# 「FUJITSU Hybrid IT Service プレフィックス型インテグレーションサービス セキュリティインテグレーション」ご紹介

富士通株式会社

FUJITSU-RESTRICTED

© 2023 Fujitsu Limited

# 登録商標および免責事項について

FUJITSU

- 商標登録
  - 記載されている会社名、製品名等の固有名詞は各社の商号、登録商標または商標です。
  - その他、本資料に記載されている会社名、システム名、製品名等には必ずしも商標表示を付記しておりません。
- 免責事項
  - このドキュメントは単に情報として提供され、内容は予告なしに変更される場合があります。
  - また、発行元の許可なく、本書の記載内容を複写、転載することを禁止します。
  - このドキュメントに誤りが無いことの保証や、商品性又は特定目的への適合性の黙示的な保証を含め明示的又は黙示的な保証や条件は一切無いものとします。
  - 富士通株式会社は、このドキュメントについていかなる責任も負いません。また、このドキュメントによって直接又は間接にいかなる契約上の義務も負うものではありません。
  - このドキュメントを形式、手段（電子的又は機械的）、目的に関係なく、富士通株式会社の書面による事前の承諾なく、複製又は転載することはできません。



© 2023 Fujitsu Limited

# Agenda

- セキュリティ対策の動向
- サービスの特長
- サービス内容
- サービス適用時の注意事項
- 【参考】各メニュー詳細


© 2023 Fujitsu Limited

# セキュリティ対策の動向


© 2023 Fujitsu Limited

# COVID-19がもたらしたセキュリティへの影響

FUJITSU

## ● デジタル依存の拡大に伴い、サイバー脅威が深刻化

パンデミックによって激化したデジタルシステムへの依存の高まりは、社会を大きく変えた。
この1年半の間に、産業界では急速にデジタル化が進み、労働者は可能なかぎり
リモートワークにシフトし、この変化を促進するプラットフォームやデバイスが急増している。
同時に、サイバーセキュリティの脅威もまた増大している。

2020年にはマルウェアによる攻撃が358%、ランサムウェアによる攻撃が435%増加しており、
それらを効果的に防止または対処するには、社会の能力が追い付いていない。
サイバー脅威アクターに対する参入障壁の低下、より過激な攻撃手法、
**サイバーセキュリティ専門家の不足**、
パッチワークのようなガバナンスの仕組みなど、あらゆる要素がリスクを悪化させる方向に作用している。

グローバルリスク報告書2022年版 P.9　より抜粋
https://www3.weforum.org/docs/WEF_Global_Risks_Report_2022_JP.pdf



© 2023 Fujitsu Limited

# 深刻化するセキュリティ問題への対策における悩み

FUJITSU

- **セキュリティ対策の強化を検討しているが、対応が困難な課題が多い**

セキュリティ対策導入のための
スキル保有者を確保できない

セキュリティ対策の種類が多く、
対策毎に構築作業を
覚えるのが大変

現在の業務システムに
適したセキュリティ対策や、
システム構成がわからない

DX推進にもセキュリティ
対策は避けて通れない

**<u>対策の種類も多く、高度なスキルが必要なセキュリティ設計/構築業務から脱却したい</u>**



© 2023 Fujitsu Limited

# サービスの特長

FUJITSU-RESTRICTED

© 2023 Fujitsu Limited

# セキュリティ対策に対する富士通の考え方

FUJITSU

## セキュリティ対策への期待

**製品選択の自由度の確保** ：クラウド・オンプレ環境問わず各種セキュリティ製品を自由に選択でき、柔軟に組み合わせ、活用できること（※製品順次拡充予定）

**対策の品質担保** ：多様化・複雑化するサイバーセキュリティの脅威に対し、蓄積されたノウハウを活用することで、セキュリティ対策の品質を担保できること

**短納期化と低コストの実現** ：徹底的な標準化により、セキュリティ対策導入のリードタイムを短縮し、低コスト化を実現できること

## 富士通のセキュリティ対策に対する取り組み

セキュリティ対策導入における実践経験から標準化を徹底

最新技術、業界標準に準拠し最新の脅威に対応できる技術の提供

**将来性・柔軟性の担保、IT人材問題の解決、リードタイムの短縮に向け、富士通はプレフィックス型インテグレーションサービスをご提供いたします**



© 2023 Fujitsu Limited

# プレフィックス型インテグレーションサービス（セキュリティインテグレーション） とは

- プレフィックス型インテグレーションサービス（セキュリティインテグレーション）は、多様化・複雑化するセキュリティ対策導入作業をメニュー化し、お客様に選択いただけるようにしたデリバリーサービスです
- 富士通のノウハウと実践知から、設計指針、実現方式、パラメータ、構築テスト手順一式をドキュメント化・コード化し、ベストプラクティスとして型決めしています

**3つの特長により、加速するDXを支えるセキュリティ対策導入を実現**

| | |
|---|---|
| 1 | 共通の設計指針によりセキュリティ製品選択の自由度を確保 |
| 2 | ベストプラクティスと推奨値で安定した品質を担保 |
| 3 | 標準化により構築リードタイムを短縮 |


