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 Threat Research

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 **T**hreat **R**esearch

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ットリサーチへ異動。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。

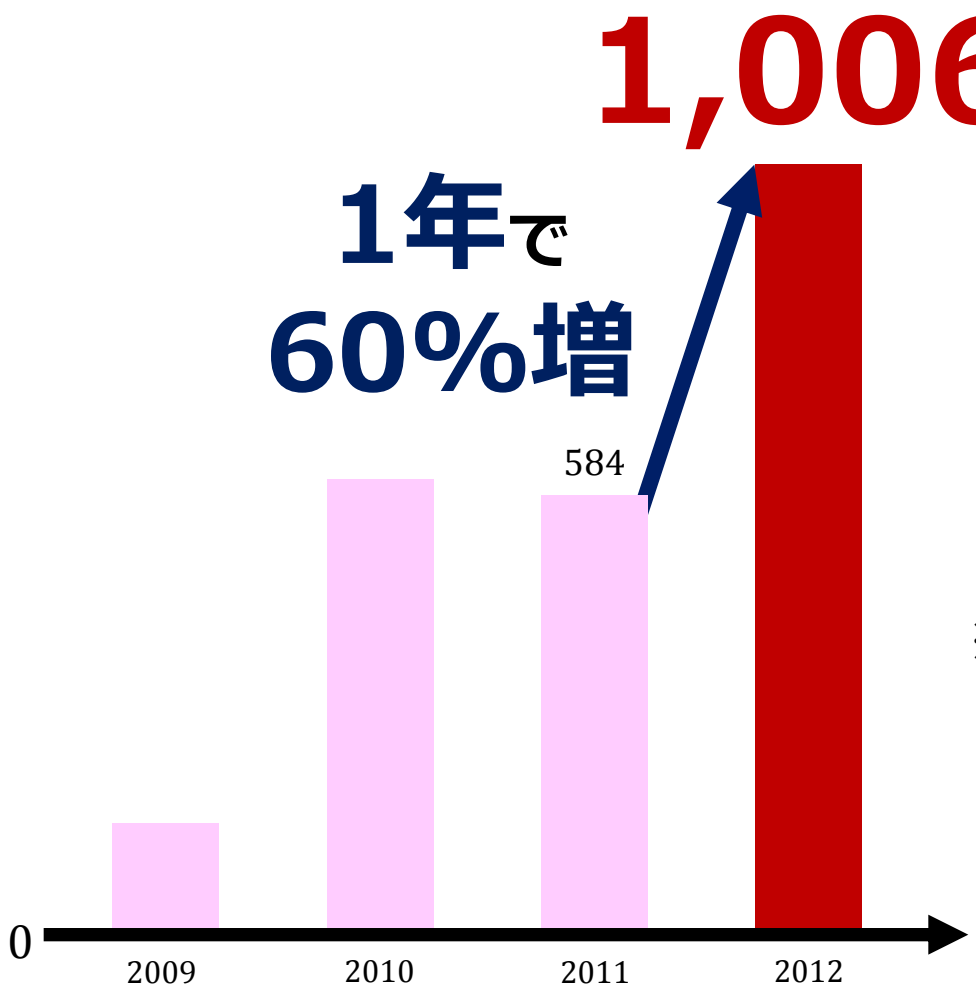
フィッシング対策協議会
運営委員

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

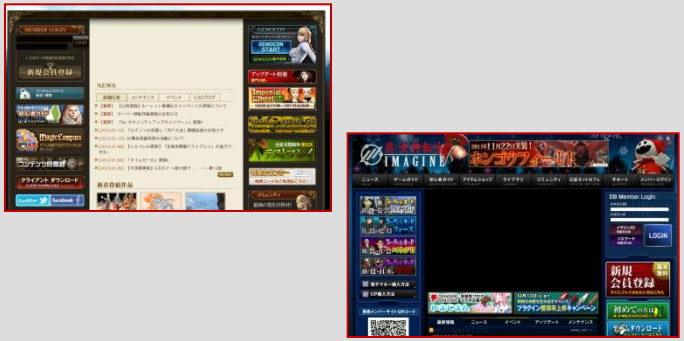
※出典：フィッシング対策協議会　月次報告書「フィッシング報告状況」より、「フィッシングサイトのURL件数」を抽出。
講演者集計、グラフ作成

