SYSCOM
GLOBAL SOLUTIONS

1. はじめに（自己紹介・会社紹介）
2. 第1回/第2回セミナーおさらい
3. 本セミナーの背景と課題
4. フィッシング：最も頻繁に実行されるサイバー攻撃
5. エンドポイント対策①（フィッシングEmail Training）
6. ゼロトラストモデルとは
7. エンドポイント対策②（EDR）
8. サマリー

はじめに（自己紹介・会社案内）

はじめに（自己紹介）

プロフィール（宮本将光）(第三回目講師）

年齢・趣味

- 32歳
- ゴルフ

シスコム歴・部署・役職

- 5年
- NY営業2部
- マネージャー

プロジェクト実績

- EDR (Endpoint Detection and Response)
- SOC (Security Operation Center)
- Security Training　など

会社紹介

会社名	SYSCOM GLOBAL SOLUTIONS
代表	佐藤誠詞
設立	1990年5月
資本金	$3,200,000-
株主構成	佐藤 誠詞 President & CEO 199株(66.3%) ITOCHU Techno-Solutions America, Inc. 101株(33.7%)
本社	米国 ニューヨーク マンハッタン
従業員数	約140名

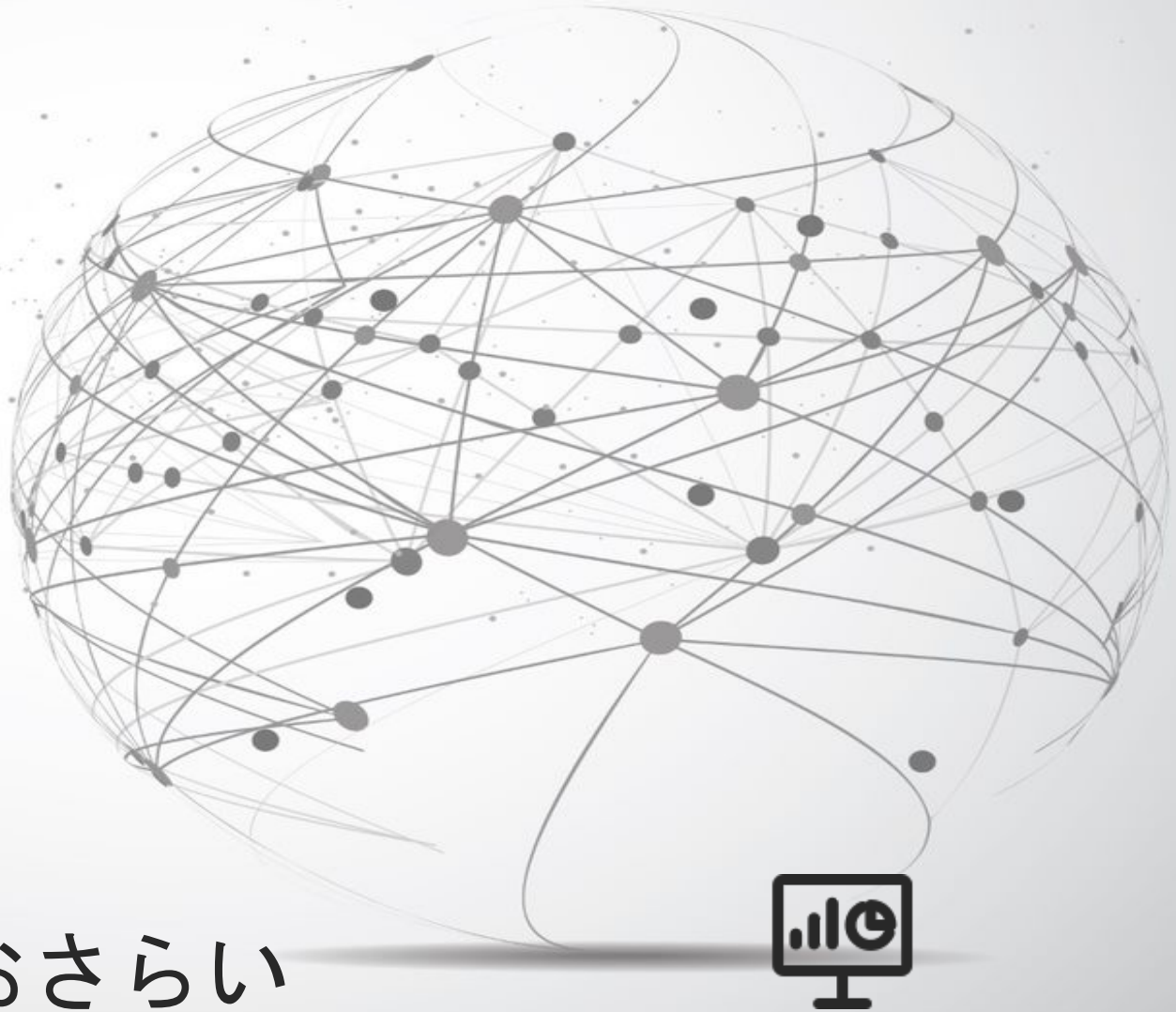
30年以上のUSでのITサポート実績

パートナー、
ベンダーフリーの
トータルITサポート

日系企業**1000**社以上の取引実績

24時間
365日の
保守・
運用サービス

従業員の**7**割以上がエンジニア



第一回/第二回セミナーおさらい

2021年最新サイバーセキュリティ事故の実態 第一回のおさらい

SYSCOM GLOBAL SOLUTIONS

個人データ	情報漏洩のうち**58%**は個人データが関与
対応	情報漏洩のうち**60%**はパッチが適応されていない事が要因
中小企業	中小企業の**43%**でサイバーセキュリティ対策の計画ができていない
経営者	経営者のうち**68%**はサイバーセキュリティリスクが増加していると感じている
被害と対応	2019年には **63%**の中小企業が情報漏洩があったと報告 - **58%** in 2018, **54%** in 2017 情報漏洩の**6割**は対応不足が原因
パンデミック	•パンデミック後のサイバー犯罪は**300%**増加

安全なクラウドセキュリティ対策のためのCASB 第二回のおさらい

安全なクラウド利用を実現するためのセキュリティ対策ソリューション
CASBについてご説明しました。

CASB （キャスビー（Cloud Access Security Broker））

・2012年に米ガートナーが提唱したクラウドサービスに対する情報セキュリティのコンセプト

・システム・データのクラウド移行が進み、（またテレワーク等のゼロトラスト環境が増える中）セキュリティを担保しながらクラウドへアクセスさせる必要性が高まっている。

・業務効率や利便性を損なわないように、一貫性のあるセキュリティポリシーを適用しながらクラウドサービスを利用する事ができる。

可視化	コントロール
データセキュリティ	脅威防御

本セミナーの課題/ゴール

本セミナーの課題/ゴール

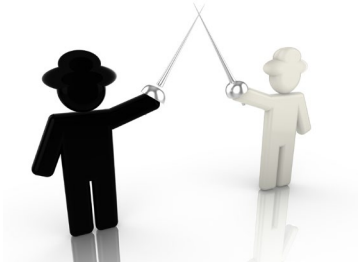
課題：
テレワーク化（働き方改革）によるクラウド活用などの利便性向上に伴い、情報漏えいやマルウェア感染などの被害が増加

