****
**   **
**   Syswtemwalker XSCF監査ログ管理ツール 説明書(readme)   **
**   **
****

■商標について
Microsoft、Windows、Windows NT、Windows Serverは、米国Microsoft Corporation
の米国およびその他の国における登録商標です。
UNIXは、X/Openカンパニーリミテッドが独占的にライセンスしている米国ならびに
他の国における登録商標です。
Systemwalkerは、富士通株式会社の登録商標です。
Oracle SolarisはSolaris, Solaris Operating System, Solaris OSと記載すること
があります。
OracleとJavaは、Oracle Corporationおよびその子会社、関連会社の米国およびその
他の国における登録商標です。
すべてのSPARC商標は、米国SPARC International, Inc.のライセンスを受けて使用して
いる同社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。
Linuxは、Linus Torvalds氏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。
Red Hat、RPMおよびRed Hatをベースとしたすべての商標とロゴは、Red Hat, Inc.
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。

その他、本書に記載されている社名、商品名等は各社の商標または登録商標である場合
があります。
本文中の記載内容は予告なしに変更される場合があります。
また、Systemwalker Centric Managerのエディションで、Standard Editionを"SE"、
Enterprise Editionを"EE"、Global Enterprise Editionを"GEE"と略しています。

■本書の構成

---

1. XSCF監査ログ管理ツールの使用条件
本ツールのご使用にあたっては、下記の使用条件をお守りください。
・XSCF監査ログ管理ツールの再配付はできません。
・XSCF監査ログ管理ツールの利用により損害が発生した場合、弊社は損害賠償等の
責任を負いません。

