NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

最新のセキュリティ脅威と対策ポイント

JNSA マーケティング部会

agenda

- 最近のセキュリティリスクの傾向
- 標的型攻撃にみる攻撃の構造例
- サプライチェーン攻撃で鉄壁の守りも突破
- ビジネスメール詐欺の被害拡大
- サイバーセキュリティ経営ガイドライン
- 攻撃の組織化とCSIRT
- CSIRTによるインシデント対応

最近のセキュリティリスクの傾向

IPA 情報セキュリティ10大脅威 2018

昨年順位	個人	順位	組織	昨年順位
1位	インターネットバンキングやクレジットカード情報の不正利用	**1位**	標的型攻撃による情報流出	1位
2位	ランサムウェアによる被害	**2位**	ランサムウェアによる被害	2位
7位	ネット上の誹謗・中傷	**3位**	ビジネスメール詐欺 **[NEW]**	ランク外
3位	スマートフォンやスマートフォンアプリを狙った攻撃の可能性	**4位**	脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加	ランク外
4位	ウェブサービスへの不正ログイン	**5位**	セキュリティ人材の不足 **[NEW]**	ランク外
6位	ウェブサービスからの個人情報の窃取	**6位**	ウェブサービスからの個人情報の窃取	3位
5位	情報モラル不足に伴う犯罪の低年齢化	**7位**	IoT 機器の脆弱性の顕在化	8位
8位	ワンクリック請求等の不当請求	**8位**	内部不正による情報漏えい	5位
10位	IoT 機器の不適切管理	**9位**	サービス妨害攻撃によるサービスの停止	4位
ランク外	偽警告 **[NEW]**	**10位**	犯罪のビジネス化（アンダーグラウンドサービス）	9位

サイバーキルチェーンによる攻撃フェーズと攻撃例

フェーズ	攻撃例
偵察	•外部からの脆弱性スキャン •社員のSNSの情報収集 •フィッシングメール送信
配送	•マルウェア付きメール送信 •なりすましメール送信 •悪意のあるWebサイトURL付きメール送信 •脆弱性を悪用した外部からのコマンド実行
攻撃	•添付ファイルを開かせる •悪意のあるWebサイトにアクセスさせる •悪意のあるコマンドを実行させる
インストール	•添付ファイル実行によるマルウェア感染 •悪意のあるWebサイトアクセスによるマルウェアのダウンロード・感 •悪意のあるコマンド実行による設定の変更、別のマルウェアのダウン
遠隔操作	•データの搾取 •別のマルウェアのダウンロード •OSの設定変更、OS情報の送信
侵入拡大	•同一ネットワーク上の端末への感染拡大
目的達成	•目的の情報やデータを外部へ送信 •目的の設定や、バックドア・トロイの木馬の埋め込み

いくつかの手法を組み合わせ、段階的に重要情報にリーチする

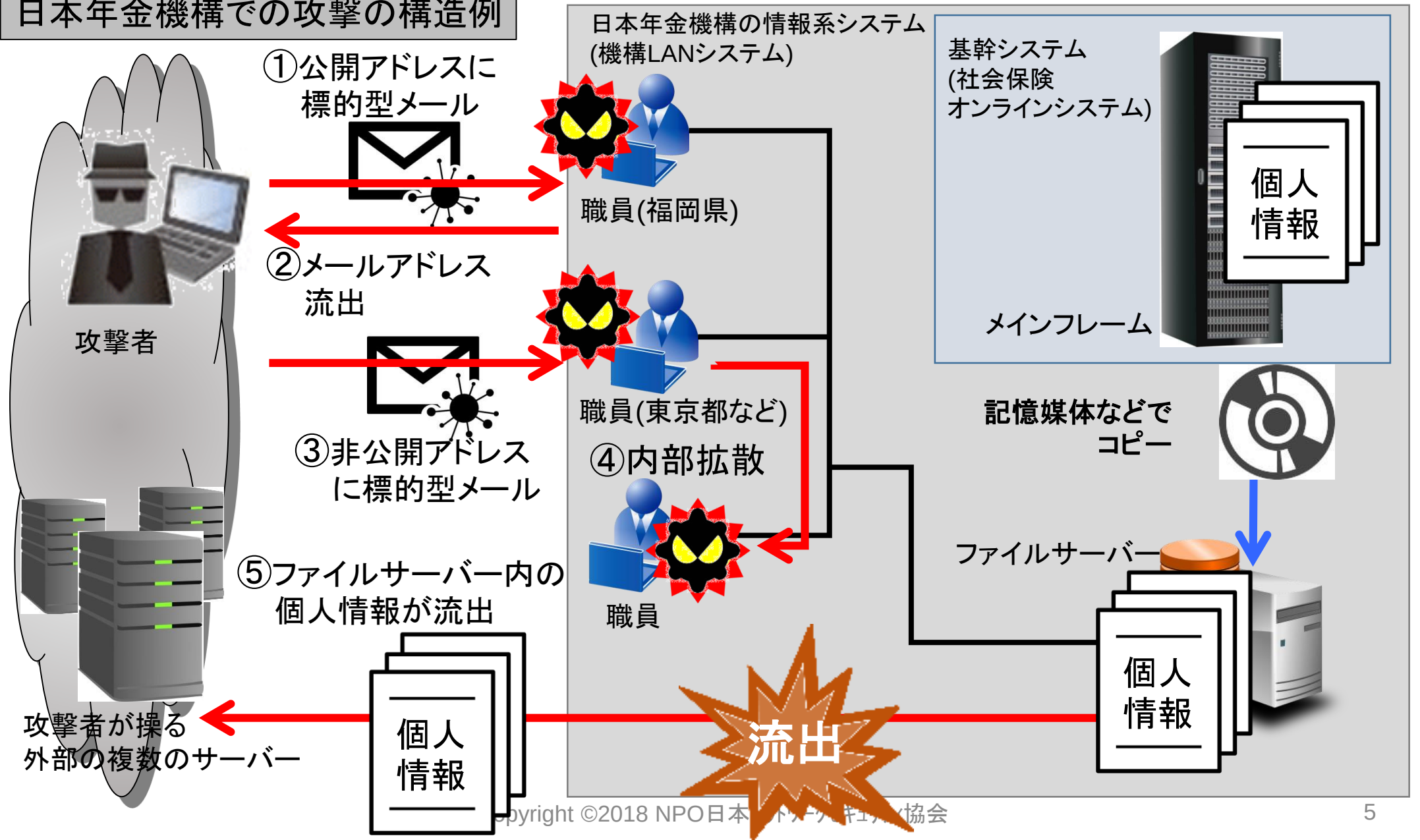
転換ポイント

- サイバーセキュリティ政策に係る年次報告（2017年度）2018年７月25日　NISC
  - サイバー攻撃はより深刻化・巧妙化し被害も拡散
    - Java脆弱性により漏えい事案が発生
    - 攻撃ツールセットが公開され、ランサムウェア「WannaCry」が世界的に大流行
    - 多額の仮想通貨が不正に送信、他の仮想通貨等へ交換
    - 平昌オリ・パラにおいて、大会運営用システムがサイバー攻撃の影響で停止
  - サイバー空間に係る国際的な動向
    - 米国、EU、中国、ロシアの動向
    - 各国との二国間協議

