

# 国内外の最新動向とJPCERT/CCの取り組み

2008/1/30 「ID盗難・フィッシング詐欺の動向と対策」セミナー 於三田共用会議所

有限責任中間法人

JPCERT コーディネーションセンター

小宮山 功一郎

# 内容

---

- JPCERT/CCとは
  - 組織の概要
  - フィッシング対策の分野でのJPCERT/CCの取り組み
- 日本のフィッシングの現状
  - 未だ主流は”振り込め詐欺”
  - JPCERT/CCへの依頼方法
- 今出来る予防策

---

# JPCERT/CCとは

# JPCERT/CCの概要

---

- JPCERT/CC (ジェーピーサート・コーディネーションセンター)
  - Japan Computer Emergency Response Ieam  
Coordination Center
  - <http://www.jpccert.or.jp/>
  - 非営利組織
- 活動
  - コンピュータセキュリティインシデントに関する調整、連携などの活動をおこなっている
  - インシデントや脆弱性に関するコーディネーション業務
  - 情報収集・分析・発信
  - 国内組織や海外組織との連携(特に各国のCSIRT組織)

# ちなみにCSIRTとは

---

## ※CSIRT(シーサート)とは

- Computer Security Incident Response Team
- 起源と概要:
  - 1988年11月に不正プログラム(the Morris worm)の蔓延によりインターネットの利用が困難となる重大なインシデントが発生したことをきっかけに、インシデント発生から20日後、DARPAによって、Carnegie Mellon University の Software Engineering Institute(CMU/SEI)に“CERT/CC”設立。
  - サービス対象、サービス内容には様々なバリエーションがある。
- CSIRTの代表的な機能
  - インシデントハンドリング
  - 注意喚起、勧告、などのセキュリティ関連情報の提供
  - 適切な情報流通コミュニケーションチャネルの構築
  - 脆弱性ハンドリング

# 活動の概要

## インシデント予防

### 脆弱性情報ハンドリング

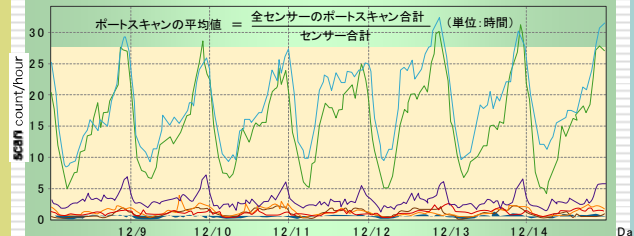
未公開の脆弱性関連情報を製品開発者へ提供し対応依頼  
国際的に情報公開日を調整



## インシデントの予測と捕捉

### 定点観測 (ISDAS)

ネットワークトラフィック情報の収集分析  
定期的なセキュリティ予防情報の提供



### 早期警戒情報

重要インフラ事業者等の特定組織向け情報発信

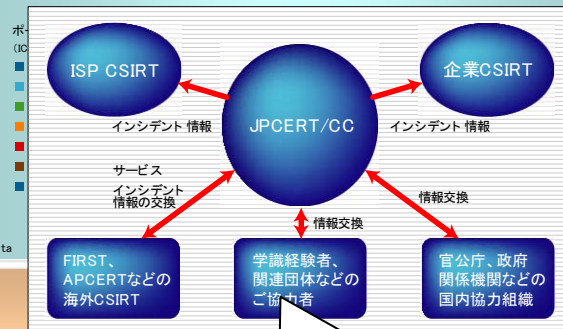
### CSIRT構築支援

企業内のセキュリティ対応組織の構築支援

## 発生したインシデントへの対応

### インシデントハンドリング

インシデントレスポンスの時間短縮による被害最小化  
再発防止に向けた関係各関の情報交換および情報共有



インシデントレスポンスの一環としてフィッシングサイトの停止(テイクダウン) 依頼業務を行う

---

# 日本のフィッシングの現状

# そもそもフィッシングとは？

フィッシングとは、**金融機関**(銀行やクレジットカード会社)などを装った**電子メール**を送り、**住所、氏名、銀行口座番号、クレジットカード番号**などの個人情報  
を詐取する行為です。電子メールのリンクから**偽サイト**に誘導し、そこで個人情報を  
入力させる手口が一般的に使われています。(フィッシング対策協議会 | フィッシングと  
は?)

