Internet Week 2008　「2008年我々を悩ませた脆弱性たち」

2008年を生暖かい目で振り返って

北陸先端科学技術大学院大学
情報科学センター
篠田陽一

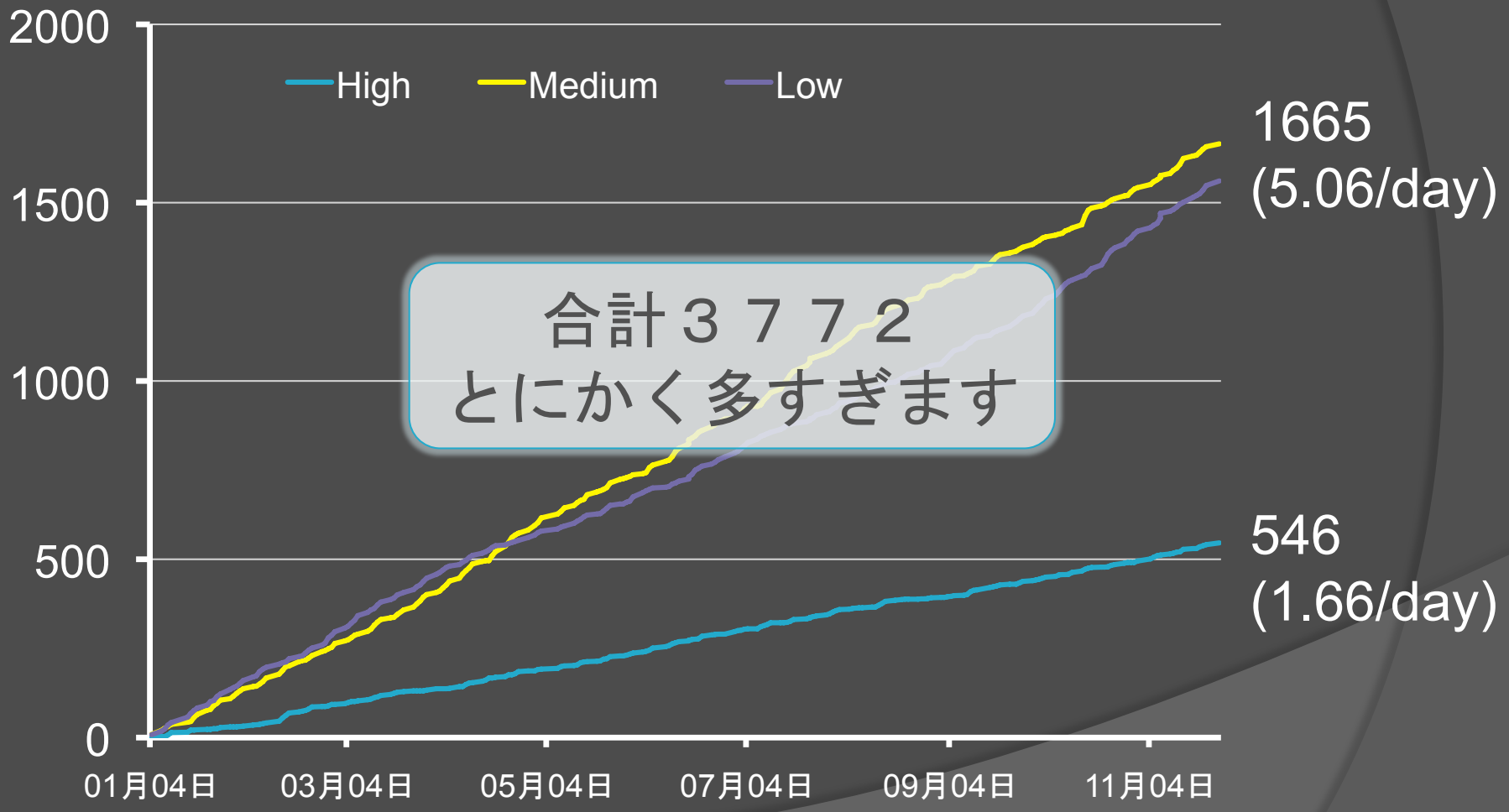
数の暴力

ある脆弱性情報流通サービスが伝えた脆弱性の数

- あらゆる種類のソフトウェア（PC-OS、サーバーOS、デバイスOS、メジャーなアプリ、ライブラリ、etc.）を含む。
- 深刻度（High, Medium, Low）はサービスの独自判断。