NEWS①
標的型攻撃に見るサイバーキルチェーン

JNSA

日本年金機構での攻撃の構造例



調査結果報告のポイント

① インシデントへの対応体制
- 担当者任せ、責任所在不明確、など

② 共有ファイルサーバの管理
- 個人情報の保管場所に関する問題のあるシステム設計とリスク認識の甘さ、ルールチェックなし

③ 情報セキュリティポリシー等
- 改正等遅れ、省の反映のみで緊張感欠如

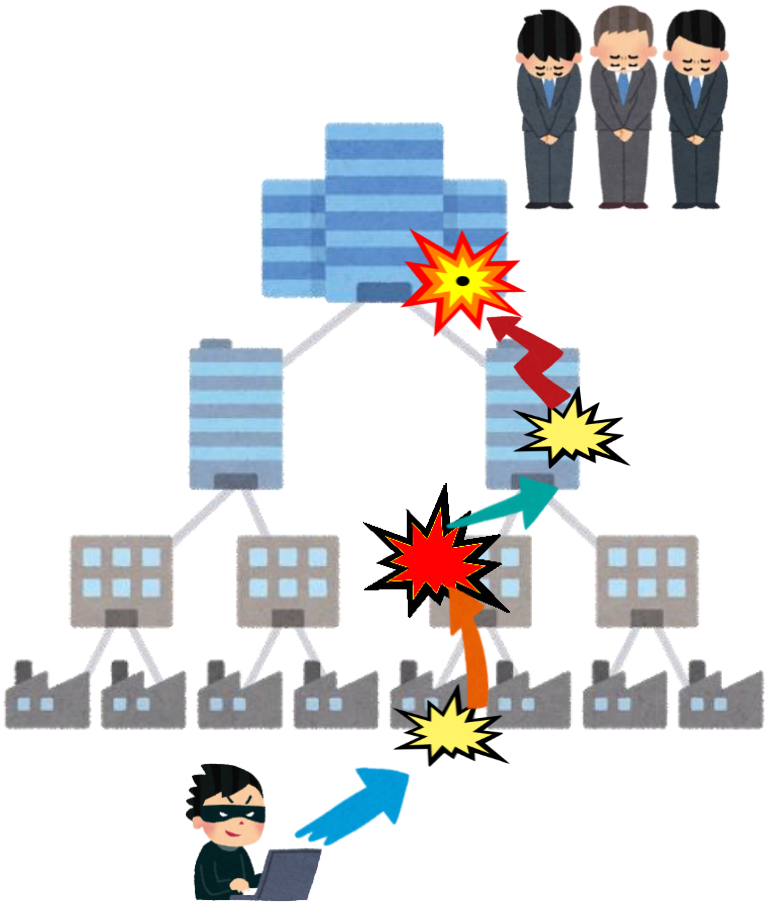
④ 職員研修
- 責任を持った意思決定なし

⑤ ガバナンス・組織風土のゼロベースからの抜本改革
- 上層部に情報集約されず、など

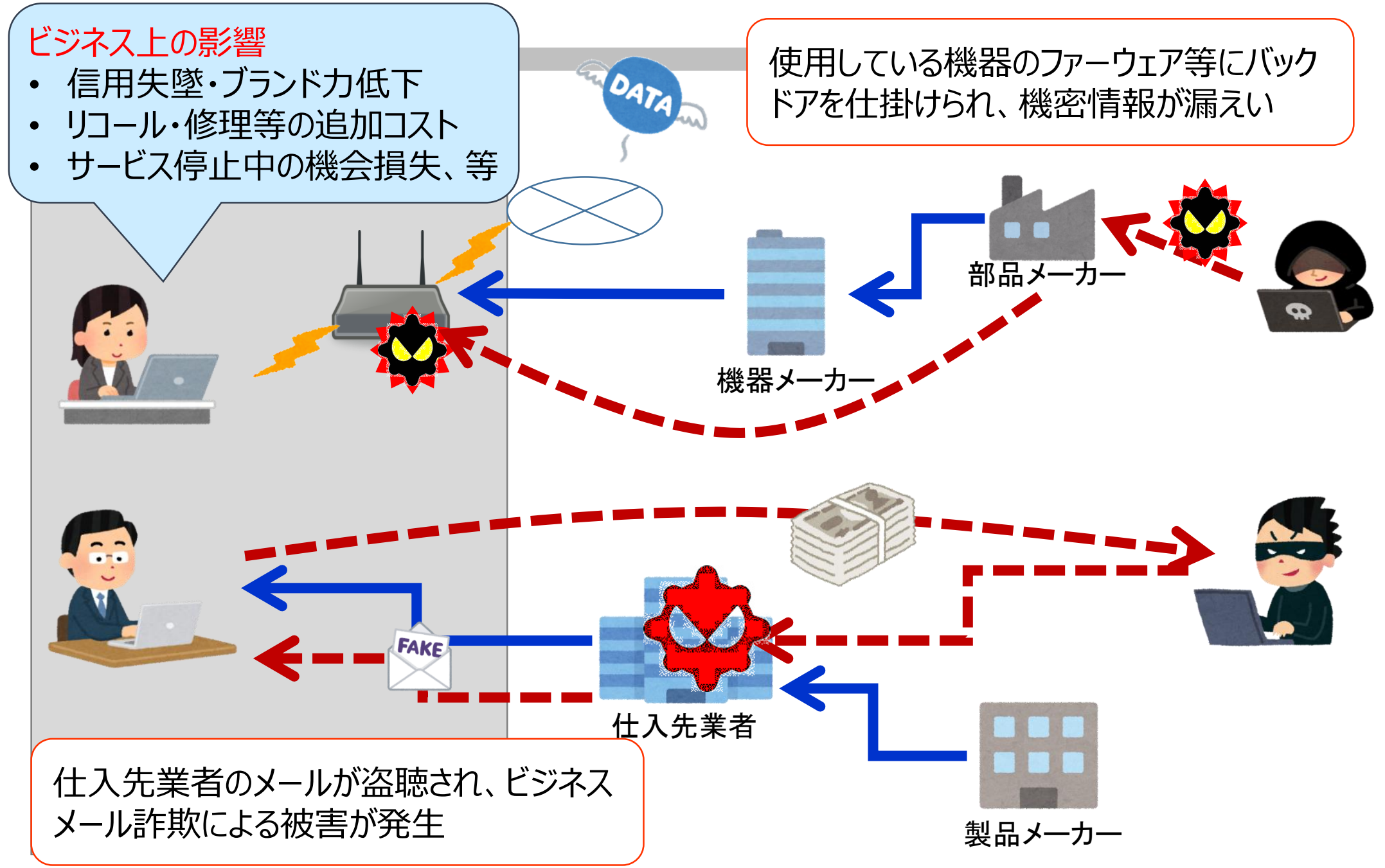
日本年金機構(2015/8/20)「不正アクセスによる情報流出事案に関する調査結果報告書」

