使ってみなければわからない！～クラウド時代の”XX“シリーズ
第2回：クラウド時代のネットワークとは？

O365活用におけるネットワークのTo-Beモデル

シスコシステムズ合同会社

本日の内容

- Office 365導入時の考慮事項
- Office 365導入を成功を支援するCiscoソリューション

Office 365の特徴と導入の背景

効率的なコスト

- Office 365とはMicrosoft社のクラウド型サービス
- 資料作成・共有、メール、ビデオチャット、ストレージ等、ビジネスに必要な機能がクラウド経由で提供されている

利用者の生産性

Windows OSのUpdate ないしは Office365への移行が必要

- Office2016サポート終了:2020年10月
- Windows7:2020年に延長サポート切れ
- Windows8.1:2018年にメインサポート切れ

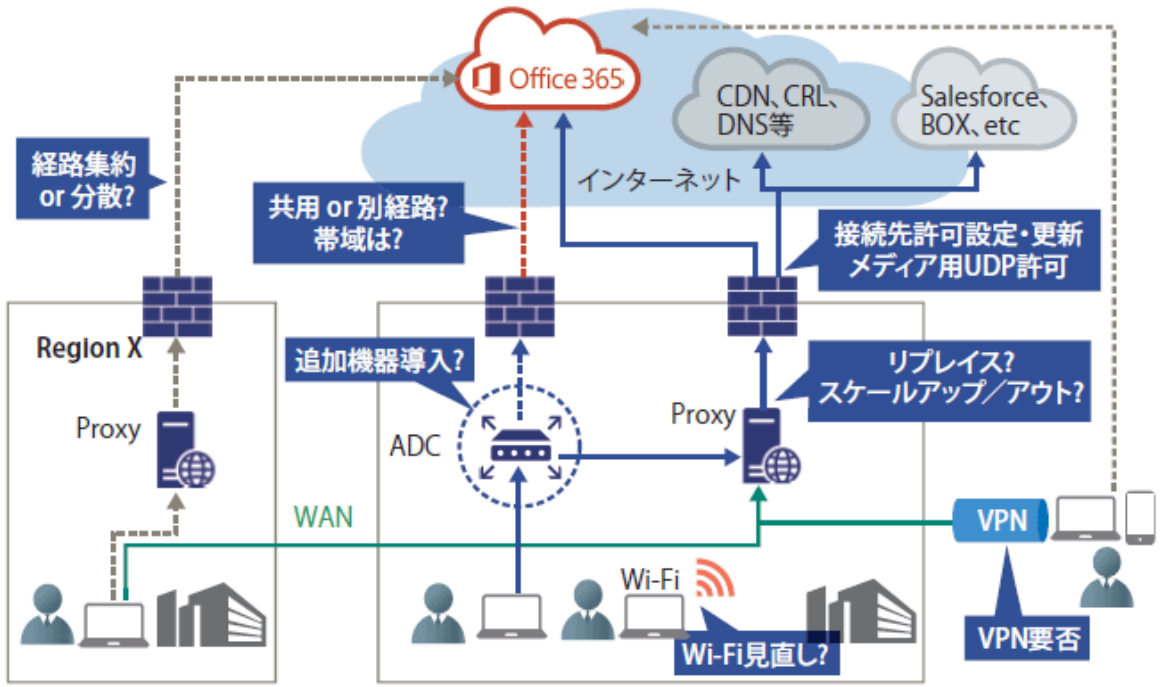
Office 365の導入を成功に導くためのポイント

出展：businessnetwork.jp
Office 365の導入を成功に導くためのネットワークを見直すべき10のポイント
提供◎日本マイクロソフト株式会社 2017.10.30

図表1　クラウドサービスを利用する時に気をつけるべき10のポイント

1	ネットワーク帯域	6	既存ITシステムに影響を与えない設計・構築
2	接続先IPアドレス/FQDNの対応	7	特定クラウドサービスだけルートを分ける
3	プロキシサーバー/FW増強	8	ワイヤレスネットワークへの対応
4	リアルタイムコミュニケーションサービスのUDP通信	9	ネットワークトポロジー
5	セッション数	10	クラウド時代のソフトウェアのアップデート方法

図表2　クラウド利用におけるネットワークの考慮点



Office 365の導入を成功に導くためのポイント

10のポイント	要点	考えられる対応策
ネットワーク帯域	一日中の大量のインターネットアクセス	回線の増強
接続先IPアドレス・FQDNの対応	Office 365等のSaaSでは、接続先のIPアドレス/FQDNが不定期に更新される	O365の識別と別経路化
プロキシサーバー/FW増強	既存のプロキシ/FW設備がOffice 365の膨大なトラフィックを処理しきれない	O365の識別と別経路化
リアルタイムコミュニケーションサービスのUDP通信	快適な通話を行うためUDPが使われる	UDP通信の許可
セッション数	Office 365は1クライアントで多くのセッションを同時に使用・プロキシサーバーのポートが枯渇するなどの問題が起こる	プロキシ増強 プロキシをバイパス
既存ITシステムに影響を与えない設計・構築	既存サービスのパフォーマンスまで劣化するケース	O365の識別と別経路化 直接のインターネットアクセス
特定クラウドサービスだけルートを分ける	すべてのクラウドの通信を「1つの出入口」に集約することから起こる障害	O365の識別と別経路化 直接のインターネットアクセス
ワイヤレスネットワークへの対応	大半の企業はデータ通信のみを前提に社内Wi-Fiを設計・構築している	無線LANの音声・ビデオ対応
ネットワーク・トポロジー	一極集中型のWAN構成が多い	直接のインターネットアクセス
クラウド時代のソフトウェアのアップデート方法	頻繁に配信されるセキュリティ修正やアップデートファイル	各拠点からの効率的なアップデート

