インターネットセキュリティ トピックス

有限責任中間法人
JPCERTコーディネーションセンター
業務統括　伊藤 友里恵

JPCERT CC™

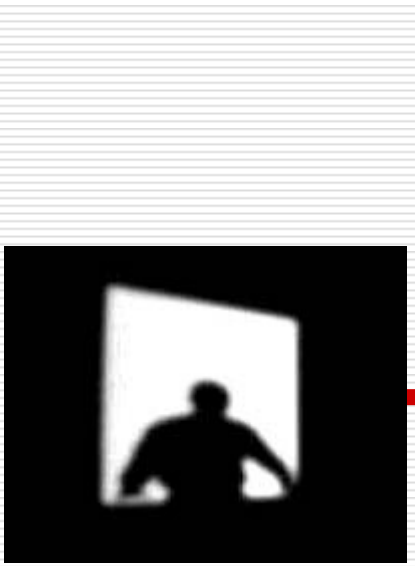
本日のプレゼンテーション内容

1. インシデント動向 – 目的/動機、手口
2. セキュリティ動向 – 対策、体制
3. 重要インフラ防護の動き
4. CSIRTコミュニティにおける動向

JPCERT CC™

1. インシデント動向

強い動機と手段を選ばない攻撃



行為者

Spyware
Botnets
Phishing
トロイの木馬
等....

ツール
メソッド

ソーシャルエンジニアリング

脆弱性への攻撃など

技術

資産

JPCERT CC™

インシデント動向

- 相手はもはや愉快犯や Script Kiddy ではない
- 組織的に明確な目的を持って Underground の非常に高い技術力と結びついている
- 特定のサイトを攻撃目標にした大規模攻撃
- 動機は様々：金、政治、強い悪意

インシデント　ー　ボットネット

- ボットネット:
  SPAM メール、DDoS の元凶となっている。
  広域に拡散するワームやウイルスと異なり、ボットは局地的に拡散する傾向にある。

  - 大量の亜種　ー　ボットの作成は簡単
  - 探知が困難　ー　ボットネットは密かに活動
  - 検出が困難　ー　パターンマッチングの限界

ボットネットはさらに高度化していく

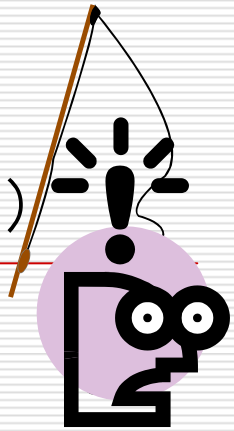
インシデント　ー　ボットネット

- ボットは、一日80種以上の亜種が発生
- セキュリティ対策が行われていないPCをインターネットに接続すると、平均4分で感染
- 日本国内のISPユーザの　**2～2.5%**　がボットに感染
  - ブロードバンドユーザ数：2000万契約とした場合、**40～50万人(台)**が感染していると推測される

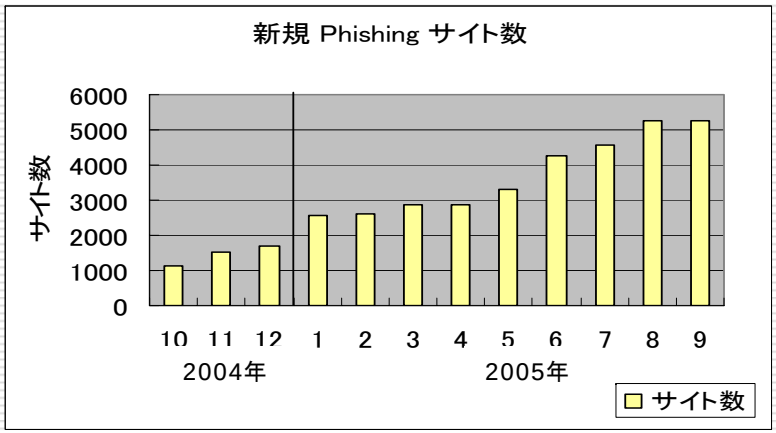
JPCERTコーディネーションセンタとTelecom-ISAC Japan 共同調査結果より

