20th Anniversary

JPCERT CC®

高度サイバー攻撃への備えと対応

JPCERT コーディネーションセンター
洞田慎一

Agenda

- **はじめに**
- **高度サイバー攻撃**
  —標的型メールとマルウエア感染だけではない
- **組織における攻撃への備え**
- **まとめ**

はじめに

JPCERT/CCとは

一般社団法人　JPCERTコーディネーションセンター

Japan Computer Emergency Response Team Coordination Center
ジェーピーサート コーディネーションセンター

- 日本国内のインターネット利用者やセキュリティ管理担当者、ソフトウエア製品開発者等（主に、情報セキュリティ担当者）がサービス対象
- コンピュータセキュリティインシデントへの対応、国内外にセンサをおいたインターネット定点観測、ソフトウエアや情報システム・制御システム機器等の脆弱性への対応などを通じ、セキュリティ向上を推進
- インシデント対応をはじめとする、国際連携が必要なオペレーションや情報連携に関する、我が国の窓口となるCSIRT（窓口CSIRT）

CSIRT: Computer Security Incident Response Team

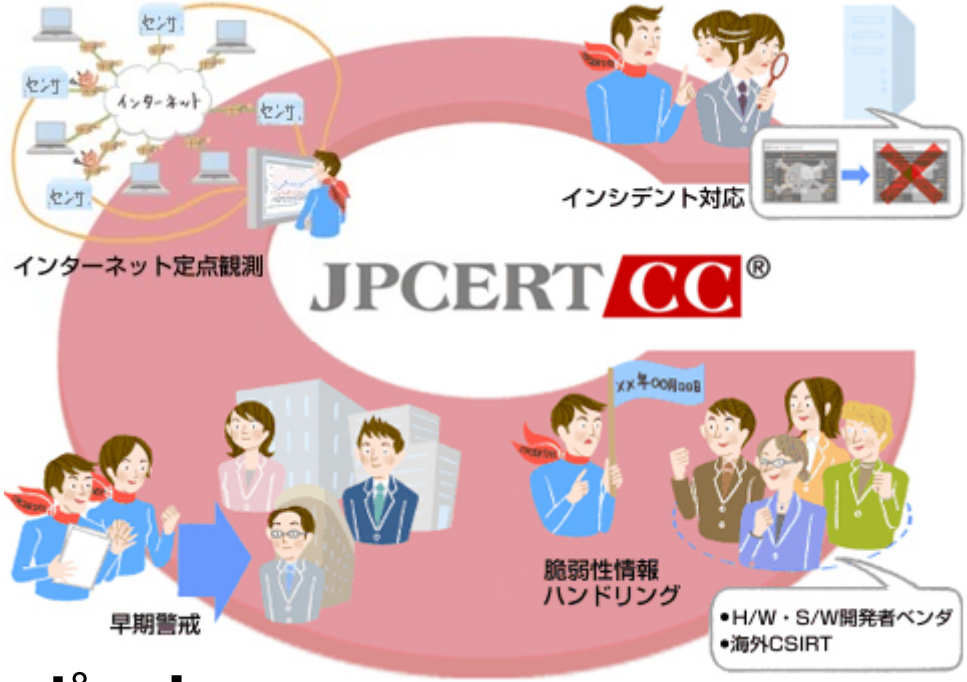
※各国に同様の窓口となるCSIRTが存在する(米国のUS-CERT、CERT/CC、中国のCNCERT、韓国のKrCERT/CCなど)

- 経済産業省からの委託事業として、サイバー攻撃等国際連携対応調整事業を実施

JPCERT/CC の活動

■ コンピュータセキュリティインシデントへの対応

―報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言など



■ 公開情報・レポート

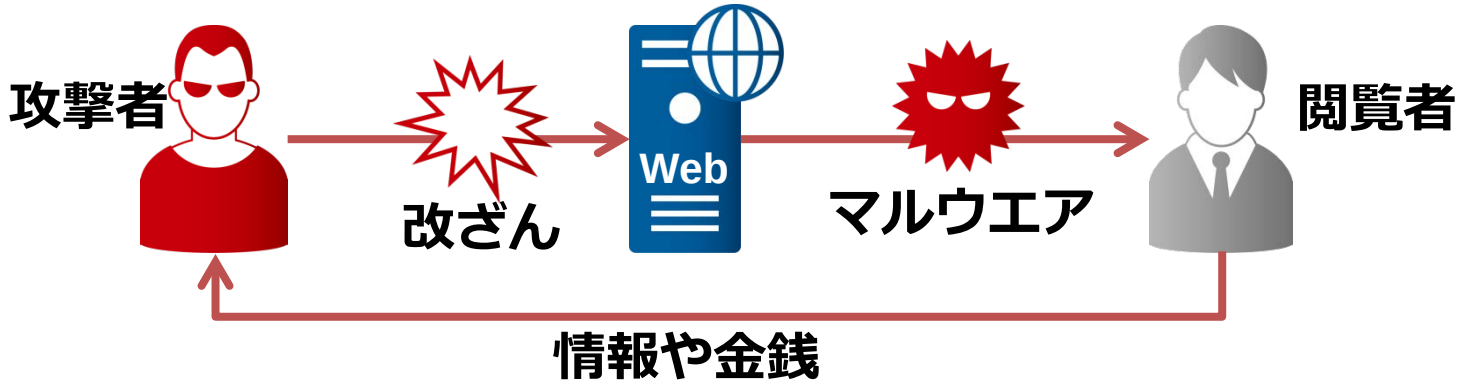
―注意喚起、JVN、インシデントレポート、定点観測レポート等

インシデントとは

- コンピュータセキュリティインシデント・・・
  - **―コンピュータセキュリティに関わる事象（事件・事故）**

    例）■ウイルスに感染した
    ■ウェブサーバが侵入された
    ■フィッシングサイトが立ち上げられてしまった
  - **―必ずしも自組織だけが被害をこうむるとは限らない**

