TLP:GREEN

緊急事態の対処能力の向上策に類似する「サイバー攻撃対処態勢の整備」

2020年 2月

名和 利男

アジェンダ

1. 緊急事態としての「**サイバーテロ**」

2. 民間分野では回避・防御することが困難な
   サイバーテロ事態への対策 = **対処能力の構築**

3. 構築した**対処能力の維持・向上**

トピック１

緊急事態としての「サイバーテロ」

「緊急事態」とは

- 緊急事態(Emergency):一般に、健康(身体)・生命・財産・環境に危険が差し迫っている緊急の状態のこと。

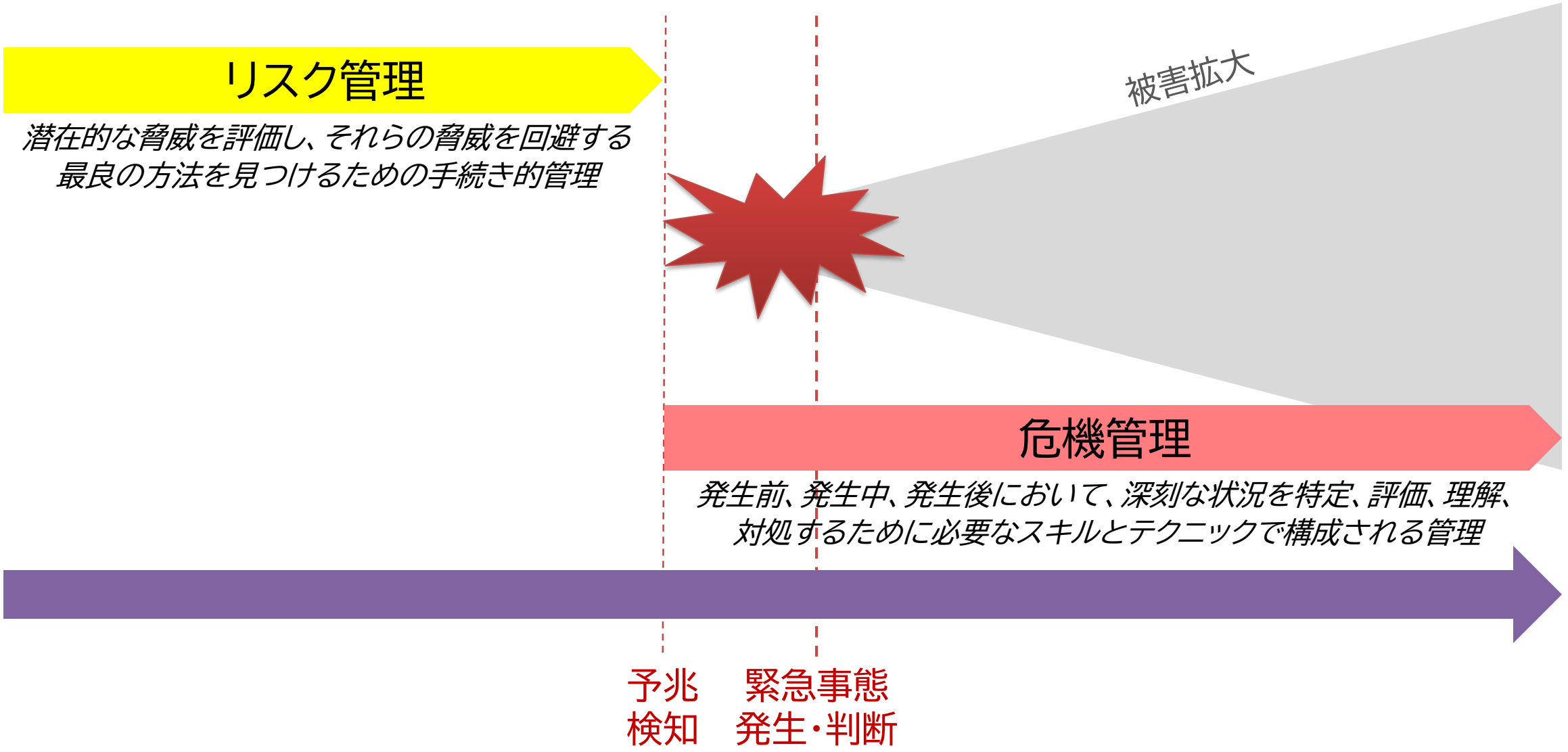
【判断の観点】

- **「(自然災害のような)明らかに多くの生命が脅かされる事態」は、あらゆる主体者が迅速に判断する。**
- **「(サイバーテロのような)緊急性の有無を判断するために必要な事態」は、観察者(あるいは当事者)による主観的な評価を必要とする。**

【対処の観点】

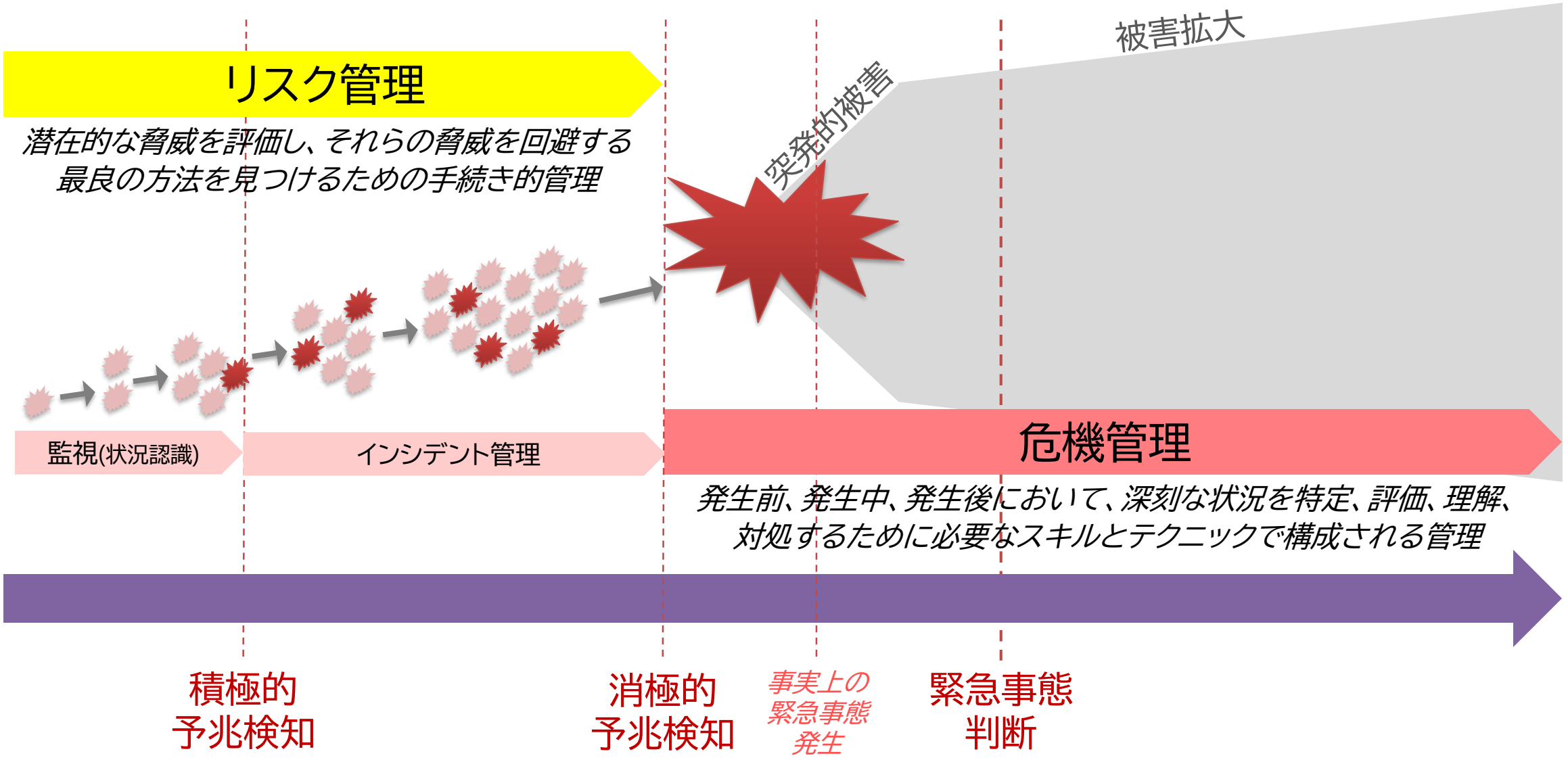
- 「事態の悪化を防ぐための介入等」に急を要するケースが多い。
- 「事態が自然に収束するのを待ってから緩和措置を取る(事後処理)」しか手段がないケースもある。

自然災害のような「明らかに多くの生命が脅かされる緊急事態」



TLP:GREEN

サイバーテロのような「緊急性の有無を判断するために必要な事態」



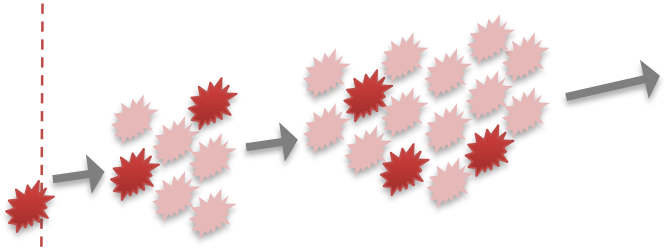
TLP:GREEN

サイバーテロのような「緊急性の有無を判断するために必要な事態」

サイバー攻撃の態様変化による「リスク管理」の限界

リスク管理

潜在的な脅威を評価し、それらの脅威を回避する最良の方法を見つけるための手続き的管理



インシデント管理

積極的
予兆検知

- サイバー攻撃の態様が急激に変化している。
  - ✓ サイバー攻撃が、**極めて複雑化(sophisticated)・大規模化(large-scale)**
  - ✓ **攻撃対象領域(Attack Surface)**が、拡大・深化
  - ✓ **攻撃戦略(Attack Strategies)**が、多様化・重層化・個別化・高度化・弾力化
- 旧来の体制と能力では、「潜在的な脅威」の**見出し・識別・特定・評価は困難**になってきた。
- 「最良の回避方法」の適用可能な範囲は、**急速に縮小**する。（すぐに最良でなくなる）

