



# 自治体ニーズに柔軟に対応するための機能を 備えた次世代の広域ネットワークソリューション Cisco SD-WANのご紹介

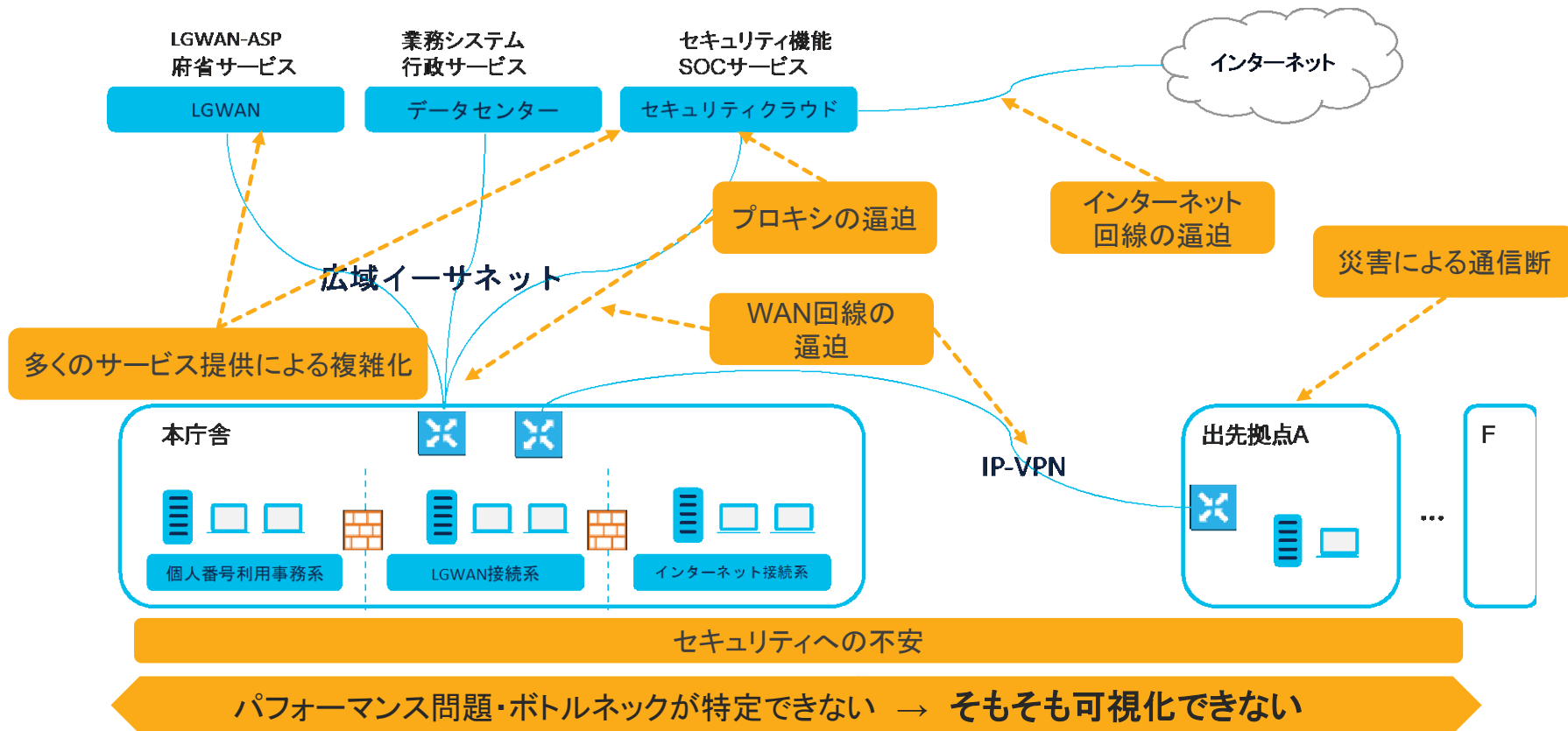
シスコシステムズ合同会社

東日本公共システムズエンジニアリング

菅野 翔太

2022年10月

# 新型コロナウイルスで顕在化する／した、自治体WANの課題



# こんなお悩みを抱えられていませんか？

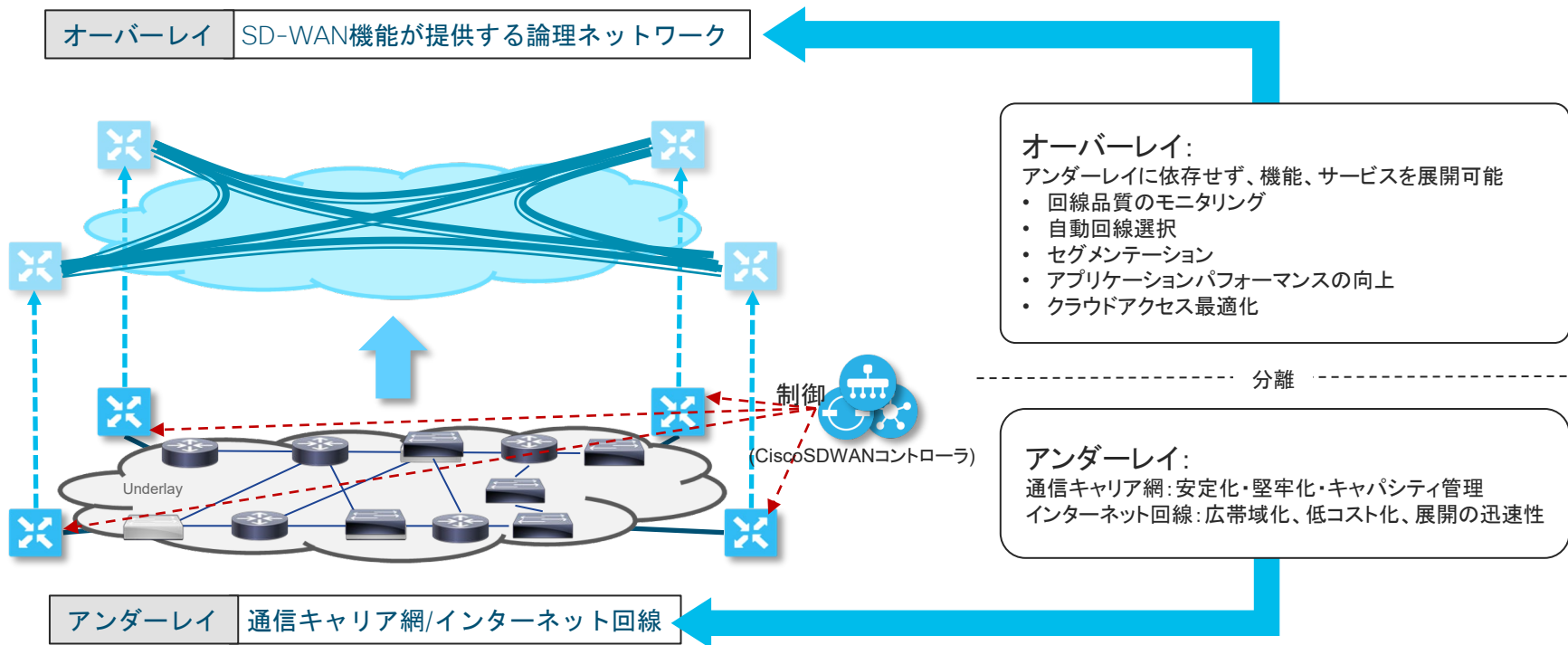
- 有線で2回線引き込み冗長化していたのに災害で両方使えなかった
- 回線費用が高額で削減したい
- ローカルブレイクアウトをしたいけどセキュリティ対策が高額で踏み込めない
- SD-WANを構築したいけどクラウドコントローラーは使いたくない

