「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

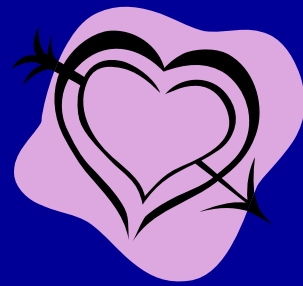
ネットワーク、この魅惑的なもの

- 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

心の平穏



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・スパイウエア・ボット・・
- フィッシング、スパム、スピア・・・・
- 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、スパイウエア、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エアなどの情報流出等につながりう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

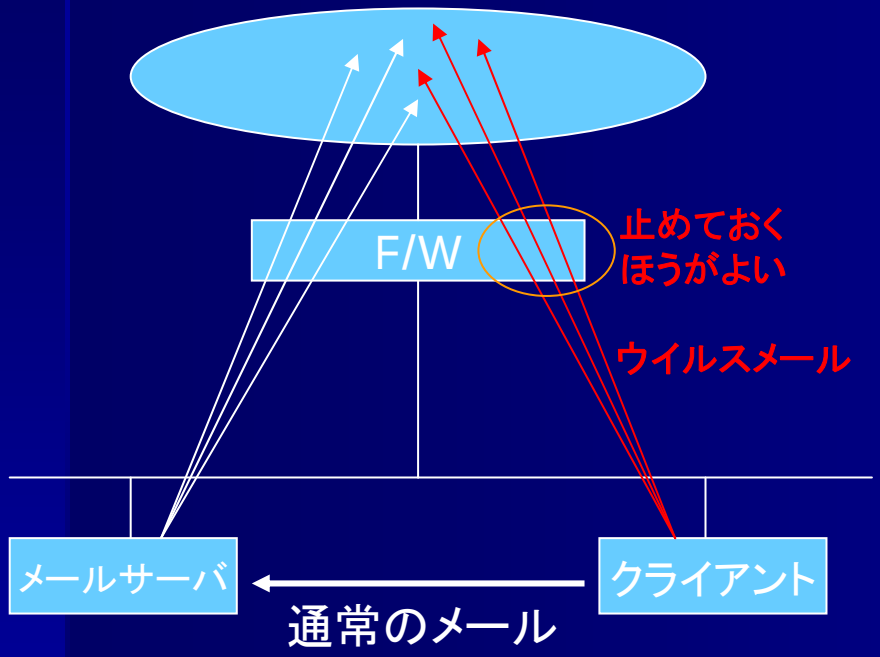
まずはF/Wのログから

- 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

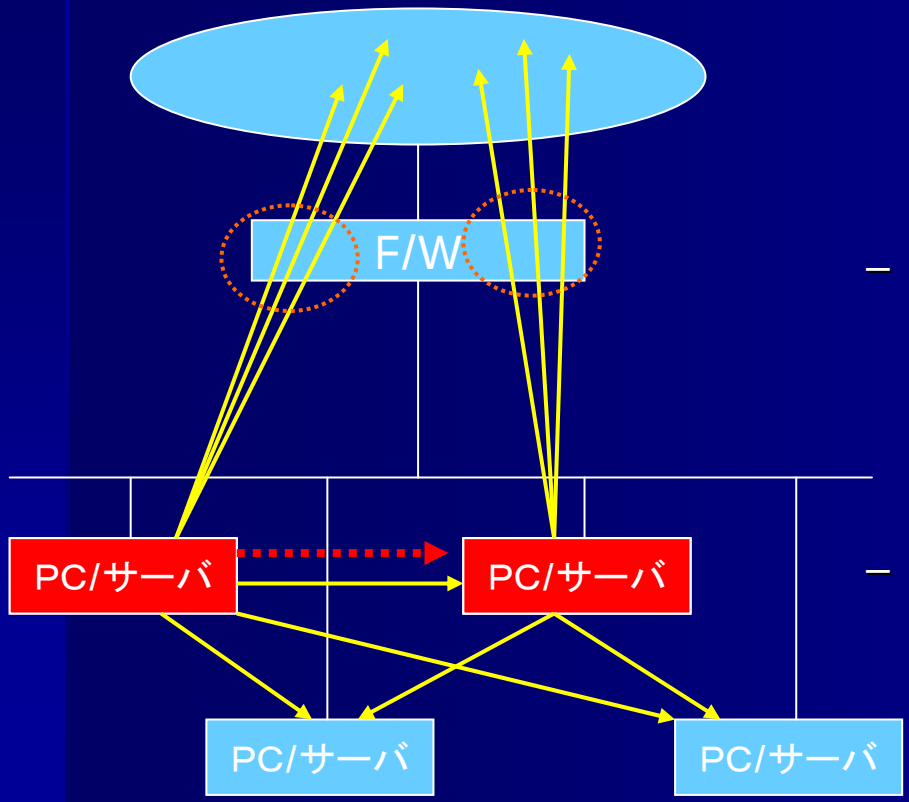
- 通過許可状況（Acceptログ、セッションログなど）
- 通過拒否状況（Denyログ、Dropログ・・・など）
- 攻撃・アノマリー検出（不正形式のパケット、一部のプロトコル異常やIP詐称攻撃）
- 付加機能（AV，IDS/IPS機能）を使ってのウイルス・脆弱性への攻撃検出
- Proxy型F/Wの場合、一部のアプリケーション依存情報（電子メールの発信元、宛先、Webアクセス URLなど）

