JPCERT CC®

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

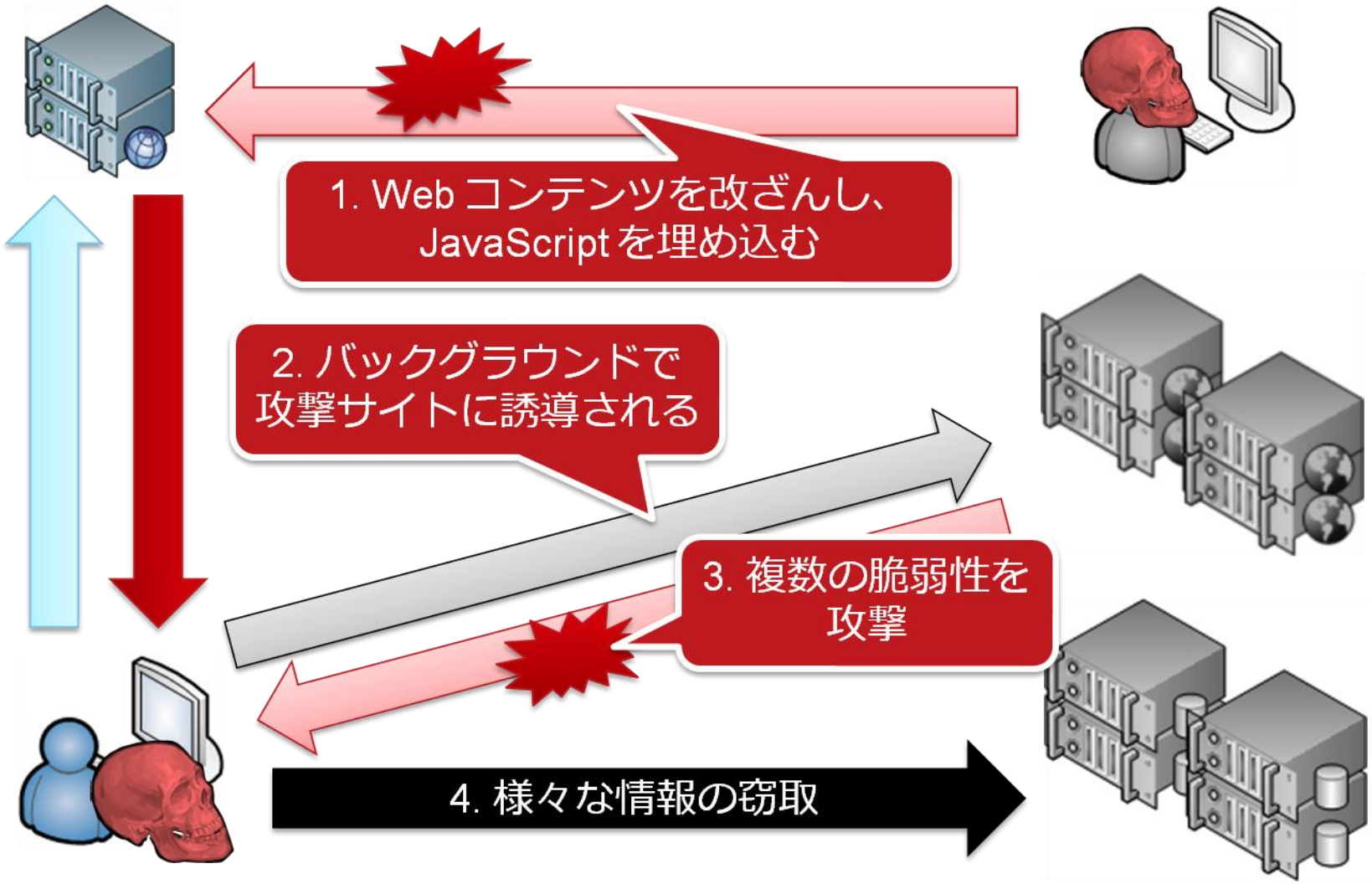
前提

- 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:d27cdb6e-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                                    097
<param name="quality" value="hig
