



企業利益を損なう結果を招く サイバー脅威

2021年 11月
名和 利男

本講演における問題意識

国内で目立っているサイバーセキュリティ対策の焦点は、

- 内閣府・個人情報保護委員会による「個人情報」、
- 経済産業省による「知的財産」、
- 内閣官房・NISCによる「重要インフラサービス」、
- 所管省庁による「法規制、ガイドライン(手引き)、標準等」

となっており、**これらは行政機関の所掌事務に基づいたもの**と言えます。

ところが、なぜか**企業目線のものが少ない**印象です。

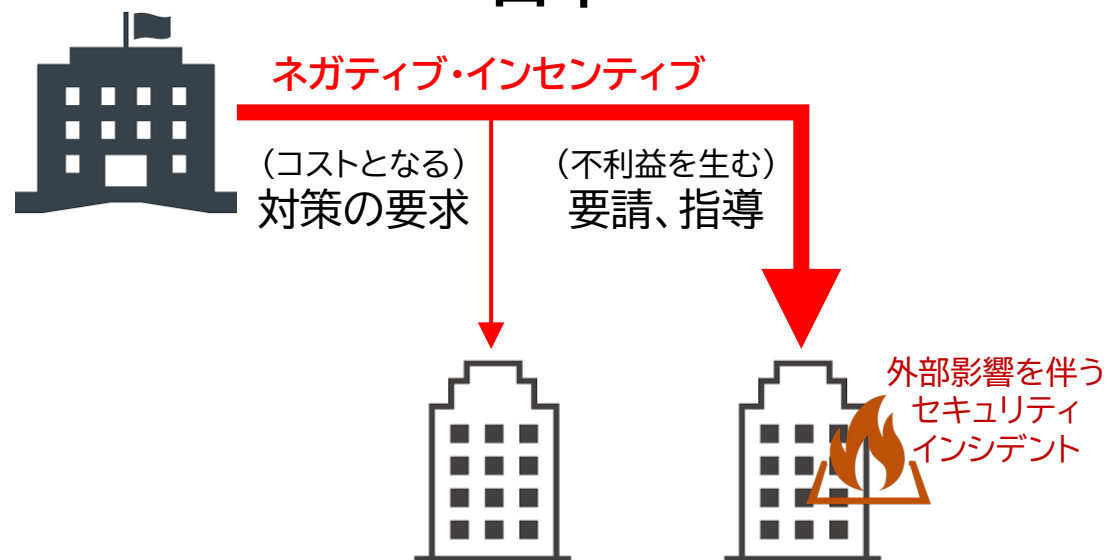
これらは、**コンプライアンス**（企業の外側にある規則等に従うこと）の領域である。

ところが、（規則等を制定する）行政機関は、サイバーセキュリティの**状況認識と知識・経験が非常に低い**。

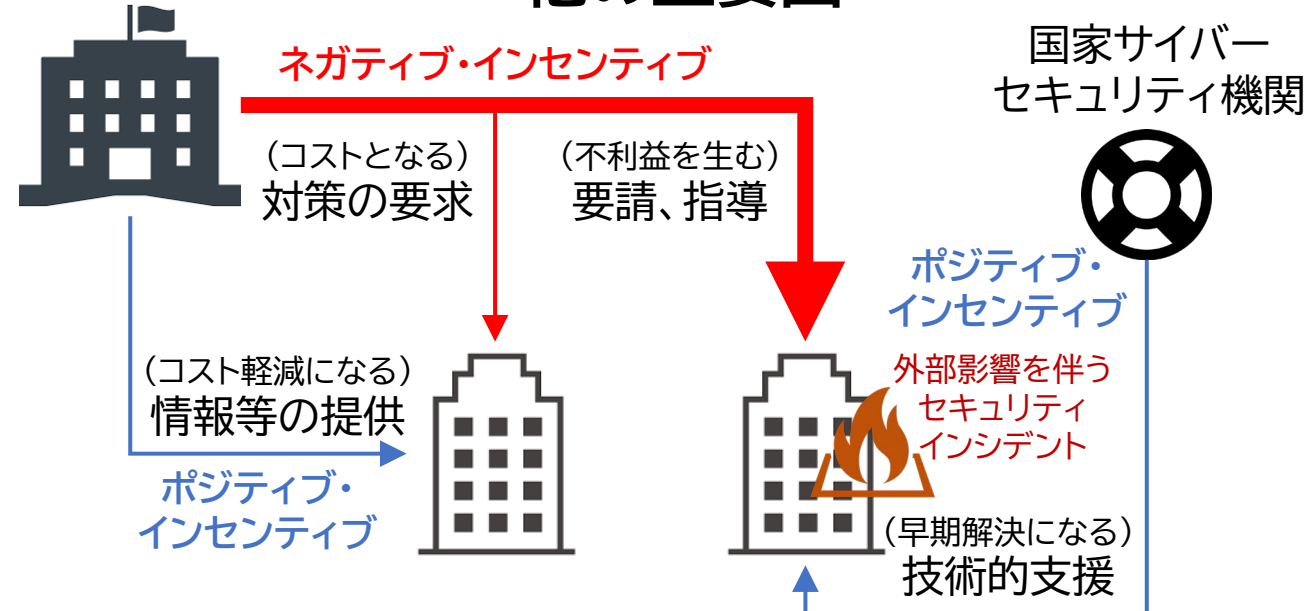
したがって、これらの対策焦点に基づいた対策は、**現実のサイバー脅威に適応したものではない**。

本講演における問題意識

日本



他の主要国



企業は「営利を目的に事業を行う経済主体」であるため、現実論としてのサイバーセキュリティ対策の焦点は、「企業利益」であるはずです。

これを踏まえ、企業経営者に把握していただきたい「**企業利益**」を守るための対策について、支援活動で得られた知見と考察を共有いたします。

アジェンダ

1. 日本型組織の特性とサイバーセキュリティの現状
2. 日本型組織が獲得すべきこと
3. 意思決定層に対するサイバー脅威の説明(あり方)
4. 意思決定層に対するサイバー脅威の説明(ポイント)
5. まとめ

