

標的型メール攻撃対策 ～ITセキュリティ予防接種による組織の防御力強化～

2009年2月20日

重要インフラ情報セキュリティフォーラム 2009

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

■ 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(以後予防接種)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

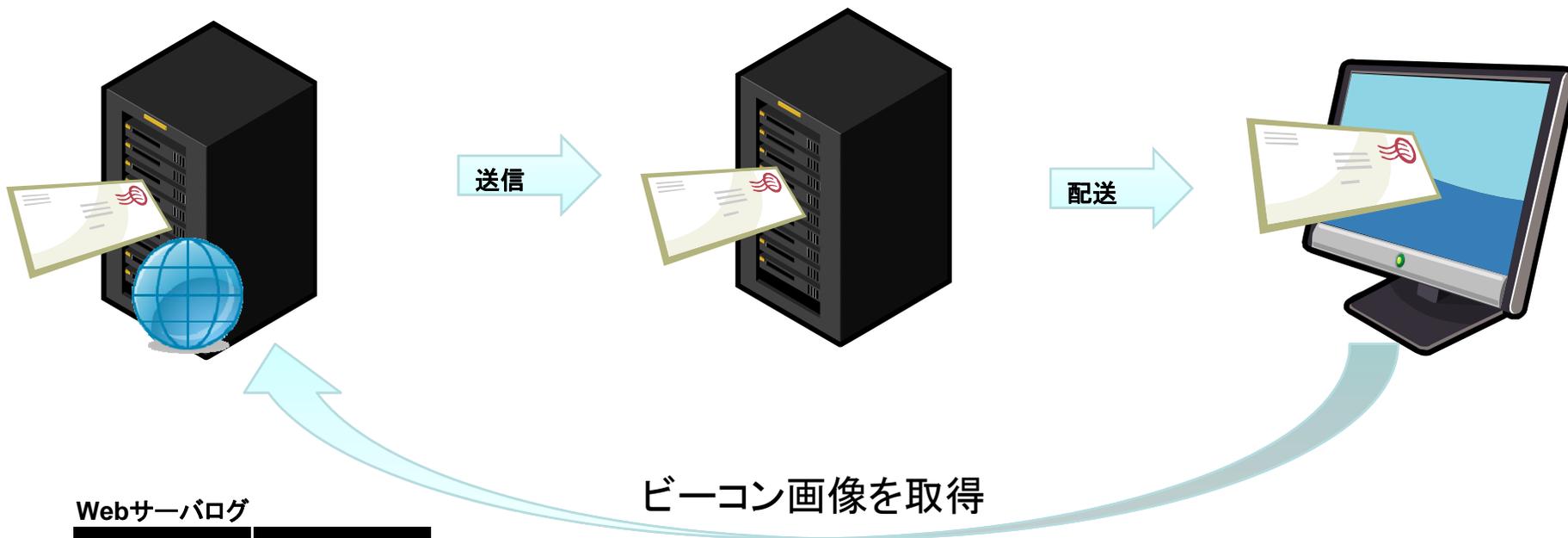
- － 標的型攻撃対策としての予防接種の有効性を確認する。
- － 予防接種を安全に実施するための手法を確立する。

作業のイメージ

JPCERT/CC

各協力企業

被験者



Webサーバログ

アクセス日 時	画像番号
2/2 13:00	A01.bmp
2/2 13:08	B32.bmp

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・●●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)

本添付ファイルを届けたメールは、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**す。

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。事後のお願いとなりますが、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。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に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は検出されず、パソコンを迂回してあなたのメールボックスまで直接届きます。もっとも、開封してしまうと、ウイルス等への感染や情報漏洩の恐れがあります。被害を避けるためには、各自が不審なメールを見つけたら、すぐに削除し、開封しないことが重要です。

