



# フィッシング 認証情報詐取の実態と その対抗手段

**Noriaki HAYASHI**  
Senior Researcher

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

第17回 サイバー犯罪に関する白浜シンポジウム  
Shirahama Cyber Crime Symposium Vol. 17  
2013.05.24 (fri) Big-U



# Introduction



## 林 憲明

### Forward-looking Threat Research

大学卒業後、2002年トレンドマイクロ入社。国内専門のウイルス解析機関である「リージョナルトレンドラボ」を経て、2010年に新設されたフォワードルッキングスレトリサーチへ異動。現在に至る。「先読み（フォワードルッキング）係」として、テクノロジーやユーザーの調査／分析に留まらず、脅威を生み出す側（犯罪者）が何を狙い／計画しているかに着目し、トレンドマイクロが備えるべき製品／技術の方向性立案を担当している。



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

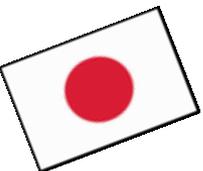
**1. フィッシング詐欺に関する背景**

**2. フィッシング詐欺の早期発見**

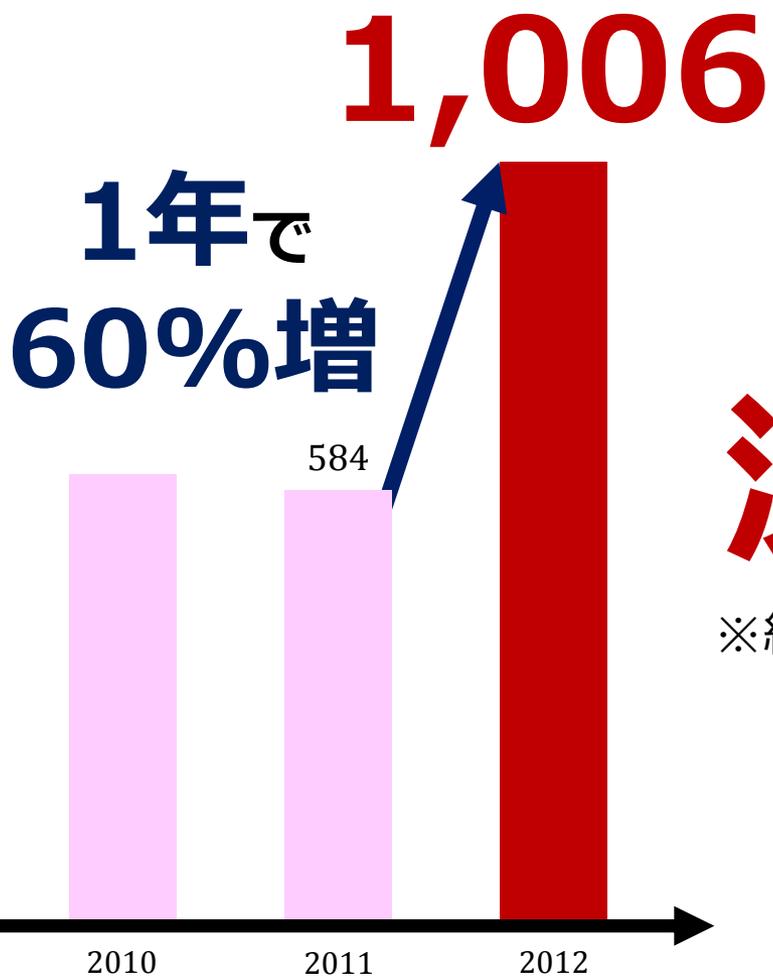
**3. オンライン銀行詐欺ツールの変遷**

**4. モバイル決済を狙った攻撃**

**5. 協議会による取り組み**



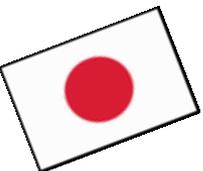
# フィッシングサイトのURL件数



## 深刻な被害

※約20%は日本のブランドを狙ったもの

※出典：フィッシング対策協議会 月次報告書「フィッシング報告状況」より、「フィッシングサイトのURL件数」を抽出。  
講演者集計、グラフ作成



# ファイッシャーが狙う4つの業界

## 金融業界

Sanwa Bank (三井住友銀行) login page with fields for account number and password.

Shinsei Bank (新生銀行) website with various service advertisements and a calendar.

## Social Network

Twitter login page with fields for username/email and password.

Facebook login page with fields for email/phone and password.

Ameba website with a yellow banner and user avatars.

## オンラインゲーム

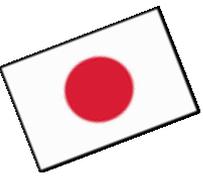
DMM.com website showing various game titles and promotional banners.

GREE website with a dark theme and game advertisements.

## プロバイダ

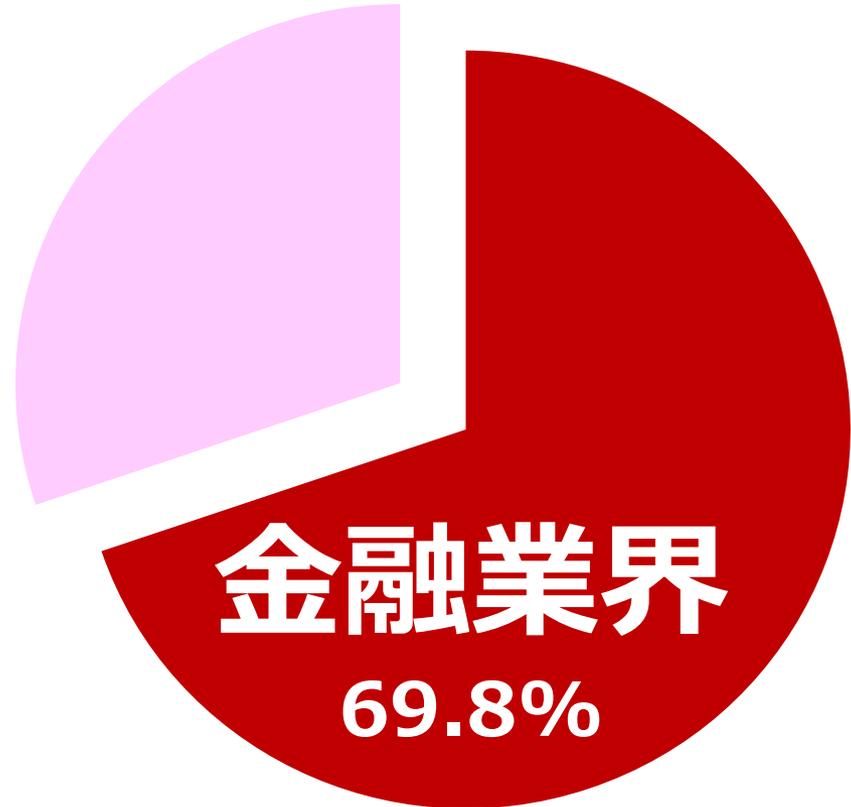
OCN (Optical Communications Network) email login page with fields for email and password.

BIGLOBE email login page with fields for email and password.

