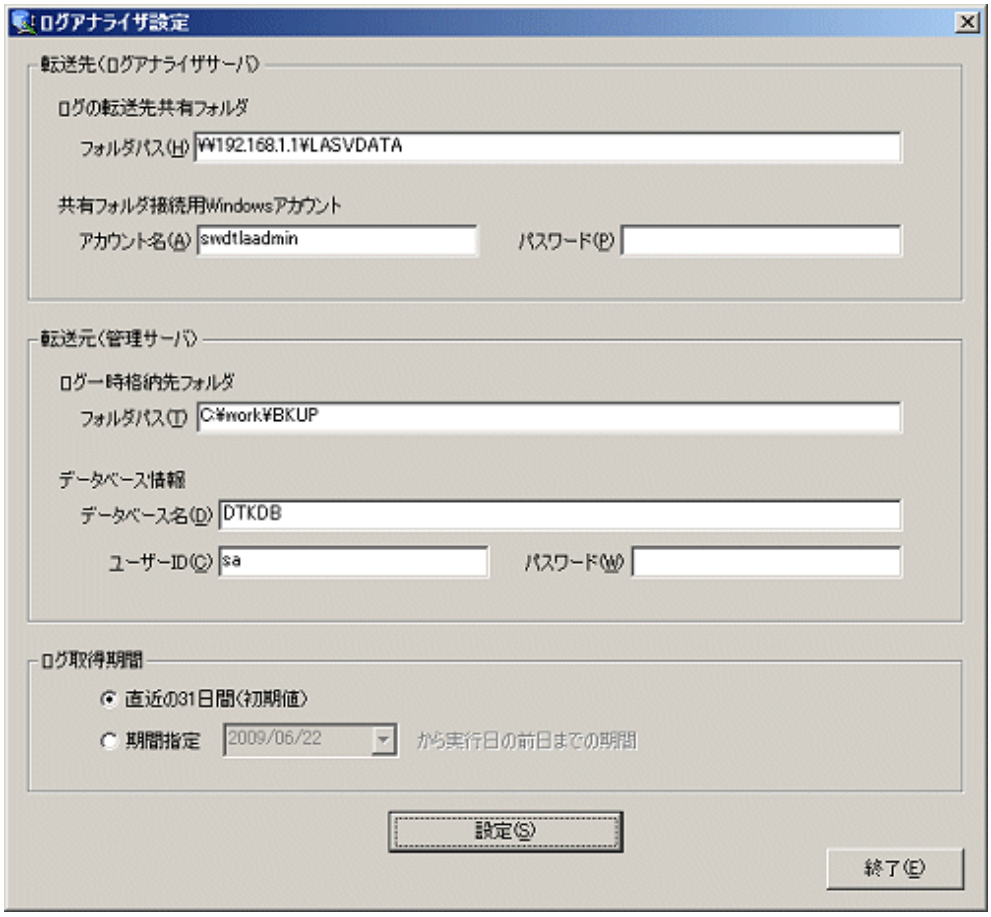
管理サーバからログアナライザサーバへログを転送する場合、以下の3項目を設定する必要があります。

- 転送先(ログアナライザサーバ)
- 転送元(管理サーバ)
- ログ取得期間

転送先と転送元は、導入時に管理者情報を転送するために、設定済みです。設定項目については、“Systemwalker Desktop Keeper 導入ガイド”の“管理サーバ/統合管理サーバ上で、ログアナライザ環境を設定する”を参照してください。

ここでは、ログ取得期間の設定について説明します。

1. [スタート]メニューから[プログラム]-[Systemwalker Desktop Keeper]-[サーバ]-[ログアナライザ設定]を選択し、[ログアナライザ設定]画面を起動します。



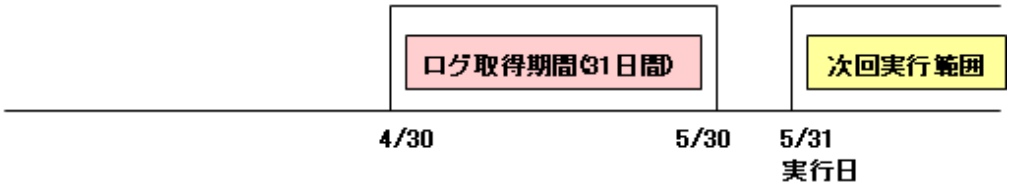
2. [ログ取得期間]で、データ取得開始日を設定します。

ログ取得期間の設定値と、転送されるログの関係

ログの転送は、タスクの実行日(データ転送コマンド実行日)の前日までのログを対象とします。
ログ取得期間が対象とする日時は、管理サーバにログが登録された日時です。クライアント(CT)での操作ログ発生日時ではありません。
以下に、ログ取得期間の設定値と、転送されるログの範囲について説明します。

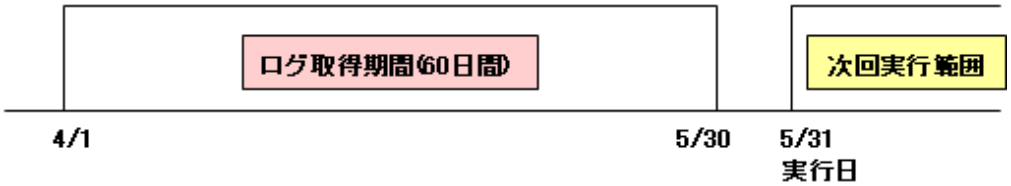
ー ログ取得期間が[直近の31日間(初期値)]の場合

タスクの実行日(データ転送コマンド実行日)の前日から31日前のログデータを転送します。
以下に、5/31にタスクを実行した場合の例を示します。



ー ログ取得期間が[期間指定]の場合

タスクの実行日の前日から、ログ取得期間に指定された日までのログデータを転送します。
以下に、ログ取得期間に2007/04/01を指定し、5/31にタスクを実行した場合の例を示します。



ログ取得期間は、管理サーバ/統合管理サーバ上のログのうち、ログアナライザサーバに移入する開始時点を指定するものです。
したがって、運用を開始してからは、ログ取得期間を再設定する必要はありません。

2.8.2.1.2　管理サーバで転送スケジュールを設定する

管理サーバからログアナライザサーバへ、ログやユーザー情報を転送します。

この場合、管理サーバのOSのタスク機能に、TRANS.bat(ログアナライザサーバへのデータ転送)コマンドを登録し、定期的に転送できるように設定します。なお、転送処理は毎日実施することを推奨しています。以下の設定例では、毎日転送する場合を想定して説明しています。

TRANS.bat(ログアナライザサーバへのデータ転送)コマンドを使用してログを転送する場合、共有フォルダにアクセスしているユーザーがいない状態にする必要があります。
共有フォルダに対して他のユーザーでアクセスしていた場合は、ネットワークの切断またはログオフを行う必要があります。

約500万件のログの転送に、およそ25分かかります(ただし、処理時間例は参考値です。PCの性能や、ネットワーク状態などの要因で変化します)。

注意

ログの転送は、クライアント(CT)の利用者が少ない時間帯に実行してください

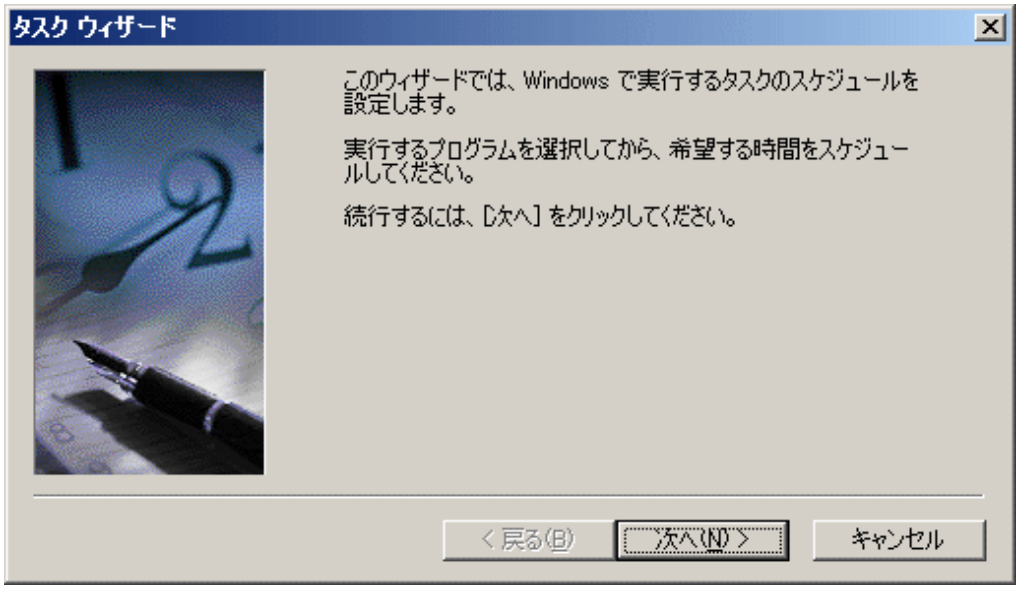
TRANS.batを実行した場合、ログデータの保存や送信処理を実行している間、管理サーバの以下のサービスが停止します。したがって、管理サーバで管理するクライアント(CT)の利用者が少ない時間帯に実行してください。

- SWLevelControlService
- SWServerService

以下に、設定手順を説明します。

Windows Server® 2008以外での登録方法

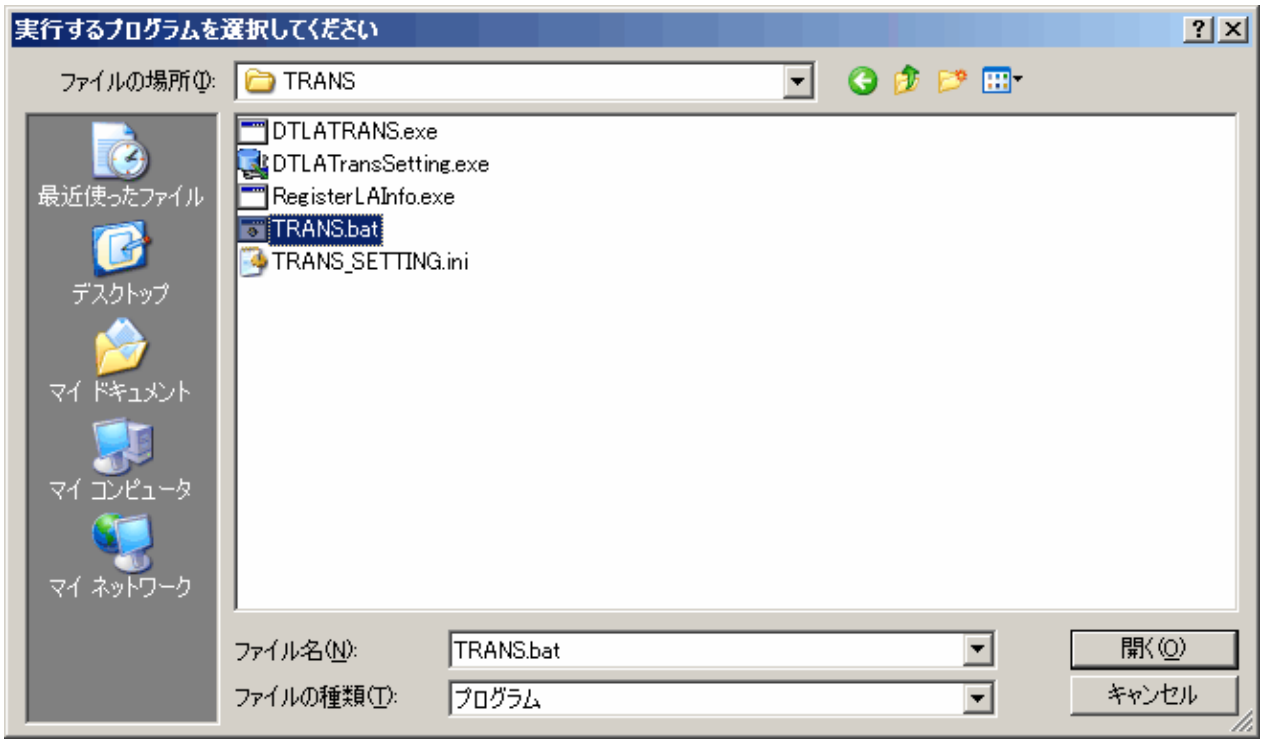
1. [スタート]メニューから[設定]－[コントロールパネル]－[タスク]を選択し、[スケジュールされたタスクの追加]をダブルクリックします。
   →以下の画面が表示されます。[次へ]ボタンをクリックしてください。



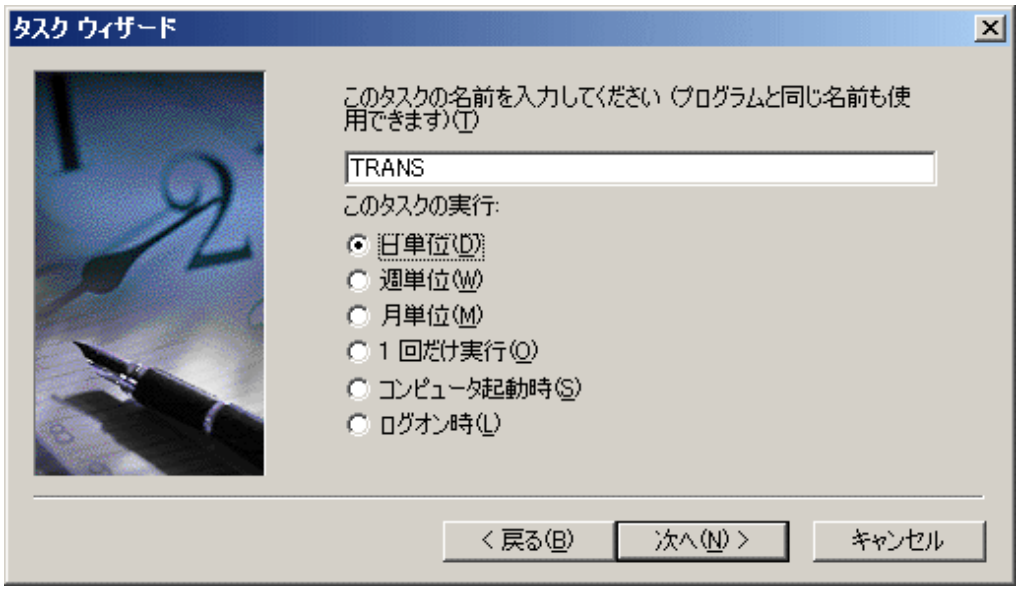
2. タスクウィザードの実行するプログラムの選択画面で、[参照]ボタンをクリックします。

3. 以下に格納されているバッチコマンド「TRANS.bat」を選択します。

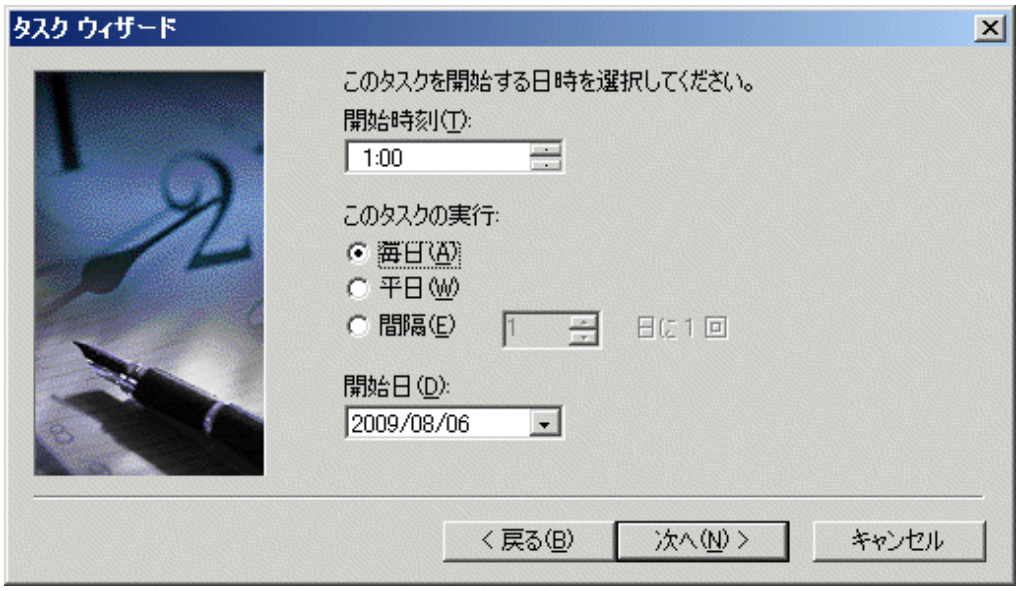
```
[Systemwalker Desktop Keeperインストールフォルダ]¥LogAnalyzer¥TRANS¥TRANS.bat
```



4. タスクの名前を入力し、タスクの実行で[日単位]を選択します。



5. タスクの開始時刻、実行間隔、開始日を設定します。開始時刻は夜間など、クライアント(CT)の利用者が少ない時間帯を指定します。実行間隔は[毎日]を選択します。

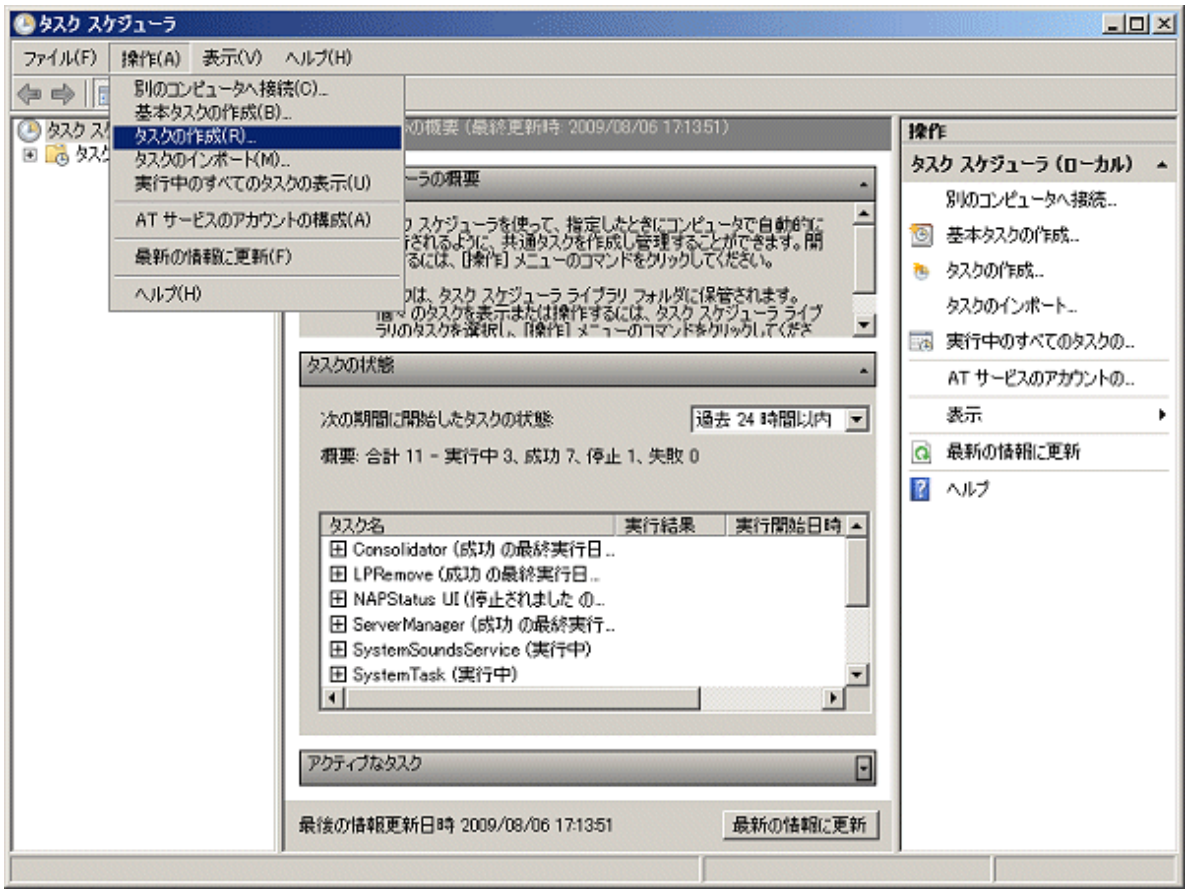


6. 実行時のユーザー名とパスワードを登録します。
Administrator権限のあるユーザー名とパスワードを指定してください。

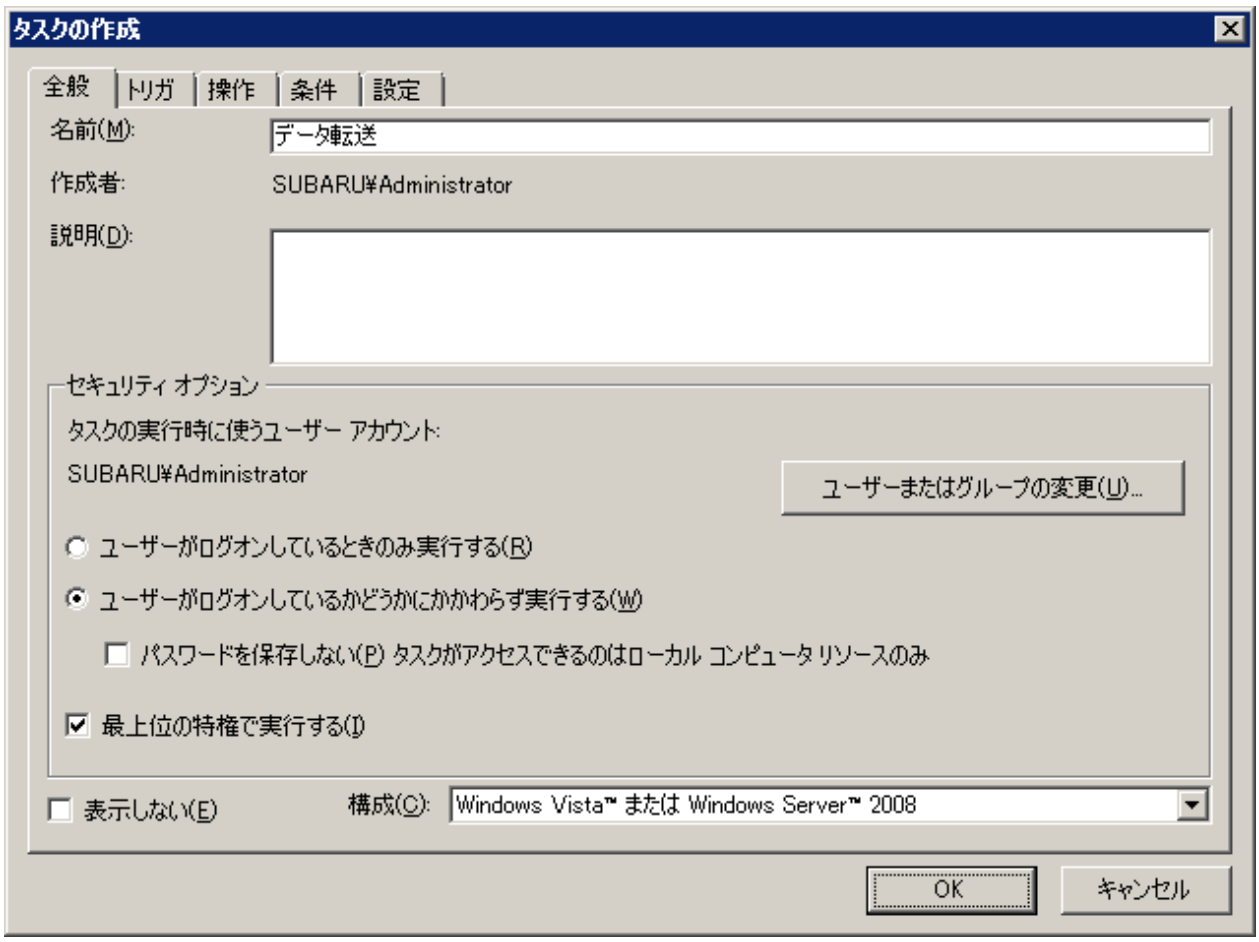
7. [完了]ボタンをクリックします。

Windows Server® 2008での登録方法

1. [スタート]メニューから[すべてのプログラム]-[アクセサリ]-[システム ツール]-[タスク スケジューラ]を選択します。
   →[タスク スケジューラ]画面が表示されます。
2. [操作]メニューから[タスクの作成]を選択します。



→[タスクの作成]画面が表示されます。



3. [全般]タブを選択し、以下の情報を設定して、[OK]ボタンをクリックします。

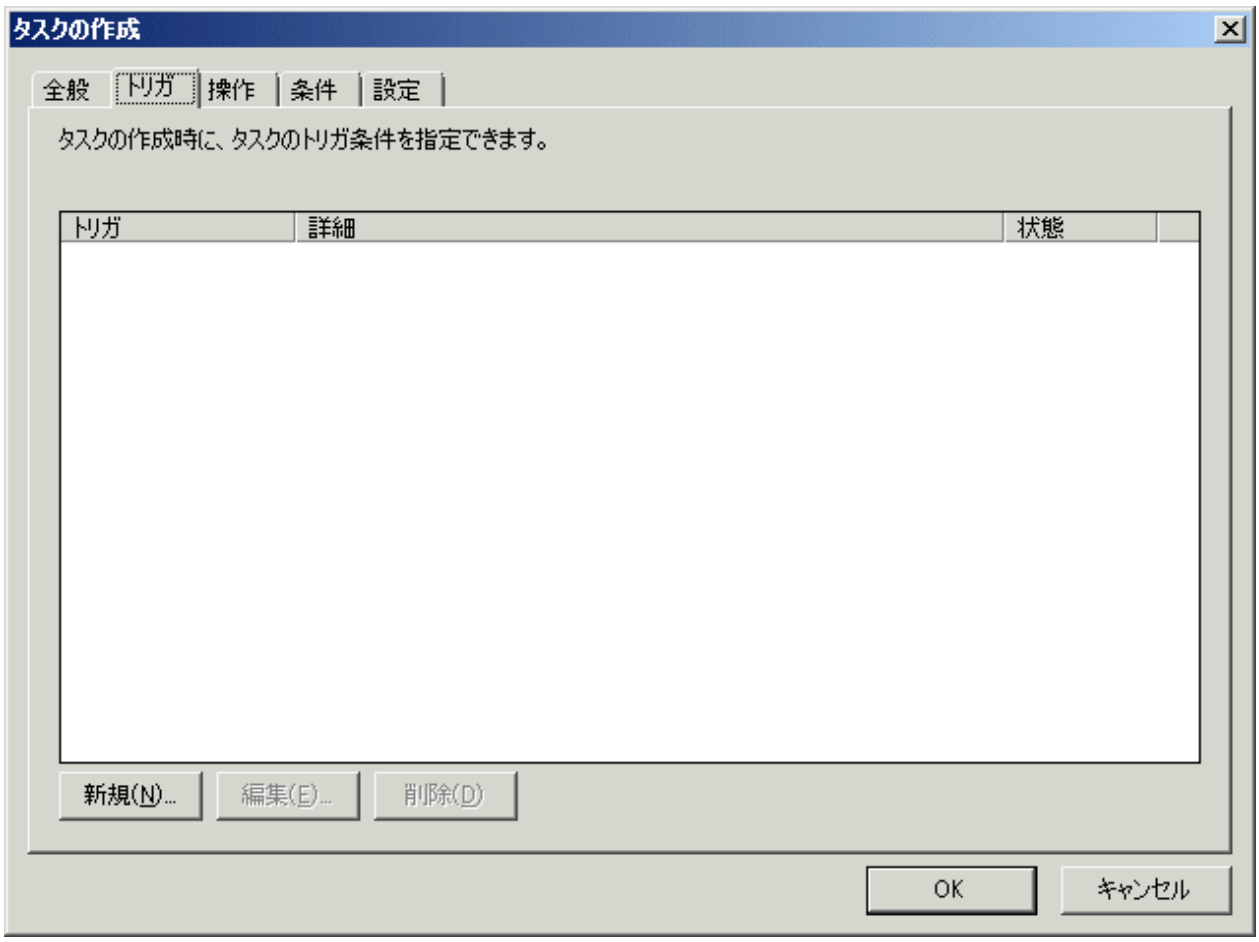
   ー [名前]に、登録するタスク名を設定します。

   ー [タスクの実行時に使うユーザーアカウント]にAdministrator権限のあるユーザーを設定します。[ユーザーまたはグループの変更]ボタンをクリックして設定します。

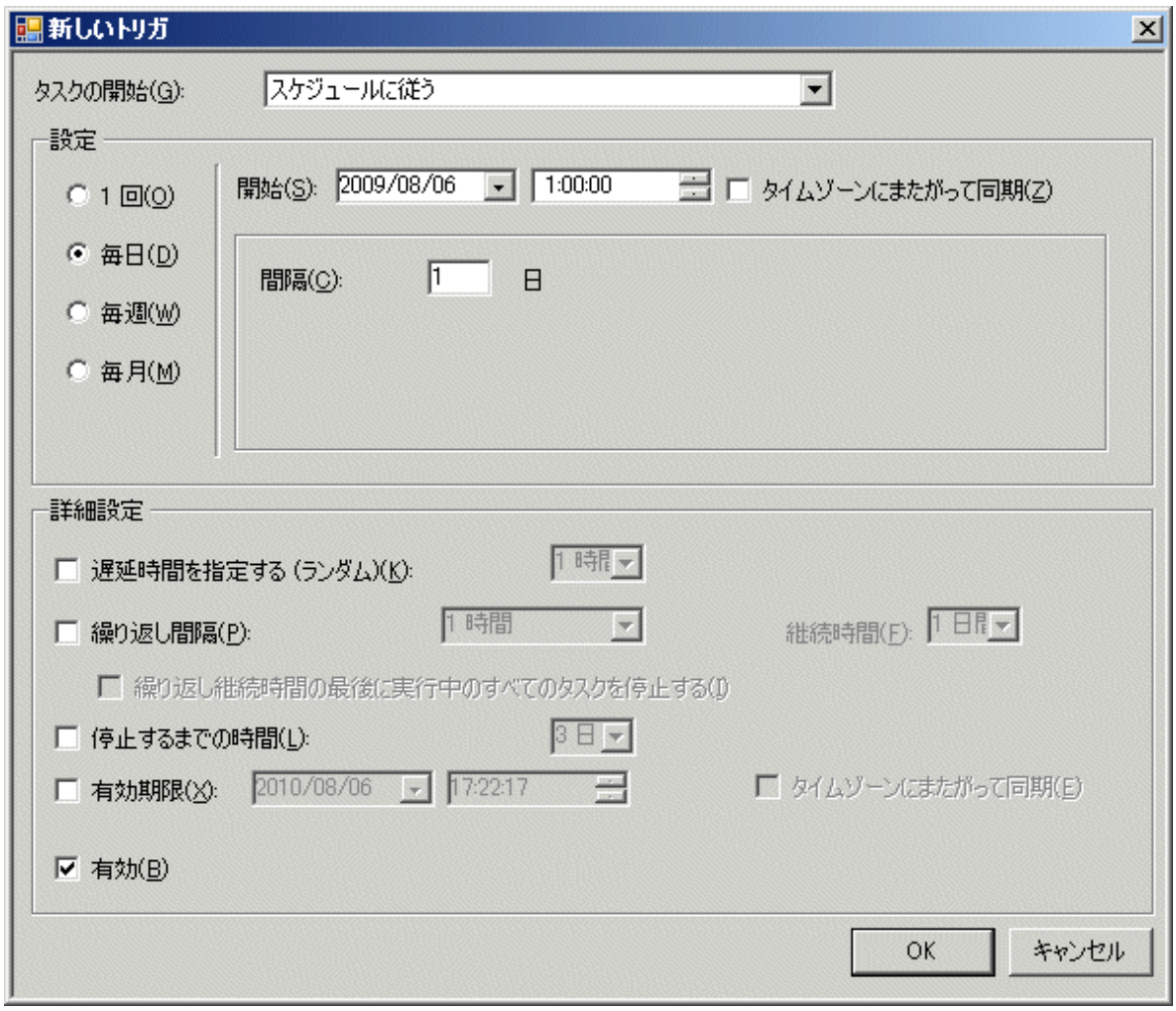
   ー [ユーザーがログオンしているかどうかにかかわらず実行する]を選択します。

   ー [最上位の特権で実行する]にチェックをつけます。

4. [トリガ]タブを選択し、[新規]ボタンをクリックします。



→[新しいトリガ]画面が表示されます。



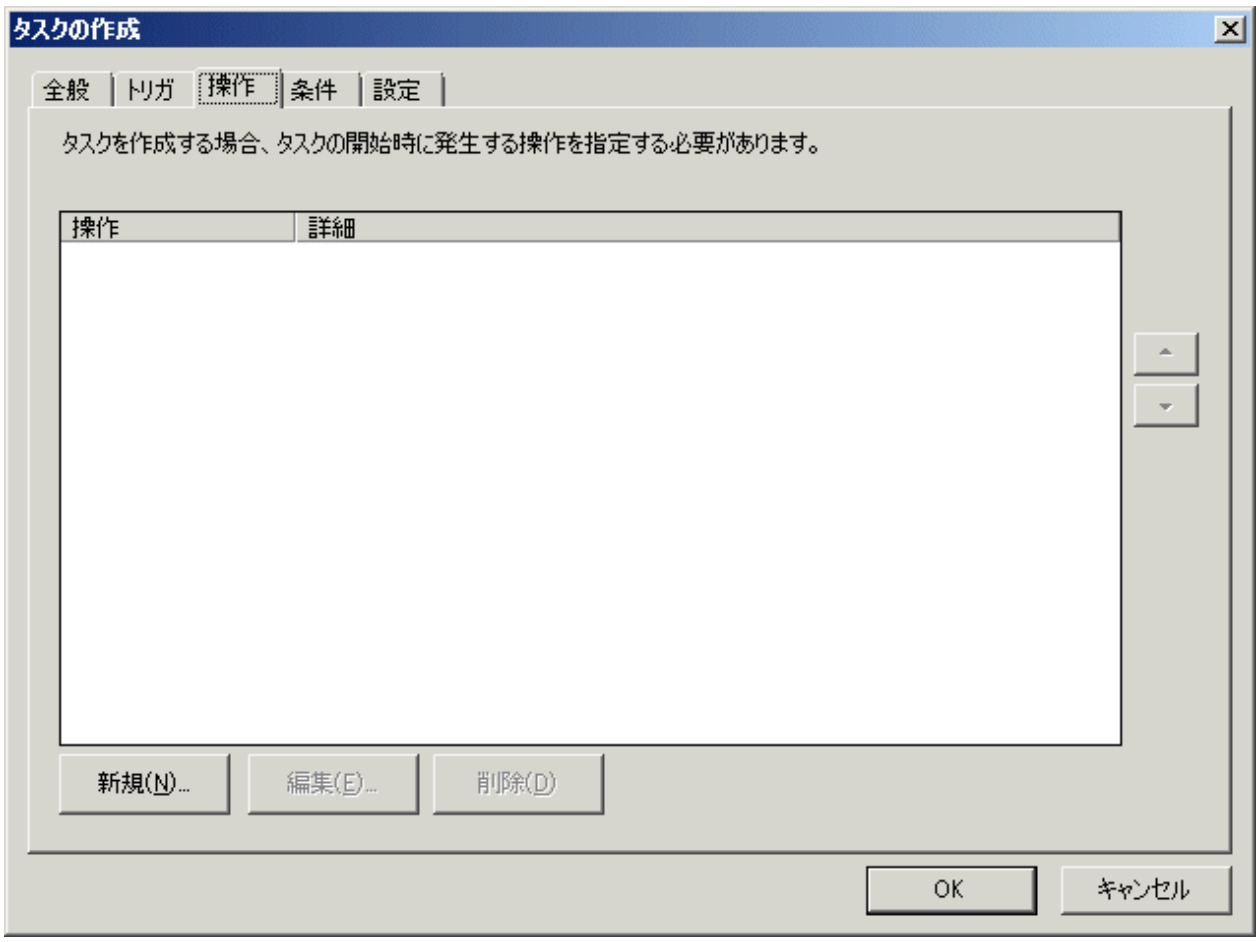
5. [設定]において以下の情報を設定し、[OK]ボタンをクリックします。

   ー [毎日]を選択します。

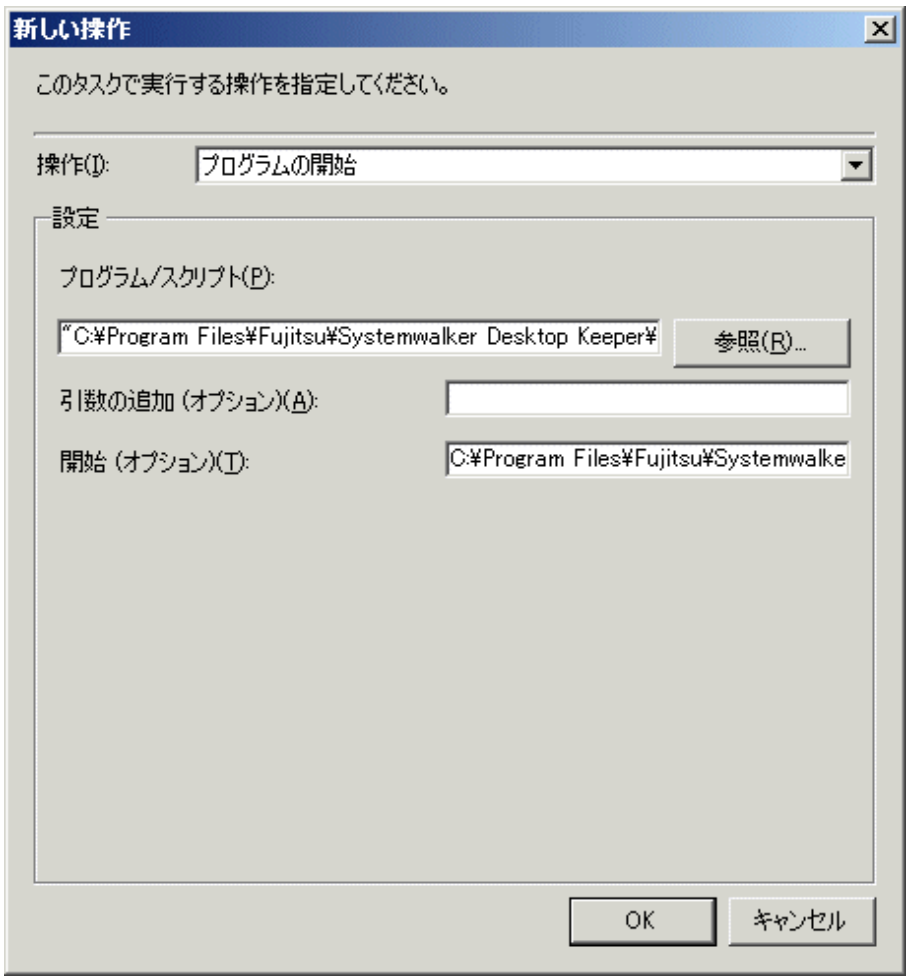
   ー [開始]に開始年月日と時刻を設定します。開始時刻は夜間など、クライアント(CT)の利用者が少ない時間帯を指定します。

   ー [間隔]に1日を設定します。

6. [操作]タブを選択し、[新規]ボタンをクリックします。



→[新しい操作]画面が表示されます。



7. [設定]において以下の情報を設定し、[OK]ボタンをクリックします。

   ー [プログラム/スクリプト]:以下に格納されているバッチコマンド「TRANS.bat」をフルパスで指定します。パスはダブルクォーテーションで囲みます。

   ```
   "[Systemwalker Desktop Keeperインストールフォルダ]¥LogAnalyzer¥TRANS¥TRANS.bat"
   ```

   ー [[開始(オプション)]:[プログラム/スクリプト]で指定した「TRANS.bat」のあるフォルダのフルパスを指定します。パスは、ダブルクォーテーションで囲まないでください。

8. [タスクの作成]画面で[OK]ボタンをクリックします。

参考

ログの転送は手動でもできます

1. コマンドプロンプトで以下のコマンドを実行し、製品をインストールしたフォルダの“TRANS”フォルダに移動します。

   ```
   cd [Systemwalker Desktop Keeperインストールフォルダ]¥LogAnalyzer¥TRANS [Enter]
   ```

2. 以下のバッチコマンドを実行し、ログアナライザサーバへログデータをCSVファイルに保存して送信します。

   ```
   TRANS.bat [Enter]
   ```

   コマンドプロンプトで実行した場合、処理終了後にコマンドプロンプト画面も自動的に閉じられます。コマンドプロンプト画面を残したい場合は以下のように実行してください。

```
cmd /c TRANS.bat [Enter]
```

2.8.2.1.3　ログアナライザサーバのデータベースにログを格納する

管理サーバから転送されたログやユーザー情報を、ログアナライザサーバのデータベースに格納します。

この場合、ログアナライザサーバのOSのタスク機能に、DTTOOLEX.EXE(ログアナライザサーバへのデータ移入・削除)コマンドを登録し、定期的にデータベースに格納できるように設定します。なお、データベースへのログ格納処理は毎日実施することを推奨しています。以下の設定例では、毎日格納する場合を想定して説明しています。

DTTOOLEX.EXEコマンドが実行されると、ログデータの移入と同時に、移入したログの集計を行い、集計結果を更新します。
このとき、DTTOOLEX.EXE実行前と実行後の集計結果の差分を、ログとして出力します。

・【ログの出力先】

[ログアナライザサーバインストールフォルダ]¥bin¥batchnavi¥update0.log

ファイルサイズが10MBを超えた場合、update0.logはupdate1.logになり、update0.logが新たに生成されます(最大でupdate4.logまで順次生成されます)。最新の情報は、常にupdate0.logに記録されます。

・【ログの出力内容】

```
----------------------------------------------------------------------------------
集計実施日時 2008/04/21 01:00:00 の更新情報出力
開始
20080421 操作発生日20080408 情報漏洩(0,0,0,0,0) 端末利用(0,0,20) 違反操作(0,0,0,0,0) 印刷量監査(0)
20080421 操作発生日20080409 情報漏洩(0,0,0,0,0) 端末利用(0,0,31) 違反操作(1,0,1,0,0) 印刷量監査(2)
終了
----------------------------------------------------------------------------------
```

上記は2008年4月21日に移入したデータを集計した結果、4月8日と4月9日に操作のあったログの件数を更新したことを示し、更新したその差分件数を( )内に表示しています。
( )内の数字は、以下のように各ログ(※)の差分件数です。

ー　情報漏洩(ファイル持出し、ファイル操作、印刷操作回数、印刷操作ページ数、宛先別メール送信)

ー　端末利用(URL付きウィンドウタイトル取得、宛先別メール送信、アプリケーション起動)

ー　違反操作(アプリケーション起動禁止、印刷禁止、ログオン禁止、PrintScreenキー禁止、メール添付禁止)

ー　印刷量監査(印刷操作回数)

※) レポート出力ツールで出力したレポートに表示されるログです(情報漏洩だけは、Webコンソールの情報漏洩予防診断画面でも表示されます)。

約1000万件のログを新たに移入する場合、およそ80分かかります(ただし、処理時間例は参考値です。PCのCPU、メモリ、ディスク性能、他のアプリケーションの動作状況などの要因で変化します)。

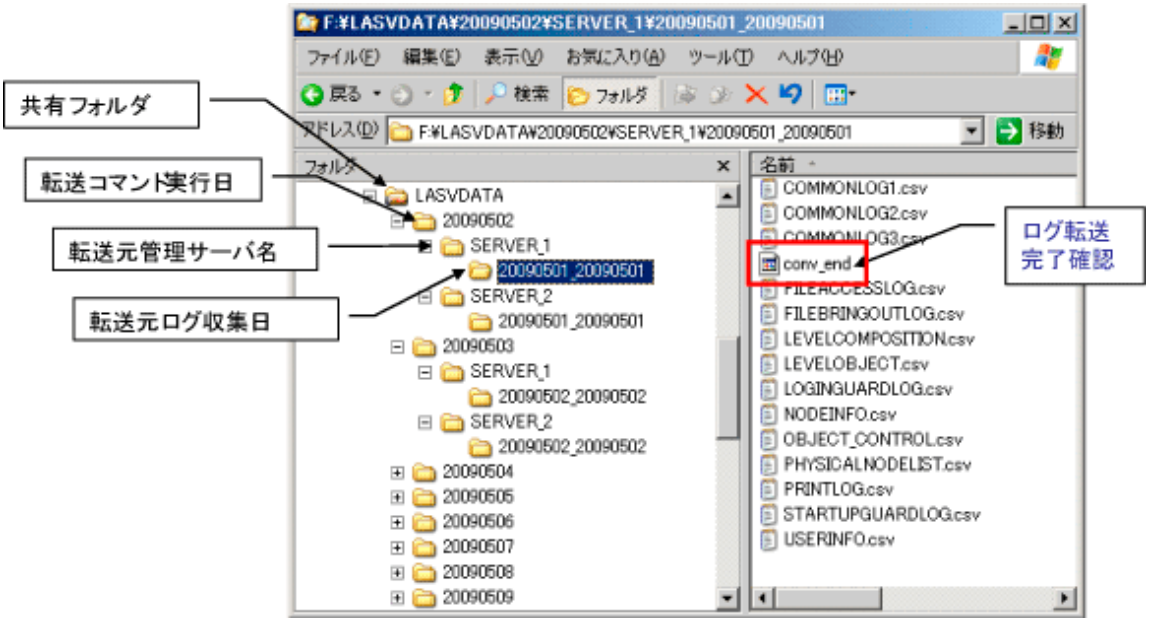
注意

ディスク容量を確保するため、不要になったログデータのCSVファイルは、定期的に外部媒体へ退避してください

管理サーバからログアナライザサーバへ送信されたログデータのCSVファイルは、ログアナライザサーバのデータベースへ格納されても、ログアナライザサーバのディスク上に残り続けます。

共有フォルダが枯渇した場合、管理サーバ/統合管理サーバからログの転送に失敗します。このため定期的に共有フォルダの容量確認を行い、分析・集計済みのログについては退避した上で、削除を行ってください。

ログアナライザサーバの共有フォルダは以下のような構成になっています。



なお、ログアナライザサーバでの分析・集計が完了していないログは、退避・削除できません。

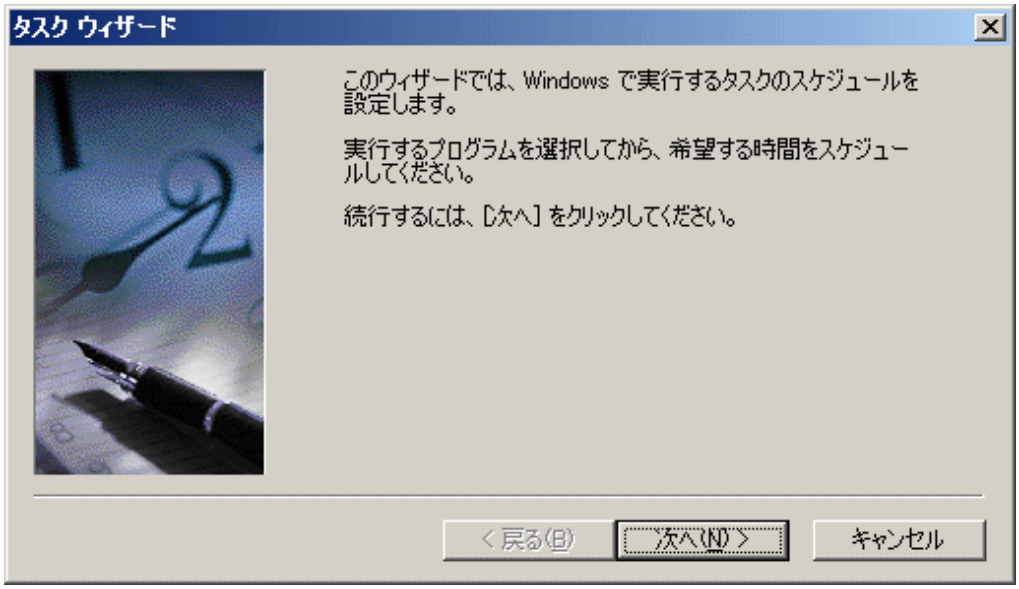
転送元ログ収集日のフォルダの配下に“ログ転送完了確認用ファイル(conv_end) ”が作成されているフォルダは、ログ分析・集計が完了し、ログアナライザサーバ上のデータベースに格納済みです。

上図の“転送コマンド実行日”フォルダ配下の“転送元管理サーバ名”フォルダに存在するすべての“転送元ログ収集日フォルダに“ログ転送完了確認用ファイル(conv_end) ”が作成されている場合に退避・削除できます。“転送コマンド実行日”フォルダ単位で、退避および削除を実施してください。

以下に、設定手順を説明します。

Windows Server® 2008以外での登録方法

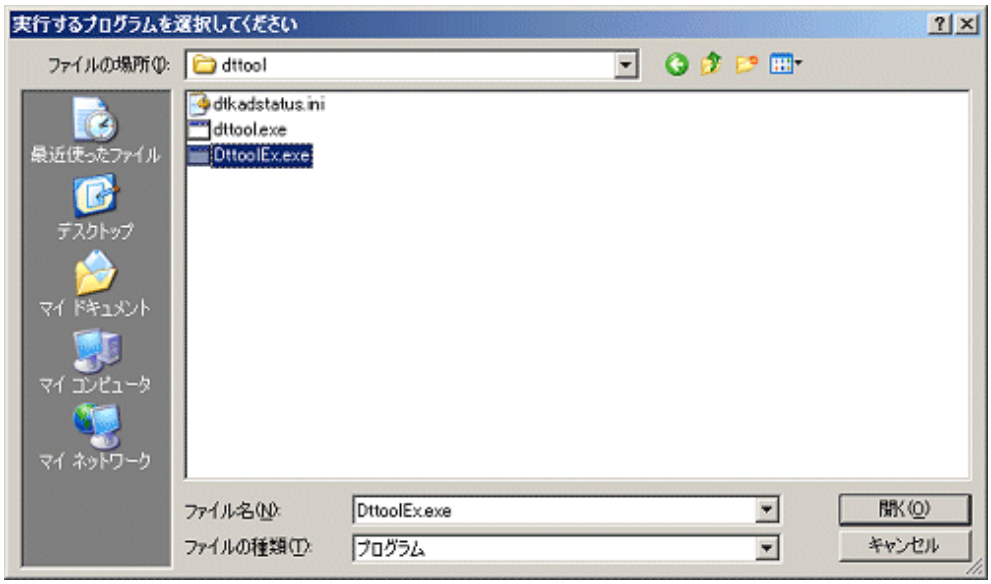
1. [スタート]－[設定]－[コントロールパネル]－[タスク]と開き、[スケジュールされたタスクの追加]をダブルクリックします。
   →以下の画面が表示されます。[次へ]ボタンをクリックしてください。



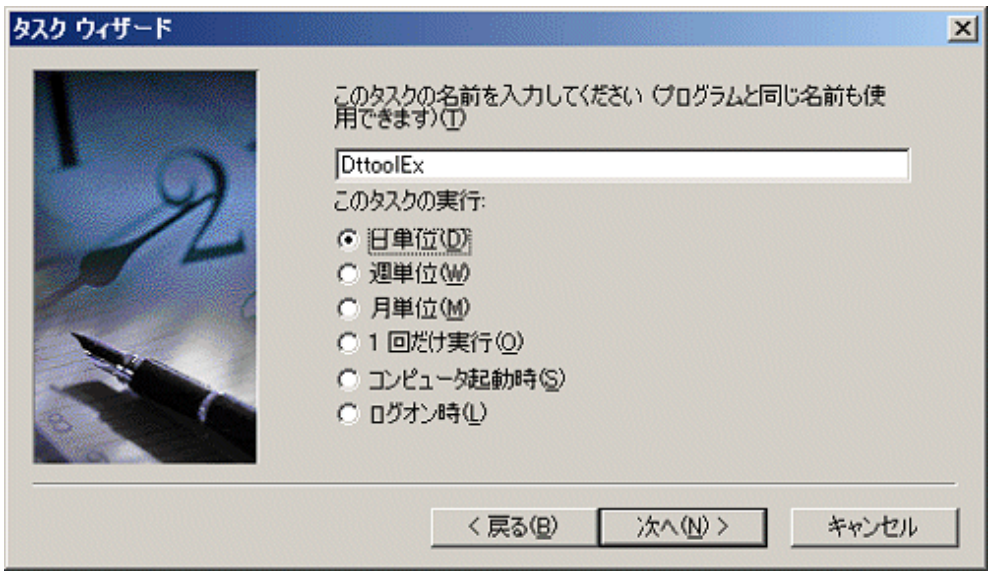
2. タスクウィザードの実行するプログラムの選択画面で、[参照]ボタンをクリックします。

3. 以下に格納されているコマンド「DTTOOLEX.EXE」を選択します。

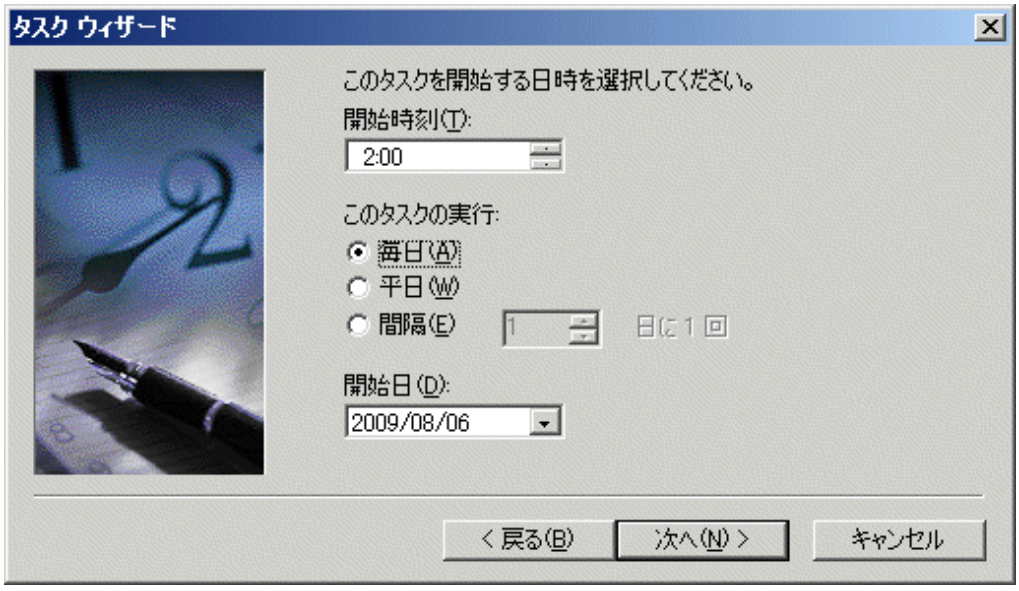
[ログアナライザサーバインストールフォルダ]¥bin¥dttool¥DttoolEx.exe



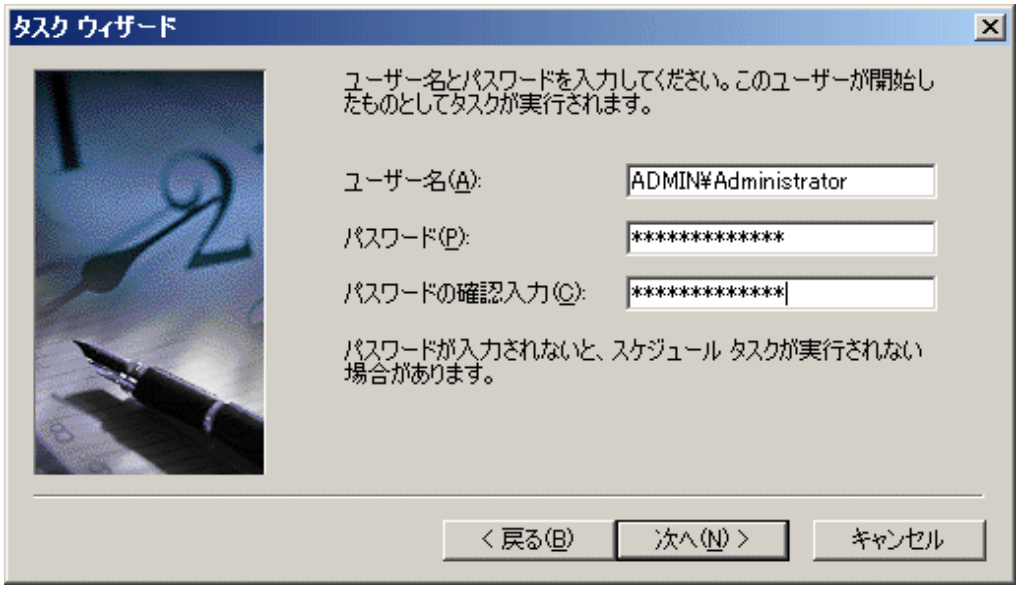
4. タスクの名前を入力し、タスクの実行で[日単位]を選択します。



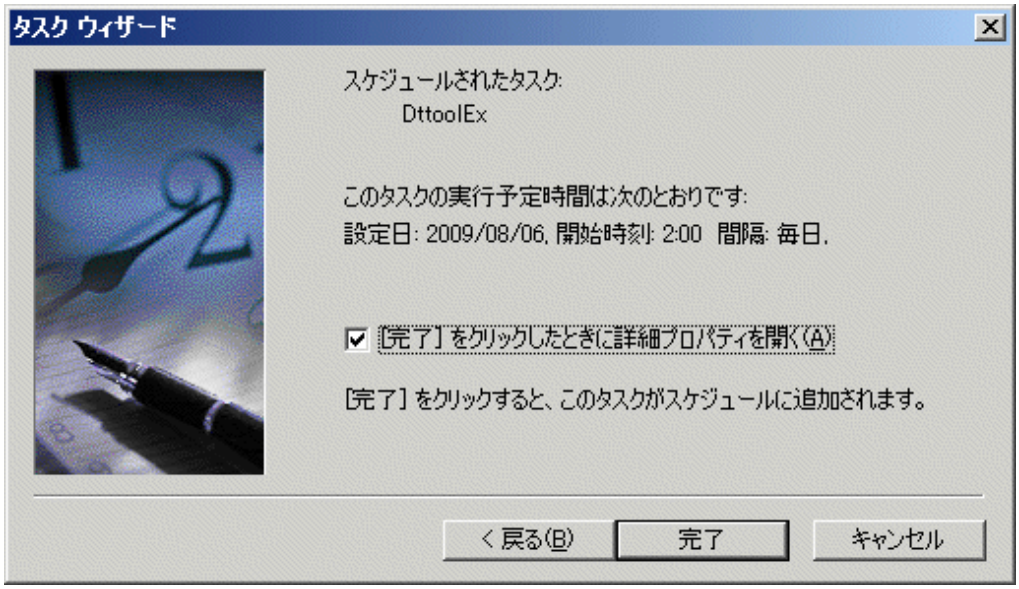
5. タスクの開始時刻、実行間隔、開始日を設定します。開始時刻はデータ転送コマンドのタスク開始時間より遅く設定し、データ転送コマンドの実行終了後にタスクが実行するようにします。実行間隔は[毎日]を選択します。



6. 実行時のユーザー名とパスワードを登録します。
   ログアナライザユーザー名とパスワードを指定してください。



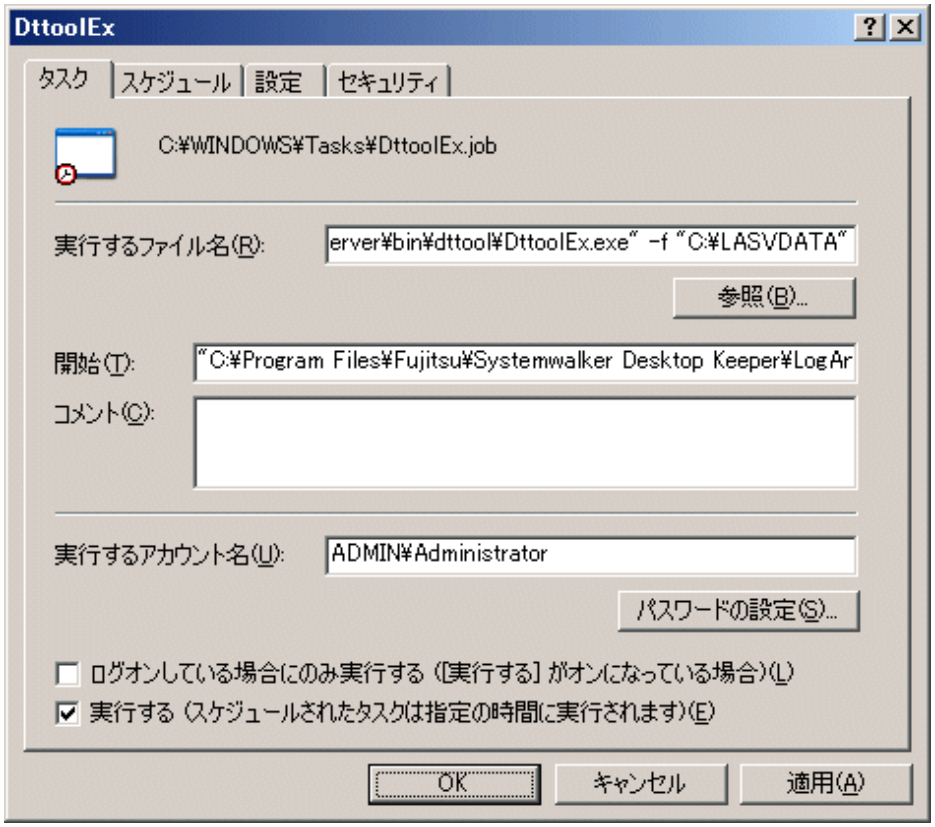
7. [[完了]をクリックしたときに詳細プロパティを開く]を選択し、[完了]ボタンをクリックします。



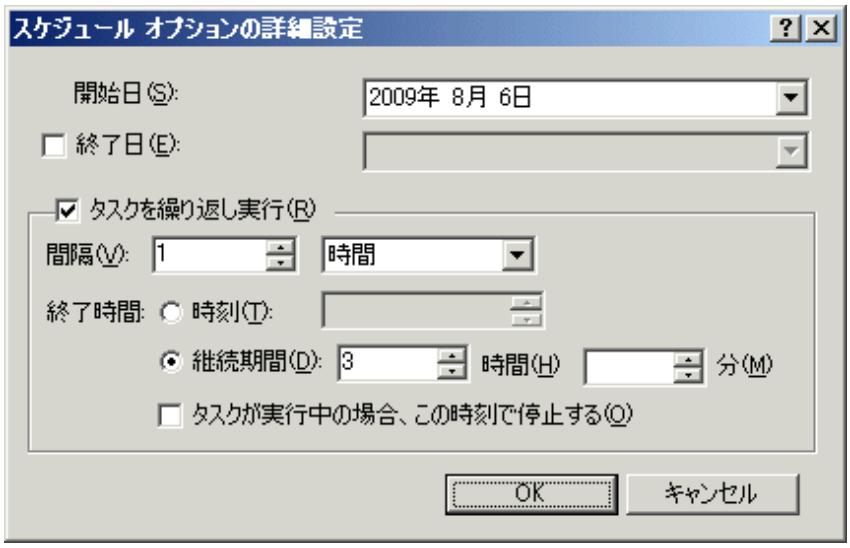
8. [タスク]タブの[実行するファイル名]に設定されているパスの後に以下のオプションを追加します。

```
-f［ログ転送先共有フォルダのパス］
```

※[ログ転送先共有フォルダのパス]はUNC形式ではなくローカルパス形式で指定します。また必ずダブルクォーテーションで囲んでください。



9. [スケジュール]タブをクリックし、[詳細設定]ボタンをクリックします。
10. [タスクを繰り返し実行]をチェックし、[間隔]、[継続期間]を設定します。

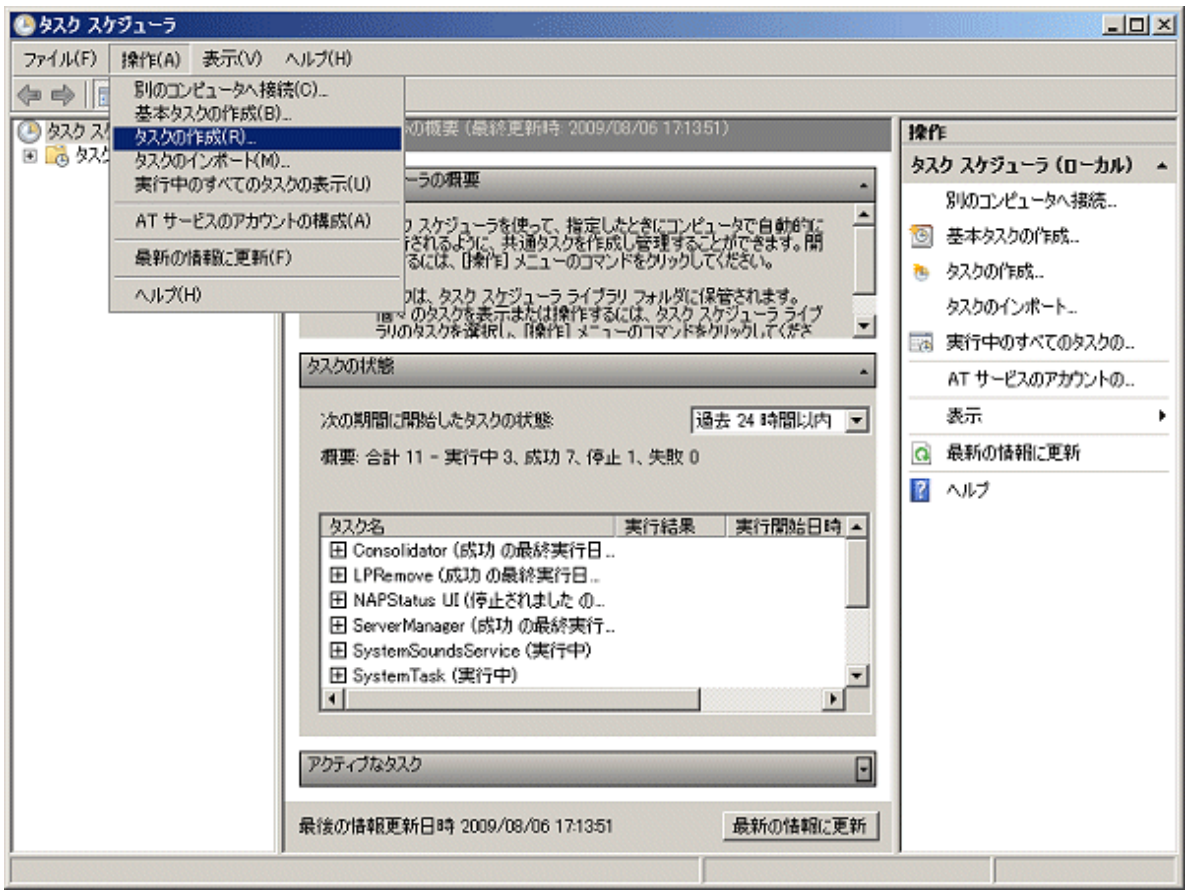


Windows Server® 2008での登録方法

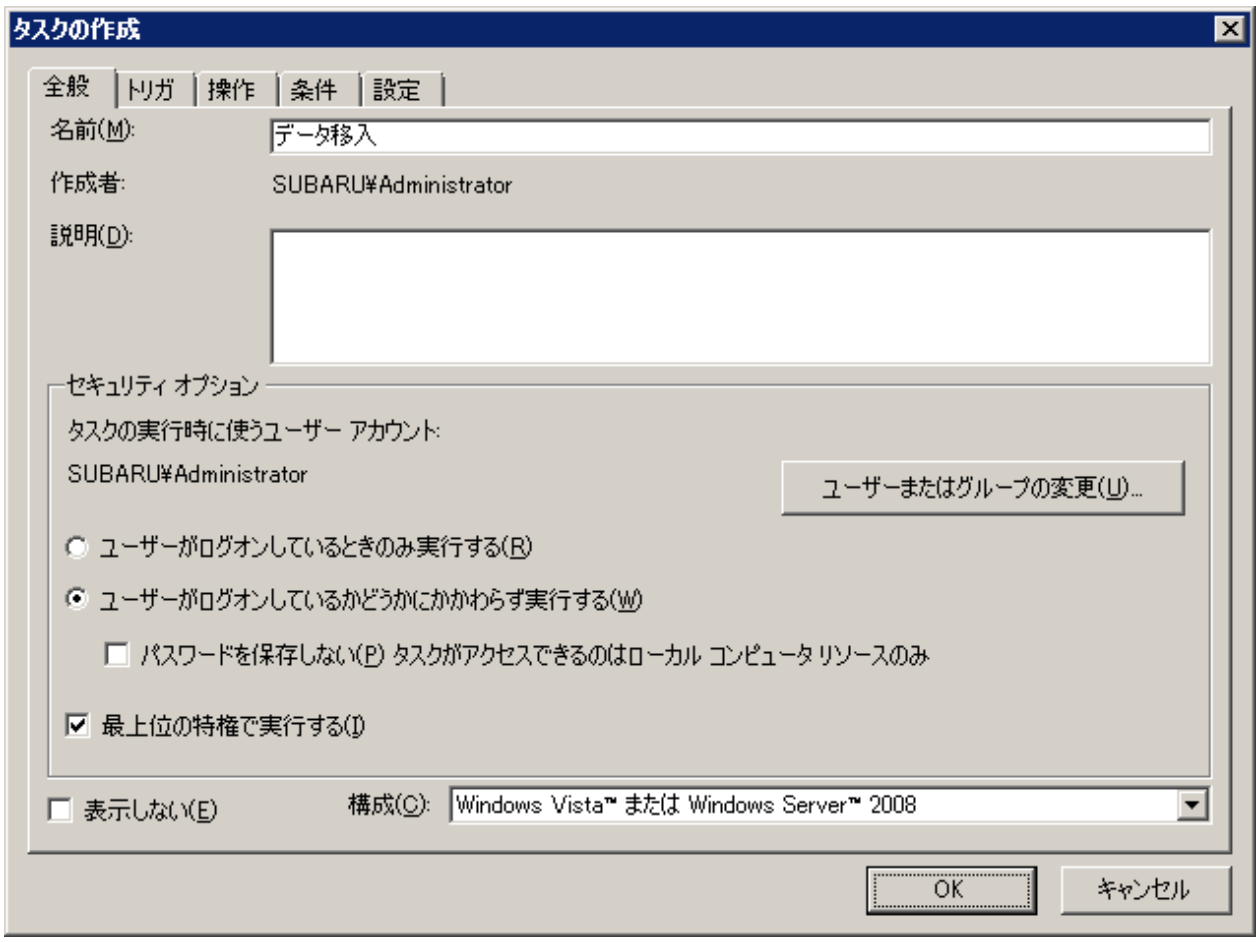
1. [スタート]メニューから[すべてのプログラム]-[アクセサリ]-[システム ツール]-[タスク スケジューラ]を選択します。

   →[タスク スケジューラ]画面が表示されます。

2. [操作]メニューから[タスクの作成]を選択します。



→[タスクの作成]画面が表示されます。



3. [全般]タブを選択し、以下の情報を設定して、[OK]ボタンをクリックします。

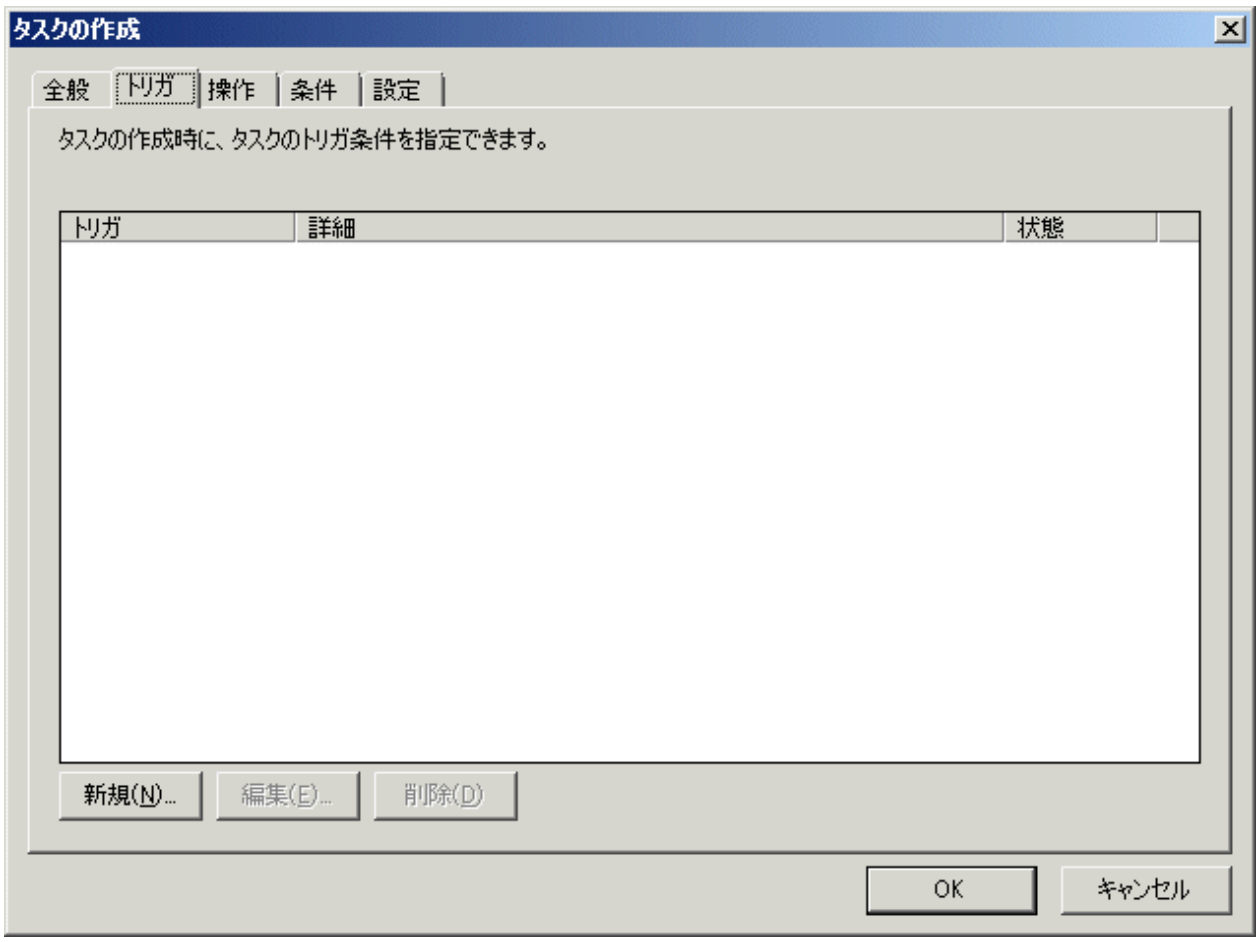
   ー [名前]に、登録するタスク名を設定します。

   ー [タスクの実行時に使うユーザーアカウント]にログアナライザユーザーを設定します。[ユーザーまたはグループの変更]ボタンをクリックして設定します。

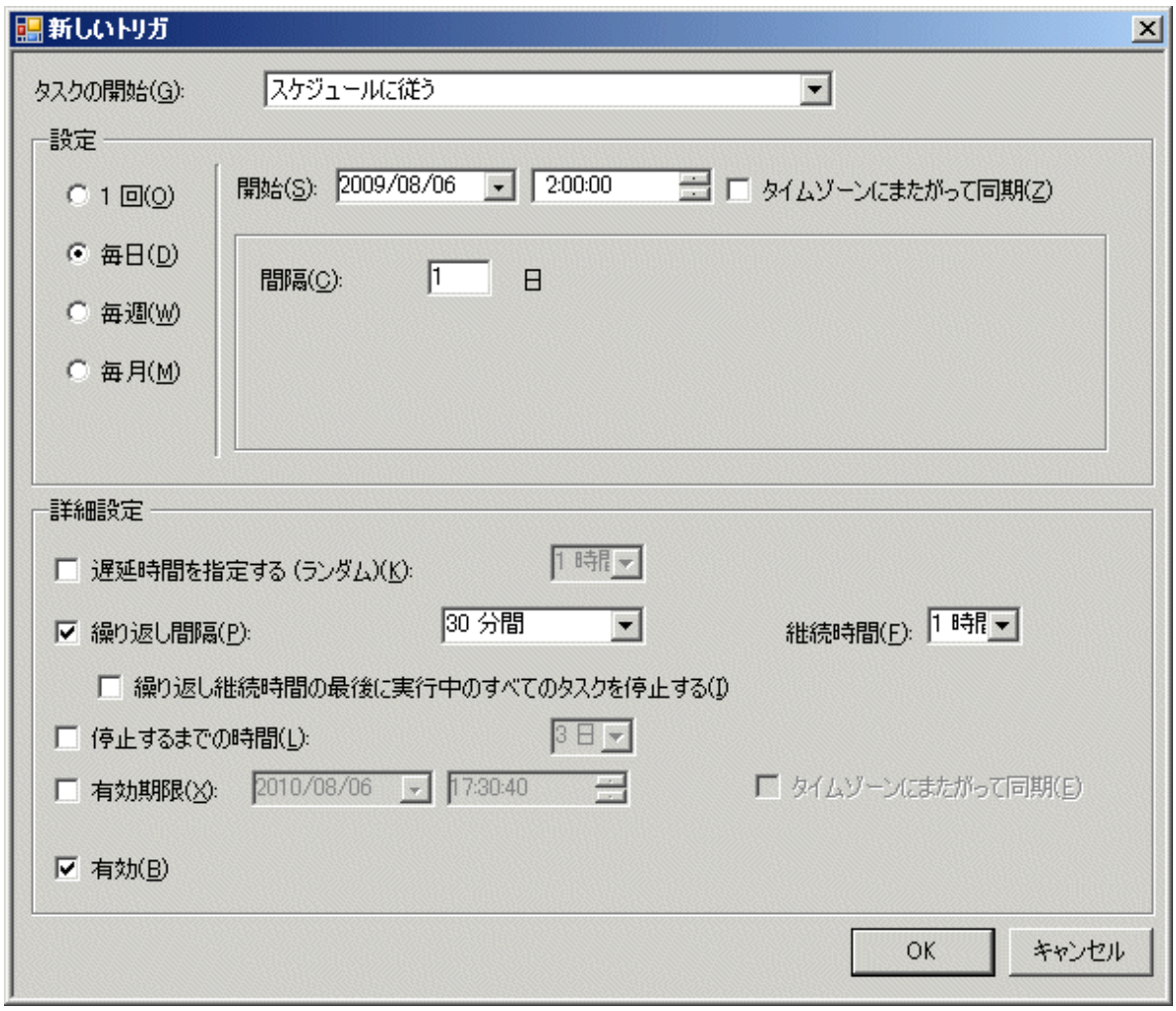
   ー [ユーザーがログオンしているかどうかにかかわらず実行する]を選択します。

   ー [最上位の特権で実行する]にチェックをつけます。

4. [トリガ]タブを選択し、[新規]ボタンをクリックします。



→[新しいトリガ]画面が表示されます。



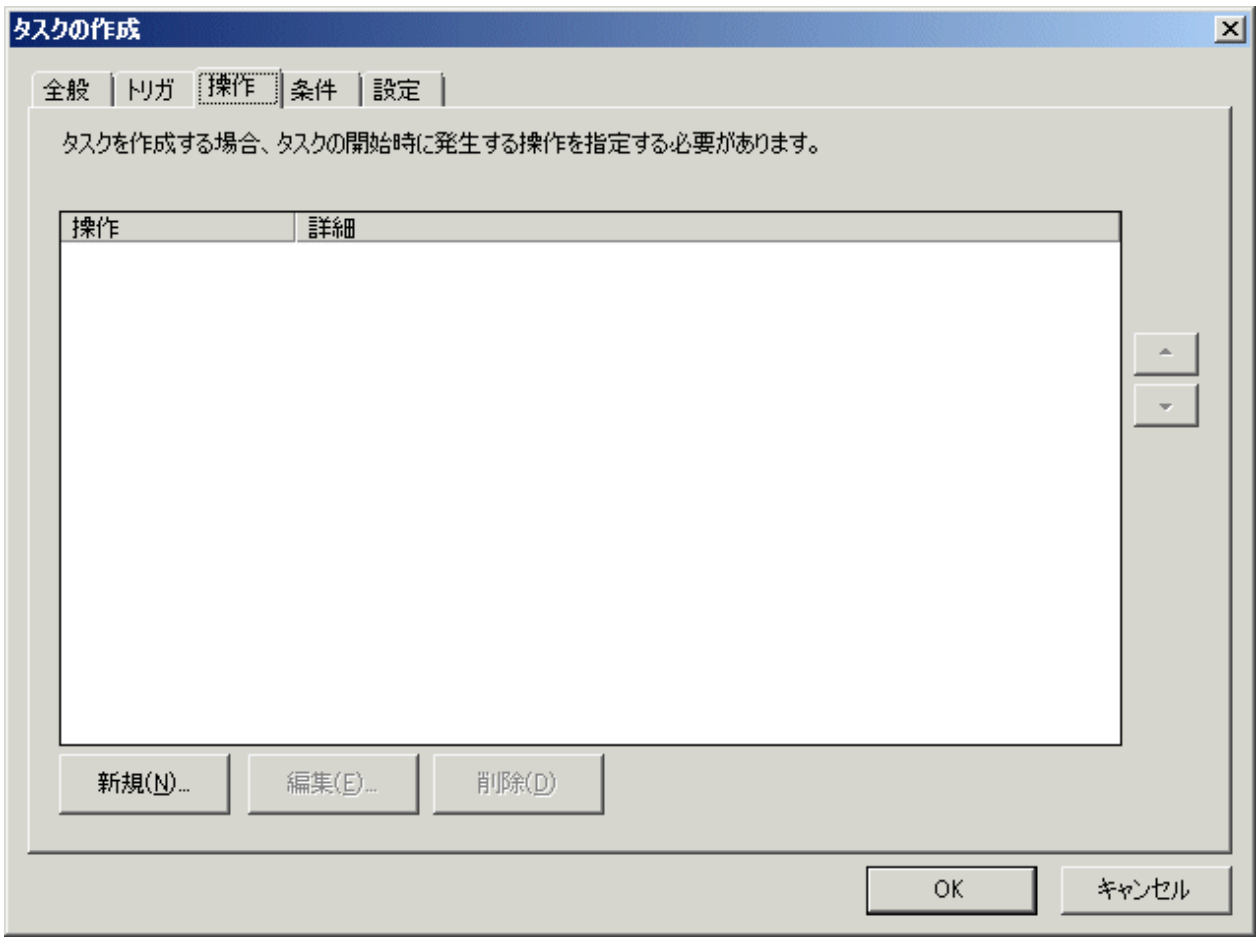
5. [設定]において以下の情報を設定し、[OK]ボタンをクリックします。

   ー [毎日]を選択します。

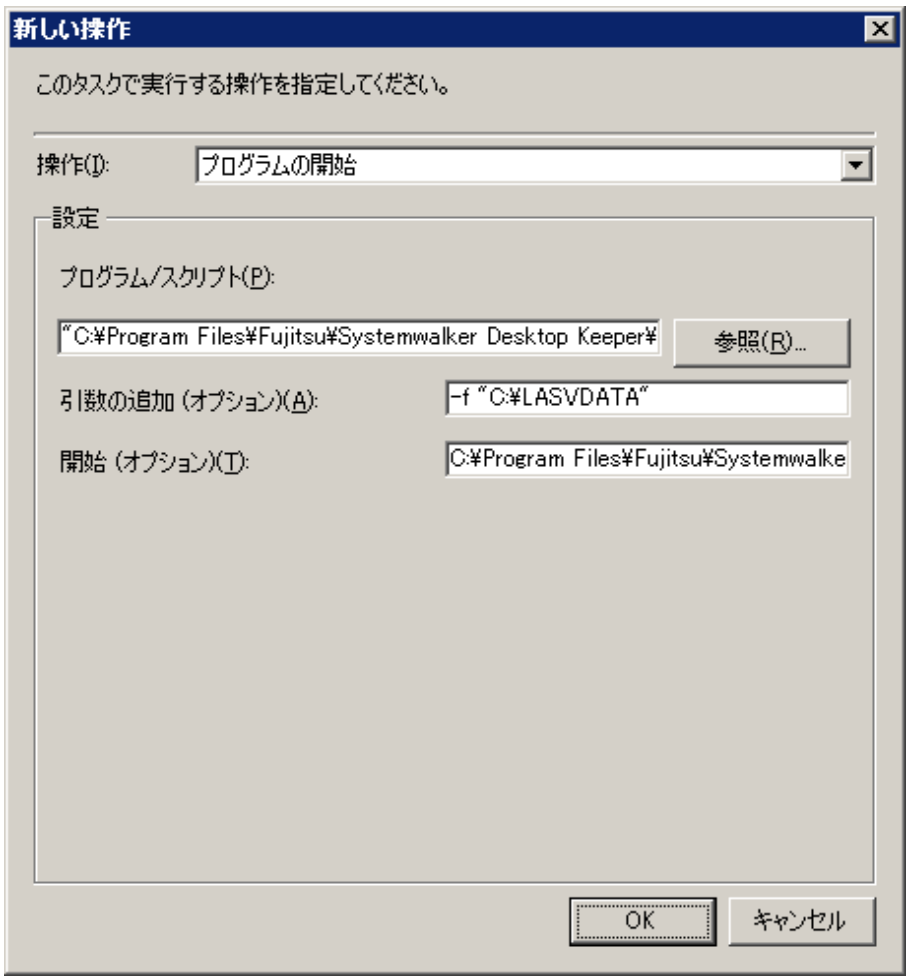
   ー [開始]に開始年月日と時刻を設定します。開始時刻はデータ転送コマンドのタスク開始時間より遅く設定し、データ転送コマンドの実行終了後にタスクが実行するようにします。

   ー [繰り返し間隔]にチェックし、[間隔]と[継続時間]を設定します。

6. [操作]タブを選択し、[新規]ボタンをクリックします。



→[新しい操作]画面が表示されます。



7. [設定]において以下の情報を設定し、[OK]ボタンをクリックします。

   ー [プログラム/スクリプト]:以下に格納されているコマンド「DttoolEx.exe」をフルパスで指定します。パスはダブルクォーテーションで囲みます。

   ```
   "[ログアナライザサーバインストールフォルダ]¥bin¥dttool¥DttoolEx.exe"
   ```

   ー [引数の追加]:「-f [ログ転送先共有フォルダのパス]」を設定します。[ログ転送先共有フォルダのパス]はUNC形式ではなくローカルパス形式で指定します。[ログ転送先共有フォルダのパス]は、ダブルクォーテーションで囲みます。

   ー [開始(オプション)]:[プログラム/スクリプト]で指定した「DttoolEx.exe」のあるフォルダのフルパスを指定します。パスは、ダブルクォーテーションで囲まないでください。

8. [タスクの作成]画面で[OK]ボタンをクリックします。

参考

ログのデータベースへの格納は手動でもできます

1. ログアナライザサーバのコマンドプロンプトで、以下のコマンドを実行し、ログアナライザサーバをインストールしたフォルダ配下の、ツールが格納されているフォルダへ移動します。

   ```
   cd [ログアナライザサーバインストールフォルダ]¥bin¥dttool [Enter]
   ```

2. 以下のコマンドを実行し、ログアナライザサーバのデータベースへデータを追加します。

```
DttoolEx.exe -f [ログ転送先共有フォルダのパス] [Enter]
```

2.8.2.2　集計条件/レポート出力条件を設定する

ログアナライザを起動して、集計条件やレポート出力条件を設定します。
PCの利用環境や、業務状況に応じて各条件を設定できるので、目的に即した集計結果が得られます。

ログアナライザを起動する

1. 以下のいずれかの方法で、メインメニューを起動します。

注意

ログアナライザ(Webコンソール)が接続するWebサーバについて

ログアナライザを起動する場合、接続できるWebサーバは1つです。3階層構成の場合、管理サーバに接続してもログビューア画面は表示されますが、ログアナライザ画面を表示することはできません。

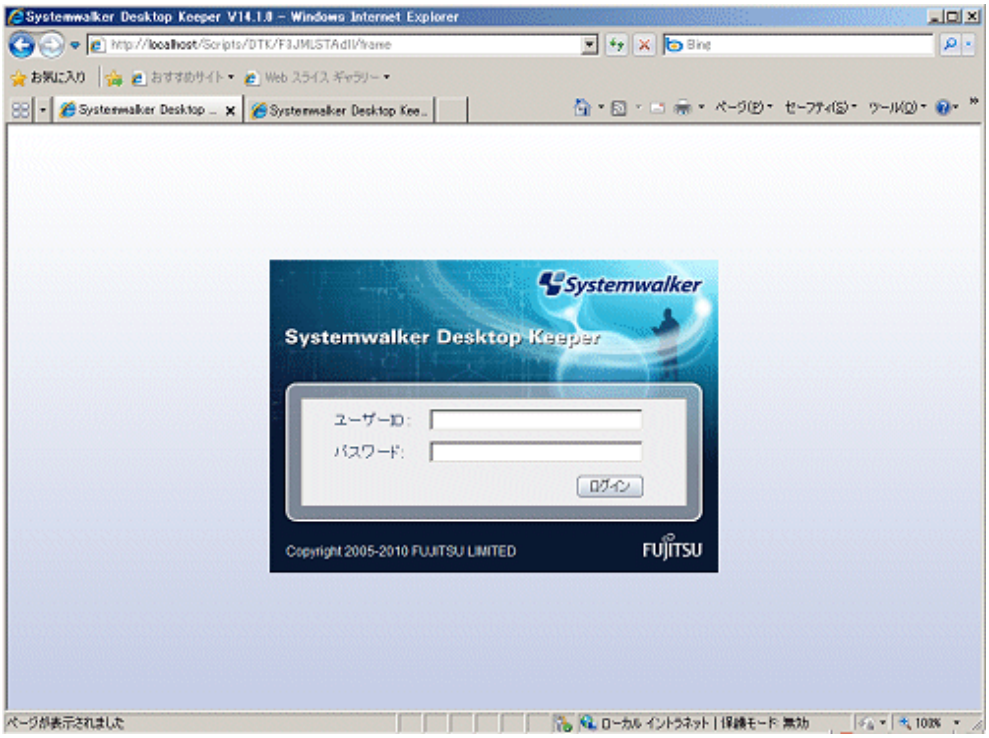
2階層構成の場合:管理サーバに接続してください。

- 管理サーバの[スタート]メニューから[プログラム]-[Systemwalker Desktop Keeper]-[サーバ]-[Desktop Keeper メインメニュー]を選択します。
- ブラウザのアドレスに“http://管理サーバのホスト名またはIPアドレス/DTK/index.html”と指定します。
  IISのポート番号に変更があった場合は、以下のように指定します。
  http://IPアドレス:ポート番号/DTK/index.html

3階層構成の場合:統合管理サーバに接続してください。

- 統合管理サーバの[スタート]メニューから[プログラム]-[Systemwalker Desktop Keeper]-[サーバ]-[Desktop Keeper メインメニュー]を選択します。
- ブラウザのアドレスに“http://統合管理サーバのホスト名またはIPアドレス/DTK/index.html”と指定します。
  IISのポート番号に変更があった場合は、以下のように指定します。
  http://IPアドレス:ポート番号/DTK/index.html

→[ログイン]画面が表示されます。



2. 以下の情報を入力し、[ログイン]ボタンをクリックします。

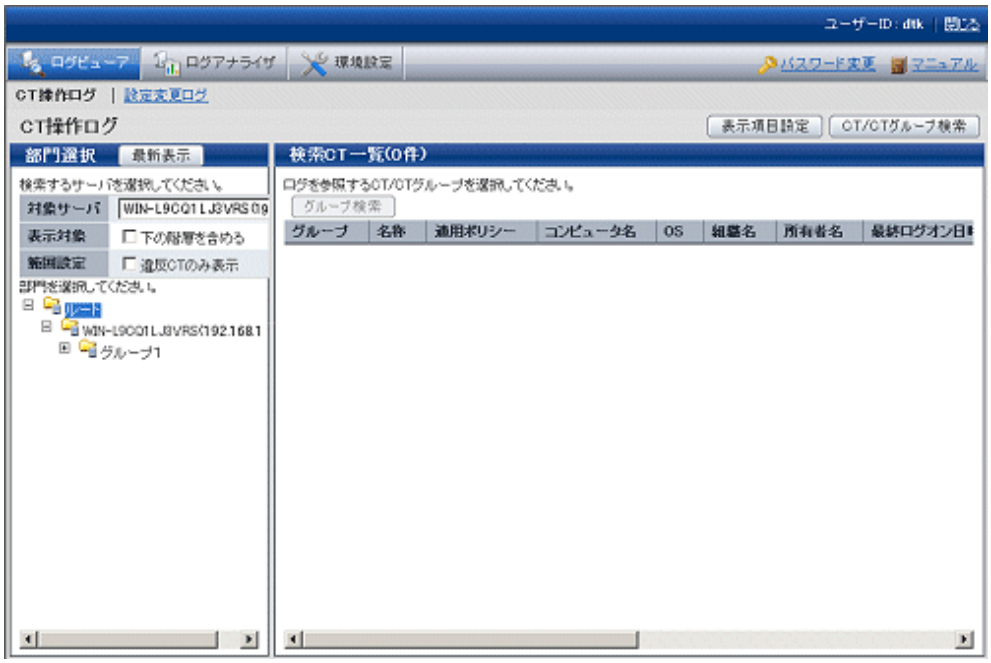
   以下の情報は、サーバ設定ツールで設定した[ユーザーID]および[パスワード]です。
   ログアナライザを使用する場合は、"ログビューア"権限を持つシステム管理者を指定する必要があります。

   - [ユーザーID]

   - [パスワード]
     パスワードは定期的に変更することを推奨します。変更方法は、“パスワードを変更する”を参照してください。

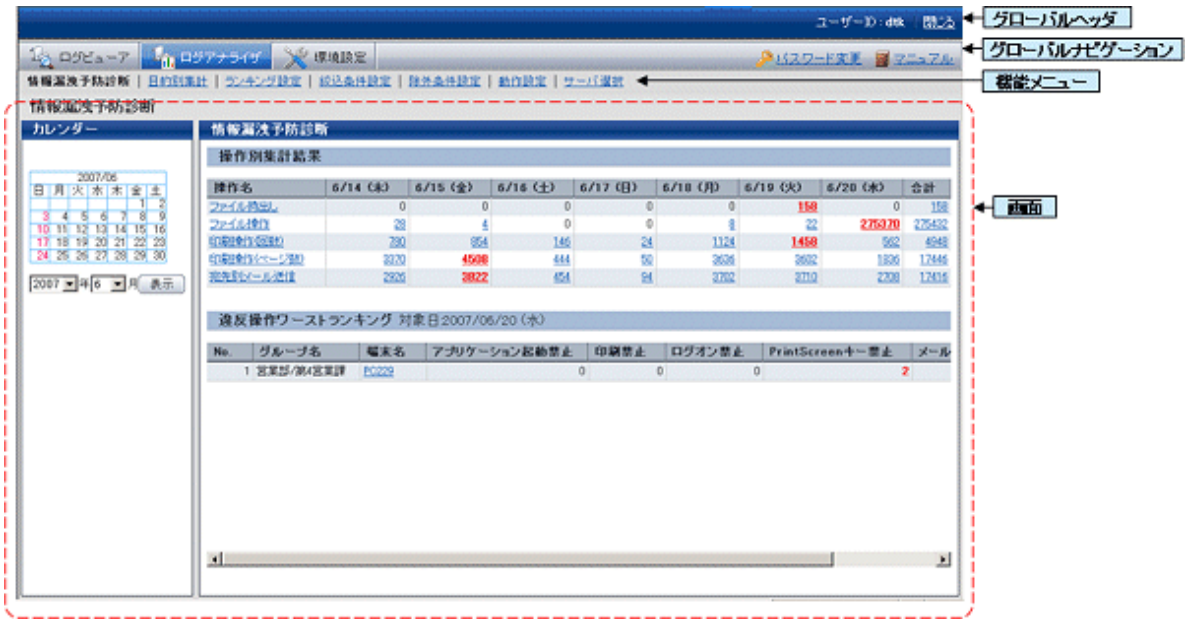
3. 表示された状況画面のグローバルナビゲーションの[ログ管理]をクリックします。

   →ログビューアが起動され、[CT操作ログ]画面が表示されます。



4. グローバルナビゲーションの[ログアナライザ]をクリックします。

→[情報漏洩予防診断]画面が表示されます。



画面の表示内容

グローバルヘッダ

- ユーザーID:ログインしているユーザーIDが表示されます。
- ログアウト:ログアウトします。

グローバルナビゲーション

- ログビューア:ログビューア画面が表示されます。
- ログアナライザ:ログアナライザ画面が表示されます。
- パスワード変更:Web画面起動時のパスワードを変更します。変更方法は、“パスワードを変更する”を参照してください。
- マニュアル:マニュアルが表示されます。

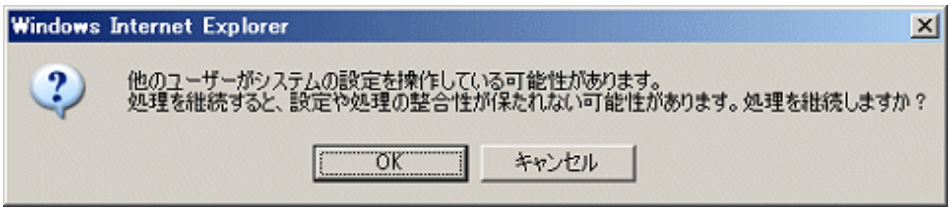
機能メニュー

- 情報漏洩予防診断:情報漏洩予防診断画面を表示します。
- 目的別集計:目的別集計画面を表示します。
- ランキング設定:グループ別、端末別、ユーザー別、端末＋ユーザー別の各ランキングの、“表示/非表示”と表示数を設定します。
- 絞込条件設定:ログを集計するときのキーワード、ドメイン、URL、またはアプリケーションを、絞込条件として設定します。
- 除外条件設定:ログを集計するとき、集計対象外とする端末を設定します。
- 動作設定:情報漏洩予防診断のランキング表示の設定、レポート出力における週報開始曜日、エコ監査の設定などを行います。
- サーバ選択:サーバ選択画面を表示します。現在選択しているログアナライザサーバを変更する場合にクリックします。
  以下の条件をすべて満たす場合、自動的に本画面が表示されます。
  ・ログアナライザサーバが複数あるシステム構成のとき
  ・メインメニューからログインして初めてログアナライザを使用するとき

注意

設定画面を終了する場合は、必ず[ログアウト]を使用してください

絞込条件設定画面、除外条件設定画面、動作設定画面を使用中にブラウザの×ボタンなどで終了した場合は、他にこれらの設定画面利用者がいない場合でも以下のメッセージが表示される場合があります。このとき、新たなユーザーが設定画面を警告メッセージなく使用できるまで、約24時間かかります(なお警告メッセージで[いいえ]を選択すると情報漏洩予防診断画面に遷移します)。
設定画面を終了する場合は、必ず[ログアウト]を使用してください。



2.8.2.2.1　ランキング表示数を設定する

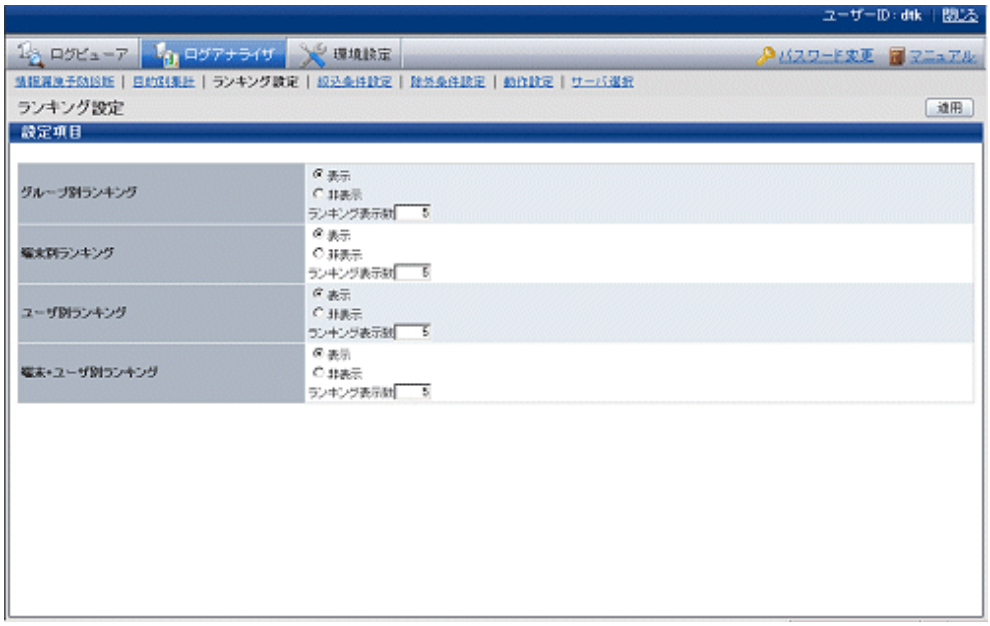
ランキング数の表示数を設定します。ランキング表示数の設定については、変更後すぐに反映されます。

注意

条件の変更は、ログの移入中やログアナライザ機能、レポート出力ツールの使用中に実施しないでください

集計結果や診断結果、レポート出力結果に矛盾が出る場合やエラーの原因となる場合があります。

1. 機能メニューの[ランキング設定]を選択します。
   →以下の画面が表示されます。



2. 各ランキングに対して、以下を設定します。

   ー [表示]/[非表示]の設定

   [表示](初期値):ランキング表示します。
   [非表示]:ランキング表示しません。

ー [ランキング表示数]の設定

表示するランキング数を1～99の範囲で入力します。初期値は、“5”です。
同順位がある場合、ランキングは、最大99行分まで表示されます。

3. [適用]ボタンをクリックします。

→設定値が反映された[情報漏洩予防診断]画面が再表示され、設定完了のメッセージが表示されます。

2.8.2.2.2　絞込条件を設定する

日々膨大に発生する操作ログから、重要ファイルへのアクセスや許可しないドメインへのメール送信などの危険操作を容易に検出できるように、集計時の絞込条件を設定することができます。

絞込条件については、設定が追加/変更./削除されてから集計情報に反映されるまでの時間にずれがあります。

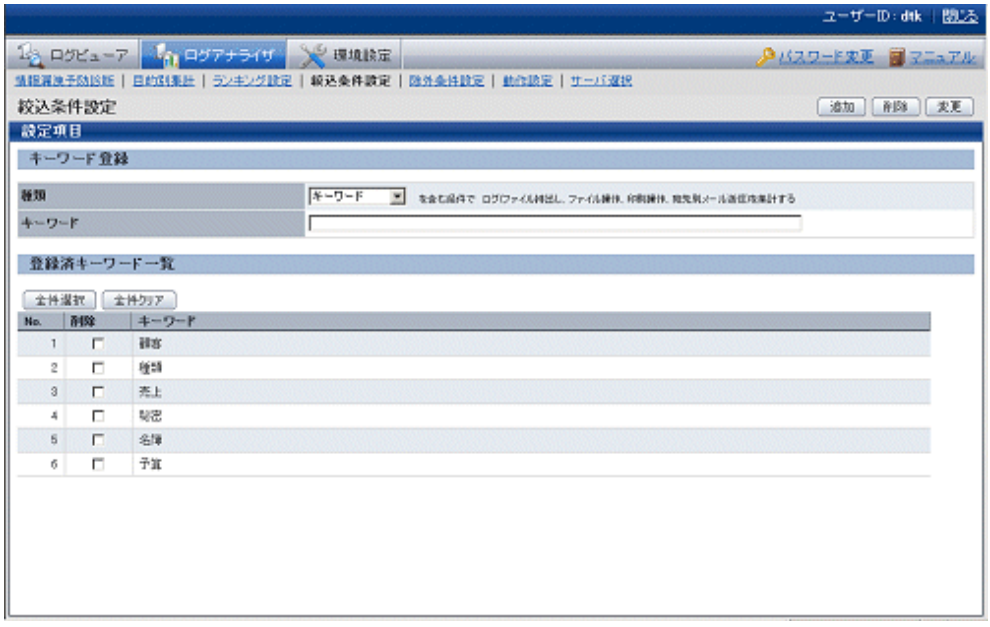
以下のようにログの移入が実施された場合
・3月1日にログが移入
・3月2日にログが移入
・3月3日にログが移入
3月2日のログ移入後に絞込条件設定を行った場合、絞込条件を適用して集計が行なわれるのは3月3日のログ移入時の集計処理以降になります。(3月2日以前のログについては、この時点では絞込条件設定が行われていないため、絞込条件は適用されません)
3月2日以前についても絞込条件を適用して集計するためには、“DTTOOLEX.EXE(ログアナライザサーバへのデータ移入・削除)”の再集計オプションを実施して再集計を行ないます。

注意

条件の変更は、ログの移入中やログアナライザ機能、レポート出力ツールの使用中に実施しないでください

集計結果や診断結果、レポート出力結果に矛盾が出る場合やエラーの原因となる場合があります。

1. 機能メニューの[絞込条件設定]を選択します。
→以下の画面が表示されます。



項目名	説明
[キーワード登録]	

項目名		説明
	[種類]	絞込条件の種類を指定します。
	[キーワード]	集計対象となるログを判別するためのキーワードを指定します。 [種類]で選択した条件により、入力域の左側に表示されるラベルが異なります。 **注意** 設定後にキーワード欄に日本語が入力できなくなる場合があります。その場合、入力欄を一度クリックすると日本語入力可能となります。
[登録済キーワード一覧]		登録されているキーワードの一覧が表示されます。
	[全件選択]	[登録済キーワード一覧]の全キーワードにチェックを付けます。
	[全件クリア]	[登録済キーワード一覧]の全キーワードのチェックをはずします。
[追加]		キーワード入力域に指定したキーワードを登録します。
[削除]		[登録済キーワード一覧]でチェックされたキーワードを削除します。
[変更]		登録されているキーワードを変更します。

2. [種類]で絞込条件の種類を選択し、キーワード入力域にキーワードを指定します。

   入力可能な文字は、以下のとおりです。

   - 全角で40文字、半角で80文字まで登録できます。ただし、「,」「’」「_」「%」「__」「％」を含む文字列は登録できません。
   - Shift-JISコードにない文字、外字、機種依存文字を入力した場合は、他の文字に置き換えられたり、正しく表示できない場合があります。

   選択可能な項目、指定できるキーワード、および集計対象となるログは以下のとおりです。

選択可能な項目	絞込条件が有効になる分析の種類	集計対象となる操作ログ	指定できるキーワード(注)
キーワード	情報漏洩分析	ファイル持出し ファイル操作 印刷操作 宛先別メール送信	ファイルまたはファイルパスに含まれる文字列(部分一致)
ドメイン	情報漏洩分析	宛先別メール送信	メールアドレスに含まれる文字列(後方一致)
	端末利用分析	宛先別メール送信	
URL	端末利用分析	URL付きウィンドウタイトル取得	URL内のドメイン部分に含まれる文字列(部分一致)
アプリケーション	端末利用分析	アプリケーション起動	拡張子を除く実行ファイル名(完全一致)

   注) 指定した文字列の大文字/小文字は区別されます。
   アプリケーションの実行ファイル名などは、OSにより大文字や小文字に変わる場合があります。どのように記録されているか、ログを確認してください。
   アプリケーションとして指定するキーワードについては、大文字の半角英字を使用せず、すべて小文字の半角英字に変換して登録してください。

3. [追加]ボタンをクリックします。
   →[登録済キーワード一覧]にキーワードが表示されます。

4. DTTOOLEX.EXEコマンドを実行し、再集計処理を行います。

   再集計しない場合、Webコンソールやレポート出力において、集計結果の数字と、ログの一覧の件数が一致しないときがあります。

   また再集計はログアナライザサーバ上に格納されているログが対象のため、現在ログアナライザサーバ上に無いログについては再集計は行なわれません。

   再集計処理については、“Systemwalker Desktop Keeper リファレンスマニュアル”の“DTTOOLEX.EXE(ログアナライザサーバへのデータ移入・削除)”の“-rオプション”を参照してください。

登録済リストのキーワードを削除する

1. [登録済キーワード一覧]で、削除するキーワードにチェックを付けます。
   登録されている全キーワードを削除する場合は、[全件選択]ボタンをクリックします。
2. [削除]ボタンをクリックします。

   →[登録済キーワード一覧]の表示が更新されます。

登録済みリストのキーワードを変更する

1. [登録済キーワード一覧]で、変更するキーワードの文字列をクリックします。
2. 変更後のキーワードを入力域に入力します。
3. [変更]ボタンをクリックします。
   →[登録済キーワード一覧]の表示が更新されます。

2.8.2.2.3　集計対象から除外する項目を設定する

業務上の重要なファイルへのアクセスが必要な端末や、日常的に大量のファイルアクセスを行う端末については、システム管理者の判断により操作ごとに集計の対象外にすることができます。

除外条件の設定には、管理サーバで管理されているグループ情報およびCT情報が必要です。この情報は、管理サーバからの管理者情報移入時、またはログ移入時にログアナライザサーバに取り込まれます。
当該クライアント(CT)のログが移入された日と、そのクライアント(CT)に対する除外条件設定が反映される日には、ずれがあります。

以下のようにログの移入が実施された場合
・3月1日に端末A,B,Cの端末情報とそれらのログが移入
・3月2日に端末A,B,C,Dの端末情報とそれらのログが移入
・3月3日に端末A,B,C,Dの端末情報とそれらのログが移入
端末Dに対して除外条件を設定できるのは、3月2日のログ移入終了後です。
また端末Dに対する除外設定が反映されるのは3月3日のログ移入時の集計処理からです(3月2日ログ移入分に端末Dのログがあっても、この時点では除外条件が設定されていないため集計対象となります)。
3月2日以前についても絞込条件を適用して集計するためには、“DTTOOLEX.EXE(ログアナライザサーバへのデータ移入・削除)”の再集計オプションを実施して再集計を行ないます。

注意

条件の変更は、ログの移入中やログアナライザ機能、レポート出力ツールの使用中に実施しないでください

集計結果や診断結果、レポート出力結果に矛盾が出る場合やエラーの原因となる場合があります。

1. 機能メニューの[除外条件設定]を選択します。
   →以下の画面が表示されます。

項目名		説明
[部門選択]		各部門の階層関係が、ツリー構造で表示されます。除外条件を設定する端末が属する部門を選択します。 ・ フォルダアイコン サブフォルダがある部門の場合は、アイコンをクリックすることで表示/非表示が相互に変化します。 ・ 部門名 部門名をクリックすると、当該部門に直属する端末のリストが、[除外対象]に表示されます。 部門を選択すると色が変化します。
	[登録済端末リスト]	クリックすると、当該操作ログについて除外対象として登録済の全端末を一覧表示します。登録済の端末をすべて削除する場合などに使用します。
[除外対象]		除外対象の端末のリストが表示されます。 集計対象除外端末リストは、操作ごとに管理されるため、[ログ種別]を切り替えると、端末リストの表示も切り替わります。 ・ [登録済端末数]：現在除外端末に登録されている数です。 ・ [除外]：すでに除外対象となっている場合に、チェックが付きます。 ・ [コンピュータ名]：コンピュータ名が表示されます。当該コンピュータに別名が設定されており、かつコンピュータ名と異なる場合はカッコ内に別名が表示されます。
	[ログ種別]	除外条件設定の対象とする操作ログを選択します。
	[全件選択]	端末リストの全端末にチェックを付けます。
	[全件クリア]	端末リストの全端末のチェックをはずします。
[適用]		指定した内容で除外条件設定を更新します。

2. [部門選択]ツリーで、除外条件を設定する端末が属する部門を選択します。

3. [除外対象]で、集計対象から除外する端末を選択します。
   400件まで登録できます。
4. [除外対象]の[ログ種別]で、除外条件設定の対象とする操作ログを選択します。

   選択可能な操作名および集計除外対象となるログは以下のとおりです。

選択可能な操作名	除外条件が有効になる分析の種類	集計除外対象となる操作ログ
ファイル持出し	情報漏洩分析	ファイル持出しログ
ファイル操作	情報漏洩分析	ファイル操作ログ
印刷操作	情報漏洩分析	印刷操作ログ
宛先別メール送信	情報漏洩分析 端末利用分析	宛先別メール送信ログ
URL付きウィンドウタイトル取得	端末利用分析	URL付きウィンドウタイトル取得ログ
アプリケーション起動	端末利用分析	アプリケーション起動ログ

5. [適用]ボタンをクリックします。

   →設定完了のメッセージが表示されます。
6. DTTOOLEX.EXEコマンドを実行し、再集計処理を行います。

   再集計しない場合、Webコンソールやレポート出力において、集計結果の数字と、ログの一覧の件数が一致しないときがあります。

   また再集計はログアナライザサーバ上に格納されているログが対象のため、現在ログアナライザサーバ上に無いログについては再集計は行なわれません。

   再集計処理については、“Systemwalker Desktop Keeper リファレンスマニュアル”の“DTTOOLEX.EXE(ログアナライザサーバへのデータ移入・削除)”の“-rオプション”を参照してください。

2.8.2.2.4　その他の条件を設定する

情報漏洩予防診断のランキング表示の設定、レポート出力における週報開始曜日や、状況の改善/悪化を判断するための目安となる値の設定、エコ監査の設定などを行います。

その他の条件の設定については、変更後すぐに反映されます。

注意

条件の変更は、ログの移入中やログアナライザ機能、レポート出力ツールの使用中に実施しないでください

集計結果や診断結果、レポート出力結果に矛盾が出る場合やエラーの原因となる場合があります。

1. 機能メニューの[動作設定]を選択します。
   →以下の画面が表示されます。

2. 各項目に設定値を入力します。

   [情報漏洩予防診断設定]

項目名	説明
[違反操作ワーストランキング]	・ [表示]/[非表示]ラジオボタン 情報漏洩予防診断画面に表示する違反操作ワーストランキングの表示/非表示を選択します。 ・ [ランキング表示数] ランキング表示数を、1～99の範囲で指定します。 ・ [赤色表示] TOP画面に表示される違反操作ワーストランキングで、警告表示(セルを赤く表示)するための、件数のしきい値を1～99999の数字で指定します。 しきい値以上の件数を示すセルは赤く表示されます。
[週報開始曜日設定]	週報期間の開始日とする曜日を指定します。 [日]を指定した場合、日～土曜日が週報期間となります。デフォルトの設定値は[日]です。 ここでの設定値は、[レポート出力ツール]画面の[基本情報]タブの設定の[分析期間]([週報])に反映されます。
[月報開始日設定]	月報期間の開始日とする日付を指定します。 [21]を指定した場合、21～翌月20日が月報期間となります。デフォルトの設定値は[21]です。 設定が可能な日付は[1]～[28]です。 ここでの設定値は、[レポート出力ツール]画面の[基本情報]タブの設定の[分析期間]([月報])に反映されます。
[情報漏洩予防診断動作]	[Desktop Log Analyzer互換で動作させる]にチェックした場合、情報漏洩予防診断のランキングから端末名などをクリックしたときの遷移先が目的別集計画面となり、Systemwalker Desktop Log Analyzerと同じ動作となります。 詳細な説明は、以下のとおりです。デフォルトはチェックなしです。 【本項目をチェックしない場合】 [情報漏洩予防診断]画面で、[操作別集計結果]の件数をクリックすると、操作別ランキング表示されます。 各ランキングの項目である、グループ名、端末名、端末+ユーザー名に表示され

項目名	説明
	ているリンクをクリックすると、ログビューアの[CT操作ログ ― ログ検索]相当の画面に切り替わります。 [CT操作ログ ― ログ検索]画面では、ログアナライザで絞り込んだ期間、対象グループ/端末/ユーザ、操作が、検索入力項目として設定された状態で表示されます。また、この条件での検索結果が、すでにログ一覧に表示されています。 つまり、情報漏洩の疑いが濃いとしてランキングされたユーザー名やPC名から、それらの具体的な操作内容(ログ)へと展開でき、情報漏洩調査をスムーズに移行できます。 【本項目をチェックした場合】 [情報漏洩予防診断]画面で、[操作別集計結果]の件数をクリックすると、操作別ランキングが表示されます。各ランキングの項目である、端末名、ユーザー名、端末+ユーザー名に表示されているリンクをクリックすると、目的別集計画面が表示されます。 目的別集計画面で、絞込期間などの条件を手動で設定し、再集計します。ランキングされたユーザー名やPC名から、それらの具体的な操作内容(ログ)への展開はできません。

[エコ監査設定]

項目名		説明
[年度開始月設定]		印刷量監査レポートや複合機の用紙使用状況レポート※で、年度累計などを計算する場合に、基準とする年度開始月を指定します。 1～12から選択できます。 初期値は4です。
[印刷量(または複合機用紙使用量)監査設定]	[1ページ(または1枚)あたりの用紙代]	印刷量監査レポートや複合機の用紙使用状況レポート※で、用紙代を算出するための係数を円単位で指定します。 小数点2桁で表示されます。 0.01～99.99の値を指定できます。 初期値は、0.60です。 印刷量監査レポートでは、本係数を1ページあたりの印刷用紙代として使用します。 複合機の用紙使用状況レポートでは、本係数を1枚あたりの用紙代として使用します。
	[1ページ(または1枚)あたりのCO2排出量]	印刷量監査レポートや複合機の用紙使用状況レポート※で、CO2排出量を算出するための係数をg単位で指定します。 小数点2桁で表示されます。 0.01～99.99の値を指定できます。 初期値は、5.16です。 印刷量監査レポートでは、本係数を1ページあたりのCO2排出量として使用します。 複合機の用紙使用状況レポートでは、本係数をA4サイズ用紙1枚あたりのCO2排出量として使用します。
	[監査の判定基準1] [監査の判定基準2]	印刷量監査レポートで印刷上限値超過端末を出力する場合に、超過量(ページ)のパターン分けの基準とする値をページ単位で指定します。 基準1は、2以上999999998以下の数値を設定できます。 基準2は、3以上999999999以下の数値を設定できます。 また、基準1＜基準2である必要があります。 初期値は、基準1が100、基準2が200です。 ここでの設定値は、印刷量監査レポートの、「印刷上限値超過状況」シートの「超過量別端末の比率」と、「超過端末一覧」シートの「[▲]または[△]」に反映されます。

