違法・有害情報対策
～フィッシング・マルウェアへの対応～

JPCERコーディネーションセンター
早期警戒グループ
マネージャ
鎌田敬介
Keisuke KAMATA
2007/11/21@Internet Week 2007

本日のTOPIC

- JPCERT/CCの概要
- JPCERT/CCのインシデント対応
- フィッシングとマルウェア
  - とそれらの対応状況/対応事例
- まとめ

JPCERT/CCの概要

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

- JPCERT/CC
  - Japan Computer Emergency Response Team Coordination Center
    - ジェーピーサート・コーディネーションセンター
  - 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活動
  - 国内組織や海外組織との連携活動
  - 情報収集・分析・発信活動
  - 「コーディネーションセンター」としての役割
  - 米国のCERT/CCを起源とする組織
  - 世界各国のCSIRT組織との連携活動

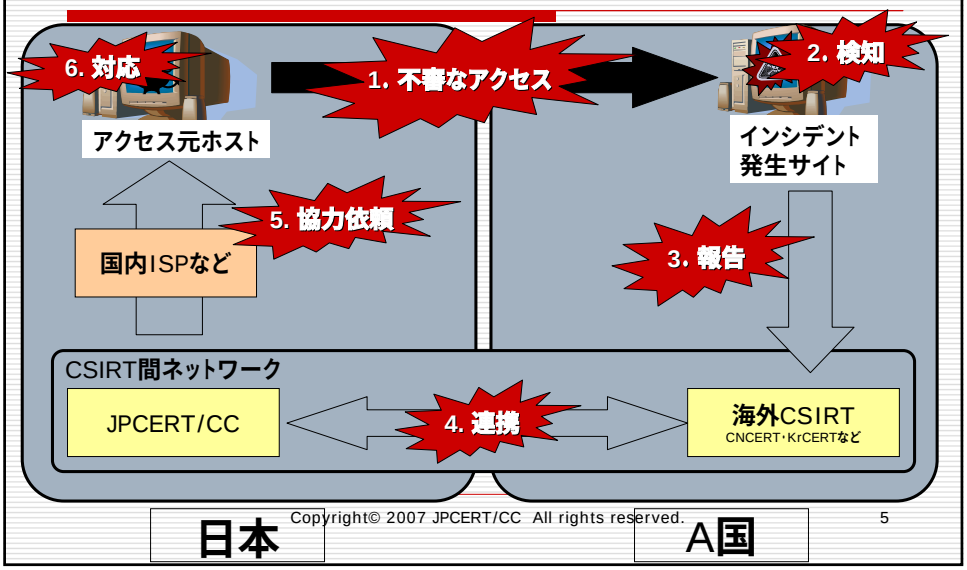
インシデント報告の受付

- JPCERT/CCでは国内外からのインシデント報告を受け付けています
  - インシデント報告の届出

    http://www.jpcert.or.jp/form/
  - 報告の目的を記載
    - インシデントの情報提供
    - 質問（インシデント対応に関するもの）
    - 関係サイトへの連絡
  - 海外のCSIRTとの連携対応

JPCERT CC®

インシデントハンドリングの国際連携



JPCERT CC®

インシデントハンドリングの国際連携

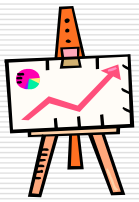
- 国際連携によって越えられる壁
  - 言語の違い
  - 文化の違い
  - 法律・制度の違い
- 各国CSIRT間の連携・協調活動として最も進んでいる分野

フィッシングとマルウェアの現状

- フィッシング
  - 海外金融機関やオークションサイトのフィッシングサイトが日本国内に設置されている
  - 日本の銀行のフィッシングサイトが海外に設置されている
- マルウェア
  - ウェブサイトに設置されている実行形式のプログラムが、実はマルウェア
  - 特定の組織を狙ったマルウェアがメールに添付されて送られてきている

