最近の情報セキュリティ脅威と今後の対応について

～今後のパロアルトネットワークス戦略～

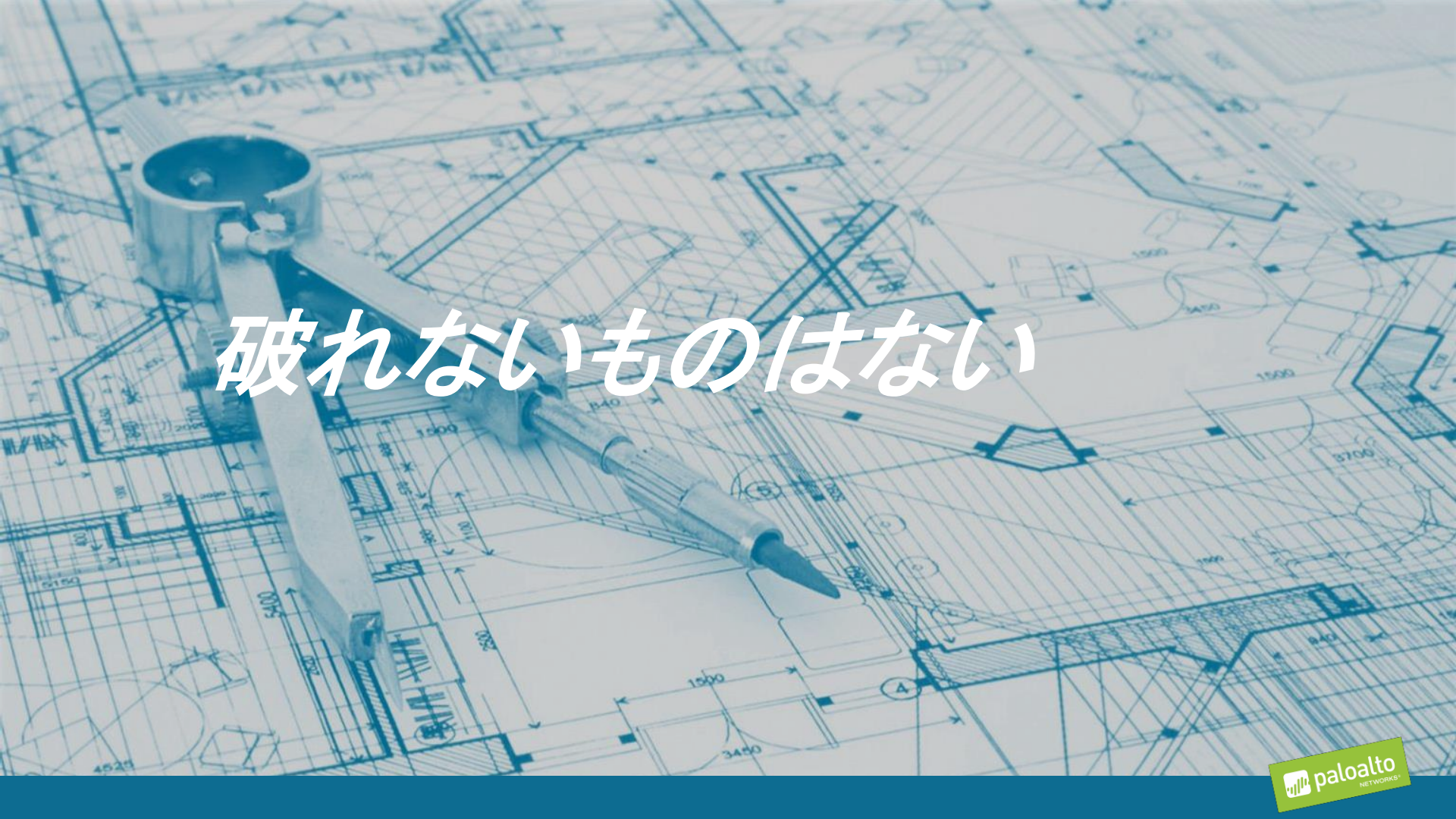
パロアルトネットワークス株式会社
シニアビジネスデベロップメントコンサルタント
藤生 昌也

2018年 9月

PROTECTING OUR DIGITAL WAY OF LIFE

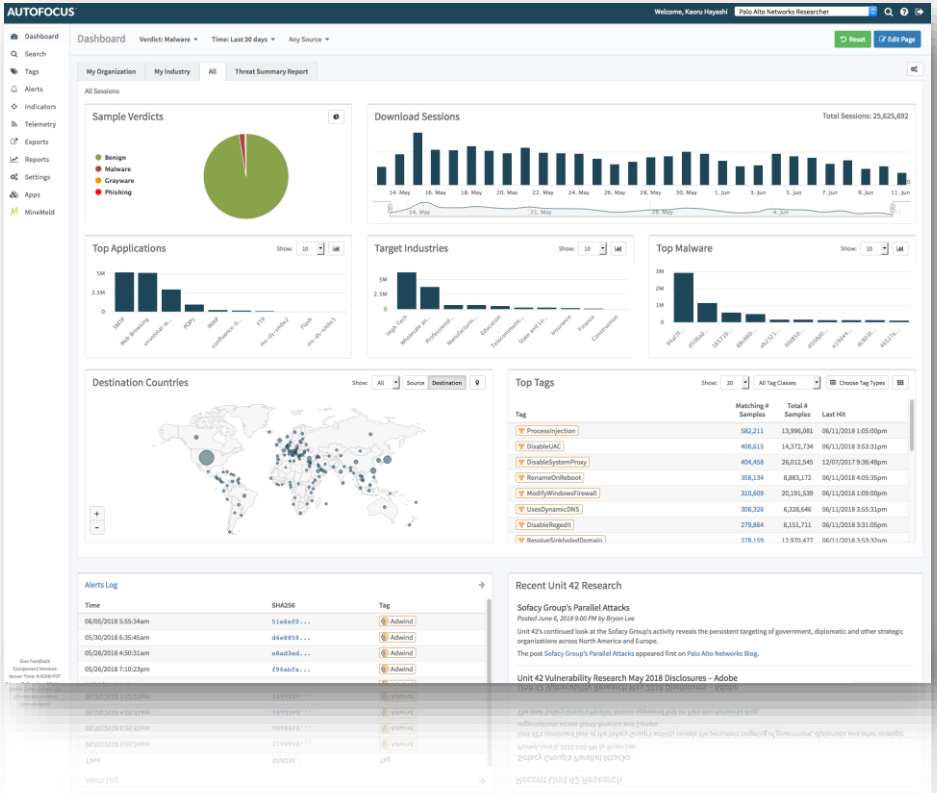

THIS TIME IN HISTORY
paloalto
NETWORKS


TRUST
paloalto
NETWORKS®


破れないものはない


高度な自動化された攻撃
paloalto
NETWORKS

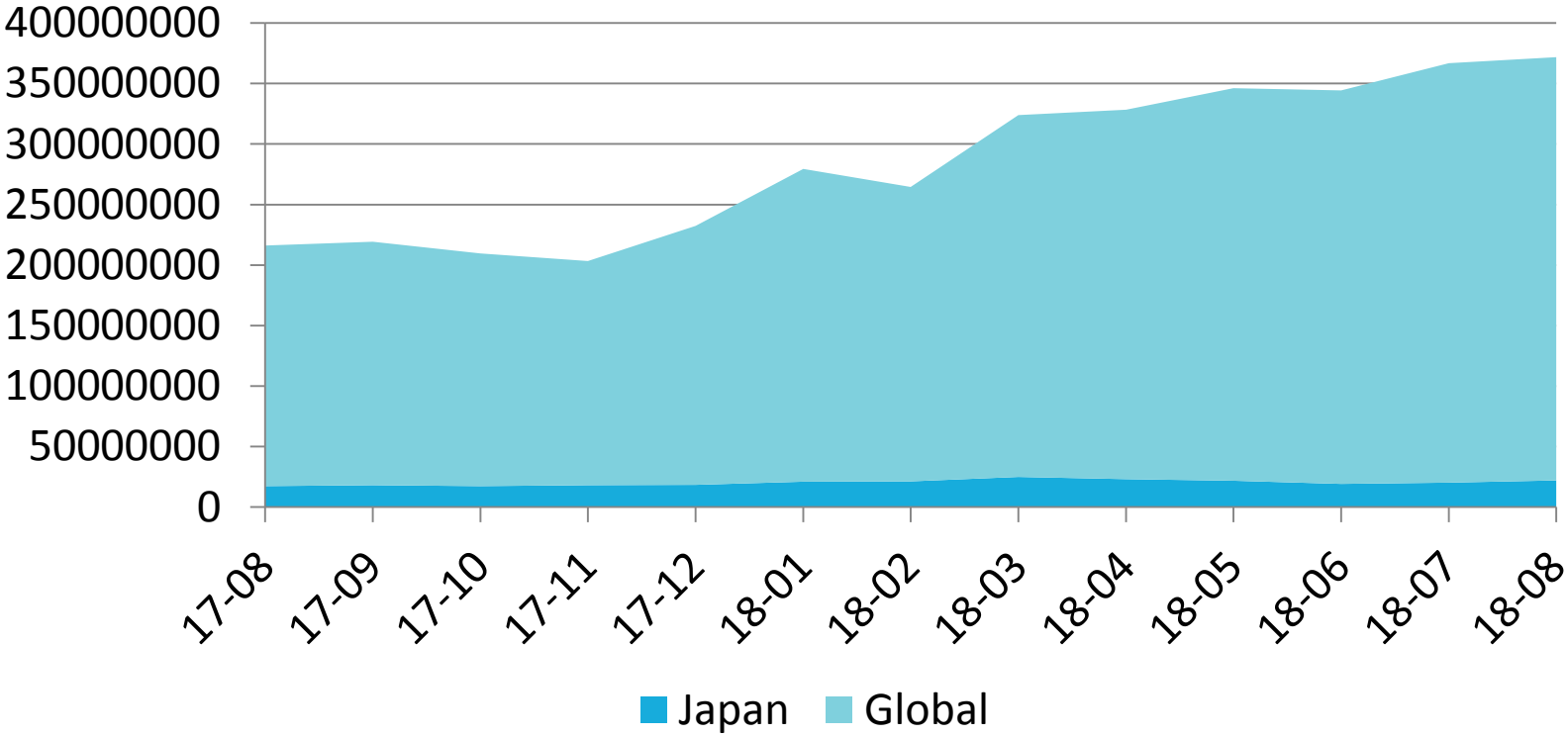
月次脅威概要


AUTOFOCUS
Dashboard
Sample Verdicts
Benign
Malware
Grayware
Phishing
Download Sessions
Total Sessions: 25,625,692
Top Applications
Target Industries
Top Malware
Destination Countries
Top Tags
Alerts Log
Recent Unit 42 Research
Sofacy Group's Parallel Attacks
Unit 42 Vulnerability Research May 2018 Disclosures – Adobe