NEWS②
サプライチェーン攻撃で鉄壁の守りも突破

- ビジネス活動の流れ(サプライチェーン)の途中を攻撃し、最終的にターゲットを攻撃する。
  - 大企業や政府組織などを攻撃するため、防御の手薄なビジネスパートナー等を“侵入口”として攻撃。そこからターゲットの組織へ潜入する。
  - 多くの組織が利用している製品・ソフトウェア等の開発元などに侵入し、密かにマルウェア等を混入し、それを利用している組織を攻撃する。

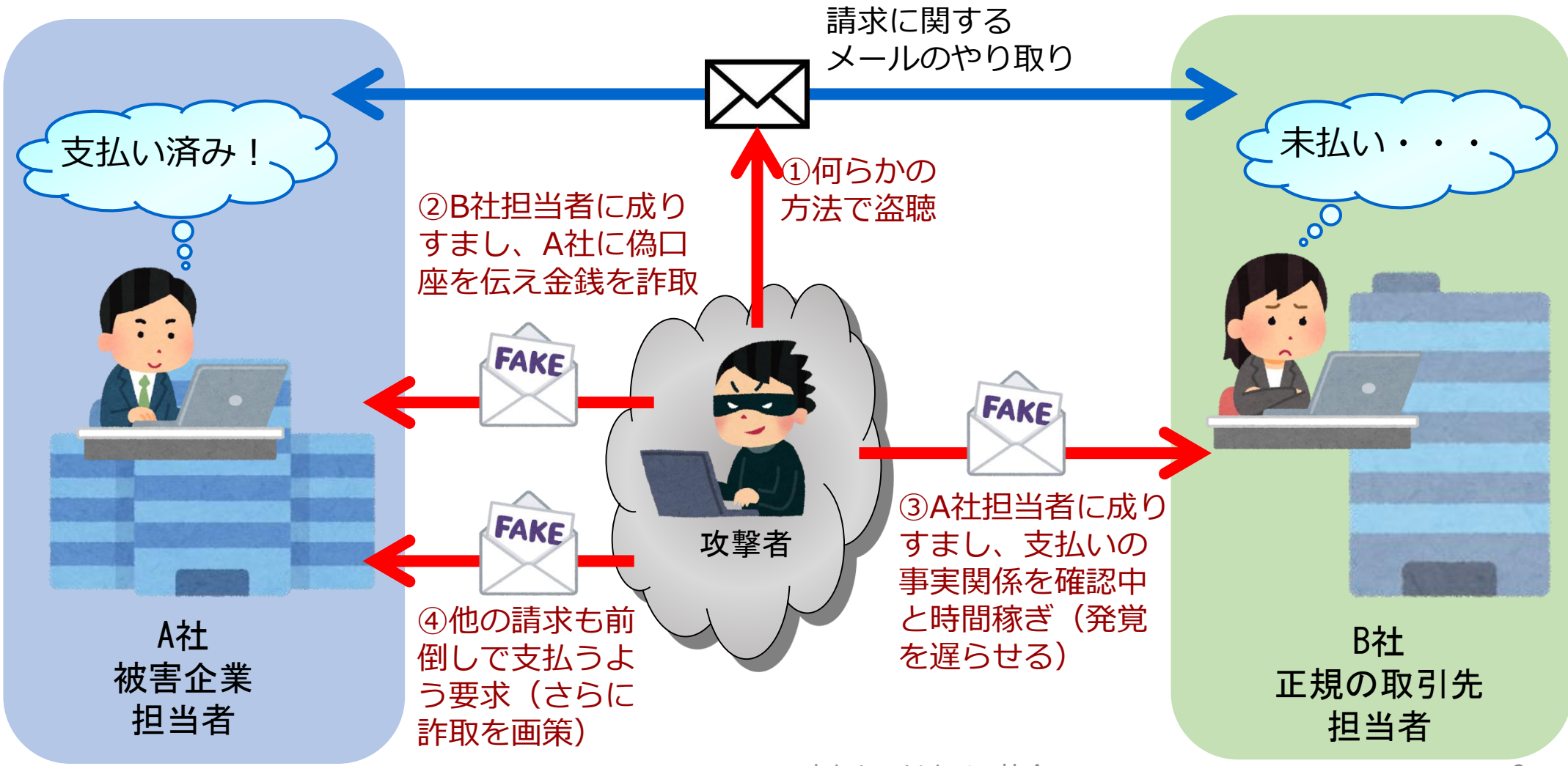


サプライチェーン攻撃のリスクイメージ



NEWS③
ビジネスメール詐欺の被害拡大

ビジネスメール詐欺（BEC：Business E-mail Compromise）事例



ビジネスメール詐欺の手口

- 取引担当者等になりすまし
  - 税務調査が入っており、従来の口座が使用できない
  - 従来の口座が不正取引に使用され、凍結されてしまった
  - 技術的な問題が発生しており、従来の口座が使用できない
- 経営者層等になりすまし。
  - 極秘の買収案件で、資金が至急必要になった
  - 緊急かつ内密に送金してほしい（他者に相談させない）
- 弁護士等になりすまし

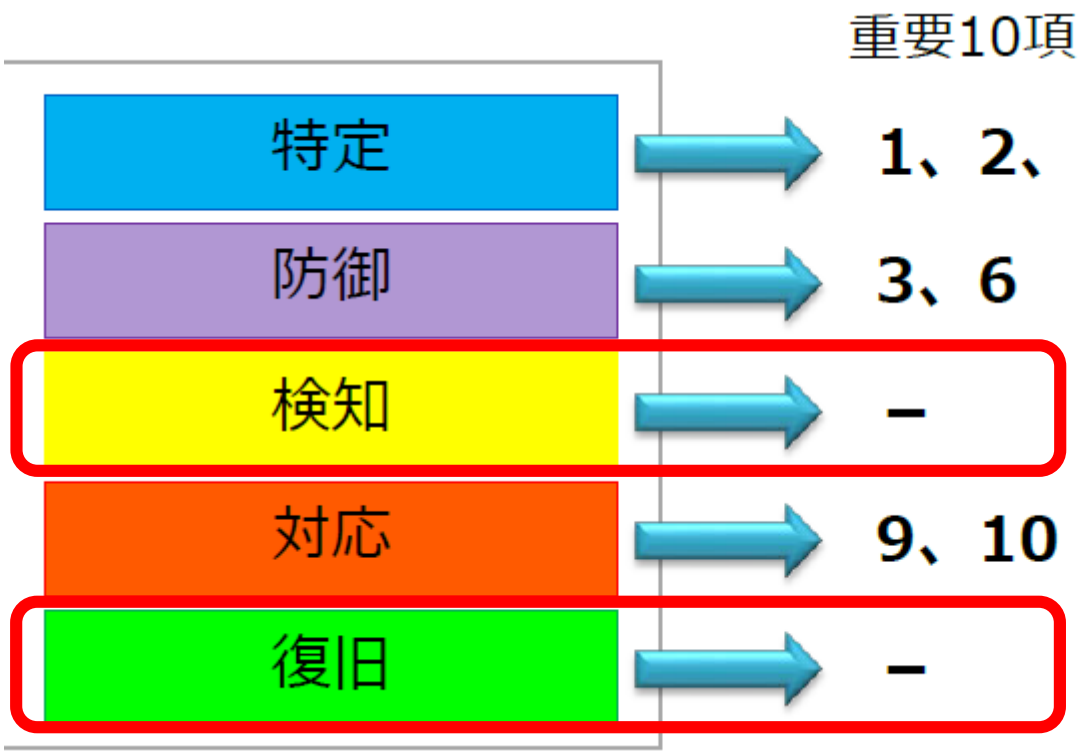
被害防止対策

- 添付ファイルやリンク先を不用意に開かない
- ウイルス対策ソフト・OSを最新の状態に更新
- 不正アクセス対策を徹底する
- 電話などメール以外の方法で確認
- メール（アドレス）をよく確認
- 組織内外での情報共有

