ありがちなインシデントとその対応

龍谷大学理工学部
小島肇

今日のおはなし

- ありがちなインシデントの種類
- 種類別の対応
  - 予防するには
  - 発生してしまったら

インシデントとは?

- 業界用語
- コンピュータセキュリティ屋さんが使う場合は、コンピュータセキュリティインシデントのこと
  - ソフト屋さんが使う場合はちょっと違う意味
- from JPCERT/CC FAQ:
  - コンピュータセキュリティに関係する人為的事象で、意図的および偶発的なもの (その疑いがある場合) を含みます。例えば、リソースの不正使用、サービス妨害行為、データの破壊、意図しない情報の開示や、さらにそれらに至るための行為 (事象) などがあります。

ありがちなインシデント

- コンピュータ・ウィルス感染
  - ファイル・ディスクの破壊
  - バックドア、トロイの木馬の設置
    - DoS / DDoS クライアント
  - 内部 / 外部への伝染
    - 電子メール
    - IM, IRC
    - ネットワーク共有
    - 直接的 IP 接続（TCP, UDP）

ありがちなインシデント

- 能動的攻撃
  - スキャンを受けている
    - port scan, 脆弱性 scan
  - 攻撃を受けている
    - 防衛できている場合は異常な log 出力などが観測
  - 侵入された
    - さらに別の機械を攻撃
    - バックドア、トロイの木馬を仕掛けられた
    - 情報を破壊された、改ざんされた
    - 情報を盗まれた

ありがちなインシデント

- 受動的攻撃
  - 電子メール経由
    - 電子メールを利用したウィルスも受動的攻撃の一種
  - web ページ経由
    - JavaScript(アクティブスクリプト)、ActiveX、plug-in を利用した攻撃
    - 詐欺的手法が多い。例: 認証だと思ったら実は ActiveX コンポーネントがインストールされ、…
  - いきなり内側から攻撃が始まることに注意

ありがちなインシデント

- 情報漏洩
  - アクセス制御を破られた
    - ファイアウォール
    - パスワード
    - パーミッション、ACL 等
  - そもそもアクセス制御がかかっていなかった
    - かけたつもりが…
    - 誰にも知らせていないはずの URL なのに…

ありがちなインシデント

- 著作権侵害、海賊行為
- net abuse（不適切なネットワークの利用）
  - spam
  - なりすまし
  - 誹謗、中傷

ありがちなインシデント

- 物理攻撃
  - テロ、戦争
- 自然災害
  - 台風、地震、洪水、…

インシデント（質的な違い）†

- 内部のみに影響 – 事故レベル
  - Code Red / Nimda / Slammer 級の大規模事故もあるが、…
- 外部にも影響 – 不祥事レベル
  - ウィルスが外部に伝染
  - 外部へ攻撃
  - 外部の掲示板に誹謗、中傷
  - 外部への情報漏えい

† ラック西本氏のうけうり

インシデント（質的な違い）

- 社会インフラに影響 – テロレベル
  - 例: 大手 ISP や Super SINET 基幹がダウンするような事態

各論 – 攻撃系

コンピュータウィルス

- 通商産業省告示 第952号†から:
  第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、次の機能を一つ以上有するもの。
  - (1)自己伝染機能
    - 自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能
  - (2)潜伏機能
    - 発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能
  - (3)発病機能
    - プログラム、データ等のファイルの破壊を行ったり、設計者の意図しない動作をする等の機能

† http://www.ipa.go.jp/security/antivirus/kijun952.html

コンピュータウィルス対策

- アンチウィルスソフトの導入
  - ゲートウェイ（メール、web）
    - 内部への侵入を阻止
    - 外部への伝染を阻止（特にメール）
  - クライアント
  - サーバ
    - ファイルサーバ
    - グループウェアサーバ

コンピュータウィルス対策

- ウィルスデータを常に最新にする
  - 最低でも毎日更新
    - ASP† 型なら手間いらず、ただしお金がかかる
  - 最新データによる問題発生もあり得るので注意が必要。誤認識、動作異常など
- 複数ベンダーのアンチウィルスソフトの利用が望ましい
  - 対応状況・対応速度に違い
  - ゲートウェイ・クライアント・サーバでベンダーを変える
    - 欠点: 手間とお金がかかる

† Application Service Provider

コンピュータウィルス対策

- アンチウィルスソフトだけで予防しきれる?
  - 絶対無理
    - ウィルスは誰にでも簡単に作成できる
  - メモリ上にのみ存在するウィルスを発見できないことがある。例: Code Red, Slammer
  - トロイの木馬やバックドア、スパイウェア、アドウェア、怪しい「商用ソフト」「フリーソフト」を検出しないことがある
    - 検出ソフト:
      Ad-aware http://www.lavasoft.nu/
      Spybot http://spybot.safer-networking.de/
      PestPatrol http://www.pestpatrol.jp/

