FORTINET

NGFW+ATP
次世代ファイアウォール

FortiGate
FortiWiFi Series

スマートフォン・タブレット時代の統合セキュリティソリューション

クラウド化の進展に伴い、ネットワークコンピューティングの利用もオフィス内にとどまらず、
ビジネスの現場、お客様先へと拡大しています。利用シーンの多様化とともに企業ユーザーが利用するデバイスも、
デスクトップパソコンからノートパソコンやスマートフォン、タブレットなど、次々と増えるとともに、
シチュエーションに応じて使い分けられるようになりました。
場所や、デバイスさえも超えて進化し続けるネットワークコンピューティングに対するセキュリティ上の脅威も、
それ以上の勢いで日々増大し続けています。

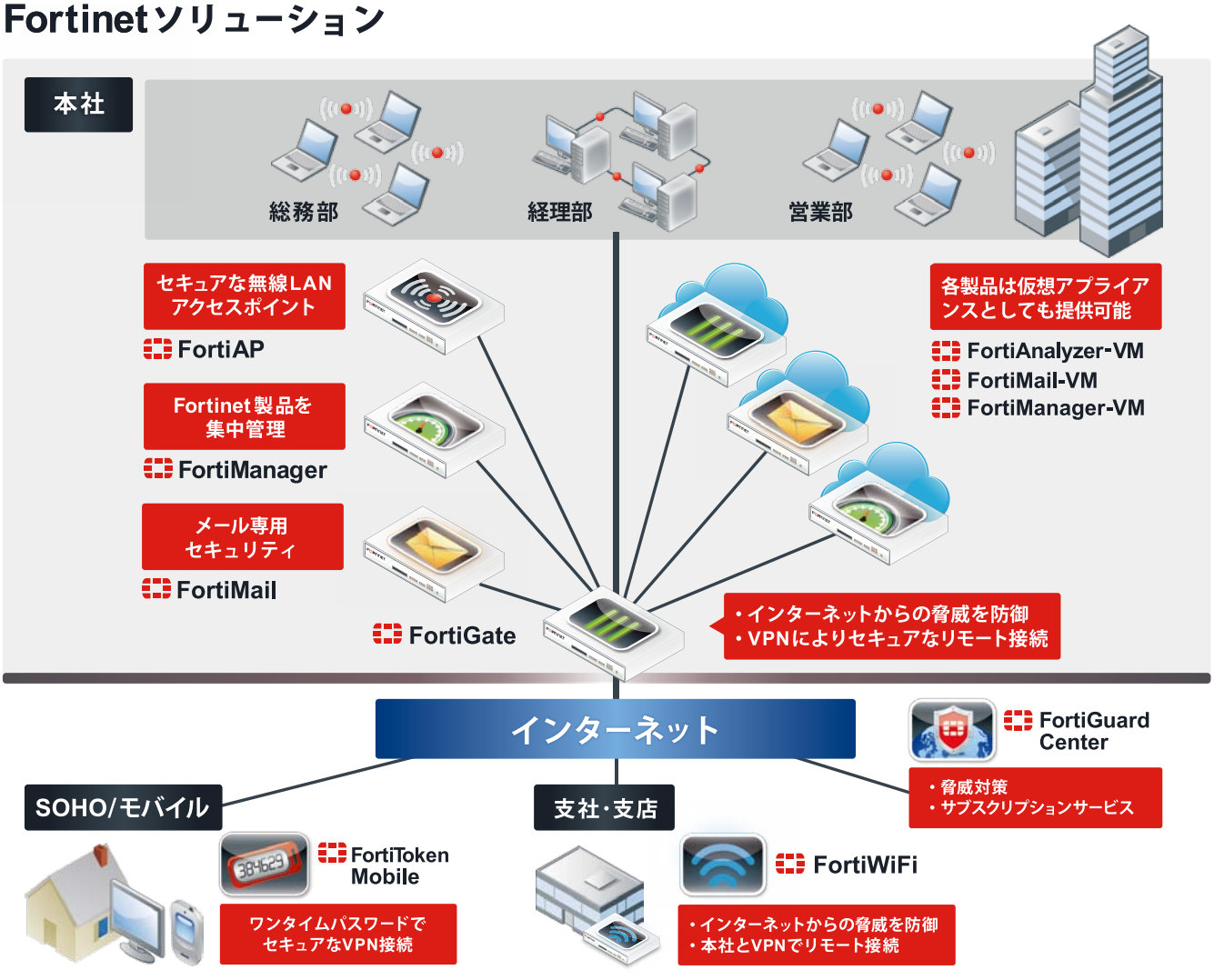
FortiGateシリーズをはじめとするFortinet社製品はスマートフォン・タブレット時代に対応した
統合ネットワークソリューションを提供します。

