TLP:GREEN

企業利益を守るための サイバーインテリジェンス

2021年 12月

名和 利男

概要

昨今のサイバー攻撃や内部犯行に立ち向かうには、経営層自らが、「網羅的な状況認識」と「客観的かつ合理的な意思決定」を伴った対策を講じなければなりません。

しかし、現実的には、特定の領域に特化した部門に対策を任せてしまい、部分最適な状態に陥っています。

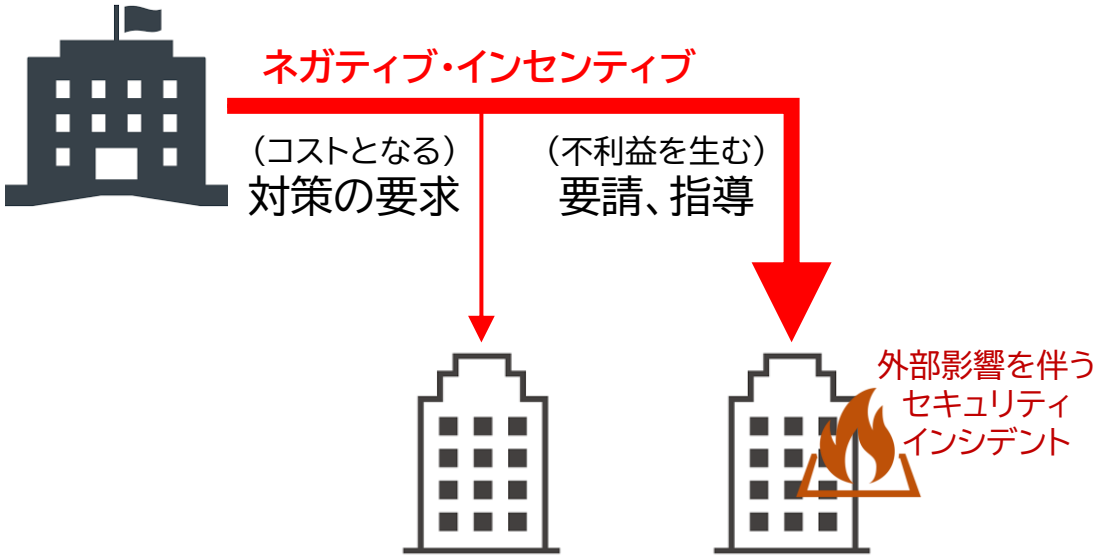
これを改善するには、**徹底的に現実を直視**することが最善策となります。

皮肉なことに、深刻な被害を経験した企業の経営層が、この重要性を強く認識し、自らが「サイバーインテリジェンス」を強化しています。

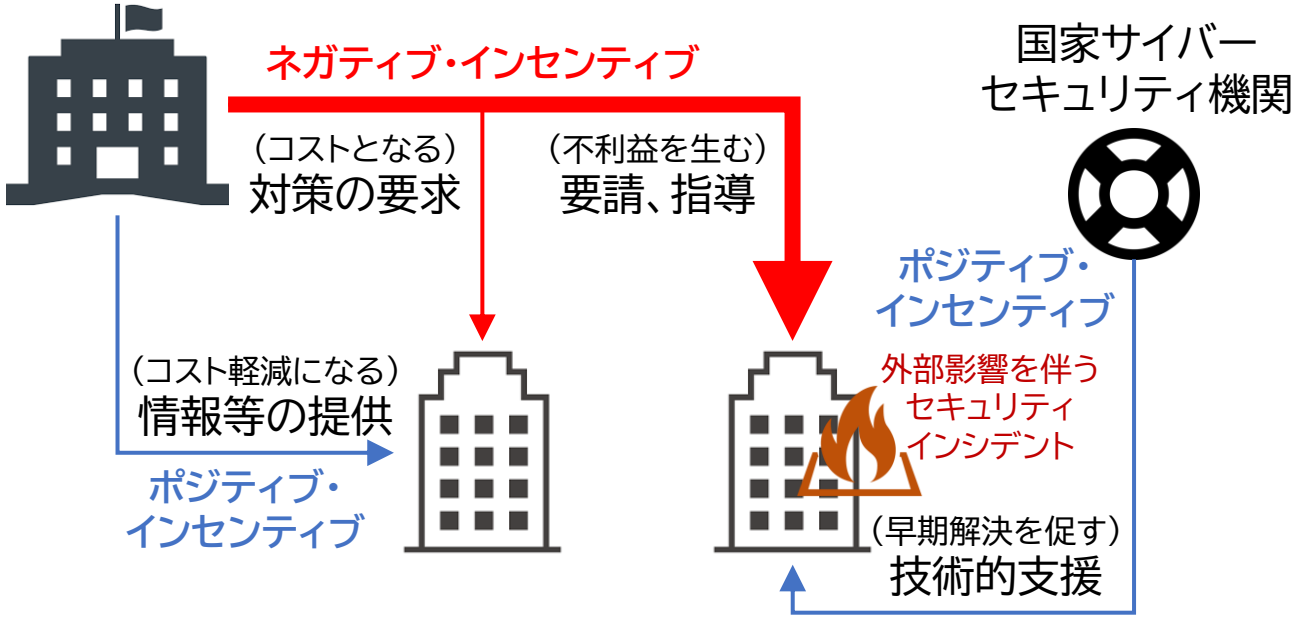
TLP:GREEN

問題意識

日本



他の主要国



