FORTINET

高度標的型攻撃対応
次世代セキュリティ製品

FortiGate

高度化するサイバー攻撃に統合力で立ち向かう新時代のセキュリティソリューション

FortiGateシリーズをはじめとするFortinet社製品は、
高度・複雑化するサイバー攻撃から企業ネットワークを守るだけでなく、
リモートアクセスやセキュアなWi-Fi環境の構築など、
多様化するビジネス環境を強固に保護する統合ネットワークセキュリティソリューションを提供します。

サイバー脅威から企業を守る

セキュリティ対策

基本的なUTM（統合脅威管理）機能に加え、外部の悪意をもったデータ収集サーバーへの不正な通信を検知・ブロックするボットネット対策機能も搭載しています。また、ウイルス特有の動作を敏感にとらえる振る舞い型検知によって未知の検体にも対応、新種や亜種のウイルスから企業ネットワークを守ります。

FortiGate　FortiSandbox Cloud　FortiGate Cloud

在宅勤務やモバイルワーク

安全（セキュア）なリモートアクセス

エンドポイント（終端）のセキュリティを強化して通信の安全を確保、ますます需要が高まる在宅勤務やモバイルワークにも柔軟に対応してユーザーに自由な働き方を提供します。また、トークンによるワンタイムパスワード（二要素認証）を併用することでなりすましを防止し、より安全な接続を実現します。

FortiGate　FortiClient　FortiToken

組織の規模や体制に合わせて

セキュアに業務を効率化

SD-WANの機能を使って、クラウド利用やビジネス拠点の拡大による通信負荷を軽減し、快適なネットワーク通信を提供します。またスマートフォンやタブレットなどのモバイル端末を導入する際も、多機能かつ安全なWi-Fi環境を容易に構築でき、多様化するビジネス基盤をサポートします。

