国内外で発生している
マルウェアの進化とその脅威

標的型攻撃はメールだけではない！！

知らないうちにあなたが標的とならないために

キヤノンITソリューションズ株式会社
セキュリティソリューション事業部
石川　堤一
2014年9月10日

キヤノンITソリューションズ　企業概要

名　　称	キヤノンITソリューションズ株式会社 Canon IT Solutions Inc.
設　　立	1982年7月1日
資　本　金	3,617百万円
事　　業	情報システムのコンサルティング・設計・構築 運用管理・保守サービスの提供、ソフトウエアの開発・販売
売　上　高	81,366百万円 （2013年12月期 連結）
株 主 構 成	キヤノンMJアイティグループホールディングス株式会社 （100%）
従　業　員	3,646人（2013年12月末日現在 連結）
関 係 会 社	佳能信息系統(上海)有限公司、 スーパーストリーム株式会社、 クオリサイトテクノロジーズ株式会社、 ガーデンネットワーク株式会社、 キヤノンITSメディカル株式会社、 キヤノンビズアテンダ株式会社、エーアンドエー株式会社、Canon IT Solutions(Thailand) Co.,Ltd. 、Material Automation (Thailand) Co., Ltd.、ASAHI-M.A.T. Co., Ltd.、MAT Vietnam Company Limited、Canon Software America, Inc.、Canon IT Solutions (Philippines), Inc.

セキュリティソリューション事業

ネットワークセキュリティ

情報漏えい対策

■電子メールフィルタリング・アーカイブ

GUARDIANWALL（ガーディアンウォール）

12年連続国内シェアNo1＊

■Webフィルタリング

WEBGUARDIAN（ウェブガーディアン）

（※） 株式会社富士キメラ総研2013ネットワークセキュリティビジネス調査総覧より

メールセキュリティ・ウイルス対策

ESET MAIL SECURITY（イーセット メール セキュリティ）

UTM（総合脅威管理）

DELL SonicWALL

FortiGate（フォーティゲート）

SECUI MF2 Virtual Edition（セキュアイ エムエフツー バーチャル エディション）

統合セキュアメールアプライアンス

FortiMail（フォーティメール）

不正侵入検知・防衛

Sniper IPS

不正PC検知・遮断

IPScan XE

エンドポイントセキュリティ

ウイルス対策

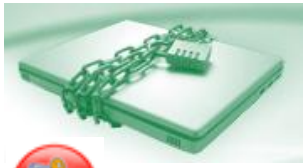
ESET ENDPOINT PROTECTION ADVANCED（イーセット エンドポイント プロテクション アドバンスド）

ESET ENDPOINT PROTECTION STANDARD（イーセット エンドポイント プロテクション スタンダード）

ESET FILE SECURITY（イーセット ファイル セキュリティ）

HDD暗号化

CompuSec（コンピュセック）



IT資産管理

■ソフトウェア ライセンス管理

QND Advance（キューエヌディー アドバンス）

■クライアント PC運用管理

SKYSEA Client View（スカイシー クライアント ビュー）

キヤノン製複合機/プリンターのシステム連携イメージ

ESET ユーザー選出の各種アワード受賞

キヤノンITソリューションズ及び、ESETセキュリティ ソフトウェア シリーズは、さまざまな顧客満足度調査やアワードにおいてユーザーより高い評価および支持を受けております。

日経コンピュータ調べ
顧客満足度調査 2014-2015
「セキュリティ製品（クライアント管理系）」
「セキュリティ製品（サーバー/ネットワーク管理系）」部門

顧客満足度 1位

顧客満足度調査 2014-2015 日経コンピュータ
セキュリティ製品（クライアント管理系）部門

顧客満足度調査 2014-2015 日経コンピュータ
セキュリティ製品（サーバー/ネットワーク管理系）部門

（2014年8月21日号）

キヤノンITソリューションズは、顧客満足度調査2014-2015のセキュリティ製品（クライアント管理系）とセキュリティ製品（サーバー/ネットワーク管理系）の2部門において、顧客満足度1位を獲得しました。
セキュリティ分野では、2年連続の1位獲得となります。

出典元：
http://itpro.nikkeibp.co.jp/atcl/news/14/072200157/

日経コンピュータ調べ
パートナー満足度調査2014
「セキュリティ製品（クライアント管理系）部門」

パートナー満足度 1位

パートナー満足度調査 2014 日経コンピュータ
セキュリティ製品（クライアント管理系）

（2014年2月6日号）

キヤノンITソリューションズは、パートナー満足度調査2014のセキュリティ製品（クライアント管理系）」部門で1位を獲得しました。中でも、パートナーの重視度が高い3項目のうち、「製品」「価格競争力」で高評価を獲得しました。