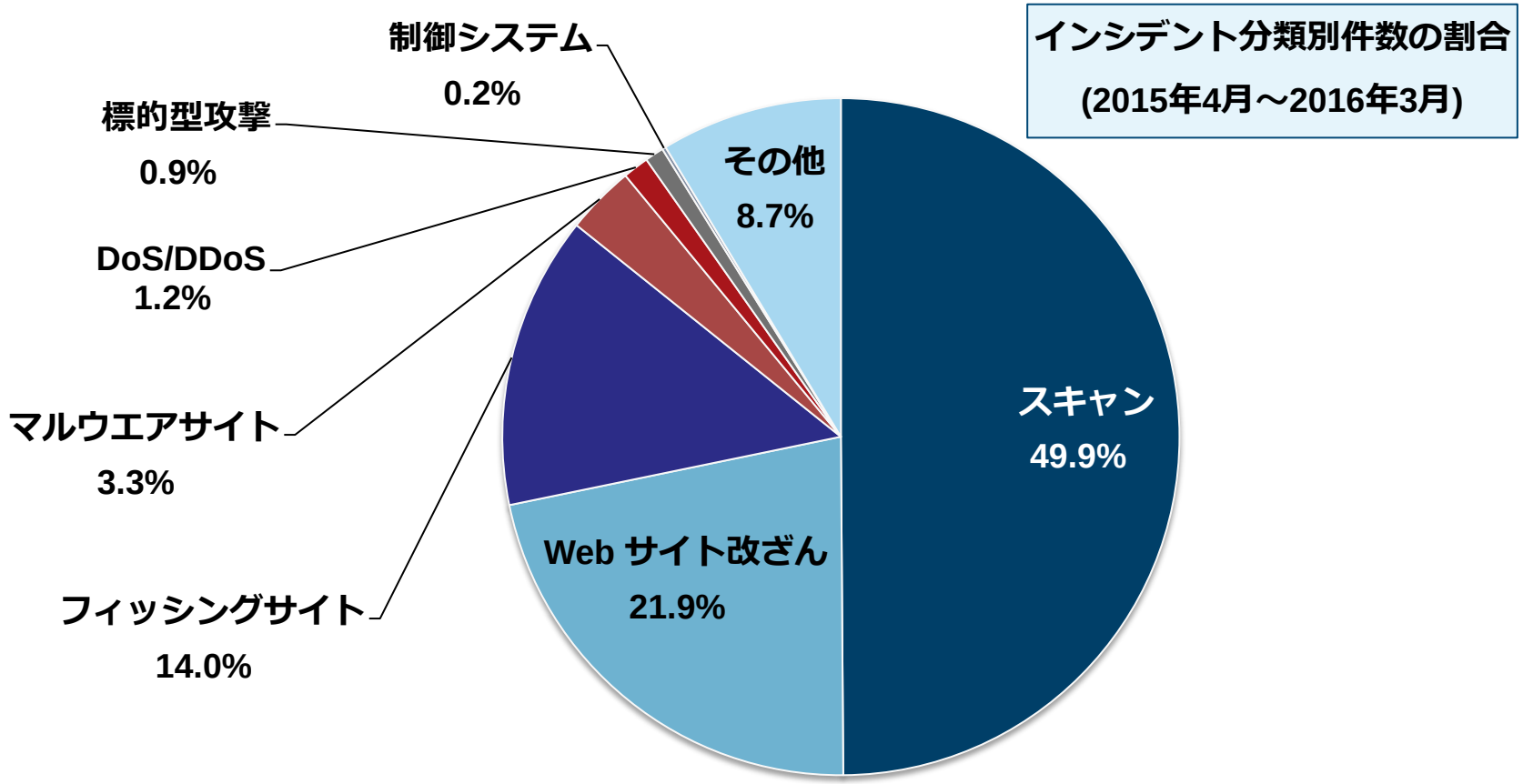
    例）■ウェブサーバに侵入され、マルウエア感染を拡大させてしまった



環境変化を背景に、企業のリスクは多様化し、
情報資産を巡るトラブルも頻発

インシデントの発生状況

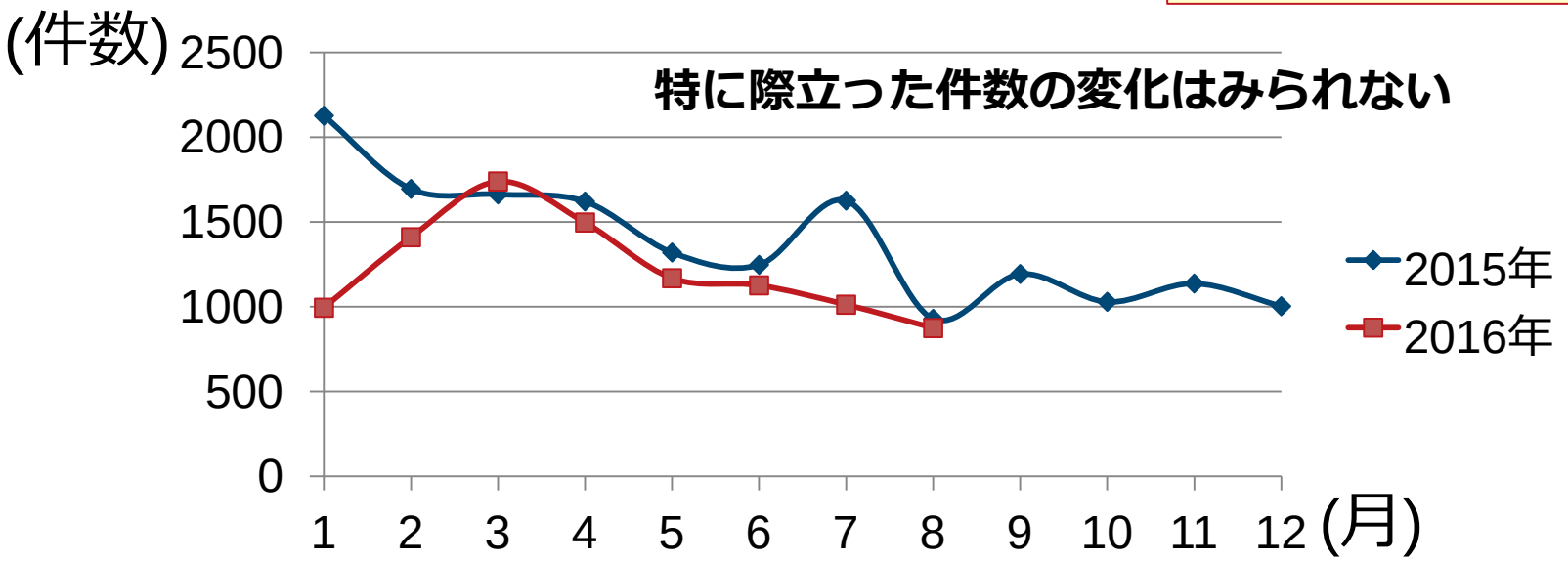
- **様々なインシデントが発生しています**
  - —年間 20,000件近くのインシデントが報告されます
  - —インシデントが発生した時、対応や備えはできていますか？



インシデント動向 (2016年)

■ インシデント件数の推移

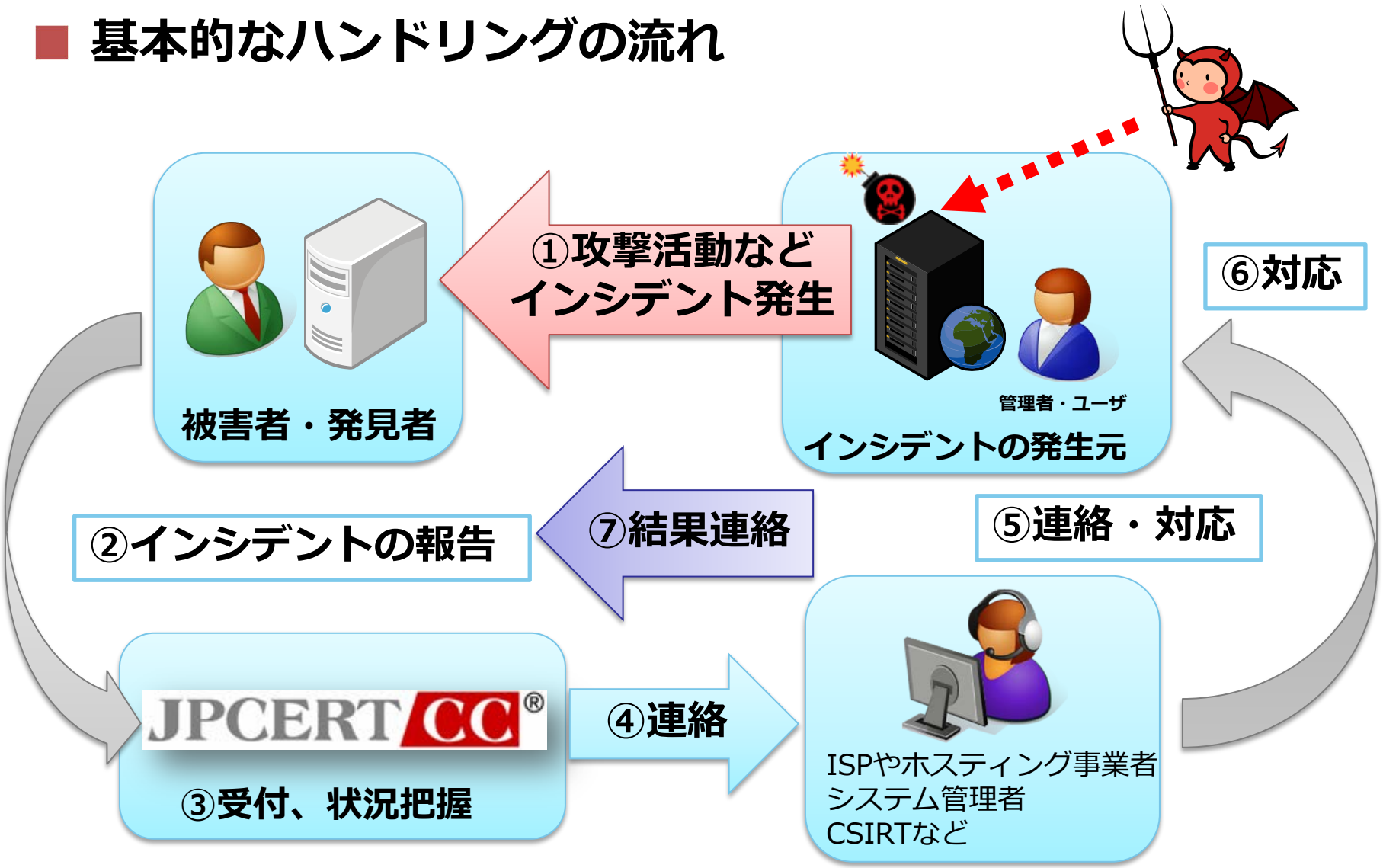
インシデント報告対応四半期レポート
http://www.jpcert.or.jp/ir/report.html



- インシデント件数に大きな変化はみられない・・・
  備えや対策が行き渡っていない可能性も
- いざというときに、慌てずに対応できますか？
  対策には事前の準備が肝要です

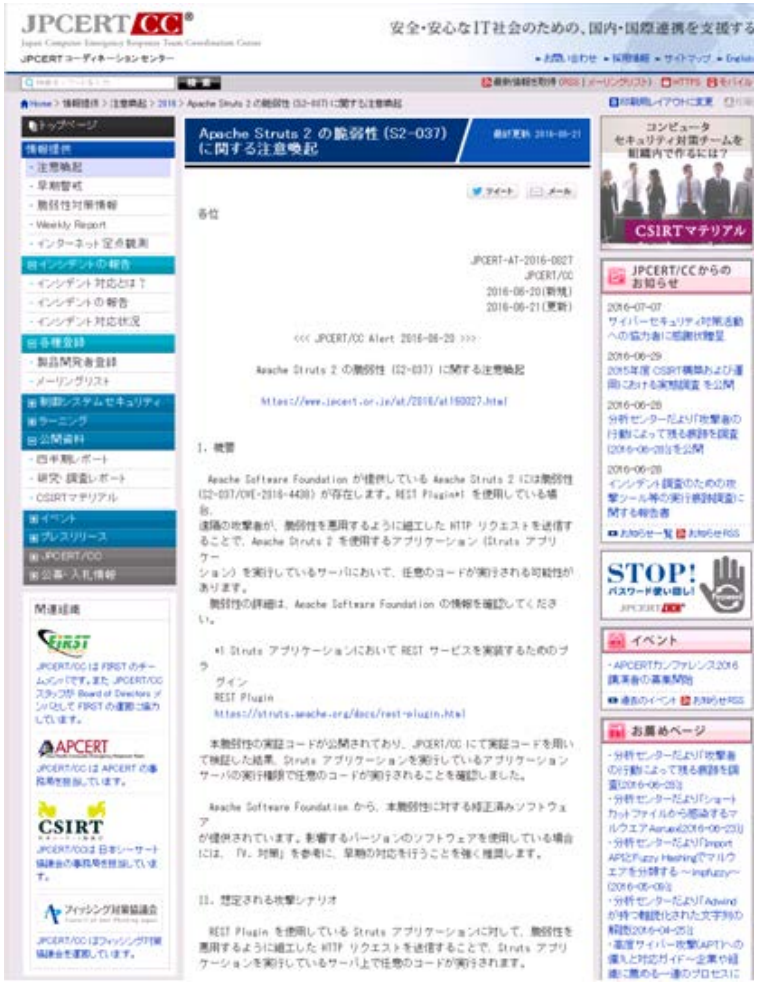
JPCERT/CC におけるインシデント対応

基本的なハンドリングの流れ



インシデントを知る・情報を得る

- **JPCERT/CC の活用**
  - —注意喚起、早期警戒情報
  - —脆弱性対策情報 (JVN)
  - —Weekly Report
  - —各種レポート
    - インシデント報告対応四半期レポート
    - ソフトウエア等の脆弱性関連情報に関する届出状況
    - インターネット定点観測レポート
    - 活動四半期レポート
  - —参考ドキュメント
- **まずは、お気軽にご相談ください**



https://www.jpcert.or.jp/

参考資料

- **高度サイバー攻撃への対処におけるログの活用と分析方法**

  https://www.jpcert.or.jp/research/apt-loganalysis.html
  攻撃を受けて侵入された場合に記録されるログについて解説をまとめた資料