※複合機の用紙使用状況レポートについては、“付録B 複合機と連携して情報を可視化する”を参照してください。

3. [適用]ボタンをクリックします。

2.8.2.2.5　ログアナライザサーバを選択する

ログアナライザサーバが複数あるシステムの場合、使用するログアナライザサーバを選択/変更します。

注意

ログアナライザサーバの選択は、ログアナライザ機能の使用中や、ログの移入中に実施しないでください

集計結果に矛盾が出る場合やエラーの原因となる場合があります。

ログイン中にサーバ構成や設定の変更を行わないでください。

この場合、正しく認識されない場合や設定・処理が正しく行われない場合がありますので、ログインし直してください。

画面表示までに時間がかかる場合があります

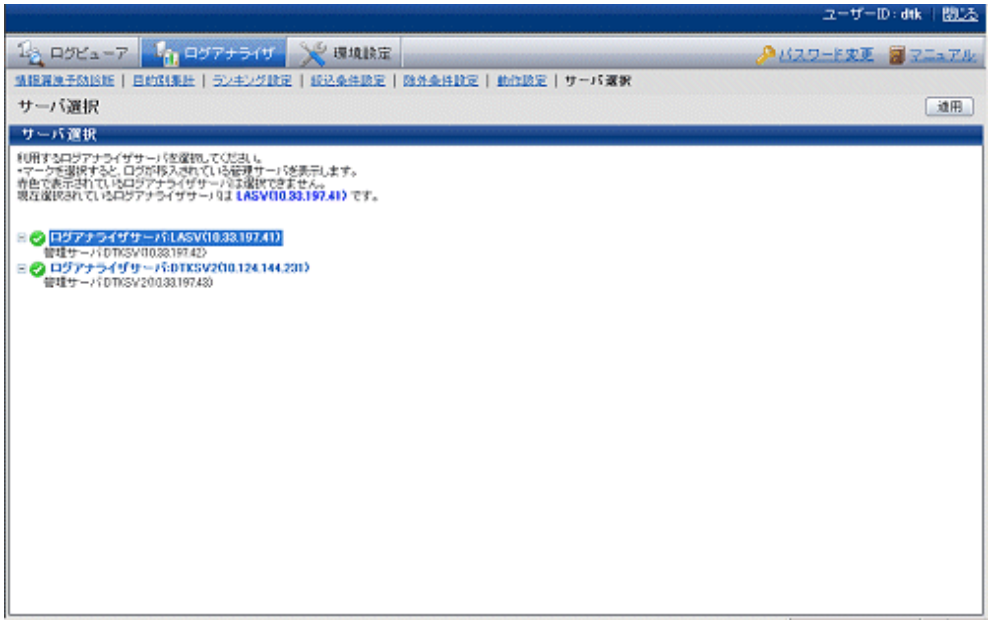
サーバの停止やネットワークの不通など、接続ができないログアナライザサーバがある場合、環境やサーバ台数によっては、画面表示までに数分かかるときがあります。

ログアナライザサーバの状態に変化があった場合、反映されるまで時間がかかる場合があります。

断線していたログアナライサーバが接続可能に変化した場合など、状態に変化があっても、即座に反映されない場合があります。しばらく待ってから、再度確認してください。

1. 機能メニューの[サーバ選択]を選択します。

   →以下の画面が表示されます。



   以下の条件をすべて満たす場合、自動的に本画面が表示されます。

   ー　ログアナライザサーバが複数あるシステム構成のとき

－ メインメニューからログインして初めてログアナライザを使用するとき

2. ログアナライザサーバを選択します。
   ツリー構成から、青色で表示されたログアナライザサーバ(サーバ名とIPアドレスが表示)を選択します。

   選択したログアナライザサーバは、表示が反転します。

   [+]ボタンをクリックすると、そのログアナライザサーバにログデータを移入している管理サーバが表示されます。

   赤色で表示されたログアナライザサーバは使用できません。したがって、選択できません。当該サーバについては、“Systemwalker Desktop Keeper リファレンスマニュアル”の“Webコンソールで出力されるメッセージ”を参照し、[ERR-DTLAC001]の対処を行ってください。

3. [適用]ボタンをクリックします。

第3章 管理コンソールでポリシーを設定する

現状の運用方針を見直した結果、ポリシーの変更が必要な場合があります。
このとき、変更対象となるクライアント(CT)やユーザーを洗い出すために、検索してポリシーを変更します。
本章では、管理コンソールでのCT情報/ユーザー情報の検索方法と、ポリシーの変更方法を説明します。

3.1 CT情報/ユーザー情報を検索する

CT情報を検索する

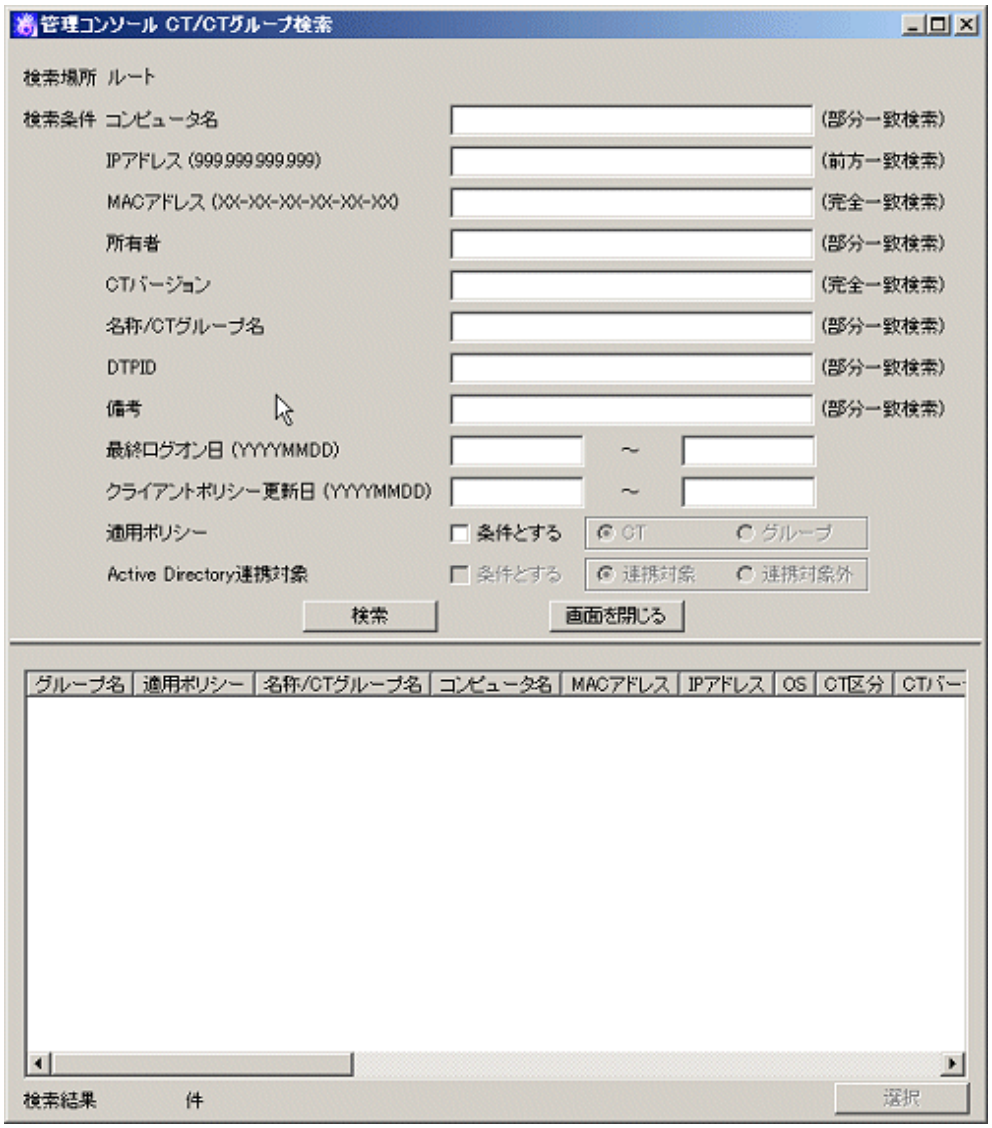
管理コンソールに表示されているCTグループやCTを検索する手順を説明します。

管理コンソールのCTグループツリーに「削除したCT」グループが表示されている場合は、「削除したCT」グループに所属するクライアント(CT)も検索対象です。
「削除したCT」グループのクライアント(CT)は、検索結果表示域の[グループ名]に「削除したCT」と表示されます。

1. [管理コンソール]を起動します。
2. CTグループツリーから検索の対象とする[ルート]または「CTグループ」を選択します。

3. [ファイル]メニューから[CT/CTグループ検索]を選択します(または、右クリックし、表示されたポップアップメニューから[CT/CTグループ検索]を選択します)。

   →[管理コンソール CT/CTグループ検索]画面が表示されます。



4. 以下の情報を、検索条件として入力します。

   検索は、複数の条件をすべて含む「AND検索」です。

   【CTグループを検索する場合】
   [名称/CTグループ名]と[備考]だけを指定します。また、[適用ポリシー]の[条件とする]は未チェックになっている必要があります。

   【クライアント(CT)を検索する場合】
   検索条件の項目を指定します。

項目名	説明
[コンピュータ名]	クライアント(CT)のコンピュータ名により検索が行えます。入力した条件と部分的に一致した結果も表示されます。 半角および全角で15バイトまで入力できます。
[IPアドレス]	クライアント(CT)のIPアドレスにより検索が行えます。入力した条件と前方が一致した結果も表示されます。「10.1」で検索した場合、「10.1.」、「10.1X.」、および「10.1XX.」の結果を表示します。(「X」は数字1文字を表す)

項目名		説明
		「XXX.XXX.XXX.XXX」の形式で入力します。 【例】140.48.23.12
[MACアドレス]		クライアント(CT)のMACアドレスにより検索が行えます。入力した条件と完全に一致した結果が表示されます。 「XX-XX-XX-XX-XX-XX」の形式で入力します。(「X」は英数字1文字を表す) 【例】02-E0-32-33-A3-C0
[所有者]		クライアント(CT)のOSに設定されている所有者名により検索が行えます。入力した条件と部分的に一致した結果も表示されます。 半角および全角で93バイトまで入力できます。
[CTバージョン]		インストールされているSystemwalker Desktop Keeperのクライアント(CT)のバージョンにより検索が行えます。入力した条件と完全に一致した結果が表示されます。 「X.X.X.X」の形式で入力します。(「X」は数字1文字以上を表す) 【例】2.1.0.1
[名称/CTグループ名]		CTグループまたはクライアント(CT)に付けられた名称により検索が行えます。入力した条件と部分的に一致した結果も表示されます。 半角および全角で40バイトまで入力できます。
[DTPID]		Systemwalker Desktop KeeperのクライアントおよびSystemwalker Desktop Patrolのクライアント(CT)が同一のPCにインストールされている場合に表示される、Systemwalker Desktop Patrolのクライアント(CT)の「ユーザーID(+)PC名」を入力します。 部分一致で検索されます。
[備考]		クライアント(CT)のポリシー反映時に入力された備考により検索が行えます。入力した条件と部分的に一致した結果も表示されます。 半角および全角で128バイトまで入力できます。
[最終ログオン日]		クライアント(CT)は起動時に統合管理サーバまたは管理サーバと通信します。その通信が可能となった時点の日時により検索が行えます。 「XXXXXXXX」の形式で入力します。(「X」は数字1文字を表す) 【例】20050701
[クライアントポリシー更新日]		クライアント(CT)が統合管理サーバまたは管理サーバから最後にポリシーを取得した日により検索が行えます。 「XXXXXXXX」の形式で入力します。(「X」は数字1文字を表す) 【例】20050922
[適用ポリシー]	[条件とする]	チェックをつけた場合、クライアント(CT)に適用されているポリシーを、検索条件に含みます。
	[CT]	検索対象は、CTポリシーが適用されているクライアント(CT)です。
	[グループ]	検索対象は、CTグループポリシーが適用されているクライアント(CT)です。
[Active Directory連携対象]	[条件とする]	チェックをつけた場合、Active Directoryから情報を取り込んだクライアント(CT)かどうかを、検索条件に含みます。
	[連携対象]	検索対象は、Active Directoryから情報を取り込んだクライアント(CT)です。
	[連携対象外]	検索対象は、Active Directoryから情報を取り込んでいないクライアント(CT)です。
[検索]		検索が開始され、結果が表示されます。
[画面を閉じる]		入力した検索条件が保存されます。

5. [検索]ボタンをクリックします。

   →検索結果が表示されます。
   表示される項目は、[CTリスト表示列設定]画面で選択した項目です。[CTリスト表示列設定]画面については、“表示される項目

と順序を変更する場合”を参照してください。
検索されたCT、または、CTグループをダブルクリックすると[管理コンソール]画面が表示され、該当するCT、または、CTグループが選択された状態になっています。[CT/CTグループ検索]画面は閉じず、最小化されています。

6. [画面を閉じる]ボタンをクリックします。

   →入力した検索条件が保存されます。
   保存される検索条件は、次回[CT/CTグループ検索]画面を起動したときに表示されます。ただし、[CT/CTグループ検索]画面右上の[×]ボタンで画面を閉じた場合は、今回入力した検索条件は保存されません。

ユーザー情報を検索する

ユーザーやユーザーグループの検索は、管理コンソールで実施できます。

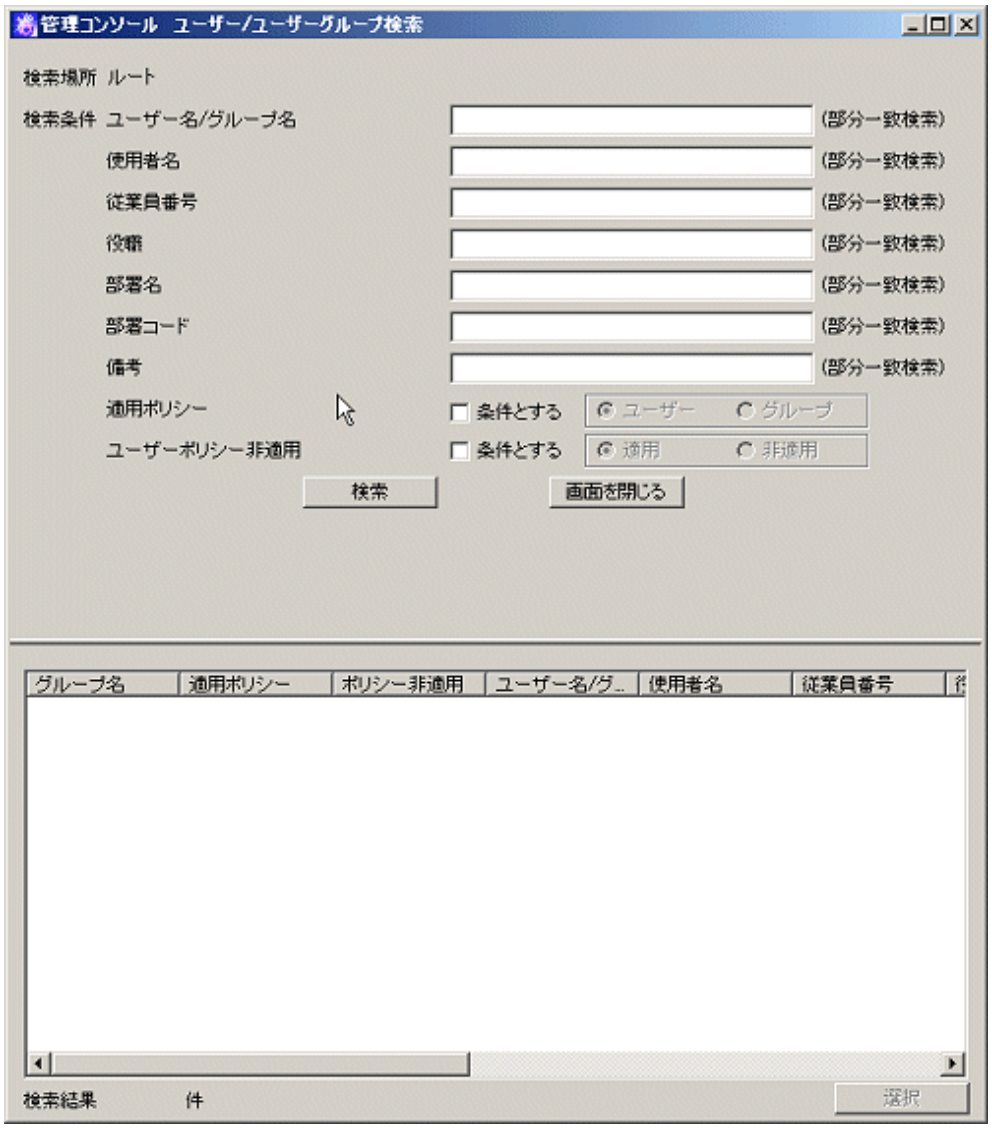
検索する手順は、以下のとおりです。

1. [管理コンソール]を起動します。
2. [ユーザー設定]メニューから[ユーザーポリシー設定]を選択します。

   →[ユーザーポリシー設定]画面が表示されます。
3. ユーザーグループツリーから検索の対象とする[ルート]または「ユーザーグループ」を選択します。

4. [ファイル]メニューから[ユーザー/ユーザーグループ検索]を選択します。(または、右クリックし、表示されたポップアップメニューから[ユーザー/ユーザーグループ検索]を選択します)

   →[管理コンソール ユーザー/ユーザーグループ検索]画面が表示されます。



5. 以下の情報を、検索条件として入力します。

   検索は、複数の条件をすべて含む「AND検索」です。

   【ユーザーグループを検索する場合】
   [ユーザー名/グループ名]と[備考]だけを指定します。また、[適用ポリシー]、および[ユーザーポリシー非適用] は未チェックになっている必要があります。

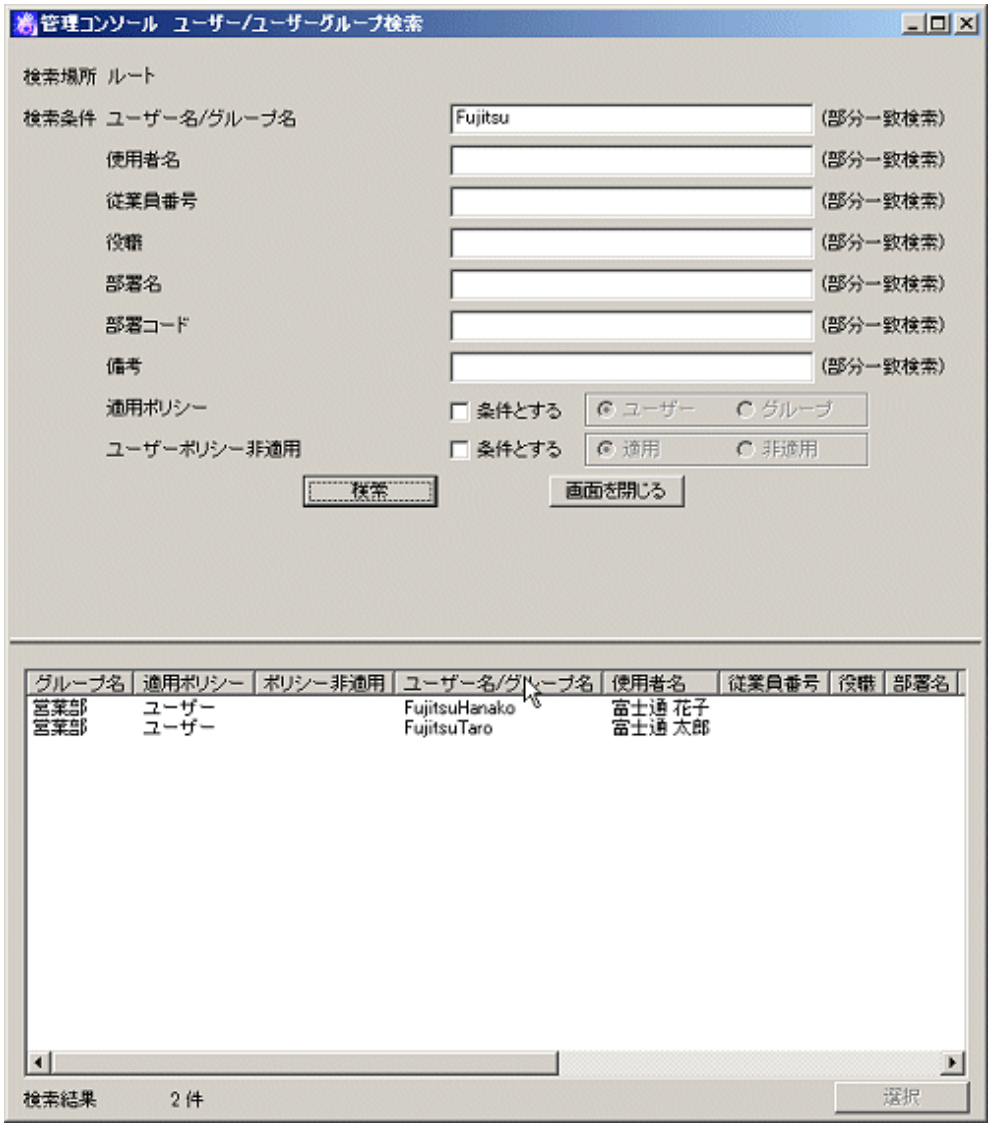
   【ユーザーを検索する場合】
   検索条件の項目を指定します。

項目名	説明
[ユーザー名/グループ名]	ユーザー名やユーザーグループ名により検索が行えます。入力した条件と部分的に一致した結果も表示されます。 半角および全角で40バイトまで入力できます。
[使用者名]	ユーザー名を使用するユーザーの名前により検索が行えます。入力した条件と部分的に一致した結果も表示されます。 半角および全角で128バイトまで入力できます。

項目名		説明
[従業員番号]		ユーザー名を使用するユーザーの従業員番号で検索を行えます。入力した条件と部分的に一致した結果も表示されます。 半角および全角で40バイトまで入力できます。
[役職]		ユーザー名を使用するユーザーの役職により検索が行えます。入力した条件と部分的に一致した結果も表示されます。 半角および全角で128バイトまで入力できます。
[部署名]		ユーザー名を使用するユーザーが所属する部署名により検索が行えます。入力した条件と部分的に一致した結果も表示されます。 半角および全角で128バイトまで入力できます。
[部署コード]		ユーザー名を使用するユーザーが所属する部署コードにより検索が行えます。入力した条件と部分的に一致した結果も表示されます。 半角および全角で40バイトまで入力できます。
[備考]		ユーザー名を使用するユーザーの備考情報により検索が行えます。入力した条件と部分的に一致した結果も表示されます。 半角および全角で128バイトまで入力できます。
[適用ポリシー]	[条件とする]	チェックをつけた場合、ユーザーに適用されているポリシーを、検索条件に含みます。
	[ユーザー]	検索対象は、ユーザーポリシーが適用されているユーザーです。
	[グループ]	検索対象は、ユーザーグループポリシーが適用されているユーザーです。
[ユーザーポリシー非適用]	[条件とする]	チェックをつけた場合、ユーザーポリシーが適用されているかどうかを、検索条件に含みます。
	[適用]	検索対象は、ユーザーポリシーが適用されているユーザーです。
	[非適用]	検索対象は、ユーザーポリシーが適用されていないユーザーです。

6. [検索]ボタンをクリックします。

   →検索結果が表示されます。



   検索されたユーザーまたは、ユーザーグループをダブルクリックすると[ユーザーポリシー設定]画面が表示され、該当するユーザー、または、ユーザーグループが選択された状態になっています。[ユーザー/ユーザーグループ検索]画面は閉じず、最小化されています。

7. [画面を閉じる]ボタンをクリックします。

   →入力した検索条件が保存されます。
   保存される検索条件は、次回[ユーザー/ユーザーグループ検索]画面を起動したときに表示されます。ただし、[ユーザー/ユーザーグループ検索]画面右上の[×]ボタンで画面を閉じた場合は、今回入力した検索条件は保存されません。

3.2 グループポリシーを変更する

構成情報ツリーを作成すると、各グループには、グループポリシーが設定されます。
グループポリシーは、必要に応じて変更します。

グループポリシーの変更については、以下の2とおりの考え方があります。

- システム管理者が、全グループのポリシーを管理する

・ 部門管理者を設定し、その部門管理者が管理できるグループについては、ポリシーの変更を任せる

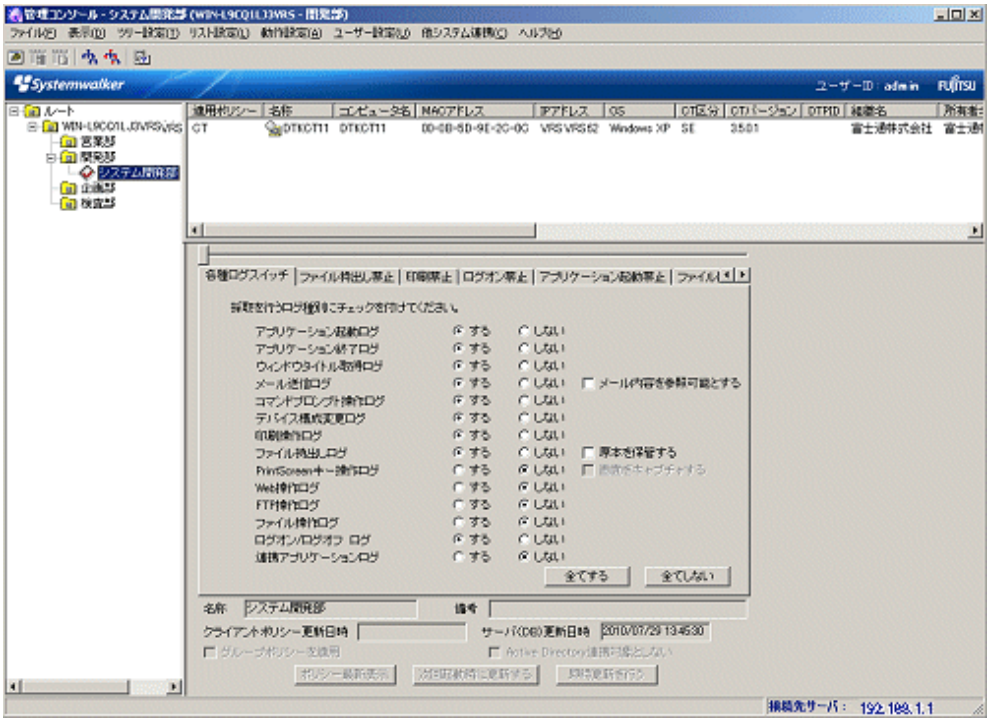
3.2.1 CTグループポリシーを変更する

管理コンソールでポリシーを更新した場合、すべてのタブのポリシーが更新されます(設定を変更していない箇所については、同じ値で更新されます)。
設定を変更したタブ、または項目のみポリシーを更新することはできません。

CTグループポリシーの変更手順を説明します。

1. [管理コンソール]を起動します。
2. CTグループツリーから、ポリシーを設定するCTグループを選択します。

   →最新のポリシー情報が表示されます。



注意

以下の場合は、CTグループやCTリストの情報を最新にしてください

以下の条件のどちらかを満たす場合、画面に表示される統合管理サーバ配下の管理サーバの、CTグループ、およびCTリストの情報は最新になっていない場合があります。

ー 管理サーバ側でCTグループツリーが変更された場合

ー Active Directory連携が実行され、グループツリーが変更となった場合

最新にするには、[ツリー設定]メニューから[ツリー最新表示]を選択してください。

3. ポリシー一覧の各タブで、ポリシーを変更します。

   ポリシーの設定項目の説明は、“2.4.1 端末初期設定をおこなう”を参照してください。

4. 必要に応じて、CTグループの[名称]または[備考]を変更します。

   [名称]および[備考]に入力できる文字は、“グループ情報を変更する”を参照してください。

5. 以下のどちらかのボタンをクリックし、ポリシーをCTグループに反映します。

   ー [次回起動時に更新する]ボタンをクリックする場合

   各タブのポリシーがデータベースに反映されます。ただしクライアント(CT)には、即時にポリシーが反映されません。次回のクライアント(CT)起動時、クライアント(CT)が接続するサーバ(統合管理サーバ、または管理サーバ)と通信が行われたときに、最新のポリシーが反映されます。

   ー [即時更新を行う]ボタンをクリックする場合

   - 各タブのポリシーがデータベースに反映され、稼働しているクライアント(CT)にも反映されます。
     ただし、[ファイル持出し禁止]タブの設定は、即時更新を行ったクライアント(CT)で持出しユーティリティが起動されていた場合は、次回の持出しユーティリティ起動時からポリシーが反映されます。
   - [印刷禁止]タブで許可しているアプリケーションが、即時更新を行ったクライアント(CT)で起動されていた場合は、次回のアプリケーション起動時からポリシーが反映されます。
   - [ログオン禁止]タブの設定でログオフまたはシャットダウンする設定にした場合、起動中のクライアント(CT)には即時に反映され、ログオフまたはシャットダウンされます。なお、稼働していないクライアント(CT)や、上位サーバと通信できないクライアント(CT)では、次回のクライアント(CT)起動時、クライアント(CT)が接続するサーバ(統合管理サーバ、または管理サーバ)と通信が行われたときに、最新のポリシーが反映されます。

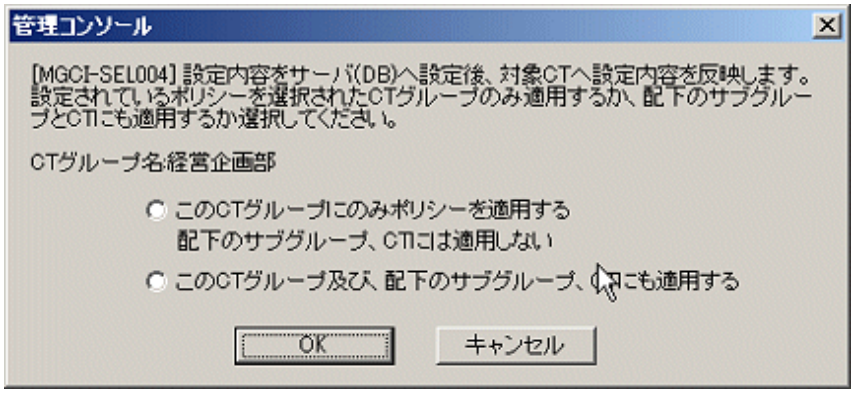
   [次回起動時に更新する]ボタン、または[即時更新を行う]ボタンがグレーアウトされている場合は、CTグループの作成、移動、削除のあと、構成反映が実施されていない可能性があります。この場合、[ツリー設定]メニューから[CTグループ構成反映]を選択し、構成反映を実施してください。

ポイント

CTグループ内のクライアント(CT)数が多い場合は、[次回起動時に更新する]を選択することを推奨します

統合管理サーバまたは管理サーバと接続されていないクライアント(CT)との接続タイムアウト時間は、クライアント(CT)1台につき5秒です。また、ネットワーク環境にも依存しますが、統合管理サーバまたは管理サーバと接続されているクライアント(CT)に、[即時更新]を行うと、ポリシー適用に要する時間は、クライアント(CT)1台につき1秒程度かかります。
そのため、CTグループに対して即時更新を行う場合など、ポリシーの設定対象とするCT数が多いときは、[次回起動時に更新する]ボタンをクリックする運用を推奨します。

→以下の画面が表示されます。



6. ポリシーの適用方法としてどちらかを選択し、[OK]ボタンをクリックします。

   ー **[このCTグループにのみポリシーを適用する 配下のサブグループ、CTには適用しない]**:

   - 設定したポリシーは選択しているCTグループだけに適用されます。配下のサブグループやCTには適用されません。
   - CTグループ名の変更の場合は、こちらを指定してください。

   ー **[このCTグループ及び、配下のサブグループ、CTにも適用する]**:

   - 設定したポリシーは選択しているCTグループおよび配下のサブグループやCTにも適用されます。

- 配下のクライアント(CT)の[名称]および[備考]は上書きされません。

7. [名称]または[備考]を変更した場合は、[ツリー設定]メニューから[ツリー最新表示]を選択します。

   →[名称]または[備考]に入力した情報が、[管理コンソール]画面上に反映されます。

3.2.2 ユーザーグループポリシーを変更する

管理コンソールでポリシーを更新した場合、すべてのタブのポリシーが更新されます(設定を変更していない箇所については、同じ値で更新されます)。
設定を変更したタブ、または項目のみポリシーを更新することはできません。

ユーザーグループポリシーの変更手順を説明します。

1. [管理コンソール]を起動します。
2. [ユーザー設定]メニューから[ユーザーポリシー設定]を選択します。

   →[ユーザーポリシー設定]画面が表示されます。
   [ユーザーポリシー設定]画面の表示内容の詳細は、“画面の表示内容”を参照してください。

3. ユーザーグループツリーから、ポリシーを変更するユーザーグループを選択します。
4. ユーザーポリシー一覧の各タブで、ポリシーを変更します。

   ポリシーの設定項目の説明は、“2.4.1 端末初期設定をおこなう”を参照してください。
5. [更新]ボタンをクリックします。

   →設定したポリシーは、次回ログオン時からユーザーグループに反映されます。

画面の表示内容

[ユーザーポリシー設定]画面に表示されている項目について説明します。

ユーザーグループツリー

Active Directory連携によって取り込まれたユーザーグループ情報や、作成したユーザーグループが表示されます。

最新のユーザーグループツリーの情報を確認する場合は、[ツリー設定]メニューから[ツリー最新表示]を選択します。
[ツリー設定]メニューから[ツリー全展開]を選択すると、すべてのユーザーグループが表示されます。
[ツリー設定]メニューから[ツリー全縮小]を選択すると、ルート直下(ドメイン表示時はドメイン直下)のユーザーグループだけ表示します。
ユーザーグループを選択した時点で、ユーザーグループ単位に設定されているユーザーポリシーは最新表示されます。

ユーザー一覧

ユーザーグループに属するユーザーが表示されます。ユーザー一覧に表示されている項目は、以下のとおりです。

項目名	表示される内容
[適用ポリシー]	ユーザーポリシーとユーザーグループポリシーのどちらが適用されているかが表示されます。 ・ [ユーザー]: ユーザーポリシーが設定されていることを表します。 ・ [グループ]: ユーザーグループポリシーが設定されていることを表します。
[ポリシー非適用]	ユーザーポリシーが適用されているか、いないかが表示されます。 ・ [非適用]: ユーザーポリシーは適用されていないことを表します。 ・ (空欄): ユーザーポリシーが適用されていることを表します。
[ユーザー名]	Windowsにログオンするユーザー名です(ユーザー名に設定できる「フルネーム」とは異なります)。
[使用者名](注)	ユーザー名を使用するユーザーの名前です。
[従業員番号](注)	ユーザー名を使用するユーザーの従業員番号です。
[役職](注)	ユーザー名を使用するユーザーの役職です。
[部署名](注)	ユーザー名を使用するユーザーが所属する部署名です。
[部署コード](注)	ユーザー名を使用するユーザーが所属する部署コードです。
[備考]	ユーザー名を使用するユーザーの備考情報です。
[最終ポリシー取得日時]	最新のポリシーが設定された日付です。
[サーバ(DB)更新日時]	管理サーバまたは統合管理サーバがクライアント(CT)のポリシーを更新し、データベースに反映した最終日時です(即時更新も含みます)。
[登録日時]	ユーザーが登録された日時です。

注) Active Directory連携で取り込んだユーザーに関しては、管理コンソールで変更できません。

ユーザー属性

ツリー構成情報部分で選択したユーザーの属性を入力できます。表示されている[登録済ユーザー件数]に、ユーザーグループ数は含まれません。入力情報は、以下のとおりです。

項目名	入力する内容
[ユーザー名] (注1) (注2)	Windowsにログオンするためのユーザー名を入力します(ユーザー名に設定できる「フルネーム」とは異なります)。 半角で40文字(全角で20文字)まで入力できます。半角英大文字、および半角英小文字は、同じ文字として認識されます。 ただし、以下の場合は、エラーとなります。 ・ ピリオド「.」だけのユーザー名

項目名	入力する内容
	• 空白だけのユーザー名 • 「"」「/」「¥」「[」「]」「:」「;」「|」「=」「,」「+」「*」「?」「<」「>」を含むユーザー名
[使用者名]	ユーザー名を使用するユーザーの名前を入力します。 半角で128文字(全角で64文字)まで入力できます。
[従業員番号]	ユーザー名を使用するユーザーの従業員番号を入力します。 半角で40文字(全角で20文字)まで入力できます。
[役職]	ユーザー名を使用するユーザーの役職を入力します。 半角で128文字(全角で64文字)まで入力できます。
[グループ名]	ユーザーグループのグループ名を入力します。 半角で40文字(全角で20文字)まで入力できます。
[部署名]	ユーザー名を使用するユーザーが所属する部署名を入力します。 半角で128文字(全角で64文字)まで入力できます。
[部署コード]	ユーザー名を使用するユーザーが所属する部署コードを入力します。 半角で40文字(全角で20文字)まで入力できます。
[備考]	ユーザー名を使用するユーザーの備考情報を入力します。 半角で128文字(全角で64文字)まで入力できます。

注1)ユーザーを追加する場合は、入力必須です。
注2)ユーザー情報を更新する場合は、入力できません。

ユーザーポリシー一覧

ツリー構成情報部分で選択したユーザーに設定するポリシーを指定できます。
設定内容の詳細は、“2.4.1 端末初期設定をおこなう”を参照してください。

メニューバー/ツールバー

[ユーザーポリシー設定]画面のメニューバーおよびツールバーについて説明します。

メニューバー		ツールバー	機能概要
[ファイル]	[ユーザー/ユーザーグループ検索]	―	[ユーザー/ユーザーグループ検索]画面を表示します。
	[ユーザーグループ作成]	―	[ユーザーグループ作成]画面を表示します。
	[ユーザーグループ削除]	―	[ユーザーグループ削除]画面を表示します。
	[ユーザーグループ部門管理者設定]	―	[グループの部門管理者設定]画面を表示します。部門管理者がログオンしている場合は、このメニューを選択できません。
	[ユーザーグループ部門管理者情報CSV取り込み]	―	[ユーザーグループ部門管理者情報CSV取り込みファイル指定]画面を表示します。
	[ユーザーグループ部門管理者情報CSV出力]	―	[ユーザーグループ部門管理者情報CSV出力ファイル指定]画面を表示します。
	[閉じる]	―	[ユーザーポリシー設定]画面を終了します。
[ツリー設定]	[ツリー最新表示]		ユーザーグループツリーの階層状態の最新情報を表示します。
	[ツリー全展開]	―	すべてのユーザーグループを表示します。

メニューバー		ツールバー	機能概要
	[ツリー全縮小]	－	ルート直下(ドメイン表示時はドメイン直下)のユーザーグループだけ表示します。
	[空のグループは表示しない]	－	配下にユーザーやユーザーグループが登録されていないユーザーグループを表示しません。
	[ユーザーグループ構成反映]		ユーザーグループツリーの階層状態を保存します。
[CSV連携]	[ユーザー情報CSV取り込み]	－	[ユーザー情報CSV取り込みファイル指定]画面を表示します。 Active Directory連携時、または部門管理者がログオンしている場合は、このメニューを選択できません。
	[ユーザー情報CSV出力]	－	[ユーザー情報CSV出力ファイル指定]画面を表示します。

3.3 CT/ユーザーをグループに割り当てる

構成情報ツリーが作成され、各グループのグループポリシーが決定したら、CTやユーザーをグループに割り当てます。

CTやユーザーのグループへの割り当てについては、以下の2とおりの考え方があります。

- システム管理者が、全CTやユーザーをグループに割り当てる
- 部門管理者を設定し、その部門管理者が操作できるグループについては、CTやユーザーの割り当てを任せる
  部門管理者を設定すると、部門内に限定したポリシーの運用やログの管理を、部門管理者に委譲することができるため、システム管理者の負荷を軽減できます。

3.3.1 CTを追加/移動/削除する

CTを追加する

管理コンソールにクライアント(CT)を追加するには、管理対象とするPCへのCTのインストールが必要です。クライアント(CT)のCTグループへの振り分け方法には、以下の2とおりがあります。

- ルート直下に配置されたクライアント(CT)を手動でCTグループへ移動する
- CT登録時自動振り分けファイルを使用して自動でクライアント(CT)をCTグループに割り当てる

ルート直下に配置されたクライアント(CT)を手動でCTグループへ移動する

管理コンソールのCTグループツリーやCTリストに、クライアント(CT)を新規に追加するために、管理対象とするPCにCTをインストールします。CTのインストールについては、“Systemwalker Desktop Keeper 導入ガイド”の“CTをインストールする”を参照してください。

インストール後にクライアント(CT)を再起動すると、統合管理サーバまたは管理サーバとの通信が開始され、CTグループツリーやCTリストにクライアント(CT)が追加されます。このとき、クライアント(CT)は、ルート直下に表示されますので、該当するCTグループへ移動してください。

CTグループツリーにおけるクライアント(CT)の表示位置については、“CTグループポリシーとCTポリシーの関係”または“構成情報ツリーの表示”を参照してください。
クライアント(CT)の移動方法については、“CTを移動する”を参照してください。

CT登録時自動振り分けファイルを使用して自動でクライアント(CT)をCTグループに割り当てる

管理対象とするPCへCTをインストールする前に、CT登録時自動振り分けファイルの設定が必要です。方法は、“CT登録時自動振り分けファイルを作成する”を参照してください。

注意

同一のCTが複数登録される原因

管理コンソールにおいて、同一のCTが複数登録される場合は、以下の原因が考えられます。

【原因1】

コンピュータ名が同じで、かつ、サーバ設定ツールのシステム設定におけるCT登録時動作で設定した内容（MACアドレス、所有者、OS種別）のどれかが違うCTがすでに登録されている状態で、CTをインストールした場合（LANカードの交換で、MACアドレスが変更となり、その後、CTをインストールした場合）

【原因2】

コンピュータ名が同じで、かつ、サーバ設定ツールのシステム設定におけるCT登録時動作で設定した内容（MACアドレス、所有者、OS種別）のどれかが違うCTがすでに登録されている状態で、CTの再登録コマンドを実行した場合（LANカードの交換で、MACアドレスが変更となり、その後、CTの再登録コマンドを実行した場合）

CTを移動する

CTリストに表示されているクライアント(CT)を、CTグループツリーのCTグループに移動する方法を説明します。

以下の場所に表示されているクライアント(CT)の移動は、システム管理者だけが実行できます。

- ルート直下
- ドメイングループ直下
- Localグループ直下

3階層のシステム構成で、統合管理サーバに接続されている管理コンソールで操作する場合、管理サーバをまたいだCTの移動はできません。

Active Directoryから構成情報を取り込んでいる場合、CTの移動については、“構成情報ツリーの表示”を参照してください。

手順を以下に示します。

1. [管理コンソール]画面を起動します。
2. CTグループツリーから、移動するクライアント(CT)が登録されているCTグループを選択します。
3. CTリストから移動するクライアント(CT)を選択します。
4. 移動先CTグループに、移動するクライアント(CT)をドラッグ&ドロップで移動します。

   →クライアント(CT)が移動されます。
5. [ツリー設定]メニューから[CTグループ構成反映]を選択します。

   →[構成反映]することで、移動したクライアント(CT)がデータベースに反映されます。

   [CTグループ構成反映]を実行しない場合、[ポリシー最新表示]、[次回起動時に更新する]、および[即時更新を行う]ボタンがグレーアウトされた状態になり、[CTグループ構成反映]を促すメッセージが表示されます。

CTを削除する

CTリストに表示されているクライアント(CT)を削除する方法を説明します。

以下の場所に表示されているクライアント(CT)の削除は、システム管理者だけが実行できます。

- ルート直下
- ドメイングループ直下
- Localグループ直下

Active Directoryから構成情報を取り込んでいる場合、CTの削除については、“構成情報ツリーの表示”を参照してください。

CTを削除すると、CTは「削除したCT」グループに移動します

管理コンソールでクライアント(CT)を削除し構成情報を反映すると、該当クライアント(CT)は管理コンソールに表示されなくなります。

このとき、クライアント(CT)は「削除したCT」グループに移動します。「削除したCT」グループは、通常は表示されません。管理コンソールの[ツリー設定]メニューで[「削除したCT」グループを表示]をチェック(システム管理者だけ操作可能)した場合に表示されます。「削除したCT」グループは、移動できません。また、「削除したCT」グループ配下にグループを作成することもできません。

「削除したCT」グループに移動したクライアント(CT)の管理情報は、(統合)管理サーバに残っているため、後で蓄積されたログを参照する場合は、ログビューアで参照できます。

また、「削除したCT」グループに移動したクライアント(CT)は、再利用することができます。この場合は、「削除したCT」グループのクライアント(CT)を、他のグループに移動します。Active Directory連携時は、Localグループ配下へ移動できます。移動後は、構成情報の反映が必要です。

不要と判断して削除するクライアント(CT)について、今後ログをログビューアで見る可能性がある場合は、「削除したCT」グループに所属させておくことをお勧めします。

「削除したCT」グループのCTを削除すると、CTは復元できません

「削除したCT」グループに所属するクライアント(CT)を削除し、構成反映を行った場合は、「削除したCT」グループにクライアント(CT)が表示されなくなり、管理情報が(統合)管理サーバから削除されます。したがって、蓄積されていたログをログビューアで参照できなくなります。バックアップコマンドを実行してCSVファイルを出力すれば、ログを確認できます。

また、削除したクライアント(CT)を再度、管理コンソールに表示するには、対象のPCでCTをアンインストール後、再インストールする必要があります。CTのインストールについては、“Systemwalker Desktop Keeper 導入ガイド”の“CTをインストールする”を参照してください。
ただし、再インストールにより管理コンソールに表示されたクライアント(CT)は、削除されたクライアント(CT)とは異なるものと判断されます。したがって、再表示されても、削除前のログをログビューアで参照することはできません。

手順を以下に示します。

1. [管理コンソール]画面を起動します。
2. CTグループツリーから、削除するCTが登録されているCTグループを選択します。
3. CTリストから削除するCTを選択し、右クリックします。

   →ポップアップメニューが表示されます。
4. 表示されたポップアップメニューから[CT削除]を選択します。

   →削除確認画面が表示されます。
5. 削除する場合は[OK]ボタンをクリックします。

   →選択したクライアント(CT)が削除されます。
6. [ツリー設定]メニューから[CTグループ構成反映]を選択します。

   →削除したCTが、「削除したCT」グループに移動します。

   [CTグループ構成反映]を実行しない場合、[ポリシー最新表示]、[次回起動時に更新する]、および[即時更新を行う]ボタンがグレーアウトされた状態になり、[CTグループ構成反映]を促すメッセージが表示されます。

   CTが「削除したCT」グループに所属している間は、ログビューアでのログビューア参照や、他のCTグループへの復帰が可能です。

7. 構成情報ツリーで「削除したCT」グループを選択します。
8. CTリストから削除するCTを選択し、右クリックし、[CT削除]を選択します。
9. 削除する場合は[OK]ボタンをクリックします。

   →選択したクライアント(CT)が削除されます。

10. [ツリー設定]メニューから[CTグループ構成反映]を選択します。

    →構成反映することで、削除したCTがデータベースに反映されます。CTは復元できません。

    [CTグループ構成反映]を実行しない場合、[ポリシー最新表示]、[次回起動時に更新する]、および[即時更新を行う]ボタンがグレーアウトされた状態になり、[CTグループ構成反映]を促すメッセージが表示されます。

3.3.2 ユーザーを登録する

ユーザーをグループに割り当てるために、該当するグループにユーザーを登録します。

Active Directoryから構成情報を取り込んでいる場合のユーザーの登録については、“構成情報ツリーの表示”を参照してください。

ポイント

ユーザーポリシーを一元管理している場合は、統合管理サーバから操作してください

サーバ設定ツールでユーザーポリシーを一元管理する設定にしている場合は、統合管理サーバでユーザーを追加、更新、移動、削除してください。

ユーザーを登録するには、以下の2とおりの方法があります。

- ユーザーを1人ずつ登録する
- ユーザーをCSVファイルを使用して一括登録する

  Active Directory連携を実施していない場合は、1回の操作で登録できる件数は10,000件までです。
  Active Directory連携を実施している場合は、1回の操作で、構成情報ツリーのLocalグループ配下に登録できる件数は、10万件までです。

  実行するには、管理コンソールに対して[CSVファイル取り込み]権限を持っていることが必要です。権限の設定は、サーバ設定ツールの[管理者情報設定]画面の[詳細権限]で行います。

  事前に、割り当てるユーザー情報のCSVファイルを作成しておく必要があります。CSVファイルの詳細は、“Systemwalker Desktop Keeper リファレンスマニュアル”の“ユーザー情報”を参照してください。

注意

登録情報を正しく設定してください

登録情報はCSVファイルに正しく設定してください。以降の説明のとおりにCSVファイルが作成されていない場合や、1行でもエラーがある場合は、すべてのユーザーが登録されません(正しく設定されている部分も登録されずに処理が終了します)。したがって、全ユーザーの再登録が必要です。

ユーザーを1人ずつ登録する

手順を以下に示します。

1. [管理コンソール]を起動します。

2. [ユーザー設定]メニューから[ユーザーポリシー設定]を選択します。

   →[ユーザーポリシー設定]画面が表示されます。

   ユーザー一覧およびユーザー属性には、何も表示されません。
   ユーザーポリシー一覧には、[端末初期設定]画面の各タブに設定されている初期値が表示されます。
   以下のログの採取は、ユーザーポリシーとして設定できません。そのため、[ユーザーポリシー設定]画面の[各種ログスイッチ]タブでは、これらのログの採取を選択するボタンはありません。以下のログを採取する場合は、CTポリシーとして設定してください。

   ー ファイル操作ログ

   ー ログオン/ログオフログ

   ー 連携アプリケーションログ

3. ユーザーグループツリーで、ユーザーを登録するユーザーグループを選択します。
4. ユーザー属性の[新しいユーザーの入力]ボタンをクリックします。
5. 必要な情報をユーザー属性に入力し、[追加]ボタンをクリックします。
   入力情報の詳細は、“ユーザー属性”を参照してください。

   →ユーザーポリシーとして端末初期設定の値が設定され、確認画面が表示されます。

6. [OK]ボタンをクリックします。

ユーザーをCSVファイルを使用して一括登録する

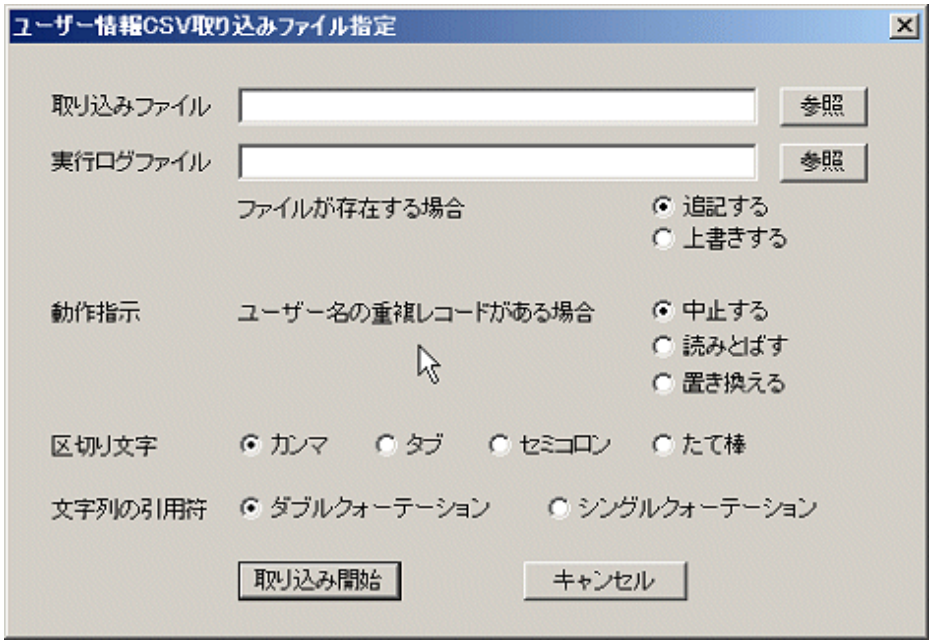
CSVファイルを使用してユーザーを一括で割り当てる方法を説明します。

1. [管理コンソール]を起動します。
2. [ユーザー設定]メニューから[ユーザーポリシー設定]を選択します。

   →[ユーザーポリシー設定]画面が表示されます。

3. [CSV連携]メニューの[ユーザー情報CSV取り込み]を選択します。

→[ユーザー情報CSV取り込みファイル指定]画面が表示されます。



項目名	説明
[取り込みファイル] (必須)	作成したCSVファイルを指定します。指定方法は、以下のとおりです。 ・ フルパスでファイル名を入力する 入力欄に取り込むCSVファイルまでのパスをフルパスで入力します。 ・ [参照]ボタンから入力する [取り込みファイルの指定]画面が表示されるので、取り込むCSVファイルを指定したあとに、[開く]ボタンをクリックします。 指定できるフルパスの長さは、半角で218文字まで入力できます。ただし、以下の記号はファイル名として使用できません。 使用できない記号:「¥」「/」「:」「*」「?」「"」「<」「>」「|」
[実行ログファイル] (必須)	CSVファイルを取り込む際の実行結果を出力するファイルを指定します。このファイルには、取り込み時のエラーも出力されます。指定方法は、以下のとおりです。 ・ フルパスでファイル名を入力する 入力欄に出力するログファイルまでのパスをフルパスで入力します。 ・ [参照]ボタンから入力する [実行ログファイルの指定]画面が表示されるので、出力するログファイルを指定したあとに、[開く]ボタンをクリックします。 指定できるフルパスの長さは、半角で218文字まで入力できます。ただし、以下の記号はファイル名として使用できません。 使用できない記号:「¥」「/」「:」「*」「?」「"」「<」「>」「|」
[ファイルが存在する場合] (必須)	[実行ログファイル]で、すでにログが出力されているファイルを指定した場合の出力方法について選択します。 ・ [追記する] 前回の情報を残した状態で、実行ログを追記します。 ・ [上書きする] 前回の情報は残さずに、実行ログを出力します。

項目名	説明
[動作指示] (必須)	CSVファイルを取り込む際に、重複する[ユーザー名]があった場合の動作を選択します。 ・ [中止する] 重複する[ユーザー名]があった時点で、CSVファイルの取り込みを中止します。なお、中止前までのユーザー情報は取り込まれます。 ・ [読みとばす] 重複する[ユーザー名]だけを取り込みません。重複しない[ユーザー名]のユーザー情報は取り込まれます。 ・ [置き換える] 重複する[ユーザー名]の情報を、取り込む情報で更新します。重複しない[ユーザー名]のユーザー情報はCSVファイルのまま取り込まれます。なお、重複していた場合、ユーザー情報はCSVファイルの情報に置き換えられますが、ユーザーポリシーは変更されません。
[区切り文字] (必須)	CSVファイルを作成するときに入力した区切り文字を選択します。選択を間違えると、エラーになります。
[文字列の引用符] (必須)	CSVファイルを作成するときに入力した文字列の引用符を選択します。 選択を間違えると、以下の不具合が発生します。 ・ CSVファイル作成時にダブルクォーテーションを使用し、ここでシングルクォーテーションを選択すると、エラーとなります。 ・ CSVファイル作成時にシングルクォーテーションを使用し、ここでダブルクォーテーションを選択すると、ユーザー情報として、シングルクォーテーションが各項目の前後に含まれて登録されます。

4. 上記の情報をすべて入力したあとに、[取り込み開始]ボタンをクリックします。

   →[ユーザー情報CSV取り込み状態表示]画面が表示され、CSVファイルの取り込みが開始されます。
   エラーがある場合は、[ユーザー情報CSV取り込み状態表示]画面に表示されます。また、同じ内容が実行ログファイルにも出力されます。エラー内容を確認してCSVファイルを修正し、すべてのユーザー情報を再度登録してください。

5. [ユーザーポリシー設定]画面に戻り、[ユーザー一覧最新表示]ボタンをクリックします。

   →CSVファイルから取り込んだユーザー情報が表示されます。

3.3.3 ユーザーを更新/移動/削除する

ユーザーを更新する

登録済みのユーザーを更新するには、以下の2とおりの方法があります。

- CSVファイルを使用して更新する
- 画面から更新する

CSVファイルを使用して更新する

更新方法は、“ユーザーをCSVファイルを使用して一括登録する”を参照してください。

画面から更新する

手順を以下に示します。

1. [管理コンソール]を起動します。

2. [ユーザー設定]メニューから[ユーザーポリシー設定]を選択します。

   →[ユーザーポリシー設定]画面が表示されます。

3. 以下のどちらかの方法により、ユーザー情報を更新します。

   ・ユーザーを1つずつ更新する場合

   ・ユーザーをまとめて更新する場合

【ユーザーを1つずつ更新する場合】

a) [ユーザー一覧]から更新する行を1つ選択し、以下の情報を入力後、[更新]ボタンをクリックします。[ユーザー名]については更新できません。

項目名	説明
[使用者名]	ユーザー名を使用するユーザーの名前を入力します。 半角で128文字(全角で64文字)まで入力できます。
[従業員番号]	ユーザー名を使用するユーザーの従業員番号を入力します。 半角で40文字(全角で20文字)まで入力できます。
[役職]	ユーザー名を使用するユーザーの役職を入力します。 半角で128文字(全角で64文字)まで入力できます。
[部署名]	ユーザー名を使用するユーザーが所属する部署名を入力します。 半角で128文字(全角で64文字)まで入力できます。
[部署コード]	ユーザー名を使用するユーザーが所属する部署コードを入力します。 半角で40文字(全角で20文字)まで入力できます。
[備考]	ユーザー名を使用するユーザーの備考情報を入力します。 半角で128文字(全角で64文字)まで入力できます。

b) 確認画面が表示されますので、[OK]ボタンをクリックします。

→入力した情報がデータベースに反映され、[ユーザー一覧]に表示されます。

【ユーザーをまとめて更新する場合】

[ユーザー一覧]から更新する行を[Shift]キーまたは[Ctrl]キーを押しながら選択し、以下の情報を入力したあとに、[ユーザー情報更新]ボタンをクリックします。
・[役職]
・[部署名]
・[部署コード]
・[備考]

[ユーザー名]、[使用者名]、および[従業員番号]については更新できません。
情報を更新しなかった項目は、現在[ユーザー一覧]に表示されている情報のまま、変更されません。ただし、半角空白または全角空白を入力した場合は、空白で更新されます。
入力値は、“【ユーザーを1つずつ更新する場合】”の表を参照してください。

→入力した情報がデータベースに反映され、[ユーザー一覧]に表示されます。

ユーザーを移動する

ユーザーを移動する場合、ユーザーポリシーは変更されません。(移動する前と変わりません)

手順を以下に示します。

1. [ユーザーポリシー設定]画面を起動します。
2. ユーザーグループツリーから移動するユーザーが所属するユーザーグループを選択します。

   →選択したユーザーグループが反転表示されます。

3. 同一サーバ配下の移動先ユーザーグループに、移動するユーザーをドラッグ&ドロップで移動します。

   →ユーザーが移動されます。

4. [ツリー設定]メニューから[ユーザーグループ構成反映]を選択します。

   →移動したユーザーがデータベースに反映されます。

   [ユーザーグループ構成反映]を実行しない場合、[ユーザーポリシー設定]画面を閉じたときに、[ユーザーグループ構成反映]を促すメッセージが表示されます。

ユーザーを削除する

登録済みのユーザーを削除する方法について説明します。

手順を以下に示します。

1. [管理コンソール]を起動します。
2. [ユーザー設定]メニューから[ユーザーポリシー設定]を選択します。

   →[ユーザーポリシー設定]画面が表示されます。

3. [ユーザー一覧]から削除する行を選択し、[削除]ボタンをクリックします。

   →確認画面が表示されます。

4. [OK]ボタンをクリックします。

   →削除した情報がデータベースに反映され、[ユーザー一覧]から削除されます。

3.4 CTポリシー/ユーザーポリシーを変更する

構成情報ツリーを作成後、グループに割り当てたCTやユーザーのポリシーを、必要に応じて変更します。

ポリシーの変更については、以下の2とおりの考え方があります。

- システム管理者が、ポリシーを変更する
- 部門管理者を設定し、その部門管理者が管理できるグループについては、ポリシーの変更を任せる

3.4.1 CTポリシーを変更する

CTポリシーを変更する

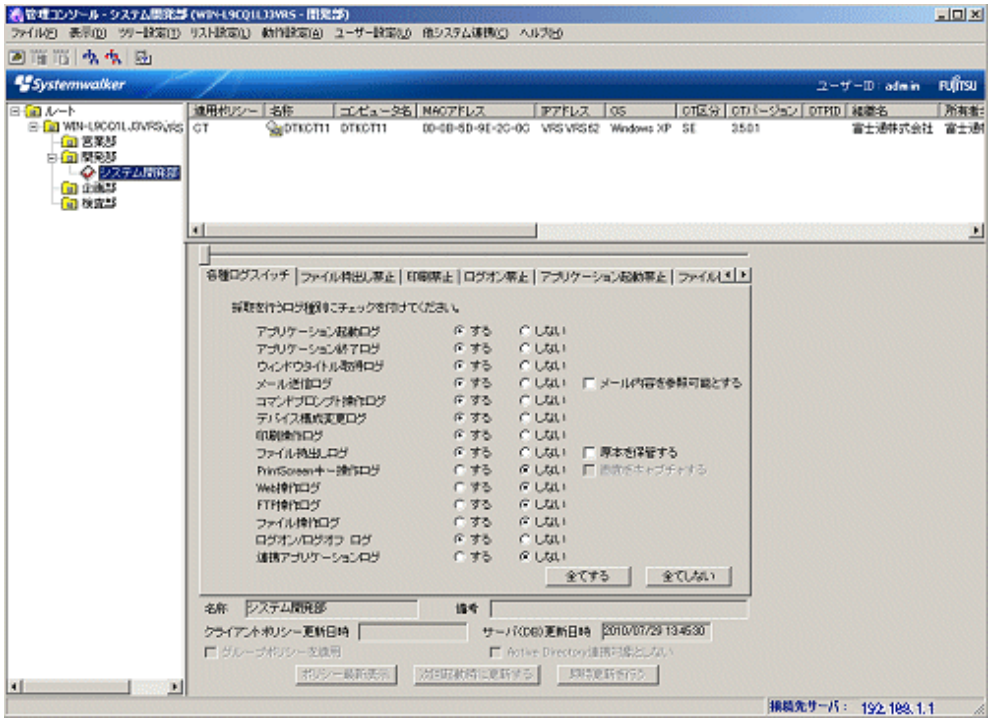
「削除したCT」グループに所属するクライアント(CT)のCTポリシーは、変更できません。名称、備考も変更できません。

CTポリシーの変更手順を説明します。

1. [管理コンソール]を起動します。

2. CTグループツリーから、ポリシーを変更するCTが所属するCTグループを選択します。

   →最新のポリシー情報が表示されます。



注意

以下の場合は、CTグループやCTリストの情報を最新にしてください

以下の条件のどちらかを満たす場合、画面に表示される統合管理サーバ配下の管理サーバの、CTグループ、およびCTリストの情報は最新になっていない場合があります。

- 管理サーバ側でCTグループツリーが変更された場合
- Active Directory連携が実行され、グループツリーが変更となった場合

最新にするには、[ツリー設定]メニューから[ツリー最新表示]を選択してください。

3. CTリストからポリシーを変更するCTを選択します。
4. ポリシー一覧の各タブで、ポリシーを変更します。

   ポリシーの設定項目の説明は、“2.4.1 端末初期設定をおこなう”を参照してください。
5. 必要に応じて、CTリストに表示されている[名称]または[備考]を変更します。

   [名称]および[備考]に入力できる文字は、以下のとおりです。

   - [名称]: 半角で40文字(全角で20文字)までの英数字、漢字、ひらがな、またはカタカナを入力できます。
   - [備考]: 半角で127文字(全角で63文字)までの英数字、漢字、ひらがな、またはカタカナが入力できます。
6. 以下のどちらかのボタンをクリックし、ポリシーをCTに反映します。

   - [次回起動時に更新する]ボタンをクリックする場合

     各タブのポリシーがデータベースに反映されます。ただしクライアント(CT)には、即時にポリシーが反映されません。次回のクライアント(CT)起動時、クライアント(CT)が接続するサーバ(統合管理サーバ、または管理サーバ)と通信が行われたときに、最新のポリシーが反映されます。

ー [即時更新を行う]ボタンをクリックする場合

- 各タブのポリシーがデータベースに反映され、稼働しているクライアント(CT)にも反映されます。
  ただし、[ファイル持出し禁止]タブの設定は、即時更新を行ったクライアント(CT)で持出しユーティリティが起動されていた場合は、次回の持出しユーティリティ起動時からポリシーが反映されます。
- [印刷禁止]タブで許可しているアプリケーションが、即時更新を行ったクライアント(CT)で起動されていた場合は、次回のアプリケーション起動時からポリシーが反映されます。
- [ログオン禁止]タブの設定でログオフまたはシャットダウンする設定にした場合、起動中のクライアント(CT)には即時に反映され、ログオフまたはシャットダウンされます。なお、稼働していないクライアント(CT)や、上位サーバと通信できないクライアント(CT)では、次回のクライアント(CT)起動時、クライアント(CT)が接続するサーバ(統合管理サーバ、または管理サーバ)と通信が行われたときに、最新のポリシーが反映されます。

ポイント

クライアント(CT)数が多い場合は、[次回起動時に更新する]を選択することを推奨します

統合管理サーバまたは管理サーバと接続されていないクライアント(CT)との接続タイムアウト時間は、クライアント(CT)1台につき5秒です。また、ネットワーク環境にも依存しますが、統合管理サーバまたは管理サーバと接続されているクライアント(CT)に、[即時更新]を行うと、ポリシー適用に要する時間は、クライアント(CT)1台につき1秒程度かかります。
そのため、ポリシーの設定対象とするCT数が多いときは、[次回起動時に更新する]ボタンをクリックする運用を推奨します。

→[名称]または[備考]を変更した場合は、ポリシーが反映されると、入力した情報が、CTリストに反映されます。

クライアント(CT)にグループポリシーを適用する場合

クライアント(CT)にCTポリシーを適用せず、そのクライアント(CT)が所属するCTグループのグループポリシーを適用することもできます。この場合は、[グループポリシーを適用]チェックボックスをチェックし、ポリシーの反映操作を実施してください。

CTグループを選択して配下のCTのポリシーを一括変更する

CTグループポリシーの設定時に、そのCTグループ配下のクライアント(CT)にも、ポリシーを一括で設定できます。この場合、CTポリシーの設定値とCTグループポリシーの設定値は、同じです。

設定手順の詳細は、“3.2.1 CTグループポリシーを変更する”を参照してください。

CTポリシーをコピーする

CTにすでに設定されているCTポリシーを、ほかのクライアント(CT)にコピーする方法を説明します。
ポリシーのコピーを利用すると、同じCTポリシーをほかのクライアント(CT)に設定できます。

手順を以下に示します。

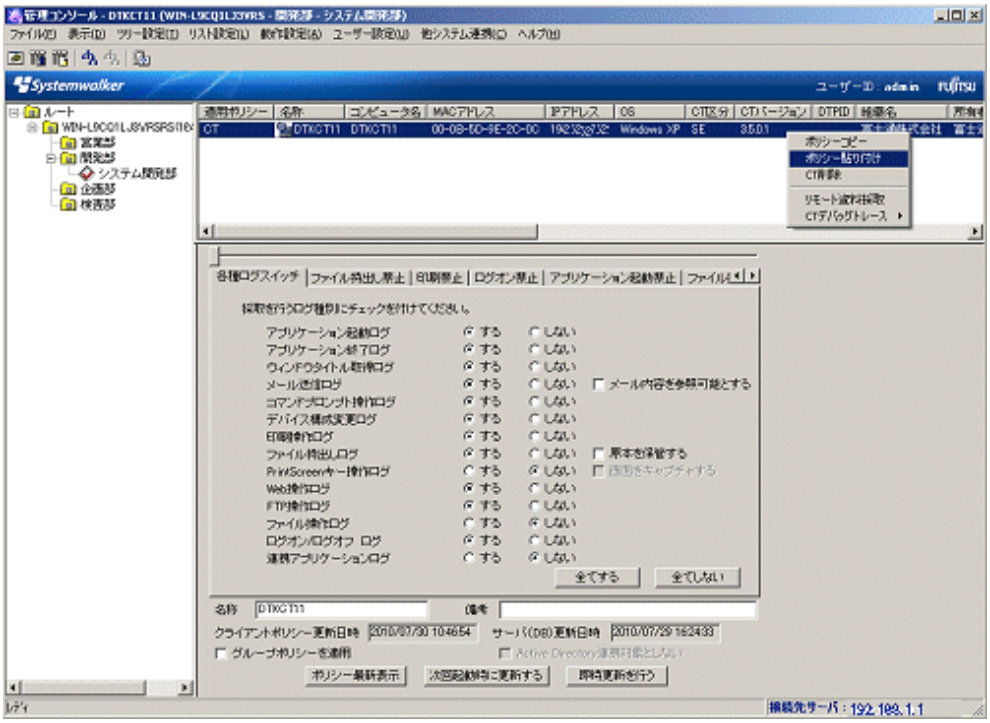
1. [管理コンソール]画面を起動します。
2. CTグループツリーから、コピー元となるクライアント(CT)が登録されているCTグループを選択します。

3. CTリストからコピー元となるクライアント(CT)を選択し、右クリックします。

   →ポップアップメニューが表示されます。

4. 表示されたポップアップメニューから[ポリシーコピー]を選択します。
5. CTグループツリーから、コピー先となるクライアント(CT)が登録されているCTグループを選択します。
6. CTリストからコピー先となるクライアント(CT)を選択し、右クリックします。

   →ポップアップメニューが表示されます。



7. 表示されたポップアップメニューから[ポリシー貼り付け]を選択します。

   →ポリシー複写の確認画面が表示されます。

8. ポリシーを複写し、複写後のポリシーをクライアント(CT)に即時反映する場合は[はい]を、ポリシーを複写し、複写後のポリシーは次回起動時に反映させる場合は[いいえ]を、ポリシーの複写をキャンセルする場合は[キャンセル]をクリックします。

3.4.2 ユーザーポリシーを変更する

ユーザーポリシーを変更する

ユーザーポリシーを変更する場合、以下の3とおりの方法があります。

- 1人ずつユーザーポリシーを変更する
- 複数人選択してユーザーポリシーを一括変更する
- ユーザーグループを選択して配下のユーザーのポリシーを一括変更する

1人ずつユーザーポリシーを変更する

手順を以下に示します。

1. [管理コンソール]を起動します。
2. [ユーザー設定]メニューから[ユーザーポリシー設定]を選択します。

   →[ユーザーポリシー設定]画面が表示されます。

[使用者名]、[従業員番号]、[役職]、[部署名]、[部署コード]、および[備考]を変更した場合は、変更した値がその[ユーザー名]の情報として反映されます。

3. ポリシー一覧の各タブで、ポリシーを変更します。

   ユーザー固有のポリシーを設定できます。ポリシーの設定項目の説明は、“2.4.1 端末初期設定をおこなう”を参照してください。

   - [端末初期設定]画面の値をポリシーとして設定する場合は、[端末初期設定値を設定]ボタンをクリックしてください。[端末初期設定]画面については、“2.4.1 端末初期設定をおこなう”を参照してください。
   - そのユーザーが所属するユーザーグループのユーザーグループポリシーを適用する場合は、[グループポリシーを適用]をチェックしてください。(複数ユーザー選択時も可能です)
   - ユーザーポリシーの適用を一時的に解除し、CTポリシーを適用する場合は、[ユーザーポリシーを無効にする]をチェックしてください。再度、ユーザーポリシーを適用する場合は、チェックを外してください。

4. [更新]ボタンをクリックします。

   →設定したポリシーは、次回ログオン時に反映されます。
   または、ポリシーを変更されたユーザーがクライアント(CT)にログオンしている場合、そのクライアント(CT)に対して、CTポリシーの即時更新を実施すれば、変更したユーザーポリシーが即時に反映されます。

複数人選択してユーザーポリシーを一括変更する

手順を以下に示します。

1. [管理コンソール]を起動します。
2. [ユーザー設定]メニューから[ユーザーポリシー設定]を選択します。

   →[ユーザーポリシー設定]画面が表示されます。

3. [ユーザー一覧]からポリシーを設定する行を[Shift]キーまたは[Ctrl]キーを押しながら選択します。

   →ポリシーには、[端末初期設定]画面の値が設定されます。
   [ユーザー名]、[使用者名]、および[従業員番号]にはマスクがかかり入力できません。
   [役職]、[部署名]、[部署コード]、および[備考]の値は、指定なし(未設定)となります。
   [端末初期設定]画面については、“2.4.1 端末初期設定をおこなう”を参照してください。

4. ポリシー一覧の各タブで、ポリシーを変更します。

   ポリシーの設定項目の説明は、“端2.4.1 端末初期設定をおこなう”を参照してください。

5. [更新]ボタンをクリックします。

   →設定したポリシーは、次回ログオン時からユーザーに反映されます。
   [役職]、[部署名]、[部署コード]、および[備考] に値を入力して[更新]ボタンをクリックした場合、選択したすべてのユーザーに対して、入力した値が設定されます。また、半角空白または全角空白を入力した場合、空白で更新されます。

ユーザーグループを選択して配下のユーザーのポリシーを一括変更する

ユーザーグループポリシーの設定時に、そのユーザーグループ配下のユーザーにも、ポリシーを一括で設定できます。
設定手順の詳細は、“3.2.2 ユーザーグループポリシーを変更する”を参照してください。

ユーザーポリシーをコピーする

すでに設定されているユーザーポリシーを、ほかのユーザーにコピーする方法を説明します。
ポリシーのコピーを利用すると、同じユーザーポリシーをほかのユーザーに設定できます。

手順を以下に示します。

1. [管理コンソール]を起動します。

2. [ユーザー設定]メニューから[ユーザーポリシー設定]を選択します。

   →[ユーザーポリシー設定]画面が表示されます。

3. ユーザーグループツリーから、コピー元となるユーザーが登録されているユーザーグループを選択します。

4. [ユーザー一覧]からコピー元となるユーザーを選択し、右クリックします。

   →ポップアップメニューが表示されます。

5. 表示されたポップアップメニューから[ポリシーコピー]を選択します。

6. ユーザーグループツリーから、コピー先となるユーザーが登録されているユーザーグループを選択します。

7. [ユーザー一覧]からコピー先となるユーザーを選択し、右クリックします。

   →ポップアップメニューが表示されます。

8. 表示されたポップアップメニューから[ポリシー貼り付け]を選択します。

   →ポリシー複写の確認画面が表示されます。

9. [はい]ボタンをクリックします。

   →コピーしたポリシーは、次回ログオン時に反映されます。
   または、コピー先のユーザーがクライアント(CT)にログオンしている場合、そのクライアント(CT)に対して、CTポリシーの即時更新を実施すれば、コピーしたユーザーポリシーが即時に反映されます。

3.5 CT情報/ユーザー情報を出力する

ログを参照した結果、不正行為が行われたクライアント(CT)や不正行為を実施した利用者の存在を確認した場合に、クライアント(CT)情報やユーザー情報の検索結果を、CSV形式で出力することができます。

管理コンソールのCTリストに表示されている情報やCTポリシー情報、ユーザーポリシーのユーザー情報をCSVファイルに出力する方法について説明します。

CT情報を出力する

管理コンソールのCTリストに表示されている情報をCSVファイルに出力する方法について説明します。

本作業は、以下の条件をすべて満たしているユーザーが実施できます。

- システム管理者、または部門管理者として登録されている。
- 管理コンソールに対するアクセス権がある。
- CSVファイル保存権限がある。

これらの条件の設定は、導入時にサーバ設定ツールで設定されています。

「削除したCT」グループに所属するCT情報を、CSVファイルに出力することはできません。

以下に手順を説明します。

1. [管理コンソール]を起動します。
2. [ファイル]メニューから[CT情報CSV出力]を選択します。

   →[CT情報CSV出力ファイル指定]画面が表示されます。

3. 以下の情報を入力したあとに、[出力開始]ボタンをクリックします。

項目名	説明
[出力ファイル]	出力するCSVファイルを指定します。指定方法は、以下のとおりです。 ・ フルパスでファイル名を入力する 入力欄に取り込むCSVファイルまでのパスをフルパスで入力します。 ・ [参照]ボタンから入力する [出力ファイルの指定]画面が表示されるので、出力するCSVファイルのドライブおよびファイル名を入力したあとに、[保存]ボタンをクリックします。 指定できるフルパスの長さは、半角で218文字まで入力できます。ただし、以下の記号はファイル名として使用できません。 使用できない記号:「¥」「/」「:」「*」「?」「"」「<」「>」「|」
[区切り文字]	CSVファイルを出力するときの区切り文字を選択します。
[文字列の引用符]	CSVファイルを出力するときの文字列の引用符を選択します。
[出力形式]	出力するCSVファイルの形式を選択します。 [V12.0L20 Base Edition 互換形式]:V12.0L20 Base Edition形式で出力します。 [V12.0L20 Standard Edition 互換形式]:V12.0L20 Standard Edition 互換形式形式で出力します。 [V13.0.0 互換形式]:V13.0.0 互換形式形式で出力します。 [V13.2.0 形式]:V13.2.0形式で出力します。 出力されるCSVファイルの項目名と出力情報の説明については、“Systemwalker Desktop Keeper リファレンスマニュアル”の“CT情報”を参照してください。

   →CSVファイルが出力されます。

   出力された項目の中に、[文字列の引用符]で選択した文字と同じ文字があった場合、その文字の前に[文字列の引用符]で選択した1文字が追加されます。

   出力先に同じ名前のファイルが存在していた場合は上書きするかどうか選択する画面が表示されます。上書きする場合は[OK]ボタンをクリックしてください。

CTグループ情報を出力する

管理コンソールのCTグループツリー表示されている情報をCSVファイルに出力する方法について説明します。

本作業は、以下の条件をすべて満たしているユーザーが実施できます。これらの条件の設定は、導入時にサーバ設定ツールで設定されています。

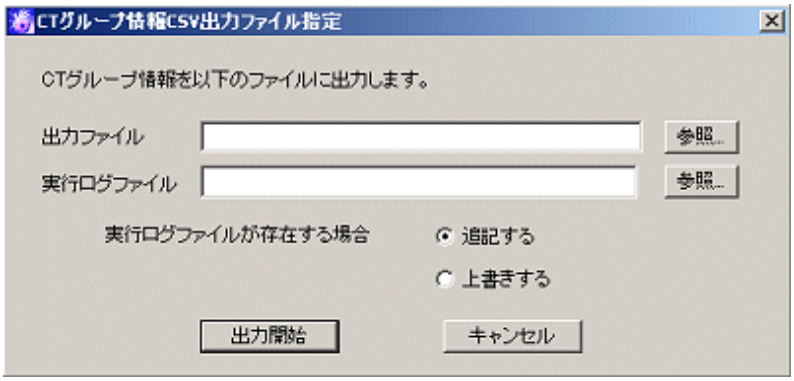
- システム管理者として登録されている。
- 管理コンソールに対するアクセス権がある。
- CSVファイル保存権限がある。

CTグループ情報は、管理サーバごとに出力できます。
統合管理サーバに接続する管理コンソールでCTグループ情報を出力する場合は、統合管理サーバ直下のクライアント(CT)のグループ情報が出力されます。
Active Directory連携時は、Localグループの情報だけ出力されます。

以下に手順を説明します。

1. [管理コンソール]を起動します。
2. [ファイル]メニューから[CTグループ情報CSV出力]を選択します。

   →[CTグループ情報CSV出力ファイル指定]画面が表示されます。



3. 以下の情報を入力したあとに、[出力開始]ボタンをクリックします。

項目名	説明
[出力ファイル] (必須)	CTグループ情報を出力するCSVファイルをフルパスで指定します。 指定できるフルパスの長さは、半角で218文字まで入力できます。ただし、以下の記号はファイル名として使用できません。 使用できない記号:「¥」「/」「:」「*」「?」「"」「<」「>」「|」 ・ Windows Vista®、Windows® 7、Windows Server® 2008以外の場合 **初期値:**[OSインストールドライブ]¥Documents and Settings¥ログオンユーザー名¥My Documents¥DTKCTEntry.csv です。 ・ Windows Vista®、Windows® 7、Windows Server® 2008の場合 **初期値:**[OSインストールドライブ]¥User¥ログオンユーザー名¥Documents¥DTKCTEntry.csv です。
[実行ログファイル] (必須)	実行結果を保存するファイルを、フルパスで指定します。 半角で218文字まで入力できます。ただし、以下の記号はファイル名として使用できません。 使用できない記号:「¥」「/」「:」「*」「?」「"」「<」「>」「|」 ・ Windows Vista®、Windows® 7、Windows Server® 2008以外の場合 **初期値:**[OSインストールドライブ]¥Documents and Settings¥ログオンユーザー名¥My Documents¥DTKCTEntry.log です。

項目名	説明
	・ Windows Vista®、Windows® 7、Windows Server® 2008の場合 **初期値：**[OSインストールドライブ]¥User¥ログオンユーザー名¥Documents¥DTKCTEntry.log です。
[実行ログファイルが存在する場合]	既存の実行ログファイルが存在する場合は必ず設定してください。 ・ [追記する]:既存の実行ログファイルに追記する場合に選択します。 ・ [上書きする]:既存の実行ログファイルに上書きする場合に選択します。

→CSVファイルが出力されます。
出力されるCSVファイルの項目名と出力情報の説明については、“Systemwalker Desktop Keeper リファレンスマニュアル”の“CTグループ情報”を参照してください。

ユーザー情報を出力する

[ユーザーポリシー設定]画面のユーザー一覧に表示されている情報をCSVファイルに出力する方法について説明します。

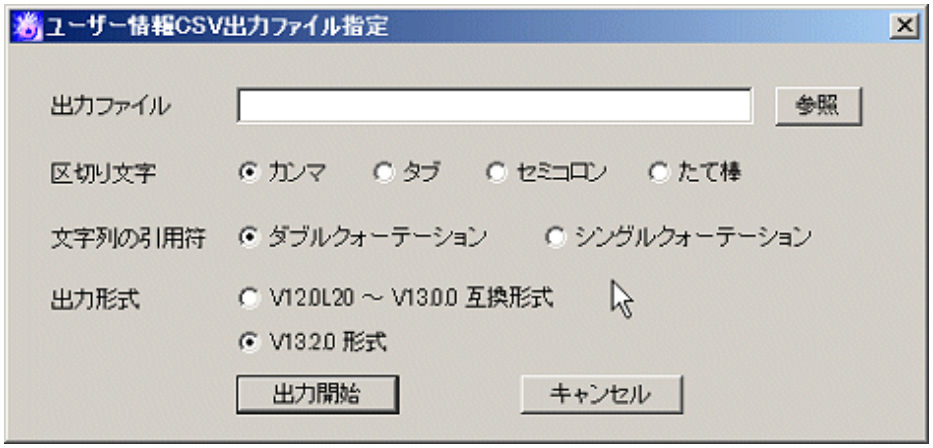
本作業は、以下の条件をすべて満たしているユーザーが実施できます。

- システム管理者、または部門管理者として登録されている。
- 管理コンソールに対するアクセス権がある。
- CSVファイル保存権限がある。

これらの条件の設定は、導入時にサーバ設定ツールで設定されています。

以下に手順を説明します。

1. [管理コンソール]を起動します。
2. [ユーザー設定]メニューから[ユーザーポリシー設定]を選択します。
   →[ユーザーポリシー設定]画面が表示されます。
3. [CSV連携]メニューから[ユーザー情報CSV出力]を選択します。
   →[ユーザー情報CSV出力ファイル指定]画面が表示されます。



4. 以下の情報を入力したあとに、[出力開始]ボタンをクリックします。

項目名	説明
[出力ファイル] (必須)	出力するCSVファイルを指定します。指定方法は、以下のとおりです。 ・ フルパスでファイル名を入力する 入力欄に取り込むCSVファイルまでのパスをフルパスで入力します。

項目名	説明
	・ [参照]ボタンから入力する [出力ファイルの指定]画面が表示されるので、出力するCSVファイルのドライブおよびファイル名を入力したあとに、[保存]ボタンをクリックします。 指定できるフルパスの長さは、半角で218文字まで入力できます。ただし、以下の記号はファイル名として使用できません。 使用できない記号:「¥」「/」「:」「*」「?」「"」「<」「>」「|」
[区切り文字](必須)	CSVファイルを出力するときの区切り文字を選択します。
[文字列の引用符](必須)	CSVファイルを出力するときの文字列の引用符を選択します。
[出力形式]	出力するCSVファイルの形式を選択します。 [V12.0L20～V13.0.0 互換形式]:V13.0.0以前と同じ形式で出力します。 [V13.2.0 形式]:V13.2.0形式で出力します。 出力されるCSVファイルの項目名と出力情報の説明については、“Systemwalker Desktop Keeper リファレンスマニュアル”の“ユーザー情報”を参照してください。

→CSVファイルが出力されます。

出力された項目の中に、[文字列の引用符]で選択した文字と同じ文字があった場合、その文字の前に[文字列の引用符]で選択した1文字が追加されます。

出力先に同じ名前のファイルが存在していた場合は上書きするかどうか選択する画面が表示されます。上書きする場合は[OK]ボタンをクリックしてください。

クライアント(CT)のIPアドレスを出力する

以下に示す状況の場合、自己版数アップするクライアント(CT)を選択できます。このとき使用するファイルのフォーマットとして、サーバ配下またはCTグループ配下の、クライアント(CT)のIPアドレスを出力します。

- クライアント(CT)のバージョンアップを全体展開する前に特定の部門だけでテストしたい場合
- 部門ごとや事業所ごとに、順次、クライアント(CT)をバージョンアップしたい場合
- 負荷分散のため、クライアント(CT)台数を区切ってバージョンアップしたい場合

出力したファイルの利用方法は、“Systemwalker Desktop Keeper 導入ガイド”の“CTをバージョンアップする”を参照してください。

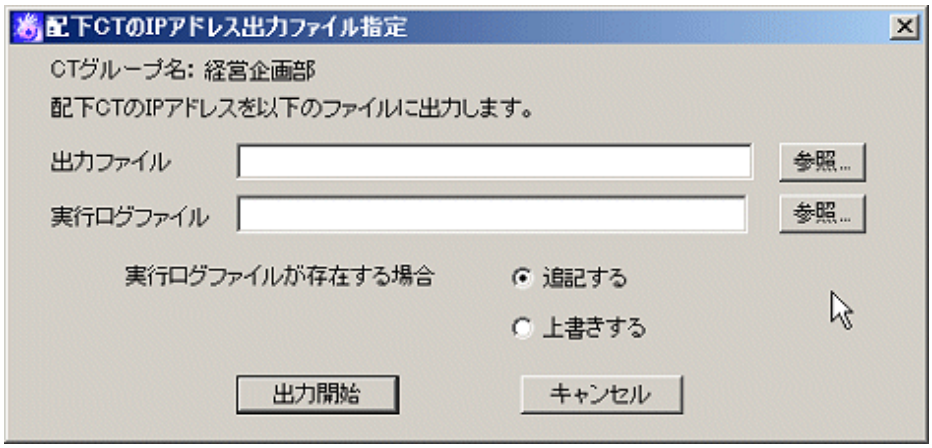
また、システム管理者や部門管理者が、CTグループ単位で管理PCを確認する場合にも利用できます。

以下にファイルを出力する手順を説明します。

1. [管理コンソール]を起動し、CTグループツリーで、サーバまたはCTグループを選択します。

2. [ファイル]メニューから[配下CTのIPアドレス出力]を選択します。
   または、サーバまたはCTグループを右クリックして[配下CTのIPアドレス出力]を選択します。

   →[配下CTのIPアドレス出力ファイル指定]画面が表示されます。



   - **[出力ファイル]**(必須):IPアドレスを出力するCSVファイルを、フルパスで指定します。

     半角で218文字まで入力できます。ただし、以下の記号はファイル名として使用できません。
     使用できない記号:「¥」「/」「:」「*」「?」「"」「<」「>」「|」

   - **[実行ログファイル]**(必須):実行結果を保存するファイルを、フルパスで指定します。

     半角で218文字まで入力できます。ただし、以下の記号はファイル名として使用できません。
     使用できない記号:「¥」「/」「:」「*」「?」「"」「<」「>」「|」

   - **[実行ログファイルが存在する場合]**:既存の実行ログファイルが存在する場合は必ず設定してください。
     [追記する]:既存の実行ログファイルに追記する場合に選択します。
     [上書きする]:既存の実行ログファイルに上書きする場合に選択します。

3. 上記の情報を設定し、[出力開始]ボタンをクリックします。
   出力されるCSVファイルの項目名と出力情報の説明については、“Systemwalker Desktop Keeper リファレンスマニュアル”の“グループ配下CTのIPアドレス出力ファイル”を参照してください。

3.6 クライアント(CT)を制御する

システム管理者は、不正行為が発覚したクライアント(CT)を制御する必要があります。
クライアント(CT)のサービス状態を変更したり、プロセスを終了したりします。

3.6.1 クライアント(CT)のサービスを制御する

クライアント(CT)に登録されているサービスの参照および制御について説明します。

サービス一覧を参照する

クライアント(CT)に登録されているサービスの一覧を参照する方法について説明します。

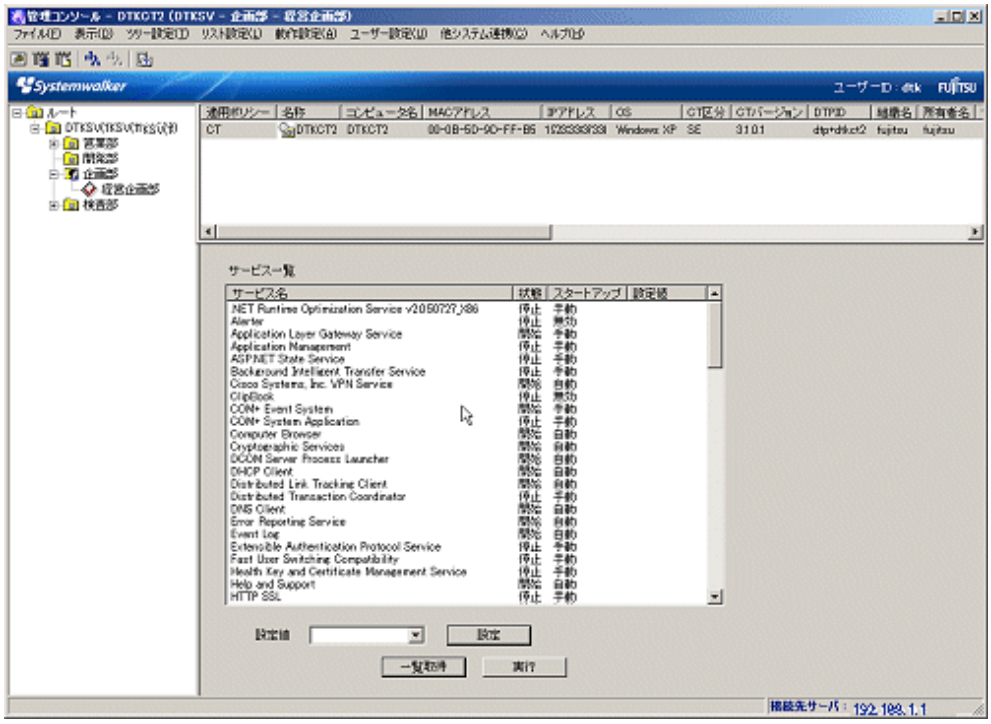
サービス一覧の参照手順は、以下のとおりです。

1. [管理コンソール]画面を起動します。
2. CTグループツリーからサービスの一覧を参照するクライアント(CT)が登録されているCTグループを選択します。
3. CTリストからサービスの一覧を参照するクライアント(CT)を選択し、[表示]メニューから[サービス一覧取得/制御]を選択します。

   →サービス一覧が表示されている画面になります。

4. [一覧取得]ボタンをクリックします。

   →選択したクライアント(CT)に登録されているサービスの一覧が表示されます。



項目名	説明
[サービス名]	クライアント(CT)に登録されているサービス名が表示されます。サービス名とは、Windowsのサービスを表示し、各項目のプロパティを表示したときの情報です。
[状態]	クライアント(CT)に登録されているサービスの状態が表示されます。
[スタートアップ]	スタートアップの種類として、[自動]、[手動]または[無効]が表示されます。
[設定値]	“サービスを制御する”でサービスの制御を行った場合に、選択した設定値が表示されます。設定値は、[開始]、[停止]、[自動]、[手動]または[無効]となります。

サービスを制御する

クライアント(CT)に登録されているサービスの状態およびスタートアップの種類を変更する方法について説明します。

注意

サービス状態やスタートアップ種別の変更について

クライアント(CT)において、手動で状態やスタートアップの種別を変更できないサービスは、本機能を使用しても状態やスタートアップの種別を変更することはできません。

サービスの制御手順は、以下のとおりです。

1. [管理コンソール]画面を起動します。
2. CTグループツリーからサービスを制御するクライアント(CT)が登録されているCTグループを選択します。
3. CTリストからサービスを制御するクライアント(CT)を選択し、[表示]メニューから[サービス一覧取得/制御]を選択します。

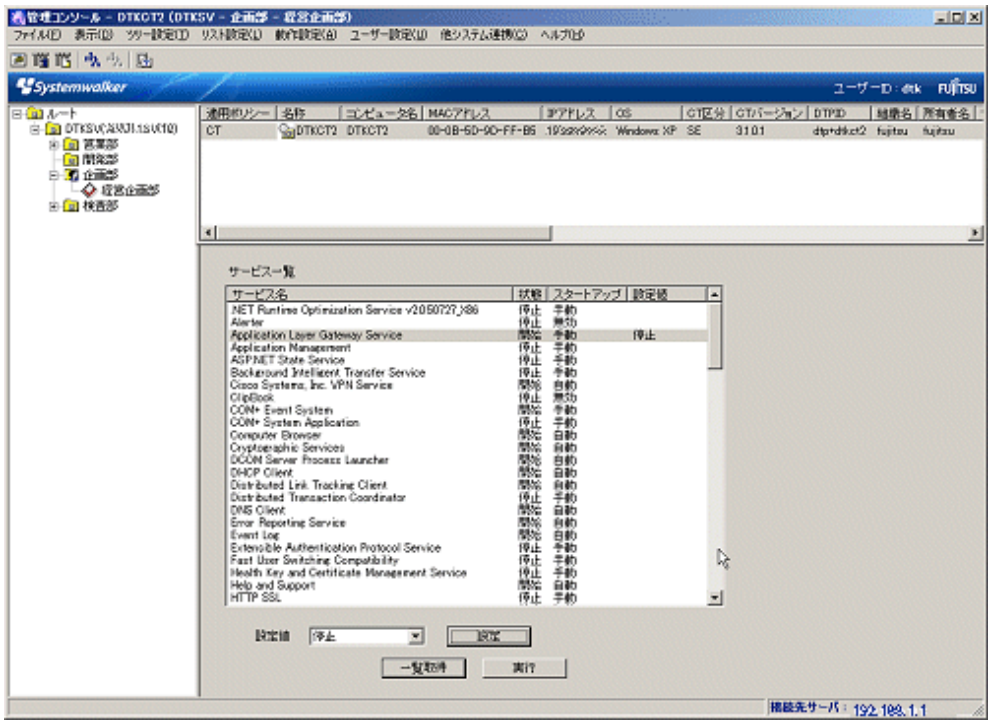
4. [一覧取得]ボタンをクリックします。

   →選択したクライアント(CT)に登録されているサービスが表示されます。

5. [サービス一覧]から状態を変更する行を選択します。

6. [設定値]をプルダウンメニューから選択して、[設定]ボタンをクリックします。

   →[設定値]のプルダウンメニューで選択した値が表示されます。



7. [実行]ボタンをクリックします。

   →設定された状態がクライアント(CT)に反映されます。

3.6.2 クライアント(CT)のプロセスを制御する

クライアント(CT)で動作しているプロセスの参照および制御について説明します。

プロセス一覧を参照する

クライアント(CT)で動作しているプロセスの一覧を参照する方法について説明します。

複数人がログオンしている場合、全ユーザーのプロセス一覧を参照します。

注意

Windows Vista® 64ビット版、Windows® 7 64ビット版、Windows Server® 2008 64ビット版、Windows Server® 2008 R2の場合は、64ビットで動作しているプロセスを参照できません

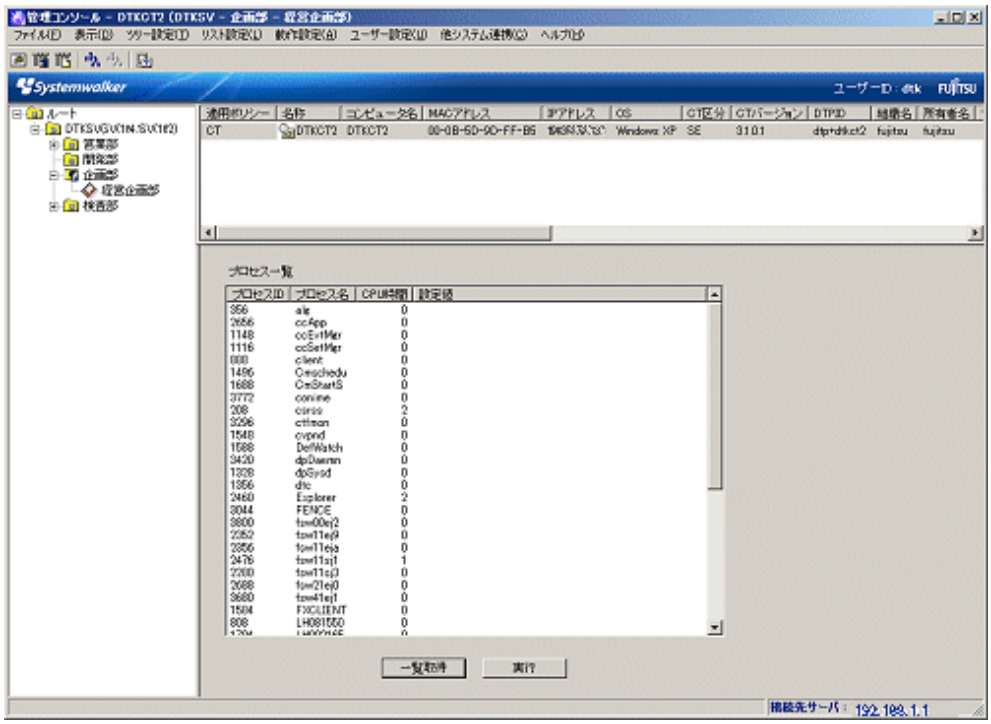
一部のプロセスは参照できません

Windowsシステム関係のプロセスは一部参照できないものがあります。
【例】

・System Idle process
・system

プロセス一覧の参照手順は、以下のとおりです。

1. [管理コンソール]画面を起動します。
2. CTグループツリーからプロセスの一覧を参照するクライアント(CT)が登録されているCTグループを選択します。
3. CTリストからプロセスを参照するクライアント(CT)を選択し、[表示]メニューから[プロセス一覧取得/制御]を選択します。
   →プロセス一覧が表示されている画面になります。
4. [一覧取得]ボタンをクリックします。
   →選択したクライアント(CT)で動作しているプロセスの一覧が表示されます。



項目名	説明
[プロセスID]	プロセスIDが表示されます。
[プロセス名]	プロセスの実行名が表示されます。
[CPU時間]	プロセスの稼働時間が表示されます。
[設定値]	“プロセスを制御する”でプロセスの制御を行った場合に、状態が表示されます。状態は、[終了]が表示されます。

プロセスを制御する

クライアント(CT)で動作しているプロセスを終了させる方法について説明します。

注意

【プロセスの参照】

- Windows Vista® 64ビット版、Windows® 7 64ビット版、Windows Server® 2008 64ビット版、Windows Server® 2008 R2の場合は、64ビットで動作しているプロセスを参照できません。
- Windowsシステム関係のプロセスは一部参照できないものがあります。
  【例】
  ・System Idle process
  ・system

【プロセスの終了】

- プロセスによっては、終了できない場合があります。
- プロセス終了時、選択したプロセス名と同一のプロセスが複数起動している場合は、すべて終了されます。
  また、複数人がログオンしている場合、全ユーザーについて、すべて終了されます。
- Windows Vista® 64ビット版、Windows® 7 64ビット版、Windows Server® 2008 64ビット版、Windows Server® 2008 R2の場合は、プロセスを終了できません。

プロセスの制御手順は、以下のとおりです。

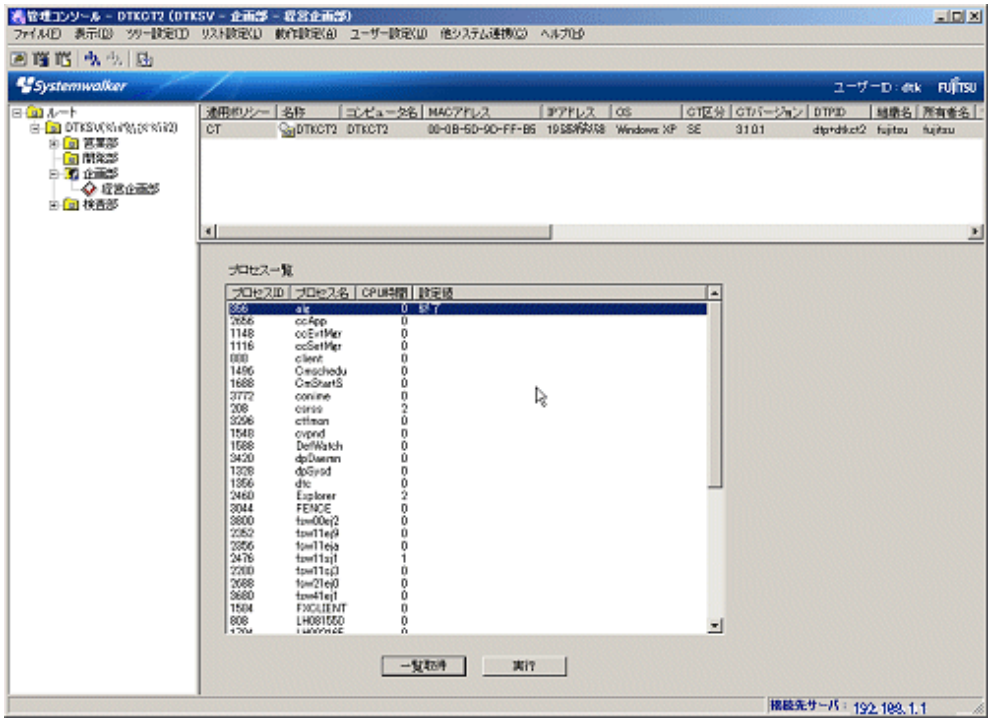
1. [管理コンソール]画面を起動します。
2. CTグループツリーからプロセスを制御するクライアント(CT)が登録されているCTグループを選択します。
3. CTリストからプロセスを制御するクライアント(CT)を選択し、[表示]メニューから[プロセス一覧取得/制御]を選択します。

   →プロセス一覧が表示されている画面になります。
4. [一覧取得]ボタンをクリックします。

   →選択したクライアント(CT)で動作しているプロセスの一覧が表示されます。
5. [プロセス一覧]から状態を[終了]する行を選択します。

6. 選択した行をダブルクリックします。

   →[設定値]に[終了]が表示されます。



7. [実行]ボタンをクリックします。

   →プロセスの終了がクライアント(CT)に反映されます。

第4章 クライアント(CT)操作の傾向をみる

本章では、状況画面およびログアナライザの使用方法について説明します。

採取された操作ログから、情報漏洩につながる可能性のある操作件数や、違反操作件数を集計して、クライアント(CT)での操作にどのような傾向があるかを把握します。

状況画面を使用した場合

情報漏洩につながる可能性が大きい以下の項目について、関連するログを集計し、該当するPCの数を表示します。

- ファイルを持出したPC
- 時間外に利用したPC
- 禁止されたUSBデバイスを利用したPC
- 禁止されたユーザーIDを利用したPC
- 禁止されたアプリケーションを利用したPC
- 禁止された印刷を行ったPC
- 禁止されたメール添付を行ったPC

集計結果から、該当PCが所属する部門の内訳を確認したり、該当PCの詳細情報(コンピュータ名、適用されているポリシー、グループ名など)を確認したりします。

こうして、注意が必要な部門やPCを発見した場合は、そのPCのログを検索することによって、行われた操作の実体を突き止めることができます。

ログアナライザを使用した場合

操作種別単位で件数を把握する

情報漏洩につながる可能性が大きい以下の操作に着目して操作件数を集計します。

- ファイル持出し操作ログ
- ファイル操作ログ
- 印刷操作ログ
- メール送信操作ログ

集計結果をグラフ表示したり、ユーザー別や端末別に操作のワーストランキングを表示したりできるため、該当操作をいつ、誰がどの端末で何回実施したかを、容易に把握できます。

集計は、2005年1月1日以降、現在までの範囲で日付を設定します。

詳細は、“4.2.2 情報漏洩のリスクを診断する”を参照してください。

調査目的ごとに件数を把握する

以下の調査目的に応じて、複数の操作種別を組み合わせて集計します。

- 違反操作状況を把握する
- ファイル持出し状況を把握する
- ファイル操作状況を把握する
- アプリケーション・メール状況を把握する
- 印刷操作状況を把握する
- Webアクセス状況を把握する
- 情報漏洩状況を把握する

詳細は、“4.2.3 目的別に集計する”を参照してください。

注意

Webコンソールの起動に関する注意

Webコンソールは同一PC上で複数起動しないでください。

PrintScreenキー禁止ログの取り扱いについて

本章で取り扱うPrintScreenキー禁止ログは、区分が「違反」のログのみが対象となります。

4.1 状況画面で傾向を見る

注意

状況画面参照中は、構成情報を変更しないでください

状況画面参照中は、CTや部門の、追加・削除・移動など、構成情報の変更を行わないでください。エラーが発生したり、正確ではない情報が表示される原因となります。

4.1.1 状況画面を表示する

1. 以下のいずれかの方法で、Webコンソールを起動します。

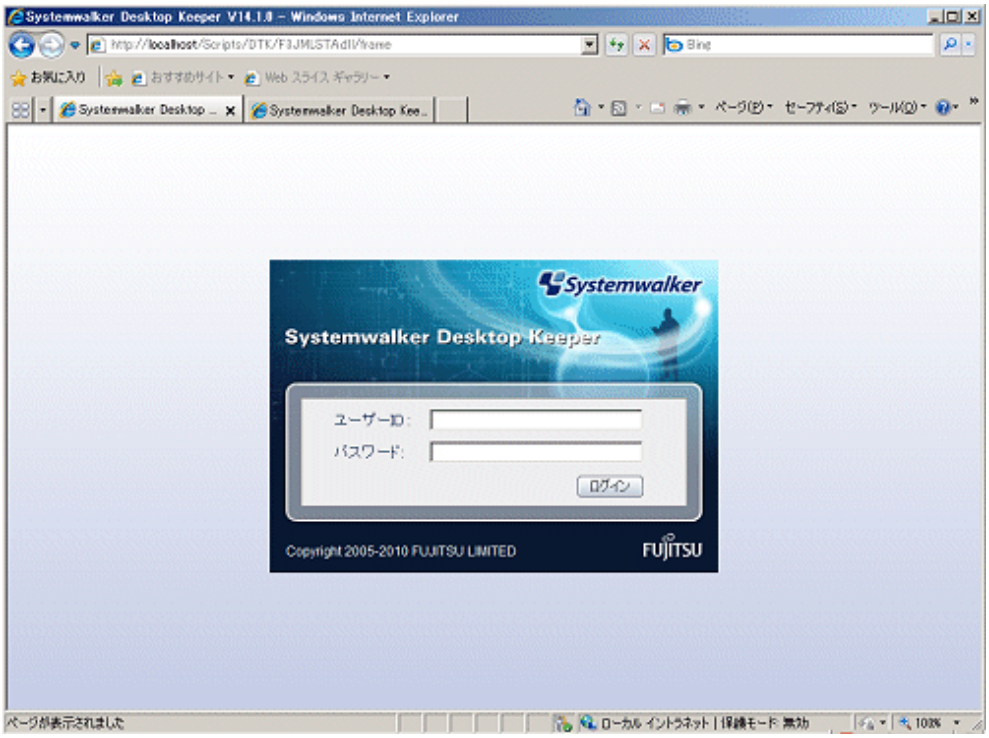
   2階層のシステム構成の場合:管理サーバに接続してください。

   - 管理サーバの[スタート]メニューから[プログラム]-[Systemwalker Desktop Keeper]-[サーバ]-[Desktop Keeper メインメニュー]を選択します。
   - ブラウザのアドレスに“http://管理サーバのホスト名またはIPアドレス/DTK/index.html”と指定します。
     IISのポート番号に変更があった場合は、以下のように指定します。
     http://IPアドレス:ポート番号/DTK/index.html

   3階層のシステム構成の場合:管理(統合管理)サーバに接続してください。管理サーバごとに集計結果を表示する場合は、各管理サーバに接続してください。

   - 管理(統合管理)サーバの[スタート]メニューから[プログラム]-[Systemwalker Desktop Keeper]-[サーバ]-[Desktop Keeper メインメニュー]を選択します。
   - ブラウザのアドレスに“http://管理(統合管理)サーバのホスト名またはIPアドレス/DTK/index.html”と指定します。
     IISのポート番号に変更があった場合は、以下のように指定します。
     http://IPアドレス:ポート番号/DTK/index.html

→[ログイン]画面が表示されます。



2. 以下の情報を入力し、[ログイン]ボタンをクリックします。

   システム管理者と部門管理者とで、ログイン方法に違いはありません。

   Systemwalker Desktop Patrolとシングルサインオン連携を行う場合は、ユーザーIDの大文字/小文字を区別して入力してください。

   ― **[ユーザーID]:** サーバ設定ツールの[管理者情報設定]画面で設定した[ユーザーID]です。

   ― **[パスワード]:** サーバ設定ツールの[管理者情報設定]画面で設定した[パスワード]です。
   パスワードは定期的に変更することを推奨します。変更方法は、“パスワードを変更する”を参照してください。

   →状況画面が表示されます。

画面の表示内容

グローバルヘッダ

― ユーザーID:ログインしているユーザーIDが表示されます。

― ログアウト:ログアウトします。

グローバルナビゲーション

ー 状況:状況画面が表示されます。

ー ログ管理:ログビューア画面が表示されます。

画面

ー [集計対象の部門]:どの部門のログを集計するかを選択します。

システム管理者がログインした場合、[ルート]と表示されます。
部門管理者がログインした場合、管理部門を複数もつ部門管理者は、プルダウンメニューから集計対象の部門(CTグループ)を選択します。プルダウンメニューには、部門管理者を設定した部門(CTグループ)だけが表示され、配下のサブグループは表示されません。

ー [集計完了日時]:集計が完了した日時が表示されます。

集計処理中の場合は、日時の後に「(集計中)」と表示されます。

集計完了日時以降に設定を変更している場合

集計完了日時以降に構成情報や環境設定の変更を行っている場合、表示されている集計情報には変更が反映されていません。変更を行った場合は、次の集計を待ってから情報を参照してください。

集計が完了してから状況画面を参照してください

(集計中)と表示されている間は、画面に表示されている集計結果が正しくない可能性がありますので、集計が終わってから参照してください。

管理(統合管理)サーバのイベントログを確認してください

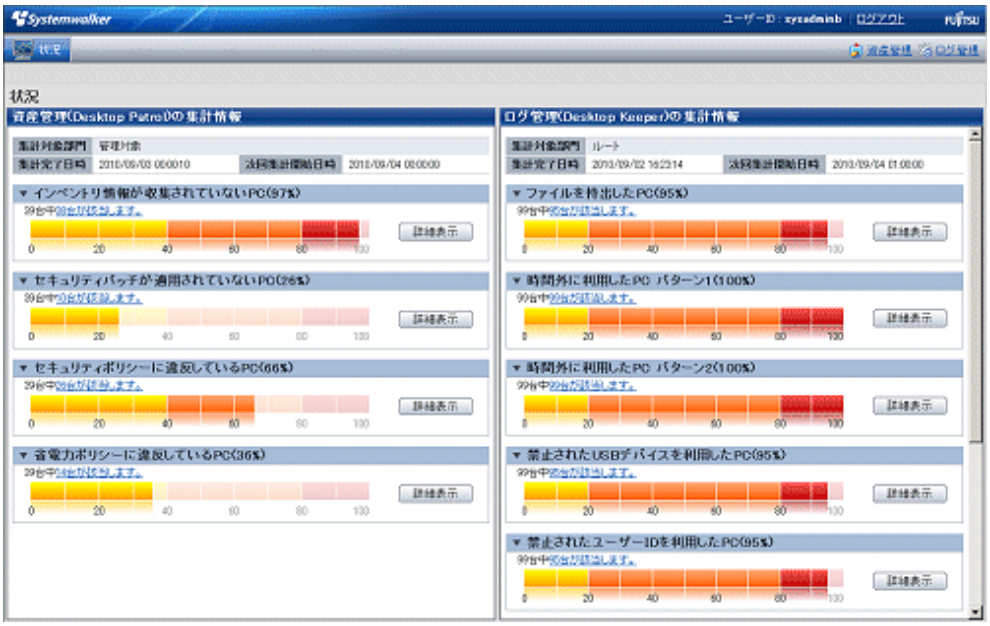
集計完了日時の日付に2日以上前が表示されている場合、集計処理がエラー終了している可能性があります。その場合は、管理(統合管理)サーバのイベントログを確認し、エラーが発生していないかを確認してください。

ー [次回集計開始日時]:次回の集計開始日時が表示されます。

ー 各項目に該当するPC数の集計結果が表示されます。

Systemwalker Desktop Patrolと連携している場合

Systemwalker Desktop Patrolと連携している場合、状況画面には、資産管理情報(Systemwalker Desktop Patrolの情報)とログ管理情報(Systemwalker Desktop Keeperの情報)が表示されます。



グローバルナビゲーションの[資産管理]をクリックすると、Systemwalker Desktop PatrolのWebコンソールが起動されます。詳細については、Systemwalker Desktop Patrolのマニュアルを参照してください。

4.1.2 ログの集計結果を確認する

状況画面では、以下の監査項目に該当するPCの数をグラフで表示します。

- ファイルを持出したPC

  ファイル持出し操作が行われたPCの数を表示します。ファイル持出しログに対して、集計期間、外部記憶媒体のドライブ種別の条件を付けて集計します。

- 時間外に利用したPC

  管理者が、PC利用時間外と定義した時間帯にログオン/ログオフされたPCの数を表示します。ログオン/ログオフログに対して、集計期間、曜日、時間帯の条件を付けて集計します。

- 禁止されたUSBデバイスを利用したPC

  使用を禁止されたUSBデバイスが装着されたPCの数を表示します。デバイス構成変更ログの区分が違反(※)のログに対して、集計期間の条件を付けて集計します。
  ※USBデバイス個体識別機能で登録/許可されたUSBデバイス以外をPCに装着した場合に、違反と記録されます。

- 禁止されたユーザーIDを利用したPC

  使用を禁止されたユーザーIDでログオン操作が行われたPCの数を表示します。
  ログオン禁止ログに対して、集計期間の条件を付けて集計します。

- 禁止されたアプリケーションを利用したPC

  使用を禁止されたアプリケーションが起動されたPCの数を表示します。
  アプリケーション起動禁止ログに対して、集計期間の条件を付けて集計します。

- 禁止された印刷を行ったPC

  使用を禁止されたアプリケーションからの印刷が行われたPCの数を表示します。
  印刷禁止ログに対して、集計期間の条件を付けて集計します。

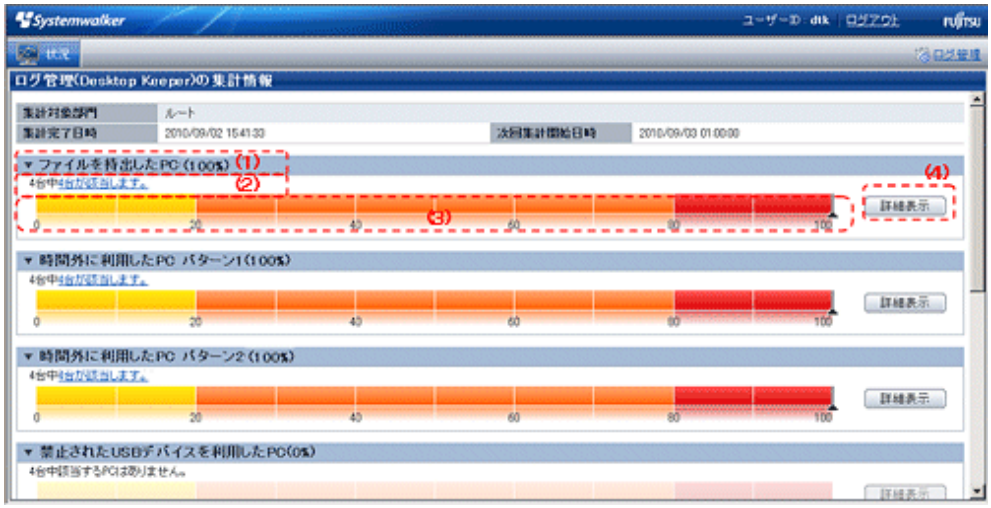
- 禁止されたメール添付を行ったPC

  添付を禁止されたファイルを添付したメール送信が行われたPCの数を表示します。
  メール添付禁止ログに対して、集計期間の条件を付けて集計します。

各項目の表示/非表示は、システム管理者が設定できます。
設定項目の詳細については、“2.8.1 状況画面を利用するための準備をする”を参照してください。

確認手順は、以下のとおりです。

1. 状況画面で、監査項目を決定します。



(1) **タイトル(割合):**監査項目のタイトルです。()内の割合は、管理対象となる全PCの何%が該当するかを示します。

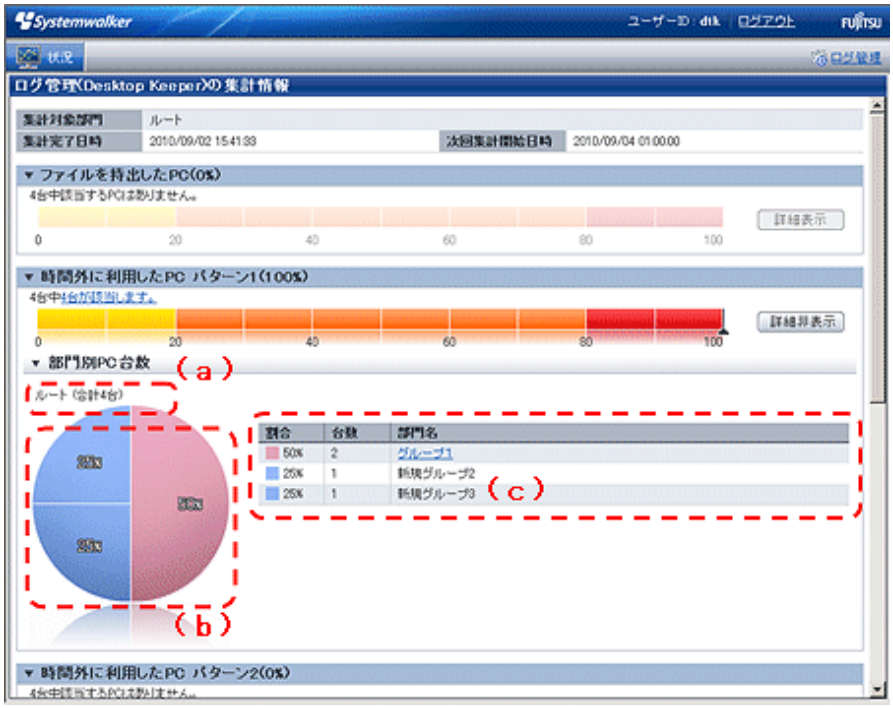
(2) **該当PC台数:**該当するPCの台数を表示します。台数をクリックすると、[CT操作ログ - 問題PC一覧]画面が表示されます。詳細は、“[CT操作ログ - 問題PC一覧]画面”を参照してください。

(3) **割合棒グラフ:**該当PC台数の割合を棒グラフで表示します。

(4) **[詳細表示]:**棒グラフの下に、部門別のPC台数が、表と円グラフで表示されます。詳細は、“部門別のPC台数”を参照してください。

2. その項目の[詳細表示]ボタンをクリックして、問題となるPCが所属する部門を把握します。
ログビューアでのログ検索時、どのCTグループを検索対象にすればよいか、分かります。