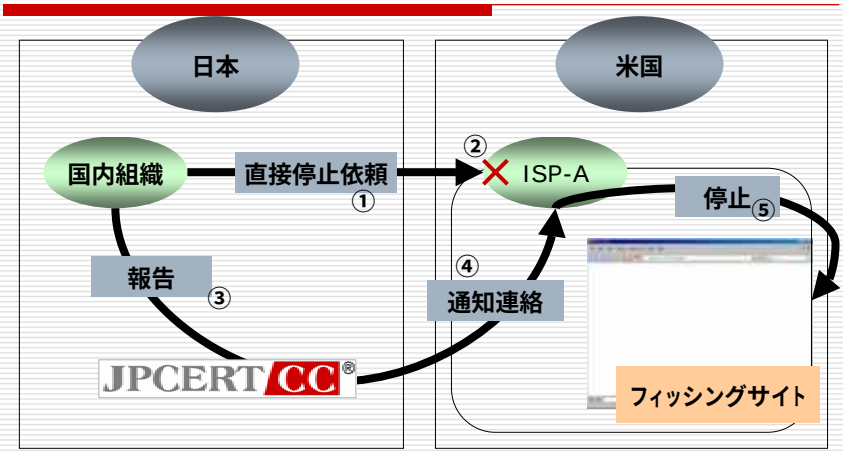
国内目線の動向

- 国内金融機関のフィッシングサイトの増加
  国内金融機関を装ったフィッシングサイトに関する注意喚起(2007-04-03)
  http://www.jpcert.or.jp/at/2007/at070009.txt
- 国内のサーバに侵入されフィッシングサイトにされたりマルウェアが置かれてしまう
  - サーバ管理者への働きかけが必要
  - ISPの皆様のご協力のおかげで
    サイトの閉鎖にこぎ着けている状況



JPCERT CC®

フィッシングサイト閉鎖コーディネーション



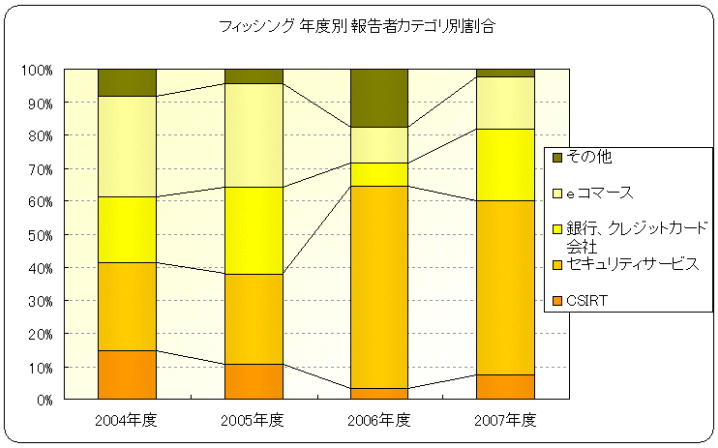
某A社が直接連絡したが、フィッシングサイトが停止せず
JPCERT/CCへ報告しコーディネーションした結果フィッシングサイトが停止した

JPCERT CC®

フィッシングサイト報告件数（月別）

フィッシング報告者 (種別件数)

2007年度9月まで

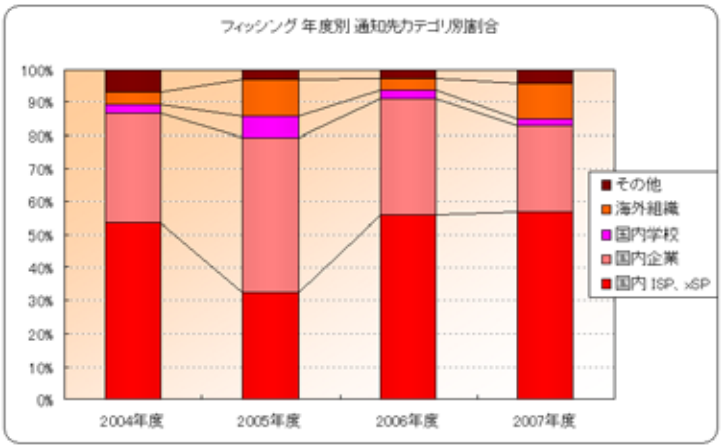


2007年度は9月まで

フィッシング報告者 (種別件数)

報告者	2004年度		2005年度		2006年度		2007年度 (9月まで)	
	国外	国内	国外	国内	国外	国内	国外	国内
CSIRT	11	0	36	0	21	0	15	11
セキュリティサービス	20	0	94	0	396	1	181	0
銀行、クレジットカード会社	15	0	81	6	37	9	73	2
eコマース	23	0	97	11	61	11	53	2
その他	2	4	5	9	102	12	1	7

