



# APAC Cohesion Connected Security (CSEC)

Tech Roundup Q3-2023

ジュニパーネットワークス株式会社

# 免責事項

この製品の方向性に関する声明は、ジュニパーネットワークスの現在の意図を示すものであり、予告なしにいつでも変更されることがあります。ジュニパーネットワークスが本ステートメントに記載された特徴や機能を提供することを条件として、購入することはできません。

# Agenda

- 第三者機関による検証と認定
- パブリッククラウド向け Connected Security ソリューション
- ジュニパー Secure Edge のご購入
- Security Director Cloud Insights



# 第三者機関による検証と認定

# 過去 4年間すべてのテストで 1位

独自に検証されたセキュリティの有効性



NetSecOPEN  
2022

99.8%

エクスプロイトに対する有効性

Cyber Ratings AAA レーティング

2023 次世代ファイアウォール



99.9%

対クライアントおよびサーバーサイド エクスプロイト



ICSA Labs  
Advanced Threat Defense

Q3 2022

Q2 2022

Q1 2022

Q4 2021

Q3 2021

Q2 2021

Q1 2021

Q4 2020

100%

マルウェア阻止率

<0.5%

誤検知率

業界の  
各大手ベンダーを凌駕

- Fortinet
- Palo Alto Networks
- Zscaler
- Checkpoint
- Cisco

Cyber Ratings AAA レーティング

2022 クラウドネットワークファイアウォール



100% 0

エクスプロイト  
ブロック率









誤検知数



パブリッククラウド向け  
**CONNECTED SECURITY**  
ソリューション

# Amazon AWS クラウドネイティブ サービスとの統合



-  エラスティック負荷分散とオートスケーリンググループ： スケーリングとエラスティック性を可能にします
-  CloudWatch と Security Hub： ネイティブアラートの統合
-  Amazon GuardDuty と SecIntel： データセンター全体へ調査結果を拡張
-  鍵マネージメントサービス： セキュア秘密鍵の統合と、動的および静的データの暗号化
-  エラスティックネットワークアダプターのサポート
-  複数の AWS インスタスタイプ - 柔軟なデプロイメントが可能
-  AWS インスタンスにおいて使用可能な全 vCPU の利用への SWRSS のサポート
-  GWLB： 優れたスケーラビリティと回復力のための L3 ゲートウェイ + L4 負荷分散機能

# Microsoft Azure クラウドネイティブサービスとの統合



Azure Load Balancer : セキュリティサービスの高可用性



VM スケールセット : オートスケーリングと vSRX の管理



Azure Sentinel 用 ジュニパー SRX コネクター : ログの統合



vSRX と Azure Key Vault サービスとの統合 : 接続の安全性



複数の Azure コンピュートインスタンス タイプのサポート



Azure インスタンスにおいて使用可能な全 vCPU の利用への SWRSS のサポート



# Google GCP クラウドネイティブサービスとの統合



パワーモード IPsec : クラウド VPN



クラウド KMS (HSM) を使用したデータ保護



複数の GCP コンピュータマシンのサポート



GCP インスタンスで使用可能な全 vCPU の利用に対して SWRSS をサポート

# AWS ゲートウェイ ロードバランサー (GWLB) の概要

## What ?

GWLB は、L3 ゲートウェイ + L4 負荷分散の機能を備えた、新しいタイプのロードバランサー  
サードパーティアプライアンスのデプロイと運用のためのもの

## Why ?

水平オートスケーリング  
耐障害性 (アクティブ/アクティブ)  
透過的なネットワーク導入  
管理者アクセスの分離  
AaaS : サービスとしてのアプライアンス

## How ?

ソリューションコンポーネント :  
「GWLB + ゲートウェイ負荷分散エンドポイント (GWLBE) + vSRX」  
より高いスケーラビリティと耐障害性を実現

## ベンダー要件

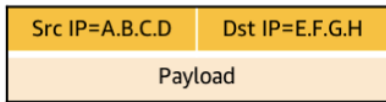
- 1 : GWLB への統合は、アプライアンス (vSRX) で GENEVE プロトコルのサポート
- 2 : GENEVE オプション (TLV) のエンコード/デコードと、GWLB ヘルスチェックへの応答

