クラウドサービスのパフォーマンス最適化
～Fortinetによるインターネット(ローカル)ブレイクアウト～

ひらめき、むすんで、その先へ
Thanks 30th ▶ Go 40th

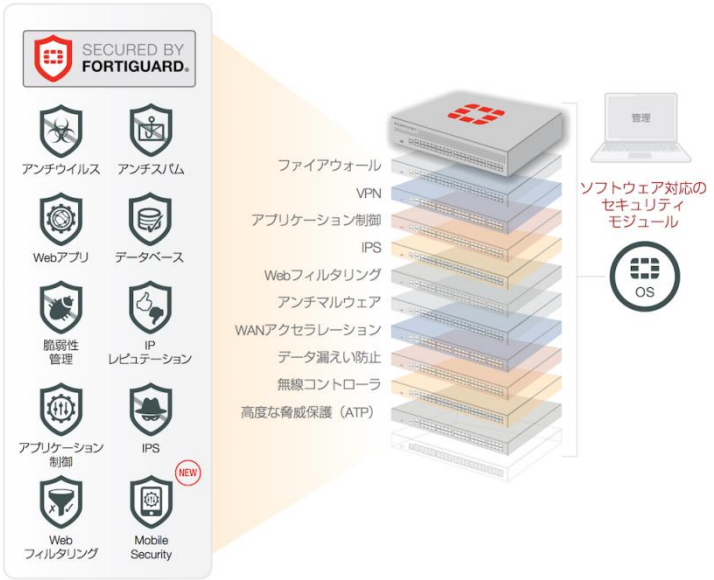
FortiGateとは？

案件登録可能

自営保守対応

UTMアプライアンス（次世代ファイアウォール）

FortiGateは、Fortinet社が独自に開発した専用プロセッサーFortiASICを搭載しており、他社を追随しない圧倒的なパフォーマンス実現することができる製品です。ファイアウォール機能以外にも複数のセキュリティ機能（アンチウイルスやIPSなど）を備えている統合脅威管理製品（UTM）として利用する事も可能です。



FortiGate-200E

FortiGate-800D

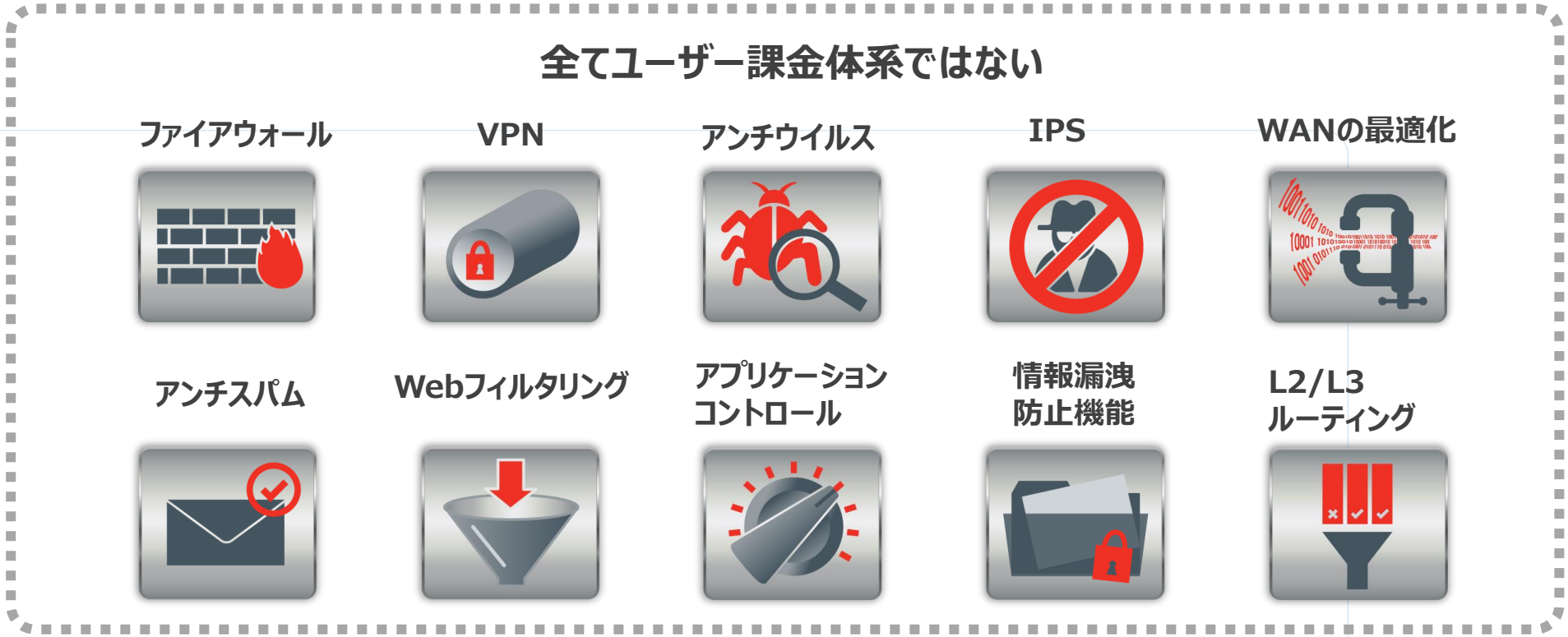
FortiASIC NPネットワークプロセッサ
ファイアウォール、VPNなどネットワークレベルの防御機能するネットワークプロセッサー