コンピュータウィルス対策

- （続）
  - アンチウィルスソフトのデフォルト設定が甘い
    - 拡張子を限定したチェックしか行わない
    - アーカイブファイルの中身がチェックされない
  - セキュリティホールを利用したウィルスの登場
    - メールをプレビューしただけで感染
    - セキュリティホールはきちんとふさぐ
      - 利用されやすいソフト（IE, OE）のセキュリティホールは特に
- 利用者自身による注意が常に必要

コンピュータウィルス対策

- 怪しい兆候
  - コンピュータの動作がおかしい、遅い、止まる、起動できない
  - 妙なプロセスが動いている
  - 異常なネットワーク接続を行っている
    - 例: 大量の接続要求、プロトコル違反の接続
  - ファイルがなくなる、知らないファイルが増えている

コンピュータウィルス対策

- 怪しい兆候があるときは…
  - とりあえず、最新のウィルスデータを利用して全ファイルのウィルスチェック
  - OS が変なだけかも
  - 兆候がなくても最低週 1 回程度は実施したい

能動的攻撃

- どこが狙われる?
  - 公開しているサービス
    - mail, WWW, DNS, …
  - 公開していないはずのサービス
    - いつのまにか起動していた
    - ユーザが勝手に立ち上げた
    - 侵入者が立ち上げた
    - ファイアウォールなどの設定不備で、見えないはずのものが見えた

能動的攻撃

- 攻撃手口
  - まずい設定を突く
    - 弱いパスワード
    - 誰でも読み書きできるファイル、ディレクトリ
  - セキュリティホールを突く
    - 修正 patch はすでにあったが適用していなかった
    - 脆弱性が明らかだったがベンダーが修正 patch を用意していなかった
    - 未知の脆弱性だった
  - 合わせ技
    - 小さな穴でも、組み合わせることで大きな結果が

能動的攻撃

- 攻撃手順
  - 調査
    - port scan, 脆弱性 scan
  - 攻撃
    - 橋頭堡の確保 – 一番弱いものを攻略
    - 証拠の隠滅
    - 裏口の設置
  - さらに…
    - 内部に侵入
    - 外部を攻撃

能動的攻撃(抑止)

- ファイアウォールで公開範囲を制限する
  - ホスト
    - 例: 外部からは、特定の内部計算機にしか接続できない。内部からは、特定の計算機からは外部と接続できるが、他の大多数はやはり接続できない。
  - サービス(ポート)
    - 例: DNS と web (http) と mail だけ
  - ICMP
    - 例: ICMP echo は通すが、ICMP redirect は通さない

能動的攻撃（抑止）

- 起動する（サーバ）サービスを制限する
  - 使わないなら起動しない
  - 起動させる場合でも、ファイアウォールや OS のパケットフィルタ等により接続元・接続先を可能な限り制限
  - 不要なオプション機能は抑止する
    - Microsoft IIS ではデフォルトで使いもしない機能てんこもり
    - Apache でも、OS 付属のパッケージは全機能が有効になっていることが多い

能動的攻撃（抑止）

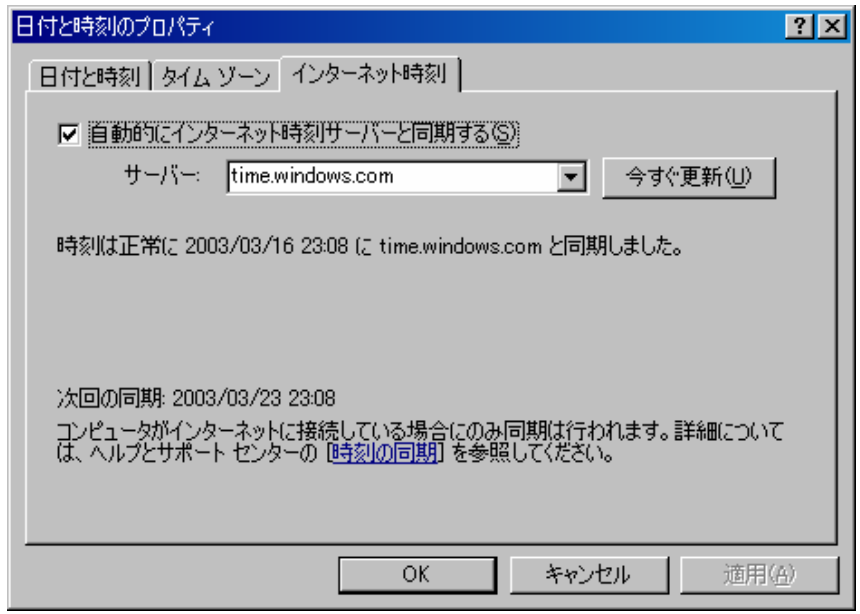
- ログを取る
  - ログから攻撃の兆候を察知できる場合がある
  - 各所で取る
    - ホスト、ファイアウォール、プロキシサーバ、…
    - Windows NT/2000 では、デフォルトで監査が無効
      - Windows Server 2003 ではちょっとだけ改善

