半径 50m の日常（Forensic 風味?）

龍谷大学理工学部　小島 肇
kjm@rins.ryukoku.ac.jp

今日のお話

- セキュリティホール memo に関するいくばくかのことがら
- 龍谷大学におけるインシデント事例
  - それらのインシデントに Forensic は適用可能なのか?（Forensic を適用すると幸せになれるのだろうか?）

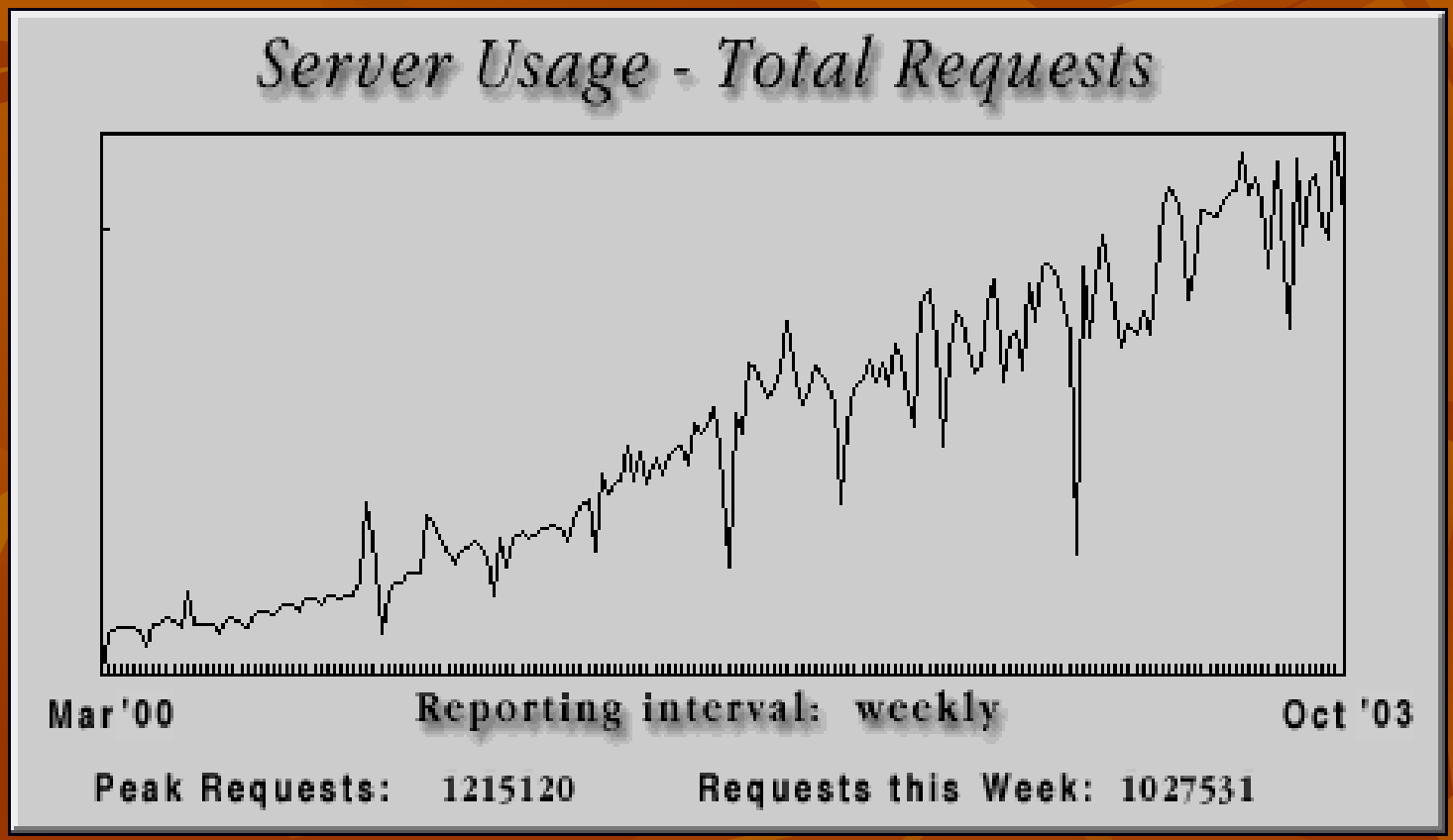
セキュリティホール memo に関するいくばくかのことがら

簡単な歴史

- 1998.10 Security Watch 閉鎖
  - 「*98/10/26* さよなら、**Security Watch**」（やじうま **Watch**）
    http://internet.watch.impress.co.jp/www/yajiuma/backno/9810/5.htm
- 1998.10.28 セキュリティホール memo 開始
  - 非公開（書けるかどうか不安だったので）
- 1998.11.24 FWD fw-wizard ML でアナウンス
- 以後だらだらと…

