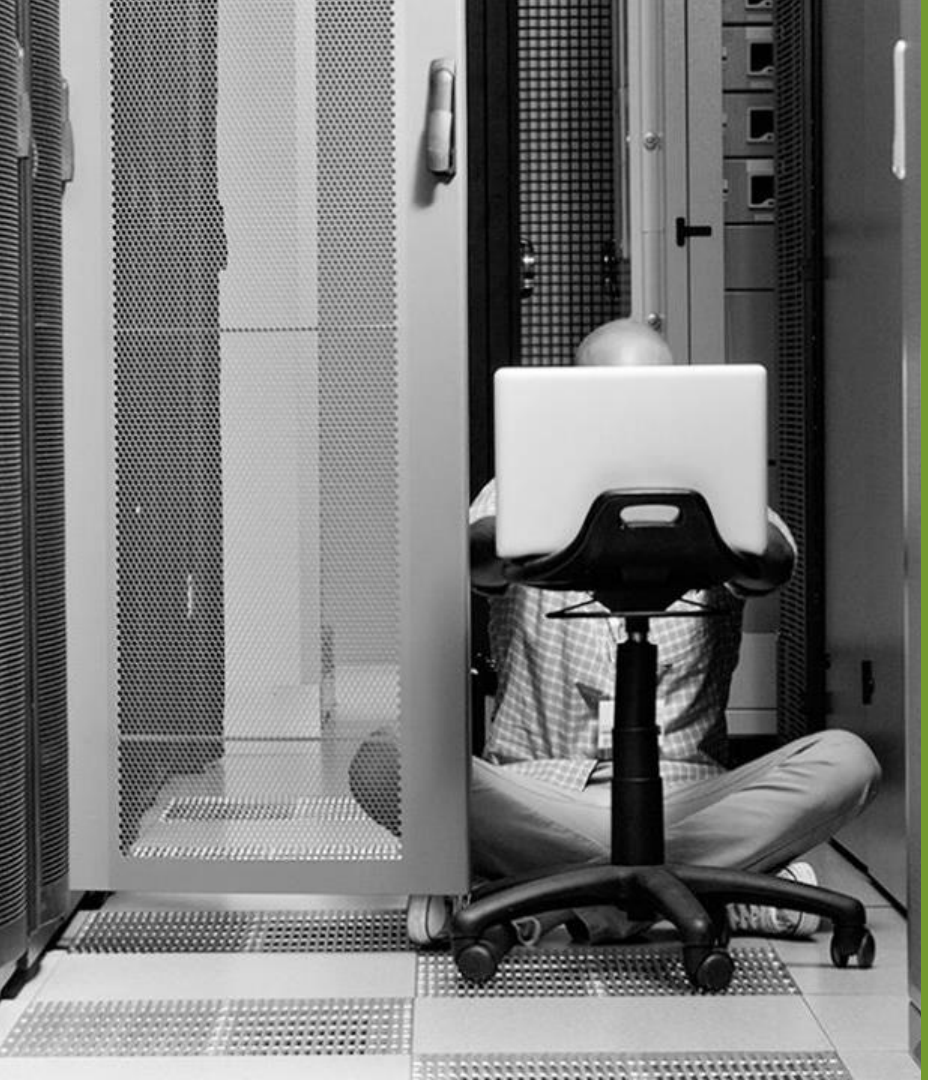
セキュリティの自動運用を可能とする
ジュニパーの コネクテッドセキュリティ とは

Oct 29, 2019

ジュニパーネットワークス
技術統括本部

Juniper Networks | Engineering Simplicity

AGENDA



サイバーセキュリティ脅威傾向と企業IT担当者の課題

情報セキュリティ 10大脅威（IPA）

情報セキュリティ 10大脅威　（2019年）　※組織対象				
1位	2位	3位	4位	5位
標的型攻撃による被害	ビジネスメール詐欺による被害	ランサムウェアによる被害	サプライチェーンの弱点を悪用した攻撃の高まり	内部不正による情報漏えい
6位	7位	8位	9位	10位
サービス妨害攻撃によるサービスの停止	ウェブサービスからの個人情報の窃取	IoT機器の脆弱性の顕在化	脆弱性対策情報の公開に伴う悪用増加	不注意による情報漏えい

フィッシングによる脅威

DoS 攻撃

人為的な情報漏洩

新たな攻撃手法による危険性

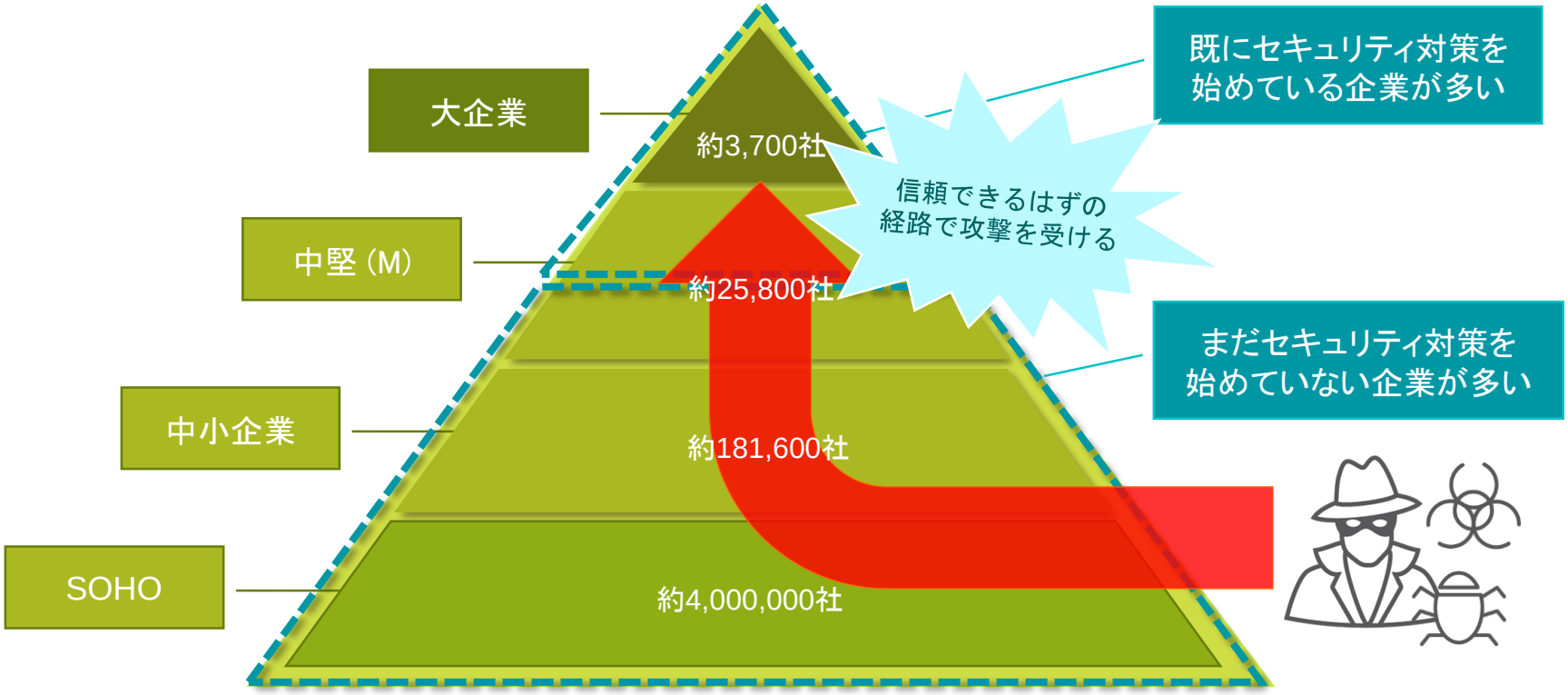
標的型攻撃

脆弱性を狙った攻撃

ランサムウェア

引用：IPA「情報セキュリティの企業向け10大脅威」より　https://www.ipa.go.jp/security/vuln/10threats2019.html

サプライチェーン攻撃



人工知能（AI）使いこなすには．．．

ARTIFICIAL INTELLIGENCE

Human intelligence exhibited by machines

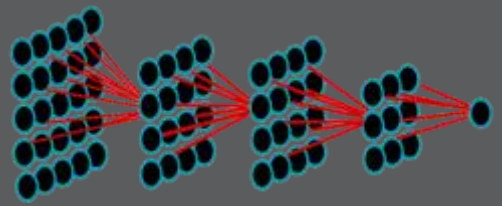
ATP
高度な脅威対策
セキュリティインテリジェンス

MACHINE LEARNING

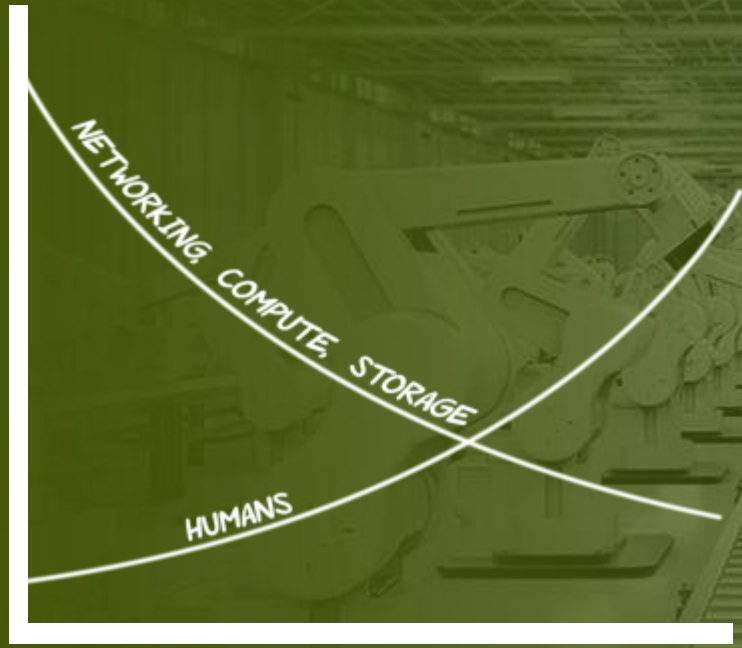
Using algorithms to parse data, learn and predict