本日の内容

- Office 365導入時の考慮事項
- Office 365導入とCiscoソリューション

Office 365の導入を成功に導くCiscoソリューション

データ保護

アクセス保護

クラウドアクセス
インフラ

Step3
松

- クラウドアプリケーション可視化とデータ保護
- メール保護（対ランサムウェア、スパム等）

Step2
竹

- クラウド直アクセスのセキュリティ

Step1
梅

- O365の識別と別経路化
- 直接のインターネットアクセス
- 各拠点からの効率的なアップデート

Office 365の導入を成功に導くCiscoソリューション

解決する課題	考えられる対応策	Ciscoソリューション
• 一日中大量のインターネットアクセス • プロキシの枯渇 • 頻繁なセキュリティ修正・アップデート	• O365の識別と別経路化 • プロキシのバイパス • 各拠点から効率的なアップデート	Cisco SD-WAN
• インターネット直接アクセス時のセキュリティ懸念	• SD-WAN組込みのセキュリティ機能 • クラウド型のセキュリティ	Cisco SD-WAN セキュリティ Cisco Umbrella
データ保護、脅威対策 • Office 365のメールセキュリティ機能は基本的なもの • クラウド アプリケーションの可視化とデータ保護	• メールセキュリティによる脅威保護（ランサムウェア、フィッシング等への防御） • クラウドアプリ利用の制御と可視化	Cisco Cloud Email Security with AMP Cisco Cloudlock

