

プロキシ環境でも容易に導入可能  
エンタープライズSD-WANとは

～ Office 365をより快適に使うためのジュニパーのクラウド最適化ソリューション～

2019年9月24日

JUNIPER  
NETWORKS

Engineering  
Simplicity



# SD-WANとは

# ONUG SD-WAN評価

No	評価項目	可否	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	<input type="radio"/>	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	<input type="radio"/>	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。
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	<input type="radio"/>	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	<input type="radio"/>	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	<input type="radio"/>	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	<input type="radio"/>	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	<input type="radio"/>	CSO / Sky Enterprise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います。
8	オープンなノースパウンド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	<input type="radio"/>	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。 <a href="https://www.juniper.net/documentation/product/en_US/contrail-service-orchestration">https://www.juniper.net/documentation/product/en_US/contrail-service-orchestration</a>
9	ゼロタッチプロビジョニングに対応すること	<input type="radio"/>	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	<input type="radio"/>	SRX、NFX250およびJunosはFIPS-140-2に対応しています。 <a href="https://www.juniper.net/documentation/en_US/junos/topics/reference/general/junos-fips-software-editions.html">https://www.juniper.net/documentation/en_US/junos/topics/reference/general/junos-fips-software-editions.html</a> <a href="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/topics/concept/understanding-junos-fips-mode.html</a> <a href="https://www.juniper.net/documentation/en_US/junos-fips12.1/information-products/pathway-pages/security/security-fips-guide-12.1x46-d40.pdf">https://www.juniper.net/documentation/en_US/junos-fips12.1/information-products/pathway-pages/security/security-fips-guide-12.1x46-d40.pdf</a> <a href="https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/3288">https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/3288</a>



何故、SD-WANが必要なのか

## SD-WANを検討するモチベーション

### 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(3<sup>rd</sup> パーティ-VNFをオンデマンドで提供)

## エンドユーザがSD-WANを必要とする理由

### 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
- ZTPI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(3<sup>rd</sup> パーティ-VNFをオンデマンドで提供)



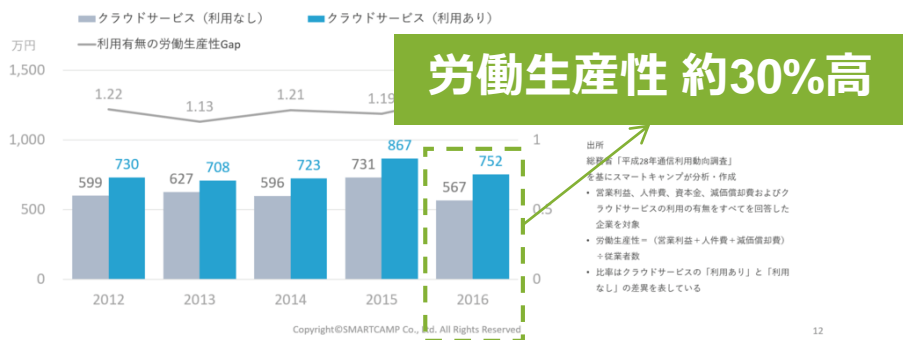
# クラウドサービスの普及と課題

## 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

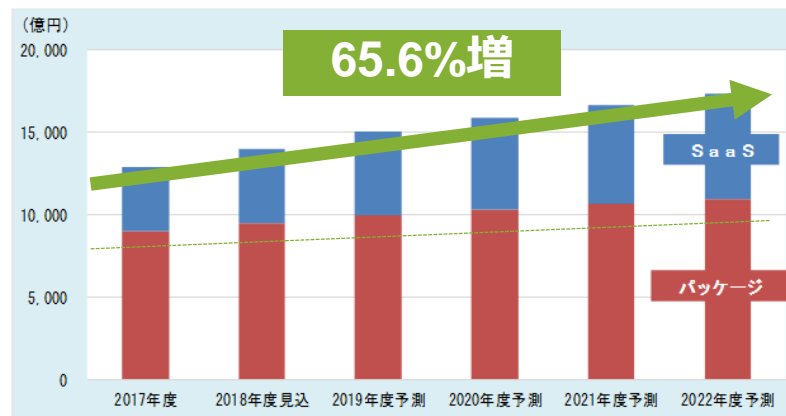
### クラウドサービスの利用による1社あたり労働生産性の向上



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。



### ソフトウェアの国内市場（パッケージ/SaaS）



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

Source : 富士キメラ総研ソフトウェアビジネス新市場 2018年版

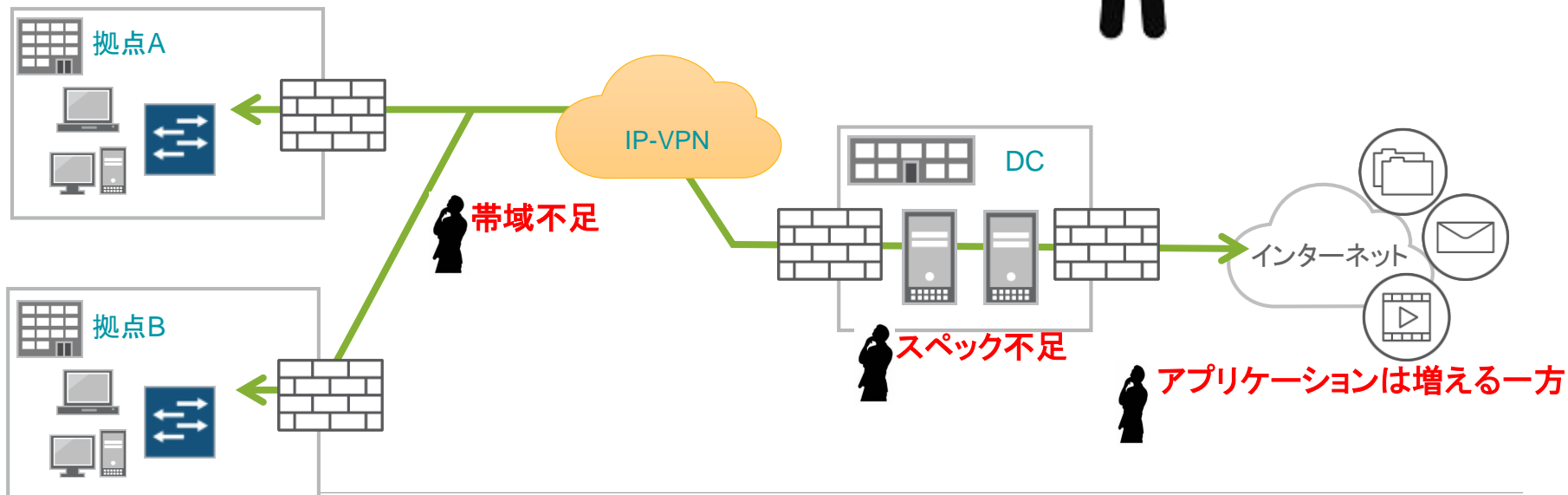
# 企業でのSaaS 利用は拡大

## 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







# アプリケーション制御による 課題の解決

# 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

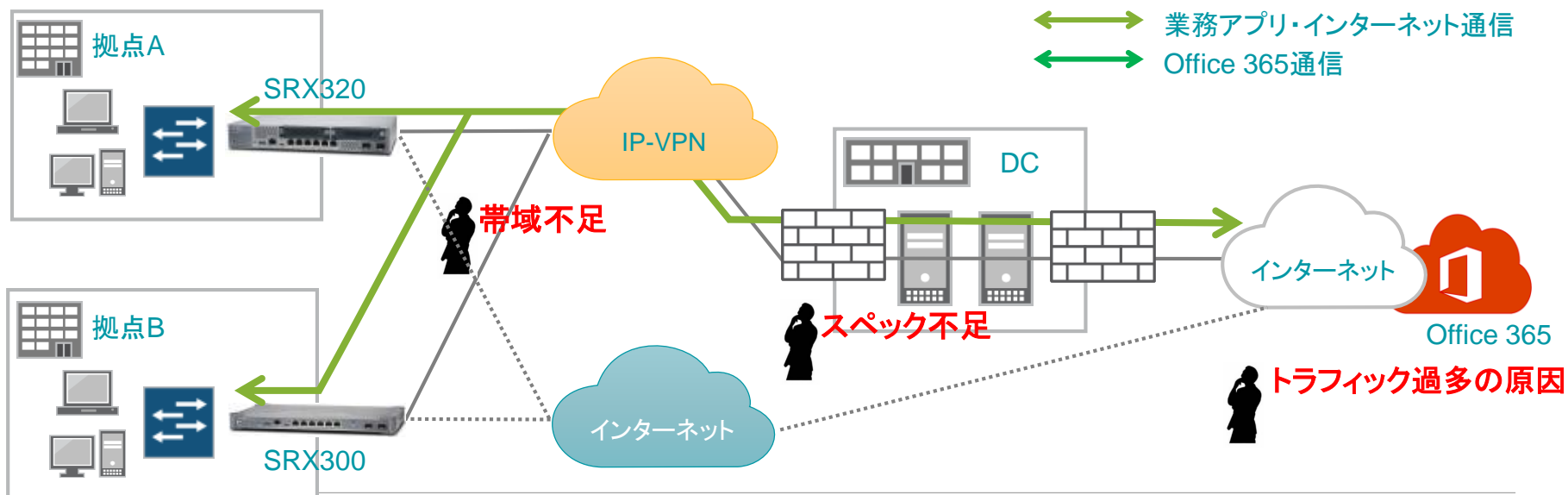


原因となっているアプリケーション、ユーザを特定できる



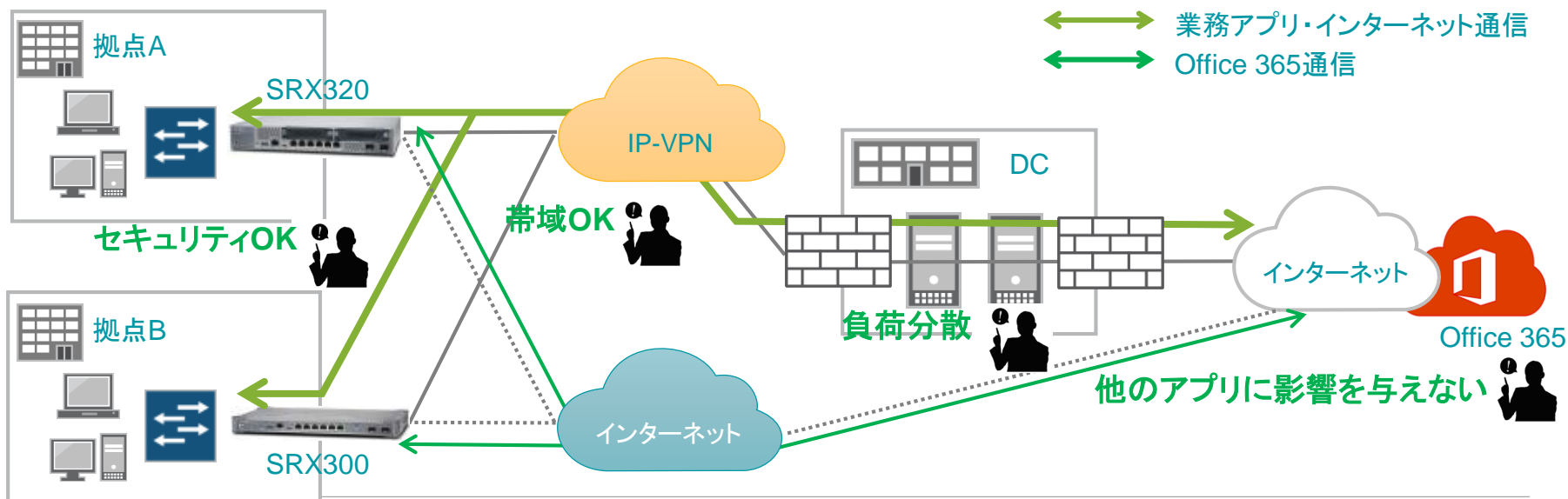
## ローカルブレイクアウトの需要

- ✓ 帯域不足でファイルのダウンロードに時間が掛かる
- ✓ 今後のどれだけクラウドサービスを使用していくか不明瞭なため単純な回線増強ではすぐに頭打ちになってしまう。
- ✓ データセンタ側のFWに負荷が掛かり処理に時間が掛かる



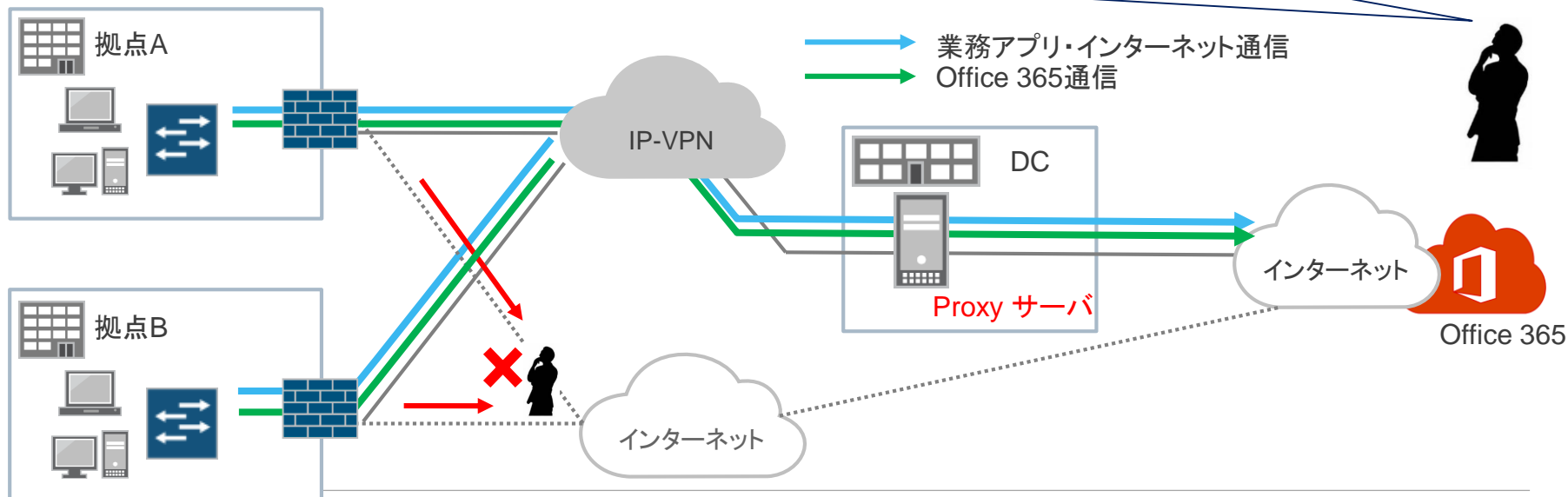
## ローカルブレイクアウトの需要

- ✓ IP-VPN回線の増強は不要
- ✓ トラフィック過多の原因となっていたO365はインターネット回線から通信
- ✓ インターネットへのアクセスもFW経由なので問題なし



