



NXTWORK[®]2019

WAN/LANおよび有線/無線の統合・
一元管理を可能にする
「SD-ENTERPRISE」最新事情

ジュニパーネットワークス株式会社

エンタープライズ技術本部

渡邊 貴之

自己紹介

- 名前
 - 渡邊 貴之
- 所属
 - ジュニパーネットワークス株式会社
 - エンタープライズ技術第一本部
- 主な活動
 - エンタープライズマーケットに対してネットワークコンサル
 - Interop Tokyo
 - ShowNet NOCメンバ ジェネラリスト
 - <https://www.interop.jp/shownet/noc/>
 - NICT(国立研究開発法人 情報通信研究機構)
 - JGN 特別研究員
 - JPNIC
 - IPv4枯渇タスクフォース
 - AITAC(一般社団法人 高度ITアーキテクト育成協議会)
 - プログラム委員
 - IoT時代のITインフラの運用・管理を担う人材の育成に寄与することを目的としています。
 - <https://aitac.jp/about/>



AGENDA

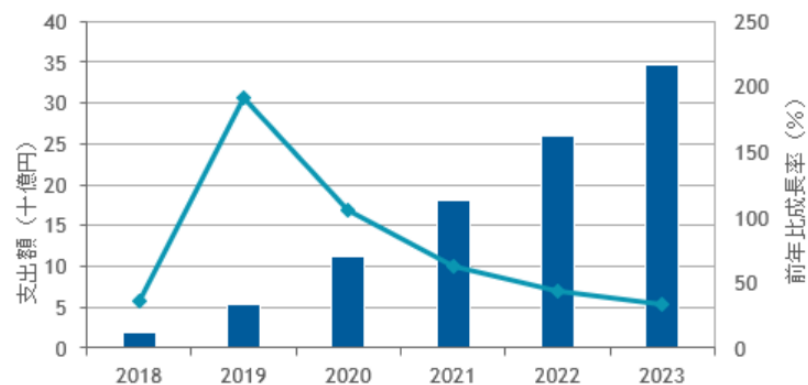
- いまさら聞けるSD-WAN
- SD-WANの現状
- SD-WANその先へ

SD-WANのマーケット状況

国内SD-WAN市場、2018年～2023年の年間平均成長率79.5%で
市場規模は2018年の18倍以上に——IDC予測

**2019年は前年比成長率191.1%で、前年の18億6,100
万円から54億1,800万円に**

IDCの調査によると、2023年には346億7,200万円（2018年～2023年の5年間における年間平均成長率79.5%）に達する。SD-WAN市場は、2019年に揺籃期から成長期に移行しつつある。SD-WAN製品や市場は、現段階ではまだ発展途上だが、今後徐々に成熟し、長期的にはSD-WAN技術は市場に広く普及するとIDCでは予測している。



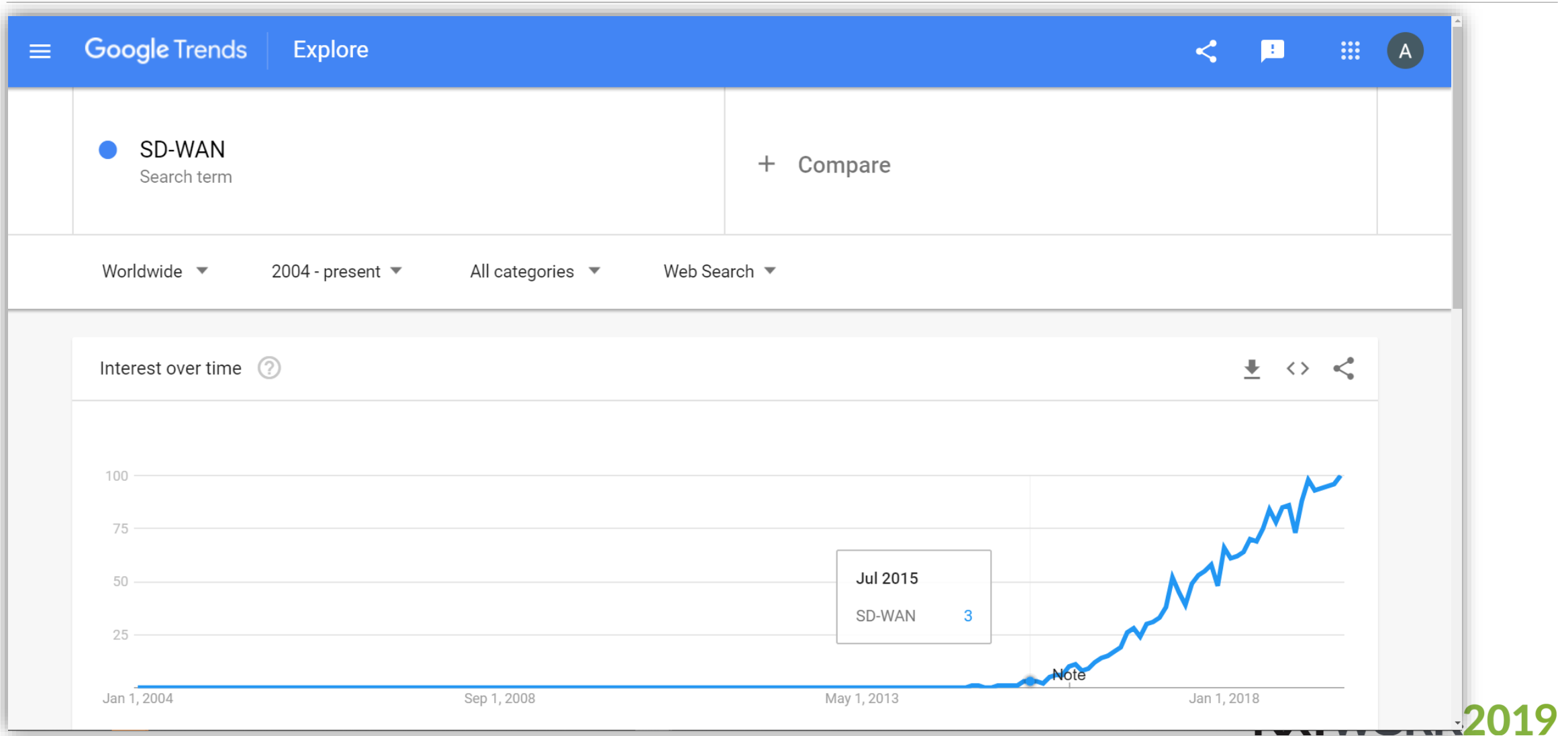
2019年に揺籃期から成長期に移行しつつある

<https://enterprisezine.jp/article/detail/12190>

参考資料：国内SD-WAN市場 ユーザー支出額予測、2018年～2023年（作成：IDC Japan）

NXTWORK.2019

GOOGLEトレンド

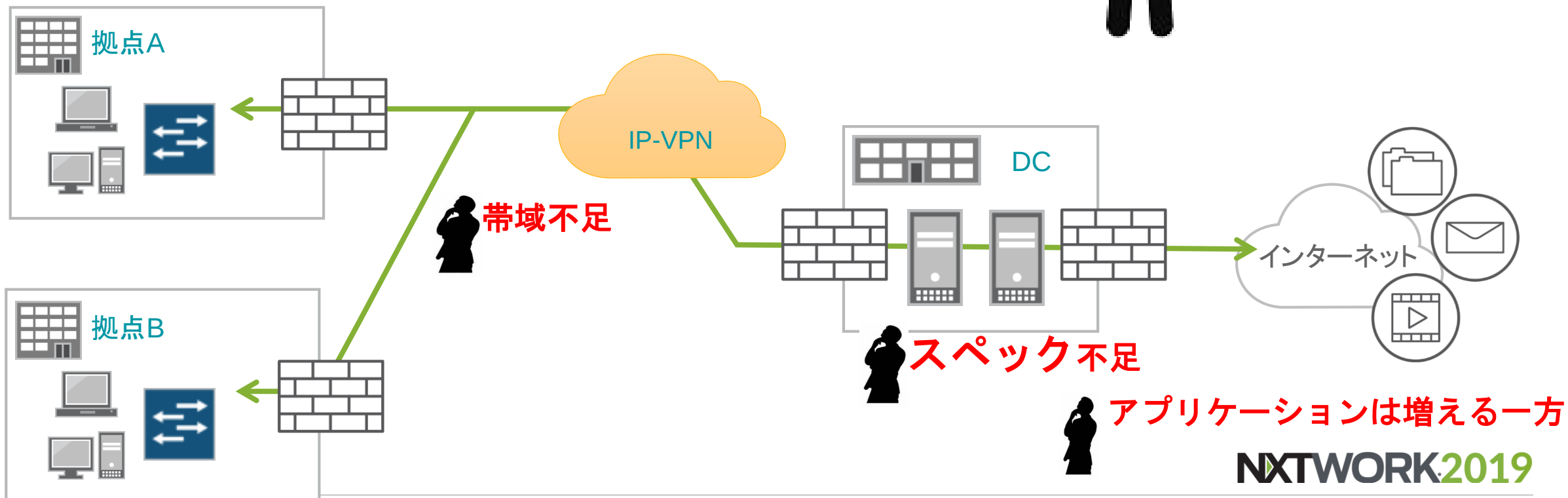


クラウドサービスの普及と課題

メールやアプリケーションサーバをクラウドに移行すると

ネットワークの帯域やFWへかかる負荷が増大

プロキシサーバを経由する場合はプロキシサーバの負荷が増大



ZTPによる機器展開のメリット（スケジュールとコスト）

※実際の数値は条件位により異なりますので参考比較情報とお考え下さい

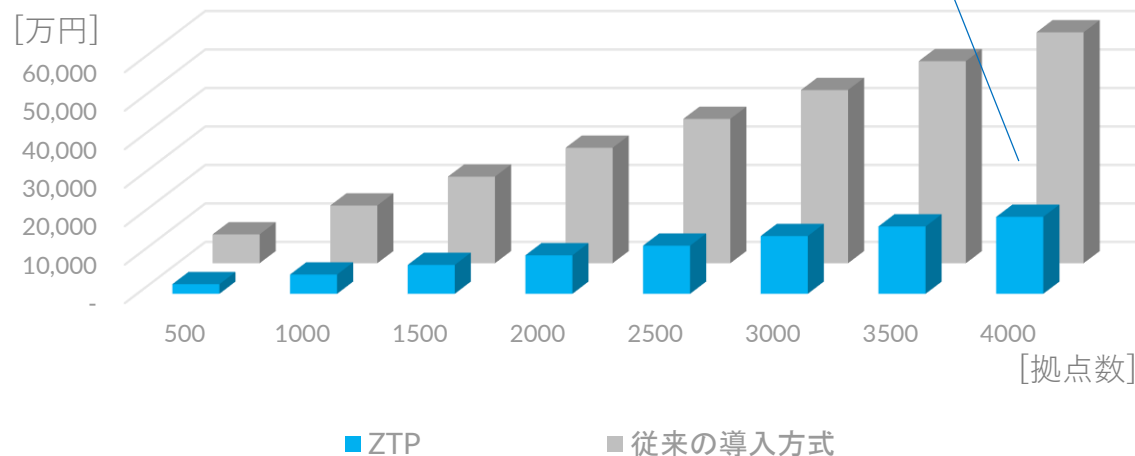
ZTPによる導入時と従来の現地による作業及び正常性確認作業によるマニュアル作業の概要比較となります。

【比較条件】

- 導入コスト： ZTPは1拠点辺り5万円／従来導入方式で15万円（最小限の工事とセンターオペレーションの自動化）
- 導入スピード： ZTPは1日30拠点／従来導入方式で1日10拠点（センター側の対応も増えるため）

