



APAC Cohesion  
Juniper Secure Edge  
いつでも どこでも ユーザーを安全に守る  
Tech Roundup Q4-2022

ジュニパーネットワークス株式会社

# あらゆる接続ポイントにセキュリティを拡張し、ユーザー、アプリケーション、インフラを保護します



## 脅威を認識するネットワークの力



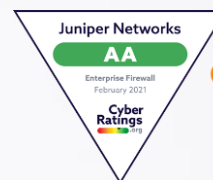
## 上位 10 社のうち 9 社

グローバルサービスプロバイダーがジュニパーを利用してモバイル加入者ネットワークの接続とセキュリティ確保を実現

ネットワーク・セキュリティ・チームの節約

# 20%

ジュニパーのセキュリティ・ソリューションの導入により、20%の時間短縮を実現



AIセキュリティ  
機械学習

2022年 ガートナー・ピアインサイト「顧客の声」。ネットワーク・ファイアウォールGARTNER PEER INSIGHTS CUSTOMERS' CHOICEバッジは、Gartner, Inc.および/またはその関連会社の商標およびサービスマークであり、許可を得てここに使用されています。

無断転載を禁じます。Gartner Peer Insights Customers' Choiceは、文書化された手法に基づき適用された個々のエンドユーザーのレビュー、評価、およびデータによる主観的な意見であり、ガートナーまたはその関連会社の見解を表すものではなく、推奨を意味するものではありません。

© 2022 Juniper Networks

Juniper Business Use Only

JUNIPER NETWORKS



# Juniper Secure Edge





# Agenda

- SASE の概要
- JSE 展開の詳細
- CASB と DLP
- ロードマップ
- リソース

# デジタルの世界は変化している



## 進化するアーキテクチャの回復力とスケーラビリティ

現在 1 つの組織は平均して 2.6 のパブリッククラウドと 2.7 のプライベートクラウドを使用しています。



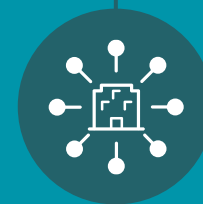
## どこからでもすべてにアクセス

労働者の 75% が週に2~3日以上自宅で仕事をするようになります。



## サイバー攻撃の成功率が急増

企業の 63% が侵害されゼロデイエクスプロイトの使用は 2021 年に2倍以上になりました。



## ネットワークは高度に分散されより複雑になっています

IT エグゼクティブの 75% は自社のネットワークが複雑すぎて「懸念される」リスクがあると述べています。

# Juniper Connected Security

クライアントからワークロードまで、どこでも、どんな場所でも



ユーザー, アプリケーション および インフラストラクチャ  
すべての接続ポイントを安全に保護





# SASE の概要

# Juniper SASE

## AI-driven SD-WAN + Juniper Secure Edge



### AI-driven SD-WAN

 Marvis Virtual Assistant

-  フルスタックのブランチオペレーション
-  先進の AI & ML
-  セッションスマート・ネットワーキング
-  ゼロトラスト
-  セグメンテーション

+



### Juniper Secure Edge

- FWaaS**  アプリケーションコントロール
- SWG**  アイデンティティとアクセスコントロール
- CASB**  侵入防止
- DLP**  アンチマルウェア
- ATP**  スレット インテリジェンス
-  セキュアなウェブアクセス

