国内外のフィッシング 傾向と対策

2007年5月28日　IAjapan 第4回 迷惑メール対策カンファレンス

小宮山 功一朗
早期警戒グループ　情報セキュリティアナリスト
JPCERTコーディネーションセンター

アジェンダ

1. オンライン詐欺事情
   - 株価操作SPAM (Pump and Dump)
   - 標的型攻撃
2. フィッシング
   - 国内の現状
   - 海外の現状
3. フィッシング傾向分析、対策
   - ボットを減らす（サイバークリーンセンター）
   - 電子署名

JPCERT/CC とは

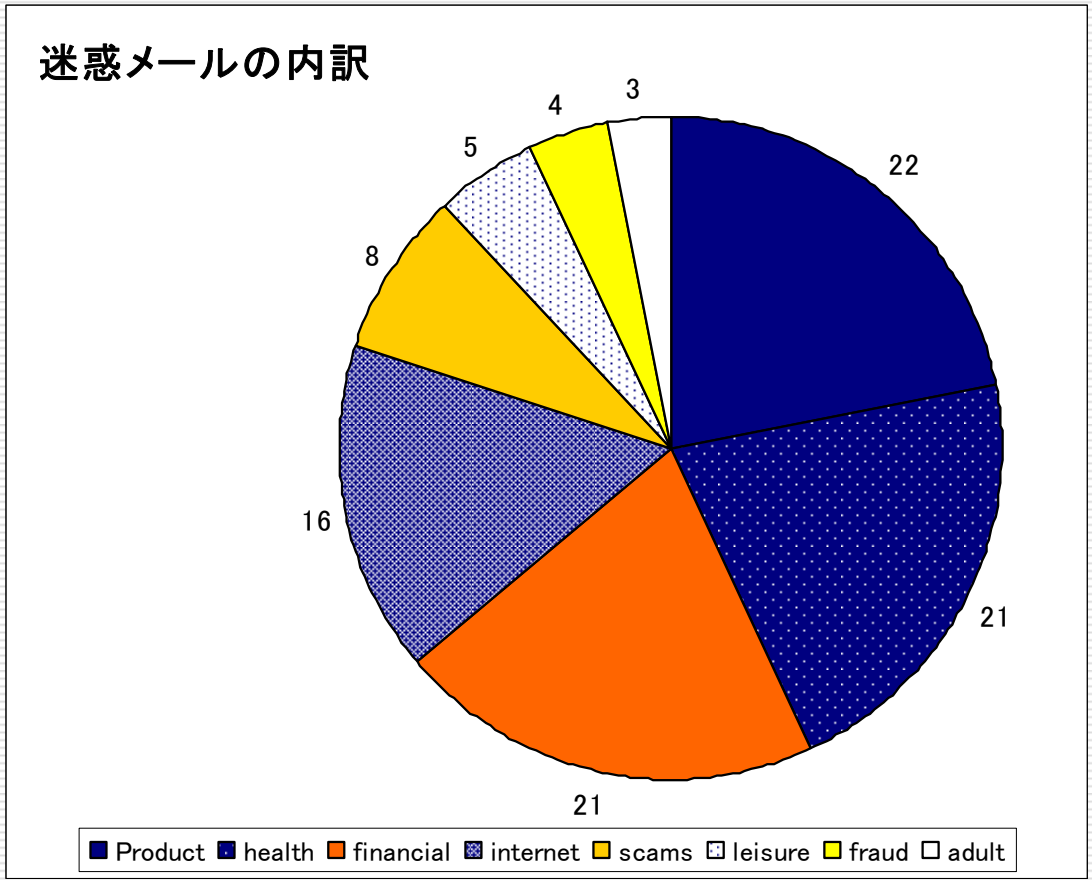
JPCERT コーディネーションセンター (**JPCERT/CC**) は、世界規模に進化するセキュリティインシデントに対応するため、我が国を代表する **CSIRT** (**Computer Security Incident Response Team**) として、国際連携、予防・対策・対処、モニタリングを行い、各国の **CSIRT** 活動の推進を支援しています。

JPCERT/CC の活動内容

	1996～	2003～	2004～	2005～	2006～
セキュリティ対応 体制の強化					**CSIRT構築支援** **ボットネット対策事業**
インシデント 発生前の予防				**早期警戒** （情報配信サービス、セキュリティ演習）	
リアルタイム 状況把握			**脆弱性情報ハンドリング**		
			インターネット定点観測		
インシデント 発生後	**インシデントハンドリング**				

