サイバーセキュリティ組織体制構築のポイント

～万が一の対応ルール、決めていますか？～

2021年10月15日

あいおいニッセイ同和損害保険株式会社
MS&AD INSURANCE GROUP

MS&ADインターリスク総研株式会社
MS&AD INSURANCE GROUP

本日のアジェンダ

1．サイバーセキュリティ組織の必要性

2．中小企業におけるサイバーリスク対応体制構築のポイント

- 組織体制整備のポイント
- 防御・検知のポイント

3．おわりに

１．サイバーセキュリティ組織の必要性

万が一の対応ルール、決めていますか？__１

202X年XX月XX日

社内に設置したセキュリティ機器に、不審な通信が記録されていました。

- 社内の誰に報告をしますか？
- 報告を受けた方は、誰に何を指示しますか？
- 社内では、何か調査することはありますか？
- 従業員に何かやってもらうことはありますか？
- やってはいけないことはありますか？
- 取引先に連絡しますか？
- 警察への届出はしますか？
- その他、外部の機関に相談・連絡することはありますか？

万が一の対応ルール、決めていますか？＿2

202X年XX月XX日

調査の結果、少なくとも5台のPCがウィルスに感染、情報が外部に流出した恐れがあることが判明した。

- 社内のインターネットを切断しますか？
- 外部との電子メールのやり取りを停止しますか？
- ウィルスに感染したのは本当に5台のPCだけですか？
- このまま業務を続けるか、止めるかを判断する基準はありますか？
- 被害者にはどのようにお詫びをしますか？
- 取引先には連絡しますか？
- 警察への届出はしますか？
- その他、外部の機関に連絡することはありますか？

- 専門の組織が必要

  サイバー攻撃の手法は高度化・多様化され、対応には高い専門性が必要。既存の単独部署での対応は困難。

  ⇒専門の対応組織を（少人数でも）整備する

- 社内外の関係者とのコミュニケーションが必要

  攻撃を受けた結果、ビジネスに大きな影響を受けることも。もはや「現場の頑張り」では対処できない。

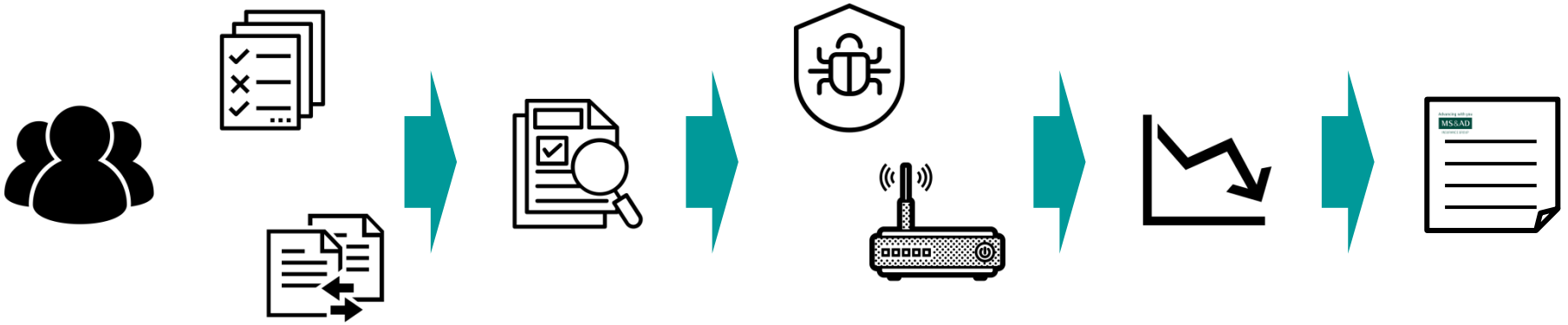
  ⇒経営（有時は緊急対策本部）、社内関係部署、外部の専門機関とのホットライン構築は必須。

２．中小企業におけるサイバーリスク対応体制構築のポイント

サイバーリスク対応体制整備の全体像

Advancing with you
MS&AD
INSURANCE GROUP

組織体制整備 → リスクの特定 → 防御・検知 → 対応・復旧 → 保険



＜組織体制整備＞	＜規程整備＞ ＜情報収集＞	＜リスクアセスメント＞	＜防御・対策＞	＜リスク低減＞	＜保険付保＞
サイバー攻撃の手口やサイバー事故事例を理解し、どのような被害があるのかを理解する。 CISOやCSIRTなどの専管組織を（少人数でも）整備する。	専管組織ができることで、規程やガイドラインが整備され、情報収集のため、外部（IPAやJNSA、CSERT協議会等）機関と接点を持つ。	①リスク分析、②リスク特定、③リスク評価を実施する。 重要で緊急性の高い課題の洗い出しとそれ以外のリスクの整理を目的とする。	リスクアセスメントの結果から、特に重要な課題・脆弱性への対応等を実施する。 ⇒ 自動化し、証跡が残る体制を構築することが重要。 そういった対応が出来ない部分については、規程やマニュアルで対応することになる。	自動化した部分については大きくリスクが逓減するが、規程やマニュアルにて対応する部分については属人的なリスクが残ることを理解する。	各種対策により低減したリスクと残ったリスクを整理し、低減できない（低減しきれない）残存リスクに対して適切な保険を手配することで、リスクヘッジを完結させる。