Office 365の導入を成功に導くCiscoソリューション

データ保護

Step3
松

- クラウドアプリケーション可視化とデータ保護
- メール保護（対ランサムウェア、スパム等）

アクセス保護

Step2
竹

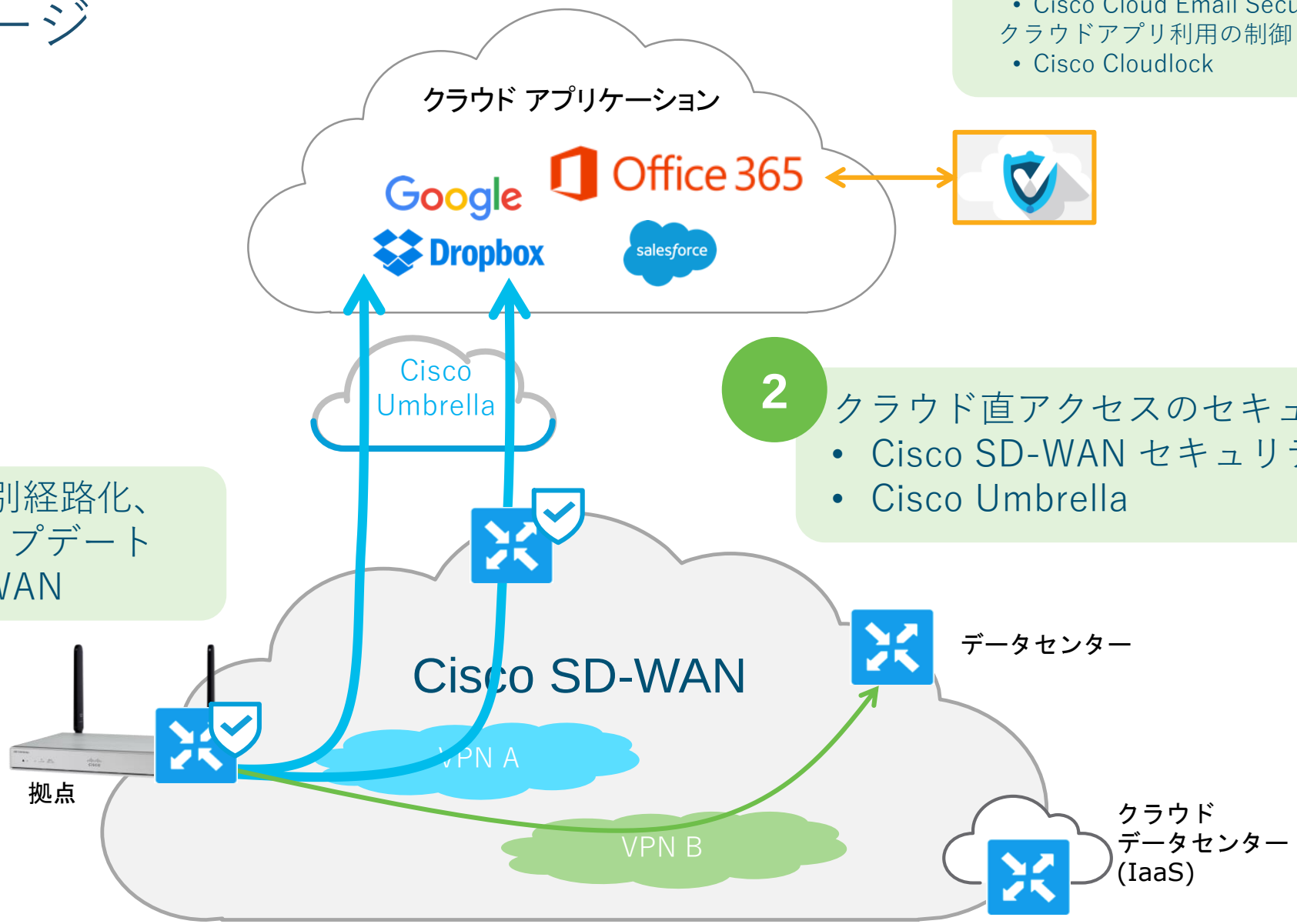
- クラウド直アクセスのセキュリティ

クラウドアクセス
インフラ

Step1
梅

- O365の識別と別経路化
- 直接のインターネットアクセス
- 各拠点からの効率的なアップデート

導入イメージ



3 メールセキュリティ
- Cisco Cloud Email Security with AMP

クラウドアプリ利用の制御と可視化
- Cisco Cloudlock

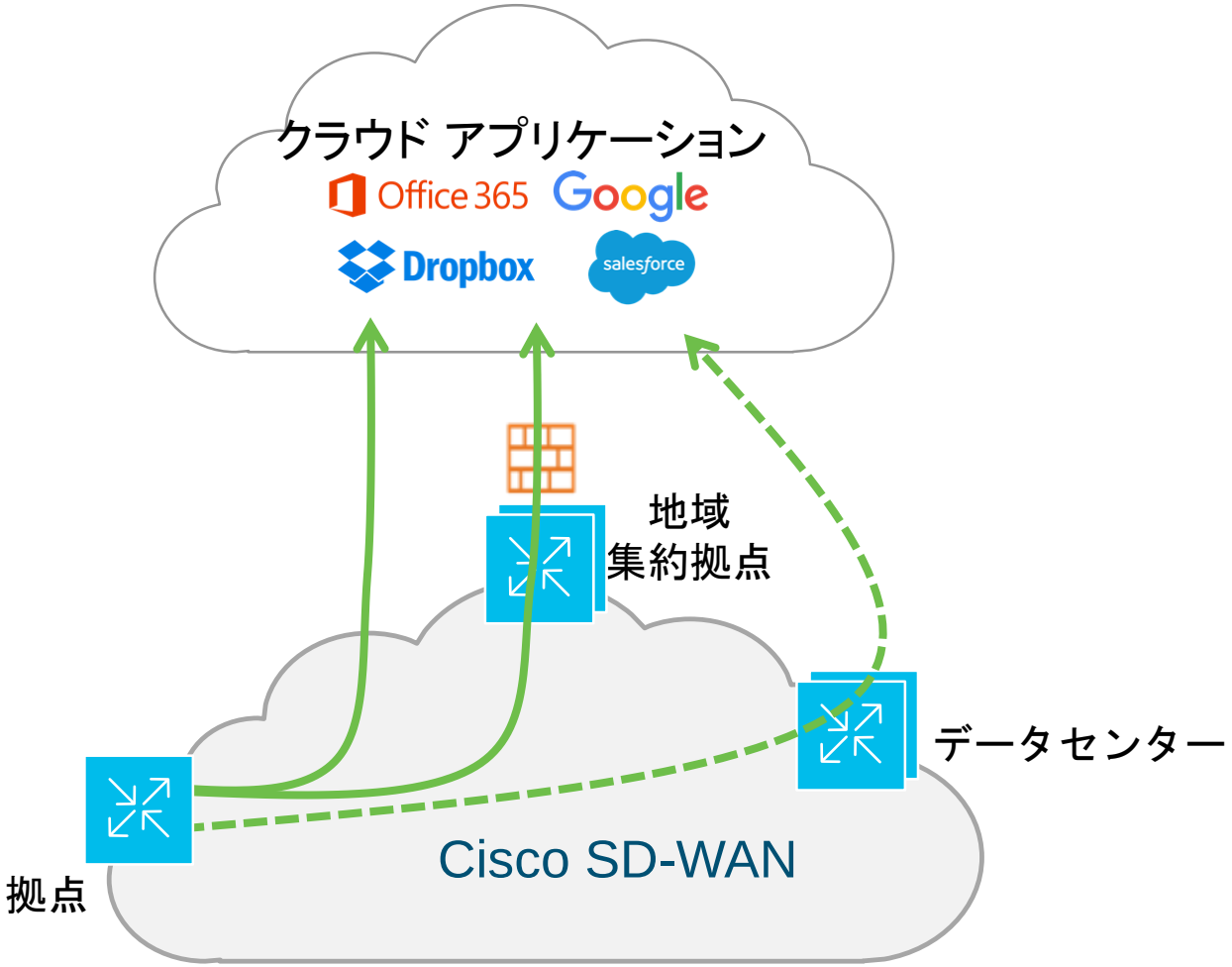
2 クラウド直アクセスのセキュリティ
- Cisco SD-WAN セキュリティ
- Cisco Umbrella

1 O365識別と別経路化、効率的なアップデート
- Cisco SD-WAN

Cisco SD-WAN　インターネットブレークアウト

1 O365識別と別経路化、効率的なアップデート

■O365など、SaaS向けに直接インターネットアクセス



✓ブレークアウトの考慮点

対象トラフィック	•全インターネット向けトラフィック •ポリシーで選択 （5-taple, DPIその他）
ブレークアウト ポイントの選択	•当該のローカル拠点 •地域集約拠点
安全なアクセス	•Port-Address Restricted NAT •地域集約拠点のFW •ローカル拠点のルータ組込み型FW
さらなる最適化	Cisco Cloud OnRamp

