Network Security Forum 2004

【A-14】スペシャルパネルディスカッション

増大するネットワーク脅威の傾向と対策

株式会社ラック JSOC 西本逸郎
itsuro@lac.co.jp
http://www.lac.co.jp/security/

スピーカ

西本（にしもと） 逸郎（いつろう）

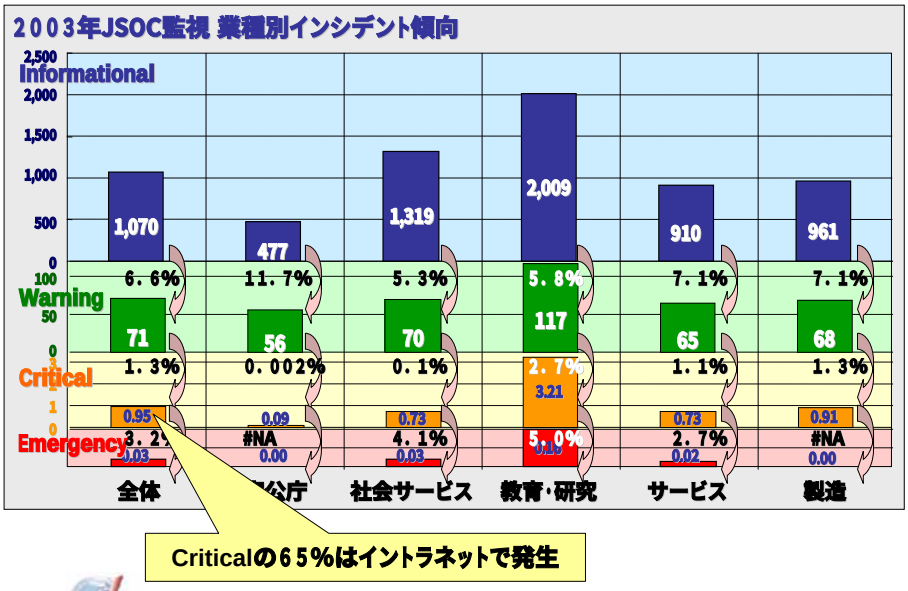
昭和33年	福岡県生まれ
昭和59年3月	熊本大学工学部土木工学科中退
昭和59年4月	情報技術開発株式会社入社
昭和61年10月	株式会社ラック入社　一貫して通信系ソフトウェアやミドルウェアの開発に従事。

その後、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（Windows POS）を世界に先駆け開発・実践投入。堅牢なシステムを如何に作って維持していくかをテーマにセキュリティ対策という観点で邁進中。

情報セキュリティ対策をテーマに展覧会などで講演会や専門雑誌への執筆を実施

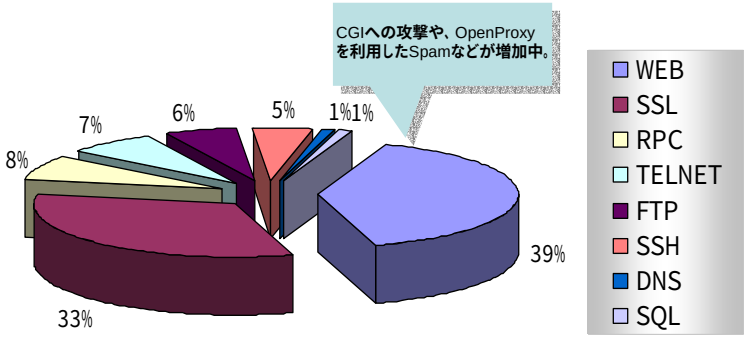
株式会社ラック JSOC事業本部 取締役本部長
特定非営利活動法人 日本ネットワークセキュリティ協会 理事
熊本大学大学院自然科学研究科

