2007年8月23日
第21回JPドメイン名諮問委員会
資料5

参考資料

フィッシングの動向

2007年8月23日

株式会社 日本レジストリサービス

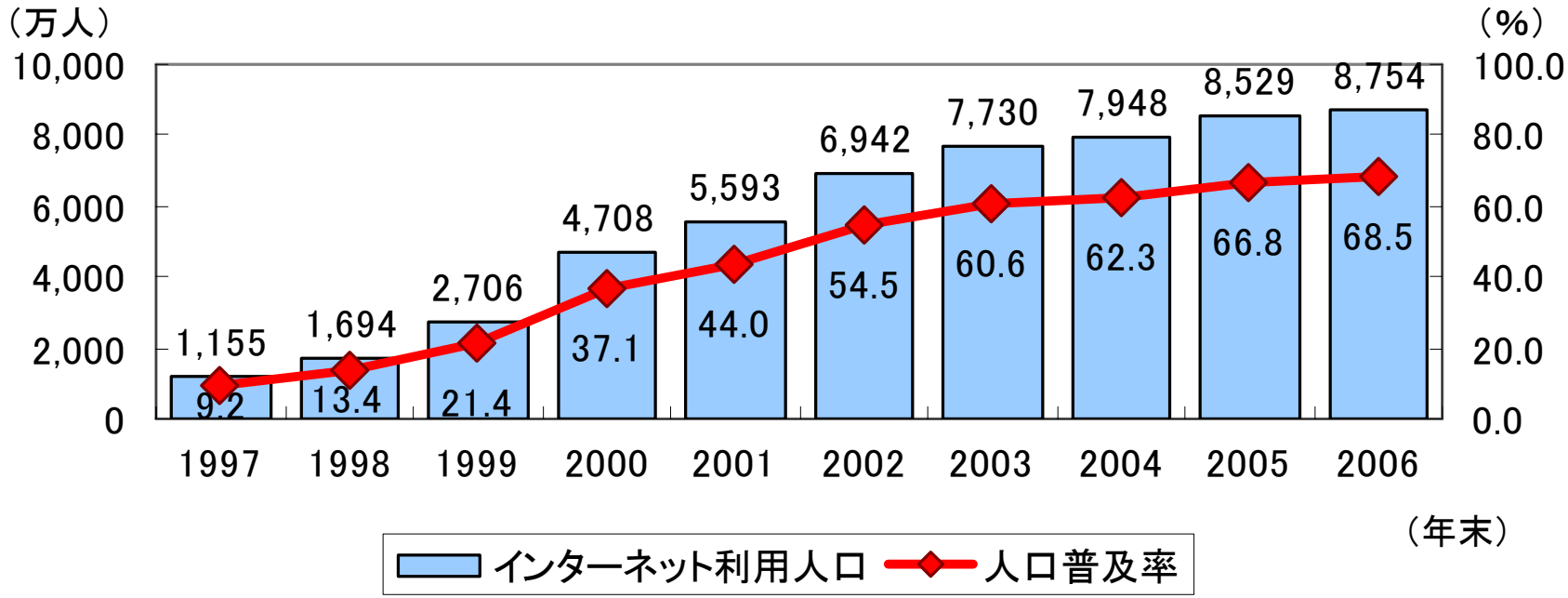
目次

1. インターネットでの重要情報のやりとり
2. フィッシングに関連した国内外の動向
3. フィッシングとドメイン名の関係

1. インターネットでの重要情報のやりとり

インターネット利用の社会への浸透

- 社会におけるインターネットの利用は、年々増え続けている。



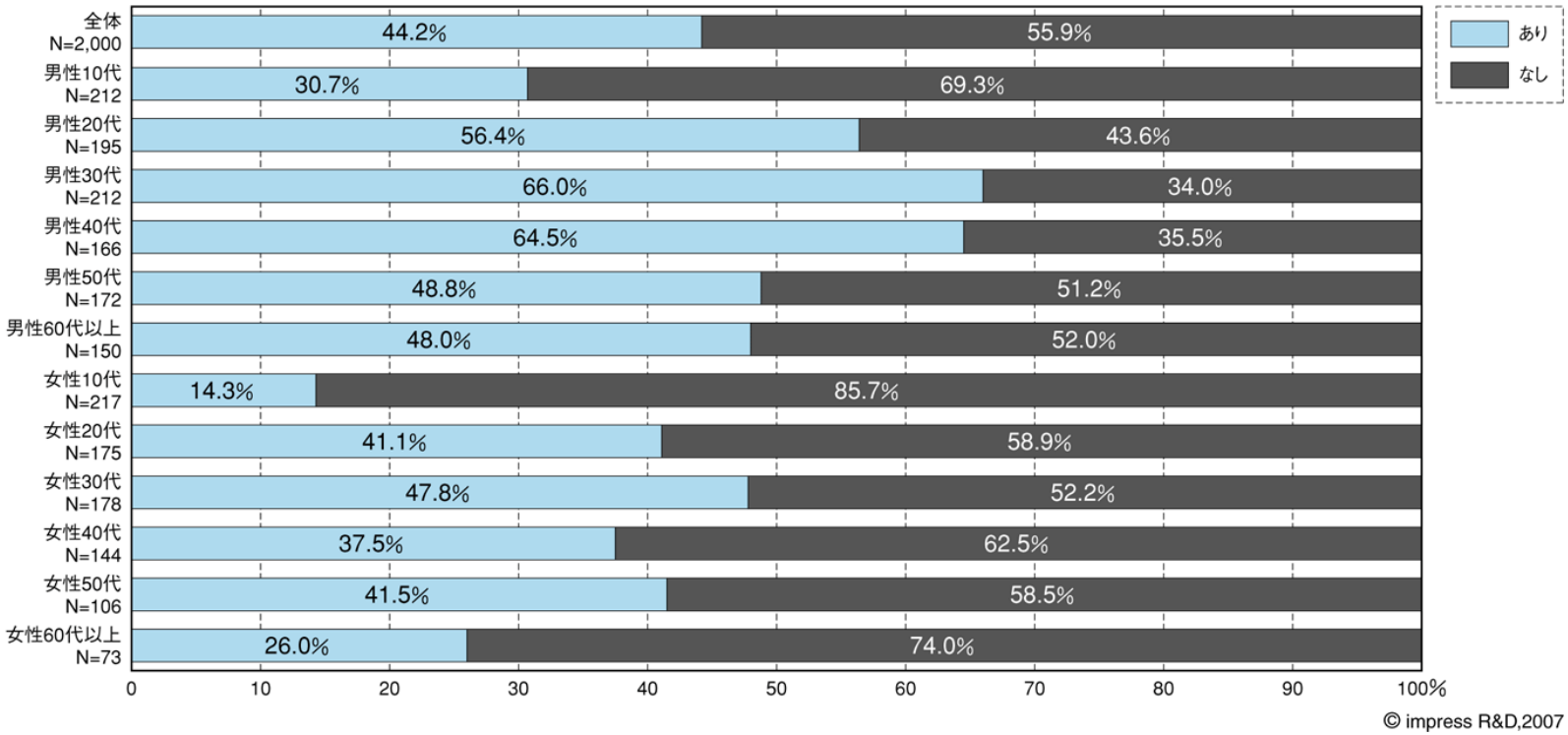
出典：インターネット利用者数及び人口普及率の動向 (平成19年版情報通信白書)

