NETWITNESS

ゼロトラスト時代の執拗な標的型攻撃から守り抜く RSA NetWitness Platformが最後の砦

RSA Security Japan合同会社
NetWitness事業部
アカウントマネージャー
柳川　玖莉亜

2021年7月21日

An RSA Business

RSAの歴史

RSA

RSA暗号の開発者が設立した情報セキュリティ業界の老舗（38年間）

世界最大のセキュリティイベントRSA Conferenceを主催

(1977) 1982 — 1984 — 1991 — 2006 — 2016 — 2020

1977 RSA暗号発明
Ronald Linn **R**ivest
Adi **S**hamir
Leonard Max **A**dleman

1982 RSA Data Security設立

Security Dynamics 設立
二要素認証 SecurID

RSA CONFERENCE

RSAラボ(暗号研究所)設立
RSA Conference確立

EMC²
RSA
The Security Division of EMC

EMCがRSAをM/A
RSAをセキュリティ部門として統合

DELL Technologies

Dell TechnologiesがEMCをM/A
RSAはセキュリティ部門として統合

RSA

9月
RSA Security LLCとして独立

NETWITNESS

RSAについて

3万社以上の
顧客

5000万以上の
アイデンティティ

20億の
ユーザー

400社以上の
グローバルパートナー

FORTUNE 100 BEST COMPANIES TO WORK FOR 2016 → **97%**

FORTUNE 500 2016 → **94%**

上位20の20社

- 製造業者
- コンシューマ製品
- 金融機関
- ヘルスケア期間
- 運輸

上位20の19社

- **上位20社の18社** テレコム
- **上位20社の16社** エネルギー
- **上位10社の10社** テクノロジー
- **15機関の内の13機関** アメリカ合衆国連邦行政部
- 米国陸軍の**すべて**の師部

RSA

RSAのポートフォリオ

RSA NETWITNESS® PLATFORM	RSA SECURID® SUITE	RSA ARCHER® SUITE	RSA FRAUD & RISK INTELLIGENCE SUITE	RSA RISK & CYBER SECURITY PRACTICE
▪ ログ、ネットワーク/パケット、エンドポイントまでの可視性 ▪ 正確な検知を可能にするための行動分析 ▪ 対応を迅速化するオーケストレーションと自動化	▪ 最新の多要素認証 ▪ 便利で安全なアクセスとSSO ▪ IDガバナンス ▪ IDライフサイクル管理 ▪ IDリスク管理	▪ ガバナンス、リスク、コンプライアンス（GRC）全体を可視化。経営判断を支援 ▪ ITセキュリティ リスク管理 ▪ コンプライアンス管理 ▪ オペレーショナル リスク管理 ▪ サードパーティ リスク管理 ▪ 内部監査	▪ デジタル コンシューマの全ライフ サイクルを通した監視 ▪ リスク ベース認証 ▪ グローバルな統合脅威インテリジェンス ▪ セキュリティとユーザー体験のバランス	▪ デジタル リスク成熟度の評価と戦略策定 ▪ インシデント対応支援 ▪ スレットハンティングサービス ▪ RSA ユニバーシティ ▪ RSA コミュニティ
全方位型SIEMと高度な脅威防御	**安全なアクセスへの変革**	**実績ある統合型リスク管理**	**オンライン不正防止**	**リスクおよびサイバーディフェンスサービス**

RSA BUSINESS-DRIVEN SECURITY™

NETWITNESS

ゼロトラストの概要とそのインフラ

NETWITNESS
An RSA Business

ゼロトラストの生い立ち

「**Never Trust, Always Verify**」はどこから生まれたか～

- 2020年: NIST(米国国立標準技術研究所) が SP800-207「ゼロトラスト アーキテクチャ」を発表
- 2018年: フォレスターリサーチ社が、ZTX (Zero Trust Extended Ecosystem) を発表
- 2010年: フォレスターリサーチ社の John Kindervag 氏が Zero Trust の概念を発表

2004年
JERICHO Forum
ネットワーク情報に基づく
暗黙の信頼を排除(制限)

1994年
RFC1636
境界線の内側が脆い
ということが問題

1977年
RSA論文や
Diffe氏、Hellman氏著書
「暗黙的な信頼」に否定的

- 信頼の対象を最小限にする(あるいは無くす)という議論は、かなり以前からある。

NETWITNESS

NIST SP800-207 ゼロトラストアーキテクチャー

1. 全てのデータソースとコンピュータならびにサービスはリソース(資産)とする
2. ネットワークのどこに存在するかにとらわれずに、全ての通信を保護する
3. リソース(資産)へのアクセスは、セッション(接続)ごとに許可する
4. リソース(資産)へのアクセスは、ダイナミック(動的)にポリシーを決定し、その際に、ユーザーのアクセス環境や動作そのものを考慮する
5. 所有するリソース(資産)が可能な限り安全であることを継続的にモニタリングして確認する
6. リソース(資産)の認証と認可をダイナミック(動的)かつ厳密に行ってから、その後のデータへのアクセスを可能にする
7. ネットワークインフラや通信の現状を可能な限り情報収集し、セキュリティ改善を行う