DEEP LEARNING

Utilizing multiple layers of neurons



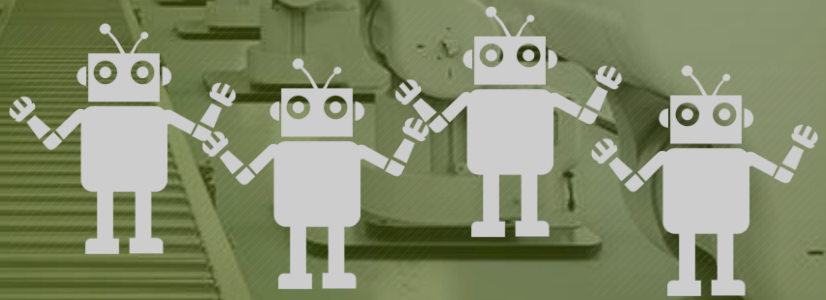
自動化 – セキュリティのためのキラーアプリ



ユニットのコスト

規模と多様性

自動化を活用し、
インフラのセキュリティコスト
および、人為的エラーを
減少させることが重要な課題



企業IT担当者の抱える課題

IT担当やセキュリティ技術者・エキスパートの不足

「働き方改革」の実現に向けて、情報システム部門においても業務改善が求められている

多様化するサイバー脅威に対して正確で迅速な対応

「多層防御」の運用負荷が増大し、コストを掛けずに的確で迅速な運用を行うことが難しい

IoTやBYOD等、増え続けるデバイスのセキュリティ

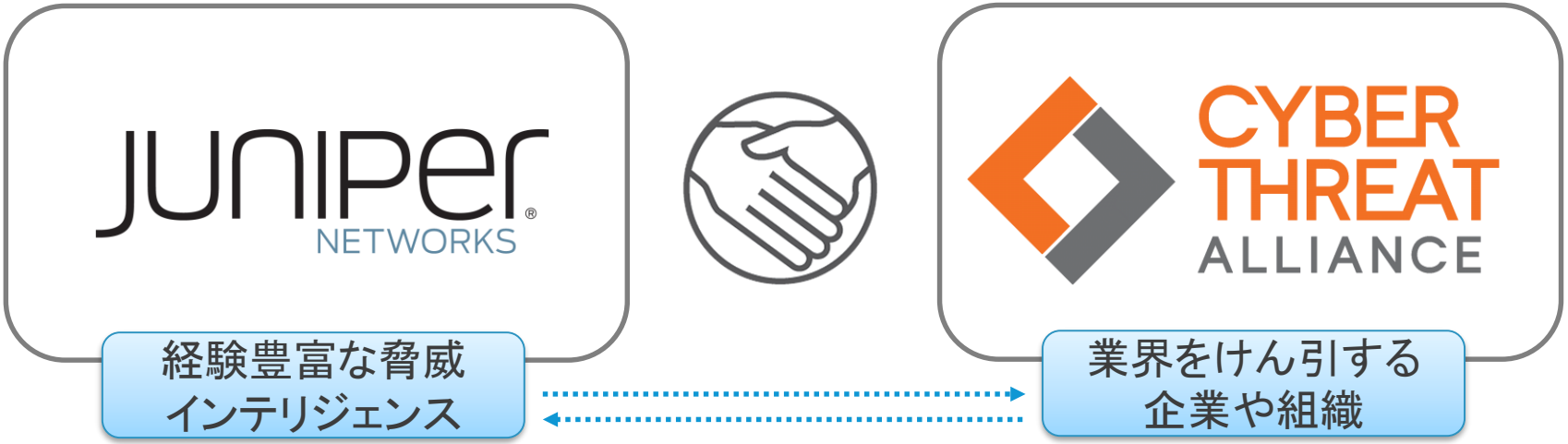
利用デバイスやサービスが増え状況を正確に把握することが困難になってきている

ジュニパー ネットワークス
セキュリティに対する取り組み

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



ジュニパーのセキュリティに対する取り組み

設立

SDセキュアネットワーク

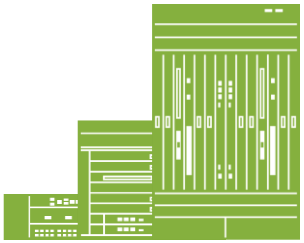
ジュニパー　コネクテッドセキュリティ

1996　2004　2008　2016　2019

ルータ製品

NetScreen
（SA/SSG/ISG）

JUNOS



SRX5000シリーズ

Sky ATP

Security
Director

SRX4600

vSRX

cSRX

JATP Appliance

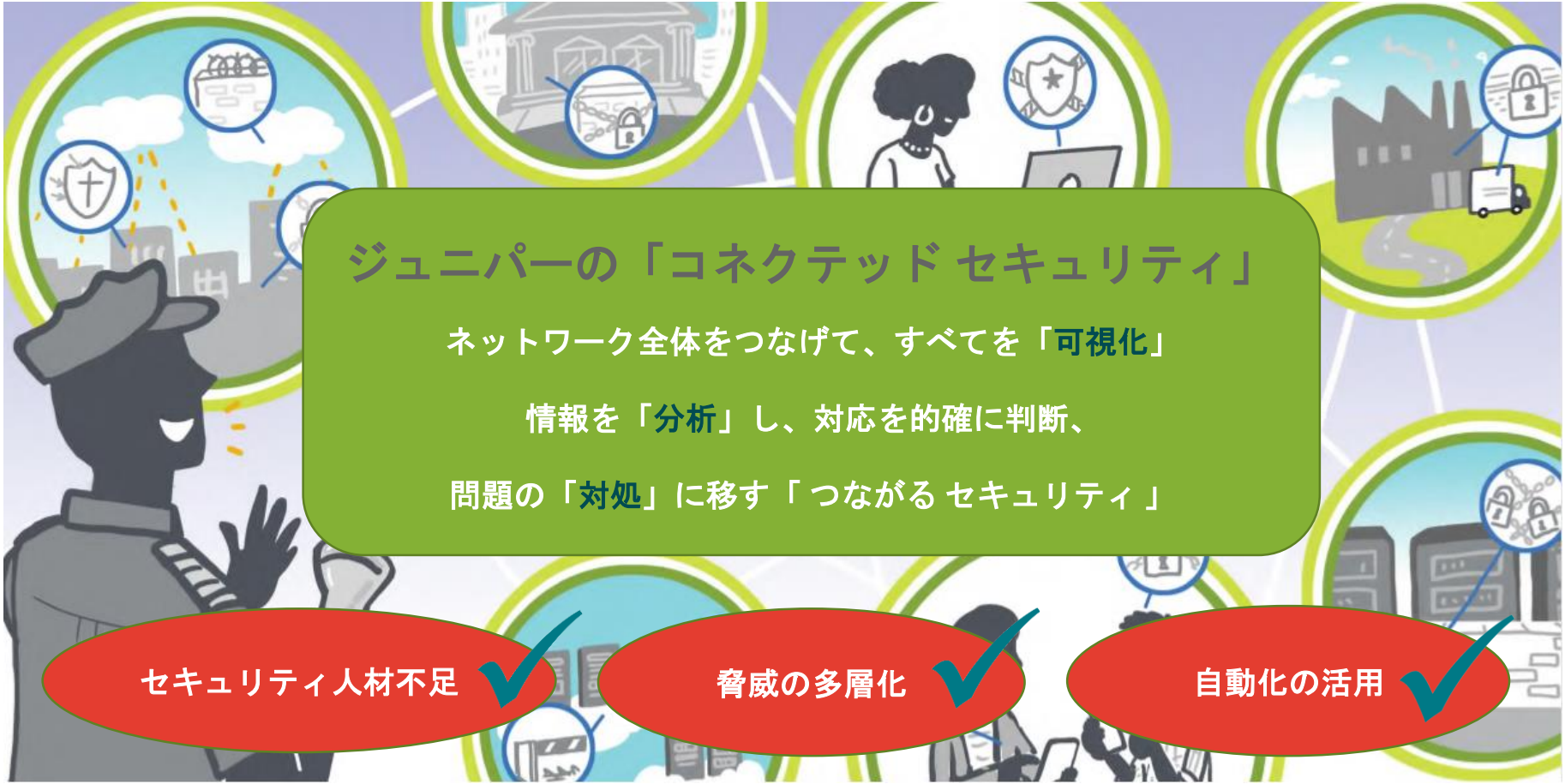
SRX300

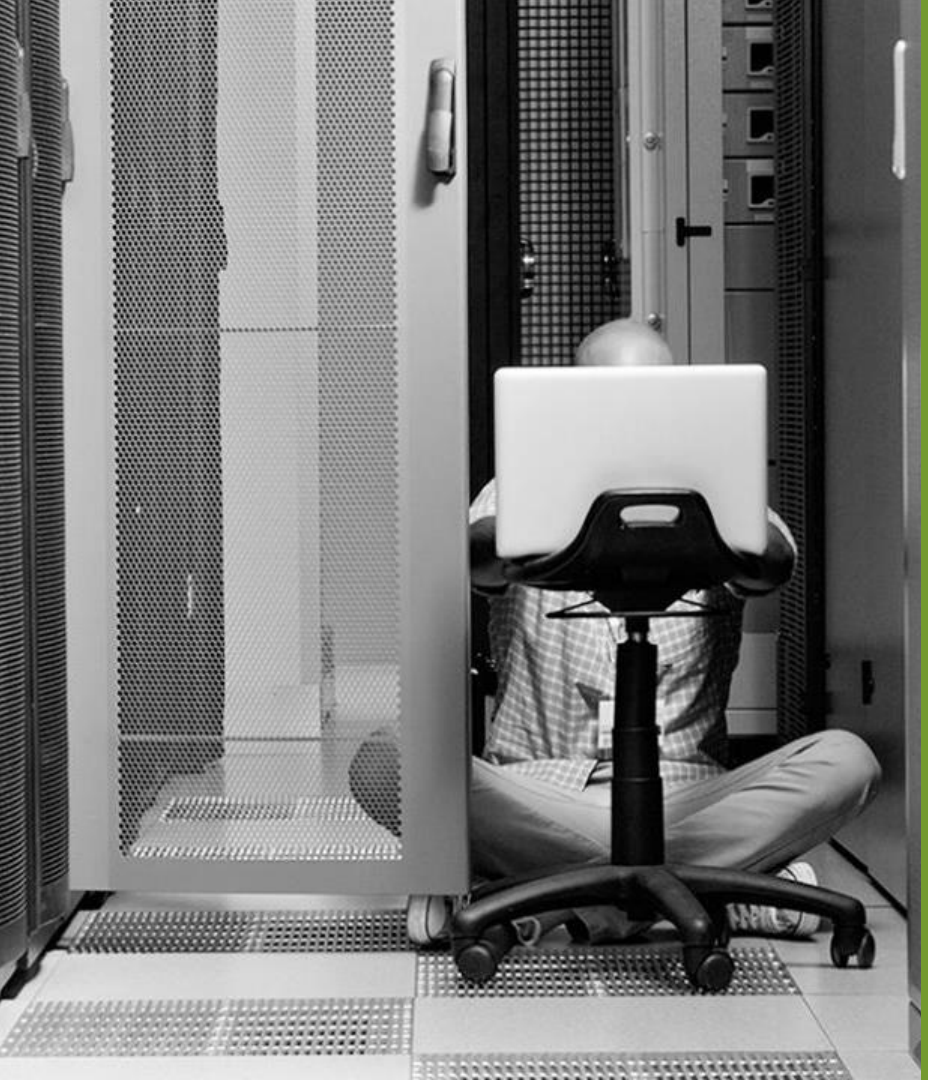
SRX1500

簡単に言うと「コネクテッドセキュリティ」とは？

ネットワークのセキュリティをつなげて

https://www.juniper.net/assets/jp/jp/local/pdf/ebooks/simplified-connected-security.pdf





