

# 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

JUNIPER  
NETWORKS®

セキュリティを  
もっと簡単に  
つなげる。

サイバーセキュリティ脅威の傾向と企業IT担当者の課題

ジュニパーネットワークスのセキュリティに対する取り組み

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

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

まとめ



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

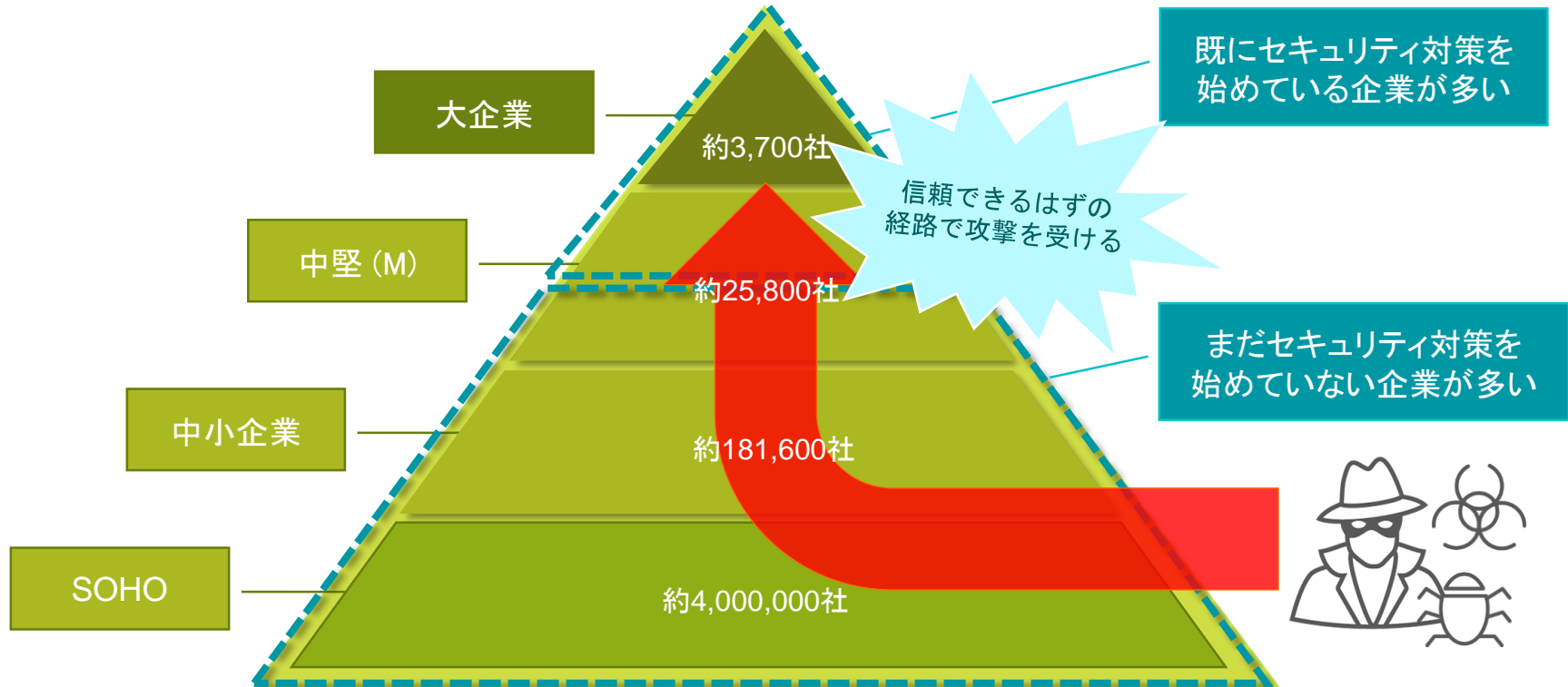
標的型攻撃

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>

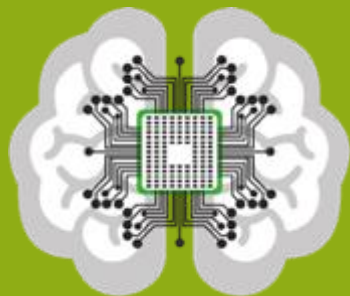
# サプライチェーン攻撃



# 人工知能（AI）使いこなすには . . .

## ARTIFICIAL INTELLIGENCE

Human intelligence exhibited by machines



## MACHINE LEARNING

Using algorithms to parse data, learn and predict

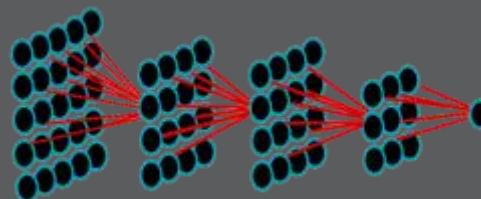
```
100110110100110011  
1011010010010001101  
1100110010100001100  
0101000011011110110  
111110001001010110
```



