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

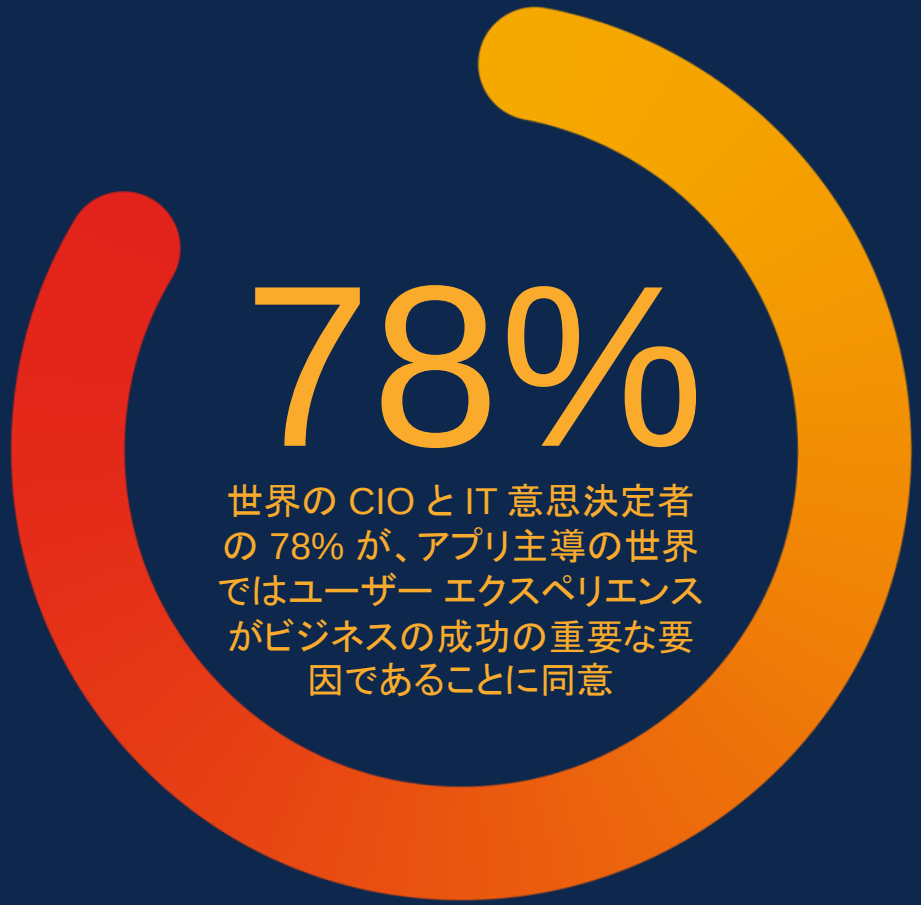
2025年5月21日

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。



ユーザエクスペリエンス
=快適性・安全性の向上

Future of Technology, Cisco

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

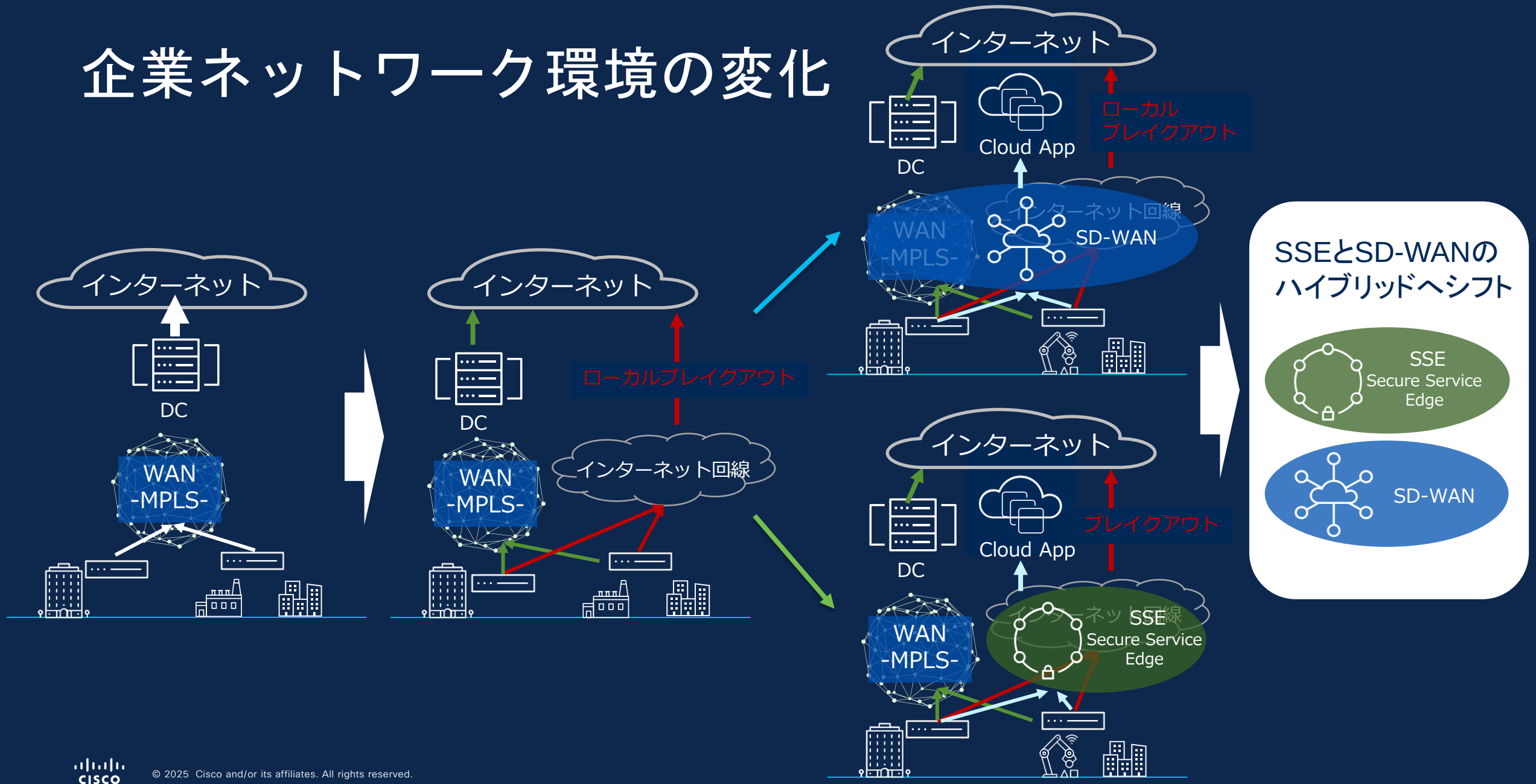
不十分な可視性とアプリ制御の欠如

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

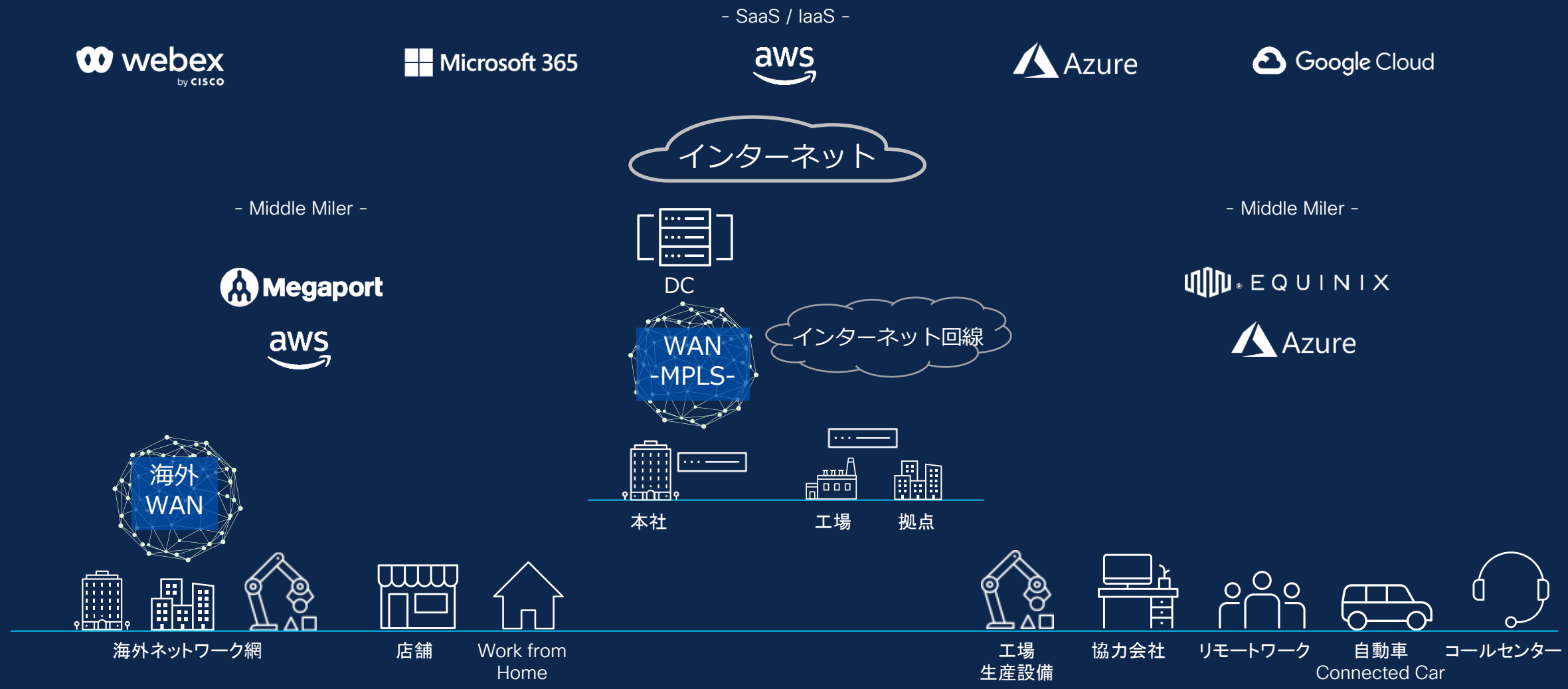
IT 部門はどのようにしてこれらの課題を克服し、
信頼できるエクスペリエンス(快適性・安全性の向上)を提供できるのでしょうか?

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



企業ネットワーク環境の変化



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？

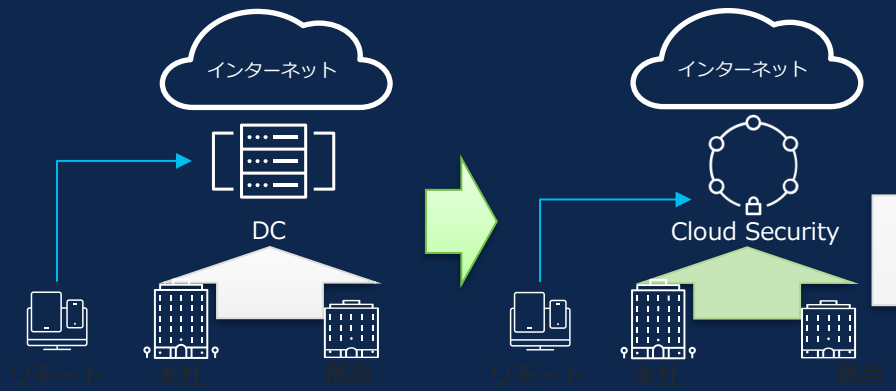
SASE成功に導くための検討・導入ポイント #1

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



一極集中による問題点

- ➢ トラフィック集中によるコスト増
- ➢ 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

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

