情報セキュリティ月間 キックオフ・シンポジウム
サイバーセキュリティ、現状と対策−企業等におけるサイバー攻撃対策

サイバー攻撃の動向とインシデント対応の状況

平成25年2月1日
専務理事　早貸淳子
一般社団法人JPCERTコーディネーションセンター

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・コーディネンションセンター

- 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

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、等)

－ JPCERT/CCをご存知ですか? －

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

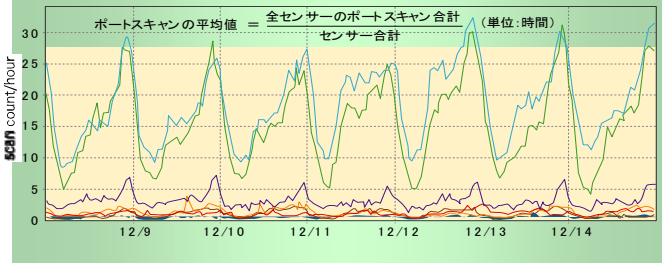
- 未公開の脆弱性関連情報を製品開発者へ提供し、対応依頼
- 関係機関と連携し、国際的に情報公開日を調整
- セキュアなコーディング手法の普及
- 制御システムに関する脆弱性関連情報の適切な流通

JVN Japan Vulnerability Notes

情報収集・分析・発信

定点観測(ISDAS/TSUBAME)

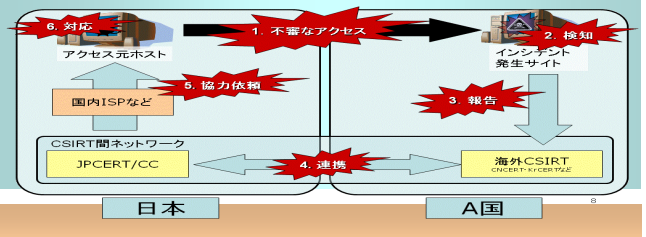
- ネットワークトラフィック情報の収集分析
- セキュリティ上の脅威情報の収集、分析、必要とする組織への提供



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

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

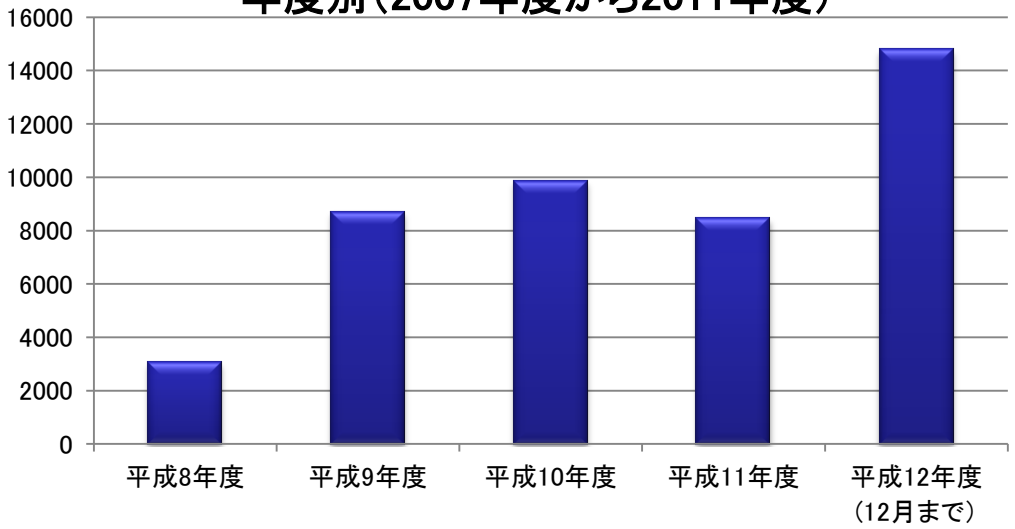
国際連携

各種業務を円滑に行うための海外関係機関との連携

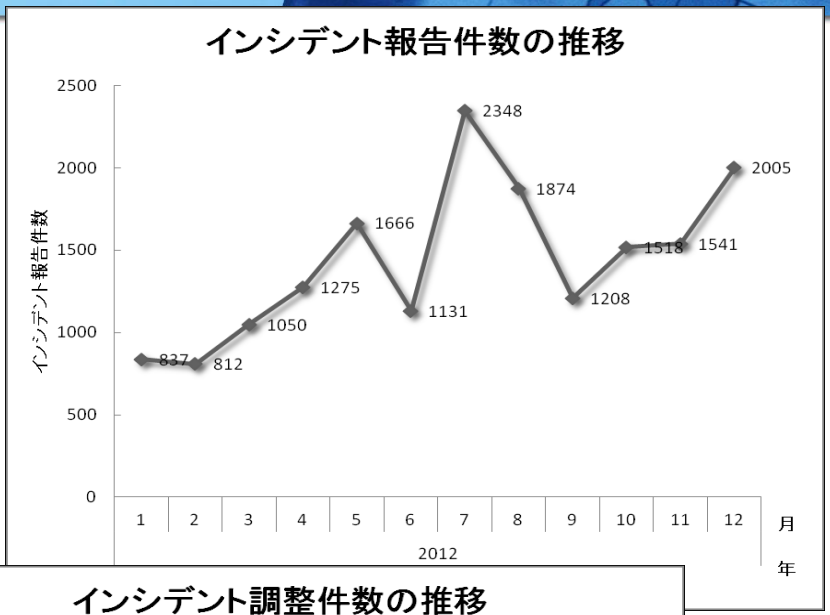
JPCERT/CCに寄せられるインシデント報告（統計）

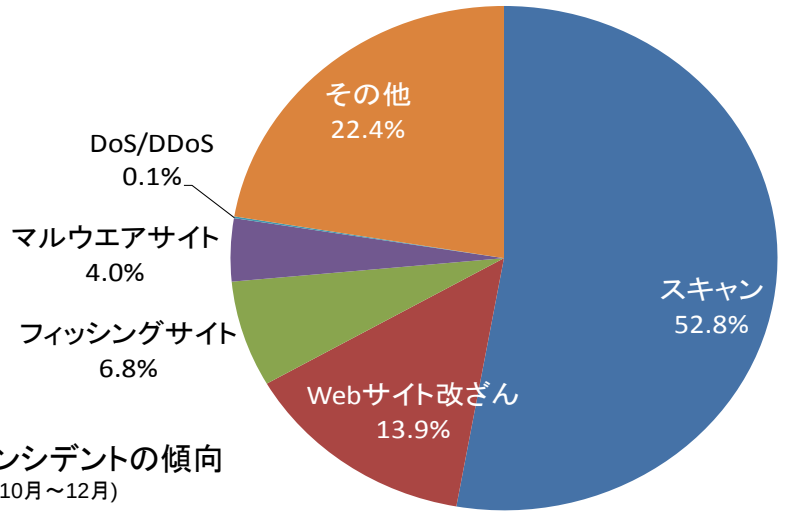
【参照】https://www.jpcert.or.jp/pr/2013/PR20130117.pdf
https://www.jpcert.or.jp/pr/2013/IR_Report20130117.pdf