FortiASIC CPコンテンツプロセッサ
アンチウイルス、IPS、 Webフィルタリングといったコンテンツレベルでの防御機能を担うネットワークプロセッサー

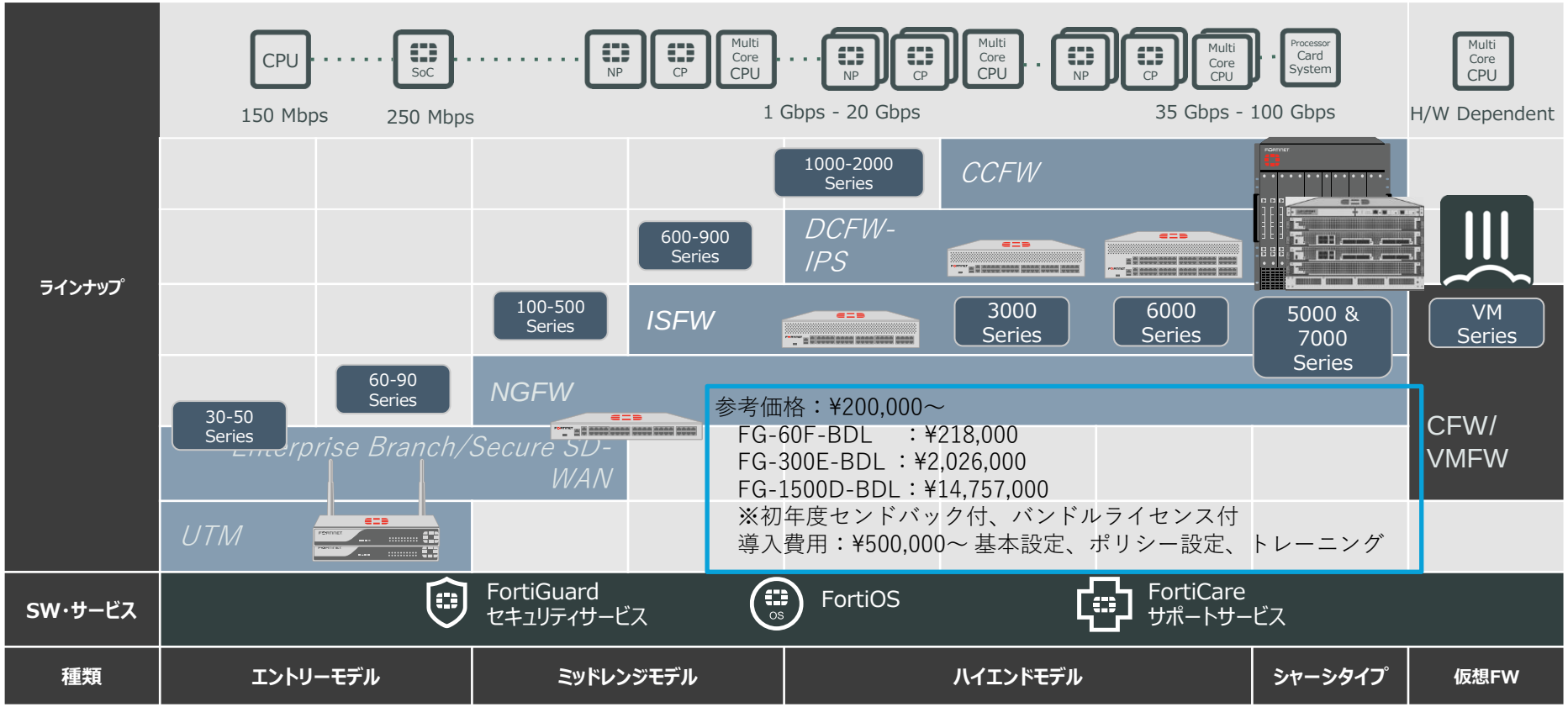
FortiGateとは？

UTMアプライアンス（次世代ファイアウォール）

複数のセキュリティ機能を統合し、コストを削減運用コンソールも１つに



UTMアプライアンス（次世代ファイアウォール）

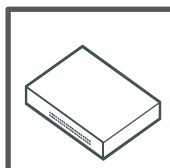


FortiGateシリーズは豊富なラインナップを提供しております！

FortiProxy Secure Web Gateway

NEW 4/1～

FortiProxy は、Web フィルタリング、DNS フィルタリング、データ漏えい防止、アンチウイルス、不正侵入防止、高度な脅威保護などの複数の検知技術採用によって、サイバー攻撃から従業員を保護する、セキュア Web プロキシです。きめ細かいアプリケーション制御の活用により、企業におけるインターネットコンプライアンスを支援します。高性能の物理アプライアンスと仮想アプライアンスをオンサイトに導入することで、あらゆる規模の企業に対応します。