- メールボックスファイルから（簡単な）スクリプトで自動生成してみました。（そのため、同一情報のアップデートなどは重複して数えています。）

ある脆弱性情報流通サービスが伝えた脆弱性の数

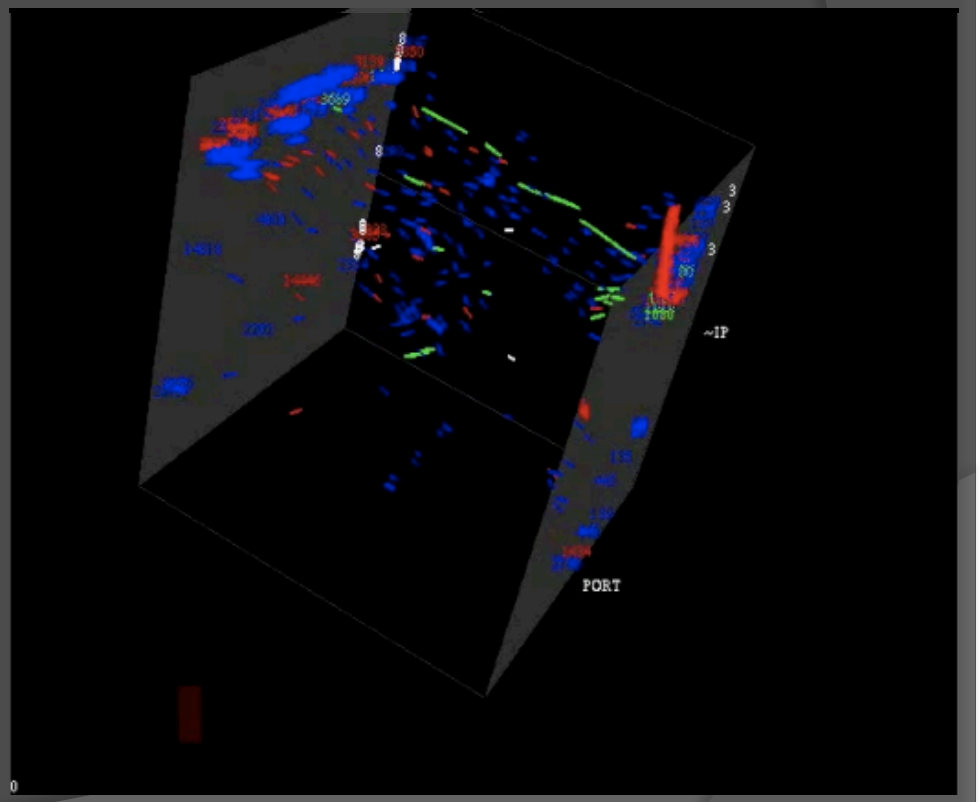


MSに限ってみても

- MS08-001 ～ MS08-069
  - うち緊急36、重要31、警告2
- 特筆すべきもの
  - MS08-001
    - TCP/IPスタック
    - カーネル内部のプロトコルスタックの脆弱性であるため、標準ネットワークAPIをフックするタイプのホストベースIDS/IDPが動作しない。
    - ドライバレベルのパッチが必要なため、事前検証が大変。
  - MS08-030
    - Bluetoothスタック
  - 2件のGDI+関係 (021, 052)

ネットワーク攻撃は廃れたのか?

