ReSM

ゼロトラスト時代、セキュリティリスクに対処できる体制になっていますか？

――SOCソリューションで盤石の体制構築へ

DTS

変化するセキュリティのトレンド

ReSM

ファイアウォールとセキュリティ（ウイルス対策）ソフトだけでは不十分

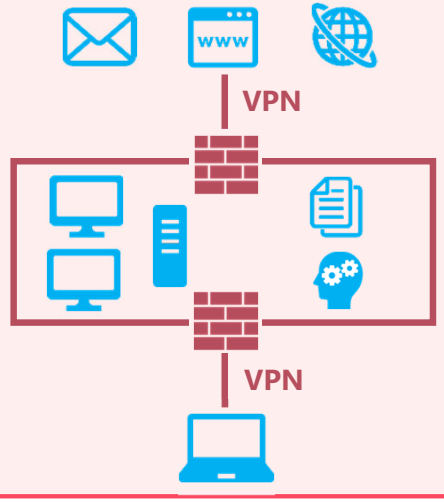
現在、多くの企業のセキュリティ対策は「境界型セキュリティ」という考えかたに基づいて設計・運用されています。
「境界型セキュリティ」とは、社内ネットワークと社内ネットワーク（インターネット）を分けて考え、社内と社外の情報のやり取りをファイアウォールやIPSなどで監視し、外部からの攻撃を防ぐ考え方です。

“境界型セキュリティ”から“ゼロトラストセキュリティ”へ

境界型セキュリティでは、守るべきデータやシステムが、境界の内側（社内ネットワーク側）にあることが前提でした。
しかし、クラウドサービスの利用が一般化した現在、守るべきデータがクラウド上にあるといった状況が急激に増加しています。
このような状況に対応するために提唱された新しいセキュリティの考え方が「ゼロトラスト」です。
社内外にかかわらず、すべての通信や端末（エンドポイント）に対してセキュリティ対策が必要であるという考え方です。

従来の境界型セキュリティ

境界の内側（社内ネットワーク側）の安全性担保を軸としたセキュリティ



ゼロトラストセキュリティ

社外アクセス・クラウド利用を前提としたあらゆるアクセスに対するセキュリティ

ゼロトラスト時代のセキュリティの考え方

ReSM

監視対象が広がり、セキュリティ業務が増大する

「ゼロトラスト」が必要になった背景には、クラウドサービスの普及拡大のほかにも、ワークスタイルの多様化が指摘されています。外出先やテレワークなど、社外から社内ネットワークにアクセスすることが日常的になりました。従来のように、社内ネットワーク上のエンドポイントだけでなく、多彩なエンドポイントを監視する必要が生じているのです。

モバイル、テレワーク、IoTなど、セキュリティ監視対象も拡大

監視が必要なのはモバイルワーク、テレワークで使用するノートPCやタブレット端末、スマートフォンだけではありません。Webカメラや各種センサーなどのIoT機器も対象になります。また、仮想マシンなども監視する必要があります。

UTM、IPS、WAF、エンドポイント、クラウドセキュリティなど幅広い対策が必要

すべての通信やエンドポイントを信用しないゼロトラストでは、複数の対策が必要になります。これを実現するためには、さまざまなセキュリティ対策製品やサービスを組み合わせて利用する必要があります。

■セキュリティの脅威と新しい領域

脅威カテゴリ	脅威の具体例	従来型の領域				新しい領域	
		DC/オフィス	インフラ	NW	アプリ	DX	OT/IoT
人為的(外的権威)	未知マルウェア・不正アクセス ランサムウェア なりすまし、標的型攻撃 踏み台攻撃、マイニング攻撃	物理セキュリティ	サイバーセキュリティ				
人為的(内的権威)	誤操作、紛失 情報漏洩 業務妨害、システム停止		内部不正対策				
故障	停電・断水・空調 ハード故障・劣化によるシステム停止 通信サービス障害	障害対策／災害復旧（DR）					
災害	地震、洪水、台風、火事、漏水						

増加する監視対象への対応が必要

ReSM

ゼロトラストでは、検知・対応が重要

NIST（Natonal Institute of Standards and Technology：アメリカ国立標準技術研究所）が提唱するNISTサイバーセキュリティフレームワークでは、セキュリティ対策を識別、防御、検知、対応、復旧の5つのコア（フェーズ）に分類しています。
監視対象が大幅に増加するゼロトラストでは、分析が必要なセキュリティ・ログも大幅に増加します。そのために、膨大なセキュリティ・ログを迅速に分析して、いち早く異常を検知していくことが重要になります。