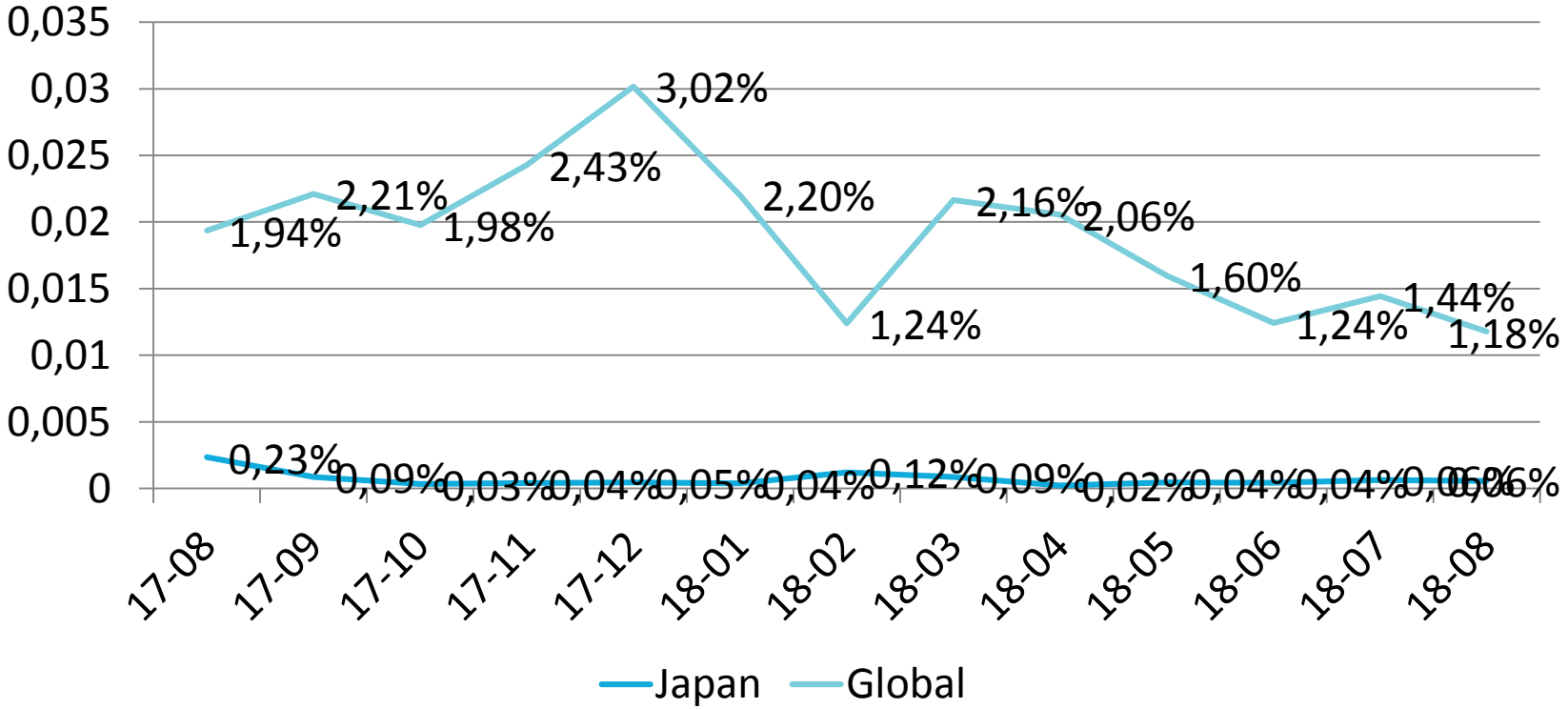
Global – マルウェアセッション: 2018年4月国別ワースト10

国・地域	セッション
アメリカ	1171456
ブラジル	551099
日本	382545
イタリア	148344
イギリス	105680
韓国	102547
トルコ	74470
カナダ	68674
中国	66006
台湾	58061

