「.JP」における
フィッシングの現状と対策

2010年1月

株式会社 日本レジストリサービス(JPRS)
白岩 一光

目次

1. ドメイン名レジストリとは
2. 「.JP」におけるフィッシングの現状
3. ドメイン名レジストリに関連したフィッシング対策

1. ドメイン名レジストリとは

1-1. ドメイン名

ドメイン名とは

- URL（ホームページのアドレス）やメールアドレスなどの一部分として使われており、インターネット上のコンピュータを識別するための名前
- その構成は、ルートを頂点とした階層構造を持っており、文字の並びを"."（ドット）でつなげたもの
- 「.JP」で終わるドメイン名はJPRSが管理

〈直感的には〉

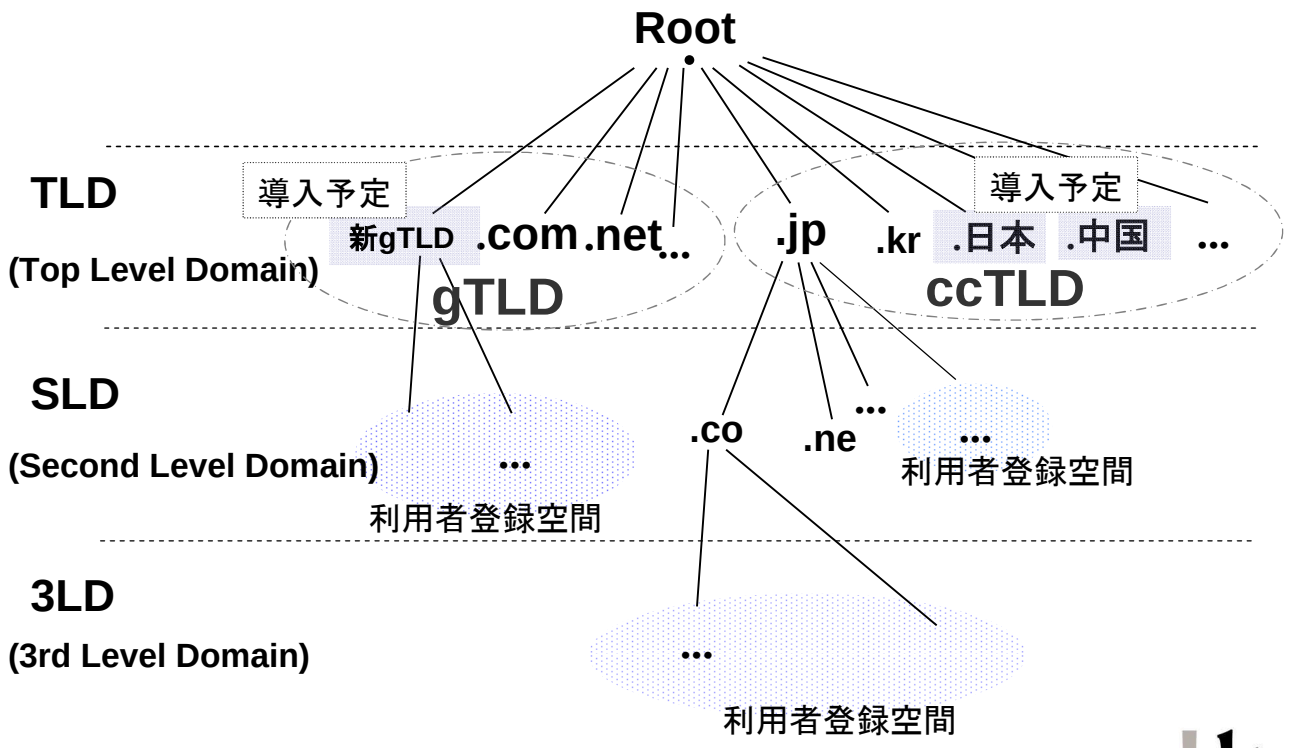
- IPアドレスの代わりに使う「識別子」
- その主な目的は
  - 人間が認知しやすい形式で通信相手を指定すること
  - ISPを変えても、同じ識別子が使えること

ドメイン名の種類

- ドメイン名の見方

- **TLD** (トップレベルドメイン)
  - 今後、数が増えていく
    - 2008年6月のICANNパリ会合にて増やすことを決定
  - **gTLD** (分野別トップレベルドメイン：約20種)
    - .com, .org, .net, .info, .museum, .asia, ...
      - 2010年に新TLDの提案募集開始予定
  - **ccTLD** (国別トップレベルドメイン：約250種)
    - .jp, .uk, .us, ...
      - 2009年11月16日から各国語のTLD（IDNccTLD）をICANNが受付開始。中国、ロシア、エジプトなど16ヶ国が申請。
      - 「.日本」も導入に向けて検討が進んでいる。