こんな悩みを持っていたら是非Cisco SD-WANのご検討を！！

# Cisco SD-WANのご紹介

# SD-WAN – SDN技術を活用したWANの仮想化

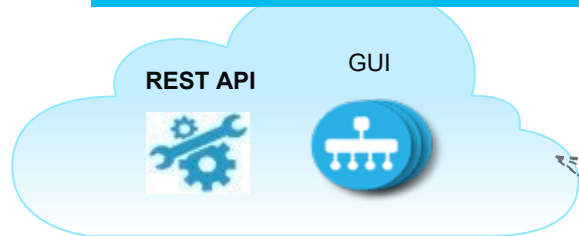
論理的なネットワーク機能(オーバーレイ)を物理接続構成(アンダーレイ)上に形成



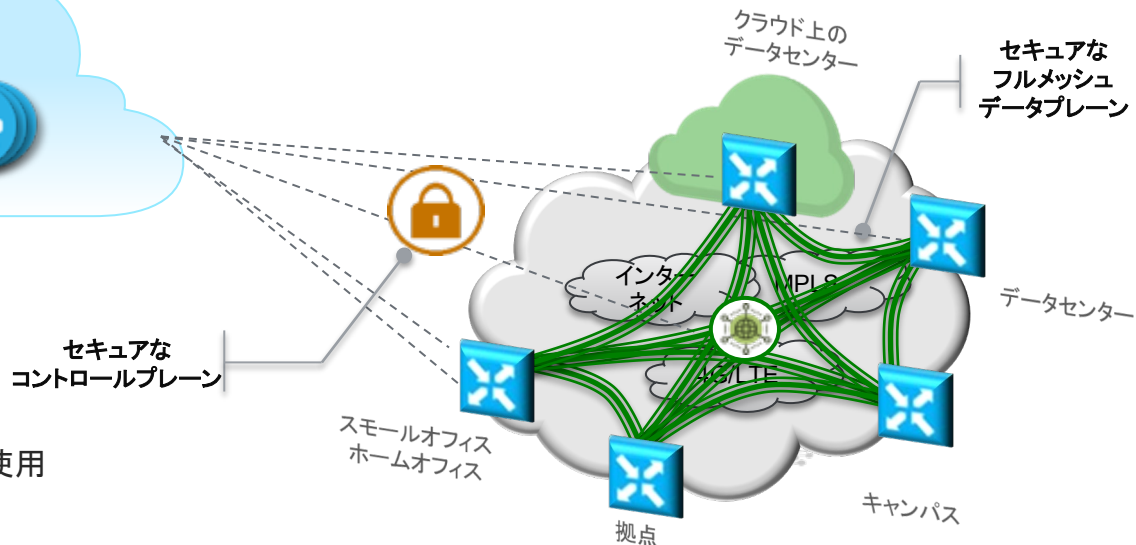
Eメールが「メール」になったように、これからはSD-WANが「WAN」になる

# Cisco SD-WAN ソリューションの構成要素

## SD-WANコントローラ (クラウドホスト or オンプレミス)



## SD-WANファブリック (物理ルータ、仮想ルータ)



- SD-WANコントローラ
  - GUIによる一元管理
- SD-WANファブリック
  - 拠点間のデータ通信に使用
  - 回線種別に非依存
- セキュアなコントロールプレーン、データプレーン

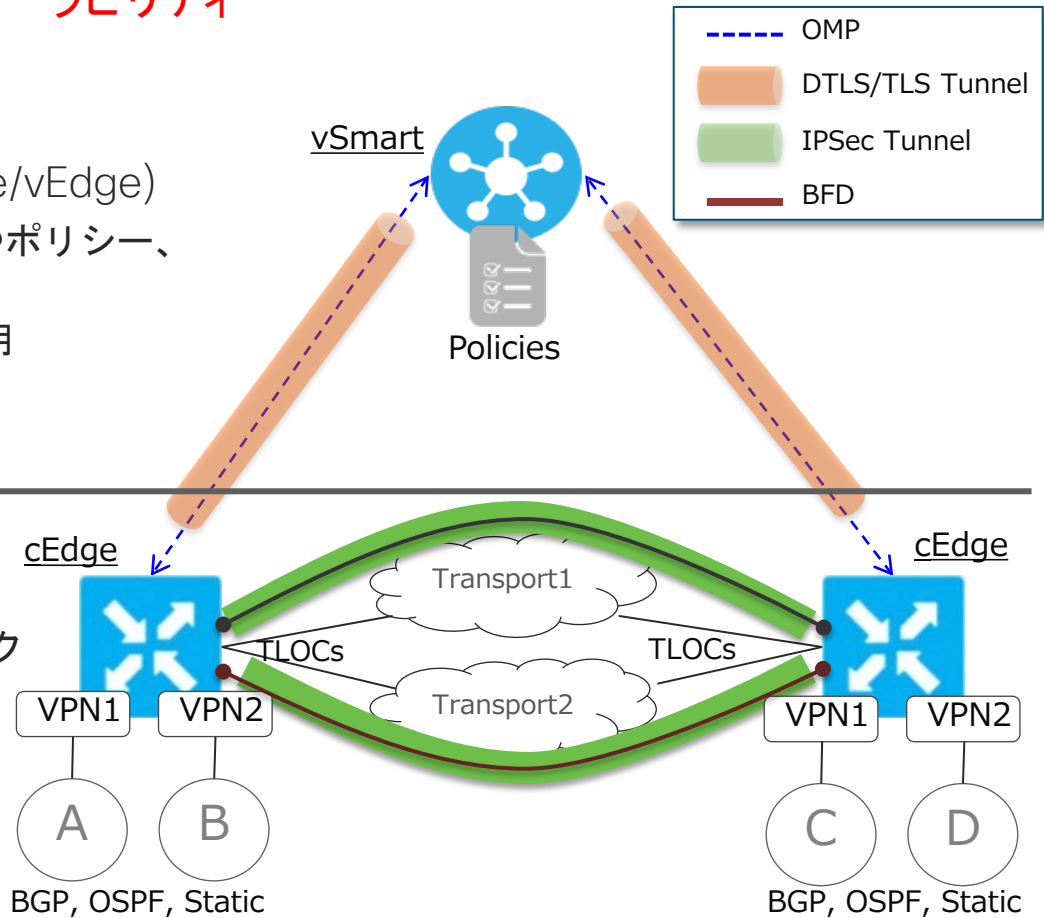


# Cisco SD-WAN アーキテクチャ概要

シンプルなアーキテクチャで高いスケーラビリティ

- コントロールプレーン(vSmart<->cEdge/vEdge)
  - データプレーン構築のための情報(TLOC)やポリシー、ルーティング情報を配信
  - Overlay Management Protocol(OMP)を使用
  - メッセージはDTLS/TLSによって暗号化
  - ユーザデータは流れない

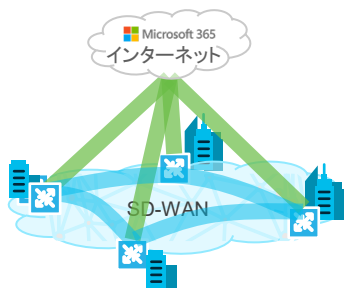
- データプレーン(cEdge/vEdge間)
  - IPSecトンネルによるSD-WANファブリック
  - BFDにより回線の状態や品質を監視
  - ユーザデータが流れる



