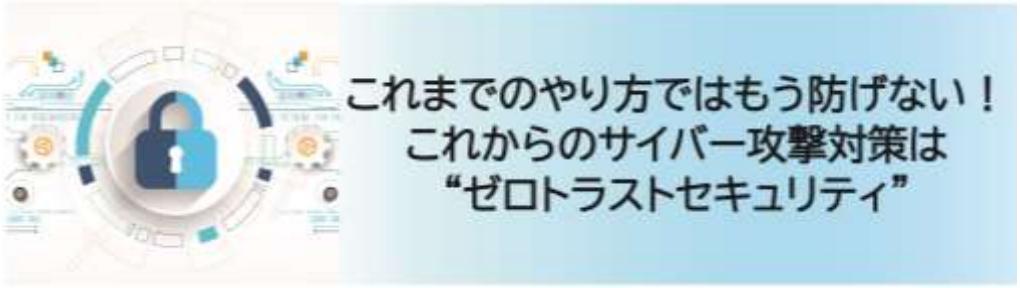
NEWS RELEASE

報道関係各位　　2022 年 1 月 12 日

始めるのは今！日々悪質化するサイバー攻撃から情報資産を守る“ゼロトラストセキュリティ”とは。

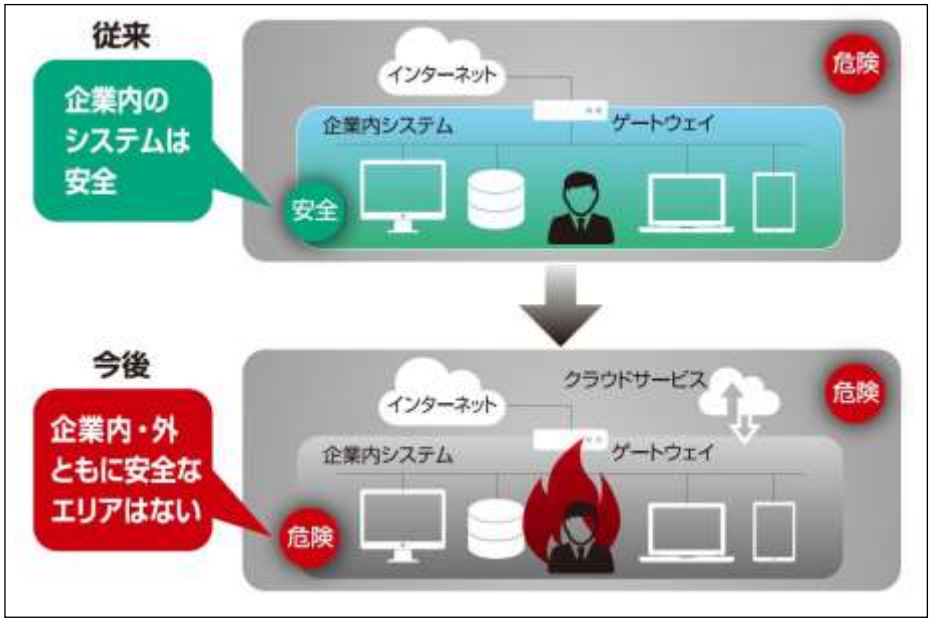
-導入に向けたコンサルティングから、各種サービスまで提供開始-

アライドテレシス株式会社（本社 東京都品川区、代表取締役社長 大嶋章禎）は、これまでのセキュリティ対策では守り切れない、悪質化するサイバー攻撃から会社の情報資産を守るべく、新しいセキュリティに対する考え方“ゼロトラストセキュリティ”について、当社独自の考え方と対策製品を提案します。



サイバー攻撃の脅威は世界的にも深刻で、先日も650億円以上の損失が発生した企業の話がニュースでも報じられました。そして日本でもサイバー攻撃は増加の一途をたどっていることから、政府は2022年度適用に向け、情報通信や医療、金融などを含む14分野の重要インフラ事業者を対象に、サイバー攻撃への備えを義務付けることを発表しました。厳重にセキュリティ対策を講じていても、日々悪質化し続ける巧みなサイバー攻撃は隙間を見つけて入り込んできます。そこでこれからのセキュリティ対策の考え方として注目されているのが“ゼロトラストセキュリティ”です。

