SYSCOM
GLOBAL SOLUTIONS

1. はじめに（自己紹介・会社紹介）
2. 数字が示すサイバーセキュリティの実態
3. 企業が避けるべきリスク
4. セキュリティ事故
5. 増大する被害
6. 対策とアプローチの変化
7. 肌で感じる事

はじめに（自己紹介）

213cm Andrea Bargnani (元NBAプレーヤー)

193cm

プロフィール（安田隆一郎）

年齢・趣味

- 37歳
- LEGO
- NYメッツ、NYニックス

シスコム歴・部署・役職

- 10年 (2011年入社)
- NY営業1部
- シニアマネジャー

プロジェクト実績

- EDR (Endpoint Detection and Response)
- SOC (Security Operation Center)
- SWG (Secure Web Gateway)
- 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

拠点

本社
ニューヨーク
1 Exchange Plaza
55 Broadway,11th Floor
New York, NY 10006
Tel: 212-797-9131 / Fax: 212-797-9132

支店
ロサンゼルス
21081 S. Western Avenue, Suite 240
Torrance, CA 90501
Tel: 310-965-4100 / Fax: 310-965-4135

シリコンバレー
2445 Augustine Drive, Suite 150
Santa Clara, CA 95054
Tel: 650-294-2500 / Fax: 650-294-2501

東京
100-0005
東京都千代田区丸の内１丁目６－２
新丸の内センタービルデング２１階
Tel: 03-3216-7351 / Fax: 03-3216-7210

プロジェクト拠点（実績）
APAC： 日本、香港、台湾、中国、タイ、シンガポール、マレーシア、タイ、ベトナム、ミヤンマー、インド

Americas：全米、カナダ、ブラジル、エクアドル、チリ、ペルー、コロンビア、パナマ、コスタリカ、ボリビア、ガテマラ、アルゼンチン、ニカラグア、メキシコ

EMEA：イギリス、オランダ、ドイツ、UAE

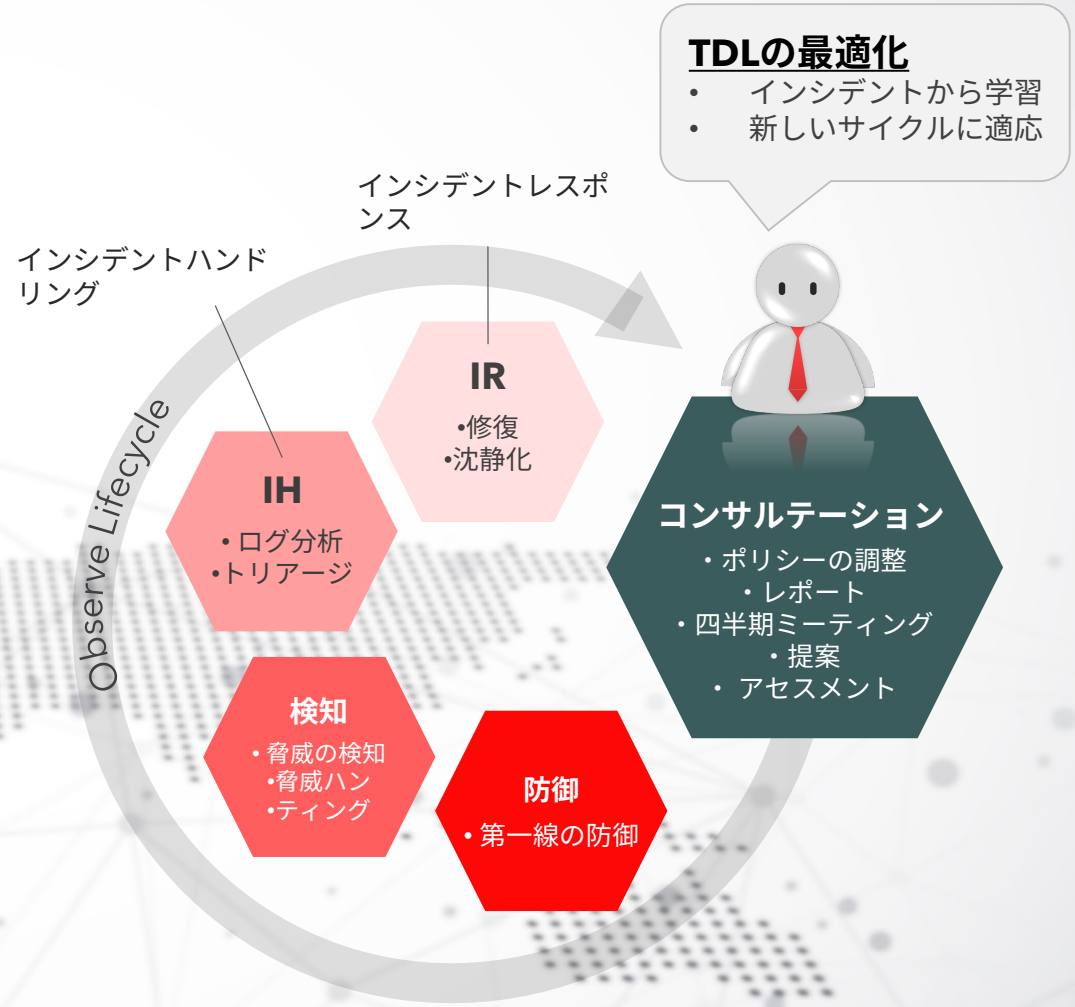
Global & Local Partners: 100社以上

当社のセキュリティ

Threat Defense Lifecycle (TDL)

一貫したサイクルの提供がサービスの主な特徴

- ソリューションの立案や製品の提供ではなく、サイクルの維持と改善が主眼
- サイクルの維持、見直しを図る事で、最新の脅威から遅れを取る事なく、着実にセキュリティ課題の解決に寄与



