セキュリティ・リスクの真実

または、情報インフラリスクの真実

園田道夫
vp5m-snd at asahi-net.or.jp
http://www.asahi-net.or.jp/~vp5m-snd/sec/
http://d.hatena.ne.jp/sonodam/

自己紹介

- 1962年生まれ
- 2004年1月1日よりフリー
- 独立法人情報処理推進機構（IPA）脆弱性分析ラボ研究員
- SISS（日本セキュリティ情報流通協議会）監事
- NPO日本ネットワークセキュリティ協会研究員
- JNSAハニーポットWG、セキュリティスタジアムWGリーダー
- 技術者教育をテーマに、教育講座企画中
- セキュリティ夜話（http://www.asahi-net.or.jp/~vp5m-snd/sec/）
- 極楽せきゅあ日記（http://d.hatena.ne.jp/sonodam/）
- vp5m-snd at asahi-net.or.jp

IPインフラにかかる過剰な期待

便利で安い
IP電話

しかしますますIPインフラにリスクが集中する

IP電話が何をもたらすか？

要求される性能が
どんどん高度化する

トラフィックの増加

ますます障害に強くなけれ
ばサービスを継続できない

ますますダウンすることが許されない状況

コールサーバー、ルーターなど、
ハイポート使いまくりetc.

新たなサーバ、新たなリスク

安全便利
VPN

しかし別なリスクを背負い込むことになってしまっている

VPNが何をもたらすのか

中身が見えない

という重大なリスク

中身が見えないことは何が問題なのか？

見えないことは安全上良いことではないのか？

他にも･･･

- いろいろなところに使われているIPネットワーク
  - インターネット銀行
  - オンライン取引（株とか）
  - 住民基本台帳ネットワーク
  - 自動受付システムなどなど
  - そこらの端末などなど
- なにしろ安い。既存のOS上に作るのが安上がり＆IPインフラならば安上がり
  - http://www.soumu.go.jp/kokusai/html/chapter09.htm
- どうかすると勘定系とかにもIPが使われている

