Internet Week 2014

個人に牙をむくサイバー攻撃…
狙うは、ずばり「お金」です

トレンドマイクロ株式会社
リージョナルトレンドラボ
木村 仁美

自己紹介

- 木村 仁美（きむら ひとみ）
  - 電子認証/PKI
  - オンライン銀行を狙うマルウェア

Agenda

- 狙われる個人のお金
- 最近の流行
  - ワンクリック詐欺
  - ランサムウェア
  - グレーウェア・アドウェア
  - オンライン銀行詐欺ツール
  - おまけ
- まとめ
- 身の守り方

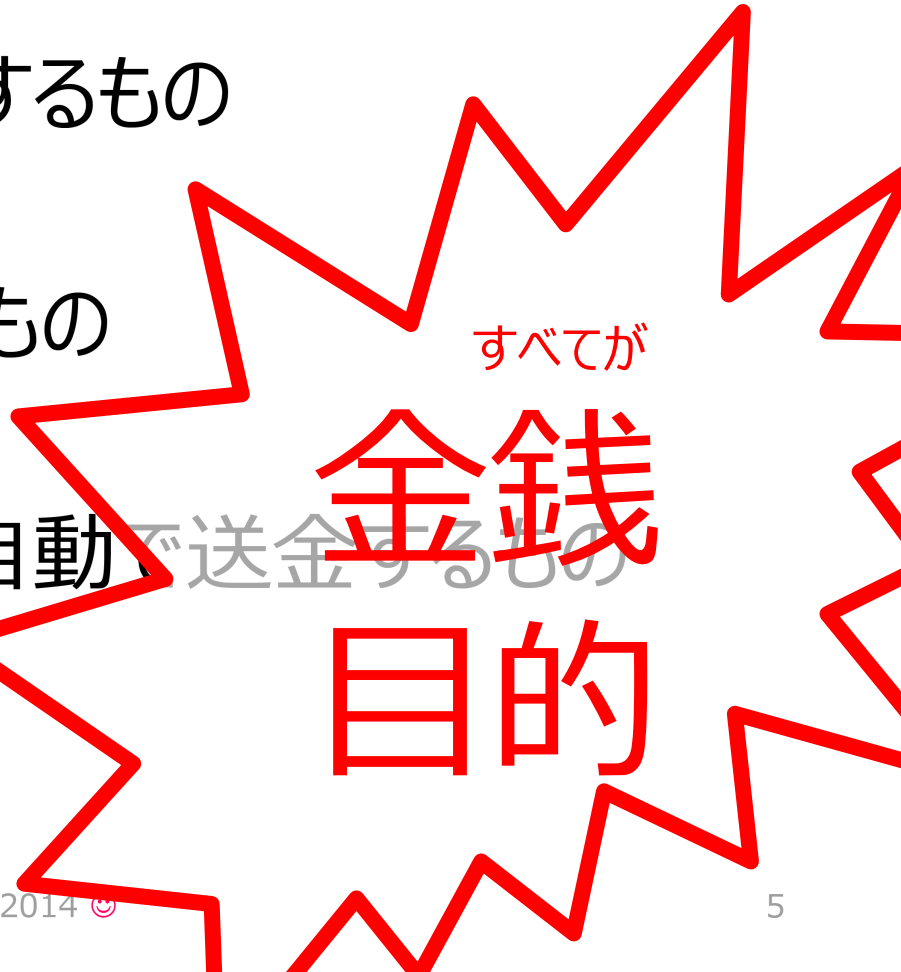
狙われる個人のお金

× ~~サイバー犯罪者がサイバー犯罪をやっている~~

○「犯罪者が効率を上げるためにサイバー犯罪をやっている」と思ってもらうほうが自然

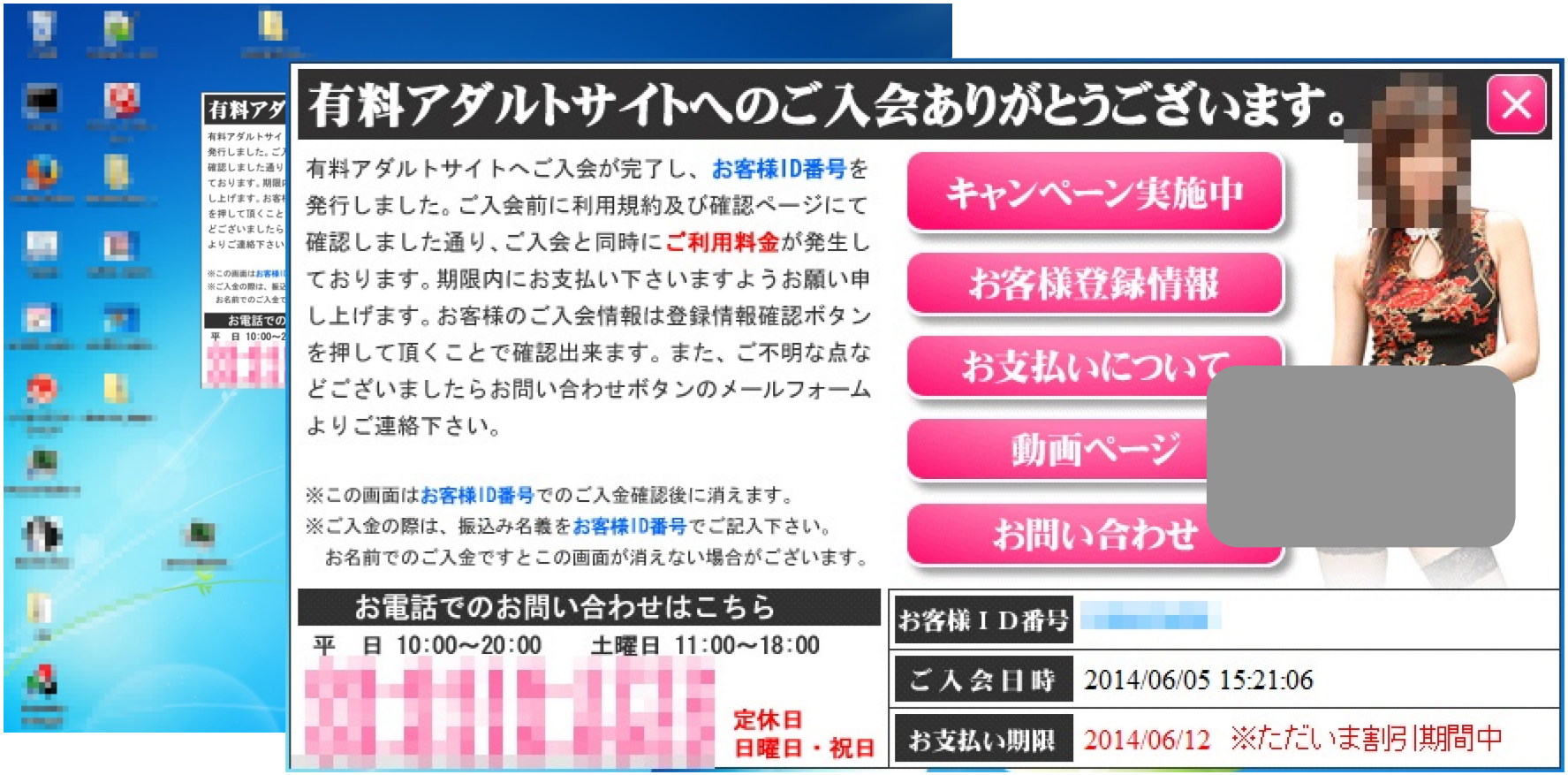
消費者シーンでの流行

- エッチな画像をデスクトップに出して脅迫するもの
  - ワンクリック詐欺
- 写真を暗号化して脅迫するもの
  - ランサムウェア
- いつの間にかいる邪魔なもの
  - グレーウェア・アドウェア
- オンラインバンキングから自動で送金するもの
  - オンライン銀行詐欺ツール



ワンクリック詐欺

- 日本特有。これを語らずして何を語るか



ワンクリック詐欺

- 詐欺なのでくれぐれもお金を払わないように！
- 無視するのが一番。連絡先を渡さないこと。

[参考]

- 国民生活センター
  あわてないで!! クリックしただけで、いきなり料金請求する手口
  http://www.kokusen.go.jp/news/click.html
  →なんと、2004年12月13日に公開された歴史あるページです

- 総務省
  国民のための情報セキュリティサイト － ワンクリック詐欺に注意
  http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/security01/06.html