フィッシャー が狙う4つの業界

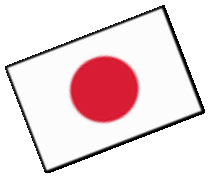
金融業界

Social Network

オンラインゲーム

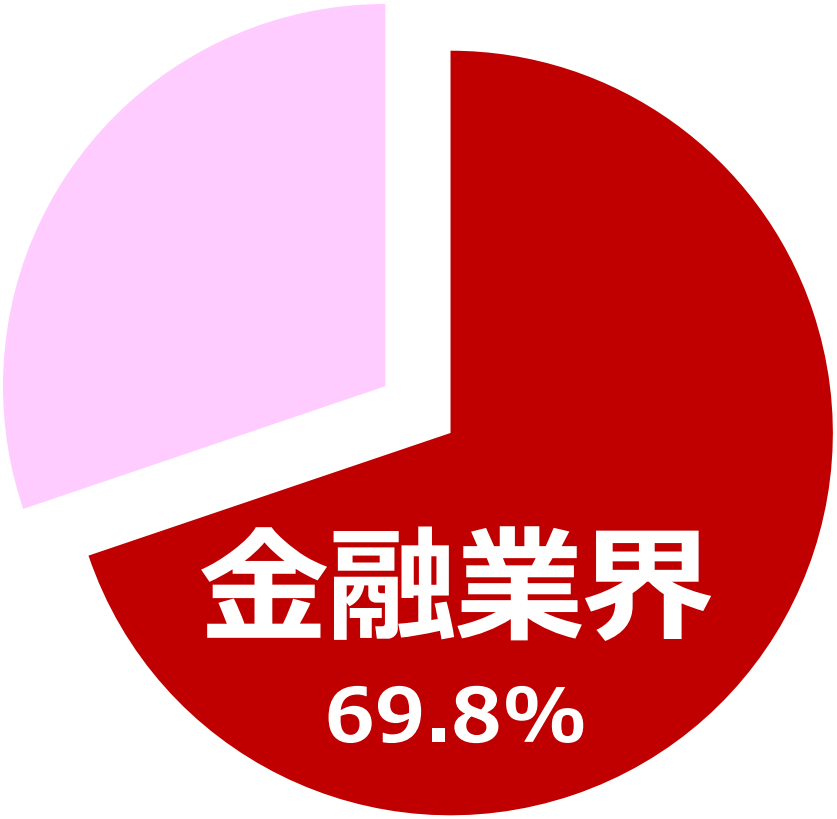


プロバイダ



金融業界

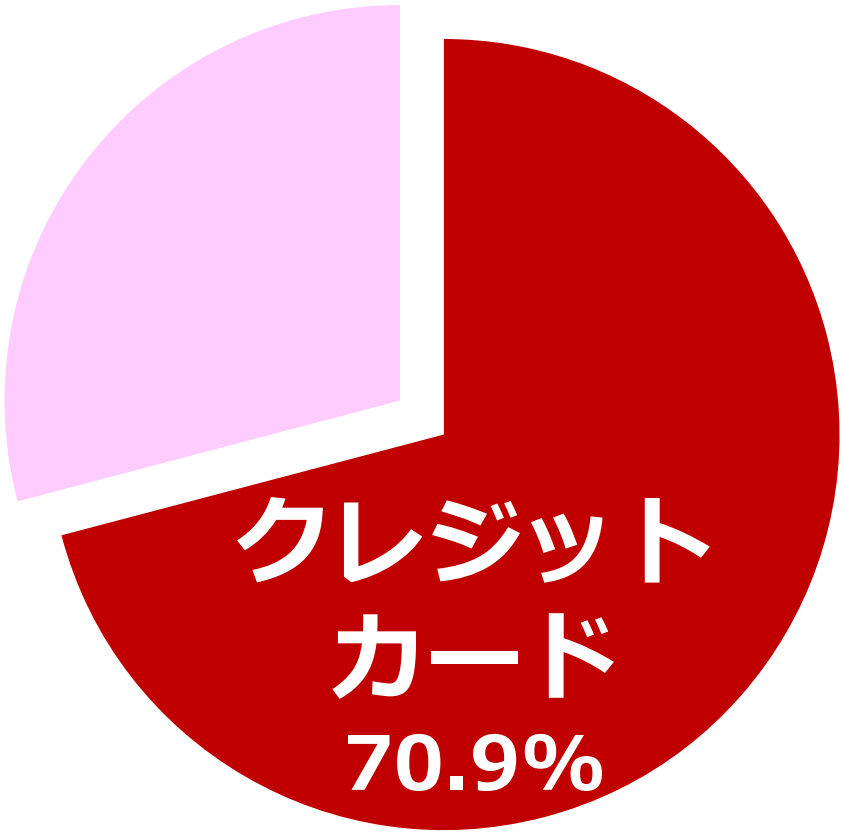
最も深刻な被害



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

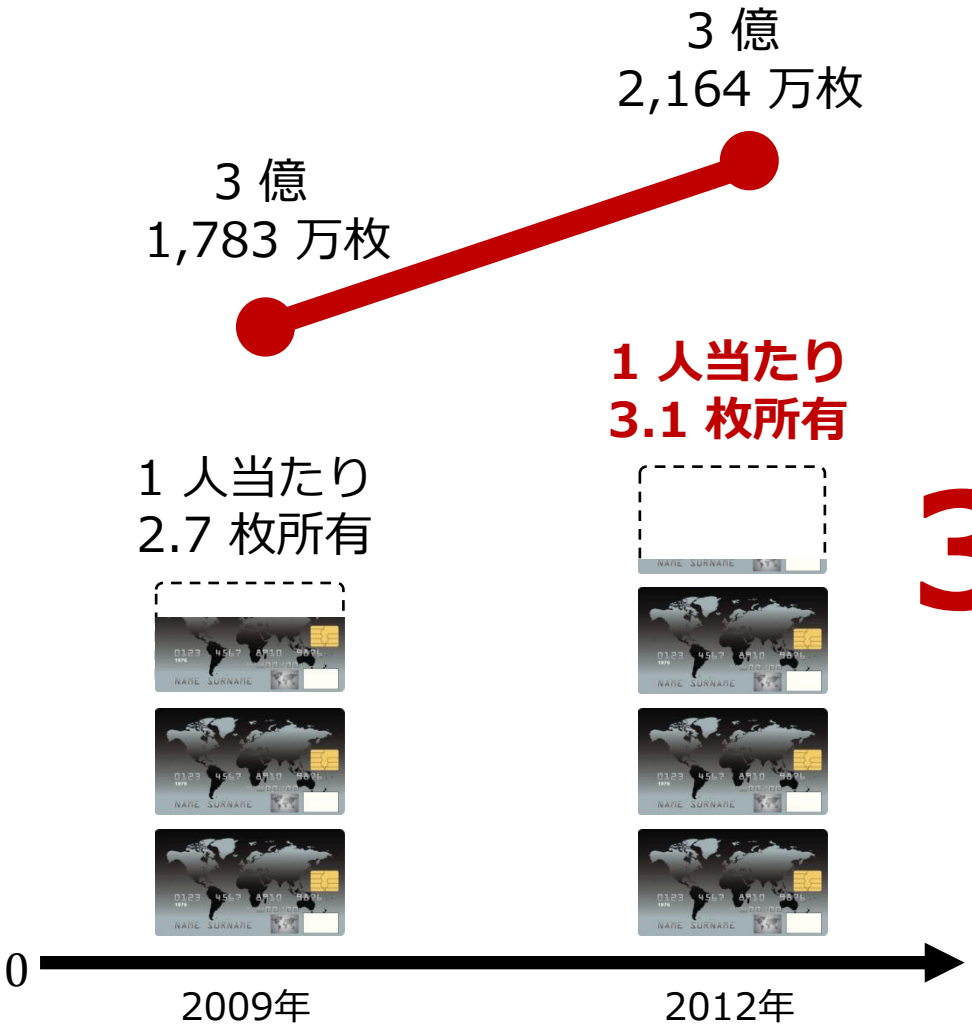
最も身近なオンライン決済方法

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



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

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があり

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.com/...

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
・VISA カード情報を
・これでアカウントが
ナ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

Agenda

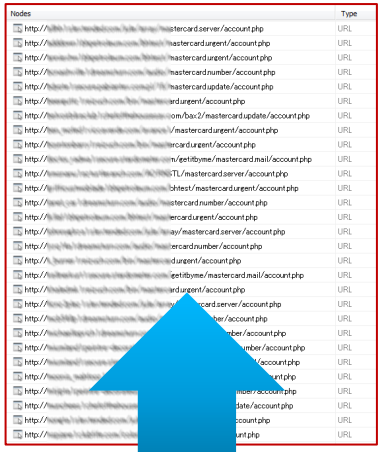
1. フィッシング詐欺に関する背景
2. フィッシング詐欺の早期発見
3. オンライン銀行詐欺ツールの変遷
4. モバイル決済を狙った攻撃
5. 協議会による取り組み

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

統計と知覚で早期発見

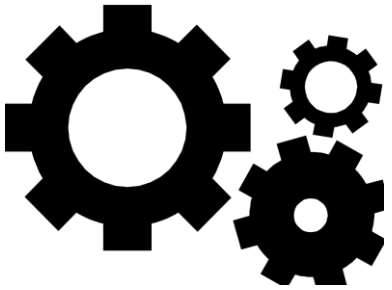
観測
統計



人間
の
知覚

Open Source Intelligence

収集情報



監視ルール

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://[redacted]stercard.server/account.php	URL
http://[redacted]mastercard.urgent/account.php	URL
http://[redacted]mastercard.urgent/account.php	URL
http://[redacted]mastercard.number/account.php	URL
http://[redacted]mastercard.update/account.php	URL
http://[redacted]rd.urgent/account.php	URL
http://[redacted]update/account.php	URL
http://[redacted]ccount.php	URL
http://[redacted].php	URL
http://[redacted]ard.mail/account.php	URL
http://[redacted]/account.php	URL
http://[redacted]ent/account.php	URL
http://[redacted].php	URL
http://[redacted]ay/mastercard.server/account.p	URL
http://[redacted]ercard.number/account.php	URL
http://[redacted]d.urgent/account.php	URL
http://[redacted]getitbyme/mastercard.mail/acco	URL
http://[redacted]ard.urgent/account.php	URL
http://[redacted]y/mastercard.server/account.ph	URL
http://[redacted]stercard.number/account.php	URL
http://[redacted]o/mastercard.number/account.p	URL
http://[redacted]n/flash/mastercard.number/	URL
http://[redacted]etitbyme/mastercard.mail/account.php	URL
http://[redacted]htest/mastercard.urgent/account.php	URL
http://[redacted]lash/mastercard.number/account.php	URL
http://[redacted]bax2/mastercard.update/account.php	URL
http://[redacted]mastercard.server/account.php	URL
http://[redacted]ercard.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 INTelligence
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。