組織体制整備のポイント

サイバーセキュリティ組織体制__実施すべき事項

組織体制整備 → リスクアセスメント → 防御・対策 → 保険

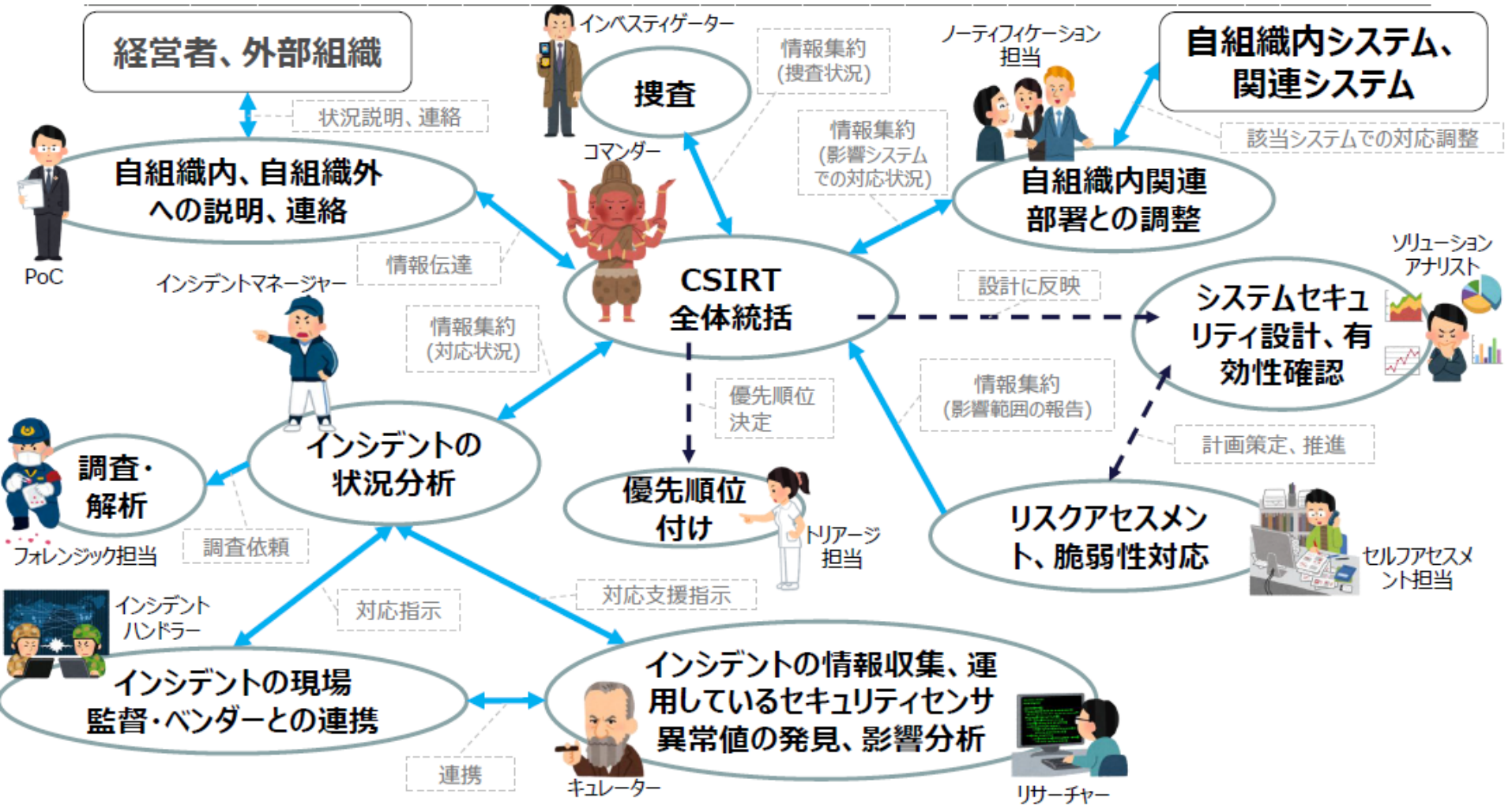
平常時に実施すべき事項	緊急時に実施すべき事項
対応方針策定	調査・状況把握/情報集約
予算・人材の確保	影響範囲把握/情報集約
対策検討・実行	優先順位決定
対策の見直し	対応指示・依頼
緊急時体制整備	経営への状況説明
外部委託先管理	外部機関への説明・連絡
最新動向の収集	

サイバーセキュリティ組織体制__実施すべき事項

組織体制整備 → リスクアセスメント → 防御・対策 → 保険

平常時に実施すべき事項	緊急時に実施すべき事項
対応方針策定	調査・状況把握/情報集約
予算・人材の確保	影響範囲把握/情報集約
対策検討・実行	優先順位決定
対策の見直し	対応指示・依頼
緊急時体制整備	経営への状況説明
外部委託先管理	外部機関への説明・連絡
最新動向の収集	

