POINT OF VIEW

セキュリティ ドリブン ネットワーキング戦略の要件（SD-WAN から SASE まで）

デジタルイノベーションによって、ネットワークを再設計し、社員と顧客のユーザーエクスペリエンスを向上させることがあらゆる組織に求められるようになりました。かつてはネットワークエッジの限定されたポイントに限られていた境界も、現在は IT インフラストラクチャ全体に拡大し、データセンター、広域ネットワーク（WAN）、ローカルエリアネットワーク（LAN）、クラウドエッジにおいては新しい要件が追加されるようになりました。また、COVID-19 のパンデミックによって、場所や時間を問わず安全なリモートアクセスを柔軟かつ広範に提供することを含めた事業継続計画が必要になっています。

セキュリティの脅威はますます巧妙になり、頻度も増加しています。2020 年のデータ漏えいの 3 分の 1 以上はソーシャルエンジニアリングによるものでした[1]。このことからも、ネットワークを再設計してセキュリティを強化することはすべての企業にとって重要です。

セキュリティ ドリブン ネットワーキング戦略では、すべてのエッジとユーザーが接続された環境で本社から支社、クラウドまでのネットワーキングとセキュリティの統合が加速されます。また、今日の動的な環境を効果的に防御しながら、社員と顧客の優れたユーザーエクスペリエンスを維持できます。

セキュリティを中核としたネットワークではハイパースケール、マルチクラウド、5G などの次世代コンピューティングでデジタルイノベーションの進化、拡張、適応が簡略化されます。ネットワーキングとセキュリティを統合することで、いつでもどこでも柔軟にセキュリティを提供できます。

セキュリティ ドリブン ネットワーキング戦略の重要な要素

セキュリティ ドリブン ネットワーキング戦略は以下の 3 つのニーズに対応します。

- ネットワークに接続するユーザーの外部および内部リスク管理
- オフネットワークのユーザーに対するクラウドネイティブセキュリティの柔軟な提供
- WAN コストの削減とユーザーエクスペリエンスの向上

セキュリティ ドリブン ネットワーキングを実現するための最初のステップは、**カスタム SPU（Security Processing Unit）**や ASIC の適用です。それによってアプリケーション制御、ファイアウォール、侵入防止システム（IPS）などの**すべてのセキュリティ機能をネットワークファイアウォールなどのソリューションに統合**できます。また、ネットワーキングとセキュリティの再設計が加速され、パフォーマンスを損なうこともありません。必要な機能には、安全な SD-WAN、次世代ファイアウォール（NGFW）、IPS、SSL インスペクション、アプリケーション制御、Web フィルタリング、ウイルス対策、マルウェア対策、サンドボックス、セグメンテーションなどがあります（多くのファイアウォールは動的な内部セグメンテーションに必要な処理のオーバーヘッドに対応できないため、最後の項目はセキュリティ ドリブン ネットワーキング戦略にとって特に重要です）。

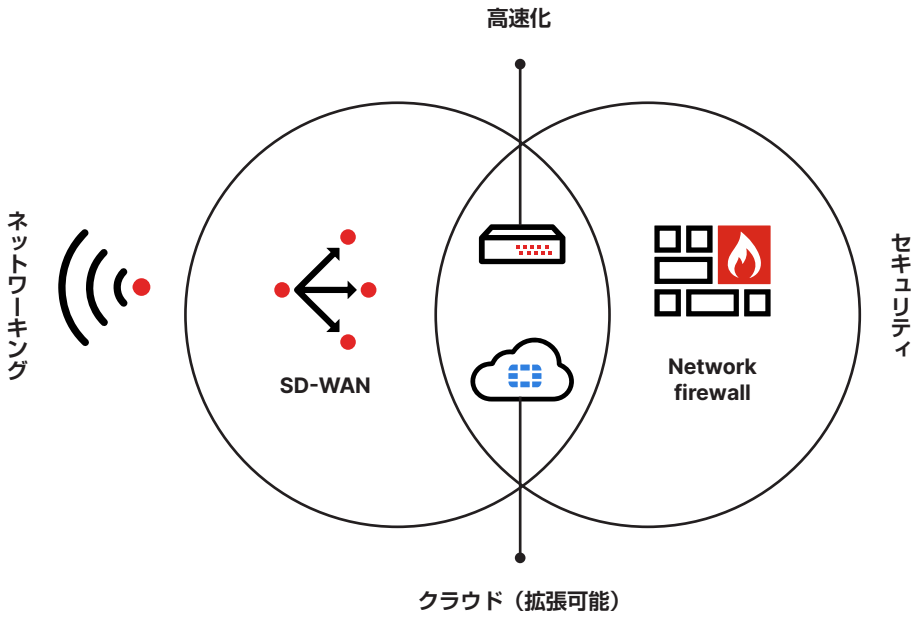
専用のクラウドアーキテクチャによって、クラウドファーストの組織や柔軟なソリューションの導入が必要な組織のセキュリティとネットワーキングの統合も可能になります。