## ローカルブレイクアウトソリューションの課題

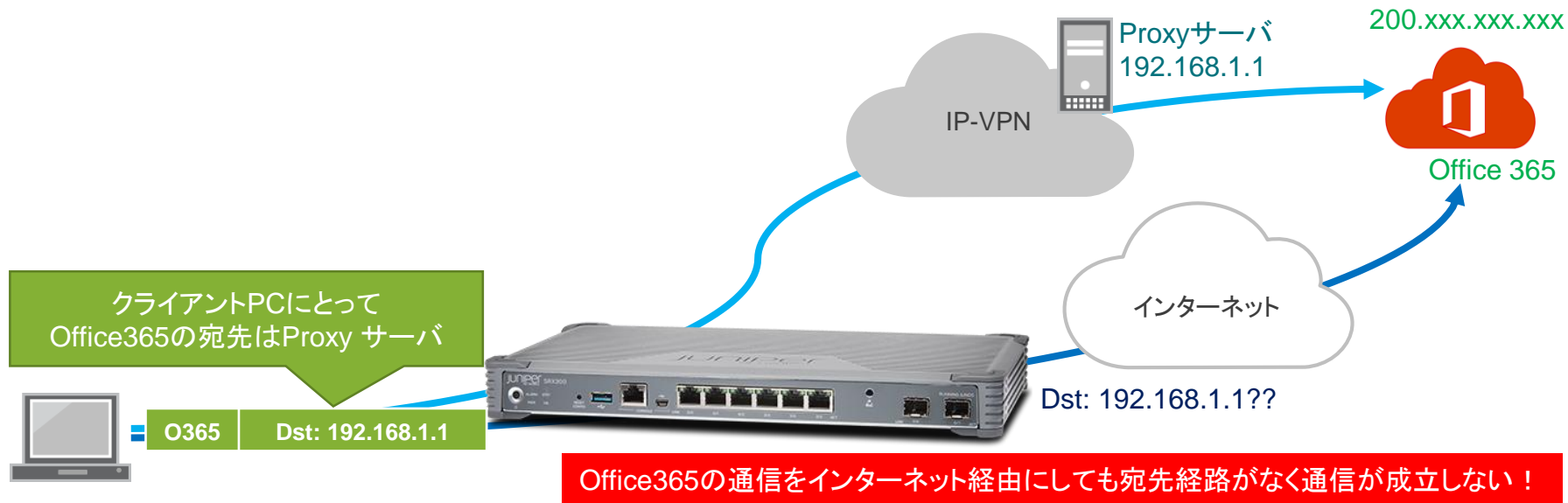
クラウド化が進む中で、DCに向かうトラフィック量が増大している。  
インターネット回線を用意してトラフィックの負荷分散をしたいが、  
**セキュリティのためにProxyサーバを導入**しており、一部のアプリケーションのみ  
**Proxyサーバを経由しない設計は困難**。そのため、**ローカルブレイクのソリューションは導入できない**。



## 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

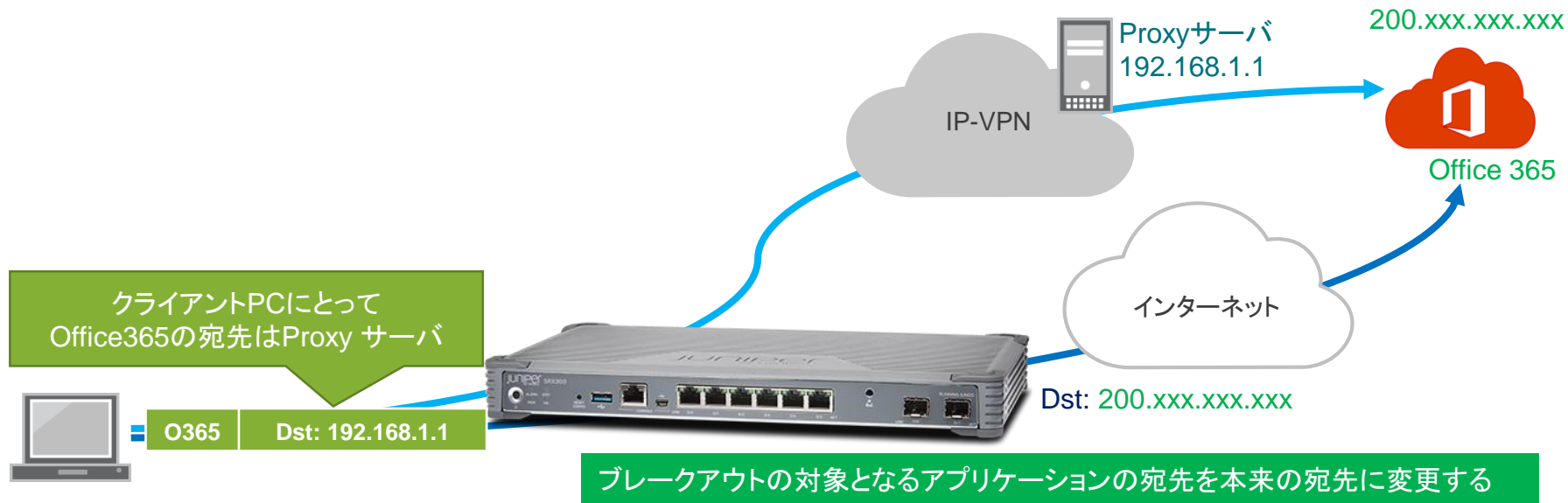
Proxyサーバを使用している環境ではクライアントはアプリケーションサーバのIPアドレスではなくProxyサーバのIPアドレスへ通信を開始する。

そのため、アプリケーションを判別して経路を変更しても通信が成立しない。



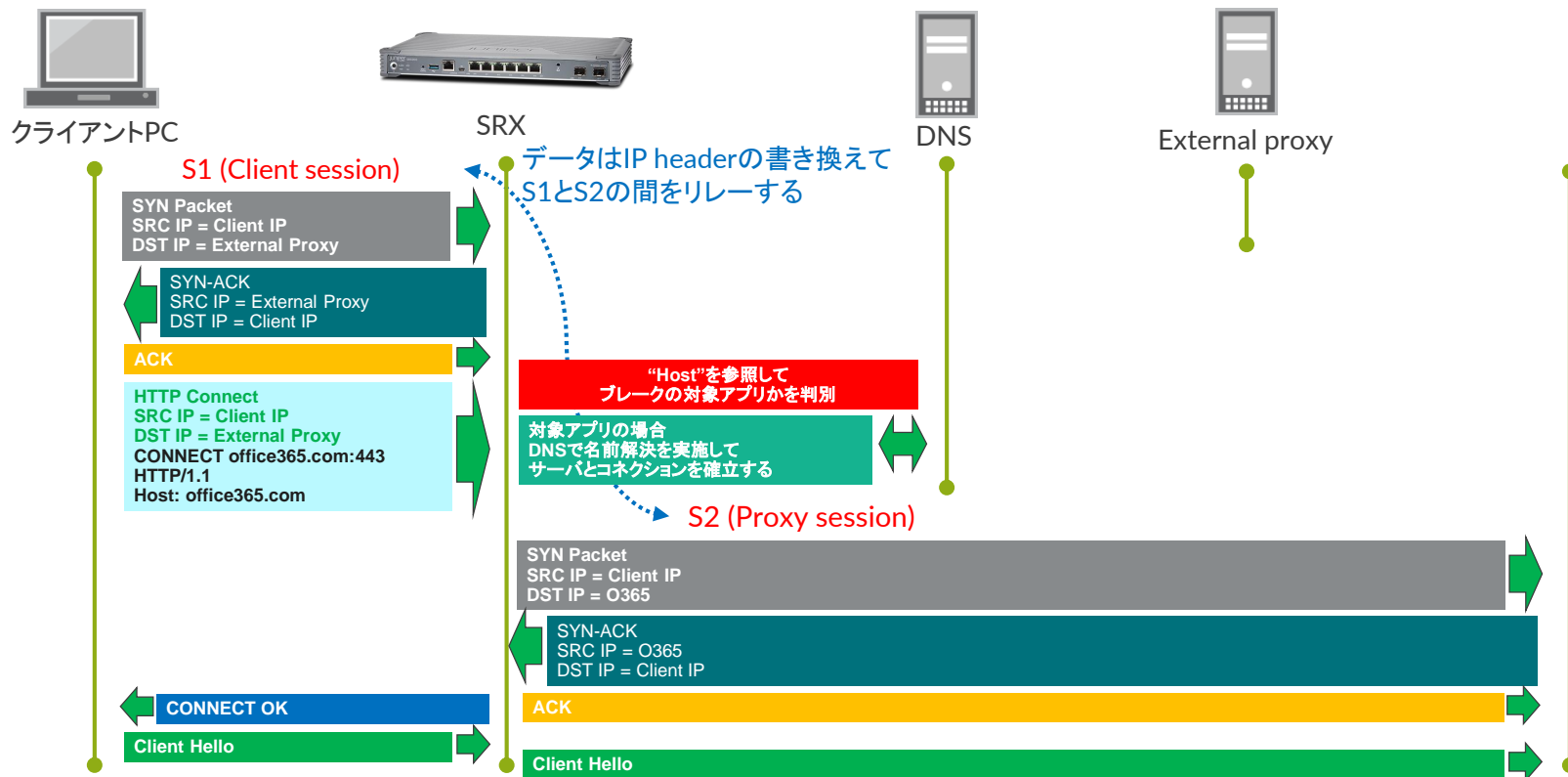
## ローカルブレイクアウトソリューションを導入できない原因の解決

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。

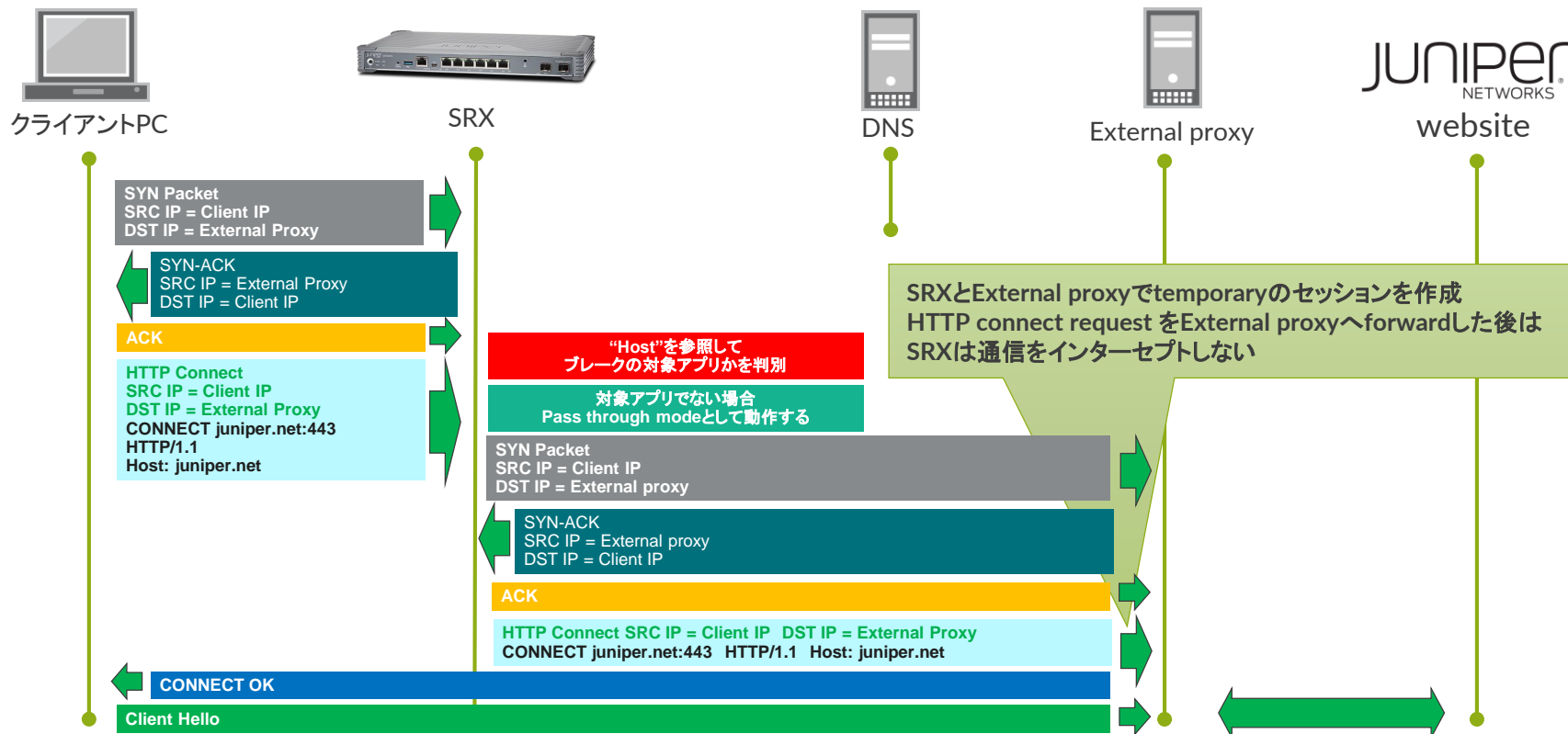




# ブレイクアウトを実施する際の動作



# ブレークアウトしない際の動作



# SRXが提供するセキュリティ機能

## 次世代ファイアウォール機能

アプリケーションの  
コントロールと可視化

侵入防御(IPS)

ユーザーベース  
ファイアウォール

## 統合脅威管理(UTM)

アンチウイルス

アンチスパム

ウェブフィルタリング

## 最新のセキュリティ情報

ボットネット/C&C

GEO-IP

カスタムフィード&  
ターゲット型攻撃

## アンチマルウェア アンチゼロデイ

サンドボックス

回避型マルウェア防御

レポートング&分析

## SRX 基本サービス

ファイアウォール

NAT(アドレス変換)

VPN  
(IPSec, SSL VPN)

冗長化  
クラスタリング

ルーティング  
(BGP, OSPF)

