SOLUTION BRIEF

従業員のテレワークを支援する大規模なセキュアリモートアクセス

概要

企業組織は、疾患、洪水、台風、停電など様々な緊急事態が発生する可能性に直面しています。潜在的な災害に備え、困難に遭遇した場合でもビジネスオペレーションを確実に遂行するためには、事業継続計画の導入が不可欠です。

事業継続計画の立案に際して考慮すべき重要事項の一つに、企業はオフィスにおける通常のオペレーション体制を維持できない可能性があることが挙げられます。事業の継続と従業員の安全の両方を確実に達成するためには、テレワークを実践する従業員を支援する環境作りが不可欠です。フォーティネットは、従業員のテレワークを支援する統合ソリューションを提供します。FortiGate 次世代ファイアウォール（NGFW）は、IPsec 仮想プライベートネットワーク（VPN）を OS 標準でサポートしているため、従業員はリモート環境から安全に企業ネットワークへ接続することができます。FortiClient が提供するエンドポイント保護、そして FortiAuthenticator による MFA（多要素認証）を活用することで、企業組織は従業員のテレワークを支援すると同時に事業オペレーションを継続させることが可能になります。

企業の事業継続や災害復旧の計画においては、安全なテレワークのサポート能力が不可欠です。停電などの緊急事態が原因でオフィスにおける通常のオペレーション体制を維持できない可能性があるほか、疾患や天災などの影響で従業員が安全にオフィスへ出社できなくなることもあります。

このような事態においては、リモート環境から安全に企業ネットワークへ接続できるように支援する体制が極めて重要です。400,000 社を超えるフォーティネットのお客様が導入済の既存テクノロジーには、このような事態に活用いただける機能が既に備わっています。FortiGate NGFW には IPsec VPN のサポートが統合されており、代替の作業環境から企業ネットワークへ安全に接続して業務を続けることが可能です。

テレワークによって、従業員は無駄な時間を平均で 27% 削減できる [1]。

テレワークを実施している従業員の年間平均労働日数は、オフィス勤務の従業員と比較して 16.8 日も多い [2]。

従業員の 85% が、テレワークの場合に生産性が最大限に高まると主張している [3]。

テレワークを許可した場合、企業組織の 95% で従業員の定着率が向上した [4]。

テレワークを保護する FortiGate NGFW

すべての FortiGate NGFW には IPsec / SSL VPN が統合されており、極めて柔軟な導入配備が可能です。リモート環境の従業員は、クライアント不要のアクセス体験のメリットを享受できるほか、FortiClient エンドポイントセキュリティソリューションに組み込まれている機能を活用し、様々な機能にアクセスすることも可能です。パワーユーザーやスーパーユーザーは、FortiAP あるいは FortiGate NGFW を導入配備することでさらなる機能を活用可能となり、大きなメリットを享受できます。

フォーティネットのソリューションは、購入からサポート終了に至るライフサイクルを通じて容易に活用できるように設計されています。FortiGate NGFW および FortiAP 無線アクセスポイントは、ZTP（ゼロタッチプロビジョニング）を可能にする機能を備えています。リモート拠点に配備するネットワーク機器は出荷前に事前構成を済ませておくことができるため、配備時の設定が自動化されビジネスオペレーションを確実に継続できると同時に、テレワークへの対応も実現します。

フォーティネット セキュリティ ファブリックは、共通のフォーティネットオペレーティングシステム（FortiOS）およびオープン API（アプリケーションプログラミングインタフェース）による環境のメリットを活かして、幅広い適用領域で（Broad）システム連携し（Integrated）、自動化された（Automated）セキュリティアーキテクチャを確立しています。フォーティネット セキュリティ ファブリックでは、テレワークを支援するために配備されたものをはじめとする企業組織のデバイスすべての監視と管理が、単一のコンソールから実行できます。企業のセキュリティ担当チームは、その導入状況を問わず企業ネットワークに接続するすべてのデバイスを、FortiGate NGFW、あるいは本社の環境に配備された FortiManager 集中セキュリティ管理プラットフォームから完全に可視化することができます。