① 運用負荷を大幅に削減する
コネクテッドセキュリティ

ジュニパーのコネクテッドセキュリティ①

監視

マルチベンダ環境における
- セキュリティのイベント
- 脅威インテリジェンス

可視化

自動化

- すべてのセキュリティシステムで連係して脅威を検知
- ノイズの多いログから脅威を発見

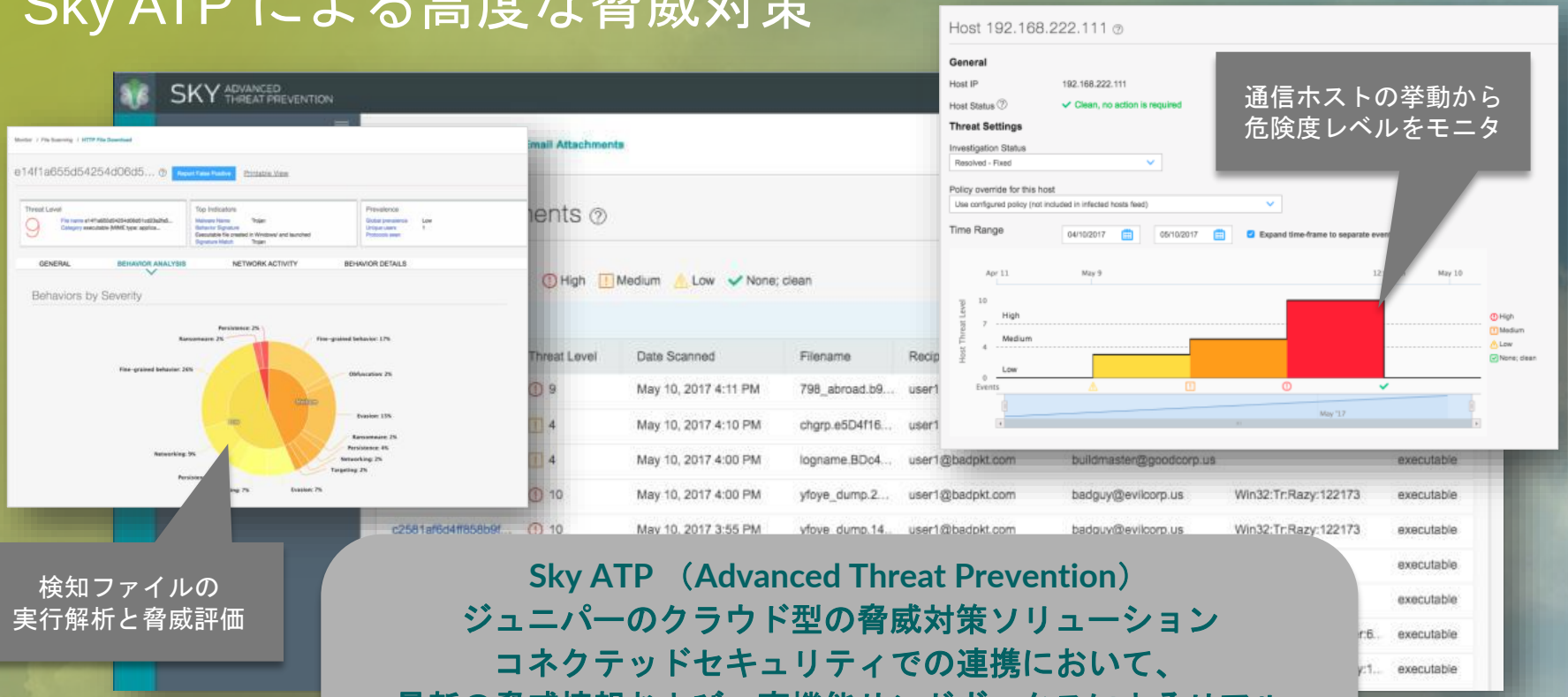
検知

- 感染ホストの自動隔離
- ワンタッチのリスク軽減
- サードパーティ連携

対処

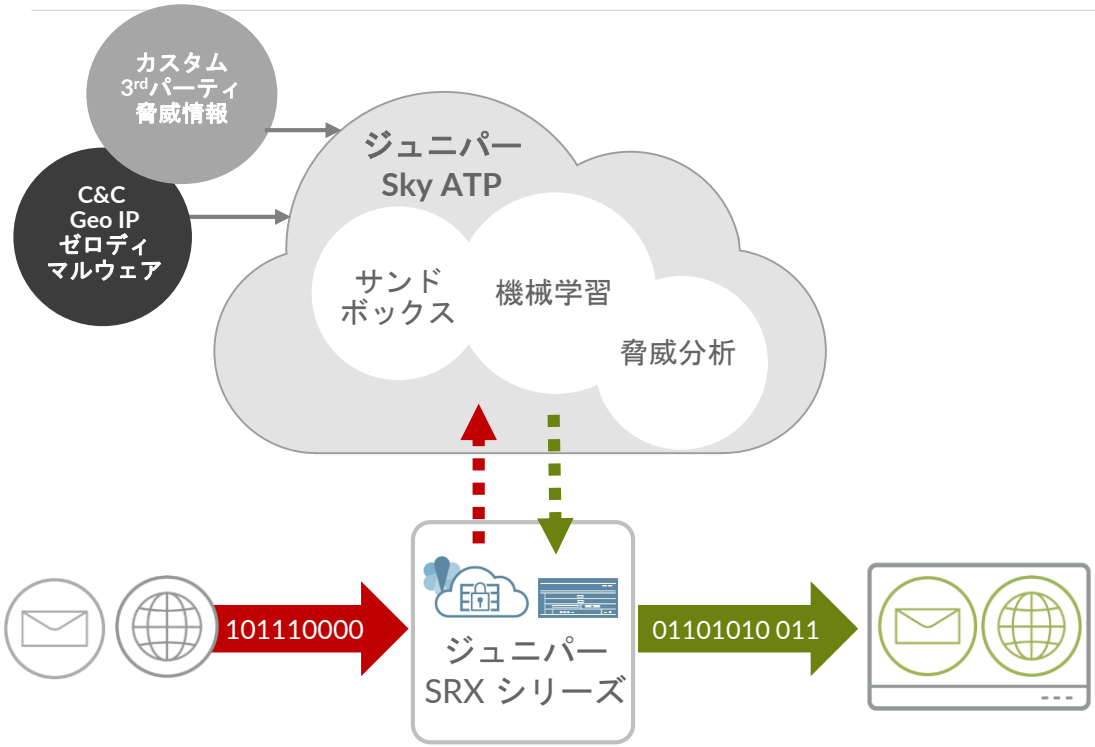
防御

Sky ATP による高度な脅威対策



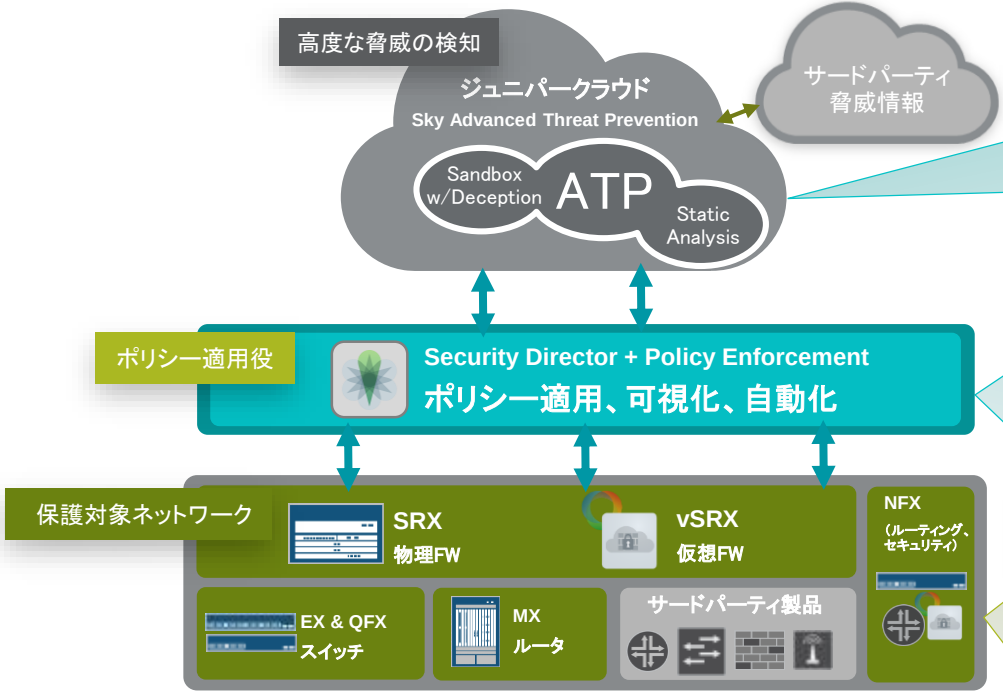
Sky ATP （Advanced Threat Prevention）
ジュニパーのクラウド型の脅威対策ソリューション
コネクテッドセキュリティでの連携において、
最新の脅威情報および、高機能サンドボックスによるリアル
タイム解析と傾向分析によるセキュリティ評価を提供します

コネクテッドセキュリティ①：
Sky ATP の主要な機能



- ウェブとメールのファイルを分析
- ランサムウェアなどの
  高度なマルウェアからの保護
  （ゼロデイ対策）
- 脅威インテリジェンス
  - レピュテーション
  - フィード情報
    （C&C, GeoIP, カスタム）
- 日本、欧州、米国、カナダに
  データセンターを設置
- STIX / TAXII
- FedRAMP認定

コネクテッドセキュリティ①：
ネットワークを一つのドメインとして守る仕組み



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

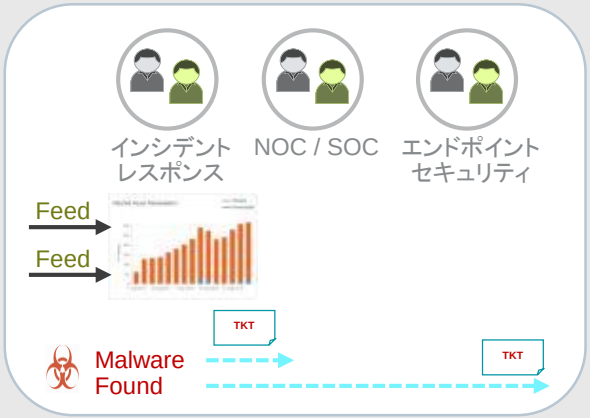
3. 対策実行

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

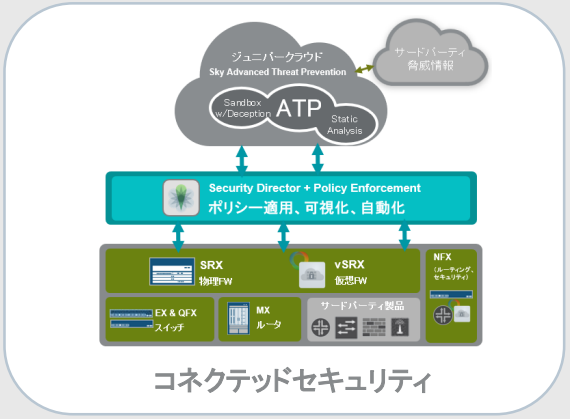
それぞれのネットワーク機器にてポリシーを適用、ネットワーク全体を単一の対策実行ドメインに！