## ユースケース

インターネットゲートウェイによる  
ノース/サウス インспекション  
トランジットゲートウェイによる  
セキュリティインспекション  
トランジットゲートウェイによる  
VPC 間のインспекション

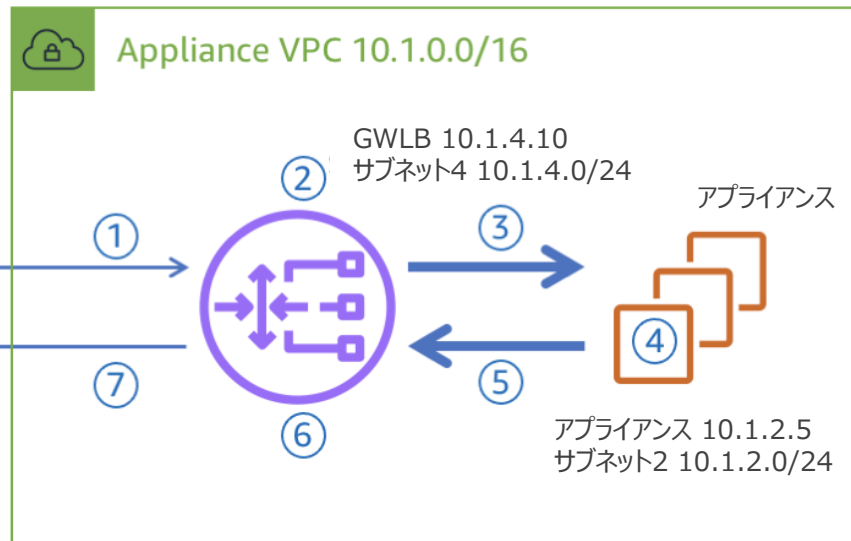
# パケットフロー：断片の解明

ステップ1：送信元からのパケット



ステップ2：

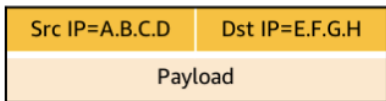
- GWLB は 5-tuple 情報によってアプライアンスを選択
- Geneve でパケットをカプセル化し、TLV を追加
- アプライアンスへ転送



ステップ6：

- GWLB はパケットを非カプセル化
- tuple 情報および、フローCookieを検証
- GWLBE を介した宛先に転送

ステップ7：宛先にて受信のパケット



ステップ3：GWLB から送信のパケット

Outer Src IP = 10.1.4.10		Outer Dst IP = 10.1.2.5	
GWLBE ENI ID	Attachment ID	Flow Cookie	
Src IP=A.B.C.D		Dst IP=E.F.G.H	
Payload			

