

# 「パンドラの箱」を開け

-あなたは自社ネットワーク利用の現実を知っていますか？-

住商情報システム株式会社 情報システム部

二木真明 CISSP (Certified Information Systems Security Professional)

NPO日本ネットワークセキュリティ協会幹事 技術部会長



A red silhouette of Cupid with wings and a bow, surrounded by small hearts, is positioned in the top-left corner of the slide.

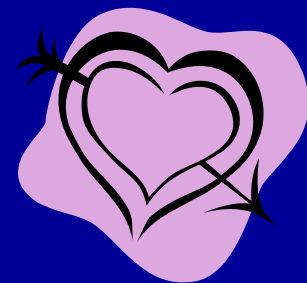
# ネットワーク、この魅惑的なもの

- 居ながらにして、世界を飛び回る快感
- 欲しい情報が瞬時に手に入る満足
- もっと速く、もっと多く……欲望

一度知ってしまうと、離れられなくなる、ネットの魔力

しかし、それを得たために失うものもある……………それは

## 心の平穩



# ネットがもたらす災厄

- ハッキング、侵入、乗っ取り……
- ウイルス・ワーム・スパイウェア・ボット…
- フィッシング、スパム、スパイア……
- ガセネタ、誹謗中傷、脅迫、ストーカー
- 情報漏洩、人間不信……

知らなければ幸せなのだが……

いっそ、目をつぶって生きようか……

「あるネットワーク管理者の日記より」



# 「現実」を直視しよう



- 恐くて(面倒で?)見られないログ……
- 知らんふりを決め込んでいるアラーム……
- それを直視するのが、あなたの仕事だ!
- 但し……
  - 始めたら最後、終わりのない戦いに身を置くことになる。
  - 覚悟を決めよ!!

# 監視すべき脅威



- 不正プログラム感染
  - ウイルス・ワーム、スパイウェア、ボット……
  - ウイルス対策ソフトのみでは不十分
    - 未知の不正プログラム感染への備えも必要
- セキュリティ問題を引き起こす可能性のあるもの
  - トンネルによる「ヤミ」外部接続
    - Softether, IPSec VPN, ssh トンネル……
  - ファイル交換ソフトウェアなどの情報流出等につながるアプリケーション
  - 不正プログラムの伝播に使われやすいアプリケーション
- その他の異常事態
  - なにが異常かを知るには、「日常」を知る必要がある
  - 多くは「カン」だのみだが、整理された情報が「カン」を冴えさせる

# まずはF/Wのログから

## ■ F/Wのログは情報の宝庫

– F/Wのログから何がわかるか

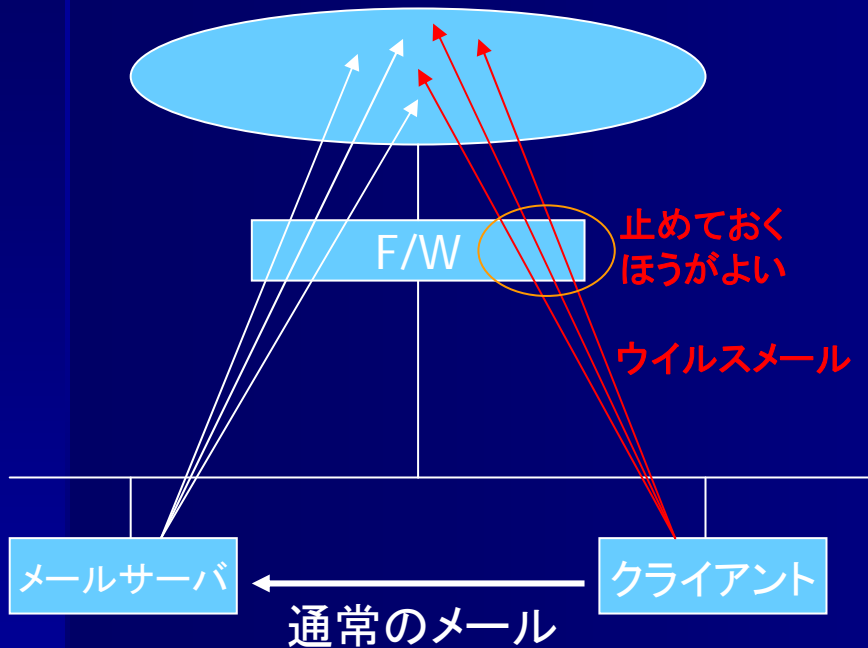
- ユーザのネット利用状況(アクセス先、使用アプリケーションなど)、ポリシー遵守状況
- ウイルス、不正プログラムへの感染疑いのある機器