NIST（米国国立標準技術研究所）のフレームワーク

特定 (Identify)	防御 (Protect)	検知 (Detect)	対応 (Respond)	復旧 (Recover)
システム・人・組織の弱点を見つける	システム・人・組織を強くする	影響のあるイベントを見つける	イベントの影響を極小化する	仕組みの改善・再発防止策を行う

重要ポイント！

24時間365日、セキュリティ脅威を検知・分析する「SOC」

SOC（Security Operation Center）は、24時間365日体制でネットワークやデバイスを監視し、異常の検知や分析したり、脅威への対応策をアドバイスしたりする組織です。
SOCを自社内に持つ企業もありますが、サイバー攻撃の巧妙化・複雑化やゼロトラストの導入などにより、近年、SOCサービスを提供する企業が増加しています。

「SOC」の役割としくみ

さまざまな監視対象のログを網羅的に監視・分析する「SOCサービス」

ゼロトラストの実現に必要な監視対象のログを24時間365日、リアルタイムでモニタリングし、蓄積した情報を専任のセキュリティアナリストが分析することで、潜在するセキュリティインシデントを発見し、早期対処を実現します。

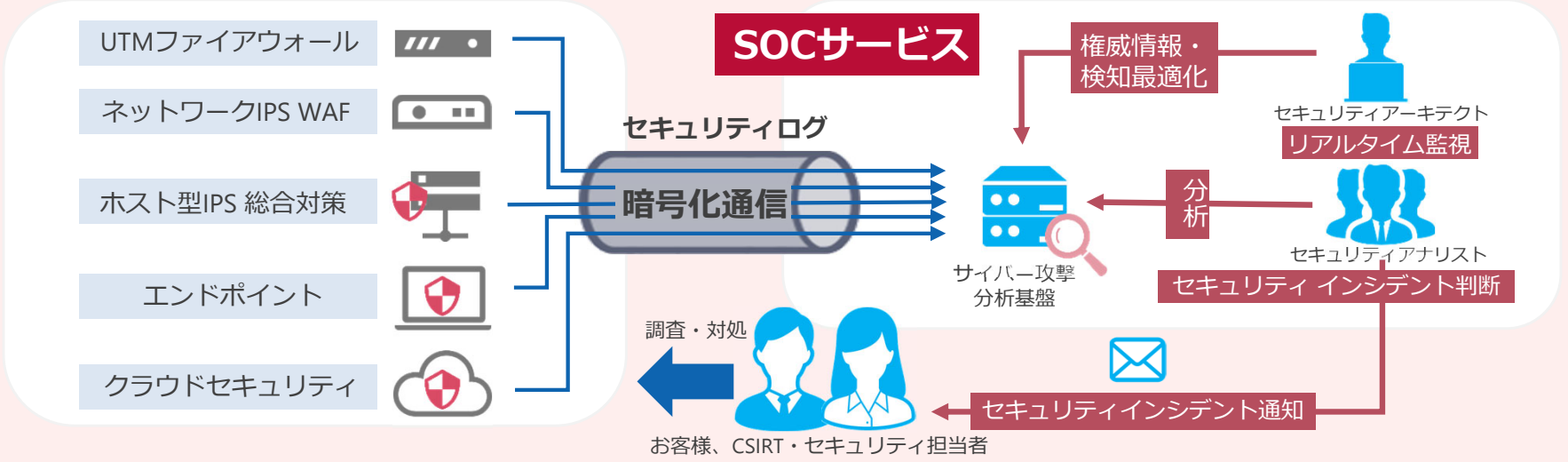
UTM、IPS、エンドポイント、クラウドなどのセキュリティログを監視

「SOCサービス」が監視するのは、UTM、IPSなどのファイアウォールのほか、各種エンドポイント、クラウド、コンテナ、仮想マシンなども含まれます。

専門組織がログを分析、セキュリティインシデントの可能性を発見

サイバー攻撃分析基盤からのアラートによりセキュリティアナリストが詳細分析を行います。分析結果は4段階のインシデントレベルに分類され、通知されます。

SOCサービス概要図



ReSM

お問い合わせ先

CONTACT

株式会社DTS

ITプラットフォームサービス 事業本部
ReSM（リズム）担当

ADDRESS : 〒104-0032
東京中央区八丁堀2-23-1エンパイヤビル
TEL : 03-6914-5215
FAX : 03-6914-5670
URL : https://www.resm.jp/
Mail : resm@dts.co.jp