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

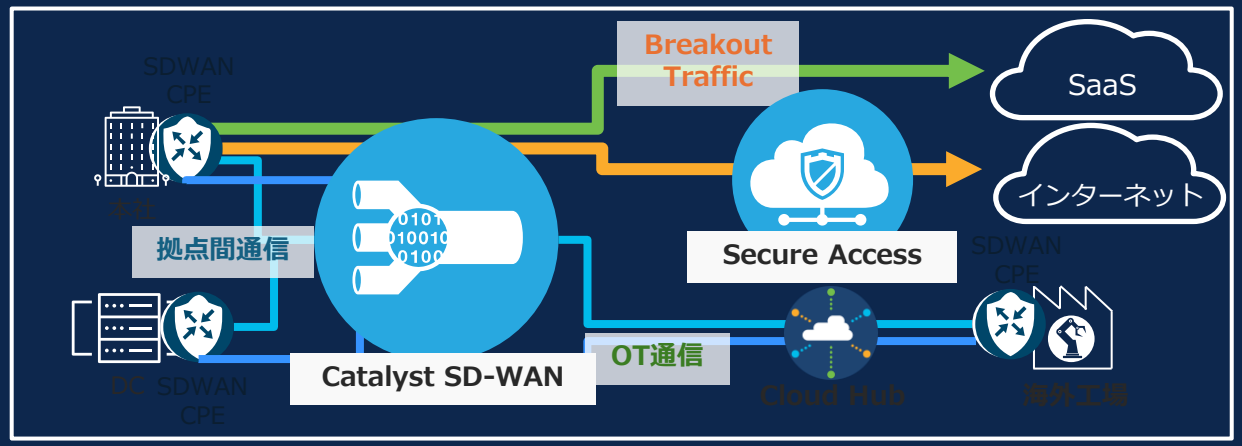
Cisco Secure Access特徴

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

Point

Cisco Catalyst SD-WANとは

https://www.cisco.com/site/jp/ja/solutions/networking/sdwan/index.html

Cisco Catalyst SD-WANとは、ソフトウェア定義型WAN (SD-WAN) ソリューションです。複数の回線（MPLS、インターネット、4G/LTEなど）を使い分け、アプリケーションの要件に応じて最適な回線を選択する、柔軟なWANネットワークを構築できます。これにより、ネットワークの運用効率を向上させ、コスト削減、セキュリティ強化、クラウド接続の最適化などが実現できます。

Cisco SD-WANの役割：

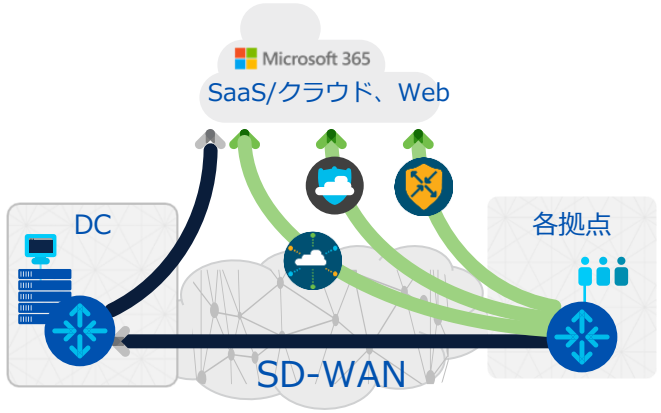
- **既存環境を踏襲したSD-WAN化**
- **WAN・RouterのSD化と可視化、自動化**
- **アプリケーションベースでのブレイクアウト（ファーストパケット問題も解消済み）**
- **クラウドセキュリティとの高い親和性 (Cisco Umbrella, Cisco Secure Access : SSE, zScaler)**
- WAN内の通信をトラフィック種別ごとにセグメンテーションを行い、拠点-DC間、拠点間、拠点-クラウドインフラ間、拠点-IaaS間をセキュアに繋ぐ
- **増加するIaaS/SaaSへの接続を行うためのアプリケーションの振り分け、最適経路の選択**
- クラウドインフラを提供するクラウドサービスプロバイダーとの連携により、SDCI(Software-Defined Cloud Interconnect)を、さまざまな業種業態に提供

