フォーティネット ソリューション別製品カタログ

Solution Guide

FORTINET®

CONTENTS

サイバーセキュリティを必要な場所に。

FORTINET®

設立	2000年10月
創立者	KenXie、MichaelXie
本社	米国カリフォルニア州サニーベール
NASDAQ上場(FTNT)	2009年11月
株式上場	NASDAQ100、S&P500
メンバー	DowJonesSustainabilityIndex
投資適確格付け	BBB+Baa1

フォーティネットは20年以上にわたり、サイバーセキュリティの進化と、ネットワーキングとセキュリティの融合をリードしてきました。当社のセキュリティソリューションは、業界で最も多くの導入実績、特許取得、評価を誇るソリューションの1つです。

会社概要

フォーティネットは、世界中の66万を超える企業、サービスプロバイダ、政府機関のセキュリティを支えています。

グローバルな顧客基盤
660,000社以上
顧客数

2022年度の取扱高
55.9億ドル以上
(2022年12月31日現在)

時価総額
382億ドル
(2022年12月31日現在)

広範で統合された
50以上
企業向けサイバーセキュリティ
製品ポートフォリオ

アナリストによる高い評価
33件
エンタープライズ
アナリストレポートに掲載

垂直統合
10億ドル以上
ASIC設計 / 開発への投資

フォーティネットのミッションは単なる技術革新ではありません

持続可能な社会の実現

2030年までに
カーボンニュートラル
の実現

ASIC
最大で
16倍
の高い電力効率

S&PグローバルのCSA評価に基づく
DJSIメンバー
(ダウ・ジョーンズ・サステナビリティ・インデックス)

ネットゼロのサニーベール
本社キャンパスが完成

**サイバーセキュリティの
スキルギャップの解消**

2026年までに
100万人のサイバー
セキュリティトレーニング

これまで発行したNSEの認定証
100万人以上

526の教育機関パートナー

34の教育支援パートナー

WORLD ECONOMIC FORUM CYBERSECURITY
サイバーセキュリティ学習拠点

サイバー攻撃の阻止

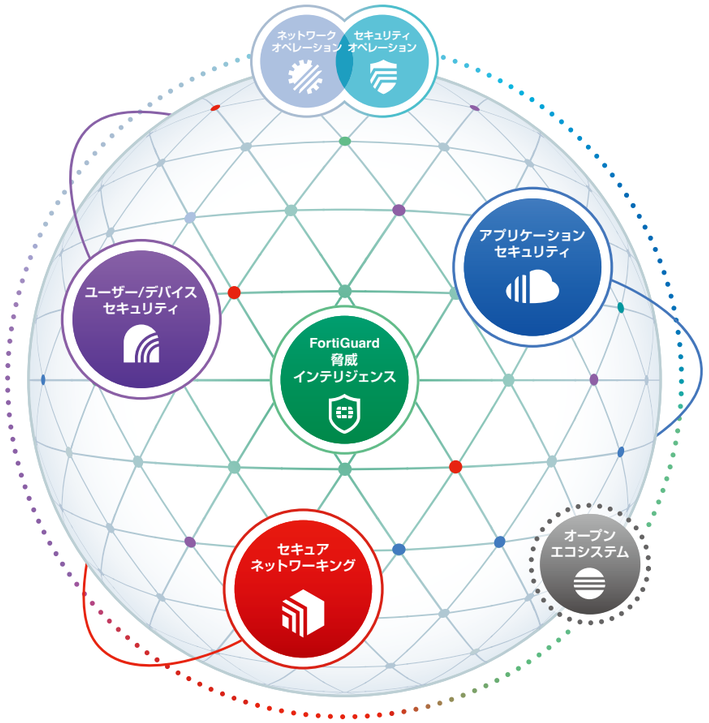
LABS
480以上
の脅威インテリジェンス、検知、保護、
および修復のパートナー

グローバルなリーダーシップとコラボレーション

MITRE ENGENUITY
INTERPOL
WORLD ECONOMIC FORUM CYBERSECURITY
CYBER THREAT ALLIANCE
NATO OTAN
FIRST

セキュリティファブリック

FortiOSをベースとする業界最高パフォーマンスのサイバーセキュリティプラットフォーム



- デジタル攻撃対象領域と攻撃サイクルの拡大に対応し、デバイス、データ、アプリケーションを保護する、自己修復型のセキュリティとネットワーキングを実現します。
- コンバージェンスと統合の概念を組み合わせることで、ユーザーからアプリケーションまでの包括的でリアルタイムのサイバーセキュリティ保護を提供します。

ファブリックを構成する3つの属性

BROAD

**あらゆる場所で脅威を検知し、
セキュリティを適用する**

フォーティネットの広範なポートフォリオは、エンドポイント、ネットワーク、クラウドを保護する、ネットワーキングとセキュリティが統合されたコンバージドソリューションを提供します。これにより、すべてのデジタル攻撃対象領域とライフサイクルにわたって、高性能な接続性と連携したリアルタイムの脅威検知とポリシーの適用が可能になります。

INTEGRATED

**セキュリティギャップを解消し、
複雑さを軽減する**

トップクラスのテクノロジーにAIを活用した一元的な脅威情報分析と自動化された防御を統合することでサイバーセキュリティプラットフォームの構築を実現します。異なるテクノロジー、場所、適用環境であっても一貫性のあるセキュリティと簡素化された運用を可能にします。

AUTOMATED

**脅威の防止にかかる時間を短縮し、
運用を効率化する**

クラウドのスケーラビリティと高度なAIを活用したコンテキスト対応の自己修復型ネットワーク/セキュリティ態勢により、ユーザーとアプリケーションを連携させた保護をほぼリアルタイムかつ自動的に提供します。プロセスの自動化によって大規模導入環境の運用が簡素化されるため、ITチームがイノベーションに集中できるようになります。

セキュアネットワーキング

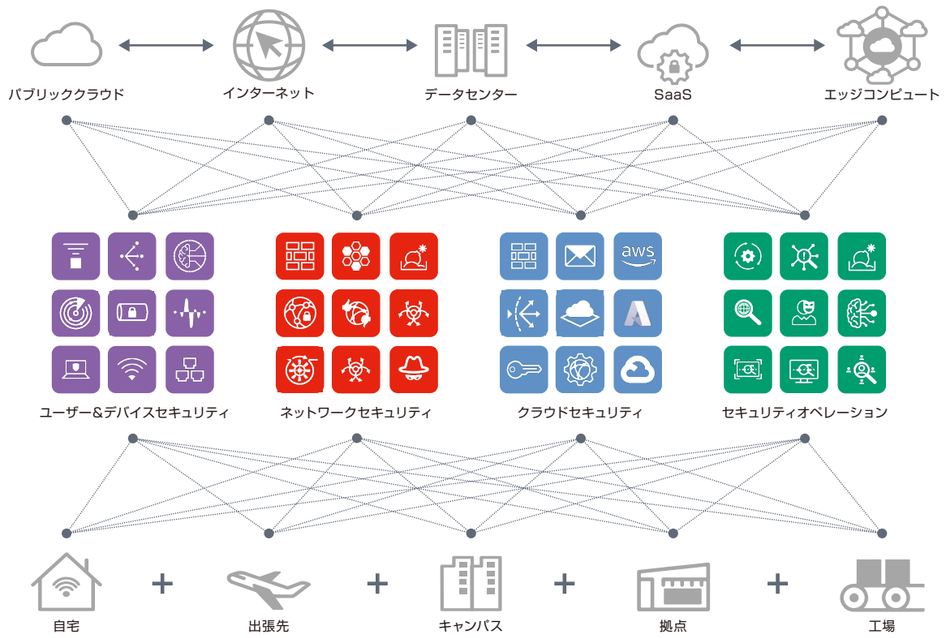
https://www.fortinet.com/jp/solutions/enterprise-midsize-business/network-security