緊急時対応体制と業務内容の関連図



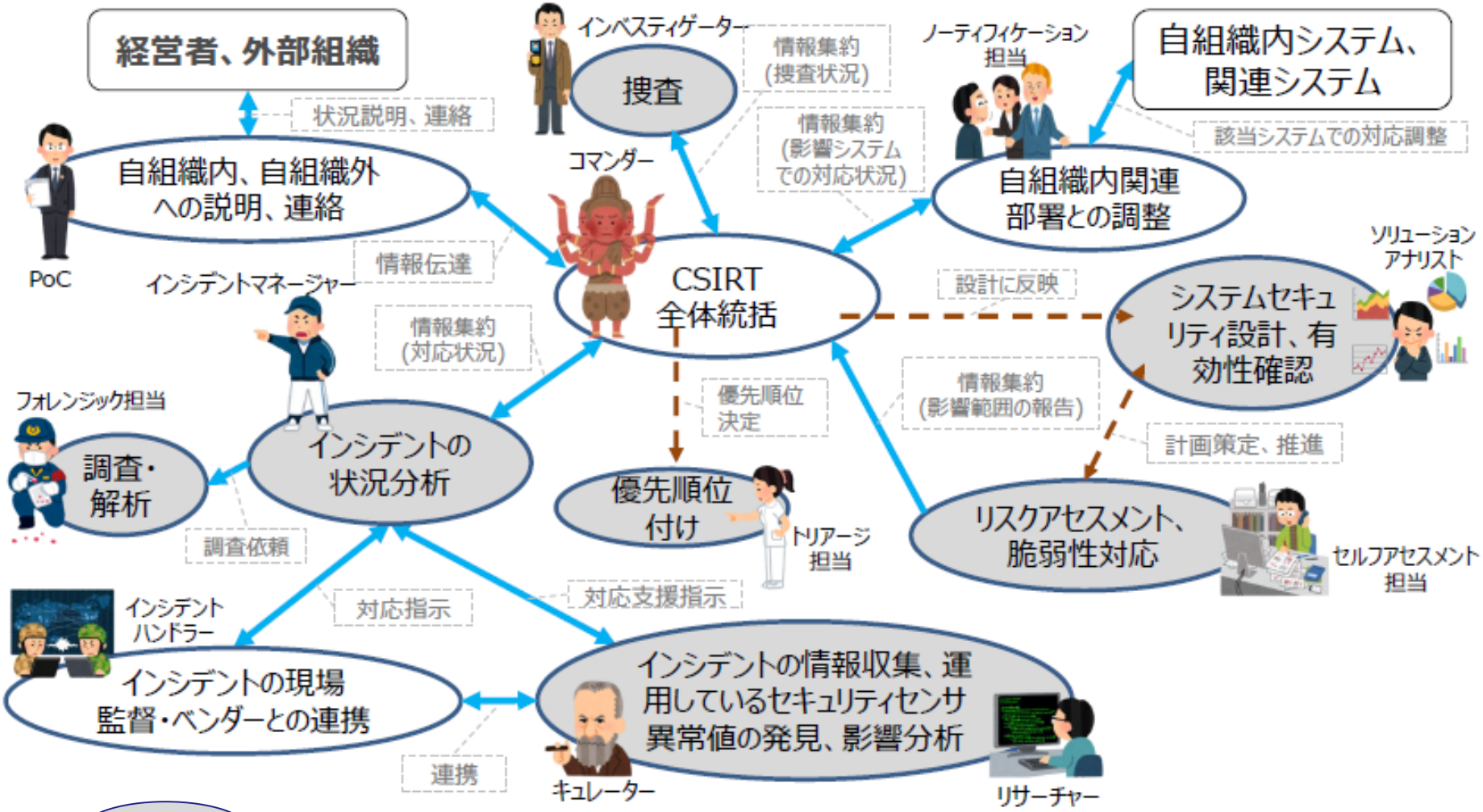
出典：日本シーサート協議会　CSIRT人材の定義と確保Ver.1.5

そんなに**ヒト**も**カネ**もかけられない…。

Advancing with you
MS&AD
INSURANCE GROUP

自衛消防隊レベルにすると・・(インシデント対応時)

実線は活動時の情報の流れ。
点線は必要時に実施する活動の流れ。



は、アウトソースが可能

□自社で対応する業務選定のポイント

- 自社で対応する役割の兼務は可。

  （例）全体統括＋トリアージ＋経営への報告・説明＋社内調整＋外部連絡

- どうしても要員がいない場合は、**守るべき領域の極小化**を検討。
  - ➢ 不要なデータは捨てる
  - ➢ 機密情報を保持するシステムをインターネットから切り離す

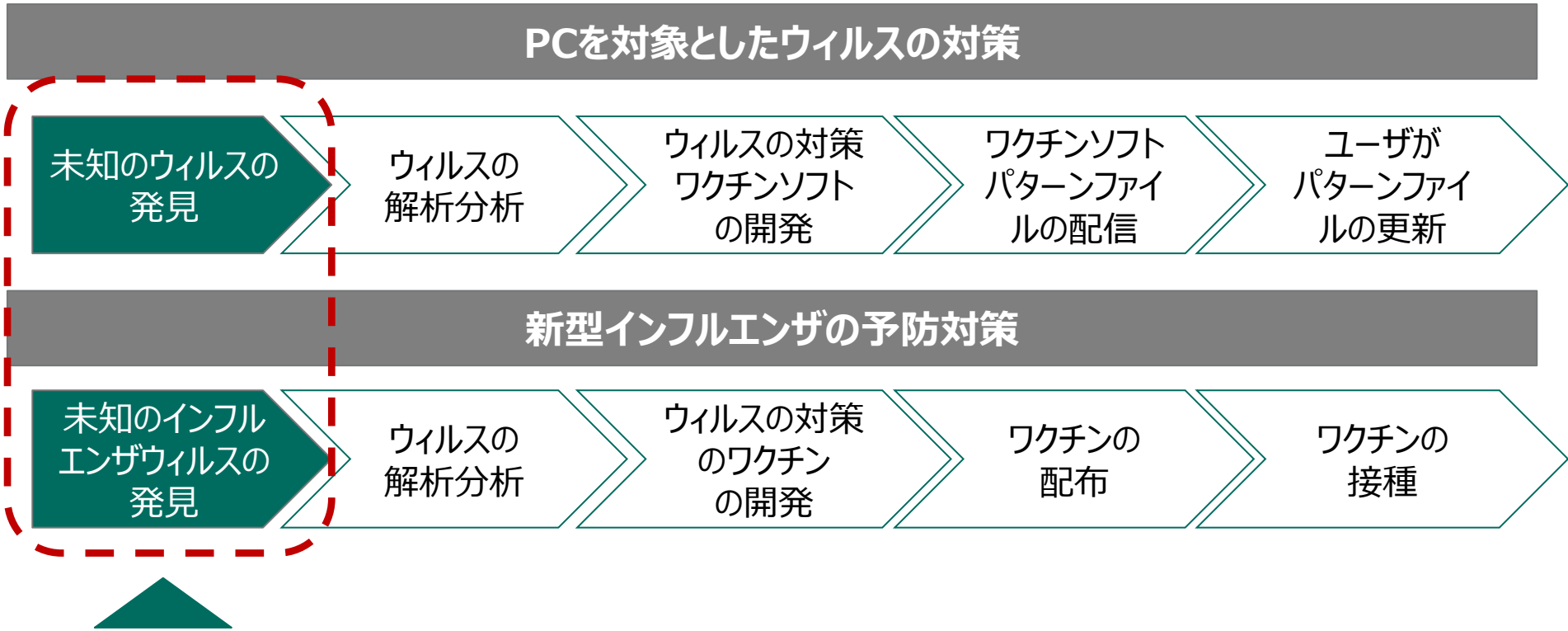
  など

□アウトソースする業務選定のポイント

- 情報の収集や高度な専門性が必要な役割に関してはアウトソースを検討。
  - ➢ 流行しているマルウェアの種類や特徴や、有効なインシデント対応の手法　など
- 社外組織との連携は一朝一夕にできるものではなく、インシデント発生前からのパイプ作りが重要。

