コネクテッドセキュリティ

ネットワーク全体でユーザ、アプリケーション、およびインフラのセキュリティを確保する

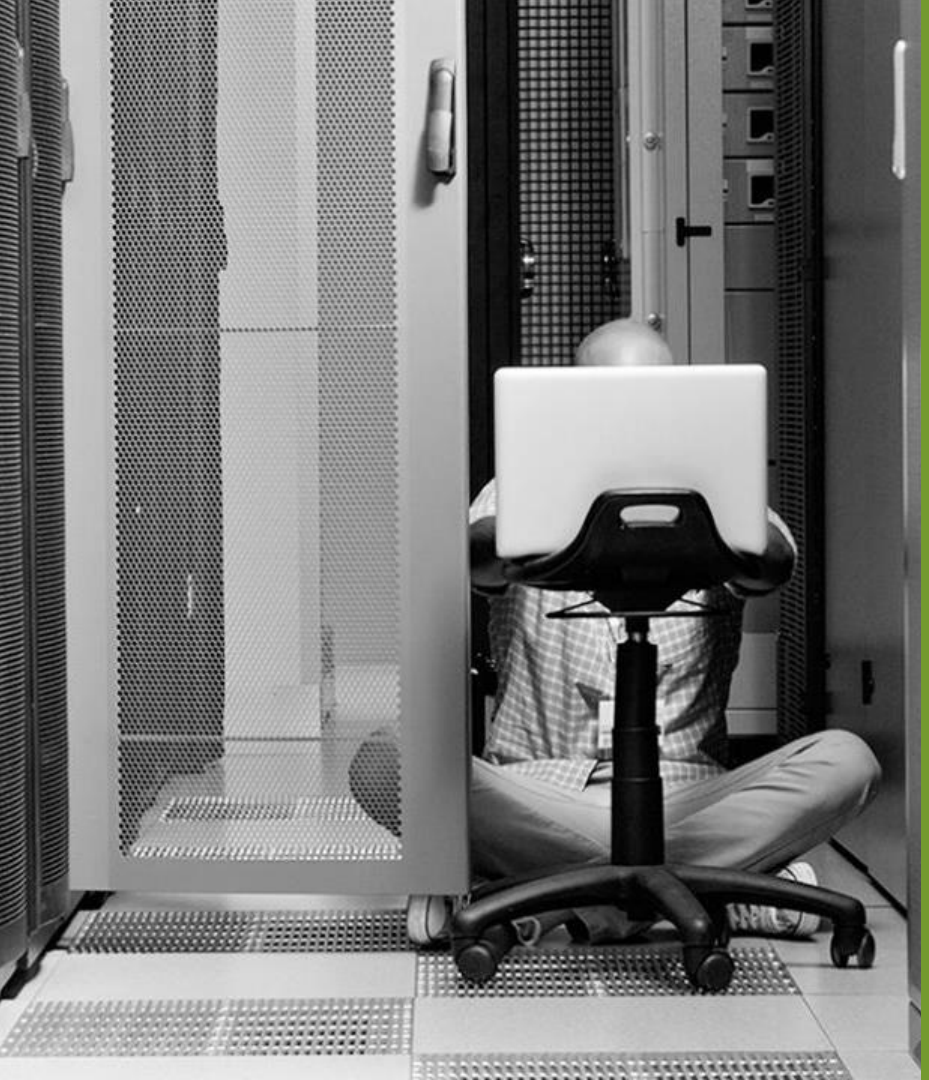
2019年9月24日

ジュニパーネットワークス株式会社
技術統括本部

Juniper Networks | Engineering Simplicity

内容

- 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セキュリティに対する取り組み
- 運用負荷を大幅に削減するConnected Security
- 多層防御の課題を解決するConnected Security
- まとめ



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

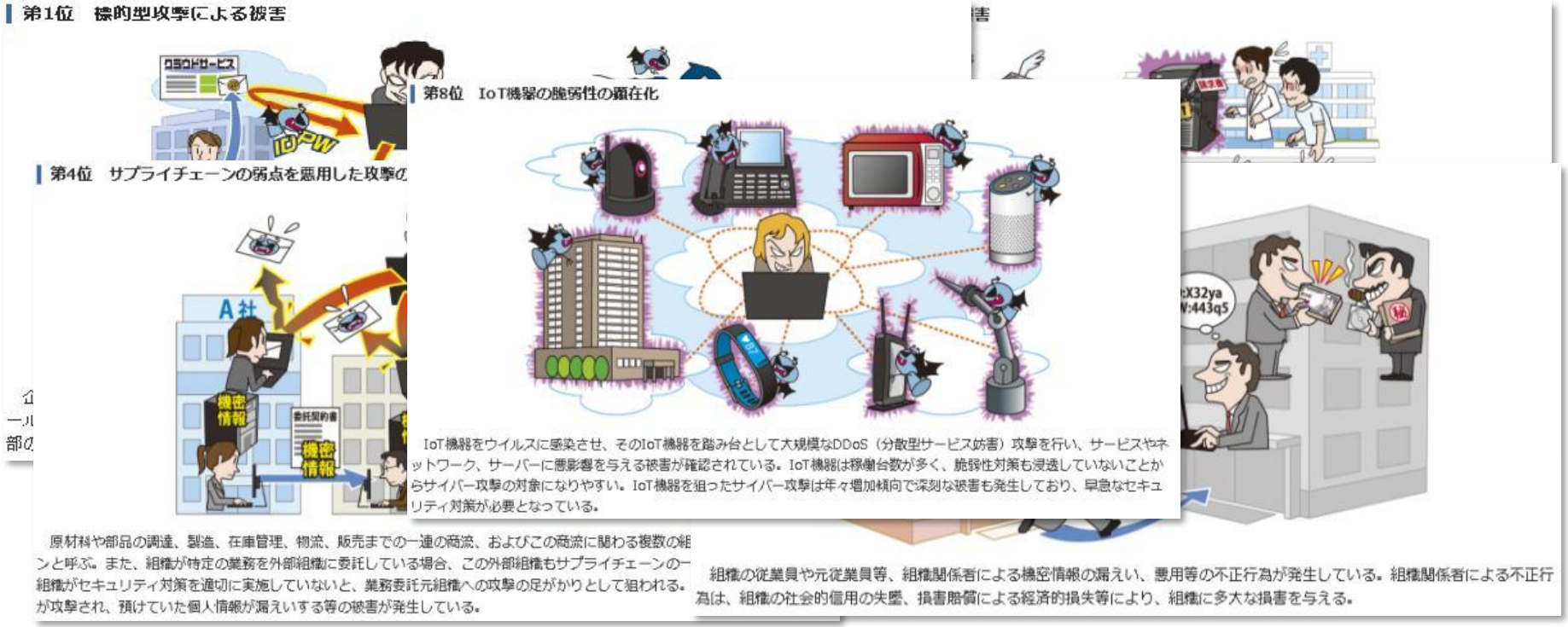
IPA 情報処理推進機構の「情報セキュリティ10大脅威 - 2019」

「情報セキュリティ10大脅威 2019」

順位		順位	
1位	標的型攻撃による被害	6位	サービス妨害攻撃によるサービスの停止
2位	ビジネスメール詐欺による被害	7位	インターネットサービスからの個人情報の窃取
3位	ランサムウェアによる被害	8位	IoT機器の脆弱性の顕在化
4位	サプライチェーンの弱点を悪用した攻撃の高まり ***New***	9位	脆弱性対策情報の公開に伴う悪用増加
5位	内部不正による情報漏えい	10位	不注意による情報漏えい