<param name="FlashVars" value="c                                    9CF
%3BGF72%3B95944454G762865EGH" />
<param name="bgcolor" value="#ffffff" />
<param name="wmode" value="opaque" />
<embed src="http://[redacted]banner.php?sid=4641B7AD85B52C037FB31DA33484
quality="high" bgcolor="#ffffff" name="EITest" FlashVars="css=2&id=hkpcxo
%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

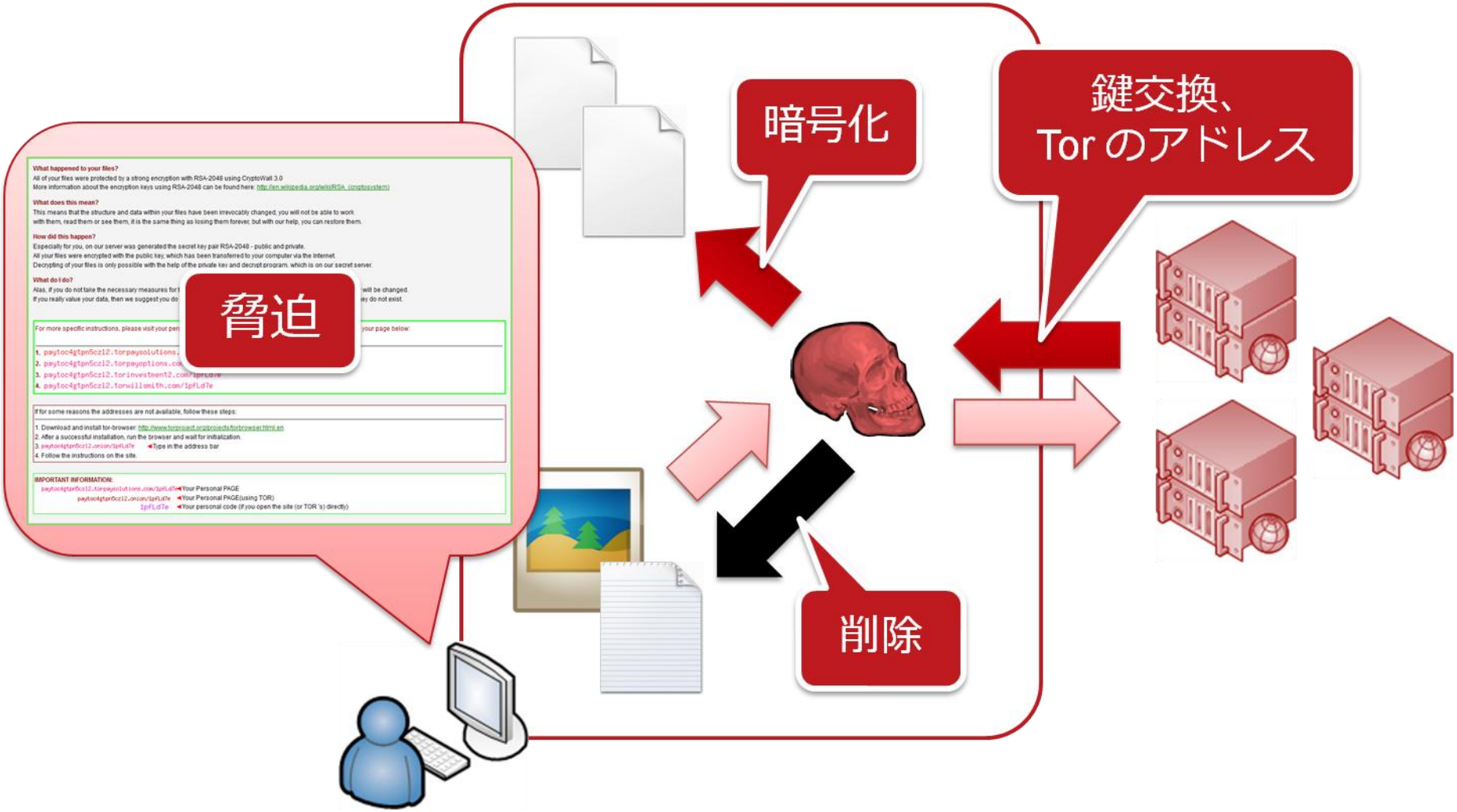
ランサムウェア

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

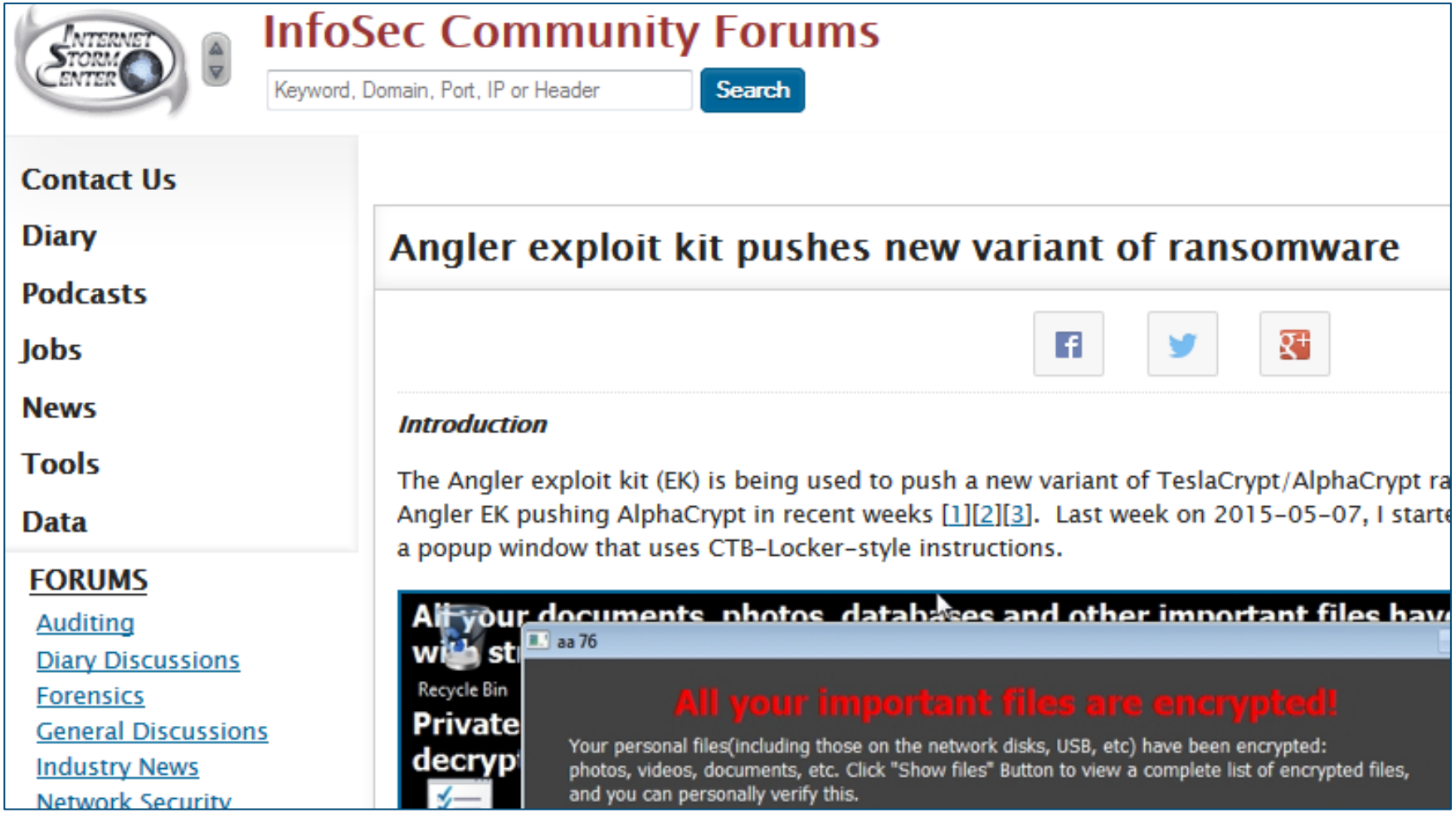
http://blog.trendmicro.co.jp/archives/8801
http://blog.trendmicro.co.jp/archives/11378

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