Point

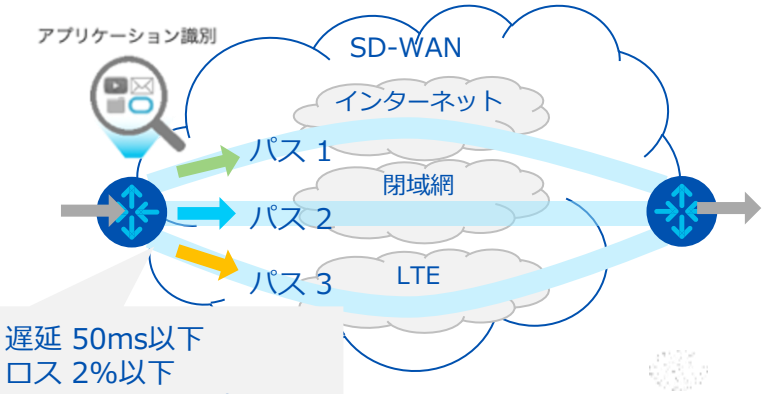
Cisco Catalyst SD-WAN　ユースケース

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



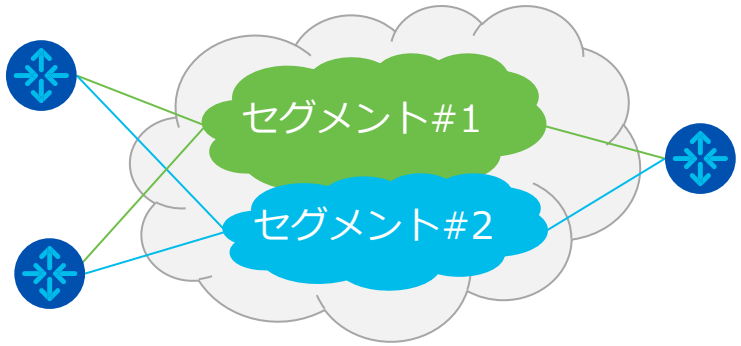
WAN利用の最適化



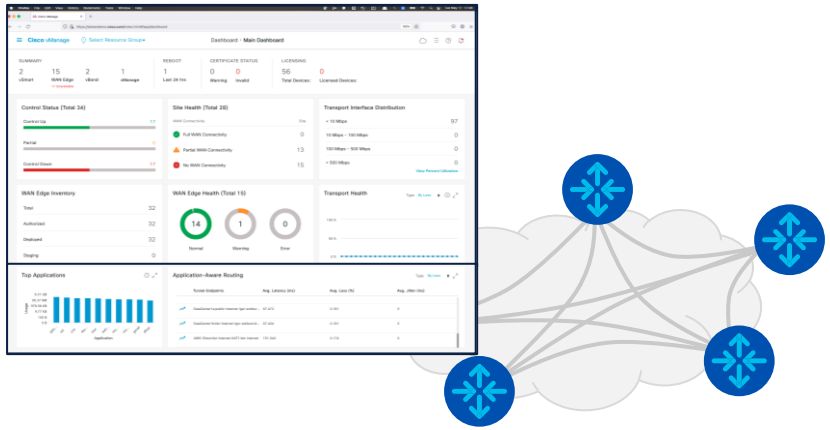
- 遅延 50ms以下
- ロス 2%以下
- ジッター 10ms以下

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

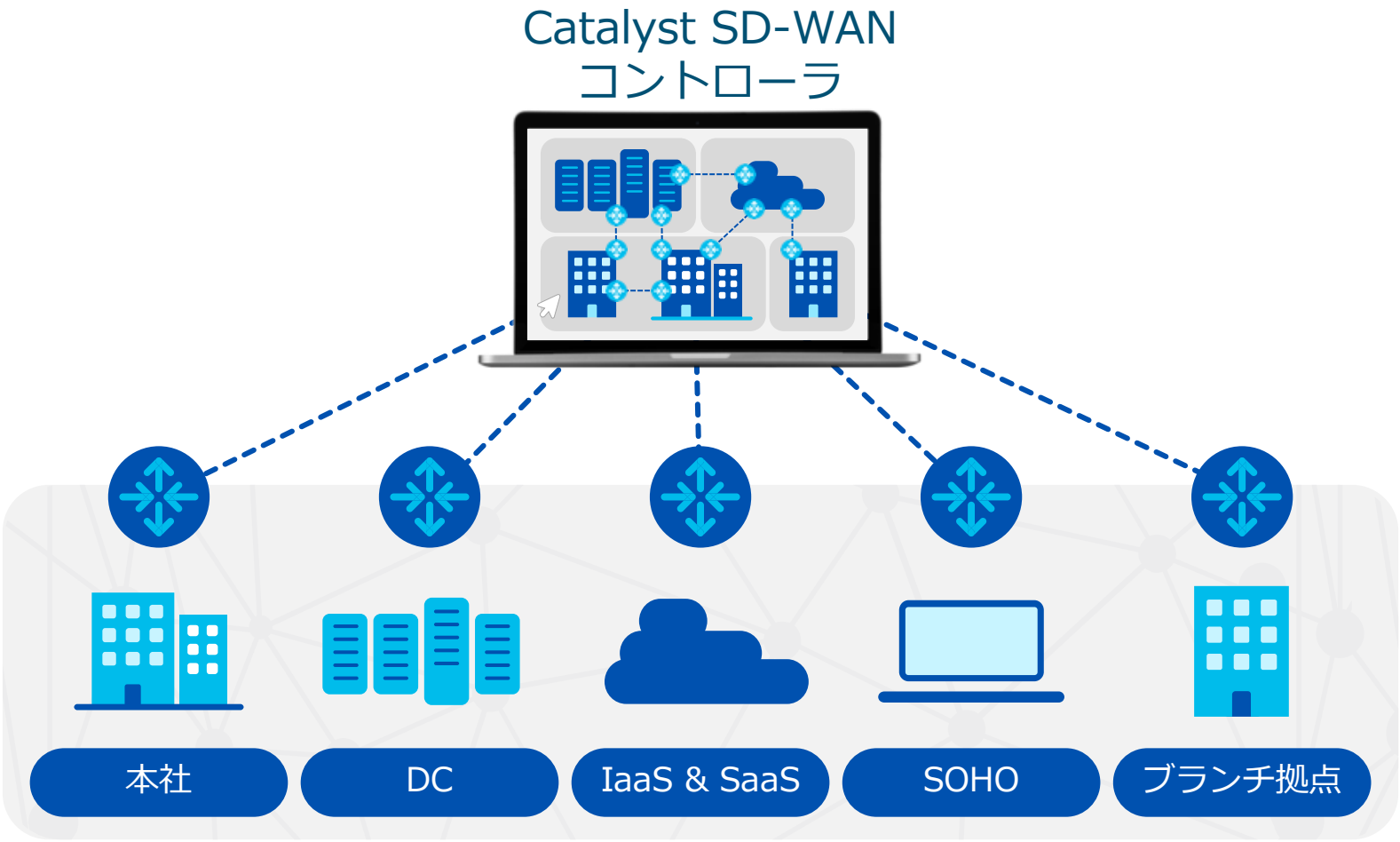


ゼロタッチプロビジョニング

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！

