

事例3: 銀行を騙った情報詐取

このメールは「三菱東京UFJ銀行」からのものです。宛先: [redacted]@biglobe.ne.jp

2014年9月29日 15:18

こんにちは！
最近、利用者の個人情報が一部のネットショップサーバに不正取得され、利用者の個人情報漏洩事件が起きました。
お客様のアカウントの安全性を保つために、「三菱東京UFJ銀行システム」がアップグレードされましたが、お客様はアカウントが凍結されないように直ちに登録のうえご確認ください。

以下のページより登録を続けてください。
https://entry11_bk_mufig.jp/ibg/dfw/APLIN/loginib/login?_TRANID=AA000_001

---Copyright(C)2014 The Bank of Tokyo-Mitsubishi UFJ,Ltd.All rights reserved---

本人認証サービス

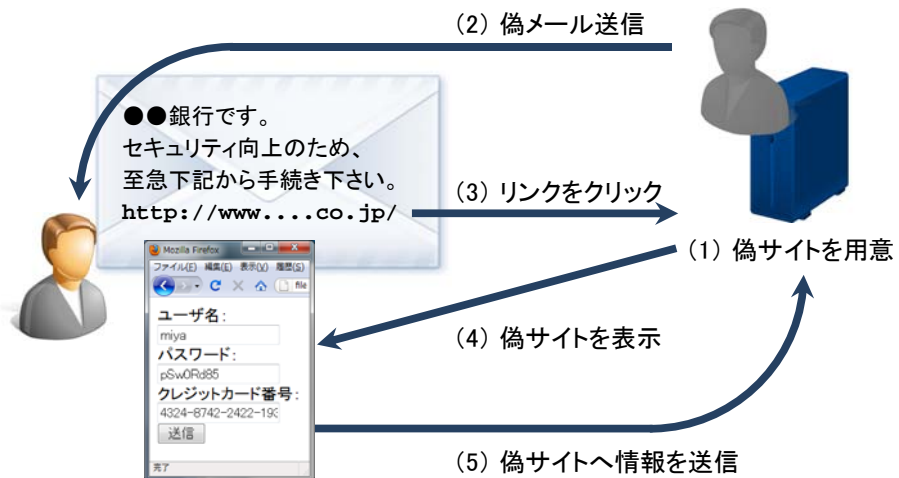
「三菱東京UFJ銀行」ではアカウントの安全性認証を行われるため、お客様はアカウントが凍結・休眠されないように、直ちにアカウントをご認証ください。

事例3: 銀行を騙った情報詐取

クレジットカード番号なんて必要？
⇒ フィッシング詐欺

フィッシング詐欺

本物そっくりの偽サイトへ誘導し、情報を入力させる




事例3: 銀行を騙った情報詐取

偽サイト
<http://61.38.30.55/ib/login/index.htm>
IPアドレス ⇒ 韓国に割り当てられているIPアドレス

正規サイト
[https://www.ufjbank.co.jp/ib/login/...](https://www.ufjbank.co.jp/ib/login/)
UFJ銀行の有する正規のドメイン名 (当時)

事例3: 銀行を騙った情報詐取

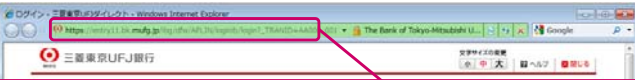
事例3: 銀行を騙った情報詐取



偽サイト

<http://zotworkow.pl/direct.bk.mufig...>

ポーランドを表す国別 **ドメイン名**



正規サイト

<https://entry11.bk.mufig.jp/ibg/dfw/...>

三菱東京UFJ銀行の有する正規の **ドメイン名**

色の違いは問題ではない
(正規サイトが、必ずしも緑色になるとは限らない)



