Advancing with you
MS&AD
INSURANCE GROUP

サイバーセキュリティ
組織体制構築のポイント

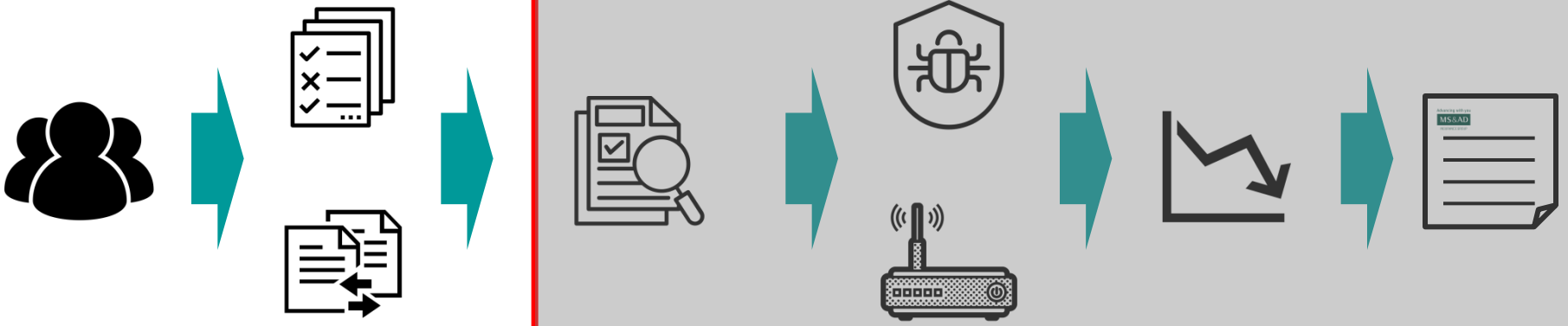
MS&ADインターリスク総研株式会社
MS&AD INSURANCE GROUP

2019年8月28日･29日
サイバーリスク室　岡田　智之

本日の解説箇所

Advancing with you
MS&AD
INSURANCE GROUP

組織体制整備 | リスクアセスメント | 防御・対策 | 保険



＜組織体制整備＞

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。

また、どんな組織であっても狙われるリスク（理由）があり得ることを理解する。

＜規定整備＞
＜情報収集＞

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、規定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。

＜リスクアセスメント＞

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。

＜防御・対策＞

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、規定やマニュアルで対応することになる。

＜リスク低減＞

自動化した部分については大きくリスクが逓減するが、規定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。
（たとえばUSBの使用ルールや外部サイトの閲覧ルールなど）

＜保険付保＞

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。

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. 平常時におけるサイバーセキュリティ組織体制

3. 緊急時におけるサイバーリスク対応体制

4. まとめにかえて

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について
サイバーセキュリティに関する主な用語説明

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

2019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？

2019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？

Advancing with you
MS&AD
INSURANCE GROUP

**「サイバー攻撃は排除できない。
サイバーリスクの管理をするべきである」**

米国国家情報局　グローバル脅威報告書
2015年2月

「不審メールの開封を完全に防ぐことを目標とする対策は現実的ではなく、メール開封（少なくとも端緒の端末１台は感染すること）を前提とした対策が必要である」

内閣サイバーセキュリティセンター
日本年金機構における個人情報流出事案に関する原因究明調査結果
2015年8月

２．平常時におけるサイバーセキュリティ管理体制

サイバーセキュリティ組織体制__平常時

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	

サイバー攻撃リスクの経営上の重要性を認識し、自社のサイバー攻撃への対応方針を社内外に明示する

- サイバー攻撃リスクの重要性と自社としての対応方針を社内外に明示することが肝要
  - 「情報セキュリティ基本方針」を策定する　等

＜イメージ＞

1. 当社は、お客様またはお取引先から提供を受けた情報を適切に取り扱い、当該個人および組織の権利および利益を保護する。
2. 当社は、営業秘密、技術情報その他の価値ある情報を適切に取り扱い、権利および利益を保護する。
3. ・・・省略・・・

- 「中小企業の情報セキュリティ対策ガイドライン」付録２「情報セキュリティ基本方針」のサンプルを活用すれば円滑な策定が可能

ルール・運用体制の整備と徹底

- 基本方針に基づいて**関連するルール**（情報管理規程等）を整備する
- 策定したルール（情報セキュリティポリシー、情報管理規程等）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

