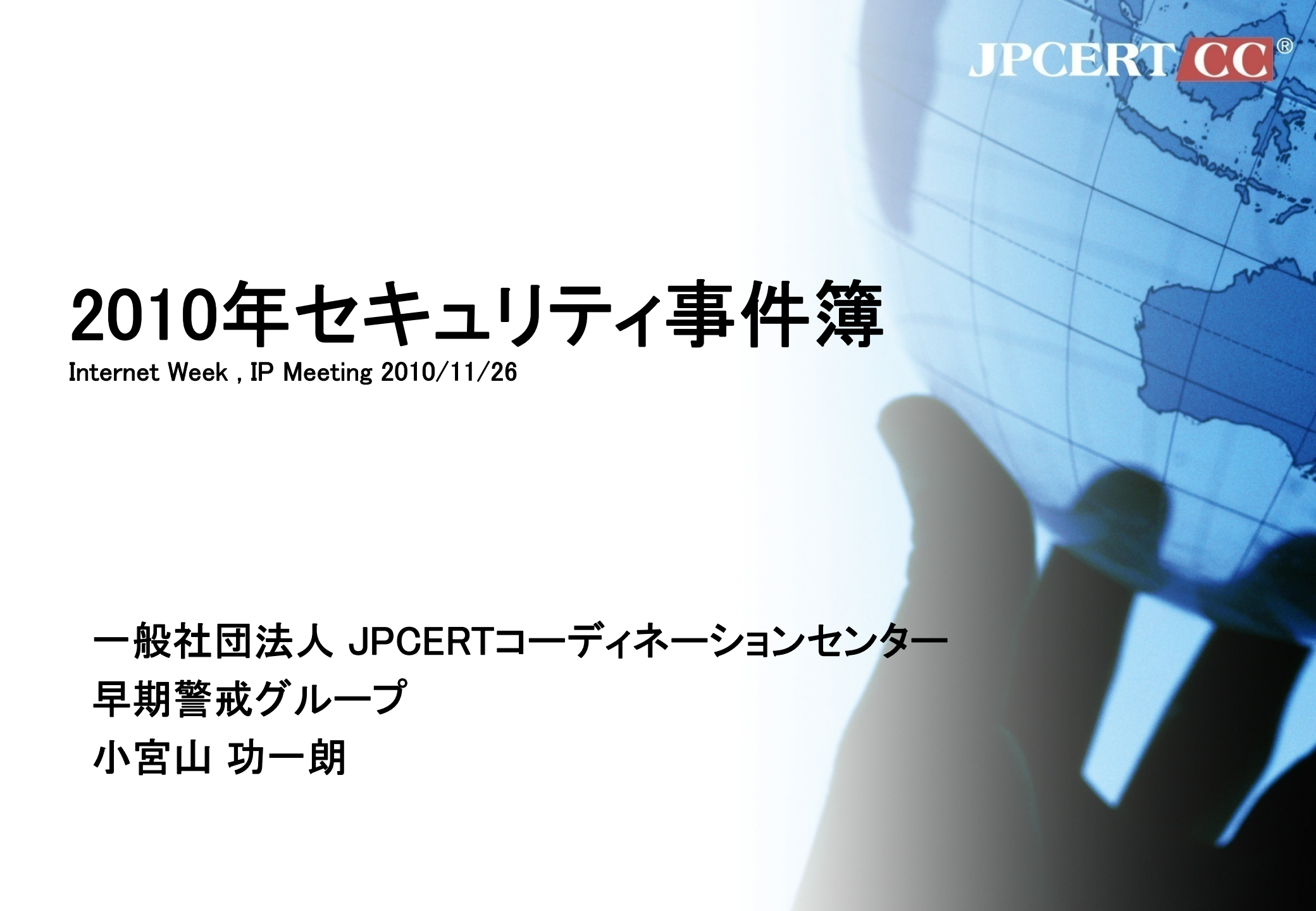


2010年セキュリティ事件簿

Internet Week , IP Meeting 2010/11/26

一般社団法人 JPCERTコーディネーションセンター
早期警戒グループ
小宮山 功一朗

目次

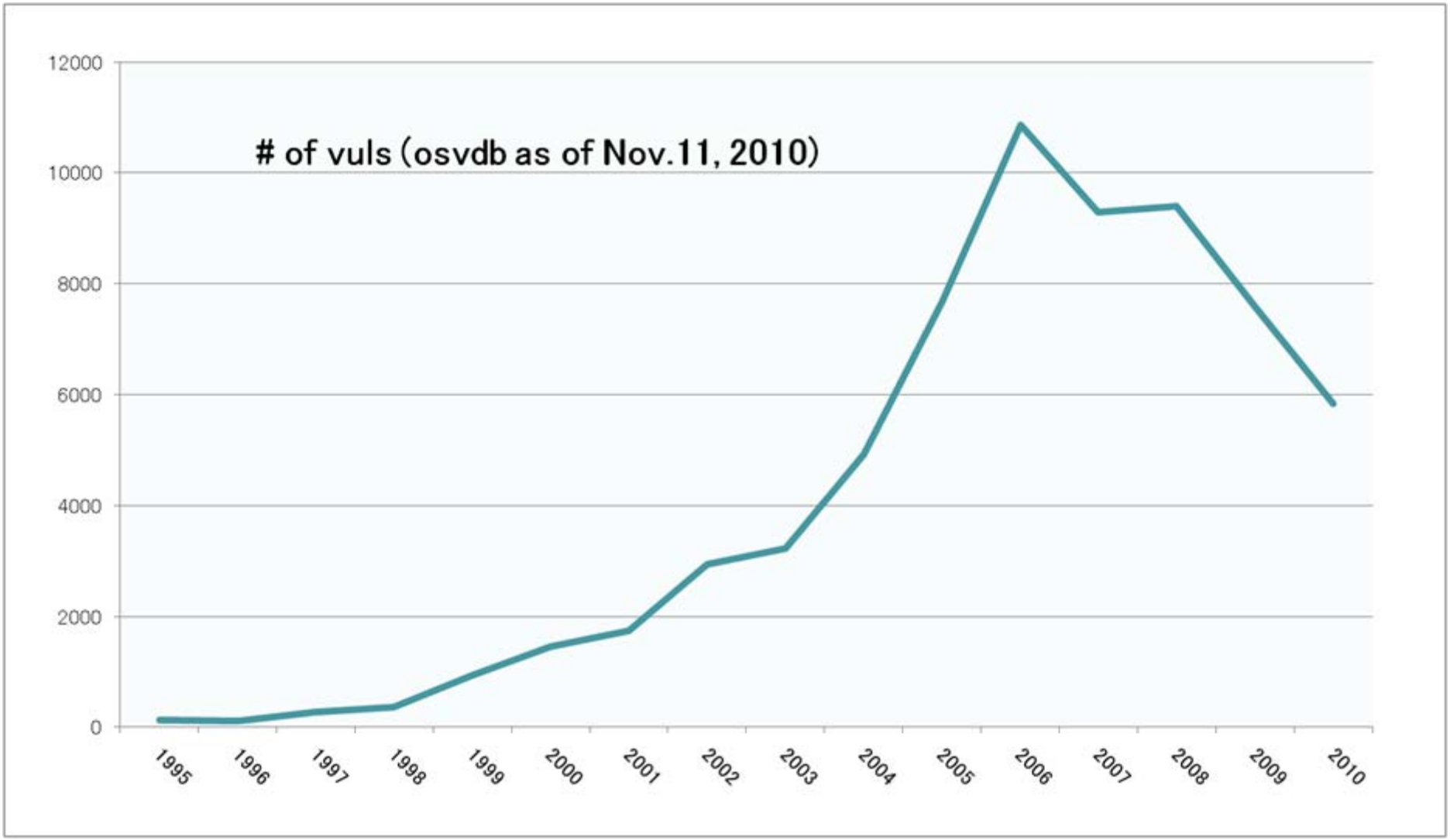
- 脆弱性を振り返る
- コントロールシステムの危機
- 岡崎図書館(Librahack)
- 日本語のフィッシング増える
- 内部犯行対策の重要性高まる
- 国際的な動向

今年の脆弱性を振り返る

~~CVEはじめました~~
CVEふりはじめました

- JPCERT/CCが国内初のCNA(CVE Numbering Authority)に認定
  - 2010/08/20　JVN#91740962: CVE-2010-2360
    Winny におけるバッファオーバーフローの脆弱性
  - 2010/08/20　JVN#21471805: CVE-2010-2360
    Winny におけるバッファオーバーフローの脆弱性
  - 2010/08/20　JVN#25393522: CVE-2010-2362
    Winny におけるノード情報の処理に関する脆弱性
  - 2010/08/20　JVN#54336184: CVE-2010-2361
    Winny における BBS 情報の処理に関する脆弱性

