



SASE 最新アップデート

～導入事例に学ぶ成功ポイントと最新機能ご紹介～

あらゆるネットワーク上のあらゆるアプリケーションに安全かつシームレスに接続

2025年2月20日

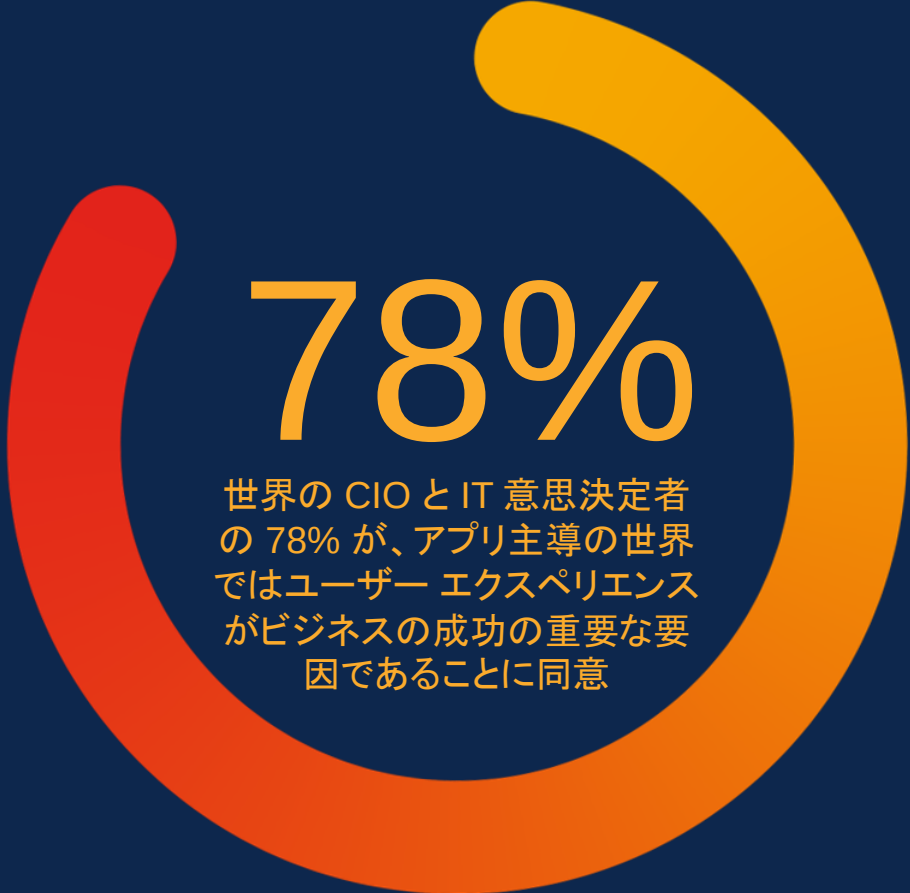
ネットワーキング事業
アカウントエグゼクティブ 次藤 則兼

Network & Security 市場動向

アプリケーションとユーザーは**様々な場所に**
存在するため、安全な接続が急務となっています。



シームレスで信頼できる
ネットワークとアプリケ
ーションを提供すること
が重要となります。



78%

世界の CIO と IT 意思決定者
の 78% が、アプリ主導の世界
ではユーザー エクスペリエンス
がビジネスの成功の重要な要
因であることに同意

ユーザエクスペリエンス
= 快適性・安全性の向上

エンドツーエンドで信頼できる エクスペリエンス(快適性・安全性の向上)の 3 つの重要な要素

自動制御

回復力のある
シームレスな接続



安全性

安全で保護された
ネットワーク



最適化

素晴らしい体験を
すべての人達に提供



統合されたプラットフォームで管理および接続

実現する上での阻害要因は何か？

柔軟性の低い
ネットワーク構成



限定的・画一的なネットワークパス設定により柔軟性・回復力が低下

均一化されていない
ネットワーク・セキュリティポリシー



サイロ化されたネットワーク・セキュリティポリシーは攻撃者にとっての扉を開く

不十分な可視性と
アプリ制御の欠如



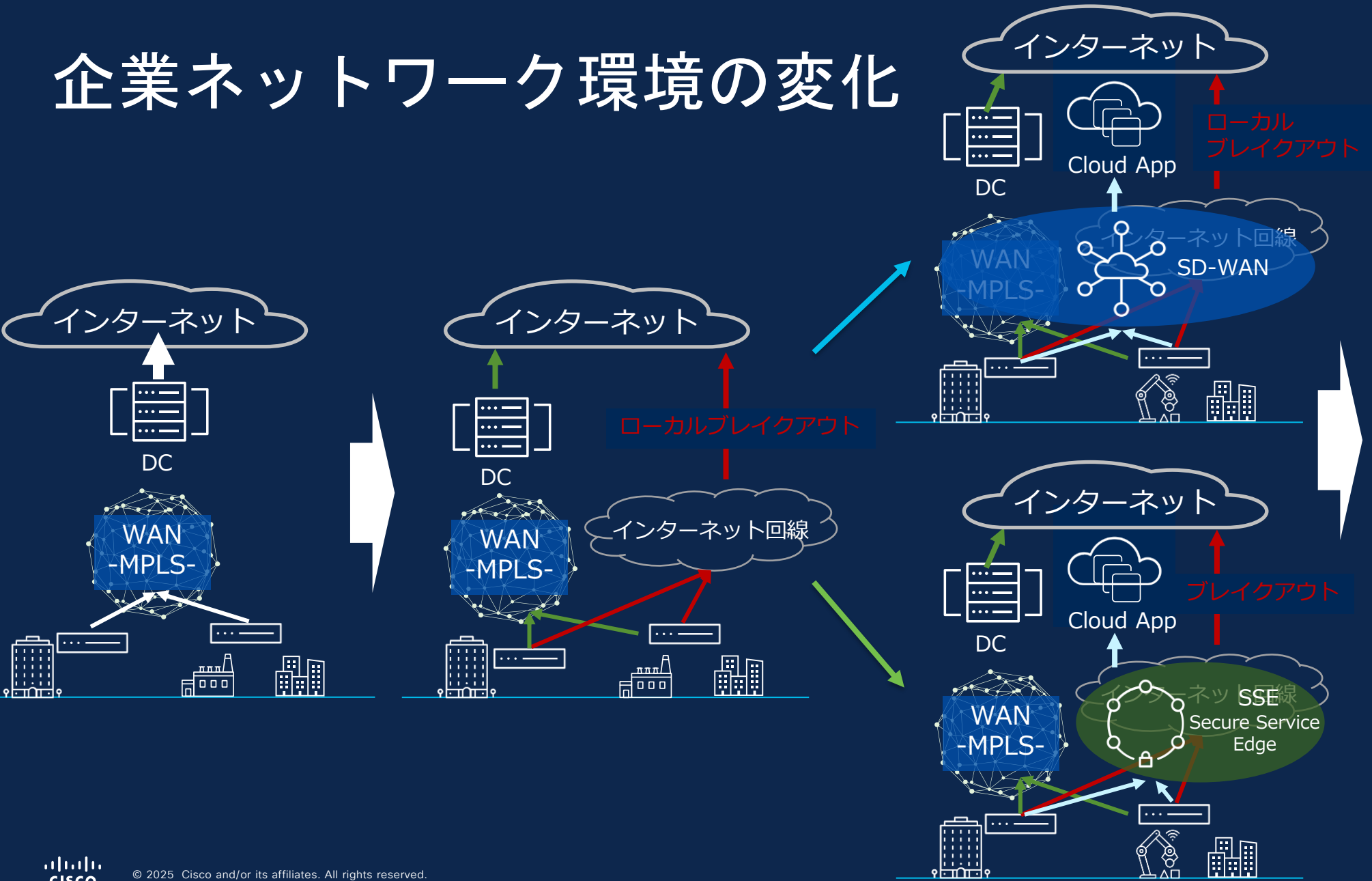
アプリへの接続性が低く、IT の可視性も低いため、ユーザーエクスペリエンスが著しく低下