年度別（2007年度から2011年度）



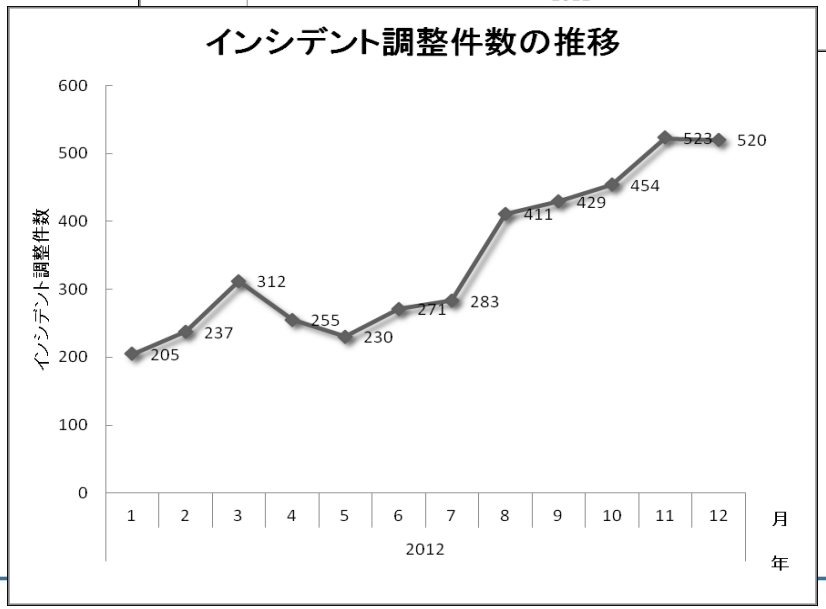
インシデント報告件数の推移



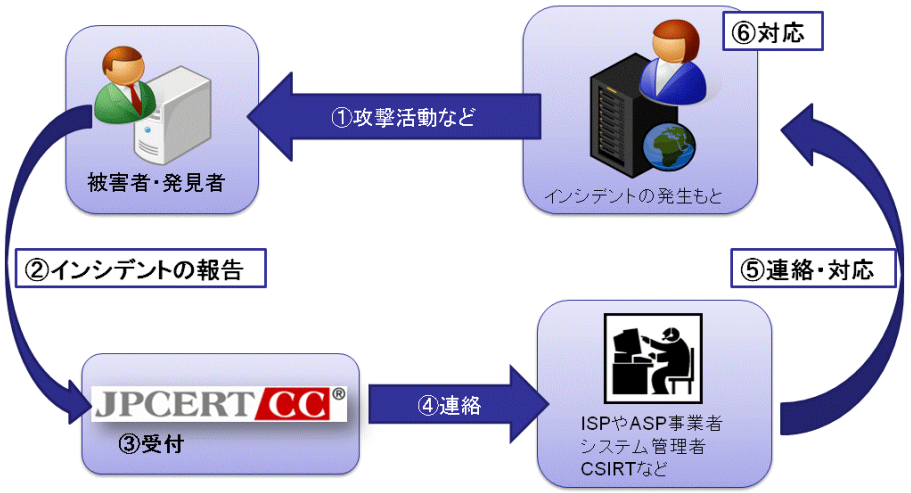


報告されたインシデントの傾向
（2012年10月～12月）

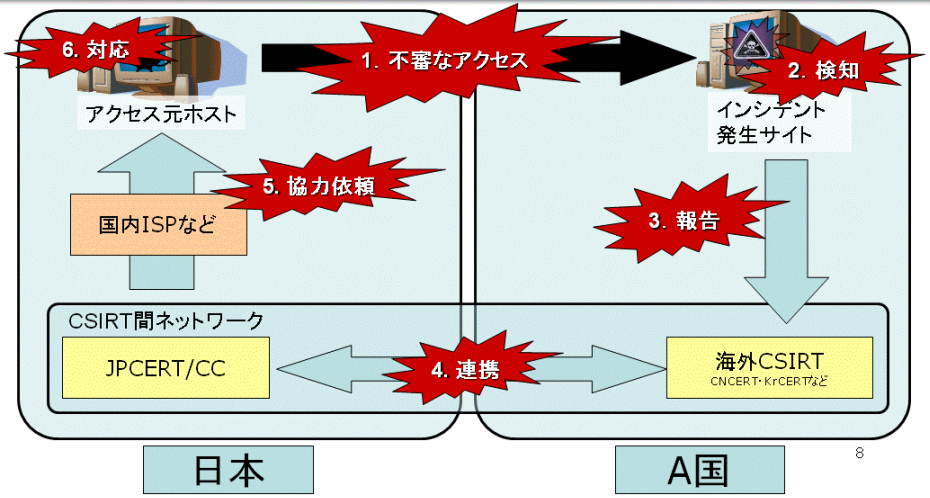
インシデント調整件数の推移

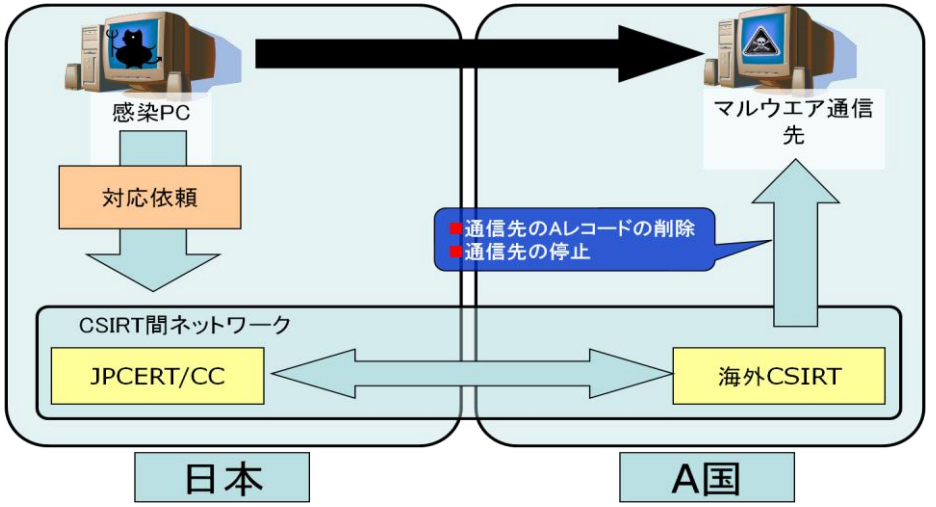


（参考1）インシデント報告に基づく調整
（インシデントハンドリング/アーティファクト解析）



1. インシデント報告の受付
2. （必要に応じ）マルウエアの解析
   - ① 挙動、機能、脅威
   - ② 被害拡大抑止のための調整を実施するための接続先等の情報の抽出
3. 被害の拡大抑止のための関係先へのコーディネーション
4. 必要に応じ、早期警戒情報、注意喚起の発行

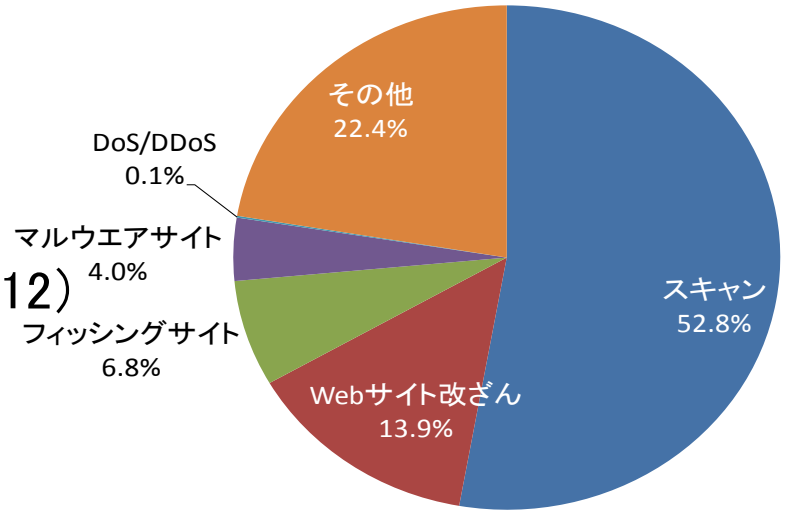




【調整の例】

報告されるインシデントの例

- 攻撃の準備行為としての脆弱性探索、スキャン等
- ウェブサイト改ざん（改ざん対象にこだわりがある場合もあれば、無差別に脆弱性探索をし対象にする場合も）
  - 主義主張のための画像などのコンテンツを挿入するタイプの改ざん
  - マルウエア配付サイト等悪意のあるサイトへ誘導するためのスクリプトなどを埋め込むタイプの改ざん
    - HTMLファイル・スクリプトファイル
    - JavaScriptやiframeによる誘導
- フィッシングサイト
  - 金融機関に関するものが約73%(2012.10～12)
- マルウエア配付サイト
- サービス妨害攻撃（DoS,DDoS等）

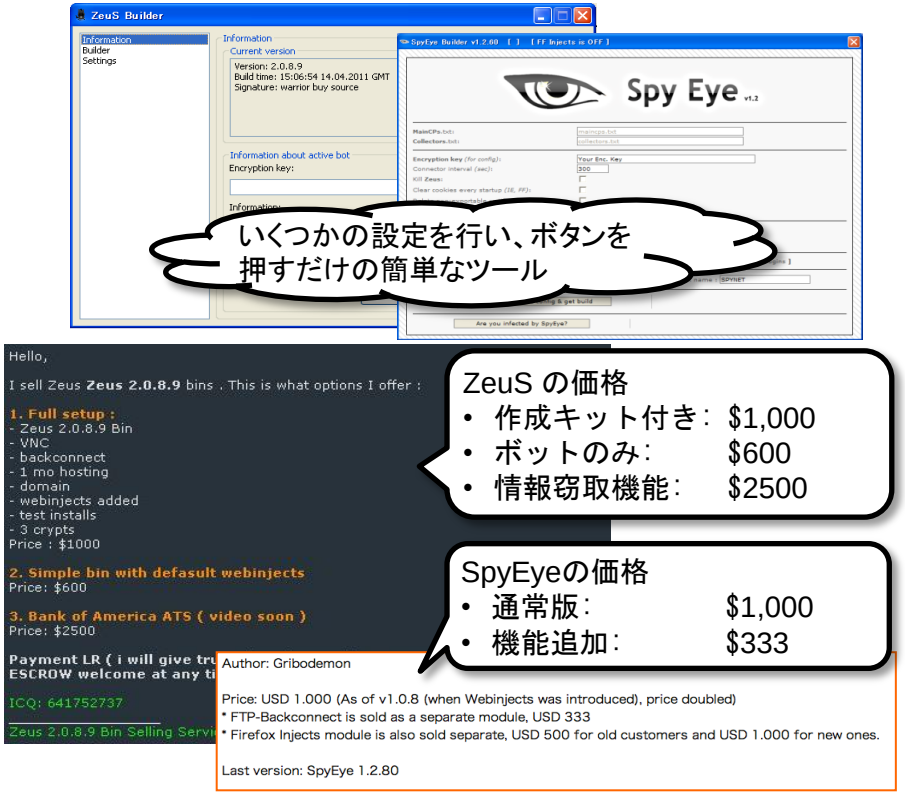


報告されたインシデントの傾向
(2012年10月～12月)