フィッシングサイトIPアドレス管理者



2007年度は9月まで

フィッシングサイトIPアドレス管理者 (種別件数)

被害サイト	2004年度	2005年度	2006年度	2007年度 (4-9月まで)
国内ISP・xSP	40	110	362	215
国内企業	25	158	231	99
国内学校	2	22	17	7
海外組織	3	38	23	38
その他	5	11	17	16

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	ー	ー	ー	100%
F	無	7時間	ー	ー	ー	100%

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
サイト復活事例

9月15日	フィッシングサイトの報告が JPCERT/CC に届く
9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
9月16日	通知先管理者より、フィッシングサイト閉鎖の連絡
9月16日	当該URLが404 Not Foundとなることを確認
9月17日	当該URLが再び閲覧可能になっていることを確認
9月17日	JPCERT/CCから、管理者へ再び通知連絡を行う
9月17日	通知先管理者より、サイト閉鎖対応の連絡
9月17日	報告者へサイト閉鎖の連絡

フィッシング対応事例3
複数のサイトが設置されていた事例

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16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404 Not Foundとなることを確認
10月17日	報告者へサイト閉鎖の連絡
10月19日	別の報告者より、同じIPアドレスにて別のフィッシングサイトが立ち上げられている、という報告が届く
10月19日	IPアドレス管理者（ISP等）にJPCERT/CCから再度連絡を行う
10月20日	通知先管理者より、サイト閉鎖対応の連絡
10月20日	報告者へサイト閉鎖の連絡

フィッシング対応事例4
再設置された事例

8月20日	フィッシングサイトの報告が JPCERT/CC に届く
8月20日	IPアドレス管理者（ISP等）にJPCERT/CCから通知連絡を行う
8月21日	通知先管理者より、フィッシングサイト閉鎖の連絡
8月21日	当該URLからサイトが消されていることを確認
8月21日	報告者へサイト閉鎖の連絡
10月23日	同一サーバに新たなフィッシングサイトが設置されているという報告がJPCERT/CCに届く
10月23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23日	通知先管理者より、サイト閉鎖対応の連絡
10月23日	報告者へサイト閉鎖の連絡

フィッシング対応事例5
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

JPCERT CC®

マルウェア対応事例

9月2日	マルウェア設置サイトの報告が JPCERT/CC に届く
9月2日	IPアドレス管理者（ISP等）にJPCERT/CCから通知連絡を行う ※この事例においては海外
9月3日	通知先管理者より、マルウェア削除の連絡
9月3日	マルウェアがサイトから削除されていることを確認
9月3日	報告者へサイト閉鎖の連絡

JPCERT CC®

まとめ

- オペレーションの限界
  - JPCERT/CCは報告された情報以上はわからない
    - 1つのサーバにフィッシングサイトがいくつ設置されているか、なぜ侵入されたか、などは把握できない
  - 個別のサイトの対応の手助けはできない
- サーバ管理者の皆様へのお願い
  - 知らない間に侵入されてしまうケースが多いです
  - 公開されている脆弱性への対策を
  - テスト目的で設置したサーバは放置しないで

参考資料

- JPCERT Coodrination Center：JPCERT/CC
  http://www.jpcert.or.jp/
  - インシデント対応とは？
    http://www.jpcert.or.jp/ir/
  - CSIRTマテリアル
    http://www.jpcert.or.jp/csirt_material/
  - コンピュータセキュリティインシデント対応チーム (CSIRT) のためのハンドブック
    http://www.jpcert.or.jp/research/2007/CSIRT_Handbook.pdf
- FIRST
  http://www.first.org/
- APCERT
  http://www.apcert.org/
- CERT/CC
  http://www.cert.org/
- CPNI
  http://www.cpni.gov.uk/

お問い合わせ先

- 有限責任中間法人
  JPCERTコーディネーションセンター
  - Email：office@jpcert.or.jp
  - Tel：03-3518-4600
  - http://www.jpcert.or.jp
- インシデント報告の届出
  - 報告様式
    http://www.jpcert.or.jp/form/
  - Email：info@jpcert.or.jp
    PGP Fingerprint：470F F413 3DCC 5D38 7CAC 3500 80C4 944B 298F 386F