- 標的型攻撃がメインになっているという噂は本当か?
- 前出の脆弱性情報から”リモート”をgrepすると、432件のエントリを抽出できる。
- まだまだ来るぞという印象。



NiCT National Institute of Information and Communications Technology nicter

トンネル効果

- 隔離・独立（していると思いこんでいる）システムに、思いこみの壁を越えてマルウェアが染み出す現象。
  - いかにもヤバそうなUSBメモリ
  - ベンダーのCEが持ち込むPCベースの測定器
  - 外部接続しているシステムと並べてオペレーションしている環境で、間違って外したケーブルを入れ替えて再接続
  - （近未来的には）お出かけから帰ってきたワイヤレスモバイルデバイス

その他

- 経路ハイジャックの流行

An another look at the Kaminsky class attack

今朝自宅でテストしてみました

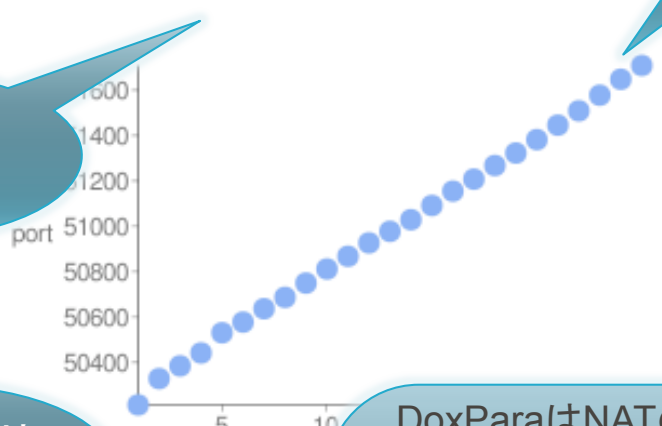
http://entropy.dns-oarc.net/test/

これ
ダメやん
（涙）

Source Port Randomness: GOOD

一見よさ
そうです

真ん中より
ヤバ目？



Number of samples:
Unique ports: 25
Range: 50213 - 51709
Modified Standard Deviation: 438
Bits of Randomness: 11
Values Seen: 50213 50329 50385 50442 50531 50578
50868 50927 50978 51029 51092 51155
51446 51509 51578 51648 51709