FortiGate　FortiAP

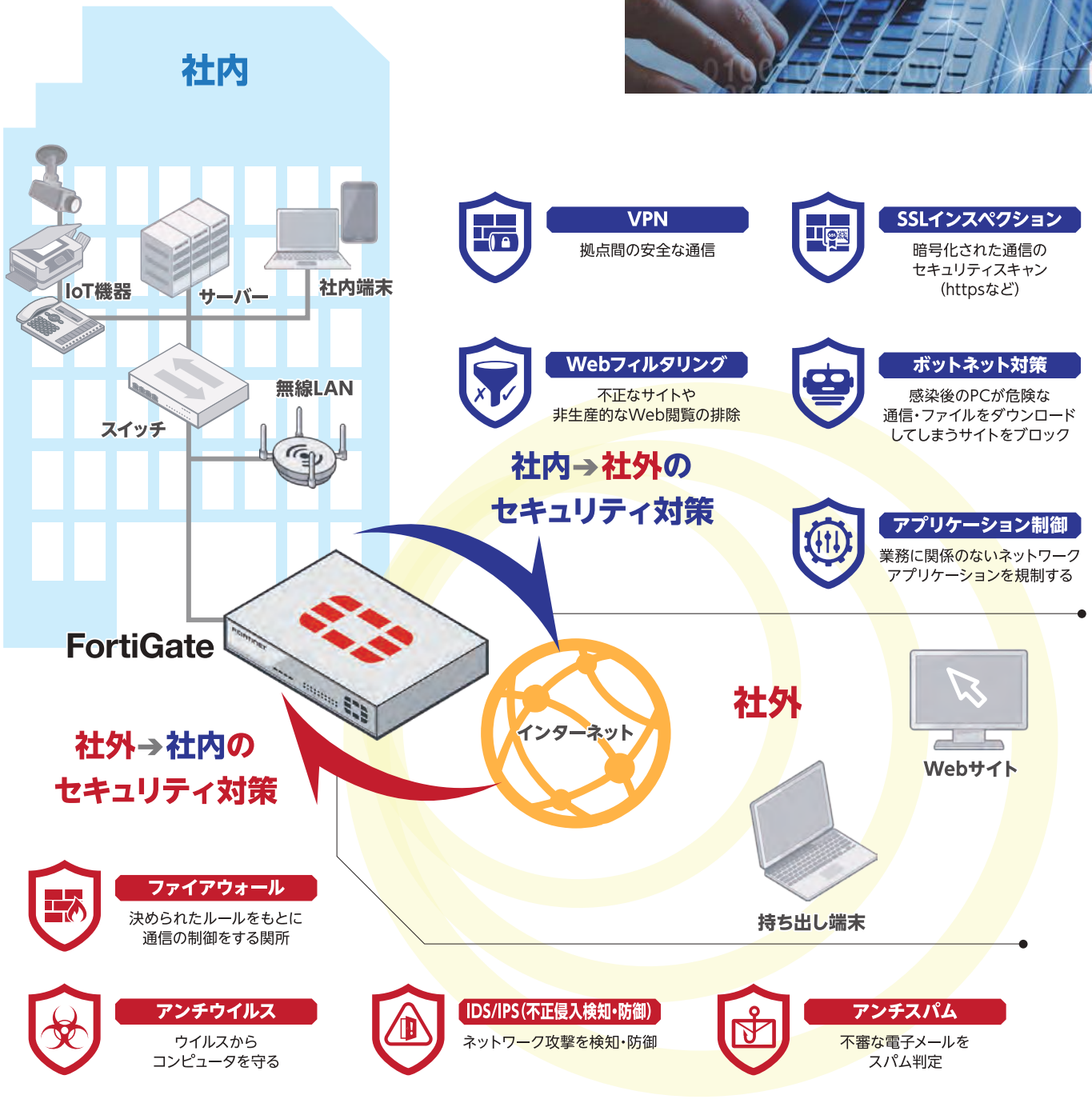
FortiGate

サイバー脅威から企業を守る

セキュリティ対策

UTM機能

UTM（統合脅威管理）とは、複数のセキュリティ機能を1つに集約して運用するネットワークセキュリティ対策です。FortiGateは次世代ファイアウォール（NGFW）として、アンチウイルスやIPS/IDS、アンチスパム、Webフィルタリングといったセキュリティ機能を1台にまとめたUTM製品で巧妙化・複雑化するサイバー攻撃から社内ネットワークを守ります。



VPN
拠点間の安全な通信

SSLインスペクション
暗号化された通信の
セキュリティスキャン
（httpsなど）

Webフィルタリング
不正なサイトや
非生産的なWeb閲覧の排除

ボットネット対策
感染後のPCが危険な
通信・ファイルをダウンロード
してしまうサイトをブロック

アプリケーション制御
業務に関係のないネットワーク
アプリケーションを規制する

ファイアウォール
決められたルールをもとに
通信の制御をする関所

アンチウイルス
ウイルスから
コンピュータを守る

IDS/IPS（不正侵入検知・防御）
ネットワーク攻撃を検知・防御

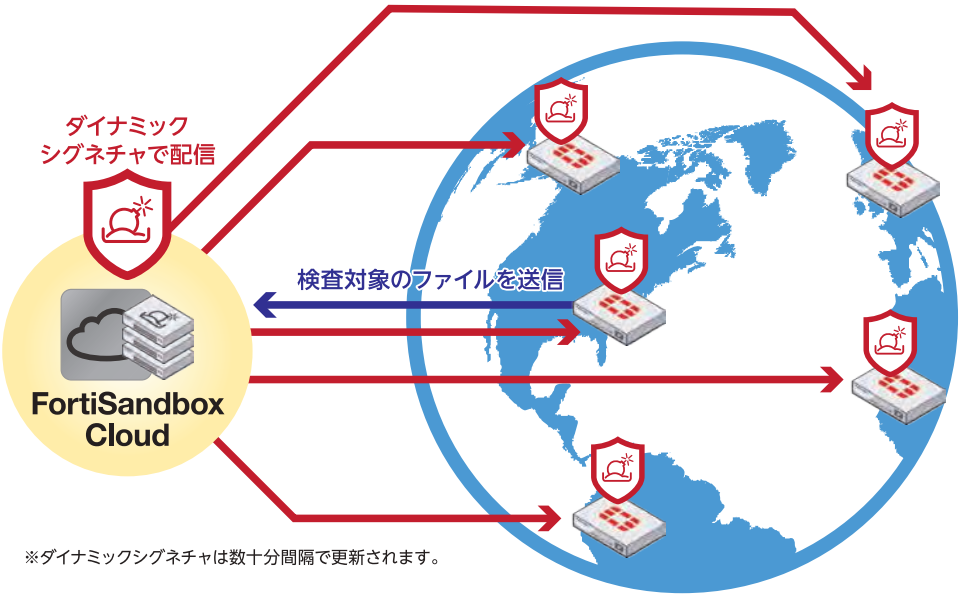
アンチスパム
不審な電子メールを
スパム判定

サイバー脅威から企業を守る
セキュリティ対策

未知のサイバー脅威から社内ネットワークを守る

FortiSandboxCloud（振る舞い型検知）

ウイルスには、正常なプログラムにはないウイルス特有の不審な挙動パターンがあります。FortiGateはクラウド上でその特徴的な挙動を見つけ出す「振る舞い型検知」を行い、既知のウイルスだけではなく、新種や亜種など未知のウイルスからも防御します。