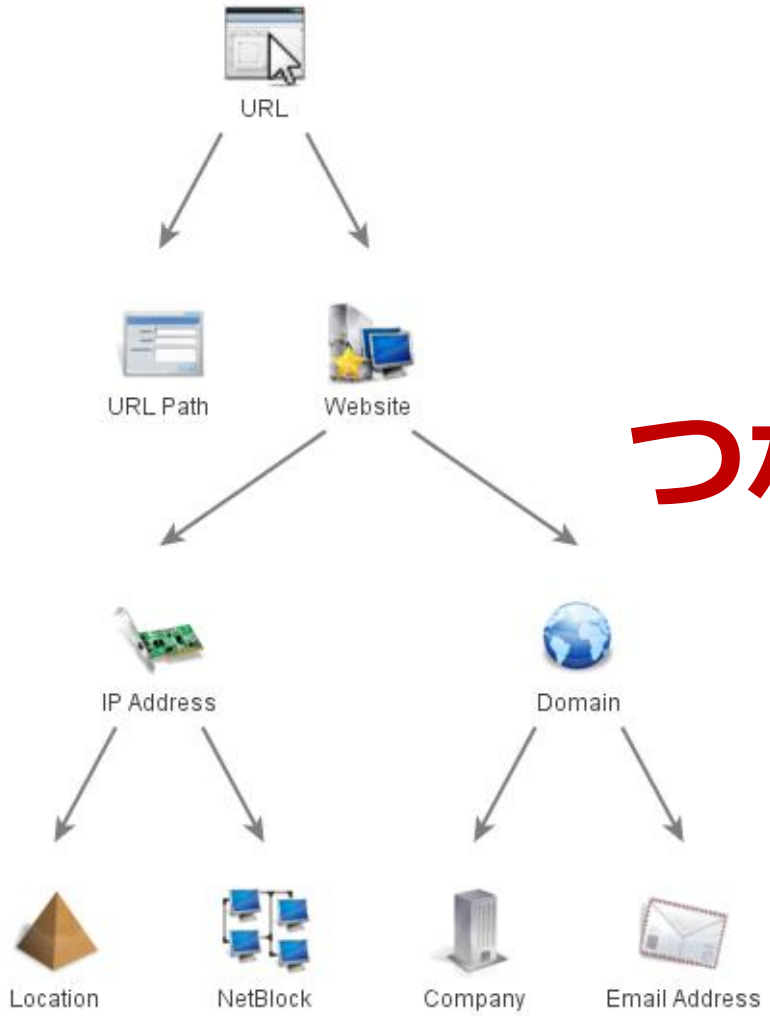
URLに隠されたパターン

URL PATH についてワードクラウド作成

データの可視化

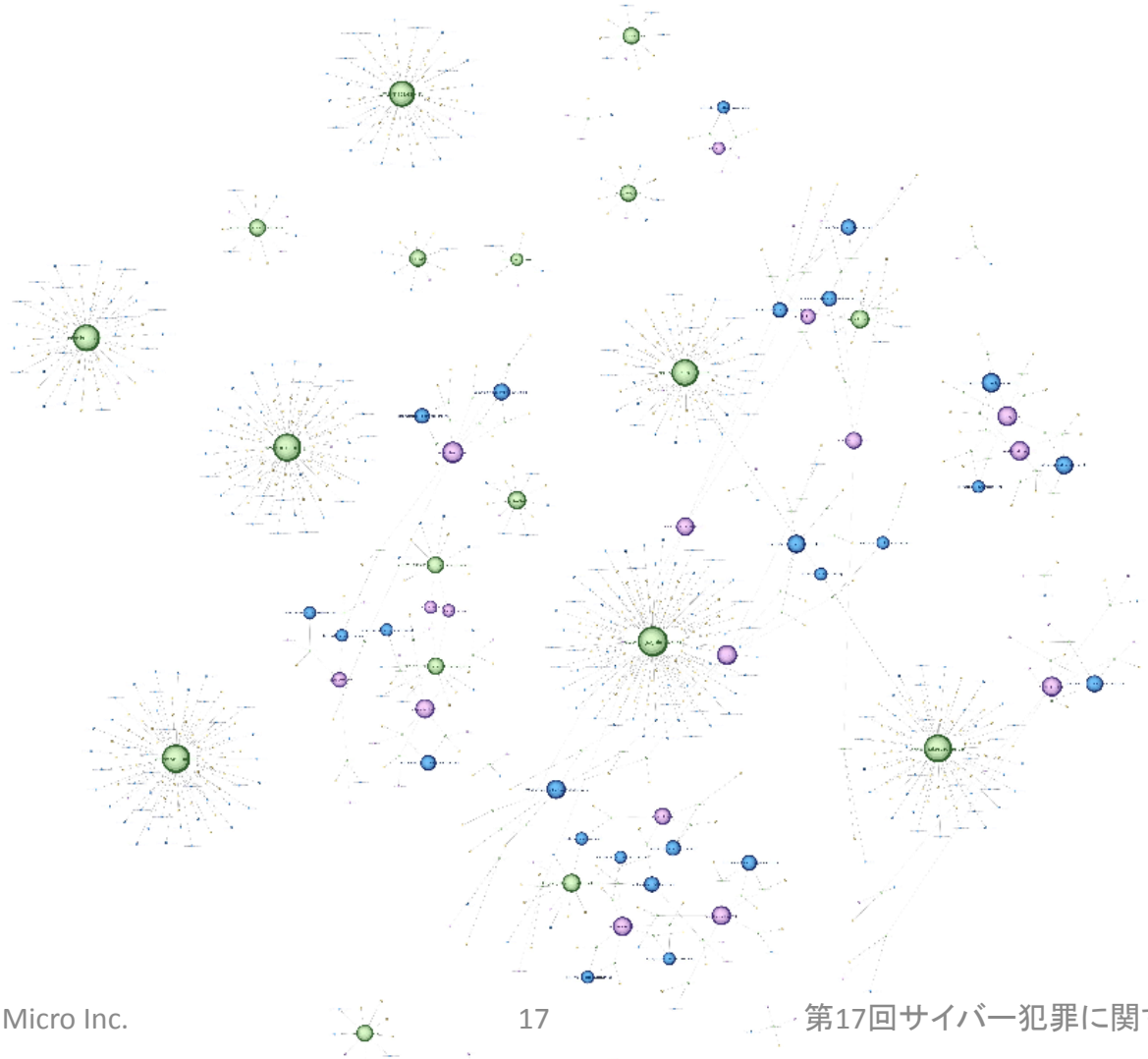
※ワードクラウド：単語の出現頻度を分析し、頻度に応じた大きさで図示

潜在的な攻撃のリンク

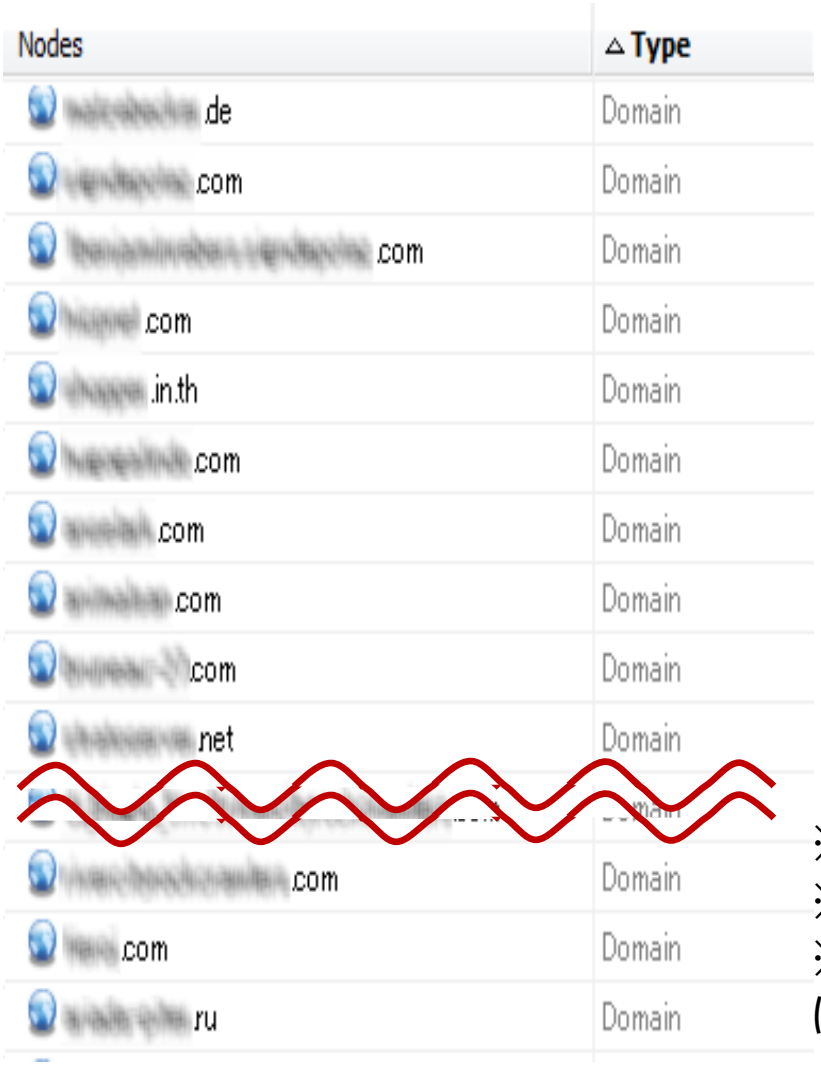


構成要素の
つながり / 重なり合い
注目

「関係」に共通するパターン
監視対象の特定



5ケ月で400件以上発見



Nodes	△ Type
.de	Domain
.com	Domain
.com	Domain
.com	Domain
.in.th	Domain
.com	Domain
.com	Domain
.com	Domain
.com	Domain
.net	Domain
.com	Domain
.com	Domain
.ru	Domain