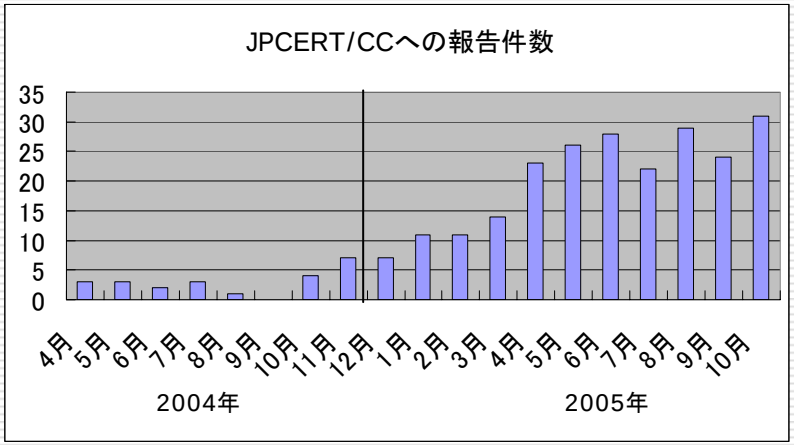
JPCERT CC™

インシデント　ー　フィッシング（Phishing）



- フィッシング（Phishing）：
  - 世界的にフィッシングサイトが急増している
  - 日本の消費者をターゲットにしたフィッシングも発生している
  - JPCERT/CCへの届け出も増加傾向に





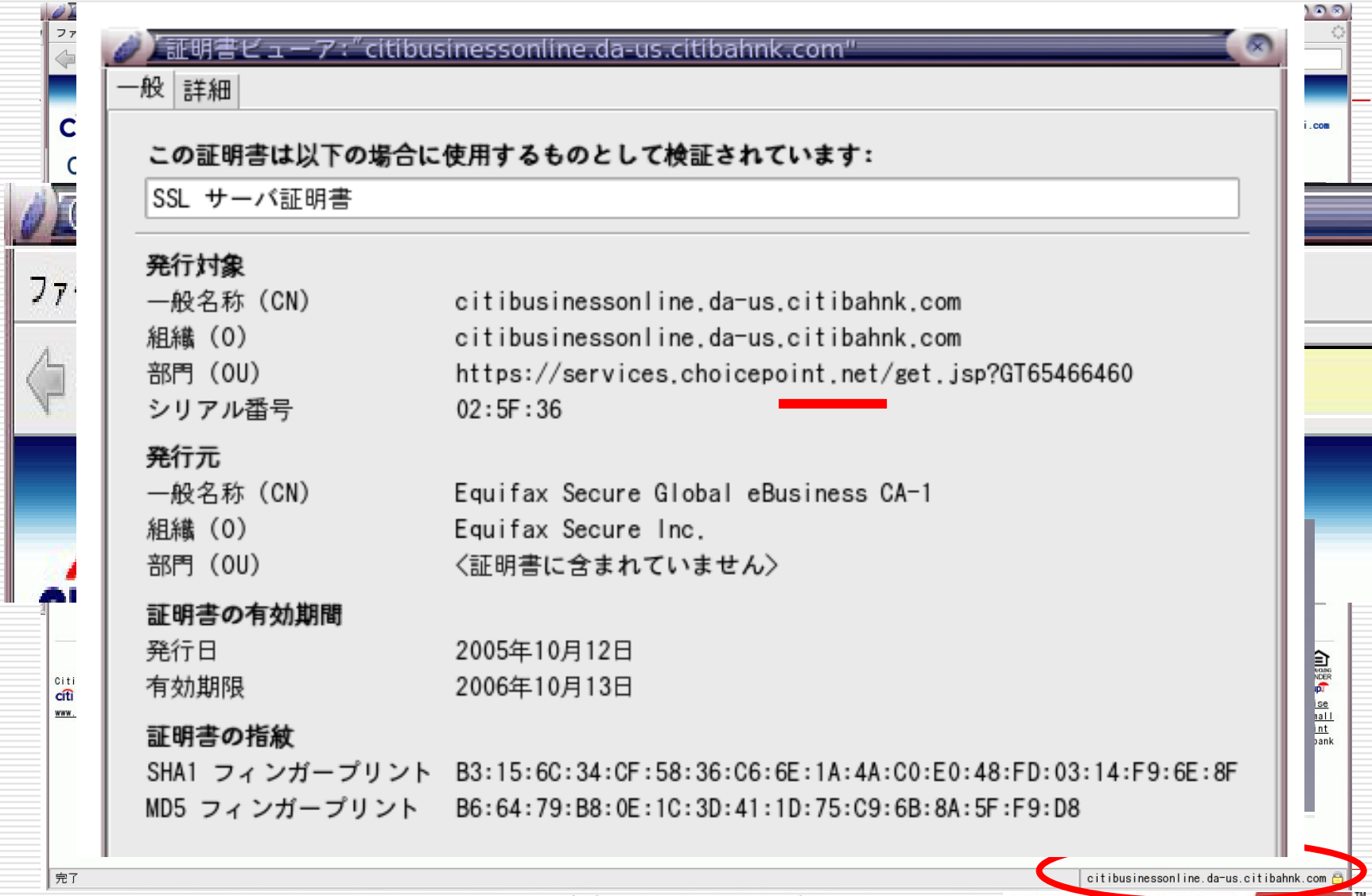
出展:Phishing Activity Trends Report September, 2005

http://antiphishing.org/apwg_phishing_activity_report_sept_05.pdf

JPCERT CC™

インシデント　ー　フィッシング（Phishing）

- 巧妙な手口
  ちょっと見ただけでは、偽物と見抜けない
  - Web ブラウザのアドレスバーを偽装
  - ドメイン名が本物と酷似したものを使用
  - SSL サーバ証明書を取得しているケースも