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

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

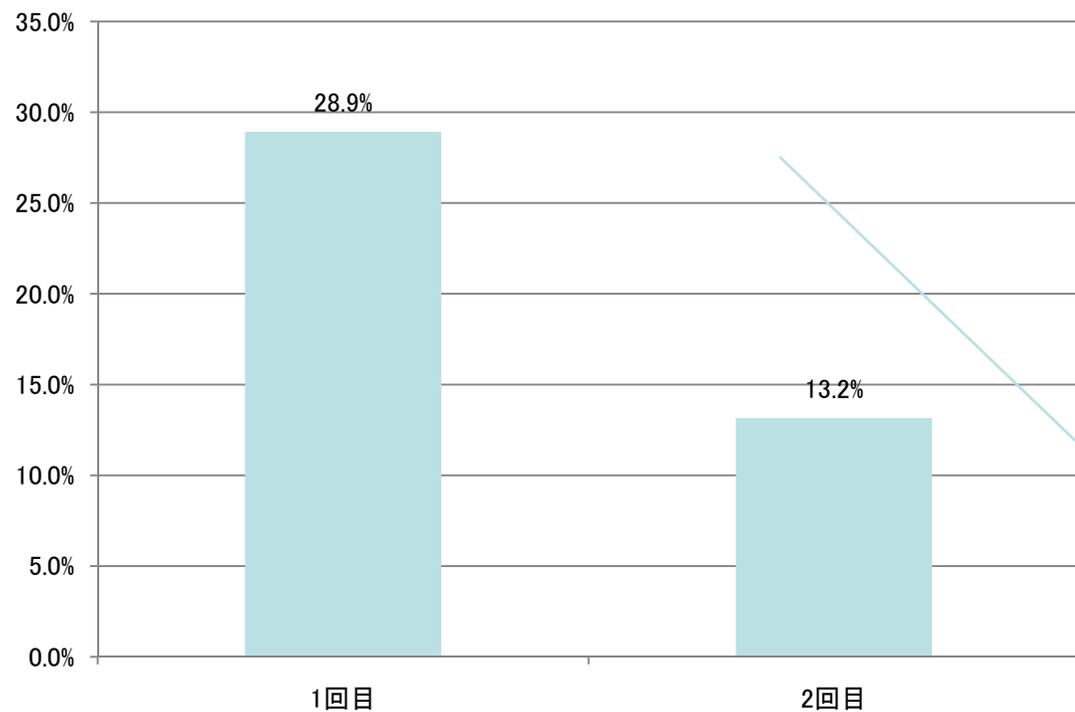
予防接種 一回目

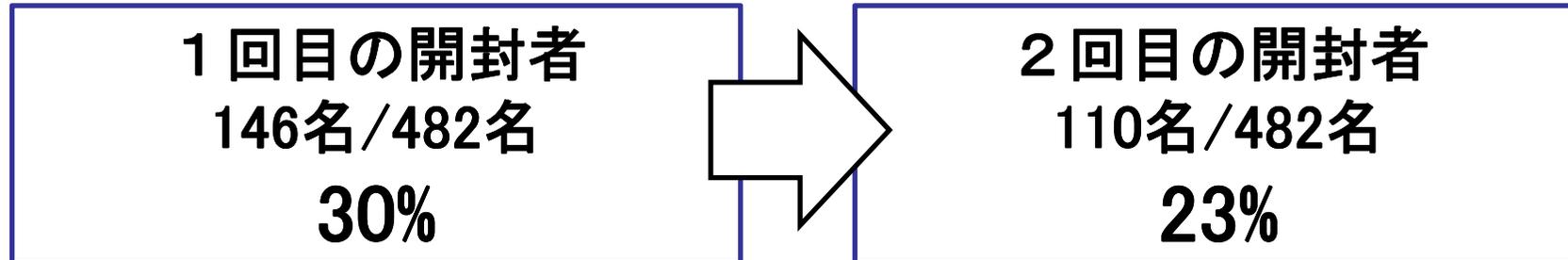
予防接種 二回目 (約2週間の間隔)

