Internet Week 2015
S10 企業経営のためのセキュリティ
～基礎と勘所～

経営におけるセキュリティのインパクト
～基本的な用語解説を交えながら～

2015年11月18日
一般社団法人JPCERTコーディネーションセンター
経営企画室
兼エンタープライズサポートグループ　部門長
村上　晃

- JPCERT/CCをご存知ですか? -

1. JPCERT コーディネーションセンターの紹介

JPCERTコーディネーションセンターとは

- **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

  - https://www.jpcert.or.jp/
  - 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
    我が国における「セキュリティ向上を推進する活動」
  - **サービス対象: 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）**
  - 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」**
    ※各国に同様の窓口となる　CSIRTが存在する
    (例、米国のUS-CERT, CERT/CC, 中国のCNCERT, 韓国のKrCERT/CC)

- **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

インシデント予防 → インシデントの予測と捕捉 → 発生したインシデントへの対応

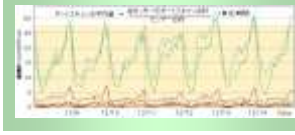
脆弱性情報ハンドリング

- 未公開の脆弱性関連情報を製品開発者へ提供し、対応依頼
- 関係機関と連携し、国際的に情報公開日を調整
- セキュアなコーディング手法の普及
- 制御システムに関する脆弱性関連情報の適切な流通

JVN Japan Vulnerability Notes

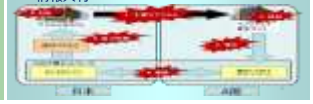
情報収集・分析・発信
定点観測（TSUBAME）

- ネットワークトラフィック情報の収集分析
- セキュリティ上の脅威情報の収集、分析、必要とする組織への提供



インシデントハンドリング
（インシデント対応調整支援）

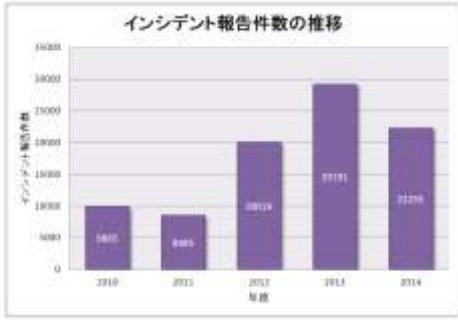
- マルウエアの接続先等の攻撃関連サイト等の閉鎖等による被害最小化
- 攻撃手法の分析支援による被害可能性の確認、拡散抑止
- 再発防止に向けた関係各関の情報交換及び情報共有



早期警戒情報	重要インフラ、重要情報インフラ事業者等の特定組織向け情報発信
CSIRT構築支援	海外のNational-CSIRTや企業内のセキュリティ対応組織の構築・運用支援
制御システムセキュリティ	制御システムに関するインシデントハンドリング、情報収集・分析発信
アーティファクト分析	マルウエア（不正プログラム）等の攻撃手法の分析、解析
国内外関係者との連携	日本シーサート協議会、フィッシング対策協議会の事務局運営等
国際連携	各種業務を円滑に行うための海外関係機関との連携

インシデント対応件数

- インシデント報告件数は増加傾向にあります



JPCERT/CC インシデント報告対応レポート [2015年1月1日～2015年3月31日] より抜粋
https://www.jpcert.or.jp/pr/2015/IR_Report20150416.pdf

数年前から継続的に、多数の組織において標的型攻撃による被害が生じています

66組織に通知　(2015年4-6月)

JPCERT/CC インシデント報告対応レポート [2015年4月1日～2015年6月30日]より
https://www.jpcert.or.jp/present/2015/JNSAWG20150625-apt.pdf

インシデント数増加の背景

ITの社会インフラ化
- 企業活動のIT化
- 電子商取引の発展
- 制御系システムへの利用

インターネットの世界的な普及
- ボーダレスの通信
- 物理的な追跡困難性

攻撃用インフラの整備
- 攻撃ツールの進歩
- 分業化された攻撃集団

今後、サイバー攻撃の増加が予想されるため、各組織においても対応体制が必要！

攻撃者の分類

- 攻撃の目的をもとに攻撃者を分類すると、それぞれの攻撃手法や技術力が異なることが推察できる

	愉快犯/ハクティビスト	**金銭目的の攻撃者**	**標的型攻撃の実行者**
攻撃の目的	- 政治的な主張 - 技術力のアピール	-金銭の獲得 (不正送金)	-標的とする組織の重要情報窃取やシステム破壊
主な攻撃手法	-Web サイトに対するDoS - 政治的な主張を目的とするWeb サイトの改ざん - SNS アカウント乗っ取り	-Web サイト改ざんによるマルウエアの配布	-マルウエアが添付されたメールの送付 - Web サイト改ざんによるマルウエアの配布 (攻撃対象のみに限定)
キーワード	- Anonymous - 歴史的な特異日	- 不正送金 -ランサムウエア	- 政府系組織、重要インフラ大手メーカなどを狙う攻撃
技術力	低	中	高