ドメイン名の構造



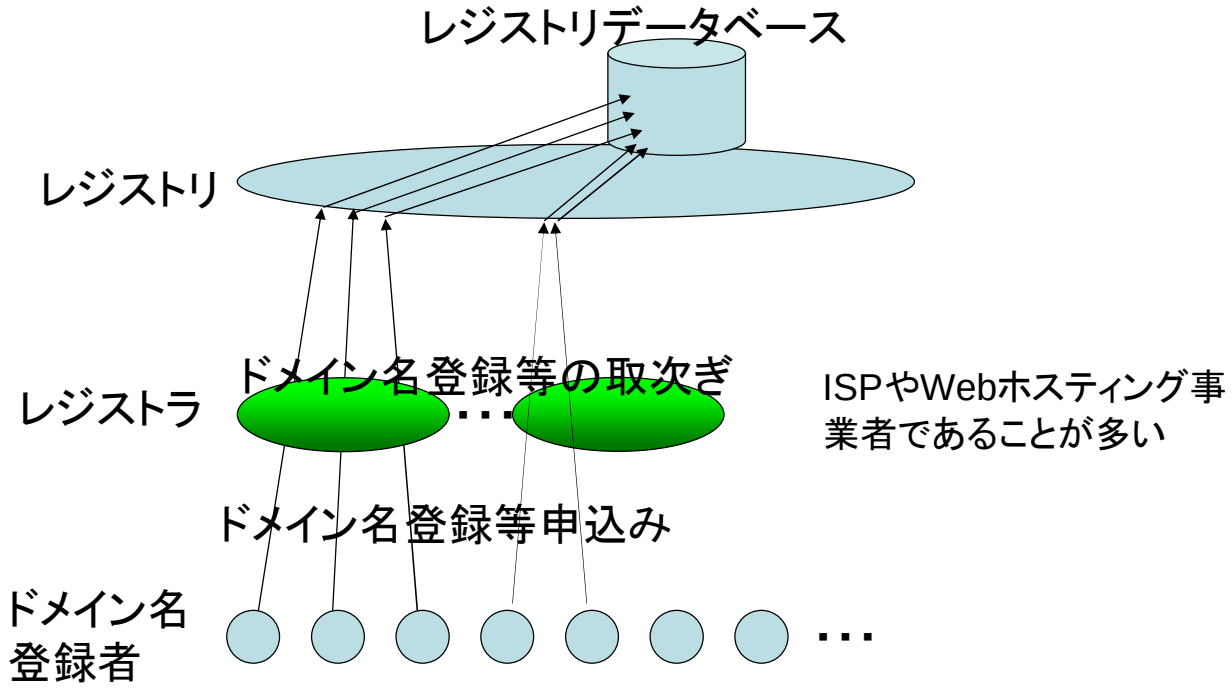
1-2. ドメイン名レジストリ

ドメイン名レジストリとは

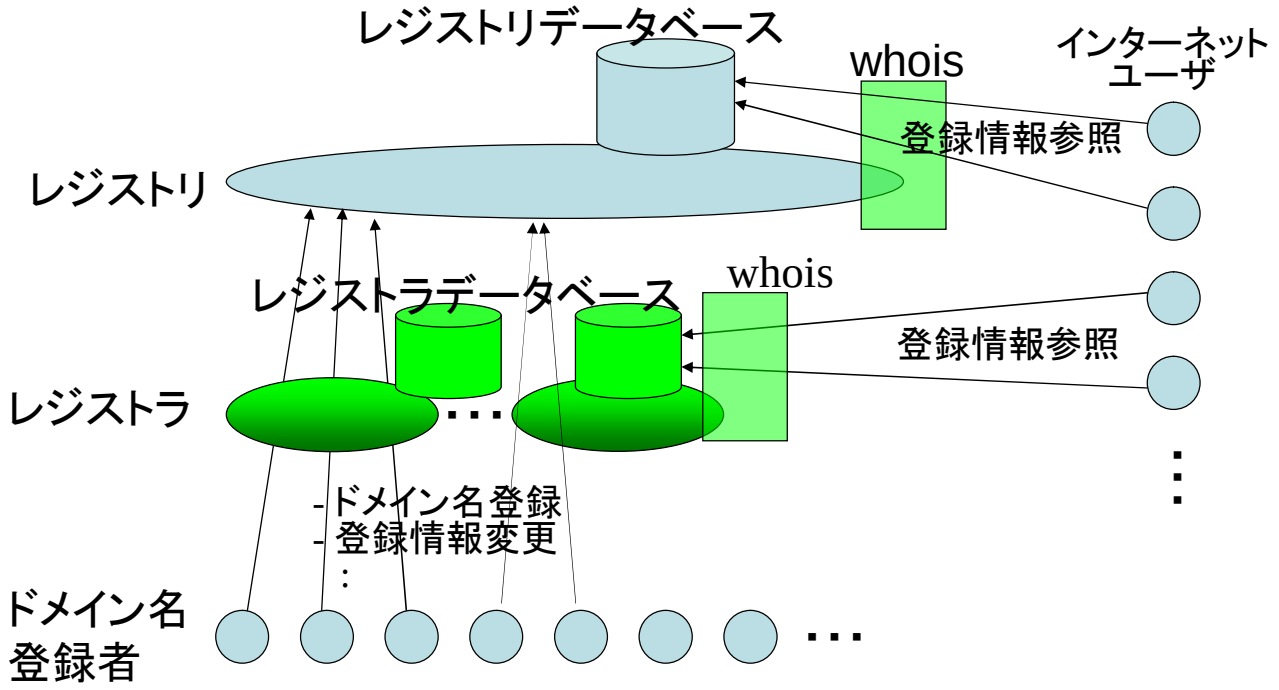
- ドメイン名レジストリとは
  - TLD毎にレジストリが1組織存在
  - レジストラを介して、SLD(例: ○○.jp), 3LD(○○.co.jp)等へのドメイン名の登録をサービスする
- ドメイン名レジストリの大きな役割は2つ
  - レジストリデータベース管理業務 (data entry function)
    - インターネット上で、ドメイン名が一意となるようにチェック
    - 新しいドメイン名をレジストリデータベースに登録
    - 各ドメイン名の登録者や有効期限などを管理
  - ネームサーバ運用業務 (name server function)
    - ドメイン名がインターネット上の電子メールアドレスやURLとして利用可能となるようにDNS(ドメイン名システム)を運用

レジストラ: ドメイン名登録者の代理として振舞い、登録申請等をレジストリに取り次ぐ。レジストラを持たないTLDもある。また、JPドメイン名の場合「指定事業者」と呼ぶ。