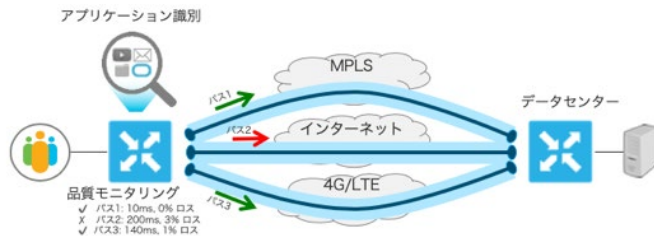
# WAN仮想化のベネフィット

## 6つのユースケース(お勧め活用方法)

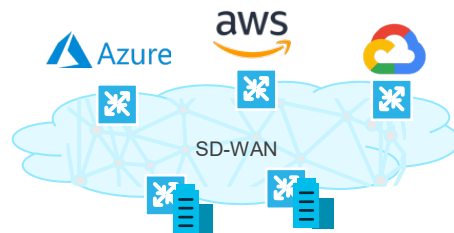
### ローカルブレイクアウト



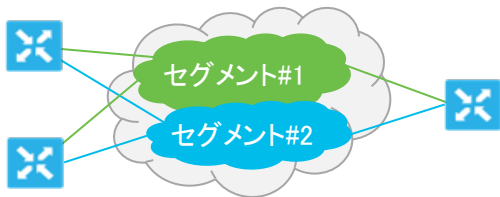
### WAN利用の最適化



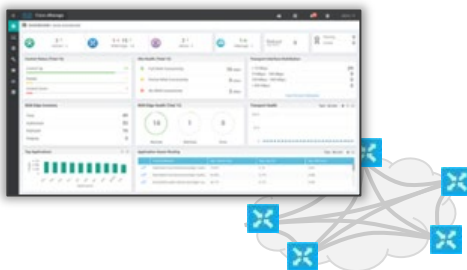
### パブリッククラウド拡張



### セグメンテーション



### 一元管理、可視化、分析



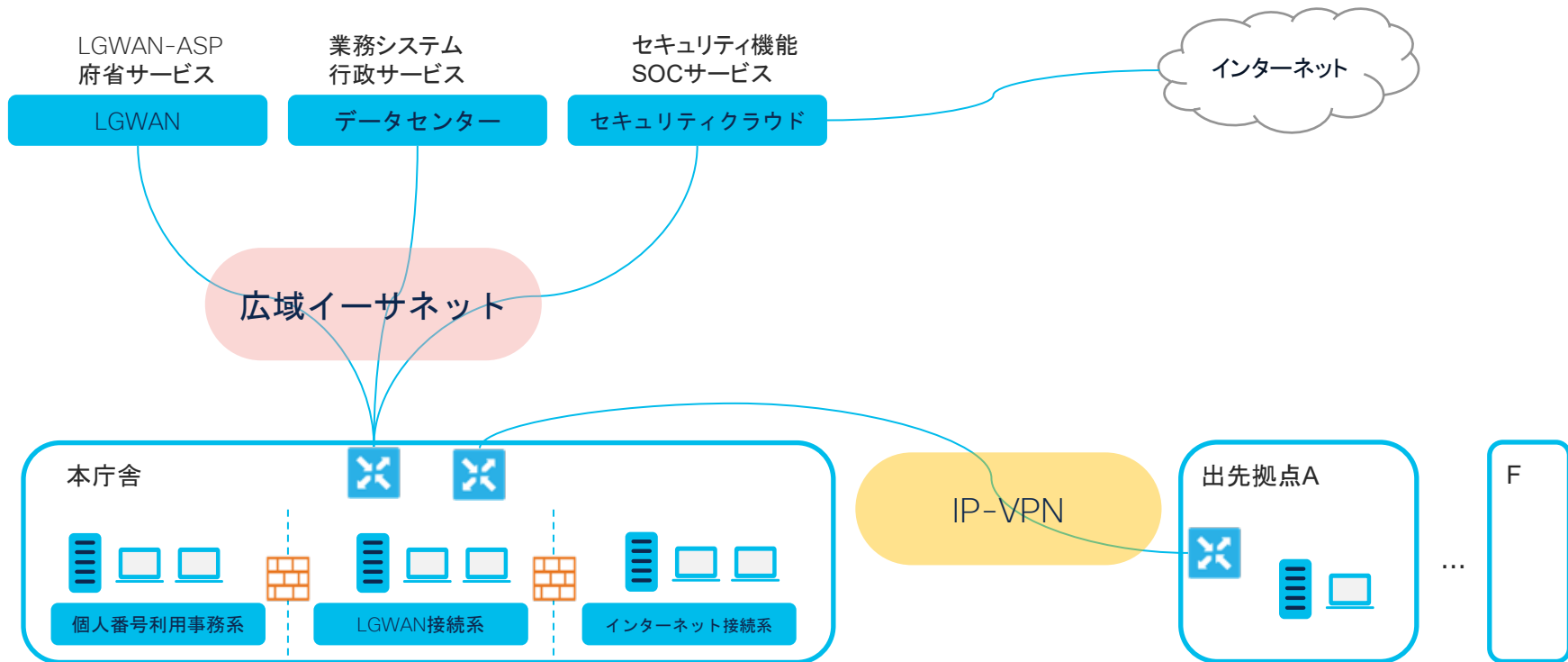
### ゼロタッチプロビジョニング



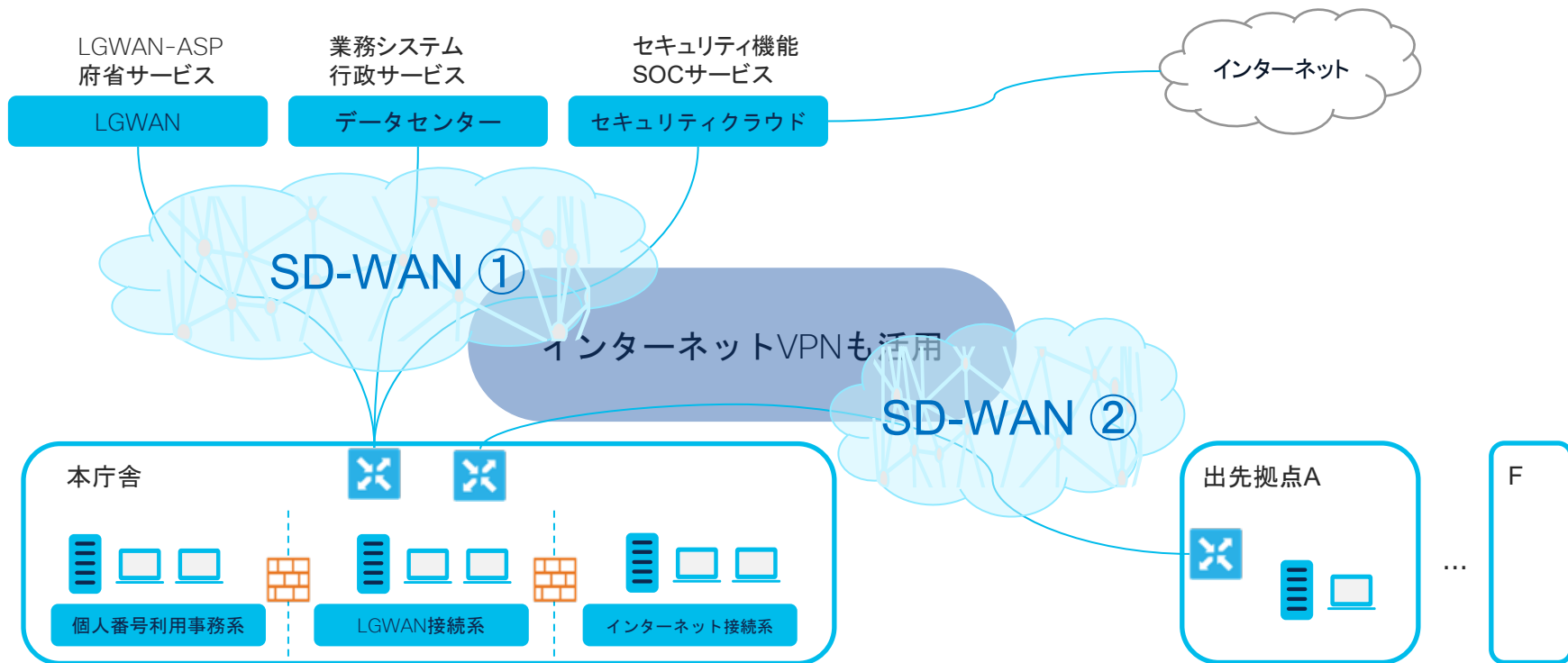


# 自治体ネットワークに適用する Cisco SD-WAN

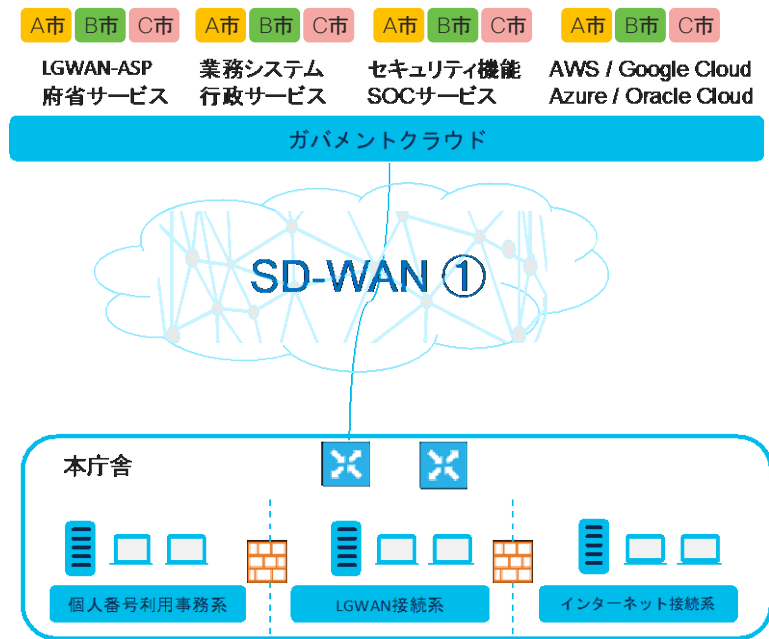
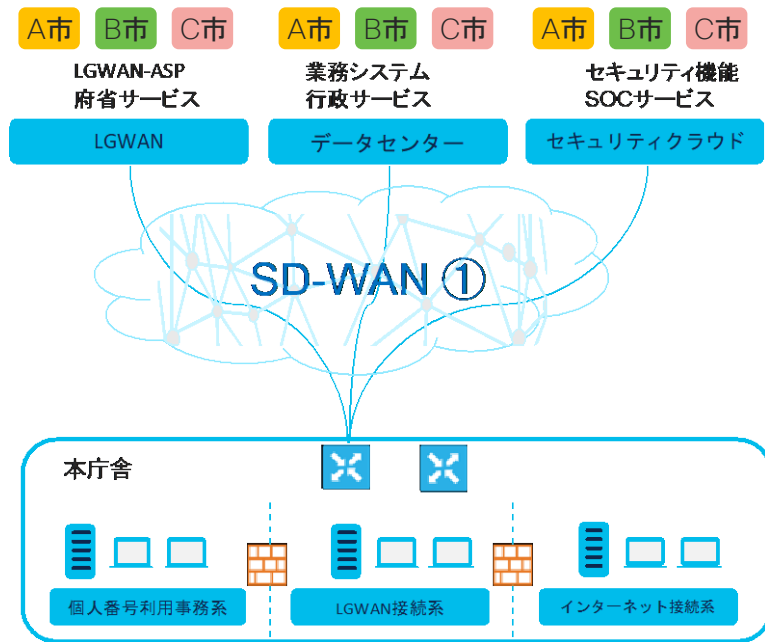
# 自治体ネットワークへのSD-WANの適用