JPCERT/CC 早期警戒グループにて独自に分類

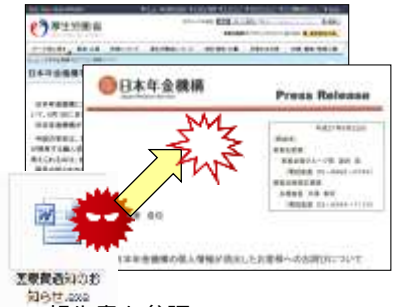
サイバー攻撃に関するご説明

標的型攻撃の事例

- 最近、**「標的型攻撃」「APT」**、という言葉を、よく耳にしませんか？
  - ✓ 実際に**攻撃の被害にあった組織**が増えています

- **平成27年6月1日**

「日本年金機構の個人情報流出」



- ✓ メールに添付されていたファイルを開封したことにより、端末がマルウエアに感染
- ✓ 計31台の端末がマルウエアに感染
- ✓ 攻撃者による不正アクセスにより、**情報流出**

詳細は内閣官房サイバーセキュリティセンターの報告書を参照
http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf

１つの組織だけの問題にとどまらず、社会的な問題に発展！

標的型攻撃とは

- **先進的で (Advanced)、執拗な (Persistent)、脅威 (Threat)**
  - ✓ **A**dvanced **P**ersistent **T**hreat とも呼ばれます

【先進的(A)】
攻撃者は**目的達成のために必要な最小限のツール**しか使用しません。そのため、一連のイベント自体が「先進的」と見なされます。

【執拗な(P)】
攻撃者は ネットワーク上に**長期にわたって居座り続けます**。例えば、**繰り返しアクセスを図り**、複数年にわたってアクセスを維持することもあります。

【脅威(T)】
攻撃者は長期的な 活動を実施するために**リソース**が必要です。そのため、攻撃者には国家が支援する能力者や先進的なサイバー犯罪者が含まれる場合があります

攻撃者は、明確な攻撃の**目的**とその能力を有しており、その活動は**組織化され、資金も十分**で、また**経験も豊富**に有した人たちが連携することで行われます。各種**ツールを提供する企業**も存在します。

標的型攻撃に関する通知連絡

- **2015年4-6月期**
  JPCERT/CCによる外部観測や他組織からの情報提供により発覚した標的型攻撃の被害組織への通知数

66組織

うち年金機構と同種の攻撃: 44組織

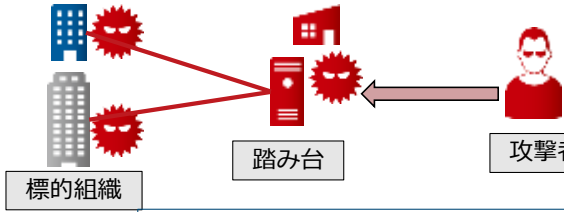
※ただし、一部調査目的の通信なども確認

- 攻撃対象となるのは、省庁(独法)、重工、航空・宇宙、商社、エネルギー、化学などの国家の基盤となる組織に加え、それらの**サプライチェーンを構成する組織**も含まれる

経済活動の源泉となる知的財産や組織の機密情報が継続的に流出する事態が発生している

標的型攻撃は対岸の火事ではありません

- **「うちは中小だから狙われない」**と思っていませんか？
- **中小企業が標的型攻撃の踏み台**になる可能性があります！
  - **標的とする組織を攻撃するための踏み台にする**
    - ✓サプライチェーンに組み込まれている中小企業を狙う
    - ✓セキュリティ対策が十分でない中小企業を狙う
  - **「水飲み場型攻撃」に使用する**
    - ✓標的とする組織が日常的に利用するウェブサイトにマルウエア等を仕掛ける

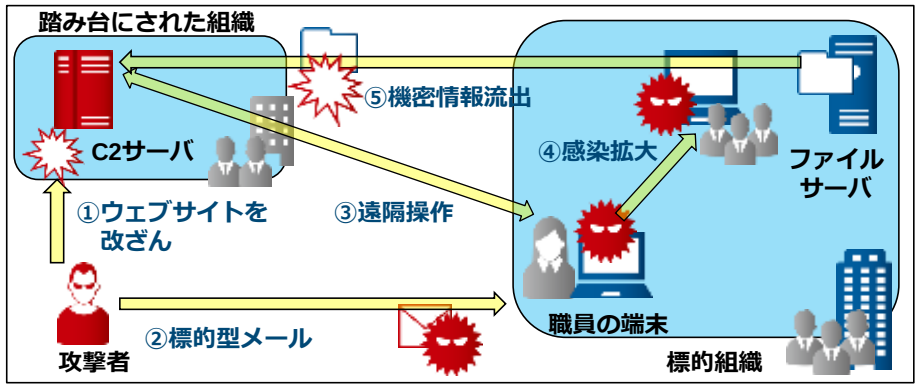



水飲み場のイメージ

自組織が被害をうけるだけでなく、
標的型攻撃の加害者になってしまう可能性があります！

標的型攻撃の全体像

- **踏み台にしたサーバから、マルウエアを遠隔操作する**
  - ―マルウエア：悪意あるソフトウエア (コンピュータウィルス)
  - ―C2サーバ(Command & Control サーバ)：指令サーバ