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

IPA 情報処理推進機構の「情報セキュリティ10大脅威 - 2019」



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

企業IT担当者の抱える課題

IT担当やセキュリティ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

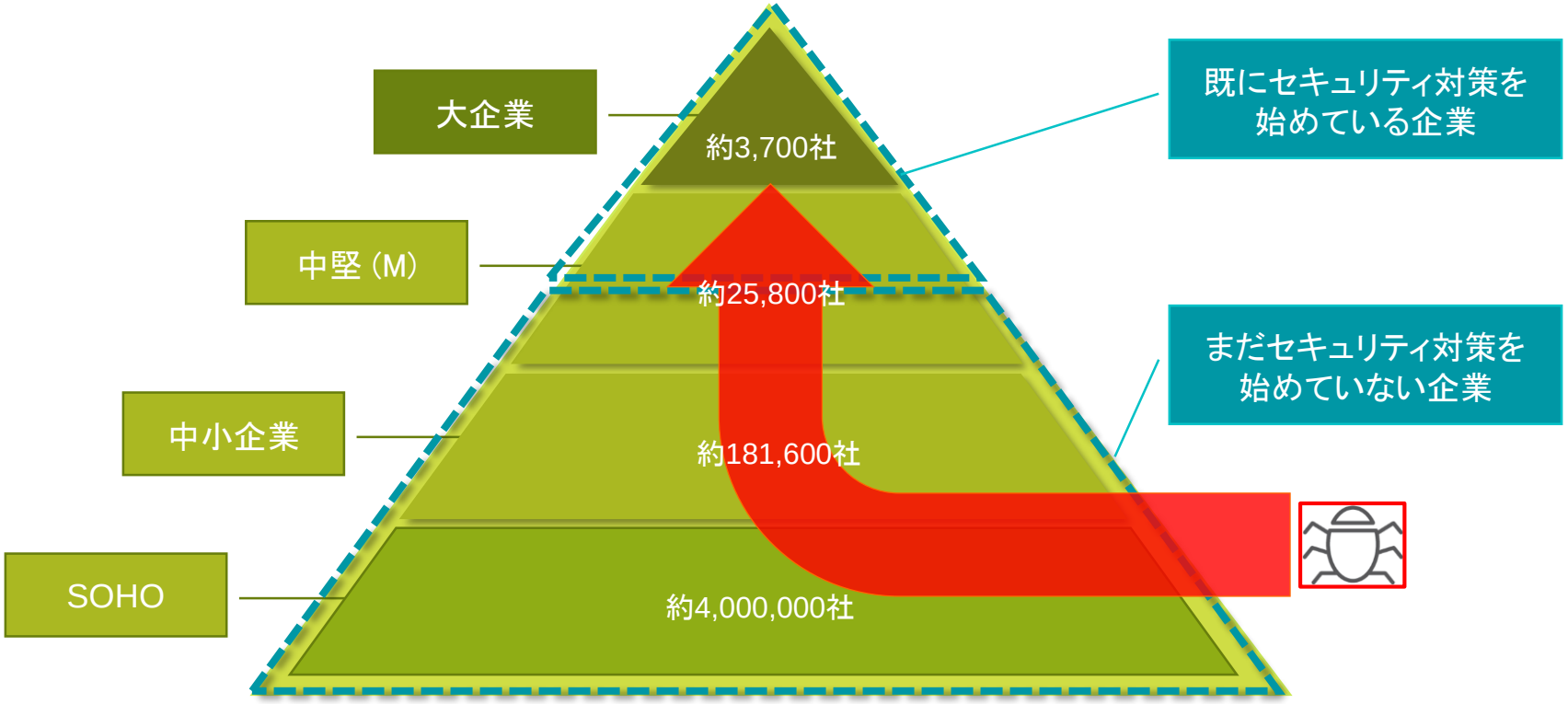
多様化するサイバー脅威に対して正確で迅速な対応

「多層防御」の運用負荷が増大し、コストを掛けずに正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管理

エージェントソフトウェアの更新、IoTやBYODデバイスの管理が困難になってきている

サプライチェーン攻撃



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

ジュニパーのセキュリティに対する取り組み

設立 | SDSN | Juniper Connected Security

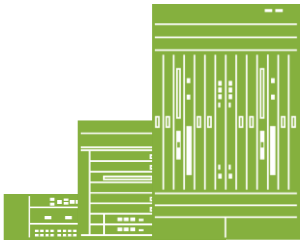
1996 | 2004 | 2008 | 2016 | 2019

ルータ製品

NetScreen
（SA/SSG/ISG）

JUNOS

SRX5000シリーズ



Sky ATP

vSRX

SRX300

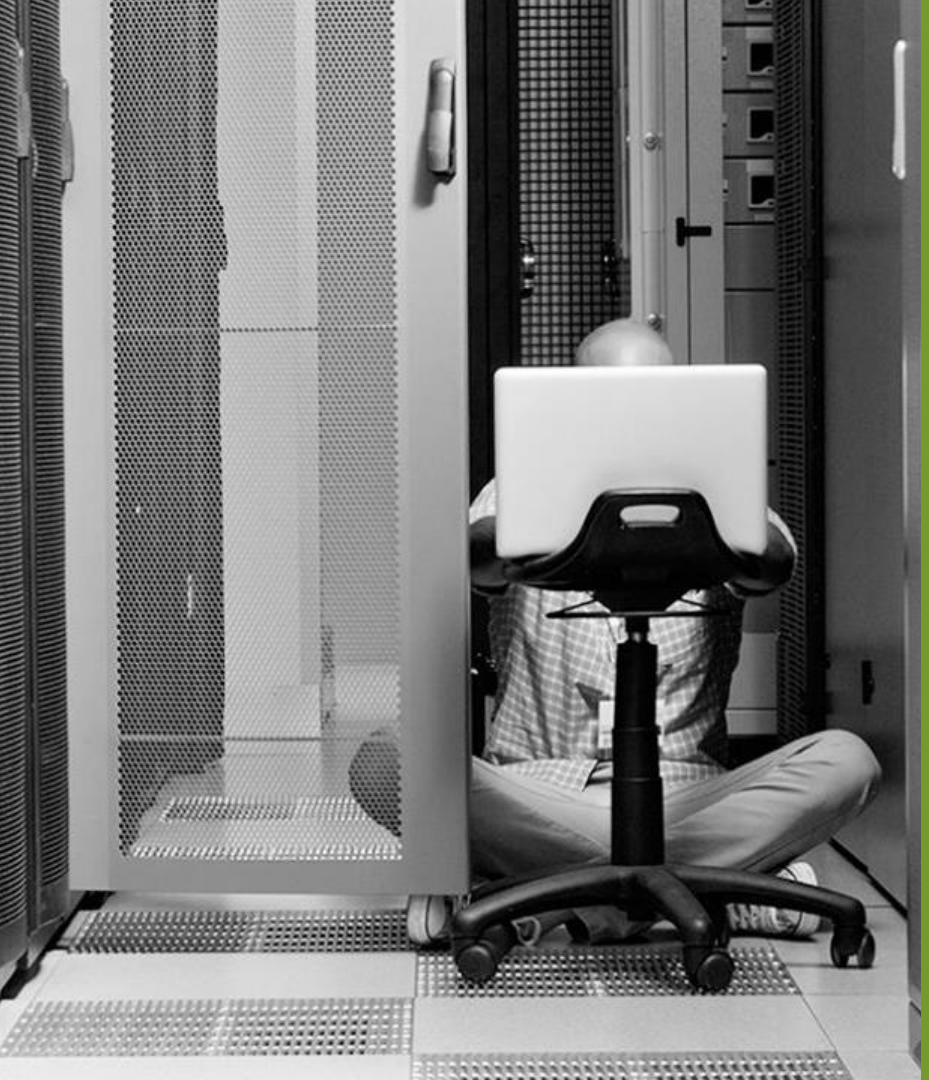
Security Director

cSRX

SRX1500

SRX4600

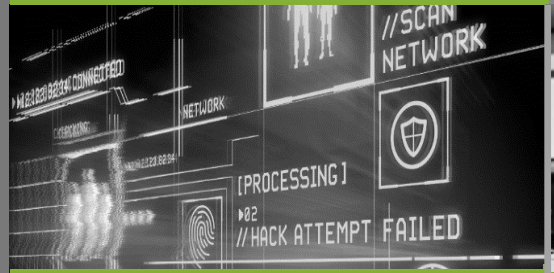
JATP Appliance



運用負荷を大幅に削減する
Connected Security

ジュニパーのConnected Security

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

- すべても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

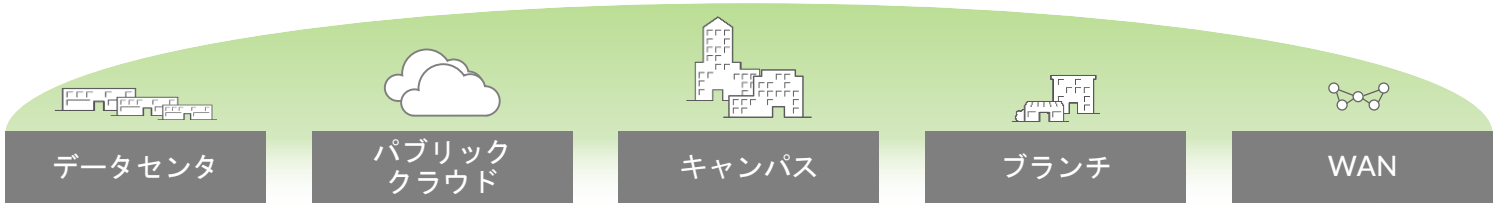
対処

防御

可視化：エンドポイントから、エッジおよびクラウドまで

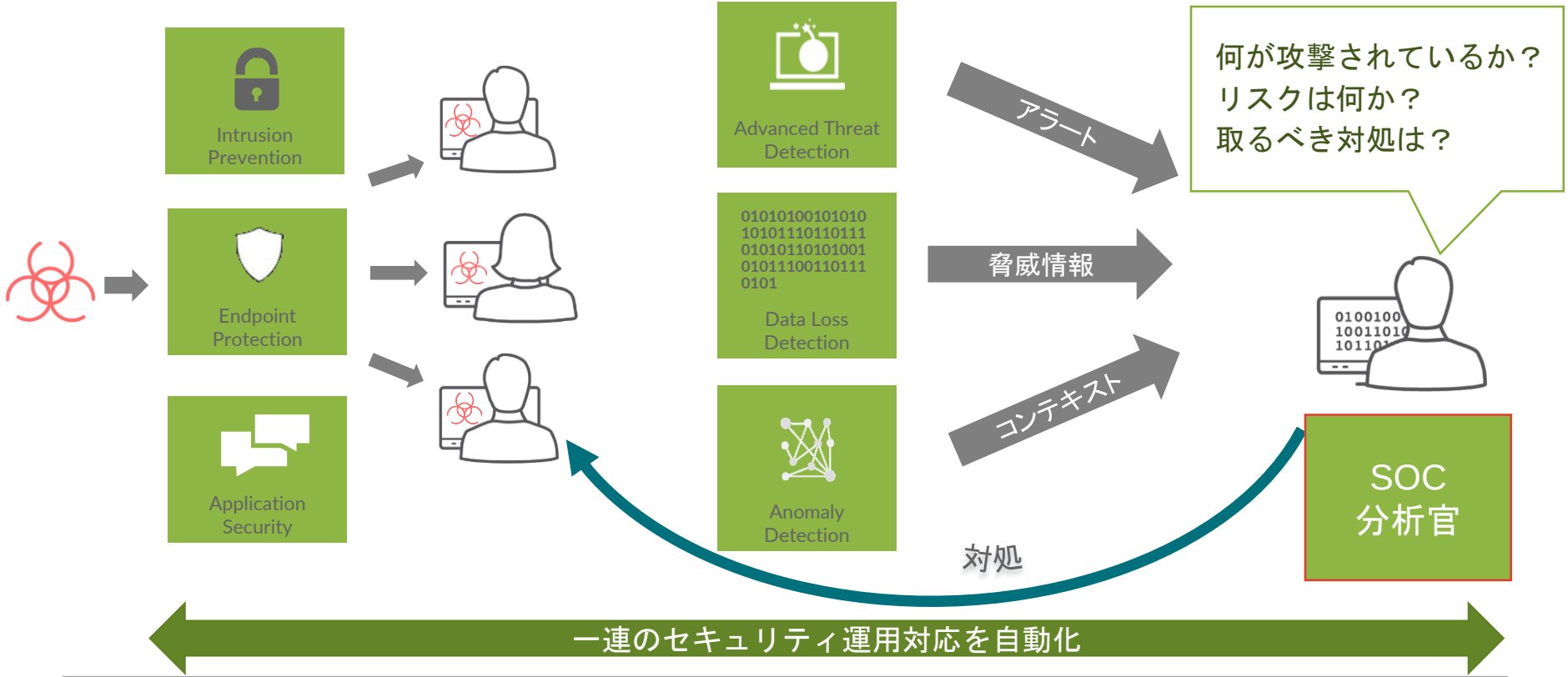
Secure top to bottom

自動化	信頼性の高いワークフロー、システム連携、サービスレベル制御
クラウド対応	大規模エンタープライズにおいても運用を簡素化
ソフトウェアデファインド	対処すべきセキュリティ脅威に対して、ポリシーを瞬時に適用
オーケストレーション	セキュリティシステムの構築および運用を自動化



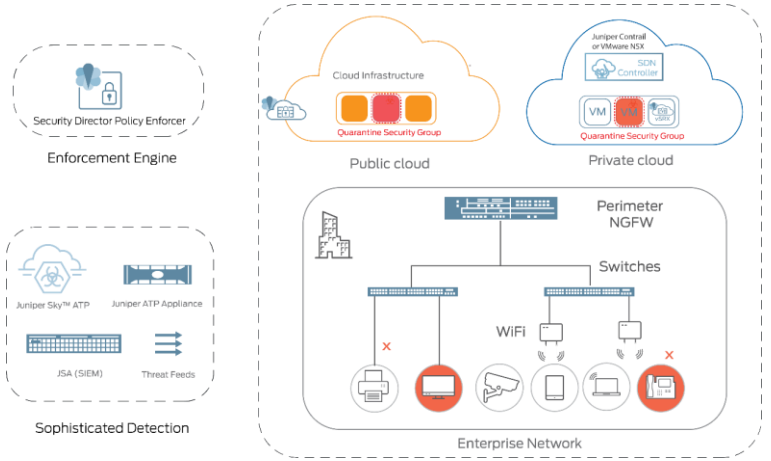
Secure end to End

機械学習による検知：データ収集および解析



自動化された対処：既定ルールまたはカスタムアクション

自動脅威制御



- 段階的な隔離レベル
- パブリッククラウド、プライベートクラウドおよびオンプレ環境において、ネットワークレベルで脅威を封じ込める
- サードパーティ製品との連携（スイッチ、WiFi AP，EDR）