課題

リモートワークやクラウド利用の広がりによって、従来の境界防御ではセキュリティを維持できない

複雑なアーキテクチャではセキュリティ態勢が脆弱に

増え続けるポイントプロダクトから生まれる大きな課題



運用負荷の増大

ネットワークとセキュリティのソリューションがバラバラに存在することで、ネットワーク全体の可視性と管理性が大幅に低下し、日々の運用負荷が増大する。

セキュリティ態勢の低下

複数のソリューションを複数の管理コンソールで個別に管理する状態では、ネットワーク全体で一貫したセキュリティを維持することが難しくなる。

ユーザーエクスペリエンスの低下

クラウド利用の拡大によりインターネット通信が大幅に増加するため、境界防御のアーキテクチャでは、クラウドアプリケーションの利用品質低下が問題になる。

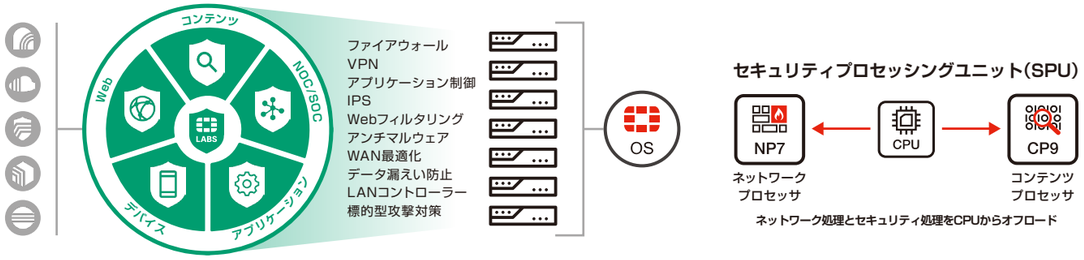
ソリューション

ネットワーキングとセキュリティのコンバージェンス(融合)を実現する、業界最高パフォーマンスのエンタープライズセキュリティ

柔軟で高性能なネットワークセキュリティ | 次世代ファイアウォール

ユーザーやデバイス、アプリケーションが分散・多様化する現代の企業ネットワークでも、1つのOSで一貫したセキュリティをパワフルに展開

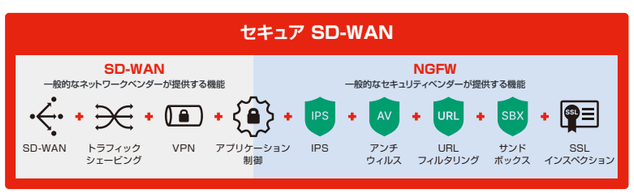
- FortiGate1台で多くのセキュリティ機能が利用可能
- 自社開発のASICを搭載しているため、負荷の高い処理もパワフルに行える

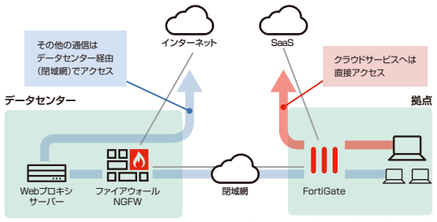


安全で快適なクラウドサービス利用 | セキュアSD-WAN

ビジネスに直結するクラウドサービスの利用品質向上とセキュリティを1台で実現

- SD-WANとセキュリティの機能を1台で利用可能
- 許可したSaaSは拠点から直接アクセス*させることで、SaaSの利用品質向上とデータセンターの負荷を軽減
- FortiSASEを組み合わせることで、オフィスのセキュリティをリモートユーザーに拡張可能



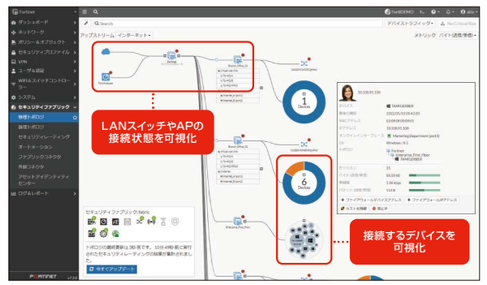


インターネットブレイクアウトのイメージ

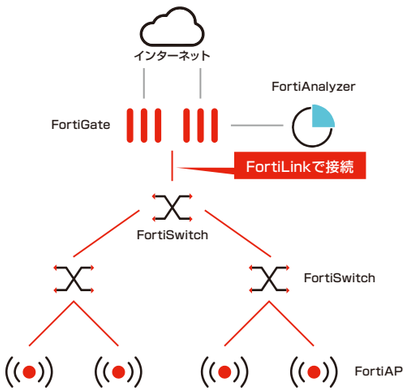
LAN環境の可視化と一元管理 | セキュアSDブランチ

スイッチやアクセスポイント、そしてエンドポイントまでLAN環境全体をビジュアル表示し、機器やデバイスの状態を可視化

- FortiGateでLANスイッチやアクセスポイントを一元管理
- LANスイッチ、アクセスポイント、エンドポイントを可視化



FortiGate GUI画面



ソリューションコンポーネント

FortiGate、FortiExtender、FortiAP、FortiSwitch、FortiManager、FortiSASEなど

次世代ファイアウォール（FortiGate）

幅広い適用領域で（Broad）システム連携し（Integrated）自動化された（Automated）サイバーセキュリティソリューション

セキュアSD-WAN & 5G（FortiGate, FortiExtender）

WANの最適化とセキュリティを確保することで、ユーザーエクスペリエンスの向上とリスク軽減を同時に実現

セキュア有線&無線LAN（FortiGate, FortiSwitch, FortiAP）

FortiGateの標準機能で、FortiSwitch、FortiAPを集中管理するセキュアSDブランチソリューション

セキュアアクセスサービスエッジ（FortiSASE）

リモートユーザー向けに、FWaaS、プロキシ（SWG）、ZTNAなどセキュリティとネットワーキング機能をSaaSで提供

ネットワーク運用（FortiManager, FortiGate Cloud, FortiLAN Cloud）

分散する複数のフォーティネット製品を1つのコンソールで一元管理

AIを活用したセキュリティサービス

FortiGuard Labsが提供するAIを活用した脅威インテリジェンスにより、最新の脅威からリアルタイム保護

事例｜株式会社サザビーリーグ

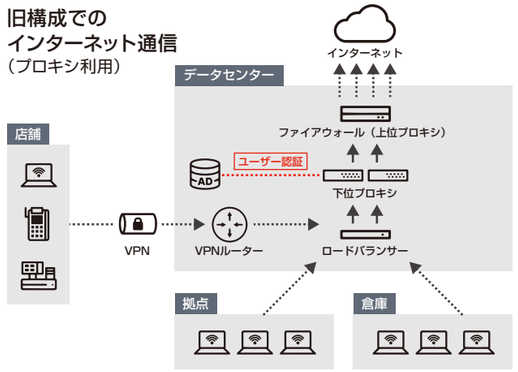
https://www.fortinet.com/content/dam/fortinet/assets/case-studies/ja_jp/cs-sazaby-league.pdf

2台のプロキシサーバーと1台のロードバランサーをFortiGate1台に集約

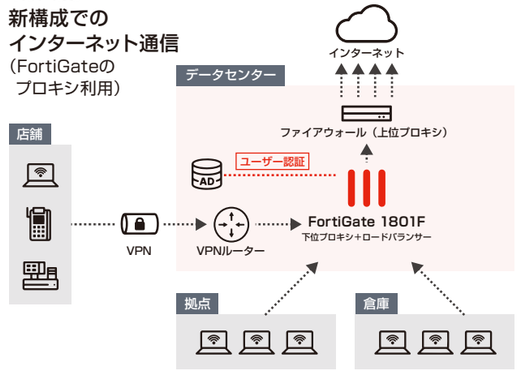
導入のポイント

- アパレル、生活雑貨、飲食など多様な業態のビジネス部門に対して、Webプロキシでポリシー統合と保護を実現
- 既存のネットワーク構成や従業員の使い勝手を変更せず、わずか3カ月で移行を実現
- 管理対象となるハードウェア台数を集約することで、ランニングコストを大幅に削減
- 直感的で分かりやすい管理画面により、設定変更などの運用負荷を軽減