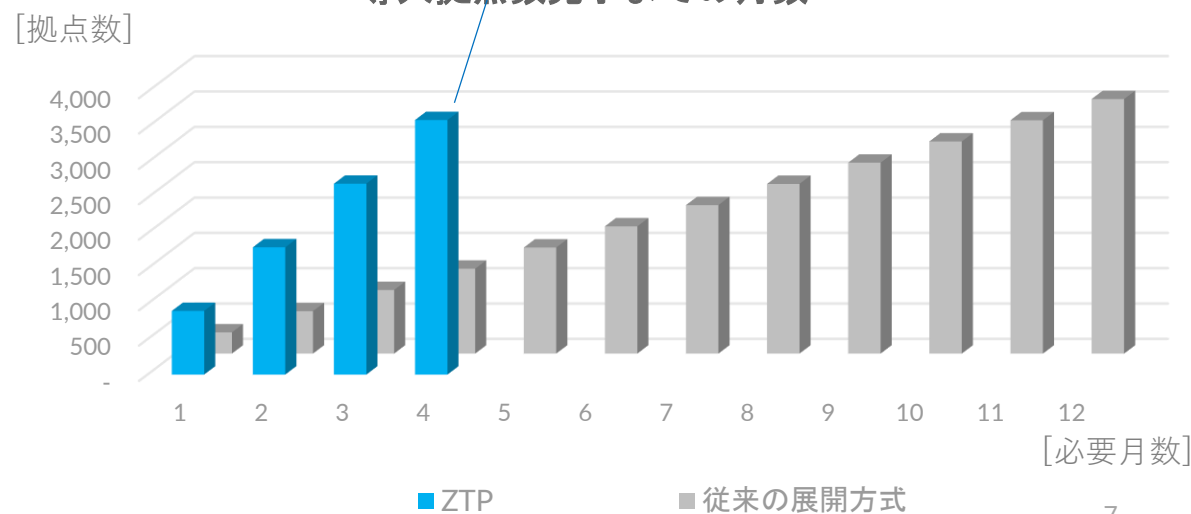
2億円のコスト削減

導入作業コスト比較

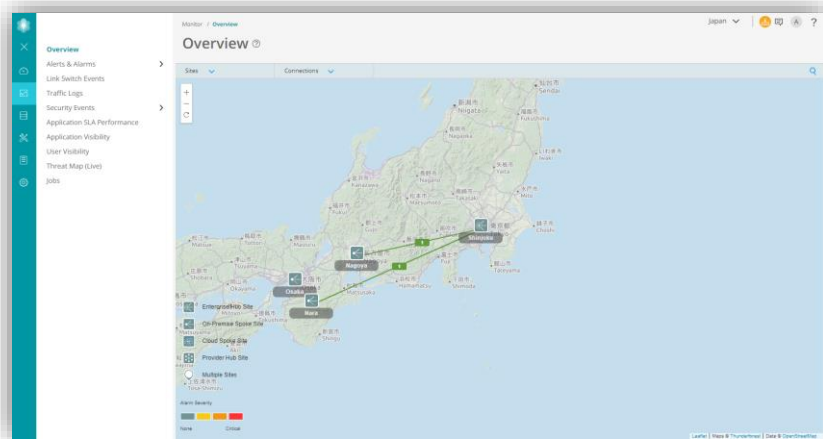


8ヶ月の導入期間短縮

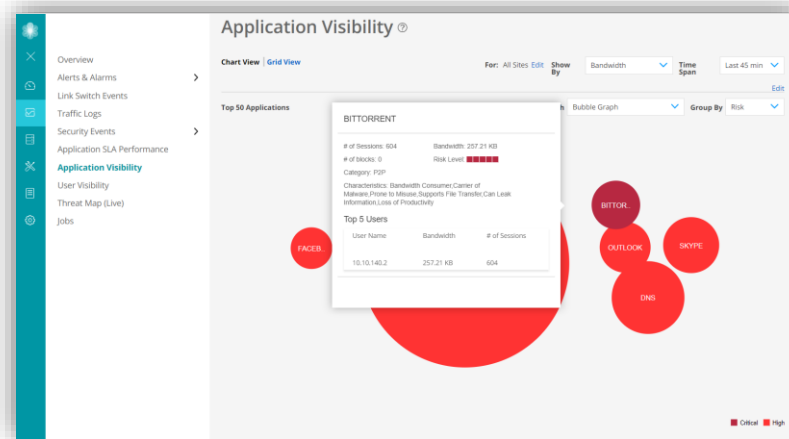
導入拠点数完了までの月数



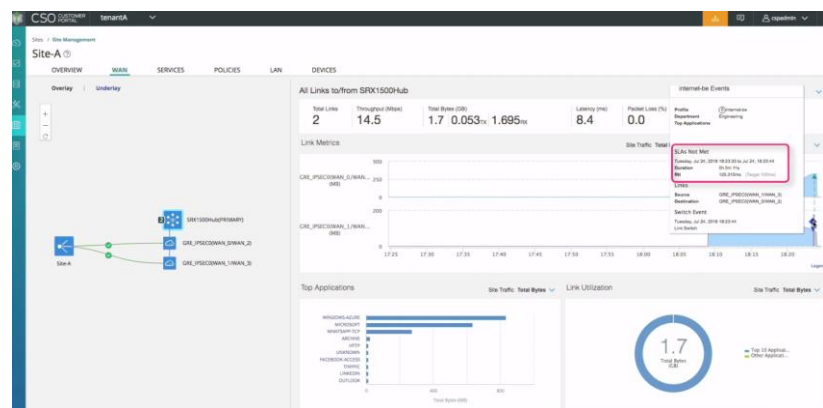
見やすい管理画面とレポート



VPNダッシュボード

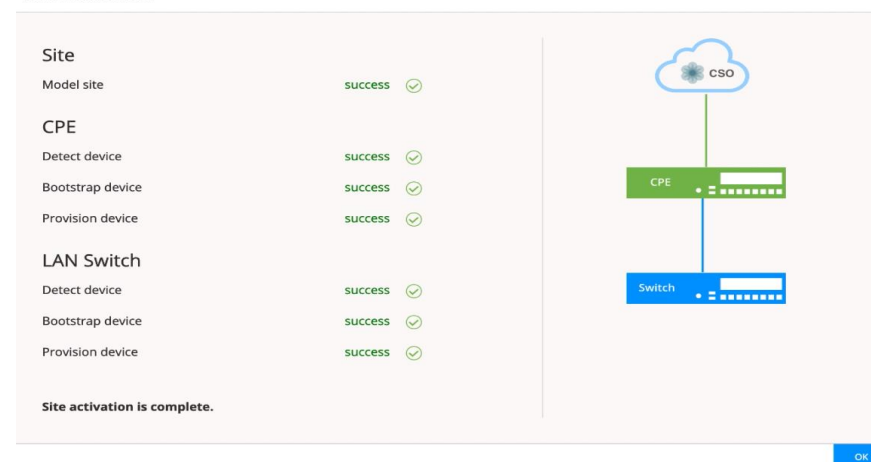


アプリケーションダッシュボード



回線モニタリング等

Site Activation

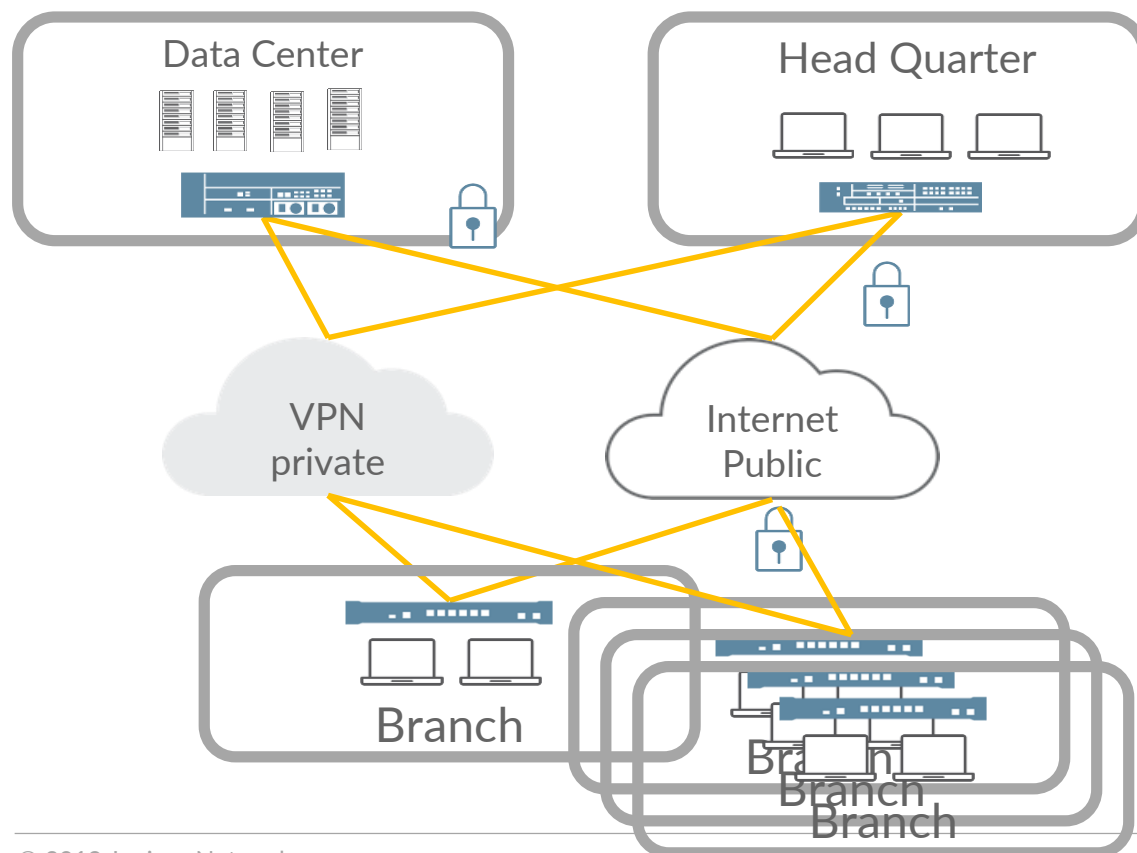


構成情報ダッシュボード

NXTWORK.2019

SD-WANの基本構成

SD-WAN



クラウドサービスの台頭

- O365、AWS、GCPなどなど

自動化へのシフト

- IT人材の不足
- 迅速なサービスへの対応

WAN回線のコスト

- Public回線の活用



- SD-WANによって次のような効果が期待できる。

- ZTPによる導入コストの軽減
- 運用管理コストの削減
- WAN回線のコスト削減
- アプリケーションの可視化と制御

NXTWORK2019

ONUG SD-WAN評価

No	評価項目	○ ×	ジュニパーネットワークス
1	Active／Active構成で様々な回線・WANの制御が可能なこと	○	Public WAN, Private WANのマルチホーミング(Active/Active)での利用ができます。
2	コモディティHW上で、仮想的にCPEを提供できること	○	vSRX（バーチャルSRX)にてSRXの機能を仮想マシン形式のCPEとしてご利用いただけます。 vNFXはのサポートは来年の予定です。
3	アプリケーション等のポリシーに基づき、ダイナミック制御が可能なこと	○	SRX、NFXのAppRoute（APBR）にてアプリケーションベースのダイナミックな制御が可能です。
4	個別のアプリに対して、可視化・優先順位付け、ステアリングが可能なこと	○	アプリケーションの可視化、アプリケーションベースでの優先制御(QoS)が可能です。
5	可用性・柔軟性の高いハイブリッドなWANの構築が可能なこと	○	複数のPrivate WAN, Public WANでの構成が可能で回線障害時も動的に切り替えが可能です。
6	L2／L3に対応	○	SRX、NFXはL2/L3に対応します。
7	拠点、アプリケーション、VPN品質等をダッシュボードでレポートができること	○	CSOでは各種ダッシュボード機能、パフォーマンスレポートの機能を備えております。
8	オープンなノースバウンドAPIを持ちコントローラーへのアクセスや制御ができること	○	REST APIをはじめ各種スクリプトを提供、資料を公開しています。 https://www.juniper.net/documentation/product/en_US/contrail-service-orchestration
9	ゼロタッチプロビジョニングに対応すること	○	SRX、NFXはZTP(ゼロタッチプロビジョニング)に対応しております。 NFXはvSRX（バーチャルSRX)を標準搭載します。
10	FIPS-140-2(セキュリティ)を取得できること	○	SRX、NFX250およびJunosはFIPS-140-2に対応しています。 https://www.juniper.net/documentation/en_US/junos/topics/reference/general/junos-fips-software-editions.html https://www.juniper.net/documentation/en_US/junos-fips12.1/topics/concept/understanding-junos-fips-mode.html https://www.juniper.net/documentation/en_US/junos-fips12.1/information-products/pathway-pages/security/security-fips-guide-12.1x46-d40.pdf https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/3288