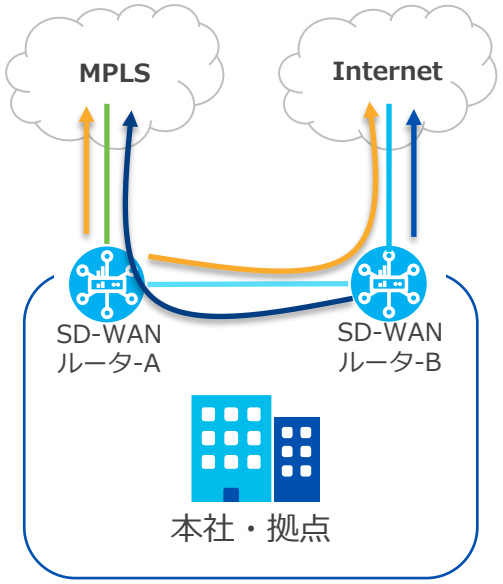
Point

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



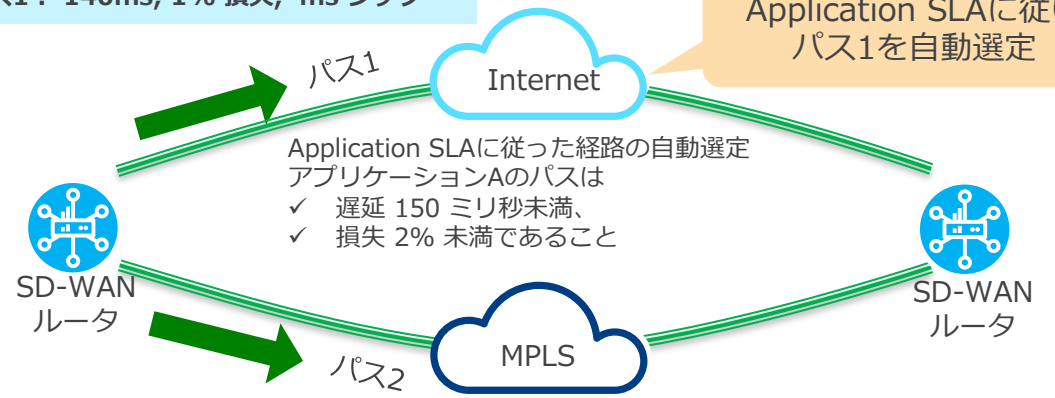
SD-WANルータは、それぞれ対応する回線にのみ接続されている状態の場合

- 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



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

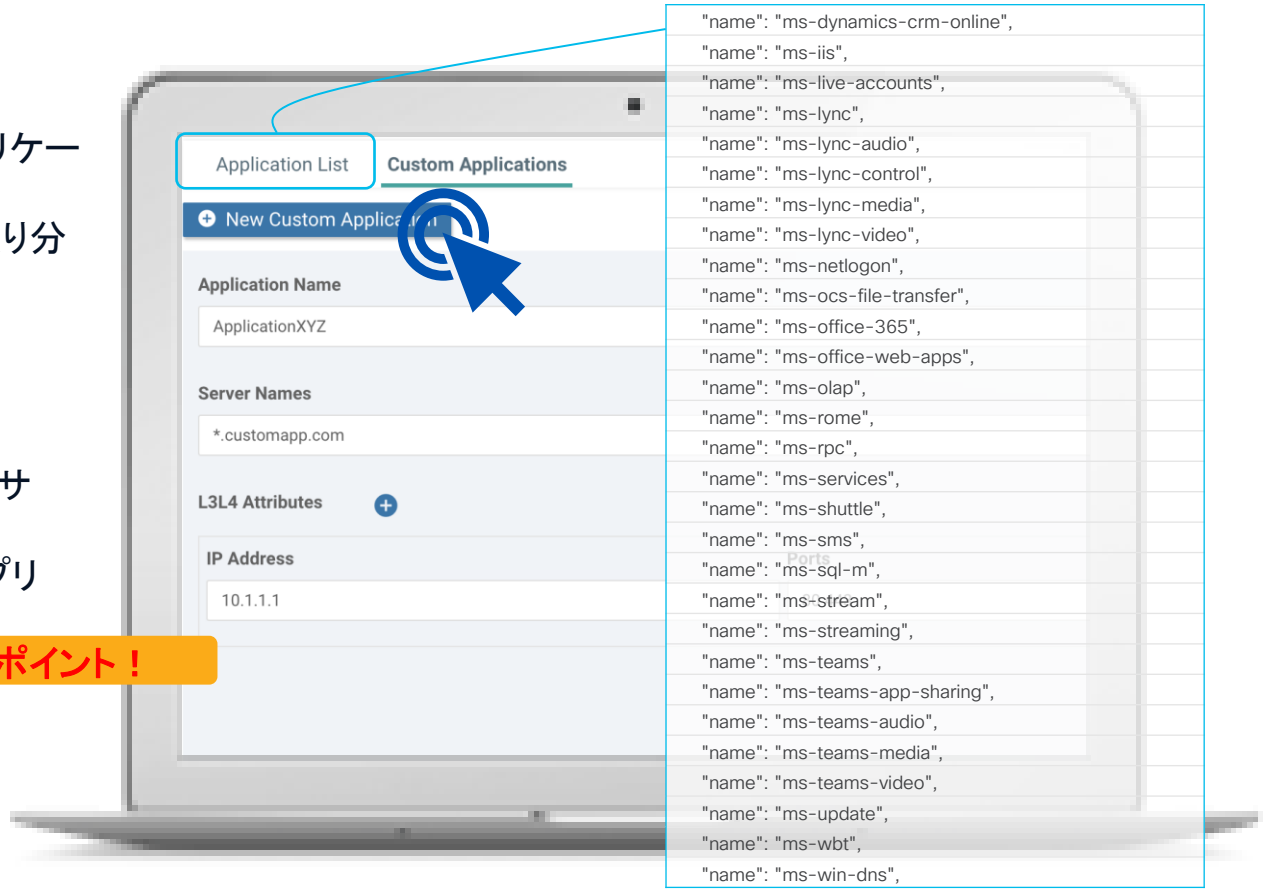
業務アプリケーションの通信を最優先すべきところ、優先度の低いアプリケーションが利用可能な帯域を占有し、業務に支障が出ることがあります。
アプリケーションを的確に識別し、制御することで、アプリケーションの振り分け、ブレイクアウト、利用制限などが可能となります。