部門別のPC台数



部門別のPC台数を表示します。
初期状態は、ログインしているユーザーが管理している部門の最上位部門の情報が表示されます。

(a) 対象部門: 表示している部門の階層を表します。[集計対象の部門]で選択された部門がいちばん左に表示されます。

(b) 円グラフ: 部門ごとの該当PCの数と、全体に占める割合を表示します。

(c) ランキング表: 部門ごとに、該当PCの数と全体に占める割合を、順位をつけて表示します。
部門名をクリックすると、対象部門、円グラフ、ランキング表が、選択した部門配下の情報に変更されます。

【例】対象部門表示が「xx本部 > xx事業部」の場合
　ランキング表の[部門名]をクリックすると、対象部門表示は「xx本部 > xx事業部 > xx部」に変化し、円グラフおよびランキング表は、部配下のxx課の階層の単位で表示されます。

3. 該当PC台数をクリックします。
   →[問題PC一覧]が表示されます。

   [CT操作ログ - 問題PC一覧]画面

   (a) [検索場所]:システム管理者がログインしている場合は、[ルート]と表示されます。部門管理者がログインしている場合は、部門管理者が選択した部門(CTグループ)が表示されます。

   (b) [条件の説明]:監査項目のタイトル、該当PC数を集計したときの条件が表示されます。

   (c) [問題PC一覧]:[条件の説明]内容に合致するPCの一覧が表示されます。[グループ]や[名称]などの項目名は、ログビューアの[表示項目設定]画面で設定した情報が表示されます。設定方法の詳細は、“検索CT一覧の表示項目を設定する”を参照してください。
   ただし、項目名の[管理サーバ]は、ログビューアの[表示項目設定]画面で設定できません。必ず、右端に表示されます。
   [名称]をクリックすると、ログビューアが起動され、検索画面が表示されます。操作方法は、“5.2.1 [CT操作ログ]画面で参照する”を参照してください。

4. [問題PC一覧]の中から、ログ検索を行うクライアント(CT)の[名称]をクリックします。
   →ログビューアが起動され、検索結果が表示されます。問題となるPCで行われた操作を把握できます。

4.2 ログアナライザで傾向をみる

4.2.1 ログアナライザを起動する

Webコンソールの使用条件

- Webコンソールは、システム管理者が使用できます。
- Webコンソールとして使用できるWebブラウザは、以下のいずれかです。
  - Microsoft® Internet Explorer® 6.0 (ServicePack1)
  - Windows® Internet Explorer® 7

ー Windows® Internet Explorer® 8

ログアナライザを起動する

1. 以下のいずれかの方法で、メインメニューを起動します。

注意

ログアナライザ(Webコンソール)が接続するWebサーバについて

ログアナライザを起動する場合、接続できるWebサーバは1つです。3階層構成の場合、管理サーバに接続してもログビューア画面は表示されますが、ログアナライザ画面を表示することはできません。

2階層構成の場合:管理サーバに接続してください。

ー 管理サーバの[スタート]メニューから[プログラム]-[Systemwalker Desktop Keeper]-[サーバ]-[Desktop Keeper メインメニュー]を選択します。

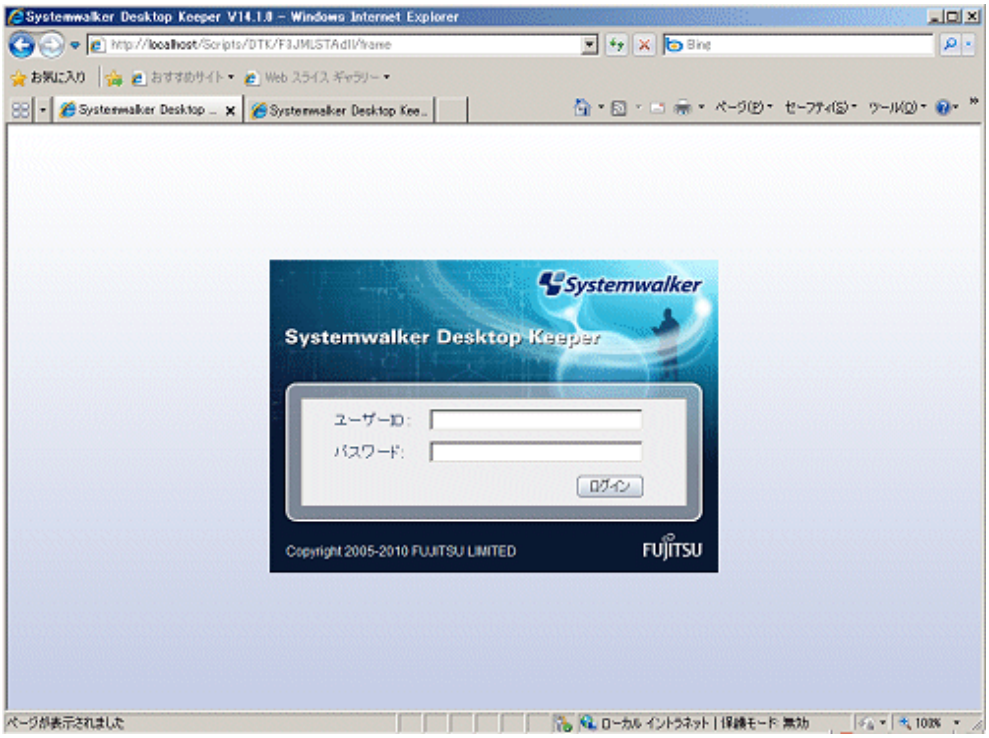
ー ブラウザのアドレスに“http://管理サーバのホスト名またはIPアドレス/DTK/index.html”と指定します。
IISのポート番号に変更があった場合は、以下のように指定します。
http://IPアドレス:ポート番号/DTK/index.html

3階層構成の場合:統合管理サーバに接続してください。

ー 統合管理サーバの[スタート]メニューから[プログラム]-[Systemwalker Desktop Keeper]-[サーバ]-[Desktop Keeper メインメニュー]を選択します。

ー ブラウザのアドレスに“http://統合管理サーバのホスト名またはIPアドレス/DTK/index.html”と指定します。
IISのポート番号に変更があった場合は、以下のように指定します。
http://IPアドレス:ポート番号/DTK/index.html

→[ログイン]画面が表示されます。



2. 以下の情報を入力し、[ログイン]ボタンをクリックします。

   システム管理者と部門管理者とで、ログイン方法に違いはありません。
   Systemwalker Desktop Patrolとシングルサインオン連携を行う場合は、ユーザーIDの大文字/小文字を区別して入力してください。

   ー [ユーザーID]:サーバ設定ツールの[管理者情報設定]画面で設定した[ユーザーID]です。

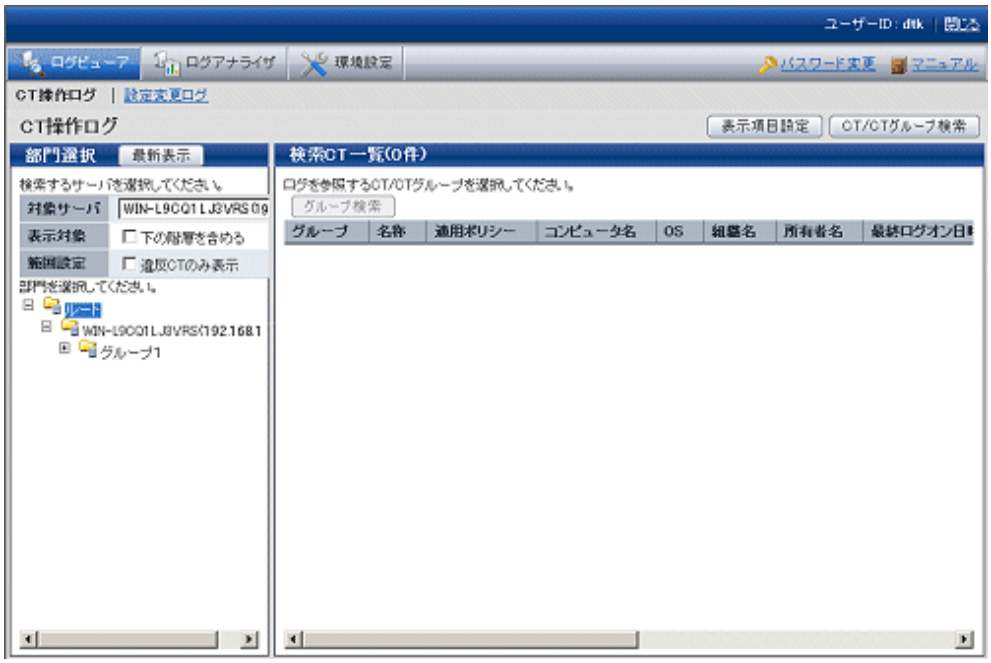
   ー [パスワード]:サーバ設定ツールの[管理者情報設定]画面で設定した[パスワード]です。

   パスワードは定期的に変更することを推奨します。変更方法は、“パスワードを変更する”を参照してください。

   →状況画面が表示されます。

3. グローバルナビゲーションの[ログ管理]をクリックします。

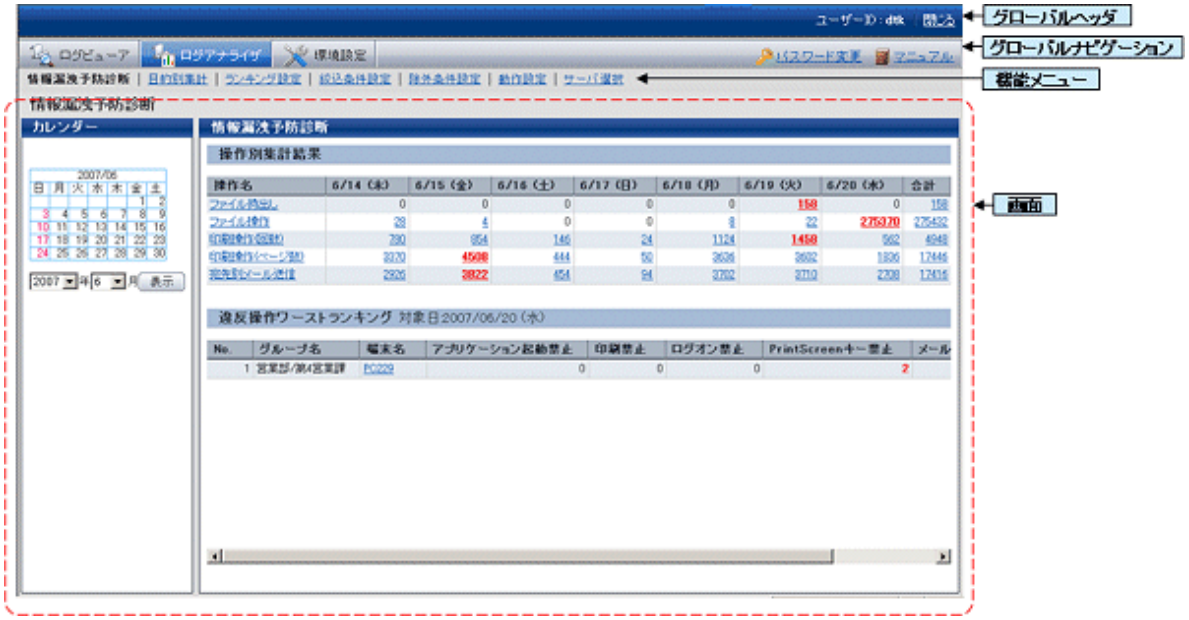
   →ログビューアが起動され、[CT操作ログ]画面が表示されます。



4. グローバルナビゲーションの[ログアナライザ]をクリックします。

   →[情報漏洩予防診断]画面が表示されます。

なお、ログアナライザサーバが複数あるシステムで、ログイン後に初めてログアナライザを選択した場合は、サーバ選択画面が表示されます。サーバ選択画面については“2.8.2.2.5 ログアナライザサーバを選択する”を参照してください。



画面の表示内容

グローバルヘッダ

- ユーザーID:ログインしているユーザーIDが表示されます。
- 閉じる:ログビューア画面を閉じます。

グローバルナビゲーション

- ログビューア:ログビューア画面が表示されます。
- ログアナライザ:ログアナライザ画面が表示されます。
- 環境設定:オプション画面(状況画面に表示される集計結果の元になる集計条件を設定する画面)が表示されます。
- パスワード変更:Web画面起動時のパスワードを変更します。変更方法は、“パスワードを変更する”を参照してください。
- マニュアル:マニュアルが表示されます。

機能メニュー

- 情報漏洩予防診断:情報漏洩予防診断画面を表示します。
- 目的別集計:目的別集計画面を表示します。日時やキーワードを指定して目的別に集計します。
- ランキング設定:グループ別、端末別、ユーザー別、端末＋ユーザー別の各ランキングの、“表示/非表示”と表示数を設定します。
- 絞込条件設定:ログを集計するときのキーワード、ドメイン、URL、またはアプリケーションを、絞込条件として設定します。
- 除外条件設定:ログを集計するとき、集計対象外とする端末を設定します。
- 動作設定:情報漏洩予防診断の違反操作ワーストランキング表示の設定、レポート出力における週報開始曜日や、エコ監査の設定などを行います。
- サーバ選択:サーバ選択画面を表示します。現在選択しているログアナライザサーバを変更する場合にクリックします。
  以下の条件をすべて満たす場合、自動的に本画面が表示されます。
  ・ログアナライザサーバが複数あるシステム構成のとき
  ・メインメニューからログインして初めてログアナライザを使用するとき

注意

画面表示までに時間がかかる場合があります

サーバの停止やネットワークの不通など、接続ができないログアナライザサーバがある場合、環境やサーバ台数によっては、画面表示までに数分かかるときがあります。

画面

- カレンダー:集計結果を表示する日を選択します。
- 操作別集計結果:ファイル持出し操作、ファイル操作、印刷操作(回数およびページ数)、メール送信操作の直近7日間の操作件数および合計数を表示します。
- 違反操作ワーストランキング:以下のログに関して、ログインした前日またはカレンダーで選択した日の件数および、各操作の合計値を表示します。

  ・アプリケーション起動禁止
  ・印刷禁止
  ・ログオン禁止
  ・PrintScreenキー禁止
  ・メール添付禁止

4.2.2 情報漏洩のリスクを診断する

情報漏洩のリスク診断は、[情報漏洩予防診断]画面で行います。

注意

情報漏洩予防診断画面に表示されるログ件数と、目的別集計結果のログ件数は、一致しない場合があります

情報漏洩予防診断画面に表示されるログ件数は、管理サーバからログアナライザサーバへログの移入処理を実施した時点での絞込条件、除外条件で集計した結果です。
このため、集計後に変更された絞込条件/除外条件や、集計後に移入されたログ(※)は反映されていません。

一方、目的別集計では、リアルタイムに集計します。最新の絞込条件/除外条件で、移入済のログを集計した結果です。

したがって、情報漏洩予防診断画面に表示されるログ件数と、目的別集計結果のログ件数は、一致しない場合があります。

集計後に変更された絞込条件/除外条件で、集計後に移入されたログを含めた集計結果を表示したい場合(最新のデータと条件で集計しなおしたい場合)は、再集計する必要があります。
再集計については、“Systemwalker Desktop Keeper リファレンスマニュアル”の“DTTOOLEX.EXE(ログアナライザサーバへのデータ移入・削除)”を参照してください。

※)集計後にログが移入される場合とは

クライアント(CT)がネットワークに接続されていなかったなどの理由で、管理サーバに操作ログが遅れて転送される場合があります。
そのためログアナライザサーバに移入されるログが遅れて反映される場合があります。

4.2.2.1　操作別集計結果を表示する

[情報漏洩予防診断]画面の[操作別集計結果]では、管理サーバからログアナライザサーバにログが転送された時点で集計した結果を利用して、各端末で採取された操作ログの件数を、過去1週間にさかのぼって表示します。
集計は、“2.8.2.2 集計条件/レポート出力条件を設定する”で設定した、絞込条件(キーワード)および除外条件(ファイル持出し、ファイル操作、印刷操作、宛先別メール送信)をもとに実施されます。
集計対象は、以下の操作ログです。

- ファイル持出し操作ログ
  本ログから、持出しユーティリティを使用して、可搬媒体へファイルを持ち出した操作の件数を集計します。
- ファイル操作ログ
  本ログから、リムーバブルと認識される媒体やCD/DVDに、ファイルの作成、更新、移動、複写を行った操作の件数を集計します。
  ファイル操作には、削除、変名、参照もありますが、これらの操作は情報漏洩のリスクが少ないため、集計の対象としません。
- 印刷操作ログ
  印刷操作の回数と、印刷した総ページ数を集計します。
  印刷操作回数は、印刷したファイルが複数ページあったとしても1件としてカウントされます。
  印刷ページ数は、印刷したファイルが複数ページある場合、ページ数がカウントされます(ファイルの総ページ数がカウントされます)。
- メール送信操作ログ
  社外へのメール発信操作の件数を集計します(社内のメールアドレスのドメインを絞込条件に登録しておく必要があります)。
  なお、同報送信したメールは別々に複数の件数としてカウントされます。

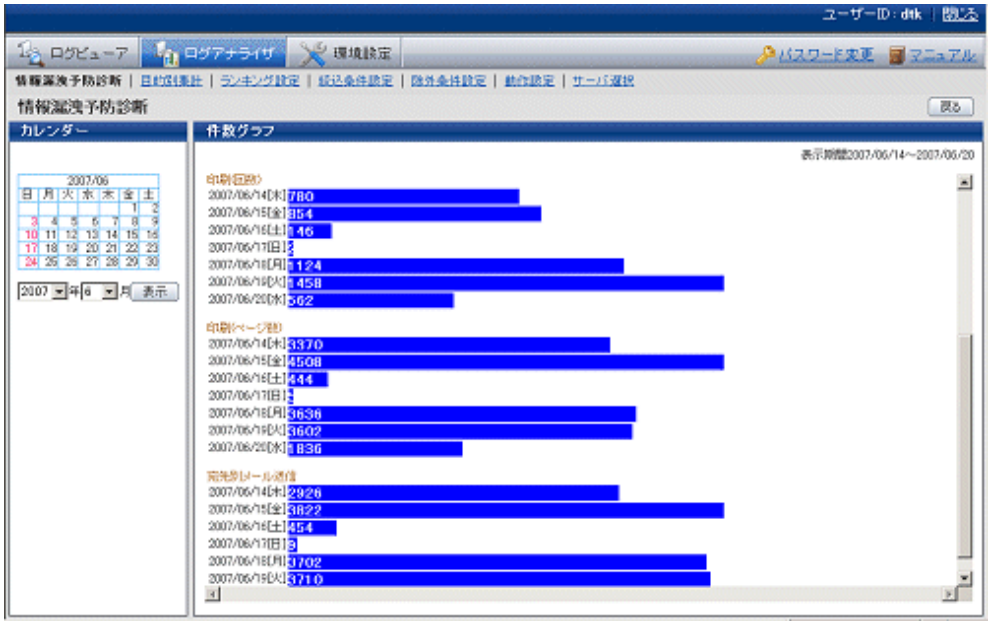
件数が多い場合、情報漏洩の可能性があると考えられます。各操作において、件数が最も多い日付のセルは、赤色で表示されます。
また、操作ごとに件数をグラフ表示したり、件数の内訳をランキング表示したりすることができます。
“2.8.2.2 集計条件/レポート出力条件を設定する”の設定を行っていないと、件数は業務や規模に比例して非常に多くなります。その場合、表示のための処理時間やデータ量が増加するだけでなく、危険な操作が埋もれてしまい見つけ出しにくくなります。必ず設定を行うようにしてください。

件数をグラフ表示する

操作別集計結果に表示される各操作名をクリックすると、表示されている1週間の件数の推移が、グラフ表示されます。
グラフの縮尺は各操作毎に異なります(各操作毎に週間最大件数をグラフの長さ100%の状態として表示されます)。

手順は以下のとおりです。

1. 操作別集計結果の[操作名]から、グラフ表示する操作をクリックします。
   →グラフが表示されます。



件数の内訳をランキング表示する

操作別集計結果の日付欄や合計欄の件数をクリックすると、件数の内訳がランキング表示されます。

ランキングは、以下のように表示されます。

- グループ別ランキング

  件数をグループ単位で集計し多い順に表示されます。
  グループ名は、最大で1024バイトまで表示されます。
  管理コンソールのCTグループツリーで、ルート直下に存在するクライアント(CT)の[グループ名]は、“ルート”と表示されます。
  階層構造で管理されているグループは、“階層1/階層2/階層3”と表示されます。

・ 端末別ランキング(注)

件数を端末名単位で集計し多い順に表示されます。端末が所属するグループ名も表示されます。

・ ユーザー別ランキング

件数をユーザー名単位で集計し多い順に表示されます。端末が異なる場合でもユーザー名が同じ場合はまとめて集計されます。

・ 端末＋ユーザー別ランキング(注)

件数を端末名とユーザー名の組み合わせ単位で集計し多い順に表示されます。端末が所属するグループ名も表示されます。

件数に同数がある場合でも、ランキング設定で設定した順位まで表示されます(同順位の表示順はランダムです)。ただし最大で99行分までしか表示されません。

注) ランキング項目の“端末名”と“端末+ユーザー名”は、以下の形式で表示されます。

・ 管理コンソールのCTリストに表示される[名称]と[コンピュータ名]が同じ場合

[名称]と[コンピュータ名]が同じになる条件は、以下のどちらかです。

－ CTインストール後、[名称]を更新していないため、初期値として[コンピュータ名]が表示されている

－ 管理コンソールで、[名称]を[コンピュータ名]と同名に更新した

このとき、端末別ランキングには、“コンピュータ名”の形式で表示されます。
【例】PC001

端末+ユーザー別ランキングには、“コンピュータ名+ユーザー名[グループ名]”の形式で表示されます。
【例】PC001+Administrator

・ 管理コンソールのCTリストに表示される[名称]と[コンピュータ名]が異なる場合

[名称]と[コンピュータ名]が異なる条件は、以下です。

－ 管理コンソールで、[名称]を[コンピュータ名]とは別名に更新した

このとき、端末別ランキングには、“コンピュータ名(名称)”の形式で表示されます。
【例】BLONO(富士通太郎)

端末+ユーザー別ランキングには、“コンピュータ名(名称)+ユーザー名”の形式で表示されます。
【例】BLONO(富士通太郎)+Administrator

日付欄の件数をクリックした場合

→選択した日の各操作のランキングが表示されます。

合計欄の件数を選択した場合

→対象となる集計期間の、該当操作のランキングが表示されます。

ランキング表示結果で、グループ名、端末名、端末＋ユーザー名のリンクをクリックすると、画面はログビューアへ遷移します(「Desktop Log Analyzer互換で動作させる」にチェックがされている場合は目的別集計画面に遷移します)。ログビューアでは、集計時の条件(集計期間、ユーザー名、端末名など)で実施されたログ検索結果が、[ログ一覧]に表示されています。なお、[宛先別メール送信」の件数をログビューア側で見た場合、ログアナライザ側では同報メールでも宛先別にカウントするのに対し、ログビューア側では同報メールを1件とカウントするため、ログの件数として一致しない場合があります。[動作設定]において[Desktop Log Anlayzer互換で動作させる]がチェックされている場合は、端末名、ユーザー名、端末+ユーザー名のリンクをクリックすると、画面は目的別集計へ遷移します。
ただし、操作別集計結果が10万件を超える場合は、ログビューアへの画面遷移はできません(ログの一覧を見ることはできません)。

なお、グループ別ランキングで[ルート]、[Local]、または[削除したCT]の名前のグループもログビューアへ画面遷移できません。

4.2.2.2　違反操作ワーストランキングを表示する

違反操作ワーストランキングでは、違反操作の合計値によるランキングを表示します。
以下の違反操作ログをもとに違反操作回数を1日単位で集計し、各操作の合計値でランキングを表示します。

- アプリケーション起動禁止ログ
- 印刷禁止ログ
- ログオン禁止ログ
- PrintScreenキー禁止ログ
- メール添付禁止ログ

ランキング表示結果で、端末名のリンクをクリックすると、画面はログビューアへ遷移します。ログビューアでは、集計時の条件(集計期間、端末名など)で実施されたログ検索結果が、[ログ一覧]に表示されています。

4.2.2.3　過去の日付けを特定して集計結果を表示する

カレンダーで日にちを指定して、指定した日付を基準に過去1週間の各操作の集計件数を表示します。

実行前に、集計対象期間のログが、ログアナライザサーバに存在することを確認してください。移入できるログ量は、過去1年間分です。

2005年1月1日以降、現在までの範囲で日付を特定し、集計結果を参照することができます。

カレンダーで該当する日をクリックします。
または、カレンダーの下のコンボボックスで、年および月を選択し、[表示]ボタンをクリックします。

4.2.3　目的別に集計する

目的に応じた集計内容を選択し、集計単位、集計期間、キーワードなどの条件を設定してログの集計を行い、結果を表示することができます。

ポイント

集計結果件数が多い場合、結果表示に時間がかかる場合があります

対象データの件数が多い場合、[集計結果]および[詳細結果]の表示処理に長時間かかり、ブラウザがタイムアウトする場合があります(処理時間は、集計条件や管理サーバの性能などにも大きく左右されます)。

【処理時間の目安】

- 印刷操作状況を把握する-印刷操作(回数)の場合、420万件で、約27秒
- ファイル操作状況を把握する-ファイル操作の場合、340万件で、約24秒
- Webアクセス状況を把握する-URL付きウィンドウタイトル取得の場合、2230万件で、約81秒

Microsoft® Internet Explorer® 6.0の場合、通常のタイムアウト時間は60分ですが、ネットワーク環境によっては他のネットワーク機器によってタイムアウトが発生することがあります。
例えばプロキシを通して管理サーバにアクセスしている場合は、プロキシによってもタイムアウトが発生します。この場合、以下の手順でプロキシを使用せずに管理サーバにアクセスすると、タイムアウトを回避できるときがあります。

[ツール]-[インターネットプション]-[接続]-[LANの設定]-[詳細設定]の、[次で始まるアドレスにはプロキシを使用しない]に、管理サーバのアドレスを設定してください。

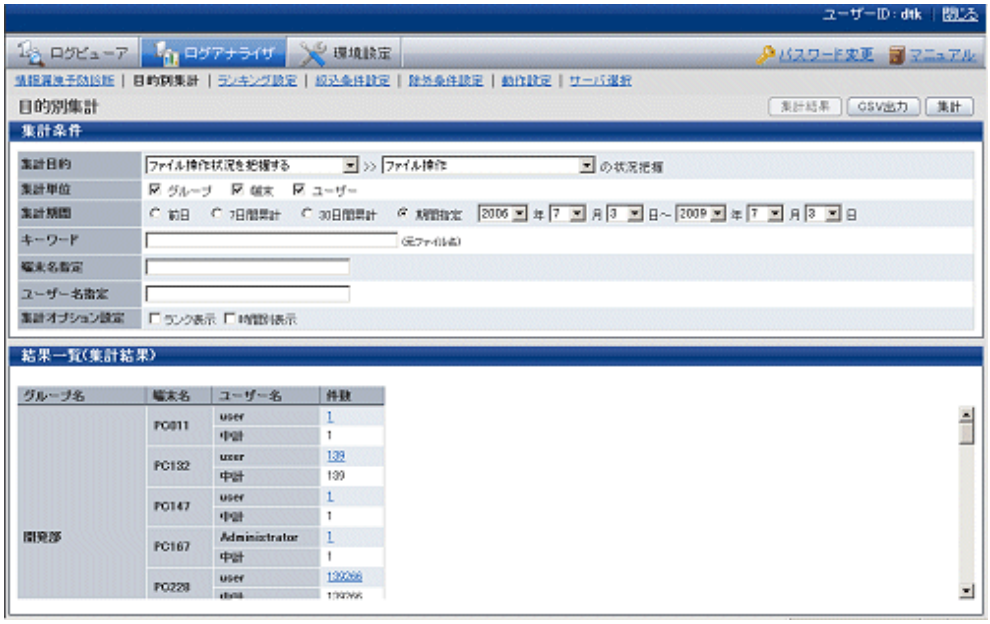
表示内容が多い場合、正しく結果表示されるまで時間がかかり、それまで表示が崩れて見える場合があります

大量のログの一覧や、24時間の集計結果など、一画面に表示される情報量が多い場合は、結果が表示されるまで時間がかかる場合があります。結果が正しく表示されるまでの間は、空白状態、表の一部だけ表示、または表の一部が点滅するなど、画面が崩れたように見える場合があります。また、表示される情報量が多い場合は、ボタンの反応やブラウザのリサイズの反応が遅くなる場合があります。

集計する

手順は以下のとおりです。

1. データ移入中ではないことを確認後、機能メニューで[目的別集計]を選択します。
   →[目的別集計]画面が表示されます。



集計条件

ログの集計目的の一覧が表示されます。
各目的を選択すると詳細なメニュー(目的)が表示されます。

集計単位、集計期間、キーワードなどを設定します。

結果一覧

集計結果が表示されます。

2. [集計目的]で、集計目的とそのサブメニューを選択します。

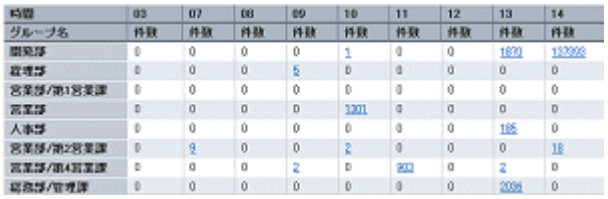
集計目的	集計目的のサブメニュー	内容
違反操作状況を把握する	アプリケーション起動禁止の状況把握	アプリケーション起動禁止に該当する件数を集計します。
	印刷禁止の状況把握	印刷禁止に該当する件数を集計します。
	ログオン禁止の状況把握	ログオン禁止に該当する件数を集計します。
	PrintScreenキー禁止の状況把握	PrintScreenキー禁止に該当する件数を集計します。
	メール添付禁止の状況把握	メール添付禁止に該当する件数を集計します。
ファイル持出し状況を把握する	ファイル持出しの状況把握	ファイル持出し件数を集計します。
	ファイル持出し(ドライブ別)の状況把握	ファイル持出し件数を、持ち出し先ドライブ種別単位で集計します。
ファイル操作状況を把握する	ファイル操作の状況把握	ファイル操作件数を集計します。
	ファイル操作(リモート)の状況把握	ネットワーク上のファイルの操作件数を集計します。
	ファイル操作(リムーバブル)の状況把握	リムーバブルメディア上のファイル操作件数を集計します。
	DTRM(ファイル登録)の状況把握	DTRMのログから、新規に共有フォルダにファイルを登録した件数を集計します。
	DTRM(アクセス権の追加/変更/削除)の状況把握	DTRMのログから、アクセス許可を追加/変更/削除した件数を集計します。
	DTRM(ファイル削除)の状況把握	DTRMのログから、共有フォルダにあるオーナ権限のファイルを削除した件数を集計します。
	DTRM(暗号化ファイル閲覧)の状況把握	DTRMのログから、共有フォルダの暗号化ファイルを閲覧した件数を集計します。
	DTRM(暗号化ファイル復号)の状況把握	DTRMのログから、共有フォルダで暗号化ファイルを復号した件数を集計します。
	DTRM(オフラインに複写)の状況把握	DTRMのログから、共有フォルダからオフラインフォルダへコピーした件数を集計します。
	DTRM(オフライン暗号化ファイル復号)の状況把握	DTRMのログから、オフラインフォルダで暗号化ファイルを復号した件数を集計します。
	DTRM(暗号化ファイル更新)の状況把握	DTRMのログから、共有フォルダの暗号化ファイルを更新した件数を集計します。
アプリケーション・メール状況を把握する	アプリケーション起動の状況把握	アプリケーション起動件数を集計します。
	宛先別メール送信の状況把握	メール送信件数を集計します。
印刷操作状況を把握する	印刷操作(回数)の状況把握	印刷操作件数を集計します。
	印刷操作(ページ数)の状況把握	印刷総ページ数を集計します。
	DTRM(暗号化ファイル印刷)の状況把握	DTRMのログから、共有フォルダの暗号化ファイルを印刷した件数を集計します。
Webアクセス状況を把握する	URL付きウィンドウタイトル取得の状況把握	インターネットアクセス件数を集計します。

集計目的	集計目的のサブメニュー	内容
	URL付きウィンドウタイトル取得(サイト別)の状況把握	インターネットアクセス件数を、サイト単位で集計します。
情報漏洩状況を把握する	ファイル持出しの状況把握	絞込条件／除外条件によりログをフィルタリングして、外部媒体へのファイル持出し件数を集計します。
	ファイル操作の状況把握	絞込条件／除外条件によりログをフィルタリングして、外部媒体のファイル操作件数を集計します。
	印刷操作(回数)の状況把握	絞込条件／除外条件によりログをフィルタリングして、印刷操作件数を集計します。
	印刷操作(ページ数)の状況把握	絞込条件／除外条件によりログをフィルタリングして、印刷総ページ数を集計します。
	宛先別メール送信の状況把握	絞込条件／除外条件によりログをフィルタリングして、メール送信件数を集計します。

3. 以下の項目を設定します。

設定項目および設定値は以下のとおりです。

項目名	説明
[集計単位]	集計する単位を指定します。複数選択できます。 ・ [グループ]:CTグループごとに集計します ・ [端末]:コンピュータ名(※)ごとに集計します。 ※) 管理コンソールのCTリストに表示されます ・ [ユーザー]:ユーザー名ごとに集計します。 複数選択した場合、単位の大小関係は[グループ]＞[端末]＞[ユーザー]の順です。大きい単位の順に左から表示されます。
[集計期間]	集計対象となるログの採取日を指定します。 ・ [前日]:目的別集計を実施する前日のログを集計します。 ・ [7日間累計]:過去1週間(7日前から前日までの7日間)のログを集計します。 ・ [30日間累計]:過去30日間(30日前から前日までの30日間) のログを集計します。 ・ [期間指定]:任意の期間のログを集計します。開始日および終了日を指定してください。指定可能期間は2004年1月1日から2024年12月31日までです。 [30日間累計]や[期間指定]のように、集計期間が長く対象データ量が多い場合は、処理時間がかかるため、タイムアウトが発生して結果が正しく表示されないときがあります。期間を1週間ごとに区切って集計するなど、集計期間には、適切な値を設定してください。
[キーワード]	集計時の検索キーワードを指定します。最大入力文字数は50文字です。 指定したキーワードに部分一致したログを集計します。

項目名	説明
	集計目的によって、有効なキーワードが異なります。詳細は“付録A 集計目的一覧”を参照してください。
[端末名指定]	指定したコンピュータ名を含むログ(部分一致)を集計します。 最大入力文字数は60文字です。
[ユーザー名指定]	指定したユーザー名を含むログ(部分一致)を集計します。 最大入力文字数は40文字です。
[集計オプション設定]	集計結果の表示形式を指定します。 ・[ランク表示]: 集計結果の表示において、件数欄の右に順位欄を設け、件数の多い順に表示します([時間別表示]を指定した場合は、[総計]の多い順に表示されます)。 ランク表示を指定した場合は、集計結果に“中計”は表示されません。 ・[時間別表示]: 時間(1時間)ごとの集計結果を表示します。 集計対象範囲に1件も該当するデータがない時間は表示されません。  上記は、15時、16時、17時、18時、20時、23時に該当するデータがあったことを示します。

グループ名	件数	順位
開発部	139409	1
営業部/第6営業課	36802	2
総務部/管理課	2036	3
営業部	1313	4
営業部/第4営業課	917	5
人事部	185	6
総務部/企画課	61	7
営業部/第2営業課	36	8
ルート	23	9

時間	03	07	08	09	10	11	12	13	14
グループ名	件数	件数	件数	件数	件数	件数	件数	件数	件数
開発部	0	0	0	0	1	0	0	1801	132908
管理部	0	0	0	5	0	0	0	0	0
営業部/第1営業課	0	0	0	0	0	0	0	0	0
営業部	0	0	0	0	1301	0	0	0	0
人事部	0	0	0	0	0	0	0	185	0
営業部/第2営業課	0	9	0	0	2	0	0	0	18
営業部/第4営業課	0	0	0	2	0	903	0	2	0
総務部/管理課	0	0	0	0	0	0	0	2036	0

4. [集計]ボタンをクリックします。

— 目的別集計は、複数ユーザーによる同時使用はできません。

他のユーザーによってすでに集計結果が出ている場合、または集計処理実施中の場合は、以下のメッセージが表示されます。

他の利用者が集計機能を使用している可能性があります。処理を継続しますか？

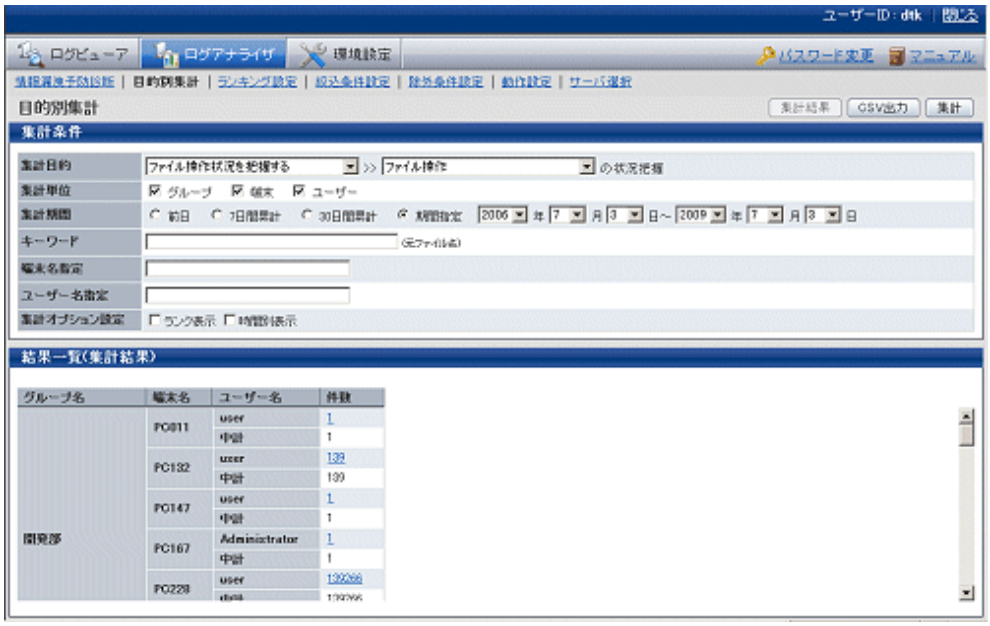
[OK]ボタンをクリックした場合、他のユーザーによってすでに集計結果が出ているときは、他のユーザーの集計結果が破棄され、集計が実施されます。

他のユーザーが集計処理実施中のときは、エラーメッセージが表示され、しばらく時間をあけて他のユーザーの使用が終わってからでないと、実施できません。

— 集計の処理中、およびそのキャンセル処理中に、以下の操作を実施しないでください。実施した場合、未完了の処理が残ったままとなり、しばらく処理が行えなくなる場合があります。

・グローバルナビゲーションおよび機能メニューに表示されている各画面への移動
・ログアウト操作
・ブラウザ機能による画面操作([閉じる]、[戻る]、[更新]など)

集計結果



- 表の左側の欄には、集計単位([グループ][端末][ユーザー]のうち選択したもの)の名前が表示されます。
  管理コンソールのCTグループツリーでのルートグループは、[グループ名]に“ルート”と表示されます。
  また、階層構造で管理されているグループは、“階層1/階層2/階層3”と表示されます。
- ランク表示を選択した場合は、右側に順位欄が表示され件数の多い順で順位が表示されます。
- 最下行には総計が表示されます。
- 集計単位を複数選択した場合は、中計行が表示されます。ただしランク表示を行った場合は中計行は表示されません。
- 件数欄には、集計単位毎の集計値が表示されます。集計値をクリックすると、内訳の詳細情報が表示されます。
  [件数]の値が大きい場合に詳細結果の表示を行うと、「[ERR-DTLAC199] 処理中にエラーが発生しました。」のエラーが発生する場合があります。その場合は、以下の対策を実施し、[件数]の値を小さくしてから、詳細結果を表示してください。

  ・[集計期間]を短くする

  ・[集計単位]を増やす([グループ]、[端末]、[ユーザー]の各項目はAND条件になるので、条件を絞り込めます)

  ・[キーワード]で絞り込む

  ・時間別で集計する

詳細結果

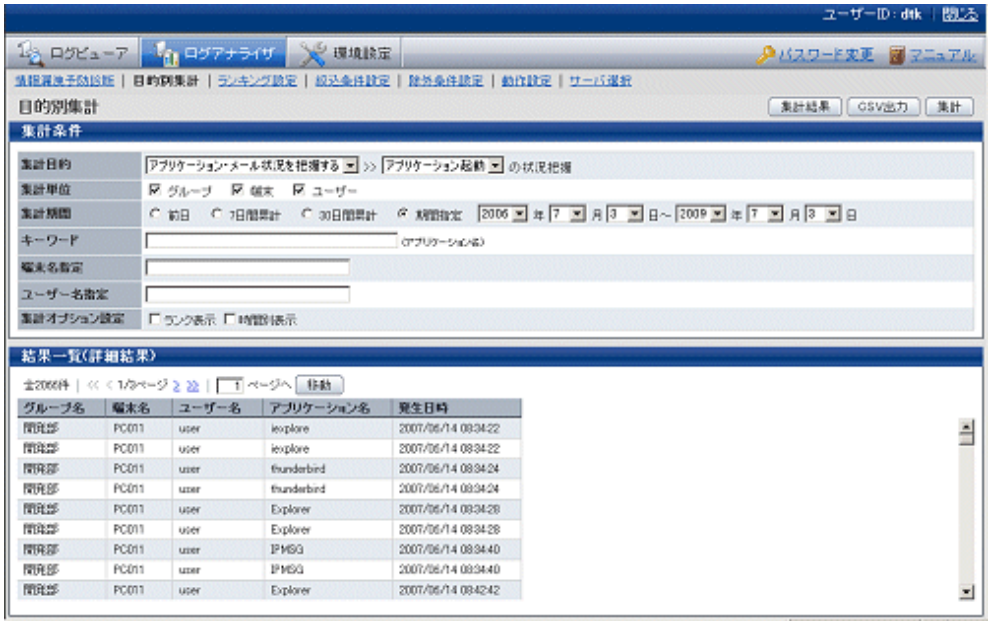
[件数]のリンクをクリックすると、集計値の内訳が表示されます。
ログにない詳細項目、または空白のみの詳細項目は「－」で表示されます。

詳細表示を行う際、件数が多い場合1000件毎に結果を表示します。
1ページあたりの表示データサイズは平均で0.5MBです。大量の詳細結果表示を行う場合、例えば10万件の詳細表示を行うには、約50MBのディスク容量が必要となります。ディスク容量が不足している場合は、集計値ができるだけ小さくなるように、集計単位を細かく指定する、集計期間を短くするなどして詳細表示してください。

詳細の処理中、およびそのキャンセル処理中に、以下の操作を実施しないでください。実施した場合、未完了の処理が残ったままとなり、しばらく処理が行えなくなる場合があります。

- グローバルナビゲーションおよび機能メニューに表示されている各画面への移動
- ログアウト操作

- ブラウザ機能による画面操作([閉じる]、[戻る]、[更新]など)



表示される内容は、集計目的ごとに異なります。詳細は、“付録A 集計目的一覧”を参照してください。

集計結果に戻る場合は[集計結果]ボタンをクリックしてください。

集計結果または詳細結果をCSV形式で出力する

目的別集計では、集計結果または詳細結果をCSV形式でファイルに出力することができます。

ダウンロードしたCSVファイルはMicrosoft® Office Excelデータとして集計結果を利用することができます。

手順は以下のとおりです。

1. 集計結果の表または詳細結果の表の下に表示されている、[CSV出力]ボタンをクリックします。

   →Microsoft® Office Excelの導入された環境では、[ファイルのダウンロード]画面が表示されます。

2. [開く]または[保存]をクリックします。

   ー 集計結果を保存した場合のファイル名は、“report.csv”です。

   ー 詳細結果を保存した場合のファイル名は、“detail.csv”です。

   どちらのファイル名も、任意のファイル名に変更できます。

第5章 ログビューアでクライアント(CT)での操作を監査する

クライアント(CT)利用者の操作は、各種ログとしてサーバに保存されています。システム管理者または部門管理者は、日常の運用として、ログビューアでクライアント(CT)利用者の操作内容を確認します。

運用方針に沿った操作が行われている場合は、特別な対応は不要です。しかし、運用方針に違反した操作や不正行為の疑いがある操作が見つかった場合は、クライアント(CT)利用者が、何をしようとしていたのか、その操作によって情報が漏洩した可能性はあるかなどを調査する必要があります。

ログに残されているファイル名から利用者のファイル操作を追跡したり、不正行為が行われたCTの情報を検索したりします。

調査の結果、ポリシーの見直しが必要な場合は、該当するクライアント(CT)やユーザーのポリシーを変更します。これにより、違反操作の再発を防ぎ、内部情報をより安全に守ることができるシステム運用を実現します。

5.1 ログビューアを起動する

注意

Webコンソールの起動に関する注意

Webコンソールは同一PC上で複数起動しないでください。

ログビューアを起動する

1. 以下のいずれかの方法で、Webコンソールを起動します。

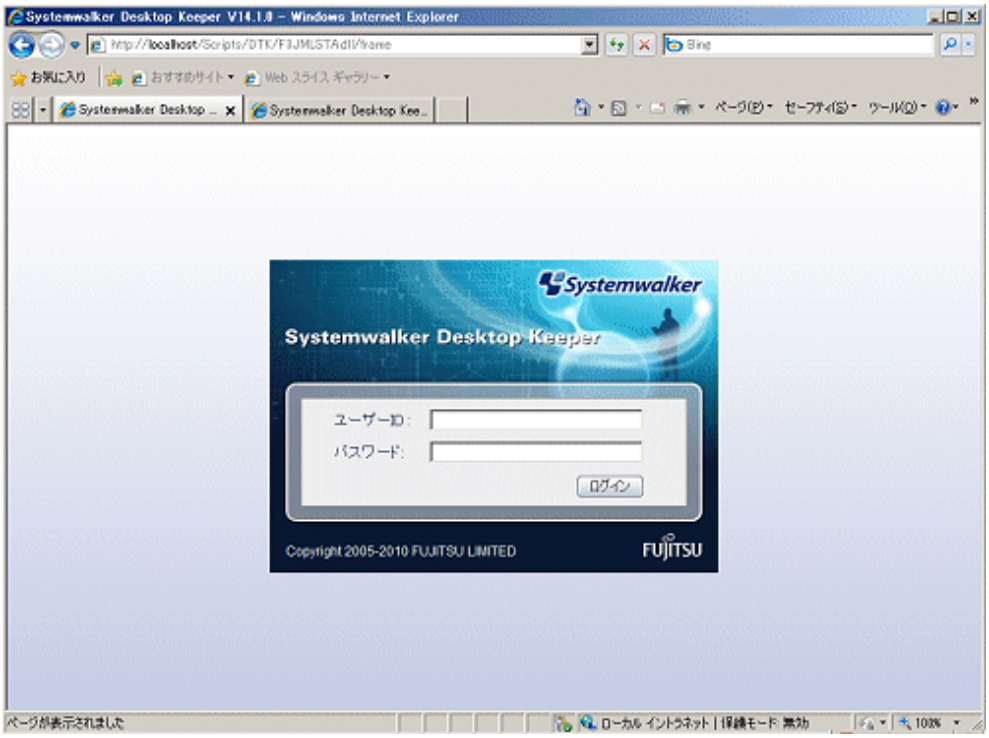
   2階層構成の場合:管理サーバに接続してください。

   - 管理サーバの[スタート]メニューから[プログラム]-[Systemwalker Desktop Keeper]-[サーバ]-[Desktop Keeper メインメニュー]を選択します。
   - ブラウザのアドレスに“http://管理サーバのホスト名またはIPアドレス/DTK/index.html”と指定します。
     IISのポート番号に変更があった場合は、以下のように指定します。
     http://IPアドレス:ポート番号/DTK/index.html

   3階層構成の場合:統合管理サーバに接続してください。

   - 統合管理サーバの[スタート]メニューから[プログラム]-[Systemwalker Desktop Keeper]-[サーバ]-[Desktop Keeper メインメニュー]を選択します。
   - ブラウザのアドレスに“http://統合管理サーバのホスト名またはIPアドレス/DTK/index.html”と指定します。
     IISのポート番号に変更があった場合は、以下のように指定します。
     http://IPアドレス:ポート番号/DTK/index.html

→[ログイン]画面が表示されます。



2. 以下の情報を入力し、[ログイン]ボタンをクリックします。

   システム管理者と部門管理者とで、ログイン方法に違いはありません。

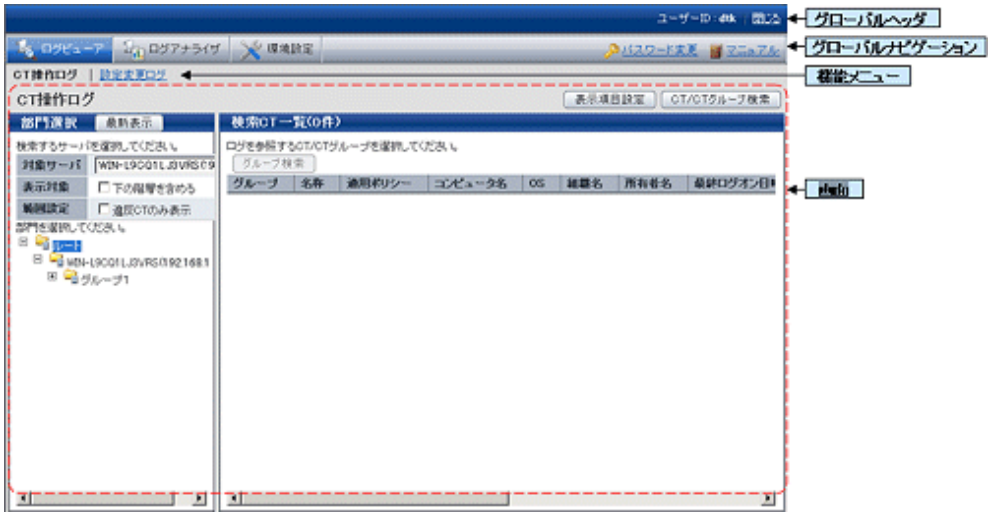
   Systemwalker Desktop Patrolとシングルサインオン連携を行う場合は、ユーザーIDの大文字/小文字を区別して入力してください。

   - **[ユーザーID]:** サーバ設定ツールの[管理者情報設定]画面で設定した[ユーザーID]です。
   - **[パスワード]:** サーバ設定ツールの[管理者情報設定]画面で設定した[パスワード]です。
     パスワードは定期的に変更することを推奨します。変更方法は、“パスワードを変更する”を参照してください。

   →状況画面が表示されます。

3. グローバルナビゲーションの[ログ管理]を選択します。

→ログビューアが起動され、[CT操作ログ]画面が表示されます。



画面の表示内容

グローバルヘッダ

- ユーザーID:ログインしているユーザーIDが表示されます。
- 閉じる:ログビューア画面を閉じます。

グローバルナビゲーション

- ログビューア:ログビューア画面が表示されます。
- ログアナライザ:ログアナライザ画面が表示されます。
- 環境設定:オプション画面(状況画面に表示される集計結果の元になる集計条件を設定する画面)が表示されます。
- パスワード変更:Web画面起動時のパスワードを変更します。変更方法は、“パスワードを変更する”を参照してください。
- マニュアル:マニュアルが表示されます。

機能メニュー

- CT操作ログ:CT操作ログの検索や表示をします。
- 設定変更ログ:設定変更ログの検索や表示をします。

内容

- [表示項目設定]:[検索CT一覧]の表示項目の選択および表示順序の変更ができます。詳細は“検索CT一覧の表示項目を設定する”を参照してください。
- [CT/CTグループ検索]:[CT操作ログ － CT/CTグループ検索]画面が表示されます。クライアント(CT)やCTグループが、管理サーバ配下のどこに存在するか分からない場合に、条件を設定して検索します。
- [部門選択]:ルートの次にサーバ名が表示され、配下のCTグループが表示されます。
  - [最新表示]:[対象サーバ]で選択しているサーバの、最新のツリー構成とCT一覧情報を取り込みます。
  - [対象サーバ]:接続する管理サーバ/統合管理サーバを選択します。
  - [範囲設定]:
    チェックする場合は、選択したCTグループおよびその配下の全CTが[検索CT一覧]に表示されます。
    チェックしない場合は、選択したCTグループ直下の全CTが[検索CT一覧]に表示されます。
  - [表示対象]:
    チェックする場合は、違反ログが発生したクライアント(CT)だけが[検索CT一覧]に表示されます。すでにグループ配下のクライアント(CT)が[検索CT一覧]に表示されている場合、本項目をチェックすると、違反ログが発生したクライアント(CT)だけ

の表示に変更されます。
チェックしない場合は、グループ配下のクライアント(CT)が[検索CT一覧]に表示されます。

CTグループツリーのアイコンについて

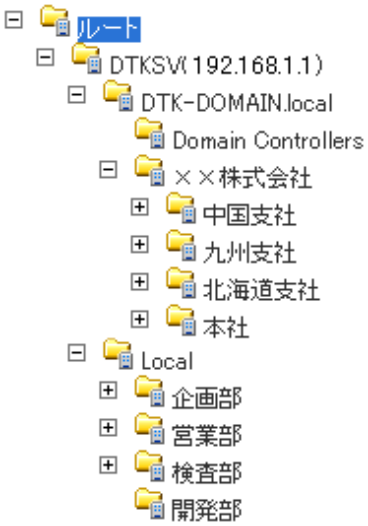
ログビューアにログインするユーザーによって、CTグループツリーに表示されるアイコンが異なります。
以下に、各アイコンが表示される条件を説明します。

ログビューアにログオンする人	表示されるアイコン	アイコンの意味
システム管理者		システム管理者がログビューアにログオンした場合は、すべてのグループが同じアイコンで表示されます。 違反ログが発生したグループやクライアント(CT)を赤字表示する設定を行っていない、または、設定しているが設定期間内に違反ログが発生していないグループです。
		違反ログが発生したグループやクライアント(CT)を赤字表示する設定を行っており、設定期間内に違反ログが発生しているグループです。
		「削除したCT」グループを示します。
部門管理者		自分が部門管理者として設定されているグループを示します。
		自分が部門管理者として設定されていないグループを示します。
		違反ログが発生したグループやクライアント(CT)を赤字表示する設定を行っており、設定期間内に違反ログが発生しているグループです。
		配下のサブグループに、自分が部門管理者として設定されているCTグループが存在するグループを示します。

ドメイン表示

Active Directory連携時には、サーバ表示と合わせてドメイン名も常に表示されます。

【Active Directory連携時のドメイン表示例】



ー [検索CT一覧]:選択したグループに所属するクライアント(CT)が表示されます。表示する項目は、選択できます。方法は、“検索CT一覧の表示項目を設定する”を参照してください。

検索CT一覧の表示項目を設定する

1. [CT操作ログ]画面の[表示項目設定]ボタンをクリックします。

   →[表示項目設定]画面が表示されます。

- [非表示項目]:検索CT一覧に表示しない項目です。
- [表示項目]:検索CT一覧に表示する項目です。初期値として表示されるのは、以下の表の項目名に※がついている項目です。
  また、表示順序を変更できます。項目名の上から表示されている順に、検索CT一覧では左から表示されます。各項目の説明は以下のとおりです。

項目名	説明
[名称](※)	クライアント(CT)に付けることができる名称で、初期値はコンピュータ名です。 変更する場合は、“CTポリシーを変更する”を参照してください。 [名称]は、非表示の項目としては設定できません。
[グループ] (※)	クライアント(CT)が所属するグループです。
[適用ポリシー] (※)	適用されているポリシーです。 [CT]:CTポリシーが設定されていることを示します。 [グループ]:CTグループポリシーが設定されていることを示します。
[コンピュータ名] (※)	クライアント(CT)のコンピュータ名です。
[MACアドレス]	クライアント(CT)のMACアドレスです。
[IPアドレス]	クライアント(CT)のIPアドレスです。
[OS] (※)	クライアント(CT)のOS名です。
[CT区分]	[SE]と表示されます。 (V13.3.0以前のStandard Edition版は[SE]と表示され、Base Edition版は空欄で表示されます。)
[CTバージョン]	インストールされているSystemwalker Desktop Keeperのクライアント(CT)のバージョンです。なお、製品のバージョン/エディションとの対応は、“Systemwalker Desktop Keeper リファレンスマニュアル”の“CTバージョン”を参照してください。
[DTPID]	Systemwalker Desktop Patrolのクライアント(CT)の「ユーザーID(+)PC名」です。

項目名	説明
	Systemwalker Desktop Keeperのクライアント(CT)およびSystemwalker Desktop Patrolのクライアント(CT)が同一のマシンにインストールされている場合に表示されます。
[組織名] (※)	クライアント(CT)のOSに設定されている組織名です。
[所有者名] (※)	クライアント(CT)のOSに設定されている所有者名です。
[サブネットマスク]	クライアント(CT)のネットワークで設定されているサブネットマスクです。
[Active Directory連携]	クライアント(CT)が、Active Directory連携によって情報を取り込んでいるかどうかが表示されます。 ・ Active Directory連携によって情報を取り込んでいるクライアント(CT)の場合: (空欄) ・ Active Directory連携以外の方法で情報を取り込んでいるクライアント(CT)の場合: [非対象]と表示されます。
[ネットワーク参加状況]	クライアント(CT)のネットワーク参加状況が表示されます。 ・ [ドメイン]: ドメインに所属している場合に表示されます。 ・ [ワークグループ]: ドメインに所属していない場合に表示されます。
[ドメイン名]	クライアント(CT)が所属しているドメイン名が表示されます。 [ネットワーク参加状況]が[ワークグループ]の場合は、ワークグループ名が表示されます。
[最終ログオン日時] (※)	クライアント(CT)は起動時に統合管理サーバまたは管理サーバと通信します。その通信でサーバがクライアント(CT)に実施した以下の処理の最終日時です。 ・ CTポリシー送信 ・ ユーザーポリシー送信
[クライアントポリシー更新日時] (※)	管理サーバまたは統合管理サーバが、クライアント(CT)にCTポリシーを送信した最終日時です。 以下の場合に表示または更新されます。 ・ CTリストに追加されたクライアント(CT)が再起動されて、統合管理サーバまたは管理サーバとの通信が開始されたとき ・ 管理コンソールの[即時更新を行う]ボタンをクリックして、クライアント(CT)に対してCTポリシーが反映されたとき
[サーバ(DB)更新日時] (※)	管理サーバまたは統合管理サーバがクライアント(CT)のポリシーを更新し、データベースに反映した最終日時です(即時更新も含みます)。
[備考]	クライアント(CT)のポリシー反映時に入力した情報です。 変更する場合は、“CTポリシーを変更する”を参照してください。
[DTPバージョン]	PCにインストールされている、Systemwalker Desktop Patrol CTのバージョンです。
[トレース状態]	クライアント(CT)でのトレース採取の設定内容です。 ・ [概要]:クライアント(CT)のトレースを概要レベルで採取します。 ・ [詳細]:クライアント(CT)のトレースを詳細レベルで採取します。 ・ 空欄:クライアント(CT)のトレースを採取しません、またはクライアント(CT)がV12.0の場合です。
[違反ログ発生日時] (※)	違反ログがクライアント(CT)で採取された日時です。

※) 初期値として表示される項目です。

2. 表示項目と表示順序を設定し、[設定]ボタンをクリックします。

[部門選択]表示域に「削除したCT」グループを表示する

管理コンソールで削除した(「削除したCT」グループに移動した)クライアント(CT)のログを参照するには、[部門選択]表示域に「削除したCT」グループを表示する必要があります。

この操作は、システム管理者だけが実施できます。

1. [CT操作ログ]画面の[表示項目設定]ボタンをクリックします。

   →以下の画面が表示されます。

2. [部門表示設定]の[「削除したCT」グループを表示]で[表示する]を選択します。

3. [設定]ボタンをクリックします。

Active Directory連携時は、Localグループの直下に、最後のグループとして表示されます。
Active Directory連携していない場合は、サーバ直下に、最後のグループとして表示されます。

「削除したCT」グループに所属するクライアント(CT)のログの参照・検索方法は、他のCTグループのクライアント(CT)のログの参照・検索方法と同じです。

違反ログが発生したグループやクライアント(CT)を赤字表示する

[違反CT表示設定]を行った場合、ログビューア起動時に、違反ログが発生したCTグループを赤字で表示できます(ただし、V14.0.1以前に採取された違反ログは、赤字表示できません)。

赤字表示されたCTグループを選択すると、[検索CT一覧]に表示されるCTのうち、違反ログが発生しているCTの列が赤字で表示されます。

[CT選択]ボタンをクリックすると、[CT選択] に表示されるCTのうち、違反ログが発生しているCTの列が赤字で表示されます。また、表示項目に、[違反ログ数]が表示されます。

1. [CT操作ログ]画面の[表示項目設定]ボタンをクリックします。

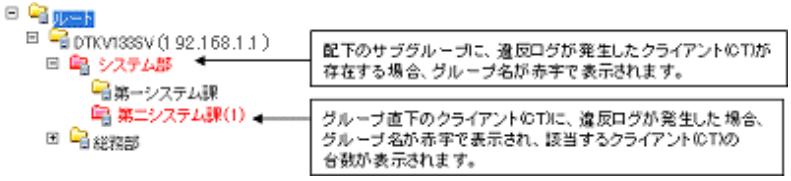
   →以下の画面が表示されます。

各項目の説明は以下のとおりです。

項目名	説明
[違反CT表示]	部門選択画面において、違反ログが発生したクライアント(CT)が所属するグループ及び、違反ログが発生したクライアント(CT)の表示方法を設定します。 ・ **表示する** 違反ログが発生したクライアント(CT)が所属するグループと、違反ログが発生したクライアント(CT)数を赤字表示します。 ・ **表示しない** 違反ログが発生したクライアント(CT)が存在しても、赤字表示はしません。 **初期値:**[表示しない]が選択されています。
[違反表示範囲]	ログビューア起動日から過去にさかのぼって、どこまでの範囲に、違反ログが発生したクライアント(CT)が存在した場合に赤字表示するかを設定します。 [違反CT表示]で[表示する]を選択した場合に設定できます。 ・ **本日** ログビューアを起動した当日に違反ログが発生した場合、そのクライアント(CT)とCTグループを赤字表示します。 ・ **昨日以内** ログビューアを起動した日からさかのぼって昨日以内に違反ログが発生した、クライアント(CT)とCTグループを赤字表示します。 (例)ログビューアを2010/2/10に起動した場合、2010/2/9と2010/2/10に違反ログが発生したクライアント(CT)とCTグループを赤字表示します。 ・ **一週間以内** ログビューアを起動した日の曜日と同じ先週の曜日から本日までに違反ログが発生した、クライアント(CT)とCTグループを、赤字表示します。 (例)ログビューアを月曜日に起動した場合、先週の月曜日から本日の間に違反ログが発生したクライアント(CT)とCTグループを赤字表示します。 ・ **当月内** ログビューアを起動した日からさかのぼって、起動した月の1日までの範囲で、違

項目名	説明
	反ログが発生したクライアント(CT)とCTグループを赤字表示します。 (例)ログビューアを2010/2/10に起動した場合、2010/2/1～2010/2/10に違反ログが発生したクライアント(CT)とCTグループを赤字表示します。 ・ **指定日以内** 指定した年月日からログビューアを起動した日までに違反ログが発生した、クライアント(CT)とCTグループを赤字表示します。
[指定日]	[違反表示範囲]で[指定日以内]を選択した場合に設定できます。 設定した年月日からログビューアを起動した日までに違反ログが発生した、クライアント(CT)とCTグループを赤字表示します。

2. 各項目を設定し、[設定]ボタンをクリックします。



パスワードを変更する

1. グローバルナビゲーションの[パスワード変更]を選択します。

   →[パスワード変更]画面が表示されます。

2. 以下の情報を入力し、[OK]ボタンをクリックします。

   ― **[現在のパスワード]**:これまで使用していたパスワードを入力します。

   ― **[新しいパスワード]**:新しいパスワードを、1～32文字の半角英数字または半角の記号で入力します。
   ただし、「&」、「¥」、「:」、「?」、「”」、「~」、「^」、「’」、「<」、「>」、「|」、および空白は使用できません。また、大文字、小文字は区別されます。

   ― **[新しいパスワードを再入力]**:新しいパスワードを再入力します。

5.2 ログを参照する

システム管理者や部門管理者が参照できるログの範囲、参照可能なログの種類、および参照方法を説明します。

参照可能なログの範囲

システム管理者がログを参照する

システム管理者は、すべてのCT/CTグループに対して、ログビューアでのログの参照、検索、CSV出力ができます。

部門管理者がログを参照する

部門管理者は、自分が部門管理者として設定されているCTグループと、その配下のグループに対して、ログビューアでのログの参照、検索、CSV出力ができます。

参照可能なログの種類

ログビューアで参照可能なログを、以下の一覧に示します。

ログを参照するには、管理コンソールでポリシーの設定が行われ、反映されている必要があります。ポリシーの設定および反映は“2.4.1 端末初期設定をおこなう”、“CTポリシーを変更する”または“3.4.2 ユーザーポリシーを変更する”を参照してください。

ログの参照方法は、“5.2.1 [CT操作ログ]画面で参照する”、“5.2.2 [設定変更ログ]画面で参照する”を参照してください。

[CT操作ログ]画面で参照するログ

参照可能なログの種類	ログの説明	ログを参照するために事前設定しておくポリシー
アプリケーション起動ログ	クライアント(CT)でアプリケーションを起動したときのログです。 Citrix XenAppと連携する場合は、Citrix XenApp クライアントで行ったアプリケーション起動操作が記録されます。	[各種ログスイッチ]タブの[アプリケーション起動ログ]を[する]に設定します。
アプリケーション終了ログ	クライアント(CT)でアプリケーションを終了したときのログです。 Citrix XenAppと連携する場合は、Citrix XenApp クライアントで行ったアプリケーション終了操作が記録されます。	[各種ログスイッチ]タブの[アプリケーション終了ログ]を[する]に設定します。
アプリケーション起動禁止ログ	クライアント(CT)で禁止されているアプリケーションを起動したときのログです。 [ログ一覧]に赤字で表示されます。	[アプリケーション起動禁止]タブの[起動禁止アプリケーション名一覧]に[起動禁止アプリケーションEXE名]を設定します。
ウィンドウタイトル取得ログ	クライアント(CT)で起動したアプリケーションが、ウィンドウで表示されたときのログです。 Citrix XenAppと連携する場合は、Citrix XenApp クライアントで起動したアプリケーションのウィンドウタイトルが記録されます。	[各種ログスイッチ]タブの[ウィンドウタイトル取得ログ]を[する]に設定します。
メール送信ログ	クライアント(CT)でメールを送信したときのログです。	[各種ログスイッチ]タブの[メール送信ログ]を[する]に設定します。 [メール送信]タブの[メール送信時宛先確認]に[確認する]を設定します。
メール送信中止ログ	クライアント(CT)でのメール送信時に、あて先を確認する警告メッセージが表示された場合、送信をキャンセルしたときのログです。	[各種ログスイッチ]タブの[メール送信ログ]を[する]に設定します。 [メール送信]タブの[メール送信時宛先確認]に[確認する]を設定します。
メール添付禁止ログ	クライアント(CT)で禁止対象となるファイルをメールに添付して、送信または保存したときのログです。 [ログ一覧]に赤字で表示されます。	[メール送信]タブからリンクしている[メール送信 ― メール添付禁止拡張子設定]画面の[拡張子一覧]に[拡張子名]を設定します。

参照可能なログの種類	ログの説明	ログを参照するために事前設定しておくポリシー
		[メール送信]タブの[禁止する]を選択します。
デバイス構成変更ログ	クライアント(CT)でデバイスの構成を変更したときのログです。 許可されていないUSBデバイスを装着した場合などは違反行為となり、[ログ一覧]に赤字で表示されます。	[各種ログスイッチ]タブの[デバイス構成変更ログ]を[する]に設定します。
印刷操作ログ	クライアント(CT)で印刷したときのログです。 Citrix XenAppと連携する場合は、Citrix XenApp クライアントで行った印刷操作が記録されます。 仮想プリンタに印刷した場合、Citrix XenApp Server側とCitrix XenApp クライアント側の両方に印刷ログが記録されます。	[各種ログスイッチ]タブの[印刷操作ログ]を[する]に設定します。
印刷禁止ログ	クライアント(CT)で印刷が許可されているアプリケーション以外の印刷があったときのログです。 [ログ一覧]に赤字で表示されます。	[印刷禁止]タブの[印刷禁止]を[する]に設定します。
ログオン禁止ログ	クライアント(CT)で禁止されたグループからログオンしたときのログです。 [ログ一覧]に赤字で表示されます。	[ログオン禁止]タブの[ログオン禁止グループ一覧]に[ログオン禁止グループ]を設定します。
ファイル持出しログ	クライアント(CT)で持出しユーティリティを使用してファイルの持ち出しを行ったときのログです。	[各種ログスイッチ]タブの[ファイル持出しログ]を[する]に設定します。
PrintScreenキー操作ログ	クライアント(CT)でPrintScreenキーを操作したときのログです。 Citrix XenAppと連携する場合は、Citrix XenApp クライアントでのPrintScreenキー操作が記録されます。	[各種ログスイッチ]タブの[PrintScreenキー操作ログ]を[する]に設定します。
PrintScreenキー禁止ログ	PrintScreenキーが禁止されているときに、クライアント(CT)でPrintScreenキーを使用したときのログです。 [ログ一覧]に赤字で表示されます。	[印刷禁止]タブの[PrintScreenキー無効化]を[する]に設定します。
Web操作ログ	クライアント(CT)で以下の操作を実施したときのログです。 ・ Webサイトからのダウンロード	[各種ログスイッチ]タブの[Web操作ログ]を[する]に設定します。
Web操作禁止ログ	クライアント(CT)で以下の操作を実施したときのログです。 [ログ一覧]に赤字で表示されます。 ・ 禁止対象となるURLへのアクセス ・ 禁止対象となるURLからのダウンロード	[URLアクセス禁止]タブの[URLアクセス]を[禁止する]に設定します。 [Webダウンロード禁止]タブの[ダウンロード]を[禁止する]に設定します。
FTP操作ログ	クライアント(CT)で以下の操作を実施したときのログです。 ・ FTPサーバへの接続 ・ FTPサーバへのファイルのアップロード ・ FTPサーバからのファイルのダウンロード ・ FTPサーバからの切断	[各種ログスイッチ]タブの[FTP操作ログ]を[する]に設定します。
FTP操作禁止ログ	クライアント(CT)から禁止対象のFTPサーバへの接続が行われた場合のログです。 [ログ一覧]に赤字で表示されます。	[FTPサーバ接続禁止]タブの[FTPサーバ接続]を[禁止する]に設定します。

参照可能なログの種類	ログの説明	ログを参照するために事前設定しておくポリシー
ファイル操作ログ	クライアント(CT)でファイルを操作したときのログです。 Citrix XenAppと連携する場合は、Citrix XenApp クライアントで行ったファイル操作が記録されます。また、Citrix XenApp Serverへログオンするときに、Citrix XenApp Serverの内部で行われたファイル操作も採取されます。ただし、Citrix XenApp Serverのデバイスマッピングされたドライブに対するファイル操作は取得されません。	[各種ログスイッチ]タブの[ファイル操作ログ]を[する]に設定します。 [ファイル操作プロセス]タブの各項目を設定します。 [ファイル操作拡張子]タブの[ファイル操作ログ取得拡張子一覧]に[拡張子名]を設定します。
ログオン/ログオフ	クライアント(CT)で以下の操作を実施したときのログです。 ・ ログオン ・ ログオフ ・ PC起動 ・ PC終了 ・ PC休止 ・ PC復帰 Citrix XenAppと連携する場合は、Citrix XenApp クライアントからCitrix XenApp Serverへの接続/切断が記録されます。 また、Citrix XenApp クライアントの起動/終了も記録されます。	[各種ログスイッチ]タブの[ログオン/ログオフログ]を[する]に設定します。
連携アプリケーションログ	クライアント(CT)と連携するアプリケーションのログです。 クライアント(CT)と連携するアプリケーションについては、“Systemwalker Desktop Keeper 解説書”の“他製品との連携”を参照してください。	[各種ログスイッチ]タブの[連携アプリケーションログ]を[する]に設定します。
コマンドプロンプト操作ログ	クライアント(CT)で入力されたコマンドおよびコマンド結果のログです。 Citrix XenAppと連携する場合は、Citrix XenApp クライアントで行ったコマンドプロンプト操作が記録されます。	[各種ログスイッチ]タブの[コマンドプロンプト操作ログ]を[する]に設定します。

ポイント

PrintScreenキー操作ログとPrintScreenキー禁止ログの見分け方

PrintScreenキー操作ログとPrintScreenキー禁止ログは、同じログ種別で管理されます(ログ種別は“PrintScreenキー禁止ログ”で管理されます)。
このため、PrintScreenキー操作ログの区分は“正規”、PrintScreenキー禁止ログは“違反”で表示し、区別しています。区分が“違反”の場合は、[ログ一覧]に赤字で表示されます。

[設定変更ログ]画面で参照するログ

設定変更ログは、管理コンソールで行った操作(CTポリシー/ユーザーポリシーの設定情報の変更や、CSV出力など)や、ログビューアで行った操作(ログの検索や、ファイル追跡など)のログです。ログを採取するために、ポリシー設定の必要はありません。
このうち、[設定変更ログ]画面では、以下の4種類のログを参照できます。

- [端末設定]:クライアント(CT)のポリシーを変更した記録です。
- [階層構成設定]:CTグループツリーでクライアント(CT)を移動したなど、CTグループツリーの変更の記録です。
- [サービス制御]:クライアント(CT)のサービスを制御した記録です。

ー [プロセス制御]:クライアント(CT)のプロセスを制御した記録です。

上記以外の設定変更ログは、DTKSTCV.EXE(設定変更ログの出力)コマンドを実行し、CSVファイルに出力して参照してください。
詳細は、“Systemwalker Desktop Keeper リファレンスマニュアル”の“DTKSTCV.EXE (設定変更ログの出力)”を参照してください。

注意

ツリー表示を最新化すると、画面はログオン直後の状態に戻ります

F5キーを押すと、ツリー表示が最新化されます。このとき、画面は、ログオン直後の状態に戻ります。

5.2.1 [CT操作ログ]画面で参照する

ログを参照する

[CT操作ログ]画面でログを参照する方法を説明します。

手順は、以下のとおりです。

1. ログビューアを起動し、[CT操作ログ]画面を表示します。
2. [部門選択]で以下の項目を設定します。
   - ー [対象サーバ]でクライアント(CT)を管理している管理サーバを選択します。
   - ー [範囲設定]の[下の階層を含める]のチェックボックスで、選択したグループ直下のクライアント(CT)だけを表示するか、すべてのクライアント(CT)を表示するかを選択します。
   - ー [表示対象]の[違反CTのみ表示]のチェックボックスで、違反ログが発生したクライアント(CT)だけを表示するか、すべてのクライアント(CT)を表示するかを選択します。
3. [部門選択]のCTグループツリーで、ログを参照するクライアント(CT)が所属するCTグループを選択します。

   CTグループツリーでの選択箇所によって、どの範囲のクライアント(CT)を対象にログを検索・参照できるかが異なります。
   - ー サーバ名を選択する場合:管理サーバ配下の全クライアント(CT)を対象に、ログを検索・参照できます。(※)
   - ー ドメイン名を選択する場合:Active Directory連携時に、選択したドメイン配下の全クライアント(CT)を対象に、ログを検索・参照できます。(※)
   - ー Localグループを選択する場合:Active Directory連携時に、Localグループ配下の全クライアント(CT)を対象に、ログを検索・参照できます。
   - ー CTグループを選択する場合:CTグループ配下の全クライアント(CT)を対象に、ログを検索・参照できます。

   ※) [範囲設定]の[下の階層を含める]をチェックしておく必要があります。

→[検索CT一覧]に、CTグループに所属するクライアント(CT)が表示されます。

違反ログが発生したクライアント(CT)とCTグループは、赤字で表示されます。詳細は、“違反ログが発生したグループやクライアント(CT)を赤字表示する”を参照してください。

注意

以下の場合は、CTグループやCTリストの情報を最新にしてください

ログビューアは、以下の動作により、画面に表示される管理サーバのCTグループ、およびCTリストの情報が最新になっていないことがあります。

- 管理コンソールでCTグループツリーが変更された場合
- Active Directory連携が実行され、グループツリーが変更となった場合
- CT登録時自動振り分けファイルの利用によって、管理コンソールのCTグループに、クライアント(CT)が新たに追加された場合
- 前日からログビューアを起動したままの場合(違反情報が変更されています)

最新にするには、[部門選択]表示域の[最新表示]ボタンをクリックしてください。[対象サーバ]で選択しているサーバの最新情報を表示できます。

4. CT操作ログの参照目的により、以下のいずれかの操作を行います。

【クライアント(CT)単位でログを参照する場合】

a. [検索CT一覧]で、ログを参照するクライアント(CT)の[名称]をクリックします。

【CTグループツリーで選択した範囲配下のクライアント(CT)のログを参照する場合】

a. [検索CT一覧]で、[グループ検索]ボタンをクリックします。

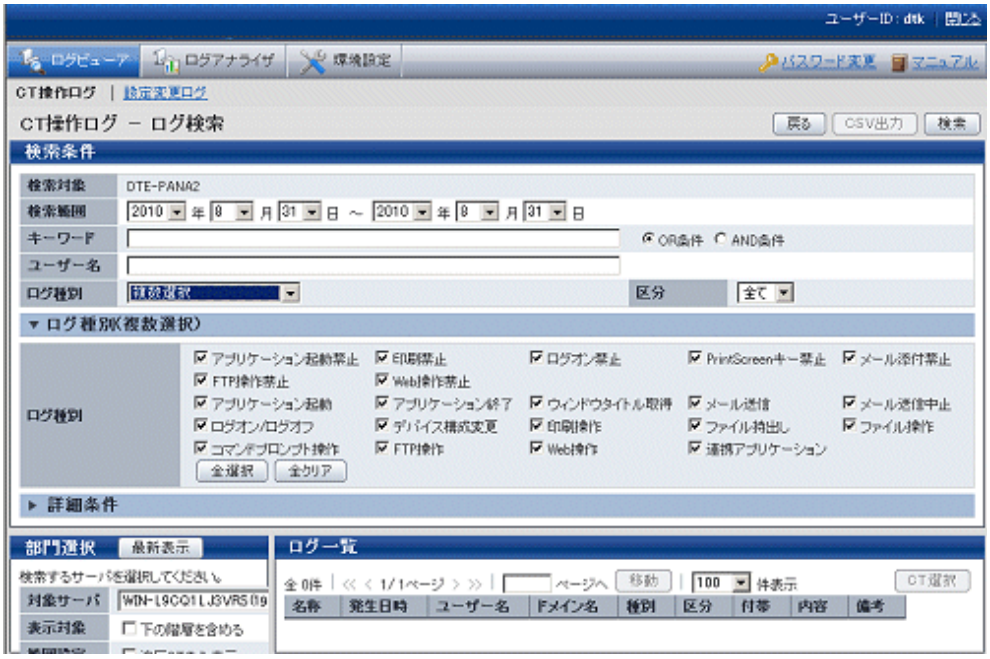
→[CT操作ログ - ログ検索]画面が表示されます。

[詳細条件]、[ログ種別(複数選択)]部分は、開いたり閉じたりできます。
[詳細条件]、[ログ種別(複数選択)](右向きの三角印)をクリックすると、検索条件が開きます。
[▼詳細条件]、[▼ログ種別(複数選択)]をクリックすると、検索条件の部分が閉じます。

注意

IE6の場合は、詳細条件を展開した場合にスクロールバーが表示されません

IE6の場合は、詳細条件を展開した場合にスクロールバーが表示されません。ログ一覧を確認する場合は、ログ種別(複数選択)、詳細条件とも折りたたんだ状態で確認してください。



5. [検索条件]を設定します。
ドライブ種別やログが採取された時間など、詳細な条件を設定する場合は、[詳細条件]をクリックします。

項目名	説明
[検索対象]	検索するログが採取されたクライアント(CT)の名称またはCTグループ名が表示されます。
[検索範囲]	期間の範囲を指定した検索を行えます。 [検索範囲]の開始および終了を指定しないと、すべての期間が検索対象になります。 開始月日を指定しないとその年の年初(1月1日)からの検索になります。 開始日を指定しないとその月の月初(1日)からの検索になります。 ・ 開始年月日の場合 2009年9月-日:2009年9月1日が指定されたとみなします。 2009年-月-日:2009年1月1日が指定されたとみなします。 -年-月-日:格納されている最初のログから検索します。 2009年-月15日:指定エラー -年9月15日:指定エラー 終了月日を指定しないとその年の年末(12月31日)までの検索になります。 終了日を指定しないとその月の月末(最終日)までの検索になります。 ・ 終了年月日の場合 2009年9月-日:2009年9月30日が指定されたとみなします。 2009年-月-日:2009年12月31日が指定されたとみなします。 -年-月-日:格納されている最後のログまでを検索します。 2009年-月15日:指定エラー -年9月15日:指定エラー ※年の指定を省略した場合、月日の指定を省略する必要があります。 月の指定を省略した場合、日の指定を省略する必要があります。

項目名	説明
	初期値として、開始年月日と終了年月日の両方に、[CT操作ログ - ログ検索]画面を表示した年月日が表示されます。 【[表示対象]の[違反CTのみ表示]をチェックして、[グループ検索]ボタンをクリックした場合】 [違反CT表示設定]の[違反表示範囲]に設定されている値が、表示されます。
[キーワード]	ログのキーワードによる検索を行えます。なお、キーワードを複数指定する場合は、キーワードとキーワードの間に半角または全角の空白を入力します。 なお、[検索条件]に[OR条件]を指定すると、指定された複数のキーワードのうち、1つ以上のキーワードを含む「OR検索」となります。また、[検索条件]に[AND条件]を指定すると、指定された複数のキーワードをすべて含む「AND検索」となります。 キーワードを複数指定した場合にそのキーワードがOR条件かAND条件かを選択します。 ログの内容欄および備考欄に表示されている情報のうち、[ ]で囲まれている内容をキーワードとして設定できます。 ログ種別によって、キーワードとして設定できる内容が異なります。詳細は、“8.2.1 アプリケーション起動ログ”～“8.2.23 設定変更ログ”の“表示内容”の内容欄および備考欄を参照してください。
[ユーザー名]	ユーザー名による検索を行えます。なお入力できるユーザー名は1つだけです。
[区分]	ポリシーの設定で、許可された操作、または、許可されていない操作を選択することができます。許可された操作を検索する場合は[正規]、許可されていない操作を検索する場合は[違反]を選択します。[全て]を選択すると、[正規]および[違反]を選択したことになります。 【[表示対象]の[違反CTのみ表示]をチェックして、[グループ検索]ボタンをクリックした場合】 [違反]と表示されます。
[ログ種別]	[ログ一覧]に表示するログの種類を選択します。 2種類以上のログ種別を検索条件に設定する場合は、[複数選択]を選択してください。直下の[ログ種別(複数選択)]が開くので、該当するログ種別をチェックしてください。

[ログ種別(複数選択)]

項目名	説明
[ログ種別]	[ログ一覧]に表示するログの種類にチェックをつけます。ログの種類については、“参照可能なログの種類”を参照してください。 [全選択]:すべてのログ種別にチェックをつけます。 [全クリア]:すべてのログ種別がチェックされていない状態にします。 **初期値:**すべてチェックされています。

[詳細条件]

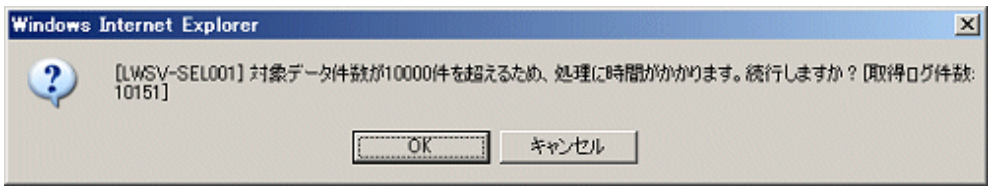
項目名	説明
[ドライブ種別]	ドライブ種別による検索を行えます。 ドライブ種別は、[ログ種別]に以下の項目を設定した場合に、有効となる条件です。 ・ [全て] ・ [ファイル操作] ・ [ファイル持出し] 指定できるのは、以下の4種類です。同時に複数指定できます。 ・ リムーバブル:ドライブレターとして認識される以下の媒体です — フロッピーディスク — 外付けハードディスク(USB、IEEE1394、PCMCIA接続など取り外し可能なハードディスクの場合)

項目名	説明
	ー MO ー USBメモリ ー コンパクトフラッシュメモリ ・ リモート:ネットワークドライブです。 ・ CD/DVD:CD/DVDを挿入できるドライブです。 ・ 固定:PCに固定されているドライブです。 【[ログ種別]と[ドライブ種別]の設定内容と、検索されるログの関係について】 ・ [ログ種別]に[ファイル操作]を設定した場合、以下のA)～J)の場所として[ドライブ種別](リムーバブル、リモート、CD/DVD、固定)が指定されているログが、検索結果として表示されます。 ー A) 新規作成時における、ファイル作成先 ー B) 更新時における、更新ファイルの存在場所 ー C) 参照時における、参照ファイルの存在場所 ー D) 削除時における、削除ファイルの存在場所 ー E) 変名時における、変名前ファイルの存在場所 ー F) 変名時における、変名後ファイルの存在場所 ー G) 複写時における、複写元ファイルの存在場所 ー H) 複写時における、ファイル複写先 ー I) 移動時における、移動元ファイルの存在場所 ー J) 移動時における、ファイル移動先 ・ [ログ種別]に[ファイル持出し]を設定した場合、ファイルの持ち出し先として[ドライブ種別](リムーバブル、リモート、CD/DVD、固定)が指定されているログが、検索結果として表示されます。
[時間]	・ [指定しない]:検索条件に[時間]を含みません。 ・ [範囲指定]:ログが採取された時間の範囲を検索条件に指定します。 ー 「a:00～b:59」と入力した場合、a時0分0秒以降、b時59分59秒以下の条件で検索します。 ー 「a:00～-:59」と入力した場合、a時0分0秒以降、23時59分59秒以下の条件で検索します。 ー 「-:00～b:59」と入力した場合、0時0分0秒以降、b時59分59秒以下の条件で検索します。 aとbの両方を入力する場合、a≦bでなければなりません。 2つの時間範囲を指定する場合、その範囲が重複しても問題ありません。 開始時刻に「-」を指定した場合は、「0」が指定されたことを意味します。 終了時刻に「-」を指定した場合は、「23」が指定されたことを意味します。 初期値は、すべての項目に「-」が設定されています(条件を設定していないことを意味します)。 ・ [時間指定] ログが採取された時間を検索条件にする場合に、該当する時間をチェックします。複数の時間を選択した場合は、1つ以上の時間を含む「OR検索」となります。1つも選択しなかった場合は、すべて選択したものとみなします。 ・ [全選択]:[時間指定]のすべてのチェックボックスがチェックされます。

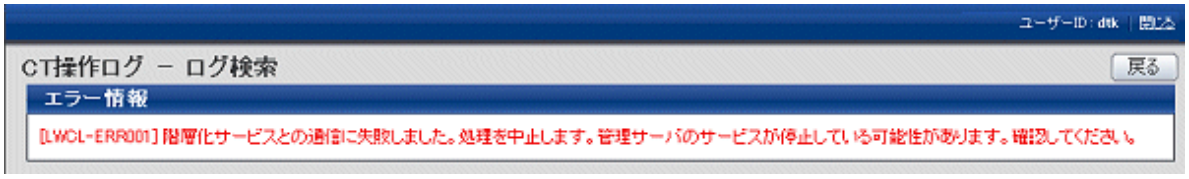
項目名	説明
	・ [全クリア]:[時間指定]のすべてのチェックボックスがクリアされます。 同時に[曜日]も条件指定した場合は、複数の条件をすべて含む「AND検索」となります。
[曜日]	[全選択]:[曜日]のすべてのチェックボックスがチェックされます。 [全クリア]:[曜日]のすべてのチェックボックスがクリアされます。 曜日チェックボックス:ログが採取された曜日を検索条件にする場合に、該当する曜日をチェックします。複数の曜日を選択した場合は、1つ以上の曜日を含む「OR検索」となります。1つも選択しなかった場合は、すべて選択したものとみなします。 同時に[時間]も条件指定した場合は、複数の条件をすべて含む「AND検索」となります。

6. [検索]ボタンをクリックします。

検索結果の件数が10000件を超える場合、以下の画面が表示されます。[OK]ボタンをクリックすると検索を継続し、[キャンセル]ボタンをクリックすると検索条件の画面になります。この画面が表示された場合は、[キャンセル]ボタンをクリックし、検索条件を見直したあとで、再度検索することを推奨します。



検索結果件数が多い場合は、タイムアウトが発生し、以下のメッセージが表示されることがあります。そのときは、検索条件を絞り込んで検索を行ってください。



【検索条件の絞り込み例】

－ 検索期間を短くする

－ 検索対象のCT台数を少なくする

－ 検索キーワード条件を設定する

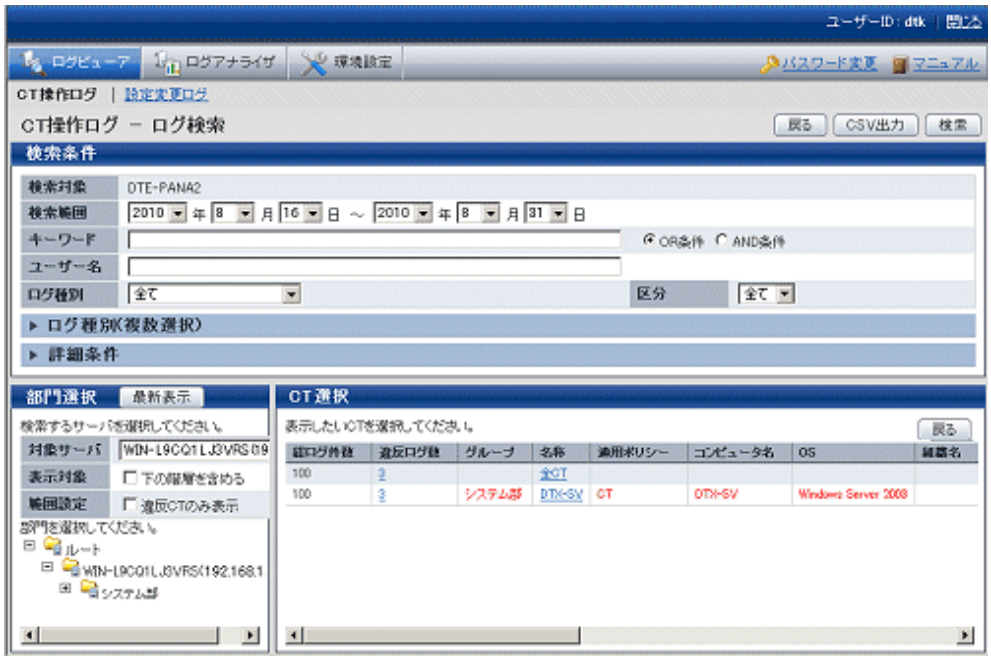
－ 検索ユーザー名を設定する

→検索結果が[ログ一覧]に表示されます。

【クライアント(CT)単位でログを参照する場合】
[ログ一覧]に該当クライアント(CT)のCT操作ログが表示されます。

【CTグループツリーで選択した範囲配下のクライアント(CT)のログを参照する場合】
[ログ一覧]に、CTグループ配下のすべてのクライアント(CT)のCT操作ログが表示されます。

a. [CT選択]ボタンをクリックします。
→[CT選択]にグループ配下のCT一覧が表示されます。



違反ログが発生したクライアント(CT)とCTグループは、赤字で表示されます。詳細は、“違反ログが発生したグループやクライアント(CT)を赤字表示する”を参照してください。

b. ログを参照するクライアント(CT)の[名称]をクリックする場合は、該当クライアント(CT)だけのCT操作ログが表示されます。
ログを参照するクライアント(CT)の[違反ログ数]をクリックする場合は、該当クライアント(CT)の違反ログだけが表示されます。

[ログ一覧]の表示内容

(1) 検索条件に該当するログ件数です。

(2) “<”をクリックすると、一つ前のページが表示され、“>”をクリックすると、次のページが表示されます。“<<”をクリックすると最初のページが表示され、“>>”をクリックすると、最後のページが表示されます。

(3) 1画面で表示するログの件数を選択します。

(4) 現在、全体の何ページ目のログを参照しているかを表示します。

(5) 他のページのログを参照したいとき、ページ数を入力し、[移動]ボタンをクリックします。

各項目名(名称、発生日時、ユーザー名など)をクリックすると、情報がソートされます。

項目名	説明
[名称]	クライアント(CT)に付けることができる名称で、初期値はコンピュータ名です。 変更する場合は、“CTポリシーを変更する”を参照してください。
[発生日時]	ログがクライアント(CT)で採取された時点の年月日および時刻です。
[ユーザー名]	クライアント(CT)へのログオン時に入力するユーザー名です。 だれもログオンしていない(タスクスケジューラによってプログラムが動作した場合など)ときに採取された以下の操作ログの場合は、“SYSTEM”と表示されます。 ・ ファイル操作ログ ・ メール送信ログ ・ メール添付禁止ログ
[ドメイン名]	ドメインにログオン時はクライアント(CT)のドメイン名です。ローカルコンピュータにログオン時はクライアント(CT)のコンピュータ名です。ただし、Windows® 98およびWindows® MEの場合(V12のクライアント(CT)接続時)は空欄です。 だれもログオンしていない(タスクスケジューラによってプログラムが動作した場合など)ときに採取された以下の操作ログの場合は、クライアント(CT)のコンピュータ名が表示されます。 ・ ファイル操作ログ ・ メール送信ログ ・ メール添付禁止ログ
[種別]	ログの種別(種類)です。 以下の禁止ログが採取された場合、その行は、赤字で表示されます。 ・ アプリケーション起動禁止ログ ・ メール添付禁止ログ ・ 印刷禁止ログ ・ ログオン禁止ログ ・ PrintScreenキー禁止ログ ・ Web操作禁止ログ ・ FTP操作禁止ログ
[区分]	ポリシーの設定で、許可された操作の場合は[正規]、許可されていない操作の場合は[違反]です。 [違反]ログが採取された場合、その行は、赤字で表示されます(表示するための設定は不要です)。
[付帯]	・ キャプチャ画面が取得されたウィンドウタイトルログの場合、[1]または[2]が表示されます。 ー [1]:キャプチャ画面が1画面取得された場合 ー [2]:キャプチャ画面が2画面取得された場合 ・ PrintScreenキー禁止ログにおいて、画面キャプチャを取得するポリシーが設定されている場合は、[1]と表示されます。 ・ ファイル持出しログ、または連携アプリケーションログにおいて、原本保管するポリシーが設定されている場合は、[1]と表示されます。

項目名	説明
	・ メール送信ログにおいて、メール内容の参照が可能なポリシーが設定されている場合は、[1]と表示されます。
[内容]	ログの内容です。 すべての内容を確認するには、以下のどちらかの操作を行ってください。 ・ [ログ一覧]に表示されたログの[発生日時]をクリックし、[ログ詳細]画面で確認する。 ・ CSVファイルに出力して確認する。CSVファイルへの出力方法は、“[ログ一覧]の表示内容をCSVファイルに出力する”を参照してください。 ファイル操作ログの対象ファイルのパス長は、519バイトまで表示されます。UNICODE文字を含むパス名は、UNICODE文字の箇所がエスケープ化された表現で表示されます。 以下の条件をすべて満たす場合、UNICODE文字は正しく表示されます。 ・ OSがWindows Vista®、Windows Server® 2008、またはWindows® 7のクライアント(CT)で採取されたログである ・ ログビューアを参照しているPCが、Windows Vista®、Windows Server® 2008、またはWindows® 7である 上記の条件を満たさない場合は、ログに含まれているUNICODE文字は、「?」やエスケープ化した表現(具体的には、“ꪪ”という表現で、AAAA部分は4ケタまたは5ケタの16進コードです)で表示されます。
[備考]	ログの備考内容です。

7. 表示されたログの[発生日時]をクリックします。

→[CT操作ログ - ログ検索 - ログ詳細]画面が表示されます。

項目名	説明
[名称]	クライアント(CT)に付けることができる名称で、初期値はコンピュータ名です。 変更する場合は、“CTポリシーを変更する”を参照してください。
[発生日時]	ログがクライアント(CT)で採取された時点の年月日および時刻です。

項目名	説明
[ユーザー名]	クライアント(CT)へのログオン時に入力するユーザー名です。 だれもログオンしていない(タスクスケジューラによってプログラムが動作した場合など)ときに採取された以下の操作ログの場合は、“SYSTEM”と表示されます。 ・ ファイル操作ログ ・ メール送信ログ ・ メール添付禁止ログ
[ドメイン名]	ドメインにログオン時はクライアント(CT)のドメイン名です。ローカルコンピュータにログオン時はクライアント(CT)のコンピュータ名です。ただし、Windows® 98およびWindows® MEの場合(V12のクライアント(CT)接続時)は空欄です。 だれもログオンしていない(タスクスケジューラによってプログラムが動作した場合など)ときに採取された以下の操作ログの場合は、クライアント(CT)のコンピュータ名が表示されます。 ・ ファイル操作ログ ・ メール送信ログ ・ メール添付禁止ログ
[種別]	ログの種別(種類)です。
[区分]	ポリシーの設定で、許可された操作の場合は[正規]、許可されていない操作の場合は[違反]です。
[内容]	ログの内容です。 ファイル操作ログの対象ファイルのパス長は、519バイトまで表示されます。UNICODE文字を含むパス名は、UNICODE文字の箇所がエスケープ化された表現で表示されます。 以下の条件をすべて満たす場合、UNICODE文字は正しく表示されます。 ・ OSがWindows Vista®、Windows Server® 2008、またはWindows® 7のクライアント(CT)で採取されたログである ・ ログビューアを参照しているPCが、Windows Vista®、Windows Server® 2008、またはWindows® 7である 上記の条件を満たさない場合は、ログに含まれているUNICODE文字は、「?」やエスケープ化した表現(具体的には、“ꪪ”という表現で、AAAA部分は4ケタまたは5ケタの16進コードです)で表示されます。 コマンドプロンプト操作ログの場合、行末に「・」が表示される場合がありますが、これは改行コードを表します。
[備考](注1)	ログの備考内容です。
[付帯](注1)	表示される情報は以下のとおりです。 ・ キャプチャ画面が取得されたウィンドウタイトルログの場合 ー [画像1] ー [画像1]、[画像2] ・ キャプチャ画面が取得されたPrintScreenキー禁止ログの場合 ー [画像1] ・ ファイル持出しログで原本保管するポリシーが設定されている場合 ー [ファイル名](保管されているファイル名が表示されます) ・ 連携アプリケーションログで原本が保管されている場合 ー [原本ファイル]

項目名	説明
	・ メール送信ログで、メール内容の参照が可能なポリシーが設定されている場合 ー [メール内容]
[セッションID](注2)	クライアント(CT)のコマンドプロンプトで実行されたコマンドおよびコマンドからの結果を表すIDです。
[内容ダウンロード](注2)	[内容]に表示される情報を、テキスト形式でダウンロードできます。

注1) コマンドプロンプト操作ログの場合には表示されません。
注2) コマンドプロンプト操作ログの場合に表示されます。

付帯データを参照する

ウィンドウタイトルログやファイル持出しログを採取する場合、キャプチャした画面データや持ち出したファイルの原本データを同時に保存できます。
また、メール送信ログを採取する場合、送信したメールの内容や添付ファイルの内容を保存できます。

これらのデータは、参照することが可能で、実際に表示していた画面、持ち出したファイルの中身、送信したメールの内容や添付ファイルの内容を把握できます。

キャプチャした画面データや持ち出したファイルの原本データは、サーバ設定ツールの[管理者情報設定]画面の[詳細権限]で[付帯情報参照/保存]がチェックされている場合に、参照、保存できます。
送信したメールの内容や添付ファイルの内容は、サーバ設定ツールの[管理者情報設定]画面の[詳細権限]で[メール内容参照]がチェックされている場合に、参照できます。

付帯データとして、ファイルがある場合は、原本保管ファイルを保存することができます。

また、画面キャプチャデータがある場合は、画面キャプチャデータを参照/保存することができます。

画面キャプチャデータを参照/保存する

画面キャプチャデータがあるウィンドウタイトルログやPrintScreenキー禁止ログの場合、[CT操作ログ - ログ検索 - ログ詳細]画面の[付帯]の項目値のリンクをクリックすると、キャプチャした画面を参照することができます。

キャプチャされた画面が2つある場合は、リンクも2つあります。

画面キャプチャデータがあるウィンドウタイトルログは、ログ一覧の[付帯]項目に1画面の画面キャプチャがある場合は[1]、2画面の画面キャプチャがある場合は[2]と表示されます。
画面キャプチャデータがあるPrintScreenキー禁止ログは、ログ一覧の[付帯]項目に[1]と表示されます。

1. [付帯]の項目値のリンクをクリックします。

   →画面キャプチャした画像が表示されます。

注意

画面キャプチャデータを表示できない場合があります

[画像表示]ボタンをクリックした場合に、以下のメッセージが表示される場合があります。

[LWSV-ERR007] 画像データがサーバに転送されていないため表示できません。

これは画面キャプチャデータがまだクライアント(CT)から管理サーバに送信されていない場合、または、CTに画面キャプチャデータを保存する設定にした場合に表示されます。画面キャプチャデータがクライアント(CT)から管理サーバに送信されていない場合は、[OK]ボタンをクリックした後、しばらく待ってから参照してください。CTに画面キャプチャデータを保存する設定の場合は、保存場所の変更が必要です。画面キャプチャデータの保存場所、送信タイミングの設定は管理コンソールの[端末動作設定]で

設定されています。設定内容を確認し、運用に応じて設定を変更してください。[端末動作設定]内容の確認方法については、“2.4.2 端末動作設定をおこなう”を参照してください。

2. [ファイル保存]ボタンをクリックします。
   →[名前を付けて保存]画面が表示されますので、保存する場所を選択し、[保存]ボタンをクリックします。画像がpngファイル形式で指定した場所に保存されます。

   ファイル名は、初期表示されています。
   画面キャプチャデータファイル名："CTの名称" + '-' + ログ発生日時(yyyymmddhhmnss) + '-' + 枚目(1または2) + '.' + 拡張子(例 PC382686-20061215203412-1.png)

3. [閉じる]ボタンをクリックします。

原本保管ファイルを保存する

原本保管ファイルがあるファイル持出しログや連携アプリケーションログの場合、[CT操作ログ - ログ検索 - ログ詳細]画面の[付帯]の項目値のリンクをクリックすると、原本保管したファイルを任意の場所に保存することができます。原本保管ファイルがあるファイル持出しログや連携アプリケーションログは、[ログ一覧]の[付帯]項目に[1]と表示されます。

1. [付帯]の項目値のリンクをクリックします。

   →[名前を付けて保存]画面が表示されますので、保存する場所を選択し、[保存]ボタンをクリックします。
   ファイル名には、原本保管時のファイル名が初期表示されています。必要に応じて、ファイル名を変更して保存してください。

   - ファイル持出しログの原本保管ファイル名：持ち出し元のファイル名
   - 連携アプリケーションログの原本保管ファイル名："CTの名称" + '-' + ログ発生日時(yyyymmddhhmnss) + '.' + 拡張子 (例 PC382686-20061226132137.wmf)

注意

原本保管ファイルを保存できない場合があります

[ファイル保存]ボタンをクリックした場合に、以下のメッセージが表示される場合があります。

[LWSV-ERR010] 原本ファイルがサーバに転送されていないため表示できません。

これは原本保管ファイルが、クライアント(CT)から管理サーバにまだ送信されていない場合、または、クライアント(CT)に原本ファイルを保存する設定にした場合に表示されます。原本保管ファイルが、クライアント(CT)から管理サーバにまだ送信されていない場合は、[OK]ボタンをクリックした後、しばらく待ってから参照してください。CTに原本保管ファイルを保存する設定の場合は、保存場所の変更が必要です。原本ファイルの保存場所、送信タイミングの設定は管理コンソールの[端末動作設定]で設定されています。設定内容を確認し、運用に応じて設定を変更してください。[端末動作設定]内容の確認方法については、“2.4.2 端末動作設定をおこなう”を参照してください。

[ログ一覧]の表示内容をCSVファイルに出力する

CSVファイルへの出力、保存は、サーバ設定ツールの[管理者情報設定]画面の[詳細権限]で[CSVファイル保存]がチェックされている場合に実行できます。

1. [ログ一覧]にCSVファイルに出力するログが表示されている状態で、[CSV出力]ボタンをクリックします。
2. ファイルのダウンロード画面が表示されます。[保存]ボタンをクリックします。
3. 保存するフォルダを選択し、ファイル名を入力して、[保存]ボタンをクリックします。

出力先に同じ名前のファイルが存在していた場合は、上書きするかどうかの選択画面が表示されます。必要に応じてどちらかを選択してください。

出力されるCSVファイルの項目名と説明については、“Systemwalker Desktop Keeper リファレンスマニュアル”の“ログ一覧”を参照してください。

ファイルのダウンロードが成功しない場合について

CSVファイル、原本保管ファイル、コマンドプロンプトログファイルのダウンロードが成功しない場合、“Systemwalker Desktop Keeper 導入ガイド”の“Webブラウザを使用するPCでの準備”を参照して、Internet Explorer®の設定を変更してください。

5.2.2 [設定変更ログ]画面で参照する

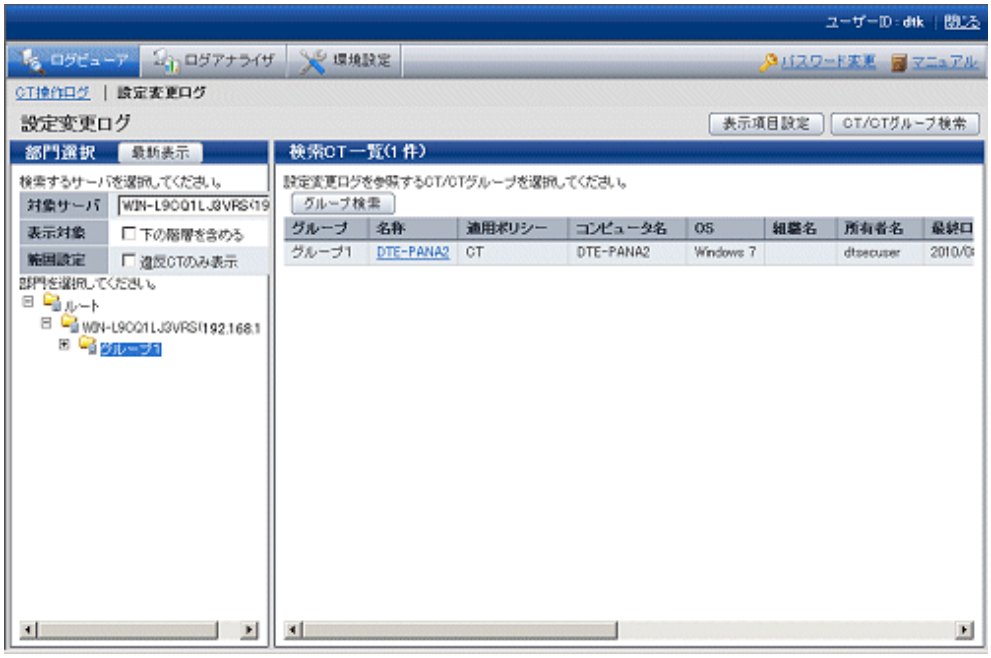
[設定変更ログ一覧]を表示して、管理コンソールでクライアント(CT)の設定情報を変更したときのログを参照する方法について説明します。

[設定変更ログ一覧]は、サーバ設定ツールの[管理者情報設定]画面の[詳細権限]で参照権を与えられている場合に参照できます。

手順は、以下のとおりです。

1. ログビューアを起動し、[設定変更ログ]を選択します。

   →[設定変更ログ]画面が表示されます。



2. [部門選択]の[対象サーバ]でクライアント(CT)を管理している管理サーバを選択します。また、[範囲設定]の「下の階層を含める」のチェックボックスで、選択したグループ直下のクライアント(CT)だけを表示するか、すべてのクライアント(CT)を表示するかを選択します。

3. 設定変更ログの参照目的により、以下のいずれかの操作を行います。

   【管理サーバで設定した[端末初期設定]ポリシーの設定変更ログを参照する場合】

   a. [部門選択]のCTグループツリーに表示されているサーバを選択します。

      →[検索CT一覧]に、クライアント(CT)が表示されます。

   b. [検索CT一覧]の[グループ検索]ボタンをクリックします。

      →[設定変更ログ - ログ検索]画面が表示されます。
      この場合、手順4は不要です。

   【単独のクライアント(CT)に対する設定変更ログを参照する場合】

   a. [部門選択]のCTグループツリーで、ログを参照するクライアント(CT)が所属するCTグループを選択します。

      →[検索CT一覧]に、CTグループに所属するクライアント(CT)が表示されます。

   【CTグループとそれに所属するクライアント(CT)に対する設定変更ログを参照する場合】

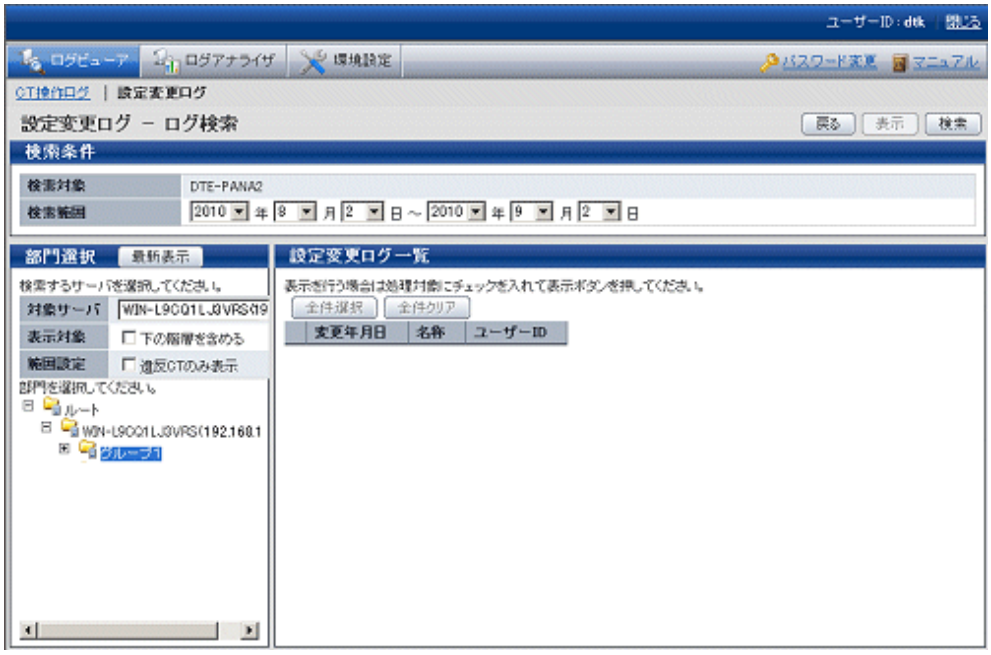
   a. [部門選択]のCTグループツリーで、ログを参照するCTグループを選択します。

   b. [検索CT一覧]の[グループ検索]ボタンをクリックします。

      →[設定変更ログ - ログ検索]画面が表示されます。
      この場合、手順4は不要です。

4. ログを参照するクライアント(CT)の[名称]をクリックします。

   →[設定変更ログ - ログ検索]画面が表示されます。

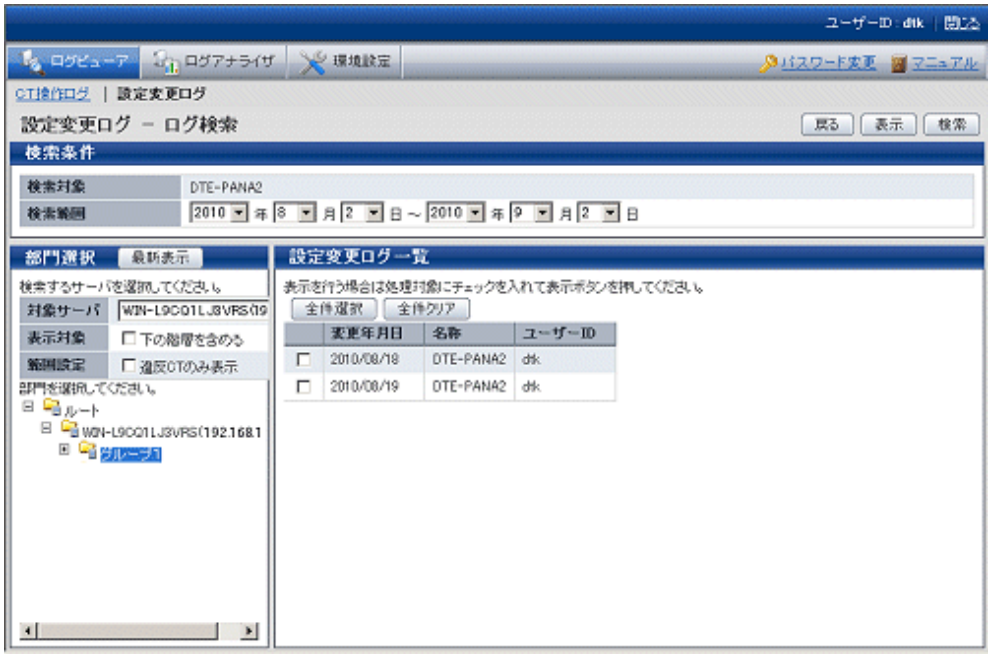


5. [検索条件]を設定します。

項目名	説明
[検索範囲]	期間の範囲を指定した検索を行えます。[検索範囲]の開始および終了を指定しないと、すべての期間が検索対象になります。 開始月日を指定しないとその年の年初(1月1日)からの検索になります。 開始日を指定しないとその月の月初(1日)からの検索になります。 終了月日を指定しないとその年の年末(12月31日)までの検索になります。 終了日を指定しないとその月の月末(最終日)までの検索になります。 初期値として、開始年月日と終了年月日の両方に、[CT操作ログ - ログ検索]画面を表示した年月日が表示されます。 ・ 開始年月日の場合 2009年9月-日:2009年9月1日が指定されたとみなします。 2009年-月-日:2009年1月1日が指定されたとみなします。 -年-月-日:格納されている最初のログから検索します。 2009年-月15日:指定エラー -年9月15日:指定エラー ・ 終了年月日の場合 2009年9月-日:2009年9月30日が指定されたとみなします。 2009年-月-日:2009年12月31日が指定されたとみなします。 -年-月-日:格納されている最後のログまでを検索します。 2009年-月15日:指定エラー -年9月15日:指定エラー ※年の指定を省略した場合、月日の指定を省略する必要があります。 月の指定を省略した場合、日の指定を省略する必要があります。

6. [検索]ボタンをクリックします。

→検索結果が[設定変更ログ一覧]に表示されます。

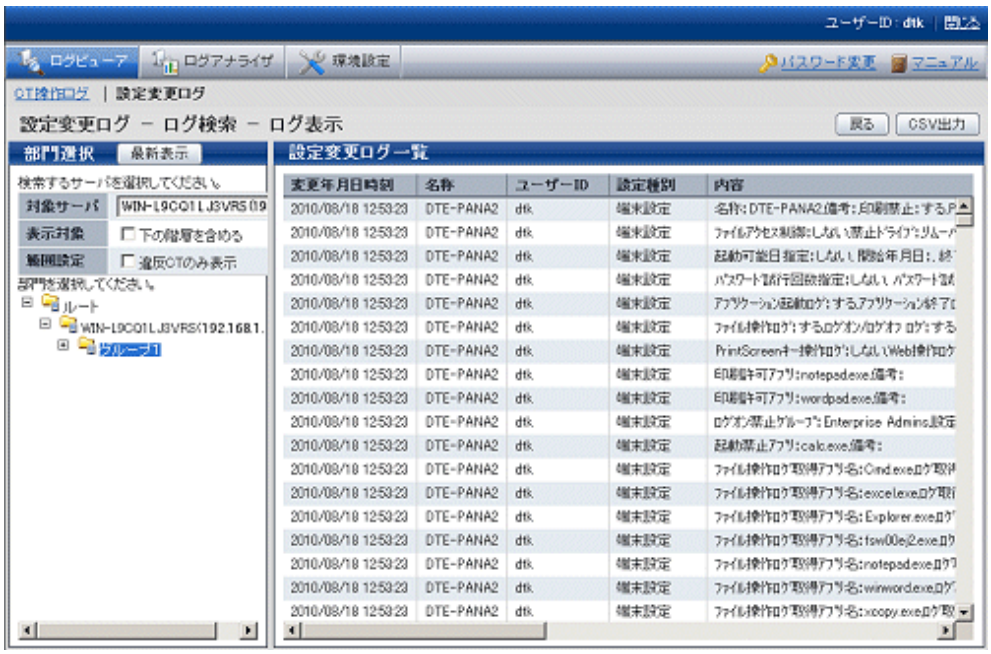


各項目名(変更年月日、名称、ユーザーID)をクリックすると、情報がソートされます。

項目名	説明
[変更年月日]	設定が変更された年月日です。
[名称]	クライアント(CT)に付けることができる名称で、初期値はコンピュータ名です。 端末初期設定ポリシーを変更した場合は[端末初期設定ポリシー]と表示されます。 CTグループに対する設定変更の場合は、CTグループ名が表示されます。
[ユーザーID]	管理コンソールにログオンして、設定を変更した人のユーザーIDです。

7. 検索結果のうち、設定変更内容の詳細を表示するものにチェックをつけ、[表示]ボタンをクリックします。
   [全件選択]ボタンをクリックすると、すべての検索結果にチェックがつきます。
   [全件クリア]ボタンをクリックすると、検索結果についているチェックが、すべてクリアされます。

   →[設定変更ログ ― ログ検索 ― ログ表示]画面に詳細が表示されます。



項目名	説明
[変更年月日時刻]	設定が変更された年月日時刻です。
[名称]	クライアント(CT)に付けることができる名称で、初期値はコンピュータ名です。 端末初期設定ポリシーを変更した場合は[端末初期設定ポリシー]と表示されます。 CTグループに対する設定変更の場合は、CTグループ名が表示されます。
[ユーザーID]	管理コンソールにログオンして、設定を変更した人のユーザーIDです。
[設定種別]	設定変更の種別(種類)として、以下が表示されます。 ・ [端末設定]:クライアント(CT)のポリシーを変更した記録です。 ・ [階層構成設定]:CTグループツリーでクライアント(CT)を移動したなど、CTグループツリーの変更の記録です。 ・ [サービス制御]:クライアント(CT)のサービスを制御した記録です。 ・ [プロセス制御]:クライアント(CT)のプロセスを制御した記録です。
[内容]	設定変更ログの内容です。内容は259文字まで表示されます。 すべての内容を確認するには、CSVファイルに出力して確認してください。CSVファイルへの出力方法は、“[設定変更ログ一覧]の表示内容をCSVファイルに出力する”を参照してください。

[設定変更ログ一覧]の表示内容をCSVファイルに出力する

CSVファイルへの出力、保存は、サーバ設定ツールの[管理者情報設定]画面の[詳細権限]で[CSVファイル保存]がチェックされている場合に実行できます。

1. [設定変更ログ一覧]に、CSVファイルに出力する設定変更ログが表示されている状態で、[CSV出力]ボタンをクリックします。
2. ファイルのダウンロード画面が表示されます。[保存]ボタンをクリックします。