自組織が踏み台となって他の組織が被害を受けた場合、
社会的信用低下、取引停止などにつながりかねません！

  JPCERT CC

DDos攻撃

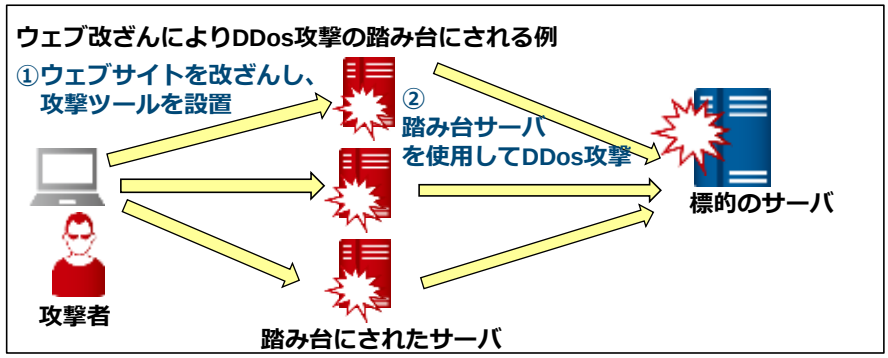
Distributed Denial of Service attack

- **脆弱なサーバがDDos攻撃の踏み台に使用されることがある**

例）

―ウェブ改ざんにより攻撃ツールを設置

―脆弱性のあるDNSサーバ等を使用する場合もある



サーバのセキュリティ対策を行っていない場合、
DDos攻撃の踏み台となってしまう可能性があります！

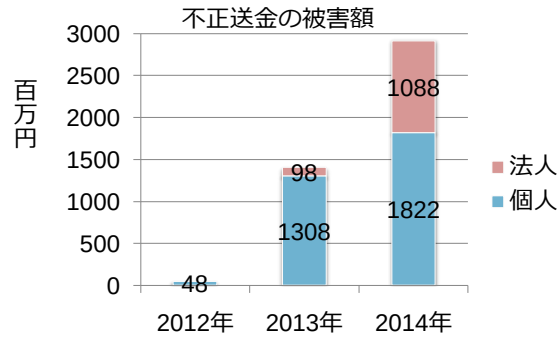
  JPCERT CC

不正送金

- 法人のインターネットバンキングを狙った不正送金が増えています
- フィッシング（従来）
  - —銀行やクレジットカード会社などを装った偽メールを送付
  - —「偽のログインページ」に誘導し、アカウントを盗む
- 不正送金マルウエア（最近）
  - —インターネットバンキングを利用する端末をマルウエアに感染させる
  - —「偽の入力項目」を表示し、アカウントを盗む
  - →ユーザがアクセスするのは正規サイトのため見極めが難しい

不正送金

- 不正送金の被害額は増加傾向にあります

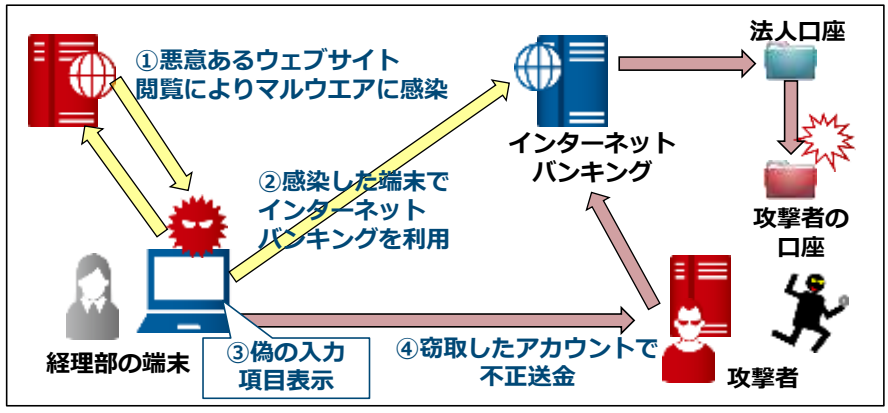


引用元：
警察庁「平成26年中のインターネットバンキングに係る不正送金事犯の発生状況等について」
https://www.npa.go.jp/cyber/pdf/H270212_banking.pdf

2014年の発生件数は1876件、被害額は約29億円。
法人口座の被害が急増している。

不正送金の攻撃手法

- 不正送金マルウエアによる攻撃の例
  —偽の入力項目を表示し、利用者が入力したアカウントを盗む



送金の上限金額が大きい場合、不正送金の被害金額が膨大になることがあります

対応体制はどうしたら？

情報連携のススメ

- 「目的をもった攻撃」を意識する
  - —様々な手段を用いて達成しようとする
  - —複数の攻撃先、繰り返される攻撃
  - —最前線は内部ネットワーク
- 「見えていないもの」に気付くための手段を確保する
  - —各組織においてデータを保全する
  - —他組織との間でデータを突合させる

知見の集約が対抗手段につながる

対応のあり方は、攻撃の性質によって異なり得る

- いわゆるAPT型の攻撃と活動家による攻撃、経済的な利得目的の攻撃では、同じ標的型攻撃であってもそれぞれ異なる対応をする方がよい場合がある。
  - — APTの場合は、被害者は気付きづらく、攻撃者は攻撃については一切公開しない
    - インシデントの発生の事実自体が公表されない。
    - 攻撃方法に気づいたことを攻撃者に気づかれずに対処する等の工夫
  - — 活動家による攻撃では、攻撃の成功についての声明が出たり、窃取した情報が公開されたりする
    - インシデント発生の事実や窃取された情報が公開される
    - インシデントへの対処ぶりについても注目があつまる
    - 社会的な反応が活動家による攻撃のエネルギーにもなる
- コーディネーションにともなうリスクの検討も必要
  - — 対応していることを気付かれる
  - — 情報の価値を気付かせる