- **高度サイバー攻撃(APT)への備えと対応ガイド～企業や組織に薦める一連のプロセスについて**

  https://www.jpcert.or.jp/research/apt-guide.html
  企業や組織においてAPT対策や活動目標を検討する際に参考となる情報をまとめた資料

- **2015年度 CSIRT構築および運用における実態調査**

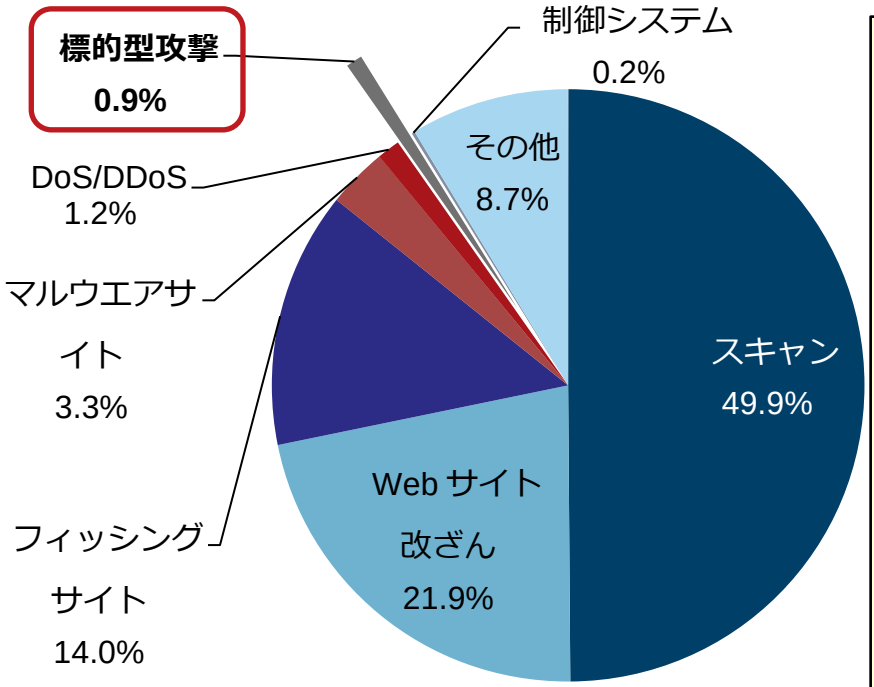
  https://www.jpcert.or.jp/research/2015_CSIRT-survey.html
  各組織でのCSIRTにアンケート等を行った結果をまとめた資料

高度サイバー攻撃

高度サイバー攻撃とは何か？

- **特定の組織を狙った情報窃取や、システム破壊を主な目的とする執拗な攻撃**
  - 標的型攻撃、APT と呼ばれることも
  - 2015年、特にこのタイプの攻撃について、社会的に注目されるようになりました

インシデント分類別件数の割合(2015年度)



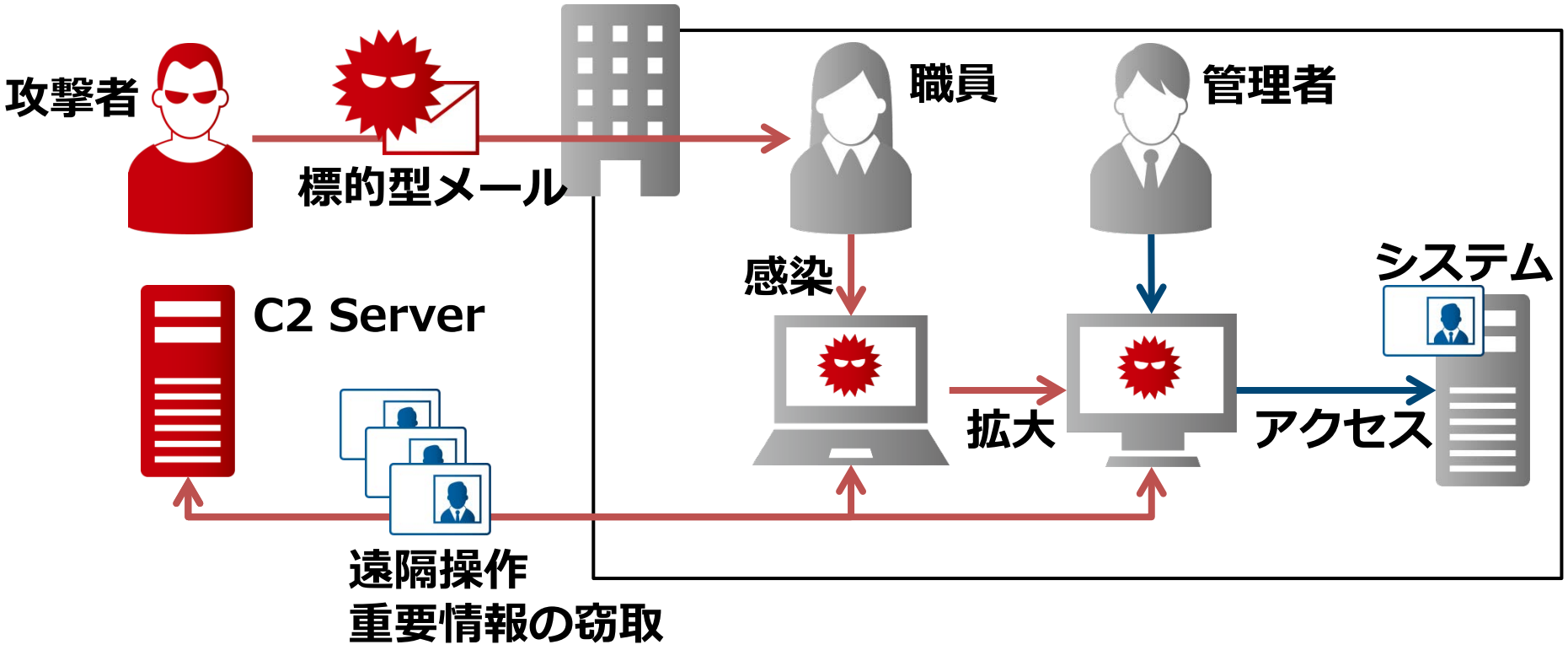
数年前から継続的に、多数の組織において高度サイバー攻撃による被害が生じています

144組織に通知　(2015年度)

JPCERT/CC インシデント報告対応レポートより
https://www.jpcert.or.jp/ir/report.html

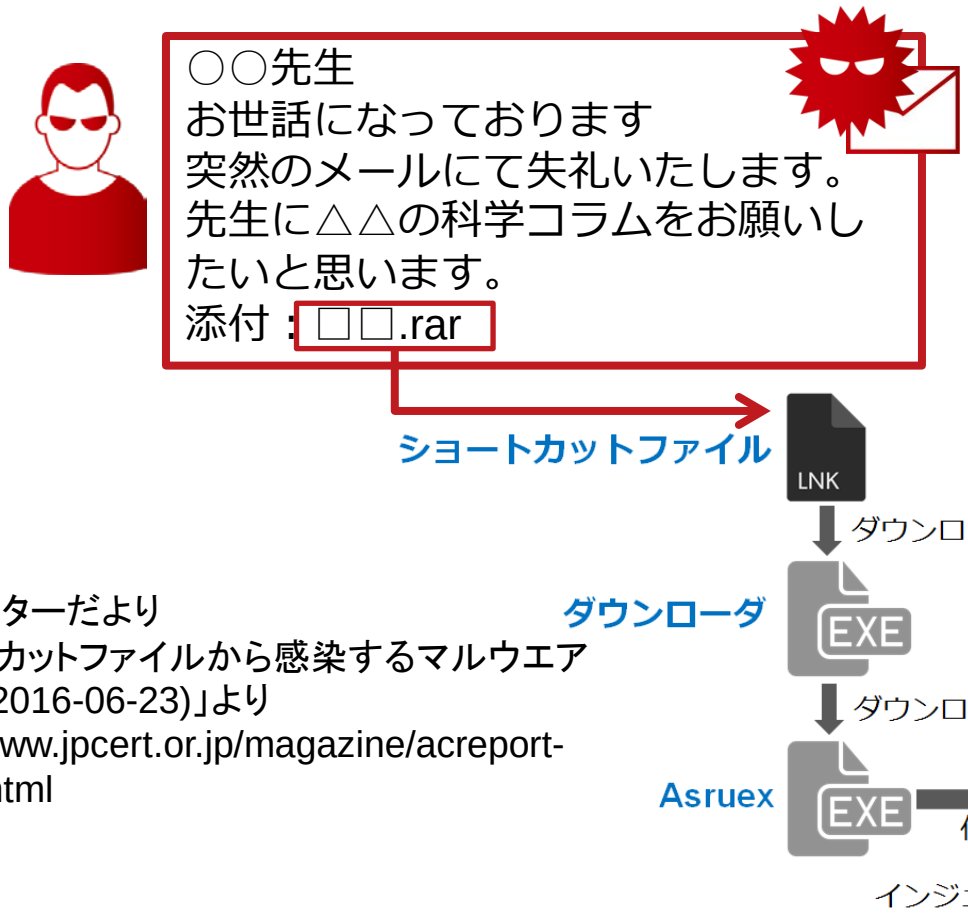
攻撃の典型的な流れ

- 典型的な標的型攻撃
  - 標的型メールによって遠隔操作型のマルウエアに感染
  - 組織内のネットワーク (LAN) を介して、他の PC へ移動
  - ファイルサーバ上の個人情報を窃取