DevOpsとの連携

標準ベース

netConf YANG OPENCONFIG gRPC gNMI REST

サードパーティ連携

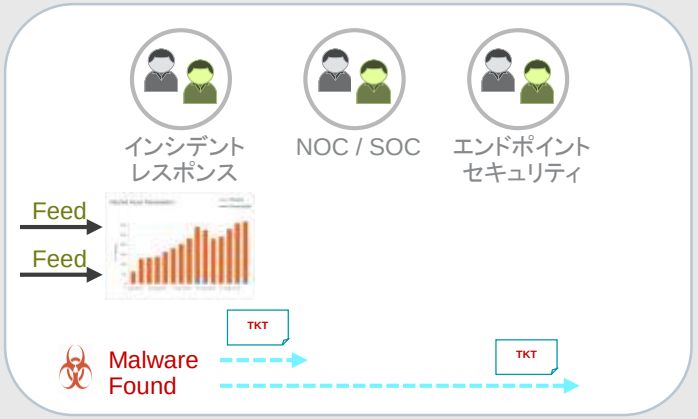
SALTSTACK CHEF puppet ANSIBLE NITA PyEZ

ネットワーク運用の簡素化

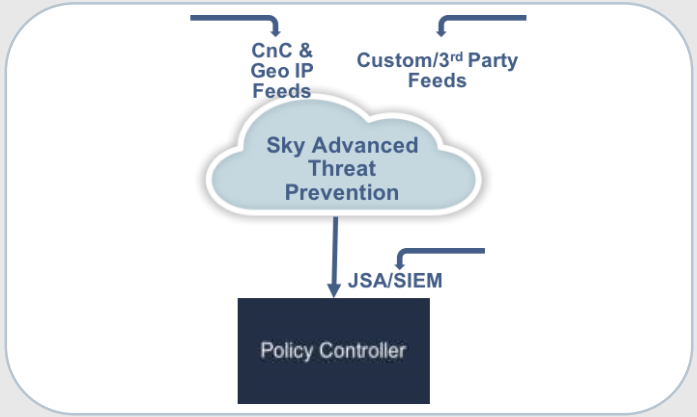
JSNAPy Automation Scripts (op/event/commit/ SNMP) python JET Telemetry (JTI)