今回のセミナーで、

1. 最も頻繁に実行されているサイバー攻撃とその対策

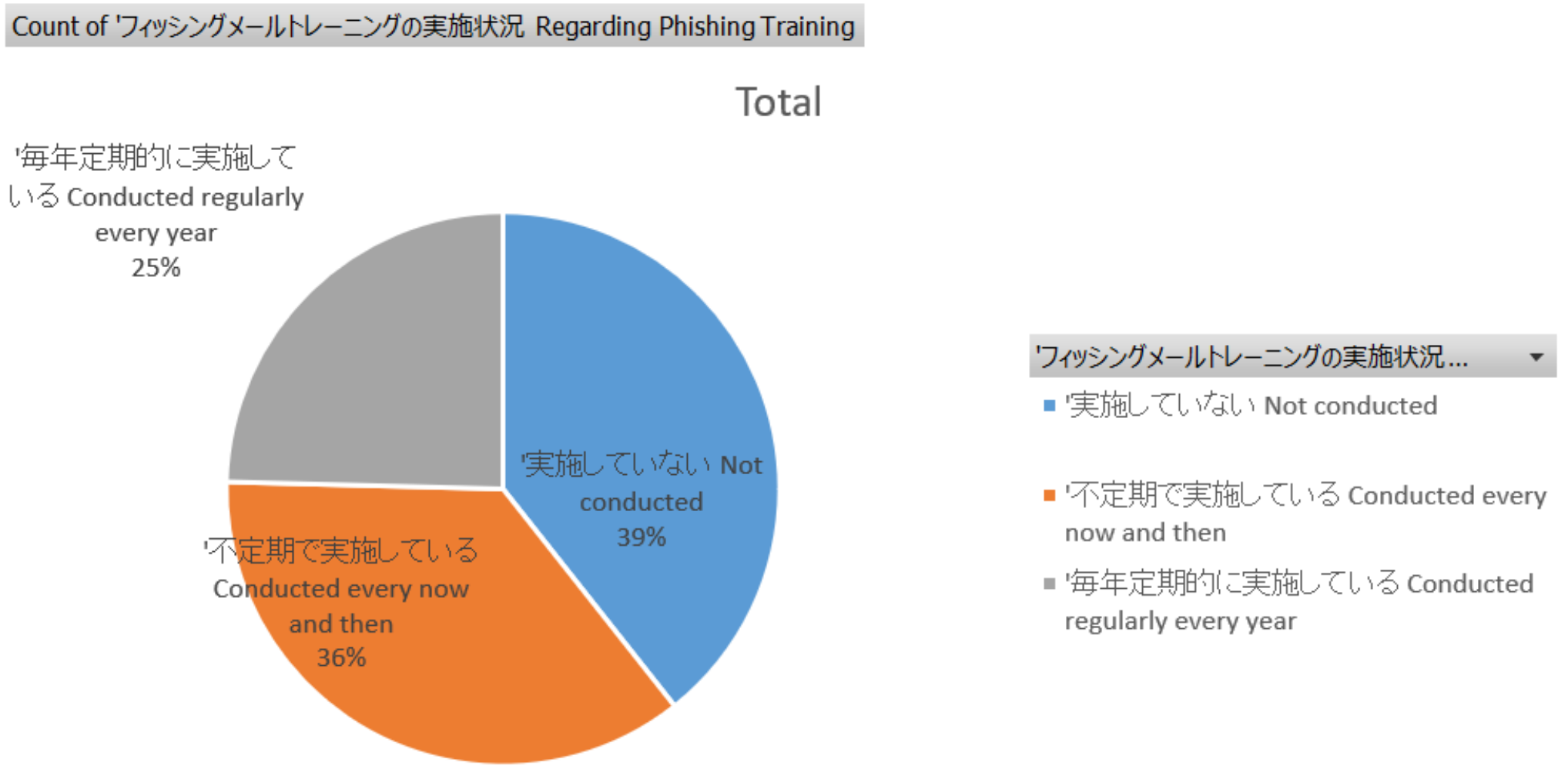
2 . “ゼロトラストモデル” の考え方と重要性

3. “EDR”とは。 その重要性とソリューション

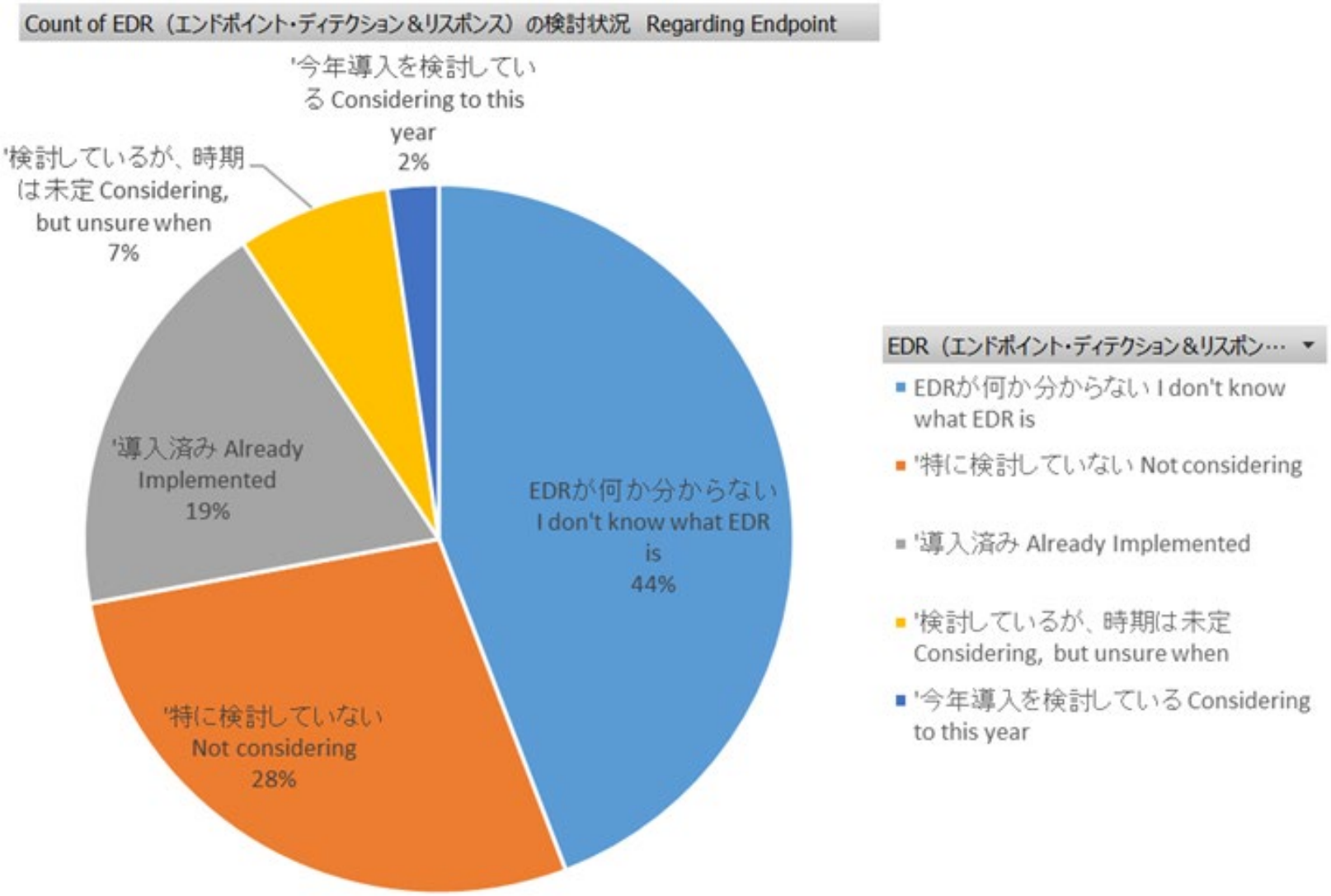


がわかります。

事前アンケート – フィッシングメール



事前アンケート - EDR

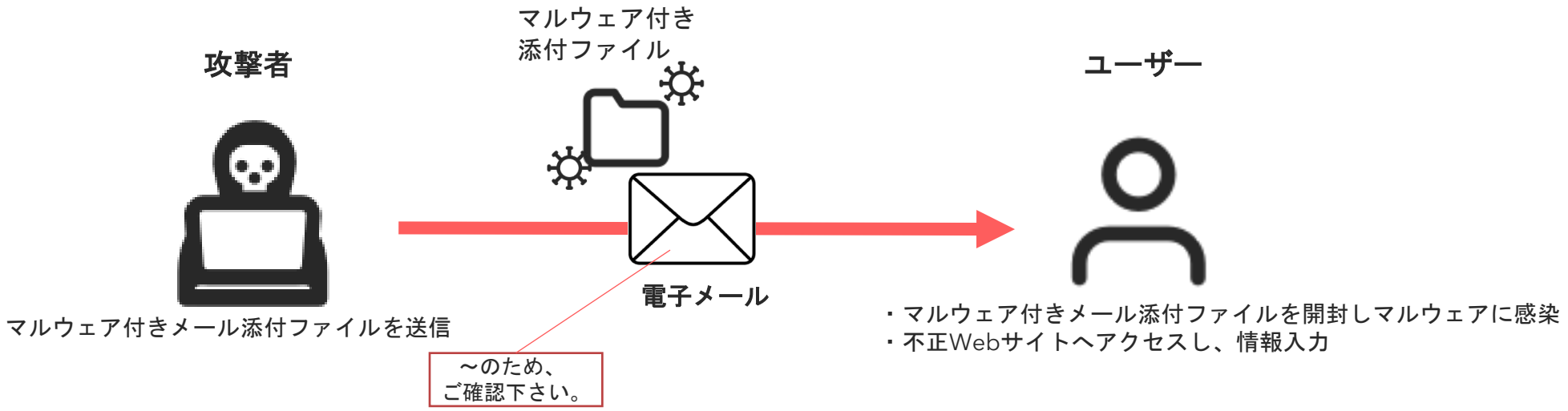


フィッシング：最も頻繁に実行されるサイバー攻撃

フィッシング攻撃とは

フィッシング（英: phishing）とは、

インターネットのユーザから経済的価値がある情報（例: ユーザ名・パスワード・クレジットカード情報）を奪うために行われる詐欺行為である。フィッシング、フィッシング詐欺



数字で見るフィッシングの実態

Phishing Email Stats…

92% のマルウェアはEmail 経由で運ばれています。 ~2021 cyber security statics~

エンタープライズネットワークに対するすべての攻撃の**95%**は、
スピアフィッシングの成功の結果です。 ~Staggering Phishing Statistics in 2020 - Security Boulevard~

フィッシング攻撃がサイバーセキュリティ侵害の**90%**を引き起こしている。

~ Verizon analysis January 21, 2020 ~

毎月**150万**近くのフィッシングサイトが作成されています。

~ Kaspersky Security Bulletin 2018~

※「**Spear Phishing**（スピアフィッシング）」とは、特定の組織や人物を狙って偽のEメールを送信し、個人情報を収集する標的型フィッシング攻撃のこと。