〈導入前〉
旧構成での
インターネット通信
（プロキシ利用）



〈導入後〉
新構成での
インターネット通信
（FortiGateの
プロキシ利用）

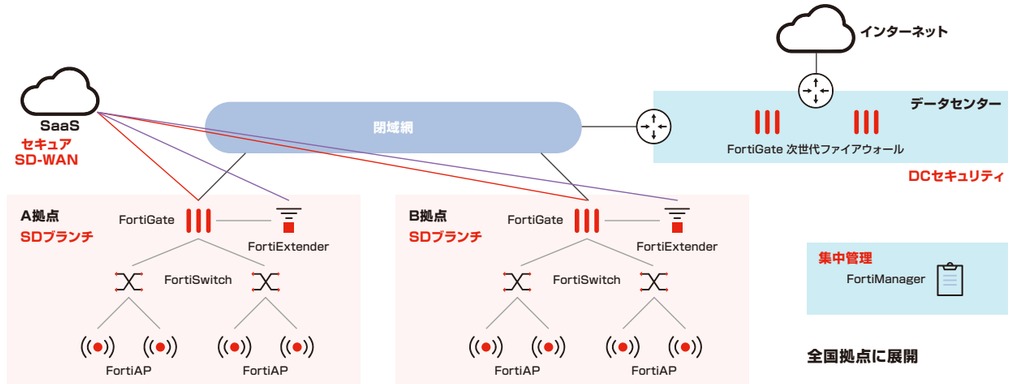


事例｜金融機関のお客様

レガシーWANルーターをSD-WANに刷新し、SaaS利用を快適に SDブランチでLAN環境の可視化も実現

導入のポイント

- 全国拠点にセキュアネットワーキング（NGFW/SD-WAN/SDブランチ）を採用
- データセンターのファイアウォールをFortiGateに置き換え
- 数百台ものフォーティネット製品をFortiManagerで集中管理



アクセス&
エンドポイントセキュリティ

https://www.fortinet.com/jp/solutions/enterprise-midsize-business/work-from-anywhere

課題

Work From Anywhere(場所に縛られない働き方)
リモートワークによる端末の増加、マルウェアや標的型攻撃のリスク、
ゼロトラストネットワークアクセスなど

ユーザーとデバイスの安全性の保護

リモートユーザーの拡大にともない、場所に依存しないユーザー/デバイスの一貫したセキュリティ対策が求められています。

リモートユーザーのセキュリティが不十分で、どこにいてもユーザーとデバイスの一貫した一貫したセキュリティ態勢を維持できません。

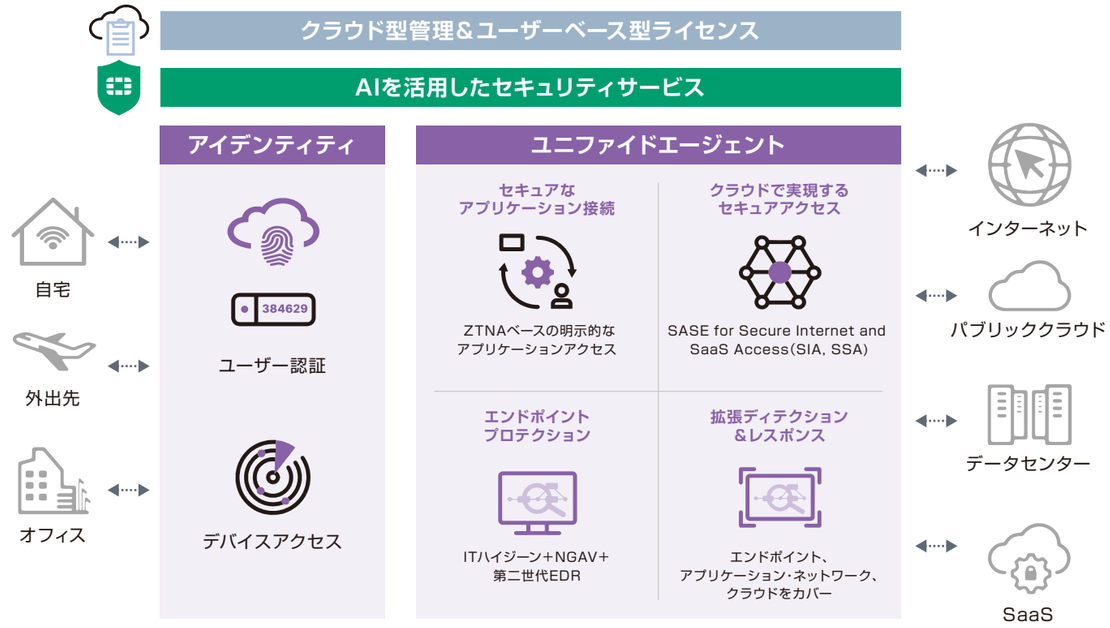
従来のVPNベースのアクセスでは、必要なきめ細かなアクセスコントロールができません。

特定のポイントプロダクトやエージェントが独立して導入・運用されているため、業務が複雑になり、全体的な可視性が不足しています。

従業員がどこからでも仕事ができるよう、デバイスはネットワークの外でも強力なセキュリティが必要です。さらに、外だけでなく内からのアクセスにも注意が必要になっています。

ソリューション

FortiSASE、FortiClient、FortiEDR、FortiAuthenticator、
FortiNACなどを利用したエンドポイント保護



・ゼロトラスト・エブリウェア

場所に縛られることなく、ユーザー/デバイスに対して一貫したセキュリティとアプリケーション制御を提供します。

・クラウドで実現するセキュリティ

エンタープライズグレードのセキュリティをクラウドから拡張し、リモートユーザーを強力に保護します。

・デバイスのアクセスコントロール

デバイスの検出、アクセス制御、およびエッジでのネットワーク保護が容易に行えます。

・モダンエンドポイントセキュリティ

最も巧妙なサイバー攻撃を阻止するためのエンドポイントの高度な脅威保護、検知、対応を自動化します。

・シングルベンダーSASE

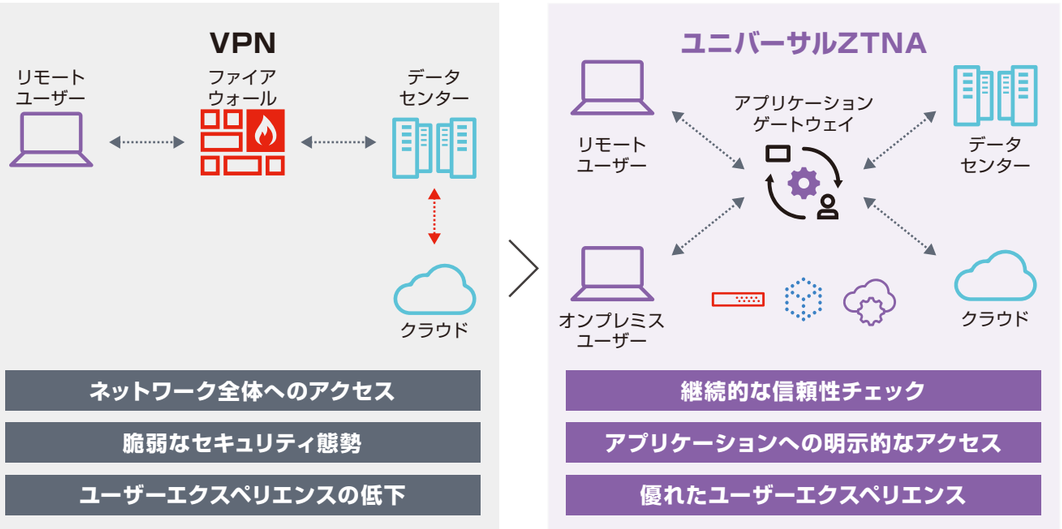
フォーティネットは単一のベンダーでSASEの環境構築に必要な全てのプロダクトを提供できます。シングルベンダーSASEにより、複数製品の使用による複雑さを軽減し運用にかかるコストを大きく削減します。