これまでのセキュリティ対策は、「内側にある社内を安全なエリア」と考えるファイアウォールやUTM（Unified Threat Management：統合脅威管理）などの“境界型セキュリティ”が主流でした。しかし、クラウドサービスの普及や働き方改革、さらにコロナ禍におけるテレワークの増加などにより、社内だけを守っていれば安心という状況ではなくなり、情報資産へアクセスするデバイスや人、それらの通信など「すべてを信頼しない=ゼロトラスト」の考え方が必要となってきました。そこでこれからの対策として当社の考える“ゼロトラストセキュリティ”を提案します。

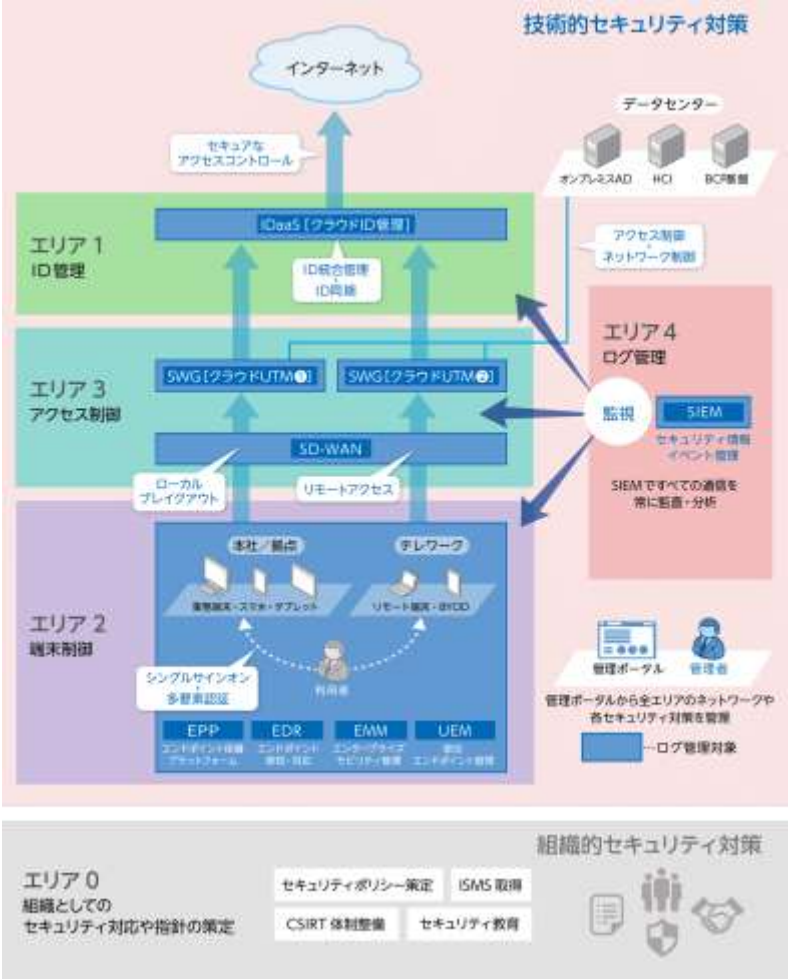


■アライドテレシスが提案する“二段階のゼロトラストセキュリティ”

当社はネットワーク製品を通じ、アクセス制御や認証など、セキュリティ機能に関わる活動を行っており、2014年からは本格的にサイバーセキュリティへの取り組みを開始しました。そして自社で導入したゼロトラストセキュリティの経験やノウハウを生かし、お客様に最適なサービスを提供してまいります。

ゼロトラストセキュリティを実現するために、まず「組織的セキュリティ対策」を強化した上で「技術的セキュリティ対策」を導入する段階的な取り組みを提案します。

最初に強化したい「組織的セキュリティ対策」とは、社内におけるセキュリティポリシーを策定することやISMS※1の取得、CSIRT※2体制の整備やセキュリティ教育など、組織的なセキュリティ対策のことを指します。まずこれらの体制を整えたあと、次に導入したいのが「技術的セキュリティ対策」です。当社でも組織の規模やシチュエーションなどに合わせたセキュリティ対策をご提案します。