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　**ここがポイント！**

ファーストパケット問題対策　**ここがポイント！**

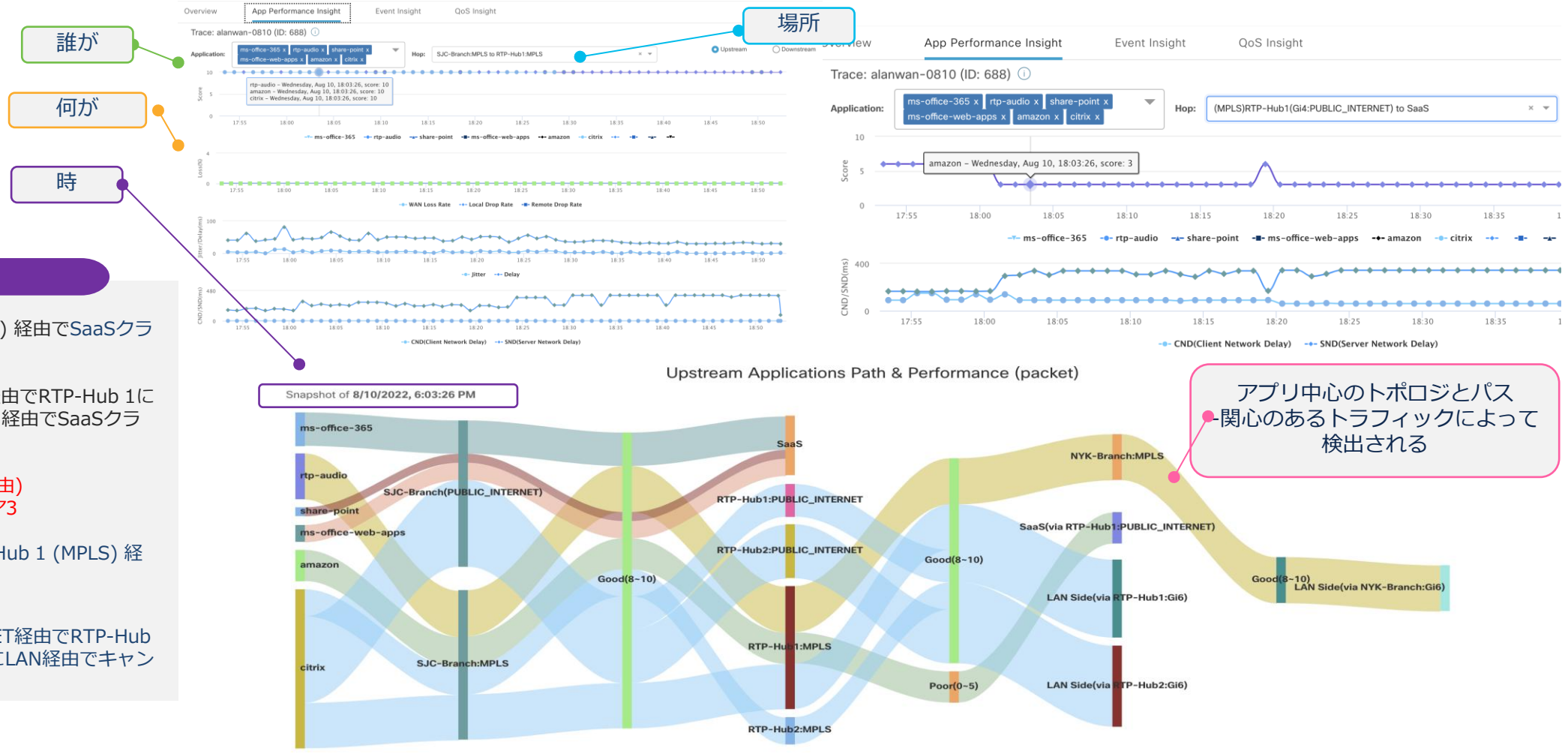


社内開発のアプリケーションやあまり一般的でないアプリケーションを認識し、これらのトラフィックに対してアクションを実行し、アプリケーション制御・ブレイクアウト・監視など、トラフィックポリシー定義が可能となっています。

Point

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



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

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ークアウト。

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。

Point

Cisco DNA Advantage

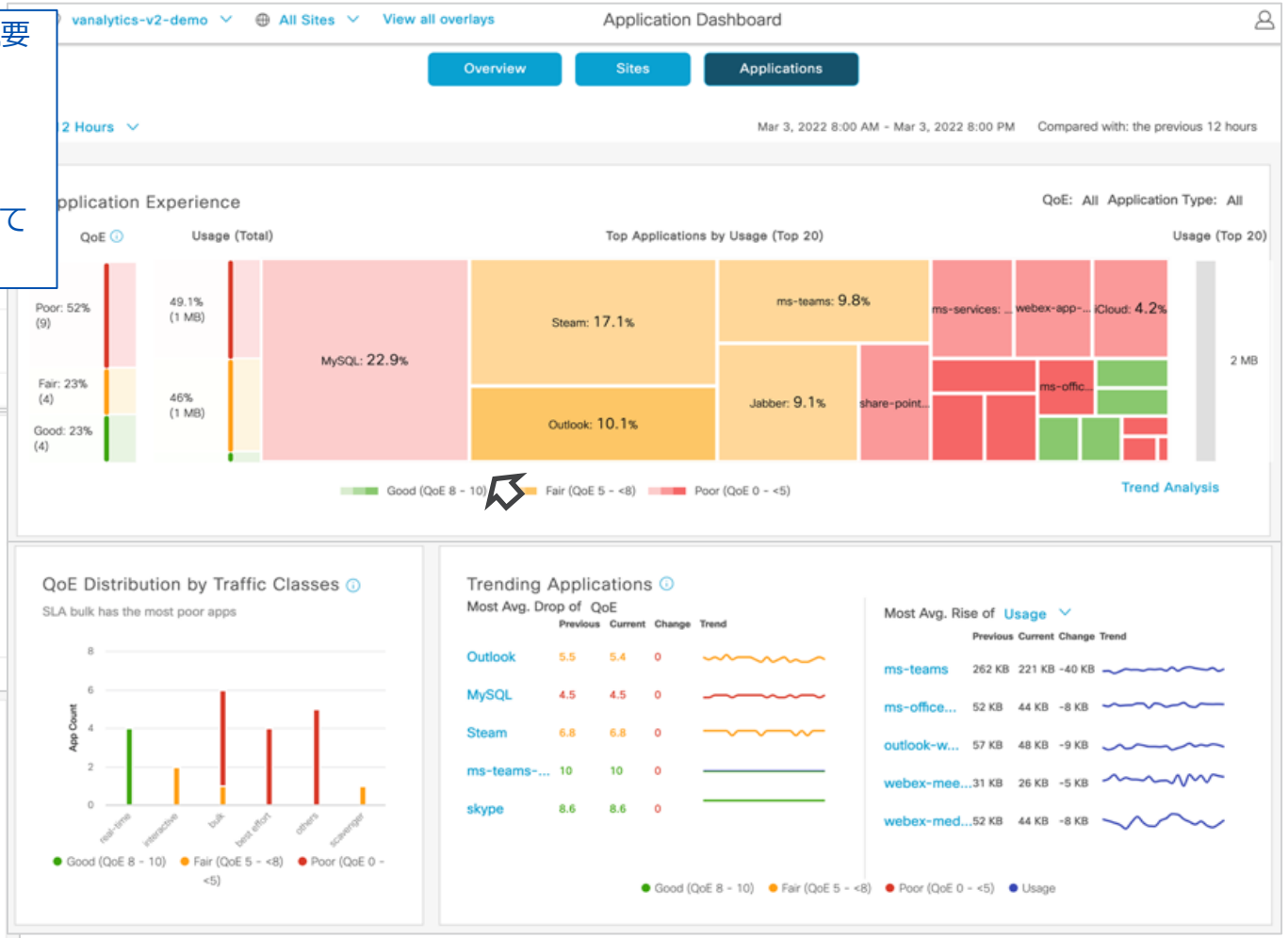
SD-WAN導入後の効果測定が可能な分析機能:vAnalytics

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

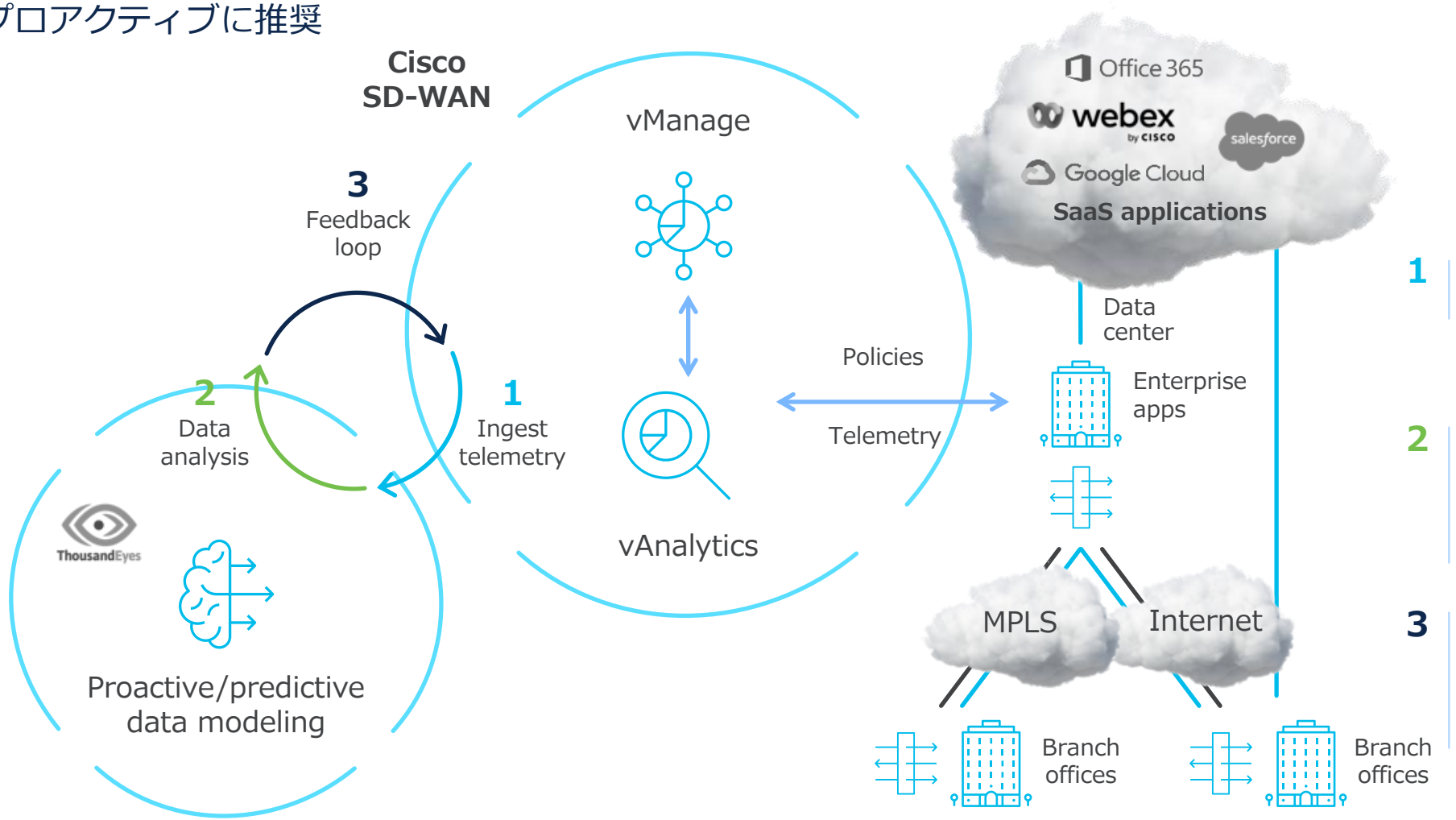
③ トレンド アプリケーション - QoE の低下や使用率の上昇などを示しているアプリの特定