悪意あるドメイン名の登録

ゼロ

※407件のフィッシングURLを発見
※フィッシングURLを構成するドメインは72件
※悪意あるドメイン名の登録（正規のブランド名によく似たドメイン名）は見られなかった。

サーバに対するハッキング

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

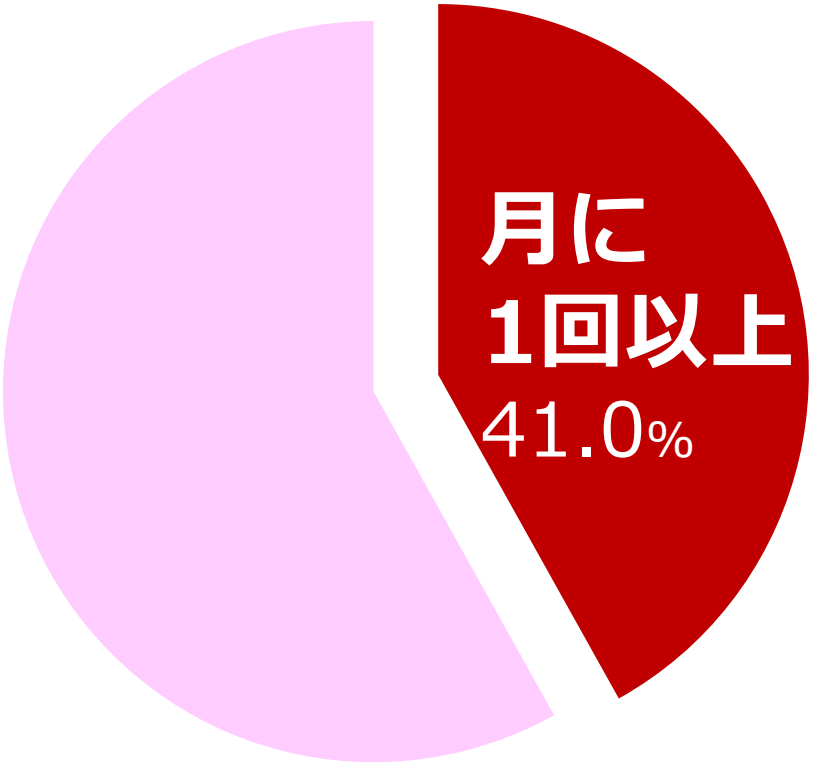
- 統計学と可視化を組み合わせた分析は短時間で高精度なルール作成が可能
- 複雑な分析を単純化して明確かつタイムリーに情報共有が可能
- 更なる性質の解析により予防と予測への利用が期待できる

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

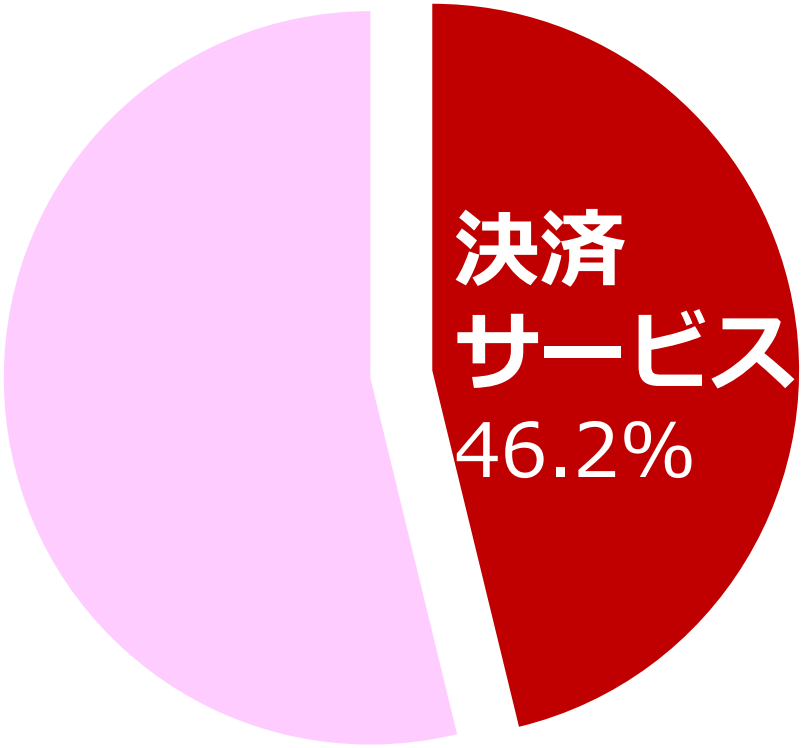
オンラインバンキングに関する調査



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/

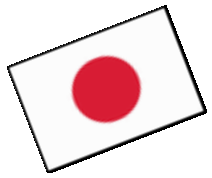
アクセス目的

オンラインバンキングに関する調査

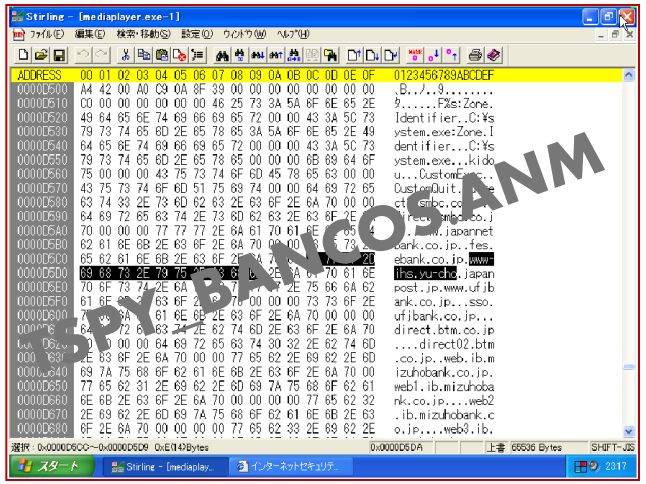


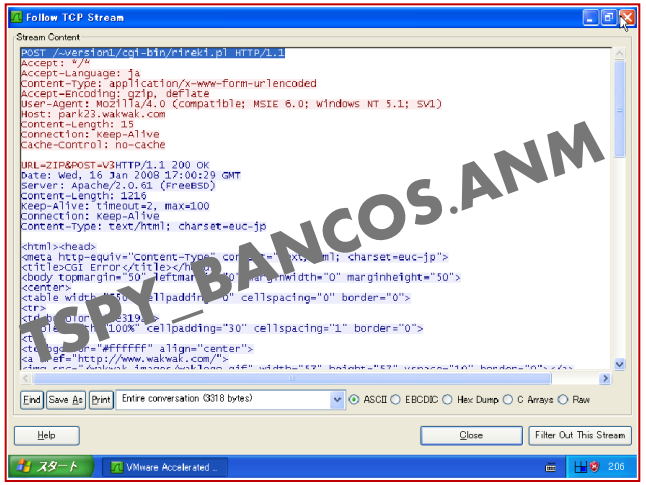
出典：楽天リサーチ株式会社『オンラインバンキングに関する調査』（2012/5/29 - 30）、N = 1,000,
http://research.rakuten.co.jp/report/20120621/