On Board GUI

MPLS






オートメーション

## 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 ?

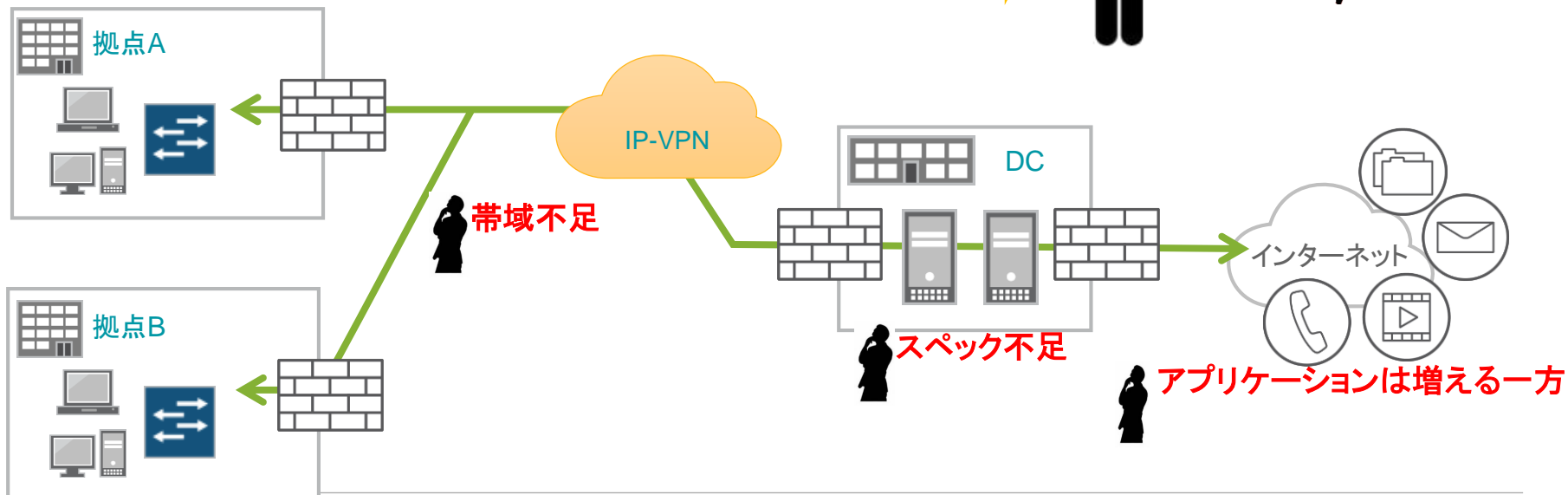
Summary View **Detail View**

				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

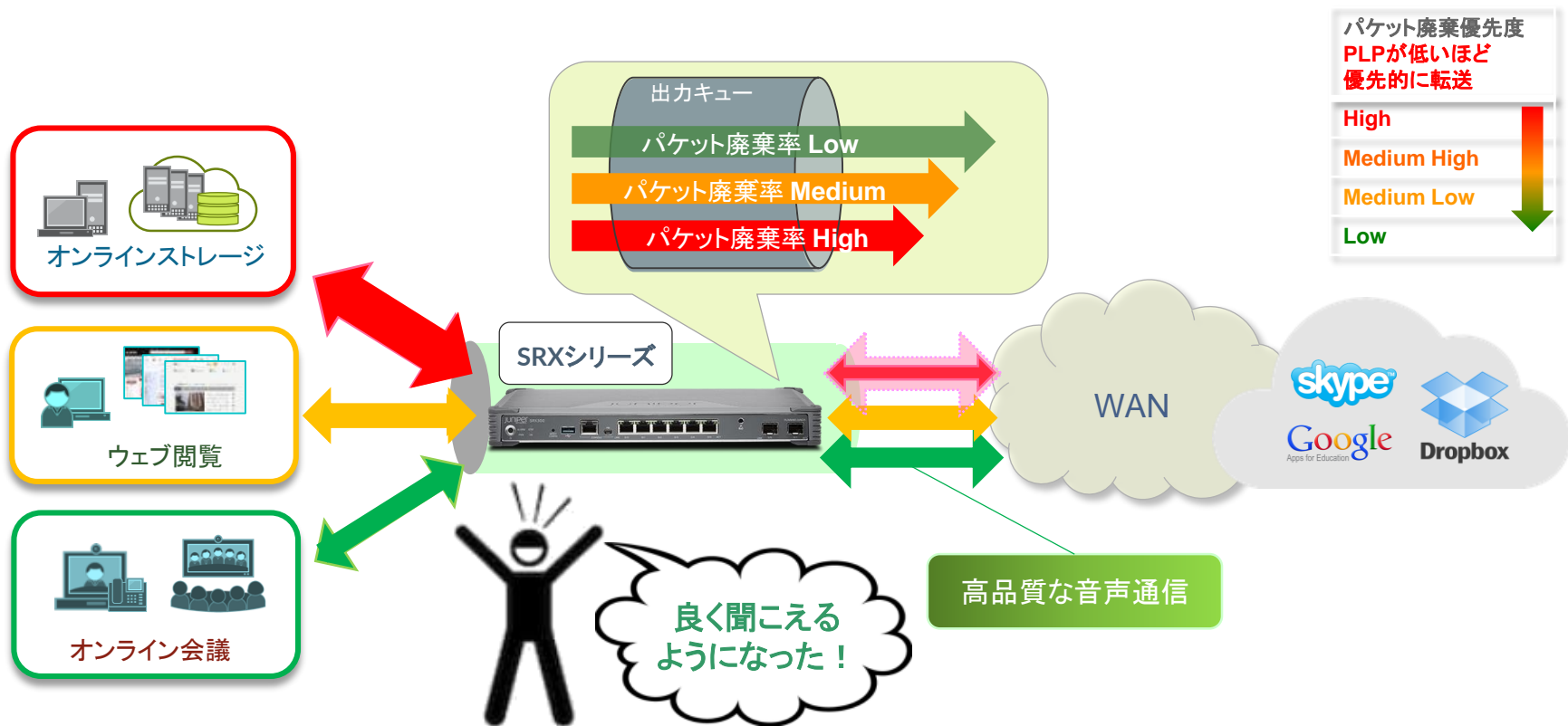
## ビデオ動画や音声通話が品質劣化する要因

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

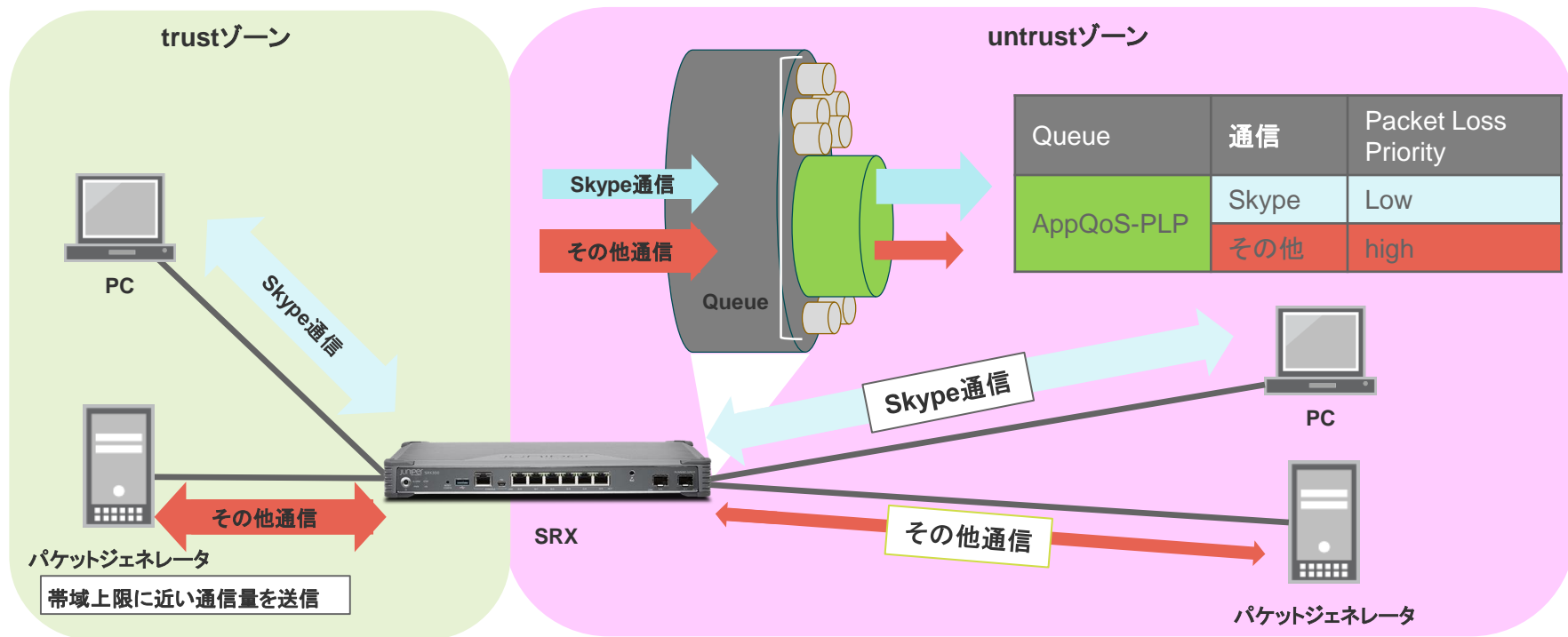


# リアルタイム性の高いアプリケーションを最優先させ通信を制御



# AppQoSデモ

帯域上限に近いトラフィックを送信し、Skypeビデオ映像の乱れを比較





## AppQoSデモ

---

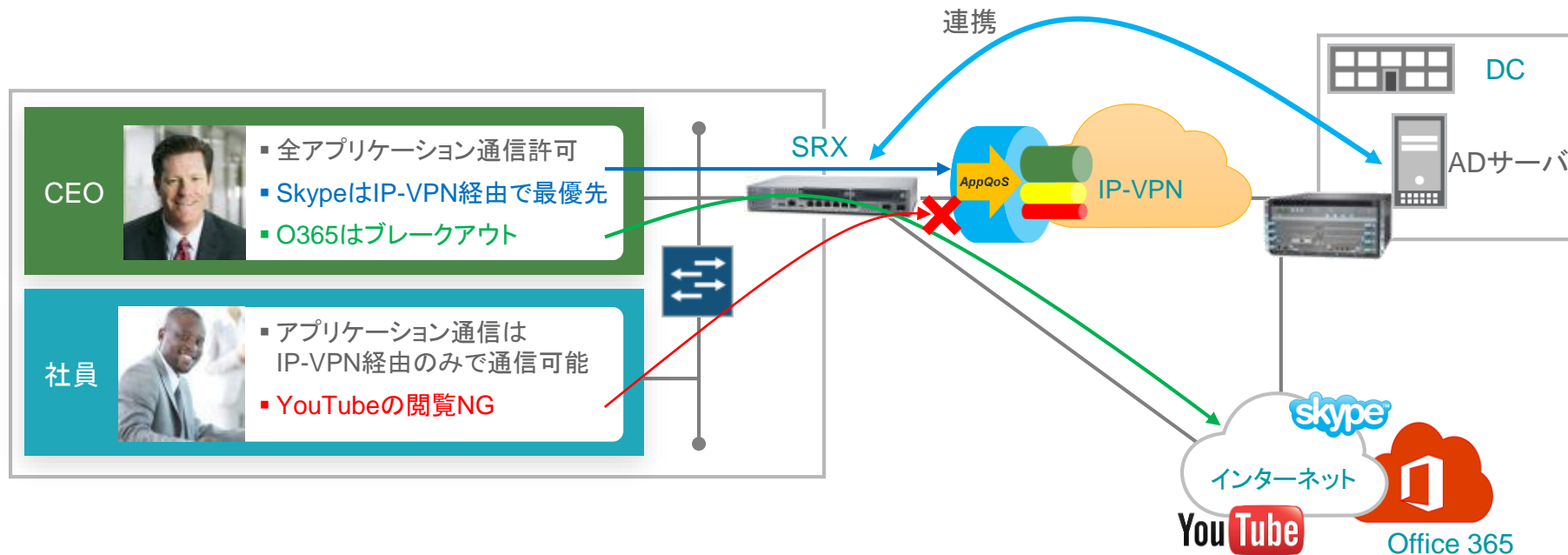
動画のリンクは下記を参照

<https://www.juniper.net/jp/jp/dm/security/>



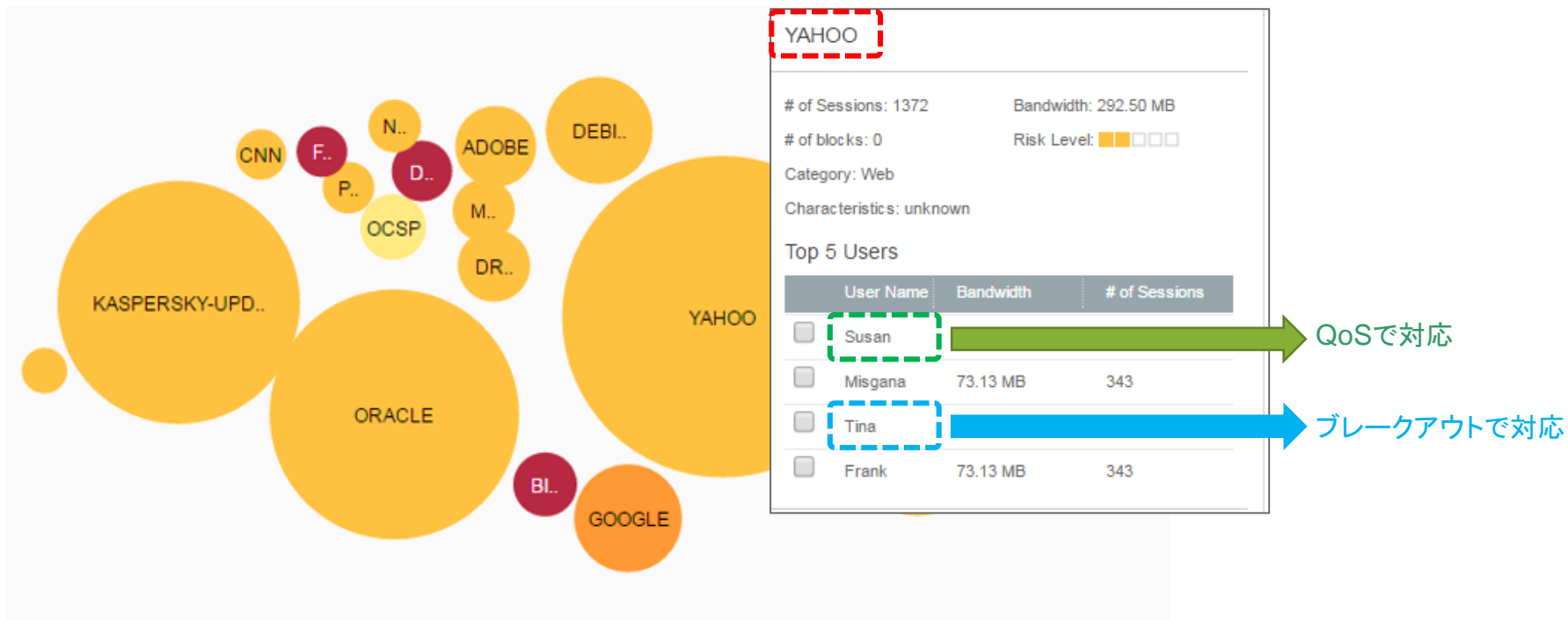
# ユーザベースのアプリケーション制御

ユーザ属性とアプリケーションを条件に通信を制御



# ユーザベースのアプリケーション制御

ユーザ属性とアプリケーションを条件に通信を制御

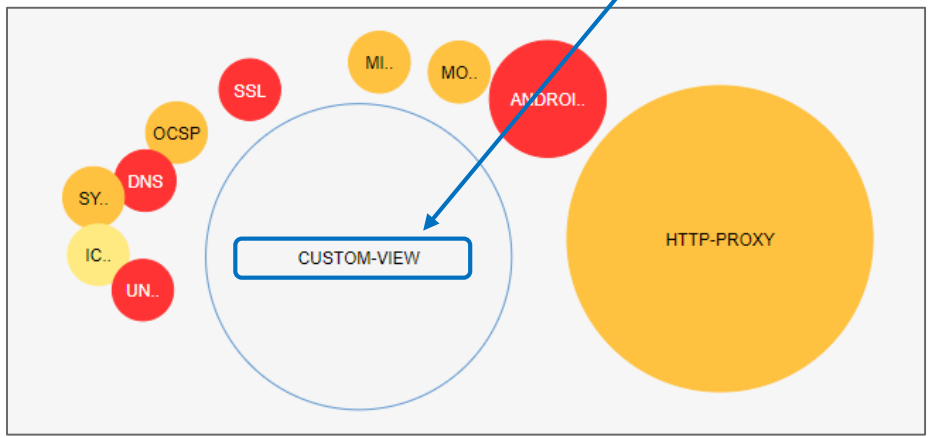


# カスタムアプリケーション

Juniper Networksが定義していないアプリケーションもユーザ側で個別に定義して制御することが可能



```
set services application-identification application CUSTOM-VIEW over SSL signature s1 member m01 context ssl-server-name
set services application-identification application CUSTOM-VIEW over SSL signature s1 member m01 pattern ".*\juniper.net*"
set services application-identification application CUSTOM-VIEW over SSL signature s1 member m01 direction client-to-server
```