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コネクション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

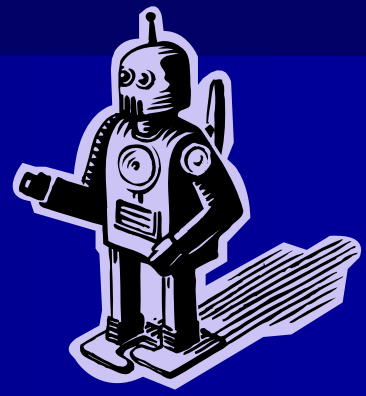


- ワームの挙動
  - 探索活動
    - いわゆるポートスキャン（アドレススキャン）
      - 複数ホスト特定ポートへの連続的パケット送信
        - TCP/SYN, UDP, ICMP(ping)
      - インターネットへの探索を行うものはF/Wログからも発見可能
  - 感染（侵入）活動
    - リモートコード実行可能な脆弱性への攻撃
    - アカウント情報奪取可能な脆弱性への攻撃
    - ユーザアカウントへのパスワードクラック攻撃
    - ・・・などの組み合わせ攻撃
  - そして、感染後は攻撃対象が攻撃元となる（攻撃の連鎖）

ワーム発見の難しさ

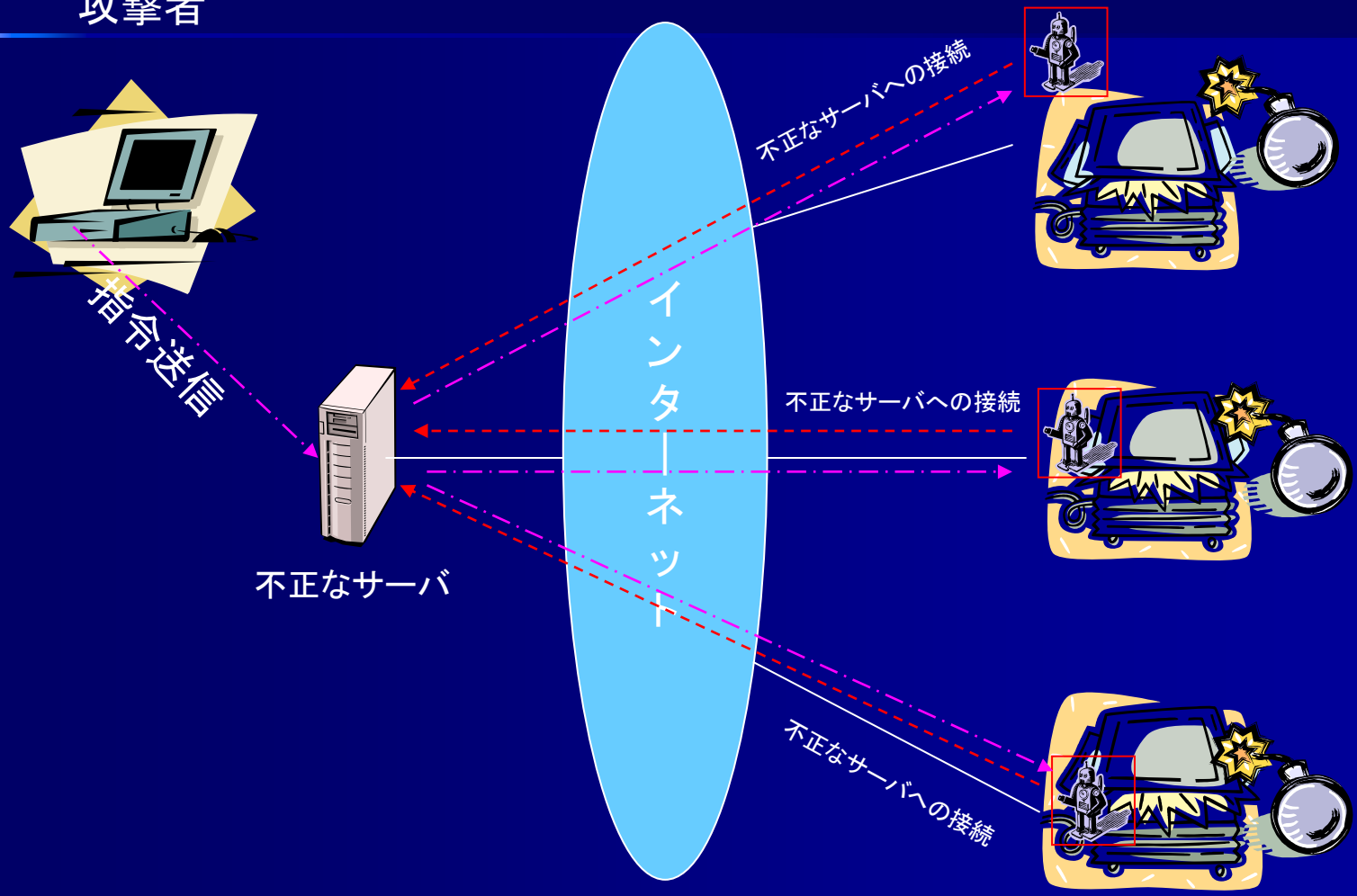
- ポートスキャンに類似の活動
  - P2P系ソフトウエアによるノード探索
    - Winny, Shareなどのファイル交換ソフトは「禁止」するのが早い
    - でも、たとえばSkypeはちょっと厄介かも・・・・
  - Webキャッシュサーバによる巡回
    - 巡回時間帯、アドレスを特定して排除
  - DMソフトによるメール送信
    - ウイルス感染とも誤認しやすいので、アドレスを特定して排除
  - ネットワーク監視（Ping, SNMP監視）
    - ノードマネジャーのアドレスを特定して排除

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