NETWITNESS

分類

前提

1 全てのデータソースはリソース(資産)とする

可視化 継続改善

2 ネットワークのどこに存在するかにとらわれずに、全ての通信を保護する

5 所有するリソースを可能な限り継続的にモニタリングして確認する

7 ネットワークインフラや通信の現状を情報収集し、セキュリティ改善を行う

認証強化

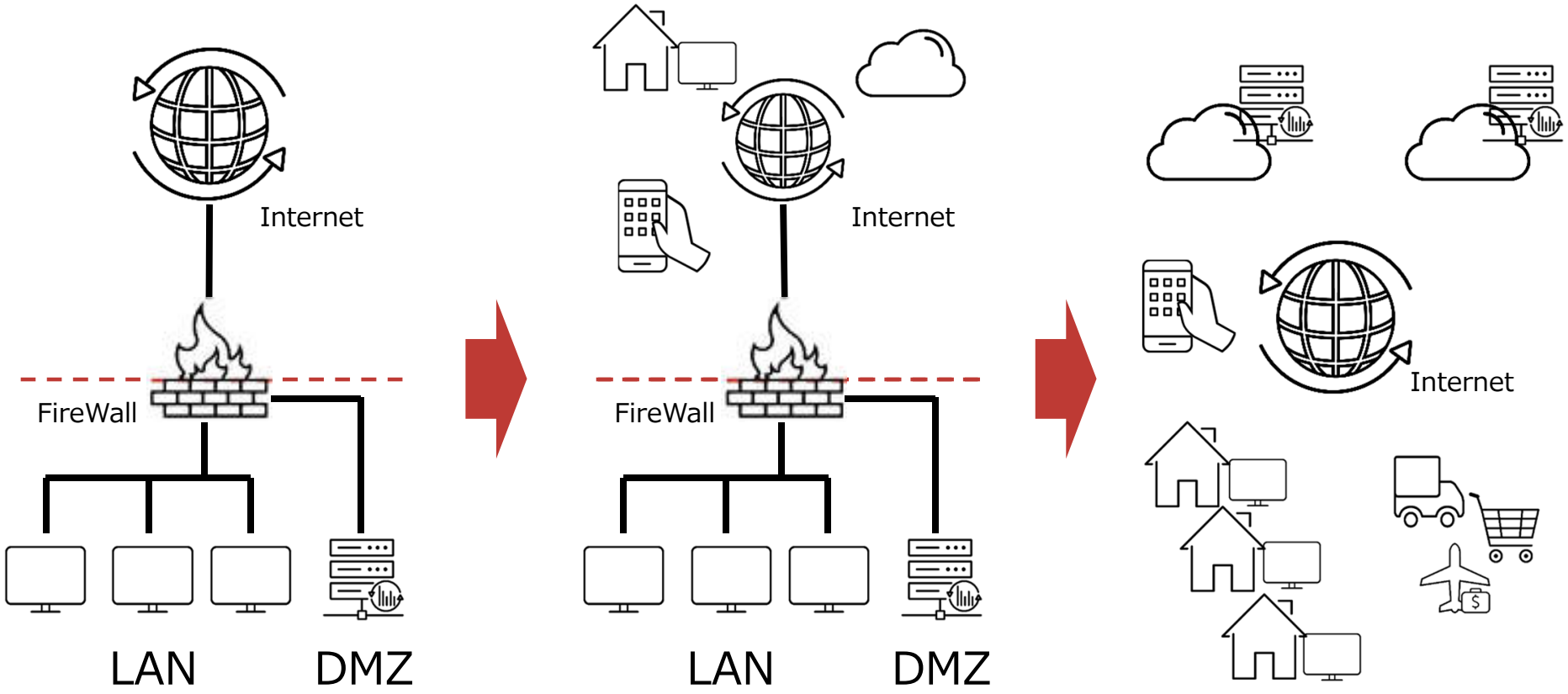
3 リソースへのアクセスは、セッションごとに許可する

4 リソースへのアクセスを動的に決定し、
ユーザーのアクセス環境や動作を考慮する

6 リソースの認証と認可を動的に行ってから、
データへのアクセスを可能にする

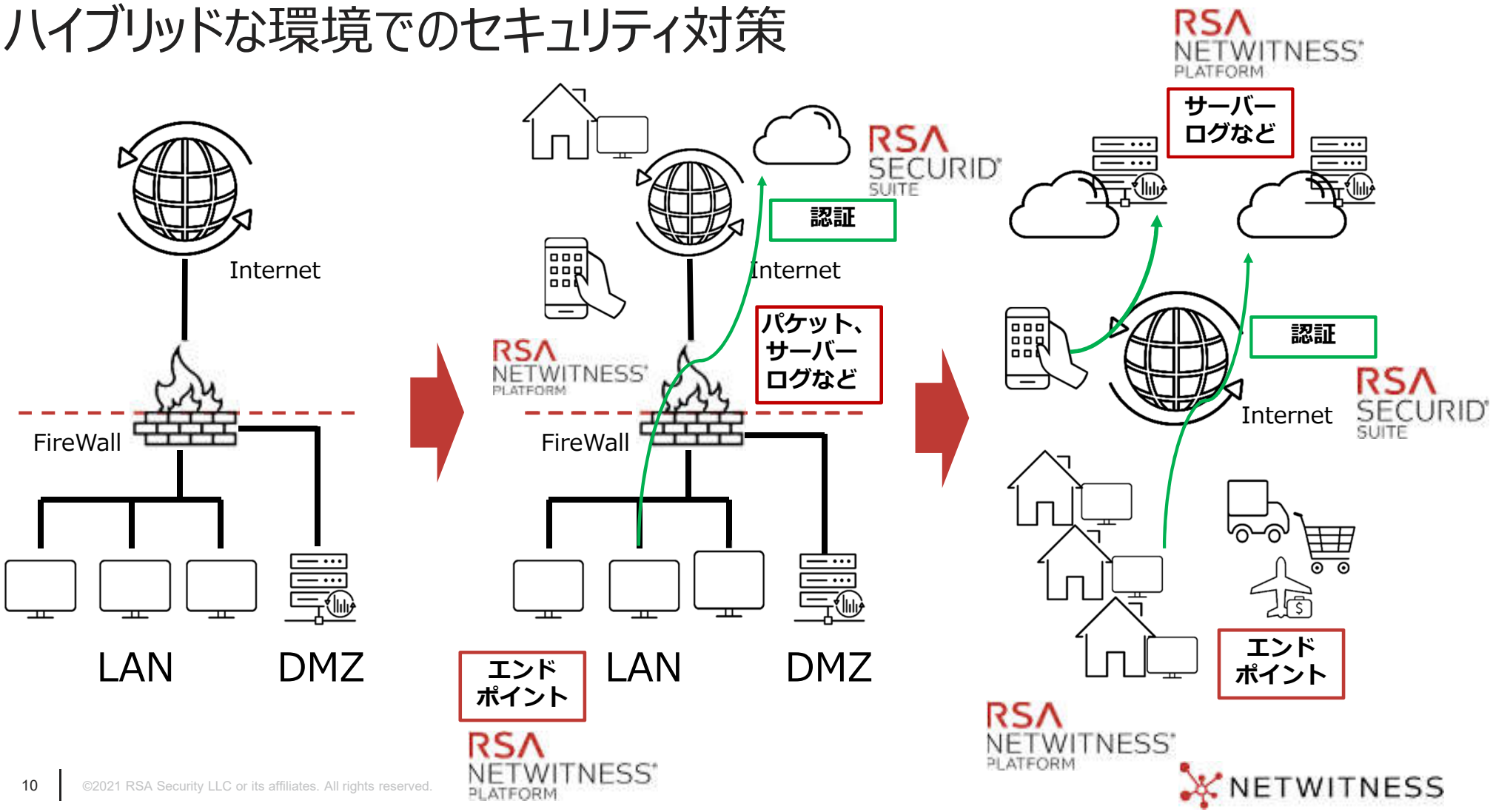
NETWITNESS

インフラの遷移



NETWITNESS

ハイブリッドな環境でのセキュリティ対策



Zero Trust時代のセキュリティ対策のポイント

✓資産および資産に関連する情報の可視化

✓継続的な監視強化

✓インシデント対応の強化

NETWITNESS

Zero Trust時代のセキュリティ対策のポイント

✓資産および資産に関連する情報の可視化
- エンドポイント・ログ・ネットワークデータを網羅的に収集する

✓継続的な監視強化
- 継続した情報収集
- 自動および手動の脅威分析機能の実装

✓インシデント対応の強化
- インシデントの全貌把握を早める
- 対応優先度の判断が行える仕組みの導入
- 対応体制（人）の強化

NETWITNESS

RSA NetWitness Platformで実現する高度なサイバーセキュリティ対策

～Detect Early Response Fast～

NETWITNESS
An RSA Business

Zero Trust時代のセキュリティ対策のポイント

✓資産および資産に関連する情報の可視化
- エンドポイント・ログ・ネットワークデータを網羅的に収集する

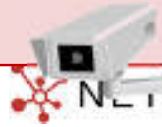
✓継続的な監視強化
- 継続した情報収集
- 自動および手動の脅威分析機能の実装

✓インシデント対応の強化
- インシデントの全貌把握を早める
- 対応優先度の判断が行える仕組みの導入
- 対応体制（人）の強化

NETWITNESS

情報ソースによる可視性の比較

	SIEM	Network Forensics	EDR
収集データ	**ログ**	**パケット**	**エンドポイント**
タイプ	各種デバイスのイベント	通信（セッション）	端末の実行プロセス
例えるなら	**断片的な証拠写真**	**ネットワークに監視カメラを設置**	**エンドポイント内に監視カメラを設置**
メリット	・インフラ全体カバー容易 ・長期保存（年単位）	・可視性（再現性）高い ・攻撃の詳細と証跡把握 ・導入が短期間	・端末だけでなくプロセスやファイルまで特定 ・秘匿化の影響受けない
デメリット	•断片的（侵害の見落とし、事実確認に制限） •ログデバイスに大きく依存	•暗号化された通信 •攻撃の横展開や内部通信（予算面の都合）	•特定のエンドポイントだけに可視化が制限
適した脅威	**重要なサーバへのアクセス**	**外部との通信攻撃全体像の把握**	**エンドポイント内部の怪しい挙動**



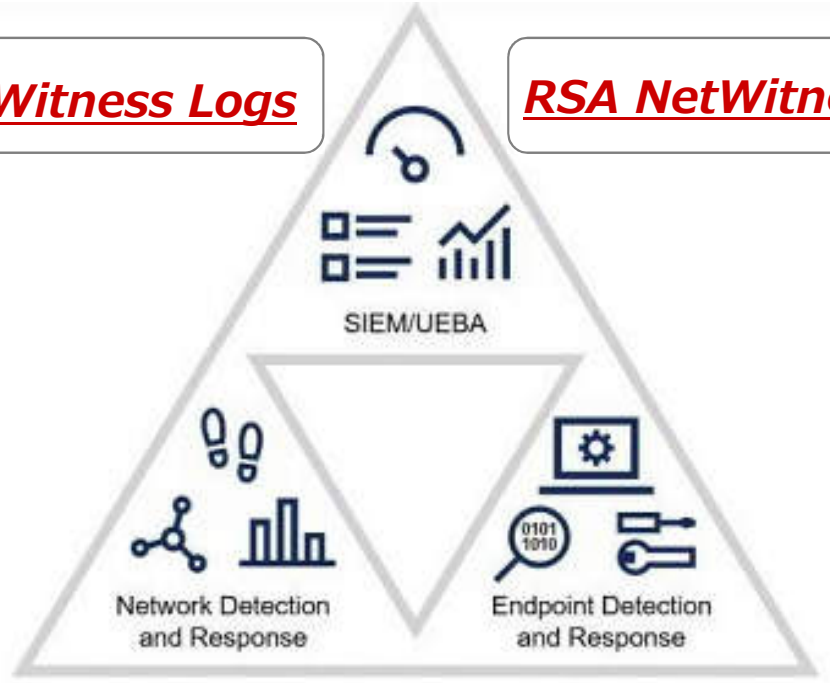
SOC VISIBILITY TRIAD

- 滞留時間と平均検出時間の短縮に注力
- 攻撃者が目的を達成する確率を下げる
- ログ、エンドポイント、およびネットワークのデータは、可視性を提供します。
- 併用することで、攻撃者が長時間に渡って検知を逃れる可能性を減らします。