数字が示すサイバーセキュリティの実態

情報漏洩

Personal data was involved in 58% of breaches in 2020. (Verizon)	情報漏洩のうち**58%**は個人データが関与
60% of Breaches in 2019 Involved Unpatched Vulnerabilities (Security Blvd)	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
28% of the Breaches in 2019 Involved Small Business Victims (Verizon)	情報漏洩被害の**28** %は中小企業で起きている
63% of SMBs Report Experiencing a Data Breach in 2019 (Keeper Security and the Ponemon Institute)	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
86% of breaches were financially motivated and 10% were motivated by espionage. (Verizon)	情報漏洩をさせる動機の**86%**は金銭であり**10%**がスパイ活動
The average cost of a data breach is $8.19 million in U.S as of 2020 (Digital Guardian)	情報漏洩による米国での平均被害額は**$8.19 Million**

*パッチ ＝ PCやサーバーのWindows アップデートや、ネットワーク機器のFirmwareアップデートなど

対策

43% of SMBs Lack Any Type of Cybersecurity Defense Plans (Bullguard)	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
68% of business leaders feel their cybersecurity risks are increasing. (Accenture)	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
40 percent of IT leaders say cybersecurity jobs are the most difficult to fill. (CSO Online)	IT管理者の**40%**がサイバーセキュリティポジションの適任者を見つけるのが難しいと感じている
the average spending on security increased from 2,337 dollars pe employee in 2019 to 2,691 dollars in 2020. It is nearly a 16% Increase from 2019. (Deloitte)	セキュリティ対策への従業員1名あたり平均投資額は**$2,691** (前年比16%Up)
Forensic Technology Market Size Worth $50.41 Billion By 2027. $19.86 Billion in 2019. (Reports and Data)	フォレンジックテクノロジー市場は2027年には**$50.41 Billion**に到達。2019年は**$19.86 Billion**

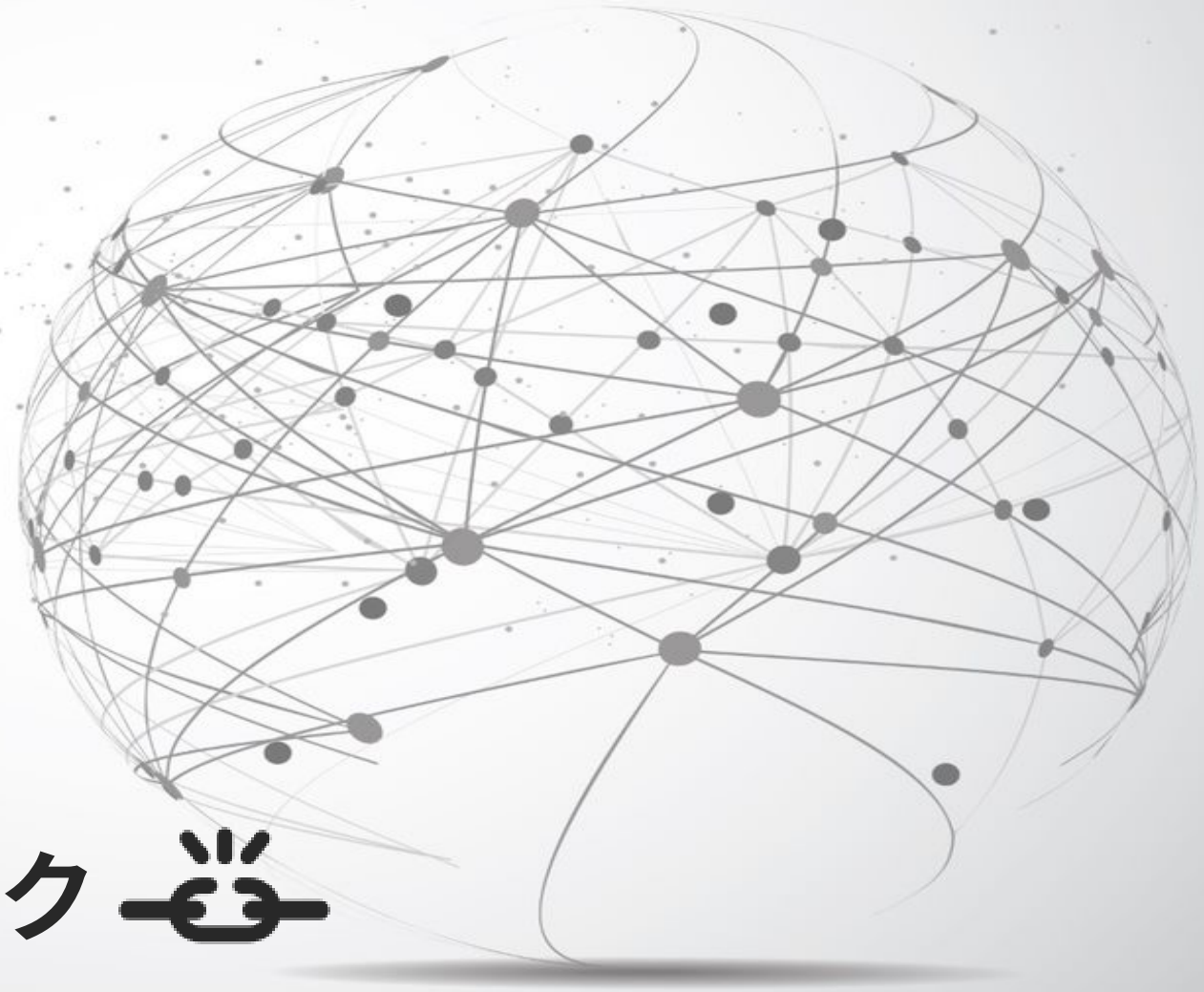
金融業、IoT、パンデミック

1 in 4 malware attacks targeted financial service firms, leading any other industry. (Insights)	• マルウェア攻撃の**1/4**は**金融業**が標的となっている（業種別一位）
According to the 2020 Phishing report, around 31% of banking employees failed to pass a phishing test. (KnowBe4)	• 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
Attacks on IoT devices tripled in the first half of 2019. (CSO Online)	• IoT機器を狙った攻撃は**3倍**増加
Since the pandemic began, the FBI reported a 300% increase in reported cybercrimes (FBI)	• パンデミック後のサイバー犯罪は**300**%増加