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

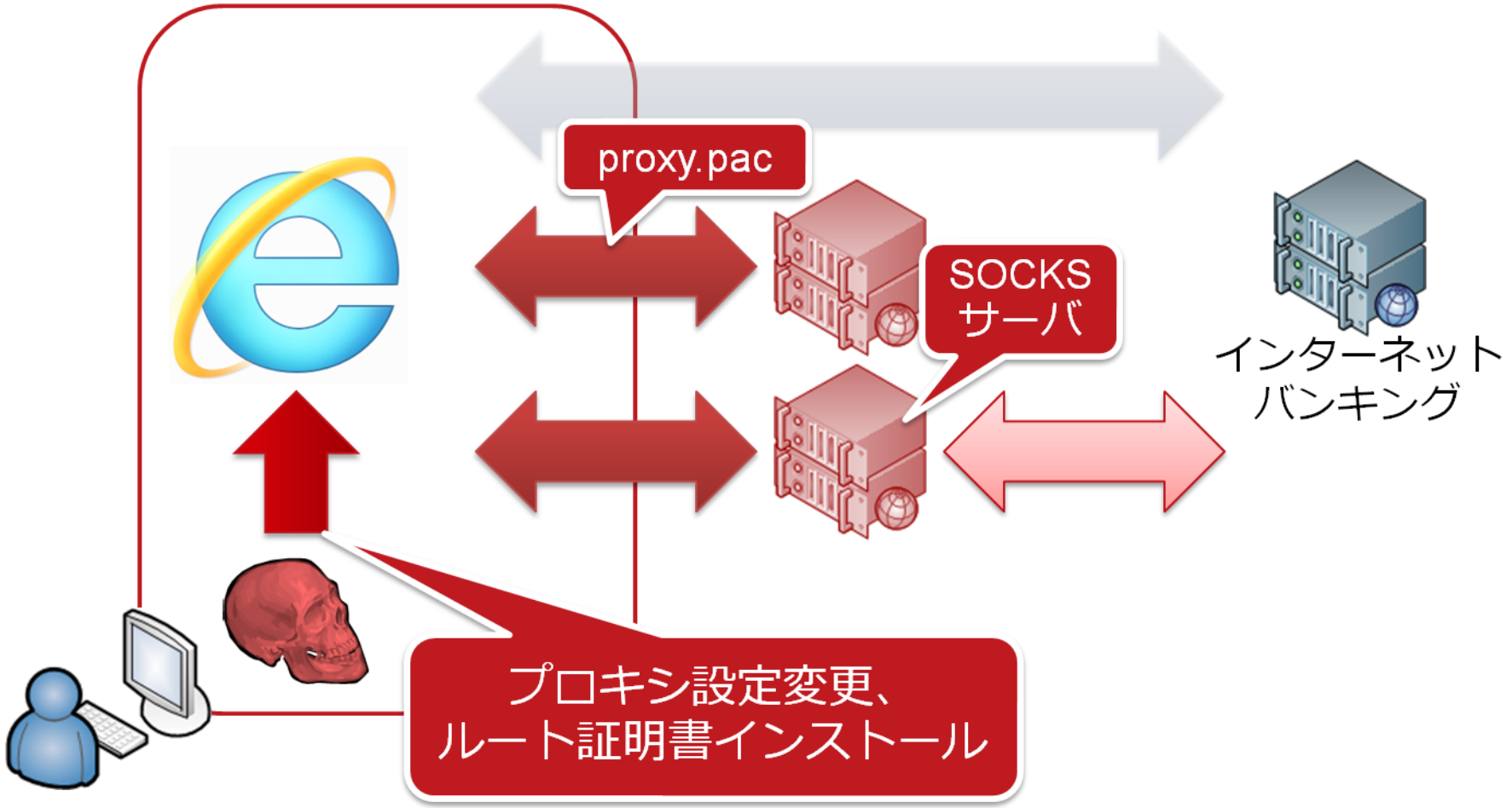
現在日本で見かけるバンキングトロイ

- ZeuS, Citadel, Gameover の時代は終焉

Vawtrak	Dyre	Tsukuba
Tinba	Dridex	Chthonic

proxy.pac を用いる手法

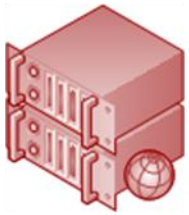
- 受信データの書き換えを中間者攻撃で行う
  - —Internet Explorer、Chrome、Firefox など