トピック 1

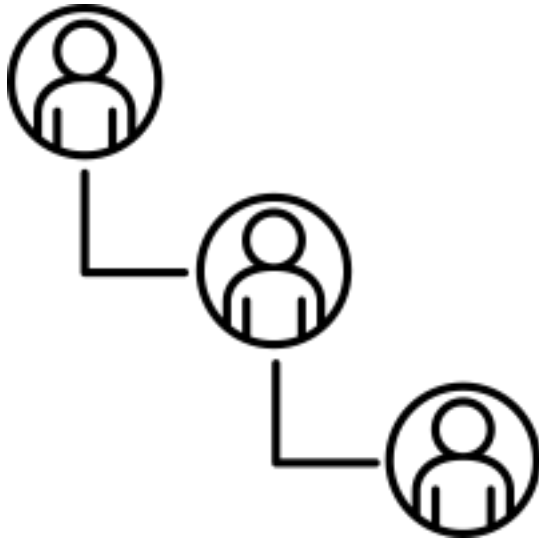
日本型組織の特性とサイバーセキュリティの現状

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。

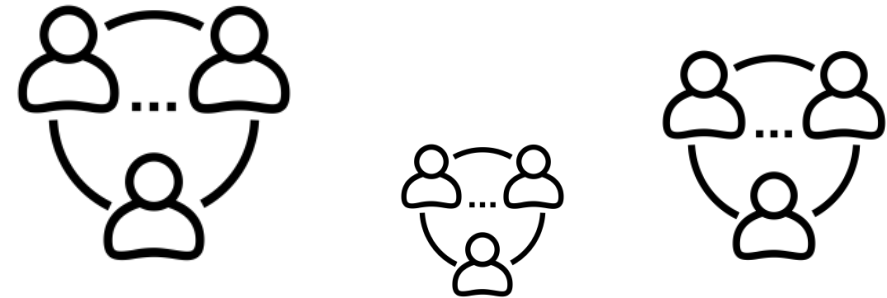
表面的な組織構造

- 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。

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



2020年 Twitter社へのサイバー侵害の発生を許した「状況認識不足」

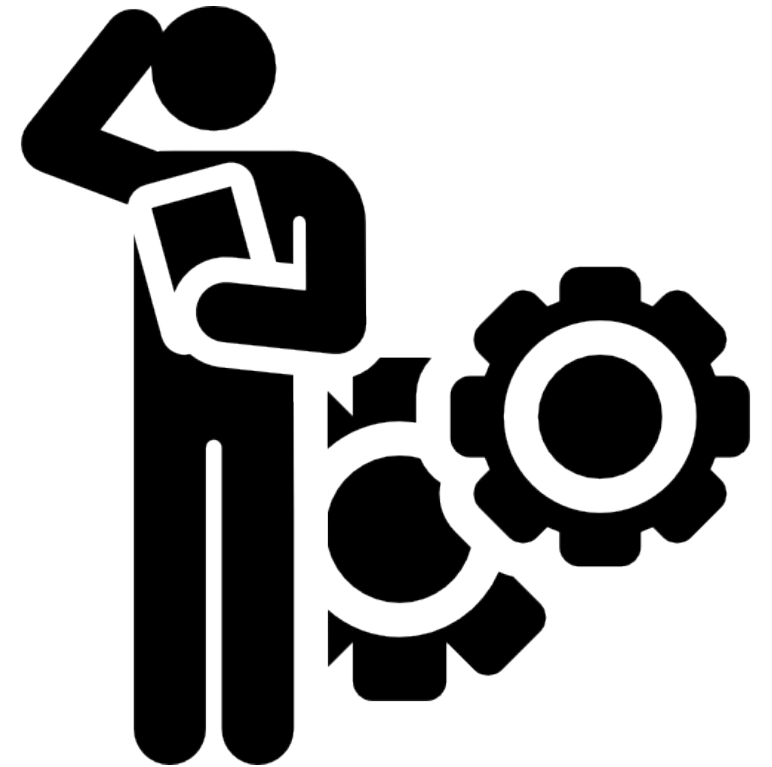
- 持続的な「**強固なリーダーシップ**」と「**シニアレベルの関与**」の重要性
 - CISOの採用や設置は、一つの手段にしか過ぎない。実務能力や行動力がないCISOはいないと同じ
- COVID-19パンデミック時のリモートワーク移行に関連した「**規制当局からのガイダンス**」や「**さまざまなセキュリティ関連組織からのアラート**」の準拠の必要性
 - 特にセキュリティリスクを特定して評価することの重要性に対する認識
- 2020年1月から増大している**ビッシング(Vishing)**に対する警戒の必要性
 - ビッシング(Vishing)とは、連絡先として偽の電話番号を案内して電話をかけさせ、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事
- **社員の個人データ**が犯罪者により取得されている可能性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。

日本型組織の不適切な行動様式 – 安直な手段を選択 (1/3)

- セキュリティ問題を**ITで解決**しようとする。
 - 多くの経営層は、サイバーリスクを技術的な問題として扱い、それをIT部門に任せる。
 - サイバーセキュリティには多くの技術的問題があることを考えると、これは自然な対応であるが、ビジネスを防御することと、システムを保護することとは異なる。
 - ビジネスを守るには、ビジネスの優先事項から導き出されるリスク感覚が必要である。
 - ビジネスモデルとバリューチェーン、会社のリスク文化、役割、責任、そしてガバナンスが求められるため、ITだけではサイバーセキュリティに取り組むことはできない。



日本型組織の不適切な行動様式 – 安直な手段を選択 (2/3)

- 問題解決のために**(単に)人材を投入**しようとする
 - ある企業は、知名度の高いハッカーを入社させれば、脅威は消え去ると思い込む。
 - 最高レベルのハッカーであっても、複雑なネットワーク内の何百万ものデバイスに対して、何万もの攻撃を予期し、防御することは不可能である。