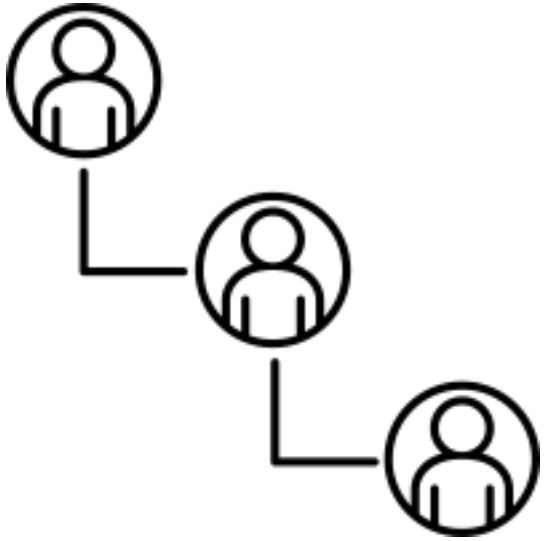
TLP:GREEN

日本型組織の二重構造 – ほぼすべての意思決定プロセスが遅い

日本型組織は、依然として**「表面的な組織構造」と「内面的な組織構造」の2つが共存**している。

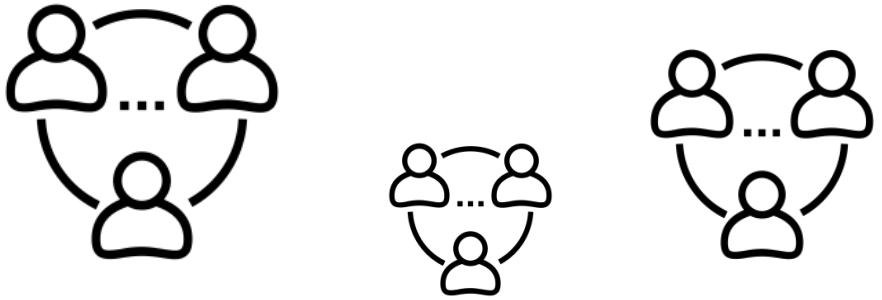
表面的な組織構造

- ピラミッド型の階層化された権限
- トップダウン型の上意下達
- 規律やルールによるガバナンス（統制）



内面的な組織構造

- 同じ階層における社員間の非公式なやり取り
- 横並び意識と同調圧力の場の空気
- 上位階層への忖度と隣接領域への根回し



昭和時代の高度経済成長時代における製造産業に最適であった内面的な組織構造といえる。
安定かつ高品質な製品や商品を生産するには、全員が一つの目標に向けた行動が求められ、尖った個性は邪魔になりやすい。