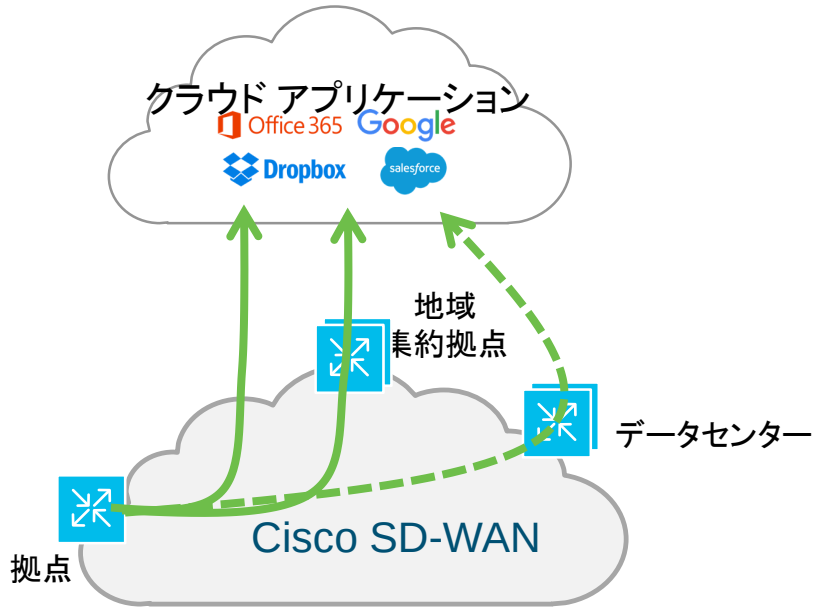
インターネットブレイクアウトの進化系
Cloud OnRamp for SaaS

