

～企業のWAN, LAN, WiFiと
セキュリティを一元管理～
最新のクラウドを活用した
これから企業ネットワーク

ジュニパーネットワークス株式会社
技術統括本部

JUNIPER
NETWORKS

Engineering
Simplicity

内容

これからの企業ネットワーク



企業ネットワークのトレンド



IT担当者が抱える課題と対策



まとめ - ジュニパーの差別化ポイント



企業ネットワークのトレンド

企業ネットワークのトレンド



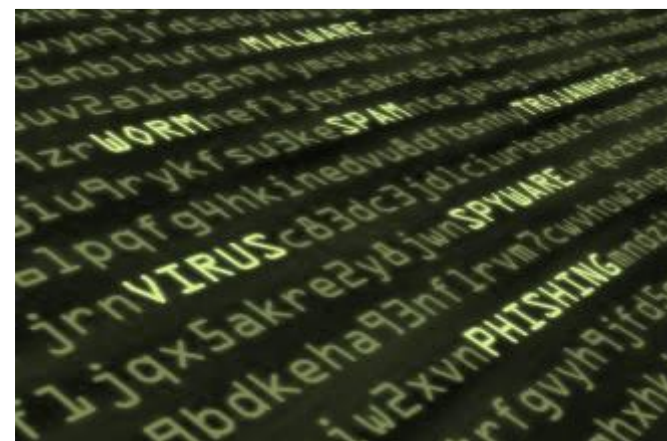
クラウドを活用した
アプリやコンテンツ



Wi-Fi, BYODおよび
IoTデバイスの増加



自動化による
業務効率アップ



内部に侵入した
セキュリティ脅威の
リスク



IT担当者が抱える課題と対策

IT担当者が抱える課題

NW管理コスト



クラウドアプリ品質



セキュリティ



1 本社や支店、キャンパスのネットワーク管理が
コスト高になっていませんか？

WAN, LAN, WiFiを一元管理でき、
管理コストを大幅に削減できます。



シンプルな ネットワーク管理と運用



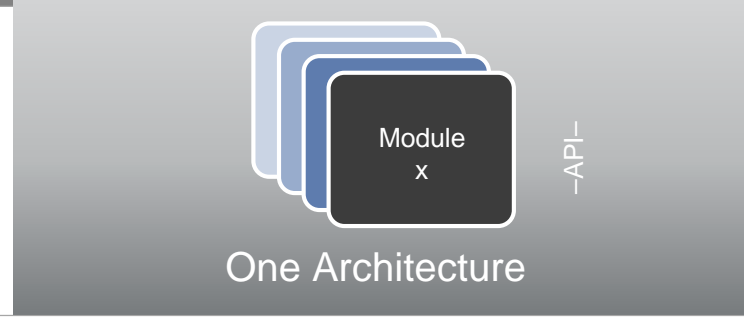
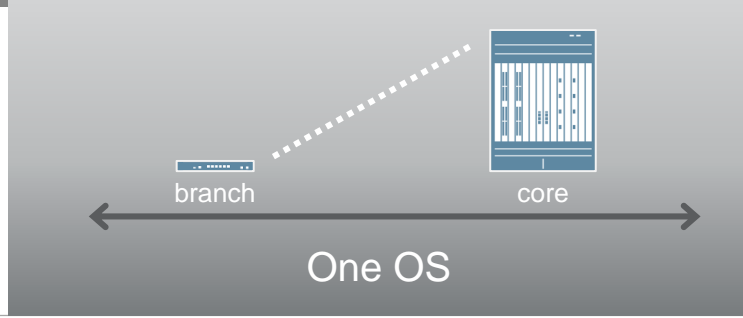
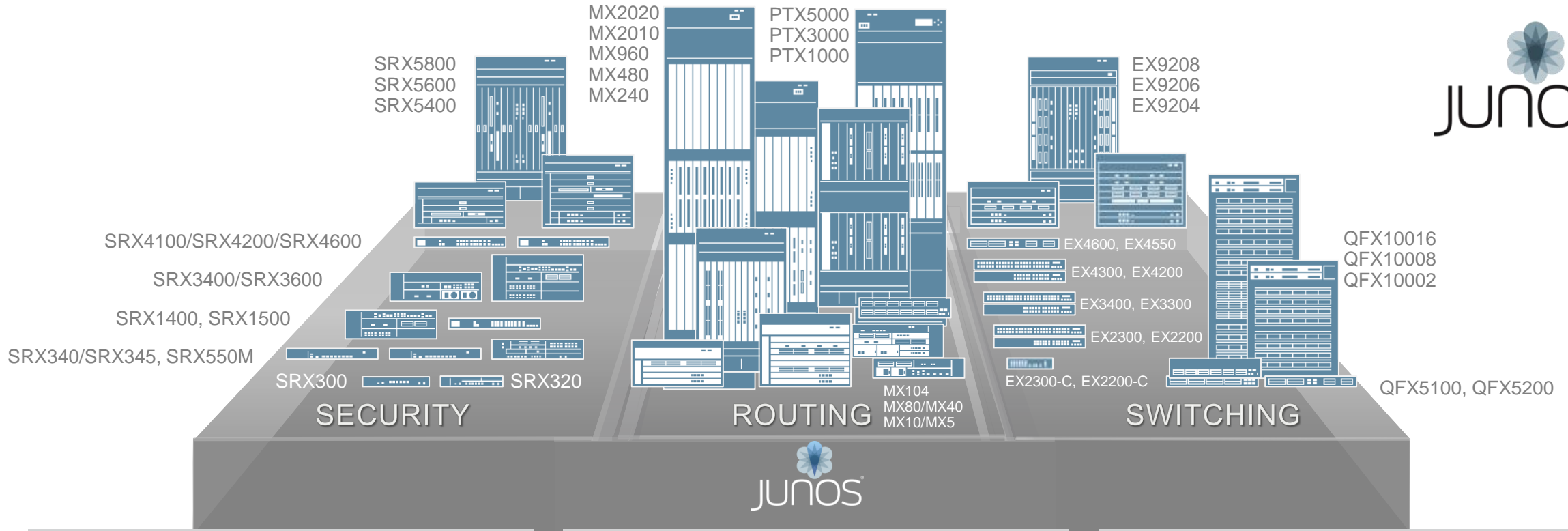
共通のアーキテクチャと操作性

シンプルなネットワーク構成

ネットワークからセキュリティまで一元管理

共通のアーキテクチャ

共通の
アーキテクチャと
操作性



共通のオペレーティングシステム

共通の
アーキテクチャと
操作性



1つのテクノロジー

- 共通のソースコード
- 同じコントロールプレーン
- 同じインフラストラクチャ

NWとセキュリティ製品

- ルーティング、スイッチング、セキュリティ
- エントリーレベル、ミッドサイズ、ハイエンドモデル
- プロダクトライン
 - 物理: SRX, EX, MX, QFX, PTX, ACX, NFX
 - 仮想: vSRX, vMX, vRR, vBNG, vQFX, vPTX



