標的型攻撃対策：ITセキュリティ予防接種

2008年11月28日
Internet Week 2008 IP Meeting 2008

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

横浜市行政運営調整局 行政システム推進部 IT活用推進課
担当係長
山口 健太郎

INSTITUTE of INFORMATION SECURITY

標的型攻撃の現状

- 定義
  - 「情報セキュリティ上の攻撃で、無差別に攻撃が行われるものでなく、特定の組織あるいはグループを標的としたもの。攻撃対象となる組織あるいはグループに特化した工夫が行われることもある」
- 事例
  - 2007年
    - 6月下旬 Lhacaの脆弱性をつく「2007年度計画」
    - JICA台北オフィスを装いPowerpointの脆弱性をつく標的型攻撃。件名は「台湾情勢について」
  - 2008年
    - IPAを騙り、関係機関に細工されたPDF文書を送付
    - 情報処理学会コンピュータセキュリティシンポジウムの論文募集を騙ったウィルスメール
- 関連機関の調査結果
  - “6.4%が過去1年間に標的型攻撃を受けている”
    JPCERT/CC（有限責任中間法人JPCERTコーディネーションセンター）「標的型攻撃についての調査」（2007）
  - “標的型攻撃の電子メールを受けとった経験（発見または被害）のある組織は7.9%”
    IPA「2007年 国内における情報セキュリティ事象被害状況調査」
  - おそらく氷山の一角

標的型攻撃増加と予防接種

標的型攻撃対策の難しさ

- 対策の種類については、配付資料の付録1をご参照下さい

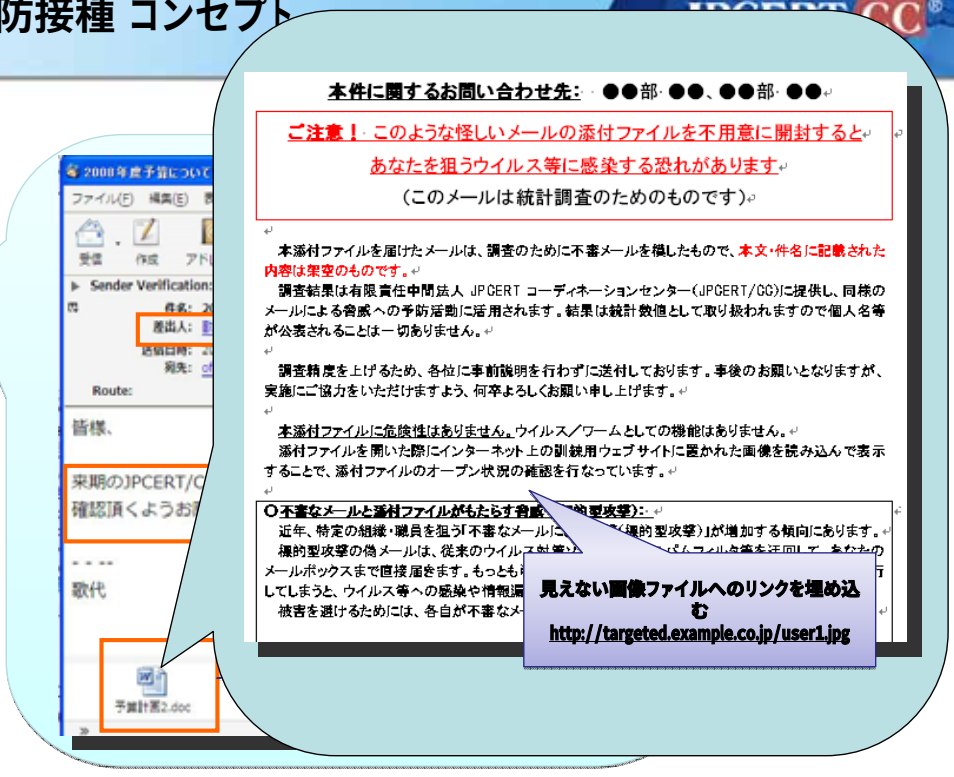
ITセキュリティ予防接種とは

- 電子メールを用いた受動型攻撃に対するエンドユーザのセキュリティ意識の向上を目的とする調査･訓練の手法で、対象者に不審メールを模した無害なメールを送付し、適切な取扱いを行えるかを試すものである。

プロジェクトの目的

- 標的型攻撃対策としての予防接種の有効性を確認する。
- 安全に実施するための手法を確立する。

ITセキュリティ予防接種 コンセプト



全体の流れ

JPCERT CC®

調整(文面の設定、リハーサル)