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

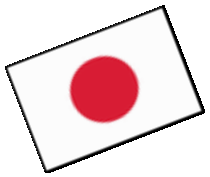
60以上の邦銀が標的

標的

ID と **パスワード**

盗む手口

KeyLogger と **Sniffer**



2011
Fake Popup
Two-Factor Auth

2011年

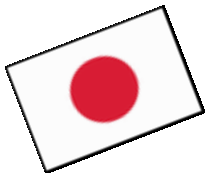
新たな対策技術を
狙うフィッシャー

NEW **標的**

二要素認証情報

盗む手口

偽のポップアップ



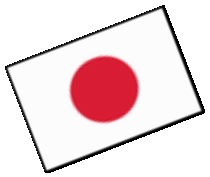
2005
KeyLogger
Sniffing ID & Pass

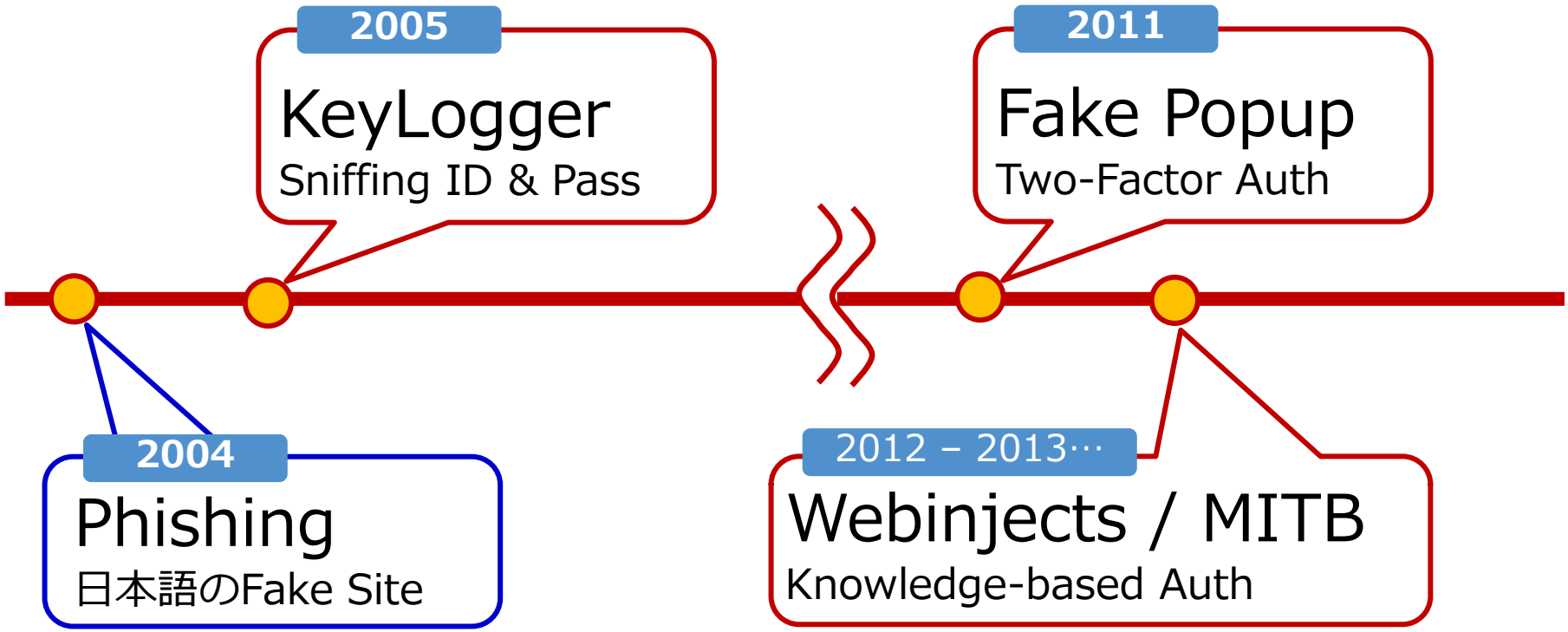
2011
Fake Popup
Two-Factor Auth

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



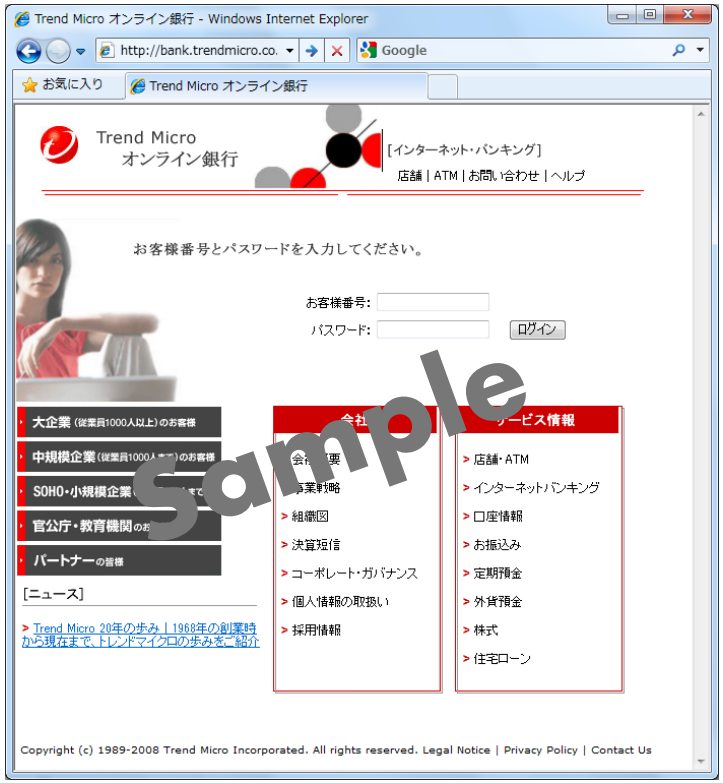


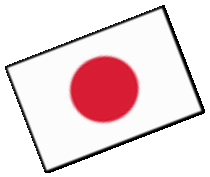
犯罪技術は年々進化

2012

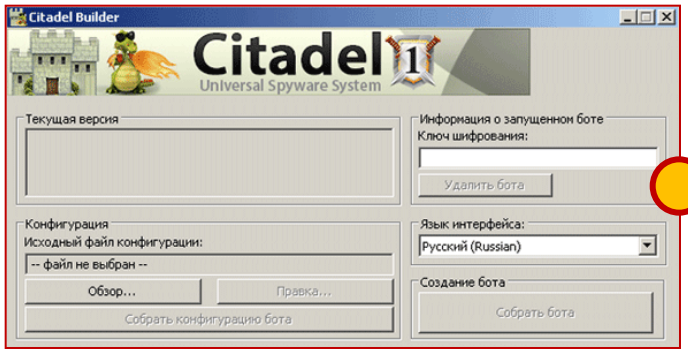
MITB - Citadel

MITBにより被害の舞台は本物へ

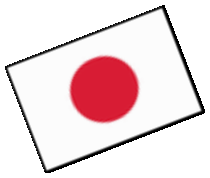




Citadel の標的を探る

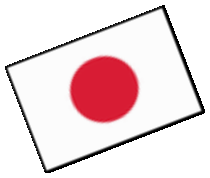


“config.bin”
の**解読**により
標的を**知る**

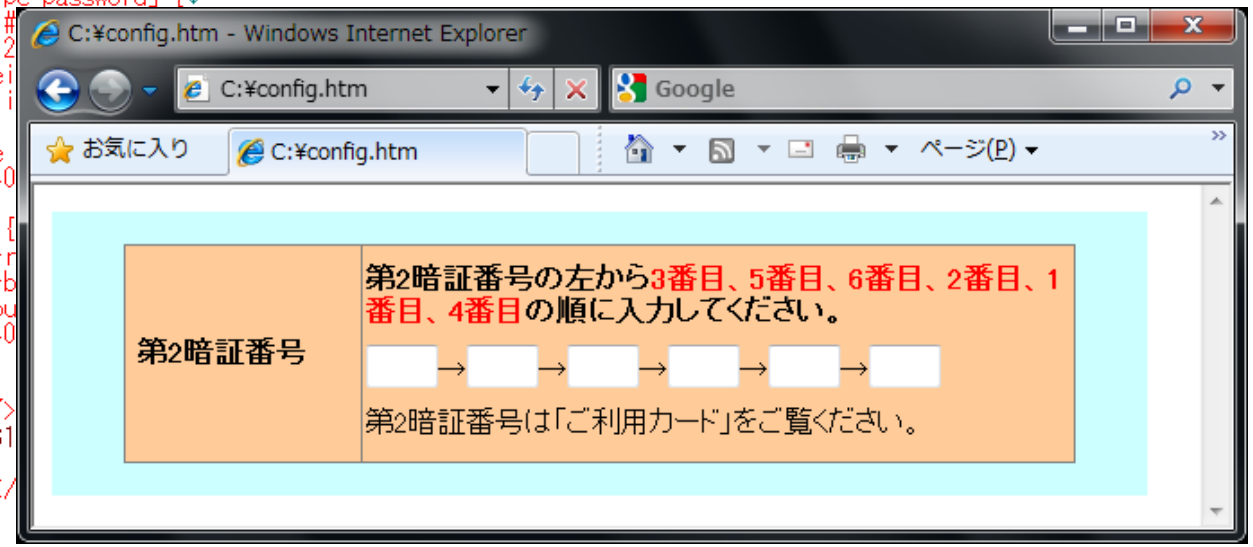


“config.bin” の解析…


```
<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>↓
```