3. 保存するフォルダを選択し、ファイル名を入力して、[保存]ボタンをクリックします。

出力先に同じ名前のファイルが存在していた場合は、上書きするかどうかの選択画面が表示されます。必要に応じてどちらかを選択してください。

出力されるCSVファイルの項目名と説明については、“Systemwalker Desktop Keeper リファレンスマニュアル”の“設定変更ログ一覧”を参照してください。

ファイルのダウンロードが成功しない場合について

CSVファイル、原本保管ファイル、コマンドプロンプトログファイルのダウンロードが成功しない場合、“Systemwalker Desktop Keeper 導入ガイド”の“Webブラウザを使用するPCでの準備”を参照して、Internet Explorer®の設定を変更してください。

5.3 ファイル操作を追跡する

ファイル操作ログを参照した結果、不正行為の疑いがあるクライアント(CT)利用者が存在する場合は、その利用者が行ったファイル操作の遷移を検索/表示できます。

ファイル追跡機能は、クライアント(CT)で行われたファイル操作を「ファイル操作ログ」「ファイル持出しログ」「メール送信ログ(添付ファイルがある場合)」「メール送信中止ログ(添付ファイルがある場合)」「メール添付禁止ログ」「FTP操作ログ(FTPアップロードログ・FTPダウンロードログ)」「Web操作ログ」から、その操作遷移を検索/表示するツールです。ファイル追跡機能は、以下の機能を提供します。

ログビューアで検索したログから、ファイル追跡対象となるファイル選択し、操作追跡を行うことができます。また追跡結果の表示およびCSVファイルへの出力ができます。

追跡対象として選択できる操作ログは、ファイルの操作情報を持った以下のログです。

- ファイル操作ログ
- ファイル持出しログ
- メール送信ログ(添付ファイルがある場合)
- メール送信中止ログ(添付ファイルがある場合)
- メール添付禁止ログ
- FTP操作ログ(FTPアップロードログ・FTPダウンロードログ)
- Web操作ログ

また、上記操作ログの補足情報として、以下のログを追跡結果に含めることができます。

- 印刷操作ログ
- 印刷禁止ログ

注意

【Citrix XenApp クライアントでのファイル操作を追跡することはできません】

Citrix XenApp クライアントで行ったファイル操作のログを利用して、ログビューアでファイル追跡機能を使用することはできません。

【Systemwalker Desktop Keeper のクライアント(CT)でのファイル操作を追跡できる範囲】

追跡の範囲は、追跡対象として設定したログが取得されたクライアント(CT)内です。複数のクライアント(CT)を横断した追跡は行えません。

ファイル操作を追跡する

追跡対象となるファイル情報を設定する方法を説明します。

ファイル追跡を行うため、追跡対象となるファイル情報を設定します。ファイル情報を設定するために、まず、ファイルの操作情報をもつ、以下のログを表示します。

- ファイル操作ログ
- ファイル持出しログ
- メール送信ログ(添付ファイルがある場合)
- メール送信中止ログ(添付ファイルがある場合)
- メール添付禁止ログ
- FTP操作ログ(FTPアップロードログ・FTPダウンロードログ)
- Web操作ログ

印刷操作ログおよび印刷禁止ログは、ファイル追跡対象ログとして選択できません。
これらのログに含まれているファイル名を追跡対象にする場合は、[CT操作ログ ― ログ検索]画面の[キーワード]に、印刷操作ログ、印刷禁止ログに含まれるファイル名を入力してログ検索してください。この検索結果に上記のログ(ファイル操作ログ、ファイル持出しログ、メール送信ログ、メール送信中止ログ、メール添付禁止ログ、FTP操作ログ、Web操作ログ)が含まれる場合は、そのログを追跡対象に設定することによりファイル追跡を行えます。

追跡対象に設定されたファイル情報からファイル追跡を行う方法を説明します。

「ファイル操作ログ」、「ファイル持出しログ」、「メール送信ログ」「メール送信中止ログ」「メール添付禁止ログ」「FTP操作ログ」および「Web操作ログ」は、追跡対象となっているファイル名(パス部分を除く)は完全一致で検索されます(パスを含む検索結果は“確度”で表現しています)。
一方、「印刷操作ログ」および「印刷禁止ログ」は、追跡対象となっているファイル名は部分一致で検索されるため、追跡対象ファイルのログが検索されると同時に、追跡対象ファイルとは関連性の低いログも検索される場合があります。

ファイル追跡条件を設定し、追跡対象ファイル情報を基準としてファイル追跡を行います。

1. ログビューアを起動します。
2. ファイル追跡を実施する操作ログの[CT操作ログ - ログ検索 - ログ詳細]画面を表示します。
   表示方法は、“5.2.1 [CT操作ログ]画面で参照する”を参照してください。

3. [ファイル追跡]ボタンをクリックします。

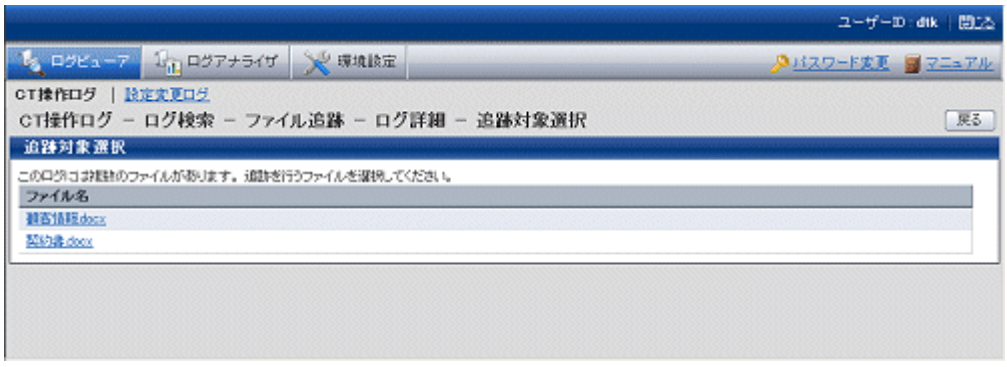
→選択されているログ種別が[メール送信]かつログの内容に添付ファイルが複数ある場合は[CT操作ログ－ログ検索－ファイル追跡－ログ詳細－追跡対象選択]画面が表示されます。表示条件に該当しない場合は、[CT操作ログ － ログ検索 － ファイル追跡]画面が表示されます。

[CT操作ログ－ログ検索－ファイル追跡－ログ詳細－追跡対象選択]画面について

以下の条件に該当する場合に[CT操作ログ－ログ検索－ファイル追跡－ログ詳細－追跡対象選択]画面が表示されます。

- 選択されているログ種別が[メール送信] かつ ログの内容に添付ファイルが複数ある場合

a) [CT操作ログ－ログ検索－ファイル追跡－ログ詳細－追跡対象選択]画面が表示されます。



b) [追跡対象選択]よりファイル追跡を行うファイルを選択します。
→選択された添付ファイル名が追跡対象ファイルとして設定されます。

4. [検索条件]を設定します。

項目名	説明
[CT名称]	[ログビューア]画面で選択したログのクライアント(CT)の名称が表示されます。ファイル追跡は、このクライアント(CT)で採取されたログの範囲内を検索対象とします。
[ログ種別]	[ログビューア]画面で選択したログの種別が表示されます。
[検索対象ファイル]	追跡対象となるファイル名が表示されます。
[実施する検索]	[バックトレース] 選択したログより、過去にさかのぼってファイルがどう扱われていたかを検索します。ファイル操作ログの「複写」「移動」「変名」「作成」「更新」「削除」の操作と、ファイル持

項目名	説明
	出しログの持ち出し操作だけを追跡します。過去のファイル操作を調査したい場合に使用します。 [フォワードトレース] 選択したログより、未来に向かってファイルがどう扱われているかを検索します。追跡対象として指定された操作ログの発生日時からの操作遷移を調査することができます。1つのファイルが複写操作によって複数になるなど、ログによっては検索対象が拡散し検索結果が多くなる場合があります。
[検索範囲]	検索範囲を指定します。期間(日数)指定と日付指定の選択ができます。 初期値は「期間(日数)指定」が選択されています。 指定できる期間(日数)または日付は以下のとおりです。 ・ 期間(日数)指定 ー 「0」～「999」まで指定できます。追跡対象として指定された操作ログの発生日を「0」とします。初期値は「10」が設定されています。 ・ 日付指定 期間の範囲を指定した検索を行えます。[検索範囲]の開始および終了を指定しないと、バックトレースの場合は発生日を含む過去のログがすべて検索対象となり、フォワードトレースの場合は発生日を含む未来のログがすべて検索対象になります。 【バックトレースの場合】 開始月日を指定しないと、その年の年初(1月1日)から、発生日までの検索になります。 開始日を指定しないと、その年月の月初(1日)から、発生日までの検索になります。 【フォワードトレースの場合】 終了月日を指定しないと、発生日から、その年の年末(12月31日)までの検索になります。 終了日を指定しないと、発生日から、その年月の月末(最終日)までの検索になります。 ー 「2004/1/1」～「2024/12/31」まで指定できます。 ー [バックトレース]の場合、追跡対象として指定された操作ログの発生日より未来日を指定することはできません。 ー [フォワードトレース]の場合、追跡対象として指定された操作ログの発生日より過去日を指定することはできません。 ー [バックトレース]および[フォワードトレース]のどちらの場合も、追跡対象として指定された操作ログの発生日を指定することはできます。 ー 開始年月日の場合 2009年9月-日:2009年9月1日が指定されたとみなします。 2009年-月-日:2009年1月1日が指定されたとみなします。 -年-月-日:格納されている最初のログから検索します。 2009年-月15日:指定エラー -年9月15日:指定エラー ー 終了年月日の場合 2009年9月-日:2009年9月30日が指定されたとみなします。 2009年-月-日:2009年12月31日が指定されたとみなします。 -年-月-日:格納されている最後のログまでを検索します。 2009年-月15日:指定エラー -年9月15日:指定エラー

項目名	説明
	※年の指定を省略した場合、月日の指定を省略する必要があります。 月の指定を省略した場合、日の指定を省略する必要があります。
[検索対象ログ]	[実施する検索]が[フォワードトレース]の場合、検索対象ログの種別を選択することができます。ファイル操作ログは必須選択のためOFF設定できません。
[最大検索階層]	検索する最大階層を指定します。「1」～「9」まで指定できます。初期値は「4」です。

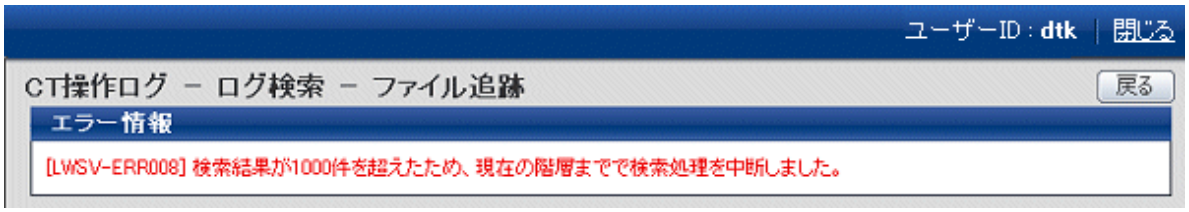
5. [検索]ボタンをクリックします。

→[ファイル追跡結果一覧]に結果が表示されます。
検索条件は自動的に保存されます。保存された検索条件は、次回[ファイル追跡]画面起動時の初期値として設定されます。

項目名	説明
[検索ルート(種別)]	選択ログを先頭に、追跡したログの結果がツリーで表示されます。
[確度]	追跡したログの一致度合い(確度)を表します。 0:調査開始対象のログ A:ドライブ、あるいはUNC表記での完全一致で検索したログ B:共有名以降の一致で検索したログ C:フォルダ名以降の一致で検索したログ D:ファイル名だけの一致で検索したログ E:印刷操作ログおよび印刷禁止ログで、ファイル名が部分一致しているログ *:追跡ログの中に同じログがある場合に表示します。 上記の確度(A～E)の前に付加されます。 +:さらに追跡可能なログがある場合に表示します。 上記の確度(A～E)の前に付加されます。
[発生日時]	ログの発生日時を表示します。 クリックすると、ログの詳細が表示されます。
[ユーザー名]	ユーザー名を表示します。

項目名	説明
[ドメイン名]	ドメインにログオン時はクライアント(CT)のドメイン名です。ローカルコンピュータにログオン時はクライアント(CT)のコンピュータ名です。
[区分]	ログの区分（正規または違反）を表示します。
[付帯]	ログの付帯データの有無を表示します。付帯データの内容については“付帯データを参照する”を参照してください。
[内容]	ログの内容を表示します。
[備考]	ログの備考内容を表示します。

検索結果の件数が1000件を超える場合、以下の画面が表示されます。また検索結果は1000件まで表示されます。

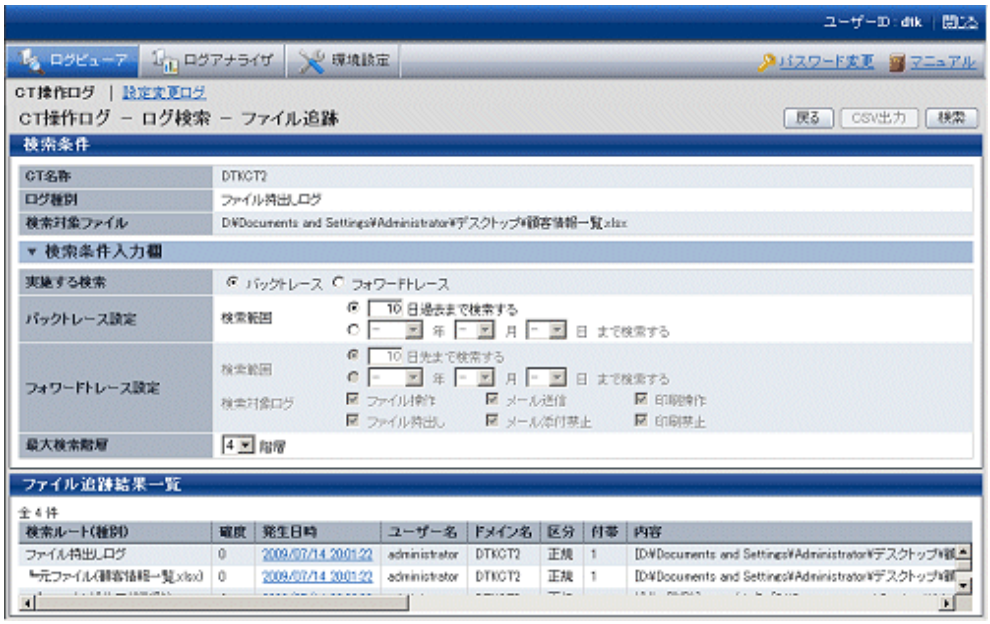


バックトレース検索の例

選択したログより、過去にさかのぼってファイルがどう扱われていたかを検索します。ファイル操作ログの「複写」「移動」「変名」「作成」「更新」「削除」の操作と、ファイル持出しログの持ち出し操作だけを追跡します。過去のファイル操作を調査したい場合に使用します。

バックトレース検索例

(調査対象ファイル:顧客情報一覧.xls)



[ファイル追跡結果一覧]の[内容]に着目します。

[検索ルート(種別)]の情報	[内容]の情報
ファイル持出しログ	[C:¥Documents and Settings¥Administrator¥デスクトップ¥顧客情報一覧.xls]を[E:¥顧客情報一覧.ex_]として[暗号化]で[E:]へ持出ししました。ドライブ種別:[リムーバブル]]

[検索ルート(種別)]の情報	[内容]の情報
元ファイル(顧客情報一覧.xls)	[C:¥Documents and Settings¥Administrator¥デスクトップ¥顧客情報一覧.xls]を[E:¥顧客情報一覧.ex_]として[暗号化]で[E:]へ持出ししました。ドライブ種別:[リムーバブル]]
ファイル操作ログ(変名)	操作:[変名]、ファイル名元:[C:¥Documents and Settings¥Administrator¥デスクトップ¥新規.xls]、ドライブ種別元:[固定]、ファイル名先:[C:¥Documents and Settings¥Administrator¥デスクトップ¥顧客情報一覧.xls]、ドライブ種別先:[固定]、アプリ名:[Explorer.exe]
ファイル操作ログ(作成)	操作:[作成]、ファイル名:[C:¥Documents and Settings¥Administrator¥デスクトップ¥新規.xls]、ドライブ種別:[固定]、アプリ名:[Explorer.exe]

調査対象ファイル(顧客情報一覧.xls)の情報が、先頭行に表示されています。下段に進むにしたがって、操作内容は過去にさかのぼります。

この検索結果を先頭行からみると、DTKCT2というクライアント(CT)において

1. 調査対象ファイル(顧客情報一覧.xls)を、リムーバブルメディアに暗号化して持ち出した。
2. 調査対象ファイルは、新規.xlsから顧客情報一覧.xlsに変名された。
3. 新規.xlsが、デスクトップに作成された。

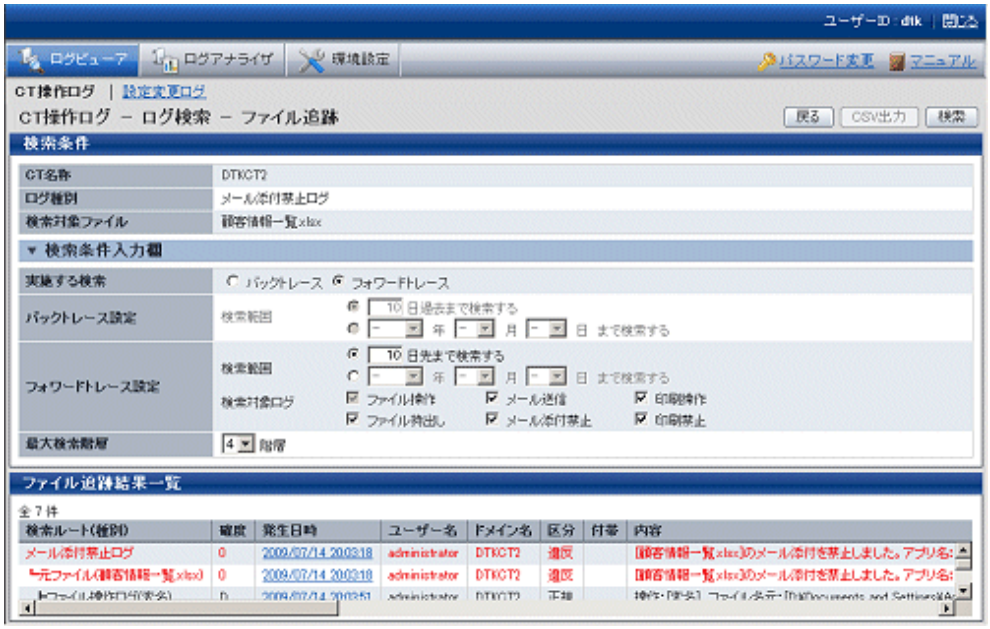
という操作履歴になっており、デスクトップ上に「新規.xls」というファイルを作成し、「顧客情報一覧.xls」に変名後、リムーバブルメディアに暗号化して持ち出したことがわかります。

フォワードトレース検索の例

選択したログより、未来に向かってファイルがどう扱われているかを検索します。追跡対象として指定された操作ログの発生日時からの操作遷移を調査することができます。1つのファイルが複写操作によって複数になるなど、ログによっては検索対象が拡散し検索結果が多くなる場合があります。

フォワードトレース検索例

(調査対象ファイル:顧客情報一覧.xls)



[ファイル追跡結果一覧]の[内容]に着目します。

[検索ルート(種別)]の情報	[内容]の情報
メール添付禁止ログ	[顧客情報一覧.xls]のメール添付を禁止しました。アプリ名:[Microsoft Office Outlook, Build 11.0.5510]
元ファイル(顧客情報一覧.xls)	[顧客情報一覧.xls]のメール添付を禁止しました。アプリ名:[Microsoft Office Outlook, Build 11.0.5510]
ファイル操作ログ(変名)	操作:[変名]、ファイル名元:[C:¥Documents and Settings¥Administrator¥デスクトップ¥顧客情報一覧.xls]、ドライブ種別元:[固定]、ファイル名先:[C:¥Documents and Settings¥Administrator¥デスクトップ¥会議資料.xls]、ドライブ種別先:[固定]、アプリ名:[Explorer.exe]
ファイル持出しログ	[C:¥Documents and Settings¥Administrator¥デスクトップ¥会議資料.xls]を[E:¥会議資料.xls]として[平文]で[E:]へ持出ししました。ドライブ種別:[リムーバブル]]

調査対象ファイル(顧客情報一覧.xls)の情報が、先頭行に表示されています。下段に進むにしたがって、調査対象ファイルが現在に向かってどのように操作されたか、表示されます。

この検索結果を先頭行からみると、DTKCT2というクライアント(CT)において

1. 顧客情報一覧.xlsをメールに添付して送信したが、禁止が設定されていたため、送信できなかった。
2. ファイル名を顧客情報一覧.xlsから会議資料.xlsに変更した。
3. 会議資料.xlsのファイル持出しを行った。

という操作履歴になっており、会議資料として顧客情報一覧をメールに添付して送信しようとしたが、できなかったため、ファイル名を変更して持ち出したことが分かります。

ファイル操作の追跡結果をCSVファイルに出力する

検索したファイル追跡の結果をCSVファイルに出力する方法を説明します。

1. [ファイル追跡結果一覧]にCSVファイルに出力する追跡ログが表示されている状態で、[CSV出力]ボタンをクリックします。
2. ファイルのダウンロード画面が表示されます。[保存]ボタンをクリックします。
3. 保存するフォルダを選択し、ファイル名を入力して、[保存]ボタンをクリックします。

   以下の記号はファイル名として使用できません。
   使用できない記号:「¥」「/」「:」「*」「?」「"」「<」「>」「|」

出力先に同じ名前のファイルが存在していた場合は、上書きするかどうかの選択画面が表示されます。必要に応じてどちらかを選択してください。

出力されるCSVファイルの項目名と説明については、“Systemwalker Desktop Keeper リファレンスマニュアル”の“ファイル追跡結果ログ一覧”を参照してください。

追跡対象ファイルを再設定し、再度ファイル追跡を行う

検索したファイル追跡の結果から、追跡対象ファイルを変更して再度ファイル追跡を行う方法を説明します。

1. [CT操作ログ ー ログ検索 ー ファイル追跡]画面の[ファイル追跡結果一覧]から、再設定するファイル情報をもったログをひとつ選択し、[発生日時]をクリックします。

   「印刷操作ログ」「印刷禁止ログ」は、[ファイル追跡結果一覧]に付帯情報として表示されますが、検索対象として選択することはできません。

2. [追跡対象再設定]ボタンをクリックします。

   →[検索対象ファイル]にファイル名が設定されます。

   複数の添付ファイルのあるメール送信ログを選択した場合は、最初に[追跡対象選択]画面が表示されます。[追跡対象選択]画面で選択したひとつのファイル名が[検索対象ファイル]に設定されます。

3. 検索条件を設定し、[検索]ボタンをクリックします。

   →追跡結果が[ファイル追跡結果一覧]に表示されます。

ファイルのダウンロードが成功しない場合について

CSVファイル、原本保管ファイル、コマンドプロンプトログファイルのダウンロードが成功しない場合、“Systemwalker Desktop Keeper 導入ガイド”の“Webブラウザを使用するPCでの準備”を参照して、Internet Explorer®の設定を変更してください。

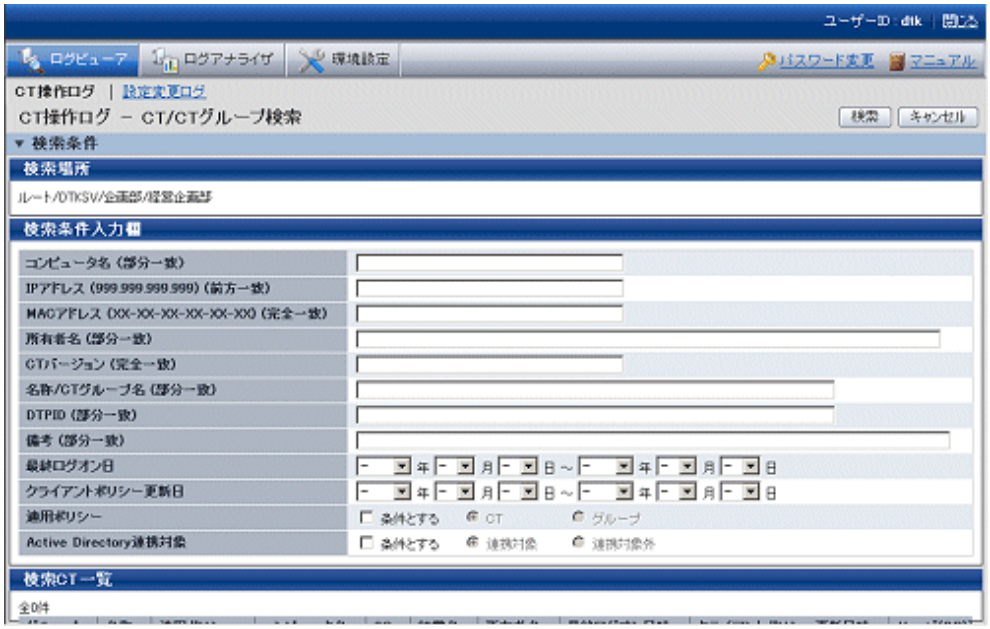
5.4 ログビューアでCT情報を検索する

クライアント(CT)やCTグループを検索する方法について説明します。

[部門選択]域のCTグループツリーに「削除したCT」グループが表示されている場合は、「削除したCT」グループに所属するクライアント(CT)も検索対象です。
「削除したCT」グループのクライアント(CT)は、[検索CT一覧]の[グループ]に「削除したCT」と表示されます。

1. ログビューアを起動します。
2. CTグループツリーから検索の対象とする[ルート]または「CTグループ」を選択します。
3. [CT/CTグループ検索]ボタンをクリックします。

   →[CT/CTグループ検索]画面が表示されます。



4. 以下の情報を、検索条件として入力します。

   検索は、複数の条件をすべて含む「AND検索」です。

   【CTグループを検索する場合】
   [名称/CTグループ名]と[備考]だけを指定します。また、[適用ポリシー]の[条件とする]は未チェックになっている必要があります。

   【クライアント(CT)を検索する場合】
   検索条件の項目を指定します。

項目名	説明
[コンピュータ名]	クライアント(CT)のコンピュータ名により検索が行えます。入力した条件と部分的に一致した結果も表示されます。

項目名	説明
	半角および全角で、15バイト以内で入力します。
[IPアドレス]	クライアント(CT)のIPアドレスにより検索が行えます。入力した条件と前方が一致した結果も表示されます。「10.1」で検索した場合、「10.1.」、「10.1X.」、および「10.1XX.」の結果を表示します。(「X」は数字1文字を表す) 「XXX.XXX.XXX.XXX」の形式で入力します。 【例】140.48.23.12
[MACアドレス]	クライアント(CT)のMACアドレスにより検索が行えます。入力した条件と完全に一致した結果が表示されます。 「XX-XX-XX-XX-XX-XX」の形式で入力します。(「X」は英数字1文字を表す) 【例】02-E0-32-33-A3-C0
[所有者]	クライアント(CT)のOSに設定されている所有者名により検索が行えます。入力した条件と部分的に一致した結果も表示されます。 半角および全角で、93バイト以内で入力します。
[CTバージョン]	インストールされているSystemwalker Desktop Keeperのクライアント(CT)のバージョンにより検索が行えます。入力した条件と完全に一致した結果が表示されます。 「X.X.X.X」の形式で入力します。(「X」は数字1文字以上を表す) 【例】2.1.0.1
[名称/CTグループ名]	CTグループまたはクライアント(CT)に付けられた名称により検索が行えます。入力した条件と部分的に一致した結果も表示されます。 半角および全角で、40バイト以内で入力します。
[DTPID]	Systemwalker Desktop Keeperのクライアント(CT)およびSystemwalker Desktop Patrolのクライアント(CT)が同一のPCにインストールされている場合に表示される、Systemwalker Desktop Patrolのクライアント(CT)の「ユーザーID(+)PC名」を入力します。 部分一致で検索されます。
[備考]	クライアント(CT)のポリシー反映時に入力された備考により検索が行えます。入力した条件と部分的に一致した結果も表示されます。 半角および全角で、128バイト以内で入力します。
[最終ログオン日]	クライアント(CT)は起動時に統合管理サーバまたは管理サーバと通信します。その通信が可能となった時点の日時により検索が行えます。 期間の範囲を指定します。[検索範囲]の開始および終了を指定しないと、すべての期間が検索対象になります。 開始月日を指定しないとその年の年初(1月1日)からの検索になります。 開始日を指定しないとその月の月初(1日)からの検索になります。 終了月日を指定しないとその年の年末(12月31日)までの検索になります。 終了日を指定しないとその月の月末(最終日)までの検索になります。 初期値は、「ー」が表示されます(すべての期間が検索対象です)。 ・ 開始年月日の場合 2009年9月-日:2009年9月1日が指定されたとみなします。 2009年-月-日:2009年1月1日が指定されたとみなします。 -年-月-日:格納されている最初のログから検索します。 2009年-月15日:指定エラー -年9月15日:指定エラー ・ 終了年月日の場合 2009年9月-日:2009年9月30日が指定されたとみなします。 2009年-月-日:2009年12月31日が指定されたとみなします。

項目名		説明
		-年-月-日:格納されている最後のログまでを検索します。 2009年-月15日:指定エラー -年9月15日:指定エラー ※年の指定を省略した場合、月日の指定を省略する必要があります。 月の指定を省略した場合、日の指定を省略する必要があります。
[クライアントポリシー更新日]		クライアント(CT)が統合管理サーバまたは管理サーバから最後にポリシーを取得した日により検索が行えます。 期間の範囲を指定します。[検索範囲]の開始および終了を指定しないと、すべての期間が検索対象になります。 開始月日を指定しないとその年の年初(1月1日)からの検索になります。 開始日を指定しないとその月の月初(1日)からの検索になります。 終了月日を指定しないとその年の年末(12月31日)までの検索になります。 終了日を指定しないとその月の月末(最終日)までの検索になります。 初期値は、「ー」が表示されます(すべての期間が検索対象です)。 ・ 開始年月日の場合 2009年9月-日:2009年9月1日が指定されたとみなします。 2009年-月-日:2009年1月1日が指定されたとみなします。 -年-月-日:格納されている最初のログから検索します。 2009年-月15日:指定エラー -年9月15日:指定エラー ・ 終了年月日の場合 2009年9月-日:2009年9月30日が指定されたとみなします。 2009年-月-日:2009年12月31日が指定されたとみなします。 -年-月-日:格納されている最後のログまでを検索します。 2009年-月15日:指定エラー -年9月15日:指定エラー ※年の指定を省略した場合、月日の指定を省略する必要があります。 月の指定を省略した場合、日の指定を省略する必要があります。
[適用ポリシー]	[条件とする]	チェックをつけた場合、クライアント(CT)に適用されているポリシーを、検索条件に含みます。
	[CT]	検索対象は、CTポリシーが適用されているクライアント(CT)です。
	[グループ]	検索対象は、CTグループポリシーが適用されているクライアント(CT)です。
[Active Directory連携対象]	[条件とする]	チェックをつけた場合、Active Directoryから情報を取り込んだクライアント(CT)かどうかを、検索条件に含みます。
	[連携対象]	検索対象は、Active Directoryから情報を取り込んだクライアント(CT)です。
	[連携対象外]	検索対象は、Active Directoryから情報を取り込んでいないクライアント(CT)です。
[検索]		検索が開始され、結果が表示されます。
[キャンセル]		入力した検索条件が保存されます。

注意

全角文字の入力には注意が必要です

以下の項目については、全角文字を使用した場合、上限を超えるサイズの文字列を入力できますが、検索実行時にエラーとなります。

ー コンピュータ名

ー 所有者

ー 名称/CTグループ名

ー 備考本文(任意)

5. [検索]ボタンをクリックします。

→[検索CT一覧]に検索結果が表示されます。
表示される項目は、[表示項目設定]画面で選択した項目です。[表示項目設定]画面については、“検索CT一覧の表示項目を設定する”を参照してください。
検索されたCTまたはCTグループの[名称]をクリックすると、[ログ検索]画面が表示され、構成情報ツリーの該当するCTグループが選択された状態になっています。

入力した検索条件は、ログオン中は保存されます。ただし、パスワード変更および最新の情報に更新を行った場合は、クリアされます。

第6章 監査資料を作成する

本章では、レポート出力ツールの使用方法について説明します。

6.1 レポート出力ツールの活用方法

注意

レポート出力ツールで作成したレポートに表示されるログ件数と、ログアナライザの目的別集計結果のログ件数は、一致しない場合があります

レポートに表示されるログ件数は、管理サーバからログアナライザサーバへログの移入処理を実施した時点での絞込条件、除外条件で集計した結果です。
このため、集計後に変更された絞込条件/除外条件や、集計後に移入されたログ(※)は反映されていません。

一方、ログアナライザの目的別集計では、リアルタイムに集計します。最新の絞込条件/除外条件で、移入済のログを集計した結果です。

したがって、レポート出力ツールで作成したレポートに表示されるログ件数と、ログアナライザの目的別集計結果のログ件数は、一致しない場合があります。

レポートに、集計後に変更された絞込条件/除外条件で、集計後に移入されたログを含めた集計結果を表示したい場合(最新のデータと条件で集計しなおしたい場合)は、再集計する必要があります。
再集計については、“Systemwalker Desktop Keeper リファレンスマニュアル”の“DTTOOLEX.EXE(ログアナライザサーバへのデータ移入・削除)”を参照してください。

※）集計後にログが移入される場合とは

クライアント(CT)がネットワークに接続されていなかったなどの理由で、管理サーバに操作ログが遅れて転送される場合があります。
そのためログアナライザサーバに移入されるログが遅れて反映される場合があります。

レポートの[グループ名]に対象グループ以外の部門が表示される場合について

対象グループに所属する端末の中に、他部門から移動してきた端末が含まれている場合は、その端末が他部門所属時に採取したログも集計対象となります。

また、これらのログは採取時点でのグループ名で集計されます。

そのため、上記のような端末が存在する場合は、グループ名として対象グループ以外の部門名が表示されることがあります。

PrintScreenキー禁止ログの取り扱いについて

本章で取り扱うPrintScreenキー禁止ログは、区分が「違反」のログのみが対象となります。

印刷量監査レポートに出力される印刷用紙代、CO2排出量について

印刷量監査レポートに出力される印刷用紙代およびCO2排出量は、それぞれ対象期間の総印刷ページ数に1ページあたりの印刷用紙代、CO2排出量を掛けて算出したものです。
そのため目安の値とはなりますが、正確な印刷用紙代、CO2排出量を表したものではありません。

レポート出力ツールとは

レポート出力ツールを利用すると、以下の目的に応じたレポートの作成、印刷およびファイル出力ができます。
レポートはMicrosoft® Excel形式のファイルで出力され、そのまま利用したり、加工して利用したりすることができます。

- システム管理者が、セキュリティ状況や、紙の使用量から換算するCO2排出量の削減状況を把握する
- 組織におけるセキュリティ管理者やコンプライアンス管理組織、および組織上層部に対して、セキュリティリスクの状況、コンプライアンス状況、またはCO2排出量の削減状況などを報告する

生成可能なレポートは以下のとおりです。

レポート種別		概要
情報漏洩分析		
	情報漏洩分析	情報漏洩の危険性という観点で、操作ログを集計・分析した結果を出力します。
	端末利用分析	端末が適切に利用されているかという観点で、操作ログを集計・分析した結果を出力します。
	違反操作分析	禁止されている操作を実施したときに記録されたログを、集計・分析した結果を出力します。
	総合分析	上記3つの観点の診断の要約を出力します。
エコ監査		
	印刷量監査	印刷操作ログを利用して、毎月の印刷量や印刷コストを算出し、CO2排出量に換算します。分析結果を、印刷量、印刷コスト、前月と比較したCO2の削減量として、レポート出力します。また、印刷上限をオーバーした端末の一覧なども出力できます。

使用できる人

レポート出力ツールは、システム管理者と部門管理者が使用できます。ただし、レポート作成時に分析可能なログの範囲は、管理者によって異なります。

管理者の種類	分析可能なログの範囲
システム管理者	当該ユーザーIDが登録されている管理サーバまたは統合管理サーバで閲覧できるすべてのログ
部門管理者	自分が部門管理者として割り当てられている部門配下のすべてのログ

使用できる環境

レポート出力ツールを使用するときは、以下の条件をすべて満たす環境を整えてください。

- レポートを出力するPCに、レポート出力ツールがインストールされている
- レポートを出力するPCに、以下のどれかのMicrosoft® Excelがインストールされている
  - Microsoft® Excel 2002
  - Microsoft® Office Excel 2003
  - Microsoft® Office Excel 2007
  - Microsoft® Office Excel 2010
- レポートを印刷できるように、印刷可能なプリンタが設定されている

レポート出力に要する処理時間に影響を与えるのは、データベースに格納されているログ量と、ログCSVファイルに出力されるログ量です。
データベースに格納されているログ量が約3000万件の場合、およそ、以下の時間がかかります(ただし、処理時間例は参考値です。PCのCPU、メモリ、ディスク性能、他のアプリケーションの動作状況などの要因で変化します)。

- レポートだけを出力する場合:約12秒
- レポートと、1種類のログCSVファイルを出力する場合:約85秒

6.2 レポート出力ツールを起動する

起動手順は以下のとおりです。

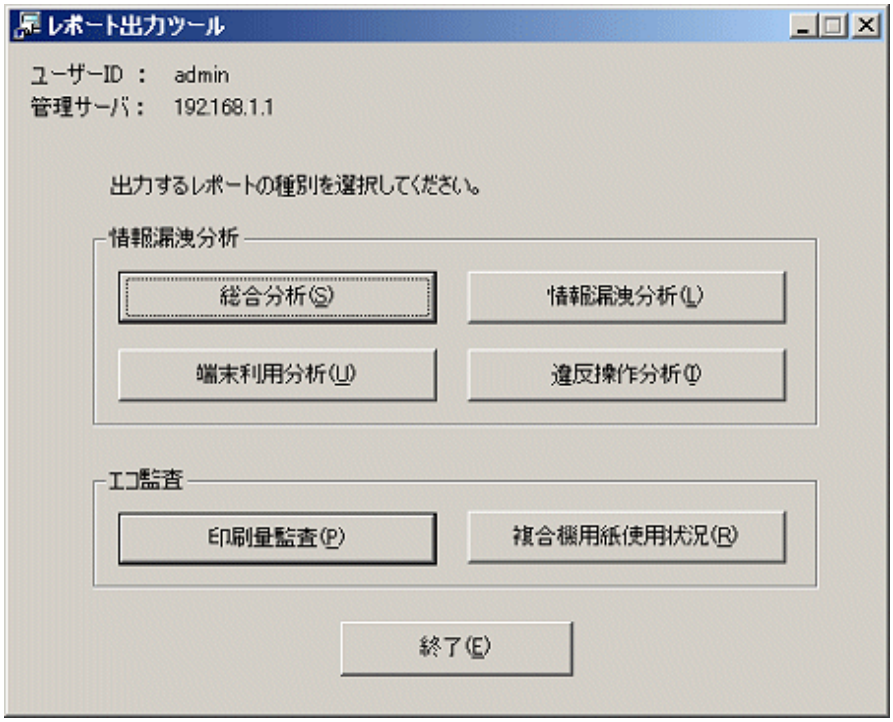
1. Administrator または Domain Admins グループに属するWindowsアカウントで、Windowsにログオンします。
2. スタートメニューから[プログラム]-[Systemwalker Desktop Keeper]-[ログアナライザ]-[レポート出力ツール]を選択します。
   →ログイン画面が表示されます。

項目名	説明
[管理サーバIPアドレス]	統合管理サーバまたは管理サーバのIPアドレスを指定します。 15文字までのIPアドレス形式の文字列を入力します。 一度認証されたIPアドレスは、10件まで記録されます。次回からは、ログイン画面で、プルダウンメニューから選択できます。
[ユーザーID]	システム管理者または部門管理者のユーザーIDです。
[パスワード]	[ユーザーID]に入力したユーザーIDのパスワードを指定します。

認証では、管理サーバからログアナライザサーバに移入された情報を使用しています。管理サーバで変更された認証情報は、ログアナライザサーバにすぐには反映されません(次回、管理情報やログが移入されたタイミングで反映されます)。したがって、変更後の認証情報が管理サーバからログアナライザサーバに移入されるまでは、変更前の認証情報でログインしてください。

3. 必要な情報を入力し、[ログイン]ボタンをクリックします。

   →以下の画面が表示されます。



   ー ユーザーID:ログインしているユーザーIDです。

   ー 管理サーバ:レポート出力するログが格納されている管理サーバのIPアドレスです。

4. 出力するレポートの種別を選択します。

6.3 情報漏洩分析レポート

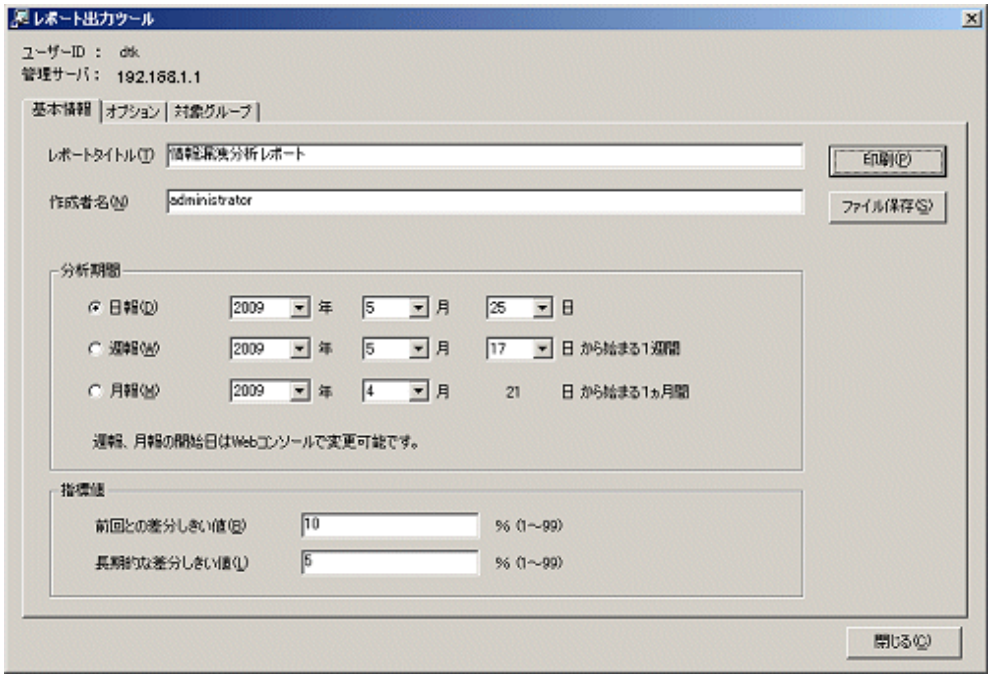
情報漏洩分析レポートは、情報漏洩リスクを評価する観点で、以下のログを集計・分析した結果を出力します。

- ファイル持出しログ
- ファイル操作ログ
- 印刷操作ログ
- 宛先別メール送信ログ

6.3.1 情報漏洩分析レポートを出力する

手順は以下のとおりです。

1. [レポート出力ツール]画面で、[情報漏洩分析]を選択します。
   →以下の画面が表示されます。



   ー ユーザーID:ログインしているユーザーIDです。

   ー 管理サーバ:レポート出力するログが格納されている管理サーバのIPアドレスです。

2. 各タブの項目を設定します。
   各タブの設定内容は、[印刷]または[ファイル保存]を行った場合は、ログインしているユーザー固有の情報として、ログアナライザサーバに保存されます。次回起動時に、保存されている情報が表示されます。

   [基本情報]タブの設定

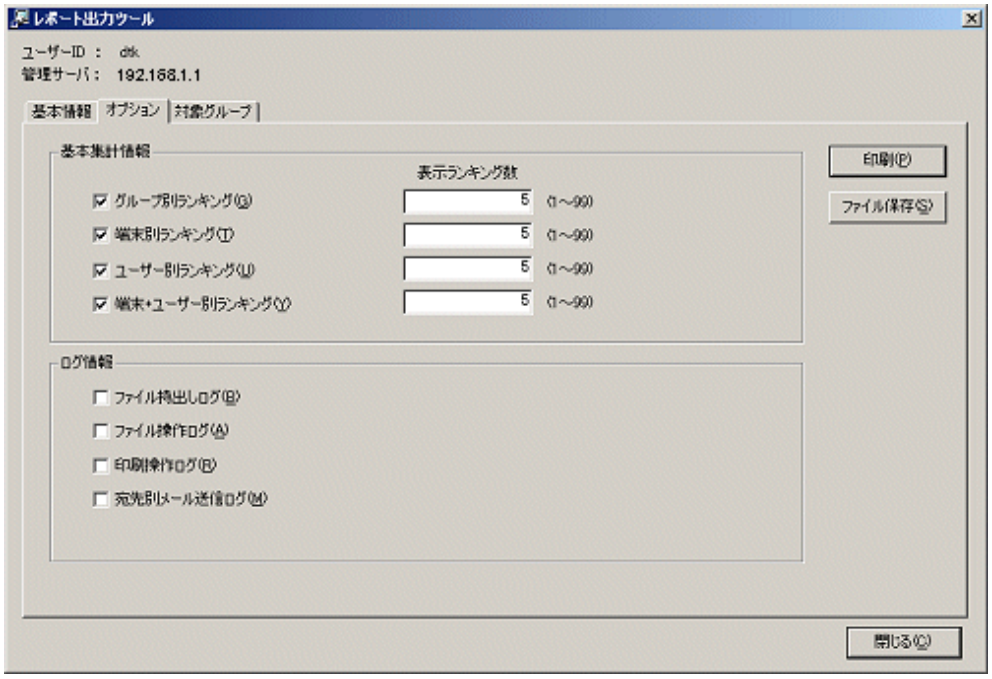
   以下の項目を設定します。

入力項目		内容
[レポートタイトル]		出力するレポートのタイトルを指定します(最大64バイト)。
[作成者名]		レポートの作成者を指定します(最大40バイト)。
[分析期間]	[日報] (初期値)	日報の集計対象を指定します。ログインした日の前日がデフォルトで設定されます。
	[週報]	週報の集計対象となる1週間の開始日を指定します。過去直近の週報期間の開始日がデフォルトで設定されます。 開始日のプルダウンメニューには、Desktop Keeper メインメニューのログアナライザの[動作設定]タブの[週報開始曜日設定]で設定した曜日と対応する日が表示されます。
	[月報]	月報の集計対象となる月度を指定します。過去直近の月報期間の開始日がデフォルトで設定されます。 表示される日付は、Desktop Keeper メインメニューのログアナライザの[動作設定]タブの[月報開始日設定]で設定した値です。
[指標値]	[前回との差分しきい値]	情報漏洩リスクの目安となる指標値が、前回のレポート出力時からどの程度変化した場合に、悪化または改善

入力項目		内容
		と判断するかを“1～99”パーセントの範囲で指定します。 初期値は10パーセントです。
	[長期的な差分しきい値]	情報漏洩リスクの目安となる指標値が、10回前のレポート出力による診断時からどの程度変化した場合に、悪化または改善と判断するかを“1～99”パーセントの範囲で指定します。 初期値は5パーセントです。

[オプション]タブの設定

以下の項目を設定します。



[基本集計情報]

レポートに出力するランキング項目を選択します。
必ず1つ以上の項目を選択してください(デフォルトではすべての項目がチェックされています)。

項目名	説明
[グループ別ランキング]	グループ単位で集計済みの結果を、件数の多い順にワーストランキング表示します。
[端末別ランキング]	端末単位で集計済みの結果を、件数の多い順にワーストランキング表示します。
[ユーザー別ランキング]	ユーザー名単位で集計済みの結果を、件数の多い順にワーストランキング表示します。異なる端末上であっても、ユーザー名で同じあれば同一ユーザーとして扱います。
[端末+ユーザー別ランキング]	端末+ユーザー名の単位で集計済みの結果を、件数の多い順にワーストランキング表示します。ユーザー名が同じでも端末が異なれば、別扱いにします。
[表示ランキング数]	1～99の範囲で入力します(初期値は、“5”です)。 同順位があり、表示するデータ数が設定値を超える場合は、最大30まで表示します。

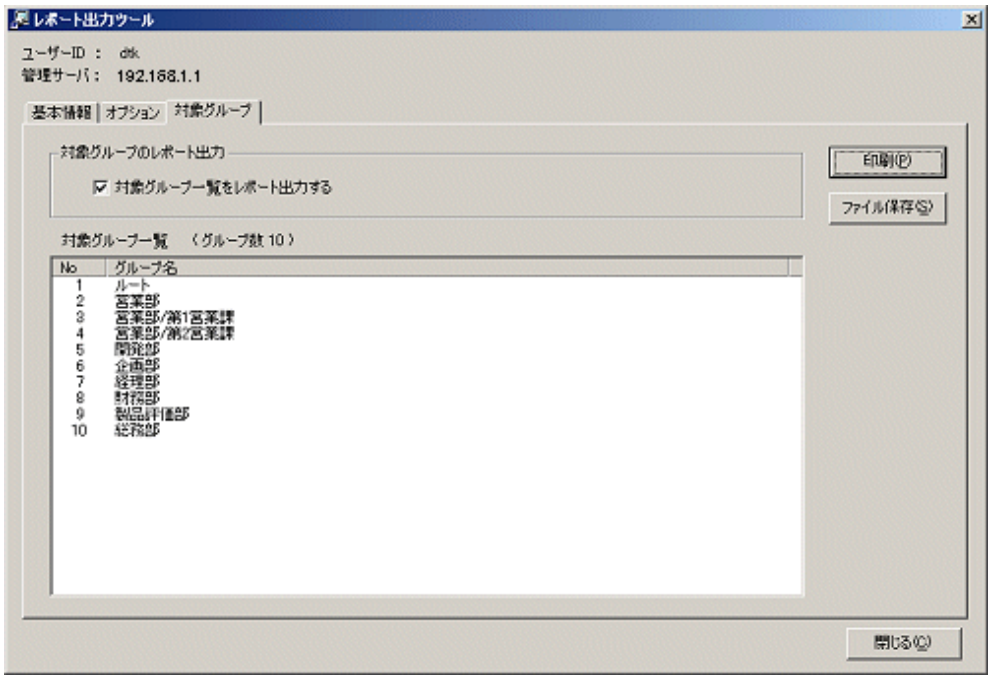
[ログ情報]

ランキングの集計で使用されたログを出力する場合に選択します(デフォルトでは、すべての項目がチェックされていません)。
情報漏洩分析レポートとは別ファイルで、CSV形式で出力されます。

項目名	説明
[ファイル持出しログ]	ファイル持出しログを別ファイルとして出力します。
[ファイル操作ログ]	ファイル操作ログを別ファイルとして出力します。
[印刷操作ログ]	印刷操作ログを別ファイルとして出力します。
[宛先別メール送信ログ]	宛先別メール送信ログを別ファイルとして出力します。

[対象グループ]タブの設定

以下の項目を設定します。



項目名	説明
[対象グループのレポート出力] [対象グループ一覧をレポート出力する]	・ チェックする場合:[対象グループ一覧]をレポートに出力します。 ・ チェックしない場合**(初期値)**:[対象グループ一覧]をレポートに出力しません。
[対象グループ一覧]	ログの分析対象である、部門とその配下の部門すべてが、レポートに出力されます。 部門名は、“/”区切りでルートからのフルパスで表示されます。 【例】開発部/第三開発課 タイトルの横には対象部門の総数が表示されます。

3. [印刷]または[ファイル保存]ボタンをクリックします。

注意

レポート出力中は、Microsoft® Excelを操作しないでください

レポート出力中は、Microsoft® Excelファイルの[新規作成]や[開く]操作を行わないでください。レポート出力が正常に行われない場合があります。

また、レポート出力前に、Microsoft® Excelが正しく起動することを確認してください。Microsoft® Excelが正しく起動しない場合は、レポート出力処理が長時間たっても終了しないなど、不具合が発生するときがあります。

【[印刷]ボタンをクリックした場合】

生成したレポートや、ランキングの集計で使用されたログを、印刷します。

[印刷]画面が表示されますので、プリンタへの印刷設定を行い、レポートを印刷します。

ポイント

印刷ダイアログがレポート出力ツールの後ろに隠れている場合があります。

長時間たっても印刷ダイアログが表示されない場合は、印刷ダイアログがレポート出力ツールの後ろに隠れている可能性があります。

【[ファイル保存]ボタンをクリックした場合】

生成したレポートや、ランキングの集計で使用されたログを、ファイルに保存します。

注意

出力したレポートは、安全なところに保存してください

出力したレポートには、個人情報やシステム構成情報が含まれる場合があります。ファイルの保存先は、十分なセキュリティ対策が施されたフォルダを指定してください。
【例】
フォルダのアクセス権を、管理者以外のユーザーが参照できないように設定する

保存画面が表示されますので、保存先を指定して、[保存]ボタンをクリックします。

各ファイルは、以下の名称で保存されます。

【レポートファイル】
デフォルト名:Leak_[分析期間]_[分析期間開始年月日].xls
(同名ファイルが存在する場合は、上書き確認ダイアログが表示されます。)

- 分析期間
  日報:daily
  週報:weekly
  月報:monthly

- 分析期間開始年月日:YYYYMMDD([基本情報]タブの[分析期間]で設定した日付)

【ログのCSVファイル】

ログ種別	CSVファイル名
ファイル持出し	Leak_Log_Filebringout_YYYYMMDD.csv
ファイル操作	Leak_Log_Fileaccess_YYYYMMDD.csv
印刷操作	Leak_Log_Print_YYYYMMDD.csv
宛先別メール送信	Leak_Log_Mailsend_YYYYMMDD.csv

同名ファイルが存在する場合は、ファイル名の末尾に()付きの数字が添付されます。
例:Leak_Log_Filebringout_YYYYMMDD(2).csv
以降(3),(4)と続きます。

注意

UNICODE文字はInternet Explorer®で確認してください

ログデータにSJISに対応する字形を持たないUNICODE文字(JIS2004を含みます)が使用されていた場合、CSVファイルではHTMLエスケープ形式で表示されます。
JIS2004を含むUNICODE文字の字形は、Internet Explorer®で以下のHTMLファイルを開いて確認してください。

・ファイルの場所:レポートファイルの保存先フォルダ配下のHTMLフォルダ

・ファイル名:CSVファイルと同名(拡張子は".html")

このHTMLファイルには、CSVファイルに出力されているログデータと同じ内容が表示されます。

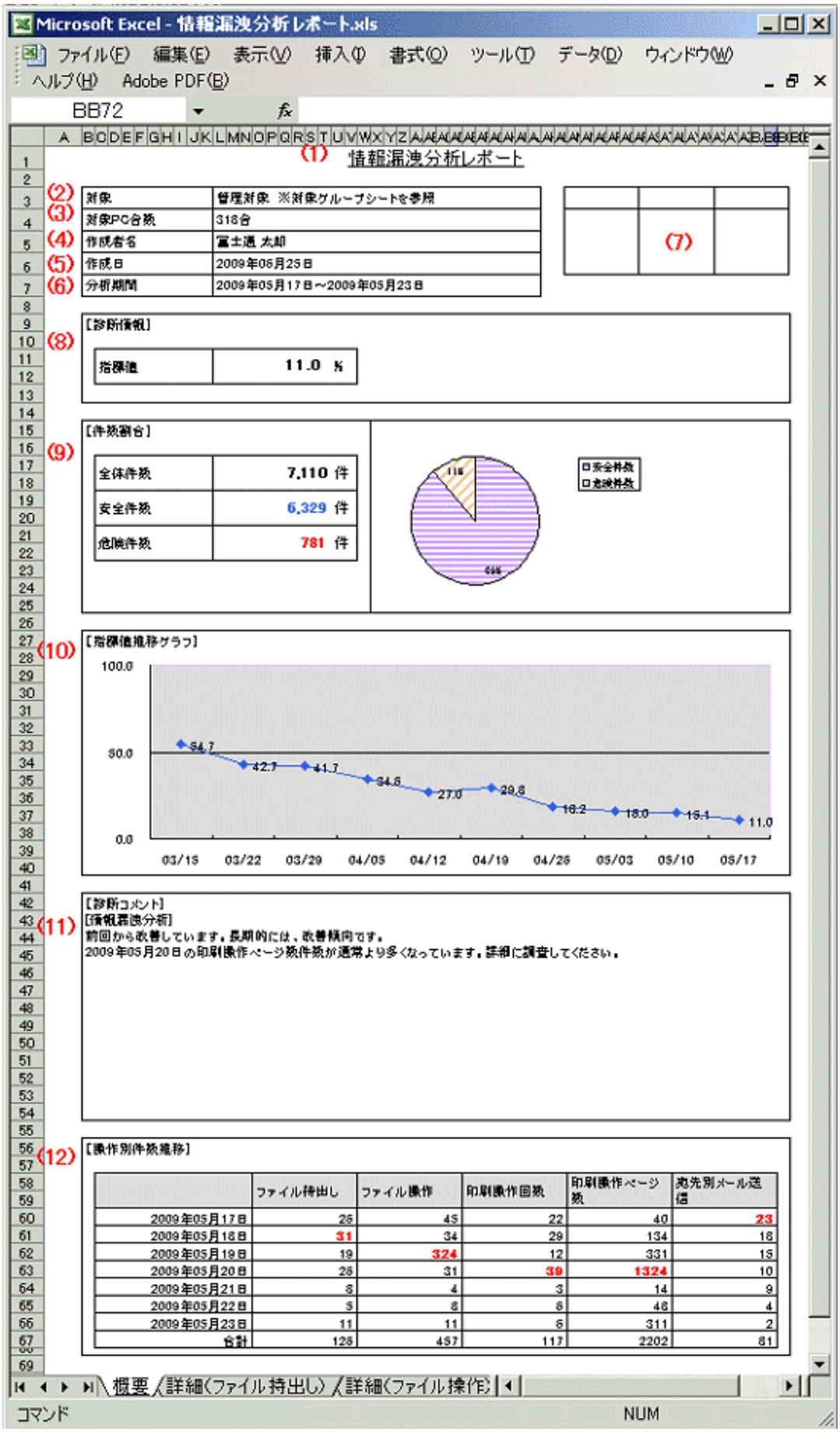
6.3.2 情報漏洩分析レポートの内容

情報漏洩分析レポートの構成は以下のとおりです。

分類	シート名	説明
概要シート	概要	生成されたレポートの概要が記述されます。
詳細シート	詳細(ファイル持出し)	操作ログごとに各種集計情報(ランキング情報)が記述されます。
	詳細(ファイル操作)	
	詳細(印刷操作回数)	
	詳細(印刷操作ページ数)	
	詳細(宛先別メール送信)	
対象グループシート	対象グループ	分析対象のログが採取された部門の一覧が記述されます。

生成したレポートファイルや印刷結果のレイアウトは、使用しているMicrosoft® Excelのバージョンやサービスパックによって異なる場合があります。

概要シート



	ファイル持出し	ファイル操作	印刷操作回数	印刷操作ページ数	宛先別メール送信
2009年05月17日	25	45	22	40	23
2009年05月18日	31	34	29	134	18
2009年05月19日	19	324	12	331	15
2009年05月20日	26	31	39	1324	10
2009年05月21日	8	4	3	14	9
2009年05月22日	5	6	6	48	4
2009年05月23日	11	11	6	311	2
合計	125	457	117	2202	81

(1)レポートタイトル

基本情報設定で指定したタイトルが記述されます。

(2)対象

管理の対象を表示します。常に「管理対象」と表示します。

(3)対象PC台数

管理対象の全PC台数を表示します。

・ 対象PCがない場合は0台と表示します。

(4)作成者名

基本情報設定で指定した作成者名が記述されます。

(5)作成日

レポート出力を行った日付が記述されます。

(6)分析期間

基本情報設定で指定した、分析期間を記述します。

(7)承認印欄

報告レポートとして使用する場合の承認欄です(欄の数は変更できません)。

(8)診断情報:指標値

全体の操作件数のうち危険操作件数(“(9) 件数割合”の“危険件数”を参照)が占める割合をパーセンテージで示します。

(9)件数割合

・ 全体件数

以下のように分析内容により異なります。

【情報漏洩分析】
ファイル持出し件数(リムーバブルまたはCD/DVDに持ち出した件数) ＋ ファイル操作件数(リムーバブルまたはCD/DVDにファイルを複写・移動した、あるいは、リムーバブルまたはCD/DVDでファイルを作成・参照した件数) ＋ 印刷操作件数 ＋ 宛先別メール送信件数(絞込条件のドメインに合致しなかった宛先別メール送信件数)

【端末利用分析】
URL付きウィンドウタイトル取得件数 ＋宛先別メール送信件数 ＋ アプリケーション起動件数

【違反操作】
情報漏洩の全体件数 ＋ 端末利用の全体件数 ＋ 違反操作の危険件数

・ 安全件数

全体件数から危険件数を除いた操作件数の合計数

・ 危険件数

以下のように分析内容により異なります。

【情報漏洩分析】
全体件数のうち絞込条件(キーワード)に合致した件数

【端末利用分析】
絞込条件(URL)に合致しなかったURL付きウィンドウタイトル取得件数 ＋ 絞込条件(ドメイン)に合致しなかった宛先別メール送信件数 ＋ 絞込条件(アプリケーション)に合致しなかったアプリケーション起動件数

【違反操作分析】
アプリケーション起動禁止件数 ＋ 印刷禁止件数 ＋ ログオン禁止件数 ＋ PrintScreenキー禁止件数 ＋ メール添付禁止件数

・ 円グラフ

安全件数と危険件数の割合を円グラフで示します。
全体件数が0件の場合、円グラフは表示されません(円グラフの表示場所に“1%”と表示されます)。

(10)指標値推移グラフ

指標値の推移(過去直近10回分)を折れ線グラフで表示します。
グラフの縦軸は指標値の値です。下端を危険率0、上端を危険率100とします。従って指標値が0に近づくほど望ましい状態と言えます。
横軸に各分析期間の開始日を表示します。横軸で、データのない分析期間は、指標値は100となります。

(11)診断コメント

- 前回との比較からの考察

  分析結果の指標値に対して、前回の診断時の指標値との差分により、危険度が増加したか低下したかで、リスク状況の判定を行いコメントを記述します。

- 長期的な傾向について

  過去の分析結果の指標値の推移から予測される指標値に対して、今回の指標値が増加しているか低減しているかで、リスク状況の判定を行いコメントを記述します。

- 要注意日／操作についての考察

  期間内において最もリスクが高く、調査が必要な状況にある日および操作を提示します。(月報、週報選択時のみ)

(12)操作別件数推移

分析期間で設定した日数分の、各操作件数の推移を、表形式で表示します。
月報の場合は1カ月分、週報の場合は7日分、日報の場合は一日分提示します。
なお、各操作ログ毎に、期間内の最大件数を赤文字で表示します。

詳細シート

詳細シートに出力される情報について、“詳細(ファイル持出し)シート”を例に説明します。
ファイルアクセスなどの他の操作も、同様の形式で出力されます。

ランキング表の各項目の内容は、最大512バイトまで表示されます。

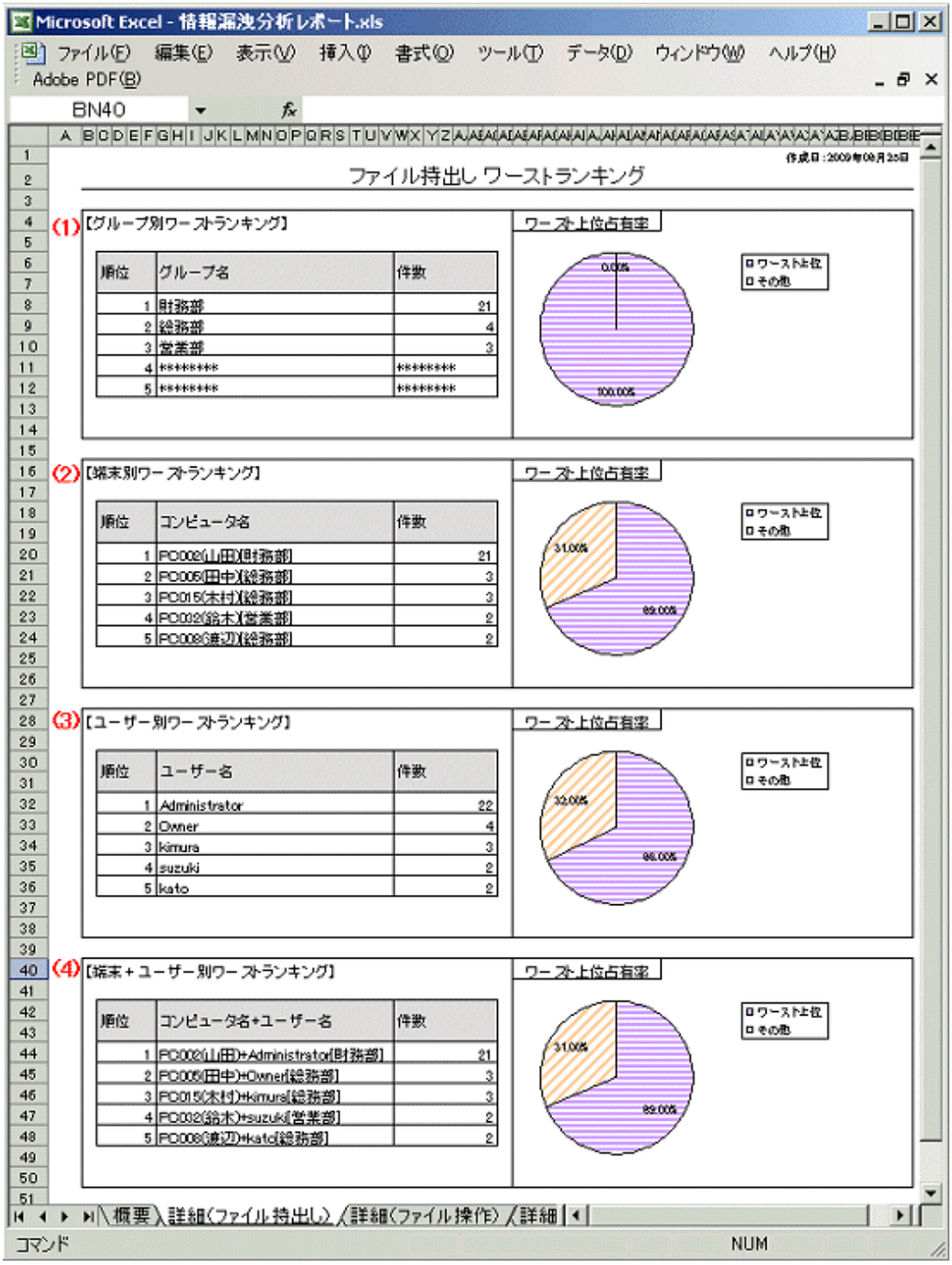
ポイント

UNICODE文字はInternet Explorer®で確認してください

ログデータやユーザー名などにSJISに対応する字形を持たないUNICODE文字(JIS2004を含みます)が使用されていた場合、レポートではHTMLエスケープ形式で表示されます。
JIS2004を含むUNICODE文字の字形は、Internet Explorer®で以下のHTMLファイルを開いて確認してください。

- ファイルの場所:レポートファイルの保存先フォルダ配下のHTMLフォルダ
- ファイル名:レポートファイルと同名(拡張子は“.html”)

このHTMLファイルには、詳細シートに表示されているランキング情報と同じ内容が表示されます(Microsoft® Excel形式ではログ種別ごとに別シートですが、HTMLでは1つのファイルにまとめられています)。
ただし、JIS2004を含むUNICODE文字に対応したフォント環境以外では、正しく表示されません。



同順位があり、表示するデータ数が表示ランキング数の設定値を超える場合は、最大30まで表示します。

(1)グループ別ワーストランキング

グループ単位での集計結果を、件数の多い順にランキング表示します。また、ランキング上位のグループの操作件数が全体のどれくらいの割合を占めるか、ワースト上位占有率グラフで示します。

(2)端末別ワーストランキング(注)

端末単位での集計結果を、件数の多い順にランキング表示し、あわせてグラフでも表示し、ワースト上位の端末での操作件数が全体のどれくらいの割合を占めるか、ワースト上位占有率グラフで示します。

(3)ユーザー別ワーストランキング

ユーザー単位での集計結果を、件数の多い順にランキング表示し、あわせてグラフでも表示し、ワースト上位のユーザーの操作件数が全体のどれくらいの割合を占めるか、ワースト上位占有率グラフで示します。

(4)端末+ユーザー別ワーストランキング(注)

端末かつユーザー単位での集計結果を、件数の多い順にランキング表示し、あわせてグラフでも表示し、ワースト上位のユーザーの該当端末での操作件数が全体のどれくらいの割合を占めるか、ワースト上位占有率グラフで示します。

注) ランキング項目の“コンピュータ名”と“コンピュータ名+ユーザー名”は、以下の形式で表示されます。

- 管理コンソールのCTリストに表示される[名称]と[コンピュータ名]が同じ場合

  [名称]と[コンピュータ名]が同じになる条件は、以下のどちらかです。

  ー CTインストール後、[名称]を更新していないため、初期値として[コンピュータ名]が表示されている

  ー 管理コンソールで、[名称]を[コンピュータ名]と同名に更新した

  このとき、端末別ランキングには、“コンピュータ名[グループ名]”の形式で表示されます。
  【例】PC001[人事部]

  端末+ユーザー別ランキングには、“コンピュータ名+ユーザー名[グループ名]”の形式で表示されます。
  【例】PC001+Administrator[人事部]

- 管理コンソールのCTリストに表示される[名称]と[コンピュータ名]が異なる場合

  [名称]と[コンピュータ名]が異なる条件は、以下です。

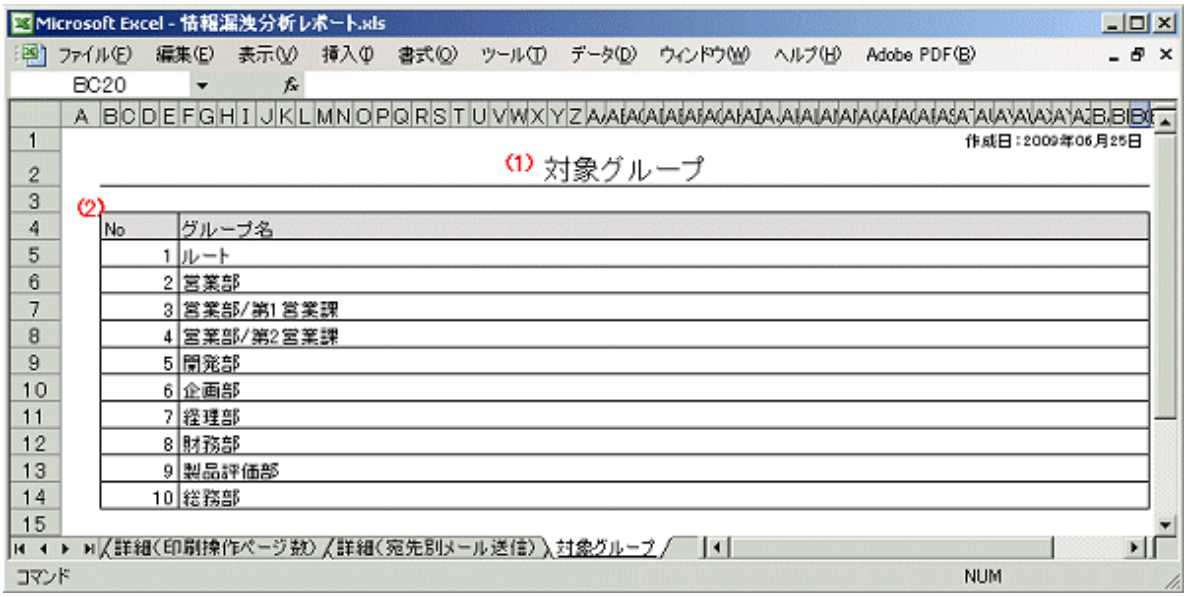
  ー 管理コンソールで、[名称]を[コンピュータ名]とは別名に更新した

  このとき、端末別ランキングには、“コンピュータ名(名称)[グループ名]”の形式で表示されます。
  【例】BLONO(富士通太郎) [人事部]

  端末+ユーザー別ランキングには、“コンピュータ名(名称)+ユーザー名[グループ名]”の形式で表示されます。
  【例】BLONO(富士通太郎)+Administrator[人事部]

対象グループシート

分析を行った部門情報が出力されます。



(1)レポートタイトル

“対象グループ”と記述されます。

(2) 対象グループ一覧

分析対象の部門が記述されます。
グループ名は、ルートからのフルパスで記述されます。
【例】開発部/第三開発課

複数の管理部門が存在する場合は、行を追加して表示されます。
記述される最大部門数は、50000部門です。

対象グループシートの各項目の内容は、最大512バイトまで表示されます。

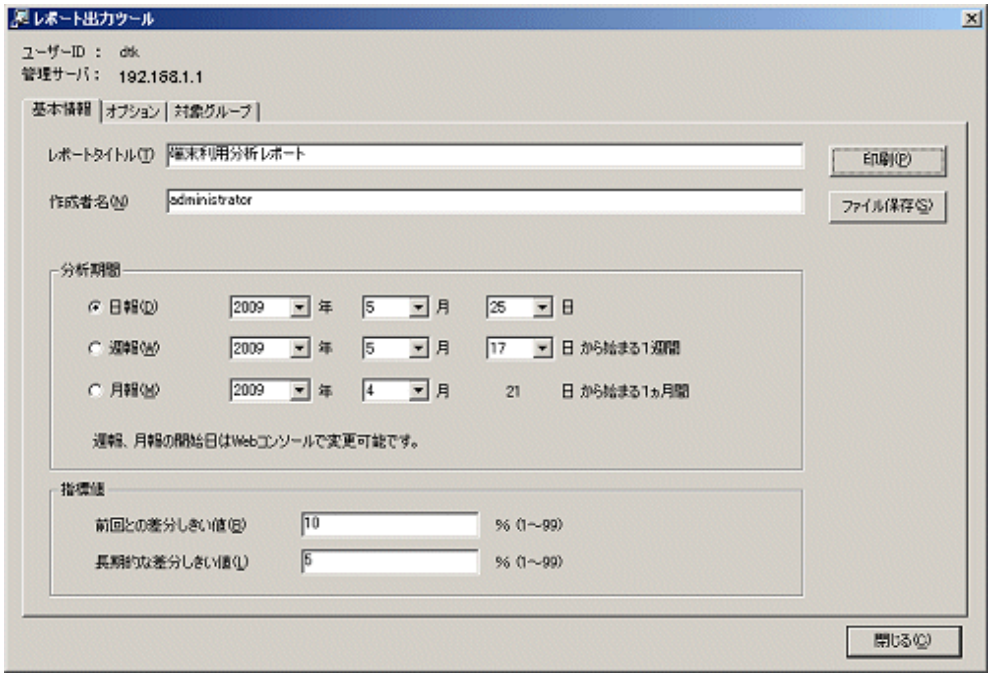
6.4 端末利用分析レポート

端末利用分析レポートは、組織のポリシーに沿ってPCが適切に利用されているかという観点で、以下のログを集計・分析した結果を出力します。

- URL付きウィンドウタイトル取得ログ
- 宛先別メール送信ログ
- アプリケーション起動ログ

6.4.1 端末利用分析レポートを出力する

1. [レポート出力ツール]画面で、[端末利用分析]を選択します。
   →以下の画面が表示されます。

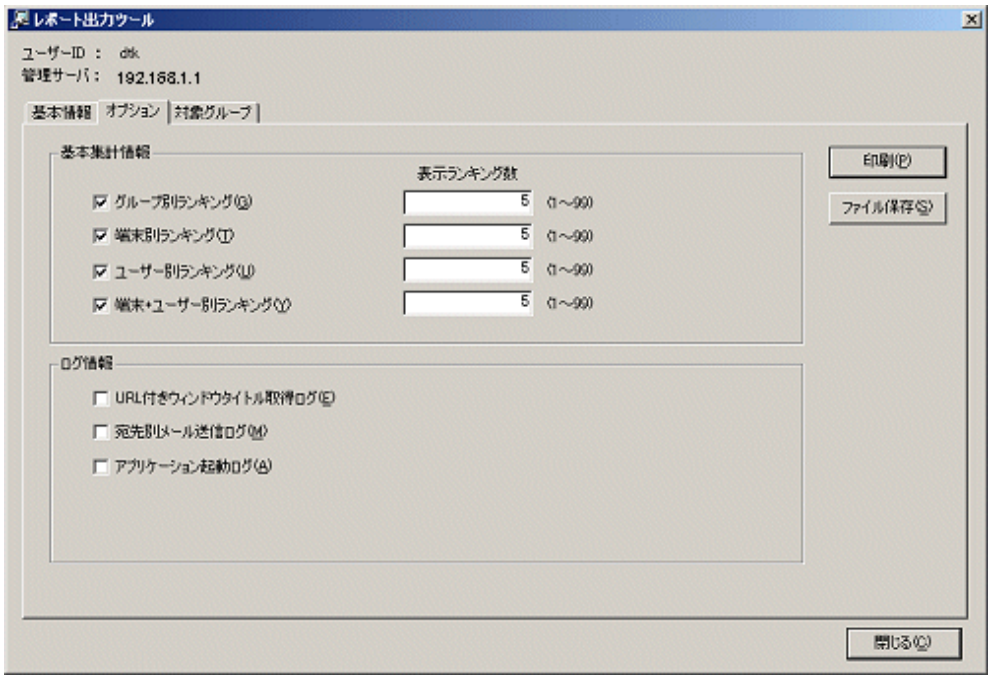


2. 各タブの項目を設定します。
   各タブの設定内容は、[印刷]または[ファイル保存]を行った場合は、ログインしているユーザー固有の情報として、ログアナライザサーバに保存されます。次回起動時に、保存されている情報が表示されます。

   [基本情報]タブの設定

   基本情報タブの設定は、情報漏洩分析レポートの出力時と共通です。“[基本情報]タブの設定”を参照してください。

[オプション]タブの設定



[基本集計情報]

基本集計情報の設定は、情報漏洩分析レポートの出力時と共通です。“[オプション]タブの設定”を参照してください。

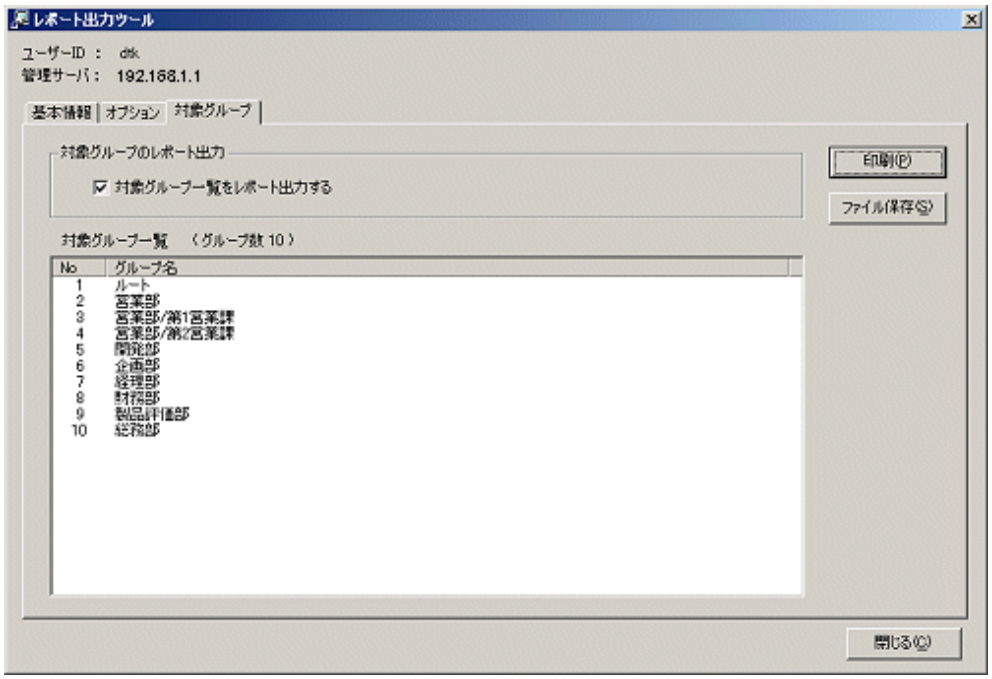
[ログ情報]

ランキングの集計で使用されたログを出力する場合に選択します。
端末利用分析レポートとは別ファイルで、CSV形式で出力されます。

項目名	説明
[URL付きウィンドウタイトル取得ログ]	URL付きウィンドウタイトル取得ログを別ファイルとして出力します。
[宛先別メール送信ログ]	宛先別メール送信ログを別ファイルとして出力します。
[アプリケーション起動ログ]	アプリケーション起動ログを別ファイルとして出力します。

[対象グループ]タブの設定

[対象グループ一覧]をレポートに出力するかどうかを設定をします。
設定は、情報漏洩分析レポートの出力時と共通です。“[対象グループ]タブの設定”を参照してください。



3. [印刷]または[ファイル保存]ボタンをクリックします。

注意

レポート出力中は、Microsoft® Excelを操作しないでください

レポート出力中は、Microsoft® Excelファイルの[新規作成]や[開く]操作を行わないでください。レポート出力が正常に行われない場合があります。

また、レポート出力前に、Microsoft® Excelが正しく起動することを確認してください。Microsoft® Excelが正しく起動しない場合は、レポート出力処理が長時間たっても終了しないなど、不具合が発生するときがあります。

【[印刷]ボタンをクリックした場合】

生成したレポートや、ランキングの集計で使用されたログを、印刷します。

[印刷]画面が表示されますので、プリンタへの印刷設定を行い、レポートを印刷します。

ポイント

印刷ダイアログがレポート出力ツールの後ろに隠れている場合があります。

長時間たっても印刷ダイアログが表示されない場合は、印刷ダイアログがレポート出力ツールの後ろに隠れている可能性があります。

【[ファイル保存]ボタンをクリックした場合】

生成したレポートや、ランキングの集計で使用されたログを、ファイルに保存します。

注意

出力したレポートは、安全なところに保存してください

出力したレポートには、個人情報やシステム構成情報が含まれる場合があります。ファイルの保存先は、十分なセキュリティ対策が施されたフォルダを指定してください。

【例】
フォルダのアクセス権を、管理者以外のユーザーが参照できないように設定する

保存画面が表示されますので、保存先を指定して、[保存]ボタンをクリックします。

各ファイルは、以下の名称で保存されます。

【レポートファイル】
デフォルト名：Cmuse_[分析期間]_[分析期間開始年月日].xls
(同名ファイルが存在する場合は、上書き確認ダイアログが表示されます。)

－ 分析期間
　日報：daily
　週報：weekly
　月報：monthly

－ 分析期間開始年月日：YYYYMMDD([基本情報]タブの[分析期間]で設定した日付)

【ログのCSVファイル】

ログ種別	CSVファイル名
URL付きウィンドウタイトル取得	Cmuse_Log_Webaccess_YYYYMMDD.csv
宛先別メール送信	Cmuse_Log_Mailsend_YYYYMMDD.csv
アプリケーション起動	Cmuse_Log_AppStartup_YYYYMMDD.csv

同名ファイルが存在する場合は、ファイル名の末尾に()付きの数字が添付されます。
例：Cmuse_Log_Webaccess_YYYYMMDD(2).csv
以降(3),(4)と続きます。

注意

UNICODE文字はInternet Explorer®で確認してください

ログデータにSJISに対応する字形を持たないUNICODE文字(JIS2004を含みます)が使用されていた場合、CSVファイルではHTMLエスケープ形式で表示されます。
JIS2004を含むUNICODE文字の字形は、Internet Explorer®で以下のHTMLファイルを開いて確認してください。

・ファイルの場所：レポートファイルの保存先フォルダ配下のHTMLフォルダ

・ファイル名：CSVファイルと同名(拡張子は".html")

このHTMLファイルには、CSVファイルに出力されているログデータと同じ内容が表示されます。

6.4.2 端末利用分析レポートの内容

端末利用分析レポートの構成は以下のとおりです。

分類	シート名	説明
概要シート	概要	生成されたレポートの概要が記述されます。
詳細シート	詳細(URL付きウィンドウタイトル取得)	操作ログ毎に各種集計情報(ランキング情報)が記述されます。
	詳細(宛先別メール送信)	
	詳細(アプリケーション起動)	

分類	シート名	説明
対象グループシート	対象グループ	分析対象のログが採取された部門の一覧が記述されます。

生成したレポートファイルや印刷結果のレイアウトは、使用しているMicrosoft® Excelのバージョンやサービスパックによって異なる場合があります。

レポートの出力形式は、情報漏洩分析レポートと同じです。
ただし、詳細シートに出力されるランキングの集計対象となるログは、URL付きウィンドウタイトル取得ログ、宛先別メール送信ログ、アプリケーション起動ログです。
出力形式は、“概要シート”、“詳細シート”、“対象グループシート”を参照してください。

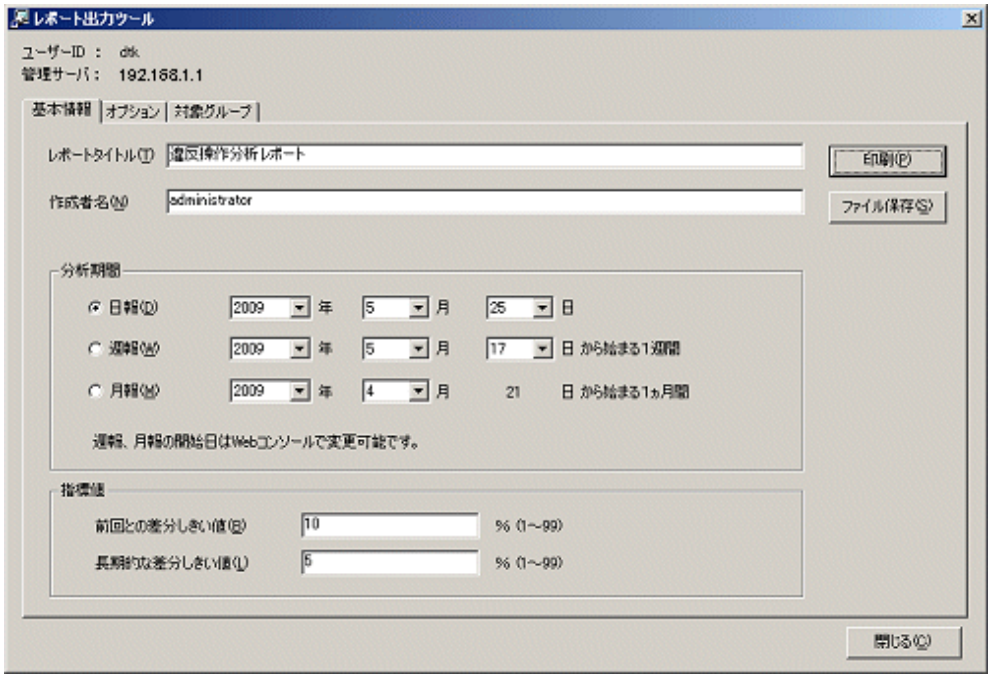
6.5 違反操作分析レポート

違反操作分析レポートでは、組織のポリシーに則り、Systemwalker Desktop Keeper で禁止されている操作を行った場合に採取される下記の禁止ログを、違反操作状況を把握する観点で、集計・分析した結果を出力します。

- アプリケーション起動禁止
- 印刷禁止
- ログオン禁止
- PrintScreenキー禁止
- メール添付禁止

6.5.1 違反操作分析レポートを出力する

1. [レポート出力ツール]画面で、[違反操作分析]を選択します。
   →以下の画面が表示されます。

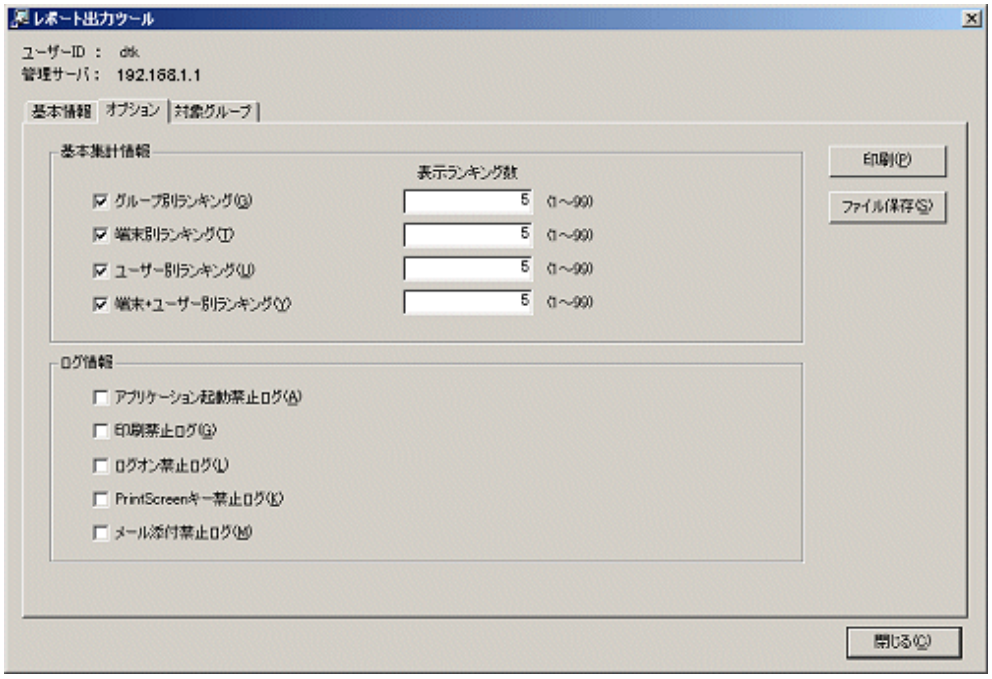


2. 各タブの項目を設定します。
各タブの設定内容は、[印刷]または[ファイル保存]を行った場合は、ログインしているユーザー固有の情報として、ログアナライザサーバに保存されます。次回起動時に、保存されている情報が表示されます。

[基本情報]タブの設定

基本情報タブの設定は、情報漏洩分析レポートの出力時と共通です。“[基本情報]タブの設定”を参照してください。

[オプション]タブの設定



[基本集計情報]

基本集計情報の設定は、情報漏洩分析レポートの出力時と共通です。“[オプション]タブの設定”を参照してください。

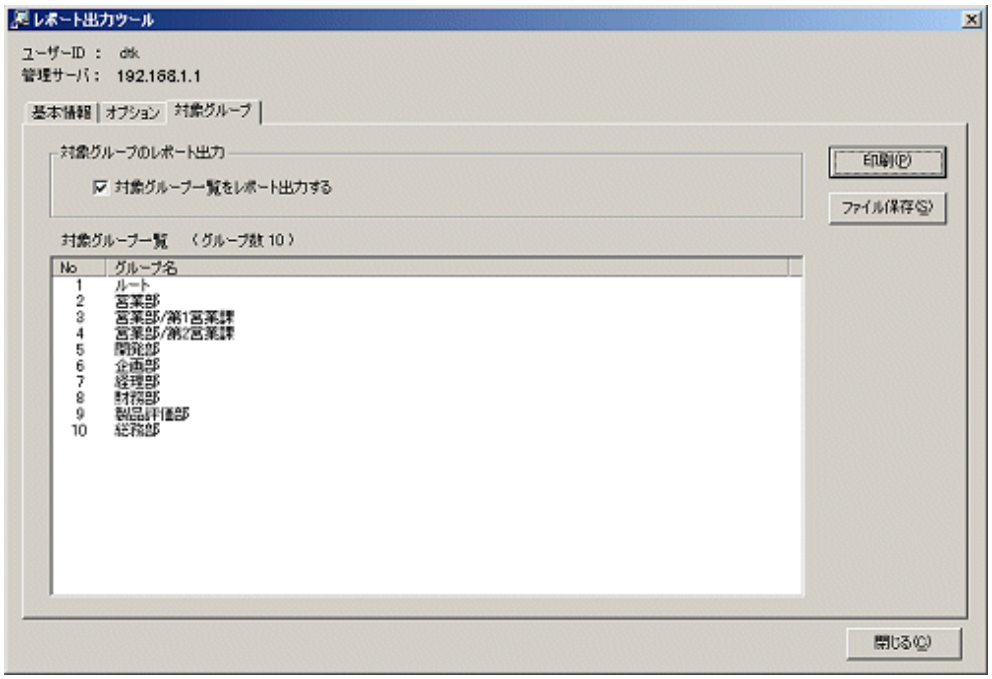
[ログ情報]

ランキングの集計で使用されたログを出力する場合に選択します。
違反操作分析レポートとは別ファイルで、CSV形式で出力されます。

項目名	説明
[アプリケーション起動禁止ログ]	アプリケーション起動禁止ログを別ファイルとして出力します。
[印刷禁止ログ]	印刷禁止ログを別ファイルとして出力します。
[ログオン禁止ログ]	禁止ログを別ファイルとして出力します。
[PrintScreenキー禁止ログ]	PrintScreenキー禁止ログを別ファイルとして出力します。
[メール添付禁止ログ]	メール添付禁止ログを別ファイルとして出力します。

[対象グループ]タブの設定

[対象グループ一覧]をレポートに出力するかどうかを設定をします。
設定は、情報漏洩分析レポートの出力時と共通です。“[対象グループ]タブの設定”を参照してください。



3. [印刷]または[ファイル保存]ボタンをクリックします。

注意

レポート出力中は、Microsoft® Excelを操作しないでください

レポート出力中は、Microsoft® Excelファイルの[新規作成]や[開く]操作を行わないでください。レポート出力が正常に行われない場合があります。

また、レポート出力前に、Microsoft® Excelが正しく起動することを確認してください。Microsoft® Excelが正しく起動しない場合は、レポート出力処理が長時間たっても終了しないなど、不具合が発生するときがあります。

【[印刷]ボタンをクリックした場合】

生成したレポートや、ランキングの集計で使用されたログを、印刷します。

[印刷]画面が表示されますので、プリンタへの印刷設定を行い、レポートを印刷します。

ポイント

印刷ダイアログがレポート出力ツールの後ろに隠れている場合があります。

長時間たっても印刷ダイアログが表示されない場合は、印刷ダイアログがレポート出力ツールの後ろに隠れている可能性があります。

【[ファイル保存]ボタンをクリックした場合】

生成したレポートや、ランキングの集計で使用されたログを、ファイルに保存します。

注意

出力したレポートは、安全なところに保存してください

出力したレポートには、個人情報やシステム構成情報が含まれる場合があります。ファイルの保存先は、十分なセキュリティ対策が施されたフォルダを指定してください。

【例】
フォルダのアクセス権を、管理者以外のユーザーが参照できないように設定する

保存画面が表示されますので、保存先を指定して、[保存]ボタンをクリックします。

各ファイルは、以下の名称で保存されます。

【レポートファイル】
デフォルト名：Islegal_[分析期間]_[分析期間開始年月日].xls
(同名ファイルが存在する場合は、上書き確認ダイアログが表示されます。)

－ 分析期間
　日報：daily
　週報：weekly
　月報：monthly

－ 分析期間開始年月日：YYYYMMDD([基本情報]タブの[分析期間]で設定した日付)

【ログのCSVファイル】

ログ種別	CSVファイル名
アプリケーション起動禁止	Islegal_Log_AppSuppress_YYYYMMDD.csv
印刷禁止	Islegal_Log_PrintSuppress_YYYYMMDD.csv
ログオン禁止	Islegal_Log_LogonSuppress_YYYYMMDD.csv
PrintScreenキー禁止	Islegal_Log_PSKeySuppress_YYYYMMDD.csv
メール添付禁止	Islegal_Log_MailattachedSuppress_YYYYMMDD.csv

同名ファイルが存在する場合は、ファイル名の末尾に()付きの数字が添付されます。
例：Islegal_Log_AppSuppress_YYYYMMDD(2).csv
以降(3),(4)と続きます。

注意

UNICODE文字はInternet Explorer®で確認してください

ログデータにSJISに対応する字形を持たないUNICODE文字(JIS2004を含みます)が使用されていた場合、CSVファイルではHTMLエスケープ形式で表示されます。
JIS2004を含むUNICODE文字の字形は、Internet Explorer®で以下のHTMLファイルを開いて確認してください。

・ファイルの場所：レポートファイルの保存先フォルダ配下のHTMLフォルダ

・ファイル名：CSVファイルと同名(拡張子は".html")

このHTMLファイルには、CSVファイルに出力されているログデータと同じ内容が表示されます。

6.5.2 違反操作分析レポートの内容

違反操作分析レポートの構成は以下のとおりです。

分類	シート名	説明
概要シート	概要	生成されたレポートの概要が記述されます。
詳細シート	詳細(アプリケーション起動禁止ログ)	操作ログ毎に各種集計情報(ランキング情報)が記述されます。
	詳細(印刷禁止ログ)	
	詳細(ログオン禁止ログ)	

分類	シート名	説明
	詳細(PrintScreenキー禁止ログ)	
	詳細(メール添付禁止ログ)	
対象グループシート	対象グループ	分析対象のログが採取された部門の一覧が記述されます。

生成したレポートファイルや印刷結果のレイアウトは、使用しているMicrosoft® Excelのバージョンやサービスパックによって異なる場合があります。

レポートの出力形式は、情報漏洩分析レポートと同じです。
ただし、詳細シートに出力されるランキングの集計対象となるログは、以下のとおりです。

- アプリケーション起動禁止ログ
- 印刷禁止ログ
- ログオン禁止ログ
- PrintScreenキー禁止ログ
- メール添付禁止ログ

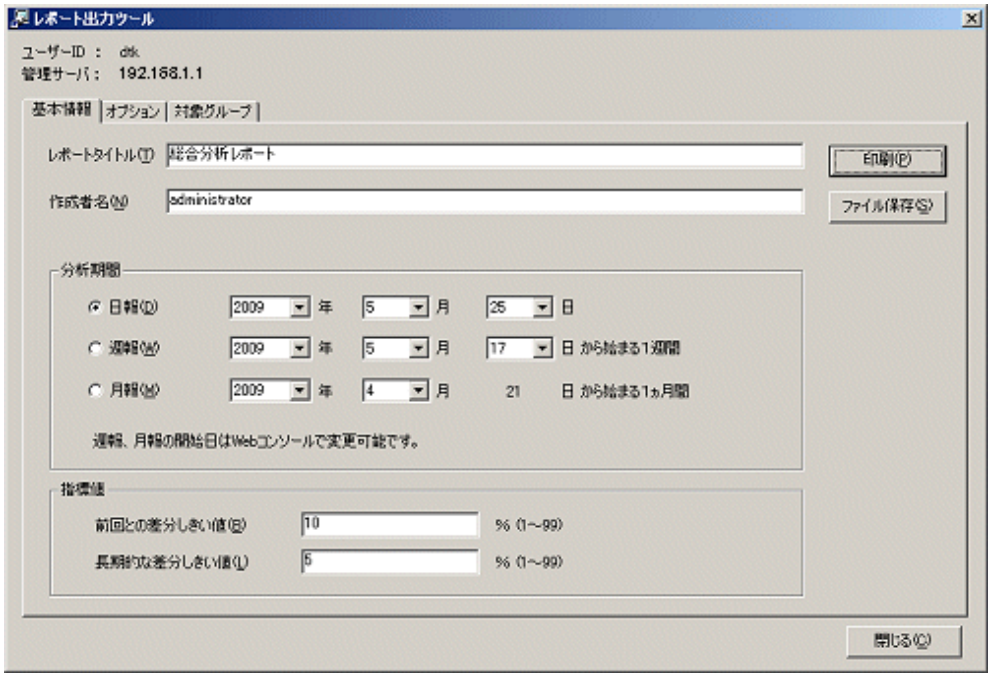
出力形式は、“概要シート”、“詳細シート”、“対象グループシート”を参照してください。

6.6 総合分析レポート

総合分析レポートは、情報漏洩分析，端末利用分析，違反操作分析の3つ観点の診断の概要をまとめ、総合的な診断結果を出力します。

6.6.1 総合分析レポートを出力する

1. [レポート出力ツール]画面で、[総合分析]を選択します。
   →以下の画面が表示されます。



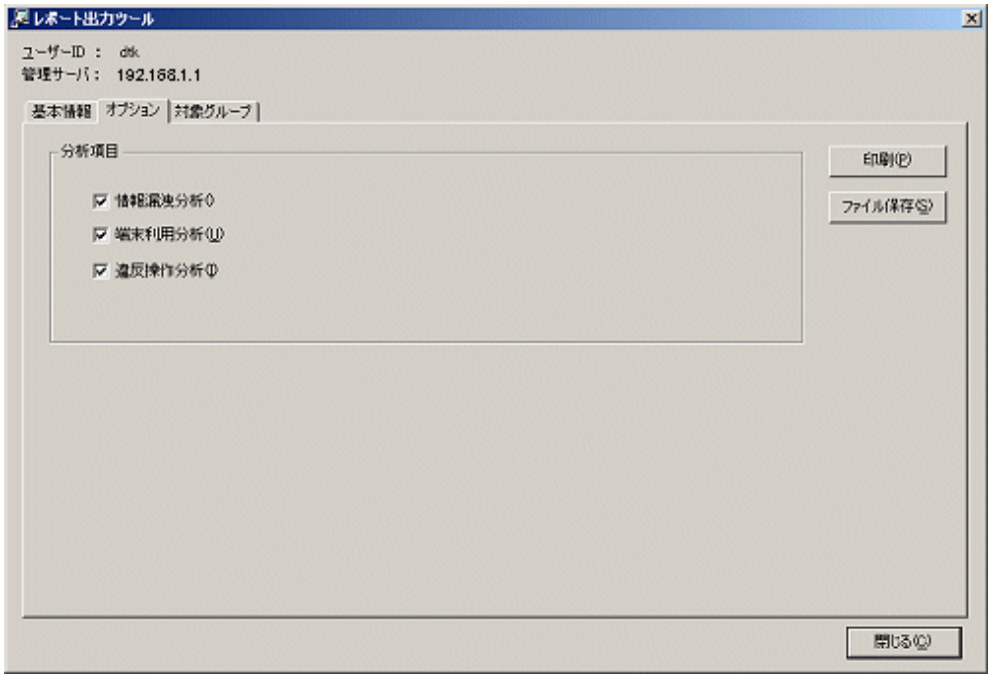
2. 各タブの項目を設定します。
各タブの設定内容は、[印刷]または[ファイル保存]を行った場合は、ログインしているユーザー固有の情報として、ログアナライザサーバに保存されます。次回起動時に、保存されている情報が表示されます。

[基本情報]タブの設定

基本情報タブの設定は、情報漏洩分析レポートの出力時と共通です。“[基本情報]タブの設定”を参照してください。

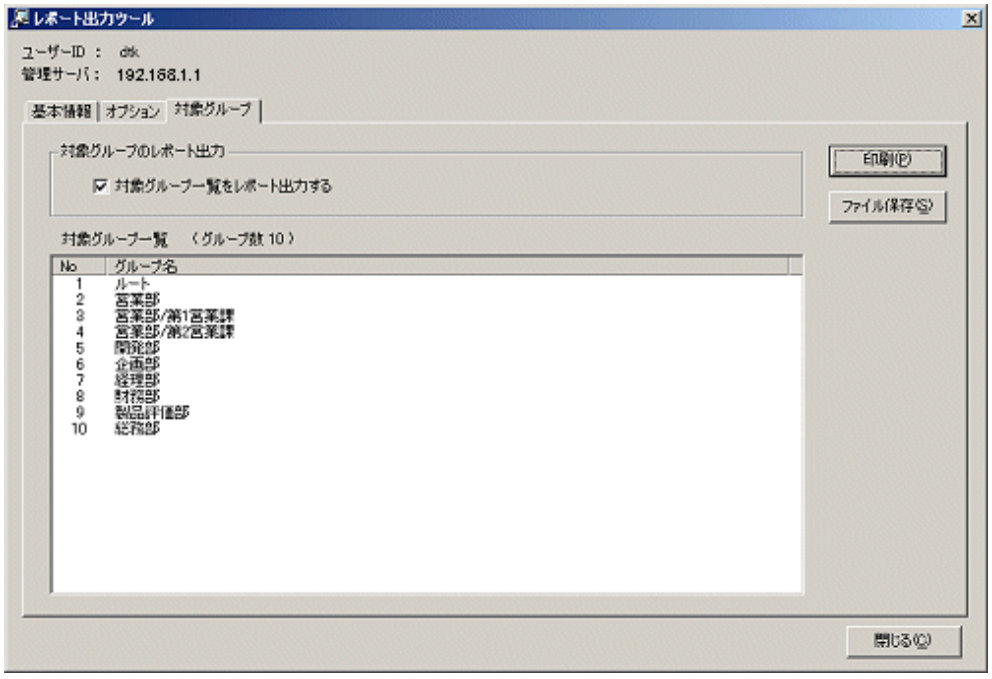
[オプション]タブの設定

分析項目を選択します。
必ず1つ以上の項目を選択してください(デフォルトではすべての項目がチェックされています)。



[対象グループ]タブの設定

[対象グループ一覧]をレポートに出力するかどうかを設定をします。
設定は、情報漏洩分析レポートの出力時と共通です。“[対象グループ]タブの設定”を参照してください。



3. [印刷]または[ファイル保存]ボタンをクリックします。

注意

レポート出力中は、Microsoft® Excelを操作しないでください

レポート出力中は、Microsoft® Excelファイルの[新規作成]や[開く]操作を行わないでください。レポート出力が正常に行われない場合があります。

また、レポート出力前に、Microsoft® Excelが正しく起動することを確認してください。Microsoft® Excelが正しく起動しない場合は、レポート出力処理が長時間たっても終了しないなど、不具合が発生するときがあります。

【[印刷]ボタンをクリックした場合】

生成したレポートを印刷します。

[印刷]画面が表示されますので、プリンタへの印刷設定を行い、レポートを印刷します。

ポイント

印刷ダイアログがレポート出力ツールの後ろに隠れている場合があります。

長時間たっても印刷ダイアログが表示されない場合は、印刷ダイアログがレポート出力ツールの後ろに隠れている可能性があります。

【[ファイル保存]ボタンをクリックした場合】

生成したレポートをファイルに保存します。

注意

出力したレポートは、安全なところに保存してください

出力したレポートには、個人情報やシステム構成情報が含まれる場合があります。ファイルの保存先は、十分なセキュリティ対策が施されたフォルダを指定してください。
【例】
フォルダのアクセス権を、管理者以外のユーザーが参照できないように設定する

保存画面が表示されますので、保存先を指定して、[保存]ボタンをクリックします。

ファイルは、以下の名称で保存されます。

デフォルト名:Summary_[分析期間]_[分析期間開始年月日].xls
(同名ファイルが存在する場合は、上書き確認ダイアログが表示されます。)

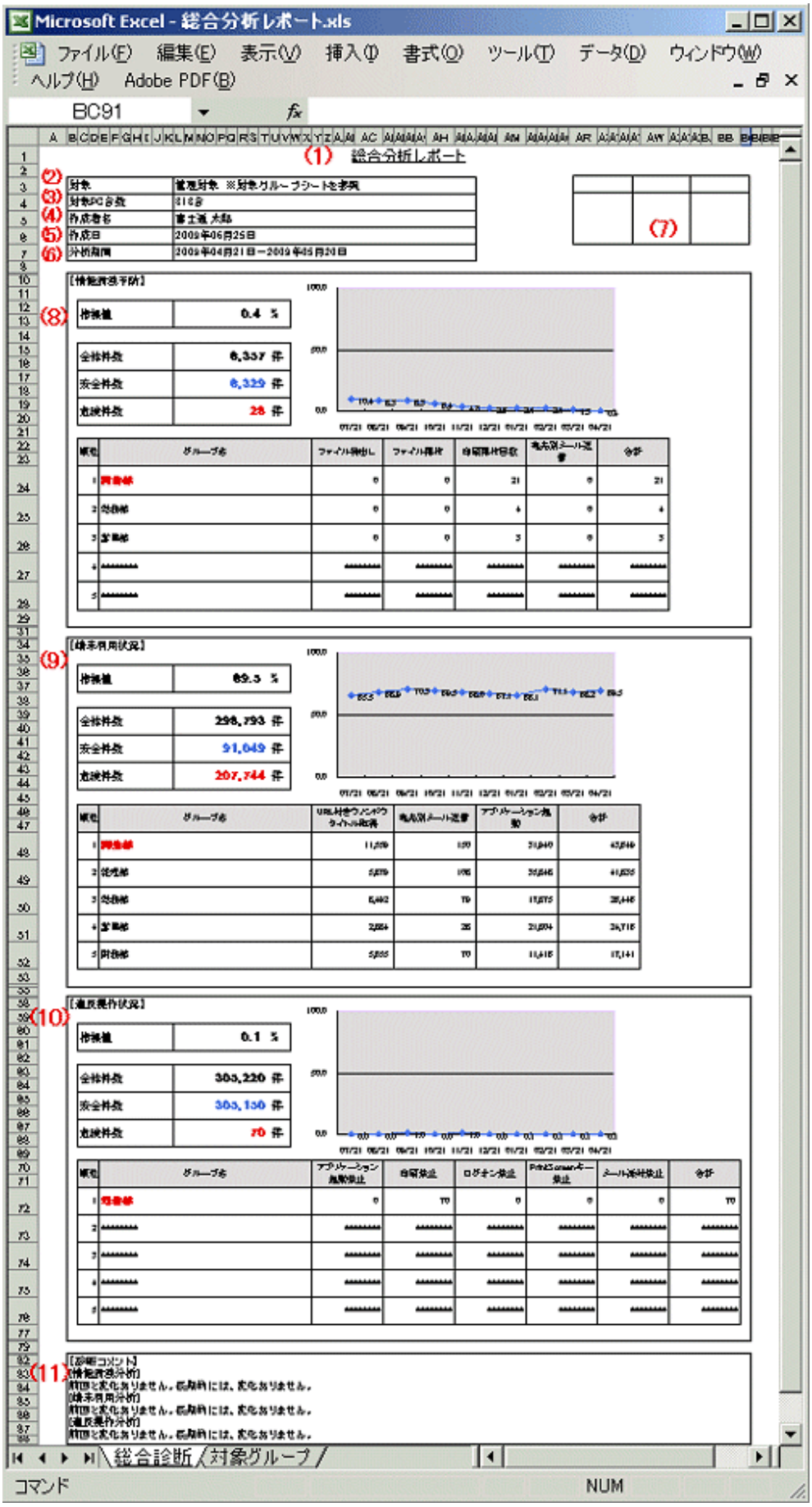
- 分析期間
  日報:daily
  週報:weekly
  月報:monthly
- 分析期間開始年月日:YYYYMMDD([基本情報]タブの[分析期間]で設定した日付)

6.6.2 総合分析レポートの内容

総合分析レポートの構成は以下のとおりです。

生成したレポートファイルや印刷結果のレイアウトは、使用しているMicrosoft® Excelのバージョンやサービスパックによって異なる場合があります。

総合診断シート


Microsoft Excel - 総合分析レポート.xls
ファイル(F) 編集(E) 表示(V) 挿入(I) 書式(O) ツール(T) データ(D) ウィンドウ(W)
ヘルプ(H) Adobe PDF(B)
(1) 総合分析レポート
(2)
(3)
(4)
(5)
(6)
(7)
(8)
(9)
(10)
(11)
総合診断
対象グループ
コマンド
NUM

(1)レポートタイトル

基本情報設定で指定したタイトルが記述されます。

(2)対象

管理の対象を表示します。常に「管理対象」と表示します。

(3)対象PC台数

管理対象の全PC台数を表示します。

・ 対象PCがない場合は0台と表示します。

(4)作成者名

基本情報設定で指定した作成者名が記述されます。

(5)作成日

レポート出力を行った日付が記述されます。

(6)分析期間

基本情報設定で指定した、分析期間を記述します。

(7)承認印欄

報告レポートとして使用する場合の承認欄です(欄の数は変更できません)。

(8)情報漏洩分析結果(※)

情報漏洩分析結果の要約を記述します。

(9)端末利用分析結果(※)

端末利用分析結果の要約を記述します。

(10)違反操作分析結果(※)

違反操作分析結果の要約を記述します。

(11)診断コメント

「総合分析」レポートの診断コメントでは、分析項目毎に以下の内容で記述します。

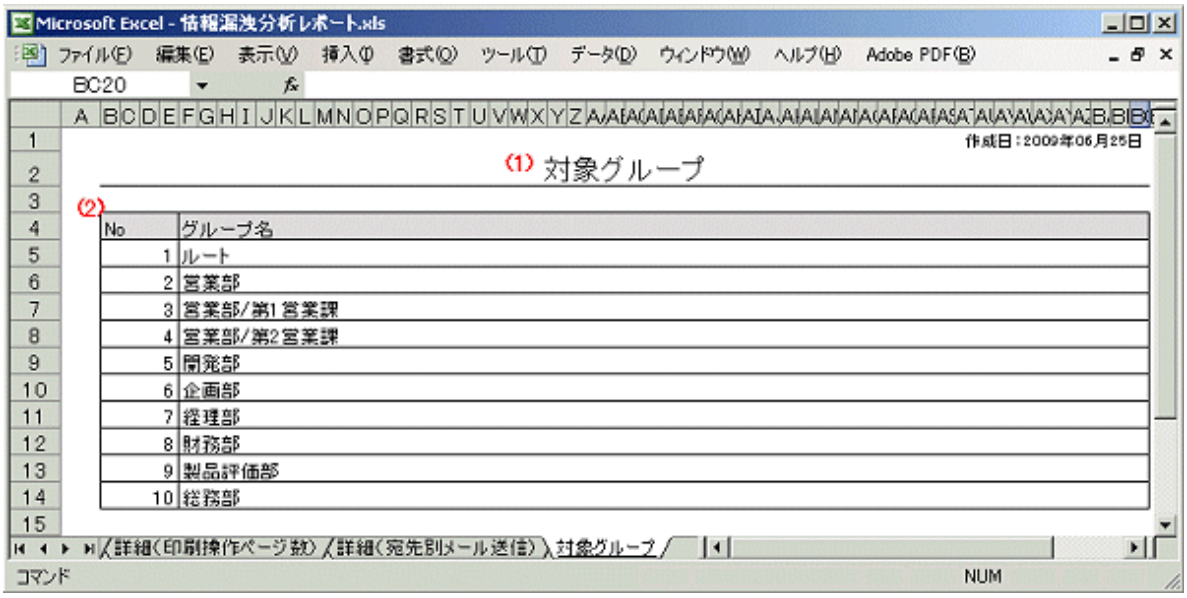
・ 前回との比較からの考察
診断結果の指標値に対して、前回の診断時の指標値との差分により、危険度が増加したか低下したかで、リスク状況の判定を行いコメントを記述します。

・ 長期的な傾向について
過去の分析結果の指標値の推移から予測される指標値に対して、今回の指標値が増加しているか低減しているかで、リスク状況の判定を行いコメントを記述します。

※) 各分析結果に記述される内容は、各分析レポートの概要シート(共通フォーマット)の要約です。項目の説明については、“概要シート”を参照してください。

対象グループシート

分析を行った部門情報が出力されます。



(1)レポートタイトル

“対象グループ”と記述されます。

(2) 対象グループ一覧

分析対象の部門が記述されます。
グループ名は、ルートからのフルパスで記述されます。
【例】開発部/第三開発課

複数の管理部門が存在する場合は、行を追加して表示されます。
記述される最大部門数は、50000部門です。

対象グループシートの各項目の内容は、最大512バイトまで表示されます。

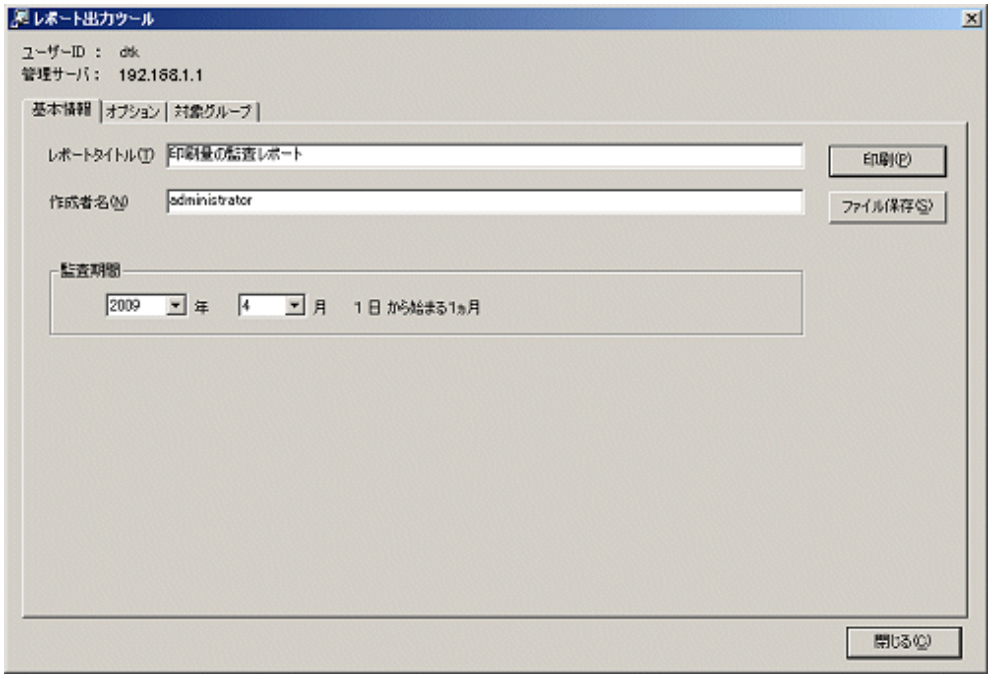
6.7 印刷量監査レポート

印刷量監査レポートは、印刷量から換算する、CO2排出量の削減具合や印刷コストの削減具合を評価する観点で、以下のログを集計・分析した結果を出力します。

- 印刷操作ログ

6.7.1 印刷量監査レポートを出力する

1. [レポート出力ツール]画面で、[印刷量監査]を選択します。
   →以下の画面が表示されます。



- ユーザーID:ログインしているユーザーIDです。
- 管理サーバ:レポート出力するログが格納されている管理サーバのIPアドレスです。

2. 各タブの項目を設定します。
   各タブの設定内容は、[印刷]または[ファイル保存]を行った場合は、ログインしているユーザー固有の情報として、ログアナライザサーバに保存されます。次回起動時に、保存されている情報が表示されます。

