リアルタイム監視による 不正プログラム発見と対応

Internet Week 2005

T13: 不正プログラム対策と侵入検知、防御技術

二木真明 (住商情報システム)

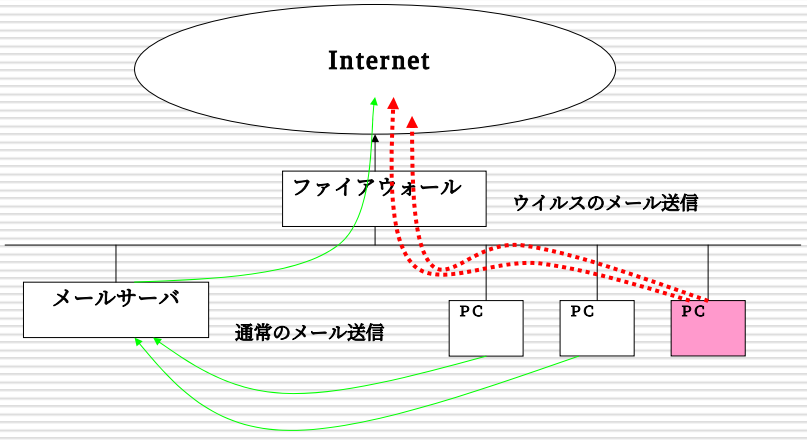
ネットワークと不正プログラム

- 不正プログラムに関連する通信の種類 (例)
  - 感染のきっかけ
    - メールサーバへのアクセス
    - Webサイトへのアクセス
    - ネットワークからの攻撃
  - 発症行動に伴うもの
    - 情報持ち出しや指令チャネル確立のための通信
    - サービス妨害、特定先攻撃のための通信
  - 感染拡大行動に伴うもの
    - メール送信 (不特定多数宛)
    - 探索活動 (ポート、ホストスキャン)
    - 攻撃実行

メール拡散型ウイルスの場合

- 通信の特徴
  - 一般に、独自のSMTPエンジンを持つため、メール送信は、その組織のメールサーバを経由せず、直接相手方のメールサーバに対して行われる
  - 短時間に多くの相手方に対してSMTP接続が発生する
  - SMTP接続に付随して大量のDNS問い合わせ(MX参照)が発生する

メール拡散型ウイルスの挙動



メール拡散型ウイルス感染を発見する

- 外部へのSMTP送信はファイアウォールを経由する
  - ファイアウォールはログにその事実を残すはず
    - 直接のSMTP接続が許可されている→セッションログ
    - 直接のSMTP接続禁止→拒否 (Reject/Deny) ログ
  - 通常の電子メール送信とは異なるパターン
    - 短時間に多数の接続／拒否ログの発生
      - たとえば1分間に数十個以上

＊特段の必要がない限り、クライアントから直接外部へのSMTPは禁止したほうが無難 (ウイルス感染ではメールアドレス漏洩の可能性もあるので)

たとえば、こんなふうに

- ログサーバ上で監視 (原始的方法)
  - ログファイル fw.log、メールサーバアドレス x.x.x.x として

```
# tail –f fw.log | grep “dst-port=25” | grep
–v “src-ip=x.x.x.x”
```

•通常のメールはメールサーバから送信されるので、この条件では表示されない。
•大量にメールを吐くアドレスがあればウイルス感染が疑われる
•世間で「新種ウイルス」蔓延が報じられた時などに感染を監視したい時は便利・・・

ネットワークワームの場合

- 通信の特徴
  - ポートスキャンの実行（特定ポートもしくはping）
    - ローカルネットワークだけでなくグローバルアドレス範囲もスキャンするものが一般的（インターネット上での拡散が目的）
    - 短時間に広範囲のスキャンが発生
  - 特定の脆弱性への攻撃
    - 既知ソフトウエアが持つ脆弱性への攻撃 (exploit)
    - 脆弱なパスワード設定など設定上の問題への攻撃

