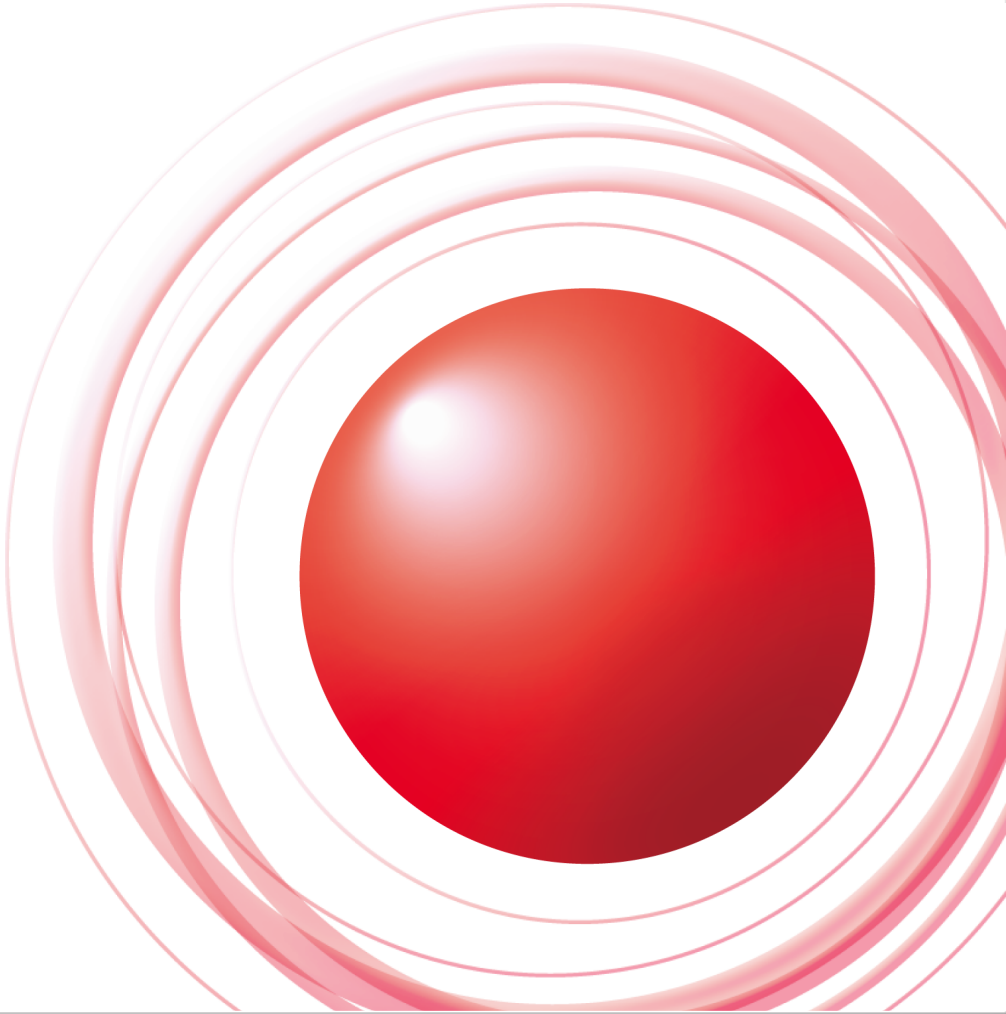
IIJ Technical WEEK 2011

セキュリティ動向 2011

IIJ Internet Initiative Japan



2011/11/11
株式会社インターネットイニシアティブ
サービス本部 セキュリティ情報統括室
齋藤 衛

Ongoing Innovation

セキュリティ動向2011

標的型攻撃

Anonymous等Hacktivismの活動

DDoS攻撃

内部犯行

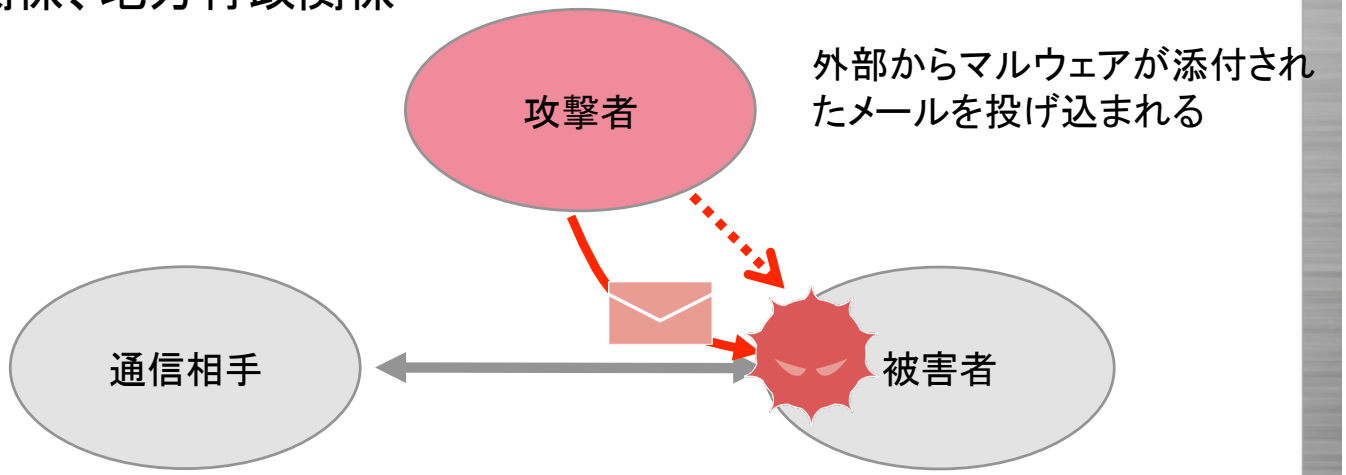
RAT

標的型攻撃について

セキュリティ動向2011

標的型攻撃

- **大手企業を狙った標的型攻撃(報道ベース)**
  - 攻撃の公開(読売新聞等 9/19)
  - メール発信元は業界団体(重工複数社の加盟する団体)。8月26日実在の人物のからのメールにマルウェアが添付。タイトル「資料事前送付」、添付ファイル「一括調達に係るコメント」。「本文は幹部が約10時間前、実際に関係者に送信した文面がほぼそのまま引用されていた。」(読売新聞 10/15)
  - 外部サーバに30万回接続(NHK 10/11)
  - 「防衛関連機密の流出なし」(日本経済新聞11/09)
- **他の攻撃**
  - 同業企業、政府関係、地方行政関係



セキュリティ動向2011

Anonymous等のHacktivismの活動

- Anonymous 海外匿名掲示板の利用者から発生した集団で、世界中に広まっている。デモなど一般的な誇示活動とともに、一部がネットワーク上での攻撃にも関与。