防御・検知のポイント

防御の限界：一般的なマルウェア（ウィルス）対策ソフトの例



発見されたウィルスへの対策
対処療法的なアプローチ

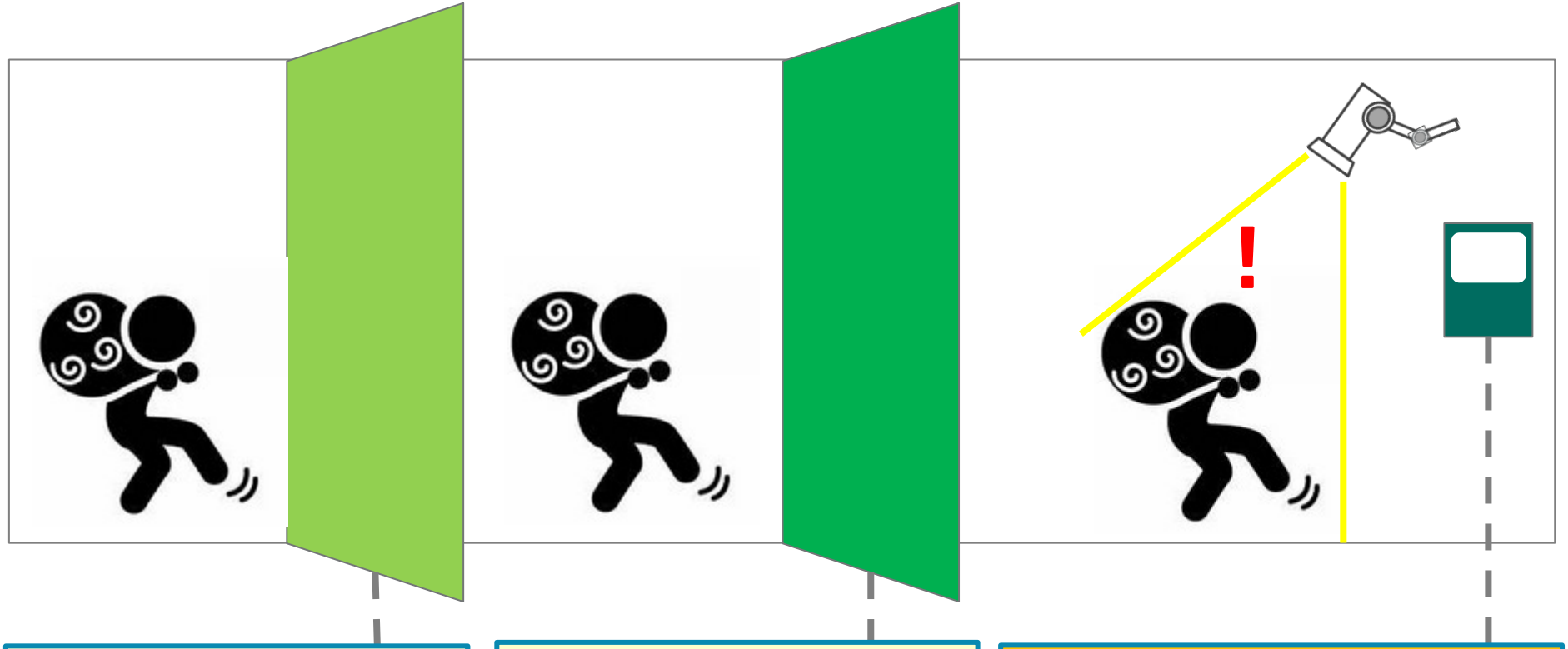
つまり・・・

未知のウィルスの発見がないと、
その対策を打つことができない

※「振る舞い検知」型やAI(人工知能）利用型など、次世代型といわれるウィルス対策ソフトも近年出ているが、攻撃者側も進化していくことが予想されるため、技術的対策の有効性が高まるとは断言できない