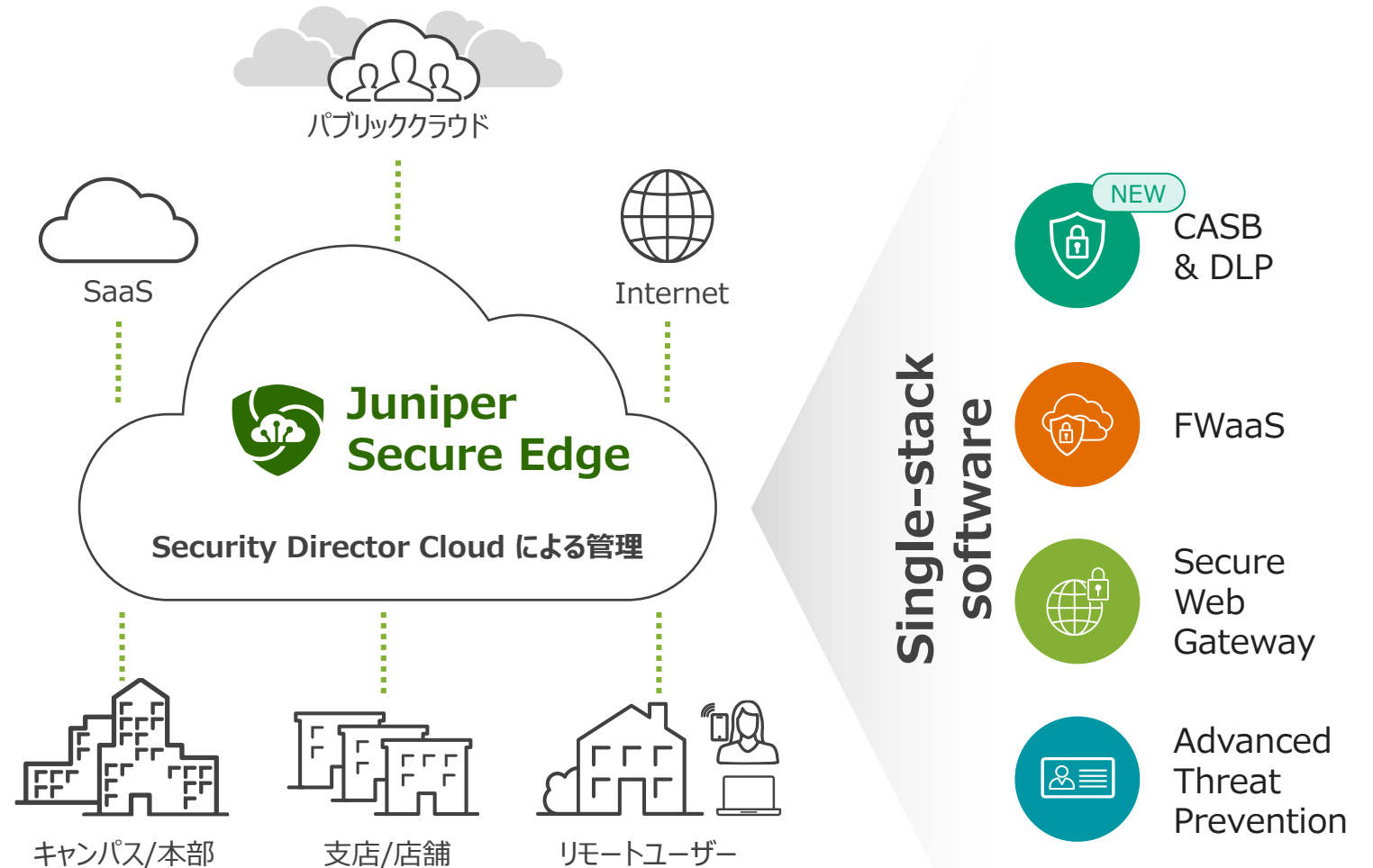


# Secure the Edge

あらゆる場所で  
ユーザーとデバイスを  
つなぎ、保護する

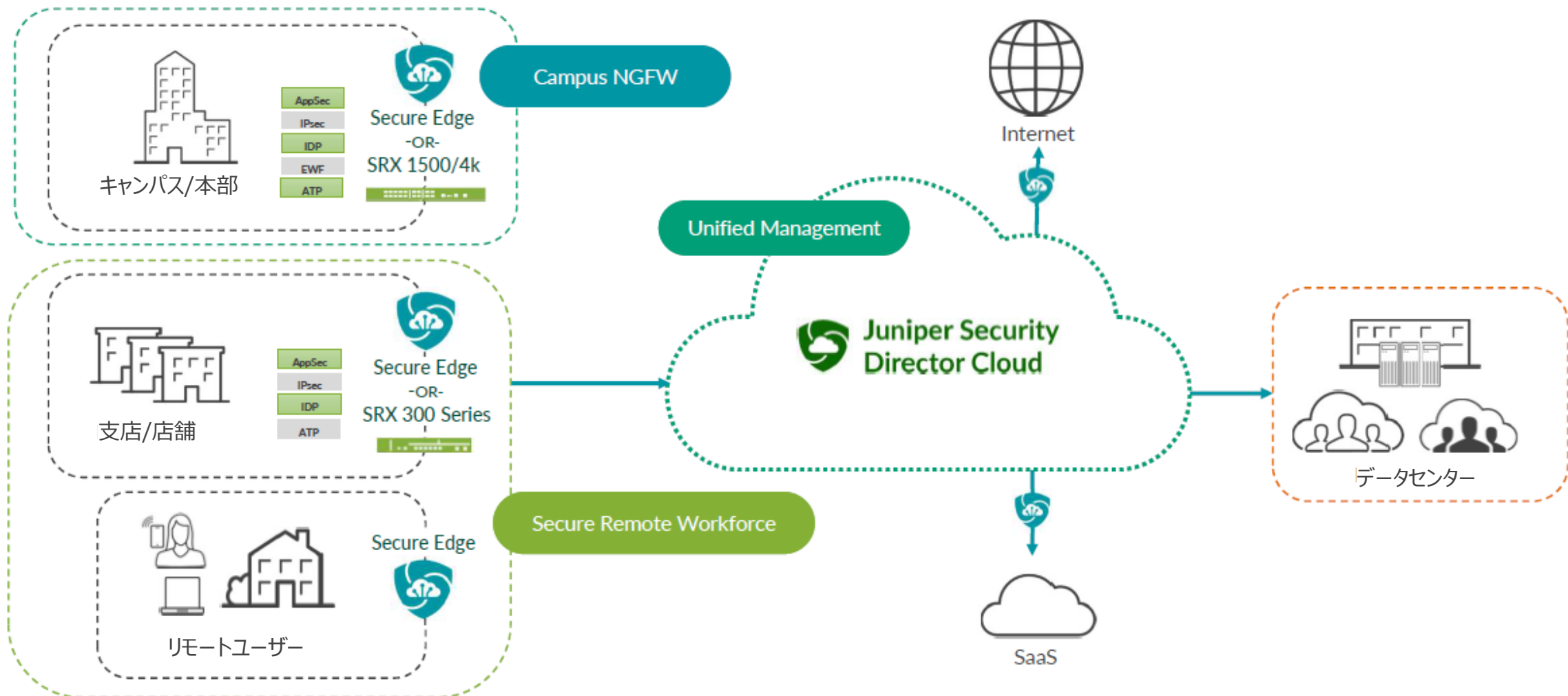
ジュニパーは優れた  
ファイアウォールセキュリティを  
提供し、ウイルスや不審な  
攻撃、脅威から ネットワークと  
資産を保護します。  
また、ファイアウォールは  
小規模なネットワークから  
大規模なネットワークまで  
パフォーマンスに影響を  
与えることなく対応することができます。