脆弱性の数の推移



Windows　のDLL読み込みの脆弱性について

JPCERT CC®

8月23日　新たな脆弱性のニュースが流れる。

『iTunes』で対応済みの問題、他の『Windows』アプリにも影響か
　ある第一線のセキュリティ専門家によると、『Windows』版『iTunes』の重大なバグはすでに修正済みだが、他にも多くの Windows アプリケーションが危険をはらんでいるかもしれないという。

http://japan.internet.com/webtech/20100823/12.html

8月20日のCOMPUTERWORLDの記事が今回の発端

Update: 40 Windows apps contain critical bug, says researcher
Separate patch required for each, says HD Moore, who declines to name affected software

http://www.computerworld.com/s/article/9180901/Update_40_Windows_apps_contain_critical_bug_says_researcher

8月24日　Microsoftがアドバイザリを公開

マイクロソフト セキュリティ アドバイザリ (2269637)　安全でないライブラリのロードにより、リモートでコードが実行される

Bainary Planting または DLL PreLoading Attack と呼ばれる問題
各プログラムの不適切なDLLのロード方法により問題が発生する。

http://www.microsoft.com/japan/technet/security/advisory/2269637.mspx

Windows　のDLL読み込みの脆弱性について

JPCERT CC®

DLLロード方法の問題

１　DLL呼び出し時に、絶対パス(a fully qualified path name)で呼び出さなかった時に、WindowsはDLLが見つかるまで様々なディレクトリを検索する。

２　検索の順番は以下のとおり。 この中のどれかのディレクトリが攻撃者のコントロールにある場合攻撃が成立する。(これはセーフサーチモード有効の時)

１　アプリの存在するディレクトリ
２　システムディレクトリ
３　16ビット・システムディレクトリ
４　Windowsディレクトリ
５　カレントディレクトリ
６　環境変数 PATH のディレクトリ

３　回避策

１　絶対パス名の使用
２　Dll redirection または Manifest を使用し、アプリが使用するDLLをしていする。
３　safe dll search mode を有効にすることでカレントディレクトリの検索順を後にし、正規のDLLが読み込まれるチャンスを増やす。
４　Windows API のSetDllDirectory　のDLL　Search Path に　“”　を入力する。
５　safe process search mode　が有効でない場合、Windows API　のSearchPath　を使用しない。
６　DLL検索に基づくシステムバージョンの推定をしない。

４　問題のある製品は

Windows　のDLL読み込みの脆弱性について

問題のある製品　8/27時点

企業名	製品名
Apple	iTunes
Avast! Antivirus Software	avast! Antivirus 5.x
BitTorrent	uTorrent 2.x
Cisco Systems, Inc.	Cisco Packet Tracer 5.x
IZArc	IZArc Archiver 4.x
Microsoft Corporation	Windows
Nullsoft	Winamp 5.x
Opera	Opera 10.x
PKWARE	PKZIP 12.x
RealNetworks, Inc.	RealPlayer SP 1
Sonic Solutions	Roxio Easy Media Creator 9.x
SweetScape Software	010 Editor 3.x
TeamViewer	TeamViewer 5.x
TechSmith Corporation	Camtasia Studio 6.x Camtasia Studio 7.x Snagit 10.x
VideoLAN	VLC media player 1.x
VMware	Vmware　製品群 http://www.vmware.com/security/advisories/VMSA-2010-0007.html

「Macなら安全」神話

- 最も脆弱性が多いのはApple 社．ただし，この数字では，深刻度やパッチ提供の早さは勘案されていない． Secuniaの報告書より
  (http://secunia.com/gfx/pdf/Secunia_Half_Year_Report_2010.pdf)

コントロールシステム/SCADA

【トピックス】

マイクロソフト セキュリティ アドバイザリ (2286198) Windows シェルの脆弱性により、リモートでコードが実行される

7月10日　ウィルス対策製品ベンダーVirusBlokAda が新たな脆弱性について報告

http://www.anti-virus.by/en/tempo.shtml

- この脆弱性は当初、USBメモリ内にある不正なlnkファイルの含まれるフォルダを開くだけで攻撃が実行されるという紹介であった。
- 感染後「Siemens WinCC SCADA systems」を探す。
- 感染後インストールされるルートキットドライバ「mrxnet.sys」「mrxcls.sys」にはRealtekの署名がされている。
- 回避策として、アイコンを表示しないファイルマネージャの使用