※ダイナミックシグネチャは数十分間隔で更新されます。

クラウド上に登録されている全世界のFortiGateから送信された検体ファイルを検査します。発見した最新の疑わしいファイルに対する一時的な定義ファイル（ダイナミックシグネチャ）を配信して対策を共有します。

- 全世界で検知された脅威の情報をいち早く共有できる
- アプライアンス製品であるFortiSandboxの機能を安価に提供
- Cloudサービスによるメンテナンスやチューニングの手間を削減

既知の脅威と未知の脅威

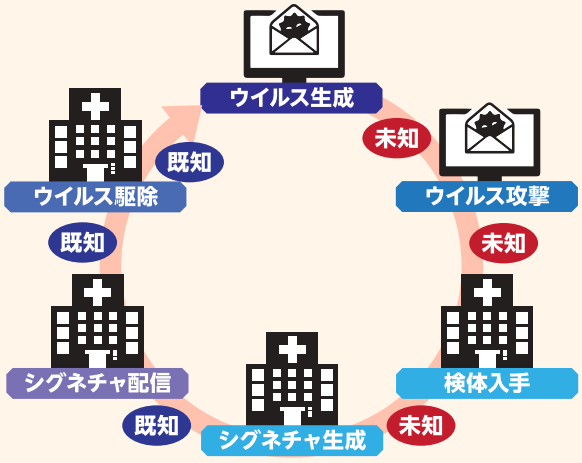
ウイルスの脅威には「既知の脅威」と「未知の脅威」があります。攻撃手法は年々多様化・巧妙化しており、「未知の脅威」への対策が不可欠となっています。

既知の脅威

既にワクチンが開発されており、データベースと照合するパターンマッチング方式（シグネチャ型）で検知可能なウイルスの脅威

未知の脅威

ワクチンが開発されておらず、データベースにないためパターンマッチング方式（シグネチャ型）では検知が難しいウイルスの脅威



社内ネットワークのインシデント発生時のログを一元管理

クラウドロギングサービス

FortiGateから収集したネットワークの利用状況やアクセス履歴などのログを可視化してクラウド上で一元管理。様々なインシデントの発生を迅速に把握し、被害を最小限に抑えます。また万が一のシステム障害発生時には原因の究明に結び付け、迅速な復旧と防止対策に役立てることが出来ます。

FortiGateのトラフィックログやセキュリティイベントログなどをクラウド上に集約し保管するFortiGate用のロギングサービスです。また、登録したFortiGateにリモートからアクセスするための機能も備えています。

サイバー攻撃者の心理

現代のサイバー攻撃は、金銭の搾取が主な理由であると言われています。被害に遭ってもバレにくく、犯人の追及が難しいことからローコストハイリターンのビジネスとして、犯罪の温床になっています。時代遅れのセキュリティ対策では、攻撃者の絶好のターゲットとして狙われてしまうため、堅牢なセキュリティシステムを構築していくことが重要です。