- ガートナー・ピインサイト 2021年6月号  
サービス機関のセキュリティ管理者



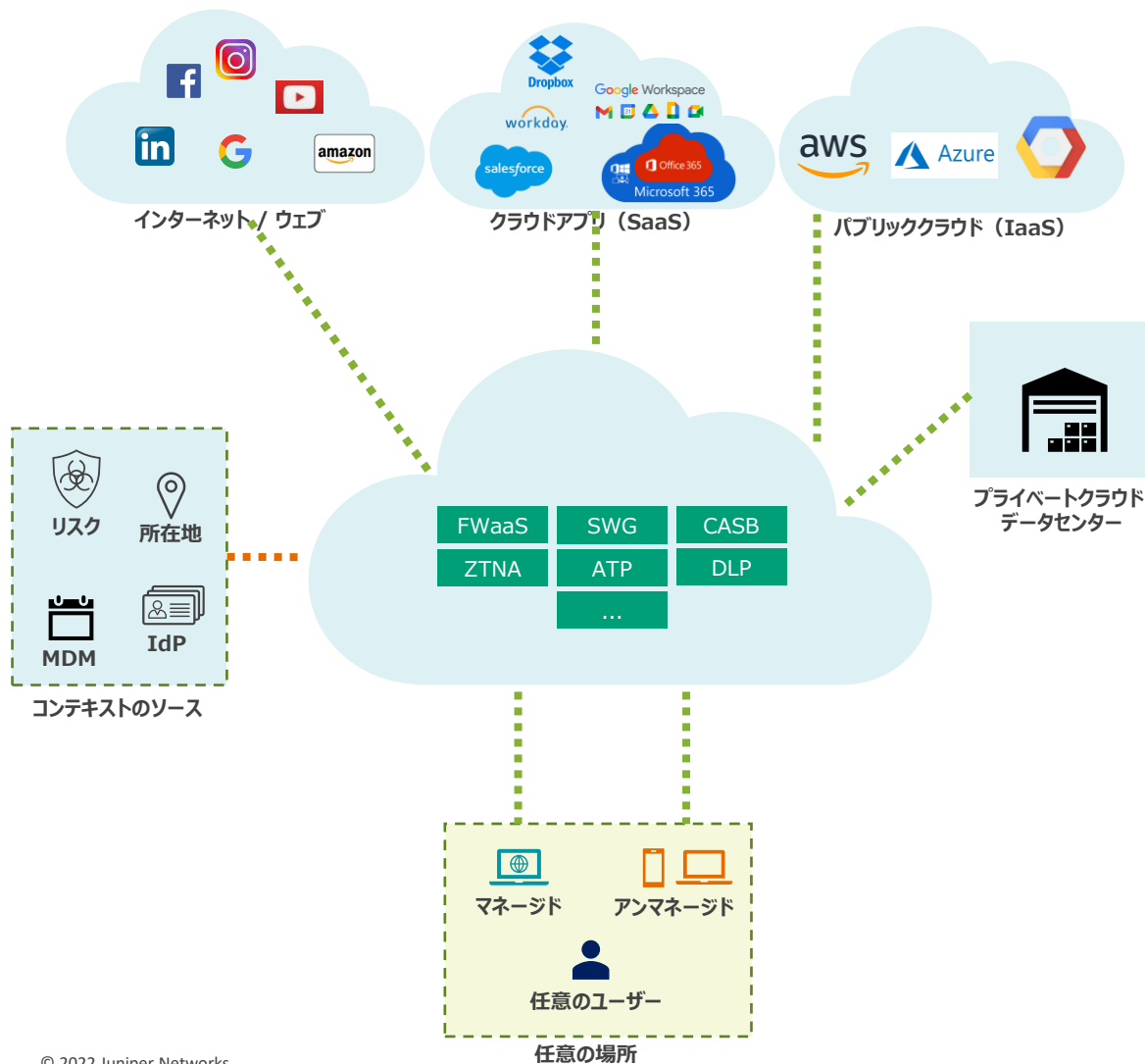
# ブランチセキュリティからセキュア（エンタープライズ）エッジへ

あらゆる場所でユーザーとデバイスをつなぎ、保護する



# SSE の主な使用例

## クラウドで実現するセキュリティ



### 視認性

- 企業資産（ユーザー、デバイス、アプリ、ネットワーク、クラウド）に関わる利用状況の把握
  - 許可された使用、許可されたものとされていないもの（シャドーIT）
  - 機密データ、異常値など

### アクセス制御

- コンテキストを考慮した**アクセス制御**と**アクティビティ制御**をリアルタイムに実行します。
  - 許可、拒否
  - コーチ/警告、隔離、暗号化、など。

### 脅威の防止

- 脅威の発見と防止
- 外部情報（EDR/XDR、SOARなど）に基づくポリシーの適用

### データ保護

- 企業のアプリ/デバイス/データベースとの間でやり取りされる機密データを検出し、保護する
  - 動いているデータ



# お客様とのパートナーシップ

JSE は目的に応じて提供可能です

## セキュア SD-WAN/SASE に興味がある

運用、デプロイメント、ポリシーが容易で  
購入プロセスも簡単です

## ファイアウォール、セキュリティに興味がある

SD-WAN ベンダーを既に選定している、もしくは  
現状、SD-WAN に興味はないが、セキュリティベンダーが  
SASE（または SSE）戦略を持っていることを期待している

## SD-WAN に興味がある

セキュリティベンダーを既に選定している、もしくは統合の  
準備が整っているものの、1年以内にチャンスがあり、  
SD-WAN ベンダーがSASE（または SSE）戦略を  
持っていることを期待している





# JSE 展開の詳細

# Security Director Cloud のユーザーインターフェース

Juniper Security Director Cloud

SE\_test

Dashboard

My Dashboard x SRX x Secure Edge x

Top 5 Users by Bandwidth

Time Span: 30 days

User	Bandwidth (Values)
null\tsuji...hirata--	~180M
unauthenticated-user	~40M
null\shirata--	~15M
null\tsuji-shirata--	~5M
juniper.net\tsuji	~2M

Last updated: Oct 24, 2022, 4:06:42 PM

Top 5 Service Locations by Users

Time Span: 30 days

Service Location	Users (Values)
jsec-california	10

Last updated: Oct 24, 2022, 4:06:42 PM

Top 3 Sites by Bandwidth

Time Span: 30 days

Site	Bandwidth (Values)
ctc_spoke_ipsec_5_11	0
bergt_test_2_ipsec_1_3	0
bergt_test_2_ipsec_1_2	0

Last updated: Oct 24, 2022, 4:06:42 PM

Overview

Bandwidth: 51.1 Kbps Average usage

Users: 5% users (10 of 200 users)

Volume: 15.43 GB

Time Span: 30 days

Last updated: Oct 24, 2022, 4:06:42 PM

Top 3 Service Locations by Bandwidth

Time Span: 30 days

Service Location	Bandwidth (Values)
jsec-california	0.08% (30.2 Kbps of 40.0 Mbps Used)
jsec-virginia	0.05% (20.9 Kbps of 40.0 Mbps Used)

