柔軟で強固なネットワークセキュリティを実現するセキュリティソリューション

Oct29, 2019

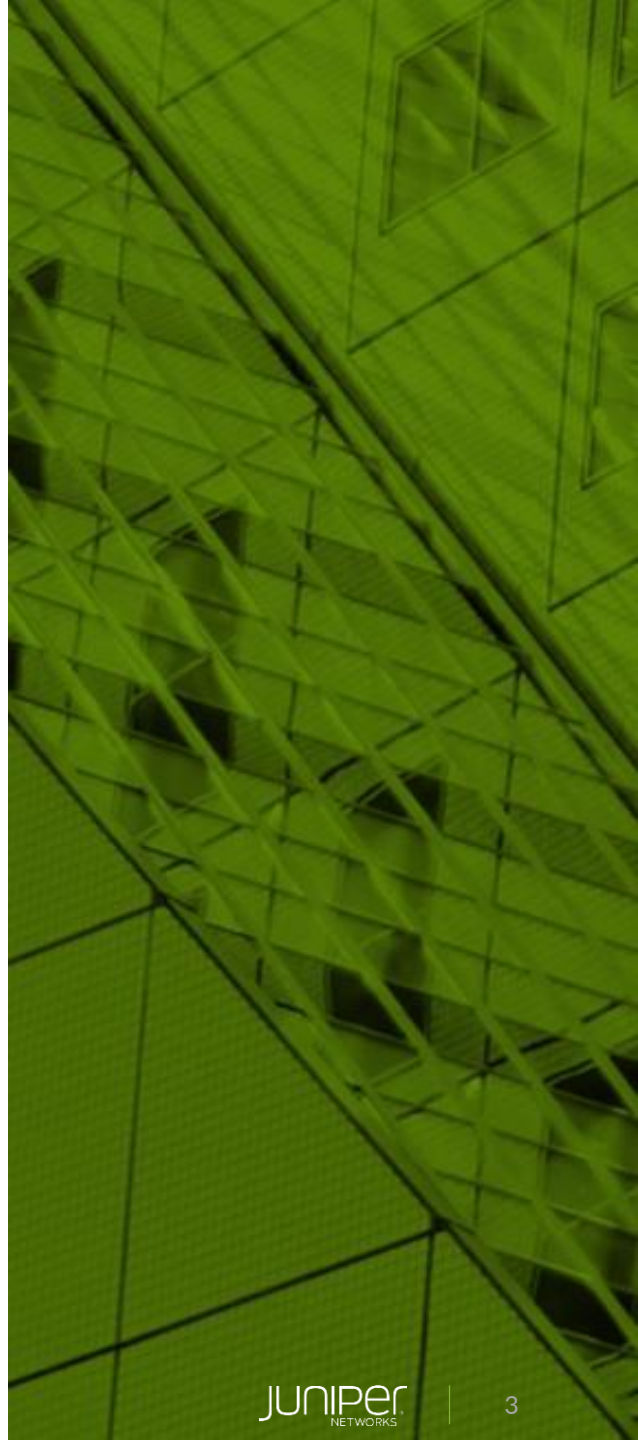
ジュニパーネットワークス
技術統括本部

JUNIPer NETWORKS | Engineering Simplicity

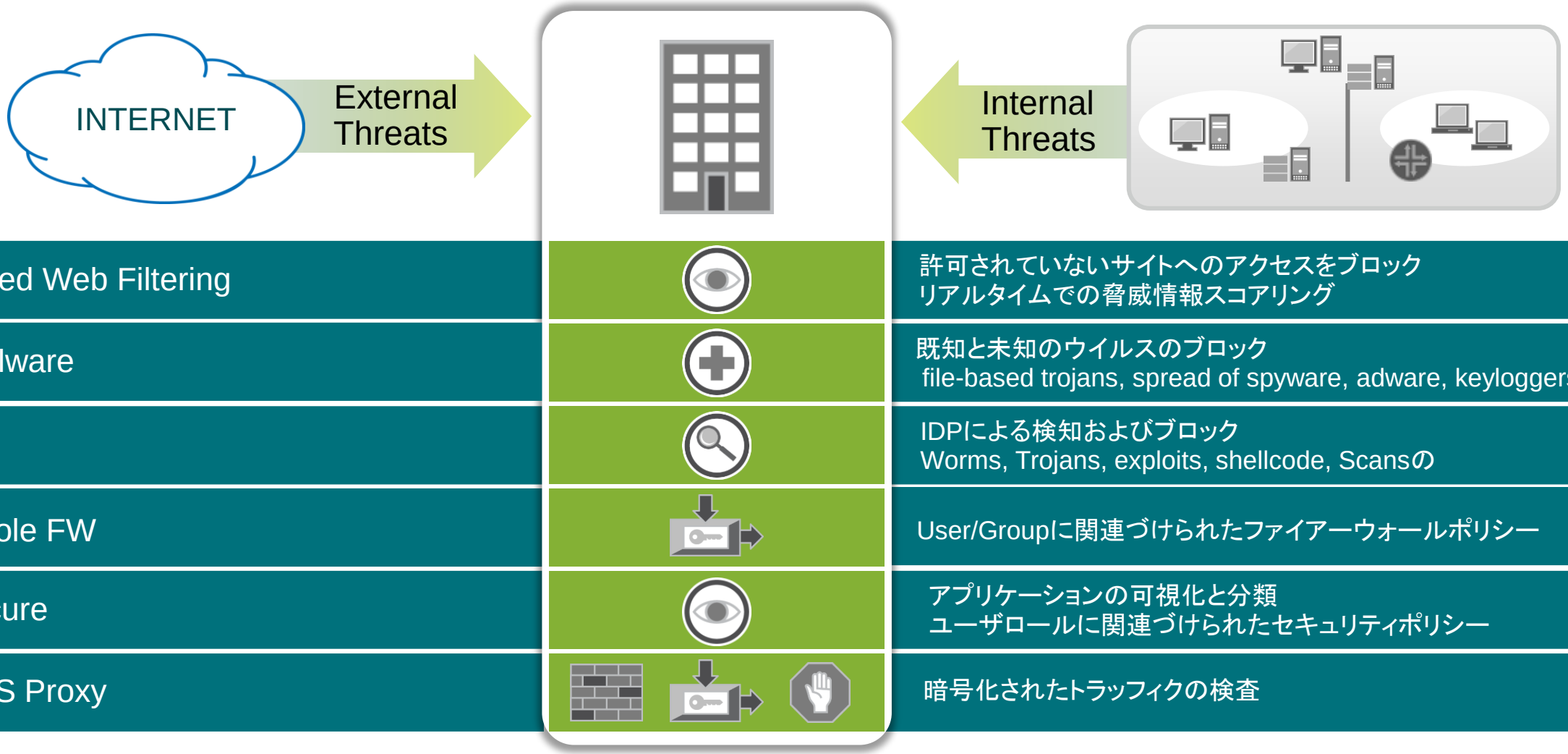
アジェンダ

- Connected Security の中核を担うSRX
  追加/新新機能・モジュールご紹介
- Connected Securityのテスト結果ご紹介
- セキュリティ機以外のSRX活用術
  容易に導入できて、ユーザ体感を改善するエンタープライズSD-WAN
- まとめ
  時代のニーズにあわせて進化し続けるSRX