今、IPインフラに求められる性能・機能とは？

耐障害性

異常検知

追跡性

耐障害性	ワーム・ウイルスに強い
異常検知	ワーム・ウイルスを検知
追跡性	内部の有資格者の追跡

結局のところ、目下の最大のリスクは

ワーム・ウイルスが帯域を食い尽くしたり、サーバーを
使用不能にしてしまうリスクと、

内部の有資格者による不正なアクセス（内部犯行）

「ワーム・ウイルスの脅威」の真実

巷で言われているワーム・ウイルスのリスクは、ほんとうのところ

どういうリスクなのか？

事例を紐解いてみると

ネットを麻痺させたブラスター

ICMPであふれさせたウエルチ

SMTPサーバーを止めたNetSkyシリーズ

どうして止まるまでになってしまうのか？

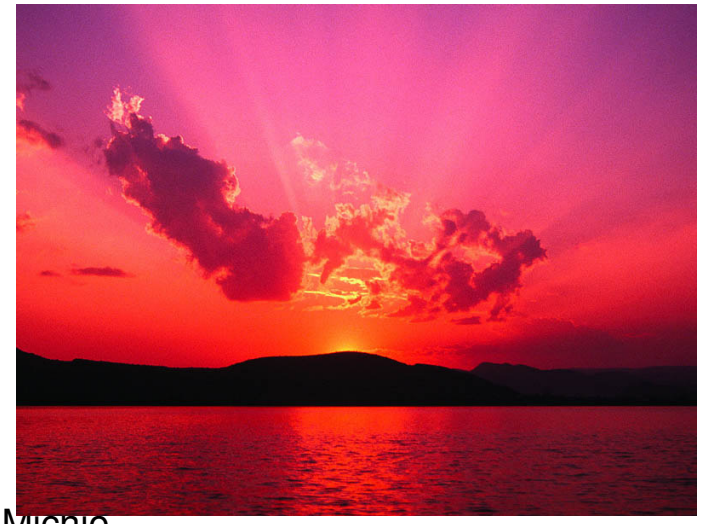
予防、被害を最小限にする、という手立て
は無いのか？

ワーム・ウイルスで止まる原因

- 異常検知する仕組みが弱い
- 隔離手段（手順）が無い
- サーバーやネットの冗長化：
- 負荷分散？

効き目が無い！

延命策でしかない！



ワーム・ウイルスの検知の真実

トラフィックを計測して異常を検知する、というのが

最も現実的なのか？

IDS（侵入検知システム）もワーム検知に使える

もちろんワーム・ウイルス対策ベンダーの提供
するウイルス対策ソフトウエアも検知に使える

アノマリー（異常）検知システムもあるが、高額

ワーム・ウイルス対策の真実

IDP（侵入検知予防システム）以外に、異常通信を
（半）自動的に遮断する仕組みは無い

ルーター、スイッチが遮断する仕組みを持っていればいいのに

単なる過剰なパケットではなくて、一つのPC、一つのソースからランダムな相手に
発信されるパケット＝いわゆるワームの拡散時の現象に対応した**「防水隔壁」機能**

防水隔壁？

単なる過剰なパケットではなくて、一つのPC、一つのソースからランダムな相手に発信されるパケット＝いわゆるワームの拡散時の現象に対応した「防水隔壁」機能

思考実験Q：一つのソースから一つの相手に大量に発信されるという攻撃は？
思考実験A：それは一つの相手側（サーバーなど）で対処すべき。特別な対処は必要としないハズ。DOSはそもそもセッションテーブルのリソースなど、通信相手のポインタがフルになることが発端となるはず
思考実験Q：一つのソースから一つの相手にソースを偽造したパケットが送られたら？
思考実験A：MACの偽装、IPの偽装など、ケースバイケースで対応可能だろう

目的は「急激な拡散の防止」。これだけを防げば現時点でのいわゆるワームは脅威でなくなる
セキュリティ面の耐障害性の目標は拡散防止ができるネットワークインフラ

「内部犯行」の真実

続発する内部犯行の情報漏洩事件というのは、

ほんとうのところどのようなリスクの結果なのか？

事例を紐解いてみると

委託先の会社

内部スタッフ

内部の有資格者が多数

なぜ、内部犯行は起きてしまうのか？

情報漏洩事件の真実

サポートセンターでアカウントパスワードを共有、
端末を使えば個別の情報は誰でも閲覧できた

顧客や会員情報を管理していたサーバーやパ
ソコンから抜き出された

個人情報の不適切な扱いが慣習化していた

用紙の廃棄・輸送中の事故

いずれにしても人の問題

（事故や仕組みの不具合は別としても ）

「内部犯行」の
真実

結局のところ、

誰も見ていないから

内部の人は情報を盗用する

内部犯行を知るための仕掛け

追跡できるようにする

利用者、管理者、その他の有資格者が、

何にどこでどうやってアクセスしたか

を記録しておく仕掛けが必要

ひとつのシステムだけでなく、**複数**

しかし！

VPNを張られたりすると、
中身が見えない！

通信記録用ゲイトウエイが必要？
しかしトンネルされてしまう？

IPsecは安全。
しかし、中身があれほど見えないものもない

VPNの真実

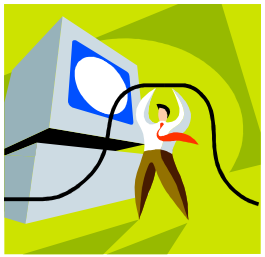
SoftEtherというキラーアプリケーションは多層的なコミュニティー構築の可能性を秘めていると思う
しかし、記録が取れない！

サーバーだけでログ、システムログなどを取っているだけでは限界がある。
誰かが他人のアカウントでサーバーにログインした。
他人の振りして何かを仕掛けた。
これを捕捉するためには、例えばファイアウォール、IDS、パケットレコーダー、通信機器の記録、といったものが必要になる。
例：何月何日何時何分にある特定のマシンから出ている通信は、そのIPの本来の持ち主とは異なるマシンからのものである。それでも、相手が偽装テクを持っていればいるほど特定が困難になる

要するにVPNは

迂回路になってしまう可能性がある

リスクは迂回して入り込む



ゲイトウエイ型集中防御はもう限界か？

すでに持ち込みPCは迂回していることがある！

VPN対策の真実

もはや個別のPCをそれぞれに守るしかない？

セキュリティポリシーに合致するかどうかで認証するようにならないか？

ディレクトリサービスなどを使って、システム設定やレジストリ、アプリケーション等が
規定以外の状態になっていないかを確認する
それに違反するPCはIPアドレスを割り当てない、など。

VPN対策の真実2

もはや個別のPC、サーバーで記録するしかない？

PCやサーバーのリソースの管理？

あるいは、暗号化されていない部分や、サーバーのホストベースなどで
詳細な記録を残しておく必要がある

じゃあ、

何でもかんでも
とにかく記録しと
けばいいのか？

いつその記録を読む、チェックするのか？

とはいえ「記録」は必要

- 訴訟に対応しなければならなくなる
  - 個人情報保護法
  - 不正アクセス禁止法
  - 民事の損害賠償
- そしてもちろん内部犯行にも対応しなければならない

- **ツールが（安価で）欲しい！**

まとめ

耐障害性	ワーム・ウイルスに強い
異常検知	ワーム・ウイルスを検知
追跡性	内部の有資格者の追跡

課題:

防水隔壁

VPN対策

記録の検索

結語

セキュリティは

細部（ディテイル）に宿る

書籍その他紹介

- TCP/IPネットワークExpert2（技術評論社）に漫画「アクセス探偵IHARA」掲載中（くりひろしさん：画）
- Snort2.0侵入検知（ソフトバンク）発売中
- 暗号技術大全（ソフトバンク）第三版発売中
- Windowsセキュリティ対策大全（日経BP）発売中
- セキュリティポリシーの作成と運用（ソフトバンク）発売中
- にわか管理者奮戦記@ITにて連載中