1 O365識別と別経路化、効率的なアップデート

■最適な出口(ブレイクアウトポイント)を自動選択

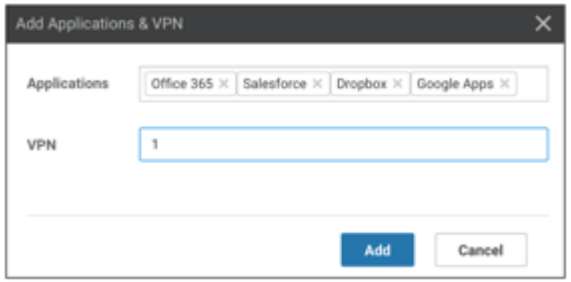
例えば

- 拠点から直接 or 地域集約拠点から
- 複数の地域集約拠点A、Bのいずれかから　等

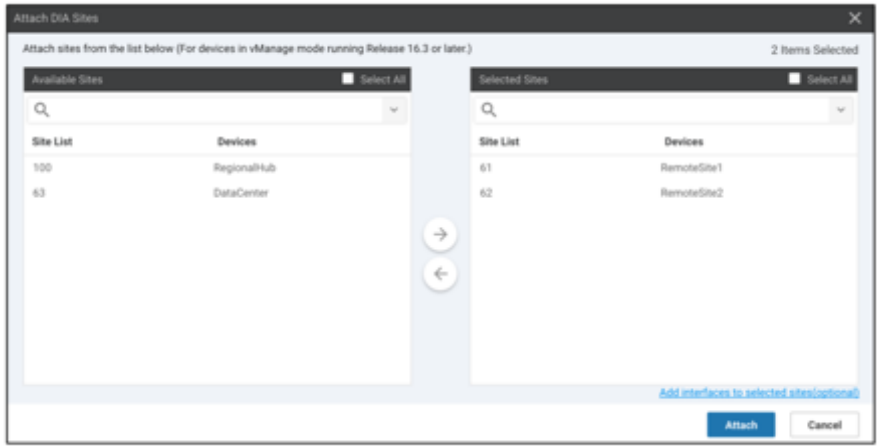


設定概要

1. ブレイクアウトするSaaSアプリケーションを選択

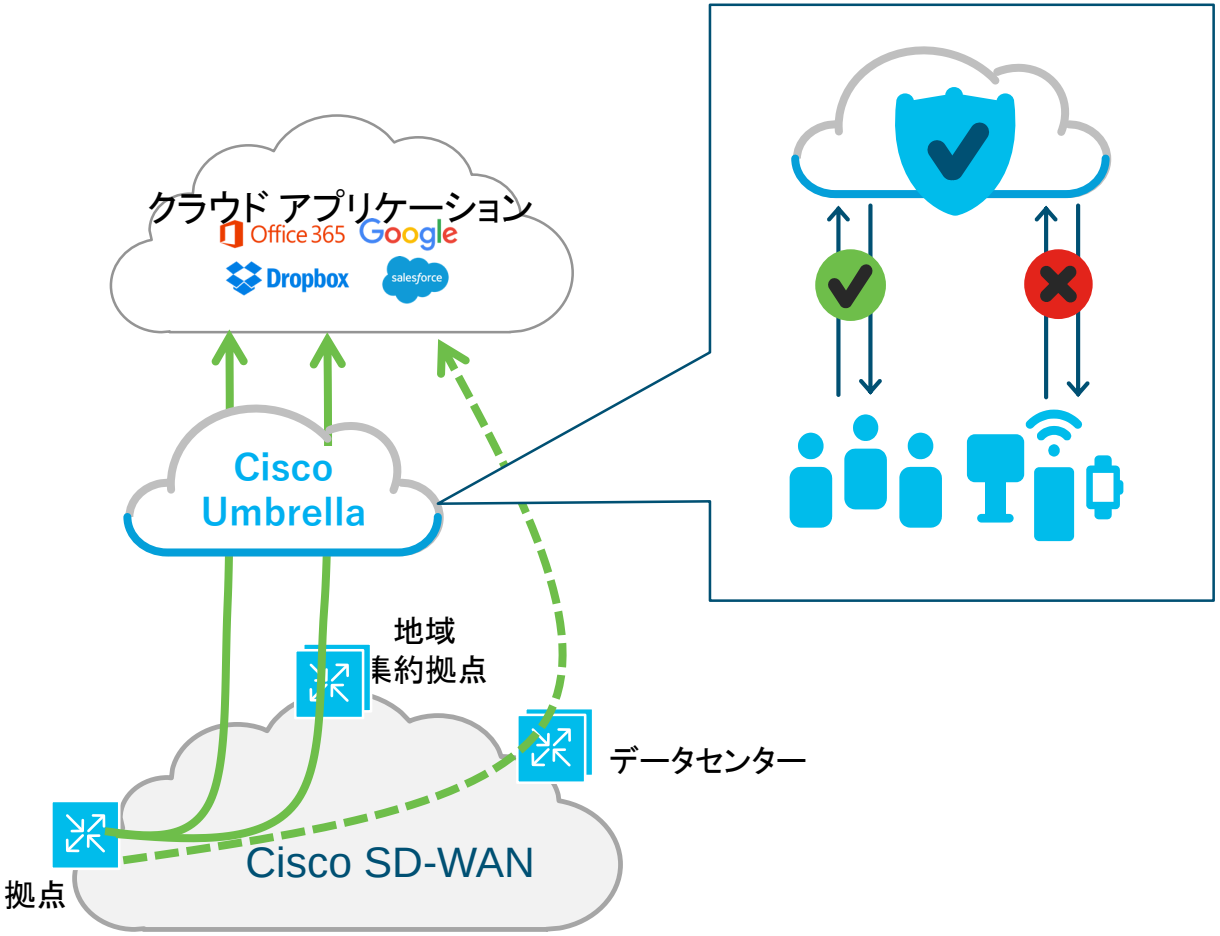


2.