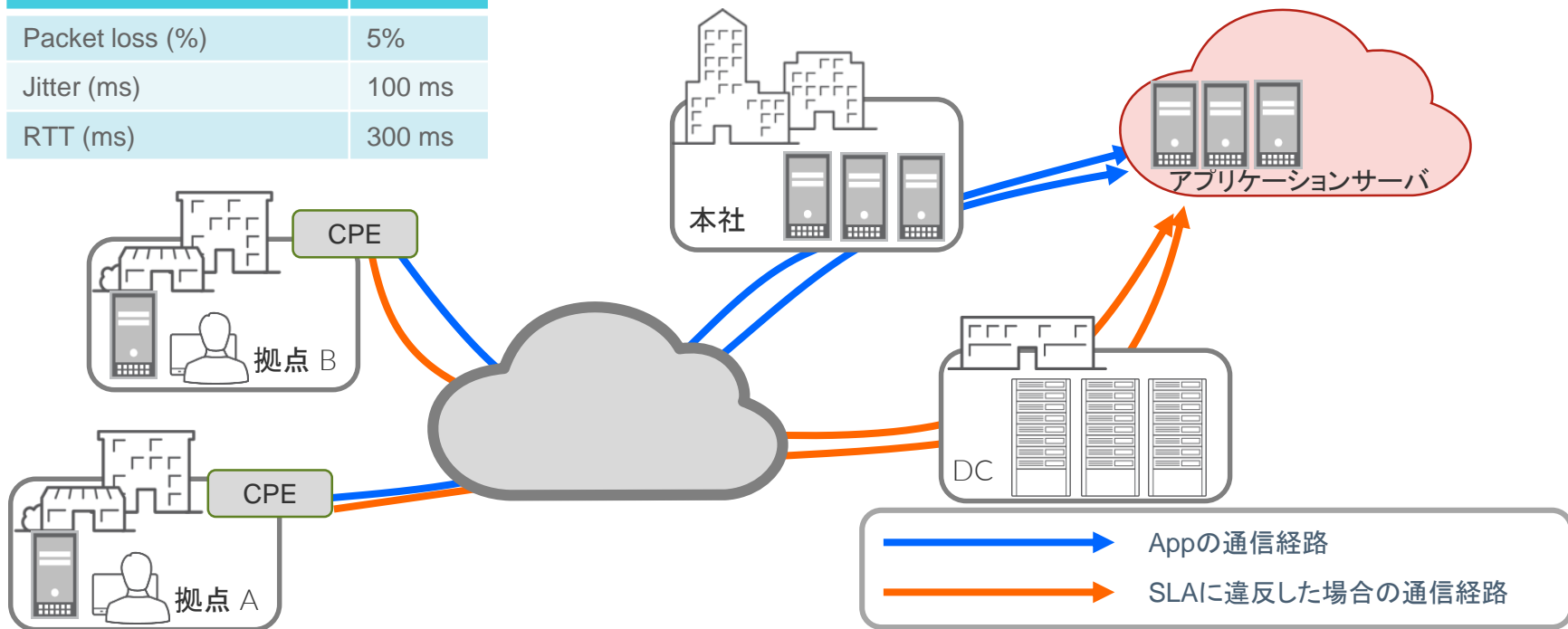


# アプリケーション通信の最適化

# 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

該当するアプリケーションがSLAに違反した場合、経路を変更する

SLA	Value
Packet loss (%)	5%
Jitter (ms)	100 ms
RTT (ms)	300 ms



# 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を定義

**SLA-Based Steering Profiles** [Watch and Learn](#)

SLA Profiles List More ▾ 🔍 🔼 ⋮

	Name	Traffic Type Profile	Packet Loss (%)	Jitter (ms)	RTT (ms)	Created By
<input type="checkbox"/>	CSO-Sec	INTERNET	5 %	100 ms	300 ms	System
<input type="checkbox"/>	CSO-Email	PREMIUM-INTERNET	5 %	100 ms	300 ms	System
<input type="checkbox"/>	CSO-Productive	PREMIUM-INTERNET	5 %	100 ms	300 ms	System
<input type="checkbox"/>	CSO-FileShare	INTERNET	5 %	100 ms	300 ms	System
<input type="checkbox"/>	CSO-AV	VOICE-VIDEO	1 %	30 ms	150 ms	System



# 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

該当する通信に紐づける

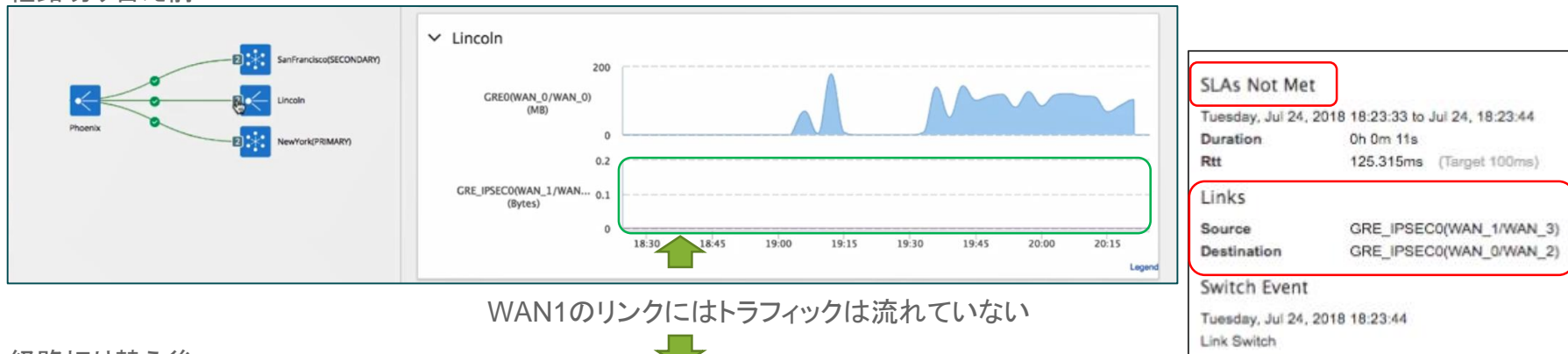
**SD-WAN Policy** [Watch and Learn](#) Last update approximately 18 days ago by admin Total Intents 5 Undeployed 5

NAME	SOURCE	APPLICATION	TRAFFIC STEERING PROFILE
> System-2	<b>SITE</b> All Sites	<b>APPS</b> CSO-Collaboration...	<b>SLA</b> CSO-Email
> System-1	<b>SITE</b> All Sites	<b>APPS</b> CSO-Collaboration...	<b>SLA</b> CSO-AV
> System-4	<b>SITE</b> All Sites	<b>APPS</b> CSO-File-Share	<b>SLA</b> CSO-FileShare
> System-3	<b>SITE</b> All Sites	<b>APPS</b> CSO-Productivity	<b>SLA</b> CSO-Productive
> System-5	<b>SITE</b> All Sites	<b>APPS</b> CSO-Security	<b>SLA</b> CSO-Sec

# 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

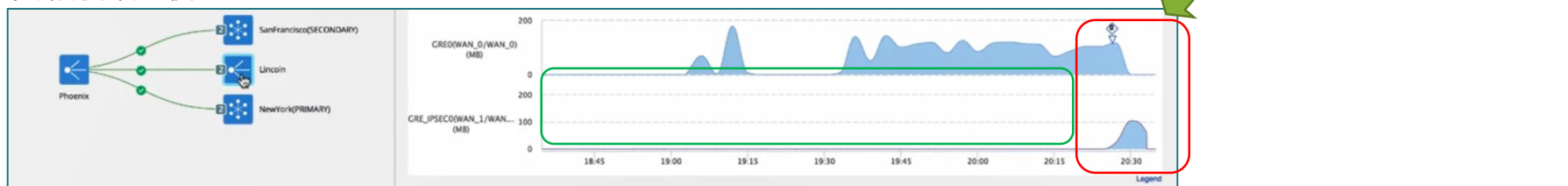
SLA違反を検知すると経路が切り替わる

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

# 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違反は時系列で確認可能



# 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

---

動画のリンクは下記を参照

[https://www.youtube.com/playlist?list=PLGvolzhkU\\_gR34Kxk\\_Qh5ONMtHXdDPEwk](https://www.youtube.com/playlist?list=PLGvolzhkU_gR34Kxk_Qh5ONMtHXdDPEwk)



## JUNIPER NETWORKSが提供するアプリケーション制御

---

- 可視化したトラフィックをほぼ100%有効活用できる。
- Proxy環境であってもブレイクアウトのソリューションを展開できる。
- お客様の環境、例えばProxyサーバのアドレスをSRXに変更する、などの変更は不要
- アプリケーションを識別するシグネチャをユーザ側で定義することができる
  - 4000種類以上あるアプリケーションで定義していない通信もユーザ側で個別に定義して制御することが可能
- アプリケーションコントロールはSRX単体が保有する機能。  
そのため、SD-WANコントローラーはあくまでオプション。
- SD-WANを検討したい場合、用途、規模に応じてコントローラーを選択できる
  - 簡易SD-WAN by Sky Enterprise, Full SD-WAN by CSO

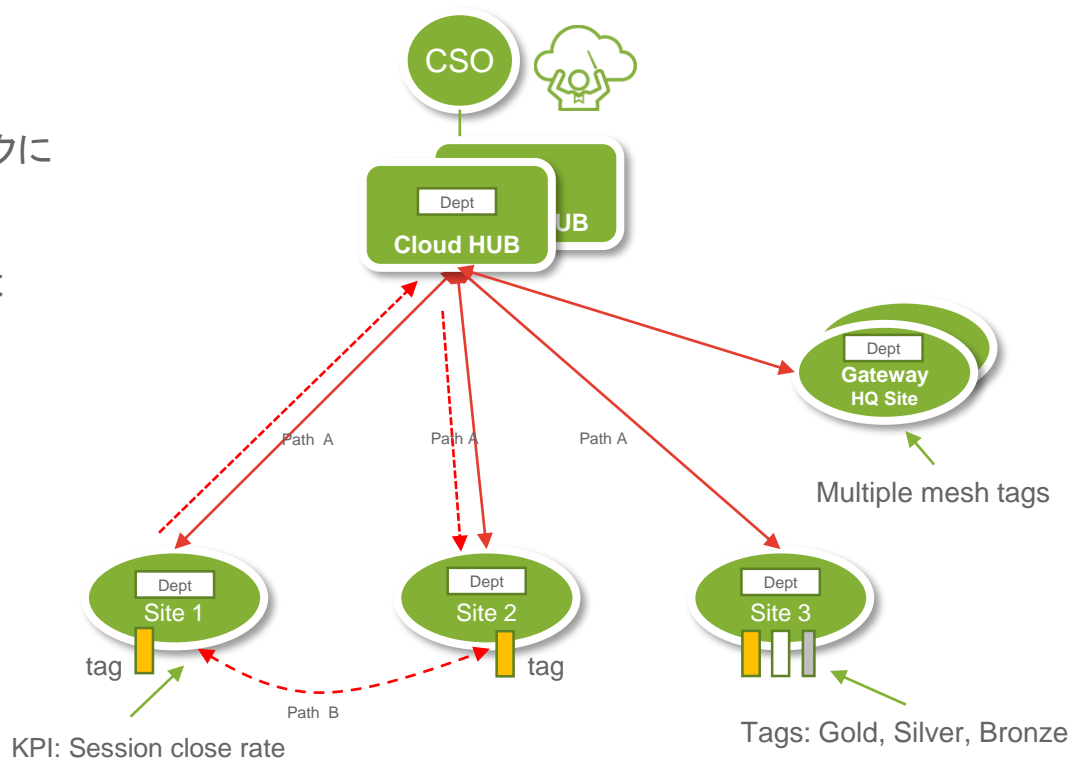


## Appendix

### 拠点間通信の最適化

# 拠点間の通信を最適化するダイナミックVPN

1. 拠点間通信はデフォルトではハブを経由
2. セッション数が閾値を超えるとダイナミックに拠点間でトンネルを自動作成
3. セッション数が閾値を下回るとトンネルは自動消滅





## 拠点間の通信を最適化するダイナミックVPN

---

動画のリンクは下記を参照

[https://www.youtube.com/playlist?list=PLGvolzhkU\\_gR34Kxk\\_Qh5ONMtHXdDPEwk](https://www.youtube.com/playlist?list=PLGvolzhkU_gR34Kxk_Qh5ONMtHXdDPEwk)





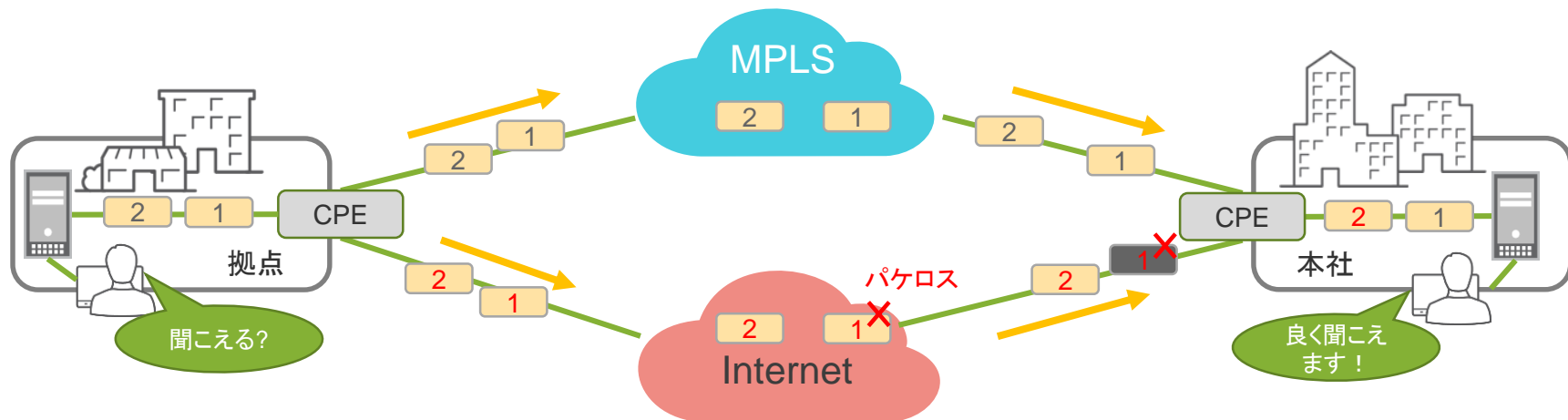
## Appendix


### 拠点間通信の品質向上

## 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





オンデマンドでネットワークサービスを瞬時に提供  
新型収益モデルSD-Branchとは  
～ 工数削減を実現する新たな収益モデルの活用術～

2019年9月24日

JUNIPER  
NETWORKS

Engineering  
Simplicity

## サービス事業者および提供者向けがSD-WANを必要とする理由

### 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

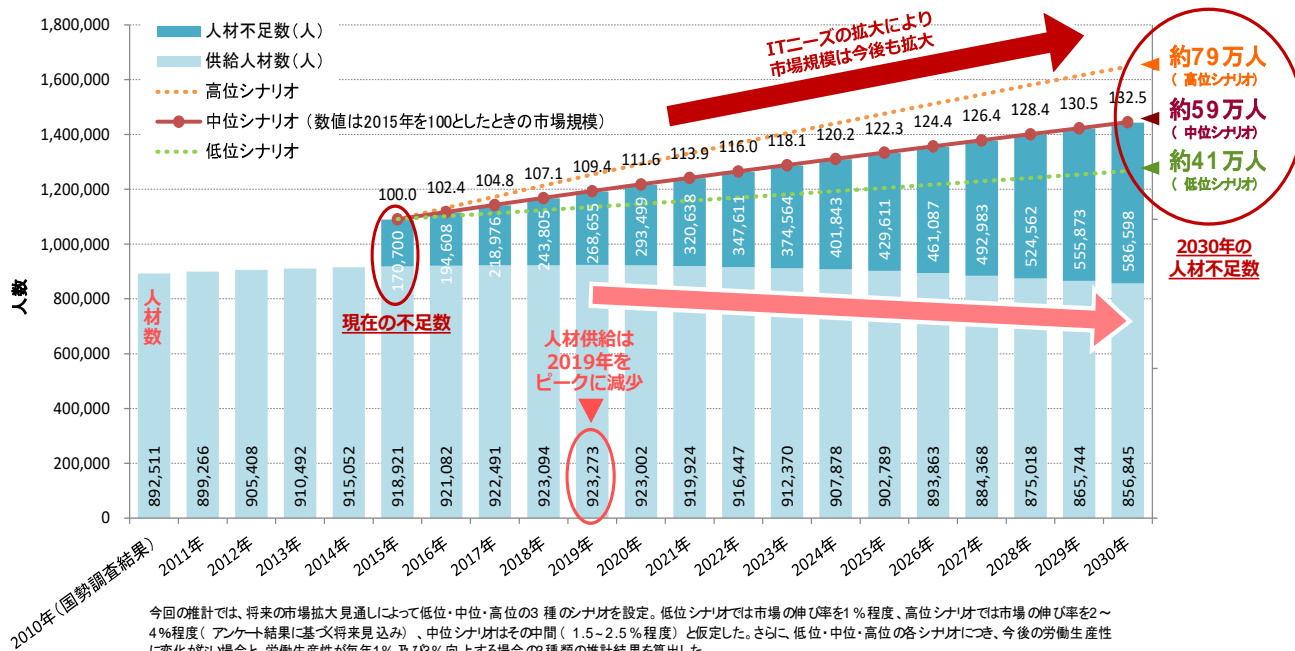
- クラウドアプリケーションを利用するユーザの体感を改善
- 拠点間通信の最適化