1. オンライン詐欺事情

迷惑メールとその内容



Symantec “The state of Spam – A Monthly Report – May 2007”より

1. 株価操作、投資/ローンの勧誘
   → 21%
2. ナイジェリアからの手紙
   → 8%
3. フィッシング/トロイの木馬を
   → 4%

- 画像を使用した迷惑メールが3割以上

株価操作スパム (Pump and Dump)

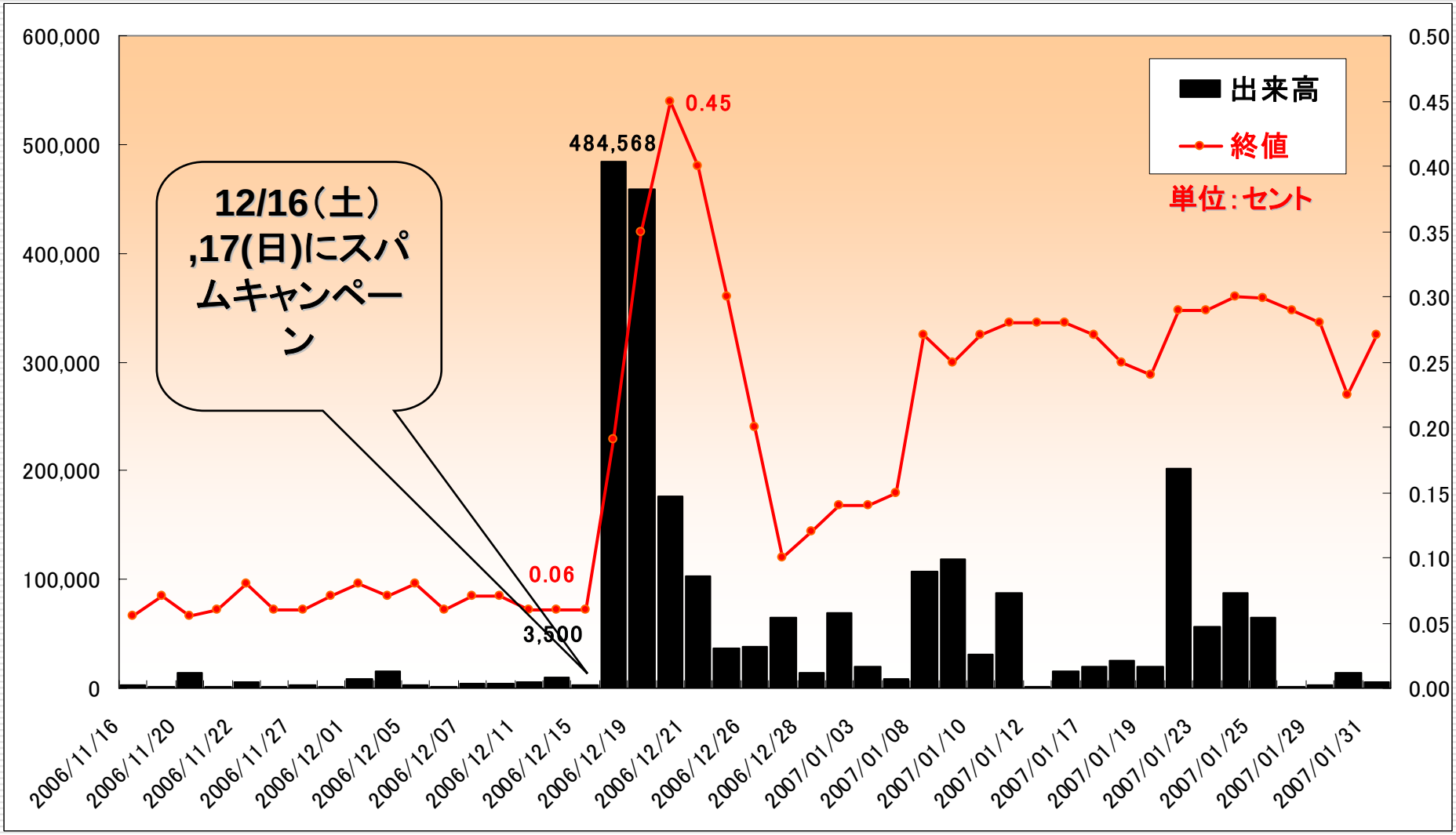
- 特定銘柄の株式を購入することを推奨するメールなどにより株価を不正につりあげた上で、自分が所有していた株式を売り抜ける行為。
- 2007年3月、米国証券取引委員会(SEC)により特定銘柄の取引が停止させられるという処置もとられた。

