2013年のインターネットを振り返る

JSOC JAPAN SECURITY OPERATION CENTER

2013年11月29日

川口　洋, CISSP
株式会社ラック
チーフエバンジェリスト
hiroshi.kawaguchi @ lac.co.jp

自己紹介

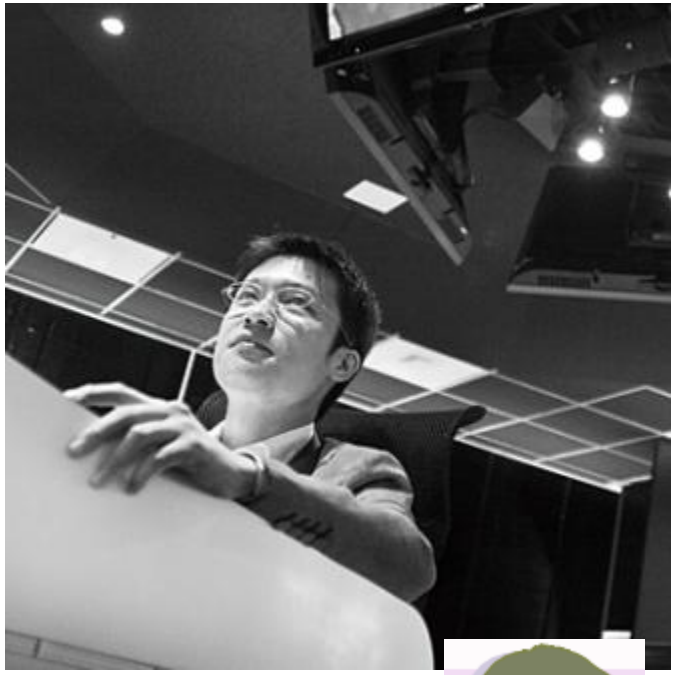
川口　洋(かわぐち　ひろし),CISSP

株式会社ラック

チーフエバンジェリスト 兼 担当部長

ISOG-J 技術WG リーダ

http://www.lac.co.jp/education/instructor/index.html



2002年　ラック入社
社内インフラシステムの維持、運用に従事する。その他、セキュアサーバの構築サービスや、サーバのセキュリティ検査業務なども行い、経験を積む。その後、IDS やFirewall などの運用・管理業務を経て、セキュリティアナリストとして、JSOC監視サービスに従事し、日々セキュリティインシデントに対応。2005年より、アナリストリーダとして、セキュリティイベントの分析とともに、IDS/IPSに適用するJSOCオリジナルシグネチャ(JSIG)の作成、チューニングを実施し、監視 サービスの技術面のコントロールを行う。

チーフエバンジェリストとして、セキュリティオペレーションに関する研究、ITインフラのリスクに関する情報提供、啓発活動を行っている。Black Hat Japan、PacSec、Internet Week、情報セキュリティEXPO、サイバーテロ対策協議会などで講演し、安全なITネットワークの実現を目指して日夜奮闘中。

2010年～2011年、セキュリティ＆プログラミングキャンプの講師として未来ある若者の指導にあたる。2012年、最高の「守る」技術を持つトップエンジニアを発掘・顕彰する技術競技会「Hardening」のスタッフとしても参加し、ITシステム運用に関わる全ての人の能力向上のための活動も行っている。

川口洋のセキュリティ・プライベート・アイズ（@IT）連載中
http://www.atmarkit.co.jp/fsecurity/index/index_kawaguchi.html

ITシステムを取り巻く課題

ITシステムにビジネスが依存している

動かしても褒められないが、止めると叱られる

ハードからアプリのレイヤまで対応すべき範囲が広い

不正アクセス以外のセキュリティ問題にも対応

技術だけではなく社内外のコミュニケーションが必要

若手や新技術で失敗させて経験を積ませる余裕がない

堅牢性 × 売上 × 信頼 ＝ ＄＄＄

Hardeningとは

ビジネスと顧客を守る総合力を競うセキュリティイベント

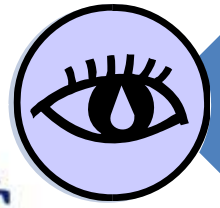
（WAS Forum Hardening Project 主催）

WASForum.jp
Web Application Security Forum

HARDENING

「ビジネス継続」を踏まえた防御戦略に焦点

「守れる」エンジニアの顕彰と発掘



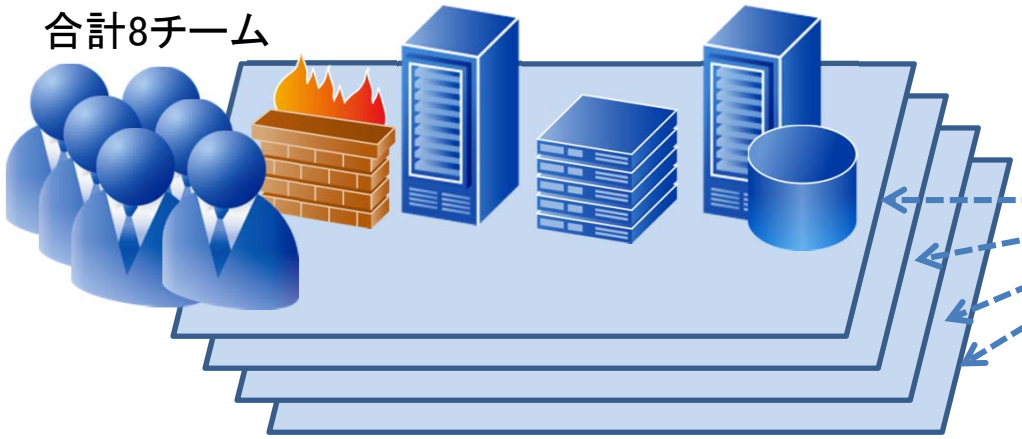
顧客・マーケット・観客の視点

LAC

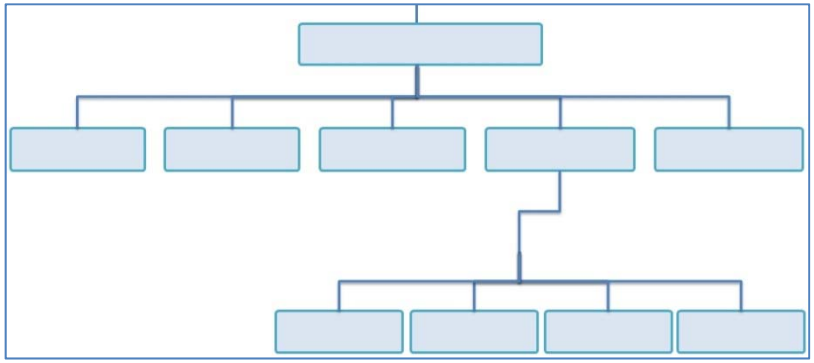
Hardening 環境

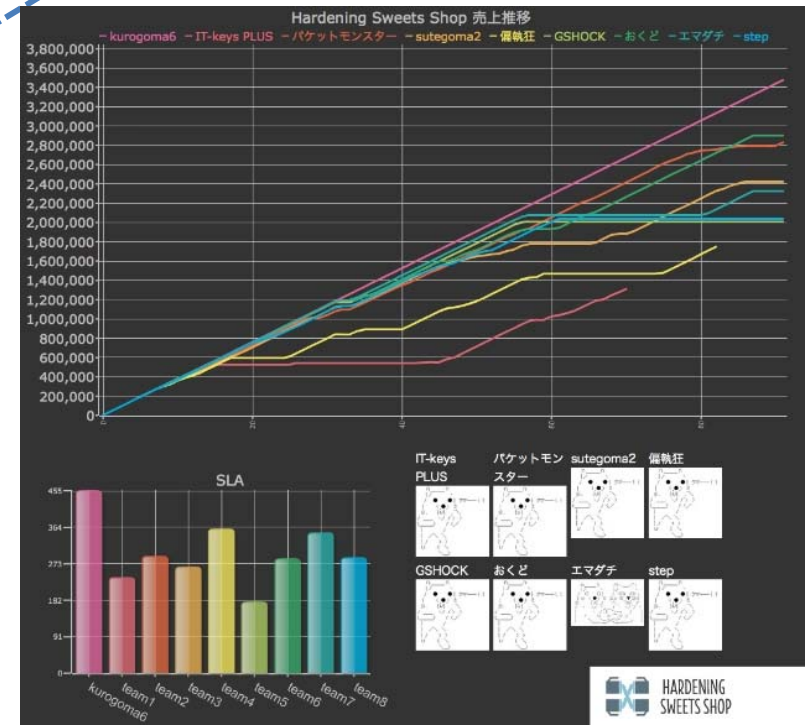
評価チーム　kuromame6

1チーム 6人
合計8チーム



イベント発生
評価を実施





NICT StarBEDにシステムを構築
参加チームに与えられる環境

- 同じ　システム構成
- 同じ　社内システム運用ルール
- 同じ　商品
- 同じ　イベント

売上の推移

（8時間の競技時間でどこまで伸ばせるかが勝負）

Hardeningイベント結果

「おたくの個人情報が漏れていますよ」と、連絡が来た

ECサイトの利用規約にクレームがついた

コンテンツのミラーリングに失敗したのでサイトがエラーを起こした

ウェブサーバが突然再起動した

顧客から送付されてきた添付ファイルが怪しいでも、放置できない

ユーザのアクセスに耐えきれないのでパフォーマンスチューニングをやらなきゃ！

同じ環境、同じ商品、同じ攻撃が発生して運用の差で売上に三倍の差がでることがわかり、ITシステム運用の重要性を示すことができた

本番のシステムで障害を起こすわけにはいかないが、この環境で痛い目にあうことはいい経験になるはずだ

限られた時間の中で対応するべき問題を取捨選択することが重要だと感じた

競技を行うHardening Dayとともに振り返りを行うSoftening Dayの時間も重要だと思う。

詳細は@ITコラムを参照
川口洋のセキュリティ・プライベート・アイズ（42）：
そのときStarBEDが動いた――「Hardening One」の夜明け前（1/3）
http://www.atmarkit.co.jp/ait/articles/1212/10/news015.html

会場に質問！！

Hardeningイベントって知っていますか？

- 参加したことがある
- 参加したいと思ったが、断念した
- 存在だけは知っていた
- 初めて知った

https://www.vot.rs/3df528
から回答、または
https://www.vot.rs/
にアクセスして
47 94 37
を入力して回答

最近のニュースを振り返る

最近のニュース：2012年5月

ロジテック製300Mbps無線LANブロードバンドルータ
（LAN-W300N/R、LAN-W300N/RS、LAN-W300N/RU2）に関するお詫びとお願い

ロジテック　300Mbps無線LANブロードバンドルータの一部において、セキュリティに脆弱性があることが判明いたしました。
この脆弱性により、インターネット接続に必要な「PPPoEの認証ID」および「PPPoEの認証パスワード」が外部より取得される可能性がございます。