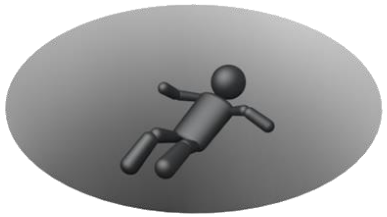
TLP:GREEN

日本型組織の状況認識不足 – 深刻なまでに酷い

不十分な状況認識

サイバー攻撃によるインシデントで、事業停止・営業機会の損失が**加重**

適切な状況認識



自組織の環境と想定するサイバー攻撃に適応したサイバーセキュリティ対策(**発生回避、拡大抑止、迅速対処、早期回復**)により、事業停止・営業機会損失を**軽減**

TLP:GREEN

米国企業でも「不十分な状況認識」で甚大な被害が発生 – **Twitter Hack**

2020年7月15日、17歳のハッカーとその共犯者が**Twitterのネットワークに侵入**し、知名度の高いユーザーに割り当てられた数十個のTwitterアカウントを掌握しました。

ハッカーたちは、数時間にわたり、**著名人のアカウントを次々と奪い取り**、「ビットコインを2倍にする」という詐欺をツイートするなど、公開サイバー攻撃を行い、世界中が注目しました。

ハッカーたちは、バラク・オバマ、キム・カーダシアン・ウェスト、ジェフ・ベゾス、イーロン・マスクなどの政治家、著名人、起業家のTwitterアカウントや、ニューヨーク州金融サービス局が規制する複数の暗号通貨会社のTwitterアカウントを乗っ取りました。

そして、数時間の間、Twitter社はこの**ハッキングを止めることができなかった**ようです。

https://www.dfs.ny.gov/Twitter_Report

Twitter社のサイバーセキュリティの弱点に起因したハッキング (1/3)

Twitter社のハッキング事件（以下、Twitter Hack）は、素朴なサイバー犯罪者であっても、多大な被害をもたらすことができるということを示す教訓的な物語です。ハッカーが成功したのは、**Twitter社の内部のサイバーセキュリティプロトコルの脆弱性**が大きな要因となっています。

問題は上層部から始まっていました。Twitter社は、ツイッターハックの7カ月前の2019年12月以降、最高情報セキュリティ責任者（以下、CISO）を置いていませんでした。**強力なリーダーシップとシニアレベルの関与の欠如**は、サイバーセキュリティの弱点の共通の原因となります。 強力なリーダーシップは、COVID-19のパンデミックによってITとサイバーセキュリティに多くの新しい課題が生じた2020年には特に必要です。

多くの組織と同様に、Twitter社も3月にパンデミックの影響でリモートワークに移行しました。**この移行により、Twitter社はサイバー攻撃を受けやすくなり、既存の弱点がさらに悪化**しました。

https://www.dfs.ny.gov/Twitter_Report

Twitter社のサイバーセキュリティの弱点に起因したハッキング (2/3)

ハッカーは、Twitterのリモートワークへの移行を直接利用しました。この問題を利用して、**ハッカーは、VPNの問題についてTwitterのIT部門から電話がかかってきたように装い、実際のVPNログイン・サイトと同じようにデザインされたウェブサイトに認証情報を入力するように従業員を説得しました。**なぜなら、Twitter社の従業員は皆、VPN接続を利用して仕事をしており、IT部門の支援を必要とするようなVPNの問題を日常的に経験していたため、ハッカーたちの主張ははるかに信頼性が高く、最終的に成功しました。

ハッカーたちは、ソーシャル・エンジニアリングというシンプルな手法でTwitter社に侵入しました。ソーシャル・エンジニアリングとは、人を騙して機密情報や個人情報を聞き出し、それを後になって不正な目的に利用することです。最もよく知られているソーシャル・エンジニアリング攻撃は、フィッシングと呼ばれるもので、受信者を騙して悪意のある添付ファイルを開かせたり、ユーザー名やパスワードを入力させたりするものです。**今回のハッカーは、電話でソーシャルエンジニアリングを行う「ビッシング」を利用しました。**フィッシングとビッシングは、ハッカーがネットワークへのアクセスを得るために用いる最も一般的な手法のひとつです。例えば、2020年1月から7月の間に、同省に提出された重大なサイバーセキュリティインシデントの通知のうち、約3分の1がフィッシングやビッシングを利用したものでした。