- 2008年Anonymousの一部(AnonOps等)がサイエントロジー教会へのDDoS攻撃を実施。以降、AnonOpsは常習的にDDoS攻撃を実施するようになった。
- 全体を指揮する中心人物や組織は存在せず、活動に関する議論は掲示板やチャットで公開されている。
- 最近ではWikiLeaksへの資金流入を止めた金融機関へのDDoS攻撃、中東ジャスミン革命に応じたインターネット遮断などに反対した活動としてのDDoS攻撃以後、理由を見つけては各方面を攻撃している。
- 2011年5月以後、メンバーと考えられる人が次々と逮捕。しかし活動は継続中。
- 主な攻撃活動
  - 特定企業に関する攻撃 #OpSony,#sonyRecon: Sony PlayStationに関連する攻撃
  - 特定国家に対する攻撃 #OpTunisia, #OpTurky,#OpTibya…
  - 特定の活動に対する攻撃 #OperationGreenRighit (環境破壊)
- 攻撃手段も多岐に及ぶ
  - DDoS、情報漏えい、アカウント盗用

ガイ・フォークスのお面をかぶった
Anonymousメンバー

Vフォー・ヴェンデッタ（***V for Vendetta***）ワーナー・ブラザーズ2006

セキュリティ動向2011

DDoS攻撃

- 依然として一般企業に対するDDoS攻撃がさまざまな理由で発生。一般のDDoS攻撃で最大3Gbpsの通信量で、45万ppsのUDP flood (7月)を観測。
- 歴史的背景等に起因するDDoS攻撃も継続・

9月18日の状況

複合攻撃(HTTP SYN flood+GET flood)	600Mbps/1.2Mpps
UDP flood	635Mbps
TCP connection flood	数千cps
HTTP get(post) flood	数千cps