## □ 例えばこんなケース

- **オンラインサービス、食品会社、企業年金**
- **CD-ROM、スパイフィッシング**
- **携帯電話番号**
- **金融機関などを装って、電話番号が書かれたメールを送る。受け取った人物が電話をかけると...**

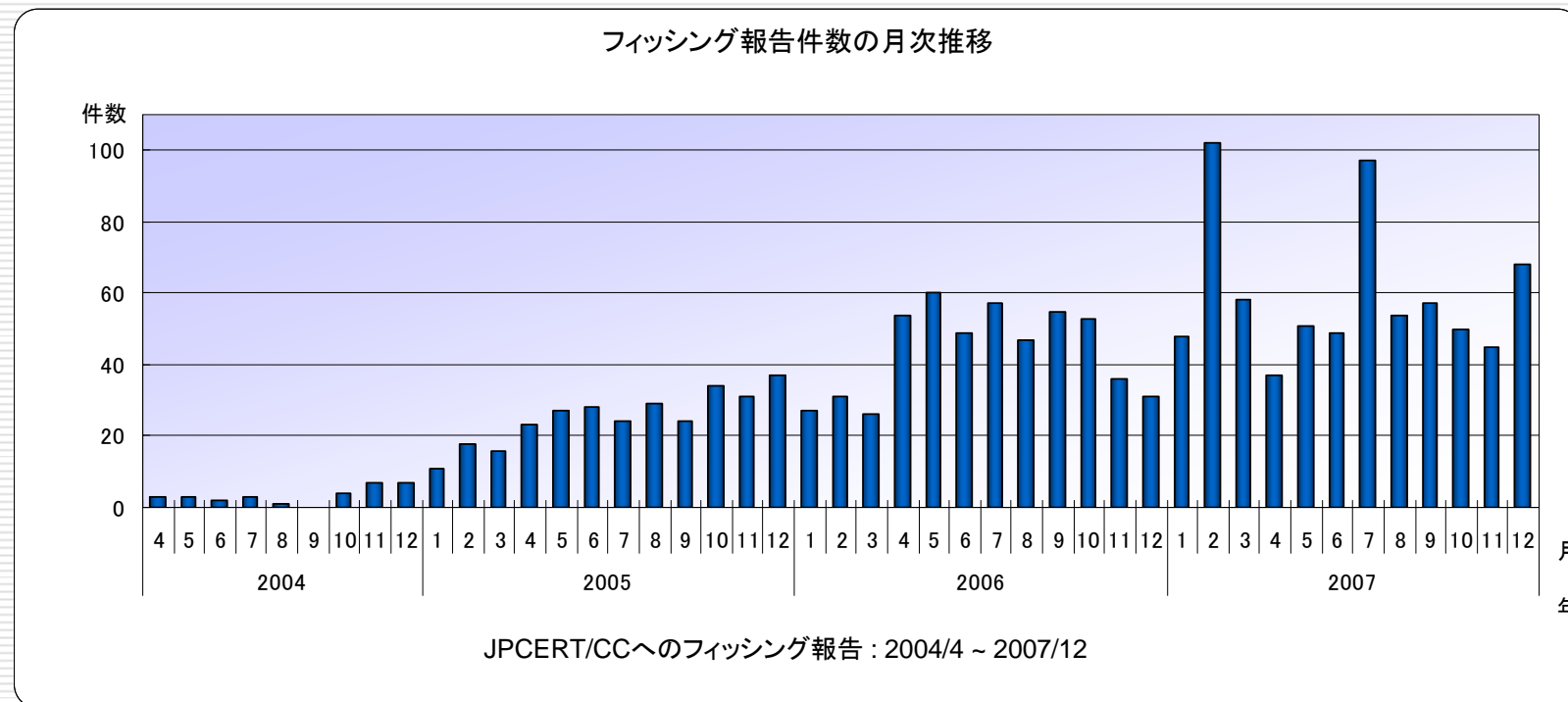
## □ 変わる手口、曖昧な定義、法整備は困難

- **不正アクセス禁止法、詐欺、商標権侵害、著作権侵害**







# フィッシング JPCERT/CCへの報告

- 報告のほとんどが、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ているケース
- 増加傾向に鈍りが見えたか？