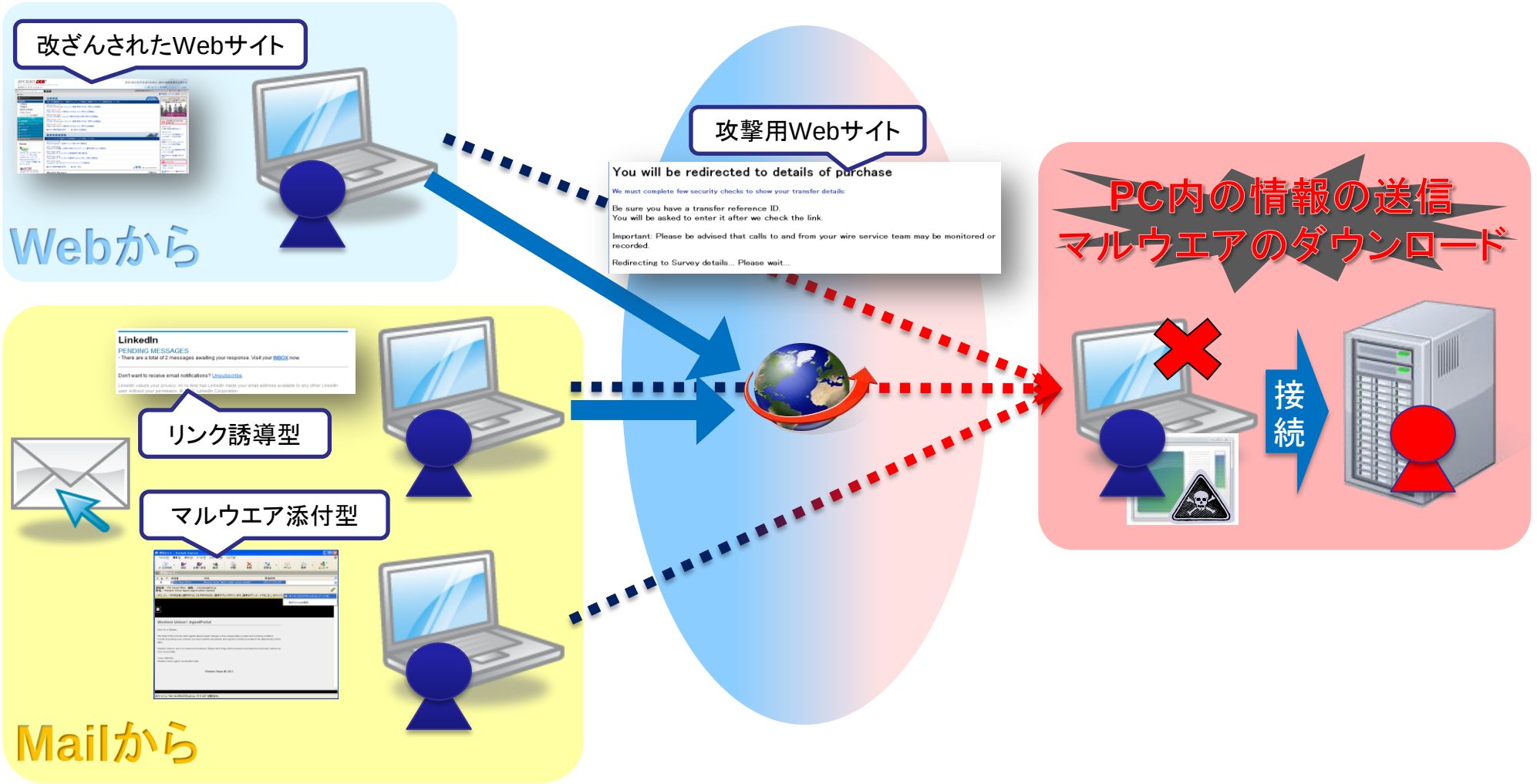
（続き）

■ 金融機関を騙るフィッシングや第二認証情報を詐取するマルウエア

■ 主に金融サービス関連情報の窃取を目的としているとされる攻撃ツール



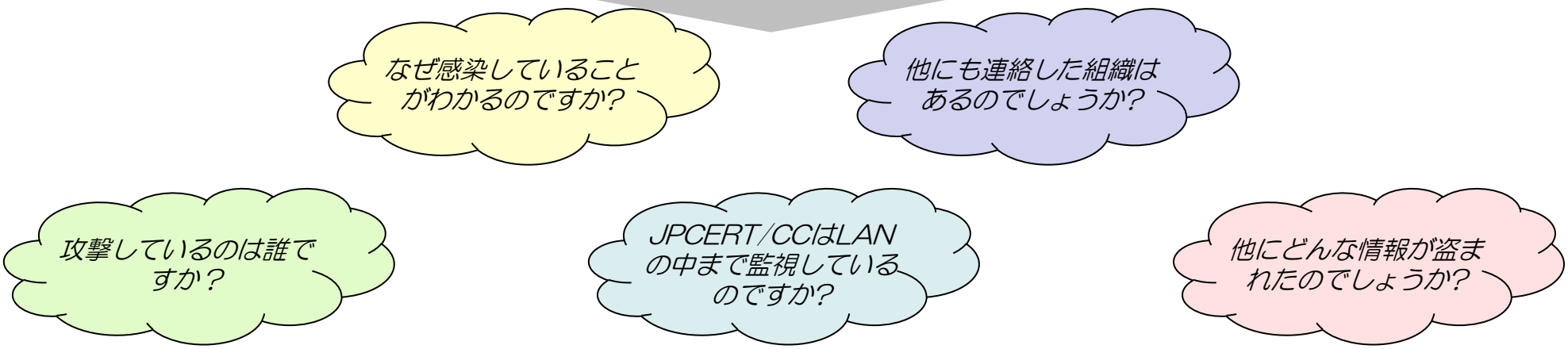
事例①
悪性Webサイトを介した攻撃



事例②
マルウエアを使った侵入

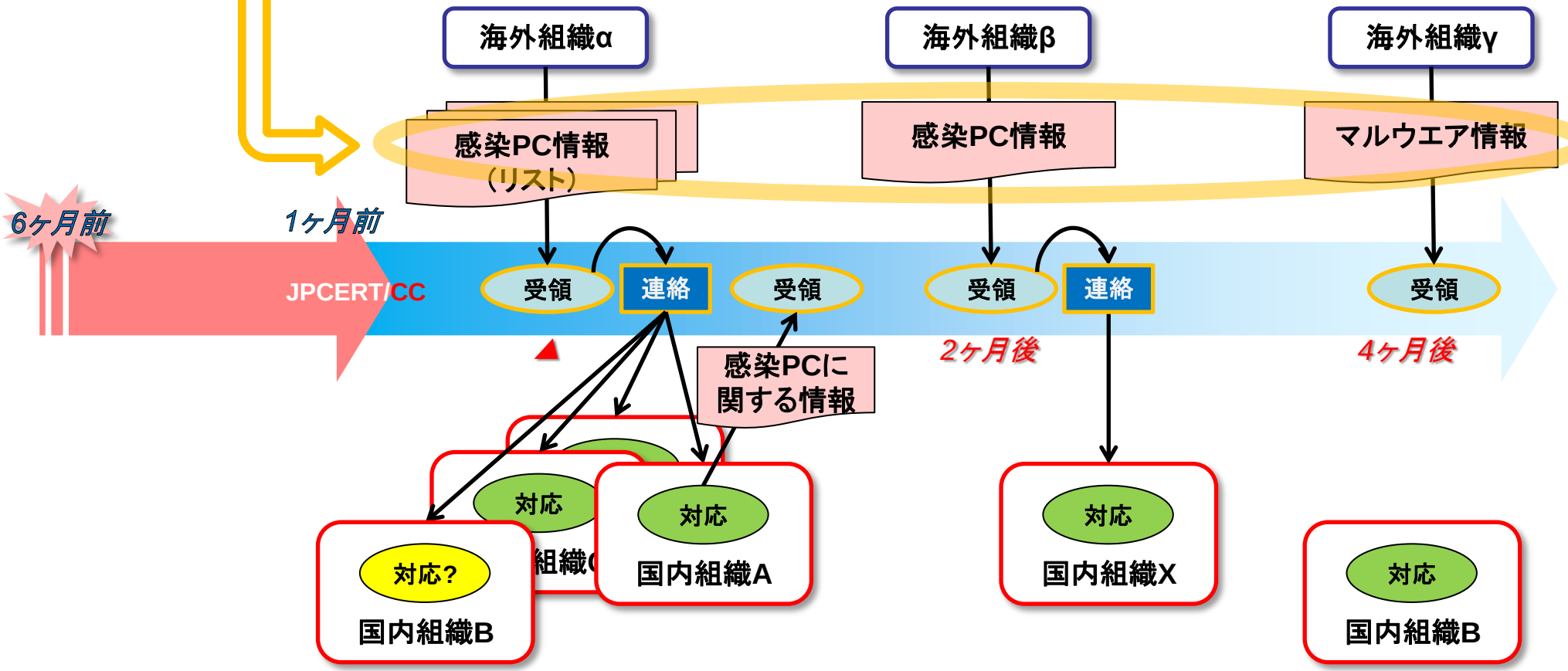
- 海外組織から感染PCに関する情報が提供されたことから調整を開始した事例
  - 国内の複数組織、合計35台の感染PCの情報
    - 接続先・接続元のIPアドレス、MACアドレス等
    - 期間は長いものでは6ヶ月以上
  - 特定の種類のマルウエアに感染している可能性
    - 共通の接続先群を持つ（18個のIPアドレス）
    - 接続先との通信プロトコルとしてHTTPを使う（プロキシ対応）

