Finding the Banking Trojan in Eastern Asia

Noriaki HAYASHI

Senior Researcher

Forward-looking Threat Research

CeCOS VII - Buenos Aires

APWG

Unifying the Global Response to Cybercrime

Introduction

林　憲明

Forward-looking **T**hreat **R**esearch

- オンライン詐欺
- スマートフォン
- 組込機器 / 車載機器

フィッシング対策協議会
運営委員

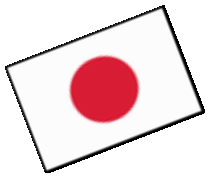
トレンドマイクロ株式会社
シニアリサーチャー

Agenda

1. 背景
2. Banking Trojanの変遷
3. 日本における“Citadel”の報告
4. Mobileを狙った攻撃
5. 協議会による取り組み

Agenda

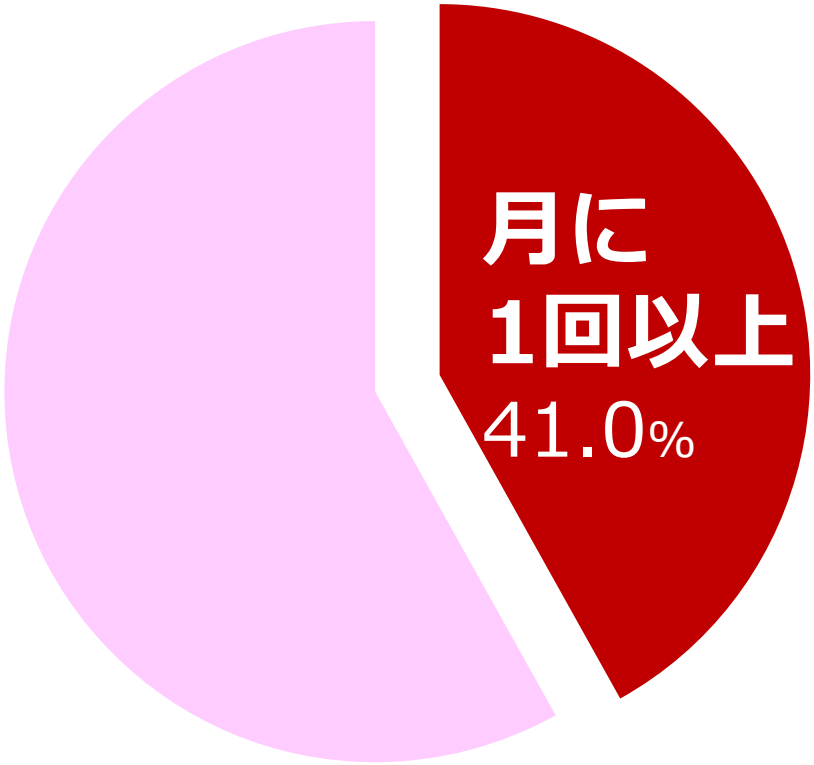
1. 背景
2. Banking Trojanの変遷
3. 日本における“Citadel”の報告
4. Mobileを狙った攻撃
5. 協議会による取り組み



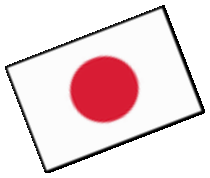
アクセス頻度

オンラインバンキングに関する調査

※出典：楽天リサーチ株式会社(2012/5/29 - 30)、N = 1,000



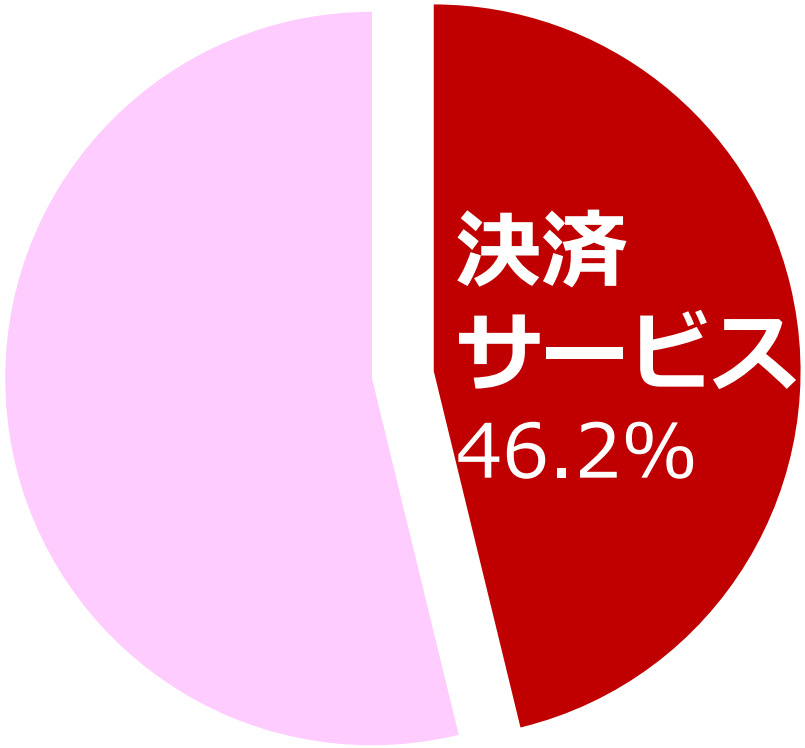
楽天リサーチ http://research.rakuten.co.jp/report/20120621/



アクセス頻度

オンラインバンキングに関する調査

※出典：楽天リサーチ株式会社(2012/5/29 - 30)、N = 1,000



楽天リサーチ http://research.rakuten.co.jp/report/20120621/

日本のインターネットを釣場とする
フィッシャー

言語がフィッシングに及ぼす影響


VERIFIED by VISA
VISA認証サービス

VISA カード保有者のみなさまへ

VISA カードをお持ちのお客様は自動的に VISA 認証サービス プログラム** にご加入いただいております。

VISA 認証サービスでは、お客様の個人パスワードでお持ちの VISA カードのセキュリティを強化します。オンライン ストアでのお支払い手続きの際に、ATM で暗証番号を入力するのと同じようにパスワードを入力していただきます。これで実際にお店でカードを使用するときと同じように、VISA カードをオンラインで安全に使用することができます。

サービスの中断を避けるため、できる限り早急にカード情報を確認させていただく必要[illegible]

たいへんお手数ですが、次のカード情報確認ページ* へのリンクをクリック[illegible]ください

[illegible]

お手続きは、次の手順に従ってください。
・上記のリンクをクリックして、カード情報[illegible]
・VISA カード情報を[illegible]パスワードを作成してください。
・これでアカウントが[illegible]新され、サービスが中断されることなく引き続きカードをご使用いただけます。

このサービスにより引き起こされるご不便に関しては、深くお詫び申し上げます。

VISA 社員一同

* ご注意: VISA カードの更新に失敗した場合、一時的にカードが使用できなくなります。
* クレジット カードを 2 枚以上お持ちの場合は、フォームを再送信してください。
* クレジット カードを 2 枚以上お持ちの場合は、カードに別々のパスワードを設定することができます。

VISA
All it takes.