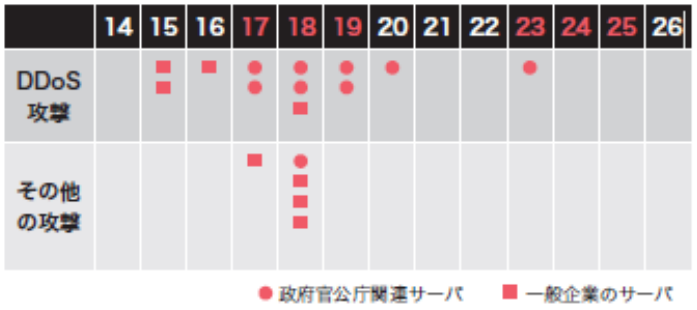
継続時間はそれぞれ1，2時間程度

その他の攻撃

SQLインジェクション

脆弱性サイト捜索

FTPパスワードブルートフォース攻撃

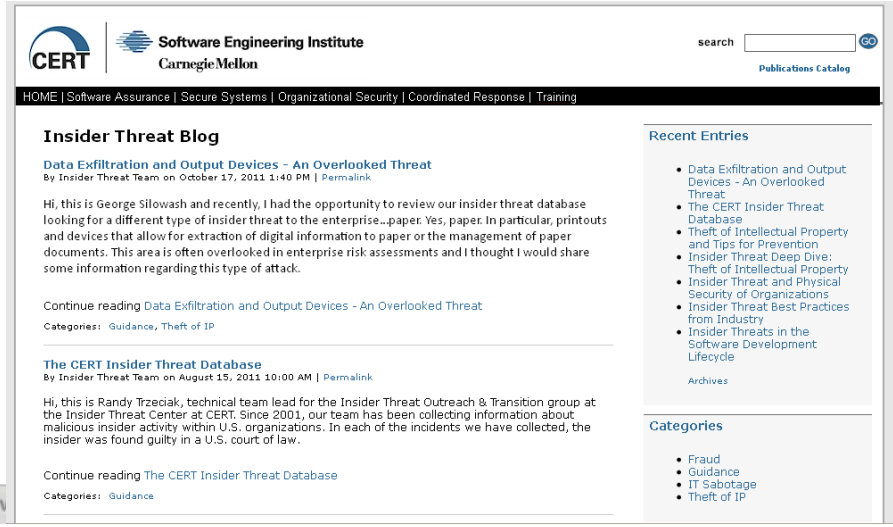


一連の攻撃の様子(2011年9月)

2011年9月18日関連の攻撃予告の例

内部犯行

- 2011年2月米国製薬会社で解雇された元従業員により社内サーバが破壊される。物理サーバ15台上のVMイメージ88台を削除、メールサーバ、財務管理サーバ等を破壊され2日間業務が停止。80万ドル程度の対応費用。
- 2011年5月携帯ゲームで130万人分のデータ(ゲーム上の服装など)が、元派遣社員により改ざん。
- 2011年5月携帯事業者で契約社員が作成した不正プログラムによる通信障害が発生。回線設定データの改ざんにより、携帯電話用基地局が停波。関西地方で約7万2700人のユーザーに影響。



CERT-CC Insider Threat Blog
http://www.cert.org/blogs/insider_threat/

RAT

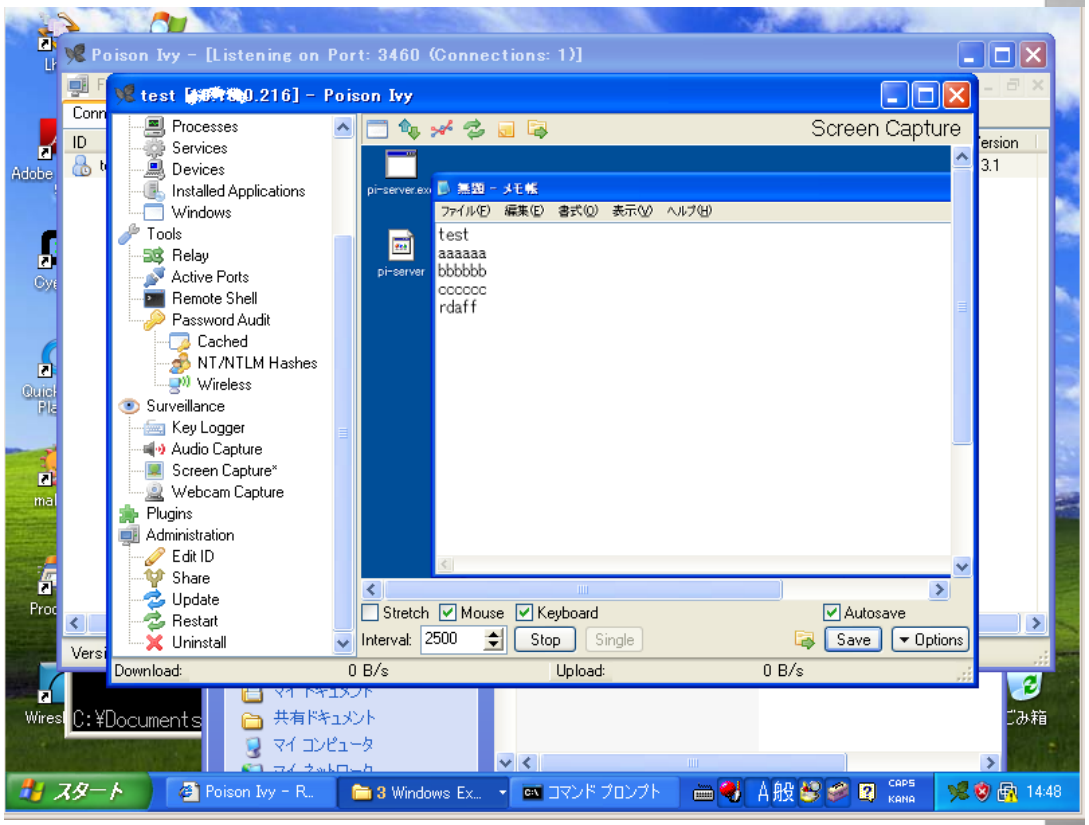
- RAT：Remote Access Trojan horse, Remote Access Tool, Remote Administration Tool等
- BackOrifis(1998),BackOrifis2000(BO2K,1999),NetBus(1998)等と同様に遠隔操作機能を提供する。
- 悪性プログラムである場合と正当なツールの悪用の場合がある。
- 標的型攻撃における悪用 Shady RAT(2011/9)
  - 過去5年間にわたって米国や韓国、インド等の政府機関、国連、大手企業、非営利組織、コンピュータセキュリティ企業、オリンピック関連団体など72の組織にRATプログラムが不正にインストールされていたことが明らかになった。
- 現在では Poison Ivy や Gh0st RATなどの悪用が見られる。