– SD-WANの現状

クラウドサービスの普及と課題

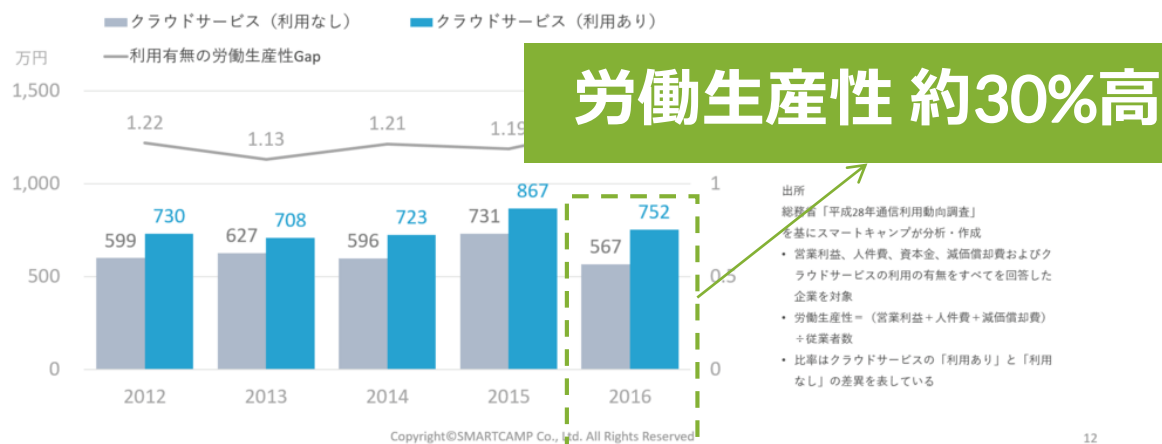
クラウドサービスの利用で労働生産性は向上
SaaS利用が急速に拡大している

日本でも

クラウドサービスの利用による1社あたり労働生産性の向上

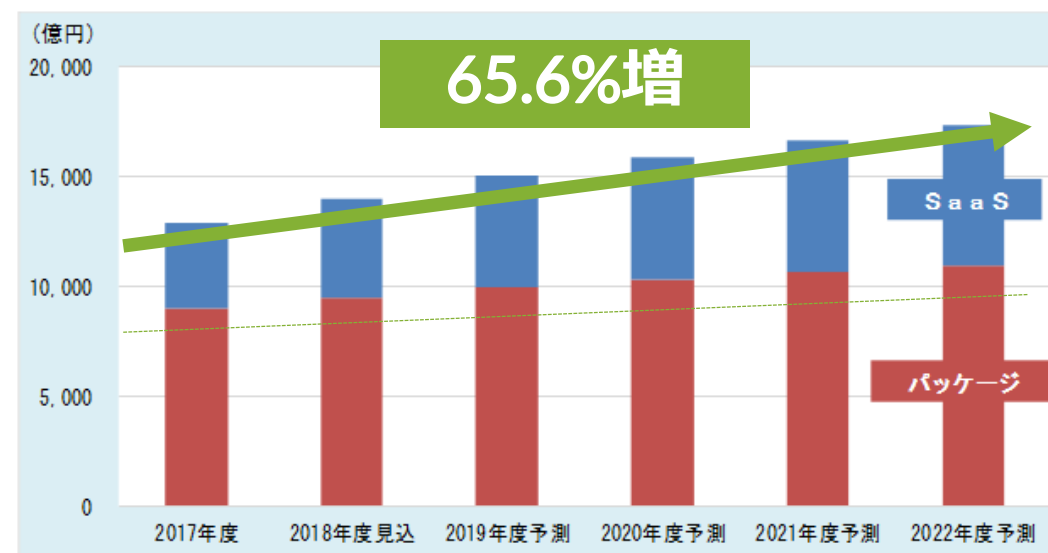
SaaS
Software as a Service

クラウドサービスを利用することで生産性向上を実現することが可能。
クラウドサービスを利用している企業は、利用していない企業に比べて労働生産性が約30%も高い。



Source : Smartcamp Co, Ltd <https://boxil.jp/mag/a5170/>

ソフトウェアの国内市場（パッケージ／SaaS）



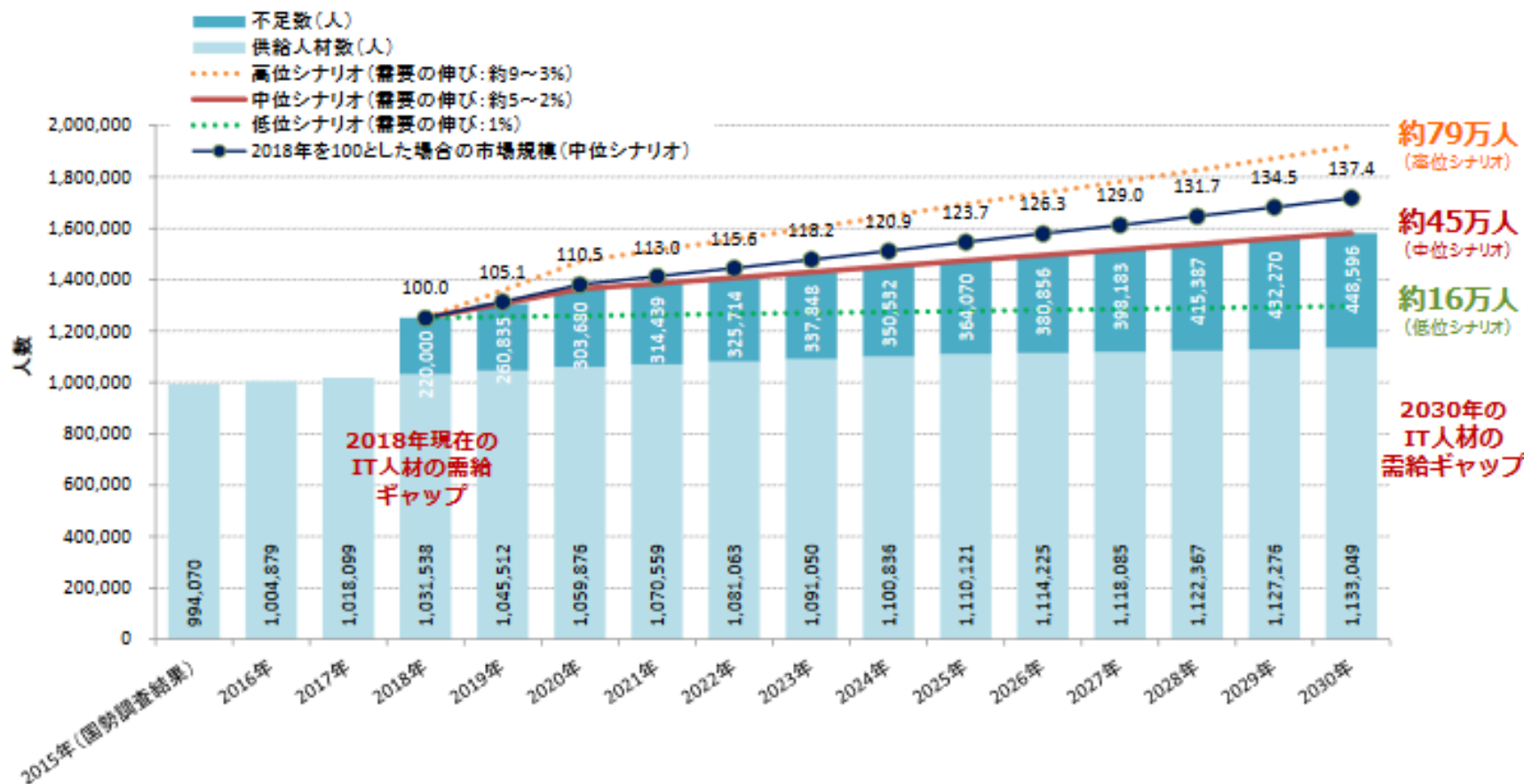
Source : 富士キメラ総研ソフトウェアビジネス新市場 2018年版

企業でのSaaS 利用は拡大

日本における自動化の必要性とITエンジニアの現状

IT技術者不足はこれからさらに深刻化

日本では

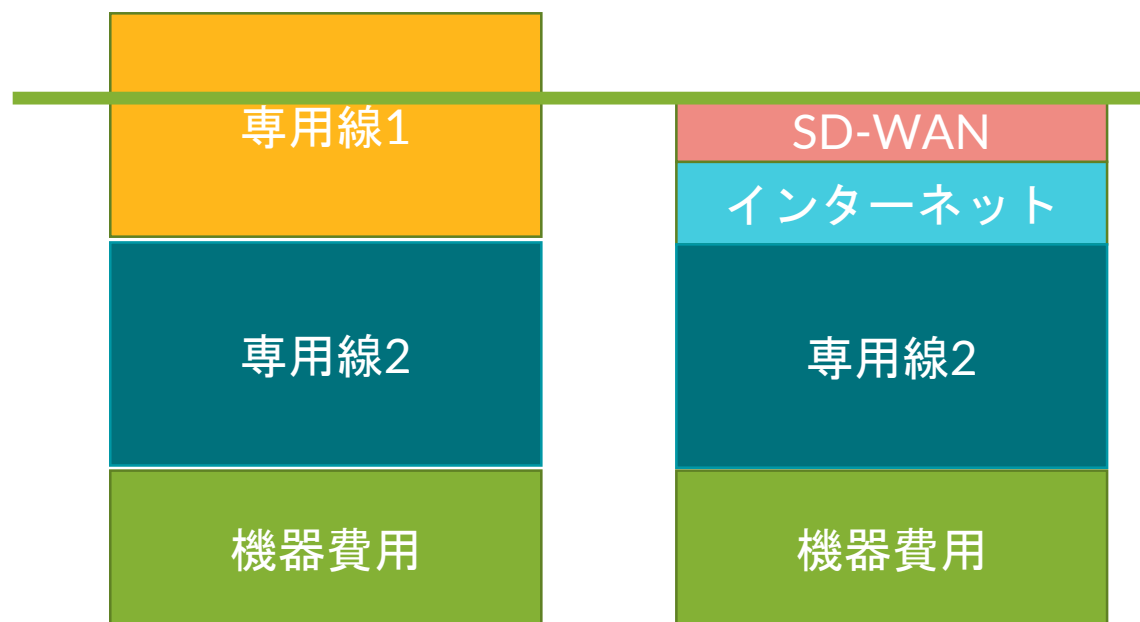


(出展) 経済産業省 IT人材の最新動向と将来推計に関する調査結果

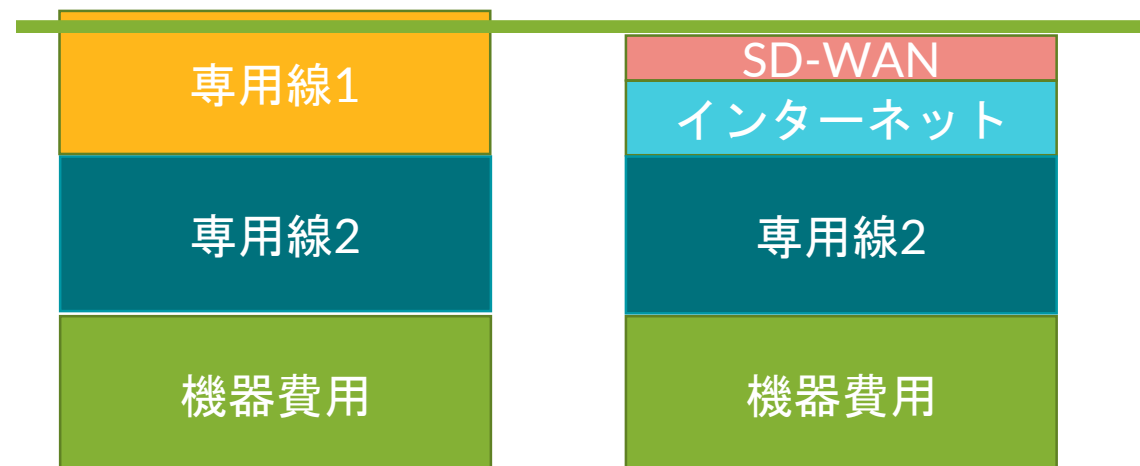
日本におけるWAN回線

- 海外では、SD-WANによって、回線のコストメリットの恩恵が十分検討余地がある。

日本では



海外の回線



日本の回線

NXTWORK2019

SD-WANの現状 エンドユーザ様の声

日々のセールス活動から、「WANに関する悩み」が見えてきたこと

日本では、WANとインターネットの料金があまり変わらないな。。

クラウドサービス導入後、ネットワークが重くなったな。

SD-WANを導入したいが、プロキシ設定を変更できないな。



ZTP/ZTRか、保守の事業者がやってくれるし関係ないかなあ。

セキュリティはやっぱり担保しないと導入は難しい

SD-WANの現状 事業者様の声

日々のセールス活動から、「WANに関する悩み」が見えてきたこと

SD-WANって言っても差別化要素
が少ないから、また価格競争。

クラウドサービス導入後、
回線を有効活用しないと！

運用するために見える化してレ
ポートしないと。



ZTP/ZTRか、これはコストがさが
るかも。

セキュリティは必ず言われるから
検討しないと。

NXTWORK.2019

立場は違えど、SD-WANのモチベーション



やりたい！！



JUNIPER[®]
NETWORKS
CSO

クラウド、仮想化、IoT、AIなどITの範囲が広がり、**ネットワークの管理負荷**を減らしたい



コントローラーによる一元管理

各ブランチオフィスには十分なIT要員がおらず、**即時展開が難しく、派遣費用も高く**なる



さまざまな方式のZTP/ZTR

セキュリティリスク対策の重要度が増しており、**セキュアなネットワーク**が必要



DPIエンジンと4000を超えるアプリ認識

クラウドアプリケーションの利用増加し、帯域も増加しており、新たなアーキテクチャが必要



APBRによるローカルブレイク

NXTWORK2019

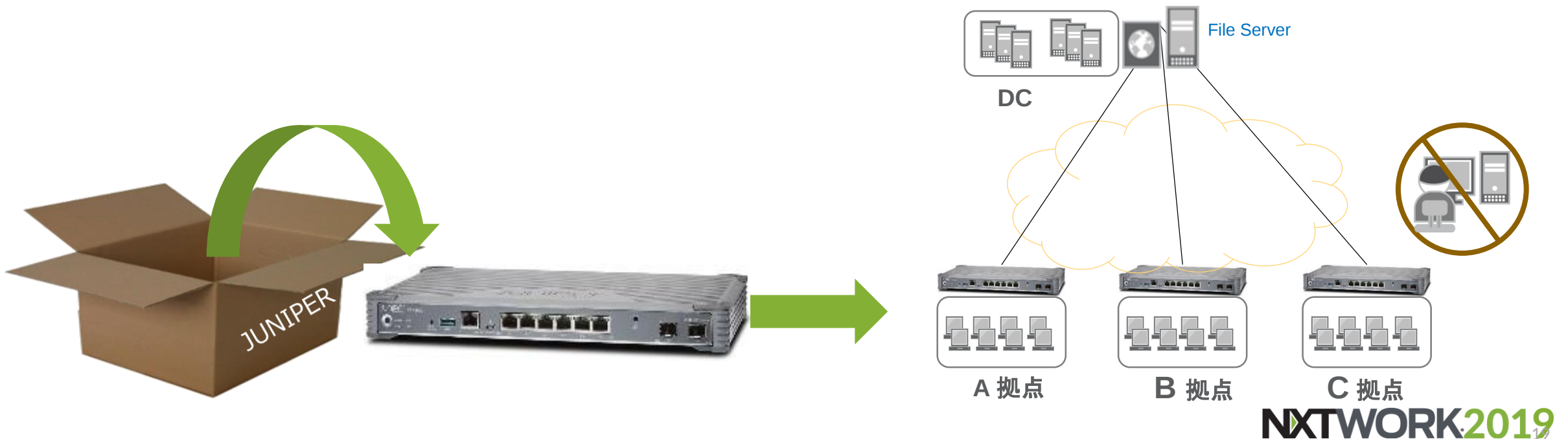
ONUG SD-WAN評価

No	評価項目	○ ×	ZTP ジュニパーネットワークス
1	Active/Active構成で様々な回線・WANの制御が可能なこと	○	Public WAN, Private WANのマルチホーミング(Active/Active)での利用ができます。
2	コモディティHW上で、仮想的にCPEを提供できること	○	vSRX (バーチャルSRX)にてSRXの機能を仮想マシン形式のCPEとしてご利用いただけます。 vNFXはのサポートは来年の予定です。
3	アプリケーション等のポリシーに基づき、ダイナミック制御が可能なこと	○	SRX、NFXのAppRoute (APBR) にてアプリケーションベースのダイナミックな制御が可能です。
4	個別のアプリに対して、可視化・優先順位付け、ステアリングが可能なこと	○	アプリケーションの可視化、アプリケーションベースでの優先制御(QoS)が可能です。
5	可用性・柔軟性の高いハイブリッドなWANの構築が可能なこと	○	複数のPrivate WAN, Public WANでの構成が可能で回線障害時も動的に切り替えが可能です。
6	L2/L3に対応	○	SRX、NFXはL2/L3に対応します。
7	拠点、アプリケーション、VPN品質等をダッシュボードでレポートができること	○	CSOでは各種ダッシュボード機能、パフォーマンスレポートの機能を備えております。
8	オープンなノースバウンドAPIを持ちコントローラーへのアクセスや制御ができること	○	REST APIをはじめ各種スクリプトを提供、資料を公開しています。 https://www.juniper.net/documentation/product/en_US/contrail-service-orchestration
9	ゼロタッチプロビジョニングに対応すること	○	SRX、NFXはZTP(ゼロタッチプロビジョニング)に対応しております。 NFXはvSRX (バーチャルSRX)を標準搭載します。
10	FIPS-140-2(セキュリティ)を取得できること	○	SRX、NFX250およびJunosはFIPS-140-2に対応しています。 https://www.juniper.net/documentation/en_US/junos/topics/reference/general/junos-fips-software-editions.html https://www.juniper.net/documentation/en_US/junos-fips12.1/topics/concept/understanding-junos-fips-mode.html https://www.juniper.net/documentation/en_US/junos-fips12.1/information-products/pathway-pages/security/security-fips-guide-12.1x46-d40.pdf https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/3288