標的型メールによる侵入経路

- 特定の組織や個人宛にカスタマイズされたメール（標的型メール）が感染のきっかけになることも
- **ショートカットファイルから感染するマルウエアAsruex**



加工されたJPGまたはGIFファイル

分析センターだより
「ショートカットファイルから感染するマルウエアAsruex(2016-06-23)」より
https://www.jpcert.or.jp/magazine/acreport-asruex.html

標的型メール

■ 【参考】「標的型攻撃メールの例と見分け方」

— https://www.ipa.go.jp/files/000043331.pdf

表 2-2　標的型攻撃メールの着眼点と本書の各節の対応表

節番号、及びページ番号 / 着眼点		標的型攻撃メールの例							添付ファイルの種類			
		2.2.1 P.7	2.2.2 P.8	2.2.3 P.9	2.2.4 P.10	2.2.5 P.12	2.2.6 P.13	2.2.7 P.14	2.3.1 P.16	2.3.2 P.19	2.3.3 P.19	2.3.4 P.20
(ア)	① 知らない人からのメールだが、メール本文の URL や添付ファイルを開かざるを得ない内容	●	●	●								
	② 心当たりのないメールだが、興味をそそられる内容											
	③ これまで届いたことがない公的機関からのお知らせ				●							
	④ 組織全体への案内											
	⑤ 心当たりのない決裁や配送通知					●						
	⑥ ID やパスワードなどの入力を要求するメール						●	●				
(イ)	① フリーメールアドレスから送信されている	●	●	●	●	●	●	●				
	② 差出人のメールアドレスとメール本文の署名に記載されたメールアドレスが異なる		●	●								
(ウ)	① 日本語の言い回しが不自然である							●				
	② 日本語では使用されない漢字が使われている	●										
	③ 実在する名称を一部に含む URL が記載されている				●							
	④ 表示されている URL と実際のリンク先の URL が異なる				●							
	⑤ 署名の内容が誤っている											
(エ)	① ファイルが添付されている	●	●	●		●			●	●	●	●
	② 実行形式ファイルが添付されている									●		
	③ ショートカットファイルが添付されている											●
	④ アイコンが偽装されている									●		●
	⑤ ファイル拡張子が偽装されている											

■ 例：日本年金機構(2015/5)

— 「厚生年金基金制度の見直しについて（試案）」に関する意見

— 給付研究委員会オープンセミナーのご案内

— 厚生年金徴収関係研修資料

— **【医療費通知】**

>本メールは、保険を利用して診察や診療を受けられた方に、医療費をお知らせしています。
>Windows-PCで開けてください。

極めて精巧に文面が作成されていることもあり、「不審メールを見極めて開かないこと」が難しいケースもある

近づく方法はメールとは限らない

- SNS による“やりとり型“標的型攻撃 (メッセンジャー)

□□さん
○○社の、△△と申します。
○□について、□□さんのお考えをお聞かせ願いたいと考えております。

△△さん
私ごときに目を向けていただきありがとうございます。
どうぞ、いらしていただいて大丈夫です。

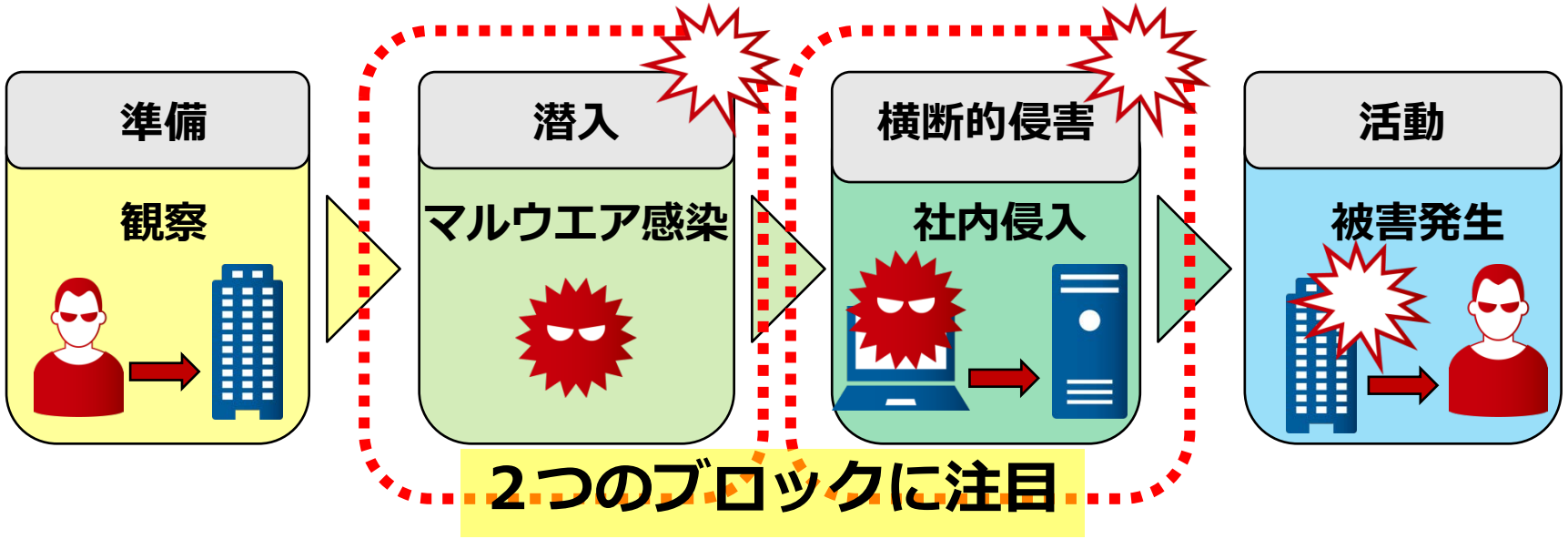
□□さん
ご訪問させていただく際に使う、内容と計画をご送付しますので、どうぞご覧ください
添付：説明書.msg

“説明書.msg”ファイルを開くとマルウエアに感染する。攻撃者は、執拗に PC の Outlook 上で添付ファイルを開くように促し続ける。

高度サイバー攻撃を考える

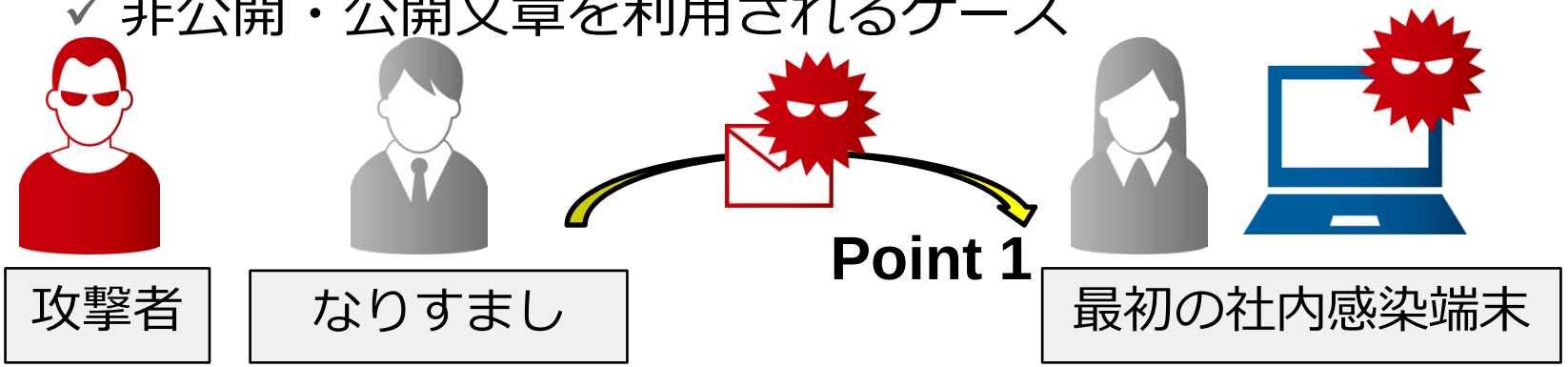
サイバーキルチェインモデル

- ✓ **高度サイバー攻撃は、複合的かつ長期**的な攻撃
- ✓ **活動に気が付いた時には、もはや手遅れ**となっていることがほとんどです
- ✓ 一つのインシデントとは捉えず、**いくつかのインシデントが複数連鎖している**と考えましょう
- ✓ **各段階で注意することが異なります**