### 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(3<sup>rd</sup> パーティ-VNFをオンデマンドで提供)

# 日本におけるITエンジニアの現状

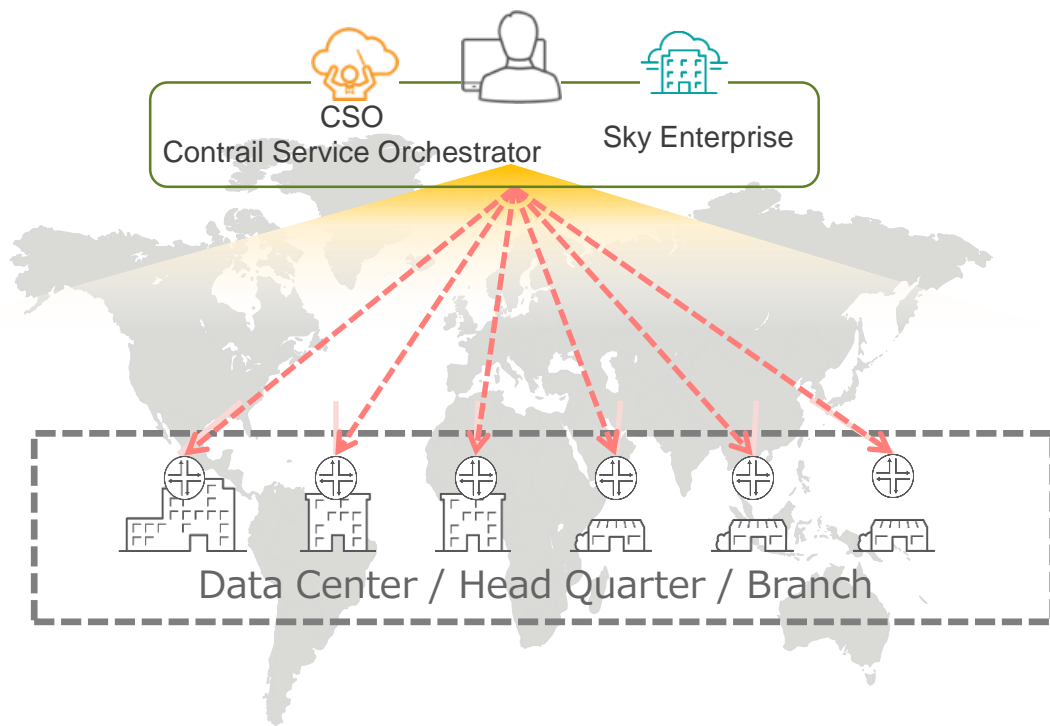
## IT技術者不足はこれからさらに深刻化



(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 平成28年6月

# SD-WANコントローラーによる自動化・統合管理

SD-WANコントローラーによる運用負荷の軽減が必要



従来の拠点毎の作業方式

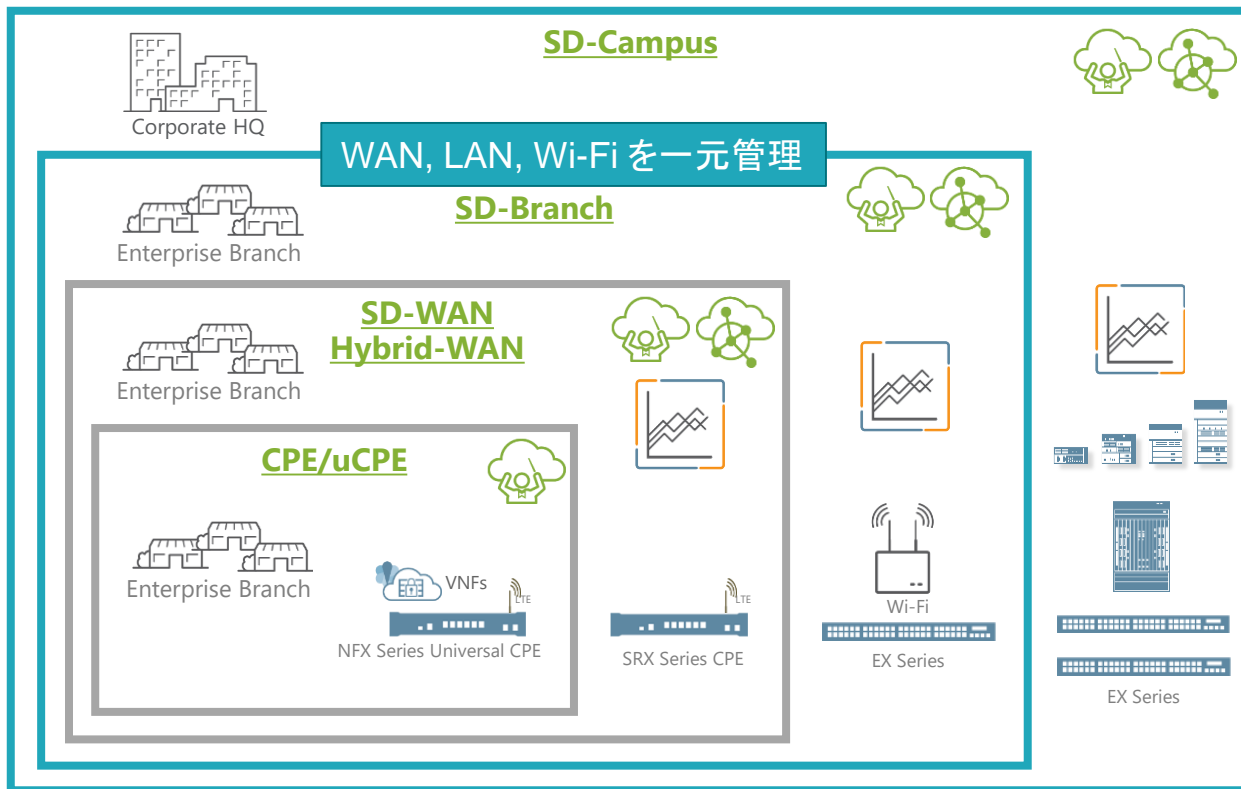
30分 x 拠点数(100) = 50時間

SD-WANコントローラーによる  
自動化・統合管理

10分 x 1(コントローラ) = 10分

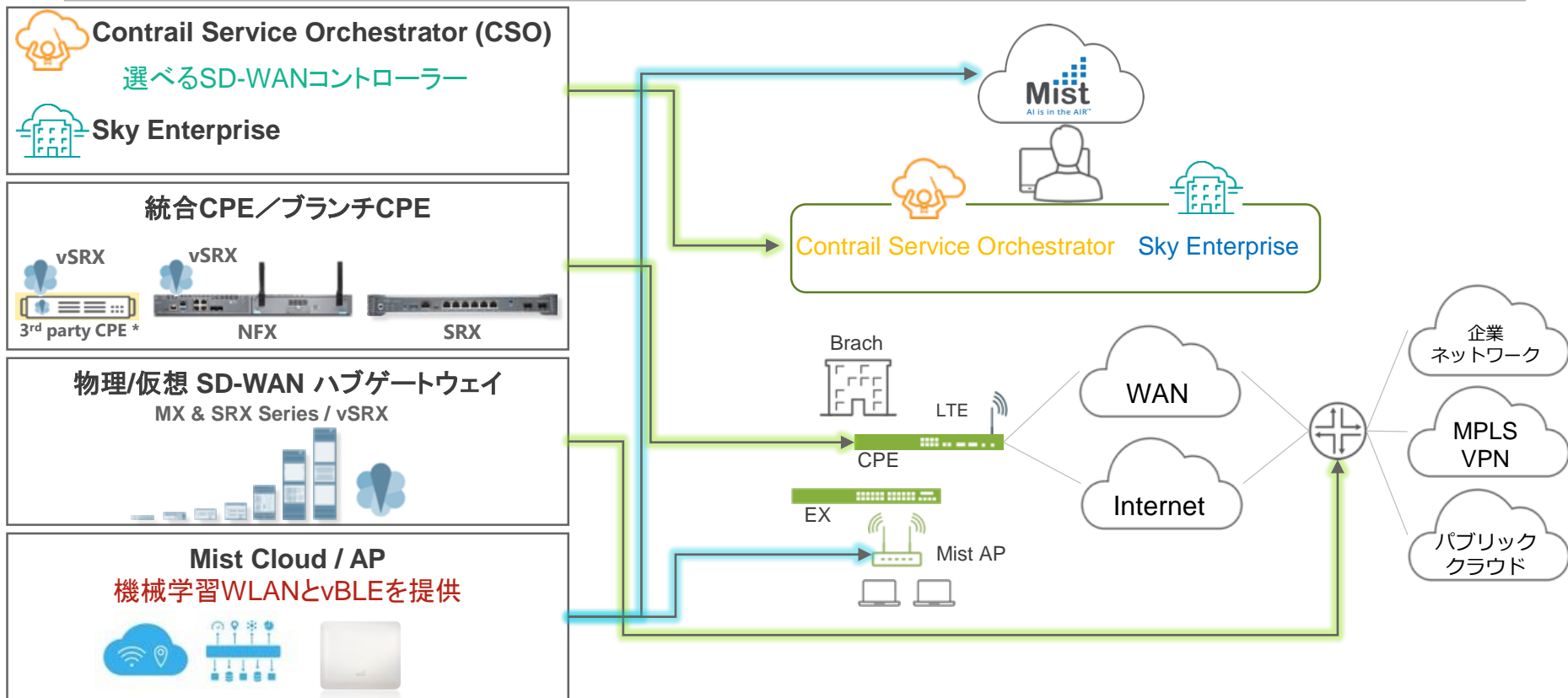


# SD-WANからSD-ENTERPRISEへ





# SD-BRANCH ソリューション コンポーネント





## 管理イメージ

# 管理イメージ (SKY ENTERPRISE)

機器の管理状況とあわせて地理分布の可視化。

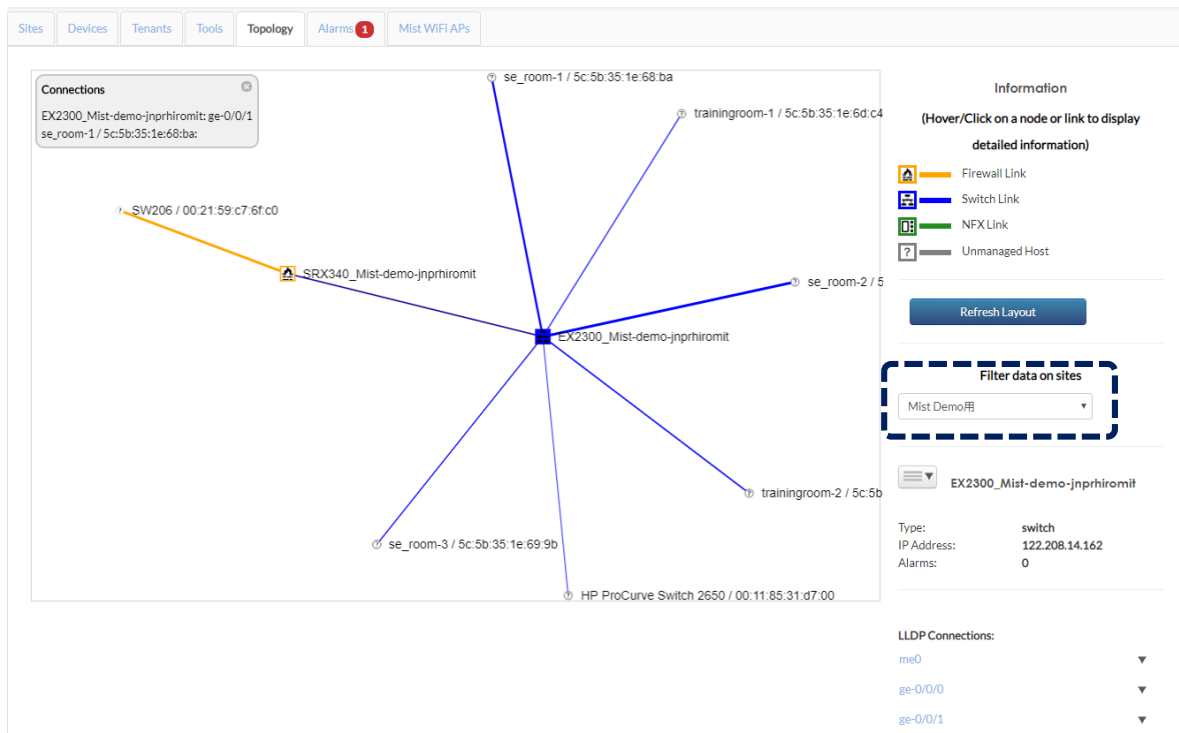
The screenshot displays the Juniper Mist Management interface. At the top, there is a navigation menu with options: Home, Services, Users, Configuration, Settings, and Support. The user is logged in as JNPR hiromit. The main content area is titled 'Sites' and includes sub-tabs for Devices, Tenants, Tools, Topology, Alarms (with a red notification icon), and Mist WiFi APs. A central map shows the location of three devices, with a blue circle and the number '3' indicating the total devices. To the right of the map, there are two summary gauges: 'Total Devices (Online/Offline): 3' shown as a green circle with '3' inside, and 'Total Alarms: 1' shown as a red circle with '1' inside. Below the map, there is a '+ New Site' button and a search bar. A table at the bottom, enclosed in a dashed blue border, lists the sites and their device counts:

Name	Devices (Connected/Offline)	Address
Secure-web-proxy Demo用	1/0	日本、〒163-1445 東京都新宿区西新宿 3丁目2 0-2 POC lab
Mist Demo用	2/0	日本、〒163-1445 東京都新宿区西新宿 3丁目2 0-2 Training Room

拠点一覧

# 管理イメージ (SKY ENTERPRISE)

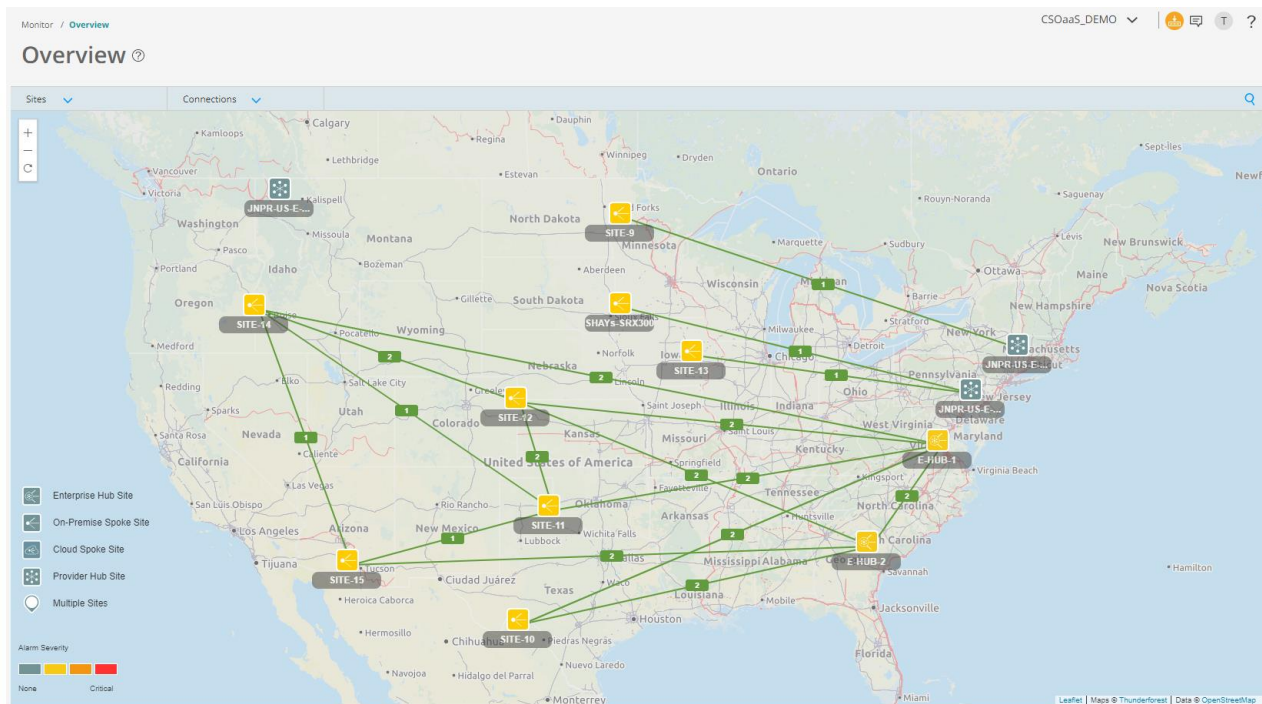
各サイトのネットワークレイアウトを動的に表示



拠点ごとのLAN構成

# 管理イメージ (CSO)

## 機器の管理状況とあわせて地理分布の可視化



# 管理イメージ (CSO)

各サイトのネットワークレイアウトを動的に表示

The screenshot displays the Juniper CSO Administration Portal interface. The main area shows a network topology diagram for a 'Create Site' configuration. The diagram is divided into two sections: SDWAN and LAN. In the SDWAN section, there are two WAN links: 'MPLS WAN Link WAN\_0' and 'Internet WAN Link WAN\_1', both connected to a central 'SRX 220' device. In the LAN section, an 'EX 150' switch is connected to the 'SRX 220' device. A '+ Add Devices' button is visible in the SDWAN section.

Overlaid on the right side of the screen is a configuration window for the 'EX 150' device, specifically the 'Port Mapping' tab. This window shows a grid of ports categorized into RJ-45 Ports, SFP Ports, and SFP+ Ports. Below the grid is a table mapping specific ports to roles.

Port	Role
ge-0/0/0	Voice
ge-0/0/1	VoIP
ge-0/0/2	Access Point
ge-0/0/3	Access Point
ge-0/0/4	Access Point
ge-0/0/5	Printer
ge-0/0/6	Printer
ge-0/0/7	PoE
ge-0/0/8	Management

## 設定変更作業の課題&解決



CLIでの設定はスキルが必要

GUIでの設定は1つの設定を反映させるために複数のメニューを変更する必要がある

設定したい項目がGUIに実装されていない

ダブルチェックにかかる工数が増大

設定変更後のレポート作成が面倒

## 設定変更作業の課題&解決

### ユースケース#1

各拠点にSecure-web-proxyの機能を追加してO365のトラフィックをローカルブレイクアウトさせる

ヒアリングシートの項目

設定項目 (拠点1)	パラメータ	設定項目 (拠点2)	パラメータ
既存のプロキシサーバのアドレス	192.168.1.100	既存のプロキシサーバのアドレス	192.168.2.100
既存のプロキシサーバのポート番号	8080	既存のプロキシサーバのポート番号	8080
ブレイクアウトの対象となるアプリケーション	office365-grp	ブレイクアウトの対象となるアプリケーション	office365-grp
インターネット回線のデフォルトゲートウェイ	122.xxx.xxx.32	インターネット回線のデフォルトゲートウェイ	122.xxx.xxx.59

ユーザ側で定義する項目は少ない





# 設定変更作業の課題&解決

## 実際に必要な設定項目

```
set services application-identification application-group office365-grp applications junos:EXCEL-ONLINE
set services application-identification application-group office365-grp applications junos:LYNC
set services application-identification application-group office365-grp applications junos:MICROSOFT
set services application-identification application-group office365-grp applications junos:MICROSOFT-LIVE-SERVICES
set services application-identification application-group office365-grp applications junos:MICROSOFT-UPDATE
set services application-identification application-group office365-grp applications junos:MS-ONENOTE
set services application-identification application-group office365-grp applications junos:MS-PLANNER
set services application-identification application-group office365-grp applications junos:MS-SWAY
set services application-identification application-group office365-grp applications junos:OFFICE-DOCS
set services application-identification application-group office365-grp applications junos:OFFICE365-CREATE-CONVERSATION
set services application-identification application-group office365-grp applications junos:ONEDRIVE
set services application-identification application-group office365-grp applications junos:OUTLOOK
set services application-identification application-group office365-grp applications junos:OWA
set services application-identification application-group office365-grp applications junos:POWER-BI
set services application-identification application-group office365-grp applications junos:POWERPOINT-ONLINE
set services application-identification application-group office365-grp applications junos:SHAREPOINT-ONLINE
set services application-identification application-group office365-grp applications junos:SKYPE
set services application-identification application-group office365-grp applications junos:WINDOWS-AZURE
set services application-identification application-group office365-grp applications junos:WINDOWS-MARKETPLACE
set services application-identification application-group office365-grp applications junos:WORD-ONLINE
set services application-identification application-group office365-grp applications junos:YAMMER
set services web-proxy secure-proxy profile office365-proxy proxy-address external_proxy ip ProxyServerIPaddress
set services web-proxy secure-proxy profile office365-proxy proxy-address external_proxy port ProxyPort
set services web-proxy secure-proxy profile office365-proxy dynamic-web-application-group Application
set security address-book global address PROXY-SERVER ProxyServerIPaddress
```

運用者が設定する項目は多い



## 設定変更作業の課題&解決

### 実際に必要な設定項目(続き)

```
set security application-tracking
set security advance-policy-based-routing tunables max-route-change 0
set security advance-policy-based-routing profile office365-local-breakout rule r01 match dynamic-application-group Application
set security advance-policy-based-routing profile office365-local-breakout rule r01 then routing-instance APBR
set security advance-policy-based-routing from-zone Trust policy NON-PROXY match source-address any
set security advance-policy-based-routing from-zone Trust policy NON-PROXY match destination-address PROXY-SERVER
set security advance-policy-based-routing from-zone Trust policy NON-PROXY match destination-address-excluded
set security advance-policy-based-routing from-zone Trust policy NON-PROXY match application any
set security advance-policy-based-routing from-zone Trust policy NON-PROXY then application-services advance-policy-based-routing-profile office365-local-breakout
set routing-instances APBR instance-type forwarding
set routing-instances APBR routing-options static route 0.0.0.0/0 next-hop GWIPaddress
set routing-options interface-routes rib-group inet RIB_GROUP
set routing-options rib-groups RIB_GROUP import-rib inet.0
set routing-options rib-groups RIB_GROUP import-rib APBR.inet.0
```

設定が複雑なためスキルのある運用者でないと設定が難しい。  
設定変更のダブルチェックに時間がかかる。。  
複数拠点に設定を反映させるにはさらに時間を要する。。。



## 設定変更作業の課題&解決

---

### テンプレート運用による設定変更作業のフロー

- 1: テンプレートを適用させる対象を選択。対象はデバイス、拠点、Tag単位で選択可能。
- 2: 適用するテンプレートを選択
- 3(オプション): 設定を反映させる日時を指定
- 4: デバイスごとに異なる変数を入力
- 5: 設定変更後のレポートを作成

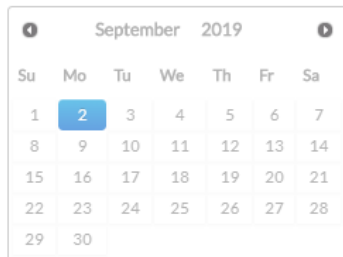
## 設定変更作業の課題&解決

1: テンプレートを適用させる対象を選択。対象はデバイス、拠点、Tag単位で選択可能

### New Bulk Update

Schedule update?

Yes No



Select Devices ▼ Input type: Basic Advanced

	Add all	1 items selected	Remove all
Device: EX2300_Mist-demo	+	↕ Tag: DeviceA	-
Device: SRX340_Mist-demo	+		
Device: SRX345_SWP	+		
Site: Mist Demo用	+		
Site: Secure-web-proxy Demo用	+		

Please select

各CPE FWには"DeviceA"といったタグを紐づけている  
この場合、各拠点のCPE FWを選択していることと同義

# 設定変更作業の課題&解決

## 2: 適用するテンプレートを選択

**New Bulk Update**

Schedule update? **Yes** **No** Select Devices ▼

September 2019

Su	Mo	Tu	We	Th	Fr	Sa
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

Please select a time: 00:00 ?

Input type: **Basic** **Advanced**

Select a template:

- Branch template ▼
- Branch template
- Google-Suite
- Poxy環境におけるローカルブレイクアウトの設定**
- Secure-web-proxy

## 設定変更作業の課題&解決

### 3(オプション): 設定を反映させる日時を指定

#### New Bulk Update

Schedule update?

Yes No

Select Devices ▼

August 2019						
Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

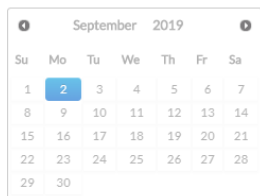


Please select a time:

00:00 ▼ ?

# 設定変更作業の課題&解決

## 4: デバイスごとに異なる変数を入力



Please select a time: 00:00

Select a template: Poxy環境におけるローカルプレ



選択されたテンプレート

Update input:

Tag: DeviceAに紐づいたデバイス

Input format: **Inputs** Table

SRX340_Mist-demo-jnprhiromit variables:			
ProxyServerIpAddress	192.168.1.100	ProxyPort	8080
Application	office365-grp	GWIPaddress	122.xxx.xxx.163

SRX345_SWP-jnprhiromit variables:			
ProxyServerIpAddress	192.168.2.100	ProxyPort	
Application		GWIPaddress	

ヒアリングシートの内容を入力するだけ  
ダブルチェックも簡単



# 設定変更作業の課題&解決

## 拠点1に反映された設定

```
set services application-identification application-group office365-grp applications junos:EXCEL-ONLINE
set services application-identification application-group office365-grp applications junos:LYNC
set services application-identification application-group office365-grp applications junos:MICROSOFT
set services application-identification application-group office365-grp applications junos:MICROSOFT-LIVE-SERVICES
set services application-identification application-group office365-grp applications junos:MICROSOFT-UPDATE
set services application-identification application-group office365-grp applications junos:MS-ONENOTE
set services application-identification application-group office365-grp applications junos:MS-PLANNER
set services application-identification application-group office365-grp applications junos:MS-SWAY
set services application-identification application-group office365-grp applications junos:OFFICE-DOCS
set services application-identification application-group office365-grp applications junos:OFFICE365-CREATE-CONVERSATION
set services application-identification application-group office365-grp applications junos:ONEDRIVE
set services application-identification application-group office365-grp applications junos:OUTLOOK
set services application-identification application-group office365-grp applications junos:OWA
set services application-identification application-group office365-grp applications junos:POWER-BI
set services application-identification application-group office365-grp applications junos:POWERPOINT-ONLINE
set services application-identification application-group office365-grp applications junos:SHAREPOINT-ONLINE
set services application-identification application-group office365-grp applications junos:SKYPE
set services application-identification application-group office365-grp applications junos:WINDOWS-AZURE
set services application-identification application-group office365-grp applications junos:WINDOWS-MARKETPLACE
set services application-identification application-group office365-grp applications junos:WORD-ONLINE
set services application-identification application-group office365-grp applications junos:YAMMER
set services web-proxy secure-proxy profile office365-proxy proxy-address external_proxy ip 192.168.1.100/32
set services web-proxy secure-proxy profile office365-proxy proxy-address external_proxy port 8080
set services web-proxy secure-proxy profile office365-proxy dynamic-web-application-group office365-grp
set security address-book global address PROXY-SERVER 192.168.1.100/32
```



## 設定変更作業の課題&解決

### 拠点1に反映された設定(続き)

```
set security application-tracking
set security advance-policy-based-routing tunables max-route-change 0
set security advance-policy-based-routing profile office365-local-breakout rule r01 match dynamic-application-group office365-grp
set security advance-policy-based-routing profile office365-local-breakout rule r01 then routing-instance APBR
set security advance-policy-based-routing from-zone Trust policy NON-PROXY match source-address any
set security advance-policy-based-routing from-zone Trust policy NON-PROXY match destination-address PROXY-SERVER
set security advance-policy-based-routing from-zone Trust policy NON-PROXY match destination-address-excluded
set security advance-policy-based-routing from-zone Trust policy NON-PROXY match application any
set security advance-policy-based-routing from-zone Trust policy NON-PROXY then application-services advance-policy-based-routing-profile office365-local-breakout
set routing-instances APBR instance-type forwarding
set routing-instances APBR routing-options static route 0.0.0.0/0 next-hop 122.xxx.xxx.32
set routing-options interface-routes rib-group inet RIB_GROUP
set routing-options rib-groups RIB_GROUP import-rib inet.0
set routing-options rib-groups RIB_GROUP import-rib APBR.inet.0
```