対応の仕方について、一組織のみで判断することは難しい。対応について相談したり、類似の状況の有無について情報を得る体制が必要！

何に（どのような問題に）対処したいのか、何を護ることが優先せるのか
対策の目的と優先順位を定める。

＝リスクも認識する

- 攻撃の対象になること自体は避けられない。
- 本気で狙われた場合には、必ず、何らかのインシデントは発生してしまう（そのことも避けられない）。
- 発生してしまったインシデントが、機密情報や重要情報の漏えいや消失、業務の停止、他者への攻撃への加担などの被害につながらないようにすることが事前の対策。＝一切のインシデントが発生しないようにする対策などは存在しない（と言わざるを得ない。）
  - 技術的な措置
  - 対処のための意思決定権限の移譲（組織内CSIRT等）
- 攻撃を受けた場合に、何を一番優先するかについて組織としての意思決定が行われている？

  → どんな情報が流出したのか（していないのか）の確認が最重要なのか、業務の中断時間を最短にすることが最重要なのか、攻撃元を特定することが最重要なのか・・ → その目的に応じたシステム構成やサービス購入が行われている？

  → 何のログをどのくらいの期間のこしておく必要があるのか、どの程度の効率で検索ができる必要があるのか（効率的な検索を可能にするシステム）など。

脅威は変化する＝対策についても適時の有効性の確認・見直しが必要

気づきにくい攻撃については、
外部からの連絡が認識の端緒になる場合が多い。

- 攻撃を受けていることに気付きにくい → 外部からの連絡が攻撃を認識する端緒になる場合が多い
  - —連絡を受けて、適切に情報をハンドルできる窓口（組織内インシデント対応体制の本質的な機能）を備える
  - —提供された情報をもとに、攻撃の有無を確認できるようにするためには、必要なログが適切に、検索可能な状態で保存されていることが必要となるが・・・・
- 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必要なこと
    - 事前の準備として
    - 一社の情報だけでは判断が難しい ＝ 情報集約・共有

おさらいですが・・インシデントとは？

- 一般的な「インシデント」とは
  —重大な事故に至る可能性がある出来事をいう

- 情報セキュリティの分野での「インシデント」とは
  —IT システムの正常な運用または利用を阻害するウィルス感染、不正アクセス、情報漏えい、DoS 攻撃などの事案や現象の発生をいう

インシデント対応（活動）とは

- 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一連の活動

業務の多様性及び複雑性の状況や、それに伴うセキュリティコントロール（技術面、運用面、管理面）の難しさが見られるようになってきた

セキュリティに関する対応体制

- インシデント(*)発生時の対応体制
  - ユーザ部門、システム管理、営業、法務、広報などの関連部署間で情報の共有及び対策の一元化
  - システム責任者、対応フローの明確化(例：誰がサーバを止めれるか？)

インシデント(*)・・IT システムの正常な運用または利用を阻害するマルウエア感染、不正アクセス、情報漏えい、DoS 攻撃などの事案や現象の発生をいう

インシデント対応活動の必要性
完全な予防策はない

- 「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
  - 社員の意識に頼るところ[illegible]ず存在

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（インシデントの発生は避けられない）

（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）

インシデント対応体制を設置する意義

インシデント対応体制について

- 組織的なインシデント対応活動を実現するためには
  - ―組織内におけるインシデント対応活動に関する機能要素を見出す
    - インシデントを発見する要素、インシデントを報告する要素、インシデントの報告を受ける要素、・・・・
  - ―その機能要素を有機的に結びつける
    - 各要素の役割や機能の設定、各要素間のインタフェース及びコミュニケーションの確立、・・・・
  - ―全体として、統一性及び一貫性のある状態にする

組織的なインシデント対応体制の構築へ

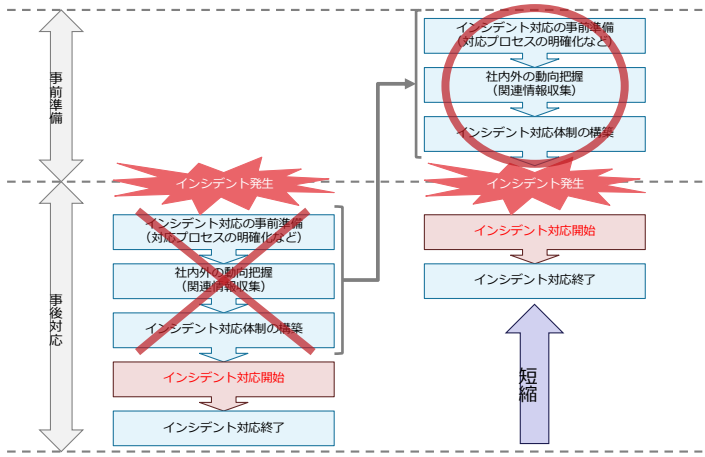
インシデント対応体制を設置する意義

組織的なインシデント対応体制に求められる主な機能

- 組織内の情報共有及び連携
  - ―インシデント報告を集める窓口の一本化
  - ―組織内のインシデントの一元管理と部署間調整
- 外部組織との調整
  - ―外部に起因するインシデント（DDoS、フィッシング など）を解決するため、他組織に対する適切な依頼
  - ―外部からのインシデント関連情報を受け取る窓口の一本化
  - ―組織間で連携しなければならないインシデント対応のため、外部組織との強い信頼関係の構築

