証拠保全ガイドライン 第3版の解説

2013年11月

デジタル・フォレンジック研究会 理事
「技術」分科会WG 座長
（所属元：サイバーディフェンス研究所 理事）

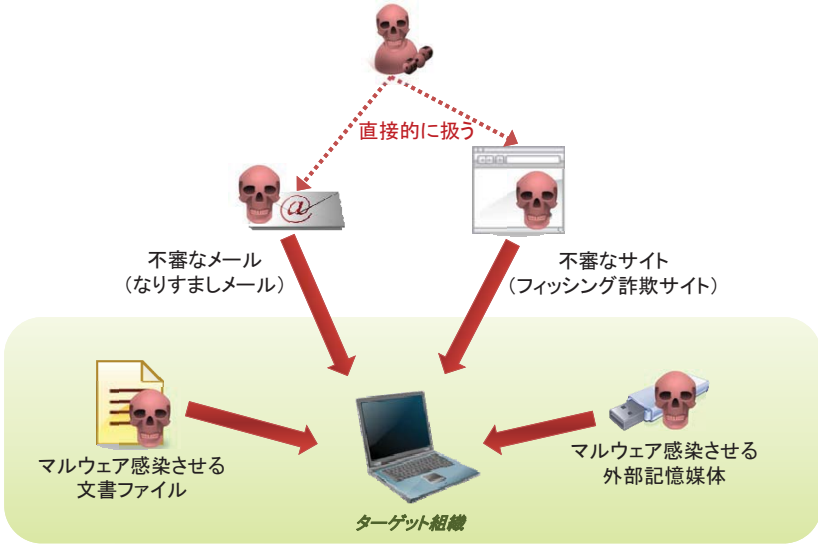
トピック 1

改訂にあたっての状況認識

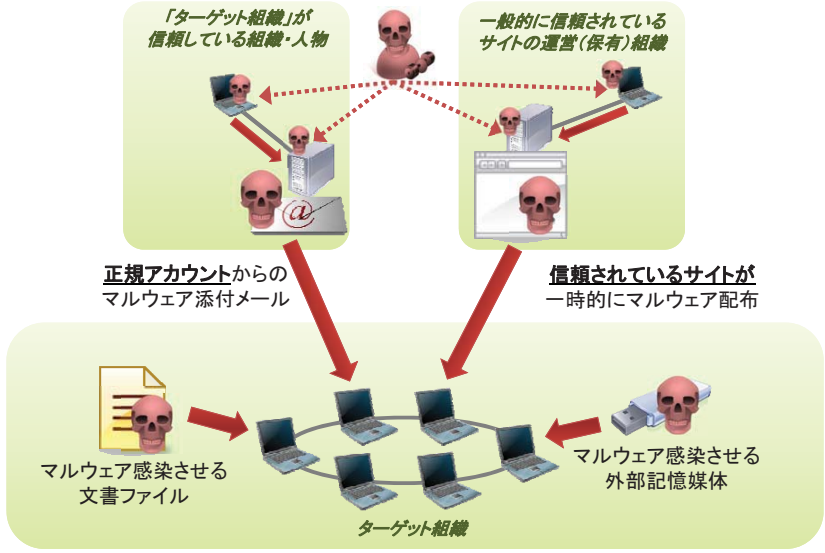
アジェンダ

1. 改訂にあたっての状況認識
2. 改訂ポイント：ネットワーク・フォレンジック
3. 改訂ポイント：相関的な分析
4. 今後の改訂の方向性について

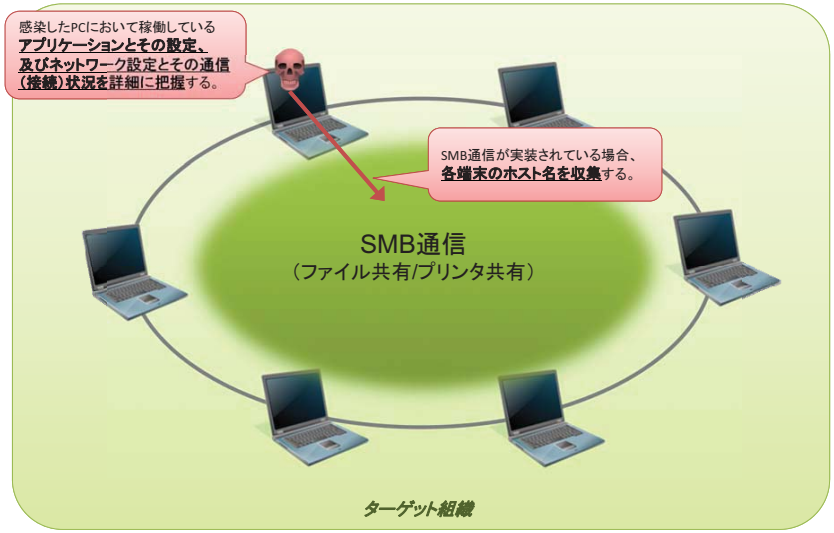
昨年まで、よく見られた「標的型攻撃」



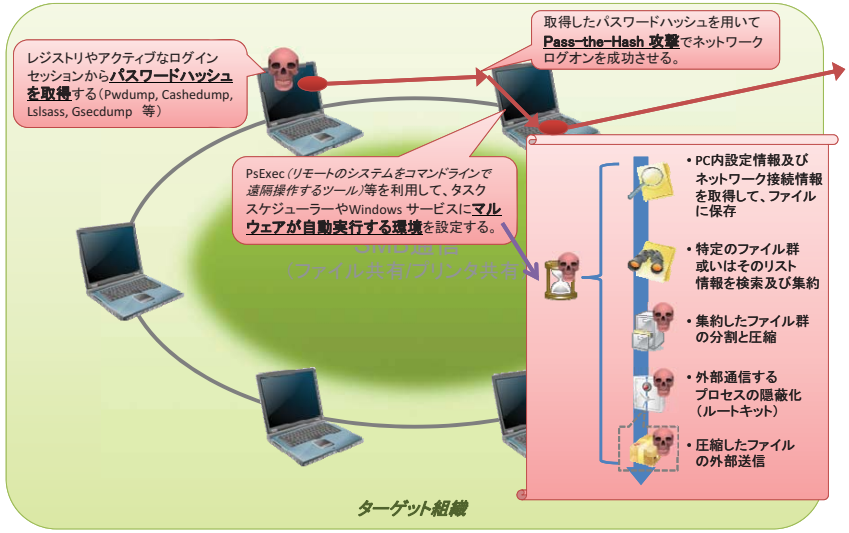
今年（2013年）、よく見られる「標的型攻撃」



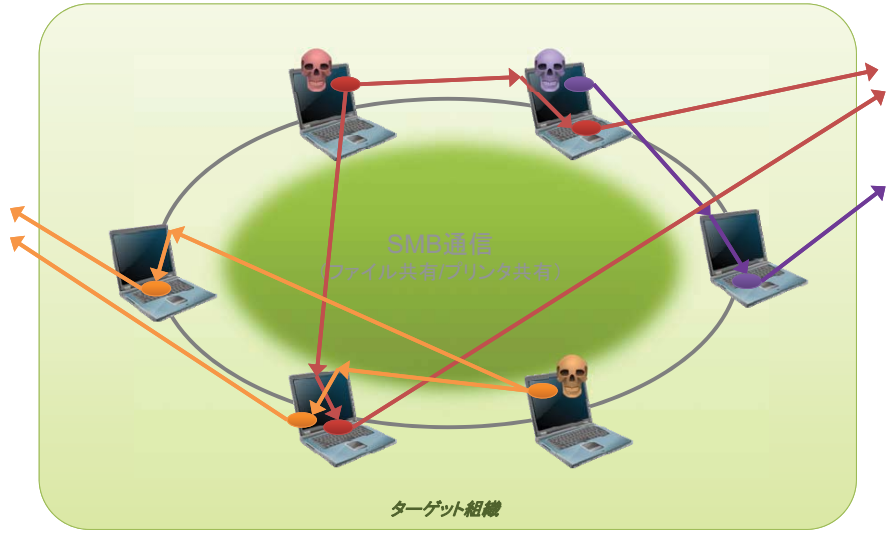
今年（2013年）、緊急対処支援で最も多かった「標的型攻撃」



今年（2013年）、緊急対処支援で最も多かった「標的型攻撃」



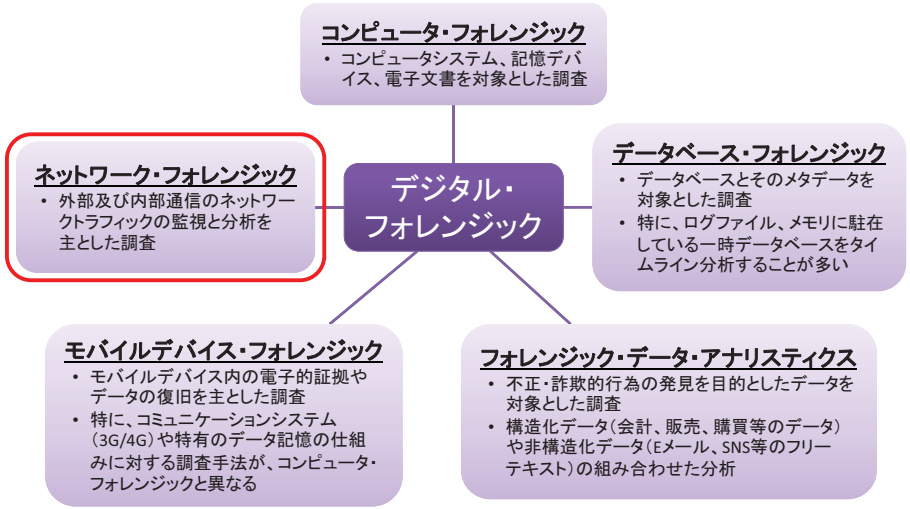