ユーザへの事前教育

・怪しいメールの条件、取るべき対応、問い合わせ窓口などを事前に教育。被験者によっては省略

予防接種 一回目

予防接種 二回目 (約2週間の間隔)

被験者への趣旨説明/アンケートの依頼

ケーススタディ: 横浜市役所

JPCERT CC®

1回目の開封者
146名/482名
30%

→

2回目の開封者
110名/482名
23%

意図をもって開封した場合などもあるためアンケートを実施

2通のメールを経験した186名中何らかの意識変容を感じた者

→

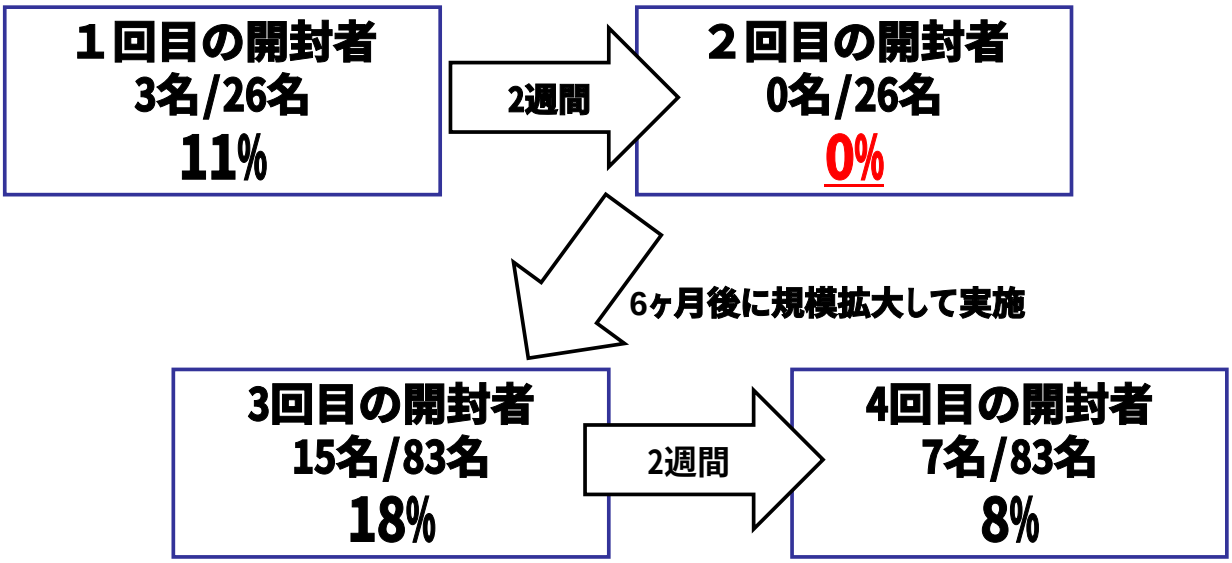
137名
(73%)

1. 予防接種は確かに効果があった。開けたとしても、意識が変わった人が多い
2. しかし実施の詳細については、さらなる検討が必要。

ケーススタディ: ITセキュリティ関連企業 A社

JPCERT CC®

- 合計4回実施



まとめ

JPCERT CC®

- 多くの企業において、低コストで
  - 開封率が減少
  - セキュリティインシデントの実体験、経験 (≠知識)
  - セキュリティ教育の効果測定
  - ユーザのセキュリティや社内ルールに対する意識の変化

  などの効果をもたらした

- 最終レポート(2008/3末)に請うご期待!
  - 現在合計1000人～2000人規模での統計データと実施ノウハウを公表予定
  - 情報処理学会で発表予定
- **ありがとう Internet Week**

Internet Week 2008のコンセプト

「インターネットコミュニティにおける『人との連携』を促進」

IT技術の高度細分化が進む現在、自分の周りの純粋な技術だけで解決こで、開催12回目を迎える今年は、「インターネットコミュニティに題解決への糸口を、少しでも多く提示したいと考えています。

付録1: 3つの側面からの標的型攻撃対策

攻撃を判別する技術的対策	被害を最小範囲に留める仕組み	ユーザ教育
攻撃とそうでないものを判別するのを手助けする技術的な方策	攻撃が成功した場合にその被害を限定的にするために。	ユーザー人一人が攻撃に気づき、危険を避け、情報を報告･共有するために。
• 送信ドメイン認証 SPF/Sender ID, DKIM • メッセージ署名 S/MIME, PGP • 拡張子による添付ファイルの制限	•オフィス文書の無害化 Microsof Office 2007 , MOICE • 最新のプログラムを使う (Windows Vista) • ファイルを開く専用マシン •通信の監視、認証プロキシ	•“不審な”メールの見分け方 • 集合研修 • Eラーニング • **予防接種**