- 共通のユーザインタフェース
- 共通の自動化ツール
プログラミングAPI, ツール, マネジメント
- 同じリモートオペレーションメカニズム

- 同じコードベースで全てのプラットフォームをサポート
- 共通のソフトウェア実装のポリシーと手順
- 共通の仮想化と自動化テストフレームワーク



1つのオペレーション

1つのリリーストレイン

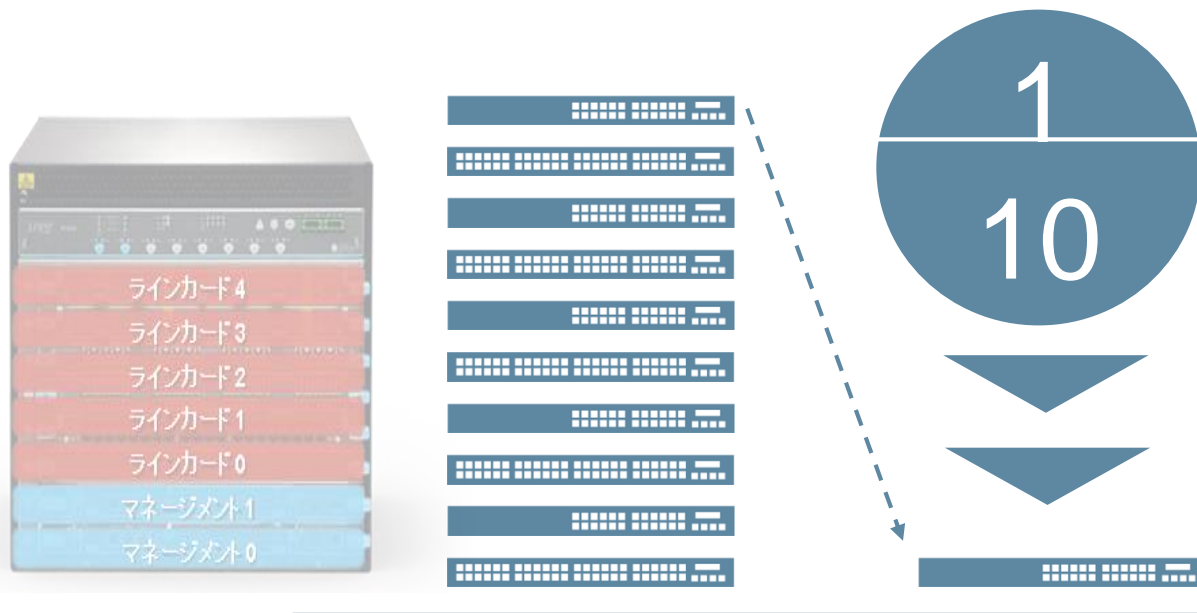


バーチャルシャーシテクノロジー (VC): 複数のスイッチを仮想的に1台のスイッチにする技術

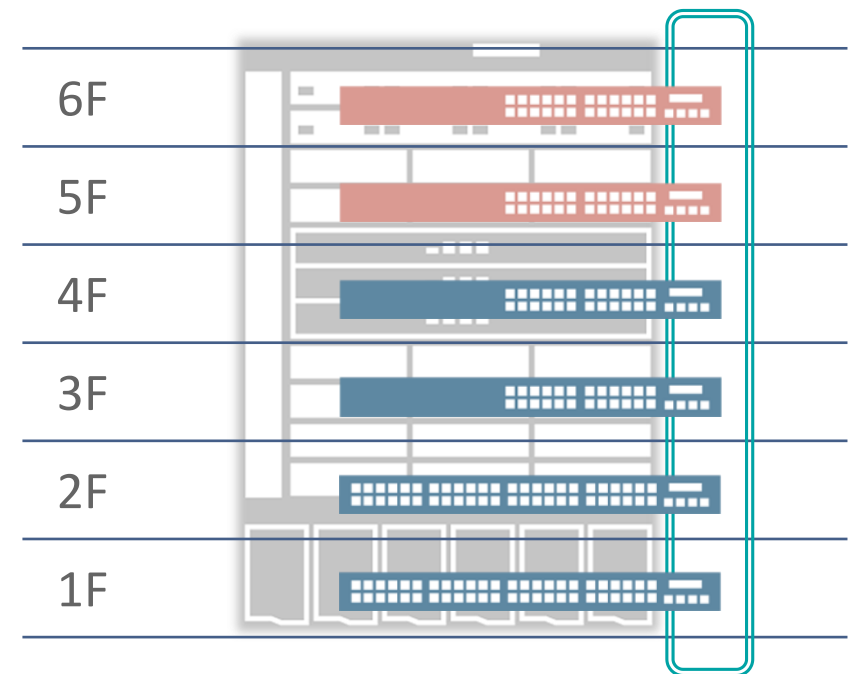
シンプルな
ネットワーク構成

- 1台のスイッチとして、OSおよびコンフィグを管理
- 管理・制御プレーンとファブリック接続は冗長化

2~10台のスイッチを1台として管理



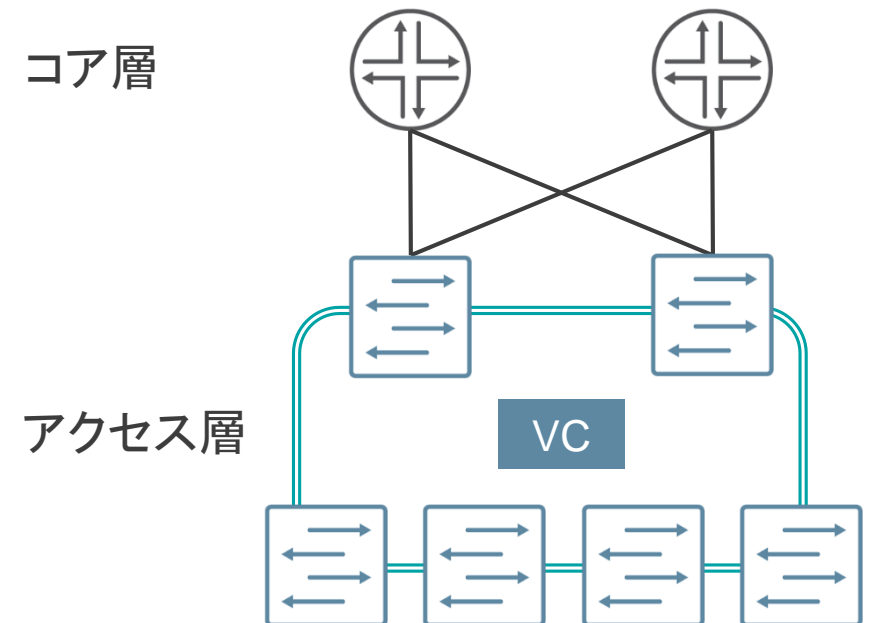
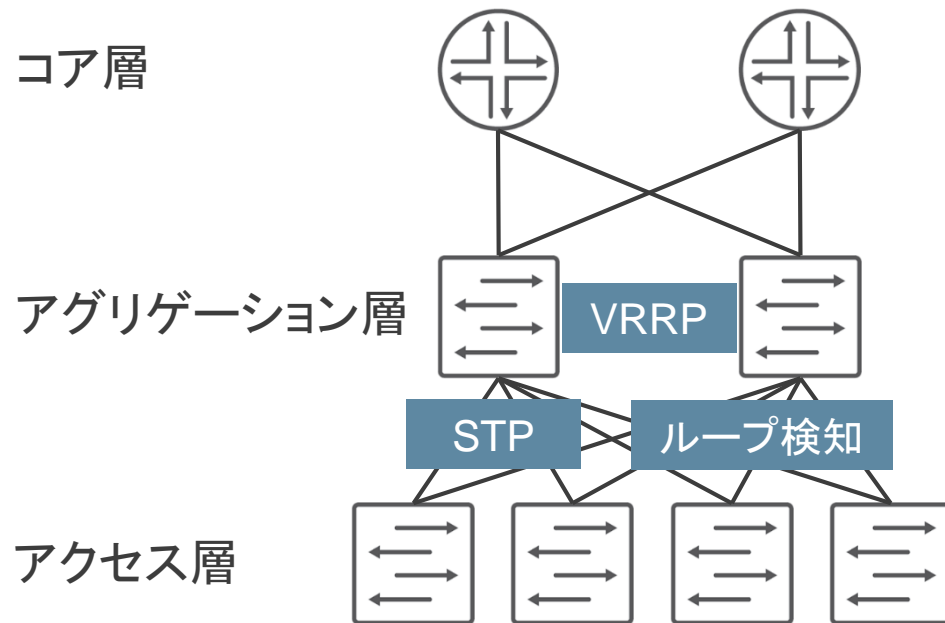
複数フロアに跨る仮想的なシャーシ



バーチャルシャーシテクノロジー (VC): 複雑なプロトコルを排除し、シンプルな構成に

シンプルな
ネットワーク構成

- 従来の多段ネットワーク構成をシンプルにして、保守交換や機器追加を容易にする
 - VRRPやxSTP等のプロトコルに依存せず、効率的に帯域を活用
 - プラグ&プレイでメンバースイッチの追加と削除



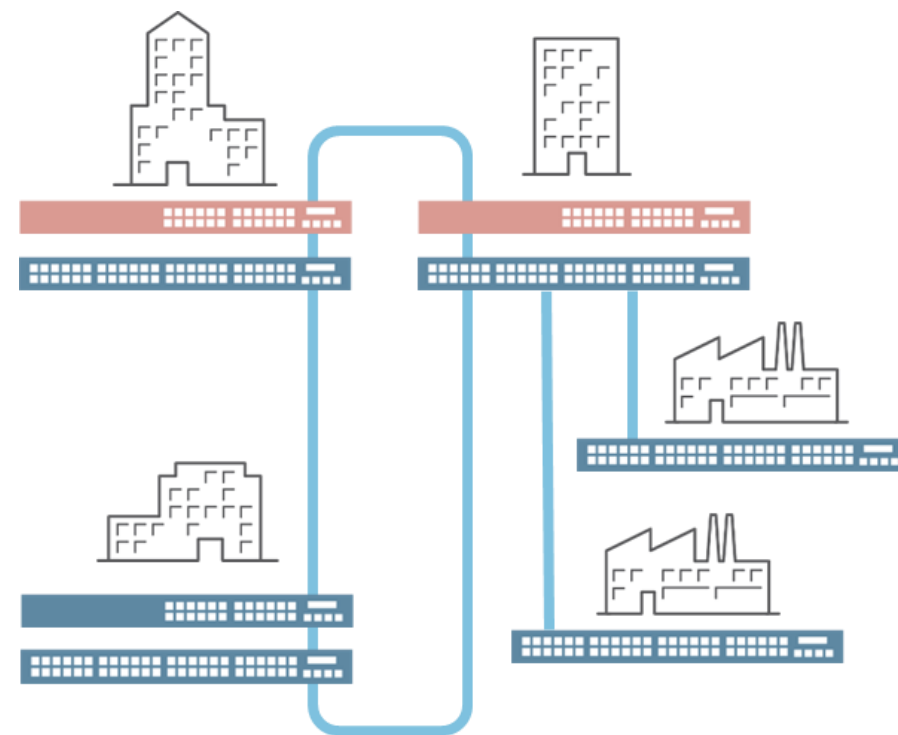
バーチャルシャーシテクノロジー（VC）： 接続距離の延伸とトポロジーフリーな構成

シンプルな
ネットワーク構成

バーチャルシャーシのノードスイッチ間を
10GE-ZR トランシーバ接続することで、
80kmの接続距離



バーチャルシャーシ構成は、トポロジーフリー
（リング、バス、スター等）

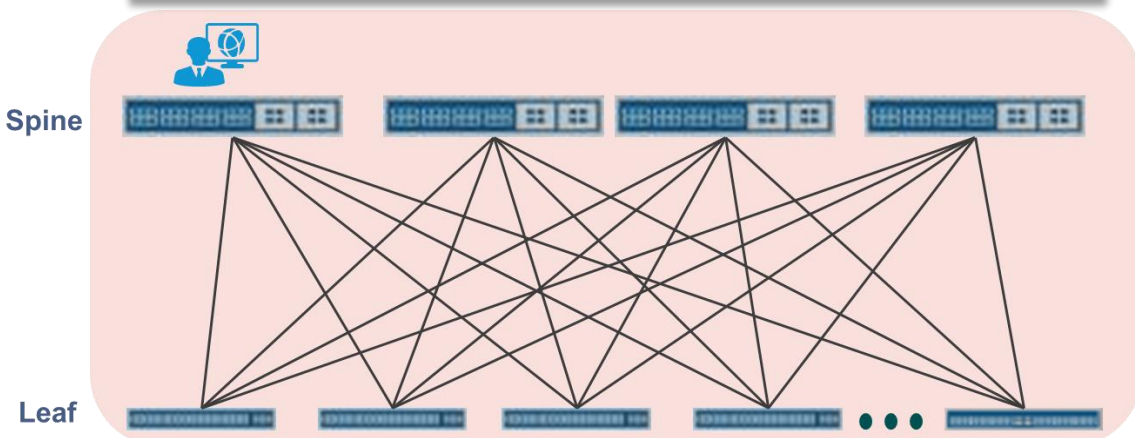


ネットワークトポロジーやノード間距離を気にせず、柔軟なネットワーク設計が可能

柔軟に設計および運用できるファブリック技術

シンプルな
ネットワーク構成

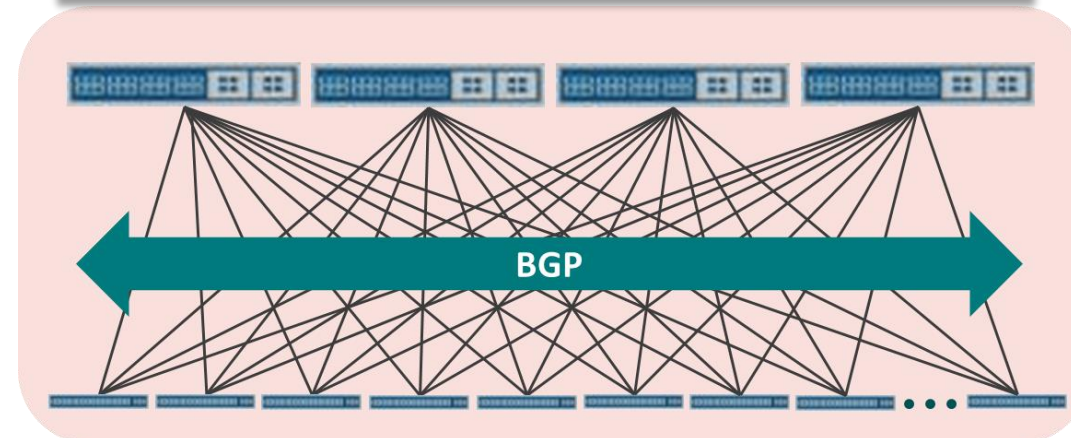
バーチャルシャーシファブリック (VCF)