能動的攻撃(抑止)

- ログサーバに転送する
  - UNIX やルータ、スイッチなどのネットワーク機器では syslog の利用が一般的
    - RFC3164: The BSD Syslog Protocol. http://www.ietf.org/rfc/rfc3164.txt
    - RFC3195: Reliable Delivery for syslog. http://www.ietf.org/rfc/rfc3195.txt
  - Windows は標準では syslog 対応ではない
    - WinSyslog http://adiscon.port139.co.jp/

能動的攻撃（抑止）

- 時間を合わせる
  - NTP（Network Time Protocol）の利用が一般的
    - Windows 2000 以降には SNTP 機能が付属
    - Windows 対応のフリーな NTP ソフト多数あり
    - Windows XP では「日付と時刻」コントロールパネルで NTP サーバを設定可能



能動的攻撃（抑止）

- 設定をより強固にする
  - 長くて推測しにくいパスワード
  - よりセキュアなプロトコルの選択
    - 認証: LM < NTLM < NTLMv2 < Kerberos
  - 不要なサービス・機能の停止
  - サービス動作権限の縮小
  - etc, etc…

能動的攻撃（抑止）

- 書籍
  - クラッキング防衛大全
    - 第3版 http://www.shoeisha.com/book/Detail.asp?bid=1407
    - Linux編 http://www.shoeisha.com/book/Detail.asp?bid=1428
    - Windows 2000編 http://www.shoeisha.com/book/Detail.asp?bid=1487
  - UNIX & インターネットセキュリティ
    http://www.oreilly.co.jp/BOOK/puis/
  - ファイアウォール構築 第2版
    http://www.oreilly.co.jp/BOOK/firewall2v1/
- web
  - Microsoft　セキュリティ：ツールとチェックリスト
    http://www.microsoft.com/japan/technet/security/tools/tools.asp
  - port139: NT セキュリティ
    http://www.port139.co.jp/ntsec.htm
  - IPA: セキュアなWebサーバーの構築と運用
    http://www.ipa.go.jp/security/awareness/administrator/secure-web/index.html

能動的攻撃(抑止)

- 最新のセキュリティ修正プログラム(patch)を適用する
  - 最新のセキュリティ修正プログラム情報を入手する
    - ベンダーの web, mail はこまめにチェック
  - 事前テストは必要、mission critical なシステムでは特に
    - patch による不具合発生の可能性
  - Windows Update に代表される(半)自動インストールシステムは便利だが…
    - 間違った / 古いプログラムが登録されていることも

