網屋 「Verona SASE」

中堅・中小企業のゼロトラストを実現！導入・運用の負担を軽減するSASEとは？

「運用負荷“ゼロ”でゼロトラストを実現」。網屋の「Verona SASE」は導入後の運用・管理をセキュリティのプロが代行することで、大企業だけでなく、中堅・中小企業でも容易に使いこなせる。ライセンス体系は利用規模に合わせて3種類とシンプルで、コストも抑えられる。中堅・中小企業にとってハードルの高かった、「境界型」から「ゼロトラスト」への移行を可能にする。

ネットワークとセキュリティをクラウド上で一元的に運用・管理するSASE(Secure Access Service Edge)は、大企業向けで、高度なIT人材と多額のコストが必要であった。

今回はこれらの課題を解決するサービスが登場したのでご紹介しよう。

サイバーセキュリティプロバイダーの網屋が7月3日に提供開始した中堅・中小企業向けの「Verona SASE」だ。

なぜ今、中堅・中小企業向けなのか。

「中堅・中小企業がテレワーク時に導入したVPNの脆弱性を狙った攻撃が急増しています。ネットワーク機器を運用・管理する人材が不足しているのが原因です。中堅・中小企業を踏み台に大企業にも被害を及ぼしていることから、この課題を解決したいと考えました」と網屋 執行役員 マーケティング部 部長の別府征英氏は説明する。

従来、企業のセキュリティ対策は、社内ネットワークと外部ネットワークの境界を防御する「境界型」が中心だった。しかしコロナ禍によって、働く場所が多様化し、またWeb会議システムなどのSaaS導入が進んだことから、社内外の区別なくあらゆる端末や通信を検証・監視する「ゼロトラスト」へと移行しつつある。このゼロトラストセキュリティを実現するソリューションがSASEだ。

ただ、中堅・中小企業がSASEを導入・運用するには人材・コスト面のハードルが高く、普及が進んでいなかった。そこで、中堅・中小企業へSASEの裾野を広げることを目的に開発されたのがVerona SASEというわけだ。

Verona SASEの最大の特長は、簡単かつ短期間で導入できることである。

一般的にSASE導入は、既存環境の棚卸から始まって半年〜1年という大規模プロジェクトとなる。高度なIT人材も必要だ。これに対し、Verona SASEは

（右から）網屋 執行役員 マーケティング部 部長 別府征英氏、マーケティング部 ネットワークセキュリティTM 吉川真希氏、データセキュリティ事業部 セキュリティサービス部 伊東一陽氏

ヒアリングシートに記入するだけ。複雑な作業は網屋に任せられるので、最短2週間で導入することが可能だ。

また、導入後の設定管理や運用もネットワーク・セキュリティのプロがすべて代行する。障害や不具合が発生した際には、その原因発見と対処、適切な設定指南を行ってくれる。このため情報システム担当者が不在だったり、数人しかいない企業でも負担なく運用することができる。

社内ネットワークもアクセス制御 Verona Cloud Consoleで一括管理

「従来のSASEは、機能が多く複雑すぎることも中堅・中小企業の導入を阻んでいます」と別府氏は指摘する。

その点、Verona SASEは中堅・中小企業のゼロトラストセキュリティに必要な機能に絞り込んでいる。

具体的に何ができるのか。1つめに、リモートワークにおけるセキュリティを実現する。

Verona SASEは、クライアント証明書をベースにした独自の認証システムを採用している。

Verona SASEに接続する際、クライアントから認証要求を出すと、クラウド上の管理センターで認証を行い、接続を許可された端末の情報のみがVerona SASEに送られ、通信を開始する。また、ダイナミックポートコントロール機能により、正規ユーザーからの認証要求があったときだけ応答する。

「従来のVPNと違い、正規かつ認証されたユーザー以外は接続できません。ログインするまで総当たりにパスワードを入力しても認証を突破されないので、不正アクセスを防止します」と網屋 データセキュリティ事業部 セキュリティサービス部の伊東一陽氏は胸を張る。