ソリューションコンポーネント

FortiSASE、FortiClient、FortiEDR、FortiAuthenticator、ZTNA、FortiNACなど

ユニバーサルZTNA(ゼロトラストネットワークアクセス)

安全な接続を実現するために、継続的なユーザー/デバイスの検証を行い詳細なアプリケーション制御を提供します。



セキュアアクセスサービスエッジ(FortiSASE)

SaaS型セキュリティとネットワークにより、リモートユーザーをより安全に、より優れたユーザーエクスペリエンスで保護することができます。

エンドポイントディテクション&レスポンス(FortiEDR)

ランサムウェアや高度なサイバー攻撃を阻止する最新のエンドポイントセキュリティを提供します。

AIを活用したセキュリティサービス

FortiGuardによってAI分析された脅威インテリジェンスにもとづき、リアルタイムにセキュリティの脅威に対抗する機能を提供します。

アイデンティティ&アクセス管理(IAM)

企業リソースに安全にアクセスするために、ユーザーアイデンティティの管理・認証・認可の機能を提供します。

ネットワークアクセスコントロール(FortiNAC)

企業ネットワーク上のデバイスに対して可視化、制御、自動応答を実現します。ゼロトラストネットワークアクセスを実現するためには、ネットワークに接続するデバイスとユーザーの可視化と制御が必要です。

事例｜大学共同利用機関法人 自然科学研究機構

https://www.fortinet.com/content/dam/fortinet/assets/case-studies/ja_jp/cs-nins.pdf

SaaS利用環境、9,000台のマルチOS端末環境で、SSO/SAMLを実現

概要

大学共同利用機関法人自然科学研究機構(NINS)は、旧岡崎国立共同研究機構から引き継いだ基礎生物学研究所、生理学研究所、分子科学研究所という3つの研究機関(岡崎3機関)に加え、国立天文台、核融合研究所という5つの研究所から構成された大学共同利用機関法人です。

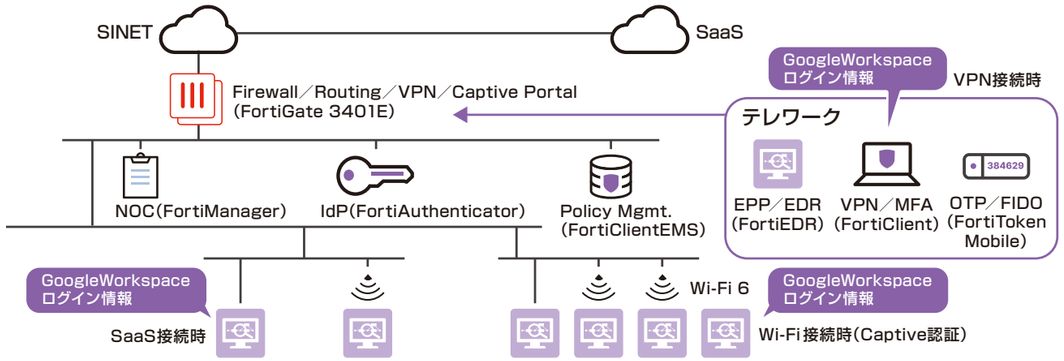
既存のネットワークシステムの更改をきっかけに、個人を認証する仕組みに作り変えることにしました。また、メーカーを統一したいという要望から、フォーティネットが選ばれました。具体的には、SINETとの100GbE接続が可能であることから処理性能が高いこと、認証システムとしてSAML、SSOに対応していること、多くの種類のPCやスマートデバイスに対応していること、少人数運用が可能なEDRがあることが要因となりました。

導入のポイント

- 一人一アカウント制を活用し、機器単位ではなくユーザー単位の強固な認証を実現
- セキュリティ領域の機能をフォーティネット製品に統合
- 各製品のAPIと開発者向け情報を活用し、運用ツールを開発

ORION2022:ネットワーク/SaaSセキュリティ

SaaS IDを利用したSaaSおよびネットワークアクセス制御



※ORION22 (Okazaki Research Institutes Organization Network 2022)

セキュアアプリケーションジャーニー

https://www.fortinet.com/jp/solutions/enterprise-midsize-business/cloud-security

課題

クラウド移行/利用に伴うデータ保護、アプリケーションの脆弱性、アクセス管理など

アプリケーションはデータセンター、マルチクラウド、エッジコンピュートまであらゆる場所に存在することができます。多くの企業は拡張性やサービスの統合などを理由に2つ以上のクラウドサービスを利用しています。

企業はセキュリティリスクの増大、運用の複雑さ、設定の誤り、可視性の欠如など、加速するクラウド利用の余波に対処を続けています。

アプリケーションとデータをユーザーやデバイスに近い場所に配置するエッジコンピューティングの出現。さらに、2026年にはエッジコンピューティングの採用が2021年と比較して15%増加すると言われています。

クラウドセキュリティの設定ミス、安全でないインタフェース/API、機密データの漏洩、不正アクセスは、引き続きクラウド環境における脅威の上位を占めています。

組織的な事情、プロセス、技術要件の検討の結果、ツール、ソリューション、プラットフォームが増え続ける。

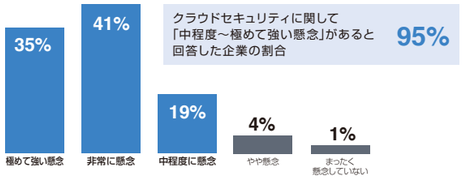
ソリューション

FortiGate、FortiWeb、FortiMail、FortiGate CNFによるアプリケーション保護

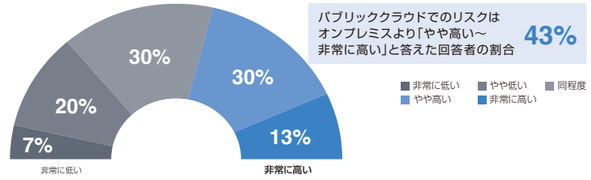
パブリッククラウドのセキュリティに関する懸念

クラウド導入は拡大しているものの、クラウドセキュリティに関する懸念に改善の兆候は見られません。パブリッククラウド環境の自社のセキュリティポスチャについては、ほぼすべての企業(95%)が「中程度～極めて強い懸念」があると回答しています。パブリッククラウドのセキュリティに極めて強い懸念を抱いている企業の数は昨年の32%から、今年は35%に増加しています。

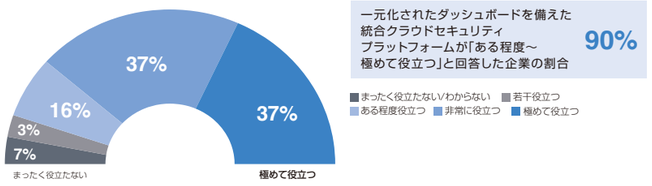
パブリッククラウドのセキュリティについてどの程度懸念がありますか？



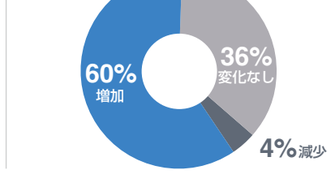
従来のオンプレミスIT環境と比べて、パブリッククラウド環境でのセキュリティ侵害リスクは高いと思いますか、それとも低いと考えますか？