■対象製品

製品名　製品名 300Mbps無線LANブロードバンドルータ

型番


▲LAN-W300N/R


▲LAN-W300N/RS


▲LAN-W300N/RU2

シリアルナンバー 末尾が「B」

ファームウェア バージョン2.17

▼※パッケージ裏面の右下、バーコードに青色の識別シールが貼られた製品は対策済み製品です。

http://www.logitec.co.jp/info/2012/0516.html

最近のニュース:2013年8月

情報通信基盤の安心・安全を確保するために活動している一般財団法人日本データ通信協会テレコム・アイザック推進会議(所在地:東京都港区、会長:飯塚久夫、以下、Telecom-ISAC Japan)は、国内主要通信事業者、ISP(インターネットサービスプロバイダ)の業界団体として、インターネットの安定運用に関わる事象の検出および対処に取り組んでおります。

I. 背景・概要

Telecom-ISAC Japanでは昨年7月30日に以下の注意喚起を行い、その状況を追い続けておりました。

【注意喚起】ロジテック製ルータの脆弱性、および、利用者が行うべき必要対策
https://www.telecom-isac.jp/news/news20120730.html

その結果、本年5月頃より発生している不正アクセスインシデントのいくつかは、本脆弱性の悪用によって得られた情報を攻撃者が利用したものであることが判明しました。そのため、主管省庁とも相談のうえ、会員企業および製品ベンダーによる対策実行について、状況調査から協力し支援していくことにいたしました。

II. 調査内容・時期について

この調査は、協力要請をいただいた会員ISPのIPアドレス帯に対して、該当製品の所在を簡易な通信コマンドで確認するものです。ネットワーク利用者に負荷をかけるものや、通信の内容を見るようなものでは一切ありません。

また、調査の実施につきましては、8月30日から順次行うことを予定しております。

https://www.telecom-isac.jp/news/news20130830.html

- **Telecom-ISAC Japan が脆弱性を持つ機器の調査を実施**
- **ロジテック製ブロードバンドルータの脆弱性を悪用した攻撃を危惧**
- **ISPが積極的に脆弱性を持つ機器の把握、注意喚起に乗り出した貴重な取り組み**

会場に質問！！

この問題を把握していましたか？

- 把握していた
- 初めて知った
- 関係ないと思っていた

https://www.vot.rs/33e943
から回答、または
https://www.vot.rs/
にアクセスして
61 80 73
を入力して回答

最近のニュース:2013年2月

Facebook、「ゼロデイ攻撃を受けたがユーザーデータは無事」と発表

Facebookが、先月ゼロデイ攻撃を受けていたことを発表した。ユーザーデータが危険にさらされた証拠はないとしている。

[佐藤由紀子，ITmedia]

Apple社内のMacもマルウェア感染、Javaの脆弱性を悪用

FacebookやTwitterに続き、Appleもマルウェア感染の被害に遭っていたことが分かった。

[鈴木聖子，ITmedia]

Microsoftにもサイバー攻撃、Mac事業部門でマルウェア感染

MicrosoftもFacebookやAppleと同様の被害に遭っていたことを明らかにした。

[鈴木聖子，ITmedia]

最近のニュース：2013年4月

AP通信のTwitterがハッキング被害、「爆発で大統領が負傷」のデマ流す

通信社のAPのTwitterに掲載された「ホワイトハウスで2度の爆発。オバマ大統領が負傷」という速報はデマだった。

http://www.itmedia.co.jp/enterprise/articles/1304/24/news034.html

[鈴木聖子，ITmedia]

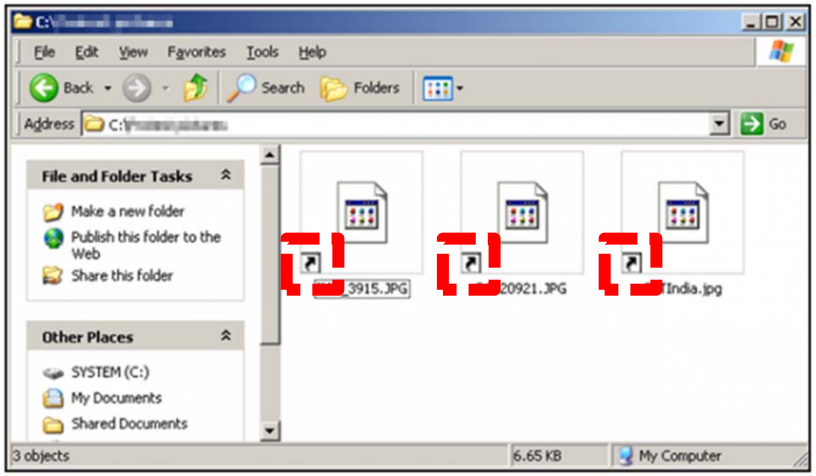
会場に質問！！

TwitterやFacebookのアカウントが乗っ取られたことがある？

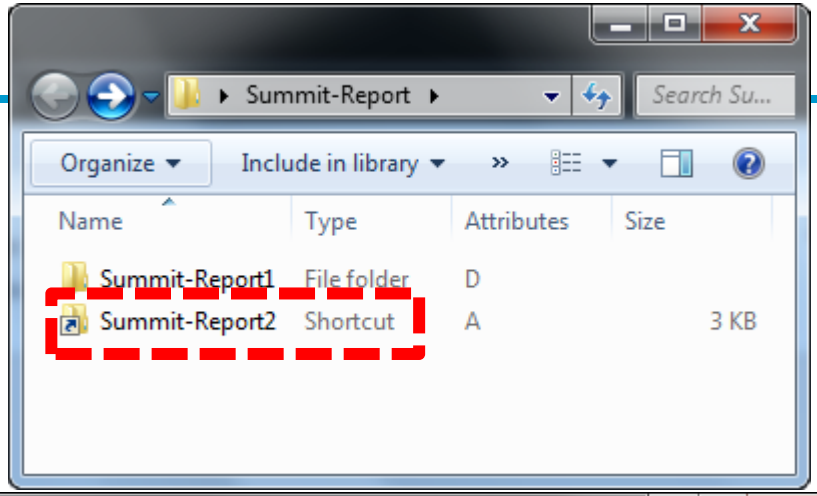
- ある
- ない
- ないが、知人がやられた

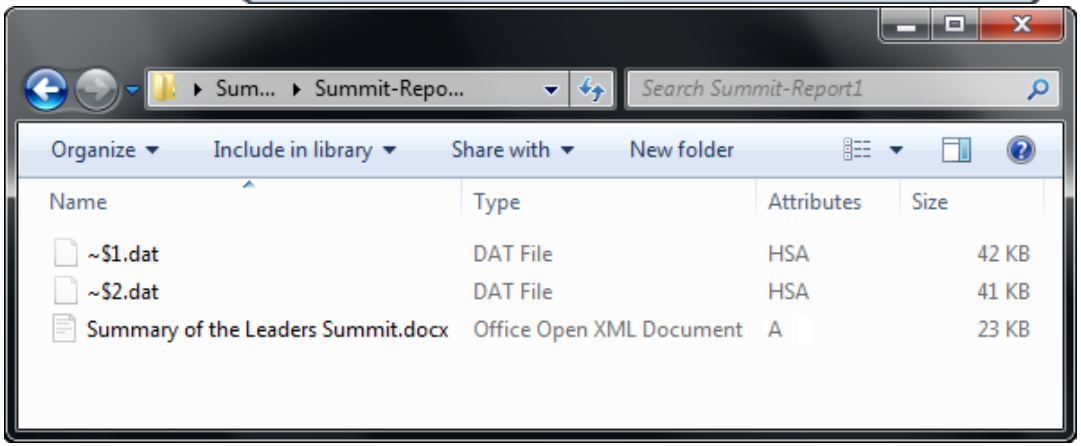
https://www.vot.rs/a9cb94
から回答、または
https://www.vot.rs/
にアクセスして
61 20 19
を入力して回答

最近のニュース：2013年5月



http://www.symantec.com/connect/ja/blogs/lnk

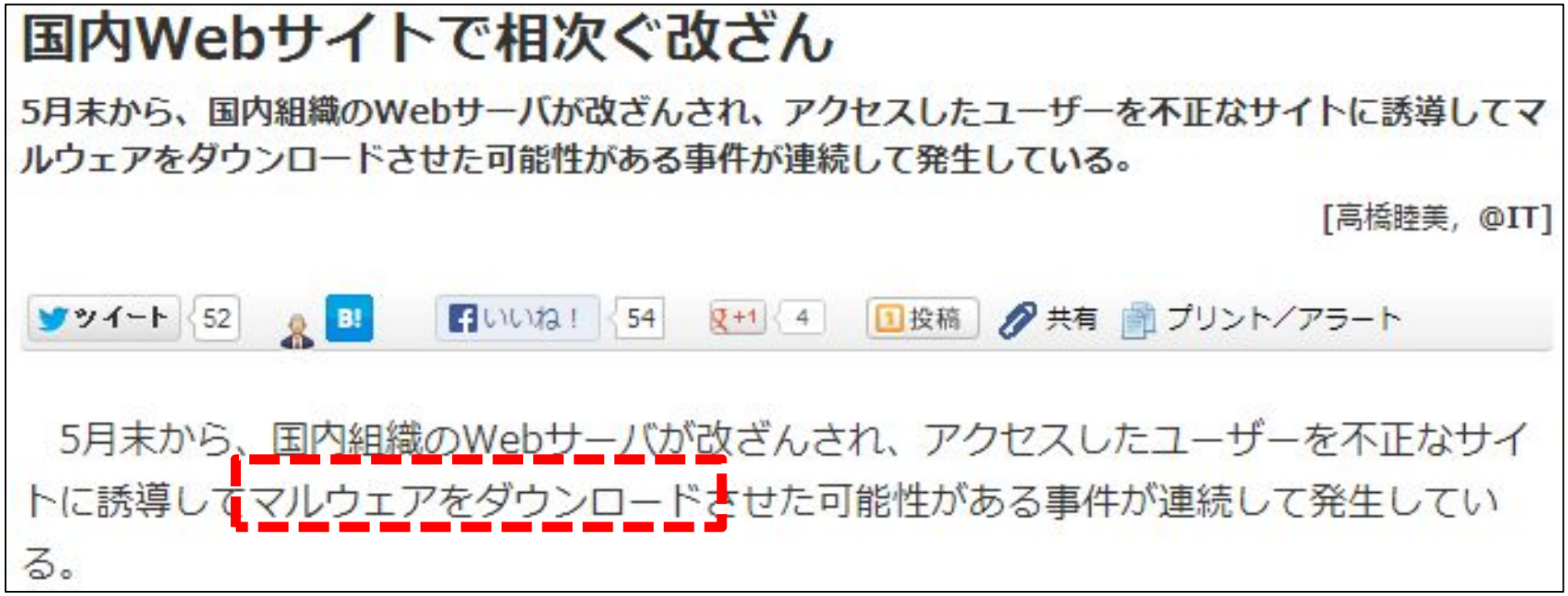




http://www.symantec.com/connect/ja/blogs-300

- ショートカットファイルを添付したメールを送付
- ショートカットファイルを実行すると、外部からマルウェアをダウンロードして実行
- 一般のユーザは「ショートカットファイルは危ないの？」という認識
- カモフラージュのため、フェイクのテキストファイルを開くことも