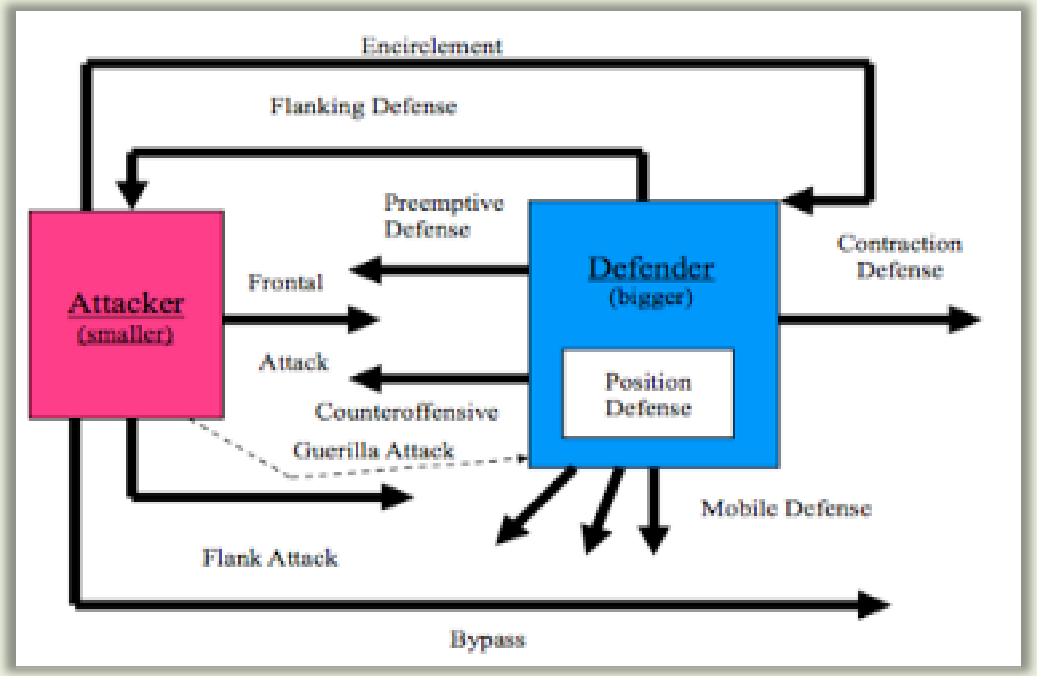
リスク管理領域のセキュリティ投資を強化!

TLP:GREEN

【参考】攻撃対象領域(Attack Surface)と攻撃戦略(Attack Strategies)

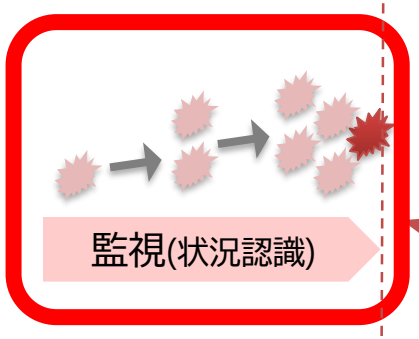
- **攻撃対象領域(Attack Surface)**とは
  - 主にソフトウェア環境を攻撃対象として、許可されていないユーザー(攻撃者)が当該環境にデータを入力する或いはデータを抽出することを可能とするさまざまなポイント(攻撃ベクトル)の総計のこと。

- **攻撃戦略(Attack Strategies)**とは
  - 攻撃対象における不確実性の条件下で1つ以上の攻撃目標を達成するための高レベルの計画のこと。



サイバーテロのような「緊急性の有無を判断するために必要な事態」

サイバー脅威に適合しない「監視」は、攻撃挙動を見逃す



- サイバー脅威の動向変化に適合(Adapt)したセキュリティ監視を実施・強化(対象増強、選択と集中)していない。
- 初期段階のセキュリティ事象の検知あるいは識別ができない。
- 潜在化した攻撃挙動を見逃す。

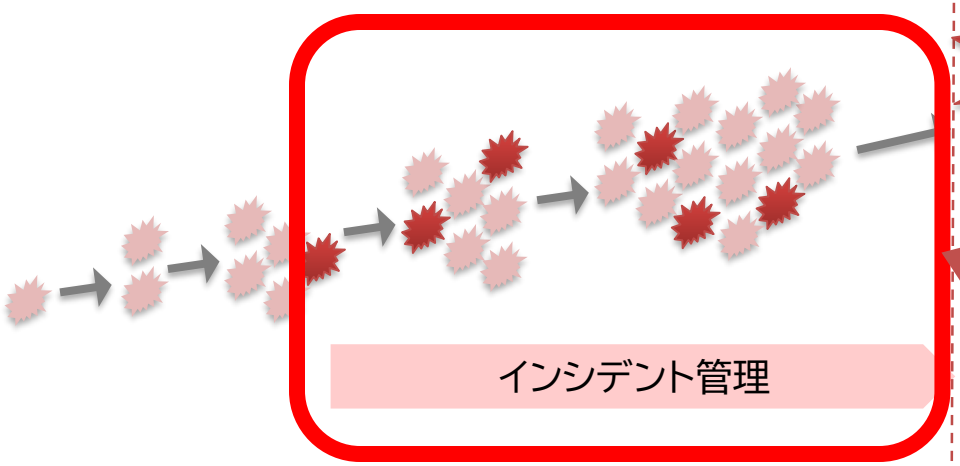
積極的
予兆検知

動向情報の適宜入手と脅威監視への反映!

TLP:GREEN

サイバーテロのような「緊急性の有無を判断するために必要な事態」

挙動痕跡を残す設計思想のない「インシデント管理」は、機能不全になる



- いまだに、「サイバー攻撃の挙動痕跡を積極的に残す設計思想」が適切に組み込まれていない。
- 発生したセキュリティ事象を検知あるいは識別ができない。
- (インシデント対処の対象にならない)セキュリティ事象が潜在的に活動する。
- 事前に規定・マニュアル化したインシデント管理が機能しない。

消極的
予兆検知

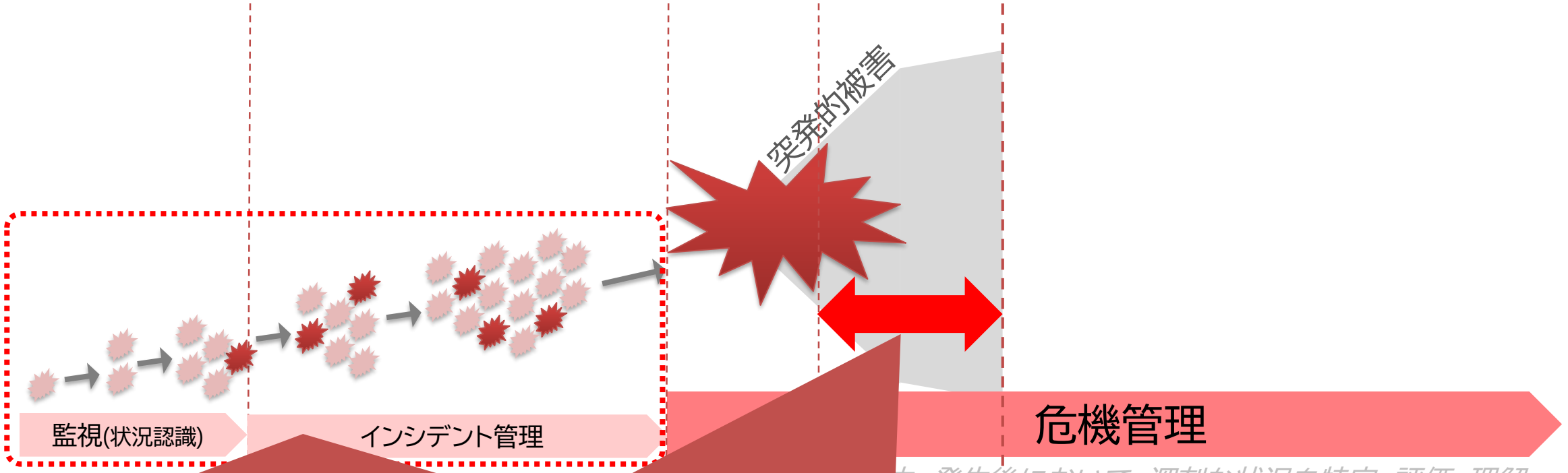
事実上の
緊急事態
発生

挙動痕跡を残す
システム設計を強化!

TLP:GREEN

サイバーテロのような「緊急性の有無を判断するために必要な事態」

監視やインシデント管理の不足は、「発生判断」を遅延させる



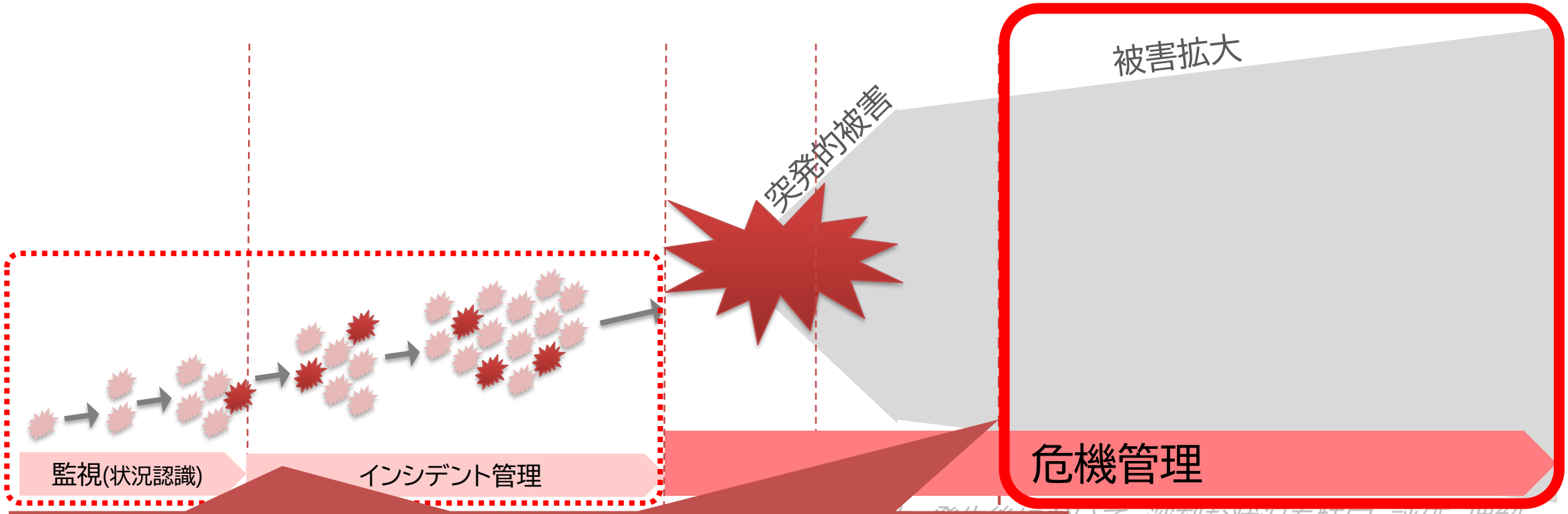
- 発生判断のために、当事者や観察者による**評価(事象の識別、今後の被害推定等)に一定時間を要する**。
- 監視やインシデント管理の不足が多いほど、発生判断に長期間かかり、**推定に頼る領域が発生**する。

挙動痕跡を残す
システム設計を強化!