ランサムウェア

- 盛り上がりを見せた「暗号化型」

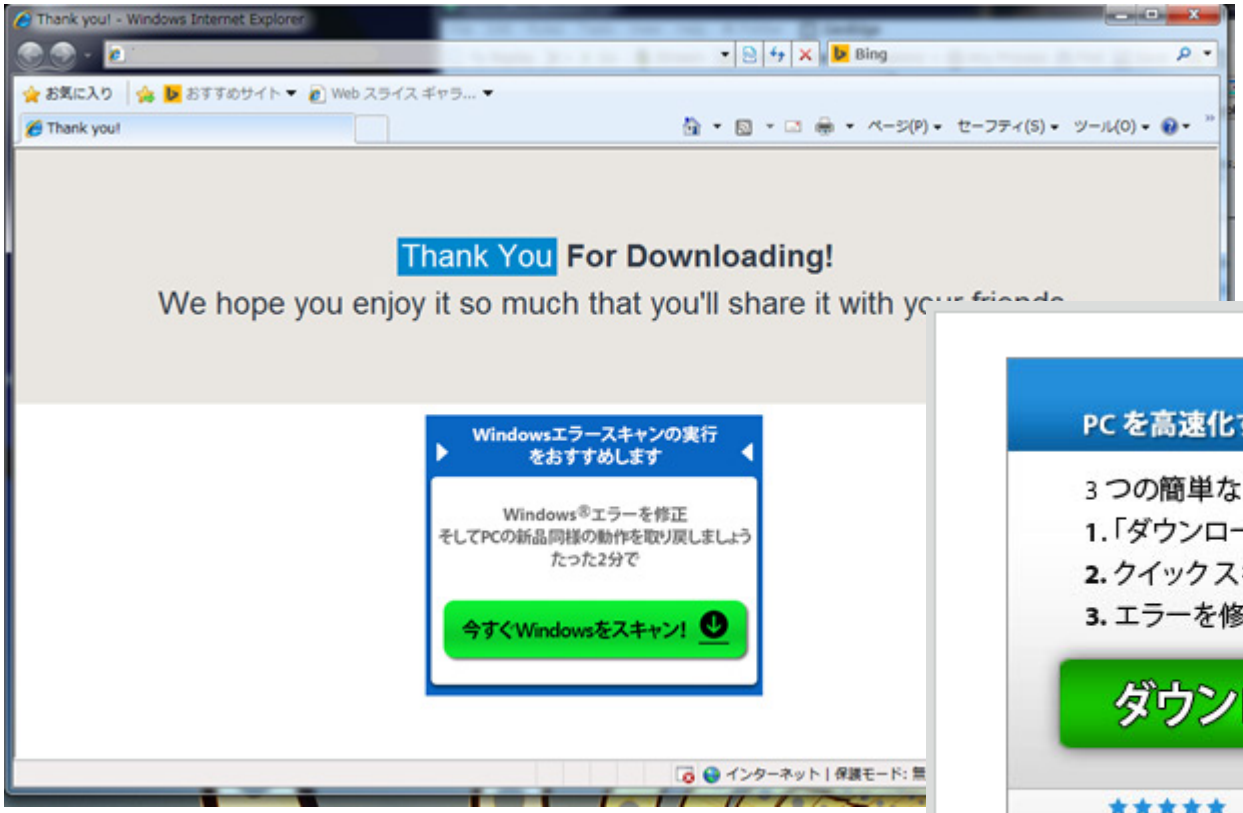
企業の業務用PCが感染し
ネットワークドライブのファイルが
軒並み暗号化される事例も
観測されています…☠