Cisco DNA Advantage

ネットワークのナビゲーションシステム “WAN Insights”

Cisco Catalyst SD-WAN & vAnalytics + ThousandEyes “WAN Insights”
過去 30 日間のネットワーク パスのパフォーマンスを監視し、問題を予測して、アプリケーション ネットワーク パスをプロアクティブに推奨



ThousandEyes

1 vAnalytics を介して Thousand Eyesよりネットワーク テレメトリ データを収集する

2 テレメトリ データ (過去 30 日間) を分析して、アプリの最適なパスに関するプロアクティブな洞察を生成します

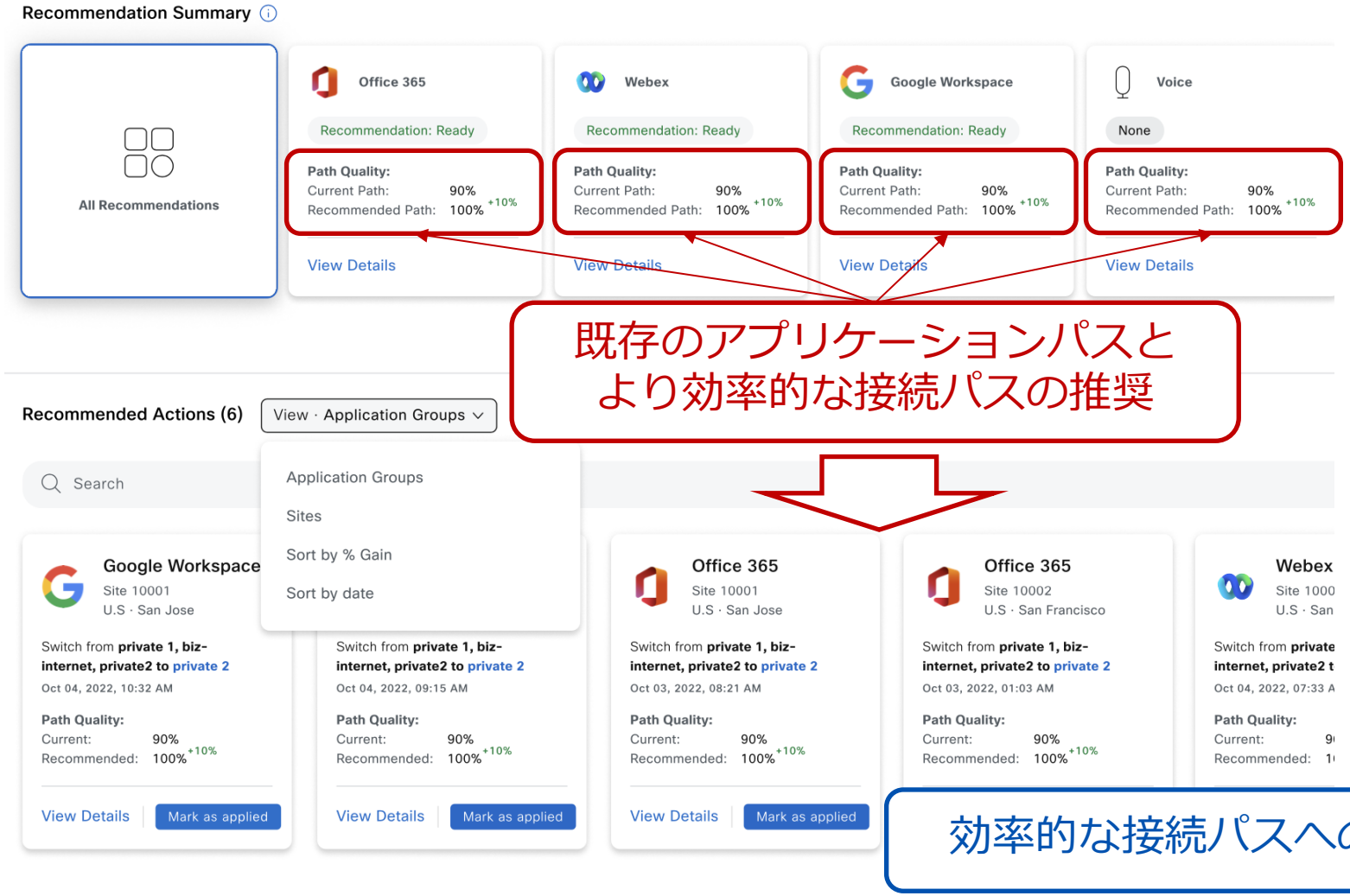
3 ポリシーを更新してアプリのエクスペリエンスを最適化するためのフィードバック ループ (最初は手動、将来的には自動化)

Point

Cisco DNA Advantage

ネットワークのナビゲーションシステム “WAN Insights”