今年（2013年）、緊急対処支援で最も多かった「標的型攻撃」



トピック 2

改訂ポイント：ネットワーク・フォレンジック

ネットワーク・フォレンジックの位置付け



ネットワーク・フォレンジックとは

ネットワーク・フォレンジックとは、「セキュリティ上の攻撃や問題を発生させるインシデントの発生源を発見するために、ネットワーク上のイベントをキャプチャ、記録、分析すること」である。

Marcus J. Ranum

Marcus J. Ranum is a computer and network security researcher and industry leader. He is credited with a number of innovations in firewalls, including building the first Internet email server for the ... Wikipedia

Born: November 5, 1962 (age 51), New York City, New York, United States

Education: Johns Hopkins University

Books: The myth of homeland security

http://en.wikipedia.org/wiki/Marcus_J._Ranum

セキュリティ・システムの設計や開発の専門家として世界的に有名。プロキシー型ファイアウォールの発明者として、1980年代に最初の商用ファイアウォールを提供。多くのセキュリティ製品を設計し、その中にはDECのSeal（Digital Equipment Corp, Secure External Access Link）やTIS（Trusted Information Systems）のFirewall toolkit、Gauntletファイアウォールがある。

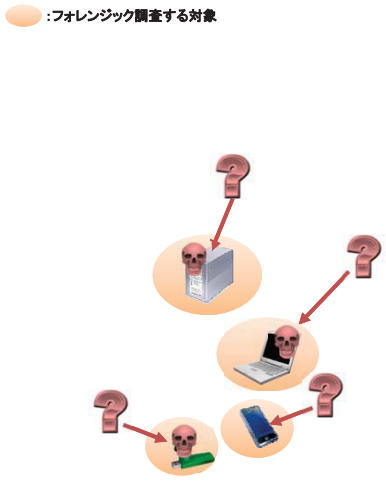
ネットワーク・フォレンジックの分析アプローチ

- “Catch-it-as-you-can”（可能な限りの捕捉）
  - 全てのパケットを特定のポイントでキャプチャして記憶媒体に書き込んでいき、事後、ひとまとめになったデータを分析すること。
  - このアプローチは、巨大な記憶媒体が必要になる。