2. XSCF監査ログ管理ツールの概要
2.1 機能概要
Systemwalker Centric Manager において、
以下のXSCFログの収集・検索を可能にします。
- auditログ: 認証や操作の記録。

- monitorログ: システムの各種動作。イベントのメッセージ。

・運用管理サーバに以下の機能を提供します。(注1)
- XSCFログの管理機能
- XSCFログの検索機能

・Solarisの部門管理サーバおよび業務サーバに以下の機能を提供します。
- XSCFログの収集機能

注1)Windows/Solaris/Linuxが対象となります。
Solaris版運用管理サーバには、XSCFログの収集機能も提供します。

2.2 システム構成

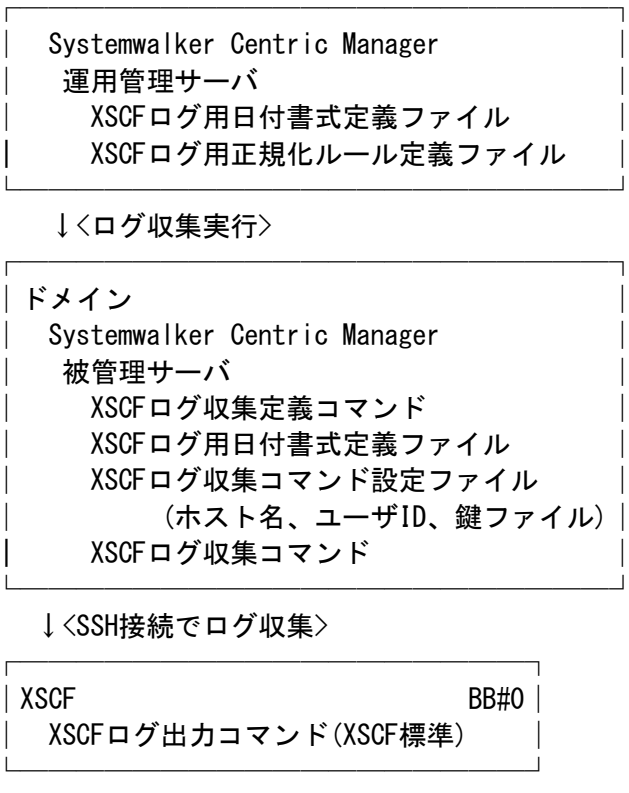
XSCF監査ログ管理ツールは以下で構成されています。

運用管理サーバ
- XSCFログ正規化ルール定義ファイル
- XSCFログ用日付書式定義ファイル

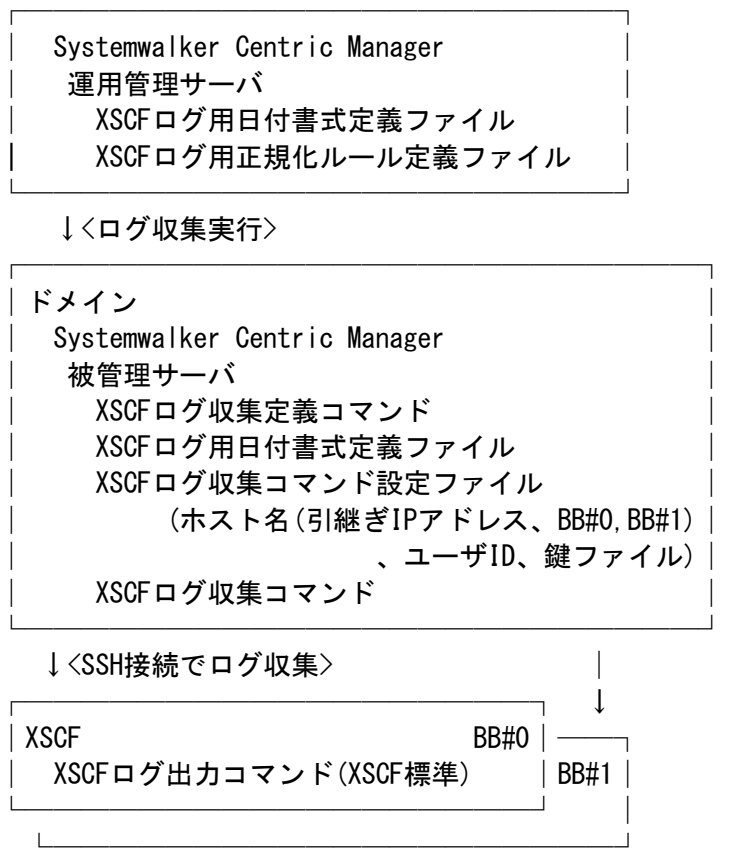
被管理サーバ(運用管理サーバ、部門管理サーバ、業務サーバ)
- XSCFログ用日付書式定義ファイル
- XSCFログ収集定義コマンド
- XSCFログ収集コマンド
- XSCFログ収集コマンド設定ファイル

XSCF監査ログ管理ツールを利用する際のシステム構成の例を以下に示します。

(例) XSCFのビルディングブロック(以下BB)構成が1BBの場合



(例) XSCFのBB構成が2BBの場合



2.3 留意事項

・Administratorユーザまたはrootで作業を実施する必要があります。
・XSCFのBB構成が2BB以上の場合、auditログの収集設定を2つ設定する必要があります。
・XSCFとドメインOSはネットワーク接続可能な状態である必要があります。
・ドメインOSと運用管理サーバはネットワーク接続可能な状態である必要があります。
※XSCFと運用管理サーバは直接ネットワーク接続可能である必要はありません。

3. XSCF監査ログ管理ツールの適用条件

(1) 本ツールの対象バージョン・レベル

・Windows版
Systemwalker Centric Manager SE/EE V15.0.0～V15.1.0
・Solaris版
Systemwalker Centric Manager SE/EE/GEE V15.0.0～V15.1.1
・Linux版
Systemwalker Centric Manager SE/EE/GEE V15.0.0～V15.1.0

(2) 本ツールの容量・インストール先について

本ツールのダウンロードしたファイルは圧縮データとなって
います。インストール前に解凍が必要です。必要なディスク容量は
以下の通りです。

インストール時に必要な作業ディスク容量:
100KB

インストール先の必要ディスク容量:

Windows版	Systemwalkerインストールディレクトリ		25KB
Solaris版	運用管理サーバ	/opt	25KB
		/etc	25MB
Solaris版	部門管理サーバ・業務サーバ	/opt	25KB
		/etc	25KB
Linux版		/opt	25KB
		/etc	25KB

4. XSCF監査ログ管理ツールの導入

(1) インストール前の準備

XSCF監査ログ管理ツールをインストールする前に、以下の製品の
インストールおよび環境構築が完了している場合があります。

・Systemwalker Centric Managerの運用管理サーバ
・Systemwalker Centric Managerの部門管理サーバまたは業務サーバ(注)

注) 運用管理サーバがSolaris版の場合、かつ、XSCFにネットワーク接続する
ドメインOSに運用管理サーバを構築している場合は不要です。

(2) インストール方法

XSCF監査ログ管理ツールをSystemwalker技術情報ホームページより
ダウンロードし、インストールを行います。

- Windows版 の場合

①sw_xscflogtool_yyyymmdd.exe(自己解凍形式)の実行・解凍
sw_xscflogtool_yyyymmdd.exeを実行・解凍します。
※ yyyymmddは、本ツールの公開日付です。

```
sw_xscflogtool_yyyymmdd.exe
```

②解凍後に作られたフォルダへ移動

```
cd sw_xscflogtool_yyyymmdd
```

③ツールのファイルをコピー

```
xcopy /E mpatm %SWRoot%¥mpwalker.dm¥mpatm
xcopy /E mpata %SWRoot%¥mpwalker.dm¥mpata
```

※ %SWRoot%:Systemwalkerインストールディレクトリ

- Solaris/Linux版 の場合

①sw_xscflogtool_yyyymmdd.tar.gzの解凍
sw_xscflogtool_yyyymmdd.tar.gzを解凍します。
※ yyyymmddは、本ツールの公開日付です。

```
gunzip < sw_xscflogtool_yyyymmdd.tar.gz | tar xvf -
```

②解凍後に作られたディレクトリへ移動

```
cd sw_xscflogtool_yyyymmdd
```

③ツールのファイルをコピー

・Solaris版 運用管理サーバの場合

```
cp -Rp ./FJSVmpata/etc/*  /etc/opt/FJSVmpata/
cp -Rp ./FJSVmpatm/bin/*  /opt/FJSVmpatm/bin/
cp -Rp ./FJSVmpatm/etc/*  /etc/opt/FJSVmpatm/
```

・Solaris版 部門管理サーバまたは業務サーバの場合

```
cp -R ./FJSVmpatm/bin/*  /opt/FJSVmpatm/bin/
cp -R ./FJSVmpatm/etc/*  /etc/opt/FJSVmpatm/
```

・Linux版の場合

```
cp -R ./FJSVmpata/etc/*  /etc/opt/FJSVmpata/
cp -R ./FJSVmpatm/etc/*  /etc/opt/FJSVmpatm/
```

[注意事項]

・運用管理サーバへのインストールは必須です。

・中継サーバの設定を行う場合、運用管理サーバの日付定義ファイルを中継サーバ上にコピーしてください。
日付定義ファイルの格納場所は以下の通りです。

- Windowsの場合
  <Systemwalkerインストールディレクトリ>¥Mpwalker.DM¥mpatm¥fmt¥
  mpatmxscfaudit.fmt
  mpatmxscfmonitor.fmt
- Solaris/Linuxの場合
  /etc/opt/FJSVmpatm/fmt
  mpatmxscfaudit.fmt
  mpatmxscfmonitor.fmt

・クラスタ環境に本ツールをインストールする場合は、下記について留意願います。

- Windowsの場合は、ローカルコンピュータ上のAdministratorユーザでログオンしてください。
- 運用系、待機系それぞれに本ツールをインストールしてください。