- サイバー攻撃に関するリスク対策を立案・推進する**責任者を明確化**する
- また、専任組織または担当者の設置を検討する

- あわせて、**緊急時（サイバー攻撃を検知した場合等）の通報手順**も整備

※「中小企業の情報セキュリティ対策ガイドライン」付録５「情報セキュリティ関連規程（サンプル）」を活用

- 緊急時の通報手順は、平時から訓練を通じて手順を浸透させる

【参考】セキュリティ対策自己宣言「SECURITY ACTION」

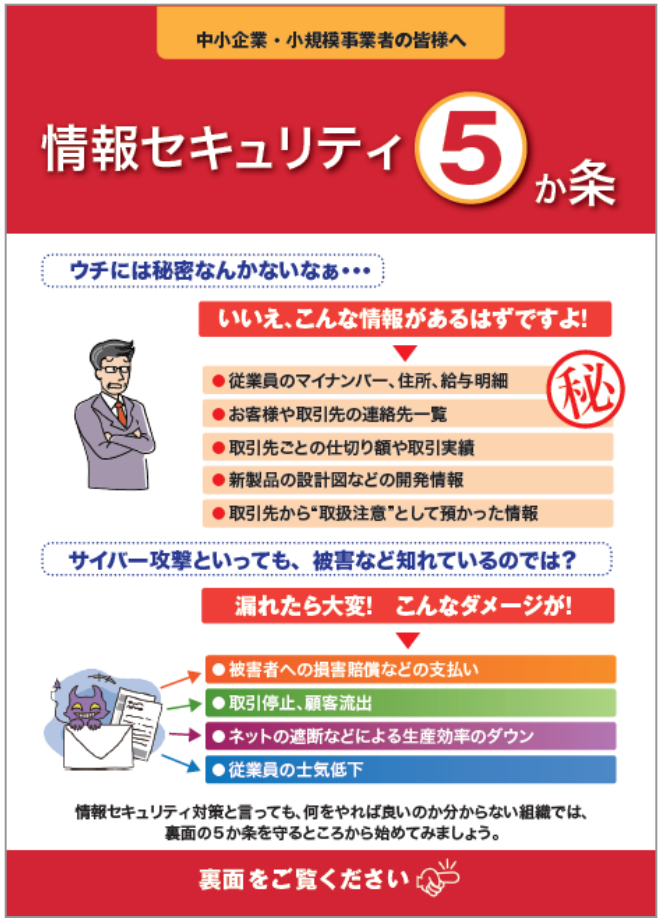
- 情報処理推進機構が運営する、中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度。
- 自己宣言を行ったうえで申し込むと、制度のロゴマークを使用できる等のメリットを享受できる。

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

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



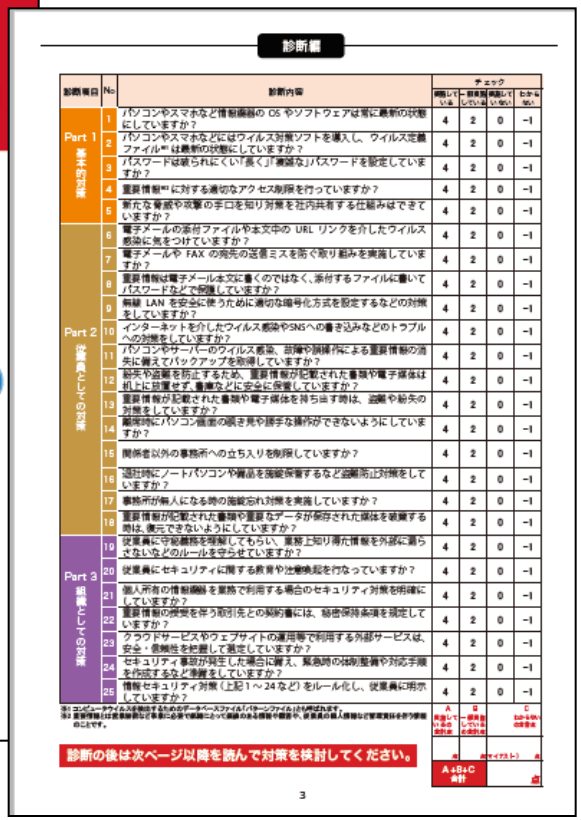
1. OSやソフトウェアは常に最新の状態にしよう！
2. ウイルス対策ソフトを導入しよう！
3. パスワードを強化しよう！
4. 共有設定を見直そう！
5. 脅威や攻撃の手口を知ろう！

【参考】★★二つ星__5分でできる！情報セキュリティ自社診断

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

★★二つ星
「５分でできる！情報セキュリティ自社診断」（「ガイドライン」付録３）で自社の状況を把握したうえで、「情報セキュリティポリシー（基本方針）」（「ガイドライン」付録２）を定め、外部に公開したことを宣言