    - 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い）
    - 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
指令送信
不正なサーバ
インターネット
不正なサーバへの接続
不正なサーバへの接続
不正なサーバへの接続

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系ソフトウエアにおいては、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

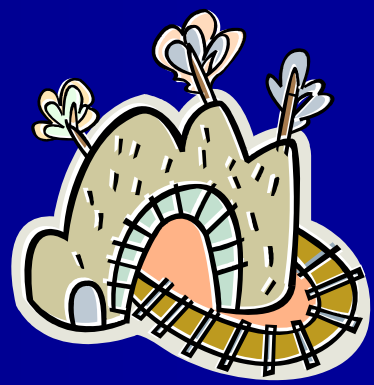
- メジャーなP2PはIDSで検出可能なものも（但し、完璧ではない）
- ワーム感染疑い→ウイルススキャンで発見できず→
  →P2P系利用を疑うべし
- 管理者のテクニック
  - アクセス先を調べよう（ドメインは？、どこの国？、Webサイトなの？・・・）
  - 相手が怪しそうならウイルス・ワーム感染疑い扱いで利用者に連絡しよう
  - ウイルス検査ソフトでフルスキャンしてもらい、結果を報告
  - ウイルス・ワーム感染が発見されなければ、P2P系ソフトをいくつか例示して使用の有無を問い合わせ。（「P2P」系の利用がただちに「悪」ではないので、ソフトに問い合わせること）
  - しばらく経過観察。（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（メッセンジャー）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 カプセリング)
  - Soft Ether の keep alive検出 (ping to 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。レポーティングもビジュアルにできる。