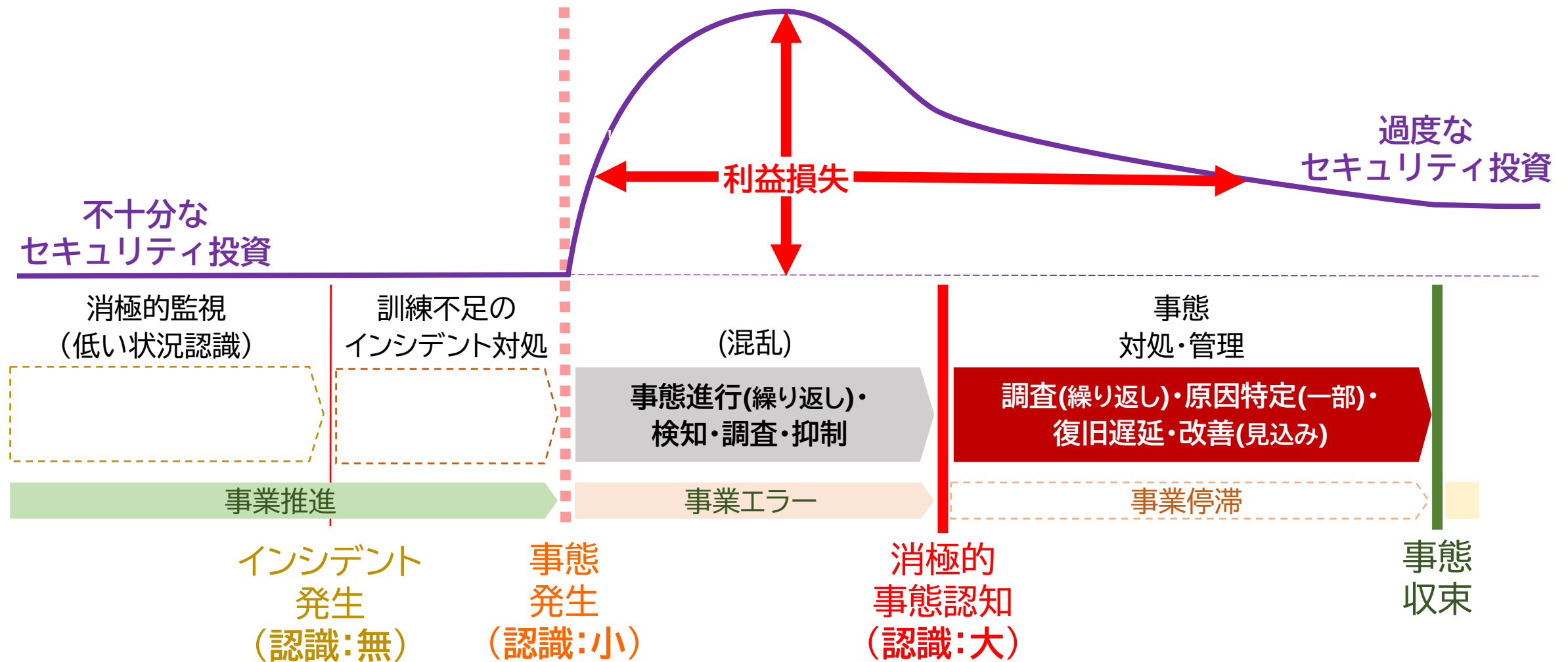


日本型組織の不適切な行動様式 – 安直な手段を選択 (2/3)

- 問題を**コンプライアンスで解決**しようとする。
 - 一部の企業は、一日おきに新しいサイバーセキュリティに係るプロトコルとチェックリストを導入しているが、これらの取り組みは、本当の回復力ではなくコンプライアンスに過度の焦点を当てたものである。
 - CISOのチェックリストにおいて、全てのボックスがチェックされていても、以前よりもサイバー攻撃に対して脆弱となっている可能性がある。