IT 部門はどのようにしてこれらの課題を克服し、
信頼できるエクスペリエンス(快適性・安全性の向上)を提供
できるのでしょうか？

Network & Security お客様(マーケット)動向

企業ネットワーク環境の変化



SSEとSD-WANのハイブリッドヘシフト

The diagram shows two overlapping ovals representing the hybrid shift between **SSE** (Secure Service Edge) and **SD-WAN**. The top oval is green and labeled **SSE Secure Service Edge**. The bottom oval is blue and labeled **SD-WAN**. The ovals overlap, indicating a hybrid architecture.

企業ネットワーク環境の変化

- SaaS / IaaS -



- Middle Mile -



- Middle Mile -



DC



本社



工場



拠点



海外
WAN



海外ネットワーク網



店舗



Work from
Home



工場
生産設備



協力会社



リモートワーク



自動車
Connected Car

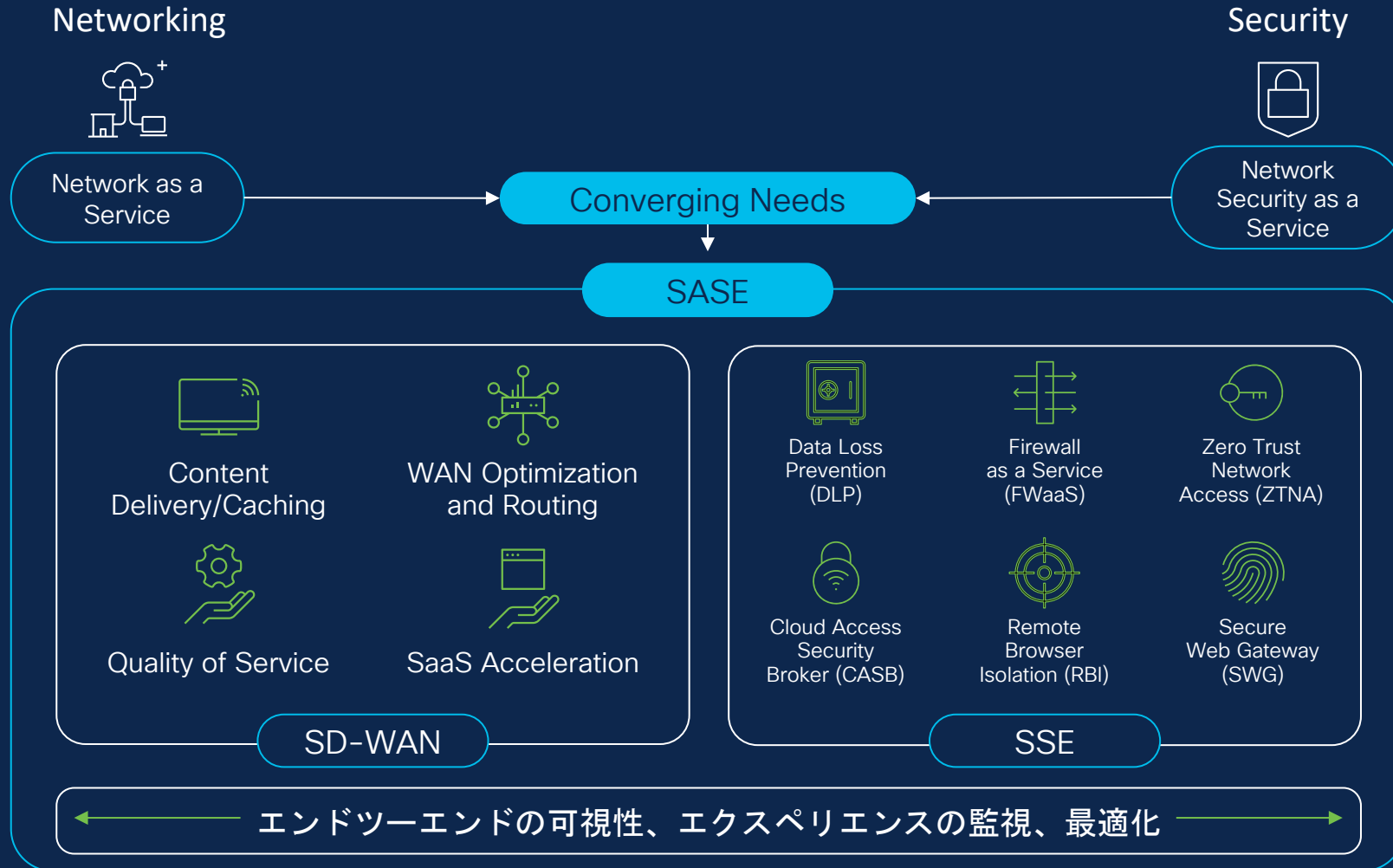


コールセンター



Secure Access Service Edge (SASE)

現在の分散環境におけるユーザエクスペリエンス(快適性・安全性の向上)を実現するアーキテクチャ



SASE成功に導くための 検討・導入ポイント

Secure Access Service Edge (SASE) とは

現在の分散環境におけるユーザエクスペリエンス(快適性・安全性の向上)を実現するアーキテクチャ

<https://www.gartner.com/en/information-technology/glossary/secure-access-service-edge-sase>

Secure Access Service Edge (SASE) Definition by Gartner

Secure access service edge (SASE) delivers converged network and security as a service capabilities, including [SD-WAN](#), [SWG](#), [CASB](#), [NGFW](#) and [zero trust network access \(ZTNA\)](#). SASE supports **branch office, remote worker and on-premises secure access use cases**. SASE is primarily delivered as a service and enables zero trust access based on the identity of the device or entity, combined with real-time context and security and compliance policies.