出典元：
http://itpro.nikkeibp.co.jp/article/COLUMN/20140217/537205/

イード
中小企業セキュリティアワード2014
クライアントPCウイルス対策の部
総合満足度部門

最優秀受賞

イード・アワード セキュリティアワード 顧客満足度 最優秀賞 2014

（2014年2月）

キヤノンITソリューションズは、従業員300名未満の企業および、組織を対象としたイード・中小企業セキュリティアワード2014のクライアントPCウイルス対策の部総合満足度部門において最優秀を受賞しました。

出典元：
http://www.iid.co.jp/

今日のお話

昨年から今年にかけて
確認された新しい脅威

法人口座を狙う脅威

昨年から今年にかけて確認された新しい脅威

マルウェアの歴史

- コンピュータウイルスは、元々コンピュータに被害を与える。

- コンピュータはいつしかマルウェア（主にトロイ、ボット感染）の踏み台に代わり、狙いは「コンピュータ」から「人（企業）」「金」へと変化。

- そして、標的型攻撃へと変化し、ばらまき型だけではなくなり、手口や難読化も高度化。簡単に見つけ出すことが困難な状況へ。

さらに注目すべき国内事件

- 某教育関係会社員の内部不正による情報漏えい

USBメモリによる持ち出し

- 派遣SEによるパソコン遠隔操作ウイルス事件

会社支給PCに感染

多様化するデバイスとどう対応していくか

エンドポイント領域のセキュリティ対策

プライベートクラウド
オンラインストレージ
サーバー同様の対策

利便性が高まる一方
管理端末の種類も増えている

スマートフォン
リモート管理
パスワード・暗号化付与
持ち出し管理など

タブレット
ウイルス対策
パスワード・暗号化付与
持ち出し管理など

ルーター
認証
接続制限など

仮想端末
PC同様の対策

2014年上半期
多く相談受けた攻撃やマルウェア

サーバー
•Web改ざん
•水飲み場型攻撃

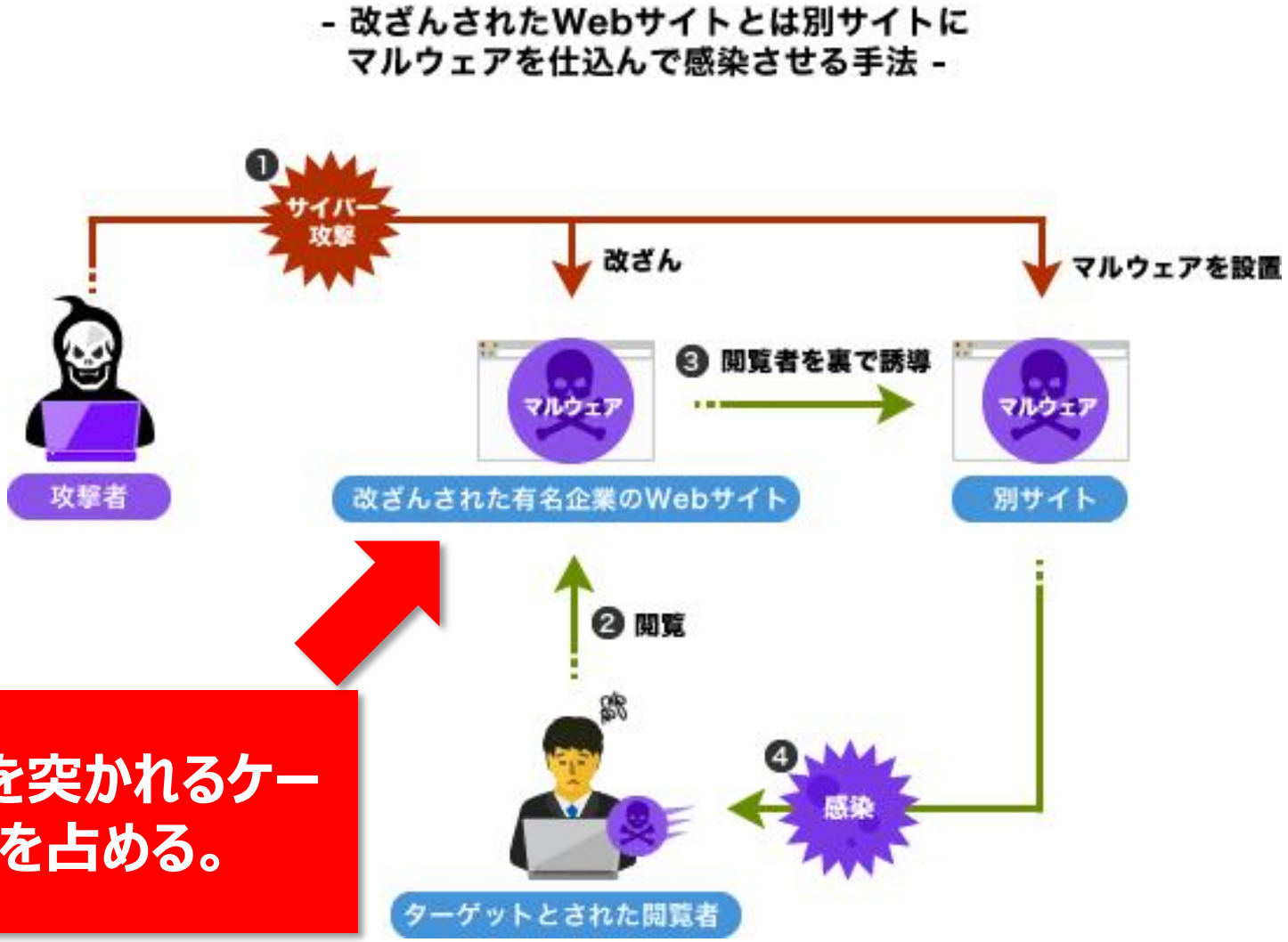
クラウド
・サーバー系の攻撃
・パスワードリスト攻撃