インシデント対応体制を設置する意義
インシデント対応体制を構築すべき時期

- 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必要がある



インシデント対応体制を設置する意義
事前のインシデント対応計画の策定

- インシデント対応体制の構築には、事前の インシデント対応計画の策定が重要である

- 組織的なインシデント対応計画を策定するためのポイント
  - ―複雑化するネットワーク及びシステムの把握
  - ―インシデント対応の担当者／責任者の明確化
  - ―インシデント発生時の報告窓口の一元化
  - ―インシデント対応に必要な技術的支援、ノウハウ、関連情報の入手を支援する人／チーム／部署の設置
  - ―インシデント対応に必要なポリシー及びマニュアル等の整備
  - ―外部組織に依頼する場合の、外部の対応能力の把握と適切な報告
  - ―リスク評価の実施とリスク許容度の設定

組織内 CSIRT の有用性

インシデント対応体制と組織内 CSIRT

- 組織内 CSIRT について
  - —Computer Security Incident Response Team の略であり、「シーサート」と呼ぶことが多い
  - —組織内でインシデント対応に関する業務を専門に担当するチームのこと
  - —組織によっては、他の関連業務と兼務することによって、組織内に CSIRT の機能のみを実装している場合もある

組織的な「インシデント対応体制」のベストプラクティス（最善策） ＝ 組織内 CSIRT

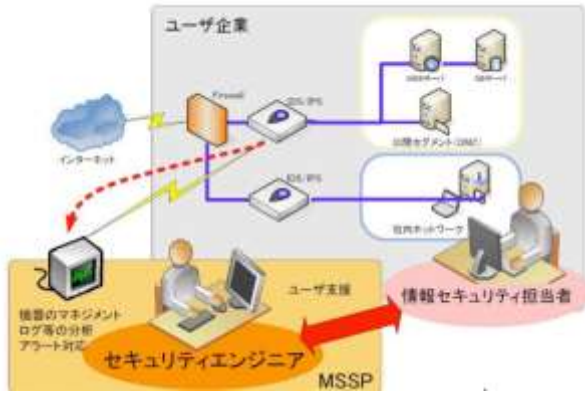
組織内 CSIRT の必要性

組織内 CSIRT の機能

- 組織内 CSIRT の内部に対する側面
  - —組織内で発生したインシデントを報告するための、一本化された窓口を提供する
  - —発生したインシデントに対応する、或いはその対応に必要な技術的支援及びノウハウを提供する
  - —インシデント対応に必要な、組織としての意思決定を支援する
  - —部署間で発生するインシデントの調整役として活動する
  - —組織内の業務システムのユーザに対するセキュリティ意識を啓発する
- 組織内 CSIRT の外部に対する側面
  - —外部のインシデント対応組織との連絡調整をする
  - —最近のインシデント動向及びインシデント対応手法・技術に関する情報を外部から収集し、必要なところに提供する
  - —従業員・報道・国民へ適切な情報を提供する

SOCの概要

- 日本セキュリティオペレーション事業者協議会
  - —（ISOG-J） http://isog-j.org/index.html



マネージドセキュリティサービス（MSS）選定ガイドライン
http://isog-j.org/output/2010/MSS-Guideline_v100.pdf
からの抜粋引用図

Security Operation Center（SOC)
セキュリティオペレーションセンター

- 主に企業や組織向けのセキュリティの監視・管理サービスを行う。マネージド　セキュリティ　サービス（MSS)とも言う。
- ３６５日・２４時間の対応を行っているベンダーが多い。
- 監視・運用は　不正侵入防止装置（IDS,IPSやファイアウォールなどのセキュリティ機器）の運用とそれらの機器からのアラートを分析し、攻撃の予兆、攻撃の警告、侵入・侵害の事実の確認等によって、監視対象の組織へ通知したりアドバイス支援等を行うサービスが多い。（外部委託ではなく、自組織でSOCを運用する形態もある）
- 監視対象は主にインターネッのトに接続されている外部セグメントにあるWebサーバ、DNSサーバ、メールサーバ等が多いが、内部ネットワークを監視するサービスもある。

（参考）CERT/CC におけるサービスの分類の例

事後対応型サービス	事前対応型サービス	セキュリティ品質管理サービス
・アラートと警告（SOC） ・インシデントハンドリング - インシデント分析（SOC） - オンサイトでのインシデント対応 ※緊急対応サービス等 - インシデント対応支援（SOC） - インシデント対応調整 （CSIRT/SOC） ・脆弱性ハンドリング - 脆弱性分析 - 脆弱性対応 - 脆弱性対応調整 ・アーティファクトハンドリング - アーティファクト分析 - アーティファクト対応 - アーティファクト対応調整	・告知 ・技術動向監視 ・セキュリティ監査または審査 ・セキュリティツール、アプリケーション、インフラ、およびサービスの設定と保守 ・セキュリティツールの開発 ・侵入検知サービス（SOC） ・セキュリティ関連情報の提供（SOC）	・リスク分析 ・ビジネス継続性と障害回復計画 ・セキュリティコンサルティング ・意識向上 ・教育 / トレーニング ・製品の評価または認定