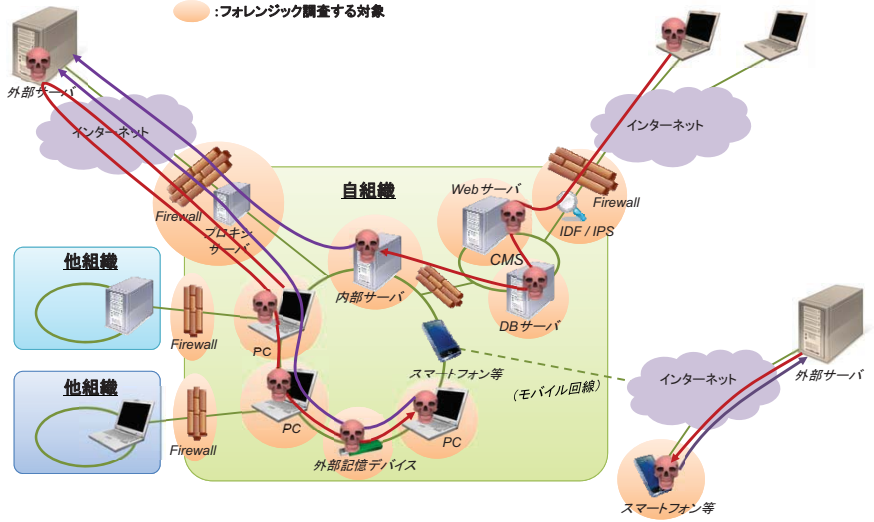
交差点で車に気を付けることを教える歌の題名

- “Stop, look and listen”（止まって、見て、聞いて。）
  - 通過するすべてのパケットを逐次分析し、事後に分析が必要となる特定の情報のみを保存すること。
  - このアプローチは、高速プロセッサが必要になる。

コンピュータ・フォレンジックのイメージ



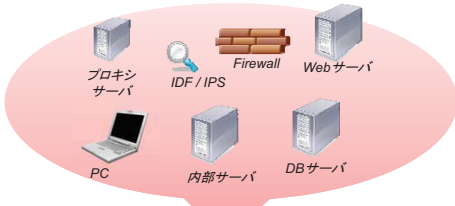
最近のデジタル・フォレンジックの調査対象



「コンピュータ・フォレンジック」と「ネットワーク・フォレンジック」

・ハードディスク等から証拠となる**ファイルを抽出**
・サーバー等のログファイルから不正アクセスの**記録を特定**
・破壊や消去されたディスクを復元して証拠となる**データを確保**

電磁的証拠の保全手続き



・アクセス（エラー）、認証（可否）、イベント等の**ログ等の情報を確保**

・各機器からの**ログ等の情報同士の相関関係や因果関係を見出し**つつ、段階的に攻撃プロセスを特定

サイバー攻撃の実態解明

「コンピュータ・フォレンジック」と「ネットワーク・フォレンジック」

- フォレンジック対象となる「電磁的証拠」と「ログ等の情報」の違い
  - 「電磁的証拠」は、コンピュータ・システムにより必然的に記録されるものである。
    - コンピュータ・システムの種類が少なければ、電磁的証拠の保全手続きのための統一された技術や手法を確立することができる可能性が高い。

  - 「ログ等の情報」は、設計者や運用者の設定したルールにより記録されるものである。
    - プロダクト（機器）によっては、必要なルールを設定できないものがある。
    - 設計者や運用者によって設定するルールが大きく異なる場合がある。
    - ネットワーク化されたシステムは、マルチベンダー化のために多様化されているため、確保したログ等の情報の構成要素に大きなばらつきがある。
    - ログ等の情報は、時刻が全て一致しているという前提がある。
    - 一般的に、ログ等の情報は膨大な量となる。