ランサムウェア

The average total cost of recovery from a ransomware attack doubled, increasing from $761,106 in 2020 to $1.85 million in 2021 (Sophos)	• ランサムウェア被害からの復旧に掛かる平均費用は**$1.81million** in 2021 （前年比 約**2倍**）
The average ransom paid was $170,404 in 2021 (Sophos)	• ランサムウェアの平均支払い額は**$170,404**
8% of organizations managed to get back all of their data after paying a ransom, with 29% getting back no more than half of their data (Global Findings)	• ランサムウェアを支払った企業のうち**8%**が全データの復旧に成功し、**29%**は全データのうち半分しか復旧できなかった
Ransomware Attacks Predicted to Occur Every 11 Seconds in 2021 (Cybersecurity Ventures)	• **11**秒に一度ランサムウェア攻撃が仕掛けられている

Live Attack Map https://threatmap.bitdefender.com/



企業が避けるべきリスク

直接的被害

業務の停止

・コアシステムの停止　・生産システムの停止　・出入庫システムの停止　・ファイルサーバー停止

・メール送受信の停止　・経理システムの停止

情報の紛失・改ざん・漏洩

・営業活動の停滞、中断　・Webページの閉鎖　・関係の連絡・お詫び

インシデント費用、なりすまし

・ランサム支払い　・原状回復までの復旧費用　・事故の原因究明・調査費用

・なりすましによる架空請求への支払い

間接的被害

SYSCOM GLOBAL SOLUTIONS

損害賠償

・情報漏洩した情報の持ち主　・二次被害を与えた他者への損害賠償

公的な処罰

・事業免許の取り消し・停止　・行政指導による業務停止

社会的信用の低下

・社会的信用の喪失　・ブランドイメージや風評の悪化　・株価下落

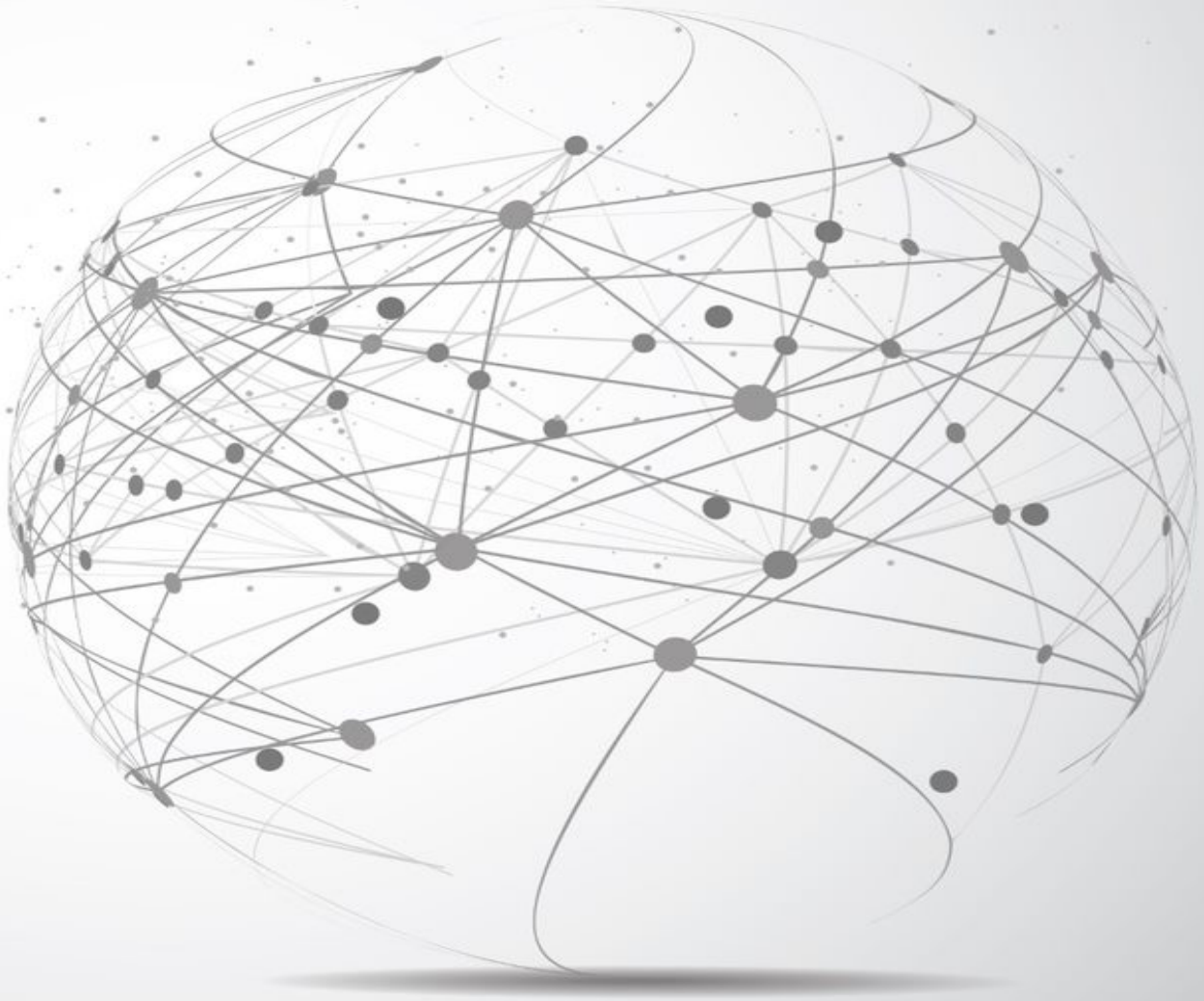
売上の減少

・顧客からの取引縮小・停止　・営業機会の損失　・マーケットシェア低下

社内の業務効率・モラル低下

・業務効率の低下・過重労働　・従業員の不安・不満　・モラル低下

セキュリティ事故



某通信会社

事件プロフィール

事件概要

- 電子決済サービスを通じて、利用者の預金が不正に引き出された事が判明

着眼点

- **利便性**を上がった一方で、**セキュリティ**の脆弱性を突かれた事が要因。なりすました銀行口座の開設が出来る仕組みとなっていた。

アクセス管理

- MFA (Multi-Factor Authentication)
- IAM (Identity Access Management)
- PAM (Privilege Access Management)