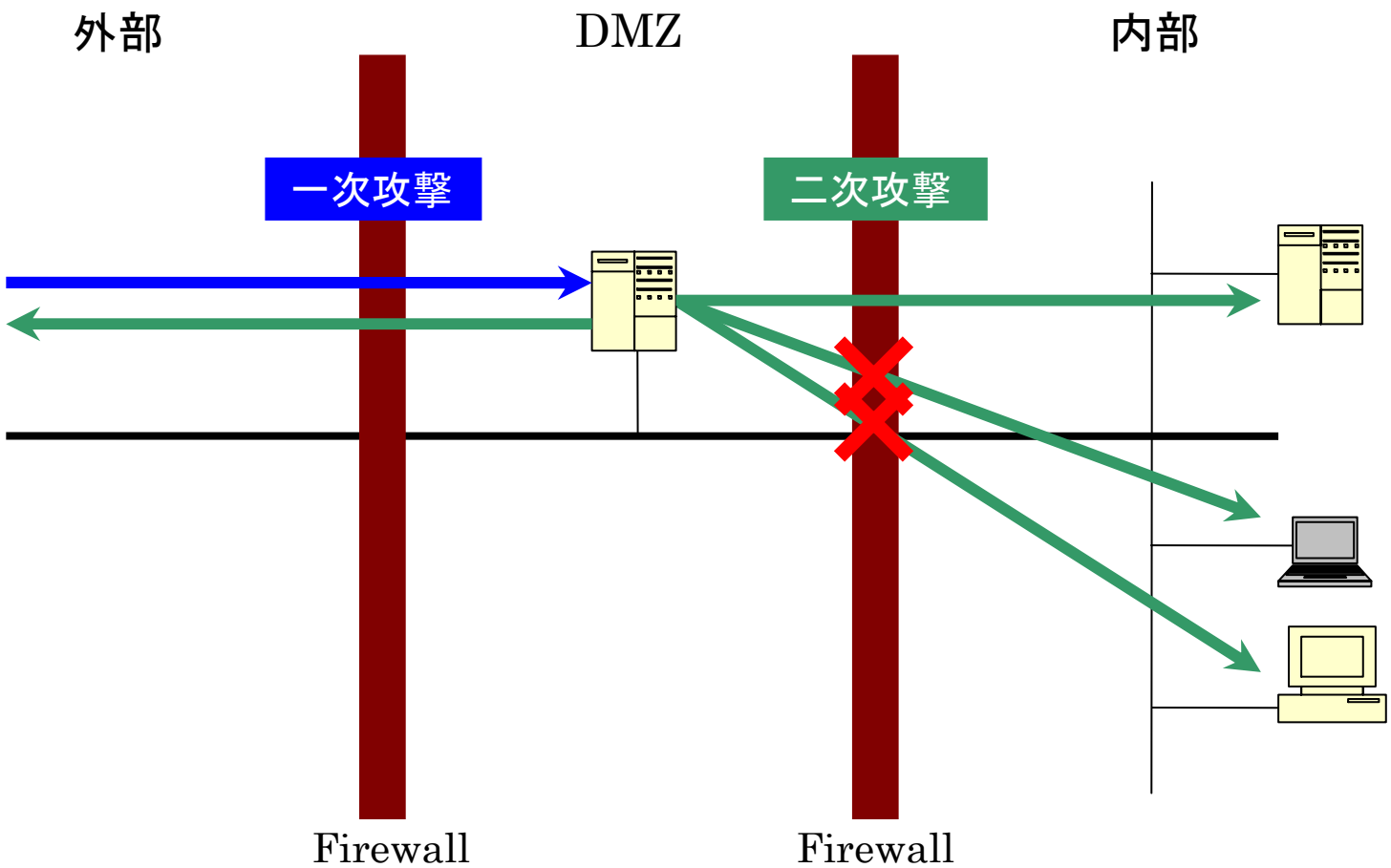
能動的攻撃（抑止）

- 最新のセキュリティ情報を入手する
  - 製品ベンダー
  - 中立組織（JPCERT/CC, IPA, CERT/CC, …）
  - （マス）メディア
  - セキュリティ関連メーリングリスト、web ページ
- 情報の中には、ガセや間違いもあるので注意
  - 製品ベンダーすら間違えることも