FortiGate / FortiWiFi シリーズの特徴

FortiGateシリーズは**次世代ファイアウォール**(NGFW)として、アンチウイルスやアンチマルウェア、Webフィルタリング、VPN、侵入検知・防御、アンチスパムなどの機能を搭載した**統合脅威管理(UTM)製品**です。さらに、企業の私的端末活用(BYOD)のニーズに応えるため、無線LANアクセスポイントの制御、スマートフォンやタブレットなどのクライアント端末の接続制御まで、企業のネットワーク・セキュリティに必要な機能を1台に凝縮しています。

また、**FortiGate**を中核として、クライアント向け製品、大規模管理向け製品なども提供しており、企業ネットワークのコアからエッジまで、一貫したソリューションを提供いたします。

Fortinetソリューション



SOHOから大規模企業まで対応する幅広いラインアップ

FortiGateシリーズは、SOHOや営業所に最適なコンパクトなタイプから、中規模・大規模企業、キャリアクラスの大型タイプまで、お客様の環境や規模に合わせて、様々な用途に対応するラインアップを取り揃えています。

FortiGate / FortiWiFi | 主な機能

NGFW（次世代ファイアウォール）

外部からの不正侵入や脅威の防御に加えて、アプリケーションの可視性を確保し、ネットワーク内で稼動するアプリケーションを制御します。これによりパフォーマンスの犠牲を最小限にして高いセキュリティを確保することができます。

不正侵入検知/防御（IDS/IPS）

外部からネットワークに不正アクセスを試みる通信を検知し、必要に応じてブロックを行います。IPSシグネチャの自動アップデートにより最新の脅威にも対抗します。

アプリケーションコントロール

ネットワークを通じて送受信されるデータからセキュリティリスクの高いアプリケーション（不正なP2Pなど）の挙動を検知し、必要に応じて帯域幅の制御や通信のブロックを行います。

ATP（Advanced Threat Protection）

最新のネットワーク脅威の１つであるATA（高度な標的型攻撃）に対応するため、従来のアンチウイルス機能を中心とした多層防御を提供するオプションです。このオプションには主に下記の機能が含まれます。

Fortinet Webフィルタリング

URLの照合やDNSベースの高度なWebフィルタを使用して、有害な恐れのあるWebサイトの閲覧を防止します。

Fortinet アンチウイルス

一般的なウイルス脅威を検出し、ネットワーク内のデバイスを感染から守ります。

FortiGuardボットネットデータベース

IPレピュテーションに関する最新情報を蓄積し、その情報から悪意を持つC&Cサーバーとの通信を防止します。

その他の機能

ファイアウォール基本機能

通常のNAT/Routeモードの他、トランスペアレントモードを実装し、既存のネットワーク構成を変えることなく、セキュアな環境を提供できます。

管理機能

多言語に対応したグラフィカルなWebインターフェイスを提供し、日本語により直感的な操作を可能にします。

VPN機能

SSL-VPNやIPSec-VPN、L2TPなどに対応し、インターネット越しにセキュアなVPN環境を容易に構築できます。

IPv6対応

現在主流のIPv4に代わって普及が進んでいるIPv6に関して、アンチウイルスや侵入検知などのセキュリティ機能においても完全対応しました。

FortiGate / FortiWiFi | BYODソリューション

FortiGate / FortiWiFi で実現するセキュア・モバイル環境

新しい**FortiOS 5.0**では、スマートフォンやタブレットなどの新しい形態のデバイスを利用したBYODに対応したネットワークセキュリティを提供します。

デバイス認識 / 識別のフェーズ

デバイス識別（アイデンティフィケーション）	アクセスコントロール	セキュリティアプライアンス
監視/管理：・エージェントレス ・エージェントベース	認証/許可：デバイス識別ポリシー	情報保護：UTMプロファイル