事故事例

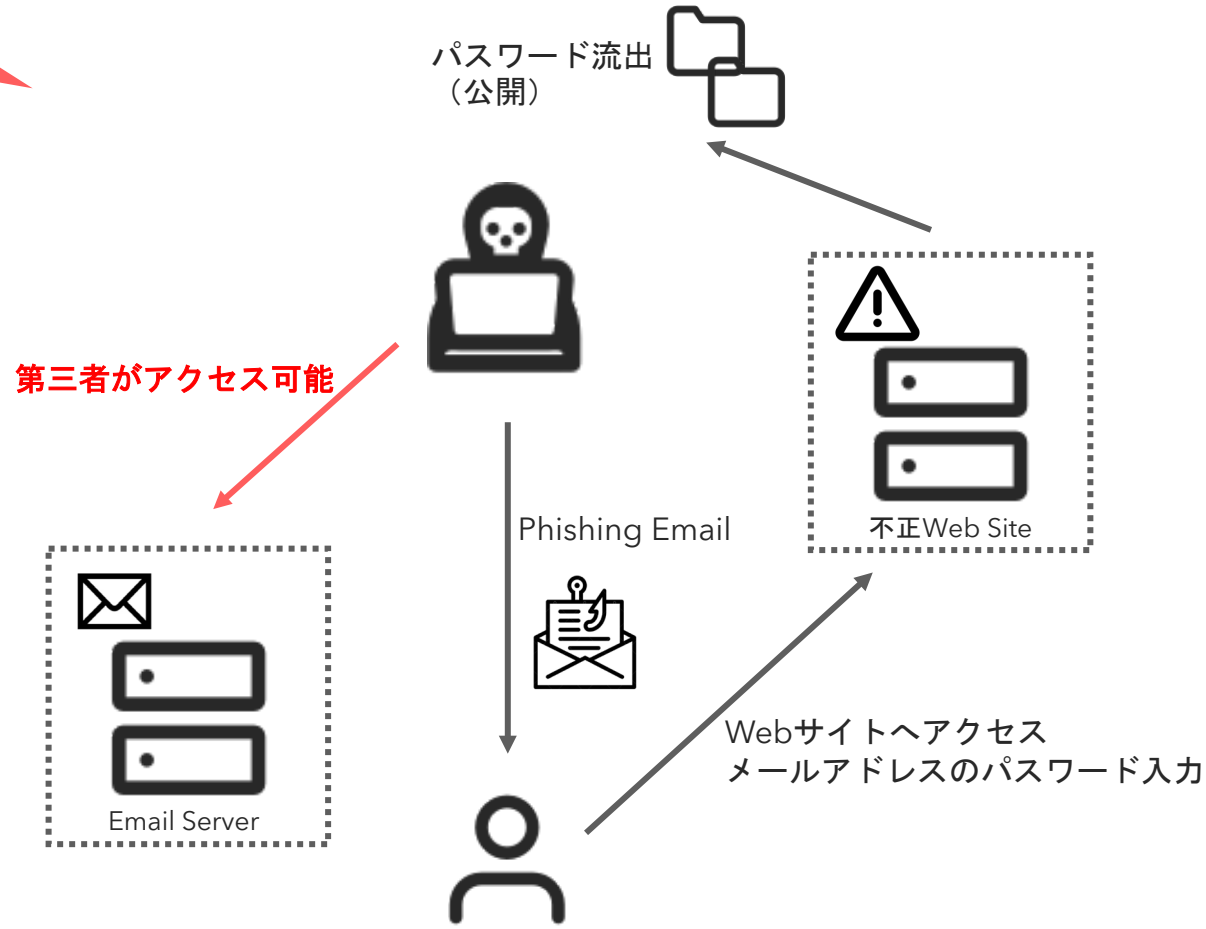
事件プロフィール

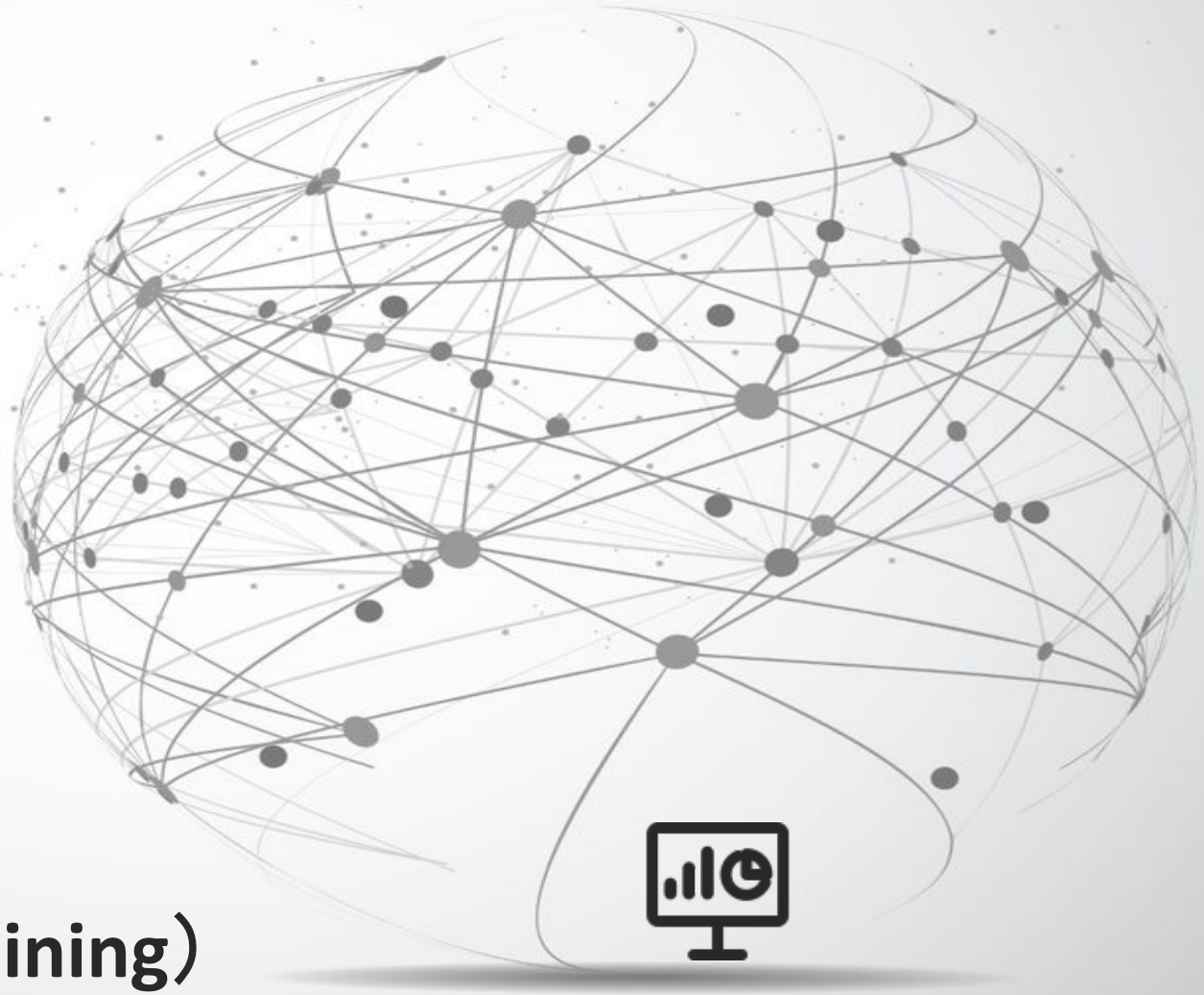
事件概要

- フィッシングメールを受信した従業員が誤って不正なWebサイトのURLをクリックし、サイト上のフォームでメールアドレスのパスワードを入力してしまった。フィッシングメール詐欺の発覚後、当該メールアドレスのパスワードは変更されたものの、その間にメールサーバーが不正アクセスを受けていた。

着眼点

- 顧客情報等が外部に流出した事実は確認されていないと報告されつつも、第三者がメールを閲覧できる状況にあった。





エンドポイント対策①
（フィッシングEmail Training）

Email セキュリティ

Protection
- Filtering
- Advanced Threat Encryption
- Archive
- MFA
- Rule Engine

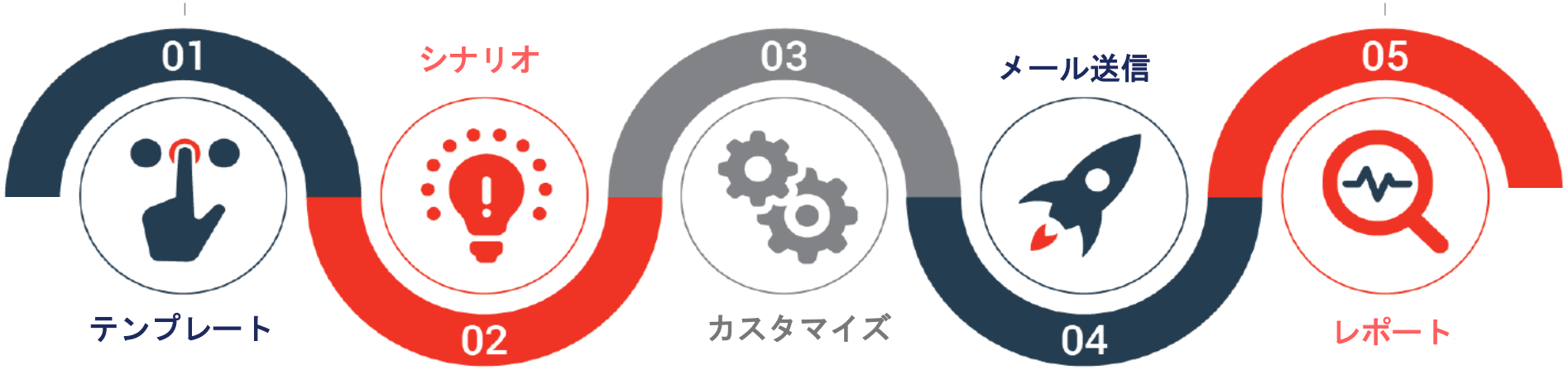
+

Training
- Training
- Analysis
- Reporting

Researchers from Stanford University and a top cybersecurity organization found that approximately **88 %** of all **data breaches** are caused by an employee mistake.