ZTP(ZERO TOUCH PROVISIONING)とは

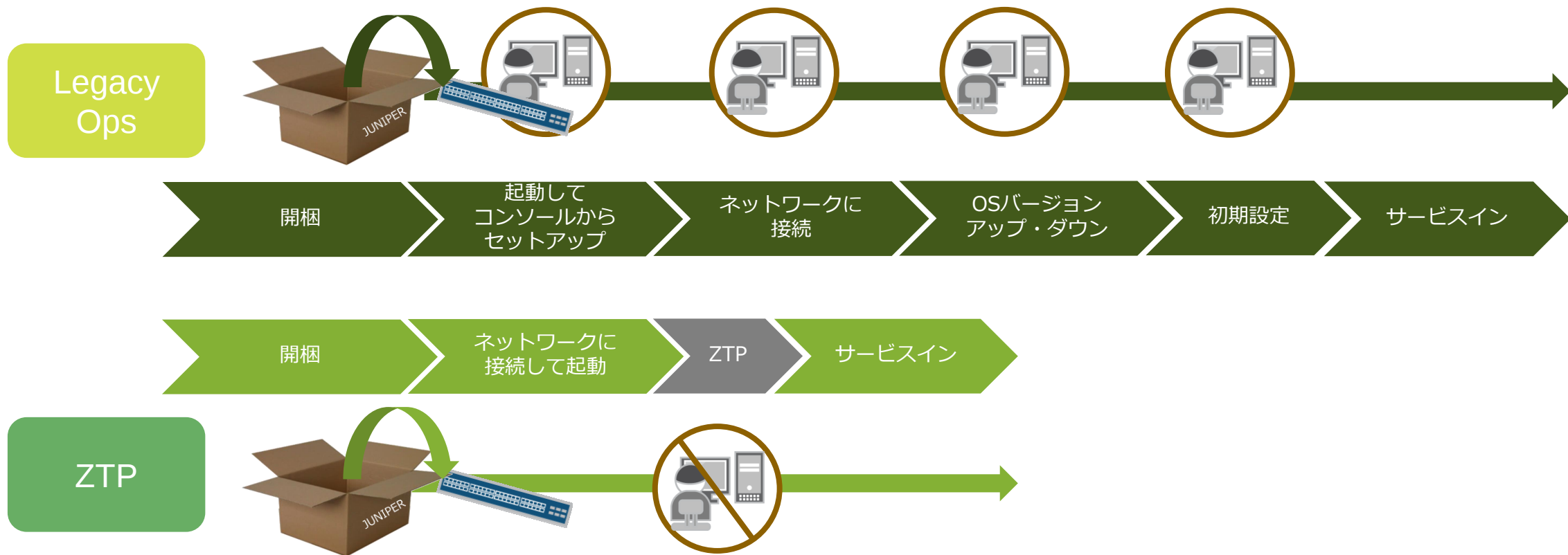
デバイスを新設するオペレーションは簡単だが、他拠点にデバイスを展開することを考えると手間とコストは膨大

ZTPとは、デバイスの初期導入時において、デバイスのOSのバージョンやコンフィグを自動でプロビジョニングする機能



ZTPと従来のオペレーションとの比較

サービスインまでの流れ

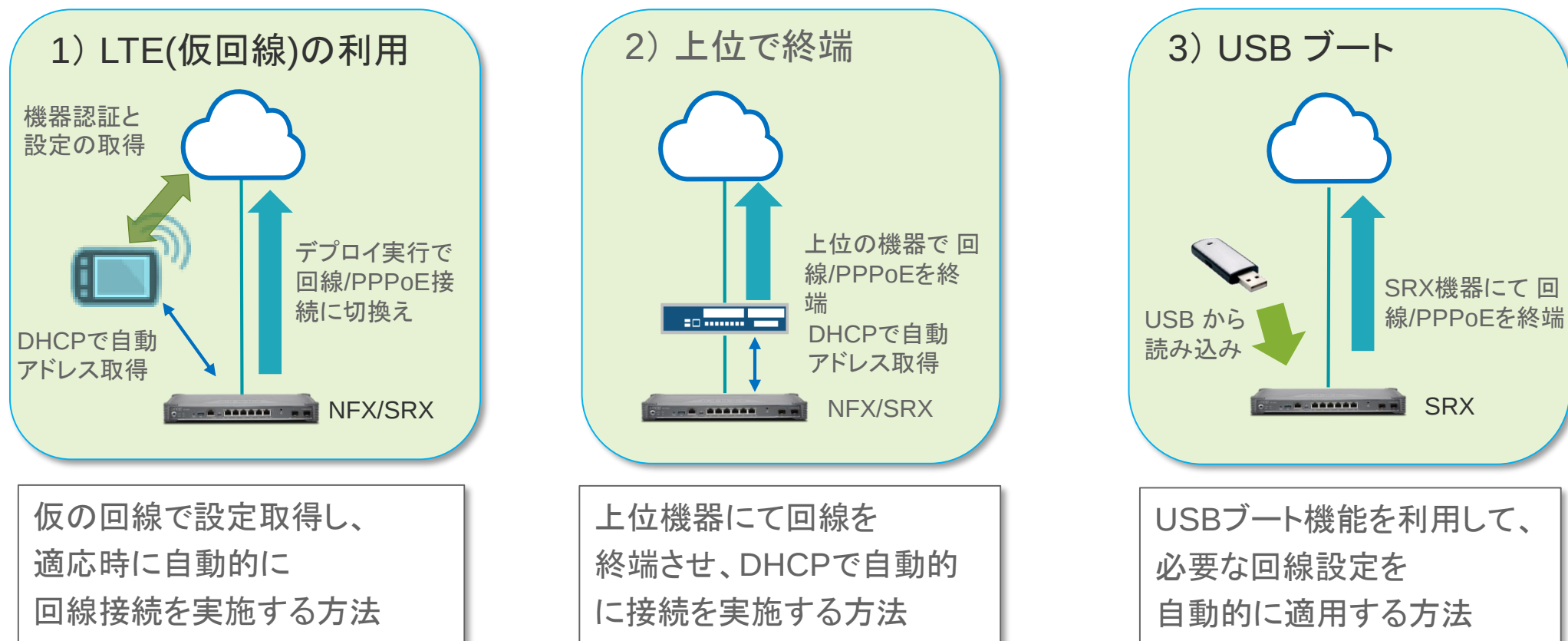


膨大な数のデバイスを設置しなくてはならない場合には、ZTPによるOPEXの削減効果は絶大

NXTWORK.2019

環境に合わせたZTPによる自動インストール

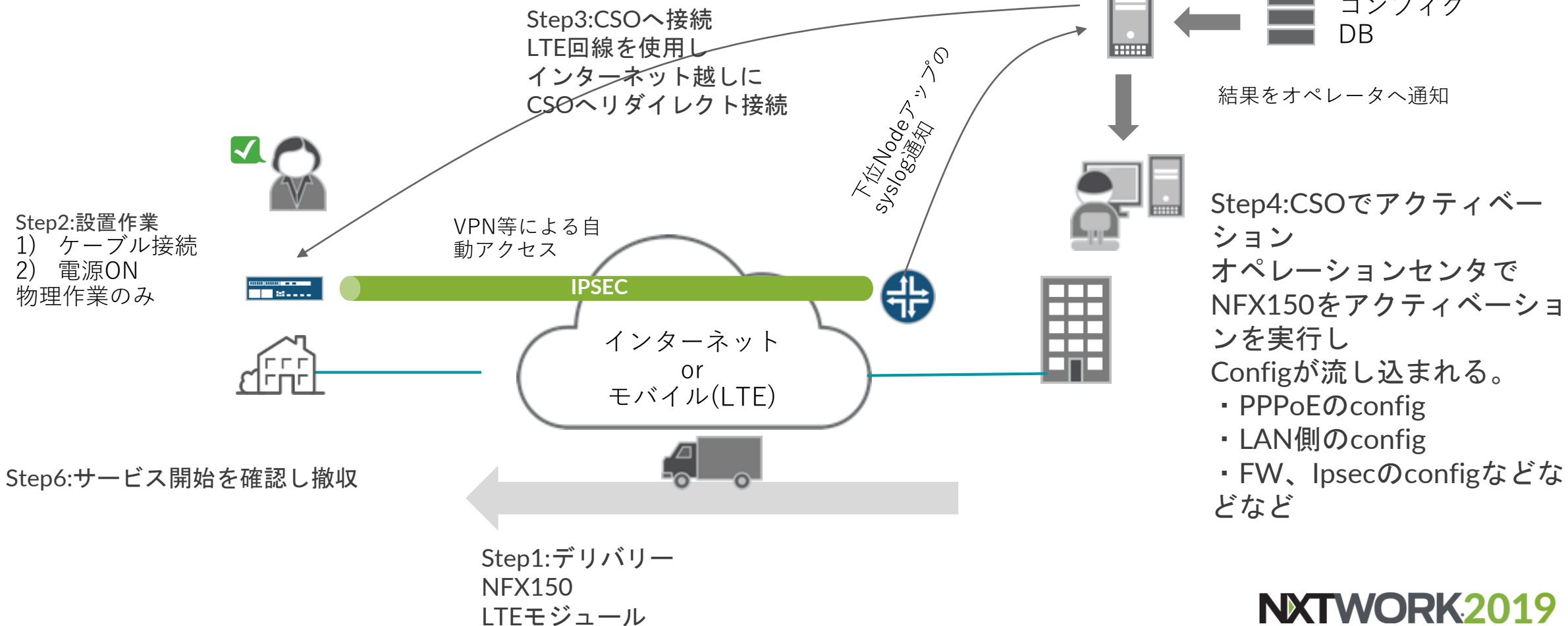
Private回線やPPPoEなどの回線を使用した環境での利用例（3構成）



ZTP : LTEモジュール、PPPoE認証あり回線

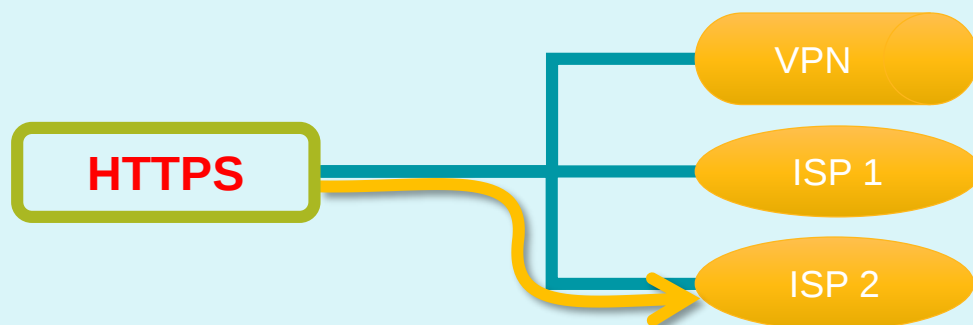
Step5:拠点開通

NFX150はPPPoE回線でインターネットに接続しサービス開始



アプリケーションを知るということは、

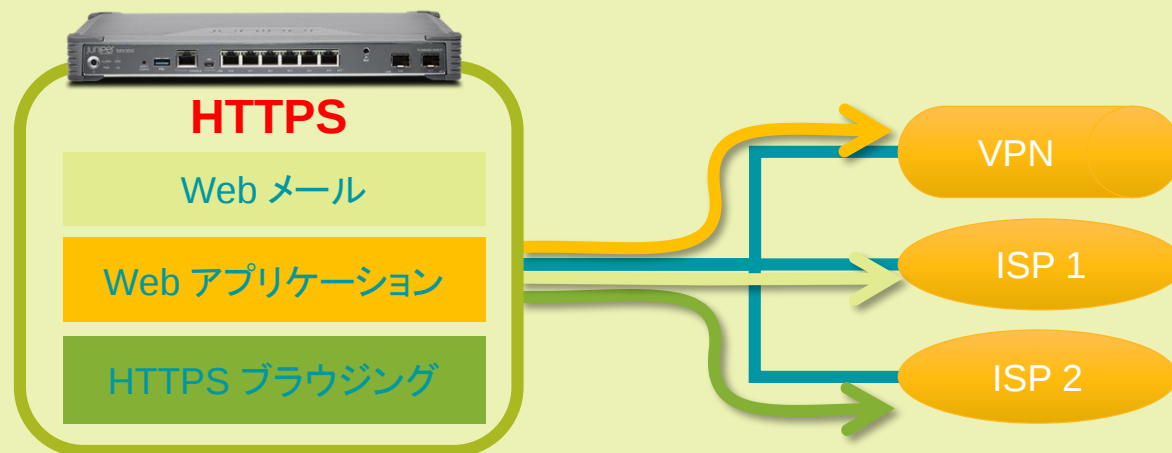
これまでの Policy-Based Routing



送信元やプロトコル/サービスによってルーティング先を指定することは可能だがアプリケーション別での制御は行えなかった

現在、多くのアプリケーションがブラウザ (HTTP / HTTPS) を介して動作するため、増加する通信量を効率的に振り分けられない

AppRoute を使用した「Advanced Policy-Based Routing」(APBR機能)



Application 識別 (AppID) を利用することにより、同じウェブ通信をアプリケーション別に認識することが可能

それぞれのアプリケーションに対して、特定したルーティングを定義し、振り分けられる

アプリケーションごとに制御するということは、

JUNOS AppSecure 機能

AppTrack

通信の可視化

AppFW

セキュリティ制御

AppQoS

優先度の制御

AppRoute

通信経路の制御

※ AppSecure 機能:

アプリケーション認識機能「AppID」によって、通信に利用されているアプリケーションを識別し、選定的に処理することを可能にする機能。

AppTrack、AppFW、AppQoS 機能に加えて、AppRoute の機能が追加されました。

※Junos 15.1X49-D60 より実装

(対応機種: vSRX、SRX300 シリーズ、SRX550 HM、SRX5000 シリーズ)

IP 情報や通信ポート情報を使用した制御 (Policy-Based Routing) を拡張し
「Advanced Policy-Based Routing」 機能として SRX に実装