さらに、社内ネットワークの中もIPアドレスで接続を制限することができる。

例えば、営業部のみサーバーAへのアクセスを許可し、開発部など他部署はアクセスを禁止するといった設定を行える。万が一、不正ユーザーがVPNに接続しても横展開を防ぐことができる。

2つめに、セキュアなインターネットアクセスを実現する。

テレワークの普及とともに、企業が把握していないクラウドサービスを社員が業務に利用するシャドーITの問題が顕在化している。Verona SASEはアプリケーションレベルで可視化・制御することで、使用を許可していないクラウドサービスの無断利用をブロックする。もちろん、不適切なサイトへのアクセスを監視・制御するURLフィルタリング、マルウェアなどを検知しウィルス感染を未然に防ぐアンチウィルスといった基本機能も備える。

3つめに、回線のひっ迫を解消する。

特定のクラウドサービスを各拠点から直接インターネット経由で接続可能にするローカルブレイクアウト機能により、回線負荷を軽減できる。

4つめとして、ファームウェアの自動更新により、不正侵入を予防する。

脆弱性が見つかると、セキュリティベンダーからファームウェアのアップデートがリリースされるが、中堅・中小企業では手が回らず放置されてしまいがちだ。その点、Verona SASEは網屋のエンジニアがファームウェアを随時更新するので、脆弱性からの侵入を防ぐ。

これらの機能のステータス情報は、Verona Cloud Consoleと呼ばれる管理画面上にまとめて表示される。企業の管理者は、遠隔の拠点やテレワーク中のクライアントも含めて、スムーズに状況を把握することが可能だ。

3種類のシンプルなライセンス体系 個別テナントでセキュアに

Verona SASEのライセンスは、利用規模に合わせて3タイプを用意する。

100ユーザー程度のベーシックは月額21万円、100〜500ユーザー向けのスタンダードは同40万円、500〜1000の大規模ユーザーを対象とするハイスペックは同60万円。いずれも初期費用は5万円。オプションとして、年額15万円でログ保管を1年延長することができる。

「一般的なSASEは、拠点コストや機能別コスト、製品サポート費など様々な費用が上乗せされますが、Verona SASEは月額サービス費用にすべて含まれており、コストも抑えられます」と網屋 マーケティング部 ネットワークセキュリティTMの吉川真希氏は述べる。

プランに応じて、SASE側のゲートウェイが2〜4台割り当てられるので、拠点が多い場合は拠点間接続重視、リモートで働く社員が多い場合はリモート接続重視というように、状況に合わせて接続先を設定することができる。

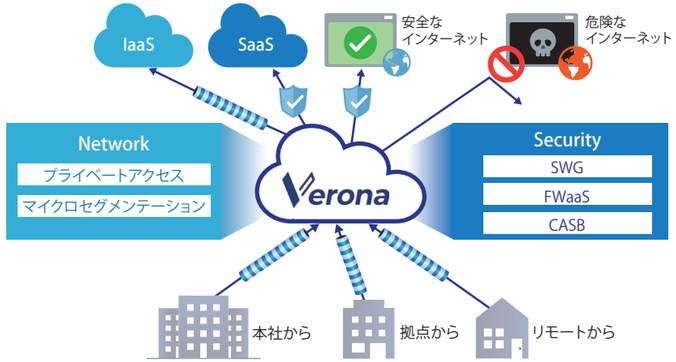
また、Verona SASEはクラウド上に顧客ごとの個別テナントを作成する。複数ユーザーと同一システムを利用するマルチテナントと違い、データが混ざったり、情報が漏えいするなどのリスクもない。

リーズナブルでありながら、細やかな配慮がされたサービスといえるだろう。

セキュリティ対策に不安のある中堅・中小企業は、Verona SASEを検討することをぜひお勧めしたい。

お問い合わせ先
株式会社網屋
ネットワークセキュリティ事業部
TEL：03-6822-9995
E-mail：infra-sales@amiya.co.jp

図表1 「Verona SASE」の全体イメージ



図表2 「Verona SASE」のポイント