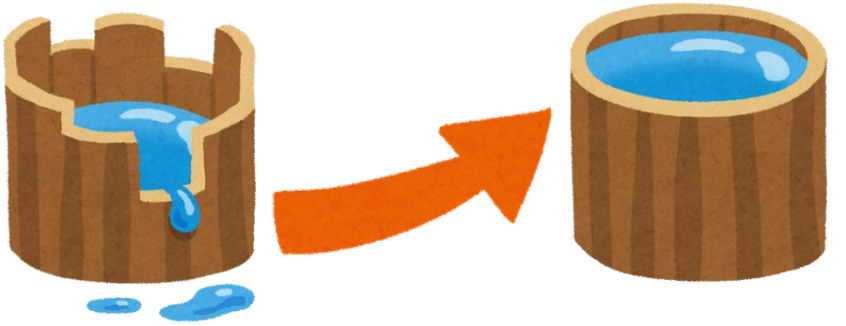
いかに早く気づけるかが重要！

NEWS④
改訂「サイバーセキュリティ経営ガイドライン」

- 昨今のサイバー攻撃の巧妙化により事前対策だけでは対処が困難。



平成29年11月16日
検知と復旧を入れて
Ver2に改訂

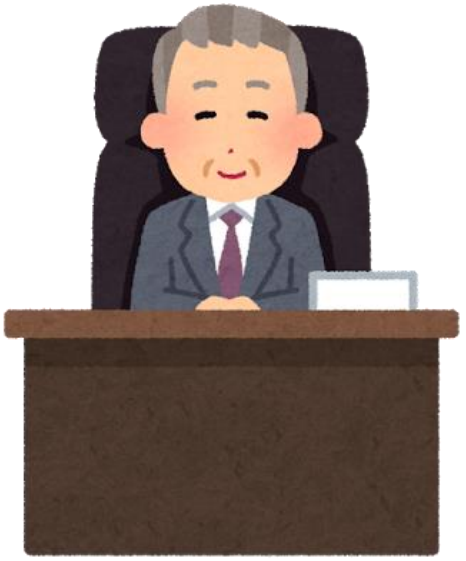


サイバーセキュリティ経営ガイドラインの構成

【本編】
概要
1．　はじめに（経営問題、3原則、重要10項目）
2．　経営者が認識すべき３原則
3．　サイバーセキュリティ経営の重要１０項目

【付録】
A) サイバーセキュリティ経営チェックシート
B) サイバーセキュリティ対策に関する参考情報
C) インシデント発生時に組織内で整理しておくべき事項（別紙）
D) 国際規格ISO/IEC27001及び27002との関係
E) 用語の定義

経営者が認識すべき３原則



① 経営者は、サイバーセキュリティリスクを認識し、**リーダーシップによって対策を進める**ことが必要

② 自社は勿論のこと、ビジネスパートナーや委託先も含めた**サプライチェーンに対するセキュリティ対策が必要**

③ 平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報開示など、**関係者との適切なコミュニケーションが必要**

インシデント発生時の報告内容
組織内で整理しておくべき事項（付録C）

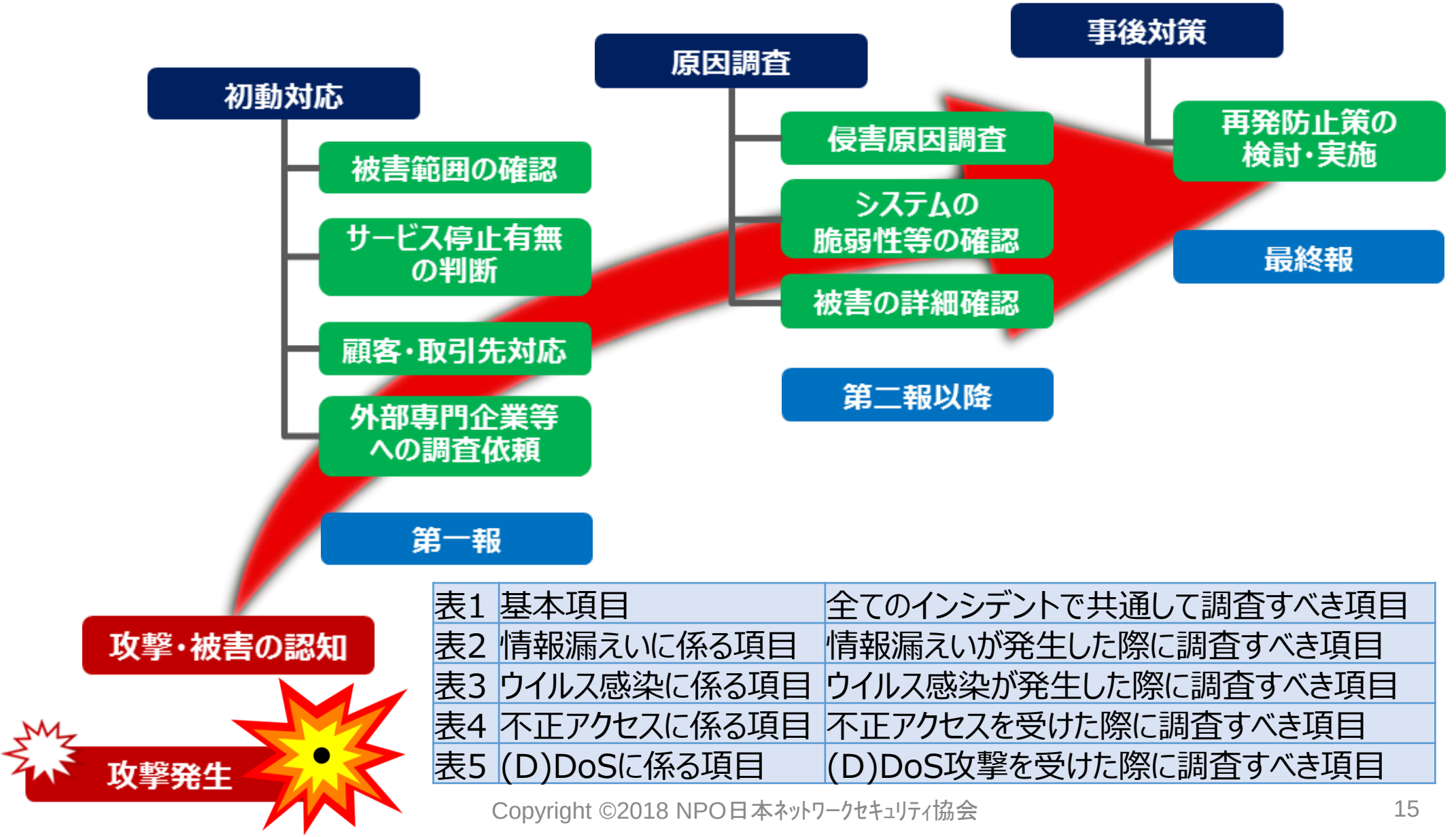
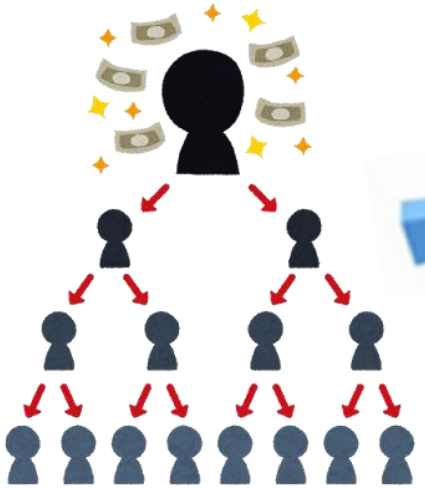


