JPCERT CC®

あなたも狙われている!?

インターネットバンキングの不正送金とマルウエアの脅威

2013年12月9日

JPCERT/CC 竹田春樹

SecurityDay 2013

Agenda

1 状況の把握
不正送金の事例について

2 脅威の確認
不正送金に関わるマルウエア

3 状況の打開
対策・対応について

- JPCERT/CCをご存知ですか? -

JPCERT/CCとは

一般社団法人　JPCERTコーディネーションセンター

Japan Computer Emergency Response Team Coordination Center
ジェーピーサート・コーディネーションセンター

- 日本国内のインターネット利用者やセキュリティ管理担当者、ソフトウエア製品開発者等（主に、情報セキュリティ担当者）がサービス対象
- コンピュータセキュリティインシデントへの対応、国内外にセンサをおいたインターネット定点観測、ソフトウエアや情報システム・制御システム機器等の脆弱性への対応などを通じ、セキュリティ向上を推進
- インシデント対応をはじめとする、国際連携が必要なオペレーションや情報連携に関する、我が国の窓口となるCSIRT（窓口CSIRT）

CSIRT: Computer Security Incident Response Team

※各国に同様の窓口となるCSIRTが存在する(米国のUS-CERT、CERT/CC、中国のCNCERT, 韓国のKrCERT/CC、等)

- 経済産業省からの委託事業として、情報セキュリティ対策推進事業（不正アクセス行為等対策業務）を実施

- JPCERT/CCをご存知ですか? -

JPCERT/CCの活動

インシデント予防 | インシデントの予測と捕捉 | 発生したインシデントへの対応

脆弱性情報ハンドリング

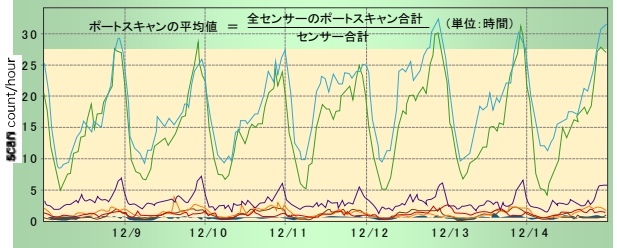
- 未公開の脆弱性関連情報を製品開発者へ提供し、対応依頼
- 関係機関と連携し、国際的に情報公開日を調整
- セキュアなコーディング手法の普及
- 制御システムに関する脆弱性関連情報の適切な流通

JVN Japan Vulnerability Notes

情報収集・分析・発信

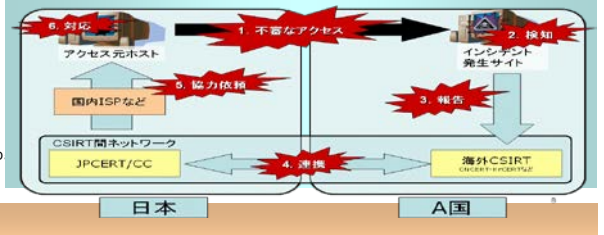
定点観測（ISDAS/TSUBAME）

- ネットワークトラフィック情報の収集分析
- セキュリティ上の脅威情報の収集、分析、必要とする組織への提供



インシデントハンドリング（インシデント対応調整支援）

- マルウエアの接続先等の攻撃関連サイト等の閉鎖等による被害最小化
- 攻撃手法の分析支援による被害可能性の確認、拡散抑止
- 再発防止に向けた関係各関の情報交換及び情報共有