[SD-WAN](#)、[SWG](#)、[CASB](#)、[NGFW](#)、[ゼロトラストネットワークアクセス \(ZTNA\)](#) など。SASE は、**ブランチオフィス、リモートワーカー、オンプレミスのセキュアアクセス**のユースケースをサポートします。SASE は主にサービスとして提供され、**デバイスまたはエンティティの ID と、リアルタイムのコンテキスト、セキュリティおよびコンプライアンスポリシーに基づいてゼロトラストアクセス**を可能にします。

SASE実現にむけた重点項目

SASE (Secure Access Service Edge)化にあたり、ユーザがどの部分を重要視しているのか？
可用性やコネクティビティ、Cloud/IaaSシフトをしているのか？セキュリティのCloud化や強化を考えているのか？ゼロトラストを基軸としたセキュリティの強化を考えているのか？

コネクティビティ

SD-WAN, VPN, Remote Access

Catalyst SD-WAN

Cisco Secure Client

セキュリティ

SWG, Firewall, CASB

Cisco Secure Access

アイデンティティ

MFA, ZTNA
Posture

ISE, Duo

SASE成功に導くための検討・導入ポイント #1



目指すべき将来像の創出

- ✓ リモートワークの増加への対応
- ✓ デジタルシフトにおけるDCからIaaS/SaaSへの移行
- ✓ セキュリティ対策の強化



現状の構成の把握

- ✓ リモートワークとオフィスワークの割合
- ✓ アプリケーションの所在と利用量の把握
- ✓ 不足している部分の把握: Network, Security, 可視化



問題点・課題の抽出

- ✓ 通信の一極集中による帯域の逼迫
- ✓ 不揃いなセキュリティ対策
- ✓ シャドーITなど管理外のアプリや機器がある



スコープの設定

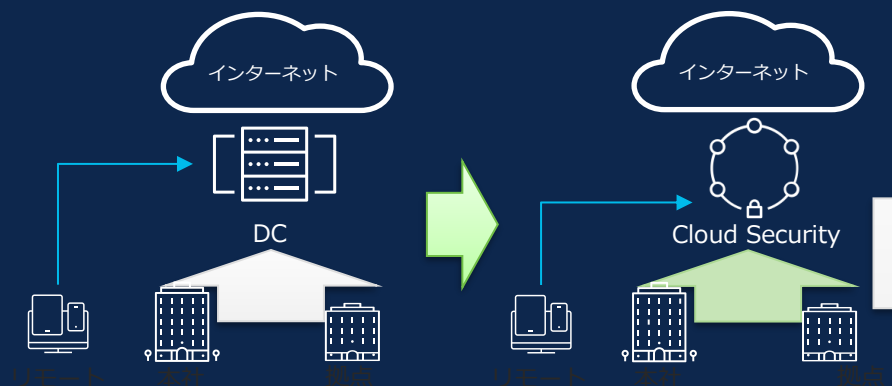
- ✓ どこから始めて、どこで終わるのか: Architecture
- ✓ 特にSASEの適用範囲を事前に決めておく: 本社、拠点、工場
- ✓ 残すもの、変えるもの、残さないもの: DC, App

SASE成功に導くための検討・導入ポイント #2

現状

DC・Cloud Security一極集中からの脱却

- ✓ SaaSアプリケーションの増加によりネットワークトラフィック急増
- ✓ データセンター一極集中からCloud Securityへとシフト
- ✓ Cloud Securityによる一元的なセキュリティ対策
- ✓ リモートワーカーのVPN接続も、データセンターからCloud Securityへシフト



課題

アプリケーション毎に経路と行き先をコントロール

- ✓ アプリケーションの種別と重要度、トラフィック量を把握
 - 切れると業務に大きく影響する通信 → OT/生産系, Web会議, 勘定系
 - 侵害されると困る通信 → R&D, 機密情報・パテント
 - 多くの人が定常的に利用する通信 → Officeアプリ, 業務アプリ
 - リスクの多い一般的なInternet通信 → Web閲覧, ライブラリ参照

一極集中による問題点

- トラフィック増によるコストUp
- 期待しているスピードが出ない
→ 特にSaaS, 拠点間通信
- Single Point of Failure: 単一障害点

アプリケーションの重要度に応じた選択

- 通信経路の選択: 可用性、冗長性を重視
- 通信経路の分離: 完全性、機密性
- セキュリティの適用: 完全性、安全性

インターネットトラフィックのセキュリティ対策

- 主要なSaaS(MS365, Webexなど) → Breakout可能
- 一般的なInternet通信 → 要Cloud Security

SASE成功に導くための検討・導入ポイント #3

アプリケーションの重要度と特性、所在により、DIA(Direct Internet Access)、SSE経由、IaaS(SD-WAN接続)、DC (SD-WAN接続)と実装するセキュリティ対策を検討する

- ✓ M365通信:DIA推奨の宛先
- ✓ M365通信:上記以外の宛先
- ✓ Microsoft Update系の通信
- ✓ SCCM通信
- ✓ ファイルサーバ・共有サーバ
- ✓ 業務アプリケーション
- ✓ OT・生産管理系通信
- ✓ IP電話
- ✓ Web Meeting
- ✓ RDP/SSH/FTP通信