(3) XSCFログ収集ツールの初期設定

①被監視サーバ上でパスフレーズ無しのSSH鍵を作成

被監視サーバ上でssh-keygenコマンドでSSH鍵を作成します。
このときパスフレーズには何も入力しないでください。
(例) 鍵ファイルnopass_id_rsaの作成

```
# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
```

```
|                                    /root/nopass_id_rsa <ENTER>  |
|Enter passphrase (empty for no passphrase): <ENTER>              |
|Enter same passphrase again: <ENTER>                             |
|Your identification has been saved in /root/nopass_id_rsa.       |
|Your public key has been saved in /root/nopass_id_rsa.pub.       |
|The key fingerprint is:                                          |
|xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx root@example.com |
```

秘密鍵と公開鍵のペアが作成されたことの確認

```
|# ls /root/nopass_id_rsa*                                        |
|/root/nopass_id_rsa      /root/nopass_id_rsa.pub                 |
```

②XSCF上でXSCFのアカウントを作成

useradm権限のあるユーザでXSCFにログインしてアカウントを作成します。

(例)アカウントcmgruserの作成

```
|XSCF> adduser cmgruser                                           |
|XSCF> setprivileges cmgruser platop auditadm                     |
```

ユーザ権限の確認

```
|XSCF> showuser cmgruser                                          |
|User Name: cmgruser                                              |
|UID: 103                                                         |
|Status: Enabled                                                  |
|Minimum: 0                                                       |
|Maximum: 99999                                                   |
|Warning: 7                                                       |
|Inactive: -1                                                     |
|Last Change: Apr 23, 2015                                        |
|Password Expires: Never                                          |
|Password Inactive: Never                                         |
|Account Expires: Never                                           |
|Privileges: platop                                               |
|            auditadm                                             |
```

③XSCF上で①で作成したSSH公開鍵を登録

XSCFに被監視サーバで作成したSSHの公開鍵(nopass_id_rsa.pub)を登録します。

(例)アカウントcmgruserにSSH公開鍵を登録

```
|XSCF> setssh -c addpubkey -u cmgruser                                    |
|Please input a public key:            (nopass_id_rsa.pubの内容)    |
|ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApAstrGL44rm+GVaadlox/Bo7gfgpP3|
|+bO8O9/wBDno+uvCqHO+OuBk9bex26uAkr2HCjyDeG+q2s4whNkTmT5ObbKpxPQFYV|
|yuYYpYpr48R4dSp5djrSS37kkdD92+yM5UZk1K9MuzMyxZ/LJqDZrqww7xOSL7ZU4a|
|9Pj/KzNysmQNSsquFBKk4d5lwaRsEcON7l2IOeo168uJuJaQyewyfoV76TtpLlE5ai|
```

```
|fHCbzTOYetgYjHmlKXgLZ47qfUfwi2zTbOBUaXsLb+CqN+pLkIPpV4P/YLcA5iuJD4|
|fG/YJJTdmSkoWsI82SlyIYmOWOn9CeqCHLhWZ8CB1u24OcCQ== root@example.co|
|m <Ctrl+D>                                                        |
```

SSH公開鍵が登録されたことの確認

```
|XSCF> showssh -c pubkey -u cmgruser                               |
|Public key:                                                       |
|     1 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApAstrGL44rm+GVaadlox/Bo|
|7gfgpP3+bO8O9/wBDno+uvCqHO+OuBk9bex26uAkr2HCjyDeG+q2s4whNkTmT5ObbK|
|pxPQFYVyuYYpYpr48R4dSp5djrSS37kkdD92+yM5UZk1K9MuzMyxZ/LJqDZrqww7xO|
|SL7ZU4a9Pj/KzNysmQNSsquFBKk4d5lwaRsEcON7l2IOeo168uJuJaQyewyfoV76Tt|
|pLlE5aifHCbzTOYetgYjHmlKXgLZ47qfUfwi2zTbOBUaXsLb+CqN+pLkIPpV4P/YLc|
|A5iuJD4fG/YJJTdmSkoWsI82SlyIYmOWOn9CeqCHLhWZ8CB1u24OcCQ== root@exa|
|mple.com                                                          |
```