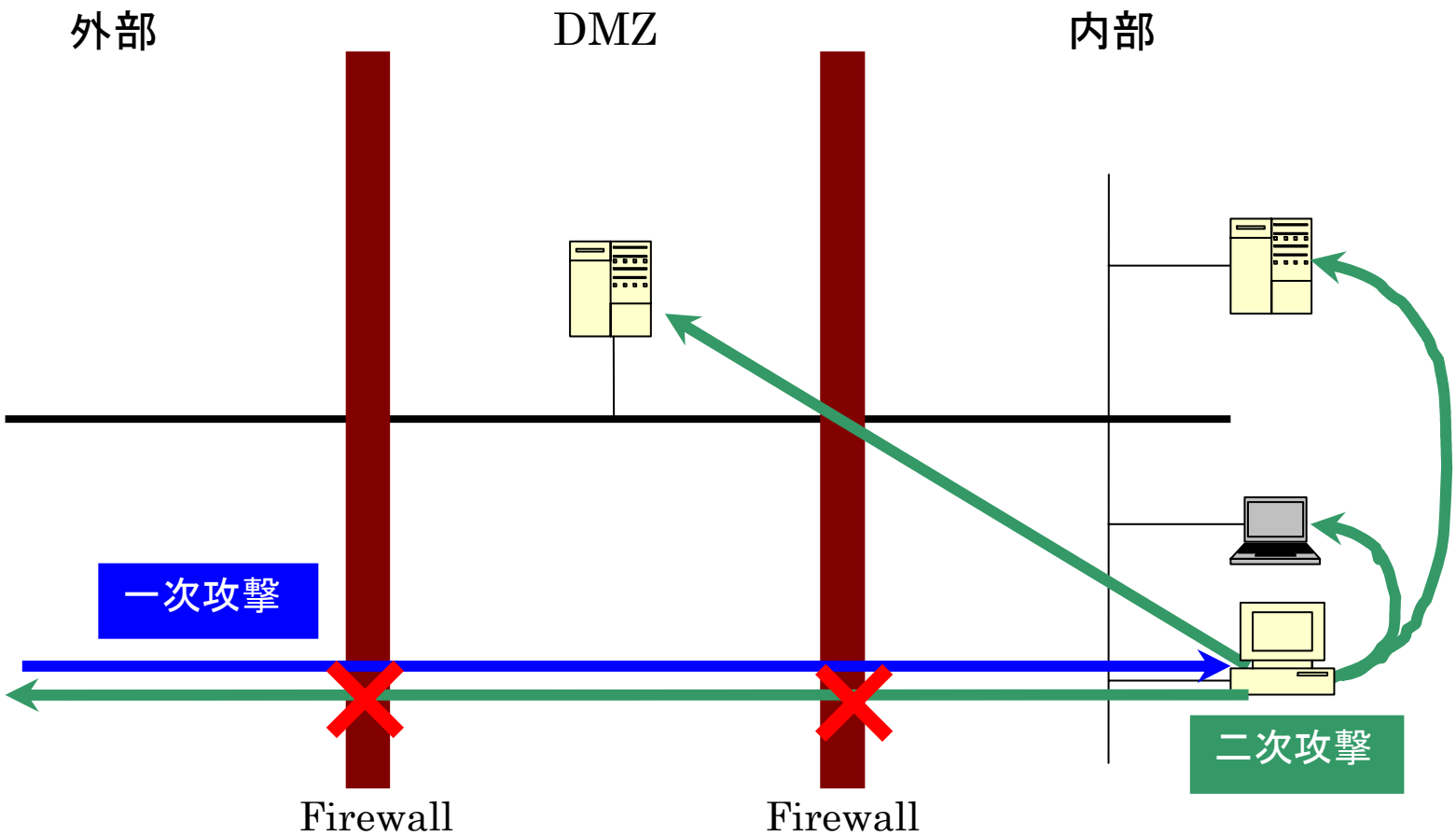
受動的攻撃

- mail や web、データファイルを仲介して攻撃
  - 添付ファイル
    - 2 重拡張子（.txt.exe）などを利用したごまかし
      - 拡張子は常に表示するように Exploler を設定
    - セキュリティホールを利用して自動実行
  - HTML ファイル（メール）内のスクリプト、ActiveX
  - データファイル
    - Microsoft Office 文書（マクロ言語を利用した攻撃）
    - Acrobat （.pdf）の Javascript
- いきなり内側から攻撃を開始
  - ファイアウォールが役に立たない

能動的攻撃



受動的攻撃



受動的攻撃（抑止）

- ウィルス対策をきちんと実行
  - 受動的攻撃の多くはウィルスの攻撃手法と酷似
  - ゲートウェイ（mail, web）での対策は有効
- web ブラウザ、メールソフト（メールクライアント）のセキュリティ対策
  - セキュリティホールをふさぐ
  - 安全な設定（= 利便性は低下）
    - インターネットゾーンではアクティブスクリプト、ActiveX は停止
    - 安全だと判断したサイトを明示的に信頼済みサイトゾーンに追加
  - いざという時のための代替プログラムを検討する
    - メールソフトは困難か?

受動的攻撃（抑止）

- ゾーニングをしっかり行う
  - 内部も複数区画に分割
  - 攻撃されても被害を最小限に抑える
  - ファイアウォールの考え方と同じ
- パーソナルファイアウォールの導入
  - 1 次攻撃はもちろん、2 次攻撃も防ぐ
  - またまたコストが…
  - 突破方法あり

IDS – 侵入検出システム

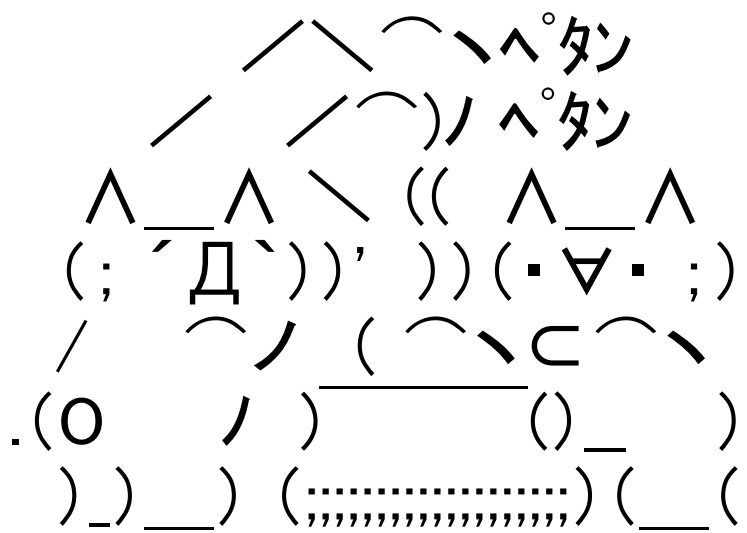
- 監視カメラ、のようなもの
  - ネットワークベース
    - 通信内容から検出
    - 境界地点での実行が効果的
  - ホストベース
    - Personal Firewall とホストベース IDS との違いは?
- 維持が大変
  - 無用なルールの削除
    - 無用なルールとは? 本当に削除してしまっていいの?
  - 新たなルールの追加
    - 攻撃手法が登場してからルールが追加されるまでの時差?

