SOLUTION BRIEF

# フォーティネット セキュア SD ブランチで支社のネットワークエッジを保護

## 概要

デジタルトランスフォーメーション（DX）によって支社のネットワークは非常に複雑化し、攻撃に対して脆弱になっています。そのため多くの企業が複数のポイント製品を導入して次々と現れる新たな脅威に対応しています。しかしこのアプローチでは支社のインフラストラクチャの複雑化が進み、コスト、労力、脆弱性がさらに増大します。この問題に対処するため、支社では、WANエッジ、アクセスレイヤー、エンドポイント全体でネットワーキングとセキュリティ機能を統合する必要があります。フォーティネットセキュアSDブランチソリューションはセキュアプラットフォームにネットワークアクセスレイヤーを統合し、ネットワークとネットワークに接続されたすべてのデバイスに対する可視性とセキュリティを提供します。

**IT 意思決定者の 64% が自社の SaaS 導入スピードがセキュリティ確保のスピードよりも遅いと考えている。[1]**

**サイバー攻撃の 25% が 2020 年までに IoT を標的とすると予測された一方で、IoT デバイスの保護に充てられる IT セキュリティ予算は 10% 未満。[2]**

**NSS Labs が推奨するセキュア SD-WAN[3]：**

- 侵入を 100% ブロックし、99.9% のセキュリティ有効性を達成
- 業界で最も優れた TCO（所有コスト）—競合他社に比べ 10 倍の優位性
- テストされたソリューションの中で最も高い VoIP/ ビデオアプリケーションのエクスペリエンス品質

## 拡大する攻撃対象領域への対応

IoT（Internet-of-Things）デバイス、SaaS（Software-as-a-Service）アプリケーション、デジタルボイス/ビデオツール、BYOD（bring-your-own-device）エンドポイントを含むDXテクノロジーの急速な導入により、支社において保護を要するネットワークエッジの数が増えました。ネットワーク自体と支社インフラストラクチャを保護するためのポイントソリューション製品はいずれも複雑化し、管理コストもかかるようになりました。

コネクテッドな電子事務用品、照明や空調、社員の個人的なフィットネス製品に至るまで、こういったIoTの増加はネットワークに接続されるデバイス数を大幅に増加させています。その中にはセキュリティや可視性が低いものも多々あります。

## フォーティネット セキュア SD ブランチソリューション

他では得られないコストパフォーマンスで、ネットワークセキュリティに対して広範で統合·自動化されたアプローチを提供します。セキュア SDブランチはネットワークの新たなエッジにシームレスに拡大し、非常に優れたパフォーマンスと信頼性を提供しながら、支社全体の攻撃対象領域を一元管理し、把握できるようにします。

セキュアSDブランチはネットワーキングとセキュリティ機能を単一のソリューションに統合し、分散された環境をシームレスに保護します。WANエッジから支社のアクセスレイヤー、あらゆるエンドポイントデバイスまで支社の重大なリスクをすべて網羅します。そしてフォーティネットのセキュアなSD-WAN機能を有線·無線ネットワーク全体に拡大すると共に、支社のインフラストラクチャ管理を簡略化します。

フォーティネット セキュア SDブランチには他社製品と大きく異なる点がいくつかあります。1つめはセキュリティドリブンネットワーキングが可能だという点です。FortiGateの次世代ファイアウォール（NGFW）と広範なフォーティネット セキュリティ ファブリック アーキテクチャを使用してネットワークアクセスレイヤー全体を保護します。これにはFortiAP（セキュアワイヤレスアクセスポイント）や、FortiLink（セキュアEthernet）を使用しているFortiSwitchなどのフォーティネットソリューションが含まれています。FortiNACネットワークアクセスコントロール（NAC）ではIoTデバイスの可視化、検出、コントロールに加え、トラフィック分析によるアノマリ検知の追跡機能も利用できます。[4]

フォーティネットセキュアSDブランチにはセキュリティ、ネットワークアクセス、SD-WANを単一画面で管理する機能も含まれていますが、FortiManagerソリューションではゼロタッチ導入によって大規模な管理を行うことができます。セキュリティとネットワーキング用の統合インタフェースを使って、最小限のTCOで限られたIT管理者の負担を軽減することができます。