④被監視サーバからパスワード入力無しでXSCFに接続できることを確認
（例）xscf.example.comへの接続確認

```
|# ssh -l cmgruser -i /root/nopass_id_rsa xscf.example.com         |
|XSCF>                                                            |
```

2BB以上の構成の場合、引継ぎIPアドレス,BB#0,BB#1の3通りでXSCFに接続できることを確認します。
（例）引継ぎIPアドレス,BB#0,BB#1への接続確認
xscflan0.example.com … 引継ぎIPアドレスまたはホスト名
xscfbb0.example.com … BB#0 IPアドレスまたはホスト名
xscfbb1.example.com … BB#1 IPアドレスまたはホスト名

```
|# ssh -l cmgruser -i /root/nopass_id_rsa xscflan0.example.com     |
|XSCF>                                                            |
```

```
|# ssh -l cmgruser -i /root/nopass_id_rsa xscfbb0.example.com      |
|XSCF>                                                            |
```

```
|# ssh -l cmgruser -i /root/nopass_id_rsa xscfbb1.example.com      |
|XSCF>                                                            |
```

⑤XSCFアクセス情報ファイルの設定
XSCFアクセス情報ファイル(/etc/opt/FJSVmpatm/data/xscfinfo.ini)にXSCFのホスト名、ユーザ名、SSH鍵ファイル名を設定します。

・1BBの場合
XSCFHOST : ログを採取するXSCFのホスト名またはIPアドレス
USER : ログを採取するXSCFにログインするためのユーザ名を指定する
　　指定されたユーザは、少なくとも以下のa)とb)の両方の権限を持つ

a) platadmまたはplatopまたはfieldeng (platop推奨)
b) auditadm

KEYFILE : 上記USERで指定したユーザでXSCFにSSHでログインするための
秘密鍵

(例)

```
XSCFHOST=xscf.example.com
USER=cmgruser
KEYFILE=/root/nopass_id_rsa
```

・2BB以上の場合

XSCFHOSTM: XSCFの引継IPアドレス(またはそれに対応するホスト名)を
指定する
XSCFのlan#0, lan#1のどちらを指定しても良い

XSCFHOST0: 以下のXSCFのIPアドレス(またはそれに対応するホスト名)を
指定する
XB-Boxありの構成の場合XB-Box#80
XB-Boxなしの構成の場合BB#0
XSCFのlan#0, lan#1のどちらを指定しても良い

XSCFHOST1: 以下のXSCFのIPアドレス(またはそれに対応するホスト名)を
指定する
XB-Boxありの構成の場合XB-Box#81
XB-Boxなしの構成の場合BB#1
XSCFのlan#0, lan#1のどちらを指定しても良い

USER : 1BBの場合と同じ
KEYFILE : 1BBの場合と同じ

(例)

```
XSCFHOSTM=xscflan0.example.com
XSCFHOST0=xscfbb0.example.com
XSCFHOST1=xscfbb1.example.com
USER=cmgruser
KEYFILE=/root/nopass_id_rsa
```

(4) XSCFログ収集定義

XSCF監査ログを収集する被管理サーバ上でログ収集定義を実行します。
XSCF監査ログのログ識別名は以下となります。

・auditログ:
- 1BBの場合、または、2BB以上の場合のマスタ
XSCFaudit0
- 2BB以上の場合のスタンバイ
XSCFaudit1

・monitorログ:
XSCFmonitor

①ポリシーファイルの準備

運用管理サーバにおいて、以下に格納されているポリシーファイルのサンプルを

コピーします。
(例)
【Windows】

```
copy %SWRoot%¥mpwalker.dm¥mpatm¥sample¥mpatmxscflogdef.csv
                              <ポリシーファイルの格納ディレクトリ>
```

※ %SWRoot%:Systemwalkerインストールディレクトリ

【Solaris/Linux】

```
cp /etc/opt/FJSVmpatm/sample/mpatmxscflogdef.csv
                              <ポリシーファイルの格納ディレクトリ>
```