被験者への趣旨説明/**アンケートの依頼**

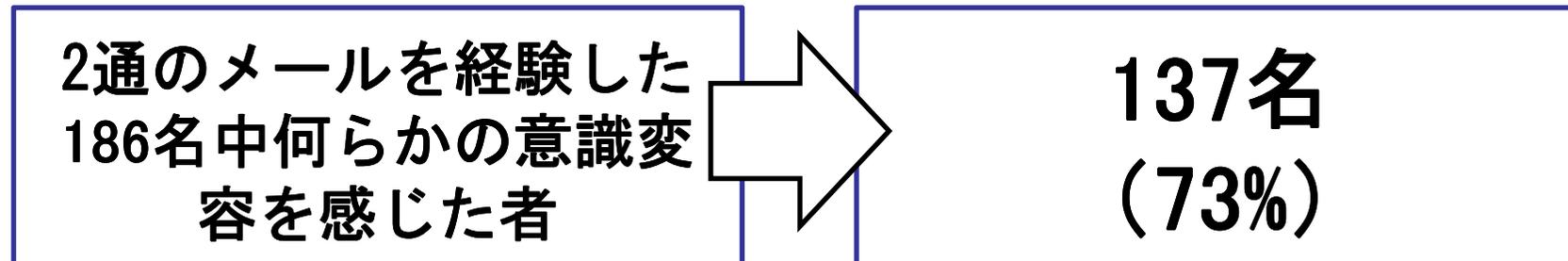
分かったこと

- お断り: 以下の集計は全て暫定的なものです。2009/4公開予定の調査報告書とは内容が異なる可能性があります。
- 14組織、延べ2600名への予防接種実施の実績から分かったこと。