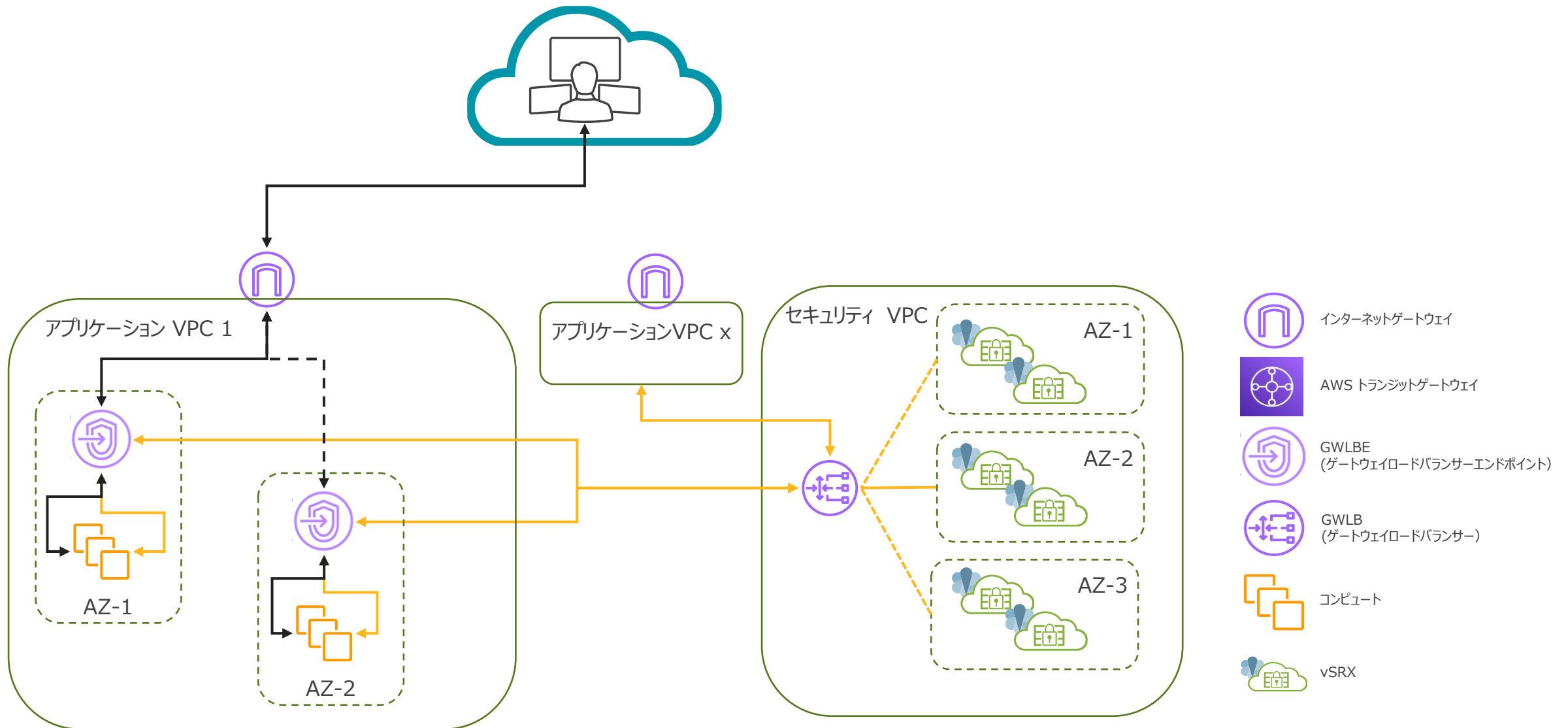
ステップ4：

- アプライアンスはパケットを非カプセル化
- TLV を読み取り、フローCookieを保存
- アプリケーションは自身の処理を実行
- パケットをカプセル化し、同じ TLV を添付
- ※内部パケットの 5-tuple 情報とフローCookieは元のパケットと一致する必要がある
- GWLB を介してパケットを送信