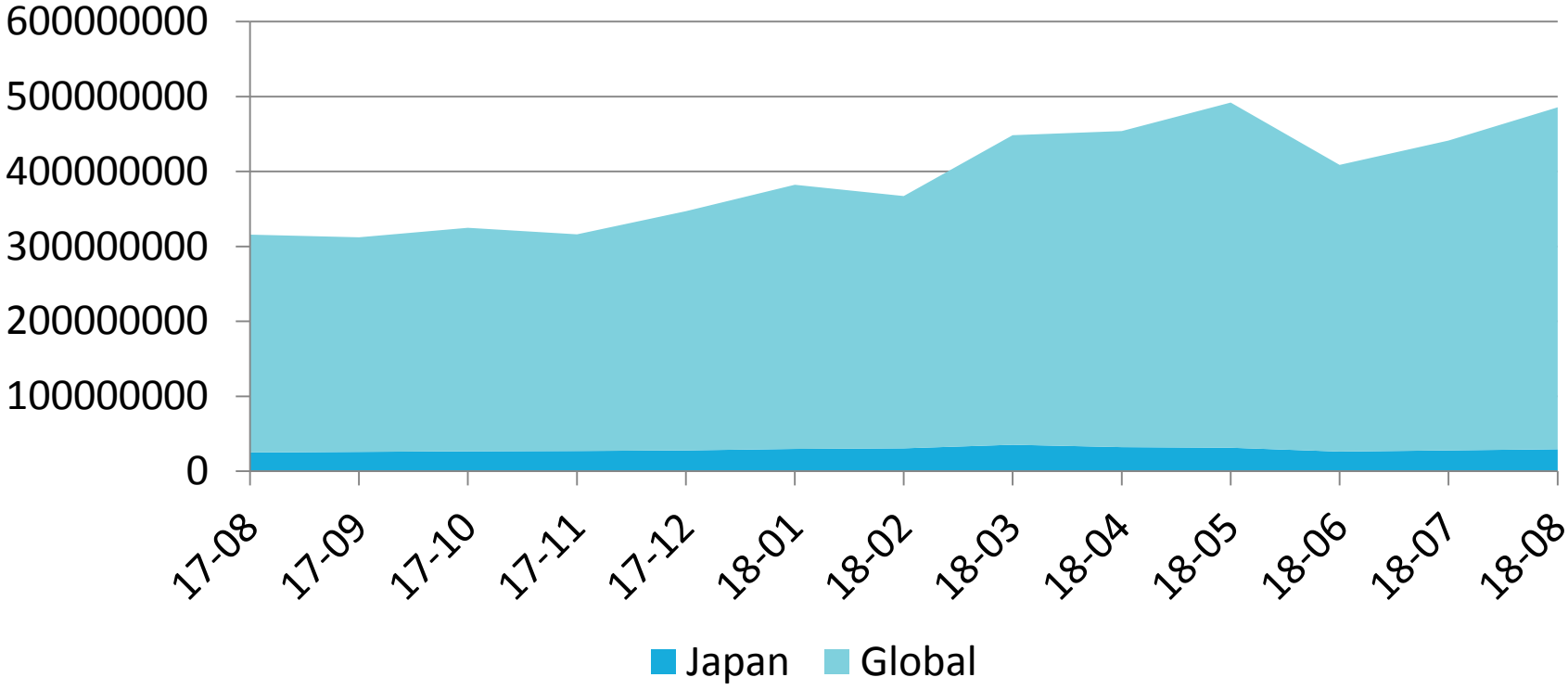
WildFire分析ファイル数の推移



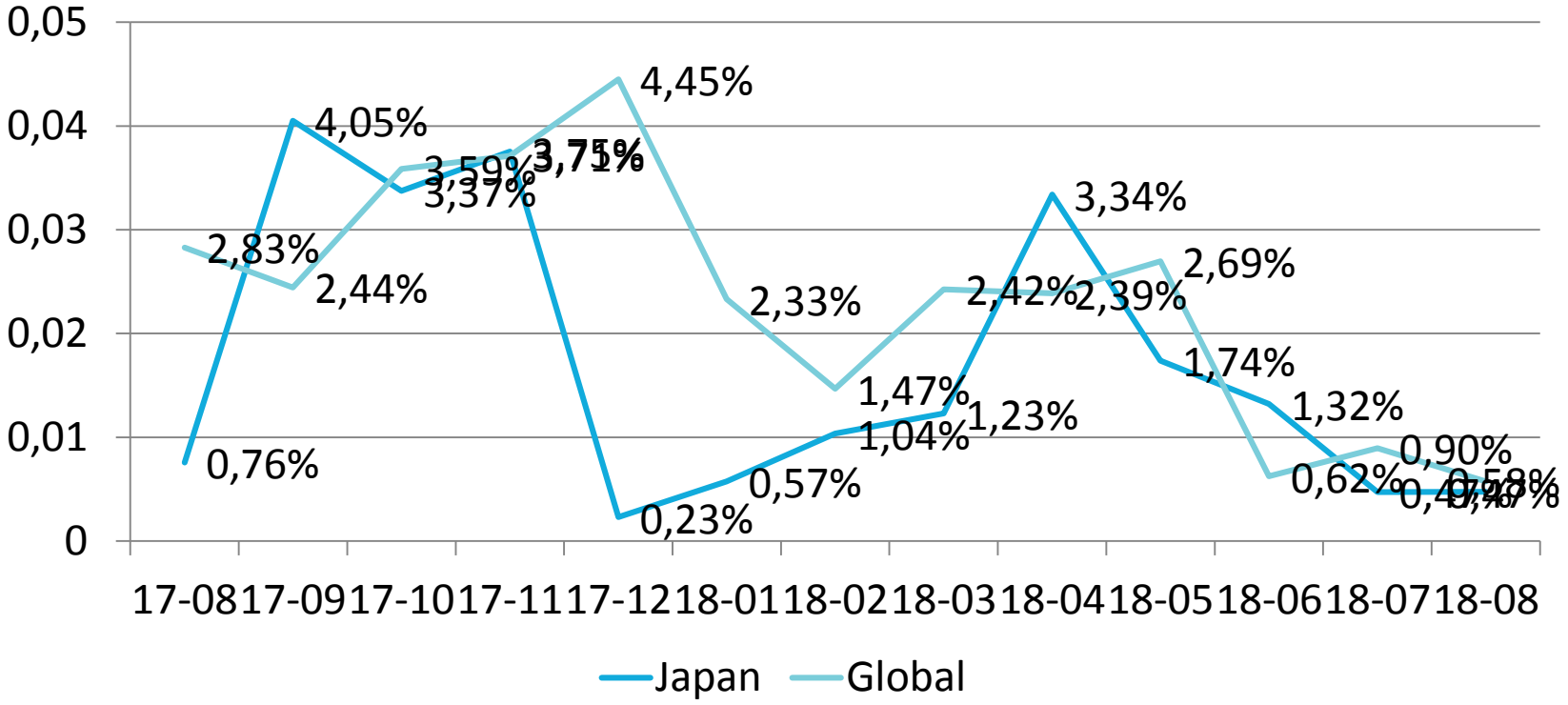
全分析ファイル中の未知マルウエアの割合



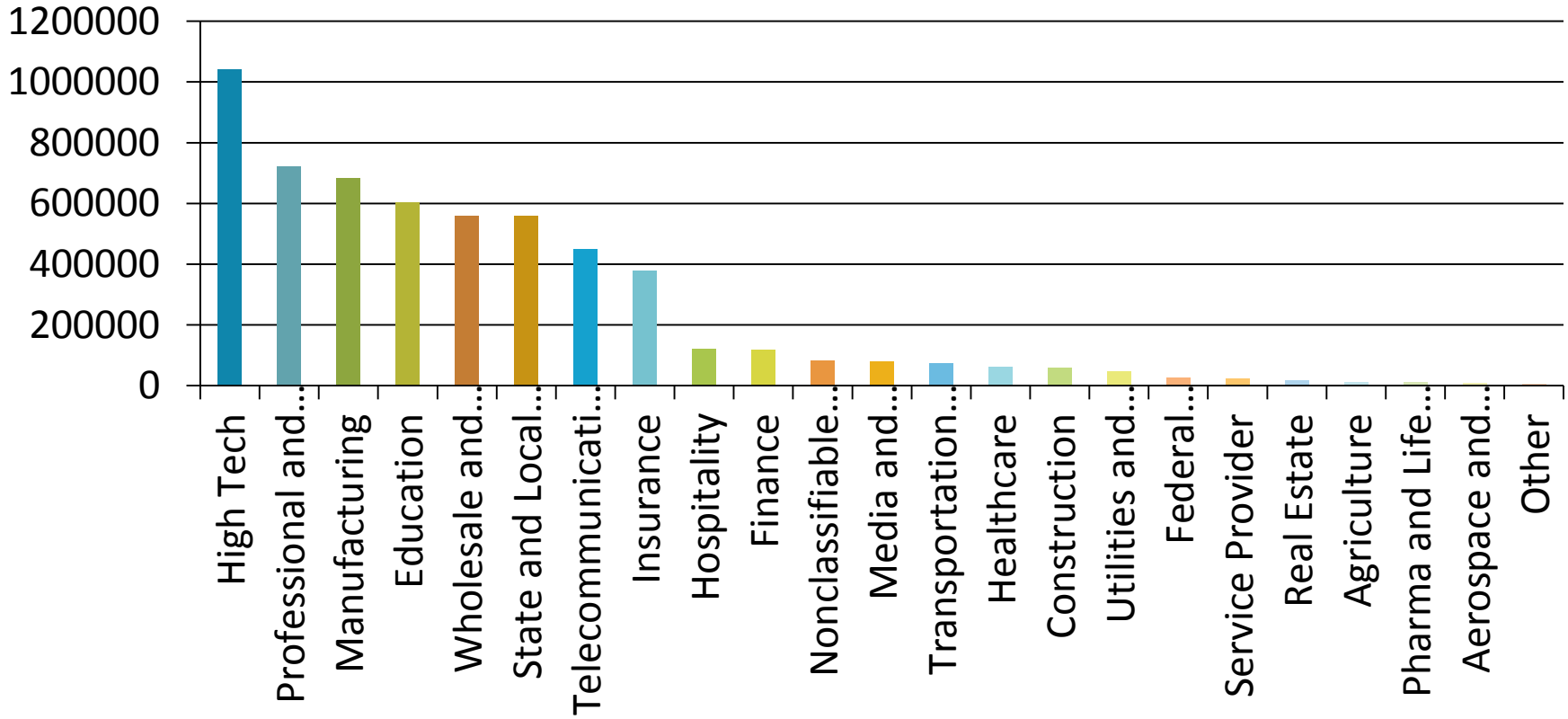
WildFire分析セッション数の推移



全分析セッション中の未知マルウエアの割合



Global：2018年4月ワースト 業界別



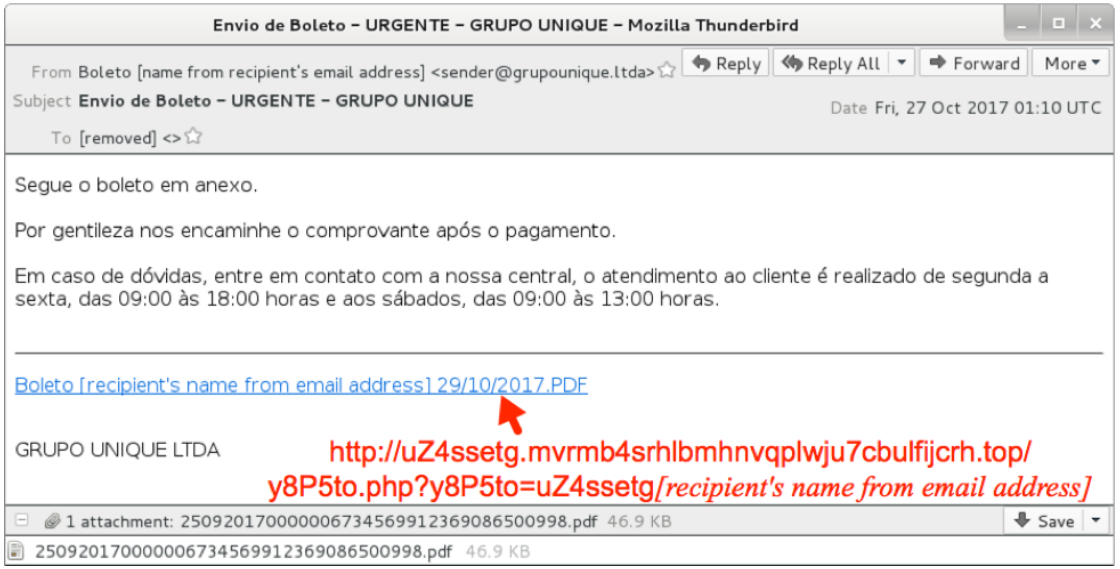
Global – 2018年4月マルウェア　セッション数: トップ 5 アプリケーション

アプリケーション	セッション数	前月のセッション数
smtp	3015021	2499641
web-browsing	1675099	2151851
pop3	640310	536194
confluence-base	165565	166175
imap	110393	32639

Global – ワースト10 マルウェア

ファイルタイプ	マルウェア	数
PDF	BoletoMestre	495325
Microsoft Excel 97 - 2003 Document	Shiotob	140463
PDF	BoletoMestre	63205
Microsoft Word 97 - 2003 Document	GandCrab	62240
Microsoft Word 97 - 2003 Document	GandCrab	58182
Microsoft Word 97 - 2003 Document	GandCrab	52214
Microsoft Word Document	TrickBot	50916
Microsoft Excel 97 - 2003 Document	Shiotob	50896
Microsoft Excel 97 - 2003 Document	Shiotob	49204
Microsoft Word 97 - 2003 Document	GandCrab	47010

BoletoMestre オンライン決算を悪用した例



Windowsコンピュータに情報を盗むトロイの木馬を感染させるように設計

出展: https://researchcenter.paloaltonetworks.com/2017/12/unit42-master-channel-the-boleto-mestre-campaign-targets-brazil/

Global まとめ

2018年3月

ブラジルをターゲットにした不正送金マルウェアキャンペーンがあったため大量のドキュメントがメールにて配信。そのため、ブラジルで検出されたセッションが増加。

Emotet不正送金マルウェアが弊社製品で多数検出。
Emotetはメールに添付されたリンクのクリック、もしくは添付されたWordドキュメントに埋め込まれたマクロによる端末にPEファイルがダウンロード。

2018年4月

ワースト10に入ったマルウェアはいずれもドキュメントをメールでばらまくもの。しかも最終的なペイロードは実質以下の3種類のみ。特定の国を狙うものと、不特定多数のものがあり。