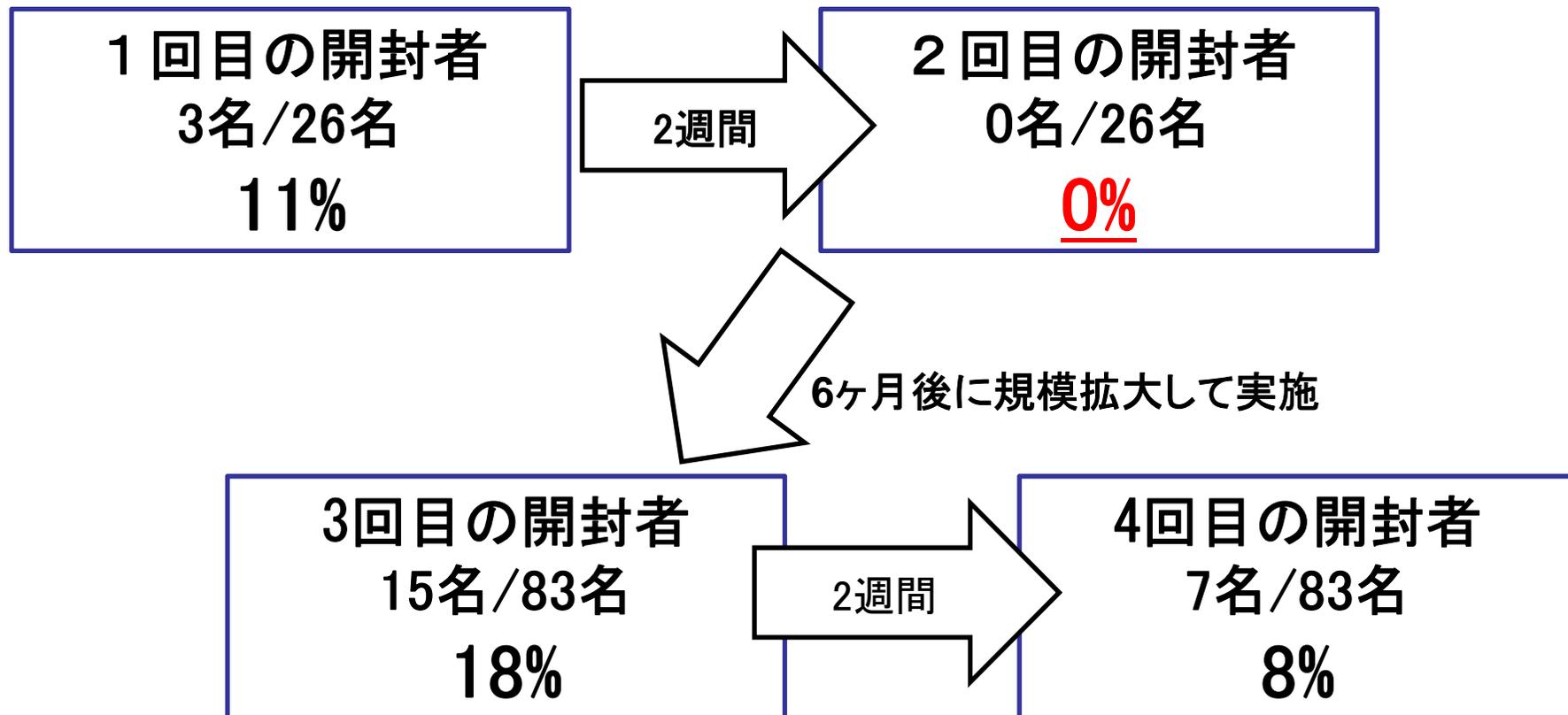


意図をもって開封した場合などもあるためアンケートを実施

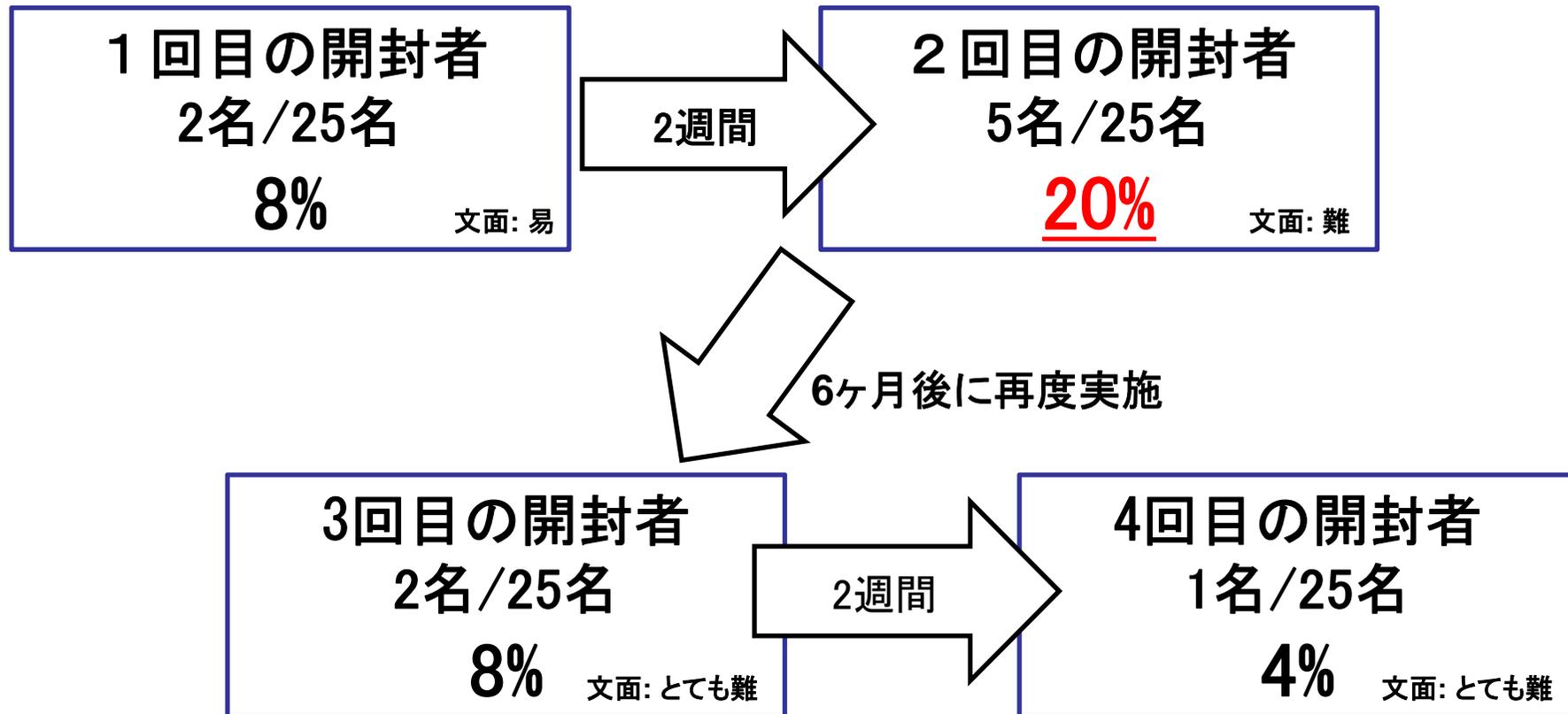


1. 予防接種は確かに効果があった。開けたとしても、意識が変わった人が多い
2. しかし実施の詳細については、さらなる検討が必要。

■ 合計4回実施



■ 合計4回実施



とても易しい文面

件名: 報道発表について
差出人: 広報 高橋 <motok2501@gmail.com> ①
送信日時: 2008/12/09 21:15
宛先: 小宮山 功一朗
Route: \$. . . \$

皆様
②
広報の高橋です。お世話になります。

本日午後3時、新サービスのプレスリリース（報道発表）を行いますので、
お問い合わせ対応等、宜しくお願い致します。
* 午後3時以降にHPで閲覧できます。

プレスリリース内容の詳細については添付ファイル参照


新サービスプレス.doc

- ① アドレスがフリーメール
- ② 架空の人物/部署

とても難しい文面

件名: 実験台募集 (12月16日のMicrosoftセキュリティ情報の検証)
差出人: JPCERT/CC 再現検証班 <office@jpcert.or.jp>
送信日時: 2008/12/05 13:00
宛先: 小宮山 功一朗
Route: ● ● ● ●

①

社員各位:

②

先日公表された2008年12月度の Microsoft 社のセキュリティ情報について
検証環境が不足しています。
恐縮ですが、みなさんのお使いになっている PC で再現試験をお願いできれば
助かります。

MS08-78 は「Microsoft Office の脆弱性により、任意のコードが実行される」
というもので、あるシーケンスにしたがって Microsoft Excel を操作するこ
とによって制限ユーザから特権ユーザへの権限昇格が可能となるものです。
具体的な手順を添付ファイルに示しますので、お手元の環境で実際に権限昇格
が可能か否かを実験してください。

手順書の末尾に結果報告用のシートがありますので、これに記入後
patchtesters@jpcert.or.jp まで返送をお願いします。

③

お忙しいところをすみませんが、よろしくお願ひします。

再現検証班



MS08-78_検証手順.doc

- ① 存在しない部署
- ② 時期が違う