また、ハッカーたちは、自分たちの欺瞞の信憑性を高めるために、Twitter社とその従業員に関する基本的な情報に依存していました。**ハッカーたちは、TwitterのIT部門になりすますために、Twitterの従業員の基本的な機能や肩書きを特定する調査を行っていた**ようです。これらの個人情報で武装したハッカーは、複数のTwitter社員に自分がTwitterのIT部門の人間であると信じ込ませ、認証情報を盗むことに成功しました

Twitter社のサイバーセキュリティの弱点に起因したハッキング (3/3)

今年の初めには、パンデミックによって生じた新たなセキュリティリスクを特定して評価するよう、規制対象の企業にガイダンスを発行し、他の公的・民間の情報源からも同様のアラートが出されました。

注目すべきは、Twitter社が2020年3月以降、**遠隔地にいる従業員に対するこのリスクの高まりを緩和するための重要な代償措置を実施しなかった**ため、ハッカーたちがそれを利用したということです。

Twitter社の功績として、Twitter社は今後同様の攻撃を防ぐために、MFA（多要素認証）の改善やサイバーセキュリティ意識の向上のための追加トレーニングなど、追加のセキュリティ管理を実施中であることを同省に通知しており、2020年9月下旬には新しいCISOの採用を発表しました。

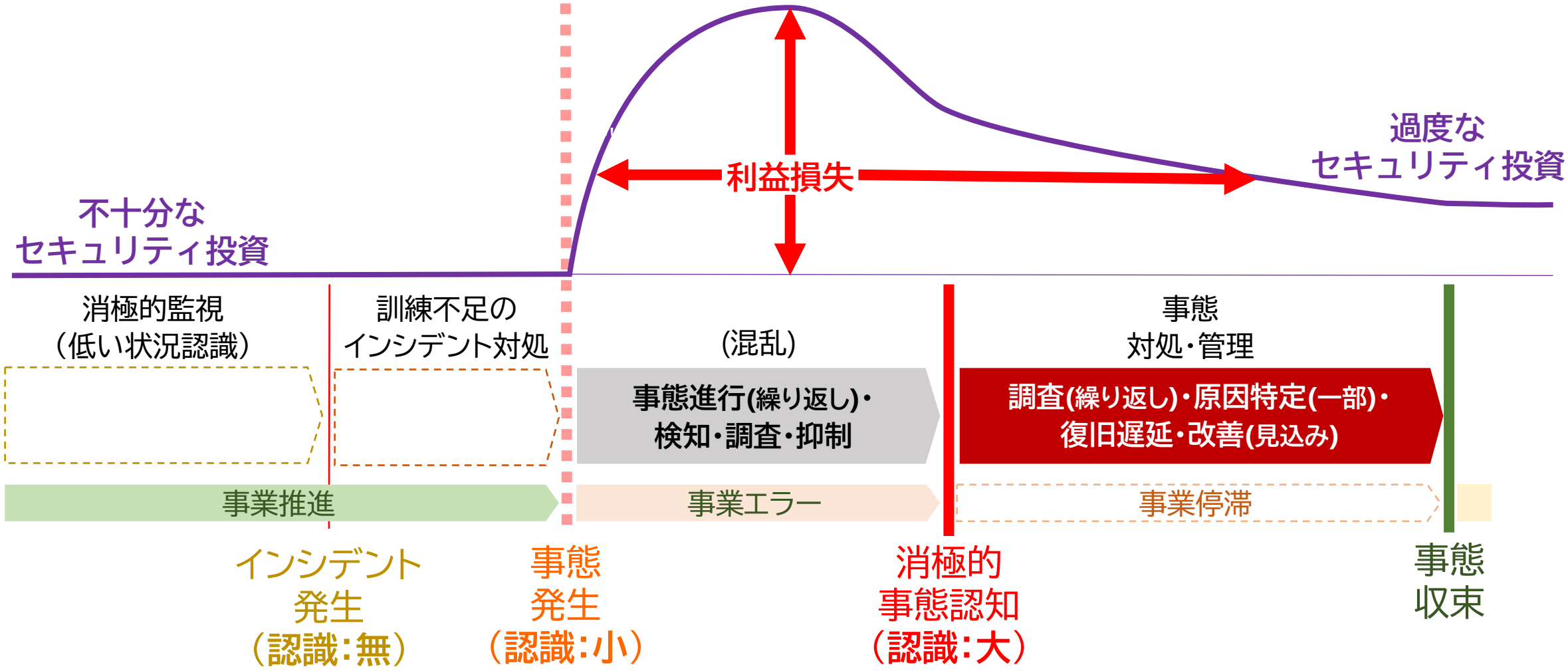
しかし、Twitter Hackの結果は、Twitterや他のソーシャルメディア企業が、サイバーインシデントを経験した後ではなく、**その前に強固なコントロールを導入することが重要**である理由を示しています