# 自治体ネットワークへのSD-WANの適用



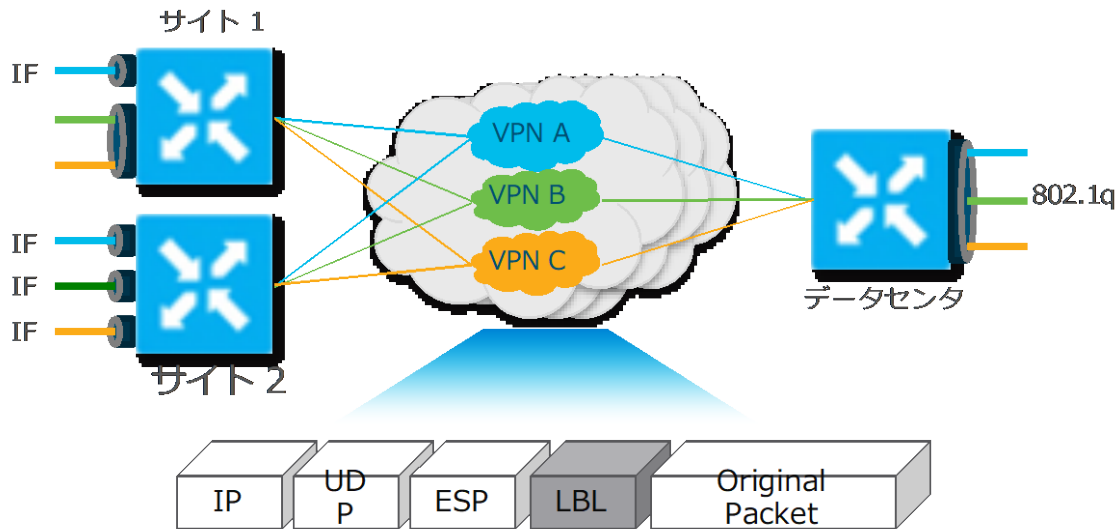
# SD-WANの適用 ① 本庁舎から外部へのアクセス



例えば・・・今でも複雑なネットワークから・・・  
ガバメントクラウドやLGWANに多くのサービスが乗ったらそれを制御できますか？

# セグメンテーション

- WAN回線に依存せず、エンドツーエンドのセグメンテーションを実現

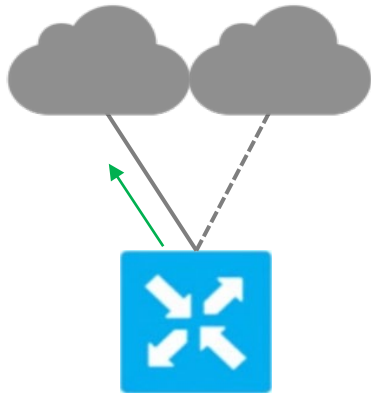


- SD-WANルータはVPN毎にルーティングテーブルを保持
- インターフェイス、サブインターフェイス(802.1Q)をVPNにマップ

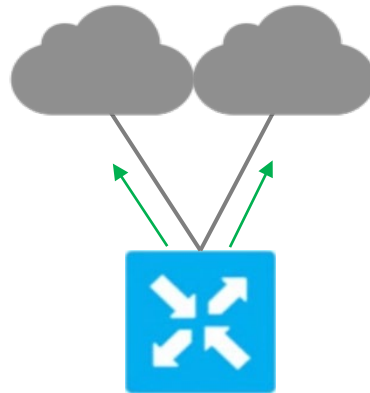
# WAN フォワーディング

- 通信によって自動的に最適なWAN選択を実現

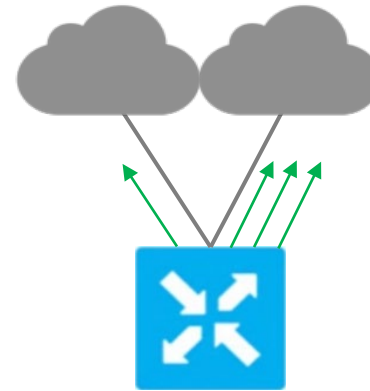
トラフィックエンジニアリング  
アクティブ/スタンバイ



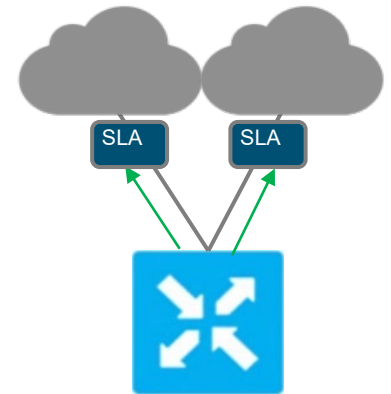
等コストバランシング  
アクティブ/アクティブ



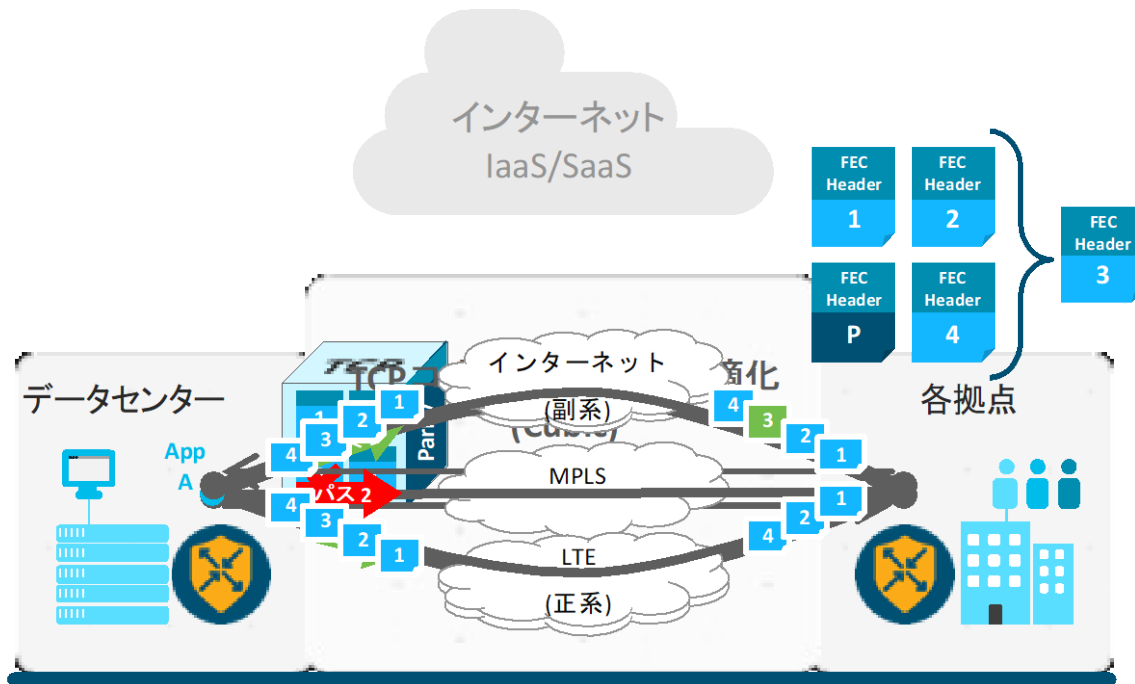
重み付け  
アクティブ/アクティブ



Application Aware Routing  
SLAベース



# 提供サービスのパフォーマンスを向上する Application Aware Routing



SLAベースのパス選択