セキュリティ動向2011

RAT(Poison Ivy)

- Poison Ivy はRATの一種であり、現状でも配布用Webサイトからだれでも入手可能。
- 機能としては
  - 画面操作
    - アプリケーションの操作
    - サービスの停止開始
    - マウスやキーボードの操作
    - 任意のファイルのdownload, upload、実行
  - 他の利用者への操作
    - Key logger
    - Webcam(カメラ)による盗撮
    - マイクの盗聴

  などが可能。またプラグインで拡張できる。



Poison Ivy で他のPCの画面を操作している様子

セキュリティ動向2011

標的型攻撃について

標的型攻撃の例

標的型攻撃とは

標的型攻撃への対策

標的型攻撃とは

公開された事例: CSS2008のCFPを騙ったウイルスメール

- 「CSS2008のCFPを騙ったウイルスメール」の対応について
  http://www.iwsec.org/csec/css2008-cfp-secinfo.html
- CFP(論文募集)の内容のウイルス付きPDF添付。学会会員から4件報告。
- From: は学会事務局に詐称、国外のアドレスから送信

Date(Dateから取得)	srcIP(Receivedから取得
Thu, 5 Jun 2008 10:45:24 +0900	210.108.xxx.yy 報告3
Thu, 5 Jun 2008 10:45:51 +0900	210.108.xxx.yy 報告2
Thu, 5 Jun 2008 10:45:57 +0900	210.108.xxx.yy 報告1
Thu, 5 Jun 2008 10:46:16 +0900	210.108.xxx.yy 報告3
Thu, 5 Jun 2008 10:46:46 +0900	210.108.xxx.yy 報告4

- 2008年6月5日 注意喚起
  「CSS2008のCFPを騙ったウィルスメールが
  送付されているとの 情報がはいっております。
  (略)電子メールによるCSS2008のCFP(PDF)
  配布は行っておりません。」
  http://www.iwsec.org/css/2008/attention.html
- ウイルス解析(認証情報を盗む)
- 関係各所への報告等

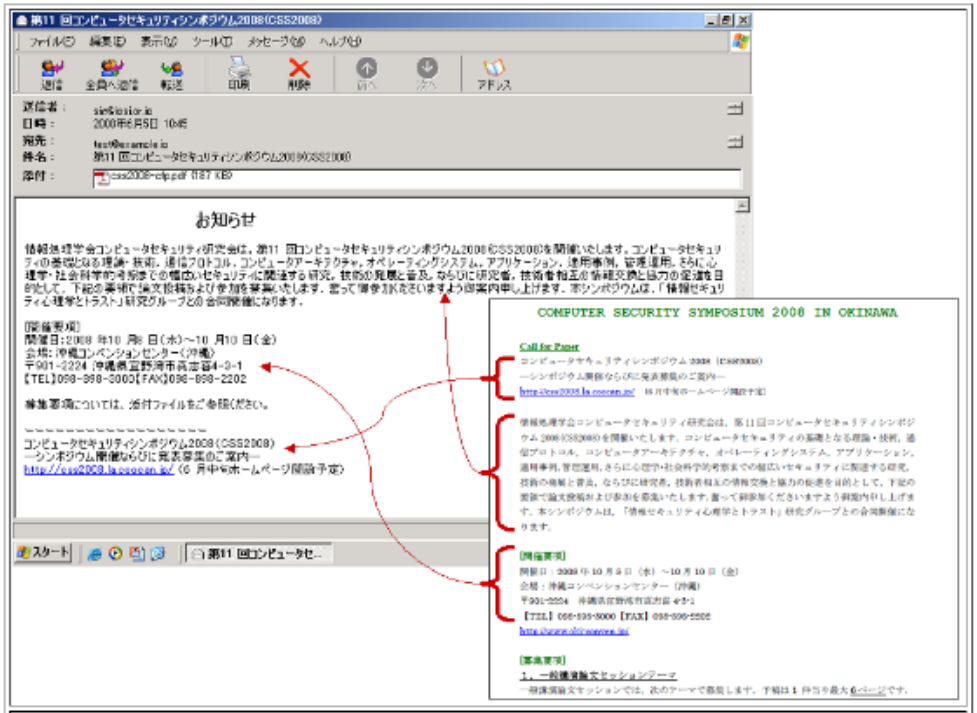


図1: 受信したウイルスメールの画像(スナップショット)
受信したウイルスメールの本文は、CSS2008 CFP (PDF) を切り貼りした文章で構成されていました。