IDS – 侵入検出システム

- 完全ではない
  - 未知の攻撃手法による攻撃は発見できない場合がある（特にネットワーク型 IDS）
- 関連ソフト
  - プロトコルアナライザー
    - Sniffer, tcpdump, Ethereal, …
  - トラフィックロガー
    - iplog, monyolog, syunlog
    - tcpflow

やられてしまったら

- 冷静になろう
  - もちつけ!



やられてしまったら – 状況の把握

- （被害）状況の把握
  - ネットワーク接続・利用状況
  - プロセス動作状況
  - ファイル状況（ファイル正当性検査）
    - すべてのファイルは改変されている可能性ありとして調査
  - rootkit やトロイの木馬、バックドアに注意
    - login したらドカン…
    - reboot したらドカン…
  - 「正常な状態」の把握が重要
    - 常日頃の監視・観測がものを言う

やられてしまったら – 状況の把握

- （被害）状況の把握（続）
  - ログ調査
    - ホストのログ（OS, アプリ）
    - ファイアウォールのログ
    - プロキシサーバのログ
  - ホストのログは改変されているかもしれない
    - 事前に、安全な場所（ログサーバ）へ（も）ログを配送するようにしておくのがよい
    - UNIX では標準機能の syslog を用いて簡単に設定可能
    - Windows ではフリーソフトやリソースキット、市販ソフトを活用

やられてしまったら – 2 次攻撃

- 重大な 2 次攻撃・ウィルス伝染が発生していることが明白なら
  - まずは該当ホストからのアクセスを止める
    - ファイアウォールでふさぐ、線を抜く
  - 関係方面に通報
    - 誰に報告すべきかは、2 次攻撃の内容（内部 / 外部、規模、…）によって異なるはず
  - 連絡体制・対応手順をあらかじめ決めておく
    - 決まっていないと大変、特に外部攻撃・伝染（不祥事レベル）の場合
    - 緊急対応チームの事前結成・訓練が望ましい

やられてしまったら – ウィルス感染

- ウィルスに感染していることが（ほぼ）明らかな場合
  - ネットワークから分離（既にネットワーク経由で伝染活動をしている場合）
  - アンチウィルスソフトによる隔離・駆除
  - 怪しいファイルをアンチウィルスベンダーに送付（未知のウィルスの場合）

やられてしまったら – 攻撃を受けている

- 怪しいアクセス元に問い合わせたい場合
  - 直接コンタクト
  - JPCERT/CC などの CSIRT を経由する（お勧め）
  - 技術メモ - 関係サイトとの情報交換
    http://www.jpcert.or.jp/ed/2002/ed020001.txt
  - whois については geektools whois proxy や SamSpade.org Tools を使うと便利
    http://www.geektools.com/cgi-bin/proxy.cgi
    http://www.samspade.org/t/

やられてしまったら – 復旧

- リストア
  - OS、アプリ、データ
  - バックアップから? 新規インストール?
  - バックアップはきちんと取れている? バックアップが壊れている・汚染されている可能性は?
  - リストアにかかる時間は?
- 脆弱点をきちんとふさぐ
  - 再インストール・最新 patch 適用 + データのみリストア、のほうが早い場合が多い
  - 原因調査がきちんとできていないと再発する恐れ

やられてしまったら – 告知

- 状況の把握・復旧と平行して行う
- 外部に影響が出ている場合には特に重要
  - 外部にウィルスが伝染…
  - 外部に情報漏洩…
- 事前に告知方法・手順を確認しておく
  - インシデントが発生してからでは遅い
  - 一例
    - 被害者に対して: (電子)メール、電話
    - 一般に対して: web、記者会見((マス)メディア)
    - (マス)メディアは情報を歪めて伝達する傾向があるので、web などで、自身による情報発信も行う
  - 誰(どの部署)がどのような判断で行うのか?