VCFの利点

- 最大20ノードを1台のスイッチとして管理可能
- 制御プレーンの冗長化
- プラグアンドプレイ
- ローカルスイッチング

IPファブリック



IPファブリックの利点

- ハンブロッキングIP Closアーキテクチャ
- 10万ポート以上の10GE収容
- ECMPによるスケーリング
- 分散型マネージメント

Sky Enterprise (クラウドポータル)によるNW統合管理

クラウドポータルを介した総合管理



- ・ロール別ユーザの登録管理
- ・スイッチング・ルーティング・セキュリティー設定
- ・自動プロビジョニング機能 (ZTP)

設定管理



- ・世代管理 / バックアップ
- ・設定の一括変更機能
- ・動的アドレスフィード機能
- ・OS アップデート

モニタリング



- ・サイトマップ機能
- ・トポロジーマッピング機能
- ・ライセンス管理
- ・アラーム / アラート管理

レポートニング



- ・脅威分析レポート機能
- ・システムリソースグラフ
- ・インタフェースグラフ
- ・セキュリティセッション情報

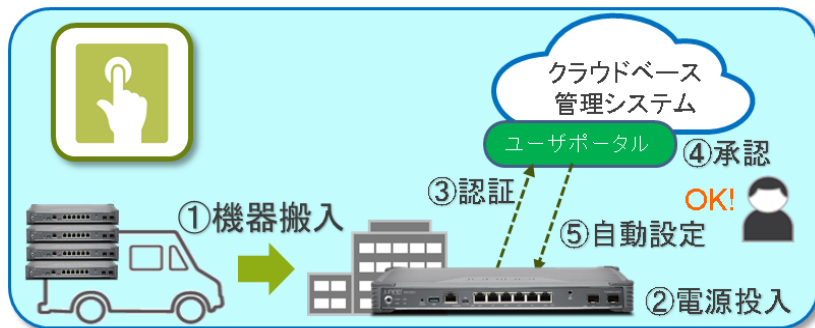
クラウドベースのマネージメントシステム： 多拠点展開する機器の運用管理コストを軽減

ネットワークから
セキュリティまで
一元管理

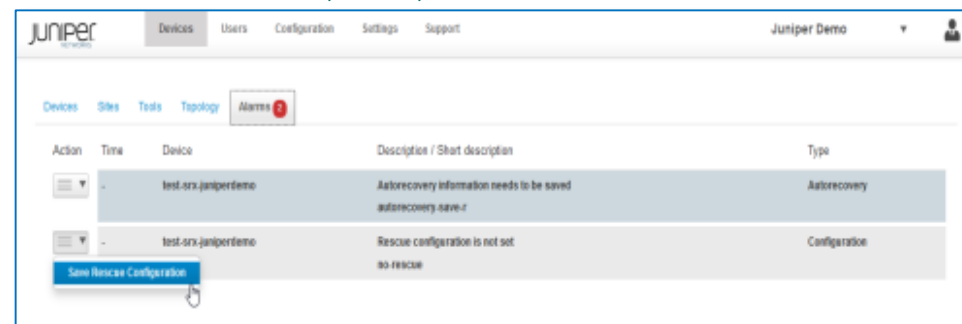


管理設定

ZTP



設定管理 (CPE, FW, LANスイッチ、ワイヤレス)

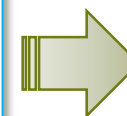


モニタリング

サイトマップ



トポロジー・アラーム管理



レポート

システム管理

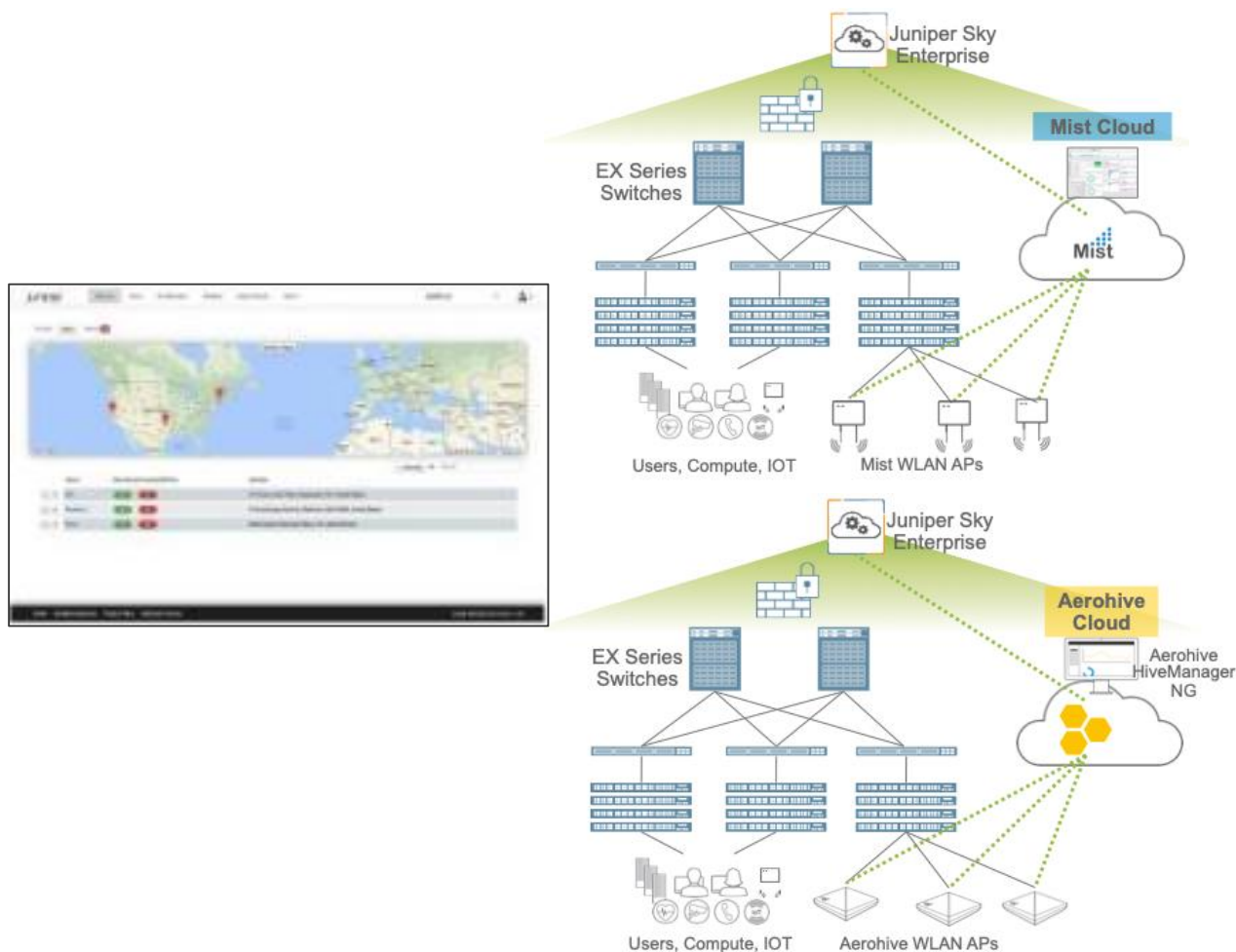


アプリケーション&NW脅威レポート



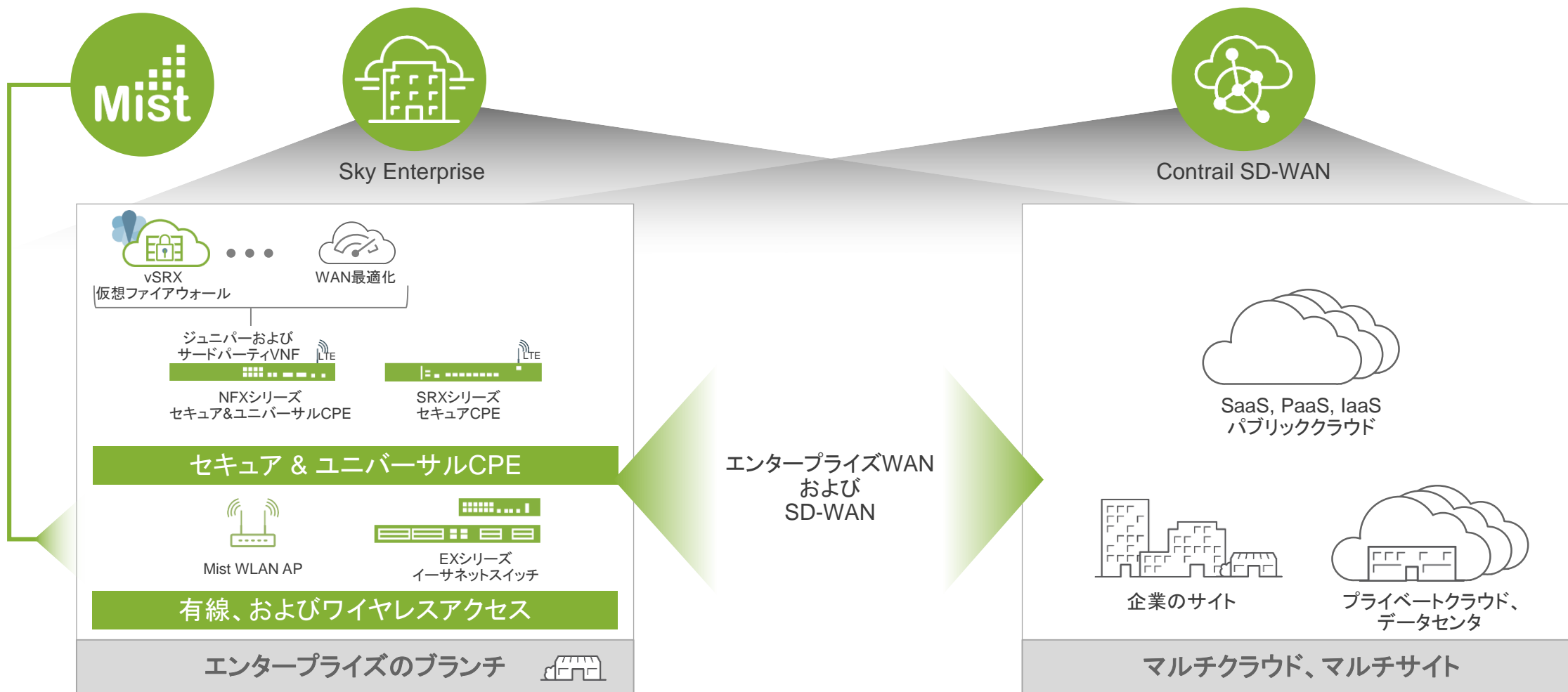
クラウドベースのマネージメントシステム: WANからLAN, WiFiまで一元管理