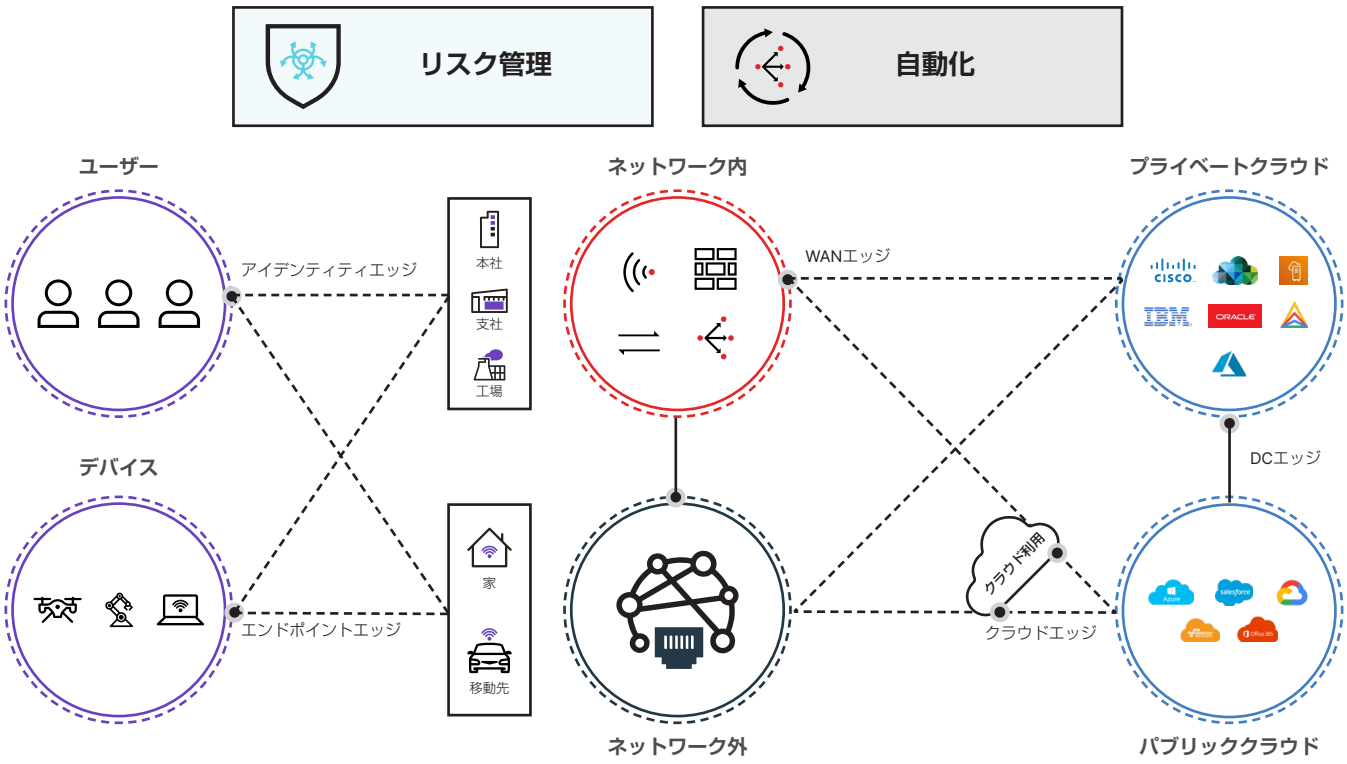
ネットワークファイアウォールソリューションは今後、**ハイパースケールのハイブリッド型データセンターと 5G のパフォーマンス要件もサポート**する必要があります。エレファントフロー、エッジコンピューティング、HDTV などのリッチメディアトラフィックの保護、5G ネットワーク、動的コアセグメンテーションなどの新しい高パフォーマンスのイノベーションには、NGFW の業界最高レベルのパフォーマンスが必要です。ソリューションによっては高パフォーマンスに対応するように設計されていないため、高額の費用をかけても将来のイノベーションに対応できるとは限りません。