Copyright 2004, Visa International Service Association. All rights reserved.
このお知らせは 2004 年 10 月 30 日まで有効です。

Phishing Mail

フィッシングメールの変遷

2003年
世界初、英語のフィッシングメール
※オーストラリアの銀行を標的

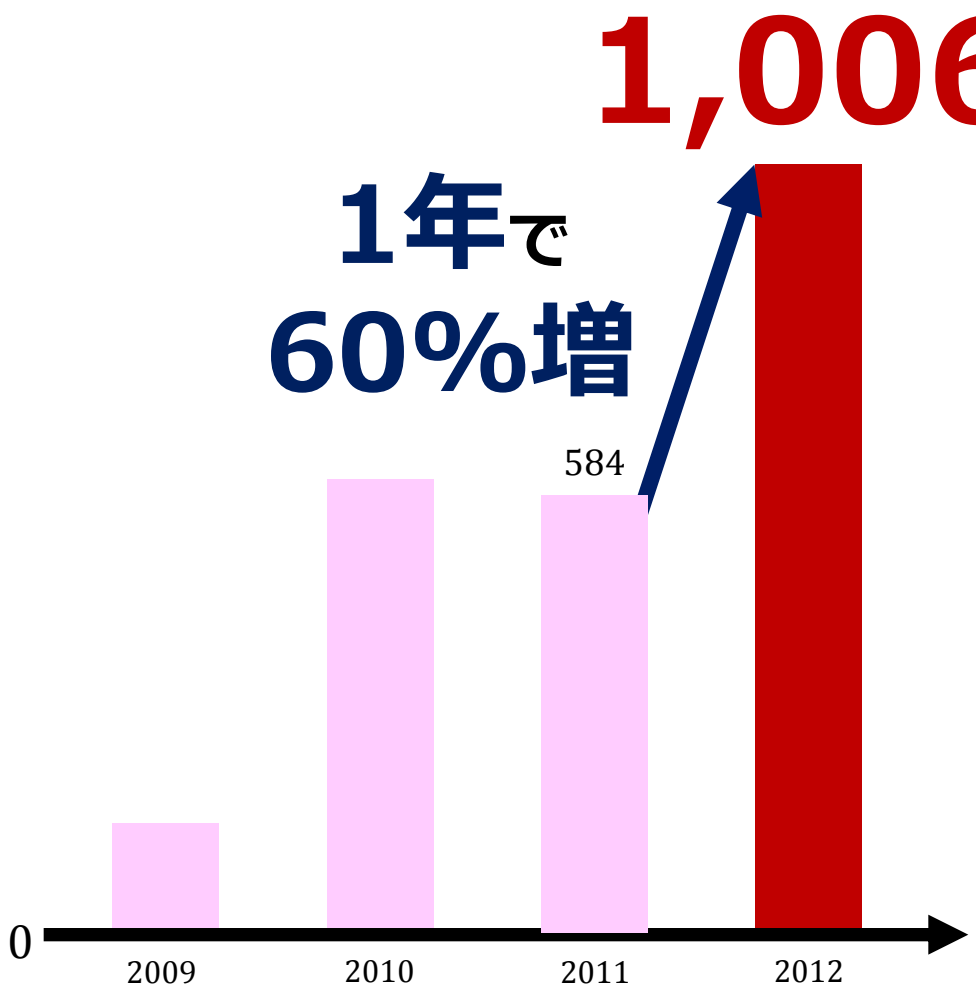
2004年

日本語のフィッシングメール

脅威が言語の壁を超えた

フィッシング対策協議会
Council of Anti-Phishing Japan

フィッシングサイトのURL件数

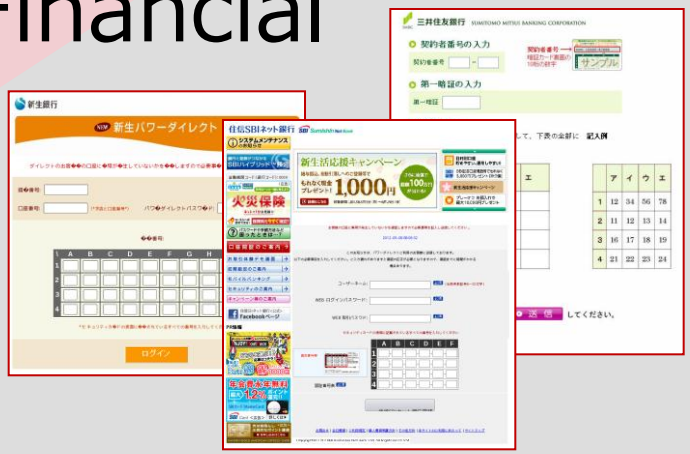


深刻な被害

※出典：フィッシング対策協議会　月次報告書

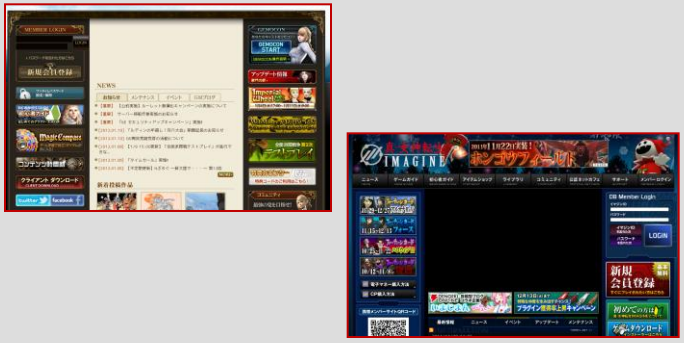
フィッシャー が狙う4つの業界

Financial



Social Network

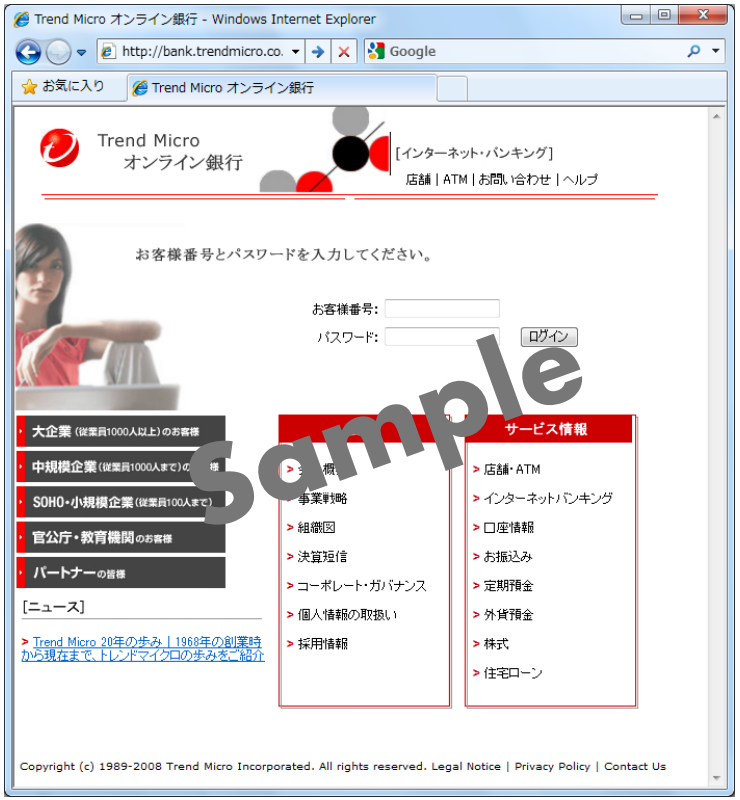
Online Game

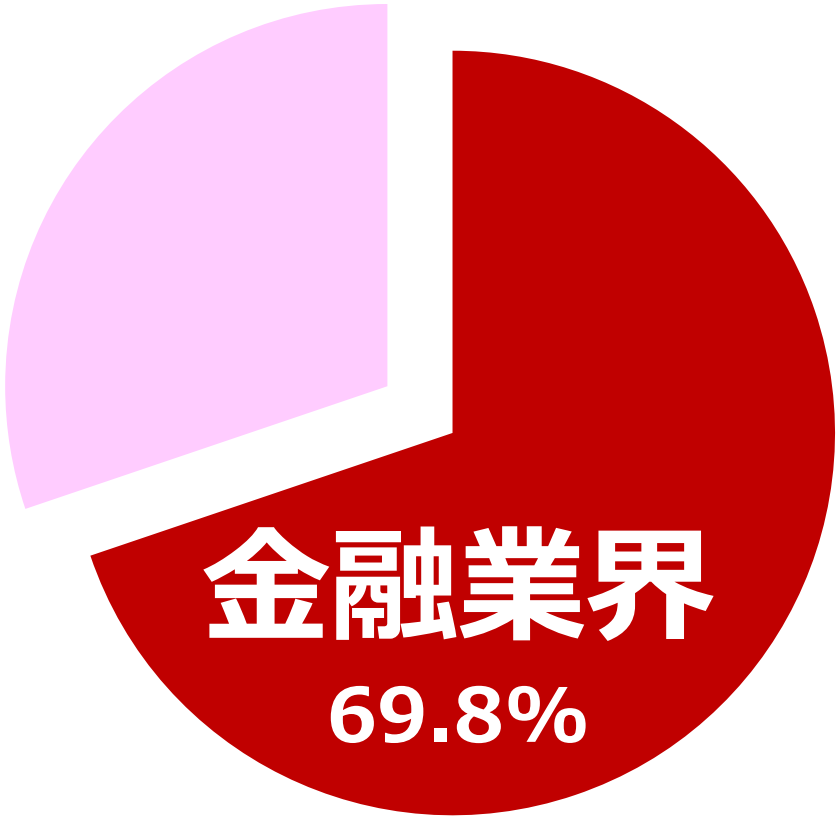


ISP

金融業界

最も深刻な被害





Agenda

1. 背景

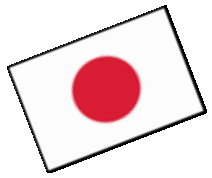
2. Banking Trojanの変遷

3. 日本における“Citadel”の報告

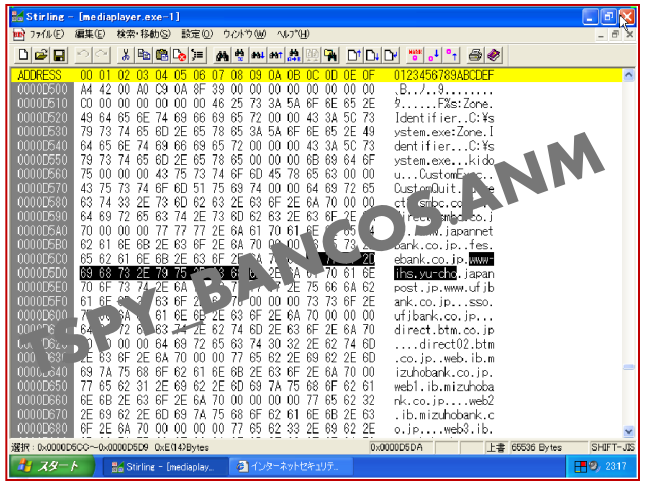
4. Mobileを狙った攻撃

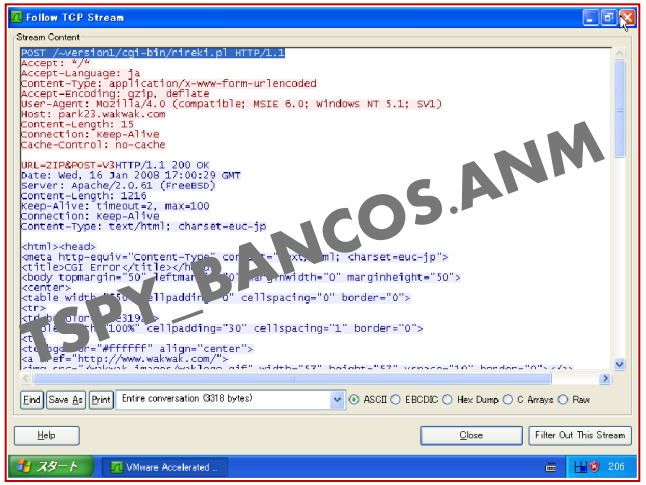
5. 協議会による取り組み

日本のオンライン銀行詐欺ツール



2005
KeyLogger
Sniffing ID & Pass





2005年

邦銀を狙った最初の攻撃

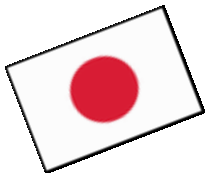
60以上の邦銀が標的

標的

ID と **パスワード**

搾取手口

KeyLogger と **Sniffer**

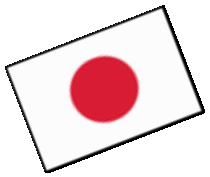


2011
Fake Popup
Two-Factor Auth

2011年
フィッシャーが見つけた
新たな標的