アプライアンス型：3種類
400E、2000E、4000E
仮想アプライアンス：6種類
01、02、04、08、16、UL

FortiASIC CPコンテンツプロセッサ
アンチウイルス、IPS、 Webフィルタリングといったコンテンツレベルでの防御機能を担うネットワークプロセッサー

ターゲットとなるお客様の背景

海外性のProxyを利用しているお客様

- リプレースや移行に困っているお客様
- 保守のルール変更や体制変更が多く現状お困りのお客様
- イニシャル・ランニングの費用でお困りのお客様

FortiGate SD-WANをご検討のお客様

- ネットワーク刷新をご検討のお客様
- DC側のProxyの新規導入およびリプレースをご検討のお客様

FortinetによるインターネットブレイクアウトについてFortinetによるインターネット(ローカル)ブレイクアウトについて

クラウド活用から生じるWAN環境の課題

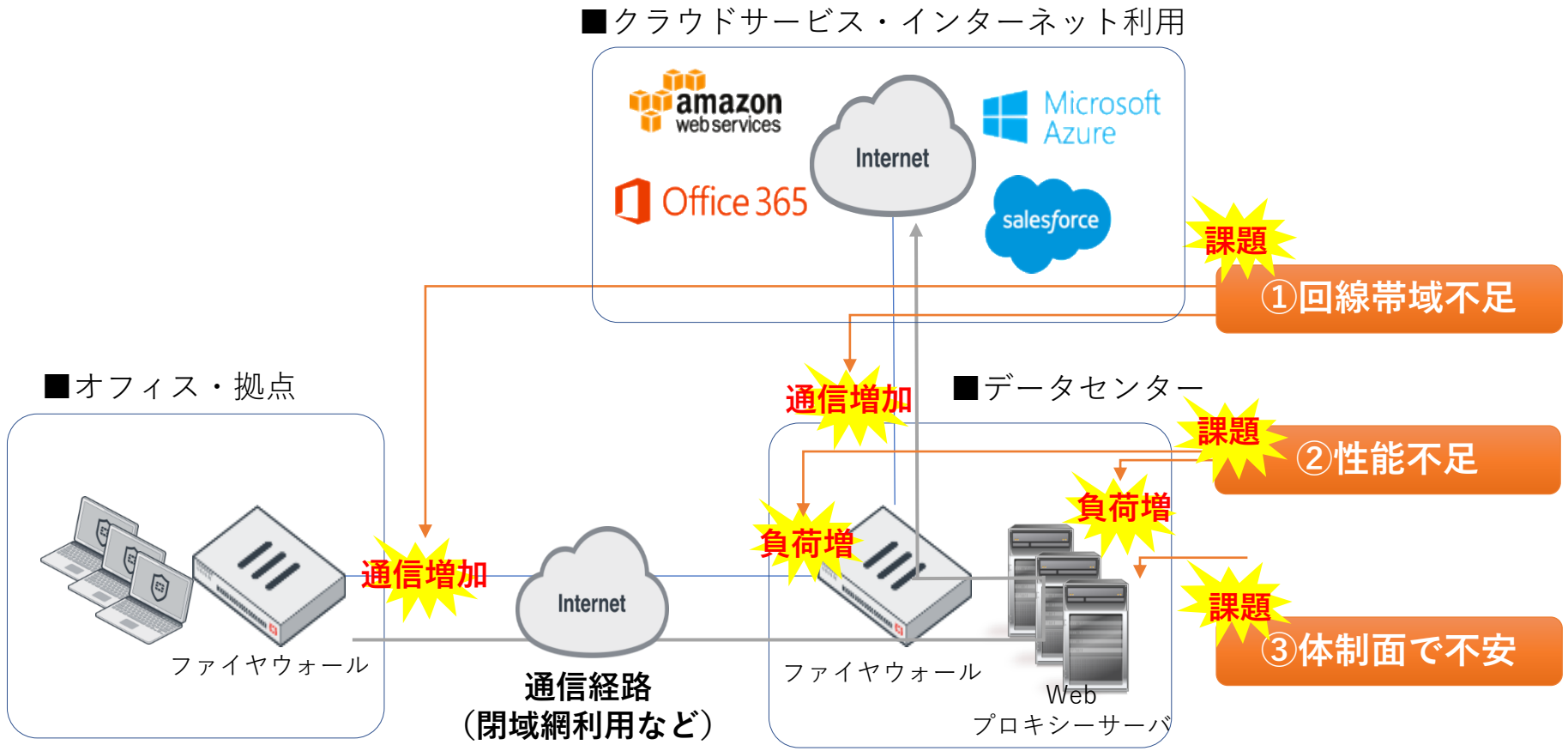
クラウドに起因する課題

- クラウド移行で処理が遅くなった
- トラフィックパターン（IP変更）
- ネットワーク機器・回線の負担増
- 不注意によるデータ流出懸念

FortiGateによる課題解決

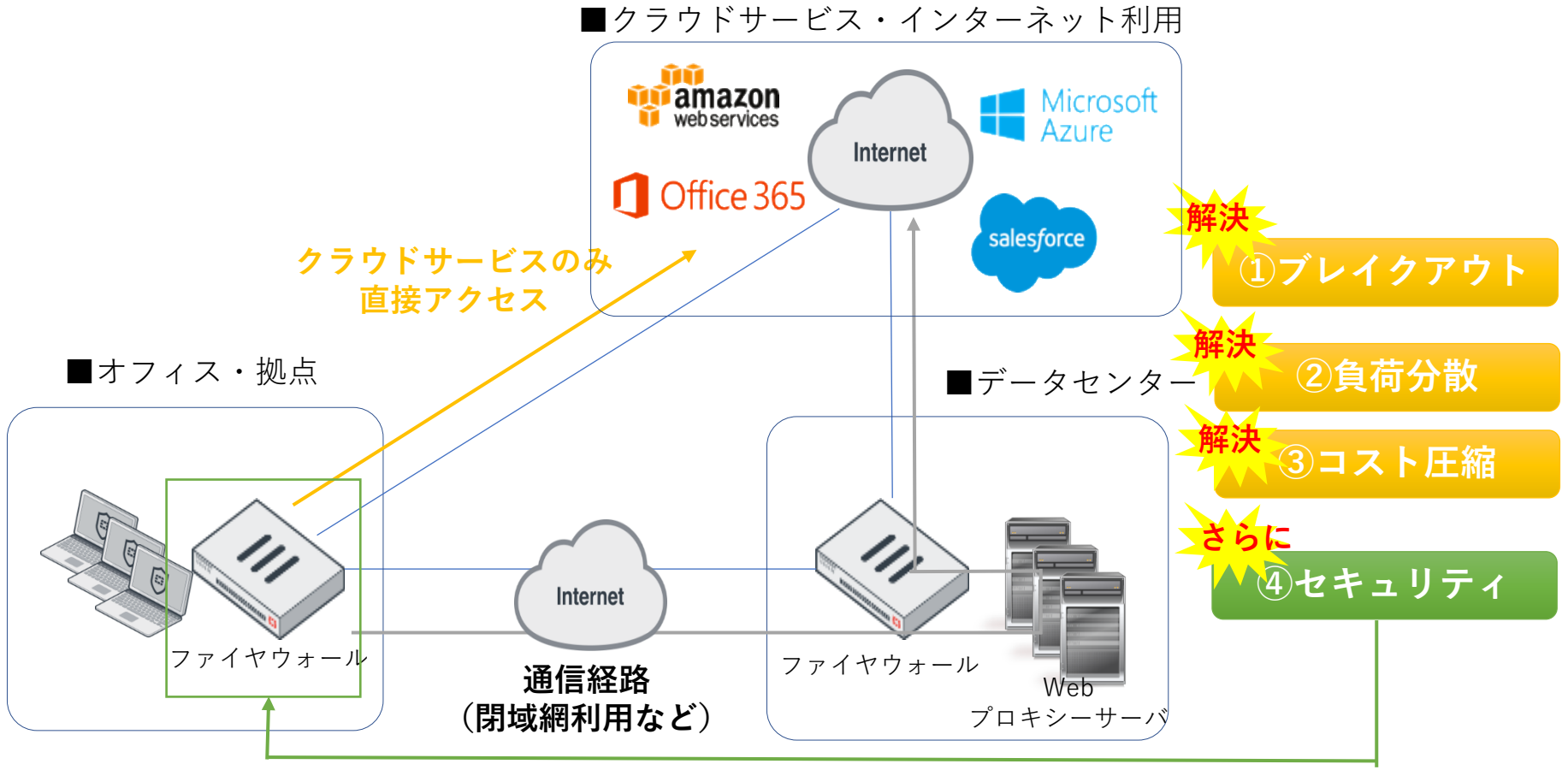
- クラウドアプリケーションの可視化
- アプリケーションに応じた回線やWANの柔軟な制御（インターネットブレイクアウト）
- Office365専用プロキシ
- テナントの制限