双方の組み合わせでの対策が必要

Email フィッシングトレーニングの仕組み



01 Email のテンプレートを作成

02 フィッシングシミュレーションシナリオを作成する

03 必要に応じて、選択したテンプレートをカスタマイズします

04 すべてのユーザーにフィッシングシミュレーションメールを送信する

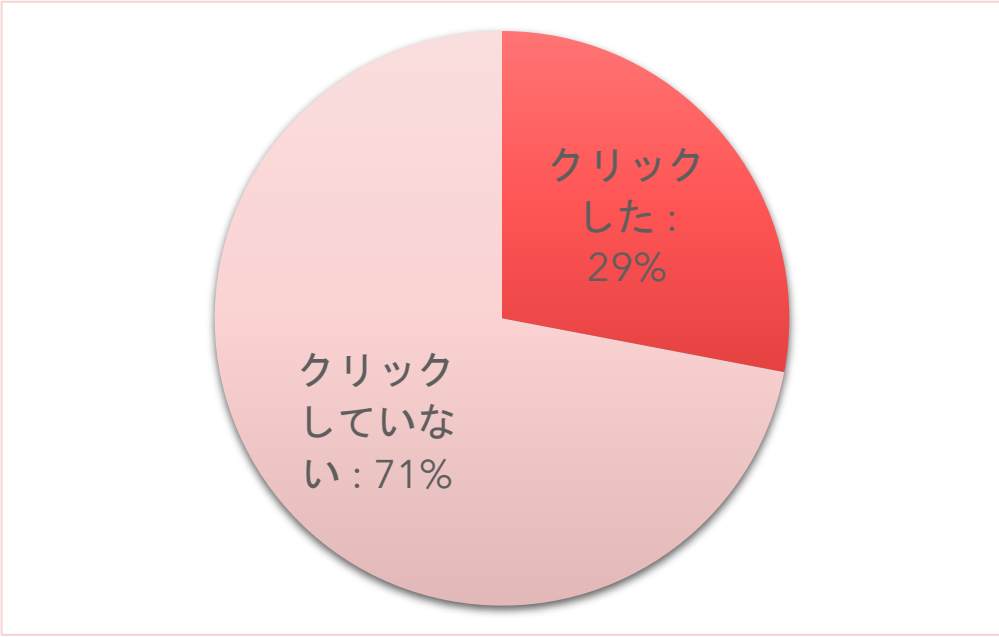
05 ユーザー/グループごとに結果を分析する

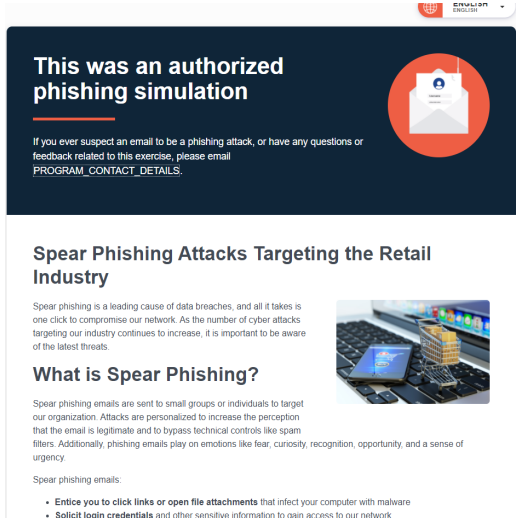
実際のクリック数、効果

銀行で勤める従業員の約31%がフィッシングテストに不合格

According to the 2020 Phishing report, around 31% of banking employees failed to pass a phishing test. (KnowBe4)

SYSCOMの今までのお客様のテスト初回のクリック数平均：29%





継続的なトレーニング、教育が必要となります。

実施の意義

直接的な意義

- トレーニングを実施、社員の教育を行い、フィッシング攻撃が原因の事故を防ぐ。

関節的な意義

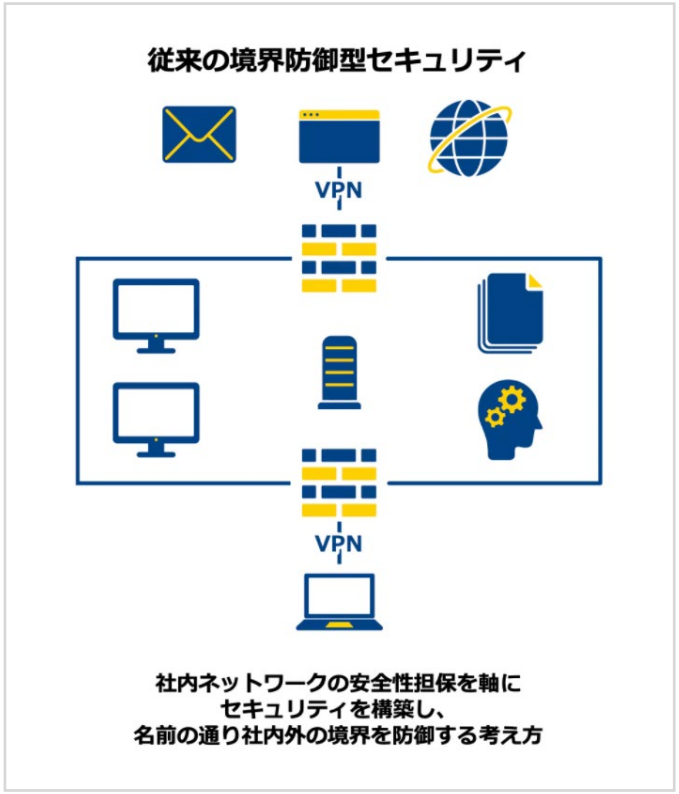
- 万が一事故が発生した際に、未然に防ぐための対策を実施していたか。が問われる。
- サイバーセキュリティ保険への加入、SOCなどの取得をする際は、必須の事項となっている。

SOCは「Service Organization Controls」の略。「サービス組織の統制」
「セキュリティ」「可用性」にかかる内部統制のデザインを外部監査人が評価したもの