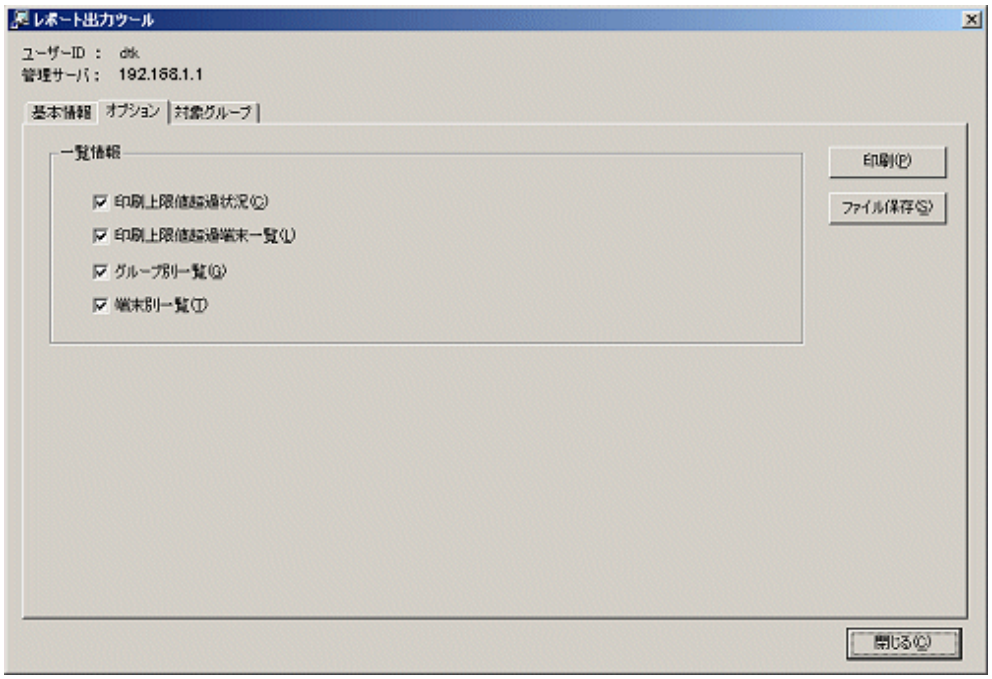
[基本情報]タブの設定

以下の項目を設定します。

入力項目	内容
[レポートタイトル]	出力するレポートのタイトルを指定します。 半角の英数字、半角の記号、および全角2バイト文字を合わせて、64バイトまで設定できます。 初期値は“印刷量の監査レポート”です。
[作成者名]	レポートの作成者を指定します。 半角の英数字、半角の記号、および全角2バイト文字を合わせて、40バイトまで設定できます。 初期値はログイン中のユーザーIDです。
[監査期間]	出力するレポートの監査期間を設定します。 監査期間は、2005年1月～すでに完了している最も直近の月度・年度の中から選択可能です。

[オプション]タブの設定

以下の項目を設定します。



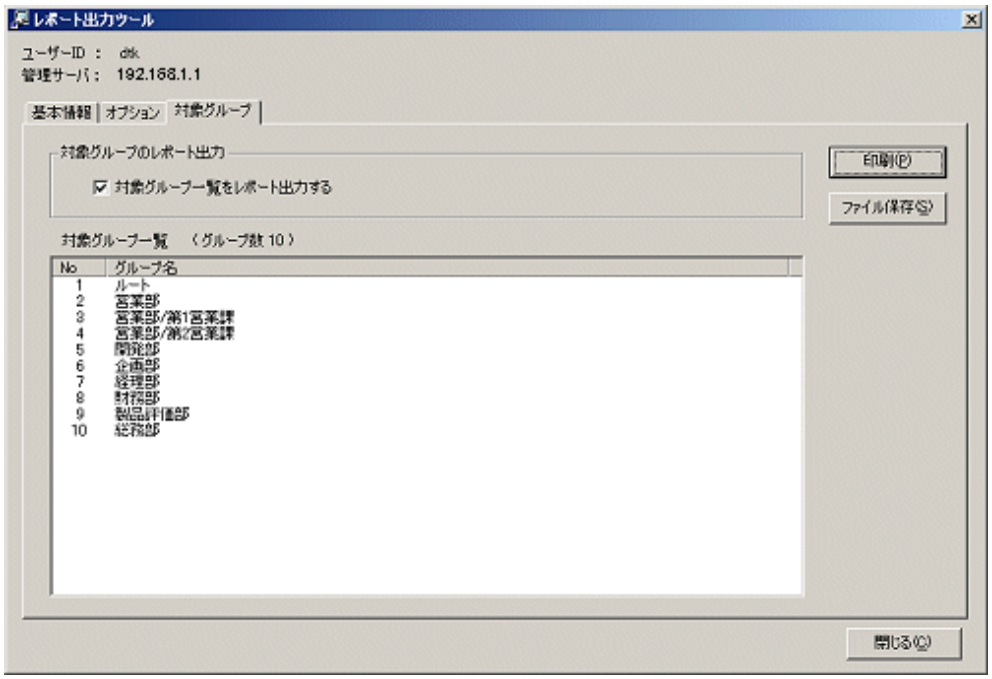
[一覧情報]

レポートに出力する項目を選択します。

項目名	説明
[印刷上限値超過状況]	監査月の印刷上限超過状況のレポートを出力する場合にチェックします。初期値はチェックONです。
[印刷上限値超過端末一覧]	監査当月の印刷上限値を超過する端末一覧のレポートを出力する場合にチェックします。初期値はチェックONです。
[グループ別一覧]	監査月に対し、グループ別で印刷量を出力する場合にチェックします。初期値はチェックOFFです。
[端末別一覧]	監査月に対し、端末別で印刷量を出力する場合にチェックします。初期値はチェックOFFです。

[対象グループ]タブの設定

以下の項目を設定します。



項目名	説明
[対象グループのレポート出力] [対象グループ一覧をレポート出力する]	・ チェックする場合:[対象グループ一覧]をレポートに出力します。 ・ チェックしない場合**(初期値)**:[対象グループ一覧]をレポートに出力しません。
[対象グループ一覧]	ログの分析対象であるグループが、レポートに出力されます。 グループ名は、“/”区切りでルートからのフルパスで表示されます。 【例】開発部/第三開発課 タイトルの横にはグループの総数が表示されます。 最大50000グループまで表示します。

3. [印刷]または[ファイル保存]ボタンをクリックします。

注意

レポート出力中は、Microsoft® Excelを操作しないでください

レポート出力中は、Microsoft® Excelファイルの[新規作成]や[開く]操作を行わないでください。レポート出力が正常に行われない場合があります。

また、レポート出力前に、Microsoft® Excelが正しく起動することを確認してください。Microsoft® Excelが正しく起動しない場合は、レポート出力処理が長時間たっても終了しないなど、不具合が発生するときがあります。

【[印刷]ボタンをクリックした場合】

生成したレポートを印刷します。

[印刷]画面が表示されますので、プリンタへの印刷設定を行い、レポートを印刷します。

ポイント

印刷ダイアログがレポート出力ツールの後ろに隠れている場合があります。

長時間たっても印刷ダイアログが表示されない場合は、印刷ダイアログがレポート出力ツールの後ろに隠れている可能性があります。

【[ファイル保存]ボタンをクリックした場合】

生成したレポートをファイルに保存します。

注意

出力したレポートは、安全なところに保存してください

出力したレポートには、個人情報やシステム構成情報が含まれる場合があります。ファイルの保存先は、十分なセキュリティ対策が施されたフォルダを指定してください。
【例】
フォルダのアクセス権を、管理者以外のユーザーが参照できないように設定する

保存画面が表示されますので、保存先を指定して、[保存]ボタンをクリックします。

ファイルは、以下の名称で保存されます。

デフォルト名：Ecoprint_monthly_YYYYMMDD.xls (月報レポート)
(同名ファイルが存在する場合は、上書き確認ダイアログが表示されます。)

－ レポート開始日：YYYYMMDD([基本情報]タブの[監査期間]で設定した日付)

6.7.2 印刷量監査レポートの内容

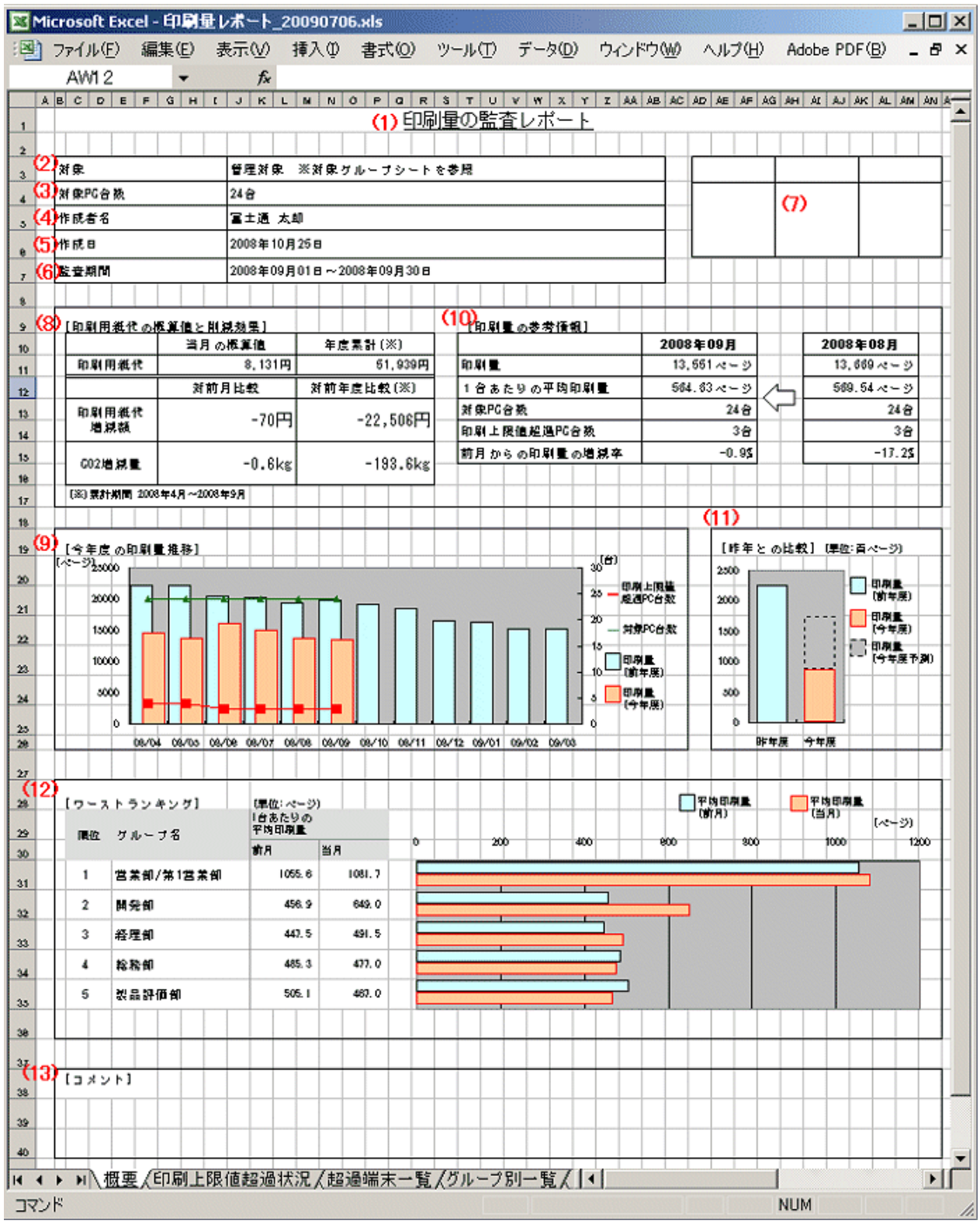
印刷量監査レポートの出力内容は以下のとおりです。

分類	シート名	説明
概要シート	概要	監査月に対し、印刷コストを印刷用紙代・CO2排出量の観点で出力します。
詳細シート	印刷上限値超過状況	監査月に対し、印刷上限超過状況を出力します。
	超過端末一覧	監査当月の印刷上限値を超過する端末一覧を表示します。
	グループ別一覧	監査月に対し、グループ別で印刷量を出力します。
	端末別一覧	監査月に対し、端末別で印刷量を出力します。
対象グループシート	対象グループ	レポートの監査対象のグループの情報を出力します。

生成したレポートファイルや印刷結果のレイアウトは、使用しているMicrosoft® Excelのバージョンやサービスパックによって異なる場合があります。
レポートに出力される各値については、特に断りがない限り表示桁数以下を四捨五入して表示します。またデータが存在しない場合は0と表示します。
レポートに出力される値のうち、年度の概念を含むものについては、監査月以降のデータは集計値に含まれません。またレポート上にも表示されません。

本レポートの説明にある、「年度(年度開始月)」「1ページあたりの印刷用紙代」「1ページあたりのCO2排出量」については、それぞれWebコンソールのログアナライザ動作設定[エコ監査設定]の「年度開始月設定」「1ページ(または1枚)あたりの用紙代」「1ページ(または1枚)あたりのCO2排出量」が使用されます。これらの値を変更する場合は、Webコンソールの設定を変更してください。詳細は“2.8.2.2.4 その他の条件を設定する”を参照してください。

概要シート:概要



(1) レポートタイトル

レポート出力ツールで指定したレポートタイトルが表示されます。

(2) 対象

管理の対象を表示します。常に「管理対象」と表示します。

(3) 対象PC台数

管理対象の全PC台数を表示します。

(4) 作成者名

レポート出力ツールで指定した作成者名が表示されます。

(5) 作成日

レポートを出力した日付が表示されます。

(6) 監査期間

レポート出力ツールで指定した監査期間が表示されます。

(7) 捺印欄

作成したファイルに捺印をするための領域です。必ず出力されます。

(8) 印刷用紙代の概算値と削減効果

当月・年度累計の印刷用紙代の概算値、前月・前年度と比較しての印刷用紙代、CO2排出量の増減分について表示します。

- 当月の印刷用紙代の概算値の求め方
  印刷用紙代＝印刷ページ数×1ページあたりの印刷用紙代
- 当月のCO2排出量の概算値の求め方
  CO2排出量＝印刷ページ数×1ページあたりのCO2排出量
- 年度累計の印刷用紙代の概算値の求め方
  印刷用紙代＝当年の年度開始月～監査月までの合計印刷ページ数×1ページあたりの印刷用紙代
- 年度累計のCO2排出量の概算値の求め方
  CO2排出量＝当年の年度開始月～監査月までの合計印刷ページ数×1ページあたりのCO2排出量
- 「(※)累計期間」には、監査期間に対応した期間が表示されます。
- 対前月比較は、以下のように算出しています。対前月比較は、値がマイナスの場合、改善傾向にあると判断します。

  印刷用紙代増減額＝当月の印刷用紙代－前月の印刷用紙代

  CO2増減量＝当月のCO2排出量－前月のCO2排出量
- 対前年度比較は、以下のように算出しています。対前年度比較は、値がマイナスの場合、改善傾向にあると判断します。

  印刷用紙代増減額＝当年の印刷用紙代年度累計(※)－前年の印刷用紙代年度累計(※)

  CO2増減量＝当年のCO2排出量年度累計(※)－前年のCO2排出量年度累計(※)

  ※対象年度の開始月～監査月までを対象

「1ページあたりの印刷用紙代」「1ページあたりのCO2排出量」「年度開始月」について“2.8.2.2.4 その他の条件を設定する”を確認してください。

(9) 今年度の印刷量推移

今年度の印刷量(ページ)とPC台数(全体数、印刷上限値超過数)の推移をグラフ出力します。

- 印刷量については前年度の印刷量データがあれば、あわせて表示します。
- 横軸は年度固定(年度開始月～年度終了月)です。

(10) 印刷量の参考情報

以下のデータについて、前月と今月の情報を表示します。

- 印刷量
- 1台あたりの平均印刷量
- 対象PC台数
- 印刷上限値超過PC台数
  印刷上限値超過PCとは、“当月の印刷ページ数の合計が当月の印刷上限値を超過したPC”です。

印刷上限値は「印刷監視動作設定」の設定によって求め方が異なります。求め方は以下の通りです。
(印刷上限値は小数点以下を切り捨てます。)

ー 「印刷ページ数を集計する単位」が「日ごと」の端末

印刷上限値＝ (端末の基準値) × 当月の日数(日)

ー 「印刷ページ数を集計する単位」が「週ごと」の端末

印刷上限値＝ (端末の基準値 ÷ 7) × 当月の日数(日)

ー 「印刷ページ数を集計する単位」が「月ごと」の端末

印刷上限値＝ (端末の基準値)

端末の基準値の求め方:

- [設定した印刷ページ数に達した時の動作]として「警告する」のみにチェックが入っている端末

  端末の基準値 ＝「警告する」の設定ページ数

- [設定した印刷ページ数に達した時の動作]として「警告する」と「印刷を禁止する」の両方にチェックが入っている端末

  端末の基準値 ＝「印刷を禁止する」の設定ページ数

・ 前月からの印刷量の増減率(値がマイナスの場合、改善傾向にあると判断します。)

・ 前月からの印刷量の増減率とは、月内の実績が前月に対してどれだけ削減できたかを示す値です。以下の式で算出しています。

増減率= (当月印刷量-前月印刷量)÷(前月印刷量)×100

・ 前月からの印刷量の増減率は、前月印刷量が0ページの場合は算出を行わずハイフン(-)が表示されます。

(11) 昨年との比較

印刷量について、前年度と今年度の実績、予測をグラフ表示します。

・ 予測値については、今年度の実績を月平均し、その月平均を残りの月数で掛けた値となります。

(12) ワーストランキング

印刷量について、当月の1台あたりの平均印刷量が大きいグループからランキング表示します。またグラフ表示もします。

・ 前月のデータもある場合は、前月のデータもあわせて表示します。

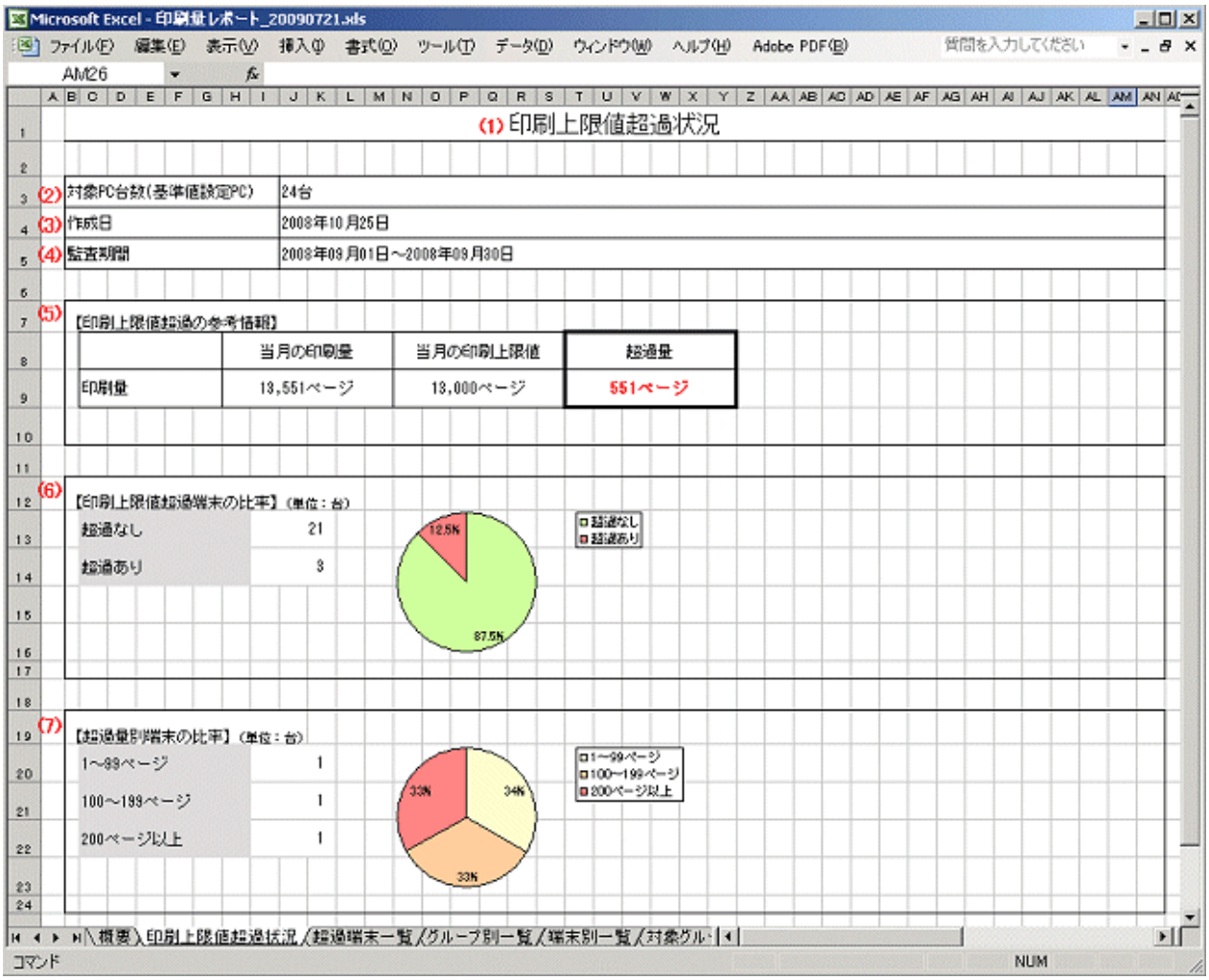
・ 最大5グループまで表示されます(同一順位でも6件以上は表示しません)。

・ 対象グループが5グループより少ない場合は、空欄に対しハイフン(-)を表示します。

(13) コメント

ユーザーの自由コメント欄です。

詳細シート:印刷上限値超過状況



(1) レポートタイトル

「印刷上限値超過状況」と表示されます。

(2) 対象PC台数(基準値設定PC)

本シートの対象となる、印刷監視動作設定がONのPC台数を表示します。

(3) 作成日

レポートを出力した日付が表示されます。

(4) 監査期間

レポート出力ツールで指定した監査期間が表示されます。

(5) 印刷上限値超過の参考情報

当月の印刷量、当月の印刷上限値、超過量が表示されます。

- 当月の印刷量が印刷上限値を超過していない場合は、超過量には0と表示されます。
- 超過量が1以上の場合は、赤太字で表示されます。
- 印刷監視動作設定において、[警告する]または[印刷を禁止する]にチェックが入っているPCだけが集計対象となります。
  印刷監視動作設定については、“2.4.1.11 [エコ監視設定]タブの設定”を参照してください。

(6) 印刷上限値超過端末の比率

端末について、「超過なし」、「超過あり」の2パターンで台数表示、および比率をグラフ表示します。

・ 印刷監視動作設定がONのPCのみ集計対象となります。

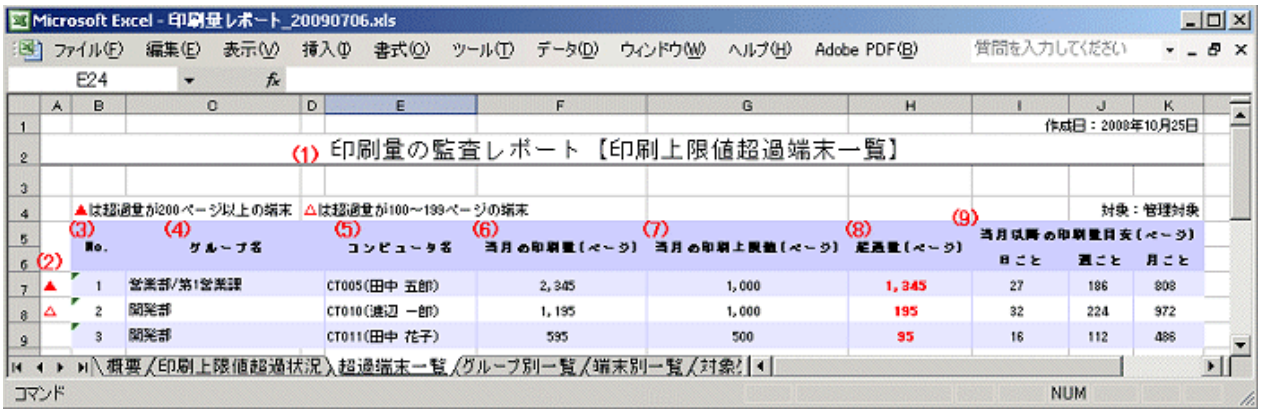
(7) 超過量別端末の比率

超過端末について、「1～基準1-1」、「基準1～基準2-1」、「基準2以上」の3パターンで台数表示、および比率をグラフ表示します。

・ 「基準1」、「基準2」は、ログアナライザの[動作設定]画面で設定する「監査の判定基準1」「監査の判定基準2」の値がそれぞれ対応します。

・ 印刷監視動作設定がONのPCのみ集計対象となります。

詳細シート:超過端末一覧



(1) レポートタイトル

「印刷量の監査レポート【印刷上限値超過端末一覧】」と表示されます。

(2) [▲]または[△]

端末の超過状態を示します。

▲:「基準2」ページ以上超過した端末を示します。

△:「基準1」～「基準2」-1ページ以上超過した端末を示します。

・ 「基準1」、「基準2」は、ログアナライザの[動作設定]画面で設定する「監査の判定基準1」「監査の判定基準2」の値がそれぞれ対応します。

(3) No.

通し番号です。

(4) グループ名

グループ名です。

(5) コンピュータ名

コンピュータ名が表示されます。
コンピュータ名と名称が異なっていた場合、コンピュータ名(名称)の形式で表示されます。

(6) 当月の印刷量

当月の印刷量です。

(7) 当月の印刷上限値

当月の印刷上限値です。

(8) 超過量

超過量です。この値をキーに一覧を降順ソートします。赤太字で表示されます。

(9) 当月以降の印刷量目安

該当端末が当月の印刷上限値を年度単位で守る場合に、来月以降遵守する必要のある印刷量です。月ごと、週ごと、日ごとの3パターンで表示されます。
年度末となる月のレポートなど、年度の残日数や年度の残月数が0となる場合は算出を行わずハイフン(-)が表示されます。

・ それぞれの値は以下の計算式で算出しています。

日ごと＝(当月の印刷上限値×(年度の残月数+1)－当月の印刷量)÷(年度の残日数)

週ごと＝(当月の印刷上限値×(年度の残月数+1)－当月の印刷量)÷(年度の残日数)×7

月ごと＝(当月の印刷上限値×(年度の残月数+1)－当月の印刷量)÷(年度の残月数)

※少数点以下は切り捨てる。

当月の印刷量が当月の印刷上限値を大きく超過し、印刷上限値を年度単位で守れない端末については、値がマイナスで表示されます。

詳細シート:グループ別一覧

(1) レポートタイトル

「印刷量の監査レポート【グループ別一覧】」と表示されます。

(2) No.

通し番号です。

(3) グループ名

グループ名です。本項目をキーにソートし表示します。

(4) 当月の端末台数

当月の印刷台数を表示します。

(5) 当月の印刷量

当月の印刷量を表示します。

(6) 当月の1台あたりの平均印刷量

当月の1台あたりの平均印刷量を表示します。

(7) 当月の基準値設定端末台数

当月の端末台数のうち、印刷監視動作設定がONの端末台数を表示します。

(8) 当月の基準値設定端末の印刷量

当月の印刷量のうち、印刷監視動作設定がONの端末の印刷量を表示します。

(9) 当月の印刷上限値

当月の印刷監視動作設定がONの端末の印刷上限値です。

・ 所属端末の印刷監視動作設定が全てOFFのグループはハイフン(-)が表示されます。

詳細シート:端末別一覧

(1) レポートタイトル

「印刷量の監査レポート【端末別一覧】」と表示されます。

(2) No.

通し番号です。

(3) グループ名

グループ名です。本項目を第1優先キーとしてソートし表示します。

(4) コンピュータ名

コンピュータ名とユーザー名が表示されます。一覧は本項目を第2優先キーとしてソートし表示します。

(5) 当月の印刷量

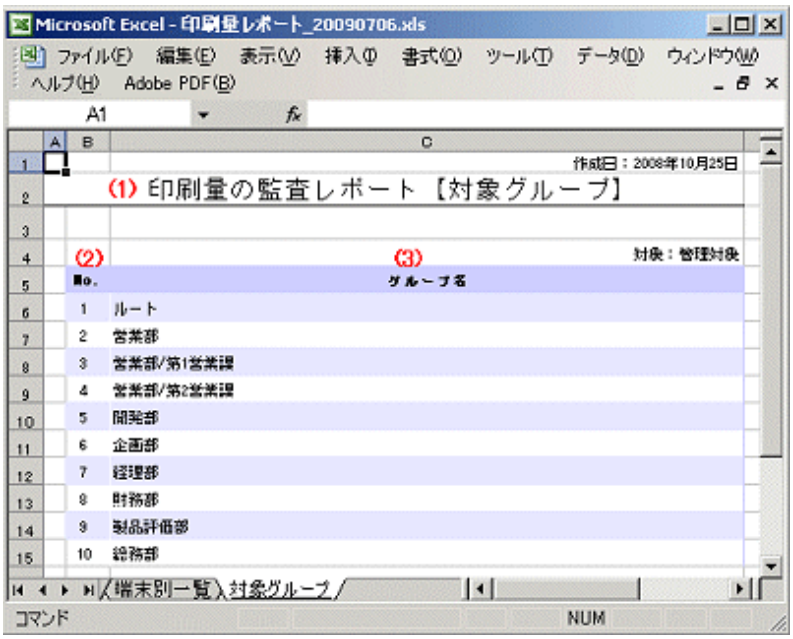
当月の印刷量を表示します。

(6) 当月の印刷上限値

当月の印刷上限値

※印刷監視動作設定がOFFの端末はハイフン(-)が表示されます。

対象グループシート:対象グループ



(1) レポートタイトル

「印刷量の監査レポート【対象グループ】」と表示されます。

(2) No.

通し番号です。

(3) グループ名

レポートの対象となるグループ名です。本項目をキーにソートし表示します。

6.8 レポート出力スケジュールを設定する

レポート出力バッチコマンドをタスクスケジューラに設定することによって、レポート出力を、自動的かつ定期的に実行できます。

ただし、レポート出力バッチコマンドは同時使用できません。バッチコマンドを使用するバッチファイル、またはバッチコマンドを、タスクスケジューラに複数登録しないでください。

注意

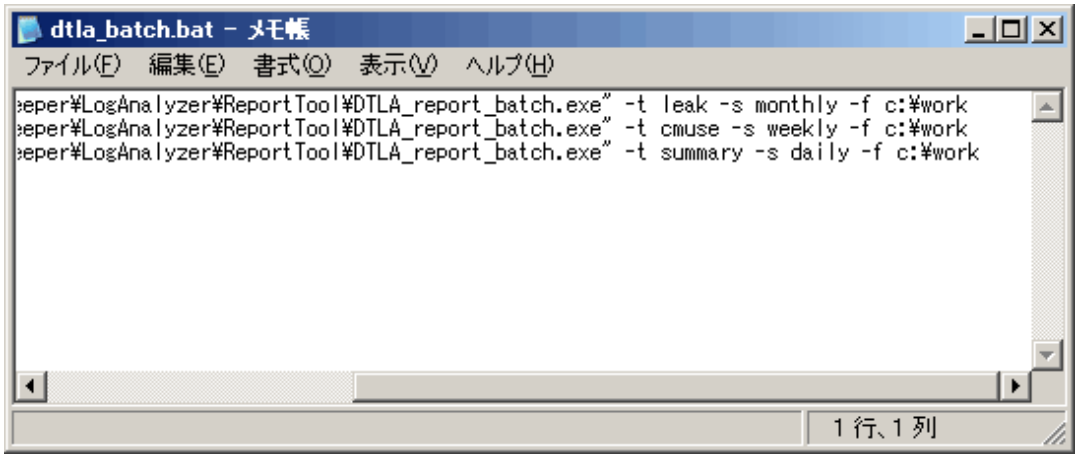
Windows Vista®、Windows Server® 2008、Windows® 7の場合

Windows Vista®、Windows Server® 2008、またはWindows® 7の環境において、コマンドプロンプトで作業を行う場合は、コマンドプロンプトを[管理者として実行]で開いてください。

手順は、以下のとおりです。

1. 出力するレポートに応じて、レポート出力コマンドをバッチファイルに記述します。
   レポート出力コマンドの詳細は、“Systemwalker Desktop Keeper リファレンスマニュアル”の“DTLA_REPORT_BATCH.EXE(レポート出力)”を参照してください。
   - コマンド名や出力先フォルダはフルパスで指定してください。
   - パスに空白を含む場合は、"(ダブルクォーテーション)で囲んでください。

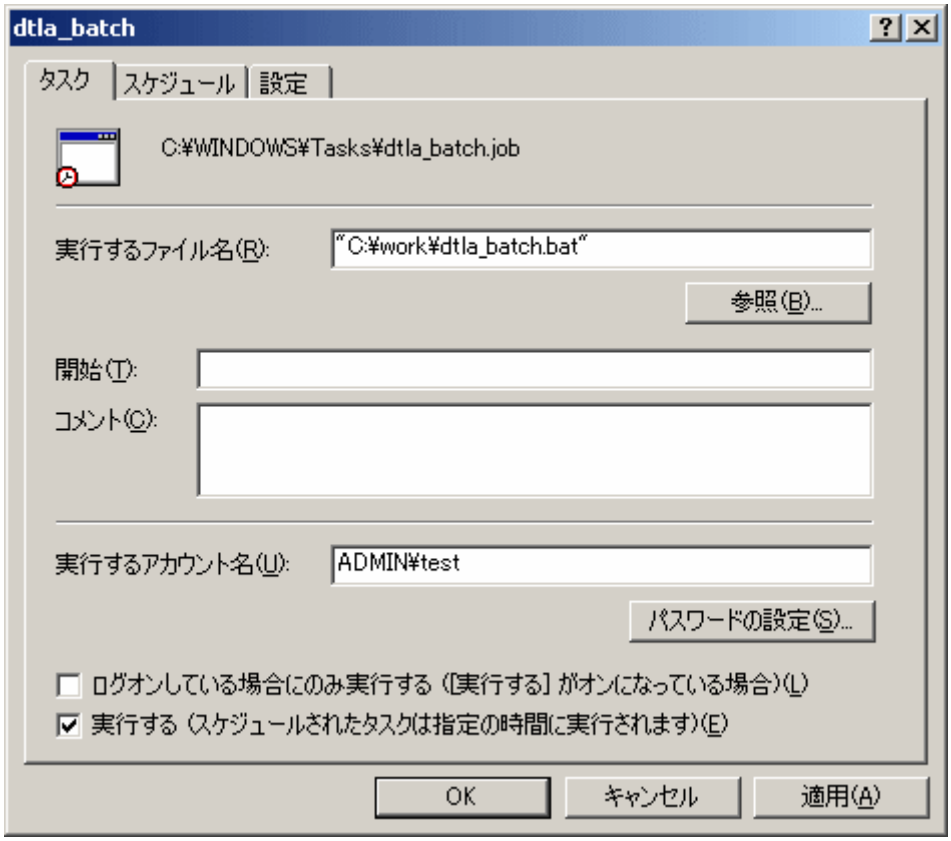
ー 複数のレポートを出力する場合は、コマンドを並べて記述してください。



2. タスクスケジューラに、バッチファイルを登録します。

[Windows® 2000 Professional/Windows® XP Professionalの場合]

1. タスクスケジューラを起動し、[タスク]タブを選択します。



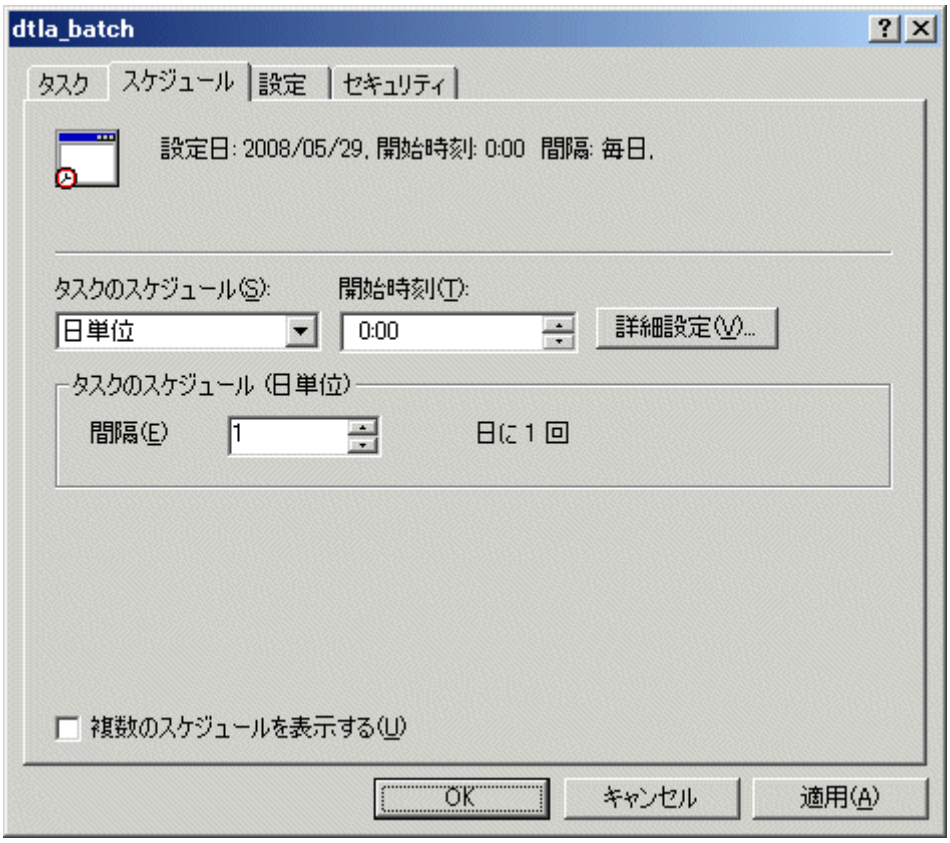
2. 以下の情報を設定します。

・[実行するファイル名]:バッチファイルをフルパスで指定します。パスに空白を含む場合は、"(ダブルクォーテーション)で囲ってください。

・[実行するアカウント名]:Windowsのユーザーアカウントを指定します。バッチユーザー設定を行ったときにログオンしていたユーザーアカウントを指定します。

・[実行する]:チェックボックスをチェックします。

3. [スケジュール]タブを選択し、バッチファイルの開始スケジュールを設定します。



4. [適用]ボタンまたは[OK]ボタンをクリックします。

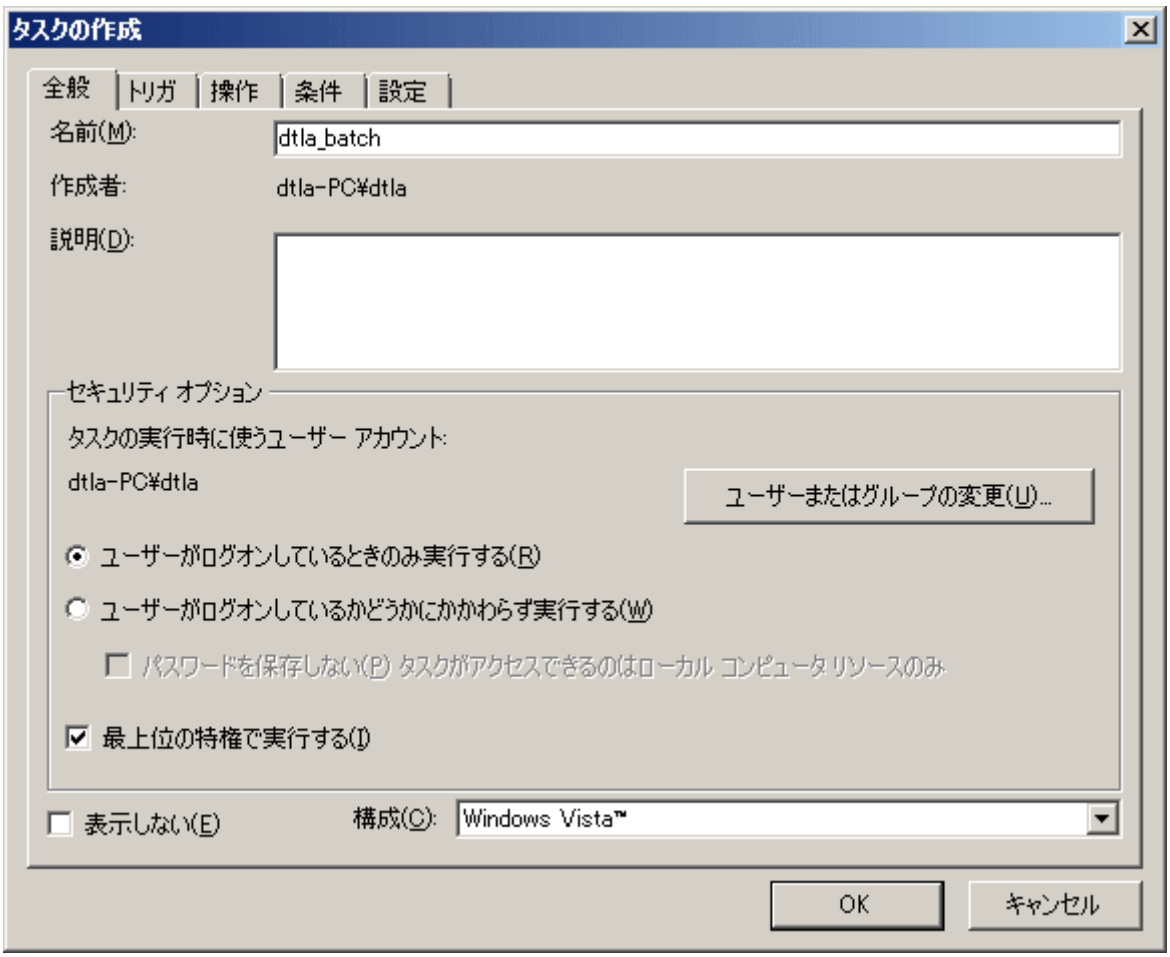
レポート出力コマンドのログは、以下の場所に格納されます。

```
%ALLUSERSPROFILE%¥Application Data¥Fujitsu¥Systemwalker Desktop Keeper¥LogAnalyzer
```

環境変数%ALLUSERPROFILE%は、通常“C:¥Documents and Settings¥All Users”です。

[Windows Vista®、Windows® 7の場合]

1. タスクスケジューラを起動し、[全般]タブを選択します。



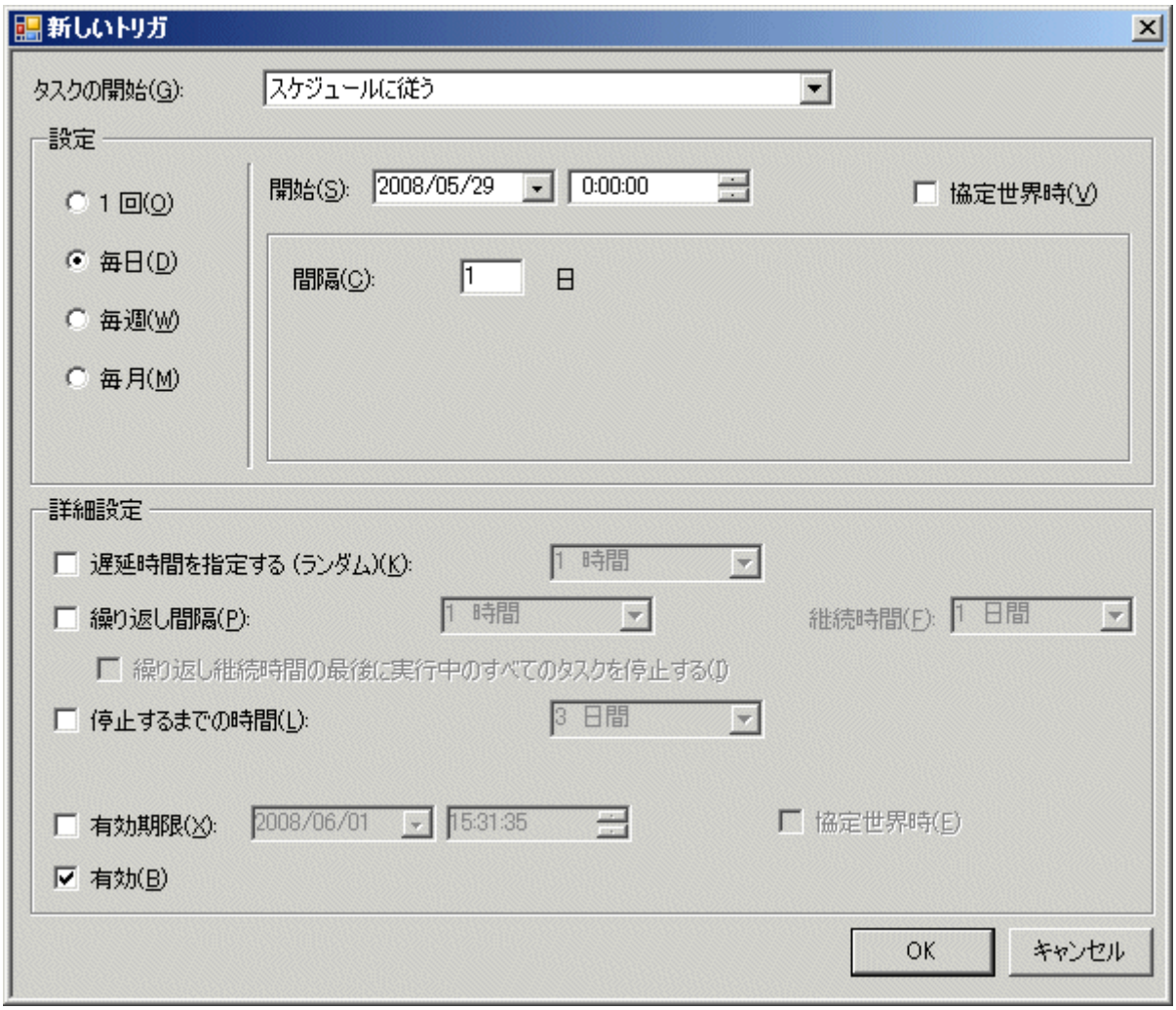
2. 以下の情報を設定します。

・[タスクの実行時に使うユーザーアカウント]:Windowsのユーザーアカウントを指定します。バッチユーザー設定を行ったときにログオンしていたユーザーアカウントを指定します。

・[ユーザーがログオンしているときのみ実行する]:必ず選択します。本項目を選択しない場合は、バッチコマンドが正常に動作しないときがあります。

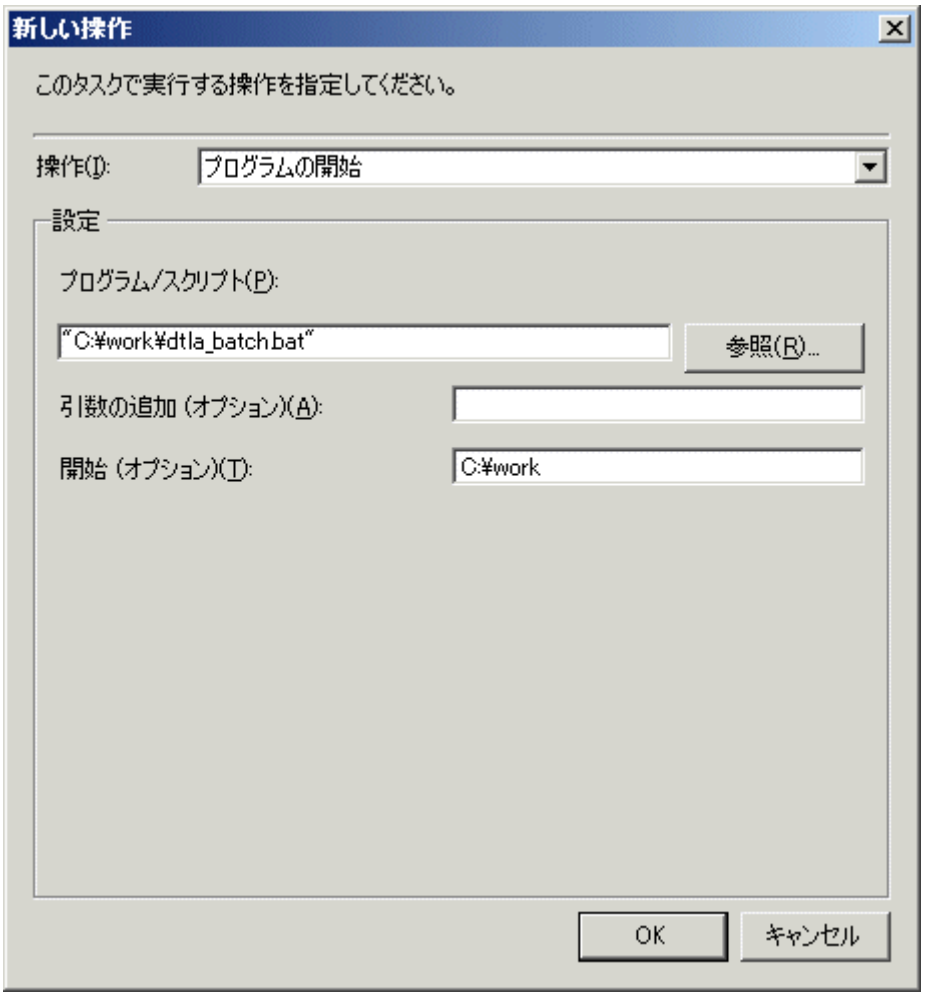
・[最上位の特権で実行する]:チェックボックスをチェックします。

3. [トリガ]タブを選択し、[新規]ボタンをクリックします。



4. バッチファイルの開始スケジュールを設定し、[OK]ボタンをクリックします。

5. [操作]タブを選択し、[新規]ボタンをクリックします。



6. 以下の情報を設定し、[OK]ボタンをクリックします。

   ・[操作]:[プログラムの開始]を選択します。

   ・[プログラム/スクリプト]:バッチファイルをフルパスで指定します。パスに空白を含む場合は、"(ダブルクォーテーション)で囲ってください。

   ・[開始(オプション)]:実行ファイルのあるフォルダをフルパスで指定します。パスは、"(ダブルクォーテーション)で囲まないでください。

7. [OK]ボタンをクリックします。

レポート出力コマンドのログは、以下の場所に格納されます。

```
%ALLUSERSPROFILE%¥Fujitsu¥Systemwalker Desktop Keeper¥LogAnalyzer
```

環境変数%ALLUSERPROFILE%は、通常“C:¥ProgramData”です。

第7章 運用環境を変更する

運用中に環境の変更が必要になった場合に実施する操作を説明します。

7.1 構成情報の取り込み方を変更する

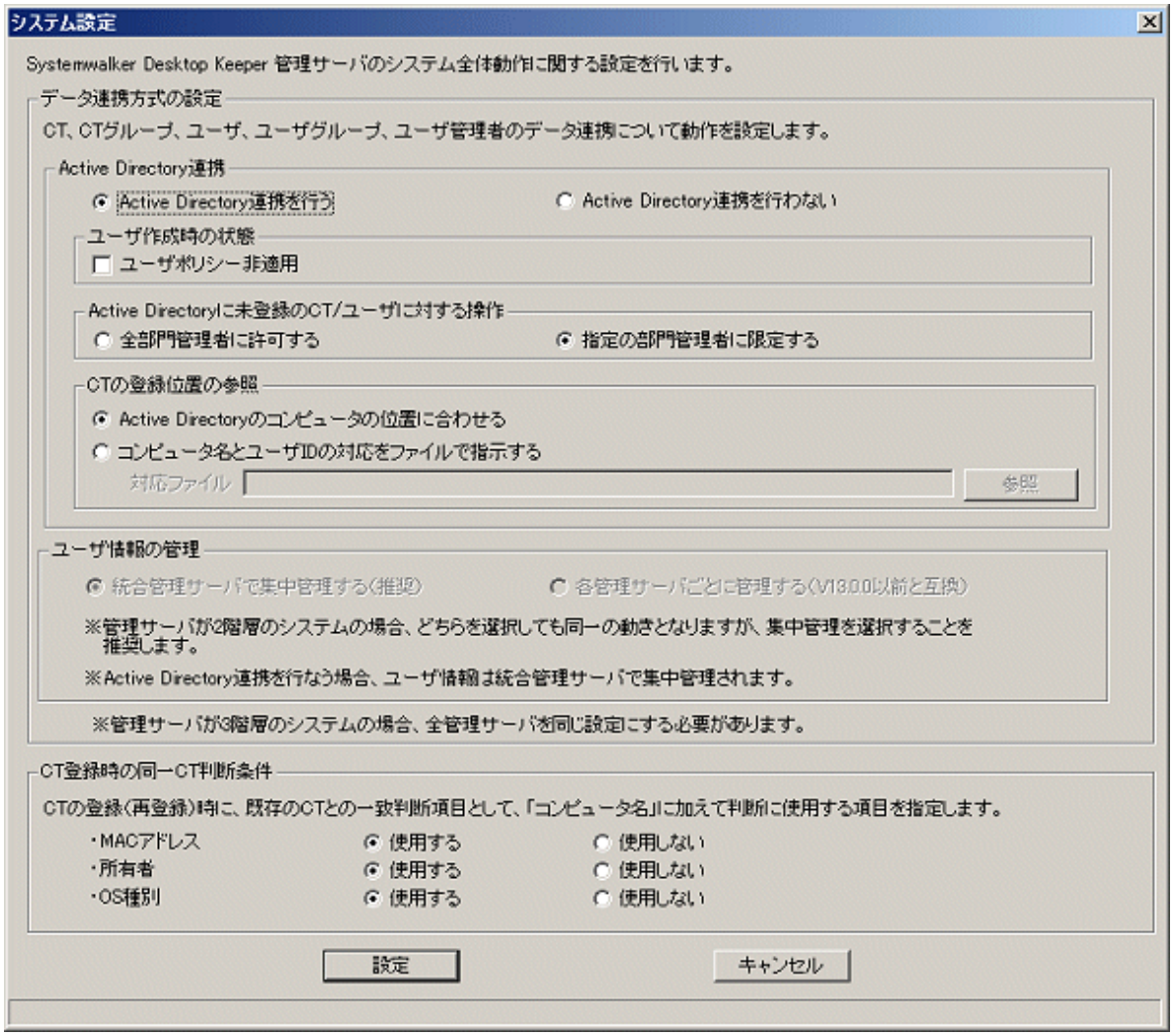
管理コンソールでの手動作成からActive Directory連携による取り込み方法に変更する場合

Active Directoryサーバから構成情報を取り込む運用で必要となる情報は、“2.5.1 Active Directoryから情報を取り込む”を参照してください。

構成情報の取り込み方法を変更した場合、Active Directoryとの連携前に設定したユーザーポリシーは引き継がれません。Active Directory連携で自動作成されたユーザー情報(ユーザー名)にユーザーポリシーを再度設定してください。

1. サーバのサービスを停止します。
2. サーバ設定ツールを起動し、[システム設定]ボタンをクリックします。

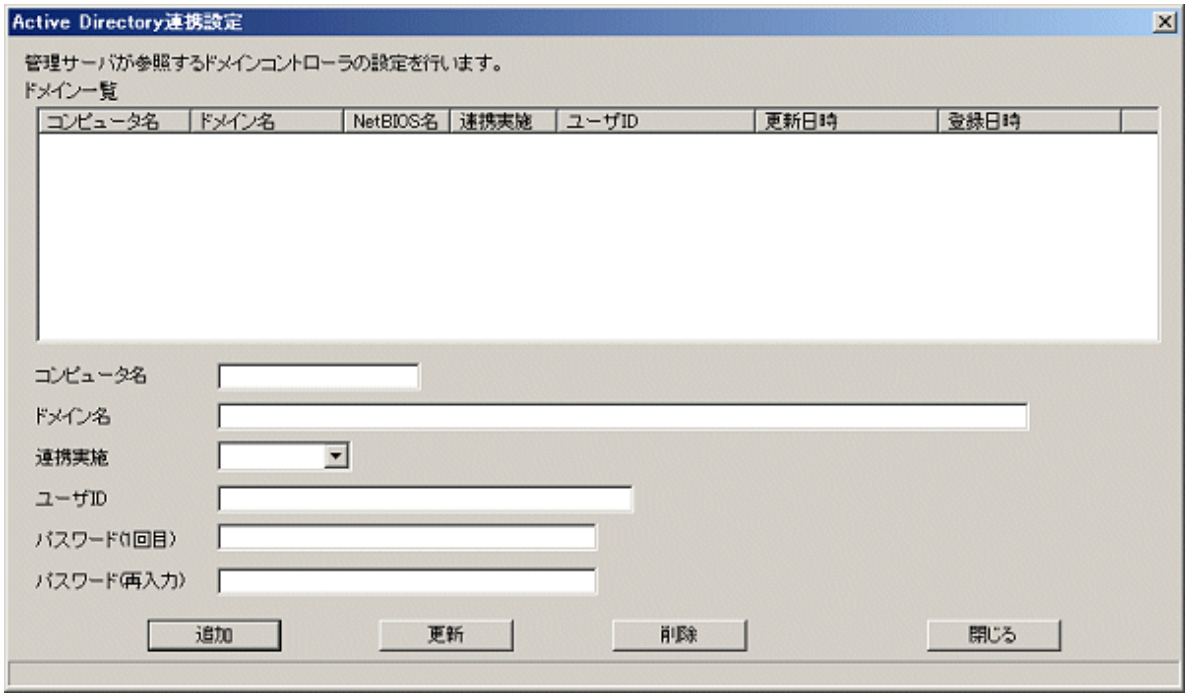
   →[システム設定]画面が表示されます。



3. [Active Directory連携を行う]を選択します。
   その他の設定項目の詳細については、“Systemwalker Desktop Keeper 導入ガイド”の“システム設定を行う”を参照してください。
4. [設定]ボタンをクリックします。

5. [サーバ設定ツール]画面の[Active Directory連携設定]ボタンをクリックします。

   →[Active Directory連携設定]画面が表示されます。



6. 連携するActive Directoryサーバの情報を設定し、[追加]ボタンをクリックします。
   設定項目の詳細については、“Systemwalker Desktop Keeper 導入ガイド”の“Active Directory連携の設定を行う”を参照してください。

7. サーバ設定ツールの[設定]メニューで[Active Directory連携実施]を実行、または、Active Directory連携コマンドを実行します。
   実行手順は、“2.5.1 Active Directoryから情報を取り込む”を参照してください。

   →構成情報が取り込まれます。
   既存のグループツリーは、Localグループ配下に移動します。

8. Active Directory連携で自動作成されたユーザーグループ(ユーザー名)にユーザーポリシーを設定します。
   設定方法は、“3.4.2 ユーザーポリシーを変更する”を参照してください。

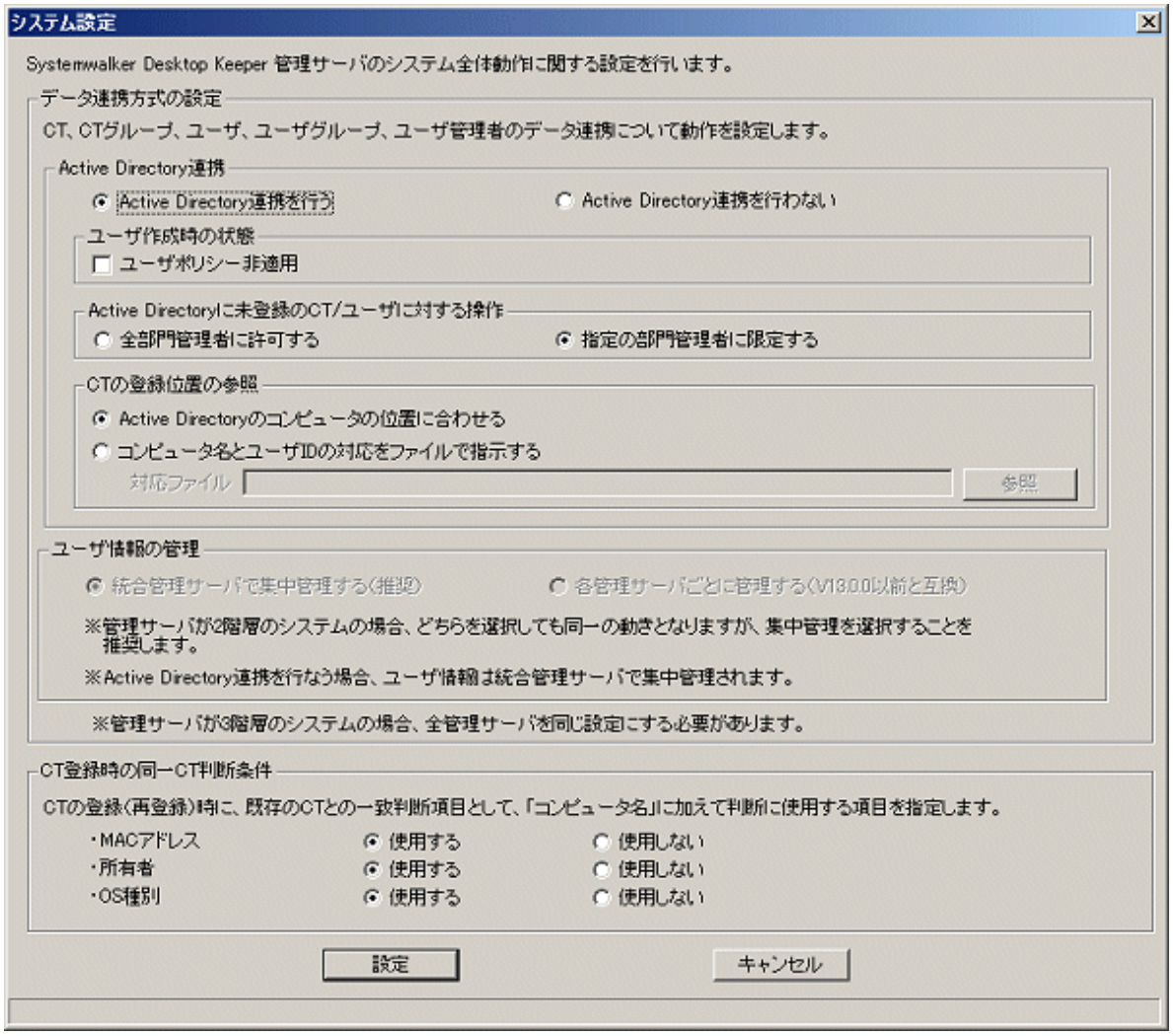
9. サービスを起動します。

Active Directory連携による取り込みを解除する場合

1. サーバのサービスを停止します。

2. サーバ設定ツールを起動し、[システム設定]ボタンをクリックします。

   →[システム設定]画面が表示されます。



3. [Active Directory連携を行わない]を選択し、[設定]ボタンをクリックします。
4. サービスを起動します。

Active Directory連携による構成情報の取り込みを解除すると、ドメイングループ配下のグループ情報、ユーザー情報、およびポリシーがすべて削除されます。
Localグループ配下に作成されていたグループツリーは、ルート配下に移動します。

ルート配下に、手動でまたはSystemwalker Desktop Patrol連携によって、構成情報を構築してください。

7.2 ユーザー情報の管理方法を変更する

ユーザー情報の管理方法を変更できるのは、以下の条件をすべて満たしている場合です。

- 3階層のシステム構成のとき
- 構成情報の取り込みで、Active Directoryと連携していないとき

各管理サーバでの管理から統合管理サーバでの一元管理に変更する場合

1. ユーザー情報を移動します。

   DTKTBLCV.EXE(ユーザー定義の移行)コマンドを使用して、各管理サーバで設定した情報を、統合管理サーバに移行します。
   コマンドの詳細は、“Systemwalker Desktop Keeper リファレンスマニュアル”の“DTKTBLCV.EXE(ユーザー定義の移行)”を参照してください。

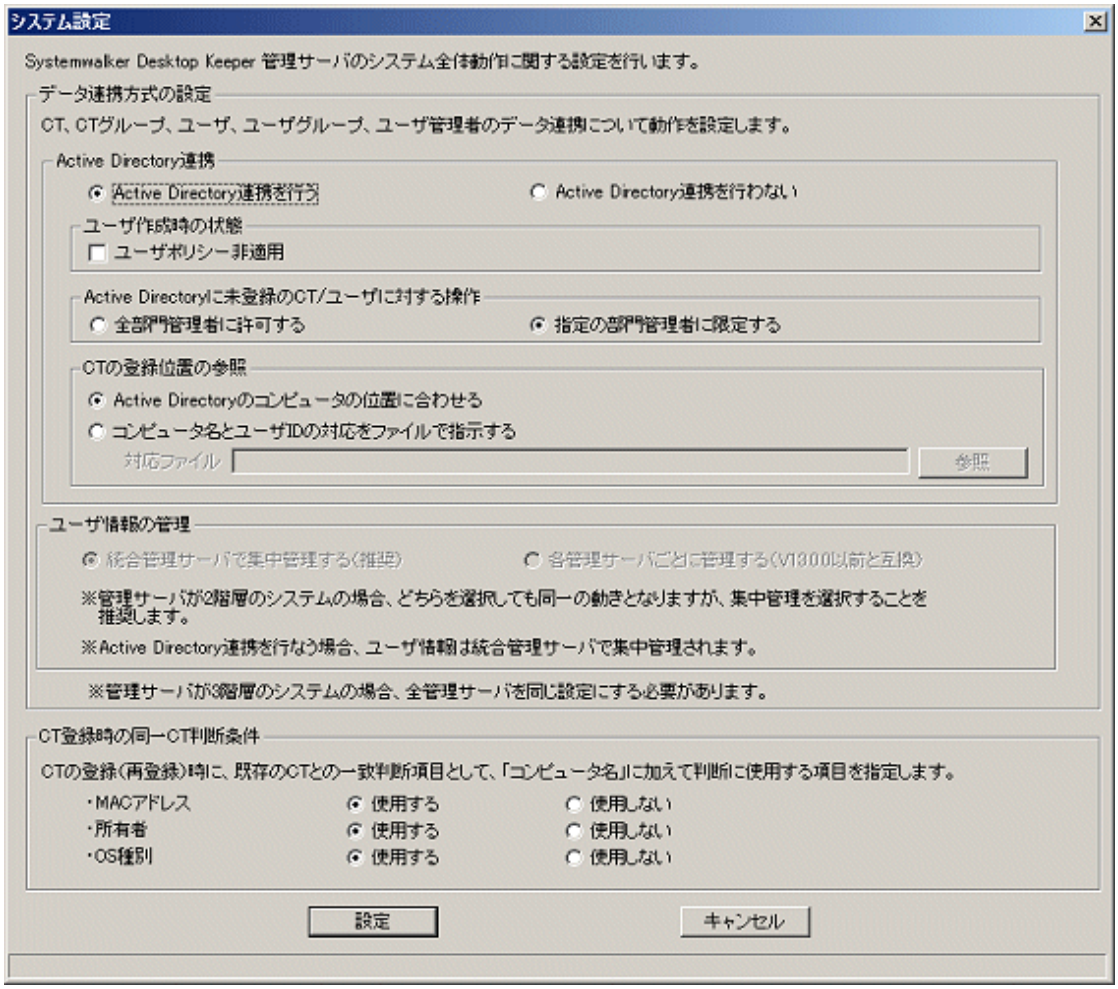
   各管理サーバで、同階層で同名のユーザーグループが存在する場合は、一元化後、ユーザーグループツリー上に同名のグループが作成されます。情報を管理しやすくするために、ユーザーの移動やユーザーグループの削除など、ユーザー情報を整理することを推奨します。

2. 統合管理サーバに接続されている管理コンソールで、移行後のユーザー情報を管理します。

   a. 統合管理サーバのサービスを停止します。

   b. サーバ設定ツールを起動し、[システム設定]ボタンをクリックします。

      →[システム設定]画面が表示されます。



   c. [Active Directory連携]で[Active Directory連携を行わない]を選択します。

   d. [ユーザー情報の管理]で[統合管理サーバで集中管理する]を選択します。

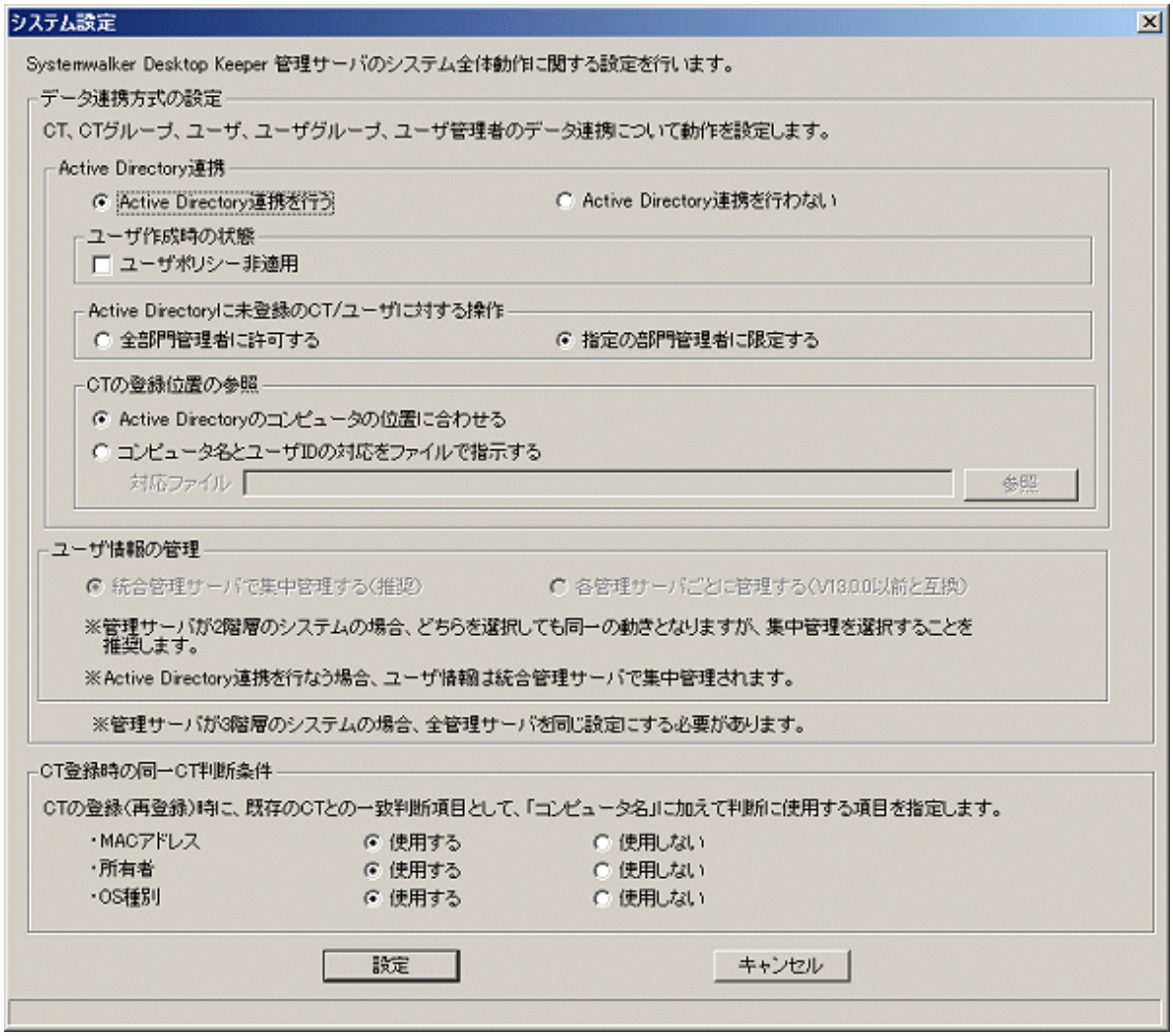
   e. [設定]ボタンをクリックします。

   f. サービスを起動します。

統合管理サーバでの一元管理から各管理サーバでの管理に変更する場合

1. 統合管理サーバのサービスを停止します。
2. サーバ設定ツールを起動し、[システム設定]ボタンをクリックします。

   →[システム設定]画面が表示されます。



3. [Active Directory連携]で[Active Directory連携を行わない]を選択します。
4. [ユーザー情報の管理]で[各管理サーバごとに管理する]を選択します。
5. [設定]ボタンをクリックします。
6. サービスを起動します。

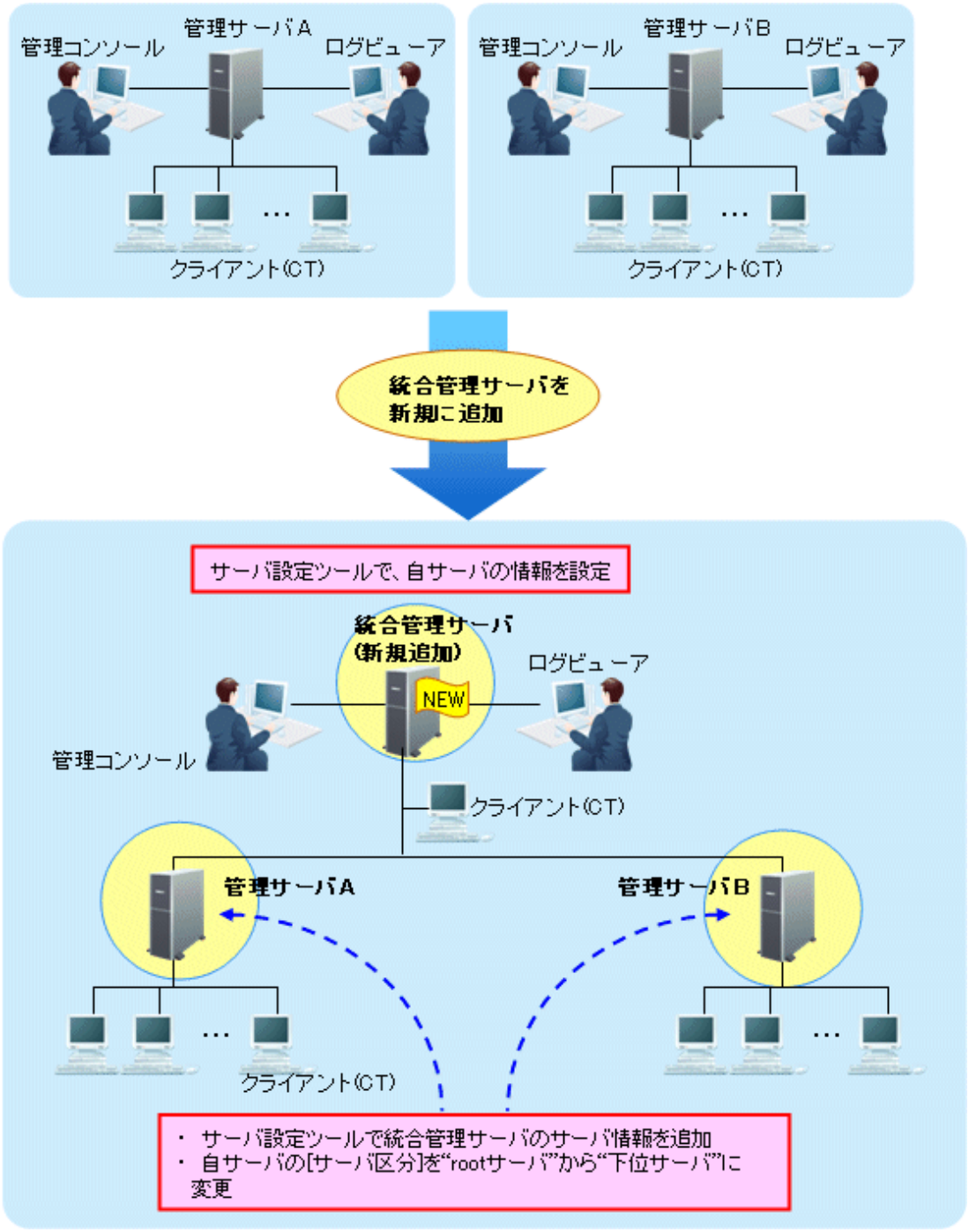
移行後のユーザー情報の管理は、各管理サーバに接続されている管理コンソールで実施します。

7.3 システム構成を2階層から3階層へ変更する

システム構成の2階層から3階層への変更について、以下の2とおりの方法を説明します。

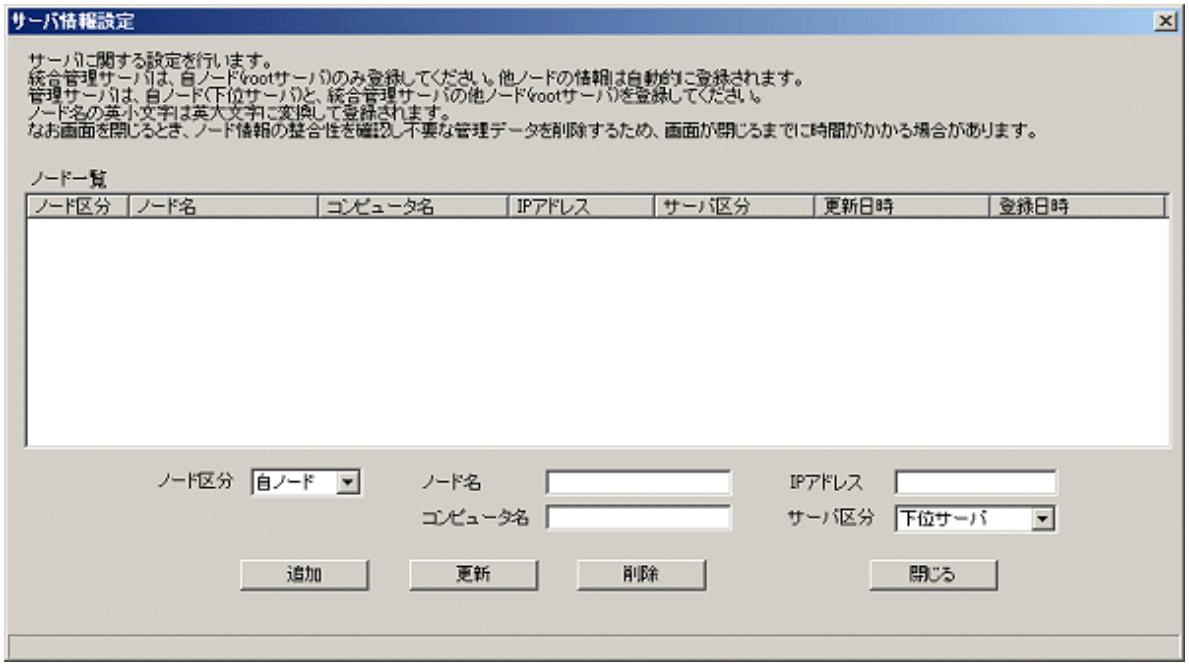
- 統合管理サーバを新規に追加する場合
- 既存の管理サーバを統合管理サーバに変更する場合

統合管理サーバを新規に追加する場合



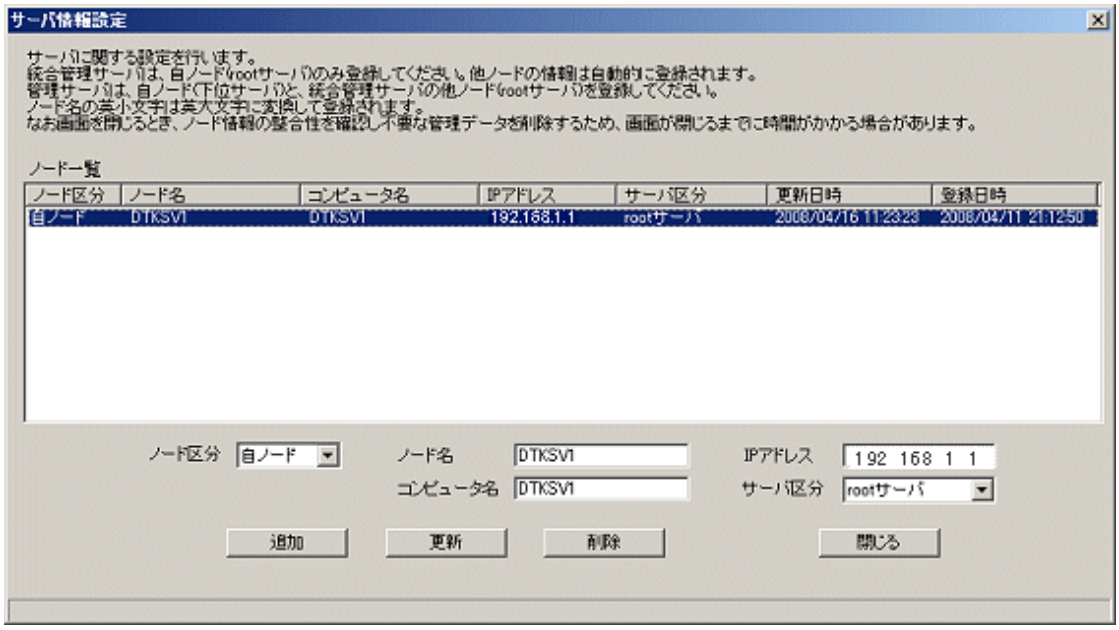
1. 統合管理サーバを新規に構築します。
   構築方法は、“Systemwalker Desktop Keeper 導入ガイド”の“導入”を参照してください。

   サーバ設定ツールの[サーバ情報設定]画面では、自サーバの情報を設定します。



2. 管理サーバ(管理サーバAおよび管理サーバB)の階層化サービスおよびサーバサービスを停止します。

3. 管理サーバにおいて、サーバ設定ツールの[サーバ情報設定]画面で、以下の情報を設定します。



   ー 自サーバの[サーバ区分]を“rootサーバ”から“下位サーバ”に変更します。

   ー 統合管理サーバの情報を追加します。
   設定項目の詳細は、“Systemwalker Desktop Keeper 導入ガイド”の“サーバ情報を設定する”を参照してください。

4. 統合管理サーバの階層化サービスおよびサーバサービスを起動します。

5. 管理サーバの階層化サービスおよびサーバサービスを起動します。

   →管理サーバのサービスが起動されると、統合管理サーバには、配下の管理サーバの情報が自動的に設定されます。

6. 統合管理サーバ直下にクライアント(CT)を接続する場合は、以下のどちらかの操作を実施します。

   ー PCにCTを新規インストールします。
   インストール方法は、“Systemwalker Desktop Keeper 導入ガイド”の“CTをインストールする”を参照してください。

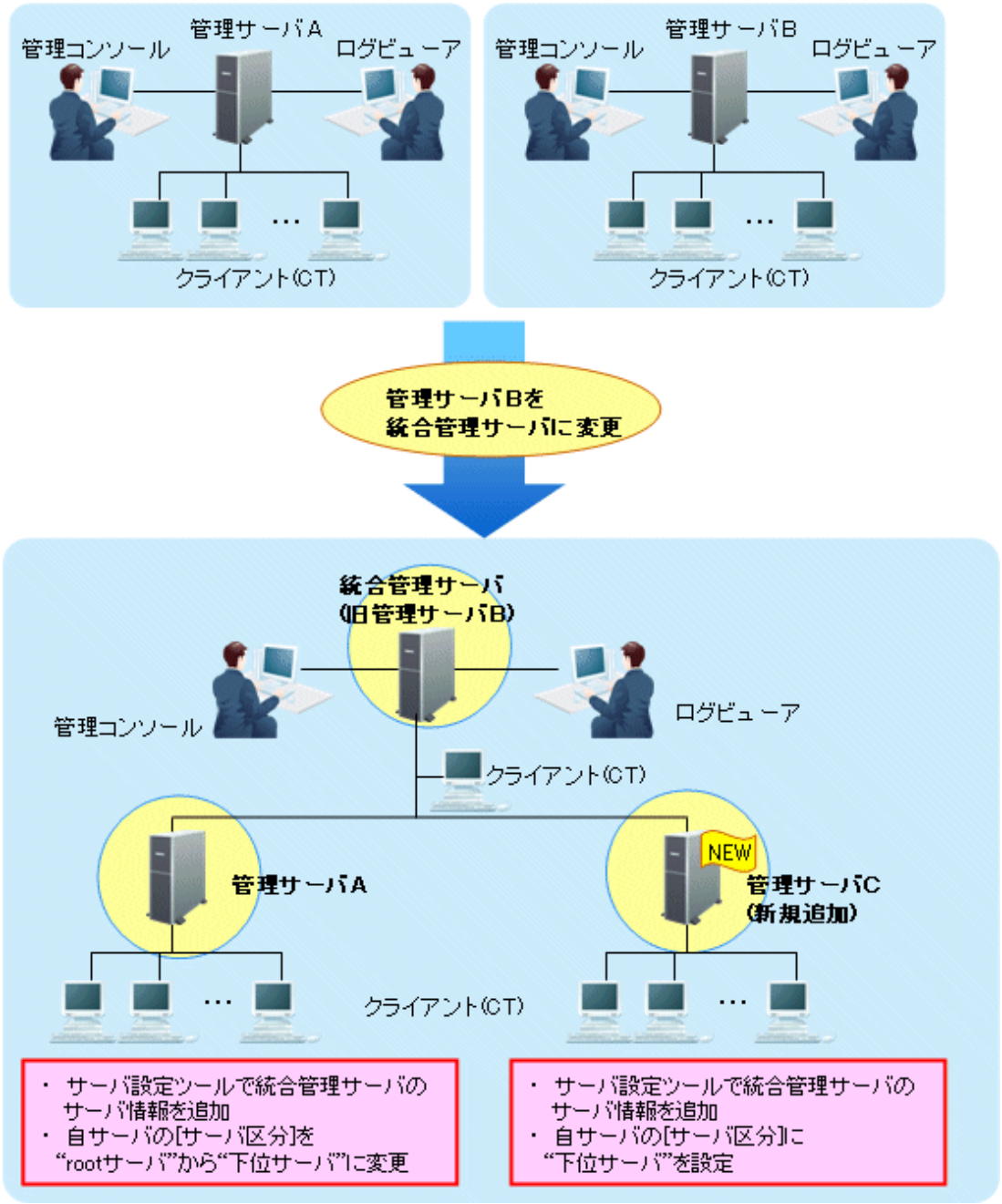
   ー 既存のクライアント(CT)環境を変更します。
   変更方法は、“7.7.1 接続先の管理サーバ/統合管理サーバを変更する”を参照してください。

7. ログビューア環境および管理コンソール環境を設定します。
   以下のどちらかの操作を実施します。

   ー 管理コンソールを新規にインストールします。
   インストール方法は、“Systemwalker Desktop Keeper 導入ガイド”の“管理コンソールをインストールする”を参照してください。

   ー ログビューアや管理コンソールの、既存の環境を変更します。
   変更方法は、“7.8 管理コンソール環境を変更する”または“ログビューアを起動する”を参照してください。

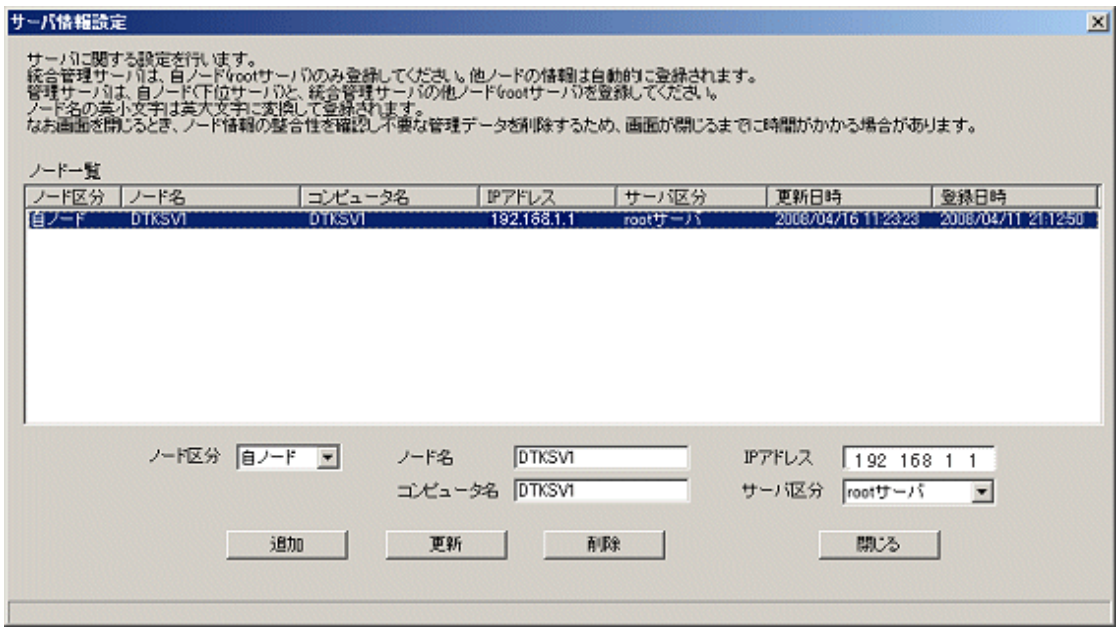
既存の管理サーバを統合管理サーバに変更する場合



統合管理サーバ(旧管理サーバB)は、管理サーバBでのサーバ情報をそのまま利用できるため、変更操作は不要です。
(管理サーバBでは、[サーバ区分]に[root]が設定されています。統合管理サーバに変更しても、[サーバ区分]は同じだからです。)

1. 統合管理サーバ(旧管理サーバB)および管理サーバAの、階層化サービスおよびサーバサービスを停止します。

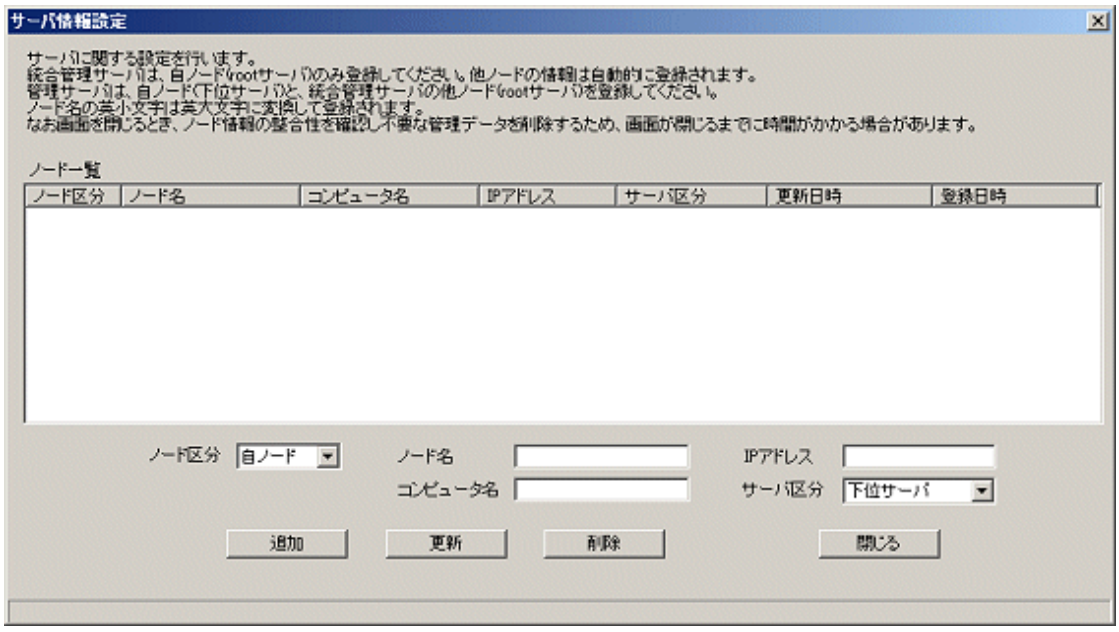
2. 管理サーバAにおいて、サーバ設定ツールの[サーバ情報設定]画面で、以下の情報を設定します。



- 自サーバの[サーバ区分]を“rootサーバ”から“下位サーバ”に変更します。
- 統合管理サーバの情報を追加します。
  設定項目の詳細は、“Systemwalker Desktop Keeper 導入ガイド”の“サーバ情報を設定する”を参照してください。

3. 管理サーバCを新規に構築します。
   構築方法は、“Systemwalker Desktop Keeper 導入ガイド”の“導入”を参照してください。

   サーバ設定ツールの[サーバ情報設定]画面では、以下の情報を設定します。



- 統合管理サーバの情報を追加します。
  設定項目の詳細は、“Systemwalker Desktop Keeper 導入ガイド”の“サーバ情報を設定する”を参照してください。
- 自サーバの[サーバ区分]に“下位サーバ”を設定します。

4. 統合管理サーバの階層化サービスおよびサーバサービスを起動します。

5. 管理サーバAおよび管理サーバCの階層化サービスおよびサーバサービスを起動します。

   →管理サーバのサービスが起動されると、統合管理サーバには、配下の管理サーバの情報が自動的に設定されます。

6. 統合管理サーバ直下にクライアント(CT)を接続する場合は、以下のどちらかの操作を実施します。

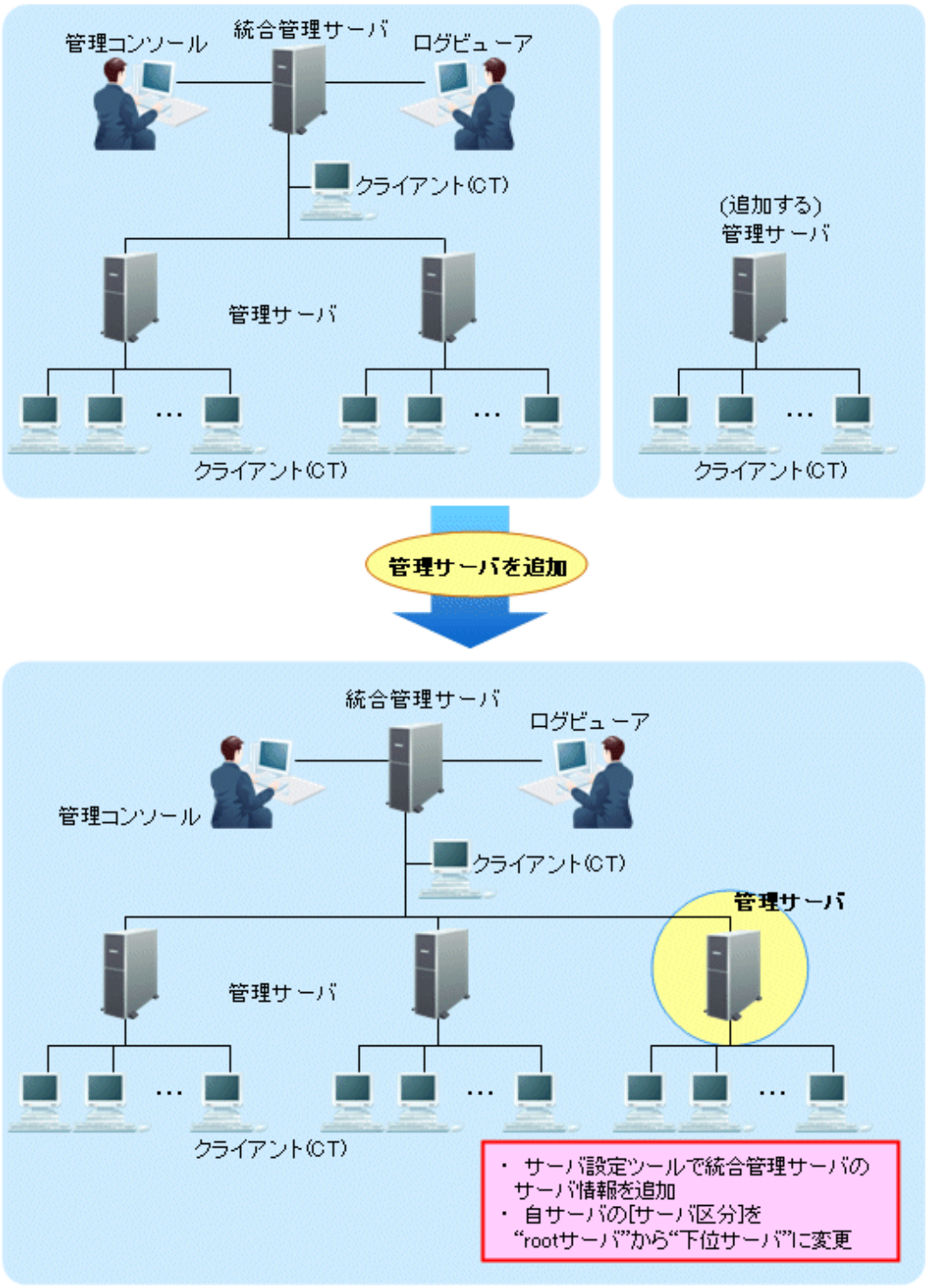
   ー PCにCTを新規インストールします。
   インストール方法は、“Systemwalker Desktop Keeper 導入ガイド”の“CTをインストールする”を参照してください。

   ー 既存のクライアント(CT)環境を変更します。
   変更方法は、“7.7.1 接続先の管理サーバ/統合管理サーバを変更する”を参照してください。

7.4 3階層のシステム構成で管理サーバを追加/削除する

管理サーバを追加する

3階層のシステム構成に管理サーバを追加する手順を説明します。

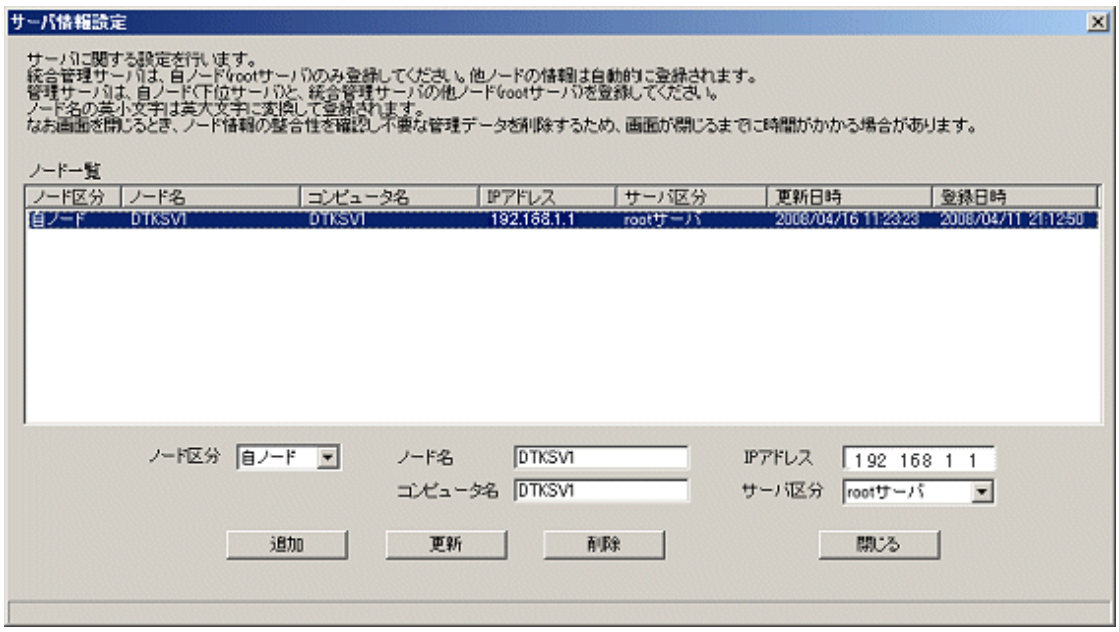


1. 統合管理サーバでユーザー情報を一元管理している場合は、追加する管理サーバのユーザー情報を、統合管理サーバに移行します。

   ユーザー情報の移行は、DTKTBLCV.EXE(ユーザー定義の移行)コマンドを使用します。
   詳細は、“Systemwalker Desktop Keeper リファレンスマニュアル”の“DTKTBLCV.EXE(ユーザー定義の移行)”を参照してください。

2. 追加する管理サーバの階層化サービスおよびサーバサービスを停止します。

3. 追加した管理サーバにおいて、サーバ設定ツールの[サーバ情報設定]画面で、以下の情報を設定します。



- 自サーバの[サーバ区分]を“rootサーバ”から“下位サーバ”に変更します。
- 統合管理サーバの情報を追加します。
  設定項目の詳細は、“Systemwalker Desktop Keeper 導入ガイド”の“サーバ情報を設定する”を参照してください。

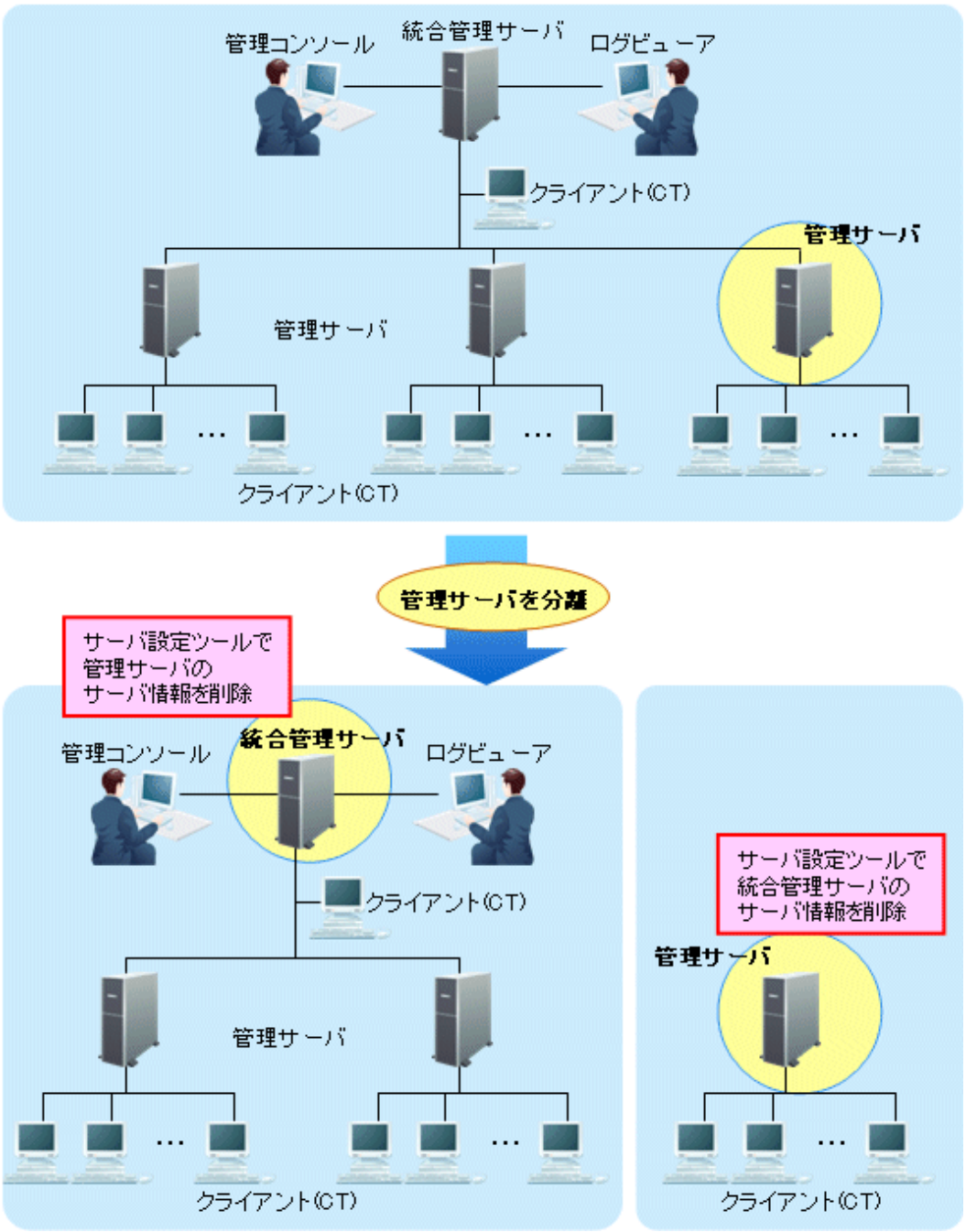
4. 追加した管理サーバの階層化サービスおよびサーバサービスを起動します。

   →管理サーバのサービスが起動されると、統合管理サーバには、追加した管理サーバの情報が自動的に設定されます。

管理サーバを削除する

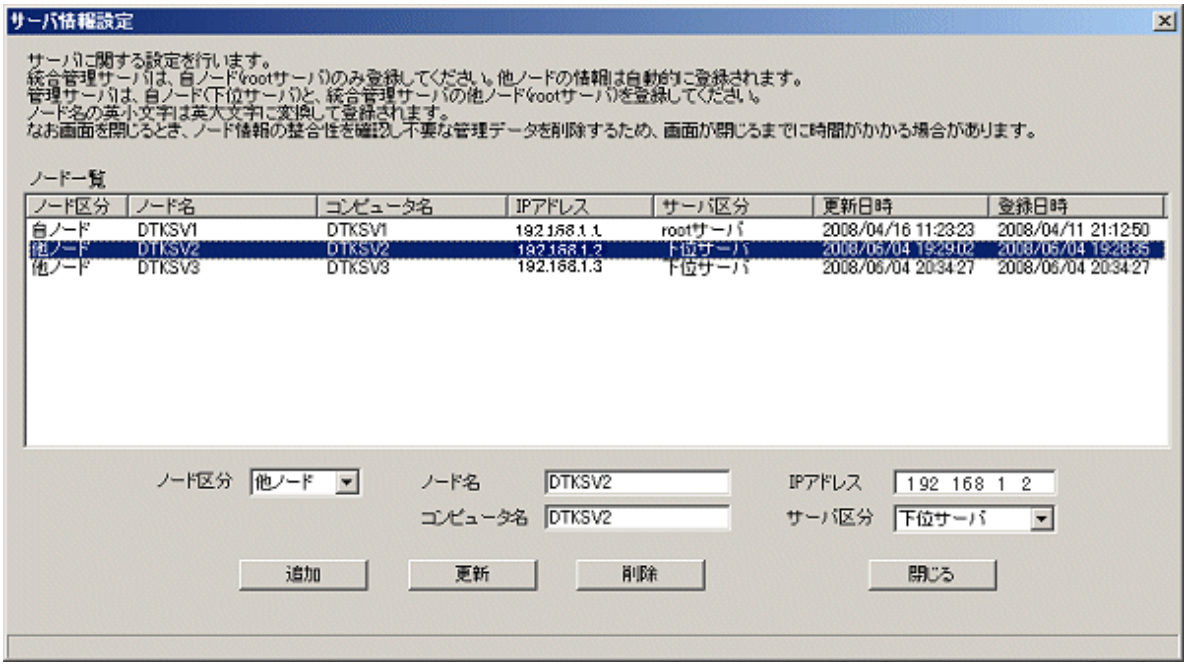
管理サーバで統合管理サーバのサーバ情報を削除した場合は、統合管理サーバでも、管理サーバのサーバ情報を削除してください。
統合管理サーバで管理サーバのサーバ情報を削除した場合は、管理サーバでも、統合管理サーバのサーバ情報を削除してください。

以下に、互いに相手のサーバ情報を削除する例を示します。

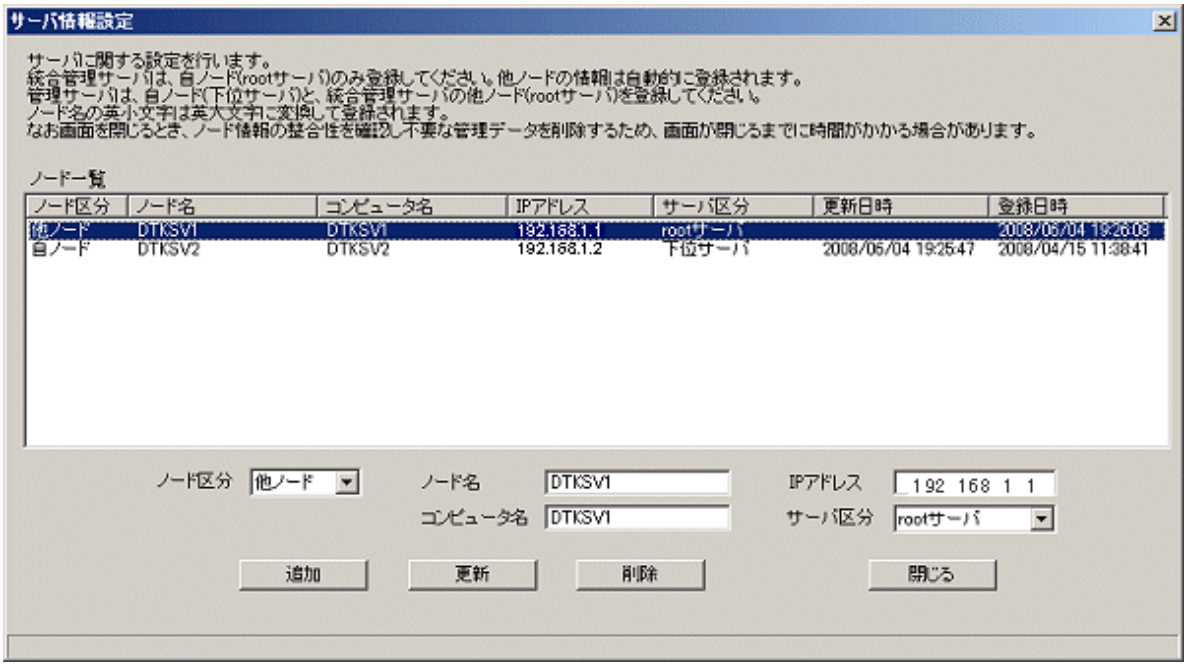


1. 統合管理サーバおよび分離する管理サーバの、階層化サービス、サーバサービスを停止します。

2. 統合管理サーバにおいて、サーバ設定ツールの[サーバ情報設定]画面で、分離した管理サーバを選択し、[削除]ボタンをクリックします。



3. 分離した管理サーバにおいて、サーバ設定ツールの[サーバ情報設定]画面で、以下の情報を設定します。



- 統合管理サーバ(他ノード)を選択し、[削除]ボタンをクリックします。
- 自サーバの[サーバ区分]を“下位サーバ”から“rootサーバ”に変更します。

4. 管理サーバ、統合管理サーバの順に、階層化サービスおよびサーバサービスを起動します。

7.5 指定したUSBデバイスだけにファイルを持ち出す

情報漏洩のリスクを低くするため、持出しユーティリティや、エクスプローラなどからファイルやフォルダを持出す場合に、使用できるUSBデバイスを個別に制限することができます。
使用を許可するUSBデバイスは、管理コンソールでポリシー設定します。
これらの手順は、“USBデバイスを登録する”および“使用を許可するUSBデバイスをポリシーに設定する”を参照してください。

持出しユーティリティから持出された情報、使用した媒体、持出し日時、持出した人物などは、ファイル持出しログとして採取されます。
エクスプローラなどから持出された情報、使用した媒体、持出し日時、持出した人物などは、ファイル操作ログとして採取されます。
また、USBデバイスを個別に使用制限する場合、使用許可されていないUSBデバイス(リムーバブルと認識するものに限る)を装着したとき、「違反」としてデバイス構成変更ログに記録されます。この情報は、管理者へメール通知することができます。また、イベントログとして記録できます。

登録したUSBデバイス情報は、CSVファイルに出力できます。以下の用途があります。

- 登録済みのUSBデバイスを確認する
- 登録済みのUSBデバイス情報を別の管理サーバに移行する
- 登録済みのUSBデバイス情報を変更する
- 登録済みのUSBデバイス情報を削除する

手順は、“登録されているUSBデバイス情報をCSVファイルに出力する”および“登録されているUSBデバイス情報を変更する”を参照してください。

運用例

管理者が使用を許可したUSBデバイスだけを使用して、ファイルの持出しや読み込みを行う場合の、運用例を説明します。

運用例1:ファイル持出しはすべて禁止・許可されたUSBデバイスのファイルだけ参照可能とする

USBデバイスへのファイル持出しは一切禁止しますが、業務上必要として許可されたUSBデバイスに格納されているファイルの持込、参照は、許可したい場合です。

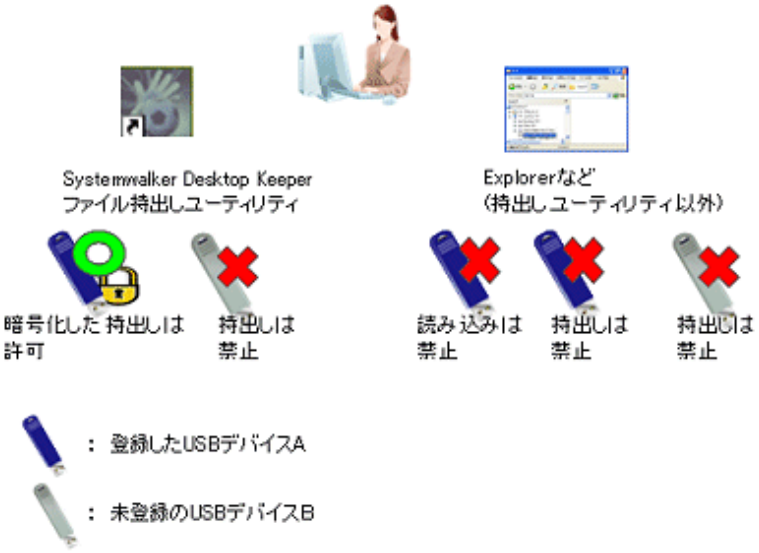
この運用は、以下の設定により実現できます。

持出しユーティリティを使用した持出しを禁止します。また、エクスプローラなど(持出しユーティリティ以外)を使用した持出しも禁止します。エクスプローラなど(持出しユーティリティ以外)を使用した読み込みだけ許可します。

ポリシーの設定については、“運用例1のポリシー設定”を参照してください。

運用例2:許可されたUSBデバイスを、ファイル持出しユーティリティに限定して使用する

ファイル持出しは、持出しユーティリティを使用して暗号化した場合だけ許可します。また、管理者が想定していないソフトウェアなどを、外部から持ち込む(コピー)ことを禁止するため、エクスプローラなど(持出しユーティリティ以外)からは、USBデバイスへのアクセスを禁止したい場合です。



この運用は、以下の設定により実現できます。

持出しユーティリティを使用し、暗号化しての持出しだけを許可します。エクスプローラなど(持出しユーティリティ以外)を使用した持出しや読み込みは禁止します。

ポリシーの設定については、“運用例2のポリシー設定”を参照してください。

運用例3:許可されたUSBデバイスへのファイル持出しは、ファイル持出しユーティリティに限定し、許可されたUSBデバイスからの読み込みはエクスプローラで可能にする

ファイル持出しは、持出しユーティリティを使用して暗号化した場合だけ許可します。エクスプローラなど(持出しユーティリティ以外)からは、読み込みだけ許可したい場合です。

この運用は、以下の設定により実現できます。

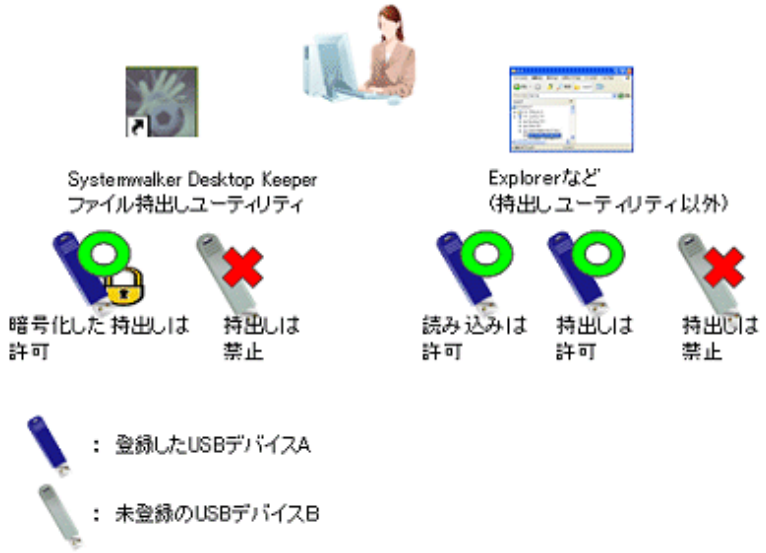
持出しユーティリティを使用し、暗号化しての持出しだけを許可します。エクスプローラなど(持出しユーティリティ以外)を使用した読み込みは許可しますが、持出しは禁止します。

ポリシーの設定については、“運用例3のポリシー設定”を参照してください。

運用例4:許可されたUSBデバイス(ロック機能や暗号化機能を持つ)に対して、エクスプローラなどを使用した自由な持出しを許可する

ロック機能や暗号化機能を持つUSBデバイスはセキュリティ機能があるため、利便性を考慮しエクスプローラなど(持出しユーティリティ以外)を使用しての持出しを許可したい場合です(ファイル持出しユーティリティを使用せず、USBデバイスに装備されているセキュリティ機能を使用します)。
または、許可されたUSB接続の外付けHDDに対して、バックアップを取得したい場合です。

運用例4では、ファイル持出しユーティリティを使用せず、エクスプローラなど(持出しユーティリティ以外)からUSBデバイスにファイルをコピーできます。ただし、ファイル持出しユーティリティを使用していないため、ファイル持出しログの取得や、持出したファイルの原本を保管することはできません。USBデバイスへのアクセスは、ファイル操作ログを取得することにより確認できます。
ファイル持出しログの取得や、持出したファイルの原本を保管する場合は、ファイル持出しユーティリティの設定を行い、ファイル持出しユーティリティからファイル持出しを行う運用にしてください。



この運用は、以下の設定により実現できます。

エクスプローラなど(持出しユーティリティ以外)を使用した持出しも読み込みも許可します。

※ 持出しユーティリティに関する設定は必須ではありませんが、ファイル持出しログの取得や、持出したファイルの原本を保管したい場合も考慮し、上記の図では設定する例となっています。

ポリシーの設定については、“運用例4のポリシー設定”を参照してください。

USBデバイスを登録する

登録は、システム管理者または部門管理者が行います。
サーバ設定ツールの[管理者情報設定]画面の[詳細権限]で、[USBデバイス登録/更新/削除]権限が設定されている必要があります。

登録は、管理コンソールで行います。
3階層のシステム構成の場合は、統合管理サーバに接続する管理コンソールで登録します。ユーザー情報の一元管理の実施には関係ありません。

登録可能なUSBデバイスは、10,000個です。
以下の条件をすべて満たすUSBデバイスを登録できます。

- USBインタフェースである(USBインタフェースでも、CD/DVD-R/RW装置などは登録できません)
- ドライブ種別がリムーバブルと識別されるデバイスである

・ メーカーID/製品ID/内部シリアル番号、または、メーカーID/製品IDが、USB装置から取得できる

登録できるUSBデバイスの例は、以下のとおりです。

USBデバイス	説明および注意
USBフラッシュメモリ	USB-HUB経由も登録できます。
USBハードディスク	USB-HUB経由も登録できます。
USBカードリーダ/ライタ経由SDカード、など	装置自身を登録可能なUSBデバイスとして認識します。装着したメモリ媒体を個々に認識することはできません。
USBフロッピーディスク装置	装置自身を登録可能なUSBデバイスとして認識します。装着したフロッピーメディアを個々に認識することはできません。
USB MO装置	装置自身を登録可能なUSBデバイスとして認識します。装着したMOメディアを個々に認識することはできません。