- ルーティング制御を「**アプリケーション毎**」で行うことが可能

NXTWORK2019

SRXを利用したネットワークが遅くなった原因の判別

アプリケーションの使用帯域、セッション数、使用したユーザを表示



NXTWORK.2019

アプリケーションごとの最適化

キャッシュ処理：

- アプリケーション識別をキャッシュ処理し 機器負荷を軽減した動作仕様

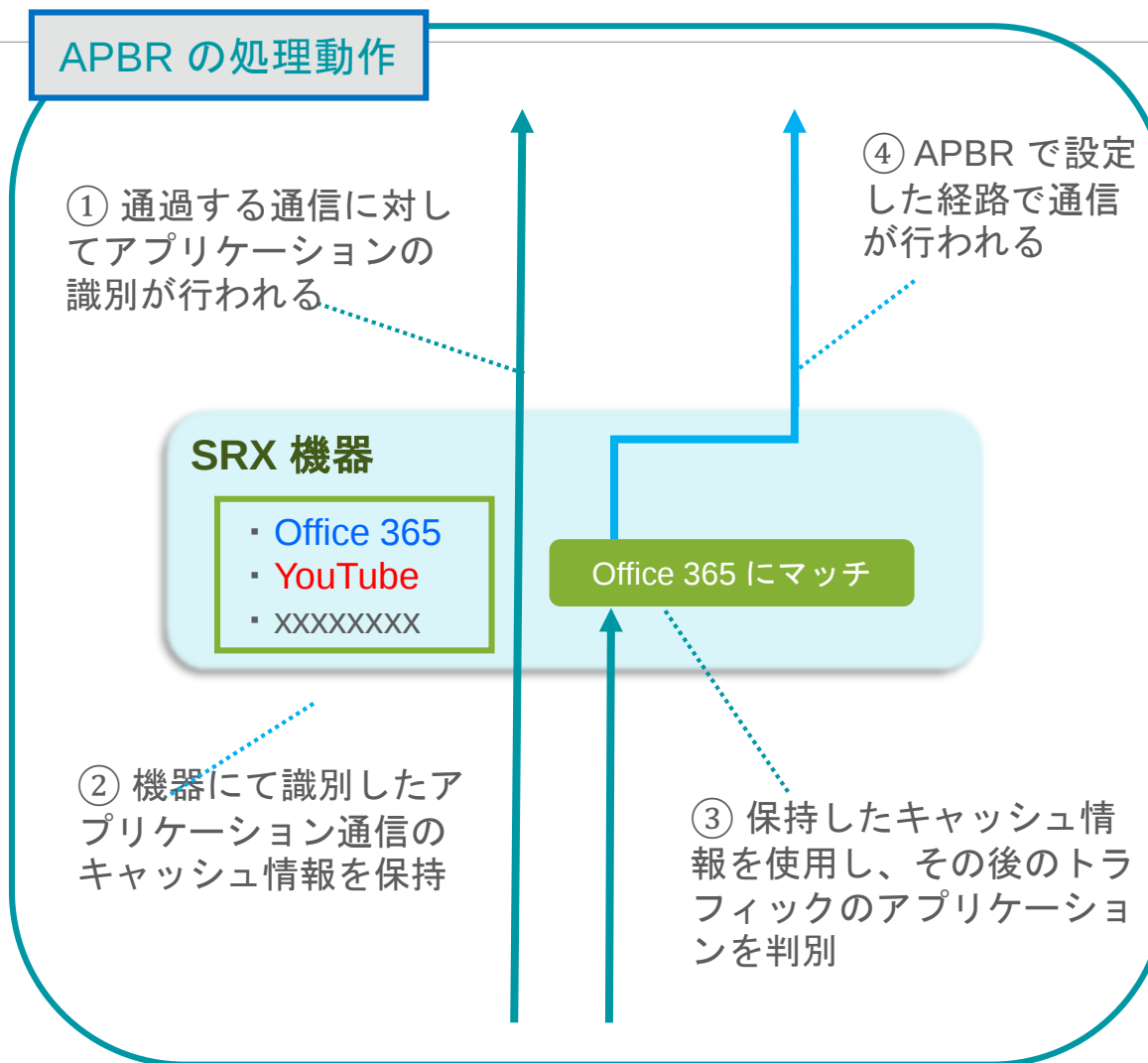
アプリケーション対応：

- 豊富なアプリケーション定義が利用可能(4000 種以上)
- 容易なカスタムシグネチャ定義によって 特定の通信要件に柔軟に対応

利用構成：

- SNI 情報を認識し SSL 通信の解読処理を不要としたアプリケーション識別
- ルーティング制御に加え「AppQoS」機能による帯域制御にも対応
- エントリーモデル（SRX300）にて利用可能

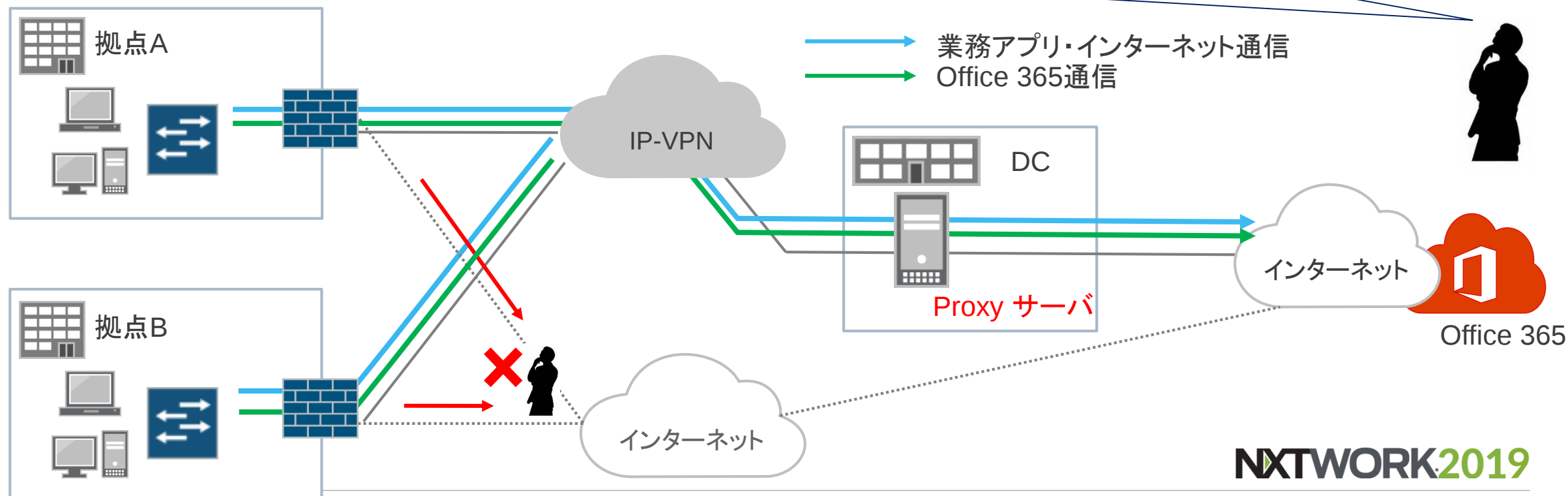
(※JSE ライセンスまたは、IDP機能ライセンスが必要になります)



NXTWORK2019

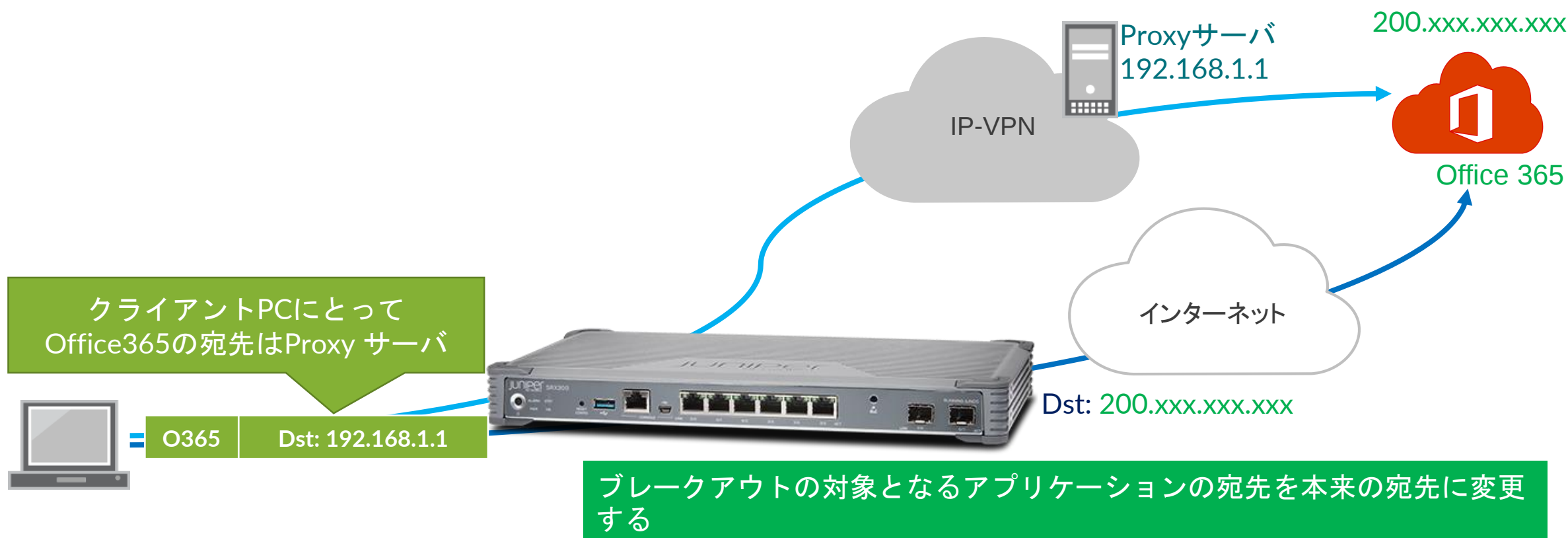
APBR(ローカルブレイクアウトソリューション) の課題

クラウド化が進む中で、DCに向かうトラフィック量が増大している。
インターネット回線を用意してトラフィックの負荷分散をしたいが、
セキュリティのためにProxyサーバを導入しており、一部のアプリケーションのみ
Proxyサーバを経由しない設計は困難。そのため、**ローカルブレイクのソリューションは導入できない**。



ローカルブレイクアウトソリューションを導入できない原因の解決

アプリケーションを判別した後、
ブレイクアウト対象のアプリケーション通信であれば**本来の宛先**に変更して通信させる。



NXTWORK2019

ブレイクアウトした通信ログの表示

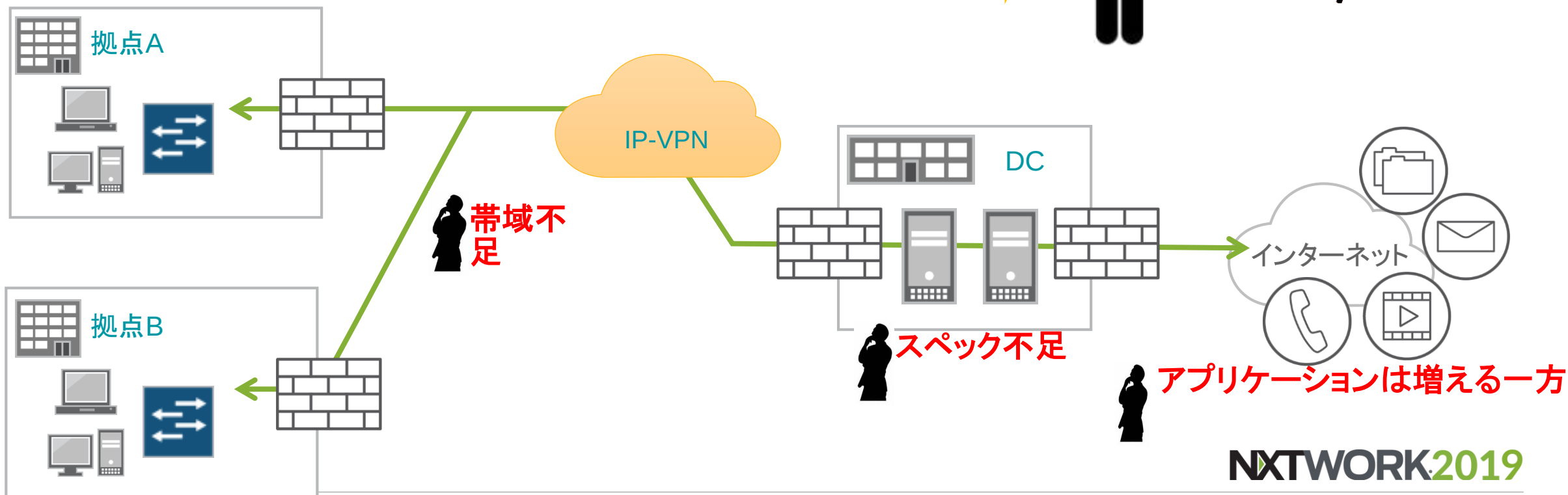
HTTPS（SSL）の通信でもアクセス先（URL）とユーザ名をログ出力することが可能。

Web Filtering Events ?					
Summary View		Detail View			
				ユーザ名	アクセス先
Source Port	Destination Country	Destination IP	Destination Port	User Name	URL
370	 Singapore	111.221.29.254	443	katagiri	v10.vortex-win.data.microsoft.com
368	 Singapore	111.221.29.236	443	katagiri	array305-prod.do.dsp.mp.microsoft.com
367	 United States	40.96.3.210	443	katagiri	outlook.office.com
364	 United States	40.77.228.92	443	katagiri	watson.telemetry.microsoft.com
363	 Singapore	111.221.29.254	443	katagiri	v10.vortex-win.data.microsoft.com