クラウド活用から生じるWAN環境の課題



データーセンター（通信経路を閉域網を利用）経由で通信をしている場合
レガシーファイヤウォール・クラウド利用をしており帯域をひっ迫している

クラウド活用から生じるWAN環境のFortiGate解決策



主要クラウドサービスを利用中の場合は各拠点から直接アクセスし、
ネットワークの分散を図り、安定的なネットワーク環境を実現

Fortinetによるインターネット(ローカル)ブレイクアウト

ご提案のポイント

追加ライセンス不要！

•セキュリティ対策とトラフィック制御の統合を安価に実現

- セキュリティ対策とクラウドサービスのトラフィック制御を単一プラットフォームで実現
- 専用機器導入コストと管理コストを削減

•豊富なラインナップ

- 豊富なラインナップから最適なモデルを選択が可能

•ISDB (Internet Service DataBase)でIPアドレス情報を自動更新

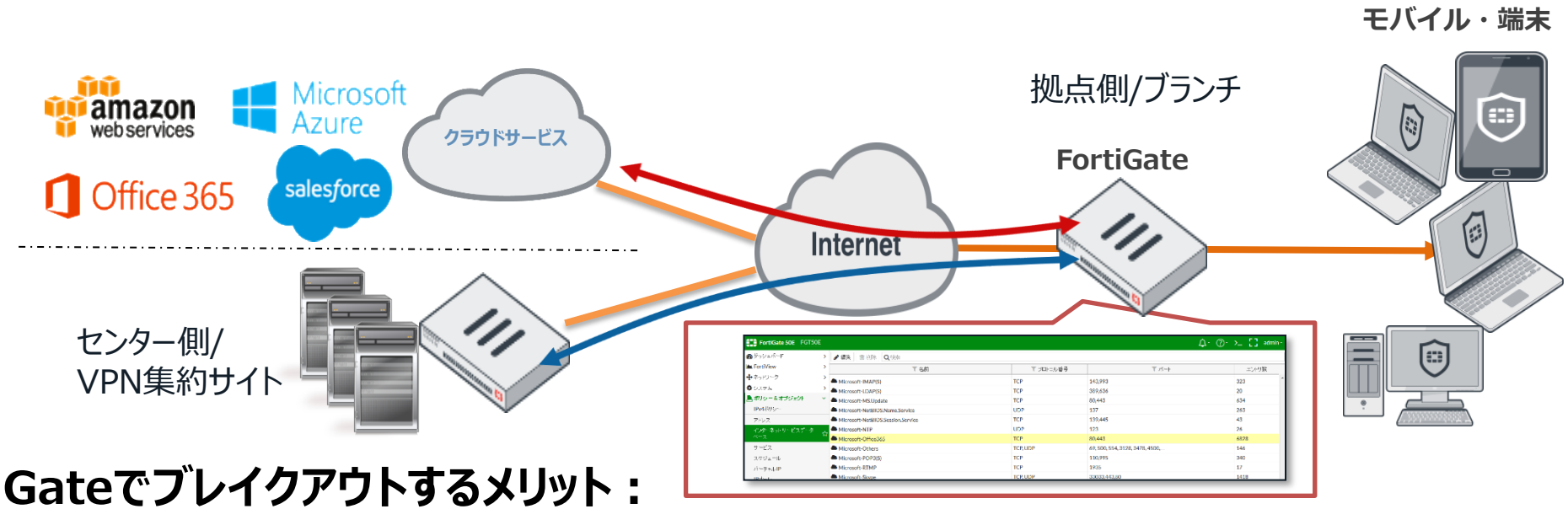
- クラウドサービスで使用されるIPアドレス情報を自動更新するので、運用コストを低減してクラウドサービスのオフロードを実現

FortiGateによるインターネットブレイクアウト

実績有

■ クラウドサービス向けのトラフィックを別回線

特定のサービスに対する通信をその他の通信とは別のゲートウェイを経由した経路で行うことができます。



■ FortiGateでブレイクアウトするメリット：

- クラウドサービス（Microsoft365等）を利用している場合、拠点毎にブレイクアウトが可能
  - Fortinet社では保守サポートに加入していれば、ライセンス無でデータベース（ISDB）を配信
  - このため、利用しているクラウドサービスのサービス/経路選択に使用可能
- クラウドサービス向けのトラフィックを直接インターネットにむかせることでオフロード可能
- 対象OS（v6.0以降）を使用していれば、利用可能（追加費用無＝保守契約があれば利用可能）

クラウドサービスのトラフィックを識別する仕組み

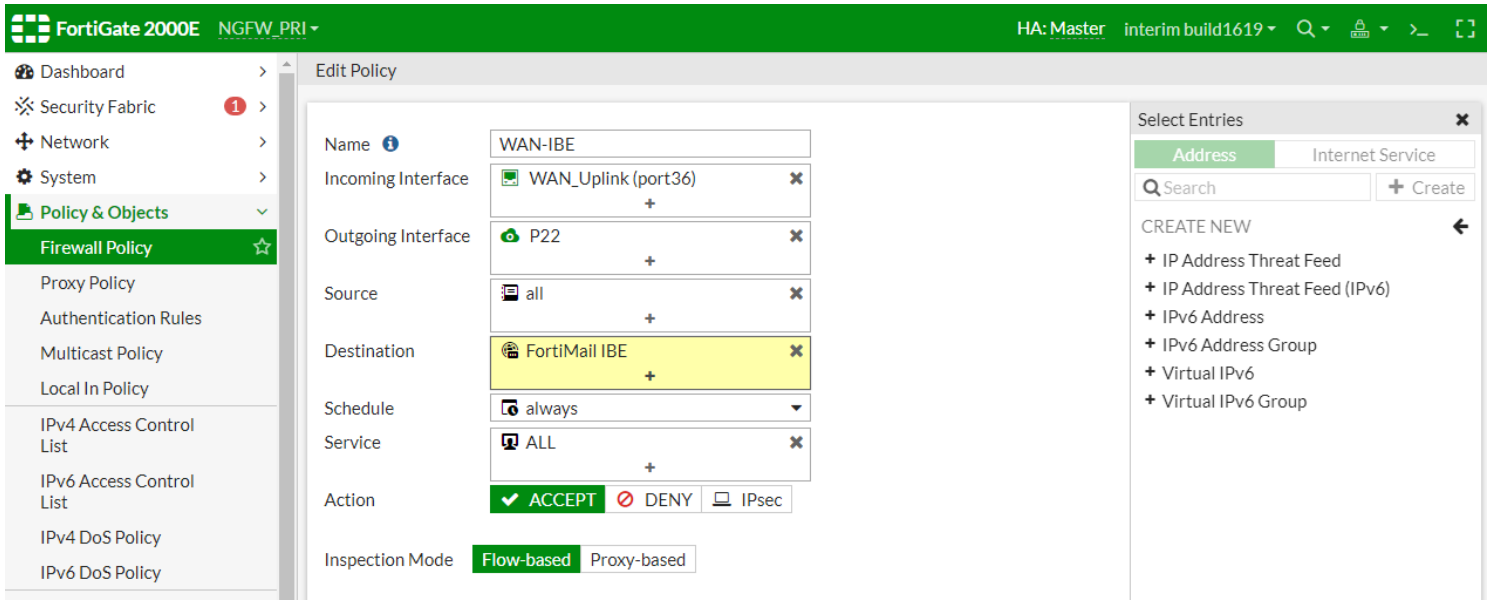
FortiGateではIPルーティングによってローカルブレイクアウトを設定します。FortiGateにはISDB(Internet Service DataBase)と呼ばれるデータベースがインストールされています。ISDBはFortinet社の管理するデータベースで、クラウドサービスで使用されるサーバのIPアドレス、ポート番号などのローカルブレイクアウトに必要な情報が記録されています。また、SD-WANは、FortiGateのASICを利用するため、高速処理可能です。