インターネットでの重要情報のやりとり(1/3)

- インターネットバンキングを使っていると答えた人の割合は44.2%

(注:使っているかどうかについては個人の判断による)

資料2-6-1　インターネットバンキングの利用状況[全体と性年代別]

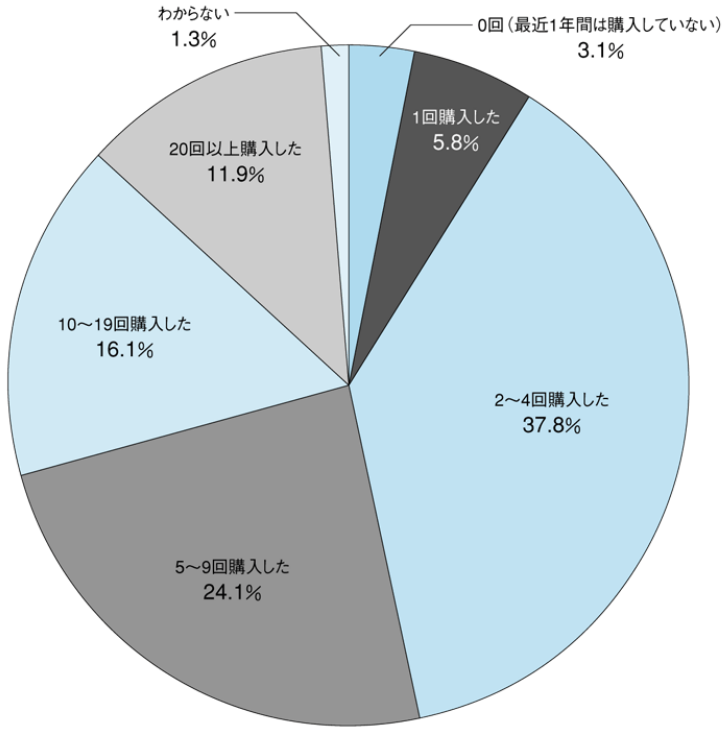


出典: インターネットバンキングの利用状況 (インターネット白書2007)

インターネットでの重要情報のやりとり(2/3)

- 回答者のほとんどが1年間に1回以上オンラインショッピングを行っている。

資料2-5-9　最近1年間のオンラインショッピングでの購入頻度　N=1,472



出典：最近1年間のオンラインショッピングでの購入頻度 (インターネット白書2007)

インターネットでの重要情報のやりとり(3/3)

- オンラインショッピングやインターネットバンキングの利用が浸透してきている。
- 利用時には主に次のような情報がやり取りされている。
  - 口座番号と暗証番号
  - クレジットカード番号
  - 住所・氏名・電話番号等の個人情報

→ これらの情報を騙し取り、不当な利益をあげようとする人が現れている。

2. フィッシングに関連した国内外の動向

日本における不正アクセスの動向(1/2)

- 不正アクセス禁止法違反で検挙された件数は年々増加

		平成12年	平成13年	平成14年	平成15年	平成16年	平成17年	平成18年
不正アクセス行為	検挙件数	62	66	102	143	142	271	698
	検挙事件数（注５）	30	35	51	58	65	94	84
	検挙人員	34	51	68	76	88	113	130
不正アクセス助長行為	検挙件数	5	1	3	2	0	6	5
	検挙事件数	4	1	2	2	0	6	3
	検挙人員	5	1	3	2	0	6	5
計	検挙件数（件）	67	67	105	145	142	277	703
	検挙事件数（事件）	31（重複3）	35（重複1）	51（重複2）	58（重複2）	65	94（重複6）	84（重複3）
	検挙人員（人）	37（重複2）	51（重複1）	69（重複2）	76（重複2）	88	116（重複3）	130（重複5）

※　（重複）とは、不正アクセス行為と不正アクセス助長行為の重複を示す。

出典：不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況 p3
http://www.npa.go.jp/cyber/statics/h18/pdf35.pdf

日本における不正アクセスの動向(2/2)

- 不正アクセス行為の手口としてフィッシングが急増

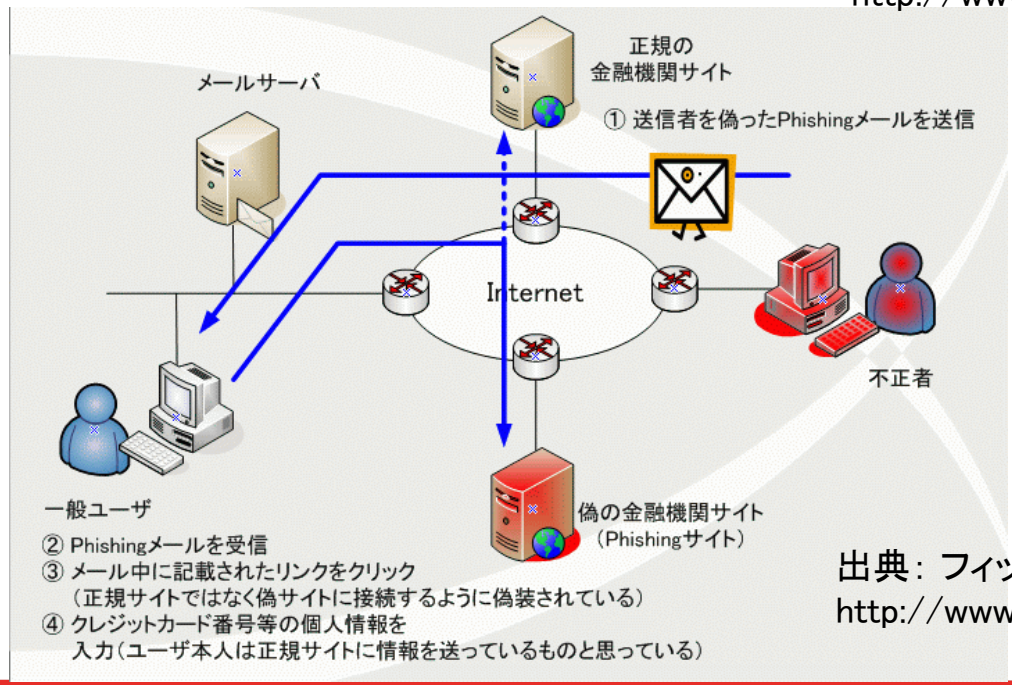
犯行の手口		平成17年 件数（件）	平成18年 件数（件）
識別符号窃用型		264	698
	フィッシングサイトにより入手したもの	1	220
	スパイウェア等のプログラムを使用して識別符号を入手したもの	33	197
	利用権者のパスワードの設定・管理の甘さにつけ込んだもの	95	178
	識別符号を知り得る立場にあった元従業員や知人等によるもの	33	49
	言葉巧みに利用権者から聞き出した又はのぞき見たもの	16	20
	ファイル交換ソフトや暴露ウイルスで流出した識別符号を含む情報を利用したもの	0	19
	他人から購入したもの	69	12
	共犯者等から入手したもの	12	0
	その他	5	3
セキュリティ・ホール攻撃型		7	0