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
        }
```

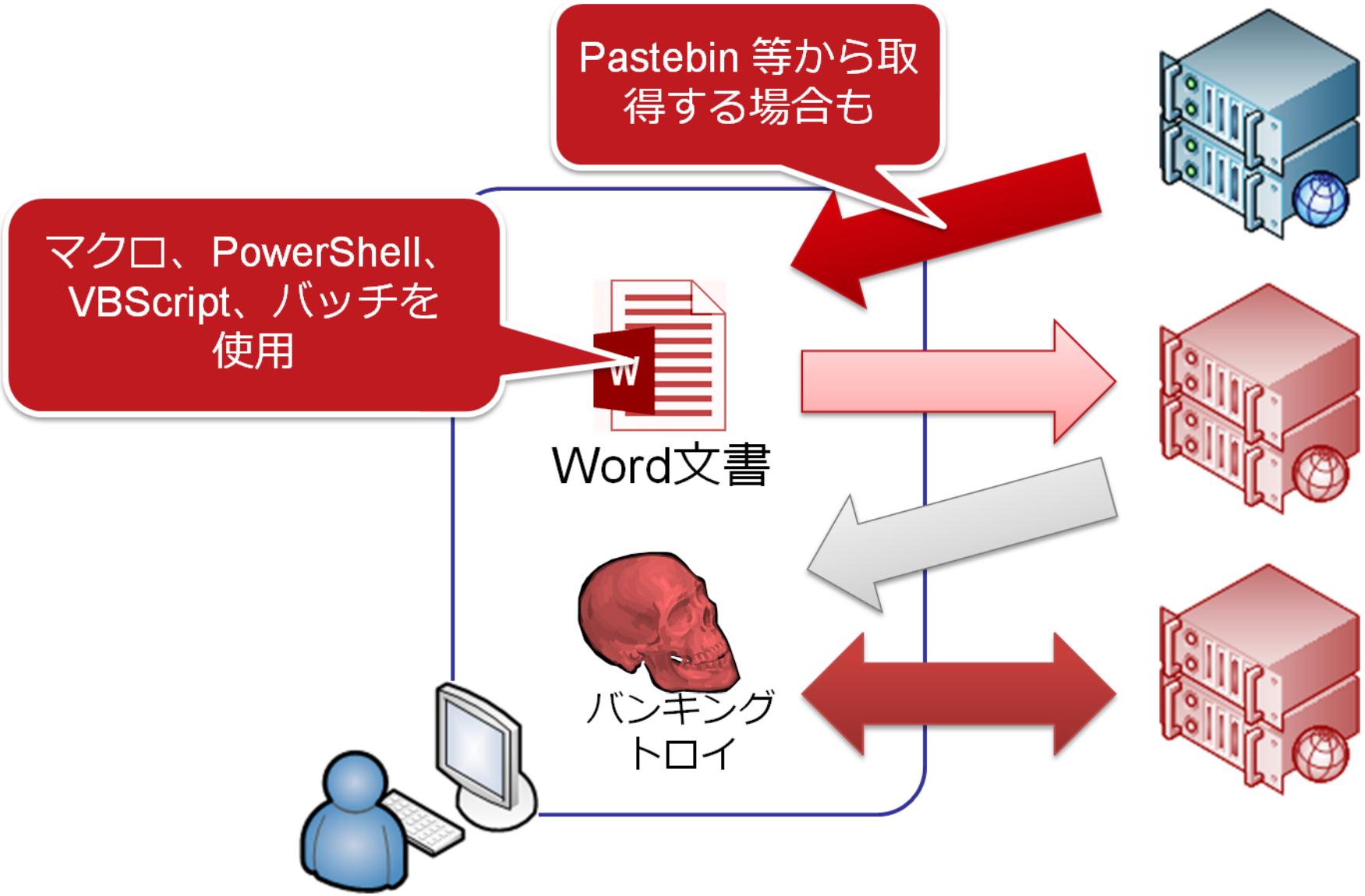
30以上のドメイン名



インターネット
バンキング

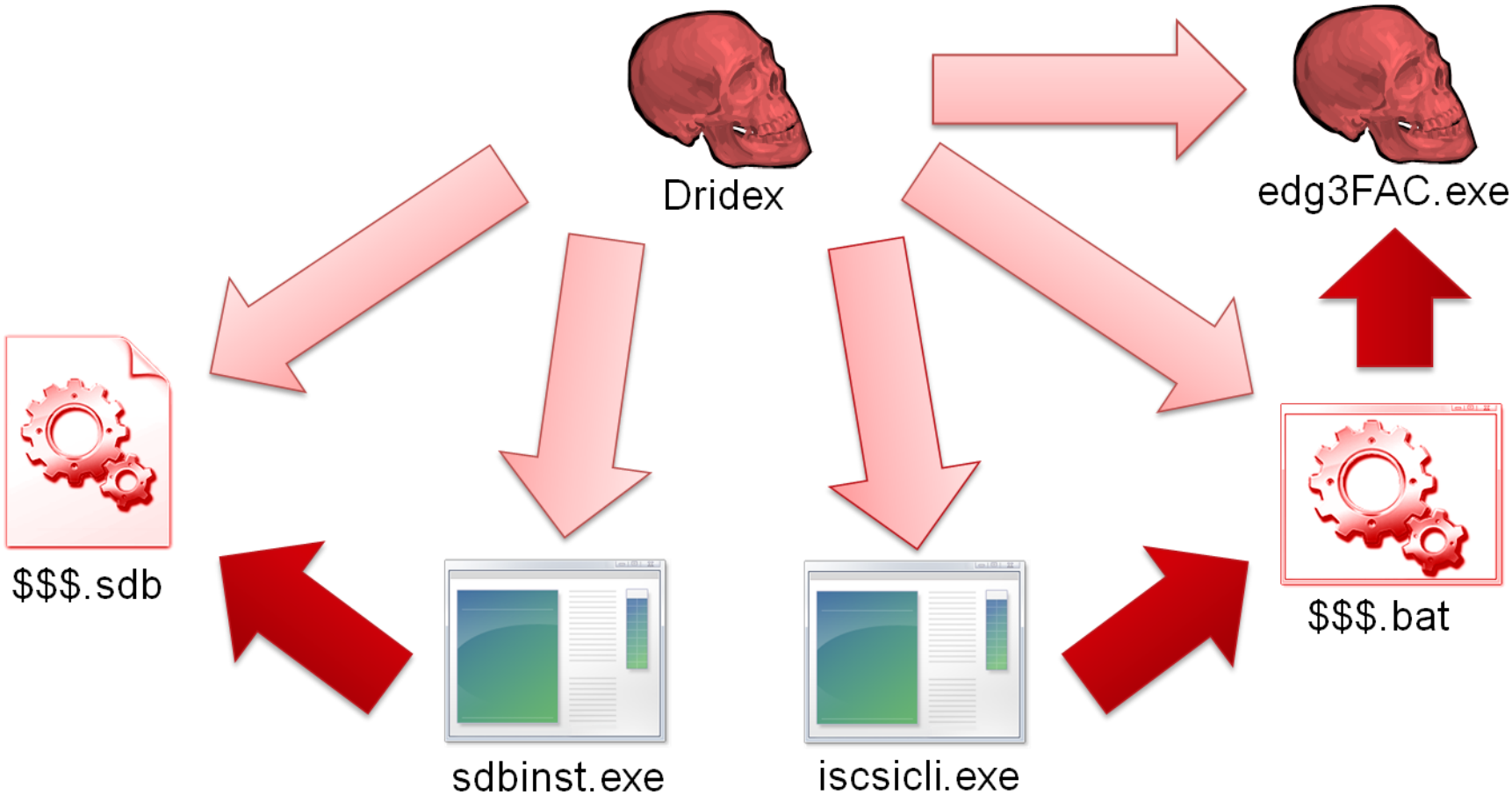
インストールされたルート証明書で検証可能な
サーバ証明書を使った暗号化通信

マクロを用いるダウンローダの感染経路



UAC 回避

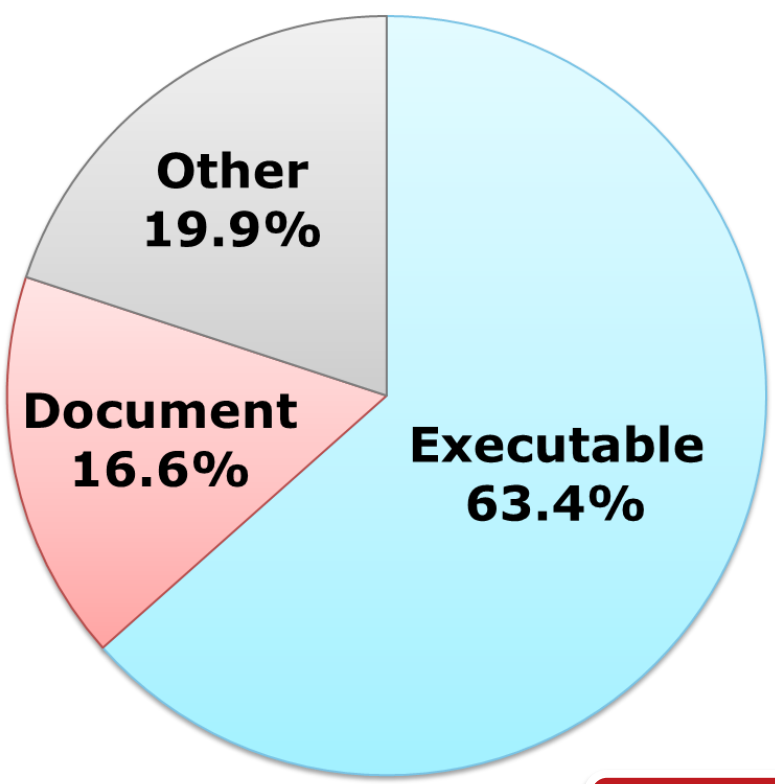
- Dridex, Vawtrak のダウンローダなどが使用