Twitter Hack の発生を許したTwitter社の「状況認識不足」

- 持続的な「**強固なリーダーシップ**」と「**シニアレベルの関与**」の重要性
  - CISOの採用や設置は、一つの手段にしか過ぎない。実務能力や行動力がないCISOはいないと同じ
- COVID-19パンデミック時のリモートワーク移行に関連した「**規制当局からのガイダンス**」や「**さまざまなセキュリティ関連組織からのアラート**」の準拠の必要性
  - 特にセキュリティリスクを特定して評価することの重要性に対する認識
- 2020年1月から増大している**ビッシング（Vishing）に対する警戒**の必要性
  - ビッシング（Vishing）とは、連絡先として偽の電話番号を案内して電話をかけさせ、音声応答システム（IVR）を通じて個人情報を窃取しようとすること
- **社員の個人データ**が犯罪者により取得されている可能が高くなっている状況理解
  - ソーシャルメディア等から、社員の自宅の住所、職場または個人の携帯電話番号、勤務先、職場または個人の従業員の名前などの個人データが第三者に取得されやすい

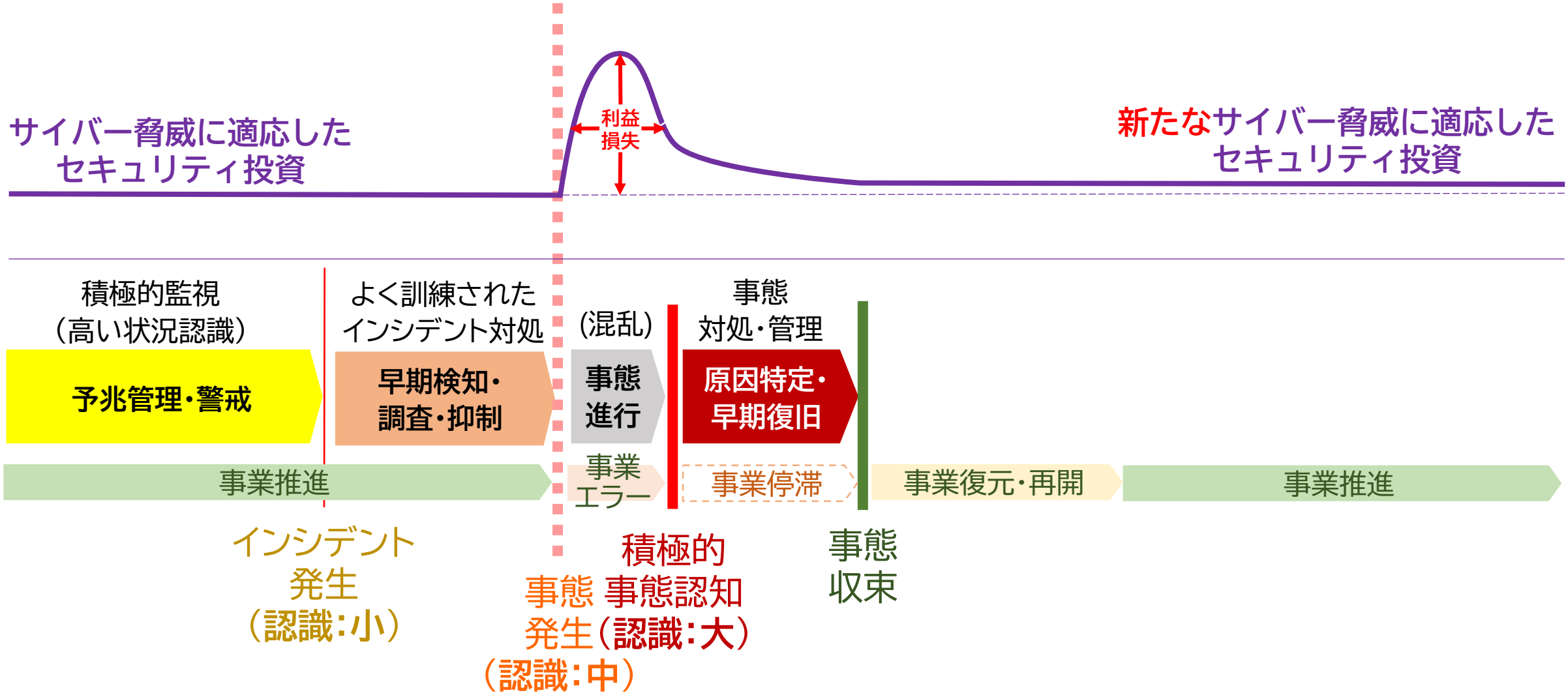
直近のサイバー脅威に適応した**包括的セキュリティコントロールを喪失**していた。