2 クラウド直接アクセス時のセキュリティ

クラウド型セキュリティ Cisco Umbrella DNSレイヤを保護



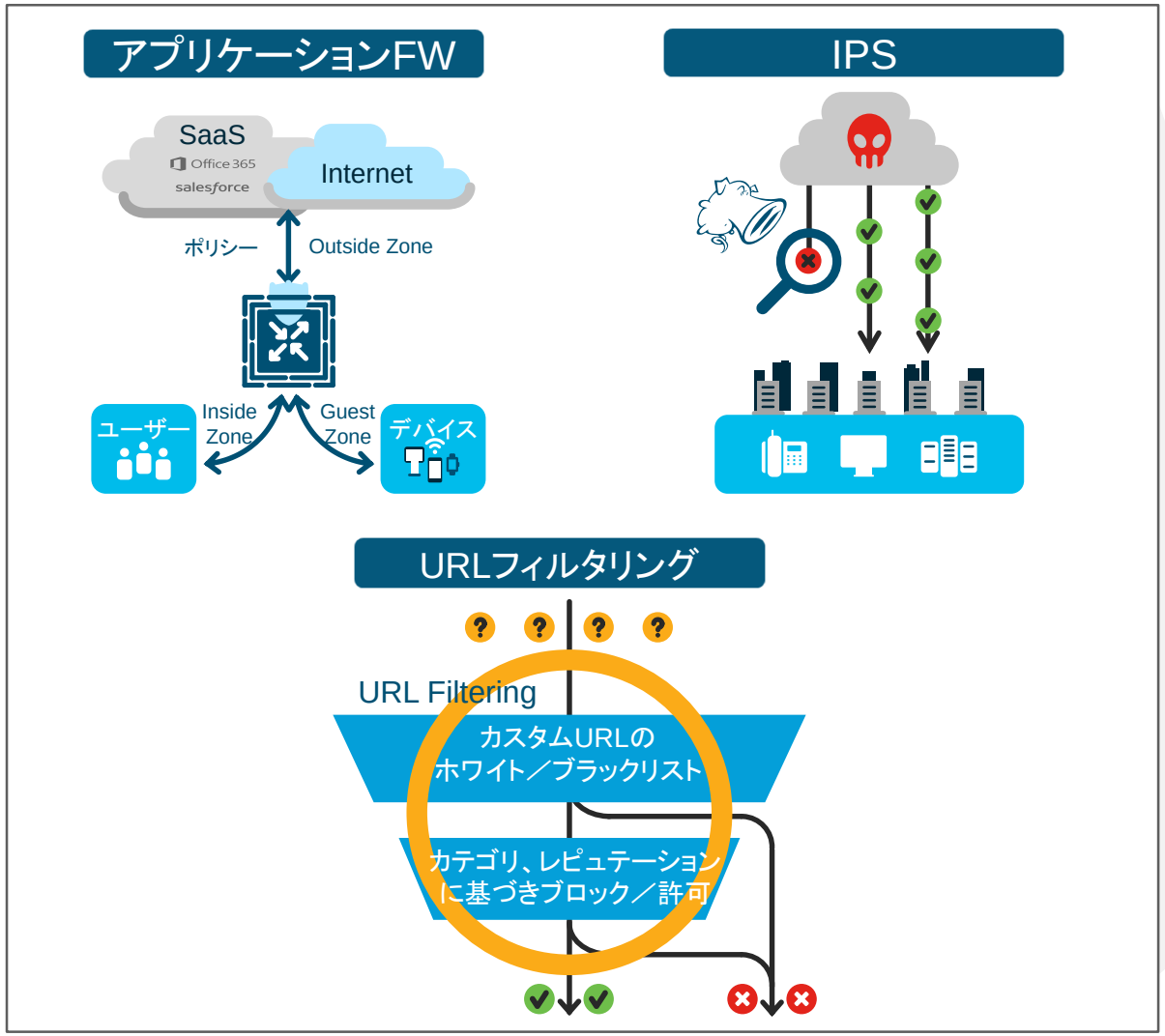
■ Cisco UmbrellaのDNSセキュリティ

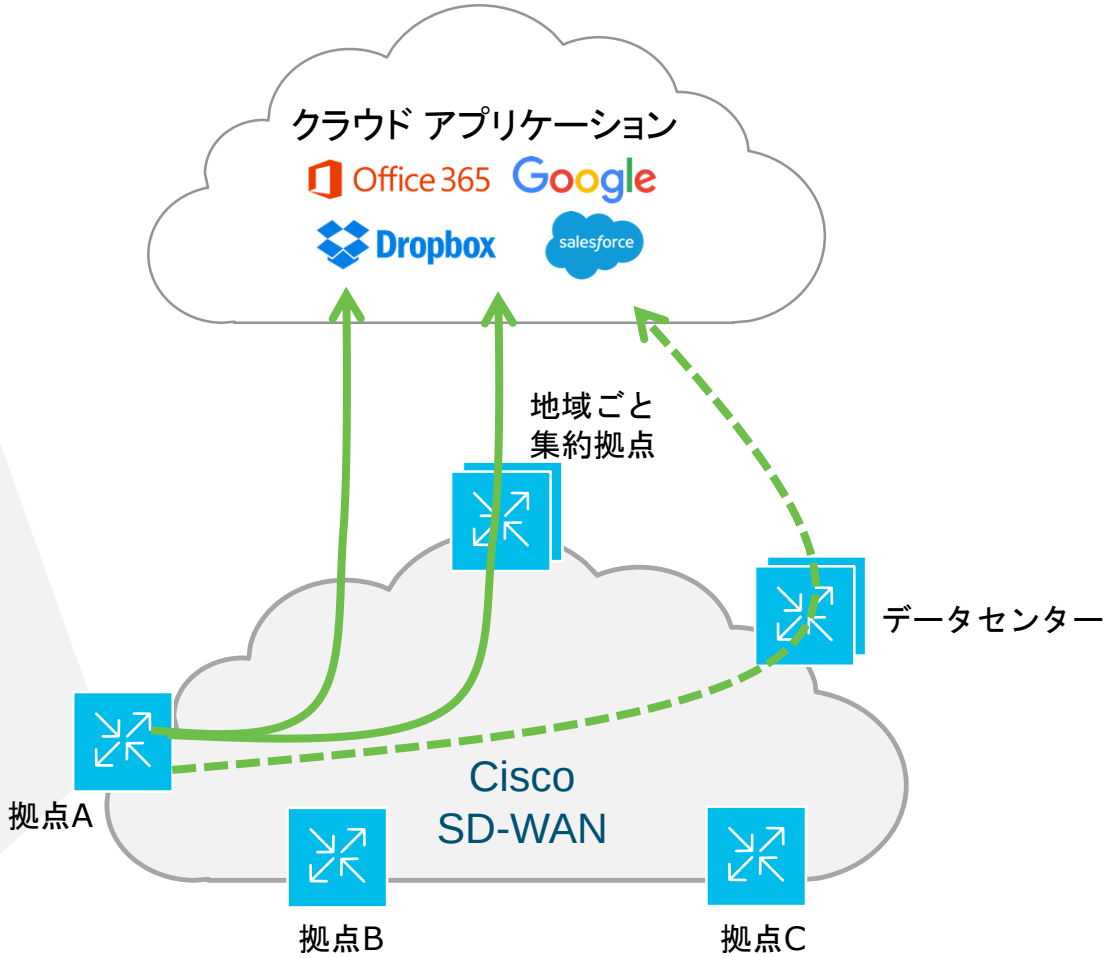
- ランサムウェアをホストするサイトへのDNS要求をブロック（C2通信のブロック）
- ポート・プロトコルに依存しない対策