明確な目的	決済手段の多様化	攻撃の効率化	市場の拡大
金銭・情報の搾取	電子マネー・仮想通貨	専門分業化	組織化・闇市場

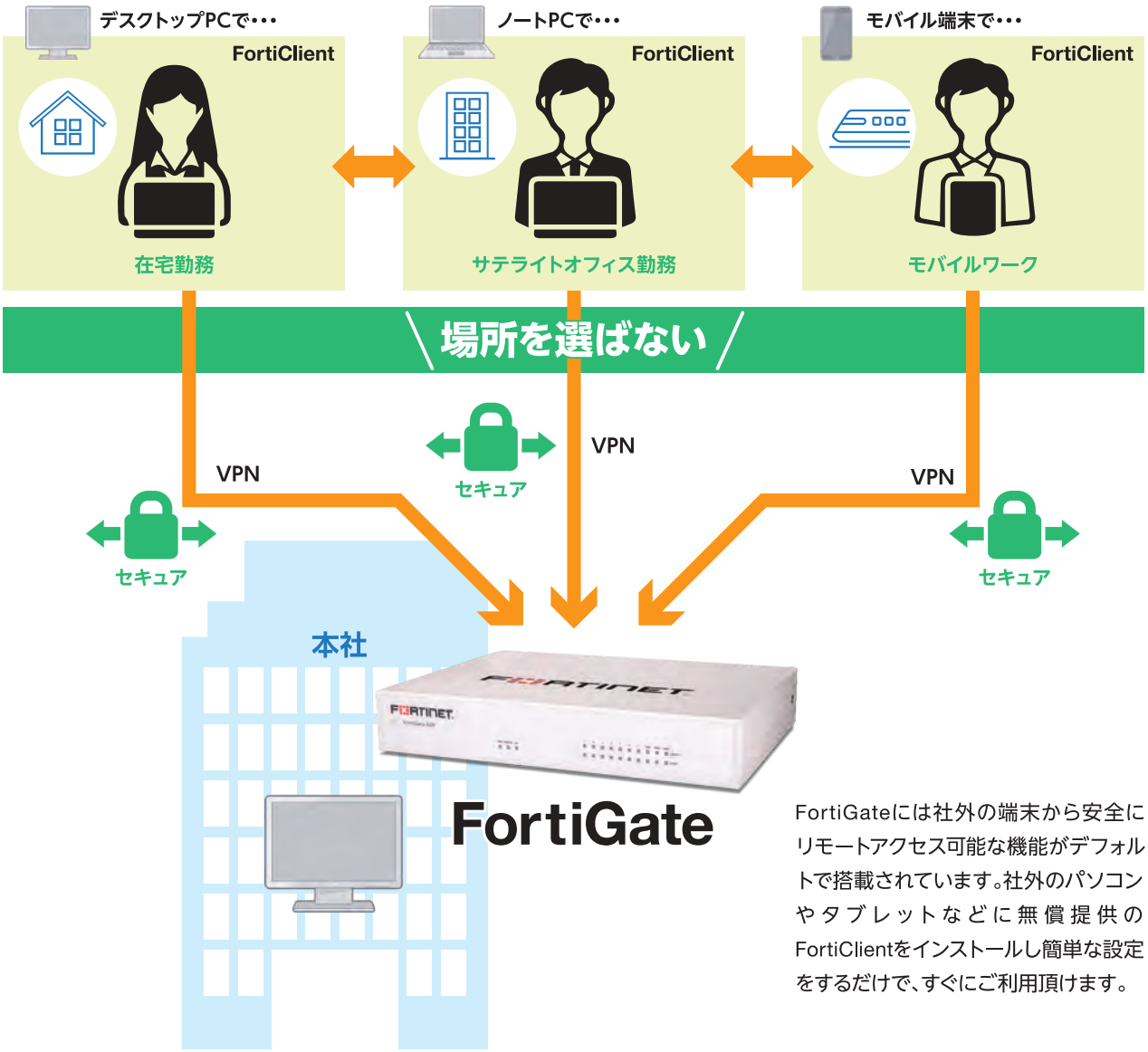
在宅勤務やモバイルワーク

安全（セキュア）なリモートアクセス

在宅勤務やモバイルワークを自由に安全に

FortiClient

テレワーク需要の高まりに伴って、ますます重要となるセキュリティ対策。FortiClientを使って自宅やカフェ、サテライトオフィスなどの遠隔地から、社内のネットワークやコンピュータに最適な経路で接続、安全で快適なリモートアクセスを実現します。

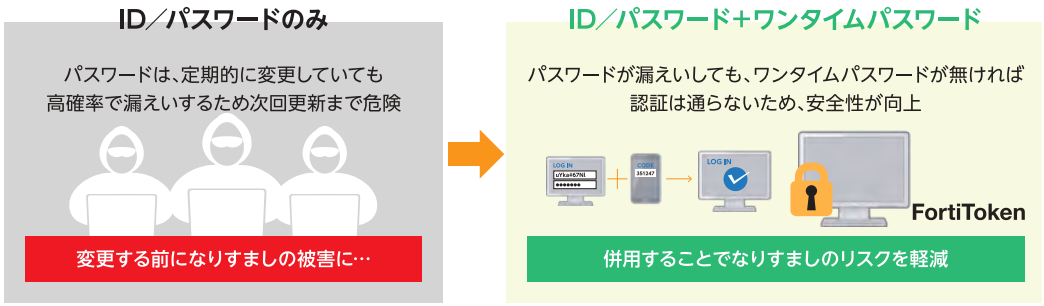


FortiGateには社外の端末から安全にリモートアクセス可能な機能がデフォルトで搭載されています。社外のパソコンやタブレットなどに無償提供のFortiClientをインストールし簡単な設定をするだけで、すぐにご利用頂けます。