「多層防衛」とは（マンションに例えると）

住居のセキュリティと同じで、オートロック、住戸の施錠、ホームセキュリティのように複数対策しておくと安心

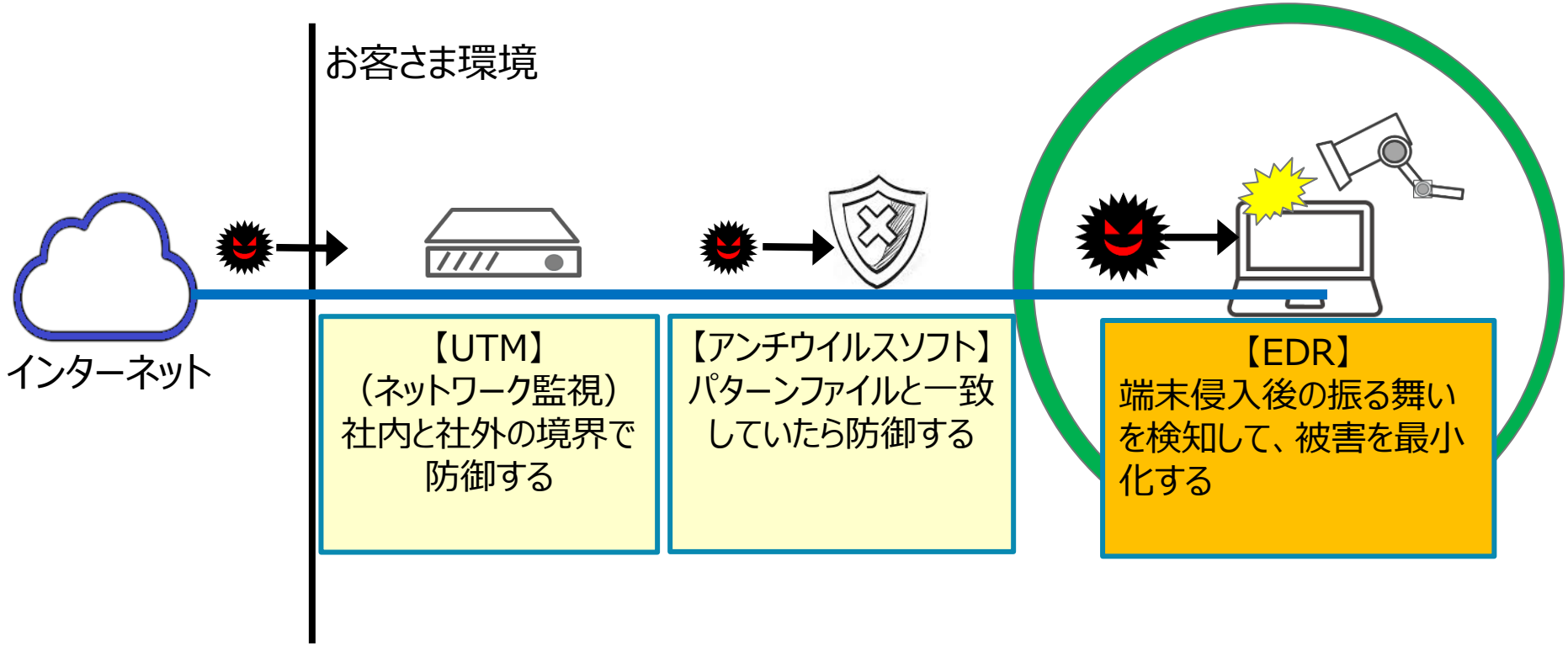


【UTMの例え】
マンション入口のオートロック
（建物への侵入を防御）

【アンチウイルスソフトの例え】
住戸の施錠
（各戸への侵入を防御）

【EDRの例え】
ホームセキュリティ
（住戸内の異常検知と見守り）

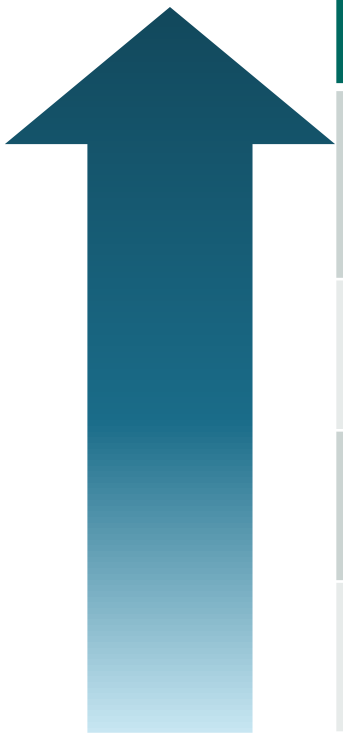
UTM、アンチウイルスソフトとEDRそれぞれの守備範囲・強みがあり、3つを組み合わせる対策（多層防御）が推奨されます。



Advancing with you
MS&AD
INSURANCE GROUP

セキュリティ製品を導入するだけではなく、自社のレベルに合わせた運用を行い、検知結果を人間の目で仕分け、インシデント発生時に適切な初動対応を行うことが重要

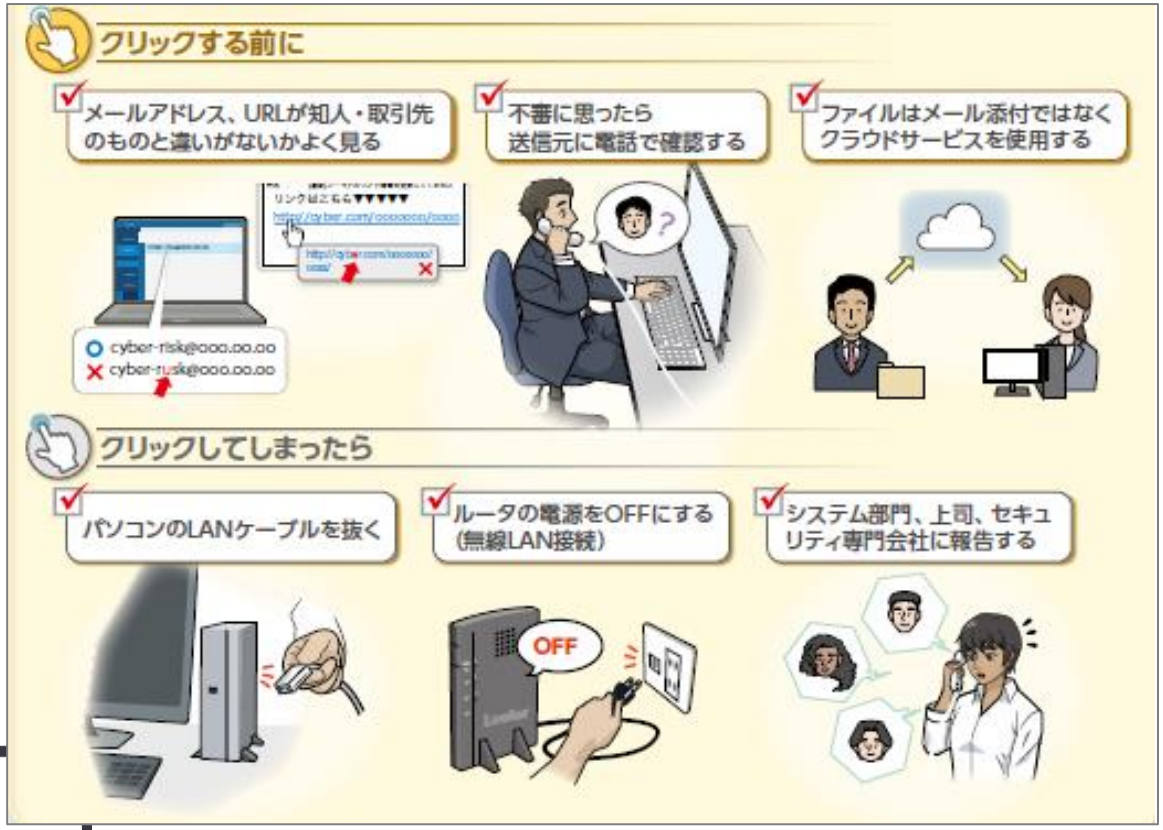
【セキュリティ製品の運用レベルの例】



	運用レベル	アクション
レベル３	**常時監視**	日々の運用を監視し、設定を見直す。 インシデント発生時はレスキュー対応を実施する。
レベル２	**ルールによる脅威の検知**	自社に合わせたルールを設定し、インシデント発生時や他部署の要請で検知結果を解析する
レベル１	**導入しただけ**	導入時の設定から見直していないため、過検知や誤検知、検知漏れが発生する
レベル０	**導入していない**	セキュリティ対策に穴がある

最後は「ヒト」が被害を防ぐ

- **策定したルールを役職員へ周知し、ルールに沿った行動を取ることを促す**
- **緊急時（サイバー攻撃を検知した場合等）の通報手順の周知は必須**
- **緊急時対応トレーニングを実施、課題を洗い出し、解消することも有効**