SCADA（*Supervisory Control And Data Acquisition* の略）は、産業制御システムの一種であり、コンピュータによるシステム監視とプロセス制御を行う。

7月16日　エフセキュアブログで一般公開　http://blog.f-secure.jp/archives/50427680.html

- 新たに、JMicron の有効な署名が使用されていることを確認

7月17日　マイクロソフト セキュリティ アドバイザリ (2286198)　公開

- pifファイルも該当する。
- WebDAV経由での攻撃の可能性
- マイクロソフト　オフィス文書のような埋め込みショートカットをサポートする文書も対象に。（**21日更新**）
- Fix itの提供開始 http://support.microsoft.com/kb/2286198

STUXNET

- 複数のゼロデイ脆弱性を用いて、感染を広げる
  - シーメンスのWinCC/PCS 7
- デジタル署名されている(Jmicron, Realtek)
- 特定周波数を使うVFD(可変電圧可変周波数制御)
- P2Pでのアップデート機能
- 日本でも感染が確認された

岡崎図書館（Librahack）

岡崎図書館（Librahack）

JPCERT CC®

- 岡崎図書館事件の流れ

1. Librahack氏によるクローラを使用した図書館へのアクセス
2. 図書館システムに不具合があった
   - 設計の問題
     - セッション管理の問題など（DBサーバへの接続可能数を超える）
3. DBサーバへの接続不能

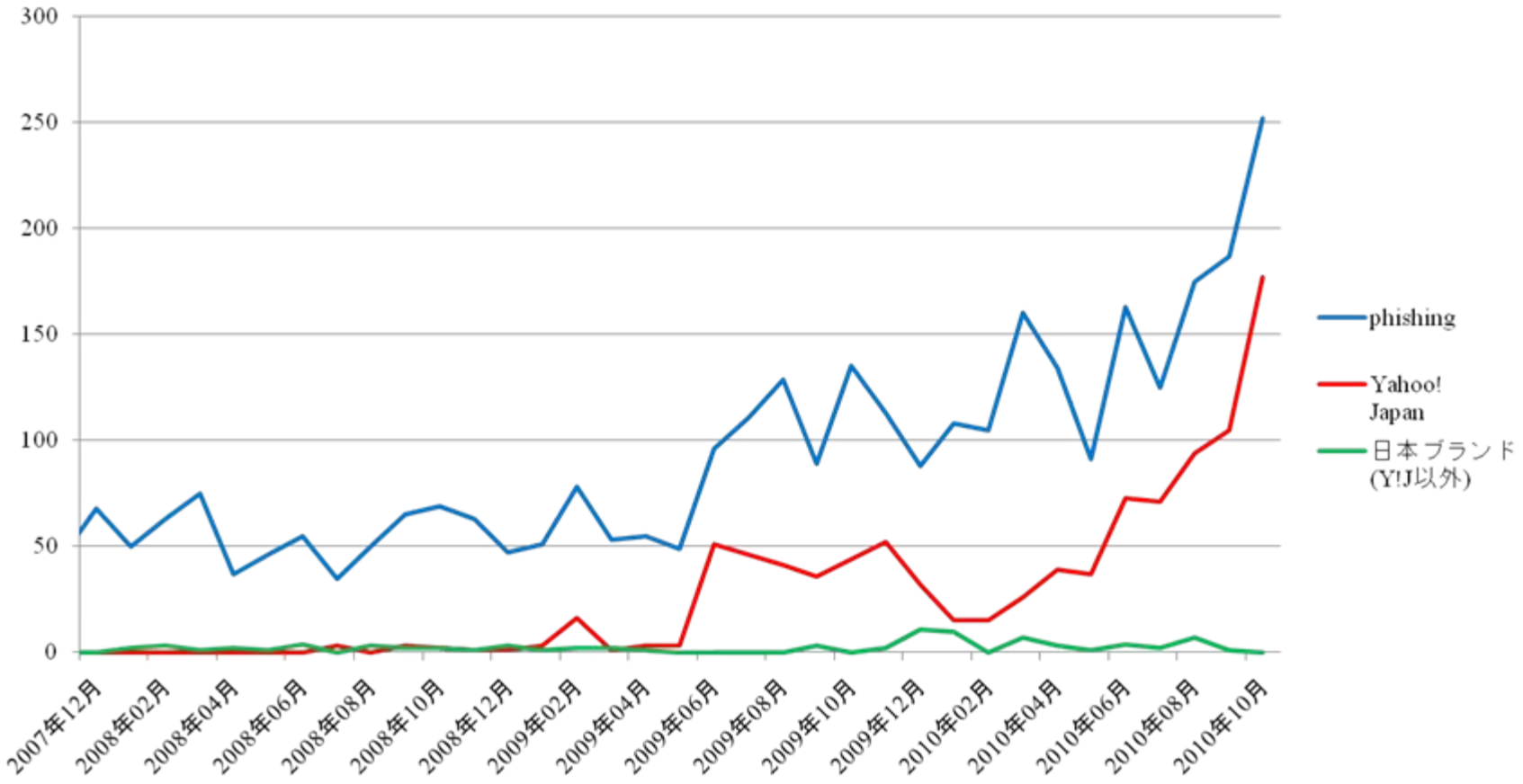
- 対応
  - 図書館側
    - 警察に相談→被害届の提出
  - 警察側
    - 家宅捜索→逮捕
  - 検察側
    - 「起訴猶予処分」による釈放