- **ブラジル向け BoletoMestre**
- 日本向け　Shiotob
- 不特定多数向け　GandGrab

GandGrab は、下火になってきているランサムウェアの中でも、飛び抜けてアグレッシブに感染を広げているものです。バラマキ型メールだけでなく、Rig Exploit Kit を使って感染させようとする活動も観測。

2018年　脅威予測

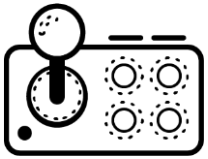
- **医療・ヘルスケア**: 機械学習が変える医療とサイバーセキュリティ
- **ICS/SCADA**: 産業用制御システムや監視制御システムに対する
  サイバー攻撃の自動検出・自動対応が進む
- **クラウドサービス**: データは次世代の石油 その完全性に注力を
- **脅威の変遷**: ソフトウェアサプライチェーンの大侵害時代が始まる
- **小売業**: 安全性の低いデバイス、匿名通貨高騰がもたらす未知の脅威が
  小売業界に影響
- **法律・規制**: 物理的破壊を伴うセキュリティ侵害が増加、規制導入相次ぐ
- **IoT**: IoT で消失する公私の境界
- **エンドポイント**: ランサムウェアの蔓延は続く

産業用制御システムや監視制御システムに対する サイバー攻撃の自動検出・自動対応が進む

2018

PREDICTIONS & RECOMMENDATIONS

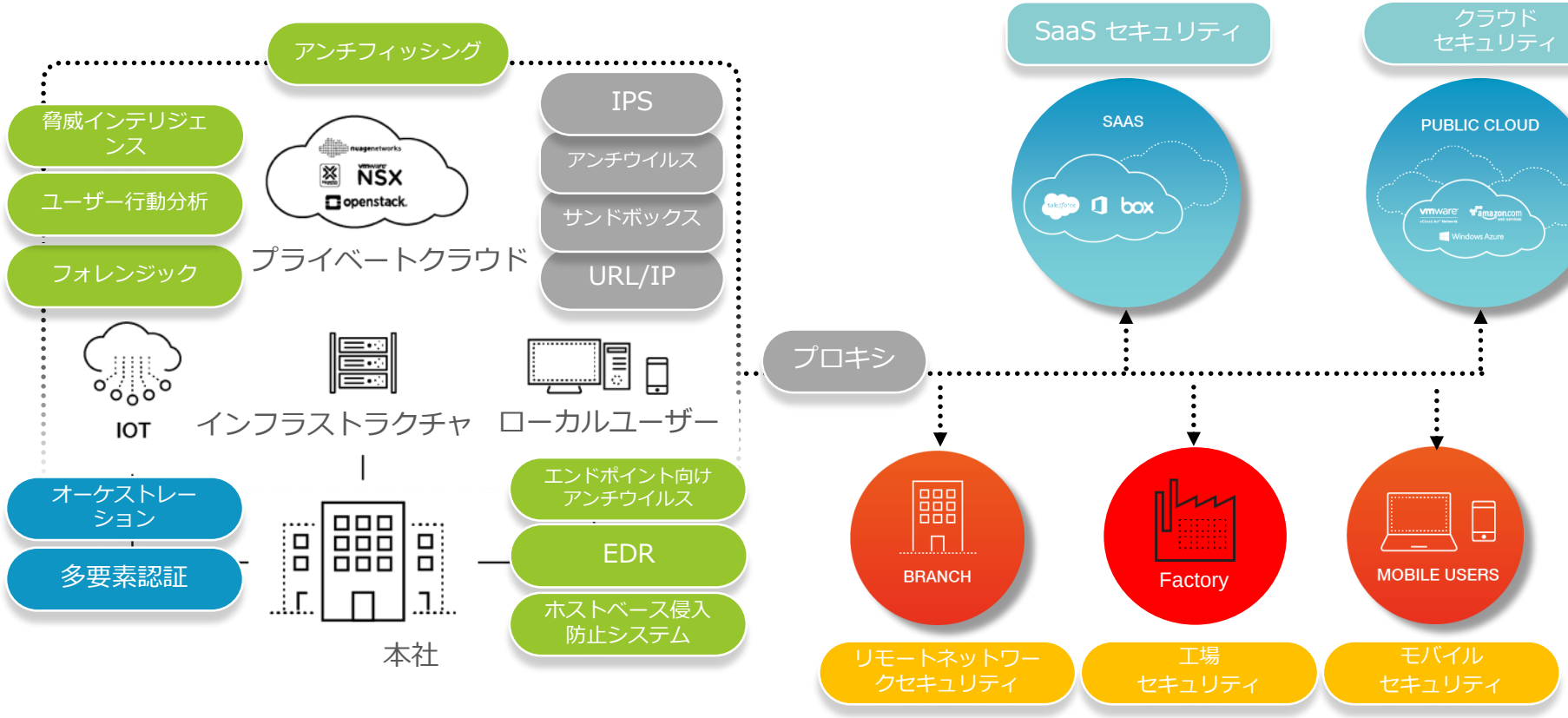
ICS/SCADA



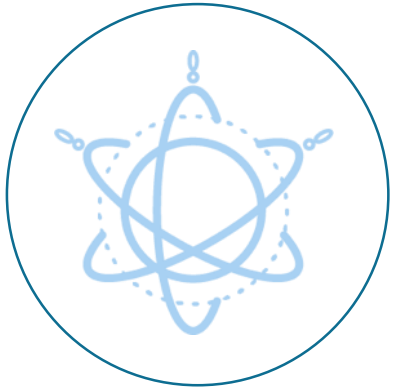
- 産業用制御システム（ICS）、監視制御システム（SCADA）は高度サイバー攻撃の標的になりやすい
- 2018 年は攻撃への自動検出・自動対応導入が進む
  - 実証実験で手応えを得た組織の増加
  - 重要インフラへの大規模攻撃頻発、損害の深刻化
- SIEM 機器・センサとシームレスに連携可能かつ設定上の柔軟性が高いセキュリティ製品で自動化を


セキュリティにも100%はない

Everywhere: ユーザー/データ/アプリケーション



今日のセキュリティは正常に機能しません



不完全な可視化と
リアクティブな防御

大量の
アラートとログ

孤立したセキュリティ
システムと
手動中心の脅威対応

敵を知り

攻撃する側に聞いてみた

匿名を条件に米国・英国・ドイツの304人の脅威の”専門家”を対象に調査を実施

- 回答者のうち、21%は実際の攻撃に関与
- 79%は脅威コミュニティに積極的に参加
- 全員が最新のハッキングメソッドやツールに精通

攻撃者のモチベーション、手口、考え方を知る

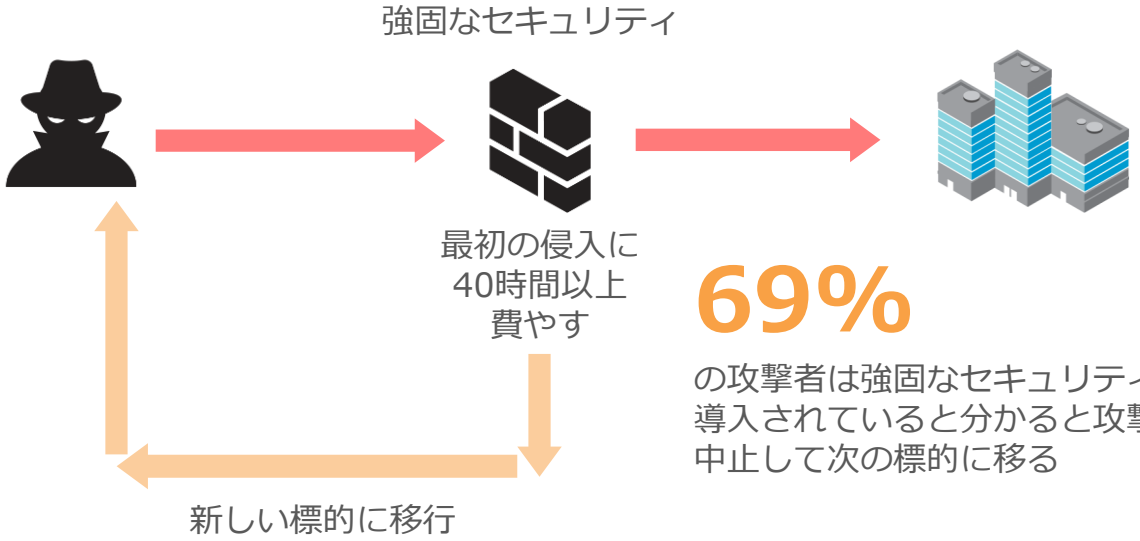
攻撃者にとってのモチベーション

69%
は経済的な利益が
モチベーション

72%
は特に理由なく標的の
企業を選んでいる

攻撃者のほとんどは特定の企業を狙うよりも
手軽 にそして簡単に **利益** を得られる標的を選んでいる

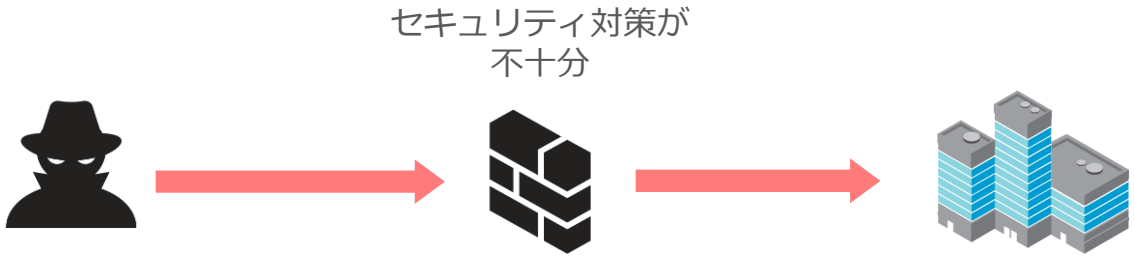
攻撃者はより簡単な標的を探す



69%

の攻撃者は強固なセキュリティが導入されていると分かると攻撃を中止して次の標的に移る

簡単なターゲット



一般的なレベルのセキュリティ対策を導入している企業でデータを入手するまでに掛かる時間は平均して **3 日 (70 時間) 程度**

侵入から検出までの平均は205日

攻撃用ツールの進化

攻撃で利用できるツール

シンプル & 自動化

マルウェア配信
リモートアクセス
改ざんされたWebサイト
…その他多数!