CONNECTED SECURITY の中核を担うSRX
追加/新機能・モジュールご紹介

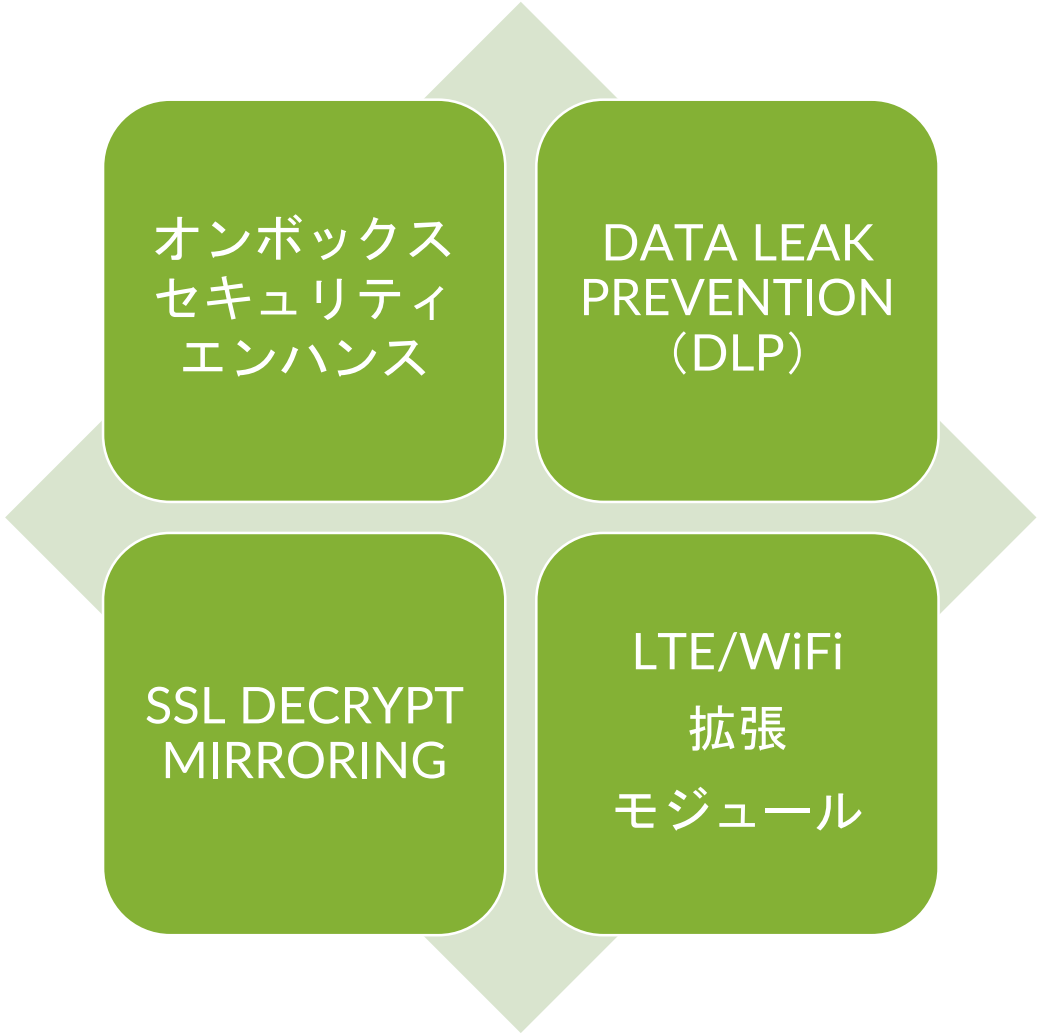


SRX セキュリティ機能概要

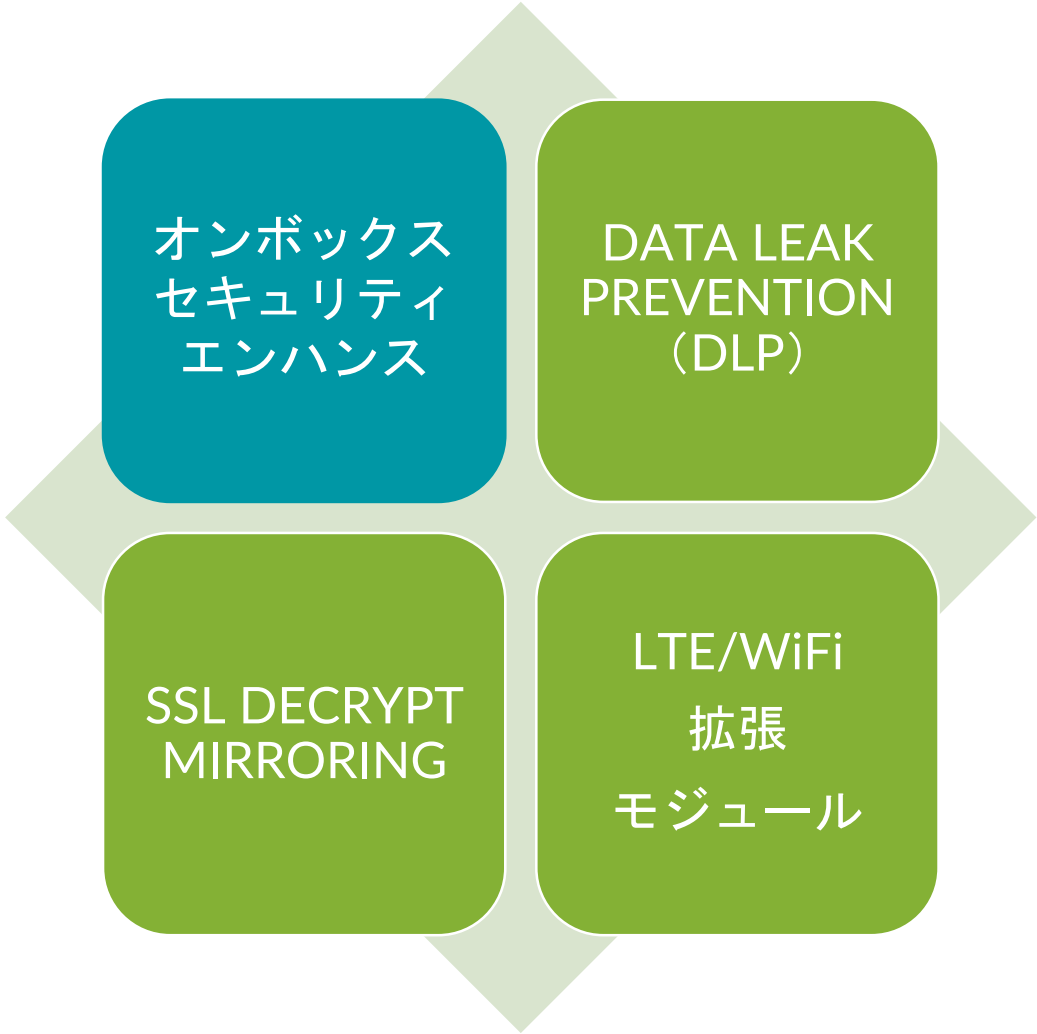


セキュリティ SWISS ARMY KNIFE

様々な機能追加により柔軟なネットワークセキュリティを実現



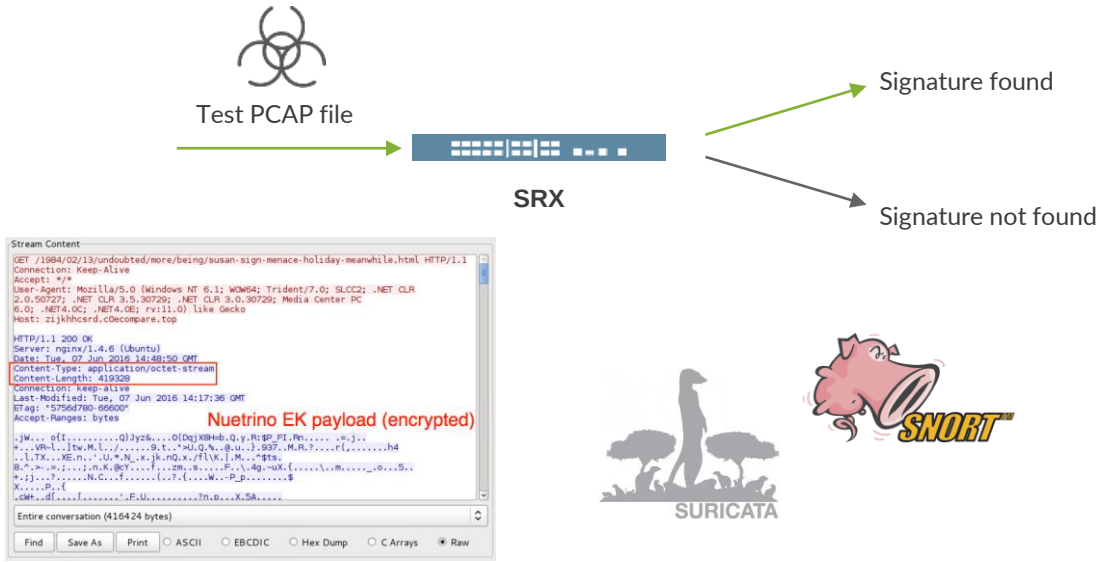
オンボックスセキュリティエンハンス



IDP インスペクションエンジンのエンハンス

想定される問題およびユースケース

- 既存のFWで更なるパフォーマンスが欲しい
- 迅速かつ簡単にシグネチャのチェックがしたい
- ”https://www.malware-traffic-analysis.net/ ”のようなopen/freeのツールで様々な攻撃に対するテストをしたい



エンハンス

- PCAPファイルをインポートして、IDP/IPSシグネチャのマッチングにより攻撃をブロックできるか確認可能
- Content-based C2 シグネチャ
- Fast Patterns を含むSNORT & Suricataのシグネチャサポート

利点

- シグネチャがある攻撃に対して検知可能か簡単に確認可能
- オープンソース（SNORT&Suricata）のサポートによるシグネチャのレバレッジ
- トラフィックジェネレータが不要に（non-slaceテスト）
- シグンネチャパターンマッチングのインプルーブメント

※ロードマップとなります

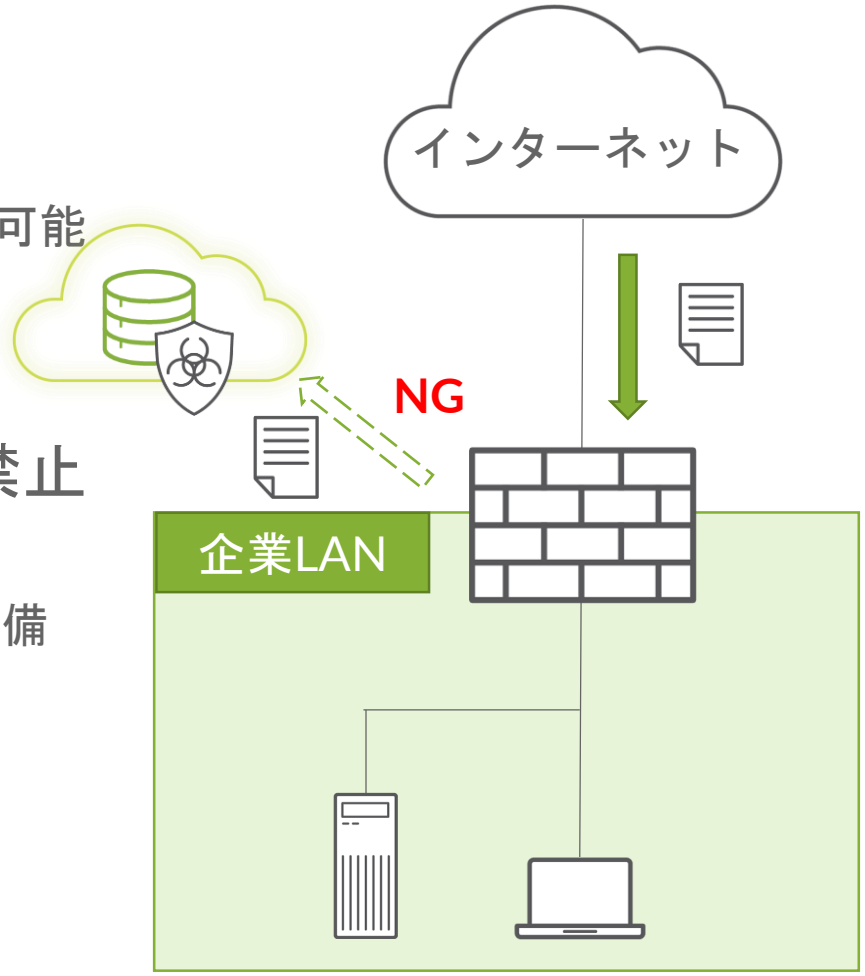
AVIRA オンボックス アンチウイルスエンジン

- SRXにデータベースをダウンロードしアンチウイルスを実施
- ウイルススキャン時に外部サーバへ問い合わせをすることなく、ローカルでのスキャンが可能となる
- インターネットに繋がっていない場合でも、ウイルス対策が可能に
- シグネチャDBのダウンロード先は、Juniper管理のクラウドもしくは、

