Internet Week 2012　～ S1 標的型攻撃の現状と対策 3) ～

攻撃事例に見る
情報連携の役割と取り組みの紹介

JPCERTコーディネーションセンター
理事・分析センター長　真鍋　敬士

2012年11月19日

本日お話ししたいこと

17:10–18:00	**3) 攻撃事例に見る情報連携の役割と取り組みの紹介** **講演者**: 真鍋 敬士(JPCERTコーディネーションセンター) **内容**: 標的型攻撃による被害というのは、攻撃の対象や進行度によって異なり、なかなかはっきりしないものです。しかし、人や組織を孤立・隔離させることもこの攻撃の特徴であり、対策をする立場からすれば少なからず発生している被害であると言えます。ここでは、対策において各組織が孤立・隔離を強いられることがないように、攻撃に使われたマルウエア等の特徴を説明するとともに、情報連携の取り組み例を紹介します。

傾向と事例

- 標的型攻撃
- 人を欺く技術
- 攻撃事例

対策と取り組み

- 攻撃を分析する
- 情報連携

JPCERT/CCをご存知ですか？

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)
- 経済産業省からの委託事業として、情報セキュリティ対策推進事業（不正アクセス行為等対策業務）を実施

－ JPCERT/CCをご存知ですか? －

JPCERT/CCの活動

インシデント予防

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

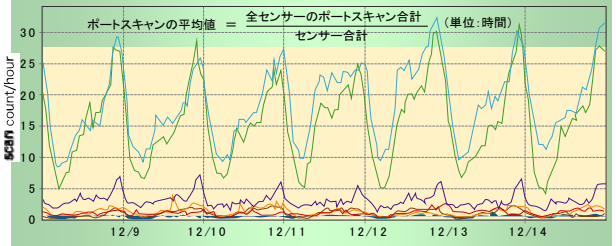
JVN Japan Vulnerability Notes

インシデントの予測と捕捉

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

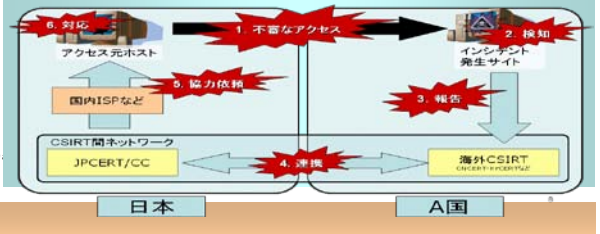


発生したインシデントへの対応

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

標的型攻撃

標的型攻撃の特徴

ソーシャルエンジニアリング的手法

- 時事ネタ（興味をひく）
  - ✓ 新型インフルエンザ
  - ✓ 震災関連情報
- 私的情報（信用させる）
  - ✓ 自分が送ったメールに対する返信
  - ✓ 上司や顧客、ビジネスパートナー等からのメール
- 機密情報（孤立させる）
  - ✓ 異動通知

未修正の脆弱性の悪用

- アプリケーションの脆弱性
  - ✓ 文書ファイル型(doc, xls, pdf, …)
- OSの脆弱性
  - ✓ 実行ファイル型(exe, dll, …)