- ✓ どの回線
- ✓ どの経路
- ✓ どのようなセキュリティ
- ✓ どれだけの帯域
- ✓ 重要度は？

アプリケーションのトラフィック量と重要度に応じた経路選択と強固なセキュリティ対策

SASE成功に導くための検討・導入ポイント #4

解決策

SSEとNetworkingをバランスよく組み合わせた
アプリケーションのトラフィック量と重要度に応じた経路選択と強固なセキュリティ対策

Ciscoソリューション

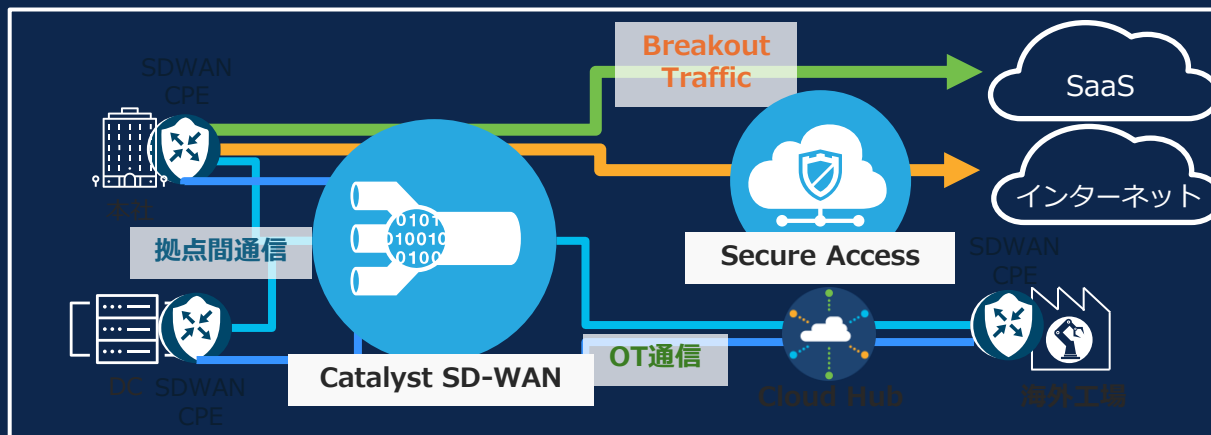
Cisco Catalyst SD-WAN特徴

詳細な
アプリケーション
振り分けによる
適切な経路選択

高い安全性と
可用性を実現する
Act/Actでの冗長構成

ルータ・SD-WAN
としての
豊富な導入実績

WANを論理分割し
通信のセキュリティを確保する
WANセグメンテーション機能



Ciscoソリューション

Cisco Secure Access特徴

数十万User単位の
大手製造業など
豊富な導入実績

Talos Intelligence
精度の高い
脅威インテリジェンスの利用

リモートアクセスでは
ZTNA/VPNの
両方を利用可能
高い利便性を実現

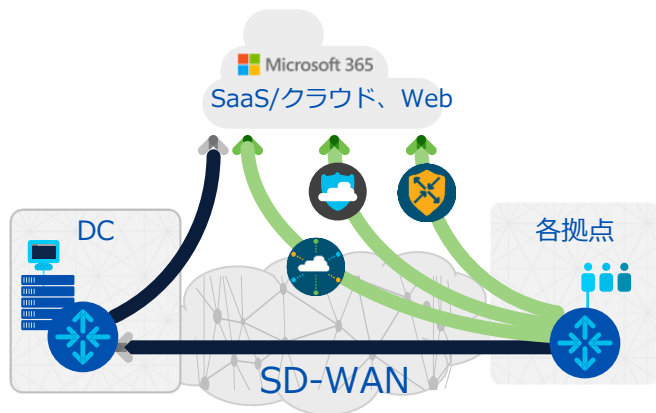
SD-WANとの
高い親和性による
真のSASE
ソリューション

Cisco Catalyst SD-WAN for Cisco SASE

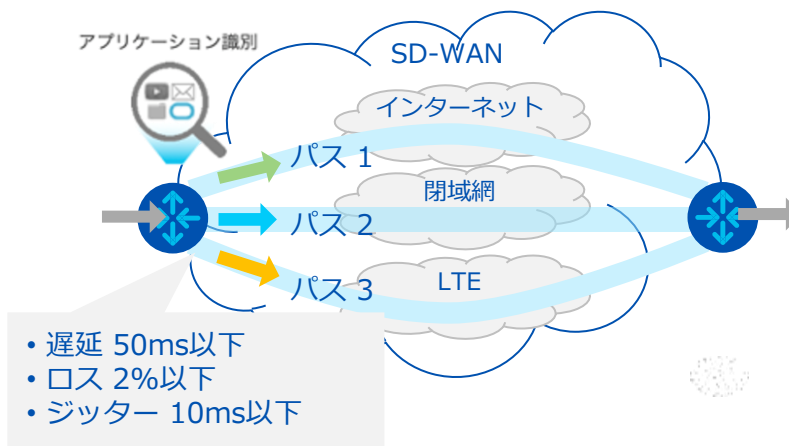
Cisco Catalyst SD-WAN ユースケース

Cisco Catalyst SD-WANは、クラウドベースのサービスとアプリケーションに迅速かつ安全にアクセスできるようにします。

ローカルブレイクアウト



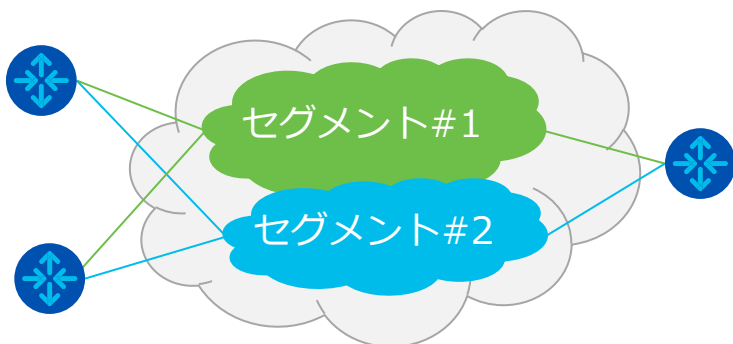
WAN利用の最適化



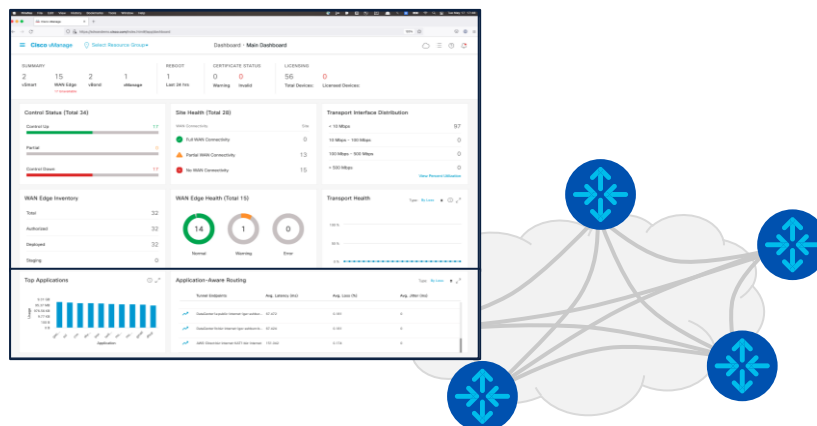
パブリッククラウド拡張



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

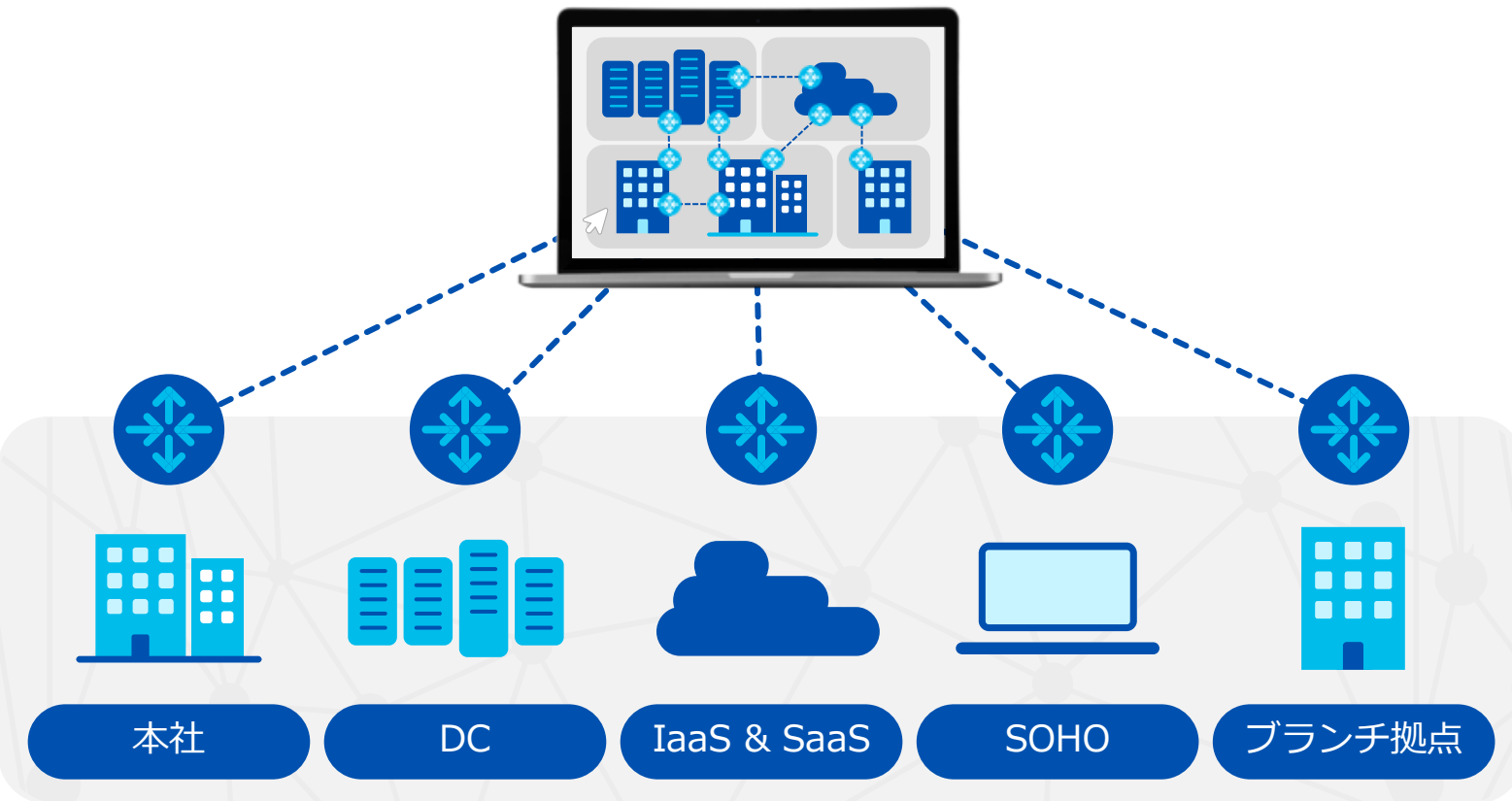