コネクテッドセキュリティ①：
セキュリティ脅威を自動的に検知し排除する仕組み

手動による脅威対策（従来型）



脅威を自動的に検知・排除



事象の
発見・通報
（ユーザ・運用者）

初動対処の可否、
情報伝達
（運用者）

被害拡大の
防止・抑制
（運用者）

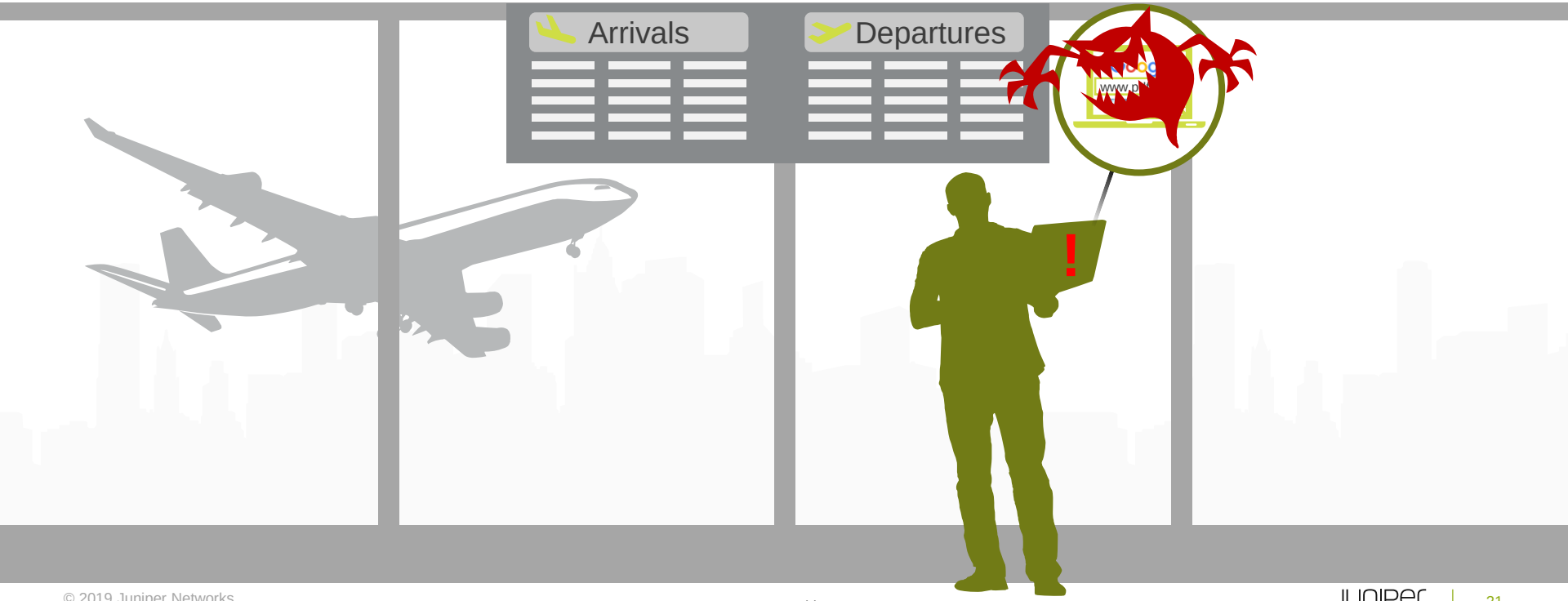
原因推定の調査
（運用者・
セキュリティ責任者・
専門組織）

再発防止策の立案
（運用者・
セキュリティ責任者・
専門組織）

脅威の検知から、対処・防止策までを自動化

標的型攻撃の罠は、あらゆる場面に存在する！

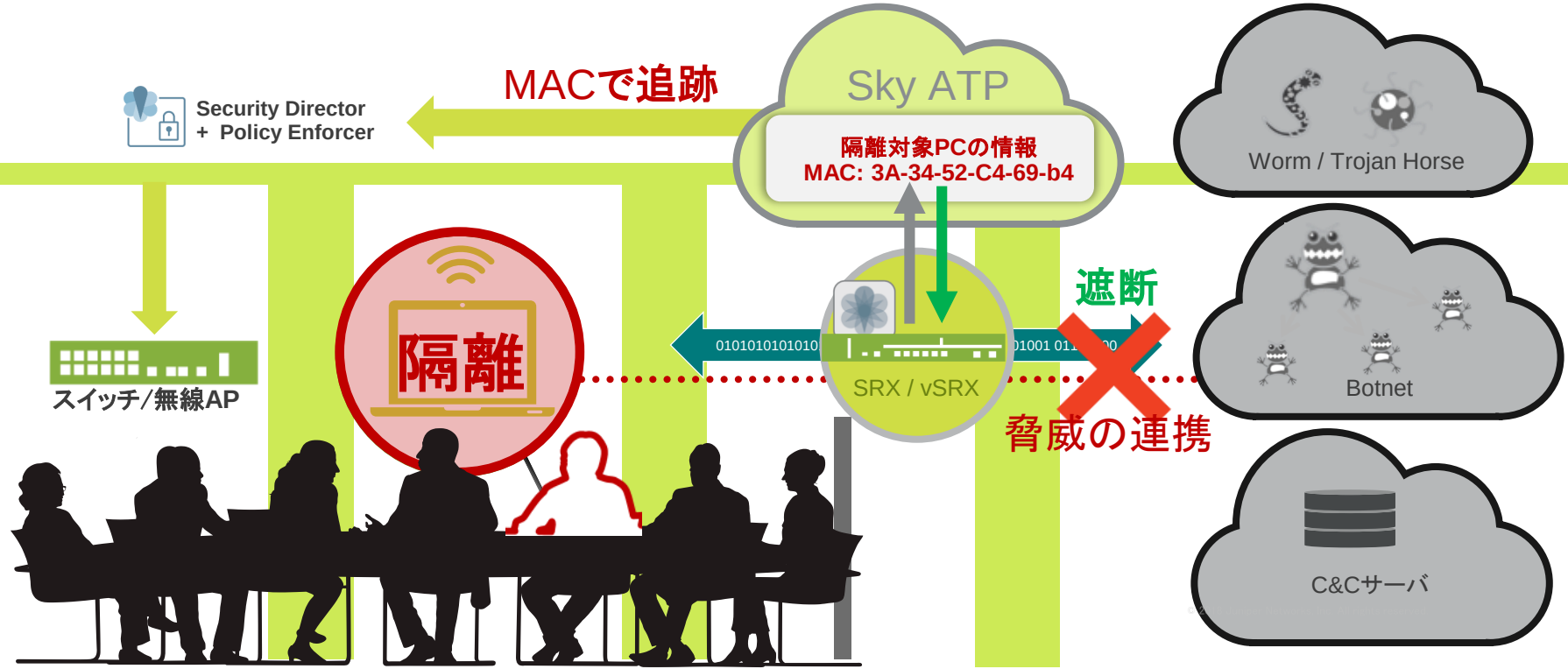
出先でのちょっとした作業で、意図しない感染に遭遇



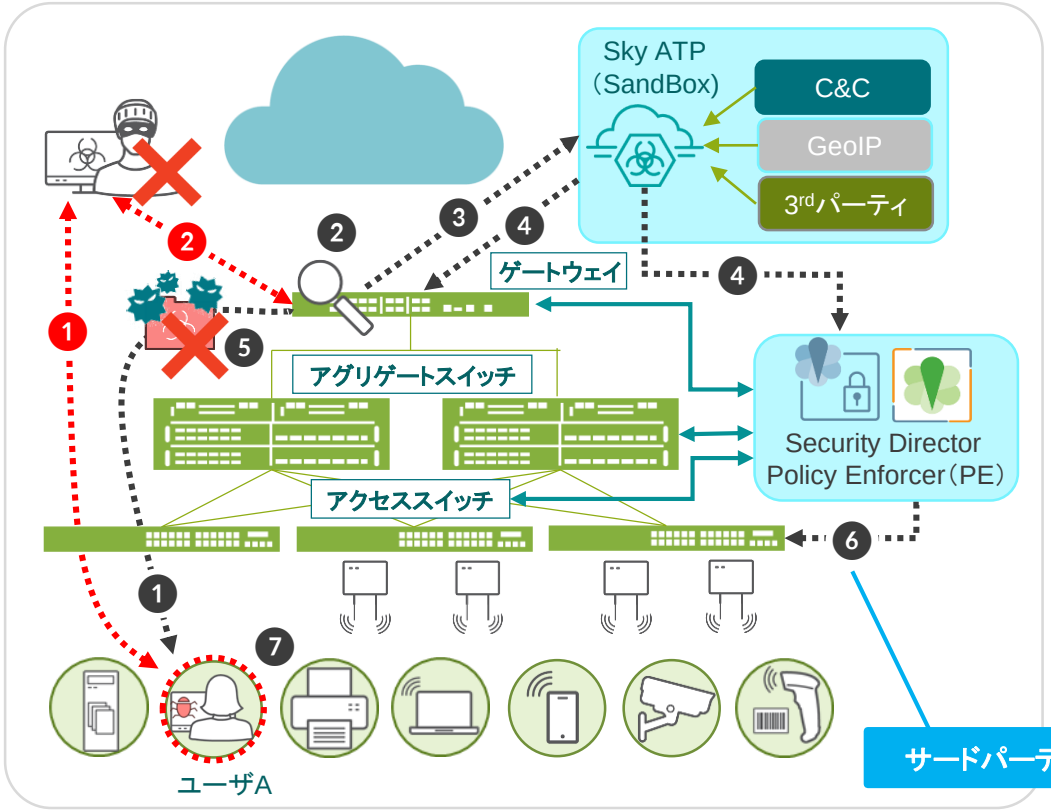
感染拡大はあっという間！！

ネットワーク内部からの攻撃は簡単に甚大な被害へとつながる

コネクテッドセキュリティ①：
拡散する脅威をMACアドレスで追跡・隔離



コネクテッドセキュリティ①：
連動するつながるセキュリティ



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, Wifi Routerのとの連携も可能

コネクテッドセキュリティ①：
Sky ATP を使ったネットワークの主な特徴

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

コネクテッドセキュリティ①：
感染の拡散への対策（動作比較）

他社ソリューションの場合

感染したホストがファイルをダウンロード

クラウドで分析し評価結果をFW機器へ返答

クラウドで不正通信へのシグネチャとアラートを生成

感染ホストがC&Cから2nd ステージのダウンロード

FW機器はフローを許可し2nd ステージのダウンロード完了

感染拡大！

脅威の分析 → 脅威への対応 → 脅威の挙動 2ndステージ：拡散活動 → 脅威（2ndステージ）への対応

ジュニパーコネクテッドセキュリティの場合

Sky ATPで分析、以下の手法にて評価した結果をSRXへ返答

分析手法
- **Hash / AV**
- **Static**
- **Dynamic**

感染ホストの通信ブロック **ポリシー生成自動適用**

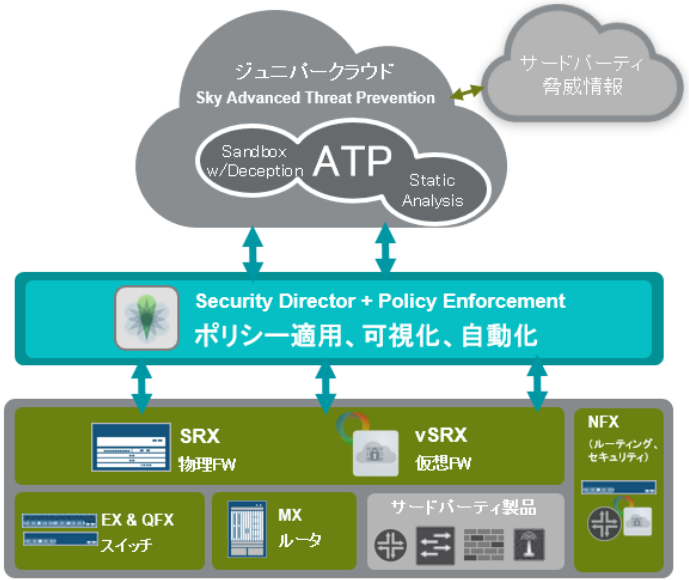
感染ホストがC&Cから2nd ステージのダウンロード

通信動作を不正と判断し、**SRXが通信を拒否**

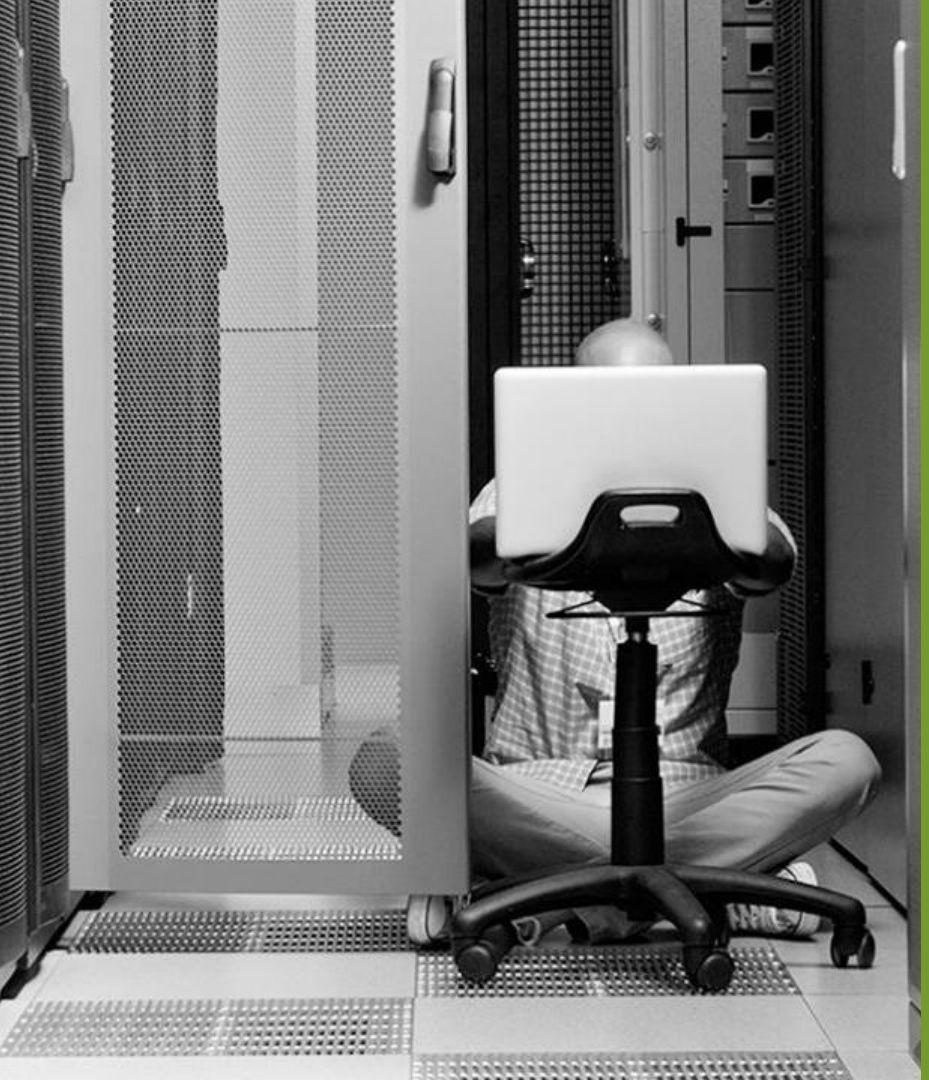
感染拡大を完全ブロック！

コネクテッドセキュリティ①：
運用負荷の大幅な削減（まとめ）

- 最新型のクラウド脅威対策を活用
- 複数の段階を必要としていた従来のセキュリティ運用をシームレスに自動化
- 内部に侵入した感染脅威をネットワーク全体にてブロック