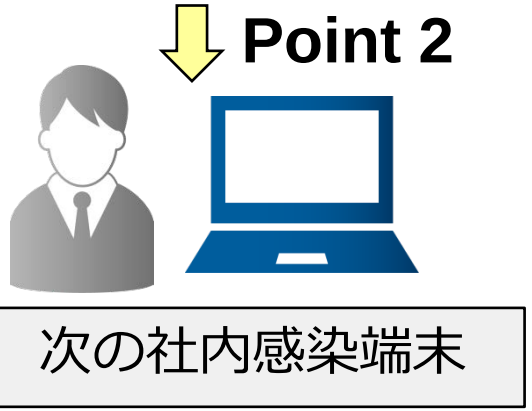
【“潜入”段階】標的型メールのポイント

- **巧妙になりすますことで、感染を誘導**
  - ✓ 業務上開いてしまいそうなメール
  - ✓ 非公開・公開文章を利用されるケース



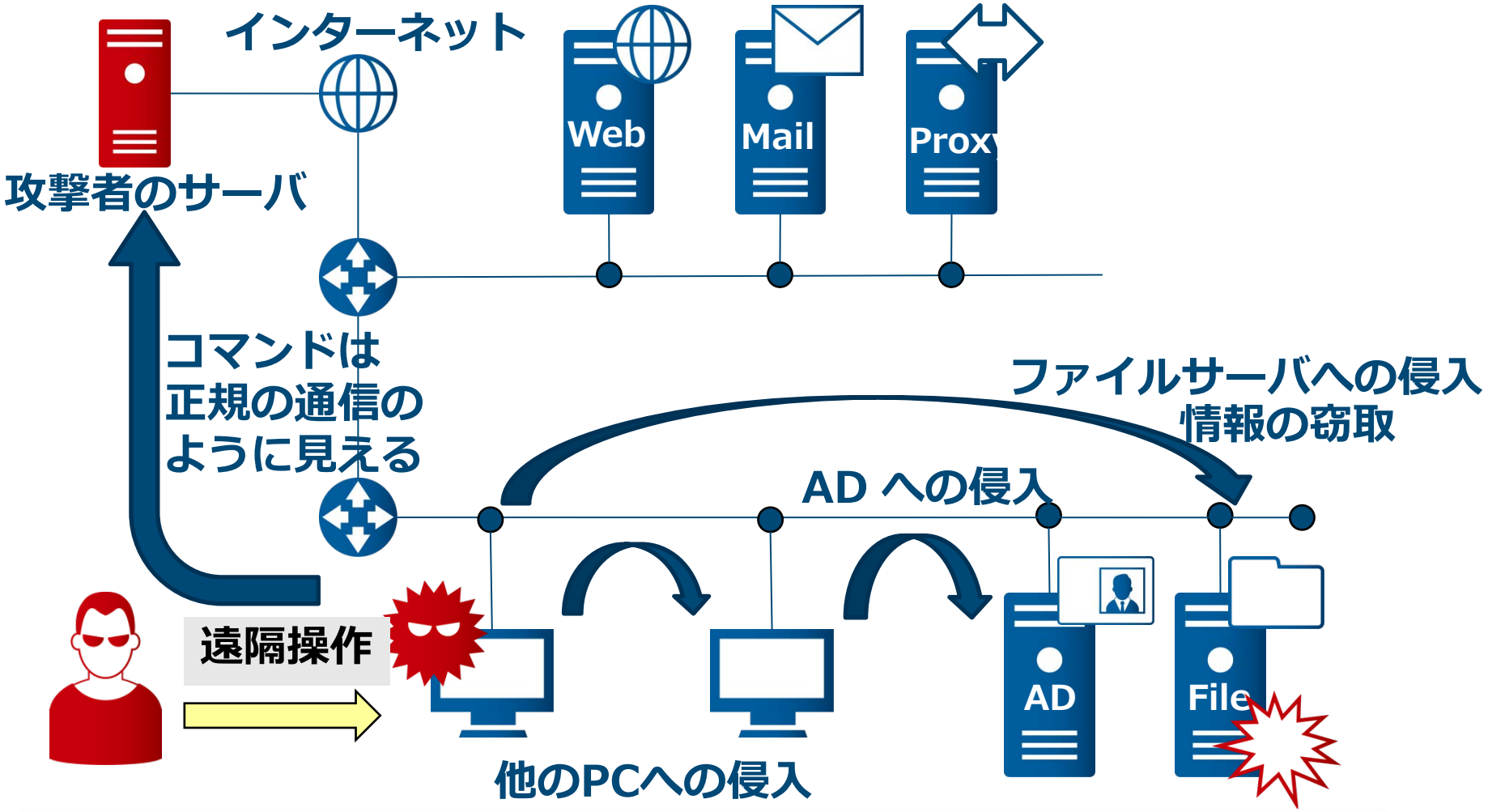
Point 1：開いたときの影響を軽減
インターネットゾーン ID の活用
社外アドレスの利用の制限

Point 2：業務端末のネットワーク分離
ネットワークの分離、記録



標的型メールだけではなく、マルウエアへ感染しにくい環境が重要

【“横断的侵害”】マルウエア感染した後の動き



- ✓横断的移動は、組織内にある感染 PC を利用
- ✓権限の付与や、システムの分離、ログ分析が重要

組織における攻撃への備え

重要な対策は「守るべきものは何か」を定めること

- **「守るべきものは何か」を見定める**
  - —失っては困るもの
  - —リスクアセスメントを行う

- **「失ったらどれだけの損失があるか」を見定める**
  - —インシデント発生時に、いったいどれだけの損失が発生するか？
  - —事後への対応：リスクファイナンスという考え方
    - リスクコントロール：予防的措置
    - リスクファイナンス：事後に備える対策

- 例：日本年金機構での101万人の情報漏えいに対して、６月の専用電話窓口の費用だけで３億円
  - —一つのインシデントが、組織に大きな影響を与えてしまう

インシデントが発生してしまったとき

リスク・コストへの対応

—紛失、誤操作、管理ミス、不正アクセス等の様々なインシデント

2015年個人情報漏えいインシデント概要データ【速報】（JNSA)

漏えい人数	496万0063人
インシデント件数	799件
想定損害賠償総額	2541億3663万円
一件あたりの漏えい人数	6578人
一件あたり平均想定損害賠償額	3億3705万円
一人あたり平均想定損害賠償額	2万8020円

[出典] JNSA, 2015年情報セキュリティインシデントに関する調査報告書【速報版】


観光庁の有識者会議、ＪＴＢの情報流出防止策を評価　九州誘客
商品の販売も容認へ

ＪＴＢの個人情報流出問題を受け、観光庁は８日、再発防止策を検討する有識者会議の初会合を開いた。委員らはシステムの強化など２ＪＴＢが取った対策について「当面必要な安全措置が講じられている」との評価で一致。観光庁は、九州観光振興のため国が助成する割安旅行商品「九州ふっこう割」のインターネット販売をＪＴＢに認める方向で検討する。

会議の冒頭、観光庁の田村明比古長官は「最大手の企業で情報流出が発生したことを深刻に受け止め、業界全体として今後どのように対応していく必要があるか考える必要がある」と述べた。

会議は、情報セキュリティーやサイバー犯罪に詳しい専門家ら６人がメンバー。会合では「システム管理担当者の経験不足が課題」「本社とグループ会社との情報共有に問題があった」といった指摘が出た。さらに議論を積み、今月中の再発防止策の取りまとめを目指す。

関連ニュース

■ 個人情報流出対策で国交省が有識者会議　ＪＴＢの大量流出を受けて
■ ＪＴＢ、最大７９３万人分流出か　顧客情報、不正アクセス
■ ７９３万人分の個人情報流出　ＪＴＢ、対応後手に　巧妙な標的メール「機密を十分に認識していなかった」
■ 【ＪＴＢ情報流出】異例の幕切れを狙え、セキュリティー対策をさらに　信頼回復には、再発防止策の実践性が分かりやすく
■ 【ＪＴＢ情報流出】個別案件特定できる情報に見識しへ、「なりすまし」をチェック
■ ＪＴＢ不正アクセス　狙われたネット予約、訪日客も含め「かき入れ時」に打撃

[出典] 産経ニュース, http://www.sankei.com/politics/news/160708/plt1607080028-n1.html

普段からの備えはできていますか？

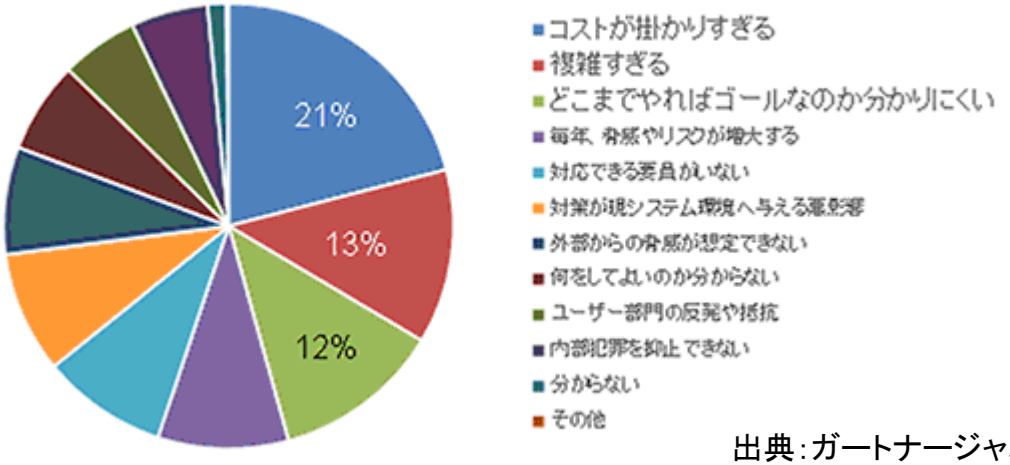
—インシデントへの対応フローは定まっていますか？

セキュリティ対策の現状 (1/2)

■ セキュリティ対策への障壁

— 「コストがかかりすぎる」、「複雑すぎる」、
「どこまでやればゴールなのか解りにくい」

図1．日本企業の情報セキュリティに関する懸念事項



出典：ガートナー／調査：2016年3月（n = 515、複数回答可）

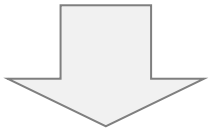
出典:ガートナージャパン, https://www.gartner.co.jp/press/html/pr20160704-01.html

- セキュリティ投資に対するリターンの算出はほぼ不可能
- 経営者がリーダーシップをとって対策を推進しなければ、企業に影響を与えるリスクが見過ごされてしまう

(参考：経済産業省, サイバー経営ガイドライン, http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf)