ワーム感染を発見する

- ファイアウォールを使う
  - ファイアウォールのポートスキャン検出機能
  - 外部へ向けた ping のログ抽出（一般の企業では極めて少ないはず）
  - 特定ポートへの通信の異常な増加を検出
    - HTTP/HTTPSなどが攻撃対象だと難しい
    - NETBIOS系もノイズが多い
- IDSを使用して外向きの通信を監視する
  - 既知の攻撃ならば検知可能
  - ファイアウォールからの出口監視のみで、多くのワームは検知可能
  - 誤検知を防ぐためのチューニングは必要

ボットやスパイウエア系の場合

- 特徴
  - ボットは外部の指令チャネルに接続するために通信を行う
    - 初期のボットはIRC (6667/UDP) を使うことが多かったが、必ずしも限定はできない
    - Covert Channelを使われると検知は困難
  - スパイウエアは情報持ち出しのために通信を行う場合が多い
    - 使うポートは種類によってまちまち・・・
    - Covert Channelを使われると検知は困難
  - バックドア系は、不正なポートをオープンすることが多い
    - 開けるポートは種類によってまちまちだが、一般的なサービスでは使わるポートだと判断が難しい

ボットやスパイウエア発見のヒント

- 既知のボットが使うポート番号を監視する
  - 6667(IRCのデフォルト)
  - 過去のボットが使ったポート番号
    - ウイルス対策ソフトメーカーの情報を活用
- 一般に使われないポート番号を監視する
  - P2P系、VoIP系など、ダイナミックポート割り当てをするアプリと混同する可能性もある
  - おかしいなと思ったらそのユーザが何を使っているか調べてみる
- 接続先から探す
  - これまでほとんどアクセスされなかったサイトやアクセス数が極めて少ないサイト (ログ集計ソフトなどを利用して特定)
  - HTTPなどの場合、非Webサイトは要注意 (HTTPのコマンドに応答しないなど)
- 極めて「アナログ的」「経験的」な作業にならざるをえない

バックドアの検査

- 脆弱性検査ツールの利用
  - 不必要なポートが空いていないかをチェック
  - ＰＣ等の管理がきちんと出来ていないと辛い
    - 不要なアプリケーションやサービスを入れない、起動しないなどのポリシーが徹底されていること
    - 野放しだと「モグラ叩き」をする結果に・・・・
  - 不審なポートが開いているＰＣは詳細にチェック
  - サービスのプロファイリング
    - ポート８０で立ち上がっているソフトは何？

情報と分析が決め手に・・・

- できるだけ多くの（角度からの）情報を集める
- できるだけ多くの（角度からの）分析をする
- パターン化出来る現象は、それを判断する手順（ルール）を作っておく
  - メール拡散型ウイルス、ネットワークワームなど
- パターン化できない現象は「日常」の掌握と「異常」の発見を心がける
  - 渡辺さんの「百葉箱」的なアプローチ

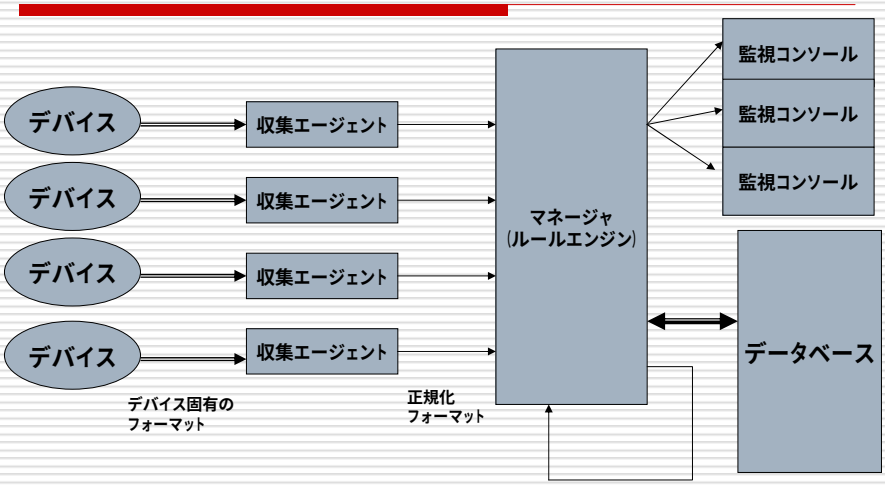
日常監視の道具

- 情報源
  - ファイアウォール
  - NIDS/IPS
  - HIDS/IPS
  - ウイルス対策ソフト、サーバ
  - 脆弱性検査ツール
- 分析の道具
  - ログ解析ソフトウエア
  - IDS/IPS/ウイルス対策ツールなどの管理レポート機能
  - セキュリティ情報マネジメント（SIM）システム

