ゼロトラストセキュリティに関するプロダクト・サービスの豊富な知識と、確かな選定力

- お客様の現状のセキュリティ課題を明確化し、マネジメントとシステムの両面を考慮した対策を提案
- 自社製品を含め国内外問わず多彩な製品・サービスラインナップでお客様の課題を的確かつスピーディーに解決
- 運用体制やリソースなどお客様の実情に合った製品・サービスを提案し、設計・構築の支援、サポートまで、シームレスかつトータルに対応

製品・サービス提案 → 設計 → 構築 → サポート

■ゼロトラストセキュリティ 主な製品・サービス

対策カテゴリー	対策ソリューション	製品・サービス	概要
アカウント管理	IAM(Identity and Access Management)	Okta Identity Cloud	ID管理や認証・アクセス制御などをクラウド上でまとめて運用
ネットワークセキュリティ	SWG(Secure Web Gateway)	Zscaler Internet Access	場所やデバイスを問わず、クラウドサービスやWebサイトへのセキュアなアクセス・利用を実現
		Palo Alto Networks Prisma Access	次世代ファイアウォールの機能をクラウドで提供。拠点間通信やモバイル端末からのセキュアアクセスを実現
		Menlo Security Web Isolation Service	ウェブコンテンツを無害化するSaaS型セキュリティサービスによりマルウェアの脅威を防止
	SDP(Software Defined Perimeter)	Zscaler Private Access	社内環境やプライベートクラウドなどに対し、セキュアなリモートアクセスを実現
エンドポイントセキュリティ	EPP(Endpoint Protection Platform)	BlackBerry® Protect	人工知能を利用した検知エンジンを使用し、高精度にマルウェアを検知する次世代マルウェア対策製品。検知率99%以上*1を実現
	EDR (Endpoint Detection and Response)	BlackBerry® Optics	端末上のイベントをモニタリングした上で、脅威の可視化・分析・調査、迅速な対応を実現するEDR
	MDR (Managed Detection and Response)	MDRサービス for BlackBerry®	BlackBerry Protect / BlackBerry Opticsの運用を代行し、インシデントの監視から対応までをワンストップで提供
		MDRサービス for Trend Micro™	セキュリティコンサルタントやホワイトハッカーといった専門技術者が、Trend Micro Apex Oneの運用から対策までのサイクルをワンストップで提供
	UEM(Unified Endpoint Management)	MobileIron UEM	スマートフォンやタブレット端末などのモバイルデバイスだけでなく、PCまで一元管理できる進化系UEM
		VMWare Workspace ONE (AirWatch)	UEM・MAM*2・MCM*3・MEM*4のさまざまな機能をシームレスに統合し、モバイル端末を最大限に活用可能
アプリケーション・データ保護	CWPP (Cloud Workload Protection Platform)	Palo Alto Networks Prisma Cloud	パブリッククラウド上のセキュリティ設定を監査・レポーティングし、脅威の付け入る隙が発生しやすいクラウド環境を分析。パブリッククラウドの安全な利用を実現
	DLP(Data Loss Prevention)	Bitglass	会社のポリシーに違反した場合、ファイルのアップロード・ダウンロードの禁止など制御を行い、情報漏洩を防止
分析・可視化・自動化	CASB(Cloud Access Security Broker)	Bitglass	サンクションIT・シャドーITの可視化やクラウドサービス利用状況の把握、リアルタイムでの制御を実現
		NetSkope	社内・社外を問わず、クラウドサービス・Webサイトへのアクセスの可視化、制御をリアルタイムで実現、セキュアな利用を可能に
	CSPM (Cloud Security Posture Management)	Palo Alto Networks Prisma Cloud	パブリッククラウド上のセキュリティ設定を監査・レポーティングし、脅威の付け入る隙が発生しやすいクラウド環境を分析。パブリッククラウドの安全な利用を実現
		クラウドワークロードセキュリティサービス	企業内におけるIaaS/PaaS環境の利用状況やセキュリティリスクを可視化し、システム運用管理の効率向上や情報セキュリティガバナンスの強化を実現
		Orca Security	パブリッククラウド上のシステムやサービスの本番環境や開発環境におけるセキュリティリスクをまとめて検出、パブリッククラウド環境の安全な利用を支援
	SIEM(Security Information and Event Management)/ SOAR(Security Orchestration and Automation Response)	Splunk	さまざまなシステムログを一元的に検索・分析・可視化することで、脅威の早期発見と被害の低減に貢献するとともに、自動化によってインシデント対応を支援