- ③ 存在しないメールアドレス

- 実施は早ければ数時間で種明かし
 - － メール依存度が高い業種では、最初の1時間でほとんどの人がメールを確認する。
- 開封率は下がる
- 社内での連絡体制が機能しないことがある
- 技術的な改良の余地
 - － スпамフィルター対策
 - － 文字化け
 - － 一括大量送信

- 多くの被験者は予防接種を前向きに受け止めている
 - － 「全社で実施を」「定期的な実施を」望む声多数
 - － 予防接種の意義を理解してもらうためには教育が必要
- アンケートをしないと真の開封率は分からない
 - － メールを見ていない人
 - － リスクを承知で敢えて開いた人
- 「管理者への連絡」に抵抗を感じている
 - － 「こんなことで忙しいIT部門の手を煩わせたくない」
- 「新人さん」は予防接種に弱い
 - － 業務知識の不足
 - － 教育が不十分
 - － 来たメールを全て確認しようとする

- 予防接種は
 - 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
- 今後の課題
 - － ゴールは開封率0%ではない
 - － 事前事後の教育が大切
 - － メール文面の難易度設定に一定のガイドラインを
- 最終レポート(2008/3末)に請うご期待!



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

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

- 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

被害を最小範囲に留める仕組み

攻撃が成功した場合にその被害を限定的にするために。

- オフィス文書の無害化
Microsoft 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

ユーザ教育

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。

- “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

お問い合わせ、インシデント対応のご依頼は

JPCERT **CC**®

■ 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/>