JPCERT/CC™

インシデント　ー　フィッシング（Phishing）

- フィッシング（Phishing）：
  - 大きな被害にあう可能性も
  - 金融機関も独自に対策を実施
  - 各ソフトウェアベンダより Phishing 防止策が提供され始めた

    Microsoft Enhances Phishing Protection for Windows, MSN and Microsoft Windows Live Customers
    http://www.microsoft.com/presspass/press/2005/nov05/11-17EnhancesPhishingProtectionPR.mspx
  - 世界的な法整備が遅れている。

インシデント動向　ー　情報流出

- 情報流出:
  P2P ソフトがインストールされた PC がワームに感染し、そこから機密情報が流出する事故が続発

  - 顧客情報、重要システム情報などが流出し、社会的問題になっている
  - 一旦情報が流出すると回収は事実上不可能
  - 社内ルールが規定されている現状でも、情報流出が後を絶たない

多種多様な製品の脆弱性

- 脆弱性が発見される製品が多様化し、今後も拡大していく
  - クライアントアプリケーションの脆弱性
    - MS IE, MS Office, セキュリティ対策ソフト（AV,FW） など
  - サーバアプリケーションの脆弱性
    - ウェブサーバ, 認証サービス, ライブラリ など
  - プロトコルの脆弱性
    - TCP/IP, IPSec、ISAKMP など
  - ネットワーク機器の脆弱性
    - ルータ, FW, IDS など
  - 情報家電、携帯情報端末の脆弱性
    - DVDレコーダ、携帯ゲーム機、携帯電話

攻撃の対象

- 広く汎用的に使われている
  - ICMP
  - DNS
- 使いやすく、機能がよい
  - MS Outlook
  - チャットサーバー (IRCサーバー)
  - P2P ファイル共有ソフトウェア
  - MS Internet Explore
- 良く使われるものは、裏返えされた時、非常に悪くも使われる。

次の脅威

- ホームユーザー
  - エンドユーザーが使うツールが、非常に複雑化
  - 環境：ハードウェアやネットワークが非常にパワフル化
    - 100,000ユーザーが、100Mbitのネットワークにつながっている状況
- ホームユーザーのマシン
  - きちんとしたシステム管理なし
  - インシデント対応なし
  - 適切なPCの知識なし

2. セキュリティ動向

DEFENCE IN DEPTH

- ユーザーを含めた多層防衛
  - 技術面では攻撃側と、防護側のいたちごっこが続く状況。
    - 情報を守るための、セキュリティオペレーションポリシーの見直しを行う
    - 企業では、情報管理者だけではなく、ユーザー全員のトレーニング、啓発が不可欠
    - ID、パスワードのみの1つの認証方法のみでなく複数を組み合わせる多段認証へ

経営トップの関与

- 経営トップが関与しないとインシデント対応しきれない。
  - 現場レベルではなく組織レベルでの対応が必須

- 組織CSIRTを構築する傾向
  - トップの関与は必須
  - インシデントに対応する際の、意思決定プロセスが事前に必要
    - インシデント対応には、様々な意思決定が、タイムリーに必要

開発段階からセキュリティを重視

- アプリケーション開発のためのセキュリティポリシー
  - 開発時に守るべきセキュリティポリシーの確立
  - 仕様変更の際にはセキュリティポリシーを侵害していないか確認する
- デバッグ機能の製品からの削除
  - コンソールポート、デバッグコマンドなどを製品には搭載しない
- セキュリティポリシーのレビュー
  - デバッグやテストのみでなく、セキュリティポリシーが侵害されていないことをレビューする

セキュリティ対策の主流

- 攻撃の技術的な進化と比例せず、技術的なセキュリティ対策は、昔からの一連の対策方法が主流。
  - 防御：ファイアーウォール、ウィルス対策ソフト
  - 検知：IDS
  - 脆弱性対応：製品を最新の状態にアップデートする パッチの適用
  - ポリシー：最小権限のポリシー

JPCERT CC™

セキュリティ対策の主流

- もう一度基本的な対策が実行できているか見直そう！
  - パッチの適用により、常に機器を最新の状態に
  - ウイルス対策ソフトウェアの導入
  - ブロードバンドルータ、ファイアウォールの導入
  - 不審な Web サイトの閲覧をしない
  - 不用意にメールの添付ファイルを開かない