※SOCサービス（SLA)や役割・」範囲によって対象は異なりますが、仮にCSIRTとSOCの役割分担を想定した場合の参考事例です。

組織内 CSIRT の必要性
組織内 CSIRT のメリット

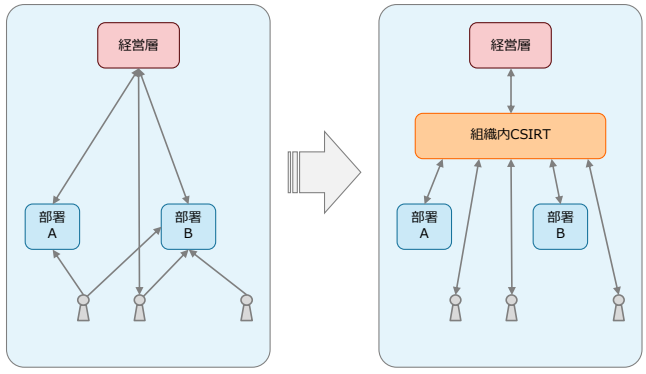
- 組織内 CSIRT を構築するメリットは、組織毎によって大きく異なるが、多く見られるメリットの例は、以下のとおり

—情報セキュリティ（インシデント関連）に関する情報管理
—（組織内のインシデントに関する）統一された窓口として
—（外部との）インシデント対応に必要な信頼関係の構築

組織内 CSIRT の必要性

参考：組織内 CSIRT のメリットのイメージ 1

- 情報セキュリティ（インシデント関連）に関する情報管理

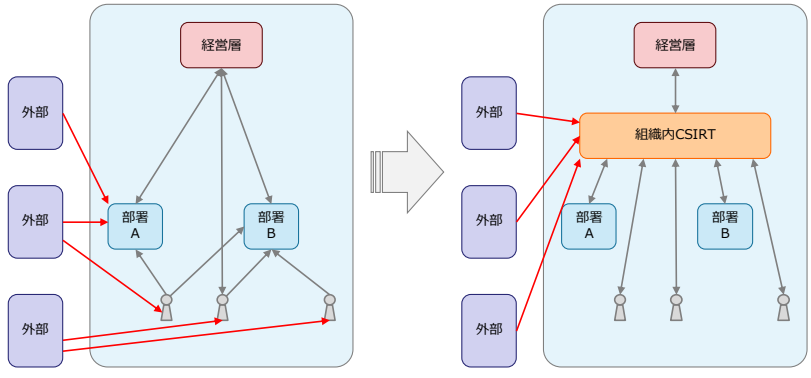


メリットの例：
①社内セキュリティ情報の共有、集中管理の実現
②セキュリティ対応にかかる指示系統の迅速化（ダイレクトリーチ）

組織内 CSIRT の必要性

参考：組織内 CSIRT のメリットのイメージ 2

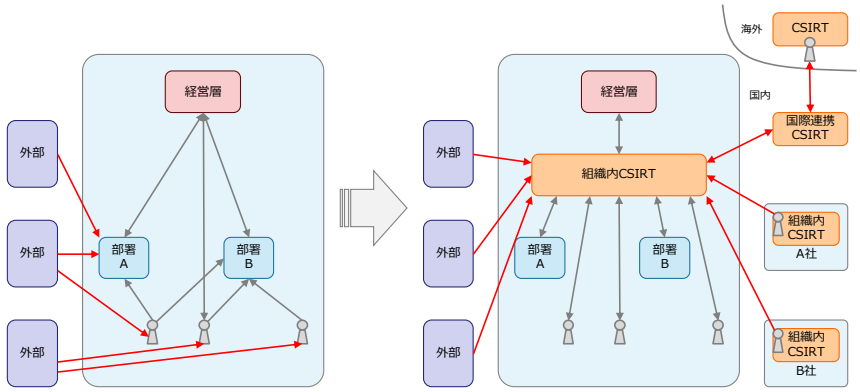
- （組織内のインシデントに関する）統一された窓口として



メリットの例：
①外部に対して信頼性のある窓口先の提供
②外部からの情報の一元管理の実現

組織内 CSIRT の必要性
参考：組織内 CSIRT のメリットのイメージ 3

■ （外部との）インシデント対応に必要な信頼関係の構築



メリットの例：
①インシデントレスポンスに必要な情報量の向上
②想定外（予想外）のインシデントへの柔軟な対応

CSIRT の役割の説明に役立つ資料
参考：CSIRT と消防署の役割の比較例

CSIRT の場合（例）	消防署の場合（例）
● 発生したインシデント対応	● 発生した火事や事故への対応
•連絡先の提供： Email アドレス／電話	•連絡先の提供： 電話（１１９番）
•連絡目的： 対応や技術支援などの要請	•連絡目的： 消火依頼、救出要請など
•CSIRT での活動	•消防署での活動
•インシデントの分類、優先度の判断と対応方法の決定	•火災規模、症状等の判断と対応方法の決定
•適切な（技術的）対応を取る人への連絡調整	•最寄の消防車や救難器材の手配に関する連絡
•被害の極限化策の実施（ネットワークからの切り離し、システムの設定変更等）	•火事の拡散防止や救出等の緊急避難等のための一部破壊
•インシデント原因の排除（脆弱性箇所へのパッチ適用、ウィルス除去、Phishing サイト停止等）	•消火活動及び救出活動
● インシデントの発生予防	● 火事や事故の発生予防
•ユーザへのセキュリティ啓発活動	•防火訓練や救出講習等の啓発活動
•インシデント脅威情報の提供	•火災／乾燥注意報による注意の呼びかけ