最近のニュース:2013年6月



国内Webサイトで相次ぐ改ざん

5月末から、国内組織のWebサーバが改ざんされ、アクセスしたユーザーを不正なサイトに誘導してマルウェアをダウンロードさせた可能性がある事件が連続して発生している。

[高橋睦美，@IT]

ツイート 52 B! いいね！ 54 +1 4 投稿 共有 プリント/アラート

5月末から、国内組織のWebサーバが改ざんされ、アクセスしたユーザーを不正なサイトに誘導してマルウェアをダウンロードさせた可能性がある事件が連続して発生している。

http://www.atmarkit.co.jp/ait/articles/1306/04/news079.html

- **複数のサイトのホームページが改ざんれる**
- **不正なサイトに誘導するiframeやJavaScriptタグが挿入される**
- **不正なサイトに誘導されたユーザにマルウェアを感染させる**
- **数年前に流行したGumblarと同様の攻撃の流れ**

最近のニュース：2013年8月

感染パソコン1.5万台超　ネットバンキング不正送金
警視庁捜査

2013/8/8 22:58｜日本経済新聞　電子版

小 中 大　保存　リプリント　▼共有

インターネットバンキングを巡る一連の不正送金事件で、利用者のIDやパスワードを盗む目的のウイルスに感染しているパソコンが、日本国内で少なくとも1万5千台あることが8日、警視庁への取材で分かった。ウイルスが仕込まれた企業や省庁のホームページの閲覧などを通じ、感染した可能性がある。

http://www.nikkei.com/article/DGXNASDG0702M_Y3A800C1CC1000/

最近のニュース：2013年8月

■発生した事象

ロリポップ！のサーバー上にインストールされた WordPress を利用して作成された一部のユーザーサイトにおいて改ざんの被害が発生いたしました。改ざんの被害にあったサイトでは、下記のいずれかの事象が確認されております。

・ 今回の攻撃によるサイト改ざん内容の特徴

サイトタイトルに「Hacked by Krad Xin」が含まれている

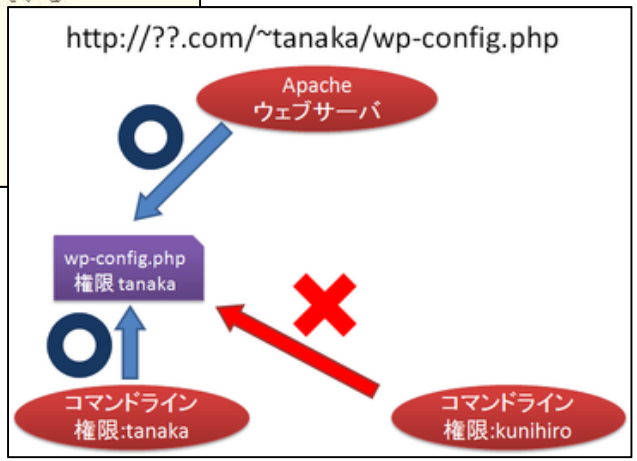
サイトのキャッチコピーが「BD GREY HAT HACKERS」になっている

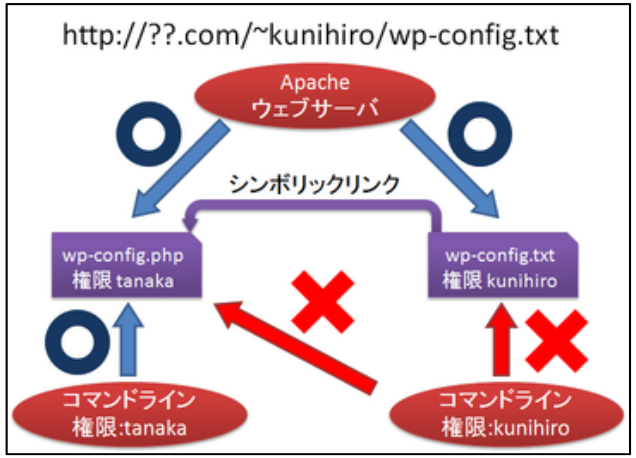
サイトが文字化けしている

・同様の改ざんを確認している対象件数

8,438件

http://lolipop.jp/info/news/4149/





http://tanaka.sakura.ad.jp/2013/09/symlink-attack.html

- ロリポップ！でWord Pressを使用しているユーザのサイトが改ざんされた
- WordPressの設定とSymlink Attacks
- コマンドラインからアクセスできないものがウェブサーバの権限でアクセス可能
- 共有サーバサービスを提供している事業者は対策を検討するべき

最近のニュース:2013年8月

ブレーキもハンドルも利かない――自動車ハッキングを実証

米誌Forbesの記者が乗った車の後部座席でセキュリティ研究者がコンピュータを操作すると、走行中に急ブレーキがかかり、パワステも利かなくなった。

LIXILのトイレ操作アプリに脆弱性 - 使用中に蓋の開閉やビデが行われる恐れ

[2013/08/05]

米国のセキュリティ会社であるTrustwaveは8月1日、LIXILが提供するAndroid向けトイレ操作アプリ「My SATIS」にハードコード化されたBluetooth PINの脆弱性が見つかったと発表した。

偽のGPS信号で豪華ヨットの乗っ取りに成功、米テキサス大が実験

研究チームは偽のGPS信号を送ってヨットのナビゲーションシステムを制御。ヨットのGPS装置では攻撃を受けていることは検知できなかった。

[鈴木聖子，ITmedia]

BlackHat 2013 – セキュリティカメラのハッキング

2013年08月16日 14:56

yj_ukai

オフィシャルコメント　by:鵜飼 裕司

ツイート

最近のニュース:2013年8月

2ちゃんねるの有料サービスでクレジットカード情報含む顧客情報が流出

インターネットの掲示板「2ちゃんねる」の有料サービス「2ちゃんねるビューア」が不正アクセスを受け、顧客情報がネット上に流出していることが明らかになった。

[高橋睦美，@IT]

「なんJ」人気まとめサイトが閉鎖　2ch情報流出で過去の荒らし行為がばれる

まとめサイト「僕自身なんJをまとめる喜びはあった」が閉鎖を告知。2ちゃんねる情報流出事件で同サイト管理人による過去の荒らし行為などが発覚したためという。

[ITmedia]

2ちゃん情報流出　「匿名の暴言」が突きつけた闇 (1/2)

2ちゃんねるビューワの情報流出で、匿名のつもりで吐いた暴言の発言者が特定される例が続出し、一部で深刻な人間不信を招いている。流出という事態は、どんな「闇」を照らし出したのか。

[産経新聞]

- 2chの有料サービスから様々な情報が漏えい
- 運営用のものを含むトリップ／キー情報、購入した人のクレジットカード情報や住所氏名といった個人情報、それにユーザー全員の過去十年の書き込み履歴など

最近のニュース：2013年8月

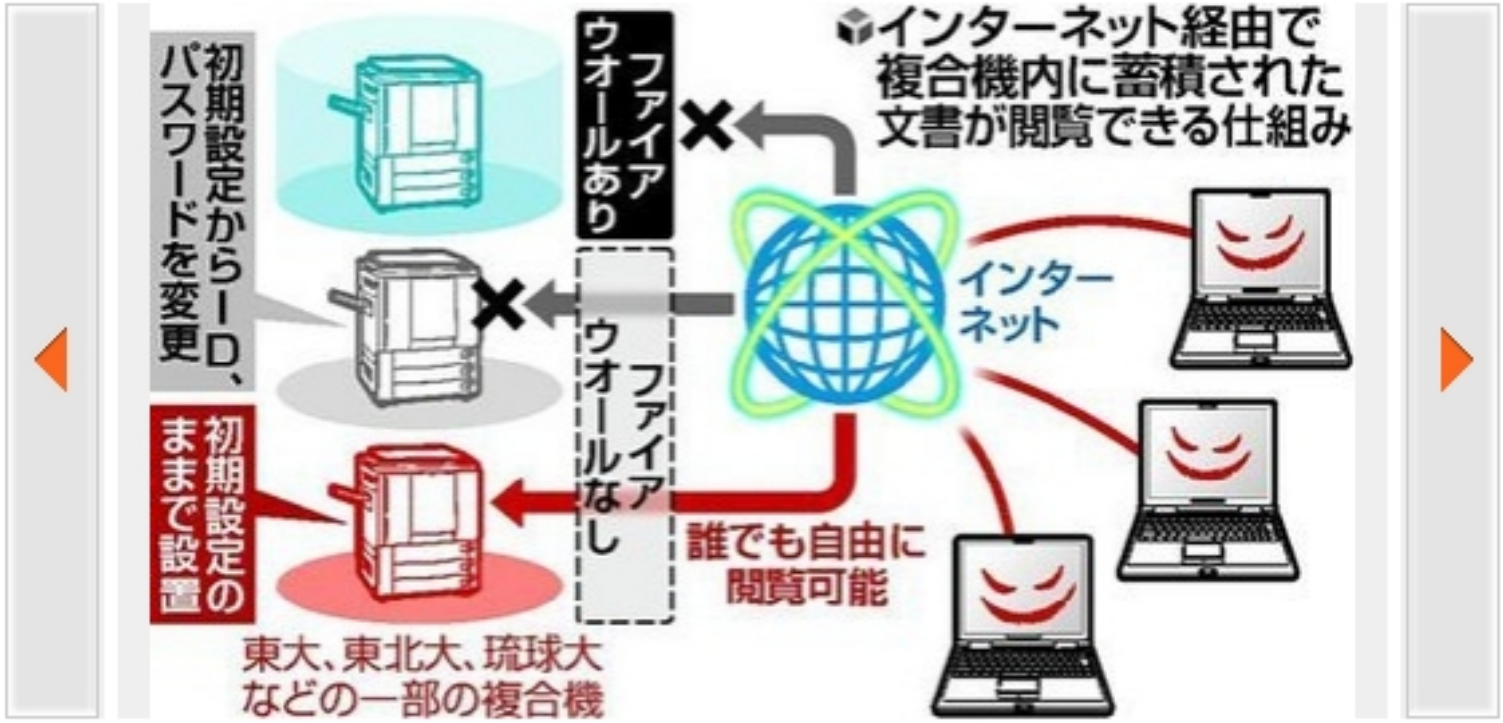
日本企業の社外秘資料、大量流出＝中国の文書共有サイトに一大手軒並み被害

【北京時事】文書・資料やデータをインターネット上で共有できる中国の有力サイト「百度文庫」に日本企業の社外秘資料や内部文書が1、2年前から大量流出し、誰でも見られる状態になっていることが7日分かった。情報流出問題を調査し、日本企業の対応にも当たる分部悠介弁護士（上海駐在）によると、大手メーカーの特許出願前の技術資料や、日本の広告会社の顧客向けプロジェクト提案資料なども流出したことがあるという。