- 特徴
  - 狙われるのは米国のピンクシート銘柄とよばれる小規模の株式
  - 株価操作から売り抜けまでは長くて1ヵ月
  - 攻撃者の手に渡った金額は追跡困難

株価操作スパム ケーススタディ

- ケーススタディ:
  - 2006年12月15日金曜日
    - 株価は6セント 出来高3500株
    - 週末にSpamキャンペーンが 行われた
  - 2006年12月18日月曜
    - 株価は19セント出来高は484568株まで上昇した
  - 2006年12月20日
    - 株価は45セントを記録
  - 2006年12月27日
    - 出来高は65350株、株価は10セントまで下降した
  - 2007年3月8日
    - SECにより10営業日の取引停止処置

株価操作スパム　効果



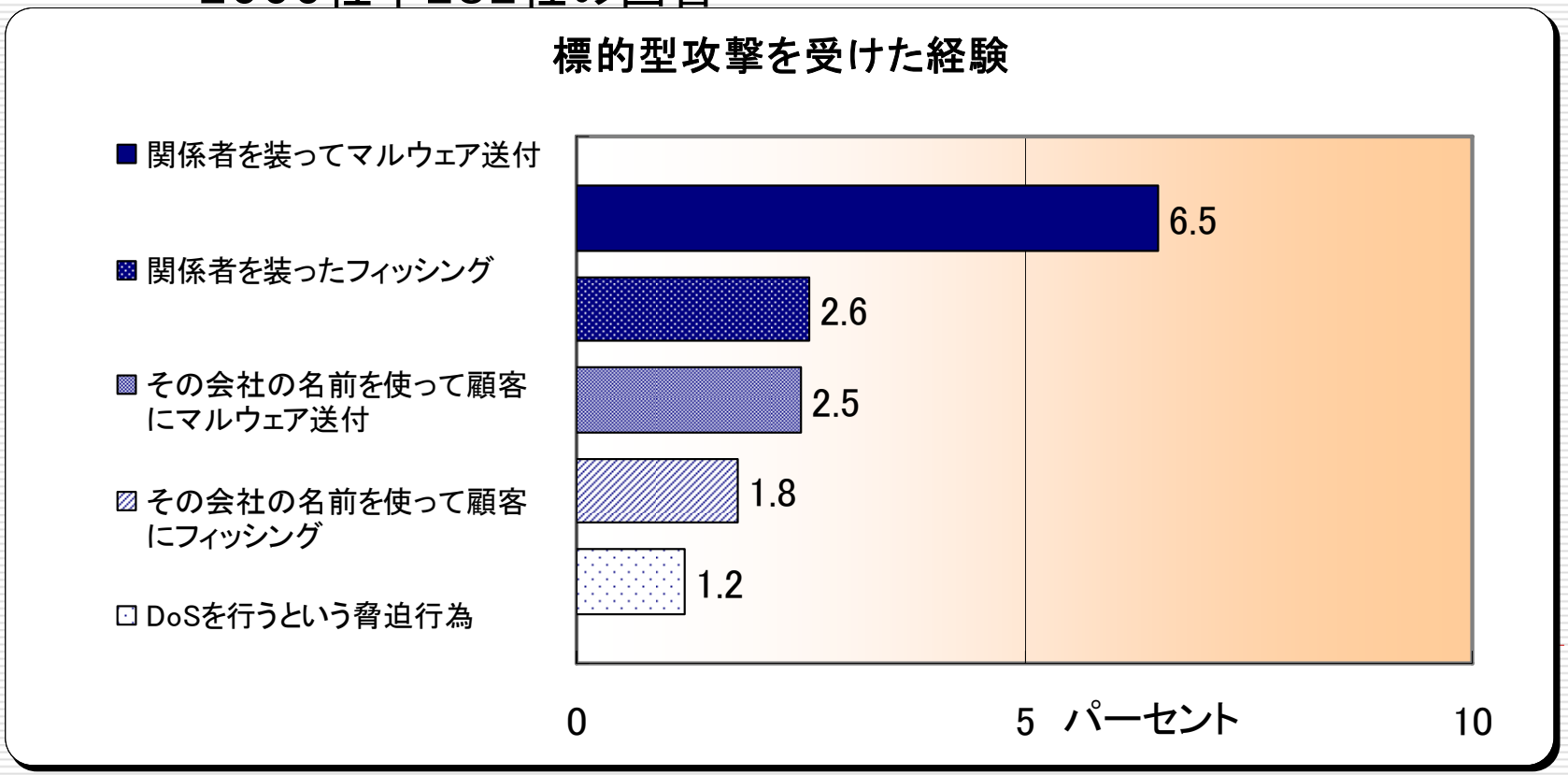
SEC公表資料より作成

標的型攻撃

- メール経由
  - 特定の組織あるいは組織グループに対して、
    - 「小泉首相靖国参拝」