早期警戒情報

重要インフラ、重要情報インフラ事業者等の特定組織向け情報発信

CSIRT構築支援

海外のNational-CSIRTや企業内のセキュリティ対応組織の構築・運用支援

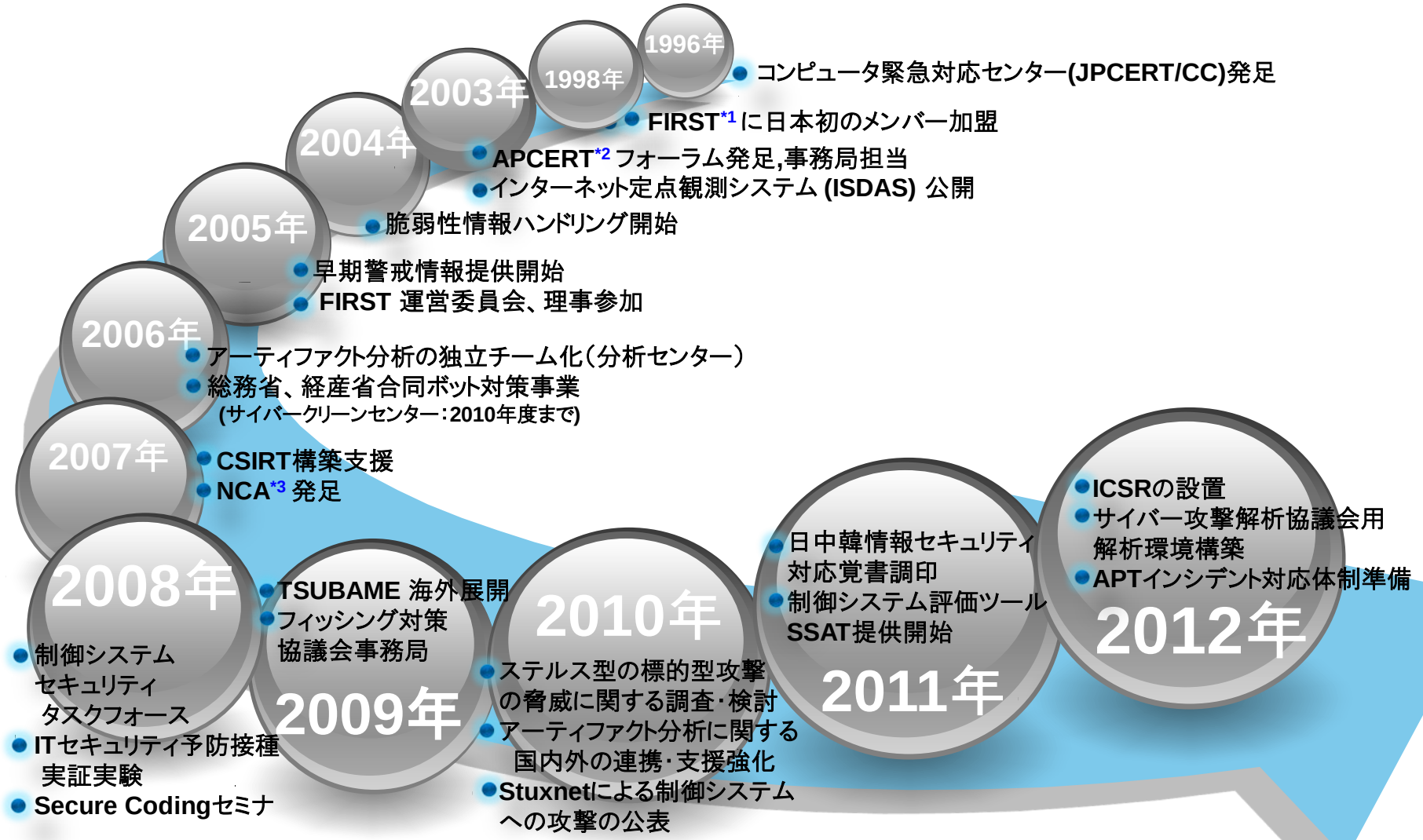
アーティファクト分析

マルウエア（不正プログラム）等の攻撃手法の分析、解析

国際連携

各種業務を円滑に行うための海外関係機関との連携

JPCERT/CC事業の沿革



FIRST : Forum of Incident Response and Security Teams) **APCERT** : Asia Pacific Computer Emergency Response Team **NCA** : 日本シーサート協議会