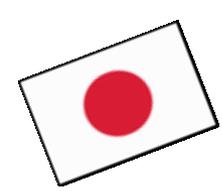


# 金融業界

## 最も深刻な被害

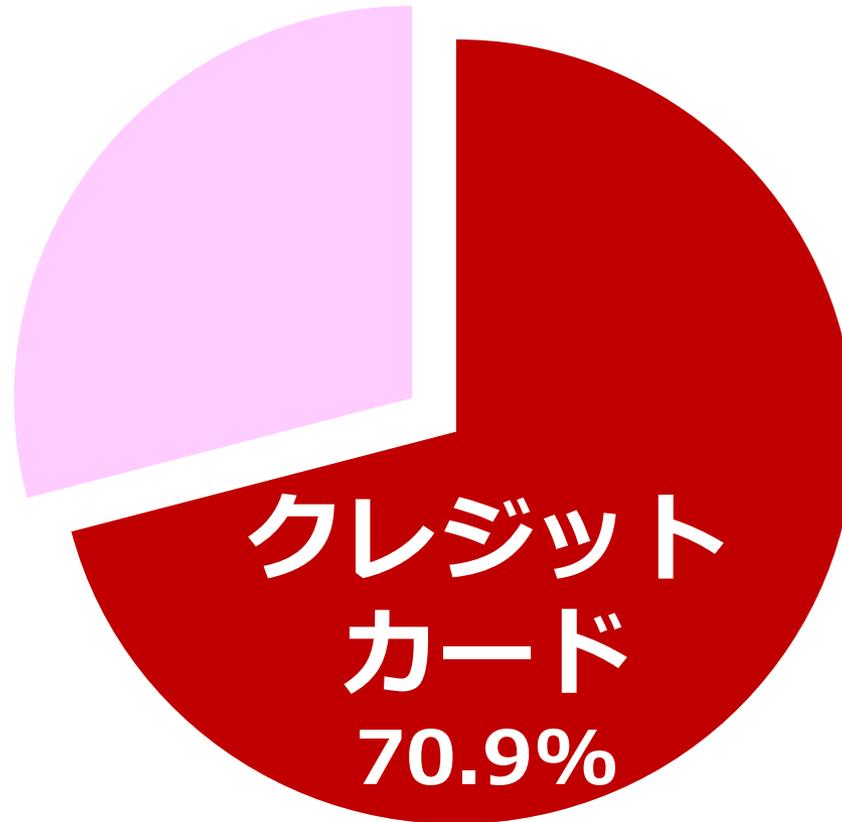


データ出典：2012年度、トレンドマイクロが日本国内で確認したフィッシングサイトについて標的業種を分類、統計

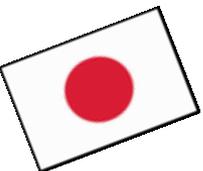


# 最も身近なオンライン決済方法

Q. 普段利用している決済方法は何ですか？



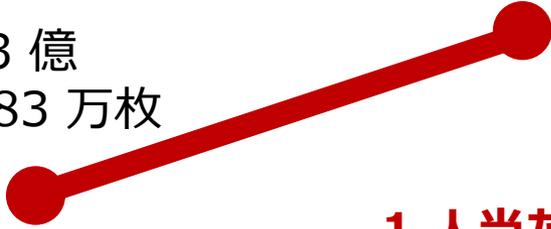
出典：株式会社ネットプロテクションズ『インターネットショッピングに関する動向調査2012』（2012/4/3 - 16）、N = 2,064,  
<http://www.dreamnews.jp/press/0000053432/>



# 一人で複数枚を持つ時代

3 億  
1,783 万枚

3 億  
2,164 万枚



1 人当たり  
2.7 枚所有

1 人当たり  
3.1 枚所有

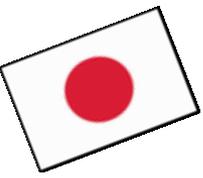


# 発行枚数

# 3億2,164万枚



出典：  
 日本クレジット産業協会、2009年3月末の国内のクレジットカード発行枚数(社数400社)は3 億 1,783 万枚  
 日本クレジット産業協会、2012年3月末の国内のクレジットカード発行枚数(社数346社)は3 億 2,164 万枚  
 総務省「人口推計」2009年3月1日現在の20歳以上の総人口 1 億 434 万人  
 総務省「人口推計」2012年3月1日現在の20歳以上の総人口 1 億 495 万人



# 言語がフィッシングに及ぼす影響



## 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をお持ちの 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。これにより、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ご確認させていただく必要がございます。ご確認のうえ、サービスが中断している場合は、早急にご連絡ください。

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してください。

<https://www.visa.co.jp/.../>

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、カード情報をご確認ください。  
- VISA カード情報を照会して、個人パスワードを再入力してください。  
- これでアカウントが更新され、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。