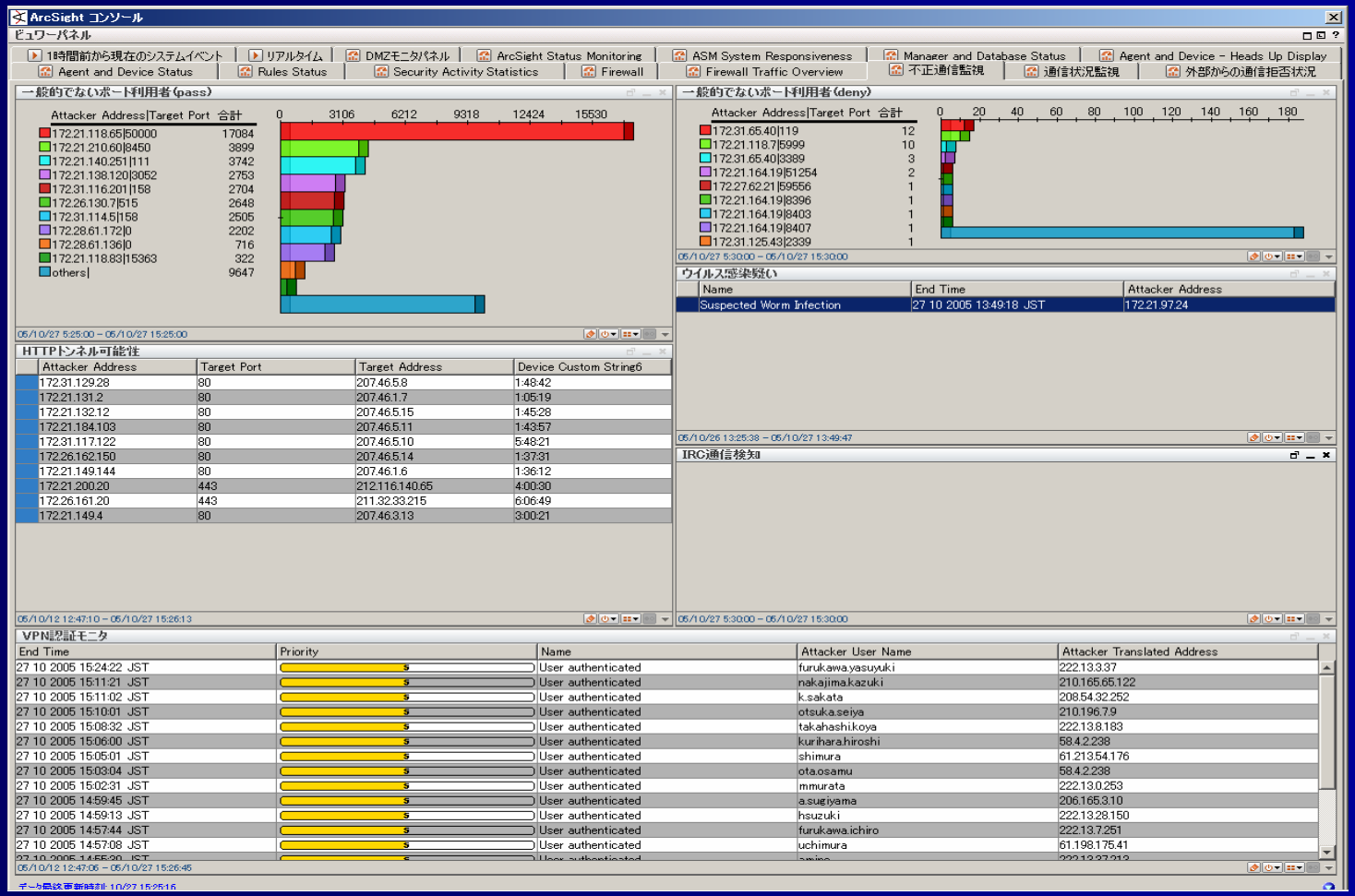
リアルタイムにできないか

- 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・・

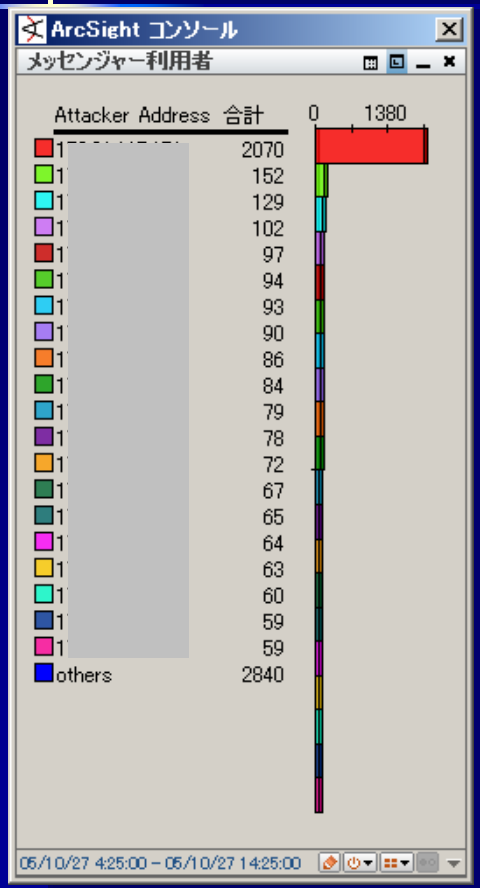
SIM (Security Information Management)
ツールを使う