自然災害をはじめ、通常のビジネスオペレーションを中断させる事態が発生した場合には、テレワークへの完全な移行を即座に実行しなければなりません。表 1 は、FortiGate NGFW の各モデルがサポートする同時 VPN ユーザー数を示しています。

伝送中のデータの暗号化だけでなく、フォーティネットのソリューションは VPN 経由でリモートから業務を行う従業員を保護する様々な機能を提供します。フォーティネットのソリューションが提供する代表的な機能をご紹介します。

- **多要素認証：**FortiToken および FortiAuthenticator は、リモート環境の従業員に対する二要素認証を可能にします。
- **データ漏えい対策（DLP）：**FortiGate および FortiWiFi は、リモート環境の従業員向けに DLP 機能を提供します。この機能は、企業の重要な機密データにリモート環境から頻繁にアクセスするエグゼクティブに不可欠です。

- **高度な脅威保護：**FortiSandbox は、マルウェアやその他の不審なコンテンツが宛先に到達する前にサンドボックス環境で分析します。
- **無線 LAN：**FortiAP / FortiWiFi は、リモート拠点でセキュアな無線アクセスを提供します。単一のコンソールからの統合や完全な管理が可能です。

モデル	同時 SSL VPN ユーザー	同時 IPsec VPN ユーザー	管理型 FortiAP（トンネルモード）
100E	500	10,000	32
100F	500	16,000	64
300E	5,000	50,000	256
500E	10,000	50,000	256
600E	10,000	50,000	512
1100E	10,000	100,000	2,048
2000E	30,000	100,000	2,048
FortiGate 3000 シリーズ	30,000	200,000	2,048