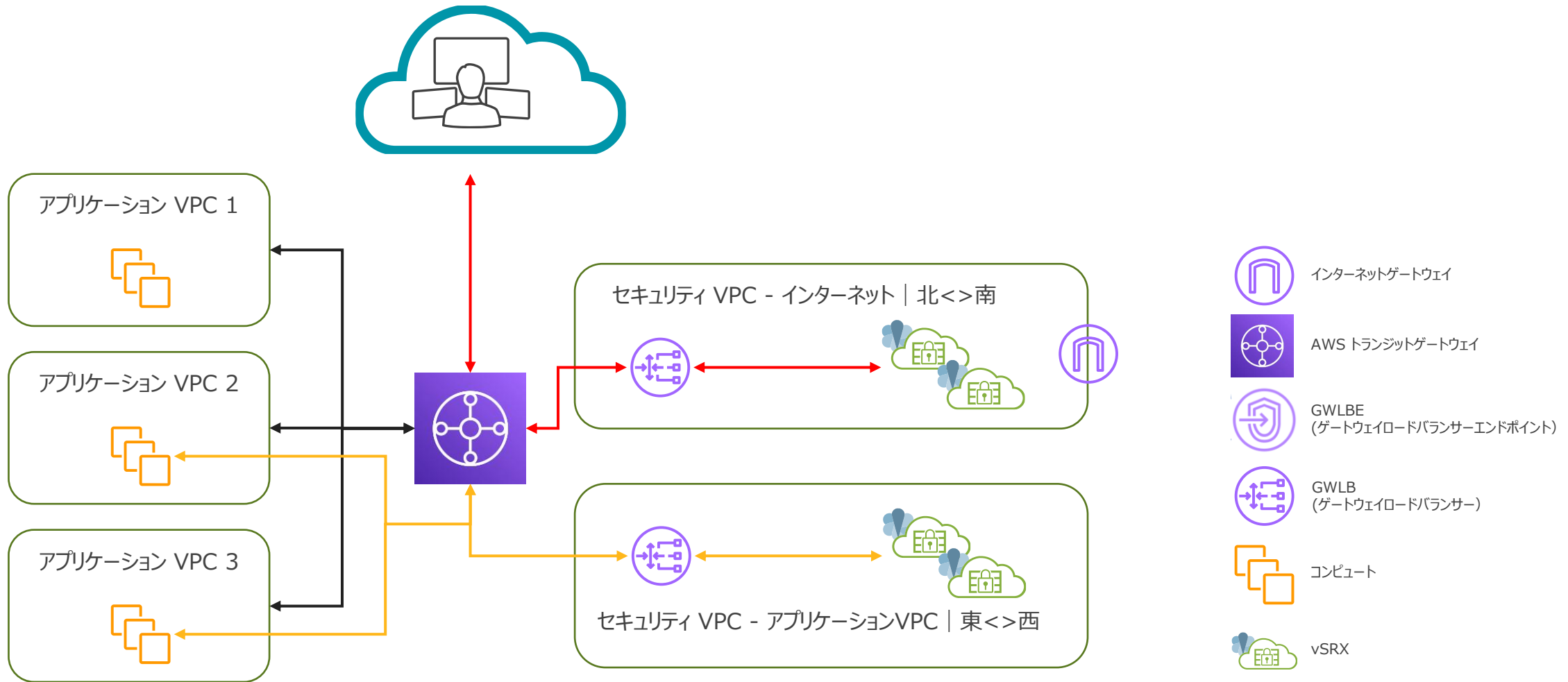
ステップ5：アプライアンスから送信のパケット

Outer Src IP = 10.1.2.5		Outer Dst IP = 10.1.4.10	
GWLBE ENI ID	Attachment ID	Flow Cookie	
Src IP=A.B.C.D		Dst IP=E.F.G.H	
Payload			

# ユースケース：インバウンドのインスペクション



# ユースケース：アウトバウンドと East/West インспекション





ジュニパー

SECURE EDGE のご購入

# ジュニパー Secure Edge ライセンス

## 従量課金制

- **ユーザー数に基づく SKU**
  - 最低 200 ユーザー (クラス 1 : 200~2499 ユーザー)
  - 最大ユーザー数制限なし (クラス 4 : 50,000 人以上)
- **SKU 段階バンドル – お求めやすく、使いやすい**
  - スタンダード : FWaaS + セキュアウェブゲートウェイ + 脅威対策
  - アドバンスド : すべての標準機能 + IPS & ATP クラウド
- **Security Director Cloud ライセンス**
- **サポート**
- **2つのクラウドサービス拠点 (POP)**
- **契約期間 : 1年 または 3年**

## 柔軟なアドオン

- **サービス拠点 (POP) 追加**
- **ログストレージ拡張**

	S-JSEC-Sx-Cx-x	S-JSEC-Ax-Cx-x
機能	スタンダード	アドバンスド
セキュアウェブゲートウェイ (TLS プロキシとインスペクション)	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
アプリケーションの可視化と制御	X	X
脅威フィード	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
クラウドマルウェアサンドボックス		X
暗号化されたトラフィックインサイト		X
CASB-DLP	アドオン	アドオン

# ジュニパー Secure Edge ライセンスに関する注意事項



## 基本ライセンス

- ・ 特定のユーザー数と期間について、基本ライセンス（Standard または Advanced）をご契約
- ・ 各ユーザーは複数のデバイスを所有することが可能。ユーザーは、ログインユーザーや IP 数のみで定義されない
- ・ 基本ライセンスに、企業全体の月間クラウドデータ転送使用量の割り当てが含まれる
  - ・ **月間割当量 = ユーザー数 x 1ユーザーあたり 年間 250GB / 12ヶ月**