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。

## 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

# Agenda

1. フィッシング詐欺に関する背景

2. フィッシング詐欺の早期発見

3. オンライン銀行詐欺ツールの変遷

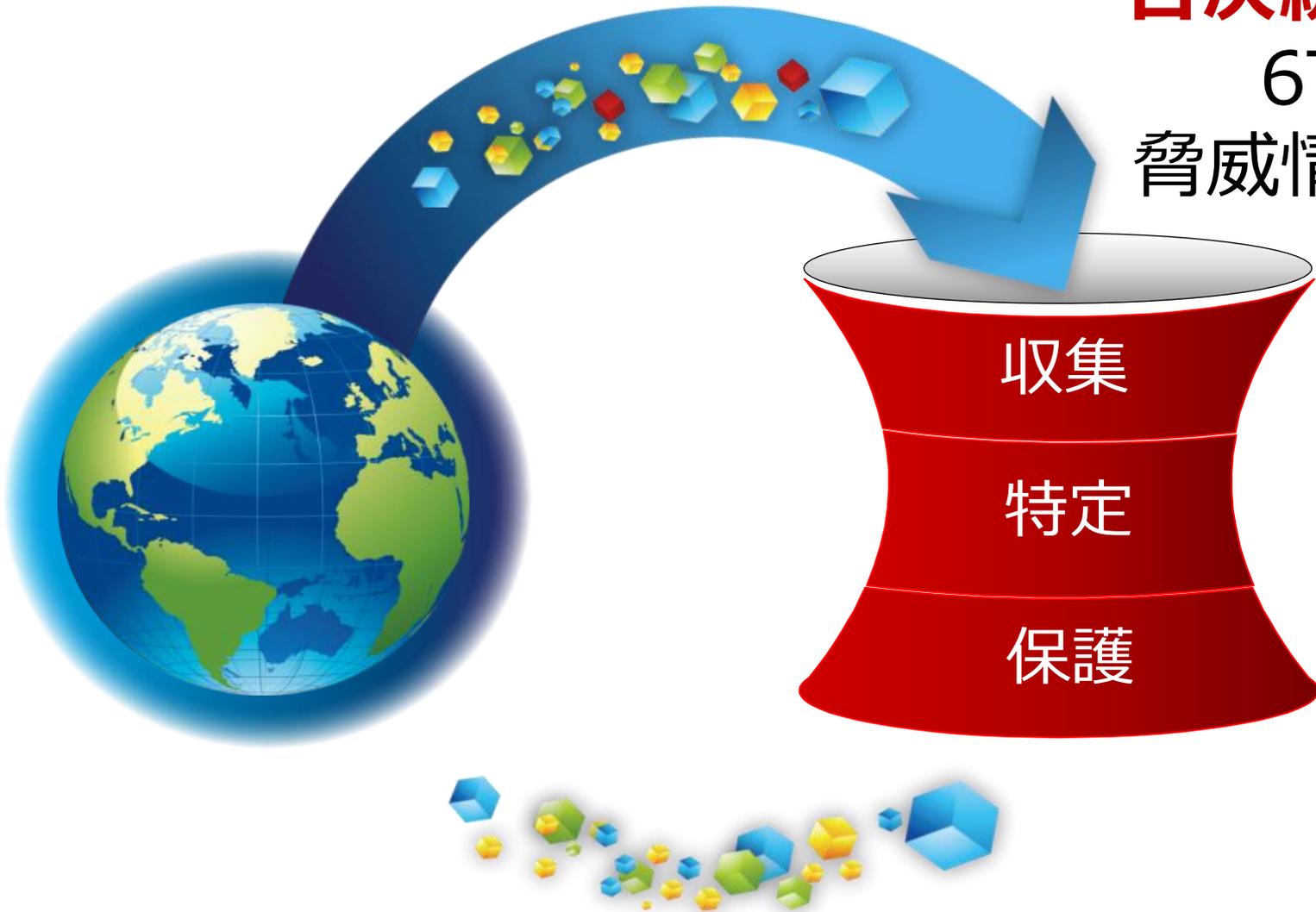
4. モバイル決済を狙った攻撃

5. 協議会による取り組み

# 特定のパターンを見つけ出す

日次統計情報

6TBの  
脅威情報入力

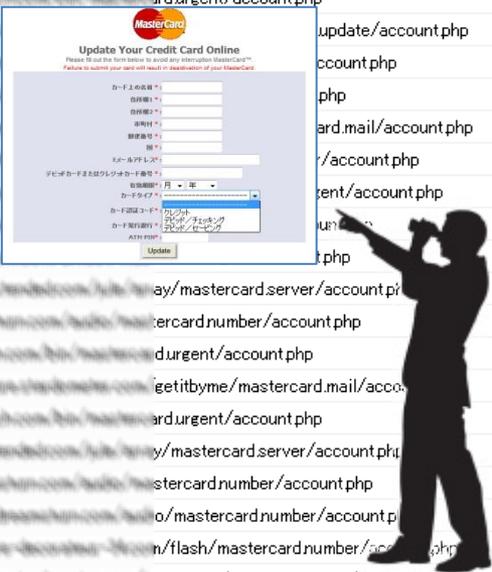




# 一連の攻撃について振り返る

## フィッシングサイトのURLリスト

Nodes	Type
http://.../mastercard.server/account.php	URL
http://.../mastercard.urgent/account.php	URL
http://.../mastercard.urgent/account.php	URL
http://.../mastercard.number/account.php	URL
http://.../mastercard.update/account.php	URL
http://.../mastercard.urgent/account.php	URL
http://.../mastercard.update/account.php	URL
http://.../mastercard.account.php	URL
http://.../mastercard.php	URL
http://.../mastercard.mail/account.php	URL
http://.../mastercard/account.php	URL
http://.../mastercard.urgent/account.php	URL
http://.../mastercard.php	URL
http://.../mastercard.server/account.php	URL
http://.../mastercard.number/account.php	URL
http://.../mastercard.urgent/account.php	URL
http://.../mastercard.mail/account.php	URL
http://.../mastercard.urgent/account.php	URL
http://.../mastercard.server/account.php	URL
http://.../mastercard.number/account.php	URL
http://.../mastercard.urgent/account.php	URL
http://.../mastercard.number/account.php	URL
http://.../mastercard.number/account.php	URL
http://.../mastercard.update/account.php	URL
http://.../mastercard.server/account.php	URL
http://.../mastercard.update/account.php	URL