アプリケーションごとのポリシー  
アプリAを通すパスは  
遅延150ms以下、かつロス2%以下であること

パス1: 10ms, 0% ロス  
パス2: 200ms, 3% ロス  
パス3: 140ms, 1% ロス

# 戦略的クラウドパートナーシップを通じて ベストのアプリケーション体験を提供



Office 365最適化  
テレメトリデータを活かした  
最適パス選択

vWANとのネイティブ統合

設定/ポリシー変更を  
自動化、一元運用



仮想インスタンスで  
AWSワークロードまで  
容易にネットワーク拡張

AWS TGWネットワークに  
SD-WANエンドポイントを  
ネイティブ統合



Cisco SD-WANを  
コロケーション  
サイトまで拡張

パブリッククラウドへの  
セキュア、低遅延な  
ダイレクトコネクト

End-Endの一貫した運用性



Google Cloud

アプリケーション中心の  
マルチクラウド  
ファブリック

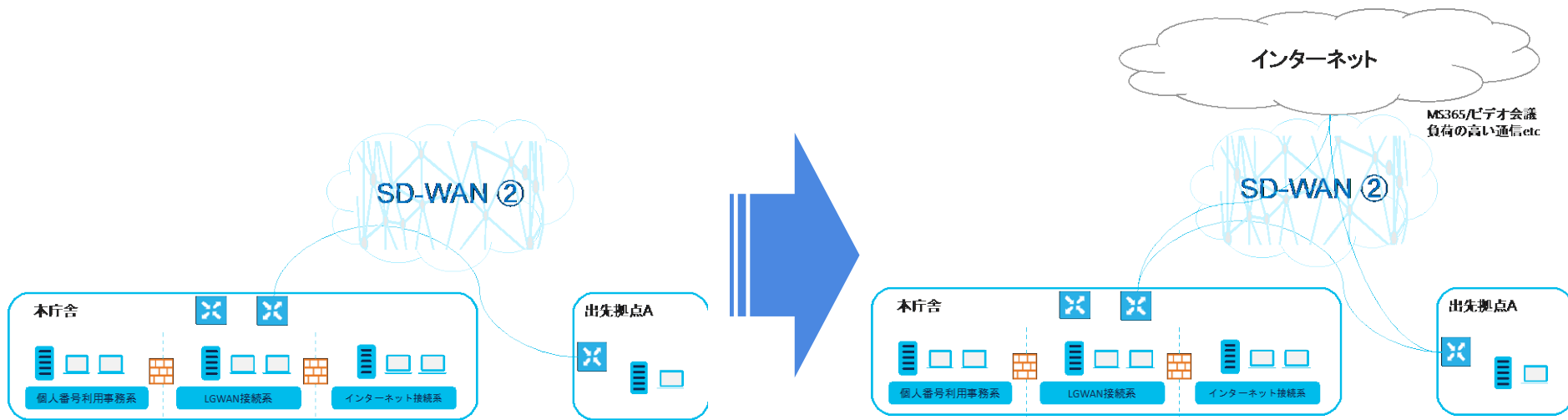
アプリメタデータに基づく  
SD-WANポリシー自動化

Google Cloudの  
高速バックボーンを活用

企業のクラウド戦略を支援・加速



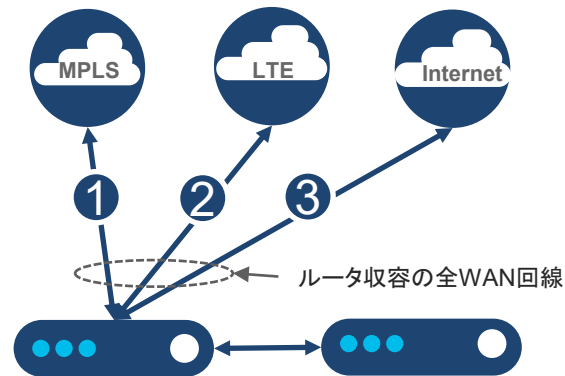
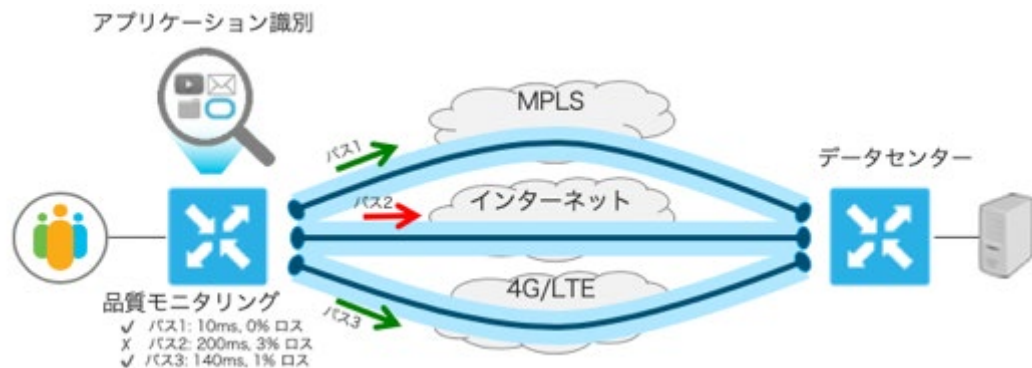
## SD-WANの適用 ② 本庁舎と出先拠点のアクセス



