マルウェア対策の現状と悩み

JSOC JAPAN SECURITY OPERATION CENTER

2012年10月31日

川口　洋, CISSP
株式会社ラック
チーフエバンジェリスト
hiroshi.kawaguchi @ lac.co.jp

自己紹介

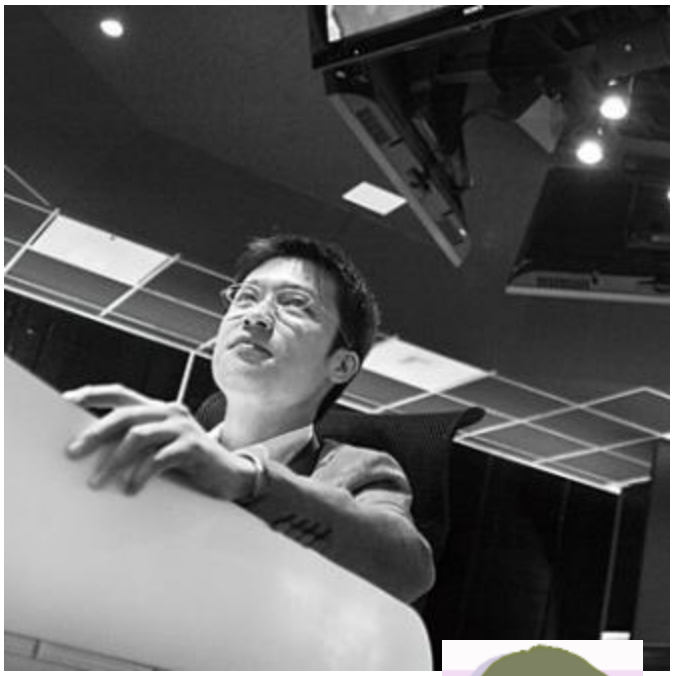
川口　洋(かわぐち　ひろし),CISSP

株式会社ラック
チーフエバンジェリスト 兼 担当部長
ISOG-J 技術WG リーダ
http://www.lac.co.jp/education/instructor/index.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。

チーフエバンジェリストとして、セキュリティオペレーションに関する研究、ITインフラのリスクに関する情報提供、啓発活動を行っている。Black Hat Japan、PacSec、Internet Week、情報セキュリティEXPO、サイバーテロ対策協議会などで講演し、安全なITネットワークの実現を目指して日夜奮闘中。

2010年～2011年、セキュリティ＆プログラミングキャンプの講師として未来ある若者の指導にあたる。2012年、最高の「守る」技術を持つトップエンジニアを発掘・顕彰する技術競技会「Hardening」のスタッフとしても参加し、ITシステム運用に関わる全ての人の能力向上のための活動も行っている。



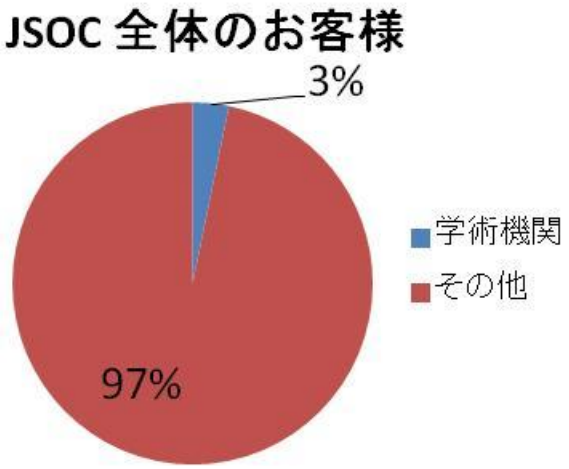
川口洋のセキュリティ・プライベート・アイズ（@IT）連載中
http://www.atmarkit.co.jp/fsecurity/index/index_kawaguchi.html

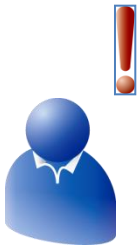
ラック入社のきっかけ

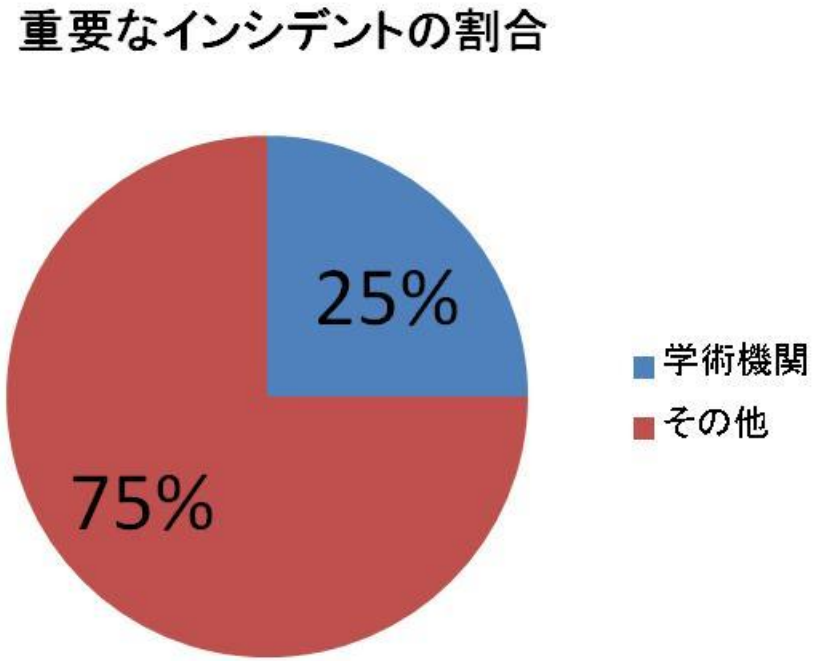
- 大学院時代
- システム管理者
- 不正侵入を発見
- 2000年当時、誰もセキュリティを知らない
- システム管理者はセキュリティで夜帰れない
- なんとかしなきゃ

マルウェアの感染状況

調査期間: 2012/1/1 ～ 2012/06/30







対策の現状

- FWとウイルス対策ソフトはかなり導入されている

- アップデートすることができない
- いまだにWindowsXPとIE6

- 端末が多すぎる
- 社員が多すぎる

ギャップ

海外（メーカ、研究者）

セキュリティリスク ＞ 可用性

まれに誤検知・誤遮断しても、*効率的*に対応できます
その問題は再起動したら解決します

日本

セキュリティリスク ＜ 可用性

誤検知・誤遮断する機能は使いたくない、無効化したい
再起動なんてできるわけない、やらずになんとかしたい

学術機関の難しさ

- グローバルIPアドレス
  - 「プライベートアドレスってどう使うんですか？」
- 専任の管理者
  - 「ちょいと片手間なんです」
- 毎年入れ替わる学生
  - 「え？セキュリティ？何すか、それ？」
- やたらと声が大きい先生
  - 「研究を阻害する気か？」
- Firewallが導入できない
  - 「通信はフラットに通すべきだ」
- 違法コピー、違法ダウンロード
  - 「それはP2P型アンチウイルスソフトです」

まとめ

敵の狙いを理解する
（狙われているところはどこか？弱いところはどこか？）

自分のシステムについて把握する
（できることとできないこと）

守る方にも戦略が必要
（モノが同じならヒトとジョウホウで差がでる）

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。

株式会社ラック
http://www.lac.co.jp