岡崎図書館（Librahack）

- 技術的な問題
  - 根本的な対策が行われてなかった
- 警察の対応
  - 原因について、肝心な捜査が行われず。
- JPCERT/CCに相談しておけば。。。
  - 違う結果になっていたかもしれない。

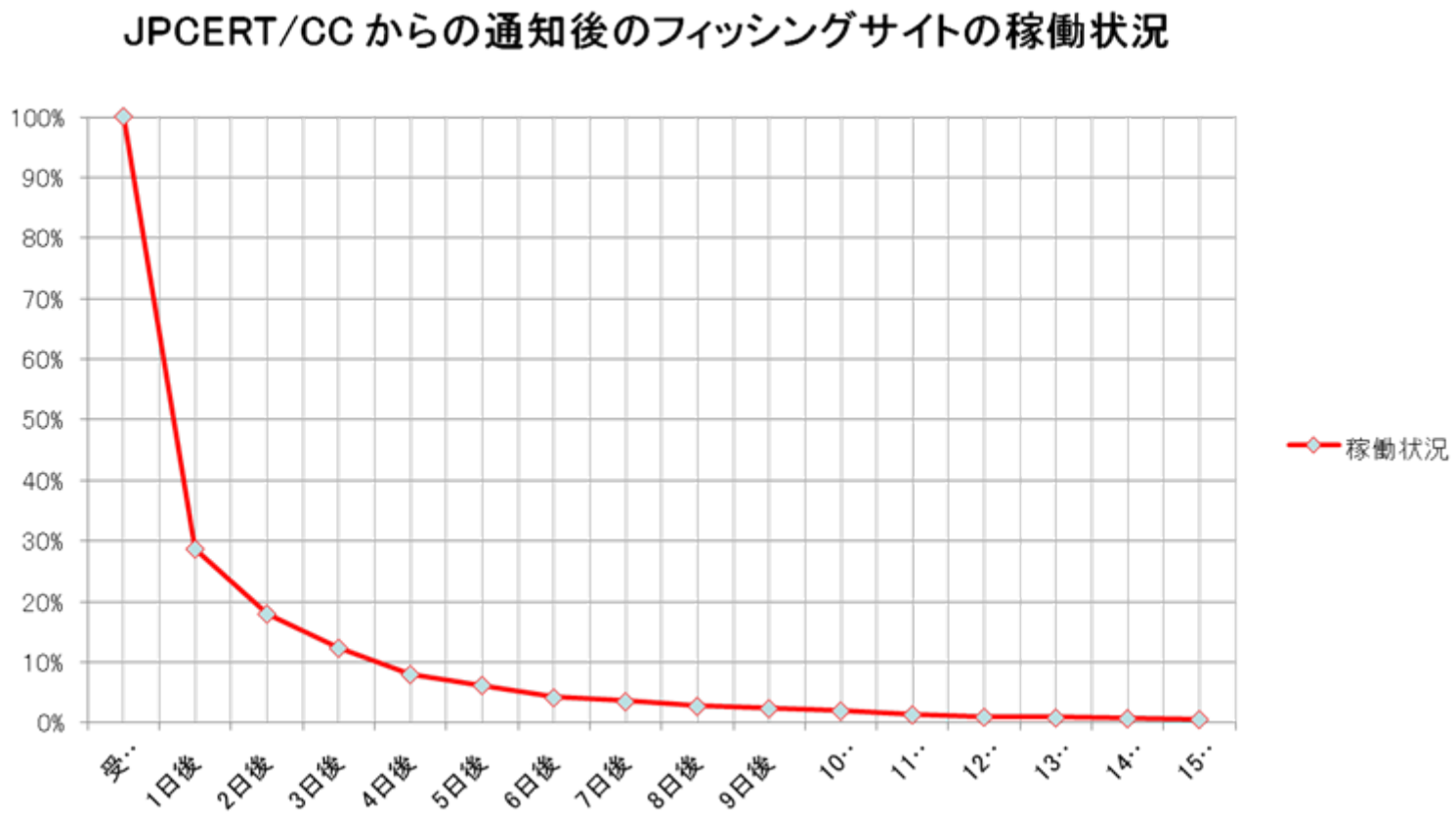
フィッシング

フィッシング報告件数の推移 ～ JPCERT/CC ～



Yahoo! Japanのフィッシングサイトが大多数を占める

フィッシングサイトの稼働状況



通知から3日で約90%のサイトが停止する

内部犯行

内部犯行の実例

- **銀行システムへの侵入・破壊**
  - インド人の元派遣社員(32)が元の勤務場所である銀行のネットワークへの不正アクセス禁止法違反容疑などで逮捕された。同容疑者は、自宅のパソコンから、銀行の内部ネットワークのサーバに67回侵入し、約2600個のファイルを削除してシステムを破壊するなどした。(読売新聞2008. 07. 17)
- **証券会社システム担当部長代理による顧客データ持ち出し・売却**
  - 2009年3月、証券会社のシステム担当であった部長代理が、同社のデータベースに不正に接続して148万人の顧客データを持ち出し、うち5万人分を名簿業者に売却していたことが判明。元部長代理は窃盗及び不正アクセス禁止法違反で懲役2年の実刑判決を受けた。(読売新聞2009年11月13日など)。

事例からあきらかになったこと

- 4つの類型にわけられる
- システム悪用
  - 自らの銀行口座に不正に入金させ組織の資金を横領する
  - メールを盗み見る/転送する
- 情報流出 I型
  - 金銭目的。顧客情報データベースを持ち出し、転売する
- 情報流出 II型
  - 心理的満足が目的。上司/同僚のメールを盗み見する
- システム破壊
  - メールを削除する
  - 退職後に職場のシステムに保存されている営業用のデータを消去したり、自らが構築したシステムのデータやプログラムの一部を消去する

