HITACHI
Inspire the Next

ゼロトラストセキュリティ

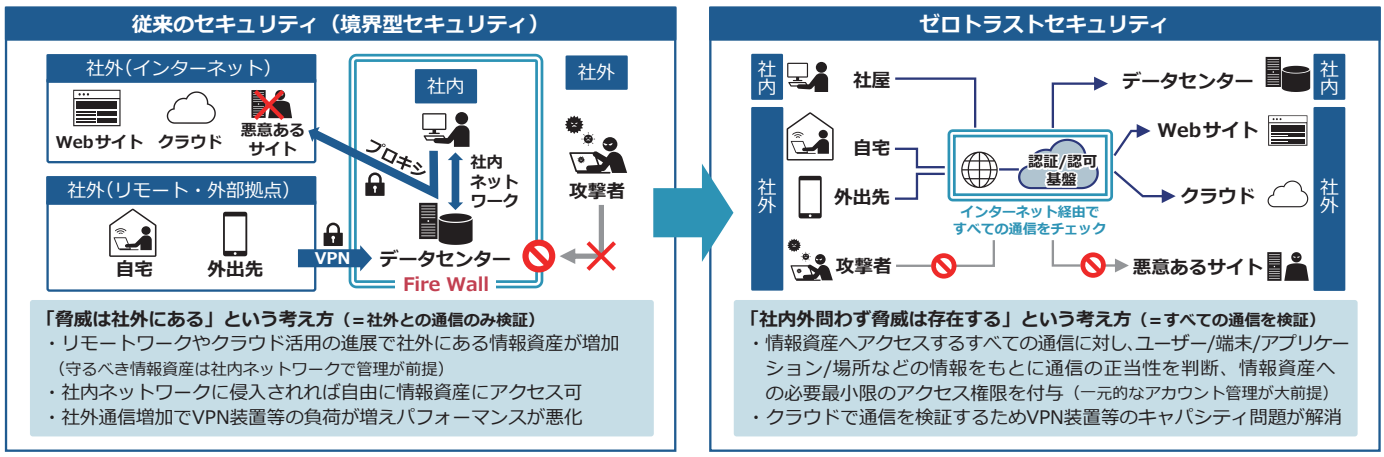
リモートワークやクラウド化によるセキュリティリスクの高まりに
対応した適切なセキュリティソリューションを提供

2024年12月版

株式会社 日立システムズエンジニアリングサービス

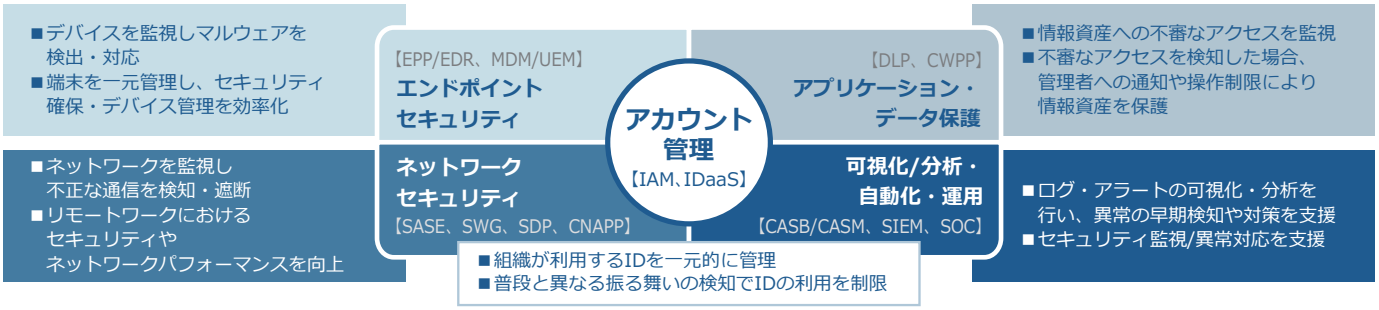
ゼロトラストセキュリティとは

ネットワークの内部と外部を区別することなく、守るべき情報資産にアクセスするものはすべて信頼しない（ゼロトラスト）ことを前提としたセキュリティアプローチです。クラウドやインターネットを前提としたオープンアーキテクチャを導入する際に重要となります。