TLP:GREEN

サイバーテロのような「緊急性の有無を判断するために必要な事態」

監視やインシデント管理の不足は、「被害拡大」を止められない



- 事実解明のために、当事者や観察者(専門家)による対処(調査、識別・特定、分析、報告・説明)に一定時間を要する。
- 監視やインシデント管理の不足が多いほど、事実解明に長期間かかり、未対処の領域(被害)が拡大する。

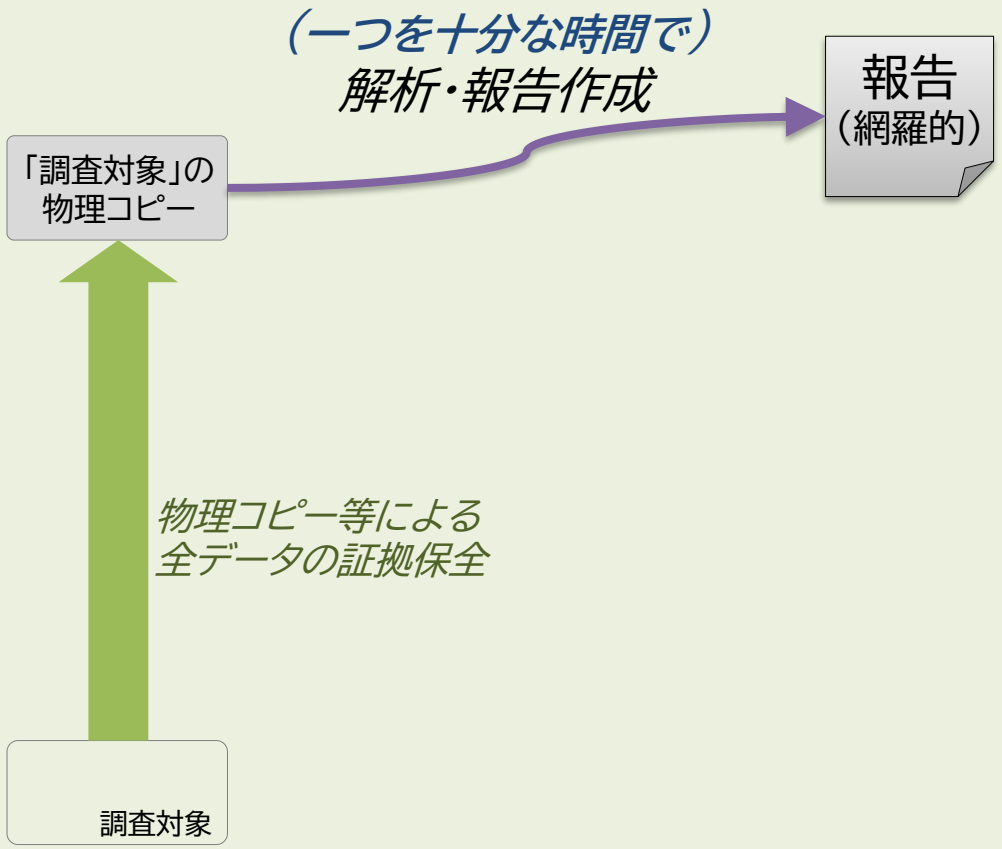
挙動痕跡を残す
システム設計を強化!

TLP:GREEN

【参考】最近の観察者(専門家)による対処(調査、識別・特定、分析、報告・説明)

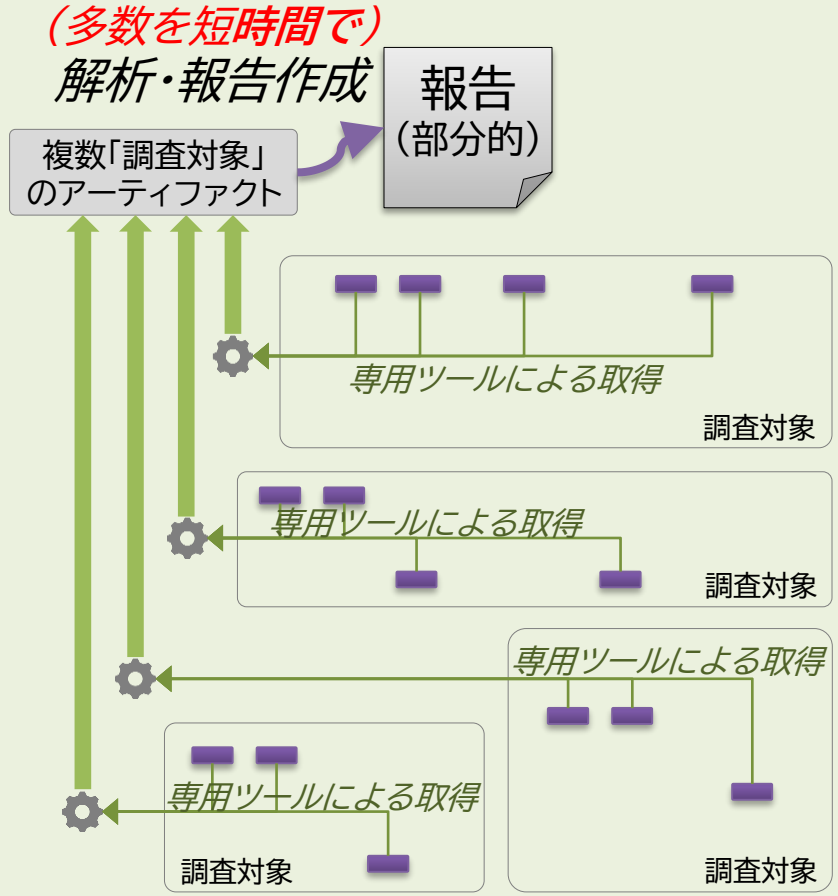
従来の「デジタル・フォレンジック」

単体の調査対象、全データの抽出と解析、長い(十分な)時間



「ファスト・フォレンジック」

複数の調査対象、アーティファクトのみの抽出と解析、短い時間



TLP:GREEN

「緊急事態」とは

- 緊急事態(Emergency):一般に、健康(身体)・生命・財産・環境に危険が差し迫っている緊急の状態のこと。

【判断の観点】

- 「(自然災害のような)明らかに多くの生命が脅かされる事態」は、あらゆる主体者が迅速に判断する。
- 「(サイバーテロのような)緊急性の有無を判断するために必要な事態」は、観察者(あるいは当事者)による主観的な評価を必要とする。

【対処の観点】

- **「事態の悪化を防ぐための介入等」に急を要するケースが多い。**
- 「事態が自然に収束するのを待ってから緩和措置を取る(事後処理)」しか手段がないケースもある。

2019年11月 オランダNCSCがランサムウェア攻撃状況を公表

- オランダの国家サイバーセキュリティセンター(NCSC)が公開した機密文書によると、世界中の企業少なくとも1800社が3種類のランサムウェア(LockerGoga、MegaCortex、Ryuk)に感染していたことが明らかになった。
- 感染した企業名については明らかにされていないが、自動車、建設、化学、医療、食品等、様々な業種の企業が含まれる。
  - また、多国籍企業の支社も含まれており、オランダの重要インフラのサプライヤである米国の化学企業のオランダ支社も含まれている。
- マルウェアのキャンペーンは2018年7月に開始された可能性が高く、NCSCの専門家は、ゼロデイの脆弱性を悪用した可能性があるとみている。

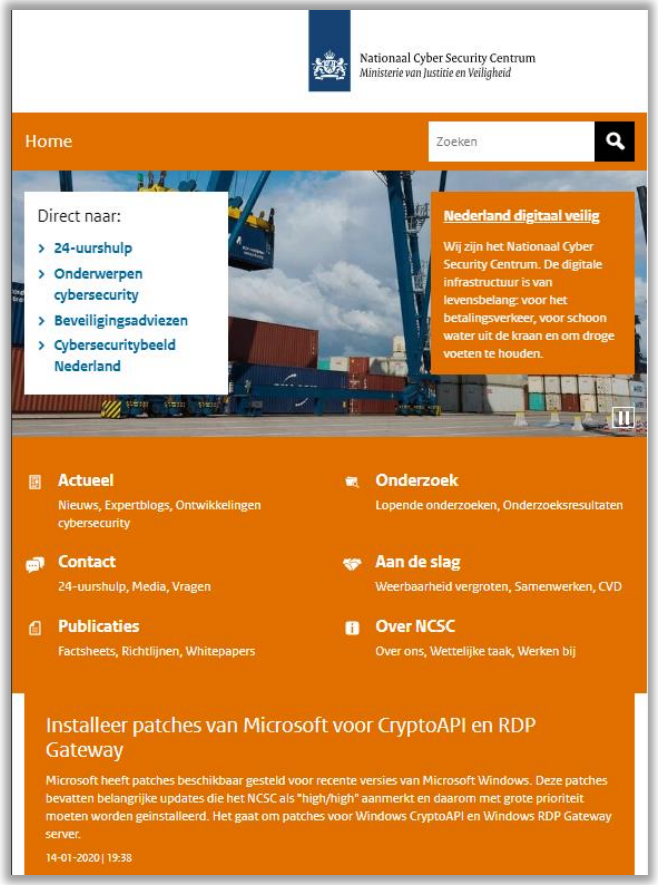
https://nos.nl/artikel/2312363-nederlandse-bedrijven-slachtoffer-van-geavanceerde-gijzelsoftware.html