Last updated: Oct 24, 2022, 4:06:42 PM

Top 5 Sites by Users

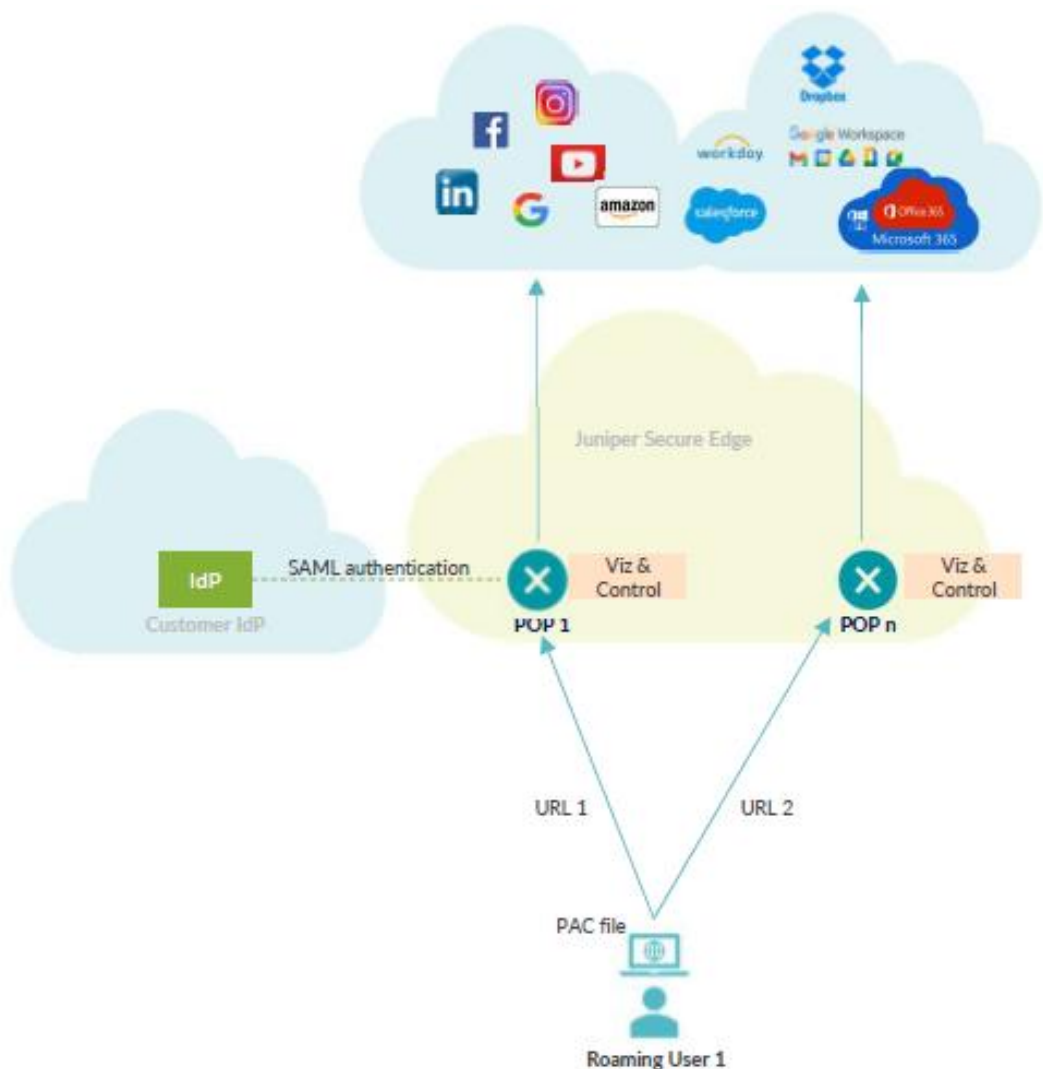
Total Service Locations



# サービス拠点 (POP)

- POPS - 合計 4 つの POP が利用可能で、今後さらに追加される予定です
- 2 つの POP を用意し、最小限のサービスを選択している
- ユーザー
  - ユーザー数で POP あたりのデータプレーンインスタンス数が決まる
  - 現在、1,000 ユーザーあたり 1 インスタンスを展開 - デバイスは考慮されない
  - ( 1 ユーザー 5 デバイス = 1 ユーザー )
- 帯域幅
  - 帯域幅は、UI では次のように表されます
    - "プロビジョニング" - 想定されるユーザー数に基づいています
    - "送信" - 管理者の参照および会計処理のために使用されます
  - トンネル最大負荷 300 Mbps

# ローミングユーザーによる Web/SaaS アクセス



エンドユーザーと エンドポイント	管理対象デバイスのローミングユーザー
トラフィック リダイレクション	HTTP/S で「最寄りの」POP へ
認証	SAML ( IdP 統合) 、LDAP、 ローカルデータベースによるユーザー認証
コンテキストを 考慮した エンフォースメント	<b>Web/SaaS のトラフィック</b> に対して、アイデンティティと アプリケーションを意識した可視化と制御
継続的な許可	ATP クラウドによる高度な脅威防御

# ローミングユーザー - PAC (Proxy Auto Configuration)

## PAC とは？

- ユースケース認証されたユーザーのみで管理される Windows、MacOS、iOS、またはAndroid クライアント
  - 対応ブラウザ Chrome、Firefox、Microsoft Edge (Safari 対応予定)
- ブラウザトラフィック (HTTP/S) にのみ適用され 全てのトラフィックはプロキシされます (Explicit Proxy)
  - エンドポイント証明書が必要
- 推奨 PAC ファイルはあらかじめ定義されています
- 推奨 PAC ファイルはクローン化し 独自のユースケースに 合わせることができる
- DNS
  - AWS で利用されている Route 53 は 「最も近い」 POP の位置の IP アドレスを返します