ゼロトラストモデルとは

ゼロトラストモデルとは

ゼロトラストとは「何も信頼しない」を前提に対策を講じるセキュリティの考え方です。



なぜゼロトラストモデルが必要なのか。

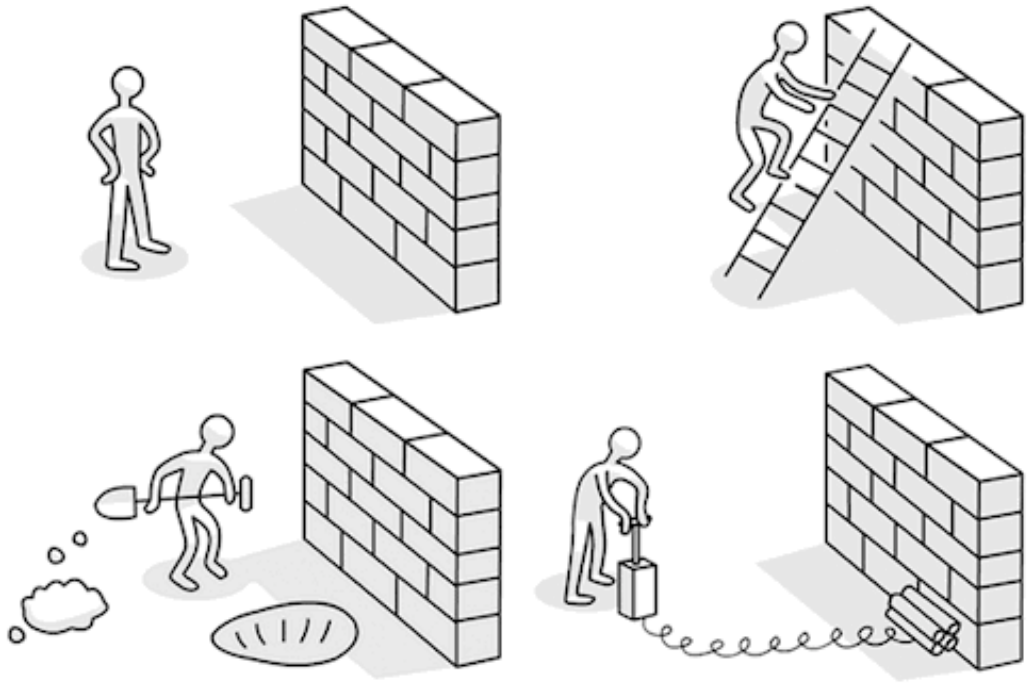
SYSCOM GLOBAL SOLUTIONS

境界線型の限界

境界線対策と巧妙な攻撃とはイタチごっこで、対策が追い付かなくなり、いつかは突破されてしまう。

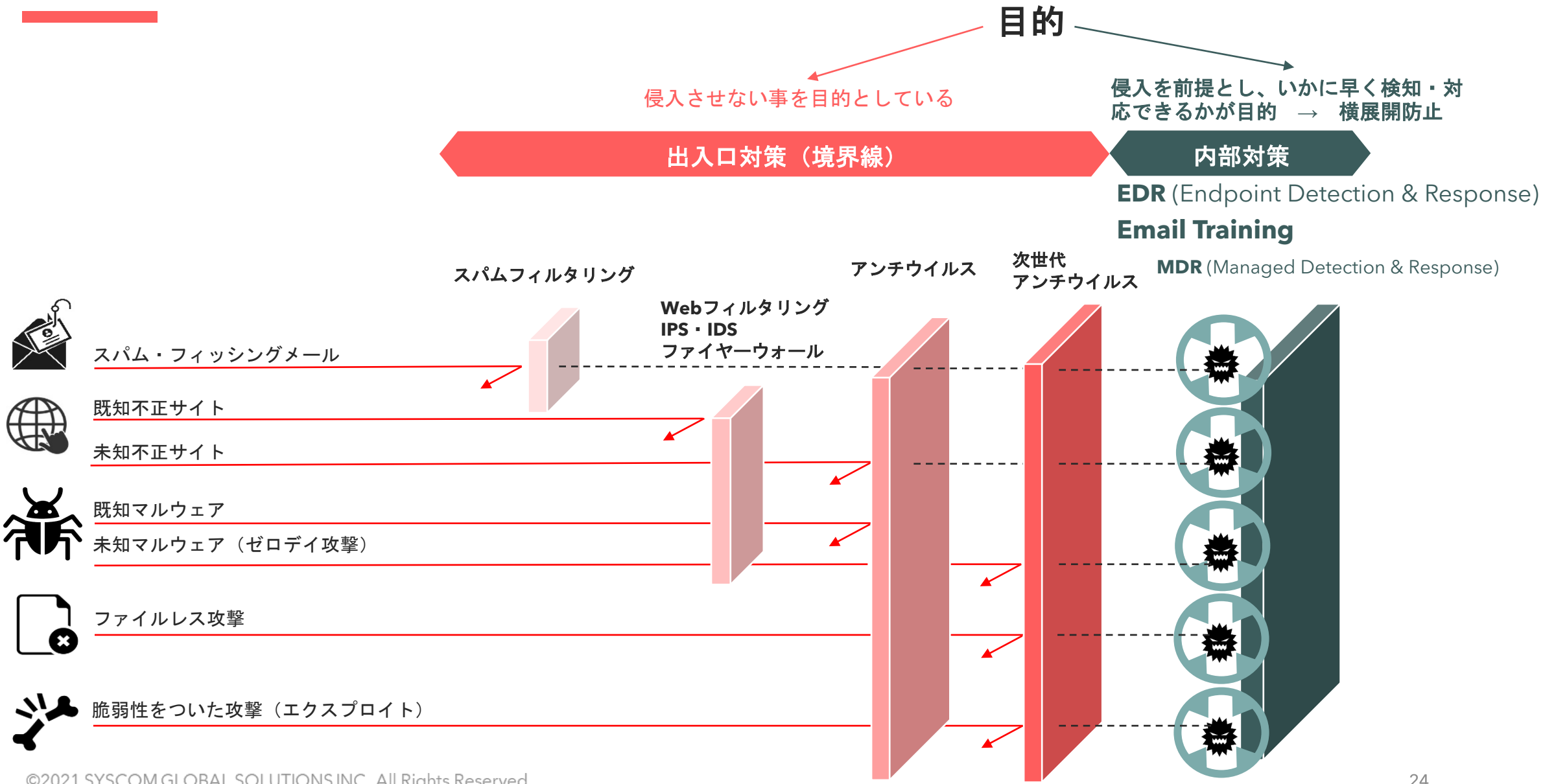
ゼロトラスト（内部対策）

感染や侵入された際の脅威や行動を可視化し、いち早く適切に対処する事で、被害を最小化する、又は未然に事故となる事を防ぐための内部対策が重要（ゼロトラスト）

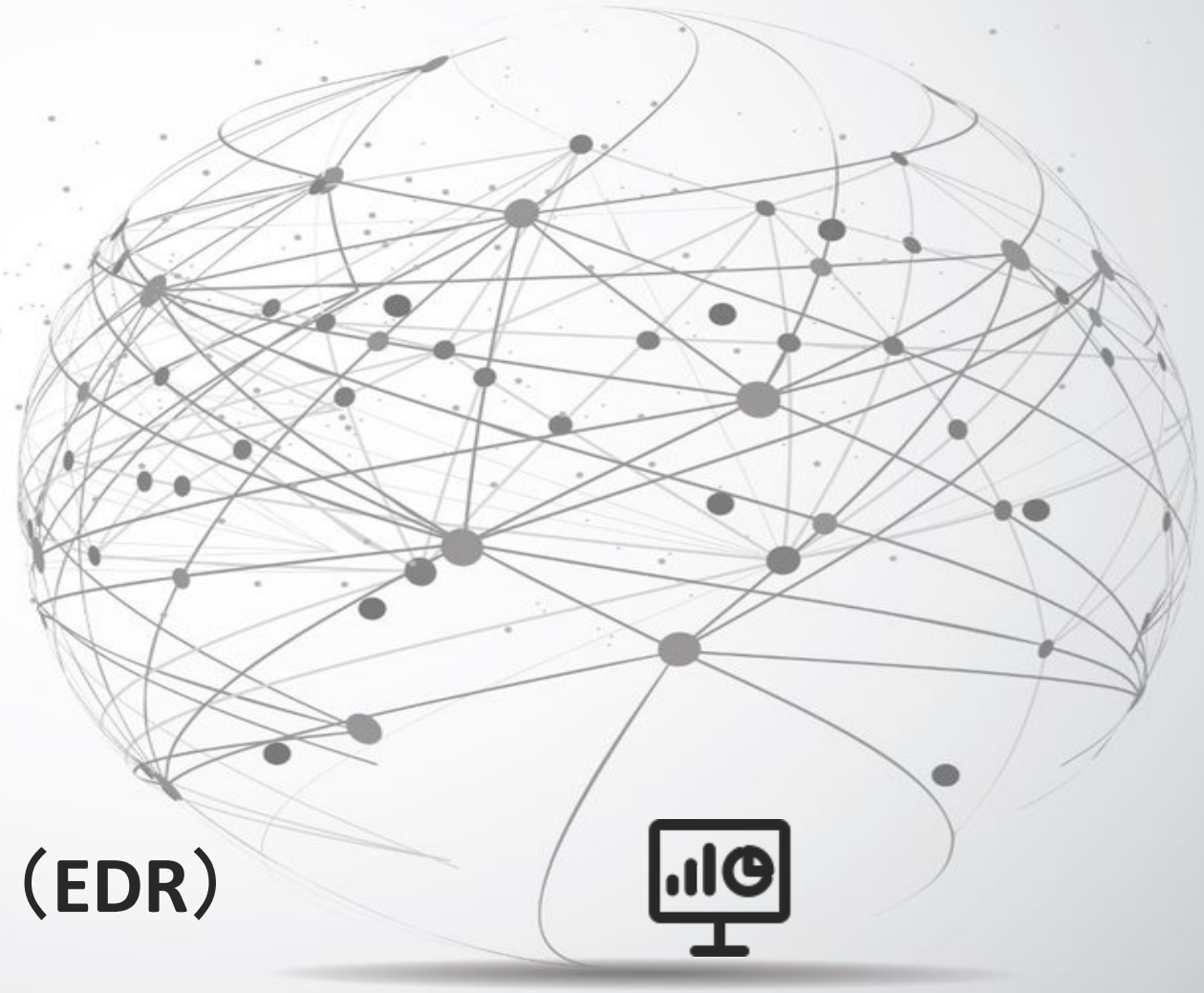


境界線は巧妙に突破されてしまう

境界線型と内部対策



エンドポイント対策②（EDR）



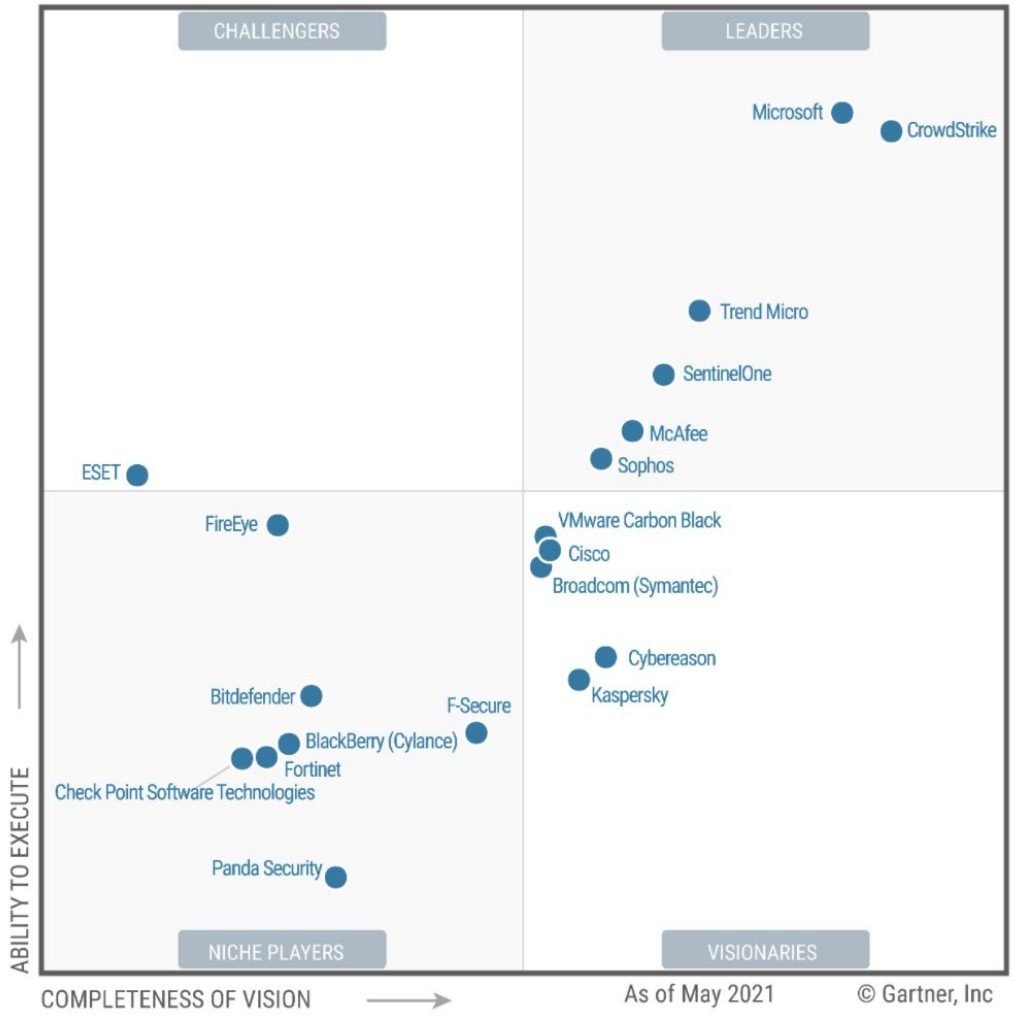
EDRとは

Endpoint Detection and Response（EDR）とは、