ATP  
高度な脅威対策  
セキュリティインテリジェンス

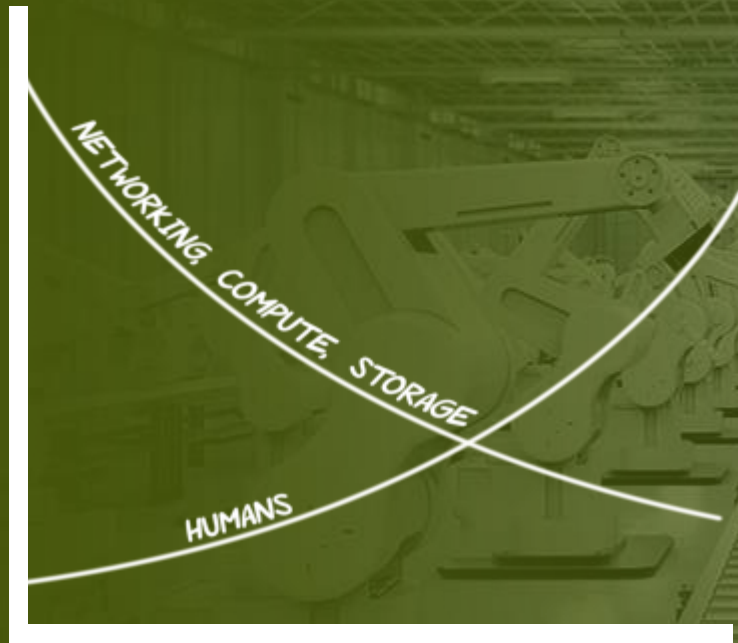
## DEEP LEARNING

Utilizing multiple layers of neurons



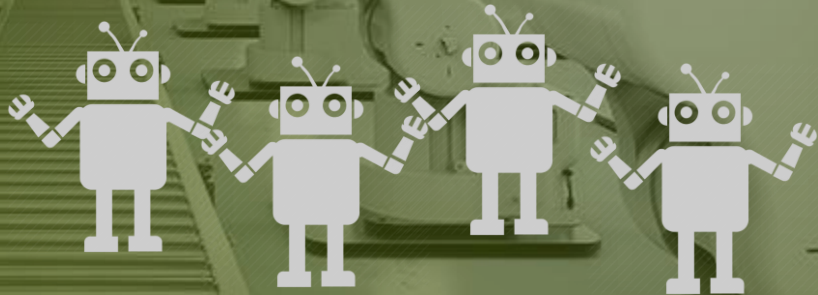
# 自動化 – セキュリティのためのキラーアプリ

ユニット当りのコスト



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



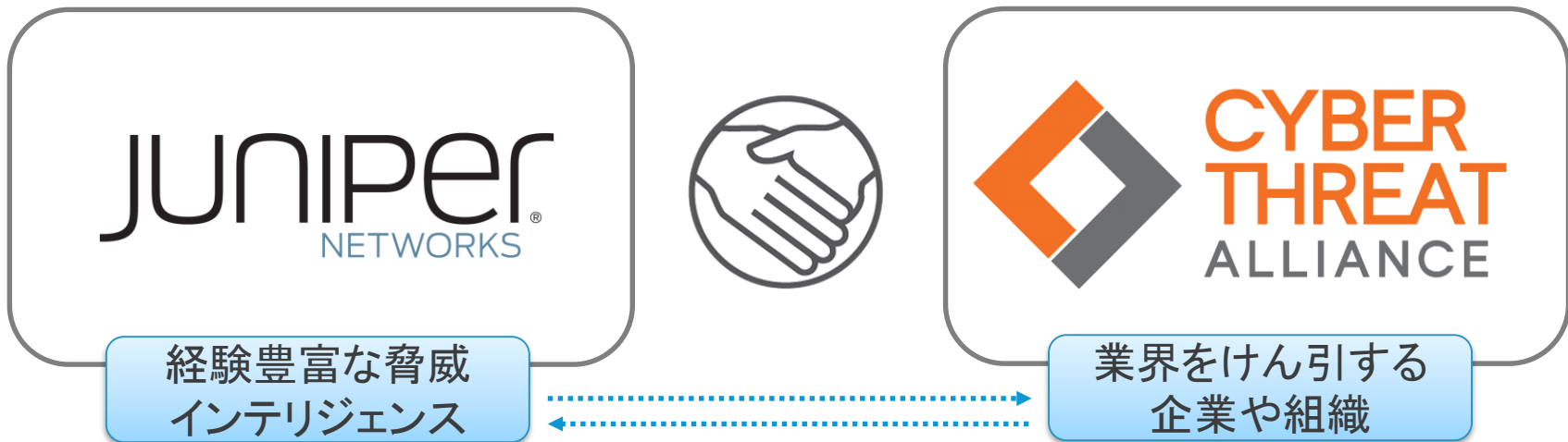


# ジュニパー ネットワークス セキュリティに対する取り組み

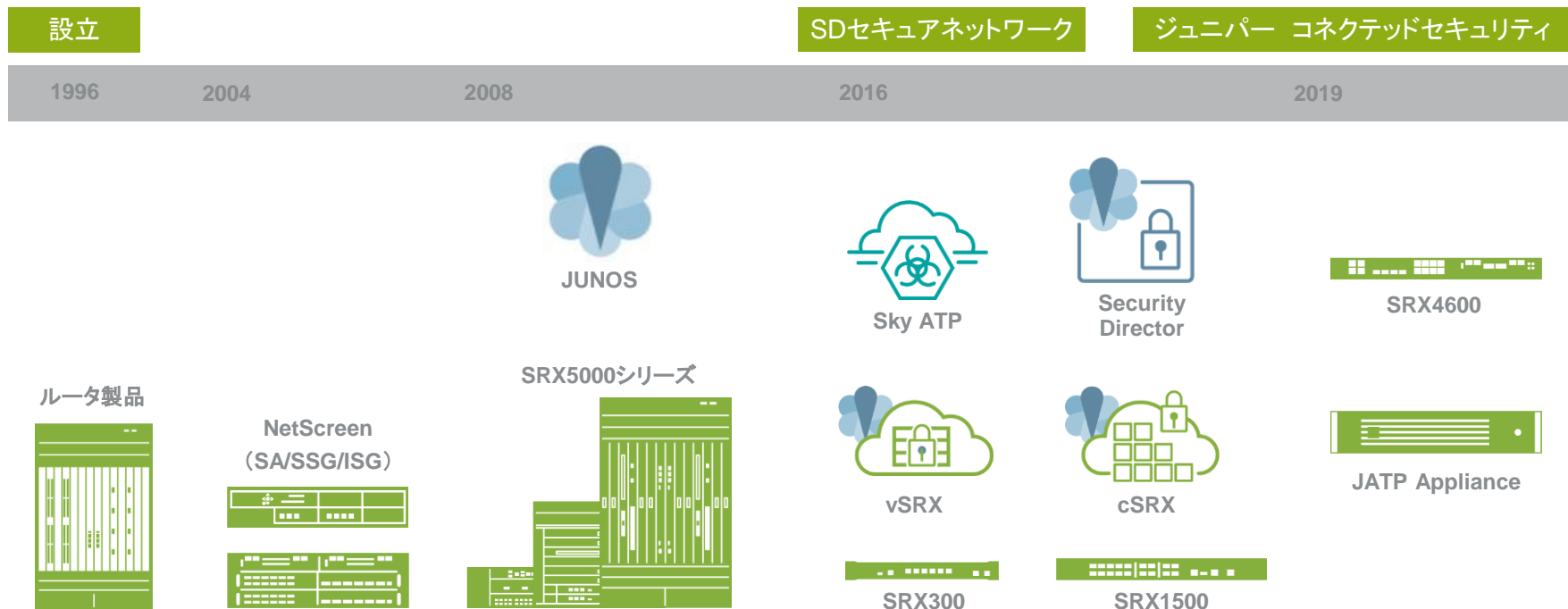
# CTA (Cyber Threat Alliance) のメンバーとして活動

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



# 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>

see what is happening ...

見る

know what to do ...

知る

and, you have to do it ...