Malicious "AntiHacker" Tool Installs DarkComet RAT to Spy on Syrian Activists

y Michael Mimoso Follow @mike_mimoso August 21, 2013 , 4:00 am

U.S. Department Of Labor Website Discovered Hacked, Spreading PoisonIvy

攻撃者にとってより優位な状況に

入手可能な
マルウェア&
エクスプロイト

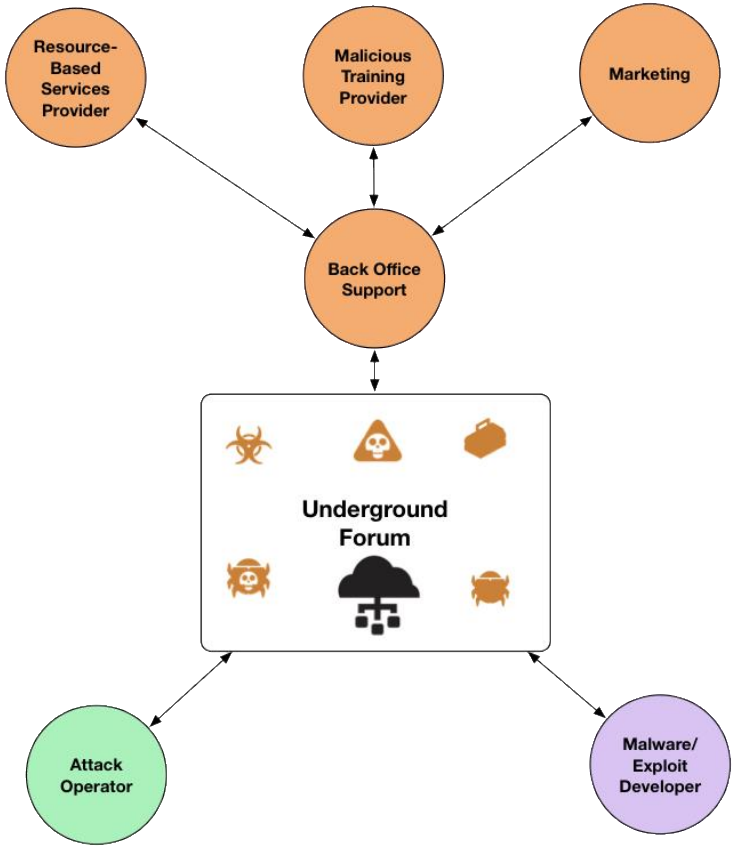
有効で自動化
されたツール
キット

劇的に安い
コンピューティング
パワー

攻撃の成功が
より簡単に

サイバー攻撃において攻撃者が優位になるロジック

進む攻撃者の分業化



https://www.paloaltonetworks.jp/company/in-the-news/2016/160831_unit42-exploring-the-cybercrime-underground-part-2-the-forum-ecosystem.html

増加・多様化する脅威への対抗

- 攻撃者数の増加と多様化
  - 毎月数百万種類見つかる新規のマルウェア
  - 様々な動機、リソースそして戦術
  - ツール化、自動化、クラウド、サービスが拡充
  - ビットコインやダークWeb等、個人を特定される可能性が低い技術が浸透
  - 分業化が進み、攻撃者自身の技術レベルが問われなくなってきた
  - 攻撃側の参入障壁が低い

- 自助努力で対応可能？
  - 膨大なコストとリソース
  - 本業へのインパクト

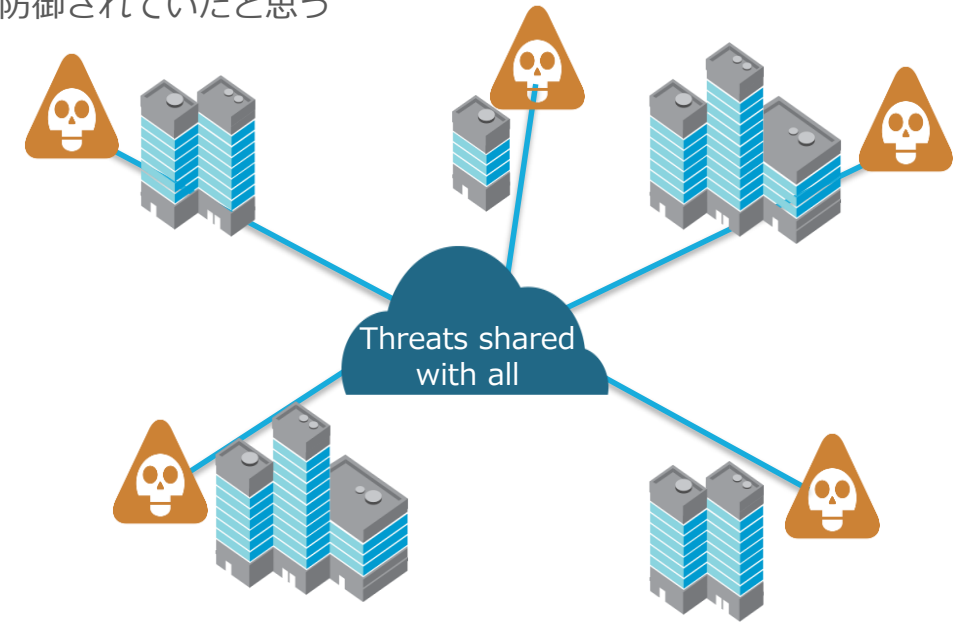
HOW?

どうすればいいのか?