**Clone PAC recommended.pac**

Name\* recommended.pac\_clone

Description PAC file generated from template: recommended

URL https://jsec-eap.juniperclouds.net/pac-mgr

```
XML Code
if (dnsDomains(host, excludeDomains[i])) {
  if (debug_pac) {
    alert("Returning EXCLUDED_DOMAINS TRUE")
  }
  return true
}
if (debug_pac) {
  alert("Returning EXCLUDED_DOMAINS FALSE")
}
return false
}

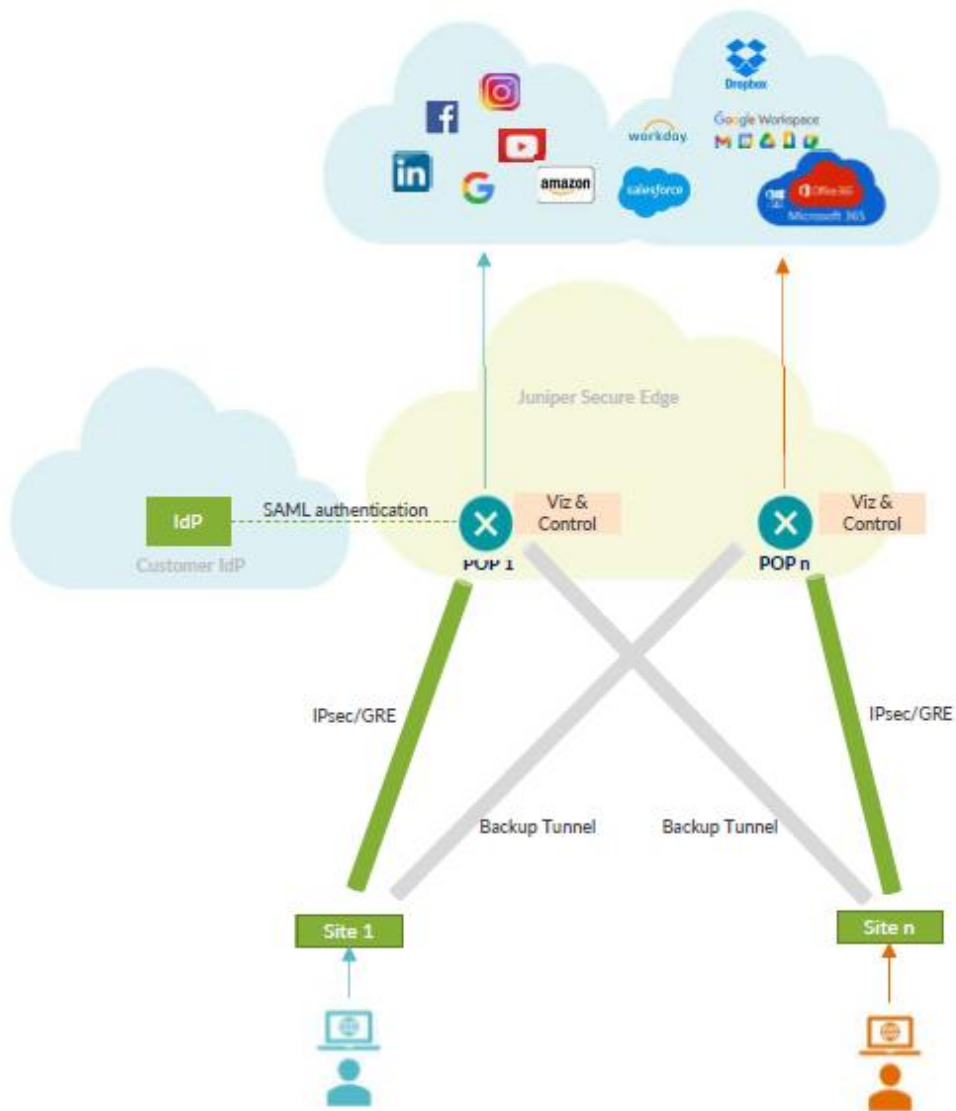
// Check if destination domain requires high bandwidth
// and so should be excluded from proxying.
function IsHighBandwidthHost(host) {
  var hosts = ['youtube.com', 'facebook.com'];

  for (i = 0; i < hosts.length; i++) {
    if (dnsDomains(host, hosts[i])) {
```

Cancel OK



# オンプレミスユーザーによる Web とインターネットへのアクセス



エンドユーザーと エンドポイント	あらゆるオンプレミスユーザー（従業員、契約社員、ゲスト）、 あらゆるデバイス（管理下、非管理下）
トラフィック リダイレクション	検査のために、すべてのトラフィックを Secure Edge にルーティングする可能性がある
認証	JIMS 経由のユーザー認証（クラウド Idp を追加予定）
コンテキストを 考慮した エンフォースメント	アイデンティティとアプリケーションを意識した、 <b>すべてのトラフィックの可視化と制御</b>
継続的な許可	ATP クラウドによる高度な脅威防御

# サイト - オンプレミスブランチユースケース

- ユースケース：すべてのユーザー（認証済み、未認証）、デバイス、ネットワークトラフィック
- ユーザー数を選択することでプロビジョニングされる帯域幅が決定されます
  - その際、トンネル構成も決定されます
- トラフィックフォワーディング
  - CPE で NAT しないこと  
ソース IP はユーザーを特定するために重要です（UserFW のマッピングのため）
  - 認証は、JIMS Collector との連携によるユーザーと IP のマッピングに基づきます（オンプレミスの Active Directory の場合）
  - プライマリとバックアップの 2 つのトンネルを設定（ECMP は必要ありません）
  - 2 種類のトンネリングオプション
    - IPSec 優先
    - GRE は暗号化されていない、ネイティブのヘルスマonitoring機能なし、GRE キープアライブサポートなし

# プロキシ

- TLS 1.3/1.2 対応
- エンドポイント SSL 証明書はローミングで使用する場合に必要であり、オンプレミスブランチでトラフィックを復号化する場合に必要です
- ローミングユーザー
  - Explicit Proxy - すべてのトラフィックがプロキシされます。
  - ユーザーと IP のマッピングはドメイン(ユーザー) Cookie に基づく
- オンプレミスユーザー - Transparent Proxy - ポリシー設定によりプロキシ動作を決定します
  - 標準的な UserFW ベースのポリシーを適用 - ポリシーで復号化が有効で、SOURCE の 設定によって制御されている場合にのみ復号化する
  - ユーザーと IP のマッピングは、IP ベース

# 認証とユーザー識別

- ユーザーの認証と識別のためのオプション
- ローミングユーザー
  - SAML: GA には Okta with MFA と AzureAD が含まれる予定です
  - LDAP
  - ホスティングデータベース
- オンプレミスユーザー
  - Juniper Identification Management Service Collector
  - IdP サービスは将来的に対応予定
- グループ情報に対応
  - 以下より抽出:
    - JIMS の Active Directory
    - SAML アサーションによる認証サービス

The screenshot displays the configuration page for a SAML Profile in the Juniper Service Management console. The breadcrumb trail at the top indicates the path: Secure Edge > Service Management > End User Authentication. Three tabs are visible: SAML Profile (selected), LDAP Profile, and Hosted Database. The SAML Profile section is divided into two main areas: Service Provider (SP) and Identity Provider (IdP).

