新たな脅威への対応まで『任せられる』。「Prisma SASE」で、組織のセキュリティ対策をシンプルに強化｜パロアルトネットワークス×Soliton OneGate

目次

ハイブリッドワークやクラウドへのシフトが多くの組織で進んでいく中、その変化によって生まれた『新たなセキュリティリスク』や、対策が追いついていない『隙間』を狙う攻撃が増加しています。人や端末、データがオフィスから外に出ていくことで、社内LANさえ守れば良いという従来の境界防御の意味合いは薄れ、いかなるネットワークやデバイスも信用しない「ゼロトラスト」という考え方に基づいたセキュリティ環境の構築が求められています。

そのような時代において、「デジタル時代の信頼性」を実現すべく、世界150か国以上でセキュリティソリューションを提供し続けているのが、パロアルトネットワークス株式会社（以下、パロアルトネットワークス社）です。特に、ゼロトラスト環境の構築に欠かせないSASE（Secure Access Service Edge）の代表的なソリューションのひとつである同社の「Prisma SASE」は、全てのコンポーネントが自社開発という特徴を持ち、国内外で唯一無二のポジションを確立しています。

現在のITセキュリティにおける共通課題に、なぜゼロトラストの考え方が、SASEソリューションが有効なのか。中でも「Prisma SASE」の強みとは。

本記事ではパロアルトネットワークス社 Business Principal, SASE GTMの和田一寿氏へのインタビューを通じて、「Prisma SASE」が導入企業にもたらすメリットや、中小企業におすすめの導入プラン、また、株式会社ソリトンシステムズ（以下、ソリトン）が提供する「Soliton OneGate」との関わりについてご紹介します。

複雑なセキュリティ対策をまとめて実現できるSASE

世の中のIT環境が多様化したことで、ITセキュリティにおける脅威もまた多様化してきました。リモートアクセス時やクラウドサービス利用時など、組織が考慮しなくてはならないセキュリティポイントは、際限なく増加しています。

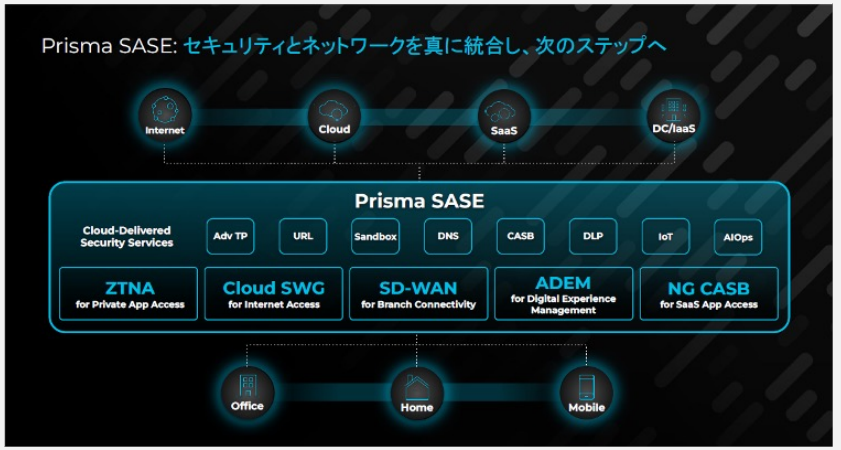
様々なセキュリティ脅威が、様々な場所で顕在化する現在、セキュリティ対策に関する考え方にも変化があらわれています。和田氏は次のように語ります。

“従来のセキュリティ対策は、外部ネットワークとの境界線にファイアウォールやIPSなどのセキュリティ措置を施し、社内ネットワークを守る「境界型」がほとんどでした。しかし境界型セキュリティは、一度社内ネットワークへ侵入を許せばその後の対応が難しいほか、クラウドの浸透などにより、そもそも守るべきデータやシステムが社外に点在するという現状にもそぐわなくなりつつあります。