二要素認証でなりすましのリスクを軽減

FortiToken

ID／パスワードなど従来の認証に加え、一度きりしか使用できない「ワンタイムパスワード」を発行。仮にID／パスワードが漏えいしても、ワンタイムパスワードがなければ認証が通らないため、ログインができません。2つの要素で認証時のセキュリティ侵害のリスクを防ぐことができます。



※FortiTokenには専用端末を使うハードタイプとスマートフォンなどにアプリをインストールして利用するモバイルタイプの2種類があります。

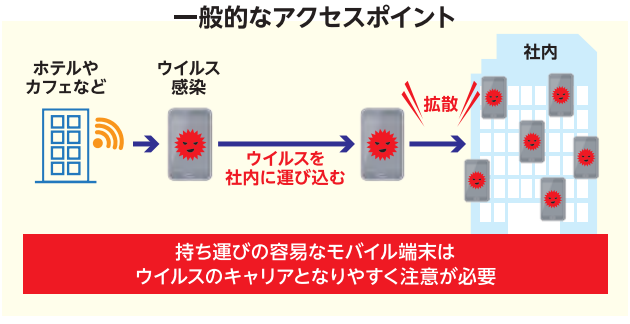
組織の規模や体制に合わせて

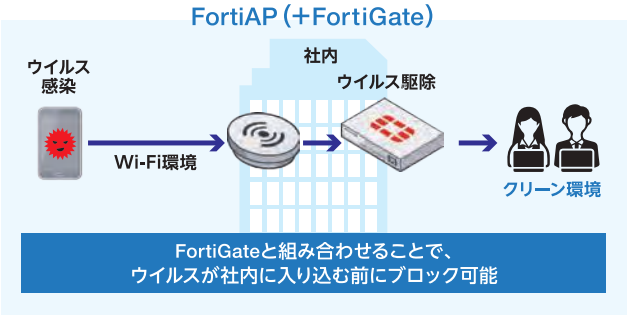
セキュアに業務を効率化

多機能で安全なWi-Fiネットワークを構築

FortiAP

業務の効率化に欠かせないノートPCやモバイル端末によるWi-Fi接続。一方で社外のネットワークを利用した際のウイルス感染など、多くの危険もはらんでいます。FortiAPは、FortiGateと組み合わせることでウイルスの流入を防止するセキュアなWi-Fi環境を構築し、セキュリティを担保しながら業務の効率化をサポートします。