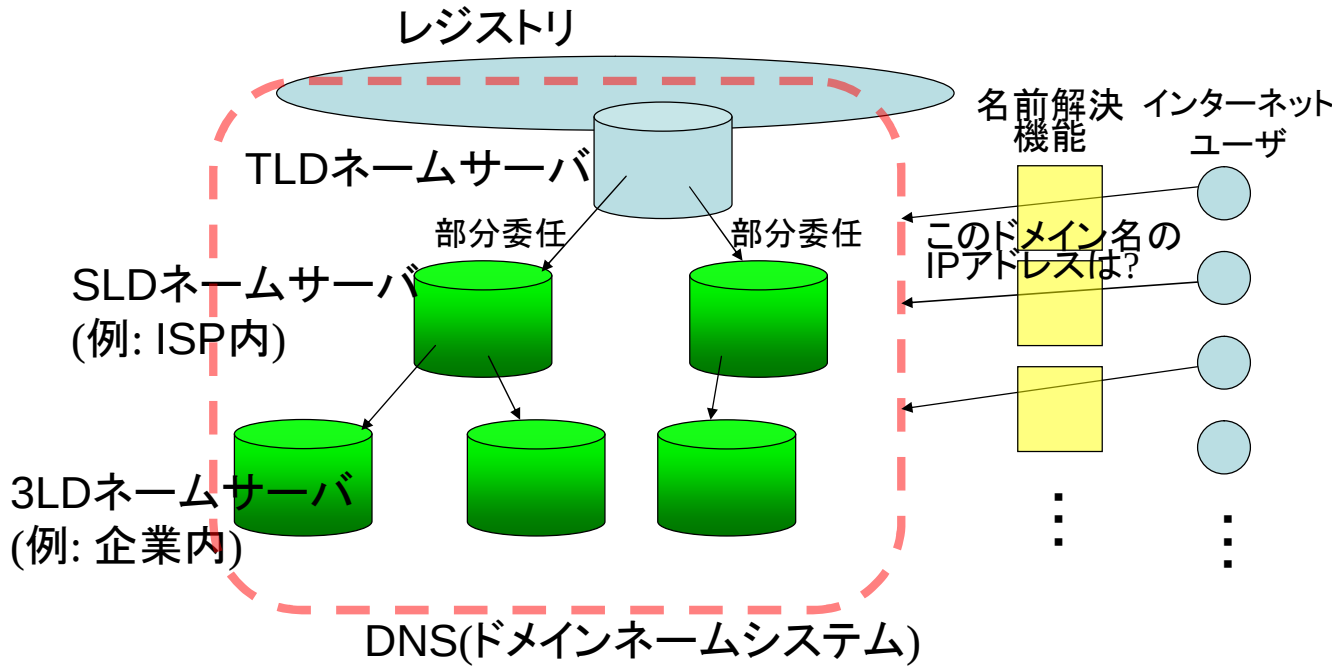
レジストリとレジストラ



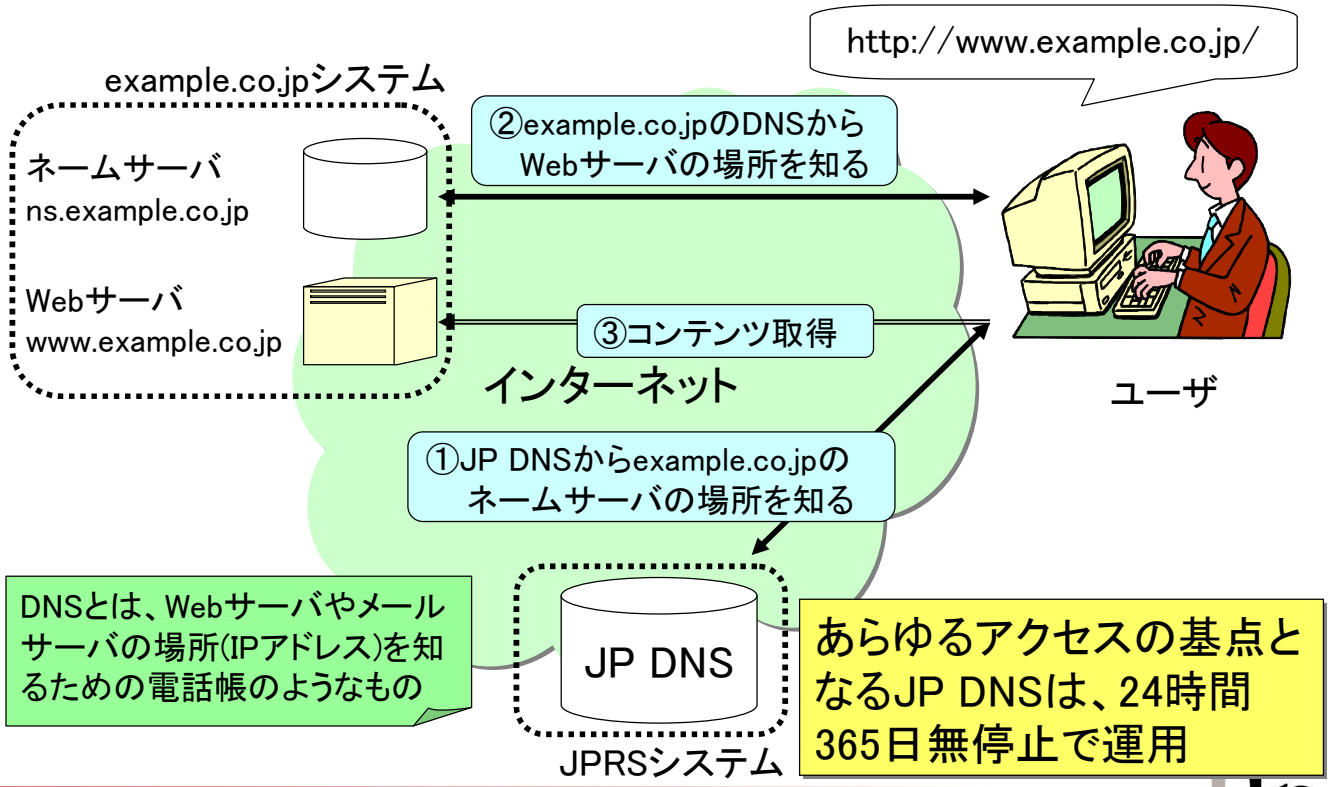
レジストリデータベース管理業務



ネームサーバー運用業務



DNSの役割（Web閲覧の例）



Whois

- レジストリデータベース管理業務の付随的サービス
  - サービスへの入力
    - ドメイン名
  - サービスからの出力
    - 個々のドメイン名の登録日や、登録期限、登録者、ネームサーバの名前、などを表示 (TLD毎に出力項目は若干異なる)
  - 主な用途
    - ネットワークの安定的運用を実施する上で、技術的な問題発生の際の連絡のために必要な情報を提供
    - ドメイン名の申請・届け出時に、同一ドメインや類似ドメインの存在を確認するために必要な情報を提供
    - ドメイン名と商標等に関するトラブルの自律的な解決のために必要な情報を提供

Whois情報は誰が持っているのか

- Thick registryの場合 (例: .jp)
  - レジストラが自分の顧客のドメイン名に関する情報を集め、それをレジストリに渡す
  - レジストリがその情報を保持し、Whoisサービスを使ってインターネット上に公開する
- Thin registryの場合 (例: .com)
  - レジストラが自分の顧客のドメイン名に関する情報を集める
  - レジストラがその情報をWhoisサービスを使ってインターネット上に公開する

ドメイン名レジストリの役割の基本的考え方

- レジストリは、ドメイン名に関する申請を受け付けて
  - そのドメイン名の一意性を確認

    ==> レジストリデータベース管理業務
  - そのドメイン名をインターネット上で利用可能にする

    ==> ネームサーバ運用業務

- レジストリは、ドメイン名の文字列の意味や利用方法に関与しない
  - これらに関与することは、ドメイン名を申込み順に与えることによる効率的で柔軟なドメイン名利用を阻害
  - ドメイン名の意味や利用方法の不適切さを判断することはほとんど不可能
  - ドメイン名登録時にその利用方法の適切さを判断することは不可能