# データ の 理解

※「ケーススタディ」としてクレジットカード会社の「MasterCard（マスターカード）」を騙った事例を取り上げる。

# 属性情報の抽出

Open Source **INT**elligence  
データベース群

メールアドレス  
評価

GeoIP  
地理位置情報

フィッシング  
URL

サイトの安定性  
評価

IPアドレス  
評価

Whois情報  
過去履歴



# データ の 濃度

※濃度とは、その列におけるデータの一意性。  
ユニークな値は濃度が濃いといえる。

# URLに隠されたパターン

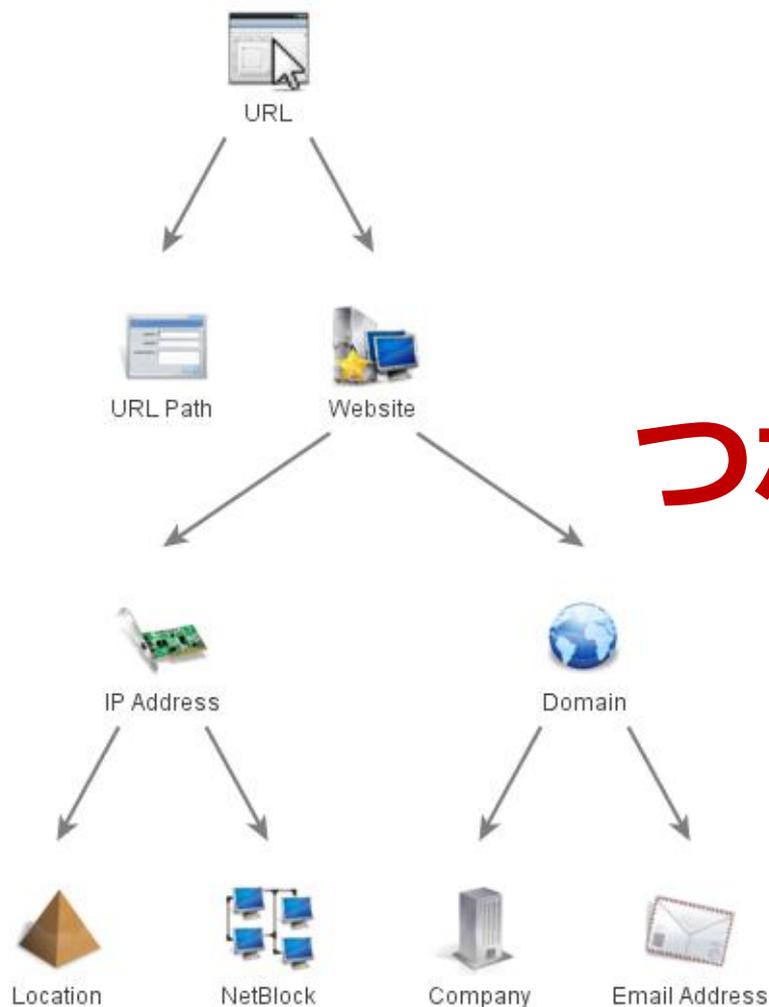
URL PATH についてワードクラウド作成



## データの可視化

※ワードクラウド：単語の出現頻度を分析し、頻度に応じた大きさで図示

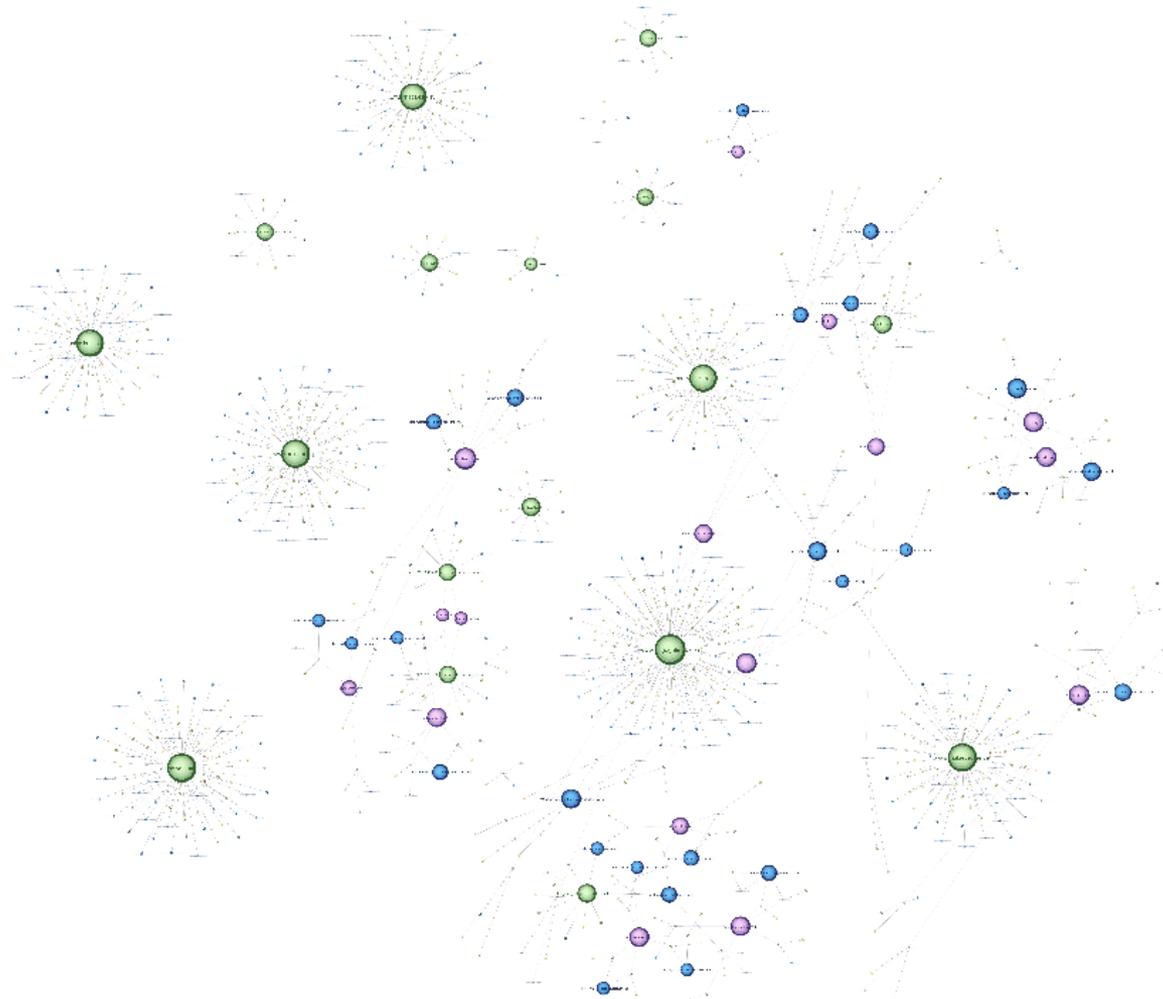
# 潜在的な攻撃のリンク



## 構成要素の

つながり / 重なり合い  
注目

# 「関係」に共通するパターン 監視対象の特定





# サーバに対するハッキング

http://...edu.et/debian/mastercard.number/account.php  
http://...com/mastercard.secure/account.php  
http://...com/mastercard.tos/account.php  
http://...com/mastercard.notify/account.php  
http://...com/mastercard.owner/account.php  
http://...com/mastercard.ssl/account.php  
http://...com/db\_img/ssl/mastercard.server/account.php  
http://...com/db\_img/ssl/mastercard.update/account.php  
http://...com/c.jpg/mastercard.server/account.php  
http://...gr/fileadmin/mastercard.update/account.php  
http://...gr/fileadmin/mastercard.mail/account.php  
http://...com/Fiero/dbConnect/mastercard.number/account.php  
http://...com/Fiero/dbConnect/mastercard.update/account.php  
http://...dk/ABC/mastercard.number/account.php  
http://...dk/ABC/mastercard.update/account.php  
http://...ru/cache\_html/mastercard.number/account.php  
http://...gr/fileadmin/mastercard.mail/account.php

## PATH に機械的な パターン

※ブランド名を確認

※無実のサイトがハッキングされて  
フィッシングに使われるケースが多い。

# ケーススタディ に対する 結論と展望

- 統計学と可視化を組み合わせた分析は短時間で高精度なルール作成が可能
- 複雑な分析を単純化して明確かつタイムリーに情報共有が可能
- 更なる性質の解析により予防と予測への利用が期待できる