© 2023 Fujitsu Limited

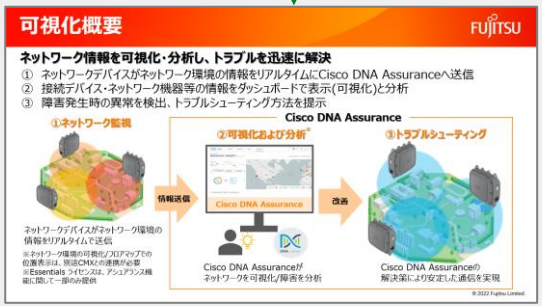
# 共通の設計指針によりセキュリティ製品選択の自由度を確保

- 共通の設計指針を定義することで、各製品の特性に影響されない柔軟なセキュリティ対策導入が可能
- 各種セキュリティ製品の実装方式を提供（※製品順次拡充予定）

## 【共通の設計指針を定義】

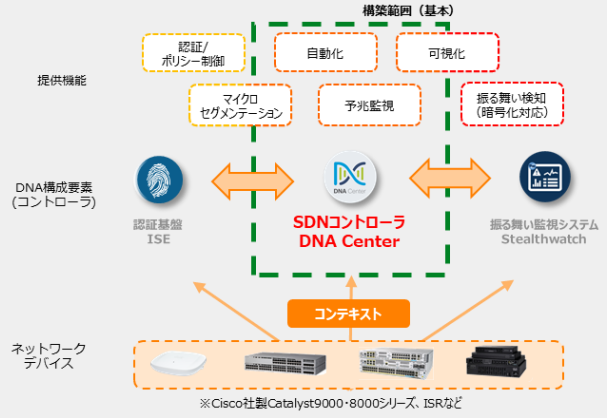
**基本項目**
インフラ機能/信頼性/運用性/セキュリティ/ネットワーク 等

| 機能 | 設計指針 |
|---|---|
| □Inventory<br>□可視化<br>□Plug-and-Play<br>・<br>・ | ・個々デバイスで資産情報管理<br>**・デバイス/クライアント/アプリケーションで可視化を設計**<br>・ゼロタッチコンフィグを設計<br>・<br>・ |




## 【設計指針に基づいた実装方式の提供】

《デバイス/クライアント/アプリケーションで可視化》




| | DNA Center | ISE | Stealthwatch |
|---|---|---|---|
| 利用する可視化 | デバイス/クライアント/アプリケーションを可視化し、ネットワーク異常を検出 | デバイスの認証、ポリシー制御を可視化 | デバイスに対するトラフィックのふるまいを可視化(検知) |

**最新技術に対応した、富士通の実践ノウハウを設計指針・方式としてご提供します**


© 2023 Fujitsu Limited

# ベストプラクティスと推奨値で安定した品質を担保

- 富士通の実践知から導いたベストプラクティスと推奨値を、設計書・パラメータ設定・手順にプリセット
- お客様がITスキルに不安があり、構築要件を全て伝えられなくても、高品質なセキュリティ設計が可能

## 初期設定　例：基本設計の型化

| | | |
|---|---|---|
| 初期設定 | | ■本サービスの環境設計に基づいた初期設定を実施します。<br>・以下の項目を実施します。<br>- Cisco DNA Centerソフトウェアのインストール<br>- アカウント登録<br>- セキュリティ設定<br>- Cisco DNA Centerソフトウェアのアップデートを実施します。 |
| ネットワーク基本設定・フロア設定 | 階層設計(有線機器のみ) | ■本サービスの環境設計に基づき、有線機器を登録するためのエリア・建物・フロアー作成を実施します。 |

目次

はじめに
アプライアンスの設定準備
モニターとアプライアンスの接続方法
Cisco IMC(CIMC)設定
CIMCコンソールにログイン
NTPサーバの設定
初期設定
USBメモリで端とアプライアンスのつなぎ方
KVMの起動方法
インストーラの起動方法
DNACのインストール
アプライアンスに初回ログイン（パスワード変更）
クイックスタートツールの設定
スマートアカウントの登録
ユーザの追加
初期設定のアップデート
ネットワーク基本設定・フロア設定
階層設定
物理機器情報登録
ネットワーク設定
テレメトリー設定
機器登録
現地作業
プロビジョニング
プロビジョニングの確認
設定と必要情報
バックアップ構築
HAの構成
プライマリーノードの設定手順
セカンダリノードの設定手順
バックアップサーバの設定
バックアップファイルの作成
バックアップスケジュールの作成
復元の操作
おわりに

## パラメータ設定　例：インターフェイスとアドレスの設計

### インターフェイスケーブル接続

Ⅰ

2 インタフェースケーブル接続

| | | | | |
|---|---|---|---|---|
| 1) | ネットワークアダプタ 1 | 10 Gbps エンタープライズポート | 必須 | |
| 2) | ネットワークアダプタ 2 | 10 Gbps クラスタ内ポート | 必須 | |
| 3) | ネットワークアダプタ 3 | 1 Gbps または 10 Gbps の管理ポート | 推奨 | Cisco IMC (CIMC)設定, |
| 4) | ネットワークアダプタ 4 | 1 Gbps または 10 Gbps のインターネットポート | 推奨 | USBメモリや端とアプライアンスのつなぎ方 |
| 5) | | 1 Gbps Cisco IMC ポート | 推奨 | |

### IPアドレス設計

Ⅱ

3 必要なアドレス

| | | | | | | |
|---|---|---|---|---|---|---|
| 1) | エンタープライズポートアドレス（Enterprise Port Address） | IPアドレス | | サブネット | 必須 | チェック表B-8, チェック表J-4 |
| 2) | クラスタポートアドレス（Cluster Port Address） | IPアドレス | | サブネット | 必須 | チェック表B-9, チェック表J-5 |
| 3) | 管理ポートアドレス（Management Port Address） | IPアドレス | | サブネット | 推奨 | チェック表B-10, チェック表C-1, チェック表J-6 |
| 4) | インターネットポートアドレス(Internet Port Address ) | IPアドレス | | サブネット | 推奨 | チェック表B-11, チェック表J-7 |
| 5) | CIMC ポートアドレス（CIMC Port Address） | IPアドレス | | サブネット | 推奨 | チェック表A-3 |
| 6) | クラスタ仮想 IP アドレス（Cluster Virtual IP Addresses） | IPアドレス | | サブネット | 必須 | チェック表B-13, チェック表J-8 |
| 7) | デフォルトゲートウェイ IP アドレス（Default Gateway IP Address | IPアドレス | | サブネット | 必須 | チェック表B-8 |
| 8) | DNS サーバの IP アドレス（DNS Server IP Addresses） | IPアドレス | | サブネット | 必須 | チェック表B-10, P-65 |

### バックアップ設計

Ⅲ

5 バックアップの設定情報

| | | | | | | |
|---|---|---|---|---|---|---|
| 1) | バックアップサーバのリモートホストの下記項目 | | | | | |
| | SSH IP | | SSHポート | | サーバ パス | 必須 |
| | ユーザ名 | | パスワード | | | チェック表I-1, チェック表I-2 |
| 2) | Cisco DNA Center(NFS)の下記項目 | | | | | 必須 |
| | ホスト | | サーバパス | | | |