標的型攻撃の例

標的型攻撃：国内事例

2005年10月　実在の外務省職員を詐称したウイルス付きのメールが複数の官公庁に到着

2006年　5月　官公庁を詐称したウイルス付きのメールが複数の大企業に到着

2007年10月　政府関係機関(IPA)を詐称したウイルス付きメールが官公庁に到着

2008年11月　標的型攻撃メールに関する注意喚起に偽装したメールが企業の従業員に到着

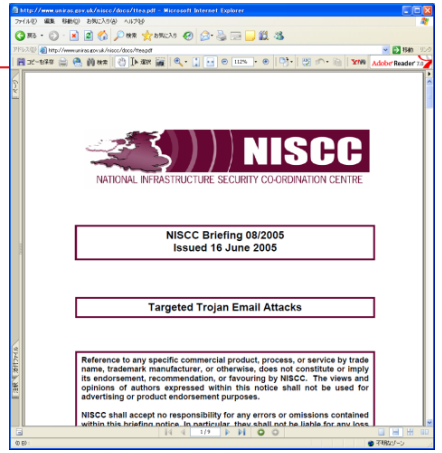
2009年　5月　新型インフルエンザ関連情報に見せかけた標的型攻撃メールが発生

2011年　3月以降　東日本大震災や原発事故関連情報に見せかけた標的型攻撃メールが複数発生

2011年　8月　国内大企業や政府関連組織に対する標的型攻撃が発覚

IPA テクニカルウォッチ：「標的型攻撃メールの分析に関するレポート」より 抜粋
http://www.ipa.go.jp/about/technicalwatch/20111003.html

標的型攻撃:海外事例



http://www.cpni.gov.uk/Docs/ttea.pdf

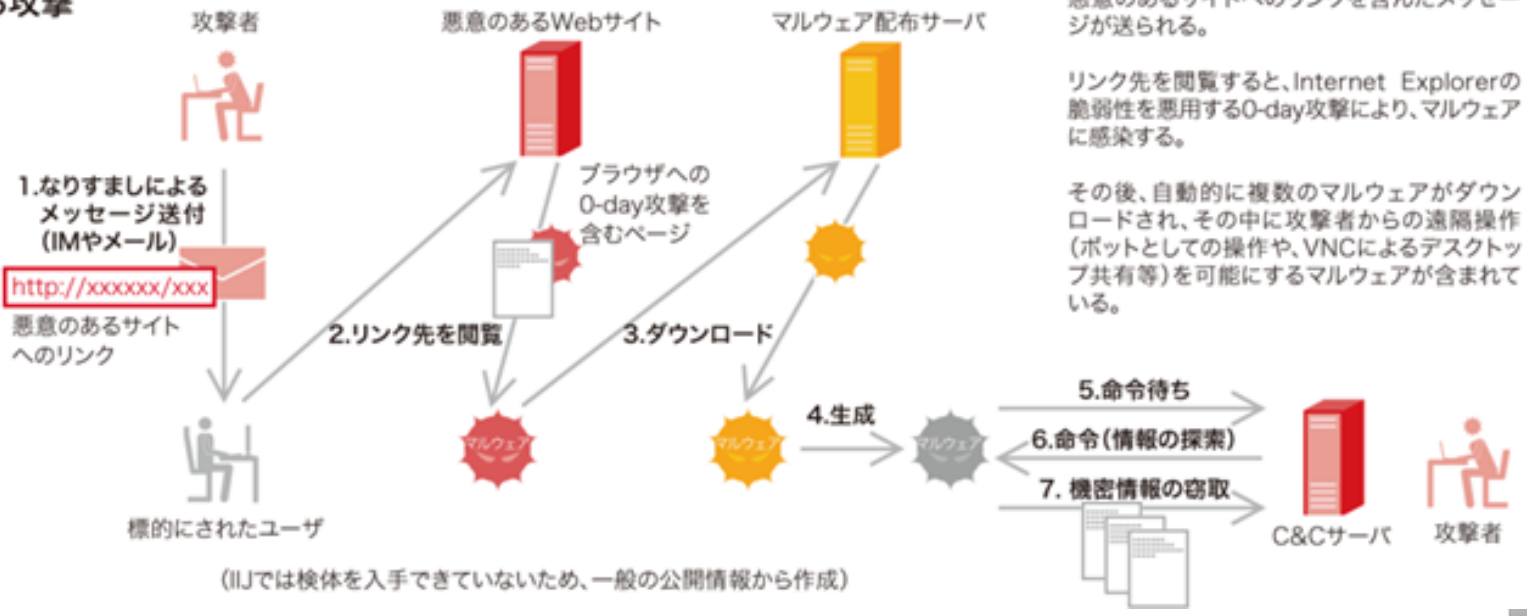
- 複数の国の官公庁関係にウイルス付きメール(2005)