出典：不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況 p4
http://www.npa.go.jp/cyber/statics/h18/pdf35.pdf

フィッシングとは

- フィッシング（Phishing）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。

出典：フィッシングとは(フィッシング対策協議会)
http://www.antiphishing.jp/doc/aboutphishing.html

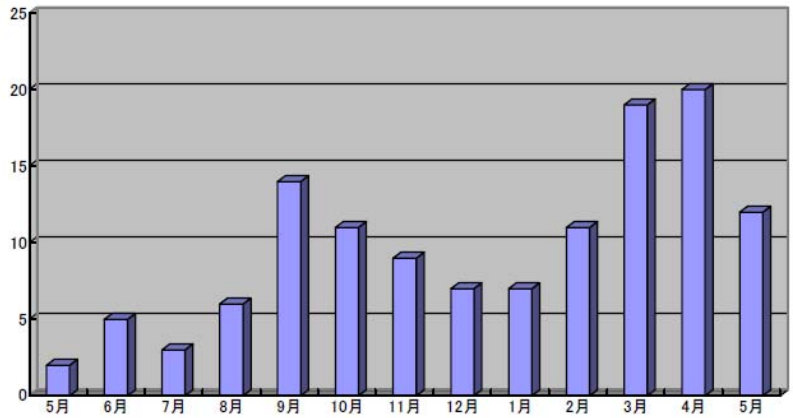


出典：フィッシングの手口（フィッシング対策協議会）
http://www.antiphishing.jp/doc/aboutphishing.html

フィッシングの動向[日本](1/3)

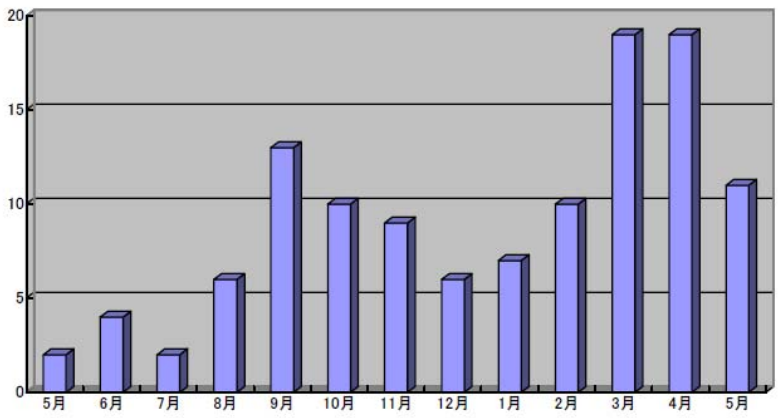
- フィッシング対策協議会に寄せられる国内のフィッシング情報届出状況

フィッシング情報の届出件数



フィッシング情報の届出件数(2006年5月～2007年5月)

フィッシングメールの件数



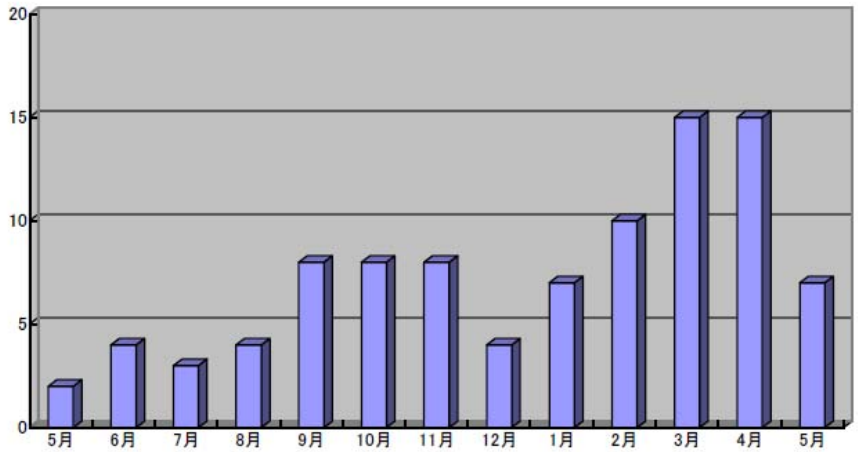
フィッシングメールの件数(2006年5月～2007年5月)

出典:2007/5 国内フィッシング情報届出状況
https://www.antiphishing.jp/report/200706-case-077.pdf

フィッシングの動向[日本](2/3)

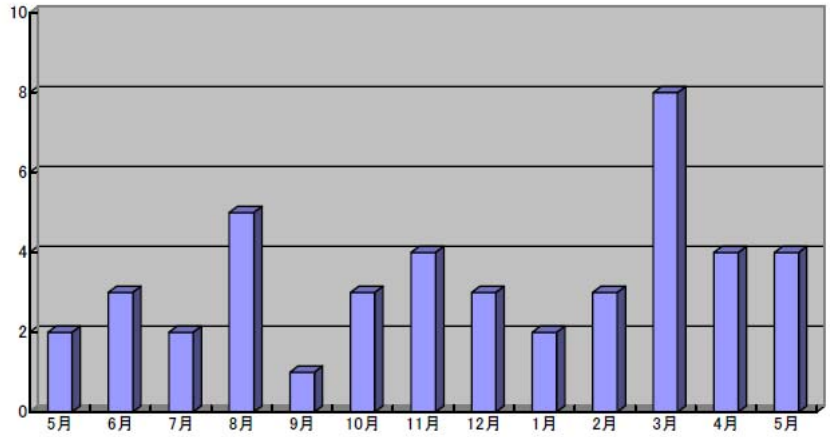
- フィッシング対策協議会に寄せられる国内のフィッシング情報届出状況

フィッシングサイトの件数



フィッシングサイトの件数(2006年5月～2007年5月)