実際には複雑な設定が投入されているが、運用者が設定しているのは赤字の変数のみ



# 設定変更作業の課題&解決

## 5: 設定変更後のレポートを作成

### Bulk Update Report

Summary

1 device success updates  
0 device errors

1 Device

Input

Log

Download PDF Close

1 / 1

### Bulk Update Report for JNPR hiromit

OneConfig  
Report Generated on 30/08/2019 16:01

Summary

1 device success updates  
0 device errors

1 Device

SRX340-jnprhiromit

Input

```
SRX340-jnprhiromit
set groups TEST system host-name TESTset groups TEST system time-zone Asia/Tokyo
set groups TEST system dump-on-panicset groups TEST system root-authentication encrypted-
password "$1$Y:XXW4H1t50RyOfagB/wMKbVM1zGH"/set groups TEST system name-server 208.67.222.22set groups TEST system name-server 208.67.220.220set groups TEST
system login user lab uid 2000set groups TEST system login user lab class super-userset groups TEST system login user lab authentication encrypted-password lab123set groups TEST
system services ftpset groups TEST system services ssh root-login allowset groups TEST system services ssh protocol-version v2set groups TEST system services telnetset groups TEST
system services netconf sshset groups TEST system services web-management http interface allset groups TEST system syslog archive size 100kset groups TEST system syslog archive
files 10set groups TEST system syslog user * any emergencysset groups TEST system syslog file messages any noticeset groups TEST system syslog file messages authorization infose
groups TEST system syslog file interactive-commands anyset groups TEST system syslog file all.log any anyset groups TEST system syslog file sessions user
infose groups TEST system syslog file sessions match RT_FLOWset groups TEST system max-configurations-on-flash 5set groups TEST system max-configuration-rollback 5set groups
TEST system license autoupdate url https://ae1.juniper.net/junos/key_retrievalset groups TEST system ntp boot-server 172.27.112.1set groups TEST system ntp server 172.27.112.1set
groups TEST chassis dump-on-panicset groups TEST interfaces fxp0 unit 0 family inet address 172.27.113.104/22set groups TEST snmp community publicset groups TEST snmp trap-
options source-address 172.27.113.104set groups TEST snmp trap-group POC targets 172.27.112.1set groups TEST routing-options static route 0.0.0.0/0 next-hop 172.27.112.1set
groups TEST routing-options static route 0.0.0.0/0 no-advertise
```

Log

```
2019-06-26 18:15 All Devices: started update
2019-06-26 18:15 SRX340-jnprhiromit: executing update
2019-06-26 18:16 SRX340-jnprhiromit: committed changes
2019-06-26 18:16 SRX340-jnprhiromit: completed update
2019-06-26 18:16: update complete
```

実際に反映された設定内容とログを  
PDFでレポート



## 設定変更作業の課題&解決

### テンプレートの作成方法

```
set services web-proxy secure-proxy profile office365-proxy proxy-address external_proxy ip {{ ProxyServerIPAddress }}
set services web-proxy secure-proxy profile office365-proxy proxy-address external_proxy port {{ ProxyPort }}
set services web-proxy secure-proxy profile office365-proxy dynamic-web-application-group {{Application }}
set routing-instances APBR routing-options static route 0.0.0.0/0 next-hop {{GWIPaddress}}
```

set xxxxxxxx

その他、固定値はそのまま入力

ユーザ個別のパラメータを{}で囲うだけ



{ }で囲った項目がSky EnterpriseのGUIに反映される

ProxyServerIPAddress

ProxyPort

Application

GWIPaddress

## 設定変更作業の課題&解決

---

### ユースケース#2

ローカルブレイクアウトの対象にG-Suiteを加えたい

ヒアリングシートの項目

設定項目 (拠点1)	パラメータ	設定項目 (拠点2)	パラメータ
ブレイクアウトの対象となるアプリケーション	Gsuite	ブレイクアウトの対象となるアプリケーション	Gsuite

# 設定変更作業の課題&解決

**New Bulk Update**

Schedule update?  Yes  No

Select Devices:  Add all 1 items selected Remove all

Device: EX2300\_Mist-demo +  
Device: SRX340\_Mist-demo +  
Device: SRX345\_SWP +  
Site: Mist Demo用 +  
Site: Secure-web-proxy Demo用 +

Input type: Basic  Advanced

Template: Google-Suite

G-Suiteを定義したテンプレート

テンプレートの適用先は全拠点のCPE FW

Update input:  Inputs  Table

No input required

拠点ごとに異なる設定は存在しないため "No input required" と表示される

```
set services application-identification application-group Gsuite applications junos:GMAIL
set services application-identification application-group Gsuite applications junos:GMAIL-BASIC
set services application-identification application-group Gsuite applications junos:GMAIL-DRIVE
set services application-identification application-group Gsuite applications junos:GMAIL-MOBILE
set services application-identification application-group Gsuite applications junos:GOOGLE
set services application-identification application-group Gsuite applications junos:GOOGLE-ACCOUNTS
set services application-identification application-group Gsuite applications junos:GOOGLE-ADSERVICES-SSL
set services application-identification application-group Gsuite applications junos:GOOGLE-ANALYTICS-TRACKING
set services application-identification application-group Gsuite applications junos:GOOGLE-APPENGINE
set services application-identification application-group Gsuite applications junos:GOOGLE-CACHE
set services application-identification application-group Gsuite applications junos:GOOGLE-CALENDAR
```

設定を反映

Cancel Update



## CSOだけの機能紹介

# WANの構成管理

The screenshot displays the Juniper CSO Customer Portal interface for 'Tenant\_A'. The left sidebar contains navigation options: Overview, Alerts & Alarms, Link Switch Events, Traffic Logs, Security Events, Application SLA, Application Visibility, Threat Map (Live), and Jobs. The main content area shows the 'Overview' page with a 'Sites By Status' widget indicating 3 sites are PROVISIONED. Below this, a map of Japan is shown with a 'Links (Saga to Kyoto)' popup window. The popup displays the current status of the GRE\_IPSEC0 link as 'Up' and lists top applications by utilization: G, HTTP, and An. A table below the popup shows columns for Current Status, Start Time, End Time, and Uptime. The map also includes a legend for Alarm Severity (None, Critical) and a search bar.

CSO CUSTOMER PORTAL Tenant\_A cspadmin

Monitor / Overview

Overview

Sites By Status

3 PROVISIONED

Sites Connections

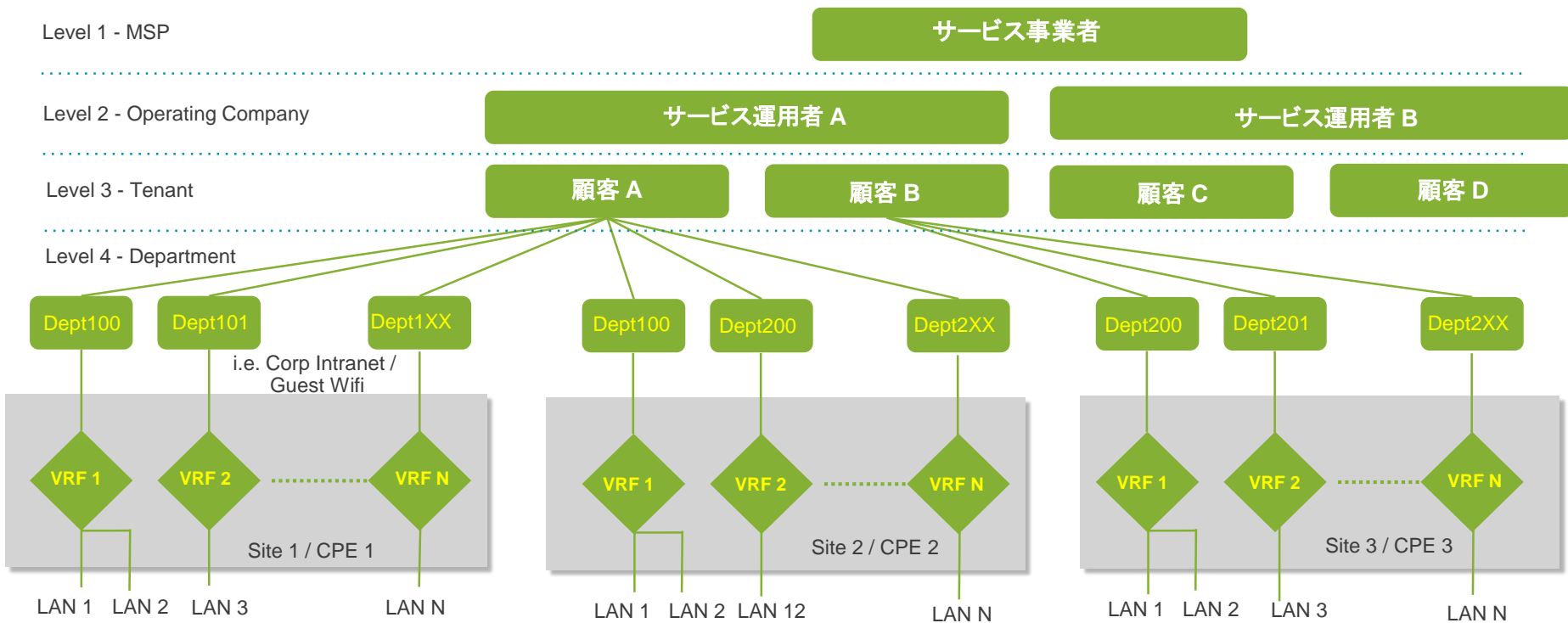
Links (Saga to Kyoto)

Current Status	Link Score	Top Applications by Utilization
Data GRE_IPSEC0 (WAN_0/WAN_0)	N/A	G HTTP An Un Dr

Current Status	Start Time	End Time	Uptime
<a href="#">More info</a>			

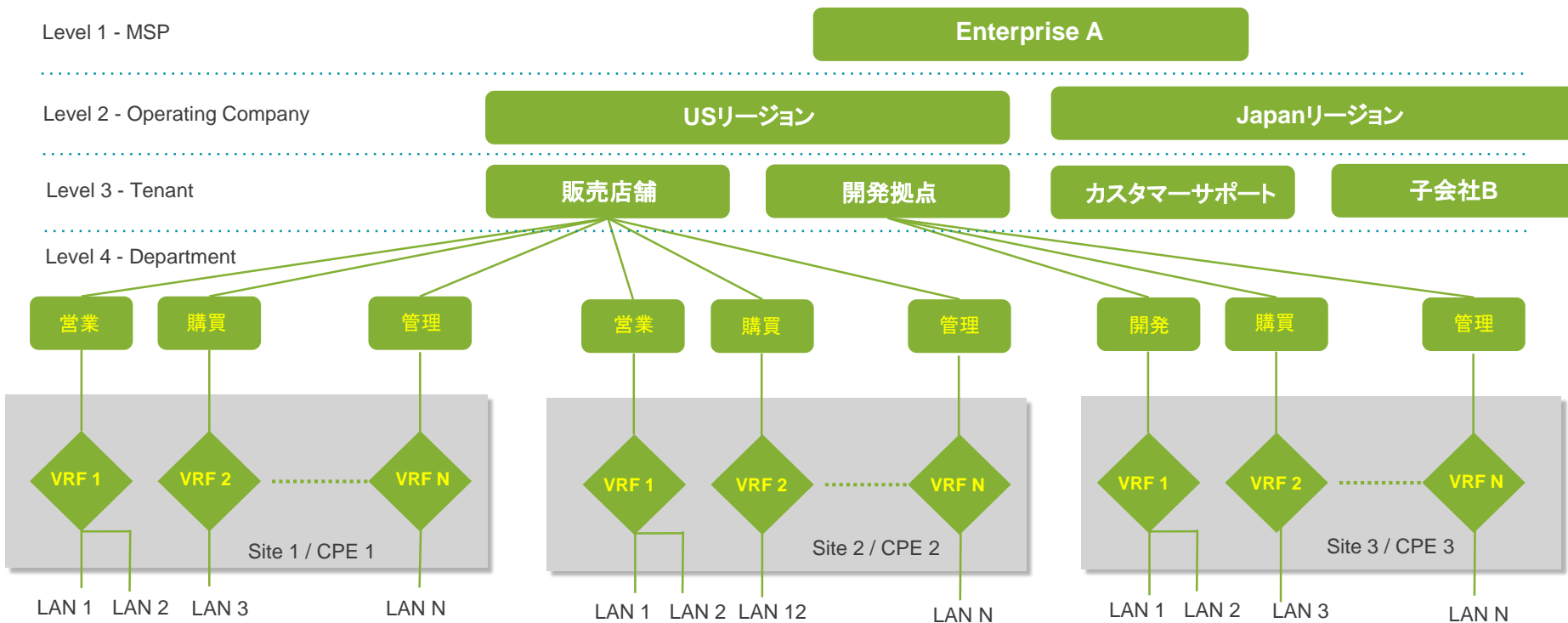
Leaflot | Maps © Thunderforest | Data © OpenStreetMap

# マルチテナント対応 (サービス事業者および提供者向け)





# マルチテナント対応 (エンタープライズ向け)



# ユーザロールごとの権限を設定

## Add Role ②

Role Name\* ②

Daytime Operator

Description

Role Scope ②

Service Provider

Access Privileges\* ②

<input type="checkbox"/>	Objects	<input type="checkbox"/>	Read	<input type="checkbox"/>	Create	<input type="checkbox"/>	Update	<input type="checkbox"/>	Delete	Other actions
<input type="checkbox"/>	> Monitor									
<input type="checkbox"/>	> Resources									
<input checked="" type="checkbox"/>	> Configuration									
<input checked="" type="checkbox"/>	Tenants	<input type="checkbox"/>		<input type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/>	OpCos	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		
<input type="checkbox"/>	> Administration									
33 items										

ユーザに割り当てる権限の名称

前/前々のスライドで説明のLevel 1に該当する権限

### Daytime Operatorの権限

- ✓ OpCoの閲覧、追加
- ✓ Tenantの変更、削除

Cancel

OK

# ユーザロールごとの権限を設定

ユーザごとに階層レベルに応じた権限を付与することでマルチテナンシーを実現

**Users** ⓘ

User List

	Username	First Name	Last Name	Status	Role	Last Login
<input type="checkbox"/>				✓ Enabled	Tenant Operator	2019-09-06 17:31:56
<input type="checkbox"/>				✓ Enabled	Tenant Operator	2019-07-24 06:56:16
<input type="checkbox"/>				✓ Enabled	Tenant Operator	2019-09-04 13:37:11
<input type="checkbox"/>				✓ Enabled	Tenant Operator	2019-08-21 07:11:30
<input type="checkbox"/>	ttakezawa@juniper.net	Taichi	Takezawa	✓ Enabled	Daytime Operator	2019-09-08 01:21:37
<input type="checkbox"/>				✓ Enabled	Tenant Operator	2019-09-07 20:50:20

**Daytime Operatorの権限**

- ✓ OpCoの閲覧、追加
- ✓ Tenantの変更、削除

## マルチテナント対応

---

動画のリンクは下記を参照

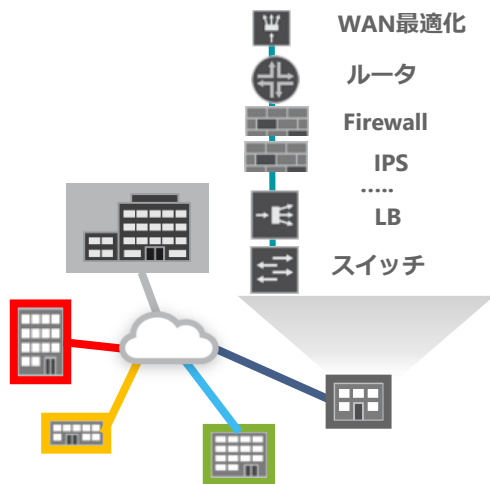
[https://www.youtube.com/playlist?list=PLGvolzhkU\\_gR34Kxk\\_Qh5ONMtHXdDPEwk](https://www.youtube.com/playlist?list=PLGvolzhkU_gR34Kxk_Qh5ONMtHXdDPEwk)