統合されたシンプルな管理を実現するCisco Catalyst SD-WAN

Cisco Catalyst SD-WANコントローラによる、SD-WANルータの一元管理

グローバルポリシーを設定し、大規模な自動化を通じてポリシーを効率的に構成し、そのグローバルポリシーの展開が1つのコンソールからすべての拠点に展開可能です。

Catalyst SD-WAN コントローラ



Catalyst SD-WANコントローラ特徴

- ポリシーを効率的に設定・適用し
スケーラブルな運用・自動化を実現
- セキュリティとネットワークの管理を同
一コンソールから
- 運用管理を簡易化
- WANネットワーク全体の可視性を向上

すべてのデバイスを手動で構成するために
費やす時間を削減できます。
そして、一元化されたコマンドから大規模
にそれを実際に行うことができます。

Point!

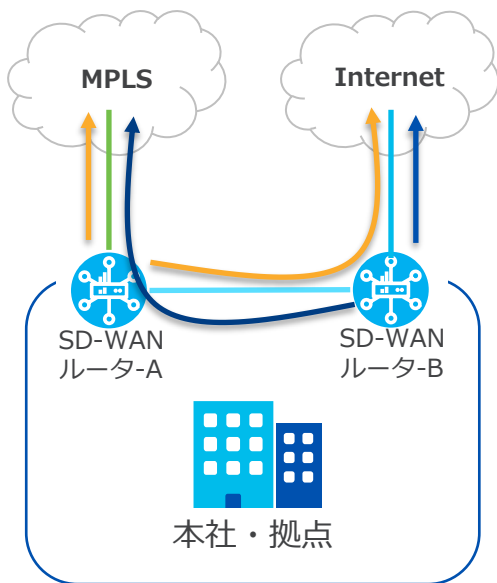
コントローラは、クラウドとオンプレの
2種類から選べます！

常に最適なアプリケーションエクスペリエンスを提供

既存回線 & インターネット回線の有効活用と、アプリケーションパスの自動切り替え

- TLOC-extensionは同一拠点の他のSD-WANルータの回線を、自分自身の回線として利用できる機能です。
- Application Aware Routing機能では、アプリケーションに接続するためのパスを自動的に選択し、リアルタイムで誘導し、さらに劣化したネットワークパスのアプリケーション トラフィックをインテリジェントに再ルーティングします。

TLOC-extension機能



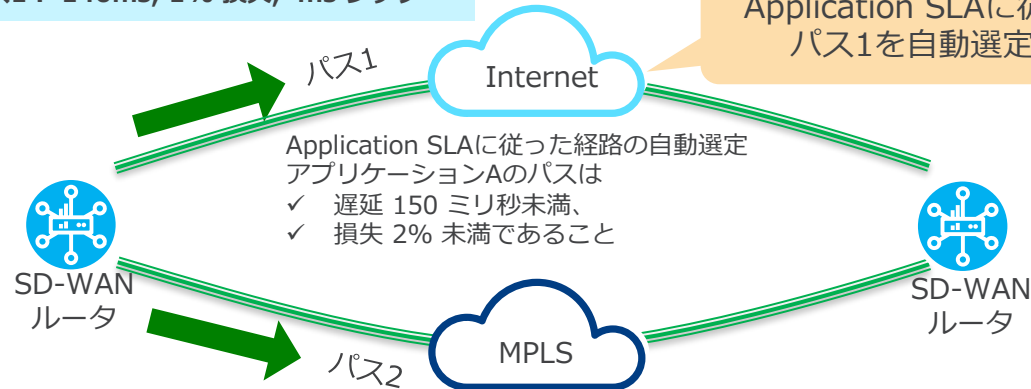
SD-WANルータは、それぞれ対応する回線にのみ接続されている状態の場合

- SD-WANルータ-A: MPLS回線
- SD-WANルータ-B: Internet回線

SD-WANルータ-Aは、直接接続された回線と、隣接するSD-WANルータ-Bに接続された回線にIPsec トンネルを構築します。隣接するSD-WAN ルータは、もう一方のSD-WANルータ-Bから開始されたトンネルのアンダーレイルータとして機能します。どちらかの回線に障害が発生した場合、他方の回線を経由して通信を確立することが可能です。