フィッシングによりブランド名を悪用された企業の件数



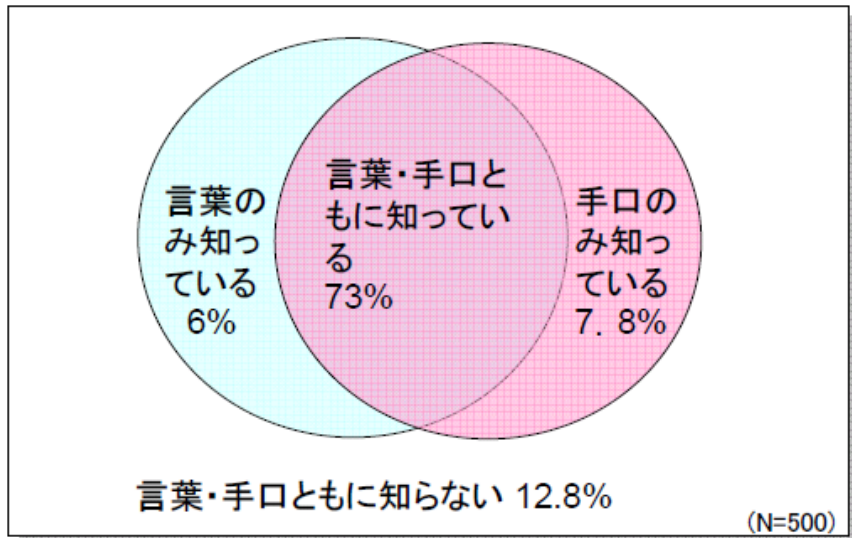
フィッシングによりブランド名を悪用された企業の件数(2006年5月～2007年5月)

出典:2007/5 国内フィッシング情報届出状況
https://www.antiphishing.jp/report/200706-case-077.pdf

フィッシングの動向[日本](3/3)

- フィッシングの認知度
  - 回答者
    - 92%がオンラインショッピングやインターネットバンキングの利用者である。

→約13%の人が言葉・手口を知らなかった。手口を知らない人を合わせると約19%となり、これらの人がフィッシングに対して特に危険な状態にあると言える。



選択肢	言葉知っている	言葉知らない	合計
手口知っていた	367	39	406
手口知らなかった	30	64	94
合計	397	103	500

出典:フィッシングに関するユーザ意識調査報告書 p9
http://www.antiphishing.jp/topics/User_Phishing_Awareness_Survey.pdf

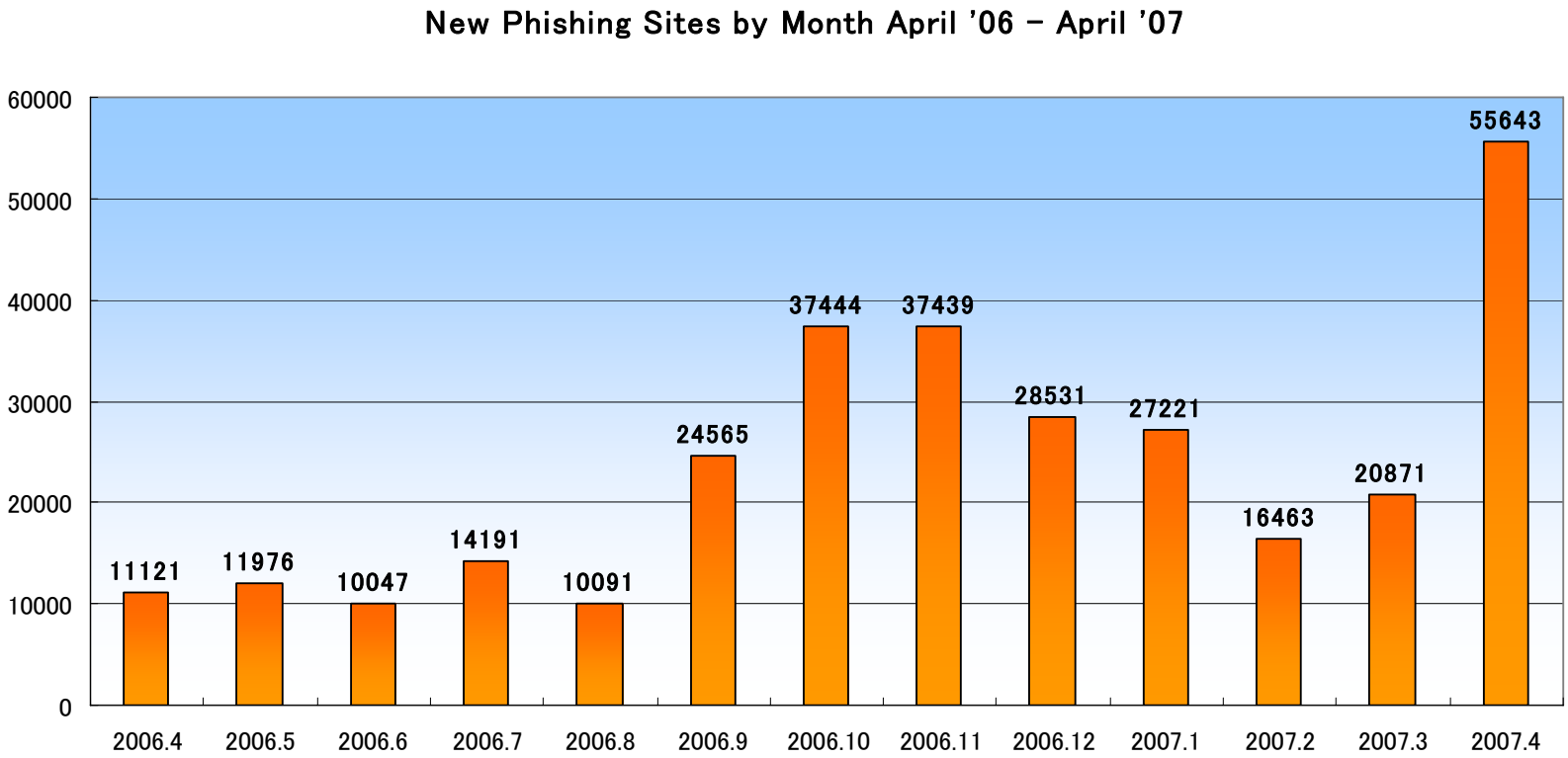
フィッシングの動向[世界](1/2)