Connected Security:
セキュリティ脅威を自動的に検知し排除する仕組み

手動による脅威への対応



自動的に脅威を検知・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）

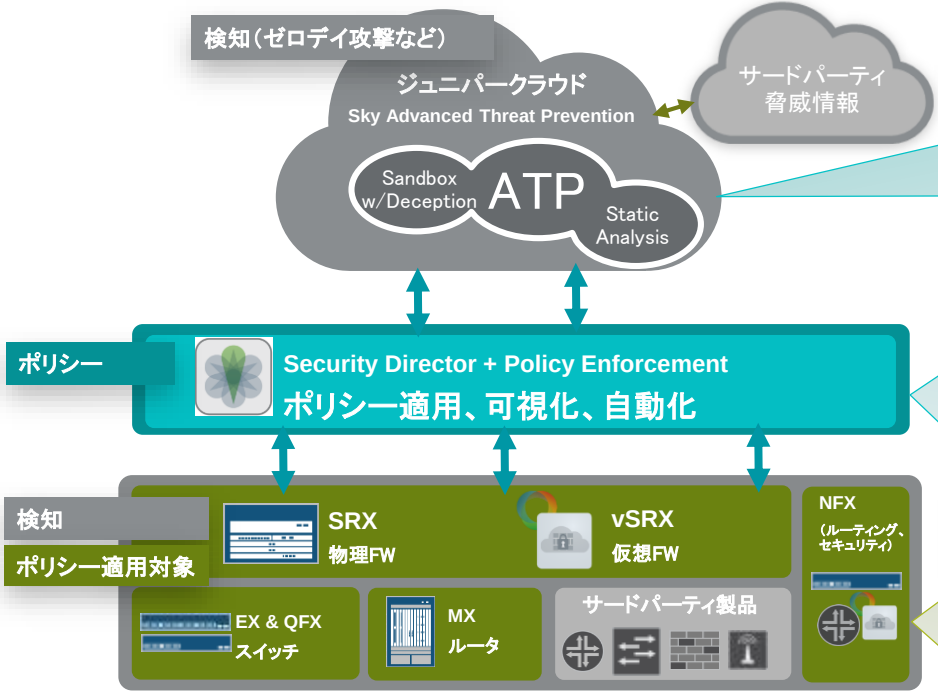
被害拡大の
防止・抑制
（運用者）

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

Connected Security:
ネットワークをセキュリティドメインとして自動検知と対処



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

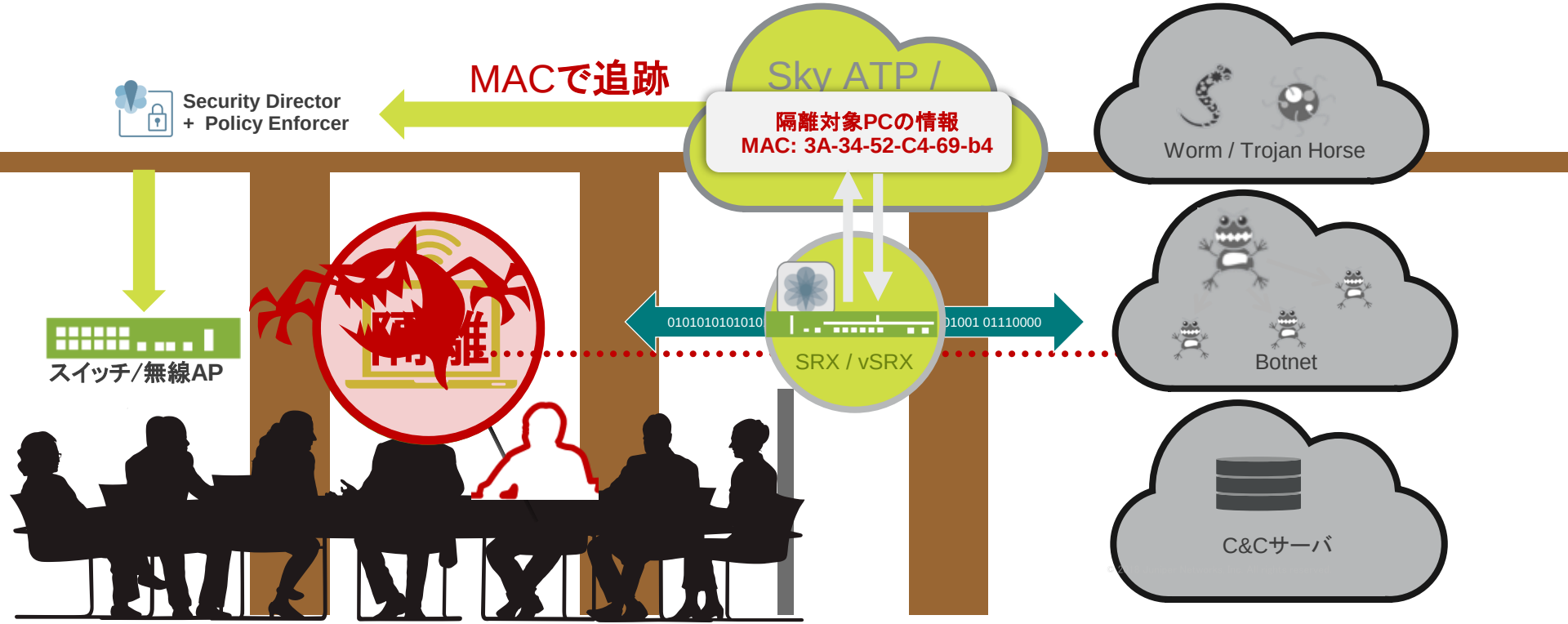
10段階の脅威レベル
ユーザ毎に情報セキュリティポリシーを設定

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

ネットワーク全体を単一の対策実行ドメインに！それぞれの機器がポリシーの適用ポイント

Connected Security:
MACアドレスで追跡・隔離



標的型攻撃対策 (ATP) のポートフォリオ

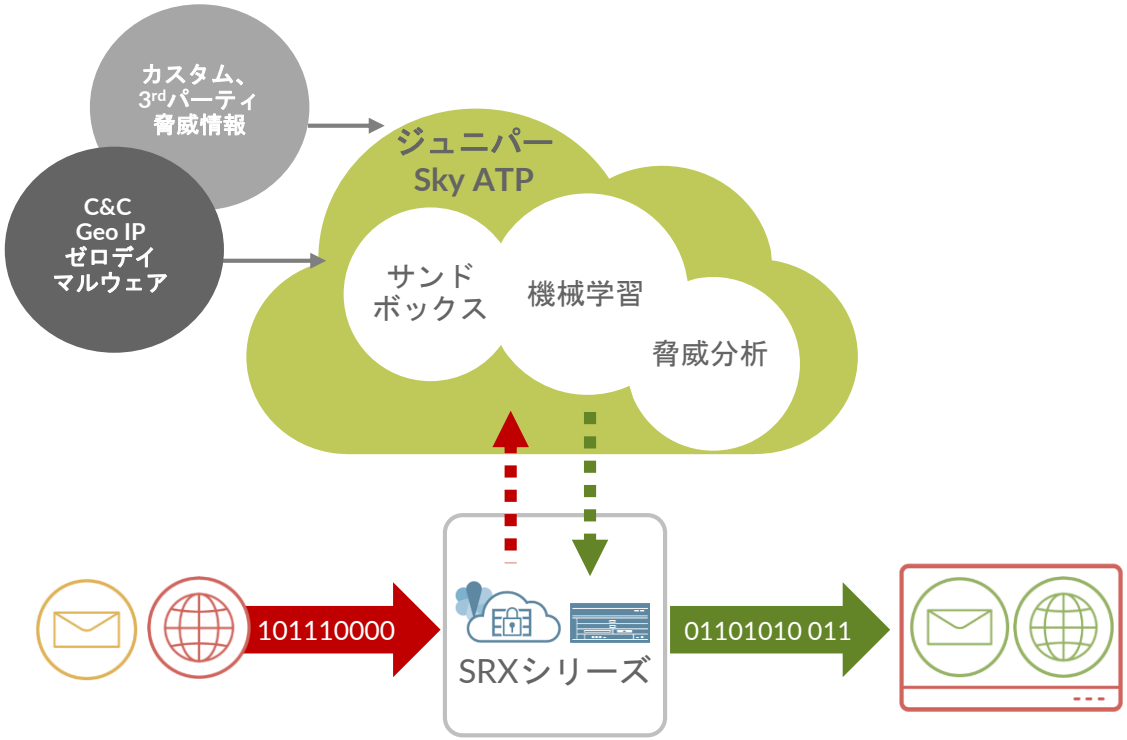
SaaS

Sky ATP

オンプレ

JATPアプライアンス

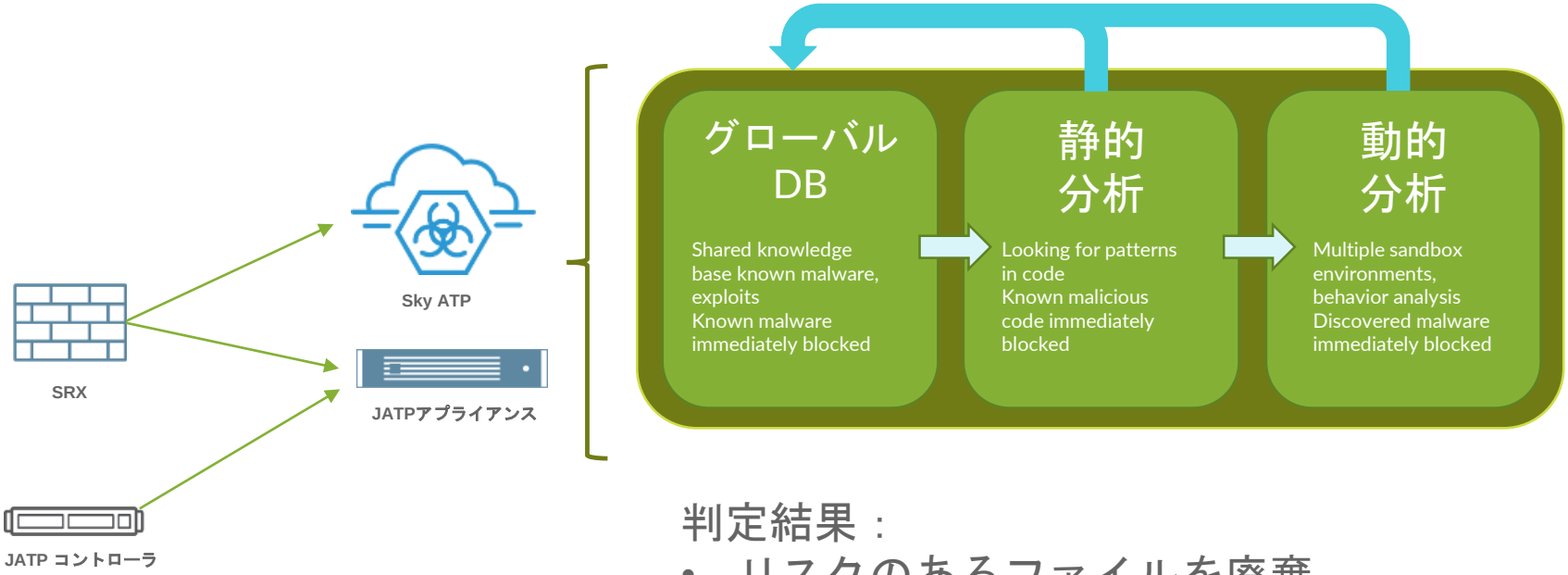
Sky ATP - クラウドベースの脅威防御サービス



- ランサムウェアなどの高度なマルウェアからの保護
- 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）
- ウェブとメールのファイルを分析
- 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