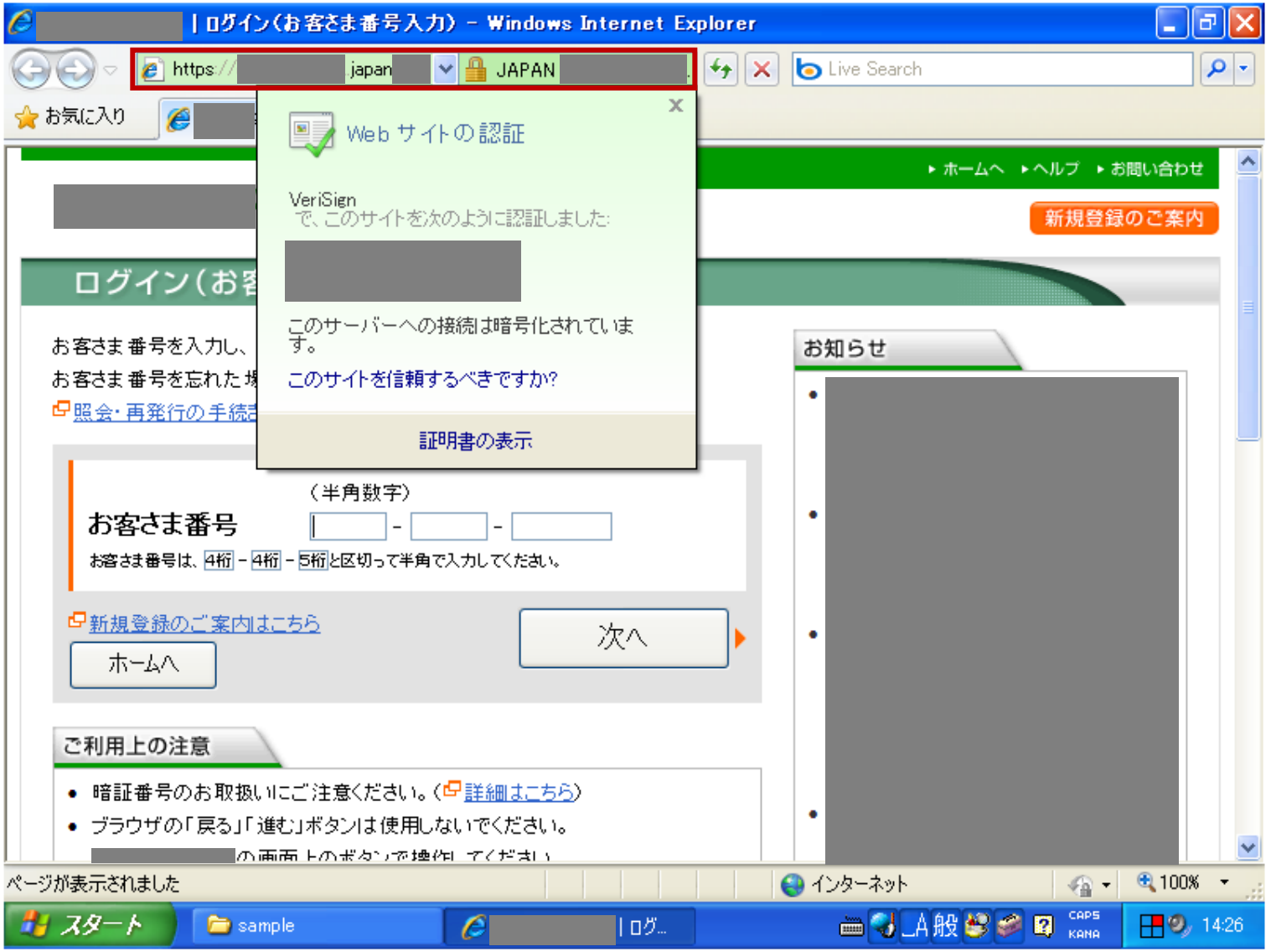


“config.bin” の解析…

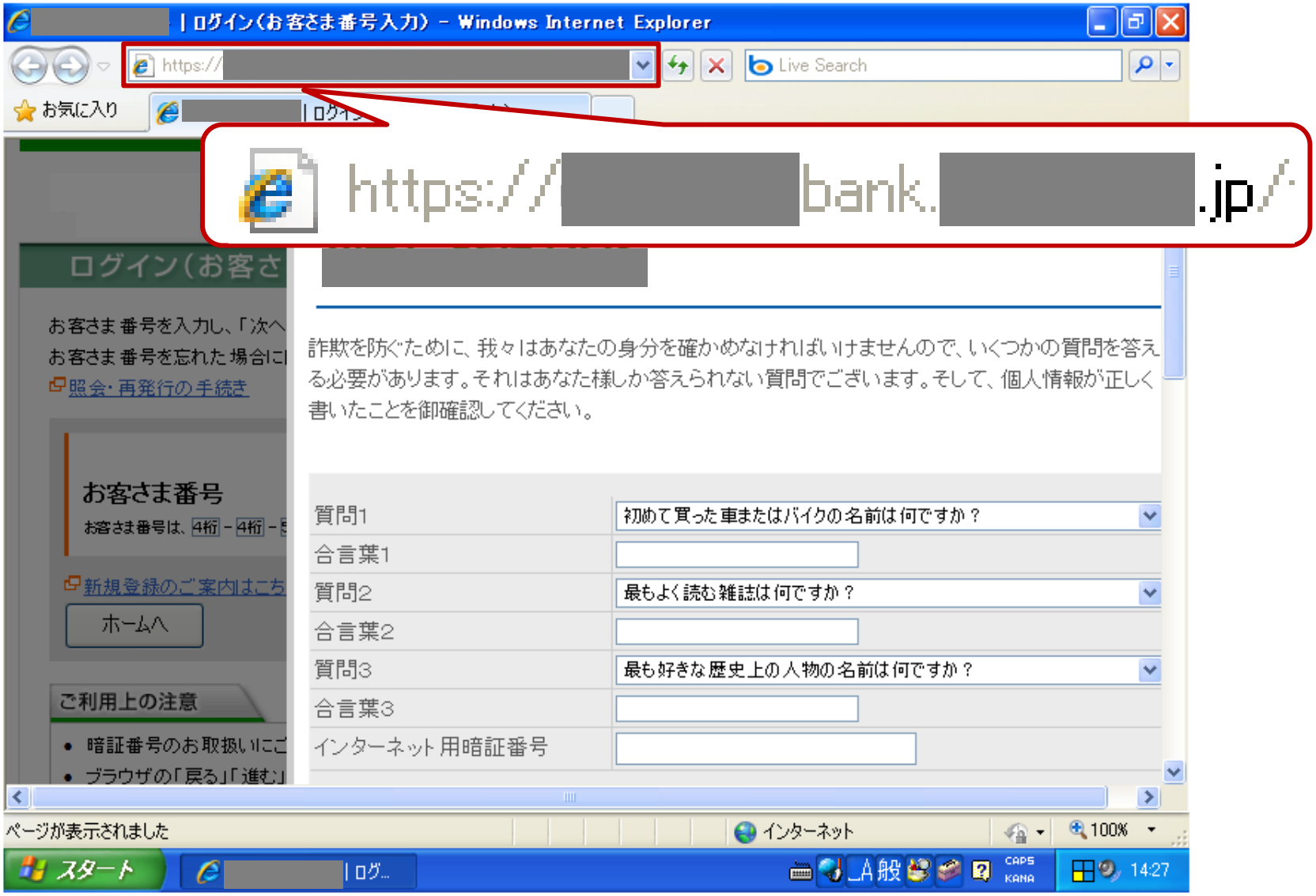


日本を標的とした事例

多くの銀行で採用されるEVSSL



機能を知ることで防げる脅威

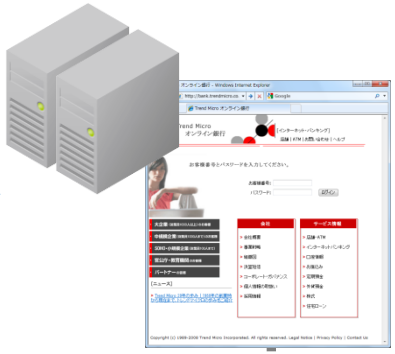


「なりすまし」から身を守る術

二経路認証(OUT-OF-BAND Auth)

