

2022 年 8 月 24 日

各 位

株式会社 JSOL

Illumio 社と提携し、ゼロトラストセグメンテーションソリューションの提供を開始

ーゼロトラストセキュリティを強化するマイクロセグメンテーションの実現ー

株式会社 JSOL(以下 JSOL)は、Illumio 社とパートナー契約を締結し、8 月より企業内ネットワークシステムのセキュリティを「マイクロセグメンテーション化」により強化する「ゼロトラストセグメンテーション ソリューション」の提供を開始しました。

本ソリューションにより、ゼロトラストセキュリティイニシアチブをさらに強化するゼロトラストセグメンテーションが、容易に実現可能となります。

【マイクロセグメンテーションとは】

「マイクロセグメンテーション」とは、ネットワークを細かくセグメント化することで、サイバー攻撃に対してセグメントごとの状況可視化やアクセスの遮断といった対応を容易にするものであり、攻撃者が企業内ネットワークに侵入した場合でも、ネットワーク内での攻撃者の横移動(ラテラルムーブメント)を防ぐことができ、セキュリティレベル向上に資するものと期待されています。

【企業ネットワークの潮流であるゼロトラストセキュリティについて】

近年、企業ネットワークは、守るべき情報資産にアクセスするものは信用せずに安全性を都度検証する「ゼロトラスト」アーキテクチャへの変換が進んでいますが、「ゼロトラストセグメンテーション」も「ゼロトラスト」アーキテクチャを実現するアプローチの一つとして位置付けられています。

2020 年 8 月に米国の国立標準技術研究所(NIST)が発表した「ゼロトラスト」に関する文書(*1)では、ゼロトラスト・アーキテクチャの 3 つのアプローチ方法が紹介されています。そのうち、「アイデンティティガバナンスによるアプローチ」と、「ネットワークインフラを使用したアプローチ」は、IDaaS 製品(*2)や SASE 製品(*3)の活用により実現可能となっており、日本国内でも導入事例が増えています。

一方 3 つ目の「マイクロセグメンテーションによるアプローチ」は、従来型のソリューションを用いる方法では、セグメントごとにファイアウォールを設置し、運用管理する必要があるため実現のハードルが高いとされ、導入が進んでいませんでした。

したがって、IDaaS 製品や SASE 製品の導入により「ゼロトラスト」アーキテクチャのネットワークを実現した企業のネットワークシステムは、一度マルウェアに侵入されると、マルウェアにラテラルムーブメント攻撃されるといった、セキュリティリスクが課題として残っていました。

また、データセンターを中心とする従来型のネットワーク構成を取る企業にとっては、クラウドサービスである SASE 製品はニーズに適合せず、オンプレミスのセキュリティ機器を活用した従来型のセキュリティ対策を実施するに留まっていました。

【Illumio 社「ゼロトラストセグメンテーション」製品の概要】

ゼロトラストセグメンテーションは、クラウドからデータセンター、エンドポイントに至るまで、ハイブリッド攻撃対象領域全体でワークロードとデバイスを分離する、急速に成長している最新のセキュリティアプローチです。

Illumio 社のプラットフォームは、業界初のクラウド・トゥ・グラウンドのゼロトラストセグメンテーションプラットフォームです。組織がワークロードの通信方法を確認し、ハイブリッド IT 全体の通信を許可または拒否するセキュリティポリシーを作成し、資産を分離して侵害の拡大を食い止めることを支援します。セグメントごとにファイアウォールを設置するといった従来型のソリューションとは異なり、Illumio 社のプラットフォームは容易に導入・運用管理でき、サイバーレジリエンスを向上させ、ランサムウェアのような日常的な攻撃が災害へと発展するリスクを低減します。

【JSOL ソリューションの概要】

JSOL は、SASE 製品や IDaaS 製品などを組み合わせて企業の「ゼロトラスト」ネットワークを構築、運用する「次世代ネットワークセキュリティソリューション」を従来から展開していますが、今回これに「ゼロトラストセグメンテーション ソリューション」を組み込む形でサービス提供することで、各企業の課題、ニーズにより適したネットワークシステムをご提供します。

検討段階においては、NIST の「ゼロトラストの原則」に基づいた現状分析を行い、対策ロードマップ作成を支援します。

設計・構築段階では、検討段階で作成した対策ロードマップを実現するために必要な製品の導入を行い、迅速、かつ確実に、マイクロセグメンテーションを含むゼロトラストネットワークセキュリティを実現します。

