セキュリティをもっと簡単に！ Juniper Connected Security によるセキュリティの自動化

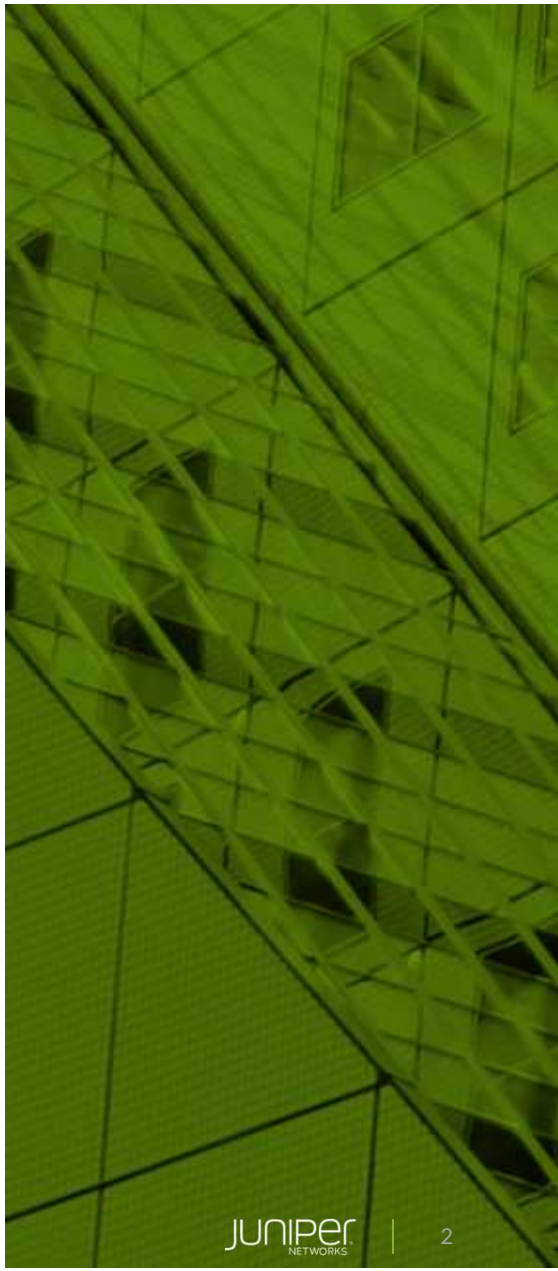
Juniper Networks

2019/10

JUNIPER NETWORKS | Engineering Simplicity

目次

1. 現在のセキュリティ対策における課題
2. Juniperセキュリティビジネスへの取組みと市場での評価
3. Juniper Connected Securityとは？



1. 現在のセキュリティ対策における課題

JUNIPER NETWORKS | Engineering Simplicity

よくお伺いするお客様からの声

①（お金の問題）セキュリティってどこまで投資すればいいの？

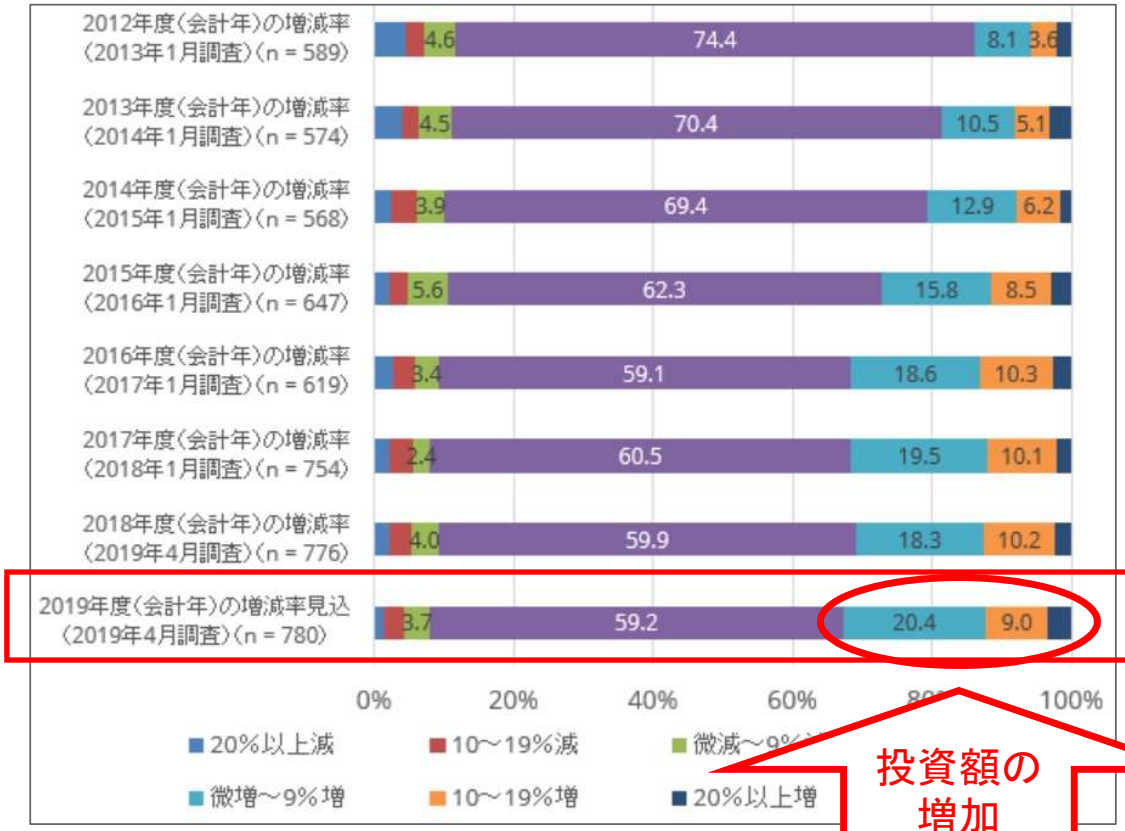
②（運用の問題）色々なソリューションがあるけど、運用どうすればいいの？

③（環境の問題）パブリック クラウドでのセキュリティってどうすればいいの？

①（お金の問題）セキュリティってどこまで投資すればいいの？

国内企業の情報セキュリティ対策の投資状況

2012年度（会計年）～2019年度（会計年）の情報セキュリティ関連投資の前年度と比較した増減率 by IDC Japan



セキュリティ導入の際の課題は、
- 「予算の確保」
- 「導入効果の測定が困難」
- 「投資効果を経営層から求められる」

重大なセキュリティ被害に遭った企業は25.2%

復旧や賠償金などにかかった費用
- 500万円未満と回答した企業が37.3%(昨年比1.8ポイント増)
- 500～1000万以上が15.8%(5.7ポイント増)