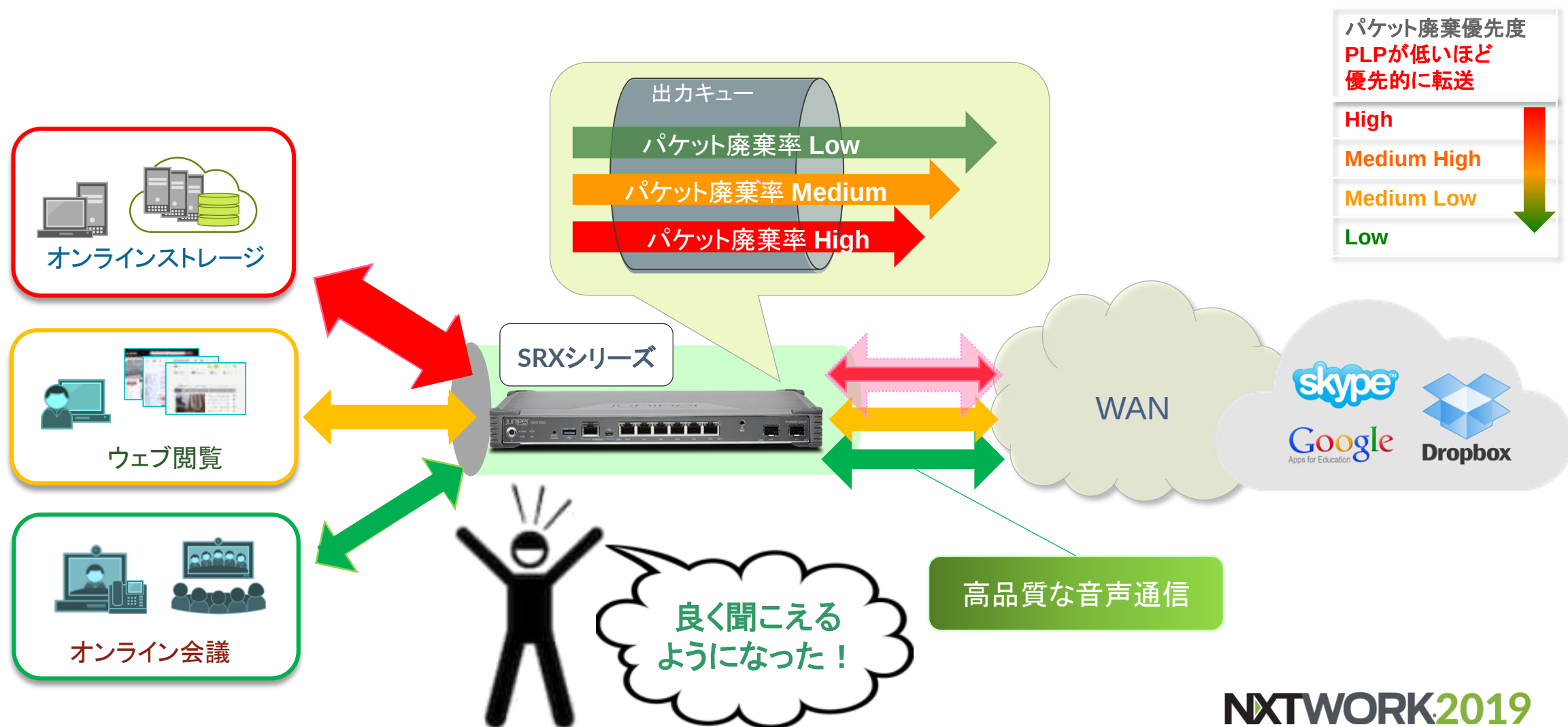
ビデオ動画や音声通話が品質劣化する要因

SaaSの普及に伴いWANに流れ込むトラフィック量が増大し
タイムクリティカルなアプリケーションが影響を受ける。

VoIPやオンライン会議の音声品質が低下し会話が聞き取り難くなる



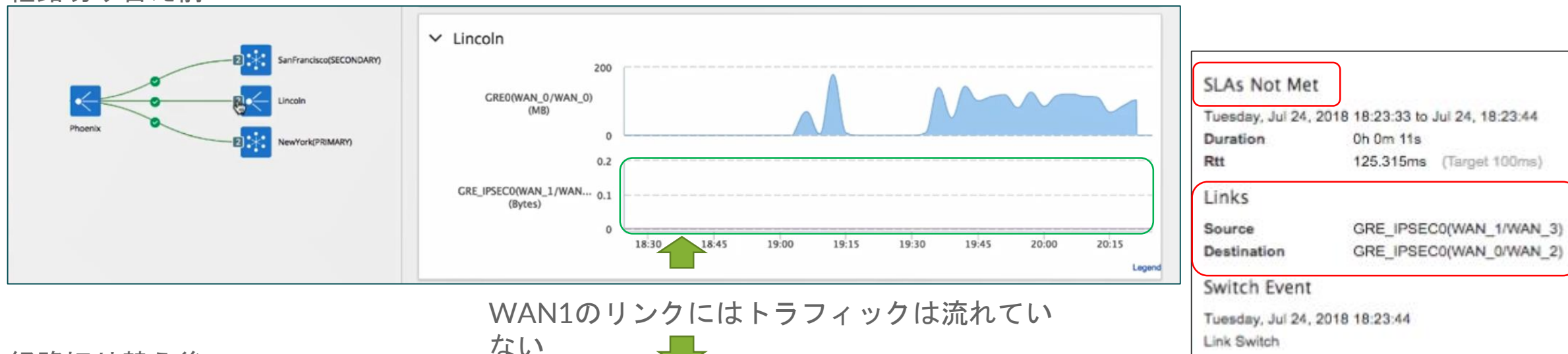
リアルタイム性の高いアプリケーションを最優先させ通信を制御



アプリケーション単位でSLAを定義して経路を動的に変更するAPPQOE

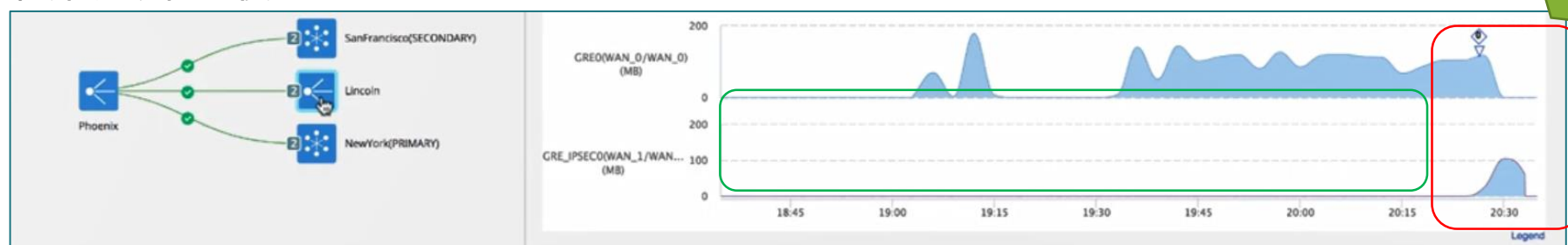
SLA違反を検知すると経路が切り替わる

経路切り替え前



WAN1のリンクにはトラフィックは流れていない

経路切り替え後



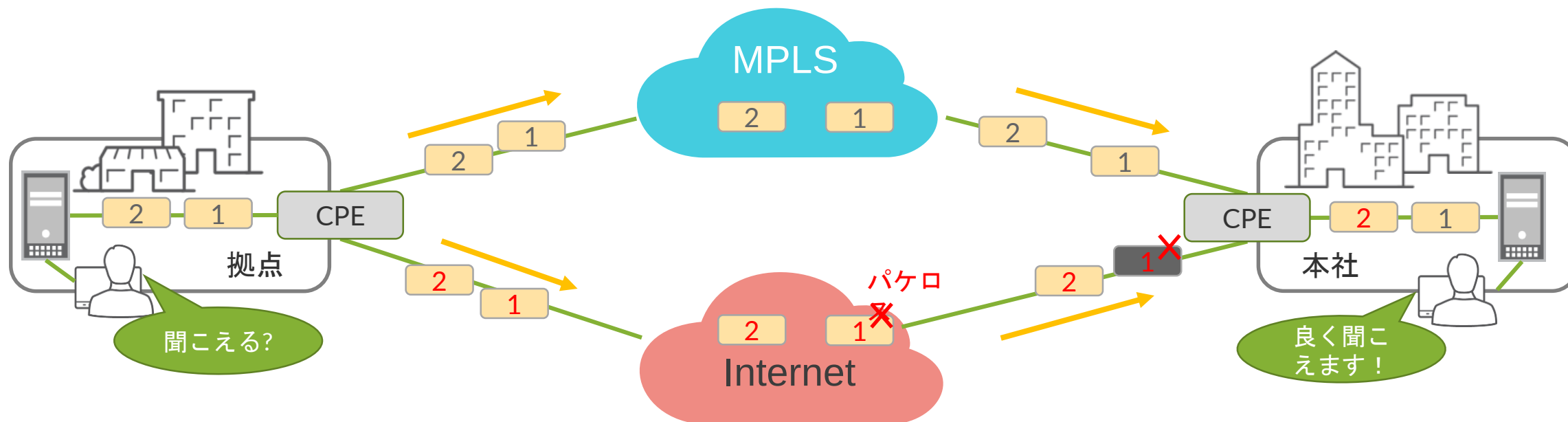
SLA違反のためWAN1からWAN2に切り替えて通信を開始

NXTWORK.2019

パケットを複製して品質を高めるMULTI PATHING SUPPORT

該当するアプリケーションを複製してデータ遅延、欠損を補完する。

- パケットロスが発生した場合、欠損したパケットを補完する
- 同じパケットを複数受信した場合は2番目に受信したパケットを捨てる



– SD-WAN その先へ

SD-WANわかってきた。。。。

メーカーの人の言っていることってあまり差別化ないなあ。

WANのデバイスの下にスイッチがあるのに。。

WifiのAPもあるんだけど。。



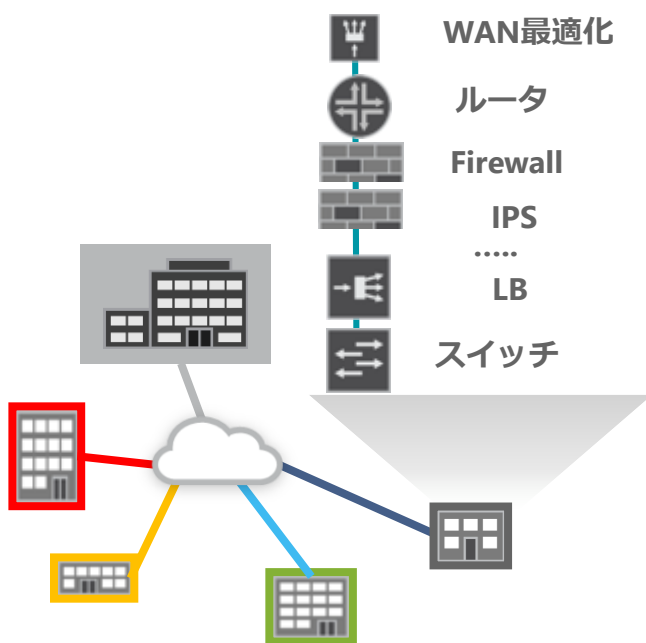
セキュリティ必須、UTMも欲しい。

独自のサービスを展開して、差別化を図りたい

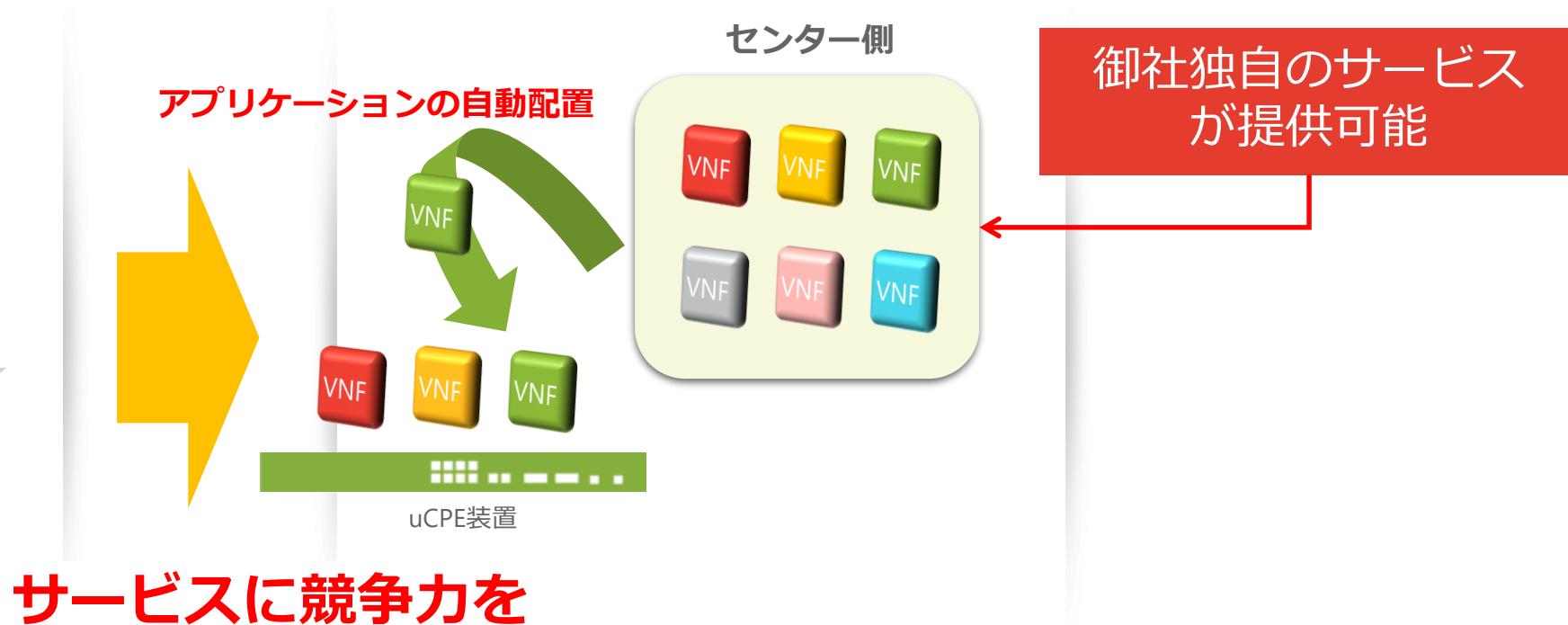
SD-WANに付加価値をプラス

オフィスや店舗で役立つネットワーク機能を敏速にお客様サイトへ提供するサービス
完全に自動化されたオーケストレーションプラットフォームによりに必要な機能を必要な時に利用
業界をリードする最新のアプリケーションをVNFサービスカタログで提供
複数の機器をお客様サイトに設置する必要なし