- Night Dragon(2009)
  - 石油、エネルギー、石油化学会社大手5社に対して仕掛けられた攻撃。油田やガス田の運営、入札や資金調達といった機密情報が窃取された可能性が報告された。
- Operation Aurora(2010)
  - Google、Adobe Systems、Symantec、Yahoo!など、IT系60社で知的財産を窃取したとされる。
- 米EMC社でRSA SecurID関連情報の流出(2011年3月)
  - Adobe Flash の脆弱性の攻撃プログラム(メールに添付されたExcelファイルに埋め込み)により、同社製品SecurIDに関する情報が引き出されたことを明らかにした。

標的型攻撃の例

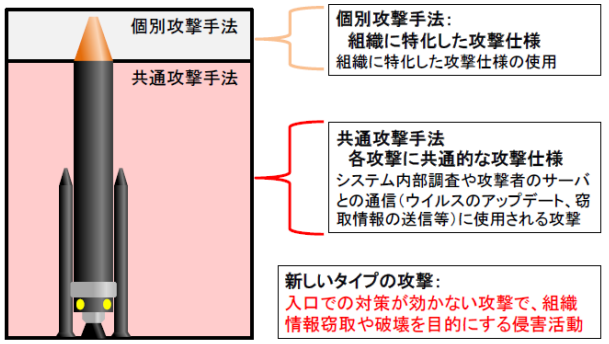
マルウェア：Operation Aurora の場合(IIR Vol. 7より)

▶Operation Auroraにおける攻撃



なぜこのような複雑な構成をとるのか→アンチウイルス避け

- 最初の攻撃プログラムを小さく見つけにくくする
  (ダウンロードの機能のみ)
- マルウェアをエンコード/暗号化してダウンロード
- マルウェアを分割した部分をダウンロード
- ファイルに保存せずメモリ上に展開



IPA「新しいタイプの攻撃」の対策に向けた設計・運用ガイド
http://www.ipa.go.jp/security/vuln/newattack.html

図 2-1:「新しいタイプの攻撃の概念」

標的型攻撃とは

標的型攻撃のリスク

- 送信元を詐称された組織のリスク
  - 情報漏えいやマルウェア感染、攻撃行為を疑われる。
- 受信した組織のリスク
  - マルウェア感染（情報漏えい、外部からの操作等）。
- 受信した組織の関連組織のリスク
  - 標的型攻撃で漏えいした情報を悪用されて攻撃される可能性。

http://www.mofa.go.jp/mofaj/press/oshirase/18/osrs_0120.html　http://www.nih.go.jp/niid/misc/warning090428.html

標的型攻撃とは

手法

- 入り口
  - メール(URL、添付ファイル)、IM、SNS等
- マルウェア感染
  - 設定情報を盗む（メールアドレスなどの漏えい）
  - ネットワーク内の他のPCへの感染（社内への感染）
  - 他のマルウェアのインストール
    - ボット(インターネット側への攻撃)
    - Keylogger (キーボードから入力した情報や画面のスナップショットの漏えい)
    - RAT（自分のPCから標的型攻撃メールを出す可能性）