コンピュータシステムのエンドポイント（端末）において脅威を継続的に監視して対応する技術である。~ウィキペディア（Wikipedia)~

Endpoint Detection and Response（EDR）とは、
PC、サーバー、スマートフォン、タブレットなどのネットワークに接続されているエンドポイントの操作や動作の監視を行い、サイバー攻撃を受けたことを発見し次第対処するソフトウェアの総称

EDRとは

Figure 1: Magic Quadrant for Endpoint Protection Platforms



Source: Gartner (May 2021)

CROWDSTRIKE

Microsoft

kaspersky

cybereason

TREND MICRO

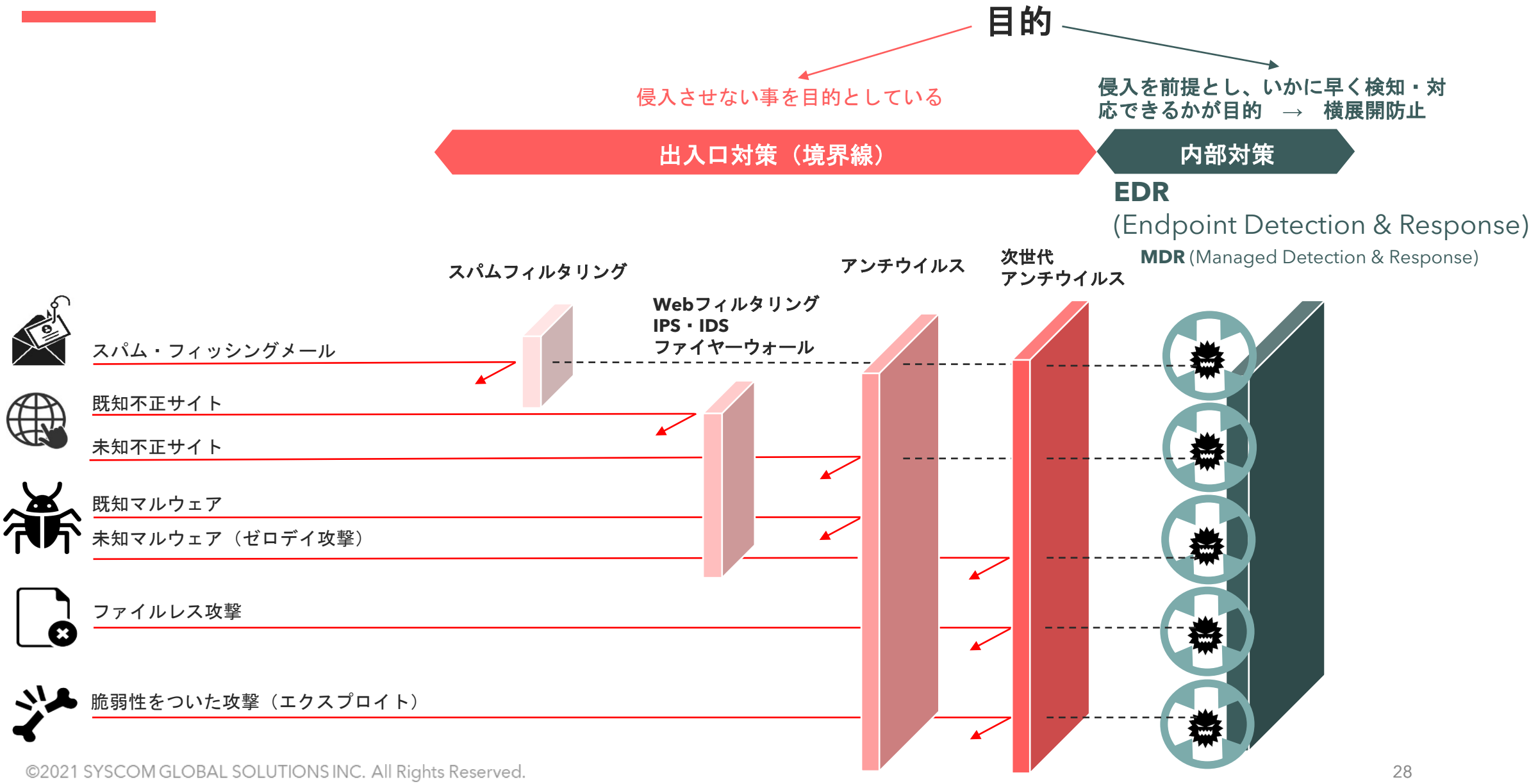
SentinelOne

Carbon Black.

McAfee
Together is power.

Symantec.

EDRとは

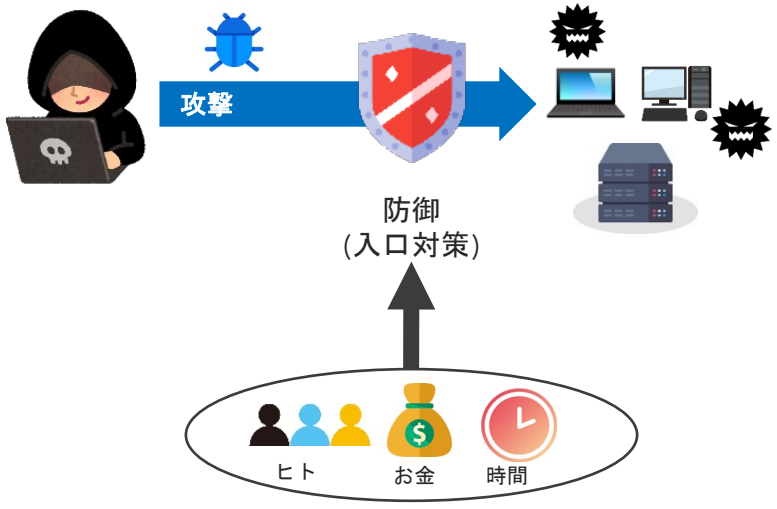


Endpoint Detection and Response (EDR)