ネットワークから
セキュリティまで
一元管理



- クラウドベースのマネージメント
 - サブスクリプションモデル
- 直感的なダッシュボードから一元管理
 - 自動プロビジョニング (ZTP)
 - 設定一括変更
 - モニタリング
 - アプリケーション可視化、レポートイング
- キャンパス全体を管理
 - SRX (セキュアルータ)
 - EX (スイッチ)
 - アライアンス製品 (WiFi AP)

2つのSD-WANオーケストレータ



2 クラウド導入後、アプリケーションの応答性が悪くなったり、ビデオ動画が止まったりしませんか？

優先度が高い動画アプリケーションのWAN帯域を保証し、ユーザ体感を改善します。

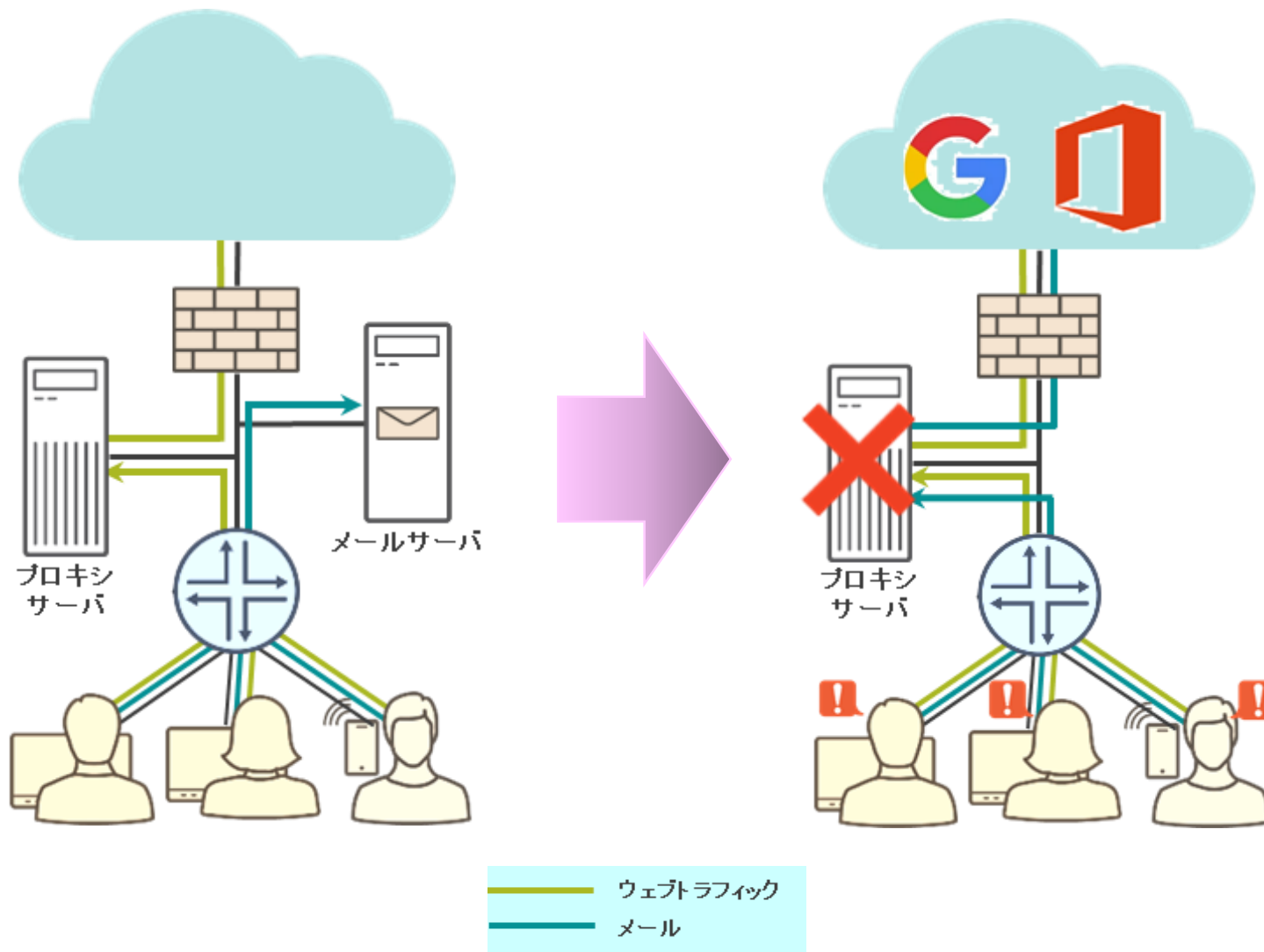
クラウド利用時の ユーザ体感品質を改善

アプリケーションを識別し、トラフィックを制御

ユーザ属性とアプリを条件に業務を優先制御

プロキシ環境でも手間なく導入

アプリケーションの応答性が低下する要因



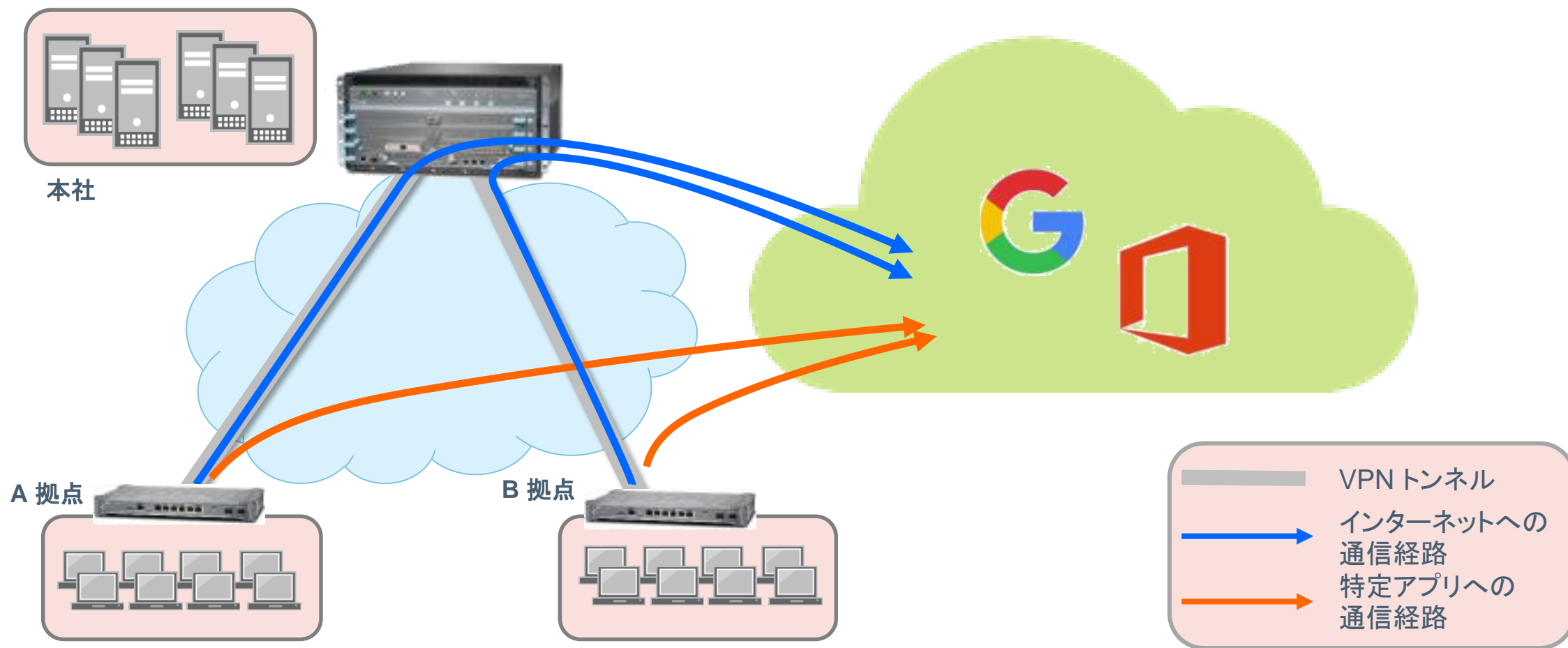
メールやアプリケーションサーバをクラウドに移行すると、インターネットやWANトラフィックを管理するサーバの負荷が増大。