共通して標的型攻撃複合もあり

PC・スマードデバイス
•バンキングトロージャン
•偽セキュリティソフト
•ランサムウェア

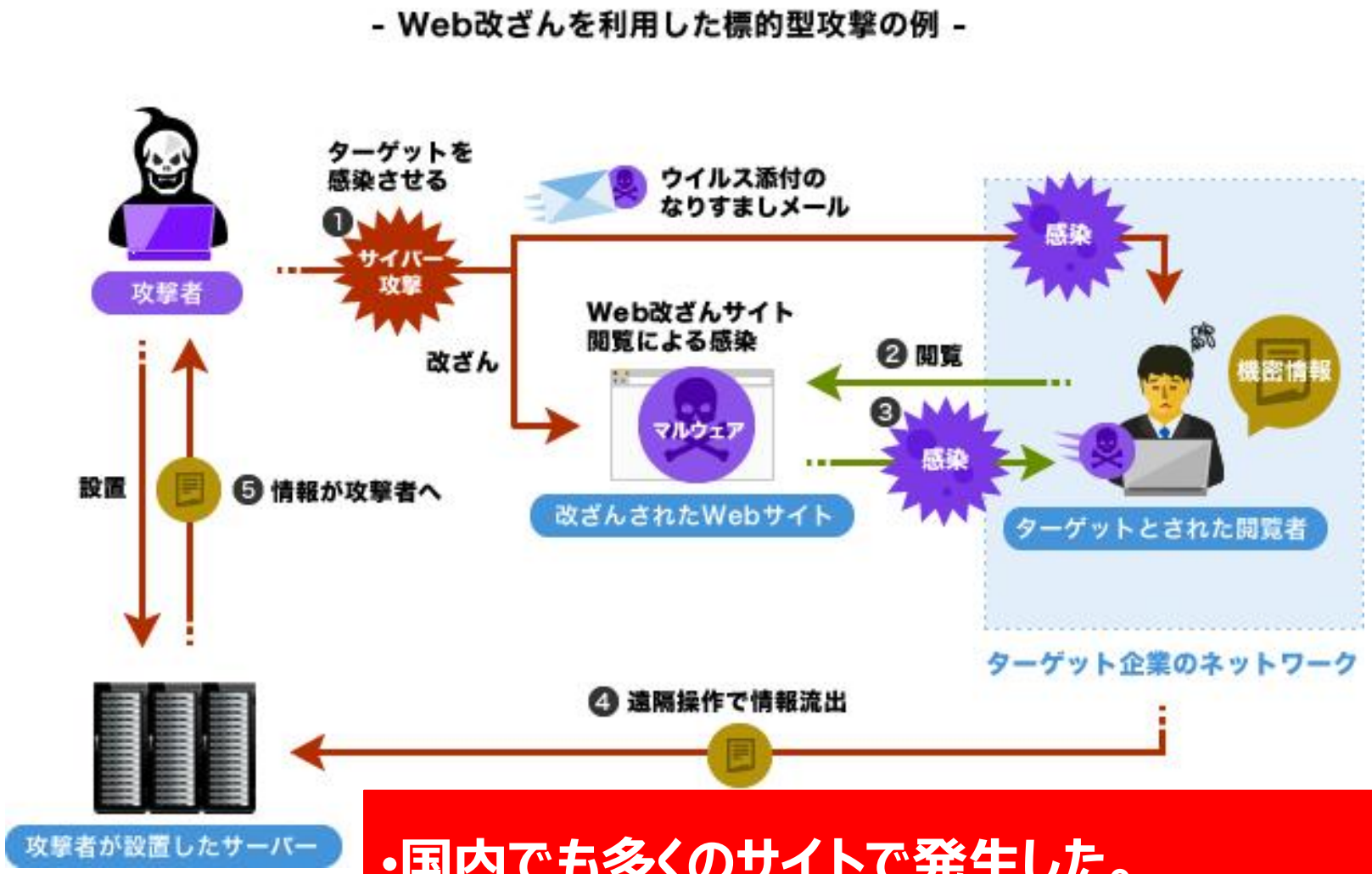
ルーター
•DNS書換攻撃

Web改ざんを利用したマルウェア感染手法



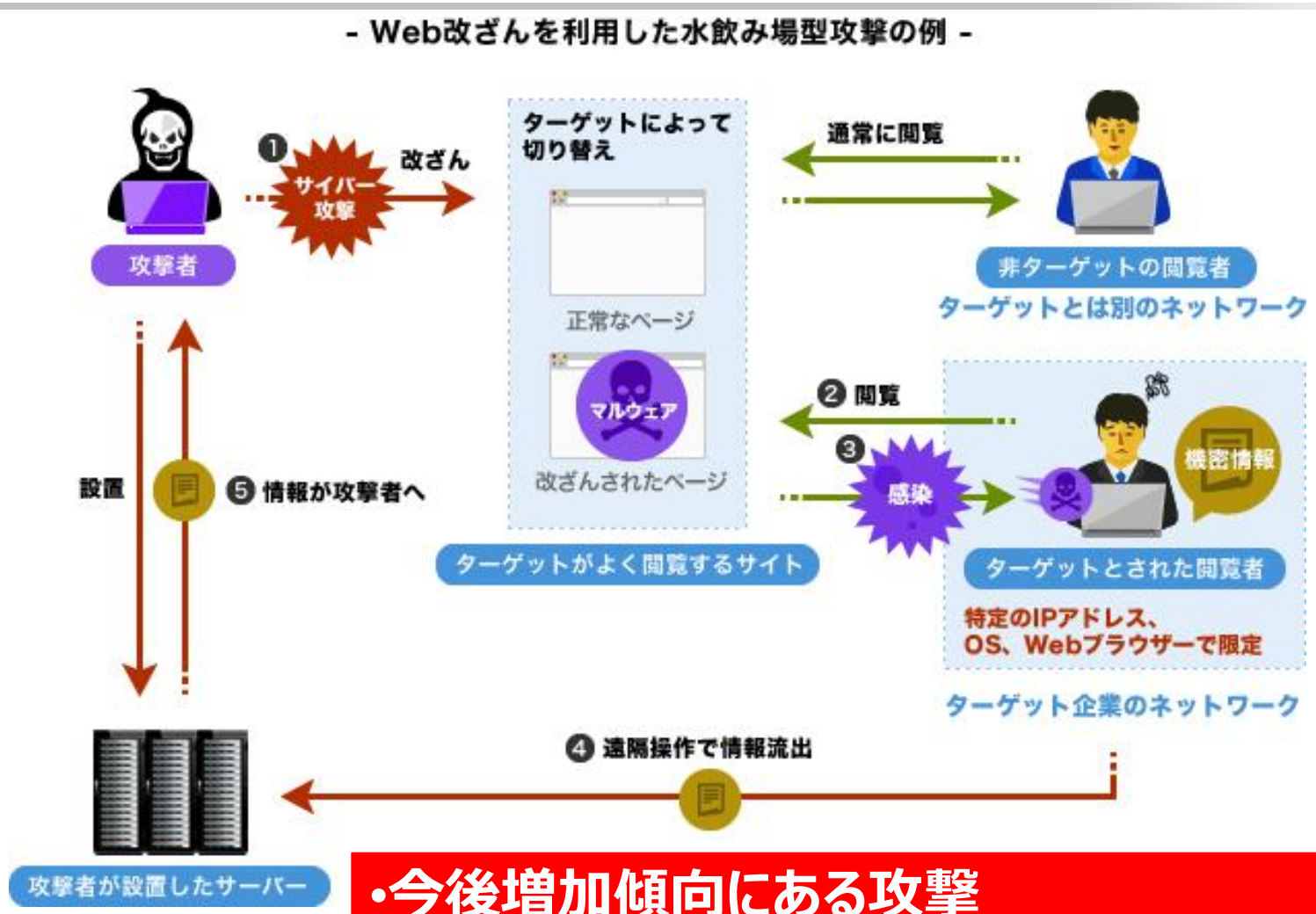
脆弱性を突かれるケースが多くを占める。

Web改ざんを利用した標的型攻撃



•国内でも多くのサイトで発生した。

Web改ざんを利用した水飲み場型攻撃



- 今後増加傾向にある攻撃
- 官公庁や企業のPCを標的にマルウェア感染

法人口座を狙う脅威

インターネットバンキング被害

- フィッシング
- 水飲み場型攻撃
- MITB
- バンキングトロージャン
- パスワードリスト型攻撃

警察庁インターネットバンキングに係る不正送金事犯の発生状況
(9/4発表)
- H26 上期 1,254件
- H25 下期 1,098件
- H25 上期 217件