FedRAMP

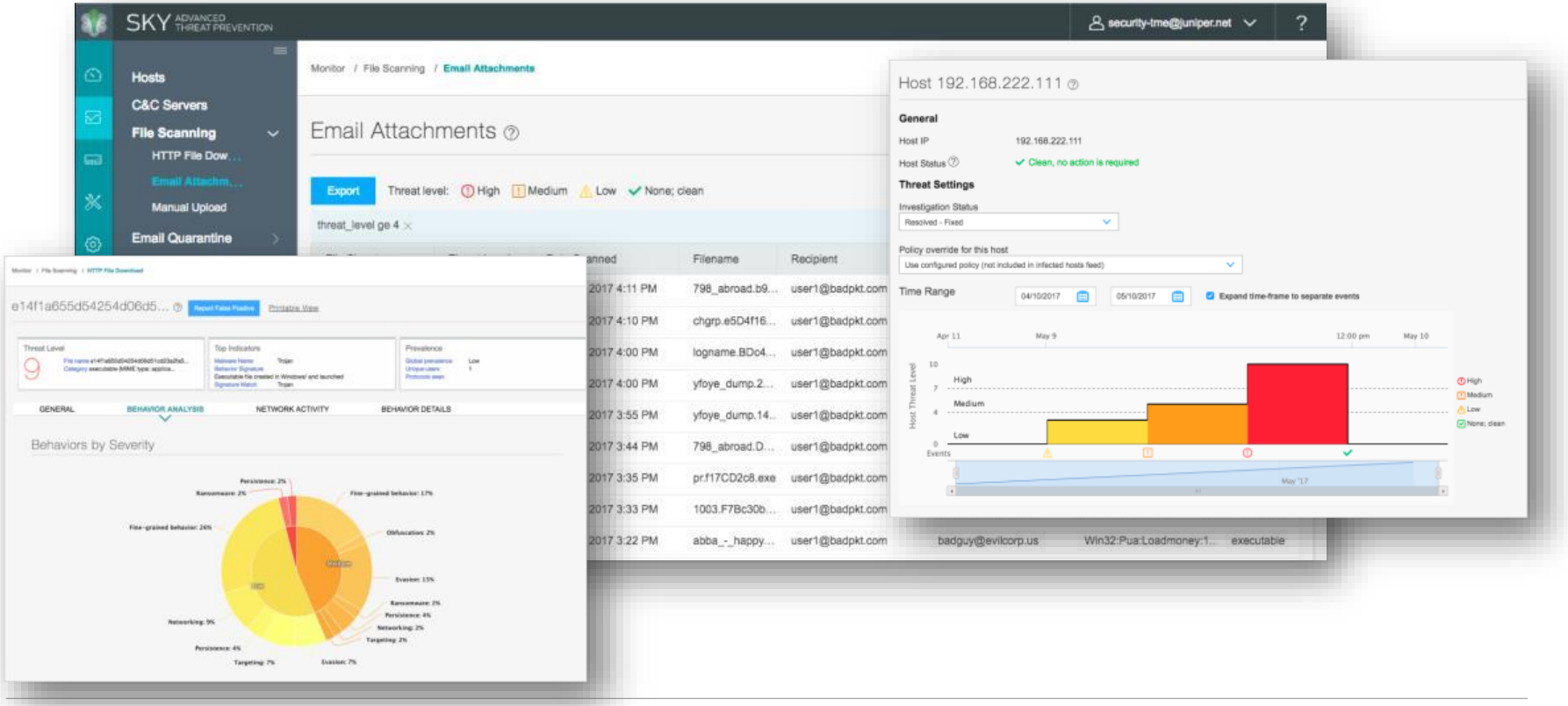
ATPマルウェア検知フロー

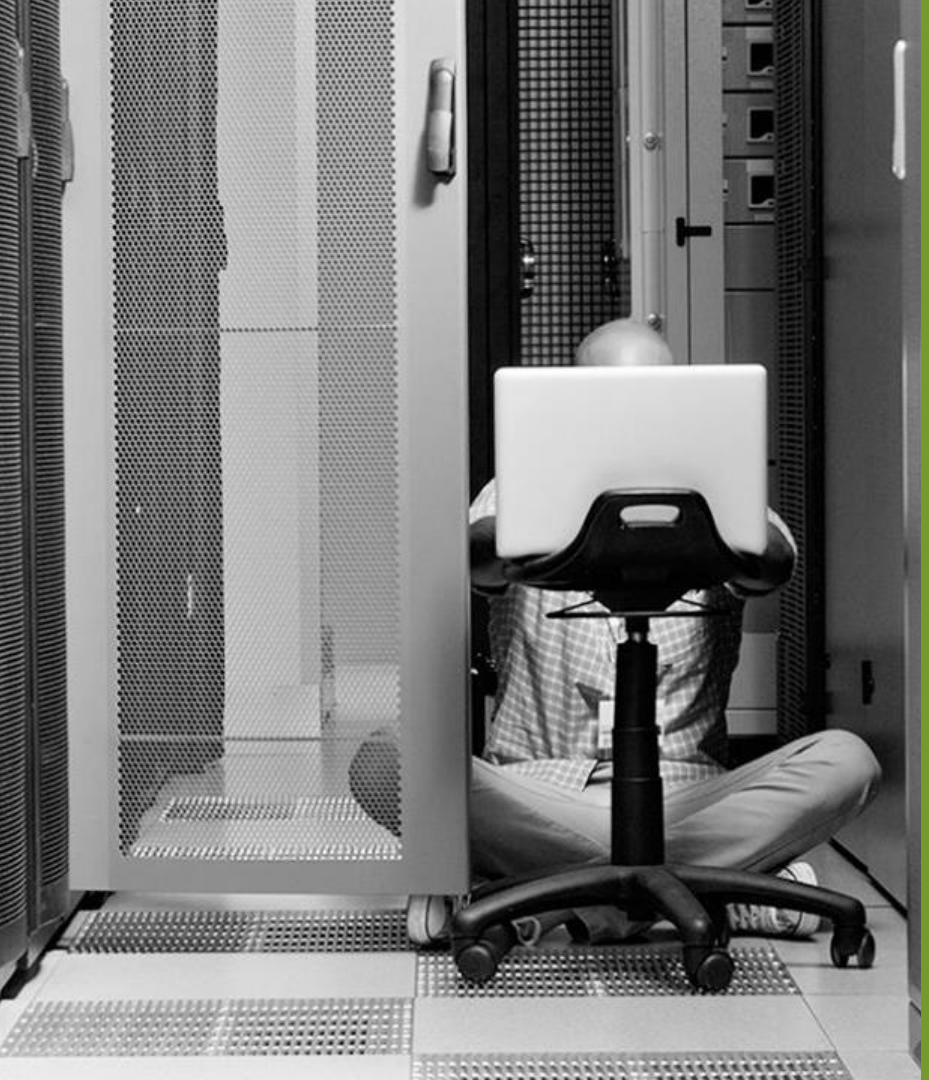


判定結果：

- リスクのあるファイルを廃棄
- グローバルDBにはHash値を追加

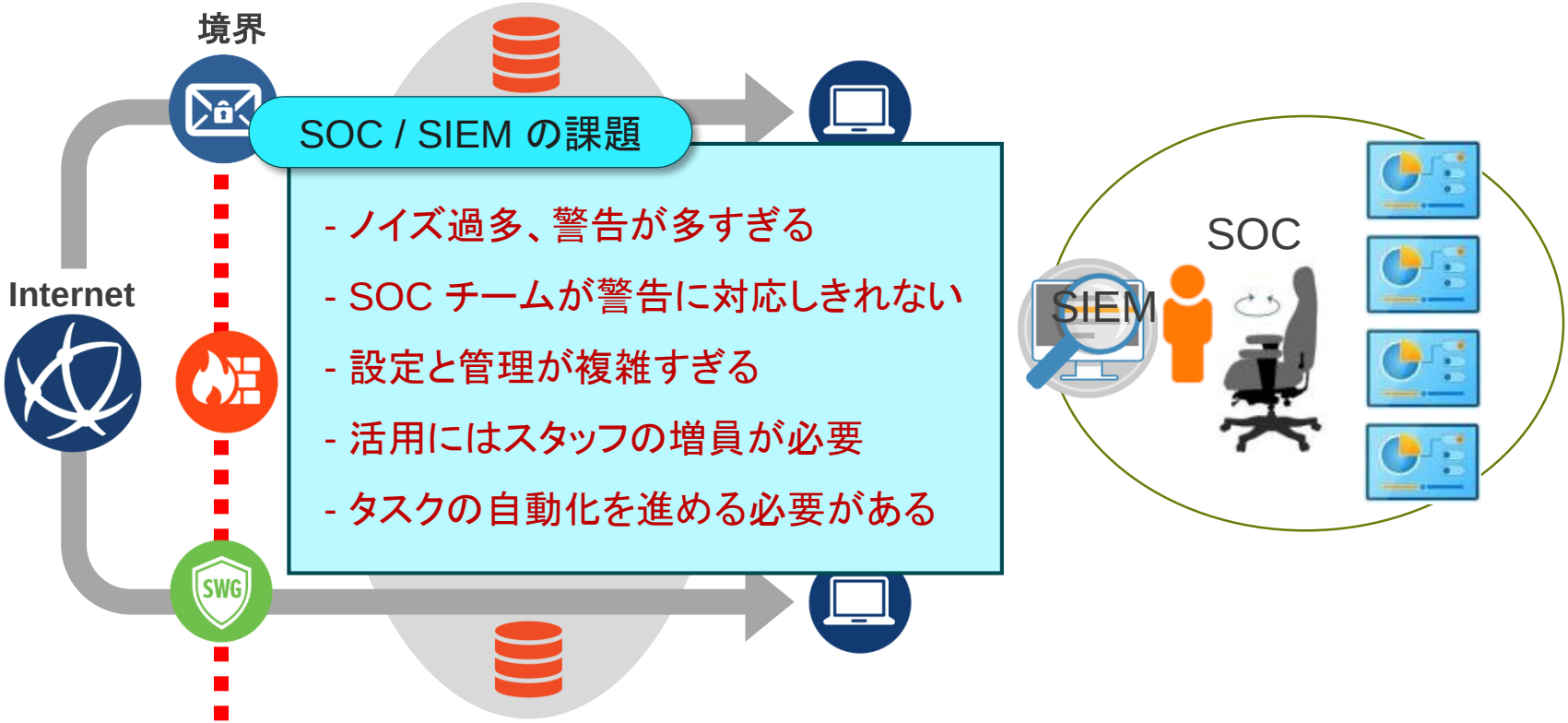
Sky ATP管理画面のイメージ



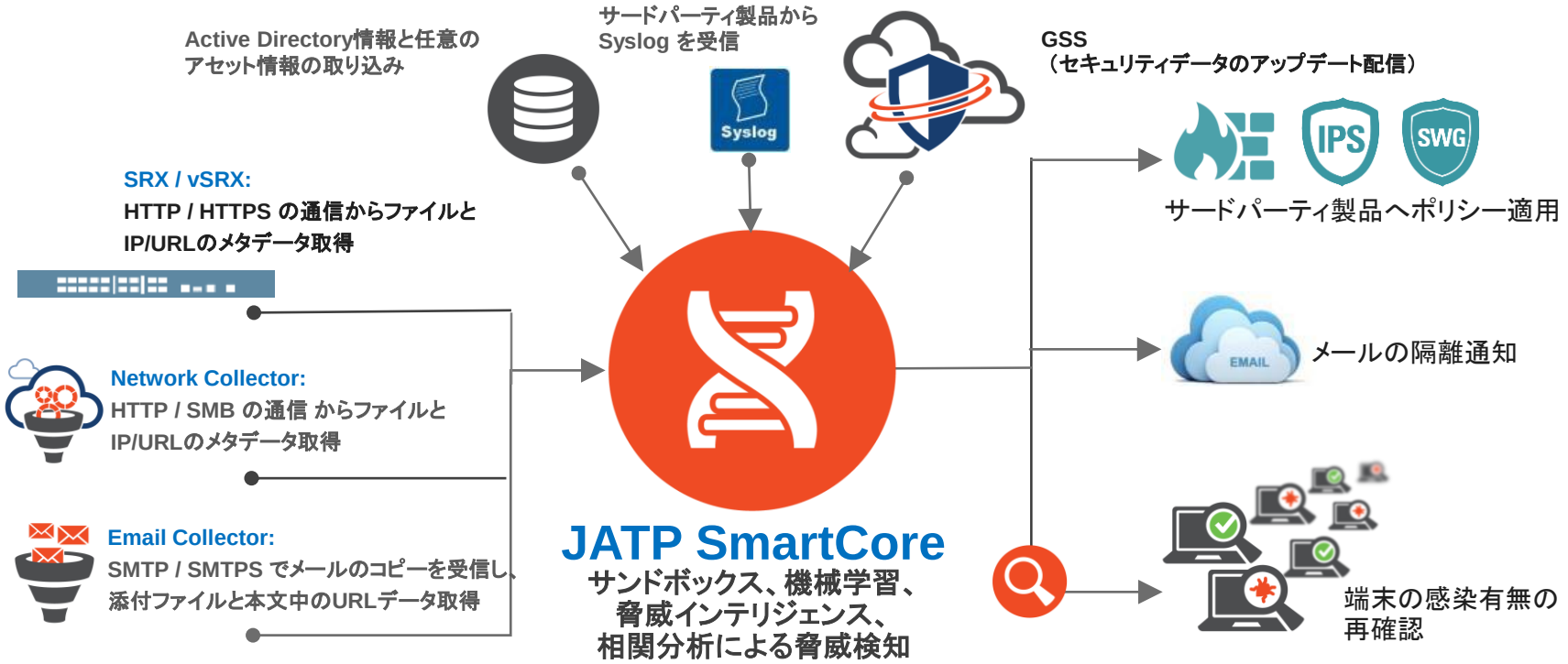


多層防御の課題を解決する
Connected Security

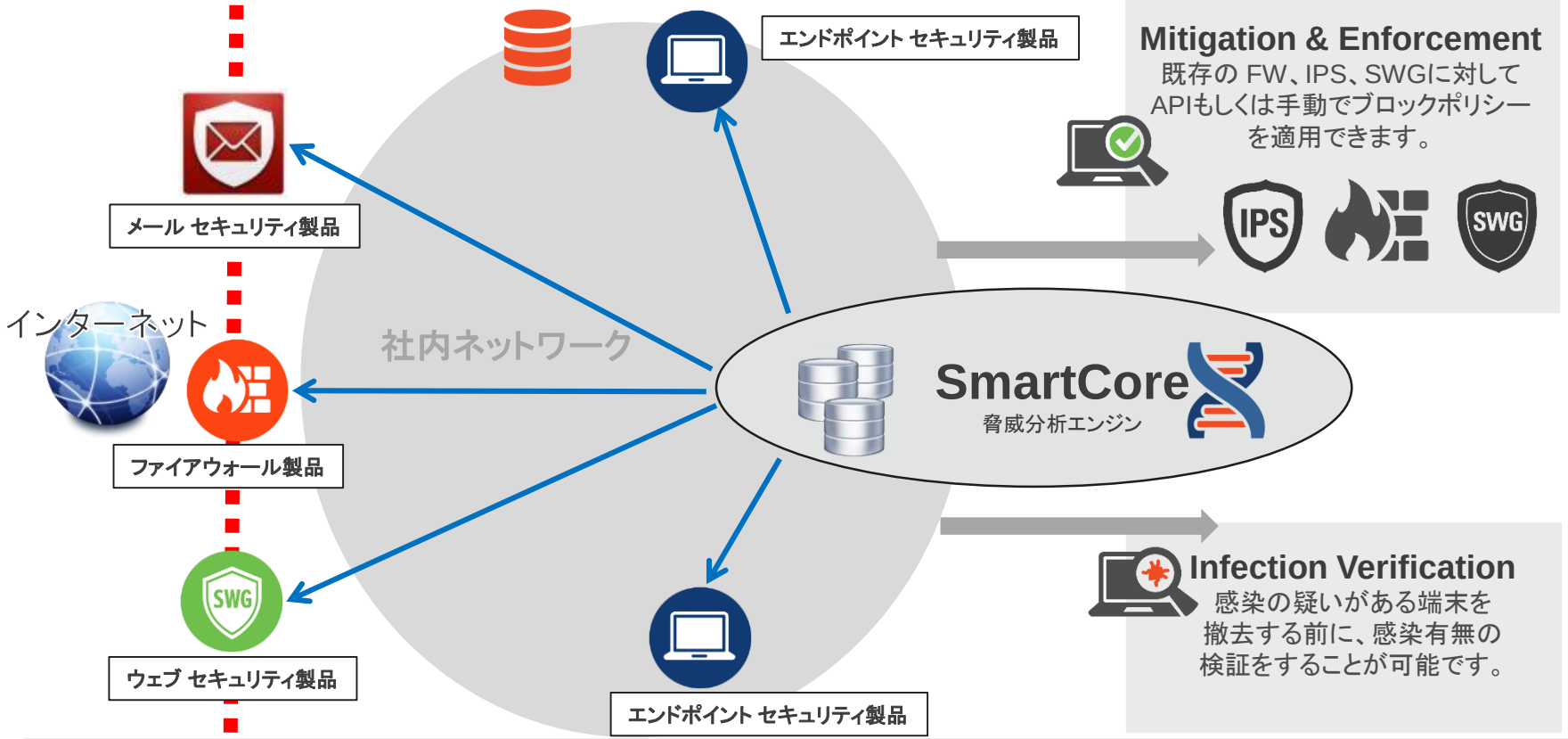
多層防御環境における課題



JATP（機械学習を駆使し、脅威を自動分析/可視化・自動対応）