スマートデバイス / BYOD環境のセキュリティ

- デバイス / デバイスグループに対して異なるセキュリティポリシーを設定できます。
- Windows AD やユーザー認証環境との連携で、ユーザーとデバイスを可視化します。

さらに、**二要素認証**も低コストで実現。
リモートアクセスでも社内と同等の高度なセキュリティが保てます。

利用が可能なトークン

FortiToken Mobile

FortiToken

E-Mail

通常ユーザーと同様に、ユーザー名 / パスワードを入力し、ログインを実行。

トークンコード入力欄に、二要素認証デバイスに表示されているワンタイムパスワードを入力します。

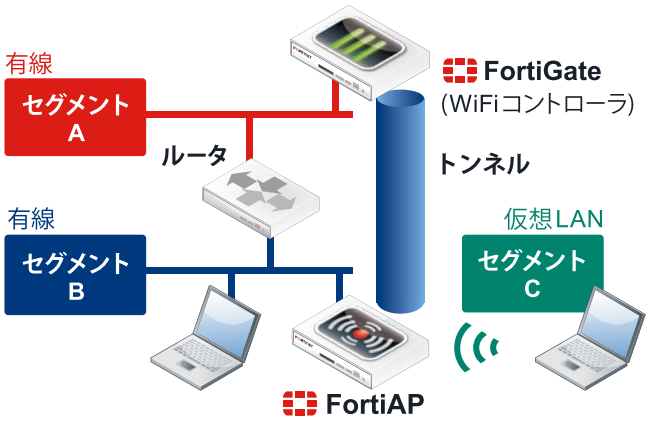
WiFi 環境をより柔軟に、簡単に構築するための 3つのモード

社内ネットワークに高度かつ安全な無線アクセスポイントを構築するため、
従来の**トンネルモード**に加えて、新たに**ローカルブリッジモード**、**Meshモード**の3つのモードを実装しています。

トンネルモード

- 無線デバイスを他の有線LANセグメントとは別の仮想LANセグメントに接続するモードです。
- WiFiインターフェイスに対して独立したファイアウォールポリシーを設定できます。
- 追加機能としてトラフィックをDTLSにて 暗号化する事が可能です。

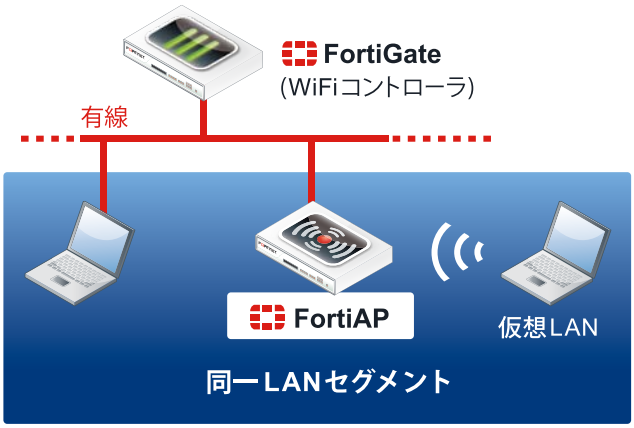
※ FortiWiFi、FortiAPの両製品で使用できるモードです。



ローカルブリッジモード

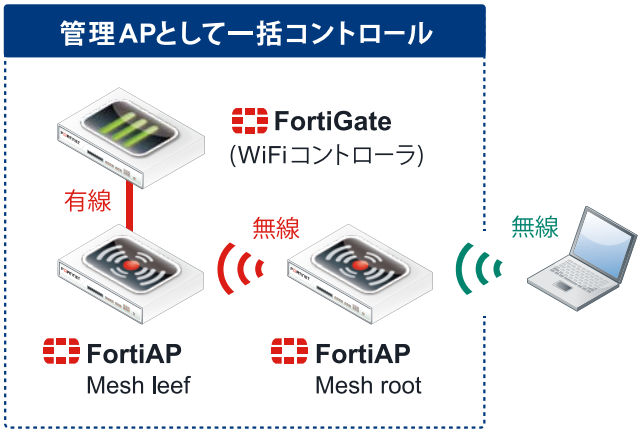
- スイッチポートまたはLANスイッチと組み合わせて使用する事により有線LANと無線デバイス用の仮想LANを同じセグメントに所属させる事ができるモードです。
- 有線デバイスと無線デバイスは同じファイアウォールポリシーでコントロールされます。
- IPアドレス等の割り当ては、有線デバイスと同じDHCPサーバーで行われます。