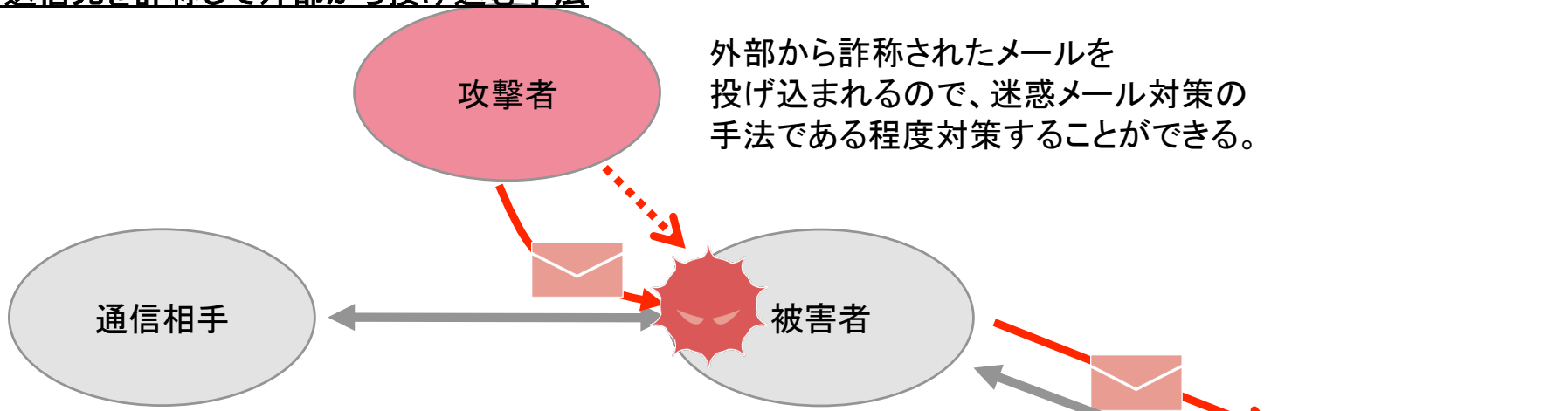
標的型攻撃の2つの類型

- 準標的型攻撃
  - 複数の組織で複数の人物に対して発生
  - 広く万人が興味を持ちそうな話題の悪用
  - 脆弱性やマルウェアの使い回しが見られる
  - 複数の事例が存在
- 真の標的型攻撃
  - 特定の組織の保有する情報を盗み出すことなどが目的
  - 特定の組織の特定の人物に対する攻撃(メールでの会話に割り込む等)
  - 非公開脆弱性や新型のマルウェアの利用
  - 事例は少ない

標的型攻撃とは

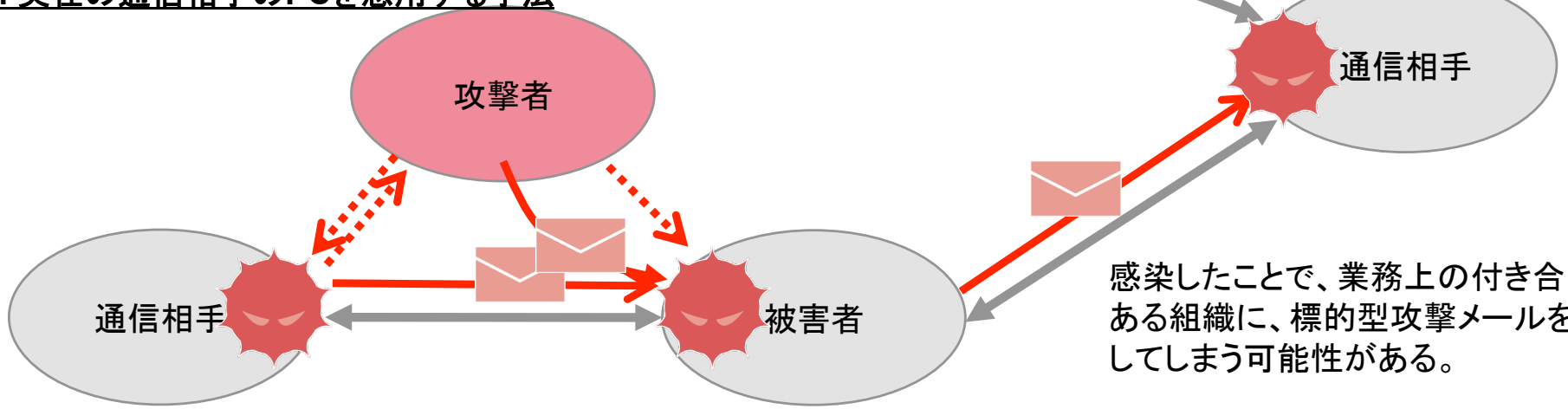
標的型メールの送信手法

1. 送信元を詐称して外部から投げ込む手法



外部から詐称されたメールを
投げ込まれるので、迷惑メール対策の
手法である程度対策することができる。

2. 実在の通信相手のPCを悪用する手法



感染したことで、業務上の付き合いの
ある組織に、標的型攻撃メールを送付
してしまう可能性がある。

実際にメールをやり取りする相手から
送出されるメールなので、判別が困難。

標的型攻撃への対策

対策活動

- 過去の活動
  - IPA　標的型攻撃に関する解析レポート
  - JPCERT/CC インターネット予防注射
  - 内閣官房情報セキュリティセンタ リスク分析モデル
  - IPA「新しいタイプの攻撃」
- 最近の活動(情報共有方法の模索)
  - 経済産業省：民間企業主導のパートナーシップ(官民連携)
    - 日本セキュリティオペレーション事業者協議会 (ISOG-J) WG5
  - 警察庁： サイバーインテリジェンス対策のための不正プログラム対策協議会(官民連携)
  - 内閣官房 ：情報セキュリティ政策会議(10/7) (官民連携)
  - 総務省(10/31)（官民連携）
- ガイドライン
  - IPA「新しいタイプの攻撃」の対策に向けた設計・運用ガイド
    http://www.ipa.go.jp/security/vuln/newattack.html
  - 出口防御の概念紹介

標的型攻撃への対策

出口防御

- マルウェアのアップデートや指令通信を断ち切るために外向けの通信を制御する。
  - マルウェア解析によるサーバの特定
  - インターネット側への通信を監視・制御する技術