# 報告の内容

- 海外企業のフィッシングサイトが国内に設置されるケース

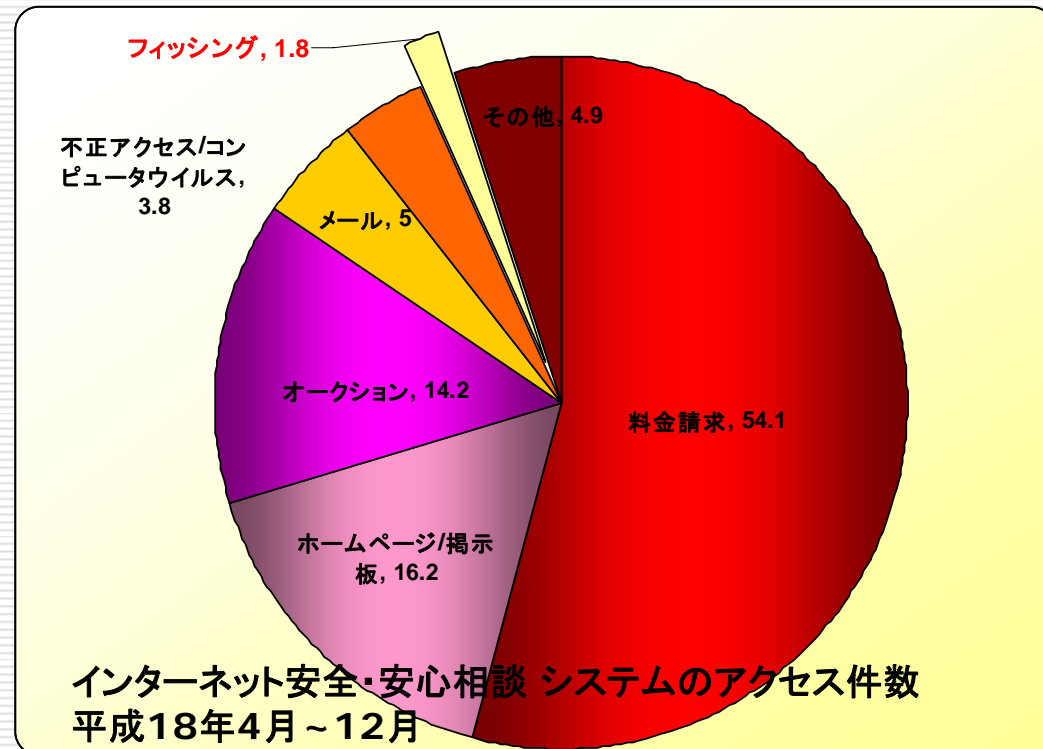
報告者	2004年度		2005年度		2006年度		2007年度	
	国外		国外		国外		国外	
CSIRT	11	0	36	0	21	0	17	16
セキュリティサービス	20	0	94	0	396	1	252	36
銀行、クレジットカード会社	15	0	82	6	37	9	91	2
その他	2	4	6	9	102	12	7	10

注) 2007年度は12月までのデータ

# フィッシング 警察への相談



警察庁 インターネット安全・安心相談  
<http://www.cybersafety.go.jp/nwqa/>



警察庁“平成18年のサイバー犯罪の検挙及び相談状況について  
 (http://www.npa.go.jp/cyber/statics/h18/pdf34.pdf)”より作図