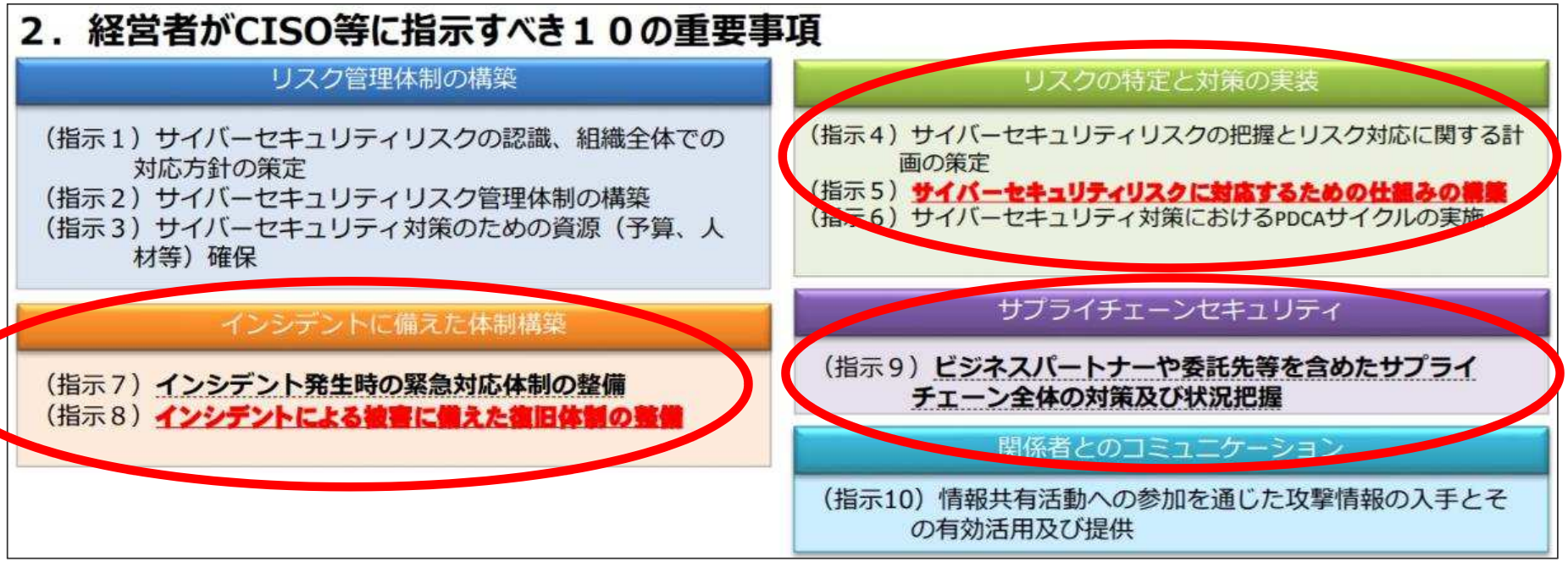
1件当たりの被害額は増加傾向

参照資料より抜粋：
https://www.idc.com/getdoc.jsp?containerId=prJPJ45163119
https://news.mynavi.jp/article/20190613-842488/

サイバーセキュリティ経営ガイドライン v2.0 (経済産業省 2017年11月)

- 昨今のサイバー攻撃の巧妙化により事前対策だけでは対処が困難。
- 米国のサイバーセキュリティフレームワークでも事前対策だけでなく、事後（**検知、対応、復旧**）対策を要求。
- 一方で従来のガイドラインはCSIRTの構築などの「対応」に関する項目はあるものの、「検知」や「復旧」に関する内容が弱く、**国際的な状況を踏まえるとガイドラインとの整合性が不十分**。

経済産業省 ホームページ “サイバーセキュリティ経営ガイドラインの改訂ポイント“ より抜粋
http://www.meti.go.jp/policy/netsecurity/downloadfiles/overview.pdf



中小企業の情報セキュリティ対策ガイドライン (IPA 2019年3月)

はじめに

1 経営者の皆様へ

本ガイドラインは、中小企業の皆様に情報を安全に管理することの重要性についてご認識いただき、中小企業にとって重要な情報[1]を漏えい、改ざん、消失などの脅威から保護するための情報セキュリティ対策の考え方や、段階的に実現するための方策を紹介することを目的としたものです。

情報セキュリティ対策は、経営に大きな影響を与えます！

情報セキュリティ対策を実施して対外的にアピールすることで、企業としての信頼性を確保し売上を伸ばしている企業がある一方、情報セキュリティ対策を疎かにしたために秘密情報や個人情報の漏えいを発生させ、業績は落ち込み、経営を揺るがしかねない高額な賠償金を支払った企業もあります。
(➡ 詳細はP6)

対策の不備により経営者が法的・道義的責任を問われます！

現代社会では金銭や物品だけでなく、情報にも価値や権利が認められます。例えば個人情報保護法では、事業者に対して個人の権利利益の保護、安全管理措置などの管理監督が義務付けられており、これらへの違反が認められると場合によっては会社に罰金刑が課されます。さらに、取締役や監査役は、別途、会社法上の忠実義務違反の責任を問われることもあります。
(➡ 詳細はP8)

組織として対策するために、担当者への指示が必要です！

企業の継続的な発展のために、また、経営責任を果たすためには、担当者に任せきりにすることなく、経営者が自社の情報セキュリティについて明確な方針を示すとともに自ら実行していくことが必要です。情報セキュリティ対策は、経営者が主導し、必要な範囲を網羅し、関係者と連携して組織的に実施しなければ機能しません。経営者はこれらを認識したうえで、情報セキュリティ対策の取り組みを担当者に指示する必要があります。(➡ 詳細はP10)

取組 1	情報セキュリティに関する組織全体の対応方針を定める
取組 2	情報セキュリティ対策のための予算や人材などを確保する
取組 3	必要と考えられる対策を検討させて実行を指示する
取組 4	情報セキュリティ対策に関する適宜の見直しを指示する
取組 5	緊急時の対応や復旧のための体制を整備する
取組 6	委託や外部サービス利用の際にはセキュリティに関する責任を明確にする
取組 7	情報セキュリティに関する最新動向を収集する

