



中小企業(中堅企業の外部拠点を含む)が DX推進において認識すべき サイバーリスクと対策の重点事項

2021年 6月
名和 利男

アジェンダ

1. 敵(サイバー攻撃を仕掛ける者たち)を知ろう
2. 己(私たちの状況)を知ろう
3. (DX推進する中小企業が認識すべき)サイバーリスクを誘発する要因
4. (DX推進する中小企業が検討すべき)セキュリティ対策の重点事項
5. まとめ

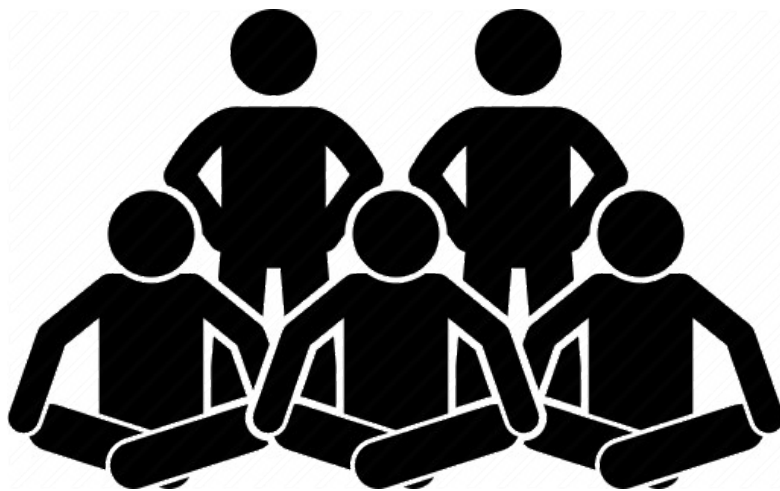
トピック 1

敵(サイバー攻撃を仕掛ける者たち)を知ろう

主なサイバー脅威主体の種別



国家の支援を受ける
「サイバー攻撃グループ」

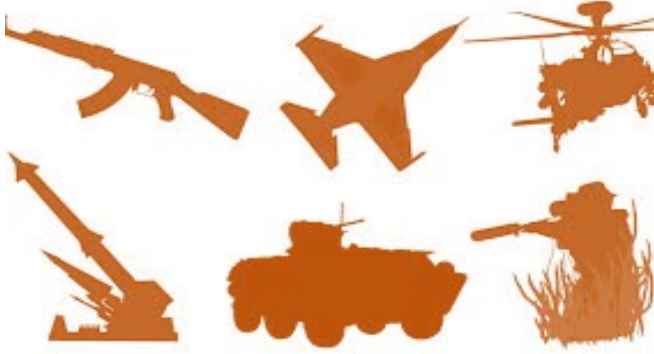
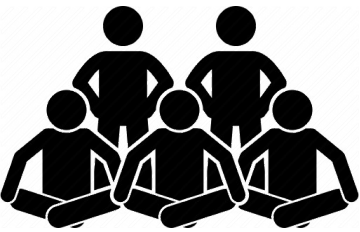


さまざまな形態を持つ
「サイバー犯罪グループ」



個人レベルの
「悪意のあるハッカー」

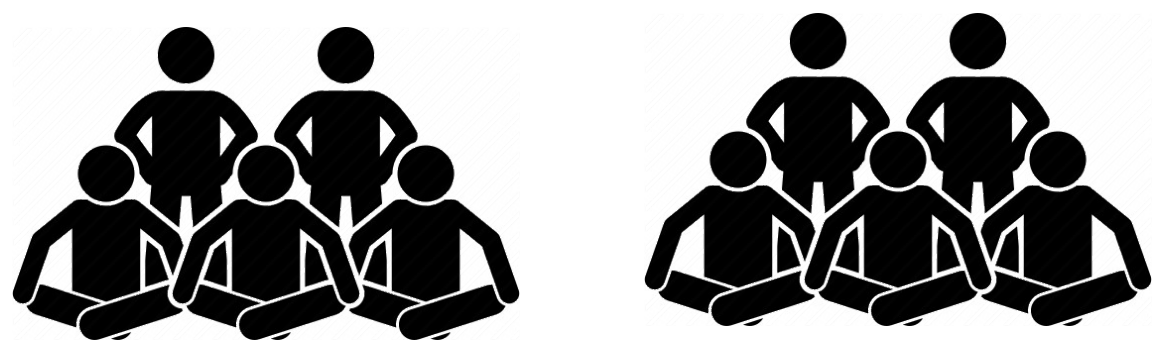
主なサイバー脅威主体の能力特性

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。)