*1 2018年4月NSS Labs調べ、 *2 MAM:Mobile Application Management、 *3 MCM:Mobile Content Management、 *4 MEM:Mobile Email Management

株式会社 日立ソリューションズ
www.hitachi-solutions.co.jp

本カタログ掲載商品・サービスの詳細情報
www.hitachi-solutions.co.jp/security/sp/solution/task/zerotrust.html

S20S-03-00 2021.04

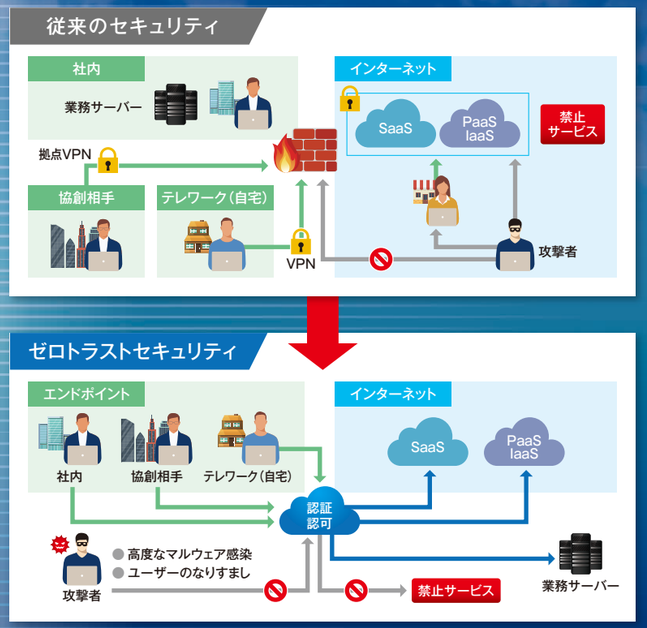
HITACHI
Inspire the Next

ゼロトラストセキュリティソリューション

株式会社 日立ソリューションズ

クラウドやテレワーク環境のセキュリティ対策、プラットフォームやビジネスモデルの変革への対応に、日立ソリューションズのゼロトラストセキュリティ。

従来の境界型セキュリティに代わる対策として注目されるゼロトラストセキュリティ。
クラウドやテレワーク環境のセキュリティ対策だけではなく、グローバル化、M&A、組織の統廃合において必要となる
セキュリティレベルの均一化を、迅速に実現します。
また、デジタルトランスフォーメーション（DX）をはじめとするプラットフォームや
ビジネスモデルの変革にも迅速かつ柔軟に対応し、ビジネスの強化に必須と言える安心・安全なセキュリティ基盤を構築します。



ゼロトラストとは？

従来は「社内」「社外」を分離する境界型のセキュリティ

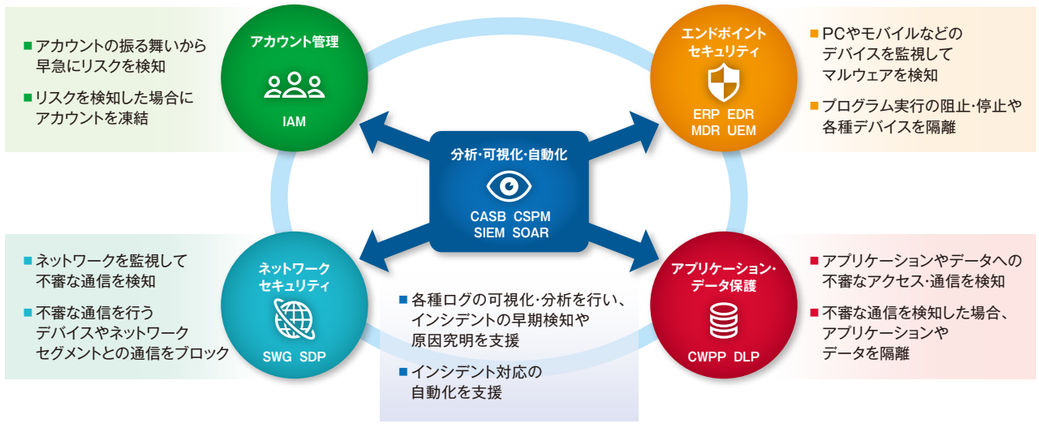
従来、情報資産の保管場所や働く場所はファイアウォールを境界とする内側の「社内」が中心でした。セキュリティも、「社内」「社外」を分離する境界型のネットワークを構築し、「社内は安全」「社外は危険」という考えのもとで対策を施してきました。しかし、クラウドシフトの加速やニューノーマルな働き方としてのテレワークの飛躍的な拡大に伴い、セキュリティ対策も「社内」「社外」という境界を設けて対策するのが困難になっています。