中小企業の情報セキュリティ対策ガイドラインより抜粋：https://www.ipa.go.jp/files/000055520.pdf

まとめ

① セキュリティの投資はセキュリティ担当部署だけで無く、経営者が率先して判断する。

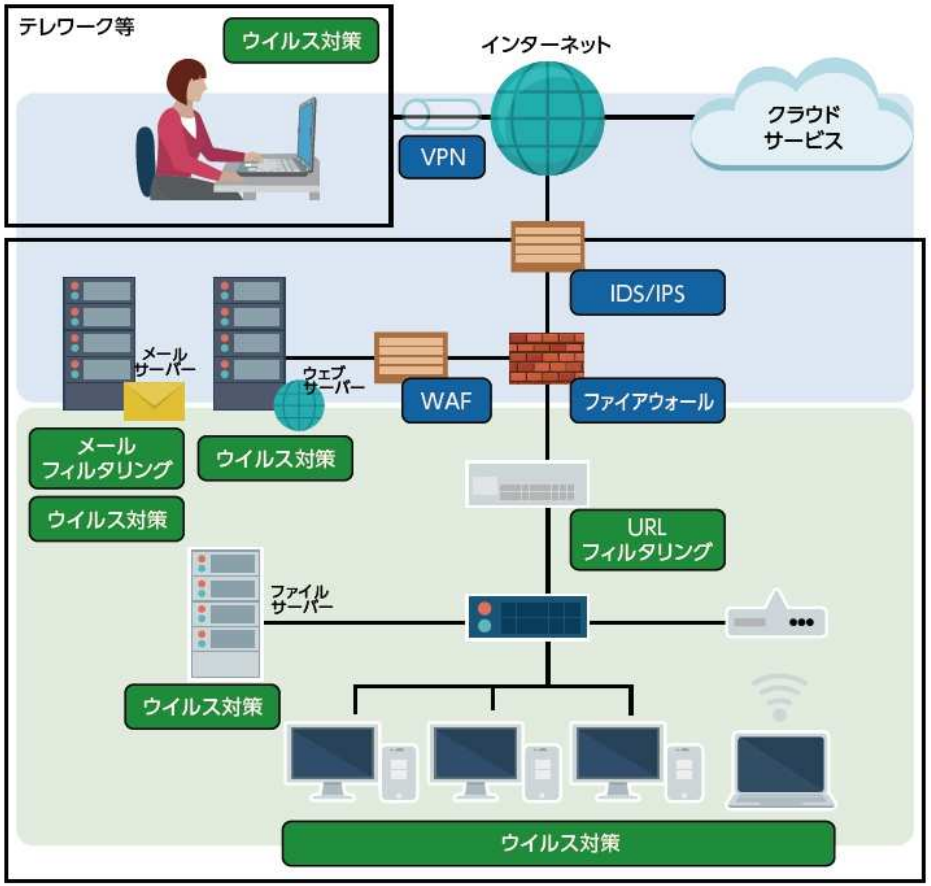
② セキュリティ脅威を受けることを前提とした対策と復旧体制を整える。

③ 自社だけでなく、ビジネスパートナーにもセキュリティを要求する。

②（運用の問題）色々なソリューションがあるけど、運用どうすればいいの？

セキュリティ運営における課題

一般的なセキュリティ対策のネットワーク図



よくお伺いするお客様の声

① セキュリティを高めるために複数の異なるベンダーを採用しているが、検知ロジックとシスログのフォーマットが異なり管理が大変。（ログ管理の工数がかかる）

② セキュリティ脅威が最終的に未然に防げたのか確認する作業に時間が掛かる。(全体の可視化に時間がかかる）

③ セキュリティ脅威の侵入を確認したが、対応に時間がかかり、その間に他の端末に脅威/感染が広がってしまった。（インシデント対応に時間がかかる）

中小企業の情報セキュリティ対策ガイドラインより抜粋：https://www.ipa.go.jp/files/000055520.pdf

SIEM の優位性と困難な部分

SIEMとは？

優位性：

複数機器からログを受信し、内容を横断的に分析し、相関分析を実施してくれる。
“ログ管理“ や“全体の可視化”に強いソリューション。

困難な部分：

- 価格が高い。（ログの数によるサブスクリプションライセンス）
- 運用するための技術者が必要 (相関分析のための設定や操作が必要）
- 分析だけなので、“インシデント対応”は自分で実施する必要がある。

EDR の優位性と困難な部分

EDRとは？

優位性：

エンドポイントにおける脅威を検知し、インシデントに対処するためのセキュリティ製品
“エンドポイント側の可視化”、“エンドポイント側のインシデント対応” に強いソリューション

困難な部分：

- 価格が高い。（端末数に応じた価格。全端末に入れるのが難しい可能性がある）
- 運用するための技術者が必要 (端末内部の動きを理解する必要がある）
- エンドポイント製品なので、ネットワーク全体の可視化やインシデント対応はできない。

まとめ

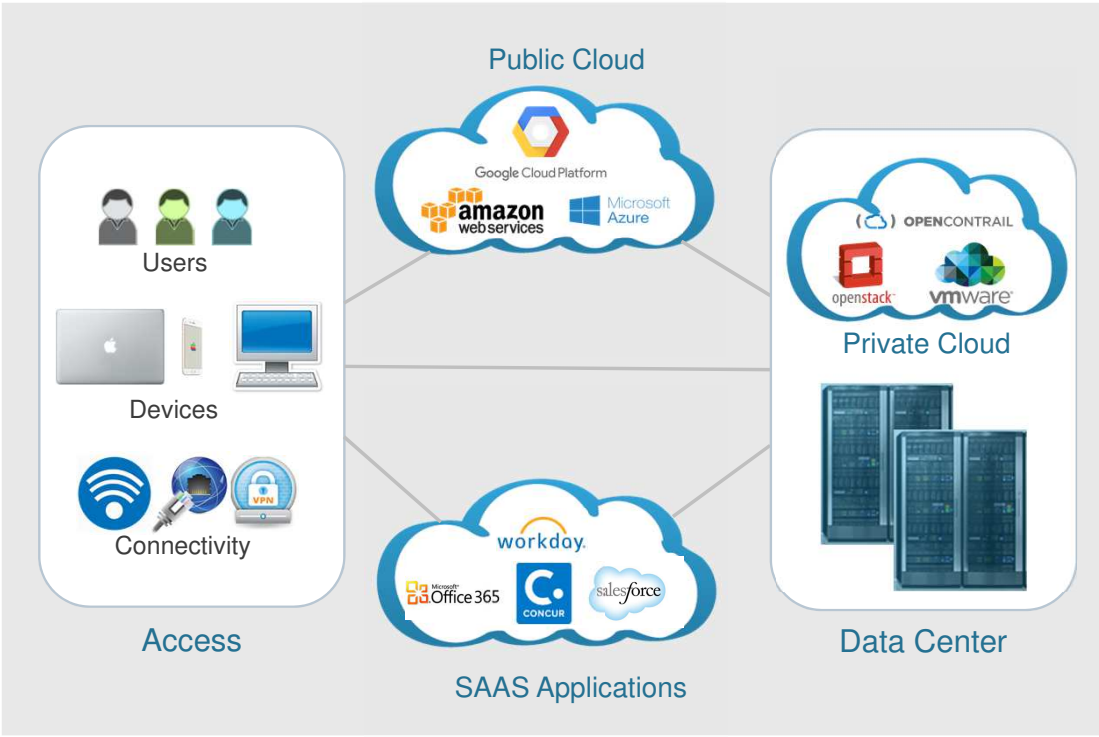
① 複数の異なるベンダーのログを管理する必要がある。

② ネットワーク、エンドポイントを個別に可視化するだけでなく、ネットワーク全体として可視化する必要がある。

③ インシデント対応をネットワーク、エンドポイント両方に対して、時間をかけずに同時に実施する必要がある。

③（環境の問題）パブリック クラウドでのセキュリティってどうすればいいの？

パブリック クラウドでのセキュリティの課題



よくお伺いするお客様の声

① パブリッククラウド側で用意されているセキュリティ ソリューションは、オンプレ環境で使っていたセキュリティ機器より細かい設定ができないケースがある。（設定の柔軟性が十分で無い）