Application Aware Routing (AAR)機能

パス1 : 140ms, 1% 損失, ms ジッター



Application SLAに従いパス1を自動選定

Application SLAに従った経路の自動選定
アプリケーションAのパスは
✓ 遅延 150 ミリ秒未満、
✓ 損失 2% 未満であること

パス2 : 200ms, 3% 損失, 5ms ジッター

常に回線状態を把握し、状態とポリシーによりアプリケーションの通信経路を自動で制御。

SD-WAN アプリケーション識別とカスタムアプリケーション制御

- -アプリケーション識別(NBAR2)と、カスタムアプリケーション制御の組み合わせで精度の高い制御が可能! -

NBAR2でのアプリケーション識別

業務アプリケーションの通信を最優先すべきところ、優先度の低いアプリケーションが利用可能な帯域を占有し、業務に支障が出てことがあります。アプリケーションを的確に識別し、制御することで、アプリケーションの振り分け、ブレイクアウト、利用制限などが可能となります。

カスタムアプリケーション

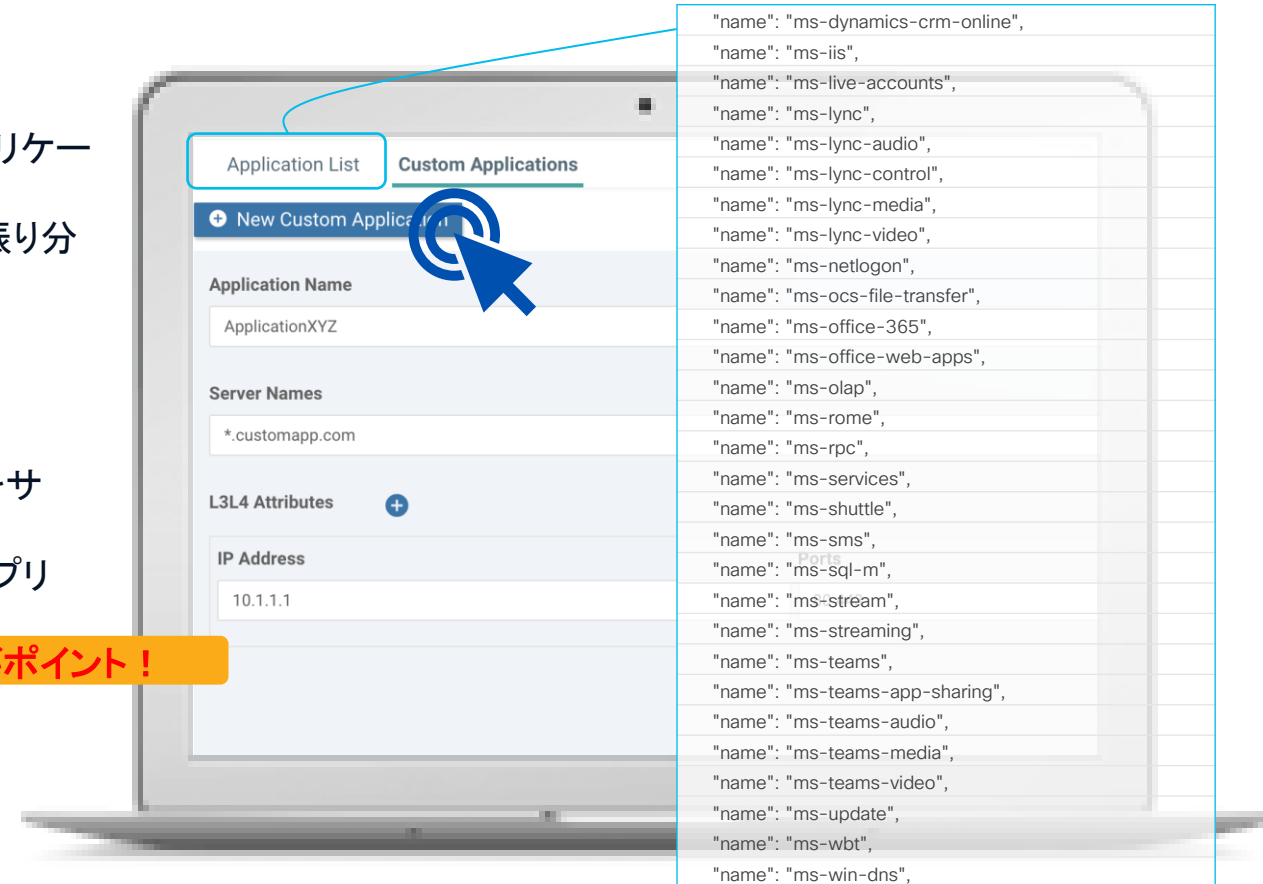
SD-WAN v17.3以降、NBAR2を利用したカスタムアプリケーション定義をサポート。

ユーザ定義のシグニチャを利用すると、トラフィックポリシーの設定とアプリケーションの監視は大幅に簡素化可能。

マイナなアプリケーション、自社開発アプリ対応可能
ファーストパケット問題対策

ここがポイント!