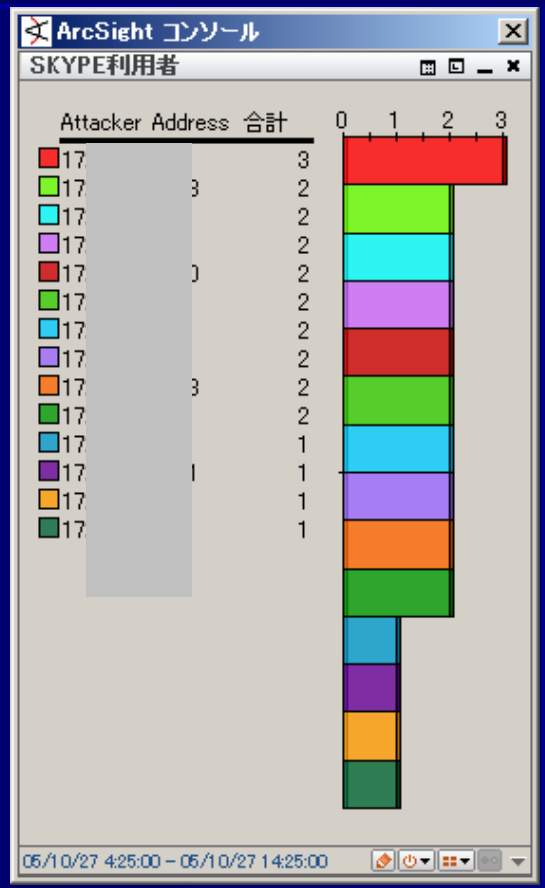
- 複雑な条件によるイベントフィルタリング
- 時系列的に発生する複数イベントの関連づけ（Correlation）
- リアルタイムな統計処理と視覚化
  - うまく使えばリアルタイムなリスク可視化も
- Open Source から大規模商用製品まで様々なSIMがある
  - カネをかけるか、体を張るか・・・・（笑）