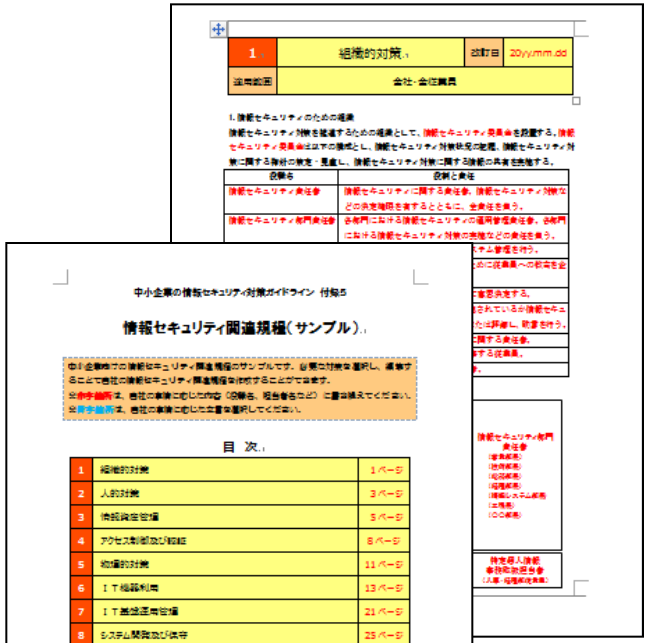

診断書

診断項目	No	診断内容	チェック			
			実施している	実施していない	わからない	
Part 1 基本的対策	1	パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？	4	2	0	-1
	2	パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル※1 は最新の状態にしていますか？	4	2	0	-1
	3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？	4	2	0	-1
	4	重要情報※2 に対する適切なアクセス制限を行っていますか？	4	2	0	-1
	5	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？	4	2	0	-1
Part 2 従業員としての対策	6	電子メールの添付ファイルや本文中の URL リンクを介したウイルス感染に気をつけていますか？	4	2	0	-1
	7	電子メールや FAX の宛先の送信ミスを防ぐ取り組みを実施していますか？	4	2	0	-1
	8	重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？	4	2	0	-1
	9	無線 LAN を安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？	4	2	0	-1
	10	インターネットを介したウイルス感染やSNSへの書き込みなどのトラブルへの対策をしていますか？	4	2	0	-1
	11	パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？	4	2	0	-1
	12	紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管していますか？	4	2	0	-1
	13	重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？	4	2	0	-1
	14	離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？	4	2	0	-1
	15	関係者以外の事務所への立ち入りを制限していますか？	4	2	0	-1
	16	退社時にノートパソコンや書類を施錠保管するなど盗難防止対策をしていますか？	4	2	0	-1
	17	事務所が倒壊等の被災時の業務継続対策を実施していますか？	4	2	0	-1
	18	重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？	4	2	0	-1
Part 3 組織としての対策	19	従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？	4	2	0	-1
	20	従業員にセキュリティに関する教育や注意喚起を行なっていますか？	4	2	0	-1
	21	個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？	4	2	0	-1
	22	重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？	4	2	0	-1
	23	クラウドサービスやウェブサイトの運用等で利用する外部サービスは、安全・信頼性を確認して選定していますか？	4	2	0	-1
	24	セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？	4	2	0	-1
	25	情報セキュリティ対策（上記１～24など）をルール化し、従業員に明示していますか？	4	2	0	-1
			A	B	C	
			対策レベル○の合計点	対策レベル△の合計点	対策レベル×の合計点	
			点	点（マイナス）	点	
			A+B+C 合計	点		

※1 コンピュータウイルスを検出するためのデータベースファイル（パターンファイル）とも呼ばれます。
※2 重要情報とは営業秘密など事業に必要で価値のある情報や顧客や、従業員の個人情報など管理責任を負う情報のことです。

診断の後は次ページ以降を読んで対策を検討してください。

3


中小企業の情報セキュリティ対策ガイドライン 付録5
情報セキュリティ関連規程（サンプル）

目 次

３．緊急時におけるサイバーリスク対応体制

サイバーセキュリティ組織体制__平常時

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	

緊急時のサイバーリスク対応体制__CSIRT

Advancing with you
MS&AD
INSURANCE GROUP

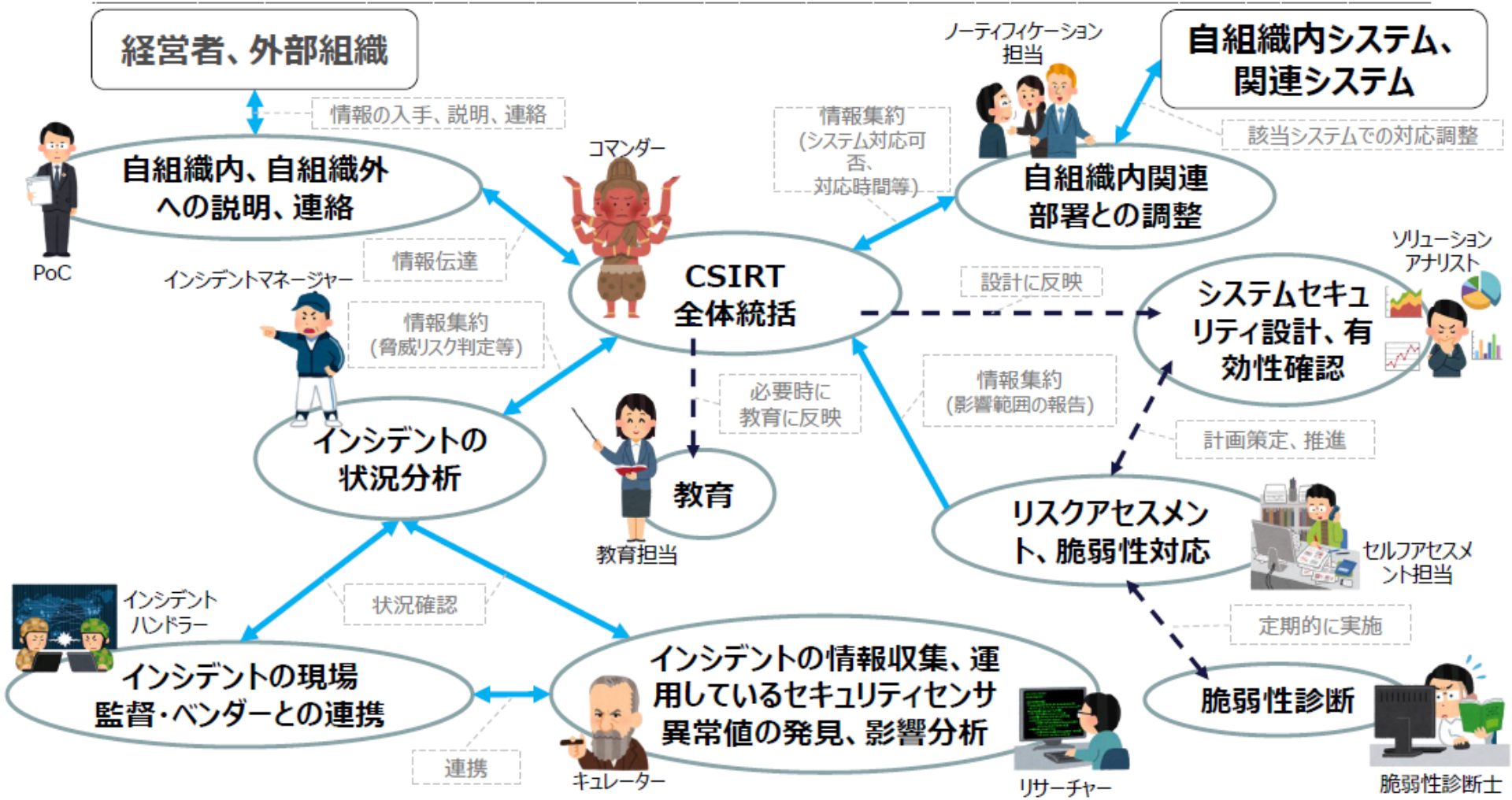
シーサート
CSIRT＝**C**omputer **S**ecurity **I**ncident **R**esponse **T**eam