– 見方を変えれば、「知らなきゃよかった」情報の伏魔殿

# ファイアウォールのログ

- 通過許可状況 (Acceptログ、セッションログなど)
- 通過拒否状況 (Denyログ、Dropログ・・・など)
- 攻撃・アノマリー検出 (不正形式のパケット、一部のプロトコル異常やIP詐称攻撃)
- 付加機能 (AV, IDS/IPS機能) を使ったウイルス・脆弱性への攻撃検出
- Proxy型F/Wの場合、一部のアプリケーション依存情報 (電子メールの発信元、宛先、WebアクセスURLなど)

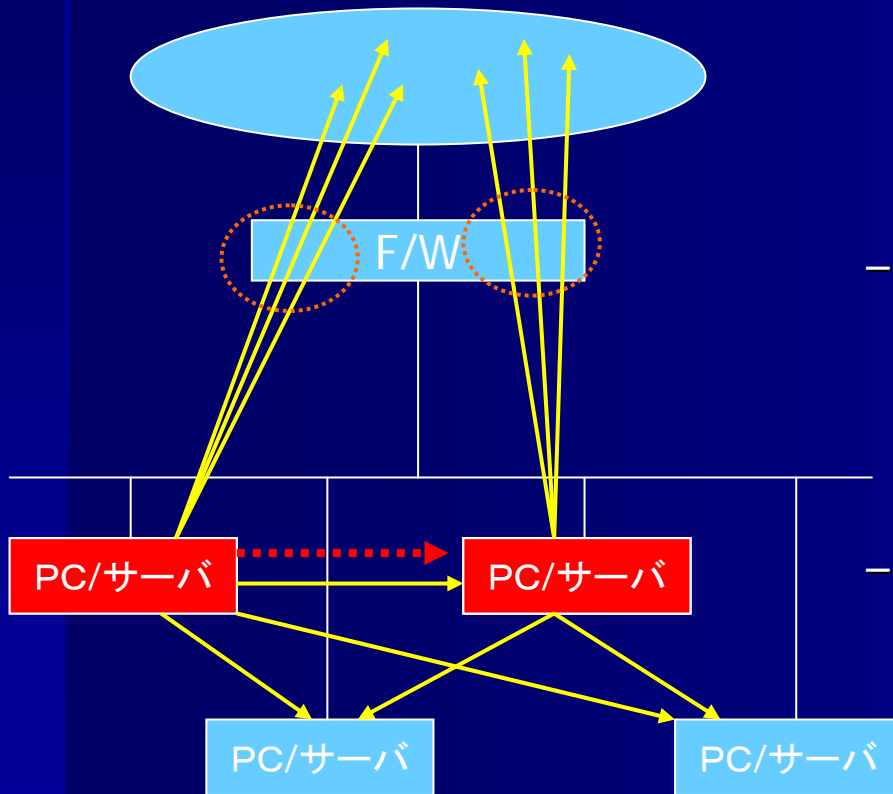
# ウイルス感染を見つける



- マスメール型ウイルス発見は比較的簡単
  - 短時間に大量のSMTP接続を複数の相手先に対して発生させているPC(メールサーバ以外のサーバ等を含む)をファイアウォールのセッションログから抽出
  - 但し、組織のポリシーとして、メールの直接配信を許していない前提が必要
    - できれば、メールサーバ以外からの直接SMTPは通過禁止にしておいたほうが安全
    - この場合はファイアウォールの通過拒否ログからチェック



# ワーム感染の場合



## ■ ワームの挙動

### － 探索活動

#### ■ いわゆるポートスキャン(アドレススキャン)

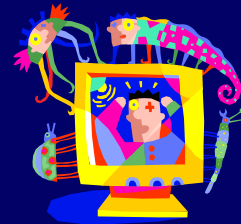
- － 複数ホスト特定ポートへの連続的パケット送信
  - TCP/SYN, UDP, ICMP(ping)
- － インターネットへの探索を行うものはF/Wログからも発見可能

### － 感染(侵入)活動

- リモートコード実行可能な脆弱性への攻撃
- アカウント情報奪取可能な脆弱性への攻撃
- ユーザアカウントへのパスワードクラック攻撃
- …などの組み合わせ攻撃