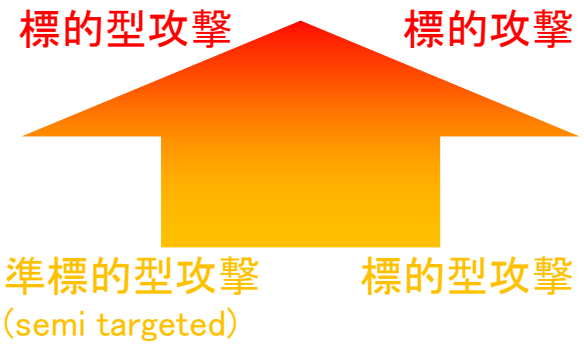
と、言われていますが…

✓低い拡散性
⇒パターン検知での対応に時間がかかることも
✓未修正の脆弱性
⇒根本的な対策ができない

被害を受ける危険性が高い

実際の攻撃に見られる傾向

- 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

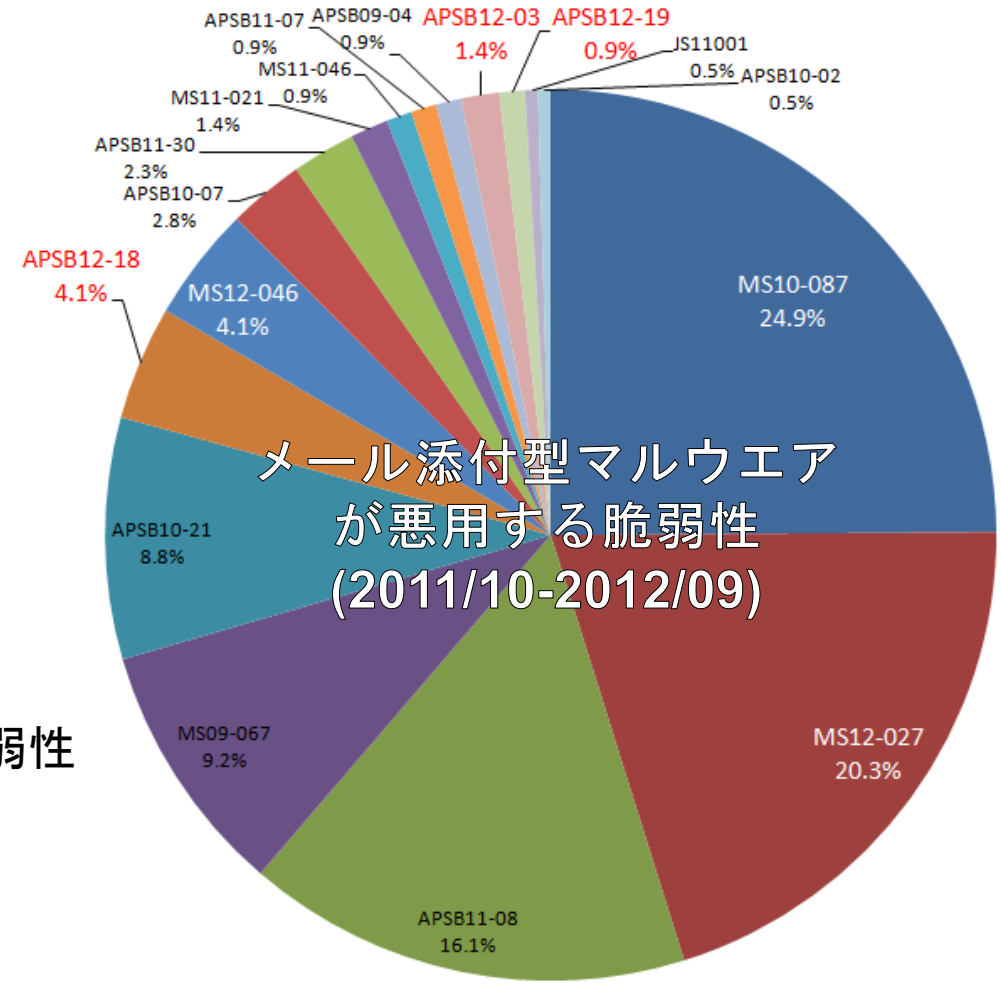
“ゼロデイ”
とは限らない!!

“特注品”
とは限らない!!