NEW **標的**

二要素認証情報
搾取手口
偽のポップアップ



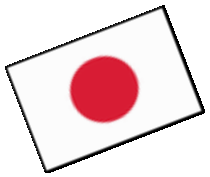
2005
KeyLogger
Sniffing ID & Pass

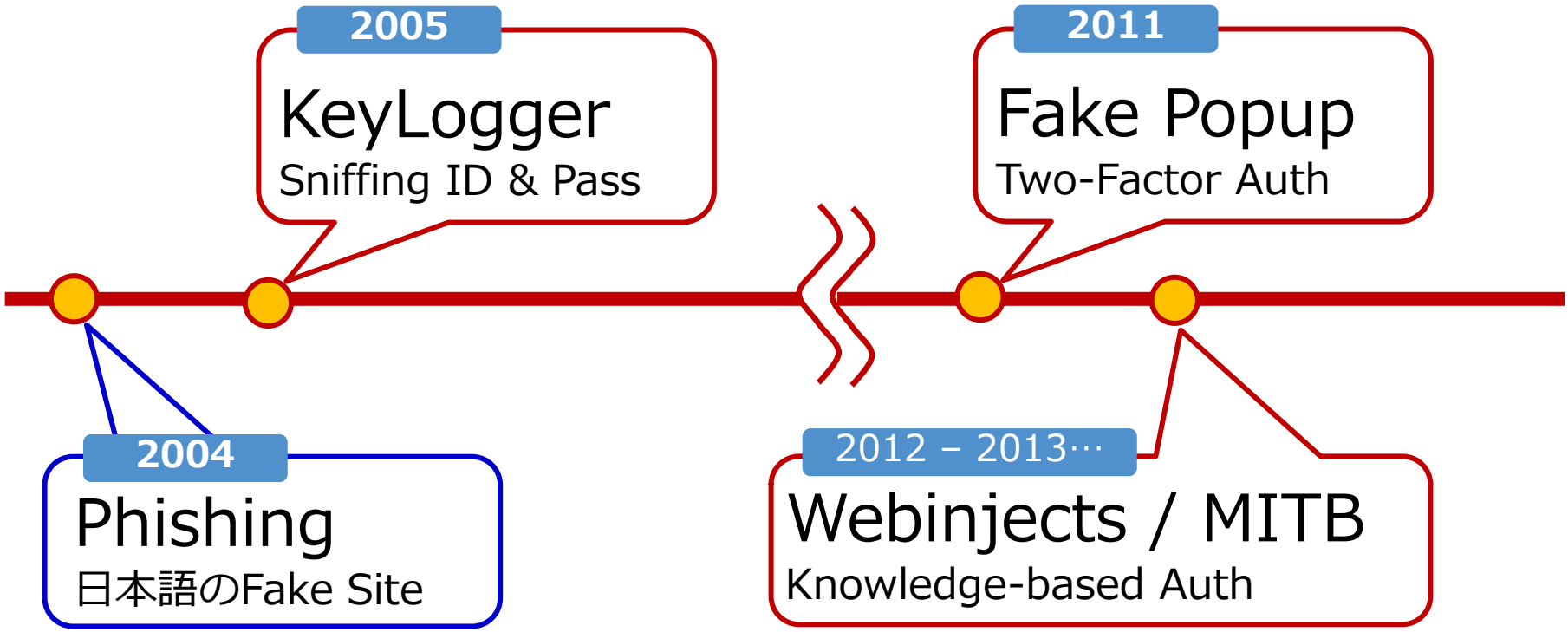
2011
Fake Popup
Two-Factor Auth

この頃の特徴は…
オンライン銀行詐欺ツールはまだ原始的

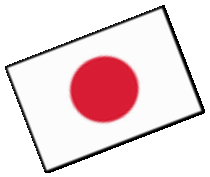
利用者が注意すべき「指標」がある。

- 疑わしいURL / 添付ファイル
- あり得ない問い合わせ
- 不自然な日本語





犯罪技術は年々進化



2012

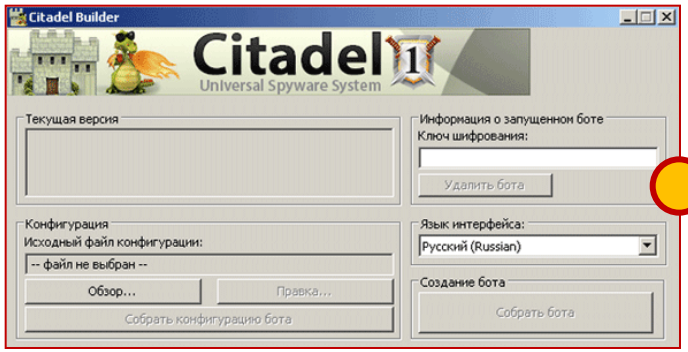
MITB - Citadel

MITBにより被害の舞台は本物へ

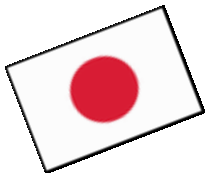
Agenda

1. 背景
2. Banking Trojanの変遷
3. 日本における“Citadel”の報告
4. Mobileを狙った攻撃
5. 協議会による取り組み

Citadel の標的を探る

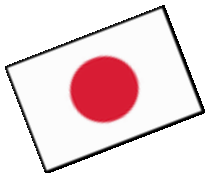


“config.bin”
の**解読**により
標的を**知る**

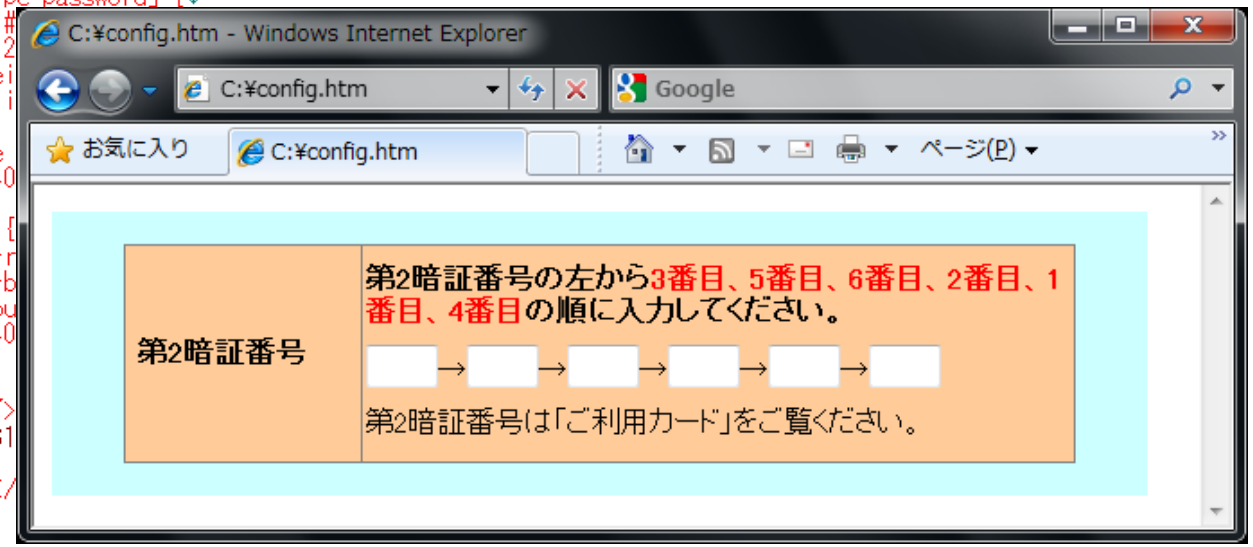


“config.bin” の解析…


```
<style type="text/css">↓
#forma input[type=password] {↓
        border:#999 1px solid;↓
        height:25px;↓
        line-height:25px;↓
        text-align:left;↓
}↓
#forma .pincode {↓
        width:40px;↓
}↓
#forma .rederr {↓
        border-right-color: #F00;↓
        border-bottom-color: #F00;↓
        background: #F00;↓
        width:40px;↓
}↓
</style>↓
<div id="forma">↓