### － そして、感染後は攻撃対象が攻撃元となる(攻撃の連鎖)

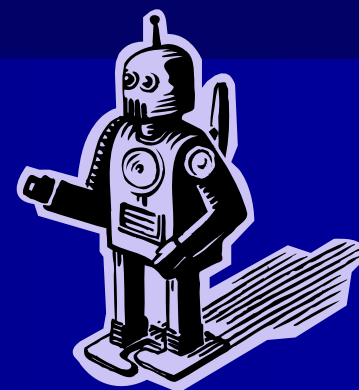
# ワーム発見の難しさ



- ポートスキャンに類似の活動
  - P2P系ソフトウェアによるノード探索
    - Winny, Shareなどのファイル交換ソフトは「禁止」するのが早い
    - でも、たとえばSkypeはちょっと厄介かも……
  - Webキャッシュサーバによる巡回
    - 巡回時間帯、アドレスを特定して排除
  - DMソフトによるメール送信
    - ウイルス感染とも誤認しやすいので、アドレスを特定して排除
  - ネットワーク監視 (Ping, SNMP監視)
    - ノードマネジャーのアドレスを特定して排除

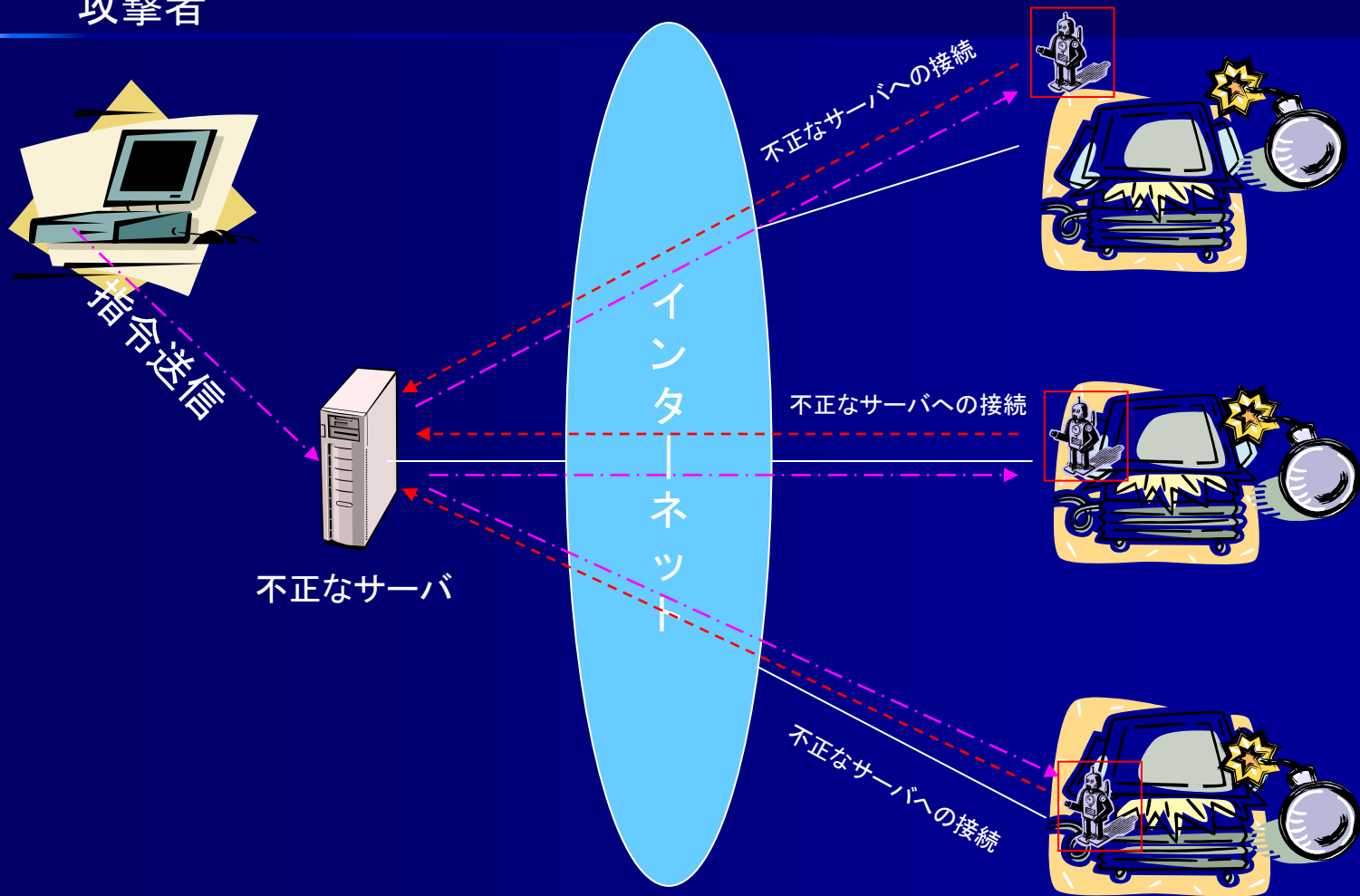
# Bot (ボット) はもっと難しい・・・

- 初期型は比較的簡単なのだが・・・
  - IRCの標準ポート(6667/TCP)を使用
  - ファイアウォールのログから発見可能
- 6667/TCP 以外を使われると発見困難に
  - よく使われるポート番号
    - 警察庁の調査 (@policeサイトに掲示)
      - [http://www.cyberpolice.go.jp/detect/pdf/20060316\\_botnet.pdf](http://www.cyberpolice.go.jp/detect/pdf/20060316_botnet.pdf)
    - 8080/TCP などを使われるとProxyアクセスとの区別が困難
    - 80/TCPだってないとは言えない。(HTTPと区別する方法を考えないといけな
    - P2P系のアプリによる誤認もある・・・(またしても、Skype・・・)