# なぜ日本でのフィッシングは少ないか

---

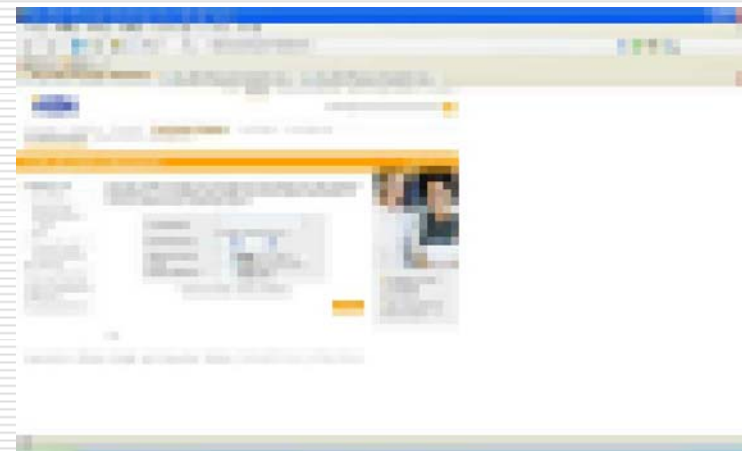
- 言葉の壁
- オンラインサービスの普及率の低さ
- 大事な書類は郵送される
- 振り込め詐欺・ワンクリック詐欺で十分?

楽観視せず、先手を打った対策をとることが大切

# フィッシング対応事例1

## 一般的なパターン

10月15日	フィッシングサイトの報告が JPCERT/CC に届く
10月15日	IPアドレス管理者 (ISP等) に JPCERT/CC から通知連絡を行う
10月15日	通知先管理者より、フィッシングサイト閉鎖の連絡
10月16日	当該URLがアクセス不可であることを確認
10月16日	報告者へサイト閉鎖の連絡