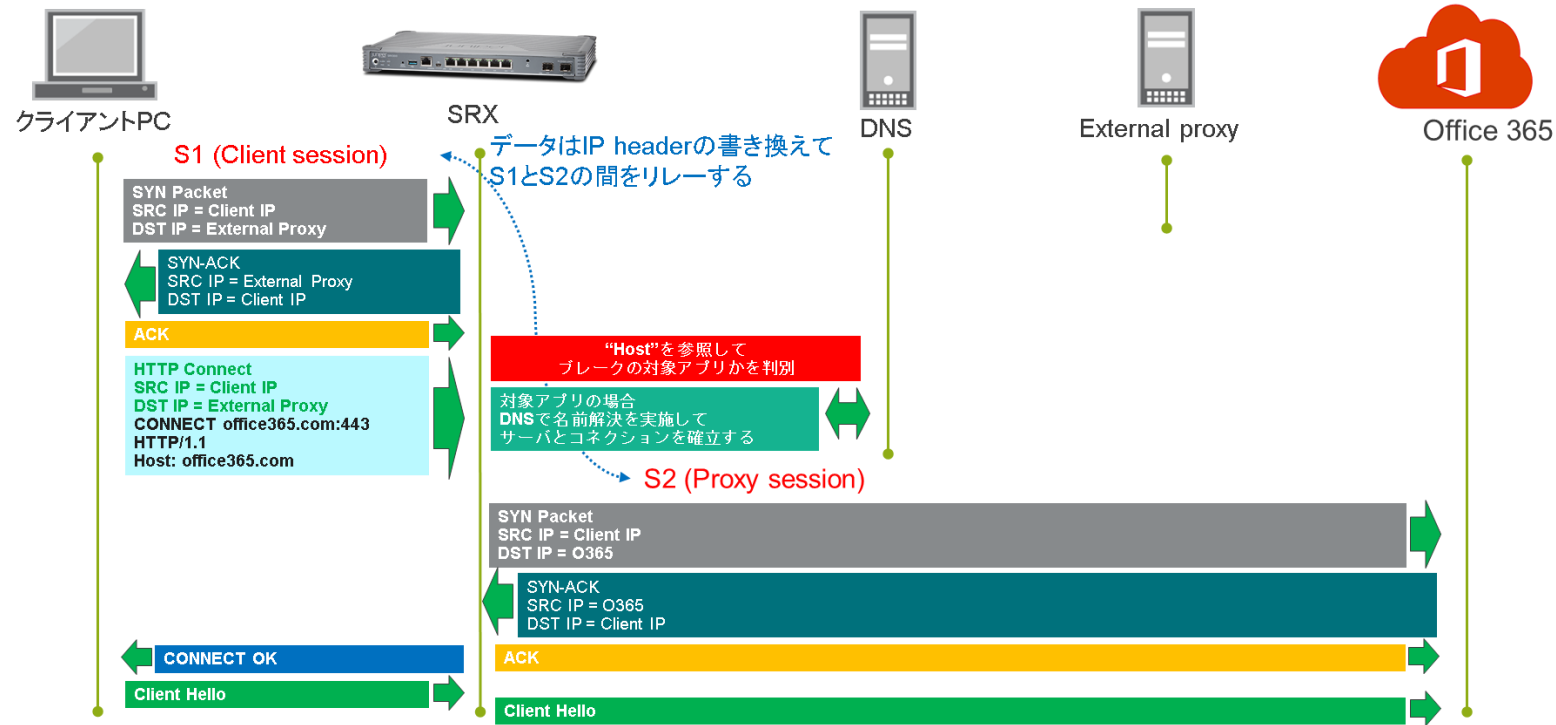
オンプレサーバの時と比べて、クラウドサービスの応答性が遅くなる。

クラウドアプリケーションを識別して最適な経路にルーティング

- Office365等のクラウドトラフィックをインターネットにオフロード



Secure-Web-Proxy機能によるプロキシ環境でのオフロード

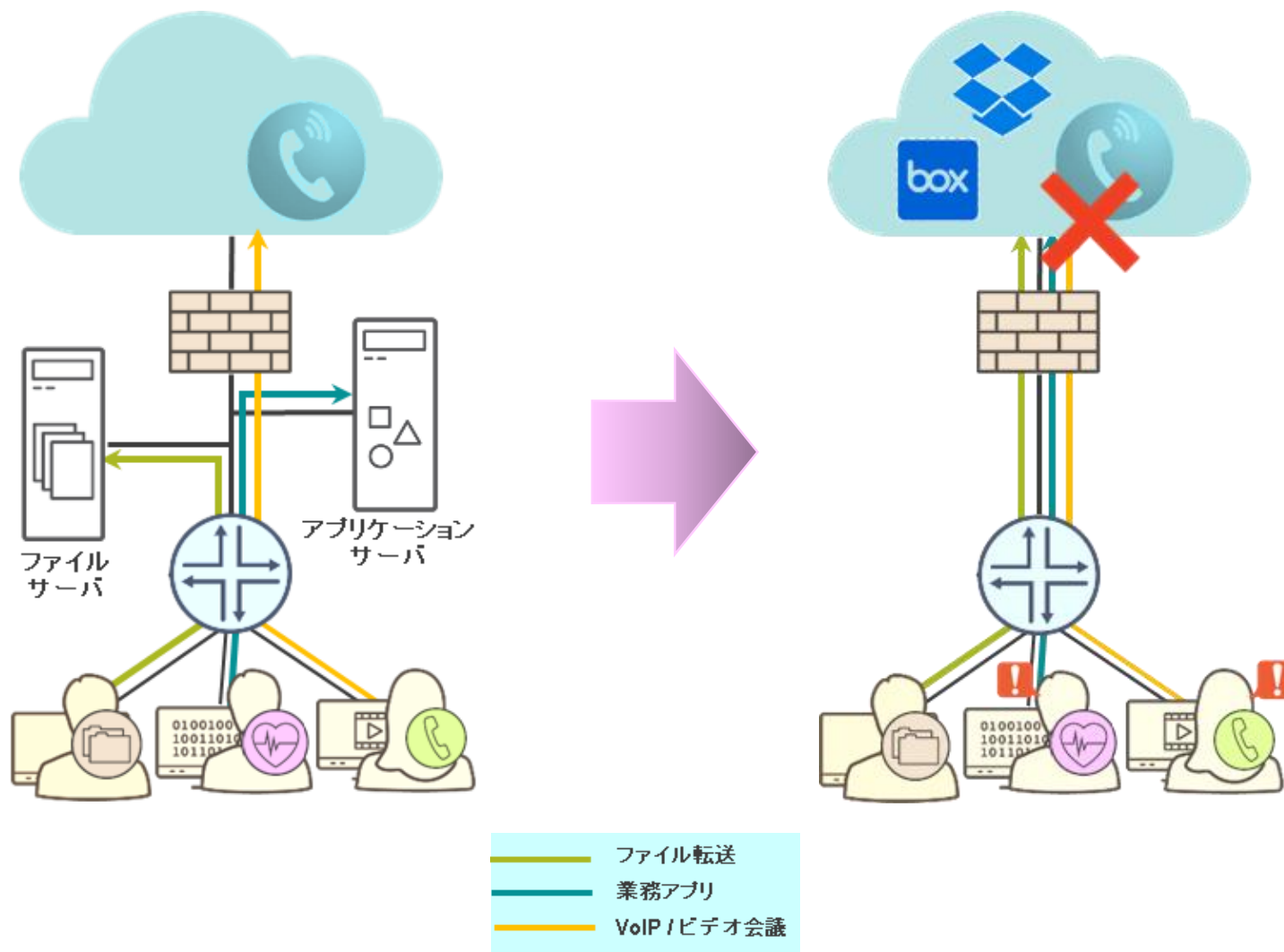


25

Secure-Web-Proxyの動作 ::

- ✓ クライアントと本来のproxy serverとのTCPコネクションをインターセプトし、SRXで終端させる
- ✓ SRXは”HTTP connect request”の”Host” から宛先を確認し、DNSによる名前解決を行う
- ✓ SRXは該当サーバとのコネクションを確立し、サーバからのレスポンスをクライアントに送信する
- ✓ SRXはサーバとの接続に自身のIPアドレスを使用せず、クライアントのIPを使用する