現状のブランチオフィス

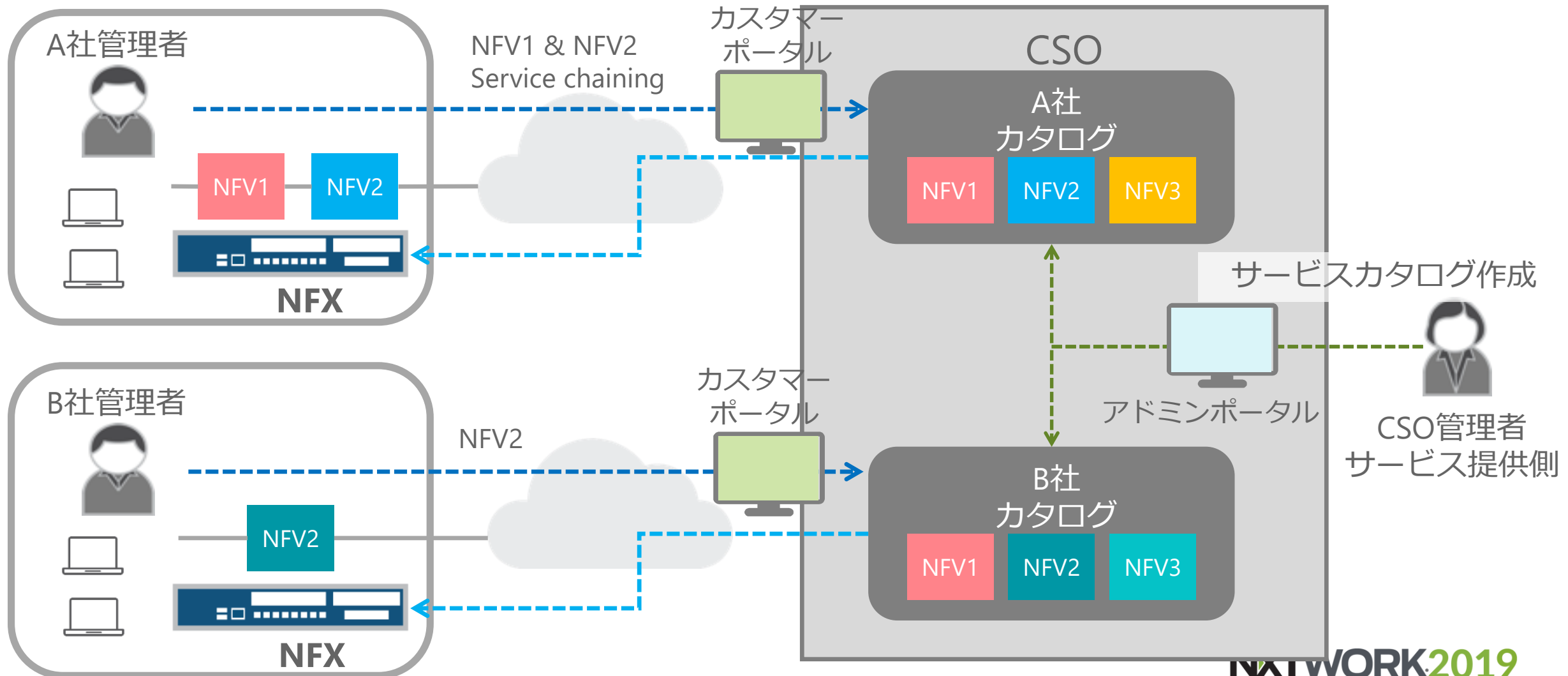


次世代ブランチオフィス(uCPE)



サービスに柔軟性とスピードを エンドユーザ毎に異なるサービスを提供

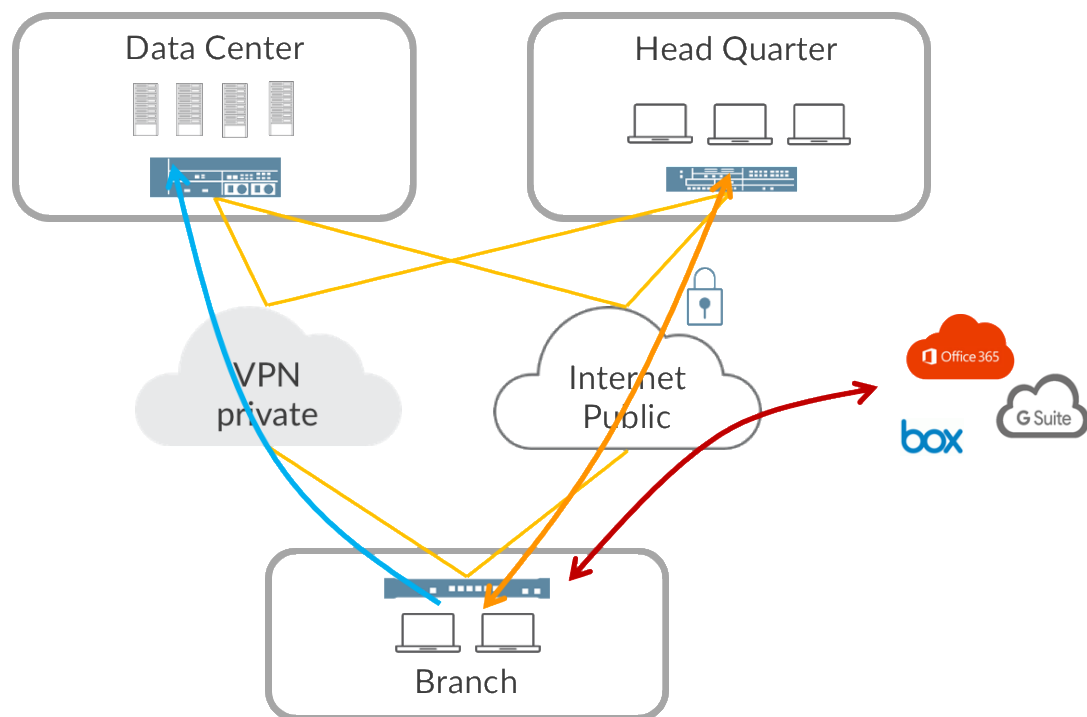
セルフオンデマンド
サービスを提供



SD-WAN + 独自サービスで柔軟性と競争力のあるサービスを

Contrail Service Orchestration (CSO)で次世代マネージドサービス

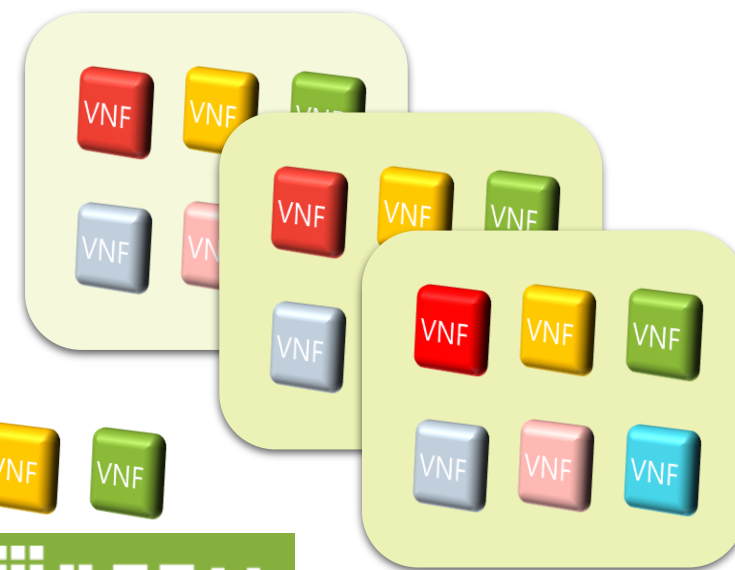
SD-WAN



オンデマンド NFV/アプリケーションサービス



VNF Service カタログ



uCPE デバイス

NXTWORK2019

広範囲なセキュリティサービス

次世代 ファイアーウォール

アプリケーションの
制御と可視化

不正侵入防御 (IPS)

ユーザーベース
ファイアーウォール

Unified Threat Management (既知の脅威に対する対策)

アンチウィルス

Web/コンテンツ
フィルタリング

アンチスパム

脅威インテリジェンス プラットフォーム

ボットネット/C&C

GEO-IP

カスタムフィード, APT

クラウドベースの 高度な脅威防御 (ゼロデイ対策)

サンドボックス

サンドボックスを
回避するマルウェア

豊富なレポーティングと
分析機能

SRX 基本サービス

ファイアーウォール

NAT

VPN

ルーティング

マネージメント

レポーティング

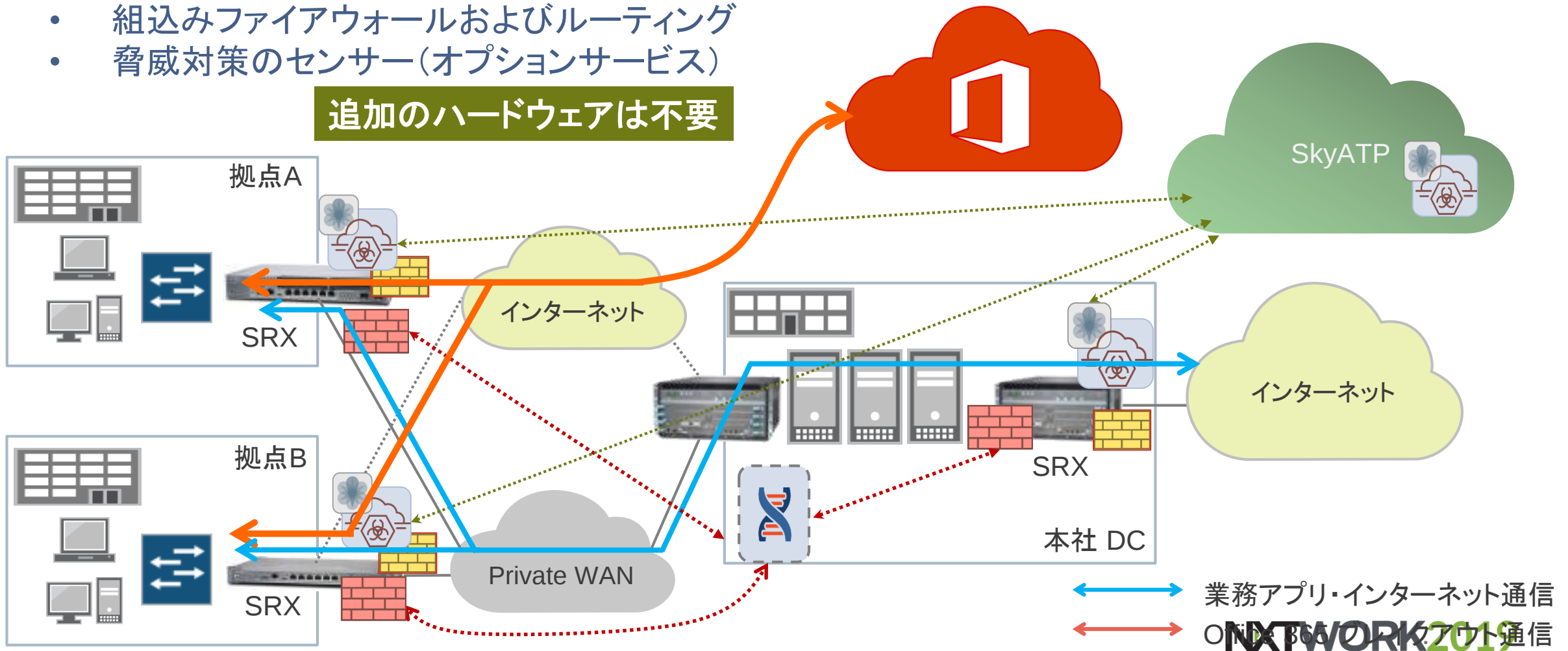
分析

オートメーション

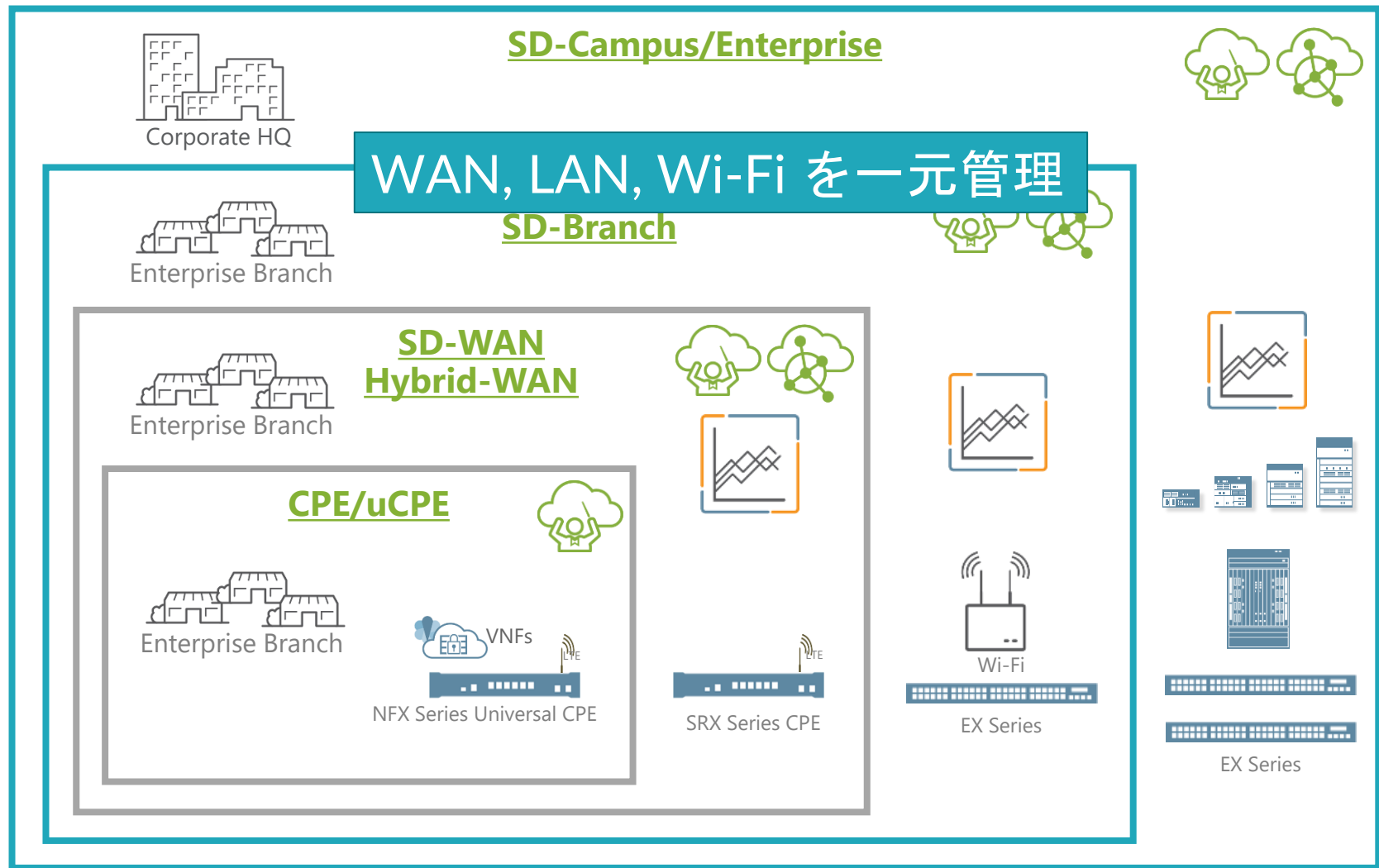
セキュアなSD-WAN: 追加ハードウェア不要でセキュリティを強化

- Office365等クラウドアプリケーションの最適化
- 組込みファイアウォールおよびルーティング
- 脅威対策のセンサー(オプションサービス)

追加のハードウェアは不要



SD-WANからSD-ENTERPRISEへ



SD-LANのマーケット状況



SD-LAN市場は定義まだ決まっていない揺籃期

We are increasingly seeing network vendors market things such as SD-LAN, SD-Access, SD-Campus...etc.