運用段階についても、セキュリティの監視や、ネットワークシステムの運用を 24 時間 365 日体制でサービス提供します。

本ソリューションで提供する主なメニューは、以下のとおりです。

1. 検討段階

・ゼロトラストアセスメントサービス

NIST が公開した「ゼロトラスト・アーキテクチャ」への準拠状況をアセスメントし、対策ロードマップ作成を支援。

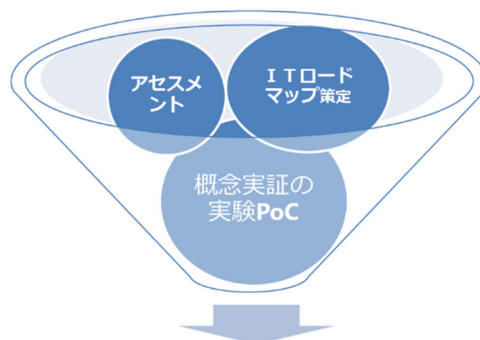
・ネットワークアセスメント&コンサルティングサービス

現有のネットワーク資料の確認や簡易ヒアリングから、構成やコストについて評価し改善策を提案し、将来を見据えた次世代ネットワーク策定を支援。

2. 設計・構築段階

・ネットワーク・セキュリティ構築サービス

広域ネットワーク(WAN) (*4)においては、2019 年にガートナーが提唱した、ゼロトラストを実現する



次世代クラウドネットワークセキュリティモデルである「SASE（＊2）」の構築。
構内ネットワーク（LAN）（＊5）については、
「ゼロトラストセグメンテーションソリューション」によりマイクロセグメンテーションを実現。
その他、IDaaS（＊2）、EDR（＊6）、NDR（＊7）等の組合せ導入を実施。

3. 運用段階

・マネージドセキュリティサービス（SOC（＊8））

24 時間 365 日体制でセキュリティ脅威を検知・分析。

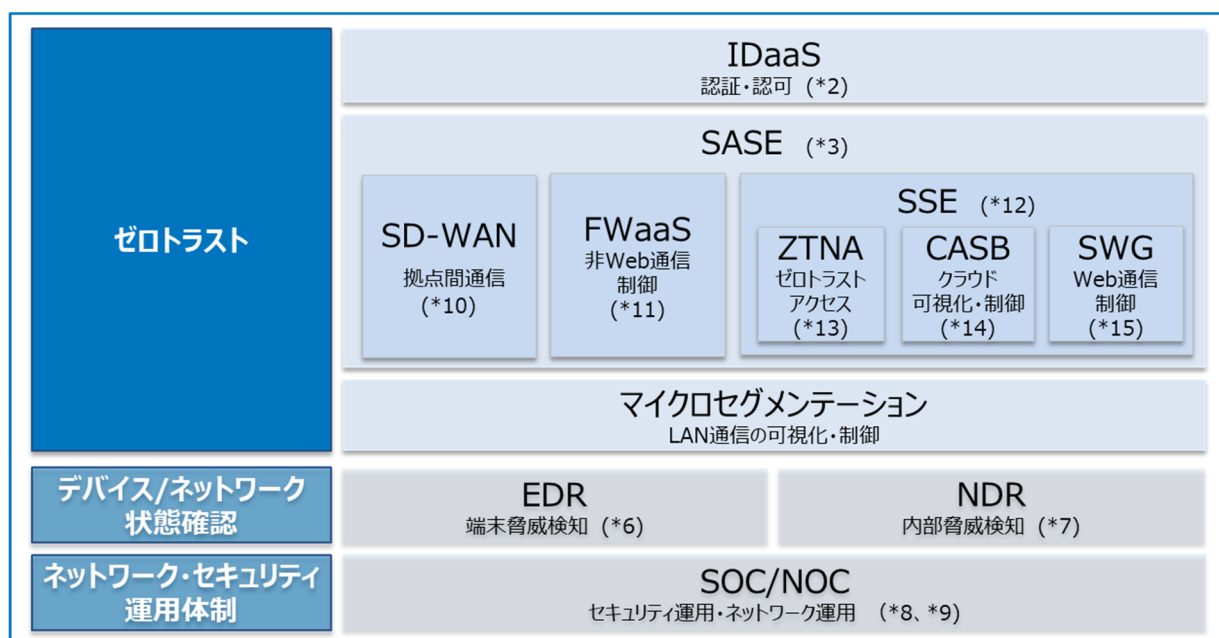
これまでの豊富な対応で培ったノウハウにより高精度かつ迅速な分析を実施。

ゼロトラスト型ネットワーク「SASE」の監視をサポート。

・ネットワーク運用サービス（NOC（＊9））

24 時間 365 日体制でネットワーク運用を実施。

アラート発生時の一次切り分けや復旧対応の他、ネットワーク基盤維持管理、構成管理、改善提案を行う。



次世代ネットワーク・セキュリティソリューション概要図

本ソリューションの詳細については、以下をご参照ください。

次世代ネットワーク・セキュリティソリューション

<https://www.jsol-platformservice.com/ns-solution.html>

ゼロトラストセグメンテーションソリューション

<https://www.jsol-platformservice.com/zerotrust-segmentation.html>

JSOL と Illumio 社が連携し、両社が培ってきたネットワーク、セキュリティに関する技術、ノウハウを結集することで、業種を問わず多くの企業のお客さまにゼロトラストセグメンテーションソリューションを提供していきます。