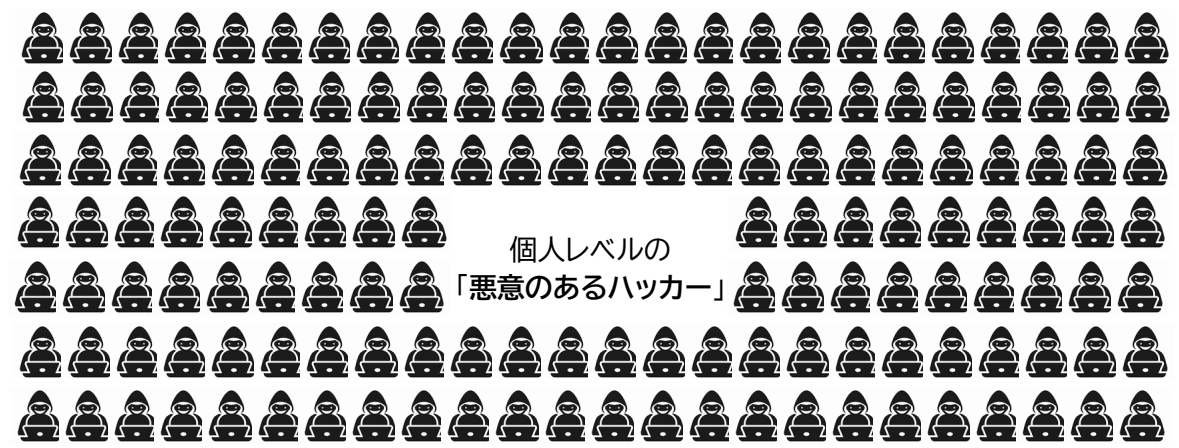
主なサイバー脅威主体の影響力



国家の支援を受ける
「サイバー攻撃グループ」

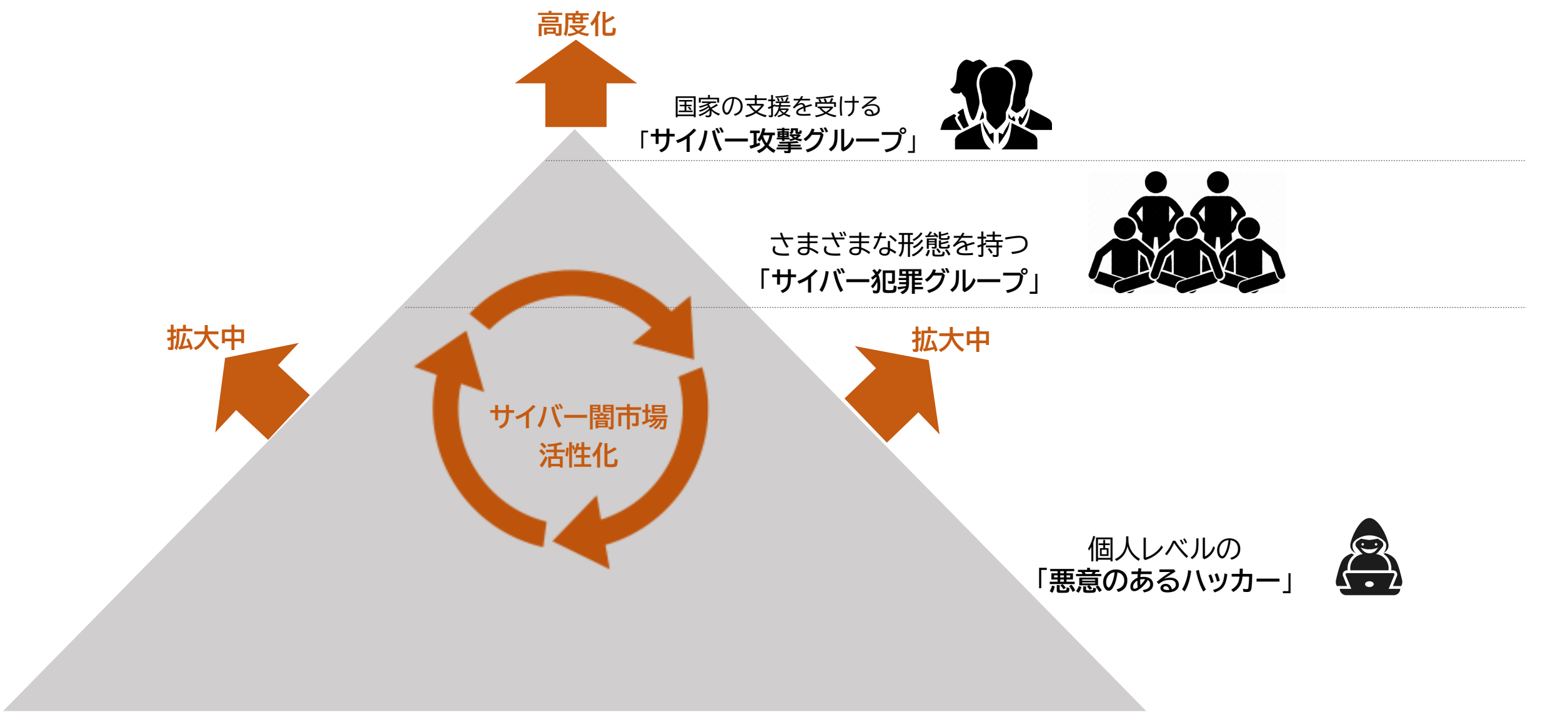


さまざまな形態を持つ
「サイバー犯罪グループ」

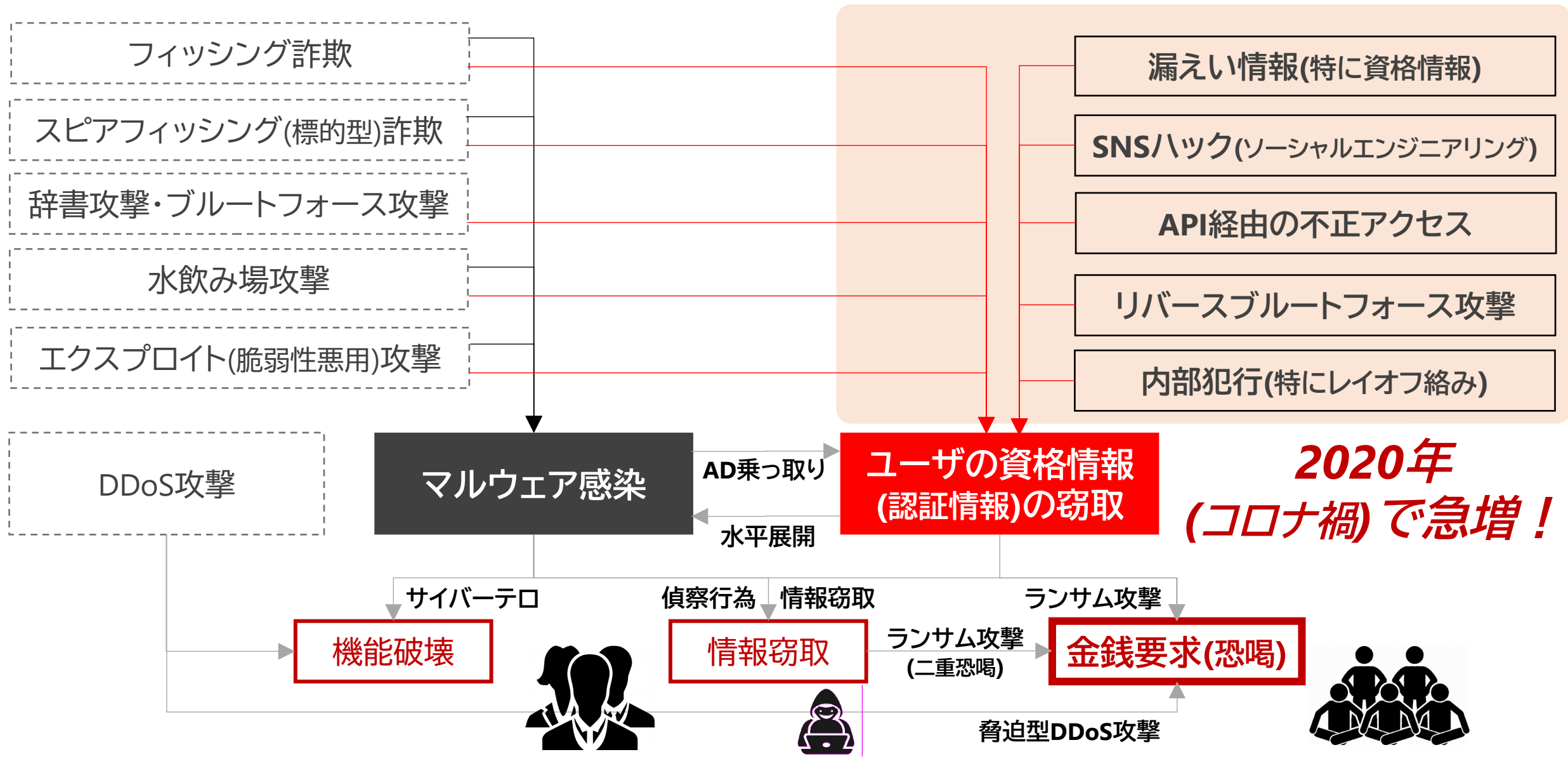


個人レベルの
「悪意のあるハッカー」

主なサイバー脅威主体の人口比



サイバー脅威主体の手法拡大と標的変化



ランサムウェア攻撃を仕掛ける脅威主体の進展

- ここ数年におけるランサムウェア攻撃グループに対する観察で得られた状況に対して、**「ランサム攻撃を仕掛ける者たち」を人間の行動として分析**すると、次のような実態を垣間見る。

「ランサム攻撃を仕掛ける者たち」の急増による**攻撃成功率低下への改善**
／(底なしの)金銭欲を満たすため競争や(自然発生的な)連携強化
(アフィリエイトプログラム、二重恐喝、モバイルランサムウェアなど)

「ランサム攻撃を仕掛ける者たち」向けの**姑息な商売の活性化**
(ランサムウェアの販売、窃取や漏洩したデータやSNS・インサイダーを通じて収集した情報などの取引)

ランサム攻撃グループの中心

「ランサムウェアの作成者やオペレーター」

侵害した標的内部からの攻撃経路や手法が急速に高度化・巧妙化し、検知回避や調査妨害するためのテクニックを進展させることに集中。

ランサム攻撃グループの周辺(複数)