1経路目

インターネット



利用申告

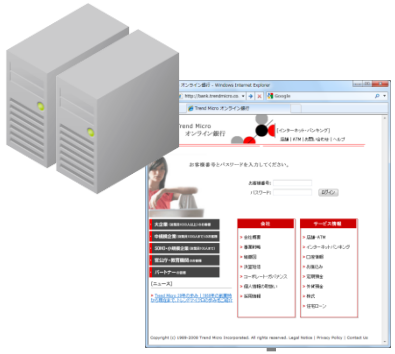
2経路目

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

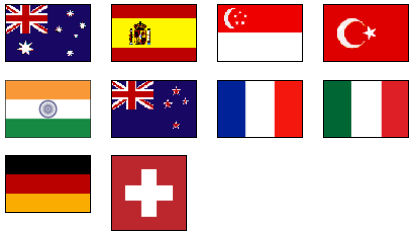
2経路目

不正検知

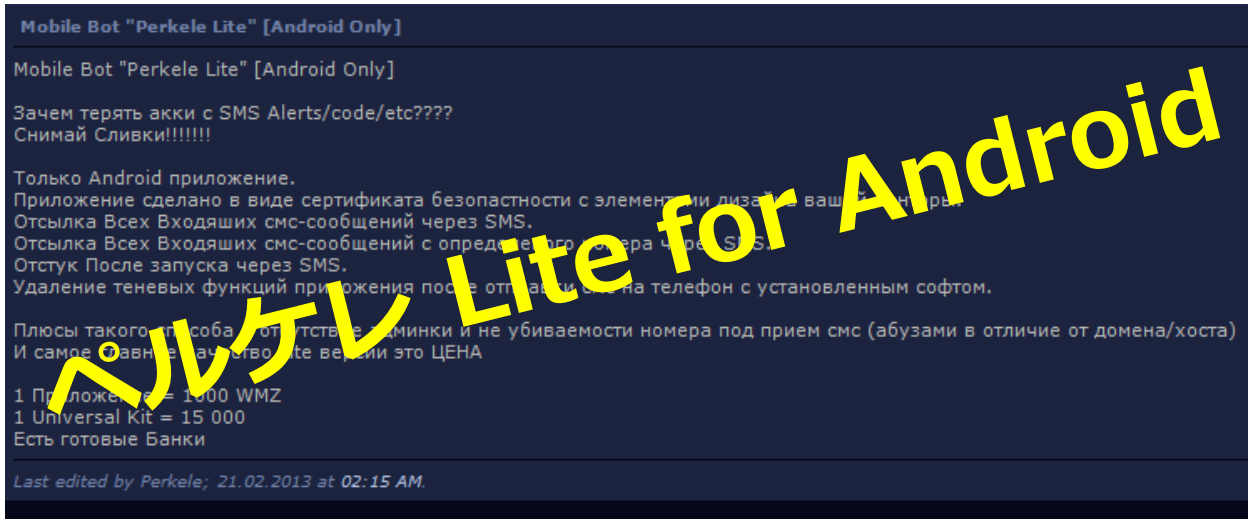
Agenda

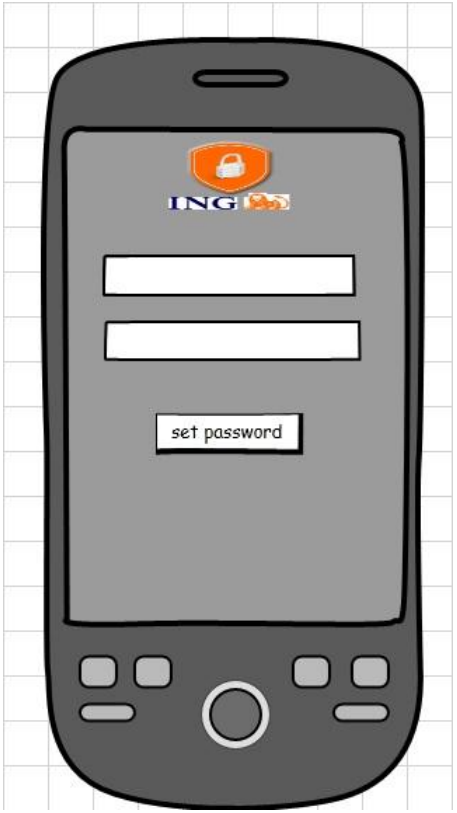
1. フィッシング詐欺に関する背景
2. フィッシング詐欺の早期発見
3. オンライン銀行詐欺ツールの変遷
4. モバイル決済を狙った攻撃
5. 協議会による取り組み