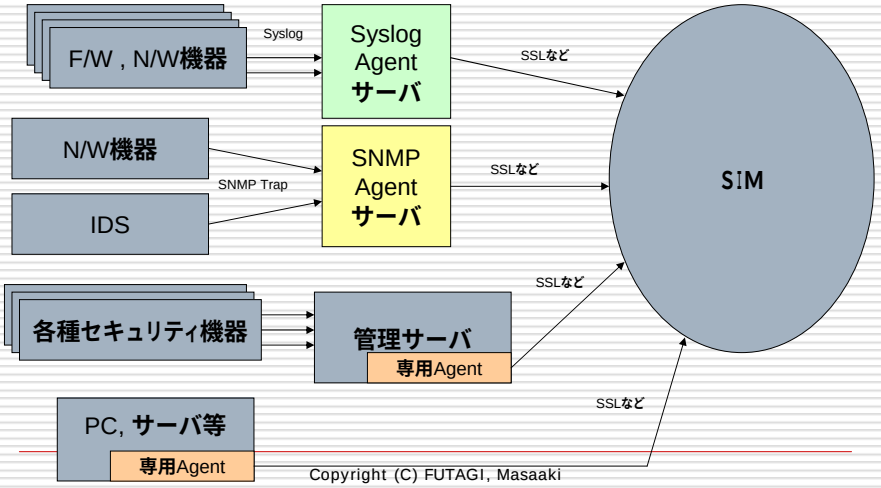
SIMって何？

- セキュリティに関する様々な情報をリアルタイムに分析、管理するためのシステム
  - 様々なセキュリティ機器、コンピュータ、ネットワーク機器・・・からログなどの情報を収集
  - リアルタイムに分析
    - パターン化された事象の検出
    - 傾向分析と異常の発見
    - インシデントリスクの計算
  - 視覚化による監視
    - グラフィカルな形でのリアルタイム表示機能
  - インシデント対応マネジメント
    - トラブルチケット管理、ワークフローのサポート

SIMの構成



ログ、アラームの収集方法



Meta IDS としての SIM

- ネットワーク全体に対する監視と不審な兆候の検出
  - 特定の部分を監視するIDS（点）に対して、ネットワーク全体（面）を時系列的に（時間軸に沿って）監視するもの。
  - 個々の事象から、その本質を見つけ出す（Intrusion Detection というよりも Incident Detectionなのかもしれない）

SIMのコンソール画面

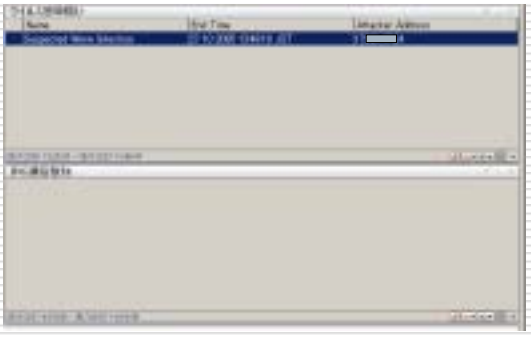
特定目的の監視パネルを並べたダッシュボード

通信状況の監視用ダッシュボード
（SIM版百葉箱？）

実際に使ってみたら・・・・

- ウイルス・ワーム感染検知
  - メール拡散型ウイルス検知は簡単
    - 一定時間内であるしきい値以上の数のSMTPコネクションを外部に対して張ろうとするＰＣをチェック
  - ネットワークワーム検知
    - ポートスキャンの検知
      - 一定時間内に
        - 特定のポートについて一定数以上のホストに対して接続を試みるもの　(NETBIOS系ポートは誤検知多い)
        - 異なるポートについて一個もしくは複数のホストに対して接続を試みるもの　(誤検知が多い・・・)

監視パネル (ウイルス・ワーム感染)