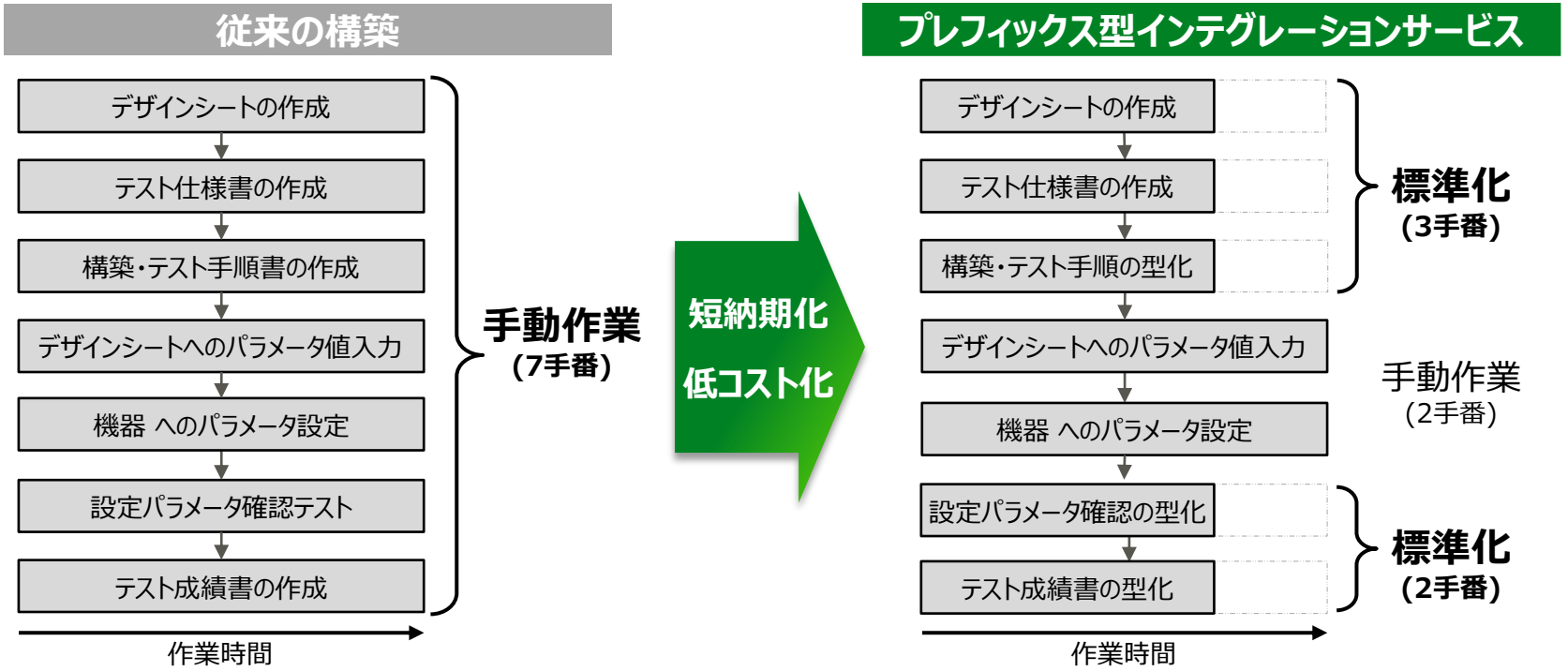
**多様化・複雑化した設計においても、実践に基づいた安定したセキュリティ環境をご提供します**


© 2023 Fujitsu Limited

# 標準化により構築リードタイムを短縮

FUJITSU

- ドキュメントと作業の標準化により、手作業の手番削減と作業時間の短縮を実現




**構築品質は担保したまま、短納期・低コストですぐに使える構築サービスをご提供します**


© 2023 Fujitsu Limited

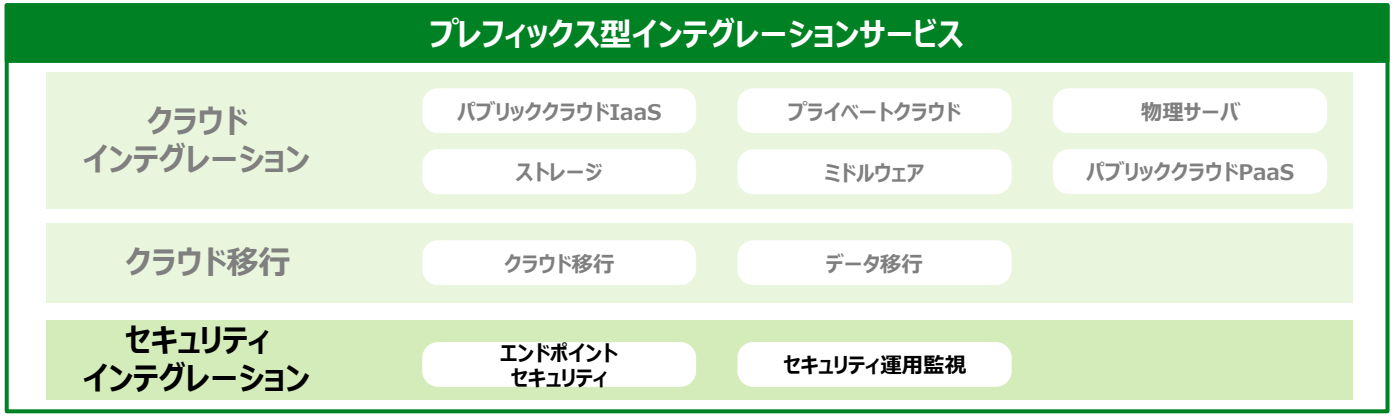
# サービス内容

FUJITSU-RESTRICTED

© 2023 Fujitsu Limited

# セキュリティインテグレーション　サービス体系

- セキュリティインテグレーションは、オンプレ・クラウド問わず必要なセキュリティ対策導入作業をメニュー化
- お客様の重要データに近い「エンドポイントセキュリティ」「セキュリティ運用監視」からサービスをご提供します