一元化されたダッシュボードを備えた統合クラウドセキュリティプラットフォームを使って必要なすべてのポリシーを設定し、クラウドのフットプリント全体で一貫して総合的にデータを保護できればどの程度役立ちますか？



今後1年でクラウドセキュリティ予算はどのように変化しますか？



アプリケーション/クラウドセキュリティ

データセンターやパブリッククラウドなどアプリケーションが稼働するあらゆる場所で、一貫したセキュリティと一元的な可視化、管理を実現

・幅広いユースケースをカバー

現在および将来にわたるアプリケーションジャーニーを保護するために、包括的でスケーラブル、かつ柔軟なセキュリティソリューション

・Webアプリケーション、メールを保護

WAFによる企業、組織のWebアプリケーションを保護

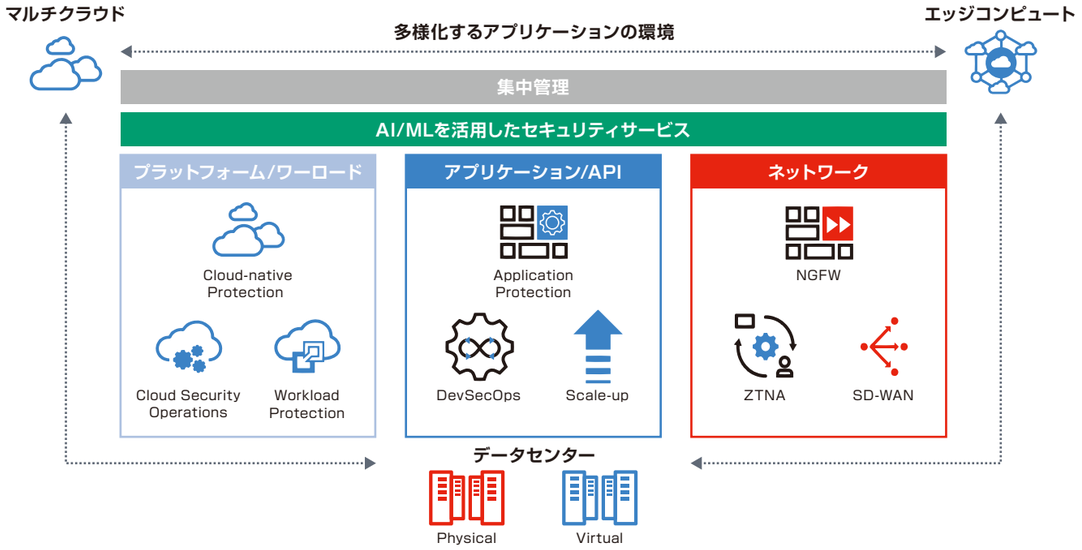
SaaS利用が進む最も普及しているメールアプリケーションの保護でランサムウェア被害を軽減

・クラウドネイティブセキュリティ

ハイブリッドクラウドを想定し、クラウド間のセキュリティギャップを減らす、クラウドネイティブの統合による運用の簡素化

ソリューションコンポーネント

FortiGate、FortiWeb、FortiMail、FortiGate CNFなど



ハイブリッドネットワークセキュリティ（FortiGate VM）

クラウド、データセンター、ハイブリッドクラウド、エッジコンピュート間のネットワークを保護し、シームレスに接続

メールセキュリティ（FortiMail VM/ FortiMail Cloud）

メールおよび添付ファイルのセキュリティ検査を実現

Webアプリケーション&API保護（FortiWeb VM / FortiWeb Cloud）

AI/MLと自動化で、Webアプリケーションおよび APIのセキュリティを実現しつつ簡素化も実践

クラウドネイティブセキュリティ（FortiGate CNF）

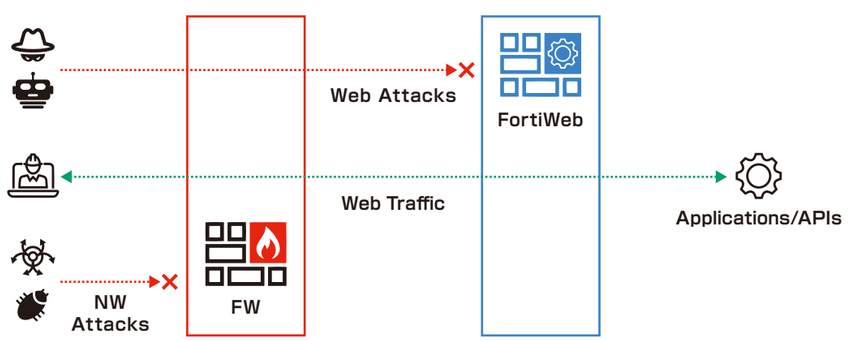
企業組織で利用中のクラウドサービスと統合し、ネイティブに動作するセキュリティで、クラウド導入時の障壁を軽減

サブスクリプションサービスの利用（FortiFlex）

FortiFlexとして従量課金型セキュリティをご用意、ポイント購入もしくは使用量に応じた課金で利用可能

FortiGuardサービス

アプリケーションやワークロードがどこにあってもリアルタイムに保護することが可能



事例｜アイビーシー株式会社

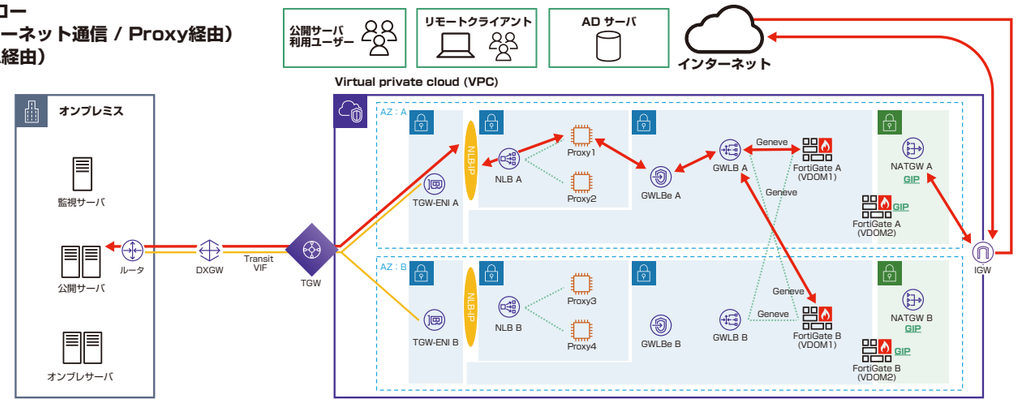
https://www.fortinet.com/content/dam/fortinet/assets/case-studies/ja_jp/cs-ibc.pdf

既設の次世代ファイアウォールをAWS上に移行し、クラウド利用における帯域圧迫を解消

導入のポイント

- 逼迫したネットワークを、クラウド上の次世代ファイアウォールで解決
- アプライアンスFortiGateと同じ操作性のFortiGate VM
- 既存のアクセスポリシーをそのまま移行できた
- 複数製品で実現していたセキュリティ機能を FortiGate VM に集約できた