CSIRTの必要性や有用性について経営層から理解を得る

- 経営層が CSIRT を理解していない場合は、CSIRT に関する説明資料の作成が必要になる
- 最初に経営層からの理解を得るのが難しい場合には、十分な情報収集及び検討した結果をまとめた文書にして伺いを立てる
- まずは、CSIRT の必要性を理解する同僚及び上司を増やしていくことが重要である

組織内の現状把握とリスクの評価

- 組織内における業務内容の把握
  - —各部署の業務フロー
  - —部署間の情報共有及び連携の状況
  - —業務活動における各部署の責任者及びキーパーソン
- 主要な人物に対するヒアリングの実施
  - —各部署のインシデント対応の責任者
  - —インシデント対応時に関わったことのある人
    - 情報セキュリティに明るい人
    - 業務システムの運用及び維持管理に明るい人
  - —情報セキュリティに関する業務の職責を持つ人
- インシデント対応に関係する規則類の把握
  - —インシデント対応に関係する項目や文言の列挙

（参考） 組織内 CSIRT に関して検討すべき事項一覧

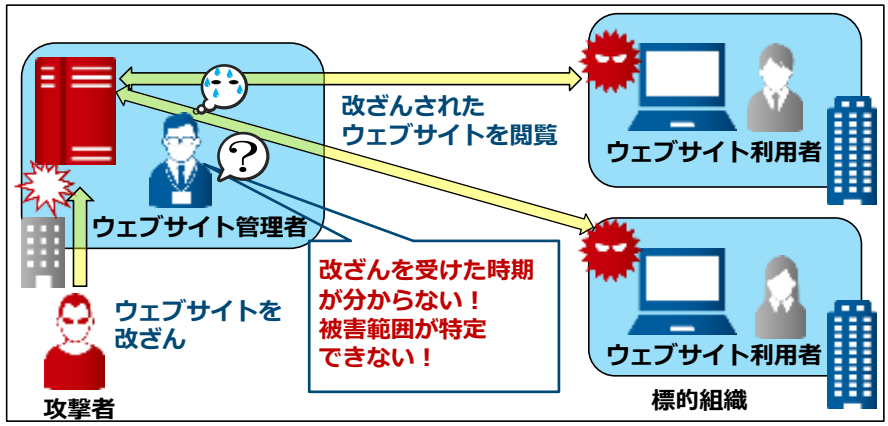
- サービス対象者は？
- 経営層及びサービス対象者の期待は？（何が必要か？）
- 保護すべき重要な資産は何か？
- 情報セキュリティに関する既存の問題は？
- どのような種類のインシデントが報告されるか？
- どのような種類の調整と対応が求められているか？
- どのような能力やスキルが必要か？
- どのようなプロセスが必要か？
- エスカレーションする先はどこか？
- どのような人が関わるか？
- どのようなコンプライアンス、組織の事業、組織文化があるか？
- 誰が担当すべきか？他に担当できる人がいるか？
- 外部との連絡調整、情報共有、連携活動の必要性はあるか？
- 組織のリスク許容度はどうなっているか？
- その他

（参考）組織のリスク許容度の評価

組織の特徴	リスク判断	取り組み方法
・組織の規模 ・組織の複雑さ ・保有する知的財産の価値 ・ITへの依存度 ・システムダウンが与える影響 ・システムエラーが与える影響 ・組織的な変化の度合い ・多国籍企業かどうか ・利害関係者/株主の期待の度合い ・規制のレベル ・評判への依存度 ・外部委託の依存度 ・事業所の地域的な不安定さ	・セキュリティ防衛能力 ・守るべき製品/サービス ・資産を防御する理由 ・潜在的なリスク - リスクの対処に必要なコスト - リスクによる減損の許容範囲 - 対処後の残存リスク	・組織の管理策の有効性/生産性を把握 ・組織の対外的な評価を維持/向上 ・企業の回復力を維持 ・内外を問わず悪意ある攻撃から防御 ・例外条件を極少化したアクセスコントロールリストを作成 ・ISO27001におけるセキュリティ管理策に準じて行動 ・予防的なログを保持 - DNSログ - プロキシログ - ファイアウォールログ - NetFlowログ - サーバログ - ホストログ