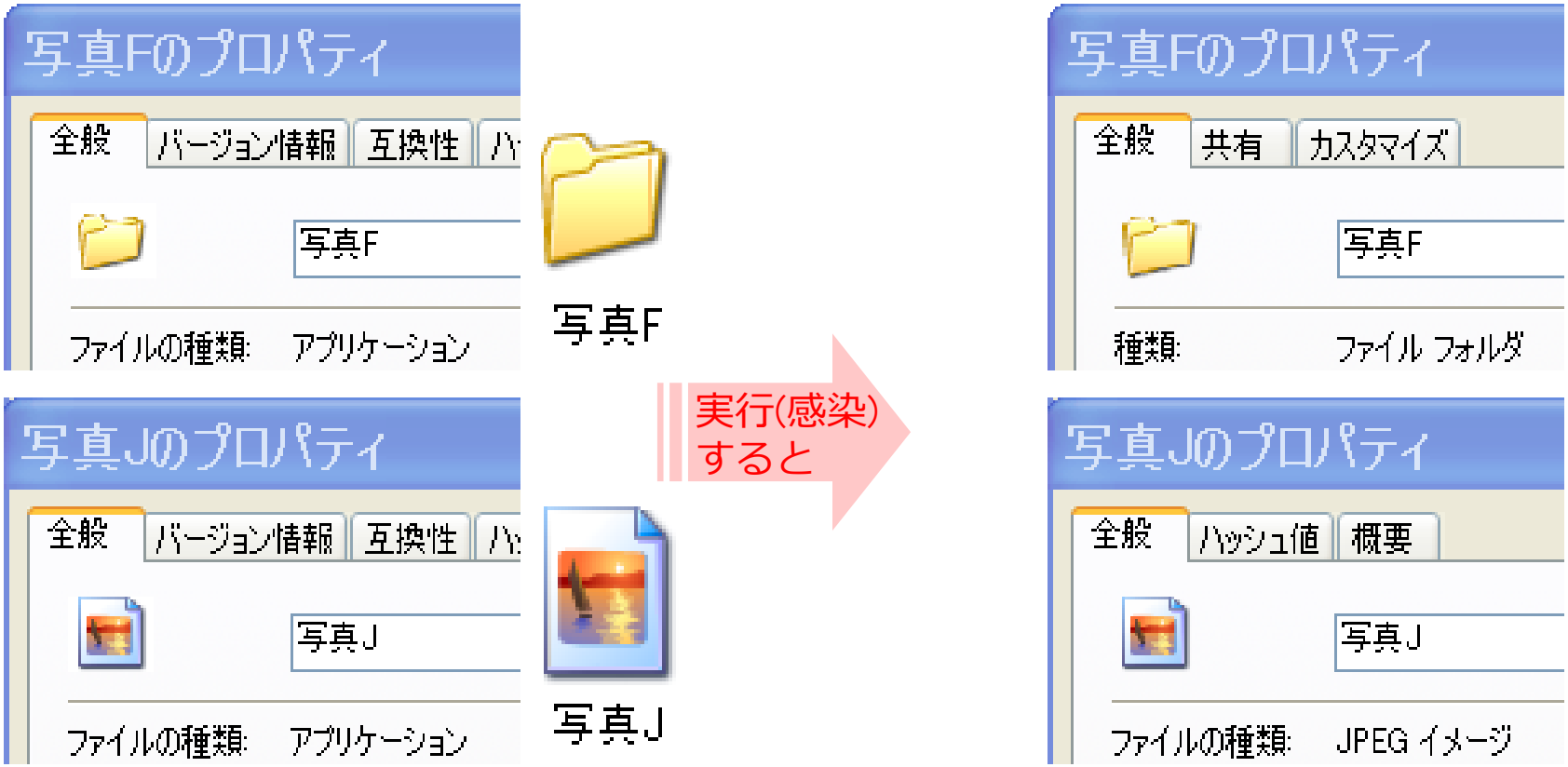
人を欺く技術

悪用される脆弱性の傾向

- Microsoft Officeの脆弱性
  - 2012年3月以前
    CVE-2010-3333(MS10-087)
  - 2012年4月以降
    CVE-2012-0158(MS12-027)
- Flash Playerの脆弱性
  - 2012年は当たり年
    CVE-2012-0753(APSB12-03)
    …
    CVE-2012-1535(APSB12-18)
    CVE-2012-41xx(APSB12-19)
    CVE-2012-52xx(APSB12-22)