http://www.jiji.com/jc/zc?k=201308/2013080700488

http://wenku.baidu.com/

最近のニュース:2013年11月



住民票・答案…複合機の蓄積データ、公開状態に

読売新聞 11月7日(木)3時1分配信

http://www.yomiuri.co.jp/net/news0/national/20131106-OYT1T01518.htm

- 複合機がインターネットに接続されており、参照可能になっている
- 印刷データ、スキャンデータ等が残っている
- SHODANを使用して検索することも可能

会場に質問！！

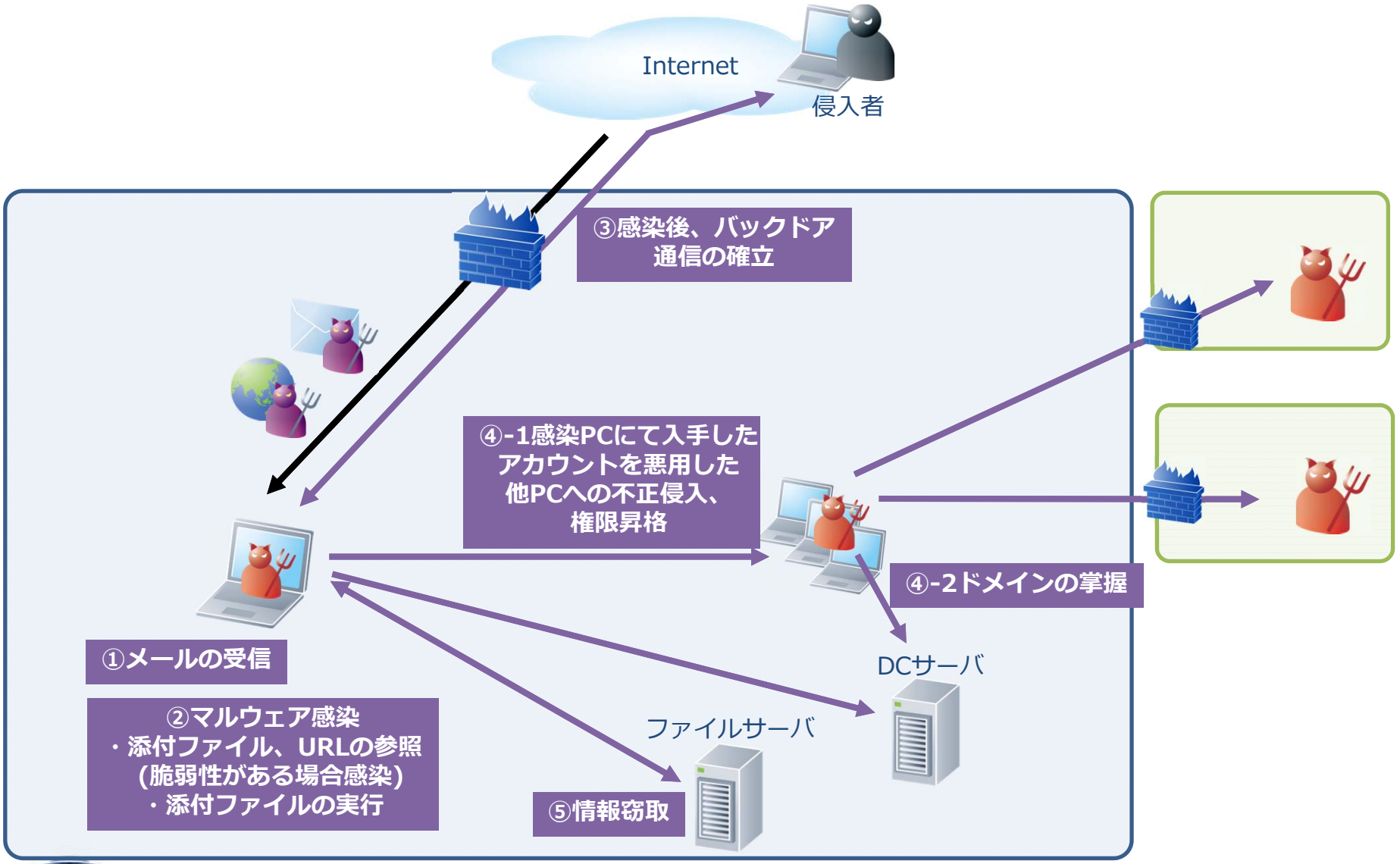
このニュースを見たときの感想は？

- 今どきこんなことが問題になるとは思わなかった
- 身の回りで起きてちょっと冷や汗をかいた
- 大学ではよくあることだと思った
- このニュースを初めて知った

https://www.vot.rs/c09482
から回答、または
https://www.vot.rs/
にアクセスして
39 22 64
を入力して回答

水飲み場型攻撃を題材に考える

一般的な標的型（メール）攻撃の流れ



MS、Apple、FBに対する攻撃

Facebook、「ゼロデイ攻撃を受けたがユーザーデータは無事」と発表

Facebookが、先月ゼロデイ攻撃を受けていたことを発表した。ユーザーデータが危険にさらされた証拠はないとしている。

[佐藤由紀子，ITmedia]

Apple社内のMacもマルウェア感染、Javaの脆弱性を悪用

FacebookやTwitterに続き、Appleもマルウェア感染の被害に遭っていたことが分かった。

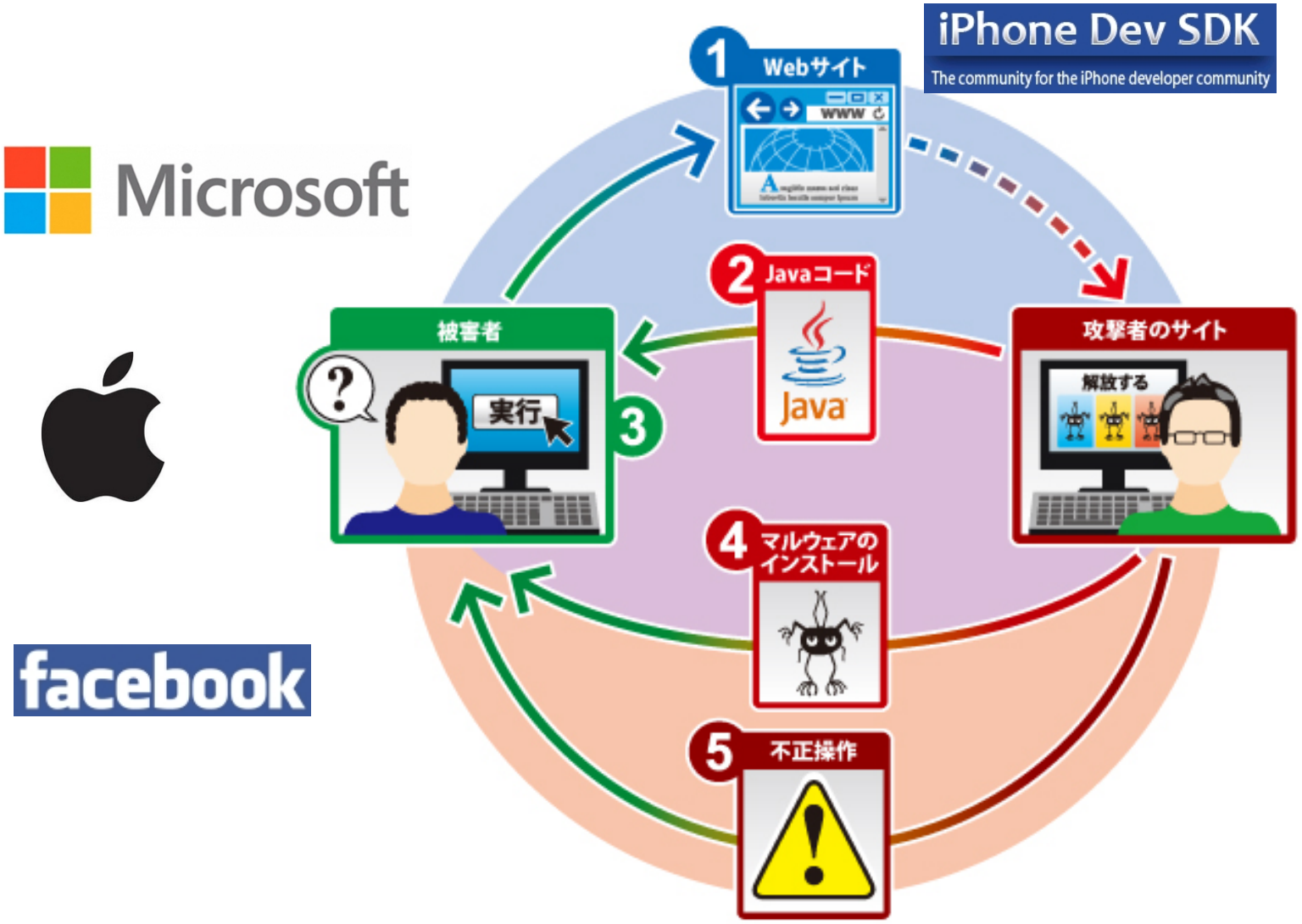
[鈴木聖子，ITmedia]