※　クラウドインテグレーション/クラウド移行の詳細はクラウドインテグレーション/クラウド移行のご紹介資料にてご確認ください。

- 提供製品（2023年3月時点）

| | |
|---|---|
| **エンドポイントセキュリティ** | PCマルウェア対策（Trellix/FFRI yarai） |
| **セキュリティ運用監視** | 稼働状況可視化（Cisco DNA Center）<br>NW脅威検知・可視化（Vectra AI） |

※詳細やその他製品対応については担当営業にご相談ください。


© 2023 Fujitsu Limited

# お客様の構築要件に応じてメニューをご用意

FUJITSU

- 作業工程の範囲や型決めのレベル別に3段階（Enterprise/Basic/Lite）のメニューを揃えています

※セキュリティインテグレーションは、Basic/Liteのご用意となります

| | Enterprise | Basic | Lite |
|---|---|---|---|
| | 基幹系など、高いセキュリティレベルが要求されるシステムのセキュリティ対策導入を自由度の高いカスタマイズによって実現したい | 細やかな設計は富士通に任せ社内・業務向けのセキュリティ対策導入をスピード感を落とさずに実現したい | 富士通既定のパラメータをフル活用しセキュリティ対策導入を手短に実現したい |
| 方式設計 | 富士通ベストプラクティスに基づく方式説明（規模によるカスタマイズ可能） | 富士通ベストプラクティスに基づく方式説明（ノンカスタマイズ） | – |
| 環境設計 | 富士通標準のデザインシートによる設計<br>設定済み推奨値の柔軟なカスタマイズが可能 | 富士通標準のデザインシート/ヒアリングシートを用いた設計<br>一部項目の変更可能 | 富士通標準のデザインシート/ヒアリングシートを用いた設計<br>最小限の項目のみ変更可能 |
| システム構築 | 環境設計に基づく構築・単体テスト | あらかじめ準備された手順書やテスト仕様書を用いた自動/手動構築・単体テスト | あらかじめ準備された手順書やテスト仕様書を用いた自動/手動構築・単体テスト |
| システム基盤テスト | 方式に基づく、<br>非機能項目の基盤テスト | 方式に基づく、<br>非機能項目（一部）の基盤テスト | – |



© 2023 Fujitsu Limited

# プレフィックス型インテグレーションサービスの構築作業提供範囲

FUJITSU

- 目的に合わせて必要な作業項目の組合せパターンを選択することが可能です
- 「基本」に加えて「オプション」を追加選択することで、お客様の要件に柔軟に対応が可能です

凡例（●：基本(必須)、▲：オプション）

| 作業項目 | Enterprise | Basic | Lite |
|---|---|---|---|
| 方式設計 | ● | ● | |
| 環境設計 | ● | ● | ● |
| 環境設計<br>（オプション） | ▲ | | |
| システム構築 | ● | ● | ● |
| システム構築<br>（オプション） | ▲ | | |
| システム基盤テスト | ● | ● | |


© 2023 Fujitsu Limited

# サービス概要：エンドポイントセキュリティ

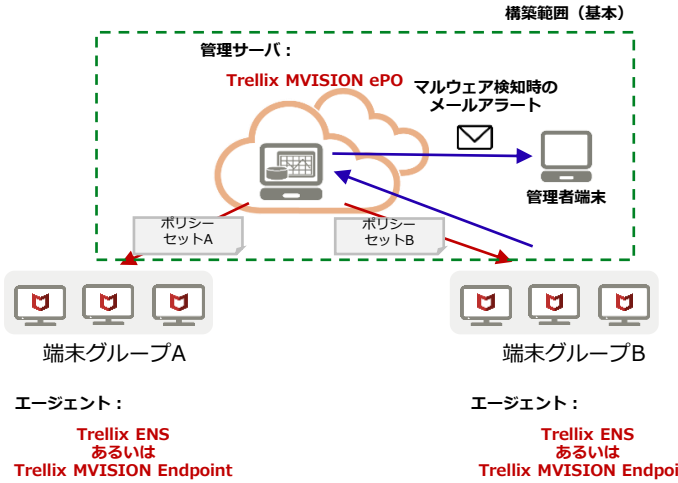
FUJITSU

## ● エンドポイントセキュリティ

**PCマルウェア対策：Trellix**
・クライアント端末を管理対象として、統合的なエンドポイント対策を実現
・MVISION ePO（SaaS）と組み合わせることにより、クライアント端末に設定するセキュリティポリシーを一元管理

対応製品（2022年8月時点）
・Trellix Endpoint Security
・Trellix MVISION Endpoint
・Trellix MVISION ePO

全体構成




■サービス概要
お客様のエンドポイント端末の統合管理を実現するエンドポイントセキュリティ管理基盤の構築を行います。

■作業範囲
- Trellix Endpoint Security のクラウド型管理サーバである MVISION ePOの構築、および管理対象端末グループのクライアントソフトウェア(Trellix ENS, MVISION Endopoint) に配信するポリシーの設定を行います。
- 管理対象端末へのクライアントソフトウェアの展開作業はお客様にて実施をお願いいたします。（オプションで展開作業中のQ&A対応メニューをご用意しています）

■注意事項/前提事項
- お客様拠点での結合テスト実施にあたり、設定ポリシーセット数1個につき1台の動作確認用クライアント端末の準備をお願いいたします。
- 動作確認用クライアント端末と MVISION ePO間の通信が可能な環境をご用意ください。(お客様FWにて通信許可をしていただくなど)

※構築作業提供範囲については、P.24【参考】各メニュー詳細を確認ください

FUJITSU-RESTRICTED



© 2023 Fujitsu Limited

# エンドポイントセキュリティの構築作業提供範囲

FUJITSU

- エンドポイントセキュリティ（PCマルウェア対策：Trellix）におけるBasicメニューの構築作業範囲については以下の通りです

凡例（●：基本(必須)、▲：オプション）

| 作業項目 | | | Basic |
|---|---|---|---|
| エンドポイントセキュリティ | PCマルウェア対策 | 方式設計 | ● |
| | | 環境設計 | ● |
| | | 環境構築/単体テスト | ● |
| | | 結合テスト | ● |
| | | 管理者向け操作手順書提供 | ● |
| | | エージェントソフトウェア操作手順書提供 | ● |
| | | クライアント展開支援（オプション） | ▲ |
| | | 定期報告（オプション） | ▲ |