  - Action Scriptの悪用
- 安全でないライブラリのロードの脆弱性
  - シェル拡張との組み合わせ
    CVE-2011-1991(MS11-071)
  - 未修正のまま悪用
    CVE-2012-1854(MS12-046)
  - マルウエアではないソフトウエアにDLL形式のマルウエアをロードさせる手法が少なからず悪用されている



アイコンの偽装

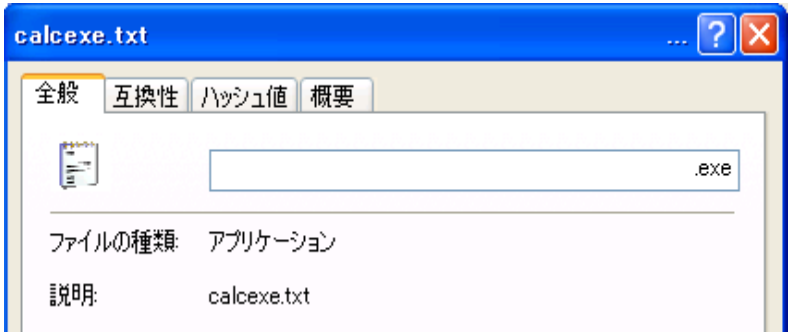


ファイル名の偽装

長いファイル名

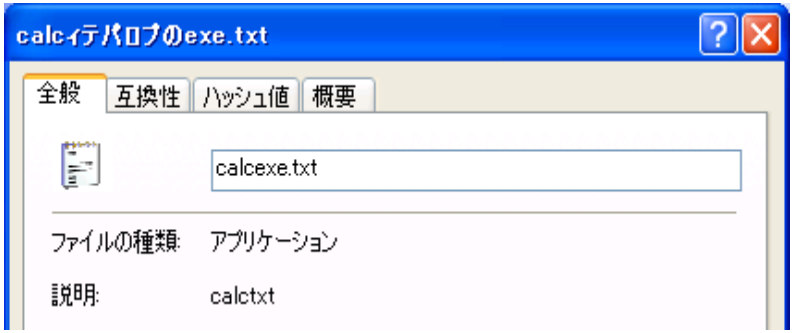
calcexe.txt

...