  - http://www.jpcert.or.jp/magazine/acreport-uac-bypass.html

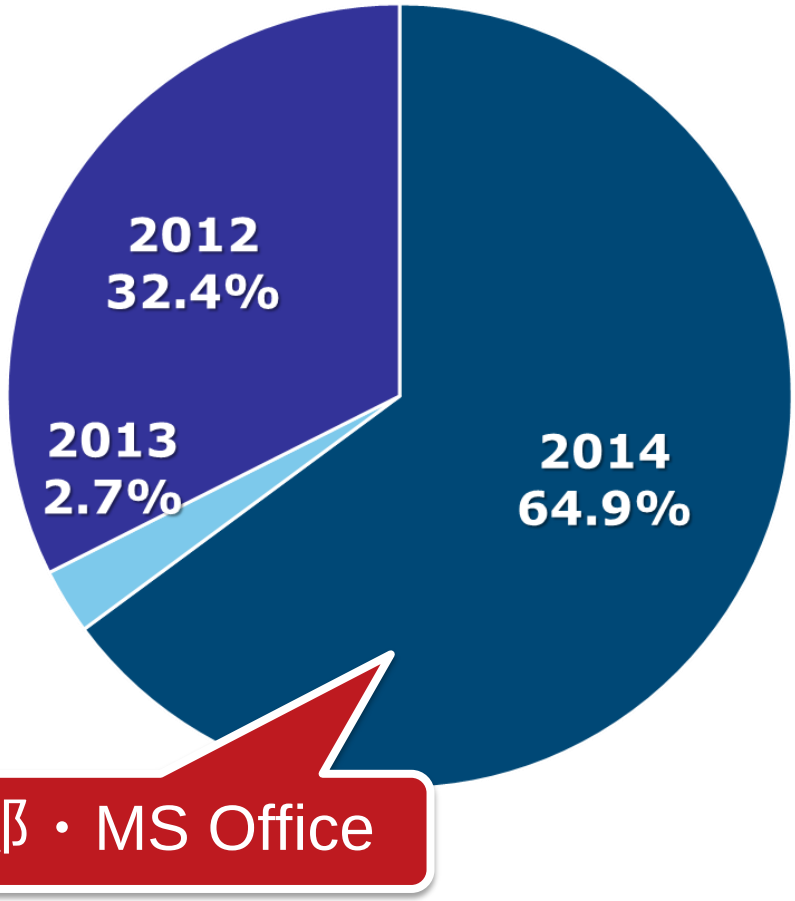


標的型攻撃

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





傾向分析: アイコン偽装

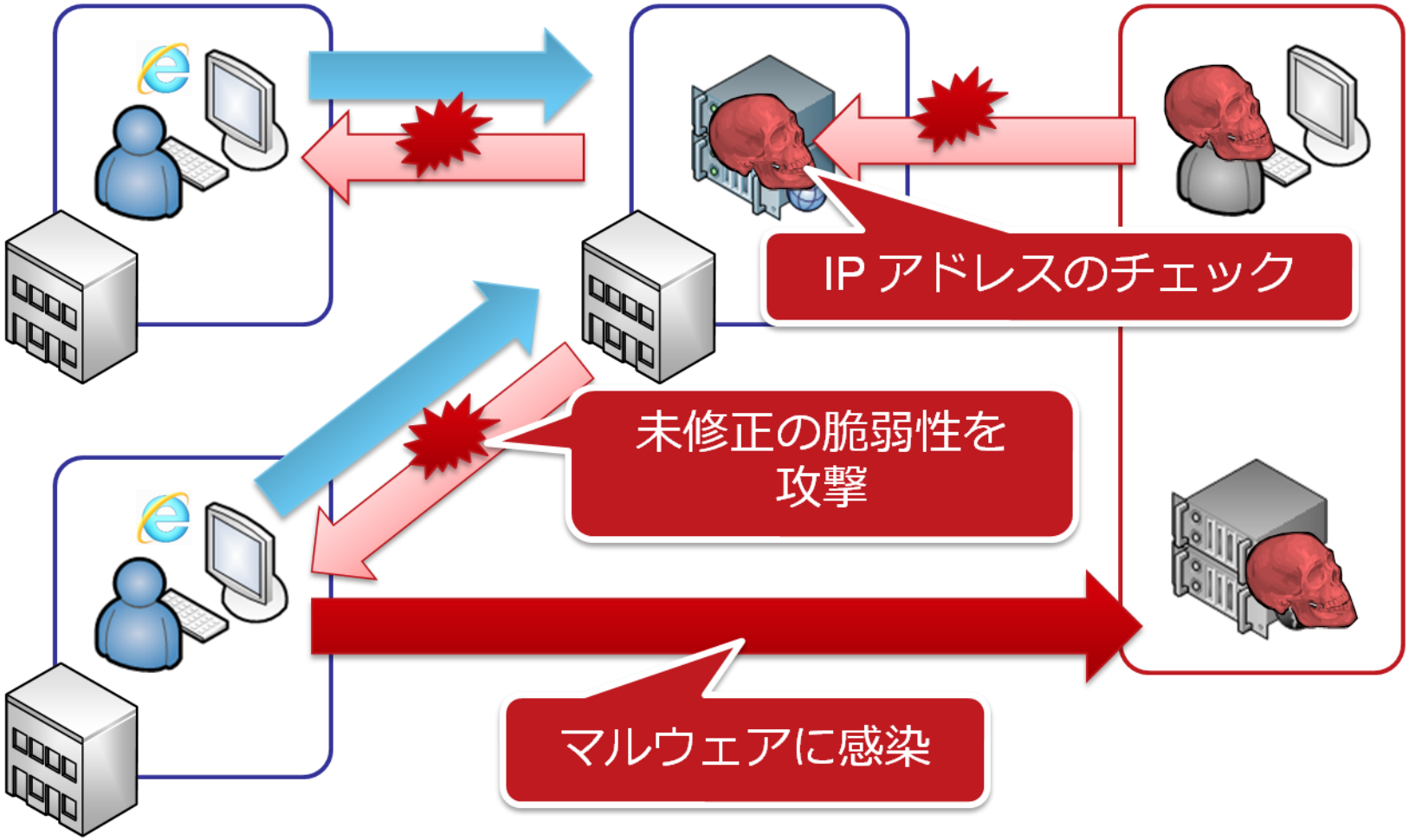
- 拡張子偽装と組み合わせて使用
  —正規アイコンからフリー素材まで様々

より高度な標的型攻撃

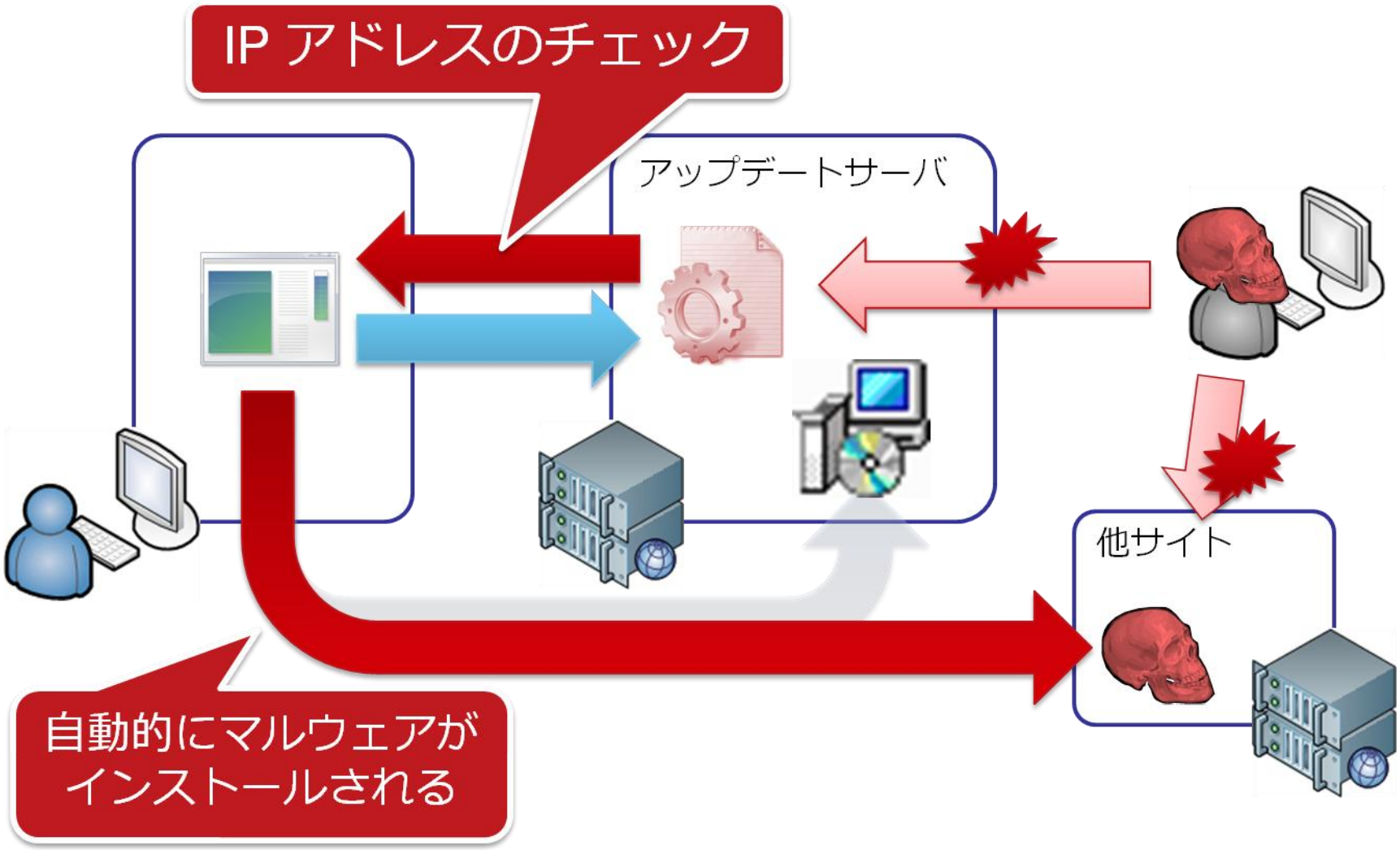