不正送金の事例について

-不正送金の事例について-

国内における動向

ネットバンキングの不正送金事件、「偽ポップアップ」による巧妙な手口

2012年11月19日

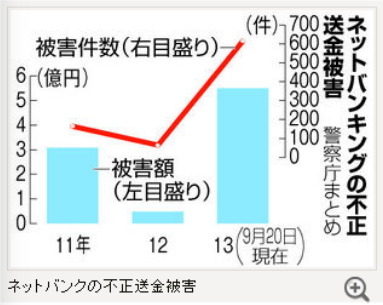
近ごろ、インターネットを舞台にした「サイバー事件」が頻発している。手口がきわめて巧妙化しており、ふとしたきっかけで犯罪に巻き込まれてしまい、被害を受けていることに気づかないまま過ごしてしまうケースも多い。実際に現金の被害が出ている「ネットバンキング不正送金事件」について、インターネットのセキュリティ事情に詳しいITジャーナリストの三上 洋氏が、図を用いながら手口と対策を分かりやすく紹介する。

正規のWebサイトへのアクセスを検知し、偽ポップアップを出す巧妙な手口

ゆうちょ銀行、三井住友銀行、みずほ銀行、三菱東京UFJ銀行などのネットバンキングで、預金を第三者へ不正に送金されてしまう事件が2012年10月から相次いで発覚している。相談が300件以上寄せられているほか、三井住友銀行で計約200万円、楽天銀行でも計数十万円の被害が出た。

参考資料: 1

ネットバンキング不正送金、被害総額5．5億円



ネットバンクの不正送金被害

【吉田伸八】インターネットバンキングの口座から預金が不正に送金される被害が止まらない。警察庁のまとめでは、今年の被害は20日までに615件、被害額は計約5億5千万円にのぼっている。送金手続きの際に1回限りで使う「ワンタイムパスワード」を盗み取る手口の広がりなどが原因とみられ、警察庁は利用者に対策を呼びかけている。

警察庁によると、被害が確認され始めた2011年は165件、約3億800万円で、12年に64件、約4800万円に減ったものの、今年急増している。月別の被害件数を見ると、5月までは1桁か2桁だったが、6月以降は100件台で推移している。

被害が出ているのは、ゆうちょ、みずほ、楽天、三菱東京UFJ、三井住友、りそな、シティバンク、住信SBIネット、セブン、ジャパンネット、北洋、十六、南都、大垣共立、八十二、埼玉りそなの16行と、行名を公表していない2行。

参考資料: 2

ネットバンキング被害額、過去最悪を更新

〈2013年10月18日 19:18〉

いいね！ 0 Tweet B! 0

このニュースをメールで伝える

このニュースをブログに書く

<a href="http://www.news コピー

インターネットバンキングの不正送金による被害総額が、今年に入ってこれまでに約7億6000万円に上り、過去最悪だった2011年の年間被害額の2倍以上になったことがわかった。