GartnerがSOC Visibility TriadとRSA NetWitness Platform

RSA NetWitness Logs

RSA NetWitness UEBA

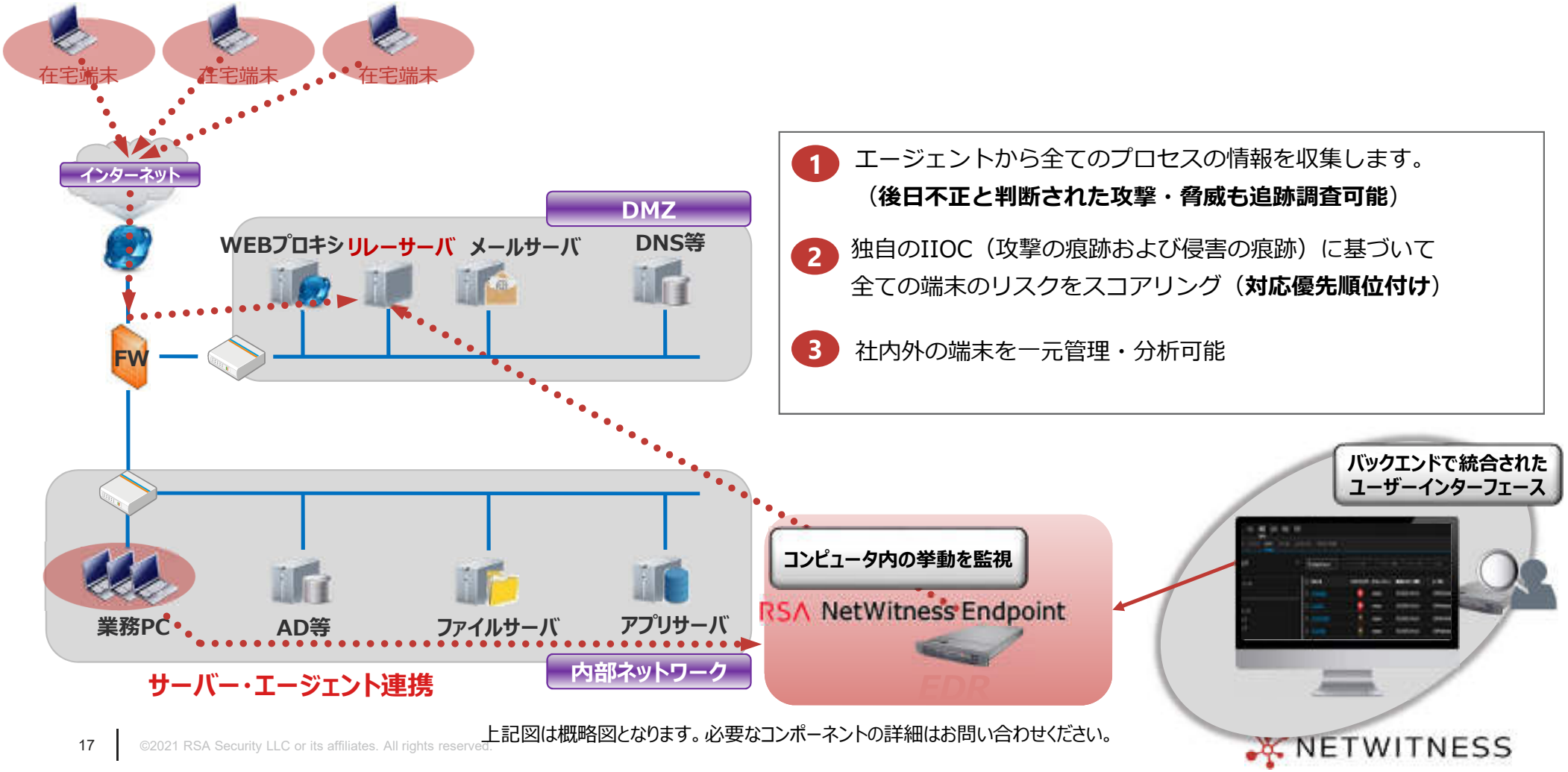


RSA NetWitness Network

RSA NetWitness Endpoint

NETWITNESS

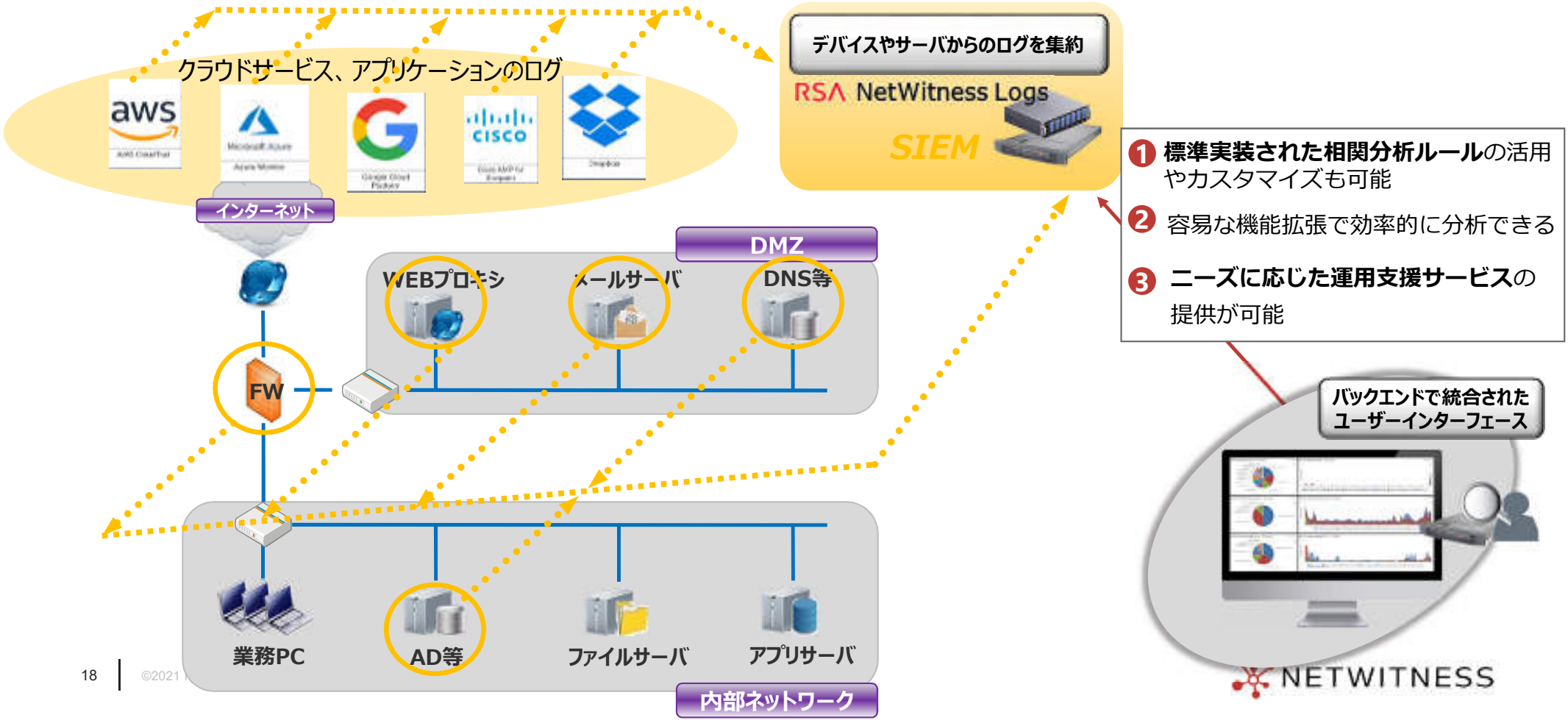
エンドポイントにおける脅威検出と対応（EDR）



1. エージェントから全てのプロセスの情報を収集します。
   （**後日不正と判断された攻撃・脅威も追跡調査可能**）
2. 独自のIIOC（攻撃の痕跡および侵害の痕跡）に基づいて
   全ての端末のリスクをスコアリング（**対応優先順位付け**）
3. 社内外の端末を一元管理・分析可能