[注意事項]
- 必要に応じて、ポリシーファイルの転送情報指定(TRANSDEF)、ログ収集設定指定(LOGDEF)を編集してください。
- 1BBの場合、ログ識別名"XSCFaudit1"の行頭に'#'を記述して、コメント行にしてください。

②日付定義ファイルの準備
ポリシーファイルの格納ディレクトリに、日付定義ファイルをコピーします。
日付定義ファイルの格納場所は以下の通りです。
- Windowsの場合
  <Systemwalkerインストールディレクトリ>¥Mpwalker.DM¥mpatm¥fmt¥
    mpatmxscfaudit.fmt
    mpatmxscfmonitor.fmt
- Solaris/Linuxの場合
  /etc/opt/FJSVmpatm/fmt
    mpatmxscfaudit.fmt
    mpatmxscfmonitor.fmt

③ポリシーの登録
編集したポリシーファイルを使用してポリシーを登録します。
(例)

```
mpatmpset -N <ノード名> -D <ポリシーファイルの格納ディレクトリ>
```

※ 被監視サーバのノード名を指定します。

④ポリシーの配付
[Systemwalkerコンソール]において、③で登録したポリシーを配付します。

⑤mpatmxscflogdef (XSCFログ収集定義コマンド)の実行
被監視サーバにおいて、mpatmxscflogdefコマンドを実行します。

```
# /opt/FJSVmpatm/bin/mpatmxscflogdef
Command is Successful.
```

⑥ログ収集定義の確認
被監視サーバにおいて、mpatmlogapdef(ログ収集設定コマンド)を実行し、
ログ収集定義を確認します。

```
/opt/systemwalker/bin/mpatmlogapdef DISP
```

"APPLICATION NAME"に、設定したXSCFログのログ識別名があることを
確認します。

[注意事項]
・ポリシーを新たに配付した場合、再度mpatmxscflogdefコマンドを実行してください。
・中継サーバを設定する場合、"(2) インストール方法"でコピーした日付定義ファイルを用いて、設定してください。中継サーバの設定方法についての詳細は、「Systemwalker Centric Manager 使用手引書セキュリティ編」を参照してください。

(5) XSCFログの正規化ルールの登録
運用管理サーバ上で、XSCF監査ログの正規化ルール定義ファイル
(mpatarule_XSCFaudit.ini,mpatarule_XSCFmonitor.ini)を登録します。

(例) mpatarulectlコマンドによる正規化ルールの登録

```
mpatarulectl -A mpatarule_XSCFaudit0.ini
```

```
mpatarulectl -A mpatarule_XSCFaudit1.ini (注)
```

```
mpatarulectl -A mpatarule_XSCFmonitor.ini
```

mpatarulectlについての詳細は、「Systemwalker Centric Manager リファレンスマニュアル」を参照してください。

注) 2BB以上の場合のみ

5. 運用
5.1 ログ収集
他の監査ログと同様に、運用管理サーバでmpatmlogコマンドを実行し、ログを収集します。
mpatmlog実行時、ドメイン上のXSCFログ収集コマンドが動作し、XSCF監査ログが収集されます。

(例) mpatmlogコマンドによるXSCFaudit0のログ収集

```
mpatmlog -H <被監視サーバのホスト名> -A XSCFaudit0
```

[注意事項]

・他の監査ログと同様に、cronやタスク等で定期的に監査ログを収集するようにしてください。

mpatmlogについての詳細は、「Systemwalker Centric Manager リファレンスマニュアル」を参照してください。

5.2 ログの正規化

他の監査ログと同様に、運用管理サーバでログ正規化コマンドを実行し、ログを正規化します。

(例) mpatalogcnvtコマンドによるXSCauditの正規化

```
mpatalogcnvt -H <被監視サーバのホスト名> -A XSCFaudit0
```