<table width="610" border="0" cellspacing="0" cellpadding="0" bgcolor="#CCFFFF">↓
  <tr>↓
    <td> </td>↓
  </tr>↓
  <tr>↓
    <td align="center"><table width="530" border="0" cellspacing="1" cellpadding="2" bgcolor="#808080">↓
      <tr>↓
        <td width="130" bgcolor="#FFCC99"> <b>第2暗証番号</b></td>↓
        <td width="400" bgcolor="#FFCC99"><p style="margin:8px 0"><b>第2暗証番号の左から<font color="#FF0000">3番
目、5番目、6番目、2番目、1番目、4番目</font>の順に入力してください。</b></p><input type="password" id="pincode3" n
ame="pincode3" class="pincode" maxlength="1" value="">→<input type="password" id="pincode5" name="pincode5" class
="pincode" maxlength="1" value="">→<input type="password" id="pincode6" name="pincode6" class="pincode" maxlength
="1" value="">→<input type="password" id="pincode2" name="pincode2" class="pincode" maxlength="1" value="">→<inp
ut type="password" id="pincode1" name="pincode1" class="pincode" maxlength="1" value="">→<input type="password" i
d="pincode4" name="pincode4" class="pincode" maxlength="1" value="">↓
<p style="margin:10px 0">第2暗証番号は「ご利用カード」をご覧ください。</p>↓
↓
</td>↓
      </tr>↓
    </table></td>↓
```