上記図は概略図となります。必要なコンポーネントの詳細はお問い合わせください。

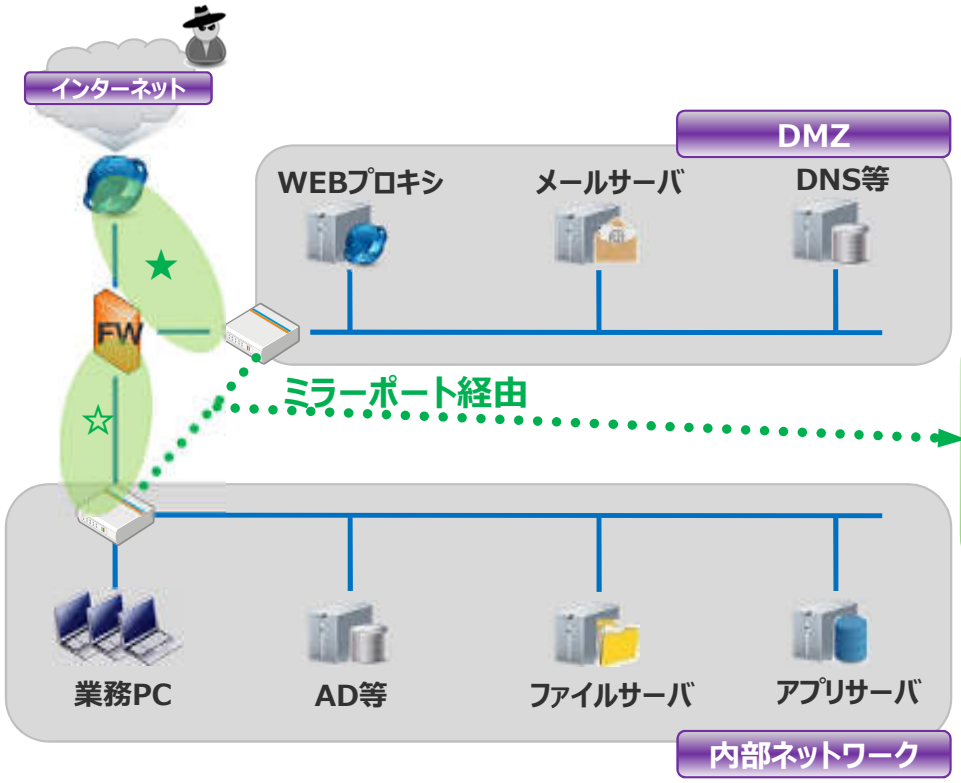
SaaSを含む各種ログの可視化・分析(SIEM)



ネットワークの可視化・分析(NDR/Network Forensics)

★社外から社内への通信（公開サーバーへのアクセス含む）

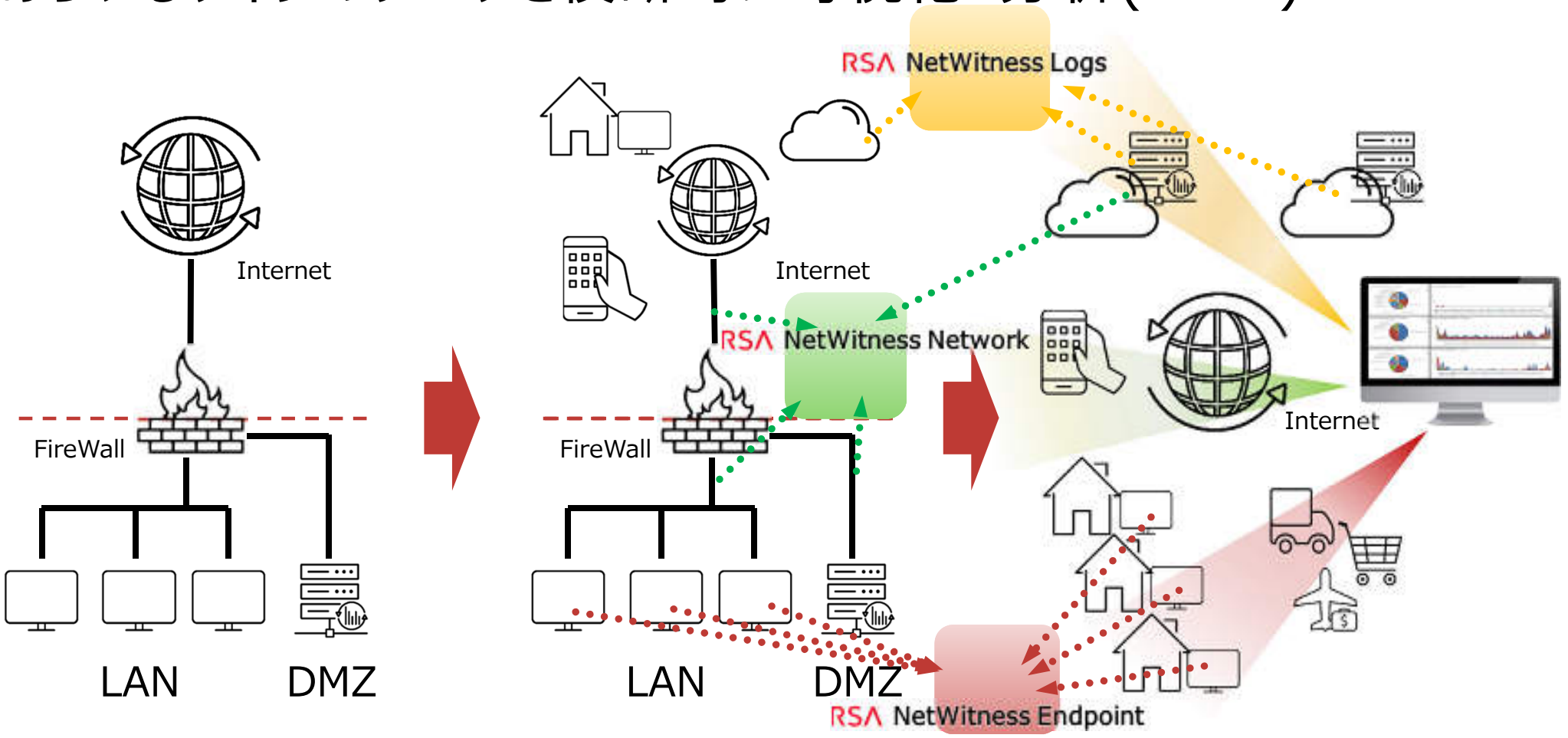
☆社内から社外への通信



1. スイッチのミラーポートSPANポートから通信を取得
   （情報漏洩の有無・攻撃内容の把握など通信から分析が可能）
2. 収集したトラフィックから豊富な属性情報（メタデータ）を生成
   任意の期間の通信データに対して多様な観点で高速な事象調査可能
   （特許取得済みアーキテクチャ）
3. セッション単位でフルパケットを保持し、数クリックでセッションの再現が可能（**インシデント発生時の全貌把握を支援、報告精度向上**）