② パブリッククラウドに流れている通信の可視化が難しいケースがある。（可視化の困難性）

③ クラウド/オンプレミス上でセキュリティ情報を共有する仕組みを確立できていない。(インシデント対応の未統合）

まとめ

① クラウド側のセキュリティ サービスで足りない場合は自分でセキュリティを準備する必要がある。

② クラウド上で流れている通信の可視化を考える必要がある。

③ インシデント対応をオンプレミス環境と同じように実施できる仕組みが必要である。

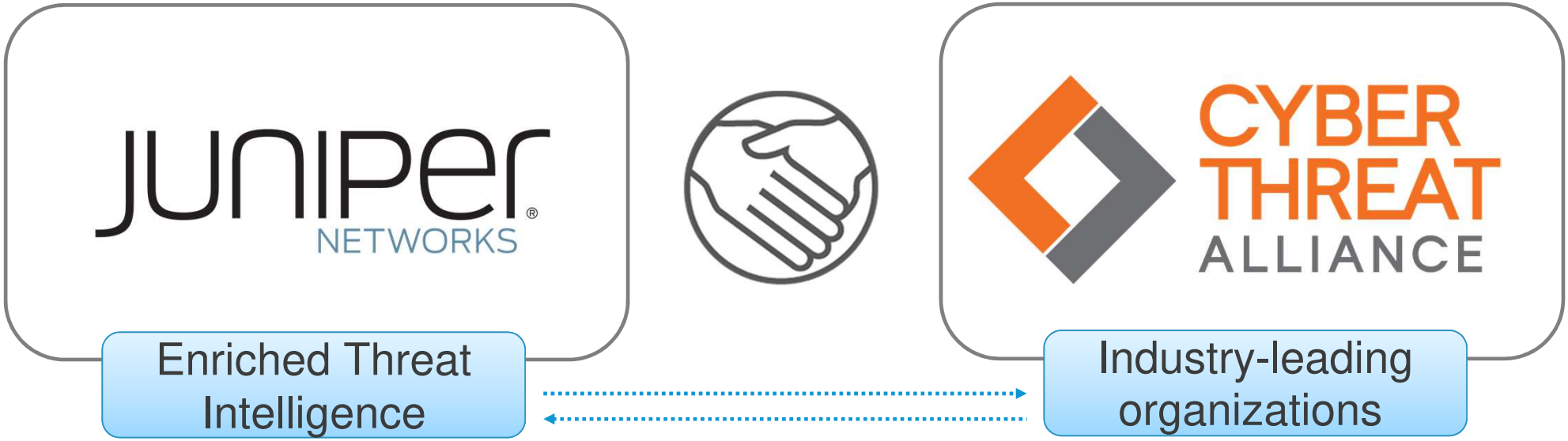
2. Juniperセキュリティビジネスへの取組みと市場での評価

JUNIPER NETWORKS | Engineering Simplicity

CTA (Cyber Threat Alliance) のメンバーとして活動

競合他社からもトップセキュリティベンダーとしての認知

直ちに実行可能な脅威情報をアライアンスメンバーと共有することで、
サイバーセキュリティ対策を強化



ICSAのAdvanced Threat Defense テストにて、未知の脅威に対する高い検知率が証明されております。

Test Length	28 days	Malicious Samples	504	Innocuous Apps	555
Test Runs	1059	% Detected	99.2%	% False Positives	1.1%

Fig. 1 – High Detection Effectiveness & Few False Positives

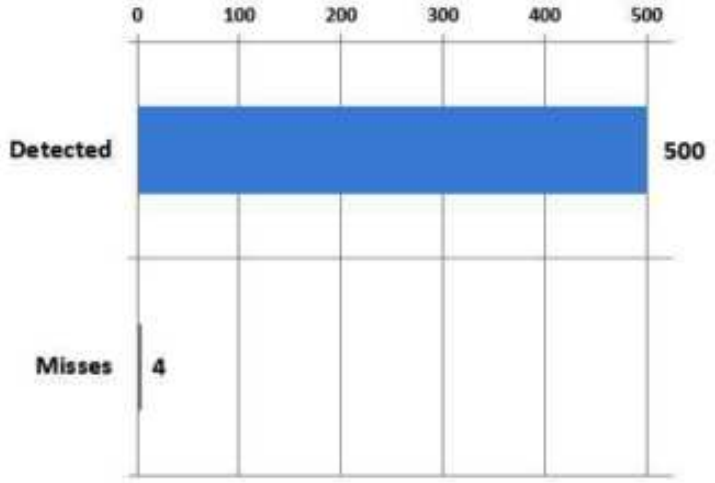


Fig. 2 – Detected 500 of 504 *New & Little-Known* Malicious Samples

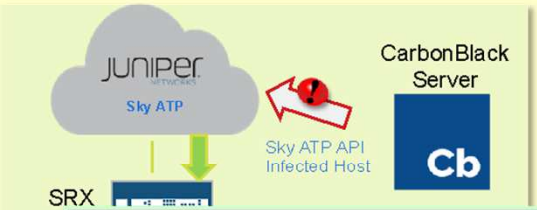
Fig. 3 – 6 Alerts on Innocuous Applications

Interop で５つの賞、ShowNet でもベスト賞を受賞
標的型攻撃対策のJATPはグランプリを受賞

- **Best of Show Award** -
  1. (Security) Grand Prix – JATP 400
  2. (AI) Grand Prix – Mist AI-Driven WLAN by Juniper Networks
  3. (Cloud Infrastructure) Grand Prix Runners-up - QFX5220 Series 400GbE Switch
  4. (NFV/SDI) Special Award – Contrail Service Orchestration (SD-Enterprise)
  5. (Management) Special Award – Contrail HealthBod
- **Best of ShowNet Award** – chosen by NOC staff of ShowNet
  1. Grand Prix - MX240 + MPC10E, QFX5220 for 400GbE (in conjunction with other vendors)

多くのメディアで取り上げられ、グローバル企業様でのご採用、サードパーティ企業との提携、マネージドサービス企業様でのご採用がされております。

ジュニパーネットワークス「JATP」,「Sky ATP」とカーボンブラックEDR製品の連携を発表（2018年5月25日）



ジュニパーネットワークス、カーボン・ブラックとのパートナーシップによる 統合型サイバーセキュリティプラットフォームの強化を発表

2019年04月16日

アウトソーシングテクノロジー、 ジュニパーネットワークスのインシデント対応自動化製品JATPを国内で販売開始

株式会社アウトソーシングテクノロジー（本社：東京都千代田区、代表取締役社長：茂手木 雅樹、以下 アウトソーシングテクノロジー）は、ジュニパーネットワークス株式会社（本社：東京都新宿区、代表取締役社長：古屋知弘、以下、ジュニパーネットワークス）とパートナー契約を締結し、「JATP（Juniper Advanced Threat

リコー、ネットワーク基盤の刷新にジュニパーネットワークスの製品群を採用 [事例]

[2018/08/09 18:45] *ブックマーク

● 関連キーワード 導入事例 ネットワークスイッチ/ルーター ネットワーク構築 ネットワークセキュリティ

ジュニパーネットワークスは8月9日、リコーが、グループの全国約500拠点のネットワーク基盤の再構築にあたり、ジュニパーネットワークスの製品群を採用したと発表した。

多数の関連企業と拠点を抱えるリコーグループでは、事業所のLANは個別に管理し、WANは通信事業者のマネジメントサービス、インターネット接続はアウトソーシングを利用するといった具合に、場所の異なるオペレーションが混在していた。

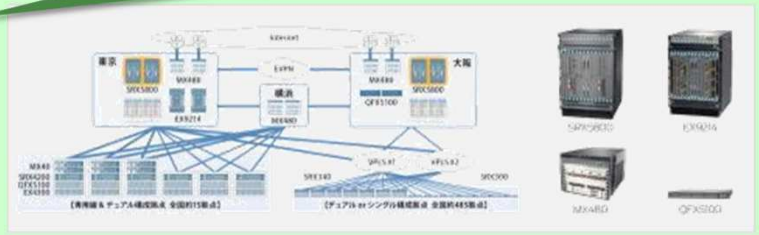
だが、クラウドの活用や働き方改革が進むにつれ、ユーザーからのITインフラに対する要求が高まり、従来の運用体制ではネットワーク機能の品質維持が困難になっていた。特に2010年頃からは、ネットワークのトラブルが増加すると共に、具体的な要求が増えていたという。

そうした課題を解決するため、同社は2011年頃からネットワークの再構築を開始。当初は2名のスタッフで運用していたことに加え、自前での設計／構築／運用を目指していたことから、「設定が容易であること」「自動化が容易であること」「異界標準の規格／プロトコルに対応してインターオペラビリティが確保できること」が優先的な要件として挙がり、検討の結果、ジュニパーネットワークスの製品群が採用された。

導入されたのは、主要なWAN回線とインターネット接続のほか、それらを束ねるコアルータとして「MX480」、ファイアウォールには「SRX5800」、イーサネットスイッチ「EX9214」、データセンターファブリックスイッチ「QFX5100」。選定にあたっては、製品群の中核を担う「Junos OS」が、分類の異なる機器や上位／下位機種でも設定方法が統一されているため、運用負荷が軽減される点、さらにPythonなどのオープンソースソフトウェアを用いた自動化が容易にできる点が高く評価されたとしている。

リコーグループ、大規模ネットワーク基盤の再構築にジュニパー製品群を採用表（2018年8月9日）

リコーでは、2018年中にSRXシリーズの導入を促進し、自動化をはじめとするテクノロジーを組み合わせた「Software-Defined Secure Network（SDSN）」を活用することで、安全性と効率性を両立したネットワークの実現を目指す。