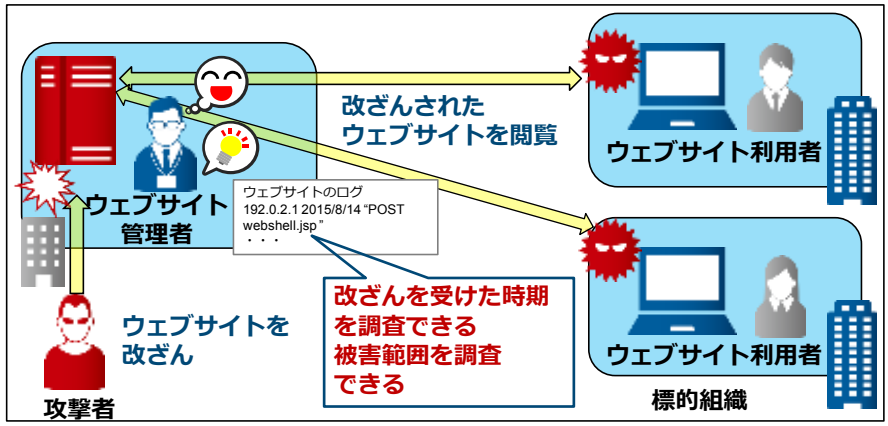
ログの取得と確認を是非検討ください！

- 攻撃を早期検知することが大切！
  - —ログを取得していないと



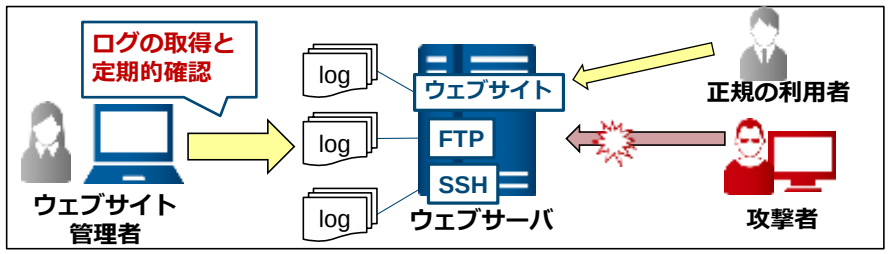
ログの取得と確認

- 攻撃を早期検知することが大切！
  - —ログを取得していると



ログの取得と確認

- ウェブサーバのログを取得する
  - —ウェブサイトのアクセスログやサーバの認証ログ
  - —ログは１年以上保存することを推奨
- ログを定期的に確認する

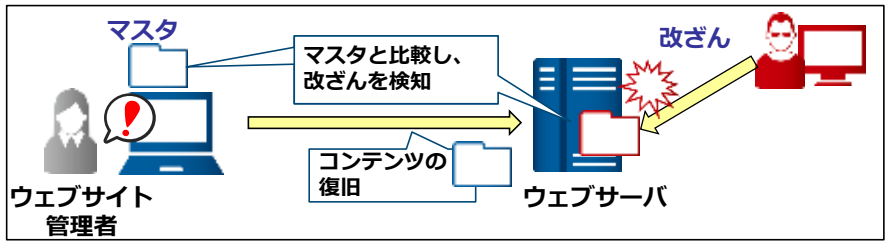


ログを適切に取得しておくと、インシデントの追跡調査に役立つことがあります。

ウェブコンテンツの確認と管理

改ざんを検知し、復旧できる準備をしておくことも大切です

- ウェブコンテンツの管理
  - —マスタ (ウェブサイトを構成するファイル群) の管理
  - —バックアップの取得
- ウェブコンテンツの定期的確認
  - —公開しているコンテンツを定期的に確認
    - マスタ(バックアップ)と比較し、変更されていないか
    - 不審なファイルが設置されていないか



サイバー攻撃による被害を
少しでも減らしていくには？

4. まとめ

リスクの認識と、対策の浸透を

- **標的型攻撃に関する社会の認識が変化してきています**

「攻撃が来るはずがない。被害を受けても被害者であり、
攻撃者が悪い。」
という意見が以前は一部でありましたが、現在は

「攻撃は来て当たり前。組織、顧客、取引先の情報を守るためには
適切な対策が必要。」
という意見が多い様に見受けられます。

セキュリティ対策を行っておらず、標的型攻撃の加害者に
なってしまった場合、組織のガバナンスを問われることになります。

情報共有：目的に応じた情報共有のススメ

「目的を持った攻撃」を意識する

- 様々な手段を用いて達成しようとする
- 複数の攻撃先、繰り返される攻撃
- 最前線は内部ネットワーク

「見えていないもの」に気付くための情報共有

- 各組織においてデータを保全する
- 他組織とデータを突合させる

セキュリティ対策は経営課題です！
知見の集約が対抗手段につながる

組織内のインシデント対応体制（CSIRT)の活用

事業継続（BCP/BCM/BIA)を意識する

- セキュリティ対策は事業継続上の課題
- 対応組織を作るのではなく機能と組織の融合
- 最前線は？内側・外側の境目のない対応

計画を立てるだけでなく訓練が必須！

- インシデントは想定の範囲内で収まらない場合もある。
- 他組織と連携が必須！（自組織で解決できない課題にどのように取り組むのか？

経営目線のプロアクティブなセキュリティ対策

（参考）組織内 CSIRT の構築に役立つ資料

- JPCERT/CC　における関連文書
  - ―組織内 CSIRT 構築支援マテリアル
    - http://www.jpcert.or.jp/csirt_material/
  - ―コンピュータセキュリティインシデント対応チーム（CSIRT）のためのハンドブック
    - http://www.jpcert.or.jp/research/2007/CSIRT_Handbook.pdf
- その他の参考資料
  - ―CERT/CC – “Creating a Computer Security Incident Response Team: A Process for Getting Started”
    - http://www.cert.org/csirts/Creating-A-CSIRT.html
  - ―TERENA – “CSIRT Starter Kit”
    - http://www.cert.org/csirts/Creating-A-CSIRT.html
  - ―AusCERT – “Forming an Incident Response Team”
    - http://www.auscert.org.au/render.html?it=2252
  - ―RFC 2350 – “Expectations for Computer Security Incident Response”
    - http://www.ietf.org/rfc/rfc2350.txt

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。