Microsoftにもサイバー攻撃、Mac事業部門でマルウェア感染

MicrosoftもFacebookやAppleと同様の被害に遭っていたことを明らかにした。

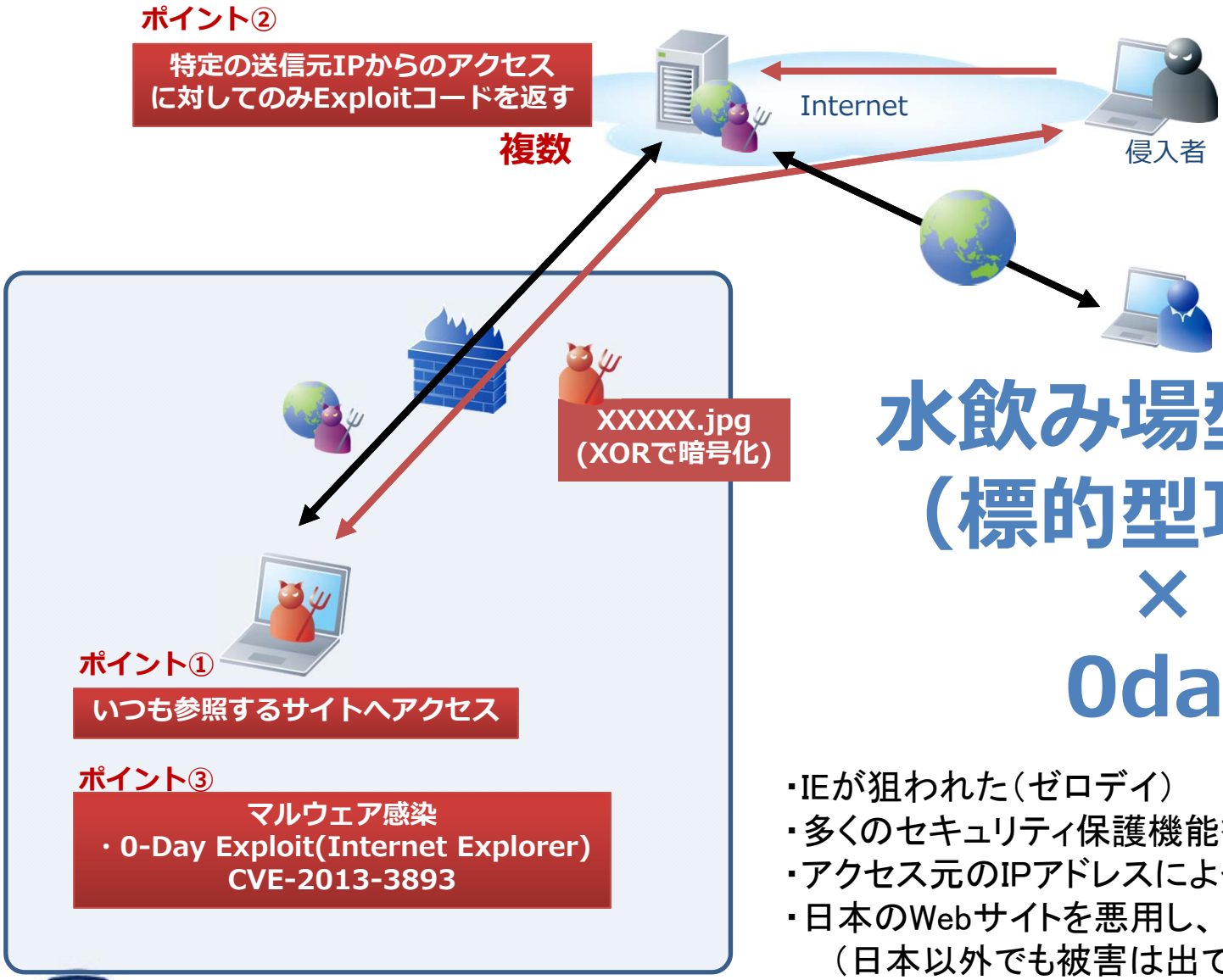
[鈴木聖子，ITmedia]

水飲み場型攻撃の攻撃の流れ



http://www.atmarkit.co.jp/ait/articles/1303/07/news004.html

2013年8月から発生していた攻撃



水飲み場型攻撃（標的型攻撃）×0day

- IEが狙われた（ゼロデイ）
- 多くのセキュリティ保護機能をすり抜けていた
- アクセス元のIPアドレスによって制御
- 日本のWebサイトを悪用し、日本の組織を狙った
  （日本以外でも被害は出ている）

現場にある悩み

- ウイルス対策ソフトで見つからない
  - みつからない時点で「ウイルス感染事故」ではない
  - 「不正アクセス事件」として処理するべき

- インターネットアクセスのログ（Outbound通信のログ）を取得していない
  - ログが取ってあれば後からでも追跡調査が可能
  - アクセス制御もついでに実施

- ウェブ改ざんの対応が不十分
  - コンテンツを戻して終わり
  - でも、誰かが調査しないとわからない

会場に質問！！

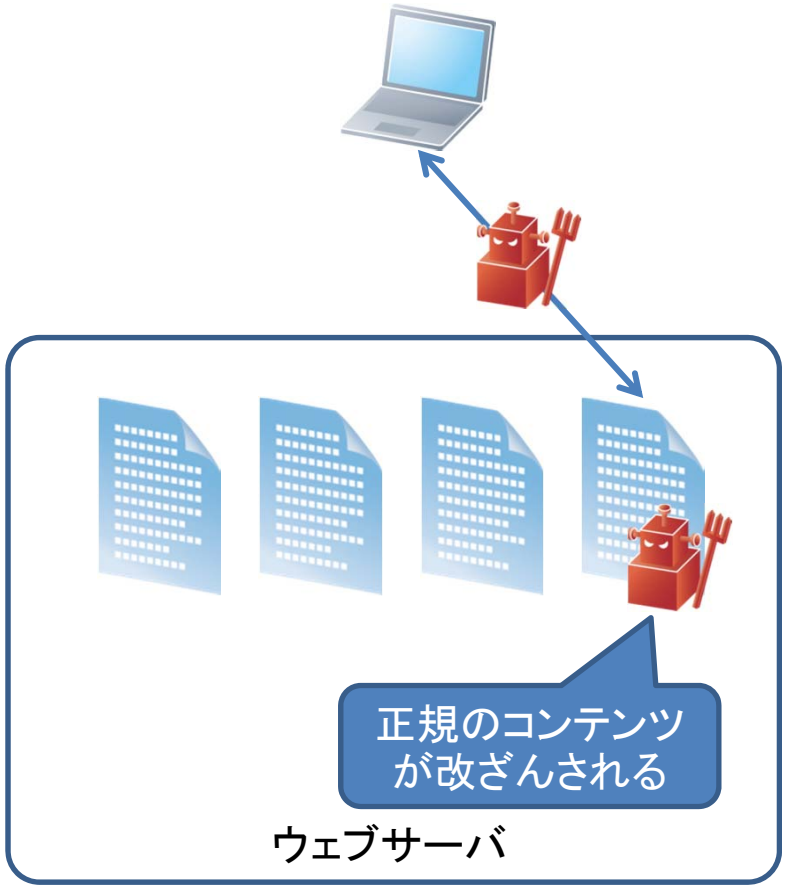
もし、あなたの管理するウェブサイトが改ざんされたらどうする？

・コンテンツを復元して終わりにする
・コンテンツを復元して、穴だけふさいで、あとは忘れる
・原因と被害内容を徹底調査する
・原因と被害内容を徹底調査して、さらに警察に届けを出す

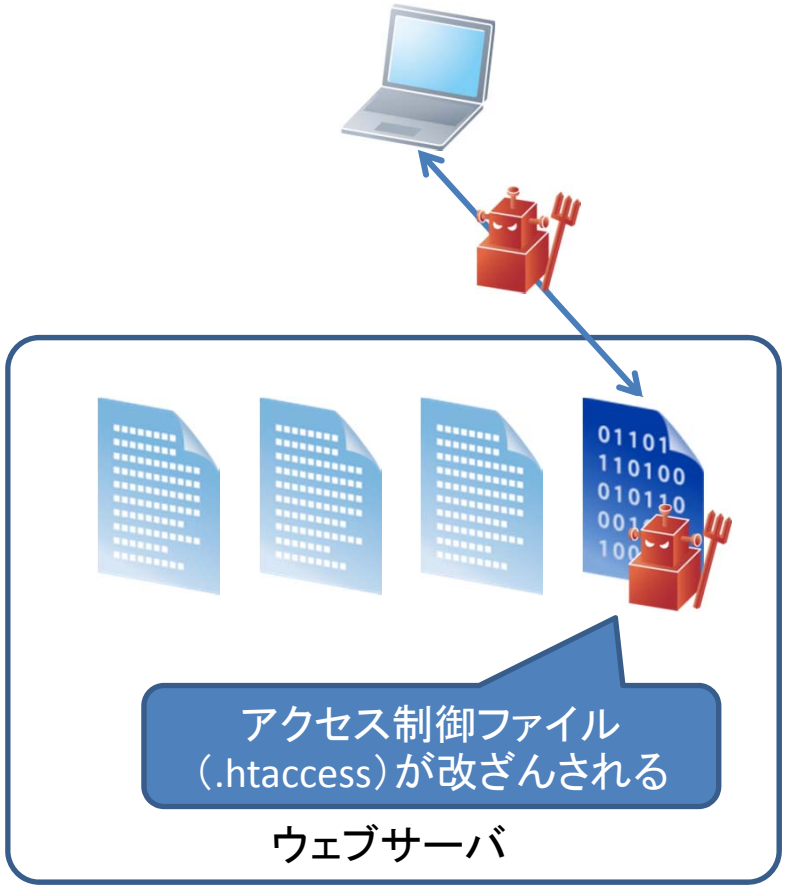
https://www.vot.rs/5e3bde
から回答、または
https://www.vot.rs/
にアクセスして
78 48 14
を入力して回答

ウェブ改ざんのパターン(1)