# Agenda

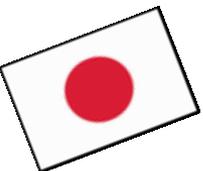
1. フィッシング詐欺に関する背景

2. フィッシング詐欺の早期発見

3. オンライン銀行詐欺ツールの変遷

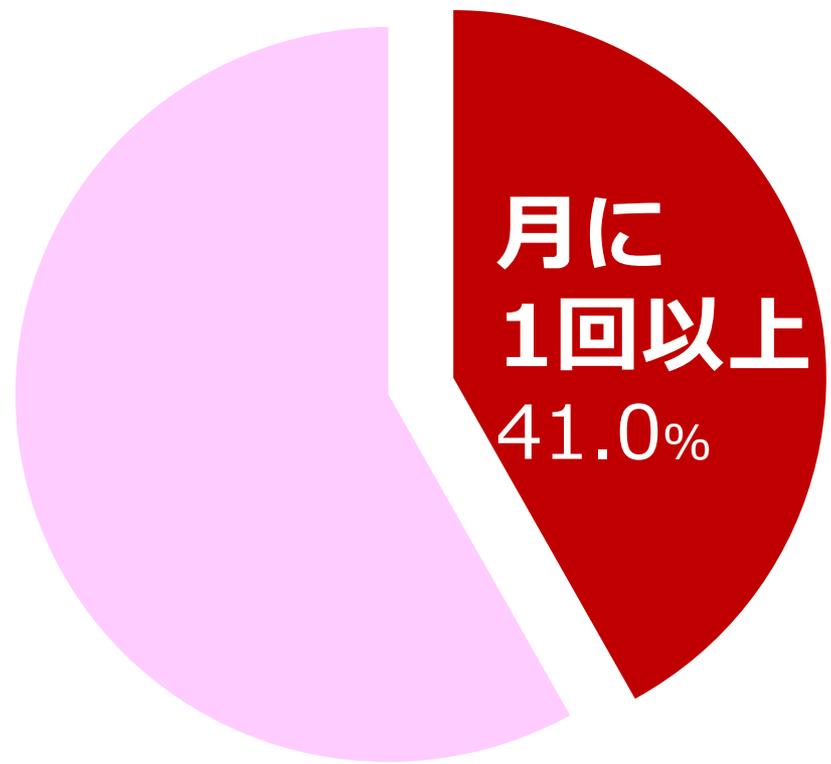
4. モバイル決済を狙った攻撃

5. 協議会による取り組み

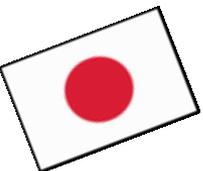


# アクセス頻度

## オンラインバンキングに関する調査

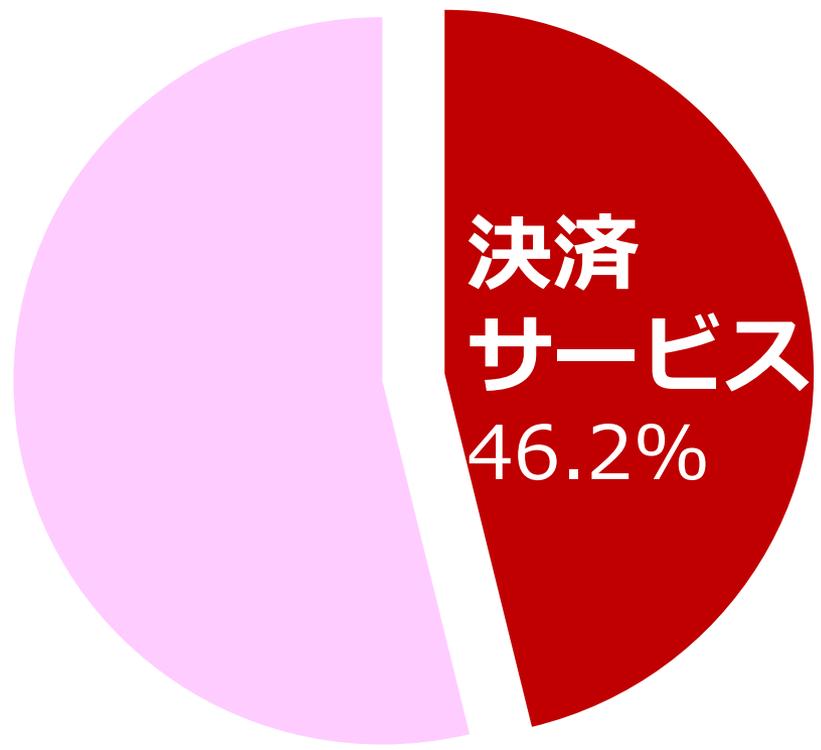


出典：楽天リサーチ株式会社『オンラインバンキングに関する調査』（2012/5/29 - 30）、N = 1,000,  
<http://research.rakuten.co.jp/report/20120621/>



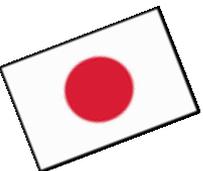
# アクセス目的

## オンラインバンキングに関する調査

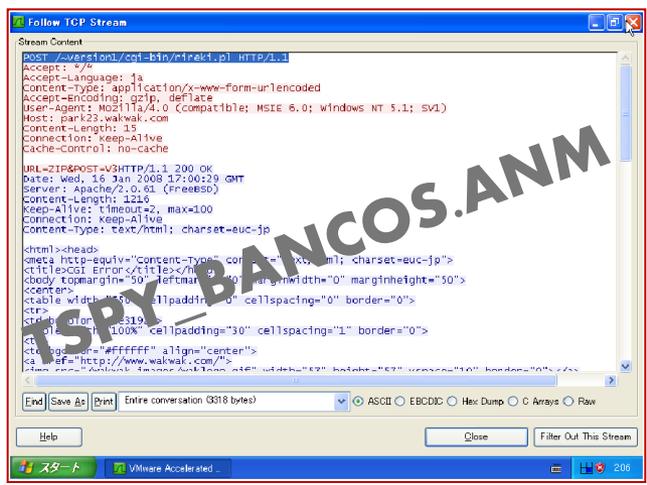
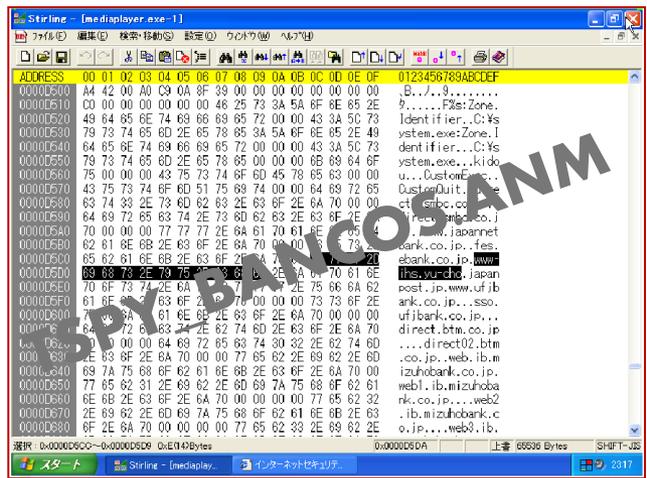


出典：楽天リサーチ株式会社『オンラインバンキングに関する調査』（2012/5/29 - 30）、N = 1,000,  
<http://research.rakuten.co.jp/report/20120621/>

# 日本のオンライン銀行詐欺ツール



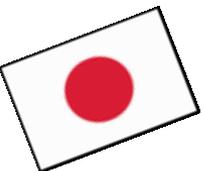
2005  
**KeyLogger**  
 Sniffing ID & Pass



**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**  
 盗む手口  
**KeyLogger と Sniffer**



2011  
Fake Popup  
Two-Factor Auth

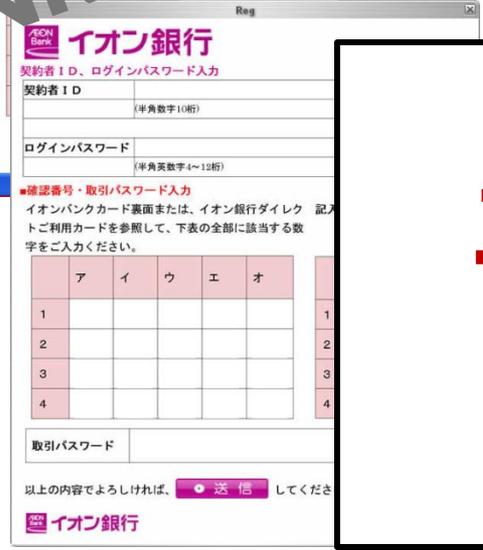


# 2011年

新たな対策技術を  
狙うフィッシャー

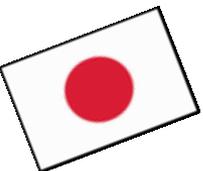


TSPY-BANKER.RJT



NEW 標的

二要素認証情報  
盗む手口  
偽のポップアップ



2005  
KeyLogger  
Sniffing ID & Pass

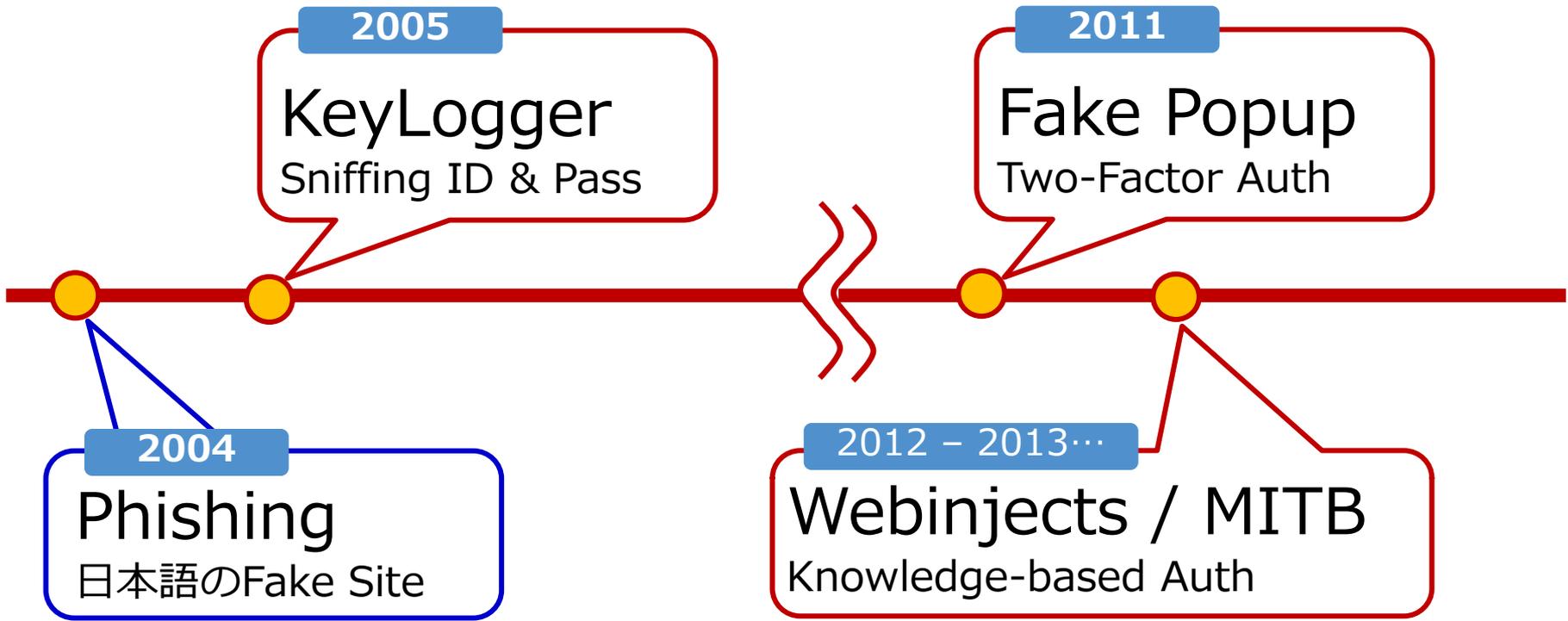
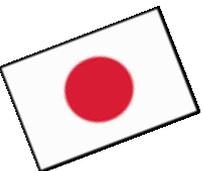
2011  
Fake Popup  
Two-Factor Auth