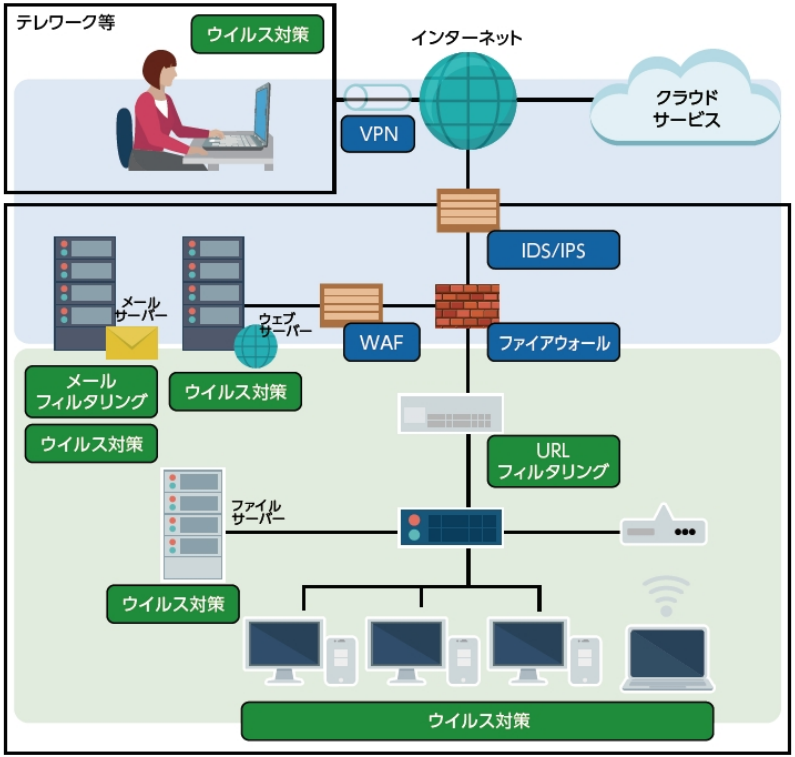
自動化を最大限に利用して、セキュリティ運用の負荷を大幅削減



② 多層防御の課題を解決する
コネクテッドセキュリティ

セキュリティ運営が抱える新たな問題

一般的なセキュリティ対策のネットワーク図



実際のお客様の声：

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

多層防衛の課題

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。

画像出典：「日本容器包装リサイクル協会」

JATP SmartCore

JATP によるネットワークの自動防御

JATP400

JATP700

JATP （Juniper Advanced Threat Prevention）
高度な機械学習を取り入れたオンプレミス型脅威検知ソリューション
コネクテッドセキュリティでの連携において、マルチベンダーの
セキュリティ情報の相関分析を行い、脅威の挙動を可視化しノイズを
削減することにより、正確で迅速な対応を可能にします

オールインワン

製品番号	パフォーマンス（オブジェクトのデトネーション）[1]	パフォーマンス
JATP400	最大 25,000 オブジェクト/日	1 Gbps
JATP700	最大 61,000 オブジェクト/日	2.5 Gbps

SmartCore

製品番号	パフォーマンス（オブジェクトのデトネーション）[1]	ロギング パフォーマンス
JATP400	最大 50,000 オブジェクト/日	1500 イベント/秒
JATP700	最大 130,000 オブジェクト/日	1500 イベント/秒

コレクター

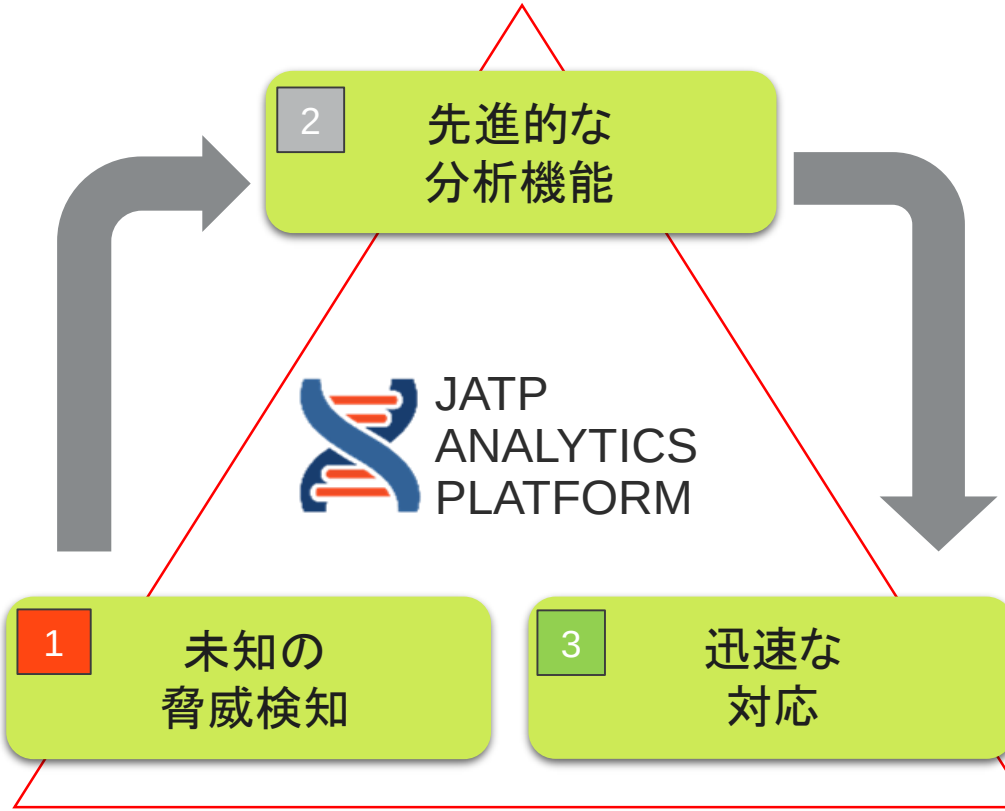
製品番号	パフォーマンス
JATP400	1.5 Gbps
JATP700	4 Gbps

電子メール MTA レシーバー

製品番号	1 日あたりの最大電子メール数
JATP400	70 万
JATP700	200 万

※仮想版においても提供

コネクテッドセキュリティ②
JATPの分析プラットフォーム



1 未知の脅威検知:

万が一未知の脅威が侵入した場合も、
ふるまい検知エンジンがウェブ、Eメール、
端末間の通信を継続的にモニターし検知します。

2 先進的な分析機能:

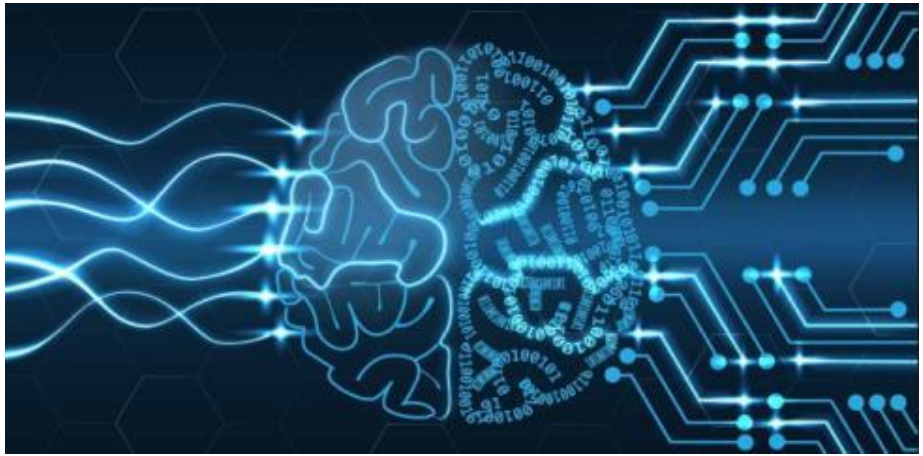
既存のサードパーティのイベントを含めた
相関分析と時間軸の分析により、
優先度の高い脅威を特定できます。

3 迅速な対応:

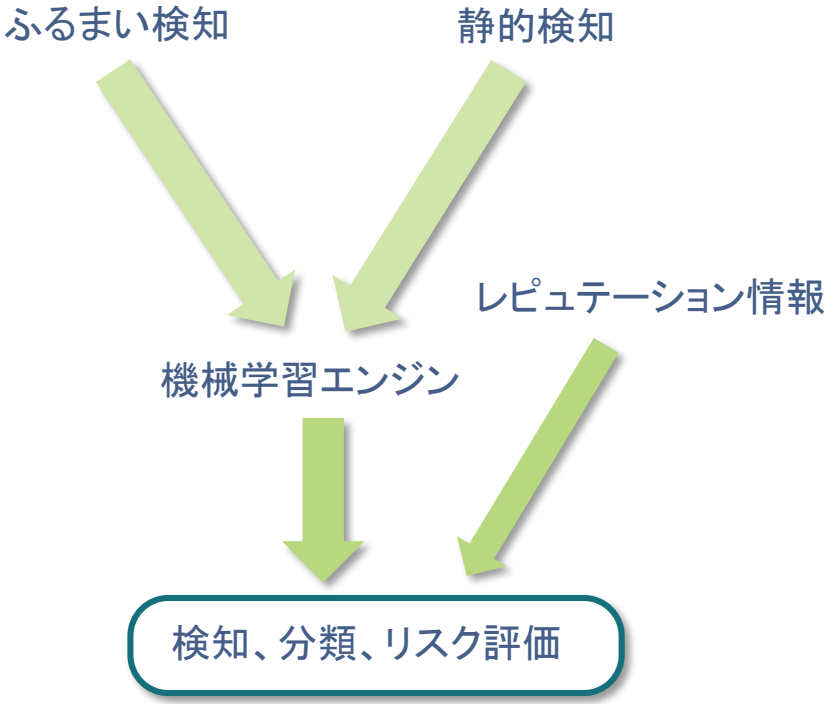
手動、もしくはAPIによる自動化により、
感染の疑いのある端末を隔離し、同じ通信を
通過させないように迅速に対応可能です。

