
# 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

# 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

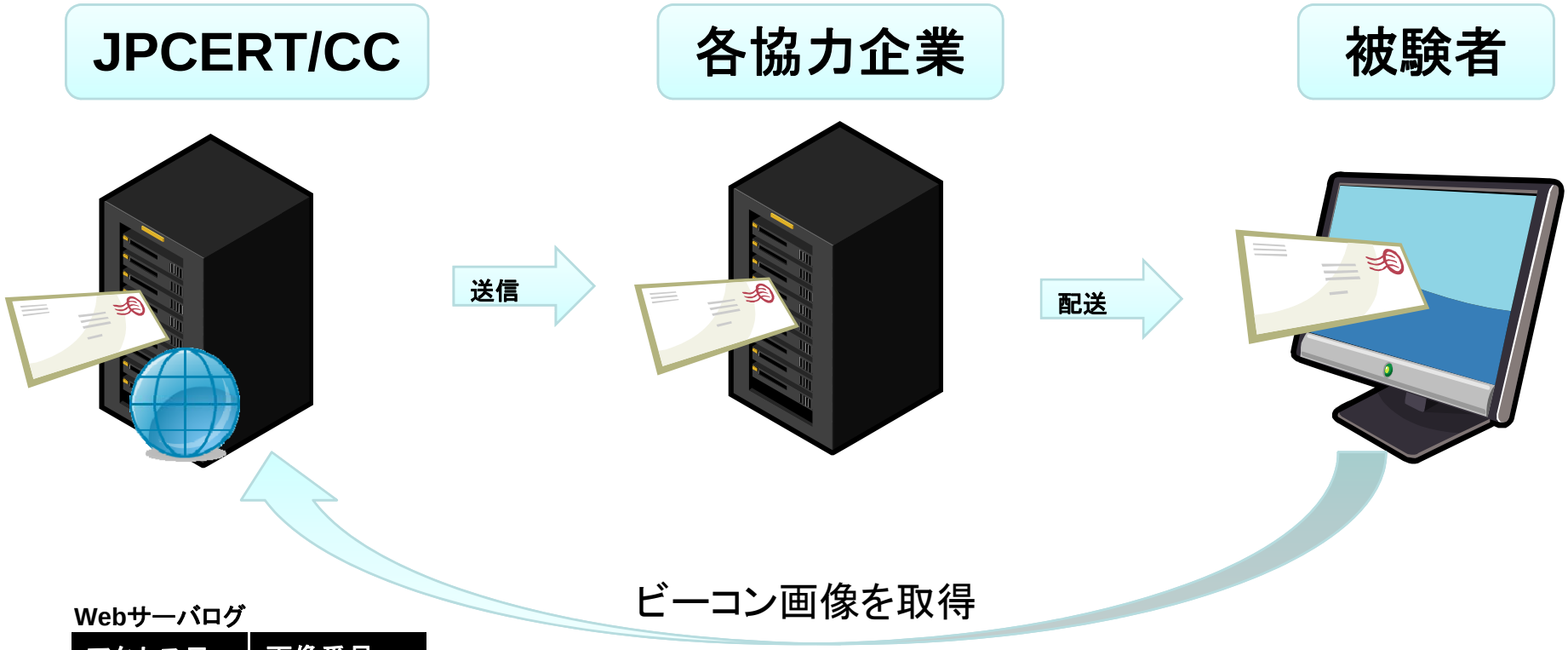
# 標的型攻撃増加と予防接種

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(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。