    - 「対日AD情報」(注:アンチダンピング)
    - 「不祥事への対応について」
  - 手口
    - 攻撃サイトへのURLが付いている場合
    - マルウェアが添付されている場合
      (未修正の脆弱性を悪用することも)

アンケート ~ 被害の把握

- 2007/3 国内の企業/組織を対象にJPCERT/CCがアンケート調査を実施。
  - 2000社中282社の回答



2. フィッシング

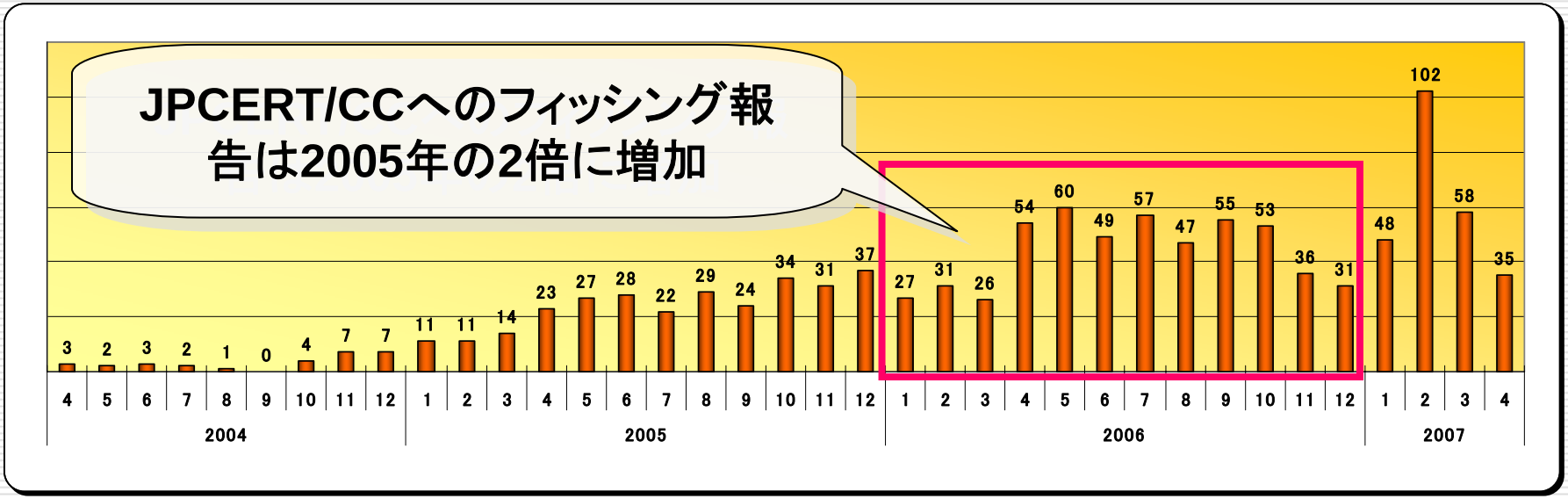
国内の現状 JPCERT/CCが把握しているもの

- フィッシング3つの被害
  - エンドユーザ：個人情報を詐取される、オンラインサービスを不正利用されることによる金銭被害
  - オンラインサービス事業者：ブランドイメージへの悪影響、エンドユーザの被害補てんのための費用
  - サーバ管理者：管理するサーバに侵入され、フィッシングサイトとして悪用される
- JPCERT/CCの対応
  - 2004年4月からコーディネーションを開始