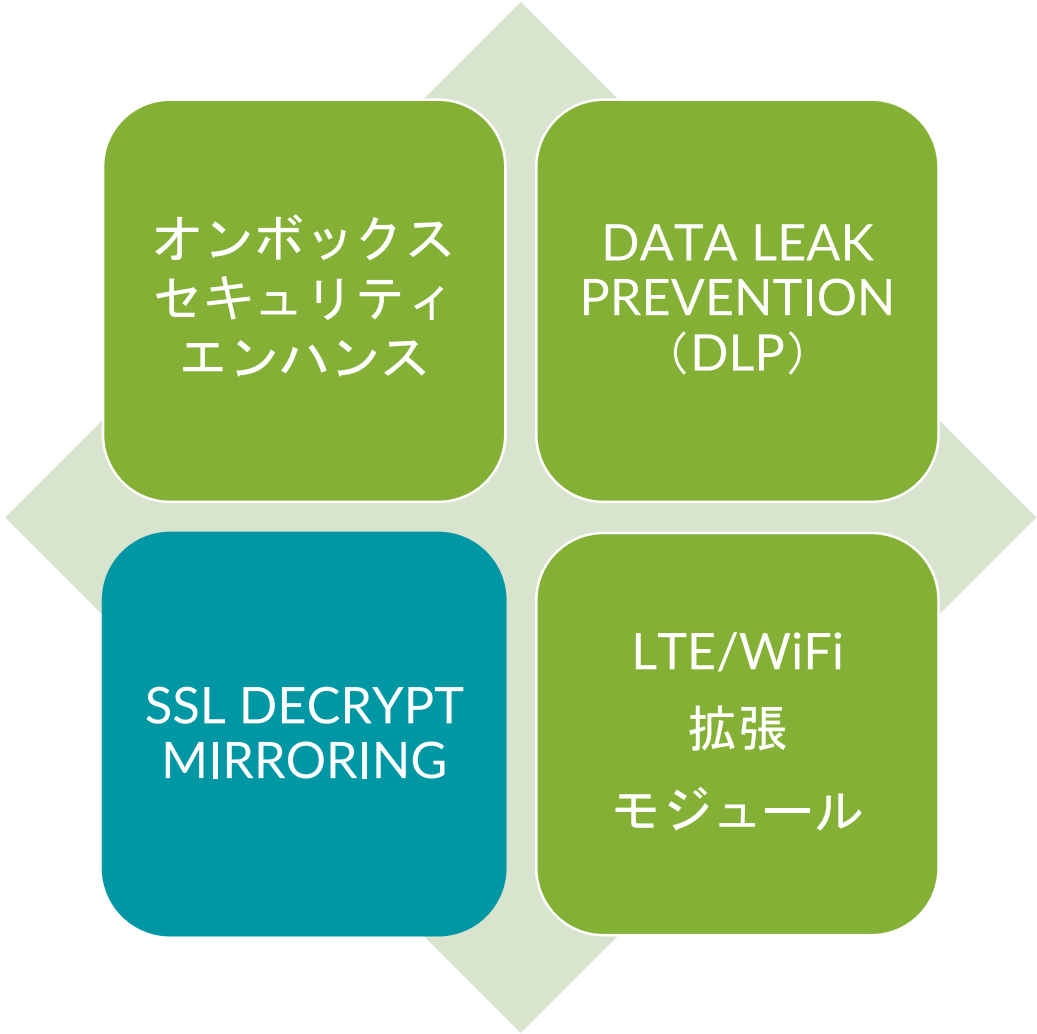
  ローカルのサーバに変更も可能

ユースケース例
～クラウド利用ができないお客様へのアンチウイルスとして～

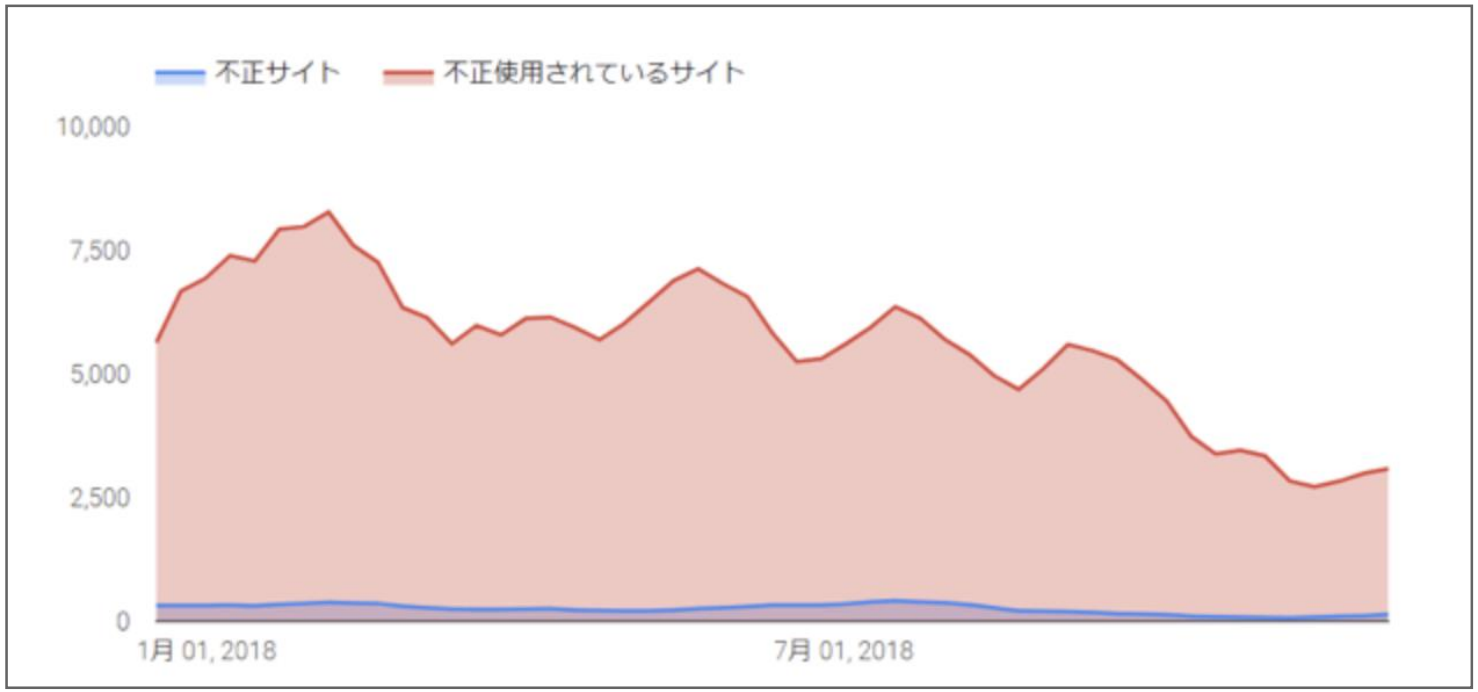
- ✓ファイルをクラウドにサブミッションできない
  - ✓ 機器の仕様書、個人情報、国家の機密情報など
  - ✓ オンボックスアンチウイルスにより、ローカルでのスキャンが可能
- ✓インターネットからのシグネチャダウンロードは禁止
  - ✓ ダウンロード先をLAN内のローカルサーバに変更が可能
  - ✓ 任意のタイミングでLAN内のローカルサーバにシグネチャを配備



SSL DECRYPT MIRRORING



SSLだからといって100%安心はできない時代に



企業などが運営する正規のWebサイトを改ざんして悪用する事例が圧倒的

“「常時SSL化」時代に向けたセキュリティ対策指南書” . 株式会社LAC
https://www.lac.co.jp/library/ssl/4.html

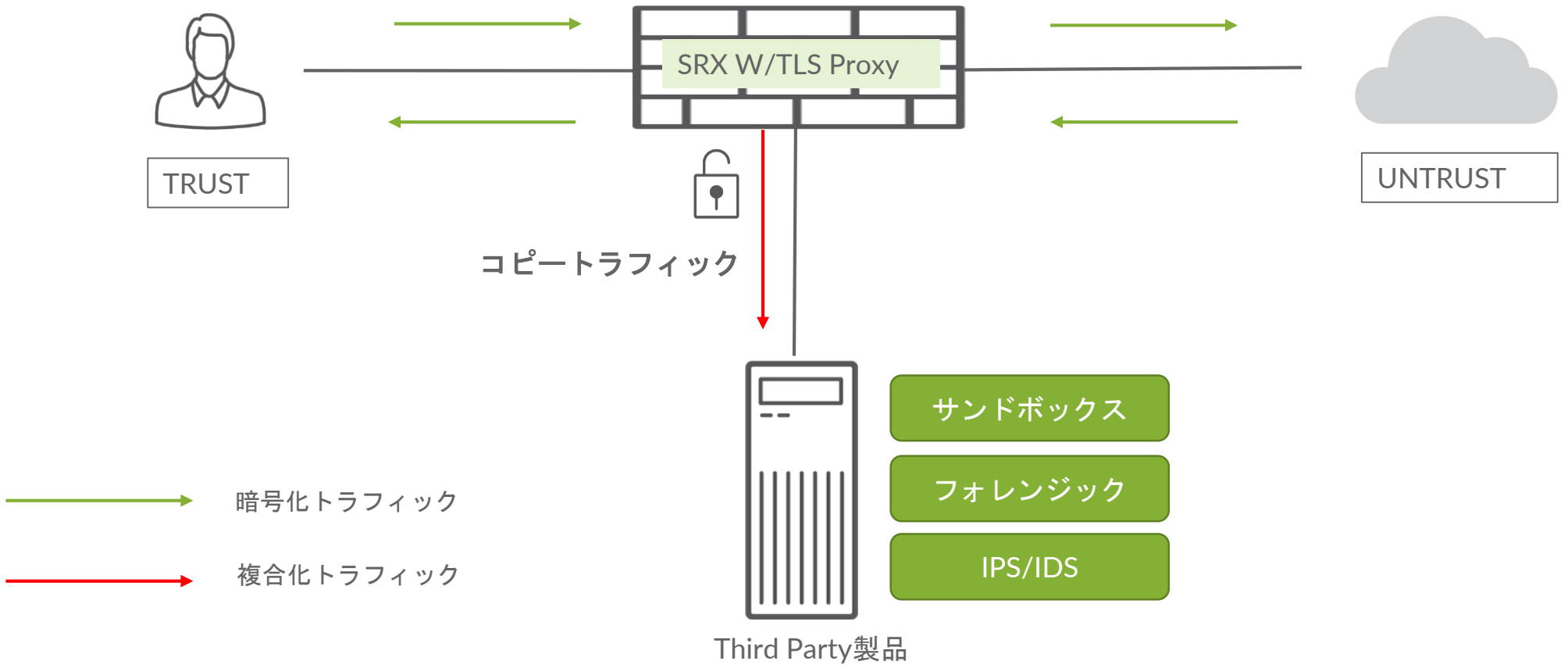
実例　米YOUTUBE 2018年4月

YouTubeで視聴回数トップだった「Despacito」のカバーイメージは、マスク姿で銃を構える集団の画像に置き換えられた（出典：The Verge）

“人気音楽ビデオが相次いで改ざん被害、YouTubeのVevoチャンネルでハッキング” . IT media エンタープライズ. https://www.itmedia.co.jp/enterprise/articles/1804/11/news058.html