セキュリティ ドリブン ネットワーキング戦略では、NGFW デバイスにエンタープライズクラスの SD-WAN を統合して WAN エッジを変革します。SD-WAN テクノロジーにセキュリティを追加するのではなく、両者が完全に統合されるため、**SD-WAN** のセキュリティが強化されます。SD-WAN のセキュリティ強化のアプローチには人工知能（AI）を利用した予測分析、直感的なオーケストレーション、自己修復も含まれます。

また、緊密な統合によって有線と無線のネットワークエッジにセキュリティを拡張し、幅広い LAN エッジに一貫してセキュリティを適用する必要があります。これらは、アクセスエッジとネットワークエッジにまでセキュリティで保護された、**セキュリティとレスポンスに優れたネットワークにとって不可欠**です。

これらのエッジは**一元管理**によって複雑さを軽減し、自動化によってネットワークの機敏性を高めます。





クラウドエッジの保護に最適な基盤：SASE

2020 年以降、セキュリティ ドリブン ネットワーキングには SASE（セキュアアクセスサービスエッジ）が含まれるようになりました。SASE は組織のセキュリティ ドリブン ネットワーキング戦略に合わせてネットワークセキュリティ機能と WAN 機能を組み合わせ、今日の動的なアクセスとそのセキュリティのニーズに対応するための新しいフレームワークです。SASE は、特にクラウドエッジにおいて、すべてのデバイスにセキュリティを提供し、リモートユーザーとモバイルユーザーを保護する上で重要な役割を担います。

SASE は一般的にクラウドコンピューティングに分類されますが、SASE をネットワークに効果的に統合するには物理ソリューションとクラウドベースのソリューションの両方が必要になります。これには SASE の接続、ネットワークアクセス制御、エッジセキュリティデバイスの組み合わせ、SD-WAN 物理デバイス（特にセキュリティのフルスタックを含むデバイス）などが含まれ、支社の無線 LAN コントローラーや Wi-Fi アクセスポイントなどのテクノロジーとの統合が必要になる場合もあります。SASE に重要な利点は、場所を問わず常時セキュリティを適用して**リモートユーザーを保護**できることにあります。また、ユーザーは業務に最適なクラウドエッジを低レイテンシーのネットワークで使用できるため、ユーザーエクスペリエンスも生産性も向上します。

SASE とセキュリティ ドリブン ネットワーキング戦略は同じものではありません。セキュアな SASE ソリューションとは、SASE の一般的な定義[2] に従った重要なクラウドベースの保護に加え、ネットワークセグメンテーションやコンプライアンスの維持に対応する必要があります。クラウドベースのセキュリティでは、トラフィックをクラウドに転送して検査しない限り、こういったニーズに対応することはできません。

そのようなニーズへの対応を実現することで初めて、SASE が完全なセキュリティ ドリブン ネットワーキング戦略の基盤となり、あらゆる組織が必要とするセキュリティとパフォーマンスが提供されるのです。

[1]「2020 Data Breach Investigations Report」、Verizon、2020 年 5 月（英語）：https://www.verizon.com/business/resources/reports/dbir/

[2]「The Future of Network Security Is in the Cloud」、Gartner、2019 年 9 月 13 日（英語）：
https://www.gartner.com/en/documents/3957375/invest-implications-the-future-of-network-security-is-in

フォーティネットジャパン合同会社

〒106-0032
東京都港区六本木 7-7-7　Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