ビデオ動画や音声通話が品質劣化する要因

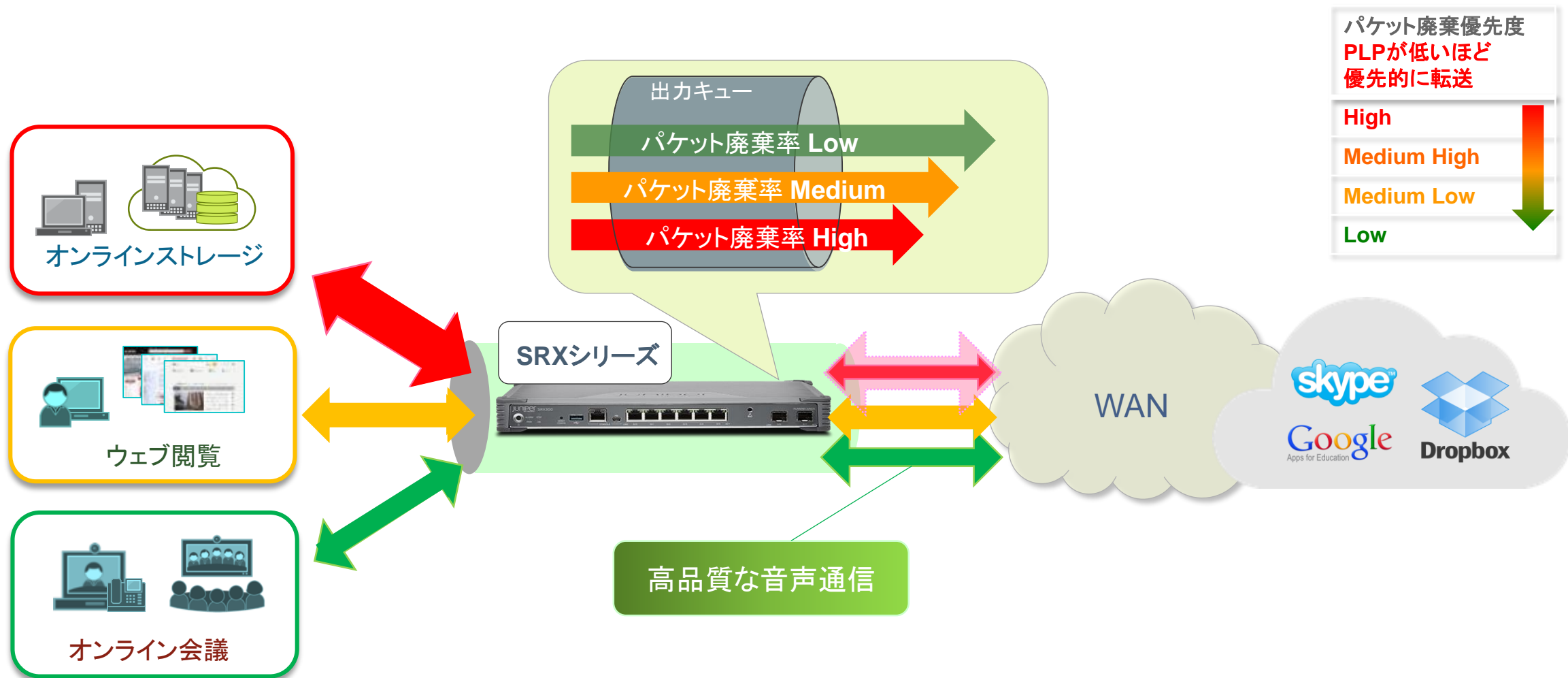


データがクラウドに移行すると、WANに流れ込むトラフィック量が増大し、タイムクリティカルなアプリケーションが影響を受ける。

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。

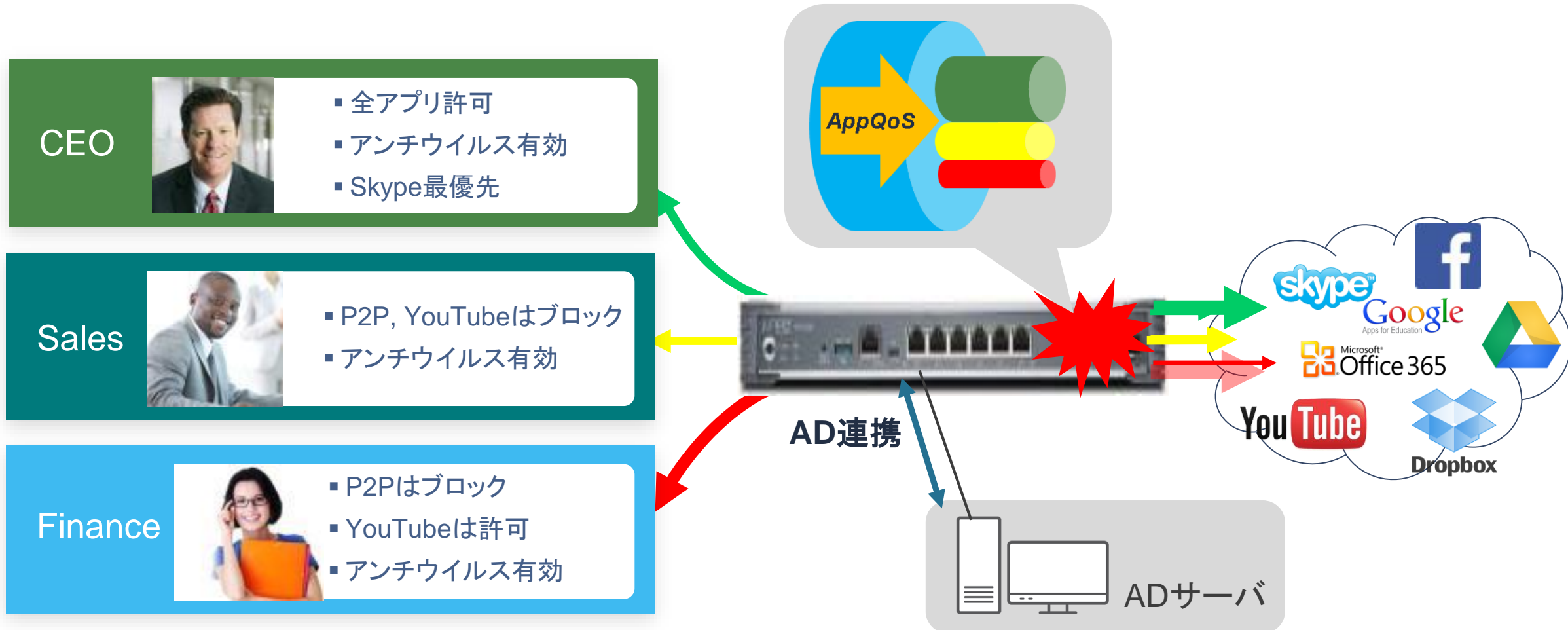
リアルタイム性の高いアプリケーションを最優先させ、ユーザ体感を向上

ユーザ体感品質の改善



ユーザベースのアプリケーション優先制御

ユーザ属性とアプリケーションを条件にポリシーを適用



3

境界を防御するセキュリティ対策に加えて、不正侵入したサイバー脅威への対策は充分ですか？

ネットワーク内部に侵入した脅威を素早く検知して、自動的に対処と防止策を講じます。

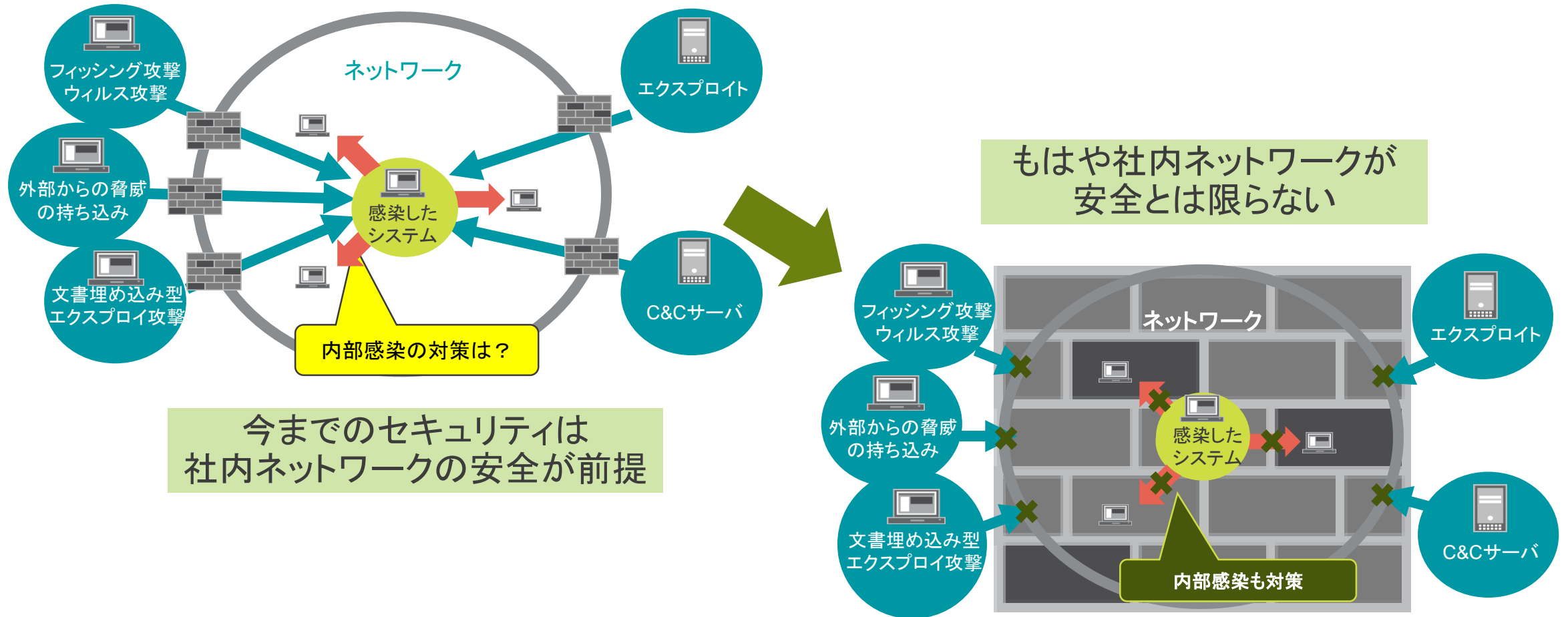
社内ネットワークに侵入した脅威の検知と対処を自動化

侵入した脅威を自動検知し、脅威を隔離

サードパーティ脅威フィードによる最新情報

端末やクライアントにエージェントは不要

境界セキュリティだけでは不十分



今までのセキュリティは
社内ネットワークの安全が前提

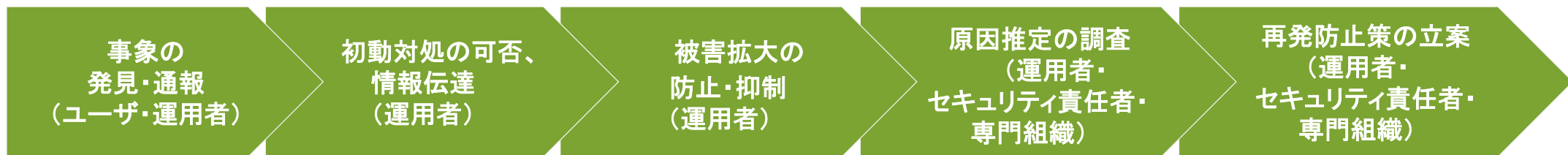
既に内部へ脅威が持ち込まれていることを前提に対処する必要がある

サイバー脅威を自動的に検知し排除する仕組みが必要

手動による脅威への対応



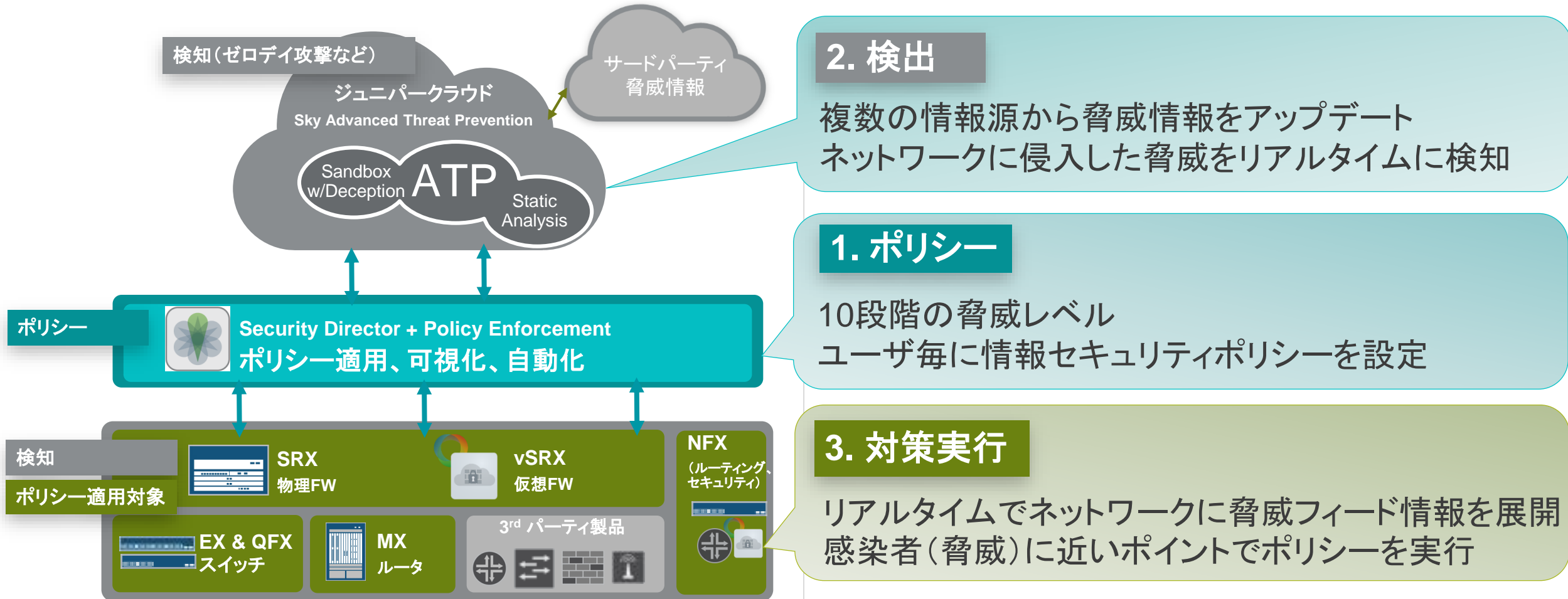
自動的に脅威を検知・排除



脅威の検知から、対処・防止策までを自動化

Connected Security: ネットワークをセキュリティドメインとして、自動検知と対処

サイバー脅威の
自動検知・対処



2. 検出

複数の情報源から脅威情報をアップデート
ネットワークに侵入した脅威をリアルタイムに検知

1. ポリシー

10段階の脅威レベル
ユーザ毎に情報セキュリティポリシーを設定

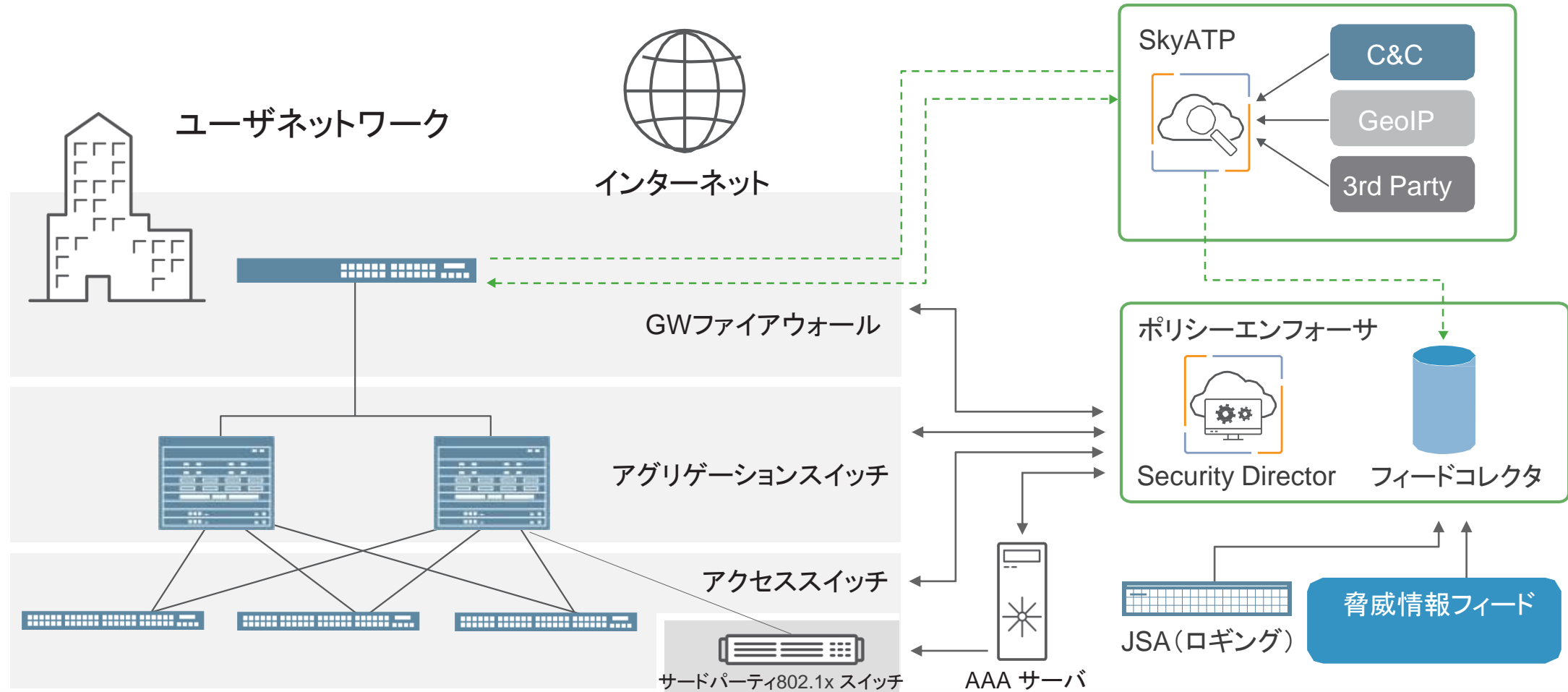
3. 対策実行

リアルタイムでネットワークに脅威フィード情報を展開
感染者(脅威)に近いポイントでポリシーを実行

ネットワーク全体を単一の対策実行ドメインに！それぞれの機器がポリシーの適用ポイント

Connected Security: 企業ネットワークの構成例

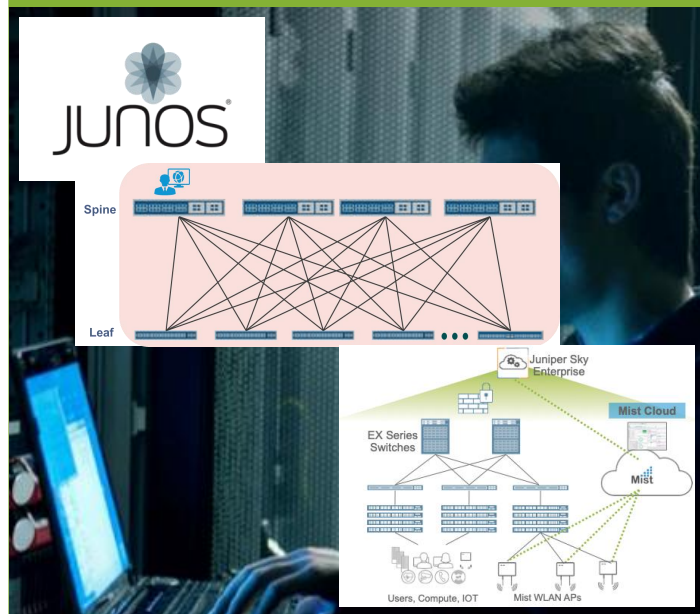