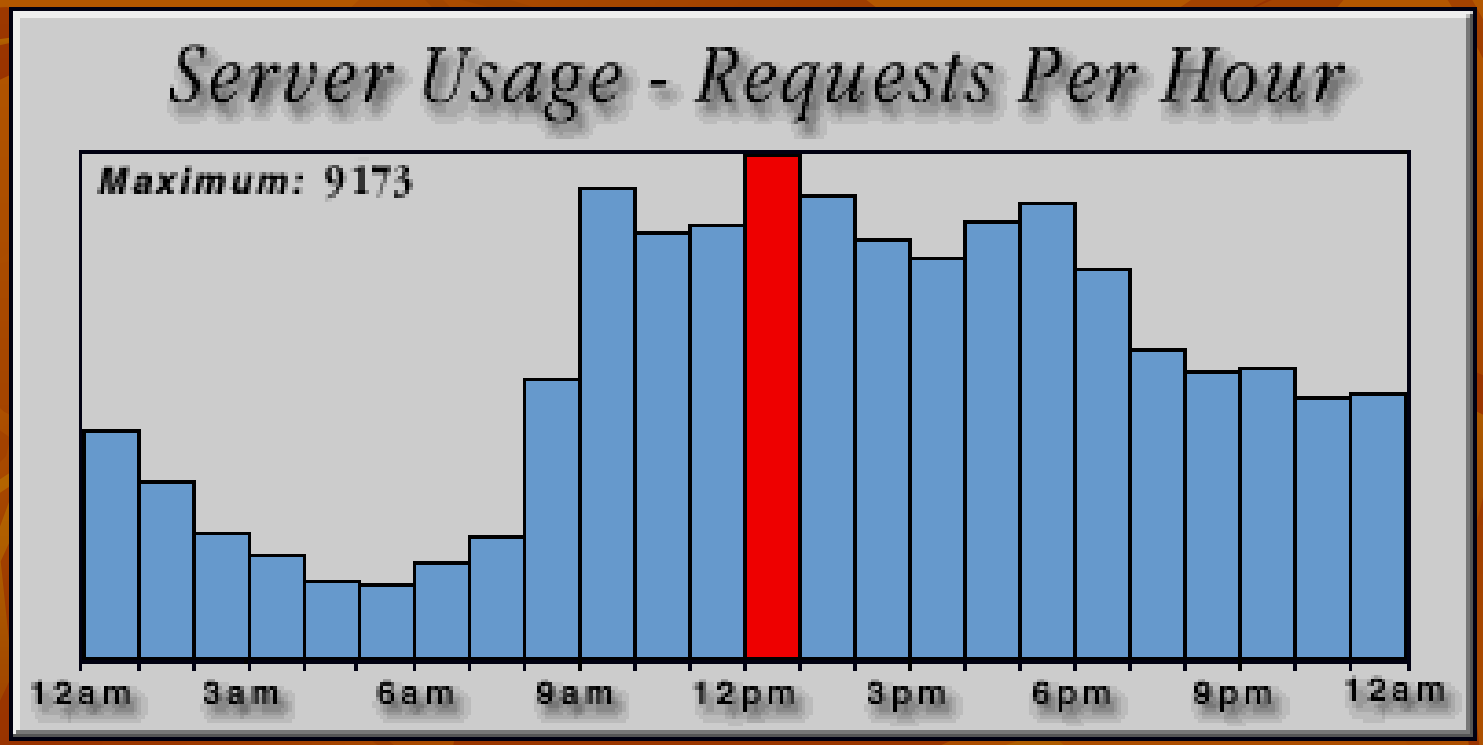
アクセス数とか

- アクセス数の推移: 左端が 2000.03



アクセス数とか

- 朝イチとお昼と帰りがけに見ている人が多い



アクセス数とか

- 20,000～22,000 PV/day くらい
  - しょせんその程度、ぜんぜんすごくないです
  - ロボットさんとかもたくさんいらっしゃるでしょうし
- リンク元
  - 調べてないから知らない

課題 – Blog ツール化

- 生 HTML で書くのに限界を感じる
- 現状は 1 ページが大きすぎ: 携帯端末などで見るのがつらい
- RSS にも対応したい
- コメント機能は無効に
  - 維持できない
  - admin 日記にはつけてもいいかも
- 懸案事項
  - マシンパワーが足りない: 次年度予算でなんとかしたい
  - grep とかできるのかなあ…

課題 - まだ続ける必要があるの?