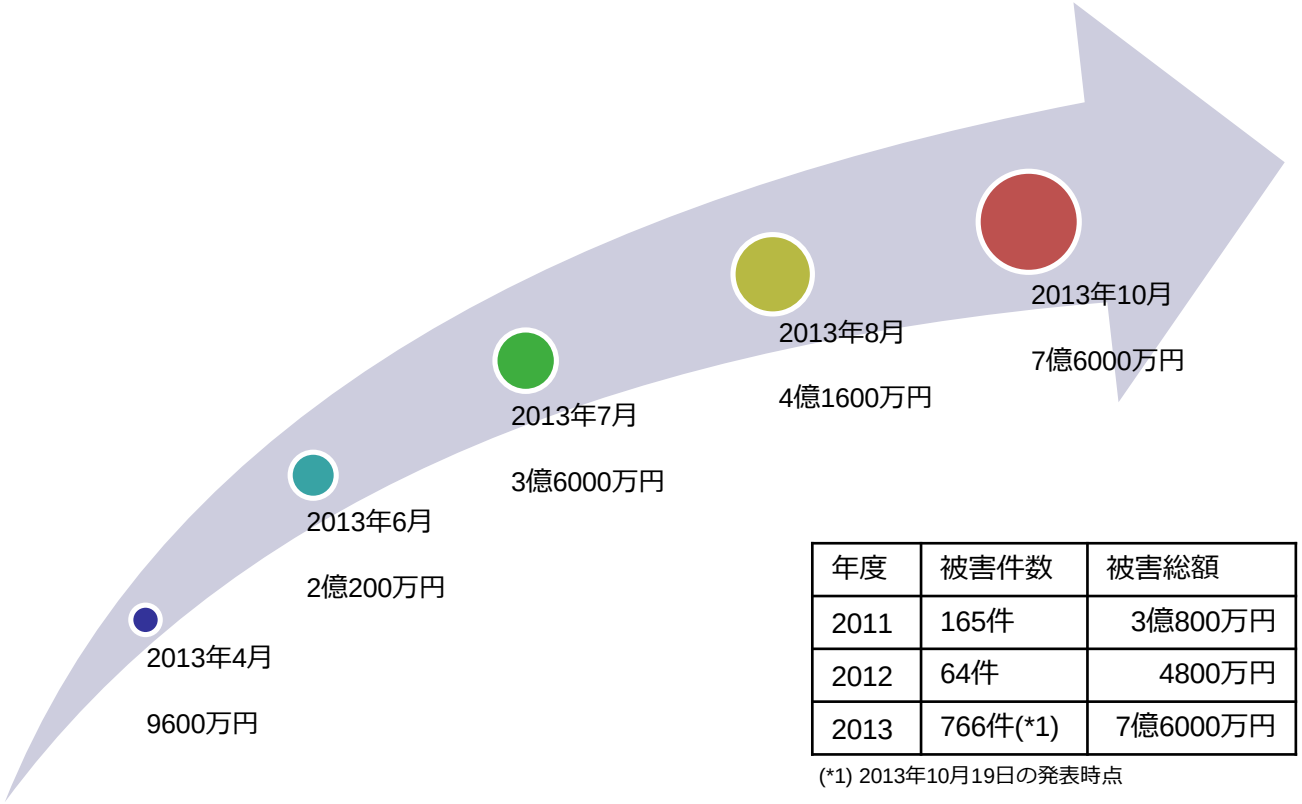
警察庁のまとめによると、インターネットバンキングのパスワードやIDを盗み出す手口の不正送金事件は、今年に入って急増しており、今月15日までに大手銀行や地方銀行など19の金融機関で766件の被害が確認されている。

被害総額は約7億6000万円で、これは過去最悪だった2011年の年間の被害総額3億800万円の2倍以上になる。

また、確認された被害のうち、約1割程度は、最終的に海外の口座に送られていることが確認されているという。

参考資料: 3

不正送金の被害金額(2013年)



年度	被害件数	被害総額
2011	165件	3億800万円
2012	64件	4800万円
2013	766件(*1)	7億6000万円

(*1) 2013年10月19日の発表時点

警察庁が発表している不正送金の被害額は、2012年の被害総額を2013年4月の時点で超えています。

不正送金に関わるマルウエア

- 不正送金に関わるマルウエア –

マルウエアに関する動向

時期	マルウエアに関わる動向
2007年	• ZeuSのオリジナルの存在が確認される（7月）
2009年	• 広範囲の被害を確認（3月） • 74,000を超えるFTPアカウントがPrevxによって確認される（6月） • ZeuSと類似の機能を持ったSpyEyeの存在が確認される
2010年	• アメリカの15行の銀行が攻撃対象となっていることをTrusteerが確認（7月） • FBIによると、$70 millionが盗まれたとされている • McAfeeによると、ZeuSの作者がZeuSのソースコードを対抗するSpyEyeの作者に販売したとされている
2011年	• ZeuSのソースコードがリークされる（3月） • ZeuSの亜種とされるIce IXが確認される（4月） • ZeuSの亜種とされるCitadelが確認される
2013年	• KINS（PowerZeuS）など新たなマルウエアが確認される