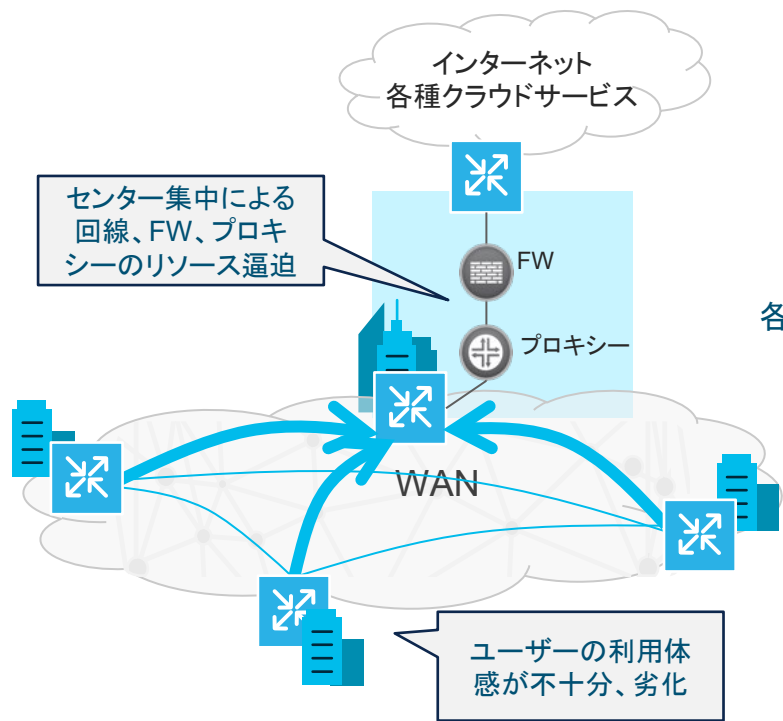
本庁舎と出先拠点の接続は冗長化されていますか？  
負荷の高い通信はローカルブレイクアウトしませんか？

# 大規模災害への対策

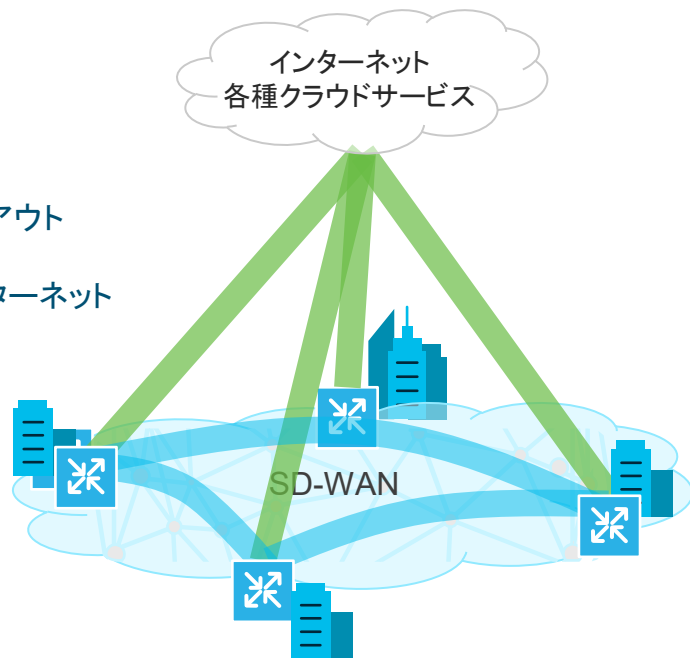
## バックアップ回線にLTE回線を採用することによる業務継続



# セキュアなローカルブレイクアウト データセンターリソースの負荷軽減、ユーザーの利用体感の向上

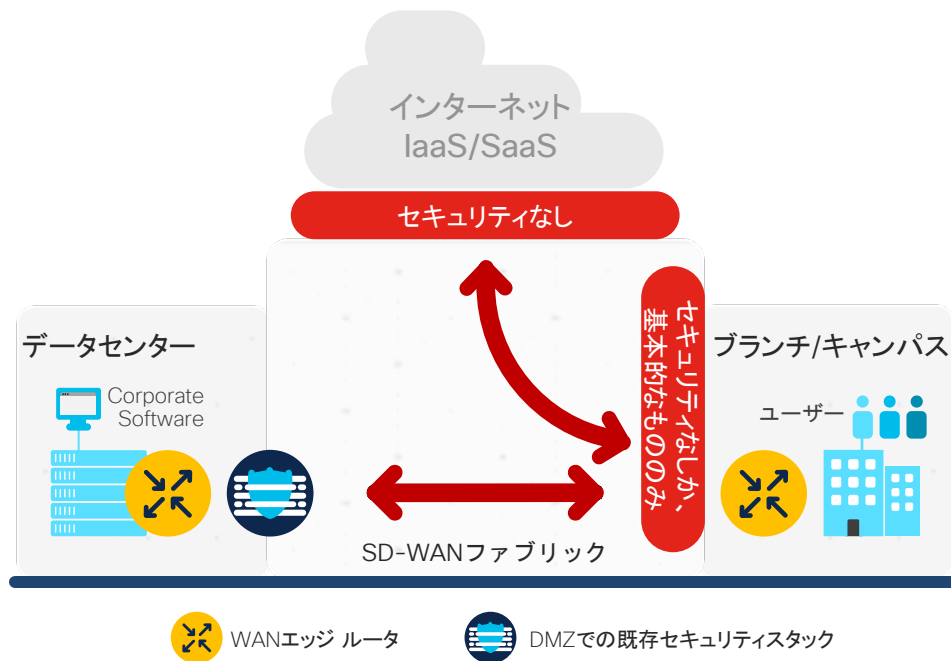


ローカルブレイクアウト  
により  
各拠点から直接インターネット  
へ



DCリソースの負荷軽減およびユーザ体感の向上

# ローカルブレイクアウト導入時のセキュリティ課題



## 内外のセキュリティ脅威

### 外部脅威

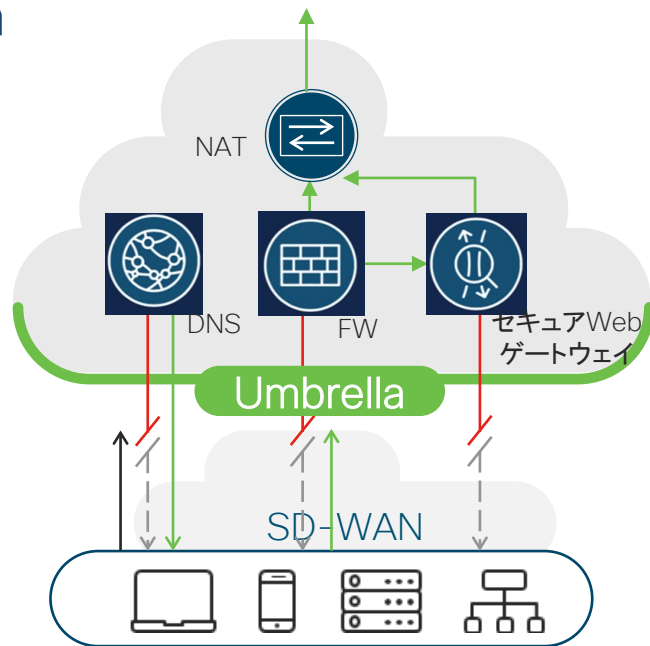
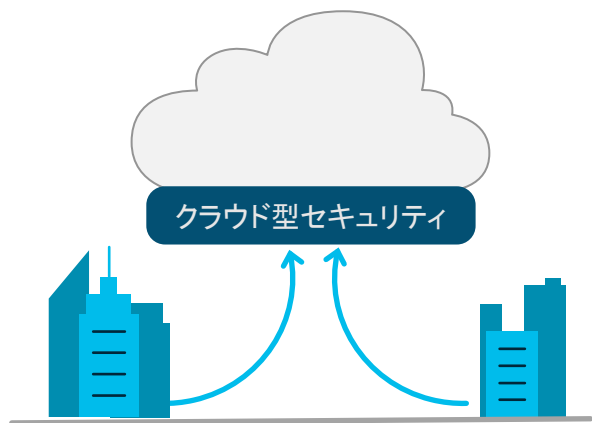
- インターネットやクラウドへの直アクセスにより、マルウェアやフィッシングの脅威
- データ漏えいの懸念
- ゲストアクセスへの対応