ここでは、ファイアウォールのログから、ウイルス感染およびワーム感染が疑われる現象を検出した場合に出力されるアラームイベントのみが表示される。実際の検出条件は

ウイルス検出条件
1分間にN個以上の異なる相手に対してSMTPコネクションを開設しようとしたアドレスを抽出

ワーム
1分間にM個以上の異なる相手の同一ポートと通信しようとしたアドレスを抽出

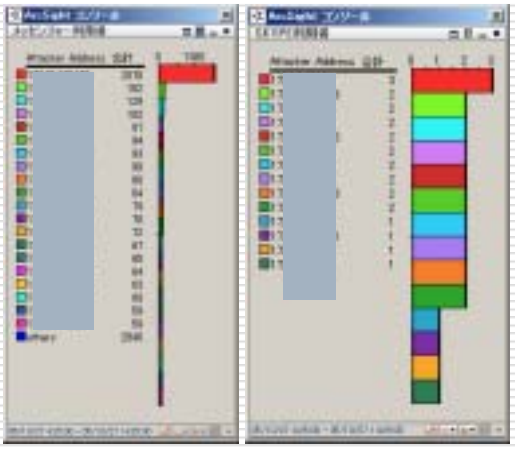
誤検知の軽減

- まぎらわしい行動をするアプリの特定と除外
  - Instant Messenger (IM)
    - 複数接続先の同一ポートまたは異なるポートへ接続を試みる
  - P2P系アプリ
    - 多数の相手先かつランダムなポート番号で接続を試みる
  - SKYPE
    - 基本的にP2Pアプリなので、同上だが、UDP,TCP,HTTPと、ありとあらゆる通信方法を試行するので、結構（管理者にとっては）邪悪

アプリケーションの特定

- IM
  - 接続先がサービスプロバイダに限定されているため、判断可能。特定のプロバイダ（サブ）ドメイン下のサーバへの接続で判断
- P2P, SKYPE
  - IDSの検出用シグネチャを利用
  - HTTPのみ許可の場合は、ファイアウォールやProxyのログ（URL request のログ）をSIMでチェック可能

特定アプリの検出パネルの例



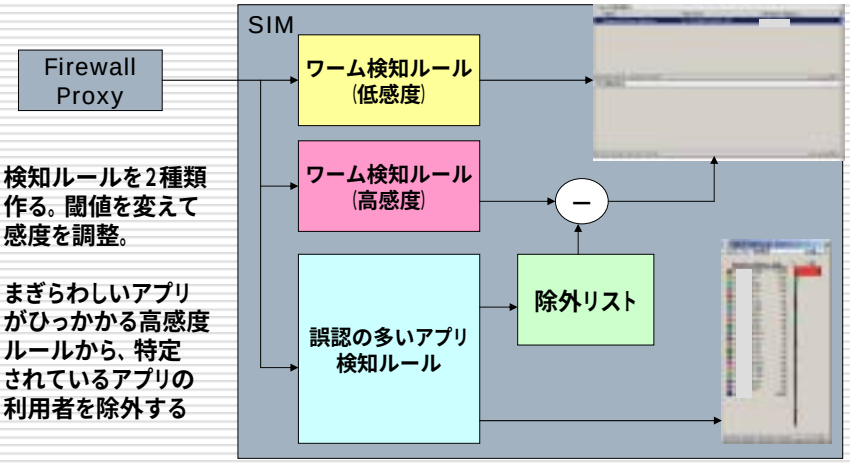
IM検出

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

誤検知軽減のしくみ



検知ルールを2種類作る。閾値を変えて感度を調整。

まぎらわしいアプリがひっかかる高感度ルールから、特定されているアプリの利用者を除外する

不正な通信発見のヒント

- 「繋ぎっぱなし」の接続を調べる
  - ファイアウォールのログからセッション継続時間の異常に長いものを抽出して調査（トンネルの可能性）
  - 外部向けの通信を規制（必要最小限のものに限定）していないと発見が難しい（たとえば、HTTPに絞れると調査は比較的容易）
- 不正な接続先を探す
  - プロトコルごとに接続先のランキングをとってみる
  - ランキング下位から順にFQDNを調べ、逆引きできないホストや不審なドメインに属するアドレスからWhoisで所有者を調査したり、相手のサービスを調べてみる。（たとえば、80/TCPにtelnet接続して挙動を見るなど）