サイバー攻撃による情報漏えいやシステム障害など、サイバーセキュリティに関連するインシデント（事故）・事象が発生した際に対応する組織。インシデント発生時（有事）以外の平時にもリサーチなどの活動を行う。

CSIRTが担う役務は、大きく3つのカテゴリに分類されます

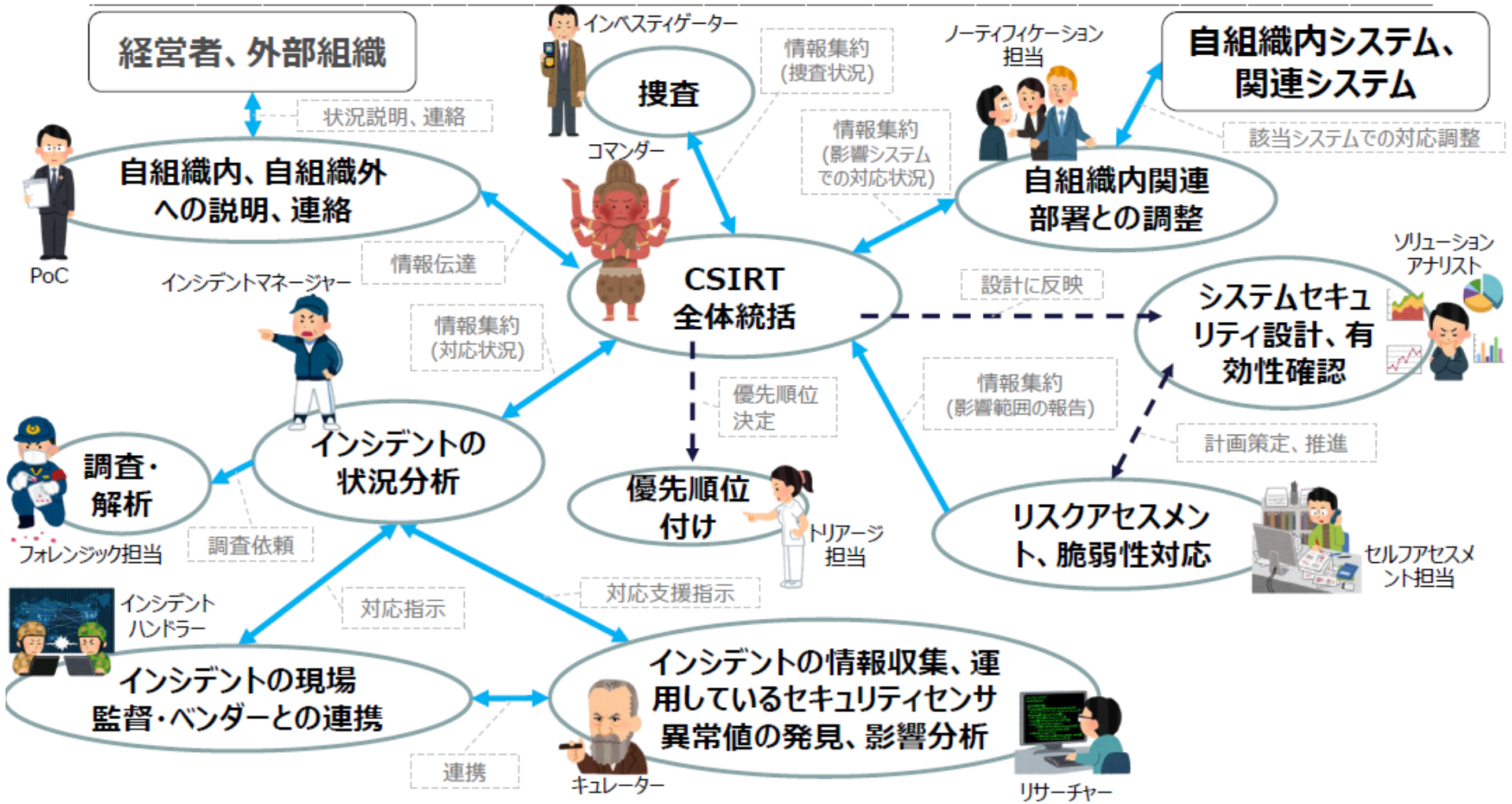
カテゴリ	概要
インシデント 事後対応	インシデントの**被害局限化を目的**とした、インシデントやインシデントに関連する**事象への対応**を行うためのサービス
インシデント 事前対応	インシデントの**発生抑制を目的**とした、インシデントやセキュリティイベントの**検知**や、**発生の可能性を減少させる**ためのサービス
セキュリティ 品質向上	社内セキュリティの品質を向上させることを目的としたサービス →間接的にインシデントの発生抑制をする