# フィッシング対応事例2

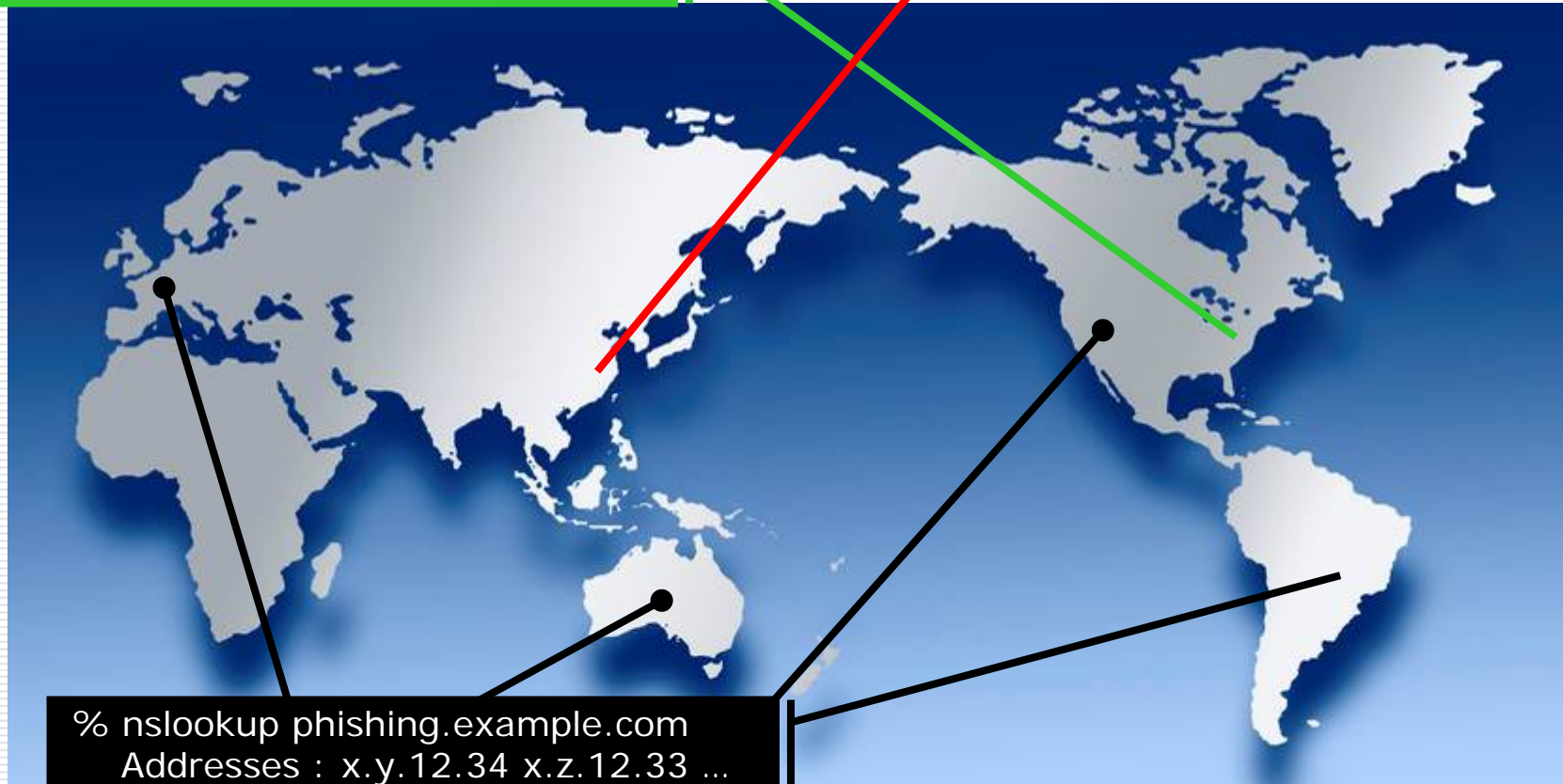
## 邦銀フィッシングサイト対応事例

X月12日	邦銀フィッシングサイト、計11サイトの報告が JPCERT/CC に →サイトの稼働状況を確認:稼働5、停止6
X月12日	IPアドレス管理者(ISP等)にJPCERT/CCから通知連絡を行う (A国1件、B国2件、C国1件、D国1件)
X月13日	追加情報として6件の報告を受理。計17サイト →サイトの稼働状況を確認:稼働3、停止14
X月13日	IPアドレス管理者(ISP等)にJPCERT/CCから通知連絡を行う (A国2件、E国1件)
X月17日	サイトの稼働状況を確認:稼働1、停止16
X月17日	IPアドレス管理者(ISP等)にJPCERT/CCから通知連絡を行う (1件)
X月18日	サイト稼働状況を確認し、すべてのサイトが停止
X月19日	報告者へサイト閉鎖の連絡

# 国境を越えたフィッシング

`http://phishing.example.com/login`

`% jwhois phishing.example.com`



`% nslookup phishing.example.com`  
 Addresses : x.y.12.34 x.z.12.33 ...

# フィッシングサイト閉鎖対応状況

対応組織	返答	サイト閉鎖までの時間			件数 (月平均)	閉鎖率
		平均時間	最短時間	最長時間		
A	有	6時間	20分	3営業日	11	100%
B	有	2営業日	1営業日	7営業日	4	100%
C	たまに	3営業日	1営業日	20営業日	4	100%
D	ほぼ無	3営業日	1営業日	14営業日	6	100%
E	有	20分	—	—	—	100%
F	無	7時間	—	—	—	100%



# フィッシング対応の難しさ

---

- フィッシングサイトと判断する基準
- あくまでISPへの依頼ベース
  - ISPの対応にばらつき
  - 強制力なし
- 国際犯罪
  - 各国にフィッシングサイト
- 何度も蘇るフィッシングサイト
- 減らない、放置されているテストサーバとボット

# JPCERT/CCへの報告

## □ JPCERTコーディネーションセンター

- Email: [info@jpcert.or.jp](mailto:info@jpcert.or.jp)  
PGP Fingerprint : BA F4 D9 FA B8 FB F0 73 57 EE  
3C 2B 13 F0 48 B8
- Tel: 03-3518-4600
- <http://www.jpcert.or.jp/form/>

## □ インシデント報告の仕方

- フォームに必要事項記入の上、  
[info@jpcert.or.jp](mailto:info@jpcert.or.jp)にメール
- 該当サーバのURL必須
- 『サイト停止希望』と明記

```

form.txt - メモ帳
ファイル(E) 編集(E) 書式(O) 表示(V) ヘルプ(H)
[[Ver 3.02]]
--- コンピュータセキュリティインシデント報告様式 ---
        JPCERT コーディネーションセンター (JPCERT/CC)

この報告様式は、コンピュータセキュリティインシデント情報を JPCERT/CC
へお送り頂く際にご利用頂くためのものです。

報告様式一式に関しては、http://www.jpcert.or.jp/form/ をご覧下さい。
初めて利用される方は「インシデント報告のガイドライン」(GUIDELINE.txt)
をお読み下さい。

報告内容の暗号化、またアーカイブの署名検証に必要な JPCERT/CC の PGP
公開鍵は以下の URL にございます。

http://www.jpcert.or.jp/jpcert.asc

-----
1. 連絡先
-----

1-1 お名前、組織名称、部署名をご記入下さい。

名前:
組織名称:
部署名:

1-2 連絡先の指定のある方はご記入下さい。指定がなければ、お送り頂いた
電子メールアドレス、もしくは FAX の発信元に返信致します。

電子メール:
FAX:
    
```