18

NECネッツエスアイ、工場向けネットワークモニタリングソリューションにジュニパーネットワークス製品を採用

クラウド管理ソリューション「AppFormix」とマルウェア対策製品「Juniper Advanced Threat Prevention（JATP）」により、工場ネットワーク基盤の安全性とセキュリティの向上を実現

ジュニパーネットワークス株式会社（本社：東京都新宿区、代表取締役社長：古屋知弘、以下、ジュニパーネットワークス）は本日、NECネッツエスアイ株式会社（本社：東京都文京区、代表取締役執行役員社長：牛島祐之、以下、NESIC）が、同社の新しい工場向けネットワークモニタリングソリューション「FAネットワークモニター」に、ジュニパーネットワークスのクラウドソフトウェアプラットフォーム「AppFormix」と、オンプレミス型のマルウェア対策製品「Juniper Advanced Threat Prevention（JATP）」を採用したことを発表しました。これ

Juniper Advanced Threat Prevention「JATP」を販売開始【丸紅情報システムズ】

2019/06/05
丸紅株式会社

丸紅情報システムズ株式会社の子会社であり、クラウドサービスを中心に、データセンター事業を展開する株式会社イーツ（代表取締役社長：上原 志津子、以下イーツ）は、ジュニパーネットワークス株式会社（代表取締役社長：古屋 知弘、以下「ジュニパーネットワークス」）との協業により、Juniper Advanced Threat Prevention（以下「JATP」）の販売を開始します。

日々巧妙化するサイバー攻撃に対する検知・防御だけでなく、それに伴うインシデント対応など、企業におけるセキュリティ対策の強化は急務を迫られています。ジュニパーネットワークスが提供する「JATP」は、高度なサイバー攻撃から企業のネットワークをエンドツーエンドで保護するセキュリティソリューションです。
主に、インターネットトラフィックやメールからの、既知および未知のマルウェアやC&Cサーバへの通信など悪意ある通信を、機械学習の機能を備えたサンドボックス※1で解析する機能、お客様が導入済みの様々なサードパーティ製セキュリティ製品から各種アラート情報を収集、攻撃の関連性を自動的に結びつけサイバーキルチェーン※2をGUI上で可視化し脅威のリスクを判別する機能により、企業のセキュリティ対策を強化します。

3. Juniper Connected Securityとは？

JUNIPER NETWORKS | Engineering Simplicity

Connected Security とは “つながる“ セキュリティ

ネットワーク /エンドポイント セキュリティ

- Juniper FW/UTM（SRX, vSRX)
- サードパーティ Firewall
- サードパーティ Proxy
- サードパーティ エンドポイント

ルーター/スイッチ/認証サーバ

- Juniper Router
- Juniper Switch
- サードパーティ Switch/Router
- サードパーティ Wifi Router
- サードパーティ 認証 Server

- Juniper Security Director/Policy Enforcer
- サードパーティ Orchestrator

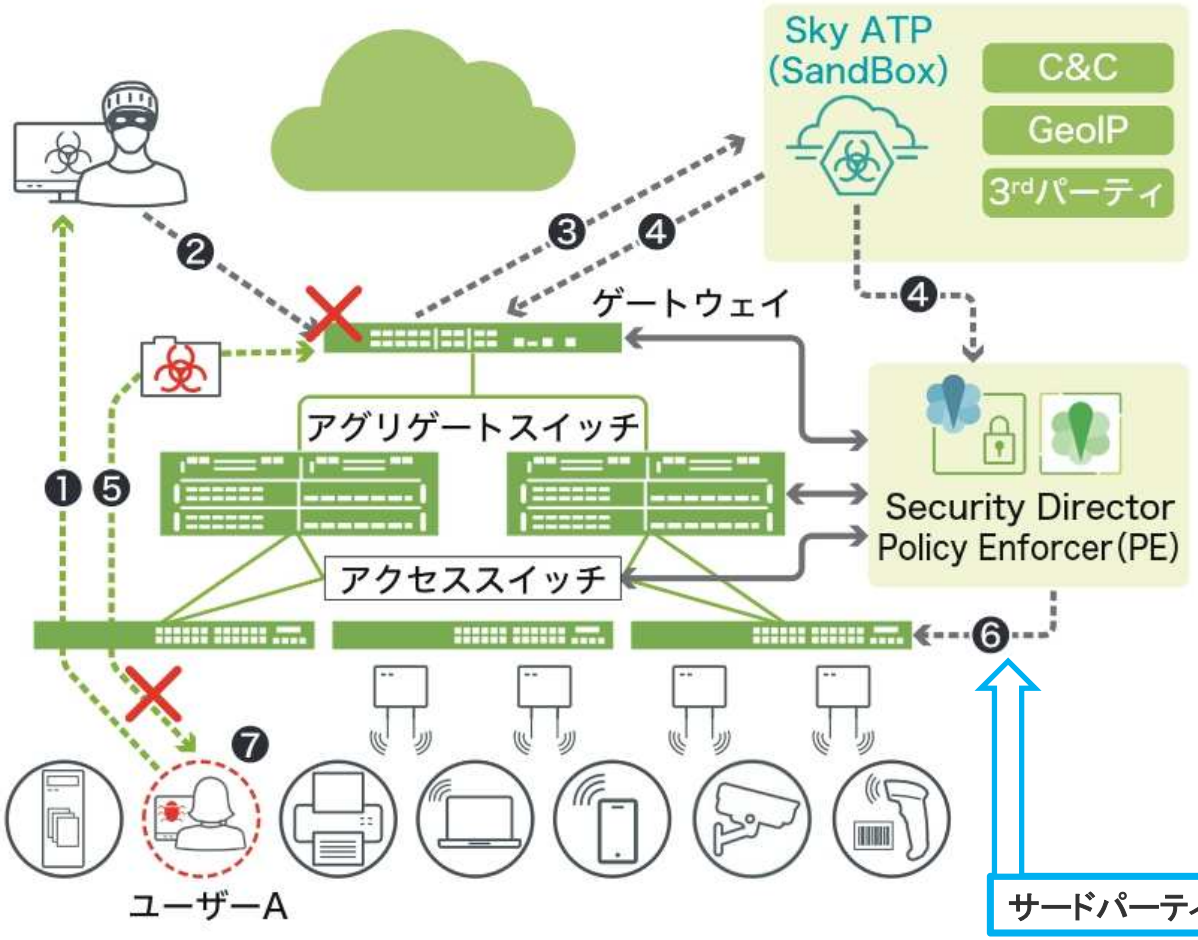
標的型攻撃対策/DDoS攻撃対策セキュリティ

- Juniper SkyATP
- Juniper JATP
- Juniper TDD

仮想環境/クラウド

- Juniper Contrail Security
- VMware NSX
- Nutanix
- AWS
- Azure

Connected Security のユースケース①
(Juniper SRX/SkyATP/SD/PE/EX + サードパーティとの連携)