ランサムウェア

- 警察を装いPCをロックする手口も引き続き観測

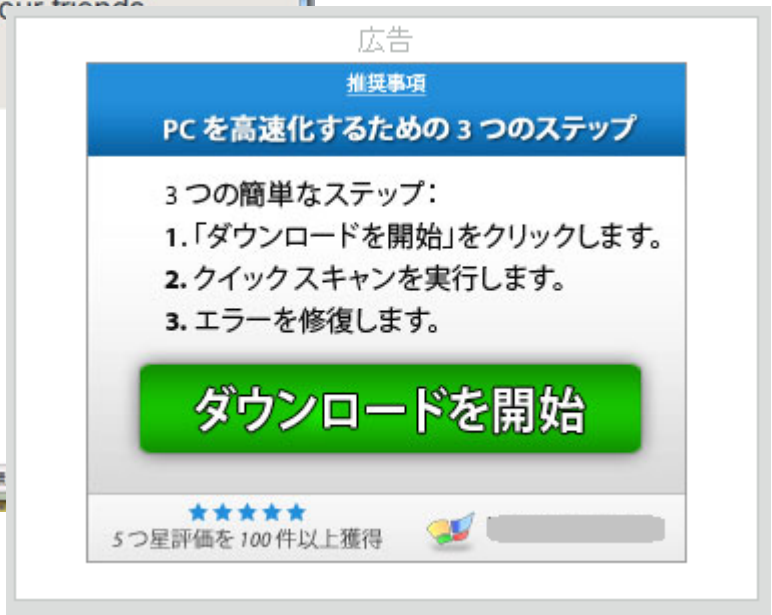
グレーウェア・アドウェア

- いつの間にかいる



Flashを
インストールした
つもり

Web広告
として出ている



グレーウェア・アドウェア

- 日本の検出数TOP10を独走するアドウェア(当社SPN調べ)
- ためしにTOP3は何かというと… (2014年第3Q集計／当社SPN調べ)

順位	検出名	数
1	ADW_INSTALLCORE	314,000
2	ADW_OPENCANDY	74,000
3	ADW_SENSAVE	49,000

- ちなみにアドウェアを除いたTOP3は… (2014年第3Q集計／当社SPN調べ)

順位	検出名	数
1	JS_AGENT.APS	17,000
2	JS_NEVAR.A	16,000
3	WORM_DOWNAD.AD	2,000

オンライン銀行詐欺ツール

- バンキングマルウェア/トロジャンとも呼ばれる
- Webインジェクションと呼ばれる手法で猛威を振るう
- 2013年6月に日本へ本格上陸
- 2014年、ついに自動送金機能が観測された
- 例) ある検体の標的
  - 国内の銀行　17行
  - クレジットカード会社　20社
  - インターネット通信販売会社　2社

オンライン銀行詐欺ツール

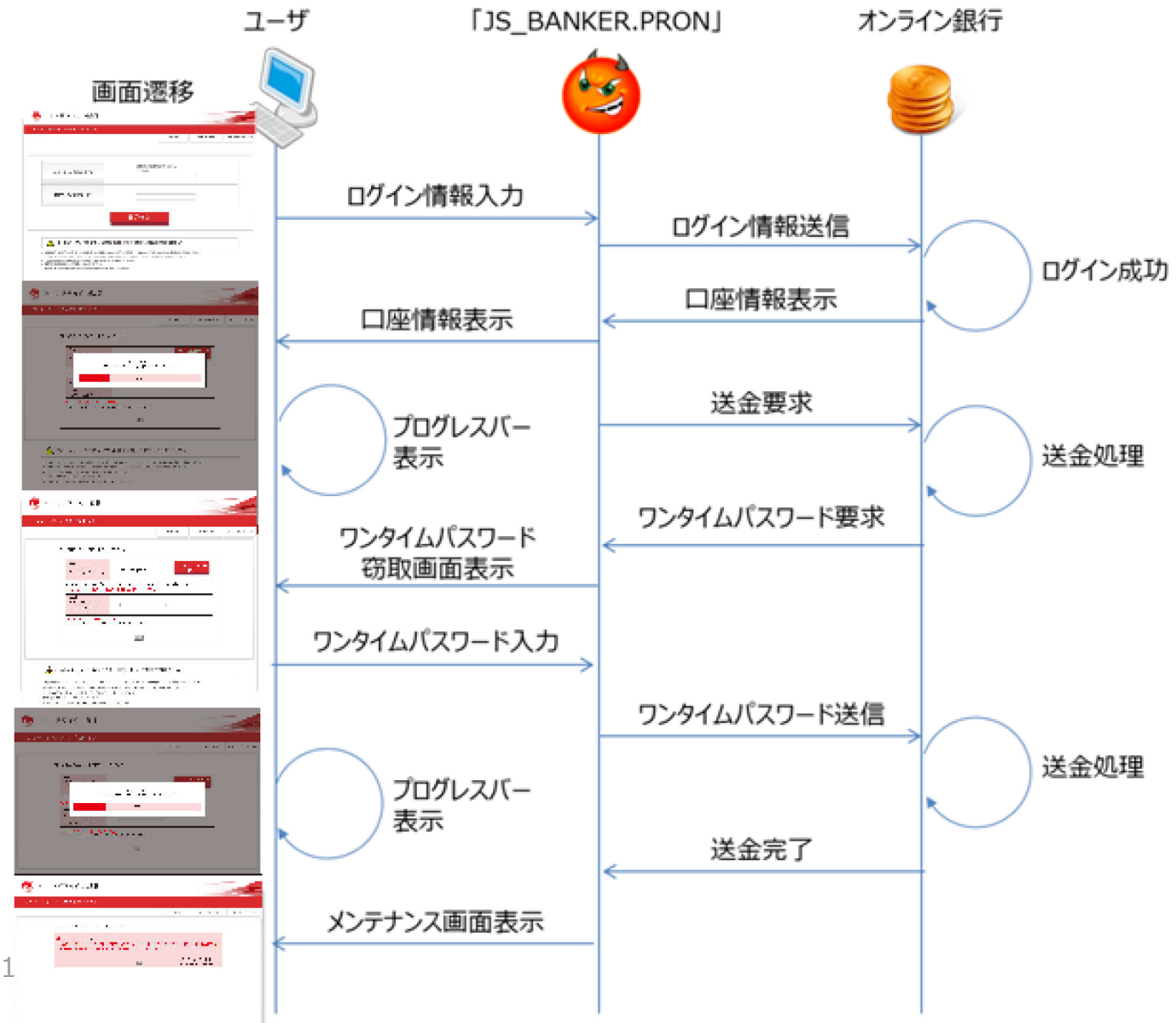
- 新しく観測されているものの特徴 (VAWTRAKファミリ)
  - 感染してしまうと、かつての護身術が通用しない
    - お気に入りからアクセスしているから大丈夫
      - 正しいURLにアクセスしている
    - アドレスバーが緑色だから大丈夫
      - EV SSLサーバ証明書もちゃんとみどり（検体の種類によるが）
    - SSLクライアント証明書を使っているから大丈夫
    - ワンタイムパスワードトークンを使っているから大丈夫