脅威情報の共有は攻撃者にとって厄介

39%

の攻撃は脅威情報の共有があれば
防御されていたと思う



攻撃者にとって不利な状況を作るために

攻撃の成功率を下げる

=

手間・コストがかかる攻撃になるようにする

+

新しい脅威に対する防御を自動化

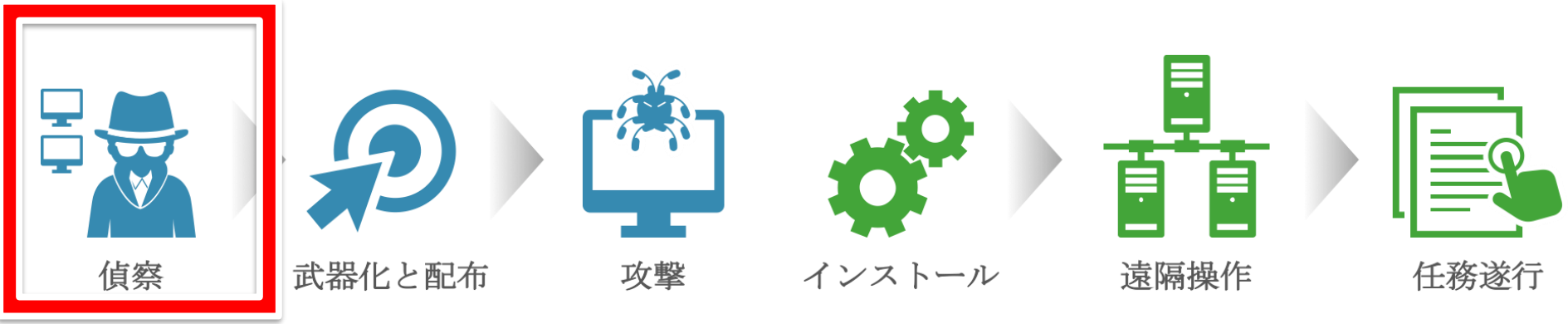
+

脅威やリスクについて可視化

+

脅威インテリジェンスの共有

サイバー攻撃ライフサイクル

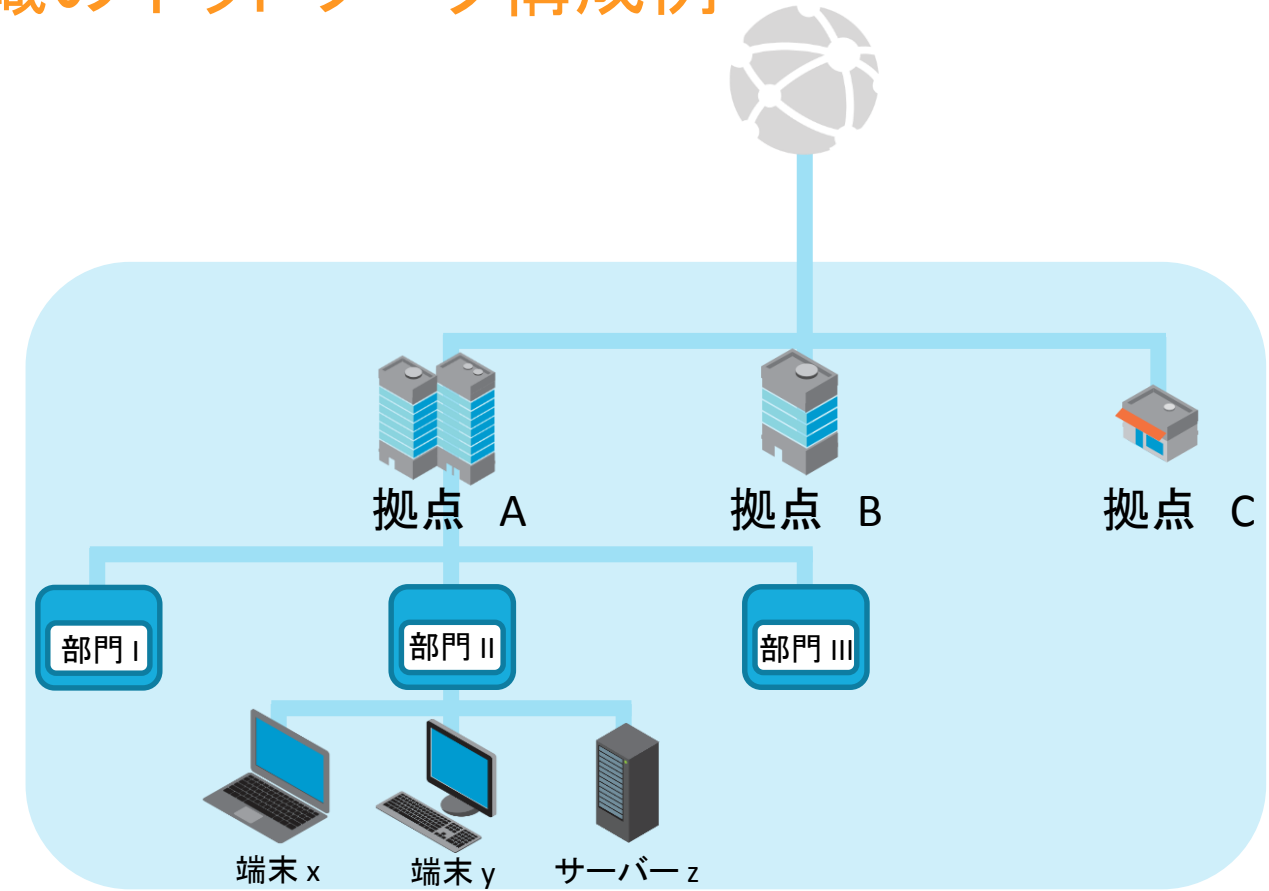


攻撃者から見たターゲット

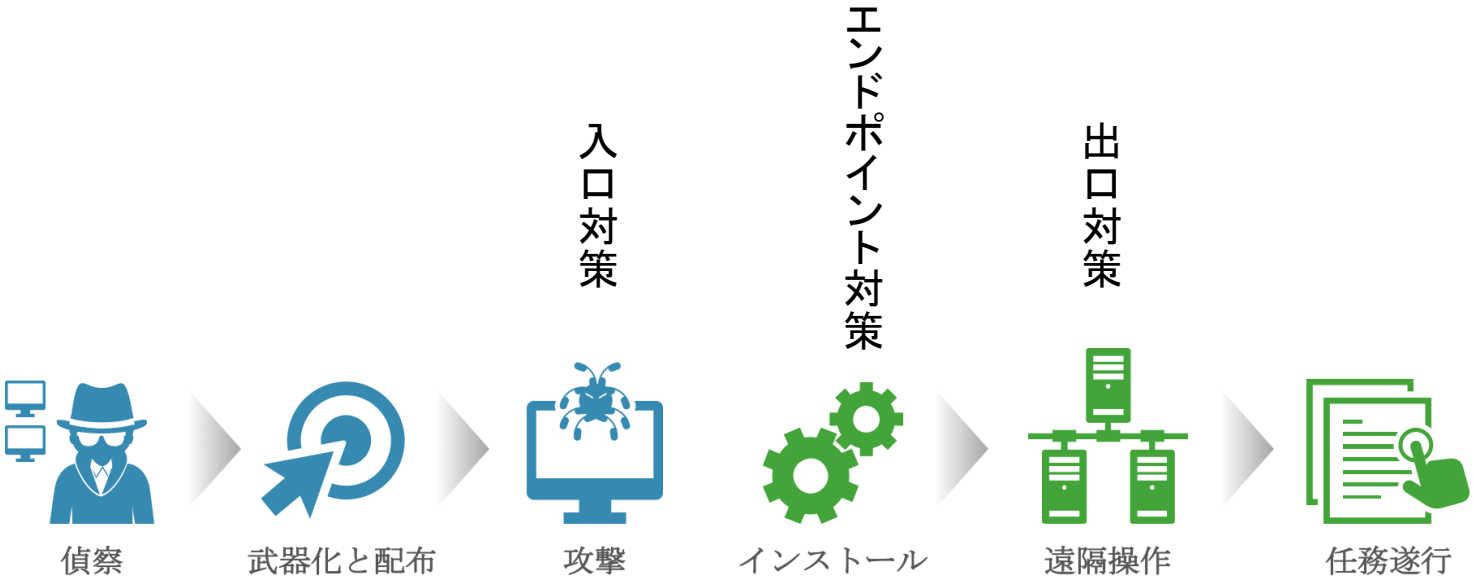
- 内部には多くの端末、サーバ、データがある
- 内部に入らないと何もわからない

最初の感染を足がかりにして、内部拡散・移動を行う

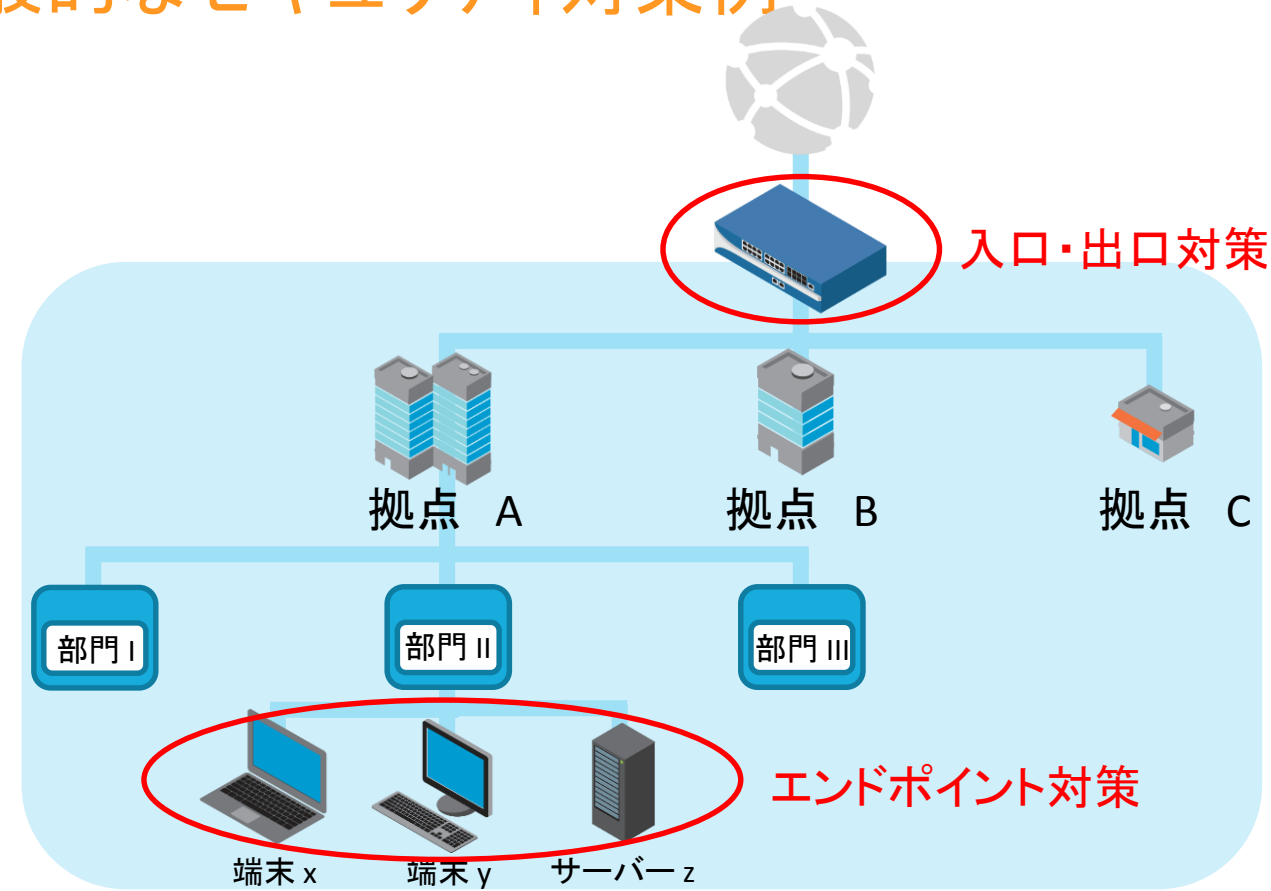
組織のネットワーク構成例



攻撃ライフサイクルからみた対策

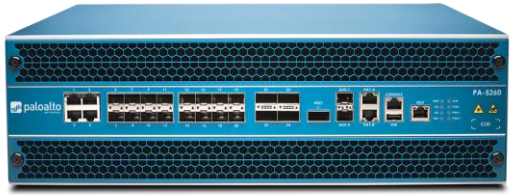


一般的なセキュリティ対策例



次世代ファイアウォール - 入口/出口対策 -

- ポート番号やプロトコル・暗号化に関わらず、全ての**アプリケーションを識別**し、その中に埋もれる非正常（不明なアプリケーション）通信までも**すべて可視化**
- IPアドレス、ロケーション、デバイスを問わず、ユーザーを識別および制御
- 全ての通信を利用**ユーザ単位で識別**して制御＆記録
- 脆弱性攻撃、情報漏洩、マルウェア等の**既知の脅威に対してリアルタイム防御**
- **未知の脅威はクラウド活用でリアルタイム分析**して、結果を自動的な防御にフィードバック
- 従来のネットワーク環境以外に、**仮想化環境**ならびに**モバイル環境**に対しても同様のセキュリティを提供可能