TLP:GREEN

2019年11月 **オランダNCSC**がランサムウェア攻撃状況を公表

コメント：

- *この情報源であるオランダの国家サイバーセキュリティセンター（NCSC）は、安全保障・法務省(Ministry of Security and Justice)内に設置されている政府機関で、**オランダのサイバーセキュリティ分野で中心的な役割を果たしており、担当分野の研究だけでなく、情報のハブとしての機能**を併せ持つ。ミッションは、**デジタル領域におけるオランダのレジリエンスの向上の貢献し、安全かつオープンで安定した情報社会を創出すること**である。*
- *このような位置づけと必要能力を有するNCSCは、このようなランサムウェア攻撃のレベルを「**独自のロケットランチャーを保有する麻薬犯罪者に匹敵する**」とみている。*
- *また、「**企業はまだすべての基本的な対策を講じていない**」と分析し、「**アップデートを実行し、社員がデジタル脅威を認識していることを確認し、バックアップを作成してほしい**」と強調している。*



https://www.ncsc.nl/

TLP:GREEN

2019年11月 フランスANSSIが病院のランサム攻撃対処に介入

- 2019年11月15日夕方、スタッフ数1万人、ベッド数2,500のヨーロッパ最大級の医療施設であるフランス・ルーアン大学病院センターがランサムウェアによる攻撃を受け、6,000台のコンピュータが感染。
  - 多くのファイルがロックされ、外部ストレージのデータも破損した。
  - 病院スタッフはペンと紙による作業を余儀なくされ、3日間、通常のサービスが提供できない状態となった。
- フランスの**国家情報システム・セキュリティ庁(ANSSI)が介入**し、18日月曜午後までに、影響を受けたアプリケーションの少なくとも4分の1を通常の状態に回復した。
- 約1週間後、CryptoMix Clopランサムウェアが使用され、身代金40ビットコイン（約3200万円）を要求されていたことが報じられた。

https://www.theregister.co.uk/2019/11/21/french_hospital_rouen_ransomware/

2019年11月 フランスANSSIが病院のランサム攻撃対処に介入

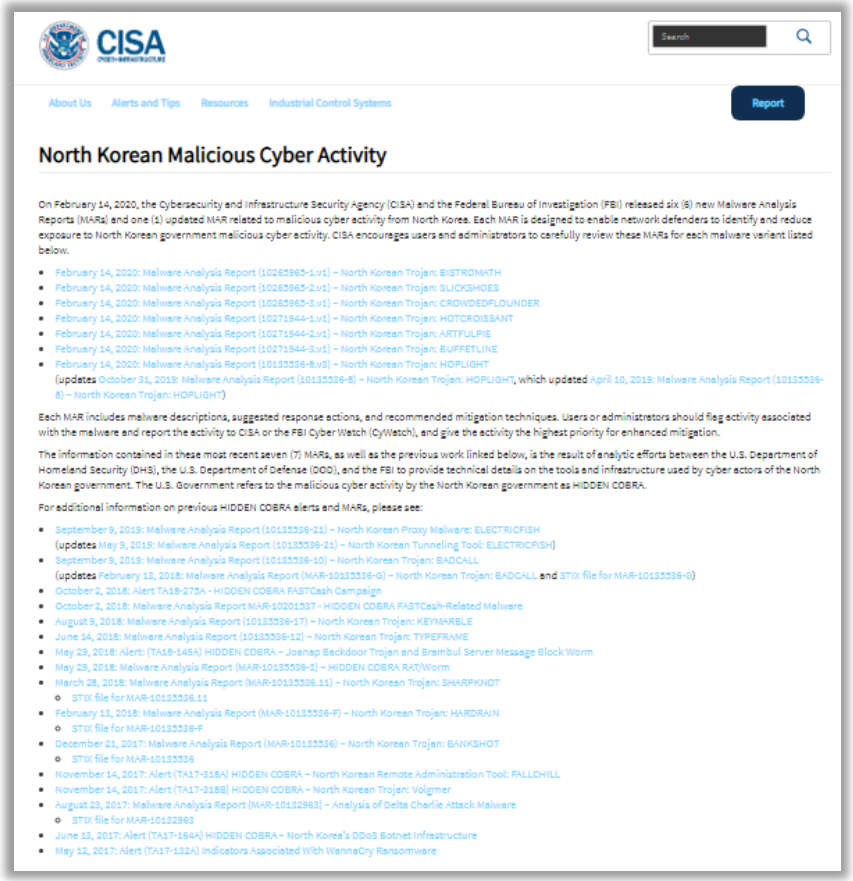
コメント：

- *フランスの国家情報システム・セキュリティ庁(ANSSI)は、**国家情報システムの保護に関する規則の提案や採用された対策の実施を検証する責任を持つ**。また、**サイバー防衛の分野では、監視、検出を提供し、特に国のネットワーク上でのコンピュータ攻撃に対する警告と対処**を行っている。*
- *一般的に、**病院は、その専門性の発揮を優先し、多忙を極めているため、サイバーセキュリティに関する知識が不足しがち**であり、一般的なセキュリティ教育では十分に啓発することが難しい。*
- *それに関わらず、**最近の病院は、医療事務の迅速化・効率化のためにコンピュータ化・ネットワーク化を推進**しており、その依存度をますます高めている。*
- *そのため、ランサムウェア攻撃で使用不能になったコンピュータやネットワークにより医療行為（診断や治療）が困難になると認識した病院は、他の分野に比べて、**復旧を確実にしようと身代金を支払おうとする傾向が強い**。*
- *攻撃者は、このような身代金を支払う傾向の強い分野を標的とした**ランサムウェア攻撃を継続・増強していく**とみられている。*

TLP:GREEN

2020年2月 米国CISA等が北朝鮮マルウェアに関する情報開示

- 米国サイバーセキュリティ・インフラストラクチャセキュリティ庁(CISA)及びFBIは、北朝鮮からの悪意のあるサイバー活動に関連する6つの新規および更新されたマルウェア分析レポート(MAR)を含む北朝鮮マルウェアに関する情報をリリースした。
  - 各MARは、手作業によるリバースエンジニアリングによって取得された詳細な分析情報を組織に提供するように設計されたものである。
  - また、米国政府が北朝鮮政府の悪意のある活動に言及していることを鑑み、ネットワーク防御者によるHIDDEN COBRAの悪意のあるサイバー活動の検出及び減少・緩和を支援するために発行されたものである。



https://www.us-cert.gov/northkorea

TLP:GREEN

2020年2月 米国CISA等が北朝鮮マルウェアに関する情報開示

コメント：

- *このレポートの中で、サイバーセキュリティ・インフラストラクチャセキュリティ庁(CISA)は、**組織に対して、セキュリティ体制を強化するためのベストプラクティス推奨**した。*
  - *最新のウイルス対策シグネチャとエンジンを維持する。*
  - *オペレーティングシステムのパッチを最新の状態に保つ。*
  - *ファイルとプリンターの共有サービスを無効にする。これらのサービスが必要な場合は、強力なパスワードまたはActive Directory認証を使用する。*
  - *不要なソフトウェアアプリケーションをインストールして実行するユーザーの能力（許可）を制限する。必要な場合を除き、ユーザーをローカル管理者グループに追加しない。*
  - *強力なパスワードポリシーを適用し、定期的なパスワード変更を実施する。*
  - *添付ファイルが予期され、送信者がわかっているように見える場合でも、電子メールの添付ファイルを開くときは注意する。*
  - *未承諾の接続要求を拒否するように構成された、管理されたワークステーションであってもパーソナルファイアウォールを有効にする。*
  - *管理されたワークステーションおよびサーバーであっても不要なサービスを無効にする。*
  - *疑わしい電子メールの添付ファイルをスキャンして削除する。スキャンされた添付ファイルが「真のファイルタイプ」であることを確認する（つまり、拡張子がファイルヘッダーとの一致）。*
  - *ユーザーのWebブラウジング習慣を監視する。不適切なコンテンツを含むサイトへのアクセスを制限する。*
  - *リムーバブルメディア(USBサムドライブ、外部ドライブ、CDなど)を使用する場合は注意する。*
  - *実行する前に、インターネットからダウンロードしたすべてのソフトウェアをスキャンする。*
  - *最新の脅威に対する状況認識を維持し、適切なアクセス制御リスト(ACL)を実装する。*

TLP:GREEN

【参考】米国のサイバーセキュリティ・インフラセキュリティ庁(CISA)

- 2017年12月11日、CISA(サイバーセキュリティ・インフラセキュリティ庁)法(H.R. 3359: CISAA31)が、下院を通過した。
  - 元の法案である**2002年の国土安全保障法**を改正して、国家防護計画局(NPPD)を格上げして、その名称を「サイバーセキュリティインフラ防護庁(CIPA)」に変更することであったが、2017年にCISA (Cybersecurity and Infrastructure Security Agency)法案に改称された。
- 主な狙いは、サイバー脅威と物理的脅威から**連邦ネットワークと重要インフラを防護することを任務とする国家防護計画局(NPPD)を政策実施機関へと再編**し、**新たにサイバーセキュリティ・インフラセキュリティ庁(CISA)として出発**させることにある。
- CISAの長官には米国のサイバーセキュリティ、緊急時通信および重要インフラの**セキュリティとレジリエンスを防護・強化する全米努力を主導する国家サイバーセキュリティ・インフラセキュリティ局長**が就任した。

「国家サイバーセキュリティ・インフラセキュリティ局長」の主な責務

① CISAのサイバーセキュリティ及び重要インフラセキュリティプログラム、オペレーションおよび**関連政策(国家サイバーセキュリティアセットレスポンス活動を含む)を主導**すること。