登録したデバイス情報は、ポリシーに「許可デバイス」として設定後、CTポリシーまたはユーザーポリシーとして配信することができます。

登録する

[USBデバイス登録]画面で1個ずつ登録します。1つのUSBデバイスに対して、1件登録します。

注意

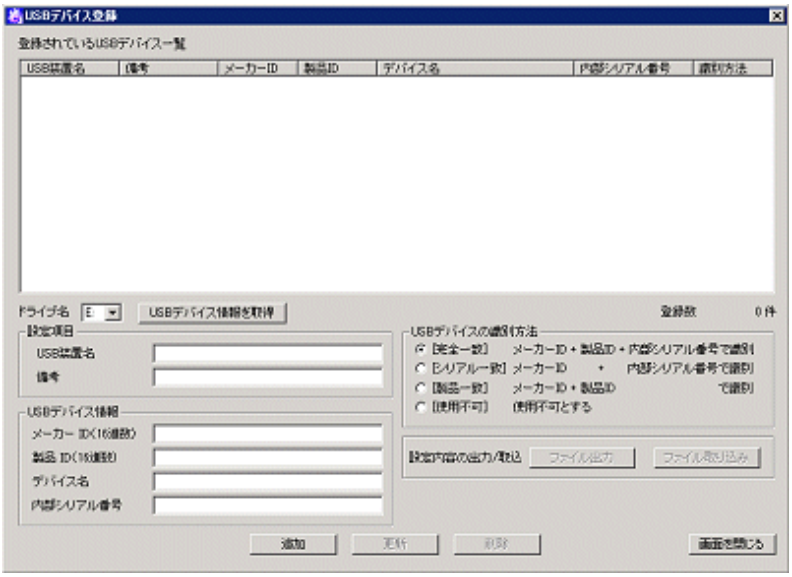
管理コンソールのOSがWindows® 2000の場合について

管理コンソールのOSがWindows® 2000の場合、ユーザー権限のユーザーでは認証機能付きのUSBデバイスを登録することができません。

以下に手順を示します。

1. [管理コンソール]を起動します。
2. [動作設定]メニューから[USBデバイス登録]を選択します。

   →[USBデバイス登録]画面が表示されます。



項目名		説明
[登録されているUSBデバイス一覧]		登録されているUSBデバイスの内容が表示されます。
[ドライブ名]		[USBデバイス情報を取得]ボタンによりUSBデバイス情報を読み込む場合、そのデバイスが装着されているドライブを選択します。 **初期値:**Cドライブ以降で、最初のデバイス未接続のドライブです。
[USBデバイス情報を取得]		クリックすると、指定されたドライブに挿入されているUSBデバイスから情報を読み込みます。
[設定項目]	[USB装置名]	半角で80文字まで入力できます。ただし、以下の文字は入力できません。 ・制御コード ・UNICODE文字 ・半角空白のみ、または、全角空白のみ(半角空白または全角空白を、先頭または最後尾に設定した場合は、その空白は削除されます) 本項目は、必ず入力してください。
	[備考]	半角で128文字まで入力できます。ただし、以下の文字は入力できません。 制御コード、UNICODE文字
[USBデバイス情報]	[メーカー ID] [製品 ID] [デバイス名] [内部シリアル番号]	読み込んだUSBデバイス情報が表示されます。
[USBデバイスの識別方法]	持出しユーティリティを使用してUSBデバイスにファイルを持ち出すときに、許可されたUSBデバイスかどうかを識別する方法です。	
	[完全一致] **(初期値)**	メーカーID + 製品ID + 内部シリアル番号で識別します。 [USBデバイスの識別方法]が[完全一致]で、[メーカーID]、[製品ID]、[内部シリアル番号]の3項目が一致する媒体が、[完全一致]ですでに登録されている場合、登録することができません。
	[シリアル一致]	メーカーID + 内部シリアル番号で識別します。 [登録されているUSBデバイス一覧]において、[製品ID]の背景色がグレーで表示されます。 認証機能付きのUSBデバイスで、認証前と認証後で製品IDが変化するもの(※)を登録する場合に、本項目を選択します。
	[製品一致]	メーカーID + 製品IDでUSBデバイスを識別します。 [登録されているUSBデバイス一覧]において、[内部シリアル番号]が、グレーアウトされます。
	[使用不可]	登録されたUSBデバイスを、一時的に使用できない設定とします。 使用許可されたUSBデバイスとしてポリシーに設定されている場合も使用できなくなります。 以下のような場合に本項目を選択します。 【例】 ・いずれ使用可能とするが、今は登録だけ実施するとき ・一時的に遊休資産となり、利用者がいないとき ・該当USBデバイスが紛失したとき [登録されているUSBデバイス一覧]において、その行全体が、グレイアウトされます。

項目名		説明
[設定内容の出力/取込]	[ファイル出力]	[USBデバイス情報出力ファイル指定]画面が表示されます。 USBデバイス情報のCSV出力条件を設定し、出力します。
	[ファイル取り込み]	[USBデバイス情報取り込みファイル指定]画面が表示されます。 USBデバイス情報を別の管理サーバに移行する場合に使用します。
[追加]		USBデバイスを登録します。 10,000個まで登録できます。
[更新]		USBデバイス情報を更新します。
[削除]		登録されているUSBデバイスを削除します。

※) あらかじめ、認証前または認証後のどちらの状態で登録するか、決めておくことをお勧めします。
認証前後で[USBデバイス情報を取得]ボタンをクリックし、[USBデバイス情報]に表示される[製品ID]だけが変化することを確認してください。

3. 登録するUSBデバイスを、管理コンソールのPCに挿入します。
4. [ドライブ名]で、PCが認識したドライブを選択し、[USBデバイス情報を取得]ボタンをクリックします。

   →[USBデバイス情報]に、挿入されているUSBデバイスの情報が表示されます。
   媒体からUSBデバイス情報を読み込めない場合は、登録できません。
5. [USBデバイスの識別方法]を選択します。
6. [USB装置名]、[備考]を入力します。

   登録情報は、3階層の場合は統合管理サーバで保存し、2階層の場合は管理サーバ単位で保存し、配下の複数部門の情報が混在します。このため、ポリシー設定時は、自部門で許可するUSBデバイスを、大量の登録情報の中から選択することが予想されます。[登録されているUSBデバイス一覧]に表示される各項目はソートできますが、[備考]に部門や利用者名などの識別情報を設定し、選択しやすくすることを推奨します。
7. [追加]ボタンをクリックします。

   →[登録されているUSBデバイス一覧]に登録内容が表示されます。

変更する

1. [管理コンソール]を起動し、[USBデバイス登録]画面を表示します。
2. [登録されているUSBデバイス一覧]で、更新するUSBデバイスを選択します。

   →登録内容が表示されます。
3. 該当する項目を更新し、[更新]ボタンをクリックします。

   →[登録されているUSBデバイス一覧]に更新内容が反映されます。

削除する

1. [管理コンソール]を起動し、[USBデバイス登録]画面を表示します。
2. [登録されているUSBデバイス一覧]で、削除するUSBデバイスを選択します。

   →登録内容が表示されます。
   情報を削除する場合は、[備考]の部門や利用者名などの識別情報も参考に、自部門のUSBデバイス情報であることを確認してから実施してください。
3. [削除]ボタンをクリックします。

   →[登録されているUSBデバイス一覧]から情報が削除されます。

使用を許可するUSBデバイスをポリシーに設定する

ポリシー設定は、システム管理者または部門管理者が行います。

運用例で説明した、運用例1～運用例4のポリシー設定を以下に説明します。

運用例1のポリシー設定

[ファイル持出し禁止]タブで以下を設定します。

ー [持出しユーティリティ]

- [ファイル持出しユーティリティを使用しての持出し]で[不可]を選択します。

ー [Explorer]

- [ファイルアクセス制御]で[する]を選択します。
- [読み込み禁止]([リムーバブルドライブの読み込み])で[禁止する]を選択します。
- [持出し禁止]の[ドライブ種別指定]で[リムーバブル]をチェックします。

ー [USBデバイス個体識別機能]

- [利用する]を選択します。
- [ファイル持出し禁止 - USBデバイス個体識別機能 - 詳細設定]画面で、[読み込み専用]を選択します。

運用例2のポリシー設定

[ファイル持出し禁止]タブで以下を設定します。

ー [持出しユーティリティ]

- [ファイル持出しユーティリティを使用しての持出し]で[可]を選択します。
- [暗号化持ち出しのみ可]をチェックします。

ー [Explorer]

- [ファイルアクセス制御]で[する]を選択します。
- [読み込み禁止]([リムーバブルドライブの読み込み])で[禁止する]を選択します。
- [持出し禁止]の[ドライブ種別指定]で[リムーバブル]をチェックします。

ー [USBデバイス個体識別機能]

- [利用する]を選択します。
- [ファイル持出し禁止 - USBデバイス個体識別機能 - 詳細設定]画面で、[読み書き可能]を選択します。
- [ファイル持出し禁止 - USBデバイス個体識別機能 - 詳細設定]画面で、[読み書きともファイル持出しユーティリティに限定]をチェックします。

運用例3のポリシー設定

[ファイル持出し禁止]タブで以下を設定します。

ー [持出しユーティリティ]

- [ファイル持出しユーティリティを使用しての持出し]で[可]を選択します。
- [暗号化持ち出しのみ可]をチェックします。

ー [Explorer]

- [ファイルアクセス制御]で[する]を選択します。
- [読み込み禁止]([リムーバブルドライブの読み込み])で[禁止する]を選択します。
- [持出し禁止]の[ドライブ種別指定]で[リムーバブル]をチェックします。

ー [USBデバイス個体識別機能]

- [利用する]を選択します。
- [ファイル持出し禁止 - USBデバイス個体識別機能 - 詳細設定]画面で、[読み書き可能]を選択します。
- [ファイル持出し禁止 - USBデバイス個体識別機能 - 詳細設定]画面で、[書き込みはファイル持出しユーティリティに限定]をチェックします。

運用例4のポリシー設定

[ファイル持出し禁止]タブで以下を設定します。

ー [持出しユーティリティ]

- [ファイル持出しユーティリティを使用しての持出し]で[可]を選択します。
- [暗号化持ち出しのみ可]をチェックします。

ー [Explorer]

- [ファイルアクセス制御]で[する]を選択します。
- [読み込み禁止]([リムーバブルドライブの読み込み])で[禁止する]を選択します。
- [持出し禁止]の[ドライブ種別指定]で[リムーバブル]をチェックします。

ー [USBデバイス個体識別機能]

- [利用する]を選択します。
- [ファイル持出し禁止 - USBデバイス個体識別機能 - 詳細設定]画面で、[読み書き可能]を選択します。配下のチェックボックスは、どれもチェックしません。

また、USBデバイス個体識別機能を使用した場合に、デバイス構成変更ログが「違反」として採取されるのは、以下のどちらかのパターンでポリシーを設定し、[使用可能USBデバイス一覧]画面に登録されていないUSBデバイスを装着したときです。

ここでは、デバイス構成変更ログが「違反」として採取される条件だけを説明しています。上記の運用例1～運用例4とは対応していません。

- パターン1
  - ー [ファイル持出し禁止]タブで、[USBデバイス個体識別機能]を[利用する]と選択したとき。
  - ー [ファイル持出し禁止]タブで、[持出し禁止]を[禁止する](ドライブ指定またはリムーバブルを指定)と選択したとき。
- パターン2
  - ー [ファイル持出し禁止]タブで、[USBデバイス個体識別機能]を[利用する]と選択したとき。
  - ー [ファイル持出し禁止]タブで、[持出し禁止]を設定しないとき。
  - ー [ファイル持出し禁止]タブで、[ファイル持出しユーティリティを使用しての持出し]を[可]と選択したとき。

設定項目の詳細は、“2.4.1.2 [ファイル持出し禁止]タブの設定”を参照してください。

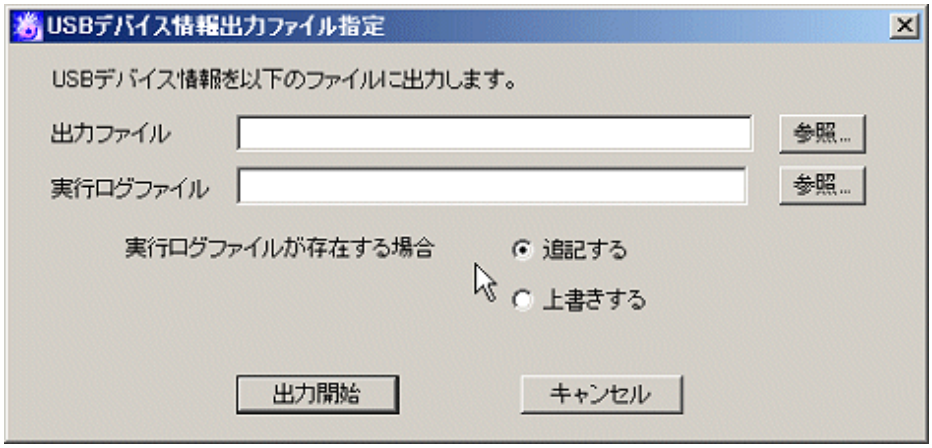
[次回起動時に更新する]ボタンまたは[即時更新を行う]ボタンをクリックして、ポリシーを設定します。
CTポリシーの場合は、CT起動時に反映されます。ユーザーポリシーの場合は、ログオン時に反映されます。
また、ポリシーの即時更新でも反映されます。

登録されているUSBデバイス情報をCSVファイルに出力する

1. [管理コンソール]を起動し、[USBデバイス登録]画面を表示します。

2. [ファイル出力]ボタンをクリックします。

   →[USBデバイス情報出力ファイル指定]画面が表示されます。



   - **[出力ファイル]**(必須):USBデバイス情報を出力するCSVファイルを、フルパスで指定します。

     半角で218文字まで入力できます。ただし、以下の記号はファイル名として使用できません。
     使用できない記号:「¥」「/」「:」「*」「?」「"」「<」「>」「|」

   - **[実行ログファイル]**(必須):実行結果を保存するファイルを、フルパスで指定します。

     半角で218文字まで入力できます。ただし、以下の記号はファイル名として使用できません。
     使用できない記号:「¥」「/」「:」「*」「?」「"」「<」「>」「|」

   - **[実行ログファイルが存在する場合]**:既存の実行ログファイルが存在する場合は必ず設定してください。
     [追記する]:既存の実行ログファイルに追記する場合に選択します。
     [上書きする]:既存の実行ログファイルに上書きする場合に選択します。

3. 上記の情報を設定し、[出力開始]ボタンをクリックします。

4. 出力が完了するとメッセージが表示されますので、[OK]ボタンをクリックします。

登録されているUSBデバイス情報を変更する

登録済みのUSBデバイス情報を出力したCSVファイルを利用して、以下の操作を行えます。

- 登録されているUSBデバイス情報の、USB装置名、備考、または識別方法を変更する
- 登録されているUSBデバイス情報を削除する
- USBデバイス情報を別の管理サーバに移行する

手順を以下に示します。

1. [ファイル出力]ボタンをクリックし、USBデバイス情報をCSVファイルに出力します。
   出力方法は、“登録されているUSBデバイス情報をCSVファイルに出力する”を参照してください。

2. 必要に応じてCSVファイルの内容を変更します。

   入力用CSVファイルは、テキストファイルとして編集してください。Microsoft® Excelなどのソフトウェアを使用して編集すると、ダブルクォーテーションなど必要な情報がなくなってしまうことがあります。

   手順1.で出力したCSVファイルの各行の1項目めは、空白になっています。この状態のまま、同じ管理サーバにUSBデバイス情報を取り込んだ場合、“新規”として情報が追加されます。識別方法に“製品一致”を指定している場合は、同じ情報が複数登録されます。したがって、登録情報の重複を避けるため、変更や削除を行わない行を削除してから、管理サーバに取り込むことを推奨します。

   CSVファイルの詳細は、“Systemwalker Desktop Keeper リファレンスマニュアル”の“USBデバイス一覧ファイル”を参照してください。

USB装置名、備考、または識別方法を変更する場合

a. 1項目目(処理フラグ)に“U”を指定します。

b. USB装置名、備考、または識別方法を変更します。CSVファイルを取り込むときは、全項目が記載されている必要があります。USB装置名、備考、または識別方法以外は、変更しないでください。

USBデバイス情報を削除する場合

a. 1項目目(処理フラグ)に“D”を指定します。

b. 2項目目(GUID)が指定されていることを確認します。

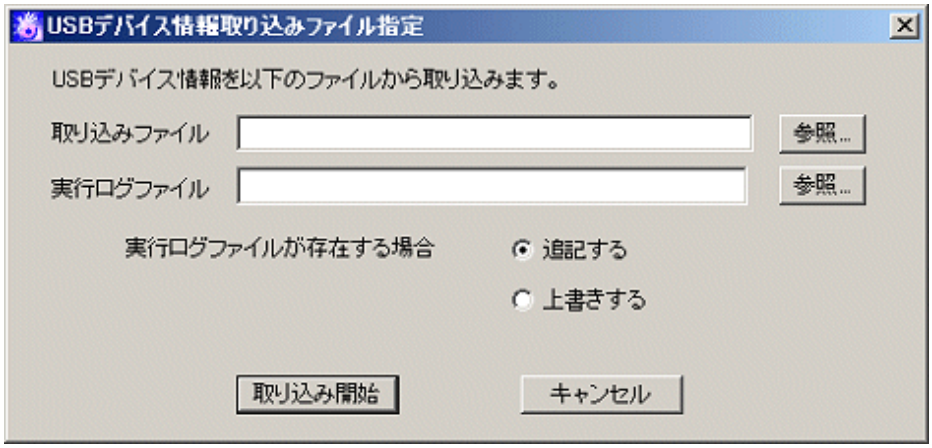
USBデバイス情報を別の管理サーバに移行する場合

移行後の管理サーバに登録するUSBデバイス情報を変更する場合は“USB装置名、備考、または識別方法を変更する場合”または“USBデバイス情報を削除する場合”を参照してください。

3. CSVファイルを保存します。

4. USBデバイス情報を取り込む管理サーバで、[ファイル取り込み]ボタンをクリックします。

→[USBデバイス情報取り込みファイル指定]画面が表示されます。



- **[取り込みファイル]**(必須):USBデバイス一覧ファイルを、フルパスで指定します。

  半角で218文字まで入力できます。ただし、以下の記号はファイル名として使用できません。
  使用できない記号:「¥」「/」「:」「*」「?」「"」「<」「>」「|」

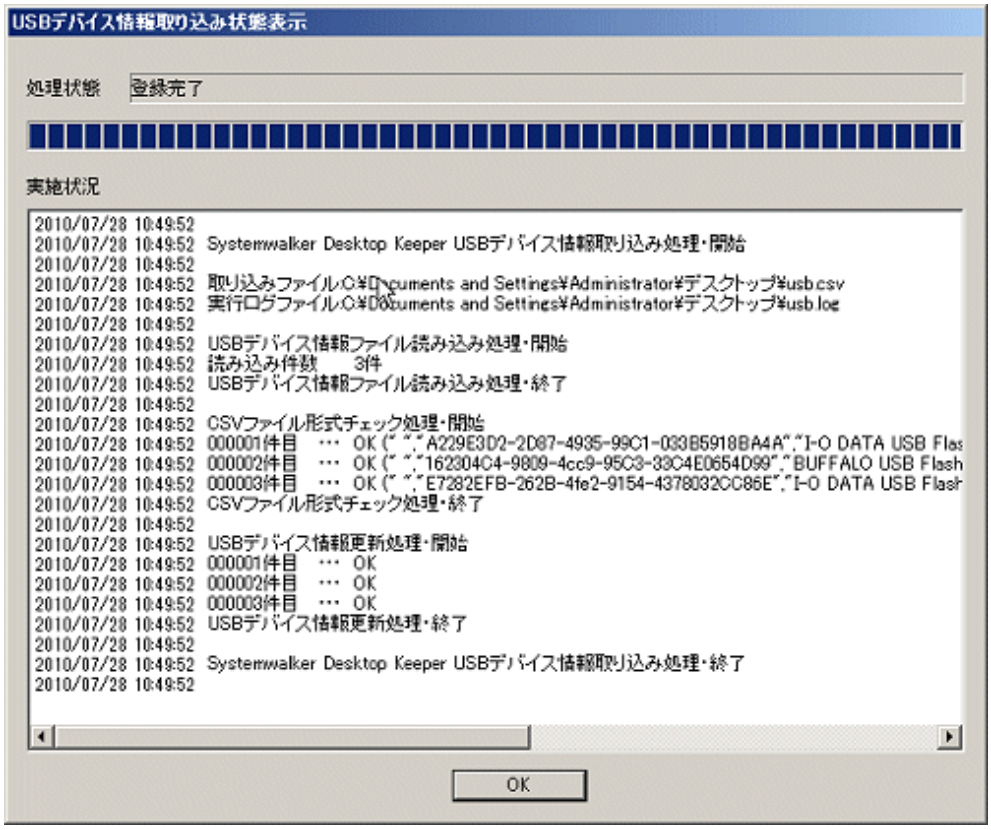
- **[実行ログファイル]**(必須):実行結果を保存するファイルを、フルパスで指定します。

  半角で218文字まで入力できます。ただし、以下の記号はファイル名として使用できません。
  使用できない記号:「¥」「/」「:」「*」「?」「"」「<」「>」「|」

- **[実行ログファイルが存在する場合]**:既存の実行ログファイルが存在する場合は必ず設定してください。
  [追記する]:既存の実行ログファイルに追記する場合に選択します。
  [上書きする]:既存の実行ログファイルに上書きする場合に選択します。

5. 上記の情報を設定し、[取り込み開始]ボタンをクリックします。

   →[USBデバイス情報取り込み状態表示]画面が表示されます。



6. USBデバイス情報の取り込みが終了すると、[処理状態]に「登録完了」と表示されます。[OK]ボタンをクリックします。

注意

取り込みに使用したCSVファイルは再利用できません

取り込みに使用したCSVファイルは再利用できません。CSVファイルを使用してUSBデバイス情報を変更する場合は、再度、手順1.のCSVファイルの出力から操作を行ってください。

7.6 ログの保存期間を変更する

ログの保存期間や、ログを退避するタイミングなどは、通常、システムの設計/導入時に設定される情報です。
しかし、採取されたログを定期的にバックアップする運用を開始後、当初の見積もりよりもログ量が多いなど、設定の変更が必要なときもあります。この場合、ログの保存期間と採取されるログの量の釣り合いが取れるように、ログの保存期間を変更できます。
変更方法には、以下の2とおりがあります。

- ログの定期的なバックアップを、バックアップツール(GUI)を使用して手動で実施している場合

  [Desktop Keeper バックアップツール]の[バックアップツール]画面で、[バックアップ対象期間]または[削除対象期間]を変更します。

- ログの定期的なバックアップを、タスクスケジューラを使用して自動で実施している場合

  登録されているコマンドのパラメーターで該当する期間を変更します。

ログの保存期間と退避するタイミングの考え方は、“Systemwalker Desktop Keeper 導入ガイド”の“ログの運用方法を決定する”を参照してください。

バックアップツールの設定項目の詳細、使用するコマンド、変更手順などは、“Systemwalker Desktop Keeper 導入ガイド”の“ユーザー資産を退避する”を参照してください。

7.7 CT環境を変更する

7.7.1 接続先の管理サーバ/統合管理サーバを変更する

以下のような運用環境の変更に伴う、接続先の(統合)管理サーバのIPアドレス、および代替(統合)管理サーバのIPアドレスの変更方法を説明します。

- 管理サーバを新規に構築し、旧管理サーバ配下の全クライアント(CT)を、新管理サーバに移動し管理する
- 管理サーバ配下の一部のクライアント(CT)を、別の既存管理サーバ配下に移動する
- 接続先の管理サーバ(代替管理サーバ)のIPアドレスを変更する
- 接続先の管理サーバ(代替管理サーバ)とクライアント(CT)両方のIPアドレスを変更する

接続先の管理サーバのIPアドレスを変更するには、以下の2とおりの方法があります。

- 管理サーバでファイルを使用して変更する

  設定を変更するクライアント(CT)のバージョンが、V14.0.0以降の場合に実施できます。
  “移行対象情報ファイル”を使用して、移行後の管理サーバのIPアドレスや、該当クライアント(CT)のIPアドレス、移行日時などを設定し、管理サーバに保存します。設定内容は、CTポリシーとしてクライアント(CT)に通知されます。通知後、PCを再起動すると、接続先管理サーバが変更されます。
  各クライアント(CT)で変更作業をする必要はありません。

  クライアント(CT)-管理サーバ間で通信を行うための通信ポート番号も同時に変更できます。

- クライアント(CT)でコマンドを使用して変更する

  設定を変更するクライアント(CT)がどのバージョンでも実施できます。
  各クライアント(CT)でコマンドを実行します。

管理サーバでファイルを使用して変更する

以下に、管理サーバで変更する方法を説明します。

管理サーバを新規に構築し、旧管理サーバ配下の全クライアント(CT)を、新管理サーバに移動し管理する

本変更方法の場合、旧管理サーバの管理情報とログを、新管理サーバへ移行します。したがって、新管理サーバへ移行後も、旧管理サーバで採取されたログを検索できます。

移行手順は、以下のとおりです。

1. 新しい管理サーバを構築します。手順の詳細は、“Systemwalker Desktop Keeper 導入ガイド”を参照してください。
2. 旧管理サーバに接続している管理コンソールを更新インストールし、新管理サーバのIPアドレスを追加します。手順の詳細は、“7.8 管理コンソール環境を変更する”を参照してください。
   これにより、管理コンソールを一時的に新旧両方の管理サーバに接続できます。
3. 旧管理サーバで、管理情報をバックアップします。
   管理情報については、“Systemwalker Desktop Keeper 導入ガイド”の“ユーザー資産”を参照してください。
4. 新管理サーバに、管理情報をリストアします。
5. 新管理サーバのサーバ設定ツールの[サーバ情報設定]画面で、サーバ情報(コンピュータ名、IPアドレス)を変更します。

   IPアドレスは、移行対象情報ファイルの“サーバIPアドレス(CT管理サーバ)”に設定した値に変更します。コンピュータ名は、旧管理サーバと同じにする場合は、変更する必要はありません。

   設定項目の詳細は、“Systemwalker Desktop Keeper 導入ガイド”の“サーバ情報を設定する”を参照してください。

6. 移行対象情報ファイル(DTKServerChange.txt)を作成し、旧管理サーバに保存します。
   移行対象情報ファイルの詳細は、“Systemwalker Desktop Keeper リファレンスマニュアル”の“移行対象情報ファイル”を参照してください。

   格納場所

   Windows Server® 2008以外の場合

   ```
   C:¥Documents and Settings¥All Users¥Application Data¥Fujitsu¥Systemwalker Desktop Keeper
   ```

   Windows Server® 2008の場合

   ```
   C:¥ProgramData¥Fujitsu¥Systemwalker Desktop Keeper
   ```

   →クライアント(CT)起動時または管理コンソールからの即時更新時に、設定内容がCTポリシーとしてクライアント(CT)に情報通知されます。
   通知結果は、移行対象情報ファイル・実行ログ(DTKServerChange.log)として、旧管理サーバの以下に出力されます。

   Windows Server® 2008以外の場合
   C:¥Documents and Settings¥All Users¥Application Data¥Fujitsu¥Systemwalker Desktop Keeper

   Windows Server® 2008の場合
   C:¥ProgramData¥Fujitsu¥Systemwalker Desktop Keeper

   →クライアント(CT)の再起動後、移行対象情報ファイルの指定に従って、クライアント(CT)の接続先管理サーバが変更されます。

   接続先管理サーバの変更状況は、以下のように確認できます。

   a. 管理コンソールを起動し、旧管理サーバに接続します。
   b. CTリストの[最終ログオン日時]が更新されていないことを確認します。
   c. 管理コンソールの接続先を、新管理サーバに変更します。
   d. 構成情報ツリーに該当クライアント(CT)が表示され、かつ、CTリストの[最終ログオン日時]が更新されていることを確認します。

7. 全クライアント(CT)での変更が完了後、旧管理サーバの全ログをバックアップします。
8. ログを、新管理サーバのデータベースにリストアします。

管理サーバ配下の一部のクライアント(CT)を、別の既存管理サーバ配下に移動する

本変更方法の場合、移動したクライアント(CT)は、移動先管理サーバで新規登録されます。
移動元管理サーバでの管理情報やログを、移動先管理サーバへ移行しないでください。管理情報の重複により、クライアント(CT)を正しく管理できない場合があります。

移行手順は、以下のとおりです。

1. 移行対象情報ファイル(DTKServerChange.txt)を作成し、移動元管理サーバに保存します。
   移行対象情報ファイルの詳細は、“Systemwalker Desktop Keeper リファレンスマニュアル”の“移行対象情報ファイル”を参照してください。

   格納場所

   Windows Server® 2008以外の場合

   ```
   C:¥Documents and Settings¥All Users¥Application Data¥Fujitsu¥Systemwalker Desktop Keeper
   ```

   Windows Server® 2008の場合

   ```
   C:¥ProgramData¥Fujitsu¥Systemwalker Desktop Keeper
   ```

→クライアント(CT)起動時または管理コンソールからの即時更新時に、設定内容がCTポリシーとしてクライアント(CT)に情報通知されます。
通知結果は、移行対象情報ファイル・実行ログ(DTKServerChange.log)として、旧管理サーバの以下に出力されます。

Windows Server® 2008以外の場合
C:¥Documents and Settings¥All Users¥Application Data¥Fujitsu¥Systemwalker Desktop Keeper

Windows Server® 2008の場合
C:¥ProgramData¥Fujitsu¥Systemwalker Desktop Keeper

→クライアント(CT)の再起動後、移行対象情報ファイルの指定に従って、クライアント(CT)の接続先管理サーバが変更されます。

接続先管理サーバの変更状況は、以下のように確認できます。

a. 移動元および移動先管理サーバに接続している管理コンソールを起動します。

b. 移動元管理サーバの管理コンソールで、CTリストの[最終ログオン日時]が更新されていないことを確認します。

c. 移動先管理サーバの管理コンソールで、構成情報ツリーに、該当クライアント(CT)が表示されていることを確認します。

2. 移行対象となるすべてのクライアント(CT)の接続先管理サーバが変更されたことを移行対象情報ファイル・実行ログ(DTKServerChange.log)で確認し、移行対象情報ファイルを削除するか、格納場所以外の場所へ移動します。

接続先の管理サーバ(代替管理サーバ)のIPアドレスを変更する

ネットワークの変更や管理サーバの移設により、管理サーバのIPアドレスが変更になる場合の対応方法です。管理サーバのIPアドレスが変更になる日付を確定しておく必要があります。

移行手順は、以下のとおりです。

1. 移行対象情報ファイル(DTKServerChange.txt)を作成し、管理サーバに保存します。
移行対象情報ファイルの詳細は、“Systemwalker Desktop Keeper リファレンスマニュアル”の“移行対象情報ファイル”を参照してください。

格納場所

Windows Server® 2008以外の場合

```
C:¥Documents and Settings¥All Users¥Application Data¥Fujitsu¥Systemwalker Desktop Keeper
```

Windows Server® 2008の場合

```
C:¥ProgramData¥Fujitsu¥Systemwalker Desktop Keeper
```

→クライアント(CT)起動時または管理コンソールからの即時更新時に、設定内容がCTポリシーとしてクライアント(CT)に情報通知されます。
通知結果は、移行対象情報ファイル・実行ログ(DTKServerChange.log)として、以下に出力されます。

Windows Server® 2008以外の場合
C:¥Documents and Settings¥All Users¥Application Data¥Fujitsu¥Systemwalker Desktop Keeper

Windows Server® 2008の場合
C:¥ProgramData¥Fujitsu¥Systemwalker Desktop Keeper

→移行対象情報ファイルに設定された変更日以降のクライアント(CT)の再起動後、移行対象情報ファイルの指定に従って、クライアント(CT)の接続先管理サーバが変更されます。

2. 移行対象情報ファイルを削除するか、格納場所以外の場所へ移動します。

接続先の管理サーバ(代替管理サーバ)とクライアント(CT)両方のIPアドレスを変更する

ネットワーク体系が全体的に変更になる場合など、管理サーバのIPアドレスも、クライアント(CT)のIPアドレスも変更される場合の対応方法です。
クライアント(CT)は、管理サーバから移行対象情報ファイルの情報を、管理サーバのIPアドレスが変更される前に取得する必要があります。管理サーバのIPアドレスが変更になる日付を確定しておく必要があります。

移行手順は、以下のとおりです。

1. 移行対象情報ファイル(DTKServerChange.txt)を作成し、管理サーバに保存します。
   移行対象情報ファイルの詳細は、“Systemwalker Desktop Keeper リファレンスマニュアル”の“移行対象情報ファイル”を参照してください。

   格納場所

   Windows Server® 2008以外の場合

   ```
   C:¥Documents and Settings¥All Users¥Application Data¥Fujitsu¥Systemwalker Desktop Keeper
   ```

   Windows Server® 2008の場合

   ```
   C:¥ProgramData¥Fujitsu¥Systemwalker Desktop Keeper
   ```

   →クライアント(CT)起動時または管理コンソールからの即時更新時に、設定内容がCTポリシーとしてクライアント(CT)に情報通知されます。
   通知結果は、移行対象情報ファイル・実行ログ(DTKServerChange.log)として、以下に出力されます。

   Windows Server® 2008以外の場合
   C:¥Documents and Settings¥All Users¥Application Data¥Fujitsu¥Systemwalker Desktop Keeper

   Windows Server® 2008の場合
   C:¥ProgramData¥Fujitsu¥Systemwalker Desktop Keeper

2. ネットワーク体系の変更に伴い、管理サーバのIPアドレスが変更されたら、クライアント(CT)のIPアドレスを変更します。

   - クライアント(CT)が固定IPアドレスの場合:
     各クライアント(CT)で手動でIPアドレスを設定します。
   - クライアント(CT)がDHCP環境の場合:
     操作は不要です。

   →移行対象情報ファイルに設定された変更日以降のクライアント(CT)の再起動後、移行対象情報ファイルの指定に従って、クライアント(CT)の接続先管理サーバが変更されます。

3. 移行対象情報ファイルを削除するか、格納場所以外の場所へ移動します。

管理サーバ上にCT機能が同居している場合、そのCT機能についてはこれらの設定は無視します。管理サーバ上のCTに対しては、管理サーバは自コンピュータ以外は指定できません。そのため、代替管理サーバのIPアドレスの変更や、送信ポート番号等の変更については、保守コマンドによる設定変更を実施してください。

クライアント(CT)でコマンドを使用して変更する

パスワードを他人に知られないようにしてください

本コマンドをコマンドプロンプトから実行する場合、パスワードを第三者またはエンドユーザーに参照される恐れがあります。本コマンドを使用する場合は、必ずバッチファイルなどを利用し、絶対にパスワードが参照されないようにセキュリティを配慮した運用を行ってください。

手順は、以下のとおりです。

1. PCに、ローカルコンピュータのAdministratorsグループに所属するユーザーまたは、ドメインのDomain Adminsグループに所属するユーザーでログオンします。
2. 接続する(統合)管理サーバのIPアドレスを変更するクライアント(CT)のコマンドプロンプトから、以下のコマンドを実行します。

   ```
   fsw11ej7.exe <Password> /D /D
   ```

   <Password>:

   クライアント(CT)のインストール時に指定したパスワードを入力します。

   →コマンドプロンプトに表示された[サーバIPアドレス]が、現在接続している(統合)管理サーバのIPアドレスです。
3. 接続する(統合)管理サーバのIPアドレス、または代替(統合)管理サーバのIPアドレスを変更するため、クライアント(CT)のコマンドプロンプトから、以下のコマンドを実行します。

   ```
   fsw11ej7.exe <Password> /C /I <変更後の(統合)管理サーバのIPアドレス> <変更後の代替(統合)管理サーバのIPアドレス>
   ```

   <Password>:

   クライアント(CT)のインストール時に指定したパスワードを入力します。

   <変更後の(統合)管理サーバのIPアドレス>:

   クライアント(CT)の接続先となる(統合)管理サーバのIPアドレスを入力します。

   <変更後の代替(統合)管理サーバのIPアドレス>:

   ユーザーポリシーを照会するときの代替(統合)管理サーバのIPアドレスを入力します。省略した場合は、“<変更後の(統合)管理サーバのIPアドレス>”と同じ値が設定されます。
4. クライアント(CT)が接続する(統合)管理サーバへCT情報を通知するため、クライアント(CT)のコマンドプロンプトから、以下のコマンドを実行します。

   ```
   fsw11ej7.exe <Password> /R
   ```

   <Password>:

   クライアント(CT)のインストール時に指定したパスワードを入力します。
5. クライアント(CT)を再起動します。

接続先(統合)管理サーバの変更状況は、以下のように確認できます。

1. 移動元および移動先(統合)管理サーバに接続している管理コンソールを起動します。
2. 移動元(統合)管理サーバの管理コンソールで、CTリストの[最終ログオン日時]が更新されていないことを確認します。
3. 移動先(統合)管理サーバの管理コンソールで、構成情報ツリーに、該当クライアント(CT)が表示されていることを確認します。

ポイント

クライアント(CT)の情報がサーバから失われた場合、CT再登録コマンドで復旧できます(CTの上書きインストールを実施しても、復旧できません)

以下のいずれかの状況が発生した場合、該当するクライアント(CT)で、CT再登録コマンド(fsw11ej7.exe <Password> /R)を実行すると、管理(統合管理)サーバにクライアント(CT)情報が再登録されます。

- 管理コンソール上で誤ってクライアント(CT)を削除し、その後、管理サーバのIPアドレスに変更がない場合
- トラブルにより管理(統合管理)サーバからクライアント(CT)の情報が失われ、その後、管理サーバのIPアドレスに変更がない場合

「fsw11ej7.exe <Password> /R」を実行後、クライアント(CT)を再起動してください。

クライアント(CT)の情報が管理(統合管理)サーバに通知されると、管理コンソール上に表示されます。

- 管理コンソールでの表示位置
  - ー Active Directory連携する運用の場合
    クライアント(CT)を表示させた直後は、localグループ配下に登録されます。Active Directory連携情報を更新した後、Active Directoryサーバに登録されている位置に表示されます。
  - ー Active Directory連携していない運用の場合
    再表示されたクライアント(CT)は、ルート配下に登録されます。
- 適用されるCTポリシー
  管理コンソールの[端末初期設定]画面で設定されているポリシーが適用されます。
- クライアント(CT)のログ
  削除前のログは、ログビューアに表示されません。

7.7.2 クライアント(CT)の動作設定を変更する

クライアント(CT)のインストール時に設定した印刷監視方式/メール制御方式の変更方法や、クライアント(CT)に一時保存するログファイルのサイズなどの変更方法を説明します。

変更するには、管理サーバで実施する方法と、クライアント(CT)で実施する方法とがあります。

変更方法		変更できる項目	変更できるクライアント(CT)のバージョン
管理サーバで変更する	CT動作パラメーター情報ファイルを使用する	・ メール送信時宛先確認メッセージ	V14.1.0以降
		・ 代替管理サーバのIPアドレス ・ 操作ログファイルのサイズ ・ 禁止ログファイルのサイズ ・ エラーログファイルのサイズ ・ エラーログの保存日数 ・ トレースログファイルのサイズ ・ 印刷監視方式(※) ・ メール制御方式 ー メール送信監視用ポート番号 ー メール添付禁止の監視方式 ー メール添付禁止通信用ポート番号 ー メール添付禁止通信用ポート番号2 ・ ログオン直後動作	V14.0.0以降
	[端末動作設定]画面で変更する	・ 印刷監視方式	全バージョン
クライアント(CT)で変更する	[プログラムの追加と削除]で変更する	・ 印刷監視方式 ・ メール制御方式 ー メール送信監視用ポート番号 ー メール添付禁止の監視方式 ー メール添付禁止通信用ポート番号 ー メール添付禁止通信用ポート番号2	全バージョン

※) CT動作パラメーター情報ファイルによる印刷監視方式の変更は、一時的にクライアント(CT)の設定を変更する場合に使用します。設定値変更後に、CT動作パラメーター情報ファイルを削除または格納場所以外の場所へ移動したあとは、次回のポリシー通知によって[端末動作設定]画面での設定値で動作します。

CT動作パラメーター情報ファイルを使用する

CT動作パラメーター情報ファイルに変更後の値を設定し、管理サーバに保存します。ファイルの情報は、CTポリシーとしてクライアント(CT)に通知されます。設定値が反映されるタイミングで、変更内容がクライアント(CT)に反映されます。

1. CT動作パラメーター情報ファイル(DTKCTSetting.txt)を作成し、管理サーバに保存します。
   CT動作パラメーター情報ファイルの詳細は、“Systemwalker Desktop Keeper リファレンスマニュアル”の“CT動作パラメーター情報ファイル”を参照してください。

   格納場所

   Windows Server® 2008以外の場合

   ```
   C:¥Documents and Settings¥All Users¥Application Data¥Fujitsu¥Systemwalker Desktop Keeper
   ```

   Windows Server® 2008の場合

   ```
   C:¥ProgramData¥Fujitsu¥Systemwalker Desktop Keeper
   ```

   →クライアント(CT)起動時または管理コンソールからの即時更新時に、設定内容がCTポリシーとしてクライアント(CT)に通知されます。
   通知結果は、CT動作パラメーター情報ファイル・実行ログ(DTKCTSetting.log)として、以下に出力されます。

   Windows Server® 2008以外の場合
   C:¥Documents and Settings¥All Users¥Application Data¥Fujitsu¥Systemwalker Desktop Keeper

   Windows Server® 2008の場合
   C:¥ProgramData¥Fujitsu¥Systemwalker Desktop Keeper

   →CTポリシー通知後、設定がクライアント(CT)に反映されます。反映されるタイミングは、設定項目により異なります。

   設定値が反映されるタイミング

設定項目	設定値が反映されるタイミング
代替管理サーバのIPアドレス	OS再起動後に反映されます。 移行対象情報ファイルでも本項目を設定している場合は、移行対象情報ファイルの設定値が反映されます。
操作ログファイルのサイズ	即時反映されます。
禁止ログファイルのサイズ	即時反映されます。
エラーログファイルのサイズ	日付が変わって新しいエラーログファイルを作成する時に反映されます。
エラーログの保存日数	日付が変わって新しいエラーログファイルを作成する時に反映されます。
トレースログファイルのサイズ	即時反映されます。
印刷監視方式	即時反映されます。 [端末動作設定]画面でも本項目を設定している場合は、CT動作パラメーター情報ファイルの設定値が反映されます。 ただし、CT動作パラメーター情報ファイルを、削除または格納場所以外の場所へ移動したあとは、[端末動作設定]画面での設定値で動作します。
メール送信監視用ポート番号	OS再起動後に反映されます。

設定項目	設定値が反映されるタイミング
メール添付禁止の監視方式	OS再起動後に反映されます。
メール添付禁止通信用ポート番号	OS再起動後に反映されます。
メール添付禁止通信用ポート番号2	OS再起動後に反映されます。
ログオン直後動作	OS再起動後に反映されます。
メール送信時宛先確認メッセージ	OS再起動後に反映されます。

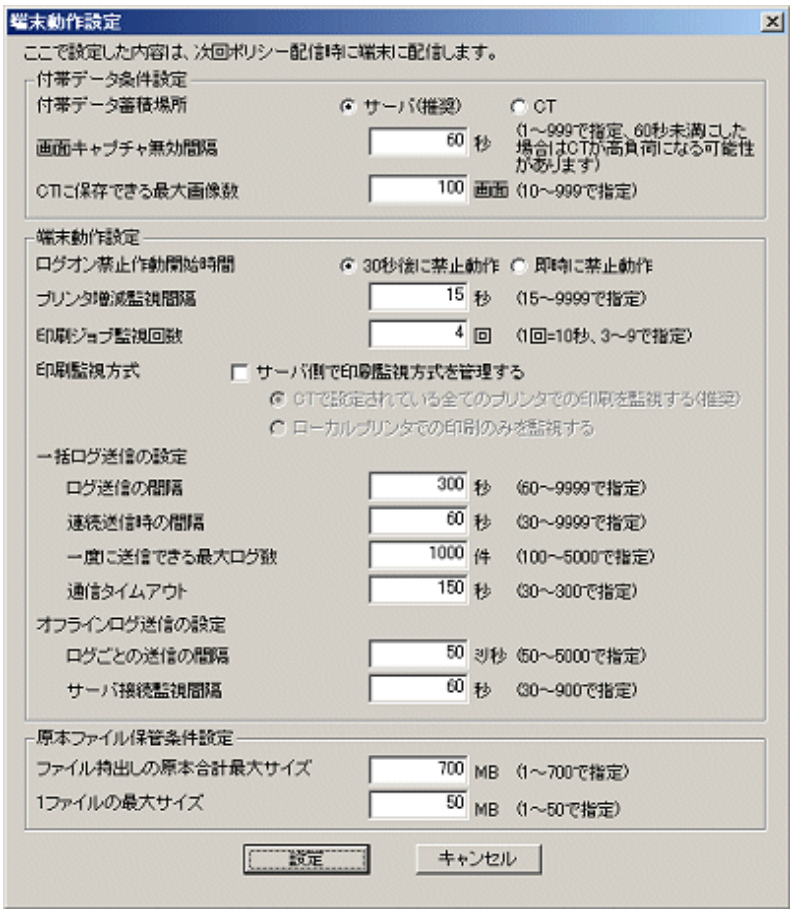
2. 設定値が変更されていることを確認します。
   設定変更を実施した各クライアント(CT)で、FSW11EJ7.EXE(システムの保守)コマンドの設定情報表示を実施し、出力内容を確認します。コマンドの詳細は、“Systemwalker Desktop Keeper リファレンスマニュアル”の“設定情報表示”を参照してください。

3. CT動作パラメーター情報ファイルを削除するか、格納場所以外の場所へ移動します。
   (本ファイルが格納場所に存在する場合、クライアント(CT)の動作環境変更が、再度実施されます。)

[端末動作設定]画面で変更する

操作手順および設定項目については、“2.4.2 端末動作設定をおこなう”を参照してください。

クライアント(CT)に通知された変更情報は、即時反映されます。
CT動作パラメーター情報ファイルでも[印刷監視方式]を設定している場合は、CT動作パラメーター情報ファイルの設定値が反映されます。

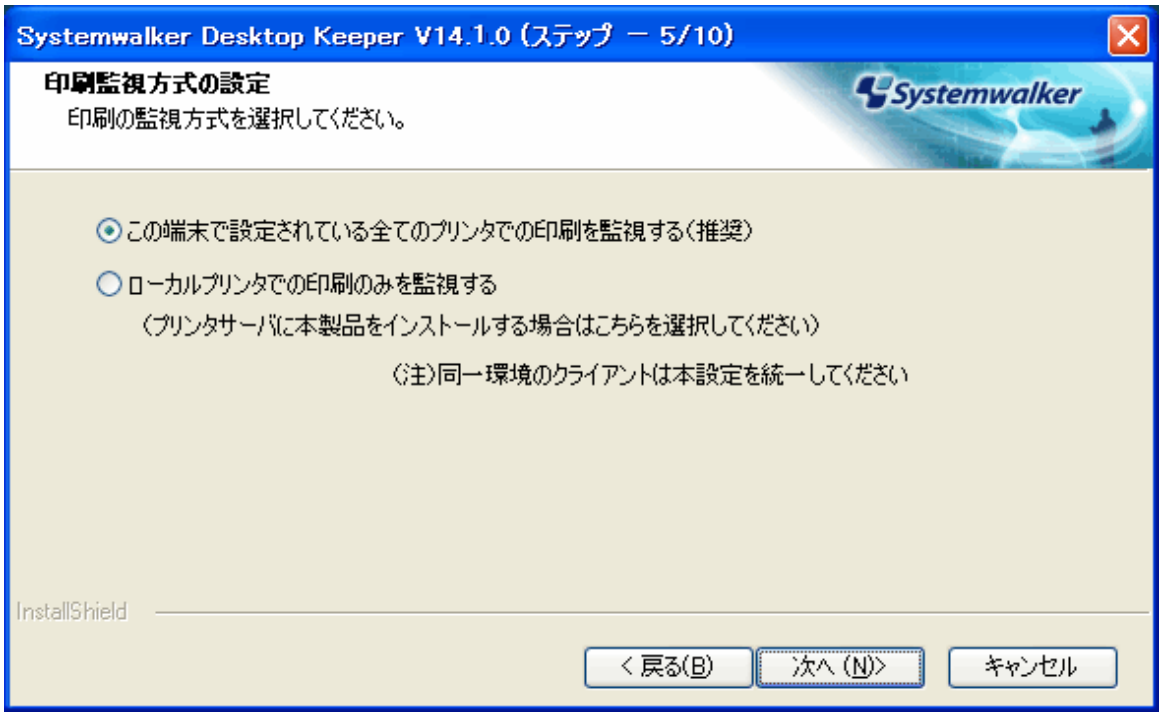


[プログラムの追加と削除]で変更する

印刷監視方式を変更する場合

1. PCに、ローカルコンピュータのAdministratorsグループに所属するユーザーまたは、ドメインのDomain Adminsグループに所属するユーザーでログオンします。
2. [コントロール パネル]の[プログラムの追加と削除]を選択します。
3. [Systemwalker Desktop Keeper クライアント(CT)]を選択し、[変更]ボタンをクリックします。

   →CTのインストール画面が表示されます。
4. [印刷監視方式の設定]画面で設定値を変更します。



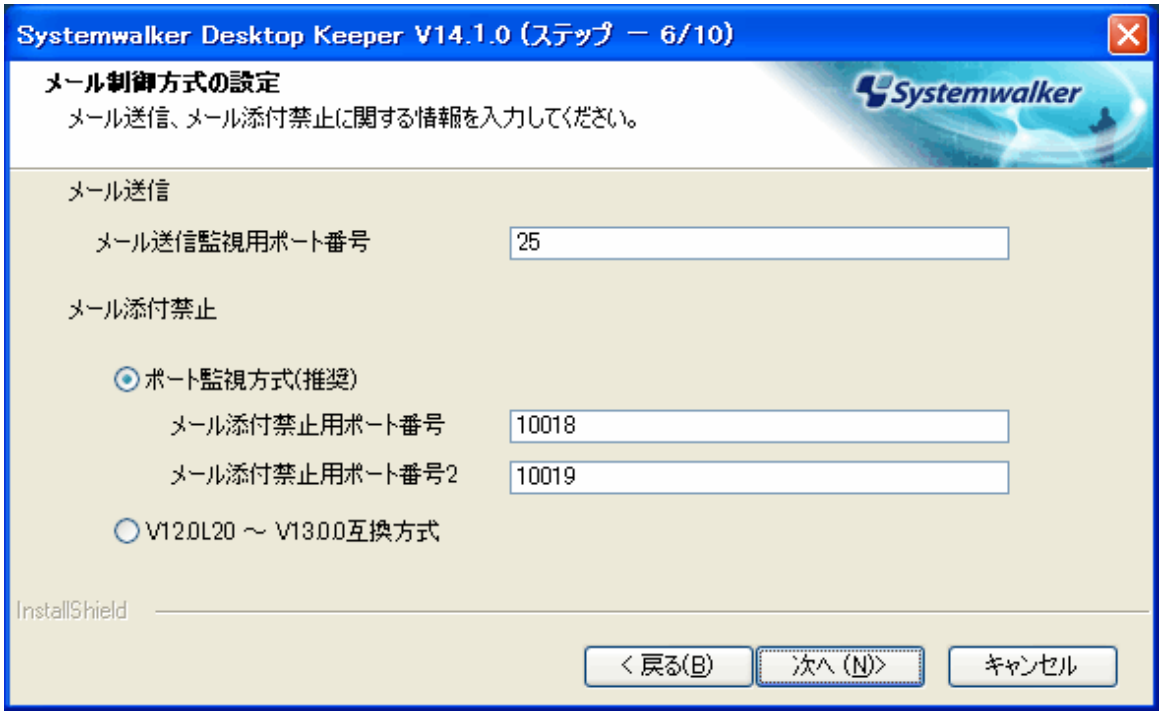
   設定値の詳細は、“Systemwalker Desktop Keeper 導入ガイド”の“ウィザード形式でインストールする”を参照してください。

メール制御方式を変更する場合

1. PCに、ローカルコンピュータのAdministratorsグループに所属するユーザーまたは、ドメインのDomain Adminsグループに所属するユーザーでログオンします。
2. [コントロール パネル]の[プログラムの追加と削除]を選択します。
3. [Systemwalker Desktop Keeper クライアント(CT)]を選択し、[変更]ボタンをクリックします。

   →CTのインストール画面が表示されます。

4. [メール制御方式の設定]画面で設定値を変更します。



設定値の詳細は、“Systemwalker Desktop Keeper 導入ガイド”の“ウィザード形式でインストールする”を参照してください。

7.8 管理コンソール環境を変更する

管理コンソールのインストール時に設定した、接続する(統合)管理サーバのIPアドレスまたはコンピューター名を変更する方法を説明します。
ここで説明する方法は、管理コンソールがインストールされている場合に、管理コンソールの接続先となるサーバのIPアドレスまたはコンピューター名に変更があったときの手順です。

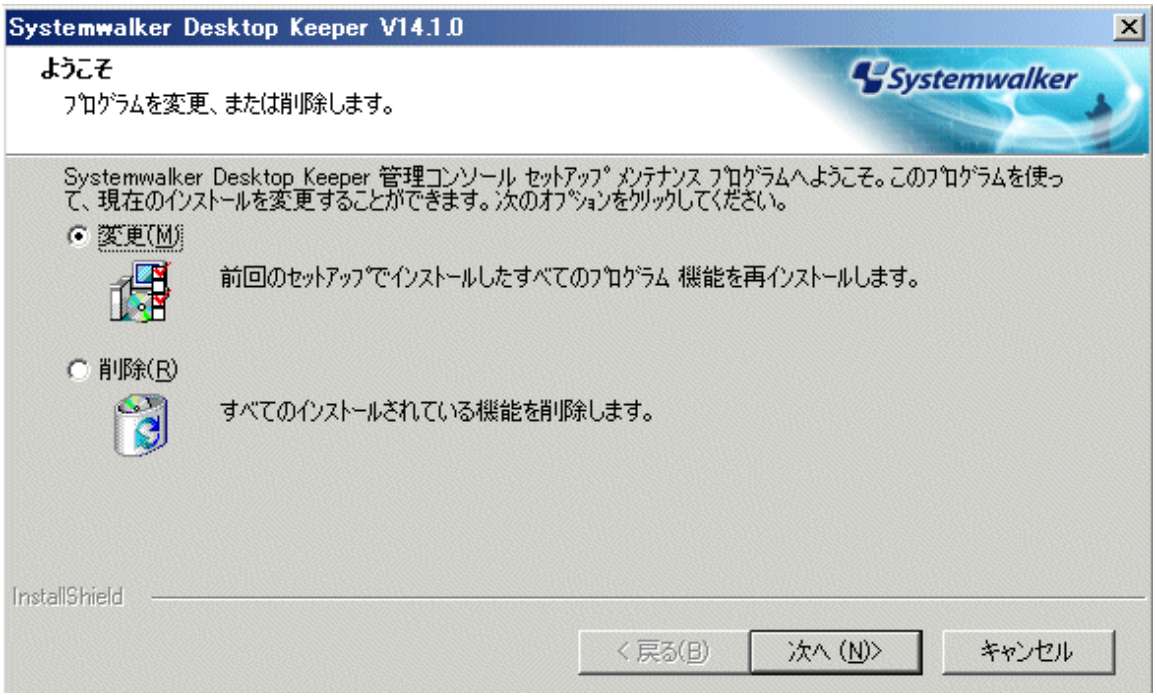
手順を開始する前に、“7.9.4 管理サーバ/統合管理サーバのIPアドレス/コンピュータ名の変更に伴ってシステム環境を変更する”によって管理サーバ・統合管理サーバ環境の変更が完了している必要があります。
また、接続先の(統合)管理サーバ変更時に、コンピューター名を指定する場合は、名前解決されていることを確認してください。

手順は、以下のとおりです。

1. PCに、ローカルコンピュータのAdministratorsグループに所属するユーザーまたは、ドメインのDomain Adminsグループに所属するユーザーでログオンします。
2. セットアップディスクをドライブにセットします。インストーラが起動しない場合は、セットアップディスクをセットしたドライブの「swsetup.exe」を起動します。

3. [管理コンソールインストール]を選択します。

   →以下の画面が表示されます。



4. [変更]を選択して、[次へ]ボタンをクリックします。
   →以下の画面が表示されます。

5. コンピューター名またはIPアドレスを変更します。

   【新しいコンピューター名またはIPアドレスを追加する場合】

   a. [接続する(統合)管理サーバのコンピューター名またはIPアドレス]を設定します。

   b. [使用するポート番号]を設定します。

   c. [追加]ボタンをクリックします。

【設定されているコンピューター名またはIPアドレスを削除する場合】

a. 削除する「接続する(統合)管理サーバのコンピューター名またはIPアドレス:使用するポート番号」を選択します。

b. [削除]ボタンをクリックします。

【設定されているコンピューター名またはIPアドレスを変更する場合】

a. 変更する「接続する(統合)管理サーバのコンピューター名またはIPアドレス:使用するポート番号」を選択します。

b. [削除]ボタンをクリックします。

c. [接続する(統合)管理サーバのコンピューター名またはIPアドレス]を設定します。

d. [使用するポート番号]を設定します。

e. [追加]ボタンをクリックします。

6. [次へ]ボタンをクリックします。
7. [インストール]ボタンをクリックします。
8. [完了]ボタンをクリックします。
9. 以下の条件の場合、インストール終了後にPCの再起動を要求されたときは、再起動を行ってください。

   ー 管理コンソールを起動した状態で上書きインストールした場合

7.9 管理サーバ環境を変更する

サーバ環境の変更方法を説明します。

変更は、サーバ設定ツールで実施します。

7.9.1 サーバ設定ツールを起動する

サーバ設定ツールを起動する

1. PCに、ローカルコンピュータのAdministratorsグループに所属するユーザーまたは、ドメインのDomain Adminsグループに所属するユーザーでログオンします。
2. [スタート]メニューから[プログラム]-[Systemwalker Desktop Keeper]-[サーバ]-[サーバ設定ツール]を選択します。
   →[Systemwalker Desktop Keeper サーバ設定ツール]画面が表示されます。

3. 初期管理者のアカウントでログオンします。初期管理者のアカウントは以下のとおりです。

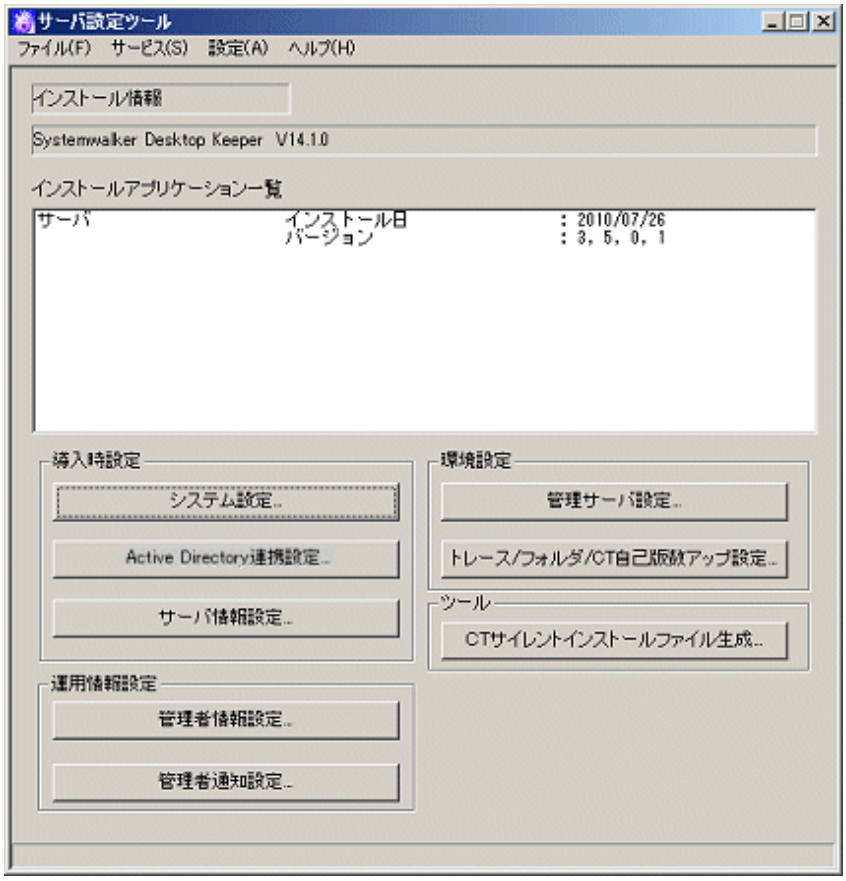
   ― **[ユーザーID]**:SecureAdmin

   ― **[パスワード]**:管理サーバ、統合管理サーバインストール時に指定したパスワード

   パスワードは定期的に変更することを推奨します。変更方法は、“7.9.2 初期管理者のパスワードを変更する”を参照してください。

   サーバ設定ツールで登録したユーザー(管理コンソールが実行できるアクセス権が必要)でもログオンできますが、使用できる機能は“管理者通知設定”だけです。

4. [OK]ボタンをクリックします。
   →[サーバ設定ツール]画面が表示されます。



画面の表示内容

[サーバ設定ツール]画面の表示項目について説明します。

項目名	説明
[インストール情報]	インストールされている製品のバージョンが表示されます。
[インストールアプリケーション一覧]	Systemwalker Desktop Keeperのインストールアプリケーションごとのインストール日とバージョンが表示されます。 ・ インストールアプリケーション 以下のアプリケーションがインストールされている場合に表示されます。 ― 管理サーバ・統合管理サーバ(表示名:サーバ) ― 管理コンソール(表示名:管理コンソール)

項目名		説明
		・ インストール日（インストールした日付をyyyy/mm/dd形式で表示） ・ インストールアプリケーションのバージョン
[導入時設定]	[システム設定]	[システム設定]画面を表示します。 統合管理サーバ、管理サーバに関する全体的な動作を設定します。
	[Active Directory連携設定]	[Active Directory連携設定]画面を表示します。 統合管理サーバ、または管理サーバと連携するドメインサーバを登録します。
	[サーバ情報設定]	[サーバ情報設定]画面を表示します。 サーバ情報を設定します。
[運用情報設定]	[管理者情報設定]	[管理者情報設定]画面を表示します。 以下を設定します ・ 管理コンソール、ログビューア、バックアップツール、リストアツール、レポート出力ツールでの認証ユーザー ・ 部門管理者 ・ 上記登録者に付与する権限
	[管理者通知設定]	[管理者通知設定]画面を表示します。 違反操作検出時の管理者への通知方法を設定します。
[環境設定]	[管理サーバ設定]	[管理サーバ設定]画面を表示します。 管理サーバの通信環境を設定します。
	[トレース/フォルダ/CT自己版数アップ設定]	[トレース/フォルダ/CT自己版数アップ設定]画面を表示します。 トレース、フォルダ、CT自己版数アップの設定を行います。
[ツール]	[CTサイレントインストールファイル生成]	[CTサイレントインストールファイル生成]画面を表示します。 サイレントインストール時の条件を設定します。

メニューバー

[サーバ設定ツール]画面のメニューバーについて説明します。

メニューバー			機能概要
[ファイル]	[終了]		サーバ設定ツールを終了します。
[サービス]	[サービス状況確認]		接続している管理サーバ上の[階層化サービス]、[サーバサービス]の動作状況を表示します。
	[サービス起動]		接続している管理サーバ上の[階層化サービス]、[サーバサービス]を起動します。
	[サービス停止]		接続している管理サーバ上の[階層化サービス]、[サーバサービス]を停止します。
[設定]	[Active Directory連携実施]		Active Directoryとの連携処理を実行します。
	[パスワード変更]		初期管理者のパスワードを変更します。 パスワードは半角の英数字と記号32文字以内で指定してください。 使用できない記号は、「&」「<」「>」「|」「¥」「"」「~」「'」「?」「:」「^」です。 全角および半角の空白は入力できません。
	[サーバ設定ツールトレース]	[しない]	サーバ設定ツールのトレースを採取しません。
		[概要]	サーバ設定ツールのトレースを概要モードで採取します。
		[詳細]	サーバ設定ツールのトレースを詳細モードで採取します。
[ヘルプ]	[オンラインヘルプ]		HTMLマニュアルを表示します。

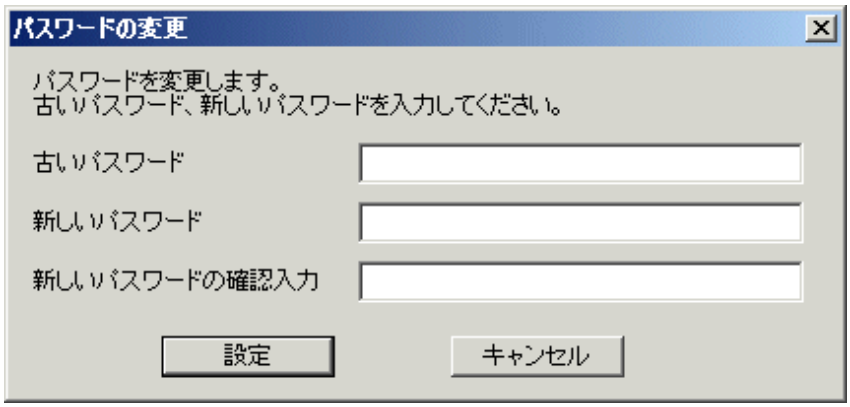
メニューバー		機能概要
	[バージョン情報]	著作権情報およびバージョン情報を表示します。

7.9.2 初期管理者のパスワードを変更する

初期管理者のパスワードを変更する方法を説明します。

1. [サーバ設定ツール]を起動します。
2. [設定]メニューの[パスワード変更]を選択します。

   →以下の画面が表示されます。



3. “古いパスワード”に従来のパスワードを、“新しいパスワード”に変更するパスワードを入力します。
   - パスワードは半角の英数字と記号32文字以内で指定してください。
   - 使用できない記号は、「&」「<」「>」「|」「¥」「"」「~」「'」「?」「:」「^」です。
   - 全角および半角の空白は入力できません。
4. [設定]ボタンをクリックします。

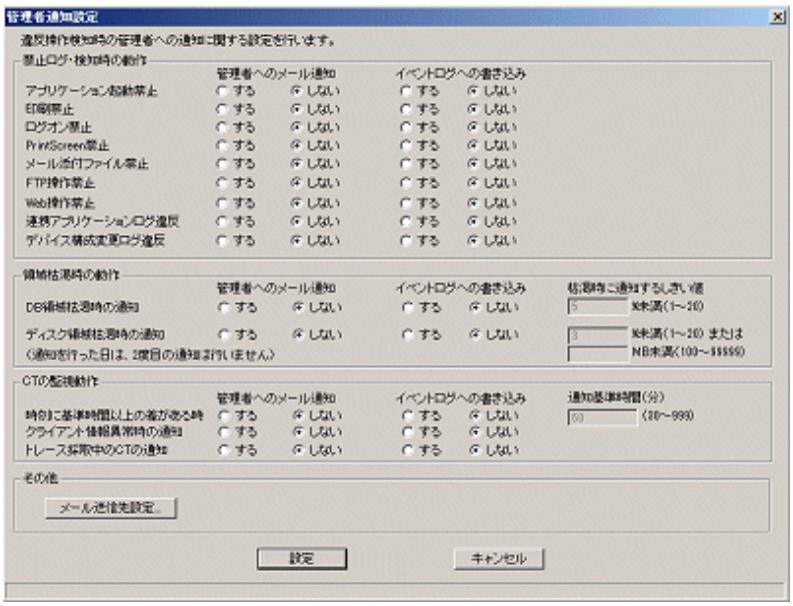
7.9.3 管理者通知を変更する

クライアント(CT)やデータベースで発生した事象の、管理者への通知(メール通知、イベントログへの書き込み)方法は、導入時に[管理者通知設定]画面で設定します。

しかし、運用状況に応じた設定値の見直しが必要な場合は、運用を開始してからでも変更することができます。

変更方法は、“Systemwalker Desktop Keeper 導入ガイド”の“管理者通知を設定する”を参照してください。

[管理者通知設定]画面



7.9.4 管理サーバ/統合管理サーバのIPアドレス/コンピュータ名の変更に伴ってシステム環境を変更する

管理サーバ/統合管理サーバのIPアドレスまたはコンピュータ名を変更した場合に、Systemwalker Desktop Keeperのサーバ設定ツールを利用して、管理サーバ/統合管理サーバ環境を変更する方法を説明します。

以下の場合について説明します。

- 3階層での統合管理サーバまたは2階層での管理サーバの環境を変更した場合
- 3階層での管理サーバの環境だけを変更した場合
- 3階層での統合管理サーバおよび統合管理サーバ配下の管理サーバの環境を変更した場合

注意

【システム環境を変更する時間帯について】

環境の変更を行う場合、管理サーバや統合管理サーバの運用を停止させる必要があります。そのため、業務に支障のないように、利用者の少ない時間帯に行ってください。

【サーバ情報の参照について】

情報の不整合が発生することがありますので、3階層の場合、すべての管理サーバや統合管理サーバでの環境の変更が完了するまで、統合管理サーバから、配下の管理サーバの情報を参照しないでください。

【バージョン・エディションの統一について】

統合管理サーバや管理サーバを異なるバージョンまたはエディションで使用する場合、データの連携に異常が発生して、正常に動作しません。また、管理コンソールとログビューアのバージョンおよびエディションも、統合管理サーバや管理サーバと同じにしてください。

【ログアナライザサーバへの変更反映について】

ログアナライザサーバを導入している場合、管理サーバ/統合管理サーバの変更がログアナライザサーバへ自動で反映されるまでには時間がかかる場合があります。

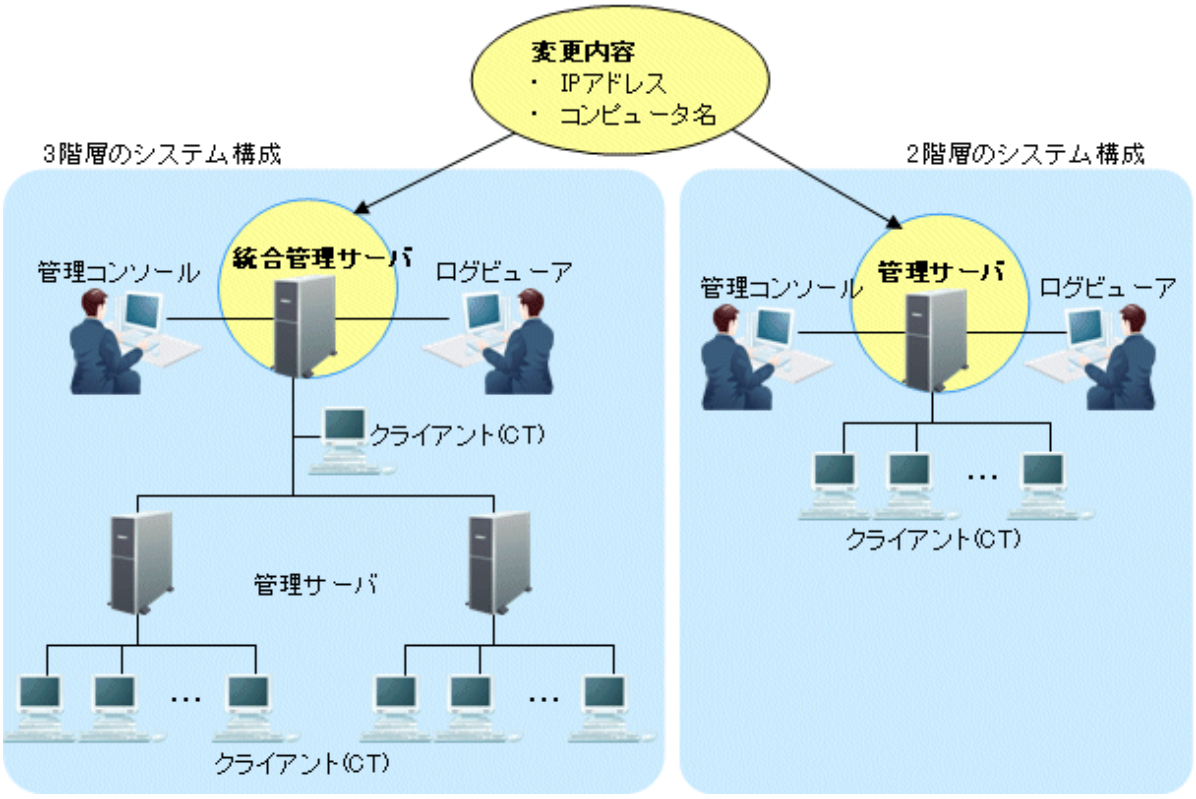
反映されるまでの間はWebコンソールのログアナライザを使用できません。即時に変更を反映してログアナライザを使用したい場合は、変更の実施後に、“Systemwalker Desktop Keeper 導入ガイド”の“ログアナライザサーバの環境を設定する”の“管理サーバ/統

合管理サーバ上で、管理者情報をログアナライザサーバに転送する”、および“ログアナライザサーバ上で、管理者情報を登録する”を行って反映させてください。

また、変更前の管理サーバ/統合管理サーバから転送したログデータや管理者情報を移入すると管理者情報が古い状態に戻るためWebコンソールのログアナライザを使用できなくなります。その場合は再度、変更後の管理サーバ/統合管理サーバから管理者情報の転送と登録を行ってください。

なお、変更前の管理サーバ/統合管理サーバからの転送をスケジュールしている場合は、転送スケジュールを解除してください。

3階層での統合管理サーバまたは2階層での管理サーバの環境を変更した場合



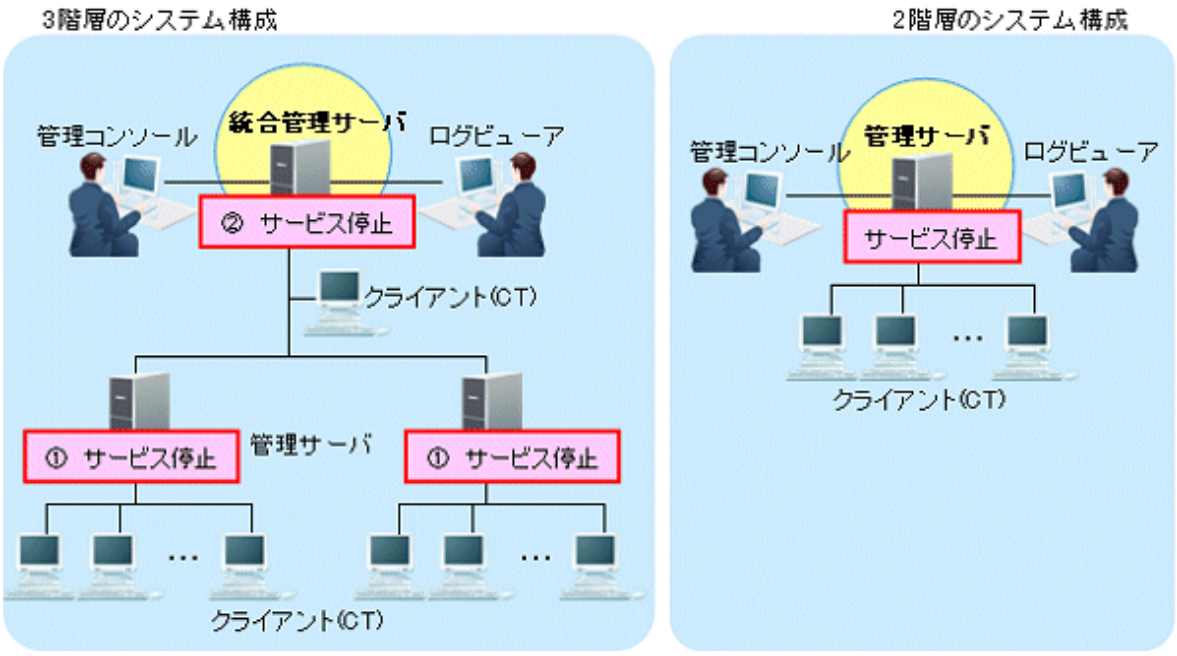
3階層での統合管理サーバ、または2階層での管理サーバで以下の情報を変更した場合に、管理サーバ/統合管理サーバ環境を変更する方法を説明します。

- IPアドレス
- コンピュータ名

管理サーバ、または統合管理サーバの環境を変更後、もとの環境に戻すために必要な情報は、保存されていません。もとの環境に戻す場合に備え、手順にしたがって、ノードの情報(ノード名、コンピュータ名、IPアドレス、サーバ区分)を控えておくことをお勧めします。

手順は、以下のとおりです。

1. 階層化サービスおよびサーバサービスを停止します。

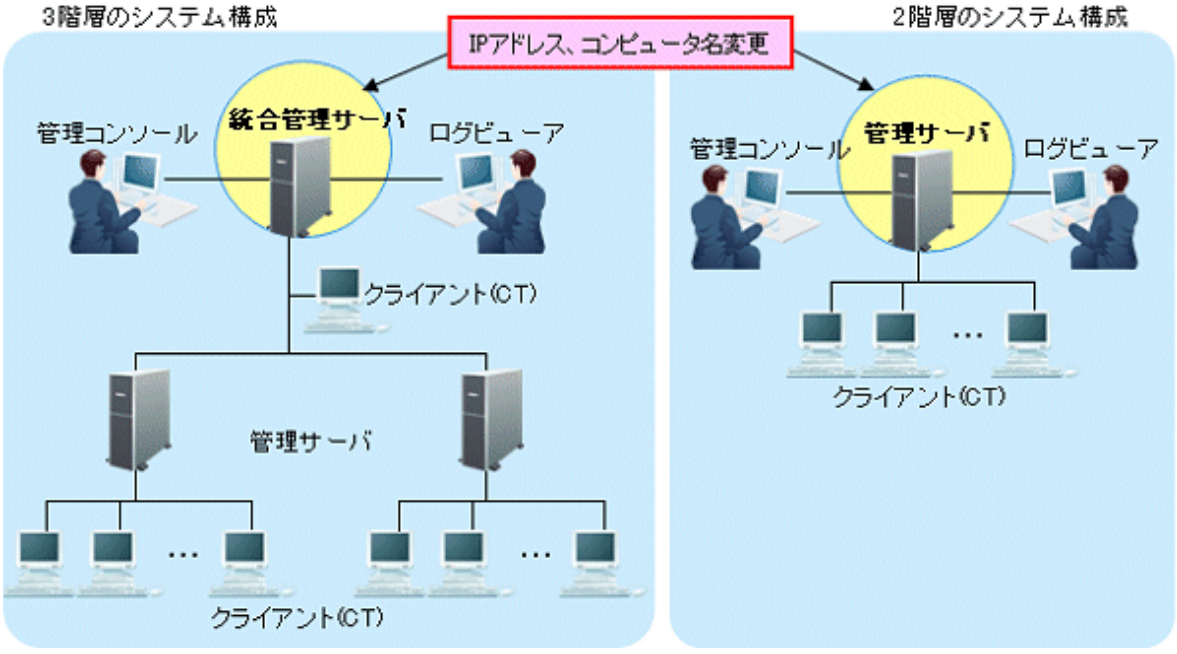


3階層の場合は、統合管理サーバおよび統合管理サーバ配下のすべての管理サーバが停止対象です。(管理サーバから停止します。)

a. [サーバ設定ツール]を起動します。

b. [サービス]メニューから[サービス停止]を選択します。

2. IPアドレス、コンピュータ名を変更します。



3階層での統合管理サーバ、または2階層での管理サーバが対象です。
コンピュータ自体の設定を変更します。

a. IPアドレスを変更します。IPアドレスの変更が不要な場合は、次の手順に進んでください。

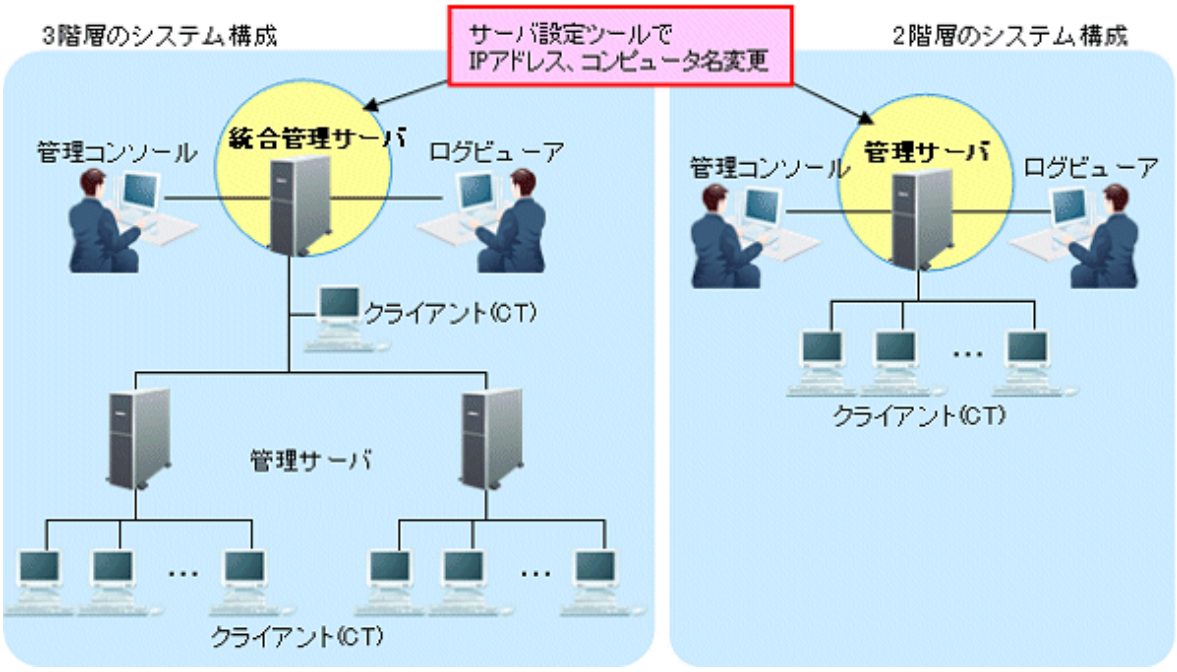
   1. [スタート]メニューから[コントロールパネル]-[ネットワーク接続]-[ローカル エリア接続]を選択します。[ローカル エリア接続の状態]画面の[全般]タブで[プロパティ]ボタンをクリックします。
   2. [インターネットプロトコル]を選択して、[プロパティ]ボタンをクリックします。
   3. IPアドレスを変更して登録します。

b. コンピュータ名を変更します。コンピュータ名の変更が不要な場合は、次の手順に進んでください。

   1. [スタート]メニューから[コントロールパネル]-[システム]を選択し、[システムのプロパティ]画面の[コンピュータ名]タブを表示します。
   2. コンピュータ名を変更して登録します。

c. サーバを再起動します。

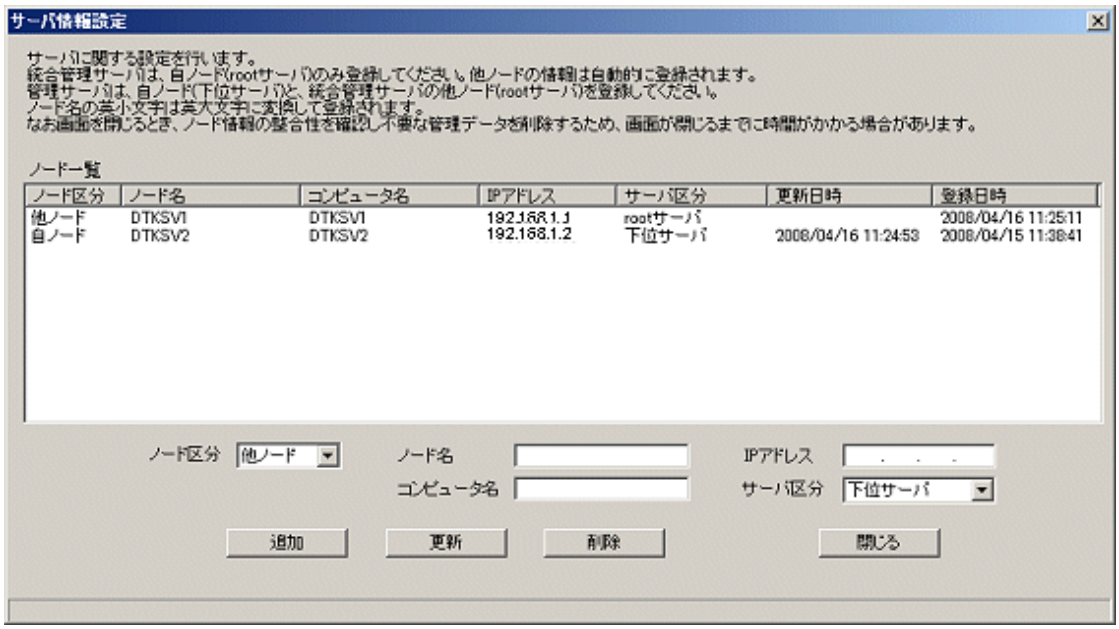
3. 3階層での統合管理サーバまたは2階層での管理サーバ上で、Systemwalker Desktop Keeperの設定を変更します。



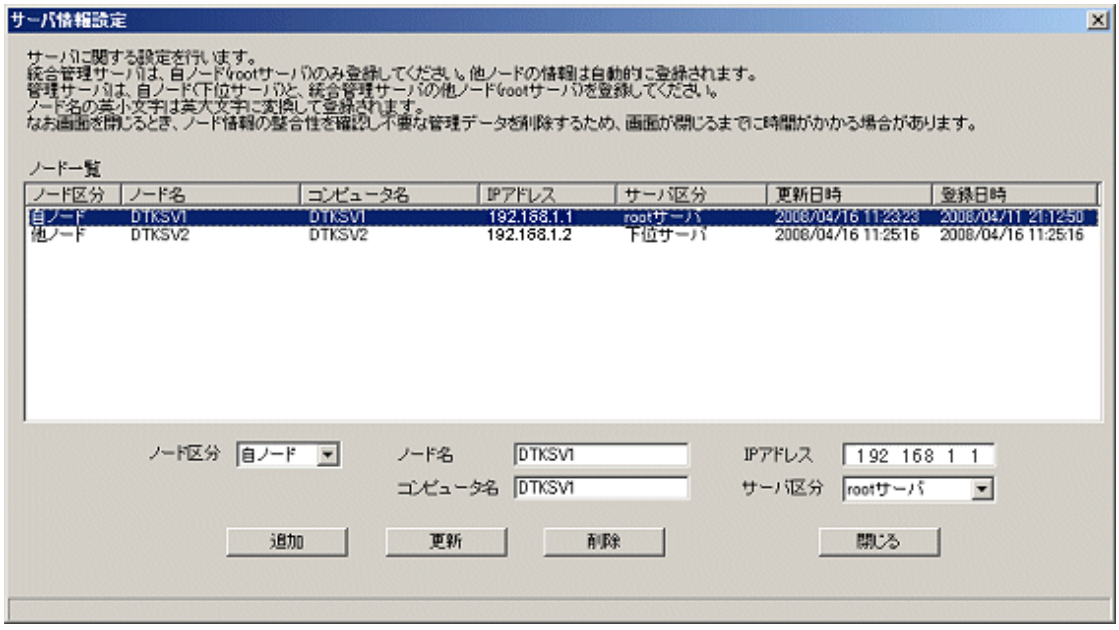
登録されている自分自身のサーバ情報設定を変更します。

a. サーバ設定ツールを起動します。

b. [サーバ情報設定]ボタンをクリックします。
→[サーバ情報設定]画面が表示されます。



c. ノード区分が自ノードのデータをクリックします。
→情報が画面下の入力フィールドに表示されます。



d. 変更する[コンピュータ名]または、[IPアドレス]を変更し、[更新]ボタンをクリックし、[閉じる]ボタンをクリックします。

注意

[コンピュータ名]と[IPアドレス]だけ変更してください

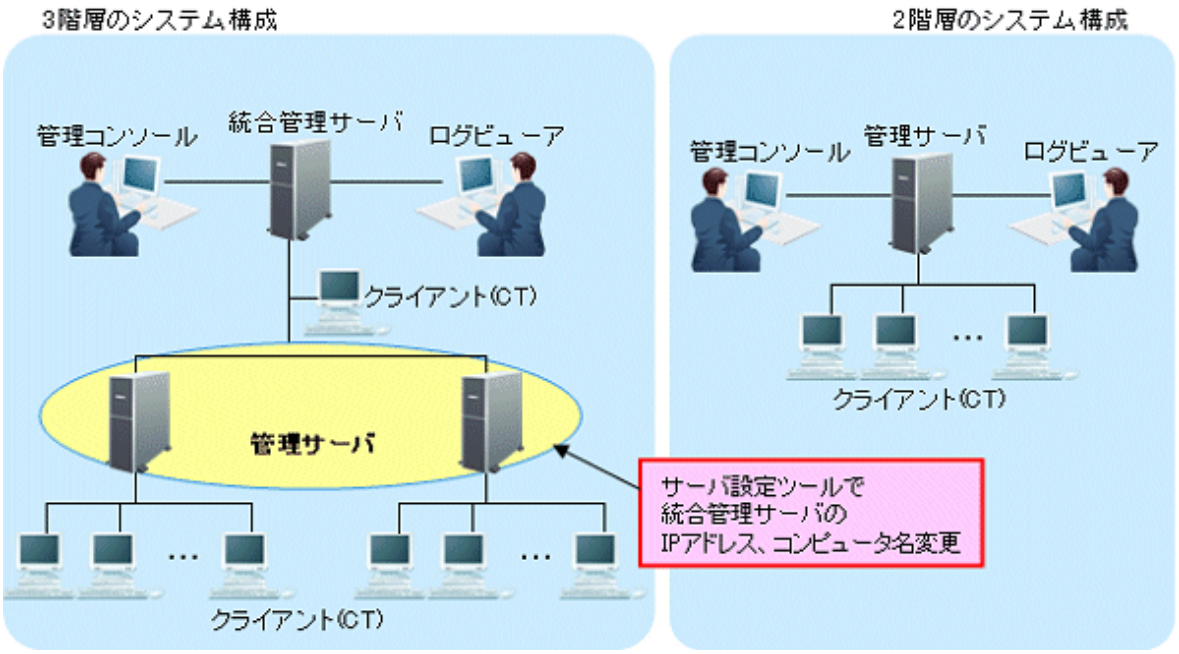
構成情報に不整合が発生するため、[コンピュータ名]および[IPアドレス]以外の項目の値は変更しないでください。

e. サービスを起動します。

設定変更を行った3階層での統合管理サーバまたは2階層での管理サーバのサービスを起動します。

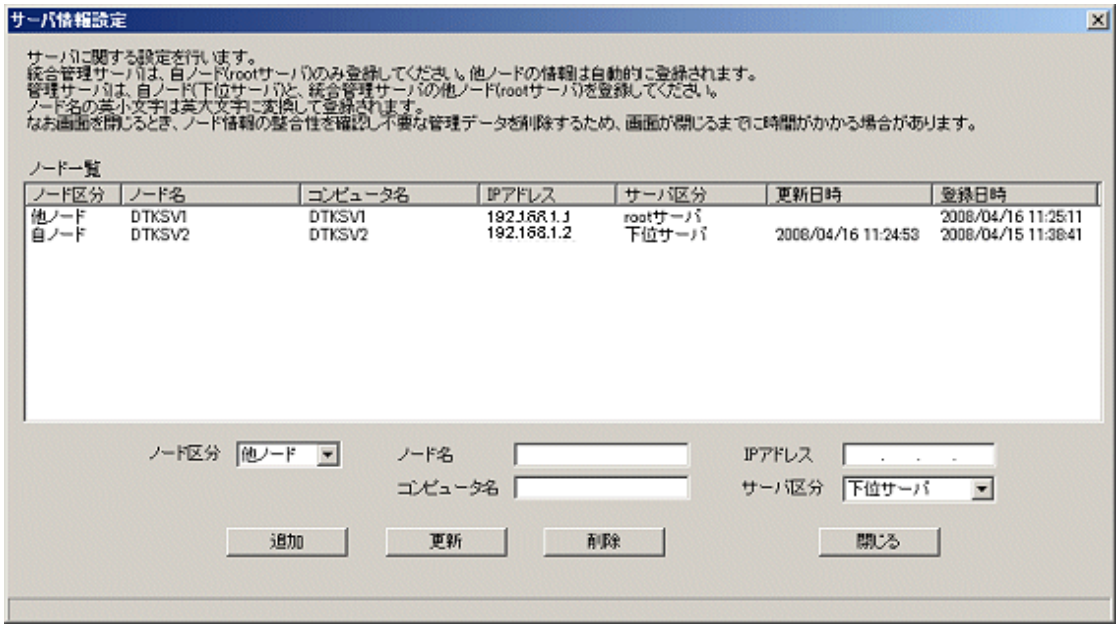
1. [サーバ設定ツール]を起動します。
2. [サービス]メニューから[サービス起動]を選択します。
3. [サーバ設定ツール]を終了します。

4. 3階層での統合管理サーバ配下の管理サーバ上で、Systemwalker Desktop Keeperの設定を変更します(3階層の場合だけ実施します)。

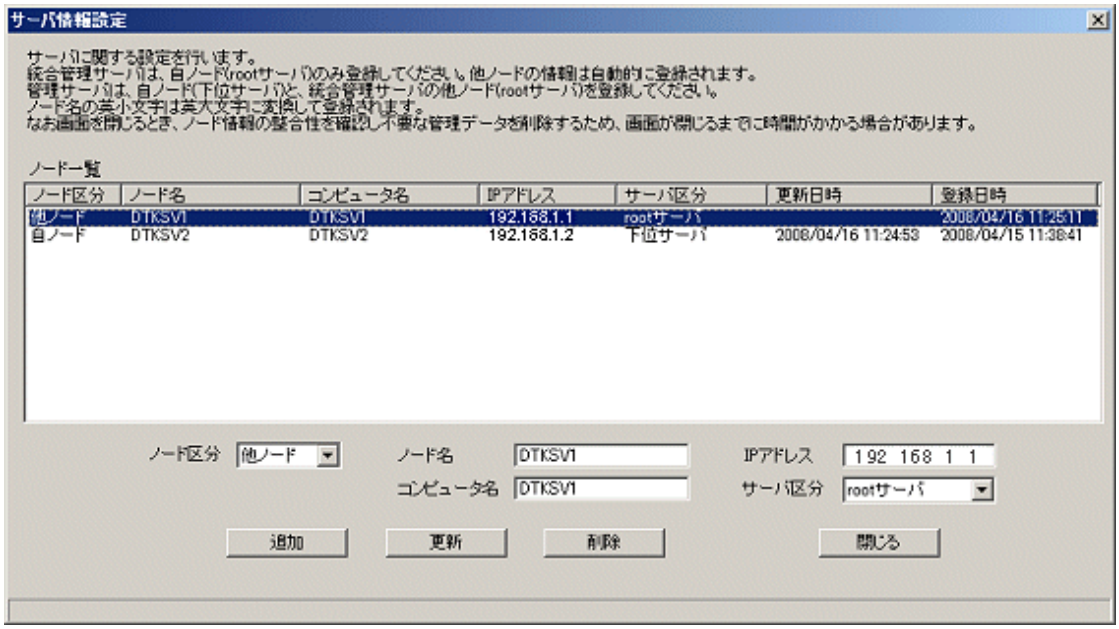


管理サーバで登録されている、統合管理サーバのサーバ情報設定を変更します。

a. サーバ設定ツールを起動します。
b. [サーバ情報設定]ボタンをクリックします。
→[サーバ情報設定]画面が表示されます。



c. ノード区分が他ノード(rootサーバ)のデータをクリックします。
→情報が画面下の入力フィールドに表示されます。



d. 以下の操作を実施します。

1. 表示されている他ノードの情報(ノード名、コンピュータ名、IPアドレス、サーバ区分)を控えます。
2. [削除]ボタンをクリックし、サーバ情報を削除します。
3. 以下の値を設定し、[追加]ボタンをクリックします。

・[ノード区分]:他ノード
・変更する統合管理サーバの[ノード名]、[コンピュータ名]、[IPアドレス]
・[サーバ区分]:rootサーバ

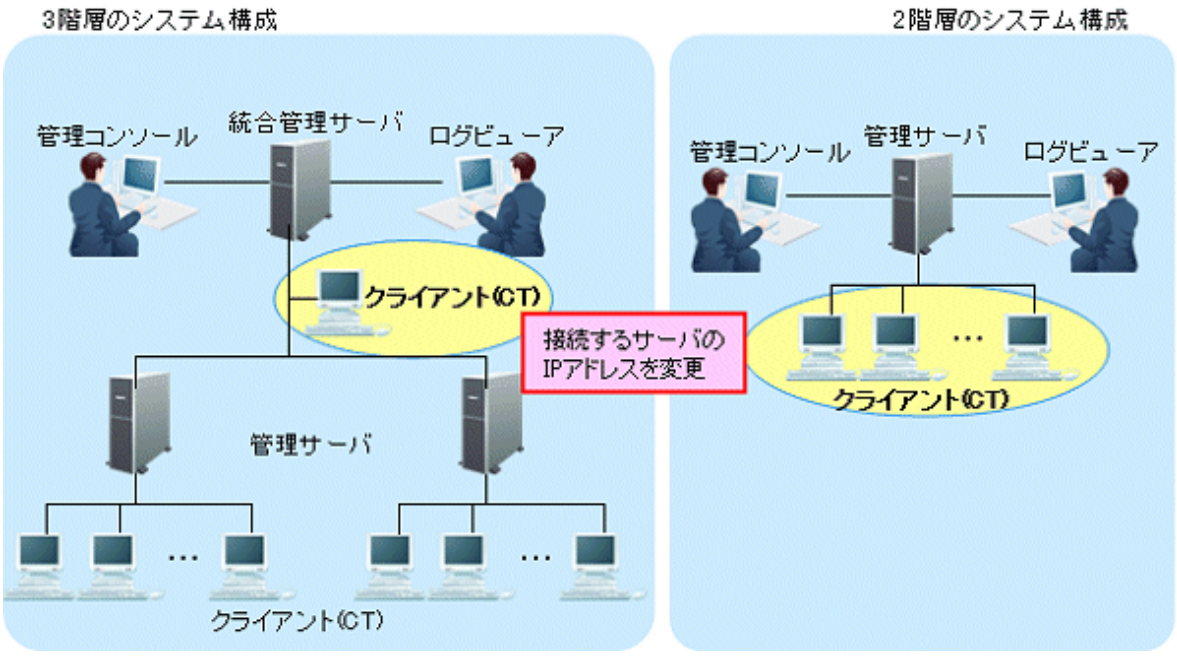
e. [閉じる]ボタンをクリックします。

f. サービスを起動します。

3階層での統合管理サーバ配下の管理サーバのサービスを起動します。

1. [サーバ設定ツール]を起動します。
2. [サービス]メニューから[サービス起動]を選択します。

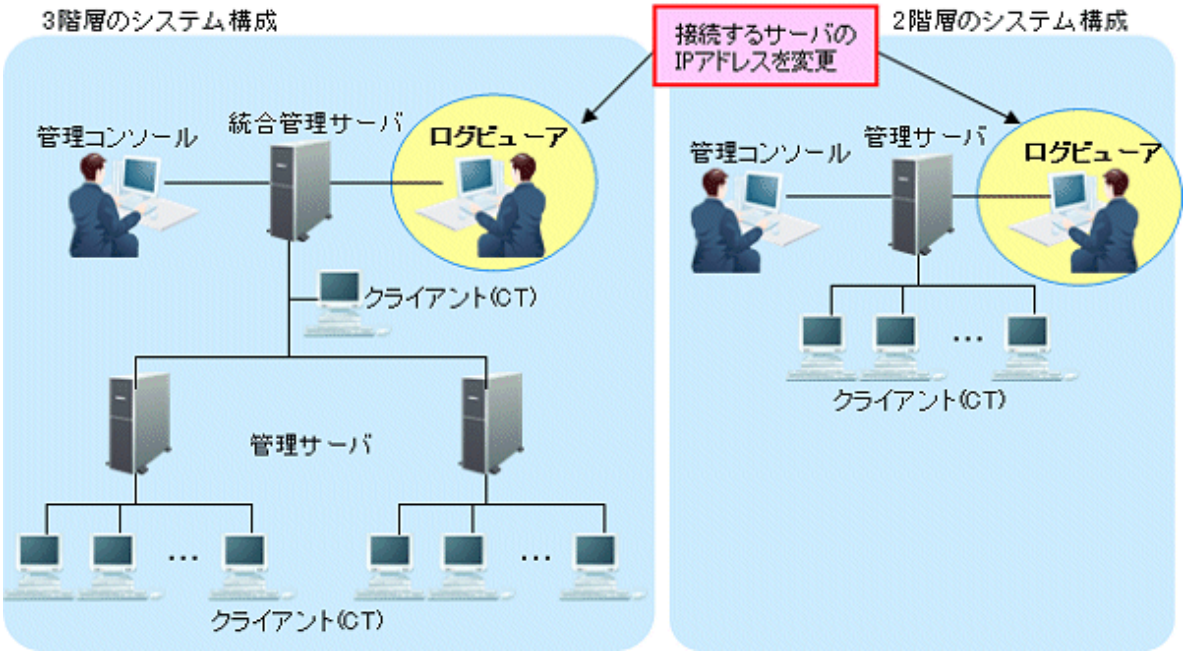
5. CT環境を変更します。



以下の場合は、“7.7.1 接続先の管理サーバ/統合管理サーバを変更する”を参照して、CT環境を変更してください。

- 3階層での統合管理サーバのIPアドレスを変更した場合で、その統合管理サーバ配下にクライアント(CT)が接続されているとき
- 2階層での管理サーバのIPアドレスを変更した場合で、その管理サーバ配下にクライアント(CT)が接続されているとき

6. ログビューア環境を変更します。

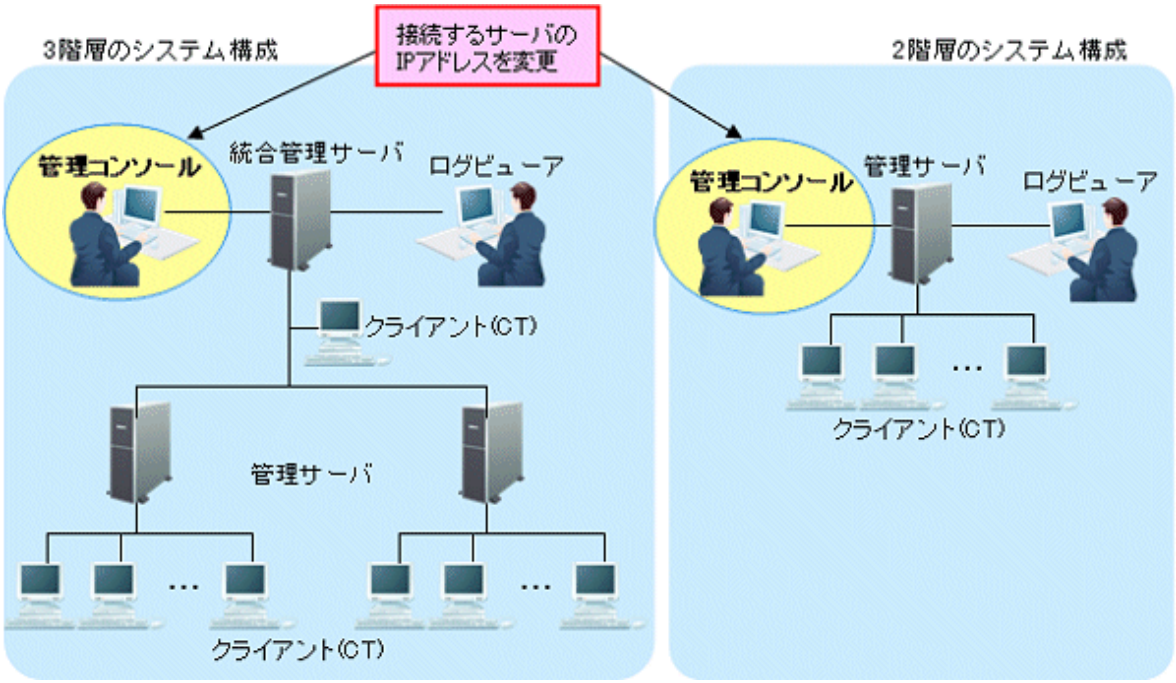


以下の場合は、“ログビューアを起動する”を参照して、ログビューア環境を変更してください。

- 3階層での統合管理サーバのIPアドレスを変更した場合で、ログビューアの接続先にその統合管理サーバが設定されているとき

ー 2階層での管理サーバのIPアドレスを変更した場合で、ログビューアの接続先にその管理サーバが設定されているとき

7. 管理コンソール環境を変更します。

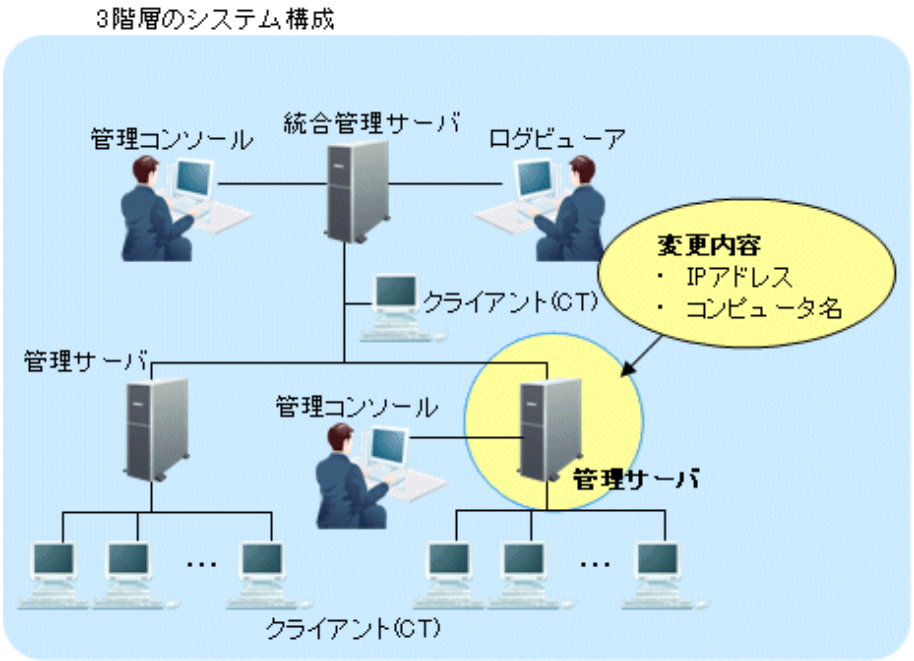


以下の場合は、“7.8 管理コンソール環境を変更する”を参照して、管理コンソール環境を変更してください。

ー 3階層での統合管理サーバのIPアドレスを変更した場合で、管理コンソールの接続先にその統合管理サーバが設定されているとき

ー 2階層での管理サーバのIPアドレスを変更した場合で、管理コンソールの接続先にその管理サーバが設定されているとき

3階層での管理サーバの環境だけを変更した場合

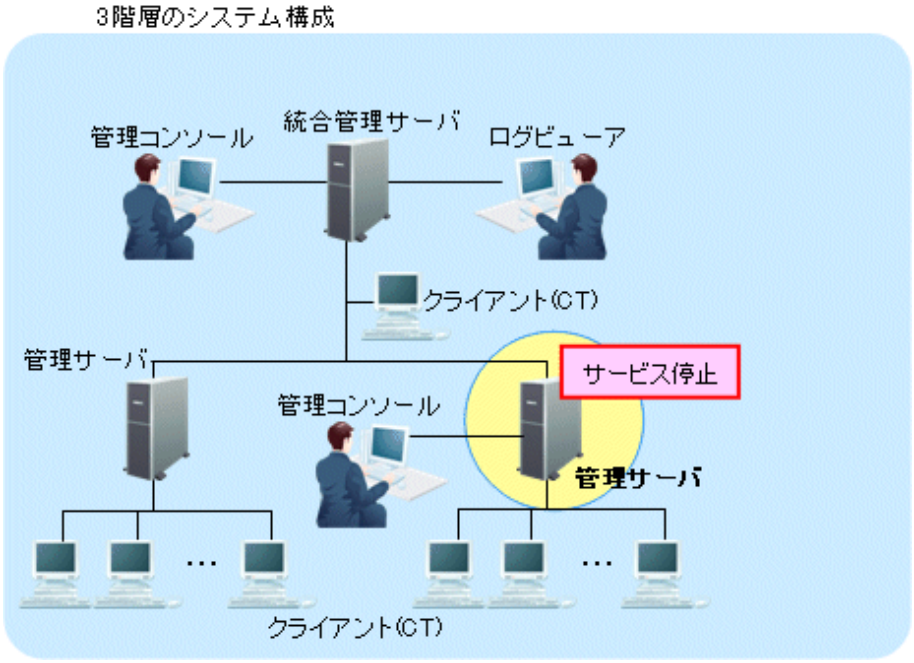


3階層での管理サーバだけで以下の情報を変更した場合に、管理サーバ環境を変更する方法を説明します(3階層での統合管理サーバの環境を変更していない場合です)。

- IPアドレス
- コンピュータ名

手順は、以下のとおりです。

1. 階層化サービスおよびサーバサービスを停止します。

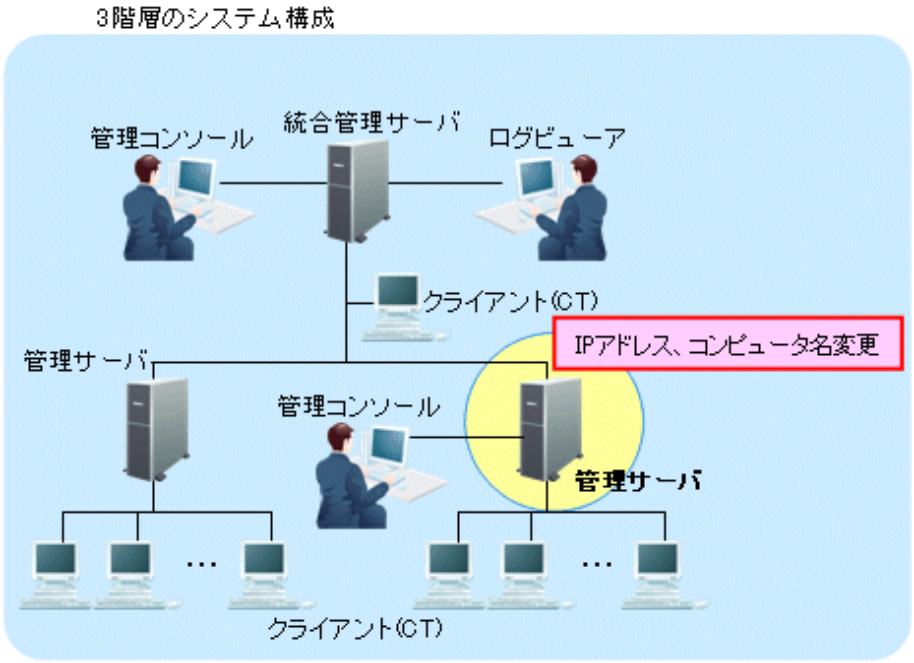


IPアドレスまたはコンピュータ名を変更する管理サーバが停止対象です。

a. [サーバ設定ツール]を起動します。

b. [サービス]メニューから[サービス停止]を選択します。

2. IPアドレス、コンピュータ名を変更します。



管理サーバが対象です。コンピュータ自体の設定を変更します。

a. IPアドレスを変更します。IPアドレスの変更が不要な場合は、次の手順に進んでください。

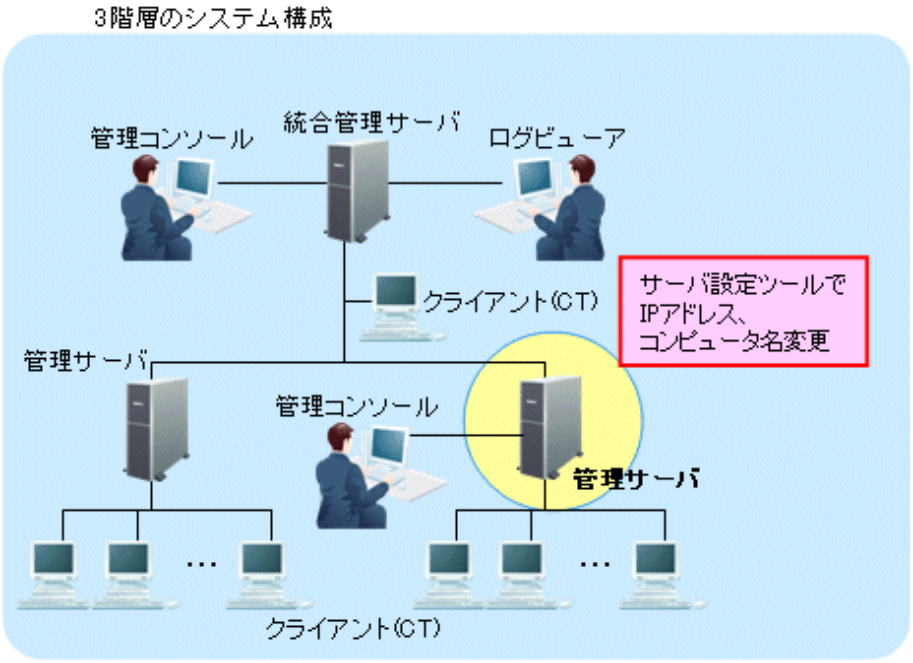
1. [スタート]メニューから[コントロールパネル]-[ネットワーク接続]-[ローカル エリア接続]を選択します。[ローカル エリア接続の状態]画面の[全般]タブで[プロパティ]ボタンをクリックします。
2. [インターネットプロトコル]を選択して、[プロパティ]ボタンをクリックします。
3. IPアドレスを変更して登録します。

b. コンピュータ名を変更します。コンピュータ名の変更が不要な場合は、次の手順に進んでください。

1. [スタート]メニューから[コントロールパネル]-[システム]を選択し、[システムのプロパティ]画面の[コンピュータ名]タブを表示します。
2. コンピュータ名を変更して登録します。

c. サーバを再起動します。

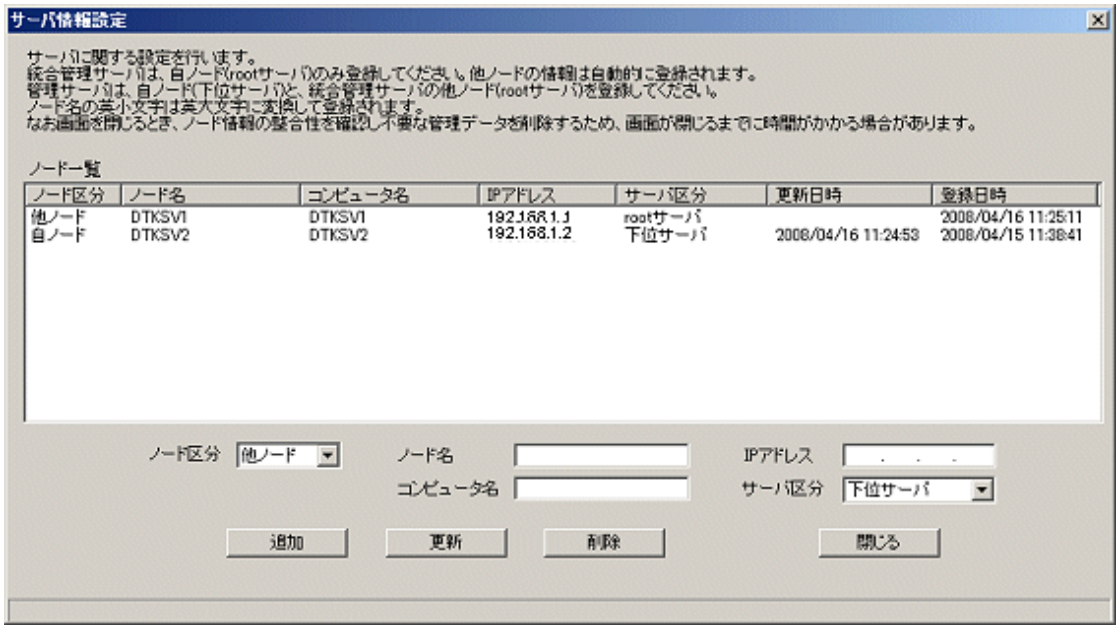
3. 3階層での管理サーバ上で、Systemwalker Desktop Keeperの設定を変更します。



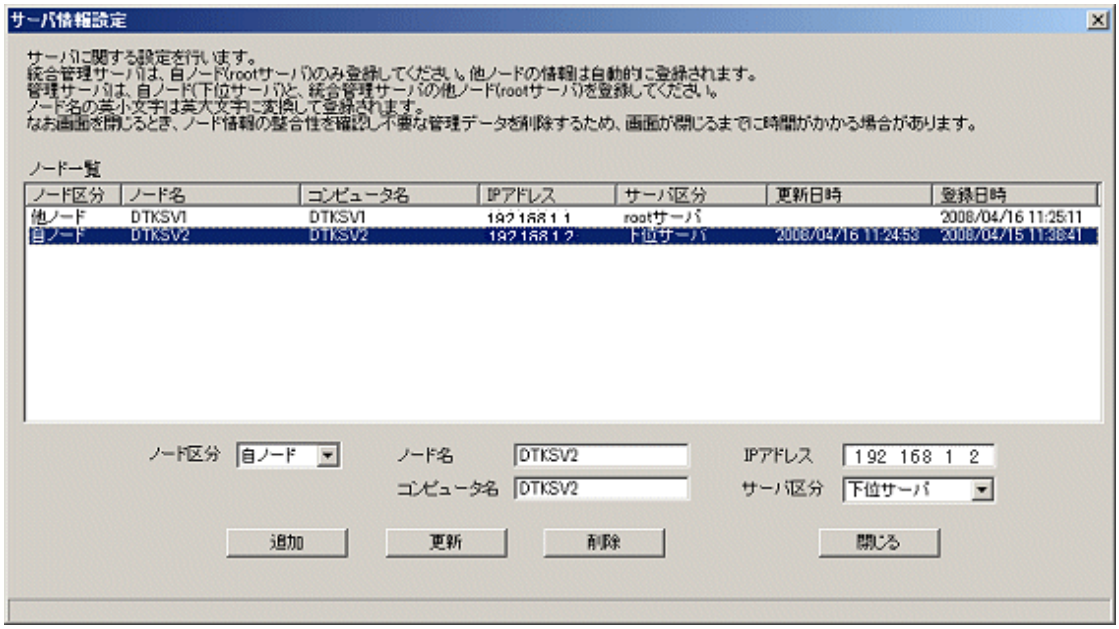
登録されている自分自身のサーバ情報設定を変更します。

a. サーバ設定ツールを起動します。

b. [サーバ情報設定]ボタンをクリックします。
→[サーバ情報設定]画面が表示されます。



c. ノード区分が自ノード(下位サーバ)のデータをクリックします。
→情報が画面下の入力フィールドに表示されます。



d. 変更する[コンピュータ名]または、[IPアドレス]を変更し、[更新]ボタンをクリックし、[閉じる]ボタンをクリックします。

注意

[コンピュータ名]と[IPアドレス]だけ変更してください

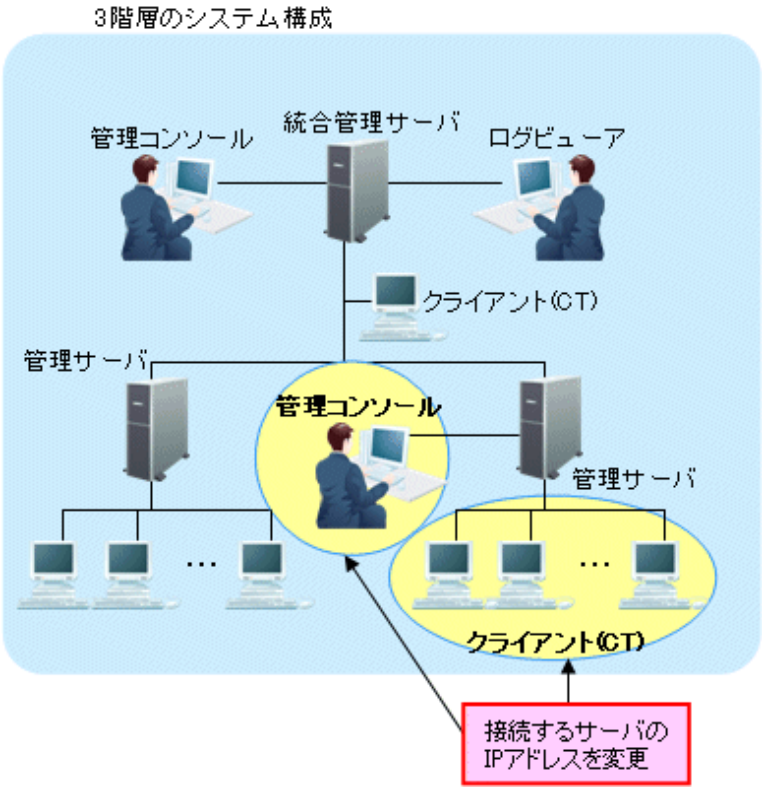
構成情報に不整合が発生するため、[コンピュータ名]および[IPアドレス]以外の項目の値は変更しないでください。

e. サービスを起動します。

設定変更を行った3階層での管理サーバのサービスを起動します。このとき、統合管理サーバを先に起動しておく必要があります。

1. [サーバ設定ツール]を起動します。
2. [サービス]メニューから[サービス起動]を選択します。
3. [サーバ設定ツール]を終了します。

4. CT環境を変更します。



以下の場合は、“7.7.1 接続先の管理サーバ/統合管理サーバを変更する”を参照して、CT環境を変更してください。

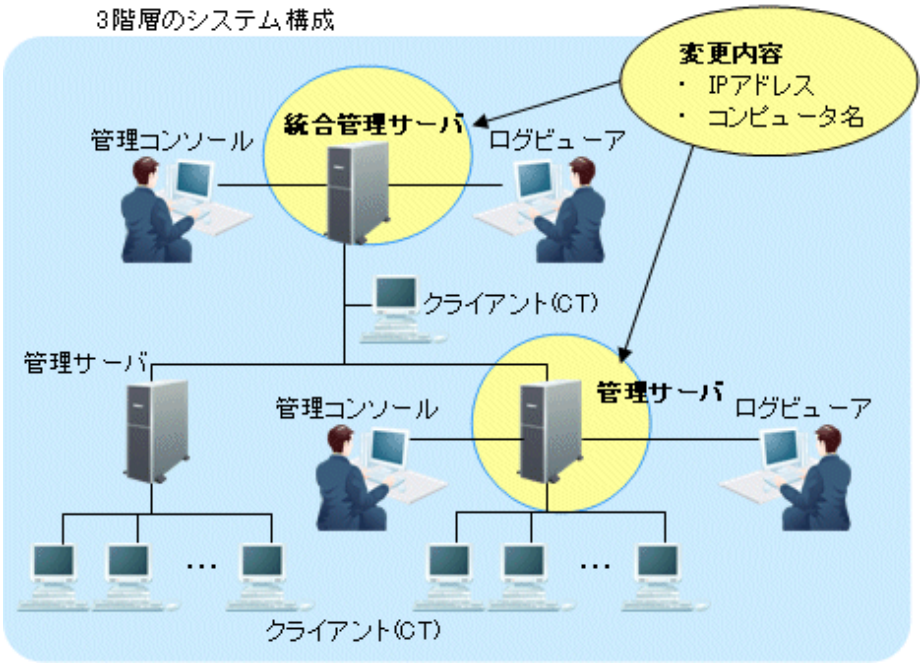
ー 3階層での管理サーバのIPアドレスを変更した場合で、その管理サーバ配下にクライアント(CT)が接続されているとき