正規ドメイン名と一致する文字列

<http://bk.mufig.jp.nioi.cc/ibg/dfw/...>

オーストラリア領ココス諸島を表す国別 **ドメイン名**

ドメイン名



組織（機器）を識別する文字記号列

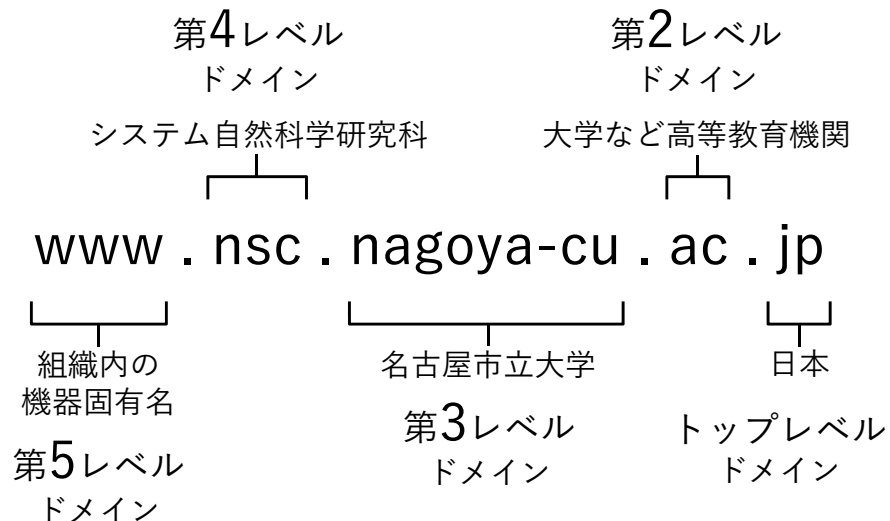
→ インターネット上の住所表示

国、組織の性質などによって階層的に表記



www.nsc.nagoya-cu.ac.jp

ドメイン名



ドメイン名の分類



属性型 JPドメイン

ドメイン名の分類

- ① 属性・ $\left[\begin{array}{l} \text{都道府県名} \\ \text{制令指定都市名} \end{array} \right] \cdot \text{jp}$
pref / metro / city
- ② 属性・市町村名・都道府県名・jp
city / town / vill
-

地域型 JPドメイン

(新規受付は停止)

ドメイン名の分類

なんでもあり.jp

(日本語文字列も使用可)

汎用 JPドメイン

ドメイン名の分類

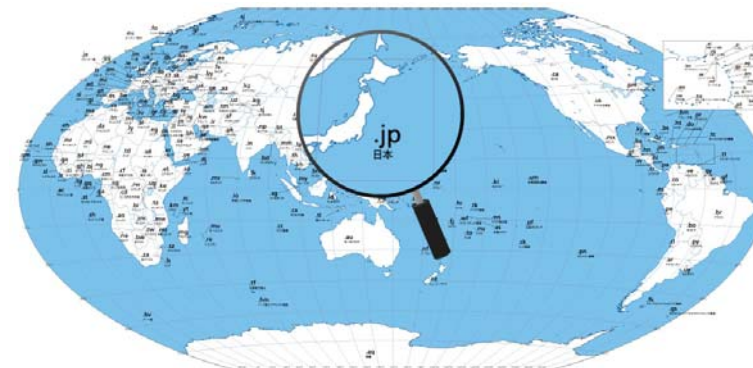
なんでもあり・都道府県名.jp

(日本語文字列も使用可)

都道府県型 JPドメイン

ドメイン名の分類

ccTLD : country code Top Level Domain
(国別トップレベルドメイン)



ISO 3166-1 に基づいた2文字のコード


(マイナビニュース ccTLD MAPより)

ドメイン名の分類

gTLD : generic Top Level Domain
(分野別トップレベルドメイン)

.com **.net** **.org**
(商業組織) (ネットワーク) (非営利組織)

.edu **.gov** **.mil** **.int**
(教育機関) (米国政府機関) (米国軍事機関) (国際機関)

 より多くのTLD導入の必要性

ドメイン名の分類

gTLD : generic Top Level Domain
(分野別トップレベルドメイン)

- 2000年11月 追加
.biz / .info / .name / .pro / .museum / .aero / .coop
- 2005年 追加
.jobs / .travel / .mobi / .cat
- 2006年 追加
.tel / .asia
- 2009年 追加
.post
- 2011年3月 追加
.xxx

gTLDのさらなる拡大

2011年より自由化

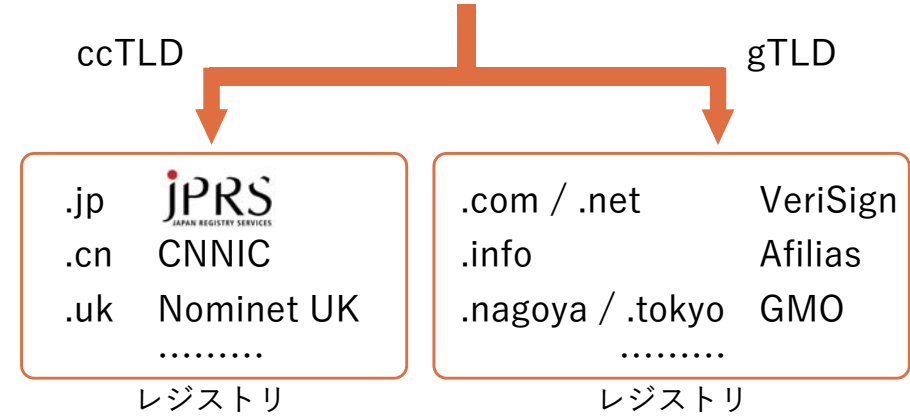
- .canon .sony .ntt .nhk
- .nagoya .nyc .car .game
- .tokyo など