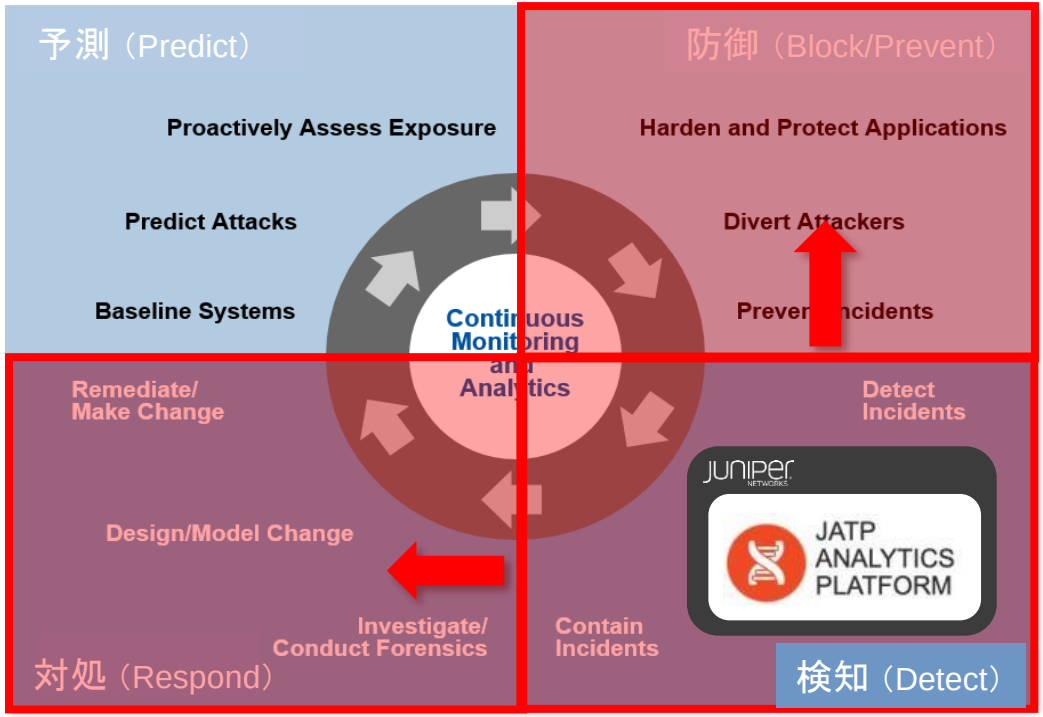


インシデントレスポンスの自動化



強固な検知能力、対処及び防御との連携

“サンドボックスの検知能力は極めて重要である。何故なら・・・
既に脅威が侵入していることを前提に、素早く対処しなければならないから。“

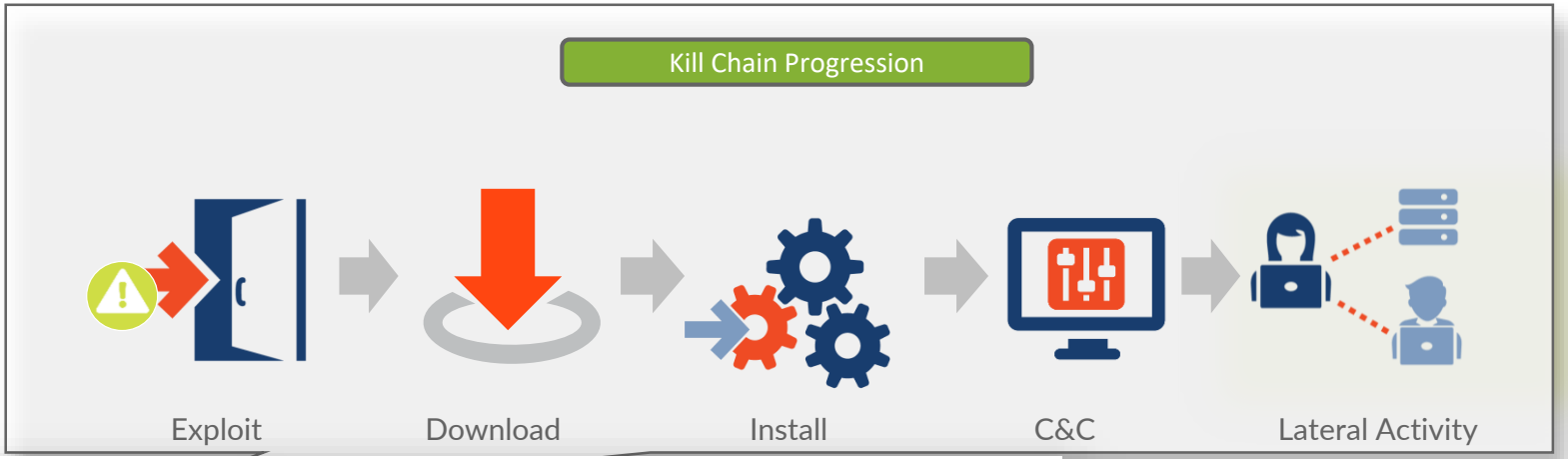


Gartner 評価の連携モデル

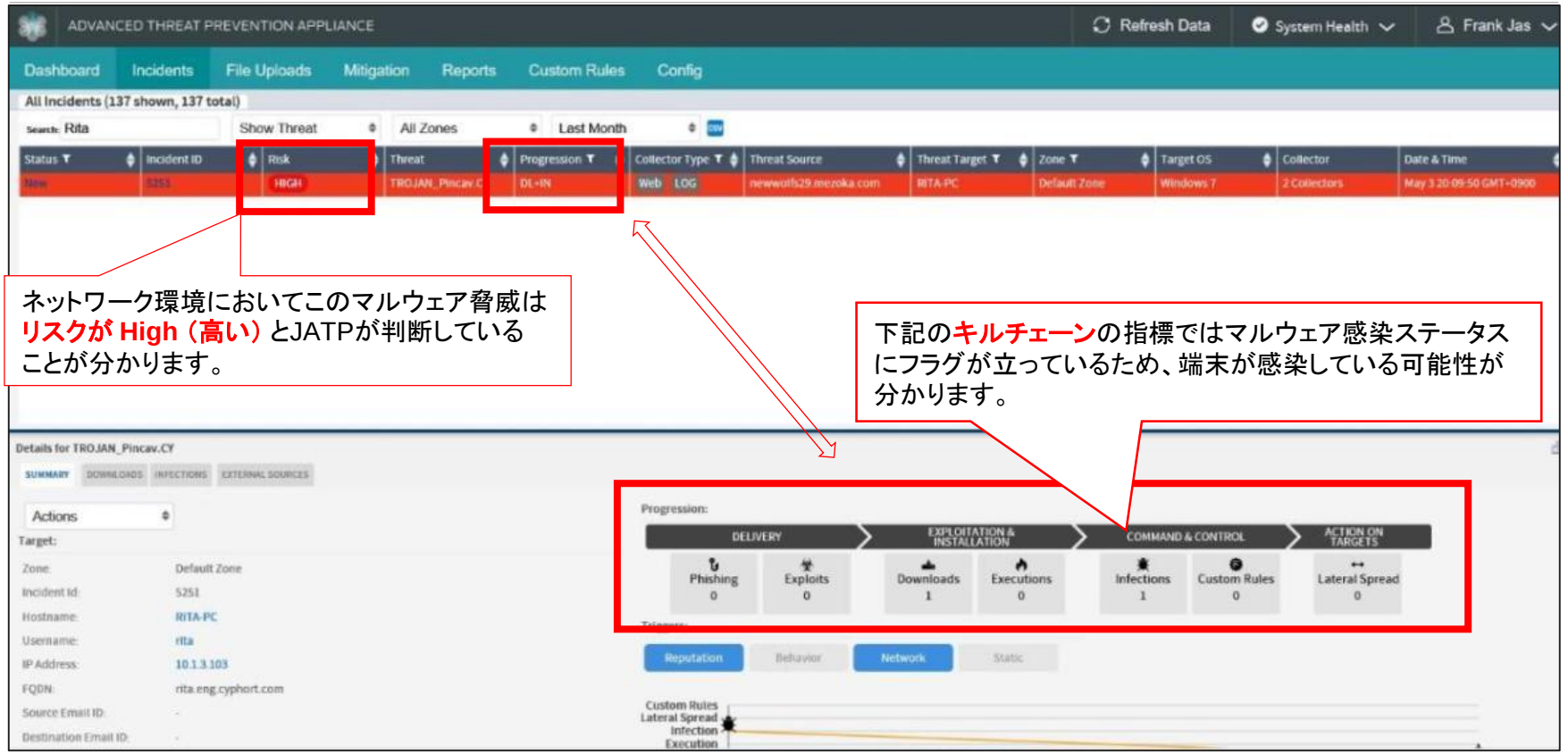
- ✓セキュリティの防衛ラインを突破した脅威を素早く発見
- ✓脅威が内在する時間を短くすることで潜在被害を最小限にする
- ✓サードパーティ機器と連携
  - ➢インシデント検知
    →「防御」へ指示して、攻撃を回避
  - ➢インシデント抑制
    →「対処」へ指示して、
    調査またはフォレンジックを促す