※システム環境に応じた対応を規定しておく必要があります

３．おわりに

■ **サイバー攻撃にあうことを前提とした組織体制の整備が必要**

- 予防に傾注した対策だけでは被害の回避は不可能

■ **サイバーリスクを認識し、平常時／緊急時の体制を構築する**

- 万が一の対応だけではなく、自社のサイバー攻撃への対応方針を社内外に明示する

■ **まずはできることからはじめてみよう**

- 自社でできることを整理し、難しいことは外部へのアウトソースを検討する

■ **練習で出来ないことは、本番でも出来ない**

- 緊急時に迅速かつ適切に動けるように、平常時より教育・トレーニングしておく

ご清聴ありがとうございました

MS&AD

MS&ADインシュアランス グループ

ＭＳ＆ＡＤインターリスク総研株式会社

〒101-0062　東京都千代田区神田淡路町2-105ワテラスアネックス

http://www.irric.co.jp

参考資料

『中小企業の情報セキュリティ対策ガイドライン第３版』（2019年3月　独立行政法人情報処理推進機構）

情報を安全に管理することの重要性

- 情報セキュリティ対策は、経営に大きな影響を与えます！
- 対策の不備により経営者が法的・道義的責任を問われます！
- 組織として対策するために、担当者への指示が必要です！

中小企業の情報セキュリティ対策ガイドライン

■経営者が認識すべき「３原則」

■実行すべき「重要７項目の取組」

出典：「中小企業の情報セキュリティ対策ガイドライン第3版」2019年3月19日公開（独立行政法人情報処理推進機構）

【参考資料】中小企業の情報セキュリティ対策ガイドライン

Advancing with you
MS&AD
INSURANCE GROUP

経営者が認識すべき「３原則」

原則１　情報セキュリティ対策は**経営者のリーダーシップ**で進める

原則２　**委託先の情報セキュリティ対策**まで考慮する

原則３　関係者とは常に情報セキュリティに関する**コミュニケーション**をとる

実行すべき「重要７項目の取組」

取組１　情報セキュリティに関する**組織全体の対応方針**を定める	取組５　**緊急時の対応**や**復旧のための体制**を整備する
取組２　情報セキュリティ対策のための**予算や人材**などを確保する	取組６　**委託や外部サービス利用**の際にはセキュリティに関する**責任を明確**にする
取組３　必要と考えられる**対策を検討**させて**実行を指示**する	取組７　情報セキュリティに関する**最新動向**を収集する
取組４　情報セキュリティ対策に関する**適宜の見直し**を指示する	

出典：「中小企業の情報セキュリティ対策ガイドライン第3版」2019年3月19日公開（独立行政法人情報処理推進機構）

【参考】セキュリティ対策自己宣言「SECURITY ACTION」

- 情報処理推進機構が運営する、中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度。
- 自己宣言を行ったうえで申し込むと、制度のロゴマークを使用できる等のメリットを享受できる。