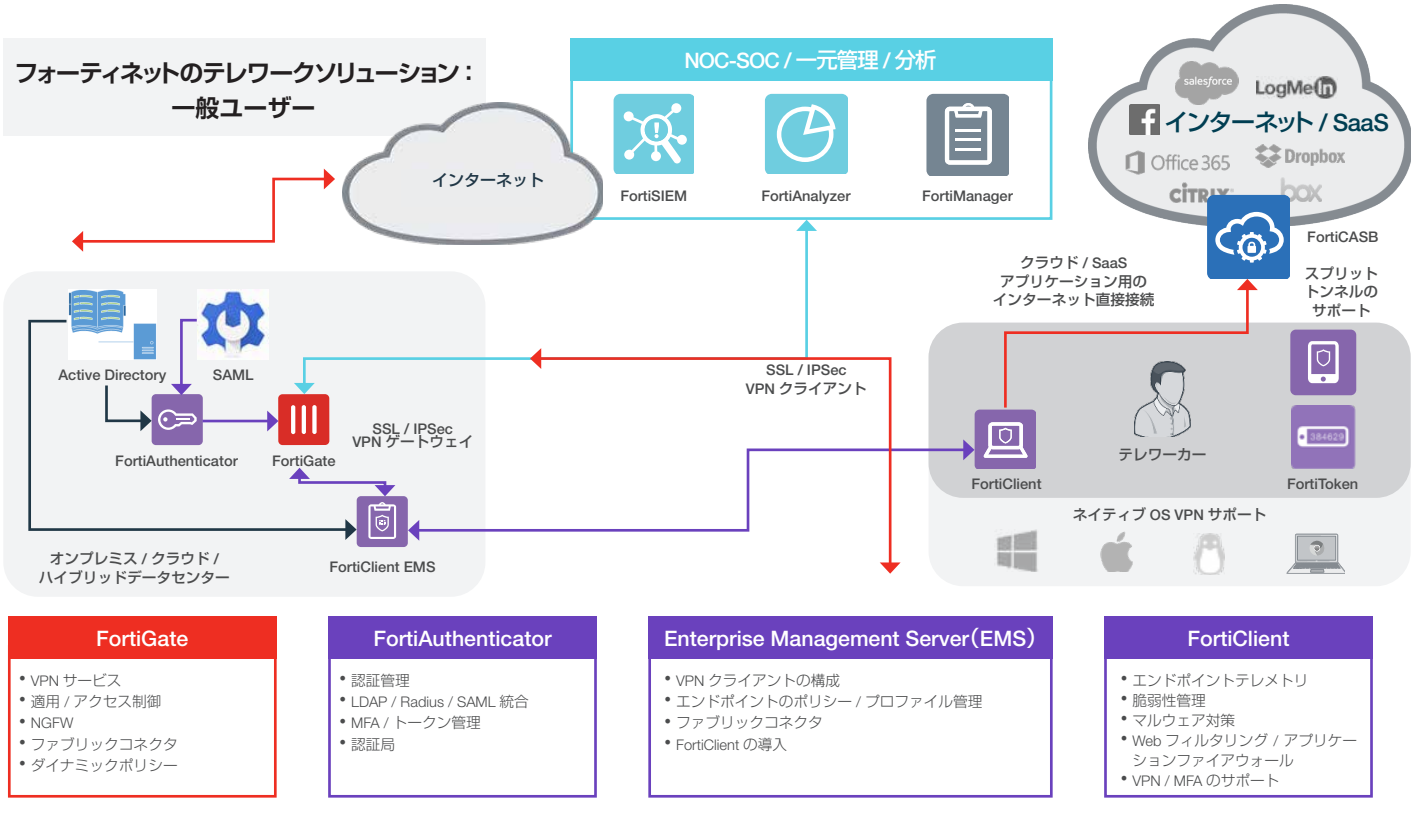
表 1：FortiGate NGFW がサポートする同時 VPN ユーザー数

テレワークを支援するフォーティネット製品のユースケース

従業員がリモート環境で業務を行う場合、企業リソースに対して全員が同じレベルのアクセスを必要としているわけではありません。フォーティネットは、すべての従業員各々にカスタマイズされたテレワークソリューションを提供します。

1. **一般的なテレワーカー：**一般的なテレワーカーは、各々が作業するリモート環境から電子メール、インターネット、電話会議、共有が制限されたファイル、部門固有のシステム（財務、人事など）へのアクセスのみが必要です。これには、Microsoft Office 365 をはじめとするクラウド上の SaaS（サービスとしてのソフトウェア）アプリケーションや、企業ネットワークへのセキュアな接続などがあります。

   一般的なテレワーカーは、VPN クライアントソフトウェアが統合された FortiClient を使用して企業ネットワークに接続し、多要素認証機能を備えた FortiToken で自身のアイデンティティを検証することができます。パワーユーザーやスーパーユーザーがリモートの作業拠点から移動を続ける場合、一般的なテレワーカーと同じレベルのアクセスのみが許可される点に留意が必要です。



FortiGate
- VPN サービス
- 適用 / アクセス制御
- NGFW
- ファブリックコネクタ
- ダイナミックポリシー

FortiAuthenticator
- 認証管理
- LDAP / Radius / SAML 統合
- MFA / トークン管理
- 認証局

Enterprise Management Server（EMS）
- VPN クライアントの構成
- エンドポイントのポリシー / プロファイル管理
- ファブリックコネクタ
- FortiClient の導入

FortiClient
- エンドポイントテレメトリ
- 脆弱性管理
- マルウェア対策
- Web フィルタリング / アプリケーションファイアウォール
- VPN / MFA のサポート

図 1：一般的なテレワーカー向けのフォーティネットソリューション導入イメージ

2. **パワーユーザー：**パワーユーザーは、リモート拠点から業務を行う際に一般的なテレワーカーよりも高度なレベルで企業リソースへのアクセスが必要な従業員を指します。彼らは複数のパラレルな IT 環境におけるオペレーションを可能にするアクセスが必要で、システム管理者や IT サポート技術者、緊急時対応の担当者などが該当します。