5. 管理コンソール環境を変更します。

以下の場合は、“7.8 管理コンソール環境を変更する”を参照して、管理コンソール環境の変更を行ってください。

ー 3階層での管理サーバのIPアドレスを変更した場合で、管理コンソールの接続先にその管理サーバが設定されているとき

3階層での統合管理サーバおよび統合管理サーバ配下の管理サーバの環境を変更した場合



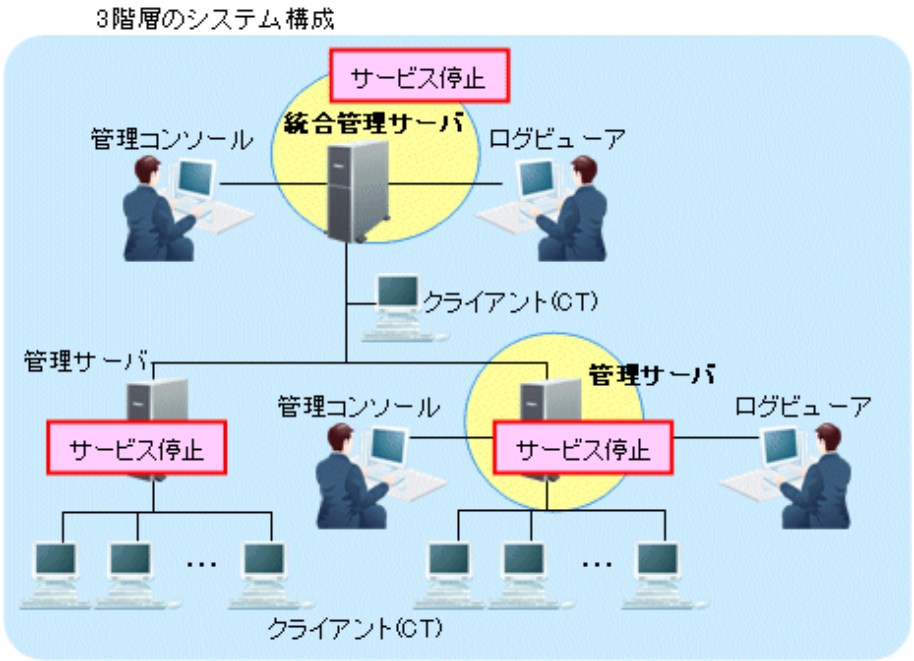
3階層での統合管理サーバ、および統合管理サーバ配下の管理サーバで以下の情報を変更した場合に、管理サーバ/統合管理サーバ環境を変更する方法を説明します。

- IPアドレス
- コンピュータ名

管理サーバおよび統合管理サーバの環境を変更後、もとの環境に戻すために必要な情報は、保存されていません。もとの環境に戻す場合に備え、手順にしたがって、ノードの情報(ノード名、コンピュータ名、IPアドレス、サーバ区分)を控えておくことをお勧めします。

手順は、以下のとおりです。

1. 階層化サービスおよびサーバサービスを停止します。

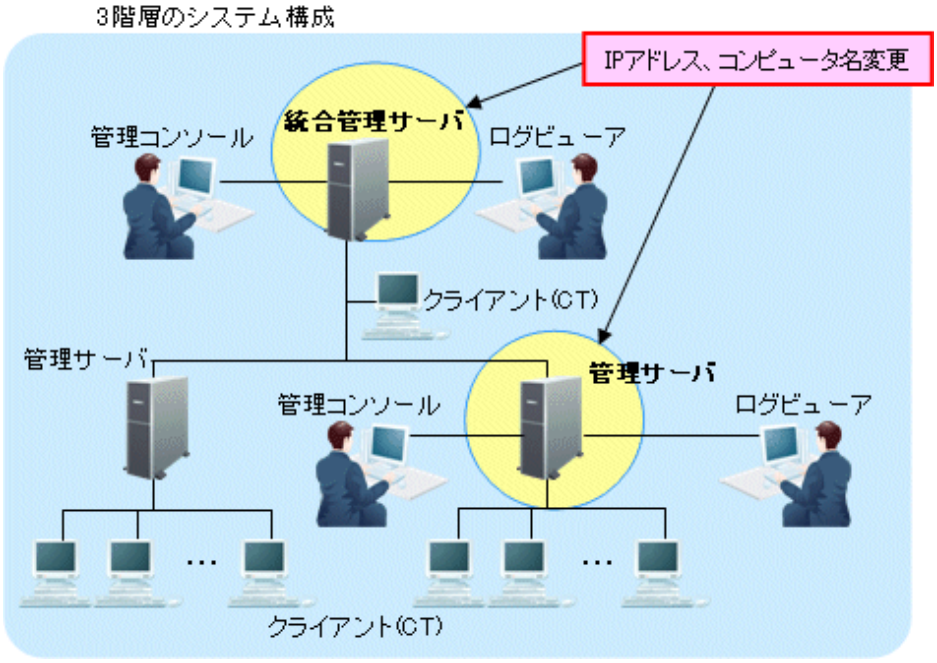


3階層での統合管理サーバおよび統合管理サーバ配下のすべての管理サーバが停止対象です。

a. [サーバ設定ツール]を起動します。

b. [サービス]メニューから[サービス停止]を選択します。

2. IPアドレス、コンピュータ名を変更します。



3階層での統合管理サーバおよび統合管理サーバ配下の管理サーバが対象です。
コンピュータ自体の設定を変更します。

a. IPアドレスを変更します。IPアドレスの変更が不要な場合は、次の手順に進んでください。

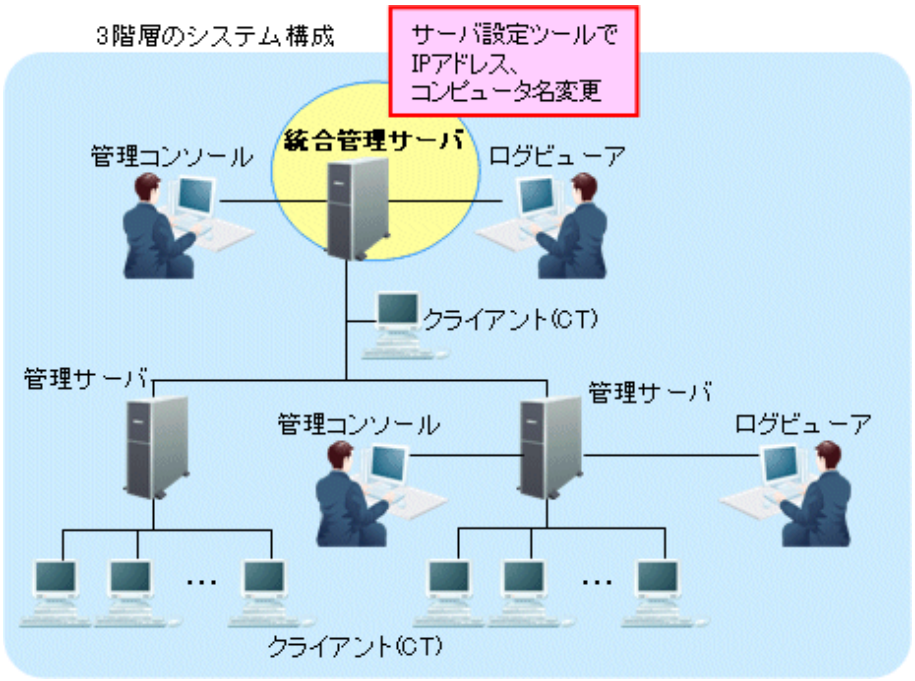
1. [スタート]メニューから[コントロールパネル]-[ネットワーク接続]-[ローカル エリア接続]を選択します。[ローカル エリア接続の状態]画面の[全般]タブで[プロパティ]ボタンをクリックします。
2. [インターネットプロトコル]を選択して、[プロパティ]ボタンをクリックします。
3. IPアドレスを変更して登録します。

b. コンピュータ名を変更します。コンピュータ名の変更が不要な場合は、次の手順に進んでください。

1. [スタート]メニューから[コントロールパネル]-[システム]を選択し、[システムのプロパティ]画面の[コンピュータ名]タブを表示します。
2. コンピュータ名を変更して登録します。

c. サーバを再起動します。

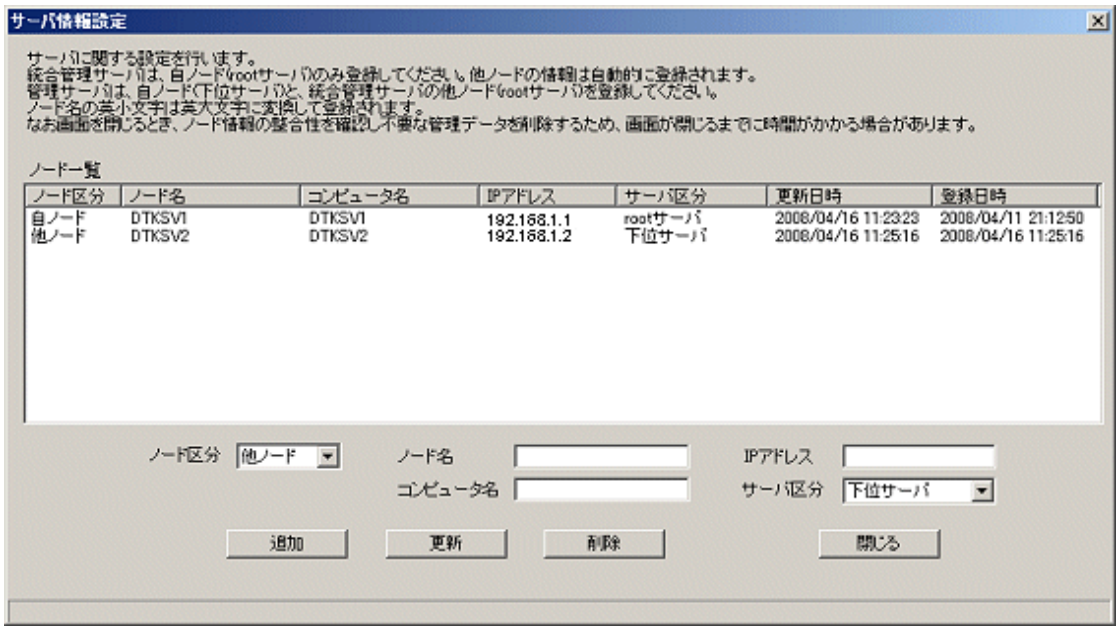
3. 統合管理サーバ上で、Systemwalker Desktop Keeperの設定を変更します。



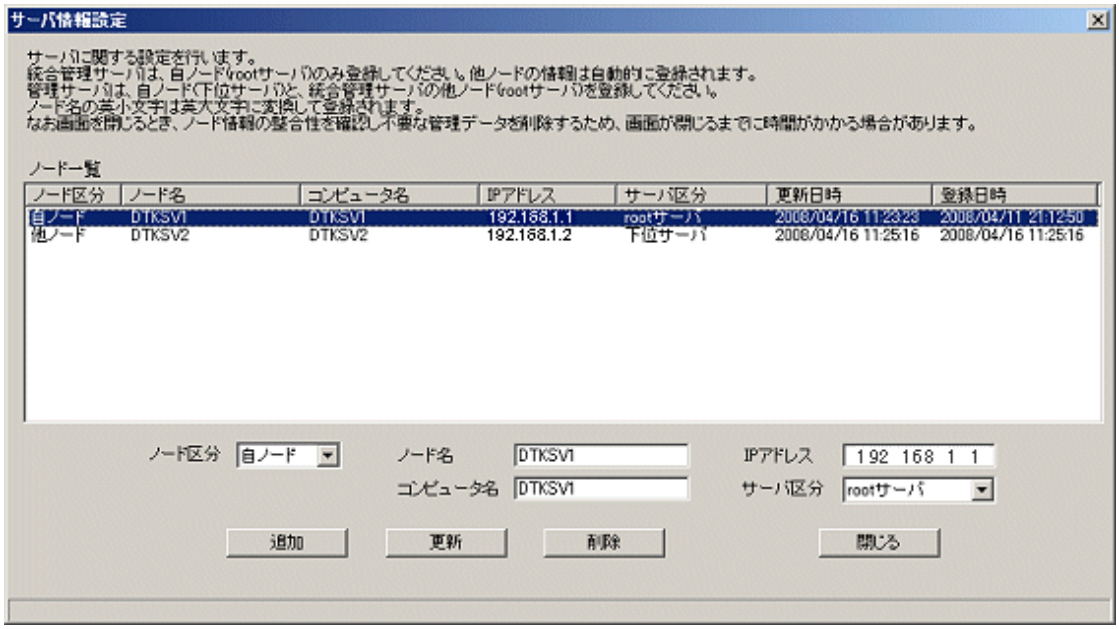
登録されている自分自身のサーバ情報設定を変更します。

a. サーバ設定ツールを起動します。

b. [サーバ情報設定]ボタンをクリックします。
→[サーバ情報設定]画面が表示されます。



c. ノード区分が自ノード(rootサーバ)のデータをクリックします。
→情報が画面下の入力フィールドに表示されます。



d. 変更する[コンピュータ名]または、[IPアドレス]を変更し、[更新]ボタンをクリックし、[閉じる]ボタンをクリックします。

注意

[コンピュータ名]と[IPアドレス]だけ変更してください

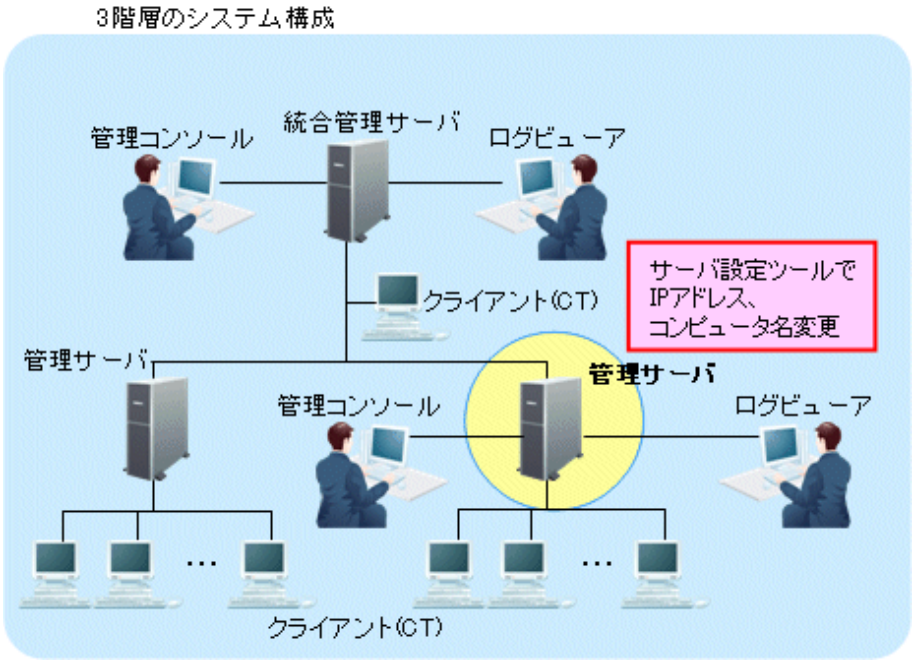
構成情報に不整合が発生するため、[コンピュータ名]および[IPアドレス]以外の項目の値は変更しないでください。

e. サービスを起動します。

設定変更を行った3階層での統合管理サーバのサービスを起動します。

1. [サーバ設定ツール]を起動します。
2. [サービス]メニューから[サービス起動]を選択します。

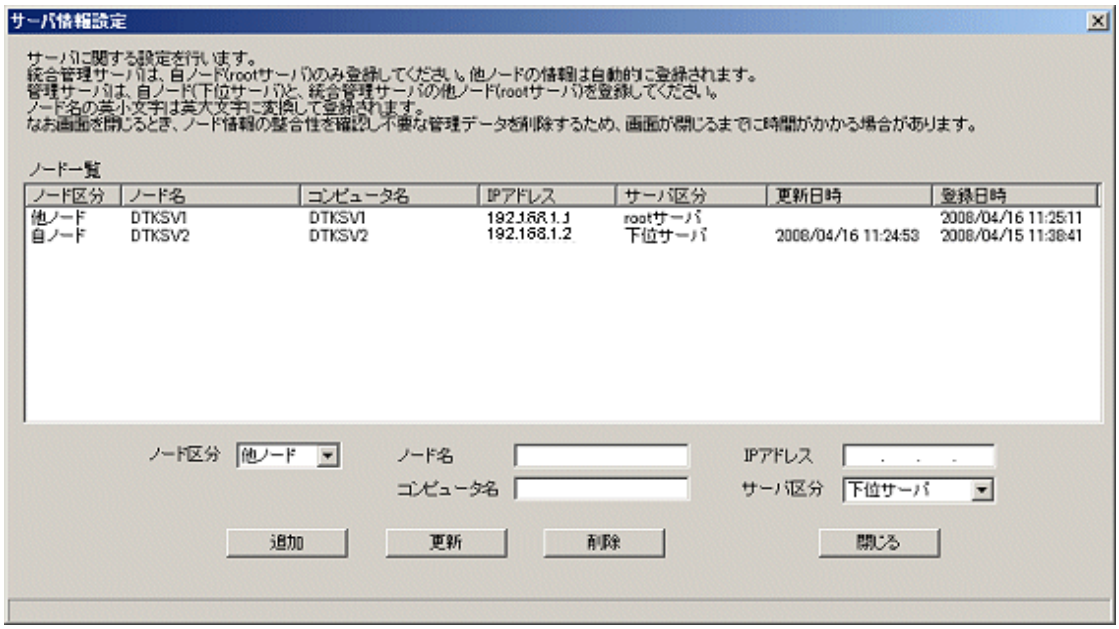
4. 管理サーバ上で、Systemwalker Desktop Keeperの設定を変更します。
(IPアドレス、コンピュータ名を変更した管理サーバでの設定)



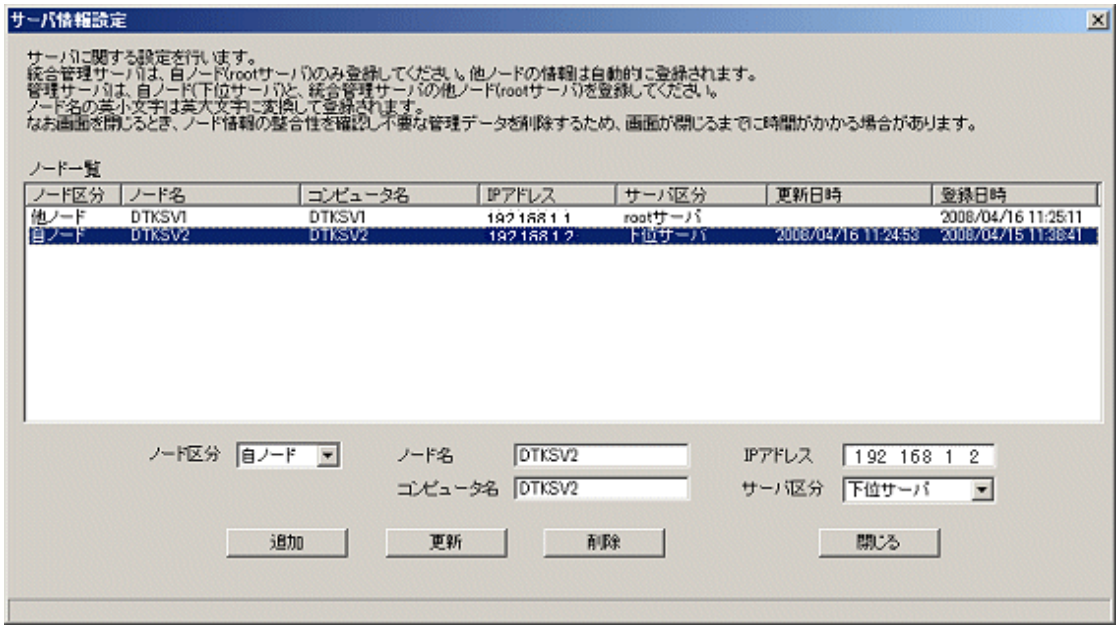
登録されている自分自身のサーバ情報設定、および統合管理サーバのサーバ情報設定を変更します。

a. サーバ設定ツールを起動します。

b. [サーバ情報設定]ボタンをクリックします。
→[サーバ情報設定]画面が表示されます。

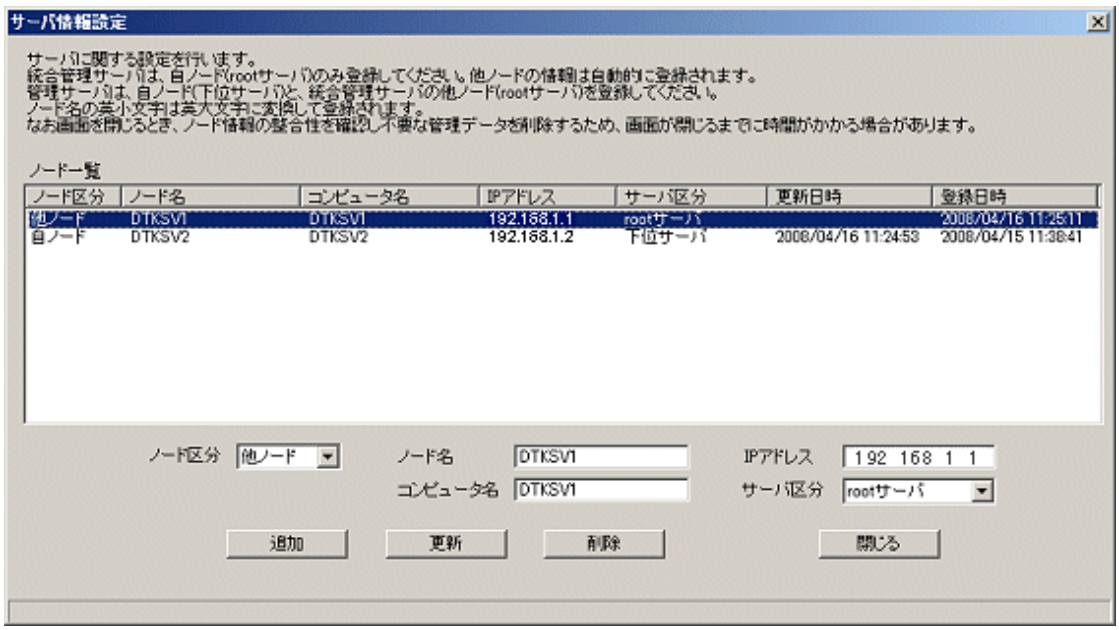


c. ノード区分が自ノード(下位サーバ)のデータをクリックします。
→情報が画面下の入力フィールドに表示されます。



d. 変更する管理サーバの[コンピュータ名]または[IPアドレス]を変更し、[更新]ボタンをクリックします。

e. ノード区分が他ノード(rootサーバ)のデータをクリックします。
→情報が画面下の入力フィールドに表示されます。



f. 以下の操作を実施します。

1. 表示されている他ノードの情報(ノード名、コンピュータ名、IPアドレス、サーバ区分)を控えます。
2. [削除]ボタンをクリックし、サーバ情報を削除します。
3. 以下の値を設定し、[追加]ボタンをクリックします。

・[ノード区分]:他ノード
・変更する統合管理サーバの[ノード名]、[コンピュータ名]、[IPアドレス]
・[サーバ区分]:rootサーバ

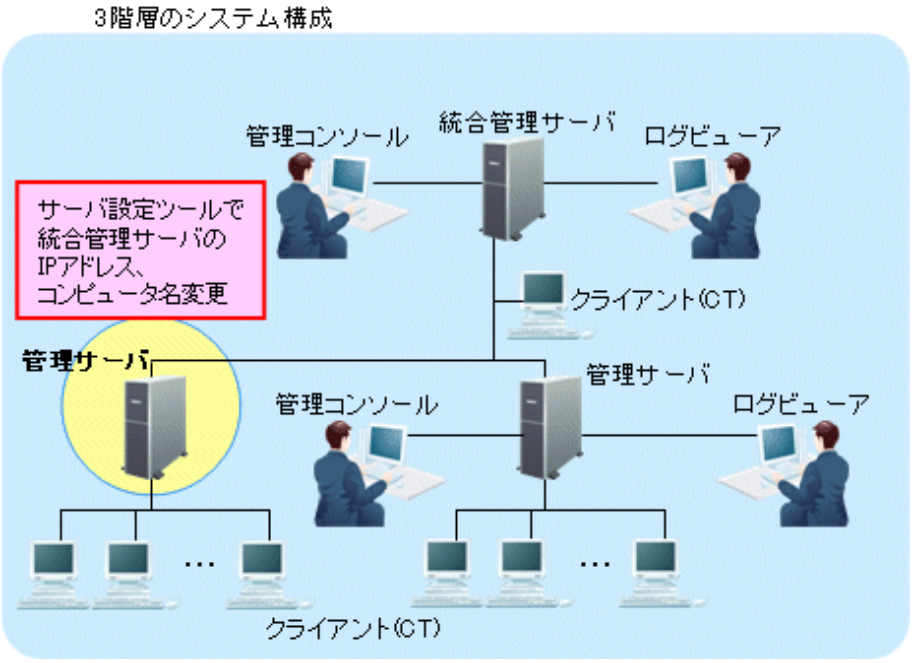
g. [閉じる]ボタンをクリックします。

h. サービスを起動します。

設定変更を行った3階層での統合管理サーバ配下の管理サーバのサービスを起動します。

1. [サーバ設定ツール]を起動します。
2. [サービス]メニューから[サービス起動]を選択します。

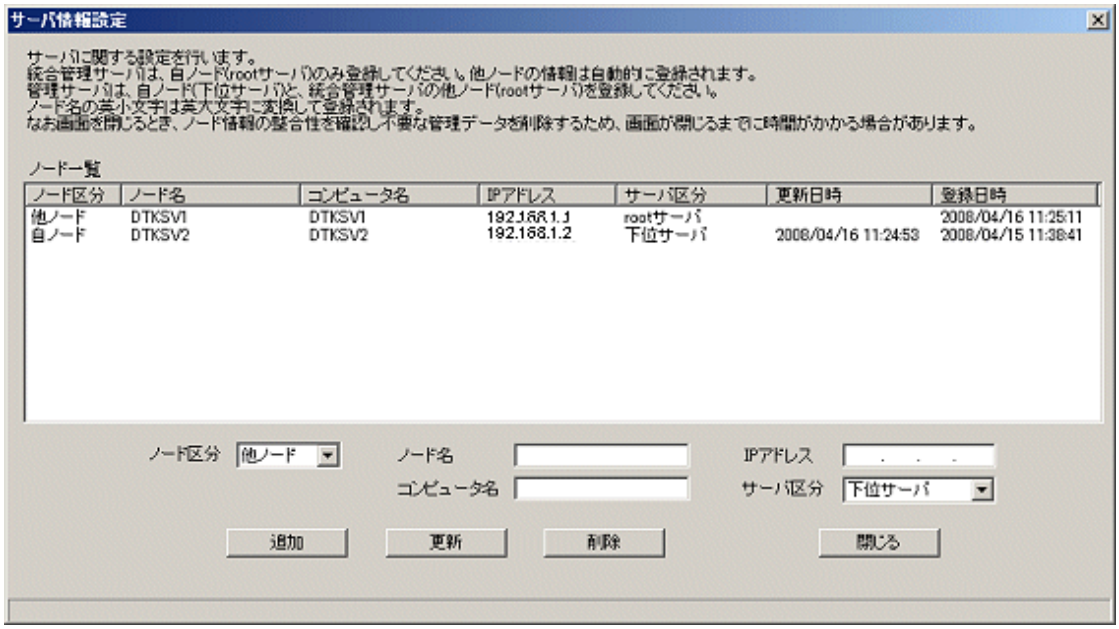
5. 管理サーバ上で、Systemwalker Desktop Keeperの設定を変更します。
(IPアドレス、コンピュータ名を変更していない管理サーバでの設定)



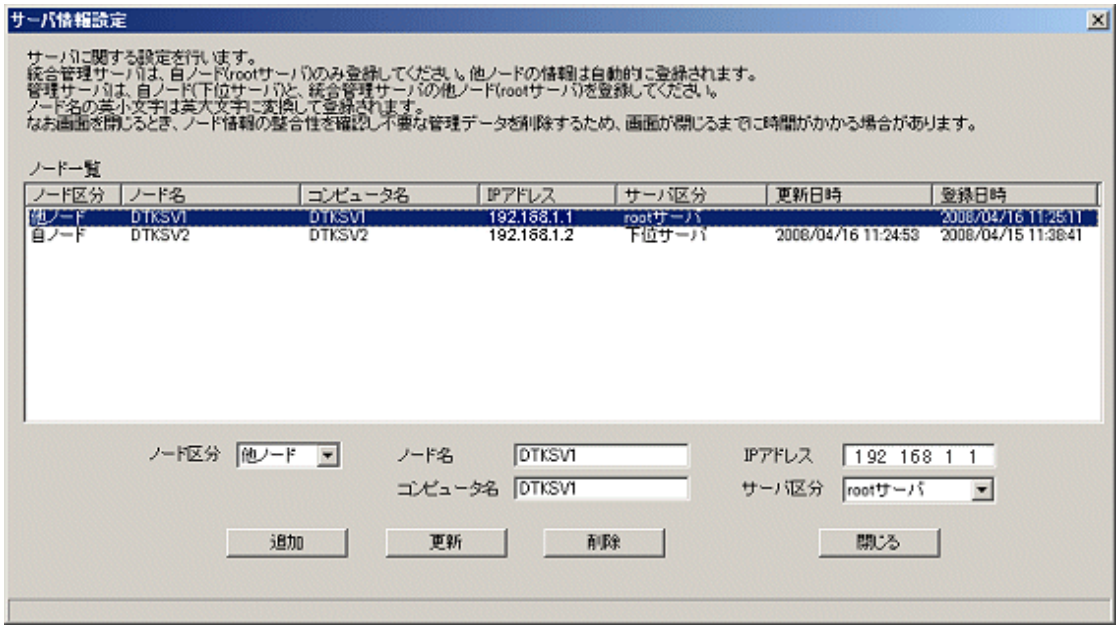
登録されている統合管理サーバのサーバ情報設定を変更します。

a. サーバ設定ツールを起動します。

b. [サーバ情報設定]ボタンをクリックします。
→[サーバ情報設定]画面が表示されます。



c. ノード区分が他ノード(rootサーバ)のデータをクリックします。
→情報が画面下の入力フィールドに表示されます。



d. 以下の操作を実施します。

1. 表示されている他ノードの情報(ノード名、コンピュータ名、IPアドレス、サーバ区分)を控えます。
2. [削除]ボタンをクリックし、サーバ情報を削除します。
3. 以下の値を設定し、[追加]ボタンをクリックします。

・[ノード区分]:他ノード
・変更する統合管理サーバの[ノード名]、[コンピュータ名]、[IPアドレス]
・[サーバ区分]:rootサーバ

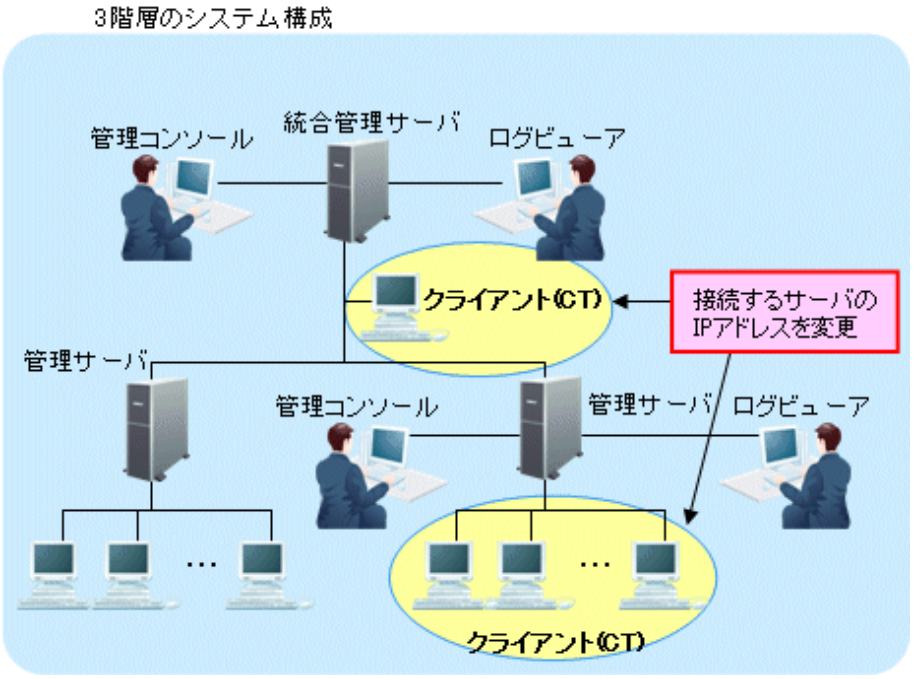
e. [閉じる]ボタンをクリックします。

f. サービスを起動します。

設定変更を行った3階層での統合管理サーバ配下の管理サーバのサービスを起動します。

1. [サーバ設定ツール]を起動します。
2. [サービス]メニューから[サービス起動]を選択します。

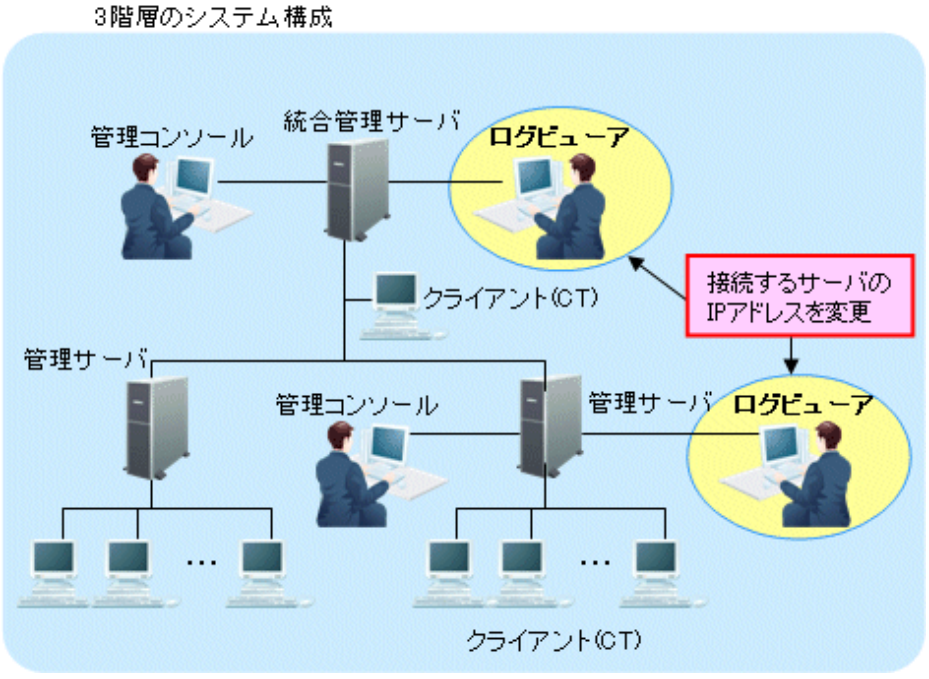
6. CT環境を変更します。



以下の場合は、“7.7.1 接続先の管理サーバ/統合管理サーバを変更する”を参照して、CT環境を変更してください。

ー 3階層での統合管理サーバおよび管理サーバのIPアドレスを変更した場合で、そのサーバ配下にクライアント(CT)が接続されているとき

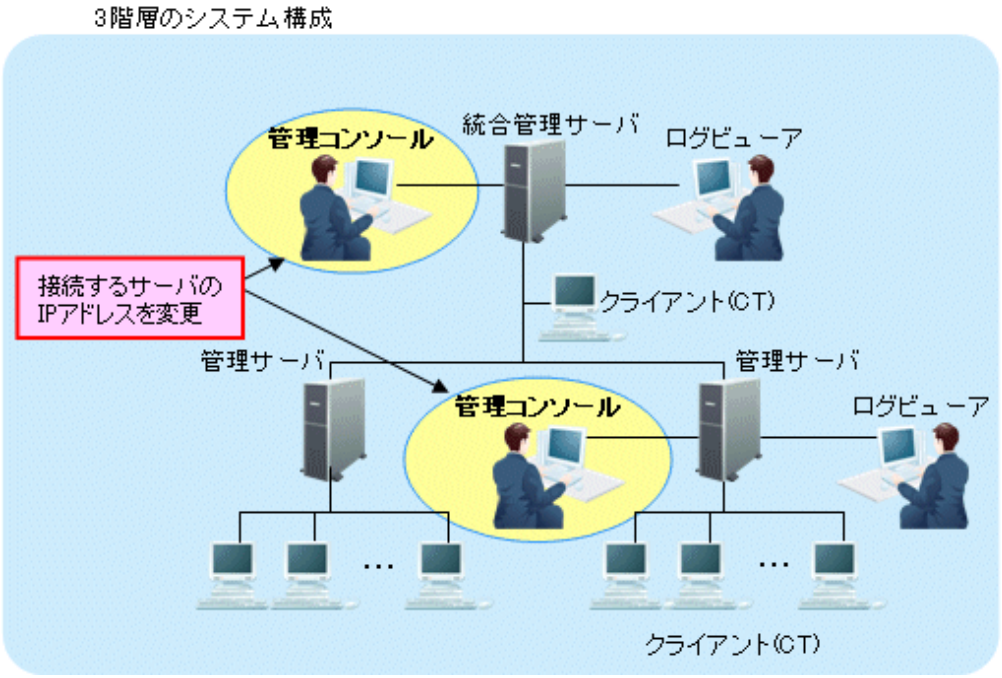
7. ログビューア環境を変更します。



以下の場合は、“ログビューアを起動する”を参照して、ログビューア環境を変更してください。

ー 3階層での統合管理サーバおよび管理サーバのIPアドレスを変更した場合で、ログビューアの接続先にそのサーバが設定されているとき

8. 管理コンソール環境を変更します。



以下の場合は、“7.8 管理コンソール環境を変更する”を参照して、管理コンソール環境を変更してください。

ー 3階層での統合管理サーバおよび管理サーバのIPアドレスを変更した場合で、管理コンソールの接続先にそのサーバが設定されているとき

7.9.5 管理サーバの通信情報を変更する

Systemwalker Desktop Keeperのインストールアプリケーション間の通信で使用するポート番号や通信設定を変更することができます。

ポート番号を変更した場合、変更したポート番号がファイアウォールで遮断されているときは、開放する必要があります。

注意

ポート番号を確認してください

ポート番号を変更する前に“Systemwalker Desktop Keeper リファレンスマニュアル”の“ポート番号一覧”を参照して、使用するポート番号を確認してください。

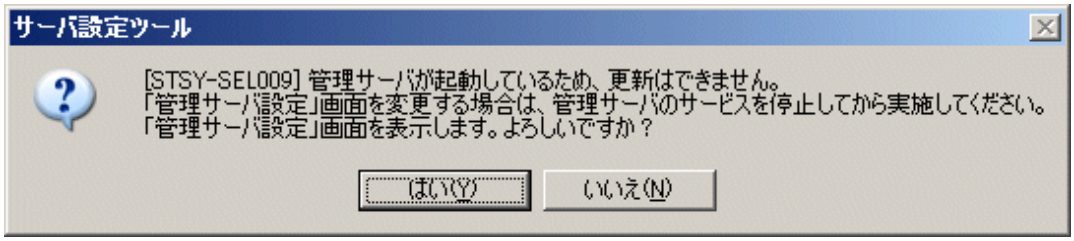
1. [スタート]メニューから[プログラム]-[Systemwalker Desktop Keeper]-[サーバ]-[サーバ設定ツール]を選択します。

   →[サーバ設定ツール]画面が表示されます。

2. 目的によって以下の操作を実施します。

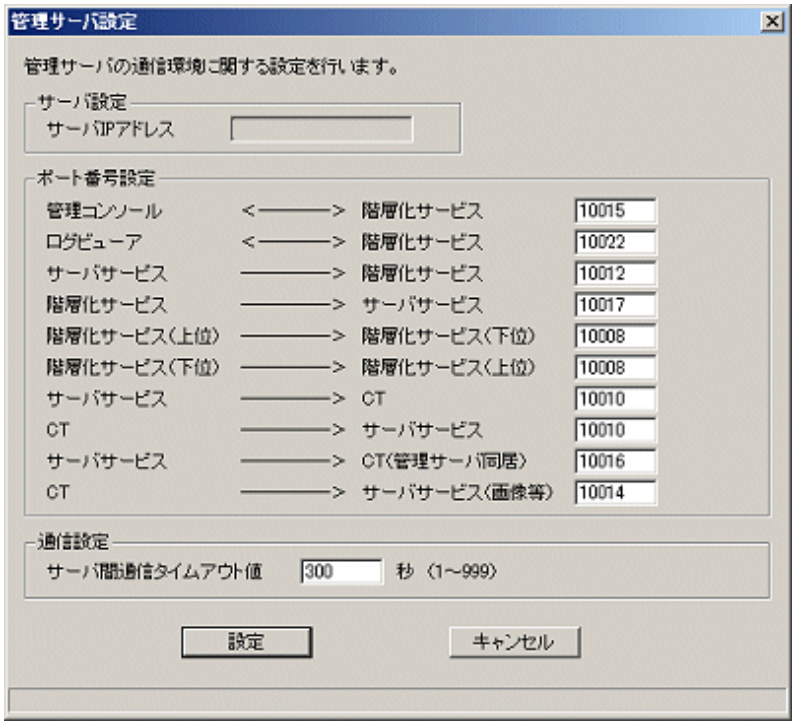
   【設定を変更する場合】
   設定を変更する管理サーバ、統合管理サーバのサービスを停止します。サービスの停止方法は、“管理サーバサービスを停止する”を参照してください。

【設定を参照する場合】
手順3に進みます。サービスが起動している場合は、以下の確認画面が表示されますが、[はい]ボタンをクリックしてください。



3. [管理サーバ設定]ボタンをクリックします。

→[管理サーバ設定]画面が表示されます(管理サーバをインストールした時に設定した値が表示されます)。



[サーバ設定]

項目名	説明
[サーバIPアドレス]	ポート番号や通信設定を変更する管理サーバのIPアドレスが表示されます。

[ポート番号設定]

項目名	説明
[管理コンソール←→階層化サービス]	管理コンソールと階層化サービスとの通信で使用するポート番号です。
[ログビューア←→階層化サービス]	ログビューアと階層化サービスとの通信で使用するポート番号です。
[サーバサービス→階層化サービス]	サーバサービスから階層化サービスへの通信で使用するポート番号です。
[階層化サービス→サーバサービス]	階層化サービスからサーバサービスへの通信で使用するポート番号です。
[階層化サービス(上位)→階層化サービス(下位)]	階層化サービス(上位)から階層化サービス(下位)への通信で使用するポート番号です。

項目名	説明
[階層化サービス(下位)→階層化サービス(上位)]	階層化サービス(下位)から階層化サービス(上位)への通信で使用するポート番号です。
[サーバサービス→CT]	サーバサービスからクライアント(CT)への通信で使用するポート番号です。
[CT→サーバサービス]	クライアント(CT)からサーバサービスへの通信で使用するポート番号です。
[サーバサービス→CT(管理サーバ同居)]	サーバサービスと同じサーバにクライアント(CT)を導入する場合にサーバサービスからクライアント(CT)への通信で使用するポート番号です。([サーバサービス→CT]で指定した番号は指定できません)
[CT→サーバサービス(画像等)]	クライアント(CT)からサーバサービスへ画面キャプチャデータを送信する場合や一括ログを送信する場合に使用するポート番号です。([CT→サーバサービス] で指定した番号は指定できません)

[通信設定]

項目名	説明
[サーバ間通信タイムアウト値]	管理コンソール、ログビューア、階層化サービス、サーバサービスの間、および上下の階層化サービス間で行われる通信タイムアウト値を入力します。

4. 必要に応じて設定を変更後、[設定]ボタンをクリックします。

7.9.6 保存先フォルダを変更する

導入時に設定した以下の保存先は、運用中に変更できます。

- コマンドプロンプト・ログ保存先
- 付帯データ保存先
- 一括ログ受信・データ保存先

変更手順は、“Systemwalker Desktop Keeper 導入ガイド”の“保存先フォルダを設定する”を参照してください。

7.9.7 管理サーバ/統合管理サーバの移行に伴ってログアナライザ設定を移行する

運用中に管理サーバ/統合管理サーバを他のコンピュータに移行する場合で、ログアナライザサーバを導入している場合に必要な手順を説明します。

移行する管理サーバ/統合管理サーバ上で以下の設定を行います。

1. 移行前(現在運用中)のコンピュータにおいて、データ転送コマンド用設定ファイル(TRANS_SETTING.ini)を外部媒体などに退避します。

   設定ファイルの格納先は以下のとおりです。

   ```
   [Systemwalker Desktop Keeperインストールフォルダ]¥LogAnalyzer¥TRANS
   ```

2. 移行前(現在運用中)のコンピュータにおいて、RegisterLAInfo.exe(ログアナライザサーバ情報の登録コマンド)の情報出力オプションを使用して、ログアナライザサーバ情報をファイル出力し、外部媒体などに退避します。

   【出力ファイルパスを“C:¥work¥lasvinfo.csv”とした場合の実行例】

   ```
   [Systemwalker Desktop Keeperインストールフォルダ]¥LogAnalyzer¥TRANS¥RegisterLAInfo.exe -e C:¥work¥lasvinfo.csv
   ```

3. 移行前のコンピュータにおいて、管理サーバのアンインストールを行います。

4. 移行先のコンピュータに、管理サーバのインストールを行います。
5. 外部媒体などへ退避したデータ転送コマンド用設定ファイル(TRANS_SETTING.ini)を、移行先のコンピュータへコピーします。

   設定ファイルのコピー先は以下のとおりです。

   ```
   [Systemwalker Desktop Keeperインストールフォルダ]¥LogAnalyzer¥TRANS
   ```

6. 外部媒体などへ退避したログアナライザサーバ情報のファイルを移行先のコンピュータへコピーし、RegisterLAInfo.exe(ログアナライザサーバ情報の登録コマンド)の情報登録オプションを使用して、ログアナライザサーバ情報を再登録します。

   【コピーしたファイルパスを“C:¥WORK¥lasvinfo.csv”とした場合の実行例】

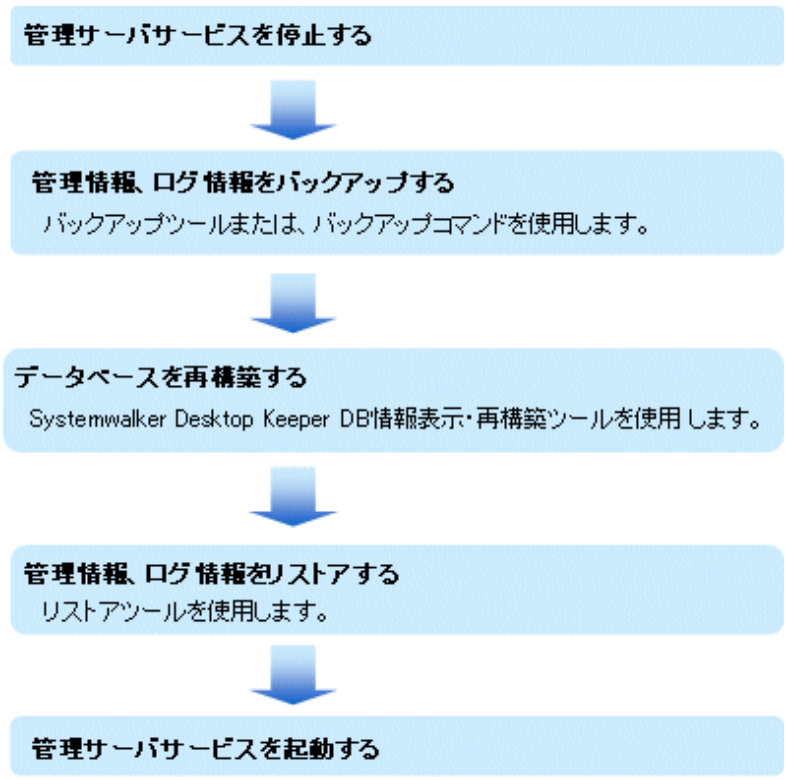
   ```
   [Systemwalker Desktop Keeperインストールフォルダ]¥LogAnalyzer¥TRANS¥RegisterLAInfo.exe -r C:¥WORK¥lasvinfo.csv
   ```

7.10 管理サーバのデータベースを再構築する

運用中にデータベースの容量変更を行う場合は、運用環境保守ウィザード(情報表示・再構築)を使用します。

データベースの再構築では、現在のデータベースは一旦削除されます。したがって、再構築前には、管理情報、ログ情報のバックアップを必ず実施してください。

データベースの再構築は、以下の手順で行います。



管理サーバサービスを停止する

再構築する管理サーバ、または統合管理サーバのサービスを停止します。

以下の手順を行わない場合、データベースに格納される前のクライアント(CT)のログが失われることがありますので、注意してください。

1. [サーバ設定ツール]を起動します。
2. [サービス]メニューから[サービス停止]を選択します。

管理情報、ログ情報をバックアップする

管理情報、ログ情報のバックアップは、バックアップツールまたは、バックアップコマンドを使用します。操作方法は“Systemwalker Desktop Keeper 導入ガイド”の“バックアップツール(GUI)を利用する”、“バックアップコマンドを利用する”を参照してください。

注意

管理情報とログ情報を、必ずバックアップしてください

データベース再構築により、データベースが初期化されます。データベースの再構築作業の前には必ず、管理情報、ログ情報のバックアップを実施してください。実施しなかった場合はシステムを復元できません。

データベースを再構築する

運用環境保守ウィザード(情報表示・再構築)を使用して、すでに構築されているデータベースを再構築します。

データベースを再構築する場合、新しく指定したフォルダにデータベースを作成した後に旧フォルダにあるデータベースを削除します。したがって、同じドライブにデータベースを再構築する場合、新しく作成できるデータベースの容量は、ドライブの残容量の範囲(ドライブの全容量から旧データベースの容量をひいた容量の範囲)内に限られます。

事前に容量の試算を実施してください。

1. PCに、データベース構築時のユーザーでログオンします。
2. [スタート]メニューから[プログラム]-[Systemwalker Desktop Keeper]-[サーバ]-[運用環境保守ウィザード(情報表示・再構築)]を選択します。

   →[運用環境保守ウィザード(情報表示・再構築)]画面が表示されます。

3. [情報取得]ボタンをクリックし、現在のデータベース容量を確認します。

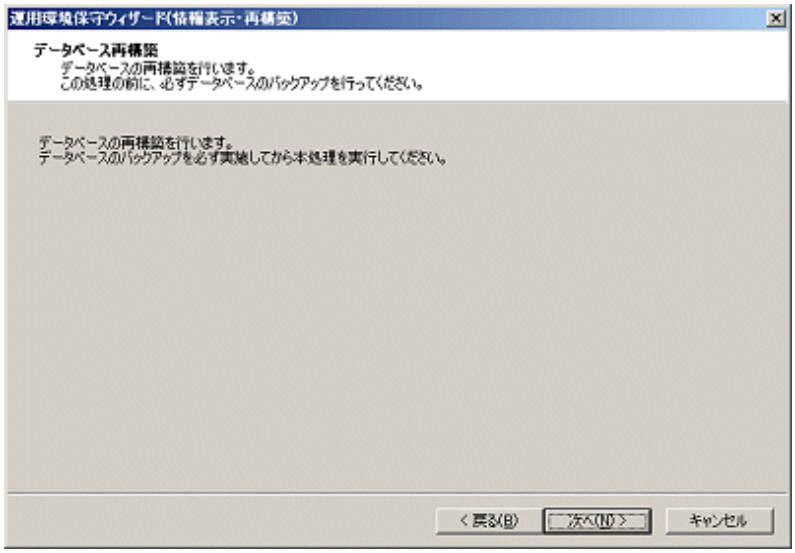
   →以下の画面が表示されます。

4. 表示内容を確認します。

項目名		説明
[データベース割当量]		割り当てたデータベース容量に対する初期割り当て容量(現在のデータベースの使用容量)の比率です。 容量値は、この値(%)に“データベース容量”を掛けて算出されます。 残りの容量は、拡張用として使用されます。
[データベース構築情報]	[データベース作成先]	現在のデータベース作成先ドライブ、フォルダが表示されます。
	[全体のCT台数]	統合管理サーバで管理するCTの総台数です。 管理サーバを選択している場合は、表示されません。
	[CT 台数]	データベース作成時に指定したクライアント(CT)台数が表示されます。
	[ファイル操作ログ件数]	データベース作成時に指定した一日当たりのファイル操作ログ件数が表示されます。
	[ファイル操作ログ以外のログ件数]	データベース作成時に指定した一日当たりのファイル操作ログ以外のログ件数が表示されます。
	[保存月数]	データベース作成時に指定したログの保存月数が表示されます。
	[データベース容量]	現在のデータベース容量(MB)が表示されます。
	[データベース割当済容量]	現在のデータベース割当済容量(MB)が表示されます。
	[データベース拡張領域の容量]	現在のデータベース拡張領域の容量(MB)が表示されます。この値はデータベース拡張のための予備領域で、データベース未使用領域の一部です
	[ディスク空き容量]	現在のデータベース作成先ドライブの空き容量(MB)が表示されます。

5. [再構築]ボタンをクリックします。

   →以下の画面が表示されます。



6. [次へ]ボタンをクリックします。

   →以下の画面が表示されます。

項目名		説明
[データベース再構築先]		データベースの構築先を変更する場合に入力します。 [参照]ボタンをクリックし、新たなデータベースの構築先フォルダを指定してください。 ネットワーク上のフォルダや、フォーマット形式がNTFS以外のファイルシステムを指定することはできません。 データベース構築先のフォルダ名として指定できる文字数は、32バイトまでです。空白、ひらがな、カタカナ、漢字などのマルチバイト文字は指定できません。
[データベース容量の試算]	[全体のCT台数]	統合管理サーバで管理するCTの総台数を1～50000の範囲で入力します。 管理サーバを選択している場合は、入力できません。

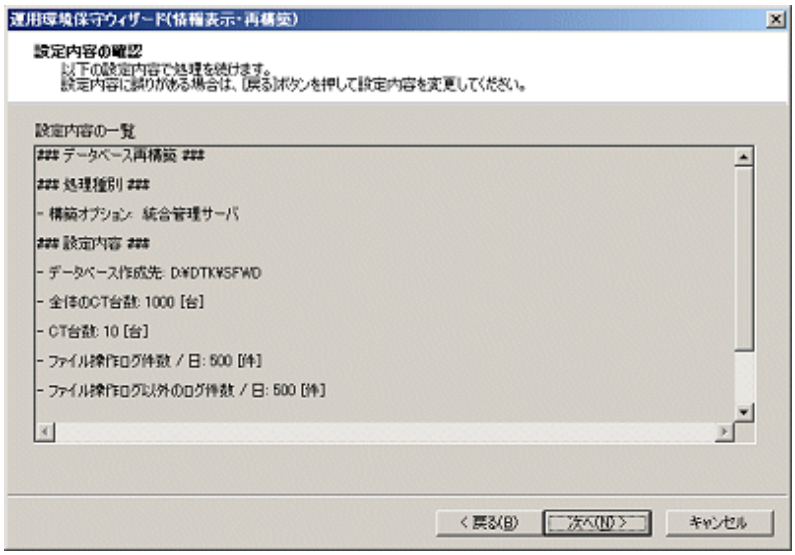
項目名		説明
	[このサーバで管理するCT台数] (必須)	接続するCT台数を入力します。 1～2000台まで入力できます。
	[ファイル操作ログ件数] (必須)	1日あたりのファイル操作ログ件数を入力します。 1～99999で入力します。 該当ログを取得しない場合は「1」を入力します。
	[ファイル操作ログ以外のログ件数] (必須)	1日あたりのファイル操作ログ以外のログ件数を入力します。 1～99999で入力します。 該当ログを取得しない場合は「1」を入力します。
	[保存月数] (必須)	ログを保存する月数を選択します。

7. 必要な項目を入力し、[容量試算]ボタンをクリックします。

   →データベース容量が算出され、[データベース容量]に表示されます。
   表示されたデータベース容量を、事前に見積もった試算値に置き替えてください。

8. [次へ]ボタンをクリックします。

   →以下の画面が表示されます。



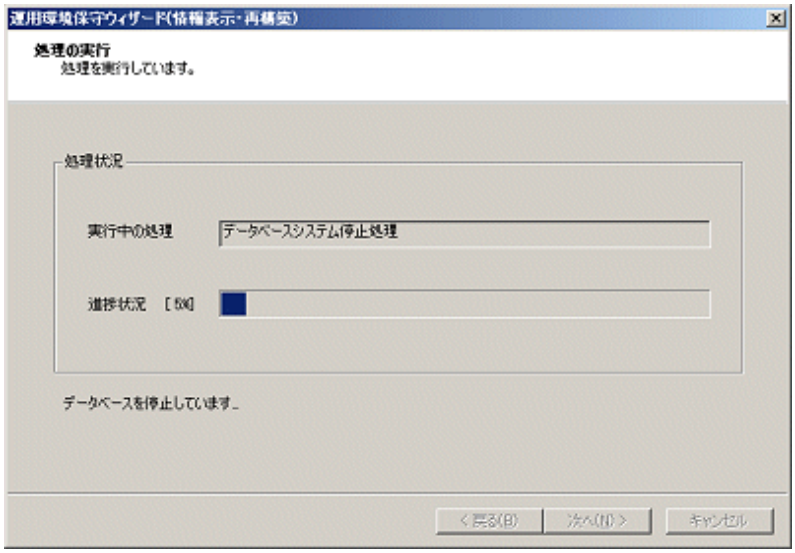
9. 設定内容を確認します。

   【表示される確認項目】

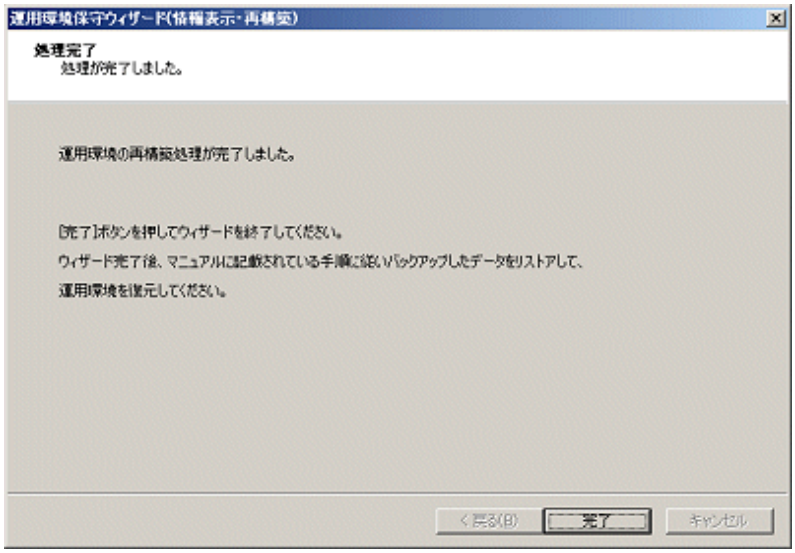
   - 対象処理
   - データベース作成先
   - クライアント台数
   - ファイル操作ログ件数(1日当たり)
   - ファイル操作ログ以外のログ件数(1日当たり)
   - 保存月数
   - データベース容量
   - ディスク空き容量

10. [次へ]ボタンをクリックします。

→以下の画面が表示され再構築処理が実施されます。



→処理が終了すると以下の画面が表示されます。



データベースの再構築処理が完了した後は、データベースの再構築作業前にバックアップした管理情報やログ情報を、必ずリストアツールを使用して再構築したデータベースにリストアしてください。

管理情報、ログ情報をリストアする

データベースの再構築作業前にバックアップした管理情報やログ情報を、リストアツールを使用して再構築したデータベースにリストアします。

管理情報、ログ情報のリストア方法は“Systemwalker Desktop Keeper 導入ガイド”の“リストアツールを利用する”を参照してください。

管理サーバサービスを起動する

以下の手順を行わない場合、データベースに格納される前のクライアント(CT)のログが失われることがありますので、注意してください。

停止している管理サーバ、または統合管理サーバのサービスを起動します。

1. サービスを起動します。
2. [サーバ設定ツール]を起動します。
3. [サービス]メニューから[サービス起動]を選択します。

7.11 ログアナライザサーバ環境を変更する

7.11.1 ログアナライザサーバを移行する

運用中にログアナライザサーバを他のコンピュータに移行する手順を、以下に説明します。

1. 移行前(現在運用中)のコンピュータにおいて、共有フォルダ(ログデータの転送に指定しているフォルダ)のログ情報退避CSVファイルを、外部媒体などへフォルダ構成を維持したままコピーします。
2. LADBBKRS.bat(ログアナライザ設定情報退避・復元コマンド)のバックアップオプションを使用して、ログアナライザ設定情報を外部媒体などへ退避します。

   【退避先フォルダパスを“E:¥LAMASTERINFO”とした場合の実行例】

   ```
   [ログアナライザサーバインストールフォルダ]¥bin¥SWDTLAENV¥LADBBKRS.bat -bs -d E:¥LAMASTERINFO
   ```

3. 移行先のコンピュータに、ログアナライザサーバをインストールします。
4. 移行先のコンピュータに、運用環境保守ウィザードを使用して運用環境を構築します。
5. LADBBKRS.bat(ログアナライザ設定情報退避・復元コマンド)のリストアオプションを使用して、ログアナライザ設定情報を復元します。

   【退避元フォルダパスを“E:¥LAMASTERINFO”とした場合の実行例】

   ```
   [ログアナライザサーバインストールフォルダ]¥bin¥SWDTLAENV¥LADBBKRS.bat -rs -d C:¥LAMASTERINFO
   ```

6. 外部媒体などへ退避した共有フォルダのデータを、フォルダ構成を維持したまま、移行先のコンピュータの共有フォルダへコピーします。

   移行するデータの量は、運用環境構築時に指定した[保存月数]を超えないようにしてください。

7. コピーしたフォルダ配下に存在する、以下のファイル名を変更します。

   ー 変更前のファイル名:conv_end

   ー 変更後のファイル名:trans_end

   上記ファイルは、期間フォルダ(例:20080421_20080421)ごとに存在します。
   フォルダ数が多い場合は、以下のようにバッチ処理で変更すると便利です。

   【バッチファイルの例】

   ```
   ECHO OFF
   IF %1.==. GOTO NOPARAM
   FOR /R %1 /D %%f IN (*) DO (
     IF EXIST %%f¥conv_end (
       move %%f¥conv_end %%f¥trans_end
     )
   )
   GOTO END
   :NOPARAM
   ECHO フォルダパスを指定してください。
   :END
   ECHO ON
   ```

   【バッチファイルを“conv.bat”、共有フォルダパスを“C:¥LASVDATA”とした場合の実行例】

   ```
   conv.bat C:¥LASVDATA
   ```

8. DttoolEx.exe(データ移入・削除コマンド)を使用して、ログアナライザサーバへデータを追加します。

   【共有フォルダパスを“C:¥LASVDATA”とした場合の実行例】

```
[ログアナライザサーバインストールフォルダ]¥bin¥dttool¥DttoolEx.exe -f C:¥LASVDATA
```

9. LADBBKRS.bat(ログアナライザ設定情報退避・復元コマンド)のリストアオプションを使用して、ログアナライザ設定情報を再度復元します。

   【退避元フォルダパスを“E:¥LAMASTERINFO”とした場合の実行例】

```
[ログアナライザサーバインストールフォルダ]¥bin¥SWDTLAENV¥LADBBKRS.bat -rs -d C:¥LAMASTERINFO
```

注意

手順9.のログアナライザ設定情報の再リストアを行わないと、ユーザーIDが削除される、設定内容が最新の状態でないなど、正しく復元されない場合があります。

7.11.2 ログアナライザサーバのIPアドレス/ポート番号を変更する

運用中にログアナライザサーバのIPアドレスやポート番号を変更した場合の、運用環境の変更手順を、以下に説明します。

統合管理サーバ上で以下の設定を行います。

1. RegisterLAInfo.exe(ログアナライザサーバ情報の登録コマンド)の情報出力オプションを使用して、ログアナライザサーバ情報をファイル出力します。

   【出力ファイルパスを“C:¥work¥lasvinfo.csv”とした場合の実行例】

```
[Systemwalker Desktop Keeperインストールフォルダ]¥LogAnalyzer¥TRANS¥RegisterLAInfo.exe -e C:¥work¥lasvinfo.csv
```

2. 手順1.で出力したファイルを編集します。

   対象ログアナライザサーバのIPアドレス/ポート番号を新しい情報に書き換えます。

3. RegisterLAInfo.exe(ログアナライザサーバ情報の登録コマンド)の情報登録オプションを使用して、ログアナライザサーバ情報を再登録します。

   【手順2.で編集したファイルパスを“C:¥WORK¥lasvinfo.csv”とした場合の実行例】

```
[Systemwalker Desktop Keeperインストールフォルダ]¥LogAnalyzer¥TRANS¥RegisterLAInfo.exe -r C:¥WORK¥lasvinfo.csv
```

4. 目的別集計用ポート番号を変更した場合は、さらに「services」ファイルの編集を行います。

   「services」ファイルは以下のフォルダ配下に格納されています。

   - Windows Server® 2008の場合:「C:¥WINDOWS¥system32¥drivers¥etc」
   - Windows Server® 2003の場合:「C:¥WINDOWS¥system32¥drivers¥etc」
   - Windows® 2000 Serverの場合:「C:¥WINNT¥system32¥drivers¥etc」

   「services」ファイルの以下の設定を変更します。

```
rn 通信ポート番号/TCP
```

変更したログアナライザサーバにログデータを移入している管理サーバ/統合管理サーバ上で、以下の設定を行います。
ポート番号だけ変更した場合は、本作業は必要ありません。

1. ログアナライザ設定を起動し、転送先共有フォルダパスを新しいパスに変更します。

   【変更前の共有フォルダパスを“¥¥192.168.1.1¥LASVDATA”、新しいIPアドレスを“192.168.2.1”とした場合の変更例】

変更前の共有フォルダパスを“¥¥192.168.2.1¥LASVDATA”に変更します。
詳細は、“Systemwalker Desktop Keeper 導入ガイド”の“ログアナライザサーバの環境を設定する”を参照してください。

レポート出力ツール上で以下の設定を行います。

1. レポート出力環境設定を起動し、[サーバ]タブのIPアドレス/ポート番号を新しいIPアドレス/ポート番号に変更します。

   詳細は、“Systemwalker Desktop Keeper 導入ガイド”の“レポート出力の環境を設定する”を参照してください。

第8章 設定できるポリシー

設定したポリシーが有効になった場合のシステムの動作と、採取されるログの利用方法を説明します。

8.1 禁止機能のポリシーの設定

禁止機能によって禁止できる操作について説明します。

禁止できる操作

どの操作を禁止するか、ポリシーを設定します。禁止できる操作は以下のとおりです。
ポリシーは、システム管理者または部門管理者が、管理コンソールで設定します。

注意

使用している環境によって、機能が制限される場合があります

ポリシーを設定した場合でも、使用している環境によって、機能が制限される場合があります。
詳細は、“1.2.9 ファイル持出し禁止”～“1.2.16 Webダウンロード禁止”を参照してください。

- ファイル持出し禁止
- ファイル読み込み禁止
- 印刷禁止
- ログオン禁止
- アプリケーション起動禁止
- PrintScreenキー禁止
- メール添付禁止
- URLアクセス禁止
- FTPサーバ接続禁止
- Webダウンロード禁止

8.1.1 ファイル持出し禁止

ポリシーとしてファイル持出し禁止を設定すると、クライアント(CT)がインストールされているPCのドライブ、リムーバブル、またはDVD/CDへのファイルやフォルダの持ち出しを禁止できます。

注意

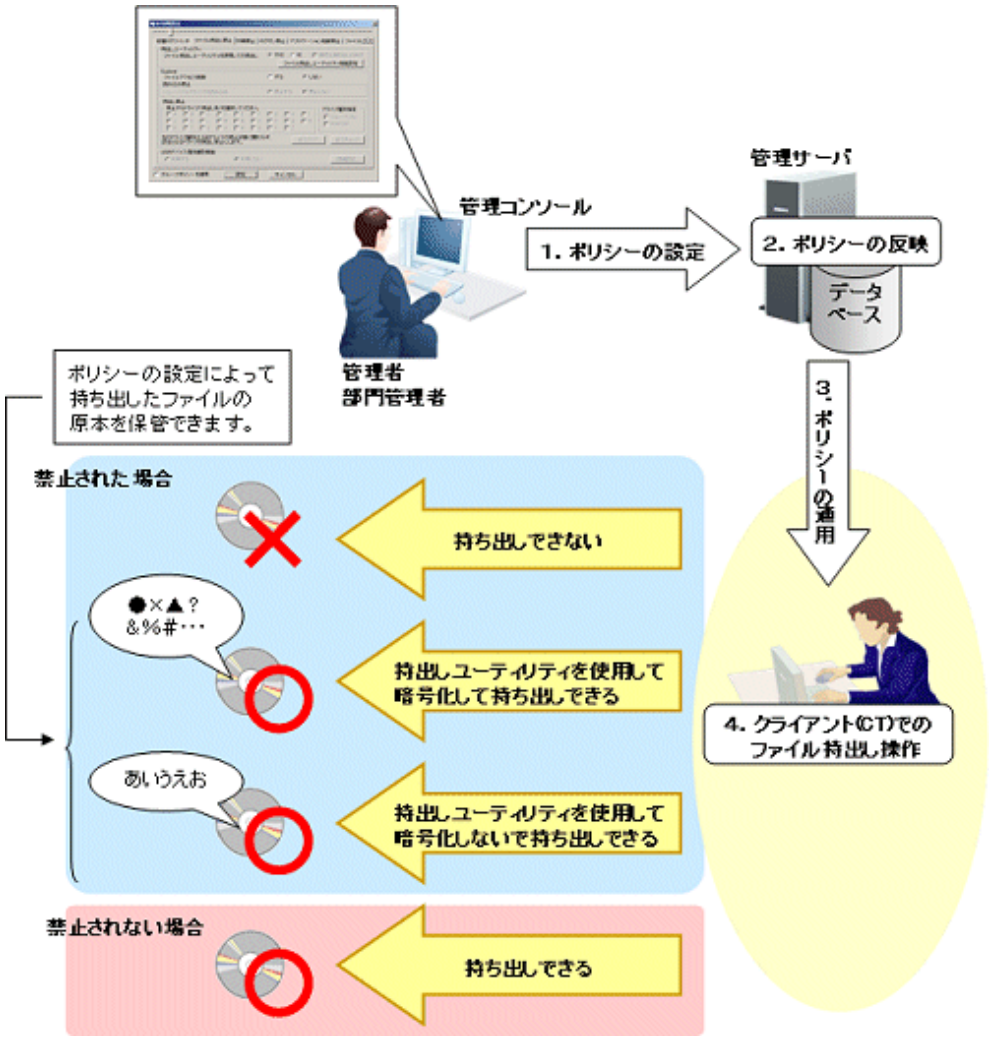
使用している環境によって、機能が制限される場合があります

ポリシーを設定した場合でも、使用している環境によって、機能が制限される場合があります。
詳細は、“1.2.9 ファイル持出し禁止”を参照してください。

禁止されていても、持出しユーティリティを使用する場合は、ファイルやフォルダの持ち出しができます。暗号化して持ち出すか、平文のまま持ち出すかを選択できます。

持出しユーティリティについては、“1.2.5 持出しユーティリティ”、および“Systemwalker Desktop Keeper 運用ガイド クライアント編”を参照してください。

ポリシーの設定から禁止が有効になるまで



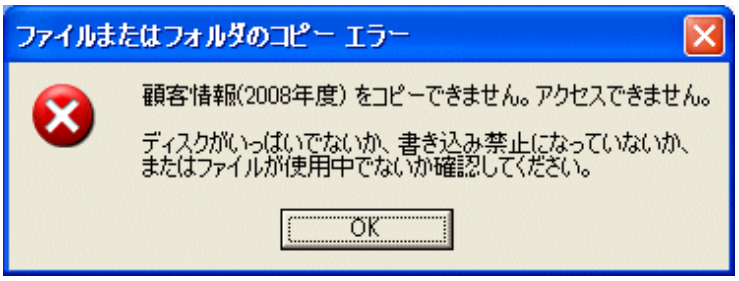
1. ポリシーの設定
   [端末初期設定]画面、[ユーザーポリシー設定]画面、またはCTポリシー設定画面で設定します。
   [ファイル持出し禁止]タブで、ファイルの持ち出しを禁止する条件を設定します。
2. ポリシーの反映
   設定したポリシーがデータベースに反映されます。
3. ポリシーの適用
   設定したポリシーがクライアント(CT)に適用されます。
4. ファイル持出し操作
   クライアント(CT)でファイルやフォルダを持ち出そうとした場合、以下のいずれかの状態になります。
   - 持ち出しできない
   - 持出しユーティリティを使用して暗号化して持ち出しできる
   - 持出しユーティリティを使用して暗号化しないで持ち出しできる
   - そのまま持ち出しできる

CD/DVDへのファイル持出しは、メディアによって動作が異なります。詳細は“1.2.9 ファイル持出し禁止”、および“1.2.5 持出しユーティリティ”を参照してください。

操作に関しては、“Systemwalker Desktop Keeper 運用ガイド クライアント編”を参照してください。

禁止された場合

禁止対象のドライブなどに、「持出しユーティリティ」を使用しないで、ファイルやフォルダを持ち出そうとした場合、クライアント(CT)では禁止画面が表示されます。以下に画面の例を表示します。



持出しユーティリティを使用して暗号化して持ち出したファイルを復号する場合、パスワード入力時に、[暗号ファイル設定]画面で表示された[パスワード試行回数]を超えたときは、以下の画面が表示され、暗号化ファイルが削除されます。

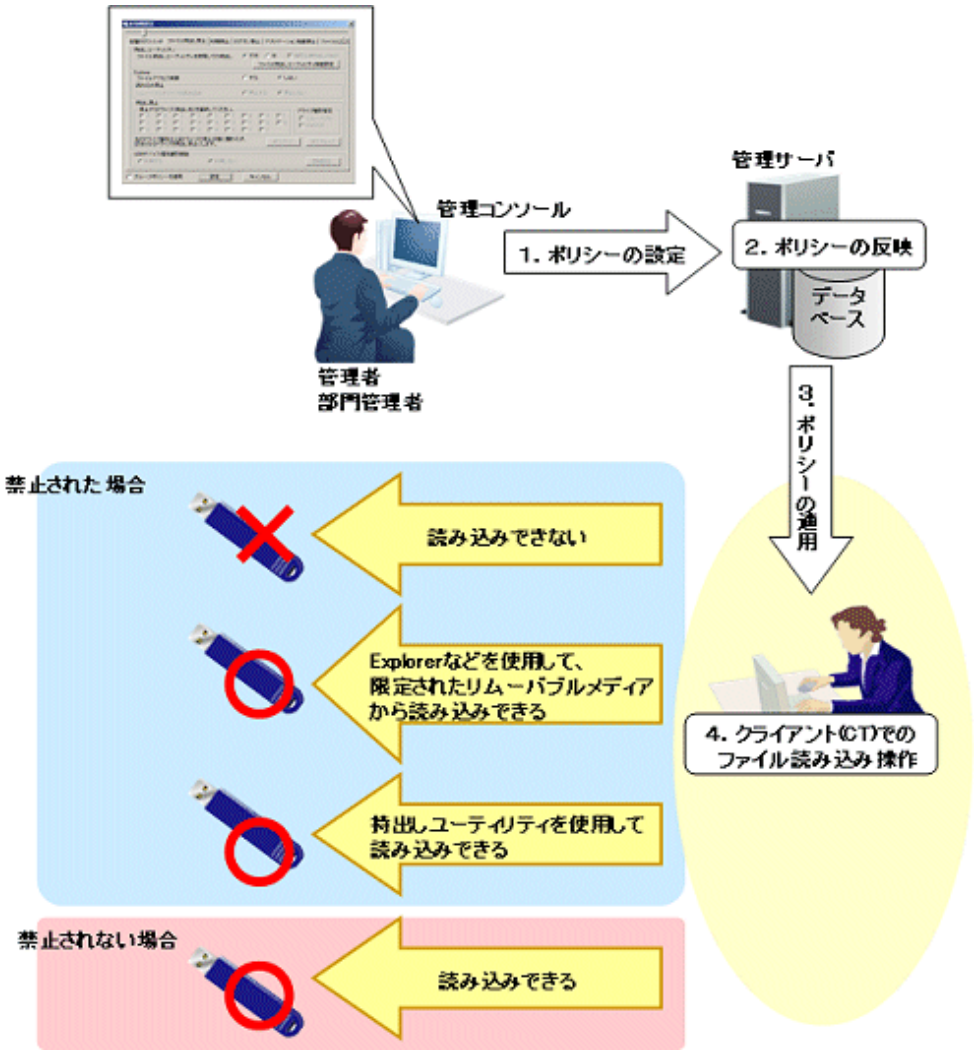
持出しユーティリティを使用して暗号化して持ち出したファイルを復号する場合、[暗号ファイル設定]画面での[パスワード試行回数]表示が4回以上のとき、パスワード入力を連続で3回失敗すると、以下の画面が表示され、復号処理が終了します。

持出しユーティリティを使用して暗号化して持ち出したファイルを復号する場合、[暗号ファイル設定]画面で表示された[復号可能期限]を超えているにもかかわらず復号操作を実施したときは、以下の画面が表示され、暗号化ファイルが削除されます。

8.1.2 ファイル読み込み禁止

ポリシーとして、ファイル読み込み禁止を設定した場合、クライアント(CT)がインストールされているPCのリムーバブルドライブからのデータ読み込みを禁止できます。

ポリシーの設定から禁止が有効になるまで



1. ポリシーの設定
   [端末初期設定]画面、[ユーザーポリシー設定]画面、またはCTポリシー設定画面で設定します。
   [ファイル持出し禁止]タブの[ファイルアクセス制御]を“する”に設定します。
   [ファイル持出し禁止]タブの[リムーバブルドライブの読み込み]を“禁止する”に設定します。
2. ポリシーの反映
   設定したポリシーがデータベースに反映されます。
3. ポリシーの適用
   設定したポリシーがクライアント(CT)に適用されます。
4. ファイル読み込み禁止動作
   クライアント(CT)でファイルやフォルダを読み込もうとした場合、以下のいずれかの状態になります。
   - 読み込みできない(注1)
   - Explorerなどを使用して、限定されたリムーバブルメディアから読み込みできる(注2)
   - 持出しユーティリティを使用して、読み込みできる(注3)

－ そのまま読み込みできる

注1) 持出しユーティリティを使用できないポリシー設定にしてください。
注2) [ファイル持出し禁止]タブの[USBデバイス個体識別機能]で、使用できるリムーバブルメディアを限定してください。指定されたUSBデバイス以外は、読み込みを行えません。許可するUSBデバイスを登録、設定する方法は、“7.5 指定したUSBデバイスだけにファイルを持ち出す”を参照してください。
注3) 持出しユーティリティを使用できるポリシー設定の場合です。持出しユーティリティの[持出し先の参照]画面で、持出したファイル名やフォルダ構成を確認できることを意味します(ファイルを開くことはできません)。

8.1.3 印刷禁止

ポリシーとして印刷禁止を設定すると、クライアント(CT)がインストールされているPCでは、指定したアプリケーション以外の印刷を禁止できます。

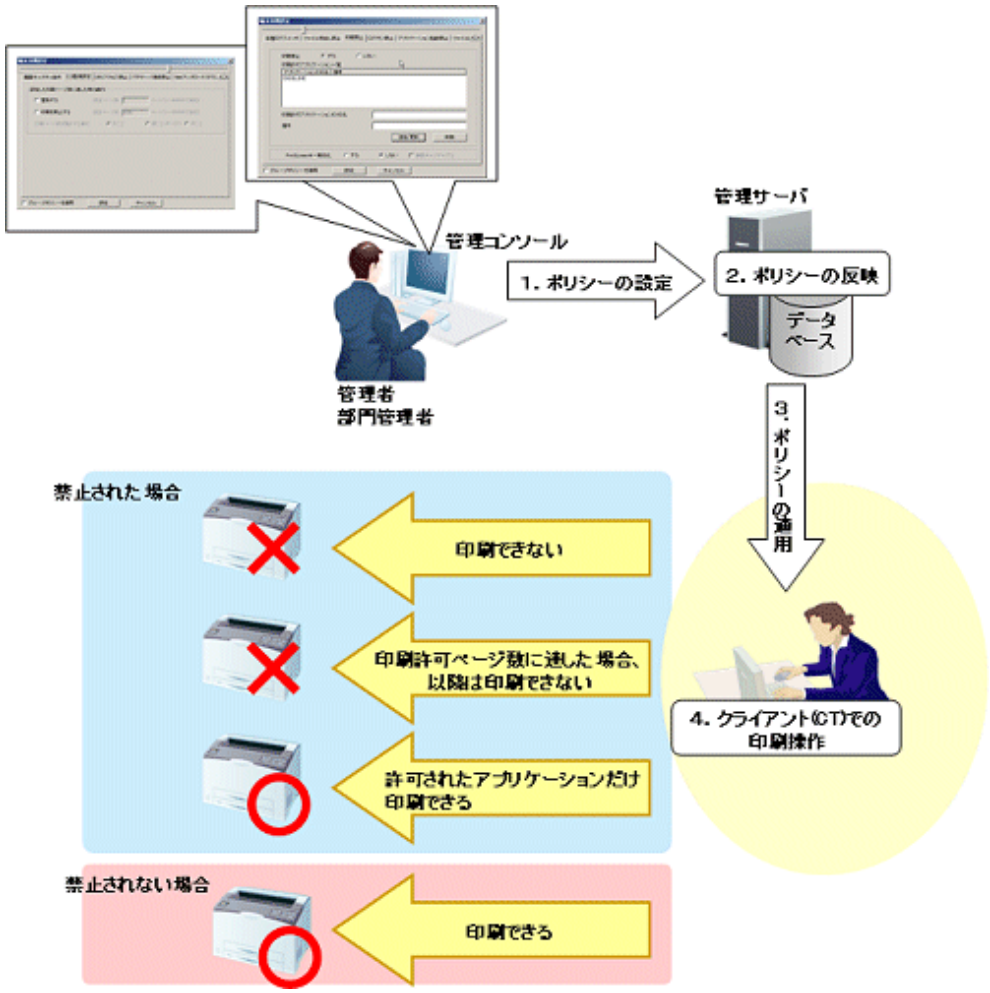
印刷ページ数を監視するポリシーで、印刷を許可するページ数を設定した場合は、設定ページ数に達した時点で印刷を禁止できます。

注意

使用している環境によって、機能が制限される場合があります

ポリシーを設定した場合でも、使用している環境によって、機能が制限される場合があります。
詳細は、“1.2.10 印刷禁止”を参照してください。

ポリシーの設定から禁止が有効になるまで



1. ポリシーの設定
   [端末初期設定]画面、[ユーザーポリシー設定]画面、またはCTポリシー設定画面で設定します。
   [印刷禁止]タブで、印刷を禁止する条件を設定します。
   [エコ監視設定]タブで、印刷を禁止する条件を設定します。
2. ポリシーの反映
   設定したポリシーがデータベースに反映されます。
3. ポリシーの適用
   設定したポリシーがクライアント(CT)に適用されます。
4. 印刷操作
   クライアント(CT)でアプリケーションから印刷しようとした場合、以下のいずれかの状態になります。
   - 印刷できない
   - 印刷許可ページ数に達した時点で、印刷できない
   - 許可されたアプリケーションからだけ印刷できる
   - 何でも印刷できる

禁止された場合

印刷を許可されていないアプリケーションから印刷を行った場合、クライアント(CT)では禁止画面が表示されます。以下に画面の例を表示します。

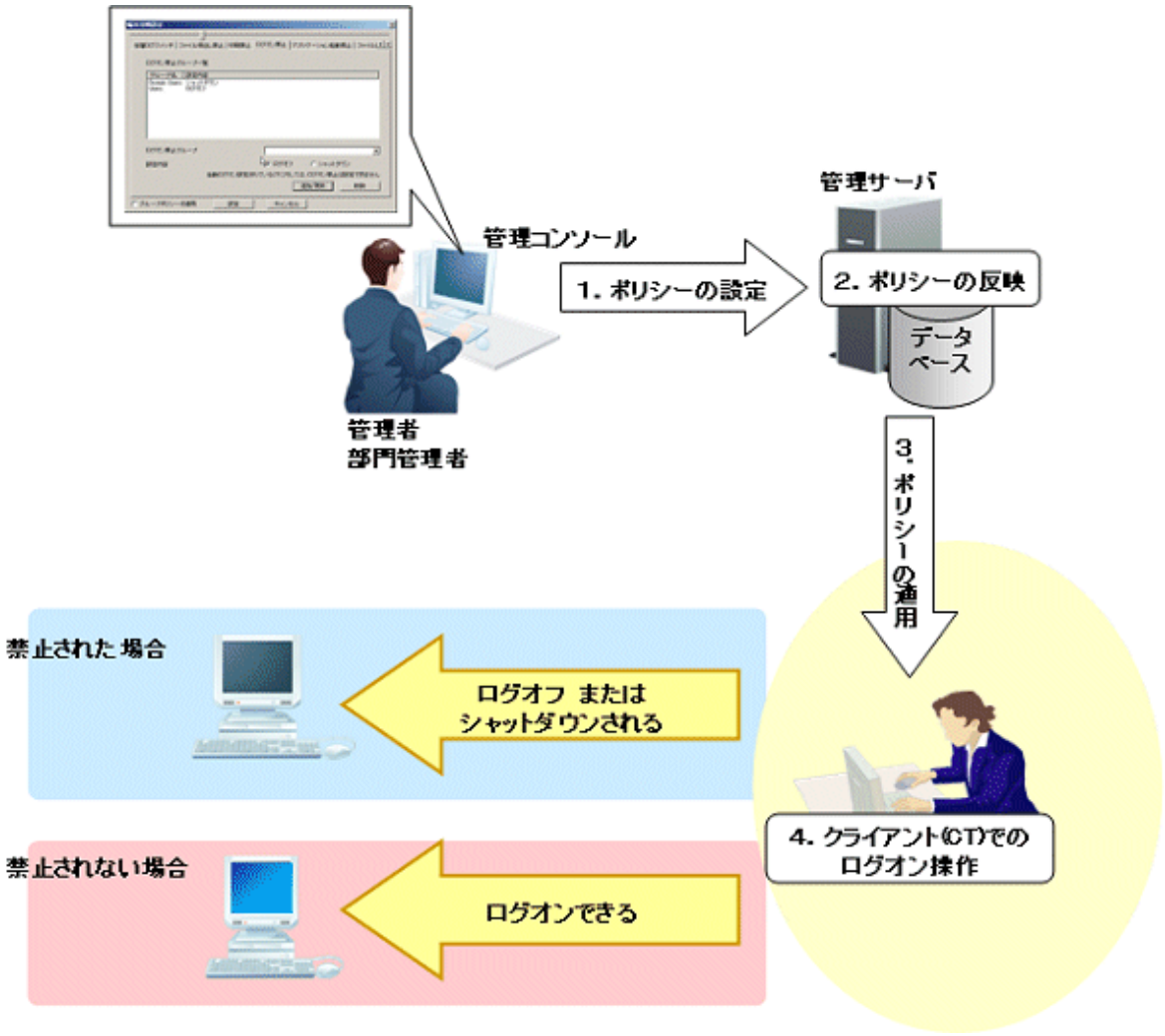
8.1.4 ログオン禁止

ポリシーとしてログオン禁止を設定すると、クライアント(CT)がインストールされているPCでは、指定したグループに所属しているユーザー名でのログオンを禁止できます。
禁止設定が可能なグループは以下のとおりです。

- Administrators
- Backup Operators
- Debugger Users
- Power Users
- Guests
- Replicator
- Users
- Domain Admins
- Domain Guests
- Domain Users
- Enterprise Admins
- Group Policy Creator Owners

ドメインログオンした場合、同じユーザーIDがローカルコンピュータにもあるときは、ローカルユーザーの所属グループについてもログオンが禁止されます。

ポリシーの設定から禁止が有効になるまで



1. ポリシーの設定
   [端末初期設定]画面、またはCTポリシー設定画面の[ログオン禁止]タブで、ログオンを禁止するグループを設定します。
   また、[端末動作設定]画面の[ログオン禁止作動開始時間]で、ログオンが検出されたあとの禁止動作(ログオフまたはシャットダウン)までの間隔を設定します。
2. ポリシーの反映
   設定したポリシーがデータベースに反映されます。
3. ポリシーの適用
   設定したポリシーがクライアント(CT)に適用されます。
4. ログオン操作
   クライアント(CT)でログオンする場合、以下のいずれかの状態になります。
   - 禁止対象となるグループに所属しているユーザー名でログオンした場合は、クライアント(CT)はログオフまたはシャットダウンされる
   - 禁止対象ではないグループに所属しているユーザー名でログオンした場合は、クライアント(CT)にログオンできる

禁止された場合

禁止対象となっているグループに所属しているユーザー名でクライアント(CT)にログオンした場合、クライアント(CT)では、ポリシーの設定によって以下のどちらかの禁止画面が表示されます。

ただし、[端末動作設定]画面の[ログオン禁止作動開始時間]で、[即時に禁止動作]が選択されている場合は、禁止画面は表示されません。

- クライアント(CT)がログオフされる場合

- クライアント(CT)がシャットダウンされる場合

8.1.5 アプリケーション起動禁止

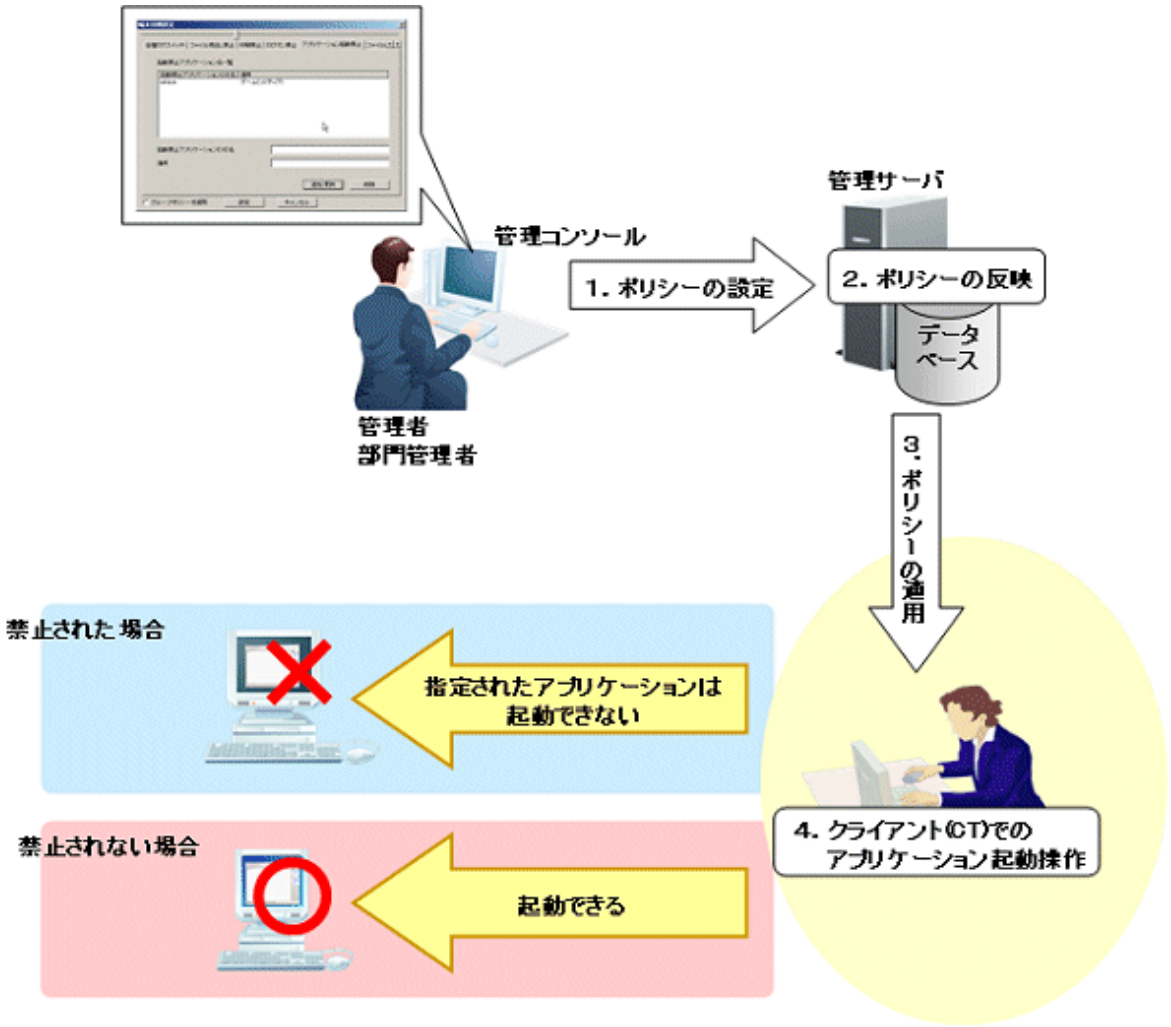
ポリシーとしてアプリケーション起動禁止を設定すると、クライアント(CT)がインストールされているPCでは、指定したアプリケーションの起動を禁止できます。

注意

使用している環境によって、機能が制限される場合があります

ポリシーを設定した場合でも、使用している環境によって、機能が制限される場合があります。
詳細は、“1.2.12 アプリケーション起動禁止”を参照してください。

ポリシーの設定から禁止が有効になるまで



1. ポリシーの設定
   [端末初期設定]画面、[ユーザーポリシー設定]画面、またはCTポリシー設定画面で設定します。
   [アプリケーション起動禁止]タブで、起動を禁止するアプリケーションを設定します。
2. ポリシーの反映
   設定したポリシーがデータベースに反映されます。
3. ポリシーの適用
   設定したポリシーがクライアント(CT)に適用されます。
4. アプリケーション起動操作
   クライアント(CT)でアプリケーションを起動する場合、以下のいずれかの状態になります。
   - 指定されたアプリケーションは起動できない
   - どのようなアプリケーションでも起動できる

禁止された場合

アプリケーションの起動が禁止されている場合、クライアント(CT)では禁止画面が表示されます。以下に画面の例を表示します。

8.1.6 メール添付禁止

ポリシーとしてメール添付禁止を設定すると、クライアント(CT)がインストールされているPCでは、禁止対象となるファイルをメールに添付して、送信または保存することを禁止できます。
禁止対象のファイルをポリシーで指定します。

ポート監視方式の場合、添付ファイルの中に1つでも、添付禁止対象のファイルがある場合、メール(メール本文と、すべての添付ファイル)は送信できません。

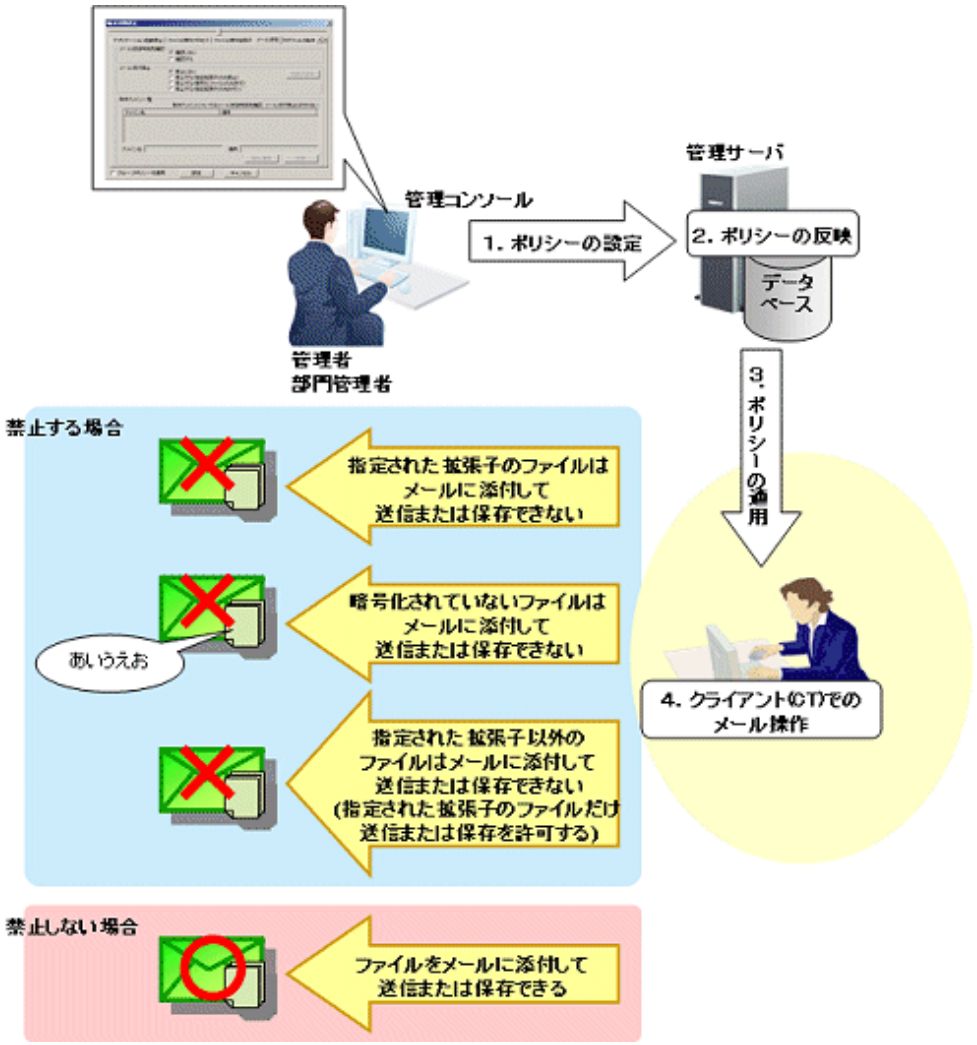
V12.0L20～V13.0.0互換方式の場合は、メール送信時宛先確認の設定に関係なく、禁止対象のファイルと禁止対象外のファイルが混在しているときは、禁止対象外のファイルだけ添付して送信できます。禁止対象のファイルだけを添付して送信した場合は、メールの本文は送信されます。

注意

使用している環境によって、機能が制限される場合があります

ポリシーを設定した場合でも、使用している環境によって、機能が制限される場合があります。
詳細は、“1.2.13 メール添付禁止”を参照してください。

ポリシーの設定から禁止が有効になるまで



1. ポリシーの設定
   [端末初期設定]画面、[ユーザーポリシー設定]画面、またはCTポリシー設定画面で設定します。
   [メール送信]タブで、メールへの添付を禁止する条件を設定します。
2. ポリシーの反映
   設定したポリシーがデータベースに反映されます。
3. ポリシーの適用
   設定したポリシーがクライアント(CT)に適用されます。
4. メール操作
   クライアント(CT)でメールを送信する場合、以下のいずれかの状態になります。
   - 指定された拡張子のファイルはメールに添付して送信または保存できない
   - 暗号化されていないファイルはメールに添付して送信または保存できない
   - 指定された拡張子以外のファイルはメールに添付して送信または保存できない
     (指定された拡張子のファイルだけ送信または保存できる)
   - ファイルをメールに添付して送信または保存できる

禁止された場合

メール添付禁止されている場合、クライアント(CT)では禁止画面が表示されます。以下に画面の例を表示します。

V12.0L20～V13.0.0互換方式の場合

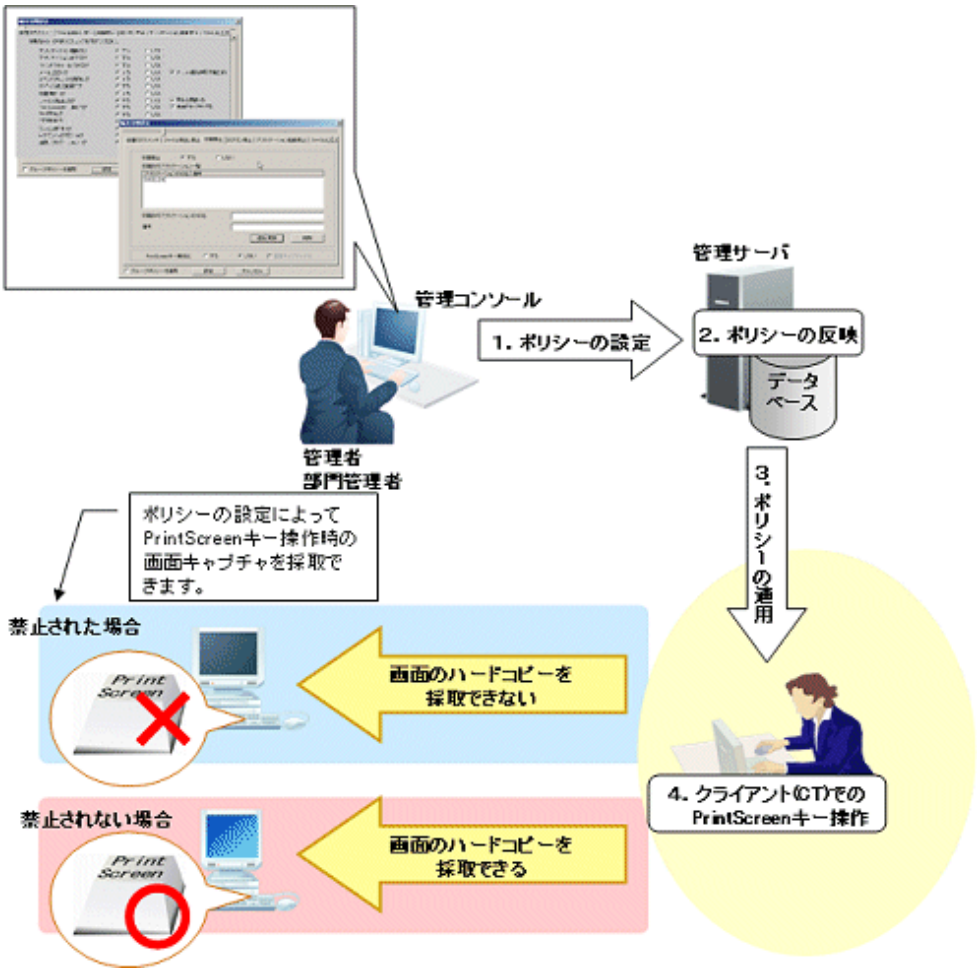
ポート監視方式の場合

8.1.7 PrintScreenキー禁止

ポリシーとしてPrintScreenキー禁止を設定すると、クライアント(CT)がインストールされているPCでは、キーボードのPrintScreenキーを使用して、画面のハードコピーを採取することを禁止できます。

また、禁止時に画面キャプチャを採取することもできます。

ポリシーの設定から禁止が有効になるまで



1. ポリシーの設定
   [端末初期設定]画面、[ユーザーポリシー設定]画面、またはCTポリシー設定画面で設定します。
   [印刷禁止]タブで、[PrintScreenキー無効化]を[する]に設定します。
   PrintScreenキー操作時の画面を採取する場合は、[画面キャプチャする]にチェックを付けます。
2. ポリシーの反映
   設定したポリシーがデータベースに反映されます。
3. ポリシーの適用
   設定したポリシーがクライアント(CT)に適用されます。
4. PrintScreenキー操作
   クライアント(CT)でPrintScreenキーを操作する場合、以下のいずれかの状態になります。

   ー PrintScreenキーは押せるが、画面のハードコピーを採取できない
   手順1.で[画面キャプチャする]にチェックを付けた場合は、PrintScreenキー操作時の画面が採取される

   ー PrintScreenキーを押して、画面のハードコピーを採取できる

禁止された場合

PrintScreenキーの使用が禁止されている場合、クライアント(CT)では禁止画面が表示されます。以下に画面の例を表示します。禁止時に画面キャプチャの採取が設定されている場合は、PrintScreenキー操作時の画面キャプチャが採取されます。

8.1.8 URLアクセス禁止

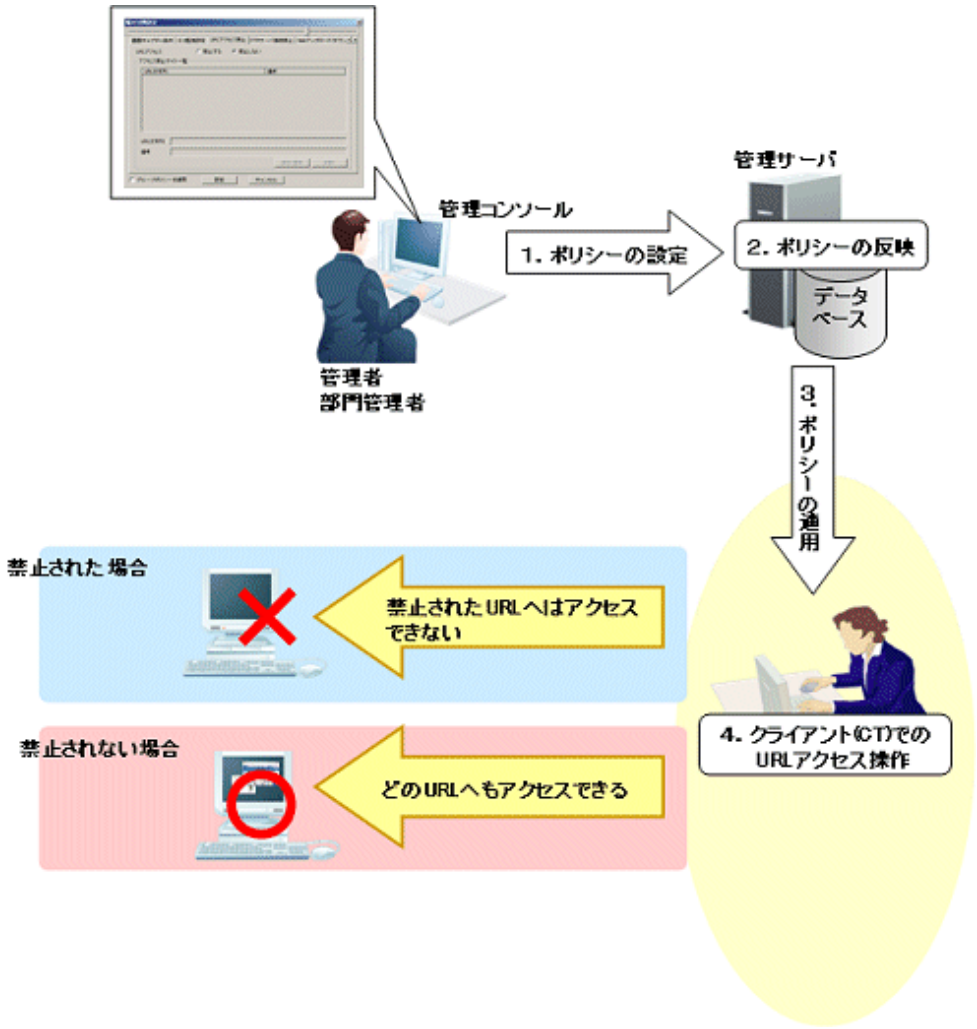
ポリシーとしてURLアクセス禁止を設定すると、クライアント(CT)がインストールされているPCでは、管理者が許可していないURLへのアクセスを禁止できます。

注意

使用している環境によって、機能が制限される場合があります

ポリシーを設定した場合でも、使用している環境によって、機能が制限される場合があります。
詳細は、“1.2.14 URLアクセス禁止”を参照してください。

ポリシーの設定から禁止が有効になるまで



1. ポリシーの設定
   [端末初期設定]画面、[ユーザーポリシー設定]画面、またはCTポリシー設定画面で設定します。
   [URLアクセス禁止]タブで、[URLアクセス]を[禁止する]に設定します。
2. ポリシーの反映
   設定したポリシーがデータベースに反映されます。
3. ポリシーの適用
   設定したポリシーがクライアント(CT)に適用されます。
4. URLへのアクセス操作
   クライアント(CT)でURLへアクセスする場合、以下のいずれかの状態になります。
   - 禁止されたURLへはアクセスできない
   - どのURLへもアクセスできる
     この場合のログは、ウィンドウタイトル取得ログとして採取されます。

禁止された場合

Webページに1つだけタブが表示されている場合、禁止されたURLへアクセスしたときは、Internet Explorer®が強制終了されます。
Webページに複数のタブが表示されている場合、禁止されたURLへアクセスしたタブだけ、強制的に閉じられます。
その後、以下のメッセージが表示されます。

8.1.9 FTPサーバ接続禁止

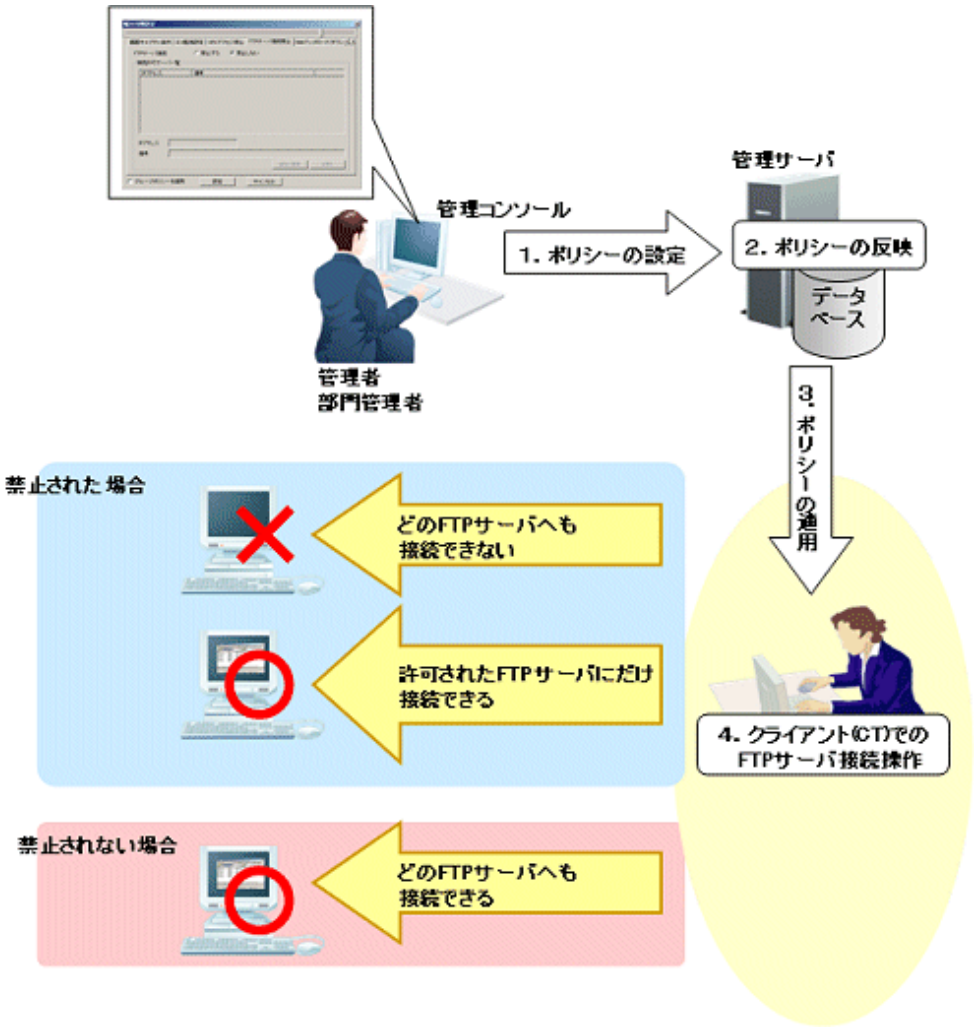
ポリシーとしてFTPサーバ接続禁止を設定すると、クライアント(CT)がインストールされているPCでは、管理者が許可したFTPサーバ以外へのアクセスを禁止できます。

注意

使用している環境によって、機能が制限される場合があります

ポリシーを設定した場合でも、使用している環境によって、機能が制限される場合があります。
詳細は、“1.2.15 FTPサーバ接続禁止”を参照してください。

ポリシーの設定から禁止が有効になるまで



1. ポリシーの設定
   [端末初期設定]画面、[ユーザーポリシー設定]画面、またはCTポリシー設定画面で設定します。
   [FTPサーバ接続禁止]タブで、[FTPサーバ接続]を[禁止する]に設定します。
2. ポリシーの反映
   設定したポリシーがデータベースに反映されます。
3. ポリシーの適用
   設定したポリシーがクライアント(CT)に適用されます。
4. FTPサーバへの接続操作
   クライアント(CT)からFTPサーバへ接続する場合、以下のいずれかの状態になります。
   - どのFTPサーバへも接続できない
   - 許可されたFTPサーバにだけ接続できる
   - どのFTPサーバへも接続できる

禁止された場合

以下のメッセージが表示されます。

8.1.10 Webダウンロード禁止

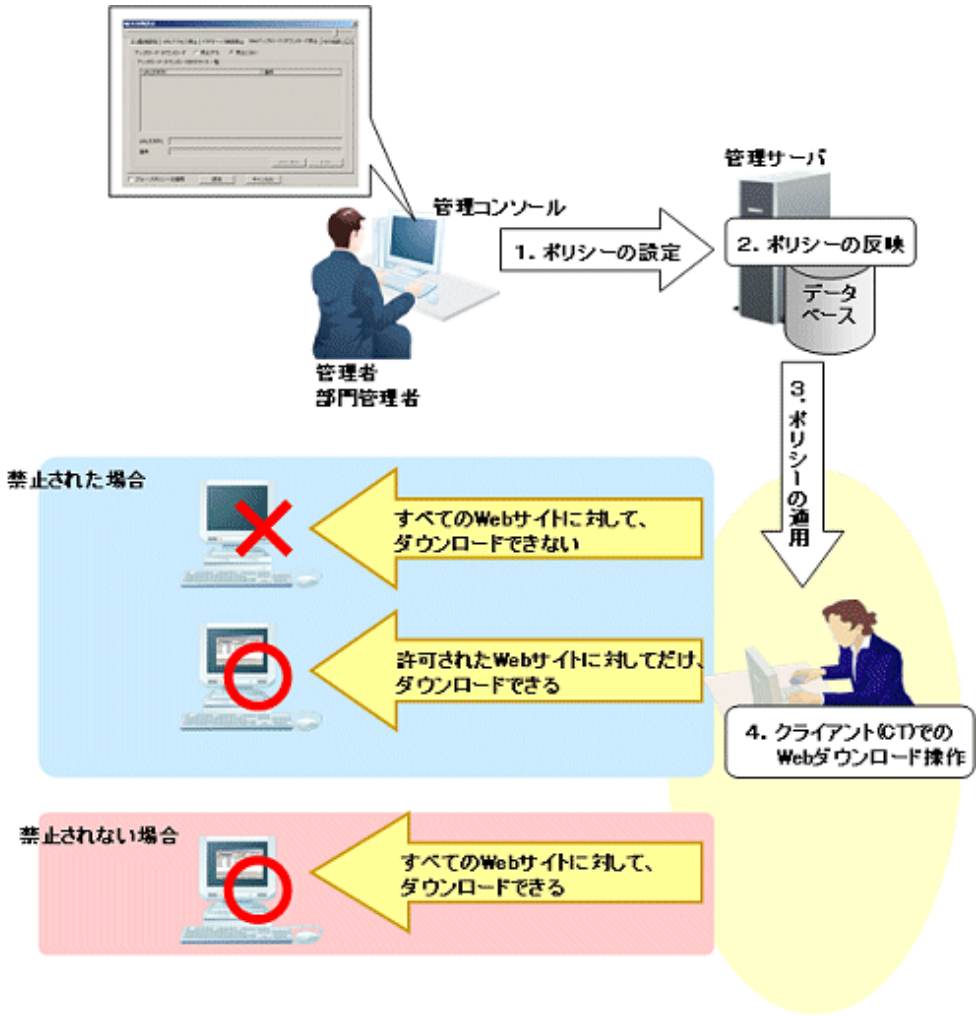
ポリシーとしてWebダウンロード禁止を設定すると、クライアント(CT)がインストールされているPCでは、管理者が許可したWebサイト以外からのダウンロードを禁止できます。

注意

使用している環境によって、機能が制限される場合があります

ポリシーを設定した場合でも、使用している環境によって、機能が制限される場合があります。
詳細は、“1.2.16 Webダウンロード禁止”を参照してください。

ポリシーの設定から禁止が有効になるまで



1. ポリシーの設定
   [端末初期設定]画面、[ユーザーポリシー設定]画面、またはCTポリシー設定画面で設定します。
   [Webダウンロード禁止]タブで、[ダウンロード]を[禁止する]に設定します。
2. ポリシーの反映
   設定したポリシーがデータベースに反映されます。
3. ポリシーの適用
   設定したポリシーがクライアント(CT)に適用されます。
4. URLへのアクセス操作
   クライアント(CT)でWebサイトへアクセスする場合、以下のいずれかの状態になります。
   - すべてのWebサイトに対して、ダウンロードできない
   - 許可されたWebサイトに対してだけ、ダウンロードできる
   - すべてのWebサイトに対して、ダウンロードできる