CSIRTの役割と業務内容の関連図__平常時



出典：日本シーサート協議会　CSIRT人材の定義と確保Ver.1.5

CSIRTの役割と業務内容の関連図__緊急時



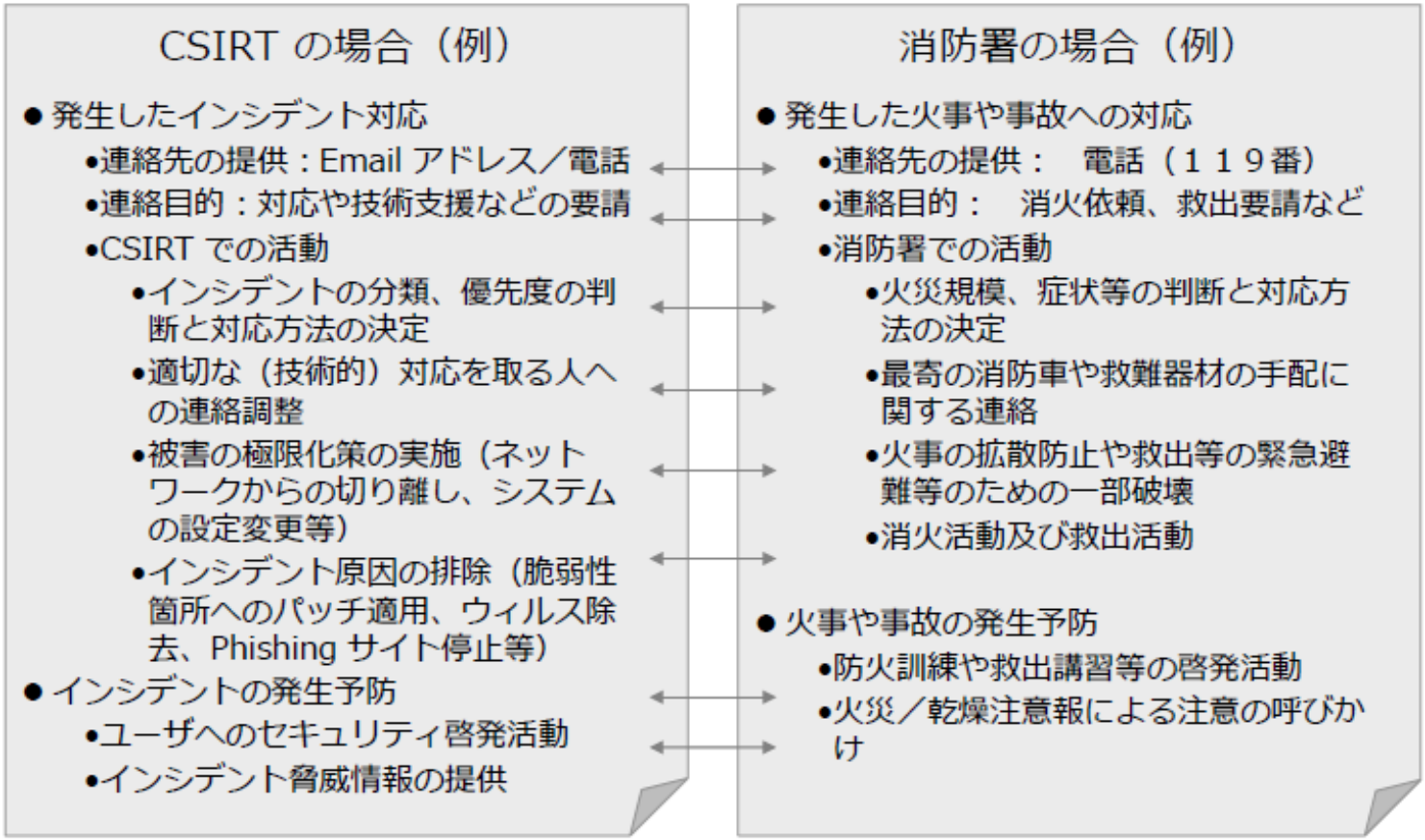
出典：日本シーサート協議会　CSIRT人材の定義と確保Ver.1.5

そんなに**ヒト**も**カネ**もかけられない…。

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

Advancing with you
MS&AD
INSURANCE GROUP

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

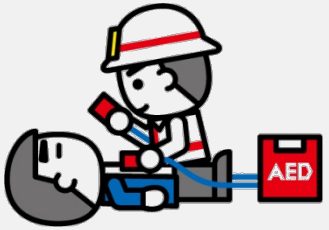
緊急時は アウトソース

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

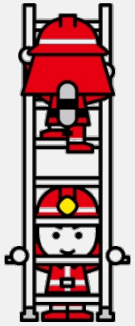
緊急時はアウトソース

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】
重要な物品をの持ち出し、保護を行う
持ち出し物の掌握、管理を行う