「アフィリエイト(標的にランサムウェアを配送する者)」

標的の外部からランサムウェアを配送するためのサイバー侵害(スパイフィッシング、水飲み場、エクспロイト、ソフトウェアサプライチェーンなど)を試行錯誤。

トピック 2

己(私たちの状況)を知ろう

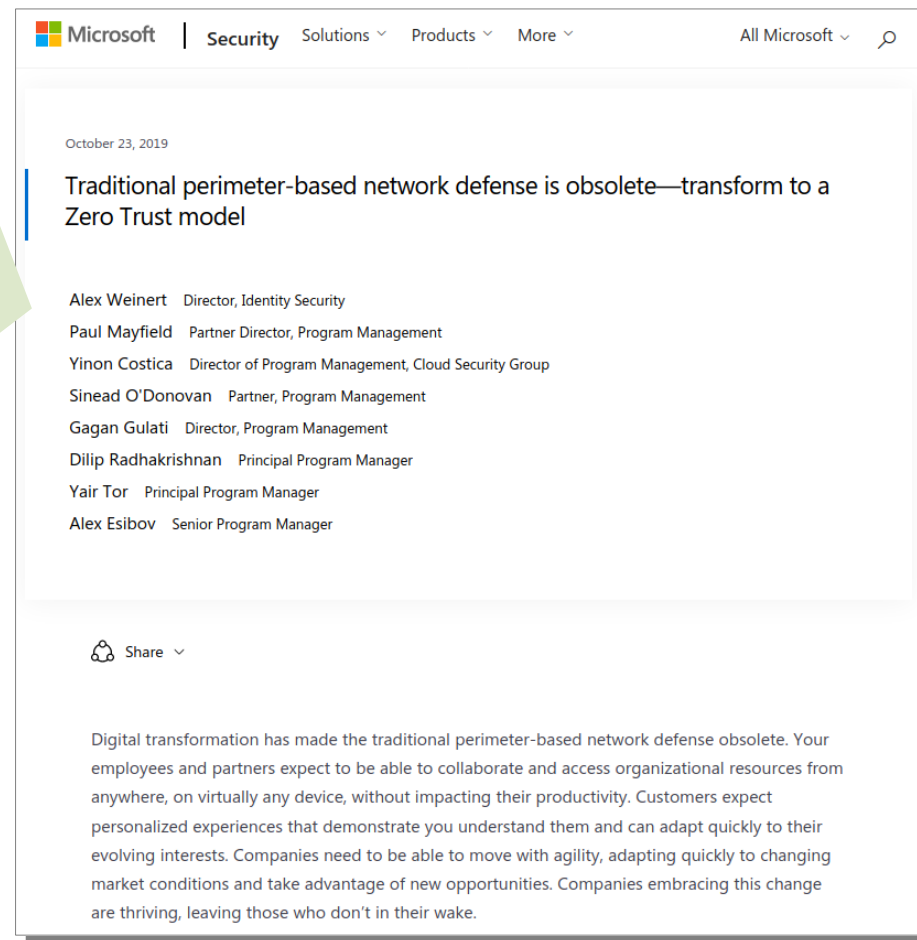
「境界防御」は廃れた – マイクロソフト社の認識

従来のファイアウォール(VPNセキュリティモデル)は、強固な境界線を確認し、その境界線内での活動が「安全」と信じることを前提としていました。

問題は、今日のデジタル資産は、パブリック・クラウドプロバイダーが管理するサービスやエンドポイント、従業員、パートナー、顧客が所有するデバイス、Web対応のスマートデバイスなどで構成されていることですが、これらは従来の境界ベースのモデルでは保護できませんでした。

私たちは、私たち自身の経験と、サポートしてきたお客様の経験から、このモデルを継続するには、あまりにも煩雑で、あまりにも高価で、あまりにも脆弱であることを学びました。

従来の境界ベースのネットワーク防御は廃れた
(2019年10月23日、マイクロソフト社)



<https://www.microsoft.com/security/blog/2019/10/23/perimeter-based-network-defense-transform-zero-trust-model/>

「境界防御」とは - 定義

- 境界防御(perimeter defense)とは、「**防御区域の境界に沿って展開された戦力で構成された、露出した側面を持たない防御**」のこと。

perimeter defense (US DoD Definition)
Definition of the term '*perimeter defense*' per official documentation of the United States Department of Defense.

HOME AVIATION / AEROSPACE ARMOR & ARTILLERY INFANTRY WEAPONS NAVAL WARFARE MILITARY DICTIONARY CALCULATORS RANKS MILITARY PAY

perimeter defense

A defense without an exposed flank, consisting of forces deployed along the perimeter of the defended area. (US DoD)

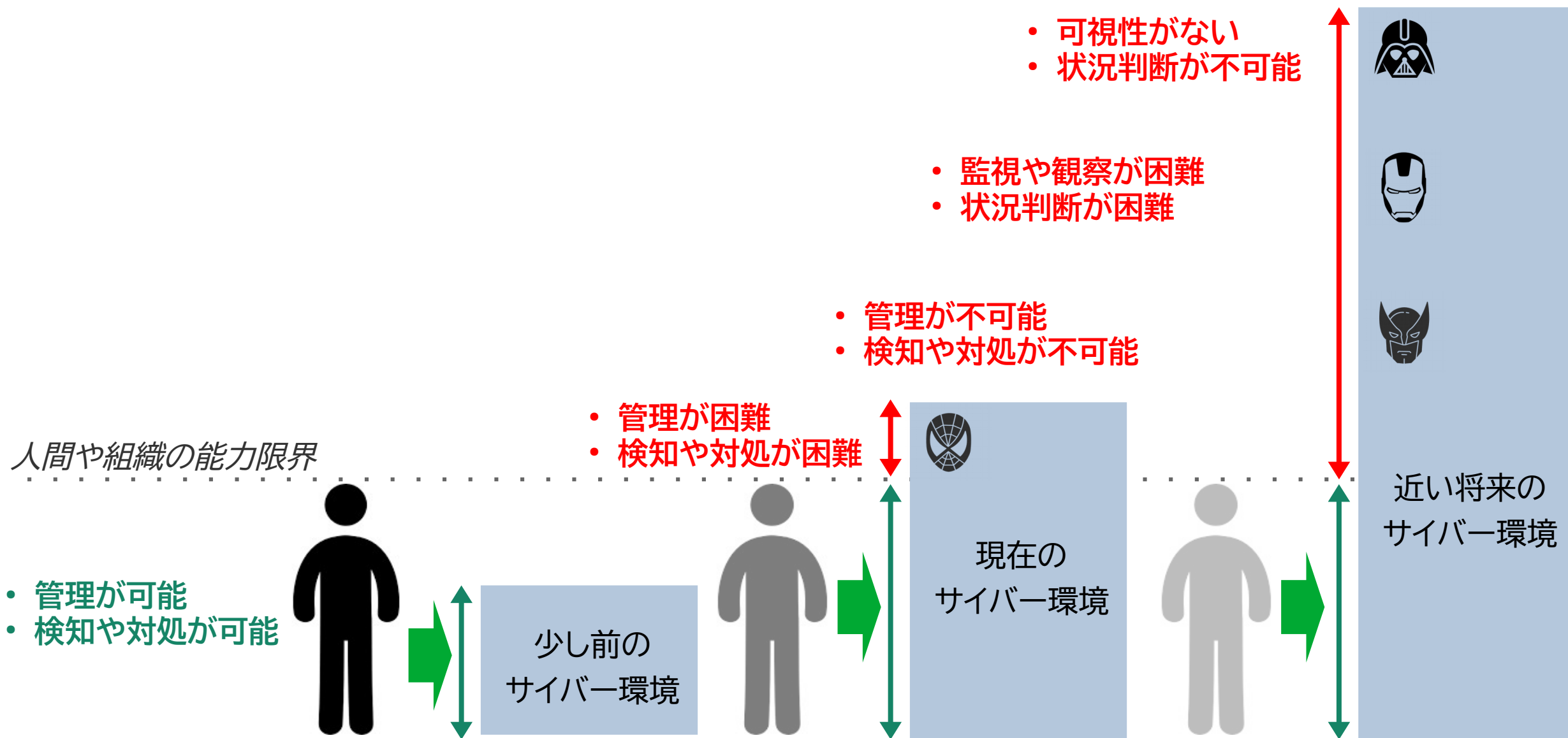
https://www.militaryfactory.com/dictionary/military-terms-defined.php?term_id=4041