表1	基本項目	全てのインシデントで共通して調査すべき項目
表2	情報漏えいに係る項目	情報漏えいが発生した際に調査すべき項目
表3	ウイルス感染に係る項目	ウイルス感染が発生した際に調査すべき項目
表4	不正アクセスに係る項目	不正アクセスを受けた際に調査すべき項目
表5	(D)DoSに係る項目	(D)DoS攻撃を受けた際に調査すべき項目

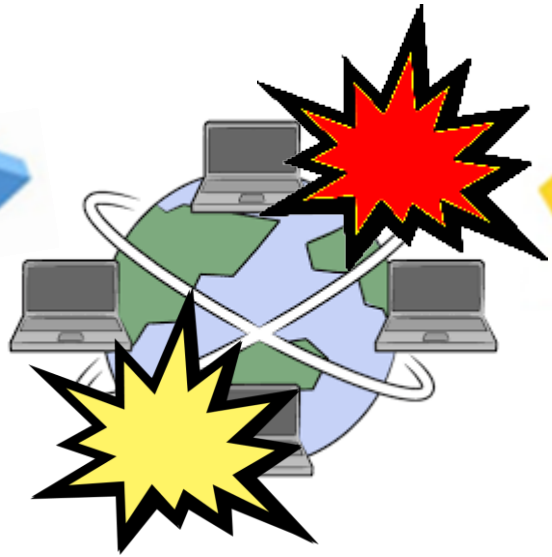
NEWS⑤
攻撃の組織化とCSIRT

攻撃側



- 指揮監督
- マルウェア作成
- DDoS攻撃
- Web改ざん
- NW侵入
- データ入手
- …..etc

VS



防御側

- 対策指揮
- 内外との連絡係
- 情報収集・分析
- …..etc

CSIRT構築
の必要性

CSIRTとは

- CSIRT：
  Computer Security Incident Response Team
  - コンピュータセキュリティにかかわるインシデントに対処するための組織の総称
  - インシデント関連情報、脆弱性情報、攻撃予兆情報を収集、分析し、対応方針や手順の策定などの活動

- 予防活動
  - 各システムのチェック
  - 対策や規定の見直し
  - ユーザ啓発
- 対応活動
  - 検知・通知
  - 対応、原因究明

これらの活動をする
「組織」が必要
＝
“CSIRT”

CSIRTを機能させるための活動

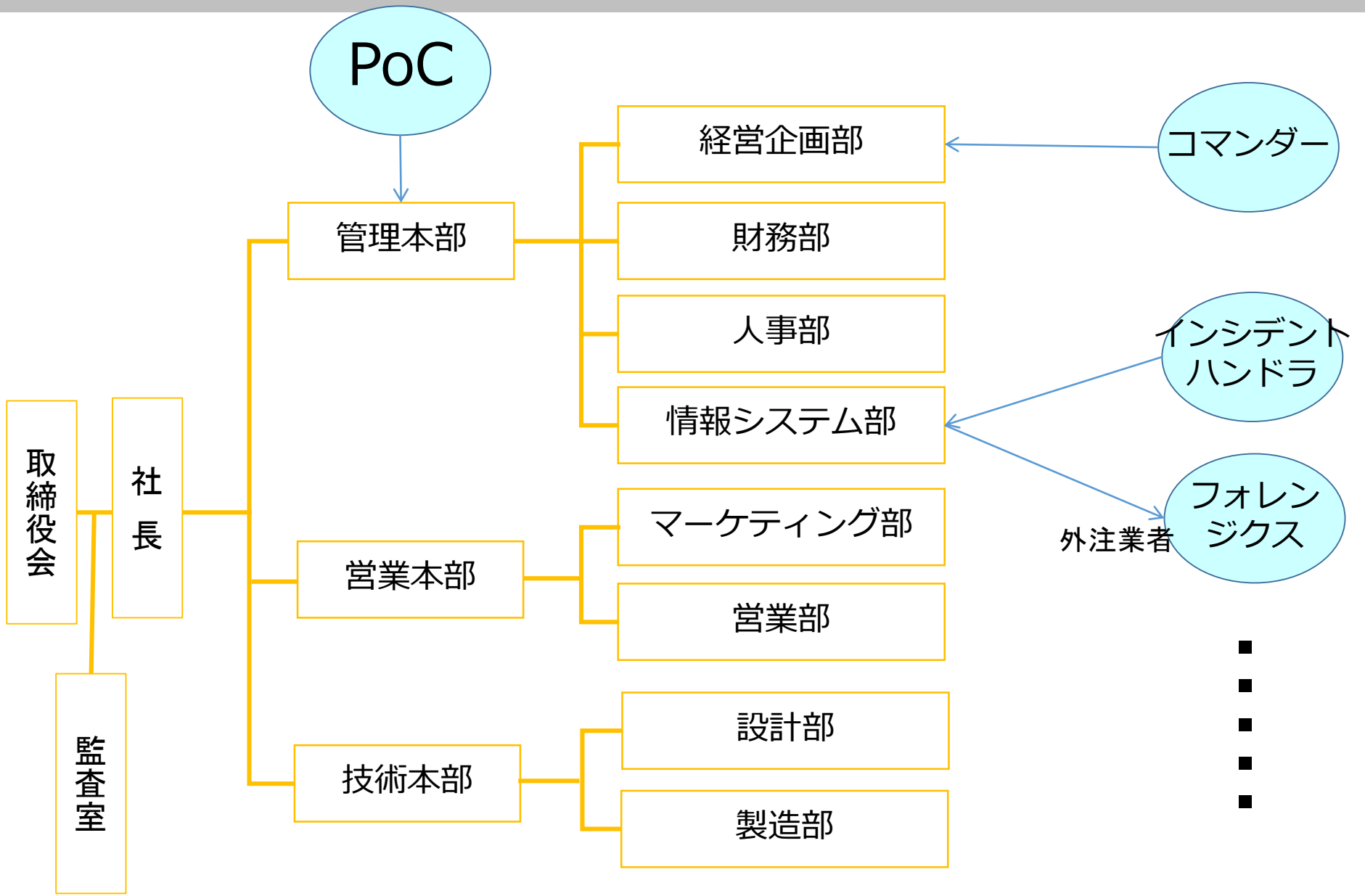
- ポイントは事前対処（インシデントレディネス）
  - インシデントレスポンス(事後対処)などの実践的な活動経験を元に、インシデントレディネス(事前対処)を進めることが重要