【ゼロトラストセキュリティの構成要素】

セキュリティの脅威に対応したさまざまなコンポーネントを組み合わせてシステム全体を網羅することで、境界を意識することなくセキュリティを担保することが可能になります。



エンドポイントセキュリティ：サーバーやPCなどの末端機器に対するセキュリティ対策

EDR/EPP（デバイス保護）

ゼロトラストルールが未知のウイルス・マルウェア攻撃を防ぎます

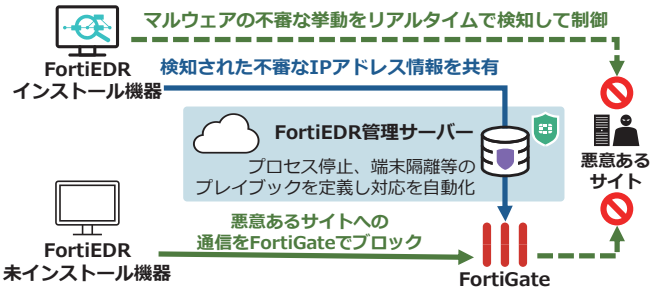
■エンドポイントセキュリティ対策 FortiEDR

1. エンドポイントを強力に保護

- マルウェア検知と感染防止（EPP）、侵入した脅威の調査 / 拡散防止（EDR）の両面でシームレスに対応
- リアルタイムに脅威を特定・防止し、可視化、分析、保護、修復を実現
- FortiGateとの連携により、FortiEDRをインストールできないIoT機器も保護

2. インシデント対応の自動化

- カスタマイズ可能なプレイブックで対応・修復を自動化

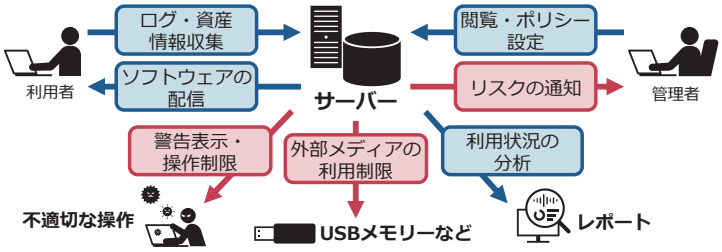


MDM/UEM（デバイス管理・保護）

情報セキュリティ対策の強化と情報資産の管理を簡単に

■SKYSEA Client View導入ソリューション

- PCやサーバーなどのハードウェア情報、ソフトウェア情報、プリンターや外部メディアなどの機器情報などを一元管理
- 情報資産の利用状況を把握し、セキュリティ対策や情報資産を有効に活用可能



EDR:Endpoint Detection and Response, EPP: Endpoint Protection Platform, MDM:Mobile Device Management, UEM:Unified Endpoint Management

アカウント管理：ユーザーアカウントの一元的な管理・認証を実現

IAM、IDaaS（ユーザー管理・認証）

シンプルなID管理と高セキュリティを提供します

■ID管理 – LDAP Manager･Extic導入ソリューション

1. LDAP Managerの特長
- 外部システムなどからID情報を取り込みが可能
- 取り込んだID情報をオンプレシステム、SaaSに自動連携
- スケジュール実行で、職制変更時の作業負担を大幅に低減

2. Exticの特長
- シングルサインオンとID管理を兼ね備えたクラウド認証基盤
- シングルサインオンで簡単ログイン
- 認証は多要素認証、パスワードレス認証等の組み合わせにより高セキュリティを実現

ID情報 **ID情報の一元化**
- セキュリティ事故防止
- 管理の簡素化
- 作業効率向上

認証情報 **認証情報の一元化**
- シングルサインオン
- 多要素認証
- アクセス認可

■多要素認証 - EVEMA/Themis/EVECLOUD -

生体認証（指紋、顔、静脈）やICカードの利用で安心安全なITシステムを実現します
- PCログオン、VDI、業務アプリケーションやクラウドサービス他の認証を強化
- お客さまの業務に合わせて認証方式を選択可能
- 認証基盤の構築、運用、サポートは当社がワンストップで提供