３．重要インフラ防護の動き

重要インフラとは？

- 重要インフラとは、他に代替することが著しく困難なサービスを提供する、国民生活・社会経済活動の基盤となるもの。その機能の停止、低下によって多大な影響を及ぼすおそれが生じるもの

政府　情報セキュリティ基本問題委員会第2次提言（本体）
http://www.bits.go.jp/conference/kihon/teigen/pdf/2teigen_hontai.pdf

定義されている10の重要インフラ分野

[既存の7分野]

情報通信

鉄道

ガス

航空

金融

電力

政府・行政サービス

[追加3分野]

物流

水道

医療

JPCERT CC™

政府の取り組み

- 国内 情報セキュリティ対策体制
  - IT戦略本部（本部長：内閣総理大臣）に「情報セキュリティ政策会議」を設置
  - 下部委員会として以下の3つの専門委員会を設置
    - セキュリティ文化専門委員会
    - 技術戦略専門委員会
    - 重要インフラ専門委員会（2005年9月設置）

重要インフラ専門委員会

- 重要インフラ専門委員会は、

「ITの機能不全を引き起こすものから重要インフラを防護し、
取るべき対策の方向性を示すこと」

を目的として活動している。

主に以下の対策を検討している

- 分野横断的な状況把握（相互依存性解析など）
- 「安全基準・ガイドライン」の作成・評価
- 重要インフラ分野内での情報共有強化
- サイバーセキュリティ演習　　など

http://www.bits.go.jp/conference/seisaku/ciip/dai1/pdf/1siryou3.pdf

4．CSIRTコミュニティにおける動向

CSIRTコミュニティ

- FIRST：186 teams にメンバー増える
  SC – board directorとして貢献
  - **18th Annual FIRST Conference on Computer Security Incident Handling**
  - June 25–30, 2006 — Baltimore, Maryland, United States

- APCERT: 17チーム 14地域
  - APCERT AGM: March 28, 2006 ーBeijin

CSIRTコミュニティにおける動向

- ユーザー側へのセキュリティサポートを重点化
  - 早期警戒情報発信サービス
    - CSIRT間国際ネットワークを通して様々な情報が集約される：脆弱性情報、インシデント情報、トラフィックモニタリング情報
    - 集約される情報を分析して、早期警戒情報を発信
    - JPCERT/CCにおいても早期警戒情報発信サービスを開始
  - 経営トップへの働きかけ
    - 世界的なCIO、CEOフォーラムの傾向
    - FIRST：Corporate Executive Programme (CEP)
      http://www.first.org/conference/2005/cep/index.html
    - 2006年1月10日： アジアパシフィック CEPプログラム
      Hong Kong
    - http://www.globalcep.com/index.cfm?id_desc=H

JPCERT CC™

CSIRTコミュニティにおける動向

- ユーザー側へのセキュリティサポートを重点化　(続)
  - サイバーセキュリティ演習の実施
    - インシデント対応、情報ハンドリングの専門組織として、これまでの実績や経験を基に、シナリオを作成したり、演習実施の実働部隊として機能
    - JPCERT/CCにおいても、サービスを開始
  - 脆弱性プライオリティの仕様作成
    - 脆弱性のシステムに対する脅威度は、ユーザーによって違う
      - Know your system.
    - CERT/CC & JPCERT/CCにて、メトリック作成進めている

CSIRTコミュニティにおける動向 (2)

- インシデント対応の為の情報共有には、重層的な協力関係が必要
  - インシデント対応、脆弱性対応するには、様々なプレーヤーとの情報共有が必須
  - 特に機密性の高い情報共有の難しさ
    - 政府機関と、民間
    - 異なる機能層－CSIRT、政策決定者、法執行機関
    - 競争関係
    - 国際間
  - CSIRTは、コミュニケーションが難しい当事者同士、プレーヤー間の情報連携を橋渡しする役目を担ってきた。
- CSIRTコミュニティとして、通信事業者だけでなく、インフラ事業者、経営者層、ベンダ、政府、司法機関含めた、さまざまなプレーヤーとのネットワーキングをはじめている。

まとめ

- 攻撃側は組織化、巧妙化、複雑化
- ユーザー側の環境は、複雑化、強力化

- インターネットの保全は、全てのユーザー、プレーヤーの責任
  - CSIRT、製品開発者、ユーザー、システム管理者、政府、ISP、メディア

- ますます関係者間の連携が必要

お問い合わせ先

JPCERTコーディネーションセンター

- Email:office@jpcert.or.jp
- Tel:03-3518-4600
- http://www.jpcert.or.jp

- 伊藤友里恵
- Email: yito@jpcert.or.jp