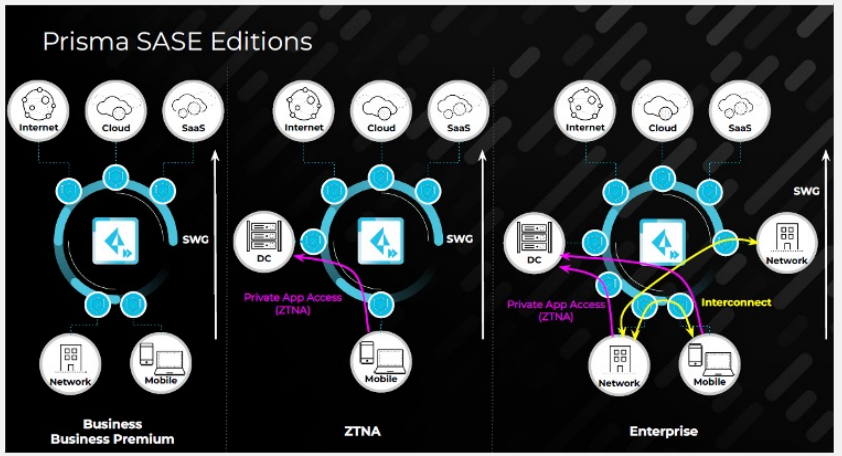
この状況を受けて、注目を集めているのが「ゼロトラスト」です。いわば性悪説の前提に立ち、全てのデジタルコミュニケーションを疑ってセキュリティ対策を行う考え方で、「境界型」の前提である境界線自体が曖昧になっている今、より重要性を増しているといえるでしょう。”

とはいえ、セキュリティ対策で「ゼロトラスト」の考え方を実践しようとすると、あらゆる領域を保護しなければならないため、非常に困難です。和田氏は、「ゼロトラスト」実現の難しさについて、次のように語ります。

（図１）



（図２）



“増え続けるセキュリティ脅威に対抗すべく、ソリューションもまた多様化しています。今や、従来的なファイアウォールやIPS、アンチウィルスに加え、DNSセキュリティ、サンドボックス、CASBなど、この他にも数多くの要素技術を組み合わせて運用することが求められるようになってきているのです。

しかし、一つ一つをつぎはぎで追加し、管理するのは、あまりにも煩雑で現実的ではない。ここに、近年のセキュリティ対策の根本的な課題があります。”

そこで有効な手立ての一つが、SASEです。SASEは、ネットワークとセキュリティの機能をクラウド上で包括的に提供する、いわばセキュリティ対策の統合管理ソリューション。和田氏はそのメリットとして、「増え続けるセキュリティの要素技術を、シンプルにまとめて管理できること」を挙げます。

類似の統合管理ソリューションであるSSE（Security Service Edge）が、モバイルアクセスのセキュリティ機能に特化しているのに対し、SASEはモバイル環境とオフィス環境、双方を包含したセキュリティ対策を実現するものとして区別されます。オフィス内外を問わず、どの環境下でも、会社の全てのデジタルコミュニケーションを一貫したセキュリティポリシーで検査、モニタリングできるようにするのがSASEというわけです。

すべてのコンポーネントが自社開発の「Prisma SASE」なら、新しい脅威にもすばやく対応

「ゼロトラスト」の考え方に基づき、包括的なセキュリティ対策を提供するSASE。パロアルトネットワークス社の「Prisma SASE」もその一つです。

本社や支社、海外拠点、モバイルといった、現代のあらゆる業務ロケーションと、社内システムやクラウドサービス、データセンターとを結びつけ、すべてのポイントあるいは通信経路において、最適なセキュリティ要素と一貫したポリシーを適用します（図1）。

特に、新たなセキュリティ脅威への対応スピードにおいては、他を寄せ付けない優位性があると和田氏は語ります。

“新しい攻撃手法に対する防御策は、必ずしも一つではなく、複数の要素技術に必要なシグネチャや機構を組み込むことが多いです。そのため、インシデントが発生した際は即座に解析を行い、適切な対策を各コンポーネントに適用し、実装する必要があります。

しかし、新規の脅威を解析するには相当な技術力を要しますし、サードパーティーの要素技術を使用しているSASEの場合、各コンポーネントに新たなルールセットを適用するのに時間がかかる、もしくは実装できない可能性がある上に、そもそも権限を持っていません。

当社では、インシデント発生時、セキュリティコンサルティングの精鋭チーム「Unit 42」が解析に当たり、迅速に対策を導き出します。また、「Prisma SASE」で提供されるセキュリティ要素技術は全て自社で開発しているため、全コンポーネントに対して迅速に対策を配信・適用することができるのです。”

次に和田氏が特長として挙げるのは、「AI（人工知能）/ML（機械学習）を活用したセキュリティ脅威の検知」です。

“ネットワーク侵入から情報流出までにかかる時間は、数年前までは平均一か月程度だったのが、現在はわずか数時間にまで短縮されています。これでは、いかにインシデント解析と対策適用を早めても、間に合わないケースが出てくるでしょう。