Unicode制御文字(RLO: Right-to-Left Override)

calcexe.txt

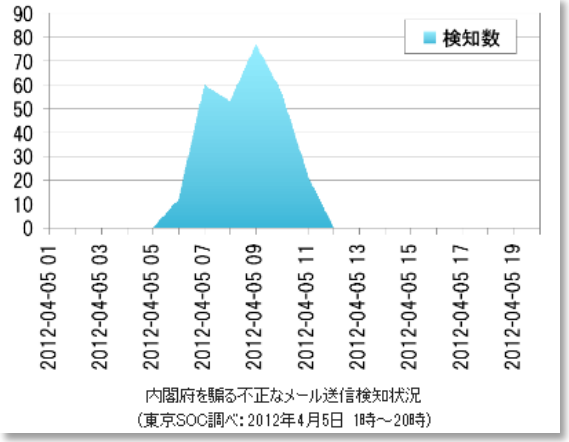


攻撃事例

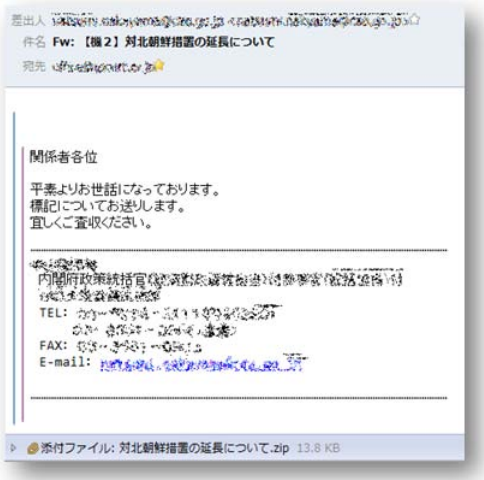
標的型“ばらまき”攻撃???

【標的型攻撃メールの体裁でマルウエアがばらまかれる】

- 典型的な特徴
  - 公的機関の個人を騙りつつもフリーメールから送信
  - Poison Ivy RATに接続可能なマルウエア
  - 一回の“ばらまき”に見られる共通性・類似性
    - 送信元IPアドレス
    - 配送用メールサーバ
    - Fromアドレス
    - マルウエア
- 2012年の代表的な“ばらまき”攻撃
  - 3月15日頃
  - 3月19日頃
  - 4月5日頃
  - 10月10日



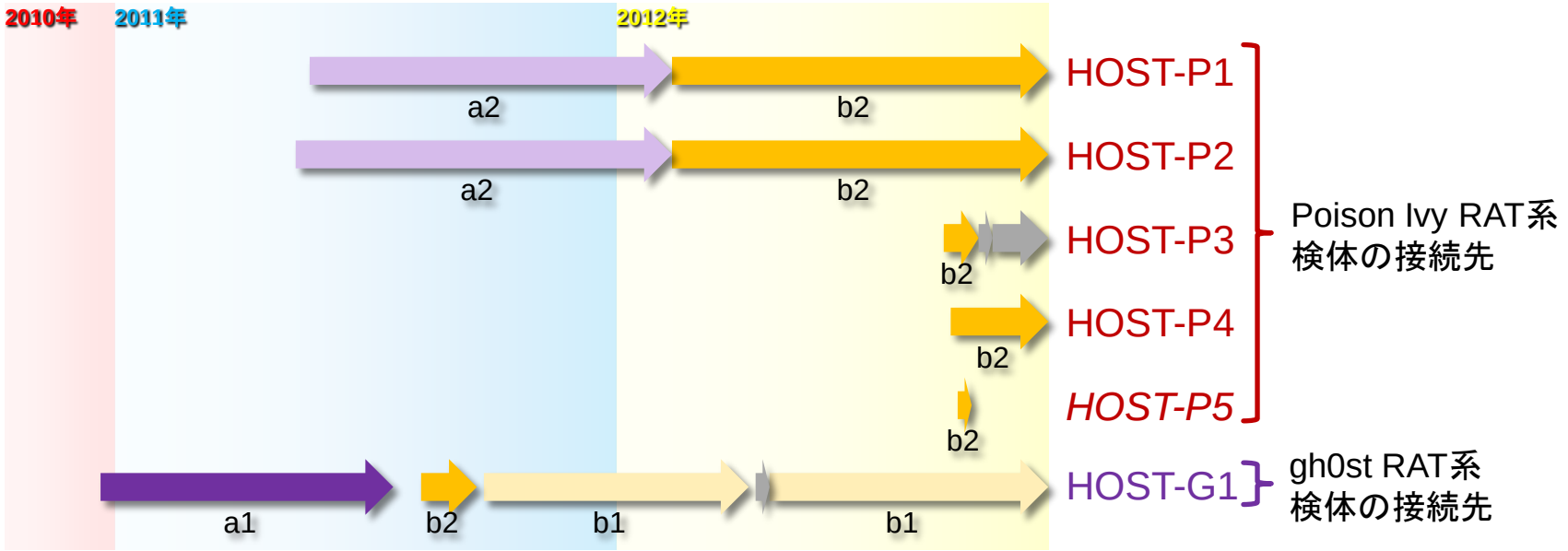
【出典】https://www.ibm.com/blogs/tokyo-soc/entry/virus_mail_20120405?lang=ja