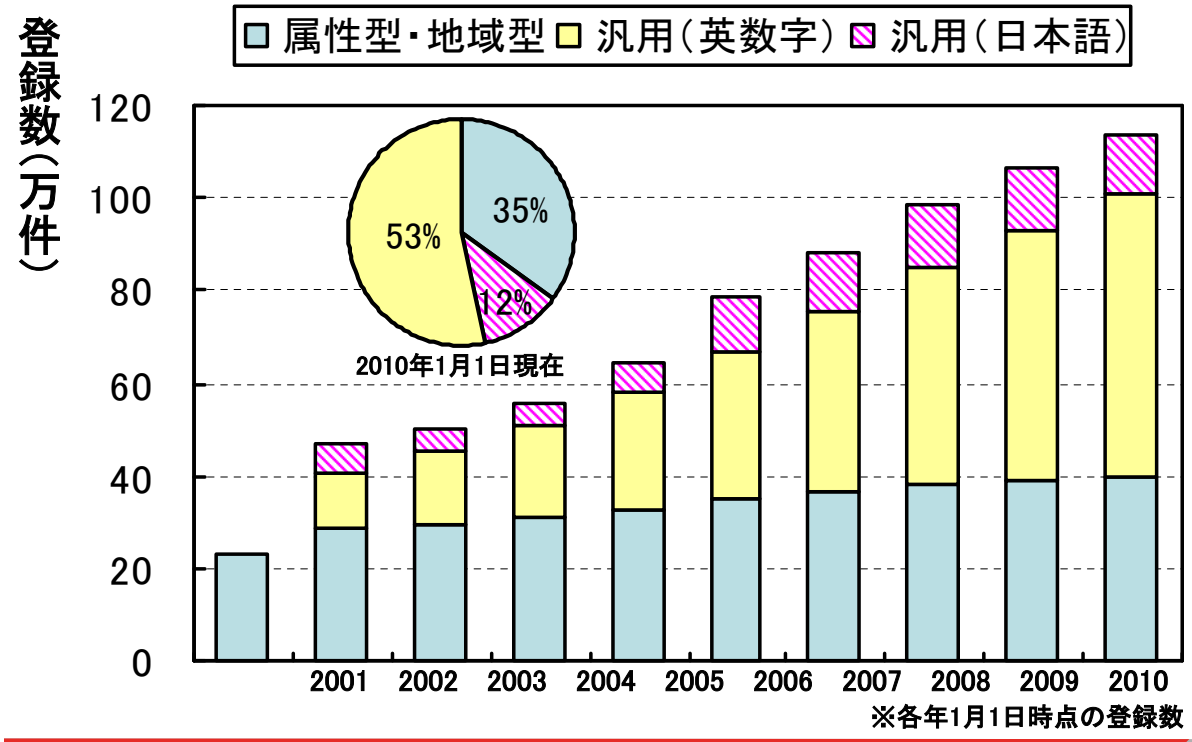
1-3. JPドメイン名の状況

JPドメイン名の種類と登録数（2010/1/1現在）

属性型・地域型JPドメイン名（合計：399,339）		
○○.AD.JP	JPNIC会員	274
○○.AC.JP	大学など高等教育機関	3,528
○○.CO.JP	企業	334,755
○○.GO.JP	政府機関	791
○○.OR.JP	企業以外の法人組織	25,658
○○.NE.JP	ネットワークサービス	16,987
○○.GR.JP	任意団体	8,024
○○.ED.JP	小中高校など初等中等教育機関	4,562
○○.LG.JP	地方公共団体	1,876
地域型	地方公共団体、個人等	2,884
汎用JPドメイン名（合計：740, 820）		
○○.JP	組織・個人問わず誰でも（英数字によるもの）	607,066
□□.JP	組織・個人問わず誰でも（日本語の文字列を含むもの）	133,754

総計　1,140,159

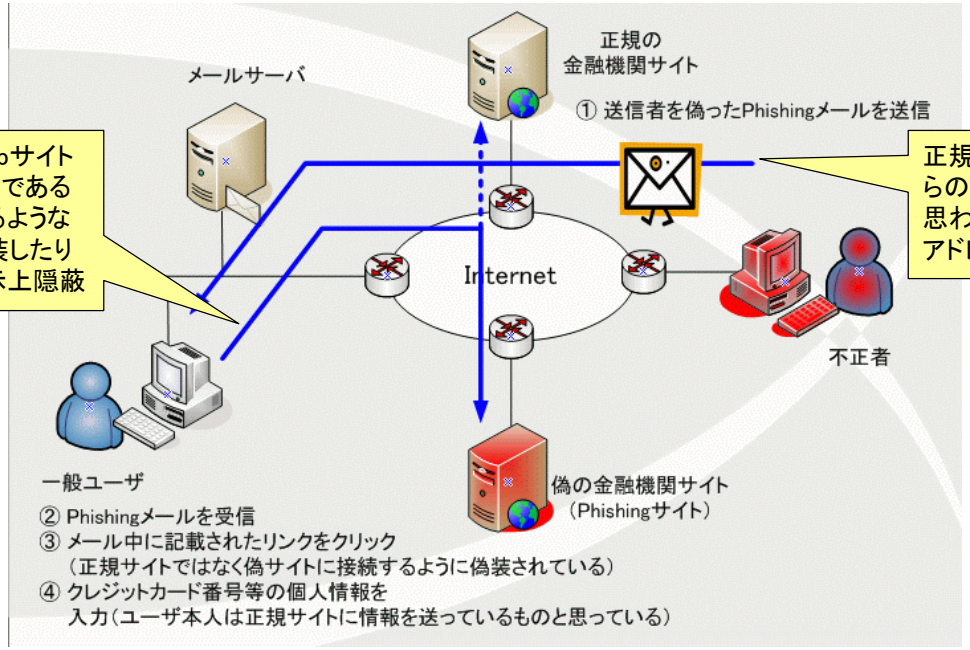
JPドメイン名の登録数推移（2010/01/01現在）



2.「.JP」におけるフィッシングの現状

2-1. フィッシングとドメイン名の関わり

フィッシングにおけるドメイン名の関わり



元図の出典：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

- 正規の金融機関のドメイン名を使用
  - Fromアドレスを実在する正規の金融機関のドメイン名に書き替えてメール送信
- 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

フィッシングサイトのURLに関して

（1）正規の金融機関とよく似たURLを利用

- 正：http://abc-bank.jp/customer/login.html（ドメイン名はabc-bank.jp）
- 偽：http://abc-bank.jp.customer.xxx.xx/login.html（ドメイン名は何でも良い）
  http://xxx.xx/abc-bank.jp/customer/login.html（ドメイン名は何でも良い）