トピック 3

改訂ポイント：相関的な分析

様々な相関的な分析の例（1）

① 特定**端末で事象**発生

不正挙動の目視確認・推定

② 特定端末のフォレンジック調査
（コンピュータ・フォレンジック）

不正挙動と外部通信先を特定

③ プロキシログ等の調査
（ネットワーク・フォレンジック）

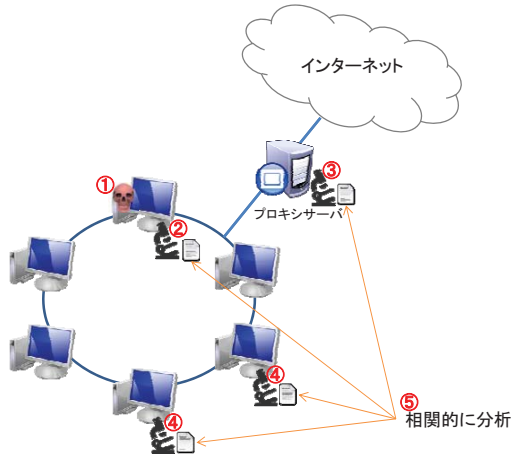
他の不正通信端末を特定

④ 他の端末のフォレンジック調査
（コンピュータ・フォレンジック）

不正挙動と外部通信先を確認

⑤ 特定端末とプロキシログ等の
調査結果を相関的に分析

**分析結果に基づく実態解明は
できるが、完全ではないことが
多い。（残存している可能性）**



様々な相関的な分析の例（2）

① NW不正監視**装置で検知**

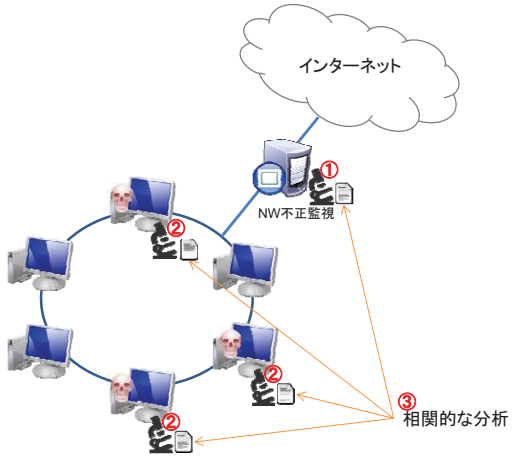
不正通信端末の特定

② 特定端末のフォレンジック調査
（コンピュータ・フォレンジック）

不正挙動と外部通信先を特定

③特定端末の調査とNW不正監
視装置の出力間の相関的な分析

**分析結果に基づく実態解明は
できるが、完全ではないことが
多い。（残存している可能性）**



様々な相関的な分析の例（3）

① 適用された**ブラックリスト**中
のIPアドレスの通信を検知

該当するゲートウェイサーバを特定

②特定端末のフォレンジック調査
（コンピュータ・フォレンジック）

不正挙動と外部通信先を特定

③ プロキシログ等の調査
（ネットワーク・フォレンジック）

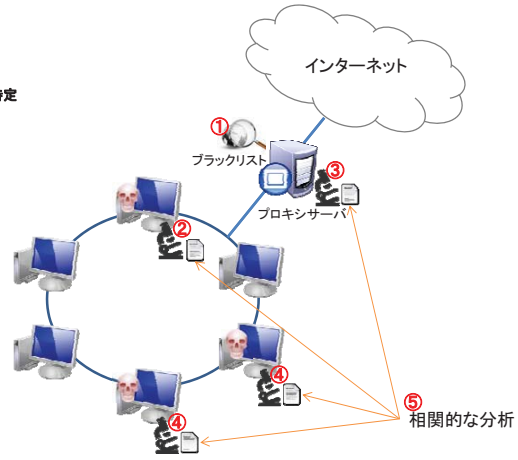
他の不正通信端末を特定

④ 他の端末のフォレンジック調査
（コンピュータ・フォレンジック）

不正挙動と外部通信先を特定

⑤ 特定端末とプロキシログ等の
結果間の相関的な分析

**分析結果に基づく実態解明は
できるが、完全ではないことが
多い。（残存している可能性）**



「コンピュータ・フォレンジック」と「ネットワーク・フォレンジック」

- 「ログ等の情報同士の相関関係や因果関係を見出し」の実態
  - ログ等の情報の構成要素にばらつきが多いため、信頼出来る「共通キー」を見出すことが重要となる。
    - IPアドレス、タイムスタンプ、ホスト名、プロセスID、プロトコル等が共通キーになることが多い。
    - 特に、アプリケーションの活動履歴の調査から得られたタイムスタンプが、重要な手がかり（他のログ等の情報で利用する「共通キー」）になることが多い。
  - 期待通りにログ等の情報が記録されていることは稀である。
    - 他の類似事象（攻撃）の分析情報を参考にする、或いは調査対象のネットワーク化されたシステムの脆弱な部分を見極めながら、仮説と検証を根気よく繰り返すことがある。
  - 調査する者は、高いレベルのネットワークスキルと豊富な製品知識に加え、最新の攻撃技術や手法に関する知識・知見が必要となる。