   このようなパワーユーザーに対しては、代替の作業環境に FortiAP アクセスポイントを配備し、必要なレベルのアクセスとセキュリティを提供します。これにより、企業ネットワークへのセキュアなトンネルを活用するセキュアな無線接続が可能になります。FortiAP は ZTP（ゼロタッチプロビジョニング）による容易な配備が可能で、オフィスに導入されている FortiGate NGFW で管理されます。

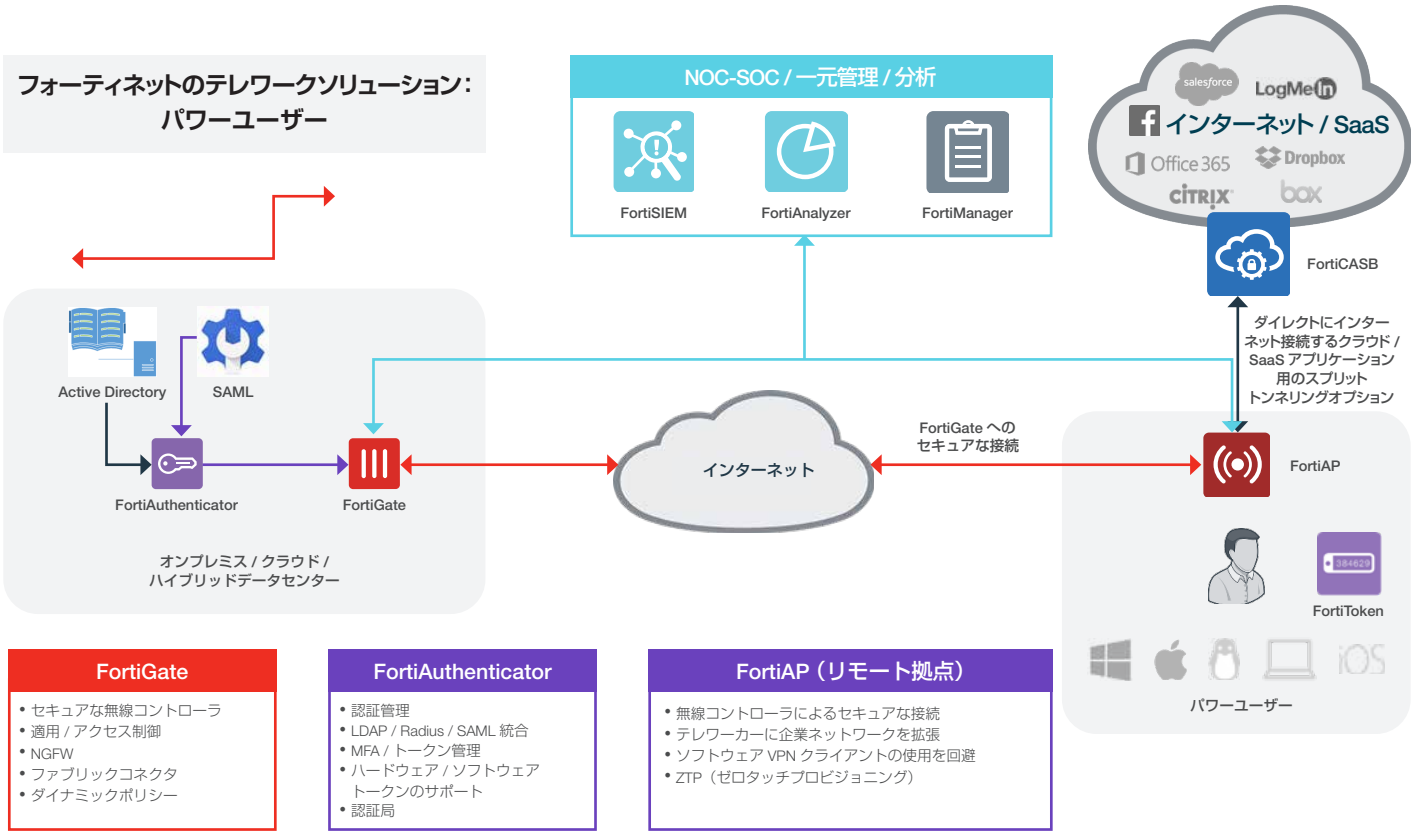


図 2：パワーユーザー向けのフォーティネットソリューション導入イメージ

3. **スーパーユーザー：**スーパーユーザーとは、代替のオフィス拠点で業務を行う場合でも、企業の機密情報リソースへの高度なアクセスが必要な従業員を指します。彼らは、極めて重要な機密情報を頻繁に処理します。この従業員向けプロファイルには、システムへの特権アクセスのある管理者、サポート技術者、事業継続計画において提携している主要パートナー、緊急時対応の担当者、経営陣などが含まれます。

   このようなスーパーユーザーに対しては、代替の作業拠点を代替のオフィス拠点として構成しなければなりません。彼らは一般的なテレワーカーやパワーユーザーと同じソリューションが必要ですが、それと同時に高度な追加機能も必要になります。FortiAP は FortiGate NGFW あるいは FortiWiFi アプライアンスとの統合が可能で、DLP 機能を備えたセキュアな無線接続を提供します。