参考情報4、 5 、6、7、8から抜粋

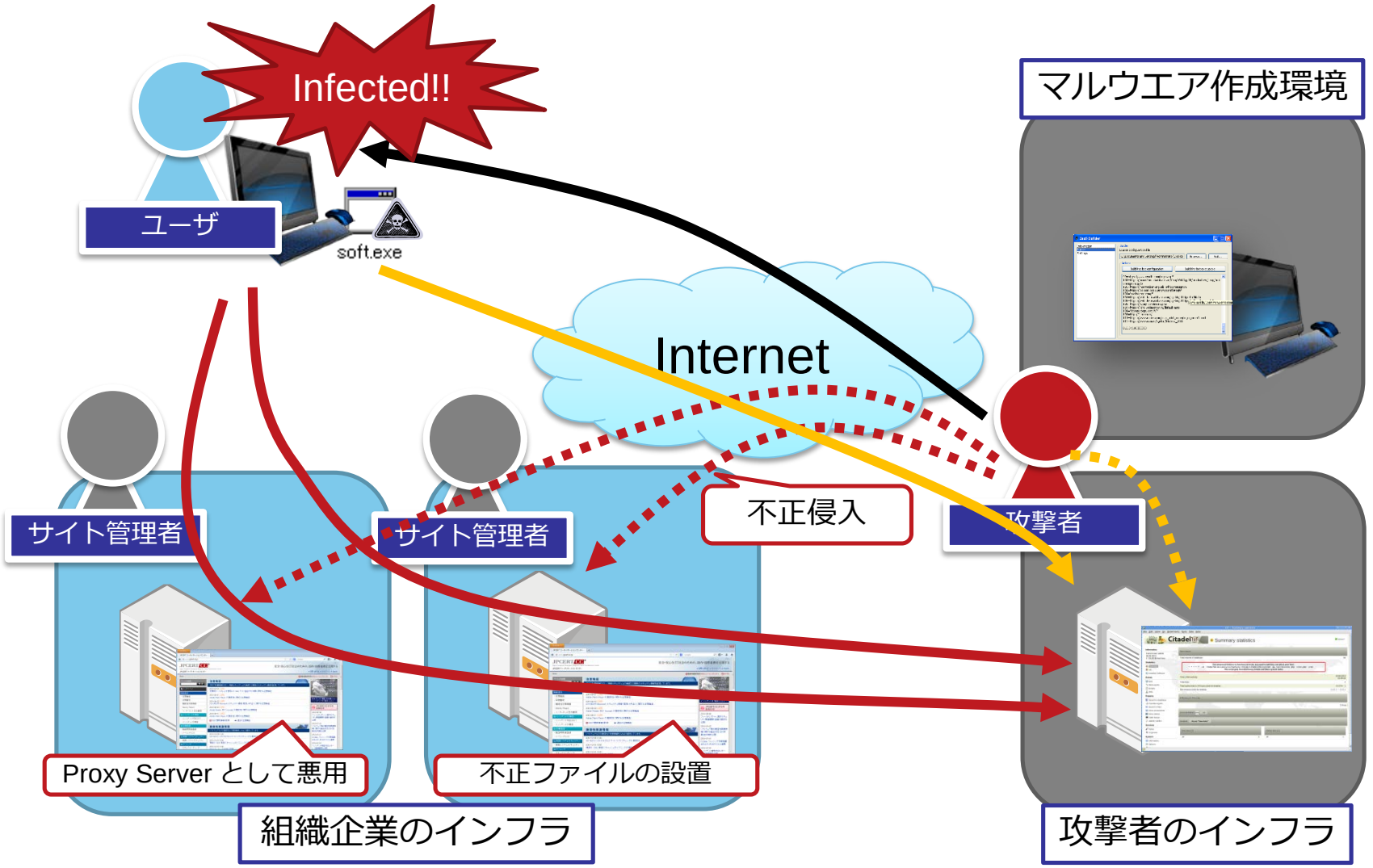
マルウエアの特徴

不正送金に関わるマルウエアの特徴的な機能として、以下の機能があることを確認しています。