© 2023 Fujitsu Limited

# サービス概要：エンドポイントセキュリティ

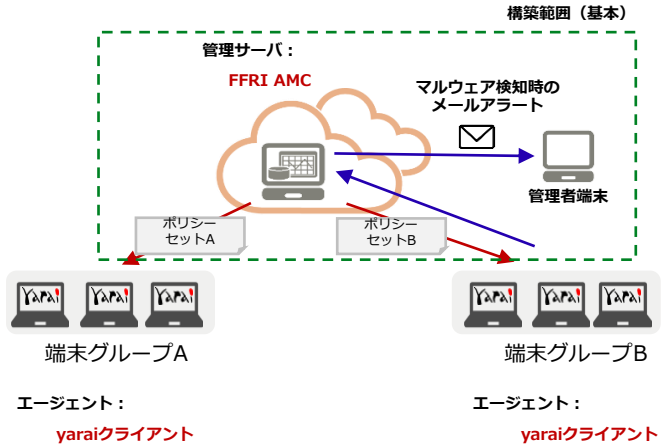
FUJITSU

## ● エンドポイントセキュリティ

**PCマルウェア対策：FFRI yarai**
・クライアント端末を管理対象として、統合的なエンドポイント対策を実現
・FFRI　AMCと組み合わせることにより、クライアント端末に設定するセキュリティポリシーを一元管理

対応製品
・FFRI yarai Cloud

全体構成




■サービス概要
お客様のエンドポイント端末の統合管理を実現するエンドポイントセキュリティ管理基盤の構築を行います。

■作業範囲
- 管理サーバである FFRI AMCの構築、および管理対象端末グループのクライアントソフトウェア(yaraiクライアント) に配信するポリシーの設定を行います。
- 管理対象端末へのクライアントソフトウェアの展開作業はお客様にて実施して頂く前提とします。
（展開作業中のQ&A対応メニューをオプションでご用意します）

■注意事項/前提事項
- お客様拠点での結合テスト実施にあたり、設定ポリシーセット数1個につき1台の動作確認用クライアント端末をお客様に準備頂く前提とします。
- 動作確認用クライアント端末と FFRI AMCの通信が可能な環境をお客様にご用意頂く必要がございます。(FWにて通信許可をしていただくなど)


© 2023 Fujitsu Limited

# エンドポイントセキュリティの構築作業提供範囲

FUJITSU

- エンドポイントセキュリティ（PCマルウェア対策：FFRI yarai）におけるBasicメニューの構築作業範囲については以下の通りです

凡例（●：基本(必須)、▲：オプション）

| 作業項目 | | | Basic |
|---|---|---|---|
| エンドポイントセキュリティ | PCマルウェア対策 | 方式設計 | ● |
| | | 環境設計 | ● |
| | | 環境構築/単体テスト | ● |
| | | 結合テスト | ● |
| | | Defender連携導入（オプション） | ▲ |
| | | クライアント展開支援（オプション） | ▲ |
| | | 定期報告（オプション） | ▲ |

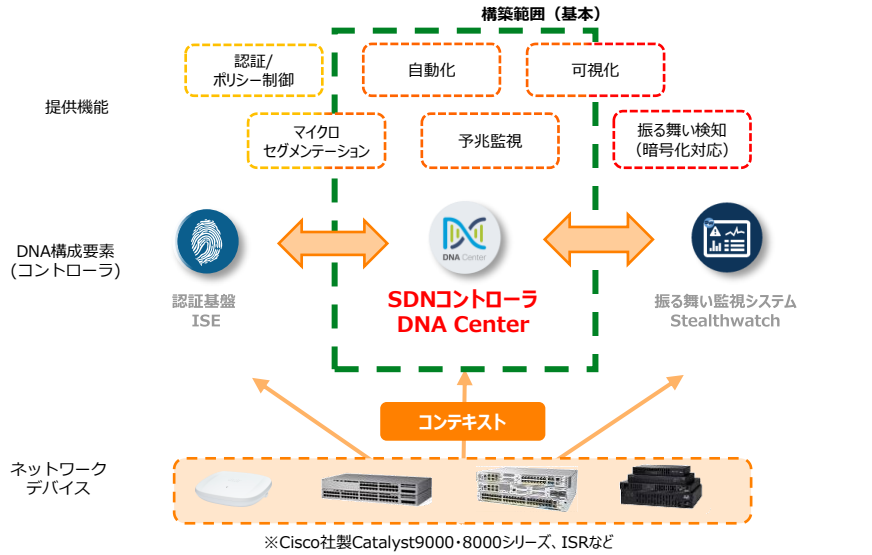

© 2023 Fujitsu Limited

# サービス概要：セキュリティ運用監視

## ● セキュリティ運用監視

**稼働状況可視化**
・ネットワーク機器を管理対象として、インフラの可視化や監視などの運用高度化を実現

対応製品（2022年8月時点）
・Cisco DNA Center




■サービス概要
お客様の保有するCisco社製ネットワーク機器を可視化・分析、セキュリティ設定、 運用省力化し、全自動のネットワーク制御を目指すCisco DNA Centerアプライアンス(以下DNACアプライアンス)の構築を行います。

■作業範囲
- 新規にDNACアプライアンスを構築します。
- お客様の既存監視システムとの連携作業は対象外とします。

■注意事項/前提事項
- 監視対象ネットワーク機器はDNACアプライアンスに対応している機器である必要があります。
- 監視対象ネットワーク機器に必要な設定は事前に実施いただく必要がございます。

※構築作業提供範囲については、P.26【参考】各メニュー詳細を確認ください


© 2023 Fujitsu Limited

# セキュリティ運用監視の構築作業提供範囲（新規構築）

- セキュリティ運用監視（稼働状況可視化：Cisco DNA Center ）におけるLiteメニュー（新規構築）の構築作業範囲については以下の通りです

凡例（●：基本(必須)、▲：オプション）

| 作業項目 | | | | Lite |
|---|---|---|---|---|
| セキュリティ運用監視 | 稼働状況可視化 | 環境設計 | | ● |
| | | 初期設定 | | ● |
| | | ネットワーク基本設定・フロア設定 | 階層設定 | ● |
| | | | ネットワーク設定 | ● |
| | | | テレメトリー設定 | ● |
| | | 機器登録 | | ● |
| | | 現地作業（オプション） | 現地設定・確認(ISE連携なし) | ▲ |
| | | | 現地設定・確認(ISE連携あり) | ▲ |
| | | バックアップ構築（オプション） | HA構成 | ▲ |
| | | | DNACアプライアンスのバックアップ | ▲ |
| | | トレーニング（オプション） | | ▲ |
| | | 定期報告（オプション） | | ▲ |