実行する



## ジュニパーの「コネクテッドセキュリティ」

ネットワーク全体をつなげて、すべてを「可視化」

情報を「分析」し、対応を的確に判断、

問題の「対処」に移す「つながるセキュリティ」

セキュリティ人材不足 ✓

脅威の多層化 ✓

自動化の活用 ✓



## 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



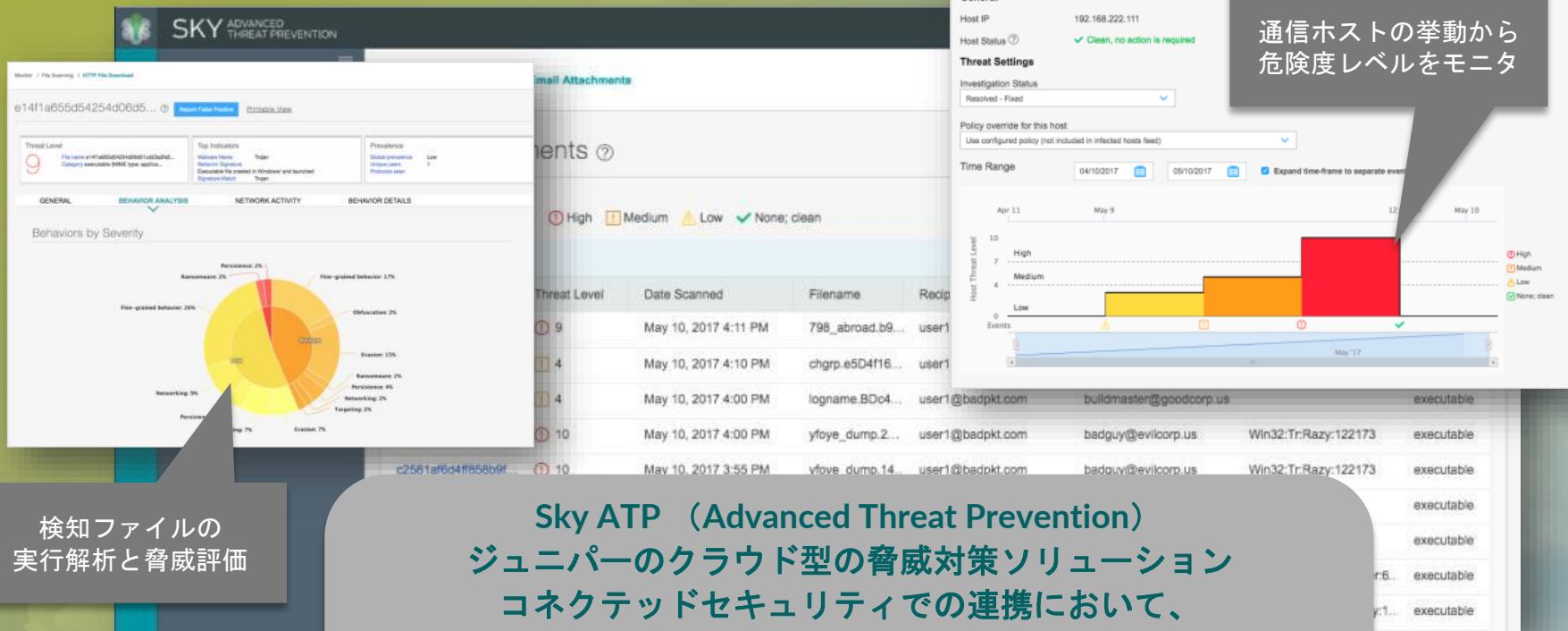
- 感染ホストの自動隔離
- ワンタッチのリスク軽減
- サードパーティ連携

## 対処

## 防衛

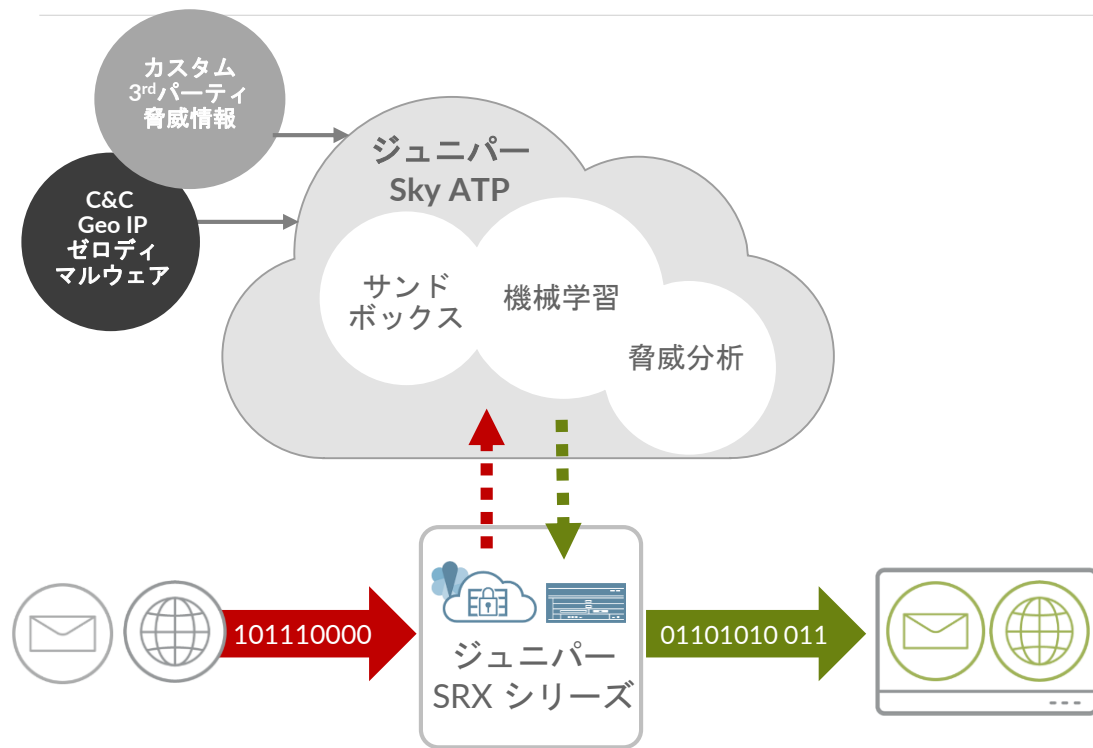


# Sky ATP による高度な脅威対策



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

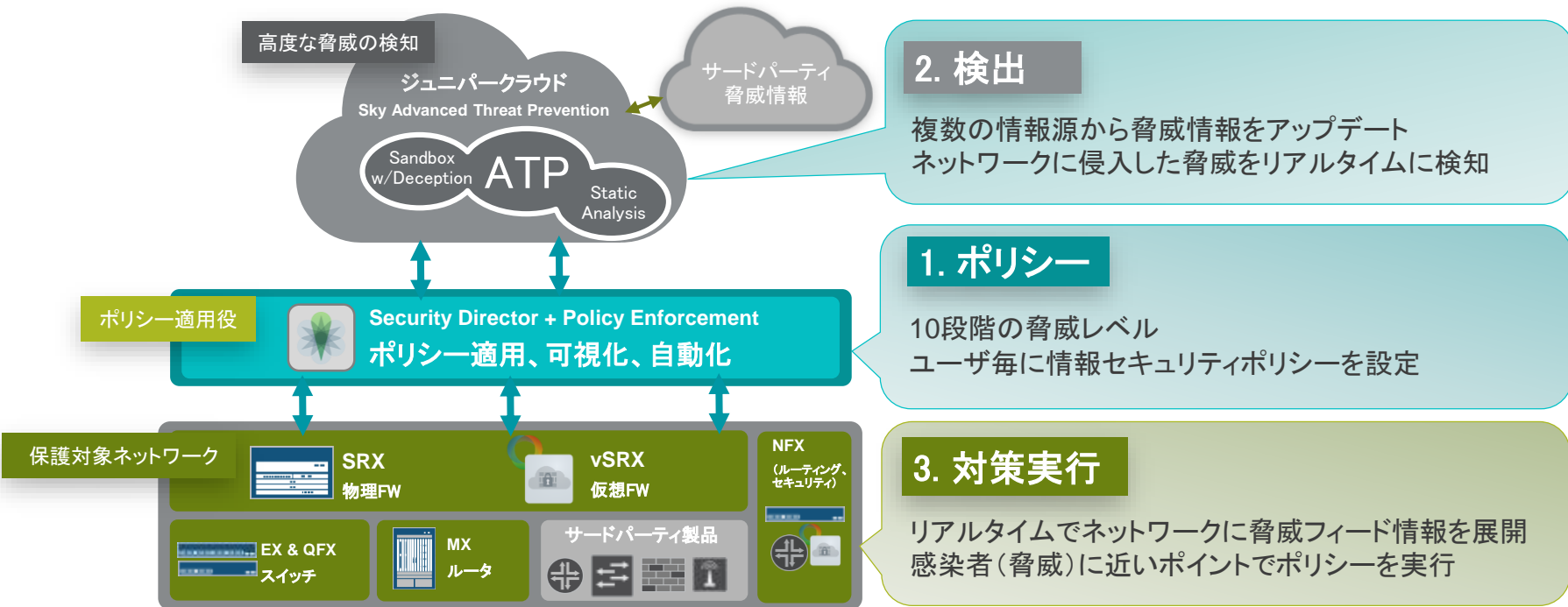
# コネクテッドセキュリティ①： Sky ATP の主要な機能



- 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

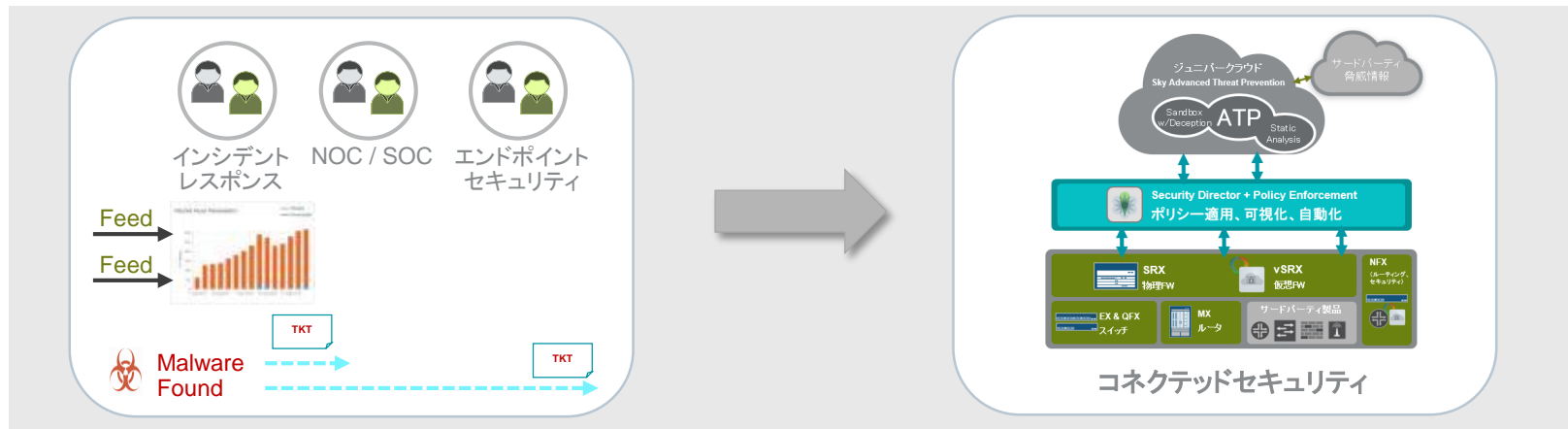


それぞれのネットワーク機器にてポリシーを適用、ネットワーク全体を単一の対策実行ドメインに！

# 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)

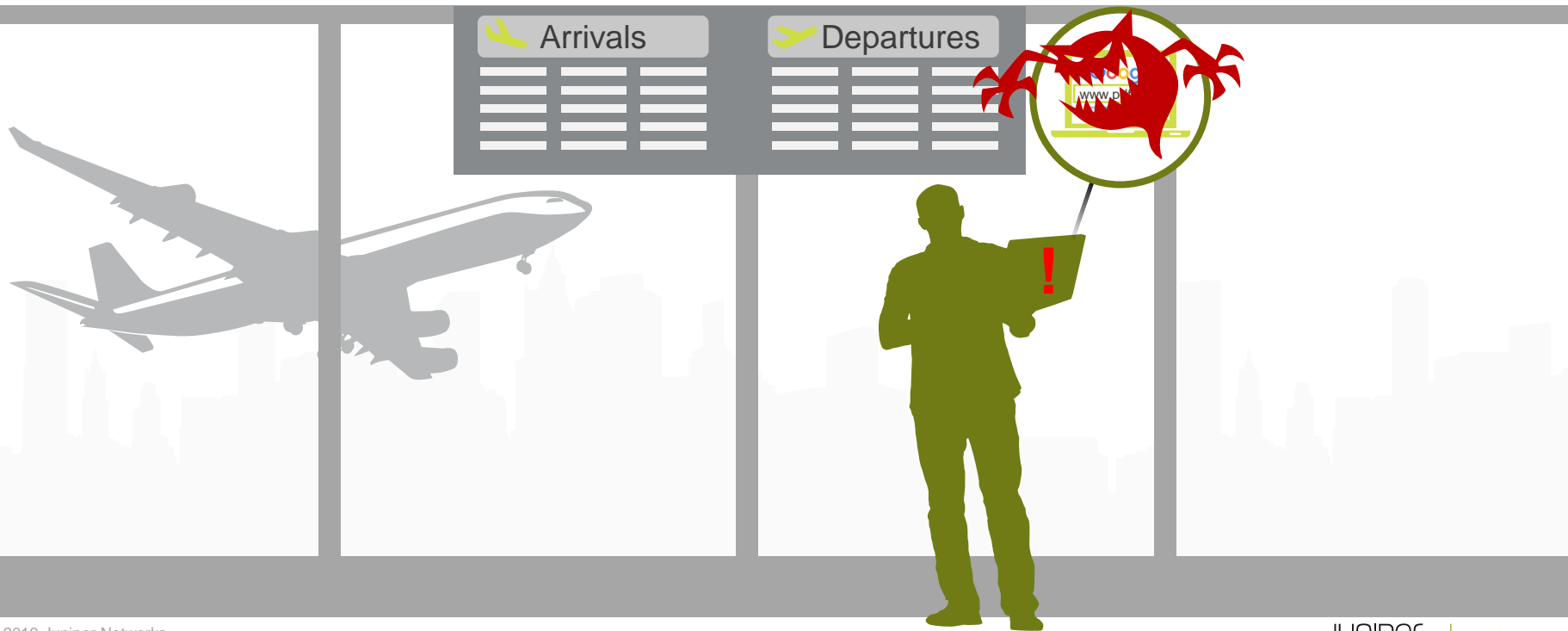