mpatalogcnvtについての詳細は、「Systemwalker Centric Manager リファレンスマニュアル」を参照してください。

5.3 ログの検索

他の監査ログと同様に、Systemwalkerコンソールの[監査ログ分析－検索]画面でXSCFログの検索をします。

6. XSCF監査ログ管理ツールの削除

XSCF監査ログ管理ツールのアンインストール手順を以下に示します。

(1) 追加した正規化ルールの削除

運用管理サーバにおいて、XSCF監査ログの正規化ルール定義を削除します。

(例)

```
mpatarulectl -D mpatarule_XSCFaudit0.ini
```

```
mpatarulectl -D mpatarule_XSCFaudit1.ini (注)
```

```
mpatarulectl -D mpatarule_XSCFmonitor.ini
```

注) 2BB以上の場合のみ

(2) 追加したログ収集定義の削除

①ポリシーファイルのコピー

運用管理サーバにおいて、以下に格納されているポリシーファイルのサンプルをコピーします。

(例)

【Windows】

```
copy %SWRoot%¥mpwalker.dm¥mpatm¥sample¥mpatmxscflogdef.csv
                                <ポリシーファイルの格納ディレクトリ>
```

【Solaris/Linux】

```
cp /etc/opt/FJSVmpatm/sample/mpatmxscflogdef.csv
                              <ポリシーファイルの格納ディレクトリ>
```

②削除用ポリシーファイルの編集

運用管理サーバにおいて、ポリシーファイルを編集します。

"APDEF"セクションの"ADD"行をコメント行にして、"DEL"行を有効にします。

（例）

```
:
#ADD,XSCFaudit0,～
#ADD,XSCFaudit1,～
#ADD,XSCFmonitor,～
DEL,XSCFaudit0,,,,,,,,
DEL,XSCFaudit1,,,,,,,,
DEL,XSCFmonitor,,,,,,,,
```

[注意事項]

- 必要に応じて、ログ収集設定指定と収集ログ情報指定を編集してください。
- 1BBの場合、ログ識別名"XSCFaudit1"の行をコメント行にしてください。

③ポリシーの登録

編集したポリシーファイルを使用してポリシーを登録します。

（例）

```
mpatmpset -N <ノード名> -D <ポリシーファイルの格納ディレクトリ>
```

※ 被監視サーバのノード名を指定します。

④ポリシーの配付

[Systemwalkerコンソール]において、③で登録したポリシーを配付します。

(3) XSCFログ収集ツールの初期設定の削除

被管理サーバにおいて、インストール時に追加したXSCF接続用の設定が
不要な場合、削除します。

①XSCFのアカウントを削除

XSCF上で、インストール時に追加したアカウントを削除します。

（例）アカウントcmgruserの削除

```
XSCF> deleteuser cmgruser
```

②パスフレーズ無しのSSH鍵を削除

被監視サーバ上で、インストール時に追加したSSH鍵を削除します。

（例）秘密鍵と公開鍵の削除

```
# rm /root/nopass_id_rsa*
```

(4) 導入時にコピーしたファイルの削除

以下が導入時にコピーしたファイルです。

・運用管理サーバ
 - Windowsの場合
  <Systemwalkerインストールディレクトリ>¥mpwalker.dm¥mpata¥etc¥rule¥
                                                mpatarule_XSCFaudit0.ini
                                                mpatarule_XSCFaudit1.ini
                                                mpatarule_XSCFmonitor.ini
  <Systemwalkerインストールディレクトリ>¥mpwalker.dm¥mpatm¥fmt¥
                                                   mpatmxscfaudit.fmt
                                                   mpatmxscfmonitor.fmt
  <Systemwalkerインストールディレクトリ>¥mpwalker.dm¥mpatm¥sample¥
                                                   mpatmxscflog.csv

 (例)

```
DEL c:¥systemwalker¥mpwalker.dm¥mpata¥etc¥rule¥mpatarule_XSCF*
DEL c:¥systemwalker¥mpwalker.dm¥mpatm¥fmt¥mpatmxscf*
DEL c:¥systemwalker¥mpwalker.dm¥mpatm¥sample¥mpatmxscf*
```