There is no official, unofficial, or even de facto definition of the terms “SDLAN,” “SD-Access” or “SD-Campus.”

Opinion: There's no such thing as SDLAN (yet)

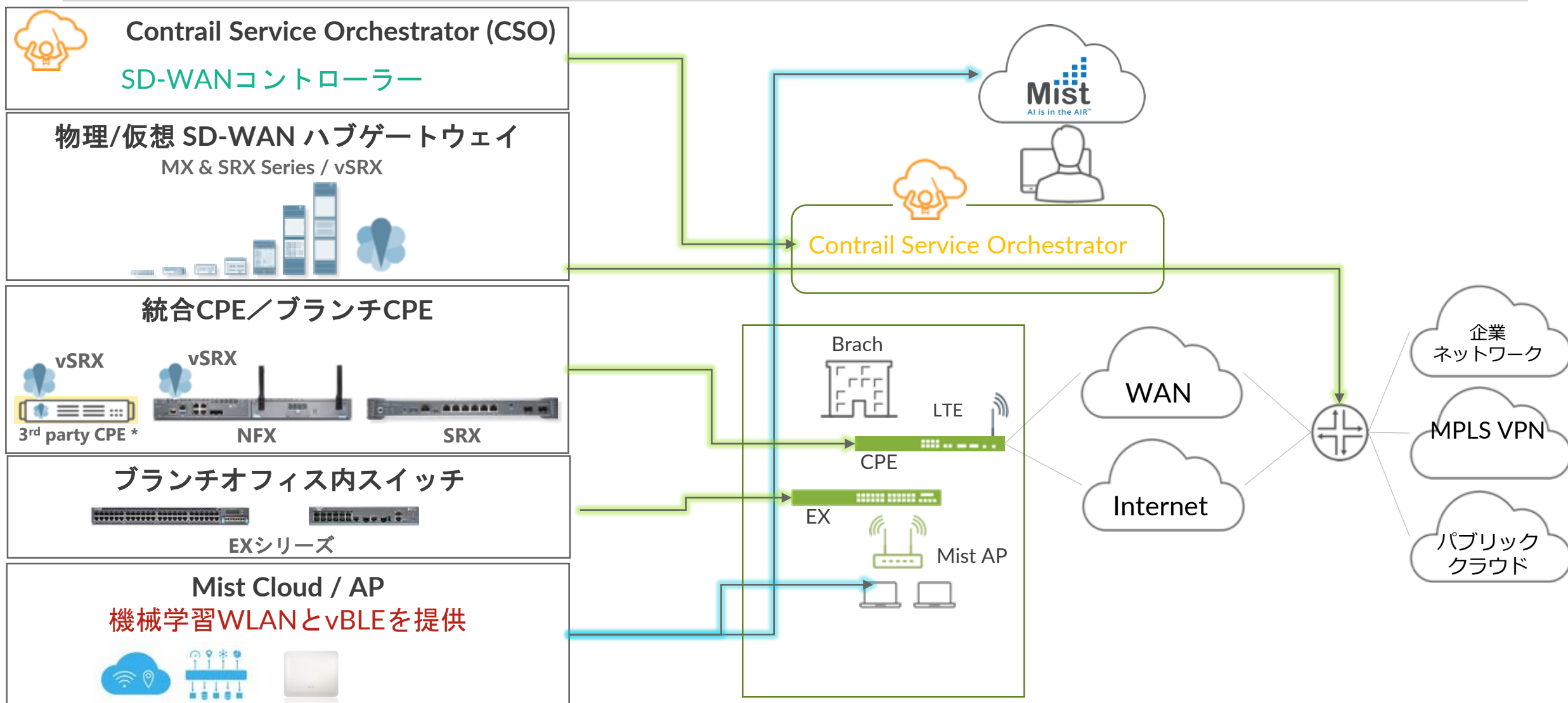
Article by Gartner Research vice president Andrew Lerner

<https://itbrief.co.nz/story/opinion-there-s-no-such-thing-as-sdlan-yet>

NXTWORK.2019

JUNIPER
NETWORKS

SD-BRANCH/ENTERPRISE ソリューション コンポーネント



スイッチ管理

Sites

	Site Name	Location	Template	Site Status	Operati...	Devices	Type	Lo
☐	Shinjuku	Shinjuku	--	PROVISIONED	Up	1	Enterprise Hub	En
☐	Kawasaki	Kawasaki	NFX150-LTE	PROVISIONED	Up	1	On-Premise Spoke	En
☒	Nara	Nara	SRX-Static	PROVISIONED	Up	1	On-Premise Spoke	En
☐	OAM-HUB-01	--	--	PROVISIONED	Up	1	Provider Hub	--
☐	INPR-HK-HUB-1	--	--	PROVISIONED	Up	1	Provider Hub	--

Create Site

GENERAL | **TOPOLOGY**

SD-WAN

LAN

EX 150

Site Activation

- Site
 - Model site: success
- CPE
 - Detect device: success
 - Bootstrap device: success
 - Provision device: success
- LAN Switch
 - Detect device: success
 - Bootstrap device: success
 - Provision device: success

Site activation is complete.

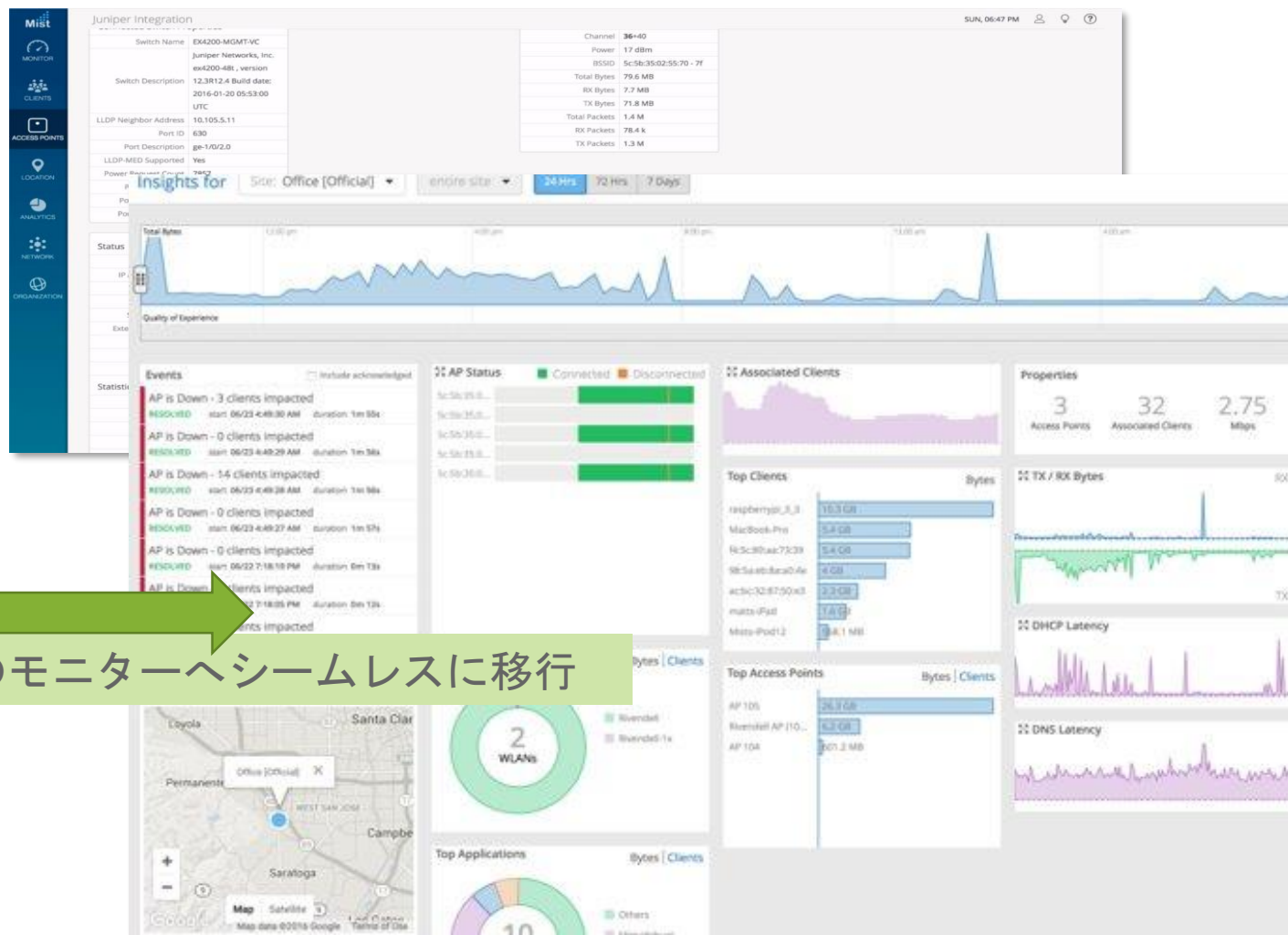
APのモニタリング

Feature Support

CSO GUIインベントリにてMist AP
のシームレスクロスモニタリングを実現

Wifi AP (Mist Systems)
をクリック

AP Cloud Managerのモニターへシームレスに移行



クラウドベースのマネージメントシステム： WANからLAN, Wi-Fiまで一元管理

可視化

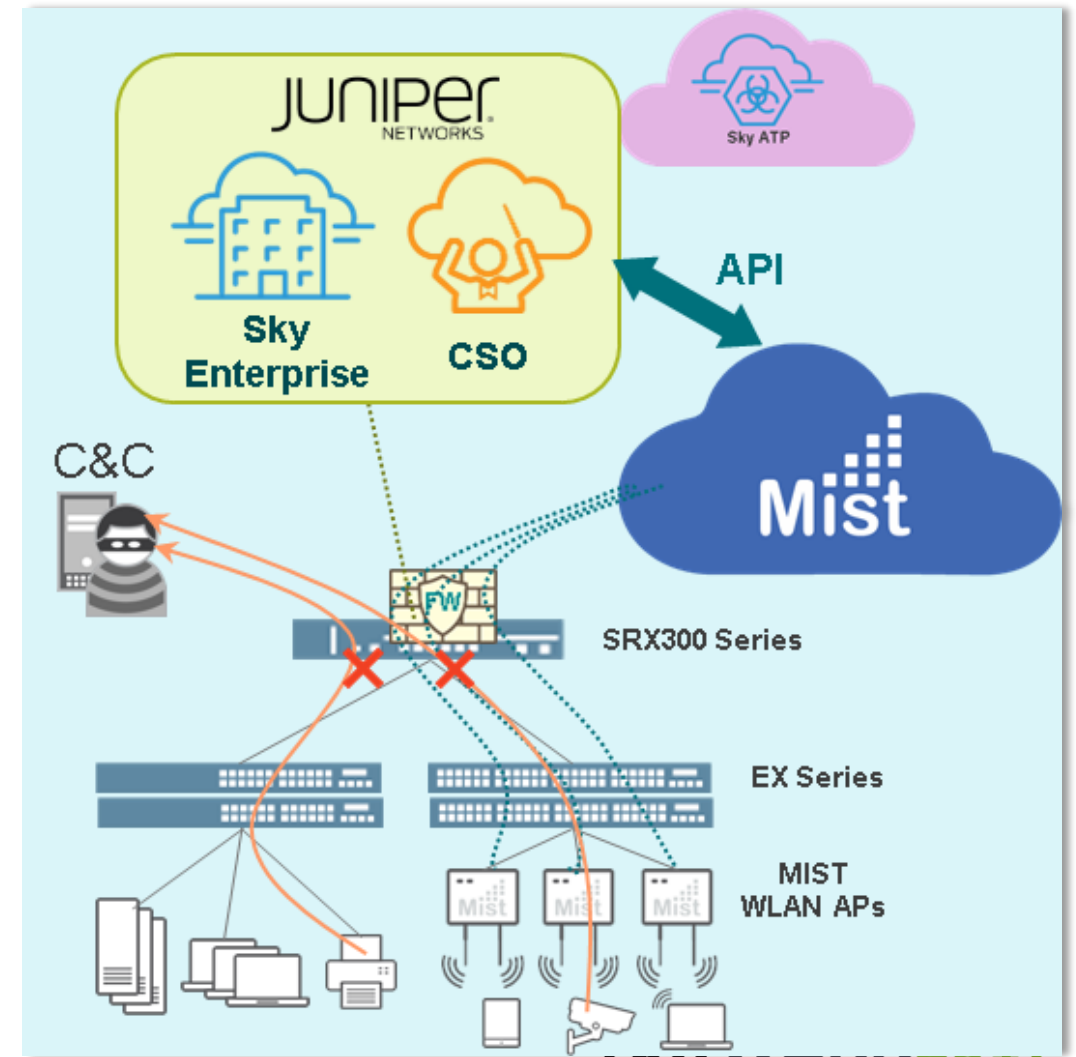
- Wi-Fi の稼働状況および通信品質の可視化
- アプリケーションの可視化とトラフィックの制御
 - ユーザ体感の最適化

一元管理

- NWデバイスの追加、操作、設定変更
 - セキュリティ、スイッチ、およびWi-Fi の一元管理
- デバイスのモニタリングとレポートニング

セキュリティ

- 境界セキュリティと脅威対策



JUNIPER NETWORKSが提供するSD-WANソリューション

CAPEX/OPEXの 軽減

- WAN, LAN, Wi-Fi を一元管理
- テンプレート作成による簡単運用
- ZTPによる拠点構築

ユーザ体感の向上

- クラウドアプリケーションを利用するユーザの体感を改善
- 拠点間通信の最適化

収益モデルの構築

- サブスクリプションモデルにより、必要に応じてセキュリティサービスを追加
- カタログモデルの販売(3rd パーティVNFをオンデマンドで提供)

ご清聴ありがとうございました。

JUNIPER
NETWORKS

Engineering
Simplicity