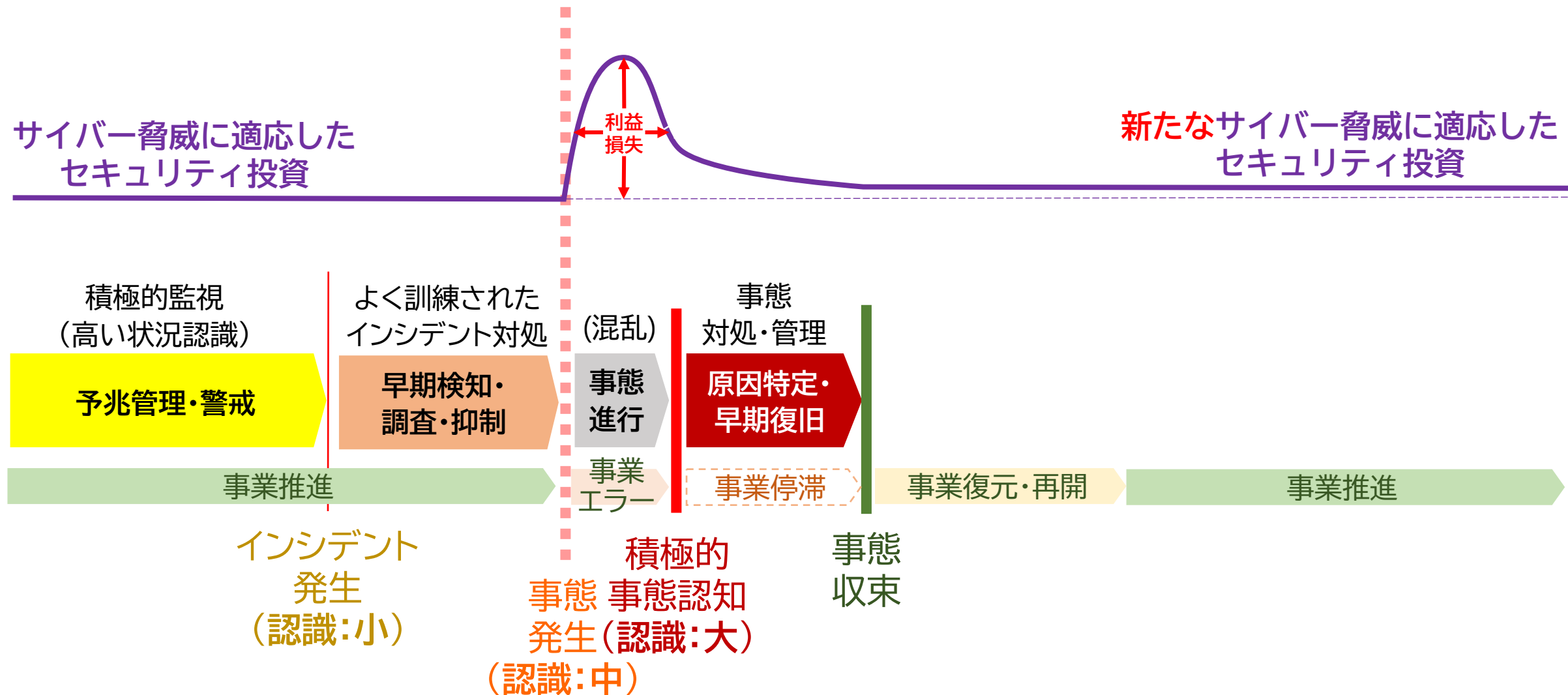
日本型組織が陥る「サイバー攻撃による利益損失」



トピック 2

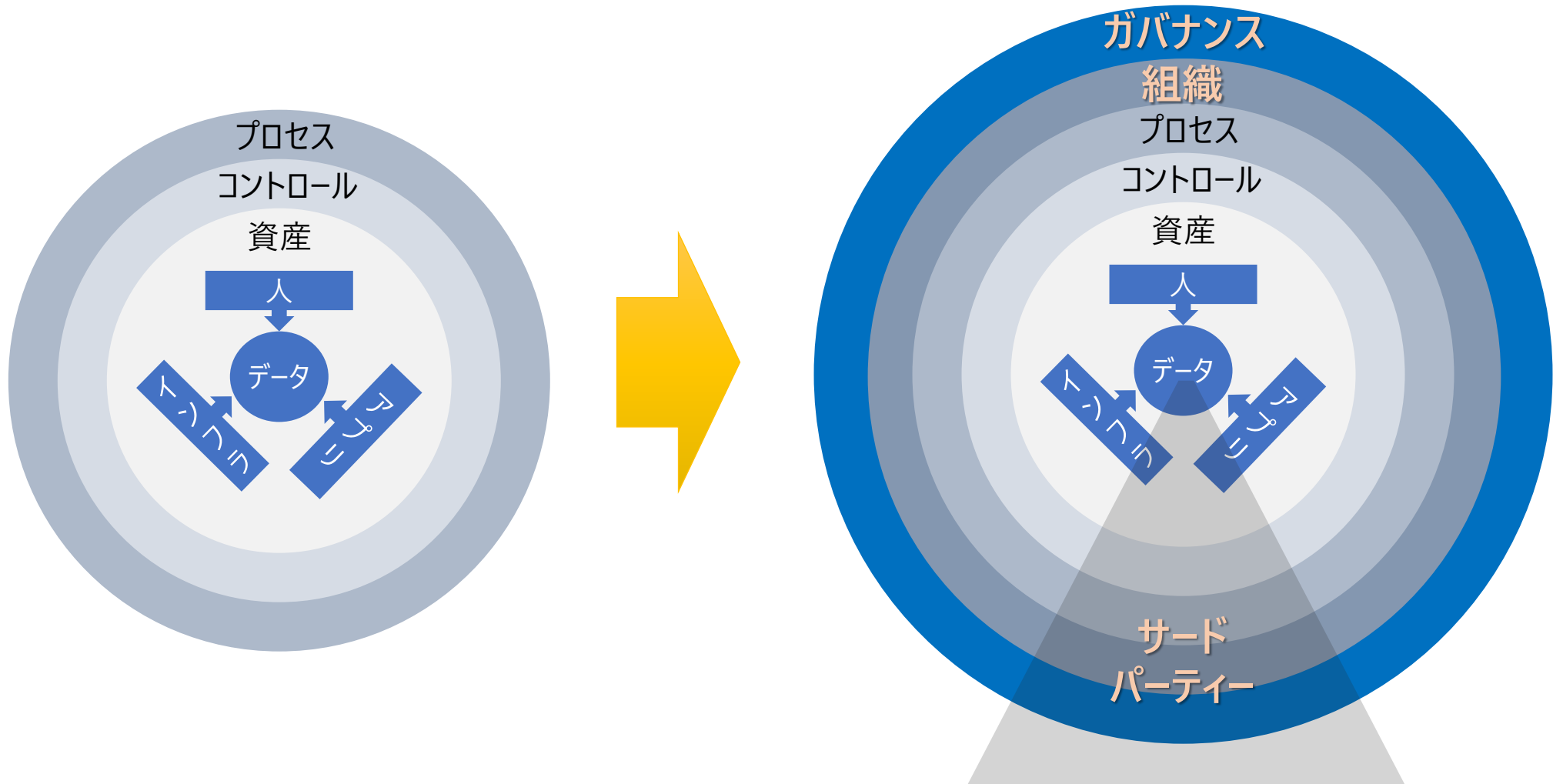
日本型組織が獲得すべきこと

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」



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

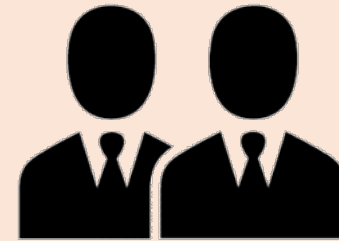


• 包括的

- 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

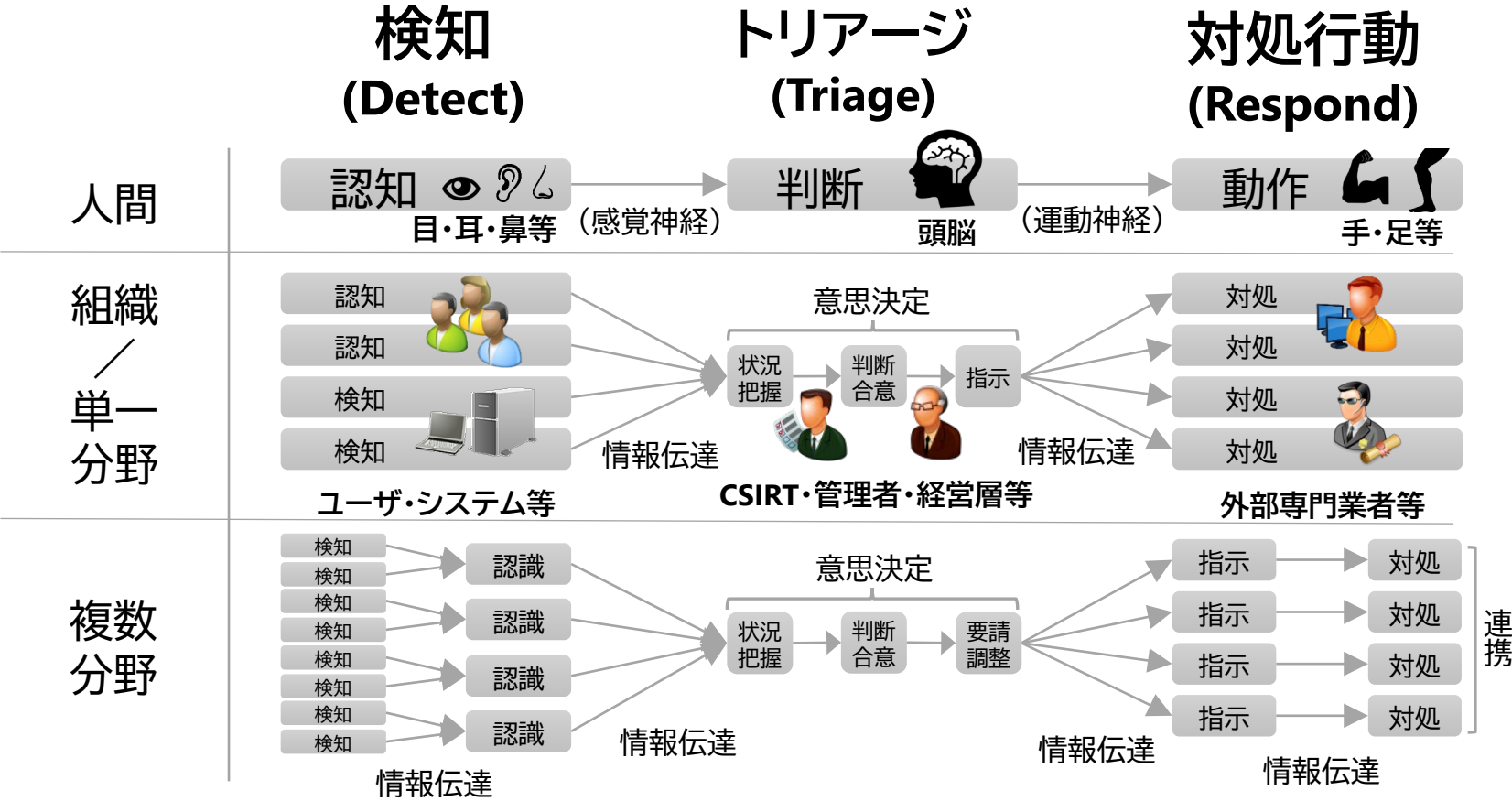


「ITセキュリティ部門」や「CSIRT」は、会社のすべての要素（施設、部門、社員など）を「ひっくるめて一つにまとめる」ことを可能にする**権限と実務能力を有しているか？**



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。

トピック 3

意思決定層に対するサイバー脅威の説明(あり方)

意思決定層に対するサイバー脅威の説明：現状と問題

- 現状：意思決定層は、ビジネスに影響が及ぶ潜在的なサイバー脅威によるリスクを把握したい
 - サイバー環境の持続的な変化により、サイバー空間の利用が経済・社会活動の重要な基盤として定着したため、さまざまな組織のビジネスやオペレーション(運用)を始めとしたさまざまな業務がサイバー脅威に晒されるようになってきた。