禁止された場合

以下のメッセージが表示されます(ダウンロード禁止の例)。

8.2 記録機能のポリシーの設定

記録機能によって採取できるログについて説明します。

採取できる操作ログ

どの操作に対してログを採取するか、ポリシーを設定します。採取できる操作ログは以下のとおりです。
ポリシーは、システム管理者または部門管理者が、管理コンソールで設定します。

注意

使用している環境によって、機能が制限される場合があります

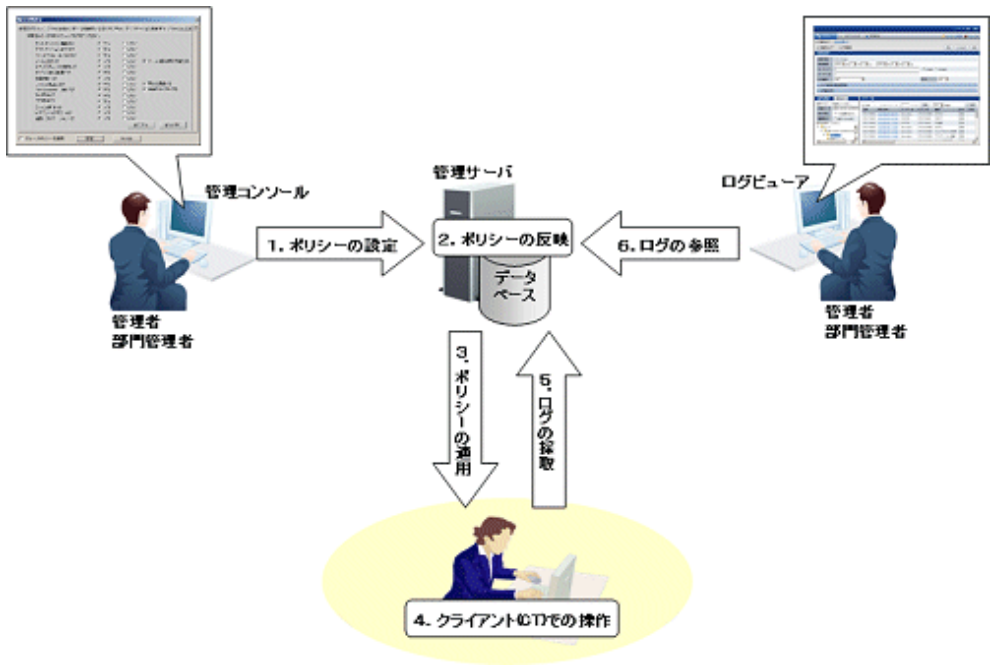
ポリシーを設定した場合でも、使用している環境によって、機能が制限される場合があります。
詳細は、“1.2.17 ログ全体”～“1.2.31 クライアント(CT)の調査用ログの採取について”を参照してください。

- アプリケーション起動ログ
- アプリケーション終了ログ
- アプリケーション起動禁止ログ
- ウィンドウタイトル取得ログ
- メール送信ログ
- メール送信中止ログ
- メール添付禁止ログ
- コマンドプロンプト操作ログ
- デバイス構成変更ログ
- 印刷操作ログ
- 印刷禁止ログ
- ログオン禁止ログ
- ファイル持出しログ
- PrintScreenキー操作ログ
- PrintScreenキー禁止ログ
- Web操作ログ
- Web操作禁止ログ
- FTP操作ログ

- FTP操作禁止ログ
- ファイル操作ログ
- ログオン/ログオフログ
- 連携アプリケーションログ
- 設定変更ログ

ポリシーの設定からログの参照まで

CT操作ログの場合



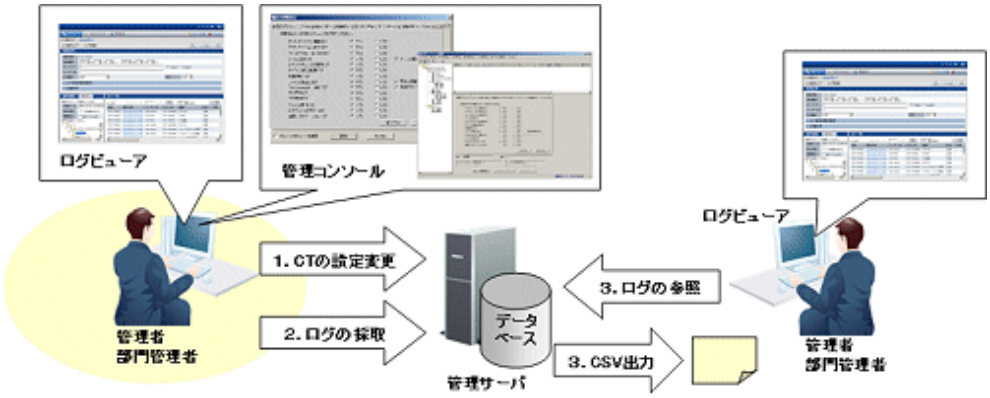
1. ポリシーの設定
   [端末初期設定]画面、[ユーザーポリシー設定]画面、または管理コンソール起動直後の画面(CTポリシー設定画面)で、各種ログを採取するポリシーを設定します。
2. ポリシーの反映
   設定したポリシーがデータベースに反映されます。
3. ポリシーの適用
   設定したポリシーがクライアント(CT)に適用されます。
4. クライアント(CT)での操作
   クライアント(CT)利用者が、各操作を行います。
5. ログの採取
   クライアント(CT)で採取されたログは、管理サーバに送信されます。

   クライアント(CT)が接続する管理サーバと通信可能な場合
   クライアント(CT)でログが採取されたあと、ポリシー設定画面の[その他設定]タブで設定されているポリシーに従って、管理サーバに送信されます。

   クライアント(CT)が接続する管理サーバと通信可能でない場合
   クライアント(CT)でログが採取されたあと、一時的にクライアント(CT)にログが格納されます。クライアント(CT)が接続する管理サーバと通信が可能になった時点で、クライアント(CT)に格納されていたログが、ポリシー設定画面の[その他設定]タブで設定されているポリシーに従って、管理サーバに送信されます。

6. ログの参照
   ログビューアで、採取されたログを参照します。

設定変更ログの場合



1. クライアント(CT)の設定変更
   管理コンソールまたはログビューアで、クライアント(CT)の設定情報を変更します。
2. ログの採取
   設定変更操作が、ログとして管理サーバに保存されます。
3. ログの参照
   ・管理コンソールで実施した設定変更操作については、ログビューアで参照します。
   ・ログビューアで実施した設定変更操作については、CSVファイルに出力して参照します([設定変更ログ一覧]画面に表示することはできません)。設定変更ログのCSV形式出力コマンドの詳細は、“Systemwalker Desktop Keeper リファレンスマニュアル”の“DTKSTCV.EXE (設定変更ログの出力)”を参照してください。

ログの参照

採取されたログは、ログビューアで参照します。

【CT操作ログの表示例】

ログビューアで参照できるログの項目については、“5.2.1 [CT操作ログ]画面で参照する”または“5.2.2 [設定変更ログ]画面で参照する”を参照してください。

8.2.1 アプリケーション起動ログ

クライアント(CT)でウィンドウを持つアプリケーションを起動したときのログです。ウィンドウを持たないアプリケーションの場合は、アプリケーション起動ログを採取できません。
画面を表示しない(不可視ウィンドウを保有している)アプリケーションの起動ログは採取されます。

活用方法

アプリケーション起動ログを採取した場合、だれがどんなアプリケーションを起動したのかが分かります。業務に不必要なアプリケーションを起動したり、情報漏えいの恐れがあるアプリケーションを起動したりする人を洗い出すことができます。システム運用が規則どおりに実施されているかを判断することができます。

採取するために設定するポリシー

[端末初期設定]画面、[ユーザーポリシー設定]画面、または管理コンソール起動直後の画面(CTポリシー設定画面)で設定します。
[各種ログスイッチ]タブで、[アプリケーション起動ログ]に[する]を設定します。

表示内容

参照できるログの内容は以下のとおりです。

[名称]:クライアント(CT)の名称

[発生日時]:クライアント(CT)におけるログ採取日時

[ユーザー名]:クライアント(CT)のログオンユーザー名

[ドメイン名]:ドメインにログオン時はクライアント(CT)のドメイン名、ローカルコンピュータにログオン時はクライアント(CT)のコンピュータ名

[種別]:[アプリケーション起動] (固定値)

[区分]:正規

[付帯]:(表示されません)

[内容]:以下の内容が表示されます。

- 起動したアプリケーション名(※)

  [内容]の表示例

[EXCEL]を起動しました。

  ※) ログビューアでのキーワード検索時、キーワードとして指定できます。

[備考]:(表示されません)

8.2.2 アプリケーション終了ログ

クライアント(CT)でウィンドウを持つアプリケーションを終了したときのログです。ウィンドウを持たないアプリケーションの場合は、アプリケーション終了ログを採取できません。

活用方法

アプリケーション終了ログを採取した場合、だれがどんなアプリケーションを終了したのかが分かります。

採取するために設定するポリシー

[端末初期設定]画面、[ユーザーポリシー設定]画面、または管理コンソール起動直後の画面(CTポリシー設定画面)で設定します。
[各種ログスイッチ]タブで、[アプリケーション終了ログ]に[する]を設定します。

表示内容

参照できるログの内容は以下のとおりです。

[名称]:クライアント(CT)の名称

[発生日時]:クライアント(CT)におけるログ採取日時

[ユーザー名]:クライアント(CT)のログオンユーザー名

[ドメイン名]:ドメインにログオン時はクライアント(CT)のドメイン名、ローカルコンピュータにログオン時はクライアント(CT)のコンピュータ名

[種別]:[アプリケーション終了] (固定値)

[区分]:正規

[付帯]:(表示されません)

[内容]:以下の内容が表示されます。

- 終了したアプリケーション名(※)

  [内容]の表示例

[EXCEL]を終了しました。

  ※) ログビューアでのキーワード検索時、キーワードとして指定できます。

[備考]:(表示されません)

8.2.3 アプリケーション起動禁止ログ

クライアント(CT)で起動を禁止されているウィンドウを持つアプリケーションを起動しようとしたときのログです。ウィンドウを持たないアプリケーションの場合、アプリケーション起動禁止ログは採取できません。
画面を表示しない(不可視ウィンドウを保有している)アプリケーションは、アプリケーション起動禁止ログが採取されます。

活用方法

アプリケーション起動禁止ログを採取した場合、使用が禁止されている、業務に不必要なアプリケーションを起動しようとしたり、情報漏えいの恐れがあるアプリケーションを起動しようとしたりする人がいないか確認できます。システム運用が規則どおりに実施されているかを判断することができます。

採取するために設定するポリシー

[端末初期設定]画面、[ユーザーポリシー設定]画面、または管理コンソール起動直後の画面(CTポリシー設定画面)で設定します。
[アプリケーション起動禁止]タブで、起動を禁止するアプリケーション名を設定します。

表示内容

参照できるログの内容は以下のとおりです。

[名称]:クライアント(CT)の名称

[発生日時]:クライアント(CT)におけるログ採取日時

[ユーザー名]:クライアント(CT)のログオンユーザー名

[ドメイン名]:ドメインにログオン時はクライアント(CT)のドメイン名、ローカルコンピュータにログオン時はクライアント(CT)のコンピュータ名

[種別]:[アプリケーション起動禁止] (固定値)

[区分]:違反

[付帯]:(表示されません)

[内容]:以下の内容が表示されます。

- 禁止したアプリケーション名(※)
- 禁止処理([強制終了])
- 禁止結果([成功]または[失敗])

[内容]の表示例

```
[sol]の起動を[強制終了]しました。結果：[成功]
```

※) ログビューアでのキーワード検索時、キーワードとして指定できます。

[備考]:(表示されません)

8.2.4 ウィンドウタイトル取得ログ

クライアント(CT)でウィンドウを持つアプリケーションを起動した場合、ウィンドウが表示されたときのログです。ウィンドウを持たないアプリケーションを起動した場合は、ウィンドウタイトル取得ログは採取できません。

「Microsoft® Internet Explorer® 6.0 Service Pack1 以降」、「Windows® Internet Explorer® 7」、「Windows® Internet Explorer® 8」または「エクスプローラ」を使用している場合、以下のどれかの条件に当てはまるとき、ウィンドウタイトル取得ログとして「アドレスバーに表示されるURL情報」も採取されます。

- URL情報中に「http://」、「https://」または「ftp://」が含まれる。
- URL情報の先頭2、3バイト目に「:¥」が含まれない。
- URL情報の先頭が「¥¥」ではない。

ただし、下記のアプリケーションを交互に切り替えた場合に前回と同じ「アプリケーションのウィンドウタイトル名」および「アドレスバーに表示されるURL情報」だった場合はウィンドウタイトル取得ログは採取されません。

- Internet Explorer®とエクスプローラ
- Internet Explorer®とInternet Explorer®
- エクスプローラとエクスプローラ

注意

使用している環境によって、機能が制限される場合があります

ポリシーを設定した場合でも、使用している環境によって、機能が制限される場合があります。
詳細は、“1.2.20 ウィンドウタイトル取得ログ”を参照してください。

採取するために設定するポリシー

[端末初期設定]画面、[ユーザーポリシー設定]画面、または管理コンソール起動直後の画面(CTポリシー設定画面)で設定します。

- [各種ログスイッチ]タブで、[ウィンドウタイトル取得ログ]に[する]を設定します。

・ [ログフィルタ条件]タブで、ウィンドウタイトル取得ログのフィルタ条件を設定します。

[ウィンドウタイトル取得ログ]に[する]が設定されている場合に、設定できます。

・ [画面キャプチャ条件]タブで、画面キャプチャを採取する条件を設定します。

[ウィンドウタイトル取得ログ]に[する]が設定されている場合に、設定できます。

設定値の詳細は、“2.4.1.9 [ログフィルタ条件]タブの設定”および“2.4.1.10 [画面キャプチャ条件]タブの設定”を参照してください。

ログフィルタ条件

ログフィルタ条件として設定できる項目は、以下のとおりです。

ー 重複ログフィルタ設定
同じプロセス名で同じウィンドウタイトルのログの場合、初回のログだけを取得します。

ー キーワードフィルタ
プロセス名とキーワードを設定し、そのプロセス名でキーワードを含むウィンドウタイトル取得ログだけを採取または除外します。

注意

重複ログフィルタ設定が有効にならない場合があります

同じプロセスIDで交互にウィンドウを切り替えた場合、重複ログフィルタ設定は有効になりません。
【例】
Aというウィンドウタイトルのword文書とBというウィンドウタイトルのword文書を開き、
A→B→Aとアクティブなウィンドウを切り替えた場合。

画面キャプチャ

画面キャプチャ条件では、画面キャプチャを採取するプロセス名と、ウィンドウタイトルに含まれるキーワードを設定します。

画面キャプチャは、ウィンドウタイトル取得ログで参照できます。

端末動作設定で[付帯データ蓄積場所]として[CT]が選択されている場合は、画面キャプチャデータはクライアント(CT)に保存されます。

参照できるログの内容は以下のとおりです。

ー 採取した画面

ー「ログの表示結果」

表示内容

参照できるログの内容は以下のとおりです。

[名称]:クライアント(CT)の名称

[発生日時]:クライアント(CT)におけるログ採取日時

[ユーザー名]:クライアント(CT)のログオンユーザー名

[ドメイン名]:ドメインにログオン時はクライアント(CT)のドメイン名、ローカルコンピュータにログオン時はクライアント(CT)のコンピュータ名

[種別]:[ウィンドウタイトル取得] (固定値)

[区分]:正規

[付帯]:付帯(画面キャプチャ)データがある場合は“1”または“2”

[内容]:以下の内容が表示されます。

- アプリケーションのウィンドウタイトル名(※)
- 起動したアプリケーション名(※)

[内容]の表示例

```
[Microsoft Excel]ウィンドウを検出しました。アプリ名：[EXCEL]
```

[備考]:ブラウザで表示したページのURLが表示されます。(※)

※) ログビューアでのキーワード検索時、キーワードとして指定できます。

8.2.5 メール送信ログ

クライアント(CT)でメールを送信したときのログです。
メール送信時に、あて先を確認する警告メッセージが表示された場合、あて先を確認して送信したときも採取されます。

注意

使用している環境によって、機能が制限される場合があります

ポリシーを設定した場合でも、使用している環境によって、機能が制限される場合があります。
詳細は、“1.2.21 メール送信ログ”を参照してください。

採取するために設定するポリシー

[端末初期設定]画面、[ユーザーポリシー設定]画面、または管理コンソール起動直後の画面(CTポリシー設定画面)で設定します。

- [各種ログスイッチ]タブで、[メール送信ログ]に[する]を設定します。
- [各種ログスイッチ]タブで、[メール内容を参照可能とする]にチェックを付けた場合、送信したメールの内容や添付ファイルが保存され、ログビューアで参照することができます。
  [メール送信ログ]に[する]が設定されている場合に、設定できます。
- [メール送信]タブで、[メール送信時宛先確認]に[確認する]を設定します。

表示内容

参照できるログの内容は以下のとおりです。

[名称]:クライアント(CT)の名称

[発生日時]:クライアント(CT)におけるログ採取日時

[ユーザー名]:以下の情報が表示されます。

- ログオン時:クライアント(CT)のログオンユーザー名
- 未ログオン時:SYSTEM(固定)

[ドメイン名]:以下の情報が表示されます。

- ドメインにログオン時:クライアント(CT)のドメイン名
- ローカルコンピュータにログオン時:クライアント(CT)のコンピュータ名
- 未ログオン時:クライアント(CT)のコンピュータ名

[種別]:[メール送信] (固定値)

[区分]:正規

[付帯]:付帯(送信したメールの内容や添付ファイル)データがある場合は、“1”

[内容]:以下の内容が表示されます。

- メールのタイトル(※)
- 送信元アドレス(※)
- 送信先アドレス(To、Cc、Bccの情報) (※)
- 添付ファイル名(※)

[内容]の表示例

```
メール送信されました。[件名：本日の業務報告について From：Mail Address-A  To：Mail Address-B CC：Mail Address-C Mail BCC：Address-D 添付：添付ファイル名]
```

※) ログビューアでのキーワード検索時、キーワードとして指定できます。

[備考]:メール送信時に、あて先を確認する警告メッセージが表示された場合、以下の内容が表示されます。

- 許可されていないドメインのメールアドレス(※)

・ 警告メッセージ表示後の対応結果(※)

[備考]の表示例

警告アドレス：[xxxx] 結果：[確認後送信]

※) ログビューアでのキーワード検索時、キーワードとして指定できます。

8.2.6 メール送信中止ログ

メール送信時に、あて先を確認する警告メッセージが表示された場合、送信をキャンセルしたときに採取されるログです。

採取するために設定するポリシー

[端末初期設定]画面、[ユーザーポリシー設定]画面、または管理コンソール起動直後の画面(CTポリシー設定画面)で設定します。

・ [各種ログスイッチ]タブで、[メール送信ログ]に[する]を設定します。

・ [各種ログスイッチ]タブで、[メール内容を参照可能とする]にチェックを付けた場合、送信を中止したメールの内容や添付ファイルが保存され、ログビューアで参照することができます。

・ [メール送信]タブで、[メール送信時宛先確認]に[確認する]を設定します。

表示内容

参照できるログの内容は以下のとおりです。

[名称]:クライアント(CT)の名称

[発生日時]:クライアント(CT)におけるログ採取日時

[ユーザー名]:クライアント(CT)のログオンユーザー名

[ドメイン名]:以下の情報が表示されます。

・ ドメインにログオン時:クライアント(CT)のドメイン名

・ ローカルコンピュータにログオン時:クライアント(CT)のコンピュータ名

[種別]:[メール送信中止] (固定値)

[区分]:正規

[付帯]:付帯(送信したメールの内容や添付ファイル)データがある場合は、“1”

[内容]:許可されていないドメインのメールアドレス(※)

メール送信が中止されました。警告アドレス：[xxxx]

※) ログビューアでのキーワード検索時、キーワードとして指定できます。

[備考]:以下の内容が表示されます。

・ メールのタイトル(※)

・ 送信元アドレス(※)

・ 送信先アドレス(To、Cc、Bccの情報) (※)

・ 添付ファイル名(※)

[備考]の表示例

[件名：本日の業務報告について From：Mail Address-A To：Mail Address-B CC：Mail Address-C Mail BCC：Address-D 添付：添付ファイル名]

※) ログビューアでのキーワード検索時、キーワードとして指定できます。

8.2.7 メール添付禁止ログ

クライアント(CT)で、禁止対象のファイルをメールに添付して、送信または保存しようとしたときのログです。
メール添付禁止ログには、送信を禁止されたメールのタイトル、送信元アドレス、あて先、添付ファイル名が出力されます(ポート監視方式の場合のみ)。
またメールソフトのアプリケーション名も出力されます。
メールソフトの情報は、以下の2とおりの採取方法があります。

- ポート監視方式の場合(注1):

  メールソフトのアプリケーション名（メール情報のヘッダにある情報）が採取されます。

- V12.0L20～V13.0.0互換方式の場合(注2):

  メールソフトのアプリケーションEXE名が採取されます。

  注1) ドライバ方式で禁止を行う方式で、SMTPプロトコルを使用するメールソフトを利用した場合にログを採取する方式です。

  注2) メーラーの動作を制御する方式で、以下のメールソフトを利用した場合にログを採取する方式です。

  - Microsoft® Outlook® Express 5.5
  - Microsoft® Outlook® Express 6.0
  - Microsoft® Outlook® 2000
  - Microsoft® Outlook® 2002
  - Microsoft® Outlook® 2003

採取するために設定するポリシー

[端末初期設定]画面、[ユーザーポリシー設定]画面、または管理コンソール起動直後の画面(CTポリシー設定画面)で設定します。

- [メール送信]タブと、[メール添付禁止拡張子設定]で、メール添付を禁止するファイルを設定します。
  設定値の詳細は、“2.4.1.8 [メール送信]タブの設定”を参照してください。

表示内容

参照できるログの内容は以下のとおりです。

[名称]: クライアント(CT)の名称

[発生日時]: クライアント(CT)におけるログ採取日時

[ユーザー名]: 以下の情報が表示されます。

- ログオン時:クライアント(CT)のログオンユーザー名
- 未ログオン時:SYSTEM(固定)

[ドメイン名]: 以下の情報が表示されます。

- ドメインにログオン時:クライアント(CT)のドメイン名
- ローカルコンピュータにログオン時:クライアント(CT)のコンピュータ名
- 未ログオン時:クライアント(CT)のコンピュータ名

[種別]: [メール添付禁止] (固定値)

[区分]: 違反

[付帯]:(表示されません)

[内容]:以下の内容が表示されます。

- 禁止されたファイル名(※)
- メールソフトのアプリケーション名(※)

[内容]の表示例

[顧客情報一覧.xls]のメール添付を禁止しました。アプリ名：[xxx]

※) ログビューアでのキーワード検索時、キーワードとして指定できます。

[備考]:以下の内容が表示されます。ただし、ポート監視方式を指定した場合だけ取得される情報です。

- メールのタイトル(※)
- 送信元アドレス(※)
- 送信先アドレス(To、Cc、Bccの情報) (※)
- すべての添付ファイル名(※)

[備考]の表示例

[件名：本日の業務報告について From：Mail Address-A　To：Mail Address-B CC：Mail Address-C Mail BCC：Address-D 添付：添付ファイル名]

※) ログビューアでのキーワード検索時、キーワードとして指定できます。

8.2.8 コマンドプロンプト操作ログ

クライアント(CT)で入力されたコマンドおよびコマンド結果のログです。

クライアント(CT)でコマンドプロンプトを起動し、何らかのコマンドを入力して、コマンドプロンプトを閉じたあとに採取されます。

Citrix XenApp Server(TM)と連携する場合、“公開アプリケーション”で公開するコマンドプロンプトの、“コマンドプロンプト操作ログ”を取得するためには、%SystemRoot%¥system32¥fsw41ej1.exeを登録してください。方法は、Citrix XenApp Server(TM)のマニュアルを参照してください。

注意

使用している環境によって、機能が制限される場合があります

ポリシーを設定した場合でも、使用している環境によって、機能が制限される場合があります。
詳細は、“1.2.22 コマンドプロンプト操作ログ”を参照してください。

採取するために設定するポリシー

[端末初期設定]画面、[ユーザーポリシー設定]画面、または管理コンソール起動直後の画面(CTポリシー設定画面)で設定します。
[各種ログスイッチ]タブで、[コマンドプロンプト操作ログ]に[する]を設定します。

表示内容

参照できるログの内容は以下のとおりです。

[名称]:クライアント(CT)の名称

[発生日時]:クライアント(CT)におけるログ採取日時

[ユーザー名]:クライアント(CT)のログオンユーザー名

[ドメイン名]:ドメインにログオン時はクライアント(CT)のドメイン名、ローカルコンピュータにログオン時はクライアント(CT)のコンピュータ名

[種別]:[コマンドプロンプト操作] (固定値)

[区分]:正規

[付帯]:(表示されません)

[内容]:クライアント(CT)のコマンドプロンプトで入力したコマンドおよびコマンドの結果

[内容]の表示例

```
                                                --[2007/04/16 23:04:48]--

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
 E:¥Documents and Settings¥dtk-user>dir
 ドライブ E のボリューム ラベルがありません。
 ボリューム シリアル番号は 2079-E604 です
 E:¥Documents and Settings¥dtk-user のディレクトリ
2007/04/16  22:39      <DIR>          .
2007/04/16  22:39      <DIR>          ..
2007/04/16  22:39      <DIR>          Favorites
2006/11/28  21:13      <DIR>          My Documents
2006/11/28  21:13      <DIR>          スタート メニュー
2007/04/16  22:39      <DIR>          デスクトップ

               0 個のファイル                  0 バイト

               6 個のディレクトリ  10,149,437,440 バイトの空き領域

E:¥Documents and Settings¥dtk-user>exit
```

[備考]:(表示されません)

8.2.9 デバイス構成変更ログ

クライアント(CT)でデバイスの構成を変更(ドライブレターの変更を伴う記憶デバイスを追加した場合や、同一ドライブレター内での装置変更によりデバイス名や内部シリアル番号などが変わった場合)したときのログです。

Systemwalker Desktop Rights Masterと混在運用時は、クライアント(CT)においてSystemwalker Desktop Rights Masterの仮想ドライブ割り当て処理に伴い、構成変更ログが採取される場合があります。

採取するために設定するポリシー

[端末初期設定]画面、[ユーザーポリシー設定]画面、または管理コンソール起動直後の画面(CTポリシー設定画面)で設定します。
[各種ログスイッチ]タブで、[デバイス構成変更ログ]に[する]を設定します。

採取される情報

ドライブの種別によって、[備考]欄に表示される情報が異なります。

ドライブの種別	ボリューム	デバイス名	内部シリアル番号	サーバ名・共有名
固定	○	―	―	―
リムーバブル	―	○(注1)	○(注1)	―
CD-ROM	―	○(注1)	○(注1)	―
リモート(注2)	―	―	―	○

○:情報を採取します。
―:情報を採取しません。

注1) USB接続の場合だけ、情報を記録します。
注2) 他のPCに装着されているフロッピーディスク装置やUSBメモリ装置をドライブ共有した場合は、ドライブの種別は“リモート”として記録されます。

表示内容

参照できるログの内容は以下のとおりです。

[名称]:クライアント(CT)の名称

[発生日時]:クライアント(CT)におけるログ採取日時

[ユーザー名]:クライアント(CT)のログオンユーザー名

[ドメイン名]:ドメインにログオン時はクライアント(CT)のドメイン名、ローカルコンピュータにログオン時はクライアント(CT)のコンピュータ名

[種別]:[デバイス構成変更] (固定値)

[区分]:[正規]または[違反](注5)

[付帯]:(表示されません)

[内容]:以下の内容が表示されます。

- [追加]または[変更](注3)
- ドライブレター(注3)
- ドライブの種別(注3)

注3) ログビューアでのキーワード検索時、[ ]内の値をキーワードとして指定できます。

[追加]と記録されるのは、以下の場合です。

- ログオン時に、前回のログオフ時の情報と現在のドライブ情報を比較した結果、増加しているドライブがあったとき
- ログオン中に、デバイスを追加したとき
- ログオンしていないときにデバイスを追加し、ログオンしたとき
- ログオン中に、すでに接続されていたデバイスをはずし、同じドライブに別のデバイスを接続したとき

[変更]と記録されるのは、ログオン中に、以下のいずれかの操作を実施した場合です。

- ドライブ種別を変更する
- サーバの共有名を、既存のネットワークドライブに割り当てる

[備考]:以下の内容が表示されます。

- ボリューム(注4)
- デバイス名(注4)
- 内部シリアル番号(注4)
- サーバ名・共有名(注4)

注4) ログビューアでのキーワード検索時、[ ]内の値をキーワードとして指定できます。

注5) [ファイル持出し禁止 - USBデバイス個体識別機能 - 詳細設定]画面の[使用可能USBデバイス一覧]に登録されているUSBデバイスが装着された場合は、違反と記録されません([USBデバイス登録]画面において[USBデバイスの識別方法]が[使用不可]に設定されているUSBデバイスは、登録されていないものとみなします)。
違反と記録されるのは、以下の2つのパターンのいずれかにおいて、パターン内の条件をすべて満たす場合に、[使用可能USBデバイス一覧]に登録されていないUSBデバイスを装着したときです。
[端末初期設定]画面、[ユーザーポリシー設定]画面、またはCTポリシー設定画面で設定します。

・ パターン1

　ー [ファイル持出し禁止]タブで、[USBデバイス個体識別機能]を[利用する]と選択したとき。

　ー [ファイル持出し禁止]タブで、[持出し禁止]を[禁止する](ドライブ指定またはリムーバブルを指定)と選択したとき。

・ パターン2

　ー [ファイル持出し禁止]タブで、[USBデバイス個体識別機能]を[利用する]と選択したとき。

　ー [ファイル持出し禁止]タブで、[持出し禁止]を設定しないとき。

　ー [ファイル持出し禁止]タブで、[ファイル持出しユーティリティを使用しての持出し]を[可]と選択したとき。

[内容]および[備考]の表示例
情報を取得できない場合は、空欄表示([ ])されます。

内蔵ハードディスク装置を装着した場合

内容	備考
[追加 D:固定]	ボリューム[Windows2000]

OSのExplorerでのドライブ情報参照時に、“ローカルディスク(D:)”と表示されている場合、ボリュームは空欄表示([ ])されます。

USB接続のUSBメモリ装置、ハードディスク装置、フロッピーディスク装置などを接続した場合

内容	備考
[追加 G:リムーバブル]	デバイス名[BUFFALO USB Flash Disk USB Device]、内部シリアル番号[B32986]

USB接続のCD/DVD装置を接続した場合

内容	備考
[追加 E:CD-ROM]	デバイス名[MATSHITA UJD330]、内部シリアル番号[ ]

USB接続以外(IDE接続、IEEE接続など)のCD/DVD装置は、備考欄は空欄表示([ ])されます。

ネットワークドライブを追加した場合

内容	備考
[追加 G:リモート]	ボリューム[SOUMUDISK]、サーバ名・共有名[¥¥ServerSOUMU¥SOUMUDISK]

“サーバ名・共有名”は、“¥¥サーバのIPアドレス¥共有名”として表示される場合もあります。

USBデバイスの個体識別を実施しており、許可されていないUSBデバイス(リムーバブルと認識するもの)を装着した場合

区分	内容	備考
違反	[追加 G:リムーバブル]	デバイス名:[BUFFALO USB Flash Disk USB Device]、内部シリアル番号:[B32986]

ハードディスクの物理的破損や、他のアプリケーションが前回のデバイス構成を記録したファイルを排他的にアクセスしている場合には、デバイス構成変更ログの[内容]が「不明」となる場合があります。

内容	備考
[変更 A:不明→リムーバブル]	

8.2.10 印刷操作ログ

クライアント(CT)で、印刷を許可されたアプリケーションで行われた印刷のログです。

クライアント(CT)で印刷が行われてからしばらくたった後に、管理サーバへ操作ログが送信されます。

注意

使用している環境によって、機能が制限される場合があります

ポリシーを設定した場合でも、使用している環境によって、機能が制限される場合があります。
詳細は、“1.2.19 印刷操作ログ”を参照してください。

採取するために設定するポリシー

[端末初期設定]画面、[ユーザーポリシー設定]画面、または管理コンソール起動直後の画面(CTポリシー設定画面)で設定します。
[各種ログスイッチ]タブで、[印刷操作ログ]に[する]を設定します。

表示内容

参照できるログの内容は以下のとおりです。

[名称]:クライアント(CT)の名称

[発生日時]:クライアント(CT)におけるログ採取日時

[ユーザー名]:クライアント(CT)のログオンユーザー名

[ドメイン名]:ドメインにログオン時はクライアント(CT)のドメイン名、ローカルコンピュータにログオン時はクライアント(CT)のコンピュータ名

[種別]:[印刷操作] (固定値)

[区分]:[正規]

[付帯]:(表示されません)

[内容]:以下の内容が表示されます。

- 印刷ファイル名(ドキュメント名)(注)
- 印刷を行ったプリンタ名(注)
- 印刷ファイルの総ページ数
- 印刷を行った日付

内容の表示例

[imgfilelist.xls]が印刷されました。プリンタ名：[KONICA MINOLTA 750/600 PCL]、ページ数：[1]、印刷日付：[2007/04/11 19:44:59]

[備考]:(表示されません)

注) ログビューアでのキーワード検索時、キーワードとして指定できます。

8.2.11 印刷禁止ログ

クライアント(CT)で、印刷を許可されていないアプリケーションで印刷しようとしたときのログです。

採取するために設定するポリシー

[端末初期設定]画面、[ユーザーポリシー設定]画面、または管理コンソール起動直後の画面(CTポリシー設定画面)で設定します。
[印刷禁止]タブで、[印刷禁止]に[する]を設定します。

また、印刷を許可するアプリケーションも[印刷禁止]タブで設定します。
設定値の詳細は、“2.4.1.3 [印刷禁止]タブの設定”を参照してください。

表示内容

参照できるログの内容は以下のとおりです。

[名称]:クライアント(CT)の名称

[発生日時]:クライアント(CT)におけるログ採取日時

[ユーザー名]:クライアント(CT)のログオンユーザー名

[ドメイン名]:ドメインにログオン時はクライアント(CT)のドメイン名、ローカルコンピュータにログオン時はクライアント(CT)のコンピュータ名

[種別]:[印刷禁止] (固定値)

[区分]:違反

[付帯]:(表示されません)

[内容]:以下の内容が表示されます。

- 禁止した印刷ファイル名(※)
- 禁止したアプリケーション名(※)

[内容]の表示例

```
[Microsoft Word - １３. Console.doc]の印刷を禁止しました。アプリ名：[C:¥Program Files¥Microsoft Office¥OFFICE11¥WINWORD.EXE]
```

※) ログビューアでのキーワード検索時、キーワードとして指定できます。

[備考]:(表示されません)

8.2.12 ログオン禁止ログ

クライアント(CT)で、ログオンを禁止されたグループに所属するユーザー名でログオンしようとしたときのログです。

採取するために設定するポリシー

[端末初期設定]画面または管理コンソール起動直後の画面(CTポリシー設定画面)で設定します。
[ログオン禁止]タブで、ログオンを禁止するグループ名を設定します。設定値の詳細は、“2.4.1.4 [ログオン禁止]タブの設定”を参照してください。

表示内容

参照できるログの内容は以下のとおりです。

[名称]:クライアント(CT)の名称

[発生日時]:クライアント(CT)におけるログ採取日時

[ユーザー名]:クライアント(CT)のログオンユーザー名

[ドメイン名]:ドメインにログオン時はクライアント(CT)のドメイン名、ローカルコンピュータにログオン時はクライアント(CT)のコンピュータ名

[種別]:[ログオン禁止] (固定値)

[区分]:違反

[付帯]:(表示されません)

[内容]:以下の内容が表示されます。

- 禁止したユーザー名(グループ) (注1)
- 禁止処理([ログオフ]または[シャットダウン])(注2)
- 禁止結果([成功]または[失敗])

[内容]の表示例

```
[dmn-user(Domain Users)]のログオンを[ログオフ]しました。結果：[成功]
```

注1) ログビューアでのキーワード検索時、キーワードとして指定できます。
ユーザー名とグループ名が対象であり、カッコ記号は検索対象ではありません。
注2) 同一PCにログオンしているユーザーが2人以上の場合で、ログオン禁止されたときは、[ログオフ]と表示されます。

[備考]:(表示されません)

8.2.13 ファイル持出しログ

クライアント(CT)で持出しユーティリティを使用してファイルやフォルダを持ち出したときのログです。ログと同時に、持ち出したファイルの原本を保管することもできます。

注意

使用している環境によって、機能が制限される場合があります

ポリシーを設定した場合でも、使用している環境によって、機能が制限される場合があります。
詳細は、“1.2.18 ファイル持出しログ”を参照してください。

採取するために設定するポリシー

[端末初期設定]画面、[ユーザーポリシー設定]画面、または管理コンソール起動直後の画面(CTポリシー設定画面)で設定します。

- [各種ログスイッチ]タブで、[ファイル持出しログ]に[する]を設定します。
- [各種ログスイッチ]タブで、[原本保管をする]にチェックを付けた場合、持ち出したファイルの原本を保管することができます。
  [ファイル持出しログ]に[する]が設定されている場合に、設定できます。

設定値の詳細は、“2.4.1.2 [ファイル持出し禁止]タブの設定”を参照してください。

表示内容

参照できるログの内容は以下のとおりです。

[名称]:クライアント(CT)の名称

[発生日時]:クライアント(CT)におけるログ採取日時

[ユーザー名]:クライアント(CT)のログオンユーザー名

[ドメイン名]:ドメインにログオン時はクライアント(CT)のドメイン名、ローカルコンピュータにログオン時はクライアント(CT)のコンピュータ名

[種別]:[ファイル持出し] (固定値)

[区分]:正規

[付帯]:付帯(原本)データがある場合は、“1”

[内容]:以下の内容が表示されます。

- 持ち出し元のファイル名(※)
- 持ち出し先のファイル名(※)

・ 持ち出し方法(平文または暗号化)

・ 持ち出し先のドライブレター

・ 持ち出し先のドライブの種別

・ 持ち出し理由(※)

内容の表示例

暗号化持ち出しの場合

[C:¥Documents and Settings¥Administrator¥デスクトップ¥顧客情報一覧.xls]を[G:¥顧客情報一覧.exe]として[暗号化]で[G:]へ持出ししました。ドライブ種別：[リムーバブル]

平文持ち出しの場合

[D:¥製品顧客2007年10月度.XLS]を[E:¥製品顧客2007年10月度.XLS]として[平文]で[E:]へ持出ししました。ドライブ種別：[CD/DVD]

暗号ファイルの持ち出し先をUNC(先頭が“¥¥”で始まるアドレス)指定した場合

[D:¥Documents and Settings¥Administrator¥デスクトップ¥新規文書.txt]を [¥¥Server1¥UserDocument¥新規文書.txt]として[暗号化]で[リモート]へ持出ししました。ドライブ種別：[リモート]

持ち出し理由を入力するポリシー設定の場合

[C:¥Documents and Settings¥Administrator¥デスクトップ¥Ａ社様重要顧客情報.xls]を[E:¥顧客情報.ex_]として[暗号化]で[E:]へ持出ししました。ドライブ種別：[リムーバブル]、持出し理由：[××業務で○○委託先に□□情報を持出すため]

※) ログビューアでのキーワード検索時、キーワードとして指定できます。

[備考]:以下の内容が表示されます。

・ ボリューム(※1)(※4)

・ サイズ(※1)(※2)(※4)

・ デバイス名(※3)(※4)

・ 内部シリアル番号(※3)(※4)

・ USB装置名(※3)(※4)(※5)

※1) V13.2.0以前に採取されたファイル持出しログの場合は、[ ]は空欄で表示されます。
※2) フォルダを持ち出した場合は、[ ]は空欄で表示されます。
※3) 持出し先がUSB接続の媒体の場合に表示されます。
※4) ログビューアでのキーワード検索時、キーワードとして指定できます。
※5) 管理コンソールの[USBデバイス登録]画面でUSBデバイスを登録し、以下のポリシー設定を行った場合だけ、表示されます。USBデバイス登録時に[USB装置名]に設定された情報です。

・ [端末初期設定]画面、[ユーザーポリシー設定]画面、またはCTポリシー設定画面の[各種ログスイッチ]タブで、[デバイス構成変更ログ]に[する]が設定されているとき。

・ [端末初期設定]画面またはポリシー設定画面の[ファイル持出し禁止]タブで、[ファイル持出しユーティリティを使用しての持出し]を[可]と選択したとき。

・ [ファイル持出しユーティリティ機能設定]画面で、[持出しユーティリティのUSBデバイスの使用制限]に[する]を選択し、[指定USBデバイスのみ許可する]をチェックしたとき。

[備考]の表示例

V13.2.0以前に採取されたファイル持出しログの場合

ボリューム：[ ]、サイズ(バイト)：[ ]

USB接続の媒体以外へ持ち出した場合

フォルダを持ち出したとき

ボリューム：[USERVOL]、サイズ(バイト)：[ ]

ファイルを持ち出したとき

ボリューム：[USERVOL]、サイズ(バイト)：[123,456]

USBデバイスの個体識別を実施していない場合に、USBデバイスの媒体へ持ち出した場合

フォルダを持ち出したとき

ボリューム：[USERVOL]、サイズ(バイト)：[ ]、デバイス名：[デバイス名の文字列]、内部シリアル番号：[0E40986050226896]

ファイルを持ち出したとき

ボリューム：[USERVOL]、サイズ(バイト)：[123,456]、デバイス名：[デバイス名の文字列]、内部シリアル番号：[0E40986050226896]

USBデバイスの個体識別を実施している場合に、USBデバイスの媒体へ持ち出した場合

フォルダを持ち出したとき

ボリューム：[USERVOL]、サイズ(バイト)：[ ]、デバイス名：[デバイス名の文字列]、内部シリアル番号：[0E40986050226896]、USB装置名：[I-O xxyyzz社 ED-123型]

ファイルを持ち出したとき

ボリューム：[USERVOL]、サイズ(バイト)：[123,456]、デバイス名：[デバイス名の文字列]、内部シリアル番号：[0E40986050226896]、USB装置名：[I-O xxyyzz社 ED-123型]

8.2.14 PrintScreenキー操作ログ

クライアント(CT)でPrintScreenキーを使用したときのログです。ログと同時に、PrintScreenキー操作時の画面キャプチャを採取することもできます。

採取するために設定するポリシー

[端末初期設定]画面、[ユーザーポリシー設定]画面、または管理コンソール起動直後の画面(CTポリシー設定画面)で設定します。
以下の両方を設定した場合に、PrintScreenキー操作ログが採取されます。

- [印刷禁止]タブで、[PrintScreenキー無効化]を[しない]に設定します。
- [各種ログスイッチ]タブで、[PrintScreenキー操作ログ]を[する]に設定します。
- [各種ログスイッチ]タブで、[画面キャプチャする]にチェックを付けた場合、PrintScreenキーを使用したときの画面キャプチャを採取できます。
  [PrintScreenキー操作ログ]に[する]が設定されている場合に、設定できます。

表示内容

参照できるログの内容は以下のとおりです。

[名称]:クライアント(CT)の名称

[発生日時]:クライアント(CT)におけるログ採取日時

[ユーザー名]:クライアント(CT)のログオンユーザー名

[ドメイン名]:ドメインにログオン時はクライアント(CT)のドメイン名、ローカルコンピュータにログオン時はクライアント(CT)のコンピュータ名

[種別]:[PrintScreenキー禁止] (固定値)

[区分]:[正規] (固定値)

[付帯]:付帯(画面キャプチャ)データがある場合は“1”

[内容]:以下の内容が表示されます。

・ PrintScreenキーが押された情報

[内容]の表示例

```
PrintScreenキーが押下されました。
```

ログビューアでのキーワード検索時、「PrintScreenキーが押下されました。」という文字を検索できます。

[備考]:(表示されません)

8.2.15 PrintScreenキー禁止ログ

クライアント(CT)でのPrintScreenキーの使用を禁止されている場合に、PrintScreenキーを操作したときのログです。
「PrintScreenキーの使用を禁止されている」とは、PrintScreenキーを押しても画面のハードコピーは採取できない状況を指します。
ログと同時に、PrintScreenキー操作時の画面キャプチャを採取することもできます。

活用方法

PrintScreenキーの使用を認められていないのに、画面のハードコピーを採取しようとした、違反操作を行うユーザーを洗い出せます。どのような画面のハードコピーを採取しようとしたかが分かるので、何をしたかったのか予測できます。セキュリティ上の重大な問題となる行為の予防に役立ちます。

採取するために設定するポリシー

[端末初期設定]画面、[ユーザーポリシー設定]画面、または管理コンソール起動直後の画面(CTポリシー設定画面)で設定します。
以下の両方を設定した場合に、PrintScreenキー禁止ログが採取されます。

・ [各種ログスイッチ]タブで、[PrintScreenキー操作ログ]を[しない]に設定します。

・ [印刷禁止]タブで、[PrintScreenキー無効化]を[する]に設定します。

・ [印刷禁止]タブで、[画面キャプチャする]にチェックを付けた場合、PrintScreenキーを使用したときの画面キャプチャを採取できます。

表示内容

参照できるログの内容は以下のとおりです。

[名称]:クライアント(CT)の名称

[発生日時]:クライアント(CT)におけるログ採取日時

[ユーザー名]:クライアント(CT)のログオンユーザー名

[ドメイン名]:ドメインにログオン時はクライアント(CT)のドメイン名、ローカルコンピュータにログオン時はクライアント(CT)のコンピュータ名

[種別]:[PrintScreenキー禁止] (固定値)

[区分]:[違反] (固定値)

[付帯]:付帯(画面キャプチャ)データがある場合は“1”

[内容]:以下の内容が表示されます。

・ PrintScreenキーが押された情報

[内容]の表示例

```
PrintScreenキーが押下されました。
```

ログビューアでのキーワード検索時、「PrintScreenキーが押下されました。」という文字を検索できます。

[備考]:(表示されません)

8.2.16 Web操作ログ

クライアント(CT)で以下の操作を実施したときのログです。

・ Webサイトからのダウンロード

ファイル送信または受信を開始後、異常が発生したり、ユーザーによってファイル送信または受信がキャンセルされた場合でも、ログは採取されます。

採取するために設定するポリシー

[端末初期設定]画面、[ユーザーポリシー設定]画面、または管理コンソール起動直後の画面(CTポリシー設定画面)で設定します。
[各種ログスイッチ]タブの[Web操作ログ]を[する]に設定します。

検索方法

ログビューアでの検索時、ログ種別には“Web操作”、区分には“正規”を選択します。
キーワードに“Web操作”または“Webダウンロード”を設定した場合は、Webダウンロードログを検索できます。
キーワードは、部分一致で検索されます。

表示内容

参照できるログの内容は以下のとおりです。

[名称]:クライアント(CT)の名称

[発生日時]:クライアント(CT)におけるログ採取日時

[ユーザー名]:クライアント(CT)のログオンユーザー名

[ドメイン名]:ドメインにログオン時はクライアント(CT)のドメイン名、ローカルコンピュータにログオン時はクライアント(CT)のコンピュータ名

[種別]: Webダウンロード(固定値)

[区分]:正規

[付帯]:(表示されません)

[内容]:以下の内容が表示されます。

・ Webページを表示したアプリケーション名(※)

・ アクセス先のURL文字列(※)

・ ファイル名(※)

内容に表示される文字列の最大長は519バイトまでです。内容に設定される文字列が519バイトを超えた場合は、519バイト以内で表示するため、内容の長さが調整されます。

[内容]の表示例

```
[www.aaa.com]からダウンロード操作が行われました。アプリ名：[iexplore.exe]、ファイル名：[c:¥test¥test.txt]
```

※) ログビューアでのキーワード検索時、キーワードとして指定できます。

[備考]:(表示されません)

8.2.17 Web操作禁止ログ

クライアント(CT)で以下の操作を実施したときのログです。

- 禁止されたURLへのアクセス(URLアクセス禁止ログ)
- 許可されたサイト以外からのダウンロード(Webダウンロード禁止ログ)
  Webサイトの画面上のボタン、リンク、メニューなどから、ファイルのダウンロードを選択した場合

採取するために設定するポリシー

[端末初期設定]画面、[ユーザーポリシー設定]画面、または管理コンソール起動直後の画面(CTポリシー設定画面)で設定します。

- [URLアクセス禁止]タブの[URLアクセス]を「禁止する」に設定します。
- [Webダウンロード禁止]タブの[ダウンロード]を「禁止する」に設定します。

検索方法

- URLアクセス禁止ログの場合

  ログビューアでの検索時、ログ種別には“Web操作禁止”、区分には“違反”、キーワードには“iexplore.exe”、“Web操作禁止”、“URLアクセス禁止”を検索条件として入力します。キーワードには、アクセスしたサイトのURL文字列も指定できます。
  キーワードは、部分一致で検索されます。

- Webダウンロード禁止ログの場合

  ログビューアでの検索時、ログ種別には“Web操作禁止”、区分には“違反”、キーワードには“Webダウンロード”を検索条件として入力します。キーワードには、Webページを表示したアプリケーション名、アクセス先のURL文字列も指定できます。
  キーワードは、部分一致で検索されます。

表示内容

参照できるログの内容は以下のとおりです。

[名称]:クライアント(CT)の名称

[発生日時]:クライアント(CT)におけるログ採取日時

[ユーザー名]:クライアント(CT)のログオンユーザー名

[ドメイン名]:ドメインにログオン時はクライアント(CT)のドメイン名、ローカルコンピュータにログオン時はクライアント(CT)のコンピュータ名

[種別]:操作内容ごとに以下が表示されます(固定値)。

- URLアクセス禁止
- Webダウンロード禁止

[区分]:違反

[付帯]:(表示されません)

[内容]:以下の内容が表示されます。

- Webページを表示したアプリケーション名(※)
- アクセス先のURL文字列(※)

内容に表示される文字列の最大長は519バイトまでです。内容に設定される文字列が519バイトを超えた場合は、519バイト以内で表示するため、内容の長さが調整されます。

[内容]の表示例

[URLアクセス禁止]の場合

```
[www.aaa.com]への接続を禁止しました。アプリ名：[iexplore.exe]
```

[Webダウンロード禁止]の場合

```
[www.aaa.com]からのダウンロードを禁止しました。アプリ名：[iexplore.exe]
```

※) ログビューアでのキーワード検索時、キーワードとして指定できます。

[備考]:(表示されません)

8.2.18 FTP操作ログ

クライアント(CT)で以下の操作を実施したときのログです。

- FTPサーバへのファイルのアップロード(FTPアップロードログ)
- FTPサーバからのファイルのダウンロード(FTPダウンロードログ)

FTPクライアントの接続先サーバの通信ポートとして「21」が設定されているFTP通信のログだけ、記録します。

ファイル転送開始後、異常が発生したり、ユーザーによってファイル転送がキャンセルされた場合でも、ログは採取されます。

採取するために設定するポリシー

[端末初期設定]画面、[ユーザーポリシー設定]画面、または管理コンソール起動直後の画面(CTポリシー設定画面)で設定します。
[各種ログスイッチ]タブの[FTP操作ログ]を[する]に設定します。

検索方法

ログビューアでの検索時、ログ種別には“FTP操作”、区分には“正規”を選択します。
キーワードに、“FTP操作”を設定した場合は、FTPアップロードログおよびFTPダウンロードログを検索できます。
キーワードに、“FTPアップロード”を設定した場合は、FTPアップロードログを検索できます。また、“FTPダウンロード”を設定した場合は、FTPダウンロードログを検索できます。
キーワードは、部分一致で検索可能です。

表示内容

参照できるログの内容は以下のとおりです。

[名称]:クライアント(CT)の名称

[発生日時]:クライアント(CT)におけるログ採取日時

[ユーザー名]:クライアント(CT)のログオンユーザー名

[ドメイン名]:ドメインにログオン時はクライアント(CT)のドメイン名、ローカルコンピュータにログオン時はクライアント(CT)のコンピュータ名

[種別]:ログ種別ごとに以下が表示されます(固定値)。

- FTPアップロード
- FTPダウンロード

[区分]:正規

[付帯]:(表示されません)

[内容]:以下の内容が表示されます。
内容に表示される文字列の最大長は519バイトまでです。内容に設定される文字列が519バイトを超えた場合は、519バイト以内で表示するため、内容の長さが調整されます。

- FTPクライアントプログラム名(※)
- FTPサーバのIPアドレス(※)
- ファイル名(※)

[内容]の表示例

[FTPアップロード]の場合

```
[192.168.1.100]へのアップロード操作が行われました。アプリ名：[FTP.EXE]、ファイル名:[Test.txt]
```

[FTPダウンロード]の場合

```
[192.168.1.100]からダウンロード操作が行われました。アプリ名：[FTP.EXE]、ファイル名:[Test.txt]
```

※) ログビューアでのキーワード検索時、キーワードとして指定できます。

[備考]:(表示されません)

8.2.19 FTP操作禁止ログ

クライアント(CT)で、許可されたFTPサーバ以外へ接続したときのログです。

FTPクライアントの接続先サーバの通信ポートとして「21」が設定されているFTP通信のログだけ、記録します。

使用している環境によって、機能が制限される場合があります

ポリシーを設定した場合でも、使用している環境によって、機能が制限される場合があります。
詳細は、"1.2.15 FTPサーバ接続禁止"を参照してください。

採取するために設定するポリシー

[端末初期設定]画面、[ユーザーポリシー設定]画面、または管理コンソール起動直後の画面(CTポリシー設定画面)で設定します。
[FTPサーバ接続禁止]タブで、[FTPサーバ接続]を[禁止する]に設定します。

検索方法

ログビューアでの検索時、ログ種別には"FTP操作禁止"、区分には"違反"、キーワードには"FTPサーバ接続禁止"を検索条件として入力します。キーワードには、FTPクライアントプロセス名、アクセスしたFTPサーバのIPアドレスも指定できます。
キーワードは、部分一致で検索されます。

表示内容

参照できるログの内容は以下のとおりです。

[名称]:クライアント(CT)の名称

[発生日時]:クライアント(CT)におけるログ採取日時

[ユーザー名]:クライアント(CT)のログオンユーザー名

[ドメイン名]:ドメインにログオン時はクライアント(CT)のドメイン名、ローカルコンピュータにログオン時はクライアント(CT)のコンピュータ名

[種別]:FTPサーバ接続禁止(固定値)

[区分]:違反

[付帯]:(表示されません)

[内容]:以下の内容が表示されます。

- FTPクライアントプログラム名(※)
- FTPサーバのIPアドレス(※)

内容に表示される文字列の最大長は519バイトまでです。内容に設定される文字列が519バイトを超えた場合は、519バイト以内で表示するため、内容の長さが調整されます。

[内容]の表示例

[192.168.1.100]への接続を禁止しました。アプリ名：[FTP.EXE]

※) ログビューアでのキーワード検索時、キーワードとして指定できます。

[備考]:(表示されません)

8.2.20 ファイル操作ログ

クライアント(CT)で実施された、以下のドライブでのファイル操作やフォルダ操作のログです。

- ローカルドライブ
- ネットワークドライブ
- リムーバブルドライブ

注意

使用している環境によって、機能が制限される場合があります

ポリシーを設定した場合でも、使用している環境によって、機能が制限される場合があります。
詳細は、“1.2.28 ファイル操作ログ”を参照してください。

採取するために設定するポリシー

[端末初期設定]画面、または管理コンソール起動直後の画面(CTポリシー設定画面)で設定します。

- [各種ログスイッチ]タブで、[ファイル操作ログ]に[する]を設定します。
- [ファイル操作プロセス]タブで、ファイル操作ログのフィルタ条件を設定します。

  [ファイル操作ログ]に[する]が設定されている場合に、設定できます。
- [ファイル操作拡張子]タブで、どの拡張子のファイルを操作した場合にログを採取するかを設定します。

  [ファイル操作ログ]に[する]が設定されている場合に、設定できます。

設定値の詳細は、“2.4.1.6 [ファイル操作プロセス]タブの設定”および“2.4.1.7 [ファイル操作拡張子]タブの設定”を参照してください。

表示内容

参照できるログの内容は以下のとおりです。

[名称]:クライアント(CT)の名称

[発生日時]:クライアント(CT)におけるログ採取日時

[ユーザー名]:以下の情報が表示されます。

- ログオン時:クライアント(CT)のログオンユーザー名
- 未ログオン時:SYSTEM(固定)

[ドメイン名]:以下の情報が表示されます。

- ドメインにログオン時:クライアント(CT)のドメイン名
- ローカルコンピュータにログオン時:クライアント(CT)のコンピュータ名
- 未ログオン時:クライアント(CT)のコンピュータ名

[種別]:[ファイル操作] (固定値)

[区分]:正規

[付帯]:(表示されません)

[内容]:詳細は、"採取される操作ログ"を参照してください。

[内容]の表示例

```
操作：[変名]、ファイル名元：[C:¥Documents and Settings¥Administrator¥デスクトップ¥新規Microsoft Excel ワークシート.xls]、ドライブ種別元：[固定]、ファイル名先：[C:¥Documents and Settings¥Administrator¥デスクトップ¥顧客情報一覧.xls]、ドライブ種別先：[固定]、アプリ名：[Explorer.exe]
```

[備考]:以下の情報が表示されます。

- ファイル操作が[参照]、[更新]、[作成]、[複写]、[移動]、[変名]の場合は、操作後のファイルサイズが表示されます。ファイルサイズの情報が正常に取得できていなかった場合は、半角空白(サイズ(バイト):[ ])が表示されます。また、ファイルサイズが2147483647バイトを超える場合は、「サイズ(バイト):[2147483647]」と表示されます。
- フォルダ操作の場合、またはファイル操作で[削除]の場合は、備考欄は空欄です。

ログビューアでのキーワード検索時、数字をキーワードとして指定できます。
0 から 2147483647 までを指定できます。
【例】
検索条件に「0123」を指定した場合、「サイズ(バイト):[201,235]」が備考に表示されているログは、検索されます。「サイズ(バイト):[123]」が備考に表示されているログは、検索されません。

採取される操作ログ

ファイル操作ログのポリシーが設定されたクライアント(CT)で、ローカルドライブやネットワークドライブでファイルやフォルダを操作した場合に採取されるログについて説明します。

注意

以下のソフトウェア・コマンドについて説明します。

以下のソフトウェアやコマンドの場合、操作ログは、後述する表のように採取されます。

- エクスプローラ
- メモ帳
- ワードパッド
- Microsoft® Word(2000、2002、2003、2007、および2010の場合) (注)
- Microsoft® Excel(2000、2002、2003、2007、および2010の場合) (注)
- Microsoft® PowerPoint®(2000、2002、2003、2007、および2010の場合) (注)

- コマンドプロンプト中のコマンド(COPY、XCOPY、MOVE、DEL、ERASE、RD、REN、MD)

注）Windows Vista®、Windows Server® 2008、またはWindows® 7の場合は、2003、2007、2010だけサポートしています。

ただし、以下の点に注意してください。

- Microsoft® Wordによる「更新」操作は[作成]としてログが採取されます。
- エクスプローラやXCOPYのように[ファイル操作プロセス]タブで[参照以外を取得]として登録してあるプロセスは、[参照]のログは採取されません。
- 上記のソフトウェアやコマンドの場合でも、余分なログが採取されることがあります。
- 上記以外のソフトウェアやコマンドの場合には、実際の操作と異なる操作ログが採取されることがあります(たとえば、「複写」や「移動」のログが採取できず、[参照]、[作成]、[削除]、または[変名]としてログが採取されます)。
- コマンドプロンプトで、リダイレクト処理(> または >>)を使用した場合、ログが出力されないことがあります。

クライアント(CT)でファイルやフォルダを操作したときに採取されるログの種別は、以下のとおりです。

ログ種別	ログビューアの[内容]の表示
参照	操作:[参照]、ファイル名:[(注1)]、ドライブ種別:[(注2)]、アプリ名:[(注5)]
更新	操作:[更新]、ファイル名:[(注1)]、ドライブ種別:[(注2)]、アプリ名:[(注5)]
作成	操作:[作成]、ファイル名:[(注1)]、ドライブ種別:[(注2)]、アプリ名:[(注5)]
削除	操作:[削除]、ファイル名:[(注1)]、ドライブ種別:[(注2)]、アプリ名:[(注5)]
複写	操作:[複写]、ファイル名元:[(注1)]、ドライブ種別元:[(注2)]、 ファイル名先:[(注3)]、ドライブ種別先:[(注4)]、アプリ名:[(注5)]
移動	操作:[移動]、ファイル名元:[(注1)]、ドライブ種別元:[(注2)]、 ファイル名先:[(注3)]、ドライブ種別先:[(注4)]、アプリ名:[(注5)]
変名	操作:[変名]、ファイル名元:[（注1）]、ドライブ種別元:[（注2）]、 ファイル名先:[（注3）]、ドライブ種別先:[（注4）]、アプリ名:[（注5）]

注1) ローカルドライブの場合、操作対象の元となるファイル名またはフォルダ名(フルパスで表示されます)
ネットワークドライブの場合、操作対象の元となるファイル名またはフォルダ名(UNC表記またはUNC表記のマシン名の部分がIPアドレスで表示されます)

注2) 操作対象の元となるドライブの種別

注3) ローカルドライブの場合、操作対象の先となるファイル名またはフォルダ名(フルパスで表示されます)
ネットワークドライブの場合、操作対象の先となるファイル名またはフォルダ名(UNC表記またはUNC表記のマシン名の部分がIPアドレスで表示されます)
ただし、以下の場合は、ファイル名またはフォルダ名(フルパスで表示されます)

- ネットワークドライブにドライブレターの割り当てを行い、割り当てたドライブレターから変名の操作を行った
- ネットワークドライブにドライブレターの割り当てを行い、割り当てたドライブレター内で移動の操作を行った
- ネットワークドライブとして割り当てたドライブレターに対して、割り当てたドライブレターと同じネットワークドライブに直接アクセスしたフォルダから移動の操作を行った

注4) 操作対象の先となるドライブの種別

注5) 操作したアプリケーション名

ログが採取できる条件

前述した“ログ種別”がどのような条件下で、どのような操作を行ったときに採取できるかについて、以下に示します。

条件			ファイルやフォルダへの操作						
			参照	更新	作成	削除	複写	移動	変名
ファイル操作	ファイルに対するログ	同じドライブ内(注1)	参照(注3)	更新(注3)	作成	削除	複写	変名(移動)	変名
		異なるドライブ間(注2)	―	―	―	―	複写	移動	―
フォルダ操作	フォルダ配下のファイルに対するログ	同じドライブ内(注1)	―	―	―	削除	複写	×(注4)(移動)	―
		異なるドライブ間(注2)	―	―	―	―	複写	移動	―
	フォルダに対するログ	同じドライブ内(注1)	―	―	作成	削除	作成(×)	変名(変名)(削除)	変名
		異なるドライブ間(注2)	―	―	―	―	作成(×)	作成削除(削除)	―

―:不可能な操作です。

×:操作ログを採取できません。

参照/更新/作成/削除/複写/移動/変名:採取される操作ログの種別を示します。

( ):複写先または移動先に同名のファイルやフォルダが存在していた場合に採取される操作ログの種別を示します。( )のない場合は、記述されているログの種別が採取されます。

注1) 同じローカルドライブ内または同じネットワークドライブ内での操作です。たとえば、以下の場合です。

― ローカルドライブ内でのCドライブからCドライブへの操作

― ネットワークドライブ「¥¥dtk¥common¥」内での操作

注2) 異なるローカルドライブ間、ローカルドライブとネットワークドライブ間、または異なるネットワークドライブ間での操作です。たとえば、以下の場合です。

― ローカルドライブ内でのCドライブからDドライブへの操作

― ローカルドライブとネットワークドライブ間での操作

― ネットワークドライブ「¥¥dtk¥common¥」からネットワークドライブ「¥¥dtk¥com¥」への操作

注3) エクスプローラやコマンドプロンプトでのファイルのプロパティ参照は、ログの対象となりません。

注4) 移動元と移動先のフォルダ名が同じ場合、移動元のフォルダ配下には存在し、移動先のフォルダ配下には存在しないファイルに対してだけ、[変名]ログが採取されます。

上記表の見方と出力されるログについて、例を用いて説明します。

【例1】

同じローカルドライブ内でファイル操作として、参照を行った場合、前述したログの種別の「参照」に示されているログが採取されます。

次にログビューアからログを参照している画面を表示します。枠で囲んだ部分が、この場合に採取されたログになります。

上記画面の枠で囲んだ[内容]欄には、以下のように表示されています。

```
操作:[参照]、ファイル名:[D:¥report.doc]、ドライブ種別:[固定]、アプリ名:[winword.exe]
```

この場合、Dドライブの直下にある「report.doc」ファイルが、Wordにより参照されたことを示しています。

【例2】

同じローカルドライブ内でファイル操作として、複写を行った場合、複写先に同名のファイルが存在していた、または存在しなかったに関わらず、前述したログの種別の「複写」に示されているログが採取されます。

ログビューアの[内容]欄に表示されるログの例を以下に示します。

```
操作:[複写]、ファイル名元:[D:¥report.doc]、ドライブ種別元:[固定]、ファイル名先:[D:¥tmp¥report.doc]、ドライブ種別先:[固定]、アプリ名:[Explorer.exe]
```

この場合、Dドライブの直下にある「report.doc」ファイルが、エクスプローラで「D:¥tmp」に複写されたことを示しています。

【例3】

ローカルドライブでフォルダ操作として、空のフォルダを異なるドライブに移動した場合、移動先に同名のフォルダが存在しなかったとき、前述したログの種別の「削除」と「作成」に示されている2つのログが採取されます。

ログビューアの[内容]欄に表示されるログの例を以下に示します。

```
操作:[作成]、ファイル名:[D:¥log]、ドライブ種別:[固定]、アプリ名:[Explorer.exe]
操作:[削除]、ファイル名:[C:¥log]、ドライブ種別:[固定]、アプリ名:[Explorer.exe]
```

この場合、Cドライブの直下にある「log」フォルダが、エクスプローラでDドライブの直下に移動されたことを示しています。

【例4】

ローカルドライブでフォルダ操作として、空のフォルダを異なるドライブに移動した場合、移動先に同名のフォルダが存在していたとき、前述したログの種別の「削除」に示されているログが採取されます。

ログビューアの[内容]欄に表示されるログの例を以下に示します。

```
操作:[削除]、ファイル名:[C:¥log]、ドライブ種別:[固定]、アプリ名:[Explorer.exe]
```

この場合、Cドライブの直下にある「log」フォルダが、エクスプローラで異なるドライブに移動され、移動先に同名のフォルダが存在していたことを示しています。

【例5】

同じネットワークドライブ内でファイル操作として、参照を行った場合、前述したログの種別の「参照」に示されているログが採取されます。

ログビューアの[内容]欄に表示されるログの例を以下に示します。

```
操作:[参照]、ファイル名:[¥¥dtk¥common¥report.doc]、ドライブ種別:[リモート]、アプリ名:[winword.exe]
```

この場合、「dtk」というマシンの「common」共有フォルダ直下にある「report.doc」ファイルが、Wordにより参照されたことを示しています。

8.2.21 ログオン/ログオフログ

クライアント(CT)で以下の操作を実施したときのログです。

- ログオン
- ログオフ
- PC起動
- PC終了
- PC休止
- PC復帰

活用方法

ログオン/ログオフログを採取した場合、以下のように活用できます。

- 悪意を持った第三者の、セーフモードでのPC起動(Systemwalker Desktop Keeperに記録を残さない)によるファイル持出しなど、不正を見つけることができます。
- 業務終了後は電源を落とす、一定時間使用しない場合は休止モードを利用する、など、システムの運用方針に沿ってPCを使用しているか、確認できます。
- PCの電源を入れたまま、長時間使用している利用者を見つけることができます。

採取するために設定するポリシー

[端末初期設定]画面、または管理コンソール起動直後の画面(CTポリシー設定画面)で設定します。
[各種ログスイッチ]タブで、[ログオン/ログオフ ログ]に[する]を設定します。

採取される情報

ログオン/ログオフログで採取される情報について説明します。

以下の契機で該当動作が実行されたことをログとして記録します。

- PC起動ログ

  クライアント(CT)のOSを起動したときの情報です。
  起動モードとして、以下のいずれかの情報を取得します。

  ー [通常モード起動]

  ー [セーフモード起動] (コマンドでのセーフモードを含みます)

  ー [ネットワークが使えるセーフモード起動]

- ログオンログ

  クライアント(CT)でWindowsにログオンしたときの情報です。
  認証先のコンピュータ名を取得します。

- PC休止ログ

  クライアント(CT)が、スタンバイ状態または休止状態に入ったときの情報です。
  前回の電源投入後から、PC休止動作に入るまでの時間を取得します。

- PC復帰ログ

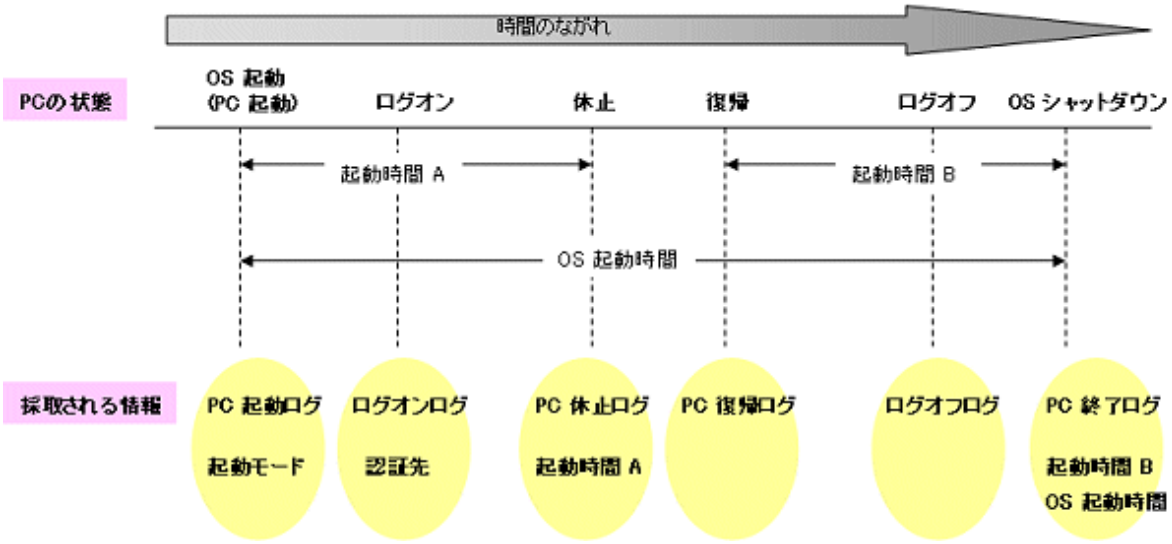
  クライアント(CT)がスタンバイ状態または休止状態から復帰したときの情報です。

- ログオフログ

  クライアント(CT)でWindowsからログオフしたときの情報です。

- PC終了ログ

  クライアント(CT)のOSがシャットダウン動作に入ったときの情報です。
  前回の電源投入後から、シャットダウン動作に入るまでの時間を取得します。
  また、OSを起動したときから、シャットダウン動作に入るまでの時間(OS起動時間)も取得します。



検索方法

- 悪意を持った第三者の、セーフモードでのPC起動(Systemwalker Desktop Keeperに記録を残さない)によるファイル持出しなど、不正を見つける場合

  ログビューアのログ一覧画面で以下の条件を設定すると、セーフモードで起動したPC起動ログだけを検索できます。

  ー [キーワード]に“セーフ”と入力します。

  ー [種別]に[ログオン/ログオフ]を設定します。

- 業務終了後はPCの電源を落とす、PCを一定時間使用しない場合は休止状態にする、など、システムの運用方針に沿ってPCを使用しているか確認する場合

  ログビューアのログ一覧画面で以下の条件を設定すると、PC休止ログとPC復帰ログを検索できます。
  これらのログから、休止状態を設定しているPCを判別できます。

  ー [キーワード]に“休止”と“復帰”を入力します。

  ー [OR条件]ボタンを選択します。

  ー [種別]に[ログオン/ログオフ]を設定します。

  また、PC休止ログとPC復帰ログが翌日にまたがって採取されているPCがある場合は、PCの電源が落とされていないと予測できます。

・ PCの電源を入れたまま、長時間使用している利用者を見つける場合

ログビューアのログ一覧画面で以下の条件を設定すると、PC終了ログとPC休止ログを検索できます。
PC終了ログの[OS起動時間]から、長時間使用されているPCを判別できます。
また、PC終了ログとPC休止ログの[起動時間]を合計することによって、休止時間を除く起動時間を把握できます。

ー [キーワード]に“PC終了”と“PC休止”入力します。

ー [OR条件]ボタンを選択します。

ー [種別]に[ログオン/ログオフ]を設定します。

キーワード検索項目について

PC起動ログの場合は、“通常モード起動”、“セーフモード起動”、“ネットワークが使えるセーフモード起動”の文字列で検索できます。
初回の検索では、キーワードを全角で入力してください。次回からは、前回入力された文字列が、プルダウンメニューに表示されます。

PC終了ログの場合は、“XX時間YY分”の文字列で検索できます。時間は、部分一致または完全一致で検索されます。大小検索は行えません。
数値(“XX”や“YY”)は、半角で入力してください。
“時間”と“分”は、全角で入力してください。

表示内容

参照できるログの内容は以下のとおりです。

[名称]:クライアント(CT)の名称

[発生日時]:クライアント(CT)におけるログ採取日時

[ユーザー名]:以下の情報が表示されます。(注)

・ PC起動時:SYSTEM(固定)

・ PC終了時:SYSTEM(固定)

・ PC休止時:SYSTEM(固定)

・ PC復帰時:SYSTEM(固定)

・ ログオン時:クライアント(CT)のログオンユーザー名

・ ログオフ時:クライアント(CT)のログオンユーザー名

[ドメイン名]:以下の情報が表示されます。

・ PC起動時:クライアント(CT)のコンピュータ名

・ PC終了時:クライアント(CT)のコンピュータ名

・ PC休止時:クライアント(CT)のコンピュータ名

・ PC復帰時:クライアント(CT)のコンピュータ名

・ ログオン時:ドメインにログオン時はクライアント(CT)のドメイン名、ローカルコンピュータにログオン時はクライアント(CT)のコンピュータ名

・ ログオフ時:ドメインにログオン時はクライアント(CT)のドメイン名、ローカルコンピュータにログオン時はクライアント(CT)のコンピュータ名

[種別]:ログ種別ごとに以下が表示されます(固定)。

・ PC起動

・ PC終了

・ PC休止

・ PC復帰

・ ログオン

・ ログオフ

[区分]:正規(固定)

[付帯]:(表示されません)

[内容]:以下の内容が表示されます。

・ PC起動時:コンピュータを起動しました。起動モード:[起動モードの表示] (※)

[起動モードの表示]部分には以下が表示されます。

ー [通常モード起動]

ー [セーフモード起動](コマンドでのセーフモードを含みます)

ー [ネットワークが使えるセーフモード起動]

・ PC終了時:コンピュータを終了しました。起動時間:[起動時間の表示] (※)、OS起動時間:[起動時間の表示] (※)

[起動時間の表示]部分には、[××時間××分]という形式で、時間と分が表示されます。
秒については切り上げて表示されます。
【例】0時間3分0秒の場合:[0時間03分]と出力されます。0時間3分1秒の場合は[0時間04分]と出力されます。

・ PC休止時:コンピュータを休止しました。起動時間:[起動時間の表示] (※)

・ PC復帰時:コンピュータを復帰しました。

・ ログオン時:ログオンしました。認証先:[認証先の表示](※)

[認証先の表示]部分には、[コンピュータ名](local認証の場合)または[ドメイン名](ドメイン認証の場合)が表示されます。

・ ログオフ時:ログオフしました。

※) ログビューアでのキーワード検索時、キーワードとして指定できます。

[備考]:以下の内容が表示されます。

・ [種別]が[ログオン]の場合

ー 接続方法(※)

ー 操作端末(※)

・ [種別]が[PC終了]で、PCの電源を強制的に切断した場合

ー 終了動作:[異常終了(※)]

※) ログビューアでのキーワード検索時、キーワードとして指定できます。

[備考]の表示例

クライアント(CT)に直接ログオンした場合

```
接続方法：[ローカル]、操作端末：[自コンピュータ名]
```

ターミナルサービス経由でログオンした場合

```
接続方法：[リモート]、操作端末：[接続操作を行ったコンピュータ名]
```

PCの電源を強制的に切断した場合

```
終了動作:[異常終了]
```

ログの表示例

```
CLIENT1  2007/11/1 14:15  SYSTEM  D-GALAXY  PC起動  正規      コンピュータを起動しました。起動モード:[通常モード起動]
CLIENT1  2007/11/1 14:20  higashi  D-GALAXY  ログオン  正規      ログオンしました。認証先:[D-GALAXY]  接続方法：[ローカ
```

```
ル]、操作端末：[D-GALAXY]
CLIENT1  2007/11/1 14:15  SYSTEM  D-GALAXY  PC休止  正規      コンピュータを休止しました。起動時間:[3時間12分]
CLIENT1  2007/11/1 14:15  SYSTEM  D-GALAXY  PC復帰  正規      コンピュータを復帰しました。
CLIENT1  2007/11/1 14:18  higashi  D-GALAXY  ログオフ  正規      ログオフしました。
CLIENT1  2007/11/1 14:15  SYSTEM  D-GALAXY  PC終了  正規      コンピュータを終了しました。起動時間:[6時間28分]、OS起動時
間:[6時間28分]
```

注)
Windows Server® 2003上で動作するActive Directoryは、オブジェクトの半角/全角、仮名の種類(カタカナ/ひらがな)、濁音、半濁音、拗音、促音を区別しません。一方、Systemwalker Desktop Keeperのログは、実際にログインした情報で作成します。
したがって、Active Directoryで登録したユーザー名とSystemwalker Desktop Keeperのログに出力されるユーザー名とは異なる場合があります。

【例】
Active Directoryへの登録時に入力したユーザー名が“fujitsu”(半角)で、ログイン時には“FUJITSU”(全角)と入力してログインした場合、その後に記録されるログのユーザー名は、“FUJITSU”(全角)になります。

8.2.22 連携アプリケーションログ

クライアント(CT)と連携するアプリケーションから送信されるログです。

クライアント(CT)と連携するアプリケーションについては、“Systemwalker Desktop Keeper 解説書”の“他製品との連携”を参照してください。

採取するために設定するポリシー

[端末初期設定]画面、または管理コンソール起動直後の画面(CTポリシー設定画面)で設定します。
[各種ログスイッチ]タブで、[連携アプリケーションログ]に[する]を設定します。

表示内容

参照できるログの内容は以下のとおりです。

[名称]:クライアント(CT)の名称

[発生日時]:クライアント(CT)におけるログ採取日時

[ユーザー名]:クライアント(CT)のログオンユーザー名

[ドメイン名]:ドメインにログオン時はクライアント(CT)のドメイン名、ローカルコンピュータにログオン時はクライアント(CT)のコンピュータ名

[種別]:[連携アプリケーション] (固定値)

[区分]:[正規]または[違反]

[付帯]:付帯(原本)データがある場合は、“1”

[内容]:以下の内容が表示されます。

- 連携アプリケーションが通知する製品名
- 連携アプリケーションが通知するメッセージコード
- 連携アプリケーションが通知するメッセージ

[備考]:(表示されません)

連携するアプリケーションによっては、原本保管情報がログに出力されます。

原本データが存在する場合は、連携アプリケーションログ一覧の[付帯]に“1”が表示されます。

8.2.23 設定変更ログ

管理コンソールでクライアント(CT)の設定情報を変更したときのログです。

ログが採取されるタイミングは、以下のいずれかです。

- 管理コンソールでクライアント(CT)の設定情報を変更したとき
- 管理コンソールでサービスを制御したとき
- 管理コンソールでプロセスを制御したとき

採取するために設定するポリシー

ポリシーの設定は不要です。

表示内容

参照できるログの内容は以下のとおりです。

[変更年月日時刻]:設定が変更された年月日および時刻

[設定種別]:以下の情報が表示されます。

- [端末設定]:クライアント(CT)のポリシーを変更した場合
- [階層構成設定]:CTグループツリーでクライアント(CT)を移動したなど、CTグループツリーを変更した場合
- [サービス制御]:クライアント(CT)のサービスを制御した場合
- [プロセス制御]:クライアント(CT)のプロセスを制御した場合

[内容]:以下の内容が表示されます。

- 管理コンソールで変更したクライアント(CT)の設定情報
- 管理コンソールで制御したクライアント(CT)のサービス名および内容([開始]、[停止]、[自動]、[手動]、または[無効])
- 管理コンソールで制御したクライアント(CT)のプロセス名

[内容]の表示例

```
移動対象名称：[MORI-PC]、移動元上位グループ名：[企画部]、移動先上位グループ名：[営業部]
名称：MORI-PC,備考：,印刷禁止：する,PrintScreen無効化：しない
印刷許可アプリ：notepad.exe,備考：
```

[備考]:(表示されません)

付録A 集計目的一覧

ログアナライザで設定されている各集計目的について説明します。

違反操作状況を把握する

No.	目的名	内容	キーワード指定対象項目	詳細表示項目
1	アプリケーション起動禁止の状況把握	アプリケーション起動禁止に該当するデータを分析します。	アプリケーション名	・ アプリケーション名 ・ 発生日時
2	印刷禁止の状況把握	印刷禁止に該当するデータを分析します。	印刷ファイル名	・ 印刷ファイル名 ・ 発生日時
3	ログオン禁止の状況把握	ログオン禁止に該当するデータを分析します。	ユーザー名	・ ユーザー名 ・ 発生日時
4	PrintScreenキー禁止の状況把握	PrintScreenキー禁止に該当するデータを分析します。	なし	・ 発生日時
5	メール添付禁止の状況把握	メール添付禁止に該当するデータを分析します。	添付ファイル名	・ 添付ファイル名 ・ 発生日時

ファイル持出し状況を把握する

No.	目的名	内容	キーワード指定対象項目	詳細表示項目
1	ファイル持出しの状況把握	ファイル持出しに該当するデータを分析します。	元ファイル名	・ 持出し元ファイル名 ・ 持出し先ファイル名 ・ 先ドライブ種別 ・ 持出種別 ・ 発生日時
2	ファイル持出し(ドライブ別)の状況把握	持ち出し先ドライブ別に、ファイル持出しに該当するデータを分析します。	元ファイル名	・ 持出し元ファイル名 ・ 持出し先ファイル名 ・ 持出種別 ・ 発生日時

ファイル操作状況を把握する

No.	目的名	内容	キーワード指定対象項目	詳細表示項目
1	ファイル操作の状況把握	ファイルアクセスに該当するデータを分析します。	ファイル名	・ 操作種別 ・ 元ファイル名 ・ 先ファイル名 ・ 先ドライブ種別 ・ アプリケーション名 ・ 発生日時

No.	目的名	内容	キーワード指定対象項目	詳細表示項目
2	ファイル操作(リモート)の状況把握	ネットワークファイルアクセスに該当するデータを分析します。	ファイル名	• 操作種別 • 元ファイル名 • 先ファイル名 • 先ドライブ種別 • アプリケーション名 • 発生日時
3	ファイル操作(リムーバブル)の状況把握	リムーバブルファイルアクセスに該当するデータを分析します。	ファイル名	• 操作種別 • 元ファイル名 • 先ファイル名 • 先ドライブ種別 • アプリケーション名 • 発生日時
4	DTRM(ファイル登録)の状況把握	DTRMの共有フォルダに新規に作成または保護ファイルを登録する操作ログ(*)を分析します。 *:DTRMの操作ID=00001および00003を集計対象とします。	ファイル名	• ファイル名 • フォルダパス • 発生日時
5	DTRM(アクセス権を追加/変更/削除)の状況把握	DTRMのアクセス許可を追加/変更/削除する操作ログ(*)を分析します。 *:DTRMの操作ID=00010を集計対象とします。	ファイル名	• ファイル名 • ユーザー/グループ名 • 発生日時
6	DTRM(ファイルを削除)の状況把握	DTRMの共有フォルダにあるファイル(保護ファイル)とライセンスを削除する操作ログ(*)を分析します。 *:DTRMの操作ID=00011を集計対象とします。	ファイル名	• ファイル名 • 発生日時
7	DTRM(暗号化ファイル閲覧)の状況把握	DTRMの共有フォルダの暗号化ファイル(保護ファイル)を閲覧する操作ログ(*)を分析します。 *:DTRMの操作ID=00020を集計対象とします。	ファイル名	• ファイル名 • 発生日時
8	DTRM(暗号化ファイル復号)の状況把握	DTRMの共有フォルダで暗号化ファイル(保護ファイル)を復号する操作ログ(*)を分析します。 *:DTRMの操作ID=00021を集計対象とします	ファイル名	• ファイル名 • 発生日時
9	DTRM(オフラインフォルダへ複写)の状況把握	DTRMの共有フォルダからオフラインフォルダへコピー(持ち出し)する操作ログ(*)を分析します。	ファイル名	• ファイル名 • フォルダパス • 発生日時

No.	目的名	内容	キーワード指定対象項目	詳細表示項目
		*:DTRMの操作ID=00023を集計対象とします。		
10	DTRM(オフライン暗号化ファイル復号)の状況把握	DTRMのオフラインフォルダで暗号化ファイル(保護ファイル)を復号する操作ログ(*)を分析します。 *:DTRMの操作ID=00031,00041,00051を集計対象とします。	ファイル名	・ファイル名 ・発生日時
11	DTRM(暗号化ファイル更新)の状況把握	DTRMの共有フォルダで暗号化ファイル(保護ファイル)を更新する操作ログ(*)を分析します。 *:DTRMの操作ID=00024を集計対象とします。	ファイル名	・ファイル名 ・発生日時

アプリケーション・メール状況を把握する

No.	目的名	内容	キーワード指定対象項目	詳細表示項目
1	アプリケーション起動の状況把握	アプリケーション起動に該当するデータを分析します。	アプリケーション名	・発生日時
2	宛先別メール送信の状況把握	宛先別メール送信に該当するデータを分析します。	添付ファイル名	・件名 ・From ・To/CC/BCC ・添付 ・発生日時

印刷操作状況を把握する

No.	目的名	内容	キーワード指定対象項目	詳細表示項目
1	印刷操作(回数)の状況把握	印刷操作に該当するデータを分析します。	印刷ファイル名	・印刷ファイル名 ・ページ数 ・プリンタ名 ・発生日時
2	印刷操作(ページ数)の状況把握	印刷ページ数に該当するデータを分析します。	印刷ファイル名	・ページ数 ・印刷ファイル名 ・発生日時
3	DTRM(暗号化ファイル印刷)の状況把握	DTRMの共有フォルダで暗号化ファイル(保護ファイル)を印刷する操作ログ(*)を分析します。 *:DTRMの操作ID=00200,00201,00210,00211,00220,00221を集計対象とします。	印刷ファイル名	・印刷ファイル名 ・発生日時

Webアクセス状況を把握する

No.	目的名	内容	キーワード指定対象項目	詳細表示項目
1	URL付きウィンドウタイトル取得の状況把握	URLアクセスに該当するデータを分析します。	URL	・ アプリケーション名 ・ URL ・ ウィンドウタイトル ・ 発生日時
2	URL付きウィンドウタイトル取得(サイト別)の状況把握	サイト別に該当するデータを分析します。	URL	・ アプリケーション名 ・ URL ・ ウィンドウタイトル ・ 発生日時

情報漏洩状況を把握する

No.	目的名	内容	キーワード指定対象項目	詳細表示項目
1	ファイル持出しの状況把握	リムーバブルへのファイル持出しに該当するデータを分析します。	元ファイル名	・ 持出し元ファイル名 ・ 持出し先ファイル名 ・ 先ドライブ種別 ・ 持出種別 ・ 発生日時
2	ファイル操作の状況把握	複写先/移動先または作成元/更新元がリムーバブルのファイルアクセスに該当するデータを分析します。	ファイル名	・ 操作種別 ・ 元ファイル名 ・ 元ドライブ種別 ・ 先ファイル名 ・ 先ドライブ種別 ・ アプリケーション名 ・ 発生日時
3	印刷操作(回数)の状況把握	印刷操作に該当するデータを分析します。	印刷ファイル名	・ 印刷ファイル名 ・ ページ数 ・ プリンタ名 ・ 発生日時
4	印刷操作(ページ数)の状況把握	印刷ページ数に該当するデータを分析します。	印刷ファイル名	・ ページ数 ・ 印刷ファイル名 ・ 発生日時
5	宛先別メール送信の状況把握	宛先別メール送信に該当するデータを分析します。	添付ファイル名	・ 件名 ・ From ・ To/CC/BCC ・ 添付

No.	目的名	内容	キーワード指定対象項目	詳細表示項目
				・ 発生日時

付録B 複合機と連携して情報を可視化する

複合機から採取された情報を利用して、紙の使用量やCO2排出量の換算結果を、レポートとして出力します。

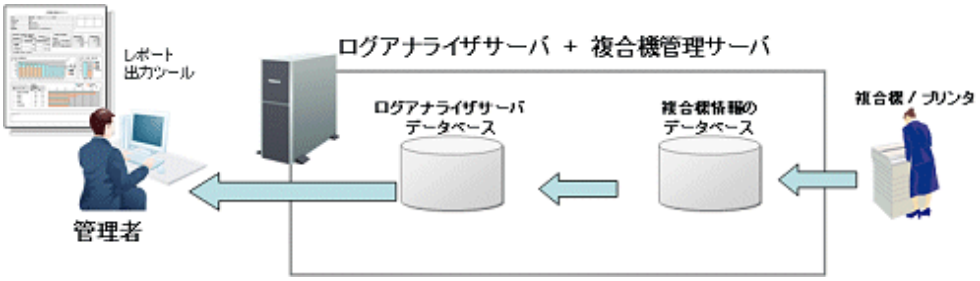
複合機ごとの紙の使用量をレポート化し、実績値の推移をみえる化することにより、無駄な印刷を抑止し、印刷コスト・CO2削減に貢献します。

また、複合機の使用状況も出力されるため、複合機の削減や維持費の安価な低機能モデルへの変更など、運営コスト削減のための判断材料としても役立ちます。

サポート対象の複合機/プリンタの詳細は、ソフトウェア説明書に記載のプリンタベンダまでお問合せください。

B.1 運用パターン

複合機から、ソフトウェア説明書に記載のプリンタベンダが提供するソフトウェアをベースにした複合機管理サーバを介してログアナライザサーバへ定期的にログを取り込みます。



複合機管理サーバとログアナライザサーバは、同じサーバ上にインストールします。

複合機管理サーバ上の複合機情報のデータベースにある集計結果を、ログアナライザサーバのデータベースへ1日1回取り込みます。

システム管理者は、レポート出力ツールがインストールされているPCで、複合機の用紙使用状況レポートを出力します。

注意

取り込み中のエラーについて

ログアナライザサーバのデータベースへの取り込み中にエラーが発生した場合は、イベントログに内容を出力します。原因および対処については、“Systemwalker Desktop Keeper リファレンスマニュアル”の“複合機のログ集計時に出力されるメッセージ”を参照してください。

B.2 動作環境

対応ハードウェア/必須ソフトウエア

- OS : Windows Server 2008 64ビット版、Windows Server® 2008 R2
- その他、対応ハードウェア/必須ソフトウェアは、ソフトウェア説明書に記載のプリンタベンダまでお問合せください。

B.3　制限事項・注意事項

- ログアナライザサーバにて、複合機管理サーバ上のジョブログを集計した後で、その時の集計期間のジョブログが複合機管理サーバに遅れて登録された場合、そのログは集計対象にはなりません。
- レポートに出力される用紙代は、対象期間の総使用枚数に1枚あたりの用紙代を掛けて算出したものです。そのため目安の値とはなりますが、正確な用紙代を表したものではありません。
- レポートに出力されるCO2排出量は、対象期間の総使用枚数をA4サイズに換算したものに1枚あたりのCO2排出量を掛けて算出したものです。そのため目安の値とはなりますが、正確なCO2排出量を表したものではありません。

B.4　導入

ログアナライザサーバが構築されていることを確認する

Systemwalker Desktop Keeperログアナライザサーバが構築されていることが必要です。ログアナライザサーバの構築方法は、“Systemwalker Desktop Keeper 導入ガイド”の“ログアナライザサーバを構築する”を参照してください。

レポート出力ツールの環境が構築されていることを確認する

レポートを出力するシステム管理者のPCに、レポート出力ツールがインストールされていて、サーバ設定およびバッチユーザー設定が行われていることが必要です。
構築方法は、“Systemwalker Desktop Keeper 導入ガイド”の“レポート出力の環境を構築する”を参照してください。

複合機管理サーバの環境を構築する

複合機管理サーバは、ログアナライザサーバがインストールされているコンピュータにインストールします。
構築方法は、ソフトウェア説明書に記載のプリンタベンダまでお問合せください。

B.5　使用方法

B.5.1　用紙代・CO2排出量の算出に必要な係数を設定する

用紙代やCO2排出量の算出に必要となる係数は、Webコンソールのログアナライザ動作設定[エコ監査設定]の「年度開始月設定」「1ページ(または1枚)あたりの用紙代」「1ページ(または1枚)あたりのCO2排出量」で設定します。詳細は、“2.8.2.2.4 その他の条件を設定する”を参照してください。

「年度開始月設定」には、基準とする年度開始月を設定してください。

「1ページ(または1枚)あたりの用紙代」には、1枚あたりの平均用紙代を設定してください。

「1ページ(または1枚)あたりのCO2排出量」には、A4サイズ用紙1枚あたりのCO2排出量を設定してください。

B.5.2　複合機の用紙使用状況レポートを出力する

用紙使用状況レポートの出力方法には、以下の2種類があります。システム管理者だけ、実行できます。

- レポート出力ツールで出力する
- DTLA_REPORT_BATCH.EXE (レポート出力)コマンドで出力する

レポート出力ツールで出力する

1. Administrator または Domain Admins グループに属するWindowsアカウントで、Windowsにログオンします。

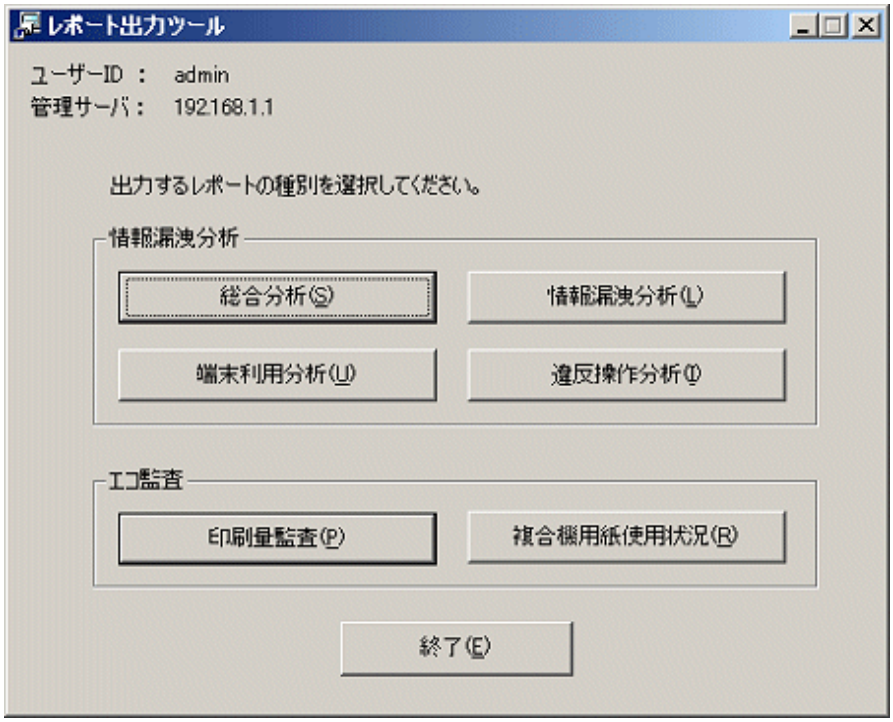
2. スタートメニューから[プログラム]-[Systemwalker Desktop Keeper]-[ログアナライザ]-[レポート出力ツール]を選択します。
   →ログイン画面が表示されます。

項目名	説明
[管理サーバIPアドレス]	統合管理サーバまたは管理サーバのIPアドレスを指定します。 15文字までのIPアドレス形式の文字列を入力します。 一度認証されたIPアドレスは、10件まで記録されます。次回からは、ログイン画面で、プルダウンメニューから選択できます。
[ユーザーID]	システム管理者のユーザーIDです。
[パスワード]	[ユーザーID]に入力したユーザーIDのパスワードを指定します。

認証では、管理サーバからログアナライザサーバに移入された情報を使用しています。管理サーバで変更された認証情報は、ログアナライザサーバにすぐには反映されません(次回、管理情報やログが移入されたタイミングで反映されます)。したがって、変更後の認証情報が管理サーバからログアナライザサーバに移入されるまでは、変更前の認証情報でログインしてください。

3. 必要な情報を入力し、[ログイン]ボタンをクリックします。

→以下の画面が表示されます。



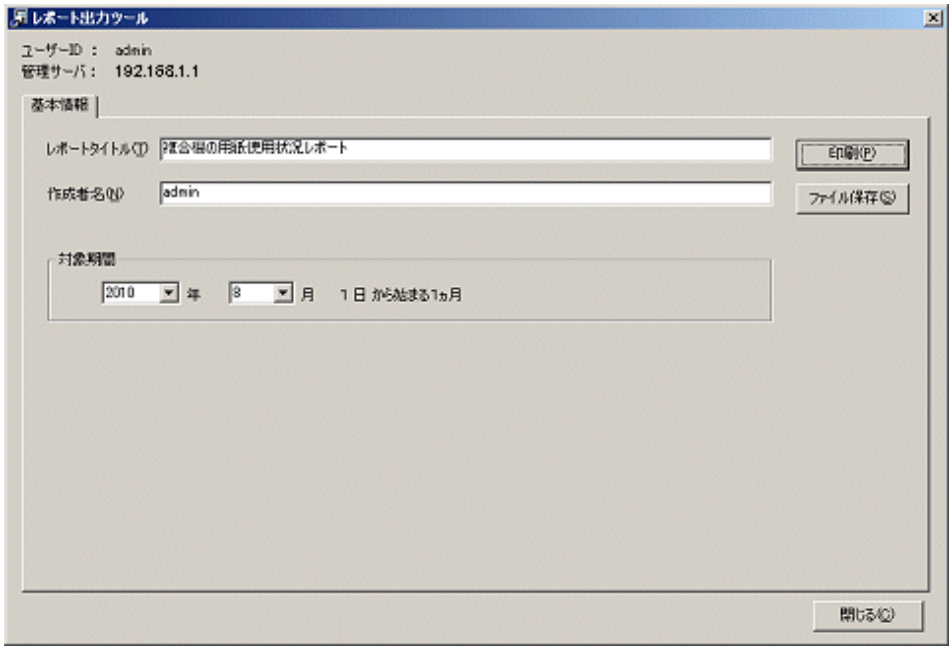
※) 複合機管理サーバの環境がインストールされていない場合、レポート出力ツール画面の[複合機用紙使用状況]のボタンは、グレーアウトされます。

― ユーザーID:ログインしているユーザーIDです。

― 管理サーバ:ログインしているユーザーの管理者情報が格納されている管理サーバのIPアドレスです。

4. [複合機用紙使用状況]を選択します。

→以下の画面が表示されます。



― ユーザーID:ログインしているユーザーIDです。

ー 管理サーバ:ログインしているユーザーの管理者情報が格納されている管理サーバのIPアドレスです。

5. [基本情報]タブの項目を設定します。
タブの設定内容は、[印刷]または[ファイル保存]を行った場合は、ログインしているユーザー固有の情報として、ログアナライザサーバに保存されます。次回起動時に、保存されている情報が表示されます。

以下の項目を設定します。

入力項目	内容
[レポートタイトル]	出力するレポートのタイトルを指定します。 半角の英数字、半角の記号、および全角2バイト文字を合わせて、64バイトまで設定できます。 初期値は“複合機の用紙使用状況レポート”です。
[作成者名]	レポートの作成者を指定します。 半角の英数字、半角の記号、および全角2バイト文字を合わせて、40バイトまで設定できます。 初期値はログイン中のユーザーIDです。
[対象期間]	出力するレポートの集計期間を設定します。 集計期間は、2005年1月～すでに完了している最も直近の月度・年度の中から選択可能です。

6. [印刷]または[ファイル保存]ボタンをクリックします。

注意

レポート出力中は、Microsoft® Excelを操作しないでください

レポート出力中は、Microsoft® Excelファイルの[新規作成]や[開く]操作を行わないでください。レポート出力が正常に行われない場合があります。

また、レポート出力前に、Microsoft® Excelが正しく起動することを確認してください。Microsoft® Excelが正しく起動しない場合は、レポート出力処理が長時間たっても終了しないなど、不具合が発生するときがあります。

【[印刷]ボタンをクリックした場合】

生成したレポートを印刷します。

[印刷]画面が表示されますので、プリンタへの印刷設定を行い、レポートを印刷します。

ポイント

印刷ダイアログがレポート出力ツールの後ろに隠れている場合があります。

長時間たっても印刷ダイアログが表示されない場合は、印刷ダイアログがレポート出力ツールの後ろに隠れている可能性があります。

【[ファイル保存]ボタンをクリックした場合】

生成したレポートをファイルに保存します。

注意

出力したレポートは、安全なところに保存してください

出力したレポートには、個人情報やシステム構成情報が含まれる場合があります。ファイルの保存先は、十分なセキュリティ対策が施されたフォルダを指定してください。

【例】
フォルダのアクセス権を、管理者以外のユーザーが参照できないように設定する

保存画面が表示されますので、保存先を指定して、[保存]ボタンをクリックします。

ファイルは、以下の名称で保存されます。

デフォルト名：PrinterPaper_monthly_YYYYMMDD.xls (月報レポート)
(同名ファイルが存在する場合は、上書き確認ダイアログが表示されます。)

－ レポート開始日：YYYYMMDD([基本情報]タブの[対象期間]で設定した日付)

DTLA_REPORT_BATCH.EXE (レポート出力)コマンドで出力する

以下のコマンドを実行します。

```
DTLA_report_batch.exe -t printer -s monthly -f [出力フォルダパス]
```

[出力フォルダパス]：レポートを出力するパスを指定します。

コマンド格納場所、注意事項などは、“Systemwalker Desktop Keeper リファレンスマニュアル”の“DTLA_REPORT_BATCH.EXE (レポート出力)”を参照してください。

- レポートは、システム管理者が、最後にレポート出力ツールで出力したときの設定内容で出力されます。
- レポートのファイル名は、レポート出力ツールで出力したときの名称と同一です。
- 対象期間は、月報、年度実績共に、直近の開始日が自動選択されます。

B.5.3 複合機の用紙使用状況レポートの内容

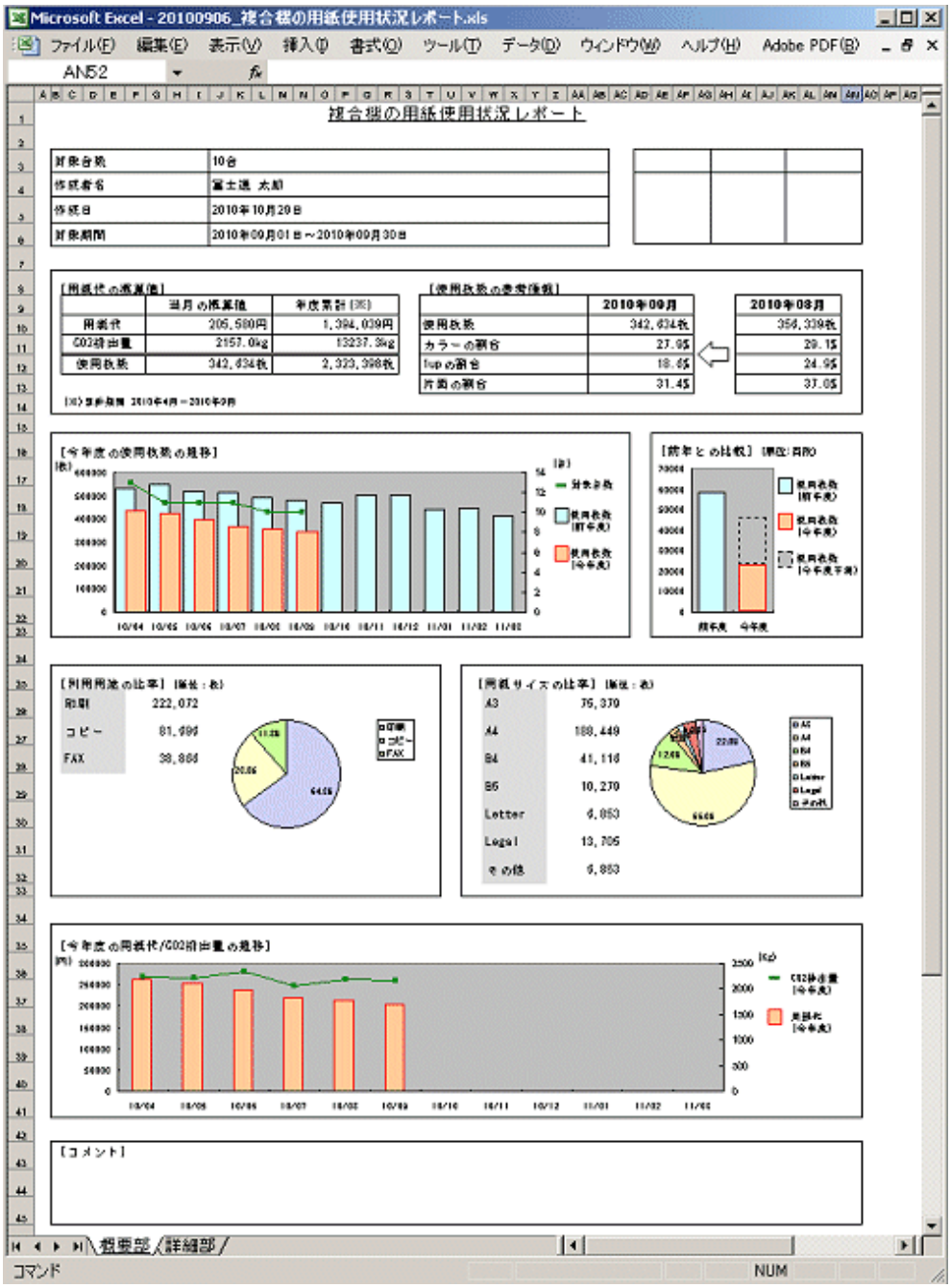
複合機の用紙使用状況レポートの構成は以下のとおりです。

シート名	説明
概要部	対象月に対し、使用枚数を印刷コスト・CO2排出量の観点で出力します。
詳細部	対象月に対し、複合機単位で、用紙の使用量の内訳を出力します。

生成したレポートファイルや印刷結果のレイアウトは、使用しているMicrosoft® Excelのバージョンやサービスパックによって異なる場合があります。
レポートに出力される各値については、特に断りがない限り表示桁数以下を四捨五入して表示します。またデータが存在しない場合は0と表示します。
レポートに出力される値のうち、年度の概念を含むものについては、対象月以降のデータは集計値に含まれません。またレポート上にも表示されません。

本レポートの説明にある、「年度(年度開始月)」「1枚あたりの用紙代」「1枚あたりのCO2排出量」については、それぞれWebコンソールのログアナライザ動作設定[エコ監査設定]の「年度開始月設定」「1ページ(または1枚)あたりの用紙代」「1ページ(または1枚)あたりのCO2排出量」が使用されます。これらの値を変更する場合は、Webコンソールの設定を変更してください。詳細は“2.8.2.2.4 その他の条件を設定する”を参照してください。

概要部



(1) レポートタイトル

レポート出力ツールで指定したレポートタイトルが表示されます。

(2) 対象台数

連携している複合機の台数を表示します。対象となる複合機がない場合は、0台と表示します。

(3) 作成者名

レポート出力ツールで指定した作成者名が表示されます。

(4) 作成日

レポートを出力した日付が表示されます。

(5) 対象期間

レポート出力ツールで指定した対象期間が表示されます。

(6) 捺印欄

作成したファイルに捺印をするための領域です。必ず出力されます。

(7) 用紙代の概算値

当月・年度累計の用紙代・CO2排出量の概算値について表示します。

・「(※)累計期間」には、対象期間に対応した期間が表示されます。

・ 用紙代は以下の計算式で求めます。
用紙代＝1枚あたりの用紙代×当月の用紙使用枚数

・ CO2排出量は以下の計算式で求めます。
CO2排出量＝1枚あたりのCO2排出量×(A3用紙使用枚数×2+A4用紙使用枚数+B4用紙使用枚数×1.5+B5用紙使用枚数×0.75+Letter用紙使用枚数×0.97+Legal用紙使用枚数×1.23+その他サイズ用紙のA4換算枚数※)
※) 一部のその他サイズ用紙については、A4換算枚数に含まれない場合があります。

(8) 今年度の使用枚数の推移

今年度の使用枚数および複合機台数の推移をグラフ出力します。

・ 使用枚数については前年度の使用枚数データがあれば、あわせて表示します。

・ 横軸は年度固定(年度開始月～年度終了月)です。

(9) 使用枚数の参考情報

以下のデータについて、前月と今月の情報を表示します。

1)使用枚数
2)カラーの割合
3)1upの割合
4)片面の割合

(10) 前年との比較

使用枚数について、前年度と今年度の実績、予測をグラフ表示します。

・ 予測値については、今年度の実績を月平均し、その月平均を残りの月数で掛けた値となります。

(11) 利用用途の比率

以下の複合機の利用用途別に使用枚数とその割合をグラフ表示します。

1)印刷
2)コピー
3)FAX

・ 各用途の表示順序は枚数・割合の大小に関わらず固定です。

(12) 用紙サイズの比率

以下の複合機用紙サイズ別に使用枚数とその割合をグラフ表示します。

1)A3
2)A4
3)B4
4)B5
5)Letter
6)Legal
7)その他

・ 各用紙サイズ用途の表示順序は枚数・割合の大小に関わらず固定です。

(13) 今年度の用紙代／CO2排出量の推移

今年度の用紙代およびCO2排出量の推移をグラフ出力します。

・ 用紙代およびCO2排出量の計算式は、(7) 用紙代の概算値 で記載している計算式と同様です。

・ 横軸は年度固定(年度開始月～年度終了月)です。

(14) コメント

ユーザーの自由コメント欄です。

詳細部

(1) レポートタイトル

レポート出力ツールで指定したレポートタイトルが表示されます。

(2) [△]

複合機の使用状態を示します。
△:使用枚数が0の複合機を示します。

(3) No.

通し番号です。

(4) IPアドレス/ホスト名

複合機を一意に識別するためのホスト名またはIPアドレスです。ホスト名が優先して表示されます。

(5) メーカ名

複合機のメーカ名です。

(6) モデル名

複合機のモデル名です。

(7) シリアル番号

複合機のシリアル番号です。

(8) 使用枚数

複合機用紙の使用枚数です。0の場合、赤太字で表示されます。

(9) 印刷枚数

複合機用紙の使用枚数のうち、印刷に使用した枚数です。

(10) コピー枚数

複合機用紙の使用枚数のうち、コピーに使用した枚数です。

(11) FAX枚数

複合機用紙の使用枚数のうち、FAXに使用した枚数です。

(12) カラー枚数

複合機用紙の使用枚数のうち、カラーで使用した枚数です。

(13) 1up枚数

複合機用紙の使用枚数のうち、1upで使用した枚数です。

(14) 片面枚数

複合機用紙の使用枚数のうち、片面で使用した枚数です。

索 引

[数字]

3階層のシステム構成....340

[A]

Active Directory....101,131
Active Directory連携....330,331

[C]

CD/DVDメディアの留意点....16
Citrix XenApp....26
CSVファイル....127
CT環境....356
CTグループ....117
CTグループの部門管理者情報....130
CTグループポリシー....188
CT情報/ユーザー情報....181
CT情報/ユーザー情報を出力....208
CT操作ログ画面....254
CT動作パラメーター情報ファイル....362
CTポリシー/ユーザーポリシーを変更....201
CTポリシーを変更....201
CTリスト....55
CTを追加/移動/削除....193

[F]

FTPサーバ接続禁止....20,422
[FTPサーバ接続禁止]タブ....92
FTP操作禁止ログ....450
FTP操作ログ....27,449

[P]

PrintScreenキー禁止....418
PrintScreenキー禁止ログ....446
PrintScreenキー操作ログ....26,445

[S]

Systemwalker Desktop Patrol....108
Systemwalker Desktop Patrol構成情報取り込みコマンド....108
Systemwalker Desktop Rights Masterとの混在運用....15

[U]

URLアクセス禁止....20,420
[URLアクセス禁止]タブ....91
USBデバイス情報....353
USBデバイスを登録....347

[V]

V12.0L20～V13.0.0互換方式....17
V13.2.0方式(ポート監視方式)....19

[W]

WEBアクセス状況....465
Webコンソールの使用条件....226
Web操作禁止ログ....448
Web操作ログ....27,447
Webダウンロード禁止....21,424
[Webダウンロード禁止]タブ....93

[あ]

扱う文字コード....4
アプリケーション起動禁止....17,414
アプリケーション起動禁止タブ....76
アプリケーション起動禁止ログ....430
アプリケーション起動ログ....429
アプリケーション終了ログ....429
アプリケーションメール状況....464
暗号ファイル....14
暗号ファイルの作成....13
暗号ファイルの復号....13
一元管理に変更....333
一括割り当て....127
違反操作状況....462
違反操作分析レポート....302,305
違反操作ワーストランキング....235
印刷監視方式....364
印刷禁止....17,410
印刷禁止タブ....73
印刷禁止ログ....441
印刷操作状況....464
印刷操作ログ....22,440
印刷量監査レポート....312,313,316
ウィンドウタイトル取得ログ....24,431
運用環境....32
運用環境を整えるときに考慮すること....32
運用環境を整える流れ....49
運用環境を変更....330
運用の流れ....1
運用をはじめる前に....1
エコ監視設定タブ....90

[か]

概要シート....293
各管理サーバでの管理....334
各種ログスイッチタブ....63
過去の日付け....235
画面キャプチャ....30
画面キャプチャ条件タブ....88
監査資料を作成....284
管理(統合管理)サーバ....9
管理コンソール....117,130,181
管理コンソール環境....365
管理コンソールでの手動作成....330
管理コンソールを起動....52
管理サーバ/統合管理サーバのIPアドレス/コンピュータ名の変更....371
管理サーバ環境....367
管理サーバサービス....397
管理サーバの通信情報....394
管理サーバのデータベース....397
管理サーバを追加/削除....340
管理者通知....370
管理情報....398
既存の管理サーバを統合管理サーバに変更....338

機能全般.....2
機能に関する留意事項.....2
記録機能のポリシーの設定.....426
禁止機能のポリシーの設定.....406
禁止できる操作.....406
クライアント(CT)操作の傾向.....219
クライアント(CT)のサービスを制御.....213
クライアント(CT)の調査用ログ.....31
クライアント(CT)の動作設定.....361
クライアント(CT)の導入.....9
クライアント(CT)のプロセスを制御.....215
クライアント(CT)を制御.....213
グループポリシー.....187
件数の内訳.....232
件数をグラフ表示.....231
公開アプリケーション起動前の操作.....132
公開アプリケーション終了後の操作.....138
構成情報ツリー.....101
構成情報の取り込み方.....330
コマンドプロンプト操作ログ.....25,437

[さ]

採取できる操作ログ.....426
サーバ設定ツール.....367
サービス.....214
サービス一覧.....213
システム構成を2階層から3階層へ.....334
指定したUSBデバイス.....345
絞込条件.....172
集計.....236
集計結果.....235,241
集計条件/レポート出力条件.....168
集計対象から除外する項目.....174
集計目的一覧.....462
詳細結果.....241
詳細シート.....295
使用できる環境.....285
使用できる人.....285
情報漏洩状況.....465
情報漏洩のリスク.....230
情報漏洩分析レポート.....287,292
使用を許可するUSBデバイス.....351
初期管理者のパスワード.....370
接続先の管理サーバ.....356
設定できるポリシー.....406
設定変更ログ.....428,461
設定変更ログ一覧.....271
設定変更ログ画面.....267
総合診断シート.....310
総合分析レポート.....306,308
操作別集計結果.....231
その他設定タブ.....94
その他の条件を設定.....176

[た]

対象グループシート.....297,312
端末初期設定.....62
端末動作設定.....96
端末動作設定画面.....363
端末利用分析レポート.....298,301
追跡対象ファイル.....279
デバイス構成変更ログ.....26,438
転送スケジュール.....146
データベース.....156
データベースを再構築.....398
統合管理サーバ.....356
統合管理サーバを新規に追加.....335
登録されているUSBデバイス情報.....352
登録方法.....157
取り込み方法.....330
取り込みを解除.....331

[は]

ファイル操作拡張子タブ.....82
ファイル操作状況.....462
ファイル操作の追跡結果.....279
ファイル操作プロセスタブ.....78
ファイル操作ログ.....28,451
ファイル操作を追跡.....272
ファイル追跡.....279
ファイル追跡機能.....31
ファイル持出し.....10
ファイル持出し禁止.....15,406
ファイル持出し禁止タブ.....66
ファイル持出し状況.....462
ファイル持出しログ.....21,443
ファイル読み込み禁止.....409
部門管理者.....124
部門管理者情報.....130
プログラムの追加と削除.....364
プロセス.....216
プロセス一覧.....215
保存先フォルダ.....396
ポリシー.....32
ポリシー適用.....41
ポリシーの初期値を設定.....62
ポリシーの設定.....427
ポリシーを設定.....181

[ま]

メール制御方式.....364
メール送信タブの設定.....83
メール送信中止ログ.....435
メール送信ログ.....24,433
メールソフトへの自動添付.....14
メール添付禁止.....17,416
メール添付禁止ログ.....436
目的別に集計.....235
持出しユーティリティ.....10

[や]

ユーザーグループ.....121
ユーザーグループポリシー.....190
ユーザー情報の管理方法.....332
ユーザーポリシーの一元管理.....9
ユーザーポリシーを変更.....205

ユーザーを更新/移動/削除.....199
ユーザーを登録.....196

[ら]

ランキング表示数.....171
レポート出力スケジュール.....324
レポート出力ツールとは.....284
レポート出力ツールの活用方法.....284
レポート出力ツールを起動.....286
連携アプリケーションログ.....460
ログアナライザ.....168,226
ログアナライザサーバ.....156,403
ログアナライザサーバ環境.....403
ログアナライザサーバのIPアドレスポート番号.....404
ログアナライザを起動.....227
ログオン/ログオフログ.....30
ログオン禁止.....412
ログオン禁止タブ.....74
ログオンスクリプト.....131
ログオン禁止ログ.....442
ログオン/ログオフログ.....456
ログ取得期間.....145
ログ情報.....398
ログ全体.....21
ログの参照.....427,428
ログの転送.....144
ログの保存期間.....355
ログビューア.....31
ログビューアでCT情報を検索.....280
ログビューアでクライアント(CT)での操作を監査.....242
ログビューアを起動.....242
ログフィルタ条件タブ.....86
ログを参照.....250
ロック機能.....16