http://www.lac.co.jp/security/alert/2013/10/09_alert_01.html

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

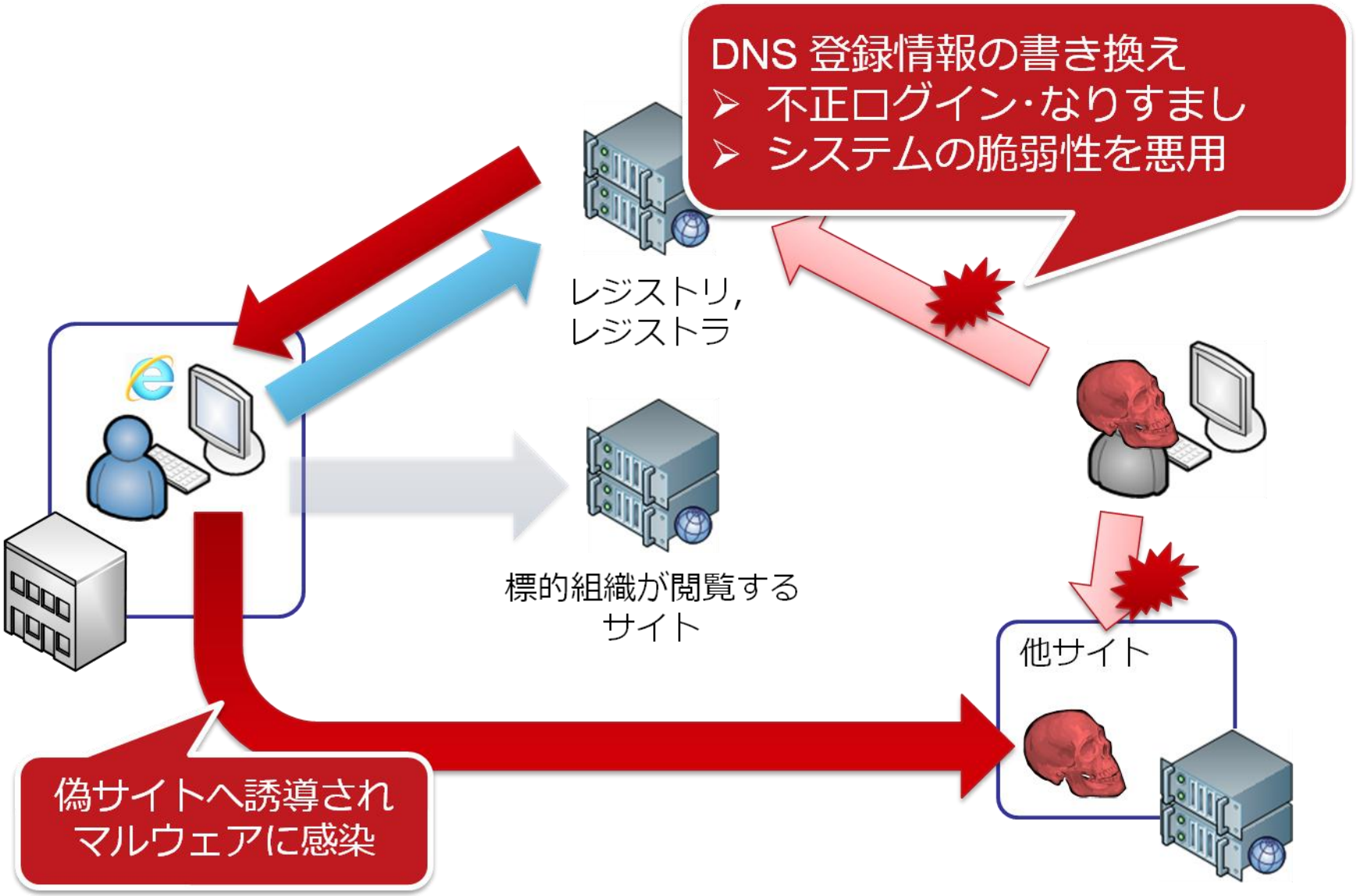
事例: Drive-by-Download 型



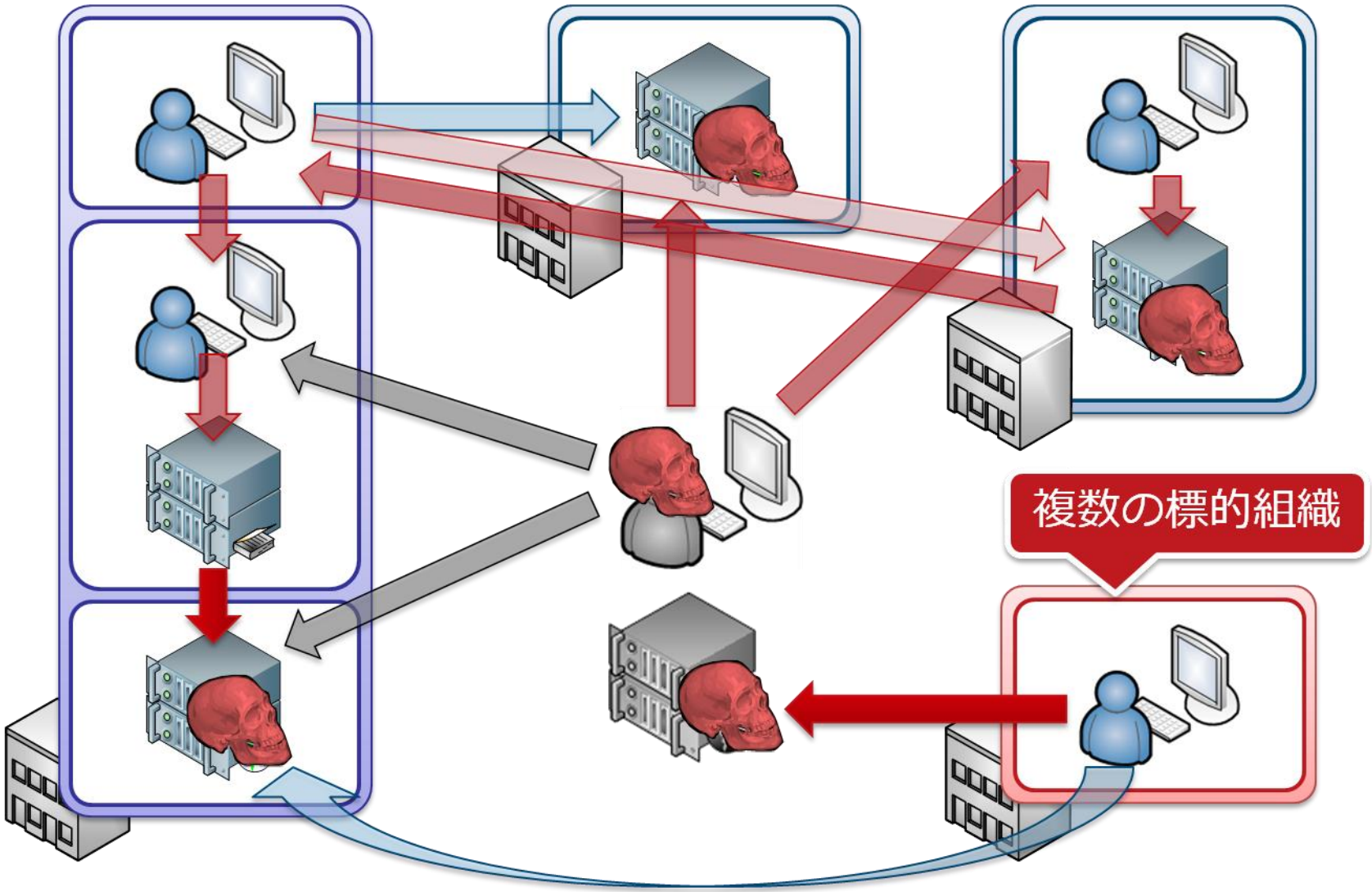
事例: 自動アップデート機能の悪用



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