よくあるウェブ改ざんのパターン



ちょっと珍しい改ざんのパターン

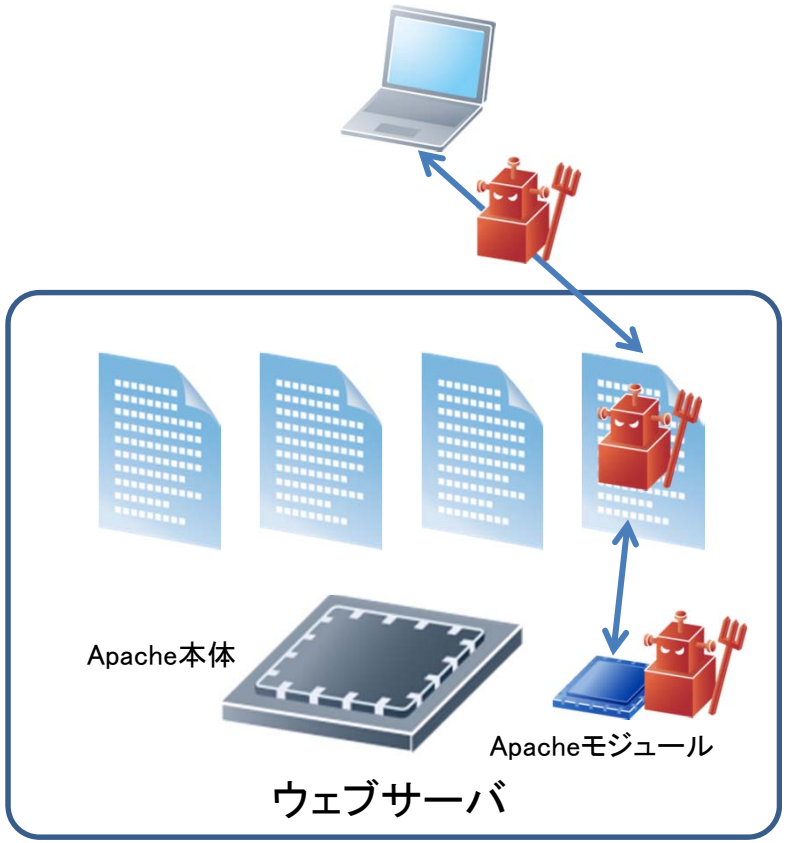


- htmlやjs、phpファイル等のコンテンツが直接改ざんされる
- バックアップファイルとの差分で調査可能

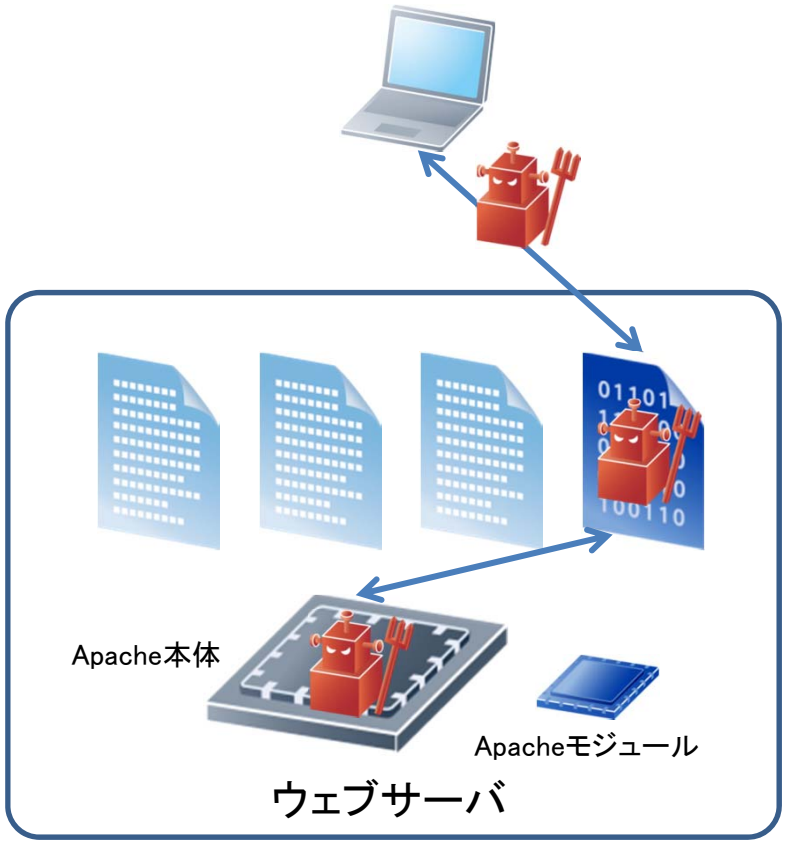
- .htaccessを設置or改ざんする
- 特定RefererやUser-Agentの場合のみ改ざんデータを送信可能

ウェブ改ざんのパターン(2)

Apacheモジュールを改ざんするパターン
Darkleech Apache Moduleの場合



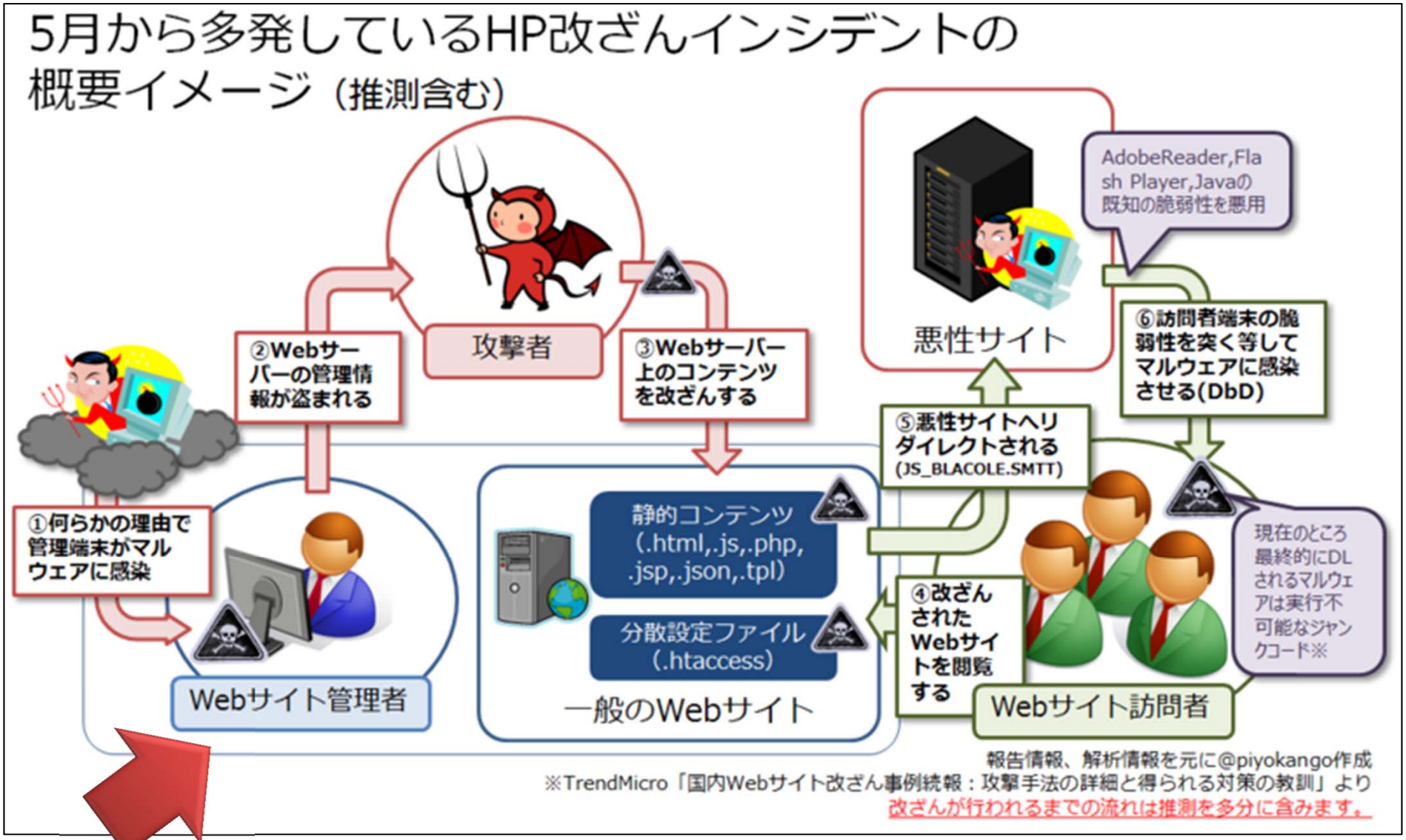
Apache本体(httpd)自体を改ざんするパターン
Apache Binary Backdoor (Cdorked)の場合



- コンテンツファイルは改ざんせず、Apacheのモジュールを改ざんする
- root権限が必要

- コンテンツファイルは改ざんせず、Apacheの本体のプログラムを改ざんする
- root権限が必要

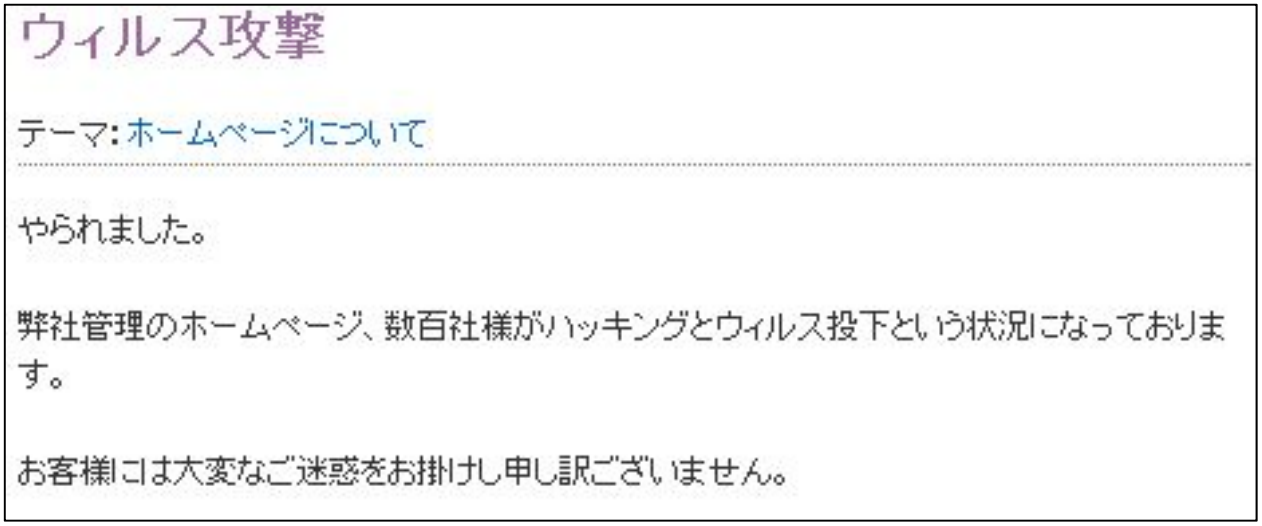
攻撃の流れ



piyologより引用
http://d.hatena.ne.jp/Kango/20130604/1370353242

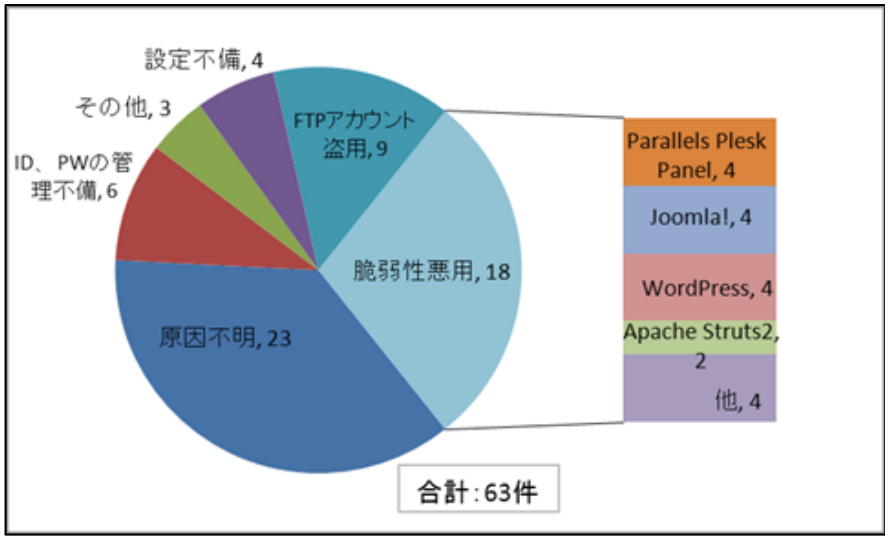
ホームページ改ざんに気づくきっかけ

- ホームページ改ざんチェックシステムのアラート
- 外部のユーザからの通報
  - 「おたくのページが改ざんされている」
  - 「おたくのページにアクセスするとウイルス対策ソフトからアラートが出た」
- 管理会社からの通報