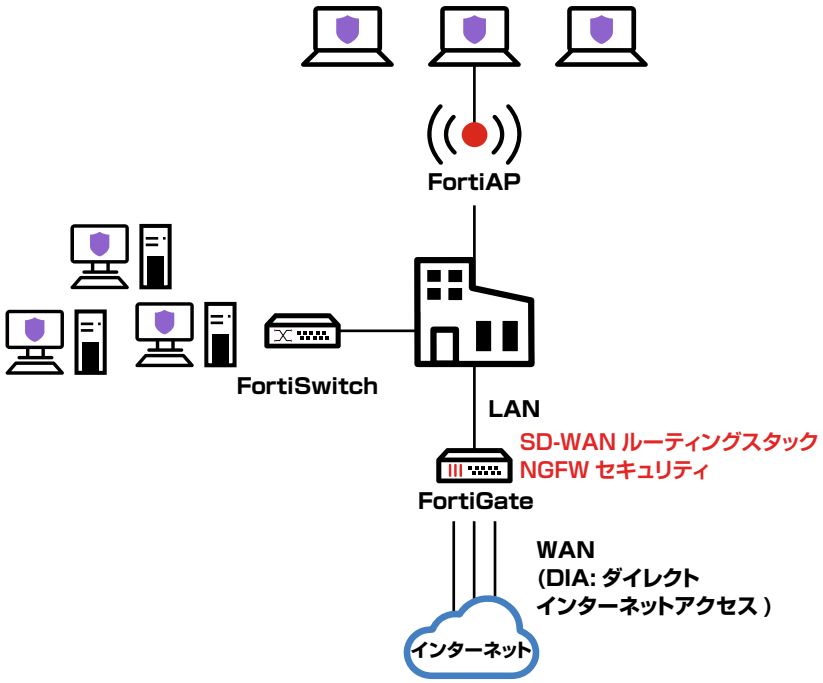


図 1：セキュア SD ブランチによる WAN と LAN インフラストラクチャの統合

**セキュリティドリブン ネットワーキング：**

- 後付けではないセキュリティ
- 標準でネットワークに組み込み
- 統合プラットフォームソリューションの一部

**全世界の SD ブランチ市場は 2023 年までに 32 億 7 千万ドル規模に達する見込み。[5]**

**「SD ブランチの最大の利点は運用上のアジリティだ。IT チームは新しい拠点向けに network branch-in-a-box（パッケージ化されたネットワークブランチ）ソリューションを迅速に導入、プロビジョニングすることができる。」[6]**

## セキュア SD ブランチがネットワークエンジニアリング・運用チームにもたらすメリット

セキュアSDブランチソリューションの主な利点は、支社でのセキュリティ強化です。すべてのWANエッジ、支社のアクセスレイヤー、全エンドポイントデバイスにグローバルポリシーを適用できます。WANとLAN環境を統合することで、セキュリティとネットワークパフォーマンスの両方をアクセスレイヤーに拡大することができます。さらにネットワークアクセスの際のIoTデバイスのディスカバリ、分類、セキュリティを自動化することもでき、定義されたビジネスロジックに基づいてアノマリ検出と修復プロセスも自動化します。そして最後に、分散された企業や組織が新たなオフィスや地理的拠点に迅速に運用を拡大できるというメリットもあります。

セキュアSDブランチはオンサイトでのリソースニーズを減少させ、結果的にTCOを下げることもできます。SDブランチはファイアウォール、スイッチ、APを単一のソリューションに統合します。単一画面での管理機能によってセキュリティとネットワークレイヤーの可視性を組み合わせることで、スタッフ効率を最大化し、プロアクティブにリスク管理を行うことができます。ゼロタッチ導入機能では最初のセットアップと長期的なビジネス拡大に伴う負担を軽減できます。

## 支社ネットワーキングに対するセキュリティドリブンアプローチの定義

支社ネットワークの継続的な進化はセキュリティ上の課題をもたらしています。リモート拠点には固有のリスクに対応できる独自の防御策が必要です。フォーティネット セキュリティ ファブリックの一部であるセキュアSDブランチは、セキュリティドリブンネットワーキングを提供します。さらに、セキュアプラットフォームにネットワークアクセスレイヤーを統合しネットワークとネットワークに接続されたすべてのデバイスに対する可視性とセキュリティを提供します。

[1] Conner Forrest、「企業によるSaaSの導入スピードが速すぎて、正しく保護することができない。」、TechRepublic、2018年4月10日。

[2] 「2020年にはサイバー攻撃の25%がIoTに到達する。」、Retail TouchPoints、2019年3月21日にアクセス。

[3] Nirav Shah、「Fortinet Secure SD-WANは永続的なパフォーマンスを提供、NSS Labsが推奨」、Fortinet、2018年8月9日。

[4] FortiNACバージョン8.6リリースで提供。

[5] 「全世界のSD-Branch（固定サイト、モバイルオフィス）市場、2018年～2023年 - 市場は32億7千万ドル規模に到達予定」、PR Newswire、2018年8月21日。

[6] Lee Doyle、「SD-Branch:概要と必要性」、Network World、2018年1月23日。

**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



SB-ky-sd-branch-202205-R1