## 脅威を自動的に検知・排除



脅威の検知から、対応・防止策までを自動化

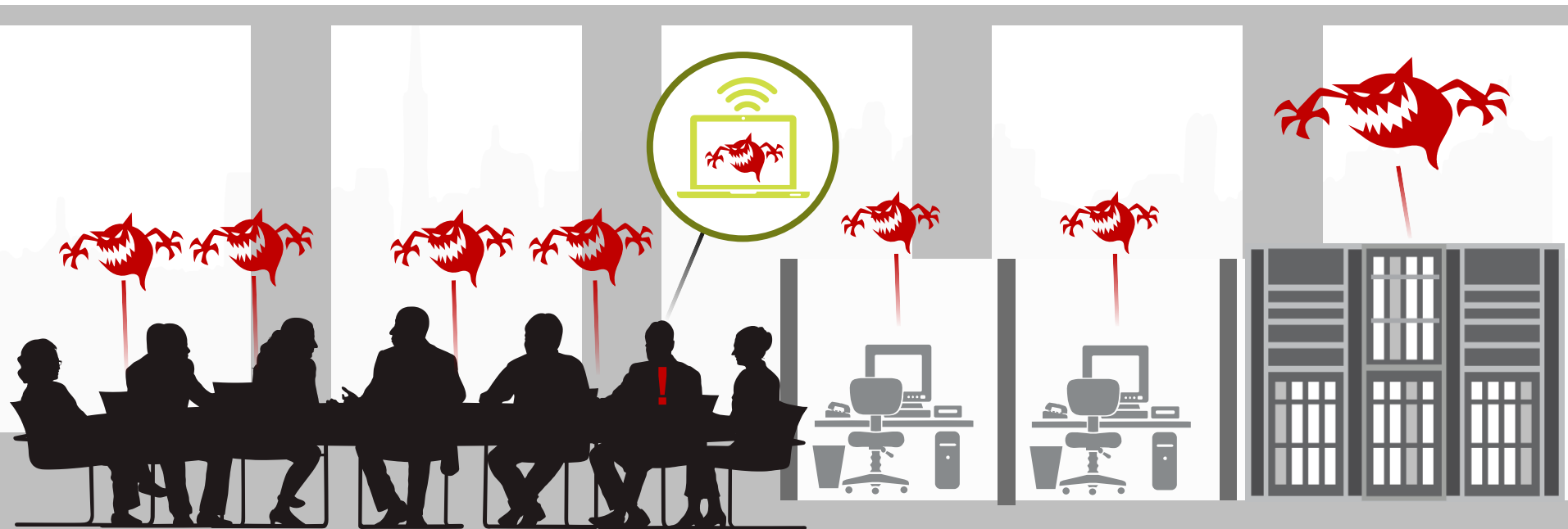
# 標的型攻撃の罠は、あらゆる場面に存在する！

出先でのちょっとした作業で、意図しない感染に遭遇

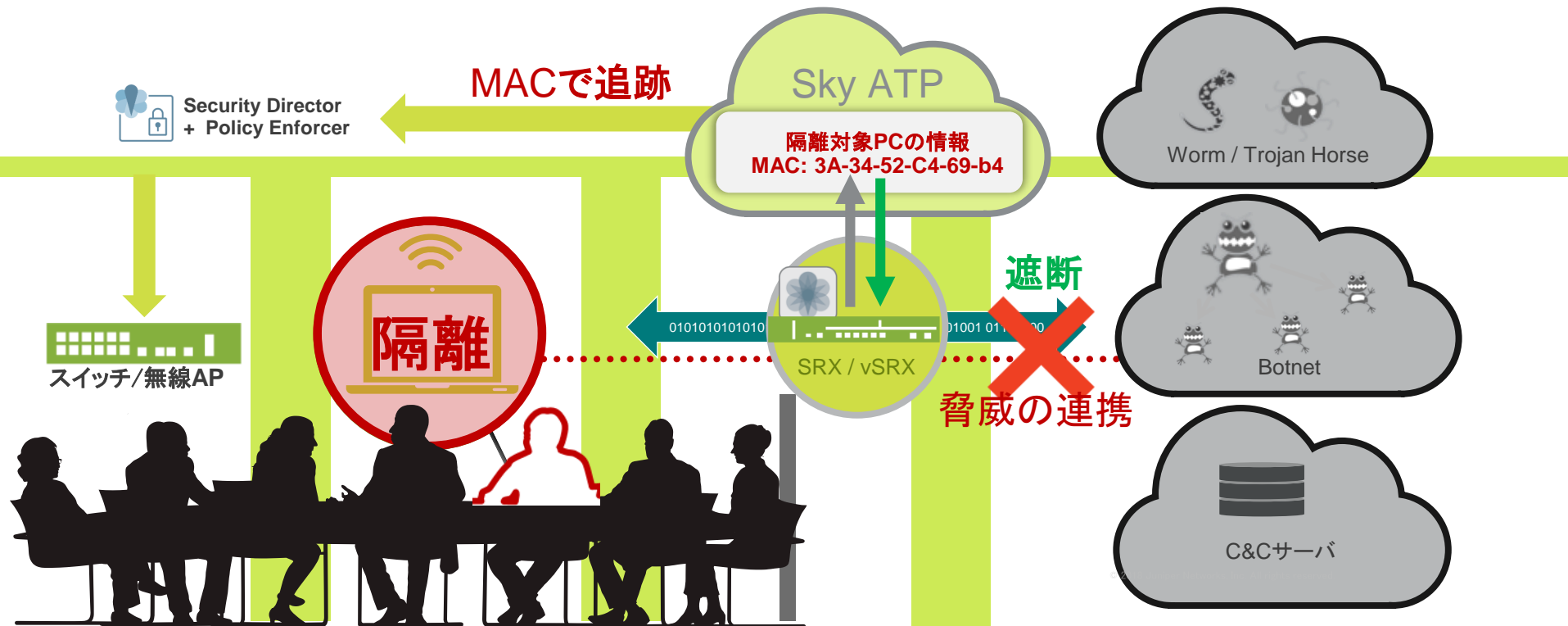


# 感染拡大はあっという間！！

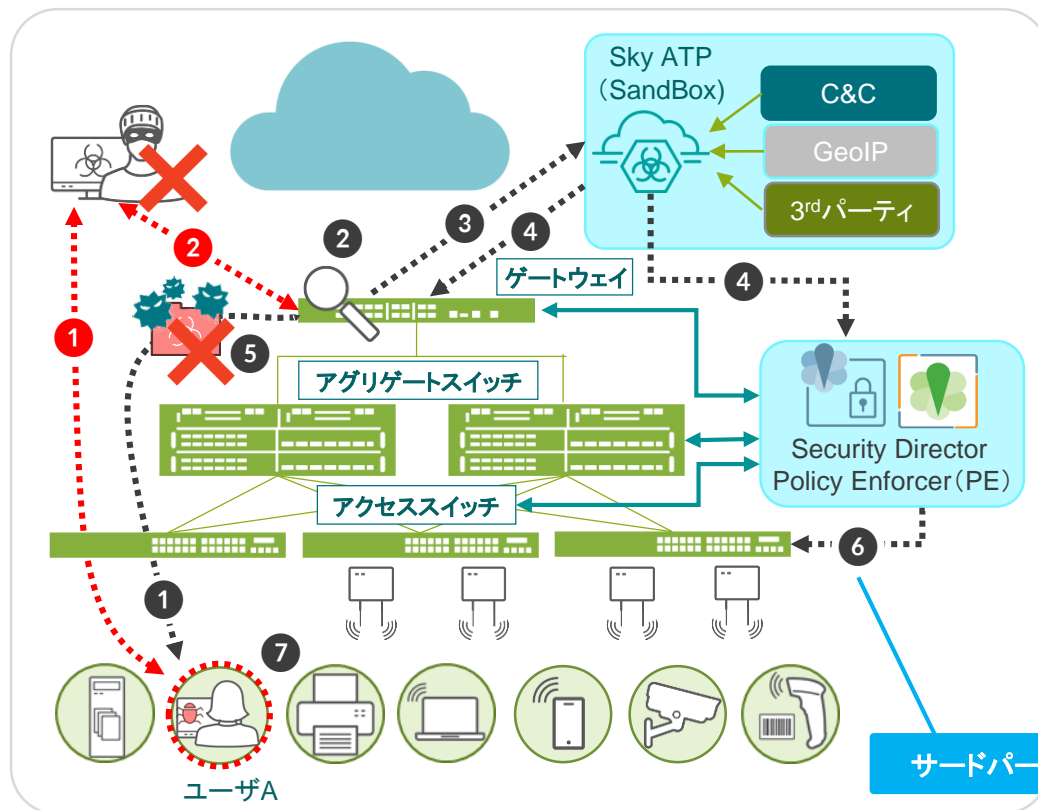
ネットワーク内部からの攻撃は簡単に甚大な被害へとつながる



# 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)

- ① ユーザーAはファイルをダウンロード
- ② SRXは対象ファイルをスキャン
- ③ SRXはファイルをSky ATPへ送信
- ④ Sky ATPはファイルのマルウェアを特定し、SRXとPEに通知
- ⑤ SRXはファイルのダウンロードをブロック
- ⑥ PEはユーザーA端末を隔離
- ⑦ 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)

- ① 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
- ② 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などの連携も可能