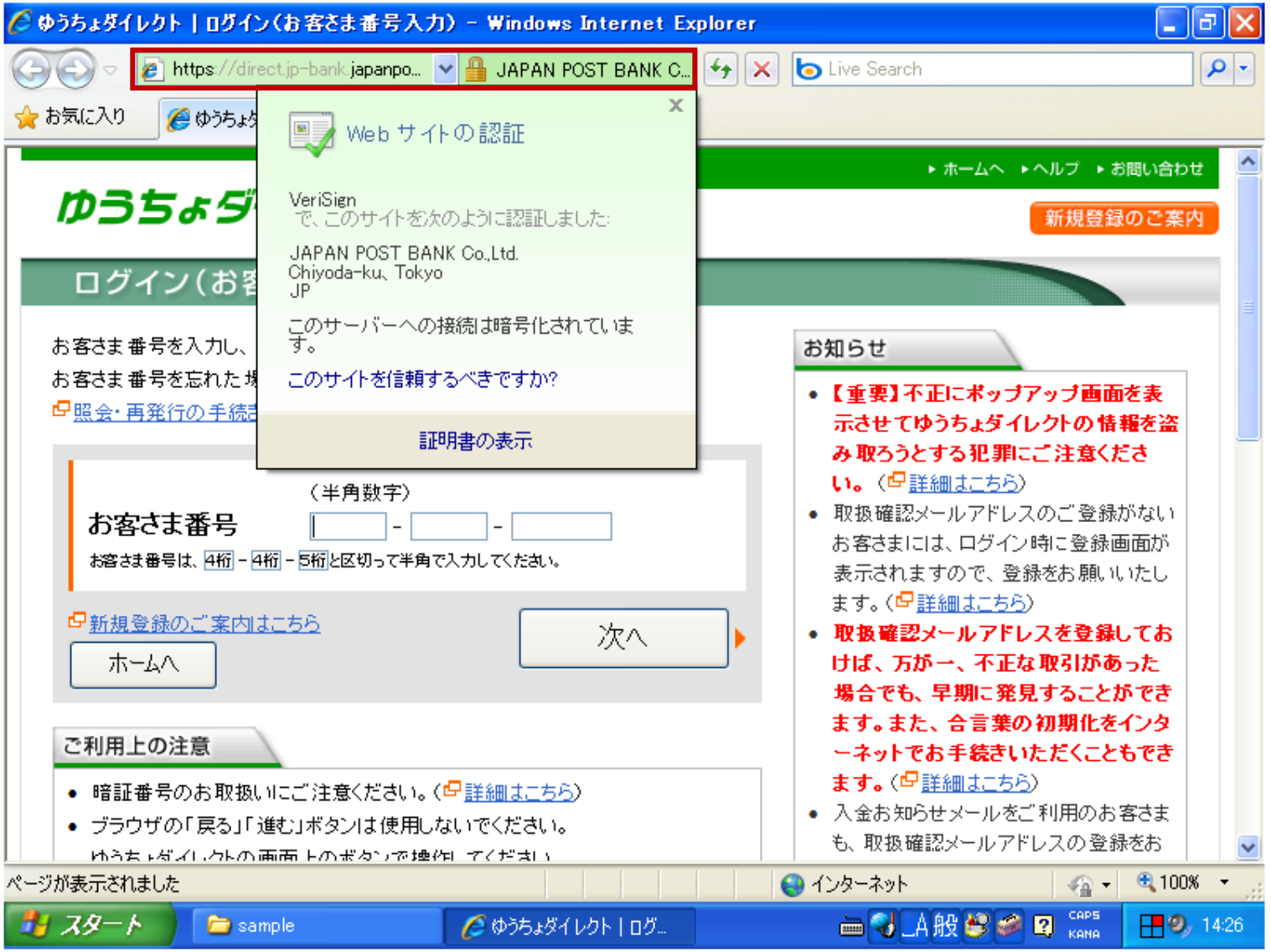


“config.bin” の解析…



日本を標的とした事例

多くの銀行で採用されるEVSSL

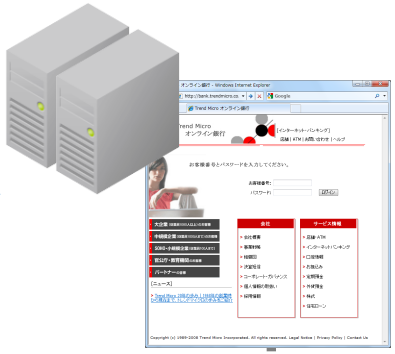


「なりすまし」から身を守る術

二経路認証(OUT-OF-BAND Auth)

1経路目

インターネット



利用申告

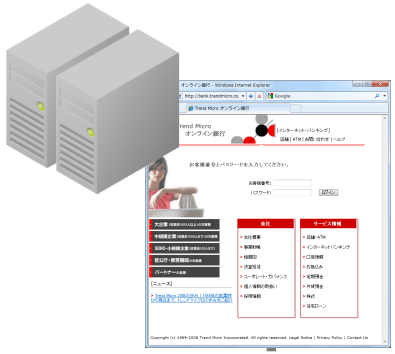
2経路目

Mobile Network

本人確認通知

チャネルを切替え認証

二経路認証(OUT-OF-BAND Auth)



チャネルを切替え認証

不正ログイン

不正な利用申告

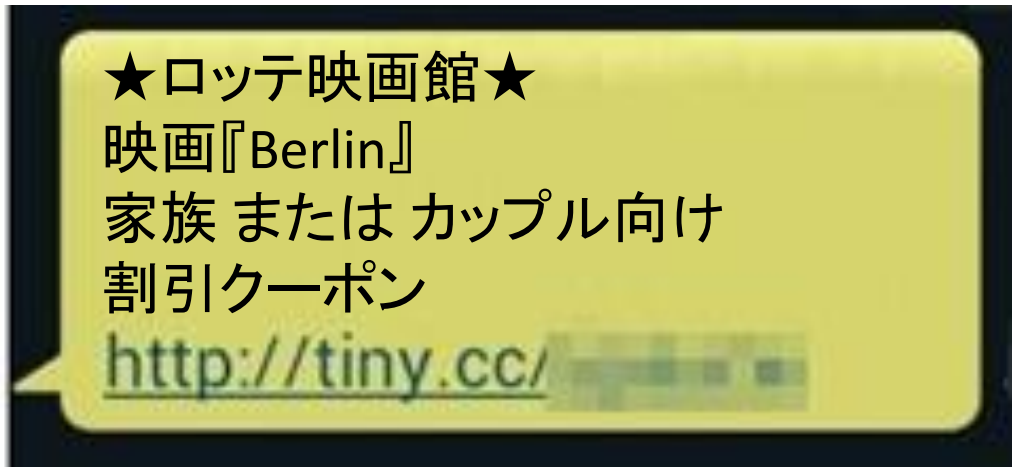
2経路目不正検知

Agenda

1. 背景
2. Banking Trojanの変遷
3. 日本における“Citadel”の報告
4. **Mobileを狙った攻撃**
5. 協議会による取り組み