この情報は常にFortinet社がアップデートを行っており、クラウドサービス側で使用するサーバが増減した場合新たな情報がFortiGateにダウンロードされます。対応サービスは以下のURLから確認をすることができます。

情報元：https://fortiguard.com/search?q=Google&type=isdb&engine=1

ISDBで識別できないサービスはスタティックで設定可

パブリッククラウドや、ISDBに情報が存在しないサービスをブレイクアウトしたい場合、通常のIPルーティングでブレイクアウトを行う必要があります。この場合、接続先のサーバや、接続に用いるポート番号等はすべて把握しておく必要があります。また、サーバの増減が発生した場合は新たにFortiGateにローカルブレイクアウト用の設定を追加する必要があります。



実際の設定画面

FortiGate(ISDB)に登録されているクラウドサービス

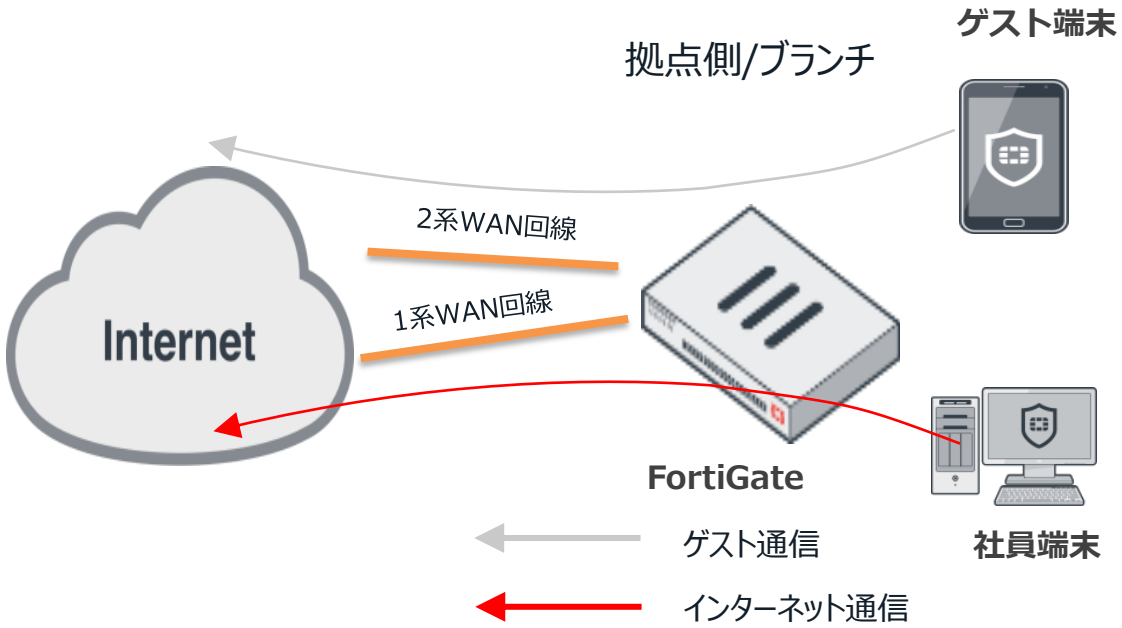
サービス名	機能名	検証結果
Gsuite	メール閲覧	○
Gsuite	メール送信	○
Gsuite	添付ファイル閲覧	○
Gsuite	添付ファイル送信	○
Gsuite	ビデオ会議	○
O365	メール閲覧	○
O365	メール送信	○
O365	添付ファイル閲覧	○
O365	添付ファイル送信	○
Zoom	ビデオ会議	○
Amazon AWS	クラウドプラットフォーム	○
Microsoft-Azure	クラウドプラットフォーム	○