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

サードパーティ認証サーバ、Switch, Wif Routerのとの連携も可能です！

Connected Security のユースケース①の特長

ネットワーク全体で脅威対策

- 侵入した脅威をMACアドレスベースで特定し、動的に追跡
- エージェントレスでクライアント端末のバージョン管理が不要

クラウドとの連携

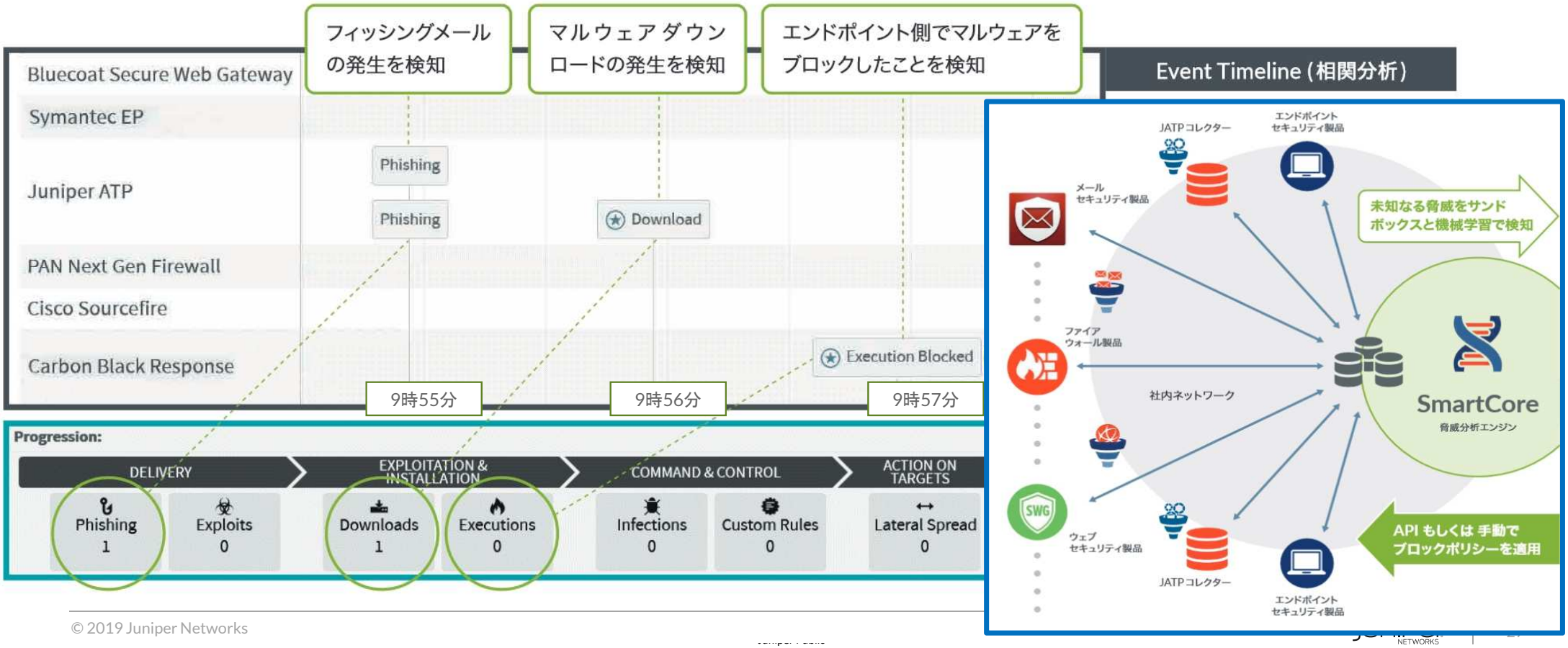
- クラウドやサードパーティと連携した最新の脅威情報
- リアルタイムでセキュリティ脅威の防御、検知および対処