Gartner

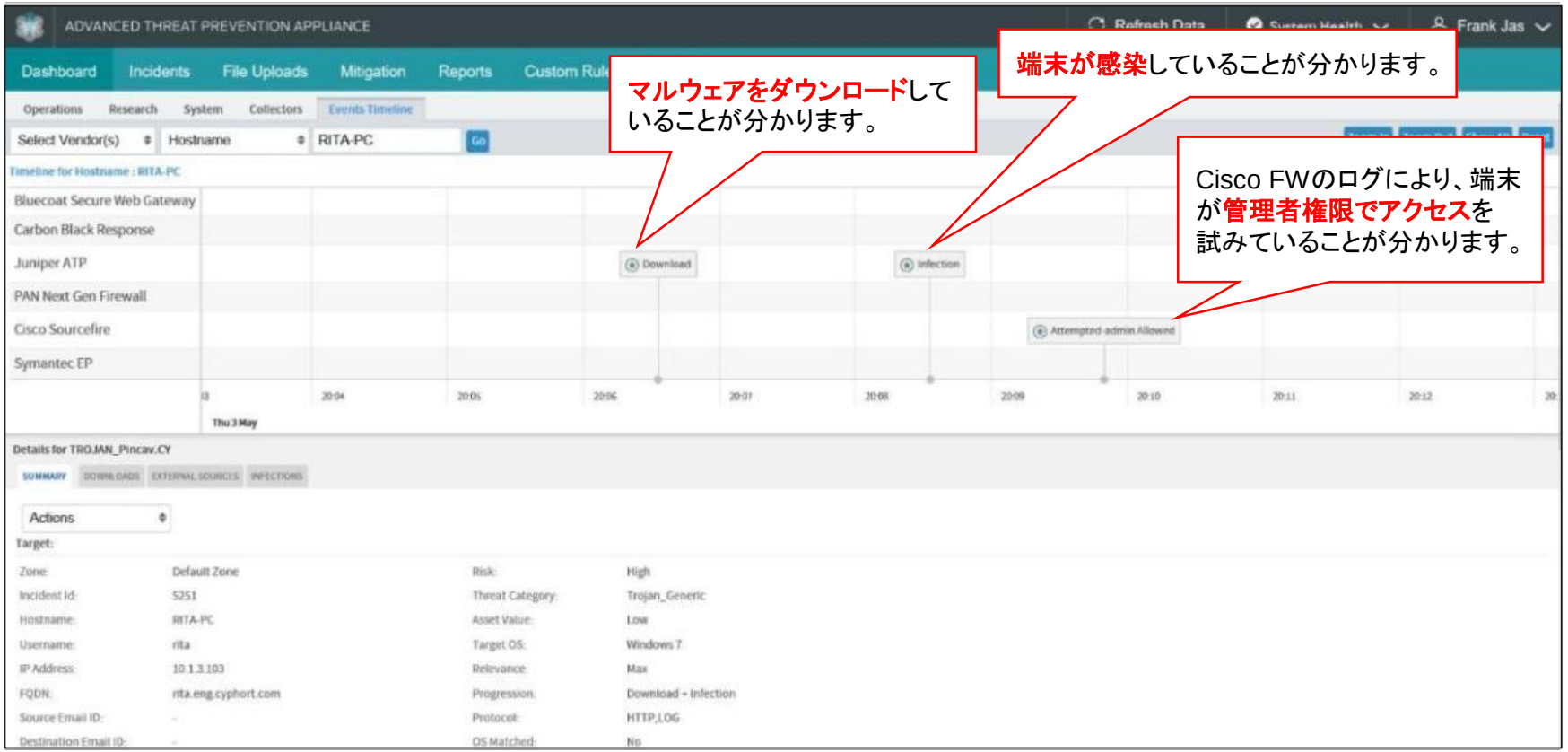
単一画面から、キルチェーンのステージを可視化



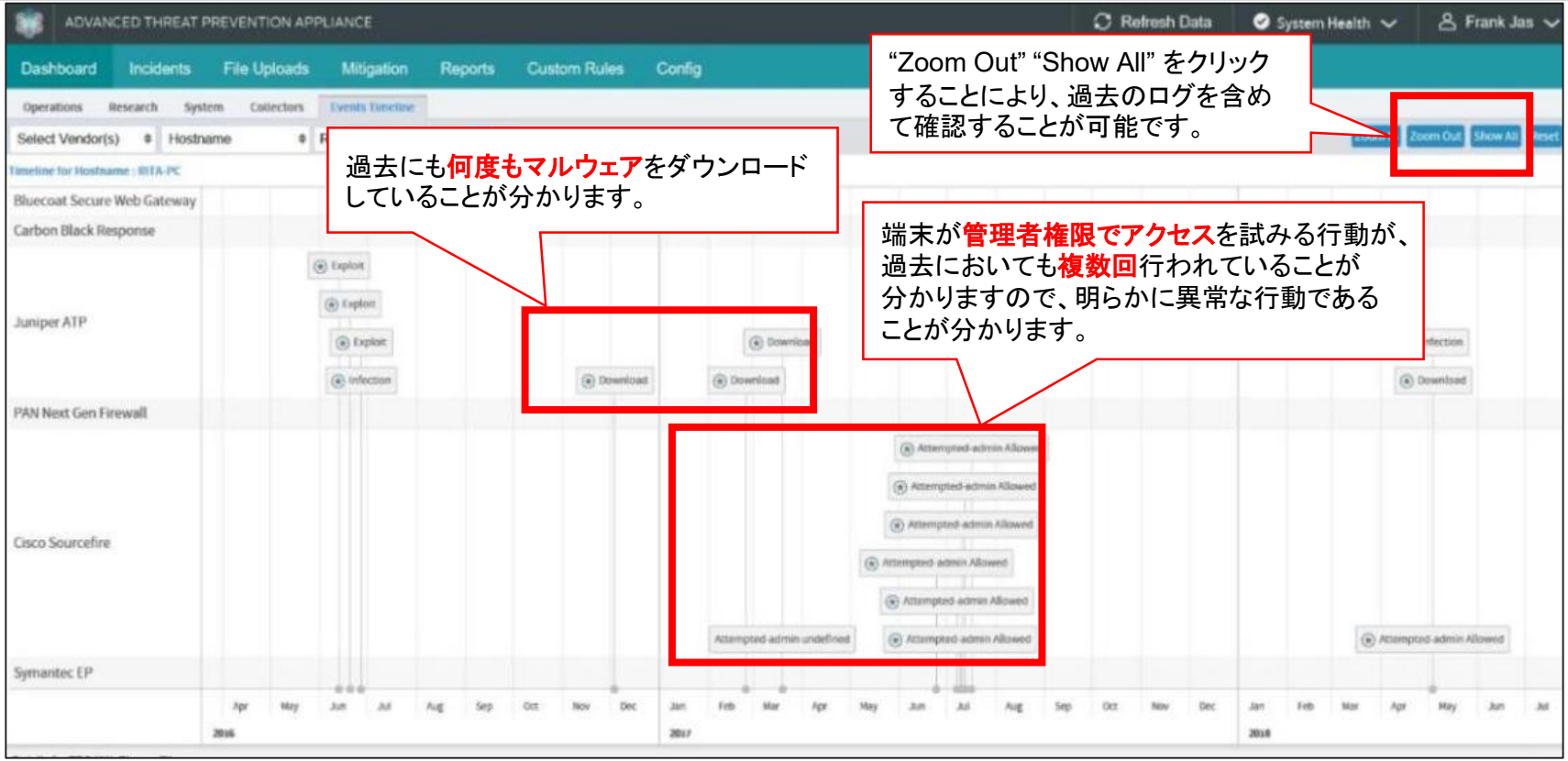
ユースケース①（脅威の検知・キルチェーンの確認）



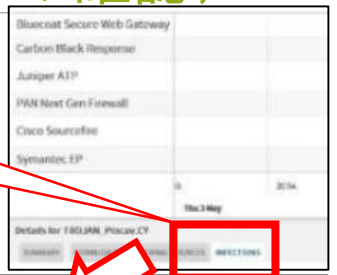
ユースケース②（タイムライン – 時系列の確認）



ユースケース③（タイムライン（時系列）全体の確認）



ユースケース④（Infection - C2サーバとの通信状況の確認）



Infectionのタブをクリックするとc2サーバへの通信状況が確認できます。

C2 Serverのドメインが確認できます。

実際に発生している通信の確認できます。

Infection Summary:

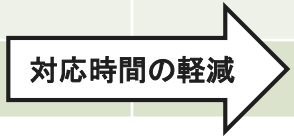
Name: TROJAN_Pincav.CY
Severity: High
Category: Trojan_Generic
Derived MD5: 1e5499640ca31e4b1f113b97a0cae08b Find on VirusTotal
Collector: demo next x collector

Network Information:

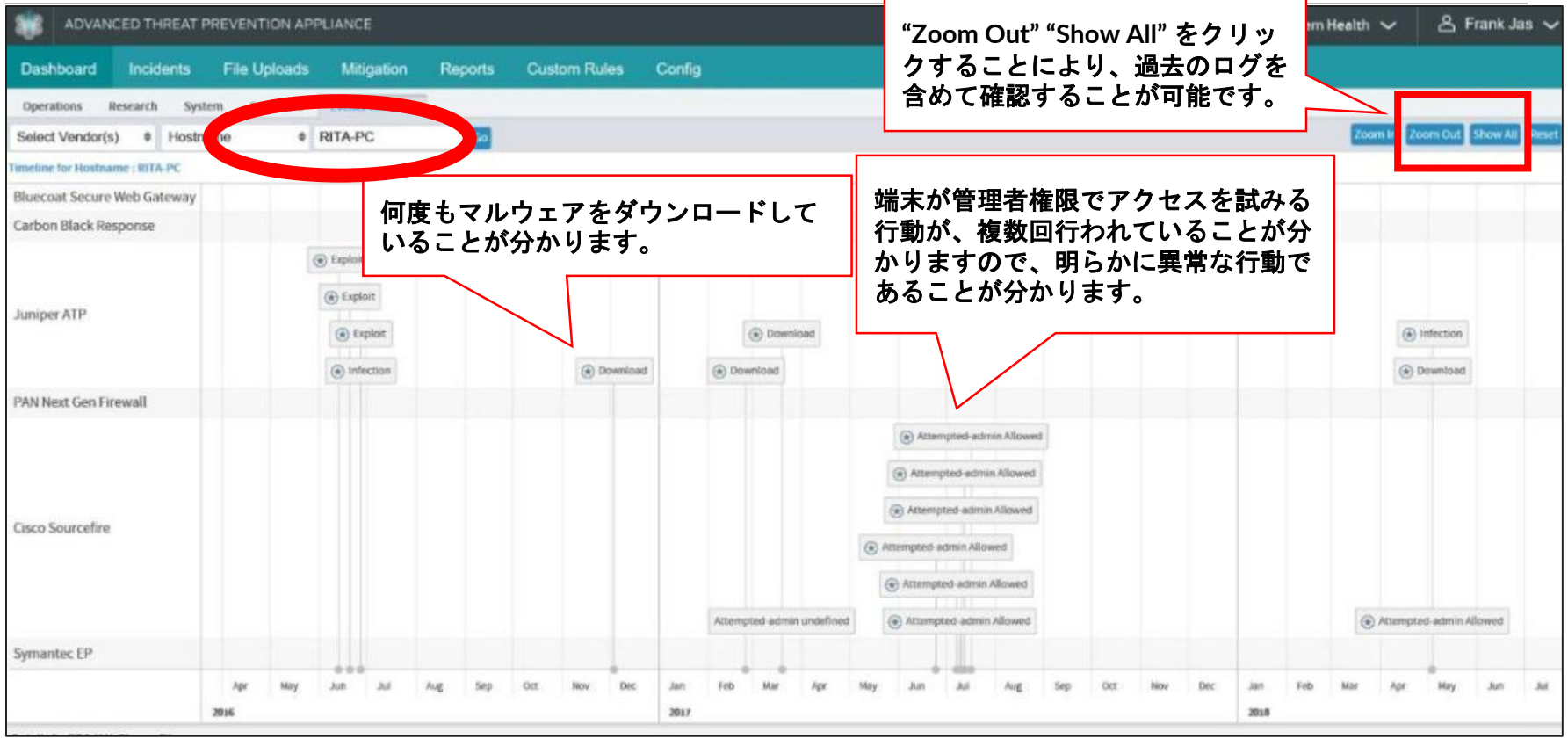
Date	Rule Id	Summary	C&C Server	Details	Actions
Mar 11 21:08:33 GMT+0900	8926319	CY AUTO TROJAN Generic ccaed7c3c6e58a2844c9896246997f62 HTTP Callback 8926319	newwolfs21.mezoka.com	POST /mits/logon.php HTTP/1.1..User-Agent: Asynchronous WinHTTP/1.0..Host: newwolfs21.mezoka.com..Content-Length: 44..Connection: Keep-Alive....CyoKCy0149093D15B2C0A1855DD9B6B5 F51362DCyoK	Add to Whitelist Report False Positive Download Signature
Mar 11 21:08:33 GMT+0900	2015753	CY1 TROJAN Pincav.cjvb Checkin	newwolfs21.mezoka.com	POST /mits/logon.php HTTP/1.1..User-Agent: Asynchronous WinHTTP/1.0..Host: newwolfs21.mezoka.com..Content-Length: 44..Connection: Keep-Alive....CyoKCy0149093D15B2C0A1855DD9B6B5 F51362DCyoK	Add to Whitelist Report False Positive Download Signature
Mar 11 21:08:33 GMT+0900	8926319	CY AUTO TROJAN Generic ccaed7c3c6e58a2844c9896246997f62 HTTP Callback 8926319	newwolfs29.mezoka.com	POST /docx/logon.php HTTP/1.1..User-Agent: Asynchronous WinHTTP/1.0..Host: newwolfs29.mezoka.com..Content-Length: 44..Connection: Keep-Alive....CyoKCy0149093D15B2C0A1855DD9B6B5 F51362DCyoK	Add to Whitelist Report False Positive Download Signature