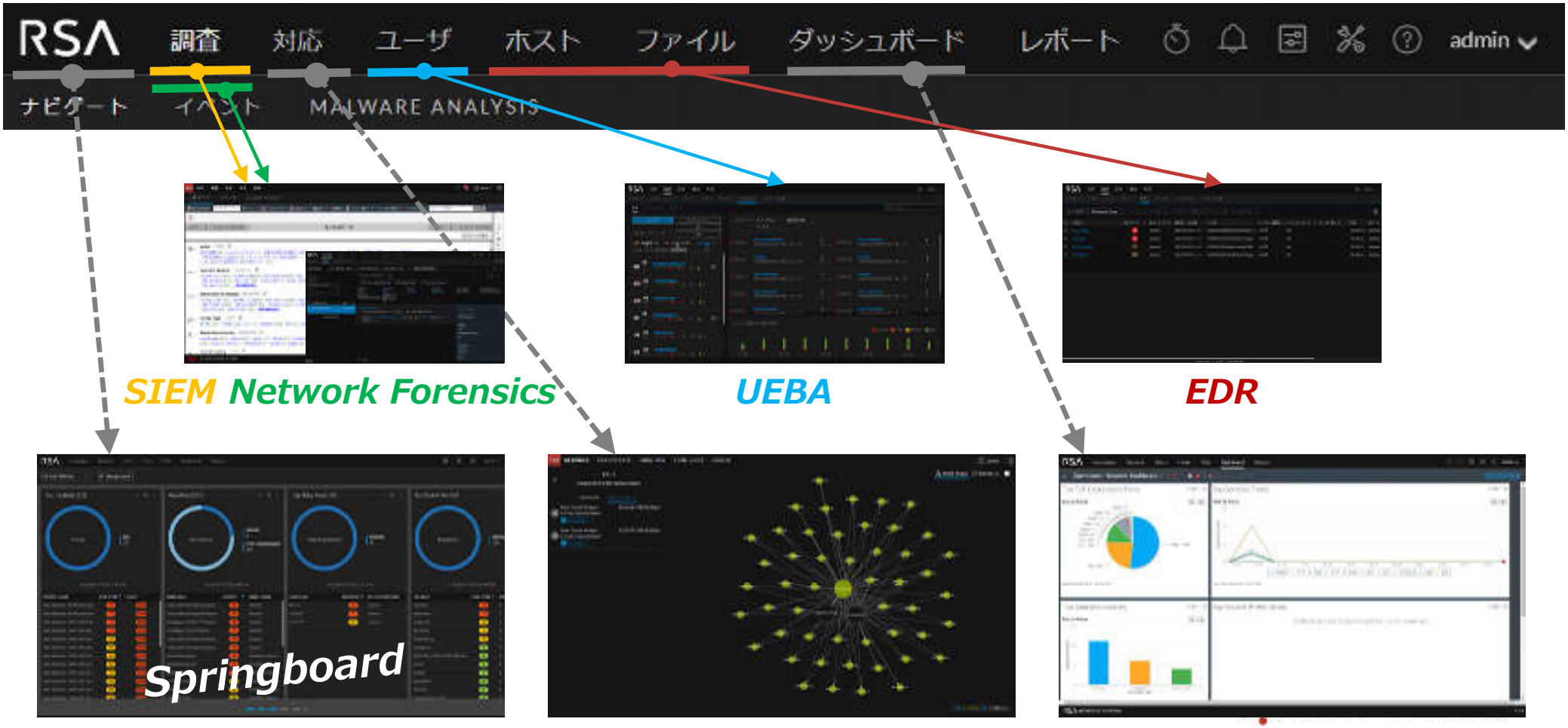
上記図は概略図となります。必要なコンポーネントの詳細はお問い合わせください。

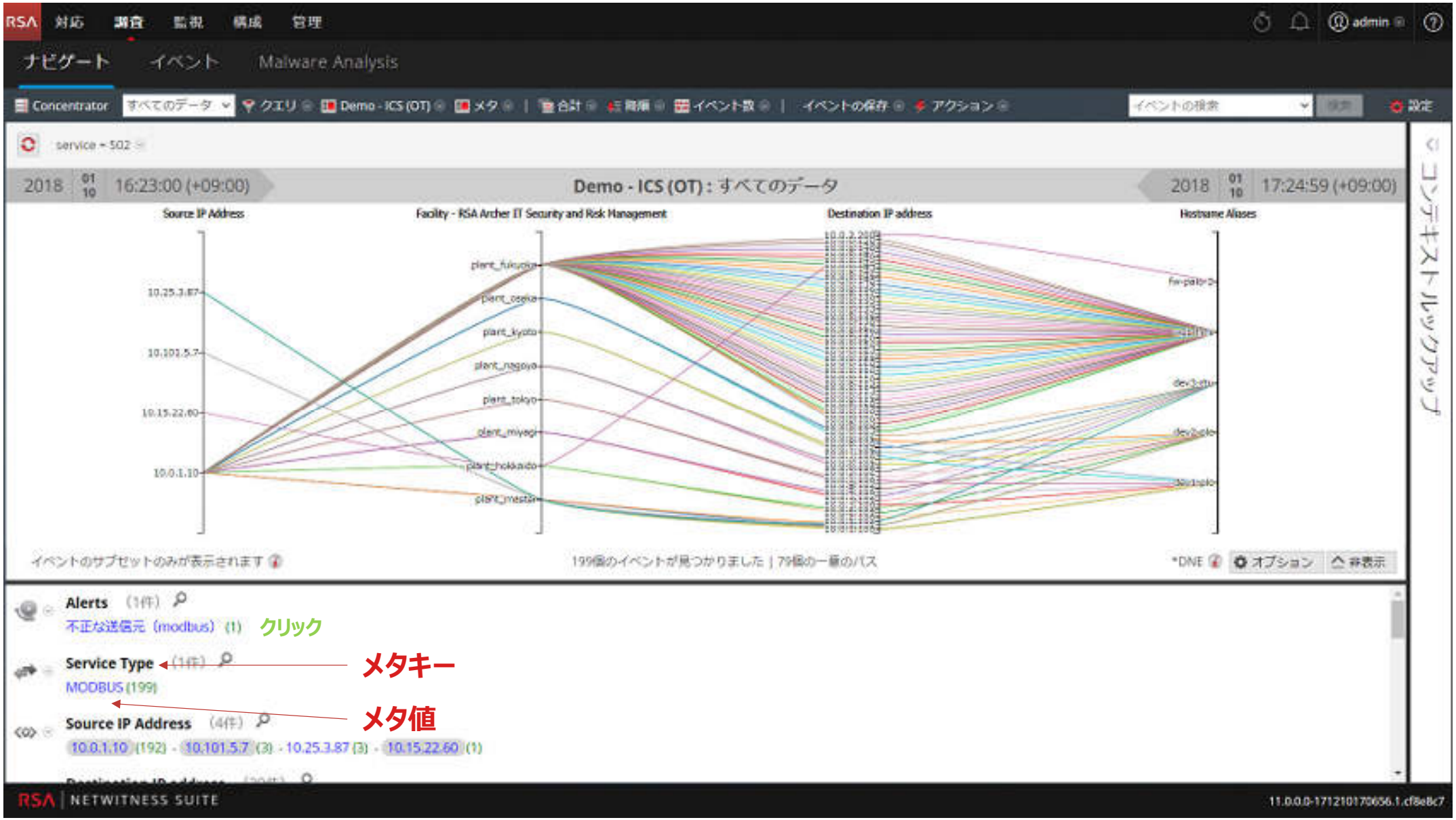
あらゆるタイプのデータを横断的に可視化・分析(XDR)



NETWITNESS

効率的な調査を実現するユーザーインターフェース




RSA
対応
調査
監視
構成
管理
admin
ナビゲート
イベント
Malware Analysis
Concentrator
すべてのデータ
クエリ
Demo - ICS (OT)
メタ
合計
頻度
イベント数
イベントの保存
アクション
イベントの検索
設定
service = 502
2018 01 10 16:23:00 (+09:00)
Demo - ICS (OT) : すべてのデータ
2018 01 10 17:24:59 (+09:00)
Source IP Address
Facility - RSA Archer IT Security and Risk Management
Destination IP address
Hostname Aliases
10.25.3.87
10.101.5.7
10.15.22.60
10.0.1.10
plant_fukuoka
plant_osaka
plant_kyoto
plant_nagoya
plant_tokyo
plant_miyagi
plant_hokkaido
plant_nagasaki
イベントのサブセットのみが表示されます
199個のイベントが見つかりました | 79個の一意のパス
*DNE
オプション
非表示
コンテキストルックアップ
Alerts (1件)
不正な送信元 (modbus) (1)
クリック
Service Type (1件)
メタキー
MODBUS (199)
Source IP Address (4件)
メタ値
10.0.1.10 (192) - 10.101.5.7 (3) - 10.25.3.87 (3) - 10.15.22.60 (1)
RSA | NETWITNESS SUITE
11.0.0.0-171210170656.1.cf8e8c7