昨年のインシデント統計から



今年の傾向（所謂ハッカー/ポート別）

集計対象：2004 / 01 ～ 2004 / 09
（ワームを除く）

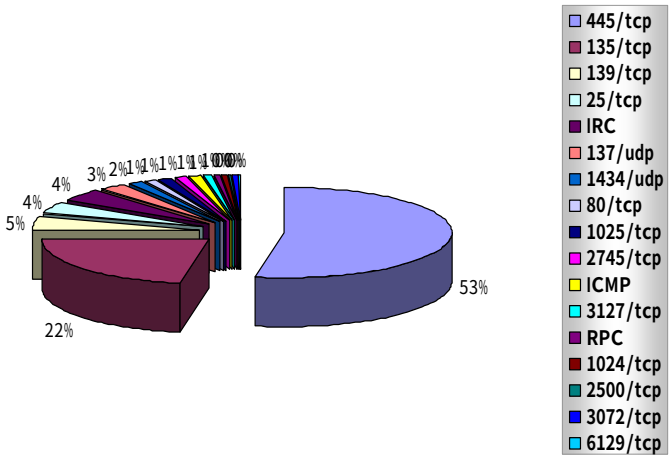


※本統計は、攻撃通信及び攻撃対象からのレスポンス通信を解析し、攻撃が成功したと判断できるインシデントの統計情報となります。

※ JSOC集計

今年の傾向（ワーム系内部持ち込み/ポート別）

集計対象: 2004 / 01 ～ 2004 / 09



※ JSOC集計

ポート別 推測ワーム

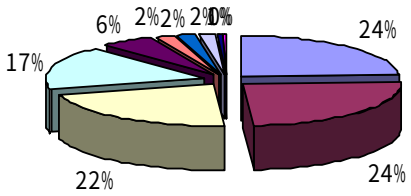
Port	Worm
445/tcp	Gaobot, Sasser
135/tcp	Blaster, Welchia
139/tcp	Deloder
25/tcp	Mydoom
IRC	Gaobot, Korgo
137/udp	Bugbear
1434/udp	Slammer
80/tcp	Welcha
1025/tcp	Keco
2745/tcp	Beagle
ICMP	Welchia
3127/tcp	Welchia, Mydoom
RPC	
1024/tcp	Randex
2500/tcp	
3072/tcp	
6129/tcp	Mockbot

※検知デバイスはファイアウォール及びIDS

※ JSOC集計

業界別インシデント発生状況

集計対象: 2004 / 01 ～ 2004 / 09
(**ワームを含む**全インシデント)



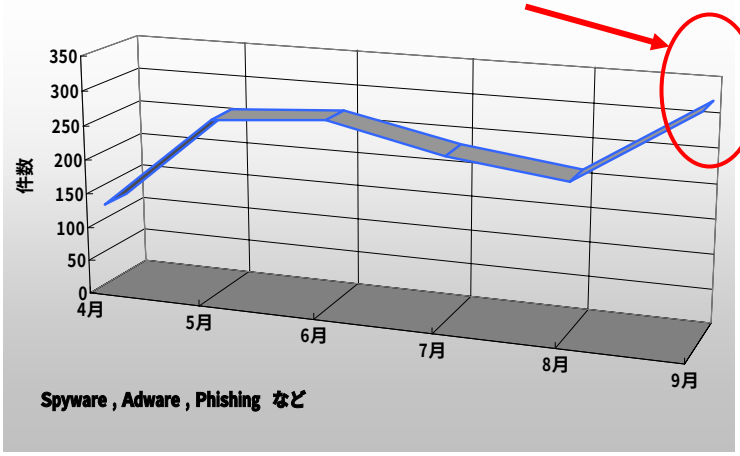
- 学術研究機関
- 情報･通信業
- 製造
- 卸売･小売
- メディア
- サービス
- 官公庁
- インフラ(電気･ガス)
- 金融
- 運輸

※ JSOC集計

受動的攻撃の検知件数

集計対象 2004 / 04 ～ 2004 / 09

MS04-028
Microsoft GDI+ Malformed JPEG Buffer Overflow Vulnerability



※企業内から悪意のあるプログラムなどが設置されたWebサイトにアクセスした件数を集計

※ JSOC集計

Attack View

今年の傾向

クリティカル件数は3～4件/月に増加
（昨年は1件/月）

内イントラネットでの発生は90%以上！（昨年は65%）

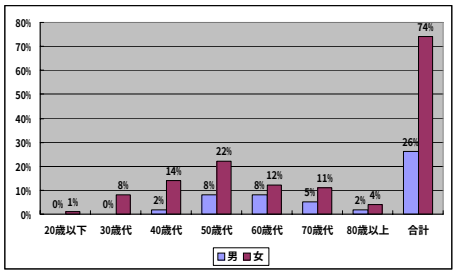
イントラネットでのインシデント件数が相対的増大した

イントラネットを監視対象とする顧客が増えてきた

いわゆる「おれおれ詐欺」などの内容

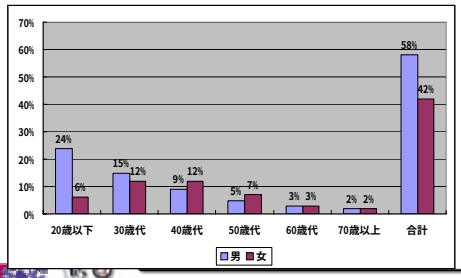
被害者の年齢 男女構成 (平成16年1月～8月)

いわゆるおれおれ詐欺

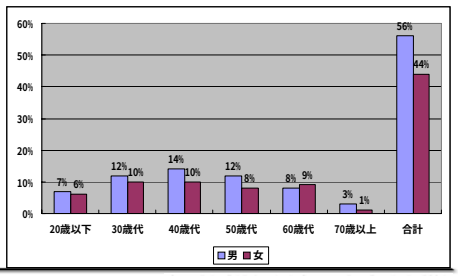


※警察庁 いわゆるオレオレ詐欺・架空請求詐欺の防犯対策を引用しグラフ化しました
http://www.npa.go.jp/sousa/souni2/oreorejoukyou16-8.pdf