- 財政的な損失の増加
  - Gartner社の調査によると、2006年におけるフィッシング攻撃による財政的な損失は28億ドル(約3,400億円)以上に上る。
  - 2006年10月、アメリカでは週に22,288のユニークなフィッシングサイトのURLが見つかった。
- 詐欺に使われるドメイン名
  - 2006年4月、26のTLDで詐欺的なドメイン名の登録に用いられた。(94%がgTLD(そのうち.comは62%))
  - 2006年10月、36のTLDで詐欺的なドメイン名の登録がなされた。(49%がgTLD(そのうち.comは10%))

出典:DNS Policy Sub-Committee Overview p9
http://www.apstar.org/bali_2007/CopingwithPhishing-Koichiro.pdf

フィッシングの動向[世界](2/2)

- フィッシングサイトの増加



出典:DNS Policy Sub-Committee Overview p9
http://sanjuan2007.icann.org/files/sanjuan/APWGOverviewPresentationICANNJune2007.pdf

国内のフィッシング対策に関連する団体等

団体	フィッシングに対する主な活動
経済産業省 フィッシング対策協議会	最新フィッシング事例、対策、注意喚起、APWGレポートなどの掲載。
総務省 フィッシング対策推進連絡会	フィッシングに関する情報共有と対策の検討。
警察庁 フィッシング110番	フィッシングに関する情報提供を受け付け、その情報をもとにフィッシングを取り締まる。
国民生活センター	フィッシングの事例紹介や対策の掲載。
独立行政法人情報処理推進機構(IPA)	フィッシングの事例紹介や対策の掲載。
JPCERT/CC	フィッシングへの対応や対策の掲載。
次世代電子商取引推進協議会(ECOM)	情報セキュリティの懇話会やEコマースのセミナーの開催。

フィッシングはどこからが犯罪になるのか？

- 他人の個人情報(銀行口座番号など)を入手する
  - 明確な罰則規定はない
- 入手した他人の個人情報を使って実際に金融機関サイトにアクセスする
  - 不正アクセス禁止法違反(不正アクセス行為の禁止)
  - 刑法の「電子計算機使用詐欺罪」
- 入手した他人の個人情報をインターネット上などで売買する
  - 不正アクセス禁止法違反(不正アクセス行為を助長する行為の禁止)

フィッシングの技術的対策と法・制度面での対策

ステップ	内容	技術的対策方法	法・制度面での対策
0:フィッシングの準備	攻撃ターゲットの選別や電子メール送信のためのアドレス収集。類似ドメインの取得	類似ドメイン取得の監視	類似ドメイン取得の禁止 JPRSによる類似ドメイン取得に関する注意喚起の提供
1:メールの送信	フィッシングサイトに誘導するために詐欺メールの送信	ISPによるメールフィルタリング技術 送信者認証、メールの電子署名 課題：迷惑メール用フィルタのため、フィッシングの場合フィルタの誤検知のとの見分けが付かない	迷惑メール法、偽装メールに対する著作権法の適用 課題：送信者認証や電子署名の技術を推進する制度が必要とされる。
2:ユーザがメールに反応	届いたメールを開封し、URLをユーザが実行	証明書付き電子メール	教育・啓発活動によるユーザの教育 フィッシング対策協議会のWebによるフィッシングの啓発活動
3:フィッシング攻撃の実行	偽装サイトにユーザが訪れる	クロスサイトスクリプティングの脆弱性の除去	偽装Webに対する著作権法の適用
4:機密情報の送信	偽装サイトにユーザが個人識別情報を入力する	ユーザが安易にフィッシングサイトを見分けられるようにするための技術 ・フィッシング対策ツールバー ・実在性も保障する厳密な証明書(EV SSL) ・サイト画像認証 ・画像を利用したユーザ認証	課題：制度面での技術の普及の後押しが必要
5:機密情報の入手	偽装サイト上の収集された個人識別情報をフィッシャーが取得	マルウェアによる識別情報の盗み取りを防止するための技術 ・ソフトキーボード、キーロガー検知	課題：個人識別情報の入手を罰する手段がない
6:機密情報の利用	個人識別情報を利用してユーザになりすましてサービスを利用	盗み出した個人識別情報を利用してもなりすましを出来ないようにするための技術 ・二要素認証 ・帯域外認証 課題：コスト	不正アクセス禁止法 課題：制度面での技術の普及の後押しが必要
7:不正行為の実行	クレジットカードの利用や預金の引き落としなど不正行為の実行	トランザクションの不正検知	現行の刑法に順ずる 課題：国際的な犯罪に対する国内法の限界

出典：フィッシング対策における技術・制度調査報告書2007 p9
http://www.antiphishing.jp/topics/WG_Report-001.pdf

海外のフィッシング対策団体(1/2)

- Anti-Phishing Working Group (APWG)
  - 米国のフィシング対策の業界団体
  - 会員数:2600以上(内、企業・団体会員数:1600以上)
  - 主な活動
    - 最新フィッシング事例、対策、注意喚起、レポート掲載
    - 各国CERT(※)との連携強化

      ※Computer Emergency Response Team
      コンピュータセキュリティインシデントに対応する活動を行なう組織体
    - 司法当局と情報共有

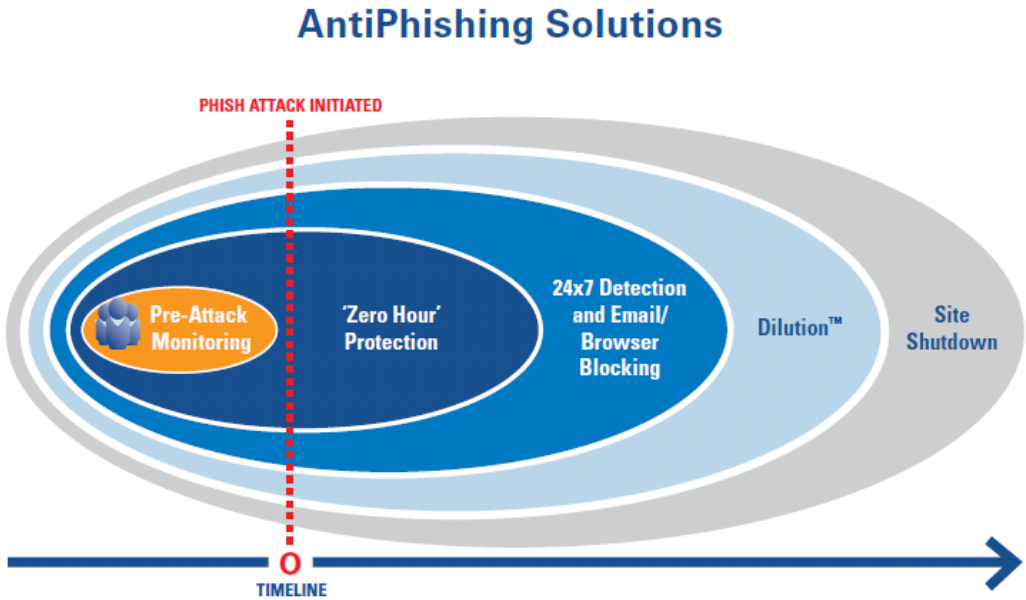
出典:Anti-Phishing Working Group
http://www.antiphishing.org/