内部犯行者

- **性別、職歴**
  - システム悪用は女性に多かった
  - 転職回数が全体的に多い傾向がみえる
- **人柄**
  - 幼稚、短気と評価される場合が多いが、真逆の事案も
- **前科**
  - 多くの場合初犯
- **履歴書の嘘**
  - 履歴書を偽るケースが複数確認された
- **動機**
  - システム悪用は金銭目的
  - ちょっとした不満+時間的余裕(暇)が犯行につながる
- **犯行手段**
  - お試しから本格的な犯行へ
  - パスワードを変更していればおよそ半分が防げた

国際連携

官民サイバー演習 cyberstom3

国際サイバー演習に日本初参加　ネット攻撃に協調対応(10/10/4)

米国の国土安全保障省が9月最終週に実施した世界最大規模の官民サイバー演習に、日本の政府機関や民間団体が初めて参加した。インターネットが社会・経済の重要な基盤になるなかで、米国は「サイバーセキュリティー（ネット空間での安全保障）」に力を入れており、各国に協調を呼びかけている。

演習はインフラのシステムがネットワークを介して攻撃を受けたことなどを想定。事態の進展に応じて、どのような指示・連絡をすべきか実際に判断する訓練をした。日本からは内閣官房情報セキュリティセンター（NISC）のほか警察庁、経済産業省からネット上の監視を委託された非営利団体「JPCERT／CC」（東京）が参加。警察庁幹部は「日本としても世界の状況を知る必要がある。万一の際に各国のどことどう連絡を取るべきかの訓練にもなる」と話している。

アフリカにCSIRTを作ろう!

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: http://www.jpcert.or.jp/

インシデント報告

- Email：info@jpcert.or.jp
- Web:　http://www.jpcert.or.jp/form/