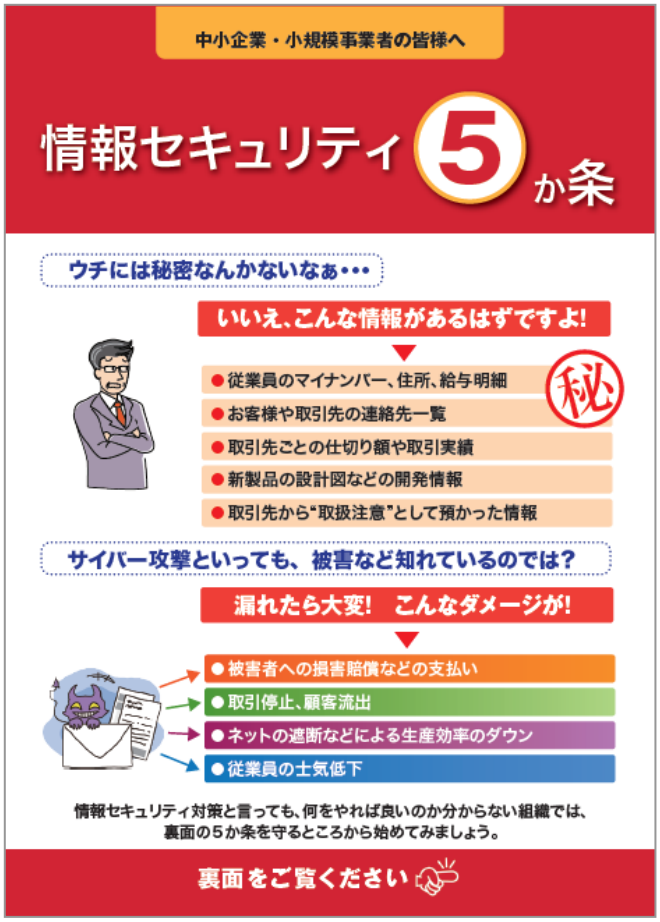
取り組み目標を決める → 自己宣言する → ステップアップする

【参考】★一つ星__情報セキュリティ5か条

Advancing with you
MS&AD
INSURANCE GROUP

取り組み目標を決める → 自己宣言する → ステップアップする

★一つ星
「情報セキュリティ５か条」（「中小企業の情報セキュリティ対策ガイドライン」（以下「ガイドライン」付録１）に取組むことを宣言する



1 OSやソフトウェアは常に最新の状態にしよう！

2 ウイルス対策ソフトを導入しよう！

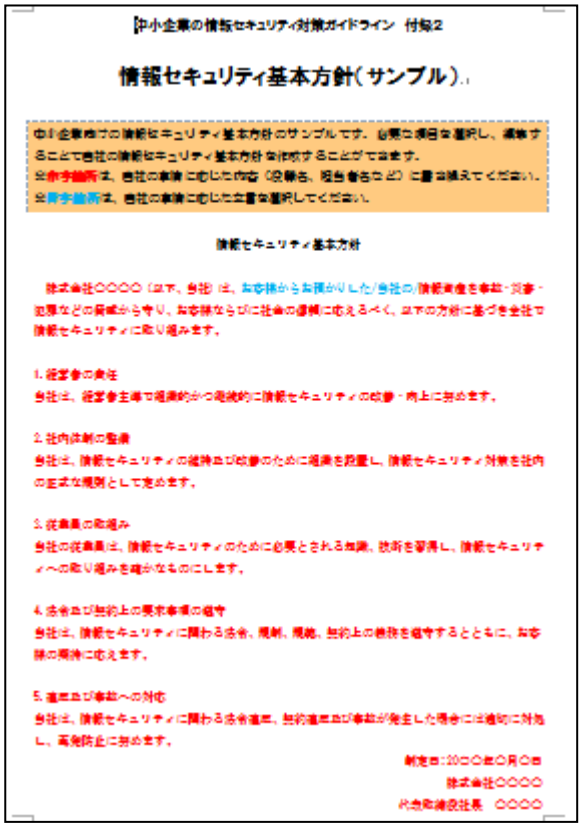
3 パスワードを強化しよう！

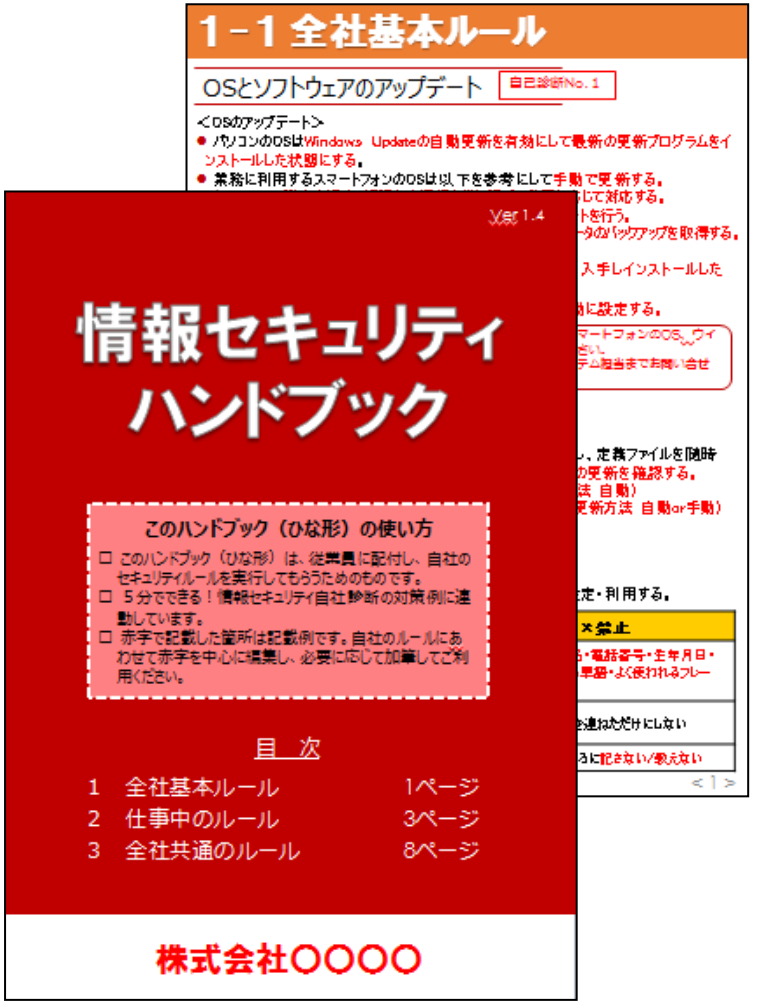
4 共有設定を見直そう！

5 脅威や攻撃の手口を知ろう！

【参考】中小企業の情報セキュリティ対策ガイドライン

- ガイドライン 付録として各種様式、ツール類のひな形も収録。
  https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html