※ FortiAPで使用できるモードです。



Meshモード

- FortiGate (WiFiコントローラ)とFortiAPの間をWiFiネットワークを中継して接続する機能です。壁や天井などで、空間的にイーサネットケーブルによる接続が難しい空間でも、WiFiネットワークの敷設が可能になります。
- それぞれのFortiAPにおいて、Mesh root用・Mesh leaf用を設定し接続する事で、WiFiコントローラ1つでデバイスの管理が可能です。



FortiGuardサブスクリプションサービス

FortiGuardサブスクリプション サービスは、FortiGate/FortiWiFiシリーズを常に最新の状態に保つための、ライセンスサービスです。アンチウイルス、侵入検知・防御、Webフィルタリング、アンチスパム等の各機能を**24時間体制**で自動アップデート。最新のセキュリティ攻撃への対策を提供します。

サブスクリプションライセンスは、FortiGate/FortiWiFiユニットベースですので、ユーザー数を気にすることなく一定のコストで維持可能です。

仮想アプライアンスでパブリック/プライベートクラウドにも完全対応

アプライアンス製品で実績のある信頼性の高いFortinet製品を、シンプルかつ同等の機能にて、仮想インフラ環境上に実装することができます。仮想インフラ上で一括管理することで、インフラの可視化、集中管理、ハードウェアスペースの削減などのメリットを得ることができ、運用中のネットワークへの迅速なセキュリティ確保と、規模に合わせた仮想環境ならではの段階的な構築・運用を実現します。

VMwareのハイパーバイザー上に、**FortiGate**、**FortiAnalyzer**、**FortiManager**、**FortiMail**などの各種ファミリー製品の導入が可能です。

Fortinet | 関連機器

FortiMail

巧妙化するスパムメールを徹底的に撃退します。

FortiMailシリーズは、**アンチスパムとアンチウイルスの機能**を搭載、メールセキュリティに特化したアプライアンス製品です。SMTPリレーの経路を変更して設置する**ゲートウェイモード**、変更が不要な**トランスペアレントモード**、メールサーバーの機能を包含する**サーバーモード**の3つのモードを選択可能です。メールの隔離、外部→内部・内部→外部双方向の検知に対応します。

- 小規模～中規模、大規模、ISPまで
  多彩な組織でご利用頂けるメッセージングセキュリティ・システムを提供します。
- 先進のメールフィルタリングは、送受信メール環境にてスパム、ウイルス、フィッシング、ワームとスパイウェアの蔓延を防ぎます。
- 細分化されたポリシー管理、レポーティング機能。
- メールセキュリティとメールサーバーの機能を1台で提供します。
- WebメールやSMTP Authもサポート。

FortiManager

複数のFortinet製品を1つのコンソールで集中管理。
大規模ネットワークの管理効率化に。

FortiManagerシリーズは、複数のFortiGate、FortiWiFiなどのFortinet製品を管理し、モニタリングするアプライアンスです。Fortinet製品に対する一貫したポリシーの定義と適用、システムステータスやトラフィックの監視、攻撃ログの参照などの集中管理を容易に実現します。