コネクテッドセキュリティ②
優れた機械学習エンジンによる未知のマルウェア対策

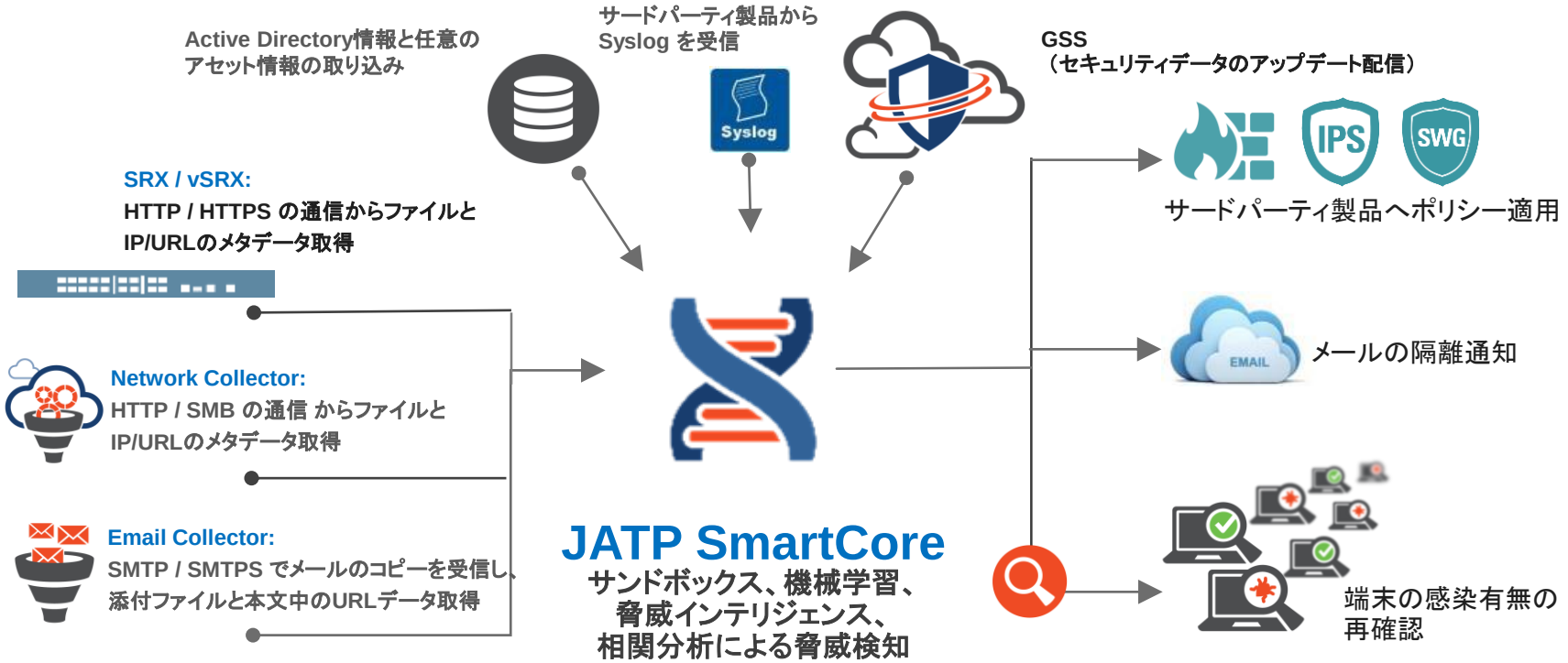
アルゴリズム ＋ 大量データによる継続的な自己学習



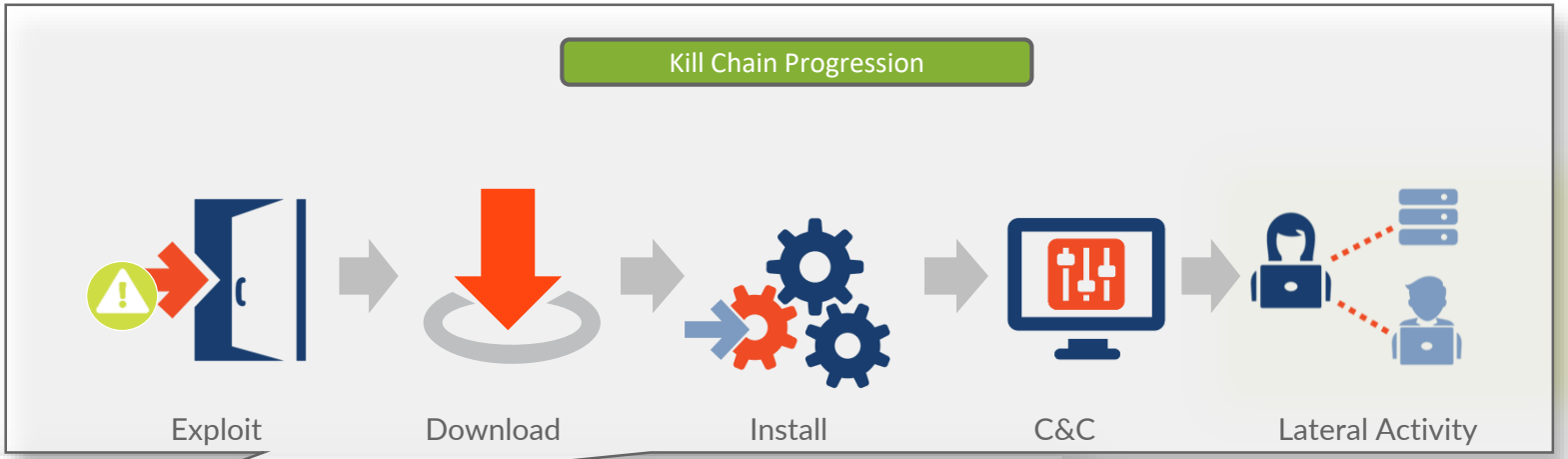
優れたアルゴリズムに継続的に学習させることにより、
高い検知率と低い誤検知率を実現