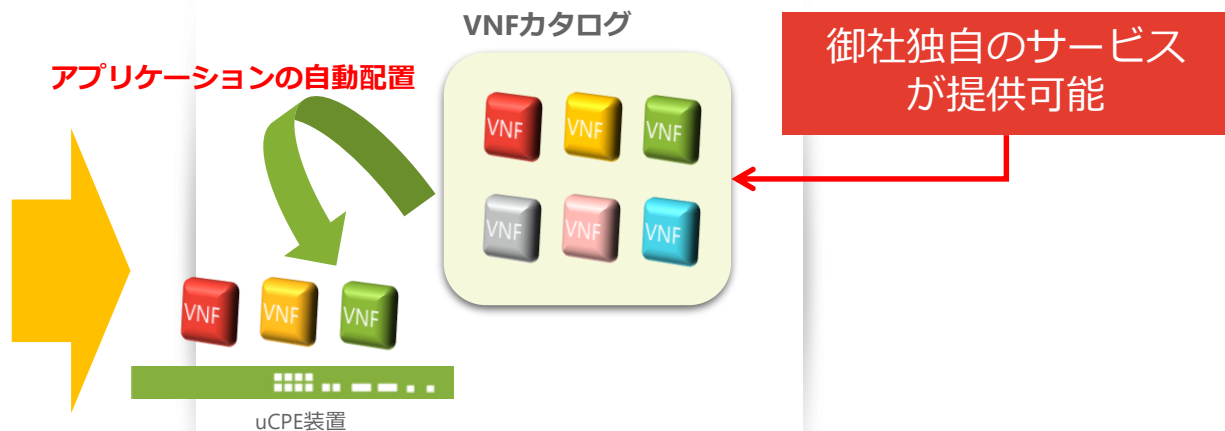
## SD-WANに付加価値をプラス

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

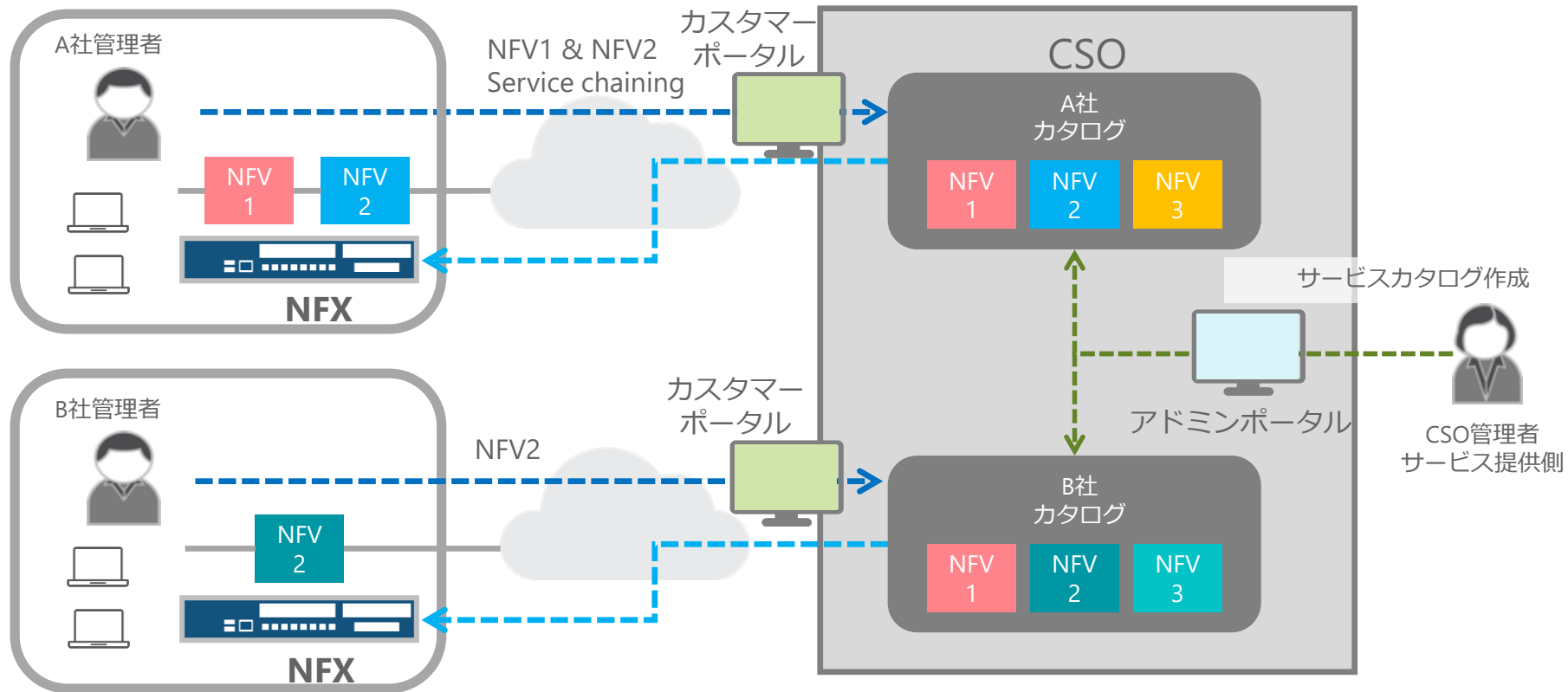


次世代ブランチオフィス(uCPE)



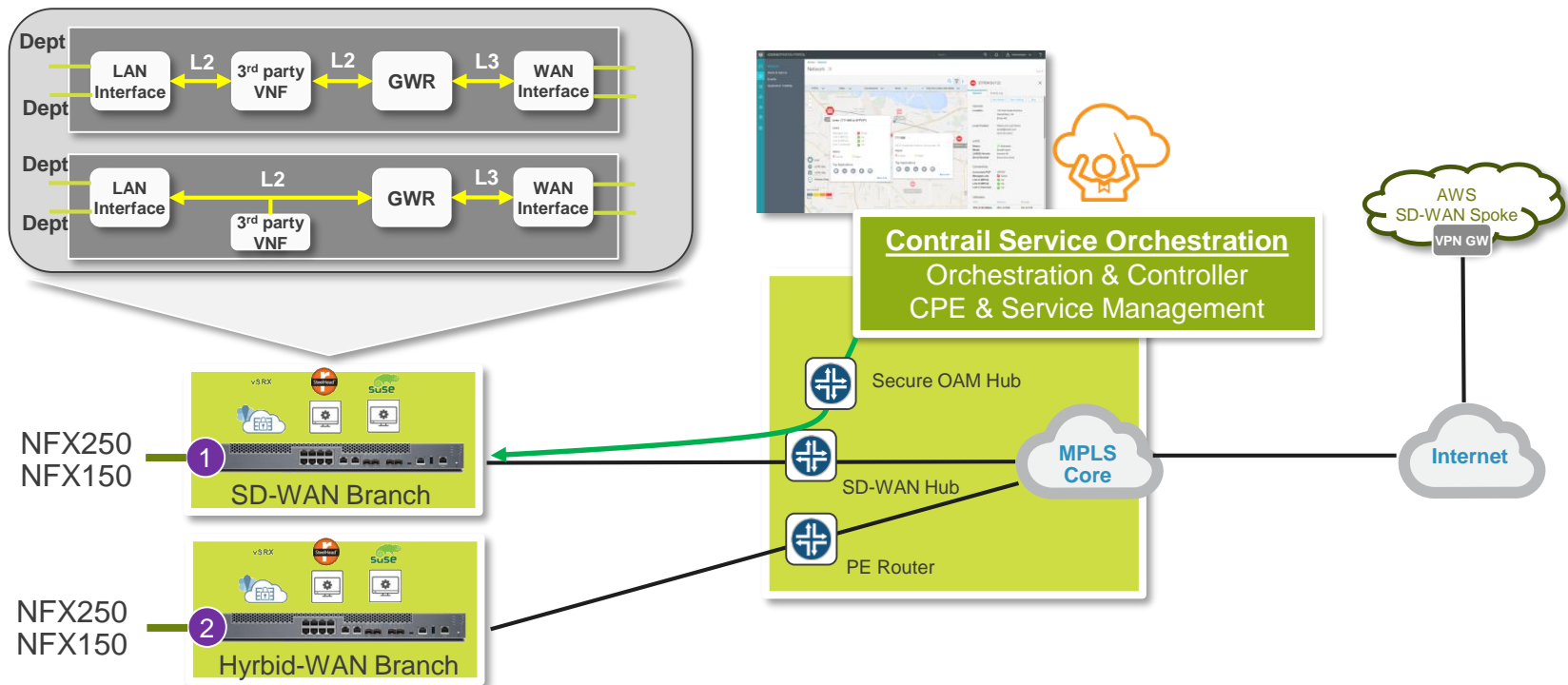
**サービスに競争力を**

# エンドユーザ毎に異なるサービスを提供

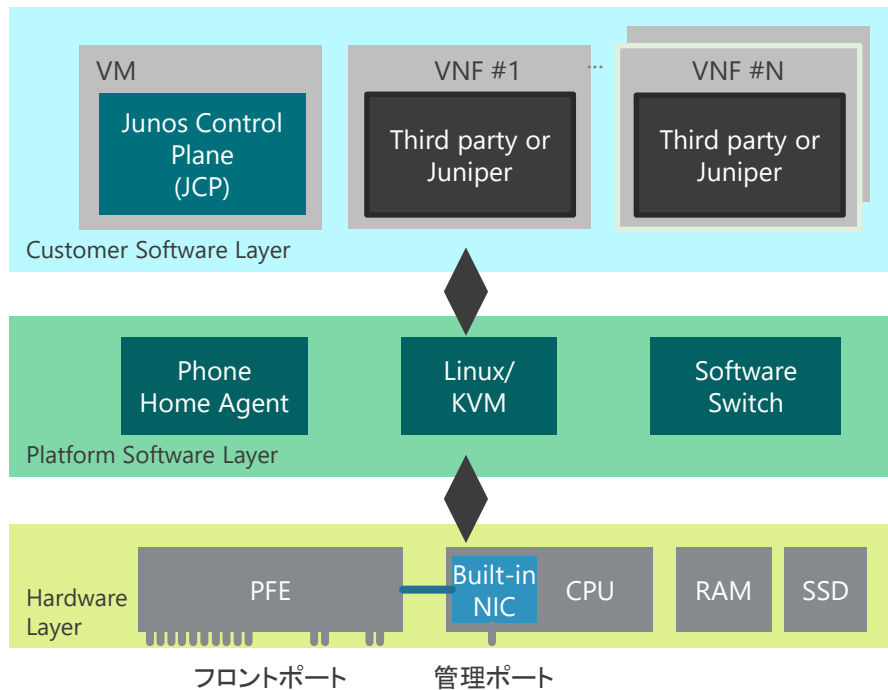


# サービスチェイニング

NFX上に3rd party VNFを展開



# 柔軟なサービスを提供可能なオープンアーキテクチャ



## Customer Software Layer

- 様々なアプリケーション、VNFが動作
  - 例 : Fortinet, Riverbed SteelHead, LxCIPtable, Ubuntu16.04, Cisco CSR-1000V

## Platform Software Layer

- Linux OS / KVM ハイパーバイザ
- ソフトウェアスイッチ(OVS)
- Phone Home エージェント(ZTP)

## Hardware

- Intel Atom / x86 CPU
- スイッチングASIC



# サービスチェイニング

---

動画のリンクは下記を参照

[https://www.youtube.com/playlist?list=PLGvolzhkU\\_gR34Kxk\\_Qh5ONMtHXdDPEwk](https://www.youtube.com/playlist?list=PLGvolzhkU_gR34Kxk_Qh5ONMtHXdDPEwk)



# SD-WANコントローラーの比較

	Sky Enterprise	Contrail Service Orchestration
導入の規模	小～中規模	中～大規模
導入の難易度	SSLでクラウドに接続	BGP/MPLS/GRE/IPsecで接続
構成の柔軟性	制限なし	Hub-Spokeが基本構成
管理対象	FW, SW, WIFI	FW, SW, WIFI, VNF
費用	low	high
提供形態	クラウド	クラウド / オンプレミス
ZTP	○	○
拠点管理	○	○
WAN構成管理	×	○
LAN構成管理	○	○
テンプレート運用	○	○
マルチテナント対応	×	○
サービスチェイニング	×	○



# Juniper Networksが提供する SD-WANソリューション

# Juniper Networksが提供するSD-WANソリューション

## 可視化

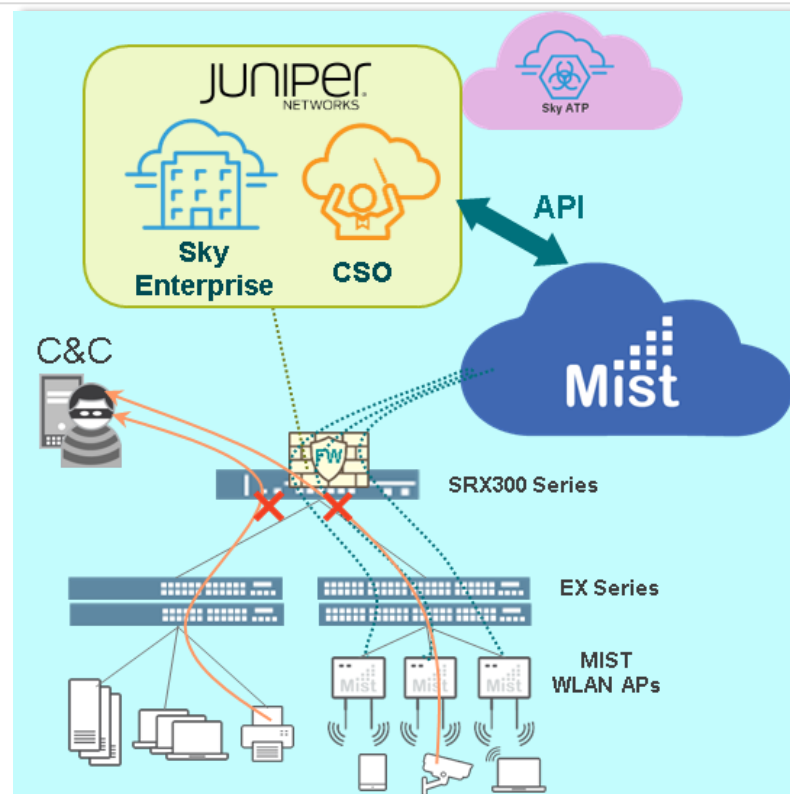
- Wi-Fi の稼働状況および通信品質の可視化
- アプリケーションの可視化とトラフィックの制御
  - ユーザ体感の最適化

## 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(3<sup>rd</sup> パーティ-VNFをオンデマンドで提供)

# Juniper Networksが提供するSD-WANソリューション

	Juniper	他FWベンダ	他SD-WANベンダ
構成の柔軟性	○ 用途に応じてコントローラーを選択	△ コントローラーを選べない	× コントローラーへのアクセスが必須
管理対象	○ FW, SW, WIFI, VNF	× FWのみ	△ RT, VNF
構築費用	○ FW単品からの購入が可能	△ Bundle licenseの購入が必要	× 検証、構築まで時間がかかる
LTE接続	○	×	○
セキュリティ機能	○	○	△ 3rd party FWと連携
アプリケーションコントロール	○	△	△
トラブルシューティング	○ CLIで情報取得が可能	○ CLIで情報取得が可能	× GUIのみ



THANK YOU

---

JUNIPER  
NETWORKS | Engineering  
Simplicity