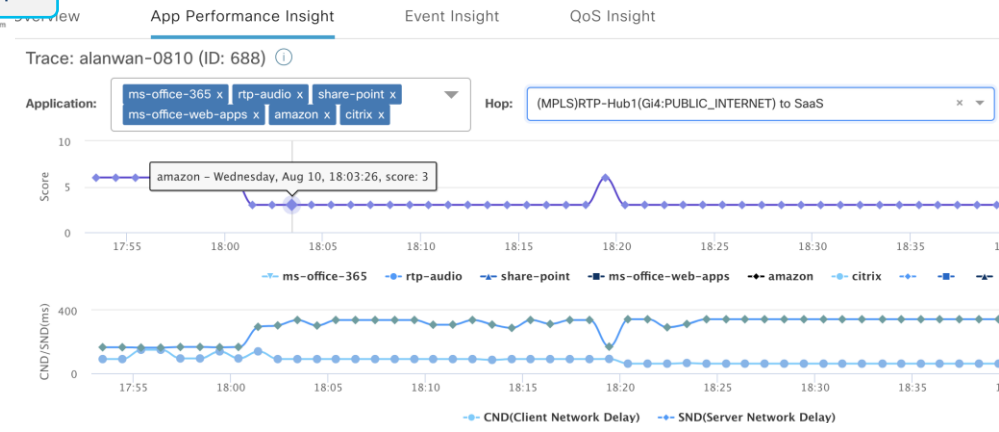
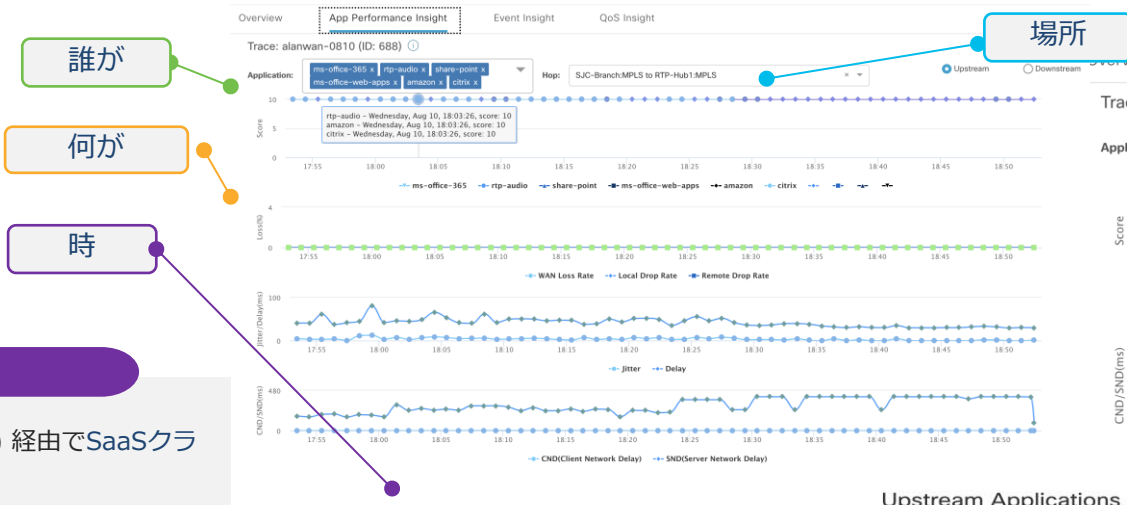
ここがポイント!



社内開発のアプリケーションやあまり一般的でないアプリケーションを認識し、これらのトラフィックに対してアクションを実行し、アプリケーション制御・ブレイクアウト・監視など、トラフィックポリシー定義が可能となっています。

日々の運用で役立つアプリケーションパスの可視化機能

NWPI(Network Wide Path Insight)では、ネットワークの運用に関する包括的な洞察を提供し、パフォーマンス分析、計画、およびトラブルシューティングに役立ちます



読み出し

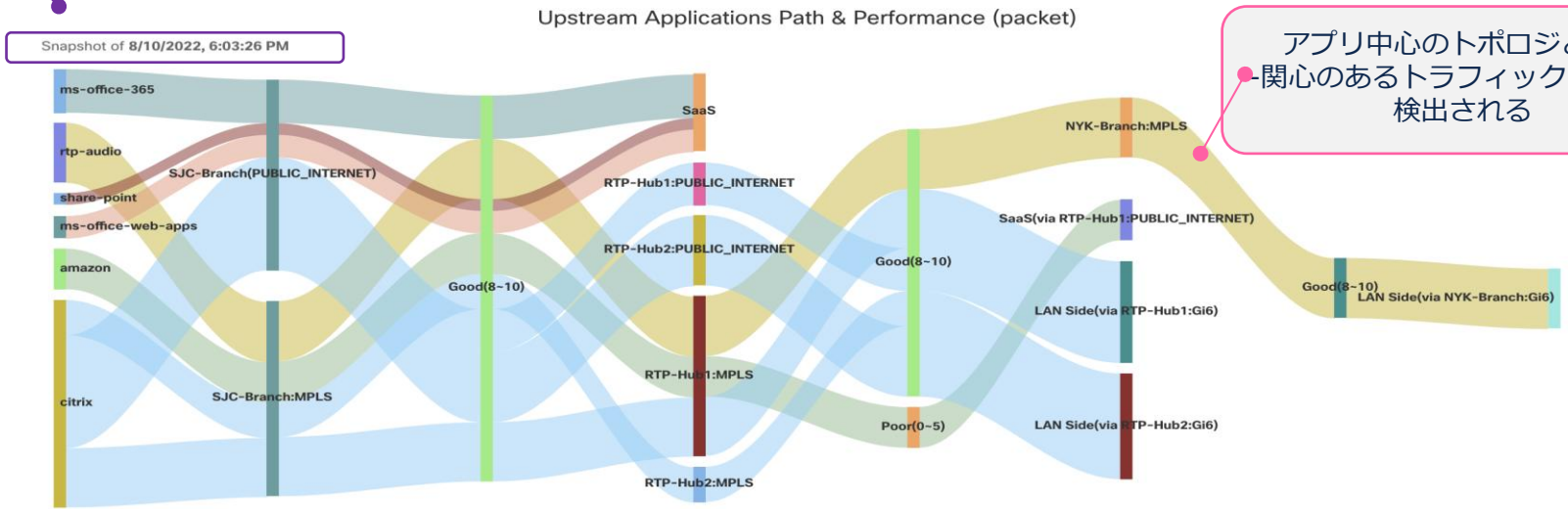
M365:SJC-BranchからINET (DIA) 経由でSaaSクラウドへのローカルブレイクアウト。

Amazon:SJCブランチからMPLS経由でRTP-Hub 1にバックホールし、次にINET (DIA) 経由でSaaSクラウドにブレイクアウトします。

ホップでのパフォーマンスが低い:
RTP-Hub 1からSaaS (INET経由)
高サーバネットワーク遅延、スコア3

rtp-audio:SJC-BranchからRTP-Hub 1 (MPLS) 経由でNYK-Branchへ

Citrix:SJCブランチからMPLS/INET経由でRTP-Hub 1/Hub 2にロードバランスし、次にLAN経由でキャンパス/DCにロードバランスします。