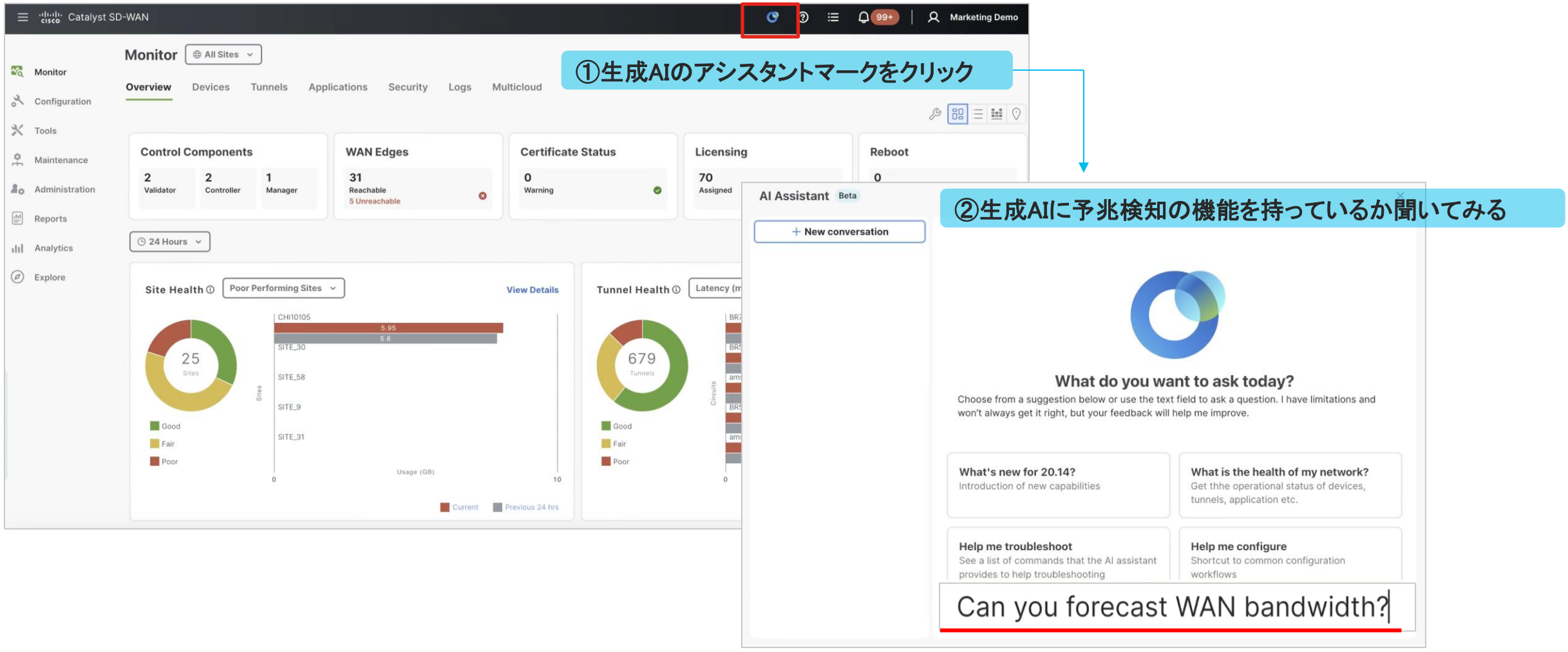
Cisco WAN Insightsは、リアルタイムのパフォーマンスデータとトレンドを提供します。これにより、管理者はネットワークの問題を迅速に特定し、解決することができます。



1. アプリケーション
2. カテゴリ現在のパフォーマンス
3. 予測のパフォーマンス
4. 品質改善
5. 推奨パス
6. 自動改善の実行

Point

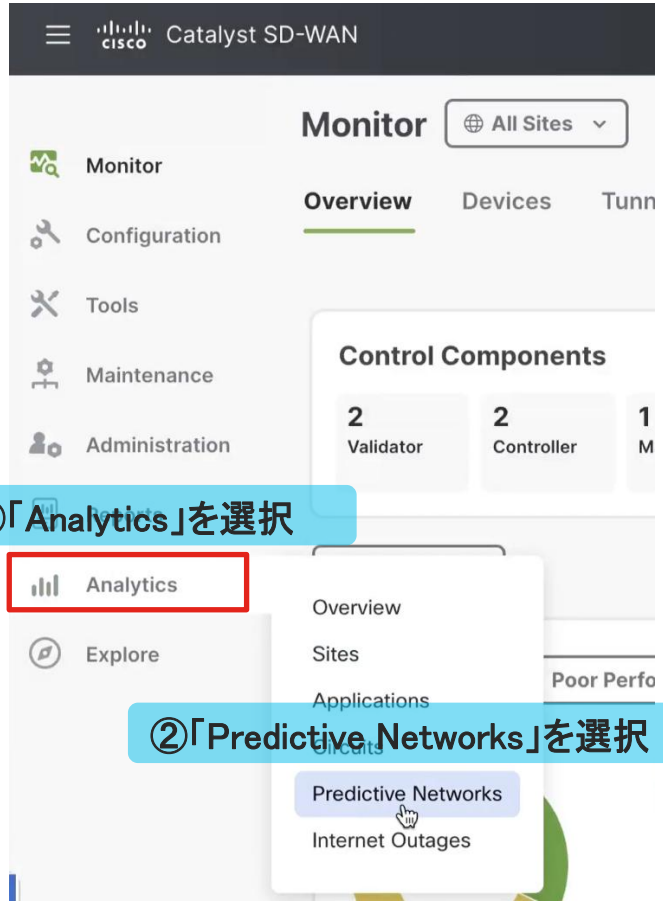
トラブルが発生する前に予兆を検知し、予防措置を取りたい（AIアシスタント）



Point

Cisco DNA Advantage

トラブルが発生する前に予兆を検知し、予防措置を取りたい（Predictive Path Recommendation）



O365において今の設定だと82.8%の品質だが、Pathを変更すると99.4%の品質に向上（16.56%改善）することが記載されている

Point

Cisco DNA Advantage

トラブルが発生する前に予兆を検知し、予防措置を取りたい（ Predictive Path Recommendation ）

現状のPathの品質を表示

推奨Pathの品質を表示

現状のPathと推奨Pathの表示
こちらを見て切り替えを判断する

推奨通りの経路変更も専門知識必要なく、Applyを押すだけ
※通信が途切れるので通信が少ない時間などに切り替えるのが良い

All sites

Search Table

Site	Location	Current path	Recommended path	Current path quality	Recommended path quality	% Gain	Impacted clients	Action
90	United States · Hutchinson	--	--	100.0%	100.0%	0.00%	1	--
10105	United States · West Town	mpls, public-internet	mpls	88.2%	99.0%	10.83%	20	Apply
10010	United States · Hutchinson	--	--	86.8%	86.8%	0.00%	1	--
10021	United States · Unknown	public-internet	mpls	77.5%	99.3%	21.80%	20	Apply

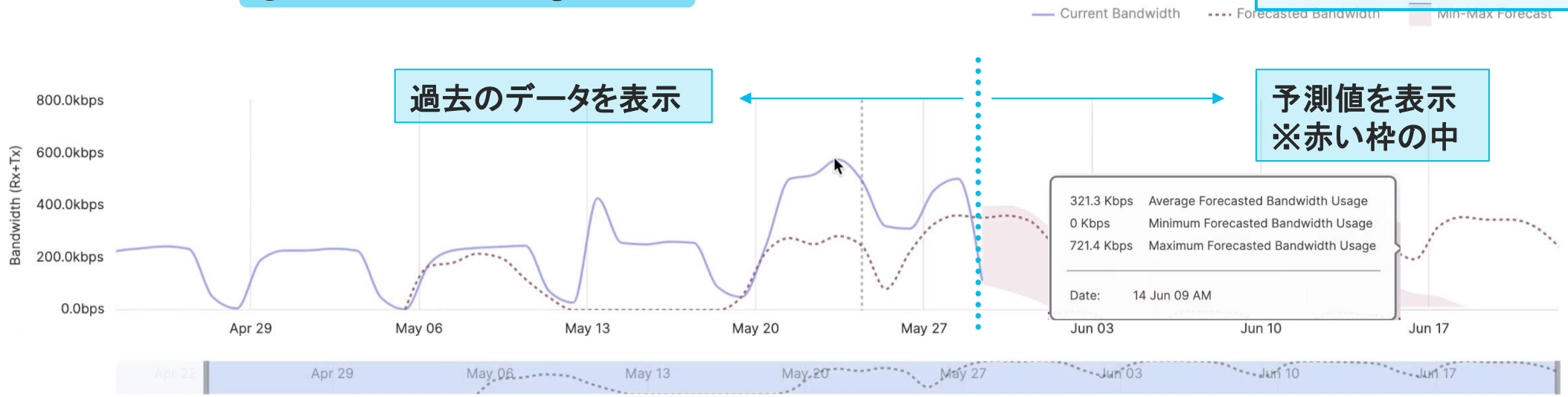
Cisco DNA Advantage

トラブルが発生する前に予兆を検知し、予防措置を取りたい（Bandwidth Forecasting）

Predictive Path Recommendations | Bandwidth Forecasting Beta

①「Bandwidth Forecasting」を選択

この予測値により、増強かコストカットか、等を決めていく指標にすることができ、効率よく管理/投資が可能



	Circuit Name	Service Provider	Site ID	Site Location	RX + TX	RX	TX	RX Utilization (%)	TX Utilization (%)
◉	DC2b:public-internet	cisco systems inc.	10021	san jose	615 Kbps	551 Kbps	64 Kbps	-	-
○	BR4-C8200:public-internet	cisco systems inc.	10104	los angeles	578 Kbps	513 Kbps	65 Kbps	-	-
○	BR5:public-internet	cisco systems inc.	10105	chicago	445 Kbps	399 Kbps	46 Kbps	-	-
○	DC2a:mpls	?	10021	milpitas	273 Kbps	254 Kbps	19 Kbps	-	-
○	BR5:mpls	?	10105	chicago	271 Kbps	236 Kbps	35 Kbps	-	-