- はじめた当時とは状況が全く違う
  - Microsoft はすごくまともになった（すばらしい）
  - Sun ですら (!!) 日本語での情報提供を開始
  - 商用サービスもいくつもある
  - 多くが CVE (cve.mitre.org) に対応
  - JPCERT/CC、IPA、@police、…
  - 他の良質な web ページの出現
    例: ヽRノ日記
- そろそろ老兵は消え去るべきかも
  - あるいは新たな展開を考える時期かも

続ける理由

- 勉強強制ギブス
  - 読まないと書けない
  - 理解した(つもり)にならないと書けない
  - 「自分自身のために」(銃夢)
- それなりに役に立っているらしい
- しかし、少しは負荷を減らさないとやばい
  - おうち方面
  - 体力方面: 闘わなきゃ、現実と

JOJOの奇妙なスタンド占い

- あなたのスタンドは「エコーズ」です。

  能力　　：音を貼り付ける。貼り付けた音を現実化する。物質の重量を増加させる。
  幸運の象徴：音楽
  不幸の象徴：海外旅行

  総合運：スゴイ
  恋愛運：超スゴイ
  金銭運：人間並み
  健康運：超スゴイ

  総評：ものすごい勢いで成長が行われる運勢です。新しい物事に手を出せば、最初は大した才能も見られないにもかかわらず、すぐにめきめきと頭角を現すことでしょう。ただし、それも地元での話。遠くの場所、たとえば海外旅行などに行った場合、その運気は低下し、たとえば盗難にあったりします。
  また、今まで縁の無かった女性に思いを寄せられるなど、良い出来事があるでしょう。ただし、悪い人に好かれる弊害もあるので、十分に注意が必要です。

  ラッキーワード：「SHIT」

龍谷大学における
インシデント事例

および:

それらのインシデントに Forensic は適用可能なのか? (Forensic を適用すると幸せになれるのだろうか?)

インシデント事例: 概要

- いわゆる侵入もの
- ウィルス感染事例: CodeRed.F
- 掲示板への不適切な書き込み
- プライバシー情報の流出
- 意図しない DoS 攻撃

Forensic

- @police セキュリティ解説「コンピュータ・フォレンジックス」より:
  - 「計算機科学などを利用して、デジタルの世界の証拠性(evidence)を確保し、法的問題の解決を図る手段。ログの改ざん、破壊等、これまでの手法で は証拠を検出することが困難な被害を受けたコンピュータに対しても、高度なツールによってコンピュータ内のデータを調査・分析することにより、不正アクセ スの追跡を行う手段を含む」 http://www.cyberpolice.go.jp/column/explanation03.html
- Conputer Forensic
  - 本稿では、コンピュータ本体を対象とした調査分析行為を Computer Forensic としています。
- Network Forensic
  - 本稿では、通信内容を長期に渡って取得・保存し、必要に応じて再生・分析する行為を Network Forensic としています。

事例: いわゆる侵入もの

- 内部から内部
- 教育系システムのパスワードファイルに対する辞書攻撃→成功
  - 誰でも読めるような場所に置かれていたものがあった（泣）
- そのパスワードを使って、教育系システムからいろいろなホストにログイン
- とあるホストのログから発見
  - 変な時刻でのログイン

現実の対応

- 侵入者(学生)のホームディレクトリから Crack 5 を発見
- 侵入されたアカウントの所有者(教員)に警告
- 似たような事例がないかどうかを調査
  - Crack していたのは他にも 2 人いた
  - パスワードを Crack しただけで終っていたようだ(ログから判断)
- 侵入者と Crack していた者(学生)から事情聴取
  - 興味本位の厨のように見える
- ファイルの改変・削除などはなかったと判断
  - 侵入されたアカウントの所有者は何も言わなかった

Forensic は有効か?

- 多分有効
  - Computer Forensic: 教育用 WS / ファイルサーバ、接続先の WS。
  - Network Forensic:教育用システムからどこに接続し、どのようなコマンドを実行したのかがわかる
- 問題
  - 教育用ファイルサーバはシャレにならない容量
  - 通信を暗号化された場合、Network Forensic は威力が半減
  - ポリシー問題（後述）

事例: CodeRed.F 感染

- 外部から内部
- 脆弱なまま放置されていた IIS が攻略された
- 転移した CodeRed.F が内部の web サーバを攻撃開始
- CodeRed.F に攻撃された apache のログから発見

現実の対応

- IIS の管理者へ連絡。patch 適用とあとしまつを推奨。
- その後、当該 IIS は Apache 2 へ置き換えられた模様。

Forensic は有効か?