CSIRTの役割と業務内容

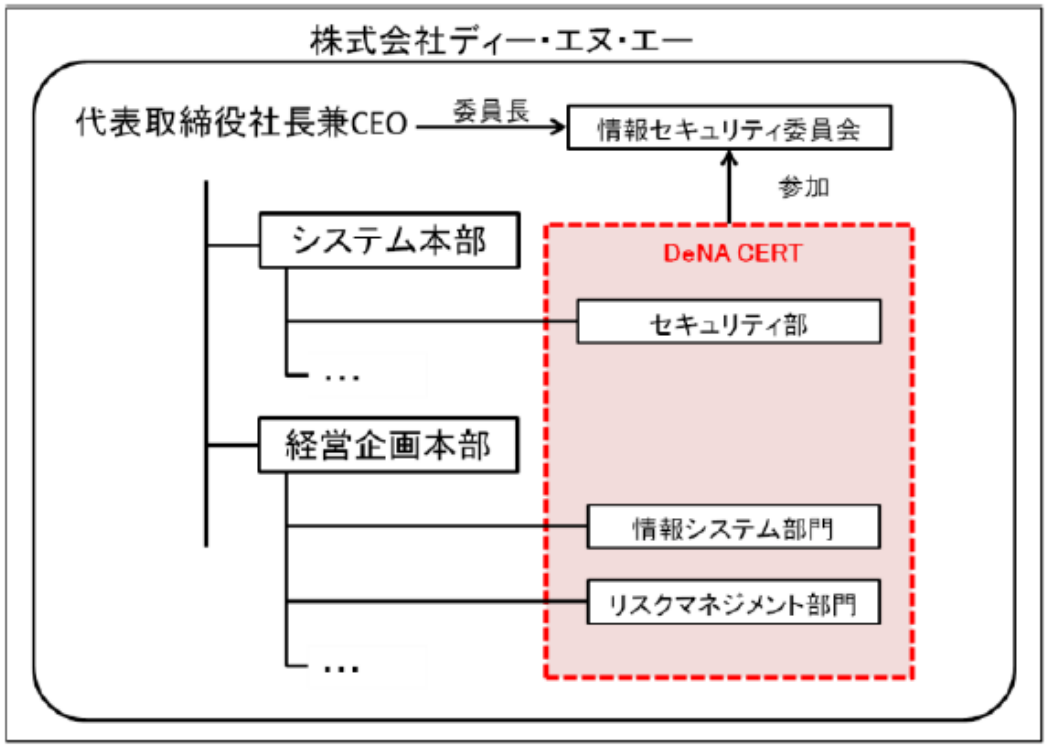
機能分類	役割名称	業務内容
情報共有	社外PoC：自組織外連絡担当	NCA、JPCERT/CC、CSIRT、警察、監督官庁、等々との情報連携
	社内PoC：自組織内連絡担当、IT部門調整担当	法務、渉外、IT部門、広報、各事業部、等々との情報連携
	リーガルアドバイザー：法務部CSIRT担当	コンプライアンス、法的内容とシステム間の翻訳
	ノーティフィケーション担当：自組織内調整・情報発信担当	各関連部署との連絡ハブ、情報発信
情報収集・分析	リサーチャー：情報収集担当、キュレーター：情報分析担当	定例業務、インシデントの情報収集、各種情報に対する分析、国際情勢の把握
	脆弱性診断士：脆弱性の診断担当	OS、ネットワーク、セキュアプログラミングの検査、診断
	脆弱性診断士：脆弱性の評価担当	OS、ネットワーク、セキュアプログラミング診断結果の評価
	セルフアセスメント担当	平時のリスクアセスメント、有事の際の脆弱性の分析、影響の調査
	ソリューションアナリスト：セキュリティ戦略担当	ソリューションマップ作成、Fit&Gap分析、リスク評価、有事の際の有効性評価
インシデント対応	コマンダー：CSIRT全体統括	CSIRT全体統括、意思決定、社内PoC、役員、CISO、または経営層との情報連携
	インシデントマネージャー：インシデント管理担当	インシデントの対応状況の把握、コマンダーへの報告、対応履歴把握
	インシデントハンドラー：インシデント処理担当	インシデント現場監督、セキュリティベンダーとの連携
	インベスティゲーター：調査・捜査担当	捜査に必要な論理的思考、分析力、自組織内システム理解力を使った内偵
	トリアージ担当：優先順位選定担当	事象に対する優先順位の決定
	フォレンジック担当	証拠保全、システム的な鑑識、足跡追跡、マルウェア解析
自組織内教育	教育担当：教育・啓発担当	自組織のリテラシー向上、底上げ