SSL DECRYPT MIRRORING 機能概要

- SRXは、暗号化トラフィックを紐解き平文トラフィックをミラーポートから出力する

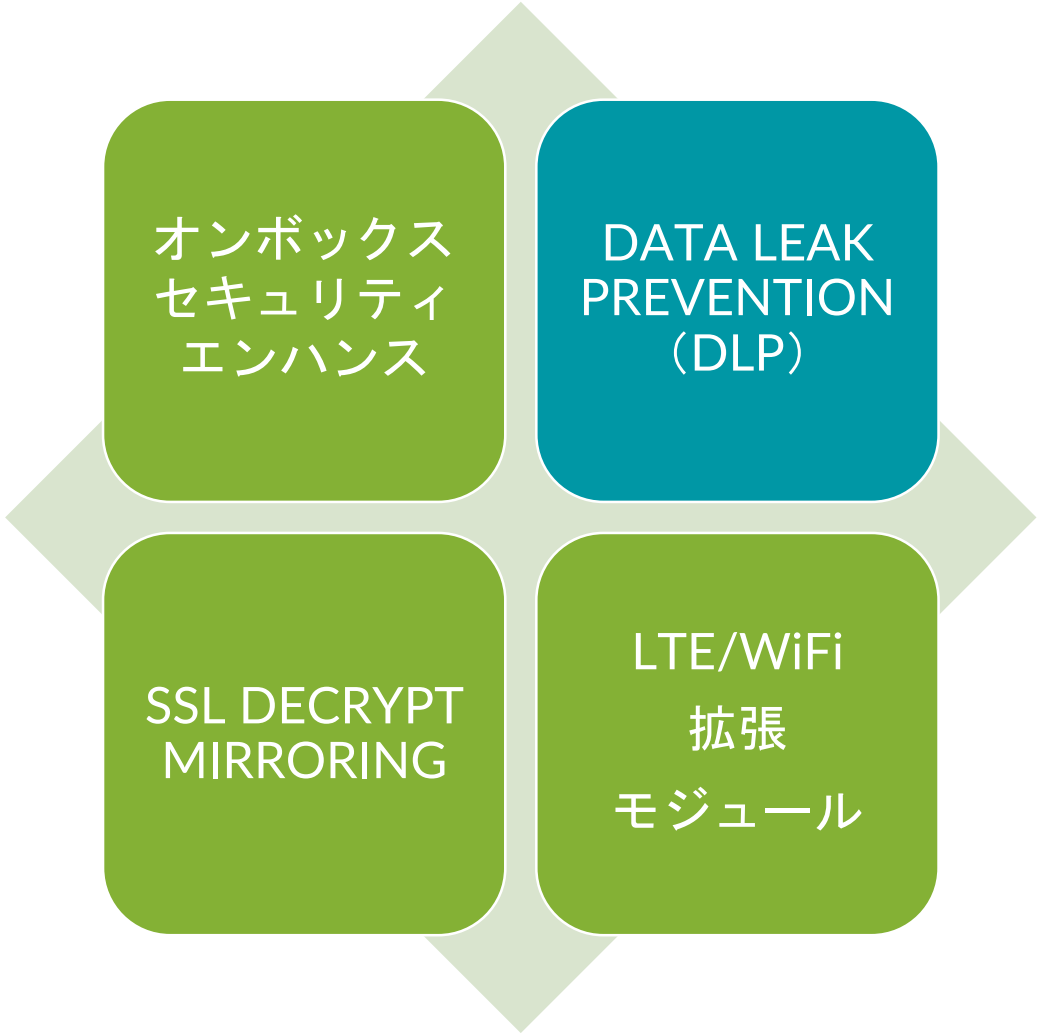


ユースケース例
～既存機器を有効活用したSSL対策として～

- ✓既にセキュリティ商材を持っているが、SSL通信は検査できていない、今後SSL通信を検査したいと考えている
- ✓セキュリティはSRXで実施しているが、有事に備えてフォレンジックでパケット情報を保存しておく必要がある

SRXでSSL Decrypt mirroringがサポート
平文でパケットの保存、セキュリティ検査も可能です
新たにSSL対応の商材を買いなおす必要はありません！

DATA LEAK PREVENTION (DLP)



データ漏洩は多大な被害をもたらす

2018年の主なデータ漏洩事件

1. Aadhar Cards – 11億件の情報
2. Mariott Starwood Hotels – 5億の予約顧客情報（パスポートなどの個人情報含む）
   Exactis – 3.4億の情報

その他のデータ漏洩

Equifax - 1.4億の機密情報

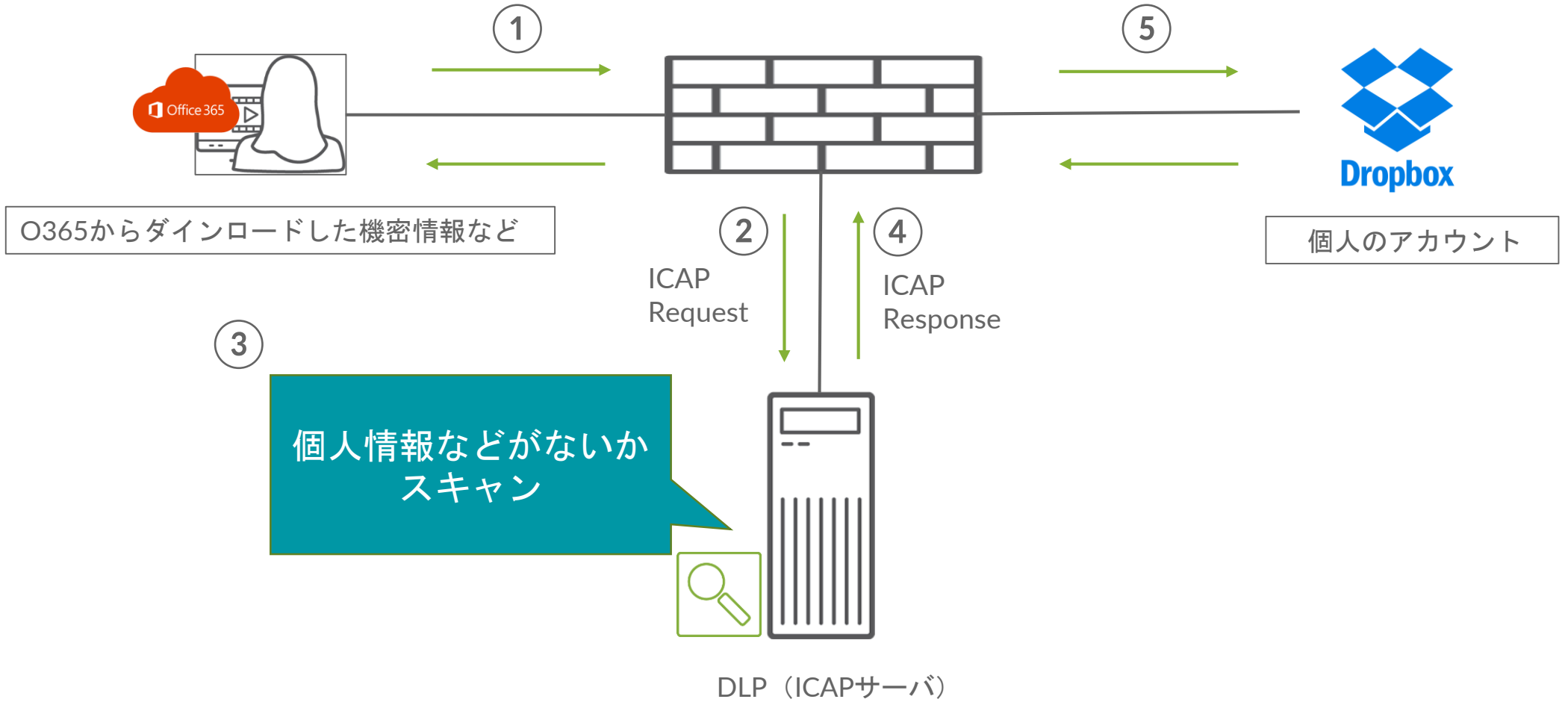
Target, Ashley Madison, Uber, Yahoo, Verizon,

その他多数

ICAP PROTOCOLとは?

- プロキシなどが外部の機器と連携して様々な機能を提供することができるプロトコル（ RFC3507で定義）
- HTTPベースのコンテンツをICAPサーバに渡す際に使用するプロトコル
- ICAPサーバは受け取ったコンテンツに対して、フォレンジックやDLP など自身が持つ機能を実施する