# 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

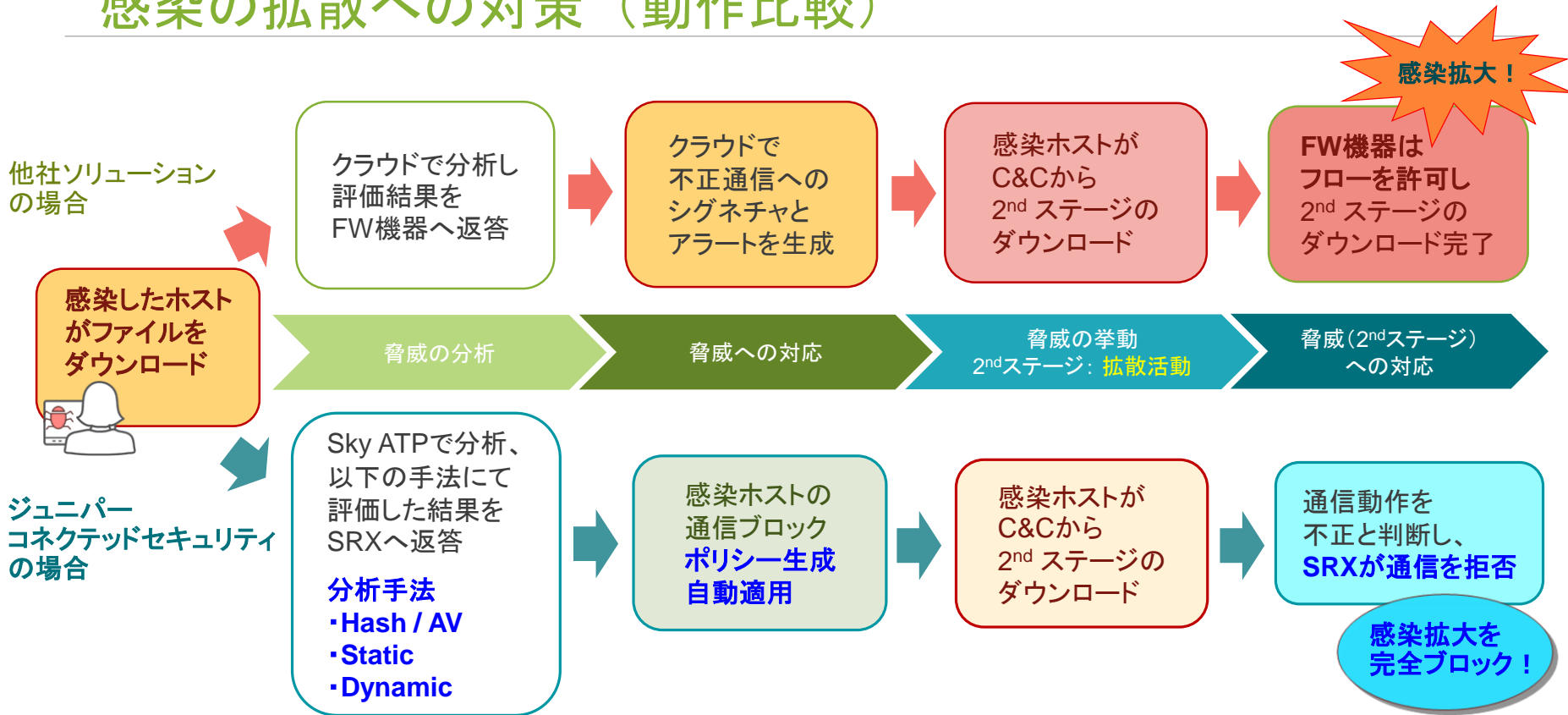
## クラウドとの連携

- 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

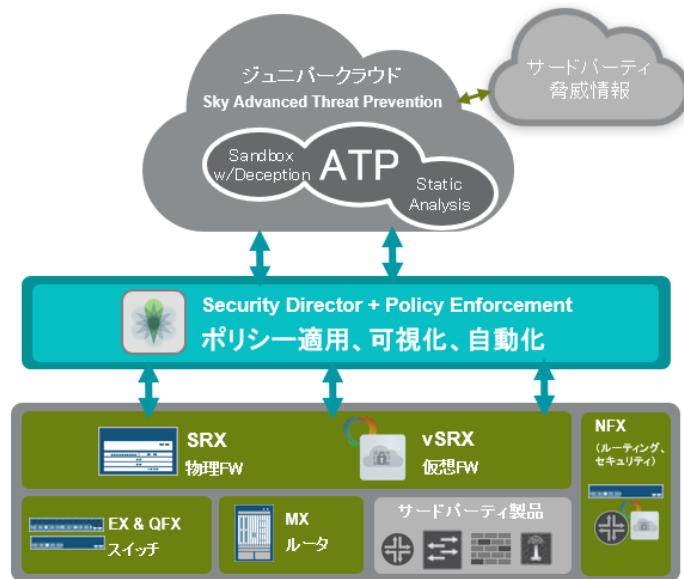
- ネットワーク内部に侵入した脅威を自動的に特定
- 事前に定義したポリシーに基づいて、自動的に脅威を排除

# 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）



# 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



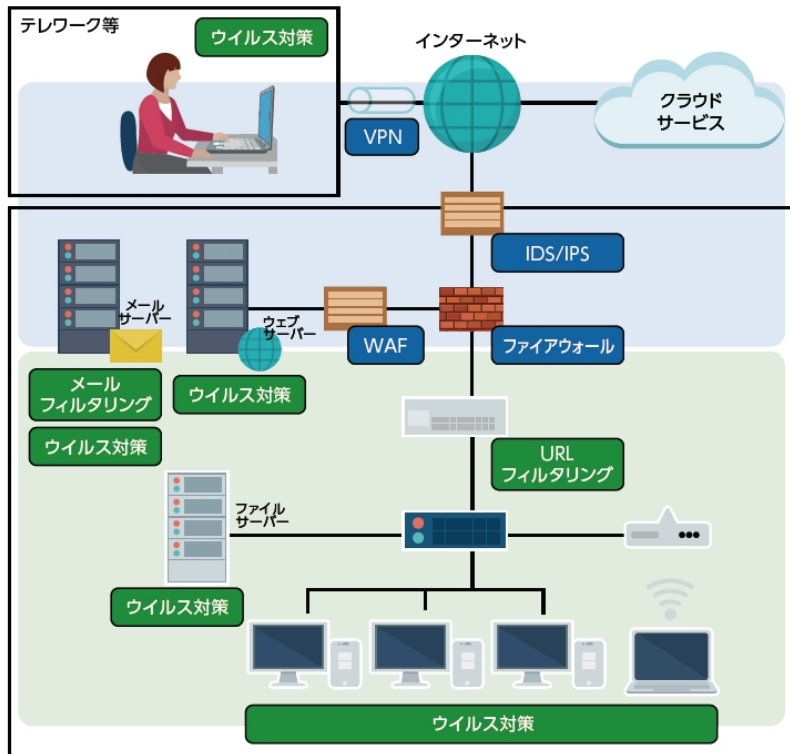
自動化を最大限に利用して、セキュリティ運用の負荷を大幅削減



## 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 によるネットワークの自動防衛



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 (オブジェクトのデテネーション) <sup>1</sup>	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 (オブジェクトのデテネーション) <sup>1</sup>	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