※上記はFortiAPを『トンネルモード』で利用した場合です。

組織の規模や体制に合わせて

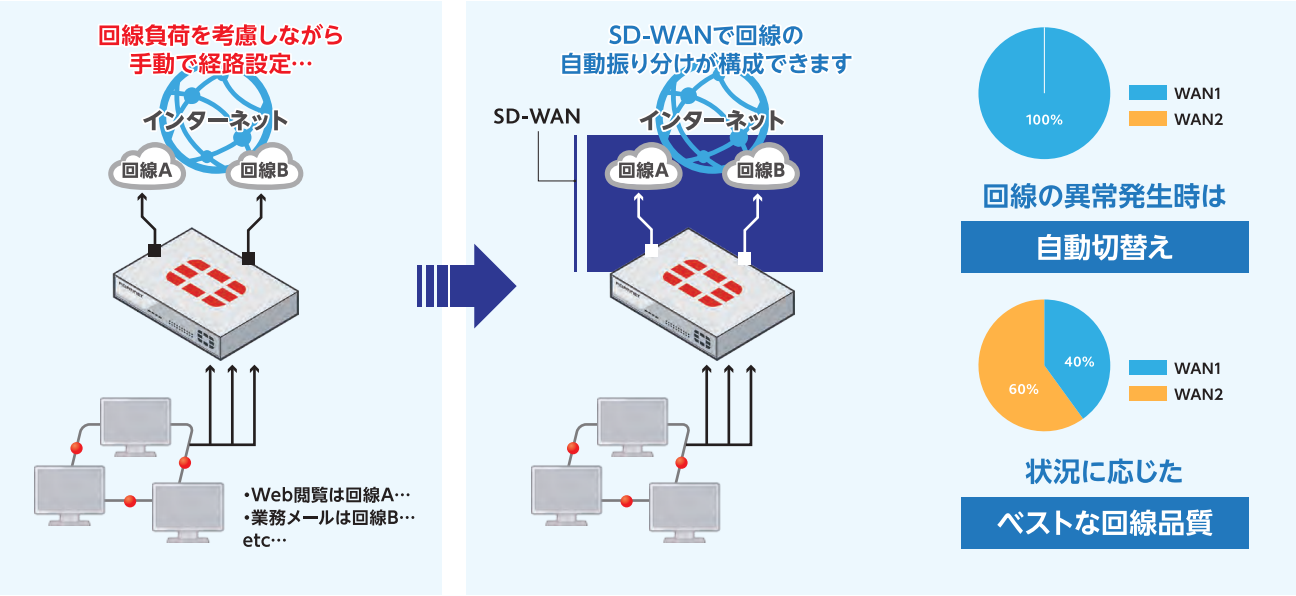
セキュアに業務を効率化

状況に合わせてWAN回線を管理・制御

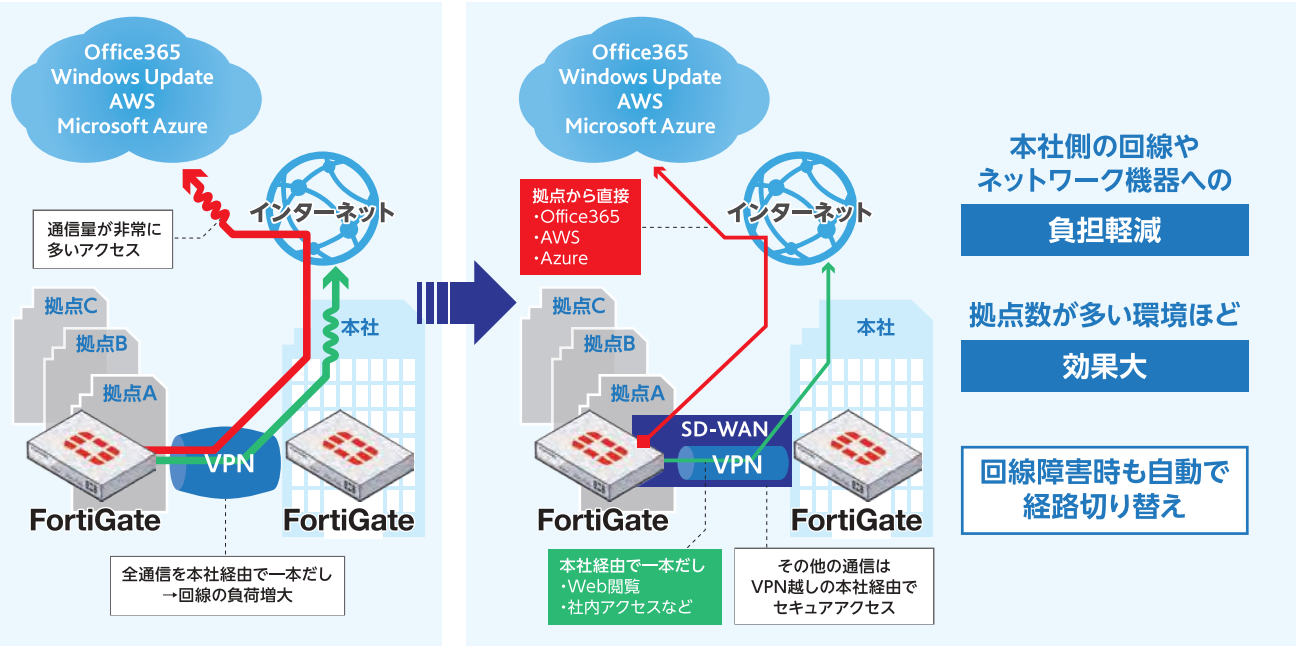
SD-WAN

FortiGateのSD-WAN機能を利用することで、複数のWAN回線の効率的な運用やバックアップ構成が可能です。
また、特定のインターネット通信の経路指定を行うことで、回線の負荷分散効果があります。

利用シーン ❶



利用シーン ❷



datacontrol
株式会社データコントロール
https://www.datacontrol.co.jp/
〒141-0031 東京都品川区西五反田1-1-8 NMF五反田駅前ビル5F
TEL:03-5434-2331 FAX:03-5434-2332