某ゲーム会社

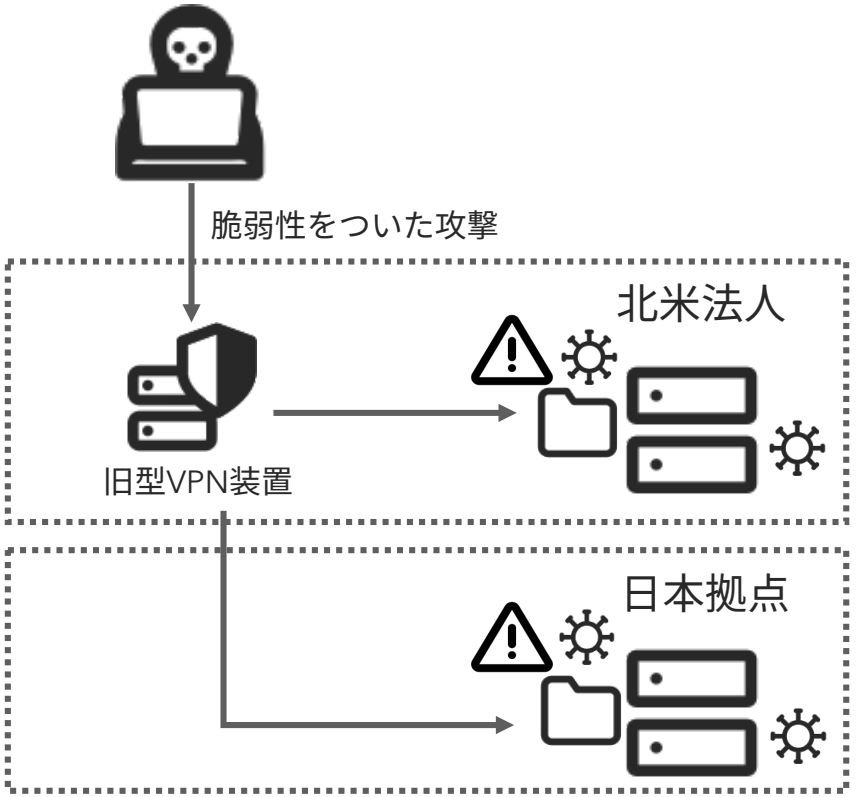
事件プロフィール

事件概要

- サイバー犯罪グループ(Ragnar Locker)からの不正アクセスにより、顧客や取引先に関する情報が最大で39万人分流出した。

着眼点

- **テレワーク**の需要が高まり、緊急対応で**旧型のVPN装置**を利用したところ攻撃され、ネットワーク内へと不正に侵入し、一部の機器に対する乗っ取りに成功



資産管理、脆弱性管理

- パッチ管理
- 資産管理
- 社内ポリシー
- 脆弱性診断・ペネトレーションテスト

某システム会社

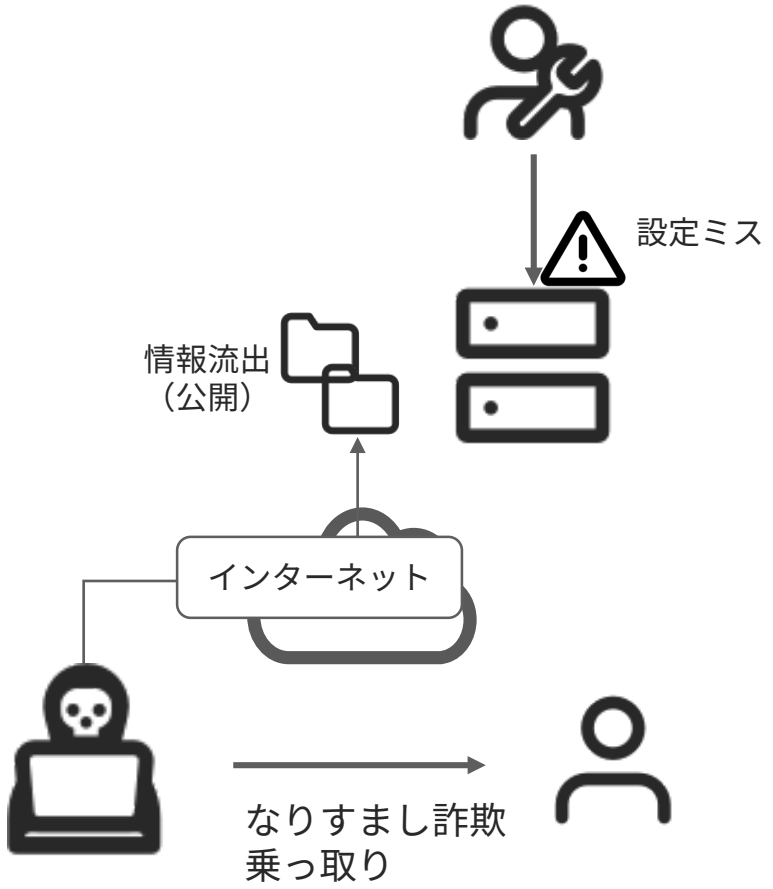
事件プロフィール

事件概要

- 設定ミスが原因で外部より少なくとも2億5000件のデータが2日間にわたって公開されていた

着眼点

- 流出したデータは個人を特定できる情報はないものの、2005年～2019年までのカスタマーサポートと顧客とのやり取りのログが含まれていたため、なりすまして顧客に連絡を取り、最終的に乗っ取りされる危険性がある