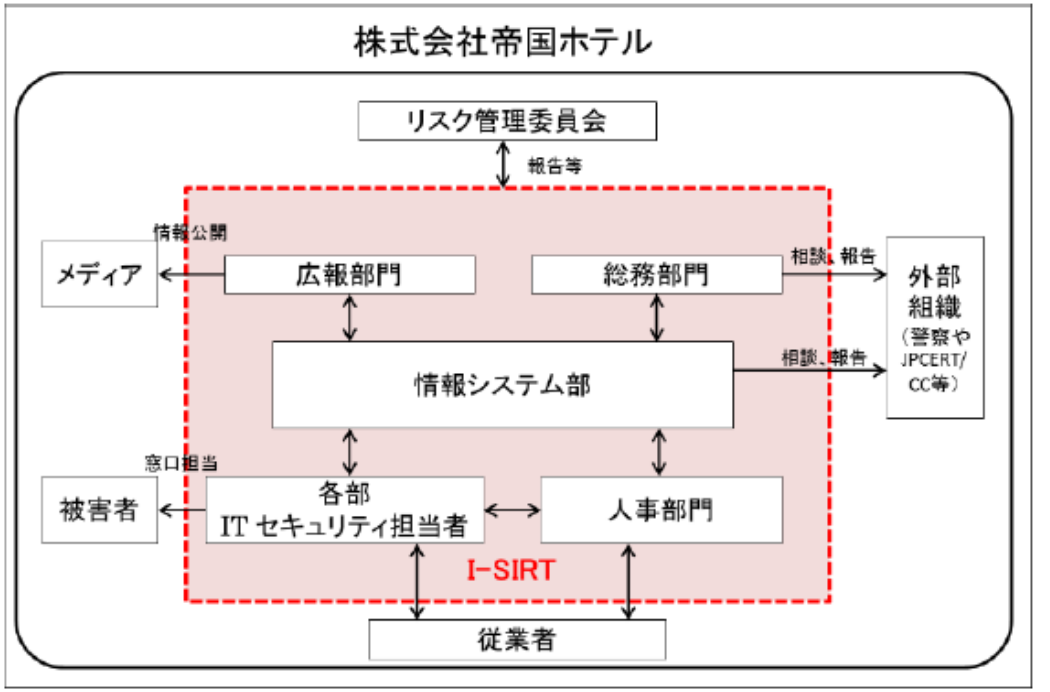
出典: 日本シーサート協議会「CSIRT人材の定義と確保ver.1.5）」

自組織をイメージして担当を検討



CSIRT組織化事例





出典：JPCERT/CC 2015年度 CSIRT構築および運用における実態調査

NEWS⑥
CSIRTで重要なのは発生時だけじゃない！

インシデント対応の考え方は多数存在するが、本セミナーではNISTのコンピュータセキュリティ部門がまとめたコンピュータセキュリティ関係のレポート**SP800-61(r1)**を解説している。

準備

- 手順書の作成
- ＣＳＩＲＴの設置
- 検知、調査機能の実装
- 訓練の実施

検知と分析

- 前兆や兆候の検出
- 兆候の分析
- 優先順位付け
- 通知や報告

封じ込め、根絶、復旧

- 状況の確認
- 被害拡大の防止
- インシデント原因の調査
- 復旧

事件後の対応

- セキュリティ対策の改善
- インシデント対応の評価と改善
- 証拠の保管

参考文献：　NIST SP800-61(r1) コンピュータセキュリティインシデント対応ガイド

Phase1：準備

インシデントレスポンスを行うための体制、手順、環境づくりを行う

①ポリシーと手順書	・経営層がインシデント対応の必要性を意識する。 ・インシデントレスポンスの手順を決め、書類等にまとめる。 ・サーバを調査するコマンド表や、チェックリストなどを作成する。 ・インシデントの検知、調査を可能とするシステムや運用の環境を作る。
②CSIRT	・インシデントレスポンスチームを構成する。 ・組織で発生するIT事故＝インシデントに対応するチーム。
③外部組織との連携	・インシデント対応には、組織方針に沿った活動や外部との連携が必須。 ・公的機関、政府、協力会社など関連組織との連携を意識した準備をする。
④訓練	・インシデントを体験しておき、いざというときも対応できるようにする。 ・突然のインシデントに対応できるよう準備も兼ねた訓練を行う。

Phase2：検知と分析

インシデントの兆候を検出し、インシデントであるかどうかの分析を行う

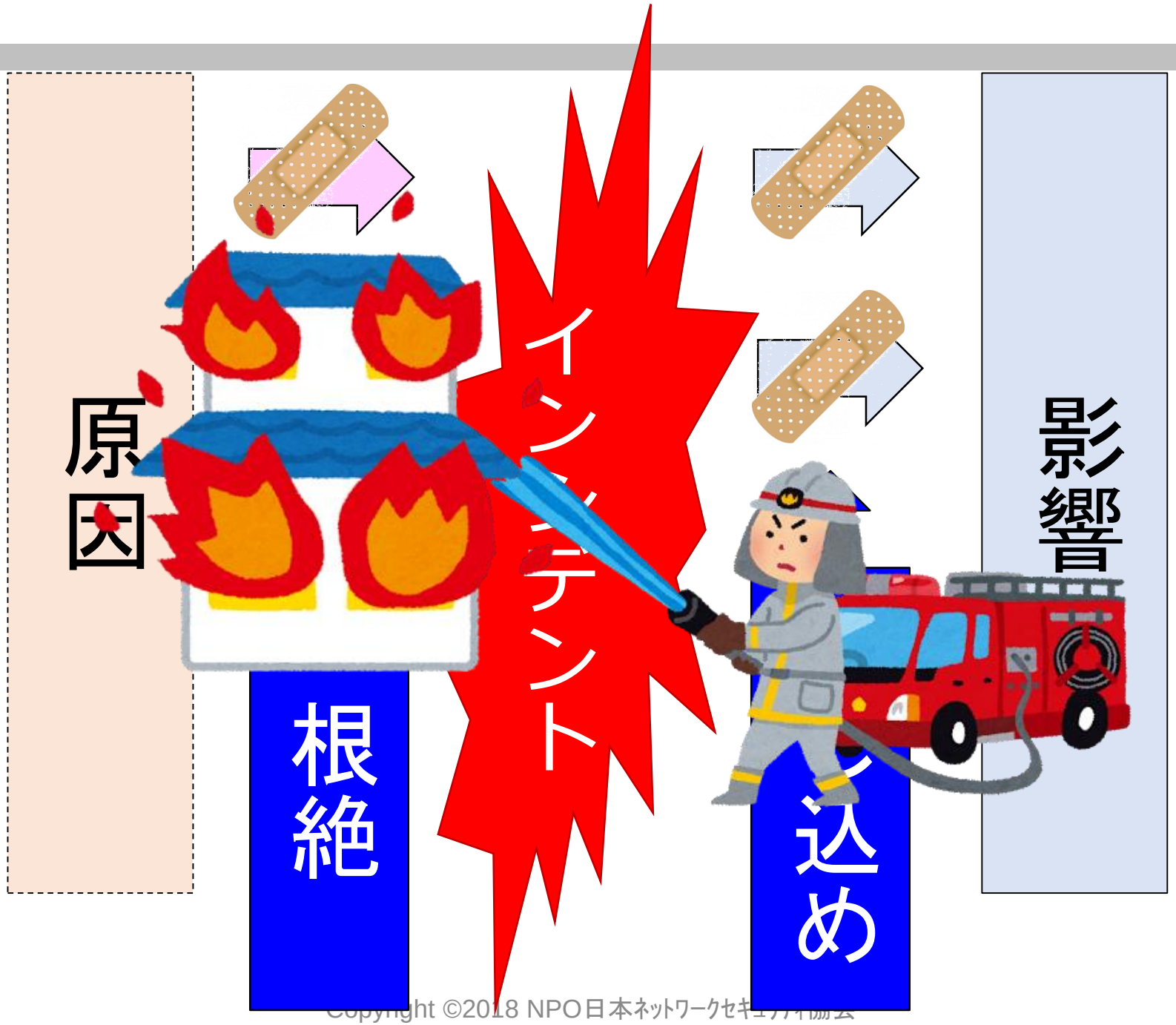
①検知	・イベントを検知。 ・システム、ログ、通報などでインシデントの兆候に気づく。
②分析	・検知した内容を確認し、本物のインシデントか誤検知かどうかを調べる。 ・どのようなインシデントであるかを分かる範囲で調査。 ・被害が出ていれば、次の封じ込めフェーズに移行。