→すべて通用しません…

オンライン銀行詐欺ツール

- ユーザー体験はこんなふう (VAWTRAKファミリ)：
  ブックマークからオンライン銀行にログインしたら、なんかステータスバーが表示されて、しばらくしたらメンテナンス画面が表示された。後日確認したら、残高がほぼ0に！

オンライン銀行詐欺ツール



おまけ：DOWNADの話

- 未だ検出上位のDOWNAD

順位	検出名	数
1	JS_AGENT.APS	17,000
2	JS_NEVAR.A	16,000
3	WORM_DOWNAD.AD	2,000

アドウェアを除いた国内検出TOP3(2014年第3Q集計／当社SPN調べ)

- 近年珍しい、大規模拡散型のウイルス
- これが出たらとにかく面倒くさい
- パッチが不十分なWindowsXPに主に感染します
- 出入りの業者のUSBメモリが怪しい！

まとめ

- うわ～！ウイルスに感染してしまった！
  - 特に慌てる必要ないです(DOWNAD以外は)
  - パッと見て変な動きをしているようなら対応は簡単
    - ワンクリック詐欺は無視して削除すればいいだけ
    - アドウェア・グレーウェアも、削除すればいいだけ
      - ウイルス対策ソフトが駆除したらそれでOK
  - 写真を暗号化されてしまった
    - 来る日に備えて、今日この後すぐバックアップを取ろう！
      - 「バックアップ大事」と君が言ったから、11/19はバックアップ記念日

まとめ

- 本当に怖いウイルスは派手な動きをしません
  - 「バックドア」
    - 企業の業務パソコンなどに感染し、情報窃取を狙う
    - 画面上、動作上変化がないので感染に気付かない
    - ひっそり入ってきて、ひっそりとずっといる
    - これはまた、別の話…。

身の守り方

- 王道しかないんです
  面白くなさ過ぎて今さら改めて言いづらい
  - パッチを当てる
    - OS・ブラウザ・Java・Adobe Reader・Flash　などなど
  - ウイルス対策ソフトのパターンを最新にする
  - 実行ファイルを実行するときは出所に注意する
  - OKボタンを連打しない
  - メールの添付ファイルやリンクは開かない
  - 怪しいサイトに行かない