海外のフィッシング対策団体(2/2)

- 米国以外のフィッシング対策に関連した団体の例
  - Anti-Phishing ITALIA (イタリア)
  - AusCERT(オーストラリア)

米国の代表的フィッシング対策サービス(1/5)

- MarkMonitor
  - MarkMonitorは企業のブランドの保護を行っており、フィッシング対策のサービスも提供している。その中では、5つの施策がとられており、時間と共にそれぞれの施策を加えていくという重層的な対策となっている。



出展:AntiPhishing Solutions
http://www.markmonitor.com/resources/docs/product-antiphishingsolutions.pdf

米国の代表的フィッシング対策サービス(2/5)

- MarkMonitorのフィッシング対策サービスの内容
  - 第1段階:事前の監視
    - 早期警戒システムにより稼働前の潜在的フィッシングサイトを探知、警告
  - 第2段階:「ゼロ時間」プロテクション
    - クライアントアプリケーションによりフィッシングサイトへのアクセスを即時阻止、警告
  - 第3段階:24時間体制による検知と電子メール/ブラウザ遮断
    - フィッシングサイト、メールを主要ISPおよびブラウザベンダに通報
  - 第4段階:希釈化
    - フィッシャー(不正者)のWebサーバに間違ったデータを送付し消費者の身元情報を希釈化
  - 第5段階:フィッシングサイトの閉鎖
    - ISPの協力を得てフィッシングサイトを閉鎖

出典:AntiPhishing Solutions
http://www.markmonitor.com/resources/docs/product-antiphishingsolutions.pdf

米国の代表的フィッシング対策サービス(3/5)

- RSA, The Security Division of EMC
  - RSA, The Security Division of EMCは、オンライン上のアイデンティティ保護とデジタル資産を大切に保護するための技術、製品、ソリューションを提供している。その中で、フィッシングサイトをシャットダウンするサービス「RSA FraudAction」を金融機関に提供している。

出典:RSAセキュリティ株式会社
http://japan.rsa.com/company/index.html

米国の代表的フィッシング対策サービス(4/5)

- RSAのフィッシング対策サービスの内容[1/2]
  - アンダーグラウンドの監視
    - アンダーグラウンドのWebサイトを継続的に監視し、情報を入手
  - 重大度評価モジュール
    - クライアントに情報を提供し、どのような対策をとるべきかの意思決定プロセスを支援
  - フィッシングサイトのシャットダウン
    - クライアントからの疑わしいWebサイトの通告により、ISPおよびホスティング事業者と連絡をとり、フィッシングサイトのシャットダウンに取り組む
  - フォレンジック対応
    - アナリストが攻撃の原因究明や犯罪の証拠発見のための情報収集及び分析

出典:RSAセキュリティ株式会社
http://japan.rsa.com/products/consumer_solutions/fraudaction/FRA_DS_060-J.pdf

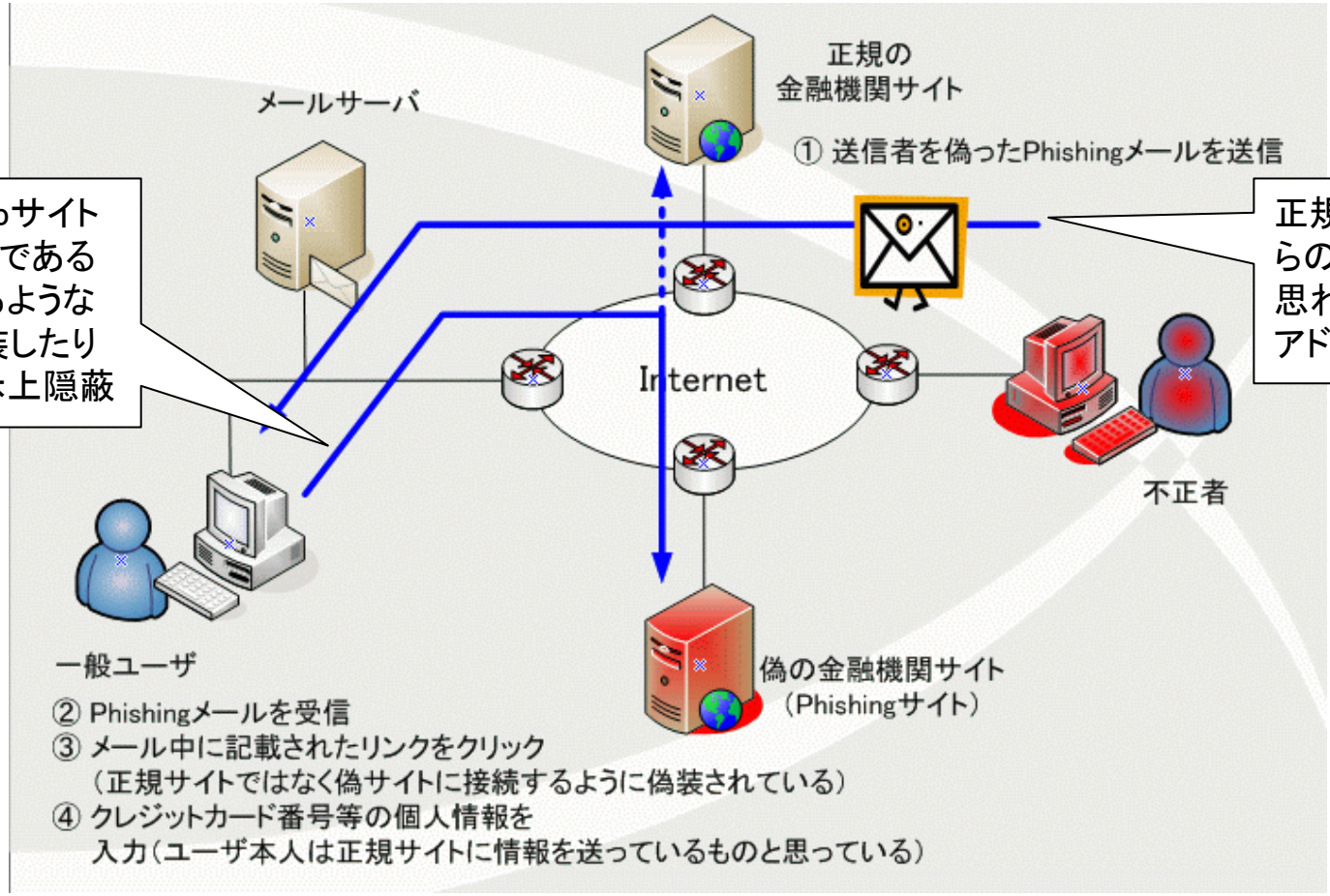
米国の代表的フィッシング対策サービス(5/5)