### 内部脅威

- 不許可・不正なアクセス
- コンプライアンス対応 (PCI, HIPPA等)
- ラテラルムーブメント、侵入拡大

# セキュリティ展開のユースケース

## クラウド型セキュリティ / Cisco Umbrella



**DNSレイヤ セキュリティ**  
DNSレイヤでマルウェアに起因する  
通信障害を未然にブロック

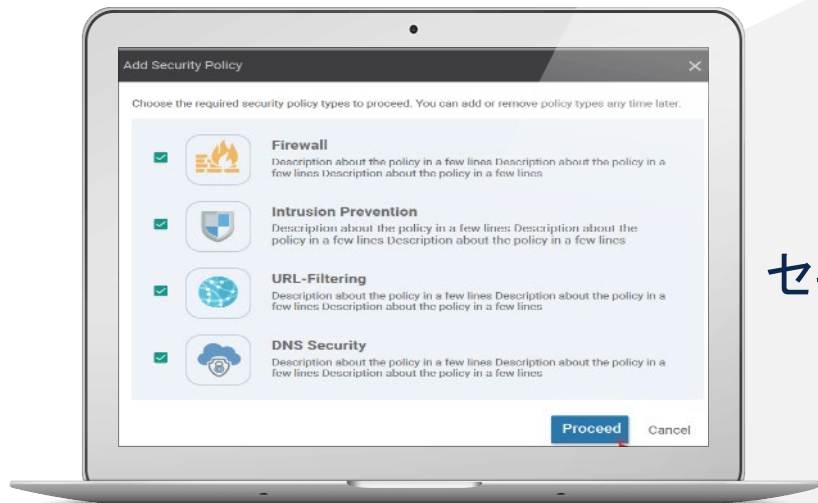


**ファイアウォール**  
IP, Port, プロトコル  
ルールによる  
ファイアウォール



**セキュア Web ゲートウェイ**  
マルウェアおよびポリシー  
違反に関するWebトラフィックの  
最終チェックを実行

# セキュリティと SD-WAN の最適な組み合わせ



Cisco SD-WAN

シスコ  
セキュリティ

エンタープライズ ファイアウォール  
1400 を超えるレイヤ 7 アプリケーションを分類

侵入防御システム  
世界最大の導入実績を持つIPS エンジン

URL フィルタリング  
82 を超える Web カテゴリフィルタと  
Webレピュテーションフィルタでのブロック

高度なマルウェア防御  
Cisco Umbrellaを使用した  
クラウドセキュアプロキシ&クラウドFW

セキュア インターネット ゲートウェイ  
Cisco Umbrellaを使用した  
DNSセキュリティクラウド FW

SSL プロキシ  
暗号化されたトラフィックの脅威を検出



『週単位・月単位』での導入・展開をわずか『時間単位』で実現

# ローカルブレイクアウトとその発展型

## シスコなら、MS365ブレイクアウトの典型的な悩みを解決！

MS365 ブレイクアウトの悩み..

- ✓ ファーストパケットから識別したい
- ✓ MS365アドレスがしょっちゅう変わる

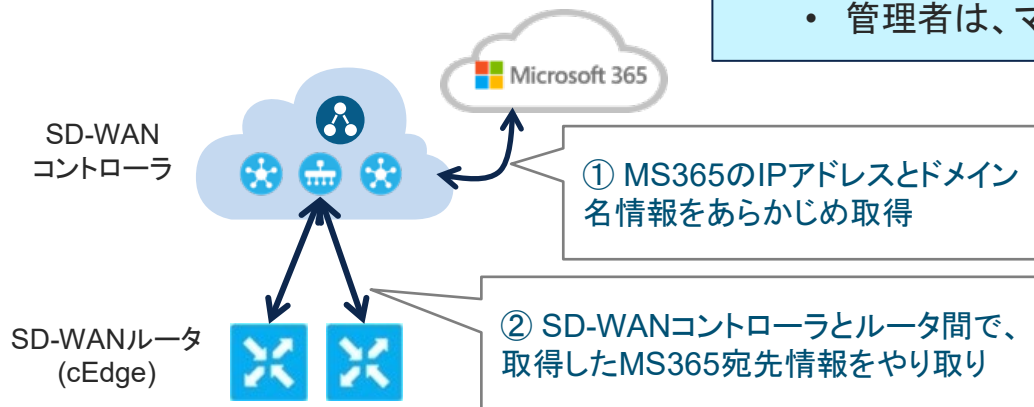
SD-AVCクラウドコネクタ for MS365で、

### 1. ファーストパケット問題を解消

- 1パケット目からMS365を識別し、ブレイクアウトできる
- センター拠点のFWに、新たな設定変更が不要です

### 2. MS365の宛先アドレス変化に自動追従

- 管理者は、マニュアルでのアドレス変化追従が不要に

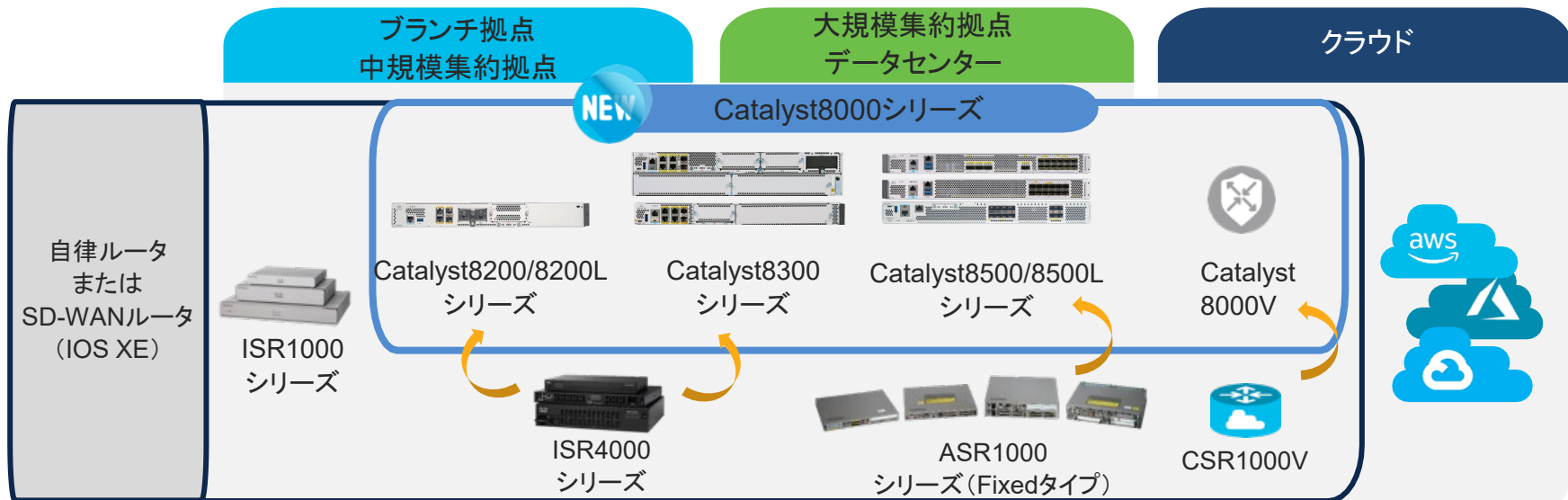


Controller Ver20.3以降でcEdgeでのみ対応

# Cisco最新ルータ・ラインナップ



# 新ルータCatalyst8000シリーズが加わった Cisco 最新ルータ・ラインナップ※



自律ルータ専用 (IOS)




Cisco 9211

SD-WANルータ専用 (IOS-XE)



ISR1100-4G  
ISR1100-6G

NFV  
プラットフォーム



Catalyst 8200 uCPE  
ENCS5000

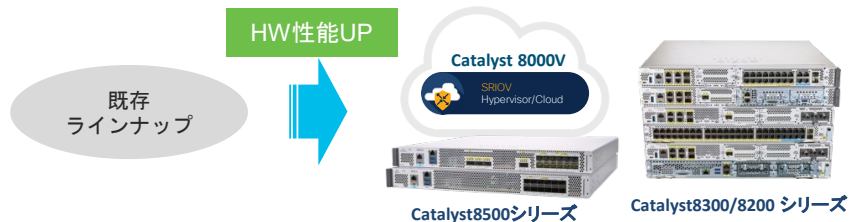
※サービス事業者様向け大型機を除く

# Ciscoルータ 4つの特徴

Cisco Catalyst8000

## 継続的な技術革新による高性能化と高機能化

Catalyst8000シリーズ投入によりHWコスト据え置きで性能最大7倍へ大幅強化。またクラウド対応・セキュリティ対応をさらに充実。



Cisco DNA Center

## ネットワーク全体の一元管理と『健康診断』

ネットワーク機器、クライアント端末、アプリケーションを『健全性』で点数化してパフォーマンスを一目で把握！

ID	IPv4アドレス	デバイスタイプ	ヘルス
Grace.Smith	10.30.100.27	Apple-iPad	7
Grace.Smith	10.30.100.45	iPhone 7	8
Dir.Dogood	10.30.100.47	iPhone 7	8
john.jacobson	10.13.4.108	Linux-Workstation	8
vema.diskley	10.11.100.50	Samsung-Device	9
Grace.Smith	10.30.100.20	Linux-Workstation	8