SYSCOM GLOBAL SOLUTIONS

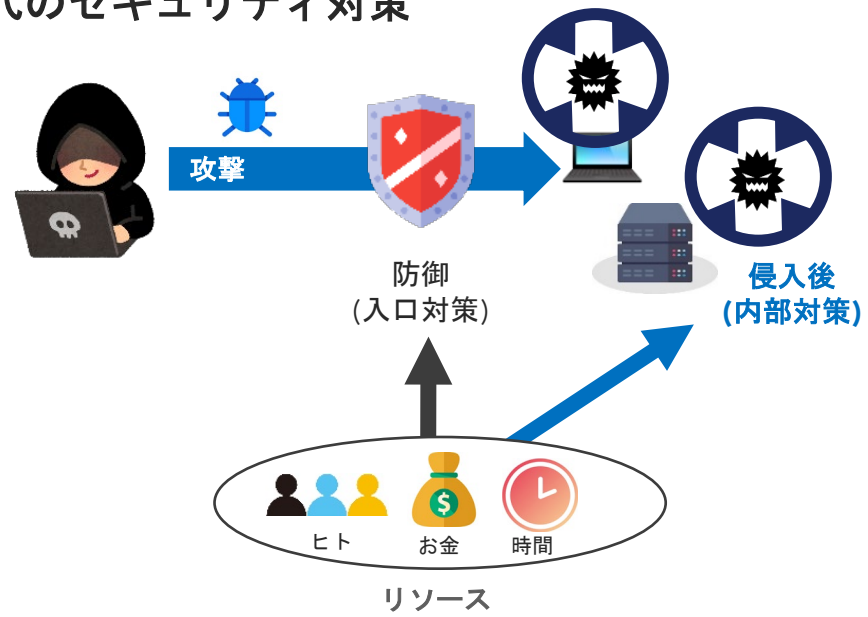
なぜEDRが必要か

従来のセキュリティ対策



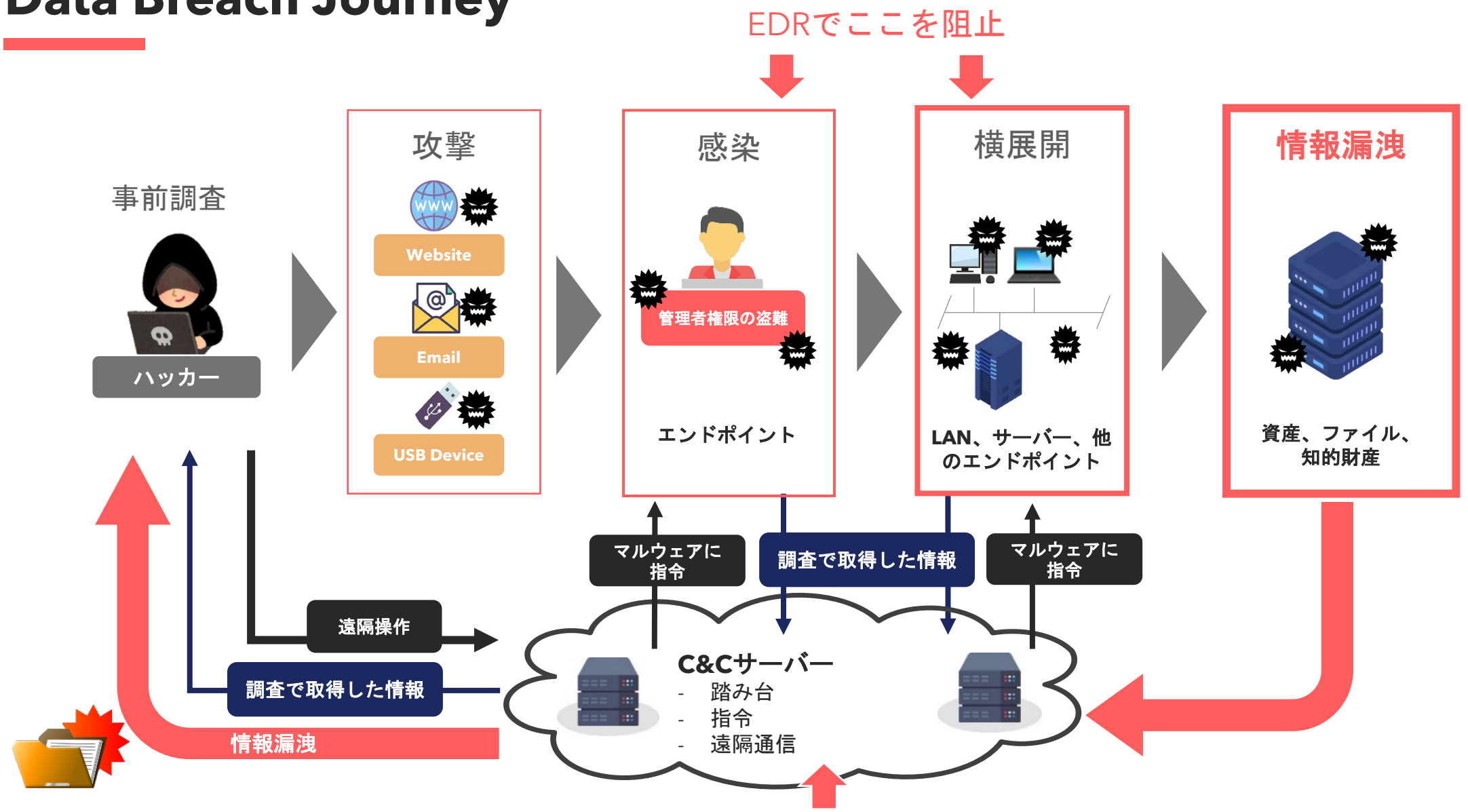
入口対策に重きをおく。侵入後の対策を講じていないため、侵入や脅威の検知が出来ず被害が発生してしまう。この入口対策の代表例の一つがアンチウイルスソフト

次世代のセキュリティ対策

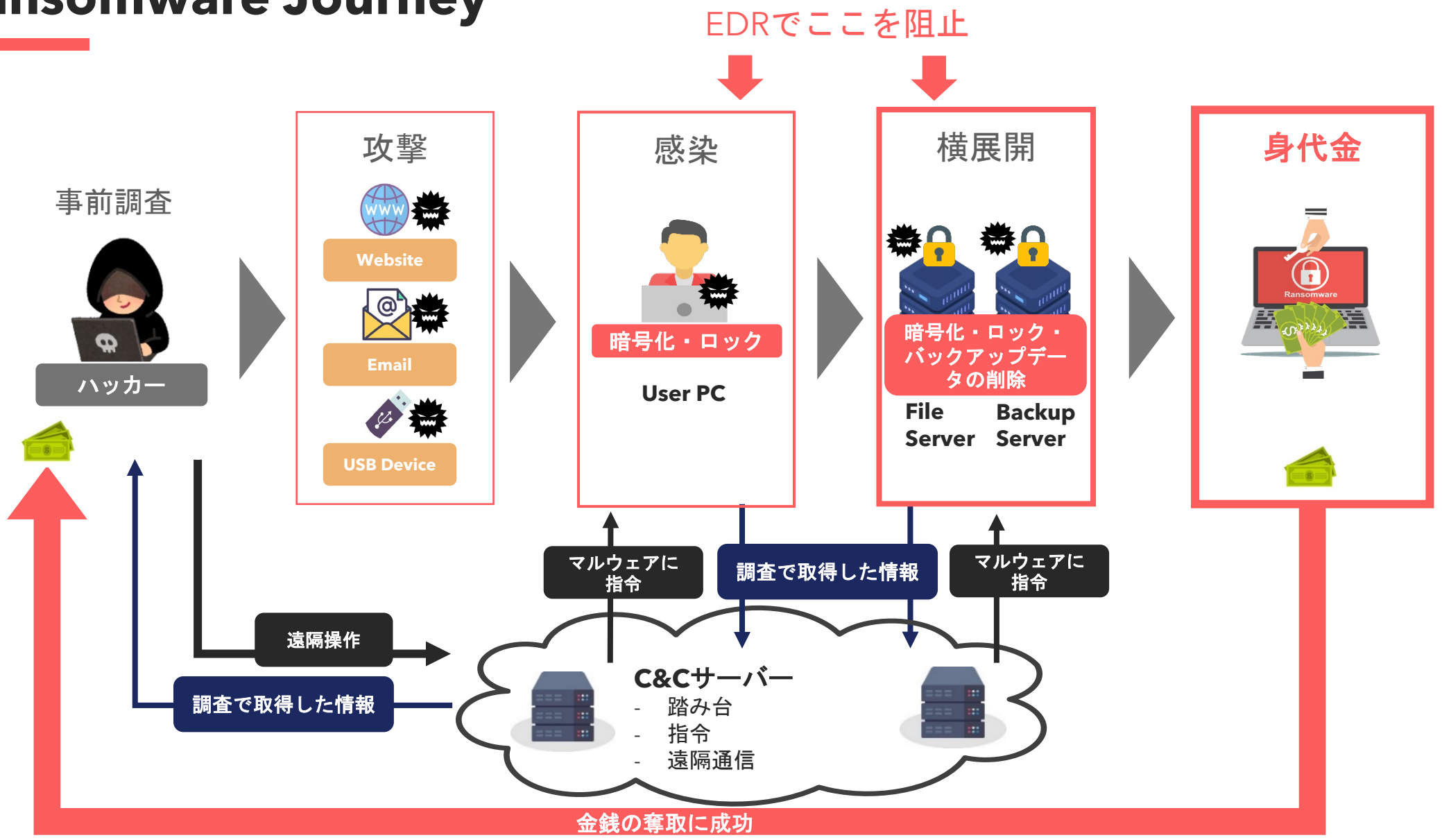


完璧な防御は無い。攻撃される又は侵入される事を前提としている。いくら入口対策にリソースを投じても、攻撃手法は常に姿形を変えて巧妙化しているため、攻撃者とは常にイタチごっことなってしまう。そこで次世代のセキュリティ対策では侵入される事を前提として、侵入や脅威をいかに早く検知し、隔離や遮断などの対応を取る事で、被害の発生を防ぐための内部対策が重要という考え方。Endpoint Detection & Response (EDR)はエンドポイントを対象とした内部対策

Data Breach Journey



Ransomware Journey



Managed Detection and Response (MDR)