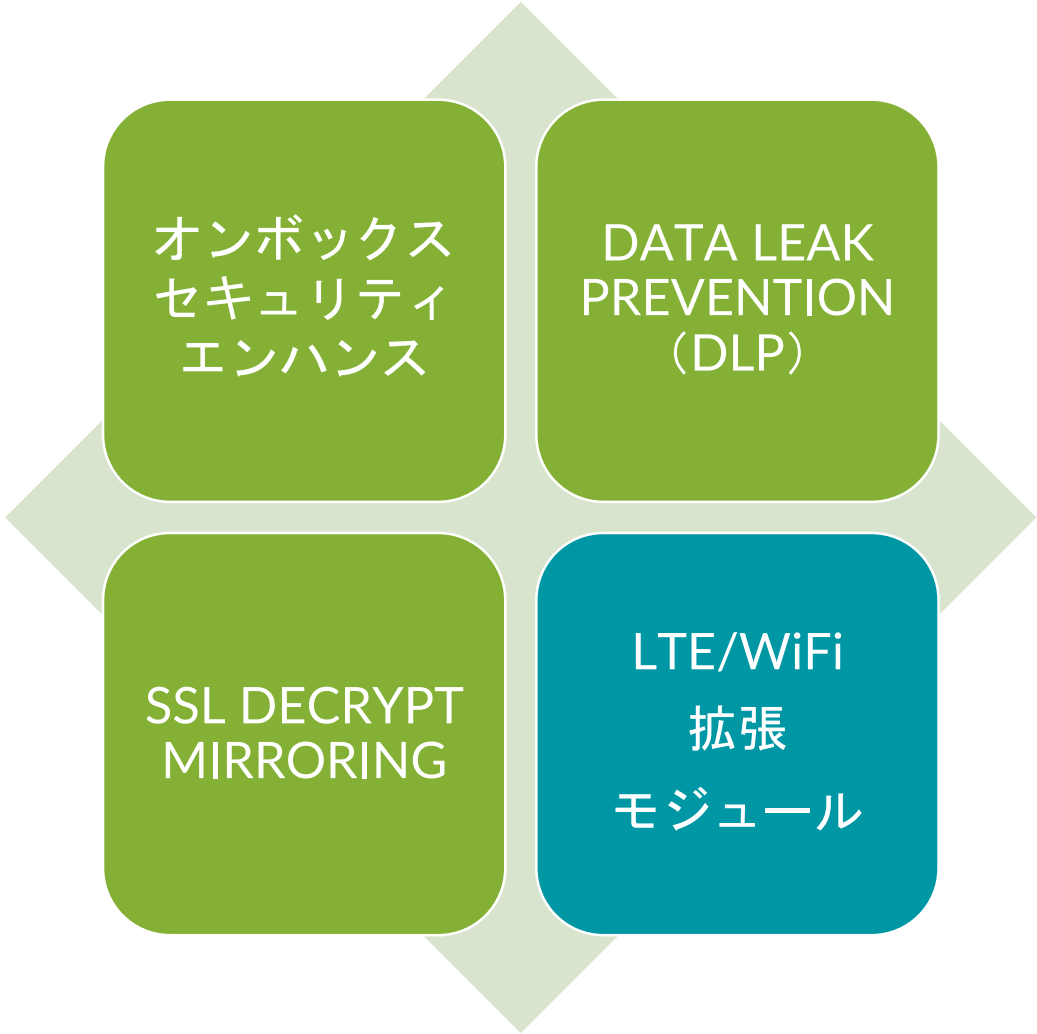
DATA LOSS PREVENTION (DLP)との連携例



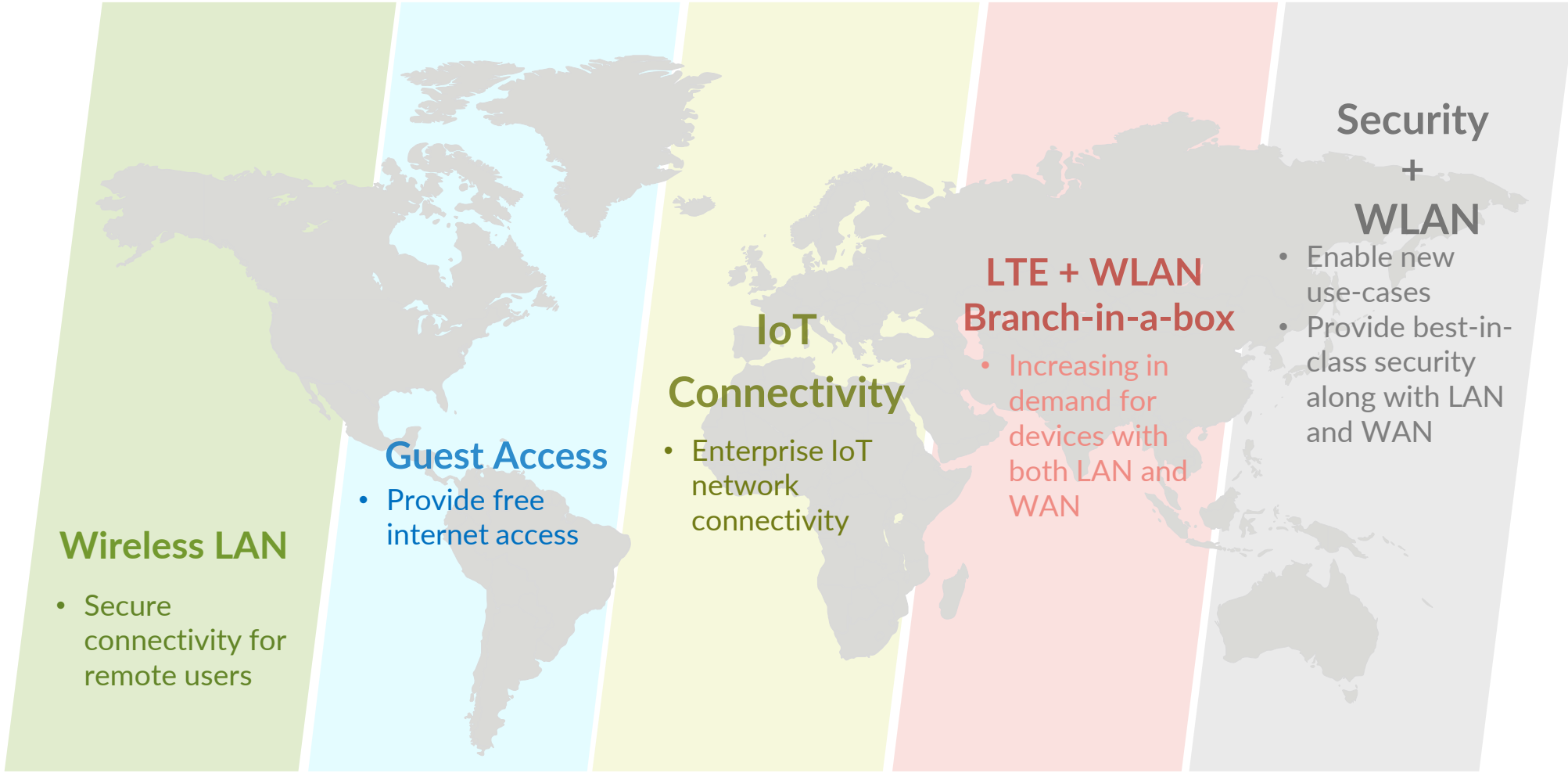
相互検証を踏まえてのICAP TIPS

- ✓機器によって実装の違いが存在する
  - ✓ REQMOD, RESPMODそれぞれの対応有無
  - ✓ ICAP Request のオプションヘッダ有無
  - ✓ ホストアドレスを確認するフィールドの違い
- ✓REQMOD対応のICAPサーバは、それぞれの実装依存
  - ✓ 悪性と判断されないURLでは検体をSubmissionしない機器も存在する
  - ✓ HTTPリクエスト先のレピュテーションのみを解析する機器も存在する
- ✓導入後にチューニングが必要な組み合わせも存在する

LTE/WIFI拡張モジュール



WIFIは現在では必要不可欠なインフラ



ユニークなLTE/WIFI拡張モジュール

- **Wi-Fi モジュール**

レイヤ3またはレイヤ2で動作
ボード上にCPUおよびメモリ搭載

- **用途**

リモートオフィスLAN
ゲストWiFi
SOHO LAN
IoT接続
キオスク
自動販売機

- **LTEモジュール**

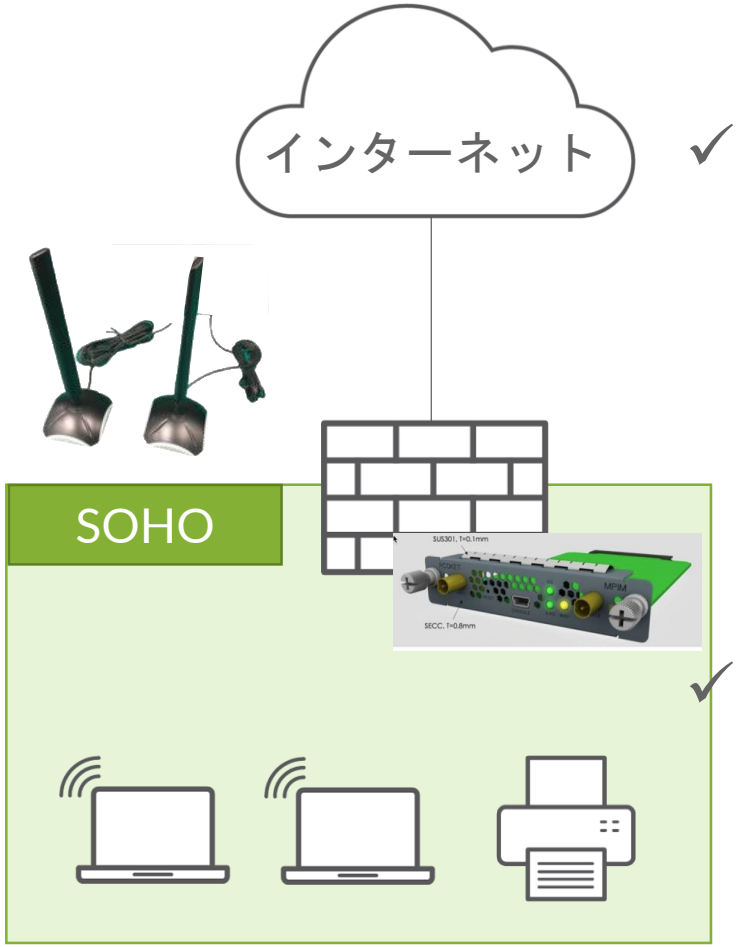
Sierra Wireless MC7430を採用
docomo, au, softbankの帯域に対応
SRX320, 340, 345,550Mで利用可能