# BOTの動き

攻撃者



# Skype・・・便利なものにはトゲがある

- 誤認、誤検知の元凶.....
  - 利用者(業務目的)が多いので排除(禁止)できず
  - 監視泣かせの「あの手この手」.....
    - まず、UDP(不特定ポート)でスーパーノード探索
    - ダメならTCP(不特定ポート)で探索
    - それでもダメなら https (443/TCP)
    - それもダメなら http (80/TCP)
    - この過程で、大量のDenyログ、セッションログを発生させる
  - 目の敵にするわけではないのだが.....
- 利用者を特定して対処するしかなし
  - IDS等によるユーザの把握
  - 異常検知時の判断(Skypeか異常かの判断はかなり高い経験値が必要)
  - いっそ、(Skypeユーザは)見捨てるか..... (^\_^;)



# Skypeユーザの特定

- IDSを使った特定
  - すべての通信を特定することは困難
  - Skype起動時に行われるバージョン問い合わせ(http)を検知(http request URI に含まれるパターンをチェック)
  - /ui/.....getlatestversion?ver=xxxxx
- Proxyファイアウォールのログを使った特定
  - Request URIをログに出せるならば可能
  - 上記パターンを探そう
- 特定しておくことのメリット
  - 誤認排除だけでなく、脆弱なバージョンを使っていないかなどのチェックも可能に
  - P2P系ソフトウェアにおいては、脆弱性の種類によって、かなりクリティカルな影響が出る可能性が高く、利用禁止できなければ、バージョン管理の徹底は必須である。

# 一般のP2P系ソフト利用の特定

- メジャーなP2PはIDSで検出可能なものも(但し、完璧ではない)
- ワーム感染疑い→ウイルススキャンで発見できず→  
→P2P系利用を疑うべし
- 管理者のテクニック
  - アクセス先を調べよう(ドメインは?、どこの国?、Webサイトなの?・・・)
  - 相手が怪しそうならウイルス・ワーム感染疑い扱いで利用者に連絡しよう
  - ウイルス検査ソフトでフルスキャンしてもらい、結果を報告
  - ウイルス・ワーム感染が発見されなければ、P2P系ソフトをいくつか例示して使用の有無を問い合わせ。(「P2P」系の利用がただちに「悪」ではないので、ソフトに問い合わせること)
  - しばらく経過観察。(P2Pソフトの業務外利用ならば、これでだいたい通信が止まる・・・、一応、ブラック(or グレー)リストに載せておく)
  - それでも出るならば、本格的に未知ワーム感染などを疑うべし

# IM(メッセージャー)利用者特定

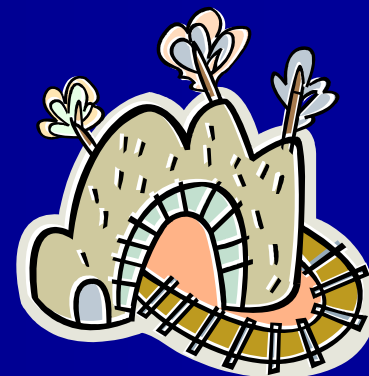
- 業務上の利用者が非常に多い「有用」なソフト
- 反面、業務外利用、添付ファイル経由のウイルス感染などの危惧もつきまとう
  - 何かあった時の利用者特定や注意喚起の伝達なども必要に
- IM は接続先から判断できる
  - MSN系、yahoo系サイトなど、IMサービスへの接続を監視
- IMを検出可能なIDSも多い





# トンネルの発見

- 難しい課題だが……
- 出来そうなところから
  - ssh での頻繁な接続、長時間接続
  - 500/UDPでの通信 (IPsec UDP カプセルング)
  - Soft Ether の keep alive検出 (ping to [keepalive.softether.com](http://keepalive.softether.com))
  - http/httpsによる長時間のコネクション (セッションログの durationから)
- でも、悪者がその気になればどんなことでも
  - Covert Channel:たとえばHTTPのヘッダに紛れて……
  - SMTP(メール)トンネルなんてことも……
  - あとは管理者の「カン」……
- 怪しいと思ったら問い合わせよう
  - 但し、最初から「悪者扱い」は絶対にしないこと
  - 宛先のアドレス情報はあらかじめ調査して得ておこう
  - あくまでソフトにやる。それが効果的な「牽制」となる