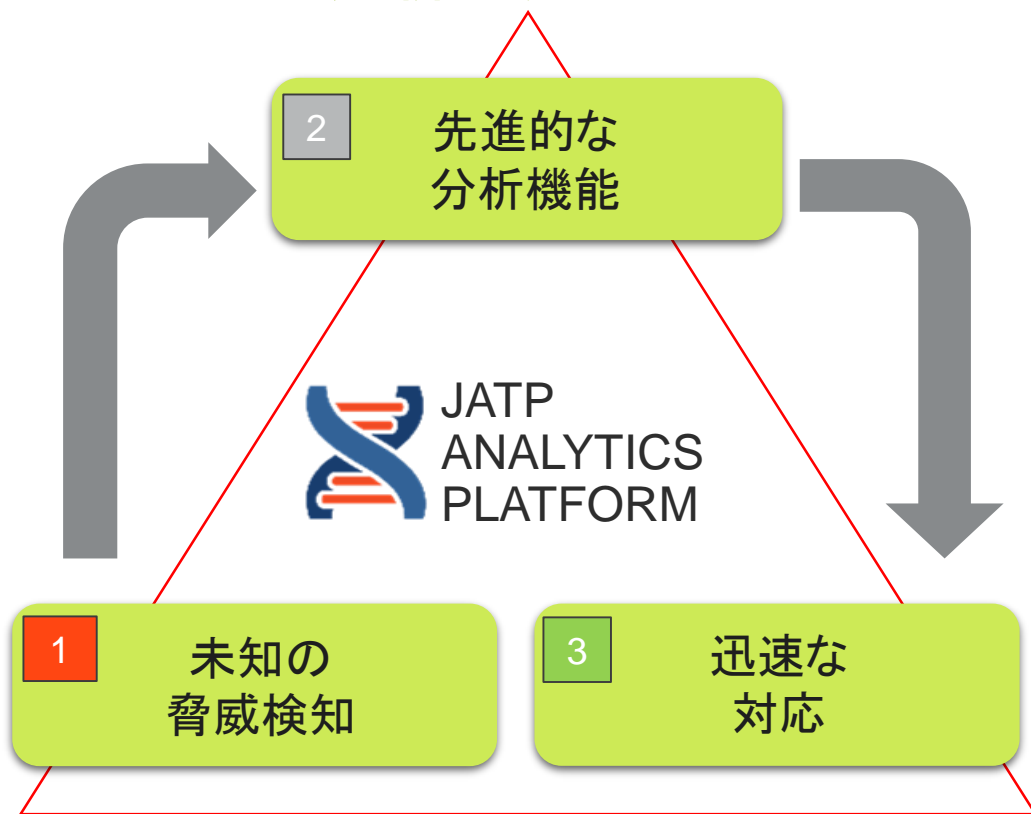
## 電子メール MTA レシーバー

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

ふるまい検知

静的検知

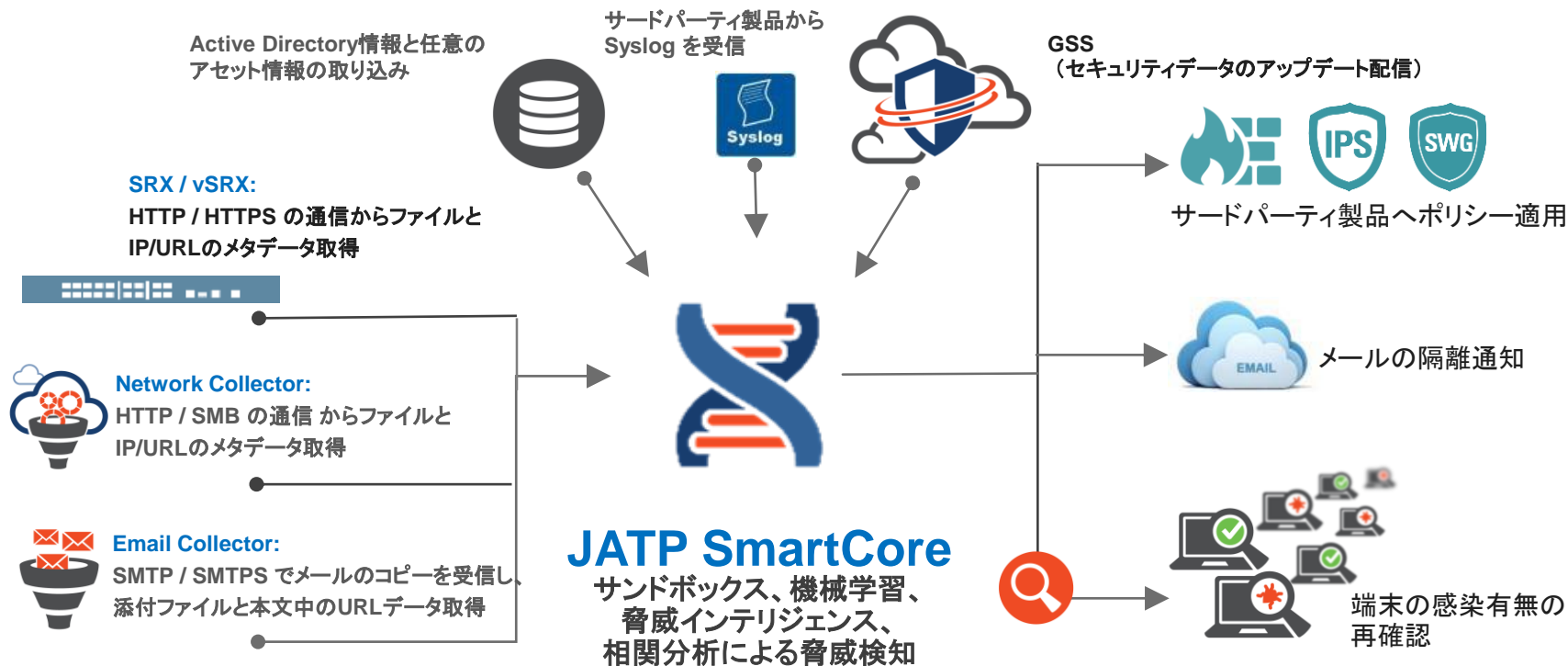
レピュテーション情報

機械学習エンジン

検知、分類、リスク評価

# コネクテッドセキュリティ②

## JATP 防衛連携の流れ



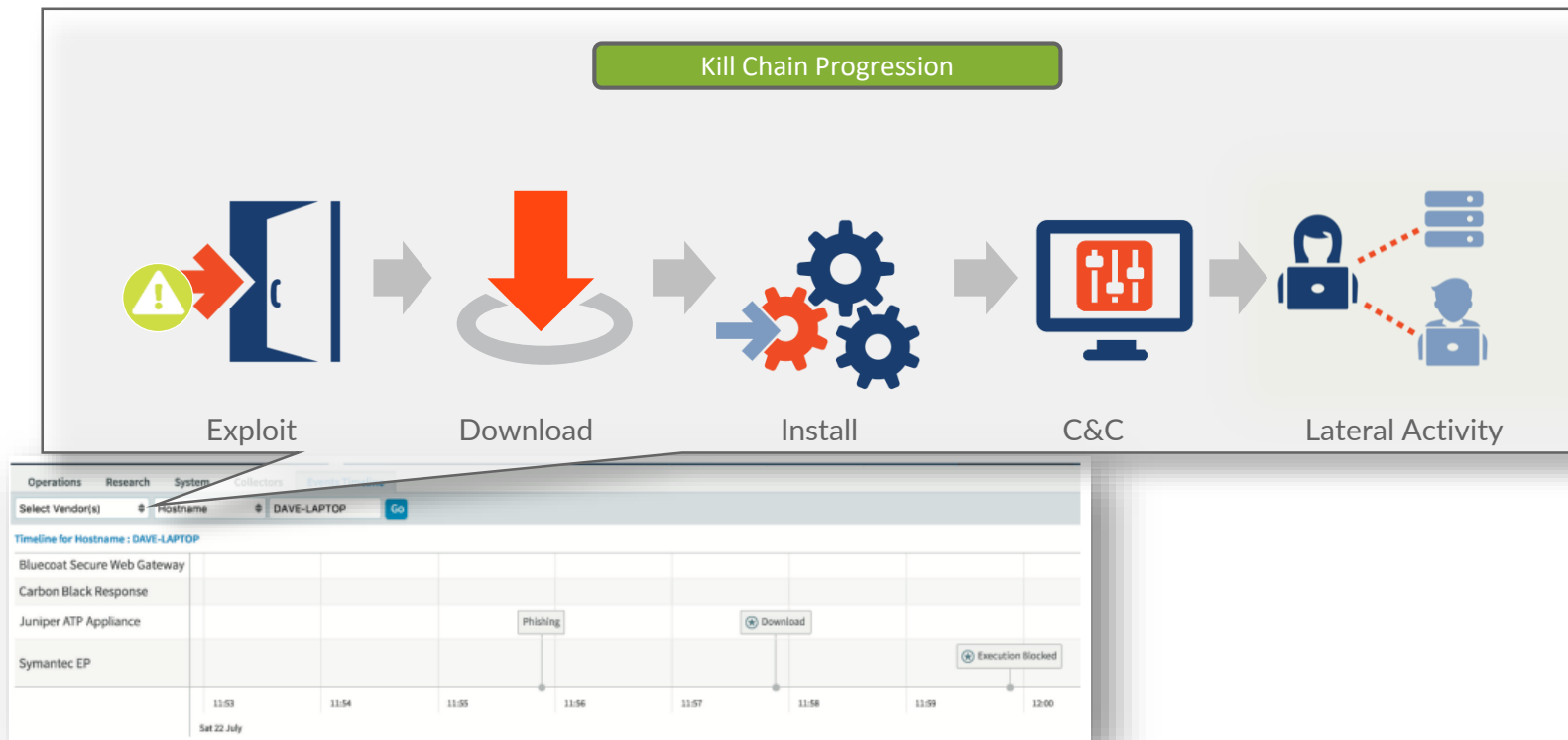
未知の脅威検知

先進的な分析

迅速な対応

## コネクテッドセキュリティ②

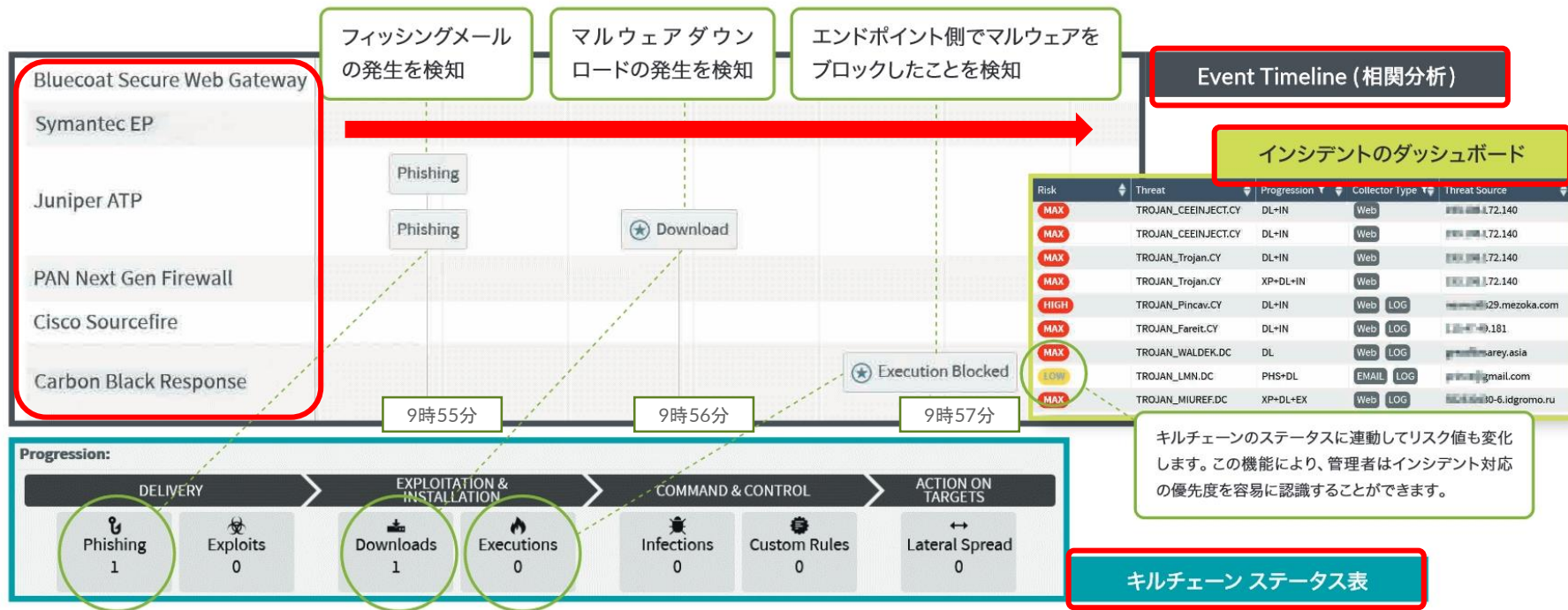
# 標的型攻撃の活動進行「キルチェーン」を可視化



## 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

The screenshot displays the Juniper Advanced Threat Prevention Appliance interface. At the top, there are navigation tabs: Dashboard, Incidents, File Uploads, Mitigation, Reports, Custom Rules, and Config. Below this, a table lists incidents. One incident is highlighted in yellow with the following details:

Status	Incident ID	Risk	Threat	Progression	Collector Type	Threat Source	Threat Target	Zone	Target OS	Collector	Date & Time
New	5272	LOW	TROJAN_LMN.DC	PHS-DL	EMAIL LOG	prince@gmail.com	dave@cydevel.com	Default Zone		2 Collectors	May 6 03:55:53 GMT-0900

Below the table, the 'Details for TROJAN\_LMN.DC' section is visible. It includes a 'SUMMARY' tab and an 'Actions' dropdown. The 'Progression' section shows a flowchart with the following stages and counts:

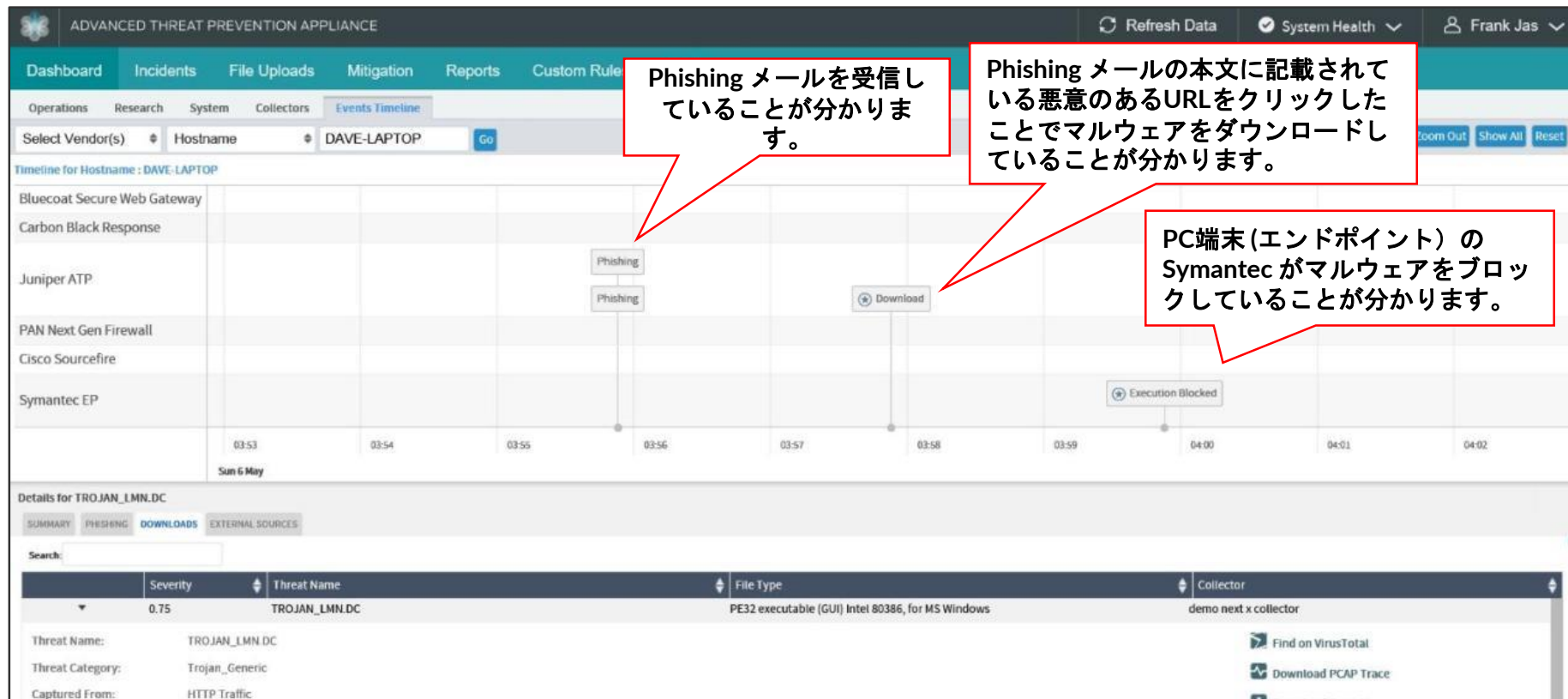
Stage	Count
DELIVERY (Phishing)	1
EXPLOITATION & INSTALLATION (Exploits)	0
EXPLOITATION & INSTALLATION (Downloads)	1
EXPLOITATION & INSTALLATION (Executions)	0
COMMAND & CONTROL (Infections)	0
COMMAND & CONTROL (Custom Rules)	0
ACTION ON TARGETS (Lateral Spread)	0

Two red callout boxes provide additional context:

- The first callout points to the 'Risk' and 'Progression' columns in the incident table, stating: "本ネットワーク環境においてこのマルウェア脅威はリスクがLOW(低い)とJATPが判断していることが分かります。" (In this network environment, it is known that the risk of this malware threat is LOW (low) and JATP has judged it.)
- The second callout points to the 'Progression' bar, stating: "下記のキルチェーンの指標ではマルウェア感染ステータスにフラグが立っていないため、感染が未然に防げている可能性があります。" (Since the indicators in the kill chain below do not have a flag for malware infection status, there is a possibility that infection has been prevented.)

## 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 メールを受信していることがわかります。

Phishing メールの本文に記載されている悪意のあるURLをクリックしたことでマルウェアをダウンロードしていることがわかります。

PC端末(エンドポイント)のSymantecがマルウェアをブロックしていることがわかります。

## 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

Bluecoat Secure Web Gateway  
Carbon Black Response  
Juniper ATP  
PAN Next Gen Firewall  
Cisco Sourcefire  
Symantec EP

Phishing

Details for TROJAN\_LMN.DC

PHISHING

SUNRISE

Sun 6 May

03:53 03:54 03:55 03:56

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。

Email Headers

Return Path: <cyphsamplest@gmail.com>

X-Original-To: journal@67.91.204.16

Delivered To: journal@67.91.204.16

Received: from mail-06-f71.google.com [mail-06-f71.google.com [209.85.214.71]] by Demo-ncw-MTA [Postfix with ESMTPS id 408FC1E2074C for <journal@67.91.204.16>; Mon, 13 Mar 2017 11:55:58 -0700 (PDT)] by mail-06-f71.google.com with SMTP id u58o53367265ita.1 for <journal@67.91.204.16>; Mon, 13 Mar 2017 11:55:58 -0700 (PDT)

X-Google-DRM-Signature: v=1, a=rsa-sha256, c=relaxed/relaxed, d=131101.mtl, m=20151025, l=rs-gm message state.drm.signature.message.id.date.from.name.version.subject.to, bh=76ppkL3uJ93k30hC210KAY1M3H1E6C6G2bY9M...

X-Gm-Message-State: ANkE3mavUjQgP1U000b4C2s4t6W4Zf6p3u3U7w7g9tYv8v8V8AAV7Df3Ost6gC:rwbdp01ppn.3du.AV0a.HFEC.XK23818WV8t816.zapF0G85SQ+QkA/GAAU.78Pshgufv6v5.S.8Z58H8v...

X-Received: by 10.98.139.195 with SMTP id e64mz39757192pr.86.1489431356249; Mon, 13 Mar 2017 11:55:57 -0700 (PDT)

X-Received: by 10.98.139.195 with SMTP id e64mz39757192pr.86.1489431356249; Mon, 13 Mar 2017 11:55:56 -0700 (PDT)

Received: from mail-pg0-k22b.google.com [mail-pg0-k22b.google.com [2607.880.400e.cts-22b]] by mx.google.com with ESMTPS id u63612289180ppl.13.2017.03.13.11.55.56 for <cydemo\_inlc.ed@cydevet.com> (a-pass [google.com: domain of cyphsamplest@gmail.com designates 2607.880.400e.cts-22b as permitted sender] client-ip=2607.880.400e.cts-22b; authentication-results=mx.google.com; dkim-pass header =; spf-pass [google.com: domain of cyphsamplest@gmail.com designates 2607.880.400e.cts-22b as permitted sender] smtp-mailfrom=cyphsamplest@gmail.com; dmarc-pass [google.com: domain of cyphsamplest@gmail.com designates 2607.880.400e.cts-22b as permitted sender] smtp-mailfrom=cyphsamplest@gmail.com); Mon, 13 Mar 2017 11:55:58 -0700 (PDT)

DRM-Signature: v=1, a=rsa-sha256, c=relaxed/relaxed, d=gmail.com, m=20151025, l=rs-gm message id.date.from.name.version.subject.to, bh=76ppkL3uJ93k30hC210KAY1M3H1E6C6G2bY9M...

X-Received: by 10.84.136.135 with SMTP id 7m5C406673JhL149.148943135355; Mon, 13 Mar 2017 11:55:55 -0700 (PDT)

Received: from reply1.erg.cyphost.com [ip6:91:400:1:2205:91:67:customer.alpha.net. [67.91.205.11]] by smtp.gmail.com with ESMTPSA id b1m30306256p.53.2017.03.13.11.55.53 for <cydemo\_inlc.ed@cydevet.com>

Message-ID: <58c6eb39.07cf620a.118ed.8a64@gmail.com>

Date: Mon, 13 Mar 2017 11:55:53 -0700 (PDT)

From: cyphsamplest@gmail.com

X-Google-Original-From: demo@cyphostdemo.com

Content-Type: multipart/mixed; boundary="\*\*\*\*\*0606088020042215@\*\*\*\*\*"

MIME-Version: 1.0

Subject: Hello Subject

To: cydemo\_inlc.ed@cydevet.com

詳細なヘッダー情報を確認できます。

Details for TROJAN\_LMN.DC

SUMMARY PHISHING DOWNLOADS EXT

Severity	File ID	URLs
0.75	58c6eb39.07cf620a.118ed.8a64@gmail.com	http://greatfilesarry.asia/WL-fab8fbf28b5d7d04ce51dc9b995d5e21-0

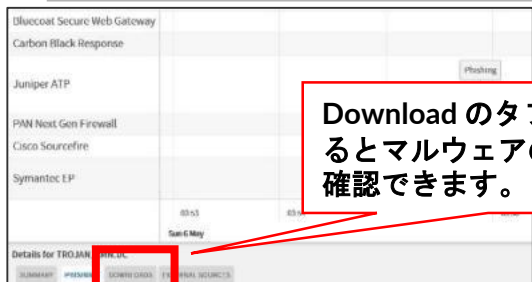
URLs

URL	Description	Actions
http://greatfilesarry.asia/WL-fab8fbf28b5d7d04ce51dc9b995d5e21-0	Downloads Sha1: b8dc3363828c77b5556b2ec2584efc3b7692d8c4d	Report False Positive Add to Whitelist