② CISAのサイバーセキュリティおよび重要インフラ活動を実施するために、**SSA(セクター別所轄官庁)を含む連邦省庁と国際機関を含む非連邦機関の調整活動を履行**すること。

③ 2015年のサイバーセキュリティ法などの法律を遵守し、**連邦の情報及び情報システムのセキュリティを確保する責任を履行**すること。

④ **重要インフラリスクに対して、セキュリティの確保及び防護のための全米努力を調整**すること。

⑤ **重要インフラの所有者及び運用者に対して、脅威等の分析結果、知見及びテクニカルアシスタンスなどを提供**すること。

TLP:GREEN

【参考】日本のNISC(内閣サイバーセキュリティセンター)について

- NISCの所掌業務は、**行政各部における情報システム、サイバーセキュリティ、施策に関する事項**に限られている。
  - 情報通信ネットワーク又は電磁的記録媒体(電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であつて、電子計算機による情報処理の用に供されるものに係る記録媒体をいう。)を通じて行われる**行政各部の情報システム**に対する不正な活動の監視及び分析に関すること。
  - **行政各部におけるサイバーセキュリティ**(サイバーセキュリティ基本法(平成二十六年法律第百四号)第二条に規定するサイバーセキュリティをいう。以下この項において同じ。)の確保に支障を及ぼし 、又は及ぼすおそれがある重大な事象の原因究明のための調査に関すること(内閣情報調査室においてつかさどるものを除く。)。
  - **行政各部におけるサイバーセキュリティ**の確保に関し必要な助言、情報の提供その他の援助に関する こと。
  - **行政各部におけるサイバーセキュリティ**の確保に関し必要な監査に関すること。
  - 前各号に掲げるもののほか、**行政各部の施策**に関するその統一保持上必要な企画及び立案並びに総合調整に関する事務のうちサイバーセキュリティの確保に関するもの(国家安全保障局、内閣広報室及び 内閣情報調査室においてつかさどるものを除く。)