（2）正規の金融機関の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

（3）正規の金融機関とよく似たドメイン名を利用

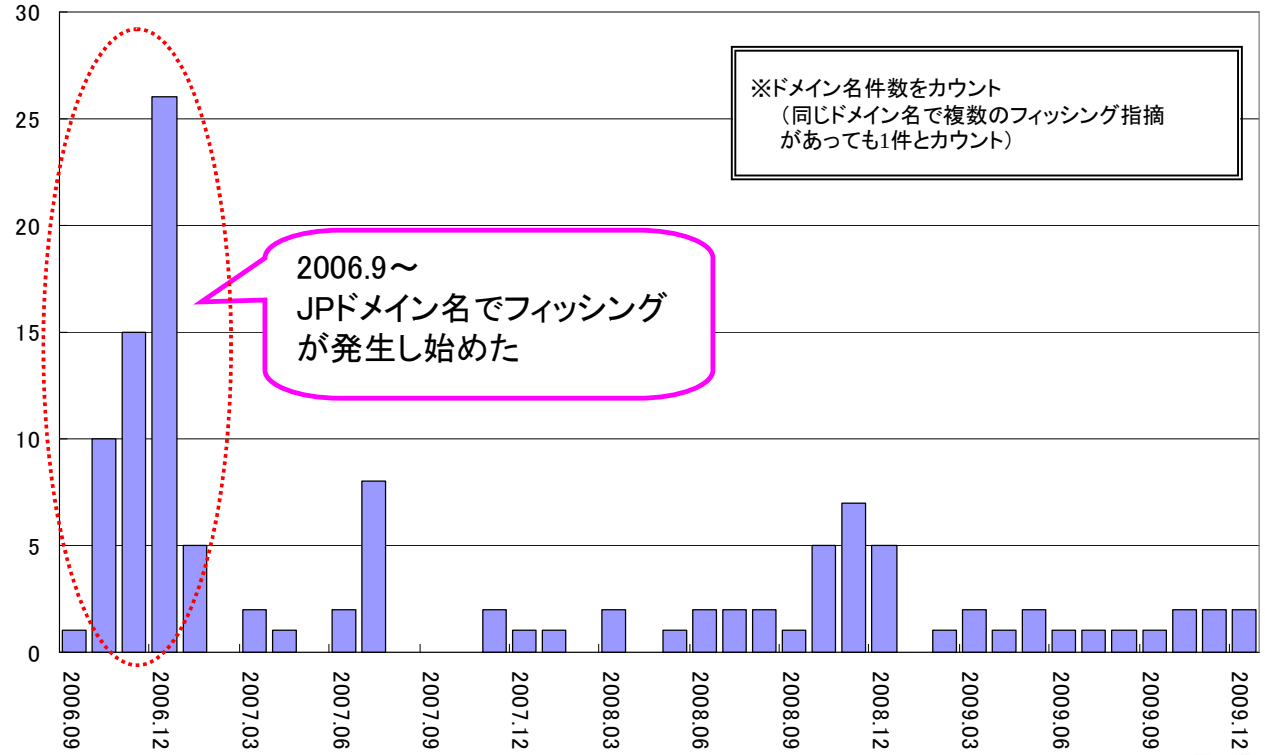
- 「**o**lbank.jp」(オーエル)と「**01**bank.jp」(ゼロイチ)

（4）サイトへのリンクURLを隠す

- フィッシングメールがHTMLメールの場合、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：この場合は、ドメイン名は何でも良い

2-2. JPRSが受けるフィッシング関連の申告

JPRSに問い合わせがあったフィッシング件数（※）



JPドメイン名を利用したフィッシングの傾向

- ターゲットは、海外の金融機関やECサイトが殆ど。

- 2006年の急増時はクラッキングの手口は皆無。
  また、同一レジストラ（リセラ）から登録されたもの。
  ⇒同一組織によるフィッシングと思われる。

- 以降、徐々にクラッキングの割合も増加。
  ターゲットや利用レジストラも複数社に分かれてきた。
  ⇒手口や犯行組織が増えてきている。

JPRSへのフィッシング対応依頼事例

- 依頼者

  フィッシング対策サービスを提供している企業

  銀行などサイトを模倣され、顧客が被害にあっている組織

  国内外CERT

- 依頼内容

  例1：すぐにフィッシングサイトを閉鎖してほしい。
  （「xxxx.jp」を扱っているレジストラを教えてほしい）

  例2：不正行為を行うサイトに利用されているドメイン名を
  即刻登録を取り消してほしい。

  例3：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。(！)

フィッシング申告へのJPRSの対応

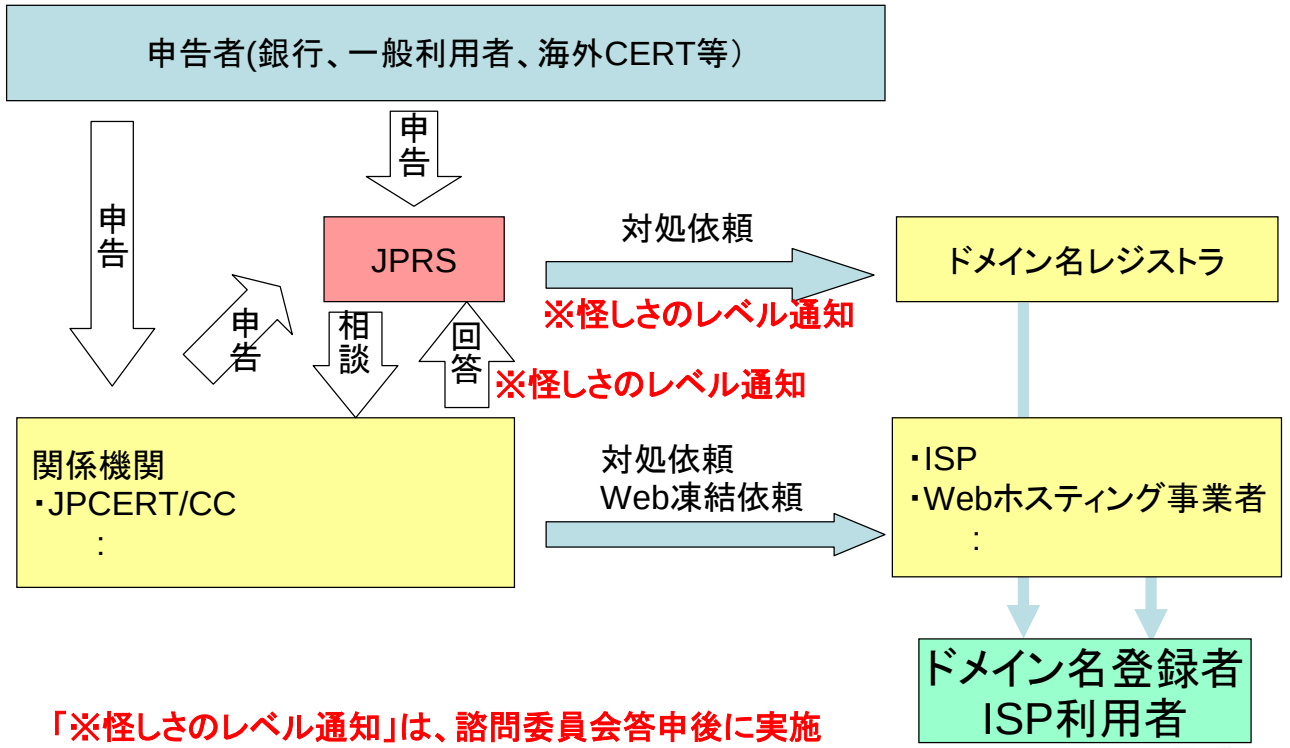
1. JPCERT/CCに共有すると共に、フィッシング確度確認
2. 当該ドメイン名のレジストラに連絡
3. 当該ドメイン名の登録者に通知（メール・文書）