# NAT, Proxyの検出

- 基幹ネットワークへの独自ネットワーク「ヤミ」接続
  - 真の利用者アドレスが隠蔽されてしまい、問題発生時にユーザ特定が困難に...
- 意外と単純な方法で見つけられるケースも
  - たとえば、発信元ポートの値が通常よりも大きな値をとるようなケースの多くは、なんらかの共有サービスを複数のユーザが利用している可能性が高い。
    - 発信元ポート番号の消費量が大きくなるため
  - 一部のファイアウォールのNAT(IPマスカレード)では、発信元ポートの初期値がかなり大きな値(たとえば32768)になる

# アクセス先の調査テクニック

- IPアドレス情報の検索
  - Nslookup / DNS逆引き情報
  - Whois / アドレス割当先情報
    - ARIN(米国など), APNIC(アジア), JPNIC(日本), RIPE(ヨーロッパ)などのWebサイトでも検索が可能。
- Webサイトの調査 (80/tcp, 8080/tcp)
  - 怪しいサイトに対しては決してブラウザ(特にIE)を使わない。(不正プログラムを喰わされる可能性あり)
  - telnet で 80番ポートなどにアクセスして
    - GET / HTTP/1.0 <crLf><crLf> などと入力
    - 送り返されたHTMLテキストを解析する。反応がなければWebサイトではない可能性あり
    - 仮想化サイトには注意(Host: ヘッダを送る必要有り)

# 日常の掌握

- どのような通信が行われているか
  - プロトコル別の利用傾向の掌握
    - 発信元別
    - 宛先別
    - ポート番号別
    - 時間帯ごとの傾向
    - ネットワーク(アドレス範囲)ごとの傾向
  - 「異常」を見つけるためには必須

# どうやってチェックするか

- ログ解析ソフトを使う
  - 日常動向は把握可能
  - アクセスランキングは下位から調べてみよう
  - 異常行動も一部見つけられるかも・・・
  - でも、それ以上は難しい
- 自分でプログラムを書くか
  - イベント種別、発信元情報、宛先情報、時刻などをログから抽出、CSVなどに落としてAccessなどのデータベースに入れておくと検索が容易。レポートイングもビジュアルにできる。

# リアルタイムにできないか

- たとえば、着目するイベントをログから検出してアラームを出すには・・・
  - 単純に `tail -f messages | grep xxxxx` とかやってウインドウに表示
  - ログ監視ツール(たとえば、swatch)を使うとより細かい条件設定ができるかも・・・
    - <http://swatch.sourceforge.net/>
  - でも、時系列条件でアラームを出すのは難しい
- リアルタイムに傾向分析ができないか・・・

# SIM (Security Information Management)

ツールを使う

- 複雑な条件によるイベントフィルタリング
- 時系列的に発生する複数イベントの関連づけ (Correlation)
- リアルタイムな統計処理と視覚化
  - うまく使えばリアルタイムなリスク可視化も
- Open Source から大規模商用製品まで様々なSIMがある
  - カネをかけるか、体を張るか…… (笑)

# SIMによる可視化の例

ArcSight コンソール

ビューバネル

1時間前から現在のシステムイベント | リアルタイム | DMZモニター | ArcSight Status Monitoring | ASM System Responsiveness | Manager and Database Status | Agent and Device - Heads Up Display

Agent and Device Status | Rules Status | Security Activity Statistics | Firewall | 不正通信監視 | 通信状況監視 | 外部からの通信拒否状況

### 一般的でないポート利用者 (pass)

Attacker Address	Target Port	合計
172.21.118.65	50000	17084
172.21.210.60	8450	3899
172.21.140.251	1111	3742
172.21.138.120	3052	2753
172.31.116.201	158	2704
172.26.130.7	515	2648
172.31.114.5	158	2606
172.28.61.172	0	2202
172.28.61.136	0	716
172.21.118.89	15363	322
others		9647

### 一般的でないポート利用者 (deny)

Attacker Address	Target Port	合計
172.31.65.40	119	12
172.21.118.7	5999	10
172.31.65.40	3389	3
172.21.164.19	51254	2
172.27.62.21	59556	1
172.21.164.19	8396	1
172.21.164.19	8403	1
172.21.164.19	8407	1
172.31.125.43	2339	1

### ウイルス感染疑い

Name	End Time	Attacker Address
Suspected Worm Infection	27 10 2005 13:49:18 JST	172.21.97.24