通信フロー（インターネット通信 / Proxy経由）（AZ:A経由）



事例｜株式会社トヨタシステムズ

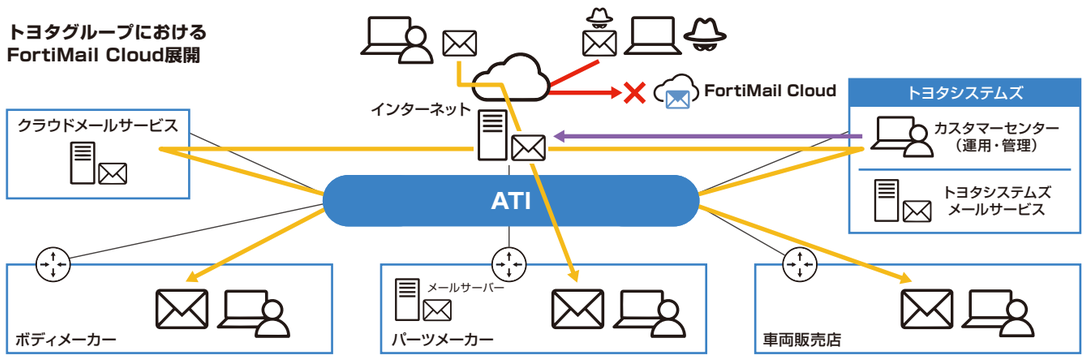
https://www.fortinet.com/content/dam/fortinet/assets/case-studies/ja_jp/cs-toyota-systems-fortimail.pdf

クラウドサンドボックスを活用し、メール経由のサイバー攻撃対策を強化

導入のポイント

- トヨタグループ約700社の新たなメールセキュリティとして短期間で更改できた
- クラウドサンドボックスで未知の脅威からの保護を実現
- 事前チューニングによる過検知、誤検知の抑制
- 管理画面が日本語対応しており、運用担当者への引き継ぎも短期間で実施

トヨタグループにおける FortiMail Cloud展開



Automated SOC

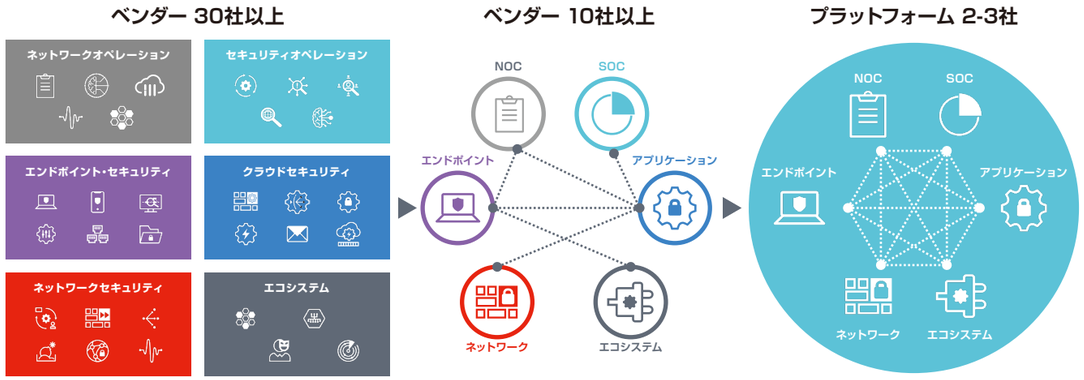
https://www.fortinet.com/jp/solutions/enterprise-midsize-business/security-operations

課題

セキュリティインシデントの迅速な検出と対応、脅威インテリジェンスの活用、スキル不足や運用負荷の軽減

サイバーセキュリティプラットフォームジャーニー

拡大された攻撃対象領域全体にわたって、進化する脅威動向に対応し続ける



攻撃対象領域の拡大

デジタルイノベーション(WFA、クラウド、サプライチェーンを含む)により、攻撃対象領域と攻撃者への露出が拡大。

進化し回避能力を持つ攻撃

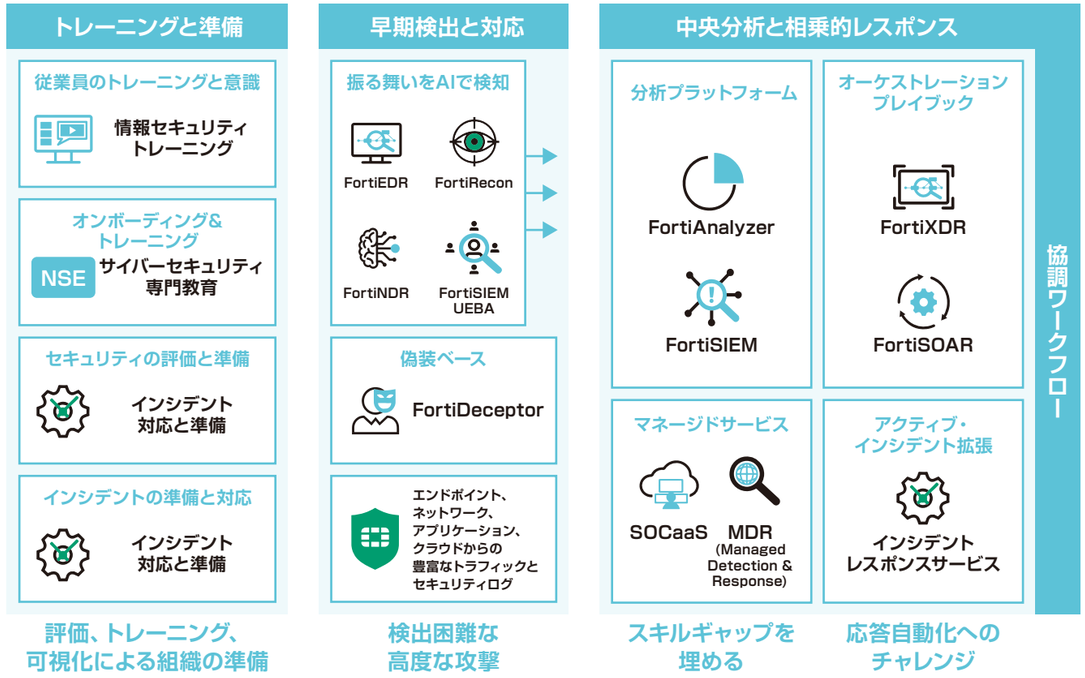
正当なアクティビティを模倣する、ますます洗練された多段階攻撃が、しばしばセキュリティを回避します(攻撃の巧妙化)。そのため、迅速な対応が求められており、多くのタスクをマシンやシステムに任せる必要が出てきます。

セキュリティの複雑さ

セキュリティ製品とその管理コンソールが多い、特定・対応が遅い、サイバースキル不足による悪化。そのため、多くの企業でセキュリティ製品のベンダーを統一しようとする動きがあるものの、まだ十分に進んでいるとは言えません。

ソリューション

プロアクティブなサイバーセキュリティを実現するFortiEDR、FortiDeceptor、FortiRecon、FortiAnalyzer、FortiSIEM、FortiSOARなどを利用した自動化されたSOC、インシデントレスポンスなどの支援サービス



・早期検出(EDR ｜ NDR ｜ Deceptor ｜ Recon)