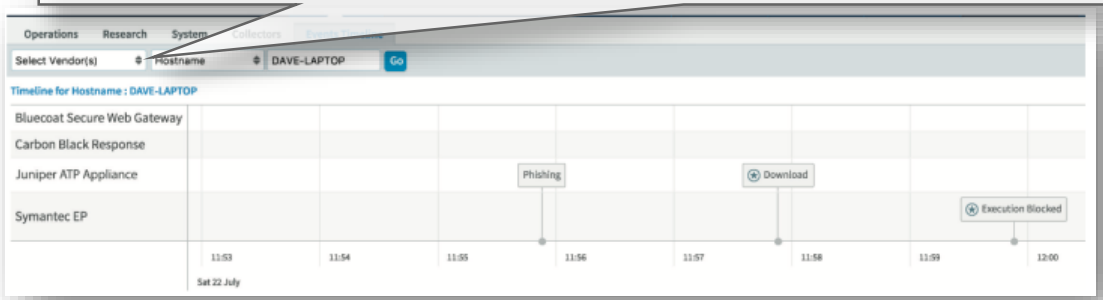


コネクテッドセキュリティ②
JATP 防衛連携の流れ



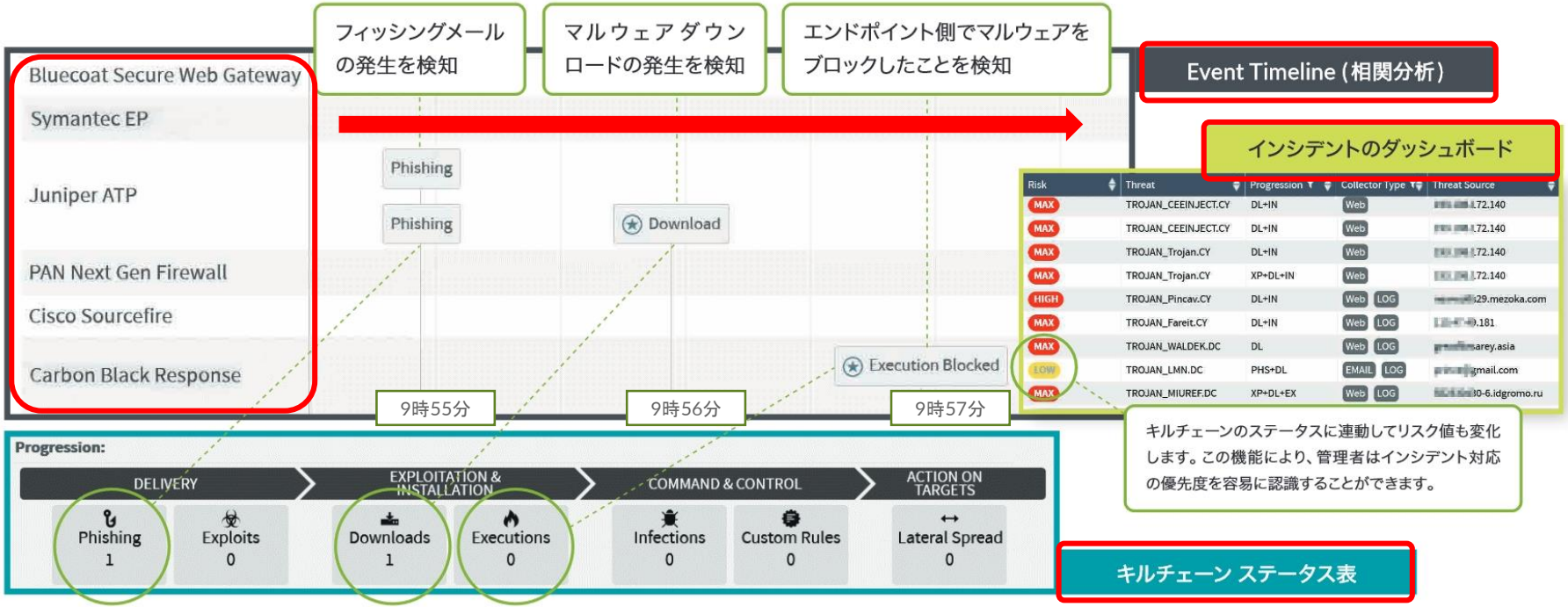
コネクテッドセキュリティ②
標的型攻撃の活動進行「キルチェーン」を可視化



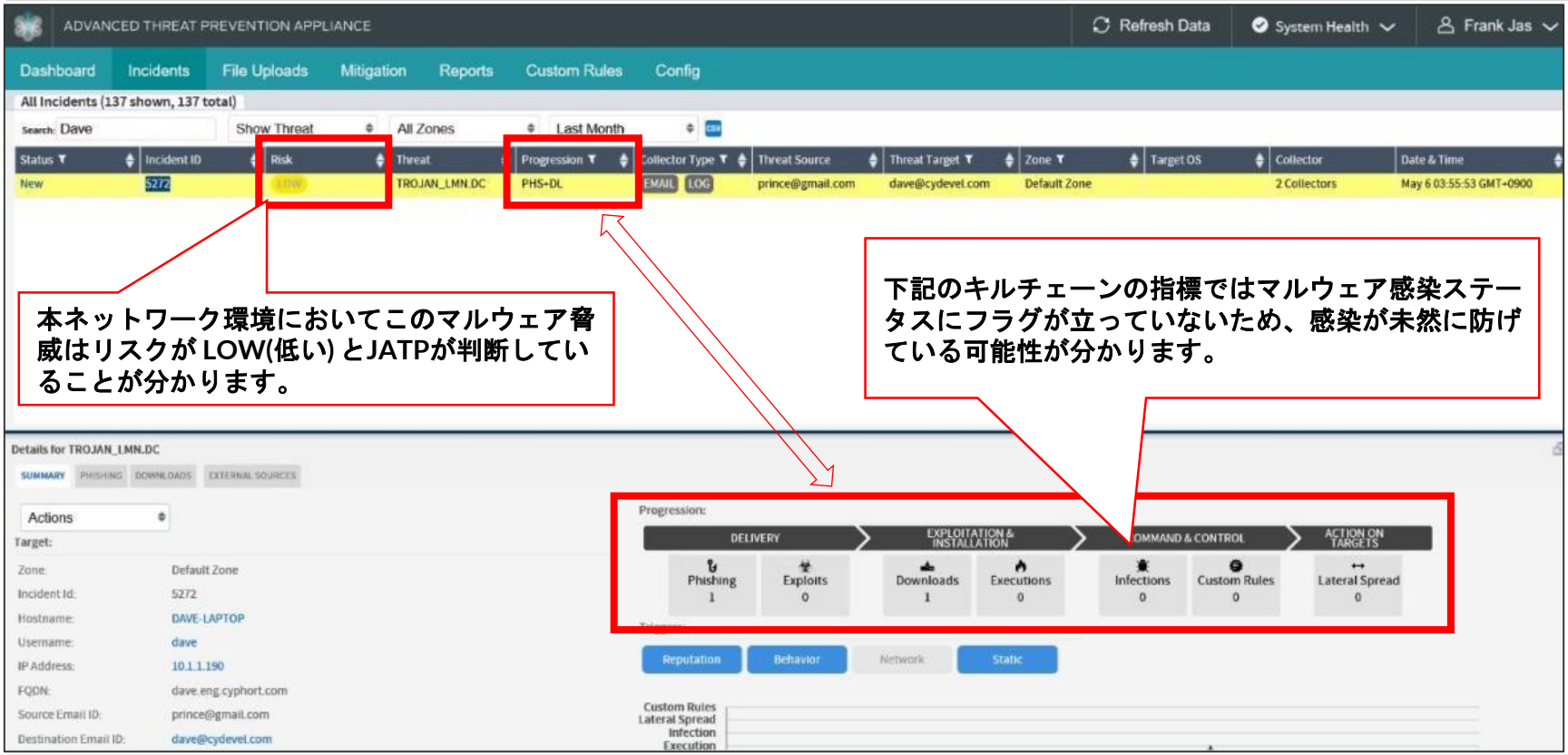


コネクテッドセキュリティ②
一つの画面から脅威の挙動分析と評価状況を可視化

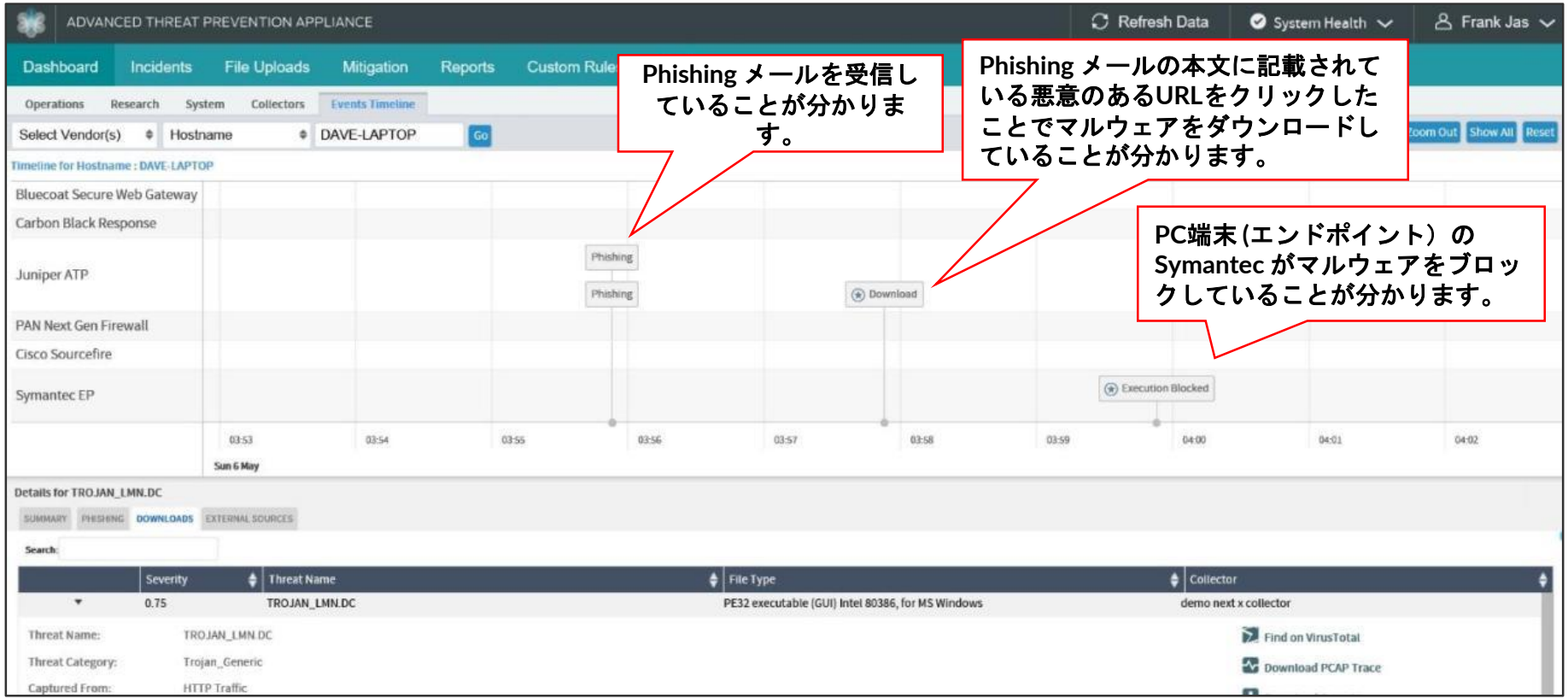
～「どのユーザ」が「いつ」「どういった脅威」に影響し、「どの製品」でアクションしたか、「時間軸」で可視化～



コネクテッドセキュリティ②
メールよりマルウェアをダウンロードさせられたケース

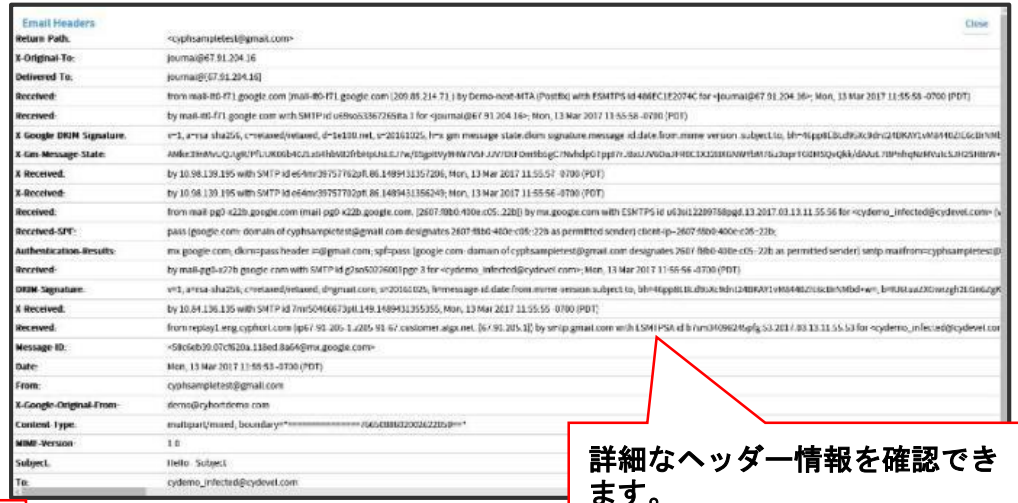


コネクテッドセキュリティ②
メールよりマルウェアをダウンロードさせられたケース



コネクテッドセキュリティ②
メールよりマルウェアをダウンロードさせられたケース

Phishing のタブをクリックするとメールの詳細情報が確認できます。



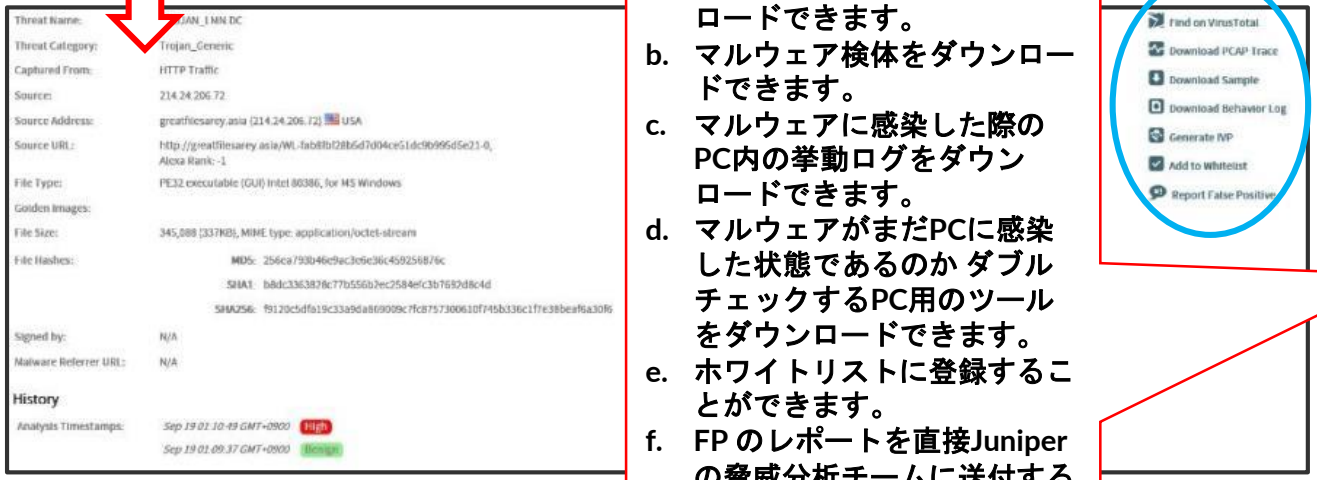
詳細なヘッダー情報を確認できます。

本文中に記載されている悪意のあるURLを確認できます。

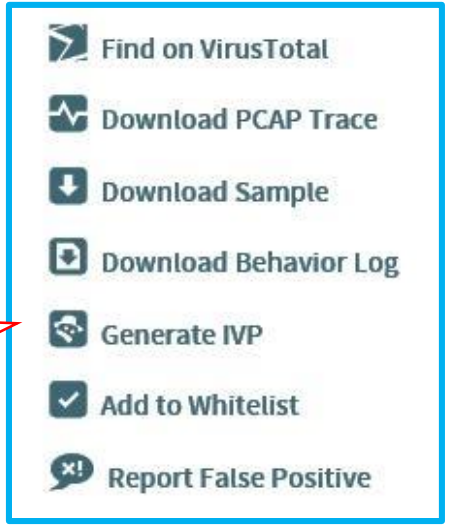
コネクテッドセキュリティ②
メールよりマルウェアをダウンロードさせられたケース

Download のタブをクリックするとマルウェアの詳細情報が確認できます。

Virus Total の情報もワンクリックで確認することが可能です。



a. マルウェアに感染した場合のインターネットへの通信挙動のPCAPファイルがダウンロードできます。
b. マルウェア検体をダウンロードできます。
c. マルウェアに感染した際のPC内の挙動ログをダウンロードできます。
d. マルウェアがまだPCに感染した状態であるのか ダブルチェックするPC用のツールをダウンロードできます。
e. ホワイトリストに登録することができます。
f. FP のレポートを直接Juniperの脅威分析チームに送付することができます。



コネクテッドセキュリティ②
メールよりマルウェアをダウンロードさせられたケース

External Source のタブをクリックするとSymantec のログ詳細情報が確認できます。

	Product	Host	Action	Response
▼	Symantec EP	10.1.1.190	Execution	Blocked

Response:	Blocked
Event Action:	Execution
Severity:	Low
Vendor Product:	Symantec EP
Category:	Trojan
File Name:	WL-fab8fbf28b5d7d04ce51dc9b995d5e21-0
File Hash:	256ea793b46e9ac3e6e36c459256876c
Device Host:	10.1.1.190
Signature:	Trojan.Gen
Raw Log:	2017-03-13 11:56:53-07,Virus found,IP Address: 10.1.1.190,Computer name: DAVE-LAPTOP,Source: Real Time Scan,Risk name::Trojan.Gen,Occurrences: 1,/Users/dave/Downloads/WL-fab8fbf28b5d7d04ce51dc9b995d5e21-0,Actual action: Deleted,Requested action: Deleted,Secondary action: Deleted,Event time: 2017-03-13 11:56:53-07 ,Inserted: 2017-03-13 11:57:53-07,End: 2017-03-13 11:57:53-07 ,Last update time: 2017-03-13 11:57:53-07,Domain: -,Group: -,Server: sepxxxxx,User: dave,Source computer: DAVE-LAPTOP,Source IP: 10.1.1.190,Disposition: Good,Download site: null,Web domain: null,Downloaded by: null,Prevalence: Reputation was not used in this detection.,Confidence: Reputation was not used in this detection.,URL Tracking Status: Off,,First Seen: Reputation was not used in this detection.,Sensitivity: Low,MDS,Application hash:256ea793b46e9ac3e6e36c459256876c ,Hash type: md5,Company name: HHHHH,Application name: ,Application version: ,Application type: -1,File size (bytes): 345088,Category set: Security risk,Category type: UNKNOWN