管理者が意図していないページ公開の停止依頼

JPCERT/CCに寄せられる報告

- 国内のサーバが侵入されフィッシングサイトとして使用されるケースは増えている。



JPCERT/CCへの報告：2004/4 ~ 2007/4

国内金融機関を装ったフィッシングサイト

- 時期
  - **2007年3月**
- 被害にあったと報道されている企業
  - DCキャッシュワン、モビット、みずほ銀行、SMBC
- 特徴
  - .infoや.biz などのgTLDを使用している
  - 詐取された情報
    - 氏名、住所、メールアドレス、携帯電話番号
      口座番号やオンラインバンクのパスワード等は対象外
  - 東急ファイナンスを騙る

  フィッシングの標的となるのは金融サービス事業者だけではない

海外の現状

- 世界的な傾向

  被害の拡大

  - **米国でのフィッシングの2006年被害額が28億ドル**

    Gartner 調査（http://www.gartner.com/it/page.jsp?id=498245）
  - このような現状を受け、”phishing” はオックスフォード英語辞書に掲載されるほどにメジャーになった
- 送金などの手法が洗練されてきている
  - E-goldが起訴される(2007/4)
- ソーシャルエンジニアリング
  - 津波、ハリケーン、銃乱射事件
  - 悲劇の後にフィッシングあり

世界中に蔓延するフィッシング

- フィッシングにもお国柄が表れる
  - スペイン　– 宝くじ
  - 韓国 – オンラインゲーム
- 加害者は東欧やロシアの場合が多いとされている。
- 被害者がどこに通報すべきか明確でない。
  - 消費者保護団体(FTC)
  - シークレットサービス/FBI
  - 地方警察
  - CSIRT （JPCERT/CC, US-CERT, CPNI）
- ISPや企業の担当者の連絡先の把握が困難。そのためサイト閉鎖などの対応の初動が遅れる