SIMによる可視化の例



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

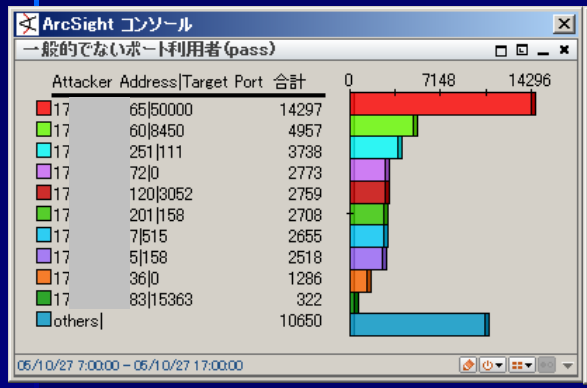
SKYPE検出

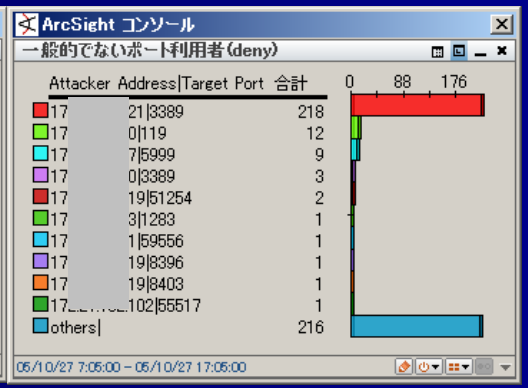
Proxyのログから、URLにSKYPE固有のパターンを含む通信を検出して集計

または、IDSを使って検知

不正通信監視パネルの例

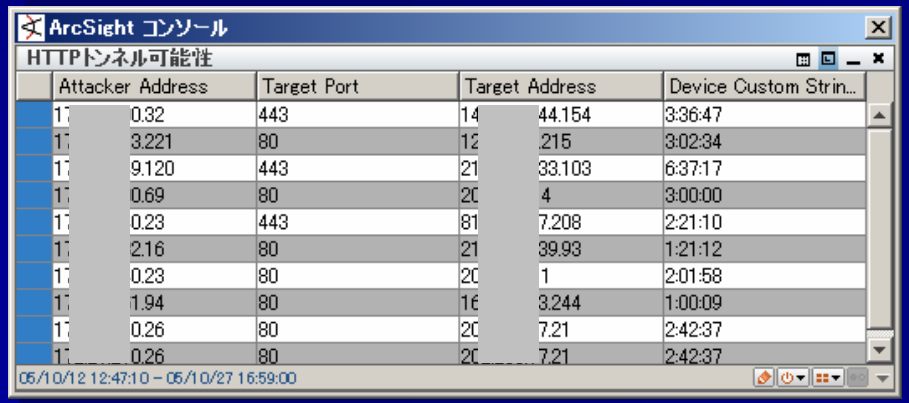