© 2023 Fujitsu Limited

# セキュリティ運用監視の構築作業提供範囲（既存環境への追加）

- セキュリティ運用監視（稼働状況可視化：Cisco DNA Center ）におけるLiteメニュー（既存環境への追加）の構築作業範囲については以下の通りです

凡例（●：基本(必須)、▲：オプション）

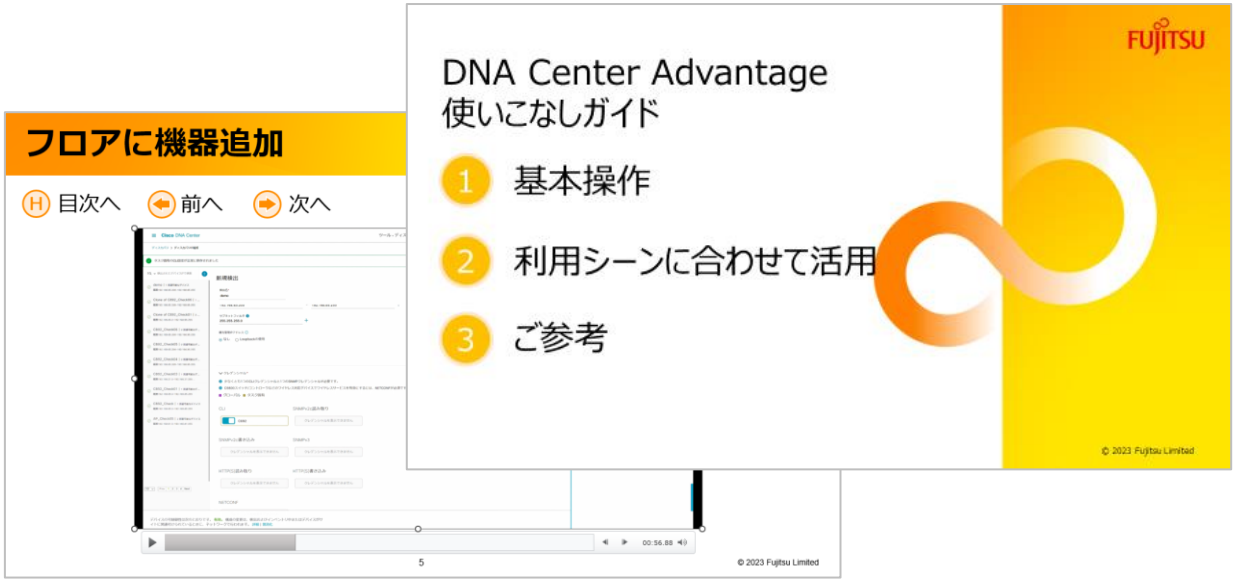
| 作業項目 | | | Lite |
|---|---|---|---|
| セキュリティ運用監視 | 稼働状況可視化 | 環境設計 | ● |
| | | 既存環境への機器追加 | ● |
| | | 既存環境へのフロア追加（オプション） | ▲ |
| | | トレーニング（オプション） | ▲ |
| | | 定期報告（オプション） | ▲ |


© 2023 Fujitsu Limited

# [参考] セキュリティ運用監視（トレーニング）について

- トレーニングでは、お客様の日々の運用におけるCisco DNA Centerアプライアンスの可視化・分析、セキュリティ設定、運用省力化に向けた、弊社講師による使いこなしトレーニングを行います。

- 実施概要
  - オンライン実施
  - 3時間（Q/A含む）




※注意事項
弊社セキュリティ運用監視メニューによって構築されたDNACアプライアンス、またはそれに準じた構築を行ったDNACアプライアンスに対して実施いたします。


© 2023 Fujitsu Limited

# サービス概要：セキュリティ運用監視

## ● セキュリティ運用監視

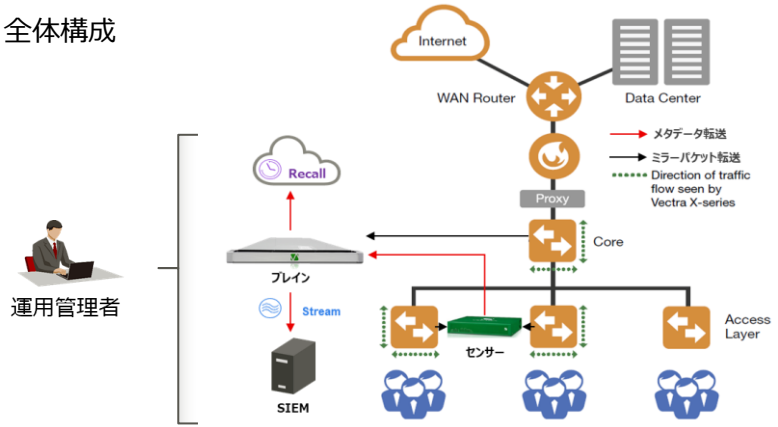
**NW脅威検知・可視化**
・ネットワーク機器を管理対象として、インフラの可視化や監視などの運用高度化を実現

対応製品
・Vectra AI

特長

- 高度な検出手法を複数採用することにより、内部脅威を早期に検出
- 社内ネットワークトラフィックを常時監視
- 脅威の内容を分析し、Vectra AIが対処の優先順位付けを実施することにより、運用負荷を軽減

全体構成




■サービス概要
お客様の対象ネットワークのトラフィックを採取・分析し、内部に侵入した脅威を、俯瞰的に可視化するアプライアンス型のNDRソリューション「Vectra AI」の構築を行います。