ゼロトラストを実現する技術的セキュリティ対策の進め方

ID 管理	正規のユーザーを特定し、必要な企業リソース（データ）にアクセスするために必要最小限の権限を付与します。アクセスごとの認証や要素認証（MFA）がポイントになります。ID管理の課題を解決する方法として、シングルサインオン（SSO）などのIDaaS※3を導入する方法があります。
端末防御	近年、社外から端末を利用するケースが増加しており、様々な脅威にさらされやすくなっています。端末がサイバー攻撃の踏み台となることを防ぐため、端末ごとに適切なセキュリティ対策をします。その方法として、ウイルスやマルウェアからデバイスを保護するEPP※4や、それに加え感染した際の被害を抑えるEDR※5があります。
アクセス制御	従来型のオンプレミス・閉域網中心のネットワークを前提とした境界型防御モデルを見直し、クラウド利用環境を想定したセキュリティ対策をします。その方法として、セキュリティゲートウェイ、SD-WAN※6で常に通信をチェックして最小限でアクセスを許可する方法があります。
ログ管理	サイバー攻撃が高度化しているため、大量のログなどから脅威や脆弱性のデータを収集し証跡を分析することで、ログ監視による攻撃経路の特定と影響範囲の調査が必要となります。ゼロトラストセキュリティに基づいたログ管理は「SIEM※7ですべての通信を常に監査・分析する」ことです。

当社では、ゼロトラストセキュリティを実現するための「技術的セキュリティ対策」を中心としたコンサルティングからソリューションまで幅広くご用意しています。ホームページでは、各ソリューションの適用内容やその解説を詳しく記載しています。次の URL よりご確認ください。

https://www.allied-telesis.co.jp/solution/zero-trust-security

また、当社が実際にゼロトラストセキュリティを導入した実際の体験談や解決策は、WEB 版コミュニケーションマガジン「FASHIONISTA」でわかりやすく解説しています。ぜひご覧ください。
https://www.allied-telesis.co.jp/magazine/zerotrust

さらに、当社のゼロトラストセキュリティについて、より詳しく技術者が解説をするオンラインセミナーも開催いたします。参加は無料です。ぜひご参加ください。
https://www.allied-telesis.co.jp/event/webinar/index.html

※1) ISMS…組織の情報を保護する有効な手段の一つで、組織の情報セキュリティのための仕組みを定めた国際規格。
※2) CSIRT (Computer Security Incident Response Team) …セキュリティインシデントが発生してしまった場合に、インシデントへの対応の他、その脆弱性を分析して情報を共有するなどを行うチームのこと。
※3) IDaaS (Identity as a Service) …クラウド上の各種サービスで利用される ID 情報などの統合管理と認証基盤を提供し、シングルサインオンを可能とするクラウドサービスのひとつ。
※4) EPP (Endpoint Protection Platform) …エンドポイント保護プラットフォームのこと。社内に入り込んだウイルスなどのマルウェアを検知して自動駆除などを行う機能をもつ。
※5) EDR (Endpoint Detection and Response) …ネットワーク配下に接続されているパソコンなどいわゆるエンドポイントを監視し、疑わしい挙動や脅威を検知して対策などを講じる機能もしくは方法のこと。
※6) SD-WAN (Software-Defined Wide Area Network) …ソフトウェア制御により広域ネットワークを運用管理する技術。従来のように現場に赴いて機器の設定や調整を行うのではなく、中央のソフトウェアで広域な WAN ネットワークの構築や設定、制御を行うこと。
※7) SIEM (Security Information and Event Management) …セキュリティ情報イベント管理。ファイアウォールなど複数のセキュリティ機器から情報を一元的に集めて分析を行い、同時に監視と驚異の検出、通知を行う仕組みもしくはその方法をさす。

<<製品に関するお問い合わせ>>
E-Mail: info@allied-telesis.co.jp
https://www.allied-telesis.co.jp

<<ニュースリリースに対するお問い合わせ>>
マーケティングコミュニケーション部
Tel: 03-5437-6042 E-Mail: pr_mktg@allied-telesis.co.jp

アライドテレシス株式会社　東京都品川区西五反田 7-21-11 第 2 TOC ビル