- 有効
  - Computer Forensic: IIS マシンの悪用され具合を判断できる。
  - Network Forensic: 攻撃された時刻やその内容、別途バックドアを仕掛けるようなやりとりの有無などを判断できる。
- 問題
  - 通信を暗号化された場合、Network Forensic は威力が半減
  - ポリシー問題(後述)

事例: web 掲示板への悪意ある書き込み

- 内部から外部
- 図書館に設置されていた PC から、とある団体が運営する掲示板に、その団体を中傷する書き込みがあった（らしい）
- 当該団体から抗議があった（らしい）

現実の対応

- 当該団体に謝罪した（らしい）
- インシデント発生当時、図書館の PC は認証手段なしで利用できたため、誰が書き込みを行ったのかは不明

Forensic は有効か?

- 部分的に有効
  - Computer Forensic: その有効性は限られるだろう。
  - Network Forensic: 書き込みが行われた時刻やその内容を確認できる。当該団体からの抗議が、実際の行為に基づいた正当なものなのか、それとも虚偽に基づいた詐欺行為なのかを判断できる。
- 問題
  - 行為を行った人物を特定するのは困難。
  - ポリシー問題（後述）

事例: プライバシー情報の流出

- 外部から内部（情報取得者の視点で）
- 2ch.net において「龍大のとある URL に興味深いファイルがある」といったような書き込みが
- その書き込みを見たある人が「こんなの出てましたぜ」と小島に知らせた
- web サーバ管理者が意図せずに公開してしまっていた模様

現実の対応

- 当該 web サーバ管理者に連絡
- まもなく web サーバは一時的に閉鎖され、設定が見直された模様

Forensic は有効か?

- ほとんど意味がない?
  - Computer Forensic: ほとんど意味がない?
  - Network Forensic: web サーバの log がきちんと確保してあれば、ほとんど意味がない? クロスチェックはできるだろうし、web サーバの log がない場合には有効だろう。
- 問題
  - 出て行った情報を回収することはできない。
  - 誰が取得したのかはわからない。
  - ポリシー問題(後述)

事例:意図しない DoS 攻撃

- 内部から外部
- Windows + IE で就職情報サイトにアクセス
- proxy は Microsoft IAS 2000
- なぜか就職情報サイトに大量のアクセスが
- 就職情報サイトのバックエンド DB サーバがダウンしたらしい
- 就職情報サイトの管理会社からの連絡で発覚

現実の対応

- 端末と proxy server を調査
  - 端末には特に異常はないようだ
  - proxy server には確かに大量アクセスの痕跡が、ただしタイムスタンプが狂っている
- 利用者に状況を聞く
  - 登録しようとボタンを押したら無反応になったので IE を終了させた。F5 連打、などは行っていない
- 管理会社の社長がやってくる: 損害賠償請求も検討
- 何が原因だったのか?
  - いま 3 つほど不明…
  - とりあえず IAS 2000 は廃棄し squid に変更

Forensic は有効か?

- 部分的に有効
  - Computer Forensic: ほとんど意味がない?
  - Network Forensic: client が悪いのか proxy が悪いのかの切り分けが可能
- 問題
  - プロダクトのバグが原因であることを示すにはどうすればいいの?
  - 誰に責任を問えばいいの?
    - ソフトベンダー
    - SI 屋
    - 龍大
    - 落ちるような DB をつくっていた管理会社

まとめ的

- Forensic が使えそうなシーンは存在する。
- Network Forensic の方が使えそうなシーンは多そう。
  - 金もかかるが
- 常に役に立つわけではない。
- 暗号化されると弱い。
  - 「インストールされた全てのバックドアが暗号化技術 (SSH) を利用していました。暗号化することによりトラフィックの解析を妨げることができます。」 http://www.lac.co.jp/security/intelligence/sombria/smbr_j_1.pdf

ポリシー問題(プライバシー問題)

- Forensic は隠された秘密を暴く行為
- 隠された秘密を暴こうとする過程でプライバシーを暴いてしまう場合が大いにあり得る
  - 意図せずに
  - 意図して
- 特に Network Forensic は強力なプライバシー収集装置と化す恐れがある
  - それを扱う人間はまともなのか? どうやって監査する?
  - 大学という場では強力すぎる? IDS くらいが限界か?

まだまだ問題

- 多くのインシデントは管理権限外で発生
  - Computer Forensic したくてもできない
- Computer Forensic はコストがかかる
  - 特に時間というコスト
  - Computer Forensic するだけの価値があるシステムなのか?
  - 実行の是非は誰が決める? → やっぱりポリシー
- だいたいの原因がわかった段階で回復段階へ移行するのが、半径 50m 以内では一般的な状況
  - 十分な回復処置がされているかどうか知らんが…

Forensic を流行らすには?

- ポリシー
  - どういう状況なら Forensic するのか（しないのか）
  - 誰が決定するのか
  - 権限の付与と操作担当者自身への監査
- 吉野家 Forensic tool が必要
  - 高速（はやい）
  - 使いやすい（うまい）
  - 安価（やすい）
  - 十分によくできていれば、end user 自身が Forensic を実施できるはず