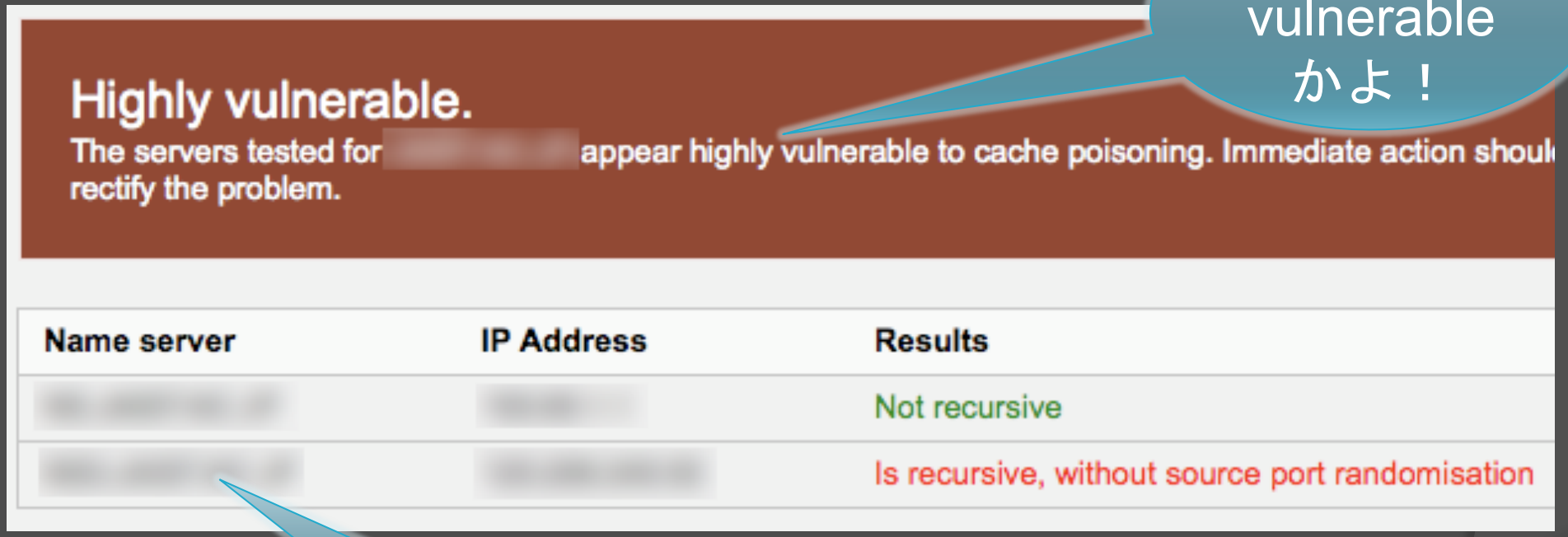
DoxParaはNATの整流効果を指摘

Your name server, at [redacted] may be safe, but the NAT/Firewall in front of it appears to be interfering with its port selection policy. The difference between largest port and smallest port was only 170.

Please talk to your firewall or gateway vendor -- all are working on patches, mitigations, and workarounds.