 - したがって、組織の意思決定層(上級幹部や役員)は、重要なサイバーセキュリティの懸念、ビジネスへの影響、考えられる軽減策を理解及び優先順位を確立した上で、必要なリソース(予算・人)を割り当てなければならない。
 - そのため、意思決定者(上級幹部や役員)は、役員会議にサイバーセキュリティ責任者や外部専門家を招聘するなどして、サイバーセキュリティのリスクを深く理解し、潜在的な問題を先取りするあらゆることをしたいと考える。
- 問題：意思決定層は、すでにIT領域のセキュリティ運用に偏重した説明を多く受けている
 - しかし、実際の意思決定層に対するサイバー脅威の説明は、ITに係るセキュリティ運用に限られ、意思決定者(上級幹部や役員)の関心事項から外れた技術的事項や関連性の薄いデータポイント(情報の個別単位)に焦点を当てたものになりがちである。

意思決定層に対するサイバー脅威の説明: WHO(説明者)

- 意思決定層が最も重視している**ビジネス上の問題や事業計画を理解**すること。
 - 例えば、特定のビジネス活動、合併・買収、パートナーシップ、または現在進行中の最優先課題が挙げられる。
- 上級幹部や役員の**性格、典型的な質問、知ろうとしていること、獲得した情報をどのように使おうとしているか等を把握**すること。
 - 上級幹部や役員を惹きつけて、理解を容易にして、ニーズを満たすことが期待できる。



意思決定層に対するサイバー脅威の説明: **WHEN**(時期)