- **用途**

バックアップ回線
イベント等一時的な設置
物理回線を引けない拠点
回線手配の間に合わない拠点

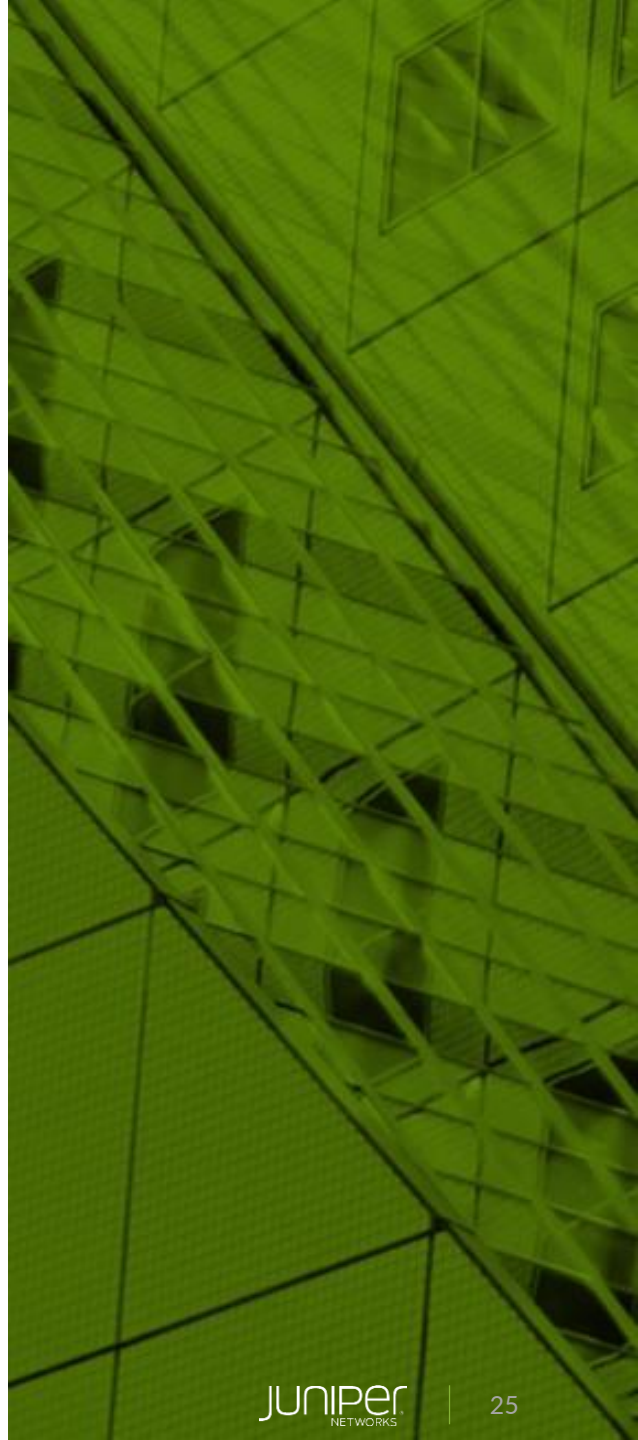
※Wi-FIモジュールはロードマップとなります

ユースケース例
～完全ワイヤレス化のALL-IN-ONE SECUREボックスとして～

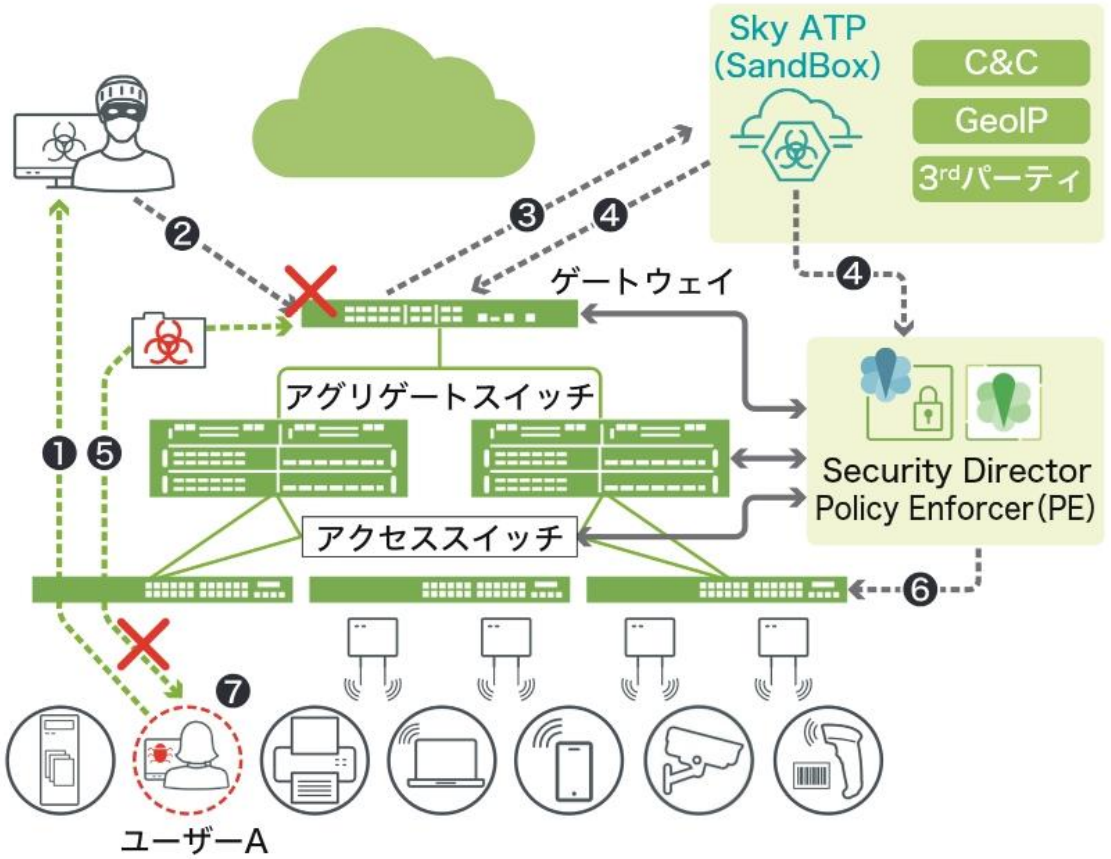


- ✓ 物理ケーブルなどは要らずWiFIのみ必要なオフィス（小規模拠点やSOHOなど）に最適
  - ✓ ルータの下に設置していたアクセスポイントが不要に
  - ✓ サブスクリプションでセキュリティ対策も可能
  - ✓ インターネットへの接続をLTEにすることで完全ワイヤレス化といった構成も可能
- ✓ 緊急時用のネットワーク提供
  - ✓ 災害発生時、避難場所でのネットワーク提供

CONNECTED SECURITY テスト結果ご紹介



SKYATPがマルウェア検知、EXにFIREWALLポリシーが設定されるまでの時間を計測



コネクテッドセキュリティの動作（1）

❶ ユーザーAはファイルをダウンロード
❷ SRXは対象ファイルをスキャン
❸ SRXはファイルをSky ATPへ送信
❹ Sky ATPはファイルのマルウェアを特定し、SRXとPEに通知
❺ SRXはファイルのダウンロードをブロック
❻ PEはユーザーA端末を隔離
❼ ユーザーA端末からの感染拡大を防止

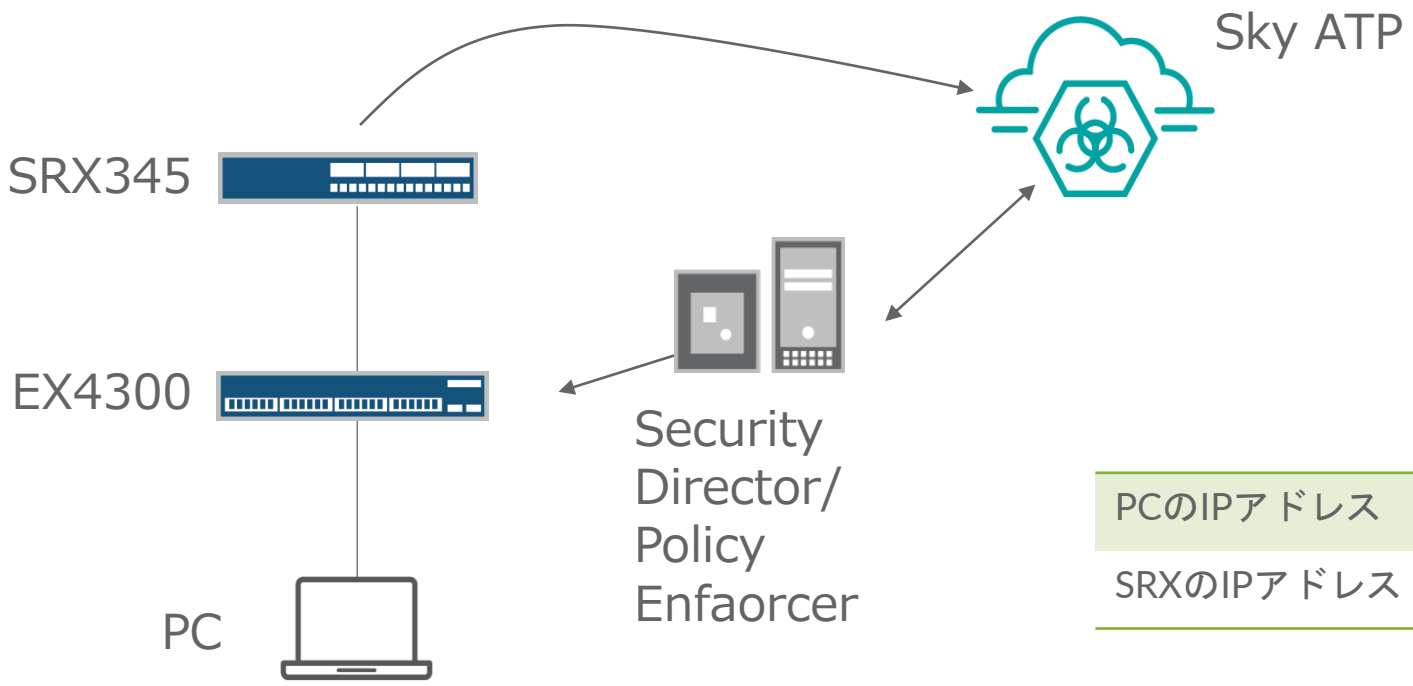
コネクテッドセキュリティの動作（2）

❶ USB等で感染したユーザーAはC&Cサーバへのアクセスを試行
❷ SRXはSky ATPからのブロックリストに基づき、C&Cサーバとの通信を遮断

①→⑥までに要した時間を計測してみました。

検証構成イメージ図

No.	検証箇所	内容	検証方法
1	PC	外部への通信がブロックされたか	ping –t 8.8.8.8が通らなくなる
2	PC	GWへの通信がブロックされたか	ping –t 192.168.1.1が通らなくなる



PCのIPアドレス	192.168.1.154
SRXのIPアドレス	192.168.1.1

テスト結果

イベント1	イベント2	平均時間
[PC] マルウェアダウンロード	[Sky ATP] 検知	0:00:04
[Sky ATP] 検知	[EX] Firewall MAC filter 作成	0:01:28

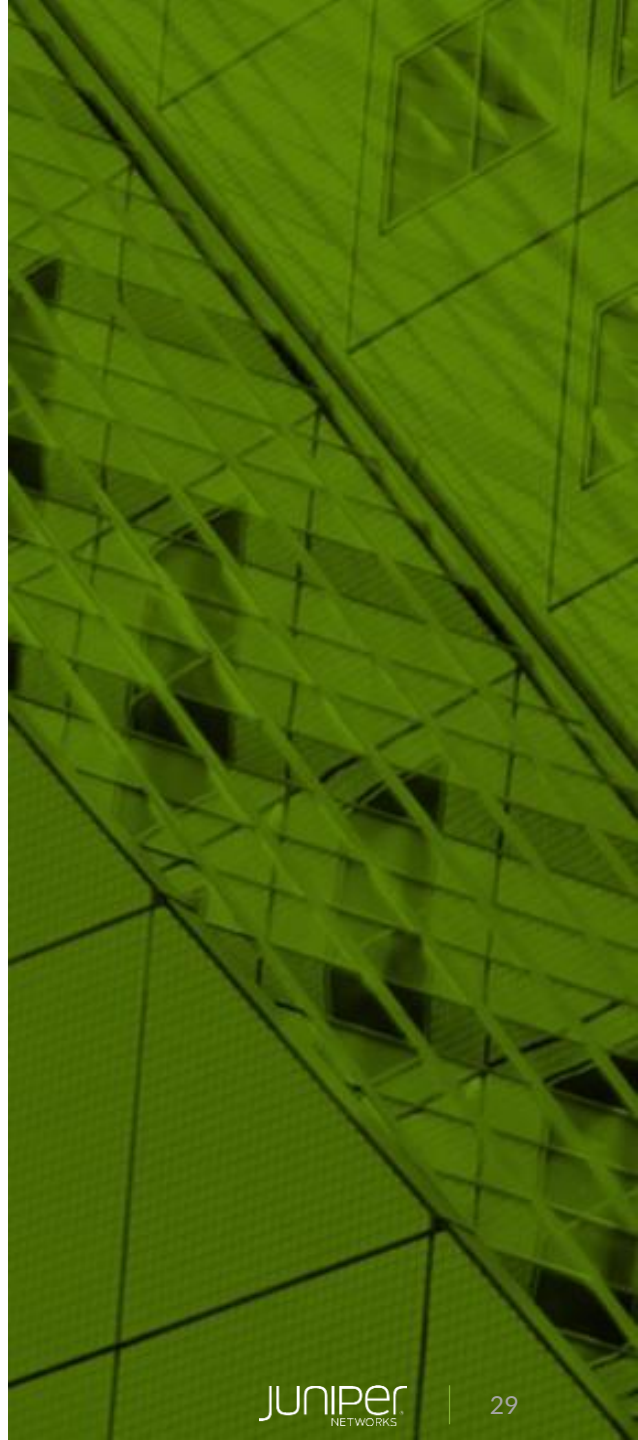
～参考タイムスタンプ～

1. テストファイルダウンロード at 4:46:00 pm.
2. SkyATPが検知 at 4:46:05 pm.
3. SkyATPが感染ホストのリストをSRXにアップデート at 4:47:34 pm.
4. SkyATPが感染ホストのリストをPolicy Enforcerにアップデート at 4:47:35 pm.
5. Policy Enforcerが感染ホストのMACアドレスをEXにアップデート at 4:47:44 pm.
6. PCからのトラフィックブロックされる at 4:47:45 pm.