   当該ドメイン名の登録内容が適切でない場合には、登録を取り消すことも可能（※）
   (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)

   ※JPドメイン名登録規則に則った手続
   （ドメイン名登録者は、その住所、氏名等を正確に申告する義務を有し、それに違反した場合は登録資格がないとみなす）

…但し、例3の依頼には対応できない（レジストリには情報が無い）

JPRSのフィッシング対応フロー



「※怪しさのレベル通知」は、諮問委員会答申後に実施

JPRSでの対応の結果

- ほぼすべてのフィッシングサイトが停止される
  - 対象ドメイン名の管理指定事業者からの指摘によるのか、JPCERT/CCなどの別組織からの働きかけによるのかは不明
  - 停止に至る代表的な要因
    - Webを乗っ取った者によって引き起こされたフィッシングの場合、ユーザーに連絡すれば、適切な対処をして正しいWebに置き換えられる
    - ISPやWebホスティング事業者が、そのユーザーに連絡しようとして、実在しない虚偽ユーザであることが発覚する
    - ISPやWebホスティング事業者がユーザーと交わしている契約の中に「不適切なコンテンツは削除する」との条項があり、それに抵触したとみなす

3. ドメイン名レジストリに関連した フィッシング対策

対策1：Whoisで正しい相手か確認 by ユーザ

- レジストリ、レジストラが提供するWhoisサービスを用いることにより、ドメイン名の登録者が表示される
- 限界
  - Webサイトが乗っ取られている場合
  - whoisの内容が虚偽の場合
  - 登録代行サービスの場合

登録代行サービス: 実際にドメイン名を使用する者に代わってドメイン名を登録するサービス (名前貸しや又貸し)

Whois情報の表示例 (JPドメイン名の場合1)

```
Domain Information: [ドメイン情報]
[Domain Name]                   JPRS.JP

[登録者名]                      株式会社日本レジストリサービス
[Registrant]                    Japan Registry Services Co.,Ltd.

[Name Server]                   ns01.jprs.jp
[Name Server]                   ns02.jprs.jp
[Name Server]                   ns03.jprs.jp

[登録年月日]                    2001/02/02
[有効期限]                      2010/02/28
[状態]                          Active
[最終更新]                      2009/11/17 14:47:28 (JST)

Contact Information: [公開連絡窓口]
[名前]                          株式会社日本レジストリサービス
[Name]                          Japan Registry Services Co.,Ltd.
[Email]                         dom-admin@jprs.co.jp
[Web Page]
[郵便番号]                      101-0065
[住所]                          東京都千代田区西神田三丁目8番1号
                                千代田ファーストビル東館 13F
[Postal Address]                Chiyoda First Bldg. East 13F,
                                3-8-1 Nishi-Kanda Chiyoda-ku,
                                Tokyo 101-0065, JAPAN
[電話番号]                      03-5215-8451
[FAX番号]                       03-5215-8452
```

Whois情報の表示例 (JPドメイン名の場合2)

```
Domain Information: [ドメイン情報]
[ドメイン名]                    白岩一光.JP
[Domain Name]                   XN--4GQX3FT2NW4Z.JP

[登録者名]                      白岩一光
[Registrant]                    shiraiwa kazumitsu

[Name Server]

[登録年月日]                    2010/01/17
[有効期限]                      2011/01/31
[状態]                          Active
[最終更新]                      2010/01/17 15:13:05 (JST)

Contact Information: [公開連絡窓口]
[名前]                          日本レジストリサービス JPDirect
[Name]                          Japan Registry Services JPDirect
[Email]                         public-contact@jpdirect.jp
[Web Page]
[郵便番号]
[住所]
[Postal Address]
[電話番号]                      03-5215-8456
[FAX番号]
```

ドメイン名登録情報の開示サービス
(JPドメイン名の場合)

- 法執行上の要請
  - 法に従い開示
- 第三者からの開示請求
  - 請求者は、請求理由を明示する必要がある
  - レジストリは、請求理由が次の一つでなければ開示しない
    - JPドメイン名の申請・届け出のため
    - ネットワークの運用やJPドメイン名の登録に関するトラブルの自律的な 解決のため
    - JPドメイン名の登録が、規則に定められたとおり行われていることを示 すため
- 開示対象情報
  - whoisで得られる以上の下記情報
  - 電子メールアドレス、住所、連絡担当者名、連絡担当者住所、連絡担当者ファックス番号、...

登録情報開示サービスを持たないTLDも多い

対策2：危険ドメイン名の登録を事前排除 by レジストリ+レジストラ

- ドメイン名登録を拒絶
  - 登録時に不正な使われ方をするかどうかを判断することは一般に不可能
  - せいぜい、商標と一致(もしくは類似)する文字列がドメイン名として登録されたら商標権者に通知し、適切な登録か否かを商標権者が確認する程度
    - この場合でも、ドメイン名登録を拒絶することはできず、危険性を公表したり、DRP(後述)を申し立てて使用を差し止めたりするしかない

対策3：フィッシングに使われたサイトを停止 by レジストリ+レジストラ

- 不正使用発見後に削除する方法
  - DRP(ドメイン名紛争処理方針)や裁判でドメイン名を取り上げ
    - 商標と一致(もしくは類似)する文字列がドメイン名として登録・利用された場合、商標権者の訴えによりドメイン名を移転もしくは使用差し止めすることが可能
      - DRP - 数十日レベルでの解決
      - 裁判 - 数ヶ月～数年レベルでの解決
  - フィッシングサイトを停止
    - ドメイン名を削除
    - ドメイン名とネームサーバの関係を切り離し
    - ネームサーバを削除
    - 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サーバを撤去