- 報道などから伝えられるサイバー脅威動向から、**自組織に特定のリスクの発生が予見された時点**で実施する。
 - どのようなリスクシナリオが優先されるか否かに関する情報に基づいた意思決定を行うために必要なデータを提供する必要がある。
 - ただし、完全な防護策は存在せず、残存リスクを受け入れる必要があり、許容可能なリスクであるか否かを示す必要がある。
- 規制当局などから示される**指針やガイドラインに準拠する必要が発生した場合**に実施する。
 - 指針やガイドラインへの準拠に係る課題などに応えることができる情報を収集する必要がある。



意思決定層に対するサイバー脅威の説明: **WHERE**(環境)

- 意思決定層がリラックスできる環境で、**周辺に認知バイアスを誘発する情報がないこと。**
 - 認知バイアスとは、自分にとって都合のいい情報だけを集めて思い込み強化してしまう心理的作用のこと。
 - 意思決定者が、説明者に対して質問やコメントをしやすい雰囲気を作り出しておくことが望ましい。
- **意思決定層の発言内容の保秘を確保する**ことが可能な仕組みを整えておくこと。
 - 意思決定者のとっさの発言の中には、ビジネスや組織管理における重要事項を示唆する情報が含まれていることがある。
 - 組織外に漏れることで不利益が発生することがある。



意思決定層に対するサイバー脅威の説明: WHAT(内容)

- 他所でよく見られる懸念事や質問とその回答を提示した上で、**既存のソリューションがどのように対処しているか、または回避・軽減されていない場合にどのように対処する必要があるのか**を提示する。
- **戦術的**(一定の目標を達成するための取られる手段が組み込まれていること)な文脈にし、**厳格かつ明確な構成**にすること。
 - 関連性がなく、提示する理由が特にならない情報は入れ込まない。
- **技術的詳細を抽象化**し、ビジネス、オペレーション(業務/運用)、法的影響に焦点を当てた分かりやすい概念を伝えるべき文脈に集中させる。
 - 技術に関する踏み込んだ話やテクノバブル(技術者の難解な専門用語)を排除すること。
 - 意思決定層(上級幹部や役員)は、普段からサイバー脅威に関する情報に触れていないことに留意すること。
 - 意思決定者が容易に理解できる用語を使用する。
- いたずらに**恐怖、不確実性、疑念を使って圧力をかけない**こと。



意思決定層に対するサイバー脅威の説明: WHY(目的・理由)

- 意思決定者が、サイバーセキュリティのリスクを深く理解し、**潜在的な問題を先取りするあらゆることを行うために必要な知識や観点を提供**するため。
 - 日本の企業経営者の大半は、「潜在的なセキュリティ問題の先取り」より、「セキュリティ問題を解決するための対策やソリューション」に強い関心を持っている。
- 意思決定層みずからが、サイバーセキュリティに対して全面的に関与することで、**組織のセキュリティ統治を強化**につなげるため。
- 意思決定層がサイバーセキュリティに関する強いメッセージを発信することで、**従業員に対するサイバーセキュリティポリシーの順守を向上**させるため。
 - 一部の組織では、従業員がサイバーセキュリティポリシーに順守していることをパフォーマンスレビューの一部とみなしている。



意思決定層に対するサイバー脅威の説明: HOW(方法)

- 意思決定層にプレゼンテーションを実施する前に、**意思決定層の関心事や課題などについて質問**する。
 - これにより、意思決定層を理解し、プレゼンテーションの目的や彼らの意思決定に必要な説明内容(文脈)にすることができる。
- 簡潔な事例を使用して、その**ストーリーラインの重要要素の中に伝えるべきことを入れ込む**。
 - 類推による説明、簡略化されたグラフやダッシュボードが役に立つ。
- 潜在的な理論上の脅威ではなく、**組織に影響を与える実際のリスクについて議論**する。
 - 合理的であり、誇張は避けること。
 - サイバーリスクの軽減策の決定の経緯や背景を提供すること。



トピック 4

意思決定層に対するサイバー脅威の説明(ポイント)

ポイント1:「サイバー攻撃」より認識しやすい「脅威アクター」を説明

ITに詳しくない方は、脅威アクターを「ハッカー」や「攻撃者」と表現しても、危機感を抱きにくいため、実世界において「害を与える主体」を表す象徴的な用語を利用する。

サイバー脅威をもたらす「ならず者」- 主な種類



国家の支援を受ける
「サイバー攻撃グループ」



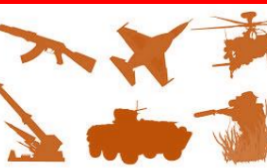
さまざまな形態を持つ
「サイバー犯罪グループ」



個人レベルの
「悪意のあるハッカー」

それぞれの脅威アクターの特性を象徴するイメージを利用することで、識別しやすくなり、印象(記憶)に残しやすくする。

ポイント2:「脅威レベル」を実感しやすくなるよう表現を工夫

サイバー脅威をもたらす「ならず者」- 能力特性		
国家の支援を受ける 「サイバー攻撃グループ」 		動機: 諜報活動、政治的、経済的、または軍事 所属: 国民国家または国民国家と関係のある組織 戦術、技術、手順(TTP): スピアフィッシングパスワード攻撃、ソーシャルエンジニアリング、直接侵害、データ漏洩、リモートアクセス型トロイの木馬、破壊的なマルウェア
さまざまな形態を持つ 「サイバー犯罪グループ」 		動機: 金銭的利益または評判の向上 所属: 個人または協力者と連携 戦術、技術、手順(TTP): フィッシング、ソーシャルエンジニアリング、ビジネスメール侵害(BEC)詐欺、ボットネット、パスワード攻撃、エクスプロイトキット、マルウェア、ランサムウェア
個人レベルの 「悪意のあるハッカー」 		動機: 個人的な怨恨、嫉妬、自己顕示欲、愉快犯、模倣犯、技量挑戦、偏重した正義感 所属: (なし。一部は緩やかなコミュニティ) 戦術、技術、手順(TTP): (多種多様な種類で常に変動する。多くは公表済み脆弱性の悪用や流通している攻撃ツールを使用。)