EXにフィルタが適応されるまで、約1分30秒

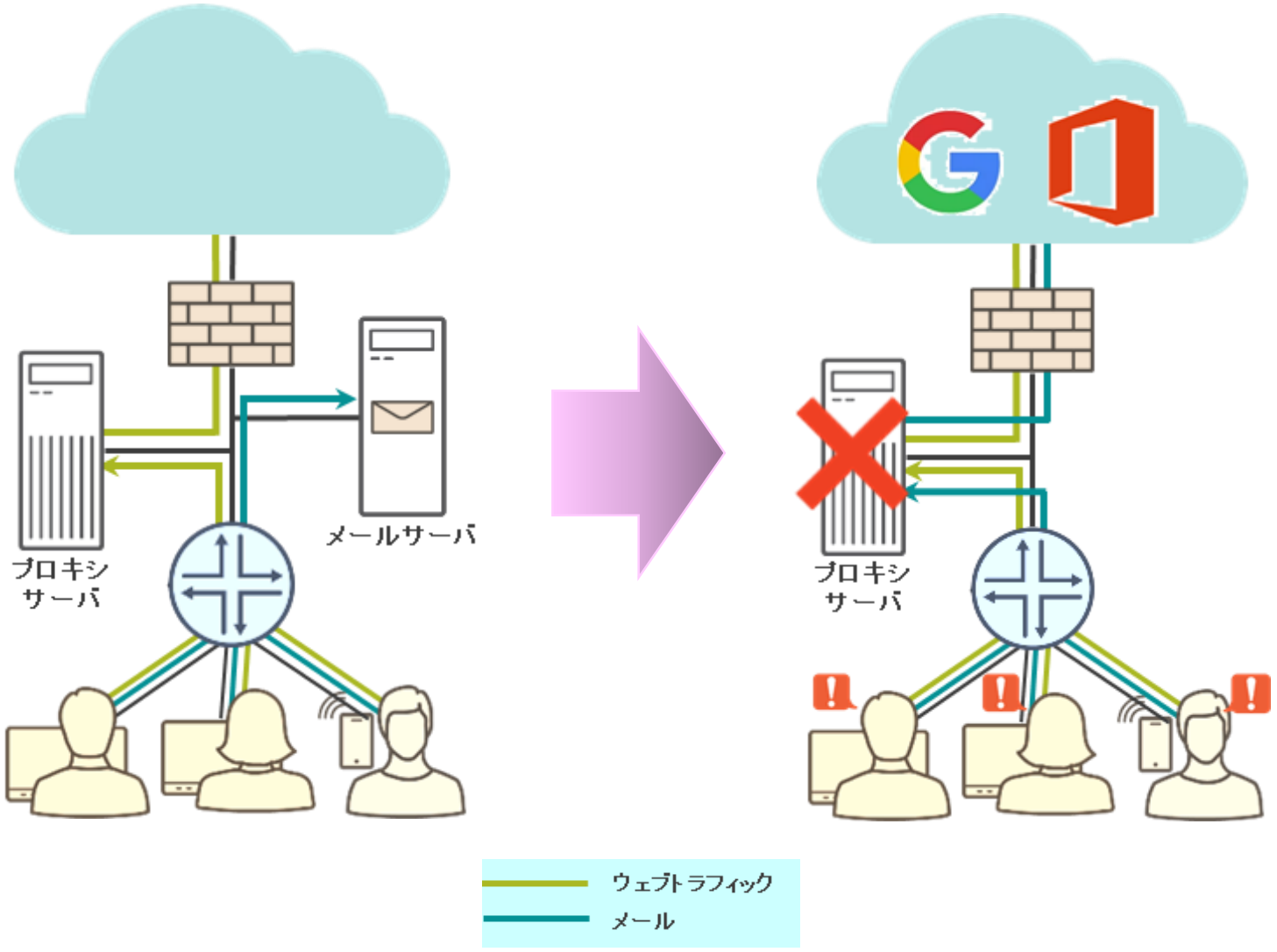
※テストするファイルによって結果は異なる可能性がございます

容易に導入できて、ユーザ体感を改善する
エンタープライズSD-WAN



アプリケーションの応答性が低下する要因

ユーザ体感品質の改善



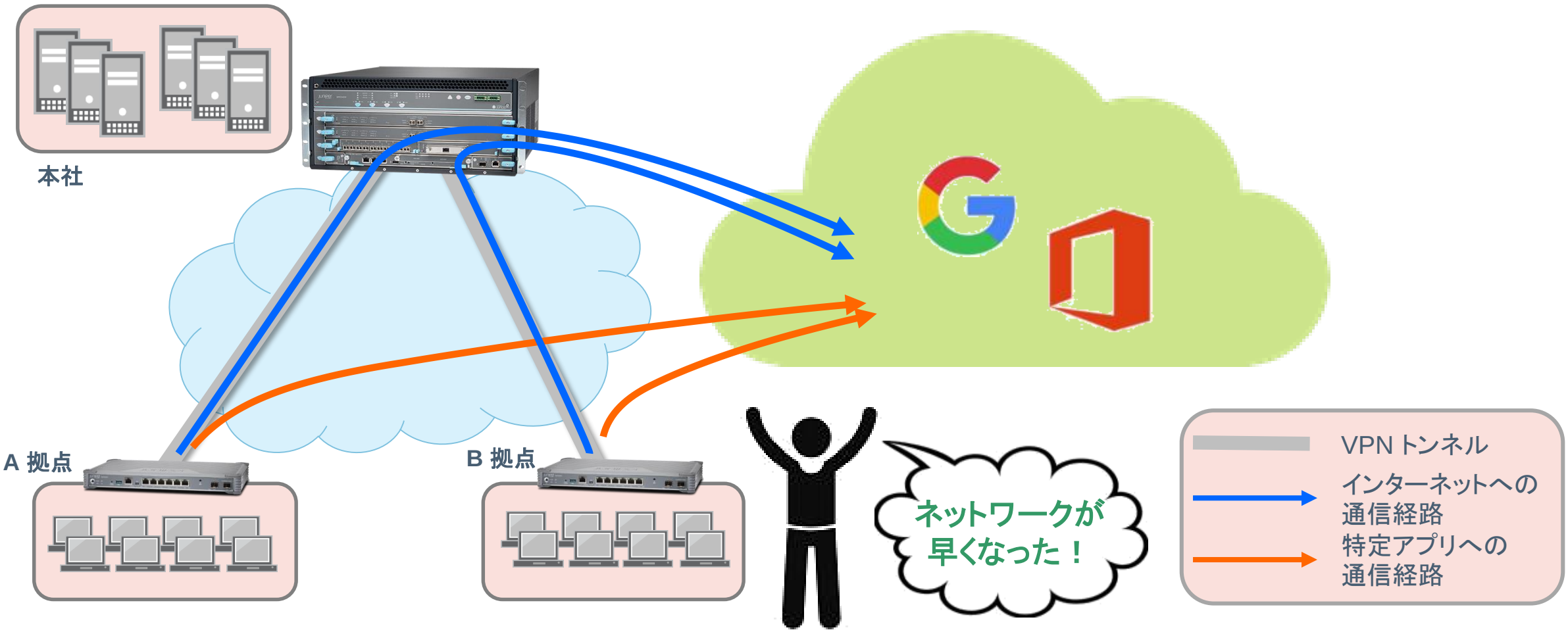
メールやアプリケーションサーバを
クラウドに移行すると、インターネットや
WANトラフィックを管理するサーバの
負荷が増大。