次世代エンドポイントセキュリティ *Traps* – エンドポイント対策 -

マルウェア／
ランサムウェア阻止

エクスプロイト／
ファイルレス攻撃を阻止

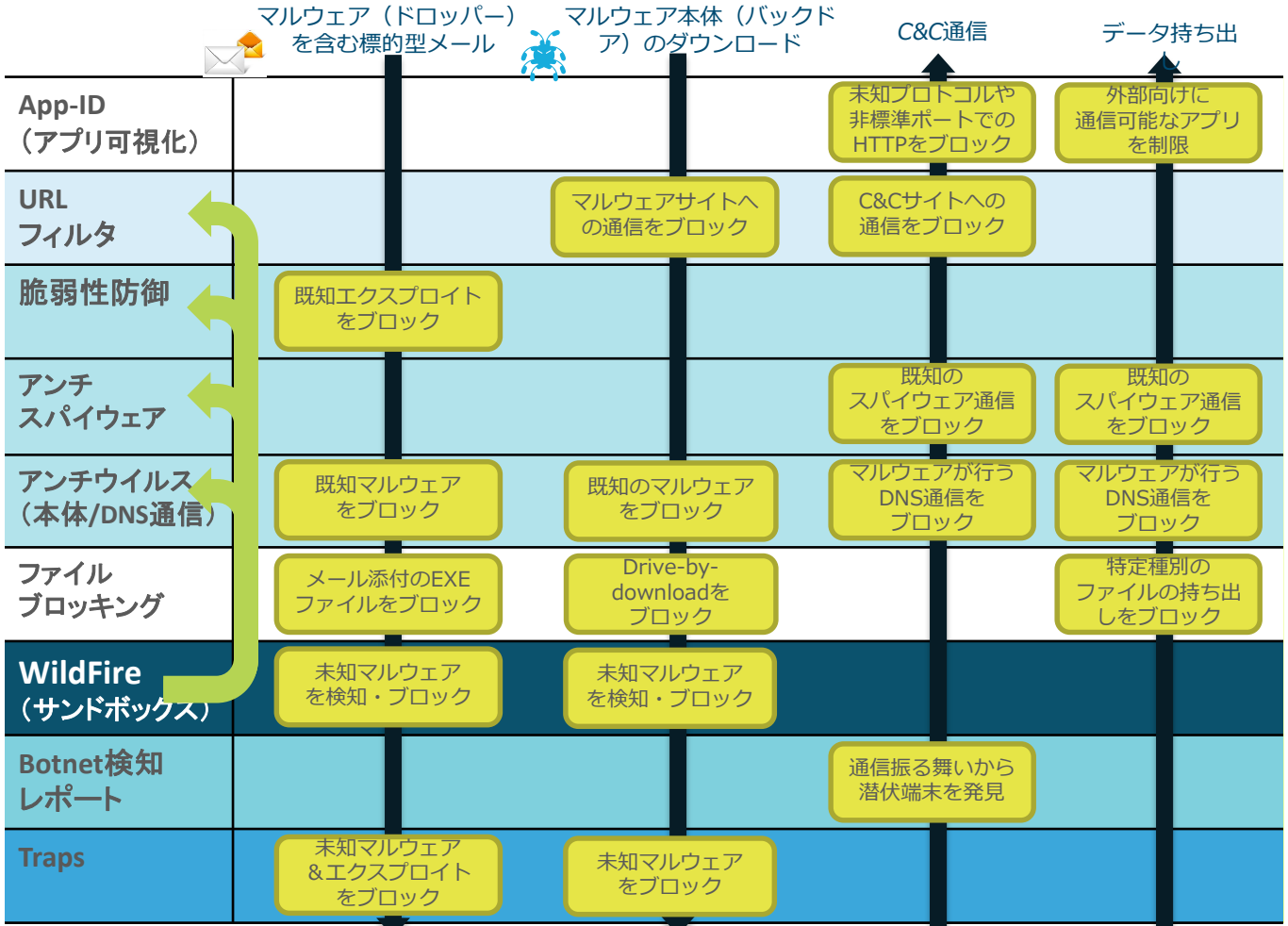
標的型攻撃の阻止

正確な阻止:
既知と未知の両方の脅威

攻撃テクニック
（ふるまい）による保護

高速な検知 & 高度な攻撃に
対する対応

攻撃の全てのステージに多層的な機能で対応



HOW?