やられてしまったら – 外部の声

- 外部からインシデント通知がやってきた
  - まず調査
  - 本当だったら
    - 礼を言う
    - 対応状況を随時通知
  - 「黙っててやるから金よこせ」
    - 所属長・顧問弁護士・警察に相談
    - ハイテク犯罪相談窓口一覧
      http://www.npa.go.jp/hightech/soudan/hitech-sodan.htm

やられてしまったら – 参考文献

- 書籍
  - インシデントレスポンス（翔泳社）
    http://www.shoeisha.com/book/Detail.asp?bid=1406
  - 不正アクセス調査ガイド - rootkitの検出とTCTの使い方（オライリー・ジャパン）
    http://www.oreilly.co.jp/BOOK/backdoor/index.htm
- JPCERT/CC 参考文書（技術メモ）
  http://www.jpcert.or.jp/ed/

各論 – 非直接攻撃系

情報漏洩

- 原因
  - アクセス制御を破られた
    - 設定ミス
    - プログラムミス（セキュリティホール）
  - そもそもアクセス制御がかかっていなかった
    - デフォルト値の問題
    - 設定ミス
    - プログラムミス（セキュリティホール）
  - 内部者が漏洩させた
    - 意図的に
    - 脅されて
  - ネットワーク盗聴
  - キーロガー（キー入力記録ソフト）

情報漏洩

- 経路
  - ネットワーク（インターネット等）
    - WWW（web ページ、ネットワークディスク（WebDAV））
    - メール
    - ftp, IRC, IM, …
    - 無線 LAN、有線 LAN
    - 偽装技術（ステガノグラフィ、情報隠蔽）
  - 足（スニーカー、革靴、…）
    - フロッピー、MO
    - CD-R(W)、DVD±R(W)、DVD-RAM
    - フラッシュメモリ（USB 接続型など）
    - ノート PC、パームトップデバイス

情報漏洩 – 抑止

- 技術的対応
  - スイッチング HUB の利用
    - ARP 詐称による対抗
    - ミラーポート機能など HUB 自身の機能を利用して対抗
    - スイッチング HUB 自身のセキュリティが重要
  - ゲリラ無線 LAN の禁止、128bit WEP + 定期的なキー変更
  - 無差別モード（promiscuous mode）になっているネットワーク機器を検知する: PromiScan http://www.securityfriday.com/ToolDownload/PromiScan/promiscan_doc.html
  - 暗号利用の推奨（SSH, SSL, IPsec）

情報漏洩 – 抑止

- セキュリティポリシー
  - 技術的対応には限界が
- 厳しく事前チェック
  - 自分たちで
  - 外部の目（セキュリティ監査サービス）
- 教育
  - 開発者、管理者、利用者

情報漏洩 – 対応

- 「やられてしまったら」とあまり変わらない?
- 一旦外部に流出したら、回収するのはまず不可能であることを認識しておく

著作権侵害、海賊行為

- 著作権侵害
  - 「引用」を超える不適切な情報利用
  - Copyright を削り取って自分が作ったかのように
- 海賊行為
  - コンピュータソフトウェア
  - 音楽
  - 映画
  - 絵画
  - 文章、論文

著作権侵害 – 抑止

- 教育（学生、教職員）
- セキュリティポリシー
- 特定のアレなプログラム・プロトコルは禁止する
- 必要なものはちゃんと買う
- 相互利用を促進する利用許諾がなされたものの活用
  - 修正 BSD ライセンス（BSD UNIX など）
    http://e-words.jp/w/BSDE383A9E382A4E382BBE383B3E382B9.html
  - GNU GPL（GNU Project）
    http://www.gnu.org
  - Creative Commons（レッシグ教授など）
    http://www.hyuki.com/trans/cc-licenses.html
  - 自由利用マーク（文化庁）
    http://www.bunka.go.jp/jiyuriyo/

著作権侵害 – 対応

- プロバイダー責任法に基づいた指摘への対応
  - 「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」
  - テレサ協†ガイドラインに基づく対応 http://www.telesa.or.jp/019kyougikai/html/01provider/index_provider.html
- その他
  - case by case だが、誠実な対応を心がける

† 社団法人テレコムサービス協会 http://www.telesa.or.jp/

net abuse（不適切なネットワークの利用）

- spam
  - spam を発信してしまった
  - spam を中継してしまった
  - spam の From: に自組織ドメインを使われてしまった
- なりすまし
  - From: 詐称メール
- 名誉毀損、プライバシー侵害
  - メールや web ページ、web 掲示板

spam – 抑止・対応

- 発信
  - 教育、セキュリティポリシー
- 中継
  - メールサーバで「予期しない中継」が行われないように設定する
    http://www.jpcert.or.jp/ed/2001/ed010001.txt
- envelope from に自組織ドメイン
  - エラーメールがたくさんやってくる
  - わかってない人からの抗議がごくまれに
  - イメージ失墜?
  - 打つ手なし?