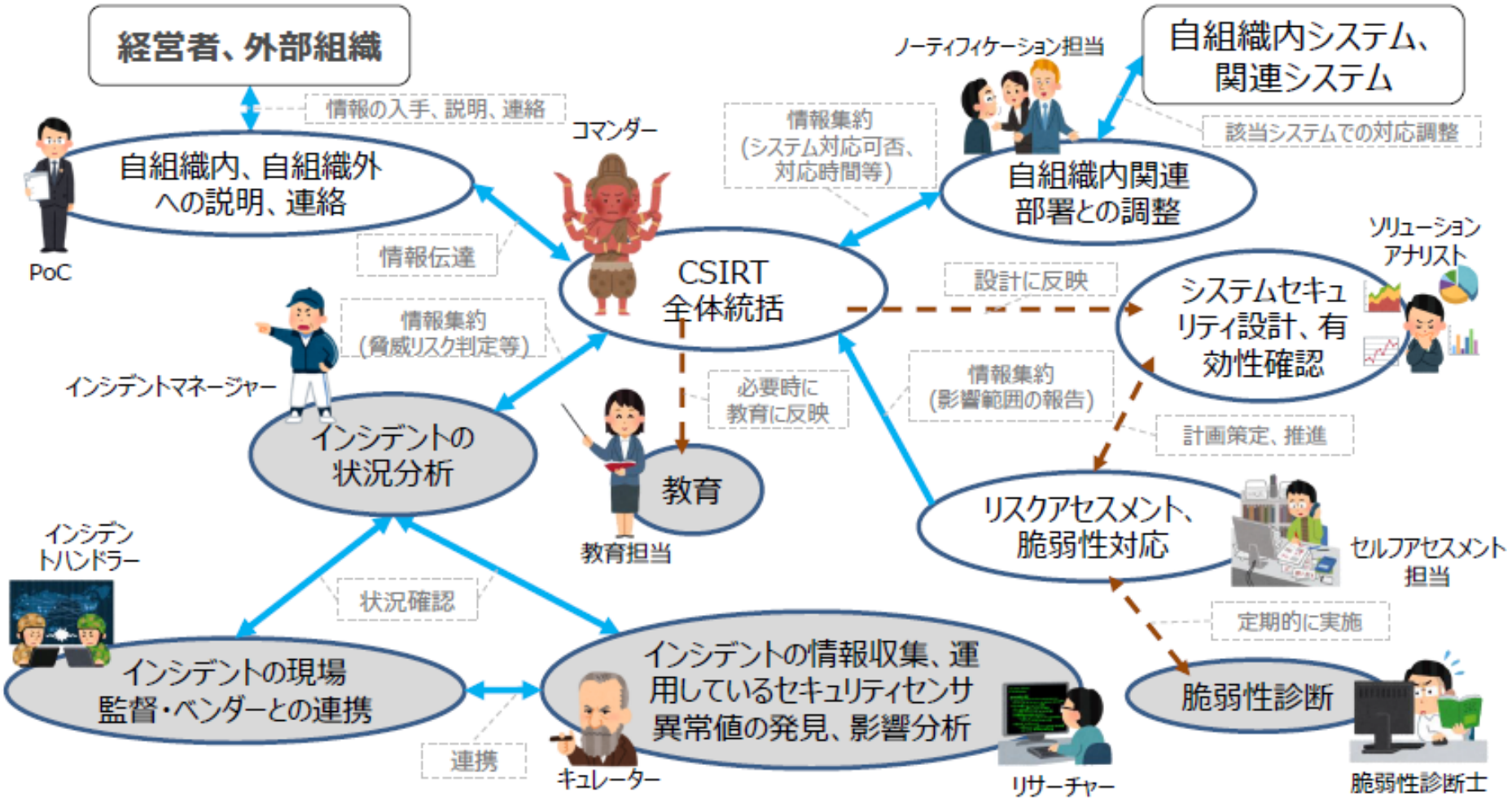
【警戒宣言発令時】
非常持ち出し品の整理と確認を行う

まとめると … CSIRTの役割と業務内容の関連図__平常時

Advancing with you
MS&AD
INSURANCE GROUP

自衛消防隊レベルにすると‥(平常時)

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

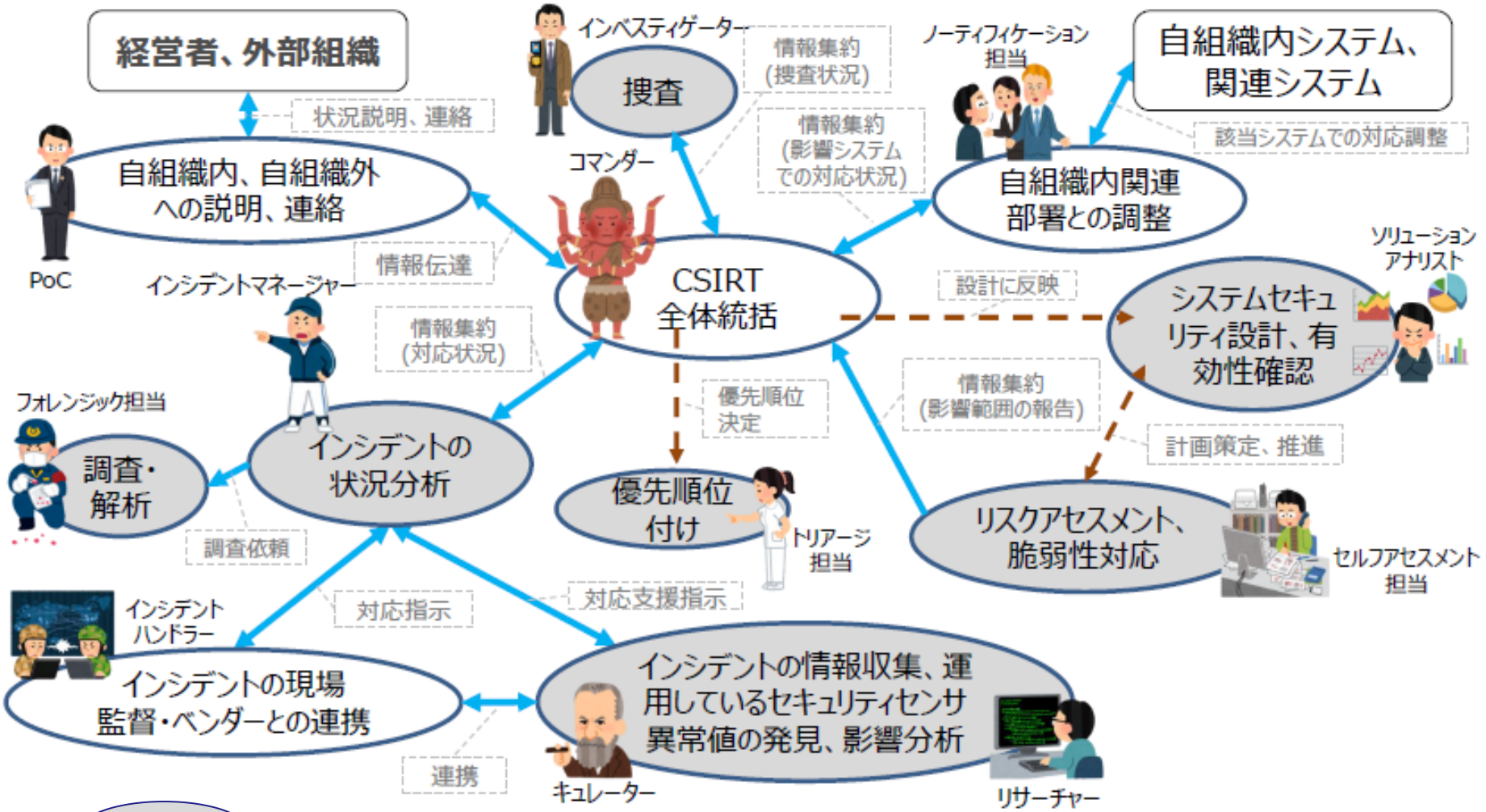
※「日本シーサート協議会　CSIRT人材の定義と確保Ver.1.5」に基づきMS&ADインターリスク総研にて追記