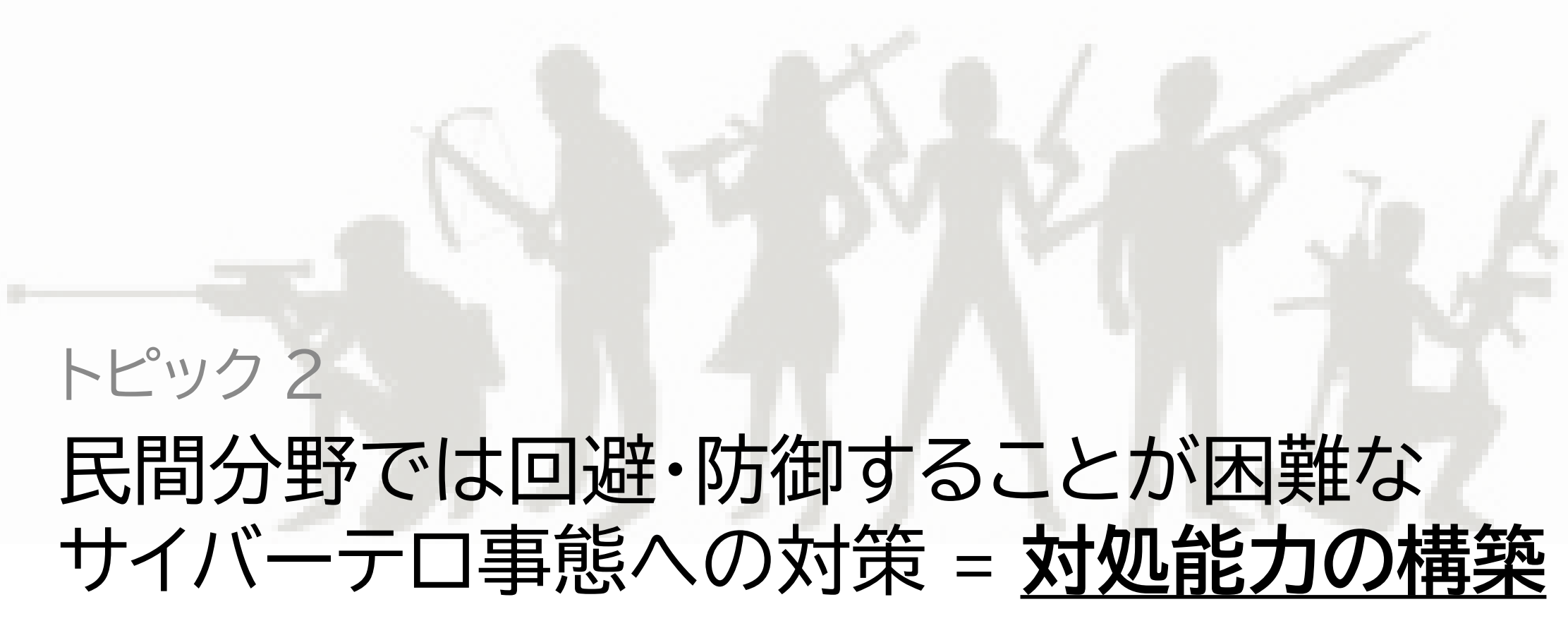
出典: 内閣官房組織令第四条の二（昭和三十二年政令第二百十九号）

「内閣サイバーセキュリティセンター長」の責務

① 内閣サイバーセキュリティセンター長は、内閣官房長官、内閣官房副長官、内閣危機管理監及び内閣情報通信政策監を**助ける**。

② 内閣サイバーセキュリティセンターの**事務を掌理**する。

TLP:GREEN

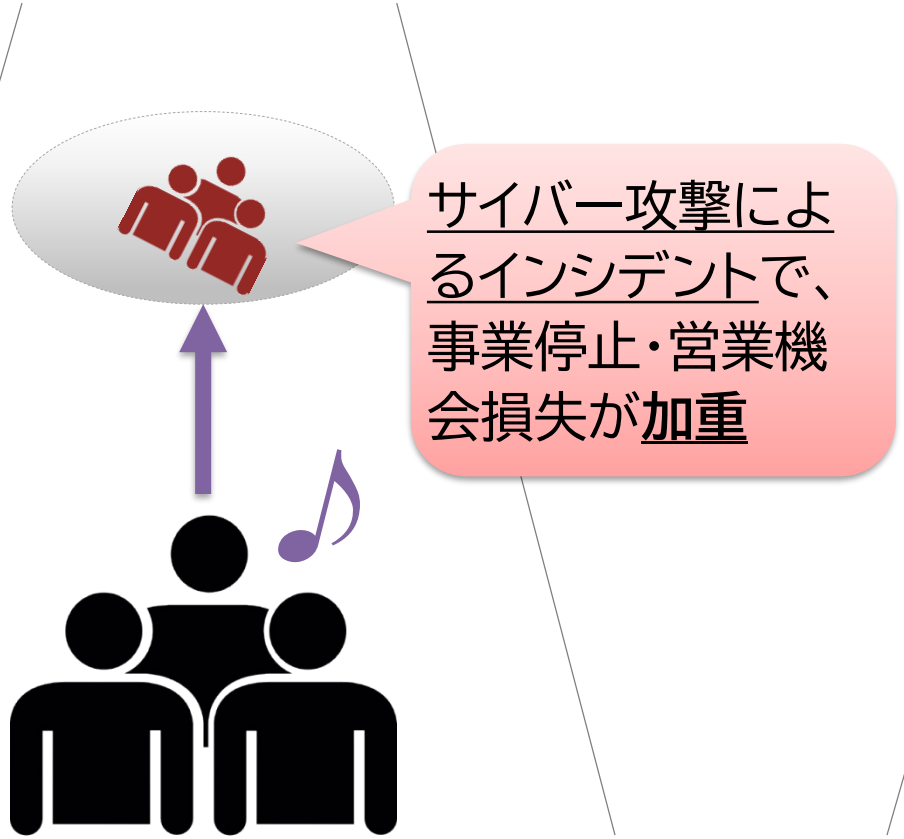


トピック 2

民間分野では回避・防御することが困難なサイバーテロ事態への対策 = **対処能力の構築**

「不十分な状況認識」と「適切な状況認識」の領域を特定する

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**

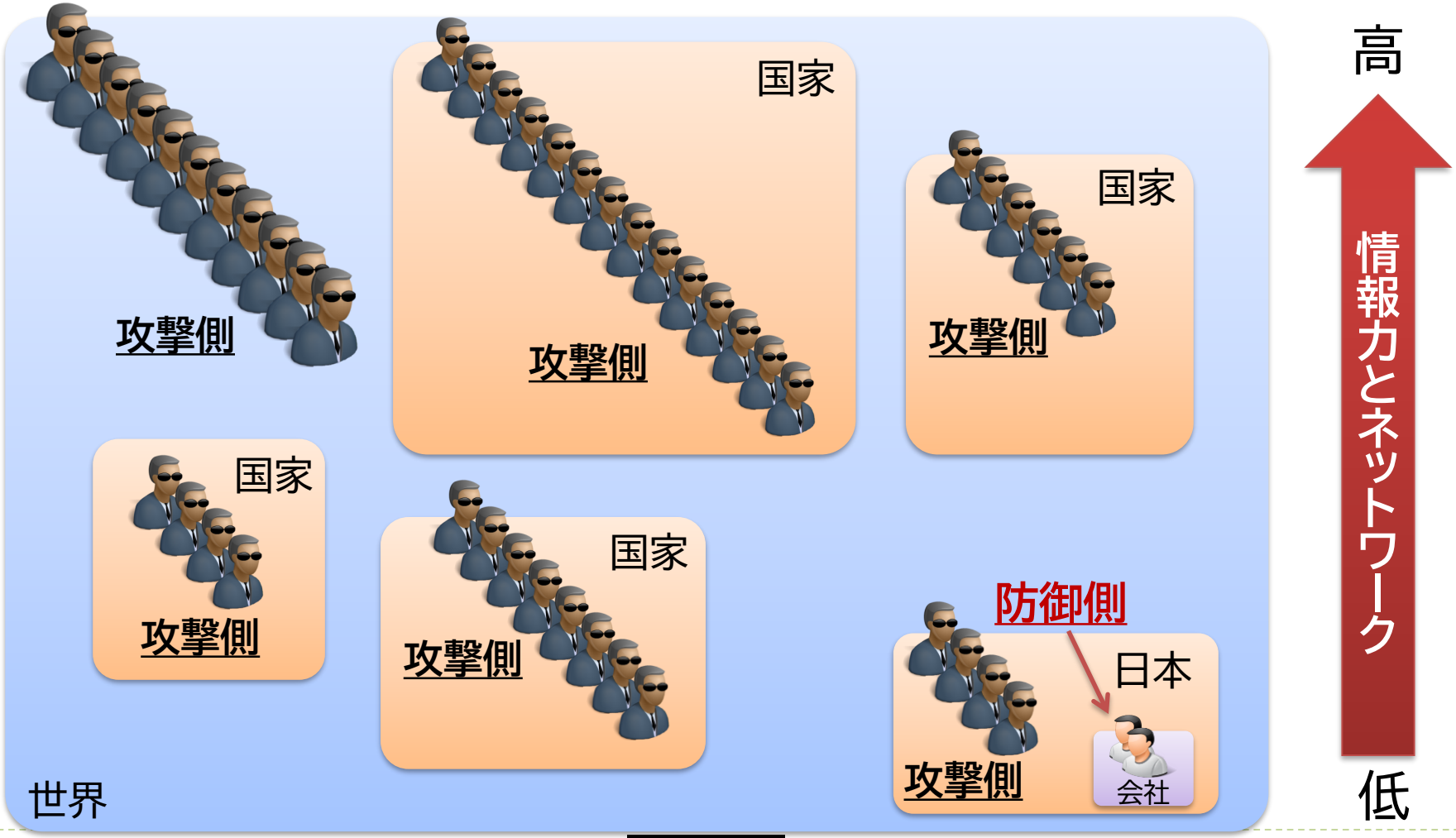
適切な状況認識

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・営業機会損失が**軽減**

TLP:GREEN

「防御側」における情報力とネットワークの圧倒的な低さを知る

- サイバー攻撃は、攻撃側の事前偵察(窃取)した情報と互助関係にあるネットワークで増大。
- サイバー攻撃は「非対称」であるが、**攻撃側と防御側の情報力とネットワークは「対称」**。



TLP:GREEN

「防御側」における情報保証(IA)に偏重 した**認知バイアスを知る**

- APT攻撃の重点事項は、CND(Computer Network Defense)概念に基づく「システムによる多層的な防御」である。
- IA(Information Assurance)概念に基づいたセキュテリィ対策は、「情報資産の単層的な防御」になりがちである。(IAを重点事項にした場合、システム管理者に対し「*適切に・・・せよ。*」という現場任せの指示になりやすい。)

- 「**外部漏洩させない**」セキュリティ対策
- 「IA的なインシデント ＝ **情報漏えい**」
- 攻撃プロセスの**後半で認識**
- **システム所有者(発注者)が対応**

「情報資産」をベースにしたセキュリティ対策

- 「**侵入させない**」セキュリティ対策
- 「CND的なインシデント ＝ **侵入**」
- 攻撃プロセスの**前半で認識**
- **システム保守管理者(委託者)が対応**

「システム防護」をベースにしたセキュリティ対策

TLP:GREEN

「防御側」における厳しい環境と**現実を認識する**

攻撃側

攻撃の強い意図や目的を有する
（経済的利得、主義主張の達成等）

➢攻撃者は、利己的行動の特性を持つ

試行錯誤の侵入行為や
マルウェア作成等による経験の蓄積

➢攻撃者は、豊富な（攻撃）経験を持つ

攻撃技術や対象組織に関する情報を
円滑かつ迅速に共有

➢攻撃者は、互いの情報共有が活発

攻撃を実施しやすい
IT環境の獲得と積極的な利用

➢攻撃者は、ITリテラシーを高く発揮できる環境

経済的困窮や利益確保のための
攻撃者の急激な増加

➢攻撃者は、インセンティブを得やすい環境

防御側 (インシデントレスポンダー)

(組織)防御に係る高い目的意識と
活動意欲を有する

➢防御者は、利他的行動の特性を持つ

インシデント対処の経験の蓄積
（サイバー演習による擬似的経験）

➢防御者は、豊富な(防御活動)経験を持つ

防御技術や攻撃主体に関する情報を
円滑かつ迅速に共有

➢防御者は、他と情報共有を活発にする

防御を実施しやすい
IT環境の獲得と積極的な利用

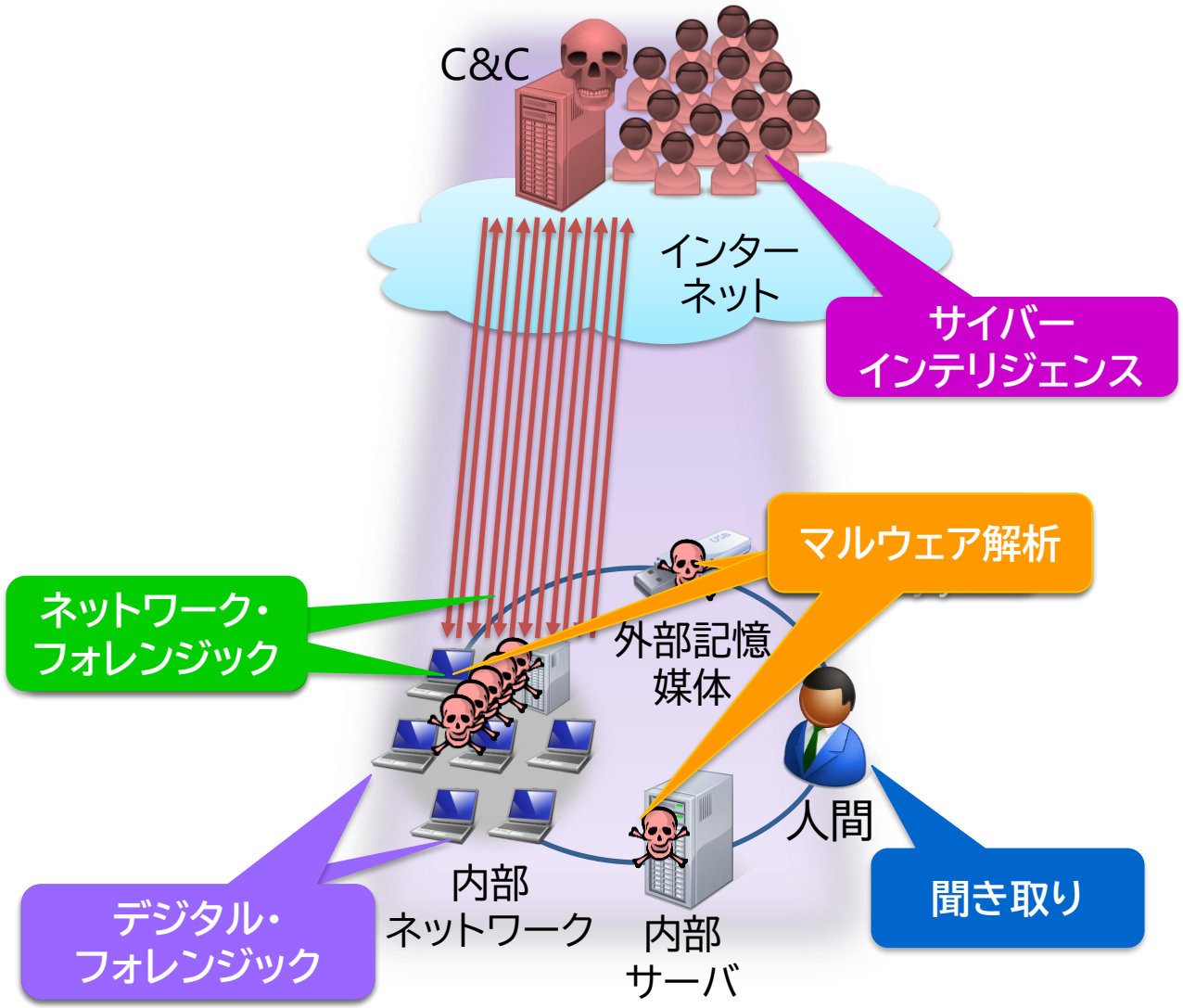
➢防御者は、ITリテラシーを高く発揮できる環境

防御活動によるインセンティブのある
対処要員の増強

➢防御者は、インセンティブを得やすい環境

TLP:GREEN

インシデントの現場で求められる対処能力を構築・獲得する



現場で必要な対処能力

＝

- デジタル・フォレンジック
- ＋ ネットワーク・フォレンジック
- ＋ マルウェア解析
- ＋ 聞き取り
- ＋ サイバーインテリジェンス

TLP:GREEN

インシデントの現場で求められる**対処能力を構築・獲得する**

以前までの対処活動	デジタル・フォレンジック	**コンピュータシステム上の痕跡**(特にファイルシステムの履歴)、及び搭載されている**ソフトウェアによる様々な記録情報**を分析すること。
	聞き取り	
	マルウェア解析	残存していたマルウェアの静的及び動的解析により、マルウェアの**活動実態やその目的を把握**するために行う分析のこと。
最近の対処活動	インシデントハンドリング／コーディネーション	現場の運用者や技術者だけではなく、**責任を持つ管理職や経営層**がどのような方針や手順で**インシデント解決までの道筋**(インシデントハンドリング)を立てるか、または、解決のために複数の組織や部署を巻き込む必要のある場合の**組織間連携**(インシデントコーディネーション)をどのようにすべきかなどのアドバイスや方法論・ノウハウを提供すること。
	ネットワーク・フォレンジック	マルウェアの挙動や内部データ(ファイル)の流出経路などを解明する、或いは不正な挙動を確認するも、マルウェアが発見できない場合などに、**サーバ／プロキシ／ファイアウォール等のログを分析**したり、コンピュータシステムにおいてネットワークコマンドやシステム管理コマンドで得られる全ての出力データを総合的に分析すること。
	サイバーインテリジェンス	技術的な分析のみでは解明が困難な場合、同じ分野のレスポンスチームやCSIRTで経験して明らかになっている**攻撃手法や技術、攻撃者コミュニティで流通している手法**、その他、類似したマルウェアによる事例等を収集し、それらの情報との類似性に着目して分析すること。