運用プロセスの見直し
社内教育の徹底

某自動車メーカー

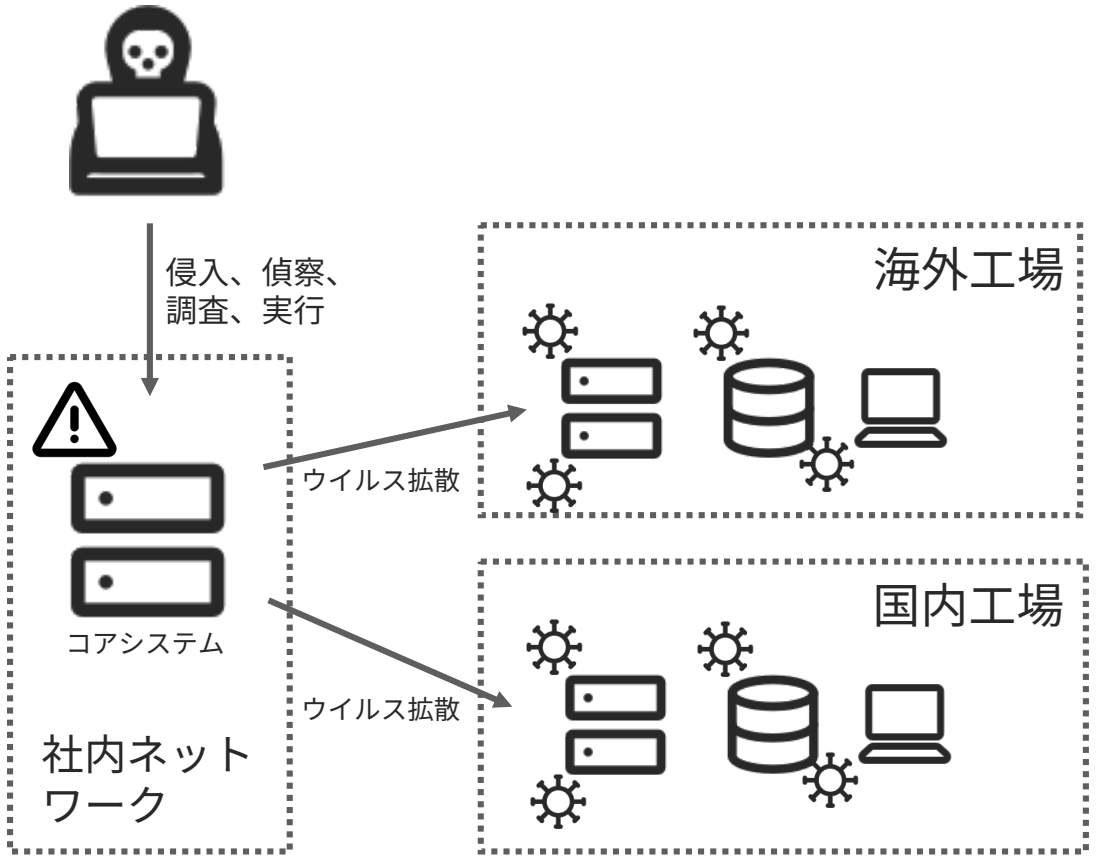
事件プロフィール

事件概要

- 社内のコアシステムをピンポイントに狙われ、社内データが暗号化された。結果、社内のネットワークに障害が起き、国内や海外の工場でのオペレーションに影響が出た

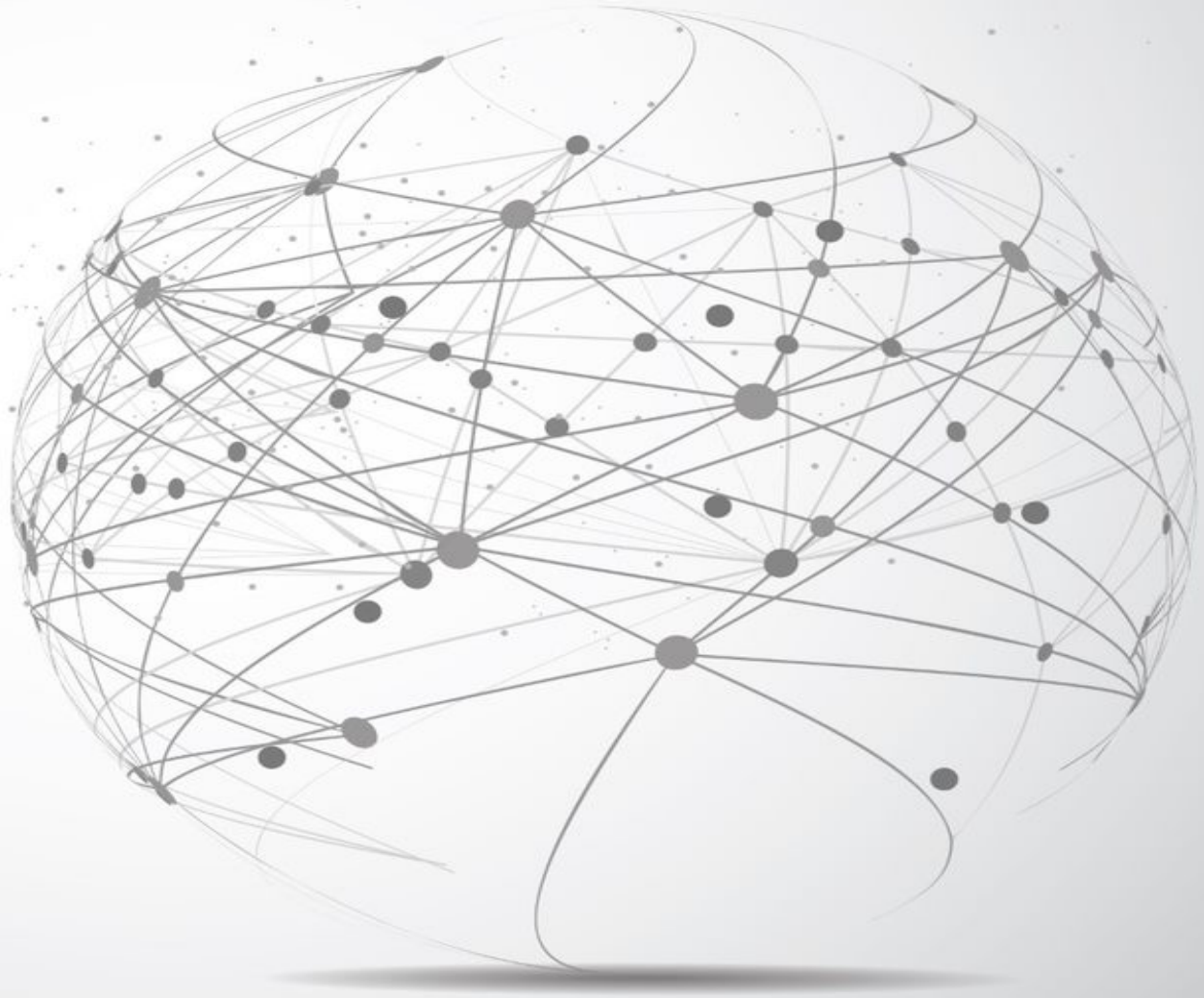
着眼点

- 特にセキュリティが厳しいコアシステムに侵入されたため、事前に内部に侵入するなどして、攻撃を仕掛けるための調査・準備を周到に進めていた可能性が高い

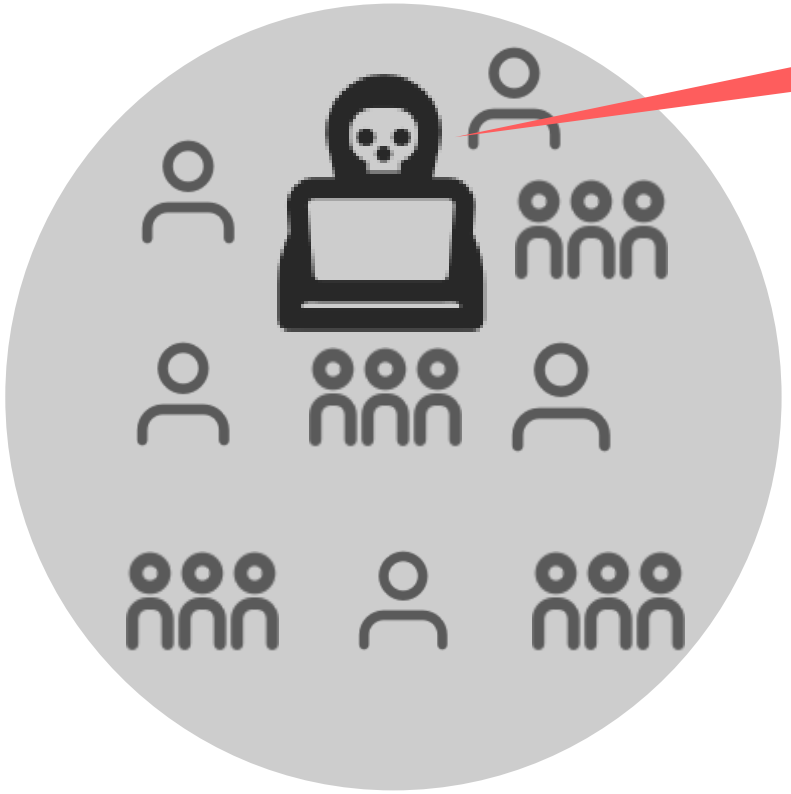


詳細についてはセキュリティー上の観点から公表されていない

増大する被害



攻撃者



犯人プロフィール

年齢・性別

- 10代~30代（80%）
- 平均17歳

タイプ別

- 国による諜報活動
- 企業のスパイ
- プロのハッキング集団
- ゲーム感覚（娯楽）

動機・目的

- 金銭目的
- スパイ行為
- 興味・達成感

手口

- Email
- ウェブサイト
- USBなどの外部デバイス

増大する要因となっているもの

SYSCOM GLOBAL SOLUTIONS

OK例
- Microsoft 365 (Office 365)
- Box
- AWS
- Azure
- 本社システム(日本)

公認（判定済み、利用許可）

NG例
- Google (Google Drive)
- Dropbox
- Evernote
- Personal Email

Shadow IT (非公認、漏洩リスク、感染リスク、未対策)

インターネット

自宅

- 自宅ネットワーク(ルーターなど)の脆弱性を狙った攻撃
- 自由にウェブ、クラウドの利用が可能
- エンドポイント対策の強化が重要に

ユーザー環境の変化

オフィス

- 従来通り（境界線型）ある程度のセキュリティ対策は取っているが、追い付かなくなっている

- ファイヤーウォール
- ウェブフィルタリング
- IPS/IDS
- スパムフィルタリング
- アンチウイルス

従来型対策の限界

工場・施設

- これまでITとは切り離れていた設備や機械のIoT化により、セキュリティリスクが発生
- デジタル化推進により、利便性はUPしたが、セキュリティとのバランスが取れなくなる