安全な領域は存在せず、すべてを信頼しない、という考え方

そこで、注目されてきたのがゼロトラストという考え方です。境界で仕切られた安全な領域は存在せず、ユーザーやデバイス、ネットワーク、アプリケーションの情報をもとに、情報資産にアクセスしてくるものは、すべて信頼せず（＝ゼロトラスト）、常に正当なアクセスであるか、正当な利用者であるかを検証（認証）したうえで、アクセスを認可することを基本とします。

ゼロトラストセキュリティを実現する要素

守りたい情報資産や対応するセキュリティ脅威に応じ、IAM、EPP/EDR、SWGなどのさまざまなコンポーネントを構成。
ユーザーやデバイス、ネットワーク、アプリケーションの情報をもとに、情報資産へのアクセスの利便性を損なわずセキュリティ強化を実現します。



ゼロトラストセキュリティ対策の進め方は？

考え方の一例として、「何も信用しない」がゼロトラストであることから、まずは利用者（ユーザーアカウント）、デバイスを認証・認可できる基盤の準備から開始します。お客様の環境によって、端末のインターネット直接接続が常態化しているようであれば、デバイス保護もしくはネットワーク管理を最優先とする場合もあります。

アカウント管理（IAM）
テレワークやクラウドサービスを駆使するゼロトラストセキュリティでは、まず初めに業務を可能にするため、クラウド上でのアカウント管理・認証（IAM）を行う必要があります。

ネットワーク管理（SWG/SDP）
エンドポイントからインターネットへ直接アクセスする際のセキュリティ強化を行います。

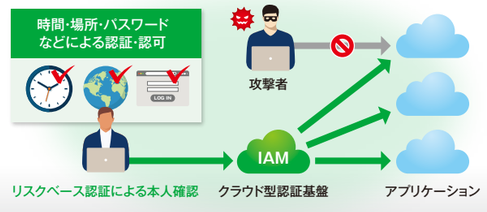
デバイス保護（EPP/EDR）
デバイス管理・保護（UEM）
これまでクライアントを守っていた入口・出口のセキュリティがなくなるゼロトラスト環境では、直接インターネットへ接続するため、エンドポイントでの防御力向上を図る必要があります。

IAM：Identity and Access Management、SWG：Secure Web Gateway、SDP：Software Defined Perimeter、EPP：Endpoint Protection Platform、EDR：Endpoint Detection and Response、
MDR：Managed Detection and Response、UEM：Unified Endpoint Management、CWPP：Cloud Workload Protection Platform、DLP:Data Loss Prevention、CASB：Cloud Access Security Broker、
CSPM：Cloud Security Posture Management、SIEM：Security Information and Event Management、SOAR：Security Orchestration and Automation Response

ゼロトラストセキュリティ 主な対策

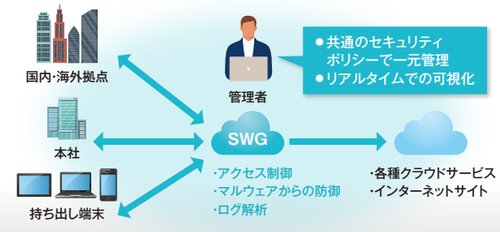
IAM

アカウント管理・認証の統合基盤で利用者の本人認証を行ないます。あらゆるシステムの認証機能を統合的に行うことで、不正アクセスへの対処が行いやすくなります。例えば、同じ時間帯に遠く離れた場所から同一ユーザーでログインが行われた場合には、警告もしくはアカウントを凍結するなど、リスクベース認証が可能になります。



SWG

クラウドサービスやWebサービスなどインターネットへのアクセスに対し、社内だけでなく社外の端末にも共通のポリシー・アクセス制御を適用し、安全なインターネット接続を実現します。
クラウドサービスとして提供され、ハードウェアに依存しないため、拡張性を求められるテレワーク環境でもセキュリティ対策を迅速に実施可能です。



EPP

エンドポイントに侵入しようとする既知・未知のマルウェアの検知・隔離を行います。従来のパターンマッチング型のマルウェア対策製品とは異なり、AI技術を活用した製品を導入すれば、高精度なマルウェア検知も可能です。

EDR

エンドポイントに不審な動きがないかを常時監視し、マルウェアの侵入活動・システムファイルアクセス・レジストリ操作・メモリー操作など、エンドポイントがどのような被害を受けているのかを迅速に可視化できます。