**Service Provider (SP) configuration:**

- Entity ID\*:
- Username attribute\*:
- Sign authentication request:
- Group attribute\*:
- First name attribute\*:
- Last name attribute:

**Identity Provider (IdP) configuration:**

- IdP settings:  Import settings,  Enter settings manually,  Enter metadata URL
- Import\*:
-



# セキュリティポリシー 対応する NGFW の機能

Secure Edge Policy ⓘ

Last update: A few seconds ago by mbergt@juniper.net | Total Rules 9 | Redeploy required | Deploy

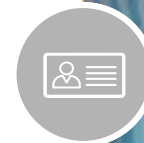
1 selected

Seq	Rule Name	Sources	Destinations	Applications/Services	Action	Advanced Security	Options
1 0 hits	khendrych_1	khendrych_10_0_10 Any	Any	Any Any	Permit	IPS Decrypt Web Filtering Content Filtering Anti-malware SecIntel	
2 0 hits	Ping-Any	Any Any	Any	Any ping	Permit	IPS Decrypt Web Filtering Content Filtering Anti-malware SecIntel	
3 0 hits	Office365 Permit traffic to Office365 by default	Any Any	Office365	Any Any	Permit	IPS Decrypt Web Filtering Content Filtering Anti-malware SecIntel	
4 0 hits	JIMS	Any ad2012.loc\Domain Users	Any Enhanced_Games +1	Any Any	Redirect	IPS Decrypt Web Filtering Content Filtering Anti-malware SecIntel	
5 0 hits	Core-Network-Services Permit Core Network Services	Any Any	Any	DNS +1 defaults	Permit	IPS Decrypt Web Filtering Content Filtering Anti-malware SecIntel	
6 0 hits	Default-Web-Inspection Permit, Decrypt, and Inspect Web Tra...	Any Any	Any	Any http +2	Permit	IPS Decrypt Web Filtering Content Filtering Anti-malware SecIntel	
7 0 hits	Redirect-Unauthenticated-Users Redirect Unauthenticated Users to th...	Any unauthenticated-user	Any	Any http-proxy +2	Permit	IPS Decrypt Web Filtering Content Filtering Anti-malware SecIntel	

- ✓ IDP
- ✓ ウェブフィルタリング
- ✓ コンテンツフィルタリング
- ✓ SecIntel
- ✓ アンチマルウェア

# クラウドアクセスセキュリティブローカー(CASB) データロス防止(DLP)

- ✓ 高度な分類とデータ損失防止 (DLP) でビジネスクリティカルなデータを保護します
- ✓ 暗号化と権限管理で外部と共有するデータを安全に管理
- ✓ ユーザーとエンティティの行動分析 (UEBA) によるインサイダー脅威の検出
- ✓ クラウドインフラとアプリケーションのセキュリティ管理



# アクセスポリシー

管理者が指定可能:

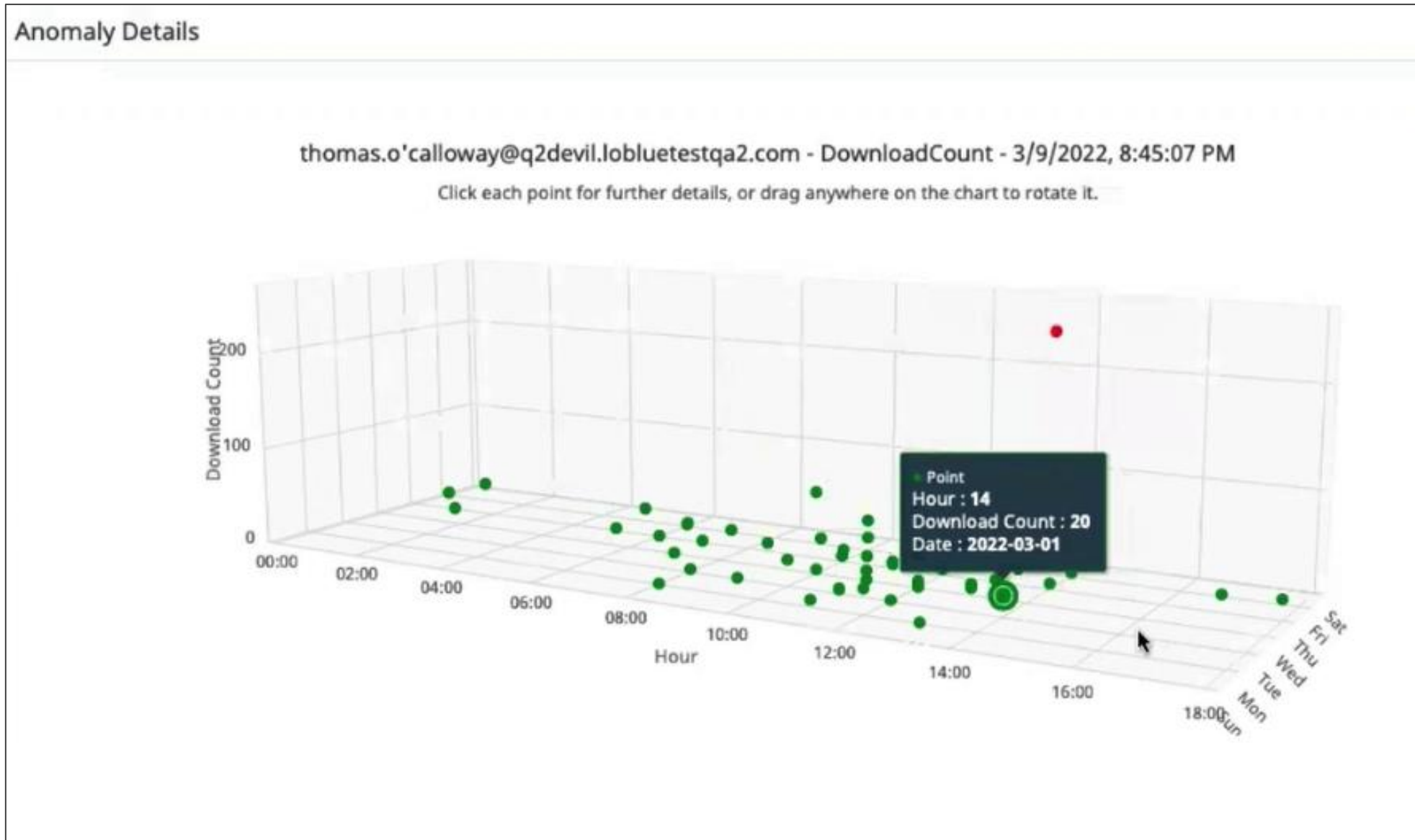
- ✓ データ型 (PCI、PII)
- ✓ アクション (ダウンロード、アップロード、共有)
- ✓ ホワइटリストドメイン
- ✓ ブロックリスト入りドメイン
- ✓ ポリシー(許可、拒否、MFA)

The screenshot displays the Juniper Secure Edge management console for configuring an API Access Policy. The interface is divided into several sections:

- Managed Apps:** A list of applications with checkboxes for selection. Under "FileSharing", "SR\_Office365\_casbqa.onedrive" is selected.
- Content Scanning:** Configuration for scanning content. "Data Type" is set to "1 Item selected". "Rule Template" is set to "Payment Card Industry (PCI) Data". "External DLP" is currently disabled.
- Context Rules:** Configuration for context rules. "Context Type" is "Sharing Type" and "Context" is "External".
- Context Exceptions:** Configuration for exceptions. "Apply to Content Actions" is enabled. "Context Type" is "Whitelist Domains" and "Whitelist Domains" is set to "2 Whitelist Domains".