7倍増

- 法人名義口座に係る被害
- H26 上期 5億7200万
- H25 下期 7500万

フィッシングメールのケース

- 実際に届いたフィッシングメール -

[redacted]銀行ーー安全確認　受信トレイ ×　2013Q4 ×

【[redacted]銀行へようこそ】login@[redacted]-bank.co.jp　2013/12/11

To [redacted]

こんにちは！

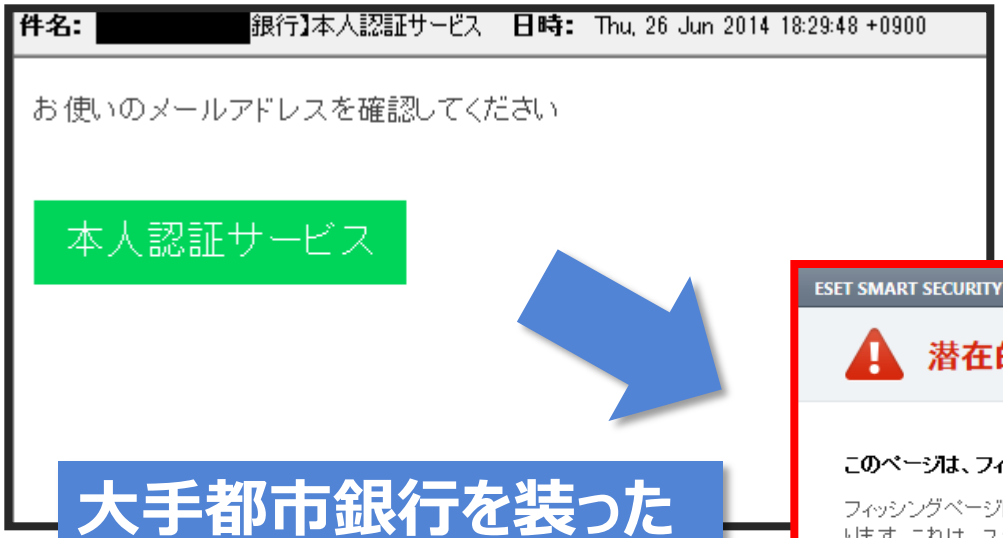
これは[redacted]銀行によって行っているユーザ番号の調査です。
あなたのユーザ番号は使用停止になっているかどうかをチェックしています。
あなたのユーザ番号は合法的であることが保障できるために、下記のリンクをクリックしてください。
https://fes.[redacted]-bank.co.jp/MS/main/RbS?CurrentPageID=START&&COMMAND=LOGIN