## 公正利用条件と データ超過

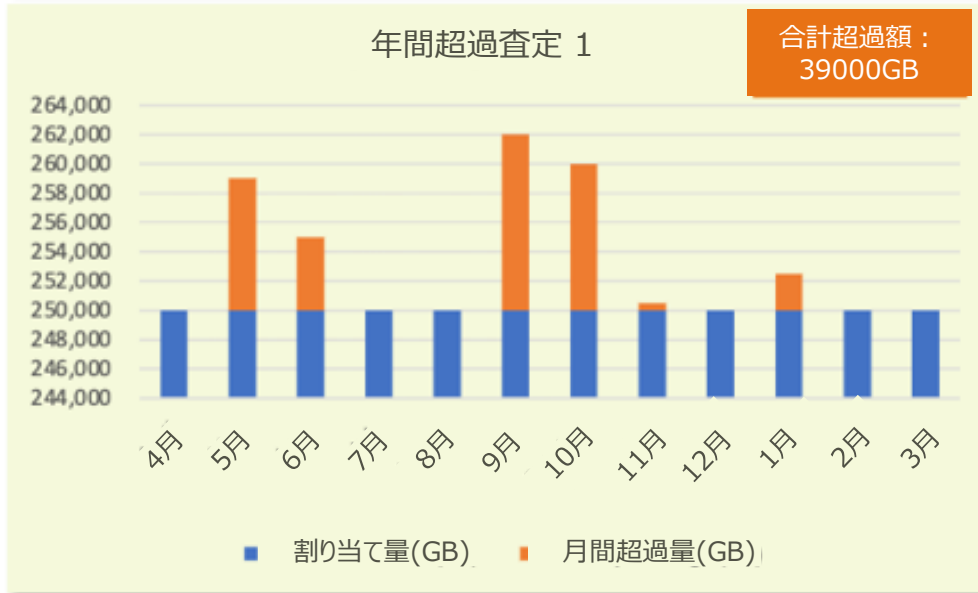
- ・ 顧客は以下の条件においてクラウドデータの月間使用量情報を受け取る：
  - 割当額を下回る場合、使用不足の差額を繰り越すことはできません
  - 割当額を超過した場合、超過額は次回の補正計算に含まれる
- ・ 補正の見直しは 12ヶ月ごとに行われ、その間サービスが中断されることはありません
- ・ ジュニパーでは、超過分を最大 9999GB まで減額調整することができます
- ・ 調整された量が 10000GB 以上の場合、顧客は、契約書のデータ超過 SKU で指定のレートで、調整量の支払いを行うものとする
- ・ 超過料金が適用される場合、ジュニパーは見積書を発行し、顧客は発注書を発行し、ジュニパーは確認書を発行する

期間	説明	価値
利用評価期間	・ 超過使用量を測定する期間の長さ	毎月
請求頻度	・ ジュニパーが超過分/超過料金を請求する頻度	年間
請求期間	・ 毎月の超過額を集計する期間 ・ 超過料金はたとえ単月で発生した場合も支払われるものとする	12カ月
グレースバッファ量	・ 全体の超過額を減額調整するデータ量	最大 9999GB
顧客支払超過額	・ グレースバッファ量を適用した後、支払いの対象となるデータ量	<b>1万GB 未滿切り捨て</b>
超過料金	・ 超過料金のレート	超過 SKU 基準 (S-JSEC-D1-CO-C)