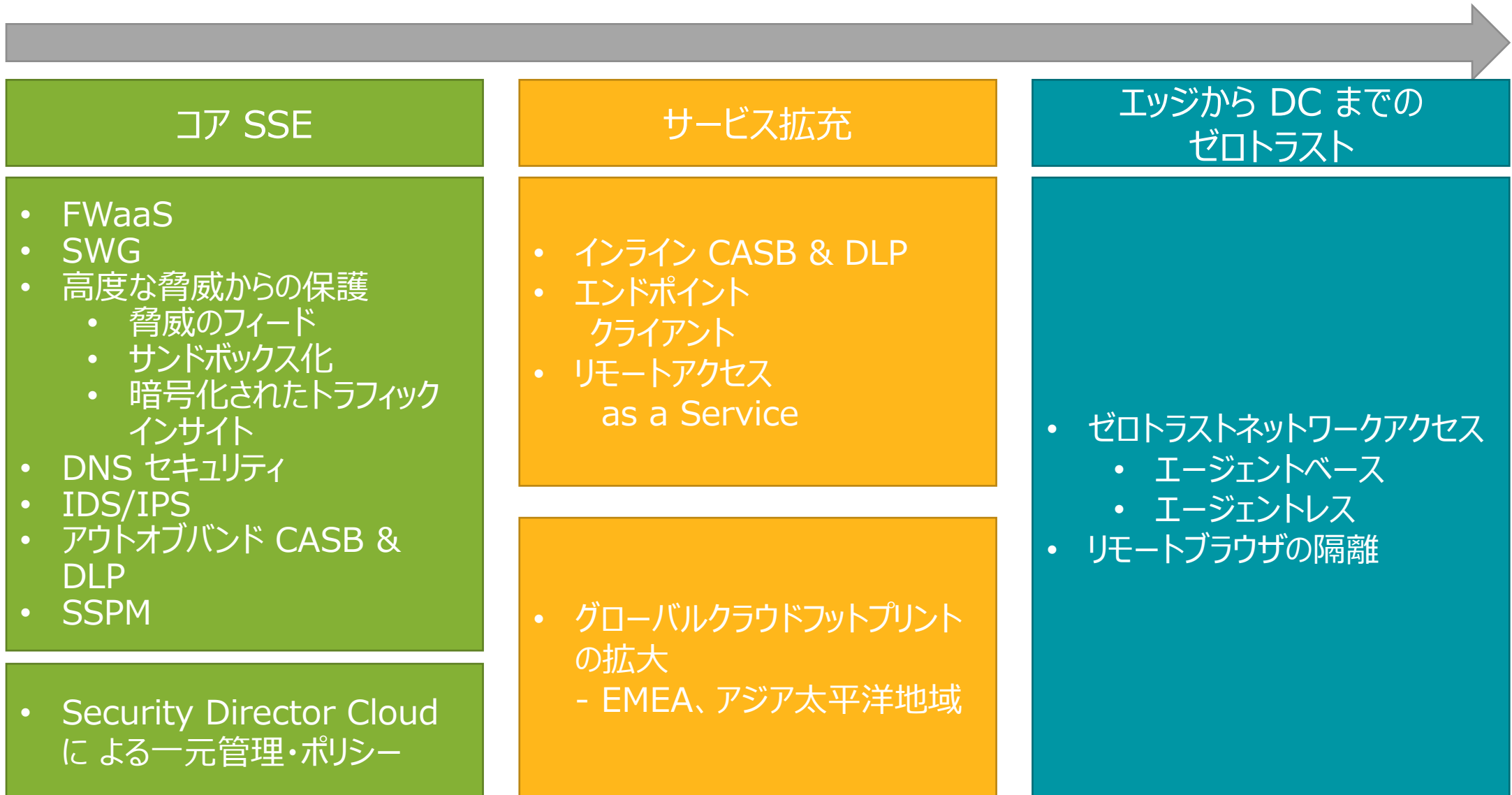
Navigation buttons at the bottom include "Previous", "Save", "Next", and "Ca".