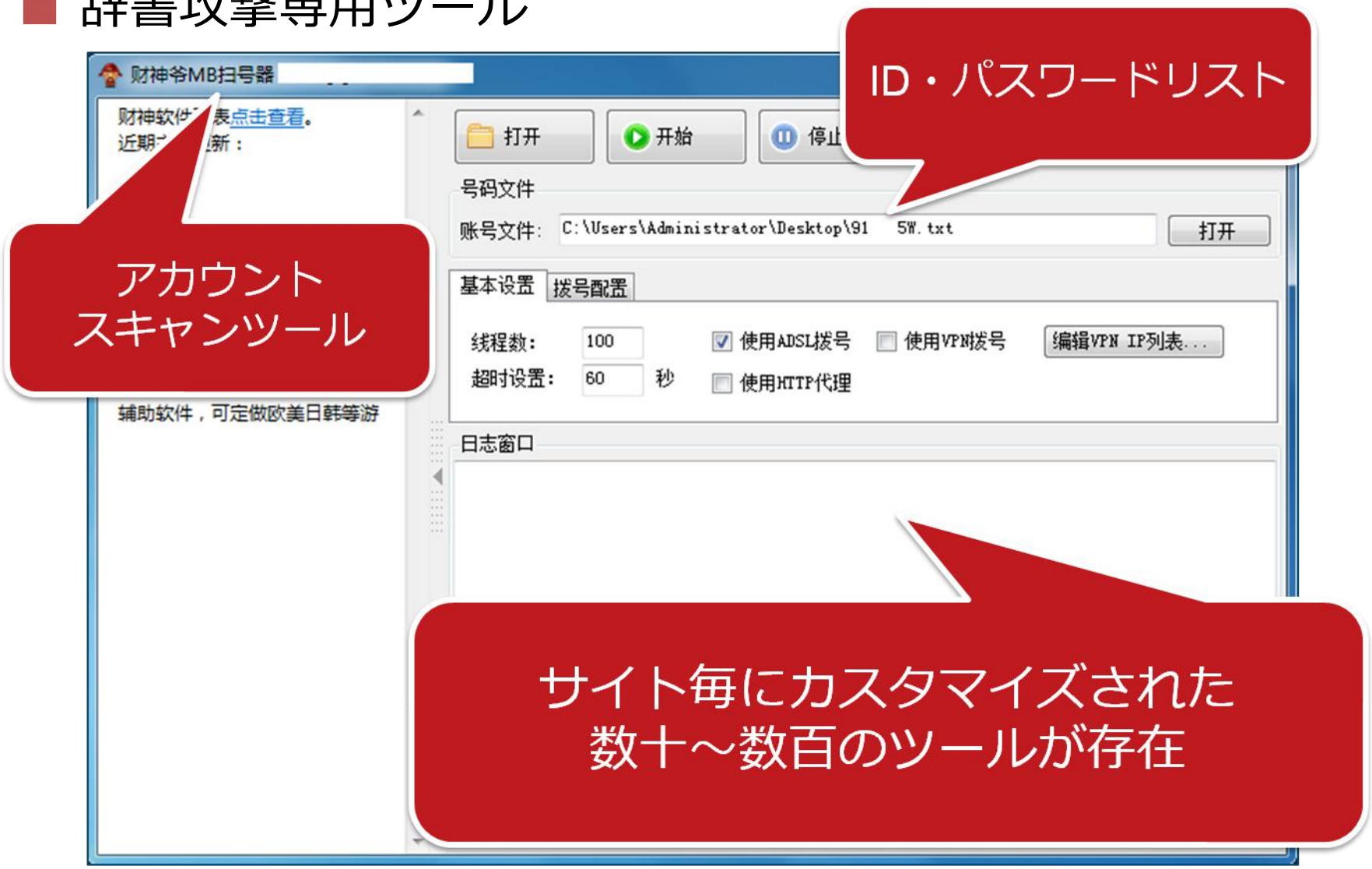
ツール系

- 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）

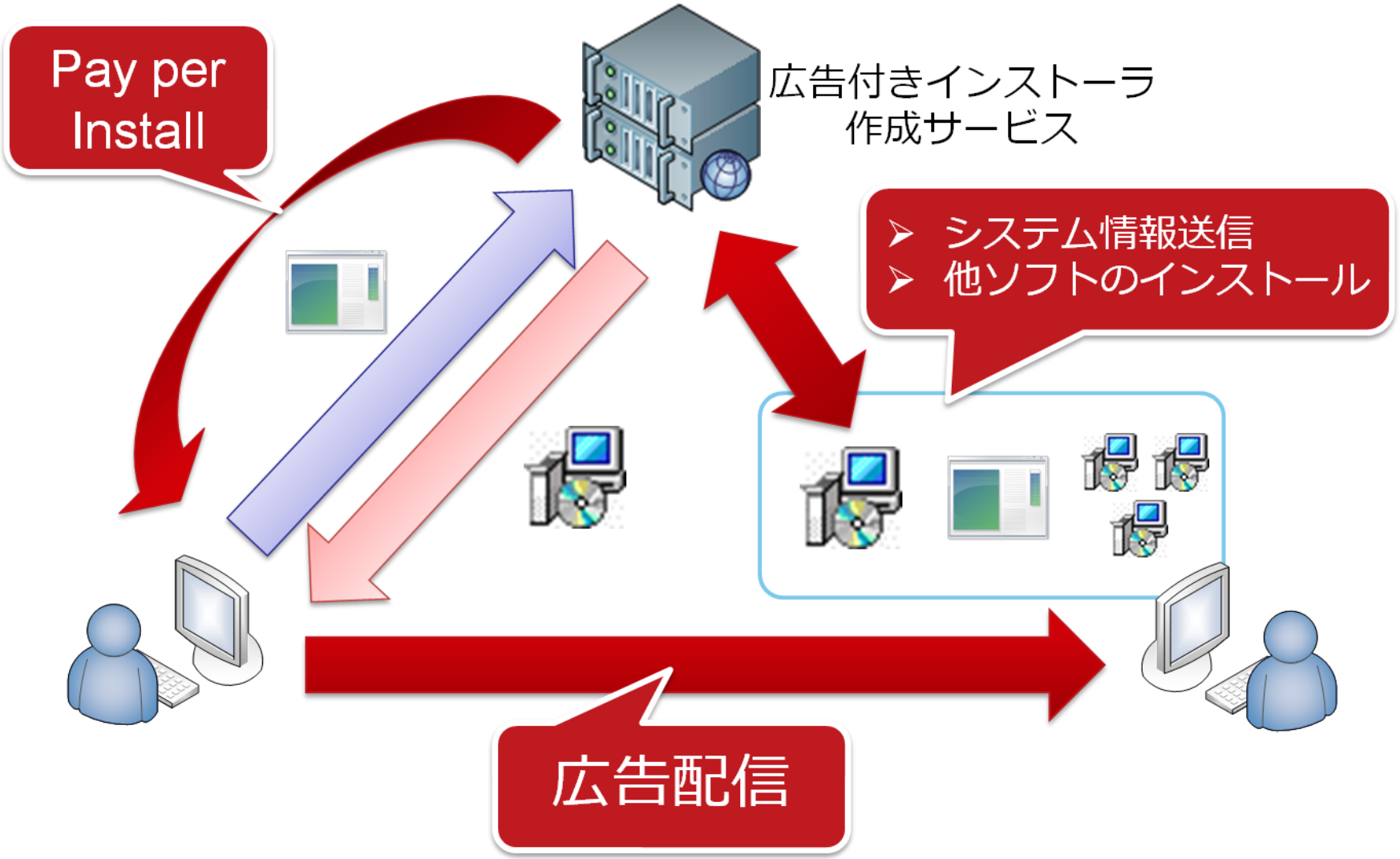
おまけ

パスワードリスト攻撃ツール

- 辞書攻撃専用ツール



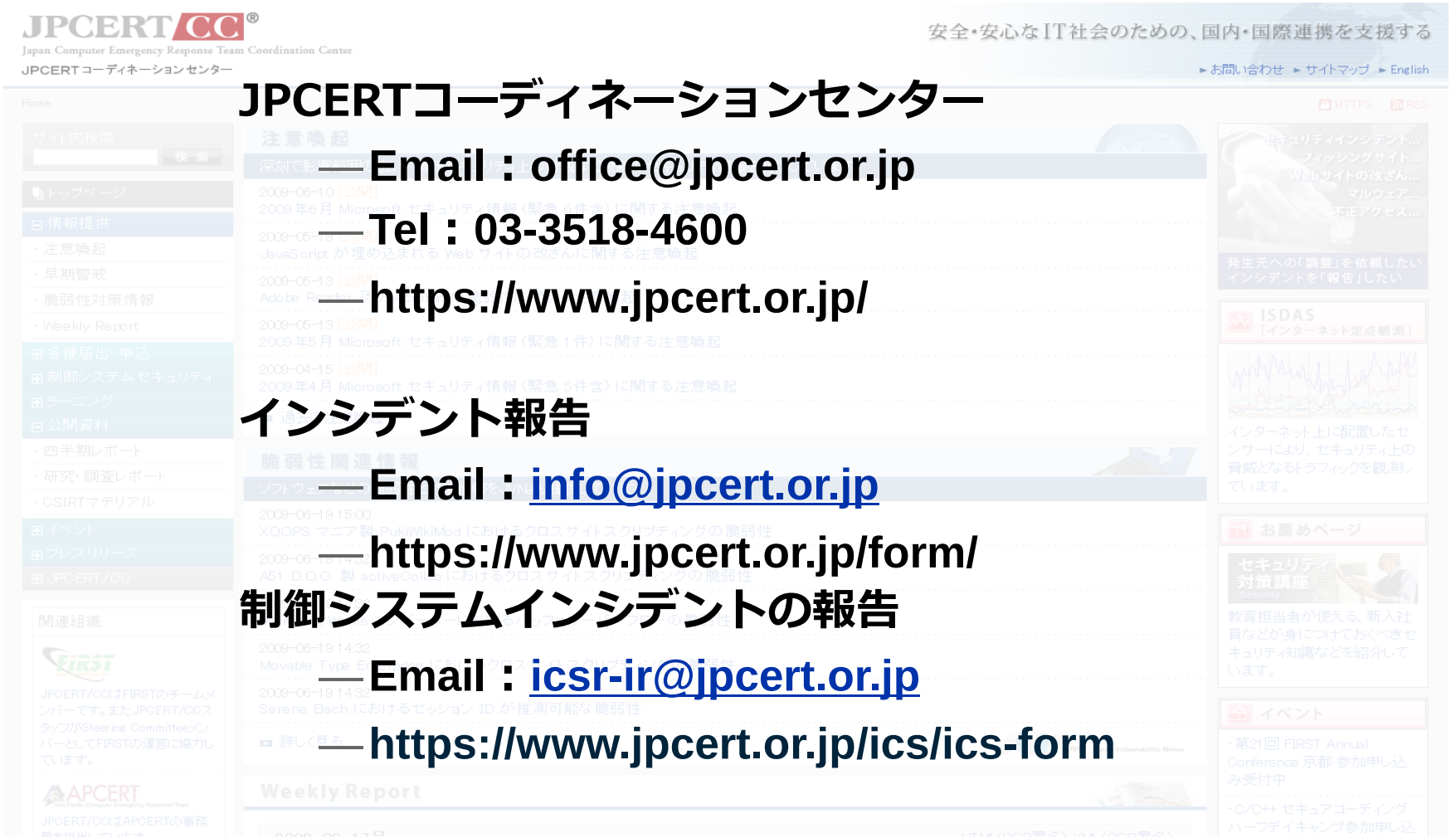
アドウェア



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

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