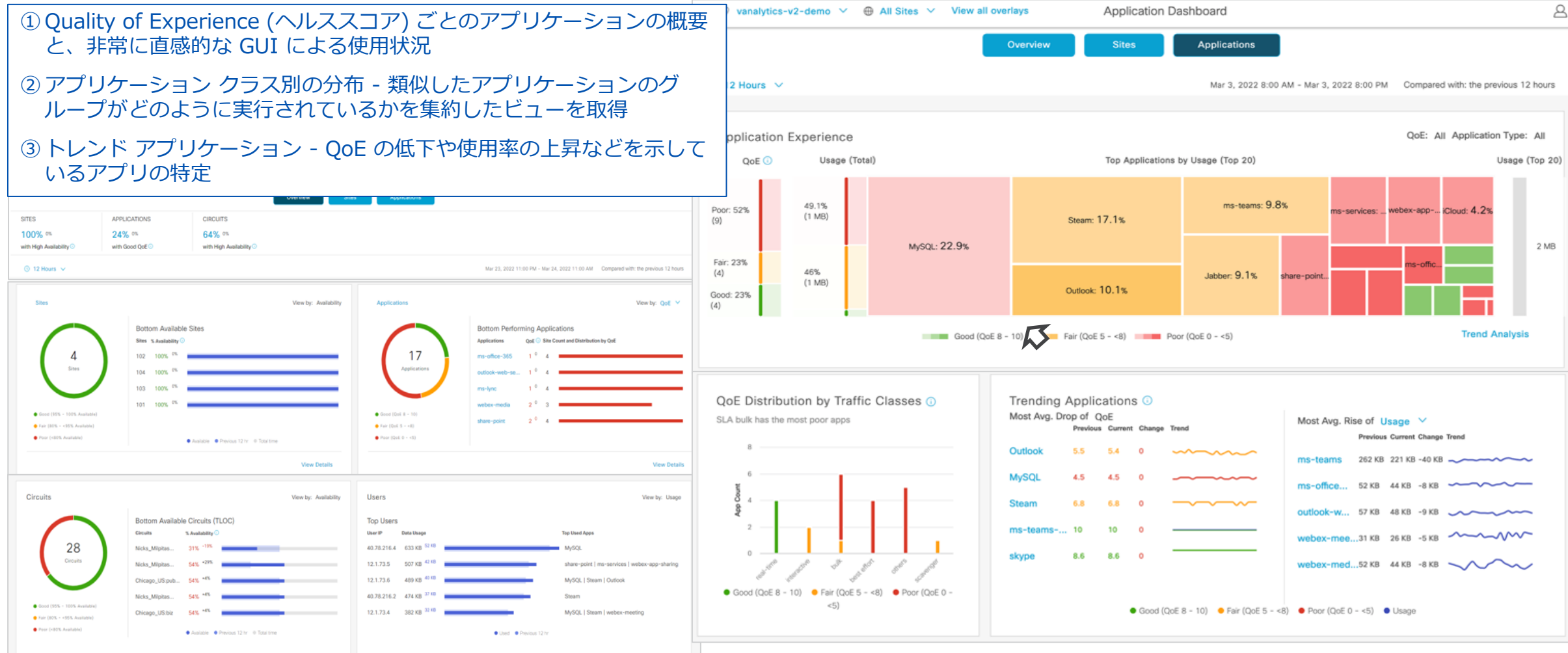


アプリ中心のトポロジとパス
-関心のあるトラフィックによって
検出される

SD-WAN導入後の効果測定が可能な分析機能:vAnalytics

ネットワークのパフォーマンスを監視し、異常や問題をリアルタイムで検出可能です。さらに、トラフィック分析: ネットワーク内のトラフィックを分析し、パフォーマンスのボトルネックや問題領域を特定します。

- ① Quality of Experience (ヘルススコア) ごとのアプリケーションの概要と、非常に直感的な GUI による使用状況
- ② アプリケーション クラス別の分布 - 類似したアプリケーションのグループがどのように実行されているかを集約したビューを取得
- ③ トレンド アプリケーション - QoE の低下や使用率の上昇などを示しているアプリの特定



An abstract graphic consisting of numerous thin lines radiating from a dark blue circular area in the top-left corner. The lines extend across the upper half of the slide, with colors ranging from light blue to white, and a few lines in orange, red, and green.

Powering Cisco SASE

SASEを成功へ導くために、Ciscoを選択する理由



#1 in SD-WAN マーケットシェア



最新のMASQUEおよびQUICプロトコルによる優れたパフォーマンス



業界最大のクラウド管理セキュリティおよびSD-WAN プラットフォーム



単一のクライアントに統合された ZTNA と VPNaaS により、シームレスなユーザー アクセス エクスペリエンスが実現します。



広範なパートナーエコシステム



最強の脅威インテリジェンスチーム“Talos”



既存の環境の大幅な変更や交換をすることなく実装できます



包括的な脅威の可視性と修復を実現するオープンで拡張性の高いCisco XDR



顧客所有ネットワークと非所有ネットワークの両方から毎日数十億の測定データを取得するエンドツーエンドの可視性

Cisco SASE: 顧客にとって重要な結果をもたらします



生産性の向上

- どこでもユニバーサルなユーザー エクスペリエンスを実現
- ハイブリッド ワークを強化
- IT 管理が簡単



コストの最適化

- 将来を見据えたインフラストラクチャによる俊敏性の向上
- ハードウェアの必要性を抑えながらコスト効率よく拡張
- 運用効率の向上



リスクを最小化する

- ネットワークの回復力の向上
- 分散環境全体にわたる継続的な可視性
- きめ細かなゼロトラスト セキュリティ

Cisco SASE 事例:電子製品製造のリーダー（台湾）

台湾の電子製品会社の製造サービスのリーダー。

世界中の拠点にCisco SD-WANを採用。

約300のサイトにCisco SD-WANを導入し、SSE(Cisco Secure)、Azure、AWS、GCPクラウドとの統合準備完了。

✓ 課題

- ✓ ネットワーク セキュリティを強化するには、Cloud Securityソリューションとの統合が必要
- ✓ パブリッククラウドへのワークロードの移行は、さまざまな国のユーザーニーズに対応するために必須
- ✓ オンプレミスのデータ センターを AWS IaaS に移行し、スケーラブルで簡単に導入できるクラウド ゲートウェイ ルーターを導入することが必須
- ✓ トラフィックパスの選択はプレフィックスのみに基づいており、リンクの品質は考慮されていない
- ✓ 規制要件を満たすには、さまざまな事業分野にわたるセグメンテーションが必要

➤ ソリューション

- ブランチとデータセンターにC8200、8300、C8500のSD-WANルーターを実装
- フェーズ 1: Catalyst SD-WANを国際的に展開
- フェーズ 2: 各国でローカルに実装してネットワークパフォーマンスを最適化
- アプリケーション認識ルーティングを使用して、リンクの品質に基づいてパスを選択
- Megaport SDCI の実装検討。複数のクラウドを使用しているため、将来的にこれを活用する可能性があります。

◆ 効果

- ◆ 国際間ネットワークの信頼性が向上
- ◆ クラウド接続の自動化を実現
- ◆ WANトラフィックパターンの視覚化が改善され、アプリケーションの最適化を実現
- ◆ トラブルシューティング時間を大幅に短縮
- ◆ クラウドへの最適なパスにより、全体的なユーザー エクスペリエンスが向上
- ◆ 一元管理により時間が節約され、より積極的なネットワーク・セキュリティポリシーの改善が実行可能