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

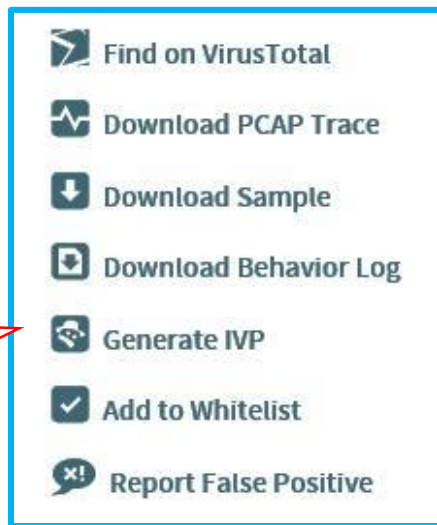
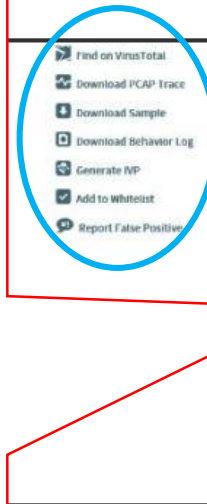


Download のタブをクリックするとマルウェアの詳細情報が確認できます。

Virus Total の情報もワンクリックで確認することが可能です。



- 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。
- マルウェア検体をダウンロードできます。
- 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。
- 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。
- ホワイトリストに登録することができます。
- 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。

Vendor 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: sepxxxx,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
アンチウイルス、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
<b>合計時間</b>	<b>4.5 時間</b>	<b>10分以内</b>

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



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

検知率

誤検知率

Fig. 1 – High Detection Effectiveness & Few False Positives

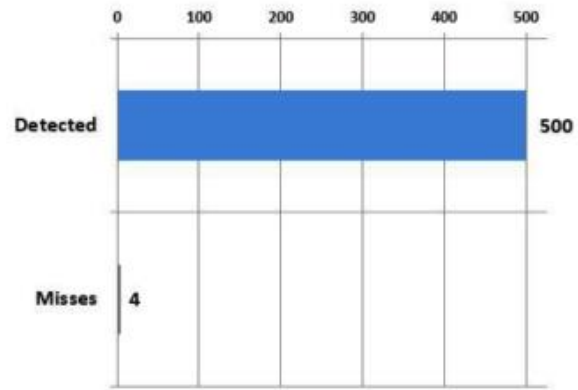


Fig. 2 – Detected 500 of 504 New & Little-Known Malicious Samples



Fig. 3 – 6 Alerts on Innocuous Applications

# 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

## JATP

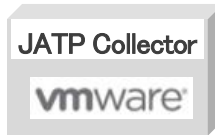


SmartCore

## 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



netskope

Carbon Black.

## NAC (端末隔離) 連携

JUNIPER Carbon Black.

ForeScout

aruba  
a Hewlett Packard  
Enterprise company

PFU  
a Fujitsu company



CISCO

## IOC (ブロックポリシ)適用可能

JUNIPER

BLUE COAT

paloalto  
NETWORKS

Carbon Black.

CISCO

CROWDSTRIKE

FORTINET

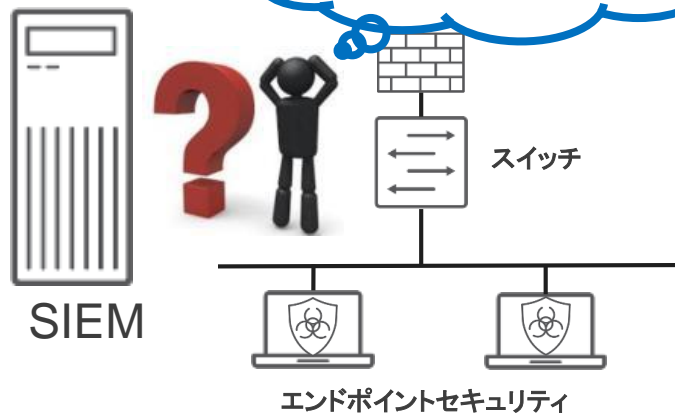
Check Point  
SOFTWARE TECHNOLOGIES LTD.

## 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

SIEMを購入したけど、  
脅威が残っているの  
か追跡が難しい。



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

ネットワークとエンドポイントからシスログ  
を受信し端末毎のインシデントとして  
自動的に紐づけ



SmartCore



SIEM



インターネット

サードパーティ製  
ファイアウォール

スイッチ

LAN

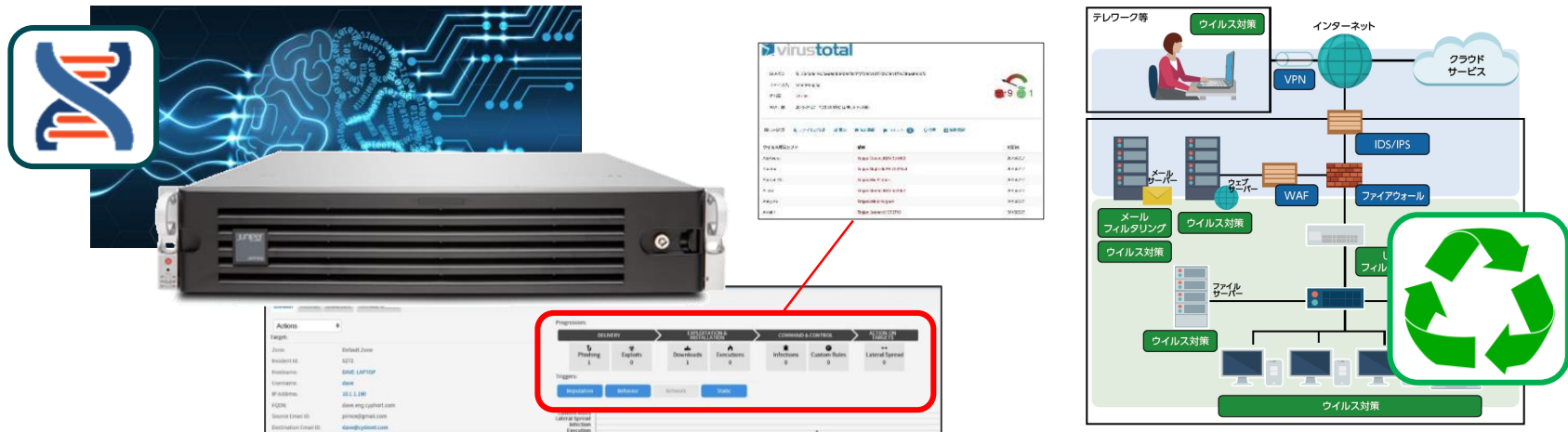


エンドポイントセキュリティ

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ーンを可視化、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か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

Are you connected?

皆さんは安全に  
つながっていますか？





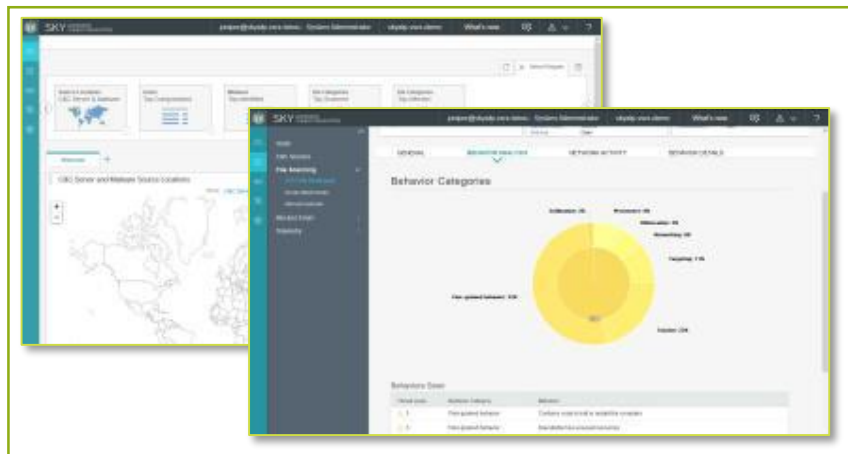
おまけ:

簡単に試せる ジュニパー  
コネクテッドセキュリティ

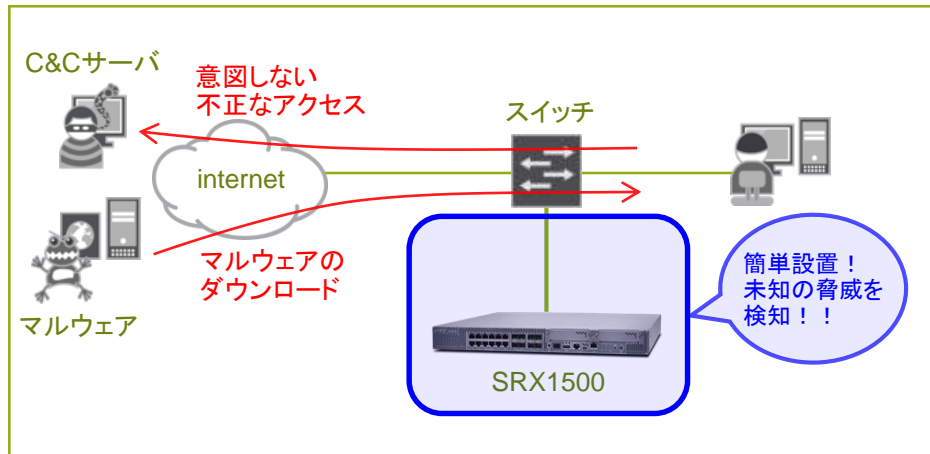
# SKY ATP (ジュニパー コネクテッドセキュリティ)

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

## Try the Juniper Advanced Threat Prevention Appliance for Free

There will always be some network threats that can sneak past your toughest perimeter security. But if they do, you don't need to worry. You can stop them from doing any damage even before they begin with the Juniper Advanced Threat Prevention (JATP) Appliance.

The only solution certified by ICSA Labs to provide 100 percent advanced threat detection, the JATP Appliance rapidly analyzes and remediates dangers that target your organization.

We invite you to try JATP free for 14 days. See for yourself why powerful detection is your strongest defense against cyber crime.

### Register Now

 I'm not a robot

JUNIPER  
NETWORKS

JATP Trial (14日間無料)<sup>www.</sup>

<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/>