 - Solaris/Linuxの場合
  /etc/opt/FJSVmpata/etc/rule
                    mpatarule_XSCFaudit0.ini
                    mpatarule_XSCFaudit1.ini
                    mpatarule_XSCFmonitor.ini
  /etc/opt/FJSVmpatm/fmt
                    mpatmxscfaudit.fmt
                    mpatmxscfmonitor.fmt
 /etc/opt/FJSVmpatm/sample
                    mpatmxscflogdef.csv
  (例)

```
rm -f /etc/opt/FJSVmpata/etc/rule/mpatarule_XSCF*
rm -f /etc/opt/FJSVmpatm/fmt/mpatmxscf*
rm -f /etc/opt/FJSVmpatm/sample/mpatmxscf*
```

・被管理サーバ
 /opt/FJSVmpatm/bin
                getxscflog
                getxscflogaudit0
                getxscflogaudit1
                getxscflogmonitor
                mpatmxscflogdef

 /etc/opt/FJSVmpatm/data
                xscfinfo.ini

 /etc/opt/FJSVmpatm/fmt
                mpatmxscfaudit.fmt
                mpatmxscfmonitor.fmt
 /etc/opt/FJSVmpatm/sample

mpatmxscflogdef.csv

(例)

```
rm -f /opt/FJSVmpatm/bin/getxscflog*
rm -f /opt/FJSVmpatm/bin/mpatmxscflogdef
rm -f /etc/opt/FJSVmpatm/data/xscfinfo.ini
rm -f /etc/opt/FJSVmpatm/fmt/mpatmxscf*
rm -f /etc/opt/FJSVmpatm/sample/mpatmxscf*
```

(5) XSCF監査ログの一時ファイルの削除

以下に格納されいてるXSCFログの一時ファイルを削除します。

```
rm -f /var/opt/FJSVmpatm/tmp/*XSCF*
rm -f /var/opt/FJSVmpatm/tmp/getxscf*
```

[注意事項]

・中継サーバを設定した場合、コピーした日付定義ファイルを削除してください。

7. メッセージ

7.1 XSCFログ収集コマンド異常終了時のメッセージ

以下のメッセージは、mpatmlogコマンド実行時、被管理サーバ上でXSCFログ収集コマンドが異常終了した場合に出力されます。

(例) XSCFaudit0ログ収集時のメッセージ

```
mpatm: エラー: 651: ログ収集は失敗しました。サーバ名＝<被管理サーバのホスト名>、エラー＝mpatm:エラー: 831: コマンドの実行に失敗しました。コマンド名＝/opt/FJSVmpatm/bin/getxscfaudit0 -o ¥"/var/opt/FJSVmpatm/tmp/<運用管理サーバのIPアドレス>_XSCFaudit0.log¥" 2> /var/opt/FJSVmpatm/tmp/<運用管理サーバのIPアドレス>_XSCFaudit0_out.txt、エラー＝1
```

[原因]

XSCFログ収集処理が失敗しました。

[対処]

「mpatm: エラー: 651」メッセージの末尾の「エラー＝」の値に応じて対処を実行してください。

1: XSCFログ収集コマンド設定ファイルが正しく設定されていることを確認してください。
2: "/var/opt"ディレクトリ配下がアクセス可能な状態であること、および、容量不足が発生していないことを確認してください。
3: XSCFにssh接続可能な状態であること、および、XSCFが正常な状態であることを確認してください。

7.2 XSCF監査ログ管理ツールのメッセージ

以下のメッセージは、mpatmxscflogdef実行時に出力されます。

以下に該当しないメッセージが表示された場合は、「Systemwalker Centric Manager メッセージ説明書」を参照してください。

Command is Abnormal End.

[原因]
以下の可能性があります。
- /etc 配下にアクセスできない状態
- /etc が容量不足。

[対処]
- 実行権限およびディスクの状態が正常であることを確認して、再度実行してください

- 以上 -