### HTTPトンネル可能性

Attacker Address	Target Port	Target Address	Device Custom String6
172.31.129.28	80	207.46.5.8	1:48:42
172.21.131.2	80	207.46.1.7	1:05:19
172.21.132.12	80	207.46.5.15	1:45:28
172.21.184.103	80	207.46.5.11	1:43:57
172.31.117.122	80	207.46.5.10	5:48:21
172.26.162.150	80	207.46.5.14	1:37:31
172.21.149.144	80	207.46.1.6	1:36:12
172.21.200.20	443	212.116.140.65	4:00:30
172.26.161.20	443	211.32.33.215	6:06:49
172.21.149.4	80	207.46.3.13	3:00:21

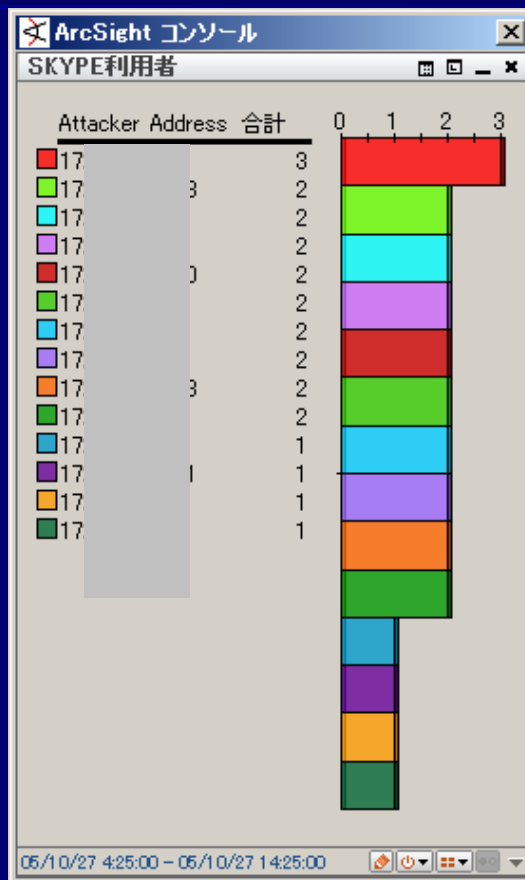
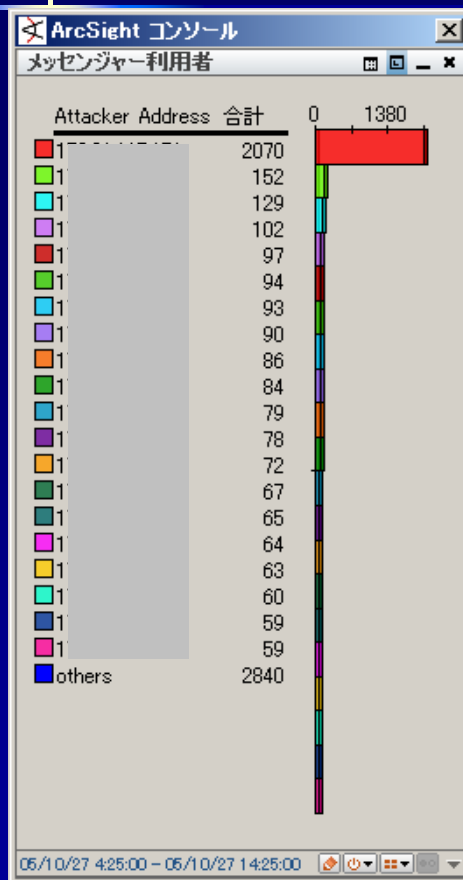
### VPN接続モニター

End Time	Priority	Name	Attacker User Name	Attacker Translated Address
27 10 2005 15:24:22 JST	High	User authenticated	furukawayassuyuki	222.13.3.37
27 10 2005 15:11:21 JST	High	User authenticated	nakajima.kazuki	210.165.65.122
27 10 2005 15:11:02 JST	High	User authenticated	k.sakata	208.54.32.252
27 10 2005 15:10:01 JST	High	User authenticated	otsuka.seiya	210.196.7.9
27 10 2005 15:08:32 JST	High	User authenticated	takahashikoya	222.13.8.183
27 10 2005 15:06:00 JST	High	User authenticated	kuriharahiroshi	58.4.2.238
27 10 2005 15:05:01 JST	High	User authenticated	shimura	61.213.54.176
27 10 2005 15:03:04 JST	High	User authenticated	otaosamu	58.4.2.238
27 10 2005 15:02:31 JST	High	User authenticated	imamura	222.13.0.253
27 10 2005 14:59:45 JST	High	User authenticated	a.suwayama	206.165.3.10
27 10 2005 14:59:13 JST	High	User authenticated	hsuzuki	222.13.28.150
27 10 2005 14:57:44 JST	High	User authenticated	furukawa.ichiro	222.13.7.251
27 10 2005 14:57:08 JST	High	User authenticated	uchimura	61.198.175.41
27 10 2005 14:55:00 JST	High	User authenticated		222.13.28.252