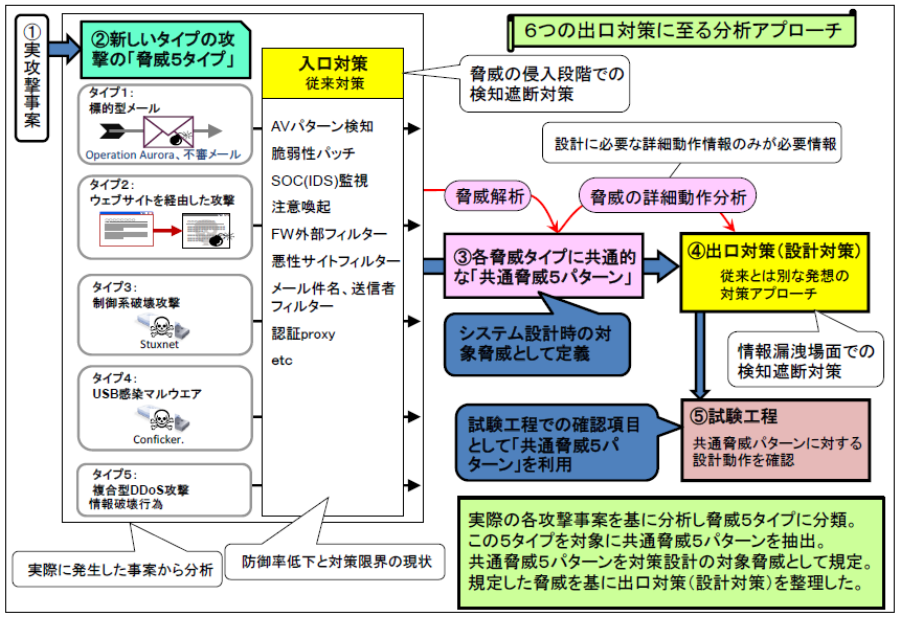


図 4-3-1:「出口対策」策定のアプローチの全体像

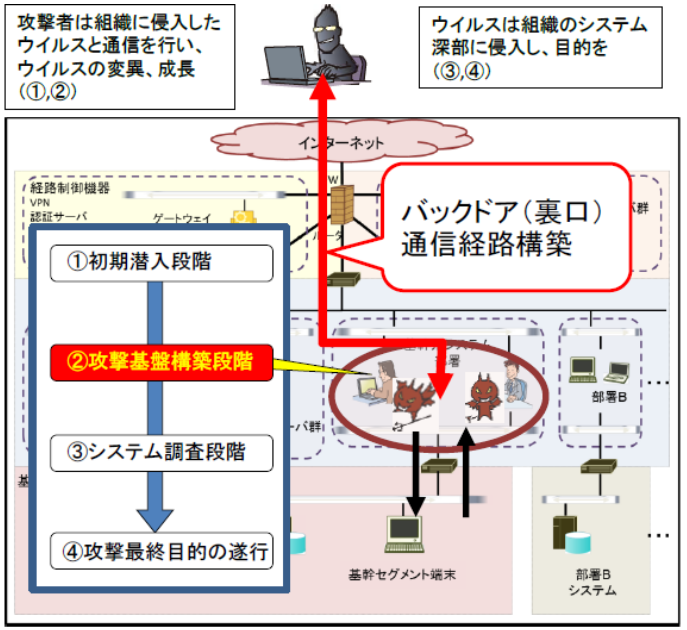


図 3-1-2:検知をすり抜け、素早く次のステップ(攻撃基盤構築)に移行するイメージ

IPA「新しいタイプの攻撃」の対策に向けた設計・運用ガイド
http://www.ipa.go.jp/security/vuln/newattack.html

標的型攻撃への対策

一般の企業における対策

- **入り口防御の強化**
  - 迷惑メイル対策手法の導入
    - DKIM、S/MIME等の電子署名
    - 業務上付き合いのある相手と双方での利用
  - ブラックリストによる送信元のアクセス制御
- **出口防御の実現**
  - ホワイトリスト(信頼できる通信先のみ許可)
  - ブラックリスト(マルウェアの動作に関連するサーバ類への制限)
  - Web Proxyまたはそれに類する機能、ファイアウォールやIPS等
- **教育**
  - 標的型攻撃に関する知識
  - 訓練
- **情報公開(共有)**
  - 関連団体、IPA、JPCERT/CC、警察、経産省パートナーシップ、内閣官房の活動など

まとめ

- セキュリティ動向2011
  - 標的型攻撃
  - Anonymous等のHacktivism
  - DDoS攻撃
  - 内部犯行
  - RAT
- 標的型攻撃について
  - 標的型攻撃の例
  - 標的型攻撃とは
  - 標的型攻撃のへ対策

IIJ Internet Initiative Japan

ご清聴ありがとうございました

お問い合わせ先　IIJインフォメーションセンター
TEL：03-5205-4466（9：30～17：30 土/日/祝日除く）
info@iij.ad.jp
http://www.iij.ad.jp/

Ongoing Innovation