完全なセキュリティ予防策はない

- **インシデント対応活動**
  - インシデントを検知し、或いはその報告を受けることにより認知し、影響の拡大を防ぐとともに、情報を収集して分析を加え、インシデントの全体像や原因について把握し、復旧措置や再発防止のための措置を取る
- **「コンピュータセキュリティ」で思い描くイメージ**
  - 「いかにしてインシデントの発生を未然に防ぐか」を主眼に置かれることが多い
- **コンピュータセキュリティを取り巻く状況を見ると．．．**
  - 人為的ミス（パッチの適用忘れなど）
  - 未知（公知になっていない）の脆弱性の悪用
  - 技術的な対応の限界　等



インシデントの発生を「完全に回避する」ための予防策はない
（事故前提の対応体制が必要）

（発生確率を低下させ、発生時の影響や被害を低減するための予防策はある）

標的型メール演習、開封率 0%だけではない

■ 「メールを開かない」、「EXE ファイルを開かない」
現実のルールとして実現不可能です
■ 「メールを開いた」、「マルウエアに感染した」
その後、どう行動するかが大切です。

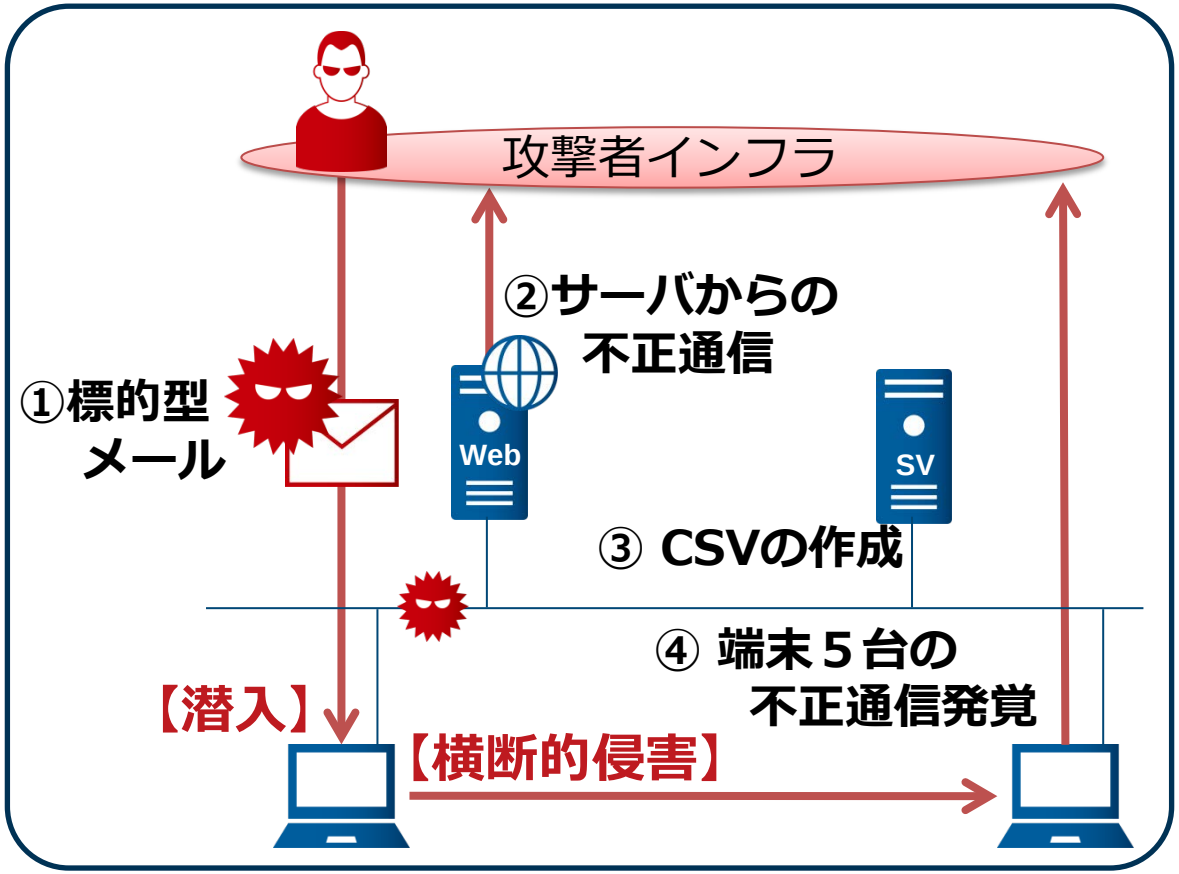
✓ 開封率 0% だから、大丈夫という保証はありません
✓ むしろ、報告率100%を目指しましょう
✓ 何の訓練をしているのか、を意識してください
✓ 訓練であるからこそ、できることがあるはずです

・高度サイバー攻撃への対応能力を向上させるために、組織として何ができるか考えてみてください

・被害を受けた際の対応費用はそれなりに高く、またブランドイメージへの影響は計り知れません

JTB が受けた標的型攻撃（報道等公開情報を基に独自にまとめたもの）

- **概要**
  - **問い合わせ受け付け用代表メールアドレスへ標的型メール**が送られる（「航空券控え / 添付のご連絡 ）
  - **実在する組織名など、内容は自然**だった
  - **定期的なメール訓練を実施**していた



月日（曜日）		主要イベント
3月15日	火	偽装ﾒｰﾙ受信、i.JTB端末がﾏﾙｳｪｱ感染
16日	水	
17日	木	
18日	金	
19日	土	ｻｰﾊﾞｰから不審通信の複数発生を確認の連絡
20日	日	
21日	月	業務上不要なCSVﾌｧｲﾙの作成
22日	火	
23日	水	
24日	木	
25日	金	端末5台の不正通信失敗を確認
26日	土	
27日	日	
28日	月	端末・ｻｰﾊﾞｰのﾏﾙｳｪｱ感染特定
29日	火	
30日	水	
31日	木	削除痕跡のある怪しいCSVﾌｧｲﾙの復元に成功
4月1日	金	委託ｾｷｭﾘﾃｨ会社がこれまでの顛末を顧客に報告

侵入
感染拡大・内部調査
攻撃基盤構築

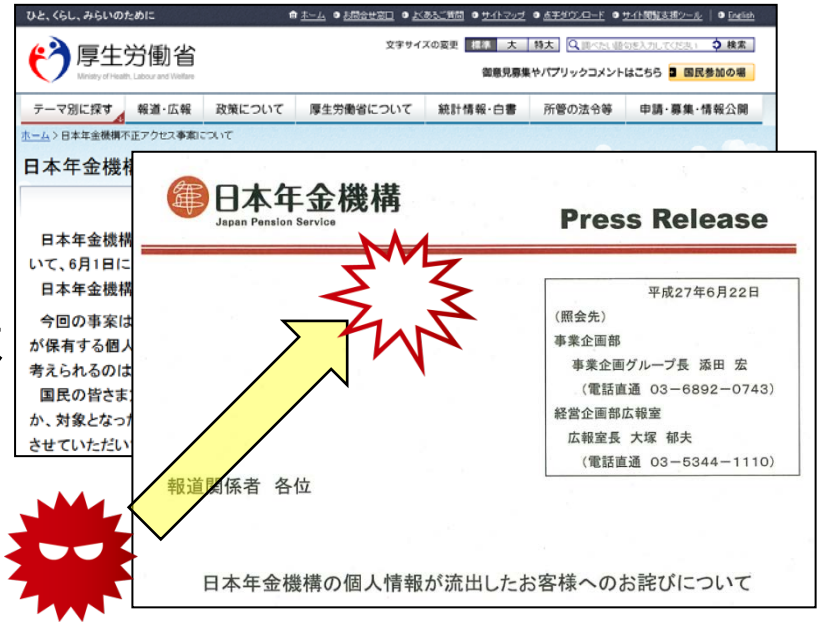
目的遂行、情報窃取

端末5台の不正通信

被害者 or 管理不備の責任

- **組織でインシデントが発生して、被害にあった時**
  - —組織の、管理責任が問われることも

- **例：日本年金機構での高度サイバー攻撃**
  - —対策不足があったにせよ、まったく対策が行われていなかったのではない
  - —現時点において（特に感染時）こうしておけば 100% 防げたとは言えない
  - —顧客の大切なデータを漏えいさせてしまったことへの責任追及



マルウエア感染の被害者ではなく、管理責任を問われる状況へ
しかし、JTB での例を見るように、この教訓は活かされていない

攻撃を受けた後、どう対応するか？

■ 従来のように、「侵入させない」という防御思想では立ち行かない
- ✓ 「侵入されていない」ことが前提の社内システムになりがち
- ✓ 「被害はあってはならないこと」＝「隠す」ことに繋がる

■ 「侵入されること」を認めた防御思想で考える
- ➢ 例１：自宅の防犯対策
  - ■ 空き巣に入られた場合、どう対策しますか
  - ■ これは、ネットワークを防御する上でも同じ発想
- ➢ 例２：おれおれ詐欺の被害に気付いた場合
  - ■ 家族間の符合を決めておくことも対策の一つ
- ➢ 「攻撃を受けることは当然」を認識し、「報告・相談」を

■ 守るべき資産を認識し、必要な対応策を施す
- ➢ 早期検知の為のログ確認
- ➢ インシデント対応のための CSIRT 体制整備

CSIRT とは

■ CSIRT (Computer Security Incident Response Team)

“サイバー攻撃による情報漏えいや障害など、コンピュータセキュリティにかかるインシデントに対応するための組織”