# データ超過の例

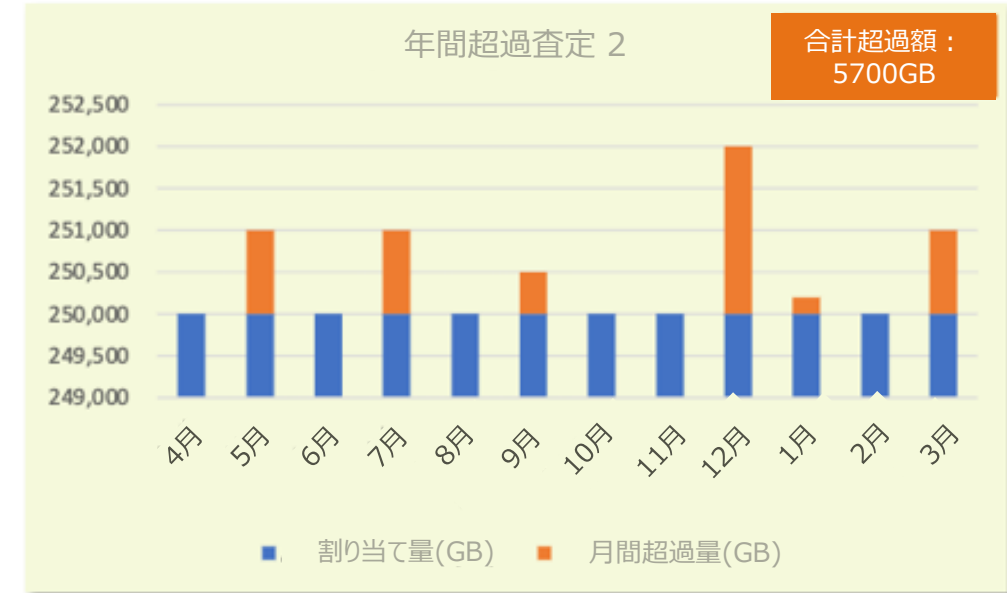
## シナリオ 1



### シナリオ 1

- ユーザー数 = 12,000
- 月間割り当て: 250,000 GB (12,000\*250/12)
- 年間超過量合計 = 39,000 GB
- グレース・バッファ = 最大 9999 GB
- 支払対象量 = 30,000 GB (39,000 GB から切り捨て)
- 超過料金 SKU を使用して 30,000 GB 分の支払いが発生
- 超過分はゼロにリセットされ、次の期間の査定が開始される

## シナリオ 2



### シナリオ 2

- ユーザー数 = 12,000
- 月間割り当て: 250,000 GB (12,000\*250/12)
- 年間超過量合計 = 5700 GB
- グレース・バッファ = 最大 9999 GB
- 支払対象量 = 0 GB (5700 GB から切り捨て)
- 超過支払は発生しない
- 超過分はゼロにリセットされ、次の期間の査定が開始される

# 初期見積もり例

## 初期見積もり

SKU	説明	数量	単価	内線単価	合計
S-JSEC-A1-C3-3	Juniper Networks : Juniper Secure Edge、A1 サービス標準 + DNS セキュリティ、クラウドサンドボックス付きゼロデイ脅威防御、暗号化トラフィックインサイト、IDS/IPS、クラス 3 (10000~49999 ユーザー) のユーザー毎ライセンス、SVC カスタマーサポート、3年間	12000	358ドル	179ドル	2,148,000ドル
<b>合計</b>					2,148,000ドル

・説明のために割引率を50%と仮定しています

# 見積もり例：補正見積

## シナリオ 1：超過使用量 30000GB の場合

SKU	説明	数量	単価	内線単価	合計
S-JSEC-D1-C0-C	Juniper Secure Edge、D1 サービス [グローバル地域におけるアウトバウンドデータ転送の月間超過料金]、クラス0 の 100GB ライセンスあたり、消費量ベース、月次評価額	300	40ドル	20ドル	6,000ドル
合計					6,000ドル

・説明のために割引率を50%と仮定しています

## シナリオ 2：顧客が支払うものがない場合

意図的に空白にしています

# Secure Edge ライセンスに関する注意事項



## 追加ライセンス

以下の追加ライセンスの追加が可能：

- 既存 POP のユーザー追加、または新規 POP のユーザー追加
- ログストレージの拡張
- アウトオブバンド CASB、DLP、SSPM サービス

アドオンライセンスとベースライセンスの同時更新は、更新チームによって次の最も早い更新時に処理されます



## ライセンスの アップグレードと ダウングレード

アップグレードとダウングレードの両方で、新しいライセンスを反映するように設定を更新する必要がある  
必ずジュニパーにご相談ください（特にダウングレードの場合、サービスへの影響が大きくなる可能性があります）

**いつでも** 基本ライセンスをアップグレードすること可能：

- ユーザー数を増やす：（例）1000ユーザーから 2000ユーザーへ、5000ユーザーから 10000ユーザーへ
- 上位の基本ライセンスへのアップグレード：（例）スタンダードからアドバンスドへ