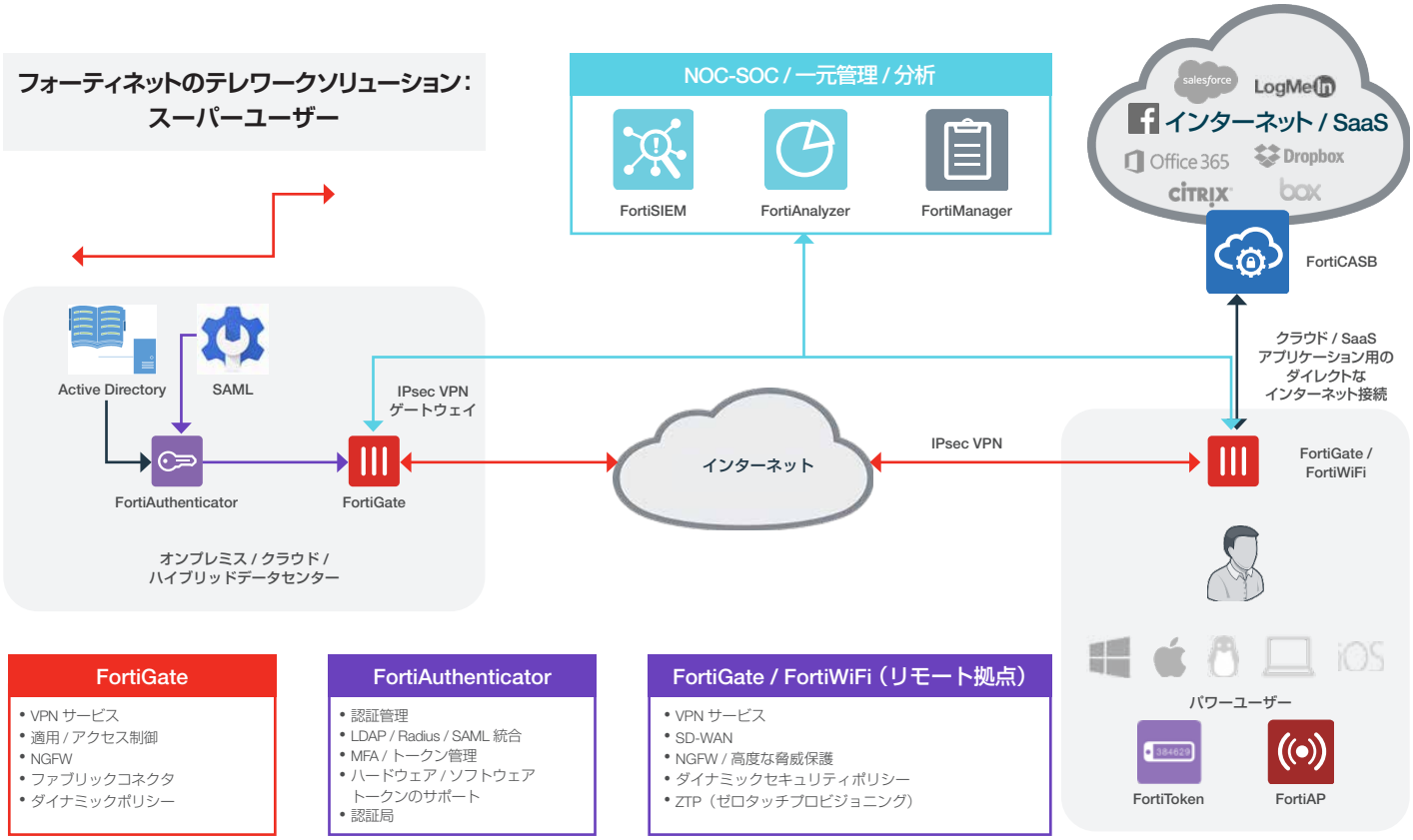


図 3：スーパーユーザー向けのフォーティネットソリューション導入イメージ

テレワーカーを支援する

フォーティネットのソリューションは、リモートの作業拠点への容易な配備が可能です。しかしながら、テレワーカーを安全にサポートするためにはオンサイトまたはクラウド上でもリソースが必要になります。

多くの企業組織は、既存のセキュリティアーキテクチャの一部としてこのようなリソースを既に備えています。FortiGate NGFW は、パフォーマンスへの影響を最小限に抑えながら企業、組織レベルで暗号化トラフィックや平文トラフィックのインスペクションが可能です。同時に、テレワーカーへの暗号化接続用エンドポイントとして機能する統合 VPN ゲートウェイも備えています。

また FortiGate NGFW は、Microsoft Active Directory（AD）、MFA、そして SSO（シングルサインオン）ソリューションなどの企業ディレクトリサービスをはじめとする一般的な IT インフラストラクチャとの統合も可能です。FortiAuthenticator は、認証ソリューションとの単一の一元統合ポイントとして機能すると同時に、ハードウェア、ソフトウェア、電子メール、そしてモバイルトークンの幅広い選択肢を提供している FortiToken だけでなく、サードパーティ製の認証ソリューションもサポートします。

リモート環境で業務を行い、地理的に分散している従業員を管理する際には、セキュリティの一元的な可視化と管理が不可欠です。すべてのフォーティネットソリューションは、フォーティネット セキュリティ ファブリックを介した統合が可能です。この統合によって、企業組織のセキュリティチームは FortiManager を活用した一元コンソールでの可視化と制御が可能となるほか、FortiAnalyzer によるログデータの集約とセキュリティ分析の実行、さらに FortiSIEM を利用した潜在的な脅威の迅速な検知とレスポンスが可能になります。

フォーティネットのソリューションを活用する完全なセキュリティ統合の実現

フォーティネット セキュリティ ファブリックは、企業組織のテレワーカーのシームレスな統合を実現します。フォーティネットのソリューションは、すべてフォーティネット セキュリティ ファブリックを介して統合され、一元的な可視化、構成、そして監視が可能になります。さらに、数多くのファブリックコネクタ、オープンな API 環境、DevOps コミュニティにおけるサポート、そして拡張された大規模なセキュリティ ファブリックのエコシステムにより、250 以上のサードパーティ製ソリューションとの統合も実現しています。