引用：経済産業省「サイバーセキュリティ経営ガイドライン ver 1.0」

■ インシデントに対応する体制とは

- サービス妨害 (DoS 、 DDoS)
- Web サイト改ざん
- マルウエア感染
- 情報漏えい

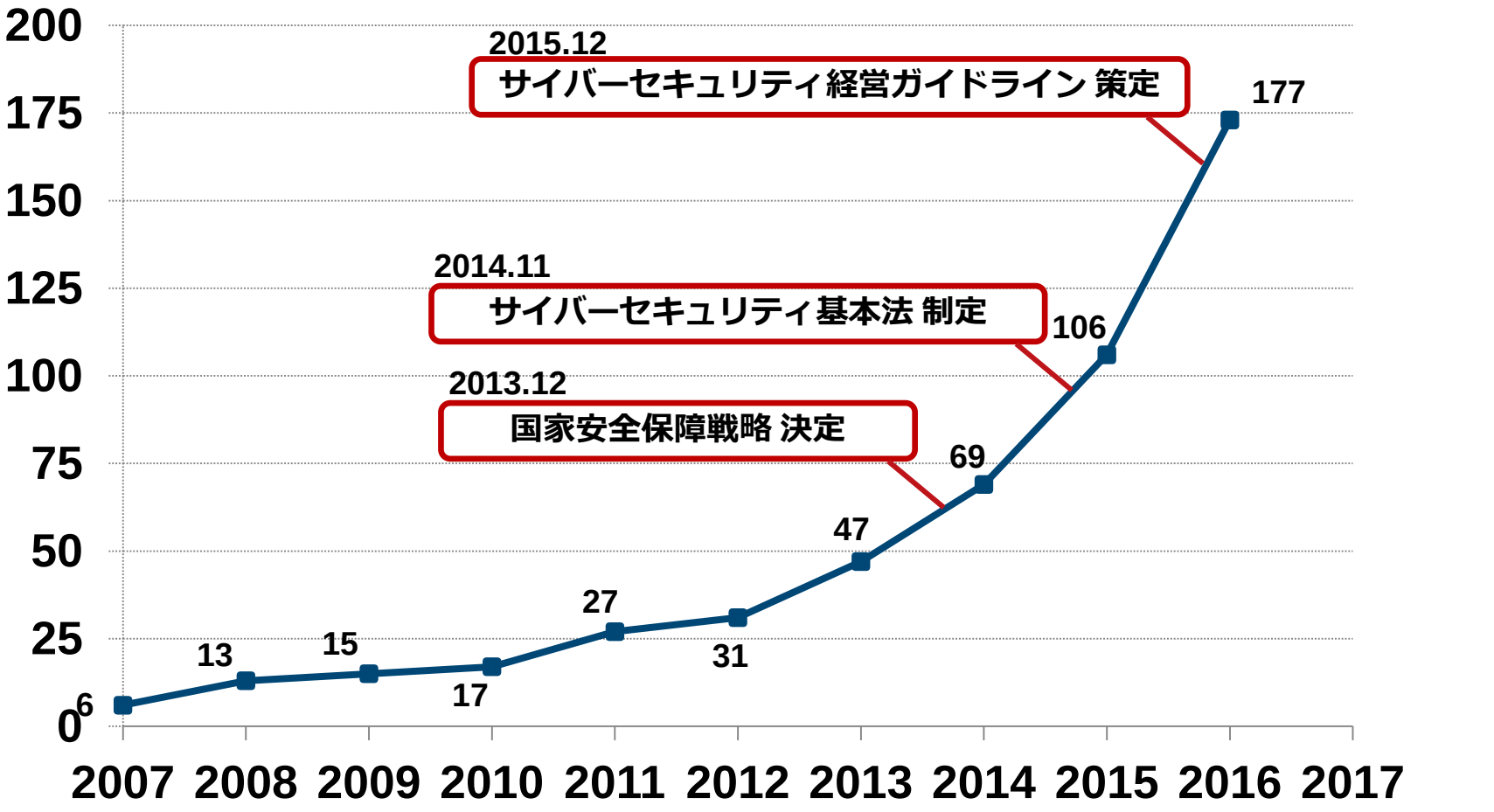
② 組織内での対応
- インシデントのトリアージ
- インシデントの対応
  - 原因分析や対策検討
  - 暫定対応の方針
  - 関係者間の連携調整
- インシデントクローズ

① 発見体制の整備
- 社内環境の整備
- 機器の導入
- 窓口の設置

③ 組織外への対応
- 通報のタイミング
- 顧客や問い合わせへの対応
- プレスリリース

CSIRT 構築推進の動き

■ 日本シーサート協議会の加盟組織数

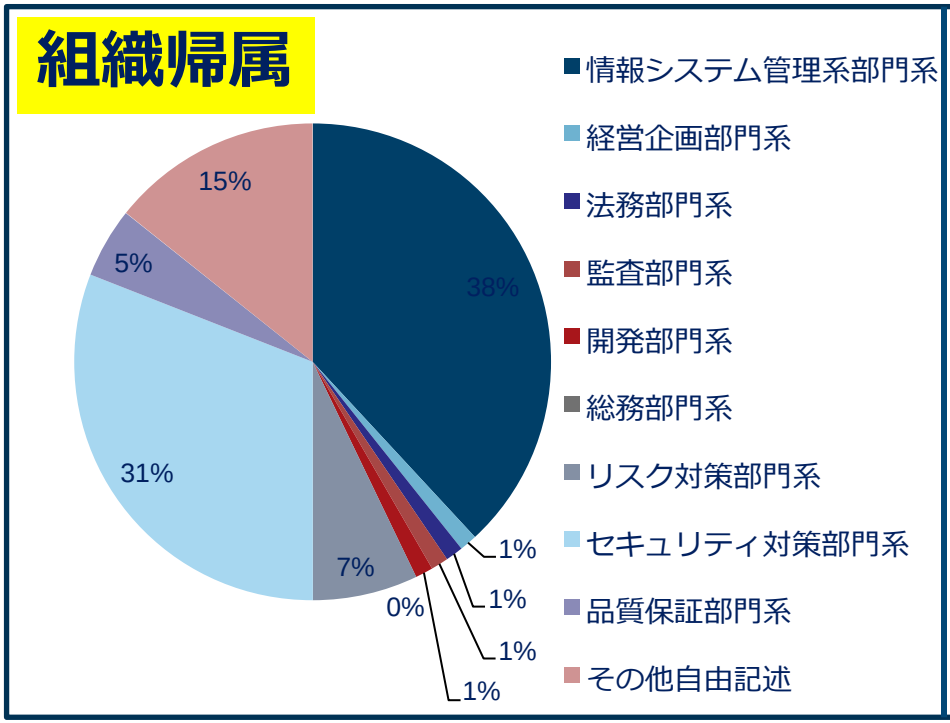


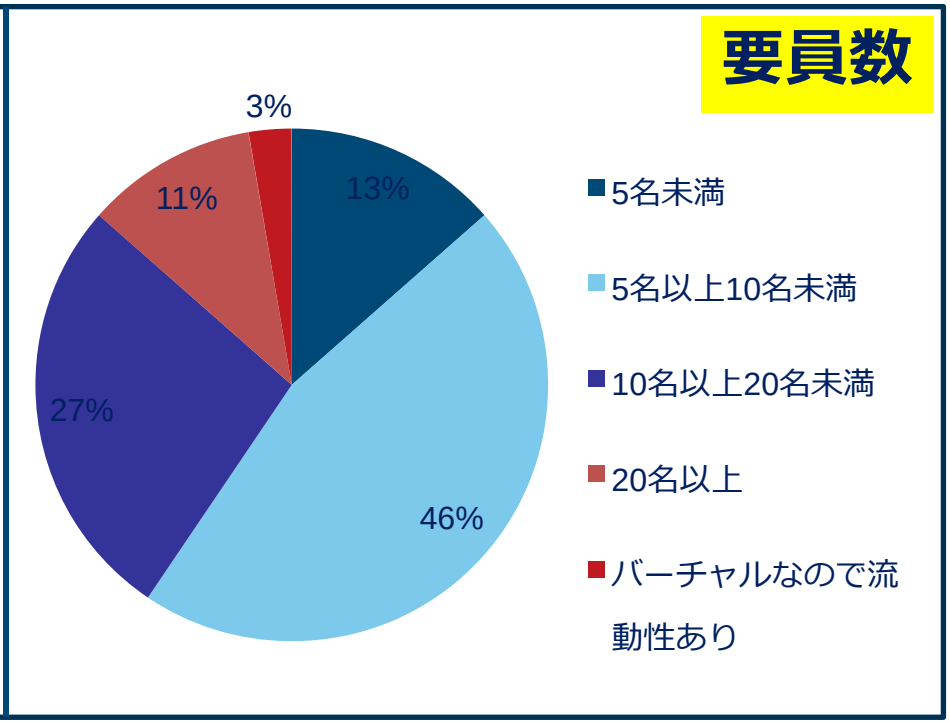
※ 2016/9/1 当時

動く組織内CSIRTを作るコツ 1

JPCERT/CC, 2015年度「CSIRT構築および運用における実態調査」より

CSIRT 組織の組織帰属・要員数





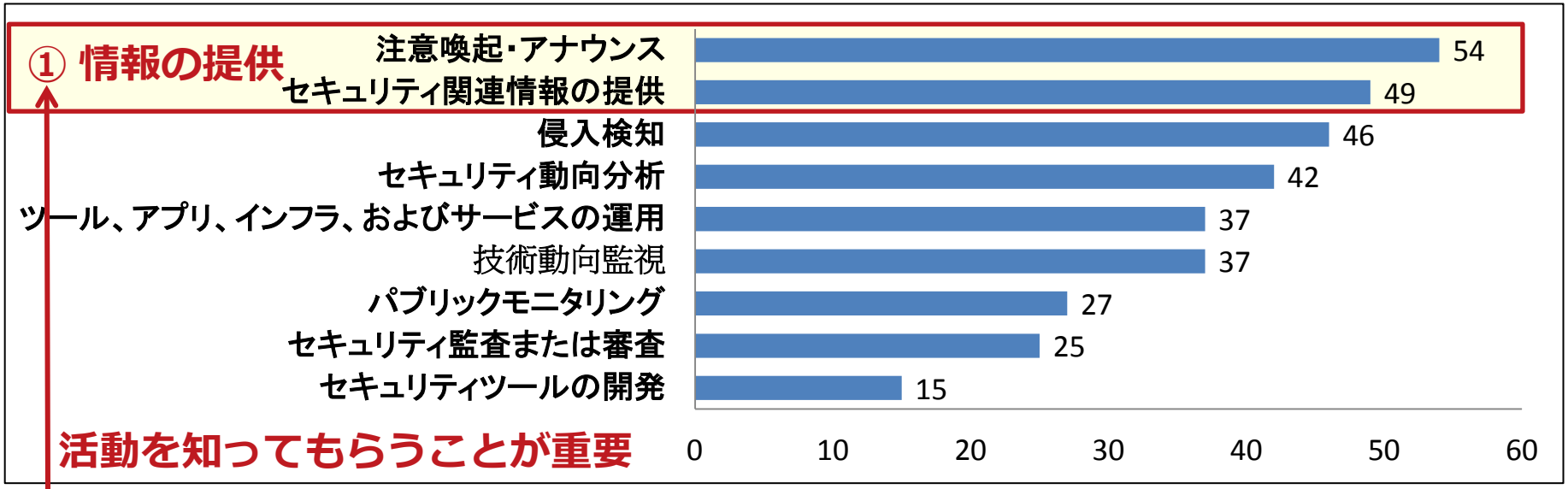
他の CSIRT からみる、“動く” CSIRT を作るコツ：「スモールスタート」