よくあるウェブ改ざんのパターン

- いわゆるGumblar型攻撃（マルウェアに感染し、FTPやCMS等のホームページ管理用IDが盗まれ、不正ログイン）
- SQLインジェクション
- CMSの設定不備、脆弱性未対策
- SSHブルートフォース攻撃
- Tomcat等のミドルウェアからの侵入
- Struts等のフレームワークからの侵入
- Plesk、cPanel等の管理画面からの侵入
- BGP、ARP、DNS等のポイゾニング
- HTTP PUTのアクセス制御不備
- FrontPage Server Extentions経由



http://www.ipa.go.jp/security/txt/2013/06outline.html

具体的な対策

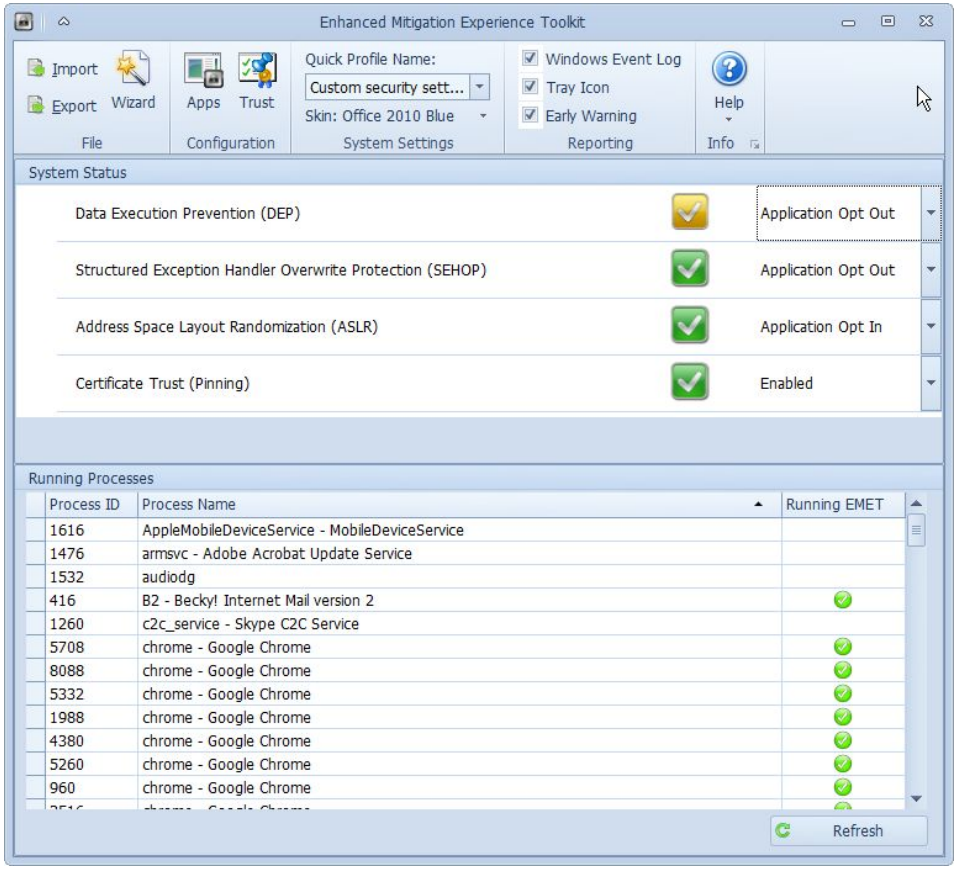
すぐにやるべき対策

対策ポイント	対策内容
システム全体	**ログ保存を行う（ログイン履歴、Outboundログは必須）** ログ保存期間を延ばす（最低1年） リモートアクセスのログイン履歴を確認
サーバ	アプリのバージョンを確認する （Tomcat, JBoss, Struts, ColdFusion, Joomla!, WordPress, Movable Type, MODX など） ウイルス対策ソフトのスキャンログを確認する
クライアント	使用しているJavaのバージョンを確認する Adobe Reader、Flash Player、Java、一太郎のアップデートを行う ウイルス対策ソフトのスキャンログを確認する (自宅の)**パソコンにEMETを入れる**
ネットワーク	**FW、Proxy、URLフィルタ等のログを確認する** アクセス制御ルールに不備がないか確認する
人・組織	緊急時の連絡網を整備する セキュリティ情報の収集を行う

共通対策：ログ確認

- FW、Proxy、URLフィルタのログから以下のIPアドレスやドメインに対するアクセスがないか調べてください。
  - ezua.com
  - zyns.com
  - ns2.name
  - livecheck.org
  - acmetoy.com
  - toh.info
  - 2waky.com
  - ibmnetvista.com
  - xxuz.com
  - myfw.us
  - www.microsoftoupdate.com
  - www.cloudsbit.com
  - nifty-login.com
  - nifty-user.com
  - nifty-japan.com
  - yahoo-user.com
  - yahoo-dns.com
  - google-login.com
  - 60.10.1.114
  - 60.10.1.118
  - 60.10.1.119
  - 60.10.1.120
  - 60.10.1.121
  - 112.213.118.31
  - 112.213.118.32
  - 112.213.118.33
  - 112.213.118.34
  - 112.213.118.43
  - 103.4.225.41
  - 217.160.91.159
  - 219.148.34.233
  - 221.8.69.25
  - 222.80.184.54
  - 103.17.117.90
  - 111.118.21.105
  - 180.150.228.102
  - 210.176.3.130
  - 211.47.206.113
  - 218.38.28.96
  - 218.38.28.99

共通対策:EMET （オススメ！！）



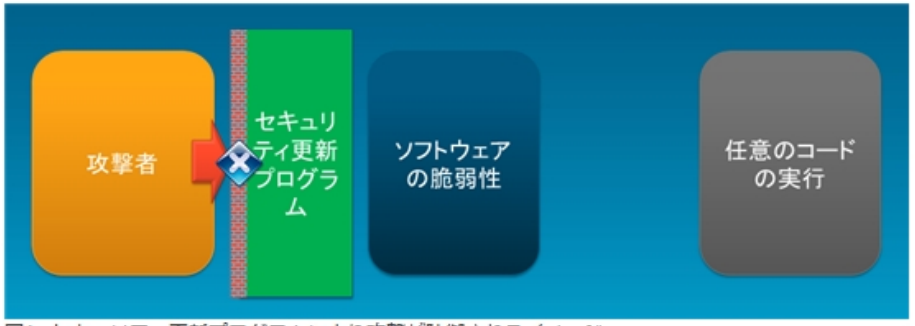


図1: セキュリティ更新プログラムにより攻撃が防御されるイメージ

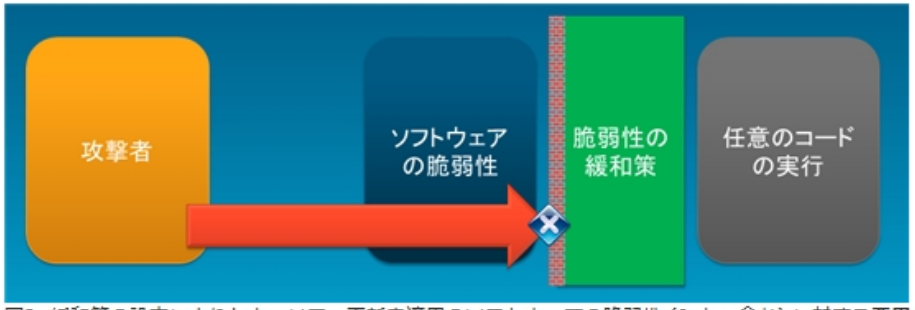
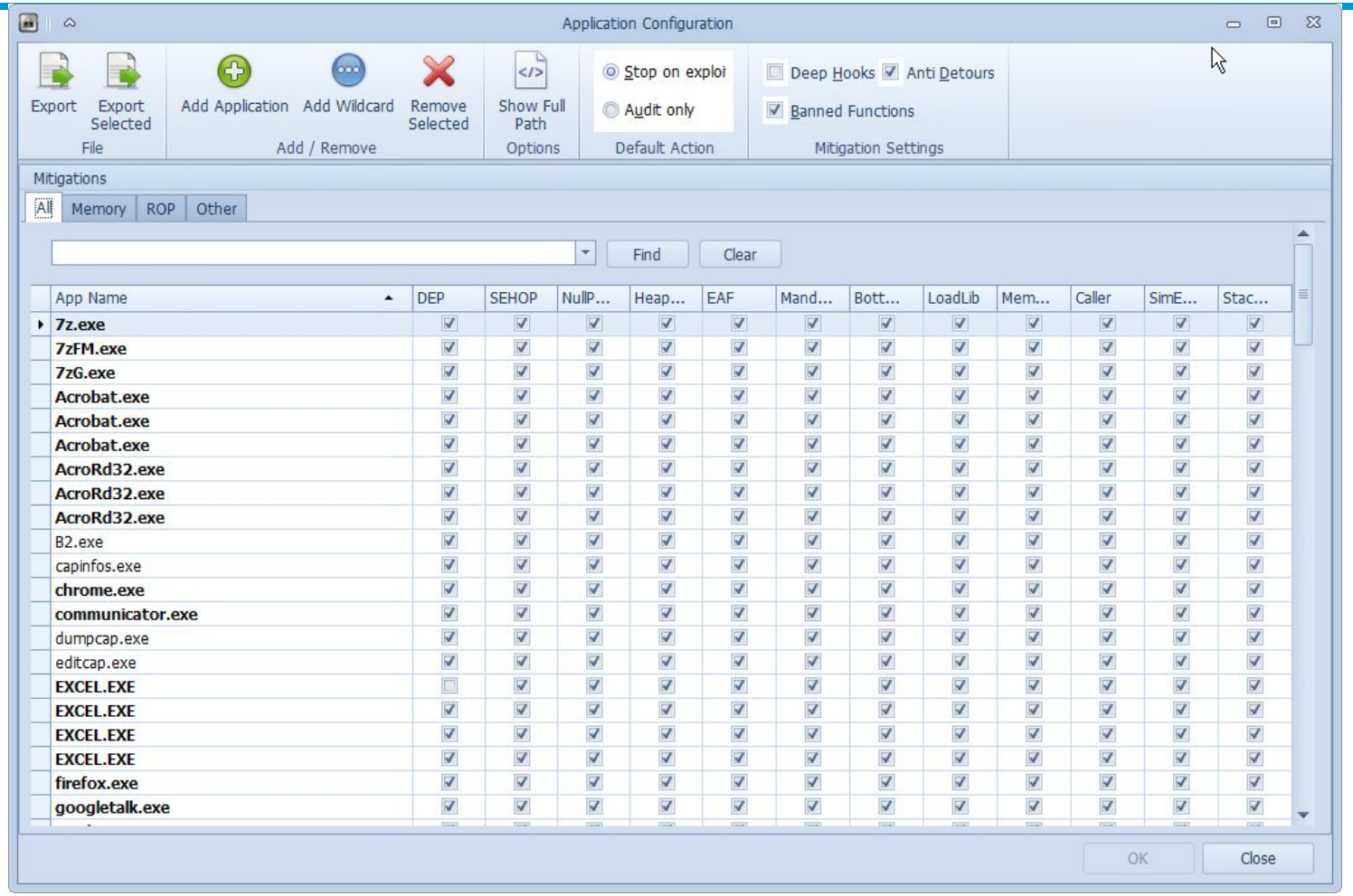