「境界防御」とは – 位置づけと役割

- 境界防御(perimeter defense)は、「**ネットワークを攻撃から守る 1つのレベルであり、外部からの攻撃から保護する。**」



(人間や組織が持続的に確保可能な)「境界防御」の限界



「境界防御」は廃れた - (私の)イメージ



トピック 3

(DX推進する中小企業が認識すべき)
サイバーリスクを誘発する要因

(DX推進する中小企業が認識すべき)サイバーリスクを誘発する要因

現実のサイバー脅威に適合しない予算と人的リソース

現実から大きく乖離した**CSIRT**の設計(過剰な責任の割り当て)

外部脅威者から影響を受けるインサイダー活動

セキュリティ担当者とネットワーク運用者の関係が遠い

ホスティングコントロールパネル脆弱性への対応不足

※ 企業が特定される恐れのある認識は全て除いているため、全体の傾向を示したものではない。

現実のサイバー脅威に適合しない予算と人的リソース (1/5)

- 以前から見られる現状

- 「CISSP、CCSP、SSCP、CSSLPなどのサイバーセキュリティ関連の認定資格を持っているというだけでセキュリティ担当部門の配置になった。」

→ 経営層が手がけた「セキュリティ担当部門の基本設計(ミッションステートメント、目的/狙い、目標/評価可能な指標など)」が曖昧あるいは実態にそぐわない。セキュリティ担当者に組織設計させる愚かさが目立つ。

- 「セキュリティ担当部門に対する割当予算の水準が非常に低い。」

→ 予算策定担当者による「サイバーセキュリティ関連の予実管理(企業の予算と管理)」を可能にする仕組みや環境が乏しい。多くの場合、セキュリティ担当部門の基本設計が原因となっている。



セキュリティ担当部門が手がけている業務のイメージ

現実から大きく乖離した**CSIRT**の設計(過剰な責任の割り当て) (2/5)

- 以前から見られる現状

- 「CSIRTに対して、”**セキュリティインシデントを発生させないための責任**が過剰に与えられている。」

→ CSIRTモデルは、セキュリティ対策に係る**サービス(役務)を提供**することがベースであり、特に、インシデントを発生させた領域に対する支援を行うことが前提となっている。(これにより、CSIRTの予実管理に必要な目標設定と評価設計が実現する。)

次の問いを考えていただくことで、この現状の問題の理解が深まる。

「発生した火災に迅速かつ的確に対応できるよう、高度な知識・技術に加え、日々の訓練を積み上げている”街の消防署”に対して、自治体の首長が、**火災を発生させないための責任を与えた**。しかし、”街の消防署”は、その責任を果たそうと努力するが、この範囲は非常に広く、住民や企業の内部領域に踏み込む必要があるため、**今の権限、予算、人的リソースでは困難であると感じている**。おそらく、この責任をはたすることは不可能に近い。

この自治体の首長の判断は適切であったか？

また、”街の消防署”の権限、予算、人的リソースを増やせば解決できるのか？」

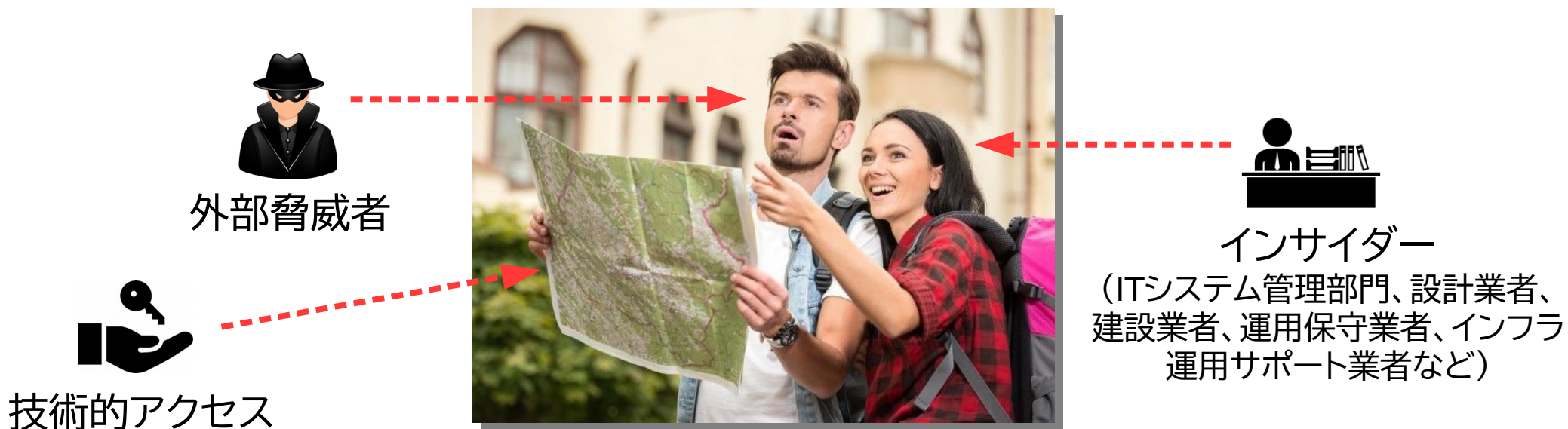


外部脅威者から影響を受けるインサイダー活動 (3/5)