- RSAのフィッシング対策サービスの内容[2/2]
  - ブロッキング・ネットワーク
    - 大手ISP、アンチウイルス企業などと提携し、それらの企業がユーザに対してフィッシングサイトへのアクセスを阻止
    - たとえば、RSA FraudActionがMicrosoftに情報を提供し、MirosoftがInternet Explorer(IE7)とMSN Search Toolbarのユーザに警告を出したり、フィッシングサイトへのアクセスをブロック
  - レポーティング・サービス
    - 最新のステータスやフィッシングサイトの解析状況を提供
  - 対抗措置
    - フィッシングサイトへおとりの情報を送り込み、金融機関と協力し、それを追跡して犯罪者の活動を察知
    - そして、たとえば、犯罪者がおとりの情報を使い口座にアクセスしようとした際にブロック

出典:RSAセキュリティ株式会社
http://japan.rsa.com/products/consumer_solutions/fraudaction/FRA_DS_060-J.pdf

3. フィッシングとドメイン名の関係

フィッシングにおけるドメイン名の関わり



出典：フィッシングの手口（フィッシング対策協議会）
http://www.antiphishing.jp/doc/aboutphishing.html

フィッシングメールのFromアドレスに関して(1/2)

- メールアドレス
  - 正規の金融機関のドメイン名を使用
    - Fromアドレスを正規の金融機関のドメイン名に書き替え
  - 正規の金融機関名と思しきドメイン名を使用
    - 実在するドメイン名
      - 実際にドメイン名を登録し、それを使用
    - 実在しないドメイン名
      - うそのドメイン名を使用

フィッシングメールのFromアドレスに関して(2/2)

ケース		対策	
		実在するかどうかをWhoisで調べる	返信をしてみて、返信可能かどうか調べる
正規の金融機関のドメイン名を使用 (Fromアドレスを正規の金融機関のドメイン名に書き替え)		・正規の金融機関が登録者であると表示されるため、正規の金融機関からのメールであると誤認する可能性が高い。	・メールアドレスが実在すれば、正規の金融機関へ返信されるため、金融機関側はフィッシングサイトが立ち上がっていることがわかる。その金融機関からの連絡により、もとのメールを受け取った人もフィッシングであることがわかる。 ・メールアドレスが実在しなければ、メールを受け取った人にエラーメールが返るため、正規の金融機関からのメールではないことがわかる。 ・正規の金融機関からの返信がない場合、メールを受け取った人はフィッシングであるかどうかの判断が出来ない。
正規の金融機関と思しきドメイン名を使用	実在するドメイン名	・正規の金融機関とは登録者が異なるため、フィッシングである可能性が高いことがわかる。	・メールを返信したら不正者に届いてしまうため、もとのメールを受け取った人はフィッシングであるかどうかの判断が出来ない。
	実在しないドメイン名	・登録がないため、フィッシングである可能性が高いことがわかる。	・メールを返信した人にエラーメールが返るため、正しいメールアドレスでないことがわかる。

フィッシングサイトのURLに関して(1/3)

- URL
  - よく似たドメイン名
    - 「olbank.jp」(オーエル)と「01bank.jp」(ゼロイチ)
  - Web上のリンクドメイン名隠し
    - フィッシングメールがHTMLの場合、表示上で実際のURL(フィッシングサイトのURL)を隠すことが可能
  - Web乗っ取り
    - 正しいURLであるが、Webサイトそのものを乗っ取る

フィッシングサイトのURLに関して(2/3)

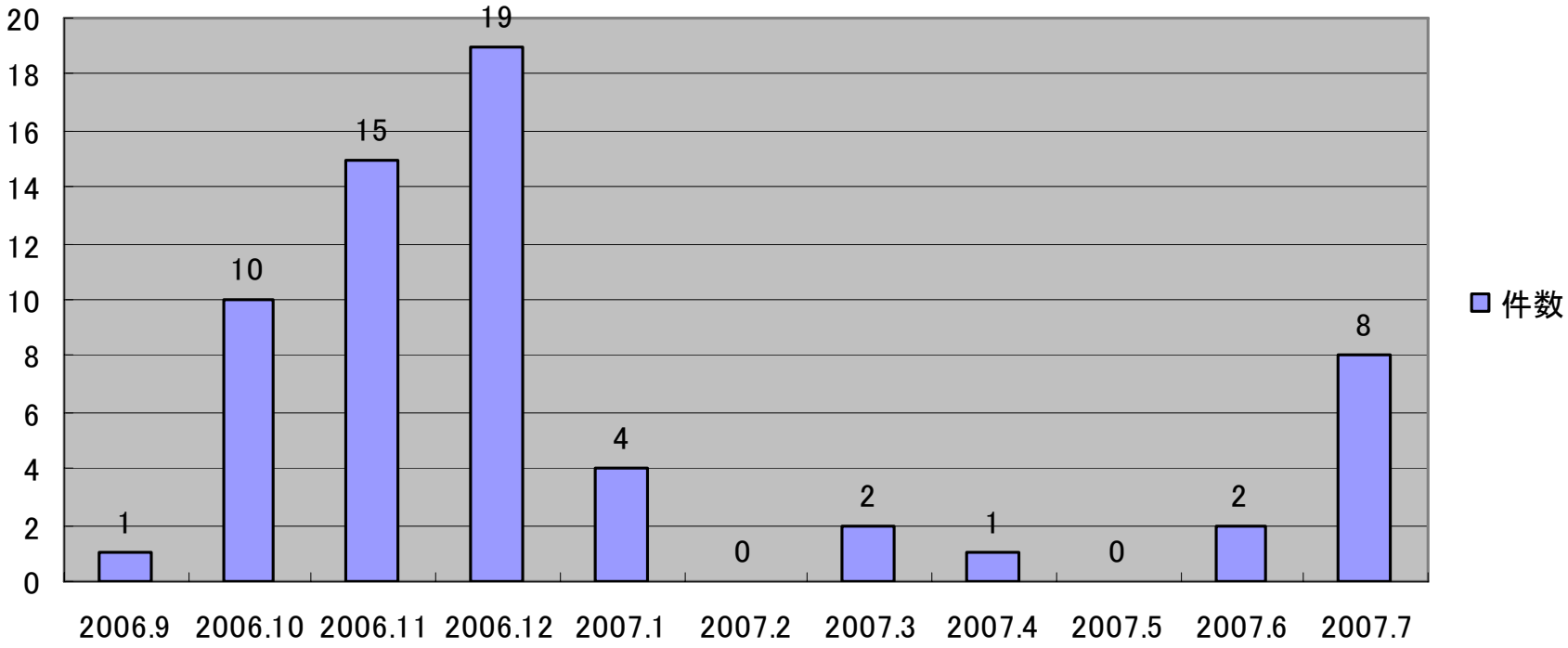
- URLを基軸にどういった対応ができるのか。
  - 事前
    - フィッシングサイトになる可能性のあるドメイン名を事前にチェックして
      - 登録させない
      - 登録されたら発見してアラートをあげる
  - 事後
    - フィッシングサイトが見つかったら
      - ドメイン名を削除
      - ドメイン名のネームサーバを削除
      - フィッシングサイトのサーバを撤去
      - フィッシングサイトのコンテンツを削除