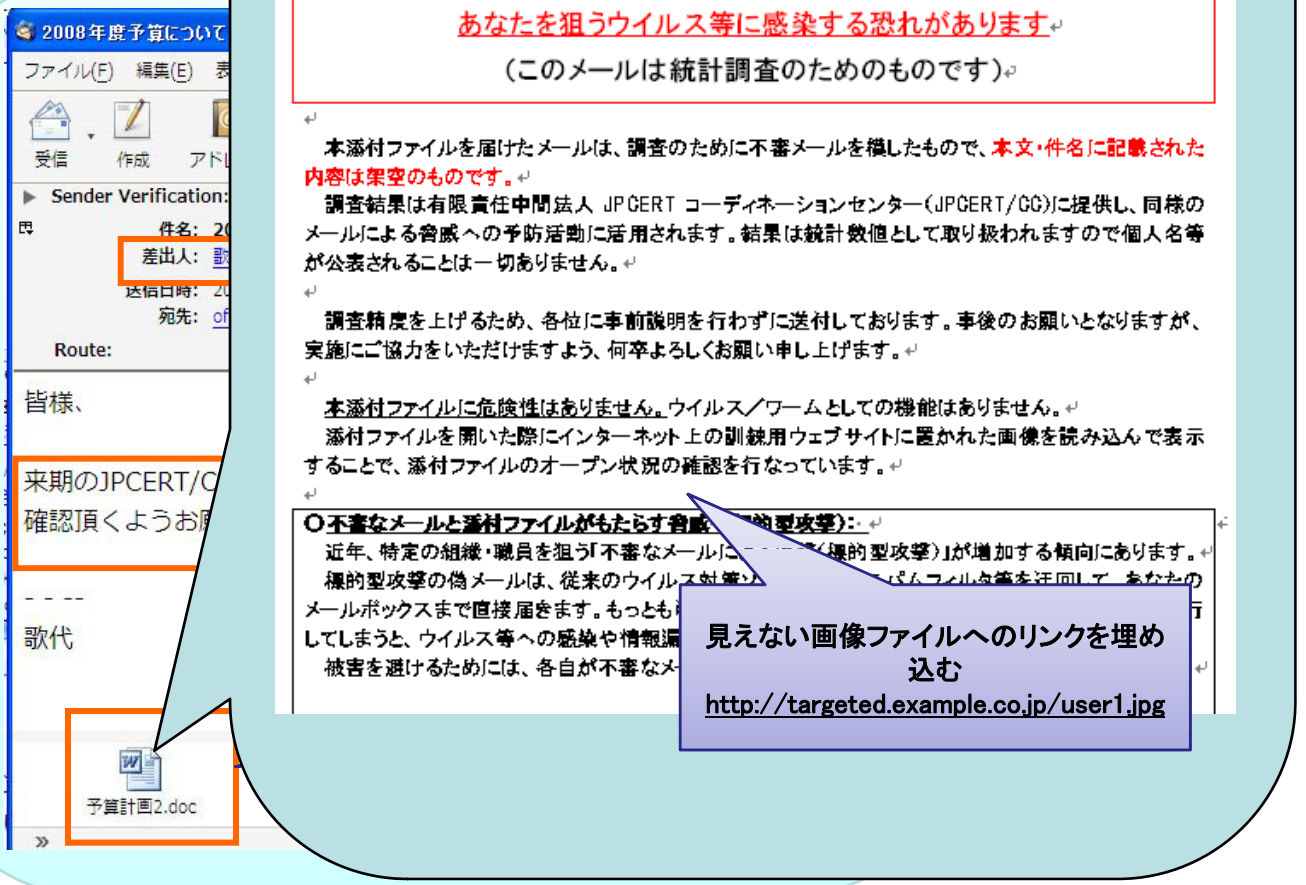
# 作業のイメージ




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



# 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

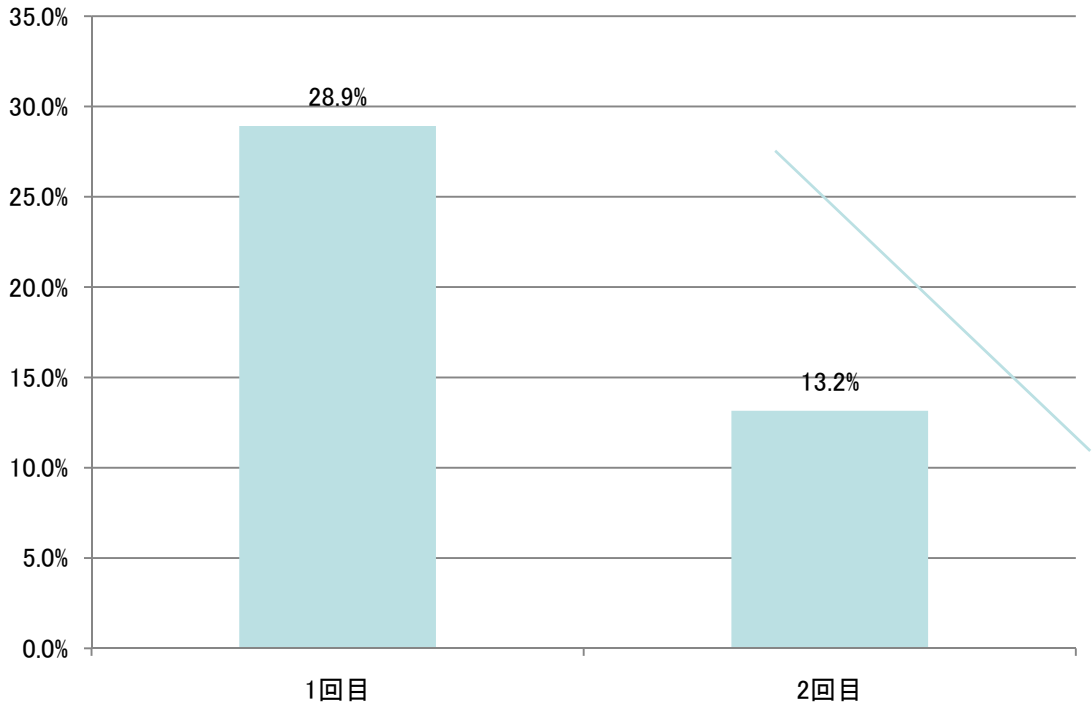
予防接種 一回目

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。