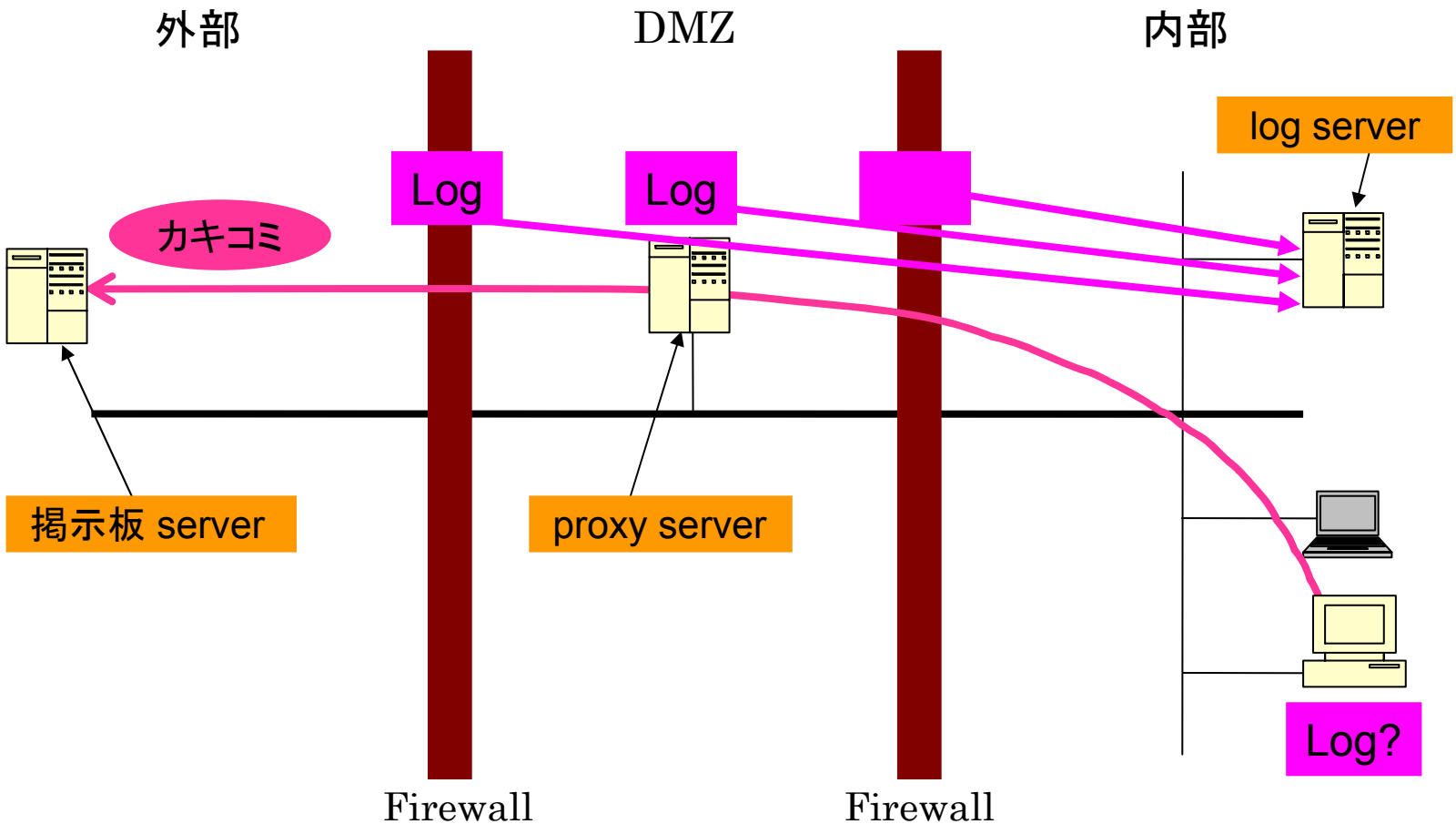
なりすまし – 抑止・対応

- 教育（学生、教職員）
- セキュリティポリシー
- PKI（公開鍵インフラ）を利用した認証?
  - お金と手間がかかる
  - 相手（メール受信者）が対応していない（鶏卵問題）

名誉毀損、プライバシー侵害 – 抑止・対応

- 抑止
  - 教育（学生、教職員）
  - セキュリティポリシー
    - 可能な限りの log を取っておく
    - 最低 3 か月
- 対応
  - log で事実を確認する
    - 末端での確認が困難である場合が多々ある
  - プロバイダー責任法に基づいた指摘への対応
    - 名誉毀損・プライバシー侵害は判断が難しい

log の話


外部
DMZ
内部
log server
Log
Log
カキコミ
掲示板 server
proxy server
Log?
Firewall
Firewall

物理攻撃、自然災害 – 抑止・対応

- 抑止
  - 鍵管理
  - 危険物管理
- 抑止・対応
  - 教育・訓練（学生、教職員）
  - セキュリティポリシー

Appendix

セキュリティ情報の入手などについて

- セキュリティ情報の入手などについては、Developers Summit 2003 の発表資料「Windows は危険? Linux なら安全?～安全性に関する真実と現実的なつきあい方」を参照してください
  http://www.shoeisha.com/event/dev/session/session.html