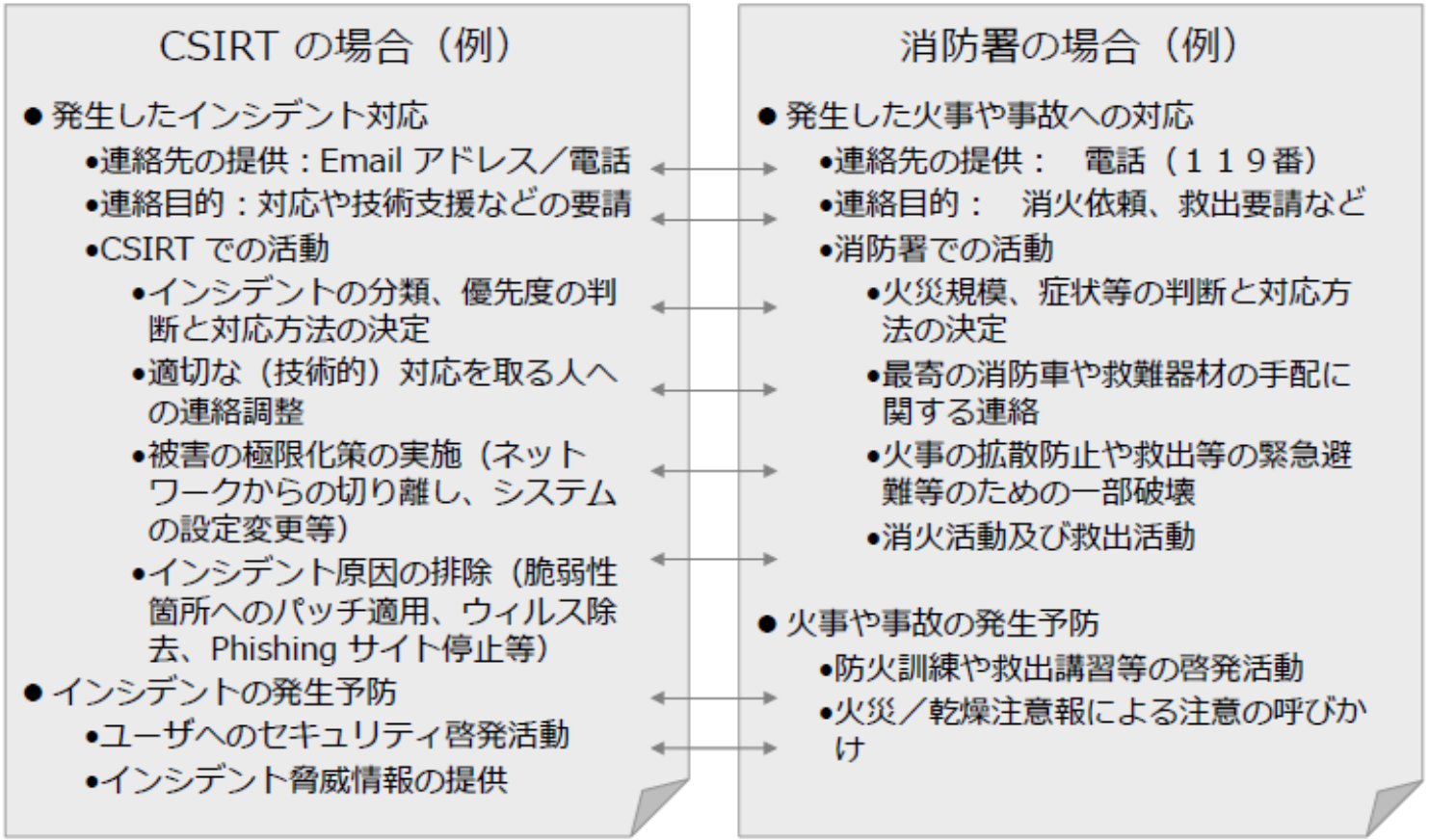




CSIRTと消防署の役割比較例

CSIRTのイメージは、たとえば火事に対する「消防署」と位置付けられます。

CSIRT立ち上げ時には、まず自衛消防隊レベルを目指しましょう。



出典：組織内CSIRTの役割とその範囲（JPCERT/CC）

【参考】CSIRTと自衛消防隊の役割対比__地区隊長

CSIRTの場合

コマンダー

自組織で起きているセキュリティインシデントの全体統制を行う。
重大なインシデントに関してはCISOや経営層との情報連携を行う。
また、CISOや経営者が意思決定する際の支援を行う。

自衛消防隊の場合

地区隊長

【火災発生時】
初動措置の指揮をとるとともに本部への報告連絡を行う

【警戒宣言発令時】
本部への状況の報告連絡を行う

【参考】CSIRTと自衛消防隊の役割対比__情報連絡

Advancing with you
MS&AD
INSURANCE GROUP

CSIRTの場合

PoC

社外窓口として、JPCERT/CC、NISC、警察、監督官庁、NCA、他CSIRT等との連絡窓口となり、情報連携を行う。
社内窓口として、IT部門、法務、渉外、IT部門、広報、各事業部等との連絡窓口となり、情報連携を行う。

リサーチャー

アウトソース

セキュリティイベント、脅威情報、脆弱性情報、攻撃者のプロファイル情報、国際情勢の把握、メディア情報などを収集し、キュレーターに引き渡す。

自衛消防隊の場合

情報連絡班

【火災発生時】
防災センターへの連絡、近隣への連絡
被害状況の連絡

【警戒宣言発令時】
テレビ、ラジオ等による情報収集

【参考】CSIRTと自衛消防隊の役割対比__初期消火・避難誘導

CSIRTの場合

インシデントハンドラー

手におえない場合はアウトソース

インシデントの処理を行う。
セキュリティベンダーに処理を委託している場合には指示を出して連携し、管理を行う。
状況はインシデントマネージャーに報告する。

ノーティフィケーション

自組織内を調整し、各関連部署への情報発信を行う。
自組織システムに影響を及ぼす場合にはIT部門と調整を行う。

自衛消防隊の場合

初期消火班

【火災発生時】
初期消火、消火状況の報告

避難誘導班

【火災発生時】
避難誘導、避難人数の確認、避難者の人数、異常の有無を報告

【警戒宣言発令時】
転落、落下防止措置を行う
混乱防止を目的とした事前の避難誘導を行う

【参考】CSIRTと自衛消防隊の役割対比__応急対応

CSIRTの場合

インシデントハンドラー

手におえない場合は アウトソース

インシデントの処理を行う。
セキュリティベンダーに処理を委託している場合には指示を出して連携し、管理を行う。
状況はインシデントマネージャーに報告する。

ソリューションアナリスト

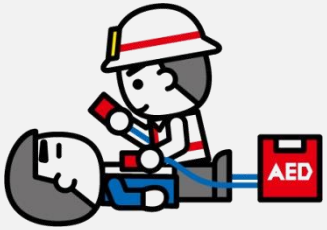
緊急時は アウトソース

自組織の事業計画に合わせてセキュリティ戦略を策定する。
現在の状況とあるべき姿のFit&Gap分析からリスク評価を行い、ソリューションマップを作成して導入を推進する。

自衛消防隊の場合

応急対応班

【火災発生時】
応急措置の実施
負傷者の状態、名前を報告



【警戒宣言発令時】
救護用品の確認を行う

【参考】CSIRTと自衛消防隊の役割対比__安全防護

CSIRTの場合

インシデントハンドラー

手におえない場合はアウトソース

インシデントの処理を行う。
セキュリティベンダーに処理を委託している場合には指示を出して連携し、管理を行う。
状況はインシデントマネージャーに報告する。

脆弱性診断士

アウトソース

OS、ネットワーク、ミドルウェア、アプリケーションが安全かどうかの検査を行い、診断結果の評価を行う。

自衛消防隊の場合

安全防護班

【火災発生時】
ガス、電気を止め、防火扉を閉める
避難経路を確保する

【警戒宣言発令時】
転落、落下防止措置を行う

【参考】CSIRTと自衛消防隊の役割対比__搬出

CSIRTの場合

フォレンジックス

アウトソース

システム的な鑑識、精密検査、解析、報告を行う。
悪意のある者は証拠隠滅を図ることもあるため、証拠保全とともに、消されたデータを復活させ、足跡を追跡することも要求される。

セルフアセスメント

緊急時はアウトソース

自組織環境や情報資産の現状分析を行う。
平常時の際にアセスメントを実施しておき、インシデント発生時にはアセスメント結果に基づいて影響範囲を特定する。

自衛消防隊の場合

搬出班

【火災発生時】
重要な物品の持ち出し、保護を行う
持ち出し物の掌握、管理を行う

【警戒宣言発令時】
非常持ち出し品の整理と確認を行う