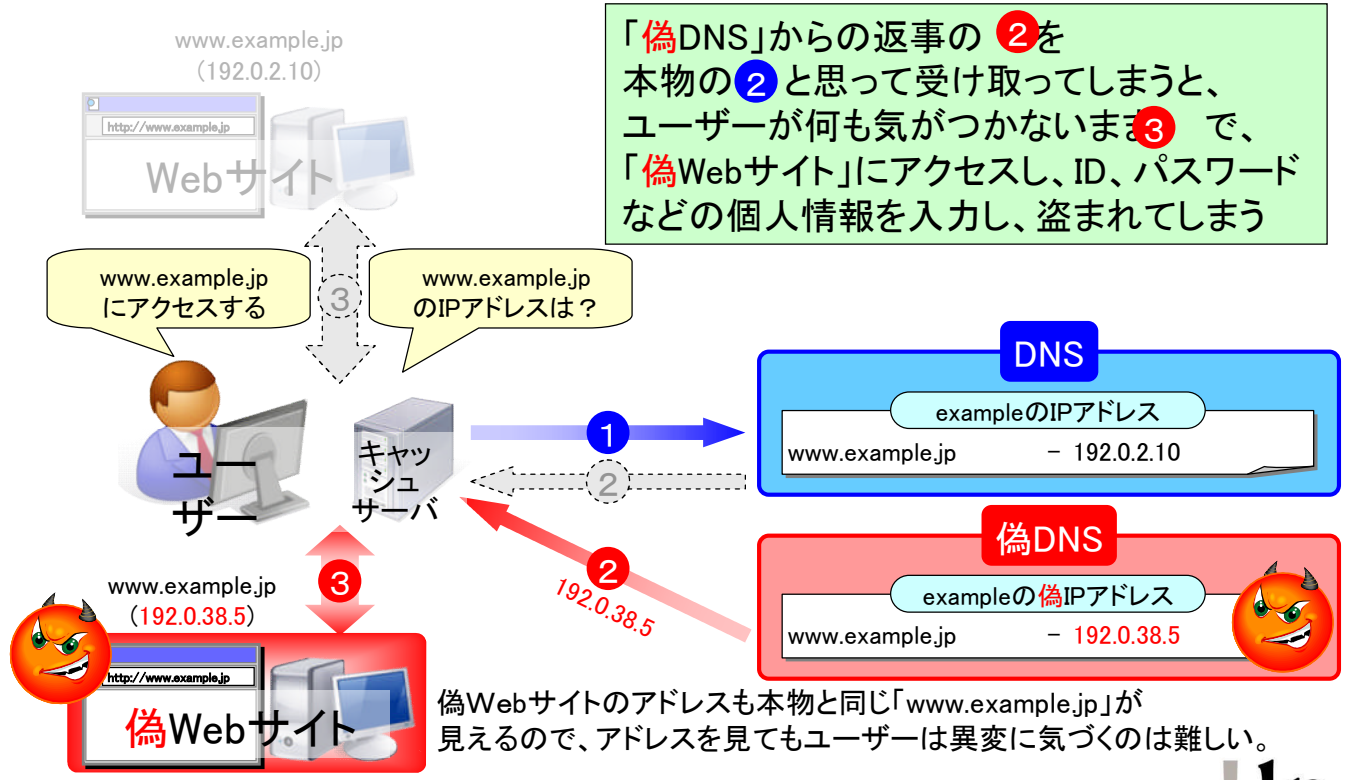
：

DRP：自分の商標や商号等と同一または類似のドメイン名が不正に登録・使用された場合、そのドメイン名の取上げを申立てる裁判外紛争解決手段

対策4：DNS応答の偽装による誤誘導を事前排除 by レジストリ+レジストラ+ユーザー

- DNSSECの導入
  - DNSの応答が改ざんされていないか検証可能
    - DNS応答の偽装を排除
  - JPドメイン名については2010年内導入予定
  - ただし、DNSSECは世界的にも新しい技術であり、普及はこれから。また、サービスの運用などもこなれていない。

DNSを悪用したフィッシングの手口

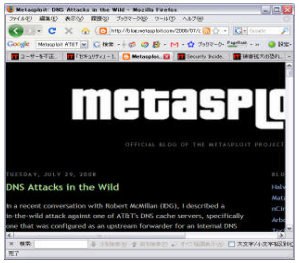


「偽DNS」からの返事の 2 を
本物の 2 と思って受け取ってしまうと、
ユーザーが何も気がつかないまま 3 で、
「偽Webサイト」にアクセスし、ID、パスワード
などの個人情報を入力し、盗まれてしまう

偽Webサイトのアドレスも本物と同じ「www.example.jp」が
見えるので、アドレスを見てもユーザーは異変に気づくのは難しい。

DNS毒入れによる被害実態

- AT&T
  - 2008/7/29にmetasploitブログにて報告.(脆弱性(非公式)公開の1週間後)
  - 汚染先:広告サイト



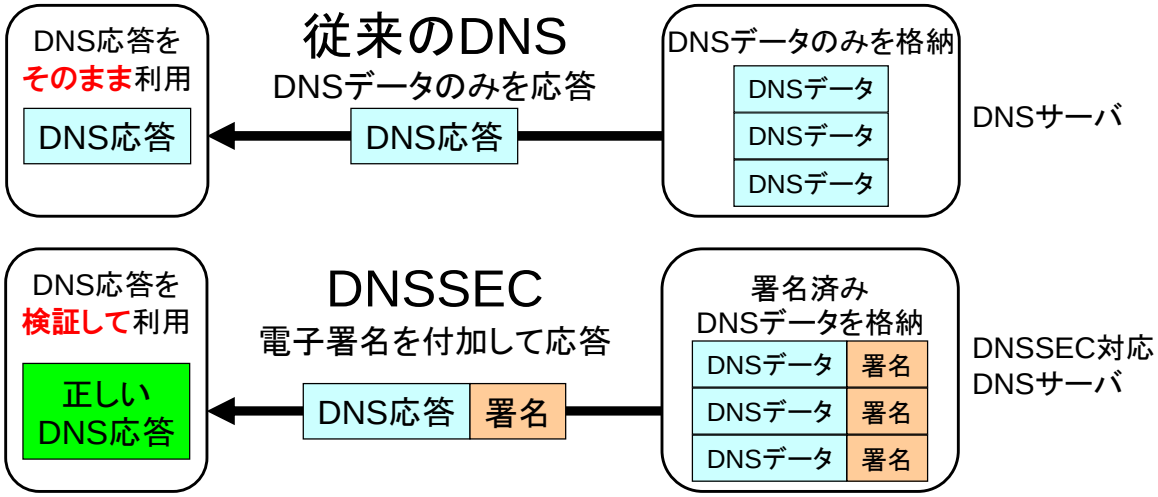
http://blog.metasploit.com/2008/07/on-dns-attacks-in-wild-and-journalistic.html