JPCERT/CCから各組織に連絡



事例② 続き
複数の“侵入”が一連の攻撃として…

- 全て同じ種類のマルウエア
- 共通の接続先もあった

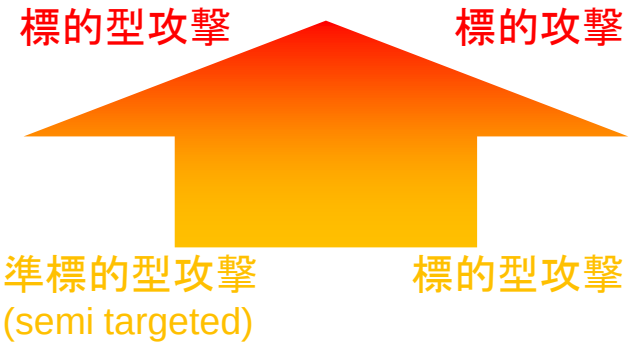


事例①と事例②の比較

	事例①	事例②
攻撃メールの傾向	●海外のサービスを騙るものが目立つ（配達、予約、SNS）	●関係者（っぽい人）や公的サービスを騙る ●会話する
攻撃メールの添付ファイル	●長いファイル名やRLO、アイコン偽装をともなう実行ファイル	●長いファイル名やRLO、アイコン偽装をともなう実行ファイル ●脆弱性を悪用する文書ファイル
マルウエアの流通性	●比較的広い	●比較的狭い
マルウエアの通信先	●概ね短命 ●多数・再利用 ●欧米が目立つ	●短命～長命 ●複数・再利用 ●アジア太平洋地域が目立つ
攻撃の内容	●ほぼ全自動で認証情報等の窃取と他のマルウエアのダウンロード・実行を行う	●遠隔操作ができる状態にしたうえで、以降は侵入してほぼ手動で作業
ウイルス対策ソフトの検知状況	●概ね良い	●概ね悪い

標的型攻撃の特徴

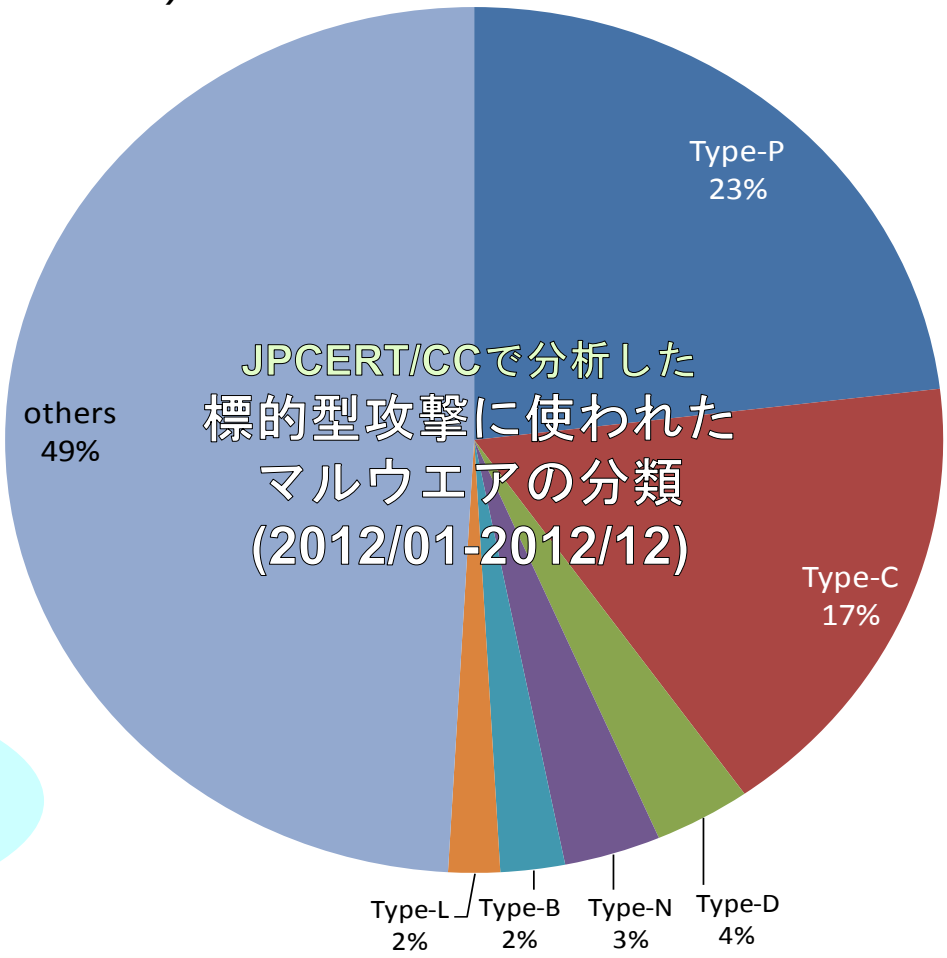
- ソーシャルエンジニアリング的手法
  - 特定の組織や個人を対象とした攻撃
    - かなり“**鋭利**”なソーシャルエンジニアリング
      - ✓ 対象にとって価値のある情報を添える
      - ✓ **鋭利さ故に攻撃を受けた事実を外部に提供し難い**
  - 特定の事柄に関心を持つ人を対象とした攻撃
    - 比較的“**広角**”なソーシャルエンジニアリング
- マルウエアの特徴
  - 未修正の脆弱性が積極的に悪用される
    - 修正アップデートが提供されている脆弱性も悪用される
    - ソフトウエア等の脆弱性を悪用するとは限らない
      → **アイコン偽装やファイル名(拡張子)偽装等で実行ファイルを開かせる**
  - インストールされるマルウエアの傾向
    - 情報収集を基本機能として有する
      → MACアドレスやコンピュータ名等を識別ID代わりに使う
    - **バックドア型のマルウエア(RAT)がインストールされる**
    - 外形的には使い捨てだが、中は同種ツールの使いまわし



攻撃に使われるマルウエアの傾向

- メールに添付されるマルウエア
  - RAT(Remote Access Trojan/Administration Tool)
  - ダウンローダ
- 侵入後に使われるマルウエア・ツール
  - RAT
    - カスタムタイプ
    - コマンドラインタイプ
  - トンネリングツール
    - HTran
  - トラブルシューティングツール
    - Windows Sysinternals