Symantec の実際のログを確認することができます。

コネクテッドセキュリティ②
自動化によるメリット

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

約30分の1

コネクテッドセキュリティ②
ICSA の最も厳しいテストにて高い検知率が証明済み

ICSA
国際コンピュータ
セキュリティ組合

検知率　　誤検知率

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

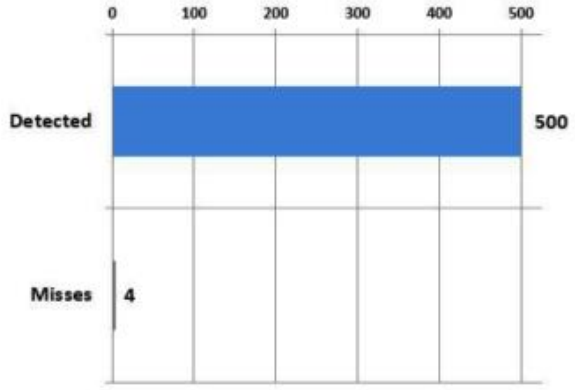


Fig. 2 – Detected 500 of 504 *New & Little-Known* Malicious Samples

6 FPs out of 555
Innocuous Apps

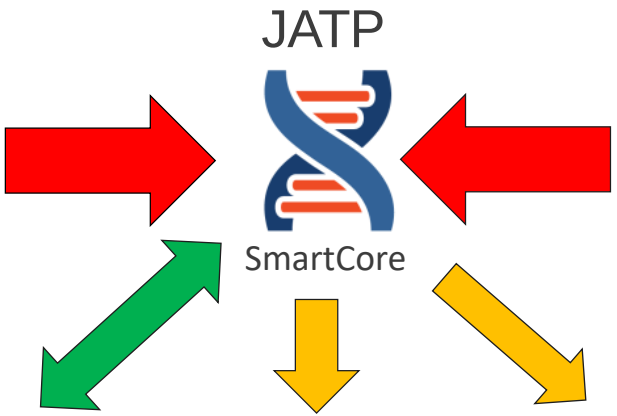
Fig. 3 – 6 Alerts on Innocuous Applications

コネクテッドセキュリティ②
JATP のセキュリティ連携

シスログ送信元

RFC3164 / 5424に準拠しているシスログであれば、

どのようなセキュリティ製品からでも受信が可能



Collector（通信モニタ）

SRX アプライアンス
vSRX 仮想アプライアンス
JATP700
JATP 仮想アプライアンス

API による連携

ForeScout
CROWDSTRIKE
netskope
Carbon Black.

NAC（端末隔離）連携

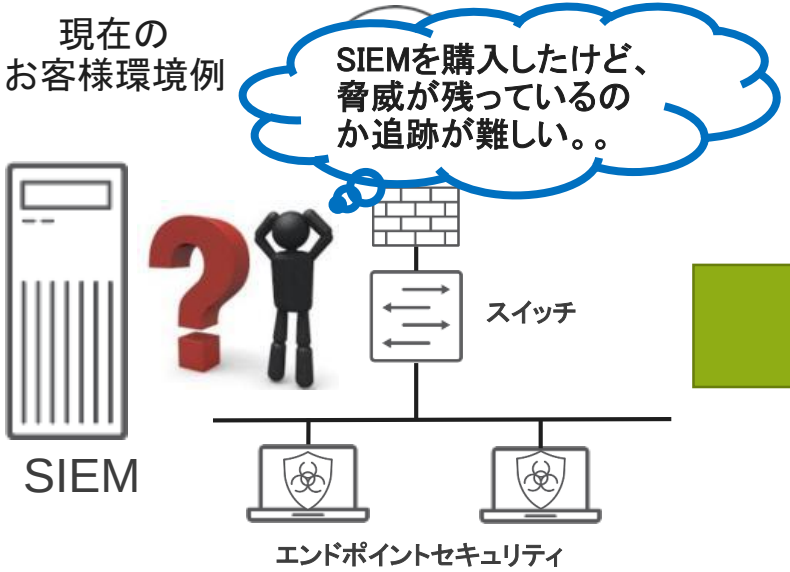
JUNIPER
Carbon Black.
ForeScout
aruba
a Hewlett Packard Enterprise company
PFU
a Fujitsu company
CROWDSTRIKE
CISCO

IOC（ブロックポリシ）適用可能

JUNIPER
BLUE COAT
paloalto NETWORKS
Carbon Black.
CISCO
CROWDSTRIKE
FORTINET
Check Point SOFTWARE TECHNOLOGIES LTD.

コネクテッドセキュリティ②
導入ケース：SIEMの代わりにキルチェーンを可視化

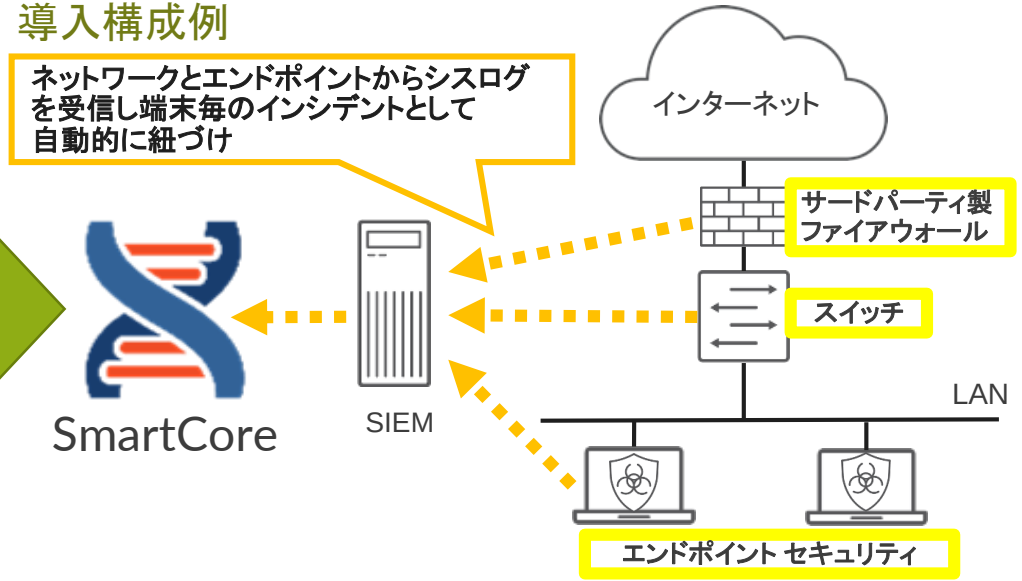
現在の
お客様環境例



お客様のご環境とニーズ

SIEMを購入したが使いこなすことが難しく、
最終的に脅威が残っているのかキルチェーンの
ステータスが可視化できていないので、
簡単に可視化できるソリューションが欲しい。

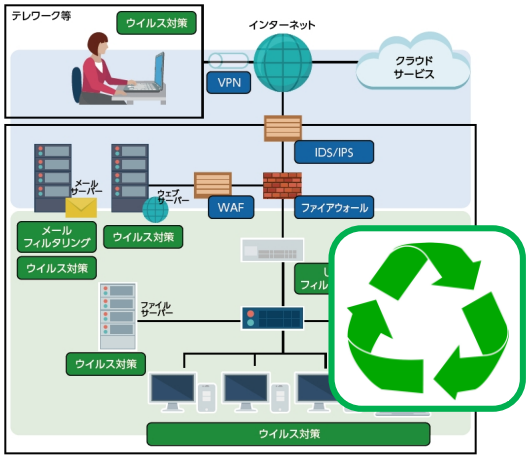
導入構成例



ご提案構成によるメリット

SIEMでシスログを集めてフィルターをかけた後に、
SIEMからJATPへシスログを飛ばして頂くことで、
簡単にキルチェーンのステータスが可視化できます。

コネクテッドセキュリティ②
多層防御の課題を解決（まとめ）



- マルチベンダーに対応した傾向分析と高精度な脅威解析
- 発生インシデントのキルチェインを可視化、即時の状況判断が可能
- 既存ソリューションとの連携を活した多層防御セキュリティソリューション

まとめ

なぜ、ジュニパーのセキュリティなのか？

ユーザの課題

セキュリティ担当者・
専任のセキュリティ技術者の不足

IoTやBYOD等の持ち込まれる脅威による
セキュリティリスクの高まり

多層防御、マルチベンダ環境における
セキュリティ管理負荷と対応に時間が掛かる

ジュニパーの提案

脅威検知および施行を自動化することで、
セキュリティ担当者のワークロードを軽減し、
迅速かつ正確に脅威への対処

ネットワーク全体で脅威を検知し、
エージェントレスで MACアドレスにより
感染デバイスを隔離

サードパーティ製品のログ分析、
および脅威を可視化することにより、
短時間で脅威の特定と対応が可能

ジュニパー
コネクテッドセキュリティ

セキュリティ脅威から、ユーザ、アプリケーション、およびインフラストラクチャを守る

脅威の可視化

タスクの自動化

検知および防御

ジュニパーは 「セキュリティを」「もっと簡単に」「つなげます」。

ネットワーク全体にセキュリティを拡張！！

「コネクテッド セキュリティ」

見る
ネットワーク全体の可視化

知る
対処方法を的確に判断

実行する
ネットワークを守る

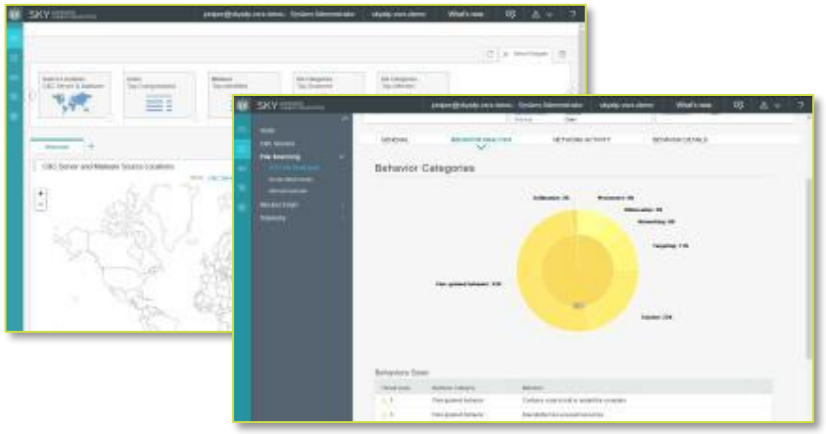
おまけ:

簡単に試せる ジュニパー コネクテッドセキュリティ

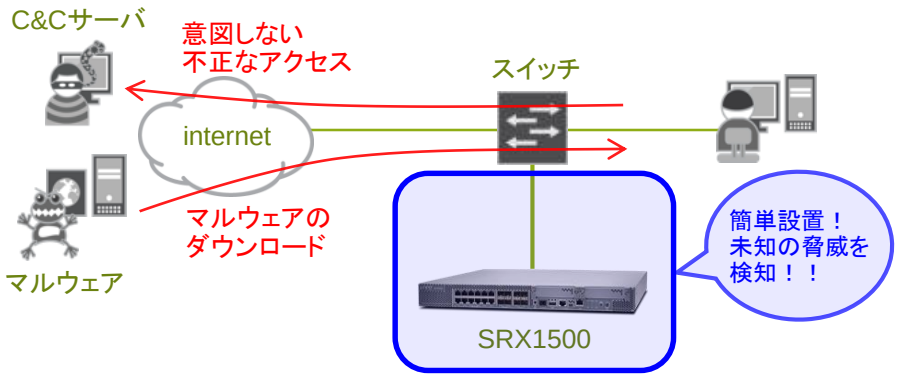
SKY ATP（ジュニパー コネクテッドセキュリティ）

Sky ATP監視モードで試してみませんか

- SRXをスイッチに接続するだけ
- 既存構成への影響なし



モニタリング画面



ご利用時の構成イメージ

JATP 無料トライアル

JATP Trial（14日間無料）
https://www.juniper.net/us/en/forms/jatp-14-day-trial/


THANK YOU
JUNIPER NETWORKS
Engineering
Simplicity
現場担当者向けセキュリティ資料まとめサイト
https://www.juniper.net/jp/jp/dm/security/