脅威検知と対処の自動化

- ネットワーク内部に侵入した脅威を自動的に特定
- 事前に定義したポリシーに基づいて、自動的に脅威を排除

Connected Security のユースケース②
（Juniper JATP とサードパーティFW/Mail/WEB/EndPointとの連携）

～「どのユーザ」が「いつ」「どういった脅威」に影響し、「どの製品」でアクションしたか、「時間軸」で可視化～

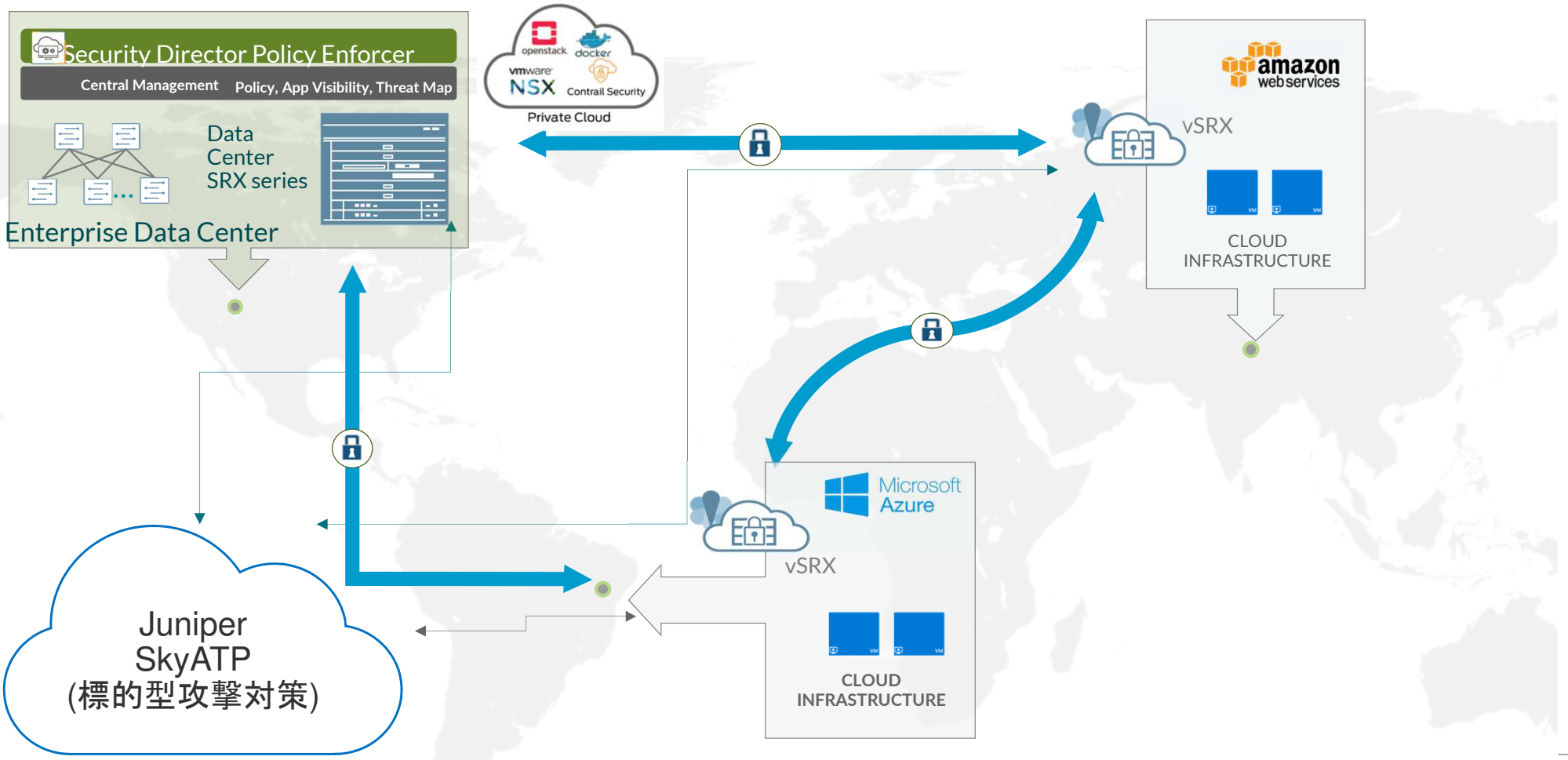


Connected Security のユースケース①と②のメリット
インシデント対応の自動化により、リアルタイムに脅威を封じ込め

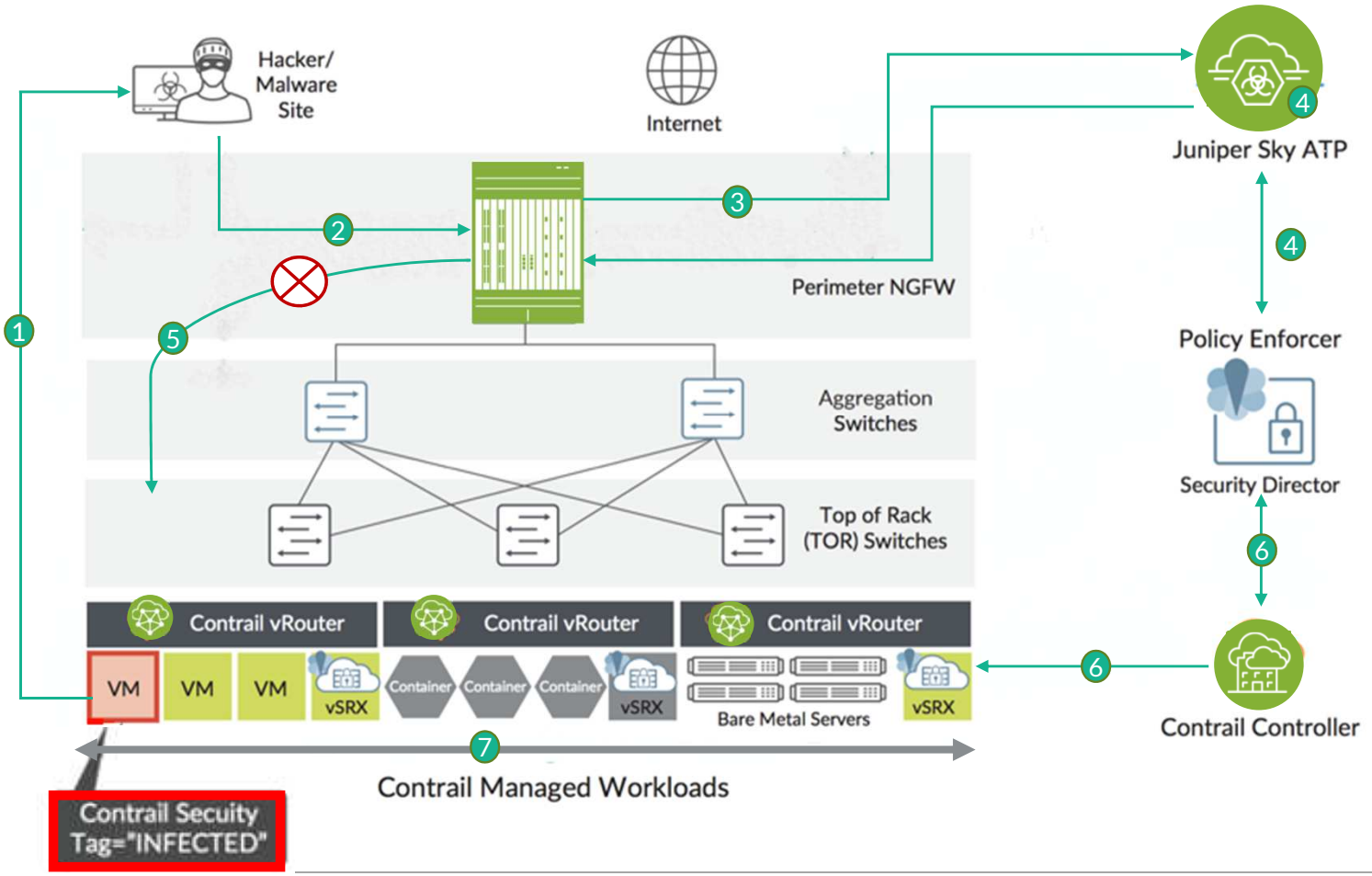
インシデント対応に掛かるプロセス	手動による対応	インシデント対応の自動化
ホスト、ユーザの特定	0.5 時間	自動
アンチウィルス、EDRのデータを収集	1 時間	自動
NGFW等からのネットワークデータ収集	1 時間	自動
相関分析	1 時間	自動
感染の進行と範囲を特定	0.5 時間	自動
一次対応を開始	0.5 時間	自動
合計時間	4.5 時間	10分以内