日本型組織が陥る「サイバー攻撃による利益損失」



TLP:GREEN

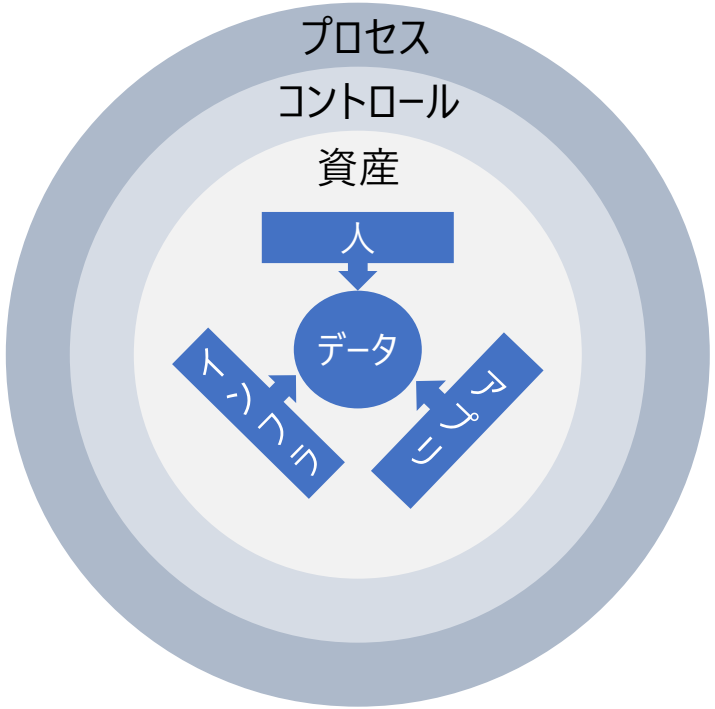
日本型組織が獲得すべき「組織的サイバーレジリエンス能力」



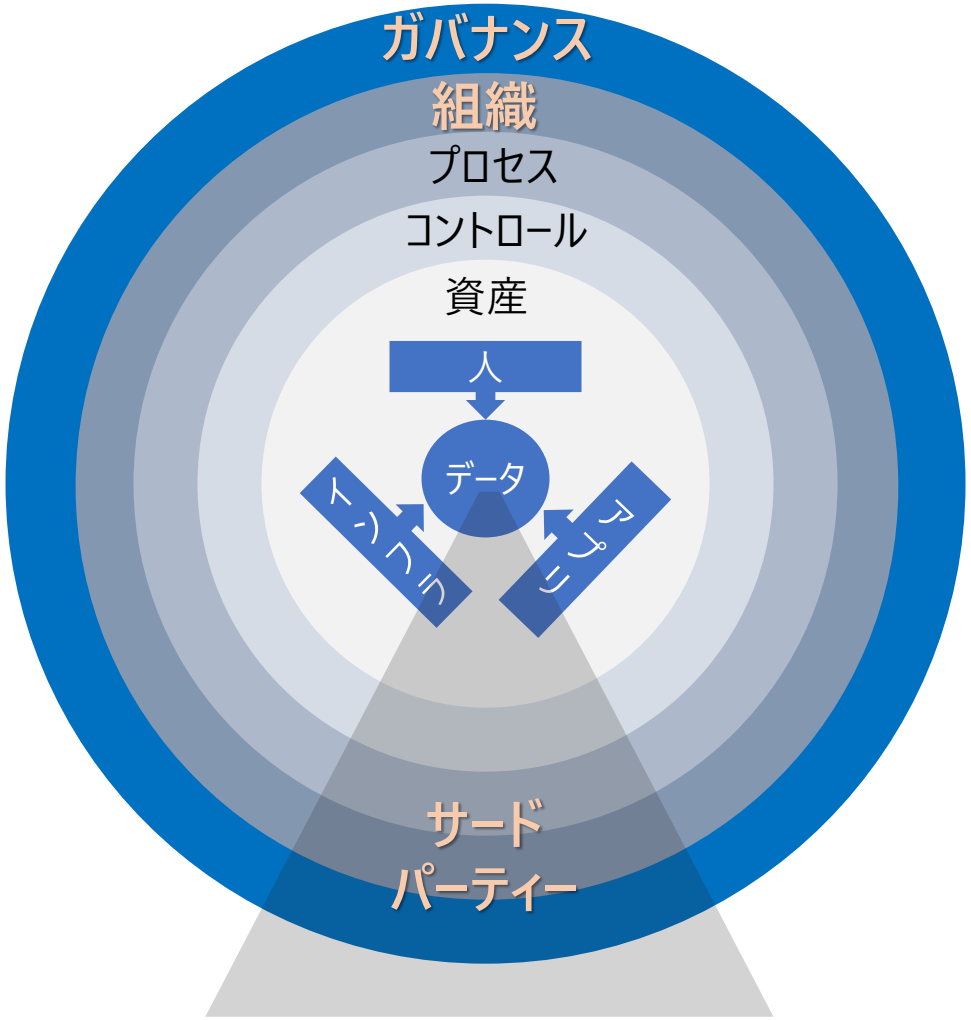
TLP:GREEN

日本型組織が獲得すべき「包括的サイバーリスクマネジメント」

古典的なサイバーセキュリティの焦点



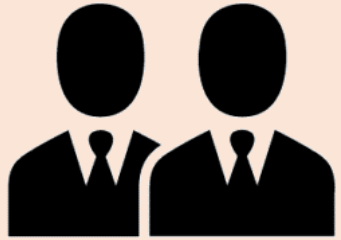
包括的なサイバーリスク・マネジメントのアプローチ



TLP:GREEN