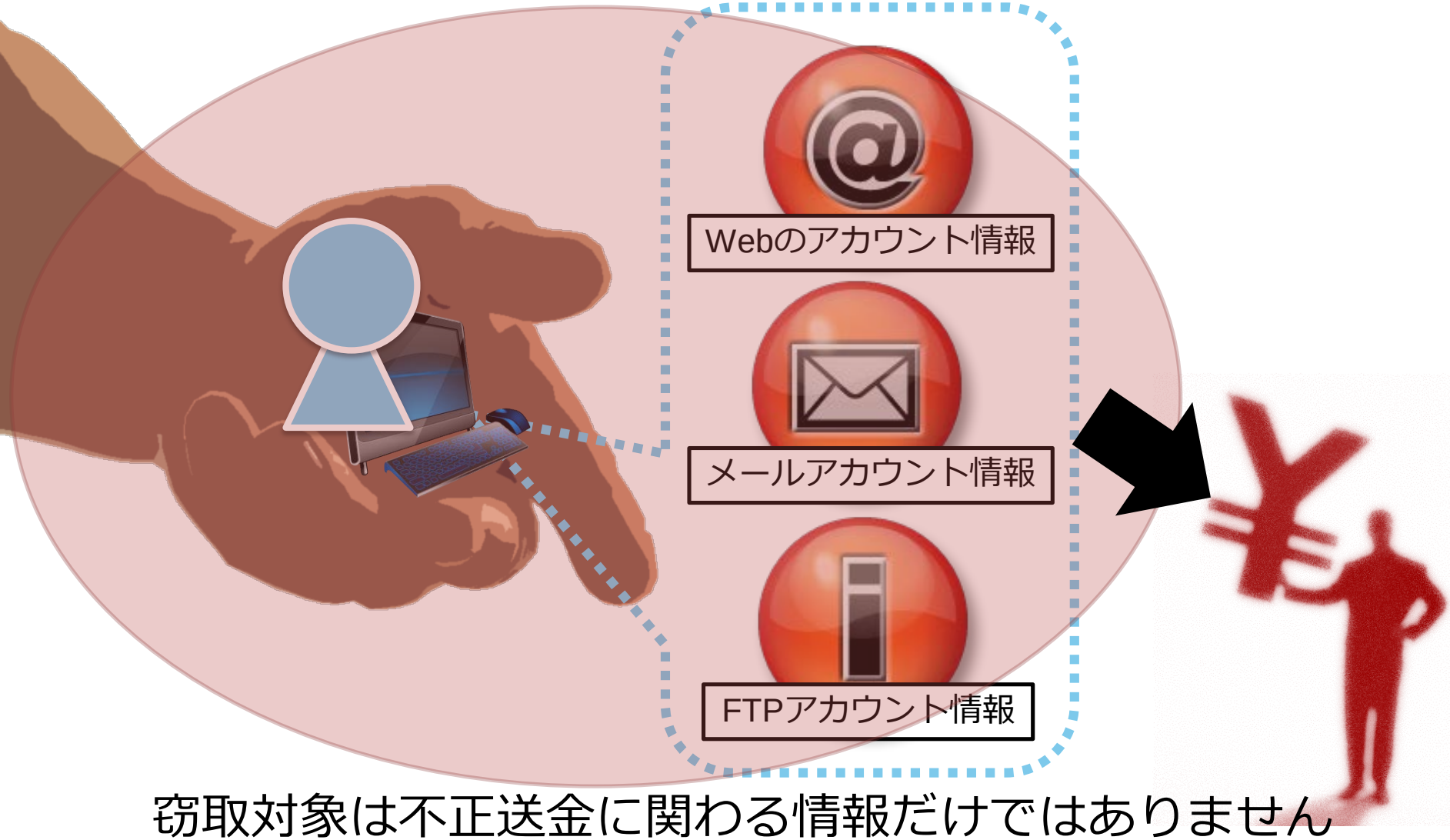
- 情報窃取機能
  Webの認証情報やFTPなどのアカウント情報を収集する機能
- Webインジェクション機能
  Webコンテンツを攻撃者が意図する内容に書き換える機能