SYSCOM GLOBAL SOLUTIONS

MDR by SYSCOM

Prevent → Detect → Respond

次世代アンチウイルス

- AI/機械学習
- 振る舞い検知
- 未知の攻撃を防御

EDR

- 侵入・攻撃検知
- 攻撃への対処
- ログ収集
- 脅威ハンティング

MDR

- アラート検知
- アラートの分析 (Triage)
- 情報収集

- 脅威の特定
- 優先度の判断
- 関係者への通知
- 隔離・根絶・復旧
- 報告・文書化
- レビュー (再発防止、対応改善)
- 注意喚起

CROWDSTRIKE

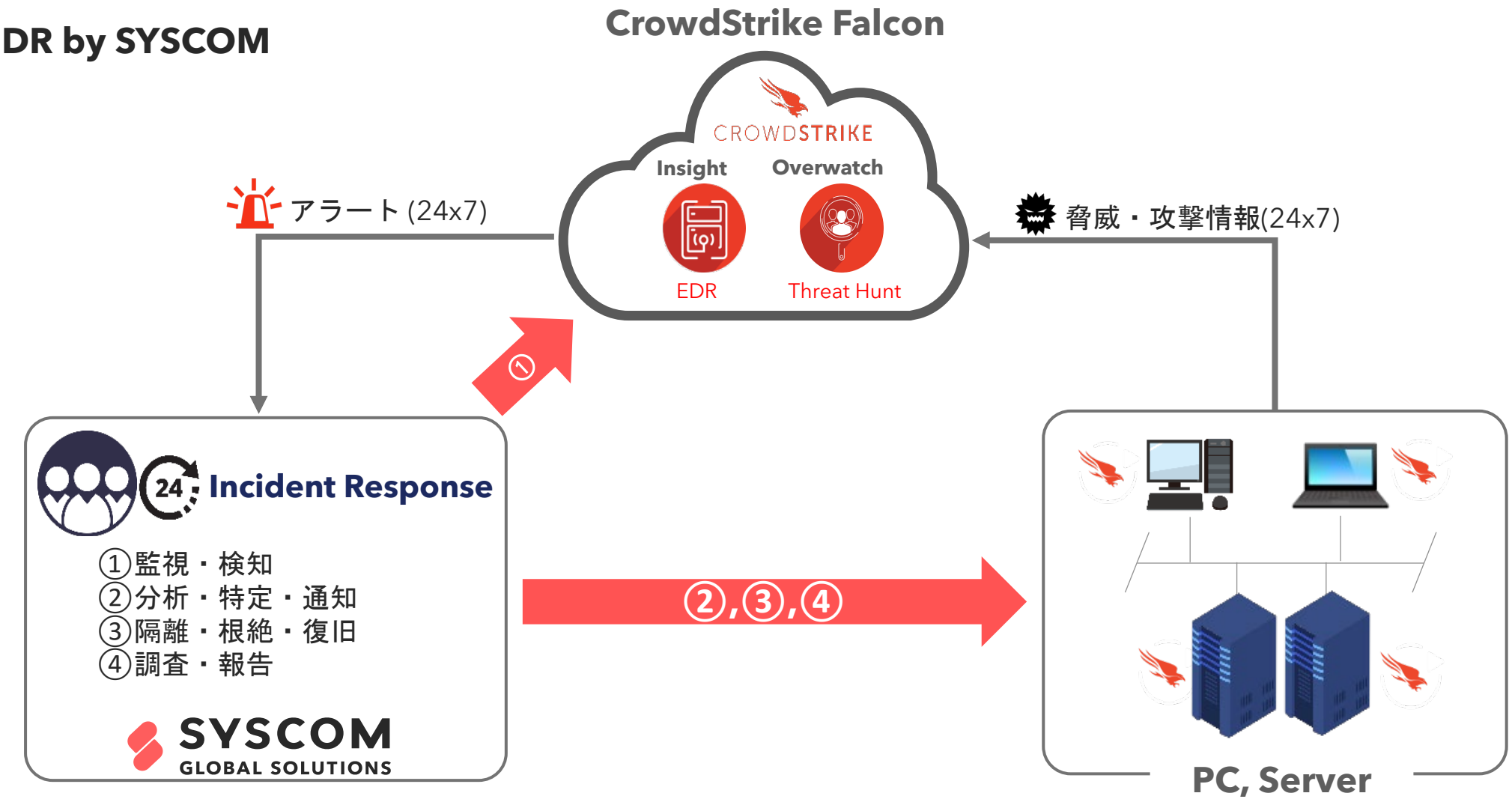
SYSCOM GLOBAL SOLUTIONS

CCFA

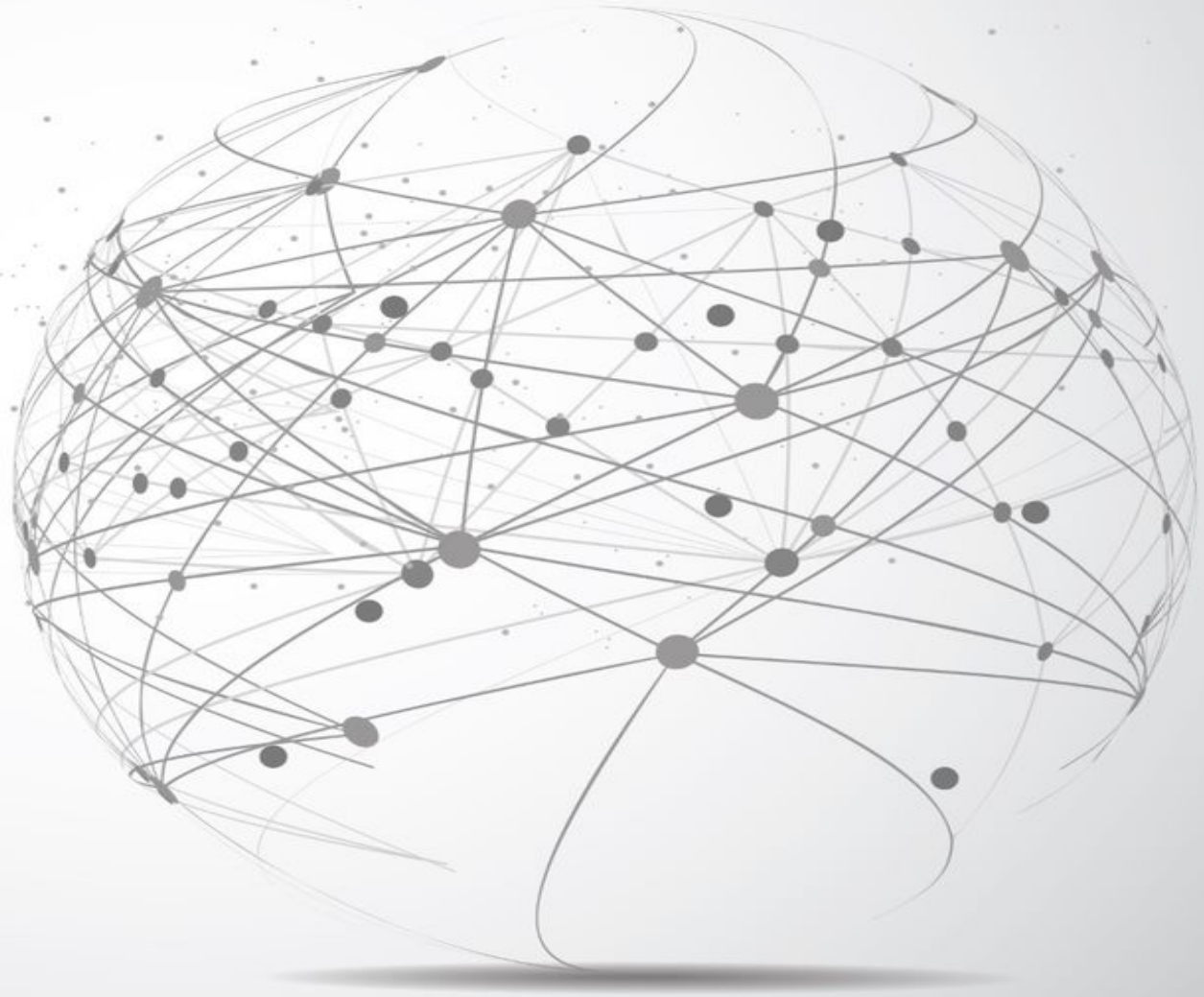
Managed Detection and Response (MDR)

SYSCOM GLOBAL SOLUTIONS

MDR by SYSCOM



サマリー



サマリー

■Email 対策は、トレーニングを継続的に実施、被害を減らすための社員の教育が重要

■従来の境界線型のセキュリティ対策→“ゼロトラスト”を前提としたセキュリティ対策

■”EDR”を用いて脅威の検知、対処までを実施し被害を最小限に抑える。

過去のウェビナービデオ・資料

SYSCOM GLOBAL SOLUTIONS

日本クラブ併催ウェビナー第1回
2021年最新サイバーセキュリティ事故の実態
~事例と数字で見る米国・日本のセキュリティ動向~

日本クラブ併催ウェビナー第2回
今求められるクラウドセキュリティ対策
~安全なクラウド利用を実現するCASBとは~

製造業向けウェビナー
短期間で効果的にDX・セキュリティ対策を推進する方法

https://syscomgs.com/ja/event