IoT化、デジタル化の推進

対策とアプローチの変化 □»□

考え方の変化（パッチ）

SYSCOM GLOBAL SOLUTIONS

パッチ管理

パッチを更新する事でシステムに不具合や障害が起きる可能性はある。ただしパッチを更新しなければセキュリティ事故に繋がってしまう。

リスク比較

システム障害　v.s　セキュリティ事故

バックアップからの切り戻しよる復旧は可能（予測可能）

場合によっては復旧に膨大な時間が掛かる、または完全な原状復帰が困難になる場合もある

情報漏洩等の重大事故を防ぐために、定期的な**脆弱性診断**によるパッチ更新状況の確認と、**パッチ更新**の運用がとても重要

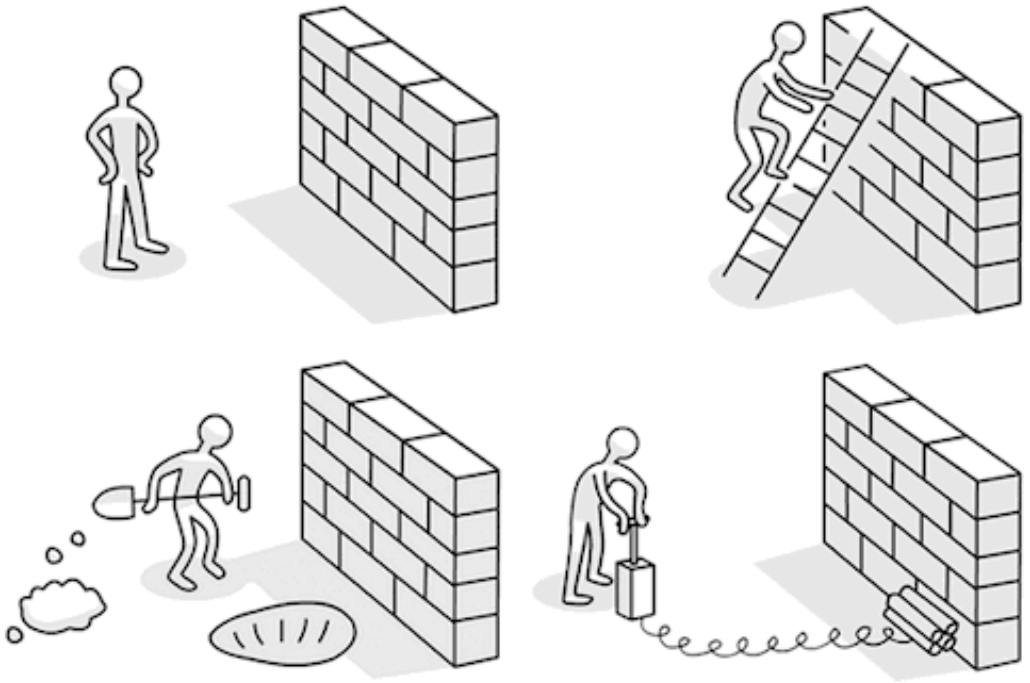
考え方の変化（内部対策）

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。

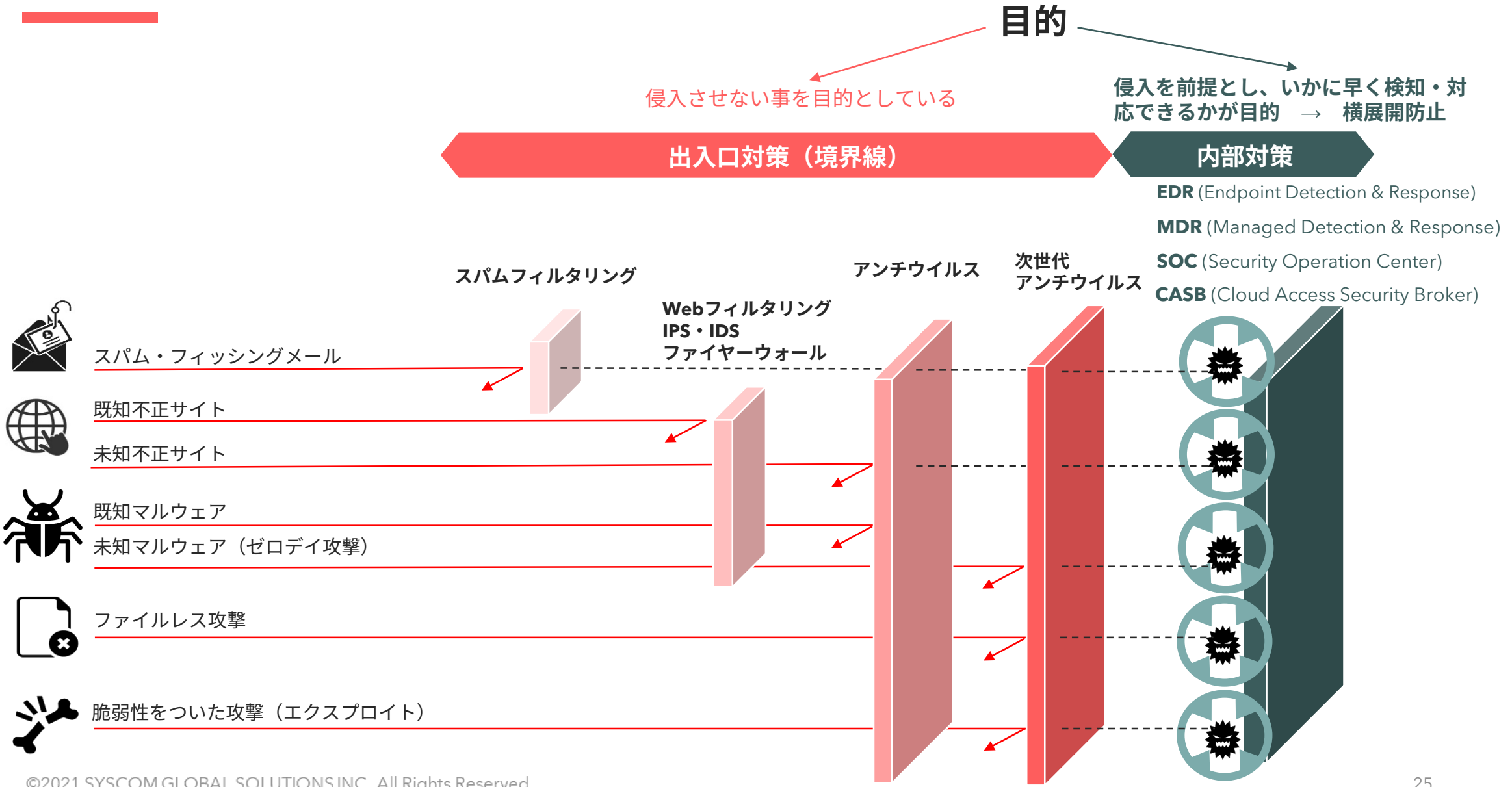
内部対策（ゼロトラスト）

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）

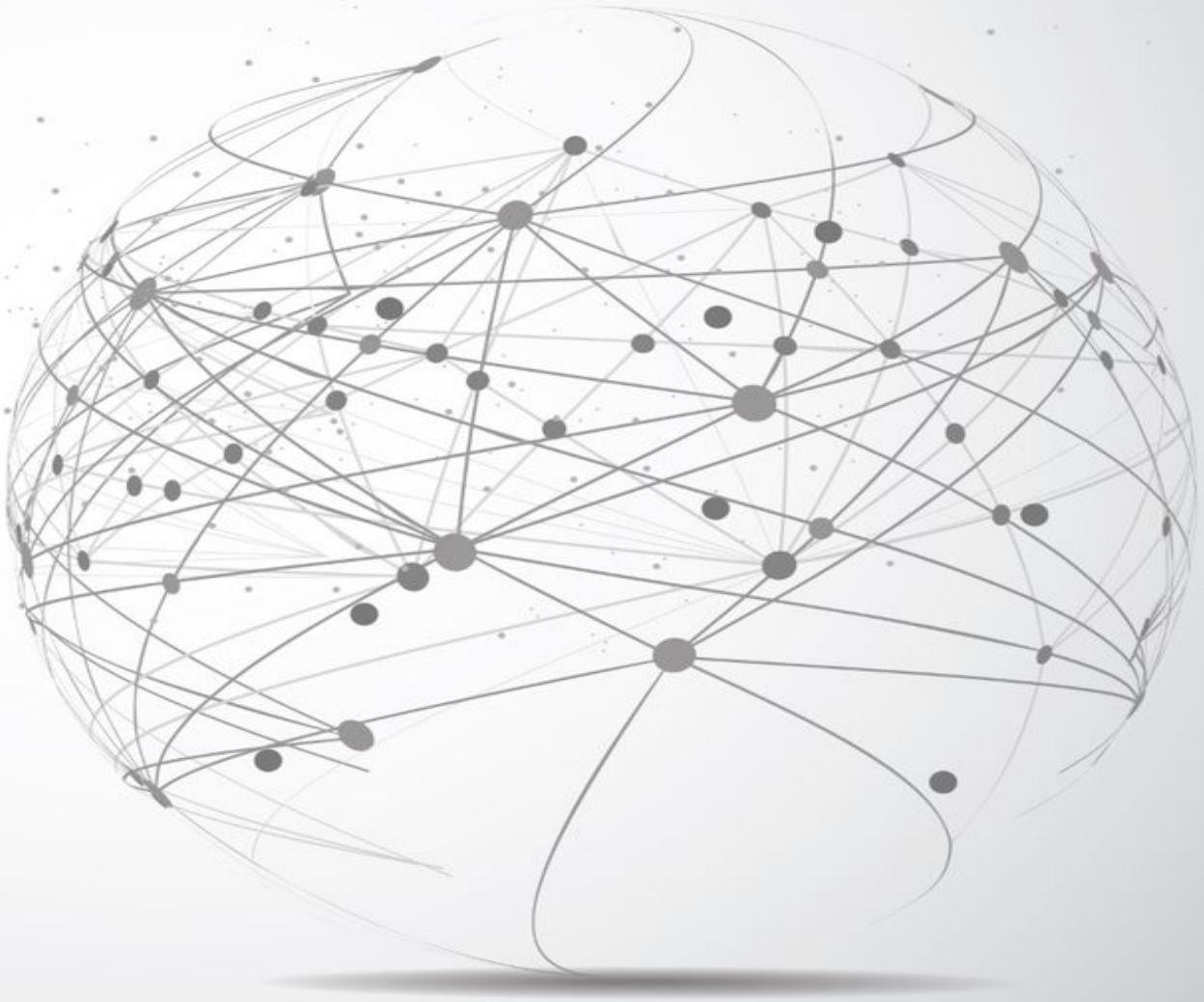


境界線は巧妙に突破されてしまう

境界線と内部対策



肌で感じること



対策が進まない６つの理由

SYSCOM GLOBAL SOLUTIONS

1. 親会社や情報システム部からの明確な指示がない
2. 計画や実施に手間、負荷、時間が掛かる
3. 今のところ大きな事故がないため、対策は万全だと思っている