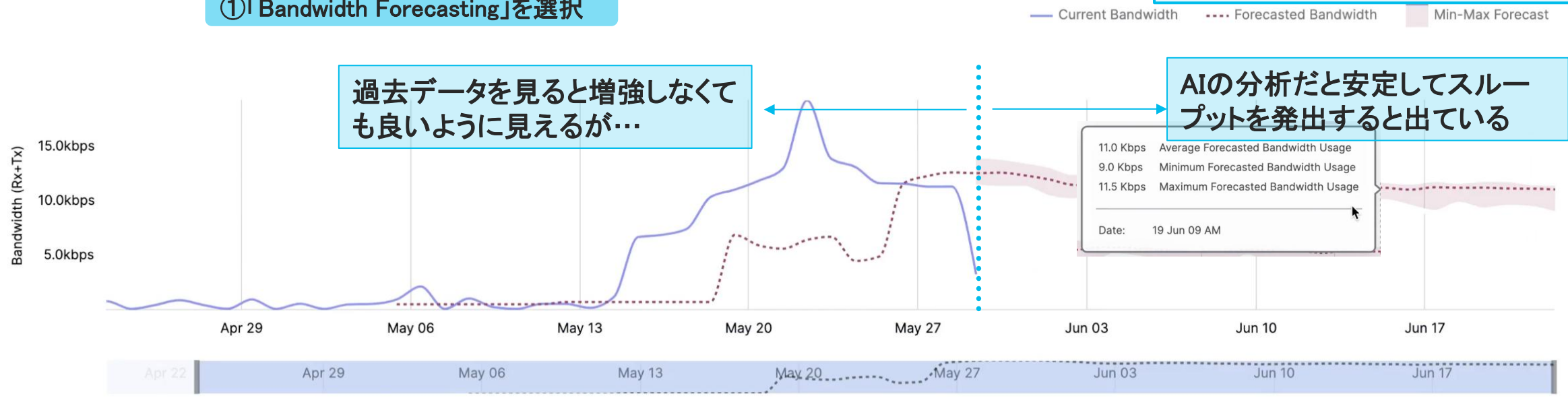
DC2bのデータを表示

Cisco DNA Advantage

AIの活用により、過去データだけでなく分析結果も判断基準とすることができ、誰でも詳細な分析が可能

トラブルが発生する前に予兆を検知し、予防措置を取りたい（Bandwidth Forecasting）

①「Bandwidth Forecasting」を選択



	Circuit Name	Service Provider	Site ID	Site Location	RX + TX	RX	TX	RX Utilization (%)	TX Utilization (%)
○	BR5:mpls	?	10105	chicago	271 Kbps	236 Kbps	35 Kbps	-	-
○	DC2a:public-internet	cisco systems inc.	10021	milpitas	181 Kbps	174 Kbps	7 Kbps	-	-
○	DC2b:mpls	?	10021	san jose	172 Kbps	158 Kbps	14 Kbps	-	-
◉	BR3-C1111X-8P:public-internet	cisco systems inc.	10103	new york	13 Kbps	5 Kbps	8 Kbps	-	-

BR3（支店）のデータを表示

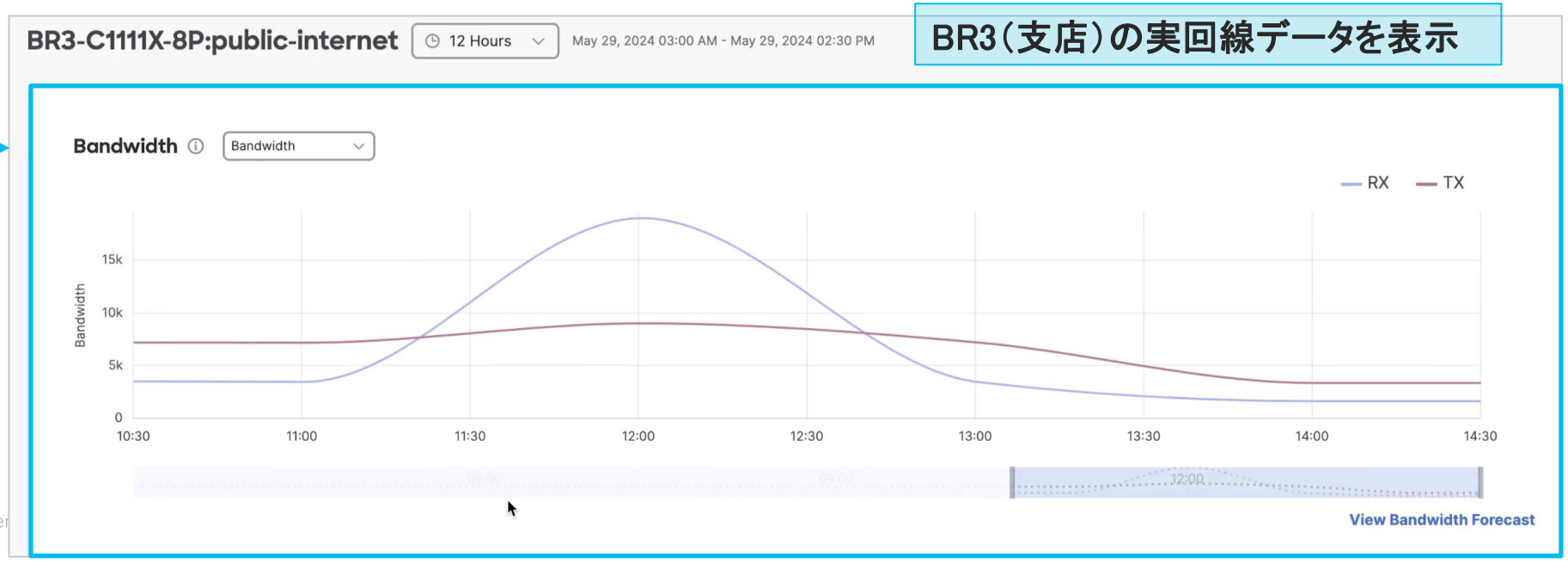
Cisco DNA Advantage

トラブルが発生する前に予兆を検知し、予防措置を取りたい（Bandwidth Forecasting）

	Circuit Name	Service Provider	Site ID	Site Location	RX + TX	RX	TX	RX Utilization (%)	TX Utilization (%)
○	BR5:mpls	?	10105	chicago	271 Kbps	236 Kbps	35 Kbps	-	-
○	DC2a:public-internet	cisco systems inc.	10021	milpitas	181 Kbps	174 Kbps	7 Kbps	-	-
○	DC2b:mpls	?	10021	san jose	172 Kbps	158 Kbps	14 Kbps	-	-
◉	BR3-C1111X-8P:public-internet	cisco systems inc.	10103	new york	13 Kbps	5 Kbps	8 Kbps	-	-

①「BR3」をクリック

BR3（支店）の実回線データを表示



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
- 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
- 広範なパートナーエコシステム
- 既存の環境の大幅な改変や交換をすることなく実装できます
- 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
- 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。
- 最強の脅威インテリジェンスチーム“Talos”
- 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


CISCO