(運用開始は2013年頃～)

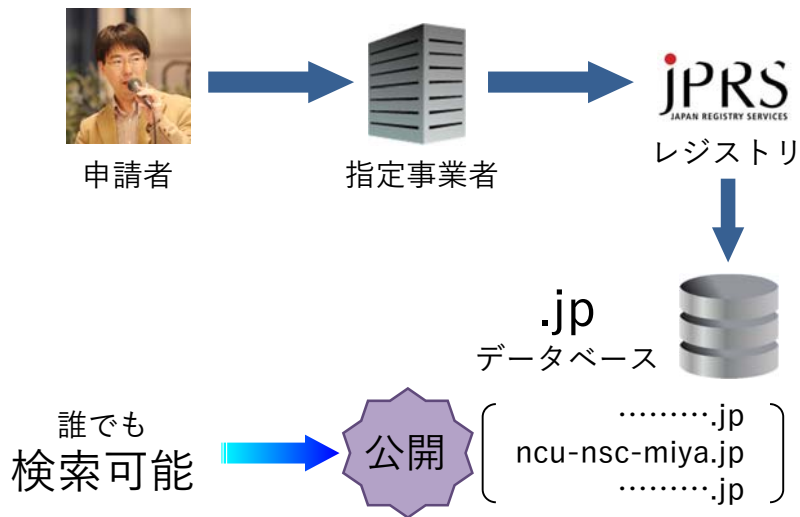
ドメイン管理体制



(Internet Corporation for Assigned Names and Numbers)



ドメインの登録



ドメイン情報の検索



ドメイン情報の検索

検索タイプ: ドメイン名情報
 検索キーワード: nagoya-cu.ac.jp
 検索

IPアドレスとホスト名の対応付け

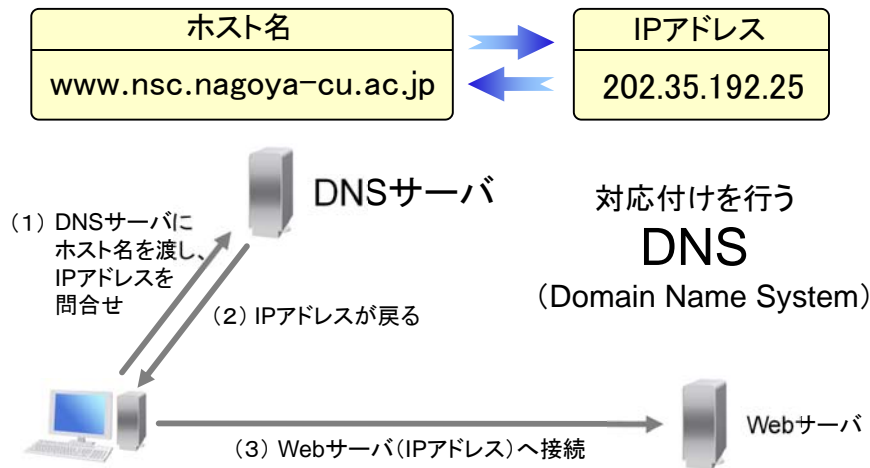
www.nsc.nagoya-cu.ac.jp

ホスト名 によってページを指定
 ↓
 通信の宛先として使用するのは IPアドレス

↓
 変換は?

Webサーバ
 { IPアドレス : 202.35.192.25
 ホスト名 : www.nsc.nagoya-cu.ac.jp }

IPアドレスとホスト名の対応付け = 名前解決



事例3: 銀行を騙った情報詐取

http://zstoworkow.pl/direct.bk.mufig...
 http://61.38.30.55/ib/login/index.htm

↓
 正規ドメイン名を利用していない
 ↓
 良く使うサイトのドメイン名を覚える
 ↓
 ドメインがポーランド割当
 IPアドレスが韓国割当
 ↓
 IPアドレス / ドメイン名の知識
 このサイト、なにかおかしいぞ!

フィッシング詐欺: 対策



本物のサイトとは、何か絶対に違う！



- (1) メールに記載されている Webアドレスを安易にクリックしない
- (2) ブラウザのアドレス欄 (ドメイン名、IPアドレス) を確認
- (3) インターネット以外の通信手段による確認
- (4) 暗号通信 (SSL/TLS) を行っているか確認
- (5) サーバ証明書の確認

手口は年々巧妙になっていく …

まとめ インターネット・必須知識(2)

ドメイン名

- (1) インターネット上で組織を識別
- (2) `example.co.jp` という形式
- (3) 国、組織の性質などにより階層的に分類
- (4) よく利用するサイトのドメイン名は覚えておく