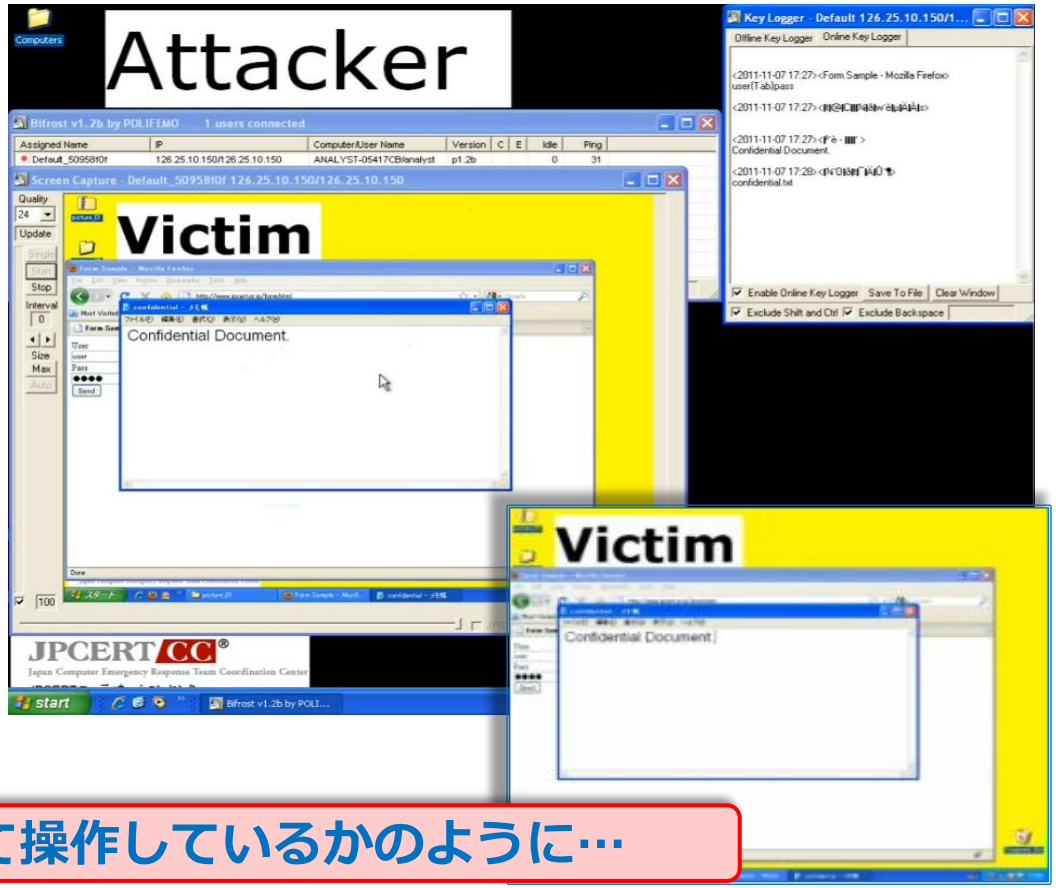
必ずしも
オーダーメイドのマルウエア
が使われるわけではない



侵入に使われるマルウエア

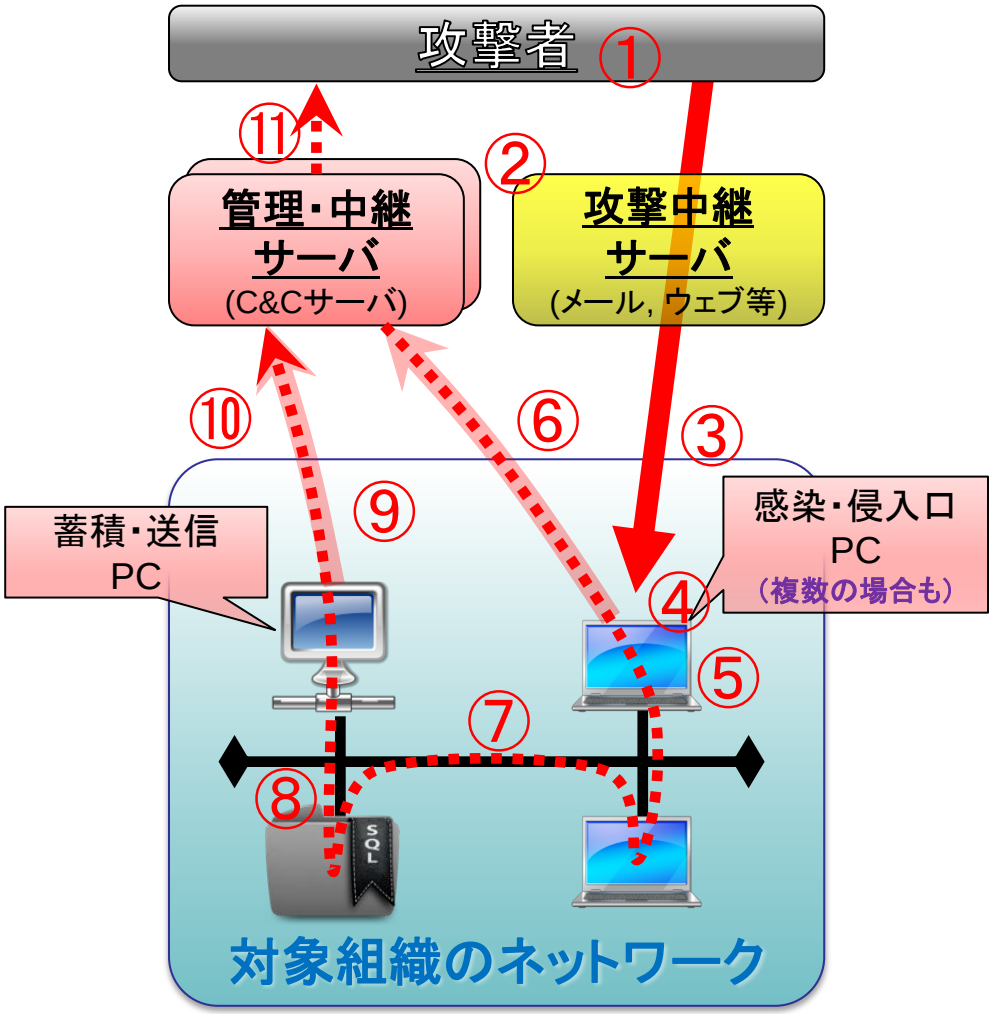
- RAT(Remote Access Trojan/Administration Tool)
  - PCの**遠隔操作**を可能にするツール
  - GUIによりマルウエアの作成やクライアントの管理が可能

  ⇒「**感染**」というよりも「**侵入**」
- 代表的な機能
  - プロセス情報の取得
  - 特定プロセスの停止
  - マシンのシャットダウン
  - 任意のプログラムの実行
  - スクリーンショットの取得
  - Webカメラの操作
  - 音声の録音
  - キーロガー
  - リモートからのデスクトップ操作
  - 特定のウイルス対策ソフトのバイパス



コンピュータの前に座って操作しているかのように…

侵入ステップ



ステージⅠ
- 攻撃のための調査…①
- 攻撃環境の準備…②

ステージⅡ
- マルウエア添付メールの送信…③
- エクスプロイト・インストール…④⑤
- 管理・中継サーバ(C&C)への接続…⑥

ステージⅢ
- 感染PCを経由してネットワークを探索…⑦
- 他のPCに侵入…⑧

ステージⅣ
- 管理・中継サーバ(C&C)への接続…⑨
- 収集した情報の送信…⑩
- 攻撃者による情報回収…⑪

誰がなんのために攻撃しているのか

- 目的、攻撃意図等の多様化
  - ハクティビスト(主義・主張のための攻撃): Anonymous等
  - 利得目的(経済犯)
  - 競争上の情報窃取(知財情報窃取等)
  - 攻撃代行、攻撃環境提供(サイバー攻撃ビジネス)
  - 諜報活動
  - サイバー戦争