FortiAP

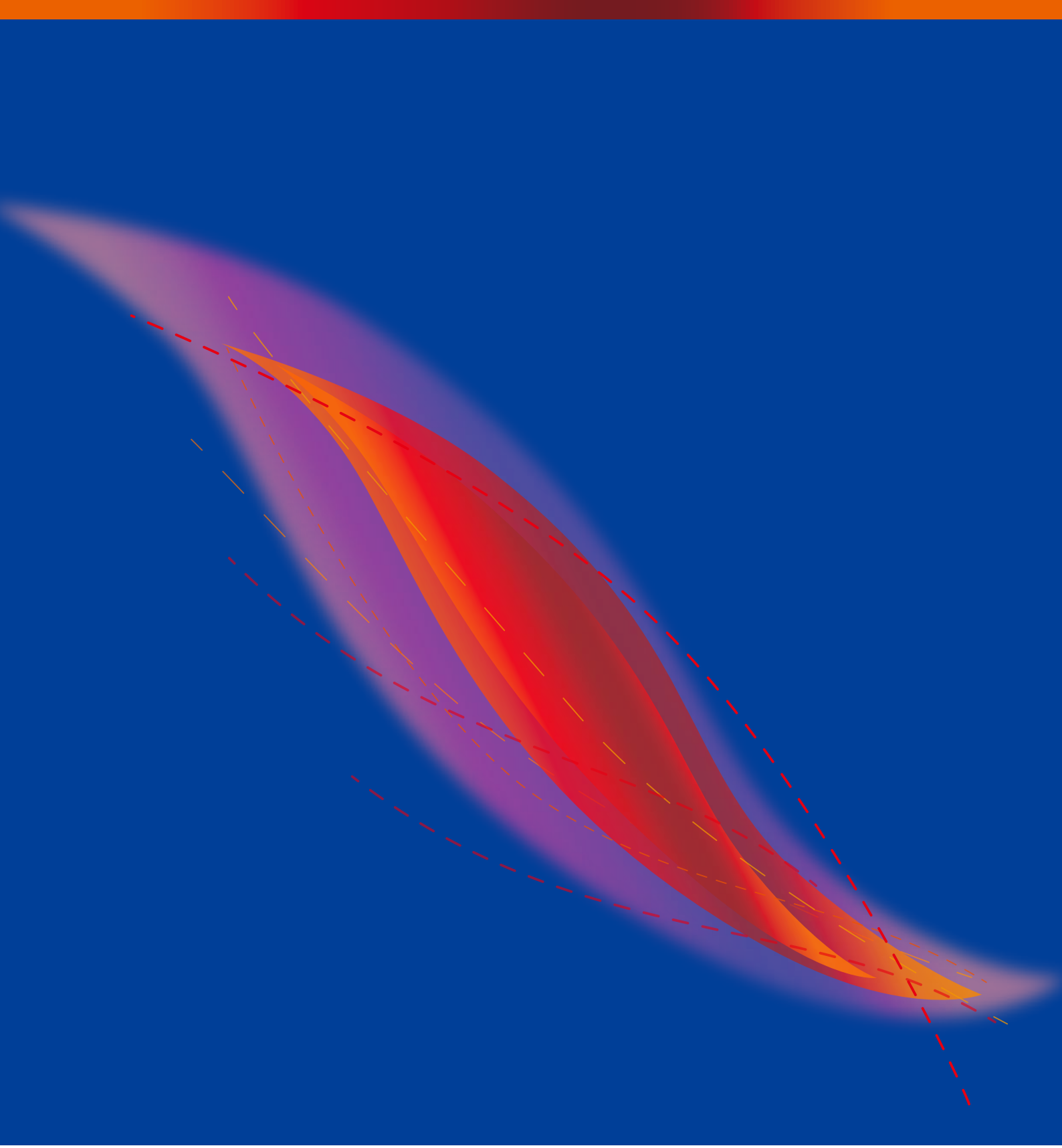
FortiGate/FortiWiFiから管理可能なアクセスポイント、WiFi環境を簡単拡張！

FortiGate/FortiWiFiが搭載する無線LANコントローラ機能と連携し、セキュアな無線ネットワークを実現します。IEEE802.11 a/b/g/nに準拠し、2.4GHzと5GHzの周波数帯におけるセキュリティ機能とPCやスマートフォン/タブレット等のデバイスからのアクセスを提供します。

FortiToken Mobile

お手元のスマートフォンがワンタイムパスワードのトークンに変身！

FortiTokenの認証ソリューションは、外部から社内ネットワークへアクセスする際の二要素認証を簡単に実装できます。ID/パスワードなどの従来の認証に加えて、スマートフォンを利用したもう一つの要素で取得したワンタイムパスワードを入力させることで、外部からの認証時のセキュリティ侵害のリスクを低コストで軽減する事ができます。



製品に関する情報はこちらでご確認いただけます。

Home Page **canon-its.jp/**

キヤノンITソリューションズ株式会社　セキュリティソリューション事業部
〒140-8526　東京都品川区東品川2-4-11　TEL(03)6701-3438　FAX(03)6701-3470

開発元：Fortinet Inc.

Canon キヤノン ITソリューションズ株式会社
〒140-8526　東京都品川区東品川2-4-11

●お求めは信用のある当社で

2014年7月現在

FG14073000HTS-541