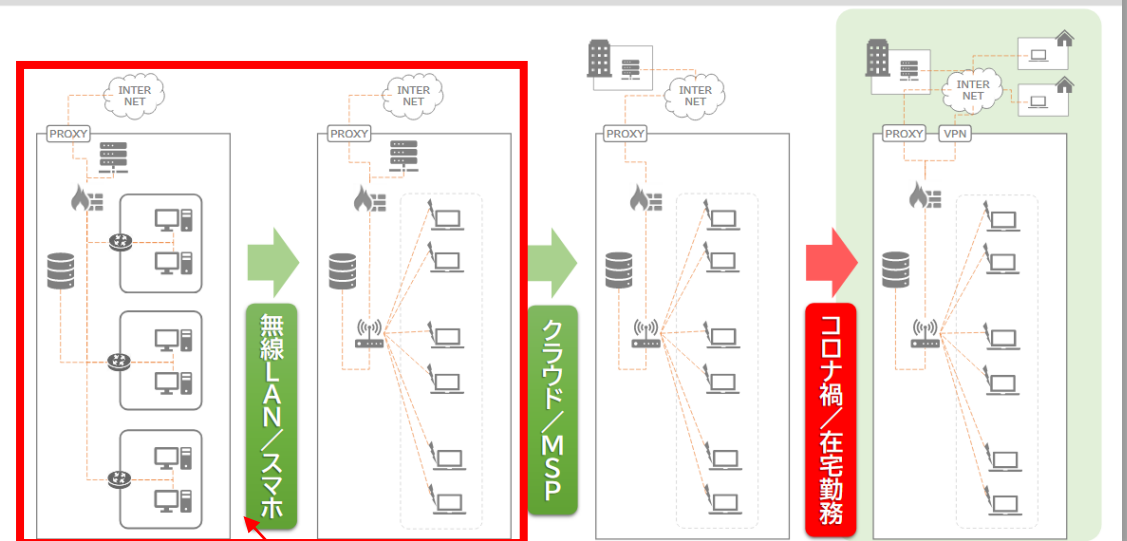
それぞれの脅威アクターが持つ攻撃能力の説明は、一見して理解することができるアイコンを併用すると、(ITリテラシーにばらつきのある)意思決定者全体に同レベルの理解を与えることが期待できる。

脅威アクターとその影響力について、「文字」のみで表してしまうと、意思決定者において腑に落ちるまでの時間に大きな差が発生する。
短時間による説明を求められる意思決定者に対しては、直前の説明とつながりやストーリー性を持った流れで表現することが望ましい。

サイバー脅威をもたらす「ならず者」- 影響力	
 国家の支援を受ける 「サイバー攻撃グループ」	 さまざまな形態を持つ 「サイバー犯罪グループ」   個人レベルの 「悪意のあるハッカー」

ポイント3: 「状況の変化」を文脈とイメージなどで印象を強調

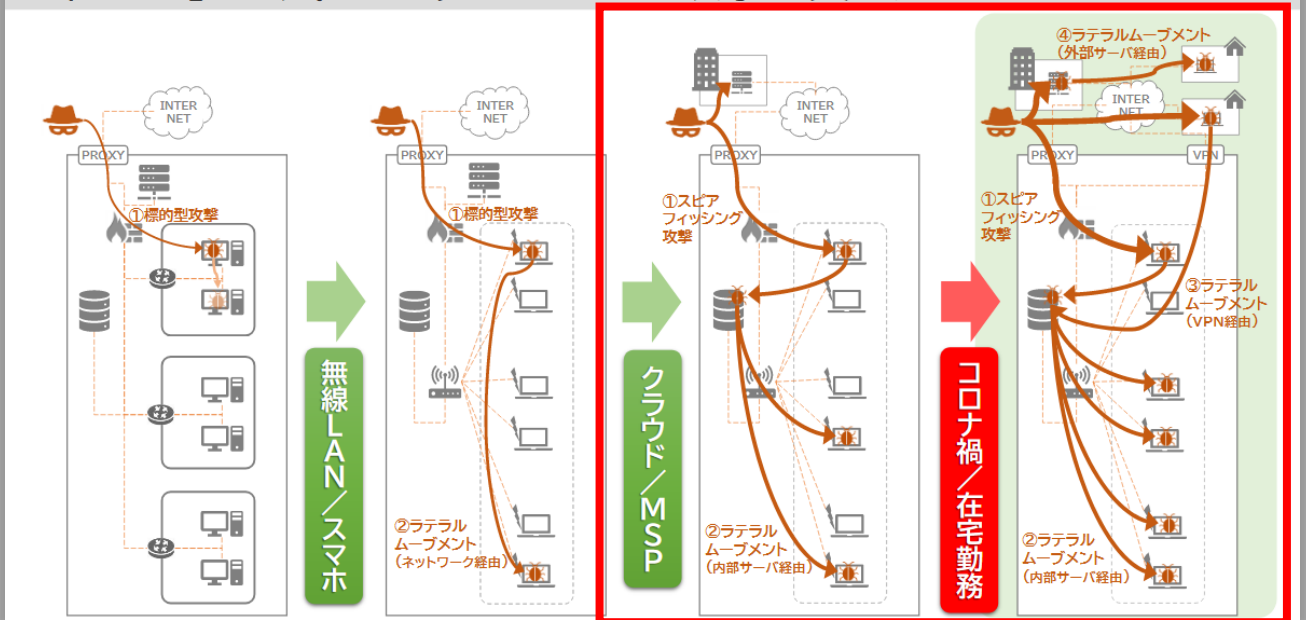
「私たち」は、より便利により安くを追求している



自社が利便性向上のためIT(情報技術)やインターネットの利用を積み上げるたびに、構造的なセキュリティを失ってきている状況について、象徴的なアイコンおよび時系列的に表現することで、意思決定層が理解すべきリスク増大の要因を視覚的に得ることができる。