2008年ロスに現れたアノニマスを名乗る人たち
ガイ・フォークスの仮面を被っている

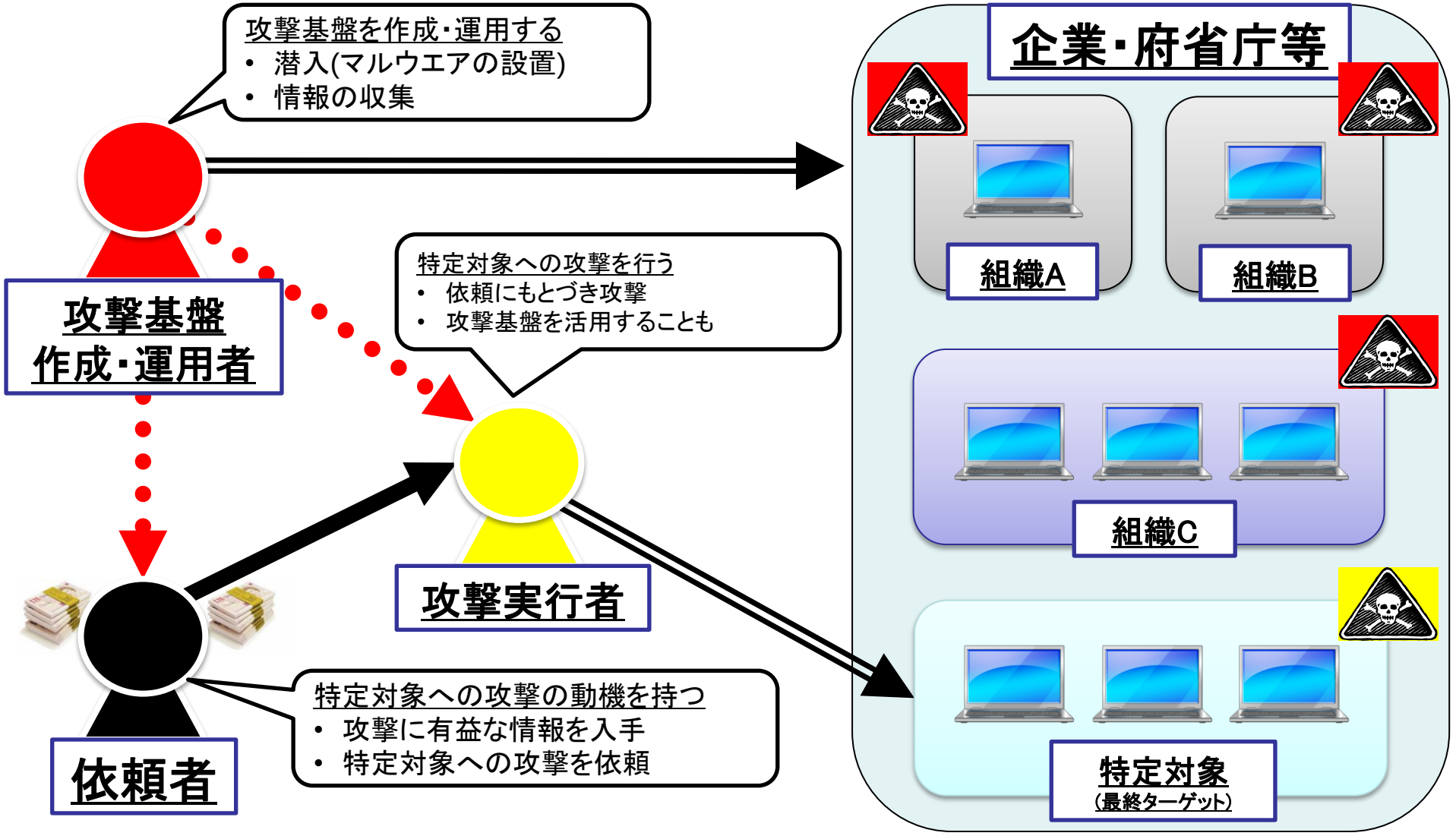
米国の金融機関への攻撃に関する犯行声明を出しているグループのうちの一つ

信頼醸成措置議論の盛り上がり

誰がなんのために攻撃しているのか

- サイバー攻撃がビジネスとして成立する市場
  - 窃取した情報を販売する市場（クレジットカード番号や、ID・パスワード等）
    - とりあえず、情報を漁って、換金
  - 攻撃のためのツールや弱点情報を販売する市場
    - 攻撃のための技術的なスキルがなくても、攻撃が可能
  - 攻撃を請け負うサービスの市場
    - みずから手を汚さなくても、知的財産情報が買えたり、業務妨害ができたりする
- 分業化・攻撃者間の連携が進む：攻撃者のビジネスインフラネットワーク

誰がなんのために攻撃しているのか



攻撃者の目的と意図の多様化（インシデントの傾向の変化）

- 攻撃の対象：

  広くばらまき　→　局所化+特定の情報資産を狙う

  ※移行と言う趣旨ではなく目立つものが変化している趣旨

  - 特定の組織・資産を狙った攻撃：targeted attack（標的型攻撃）
  - 狙った資産を長期にわたってしつこく狙う

- 攻撃の意図：

  愉快犯（攻撃の顕在化）　→　経済的な利得、知的財産・センシティブ情報の窃取、重要インフラに対する攻撃等目的の明確化

  ※移行と言う趣旨ではなく目立つものが変化している趣旨

  - 攻撃の潜行化、高度化（組織化、分業化、専門家）
  - 攻撃手法の作成にかけるコストが巨大化

参考：APT(Advanced Persistent Threat)

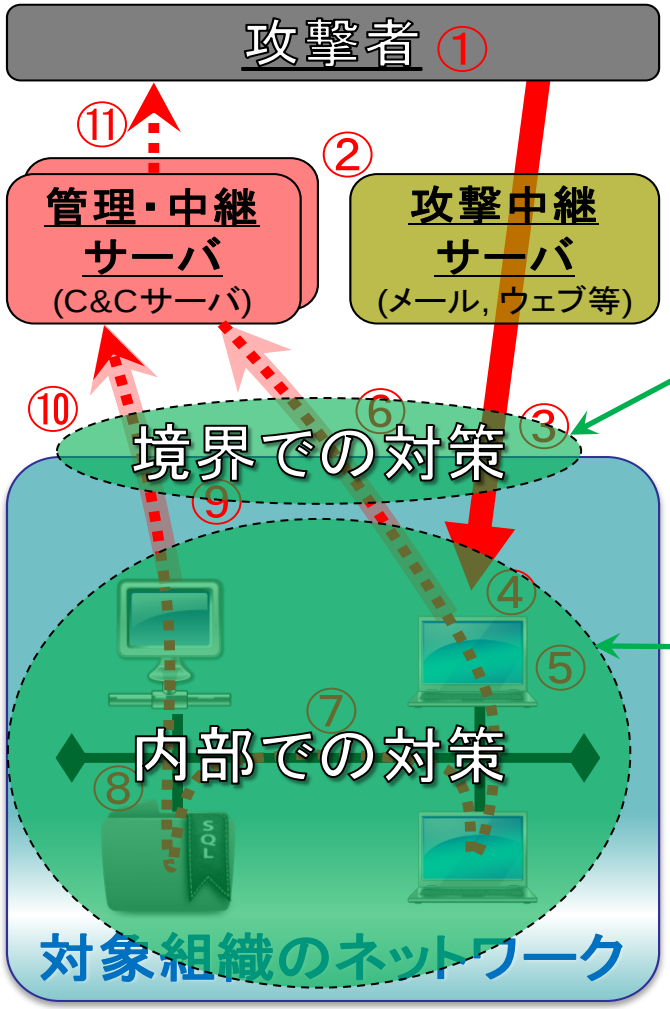
（仮訳）複合的な（たとえば、サイバー上の、物理的な、又は詐欺的な）攻撃手法を用いることにより、目的を達成する機会を作出することができる、高度な専門的知識と莫大なリソースを有する攻撃主体。ここでいう目的とは、一般的に、情報窃取や、任務・事業若しくは組織の重要な局面に関する弱体化又は妨害、あるいは将来においてこれらの目的を実現するための準備行為を目的として、標的とした組織のITインフラ中に、足場を構築し、利用し続けることが挙げられる。
advanced persistent threatは、(i) 長期にわたって、繰り返し繰り返し目的を達成しようとし、(ii) 対策を講じる側の対抗措置に応じて変化し、（iii）目的を達成するために必要となる双方向の通信レベルを維持する確固たる意志をもつ。
※NIST SP800-39 「Managing Information Security Risk: Organization, Mission, and Information System View」 【Appendix B GLOSSAR Y】 http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

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は？

各組織における対策（技術的対策+CSIRT）



情報共有

◆入口・出口対策
◆ユーザのリテラシ向上

組織内CSIRT

◆各サーバ・PCにおける基本対策と証跡保管
◆堅牢なシステム構成と安全な運用

高度解析

（続き）

- 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、機密情報の漏えい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。
  - 技術的な措置
  - 対処のための意思決定権限の移譲（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？

→ たとえば、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）

→ 脅威は変化する＝対策も随時有効性の見直しが必要

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

知見の集約が対抗手段につながる

（参考）組織として対応するための「組織内CSIRT」という考え方

- インシデントへの対応や対処にあたって優先させる事項に関する組織としての意思決定、及びそれを踏まえた事前の対策
  - 優先事項に合わせたシステムにしておかないと、対処できない場合も
- 標的型攻撃を検知し、適切な初動のレスポンス（対応）を行う機能
  - 知識、技術、体制（外部サービスの利用も可）
  - 契約の相手方等から要件として求められる可能性も
  - 初動の対応を失敗すると専門家を呼んでも対処不能になる場合も
- 活動家による攻撃の場合のように、攻撃の結果等が公表される場合には、被害を最小化するための初動の対応の良し悪しが注目を集める可能性も
  - 企業やサービスの評価につながる
- 攻撃の検知のための情報等の共有を受けることが可能となる機能や体制が必要