4. 対策を考える上での社内の専門家や知見を有した人材が不在
5. システム導入後の、管理や運用ができるパートナーがいない、知らない
6. 大きな予算の確保が困難

今やるべきこと、できること

SYSCOM GLOBAL SOLUTIONS

1

短期ー中期のロードマップを作り、適切な予算を正確に把握し、具体的な実行プランを立てる

2

与えられた現状で最大限に実施できる策を練り、時間を掛けずに実施を進める

例：棚卸、資産管理 &パッチ、MFA（多要素認証）、パスワード管理、脆弱性診断・ペネトレーションテストなど、

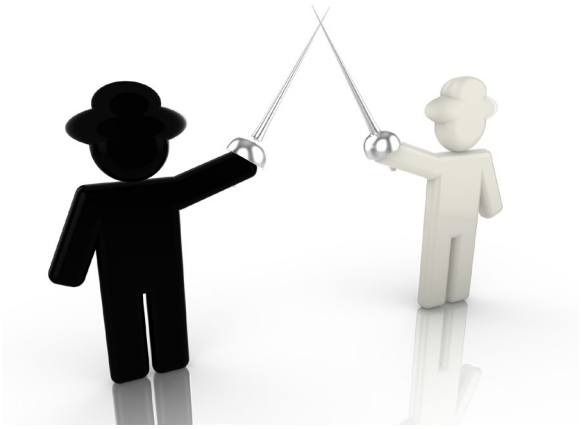
3

外部組織に相談し、情報を得るまたはサービスを受ける

（1,2が共に自社では対応が困難である場合）

サマリー

- リモートワーク、IoT化、デジタル化推進に起こるセキュリティ脅威
- 境界線型セキュリティの限界　→　内部対策の強化
- 事故は単純なエラーから発生する
- できることから　→　棚卸＆パッチ（定期＆自動化、Plan B）
- 時間との勝負



実践編、対策事例

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
05/12　~事例と数字で見る米国・日本のセキュリティ動向~

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
06/16 (仮)　~安全なクラウド利用を実現するCASBとは~

ウェビナー第3回　テレワーク環境下におけるITセキュリティリスクと最新の対策
07/14 (仮)　~ゼロトラストモデルとエンドポイントセキュリティ対策~