サイバーキルチェーンに沿った攻撃を検出および停止するためのエンドポイントおよびその他の動作判別ベースのセンサー

・インシデント検出時間の短縮:Analyzer/SIEM

機械学習を使用し正規化されたデータ分析で、攻撃対象領域全体のインシデントを検出

・迅速なインシデントレスポンス:SOAR/EDR/Recon

セキュリティ運用の統合化/自動化により迅速かつ相乗的な対応

・SOC支援/補強サービス

インシデントレスポンス(IR)、攻撃アセスメント、トレーニングにより社内チームを補強

・AI-Poweredセキュリティサービス

より早く検知・対応するためのインテリジェンスとエンジン

ソリューションコンポーネント

FortiEDR、FortiDeceptor、FortiRecon、FortiAnalyzer、FortiSIEM、FortiSOAR、など

FortiEDR

第二世代EDRとして、マルウェアなどの感染前後でエンドポイントを保護し、データの侵害と不正使用、ファイル暗号化といった攻撃をリアルタイムで自動的に阻止します。

FortiNDR

人材不足に悩むセキュリティオペレーションセンター（SOC）組織のために設計された、AIドリブンマルウェア分析の未来を開拓するアプライアンスです。

FortiDeceptor

既存の侵害防御戦略を補完するソリューションです。サイバーキルチェーンの初期段階で社内外の攻撃者に罠を仕掛け、特定、排除することで、深刻な被害を未然に防ぎます。

FortiRecon

SaaSベースのデジタルリスクプロテクション（DRP）サービスです。3つの強力なモジュールである外部攻撃対象領域管理（EASM：ExternalAttackSurfaceManagement）ブランド保護（BrandProtection）アドバイザリーセントリックインテリジェンス（ACI：Adversary-CentricIntelligence）を選択いただけます。FortiReconは、攻撃者が何を見ているのか、何をしているのか、何を計画しているのかを偵察・可視化し、脅威リスク、対応時間、事後対応コストを大幅に低減します。

FortiAnalyzer

フォーティネット製品（FortiGate、FortiEDR、FortiMailなど）のログ情報の管理、データ分析、侵害指標（IoC）の利活用に役立つ製品です。導入形態は、アプライアンス、バーチャルアプライアンス、SaaSからお選びいただけます。

FortiSIEM

既存でお使いのネットワーク製品、セキュリティ製品、サーバー製品の情報を収集し、SOCチームにおけるインテリジェンス活用に寄与する製品です。フォーティネット製品だけでなく、マルチベンダー構成のシステムでご利用いただけます。導入形態は、アプライアンス、バーチャルアプライアンス、SaaSからお選びいただけます。

FortiSOAR

SOCチームにおけるセキュリティ運用の平準化を実現するサービスで、マルチベンダー環境でご利用いただけます。プレイブックの活用でSOCチームの業務効率を強力に向上することが可能です。すでにお使いのチケットシステムなどSOCツールと連携可能です。

事例｜ホテルモントレ

https://www.fortinet.com/content/dam/fortinet/assets/case-studies/ja_jp/cs-hotel-monterey.pdf

24時間365日営業のホテル業務を支えるSOCサービスとの組み合わせでFortiEDRを選定

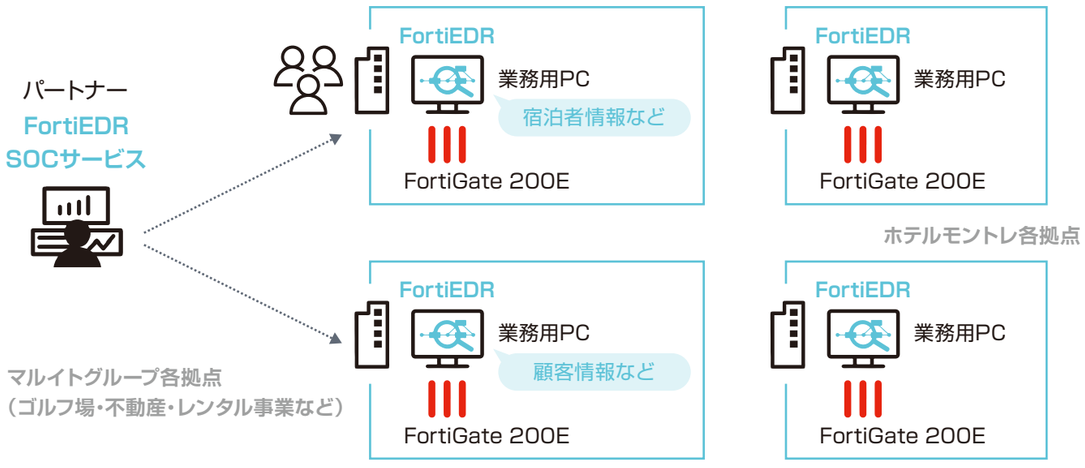
概要

全国21ヶ所に個性豊かなホテルを展開しているホテルモントレ。システムを暗号化するEmotetの大流行などサイバー攻撃の高度化及び増加を背景に、守りのデジタル戦略にも力を入れています。ホテルで取り扱う個人情報は機密性が高く保護すべきものが多くあります。もちろん情報が漏洩しないことが一番ですが、万一漏洩してしまっても、速やかに経路を調査し、対処できるように、セキュリティ環境の整備が検討されました。そこで注目したのはEDRでした。

他の製品と比較した際にFortiEDRはコストパフォーマンスが優れていると感じられ、さらにSOCと連携できることを知り、導入を決定されました。24時間365日体制のSOCサービスにより、運用への安心感を得られ、システム課の運用負荷は大きく削減されました。

導入のポイント

- 少人数のシステム課の運用負荷を大きく軽減
- フォーティネットのパートナーが提供するSOCサービスを組み合わせ、24時間365日でのEDR運用体制を整備
- FortiGateで検知した脅威情報を連携させることで、最新の脅威を速やかに検知
- わかりやすい管理画面によって、脅威の感染拡大からの保護状況を可視化



OTセキュリティ

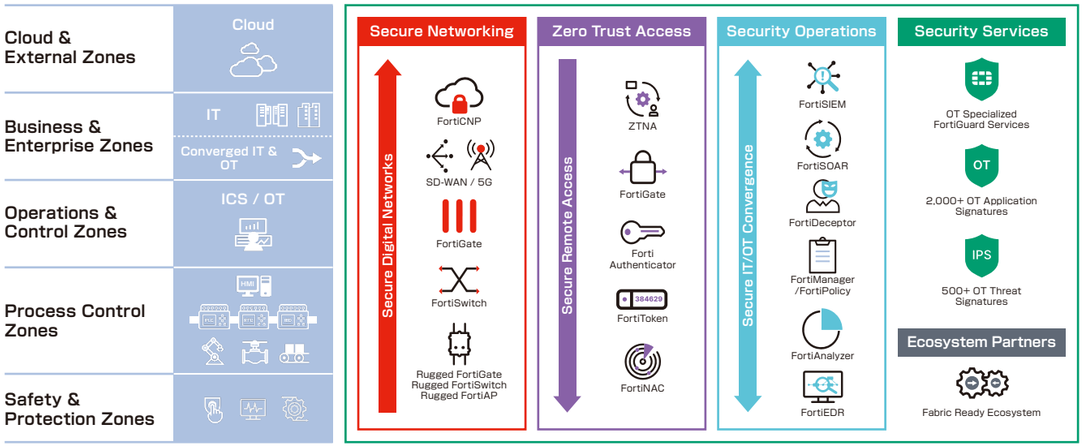
https://www.fortinet.com/jp/solutions/enterprise-midsize-business/ot-security

課題

産業制御システムのセキュリティ脅威、サイバー攻撃による生産停止リスク、リモートアクセスの安全性の確保

セキュアなOT環境を実現するために

※OTとは、産業分野で必要な製品や設備、システムを動かすための制御技術のこと。OperationalTechnology(オペレーショナルテクノロジー)の略。



- ほとんどの産業用制御システムは、設計上セキュリティが欠如しており、変化に敏感である。かつてはOTに関わるシステムは完全に分離されていたため、セキュリティを意識する必要がありませんでした。しかし、現在はビジネスやサードパーティ製品との繋がりが不可欠です。
- サイバーフィジカルアセットの攻撃対象領域は拡大し、エアギャップによる保護への依存度は低下しています。
- IT-OTネットワークの融合を促進するデジタルトランスフォーメーション(Industry 4.0)の取り組み
- 5G、IoT、クラウドなど新技術の導入が進む
- システムメンテナンス要員など第三者や従業員のリモートアクセス要件が新たなリスクを引き起こす。
- 資産所有者がOEMやSIに依存することで、重要なシステムがさらなるリスクにさらされる。
- OT環境ではセキュリティインシデントが過小評価される傾向があります。ランサムウェアの脅威が事業停止を引き起こすため、最も懸念される。