別のところも調べてみました

http://recursive.iana.org/



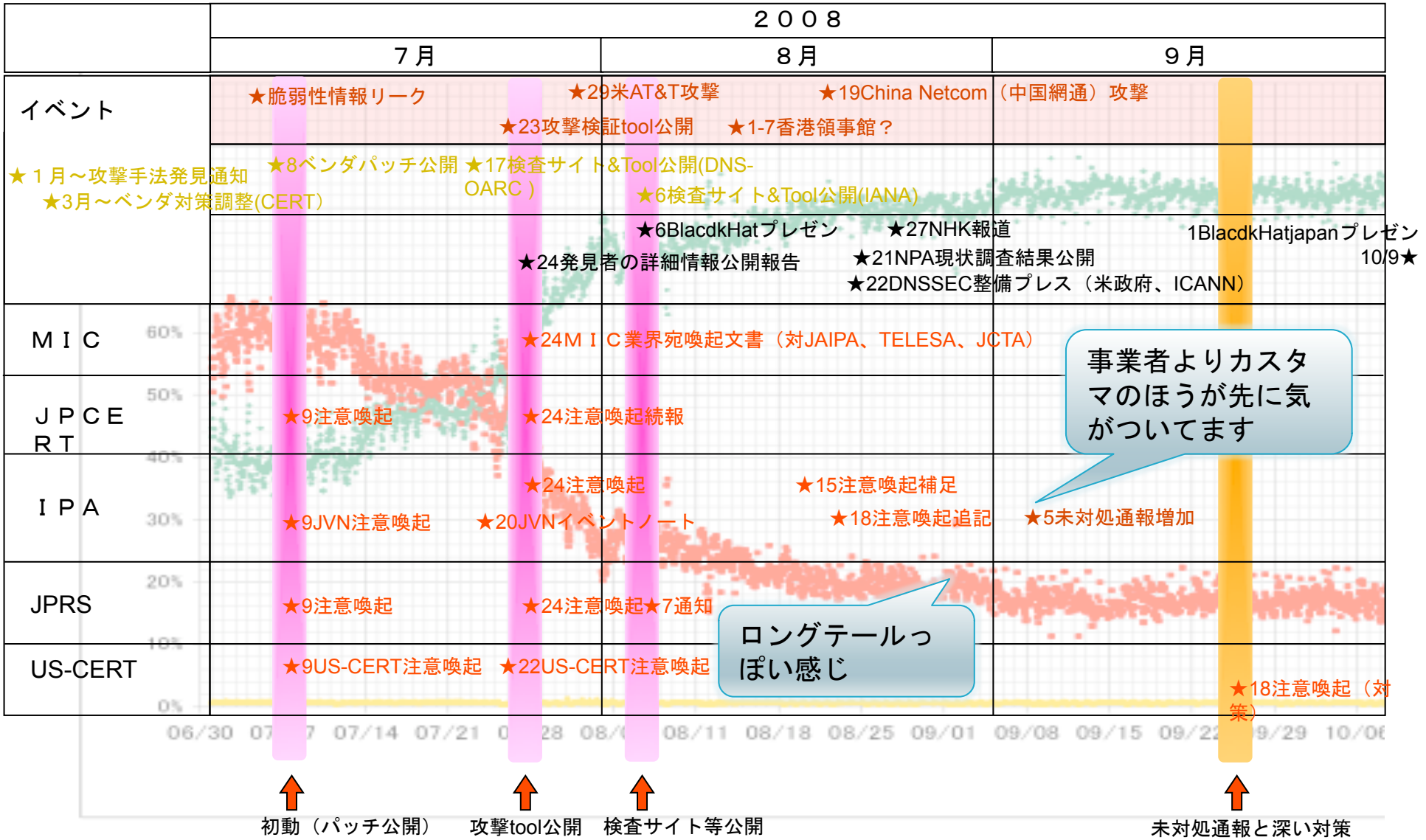
Highly vulnerable かよ！

隠れサーバ（号泣）

メールサーバが引くDNS?

- DoxParaでは、メールサーバが引くDNSの検査ツールも公開されています（いました）。
- 9/8の時点で4つのISPを調べたら、2つにアウト判定が。
- いろいろ（もっともらしい）理由はあるらしい。

イベント時系列



あるひとが言うには

- この件は、ＤＮＳの脆弱性なので、○凸△の担当者に技術的な内容を理解させるのは無理です。

  通知を保守業者にさっさと渡して、
  対策しなさい！
  終わったらこのツールで確認
  しなさい！

  というのが妥当な指示かと思います。

- やってみたけどダメだった・・・

Kaminskyが暴いた非技術的脆弱性

- PCの脆弱性対策と同じ構図
  - 最後のひと握りのシステムは（それがグローバルインフラの一部であっても、）まっとうな手段では対策できない（させられない）
- 該当しないという思いこみ（該当させたくない場合も?）
- ナイナイづくし（多くはTCO感覚の欠如）
  - 金が無い
  - 時間が無い
  - 人手が無い
  - 記憶が無い
- SQLインジェクション化?

Implications

- 組込みシステム v.s. インフラ要素
  - 「組込みシステムの脆弱性対応をきちんと考えていかなければならない」というコンセンサスは取れつつある。
  - グローバルネットワークの要素システムについても、おなじ考え方をしていく必要がある!?
  - Updateに関する状況にも共通点あり。
  - かなりドラスティックなコンセプトが必要。
- 新DNS移行 v.s. 地デジ移行?

SQLインジェクション・・・

Kaminsky攻撃 v.s. SQLインジェクション

- 対策レベルでは同様の議論が展開できる。
  - 新しい要素の加味も
- 原因レベルでは全く異なる構図が・・・
  - セキュリティレス仕様
    - 無邪気なオーバースペック
    - 扱う情報の質を考慮しないイージーな造り
    - 輸入モジュール（特にOSS）の脆弱性の伝搬
  - お行儀の悪いコーディングと開発プロセス
- セキュリティ・バイ・デザイン

誰もが
ヤバいかも
と思っている話

無線LANの暗号プロトコル

- WEP: かなりヤバい
- WPA/TKIP: そろそろヤバいかも?
- アクセスポイントの物理更新!?
- 公衆ホットスポットでの対応!?
- 安全なものと安全でないものの区別がつかないケースが多すぎます。