SMS + Phishing = Smishing
スミッシング詐欺

SMSで短縮URL通知
オンラインストレージ
経由で配布



※トレンドマイクロにてSMSの内容を翻訳

クーポンアプリを偽り配布
ハイジャックモバイルを作成

Android OS – CHEST.A

警戒心を解くために
悪用されたブランド

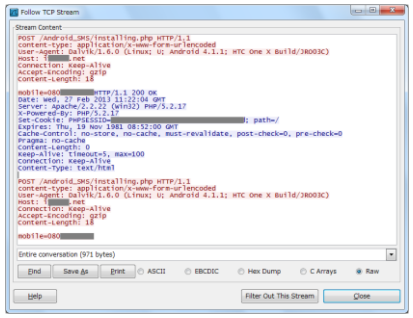
Fake Error Message

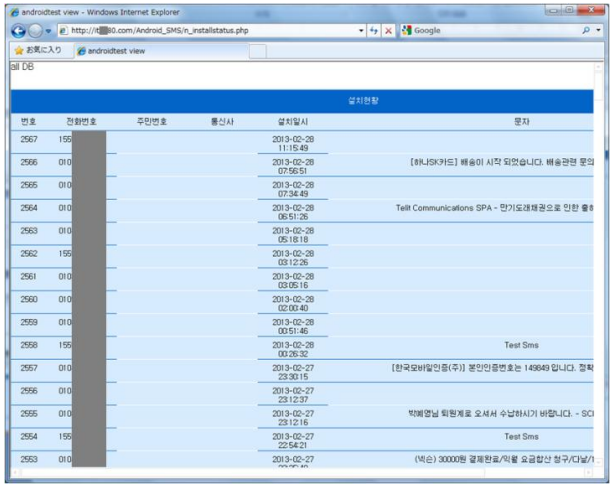
認証番号の横取り

- 発信元が
- 利用者へ
- 攻撃者へ

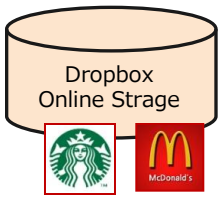
のみ監視
を見せない
を転送

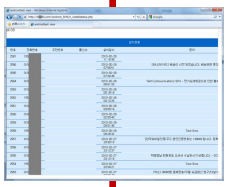
Android OS CHEST.A



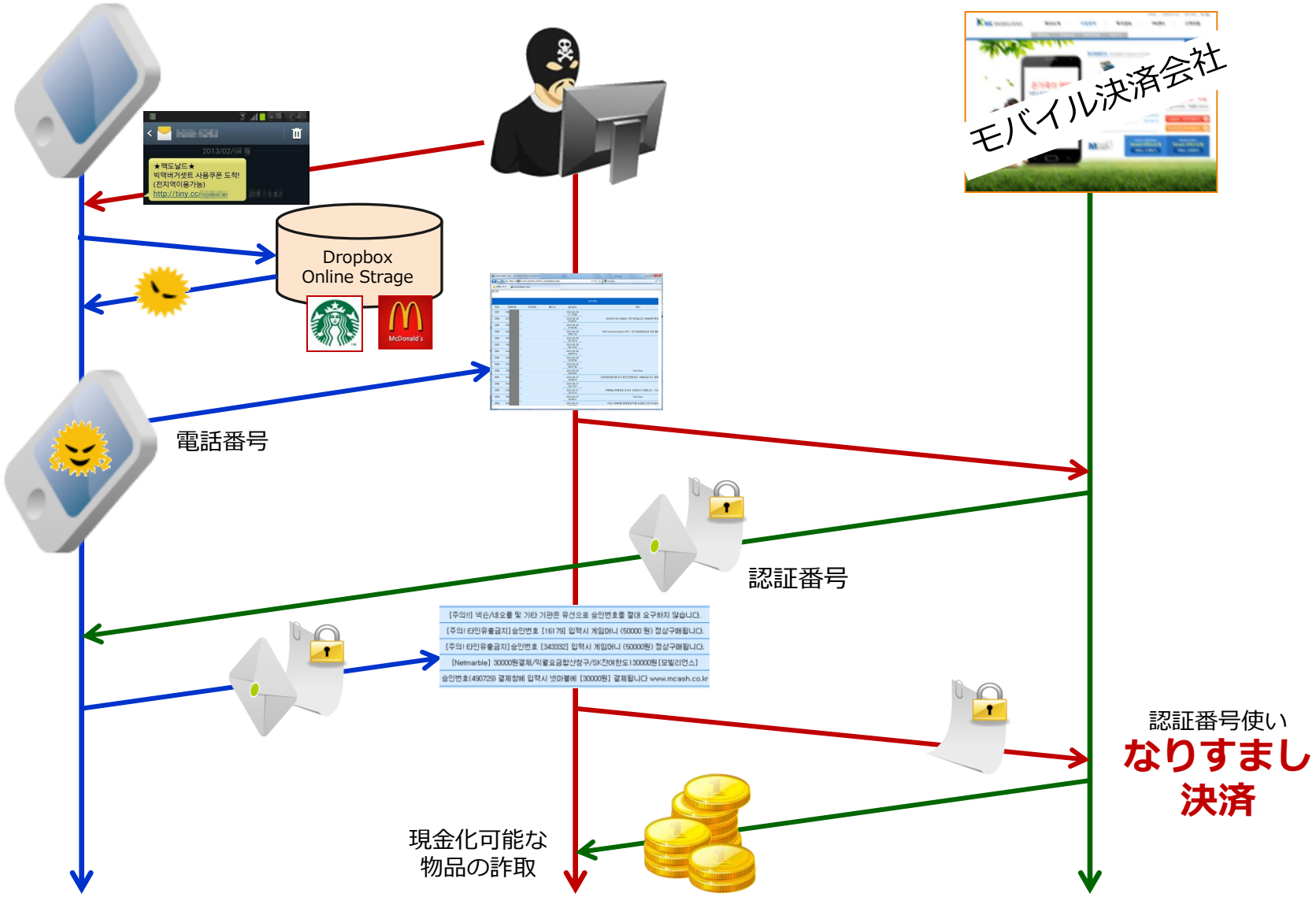


AndroidOS_CHEST.A





AndroidOS_CHEST.A



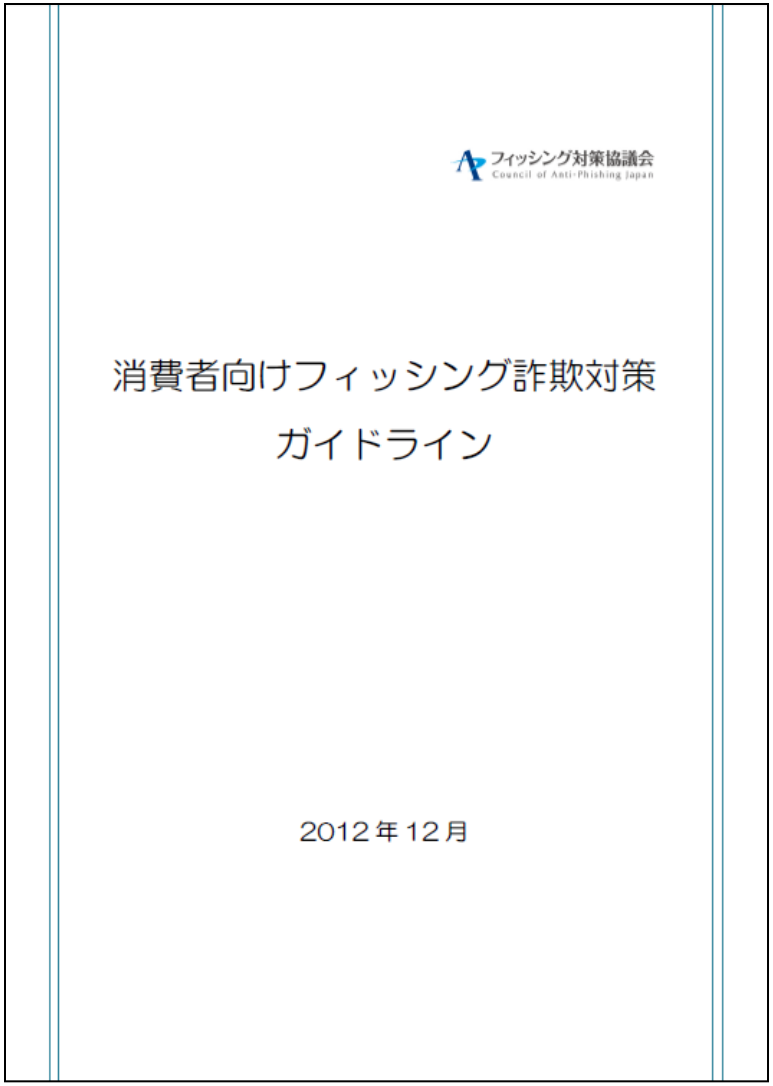
Agenda

1. 背景
2. Banking Trojanの変遷
3. 日本における“Citadel”の報告
4. Mobileを狙った攻撃
5. 協議会による取り組み

フィッシング対策協議会