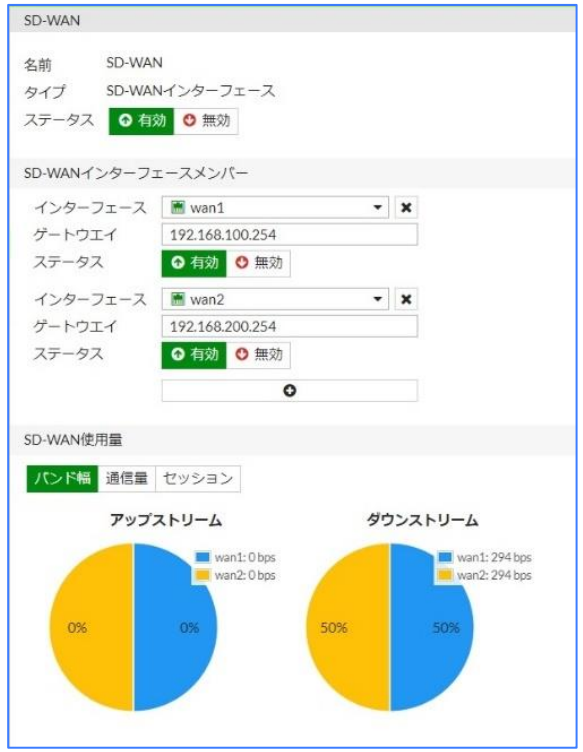
インターネットブレイクアウトの導入実績

業種	規模	導入機種	利用サービス	構成
公共	中 （100-500）	FG-500E	o365	FortiGate-500EをFirewall兼SSL-VPNサーバとして導入。ユーザ認証にお客様環境に設置されていた既存LDAPを使用し、ユーザごとにアクセス可能な社内サーバを制御する設計とした。
放送	小 （-100）	FG-60E	o365 AWS	拠点社員の本社サーバへのアクセスのため拠点間のIPSecVPN環境の構築。
放送	中 （100-500）	FG-100F	o365 Azure	FG-100Fx4台をFirewall・VPNとして構成し、導入。o365通信量が多くなっていることから、同製品でブレイクアウト実施。また、FortiSwichも同時採用
警備	大 （-10000）	FG-500E FG-100F FG-60E	o365	SaaSサービスを利用していることもあり、DC側のネットワーク環境がひっ迫している状況。このため、各拠点からブレイクアウトを行い、ネットワークの軽減を図るため採用
製造	中 (100-500)	FG-60E FMG	o365	約40の拠点に向けてFirewallを導入。 FortiManagerによるコンフィグの一元管理と導入後の設定変更、監視業務の教育を実施。

ブレイクアウト時のルーティングの設定例

要件：ゲスト端末と社内端末のWAN回線を分けたい
メリット：ユーザー毎（ゲスト・社員端末）のルーティング設定可



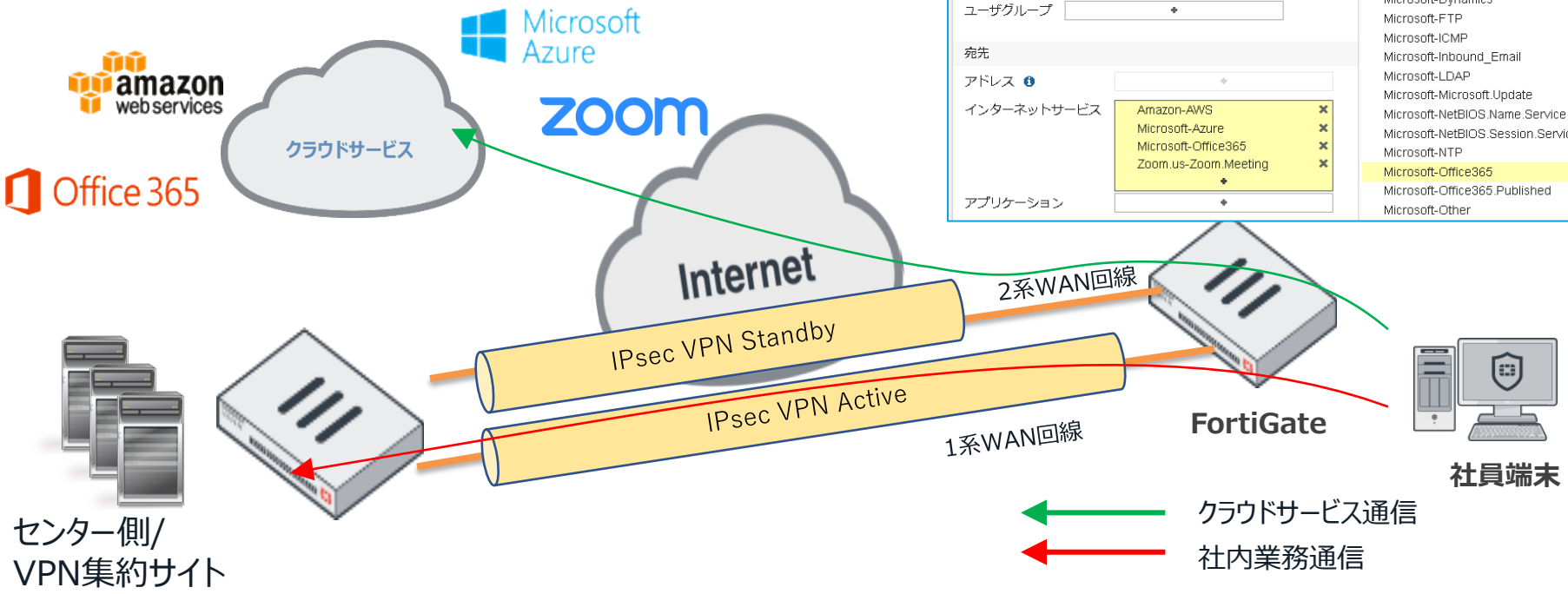


SD-WANインタフェースの管理画面（端末毎のルーティング設定例）

社員とゲストで使用するWAN回線を分けることで、社員通信の品質を保ちます。
また、回線障害時の自動切り替わり、復旧時の自動切り戻しも実現可能です。

インターネットブレイクアウトとIP-Sec VPNの併用

要件：用途毎（Saas・Cloud）にWAN回線を分けたい
メリット：Firewall・VPNとSD-WANの併用が可



クラウドサービス通信をローカルブレイクアウトすることにより、社内の業務通信の品質を保ちます。また、同一の物理インターフェースを使用したSD-WANとIPsecVPNの設定の共有も可能です。