■作業範囲
- 新規にVectra AIアプライアンスを構築します。
- Vectra AIを利用するにあたり必要となる他機器（SWやルータ、F/W、Proxy、AD等の機器）の準備／設定は対象外とします。

■注意事項/前提事項
下記はPrefixサービスの対象外となるため、お客様またはフィールドSEにて実施いただきます。
- 周辺機器の設置または設定変更
- 導入機器の設置およびケーブル敷設等の作業


© 2023 Fujitsu Limited

# セキュリティ運用監視の構築作業提供範囲

- セキュリティ運用監視（NW脅威検知・可視化：Vectra AI）におけるLiteメニューの構築作業範囲については以下の通りです

凡例（●：基本(必須)、▲：オプション）

| 作業項目 | | | | Lite |
|---|---|---|---|---|
| セキュリティ運用監視 | NW脅威検知・可視化 | 環境設計 | | ● |
| | | 初期設定 | | ● |
| | | 追加機器設定作業（オプション） | Vectraセンサー追加 | ▲ |
| | | 定期報告（オプション） | | ▲ |


© 2023 Fujitsu Limited

# サービス適用時の注意事項


© 2023 Fujitsu Limited

# サービス適用時の注意事項

- 本サービスは各製品の設計/構築サービスのみのご提供です。
  別途、ライセンス/製品の購入が必要です。
- 運用サービスが必要な場合は、担当営業にご相談ください。


© 2023 Fujitsu Limited

# 【参考】各メニュー詳細

【構築作業提供範囲・内容】
・エンドポイントセキュリティ
・セキュリティ運用監視

FUJITSU-RESTRICTED

© 2023 Fujitsu Limited

# 【構築作業提供範囲・作業内容】
# エンドポイントセキュリティ（PCマルウェア対策：Trellix）（1/2）

- エンドポイントセキュリティ（PCマルウェア対策：Trellix）における構築作業提供内容は以下の通りです

凡例（●：基本(必須)、▲：オプション）

| 作業項目 | | | メニュー | |
|---|---|---|---|---|
| | | | Basic | |
| エンドポイントセキュリティ | PCマルウェア対策 | 方式設計 | ● | 本サービスで定めた型に基づいた方式の設計を行います。<br>・以下の項目の方式及び構成設計を実施します。<br>- システム構成・環境<br>- 提供機能<br>- 運用・保守<br>- 性能・拡張性<br>- 可用性 |
| | | 環境設計 | ● | 本サービスで定めた型に基づいた環境設計を実施します。<br>以下のパラメータ設計を実施します。<br>・Trellixエージェントポリシー設定<br>・ENSポリシー設定<br>- ENS共通設定<br>- 既知のマルウェアに対する保護機能<br>- ENSの除外項目設定<br>- マルウェア検知通知設定<br>・Endpointポリシー設定<br>- Endpoint全般設定<br>- Endpointの除外項目設定<br>- ファイアウォールルール設定<br>- エクスプロイト対策プログラムの設定<br>- マルウェア検知通知設定<br>・ポリシー適用端末グループ設定<br>・クライアントタスクカタログ設定<br>・クライアントタスクカタログの配信スケジュール設定 |


© 2023 Fujitsu Limited

# 【構築作業提供範囲・作業内容】
# エンドポイントセキュリティ（PCマルウェア対策：Trellix）（2/2）

- エンドポイントセキュリティ（PCマルウェア対策：Trellix）における構築作業提供内容は以下の通りです

凡例（●：基本(必須)、▲：オプション）

| 作業項目 | | | メニュー | |
|---|---|---|---|---|
| | | | Basic | |
| エンドポイントセキュリティ | PCマルウェア対策 | 環境構築/単体テスト | ● | 本サービスで定めた型に基づき作成したデザインシートの内容をePO SaaSに設定します。 |
| | | 結合テスト | ● | テスト用クライアント端末にENSを導入し、クライアントPCが設計通りに動作することを確認します。 |
| | | 管理者向け操作手順書提供 | ● | 本サービスで定めた型に基づき作成した ePO SaaS管理者向け簡易操作手順書を提供します。 |
| | | エージェントソフトウェア操作手順書提供 | ● | 本サービスで定めた型に基づき作成したクライアント端末へのエージェントソフトウェア操作手順書を提供します。 |
| | | クライアント展開支援（オプション） | ▲ | お客様によるクライアント展開作業中にQA支援を実施します。 |
| | | 定期報告（オプション） | ▲ | 本サービスの作業の進捗報告および課題検討のための定期報告を行います。 |


© 2023 Fujitsu Limited

# 【構築作業提供範囲・作業内容】
# エンドポイントセキュリティ（PCマルウェア対策：FFRI yarai）（1/2）

FUJITSU

- エンドポイントセキュリティ（PCマルウェア対策：FFRI yarai）における構築作業提供内容は以下の通りです

凡例（●：基本(必須)、▲：オプション）

| 作業項目 | | | メニュー | |
|---|---|---|---|---|
| | | | Basic | |
| エンドポイントセキュリティ | PCマルウェア対策 | 方式設計 | ● | 本サービスで定めた型に基づいた方式の設計を行います。<br>・以下の項目の方式及び構成設計を実施します。<br>- システム構成・環境<br>- 提供機能<br>- 運用・保守<br>- 性能・拡張性<br>- 可用性 |
| | | 環境設計 | ● | 本サービスで定めた型に基づいた環境設計を実施します。<br>以下のパラメータ設計を実施します。<br>・FFRI AMCパラメータ設定<br>・yaraiクライアントパラメータ設定<br>・yaraiクライアントポリシー設定<br>・基本/Static分析/Sandbox/HIPS/機械学習/ZDP/Defender<br>例外リスト設定/検体収集/スキャン/ハンティング/隔離/クラウド連携<br>・ポリシー適用端末グループ設定<br>・通知設定<br>・ログインアカウント、ロール設定<br>・Postgre SQL／Apacheパラメータ設定<br>・SSL証明書設定 |
| | | 環境構築/単体テスト | ● | 本サービスで定めた型に基づき作成したデザインシートの内容をFFRI AMCに設定します。 |
| | | 結合テスト | ● | テスト用クライアント端末にFFRI yaraiクライアントを導入し、クライアントPCが設計通りに動作することを確認します。 |