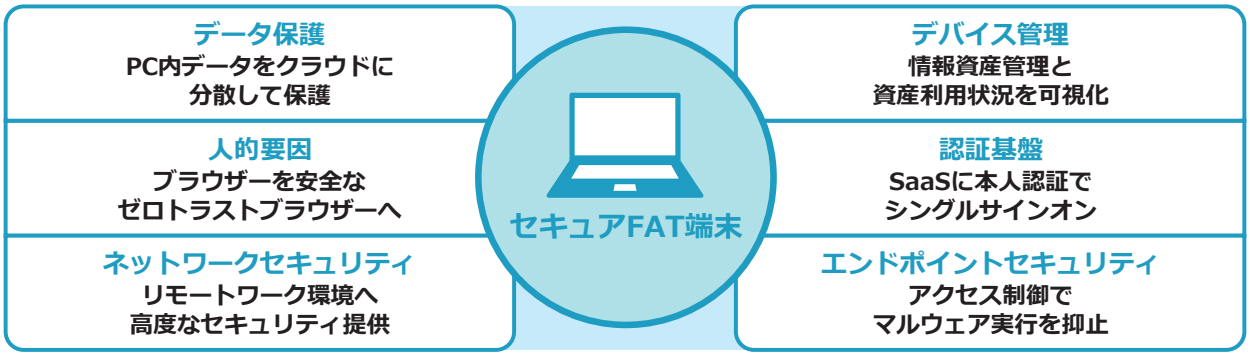
IAM:Identity and Access Management, IDaaS: Identity as a Service

アプリケーション・データ保護：情報資産の保護/情報漏えい防止

DLP（情報漏えい防止）

■セキュアFAT端末ソリューション

FAT端末のセキュリティ対策に対するお悩みを一気に解決！
お客さまのニーズをヒアリングし、さまざまなセキュリティ製品を組み合わせることで、お客さまに適切なセキュリティ機能を備えたFAT端末の導入を支援します



DLP:Data Loss Prevention

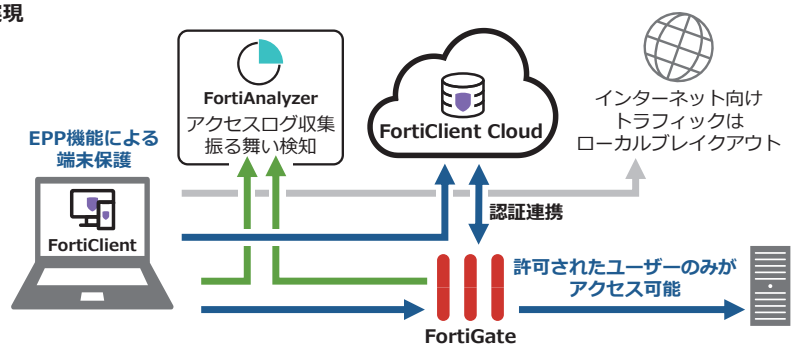
ネットワークセキュリティ：エンドポイントからインターネットへアクセスする際のセキュリティ対策

SDP（リモートアクセス動的制御）

■ゼロトラストネットワーク FortiGate ZTNA

1. FortiGateによるゼロトラストネットワークアクセスの実現
- 脱VPNによるパフォーマンス問題の改善
- FortiGateとFortiClient連携によるリソースへのきめ細かいアクセス制御
- FortiAnalyzerでアクセスログを集中管理し、マルウェアの挙動を分析、検知