フィッシングサイトのURLに関して(3/3)

対策		効果	限界
(事前対応) フィッシングサイトになる可能性のあるドメイン名を事前にチェックして	登録させない	・ドメイン名自体が登録されないため、そのドメイン名を使ったフィッシングサイトが立ち上がることはない。	・「フィッシングサイトになる可能性のあるドメイン名」を事前に網羅的にリストアップすることは不可能。
	登録されたら発見してアラートをあげる	・フィッシングサイトが立ち上がる前にドメイン名を削除もしくは一般向け注意喚起が可能である。	・アラートをあげるタイミングによっては、あがってきた時点で既にフィッシングサイトが立ち上がっている可能性がある。
(事後対応) フィッシングサイトが見つかったら	ドメイン名を削除	・削除後、そのドメイン名を使ったフィッシングサイトが立ち上がることはない。	・DNSのキャッシュが残るため、即効性がない。
	ドメイン名のネームサーバを削除	・削除後、そのフィッシングサイトにはアクセスできなくなる。	・DNSのキャッシュが残るため、即効性がない。 ・ドメイン名は残るため、同じドメイン名で別のフィッシングサイトを立ち上げることを将来にわたり防がねばならない。
	フィッシングサイトのサーバを撤去	・撤去後、そのフィッシングサイトにはアクセスできなくなる。 ・DNSのキャッシュが残っていても、アクセスできなくなる。	・ドメイン名は残るため、同じドメイン名で別のフィッシングサイトを立ち上げることが可能。 ・指定事業者やISPに連絡して対応する必要があり、即時に撤去することは不可能。
	フィッシングサイトのコンテンツを削除	・フィッシングサイトにアクセスしたとしても、カード番号や暗証番号などが騙し取られる可能性はない。	・指定事業者やISPに連絡して対応する必要があり、即時に削除することは不可能。 ・ドメイン名は残るため、同じドメイン名で別のフィッシングサイトを立ち上げることが可能。

JPRSが受け取ったフィッシング対応依頼(1/2)

- JPRSに対して「フィッシングサイトに使われている」という通報があったJPドメイン名の件数



JPRSが受け取ったフィッシング対応依頼(2/2)

- 通報内容の例
  - フィッシング対策サービスを提供している企業、CERT、銀行などから以下のような内容の問い合わせがある
    - ドメイン名「xxxx.jp」を使って、フィッシング行為をしているWebサイトがある。個人の金融に関するデータを盗もうとしているので、すぐにフィッシングサイトを閉鎖してほしい。(管理指定事業者を教えてほしいというケースもある)
    - また、被害者に連絡するため、フィッシングサイトで誤って入力された情報を提供してほしい。

JPRSでの現在の対応

- フィッシングの指摘があった場合
  1. 申告を受ける
     - 当該Webサイトを確認し、Webサイトの画像を保存する。
     - ケースによってはJPCERT/CCと情報共有する。
  2. 当該ドメイン名の管理指定事業者に連絡
     - 連絡しても対応しない場合は、継続して連絡する。
  3. 当該ドメイン名の登録者に通知（メール・文書）
     - 指定事業者が対応しない場合、登録規則に沿った取消を想定し、登録者に登録情報の適切さ確認の依頼を直接行う。
       （実際には、このプロセスで取消を行ったケースはまだ無い）

→ほぼすべてのフィッシングサイトが停止される。

（JPRSからの指摘によるものなのか、別の組織の働きかけによるものなのかは不明）

ドメイン名レジストリの役割

- ドメイン名が世界で一意の文字列となるように登録者からの申請を処理し、それをインターネット上で使用可能とすること

- ドメイン名の文字列の意味やその使用方法には関与しない

  その理由

  – ドメイン名の登録は先願(早い者勝ち)主義であり、登録処理を効率的に行う必要があるが、文字列の意味を審査対象とすると時間がかかる
  – ドメイン名の文字列の妥当性を判断するのは困難
  – ドメイン名が登録された時点ではどのように使用されるかが不明であるため、使用方法に関する審査は不可能

ドメイン名にアクセスできないようにすることの難しさと限界(1/2)

- 対策の難しさ
  - 悪意性の判断ができない
  - レジストリはドメイン名の文字列の意味やその使用方法には関与しない(DRP*を除く)
  - レジストリが指定事業者の頭越しにドメイン名を使用停止とすることは適切でない
  - 一つのドメイン名が複数のURLやメールアドレスに使われている場合、ドメイン名を使用停止とすると悪質なもの以外の通信も不通になる

＊DRP: 商標や商号と同じもしくはよく似たドメイン名の登録・使用を他人が行うことに対し一定の制限をかけるもので、JPドメイン名に対してはその方針をJPNICが策定

ドメイン名にアクセスできないようにすることの難しさと限界(2/2)

- ドメイン名を使用停止にしても、その効果は限定的である。
  - ドメイン名・DNS情報を削除しても、ISPがそのDNS情報のコピーを最大24時間持っているため、インターネットユーザはアクセス可能である。フィッシングサイトは開設されてから数時間以内の被害が大きいと言われているが、この期間の被害を防ぐことができない。
  - フィッシングでは、多くのドメイン名を登録し、多くのURLを作り、それらすべてを同じフィッシングサイトに誘導する方法が用いられている。このため、ひとつのURLを消しても、別のURLから誘導できることとなり、限定的な対応となる。

対策のオプション

マイルドな方法

- 事例を紹介し注意喚起する
- 指定事業者に依頼してフィッシングをやめるよう連絡してもらう
- ドメイン名の悪用を判断する第三者機関を選定し、その機関からの要請に基づきレジストリはアクションを起こす
- 指定事業者レベルでドメイン名を使用停止とする
- レジストリレベルでドメイン名を使用停止とする
- 法律に則り裁く

厳しい方法