組織内CSIRT（インシデント対応体制や技術、人材等）の必要性に関する認識の高まり

（参考：続き）CSIRT とは（日本CSIRT協議会作成資料から）

JPCERT CC®

What's CSIRT？ ～ CSIRT※のススメ ～

（※ Computer Security Incident Response Teamの略）

Why 毎回、同じようなトラブルに悩んでいませんか？（企業内の連携）

現 状

✓先月SI部で起こった類似のトラブルが企画部でも発生してしまった。

✓企画部は大変だったらしい。せめてSI部と情報連携できていれば‥。

CSIRTがあれば‥‥

事前予防
✓先月のトラブルをみんなに共有して、注意喚起しよう。

被害低減
✓万一トラブルに遭遇しても前の経験を活かして早期解決しよう。

Why あなたの力だけで十分ですか？（外との連携）

現 状

✓A国で同じような事例が3か月も前にあったのか‥。もし知っていれば手が打てたかもしれない。

✓私の会社は、解析は得意だが、情報収集は苦手だな‥。

CSIRTがあれば‥‥

早期警戒
✓A-CSIRTから被害情報をもらった。私たちも警戒しよう。

比較レビュー
✓他の会社ではこんなふうに情報収集を強化しているのか。参考にしよう。

相互補完
✓私たちの解析結果を外に共有して役立ててもらおう。

What CSIRTは、企業内の「セキュリティインシデント消防署」

✓CSIRTは、**事故前提**（セキュリティインシデント前提）の対応チームまたは機能です。

✓CSIRTは、セキュリティインシデントの窓口となり、情報や経験が集まってきます。

✓CSIRTは、そのノウハウを活かし、セキュリティインシデントに対する経験を積んだ消防員※として振る舞います。

※いざというときのメンバーとして振る舞えるなら、他の業務との兼務も可能です。
その意味で、消防署ではなく、消防団に例えられることもあります。

What CSIRTは、対外的な名刺になる

✓CSIRTは、対外的な交流をも解決します。あなたがCSIRTを自覚し、対外的に準備※し、名乗ることで、あなたの企業と他のCSIRTとの情報交換や協力を可能にします。
この関係は、あなたの企業のセキュリティに寄与する可能性があります。

✓CSIRTには、CSIRTの集うコミュニティ※がいくつもあります。

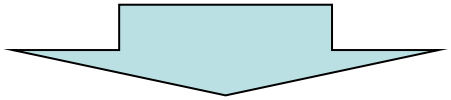
<参考（一部）>
日本シーサート協議会（国内CSIRTコミュニティ）
URL： http://www.nca.gr.jp/
FIRST（CSIRTの国際的コミュニティ）
URL： http://www.first.org/

※1※2 センシティブな情報を扱うため、コミュニティの参加には、審査が必要な場合があります。

参照http://www.nca.gr.jp/

調整機関としてのJPCERT/CCからみた対応のあり方に関する課題

- 攻撃の目的によって、ベストな対応は異なる場合がある。
- たとえば、 経済的利得目的の攻撃であれば、関連サイトの閉鎖等により攻撃者側のコストを上げる調整を迅速に行うことで、攻撃の広がりや被害の拡散を抑止できる場面が多いが、
- APT攻撃の場合は、攻撃元に対する停止依頼等は功をなさず、攻撃に気づいたことや、対象の情報に価値があることを知らせることになってしまうため、攻撃元への調整ではなく、攻撃対象側に近いところでの対処が必要になる場合が多い。
- 主義、主張のための活動家による攻撃の場合は、窃取した情報や対応ぶりが公開される可能性がある一方で、攻撃に対する注目が攻撃の継続や再攻撃のエネルギーになり得るので、水面下での情報収集、対処が求められるところ。



- 攻撃の主体や目的の切り分け（トリアージ）を、より早い段階で、適切に行うことにより、迅速かつ適切な対処を行うことができる。
- 攻撃を受ける個々の企業にとっては、現象的には同じに見える攻撃も、関連情報を集めて分析することで、切り分け、及びそれに基づく、適切な対処が可能となる。

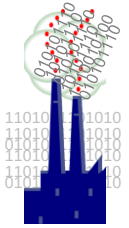
各企業等でそのように役立ててもらえる情報を提供することができるよう、
JPCERT/CCは、より多くのインシデントや攻撃に関連する情報を集約し、分析を行い、
適切な方法で情報提供を行う必要がある。

【もし時間があるようなら】
リスク低減モデルについての議論の動向

JPCERT CC®

環境問題対策モデル

- インターネットの犯罪インフラの破壊；ボットネットのサイズとパワーの縮小
  - 犯罪組織が活動しにくいサイバー環境に
  - ボットに感染したシステムのクリーンアップにより、マルウェアの伝搬を低減する
  - 公衆衛生モデルや、環境問題対策のモデルにも通じる
    - 多数の実装、マイクロソフトによる公衆衛生モデル提唱、EWI によるエクスパート論文、CCSA論文など
  - 環境対策モデルのアプローチの利点：全てのステークホルダーによる、様々なレベルの取り組みによるもの
  - グローバルな連携、コーディネーションが不可欠



Clean the environment

（続き）グローバル公衆衛生／サイバー健全性

- グローバル公衆衛生の2つの特徴
  - 罹患率/疾病の発生率の効果的な測定
  - 感染の突発/まん延への対応

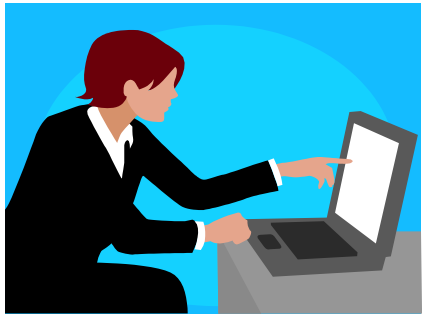
Protect international public health

- WHO仕組みの機能
  - 広範囲の関係機関の従事　－　グローバル、ローカル、政府機関、病院、研究センターの従事。政府／民間の財政的支援システム
  - 科学的手法　－　明確なメトリックス、測定方法
  - 制度化されたデータ収集、対応支援
  - 公衆衛生の専門家による教育と、ベストプラクティスの開発

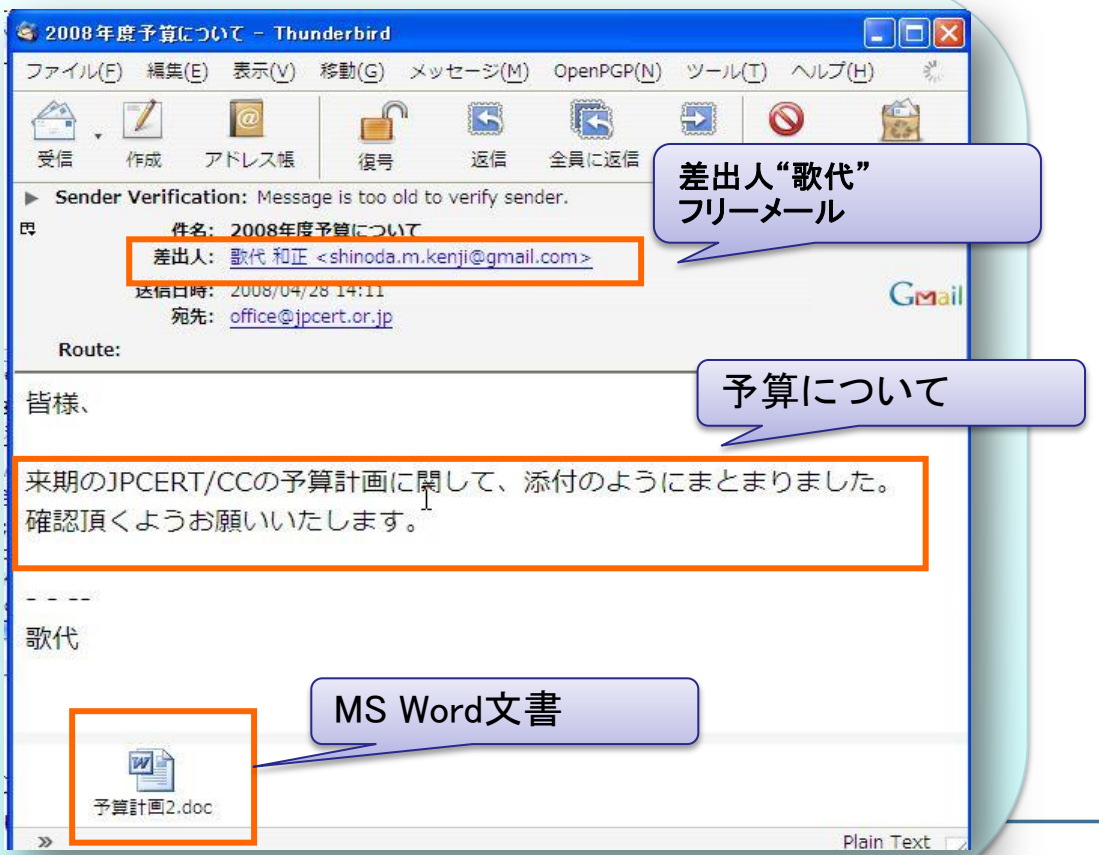
最近のイニシアティブ：
OECDにおける、サイバーセキュリティ指標の取り組みなど