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

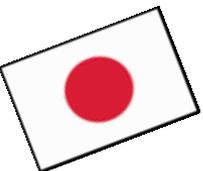
- 疑わしいURL / 添付ファイル
- あり得ない問い合わせ
- 不自然な日本語



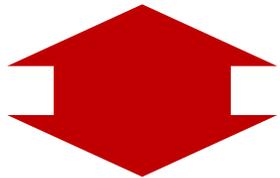
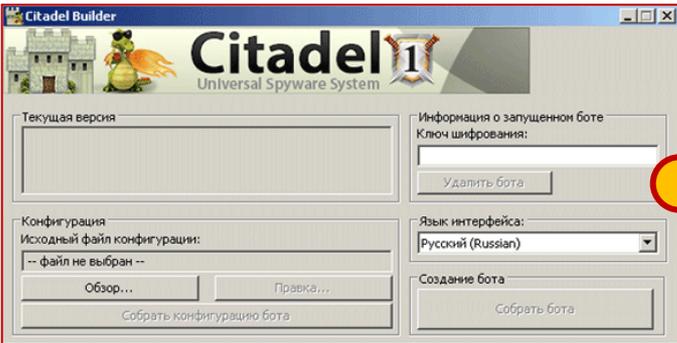
# 犯罪技術は年々進化

# MITBにより被害の舞台は本物へ





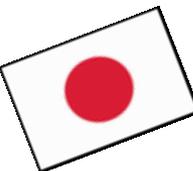
# Citadel の標的を探る



“config.bin”  
の**解読**により  
標的を知る







# 多くの銀行で採用されるEVSSL

ログイン(お客さま番号入力) - Windows Internet Explorer

https:// japan JAPAN Live Search

Web サイトの 認証

VeriSign  
で、このサイトを次のように認証しました:

このサーバーへの接続は暗号化されています。  
このサイトを信頼するべきですか?

証明書の表示

ログイン(お客)

お客さま番号を入力し、  
お客さま番号を忘れた場合は  
[照会・再発行の手続き](#)

新規登録のご案内

お知らせ

お客さま番号 (半角数字)  
[ ] - [ ] - [ ]  
お客さま番号は、4桁 - 4桁 - 5桁と区切って半角で入力してください。

[新規登録のご案内はこちら](#) 次へ

ホームへ

ご利用上の注意

- 暗証番号のお取扱いにご注意ください。([詳細はこちら](#))
- ブラウザの「戻る」「進む」ボタンは使用しないでください。

ページが表示されました

スタート sample ログ... インターネット 100%

LA般 CAPS KANA 14:26

# 機能を知ることによって防げる脅威



The screenshot shows a Windows Internet Explorer browser window. The address bar contains a partially obscured URL. A red box highlights the address bar, and a tooltip below it shows the full URL: `https://[redacted]bank.[redacted].jp/`. The page content includes a login form with a security questionnaire. The questionnaire asks for information such as the name of the first car or motorcycle, the favorite magazine, and the name of a favorite historical figure. The page also contains a sidebar with links for 'お気に入り' (Favorites), 'ログイン' (Login), and '新規登録のご案内はこちら' (Click here for new registration information).

ログイン(お客さま番号入力) - Windows Internet Explorer

https:// [redacted] bank. [redacted].jp/

ログイン(お客さま番号入力)

お客さま番号を入力し、「次へ」をクリックしてください。お客さま番号を忘れた場合は「戻る」をクリックしてください。

[照会・再発行の手続き](#)

お客さま番号  
お客さま番号は、4桁 - 4桁 - 5桁の数字で入力してください。

[新規登録のご案内はこちら](#)

ホームへ

ご利用上の注意

- 暗証番号のお取り扱いについて
- ブラウザの「戻る」「進む」ボタンはご利用できません。

詐欺を防ぐために、我々はあなたの身分を確かめなければいけませんので、いくつかの質問を答える必要があります。それはあなた様しか答えられない質問でございます。そして、個人情報が入力されたことを御確認してください。

質問1	初めて買った車またはバイクの名前は何ですか？
合言葉1	<input type="text"/>
質問2	最もよく読む雑誌は何ですか？
合言葉2	<input type="text"/>
質問3	最も好きな歴史上の人物の名前は何ですか？
合言葉3	<input type="text"/>
インターネット用暗証番号	<input type="text"/>