**更新時に** ベースライセンスをダウングレードすることが可能：

- ユーザー数を減らす：（例）2000ユーザーから 1000ユーザーへ
- 下位ライセンスへのダウングレード：（例）アドバンスドからスタンダードへ

アドオンライセンスとベースライセンスの同時更新は、更新チームによって次の最も早い更新時に処理されます

# トライアルライセンス

## トライアルライセンスの利用目的は？

- ・ 開始日と終了日の調整
- ・ 見込み客の認定

## なぜ 30日間だけなのか？

- ・ POC を動かし続けるために
- ・ クラウドのコストを抑えるために
- ・ 試用期間の延長も可能

## トライアルライセンスの注文方法は？

- ・ 0ドルのオーダーを発行  
または
- ・ SSRN について PLM へのお問い合わせ

## どのライセンスを試用するか？

- ・ すべての機能や性能がテスト可能な  
アドバンスドエディションが推奨

SKU	簡単な説明	ユーザー単価
共通機能	<ul style="list-style-type: none"><li>・ Security Director Cloud 管理コンソール</li><li>・ クラウドサービス 2拠点</li><li>・ 1ユーザーあたり 20GB のデータ転送</li><li>・ 1アカウントにつき 1TB のクラウドストレージ</li><li>・ 最大 100ユーザー</li><li>・ 30日間</li></ul>	該当なし
・ S-JSEC-S1-C0-0	・ スタンダードエディション機能	0ドル
・ S-JSEC-A1-C0-0	・ アドバンスドエディション機能	0ドル



# SECURITY DIRECTOR CLOUD INSIGHTS

# Security Director Cloud Insights

The screenshot displays the Juniper Security Director Cloud Insights interface. On the left is a navigation sidebar with options like Favorites, Dashboard, Monitor, Alerts, Logs, IPS Packet Capture, Insights, Incidents (highlighted), Mitigation, Maps & Charts, Tunnel Status, Service Locations, Advanced Threat Prevention, Reports, SRX, Secure Edge, Shared Services, and Administration. The main content area shows a list of incidents with columns for Date & Time, Incident ID, Risk, Threat Target, Progression, and Status. Below the list is a timeline view showing events across days from Sun 9 to Thu 13, with specific event markers like 'NEW AAMW MALWARE EVENT LOG Trojan-Generic' and 'NEW Ops.fw.detect'.

Date & Time	Incident ID	Risk	Threat Target	Progression	Status
Apr 13, 2023, 12:58:32 AM	c5434c0a-7463-4993-abfa-beb3e3d63017	Max	180.80.89.75	DL+IN	New
Apr 11, 2023, 12:06:37 PM	80b95a66-9cbf-4bdd-8771-b87d26aa8af7	Med	172.24.89.75	DL	New
Apr 11, 2023, 12:06:36 PM	0281b373-a78d-4b68-90d3-b75793ceed...	High	10.49.72.80	DL	New
Apr 11, 2023, 12:06:34 PM	9b2a1352-8064-4749-ab69-3db46a203...	Med	172.36.89.75	DL	New
Apr 11, 2023, 12:06:33 PM	06445cca-245b-4888-a94e-246c8a8e53a2	Med	172.35.89.75	DL	New
Apr 11, 2023, 12:06:32 PM	008ea7c5-bd7a-dc14-aa1e-fbd77b8e7d...	Med	172.36.89.75	DL	New

ネットワークと  
セキュリティモニタリング  
の力を融合

...高度な脅威インサイト 付き

...管理効率の最大化を可能とする  
**緩和対策** を実行するために

# リソース と 参考リンク

## リソース/参考リンク

2023 CyberRating エンタープライズ ネットワークファイアウォール レポート

※<https://www.juniper.net/us/en/forms/2023-cyberratings-enterprise-network-firewall-report.html>

プライベート/パブリッククラウド プラットフォーム向け vSRX 導入ガイド

※<https://www.juniper.net/documentation/us/en/software/vsrx/vsrx-consolidated-deployment-guide/index.html>

ジュニパー Secure Edge データシート

※<https://www.juniper.net/us/en/products/security/secure-edge-datasheet.html>

Security Director Cloud Insights ドキュメンテーション

※<https://www.juniper.net/documentation/us/en/software/sd-cloud/sd-cloud/Other/sd-insights-overview.html>

Amazon GuardDuty と vSRX の統合 (※動画)

※<https://www.youtube.com/watch?v=l1DfENhMhxc>





# THANK YOU

---

JUNIPER  
NETWORKS®

Driven by  
Experience™