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。

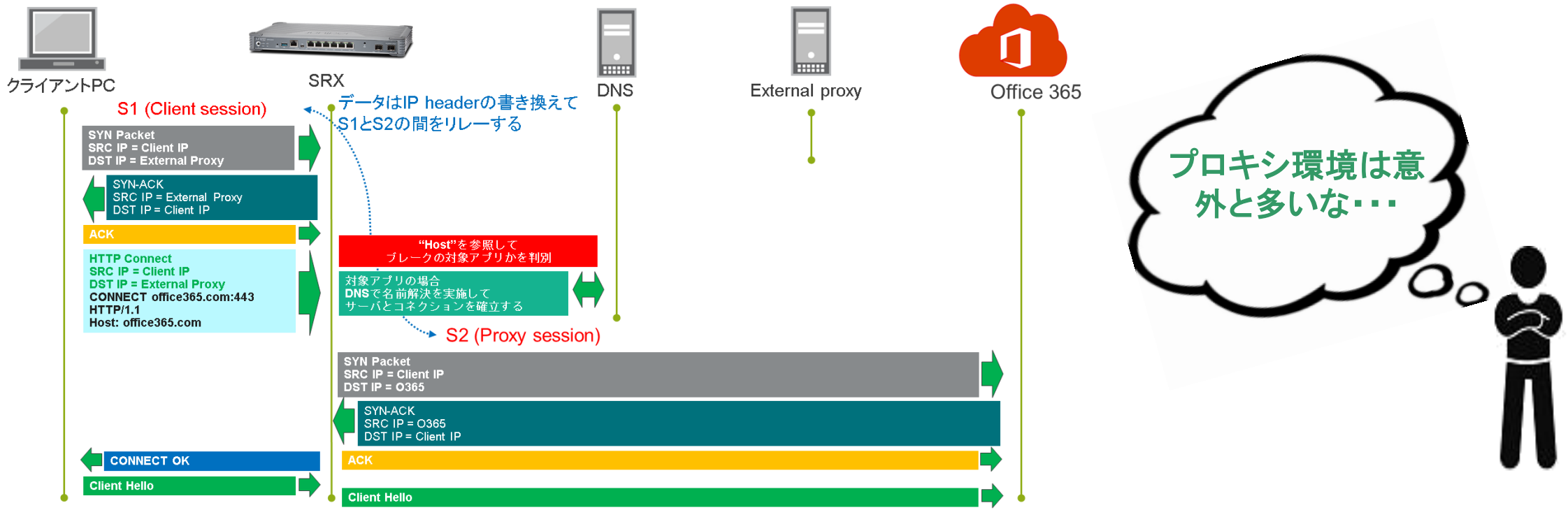
クラウドアプリケーションを識別して最適な経路にルーティング

ユーザ体感品質の改善

- 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



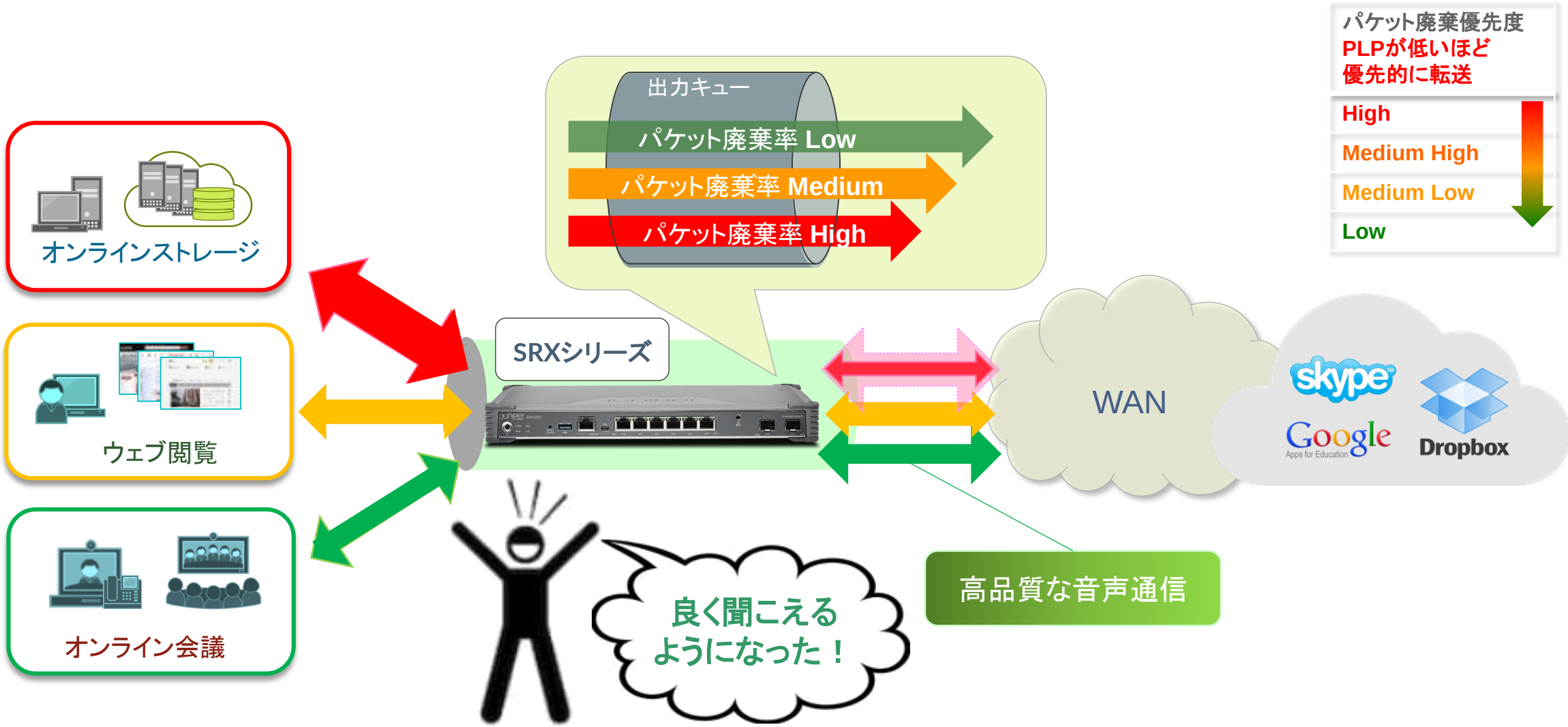
25

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

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

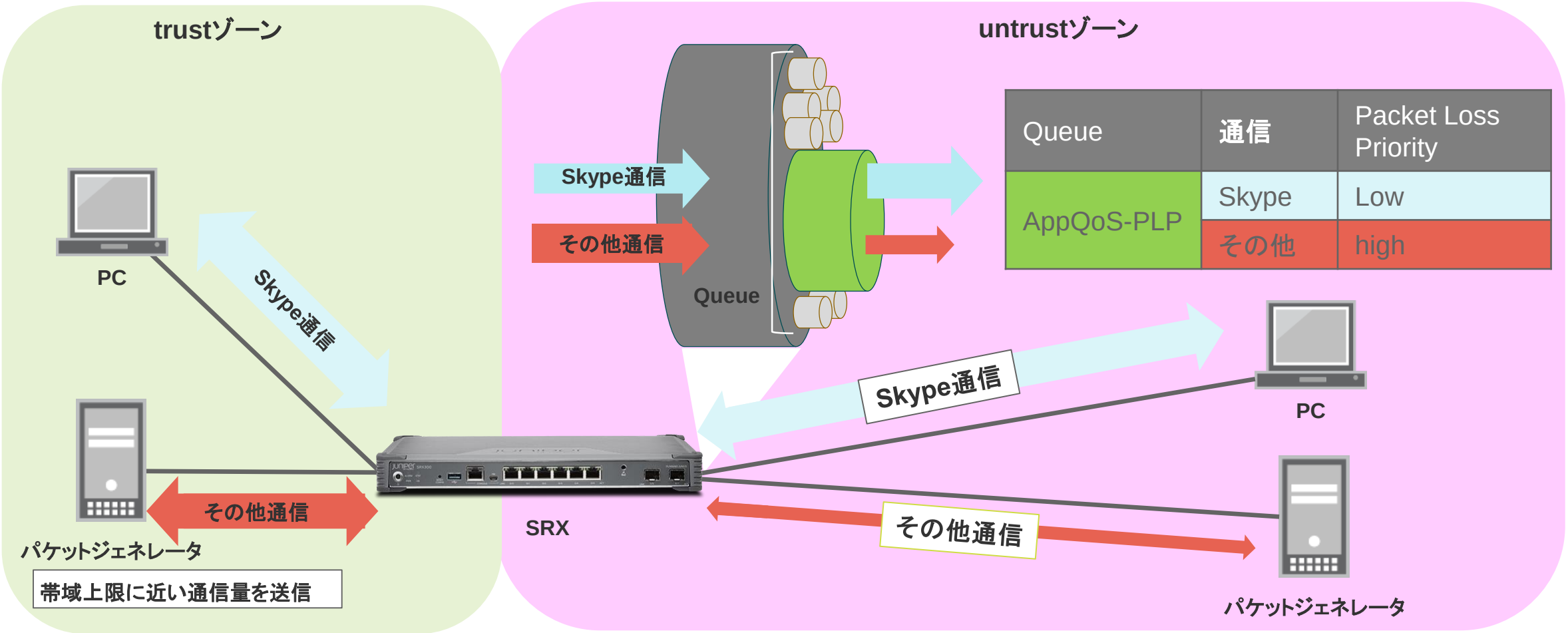
ユーザ体感品質の改善



AppQoSデモ

ユーザ体感品質の改善

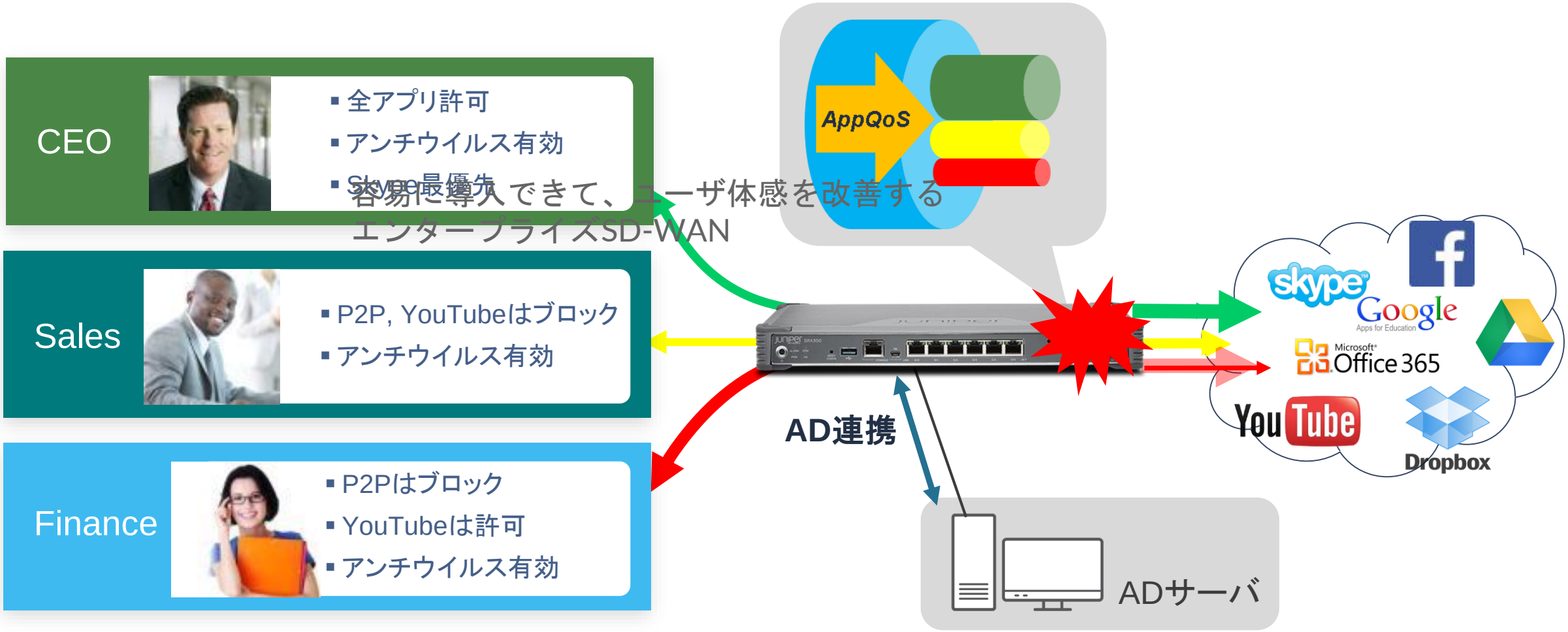
帯域上限に近いトラフィックを送信し、Skypeビデオ映像の乱れを比較



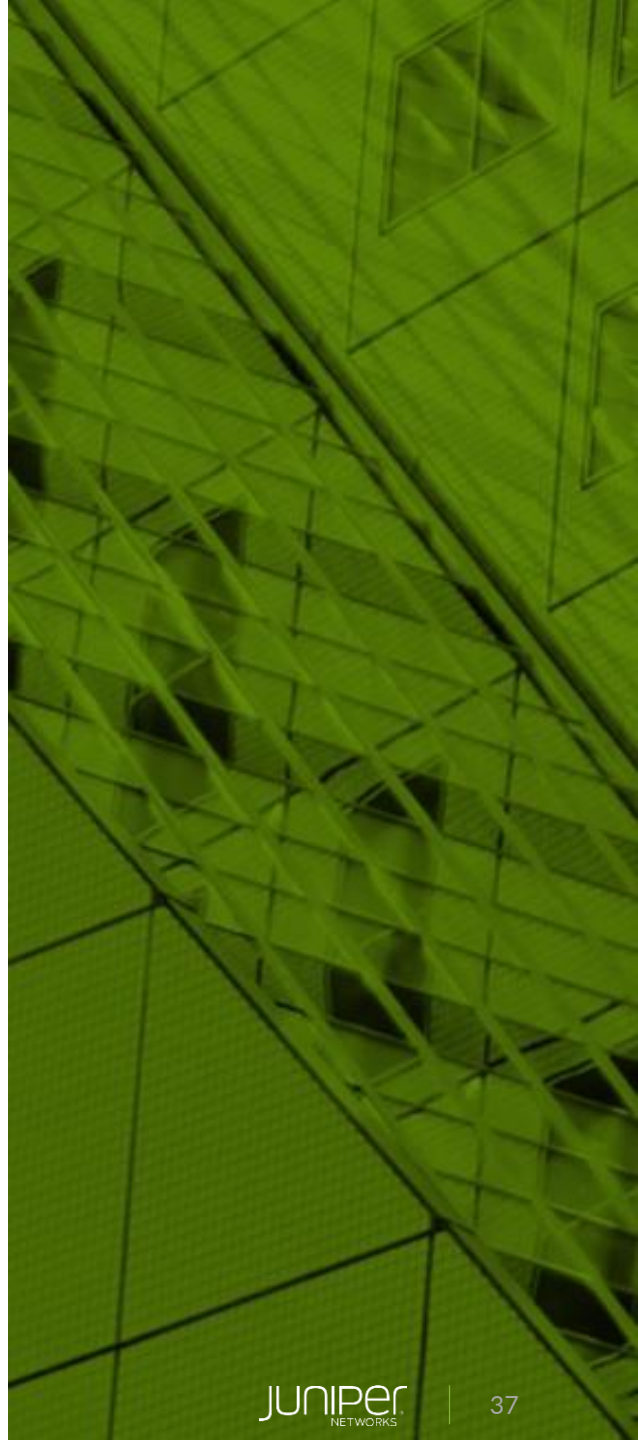
Queue	通信	Packet Loss Priority
AppQoS-PLP	Skype	Low
	その他	high

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



まとめ
時代のニーズにあわせて進化し続けるSRX



時代のニーズにあわせて進化し続けるSRX

拡張性	➢ 新たな機能をソフト/モジュールの両方で追加し続ける ➢ SRXの高い投資効果
セキュアな構成	➢ 感染ホストをアクセススイッチで隔離し横の感染を封じ込める ➢ 検知から隔離までを自動/迅速に対処
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 ➢ 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制御


THANK YOU
JUNIPER NETWORKS
Engineering Simplicity