TLP:GREEN

インシデントの現場で求められる対処能力を構築・獲得する

以前までの対処活動

最近の対処活動

デジタル・フォレンジック

聞き取り

マルウェア解析

インシデントハンドリング／コーディネーション

ネットワーク・フォレンジック

サイバーインテリジェンス

（技術的能力）

- インターネットのアーキテクチャ、理念、将来像に関する知識
- ネットワークインフラのリテラシーと設計思想の理解
- ネットワークプロトコルの深い理解
- ネットワークアプリケーション、サービス、関連プロトコルの理解
- セキュリティの基本原則
- コンピュータ及びネットワークに対するリスクと脅威の理解
- セキュリティの脆弱性や弱点、及びそれを利用した攻撃の理解
- ネットワークセキュリティ対策とその問題に関する知識と理解
- 暗号化技術、デジタル署名、ハッシュアルゴリズムの理解
- プログラミング、ネットワークコンポーネント、基本ソフトの理解と経験

（管理的能力）

- **安全管理/危機管理/危機対応能力**
- コミュニケーション（対人）能力、言語能力
- 作業編成能力
- 強い目的意識と不屈の精神

防御側

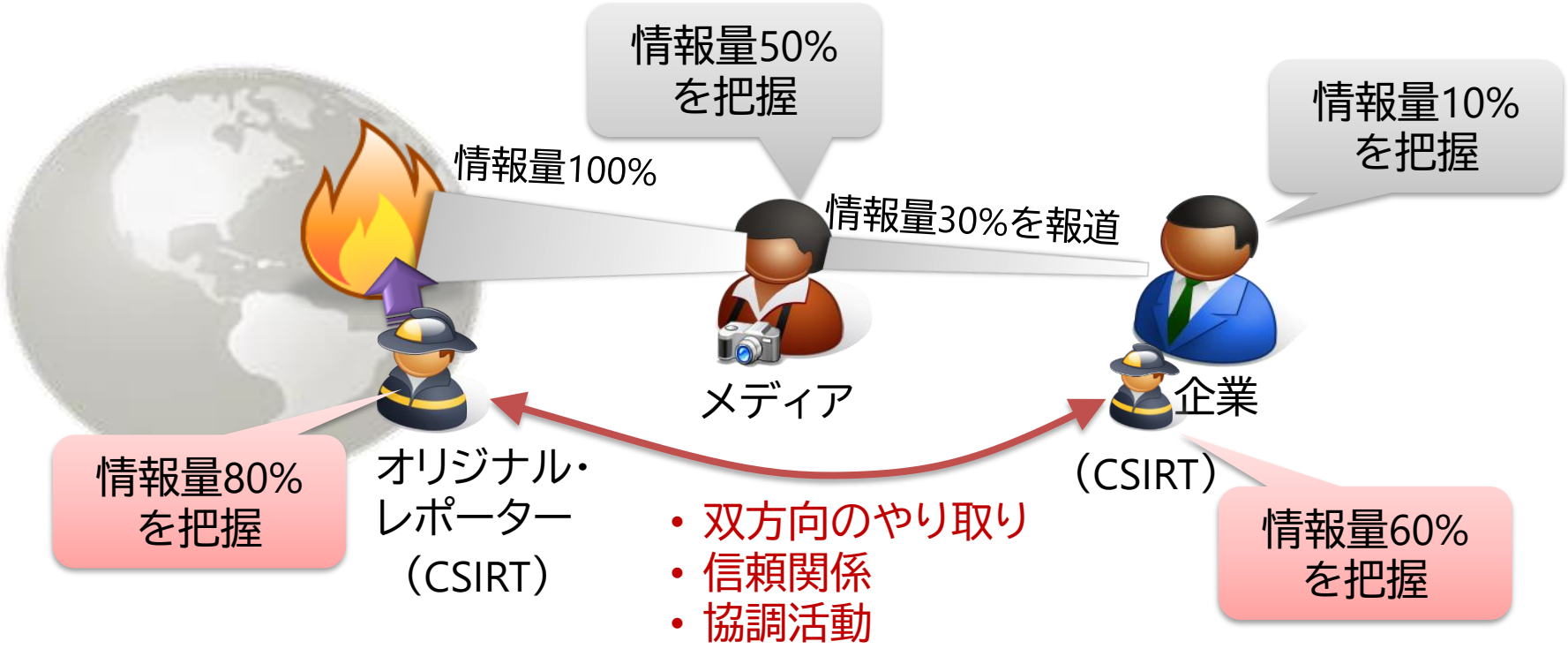
TLP:GREEN

トピック３

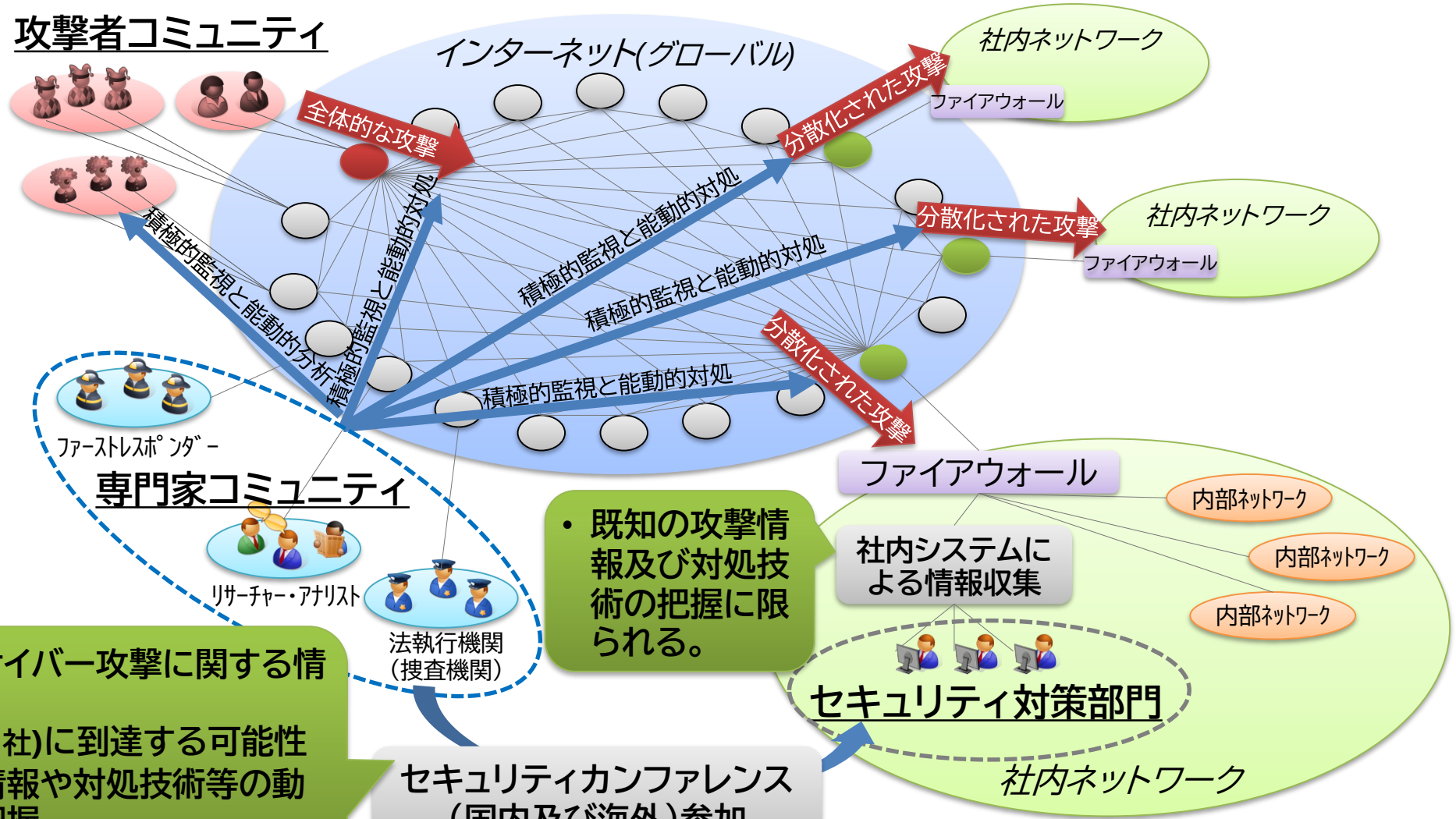
構築した**対処能力の維持・向上**

① サイバー攻撃に関する**正確な事実把握**を行う

- 一般メディア等が発信する情報を鵜呑みにしてはいけない。
- **オジリナル・レポーター(Original Reporter)**が発信する情報を追求する。



② サイバー空間における動向情報を積極的に収集する



- 既知の攻撃情報及び対処技術の把握に限られる。

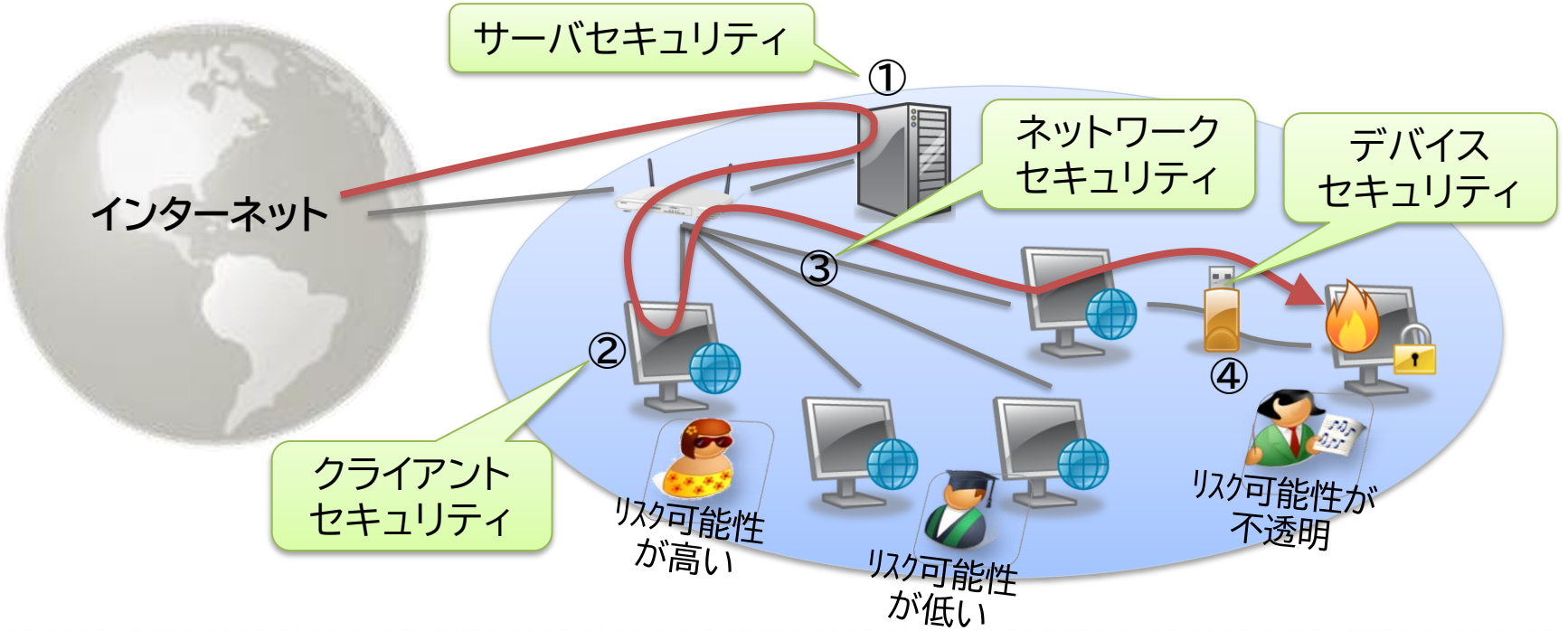
- さまざまなサイバー攻撃に関する情報を収集。
- 今後、日本(自社)に到達する可能性のある攻撃情報や対処技術等の動向を事前に把握。