# ケーススタディ: 横浜市役所

| １回目の開封者 | ２回目の開封者 |
| --- | --- |
| 146名/482名 | 110名/482名 |
| 30% | 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

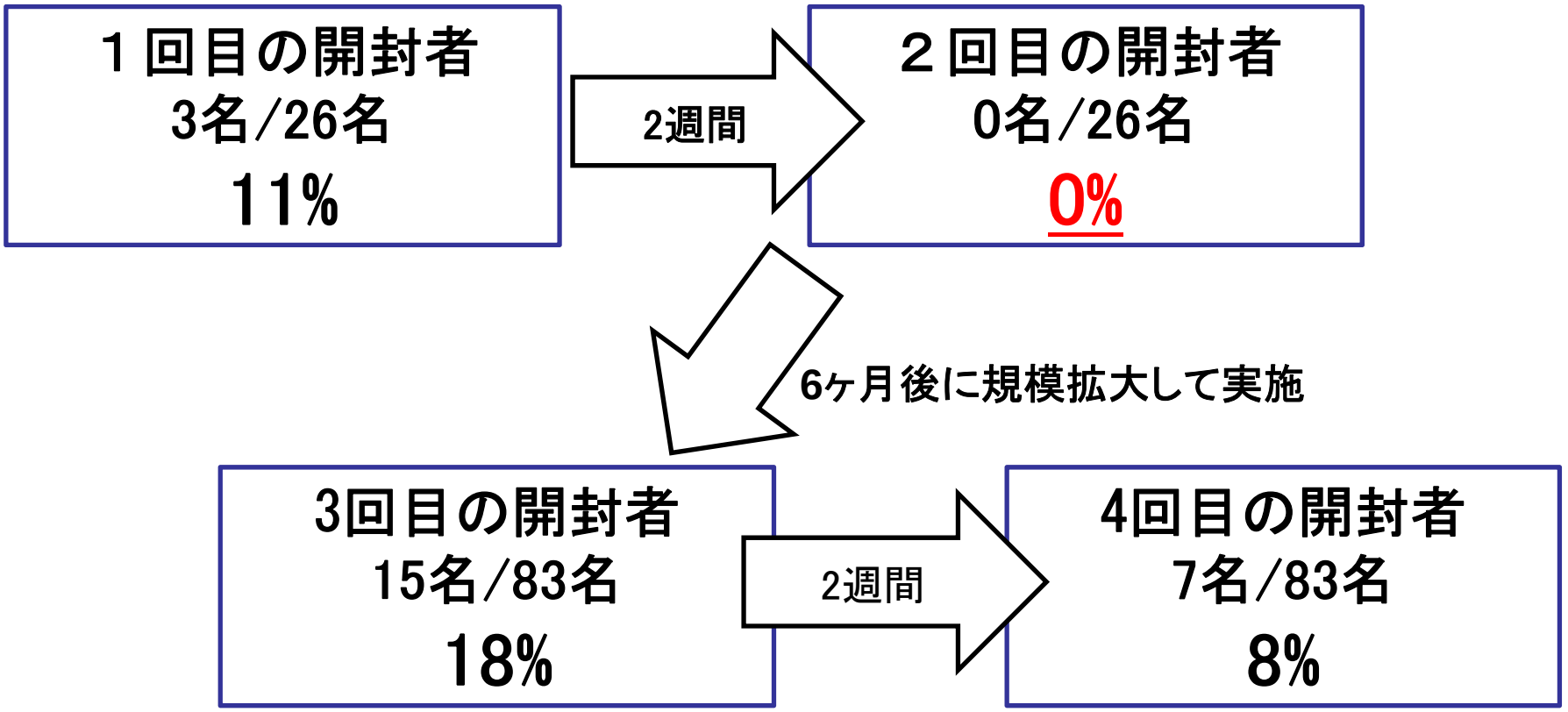
| 2通のメールを経験した186名中何らかの意識変容を感じた者 | 137名（73%） |
| --- | --- |