通常あまり使わないポート番号に対する通信監視

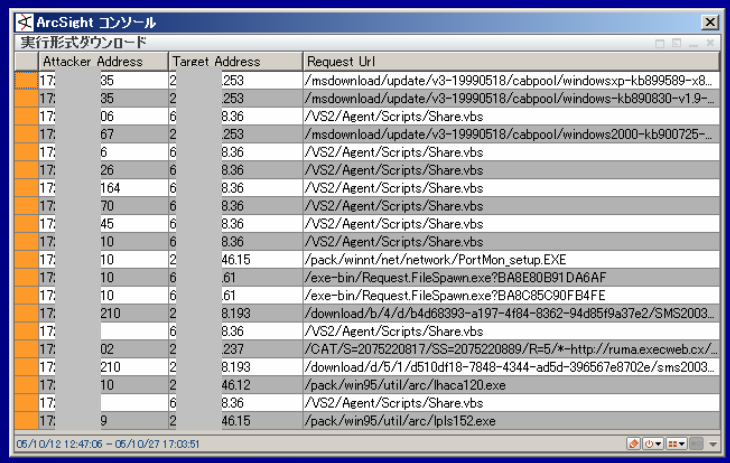




インターネットからの実行形式ファイルのダウンロード監視

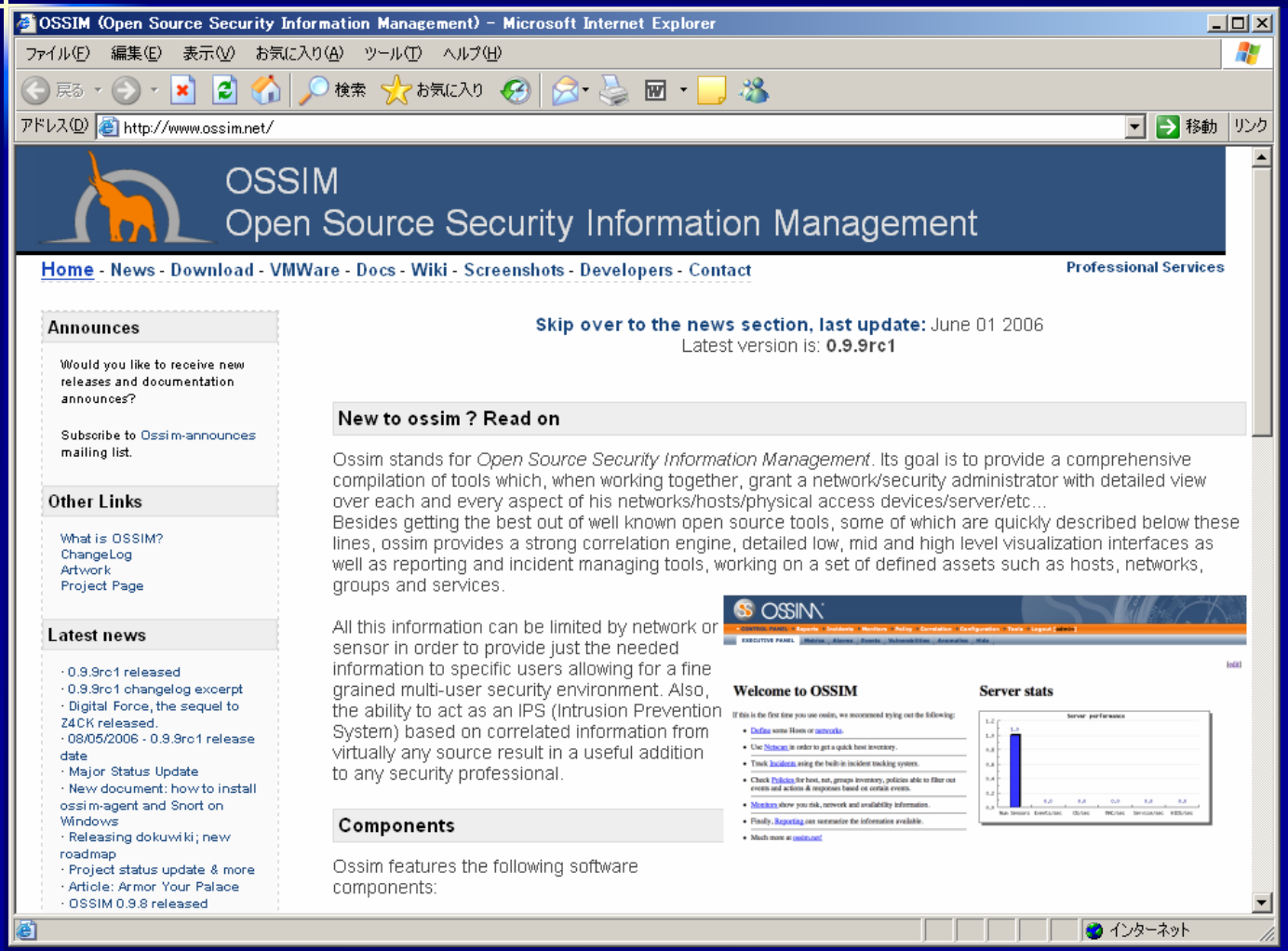
接続時間が1時間以上のHTTP / HTTPS





オープンソースのSIM

http://www.ossim.net/



“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/