    - 特に、最近は、設計者や運用者が想定しなかった手法によるサイバー攻撃が発生しているため、柔軟な発想や気づきができることが求められる。

相関関係は因果関係を含意しない (Correlation does not imply causation)
- 2つの変数の相関が自動的に一方がもう一方の原因を意味するというわけではないことを強調したものである
- もちろん、そのような関係がある場合を完全に否定するものではない

引用元：http://morrist.edublogs.org/2012/10/02/19/

トピック 4

今後の改訂の方向性について

第10期第3回「技術」分科会WG（10/16）の議論結果

1. **メモリダンプについて**
   - 揮発性情報の重要性
   - 論理ボリュームレベルで取らなければならない状況
   - マルウェアによる、ログの一部消去や破壊
   - いかに簡単に効率よくメモリダンプするか（周囲の情報を傷つけずに）
   - マルウェア感染時の対応
   - エージェントを入れ込むフォレンジックツール（エージェントを入れる場合は、最初から入れていることが多い。）
   - 国内の手続き的に問題はないか?
   - ライブフォレンジックとの整理
2. **電源断について**
   - 電源により、HDが壊れた事例はあまりない
   - OSが立ち上がらない場合はある
   - 電源断にする目的は、ファイルのタイムスタンプを変更させない目的もある
   - 不正が発覚して、内部で対応した後に依頼が来る（すでに電源断の状態）場合もある
   - SSD に関すること
3. **ケース分け（フォレンジックをする場を明記）**
   - 懲罰（内部犯行特定?）目的 / 攻撃対処目的
   - ○○○ フォレンジックを行う場
   - RAIDコントローラーの場合の電源断
   - ケースを想定して例示を示す
   - 既存の辞典/リファレンスにリンクを張る
4. **VMで動いている場合の証拠保全**
   - クラウドサービス事業者の場合（パブリック）
   - 組織内で VM を実装している場合（プライベート）
   - スナップショットで保存
   - クラウド環境での対応限界
5. **認証や暗号化された状態**
   - 保全時に暗号化された状態の対処プロセス
6. **手順の明確化・視覚化**
   - フローチャート
   - 手順以外のものをノートやリンクで説明
7. **製造者の関与**
   - PC分解時にHDベンダー（メーカー）を関与させるかどうか
8. **具体的な分析手法**
   - 特に、ネットワーク・フォレンジックの分析対象（NAT、DHCP、Pxoxy等 ）

本資料に関する連絡先

名和 利男（Toshio NAWA）
デジタル・フォレンジック研究会
理事／「技術」分科会WG 座長
Email: nawa@digitalforensic.jp
SNS: about.me/nawa