# ユーザー行動データの異常の発見



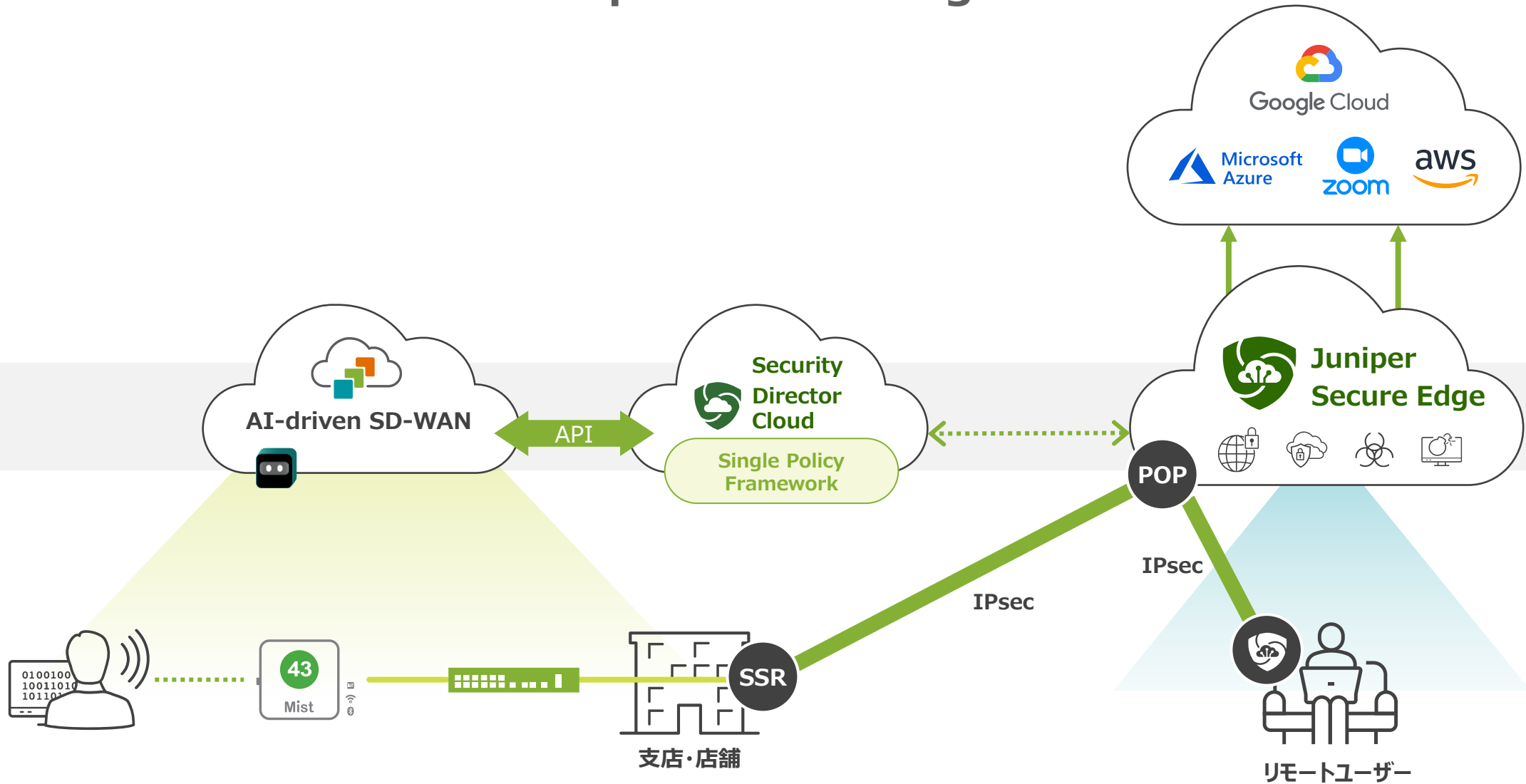


# Secure Edge ロードマップ



# ジュニパーの SASE が活躍

## AI-deiven SD-WAN + Juniper Secure Edge



# Juniper Secure Edge のライセンスング

## 従量制

- ユーザー数に応じた SKU
- SKU tier bundles - 買いやすく、使いやすい
  - 標準: FWaaS + セキュア Web アクセス
  - アドバンスド: 標準機能すべて + IPS&ATP クラウド
- Security Director Cloud のライセンスを含む
- サポート含む
- クラウドサービス拠点 (POP) 2 ヶ所含む
- サブスクリプション期間 1 年、3 年

## アドオンの柔軟性

- サービス拠点 (POP) 追加
- ログストレージの充実

	S-JSEC-S1-Cx-x	S-JSEC-A1-Cx-x
機能	Standard	Advanced
セキュアなウェブアクセス (TLS プロキシおよびインスペクション)	X	X
URLフィルタリング	X	X
コンテンツフィルタリング	X	X
アイデンティティ/ユーザー FW	X	X
アプリケーションコントロール	X	X
脅威のフィード	X	X
アンチマルウェア	X	X
DNS フィルタリング	X	X
DNS セキュリティ		X
IPS		X
マルウェアのサンドボックス化		X
暗号化された トラフィックインサイト		X
帯域外 CASB-DLP	アドオン	アドオン

# パートナー向けセキュリティ関連資料



## Partner Center のセキュリティページ

<https://partners.juniper.net/partnercenter/solutions/security/>

JUNIPER NETWORKS

Sales Programs & Promotions Products & Solutions Services Marketing Japan My Account

### Juniper Connected Security

Partner Center > Products & Solutions >

**Make your network threat aware with Juniper Connected Security.**

The move to multicloud and distributed environments creates operational complexity leading to gaps in your customer's defense against security threats. Your customers require a better approach to security that effectively safeguards their organization while streamlining operations. Juniper's seamless security architecture delivers automated enforcement, increased visibility, and cloud protection to do just that.

**Benefits of Juniper Security Products**

**Visibility:** Gain visibility to the entire network, from endpoint to edge and every cloud in between.

**Intelligence:** Automatically recognize threats, regardless of attack vector.

**Enforcement:** Every point of connection on the network, no matter how small, acts in its defense.

**Prospect** Identify prospect's challenges and how Juniper addresses

**Qualify** Provide proof points to solve the prospect's challenges

**Customize** Guide the prospect's recommendation of Juniper

**Prove** Guide the prospect's decision to purchase Juniper

**Propose** Help justify the purchase and close the deal



# Secure Edge のためのリソース





TechLibrary Day One+ Product Documentation Design Center Learning Center

Home > TechLibrary >

## Juniper Secure Edge

Juniper Secure Edge provides Firewall as a Service (FWaaS) in a single-stack software architecture managed by J

Filter by title

-  **Learn**
  - Release Notes**  
Get details about new and updated features for a release
-  **Set Up**
  - Get Started**  
Initial steps to set up your product
-  **How To**
  - User Guides**  
Discover how to configure, monitor, use, and troubleshoot your product
-  **Resources & Tools**
  - Support Resources**  
Download software and get product support in our knowledge

- [Secure Edge のデータシート](#)
- [Juniper Secure Edge Tech Library](#)
- [Juniper Secure Edge: getting started guide](#)
- [Security Director Cloud ドキュメント](#)
- デモ動画 Juniper Secure Edge のデモ CASB と DLP : <https://www.youtube.com/watch?v=QRpNIJDZZUk>
- 動画で見る Juniper Secure Edge でリモートワーカーを保護する <https://www.youtube.com/watch?v=zYBTL8kKBxw>

# Juniper Secure Edge

## お客様の成果



- ✓ いつでも、どこでも、ユーザーを保護
- ✓ 既存投資の活用
- ✓ ネットワーク全体のセキュリティを容易に確保
- ✓ クライアントからワークロードまでゼロトラストポリシーを実施
- ✓ 自分のペースでシームレスかつ安全にクラウド提供型アーキテクチャに移行することが可能



# THANK YOU

JUNIPER NETWORKS | Driven by Experience™