デジタルフォレンジック

武蔵(熊本大)*、湯浅(高エネ研)、
山田(富士通)、須永(富士通SSL)
*リーダー

SS研セキュリティマネージメントWG
フォレンジック・グループ

背景

- 個人情報漏洩
- 情報内部統制
- ソフトウェアライセンス管理
- ECサイトの事例
- 警察捜査等への協力(ログ提出)

定義: フォレンジック(法科学)

- フォレンジック(Forensics: 法科学)
- メディカルフォレンジック(法医学)
- デジタル鑑識:ICTを利用した鑑識
- デジタルフォレンジック:
  - コンピュータフォレンジック
  - ネットワークフォレンジック

デジタルフォレンジックとは何か

- 過去に起こったインシデントを科学的に立証するための証拠を保全・収集・分析することを意味する
- サーバ等の情報機器のログやシステムの状態が記録されたメディアについて詳細に調査解析を行う手法および技術を含む

刑事(民事)事件で警察へのログ提出の具体例

- A大学でネットワークストーカの犯罪捜査としてメールサーバのシステムログを提出
- B大学でたてられたフィッシングサイトに関連して被害が発生、Webサーバのログを提出し捜査に協力
- テロ予告など犯罪性の強い書き込みに関する警察への捜査協力
- 個人情報漏洩時のアクセスログ

e-Discovery

- e-ディスカバリとは:電磁的な証拠開示
- セキュリティインシデントに関連する訴訟では、IT部門と総務部門がその対応を引き受けざるを得ない
- そんな場合でも、ログをすべて提出する必要はなく、必要な範囲を適切に提出すればよいが、
  - 必要な三要素:証拠保存、解析、報告
  - 課題: 膨大なデータの取り扱い、多様な文字コードへの対応
- 多くの機関では、経験がなく急な事態に適切に対応できる体制になっていない

情報機器のトレーサビリティ

- ログの保全は必須である
  - 期間は？
    - 判例では3年がある
  - 完全性はどう保護するか
    - ログの分散バックアップ保存
- 収集の方法の一例
  - PCログエージェントとログ収集サーバ
  - メールサーバアプライアンスのログのフォレンジック解析

パケットキャプチャリングの技術

- ネットワークタップ（UTPタップ、ファイバタップ）やミラーポートの利用
- libpcapライブラリを利用したパケットダンプ
  - tcpdump
  - snort
    - https://www.ssken.gr.jp/lib/nl/2004/stg/2/3_watanabePPT.pdf
- フルロギングあるいはヘッダロギング(フロー)
- ターゲットロギング(ARGUS)
  - http://www.qosient.com/argus/index.htm
  - http://www.hawkeye.ac/micky/SA/AuditTrail.files/frame.htm
- 課題
  - 大量のストレージが必要
  - 雇用契約との整合性

ログの保全技術

- 時間認証局の採用？
- 暗号化
- ログデータのハッシュ化
- サーバサイドの完全性の保持
- ユーザクライアント側の完全性の保持
- 組織ワイドのシスログ受信サービスの必要性
- UDP/TCP通信で十分か、あるいはSSL化が必要か

フォレンジックで使われる技術

- キャプチャリングツール
  Gigabitネットワークでの確実な保存への期待
- ネットワーク
  メール(SMTP)アーカイバ
  Web(HTTP)アーカイバ
  KVMやRDP,VNC経由でのPC操作画面保全
- サーバ(改ざんされないログ)
  アクセス権(特権)の分離：SecureOS
- クライアント
  画面キャプチャ
  キーロガー
- 調査、解析ツール
  ハードディスクのイメージファイルの作成(取得)
  取得ファイルからの調査、解析
  調査結果レポート

フォレンジック製品例

- キャプチャリングツール
  SwiftWing SIRIUS LCS
  GigaProve
- ネットワーク
  NetEvidence, MSIESER, Net Detector, PBH
  NetEnrich
- サーバ(改ざんされないログ)
  SHieldWARE
- クライアント
  ESS REC
- 調査、解析ツール
  EnCase

マネージメントの視点から

- アウトソーシング化
  - 大学でシステムを持たない
  - 施設部や設備課に委譲
  - ログデータの保存をアウトソーシング
  - 解析のアウトソーシング
    - アウトソーシング先の技術レベルが問題となる
- 将来、新しいビジネスモデルへと成長する可能性がある

参考文献・参考リンク

- 上原哲太郎, “ディジタルフォレンジック”, IPSJ Magazine Vol.48, No.9, pp.889-898 (2007)
- 辻井重男 監修, “デジタル・フォレンジック事典”,日科技連出版社, ISBN4-8171-9208-9
- 特定非営利活動法人デジタル・フォレンジック研究会
  - http://www.digitalforensic.jp/