サイバー脅威の
自動検知・対処



ネットワークをSDN制御可能なセキュリティドメインとして構成することで、
侵入したサイバー脅威を自動的に検知して、その対処・防止策を実行する。

これで解決

NW管理コスト



クラウドアプリ品質



セキュリティ





ジュニパーの差別化ポイント

WHY JUNIPER?

ジュニパーの差別化ポイント

シンプルな運用管理

- WAN, LAN, WiFi を一元化されたダッシュボードから管理
- 複雑なプロトコルを排除し、シンプルで柔軟なネットワーク構成 (VC)
- 導入、運用、増設、可視化等を自動化し、IT担当者の負荷を軽減

ユーザ体感の向上

- 動画アプリや音声データを最優先させ、ユーザ体感品質を改善
- ユーザの役割とアプリケーションを条件に最適なトラフィックコントロール

セキュリティの自動化

- セキュリティ脅威を自動で検知し、内部に侵入した脅威を瞬時に隔離
- 脅威情報の最新ステータスをクラウドで常にアップデート
- エージェントレスで導入しやすく、バージョン管理も不要

必要に応じてサービスを追加できるサブスクリプションモデル



デモ (Sky Enterprise)

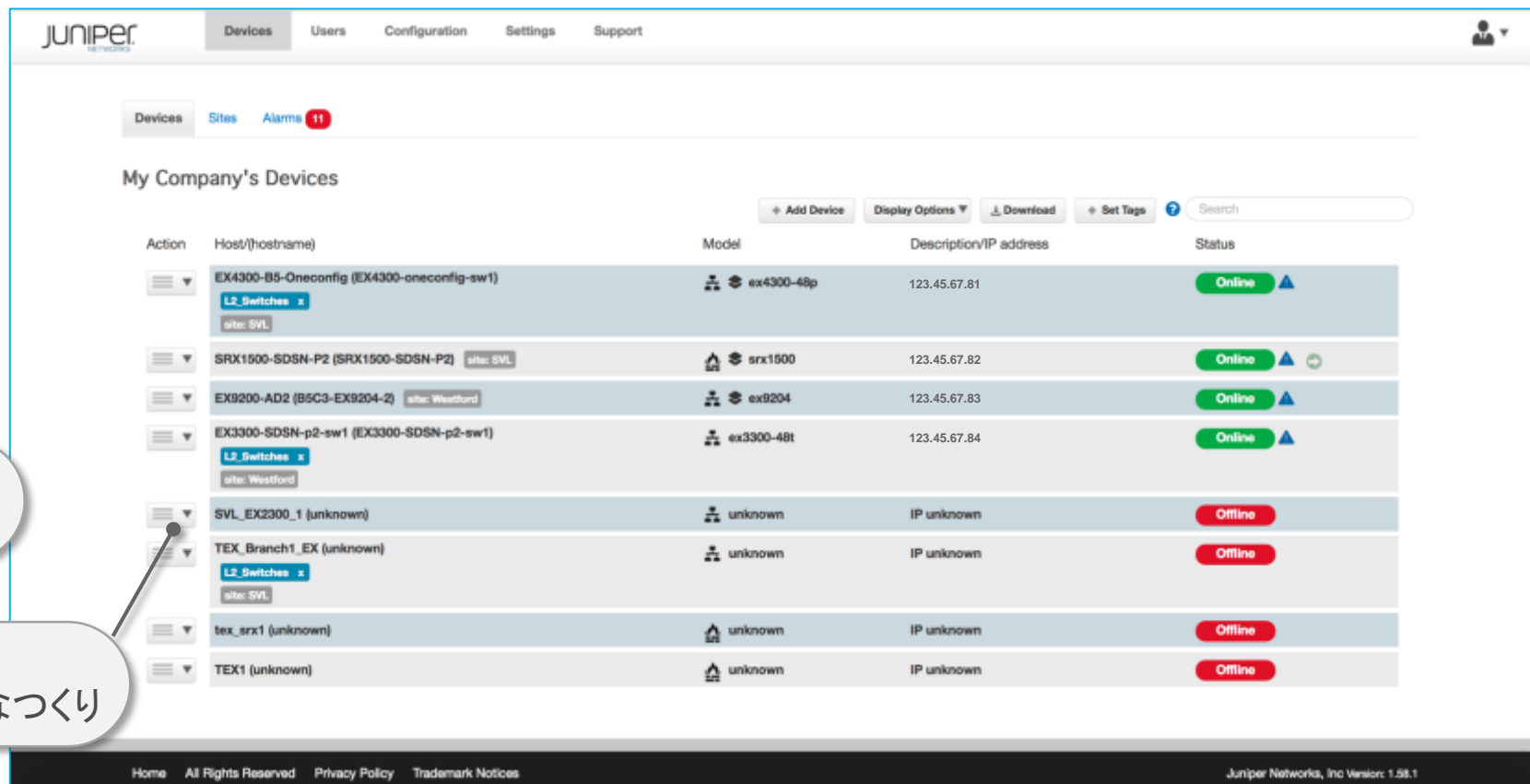
Sky Enterprise ポータルの紹介



直観的なウェブインタフェースを使用した中央管理



・グローバルのログイン画面
アカウント(メールアドレス)で管理



・管理デバイス一覧
機器ステータスが一目で確認可能なつくり

ユーザ管理 / マルチテナント機能



ロールベースのユーザ管理

Email	Role	Last Activity	Two Factor Auth	Activated
...	admin	about 4 hours		Active since 2010-01-24
...	admin	14 minutes		Active since 2010-02-01
...	admin	less than a minute		Active since 2010-04-21
...	admin	7 months		Active since 2010-02-05
...	admin	about 1 month		Active since 2010-04-25
...	admin	6 months		Active since 2010-02-05
...	admin	6 months		Active since 2010-02-01
...	admin	6 months		Active since 2010-02-21