人材育成二題

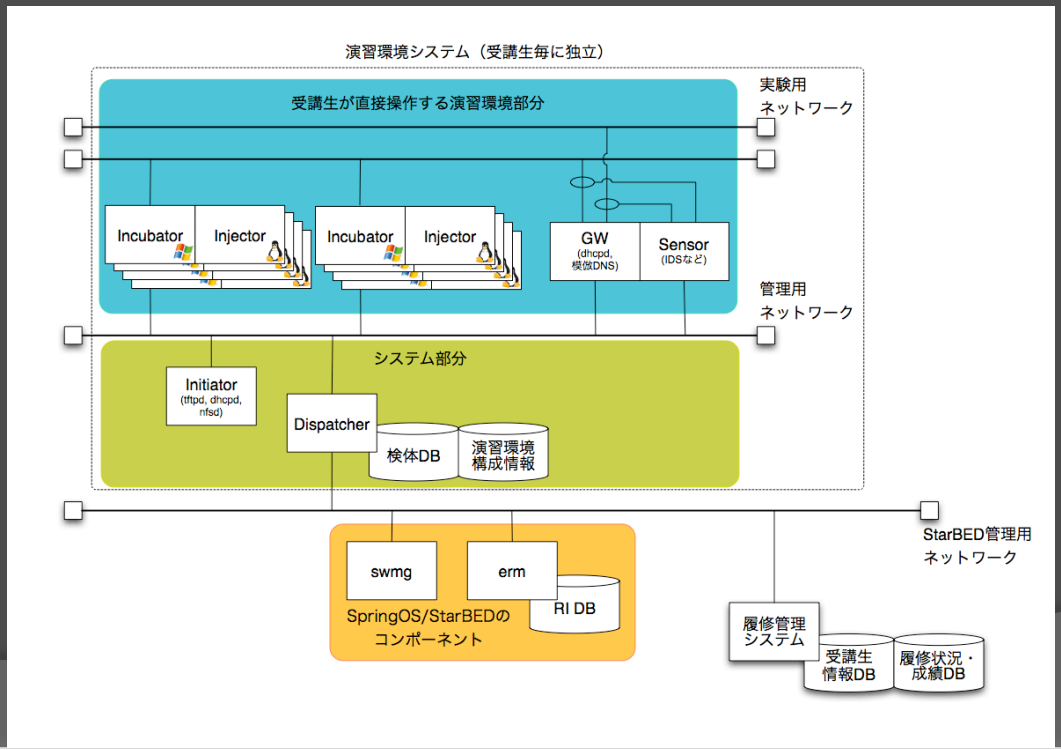
IT-Keysのとりくみ

- 先導的ITスペシャリスト育成推進プログラム「社会的ITリスク軽減のための情報セキュリティ技術者・管理者育成」
- 奈良先端大、阪大、京大、JAIST、NTTコミュニケーションズ、情報セキュリティ研究所、NICTなどによる共同プログラム

- 実践科目（演習）の重視
  - IT危機管理演習
  - インシデント体験演習
  - リスクマネジメント演習
  - 無線LANセキュリティ演習
  - システム攻撃・防御演習
  - システム侵入解析演習

IT-Keys インシデント体験実習

- StarBED上に構築した疑似サイト上で起きる侵入インシデントを2日半にわたって体験処理。



The StarBED

インターネットシミュレータ

MWS 2008の開催

- マルウェア対策研究人材育成ワークショップ2008
- Computer Security Symposium (CSS) 2008と併催で丸々3日間
- 情報処理学会、サイバークリーンセンター、IPA、 JPCERT/CC、TelecomISAC Japan

- ワークショップの目的
  - 研究用データセットの提供
  - 研究成果の共有
  - 切磋琢磨する環境の提供
- 開催状況
  - とりくみに関してポジティブな意見多し。
  - 学会にも関わらず、現場のオペレータの方々の出席があった。

それでは専門家のみなさん
よろしくお願いします