機器、クライアント、アプリケーションの  
一覧で点数化



フロアマップ上で点数化



トポロジマップ上で点数化

IOS-XEと2つのコントローラ対応

## IOS同一イメージで自律ルータとSD-WANに対応

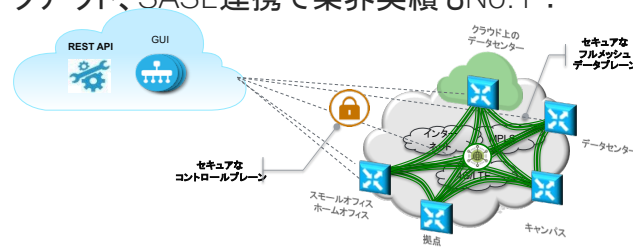
IOSの入れ替えなく2つのルータ・モードに対応し、移行も簡単。また自律ルータ時はDNA Center、SD-WANルータ時はvManageによる集中管理を実現。



Cisco SD-WAN

## WAN仮想化でアプリ高速化とコスト削減を実現

シスコ独自のルーティング技術でWANの『完全仮想化』を実現。高帯域化・コスト削減、アプリ毎のWAN最適化、精度の高いローカルブレイクアウト、SASE連携で業界実績もNo.1！



# まとめ

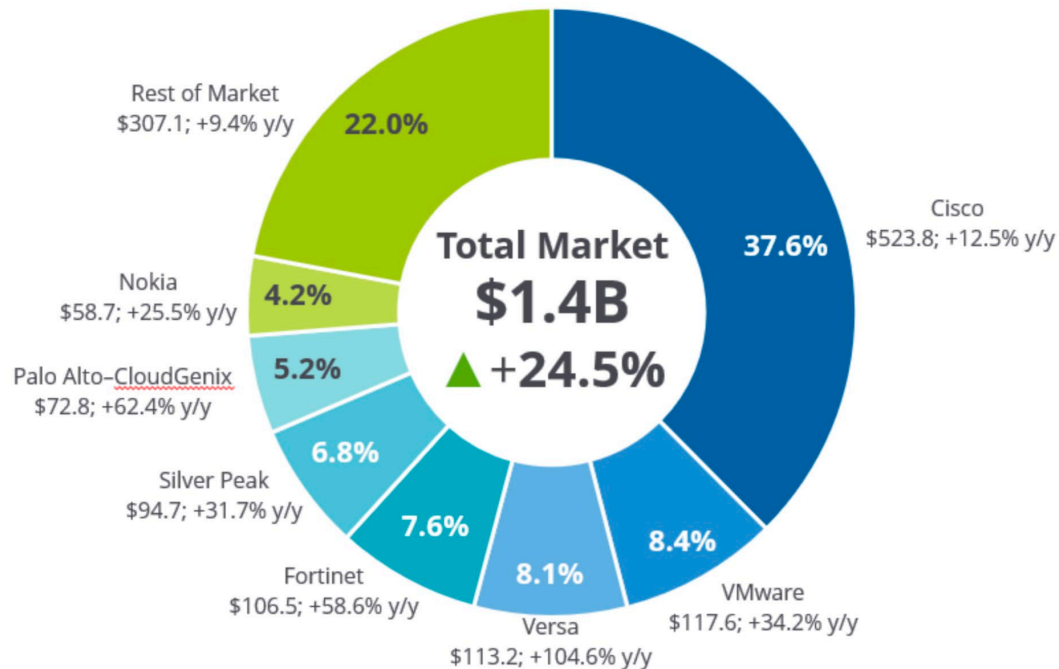
# Cisco SD-WANの特徴と優位性

	Cisco SD-WAN	競合他社
アーキテクチャ	○ MPLS VPNにIP Secや管理機能を集約した独自プロトコル（OMP）の採用で、ルーティングの機能性、トポロジの柔軟性、拡張性に優れた唯一無二のアーキテクチャを保有。	× レガシーIPSecベースのアーキテクチャに留まり、拡張性と柔軟性が不足している。
アプリケーション単位のローカルブレイクアウト	○ NW情報やFQDN情報を使用して、アプリケーション単位でファーストパケットからの精度の高いローカルブレイクアウトが可能。	× DPI方式やデータベース方式を採用するも精度が悪くファーストパケット対応が困難。
ルーティング制御	○ OSPF, BGP, EIGRP, IPv4/IPv6, IP multicast, Staticに対応。	× Static/BGP推奨が主流。IPv6非対応。
セグメンテーション	○ 最大300の論理NW（VRF）を1つのSDWAN上で構成可。	△ 16VRF対応が1社のみ。他はVRF不可。
SASE対応	○ Cisco Umbrella連携で自社ソリューションにてSASE対応を実現。3rd Party連携も実績多数。	× SASE対応を自社のみで実現不可。
SD-WANとnon SD-WANの両立	○ 同一のHW・IOSイメージでSD-WAN、nonSD-WAN(自立ルーティング)の双方に対応可能。既存NWを踏襲しながらSD-WANへ移行できる。	× SDWAN専用のHW/SWIにより、既存NWと分離したNWを構成する必要あり。

# SD-WAN 2020年上期 世界市場シェアでシスコは1位



Worldwide SD-WAN Infrastructure 1H20 Share Snapshot



Note: 1H20 Share (%), Revenue (\$M), and Growth (%)

Source: IDC, 2020

# 幅広い業種のお客様でCisco SD-WANをご採用頂いています

## 金融



## 医療／製薬／ヘルスケア



## 小売・流通・サービス



## 製造・ハイテク・エンジニアリング



## サービスプロバイダー



# まとめ

- Cisco SD-WANはコントロールプレーンとデータプレーンが分離されたセキュアなSD-WAN
- 回線のアクティブ-スタンバイ構成から無駄のないアクティブ-アクティブ構成へ
- LTE回線を含めたSD-WAN構成は大規模災害への対策に有効
- 自治体の複雑なネットワークはセグメンテーションや自動化が重要
- 通信量やセッション数の多いアプリケーションはローカルブレイクアウトすることが必要
- ローカルブレイクアウトする時にはクラウドセキュリティの導入が必要

**全てに対応しているCisco SD-WANをぜひご検討下さい！！**

# パートナーコミュニティサイトのご紹介

HOME / ... / Japan Partner Community / Japan Partner Community : パブリックセクター（公共系） /

Page Access Level: Partner, Distributor, Employee | [Add to My Briefcase](#) | [Share](#) | [Subscribe](#)

## Japan Partner Community : パブリックセクター（公共系）

[Partner HUB](#) [Contact Information](#)



パブリックセクター（公共系）関連のページへようこそ。  
トレーニング資料および録画を、是非ご活用ください。

ロードマップ等、各コンテンツ内でご案内した内容が、  
予告なく変更となっている場合もございます。  
あらかじめご了承ください。

また、トレーニングのビデオは当日の録画のため、冒頭が切れている、  
終了後しばらく何もない録画がある、等ございますが、ご了承ください。  
見積もりの組み方がわからない、見積もり構成（BOM）を組んで欲しい、などでお困りですか？  
そんな時は、販売時の支援を行なっているパートナーヘルプをご活用ください

Japan Partner Communityサイトの

[トップページへ戻る](#)



<https://salesconnect.cisco.com/c/r/salesconnect/index.html#/program/PAGE-18586>