不正な通信発見のヒント

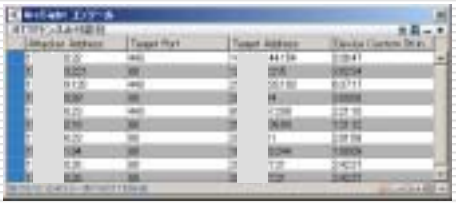
- 一般に使わない宛先ポート番号への通信
  - ポート番号ダイナミック割り当てプロトコルをどう除外するかがポイント
    - 発信元20番（FTP）除外　（ただし20番を使わないソフトもあるので困る）
    - SKYPE，P2Pソフトの通信の除外が課題
- 深夜など、だれもいない時間帯に発生する通信
  - VPN,RASセグメントからの通信は除外
  - HTTP/HTTPSは特に注意
  - アクセス先ランキングで下位にある宛先からチェック

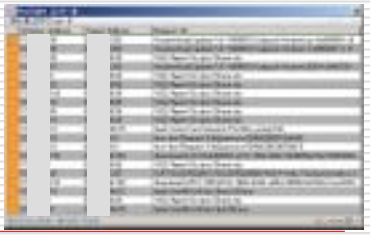
不正通信監視パネルの例

通常あまり使わないポート番号に対する通信監視

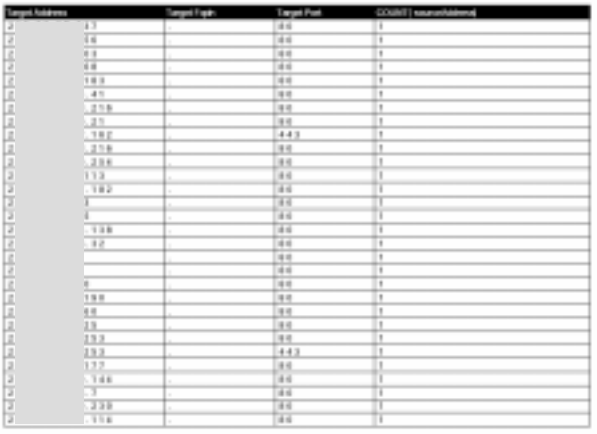
インターネットからの実行形式ファイルのダウンロード監視

接続時間が1時間以上のHTTP / HTTPS





深夜時間帯のHTTP(S)通信レポート



深夜の1時から6時までの時間帯に、これだけの通信があると、ちょっとびっくりします

実際調査したら、キャッシュサーバの定時巡回がほとんどでしたが・・・ホッ

監視するだけじゃダメです

- 不審な兆候を見つけたらどうするか
  - リスクを判断して対応レベルを決めよう
    - 不審な動きのあるホストの重要度を判断する
      - 一般のクライアントPCか
      - 特定の重要業務に携わる人のPCか
      - 機密情報、個人情報などが入っているサーバか
      - 基幹業務用サーバか‥など
    - 作業の優先度、緊急度を考える
      - すぐ現地調査する
      - リモートで調査する
      - 利用者に電話する
      - 利用者に質問表を送る
      - 様子を見る

リスクをすぐに判断するには

- あらかじめ複数のシナリオを考え、生じうる状況（脅威、対象となる資産）を分析しておく
  - インシデントの種類と対象のマトリクス表を作って、緊急度を5から10段階程度で書き込んでおく
  - 各緊急度のレベルで必要な対応をマニュアル化しておく

リスク判定表の形

	脅威1	脅威2	脅威3	脅威4
対象1	1	3	5	1
対象2	5	8	10	5
対象3	2	8	3	4

＊リスク値により、対応の緊急度を決める（例）

レベル1～3： 経過観察、24時間程度で対応（情報システム部主管）
レベル4～7： 即時対応開始、8時間以内に対応（セキュリティ部門主管）
レベル8～10： 即時対応開始、2時間以内に対応（CIO/CISO主管）