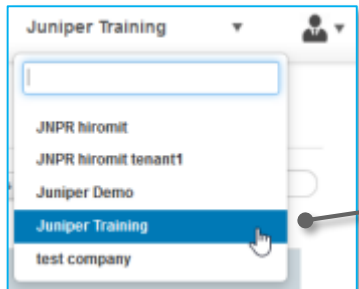
・ 閲覧権限、管理権限などの
ロールベースのユーザ管理

・ 「Google Authenticator」や
「Duo」の二要素認証の実装



柔軟なマルチテナントサポート

Action	Name	Devices (Connected/Offline)	Users (Active/Not Activated)	Services	Alarms	MSP Support
...	test	5 / 2	0 / 0	0	0	X
...	test2	0 / 1	0 / 0	0	0	X



・ テナント毎でポータル
の簡単切替
ユーザ権限別での操作

・ デフォルトで実装のマルチ
テナント対応

設定機能



各設定の操作・アクションの実行

・ スイッチング・ルーティング・セキュリティ設定
主要機能設定の設定に対応

・ 一括設定変更機能
管理デバイスに一括で設定の適用が可能

・ アクションの実行
オペレーションコマンド(再起動など)の実行

Action Host(hostname)
vSRX (test-vsrx)
Configure Security
Configure Routing
Configure DHCP
System and Monitoring
Actions
Show Device Details
Show Configlet
Delete Device

Security Policies
Security Zones
NAT
VPNs
IDP
UTM
Applications
Dynamic Address Book Feeds

Static Routes
Advanced Policy-Based Routing

System Graphs Interface Graphs ANR Reports Commits Licenses Alarms **Actions** Packet Captures Diagnostics

Actions

Delete Rescue Configuration Clear Autorecovery Information Reboot/Power options ▼

Renew DHCP lease (all interfaces) Show full configuration

Bulk Updates Software Distribution Software Library Device Provisioning

Type Set Commands Devices None selected ▼

Input

Select all
 testdevice_SRX320_settsu-jnpr
 testdevice_EX3200_kodaimurasaki-jnpr
 testdevice_SRX345-jnpr
 testdevice_EX4200-jnpr

```
set system services ssh protocol-version v2
set system login user skyenterprise class super-user
set system login user skyenterprise authentication encrypted-password $1$...
set system services outbound-ssh client skyenterprise-ncd01 device-id EX-tes...
set system services outbound-ssh client skyenterprise-ncd01 secret 4e4919a...
set system services outbound-ssh client skyenterprise-ncd01 services netcon...
set system services outbound-ssh client skyenterprise-ncd01 skyent-ncd01.juniper.net port 4087 timeout 60 retry 1000
set system services outbound-ssh client skyenterprise-ncd02 device-id EX-test-jnpr
set system services outbound-ssh client skyenterprise-ncd02 secret 4e4919a96664321cc2e8014
set system services outbound-ssh client skyenterprise-ncd02 services netconf keep-alive retry 3 timeout 5
set system services outbound-ssh client skyenterprise-ncd02 skyent-ncd02.juniper.net port 4087 timeout 60 retry 1000
```

モニタリング機能

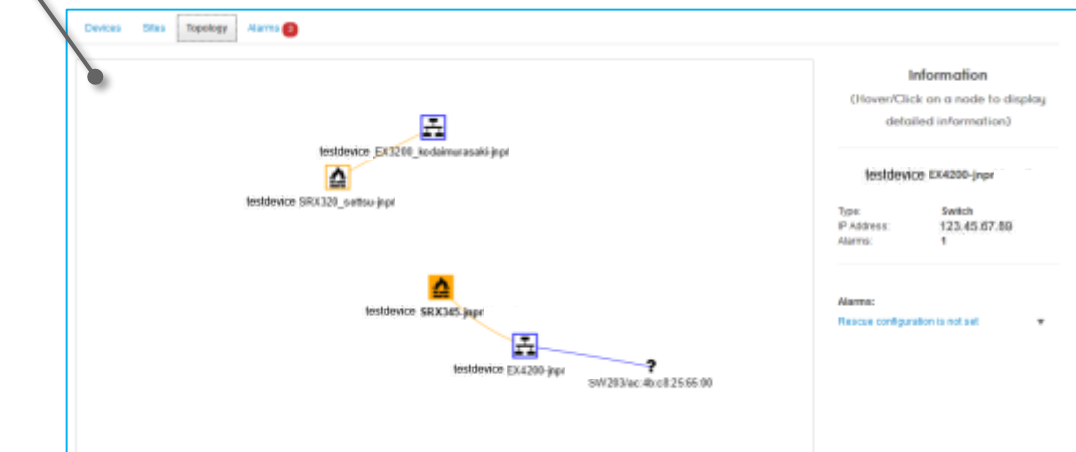


サイトマップ・トポロジーマップ・アラーム管理

・ Google Maps を使用したサイトマップ機能
機器の管理状況とあわせて地理分布の可視化

・ トポロジーマッピング機能
LLDP プロトコルを使用し、各サイトのネットワーク
レイアウトを動的に表示

・ アラーム機能
各機器アラームの発生状況を一括管理
コマンド送信によるアクション実行機能とも連携



Action	Time	Device	Description / Short description	Type
	2018-02-22 02:58	testdevice_SRX320_settsu-jpr	Autorecovery information needs to be saved autorecovery save r	Autorecovery
	2017-11-25 03:55	testdevice_EX4200-jpr	Rescue configuration is not set no-rescue	Configuration
	2018-03-13 03:38	testdevice_SRX345-jpr	Host 0 Tap0 : Ethernet Link Down Host 0 Tap0 : Link	Chassis

Mist 連携



WiFi AP、クライアント情報の一元管理

Mist Wifi Setup

Use your Username/Password to connect to Mist Systems WiFi
The authentication details supplied here are needed to generate the API connection (token). They are not stored and are discarded as soon as the token is created.

Username:

Password:

・Mist との連携
Mist Cloud のログイン情報を入力

・ Access Point、接続クライアントの一覧
Mist Cloud より各接続情報を API により収集し、
Sky Enterprise 上で確認可能

Mist Wifi Access Points

Action	Host Name	Model	Associated Device	Associated Site	Active Clients	Connected
	5c5b351e6eaa	AP21			0	
	5c5b351e6dc4	AP21			1	
	5c5b351e7cba	AP21			2	

Per Page: 1

Mist Wifi Access Point Clients

Health	Access Point	Client Name	IP Address	MAC Address	OS Type	Usage (Tx/Rx)	VLAN	SSID
	5c5b351e7cba		192.168.2.7	84c7ea8f23a1	Linux	785 KB/838 KB	1	Training room
	5c5b351e7cba	YakinikuTabetai	192.168.2.5	a45e60c36c13		111 MB/5.77 MB	1	Training room
	5c5b351e6dc4	ITJPN1-T460	192.168.2.4	e4b318ae4f8e	Microsoft OS	7.94 MB/2.55 MB	1	Training room

Per Page: 1

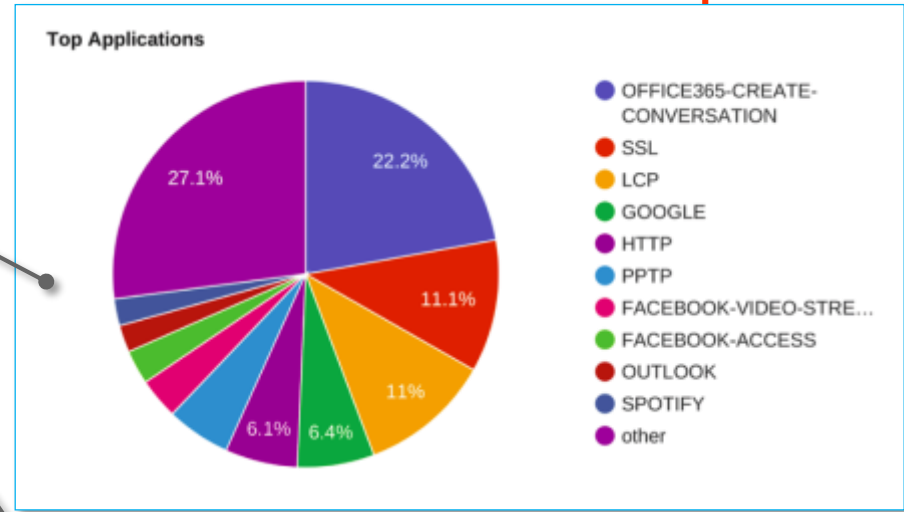
レポート機能



脅威レポート・システムモニタリング機能

・ ANR (アプリケーションとネットワーク脅威レポート) 機能
Sky Enterprise にて機器のトラフィックログを分析し、
レポートの自動生成が可能

・ システムモニタリング機能
機器データ(CPU、メモリ、セッションなど)をグラフ表示



Total AppSecure Data: 0.7 TB (top 10: 0.5 TB, others: 194 GB)

Application Name	Sessions	Bytes	Category	Risk (1= low, 5= high)
OFFICE365-CREATE-CONVERSATION	595427	159 GB	Web	4
SSL	1120819	79 GB	Infrastructure	1
LCP	688	79 GB	Infrastructure	2
GOOGLE	105584	46 GB	Web	3
HTTP	1364767	43 GB	Web	5
PPTP	220572	38 GB	Web	4
FACEBOOK-VIDEO-STREAM	22175	24 GB	Web	2
FACEBOOK-ACCESS	102023	20 GB	Web	5
OUTLOOK	53833	16 GB	Web	3
SPOTIFY	17578	16 GB	Multimedia	2



THANK YOU

JUNIPER
NETWORKS

Engineering
Simplicity