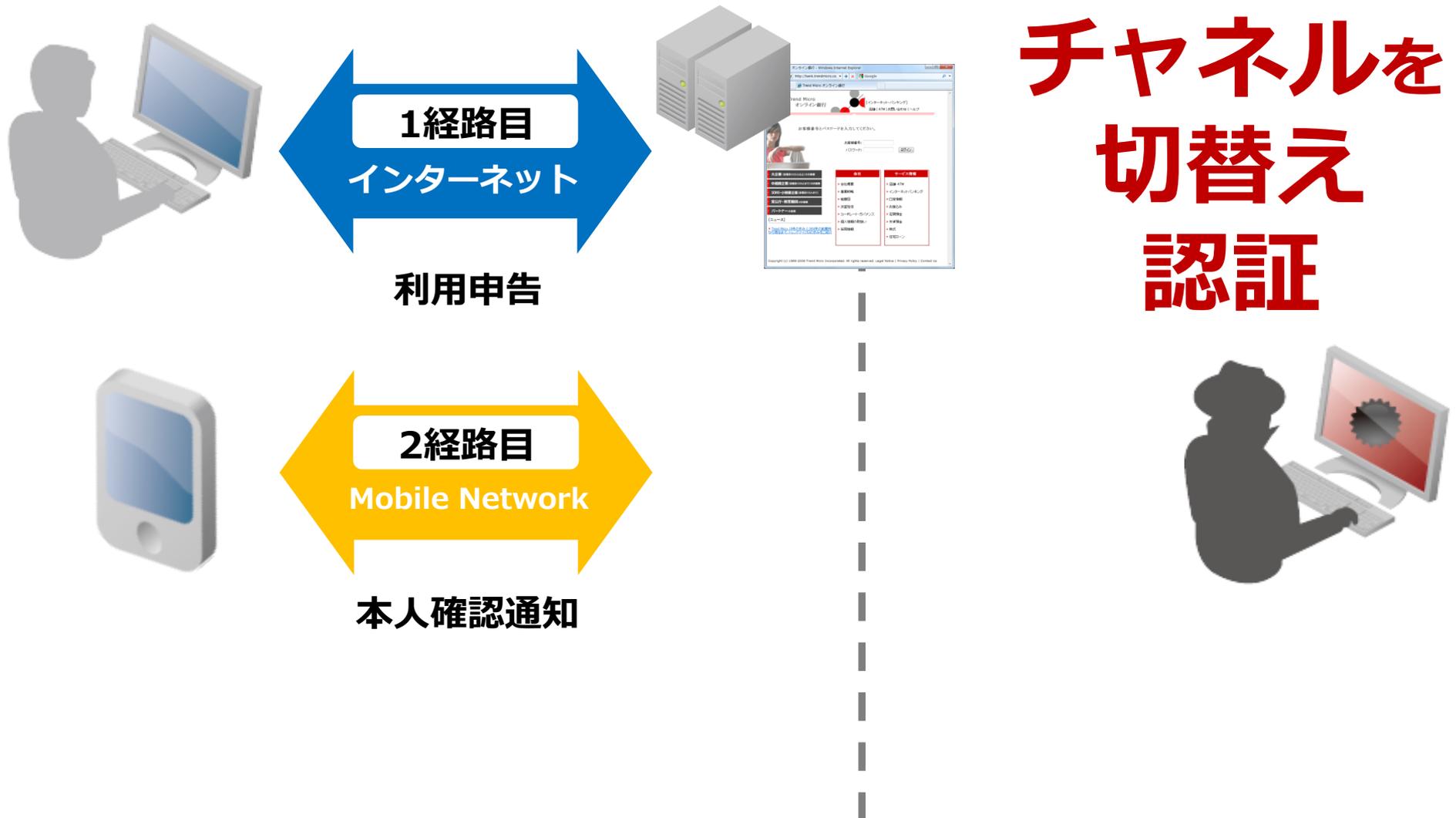
ページが表示されました

インターネット 100%

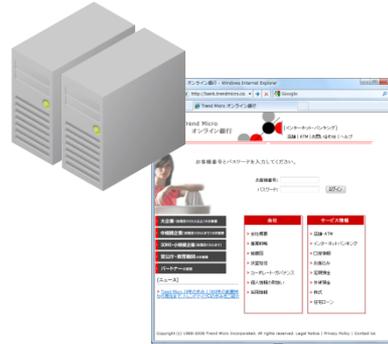
スタート | ログ... | 一般 | CAPS KANA | 14:27

# 「なりすまし」から身を守る術

# 二経路認証 (OUT-OF-BAND Auth)



# 二経路認証 (OUT-OF-BAND Auth)



チャンネルを  
切替え  
認証



2経路目  
不正検知



不正な  
利用申告



# Agenda

1. フィッシング詐欺に関する背景

2. フィッシング詐欺の早期発見

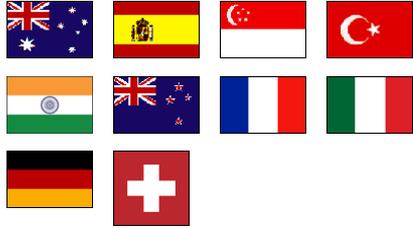
3. オンライン銀行詐欺ツールの変遷

4. モバイル決済を狙った攻撃

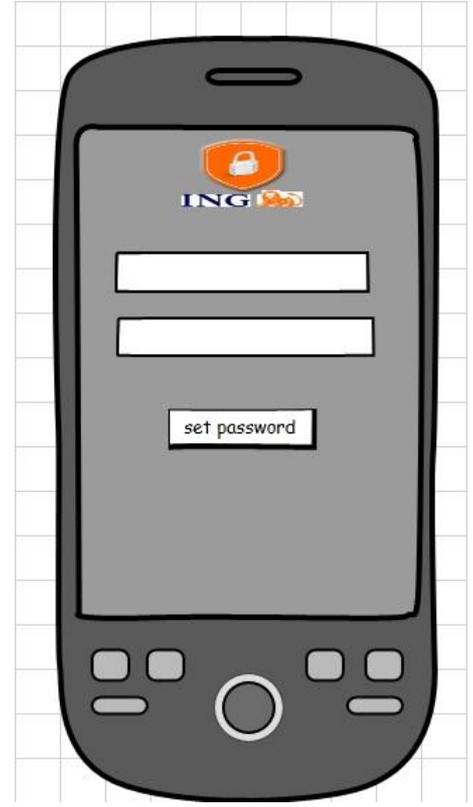
5. 協議会による取り組み



# モバイル銀行詐欺ツール



## 66社の 金融機関に対応



Mobile Bot "Perkele Lite" [Android Only]

Mobile Bot "Perkele Lite" [Android Only]

Зачем терять акки с SMS Alerts/code/etc????  
Снимай Сливки!!!!!!

Только Android приложение.  
Приложение сделано в виде сертификата безопасности с элементом дизайна вашего банка.  
Отсылка Всех Входящих смс-сообщений через SMS.  
Отсылка Всех Входящих смс-сообщений с определением номера через SMS.  
Отступ После запуска через SMS.  
Удаление теневых функций приложения после отправки SMS на телефон с установленным софтом.

Плюсы такого способа от отсутствия блокировки и не убиваемости номера под прием смс (абузами в отличие от домена/хоста)  
И самое главное преимущество это ЦЕНА

1 Приложение = 1000 WMZ  
1 Universal Kit = 15 000  
Есть готовые Банки

Last edited by Perkele; 21.02.2013 at 02:15 AM.

**Perkele Lite for Android**

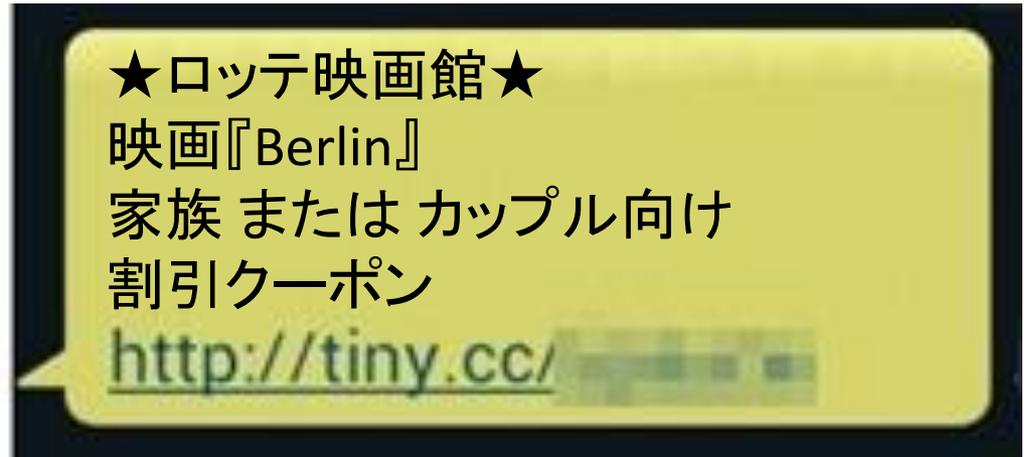
# SMSベースの 二経路認証を突破



# 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

AndroidOS\_CHESTIA



※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

## 警戒心を解くために 悪用された ブランド

Android OS CHESTIA







# Agenda

1. フィッシング詐欺に関する背景

2. フィッシング詐欺の早期発見

3. オンライン銀行詐欺ツールの変遷

4. モバイル決済を狙った攻撃

5. 協議会による取り組み



STOP | THINK | CONNECT™

# 安全なオンライン生活

1. パソコンを常にクリーンに保つ
2. あなたの個人情報を保護する
3. 注意深くネットにつなぐ
4. かしこいネットユーザーになる
5. よきオンライン市民たれ