一般的な調査の順序

- 誤認の可能性を検討、排除する
  - 意図的な通信かどうか
  - 特殊なアプリケーションの利用など通常と異なる通信を生じる原因の調査、検討
  - 必要に応じてオンラインでの脆弱性等の検査等
  - 原理的に誤認可能性が極めて低いようなケースではただちに次のステップへ
- PCをネットワークから切り離す
  - シャットダウンはしない。LANケーブルを抜くだけ
- 不正プログラムの可能性を調査
  - ウイルス対策ソフトでのフルスキャン
  - スパイウエア対策ソフトでの検査
  - PC上の起動プロセスの調査
  - ファイル、レジストリ等の改ざん、痕跡の調査

不正プログラムがみつかったら

- 一般に広く知られている不正プログラム、ウイルス対策ソフトで検出可能なもので、感染先が一般のPC等であり感染原因や経路が明らかな場合
  - 駆除・復旧作業を行う
- 正体不明のものや、感染経路が不明なもの、ボット系不正ソフトウエアなどで重要なサーバや重要情報を扱う人のPCが感染先である場合
  - 詳細な解析、影響分析の必要性を検討する
  - 必要に応じて現状保存、専門家による解析（フォレンジック）を行う

不正プログラムの駆除、感染からの復旧

- ボット活動をするウイルス、ワームや正体不明のもの
  - OSから再インストールすることを強く推奨　（本体駆除のみでは不十分な場合が多い）
- バックドアを作るもので、そのPCを感染後モバイル環境等で利用していたような場合
  - OSから再インストールすることを推奨（感染後に侵入され、他の不正操作を加えられた可能性を考慮）
- その他のウイルス、ワーム、スパイウエア等
  - ウイルス対策ソフト、駆除ツールなどを利用して駆除
  - ウイルス対策ソフトウエアメーカーなどが提供する情報に基づいて手動操作で駆除

で、これ全部、僕がやるの？・・・・ orz

- 上司の答えはとりあえずＹＥＳなんだけど・・・
- 企業のセキュリティ管理者（というより担当者）は大変かも・・・・・
- でも、全部アウトソース（まるなげ）しろ、とは言いたくない・・なぜなら最後は自社の責任だから！！
- 事故の結末をよく考えてみよう
  - SIer、MSSPは最悪でも「出入り禁止」と契約範囲内の賠償責任で「すんでしまう」
  - でも、自社の社長は、もしかしたら「クビ」かも・・・
  - 少なくとも、CSOは更迭だな・・・・

↑
Chief Scapegoat Officer

体制整備の考え方

- 社内のセキュリティ管理体制を明確にしよう
  - セキュリティポリシーに基づき、最高責任者（CISO）として経営層をまきこもう
  - 自社のセキュリティに自身で「責任」を持つ体制
- 最低限1～2名のセキュリティ技術の専門家（Generalist）を確保しよう　（養成 or 採用）
  - CISO自身がそうでない場合は、その補佐役が必要
  - セキュアド、CISSPなどの資格保有者が望ましい
  - ある程度の現場経験が必要（たとえば、監視や対応のアウトソース先専門家と会話が成り立つ程度のレベルで）
- アウトソースする場合は、社内の管理体制における位置づけと、責任範囲を明確に
- アウトソース先のパフォーマンスを時々チェックしよう

最後に

- 不正プログラム対策に「完全」はない
  - セキュリティ全般について言えることだが・・・・
- 出来ることをまず、確実にやろう
- 日常の運用の中で得られる経験を大切に
- 情報を出来るだけ多く集め多面的な分析を
- ポリシー、管理体制を含め、総合的な対策を

参考文献、参考URL

- CSI/FBI Computer crime and security survey 2005
  - http://www.gocsi.com/
- ITmedia「今ウイルス対策を再考する」
  - http://www.itmedia.co.jp/enterprise/special/0407/virus/
- @IT「変幻自在なBOTの正体を暴く」
  - http://www.atmarkit.co.jp/fsecurity/special/76bot/bot01.html
- @IT セキュリティ情報マネジメント（SIM）概論
  - http://www.atmarkit.co.jp/fsecurity/special/71sim/sim01.html
- Impress Watch 2001年12月7日記事
  - http://www.watch.impress.co.jp/broadband/news/2001/12/07/virus.htm
- 秀和システム刊　情報セキュリティプロフェッショナル教科書

Contact e-mail:　futagi@kazamidori.jp