- 中国大手ISP
  - 2008/8/21にwebsense社ブログにて報告
  - 汚染先:マルウェアダウンロードサイト

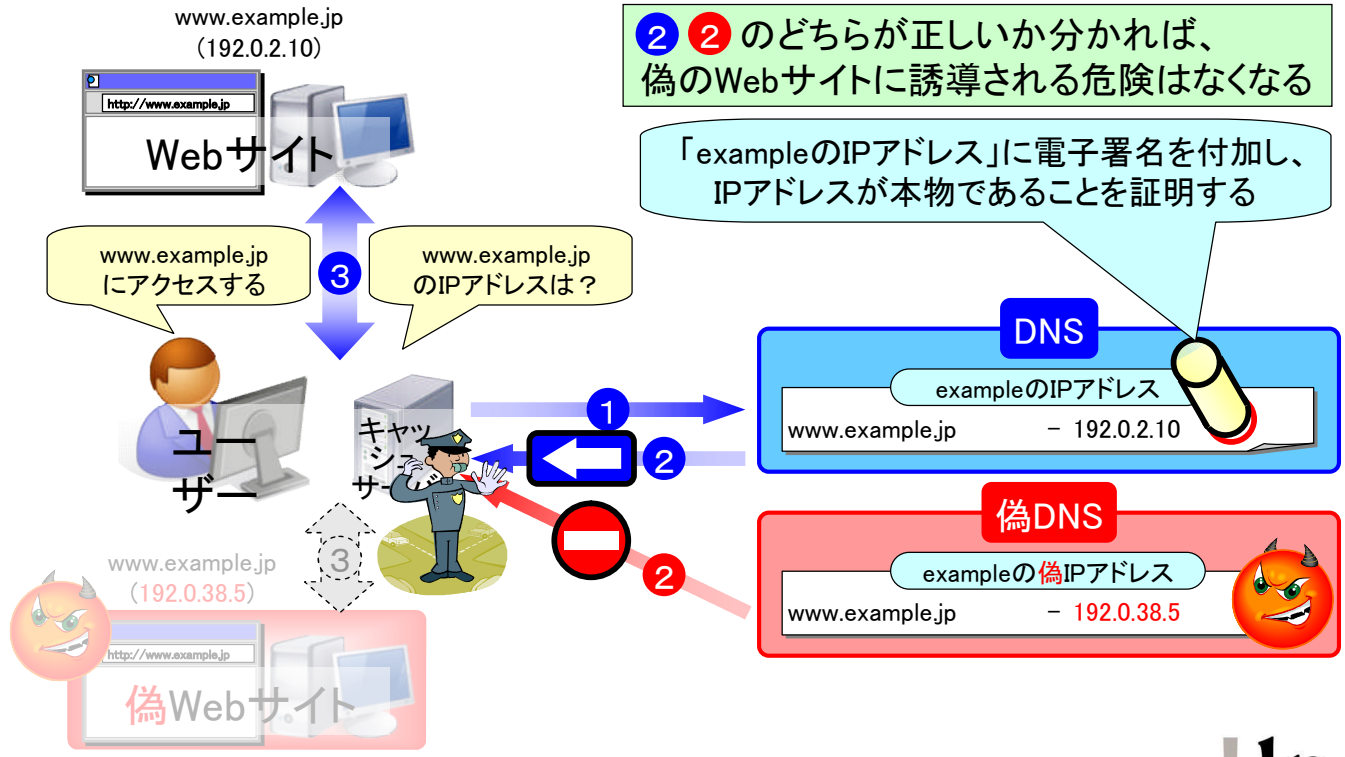
http://securitylabs.websense.com/content/Alerts/3163.aspx

DNSSECとは

- DNSサーバが応答に電子署名を付加し出自を保証
- 問合せ側でDNS応答の改ざんの有無を検出できる



DNSSEC導入後



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)
  - レジストリがレジストラ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にすると、悪質なもの以外の通信も不通になる
    - 例：ISPの一利用者が悪いからといって、ISPのドメイン名を停止できるか？
  - ネームサーバやフィッシングサイトのアドレスを短時間で切り替える攻撃(fast fluxと呼ばれる)を使ったフィッシングでは、ネームサーバの削除や切り離しは効果がない

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・ネームサーバ情報を削除しても、ISPがそのネームサーバ情報のコピーを長時間(たとえば24時間)持っている(キャッシュと呼ばれる)ため、その期間、インターネットユーザはそのドメイン名を持つWebサイトに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。

JPドメイン名諮問委員会の勧告 (諮問への答申)

- JPドメイン名諮問委員会
  - JPドメイン名の方針に関する助言を行う委員会
  - JPRS外部の有識者6名(レジストラ、企業利用者、一般利用者、学識経験者、ISP、JPNICより1名ずつ)からなる
- 答申(2008年3月18日)の概要
  - CERTやISP等関連機関と協力しフィッシング防止の啓発を行うこと
  - 現時点のJPRSの対応は適切である
    - レジストリがドメイン名が持つ意味やWebコンテンツに関わらないこと
    - フィッシング事象が発生した場合、ドメイン名登録者を代理するレジストラに対処を依頼すること
  - 重大かつ緊急な事態に対応できるようにするため、次を準備すること
    - 個別フィッシング事象への対策を判断する機関の設立を関連機関と検討
    - 上記判断に従い緊急的にドメイン名を使用停止とする仕組みを検討
  - http://jprs.co.jp/advisory/00/JPRS-ADVRPT-2007001.pdf

参考:「.jp」の安全度

「.jp」はMcAfee, Inc.が2009年12月2日に発表した調査報告書「危険なWebサイトの世界分布」の中で、世界で最も安全な国別ドメイン（ccTLD）であると評価された。（危険＝セキュリティリスクがあるWEBサイトが多い）

.jpについては過去3年間の調査により非常に安全なTLDであることが認められている。

.cmについては、comのタイポスクワッティングを目的とした登録と思われる。危険度の高いドメイン名は毎年変動しており、手口の変動の裏返しとも言える。

安全な国別ドメインランキング

（危険度の低い順）

国名または名前	ランキング
.gov	1
.jp（日本）	2
.edu	3

（危険度の高い順）

国名または名前	ランキング
.cm（カメルーン）	104
.com	103
.cn(中国)	102

※「危険なWebサイトの世界分布」（マカフィー発表）より引用

Q&A