100種類以上の標準メタデータをリアルタイムに生成

HTTPセッション

ip.src: 10.15.22.60, port: 1117
ip.dst: 95.57.120.128, port: 80

```
POST / HTTP/1.1
Host: www.skylogistic.co.cc
Accept: */*
Content-Length: 544
Content-Type: application/x-www-form-urlencoded
```

```
HTTP/1.1 405 Method Not Allowed
Allow: OPTIONS, TRACE, GET, HEAD
Content-Length: 1564
Content-Type: text/html
Server: Microsoft-IIS/6.0
Date: Thu, 27 Jun 2013 16:12:31 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML
4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>The page cannot be
displayed</TITLE>
<META HTTP-EQUIV="Content-Type"
Content="text/html; charset=Windows-1252">
```

メタ化

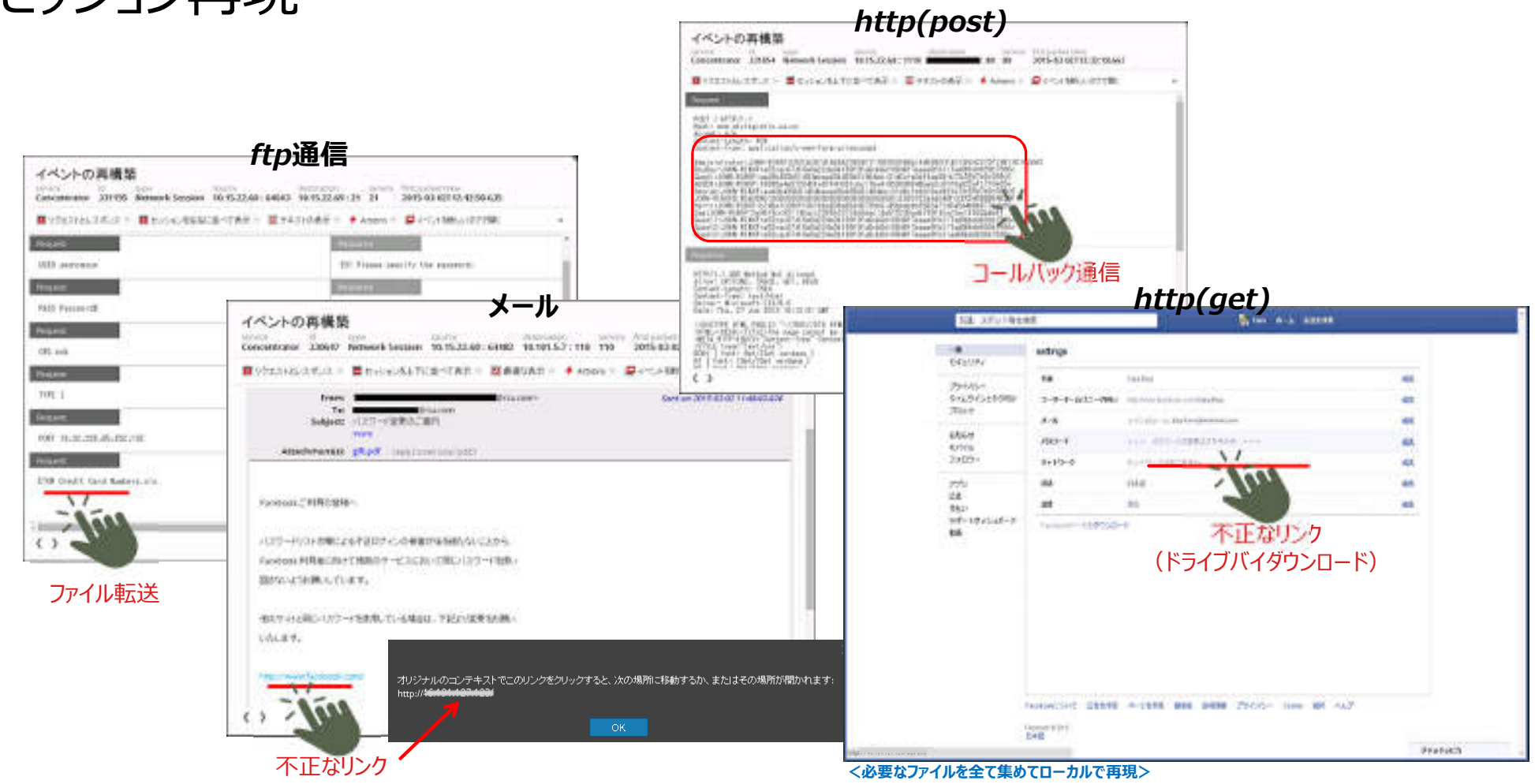
基本メタデータ（インテリジェンス）

メタキー	メタ値
ip.src	10.15.22.60
ip.dst	95.57.120.128
tcp.srcport	1117
tcp.dstport	80
action	post
alias.host	www.skylogistic.co.cc
directory	/
error	405 Method Not Allowed
content	text/html
server	Microsoft-IIS/6.0
:	

応用メタデータ（セキュリティインテリジェンス）

メタキー	メタ値
service	http
businessunit	payroll
facility	austin
country.dst	kazakhstan
ir.general	http_post_no_get
ir.general	post_no_get_no_refer
ir.general	four_or_less_headers
ir.general	web_susp_act_no_cookie
ir.general	http_no_ua
:	

セッション再現



Zero Trust時代のセキュリティ対策のポイント

✓資産および資産に関連する情報の可視化
- エンドポイント・ログ・ネットワークデータを網羅的に収集する

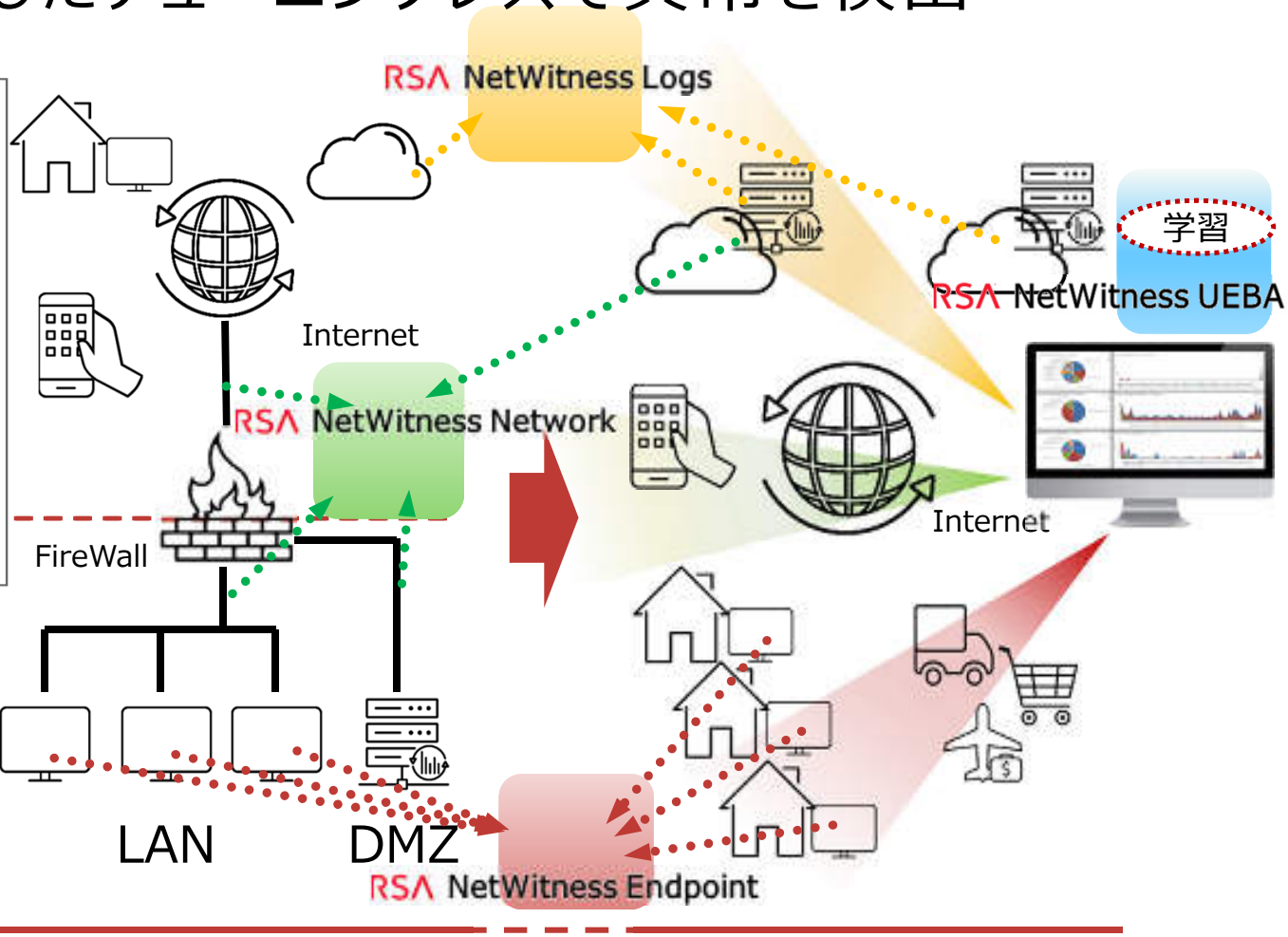
✓継続的な監視強化
- 継続した情報収集
- 自動および手動の脅威分析機能の実装