脅威の特定と対応時間を大幅に短縮

インシデント対応に掛かるプロセス	手動による対応	JATPの自動対応
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

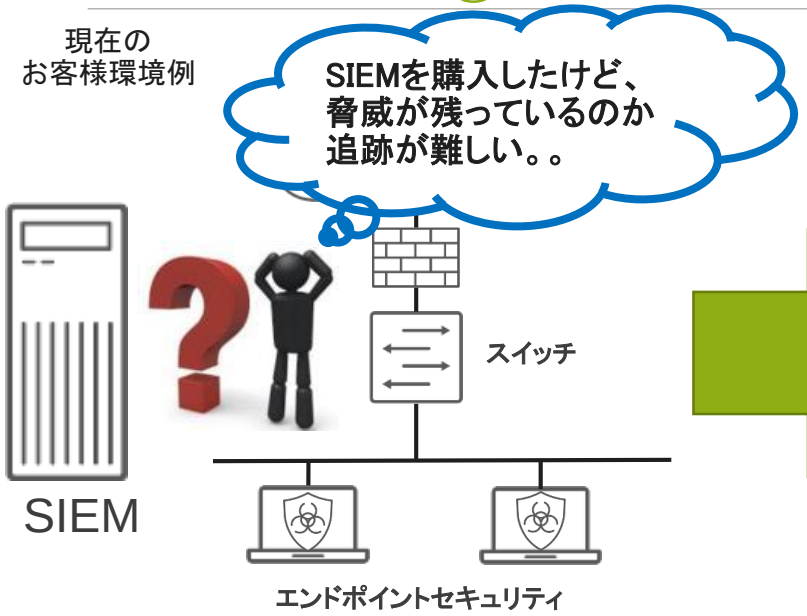


ユースケース⑤（個人の感染状況を確認）

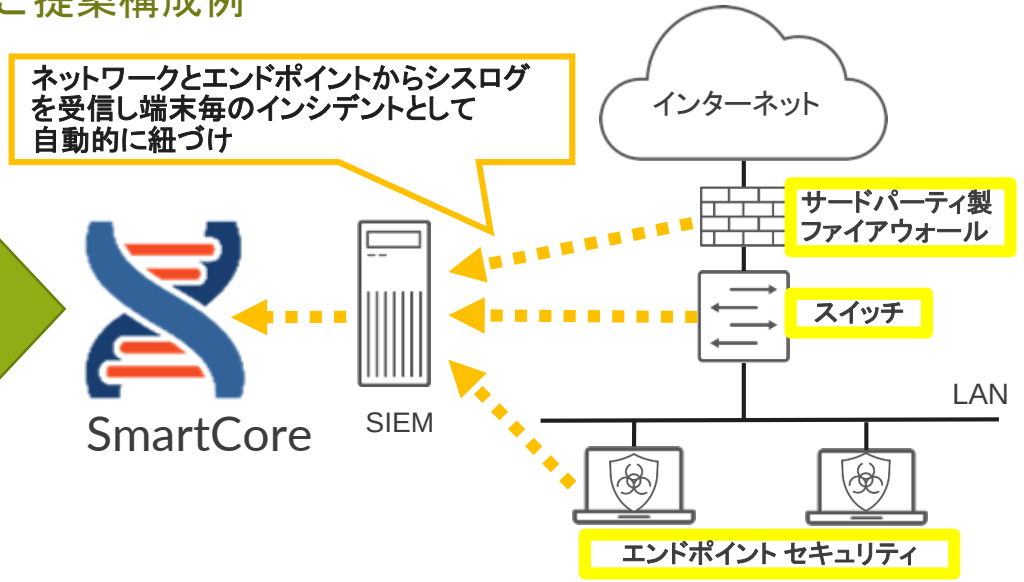


ユースケース⑥（SIEMの代わりにキルチェーンを可視化）

現在の
お客様環境例



ご提案構成例



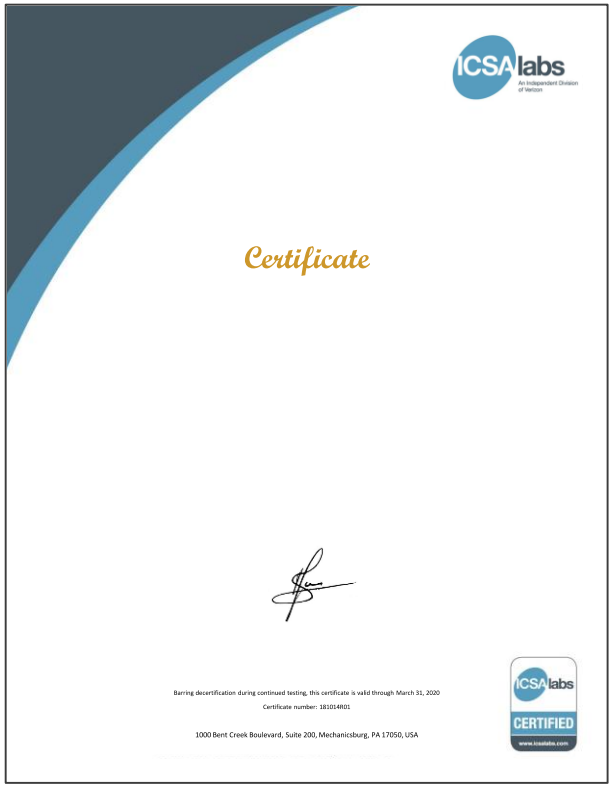
お客様のご環境とニーズ

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。

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。

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%

Fig. 1 – High Detection Effectiveness & Few False Positives

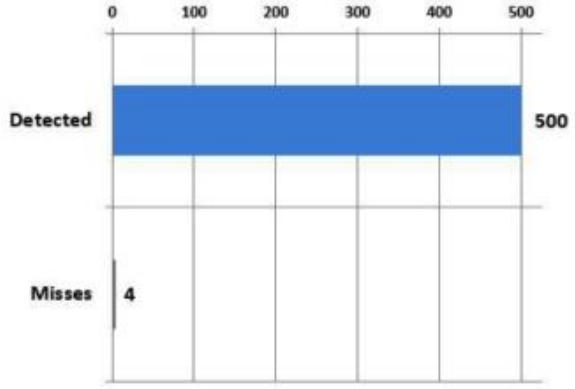
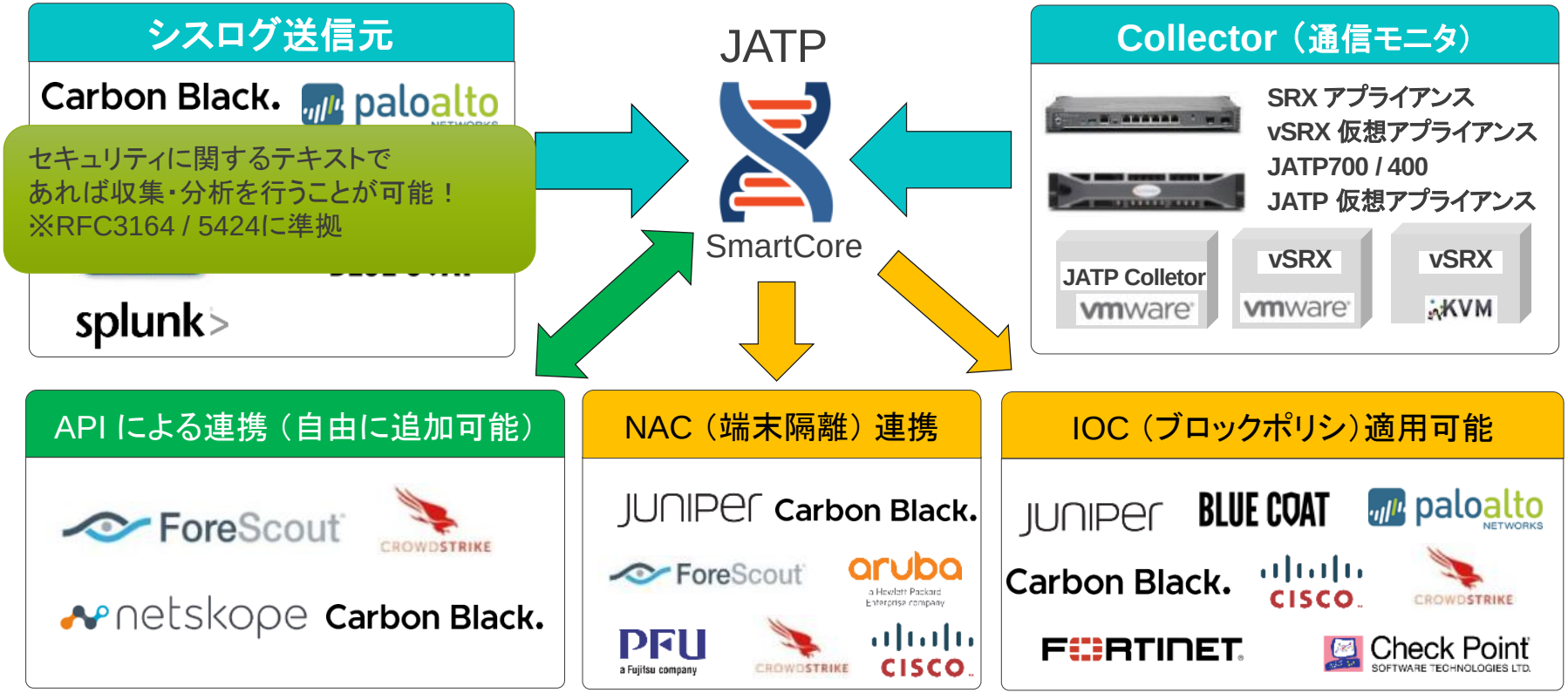


Fig. 2 – Detected 500 of 504 *New & Little-Known* Malicious Samples

Fig. 3 – 6 Alerts on Innocuous Applications

JATPによる統合セキュリティ連携例



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

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時間の長さ

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

Juniperのセキュリティで、最先端の安全 & コストの抑制！ ！

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

ネットワーク全体にセキュリティを拡張！！