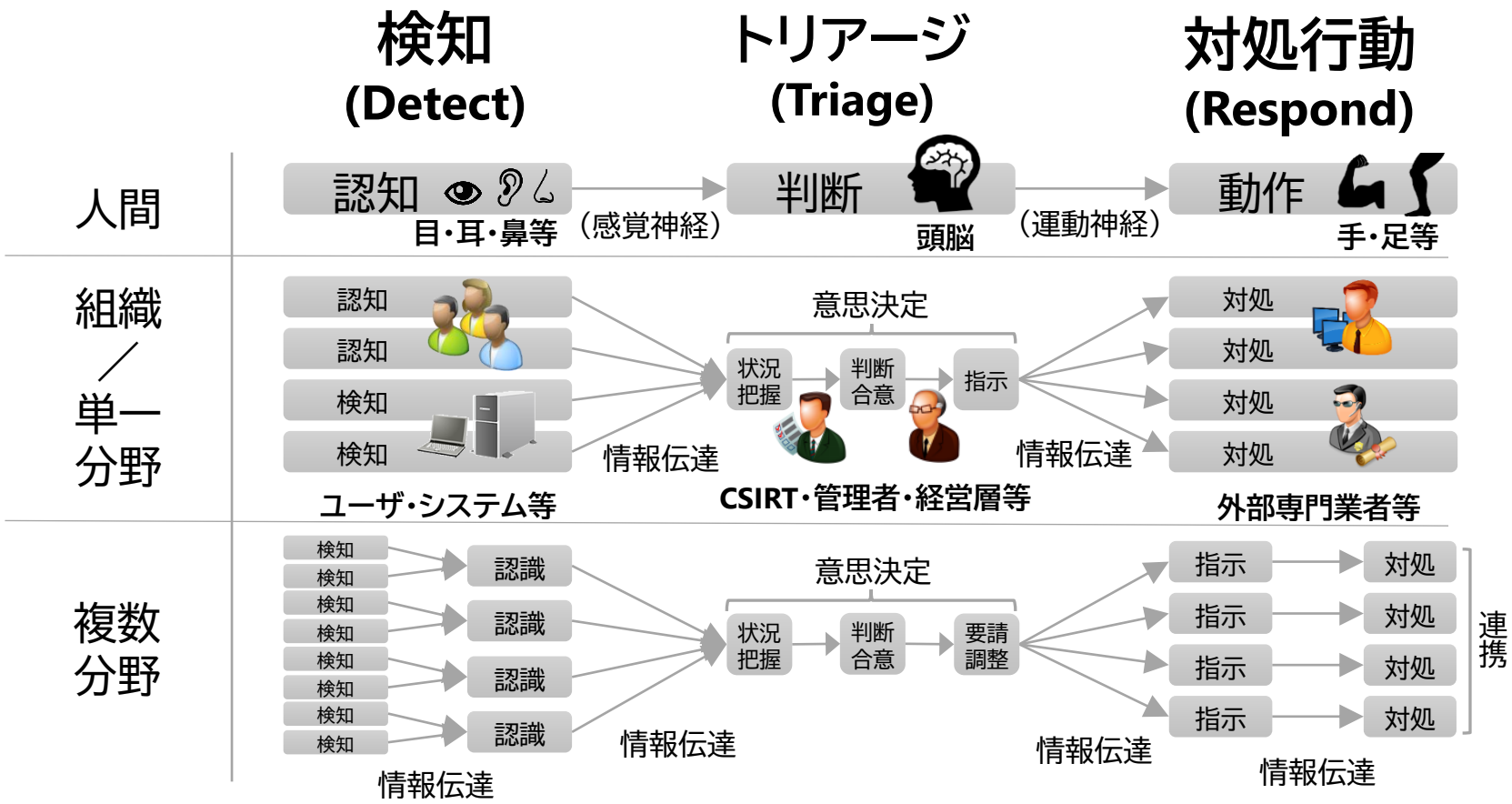
- 包括的
  - 読み方：ほうかつてき
  - 意味：　すべてをひっくるめて一つにまとめているさま
    （部分的ではなく、全ての要素を網羅していること）
  - 反意語：個別的

「ITセキュリティ部門」や「CSIRT」は、会社のすべての要素（施設、部門、社員など）を「ひっくるめて一つにまとめる」ことを可能にする権限と実務能力を有しているか？



他の（多忙な）役職と兼務している「CISO」は、会社のすべての要素（施設、部門、社員など）を「ひっくるめて一つにまとめる」ことを可能にする知識・能力を有しているか？ また、業務品質を保てるリソースを確保できるか？

日本型組織が獲得すべき「組織的対処(レスポンス)能力」



「人間の行動原理(認知⇒判断⇒動作)」をベースにして、「組織／単一分野」及び「複数分野」における
各フェーズ(検知⇒意思決定⇒対処)で実施される行動 を特定した上で、それを実現可能にする
能力スキルや知識体系等を獲得し、**サイバー訓練を積み重ねて**実施可能な状況にしておくこと。

TLP:GREEN

日本型組織の意思決定者が受け入れるべき状況のイメージ

TLP:GREEN

本資料に関する連絡先

名和 利男（NAWA Toshio）

SITE: https://www.nawa.to

PGP: 0xE38B4E01