⇒「失敗」説や「おとり」説などもあるが、毎回感染報告が…

ある“ばらまき”攻撃に注目

- フリーメールを使って送信
  - 送信元IPアドレスは同一（国内）
  - Fromアドレスは類似
- 添付されたマルウエア（Poison Ivy RAT系）の接続先はHOST-P5
  - HOST-P5を名前解決するとIPアドレスはb2
  - b2に名前解決されたことのある接続先を調査⇒6個

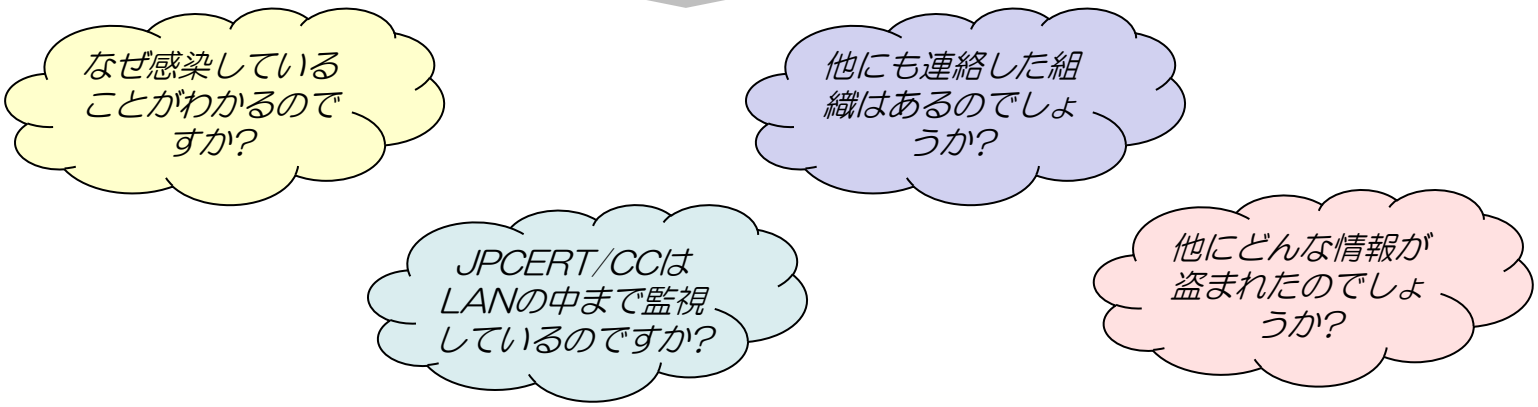


感染PCに関する情報の展開

【海外組織αから感染PCに関する情報が提供される】

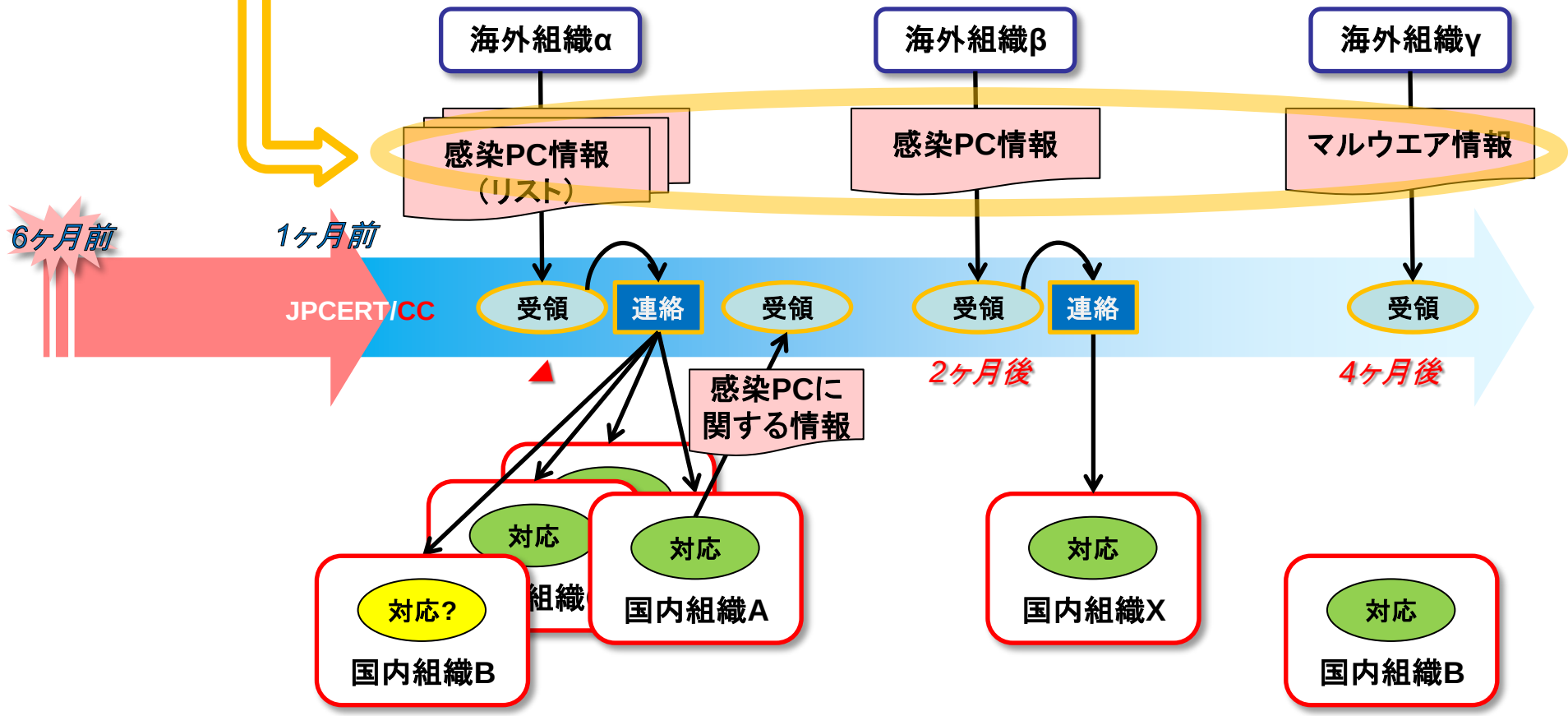
- 国内の複数組織、合計35台の感染PCの情報
  - 接続先・接続元のIPアドレス、MACアドレス等
  - 期間は長いものでは6カ月以上
- 特定の種類のマルウエアに感染している可能性
  - 共通の接続先群を持つ（18個のIPアドレス）
  - 接続先との通信プロトコルとしてHTTPを使う（プロキシ対応）