己を知れば

セキュリティ戦略のためのコンパス

1

完全な可視化
可視化は必須

2

素早い脅威対応
リアルタイム解析
アクション自動化

3

一貫した
セキュリティ
セキュリティシステムの
基盤化

サイバー攻撃の防止

ネットワーク　エンドポイント　クラウド

- 可視化

サイバー攻撃の防止

- 可視化
- 攻撃対象領域の縮小

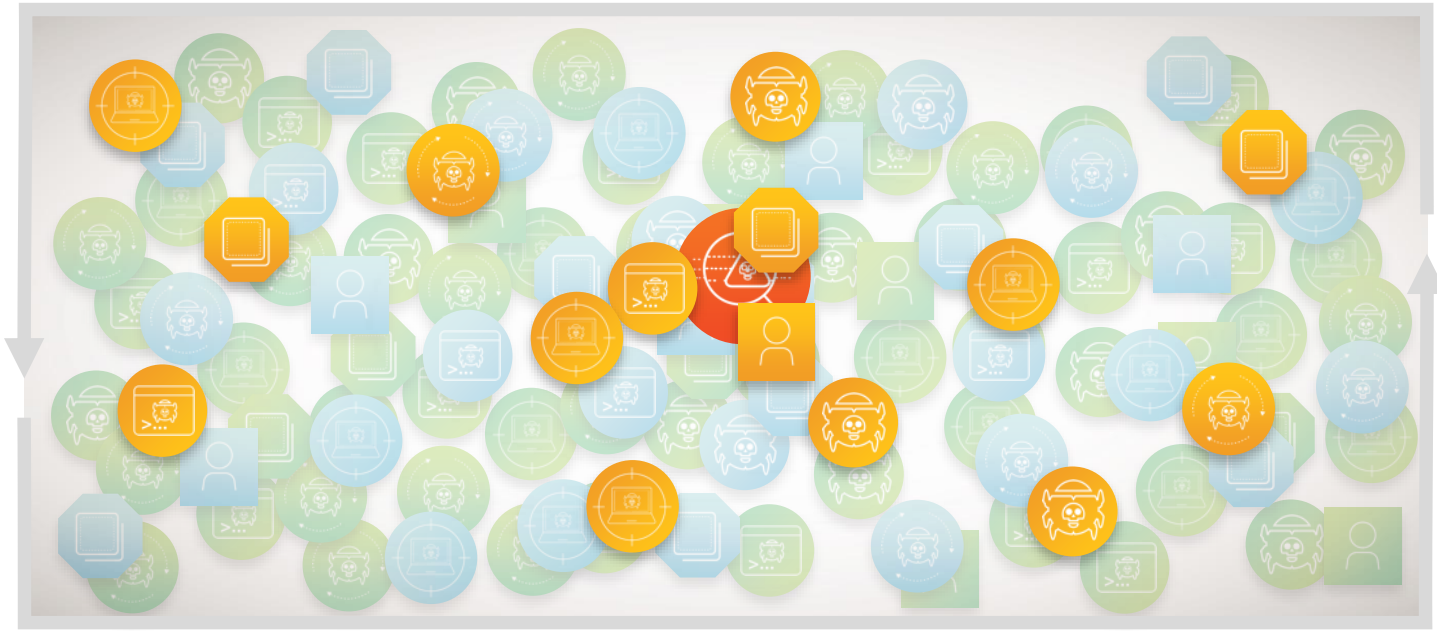
マニュアルでの分析工数を削減

自動化

サイバー攻撃の防止

- 可視化
- 攻撃対象領域の縮小
- 既知の脅威の防止

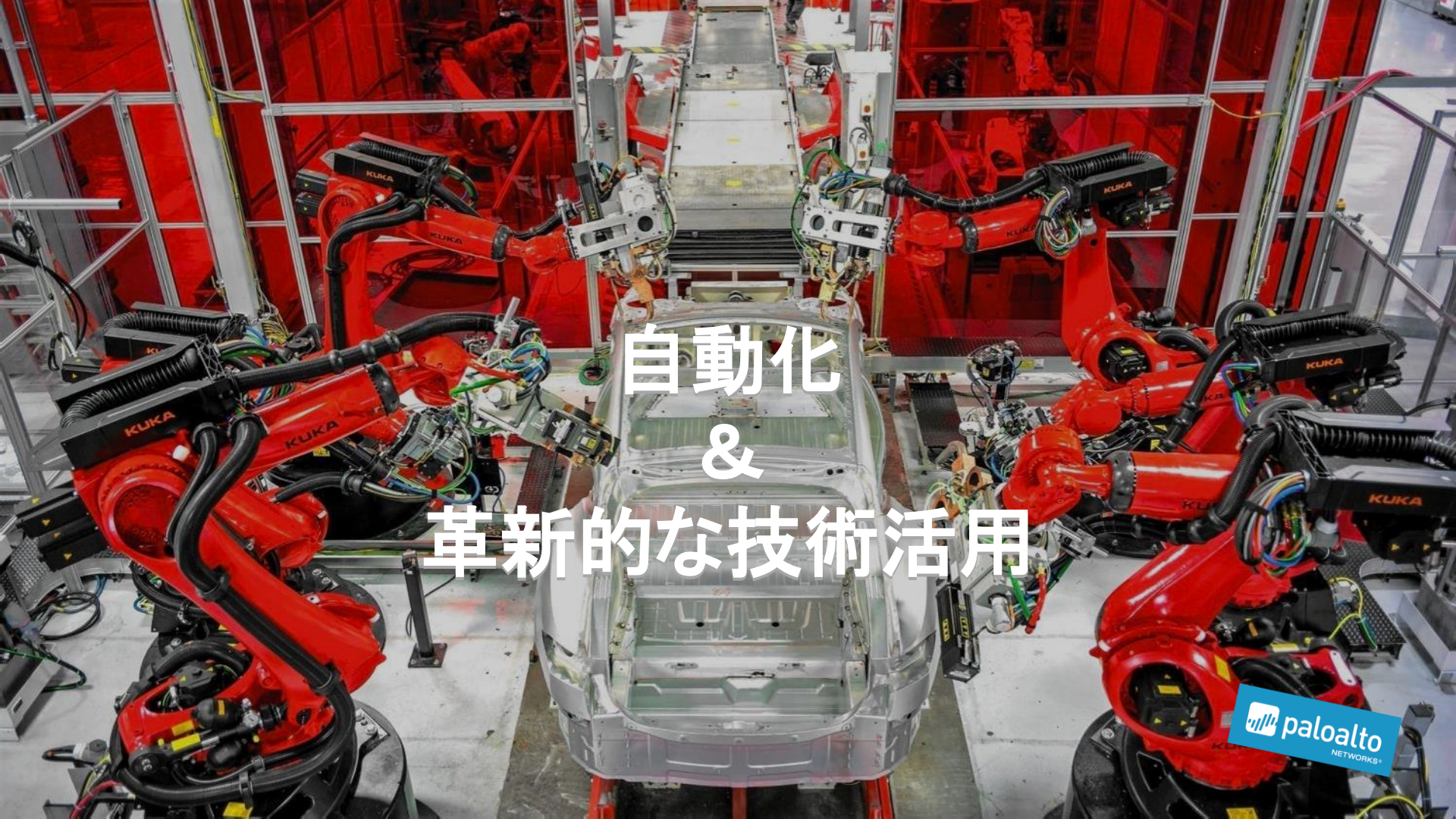
マニュアルでの分析工数を削減



自動化

サイバー攻撃の防止

- 可視化
- 攻撃対象領域の縮小
- 既知の脅威の防止
- 未知の脅威への対策


自動化
&
革新的な技術活用
KUKA
paloalto
NETWORKS

自動化された、即効性のある阻止の例

1

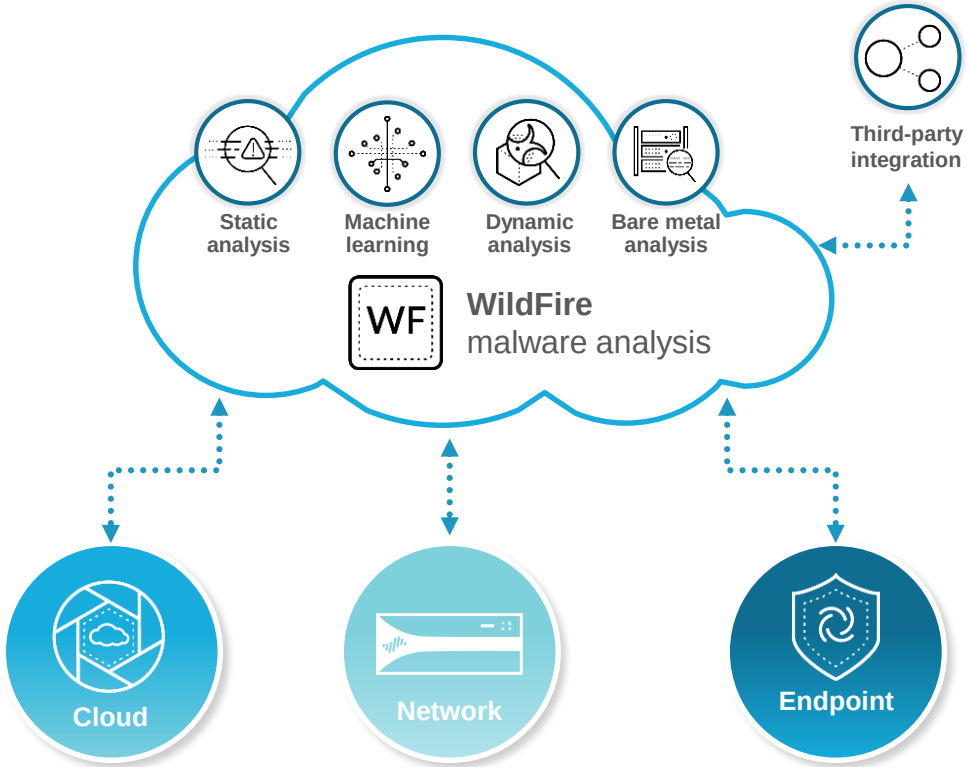
次世代ファイアウォール、Aperture、Trapsが、未知のファイルやリンクをWildFireへ送付

2

WildFireは未知を解析
判定結果を出すとともに、
脅威インテリジェンスを共有

3

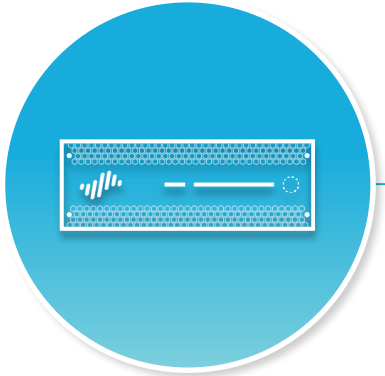
脅威情報を受け取り、ネットワーク、エンドポイント、クラウドが新たな脅威を防御するよう更新




プラットフォームの活用
paloalto
NETWORKS

プラットフォームに必要となる優れた基盤

次世代ファイアウォール



ネットワーク セキュリティ におけるリーダー

市場の3倍の成長率

次世代エンドポイント プロテクション

効果的な エンドポイント プロテクション

ランサムウェアとマルウェア
ファイルレス攻撃
エクスプロイト

継続的な クラウドセキュリティ

もっとも完全な クラウドセキュリティ の提供

インライン
API
ホスト

Security Operating Platform

全方位の自動化を実現するSecurity Operating Platform

サイバー攻撃への事前防御

ベストプラクティスによる容易な運用

本当に重要な業務への注力

コンテキストと分析による業務の自動化

最新のテクノロジーを容易に適用

パロアルトネットワークス、サードパーティ、お客様自身によるアプリケーション

自動化の確立

パロアルトネットワークスのプラットフォーム

パロアルトネットワークスのアプリケーション

3rd パーティパートナーアプリ

エンドユーザーアプリ

クラウドから提供されるセキュリティサービス

APPLICATION FRAMEWORK & LOGGING SERVICE

ネットワークセキュリティ

次世代ファイアウォール

GP cloud service

GP

エンドポイント向け
ネットワークセキュリティ
GlobalProtect /
GlobalProtect cloud service

次世代エンドポイントセキュリティ

TR

次世代エンドポイント
セキュリティ
Traps

クラウドセキュリティ

VM-Series

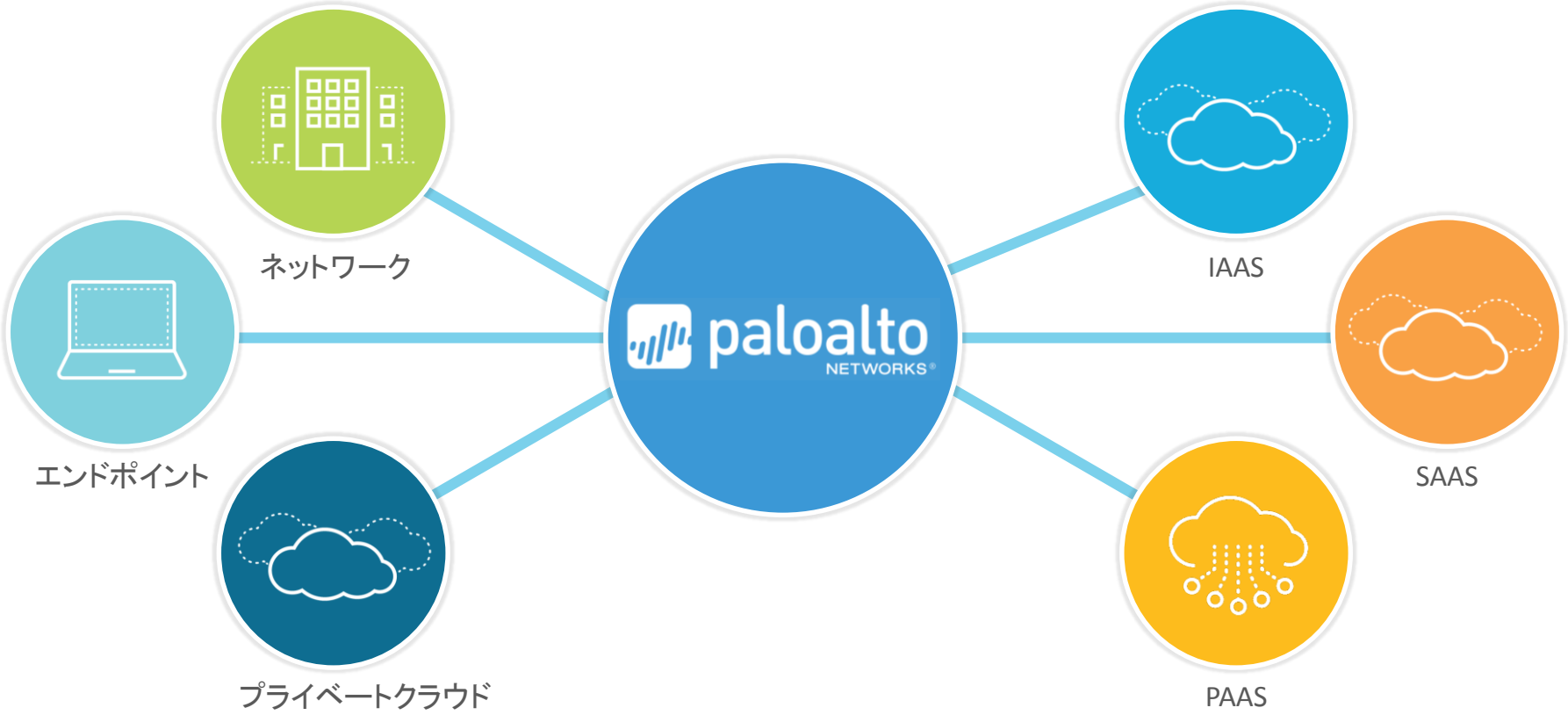
仮想次世代
ファイアウォール
VM-Series

AP

クラウドセキュリティ
サービス（CASB）
Aperture

PREVENTION EVERYWHERE

百戦危うからず




paloalto
NETWORKS®