- 最近見られる現状

- 「非常に洗練された脅威主体が、インサイダーを活用して、標的組織における脆弱性の特定、攻撃経路の選定、偵察活動の実施、物理的又はリモートからの技術的アクセスの取得などを行う。」

→ 考えられるインサイダー活動の場は、「ITシステム管理部門」、「設計業者」、「建設業者」、「運用保守業者」、「インフラ運用サポート業者」などである。
これらから、攻撃を計画して実行する外部脅威主体が、標的組織内部の「価値ある情報」へのアクセスを得ることができる。



セキュリティ担当者とネットワーク運用者の関係が遠い (4/5)

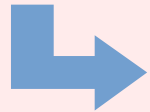
- 最近見られる現状

- コロナ禍、DX推進、サステナビリティ対応などに起因する「急なネットワーク構成変更」の過程において、脆弱性や運用管理の不備などの**セキュリティ上の問題が軽視**される。



(Webサーバー運用のケース)

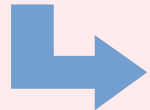
- ✓ 脆弱性や運用管理の不備により、直接的かつ一次的に被害を受ける対象は「顧客」である。
- ✓ 対処や対策のための一時中断により、優先すべき事業継続への悪影響はほとんどない。



セキュリティ担当者：「顧客を守る」という名目で正当化しやすい。(責任を果たせる！)
ネットワーク運用者：ほとんど関係ない。(責任に関係ない！)

(ネットワーク運用のケース)

- ✓ 脆弱性や運用管理の不備により、直接的かつ一次的に影響を受ける対象は「幹部や社員」である。
- ✓ 対処や対策のために一時中断により、優先すべき事業継続に対して悪影響がある。



セキュリティ担当者：「社員を守る」という名目で正当化しにくい。(責任を果たせない・・・)
ネットワーク運用者：一部の幹部や社員からクレームに対応。(責任を果たそうとする・・・)

ホスティングコントロールパネル脆弱性への対応不足 (5/5)

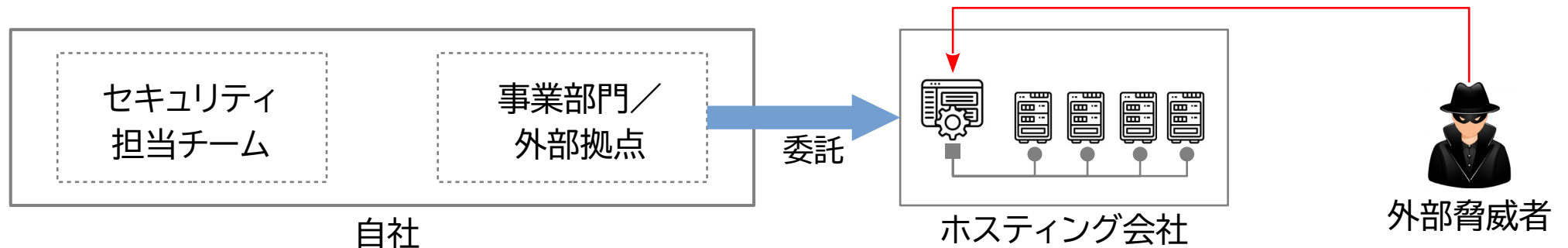
• 最近見られる現状

- 「外部委託しているサーバーを一元管理するために使用されていたコントロールパネルの脆弱性(2段階認証回避など)が発見されていた。しかし、外部のサーバー管理者が把握できずにいたため、侵害を受けて、一部あるいはすべてのサーバーが深刻な被害を受けた。」

➔ 自社(委託元)のセキュリティ担当チームは、日々のサイバー脅威情報の収集活動の中で、ホスティングコントロールパネルの脆弱性情報も収集していたが、自社内での利用がなかったため、分析・評価や共有などはしなかった。

また、社内の事業部門や外部拠点は、契約するホスティング会社(委託先)について、セキュリティ担当チームに事前相談や情報共有をする必要性を感じていなかった。

そのため、セキュリティ担当チームは、ホスティングコントロールパネルの脆弱性情報に対する対応について、委託先に確認するようなアクションを取ることができなかった。



トピック 3

(DX推進する中小企業が検討すべき)
セキュリティ対策の重点事項

(DX推進する中小企業が検討すべき)セキュリティ対策の重点事項

パーミッションと権限の厳格管理

デバイス管理ポリシーの策定と徹底

定期的な社員トレーニングの実施

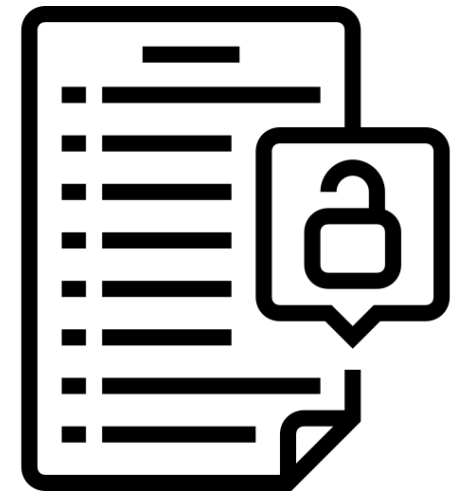
積極的なモニタリングの実施

ユーザーとエンティティの行動分析

インシデントレスポンス計画の策定と習熟

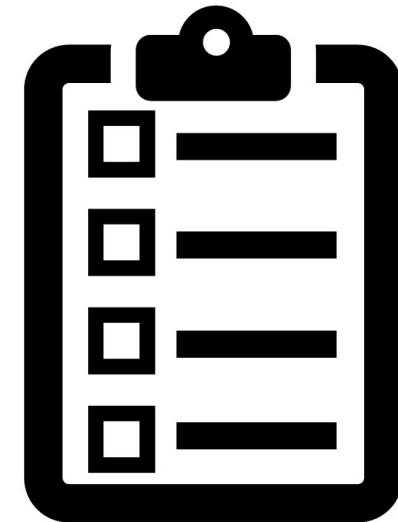
パーミッションと権限の厳格管理 (1/6)