JPCERT/CCから各組織に連絡



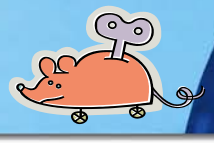
複数の“侵入”が一連の攻撃として…

- 全て同じ種類のマルウエア
- 共通の接続先もあった



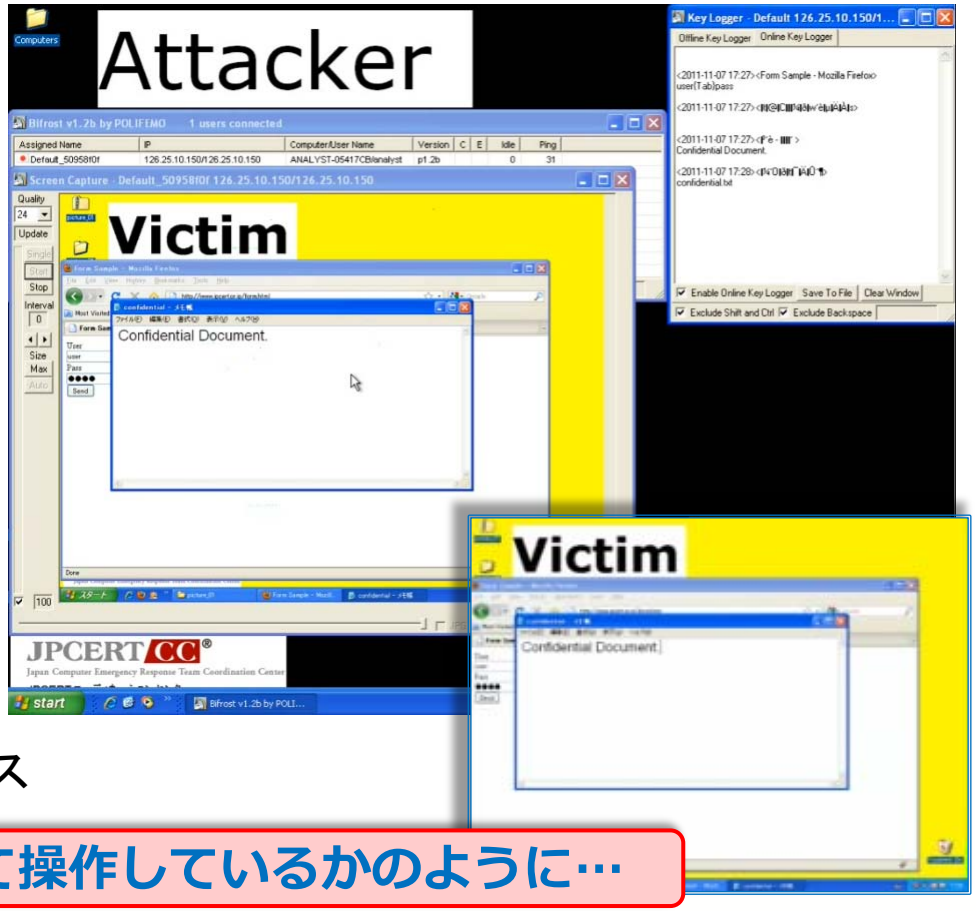
攻撃を分析する

RAT(Remote Access Trojan/Administration Tool)



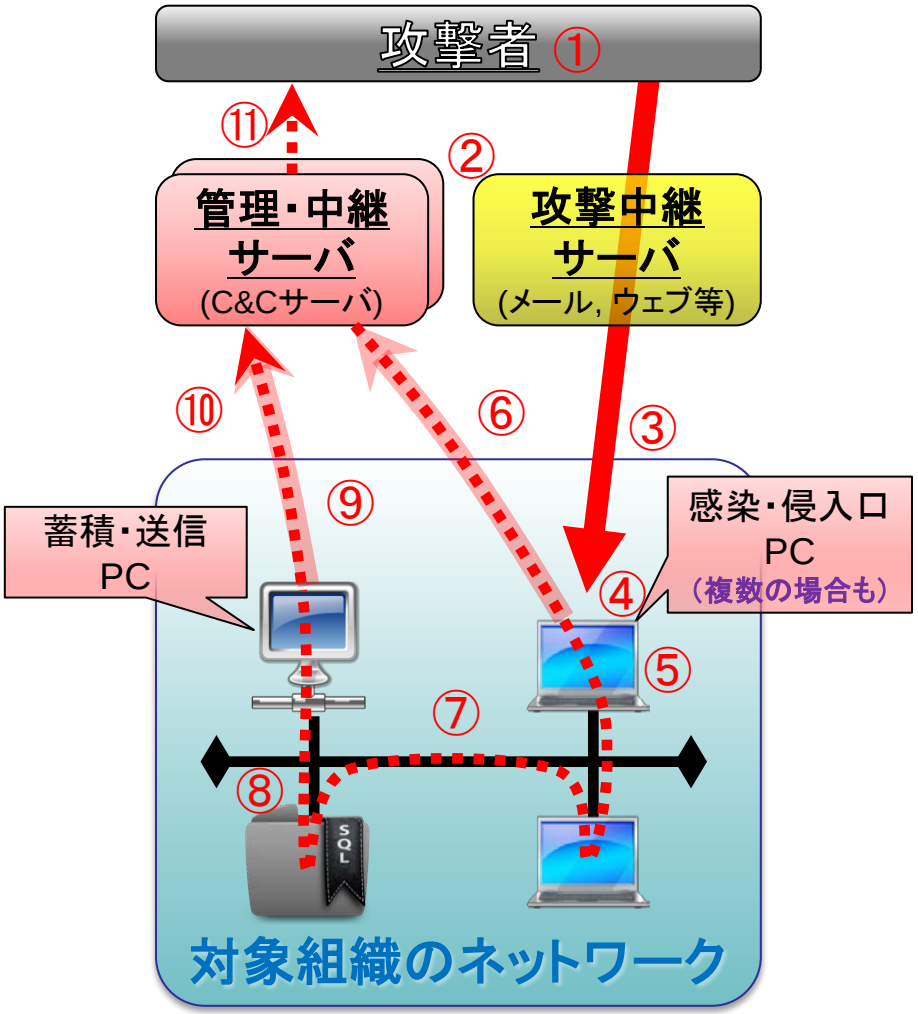
- PCの**遠隔操作**を可能にするツール
  - GUIによりマルウエアの作成やクライアントの管理が可能
    ⇒「**感染**」というよりも「**侵入**」