事業継続計画を準備している企業組織にとって、この統合は極めて重要です。これは、事前の通告も殆どなく従業員全体のテレワークへの移行を余儀なくされる可能性があるからです。セキュリティアーキテクチャの一元的な可視化と管理によって、テレワーカーに対するサポートが企業のサイバーセキュリティを脅かすことはなくなります。

以下のソリューションはフォーティネット セキュリティ ファブリックを構成する重要な要素であり、セキュアなテレワークをサポートします。

- **FortiClient：**FortiClient は、可視化、制御、およびプロアクティブな防御機能を統合することによってエンドポイントのセキュリティを強化すると同時に、リアルタイムでエンドポイントのリスクの発見、監視、そして評価を実現します。
- **FortiGate：**FortiGate NGFW は、専用設計のサイバーセキュリティプロセッサ（FortiSPU）を活用したトップクラスの保護、エンドツーエンドの可視化、そして一元的な制御だけでなく、クリアテキストや暗号化トラフィックのハイパフォーマンスのインスペクションを実現します。
- **FortiWiFi：**FortiWiFi 無線ゲートウェイは、FortiGate NGFW が提供するセキュリティのメリットを無線アクセスポイントと組み合わせた製品で、パワーユーザー向けにネットワークとセキュリティの統合ソリューションを提供します。
- **FortiToken：**FortiToken は、ワンタイムパスワードのトークン（ハードウェア、モバイルアプリケーション）で、認証プロセスに第二の要素を追加することで、より確実なユーザーのアイデンティティの検証を実行します。
- **FortiAuthenticator：**FortiAuthenticator は、SSO サービス、証明書管理、ゲスト管理をはじめとする一元的な認証サービスを提供します。
- **FortiAP：**FortiAP は、分散型のエンタープライズやパワーユーザーにセキュアな無線アクセスを提供し、FortiGate NGFW やクラウド経由の容易な管理が可能です。
- **FortiManager：**FortiManager は、大規模あるいは分散型の企業の管理とポリシー制御機能を一元化し、ネットワーク全体のトラフィックベースの脅威に対する実用的インテリジェンスを提供します。高度な脅威の封じ込めに加えて、優れた拡張性によって最大 10,000 台のフォーティネット製品の管理を可能にします。
- **FortiAnalyzer：**FortiAnalyzer は、高度な分析に基づくサイバーセキュリティとログ管理機能を提供し、脅威の検知やセキュリティ侵害の防止機能を改善します。
- **FortiSandbox：**フォーティネットのサンドボックスソリューションは、高度な検知機能、減災の自動化、実用的インテリジェンス、柔軟な導入形態の強力な組み合わせによって、標的型攻撃とそれによって引き起こされるデータ喪失を防止します。FortiGuard サブスクリプションに含まれているクラウドサービスとして提供されています。

確実な事業継続を可能にするセキュアな基盤

事業継続や災害復旧に関する準備は、すべての企業組織に不可欠です。そのような準備において重要なのは、事前の通告も殆どなくテレワーカーの大半あるいは全体を支援する能力です。

事業継続計画の立案においては、テレワーカーを保護するリソースを適切に配置しておくことが不可欠です。容易な配備と構成が可能なフォーティネットのソリューションは、その配備環境を問わず、企業組織における十分なセキュリティ、可視性、そして制御の維持を実現します。

1 「The Benefits of Working From Home」、Airtasker、2019 年 9 月 9 日（英語）：https://www.airtasker.com/blog/the-benefits-of-working-from-home/

2 同上

3 「Here's Why Remote Workers Are More Productive Than In-House Teams」、Abdullahi Muhammed 氏、Forbes、2019 年 5 月 21 日（英語）：https://www.forbes.com/sites/abdullahimuhammed/2019/05/21/heres-why-remote-workers-are-more-productive-than-in-house-teams/

4 同上

フォーティネットジャパン株式会社

〒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-Secure-Remote-Access-202003-R2