✓DNS保護が有効
- C2通信は、FWなどを通り抜けやすい
- 80/443以外のポートを使うものが増加中
- Umbrellaは全ポート・プロトコルを保護

2 クラウド直接アクセス時のセキュリティ

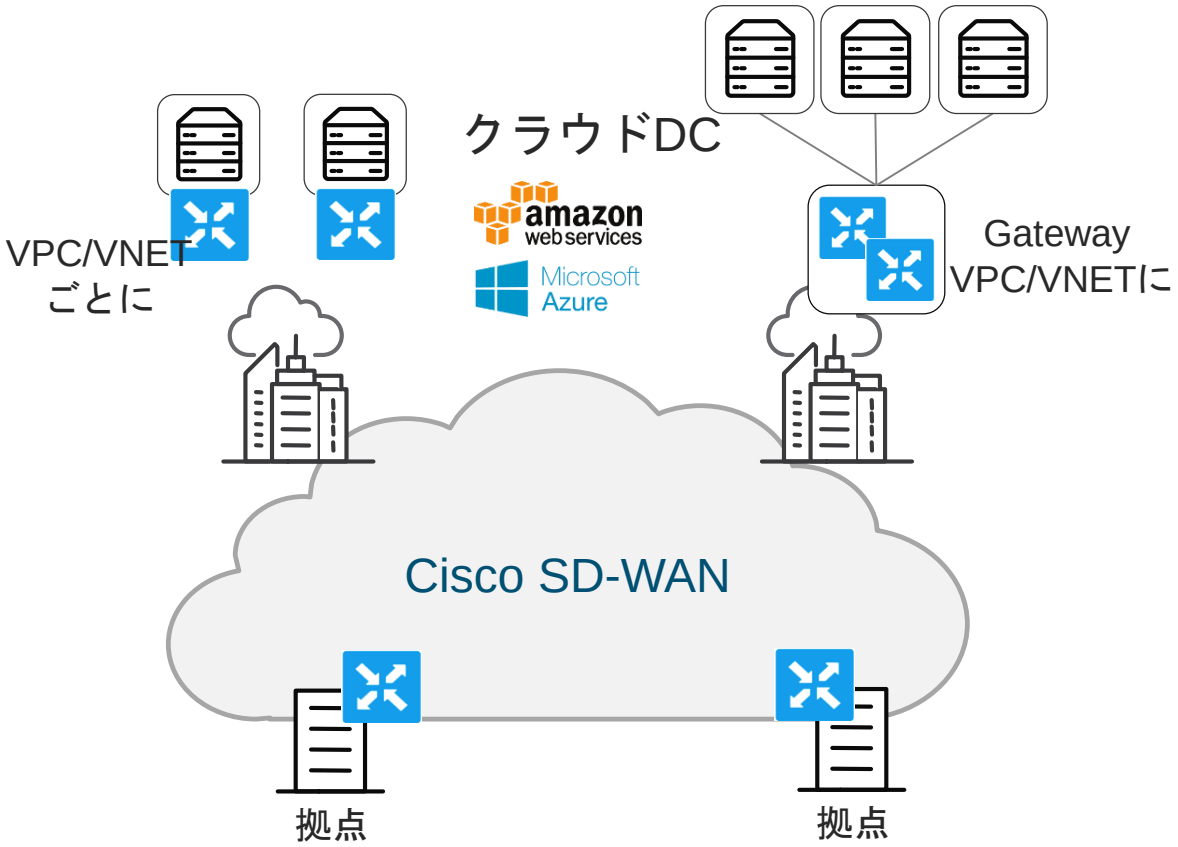
組込み型セキュリティ
Cisco SD-WANがデフォルトでアクセス保護





ところで… クラウド化対応は、O365/SaaSだけですか？

■パブリッククラウドをSD-WAN化



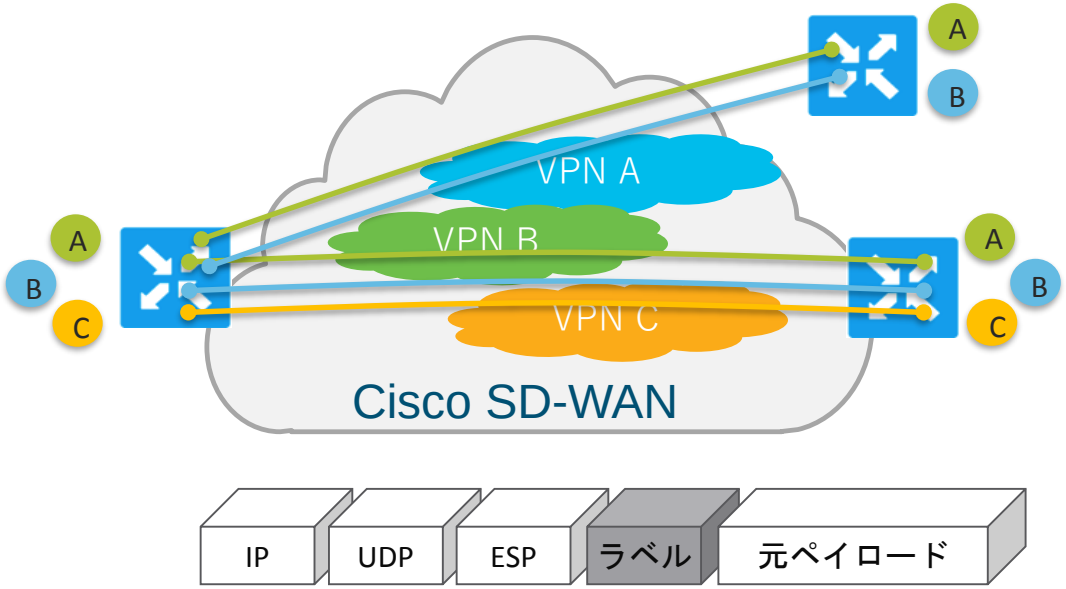
パブリッククラウド上に仮想SD-WANルータを配備
あたかも自社拠点のひとつのように！

SD-WANのメリット：可視化、管理
- クラウド／オンプレ問わず集中管理
- コンフィグ、ポリシーの共通化
- 帯域使用状況の可視化

2つの展開パターン
- VPC/VNETごとに設置
- Gateway VPN/VNETに設置

Cisco SD-WANを使いつくす セグメンテーション

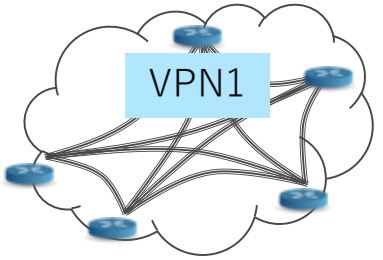
WAN回線によらず、複数VPNを構成



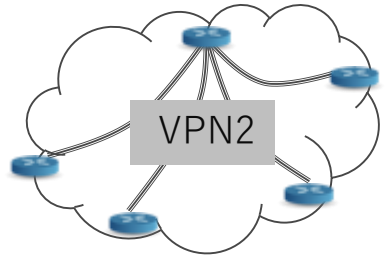
- SD-WANルータはVPN毎にルーティングテーブルを保持
- インターフェイス、サブインターフェイス(802.1Q)をVPNにマップ

VPNごとに 異なるトポロジーもOK

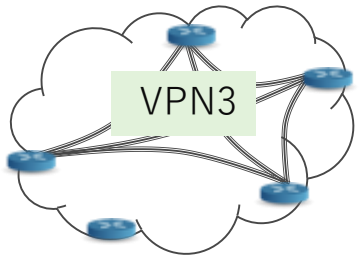
フルメッシュ
（UCなど）



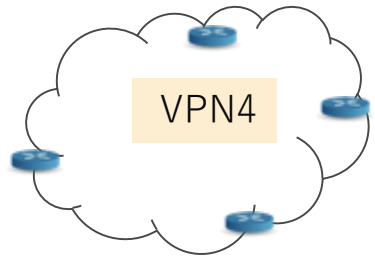
ハブ＆スポーク
（決済アプリなど）



部分メッシュ
（リージョン限定アプリなど）



ノーコネクション
（ゲストWiFiなど）



Cisco SD-WAN対応ルータ

- 従来から実績あるHWモデル、Wi-Fi, LTE対応
- 組込みセキュリティ
- 非SD-WAN拠点とも資産共用

ブランチ

ISR 1000

- 固定構成・ファンレス
- 4G LTE、Wi-Fiモデル
- DNA ~100M License

ISR 4000

- モジュラー構成
- コンテナアプリケーションの統合
- DNA ~500M License (モデルによる)