【Illumio 社の日本法人イルミオ ジャパン合同会社様からのエンドースメント】

セキュリティ侵害の頻度や重大性が高まるにつれ、セキュリティ担当のリーダーは侵害の影響を最小化することに焦点を当てた新しいアプローチに移行する必要があります。そのためには、侵害を前提とした考え方と、ゼロトラスト戦略に不可欠なゼロトラストセグメンテーションが必要です。弊社ソリューションであれば、ワークロードやデバイスがどのように通信しているかを確認して、通信を許可または拒否するセキュリティポリシーを作成し、資産を分離して侵害の拡大を阻止することが可能です。JSOL とのパートナー契約により、JSOL のお客さまのさらなるセキュリティ強化をサポートできることを大変嬉しく思います。

嘉規 邦伸(イルミオ ジャパン合同会社 代表執行役員社長)

脚注

*1 米国国立標準技術研究所(NIST)公開文書:

2020 年 8 月に米国国立標準技術研究所(NIST)が公開した文書「Special Publication(SP)800-207 ゼロトラスト・アーキテクチャ」。

保護すべきリソースを特定、整理していることや、従業員の所属や職責に応じたアクセス制御をリソース単位で認可していること、アクセスポリシーは一定ではなく状況に応じ動的に可変であることを要求。

*2 IDaaS: Identity as a Service

企業ネットワークやシステム、データにアクセスするユーザの認証、認可を行うクラウドサービス。

*3 SASE: Secure Access Service Edge

2019 年にガートナーが提唱した次世代クラウドネットワーク・セキュリティの実現モデル。包括的ネットワーク機能と包括的なセキュリティ機能を組み合わせることで、社内外に置かれた企業システムやデータへのセキュアなアクセスニーズをサポートするモデルや、それを実現するための製品の呼称。

*4 広域ネットワーク: WAN(Wide Area Network)

企業の各拠点や、インターネットに接続するためのネットワークシステム

*5 構内ネットワーク: LAN(Local Area Network)

企業の拠点構内のネットワークシステム

*6 EDR: Endpoint Detection and Response

PC 他の端末(エンドポイント)でのマルウェアなどの不振な挙動を監視し、迅速な対応を支援するソフトウェア。

*7 NDR: Network Detection and Response

企業ネットワーク上の通信を監視し、サイバー攻撃などの脅威を検知し、迅速な対応を支援するネットワーク機器。

*8 SOC: Security Operation Center

24 時間 365 日体制でセキュリティー脅威を検知・分析を行い、対応や対応策アドバイスを行う専門組織。

*9 NOC: Network Operations Center

24 時間 365 日体制でネットワークシステムの稼働を監視、運用する専門組織。

*10 SD-WAN: Software-Defined WAN

WAN をソフトウェアで制御し拠点間接続やクラウド接続などにおいて柔軟なネットワーク構成やトラフィックコントロールなどを実現する技術

*11 FWaaS: Firewall as a Service

通過させてはいけないネットワーク通信を阻止するファイアウォール機能をクラウド環境で実施するもの

*12 SSE: Security Service Edge

専用のクラウドプラットフォームから提供されるネットワークセキュリティーサービス群。
下記 ZTNA、CASB、SWG が含まれる。

*13 ZTNA: Zero Trust Network Access

社内のシステムやデータへのセキュアなアクセスを提供するための機能

*14 CASB: Cloud Access Security Broker

企業の従業員の外部クラウドサービスの利用の可視化したり、利用を制御する機能

*15 SWG: Secure Web Gateway

企業の従業員が社外のネットワークへのアクセスを安全に行うための機能

■株式会社 JSOL

(本社: 東京都中央区、代表取締役社長: 永井 健志)

<https://www.jsol.co.jp/>

JSOL は、ICT コンサルティングからシステム構築・運用までの一貫したサービスで、お客さまのより幅広いニーズにお応えできる ICT サービスコーディネーターです。

2009 年 1 月、NTT データ、三井住友フィナンシャルグループ、日本総合研究所との業務・資本提携により、社名を株式会社 JSOL に変更するとともに、NTT データグループおよび SMBC グループの一員として、お客さまのビジネスに貢献できる ICT ソリューションの提供に取り組んでいます。

※本リリースに記載されている内容は予告無く変更することがあります。

※本リリースに記載されている製品名、会社名は各社の商標または登録商標です。

【お問い合わせ先】

一般のお客さま

株式会社 JSOL プラットフォーム事業本部 梅沢

TEL:03-5859-6001 E-Mail:rfi@jsol.co.jp

報道関係者さま

株式会社 JSOL 経営企画本部 新開

TEL:090-4847-3065 E-Mail:webinfo@jsol.co.jp

JSOL CORPORATION