ソリューション

FortiGate、Ruggedモデル、FortiSwitch/FortiAP、FortiAnalyzer/FortiManager、FortiClientによるZTNA、FortiNAC、などを利用したOT環境の保護

OT環境特化製品

- Ruggedモデルのファイアウォール、スイッチ、ディセプター
- 世界で最も導入されているIT/OT次世代ファイアウォール
- OTに特化したSIEM、EDR、サンドボックス、ディセプション機能

OT環境特化の脅威インテリジェンス

- 70以上のOTプロトコルに対応したDPI
- ペイロードレベルまでの可視化と制御
- OTシステムの脆弱性の保護
- 他のサイバーセキュリティベンダーの中で最も多くのIPSシグネチャを搭載しています。

OT環境特化サービス

- 業界で検証され、参照されたソリューション
- 経験豊富なOTのプロフェッショナル
- OT専門インテグレーター
- 1000人以上のプロフェッショナルサービスエンジニア

他社製品との連携

- 豊富なソリューションインテグレーションプラットフォーム
- 500以上のSecurity Fabricエコシステムとの統合
- 主要なOTセキュリティ・ソリューションとすぐに統合できます。

・セキュアな接続性

デジタルトランスフォーメーションには、OTからデータセンター、クラウドへの安全なデータ接続が必要

・セキュアリモートアクセス

許可されたリモート技術者やサードパーティのためのZTNA(ゼロトラストネットワークアクセス)

・セキュリティ運用のIT/OT融合

OTとITのネットワークをコンバージドSOCで相乗的に管理する。

・AIを活用したセキュリティサービス

進化する脅威を先取りする産業用制御システムに特化したセキュリティサブスクリプションの提供「FortiGuard Industrial Security Service」

ソリューションコンポーネント

FortiGate、Ruggedモデル、FortiSwitch/FortiAP、FortiAnalyzer/FortiManager、FortiClientによるZTNA、FortiNAC、など

FortiGate

脆弱性をついた攻撃からの保護としてIPSや、通信可能なプロトコル、宛先を制限するファイアウォールをオールインワンで提供する次世代ファイアウォール

FortiGate/FortiSwitch/FortiDeceptor Ruggedシリーズ

産業用制御システムのネットワークに対する悪意のある攻撃からの保護、過酷な環境での利用を想定したセキュリティアプライアンス。

耐久性を考慮した設計

ファンレスで耐久性のあるコンポーネントの採用により、過酷な環境でも安定した動作が保証されます。

統合セキュリティアーキテクチャ

FortiGate は、単機能のセキュリティ製品をいくつも導入する場合と比べて所有コストが低く、より優れた保護機能を提供します。FortiGuard Industrial Security Serviceにより産業用に特化したシグネチャの利用が可能です。重要なネットワークがリアルタイムで確実に保護されます。また、SD-WAN に対応しているため、アプリケーションに最適な経路選択が必要な場合、セキュアSD-WANをOT環境でもご利用いただけます。

FortiAnalyzer/FortiManager

産業用制御システムのネットワークに対する悪意のある攻撃からの保護、過酷な環境での利用を想定したセキュリティアプライアンス。

容易な管理

堅牢な管理システムを利用した迅速なプロビジョニングと配備、デバイスおよび脅威の状態の監視が可能になるとともに、実用性の高いレポートを提供します。

FortiClient ZTNA

産業用制御システムにリモートからアクセスする場合、レガシーVPNではなく、ZTNA（ゼロトラストネットワークアクセス）でユーザー情報、デバイス情報、OSバージョンなどを確認した上でアクセス制御を行うことが可能です。

FortiNAC

産業用制御システム上にあるネットワーク機器、デバイス、IoTの可視化を実現するソリューションです。マルチベンダー構成のネットワークシステムでご利用いただくことが可能で、すべてのOT資産を把握できていない企業、組織においても適用いただけます。

事例 | 株式会社トヨタシステムズ

https://www.fortinet.com/content/dam/fortinet/assets/case-studies/ja_jp/cs-toyota-systems-factory.pdf

工場設備、R&D設備における情報共有とセキュリティ確保をFortiGateで両立

概要

自動車メーカーやサプライヤーの情報システムを支えてきたトヨタシステムズ。工場の生産制御システムはOSが古い状態のものが多いものの、「できるだけ手を触れない」ことで成り立ってきました。しかし、IT技術を活用していくためには、どうしても工場のシステムと情報システムを連携させる必要があり、そのためにはセキュリティ面に手を入れていくことが必須でした。

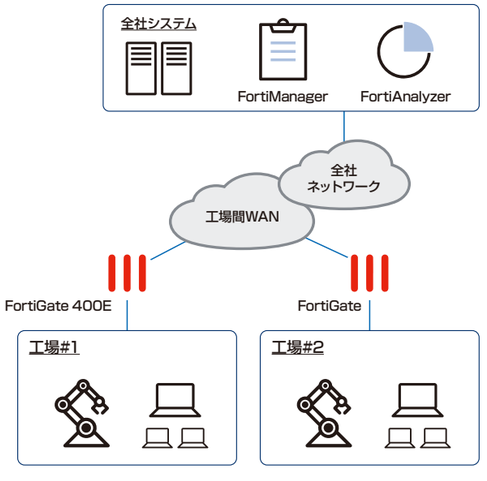
そこで、工場セキュリティのゲートウェイとして、FortiGateの導入を決定されました。他社製品と比較した際にセキュリティパフォーマンスが優れていたことが要因となりました。導入の結果、アクセス制御と不正通信の監視をFortiGate1台に集約し、既存ネットワーク構成に影響を与えない透過的保護を実現しています。

絶え間ないカイゼン活動を通して品質の高いモノづくりに取り組んできたトヨタグループ。デジタル技術を駆使して「コトづくり」へ取り組み始めた今もその精神は変わらず、絶え間なく改善しながらグループ全体のセキュリティの強化に努めていく。

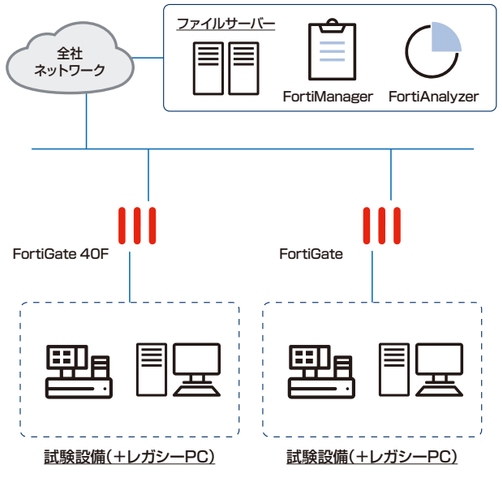
導入のポイント

- 工場とシステムのネットワーク間でアクセス制御と不正通信の監視
- セキュアな形で情報共有を進めて業務を効率化
- OSのアップデートが困難な試験設備に付随するPCをアクセス制御とIPSで保護
- コストパフォーマンスに優れた機器を監視サービスと組み合わせ、負荷の少ない運用体制を実現

工場セキュリティゲートウェイ



試験設備向けファイアウォール



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
https://www.fortinet.com/jp/contact

製品ページ

https://www.fortinet.com/jp/products

ソリューションページ

https://www.fortinet.com/jp/solutions

お問い合わせ

SB-d-SolutionGuide-2306-JP-R2