これらの機能を悪用し、インターネットバンキングに関連する情報も含む、感染端末の様々な情報の窃取を試みます。

攻撃者のネットワーク



マルウエアによって窃取される情報



窃取対象は不正送金に関わる情報だけではありません

対策・対応について

対策・対応について

- **技術面での対策**

  基本的なセキュリティ対策を徹底する

  - OSやソフトウエアの最新状態にする
    不要なソフトウエアは削除するなど
  - ウイルス対策ソフトウエアの導入する

- **運用面での対策**

  不正送金に早期に気付くための対応をユーザ自身で行う

  [例]
  - 預金確認方法を二つ用意する
  - 定期的に預金金額を確認する

対策・対応について（JPCERT/CCの取り組み）

他の事案と同様、インターネットバンキングに関わるマルウエアの通信先等に関しても、コーディネーションの対応を進めています。

また、日本国内のWebサーバにCitadelに関連する不正ファイルが設置された事案についてもコーディネーションの対応を行った実績もあります。

【金融系マルウエアが通信を行う国内サーバに関する対応】

2013 年 7 月はじめ、Citadel とよばれる金融系マルウエアの通信先となっている日本国内のサーバに関する報告が寄せられました。マルウエアは、侵入されたと見られる Web サーバ上の php スクリプトに対してリクエストを送信していました。Web サーバの管理者に連絡したところ、攻撃者によりサーバ上に設置されていた複数のファイルをご提供いただくことができました。設置されていたファイルには、マルウエアに感染したホストからのリクエストを受け取る php スクリプトのファイル、暗号化されているリクエストを復号する鍵などの情報を含む設定ファイル、リクエストに対して返されるバイナリのデータなどがありました。php スクリプトは、リクエストのサイズなどをチェックして、マルウエアからの通信である場合には暗号化されているリクエストを復号した後にデータを返し、マルウエアからの通信でなかった場合には 404 Not found と表示する仕組みになっていました。

参考資料: 11

対策・対応について

基本的なセキュリティ対策

サービス使用者による対策

サービス事業者による対策

まとめ

2013年に入り、**不正送金の被害が急増**しています。

様々な取り組みにより、対策・対応を進められていますが、攻撃者の攻撃手法も変化しており、根本的な対策・対応が難しい状況が続いています。

サービスを提供する側だけではなく、サービスを使用するユーザ側による対応・対策が必要となってきています。

普段の生活で気をつけていることを、インターネットの世界でも実践し、自身の**情報・資産**を守っていきましょう。

参考資料

1. ネットバンキングの不正送金事件、「偽ポップアップ」による巧妙な手口
   http://trendy.nikkeibp.co.jp/article/pickup/20121116/1045603/
2. ネットバンキング不正送金が激増――ウイルス感染に注意
   http://www.so-net.ne.jp/security/news/newstopics_201308.html
3. ネットバンキング被害額、過去最悪を更新
   http://www.news24.jp/articles/2013/10/18/07238588.html
4. Zeus (Trojan horse)
   http://en.wikipedia.org/wiki/Zeus_(Trojan_horse)
5. Citadel Makes a Comeback, Targets Japan Users
   http://blog.trendmicro.com/trendlabs-security-intelligence/citadel-makes-a-comeback-targets-japan-users/
6. Public-private partnerships essential to fighting cybercriminals
   http://blogs.technet.com/b/microsoft_on_the_issues/archive/2013/07/25/public-private-partnerships-essential-to-fighting-cybercriminals.aspx?Redirected=true
7. Current state of online banking Trojans
   http://www.itu.int/ITU-D/eur/rf/cybersecurity/presentations/ITU_IMPACT_banking_trojans%20by%20Symantec.pdf
8. New Trojan Ice IX Written Over Zeus' Runs
   https://blogs.rsa.com/new-trojan-ice-ix-written-over-zeus-ruins/
9. 「SpyEye」によるサイバー犯罪の手口とは
   http://about-threats.trendmicro.com/relatedthreats.aspx?language=jp&name=Trend%20Micro%20Researchers%20Uncover%20SpyEye%20Operation
10. Microsoft, financial services and others join forces to combat massive cybercrime ring
    http://www.microsoft.com/en-us/news/press/2013/jun13/06-05dcupr.aspx
11. インシデント報告対応レポート [2013年7月1日～2013年9月30日]（2013年10月10日公開）
    http://www.jpcert.or.jp/pr/2013/IR_Report20131010.pdf

お問い合わせ、インシデント対応のご依頼は

JPCERTコーディネーションセンター

- Email：office@jpcert.or.jp
- Tel：03-3518-4600
- Web: https://www.jpcert.or.jp/

インシデント報告

- Email：info@jpcert.or.jp
- Web: https://www.jpcert.or.jp/form/

ご清聴ありがとうございました。