vEdge 100

- 100 Mbps
- 4G LTE オプション

vEdge 1000

- 最大 1 Gbps
- 固定構成

データセンター

ASR 1000

- Hwベースの高パフォーマンス
- HW, SWの冗長性
- DNA ~10G License

vEdge 2000

- 10 Gbps
- モジュラー構成

仮想化

CSR 1000V

- 10Mbps ~ 10Gbps
- DNA 仮想化
- 拡張ルーティング
  セキュリティ
  クラウド マネジメント

ENCS

- VNF、サービスチェイニング
- 3rd party オープンサービス・
  アプリケーション

vEdge Cloud

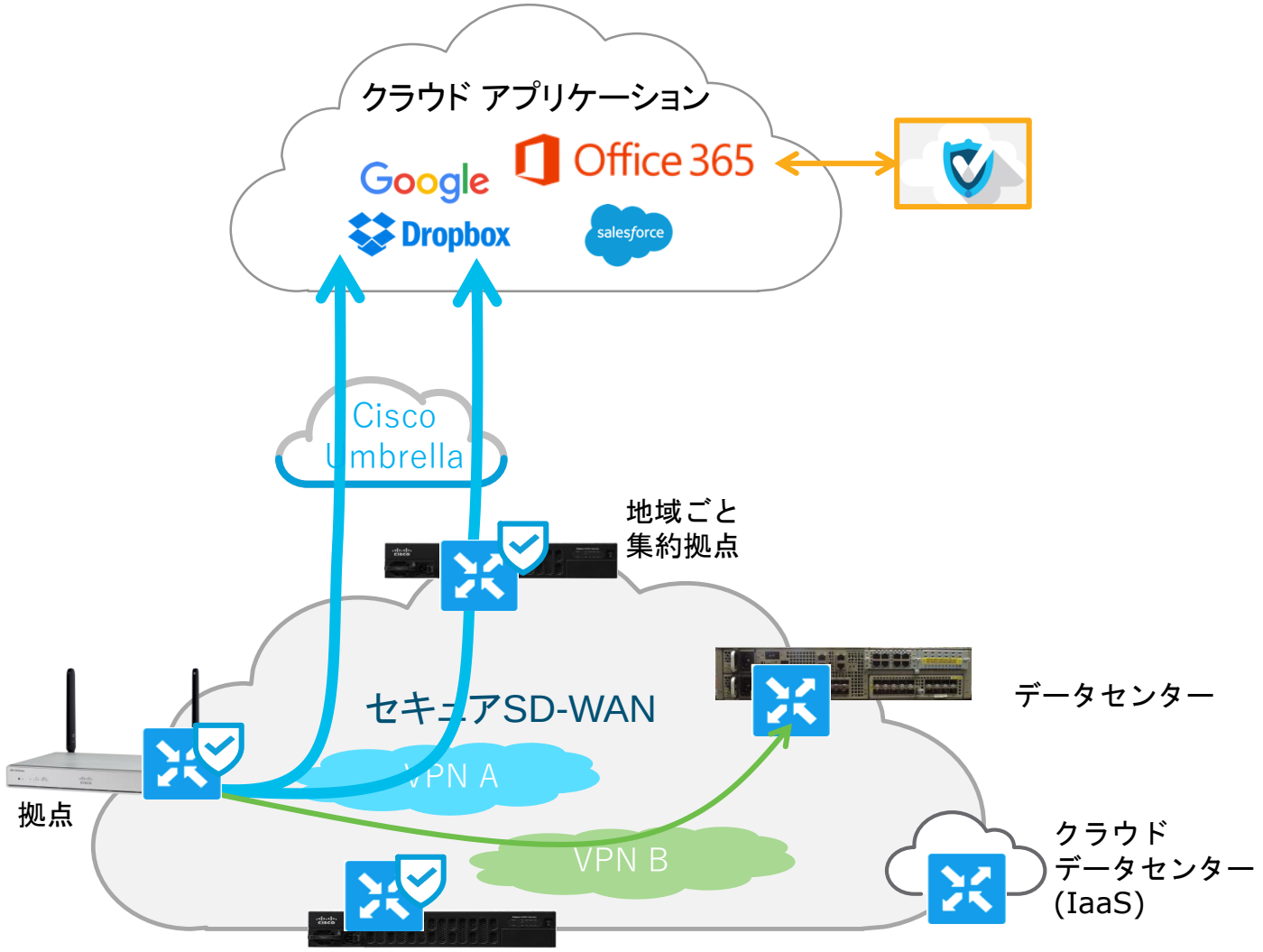
- 10Mbps ～ 100Mbps
- SD-WANオーバレイをパブリ
  ッククラウドまで拡張

まとめ　Cisco SD-WAN
セキュア SD-WAN 導入イメージ

- O365の識別と別経路化　ブレークアウト
  - 考慮点：識別法、出口選択(Cloud OnRamp)
- セキュアなクラウドアクセス
  - ルータ組込み型
    アプリケーションFW, IPS, URLフィルタリング
  - クラウド型DNAセキュリティ
    Cisco Umbrella

さらに…

- VPN機能でトラフィック分離
- メールセキュリティ、クラウドアプリ可視化




CISCO