ホーム画面更新時刻: 10/27 15:25:16



# 特定アプリの検出パネルの例



## IM検出

特定のIMプロバイダサイト  
に対する通信をIPアドレス  
ごとに集計して表示

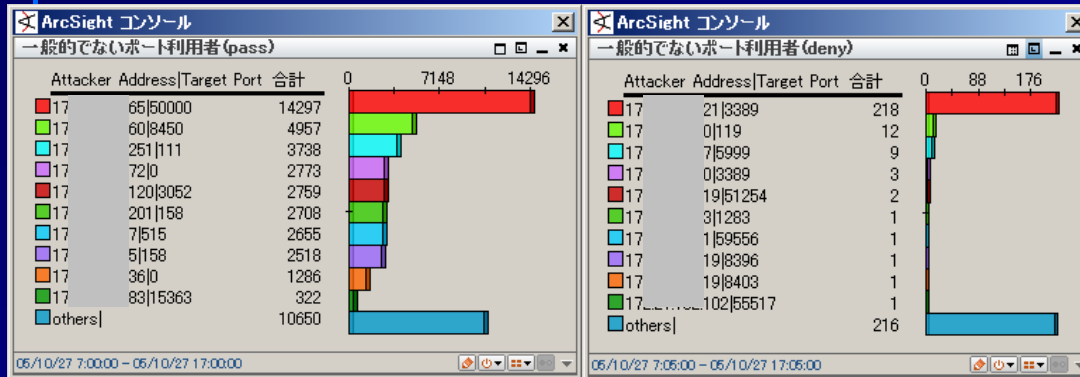
## SKYPE検出

Proxyのログから、URLに  
SKYPE固有のパターンを  
含む通信を検出して集計

または、IDSを使って検知

# 不正通信監視パネルの例

通常あまり使わないポート番号に対する通信監視



インターネットからの実行形式ファイルのダウンロード監視

接続時間が1時間以上のHTTP/HTTPS

**ArcSight コンソール - HTTPトンネル可能性**

Attacker Address	Target Port	Target Address	Device Custom Strin...
17   0.32	443	14   44.154	3:36:47
17   3.221	80	12   215	3:02:34
17   9.120	443	21   33.103	6:37:17
17   0.69	80	20   4	3:00:00
17   0.23	443	81   7.208	1:21:10
17   2.16	80	21   39.93	1:21:12
17   0.23	80	20   1	2:01:58
17   1.94	80	16   3.244	1:00:09
17   0.26	80	20   7.21	2:42:37
17   0.26	80	20   7.21	2:42:37

**ArcSight コンソール - 実行形式ダウンロード**

Attacker Address	Target Address	Request Uri
17: 35	2	253 /msdownload/update/v3-19990518/cabpool/windowsxp-kb899589-x8...
17: 35	2	253 /msdownload/update/v3-19990518/cabpool/windows-kb899830-v1.9-...
17: 06	6	8.36 /VS2/Agent/Scripts/Share.vbs
17: 67	2	253 /msdownload/update/v3-19990518/cabpool/windows2000-kb900725-...
17: 6	6	8.36 /VS2/Agent/Scripts/Share.vbs
17: 26	6	8.36 /VS2/Agent/Scripts/Share.vbs
17: 164	6	8.36 /VS2/Agent/Scripts/Share.vbs
17: 70	6	8.36 /VS2/Agent/Scripts/Share.vbs
17: 45	6	8.36 /VS2/Agent/Scripts/Share.vbs
17: 10	6	8.36 /VS2/Agent/Scripts/Share.vbs
17: 10	2	46.15 /pack/winnt/net/network/PortMon_setup.EXE
17: 10	6	.61 /exe-bin/Request.FileSpawn.exe?BA8E80B91DA6AF
17: 10	6	.61 /exe-bin/Request.FileSpawn.exe?BA8C85C90FB4FE
17: 210	2	8.193 /download/b/4/d/b4d68393-a197-4f84-8362-94d85f9a37e2/SMS2003...
17: 6	6	8.36 /VS2/Agent/Scripts/Share.vbs
17: 02	2	237 /CAT/S=2075220817/SS=2075220889/R=5/*-http://ruma.execweb.cx/...
17: 210	2	8.193 /download/d/5/1/d510d18-7848-4344-ad5d-396567e8702e/sms2003...
17: 10	2	46.12 /pack/win95/util/arc/lhaca120.exe
17: 6	6	8.36 /VS2/Agent/Scripts/Share.vbs
17: 9	2	46.15 /pack/win95/util/arc/lpl152.exe