図2: 緩和策の設定によりセキュリティ更新未適用のソフトウェアの脆弱性 (0-day 含む) に対する悪用が回避されるイメージ

- マイクロソフトが公開する無償の脆弱性緩和ツール
- Windowsの保護機能を活用して、システムに対する攻撃から保護するツール
- http://support.microsoft.com/kb/2458544/ja
- バージョンがあがり設定が簡単になった
- とりあえず、Maximumを選んでおくのもいい
- ADでの大規模展開プロファイルや通知機能が強化されており、便利になった

共通対策:EMET （オススメ！！）



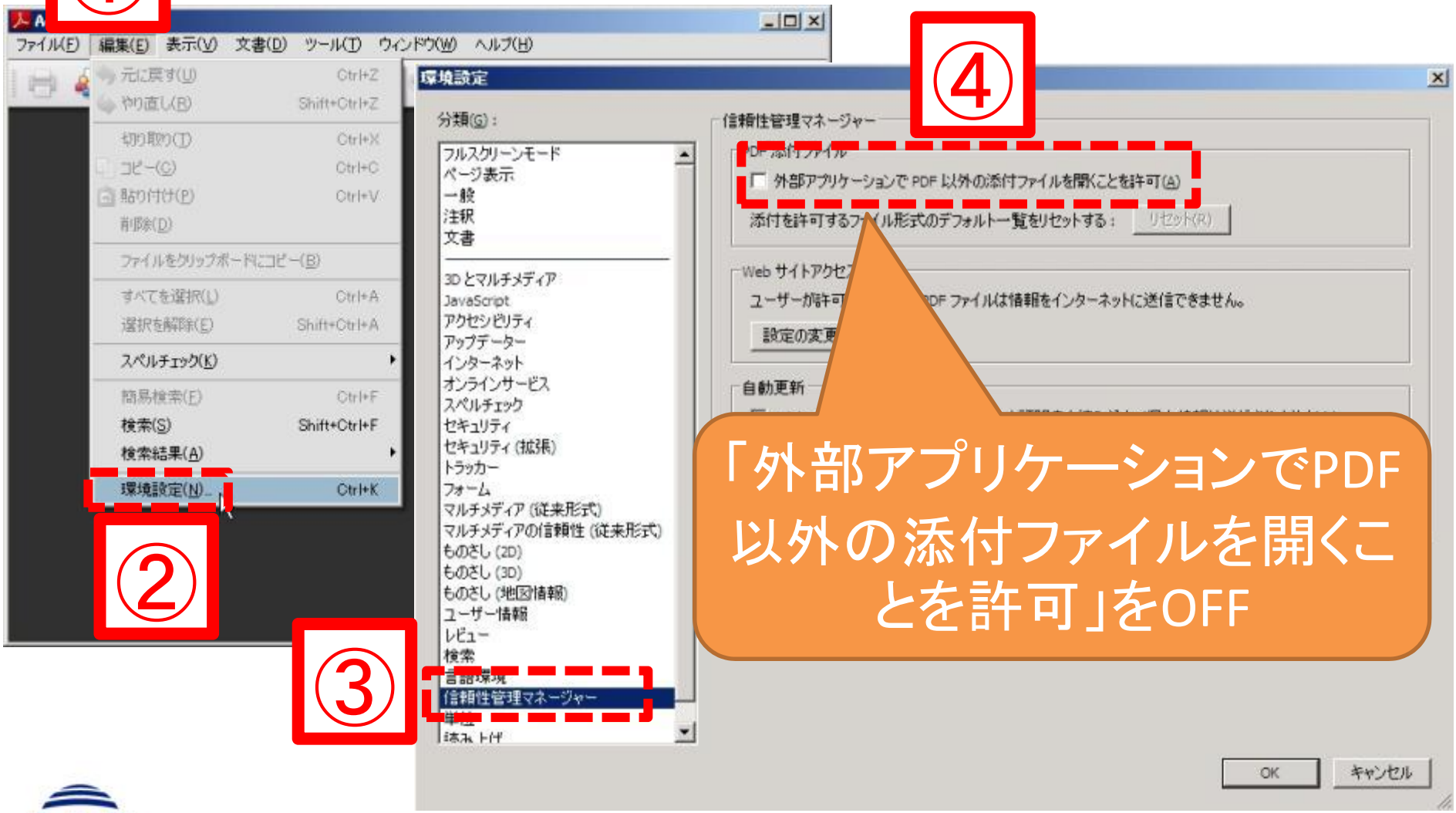
- 細かいアプリの設定を決めるところ　普段はいじる必要はない
- まれに古い（出来が悪い？）アプリがEMETにひっかかってしまう
- AutoCAD 2002やVMWare Server 1.xの管理コンソール等

参考情報：Adobe Reader設定

Acrobat JavaScriptを無効化

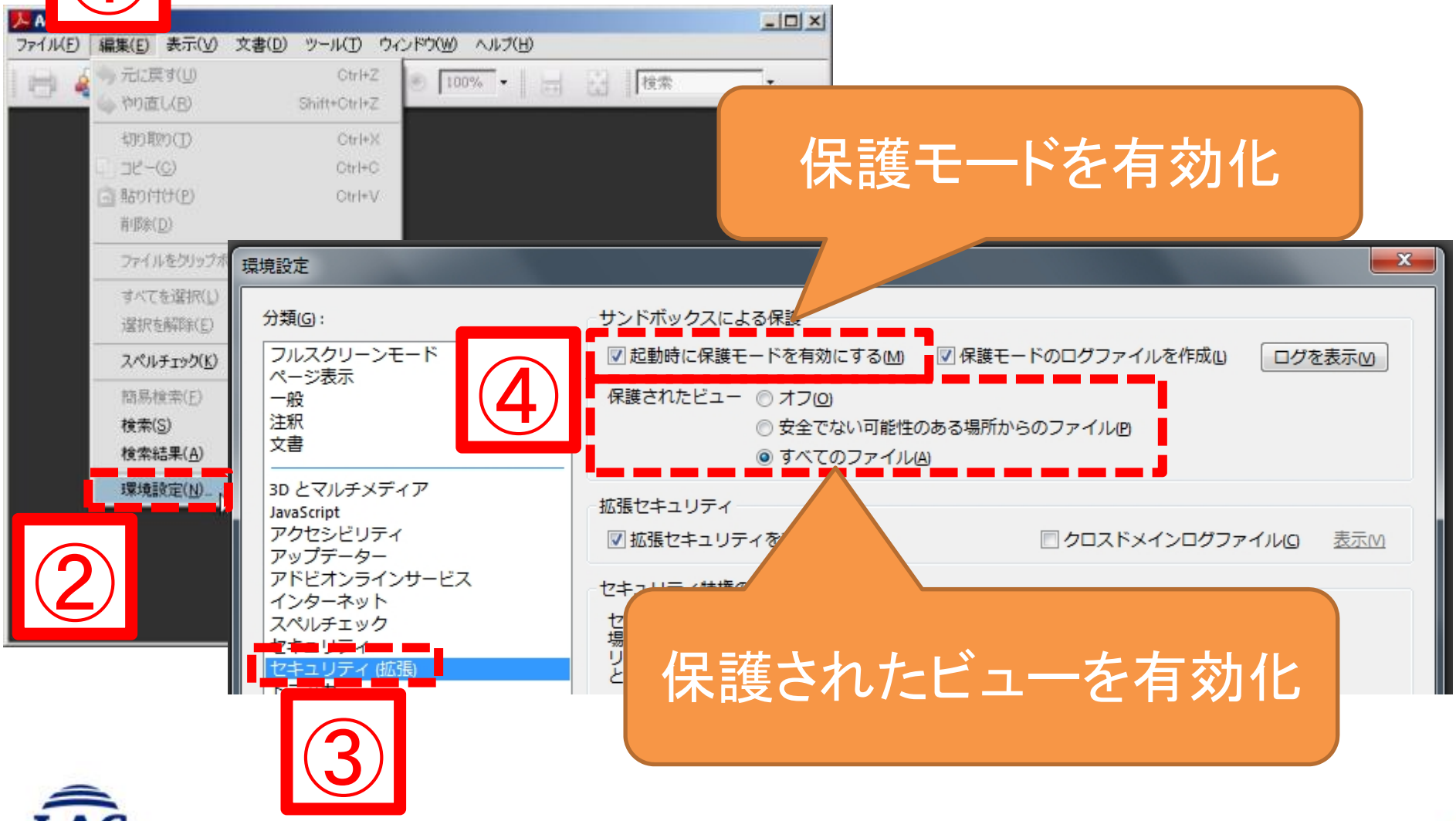
参考情報：Adobe Reader設定

① 外部アプリケーションの起動をさせない



参考情報：Adobe Reader設定

①「保護モード」「保護されたビュー」を使用する



まとめ

経営者の理解を得る

セキュリティ対策は落とし所が重要

人財と情報が明暗を分ける
（道具が同じなら使い方次第）


JSOC
JSOC
JSOC (Japan Security Operation Center)
ありがとうございました
JSOC
Japan
Security
Operation
Center