2. エンドポイントの集中管理
- 高度な次世代のエンドポイントセキュリティ機能による端末の保護
- 端末の脆弱性の有無やパッチの適用状況を一元管理



SDP:Software Defined Perimeter

可視化/分析・自動化・運用：セキュリティ運用の高度化・効率化を支援

SIEM（脅威の可視化）

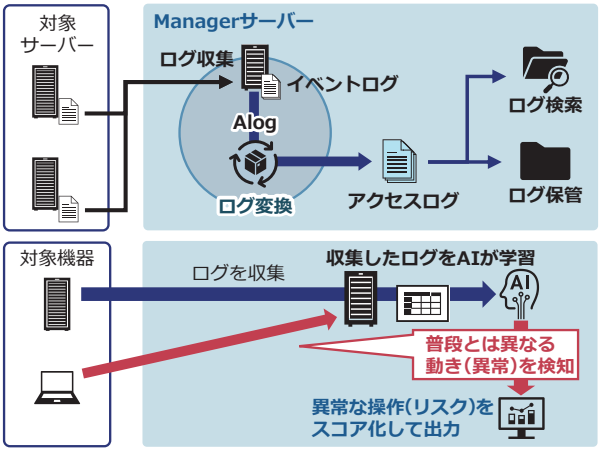
稼働状況やログの可視化で高度なセキュリティ運用を支援します

■統合ログ管理機能 AMIYA Alog適用ソリューション

1. ログ管理
AMIYAのSIEM製品である統合ログ管理機能（Alog）を活用し、多種多様な製品（WindowsやLinux、VMware等）のログ収集と管理を実現

2. AIによる異常の検知
収集したログをAIが学習して
『普段とは異なる動き（異常）』を検知
リスクスコアリング機能にて、検知結果を可視化
（グラフ化して視覚的に捉えることが可能）

3. 異常検知時の早期発見
特定の異常検出メッセージを設定することで、対象メッセージ出力時に外部（ハードウェア、ソフトウェア）からメールあるいはSyslog通知を受け取ることができ、異常検知時の早期発見が可能



SIEM:Security Information and Event Management

ゼロトラストセキュリティ 主なソリューション

対象カテゴリー	解決ソリューション	
アカウント管理	IAM、IDaaS（ユーザー管理・認証）	ID管理 – LDAP Manager·Extic導入ソリューション 多要素認証 – EVEMA/Themis/EVECLOUD - オフィスITの認証セキュリティ SmartSESAME
エンドポイントセキュリティ	EPP/EDR（デバイス保護）	エンドポイントセキュリティ対策 FortiEDR
	MDM/UEM（デバイス管理・保護）	SKYSEA Client View導入ソリューション
ネットワークセキュリティ	SDP（リモートアクセス動的制御）	ゼロトラストネットワーク FortiGate ZTNA
	SASE（セキュアアクセスサービスエッジ）	セキュアアクセスサービスエッジ FortiSASE
	CNAPP（マルチクラウドセキュリティ管理）	クラウドセキュリティ導入ソリューション
アプリケーション・データ保護	DLP（情報漏えい防止）	ZENMU Virtual Drive グローバルセキュアデータ転送サービス 秘密分散 フォー メール メールセキュリティ対策ソリューション セキュアFAT端末ソリューション
可視化/分析・自動化・運用	SIEM（脅威の可視化）	Microsoft Azure Sentinel構築ソリューション 統合ログ管理機能 AMIYA Alog適用ソリューション
	SOC（セキュリティ運用）	セキュリティ監視導入支援ソリューション

CNAPP:Cloud Native Application Protection Platform

株式会社 日立システムズエンジニアリングサービス

本社：〒220-8132 横浜市西区みなとみらい2-2-1
横浜ランドマークタワー32階

商品のお問い合わせはこちらまで
www.hitachi-systems-es.co.jp

SS-2418 | 2024.12
Printed In Japan