まとめると … CSIRTの役割と業務内容の関連図__緊急時

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

※「日本シーサート協議会　CSIRT人材の定義と確保Ver.1.5」に基づきMS&ADインターリスク総研にて追記

Advancing with you
MS&AD
INSURANCE GROUP

前提条件

✓ **あくまで自衛消防隊であり、大災害には手を出さない**
✓ **人材は３年でローテーションされる（定期異動がある）**

役割	平常時	緊急時
全体統括	○	○
外部、経営者との連絡窓口	○	○
自組織内の調整	○	○
優先順位付け	ー	△技術面はアウトソース
セキュリティ機器導入計画策定	○	ー
資産管理アセスメント	○	ー
システムセキュリティの状況監視・分析	アウトソース	アウトソース
脆弱性診断	アウトソース	ー
教育	アウトソース	ー
インシデント対応	ー	△手に負えなければアウトソース
フォレンジック／捜査	ー	アウトソース

社内人材の候補

- 全体統制＋外部、経営者との連絡窓口＋社内調整＋優先順位づけ＝１名
  - システム運用経験、障害時の全体統制経験者
  - システム障害時に報告書などを作り、関係者に説明をした事がある経験者

- セキュリティ機器導入計画策定＋資産管理アセスメント＝１名
  - システム企画や開発や提案書の作成、 SI ベンダー の比較検討や開発計画書を作成した経験、プロジェクトマネジメントの経験者
  - ISMSやＰマーク取得のために資産管理台帳の作成やリスクアセスメントを実施したことのある経験者