- 主な機能
  - 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

攻撃ビジネス（仮定）

JPCERT CC®

攻撃基盤を作成・運用する
- 潜入(マルウエアの設置)
- 情報の収集

攻撃基盤作成・運用者

特定対象への攻撃を行う
- 依頼にもとづき攻撃
- 攻撃基盤を活用することも

攻撃実行者

依頼者

特定対象への攻撃の動機を持つ
- 攻撃に有益な情報を入手
- 特定対象への攻撃を依頼

企業・府省庁等

組織A

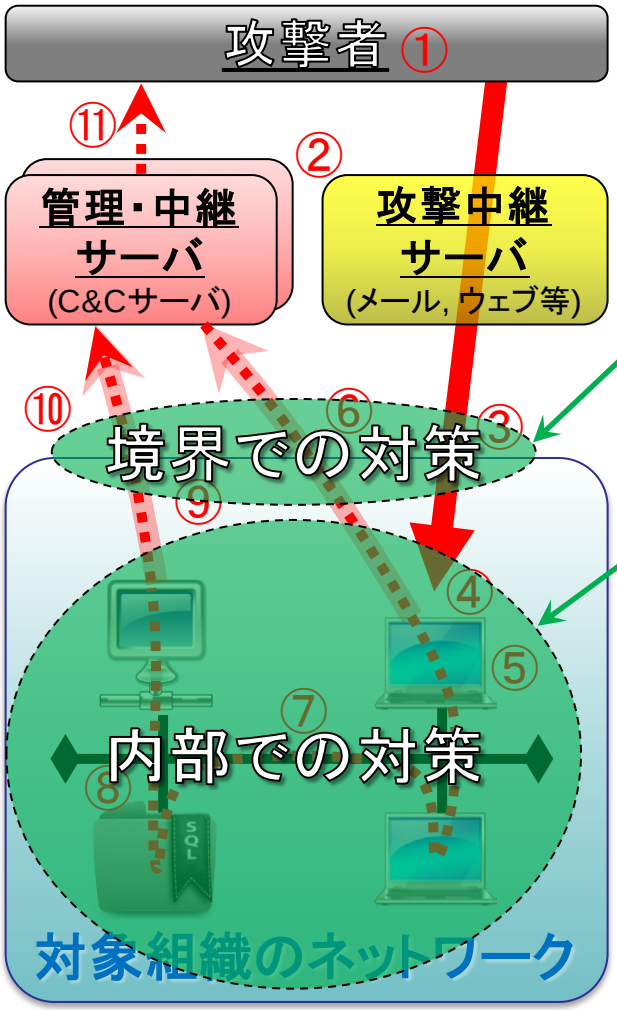
組織B

組織C

特定対象
（最終ターゲット）

情報連携

各組織における対策



情報共有

◆入口・出口対策
◆ユーザのリテラシ向上

◆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

	攻撃フェーズ
①	Target Discovery 攻撃対象の調査
②	Attack Tool Tailoring 攻撃環境・ツールの組み立て
③	Delivery メール等による配布
④	Exploit 脆弱性の悪用
⑤	Installation マルウエアのインストール
⑥⑨	Command and Control 外部との通信
⑦⑧	Action on Objectives 本来の目的の遂行

情報連携に向けた取り組み例

- 2011年: 対策のための共有
  - ISOG-J 標的型攻撃対策検討WG
  - 警察庁 サイバーインテリジェンス情報共有ネットワーク(CCI)
  - 経済産業省 サイバー情報共有イニシアティブ(J-CSIP)
- 2012年: 対策手段の拡充
  - 警察庁 サイバーインテリジェンス対策のための不正通信防止協議会
  - 総務省・経済産業省 サイバー攻撃解析協議会

    http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000021.html

    http://www.meti.go.jp/press/2012/07/20120711002/20120711002.html

    - 総務省
    - 経済産業省
    - 独立行政法人情報通信研究機構(NICT)
    - 独立行政法人情報処理推進機構(IPA)
    - テレコム・アイザック推進会議
    - 一般社団法人JPCERTコーディネーションセンター
    - 内閣官房情報セキュリティセンター(オブザーバー)

独りで闘おうとしていませんか?

攻撃者は様々な手段を用いて目的を達成しようとする

- 複数の攻撃先、繰り返される攻撃
- 真の「標的」攻撃はわけて考える

「分断・孤立」は攻撃側の拠りどころ

- ピン攻撃は攻撃側としてもリスキー
- 知見の集約が対策手段を拡大させる

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：office@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。