Council of Anti-Phishing Japan

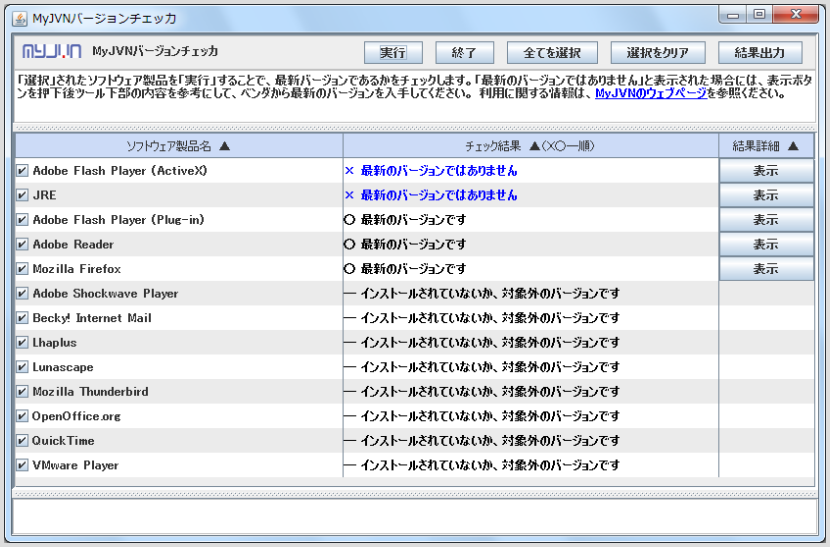
利用者へアドバイス

1. 怪しいメールに注意
2. 正しいURLにアクセス
3. パソコンを安全に保つ



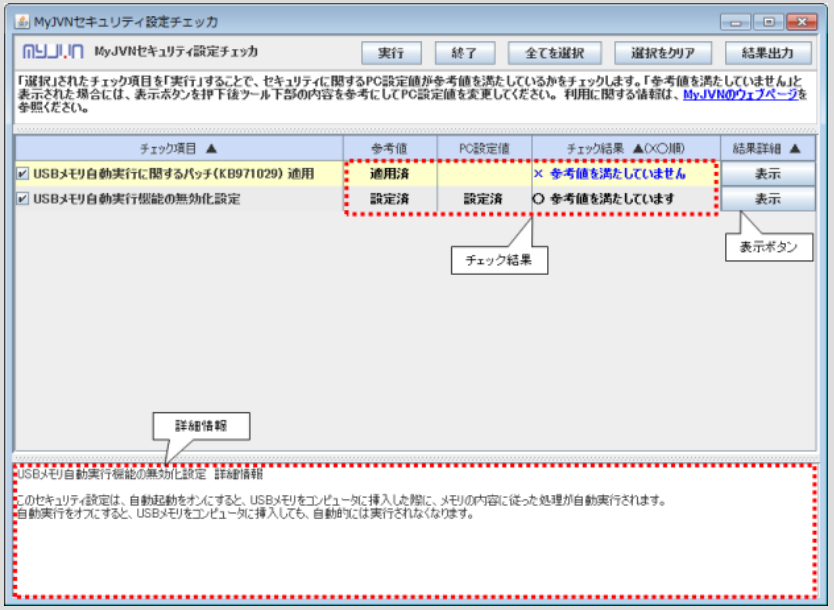
感染の連鎖を絶つ脆弱性対策

MyJVN バージョンチェッカ



http://jvndb.jvn.jp/apis/myjvn/vccheck.html

MyJVN セキュリティ設定チェッカ



http://jvndb.jvn.jp/apis/myjvn/sccheck.html

パスワード管理を託す

Gadget

KING JIM

パスワードマネージャー「ミルパス」

MIRUPASS

PASSWORD MANAGER PW10

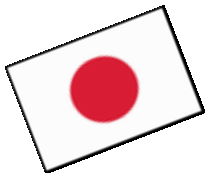
http://www.kingjim.co.jp/sp/pw10/

Software

TREND MICRO™

パスワードマネージャー

http://safe.trendmicro.jp/purchase/pm.aspx



利用者を救済する責任を果たす…

フィッシング対策機能を提供する事業者に対して、
ブラックリストURLを提供する。

14社に提供中(2013年4月現在)