✓インシデント対応の強化
- インシデントの全貌把握を早める
- 対応優先度の判断が行える仕組みの導入
- 対応体制（人）の強化

NETWITNESS

各データソースをもとにしたチューニングレスで異常を検出

1. 各データソースから普段のふるまいを**機械学習し チューニングレスで内部の異常を検出**
2. 通常時のベースラインを生成し、複数のモデルと突合させ、**逸脱度合いをスコアリング**
3. 内部の脅威を自動検出した後は、各種データへ **深堀調査を単一のインターフェースで実施**



NETWITNESS

より高度な調査へ～相関ルールのテンプレートが豊富！～

アラーティング - 相関的なルールを使用した脅威の発見と通知

スキャン		
Aggressive Internal Database Scan データベースへのスキャニング通信		単一ホストから100以上のIPアドレスへ通信 1分以内 プライベートIPアドレス間 利用ポートがTCP/1433, UDP/1434, TCP/3306, TCP/5432, TCP/3351, TCP/1521
Aggressive Internal NetBIOS scan NetBIOSへ		単一ホストから100以上のIPアドレスへ通信
	疑わしい通信挙動	
	Detection of Encrypted Traffic to Countries 特定の地域へ暗号化された通信	特定の国からの暗号化通信
Aggressiv ウェブポータル	SSH Traffic Detected from a Source to Different Destinations 単一ホストから複数先へSSH通信	単一IPアドレスから5以上の送信先へSSHの通信 3分以内
	HTTP Outbound Traffic to Multiple Destinations From Single Source 単一ホストから複数の外部先へHTTP通信	単一IPアドレスから50以上の送信先へアウトバウンド通信 1分以内 プライベートIPアドレス
Port Scan 水平型ポート	Multi Service Connection Attempts Pckt 単一ホストから	単一のホストから単一の送信先へ複数のポート番号で通信
	ファイル転送	
Port Scan 垂直型ポート	RDP traffic プライベートIP	File Transfer Using Non Standard Port 非標準ポートを利用してファイルが送信	非標準ポートを利用したファイル転送
	RDP traffic destination 単一ホストから	Non DNS Traffic on TCP or UDP Port 53 Containing Executable DNS通信を装った実行ファイル転送	53番ポート上でDNSトラフィック以外が通信 実行ファイル（exe)が含まれる
		Non HTTP Traffic on TCP Port 80 Containing Executable 非標準ポートを利用したHTTP	80番ポート上でHTTPトラフィック以外が通信 実行ファイル（exe)が含まれる
		Non SMTP Traffic on TCP Port 25 Containing Executable 非標準ポートを利用したSMTP	80番ポート上でHTTPトラフィック以外が通信 実行ファイル（exe)が含まれる

NETWITNESS

より高度な調査へ～検知をすりぬける脅威をあぶり出す～

ハンティング　- 脅威インジケータを活用して脅威を能動的に発見する

- **ログからは得られない、ハンティング（脅威の発見活動）に有用なメタデータを生成**

	メタキー / メタデータ	備考
• **POSTがあるが、GETがない** • **ヘッダに Referrer がない**	post_no_get_no_refer	GETした結果に対してPOSTをするのが一般的 また、その場合の POST には Referrer がつく
• **非常に長い User-Agent**	long_ua, long_ua2	
• **Cookieがない**	web_susp_act_no_cookie	
• **ヘッダフィールドの数が少ない**	four_or_less_headers six_or_less_headers	普通のブラウザアクセスでは少なくとも10程度ある
• **Packer テクノロジが使われた実行ファイル**	packer armadillo	
• **送信データ量が多い**	high_tx_outbound	C2による制御通信やデータアップロードの可能性
• **HTTPバイナリのペイロード**	HTTP_with_binaryPayload	ファイルのダウンロードでないのにペイロードがバイナリ
• **ペイロードがない**	zero_payload	ビーコニングの可能性
• **拡張子に惑わされず、ペイロードを解析してのファイル判定**	Forensic Fingerprint: zip, pdf, windows executable, msword, etc.	

NETWITNESS

Zero Trust時代のセキュリティ対策のポイント

✓資産および資産に関連する情報の可視化
- エンドポイント・ログ・ネットワークデータを網羅的に収集する

✓継続的な監視強化
- 継続した情報収集
- 自動および手動の脅威分析機能の実装

✓インシデント対応の強化
- インシデントの全貌把握を早める
- 対応優先度の判断が行える仕組みの導入
- 対応体制（人）の強化

NETWITNESS

情報漏洩のコスト～対応時間が重要～

$3.86M
情報漏洩の平均総コスト(2020)[1]

207Days
侵害が判明するまでの平均時間(2020)[1]

73Days
侵入を食い止めるまでの平均時間(2020)[1]