# オープンソースのSIM

<http://www.ossim.net/>

The screenshot shows a Microsoft Internet Explorer browser window displaying the OSSIM website. The browser's address bar shows the URL <http://www.ossim.net/>. The website header features the OSSIM logo (an elephant) and the text "OSSIM Open Source Security Information Management". Below the header is a navigation menu with links: Home, News, Download, VMWare, Docs, Wiki, Screenshots, Developers, Contact, and Professional Services. The main content area includes an "Announces" section with a subscription link, "Other Links" (What is OSSIM?, ChangeLog, Artwork, Project Page), and "Latest news" (0.9.9rc1 released, Digital Force sequel, 08/05/2006 release date, Major Status Update, New document: how to install ossim-agent, Releasing dokuwiki, Project status update, Article: Armor Your Palace, OSSIM 0.9.8 released). A central banner reads "Skip over to the news section, last update: June 01 2006 Latest version is: 0.9.9rc1". Below this is a "New to ossim ? Read on" section with a paragraph about OSSIM's goal and capabilities. A "Components" section lists software components. On the right, there is a "Server stats" section with a bar chart showing server performance across various metrics.

**Announces**

Would you like to receive new releases and documentation announces?

Subscribe to [Ossim-announces](#) mailing list.

**Other Links**

- What is OSSIM?
- ChangeLog
- Artwork
- Project Page

**Latest news**

- 0.9.9rc1 released
- 0.9.9rc1 changelog excerpt
- Digital Force, the sequel to Z4CK released.
- 08/05/2006 - 0.9.9rc1 release date
- Major Status Update
- New document: how to install ossim-agent and Snort on Windows
- Releasing dokuwiki; new roadmap
- Project status update & more
- Article: Armor Your Palace
- OSSIM 0.9.8 released

**Skip over to the news section, last update:** June 01 2006  
Latest version is: **0.9.9rc1**

**New to ossim ? Read on**

Ossim stands for *Open Source Security Information Management*. Its goal is to provide a comprehensive compilation of tools which, when working together, grant a network/security administrator with detailed view over each and every aspect of his networks/hosts/physical access devices/server/etc...

Besides getting the best out of well known open source tools, some of which are quickly described below these lines, ossim provides a strong correlation engine, detailed low, mid and high level visualization interfaces as well as reporting and incident managing tools, working on a set of defined assets such as hosts, networks, groups and services.

All this information can be limited by network or sensor in order to provide just the needed information to specific users allowing for a fine grained multi-user security environment. Also, the ability to act as an IPS (Intrusion Prevention System) based on correlated information from virtually any source result in a useful addition to any security professional.

**Components**

Ossim features the following software components:

**Welcome to OSSIM**

If this is the first time you use ossim, we recommend trying out the following:

- Define some [hosts or networks](#).
- Use [Networks](#) in order to get a quick host inventory.
- Think [Incidents](#), using the built-in incident tracking system.
- Check [Databases](#) for hosts, net, groups inventory, policies able to filter out events and actions & responses based on certain events.
- [Monitors](#) show you disk, network and availability information.
- Finally, [Reporting](#) use generation the information available.
- Much more at [tutorial](#).

**Server stats**

Server performance

Server	Hosts	Networks	Monitors	Incidents	Reports	Alerts
Net Server	1.0	0.0	0.0	0.0	0.0	0.0
Hosts	0.0	1.0	0.0	0.0	0.0	0.0
Networks	0.0	0.0	1.0	0.0	0.0	0.0
Monitors	0.0	0.0	0.0	1.0	0.0	0.0
Incidents	0.0	0.0	0.0	0.0	1.0	0.0
Reports	0.0	0.0	0.0	0.0	0.0	1.0
Alerts	0.0	0.0	0.0	0.0	0.0	0.0

# “Real time” P.D.C.A cycle

- 発見したいものが何かを明確にして、そのためにどんな情報が必要かを考えよう
- その情報を収集し、分析する方法を考えよう
- 考えた方法を実装、運用してみよう
- 見つけたインシデントに対処しよう

果てしのない「繰り返し」……………

それがセキュリティ管理者の「お仕事」

# 「希望」はないのか！？

- 「希望」それは現実を直視すること
- 「希望」それは戦い続けること
- そして未来こそが「希望」



# セキュリティ管理者の「希望」

- それが、自分の会社を守っている・・・という自負。
- ご清聴ありがとうございました。
- この資料は以下のサイトで掲示します
  - <http://www.kazamidori.jp/>