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®

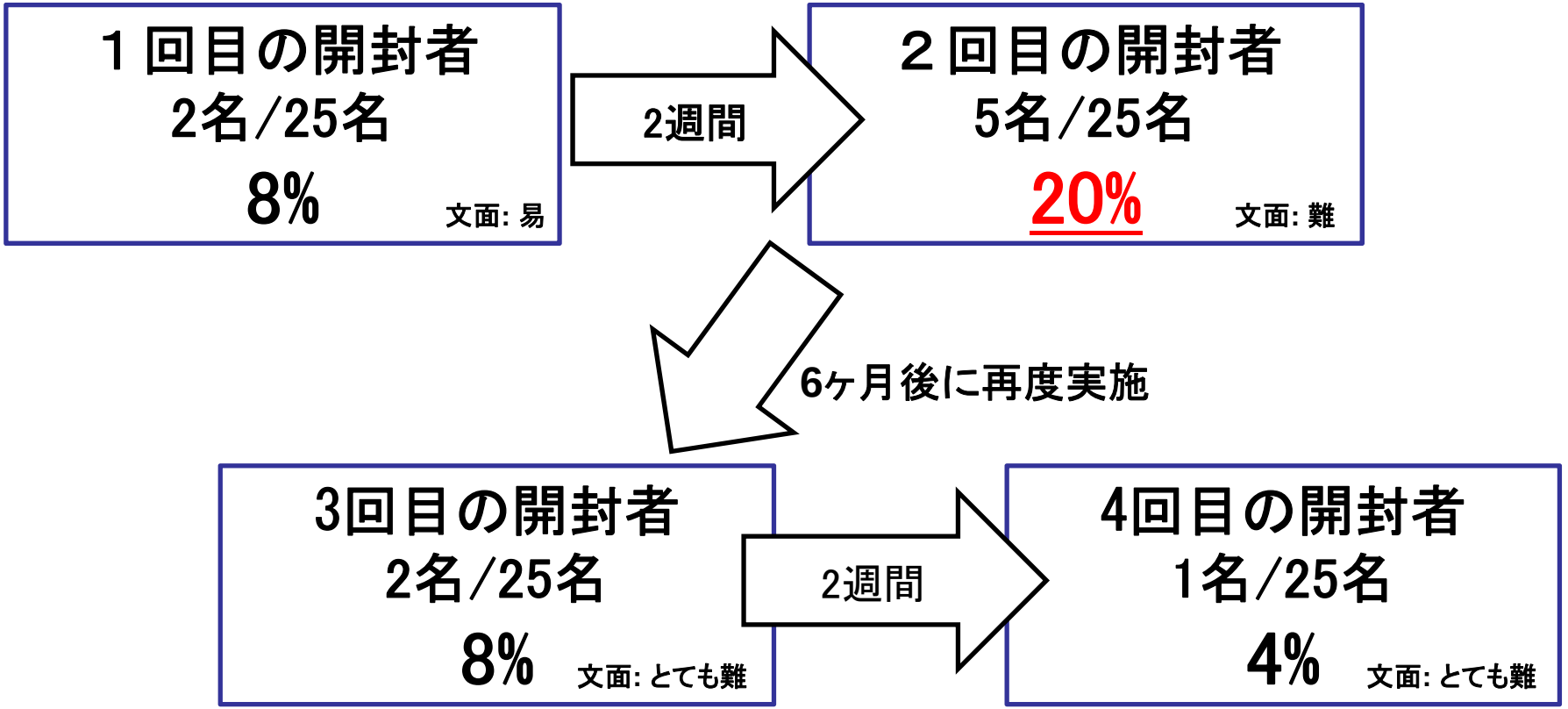
- 合計4回実施



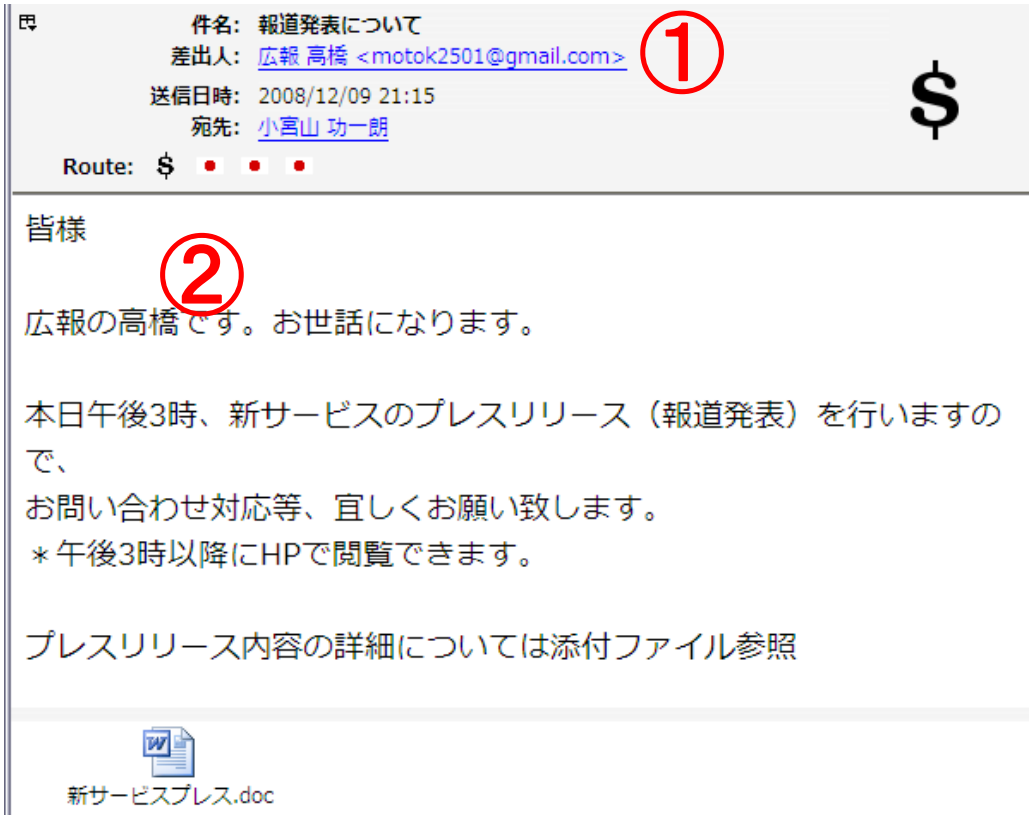
# ケーススタディ JPCERT/CC

JPCERT CC®

■ 合計4回実施



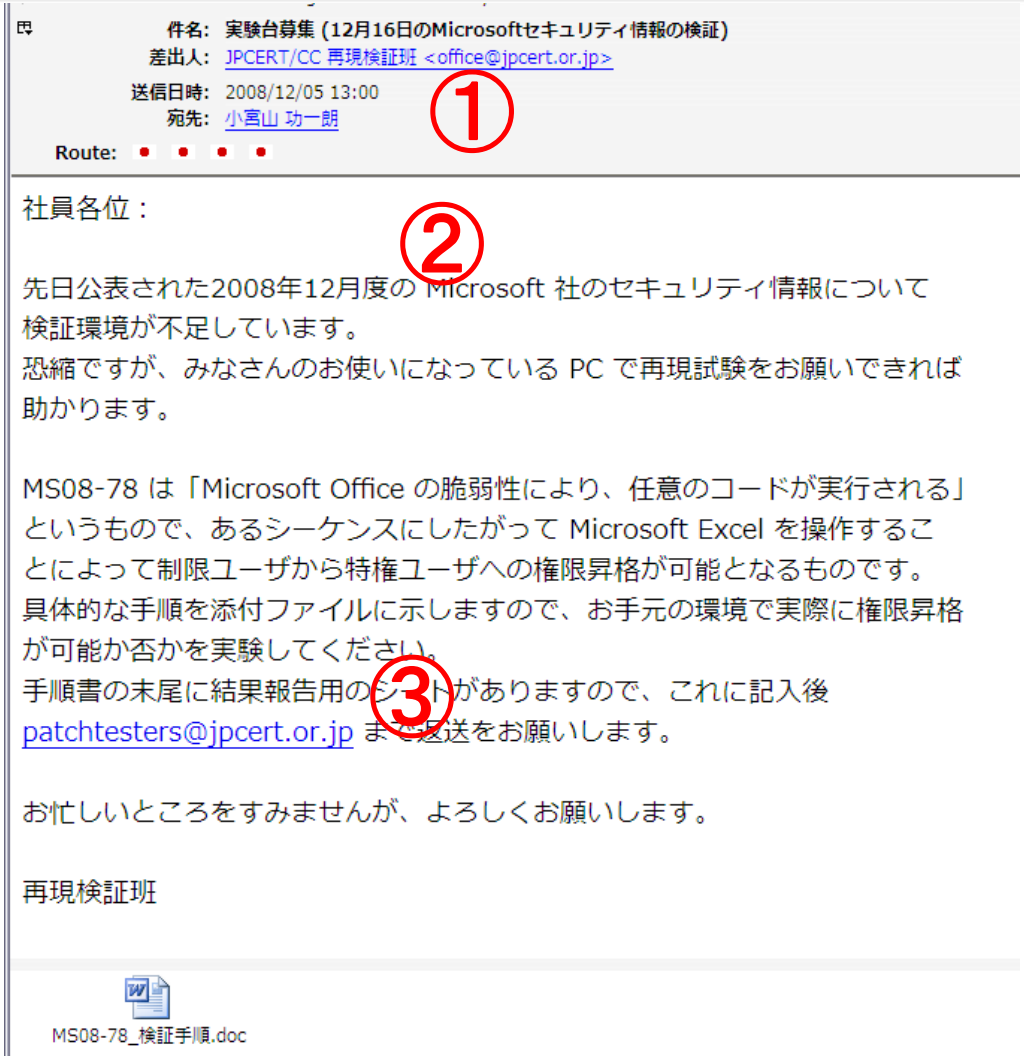
# とても易しい文面




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、よろしくお願いします。

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

# 予防接種の結果からわかったこと

- 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
  - スパムフィルター対策
  - 文字化け
  - 一括大量送信

# アンケートから分かったこと

- 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

# まとめ

- 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 | 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<br>• メッセージ署名 S/MIME, PGP<br>• 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<br>• 最新のプログラムを使う (Windows Vista)<br>• ファイルを開く専用マシン<br>•通信の監視、認証プロキシ | •“不審な”メールの見分け方<br>• 集合研修<br>• Eラーニング<br>• 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/