あなたのユーザ番号の承認が完成された後、[redacted]銀行よりあなたのユーザ番号をチェックしていただきます。

•アクセスすると偽サイトへ誘導される
•多少知識のある方であれば、URLや文章で偽判断可能

フィッシング対策によるアクセス保護

•ウイルス対策だけではなく、フィッシング対策も重要
•ブラウザ上で警告を出しアクセスをさせない対処

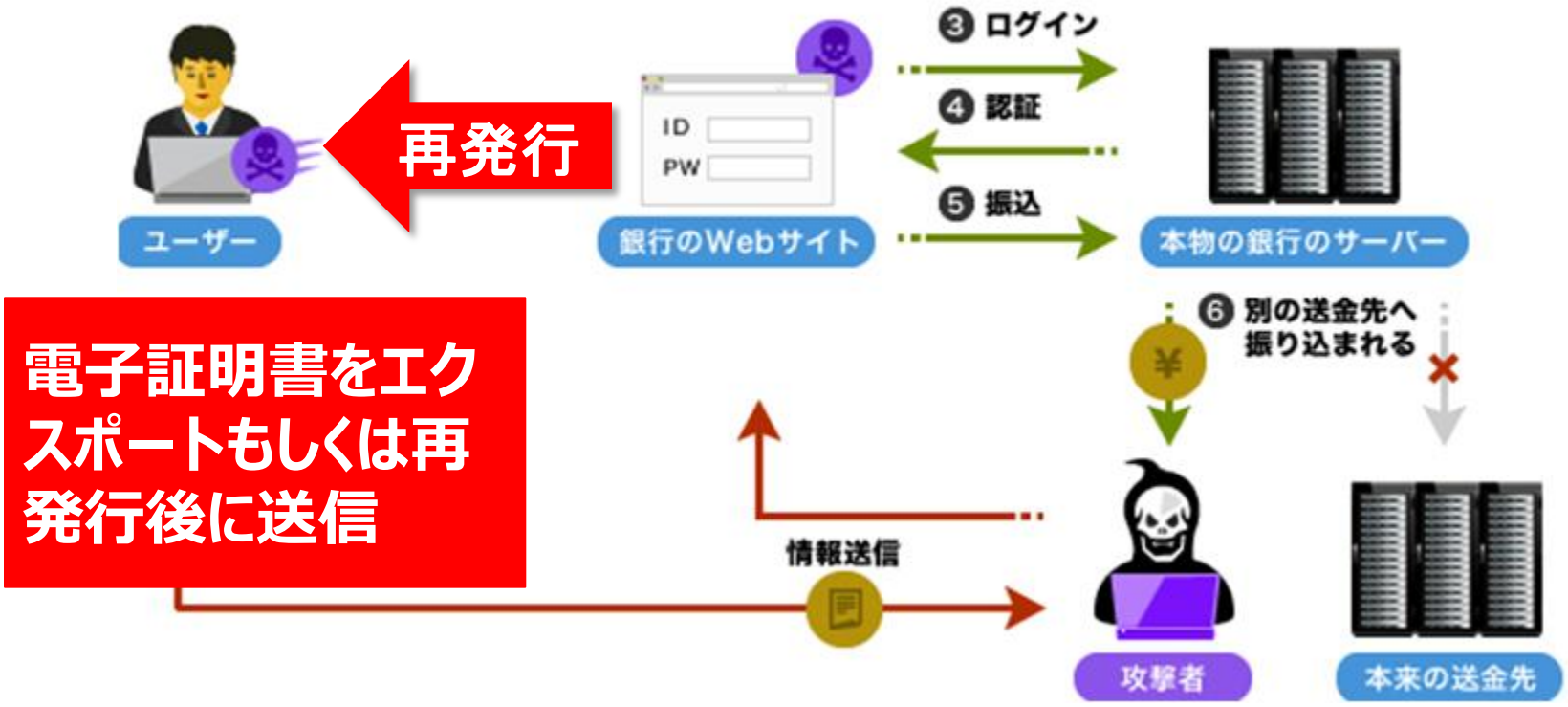


大手都市銀行を装ったフィッシングメール

ESET製品でのフィッシング対策

電子証明書を盗むウイルスと不正送金

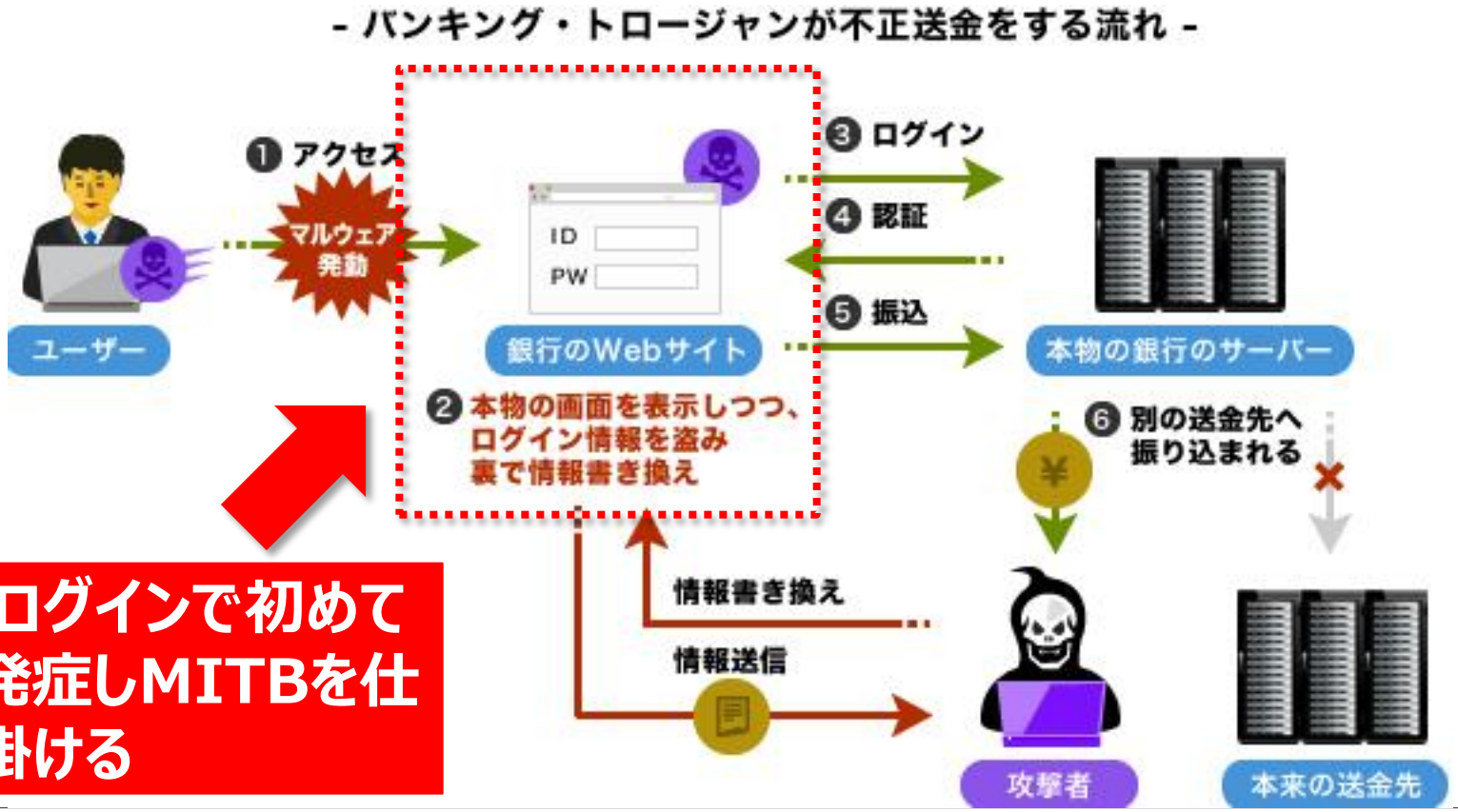
•電子証明書をエクスポートして送信
•エクスポートができない場合は、その証明を削除し再発行された証明書のコピーを送付する