モバイル銀行詐欺ツール



66社の金融機関に対応

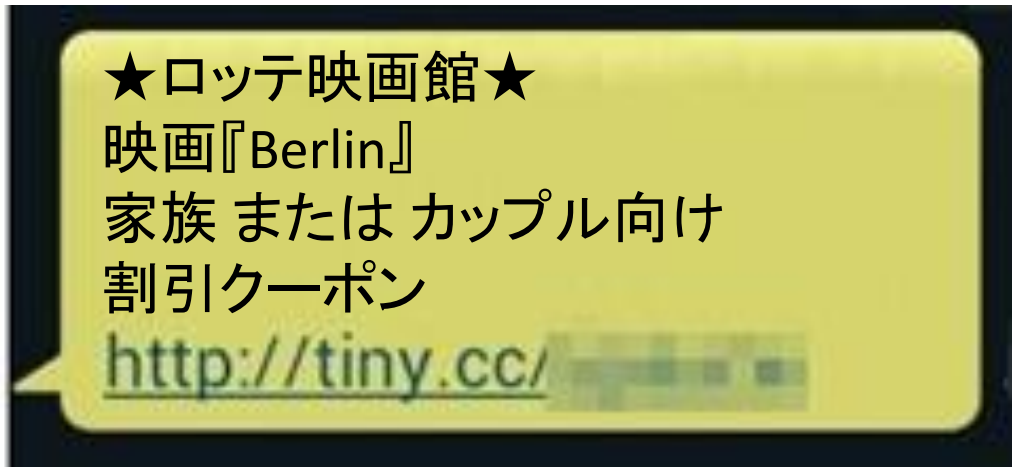




SMSベースの二経路認証を突破

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



※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

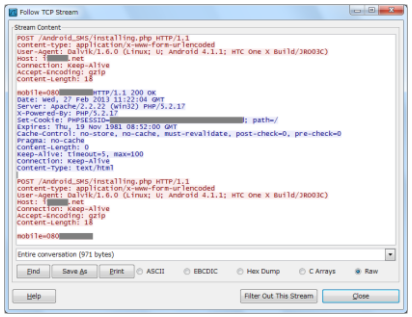
AndroidOS_CHEST.A

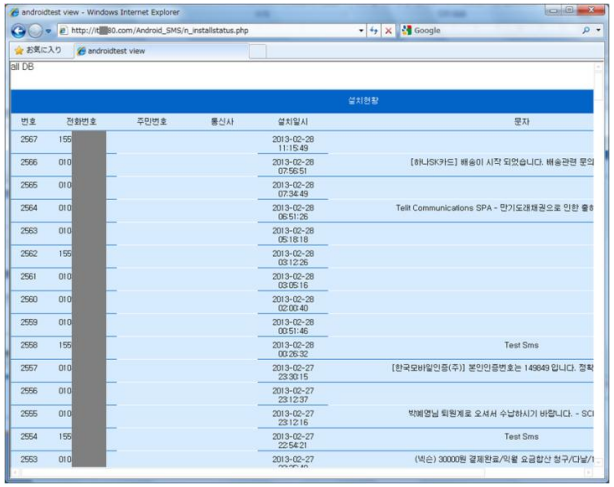
警戒心を解くために
悪用されたブランド

認証番号の横取り

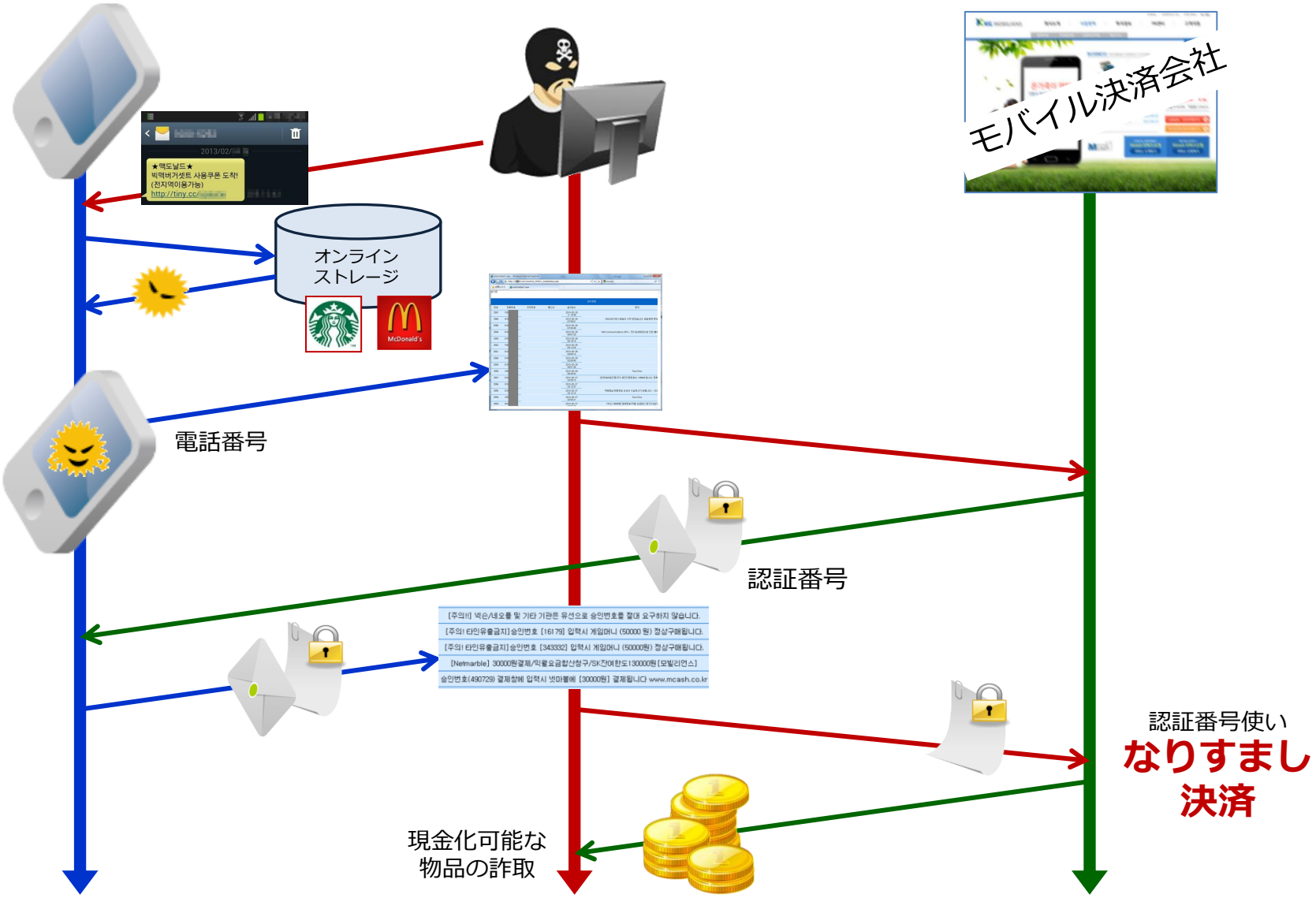
- 発信元が
- 利用者へ
- 攻撃者へ

のみ監視
を見せない
を転送





これが被害の全貌だ！


★맥도날드★
빅맥버거셋트 사용쿠폰 도착!
(전지역이용가능)
http://tiny.cc/
2013/02/
オンライン
ストレージ
McDonald's
モバイル決済会社
電話番号
認証番号
[주의!] 넥슨/네오플 및 기타 기관은 유선으로 승인번호를 절대 요구하지 않습니다.
[주의! 타인유출금지] 승인번호 [1617] 입력시 게임머니 (50000 원) 정상구매됩니다.
[주의! 타인유출금지] 승인번호 [343332] 입력시 게임머니 (50000원) 정상구매됩니다.
[Nelmarble] 30000원결제/직렬요금합산청구/SK잔여한도130000원[모빌리언스]
승인번호(490729) 결제참에 입력시 넷마블에 [30000원] 결제됩니다 www.mcash.co.kr
認証番号使い
なりすまし
決済
現金化可能な
物品の詐取

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

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**

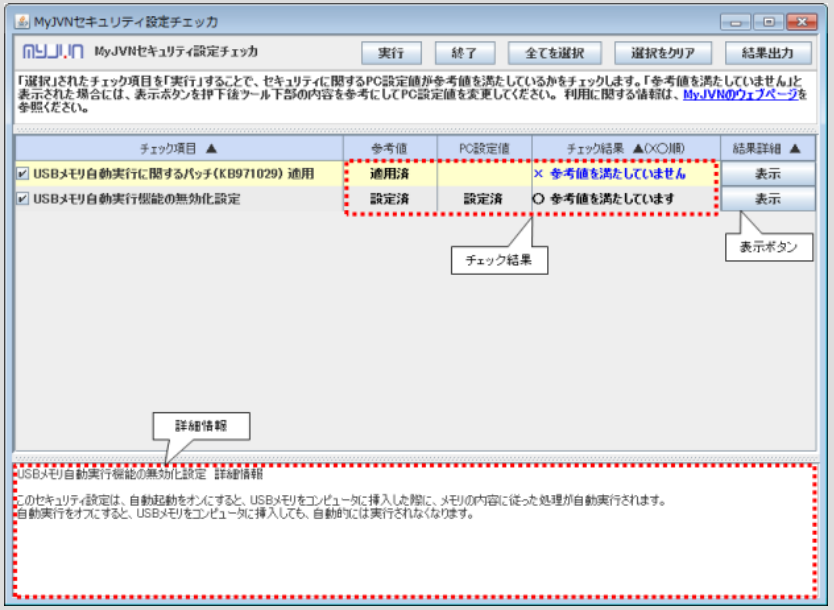
https://www.antiphishing.jp/report/guideline/consumer_guideline.html

感染の連鎖を絶つ脆弱性対策

MyJVN バージョンチェッカ

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」

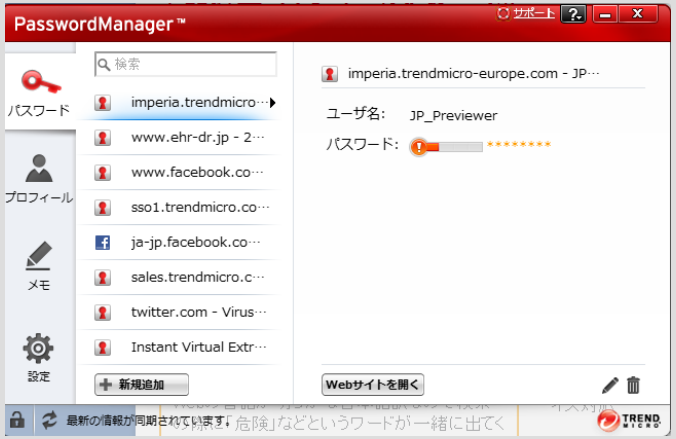
MIRUPASS

PASSWORD MANAGER PW10

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

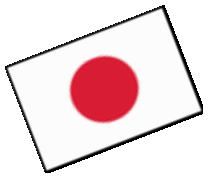
Software

TREND MICRO™



PasswordManager™

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



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

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

Thank You!

TREND MICRO™

講演者に対するお問い合わせは
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

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

フィッシングの報告、お問い合わせは
info@antiphishing.jp

協議会への入会に関しては
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

SHIRAHAMA
CYBER CRIME SYMPOSIUM