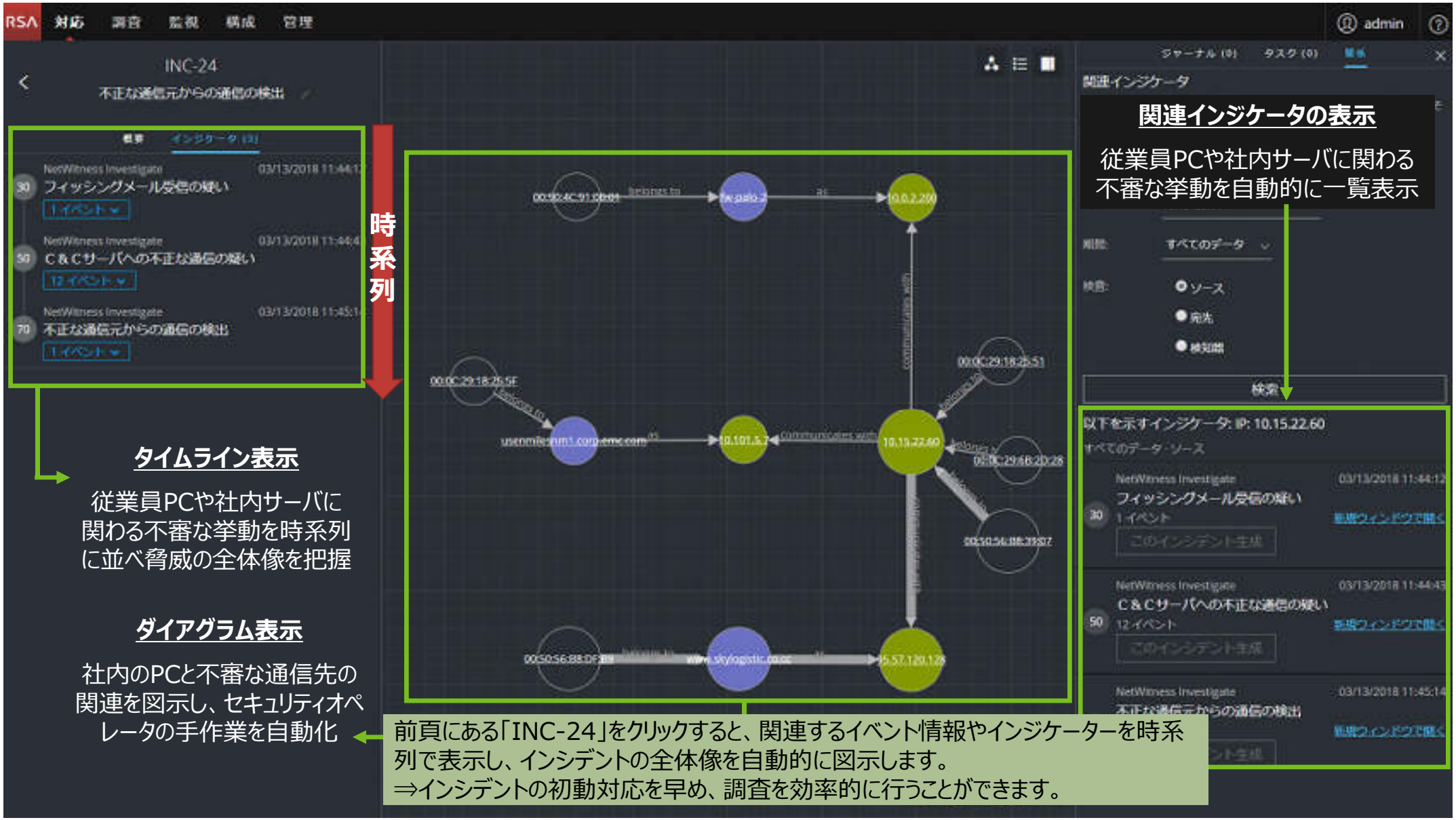
侵入を200日以内に食い止めることで、200日以上かかった場合に比べて112万ドルの節約になる

SPEED:いかに侵入した脅威を早期に検出し、根絶するかが重要

※1 https://www.ibm.com/security/data-breach

NETWITNESS


RSA
対応
調査
監視
構成
管理
admin
インシデント
アラート
タスク
フィルタ
すべてのデータ
INC-123
低
中
高
クリティカル
新規
割り当て済み
対応中
タスクリクエスト中
タスク完了
クローズ
クローズ- False Positive
フィルタのリセット
優先度の変更
ステータス変更
割り当て先の変更
削除
作成日
優先度
リスク
ID
名称
ステータス
割り当て先
アラート
03/13/2018 11:50:00 高 70 INC-26 新規 1
03/13/2018 11:49:29 高 60 INC-25 新規 1
03/13/2018 11:45:14 クリティカル 70 INC-24 割り当て済み Sam Polanco 3
01/10/2018 17:07:25 クリティカル 90 INC-19 割り当て済み Chris Gordon 1
01/10/2018 17:03:26 高 57 INC-18 割り当て済み Chris Gordon 11
01/10/2018 16:51:26 高 70 INC-14 新規 2
01/10/2018 16:25:02 クリティカル 90 INC-2 割り当て済み Chris Gordon 2
01/10/2018 16:22:56 高 70 INC-1 割り当て済み Chris Gordon 5
標準搭載の相関ルールに合致するインシデントを対応優先度順に表示
8件中8件を表示中 | 0件選択済み



関連インジケータの表示

従業員PCや社内サーバに関わる
不審な挙動を自動的に一覧表示

タイムライン表示

従業員PCや社内サーバに
関わる不審な挙動を時系列
に並べ脅威の全体像を把握

ダイアグラム表示

社内のPCと不審な通信先の
関連を図示し、セキュリティオペ
レータの手作業を自動化

前頁にある「INC-24」をクリックすると、関連するイベント情報やインジケーターを時系列で表示し、インシデントの全体像を自動的に図示します。
⇒インシデントの初動対応を早め、調査を効率的に行うことができます。

セキュリティ運用について

自組織内で実施する

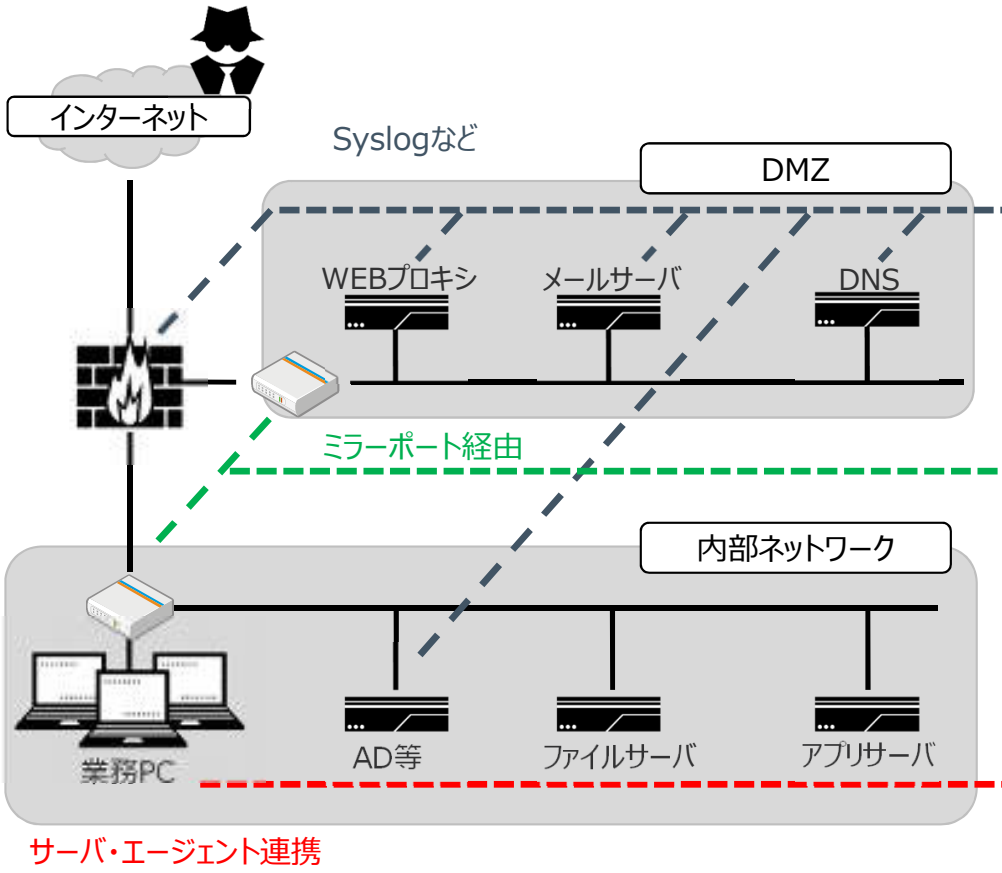
マネージドセキュリティ
サービス等を利用する

- 全貌を把握するための可視性があるか
- 迅速に対応していくための仕組みやテクノロジーがあるか
- 対応部門の教育を行う術があるか
- 属人化しない運用を支援する仕組みがあるか

- サービスの内容は明確か
- 全貌を把握するための可視性があるか
- 報告内容・項目は十分か
- サービスで担保できない部分のリスクは何か

NETWITNESS

セキュリティ運用をアウトソースする『スレットハンティングサービス』



NETWITNESS

Netwitness Logs
デバイスやサーバのログを集約

Netwitness Network
トラフィックの収取と蓄積

Endpoint
コンピュータ内部の挙動監視

Canon
キヤノンITソリューションズ株式会社

スレットハンティング
防御を回避した脅威の可視化

継続的チューニング
最新の脅威を捉える仮説検証

月次レポート
セキュリティの改善策を提案

NETWITNESS

RSA NetWitness Platformを活用されているお客様について
RSAの運用支援サービスについて
ご紹介可能なMSSやハンティングサービスについて
SOCの内製化支援
ハンズオンワークショップ（CTF）開催中！

お気軽にご相談ください。

【お問い合わせ先】
RSA Security Japan合同会社
NetWitness事業部
柳川　玖莉亜
kuria.yanagawa@rsa.com

NETWITNESS


NETWITNESS