架空請求詐欺



融資保証金詐欺



これまでのネットワークセキュリティ

ハッカーによる WEB改ざん → 省庁WEB改ざん事件

新型コンピュータウイルス による、ダウン → 第一次新型ウイルス事件 Codered、NIMDA
→ 第二次新型ウイルス事件 Blaster、Welchia

個人情報漏洩に よる、ダメージ → 個人情報保護法施行

スパム
フィッシング
新型トロイ
？？？

2000年～2001年
第一次セキュリティブーム
① セキュリティ検査と対策
② サーバ要塞化と維持
③ IDS監視 など

2003年～2004年
第二次セキュリティブーム
① パッチ管理・検疫ネット
② IPS、ウイルス対策
③ イントラネット対策 など

イベントドリブン
対症療法的
場当たり的

ありがとうございました

お問い合わせ ： itsuro@lac.co.jp

Question 1：

AntiVirusソフトだけでは何故だめなのか？

定義ファイル更新は何故遅れるのか？

1日ではない⇒ 2時間！！
それより拡散が早いんだ！
メール型は大丈夫だったが、、、ゾンビPCで最初から大量に、、
定義ファイルなしで、、インテリジェンスに、、、裏をかかれる、、う~ん
ワーム（ネットワークウイルス） ファイルI/Oの発生があるか？
EX. SQL Slammer
今年はメール型（MYDOOM,NETSKY等）＋ウイルスからDoS発生も
パーソナルファイアウォール ⇒ MSさんでは全員キャンペーンしていた
どのメーカが一番早い！ 私も聞きたい！ ○勝×敗の世界
NetSky.Qとかでは結構被害がでた、、⇒ 予定がアナウンスされないか？
　メールサーバを止めているので読めない(ToT) ⇒ FAX コスト、、、
Rapidリリースもやっている（最終評価（QA）前で、、おいくら？）S
基本はWeekly、緊急はDailyでも、、Mさん
ワームも巧妙化、、高級言語で開発 多機能、亜種との区別も難しい

Question 2：

最近よく言われているフィッシングって？

おれおれ詐欺に似ている、心理的無防備なところにつけ込む
知識差、活用技術が不足している？
1⇒N⇒N　ウイルスの場合
1⇒N　大半はSPAMメールで発生
SPAMをブロックとURLでブロックの2つの対策がある
システムでの防御は限界があるのでは？

スパイウェアとかアドウェアの脅威って？

アダルトサイトのマーケティング
操作・どういったページを見ているのか？・行動を知りたい　と思う人たちがいる
倫理観のかけたマーケティング
トロイの木馬との違い　ユーザの同意を得るかどうか？
本当にユーザは意識（同意）しているのだろうか?
　数千存在している　万人にとって悪いことではない
　トラブルになるケースもありそうだ、、、う~ん
　最近ユーザからの相談は増えている

Question 3：

IPSは使えるか？

9月にアンケートをとってみた（M社）
大企業（500名以上）が大半　　学校20%・通信20%・産業20%・地方公共20%
誤検出（フォールスポジティブ）の問題は解決できないだろう、、
有効な手段だ！ セグメンテーションが出来ていないケースも多い ⇒ 通信要件も把握できな
誤検出の対策も立てられないのでは？ 運用？ シグネチャのアップデート？

DMZ：10%

イントラネット：75%

WAN境界：15%

ホストサイド：
　大事なサーバに入れられるか？

S社では、、
① ビヘイビヤブロッキング（HIPS：ホストサイド）
② アノマリ検出
③ プロトコルアノマリ
④ EXPLOITブロック（ホストサイド）
あと、ウイルススロットル?統計的アノマリ　接続を絞る

Question 4：

Windows XP SP2は救世主か？
はたまた、トラブルメーカか？

バッファオーバランは防げるか？チップは？
フォールスポジティブ
そもそもOSは機能が多すぎるのでは？
S社にとっては、、
MSさんの努力している、、、S社の株価対策も考慮を！
　やさしくPFWが使えるのは良い、、ENDユーザとしてはうれしい
　ところもある
パーソナルFWが売れない！（USで売れていた）
セキュリティセンターに認識しない、製品もある。
POPアップブロッカは困る、、
SP2に対応していない3rdベンダ製品はまだ多い、お客さんから
要求される。Sierとしてはお金にならない仕事が増えて困る？？

Question 5：

その他有効な（気になる）対策は？

どんなもの？
効果？
費用？

リテラシの低いユーザからはPC？
NTの開発者カトラーさん　VMSの開発者
もともとセキュリティのことは考えていたはず、
ネックはWin16 ⇒ やっぱり営業からの圧力が問題だったか？
COEマシン
PCの管理は誰がやるべきか？
管理者権限　unixとの差　suはないかな？

Question 6：

Googleデスクトップサーチ

どこまで信用できるか？
現状の機能ではそこまで脅威ではないのでは？

ウイルスはOSの根本的な問題をついているのでは？

権限の問題　管理の問題　権限昇格のExploitは別
ユーザ権限では出来る範囲は少ない。

HDを使えないようにする♪

Question 7：

検疫ネットワークってどうよ？

導入のしやすさ？
効果？（何を検疫？）
費用？

Question 8：

DoSってどう考えれば良いのでしょう？

Question 9：

インターネットでの脅威は増大しているのか？

Question 10：

今後ハッカーの攻撃やコンピュータウイルスはなくなるのか？