攻撃対象領域(Attack Surface)の増大を示すためには、文脈(コンテキスト)やストーリーで説明することが最善である。さらに、一気に増大している状況について、イメージを煩雑(ビジー)にすることで与える印象が強くなる。

「私たち」は、気づかずにサイバー攻撃を受け入れている

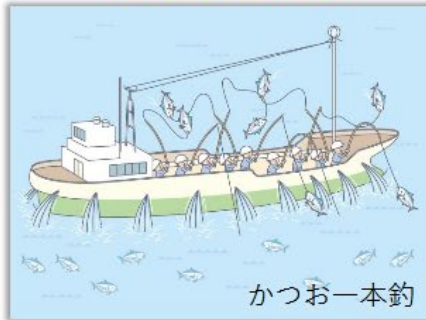


ポイント4:「難しい状況理解」は、内容ではなく感覚として提供

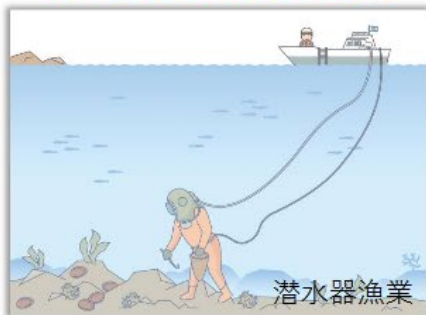
意思決定層にとって、サイバー攻撃に係るTTP(戦術、技術、手順)の理解は困難である場合があるため、担当者が「感覚として抱いている変化」を、意思決定層も容易に抱くことができるイメージを持って提供する。

最近のサイバーセキュリティを**突破する攻撃**

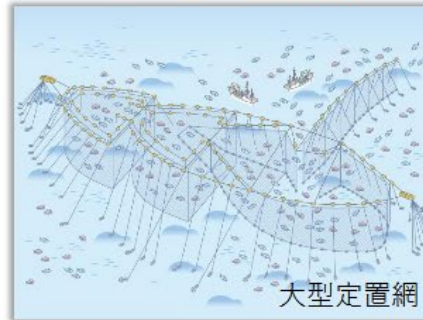
フィッシング詐欺
(標的型メール攻撃)



スピアフィッシング攻撃



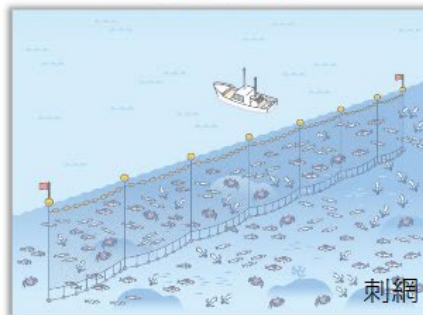
エクスプロイト攻撃



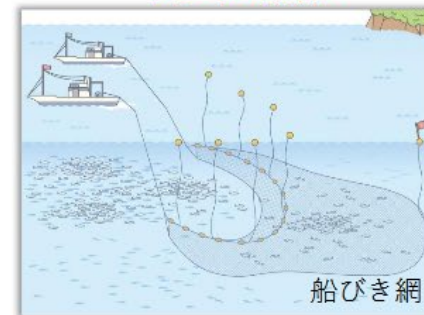
水飲み場攻撃



中間者攻撃

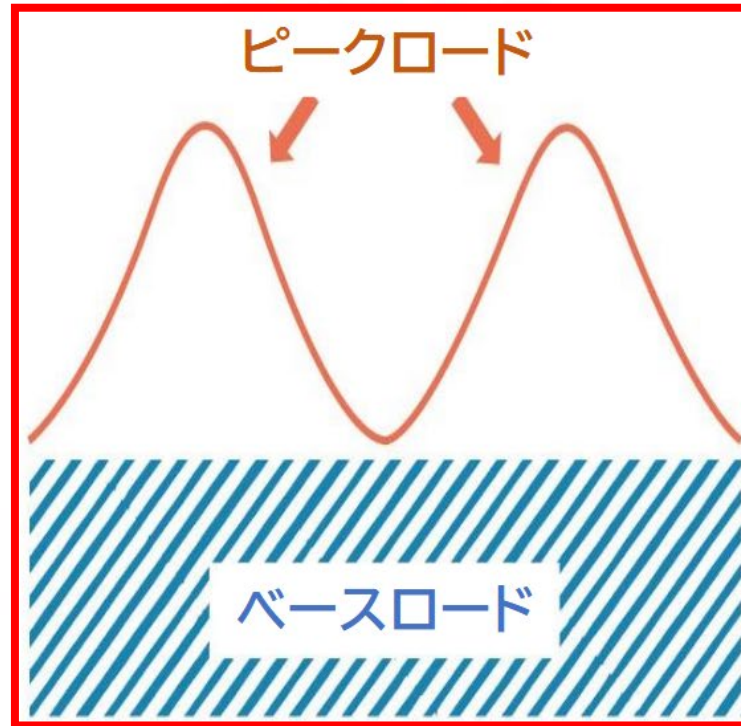


ランサム攻撃



ポイント5: 合意形成に要する時間を短くする判断根拠の表現を工夫

サイバー攻撃における「ベースロード」と「ピークロード」



機械設備のPCに対する不正プログラムの混入

敵対国のソフトウェアやサービスから流出

正規サービスの同期機能を利用するC2通信

偽Wi-Fiアクセスポイントによる中間者攻撃

正規サービスを踏み台にするC2通信

調達・窃取した認証情報の悪用

正規の更新機能を利用するマルウェア感染

スクリプト実行環境を利用した不正挙動

意思決定層に、技術的なセキュリティ対策の優先度を判断いただくためには、その判断根拠となる発生頻度や影響を身近で感じるたとえで区分けして示すことで、短い時間で合意形成に到達していただくことが期待できる。

トピック 5

まとめ

まとめ – 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



本資料に関する連絡先

名和 利男 (NAWA Toshio)

SITE: <https://www.nawa.to>

PGP: 0xE38B4E01