対応時間の軽減

Connected Security のユースケース③
（Juniper SkyATP/SRX/SD/PE とAWS/AZURE/VMware NSXとの連携）

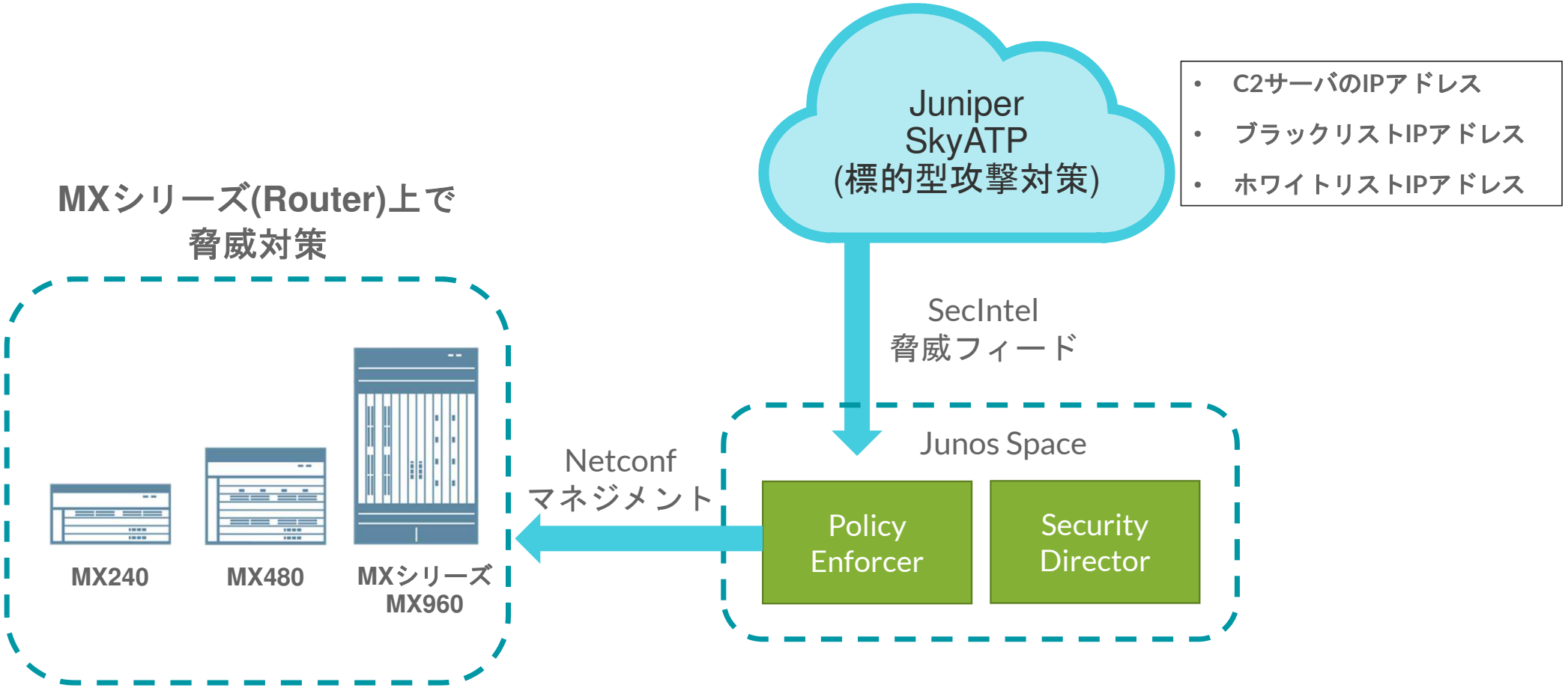


Connected Security のユースケース④
（Juniper Contrail Security/SkyATP/SD/PE/vSRXの連携）

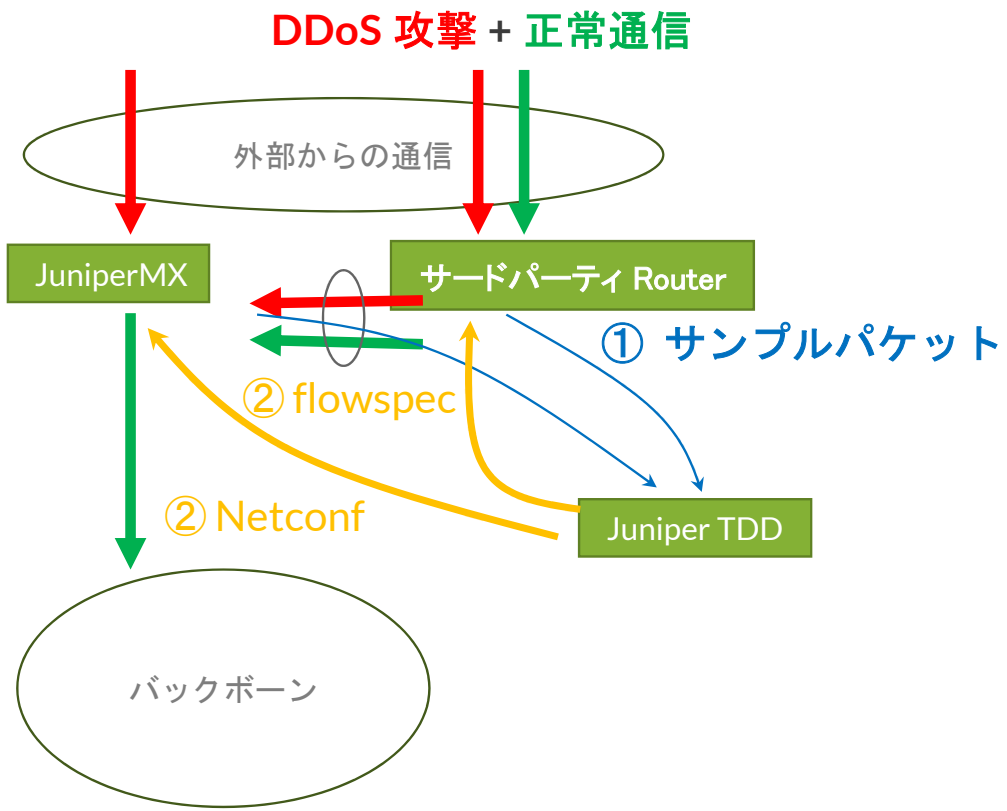


Juniper Contrail Securityとは？

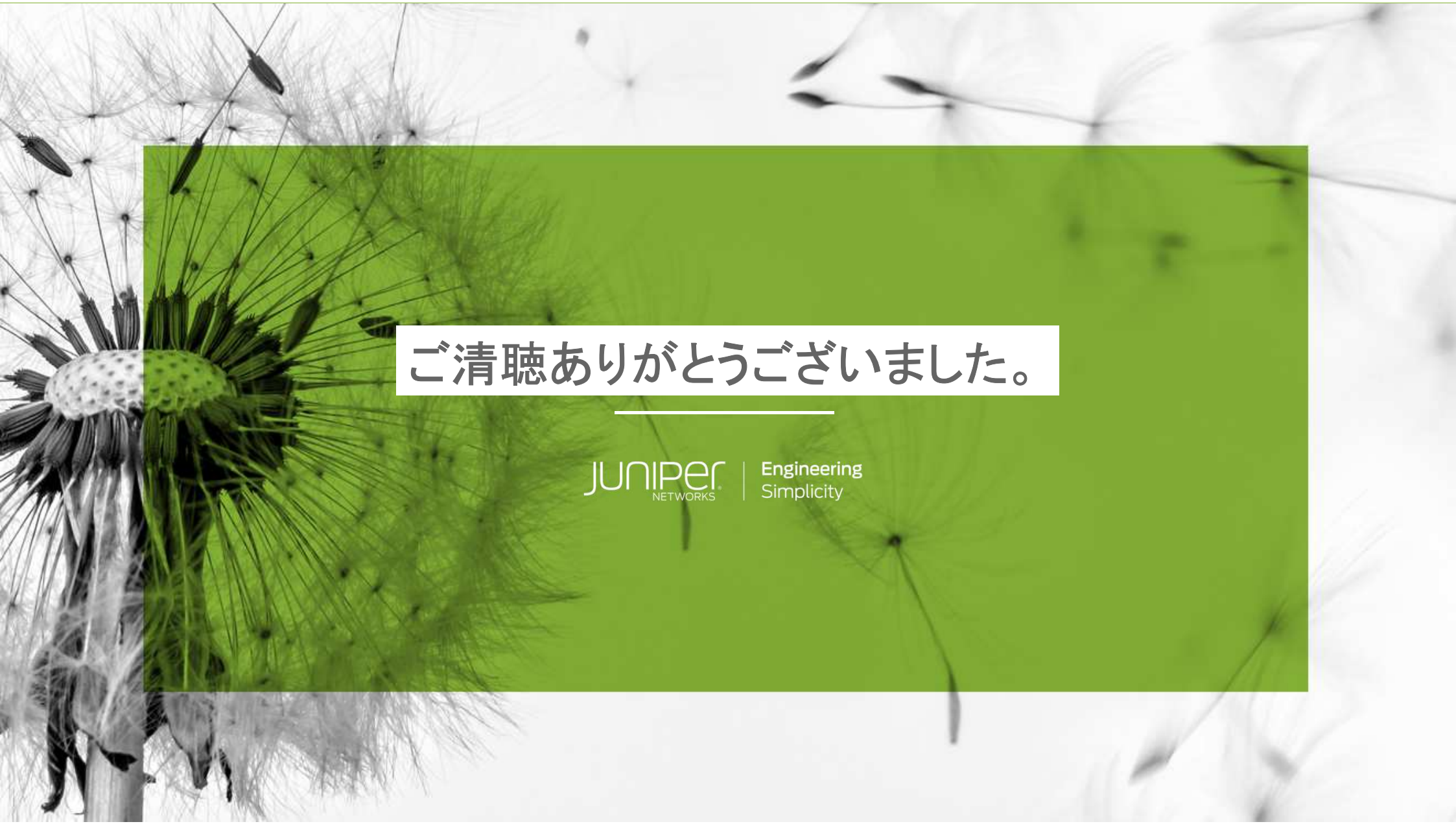
Connected Security のユースケース⑤
（Juniper MXとJuniper SkyATP との連携）



Connected Security のユースケース⑥
（Juniper TDD/MXとサードパーティRouterとの連携）



1. サードパーティRouterと Juniper MXが DDoS対策ソリューションのJuniper TDDにサンプルパケットを送付。
2. Juniper TDDが DDoS攻撃を検知
   - Flowspec をサードパーティRouterへ送付
   - Netconf（ブロックポリシ）をJuniper MX へ送付
3. サードパーティRouterがFlowspec情報を元に通信をMXへ転送（リダイレクト）
4. Juniper MXがNetconf情報を元にDDoS通信をドロップ
5. 正常な通信はそのままバックボーンへ転送


ご清聴ありがとうございました。
JUNIPER NETWORKS
Engineering
Simplicity