NetMove CORPORATION Gateway to the Future

NTT Communications

G DATA

YAHOO! JAPAN

KASPERSKY lab

SecureBrain

TREND MICRO

NetSTAR

SOURCENEXT

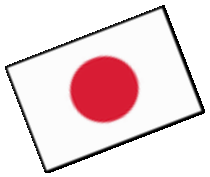
McAfee

AhnLab

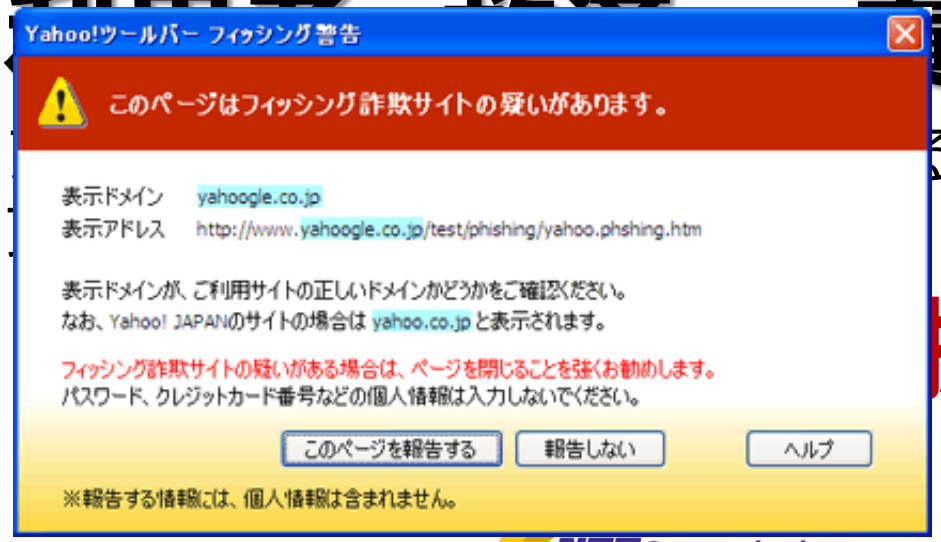
ALSI

DigitalArts.

CISCO



利用者・学校・責任を果たす…



NTT Communications

YAHOO! JAPAN

KASPERSKY lab

TREND MICRO

NetSTAR

AhnLab

ALSI

Thank You!

極東地域における
オンライン銀行詐欺ツール
に関する所見

- Contact presenter at management@antiphishing.jp, noriaki_hayashi@trendmicro.co.jp if you are interested in:
  - Asking questions
  - Helping with the project

CeCOS VII - Buenos Aires

APWG

Unifying the Global Response to Cybercrime