---

# 今出来る予防策

## 今出来る予防策

---

被害が本格化してない今だからこそ、先を見据えた対策を!

- Webのデザインを再確認
  - 正規のサイトは堂々と!
- 顧客とのコミュニケーションを見直す
- インシデントに備えた体制作り

# Webのデザイン

---

## □ 基本的な考え方

- AIST RCIS: 安全なWebサイト利用の鉄則 / サイト運営者の鉄則

<http://www.rcis.aist.go.jp/special/websafety2007/admin1.html>

- アドレスバー/ステータスバーを隠さない
- SSLサーバ証明書を購入し、ユーザからの入力を受け取る画面などはhttpsでのアクセスを提供する

# 顧客への周知

---

- ドメイン名の告知を行う
  - 「オンラインでのお取引は  
<http://www.example.co.jp/online/> へ」
  - 利用者カードや利用案内などで告知
  - キャンペーンサイト
- 「〇〇で検索」に潜む危険性
  - Googleの“怪現象”―「厚生労働省」で検索すると別サイトがトップに:ITpro
  - <http://itpro.nikkeibp.co.jp/article/NEWS/20071227/290184/>
- HTMLメールを避ける(可能であれば)
- メールに署名する

# 送信ドメイン認証 SPF

- なりすましを見破ることが可能
  - スпам対策・フィッシング対策に

```
-bash-2.05b$ dig TXT jpcert.or.jp
; <<>> DiG 8.3 <<>> TXT jpcert.or.jp
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51445
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUERY SECTION:
;;   jpcert.or.jp, type = TXT, class = IN
;; ANSWER SECTION:
jpcert.or.jp. 1H IN TXT "v=spf1 ip4:210.148.223.5
ip4:210.148.223.6 ~all"
```

jpcert.or.jpでのSPFレコード設定例

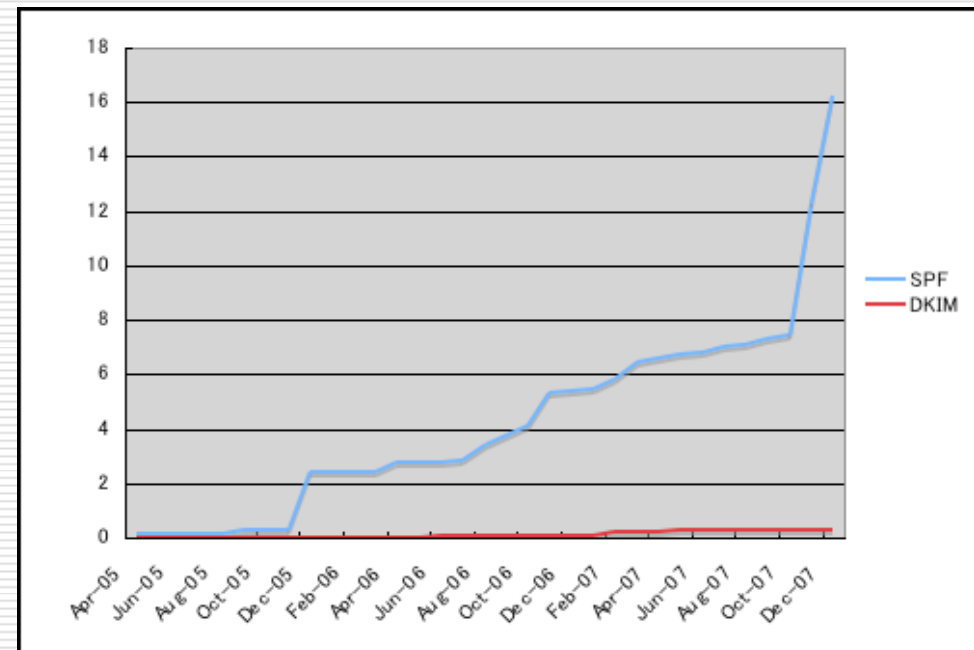
# 送信ドメイン認証 SPF

## □ 普及状況

- .jpドメインの7.47%が対応済み  
(2007/12 現在)
- ドメイン認証の普及率に対する測定結果  
<http://member.wide.ad.jp/wg/antispam/stats/index.html>