そこで現在は、蓄積されたデータをAIに学習させ、攻撃パターンを予測して自動的にブロックすることにも注力しています。”

AIやMLの活用には、膨大なデータの収集と処理が必要不可欠。その点、2005年の創業以来グローバルでサイバーセキュリティを牽引してきたパロアルトネットワークス社には、圧倒的な脅威インテリジェンスが形成されているため、一日に数十億件もの攻撃をブロックすることができているのです。

中小規模のユーザーにも。おすすめの導入プランを用意

「Prisma SASE」は大手やエンタープライズ企業向けのソリューションと思われがちですが、中小企業向けに価格を抑えたビジネスプランもあります。和田氏は、「セキュリティ脅威に晒されているのは、中小企業も同じ」とした上で、次のように説明します。

“Prisma SASEエディションの「Bussiness」や「Bussiness Premium」では、拠点間通信がサービス対象外となるものの、その他一つ一つの要素技術は、最上位の「Enterprise」と同様です。モバイルを対象として接続先がクラウド、IaaSやSaaSのみとなるような組織の場合は、「Bussiness」や「Bussiness Premium」で、強固なセキュリティを構築できます（図2）。

また、自前のデータセンターにアクセスが必要な場合は、「Bussiness」や「Bussiness Premium」にZTNA（Zero Trust Network Access）Connectorを付帯させれば、費用を抑えながら、モバイルユーザーとデータセンター接続を包含したセキュリティ体制を整備することが可能です。”

認証ソリューション「Soliton OneGate」と組み合わせ、「Prisma SASE」の入り口を強化

日々進化し続けるサイバー攻撃に対して、予防と対処を任せることができる統合管理ソリューション「Prisma SASE」。このソリューションへの橋渡しとなるのが、ユーザーやデバイスの認証情報を管理し、接続可否を判断するIdP（Identify Provider）です。

様々なサービスが展開されていますが、中でも「Soliton OneGate」は、デジタル証明書を用いた多要素認証に大きな優位性を持つIdPサービスです。正規の証明書を持たないユーザーはログイン画面にたどり着けないため、一部の多要素認証を突破してしまうフィッシング攻撃や、ブルートフォース攻撃、リプレイ攻撃などにも高い耐性があります。ソリトンの光井・前川は、「Prisma SASE」と「Soliton OneGate」を組み合わせる事例が、徐々に増えてきていると語ります。

“IDの認証は、いわばSASEの入口です。攻撃者の侵入を防ぐ、最初の砦といえます。

しかしあるお客様は、既存の認証サービスで「パスワード変更後も旧パスワードでログインできた」「他人のアカウントで接続された」といったトラブルを経験されていました。そこで、デジタル証明書を安全かつ簡単に展開できる「Soliton OneGate」を導入し、「Prisma SASE」の入口をさらに強固な多要素認証で守ることで、万全のセキュリティ環境の構築につなげました。

今後もソリトンは、IdPとしての高い運用性と、『デジタル証明書』の活用に強みを持つ「Soliton OneGate」を通じて、「Prisma SASE」との協業をより深めていければと思っています。”

「Prisma SASE」だからこそ、事業成長への貢献も

一方、和田氏は、セキュリティ強化のさらに先を見据えています。

“コロナ禍におけるSASE導入に関しては、緊急事態宣言下でのテレワーク対応という、いわば対症療法的かつ短期的な需要が目立っていました。

ただ、コロナ禍が落ち着いてきた今は、「Prisma SASE」を共通基盤として、ビジネスを刷新しようという動きが広まってきています。つまりより中長期的な視点で、「Prisma SASE」が活用され始めているのです。

例えば、最近増えているのが「Prisma SASE」でネットワークを簡素化することにより、金銭的・人的負担を軽減し、余ったリソースを別の経営課題に利用しようとするケース。あるいは、「Prisma SASE」の技術を用いて社員が安全に生成AIを活用できる仕組みを作り、事業の推進力を上げようとしているといったケースもあります。「Prisma SASE」には、顧客のビジネスを加速化させるポテンシャルがあると実感しています。

セキュリティ基盤の強化にとどまらず、様々な組織がその事業課題を解決し、成長につなげていくことでしょう。”

謝 辞

パロアルトネットワークス様、インタビューにご協力いただき誠にありがとうございました。

これからもソリトンシステムズは、引き続き国産のITセキュリティメーカーとして、企業の安全な経済活動に貢献してまいります。

パロアルトネットワークス株式会社 様

お問い合わせはこちら

https://www.paloaltonetworks.jp/company/contact-sales