- 情報システム管理系、あるいはセキュリティ対策部門から
- 10名未満の組織が、60% 近くを占める

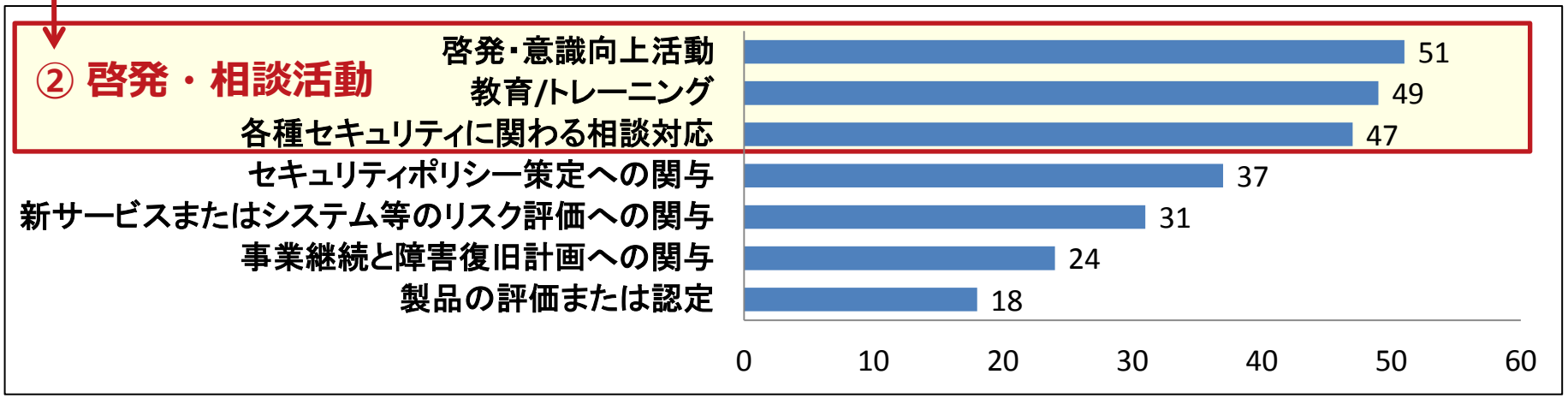
動く組織内CSIRTを作るコツ２

JPCERT/CC, 2015年度「CSIRT構築および運用における実態調査」より

■ CSIRTが提供しているサービス（事前対応サービス）



■ CSIRTが提供しているサービス（セキュリティ品質管理サービス）



CSIRT が提供するサービス範囲

JPCERT/CC, 2015年度「CSIRT構築および運用における実態調査」より

■ 回答した組織の 2/3 以上が提供していたサービス

事前対応サービス		事後対応サービス		セキュリティ品質管理サービス	
1. 注意喚起・アナウンス	54 / 66 (組織)	1. インシデントハンドリング	58 / 66 (組織)	1. 啓発・意識向上活動	51 / 66 (組織)
2. セキュリティ関連情報提供	49 / 66 (組織)	2. アラートと警告	57 / 66 (組織)	2. 教育・トレーニング	49 / 66 (組織)
3. 侵入検知	46 / 66 (組織)	3. ログ分析	56 / 66 (組織)	3. セキュリティ関連の相談	47 / 66 (組織)
		4. 脆弱性ハンドリング	55 / 66 (組織)		

組織内 CSIRT …インシデントや被害を減らす活動を展開

まとめ

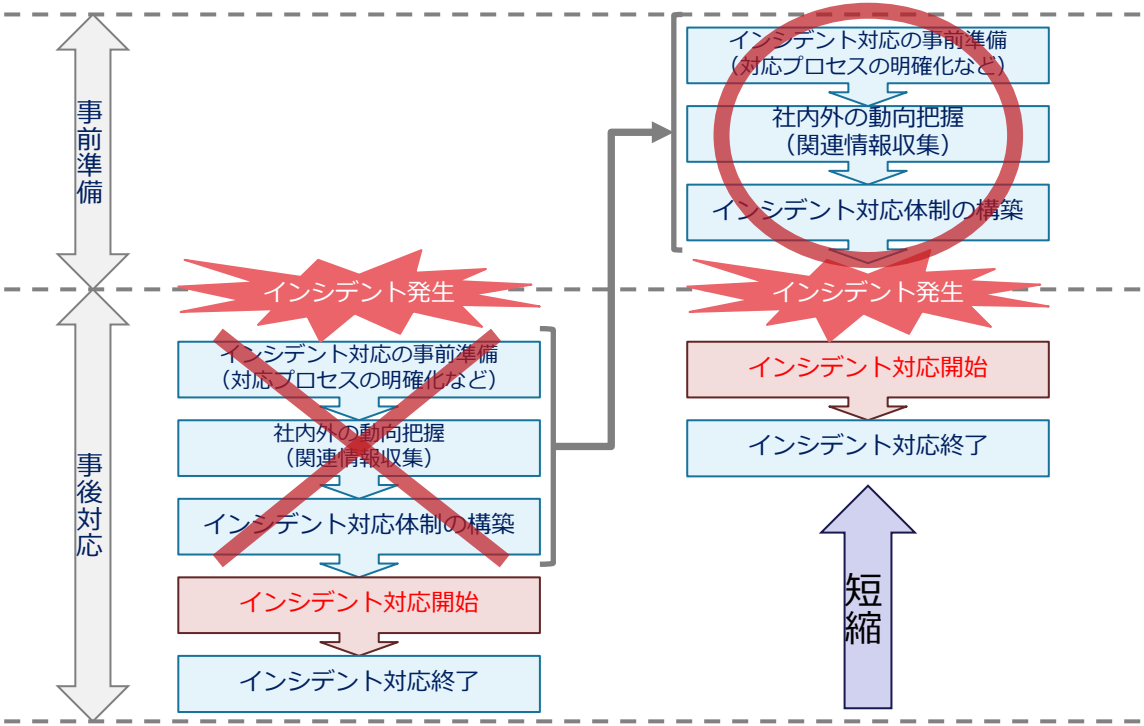
信頼できる窓口を社内に持つことが、対策には必須

- **攻撃を受けていることに気付く**
  - ―ログの定期的な確認や、複数の防御機構を設け検知しやすくする
  - ―外部からの連絡が攻撃を認識するきっかけになる場合が多い
  - ―連絡を受けて、適切に情報をハンドルできる窓口（組織内CSIRTの本質的な機能）を備える必要がある

- **さらに、認識した攻撃について、適切な対応をとるためには、攻撃の性質や実際の被害が発生しているかどうかについての判断も必要**
  - ―判断を可能にするためには事前準備は必須
  - ―一つの組織の情報だけでは判断が難しい場合は情報収集・共有を行い総合的に判断

インシデント発生に備えた事前準備の重要性

インシデント発生後、その対応方法を考え始め、対応体制をとるのは、被害を拡大させる一因となるため、**できるだけ事前に** 対応体制等を整えておくことが肝要



対応体制構築、マニュアル整備に加え、
情報セキュリティに関する”避難訓練(対応訓練)”の実施をご検討ください
事前にできる訓練は、メール訓練だけとは限りません

（参考）IT統制における一般成熟度モデル

- APT対応においても「一般成熟度モデル」の適応が可能と言えます。組織内での対応状況を把握し、可能な限り次段階へのステップアップを図りましょう。

今、どの段階にありそうですか？

第0段階：「成り行き任せ」
対応していない、問題を認識していない

第1段階：「その場しのぎ」
問題を認識し、リーダーの指示のもと何らかの対応を行う

第2段階：「再現性あり」
同様の案件を処理する事で個人単位でのノウハウの蓄積がある

第3段階：「文書化」
手続は標準化および文書化されて共有されている

第4段階：「測定可能」
手続の遵守状況をモニタリング、測定できる

第5段階：「最適化」
計測された評価に基づき、継続的改善が図られている

(参考)
「COBIT 5」 http://www.isaca.org/COBIT/Pages/COBIT-5-japanese.aspx
「IT監査とIT統制」　社団法人日本内部監査協会編

お問い合わせ、インシデント対応のご依頼は

JPCERTコーディネーションセンター

- Email：pr@jpcert.or.jp
- Tel：03-3518-4600
- Web: https://www.jpcert.or.jp/

インシデント報告

- Email：info@jpcert.or.jp
- Web: https://www.jpcert.or.jp/form/

ご清聴ありがとうございました。