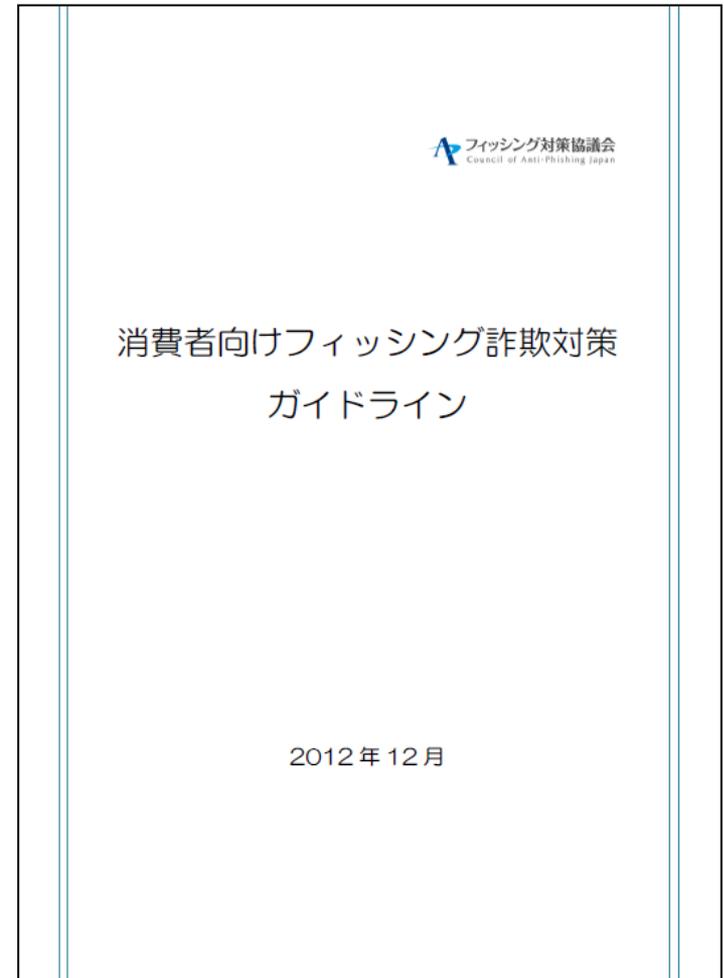
<http://stopthinkconnect.org/tips-and-advice/japanese-tips-and-advice/>

※「Stop Think Connect」とは、「National Cyber Security Alliance」と「Anti-Phishing Working Group」が行なっている、キャンペーン活動

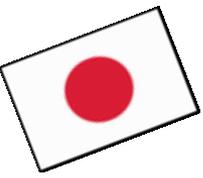
※2012年9月に米州機構、2012年11月にAPCERTと覚書、2012年10月にカナダ公安省が啓発活動で利用

# 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**



[https://www.antiphishing.jp/report/guideline/consumer\\_guideline.html](https://www.antiphishing.jp/report/guideline/consumer_guideline.html)



# 感染の連鎖を絶つ脆弱性対策

## MyJVN バージョンチェッカ



MyJVNバージョンチェッカ

実行 終了 全てを選択 選択をクリア 結果出力

「選択されたソフトウェア製品を「実行」することで、最新バージョンであるかをチェックします。「最新のバージョンではありません」と表示された場合には、表示ボタンを押下後ツール下部の内容を参考にして、ベンダから最新のバージョンを入手してください。利用に関する情報は、[MyJVNのウェブページ](#)を参照ください。

ソフトウェア製品名 ▲	チェック結果 ▲(×○一欄)	結果詳細 ▲
<input checked="" type="checkbox"/> Adobe Flash Player (ActiveX)	× 最新のバージョンではありません	表示
<input checked="" type="checkbox"/> JRE	× 最新のバージョンではありません	表示
<input checked="" type="checkbox"/> Adobe Flash Player (Plug-in)	○ 最新のバージョンです	表示
<input checked="" type="checkbox"/> Adobe Reader	○ 最新のバージョンです	表示
<input checked="" type="checkbox"/> Mozilla Firefox	○ 最新のバージョンです	表示
<input checked="" type="checkbox"/> Adobe Shockwave Player	— インストールされていないか、対象外のバージョンです	
<input checked="" type="checkbox"/> Becky! Internet Mail	— インストールされていないか、対象外のバージョンです	
<input checked="" type="checkbox"/> Lhaplus	— インストールされていないか、対象外のバージョンです	
<input checked="" type="checkbox"/> Lunascape	— インストールされていないか、対象外のバージョンです	
<input checked="" type="checkbox"/> Mozilla Thunderbird	— インストールされていないか、対象外のバージョンです	
<input checked="" type="checkbox"/> OpenOffice.org	— インストールされていないか、対象外のバージョンです	
<input checked="" type="checkbox"/> QuickTime	— インストールされていないか、対象外のバージョンです	
<input checked="" type="checkbox"/> VMware Player	— インストールされていないか、対象外のバージョンです	

## MyJVN セキュリティ設定チェッカ



MyJVNセキュリティ設定チェッカ

実行 終了 全てを選択 選択をクリア 結果出力

「選択されたチェック項目を「実行」することで、セキュリティに関するPC設定値が参考値を満たしているかをチェックします。「参考値を満たしていません」と表示された場合には、表示ボタンを押下後ツール下部の内容を参考にしてPC設定値を変更してください。利用に関する情報は、[MyJVNのウェブページ](#)を参照ください。

チェック項目 ▲	参考値	PC設定値	チェック結果 ▲(×○一欄)	結果詳細 ▲
<input checked="" type="checkbox"/> USBメモリ自動実行に関するパッチ(KB971029) 適用	適用済	適用済	× 参考値を満たしていません	表示
<input checked="" type="checkbox"/> USBメモリ自動実行機能の無効化設定	設定済	設定済	○ 参考値を満たしています	表示

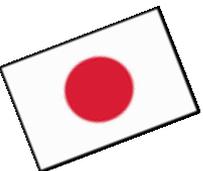
詳細情報

USBメモリ自動実行機能の無効化設定: 詳細情報

このセキュリティ設定は、自動起動をオンにすると、USBメモリをコンピュータに挿入した際に、メモリの内容に従った処理が自動実行されます。自動実行をオフにすると、USBメモリをコンピュータに挿入しても、自動的に実行されなくなります。

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

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



# パスワード管理を託す

## Gadget



パスワードマネージャー「ミルパス」  
**MIRUPASS**  
PASSWORD MANAGER PWIO

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

## Software



# PasswordManager™

<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)



# Thank You!





講演者に対するお問い合わせは  
[noriaki\\_hayashi@trendmicro.co.jp](mailto:noriaki_hayashi@trendmicro.co.jp)

**PasswordManager™ 無料版**  
5つまでのIDとパスワードを期間制限なしにご利用いただけます。  
<http://safe.trendmicro.jp/purchase/pm/trialthanks.aspx>



フィッシングの報告、お問い合わせは  
[info@antiphishing.jp](mailto:info@antiphishing.jp)

協議会への入会に関しては  
[antiphishing-sec@jpcert.or.jp](mailto:antiphishing-sec@jpcert.or.jp)

第17回 サイバー犯罪に関する白浜シンポジウム  
Shirahama Cyber Crime Symposium Vol. 17  
2013.05.24 (fri) Big-U