- ユーザーアカウントのパーミッションと権限を厳格に管理することで、「社員が直接インサイダー活動を行った場合」や「アカウントにアクセスした部外者が間接的にインサイダー活動を行った場合」に、**悪意のある侵害のリスクを抑える**ことが期待できる。
 - 社員に最小化権限ポリシーを適用すること。
 - 社員、請負業者、ビジネスパートナーは、職務を遂行するために必要最小限のシステム権限しか持たないようにする。
 - 社員の役割が変更されるたびに権限をレビューすること。
 - 社員が退職する直前に権限を取り消すこと。



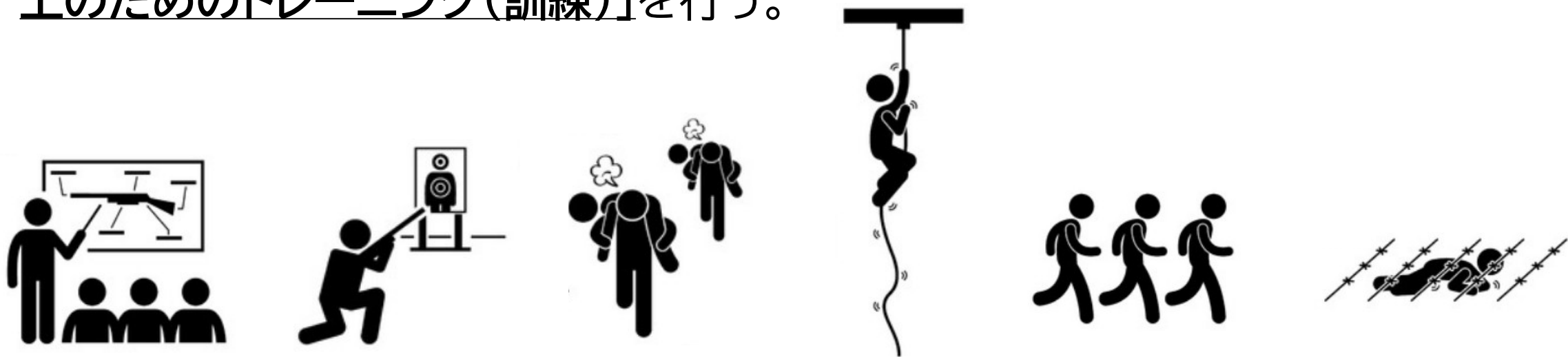
デバイス管理ポリシーの策定と徹底 (2/6)

- ほとんどの企業では、従業員はさまざまな場所からさまざまなデバイスを使って会社のシステムにアクセスしている。
 - 特に、COVID-19の影響により、多くの組織がBYODポリシーを導入しているが、**十分なセキュリティ保護がされていないデバイス**にさまざまなセキュリティ・リスクがある。
- 次の重要事項を含むデバイス管理ポリシーを策定し、実装することが重要である。
 - オフィスのネットワークから分離した、**BYODのためのWi-Fiネットワーク**を提供すること。
 - すべての社員のデバイスにエンドポイント・セキュリティ・ソフトウェアをインストールすること。
 - 許可されたアプリケーションのホワイトリストを作成し、どのツールが許可されているかを社員が確実に把握できるようにすること。
 - リスクの高いデバイスのUSBポートを無効にするか、少なくとも監視すること。



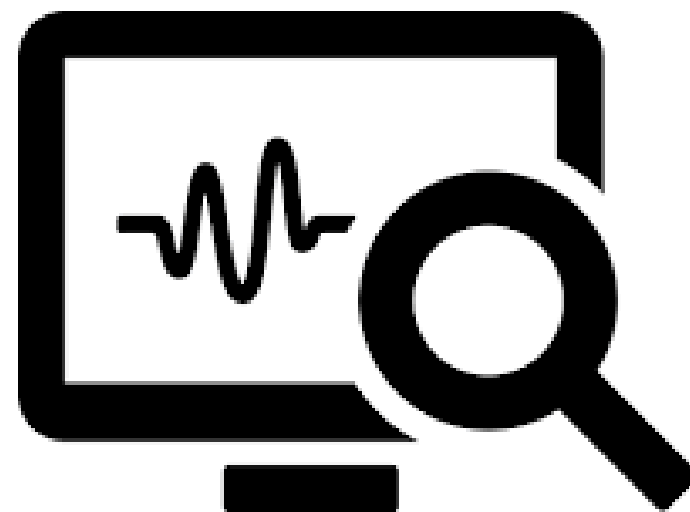
定期的な社員トレーニングの実施 (3/6)

- ヒューマンエラーは運用上の現実であり、多くの場合、**人間そのものがセキュリティチェーンの弱点**である。
- 組織は、定期的な社員トレーニングを実施するに当たり、リスクを軽減させる目的で、次の事項について重要視する必要がある。
 - 社員に、セキュリティ意識を向上させ、データセキュリティの義務について教育する。
 - データ保護、フィッシング対策、パスワード管理などを網羅した「セキュリティ意識向上のためのトレーニング(訓練)」を行う。



