

# 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イルスメール

### ■ 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

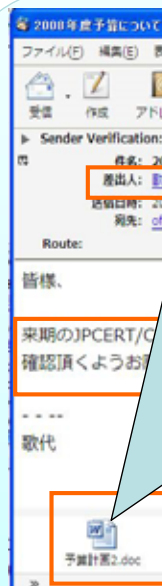
### ■ ITセキュリティ予防接種とは

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



本件に関するお問い合わせ先: ●●部●●●●部●●●●

**ご注意!** このような怪しいメールの添付ファイルを不用意に開封すると  
あなたを狙うウイルス等に感染する恐れがあります。  
(このメールは統計調査のためのものです)

本添付ファイルを開いたメールは、調査のために不審メールを模したもので、本文・件名に記載された内容は架空のもので、調査結果は有限責任中間法人 JPCERT コーディネーションセンター(JPCERT/CC)に提供し、同様のメールによる脅威への予防活動に活用されます。結果は統計数値として取り扱われますので個人名等が公表されることは一切ありません。

調査精度を上げるため、各位に事前説明を行わずに送付しております。事後のお問い合わせは、実施にご協力をいただけますよう、何卒よろしくお願い申し上げます。

本添付ファイルに危険性はありませんが、ウイルス/ワームとしての機能はありません。

添付ファイルを開いた際インターネット上の訓練用ウェブサイトに置かれた画像を読み込んで表示することで、添付ファイルのオープン状況の確認を行なっています。

○不審なメールと添付ファイルがもたらす脅威(標的型攻撃):  
近年、特定の組織・職員を狙う「不審なメール」による「標的型攻撃」が増加する傾向にあります。標的型攻撃の偽メールは、従来のウイルス対策ソフトで検出されず、添付ファイルを開いてあなたのメールボックスまで直接届きます。もっとも、添付ファイルを開いた際インターネット上の訓練用ウェブサイトに置かれた画像を読み込んで表示してしまうと、ウイルス等への感染や情報漏洩被害を避けるためには、各自が不審なメ

見えない画像ファイルへのリンクを埋め込む  
<http://targeted.example.co.jp/user1.jpg>

## 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)

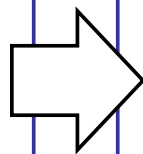
被験者への趣旨説明/アンケートの依頼

Copyright© 2008 JPCERT/CC All rights reserved.

## ケーススタディ: 横浜市役所

JPCERT CC®

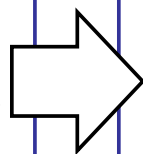
1 回目の開封者  
146名/482名  
30%



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

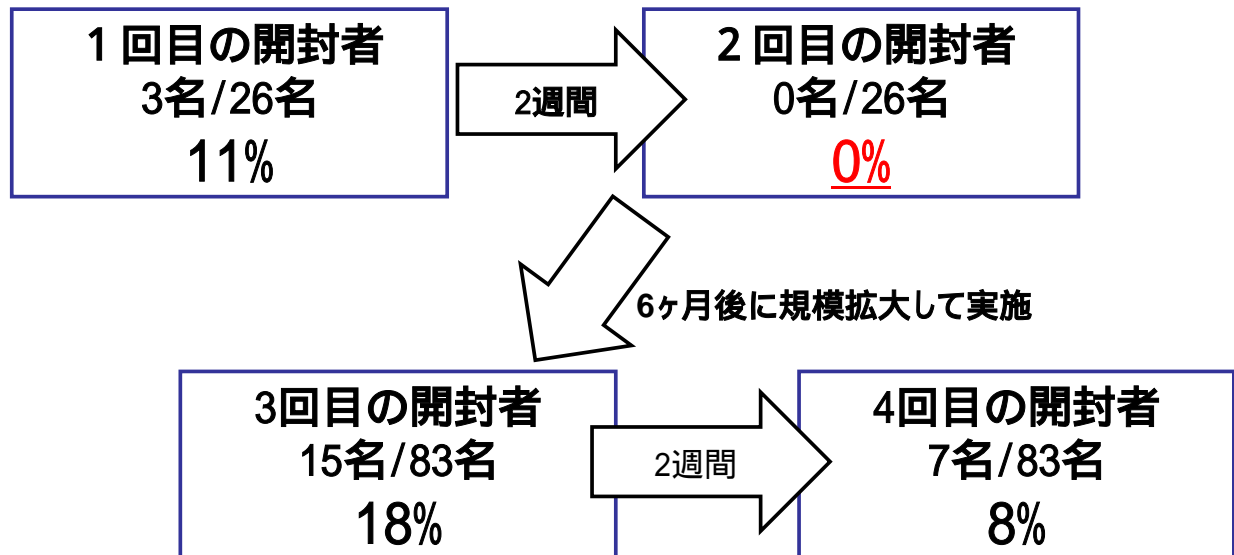


137名  
(73%)

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。

Copyright© 2008 JPCERT/CC All rights reserved.

■ 合計4回実施



Copyright© 2008 JPCERT/CC All rights reserved.

まとめ

- 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  
まで、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。

Copyright© 2008 JPCERT/CC All rights reserved.

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。	ユーザー一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。
<ul style="list-style-type: none"> <li>• 送信ドメイン認証 SPF/Sender ID, DKIM</li> <li>• メッセージ署名 S/MIME, PGP</li> <li>• 拡張子による添付ファイルの制限</li> </ul>	<ul style="list-style-type: none"> <li>• オフィス文書の無害化 Microsoft Office 2007, MOICE</li> <li>• 最新のプログラムを使う (Windows Vista)</li> <li>• ファイルを開く専用マシン</li> <li>• 通信の監視、認証プロキシ</li> </ul>	<ul style="list-style-type: none"> <li>• “不審な”メールの見分け方</li> <li>• 集合研修</li> <li>• Eラーニング</li> <li>• <u>予防接種</u></li> </ul>