セキュリティカンファレンス（国内及び海外）参加

TLP:GREEN

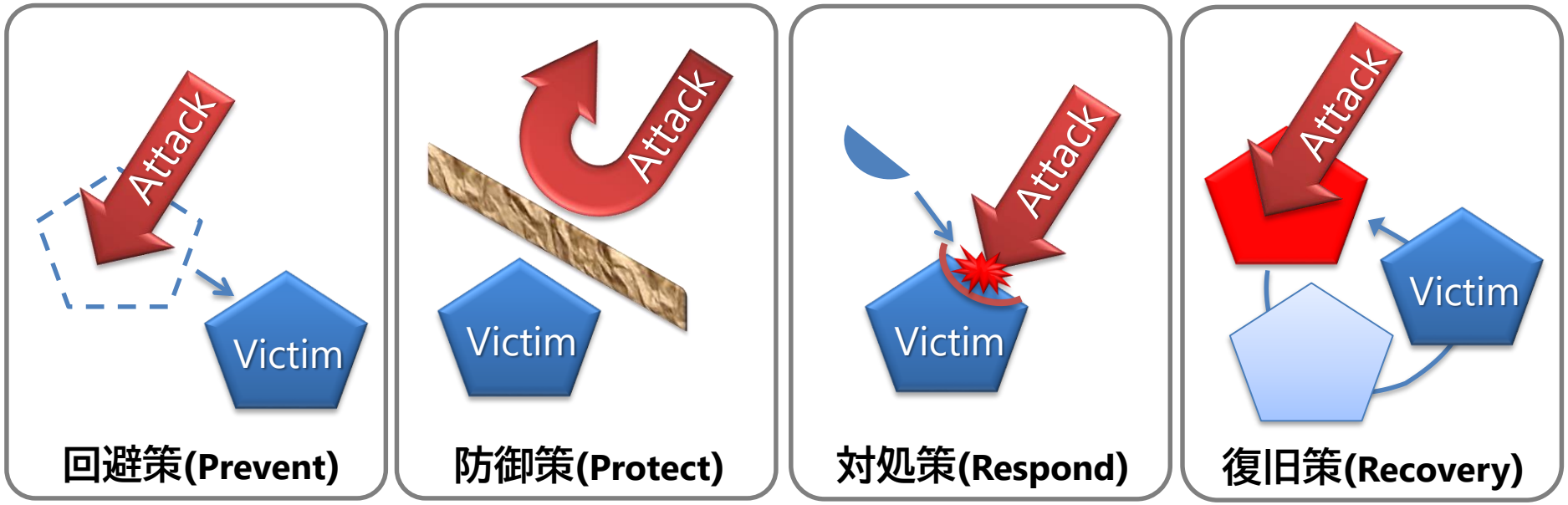
③ 攻撃経路を見出した上で、多層防御を実装する

- ある程度の**攻撃の仕組み**を理解すること
  - サイバー攻撃を「静的な絵」として理解するのではなく、組織全般に渡る＆時間の流れのある「動的ストーリー」として理解することが必要
  - 主要な（攻撃）経路ポイントにおけるセキュリティ対策の要否及びレベルの設定には、業務慣習や部署風土も考慮することが必要



④ すべてのサイバー攻撃対処に**明確な目的を設定**する

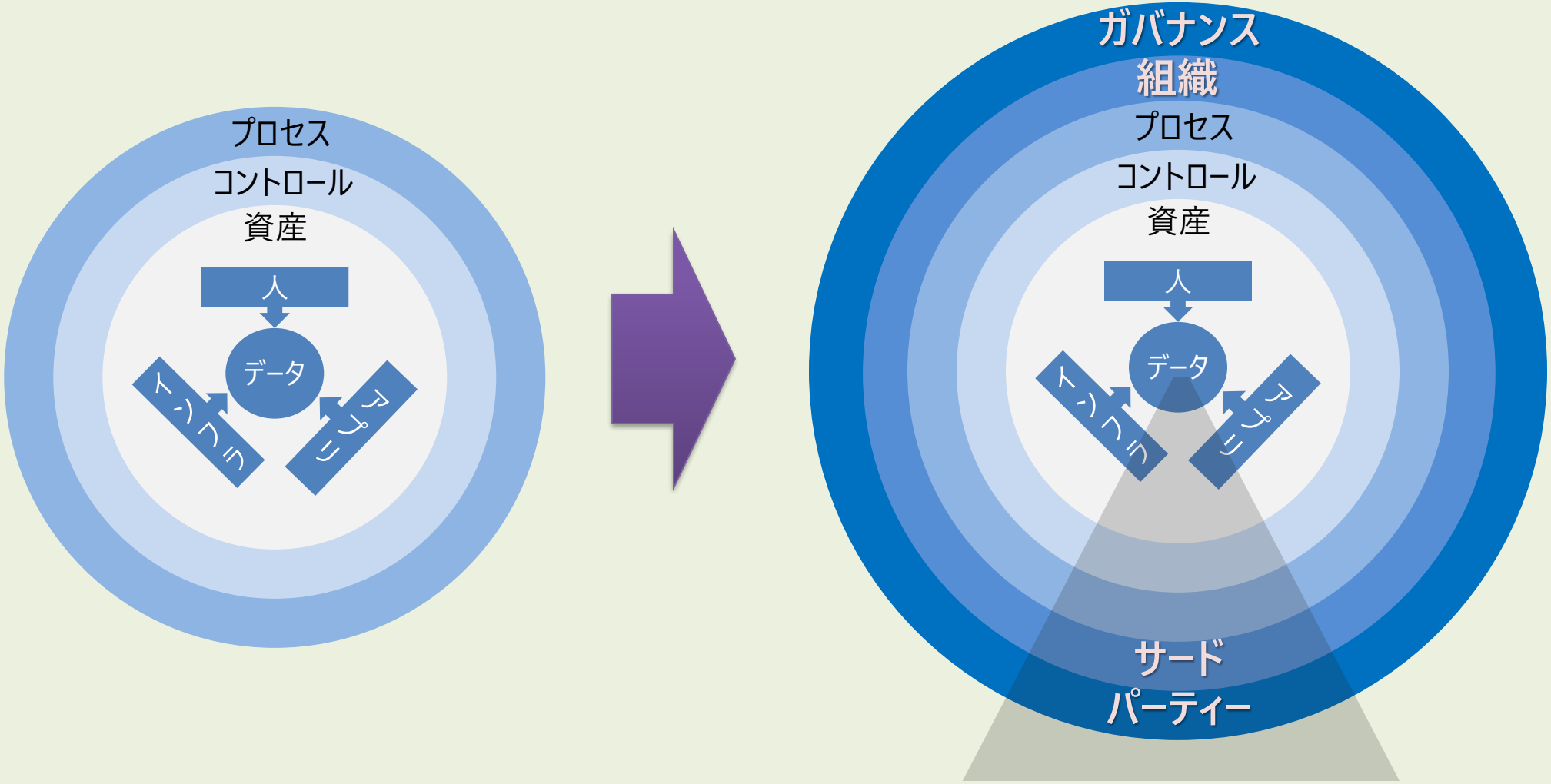
- サイバー脅威に対して、**網羅性の高い対策**を検討し、実装及び確実な運用をすること。
  - 日本国内の対策は、「防御策(Protect)に偏重」しているため、いたずらにコストがかかる。
  - 最近のサイバー防衛策における最善策(Best Practice)は、対処策(Respond)である。
    (最低限のリスクを受容し、実質的な被害を発生させないことで、結果的に有効な防衛策となる。)
  - 基本的な対策コンセプトは、次の4つのとおり。



【参考】組織が実施すべきサイバーリスク・マネジメントのアプローチ

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

【参考】事態対処の能力を維持・向上させるプログラム

オンライン・セミナー

カンファレンス／セミナー

オンライン・コラボレーション

サイバー・レンジ

アナリスト・ミーティング

オンライン・カンファレンス

ミーティング

セキュリティ評価

TLP:GREEN

本資料に関する連絡先

名和 利男（Toshio NAWA）

SITE: https://www.nawa.to

PGP: 0xE38B4E01

TLP:GREEN