Phase3：封じ込め、根絶、復旧

被害を最小化し、原因を調査した後に業務機能やシステムを復旧する

①封じ込め	・封じ込めをするためどのような原因であるかを調査。 ・システム、ネットワーク、パソコンを一時的に停止する。 ・停止の際には停止の影響と、調査のための証拠が消えないよう注意すること。 ・取引先、顧客、社内に対して、インシデントの発生を知らせる。
②根絶	・インシデントの原因を詳細に調査。 ・被害状況を詳細に調査。 ・今回のインシデントの原因となった箇所を修復する。 ・修復箇所が正しく修復されていることを確認。 ・所轄官庁、警察等に連絡、通報。
③復旧	・修復を終えたシステムを再開。 ・データの復旧等。 ・取引先、顧客への連絡。 ・Webサイト等にインシデントの顛末、復旧の旨を掲載。

封じ込めと根絶の対策ポイント



Phase4：事件後の対応

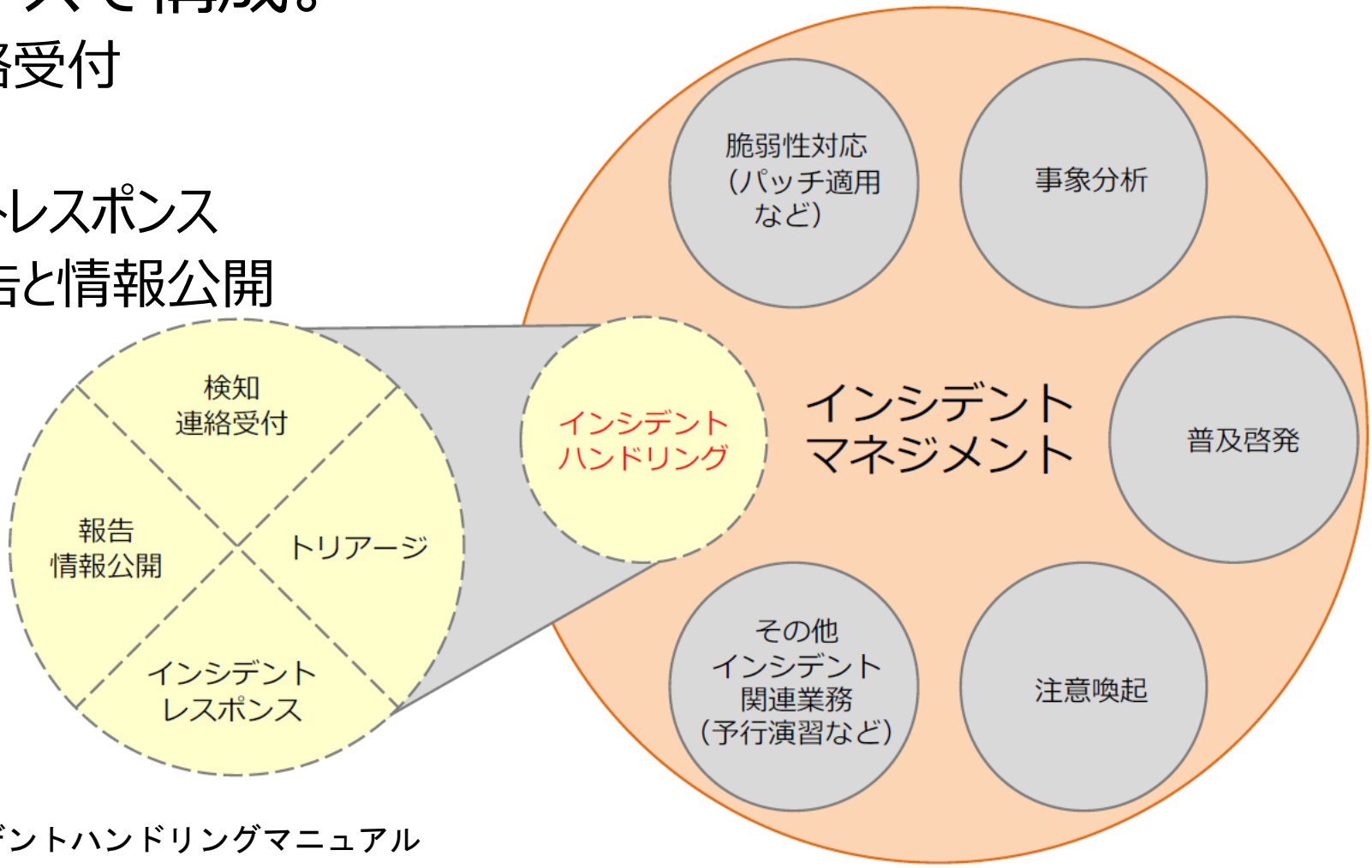
インシデントから学習し、再発防止のための改善を行う
【事前対処（インシデントレディネス）】

①教訓	・インシデントから教訓を学ぶ。 ・すべての関係者が参加して「反省会」を開催する。 ・新しい脅威に対して進化し、技術を向上させる。
②事件データの利用	・各事件に関する客観的なデータと主観的なデータの収集。 ・体系的なセキュリティの弱点や脅威、事件の動向の変化把握。 ・リスク評価プロセスへの還元。 ・追加のコントロールの選択と実施への応用。
③証拠の保管	・事件の証拠の保管期間のポリシーを確立。 ・すべての証拠を保管。

参考資料はTPOで使い分け
JPCIRT/CC 「インシデントハンドリング」

インシデント発生時の対応全般。
4つの業務フェーズで構成。

1. 検知と連絡受付
2. トリアージ
3. インシデントレスポンス
4. 事後の報告と情報公開



出典：JPCERT/CC　インシデントハンドリングマニュアル

インシデント対応マニュアルのポイント

インシデント対応マニュアル

1. インシデント対応する人及び部署の明確化
2. インシデント発生前の準備
   - ① インシデント対応に必要な連絡先の確保
   - ② 各種規則の把握と整合性の確認
   - ③ インシデント対応に有効なツールの利用

3. インシデント対応フロー
   - ① インシデントの発見及び報告
   - ② インシデントに対する初動対応
   - ③ インシデントに関する告知
   - ④ インシデントの抑制措置と復旧
   - ⑤ インシデントの事後対応

出典：JPCERT/CC

CSIRTのまとめ

CSIRT活動{組織間の協力×(事前対処＋事後対処)}

① 対外的な連絡窓口であること
② 技術的な問合せに関して対応が可能であること
③ インシデントレスポンス(事後対処)だけではなく、インシデントレスポンスなどの実践的な活動経験を元に、インシデントレディネス(事前対処)を進めていること
④ 部署間を横断した組織体制をとっていること

■ ■ ■ 本日のメッセージ ■ ■ ■
“CSIRT”と名乗らなくていい！
インシデント対応ができる体制づくりはしておこう！

安心してビジネスに
取り組める組織づくりを！！