【参考】標的型攻撃メールへの耐性をつけるための演習「ITセキュリティ予防接種」

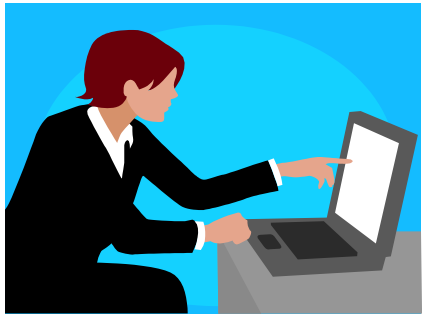
■ ITセキュリティ予防接種(以下「予防接種」)とは
「電子メールを用いた受動型攻撃に対するエンドユーザのセキュリティ意識の向上を目的とする調査・訓練の手法で、対象者に不審メールを模した無害なメールを送付し、適切な取扱いを行えるかを試すもの



2007年度から
JPCERT/CCにおいて、IT予防接種の効果及び効率的な実施方法を調査する目的で、
国内企業に対して実施。
2008年度は、
14組織 2600名 (8業種)を対象に実施



（続き）



本件に関するお問い合わせ先: ●●部 ●●、●●部 ●●

ご注意！ このような怪しいメールの添付ファイルを不用意に開封すると
あなたを狙うウイルス等に感染する恐れがあります
（このメールは統計調査のためのものです）

本添付ファイルを届けたメールは、調査のために不審メールを模したもので、本文・件名に記載された内容は架空のものです。
調査結果は有限責任中間法人 JPCERT コーディネーションセンター（JPCERT/CC）に提供し、同様のメールによる脅威への予防活動に活用されます。結果は統計数値として取り扱われますので個人名等が公表されることは一切ありません。

調査精度を上げるため、各位に事前説明を行わずに送付しております。事後のお願いとなりますが、実施にご協力をいただけますよう、何卒よろしくお願い申し上げます。

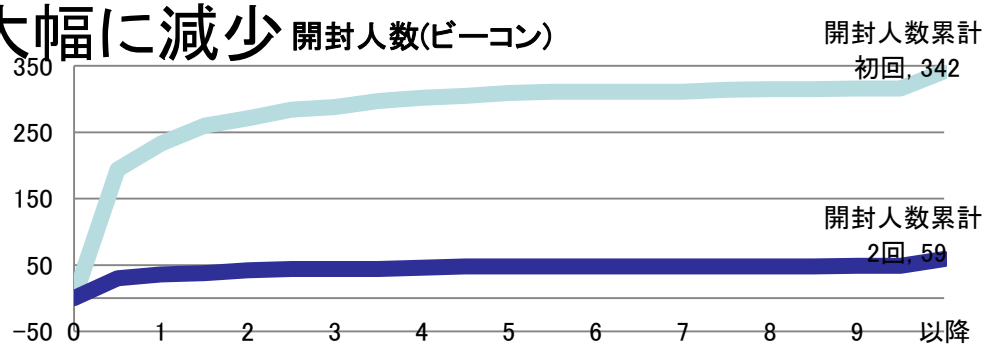
本添付ファイルに危険性はありません。ウイルス／ワームとしての機能はありません。
添付ファイルを開いた際にインターネット上の訓練用ウェブサイトに置かれた画像を読み込んで表示することで、添付ファイルのオープン状況の確認を行なっています。

○不審なメールと添付ファイルがもたらす脅威（標的型攻撃）:
近年、特定の組織・職員を狙う「不審なメール[illegible]（標的型攻撃）」が増加する傾向にあります。
標的型攻撃の偽メールは、従来のウイルス対策[illegible]
メールボックスまで直接届きます。もっとも[illegible]
してしまうと、ウイルス等への感染や情報[illegible]
被害を避けるためには、各自が不審な[illegible]

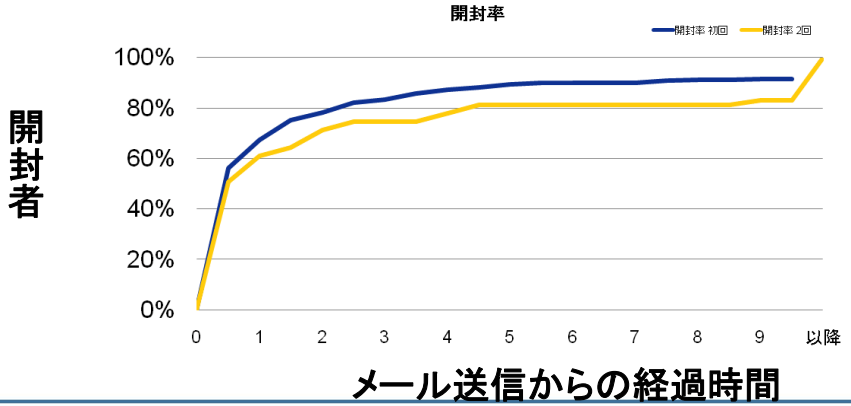
見えない画像ファイルへのリンクを埋め込む
http://targeted.example.co.jp/user1.jpg

ITセキュリティ予防接種の効果

■添付ファイルを開封する者は、大幅に減少



【参考】メール依存度が高い業種では、最初の1時間でほとんどの人がメールを確認する。→ システム管理者が気づいてからアラートを発しても間に合わない。＝日頃のトレーニングが必要



【調査結果の概要】

➢“いままでどんなに研修を受けても、情報だけは蓄積されるが、今回の予防接種メールで一気に**情報が経験**になり、これ以降のメール全てに注意を払うようになった。“

✓単なる情報を経験にするという作業が必要

➢誰もが等しく危険

✓経験年数や職種を問わない

➢組織におけるインシデントの報告体制が機能しているかどうかを確認することができる。

✓怪しいと思った時に管理者に連絡する体制の周知・確認

※JPCERT/CCの調査報告書
http://www.jpcert.or.jp/research/2009/inoculation_20090619.pdf

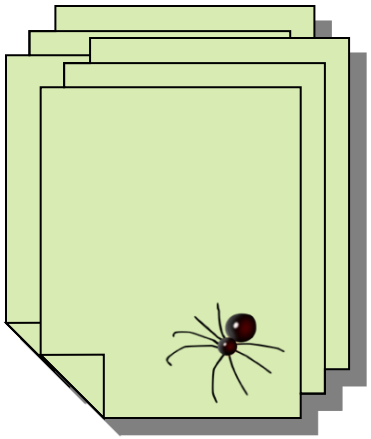
希望者へのツール提供

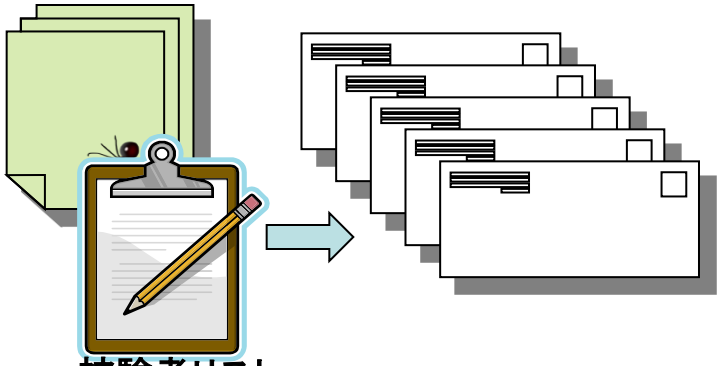
予防接種メール作成ツール

配送ツール

Webバグ挿入

メール作成





被験者リスト
メールテンプレート

無償、但しサポートは不可
お問い合わせは: office@jpcert.or.jpまで

ご質問、お問合わせは

- インシデントの報告、対応依頼
  - https://www.jpcert.or.jp/research/#webdefacement
  - 電子メール：info@jpcert.or.jp (PGP 公開鍵)
  - (*) JPCERT/CC PGP 鍵が更新されました。詳細はリンク先をご覧下さい。
  - FAX： 03-3518-2177　(インシデント報告以外のものは 03-3518-4602)
  - 電話： 03-3518-4600
- 制御システムインシデントの報告
  - https://www.jpcert.or.jp/ics/ics-form
  - 電子メール：icsr-ir@jpcert.or.jp
- 早期警戒情報の配信
  - https://www.jpcert.or.jp/wwinfo/
  - JPCERT/CC　早期警戒グループ　早期警戒情報登録受付窓口　E-mail :ww-info@jpcert.or.jp
- 注意喚起、ウィークリーレポート等を受信いただくJPCERT/CCメーリングリストへの登録
  - http://www.jpcert.or.jp/announce.html
- 脆弱性関連情報流通（自社製品に関する脆弱性情報についての連絡を受け取る）製品開発者リストへの登録
  - http://www.jpcert.or.jp/vh/regist.html
- 制御システムセキュリティ情報共有コミュニティ
  - JPCERT/CC 情報流通対策グループ 制御システムセキュリティ担当
    E-mail：cs-security-staff@jpcert.or.jp