- インシデント対応＝１名
  - システム運用にて障害対応をしたことがある経験者

４．まとめにかえて

■ **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

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

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

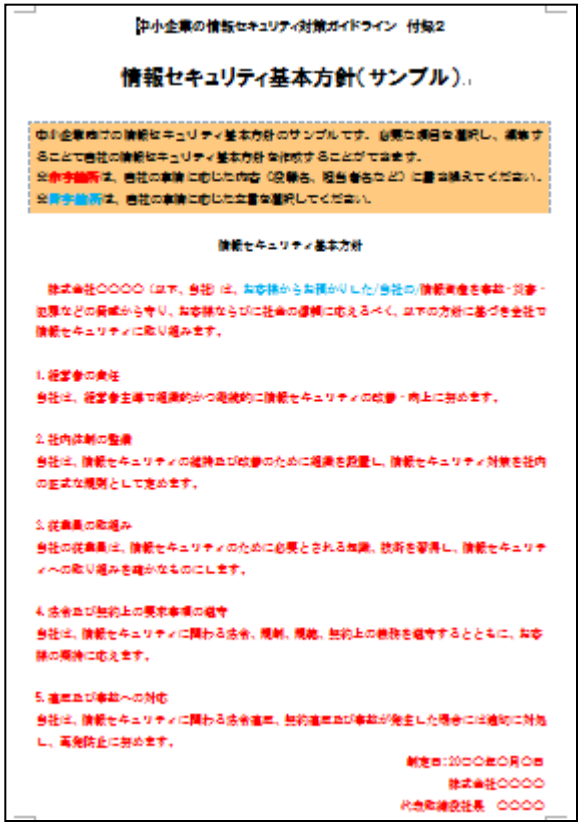
実行すべき「重要７項目の取組」

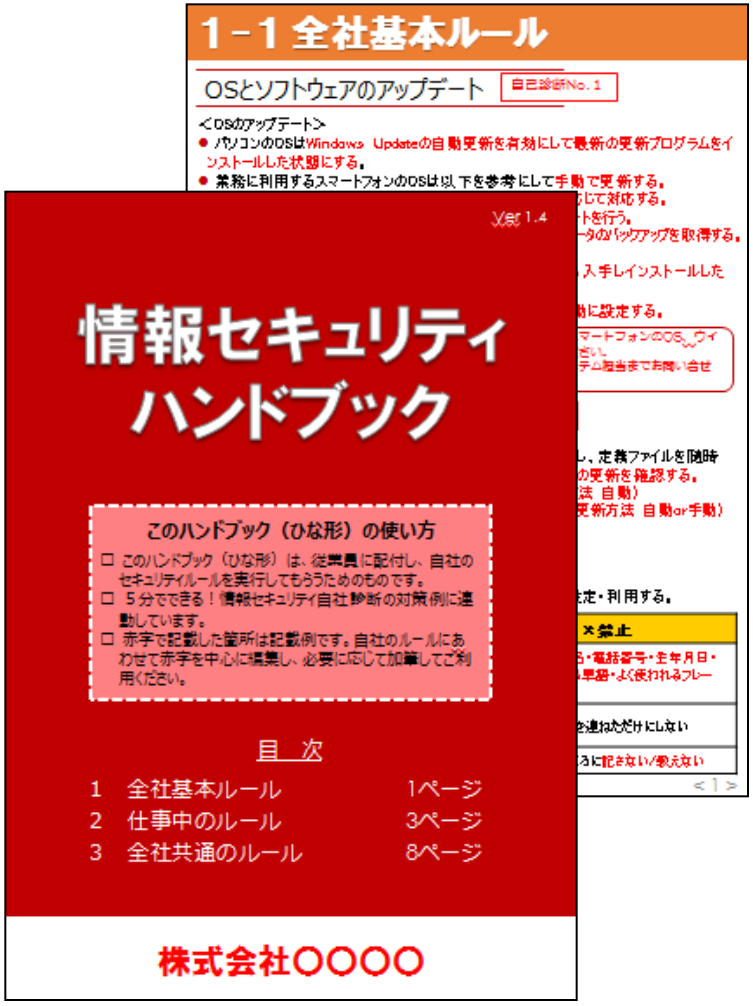
取組１　情報セキュリティに関する**組織全体の対応方針**を定める	取組５　**緊急時の対応**や**復旧のための体制**を整備する
取組２　情報セキュリティ対策のための**予算や人材**などを確保する	取組６　**委託や外部サービス利用**の際にはセキュリティに関する**責任を明確**にする
取組３　必要と考えられる**対策を検討**させて**実行を指示**する	取組７　情報セキュリティに関する**最新動向**を収集する
取組４　情報セキュリティ対策に関する**適宜の見直し**を指示する	

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）

【参考資料】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





【参考資料】サイバーセキュリティに関する主な用語説明

本資料にて使用しているサイバーセキュリティに関する主な用語とその説明は以下のとおりです。
各ページに詳細な定義・意味を記載しているものもありますが、適宜ご参照ください。

用語	意味・説明
CSIRT （読み：シーサート）	Computer Security Incident Response Teamの略。サイバー攻撃による情報漏えいやシステム障害など、サイバーセキュリティに関連するインシデント（事故）・事象が発生した際に対応する組織。
CISO	Chief Information Security Officerの略。企業内で情報セキュリティを統括する担当役員の呼称。
DDoS攻撃 （読み：ディードス攻撃）	「Distributed」+「 Denial（拒否）」+「of」+「Service attack」の略。標的としたサーバーの処理能力を超える負荷を複数の攻撃用PC(ボットネット)により与える攻撃のこと
IPA	Information- technology Promotion Agency（情報処理推進機構）の略。経産省所管のシンクタンク。日本のソフトウェア分野における国際競争力強化に向けた人材育成、政策提言、情報発信などを行っている。
ISMS	Information Security Management Systemの略。個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源を配分して、システムを運用すること。
JNSA	Japan Network Security Association（NPO日本ネットワークセキュリティ協会）の略。ネットワークセキュリティに関する啓発、教育、調査研究及び情報提供に関する事業を行う、特定非営利活動法人。

【参考資料】サイバーセキュリティに関する主な用語説明

用語	意味・説明
SOC （読み：ソック）	Security Operation Centerの略。情報セキュリティ機器、サーバ、コンピュータネットワークなどが生成するログを監視・分析し、サイバー攻撃の検出・通知を行う組織。
UTM	統合脅威管理=Unified Threat Managementの略で、複数の異なるセキュリティ機能を統合したハードウェア機器。ネットワークを管理する際に、複数の機器を導入すると手間もコストもかかるため、セキュリティ機能を集約したものがUTM。
エンドポイント	ネットワークに接続されたサーバやパソコン、携帯電話などのネットワーク端末の総称
ダークウェブ（Dark Web）	アクセスするために特定のソフトウェア、設定、認証が必要な匿名性と秘匿性の高いWebのこと。
ファイアウォール	ファイアウォールとは防火壁のことだが、コンピュータネットワーク関連では、ネットワークの境界に設けて、「通過させてはいけない通信」を阻止するシステムを指す。 外部からの攻撃に対する防御だけではなく、内側から外部への望まない通信を制御する目的も含め運用されていることもある。
（デジタル）フォレンジック	コンピュータの記憶媒体に保存されている文書ファイルやアクセスログなどからサイバー攻撃の内容調査に資する証拠を探し出すこと。
マルウェア	「Malicious（悪意のある）」+「Software」を略した造語で、様々な手法を用いて利用者のコンピュータに感染し、スパムの配信や情報窃取等の遠隔操作を自動的に実行するソフトウェアの総称（ウイルスやトロイの木馬等）
ランサムウェア	「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語。マルウェアの一種。

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