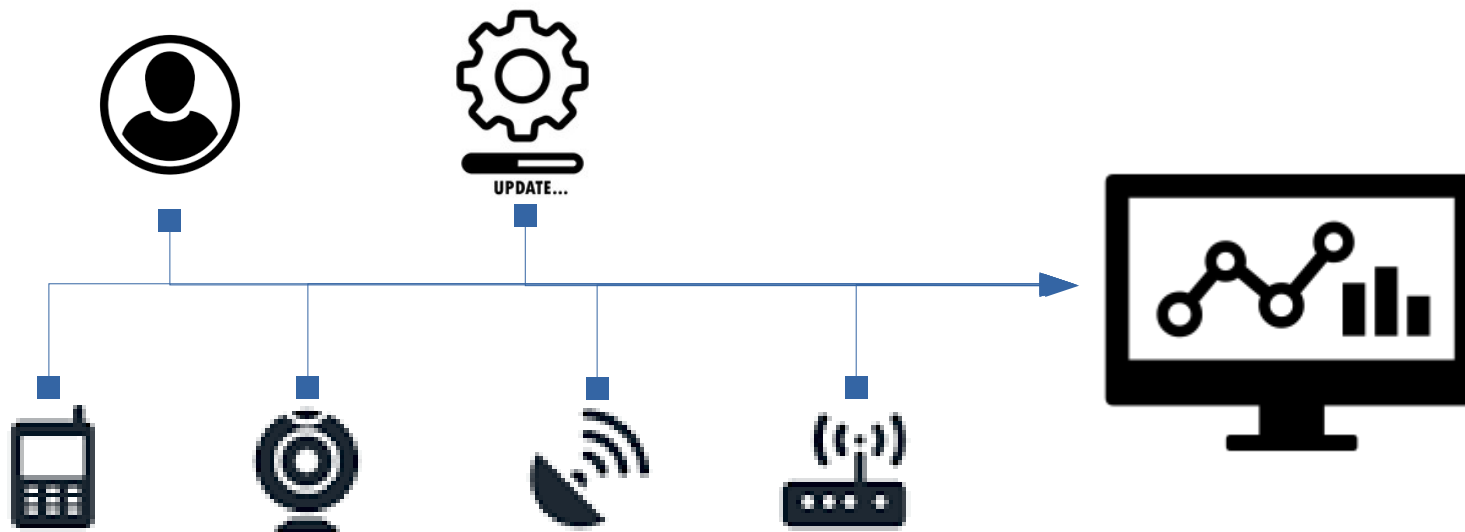
積極的なモニタリングの実施 (4/6)

- インサイダー脅威による被害や混乱が発生する前に、**積極的(プロアクティブ)に検知して即時対処を伴う「モニタリング」の仕組み**を導入する。
 - 例えば、SIEM、IDS、EDRなどの技術を組み合わせて、ネットワークセキュリティとエンドポイントの関係性に着目したモニタリングを行う。
- モニタリングは、まず「正常」なアクティビティのベースラインを確立することから始め、このベースラインから外れたアクティビティにフラグを立てて、関連するデータを集約して上で分析を行った上で、悪意があるかどうかを判断する。



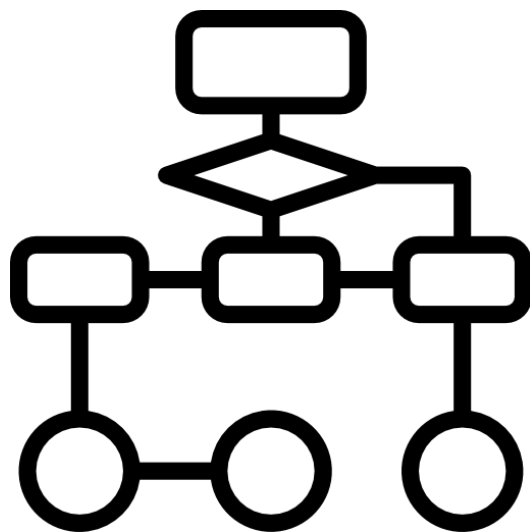
ユーザーとエンティティの行動分析 (5/6)

- 最新のモニタリングツールの多くに実装されている「**ユーザー(人間)とエンティティ(デバイスなど)の振る舞い解析**」を利用する。
 - この分析は、高度な機械学習と行動プロファイリング技術により、アカウントの侵害や権限の乱用などの異常な活動を特定することができる。
 - これにより、既知および未知のユーザーベースの脅威を検出し、無力化することが期待できる。



インシデントレスポンス計画の策定と習熟 (6/6)

- インサイダー侵害が発生した場合、どのシステムがアクセスされたのか、どのユーザーがそのシステムにアクセスしたのか、どのデータが流出したのかを確認するために、**必要なデータを収集・分析するプロセス**が重要となる。
 - 経験豊富なインシデント・レスポンス・ハンドラーに依頼して、データがフォレンジックな方法で処理され、重要な証拠が確保されるようにする必要がある。



トピック

まとめ

まとめ



発言:「我社は、〇〇対策くらいしか
できないなあ……」

行動: 〇〇対策を検討し、△△を導入、
或いは□□を利用する。



会社を守る努力が、単一的で、
一時的に中断する。

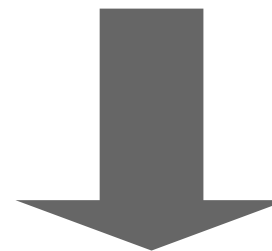


会社を守る努力を、多様化し、
徹底的に持続させる。



発言:「(ゴニョゴニョ)」

行動: 標的組織に対して、攻撃戦略を組
み立て、偵察結果に基づく準備
(武器化やコミュニケーション獲得)を行い、
デリバリ(攻撃経路の構築)やアプローチ
を成功するまで繰り返す。



標的組織に対して、多様な経路で、
高度な攻撃を持続する。

<

=

本資料に関する連絡先

名和 利男 (TOSHIO NAWA)

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

PGP: 0xE38B4E01