© 2023 Fujitsu Limited

# 【構築作業提供範囲・作業内容】
# エンドポイントセキュリティ（PCマルウェア対策：FFRI yarai）（2/2）

- エンドポイントセキュリティ（PCマルウェア対策：FFRI yarai）における構築作業提供内容は以下の通りです

凡例（●：基本(必須)、▲：オプション）

| 作業項目 | | | メニュー | |
|---|---|---|---|---|
| | | | Basic | |
| エンドポイントセキュリティ | ＰＣマルウェア対策 | Defender連携導入（オプション） | ▲ | Defender連携機能の設定追加、動作確認を実施します。 |
| | | クライアント展開支援（オプション） | ▲ | お客様によるクライアント展開作業中にQA支援を実施します。 |
| | | 定期報告（オプション） | ▲ | 本サービスの作業の進捗報告および課題検討のための定期報告を行います。 |


© 2023 Fujitsu Limited

# 【構築作業提供範囲・作業内容】
# セキュリティ運用監視（稼働状況可視化：Cisco DNA Center）（新規構築）

FUJITSU

- セキュリティ運用監視（稼働状況可視化：Cisco DNA Center）における新規構築作業提供内容は以下の通りです

凡例（●：基本(必須)、▲：オプション）

| 作業項目 | | | | メニュー | |
|---|---|---|---|---|---|
| | | | | Lite | |
| セキュリティ運用監視 | 稼働状況可視化 | 環境設計 | | ● | 本サービスで定めた型に基づいたパラメータ設定のための説明と環境設計を行います。 |
| | | 初期設定 | | ● | 本サービスの環境設計に基づいた初期設定を実施します。<br>・以下の項目を実施します。<br>- Cisco DNA Centerソフトウェアのインストール<br>- アカウント登録<br>- セキュリティ設定<br>- Cisco DNA Centerソフトウェアのアップデートを実施します。 |
| | | ネットワーク基本設定・フロア設定 | 階層設定 | ● | 本サービスの環境設計に基づき、有線機器を登録するためのエリア・建物・フロア作成を実施します。<br>また無線機器がある場合は、無線機器との連携を行う場合の機器を登録するためのエリア・建物・障害物込みのフロア作成・AP設定を実施します。 |
| | | | ネットワーク設定 | ● | 本サービスの環境設計に基づき、ネットワーク設定を実施します。 |
| | | | テレメトリー設定 | ● | 本サービスの環境設計に基づき、テレメトリー設定を実施します。 |
| | | 機器登録 | | ● | 本サービスの環境設計に基づき、機器の登録とフロアへの登録をする手順書を提示します。 |
| | | 現地作業（オプション） | 現地設定・確認(ISE連携なし) | ▲ | 本サービスの環境設計に基づき、機器登録作業を弊社にて現地で実施します。 |
| | | | 現地設定・確認(ISE連携あり) | ▲ | 本サービスの環境設計に基づき、機器登録とお客様環境のISEとの連携作業を弊社にて現地で実施します。 |
| | | バックアップ構築（オプション） | HA構成 | ▲ | 本サービスの環境設計に基づきDNACアプライアンス 3台でHigh Availability (HA)構築を実施します。 |
| | | | DNACアプライアンスのバックアップ | ▲ | 本サービスの環境設計に基づき、バックアップ設定を実施します。 |
| | | トレーニング（オプション） | | ▲ | 本サービスで構築したCisco DNACenterを効果的に使用するための方法についてオンライン会議にてご説明およびQA対応を行います。 |
| | | 定期報告（オプション） | | ▲ | 本サービスの作業の進捗報告および課題検討のための定期報告を行います。 |


© 2023 Fujitsu Limited

# 【構築作業提供範囲・作業内容】
# セキュリティ運用監視（稼働状況可視化：Cisco DNA Center）（既存環境への追加）

- セキュリティ運用監視（稼働状況可視化：Cisco DNA Center）における既存環境への追加構築作業提供内容は以下の通りです

凡例（●：基本(必須)、▲：オプション）

| 作業項目 | | | メニュー | |
|---|---|---|---|---|
| | | | Lite | |
| セキュリティ運用監視 | 稼働状況可視化 | 環境設計 | ● | 本サービスで定めた型に基づいたパラメータ設定のための説明と環境設計を行います。 |
| | | 既存環境への機器追加 | ● | 既存のDNACアプライアンスに機器を追加します。 |
| | | 既存環境へのフロア追加（オプション） | ▲ | 既存のDNACアプライアンスにフロアを追加します。 |
| | | トレーニング（オプション） | ▲ | 本サービスで構築したCisco DNACenterを効果的に使用するための方法についてオンライン会議にてご説明およびQA対応を行います。 |
| | | 定期報告（オプション） | ▲ | 本サービスの作業の進捗報告および課題検討のための定期報告を行います。 |


© 2023 Fujitsu Limited

# 【構築作業提供範囲・作業内容】
# セキュリティ運用監視（NW脅威検知・可視化：Vectra AI）

- セキュリティ運用監視（ NW脅威検知・可視化：Vectra AI）における構築作業提供内容は以下の通りです

凡例（●：基本(必須)、▲：オプション）

| 作業項目 | | | | メニュー | |
|---|---|---|---|---|---|
| | | | | Lite | |
| セキュリティ運用監視 | NW脅威検知・可視化 | 環境設計 | | ● | 本サービスで定めた型に基づいたパラメータ設定のための説明と環境設計を行います。 |
| | | 初期設定 | | ● | 本サービスの環境設計に基づいた初期設定を実施します。<br>以下の項目を実施します。<br>- Vectraのインストール<br>- パラメータ設定<br>- 単体テスト |
| | | 追加機器設定作業（オプション） | Vectraセンサー追加 | ▲ | 本サービスの環境設計に基づき、Vectraセンサーの初期設定を実施します。<br>- Vectraセンサーのインストール<br>- パラメータ設定<br>- 単体テスト |
| | | 定期報告（オプション） | | ▲ | 本サービスの作業の進捗報告および課題検討のための定期報告を行います。 |


© 2023 Fujitsu Limited

# Thank you

© 2023 Fujitsu Limited