ターゲットとなるお客様の背景

■クラウドサービスを導入している、また最近導入を増やしている

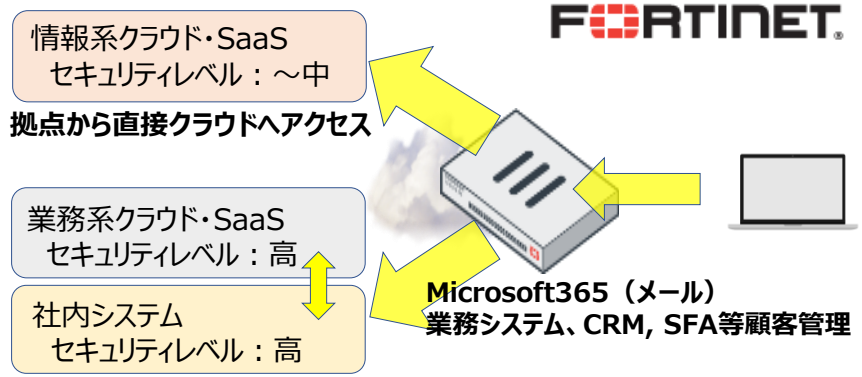
・情報基盤系：m365,GCP, box, Slack等
・開発基盤系：AWS
・コミュニケーション系：Web会議、電話帳等

■リモートアクセスの見直し

・VPNゲートウェイのパフォーマンス増強、ブレイクアウトとの併用

弊社のご支援体制図

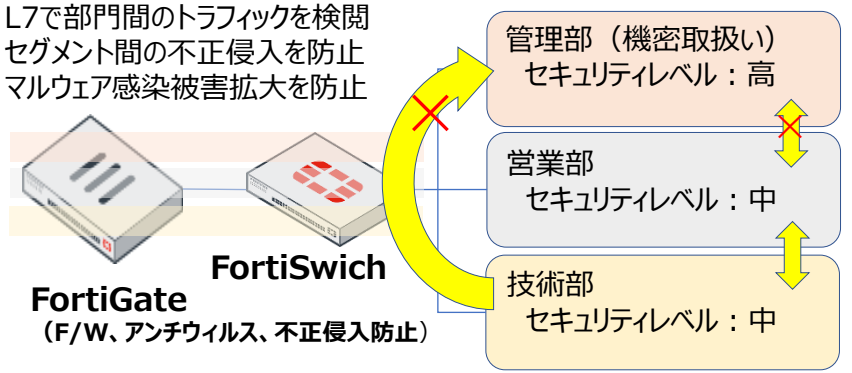
「セキュアSD-WAN」によるトラフィックの最適化



クラウドへのアクセスをエッジでオフロード

「セキュアSD-LAN」セキュリティリスク軽減

・L7で部門間のトラフィックを検閲
・セグメント間の不正侵入を防止
・マルウェア感染被害拡大を防止



セグメント間のトラフィック検疫

本日ご提案させていただく取組みにおけるCTCSPのご支援内容をご紹介させていただきます。

赤枠は自営でご対応

	プリセールス	機材貸し出し	技術支援	保守	特価対応
Fortinet FortiGate FortiSwitch FortiAP	◎ 営業・推進・技術同行	◎ CTCSP保有機材 FortiGate主要モデル	◎ CTCSP社員で対応 （PL・設計・設置）	◎ CTCT自営保守 24時間オンサイト含む	○ 案件登録で対応可

営業部
案件ご対応全体窓口
役割：営業同行、ご提案、お見積り、納期管理

ソリューション推進第２部
マーケティング全般、対ベンダー窓口
役割：顧客訪問、ベンダー交渉

ソリューション技術部
技術サービス対応
役割：顧客訪問、有償技術支援

CTCSPの優位性

No	項目概要	項目詳細	補足
1	販売実績	年間100社以上の取引実績	販売パートナーを経由して年間100社以上の販売実績を有しております。公共機関、学校、情報通信、民間機関など幅広く採用頂いております。
2	パートナー分類	ディストリビューター	-
3	取扱開始時期	2006年	当社はFortinetが設立して間もない時期より取引を開始しており多くの実績を保有しています。
4	保守体制	自営保守可能	CTCテクノロジーで自営保守を提供可能。 FortiGate、FortiAnalyzer、FortiManager、FortiMail、FortiSandbox、FortiProxyなど自営保守提供が可能。
5	認定技術者	認定資格者10名以上	-
6	研修/教育	あり	Fortinetの提供する有償サービスで提供可能。
7	検証機	あり	当社で保有している検証機があります。

弊社のご支援体制図