## □ 設定を確認したい?

- <http://www.seoconsultants.com/tools/spf/>

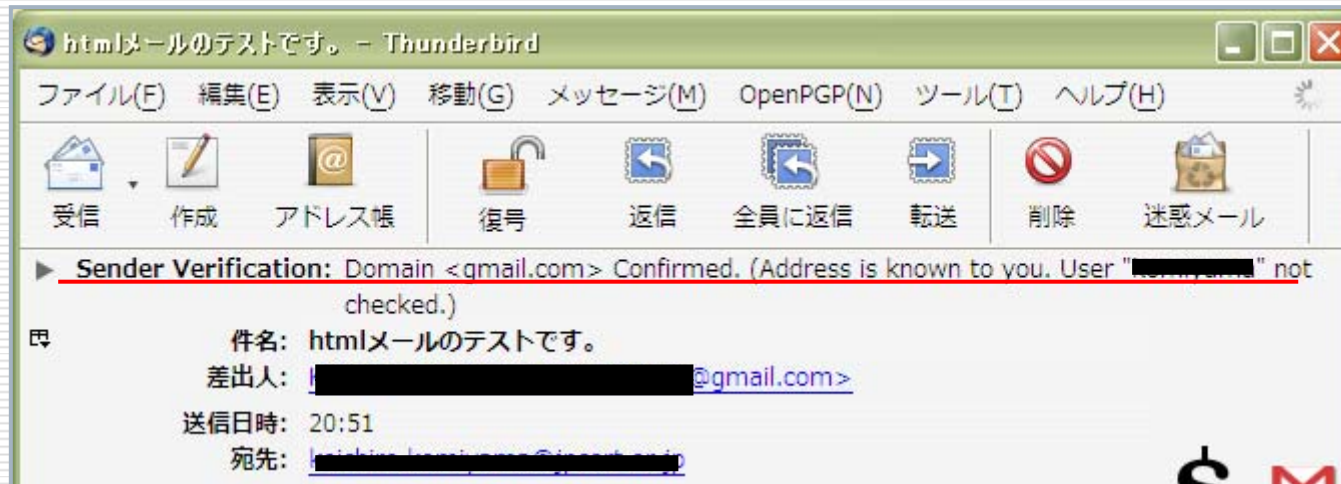


WIDEプロジェクトドメイン認証の普及率に対する測定結果



# おまけ: SPFレコードをチェックする

- メールのヘッダーとドメインのSPFレコードを照合する
  - Sender Verification Extension  
<https://addons.mozilla.org/ja/thunderbird/addon/345>



# インシデントに備えた体制作り

---

- 自社のフィッシングサイトが確認された。その時あなたがすることは?
  - 連絡体制
  - 外部組織(CSIRT、警察)への連絡
  - 顧客への連絡手段
- 情報セキュリティに関するインシデント対応のベストプラクティス
  - 「組織内 CSIRT」の構築  
[http://www.jpccert.or.jp/csirt\\_material/](http://www.jpccert.or.jp/csirt_material/)

# ご静聴有り難うございました

---

## 問い合わせ先(再掲)

### □ JPCERTコーディネーションセンター

- Email: [info@jpcert.or.jp](mailto:info@jpcert.or.jp)

PGP Fingerprint : BA F4 D9 FA B8 FB F0 73 57 EE 3C 2B 13 F0 48 B8

- Tel: 03-3518-4600

- <http://www.jpcert.or.jp/form/>

### □ インシデント報告の仕方

- フォームに必要事項記入の上、[info@jpcert.or.jp](mailto:info@jpcert.or.jp)にメール
- 該当サーバのURL必須
- 『サイト停止希望』と明記