電子証明書をエクスポートもしくは再発行後に送信

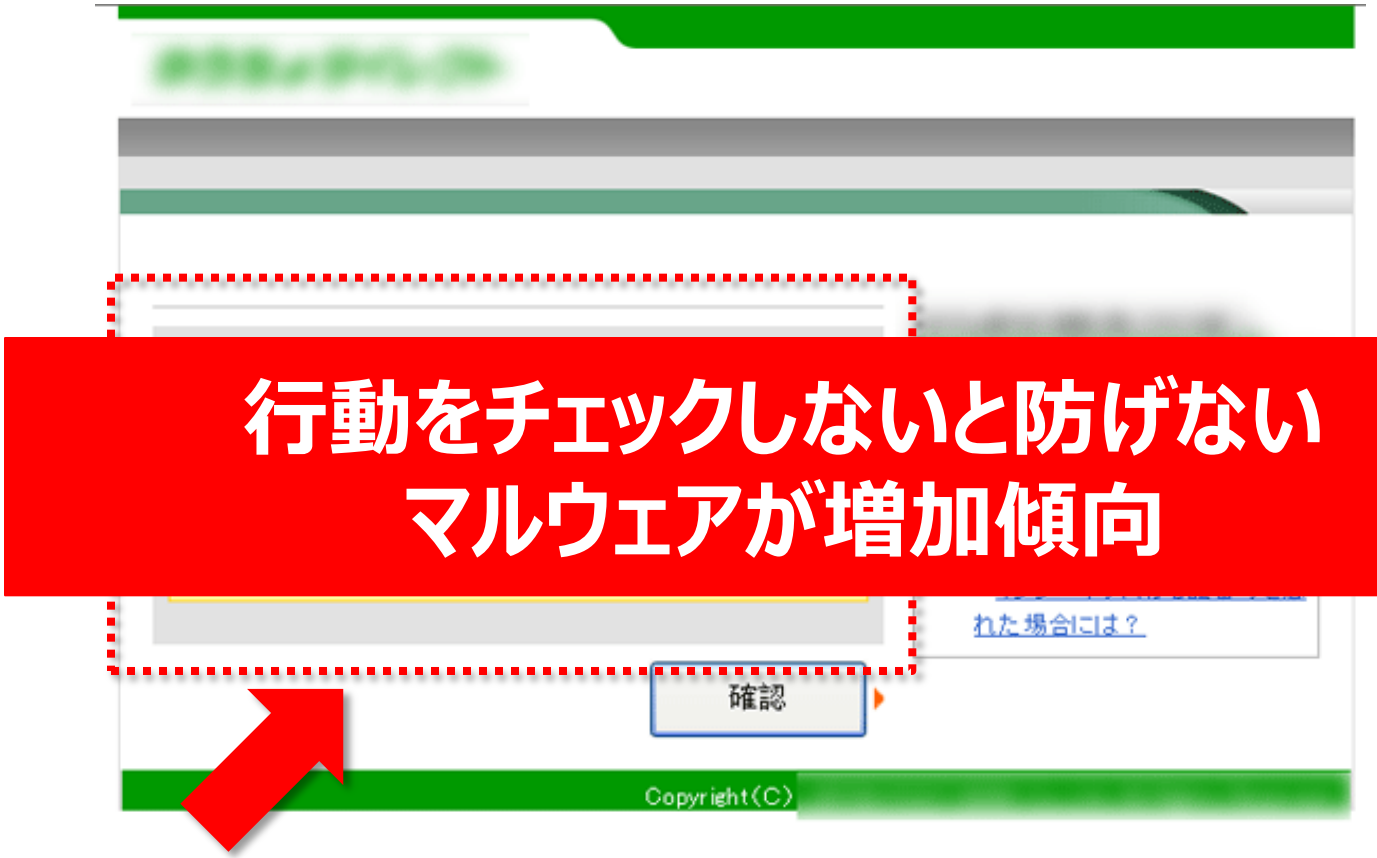
バンキングトロージャンと不正送金の流れ

•個人の興味、射幸心を煽るサイトで仕掛け
•アクセスしたユーザーは知らないうち標的となっている



•ログインで初めて発症しMITBを仕掛ける

MITBとして発症するパターン



行動をチェックしないと防げない
マルウェアが増加傾向

・入力領域のみ表示内容を書き換えユーザー情報を不正入手する。その他のURLと表示は本物。

今後のエンドポイントセキュリティ対策

- PCやスマートデバイスのポイント

「見えない外敵」には、
「行動をチェックするタイプ」が効果的

内部情報漏えい	ユーザーの操作 アプリケーションの利用 データの送受信 外部デバイスの利用	入口対策 ホワイトリスト・ブラックリストによる制御等 出口対策 ロギングによる監査等
外部攻撃	ウイルス対策	新たな手法による解析

現在ウイルス対策ソフトはどんな対応しているか

「行動をチェックする」には、ヒューリスティック検査が非常に有効的

仮にマルウェアがパターンマッチで検出できなくても、そのマルウェアの挙動で危険性を判断することができます。

マルウェアが難読化されていても復号後追って対処。

第三者機関の評価を参考にヒューリスティック品質を確認
・AV-Comparatives、Virus Bulletin、AV Test等

参考
AV-Comparatives.orgのプロアクティブテストの評価状況。ADVANCED+が最も高い評価

	ADVANCED+	ADVANCED	STANDARD	合計
ESET社	18回	1回	0回	19回
A社	12回	4回	3回	19回
B社	1回	7回	6回	14回
C社	2回	8回	3回	13回
F社	7回	3回	3回	13回
E社	1回	3回	3回	7回
D社	0回	0回	5回	5回

不正送金ウイルス(Win32/PSW.Papras)

- ウイルスにより改ざんされたページが表示される

- 2014/2～5までの検出状況

- 専用駆除ツールの提供などで対応
- 5月はヒューリスティック検査による検出も多かった

ヒューリスティックが持つ3つのチェック機能

未知への脅威対策として、3つのチェックが重要
- **静的解析**
- **動的解析**
- **遺伝子工学的解析**

個人用途での対策と応用

個人の場合、水際対策がないためPCで補う必要がある

メモリ内の検査を

•メモリ検査の強化
アドバンスドメモリスキャナ

•脆弱性に対する防御策
バルナラビリティシールド

デバイス制御
スパムメール対策
パーソナルファイアウォール
IDSとHIPS

ウイルス対策のアップデート
セキュリティ修正パッチ

•エクスプロイトをブロックする対策
エクスプロイトブロッカー

従来のパターンやルール対応

HIPS強化とヒューリスティック技術を活用し未知への対応

まとめ

「見えない外敵」に対する備えが必要

- 今回ご紹介した攻撃手法は極めて巧妙です。まずは基本であるウイルス定義ファイルやセキュリティ修正パッチ等を確実に適用しましょう。
- 「行動をチェックする」ことで、早期発見と対応につなげる仕組みを検討しましょう。
- 有事の際に、次に一手を施しやすくするため、現状把握ができる状態にしておきましょう。

エンドポイントセキュリティの強化と見直しが必要

- エンドポイント環境の変化に伴ってリスクが増大します。まずは用途範囲を明確にし、リスクをしっかり洗い出しておきましょう。
- SAMとの連携で管理の効率化も視野に入れましょう。
- “見える化”によるセキュリティ強化しましょう。必要に応じてログ監視などの投入を検討しましょう。
- 利便性とセキュリティのバランスを取りましょう。
    - タブレット → 仮想デスクトップ、MDM、MAM、盗難対策など
    - 無線LAN → IP制限(検疫)、認証など
    - モバイル → ハードディスク暗号化、盗難対策など
    - オンラインストレージ → 認証(二段階認証)、監視、仮想アプライアンスなど

マルウェア情報局

今回お話したマルウェア解説やより詳細なヒューリスティックの解説をしています。

詳しくは マルウェア情報局 **で検索**

ご清聴ありがとうございました