スピア・フィッシングの脅威

フィッシング ＋ 特定の標的 = **スピアフィッシング**

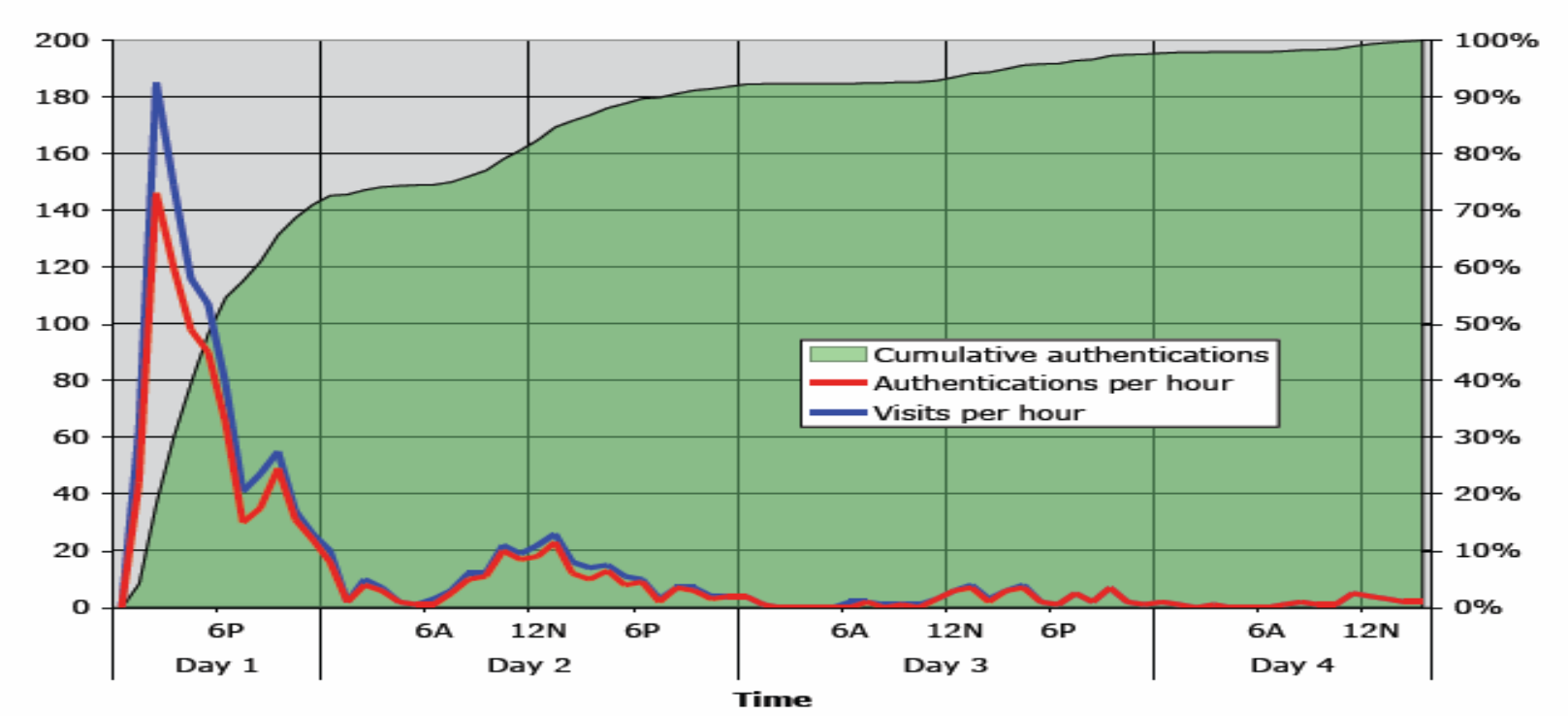
- SNS（myspace.com, facebook.com, ebay）

- インディアナ大学で2005年12月に行われた実験
  - 学生900名にフィッシングメールを送付
  - ソーシャルエンジニアリングを使うと攻撃成功率が4倍に

出典: Social Phising, Indiana University (Dec 12, 2005)
http://www.indiana.edu/~phishing/social-network-experiment/phishing-preprint.pdf

素早い対応が求められている

- 被害の70%は最初の12時間で起こっている



出典: **Social Phising, Indiana University (Dec 12, 2005)**
http://www.indiana.edu/~phishing/social-network-experiment/phishing-preprint.pdf

現状のまとめ

- 日本の企業・ユーザが堂々と狙われる時代に
  - 2007年3月の一連のインシデント
  - JPCERT/CCへの報告件数が2006年は前年比2倍
- 犯人の特定が困難
  - 組織的、計画的な犯罪
  - ロシア・東欧・(ブラジル・中国)
- 標的型攻撃(スピアフィッシング)の増加
- プロアクティブな対策、素早い対応が必要

フィッシング対策には**次の一手**が必要

これからのフィッシング対策を考える

- メール送受信と関連するもの
  - SPAM対策(OP25B)
  - 送信ドメイン認証
    SPF/Sender ID,DKIM
  - ボット対策（総務省・経済産業省 連携 サイバークリーンセンター ）
  - 電子署名技術の普及

対策：電子署名

- メールで顧客に連絡するオンラインサービスにおいてはS/MIMEの利用が効果的
- たとえば三井住友銀行は
  - 「平成18年5月22日（月）より、弊行が発信する電子メールに、電子署名をつけてお届けいたします。」と発表
  - 「署名されていないメール、警告が出るメールは信用しない」とアナウンス

対策：ボットを減らす

ボットは迷惑メール、フィッシングの発生源 そこで・・・

- サイバークリーンセンター プロジェクト
  - インターネットにおける脅威となっているボットの特徴を解析
  - ユーザのコンピュータからボットを駆除するために必要な情報をユーザに提供する
  - ISPの協力によって、ボットに感染しているユーザに対し、ボットの駆除や再感染防止を促す
  - https://www.ccc.go.jp/

対策のまとめ

- 受身のフィッシング対策から能動的な対策に切り替える必要がある
- 技術だけでは問題は解決しない
- オンライン詐欺全体への影響を意識
- 啓発活動の必要性は変わらない

JPCERT/CCは今後も関係各組織と協力の上、啓発活動を行ってまいります。

ご清聴ありがとうございました

- JPCERT/CCへのお問い合わせ
  - Email：office@jpcert.or.jp
  - Tel：03-3518-4600
  - http://www.jpcert.or.jp/
- インシデント報告
  - Email：info@jpcert.or.jp
  - http://www.jpcert.or.jp/form/