

第1章 フォレンジック概論

- 1.1 セキュリティインシデント対応
- 1.2 CSIRTとは
 - 1.2.1 CSIRT体制の確立
 - 1.2.2 セキュリティインシデント対応の標準化
 - 1.2.3 必要な資器材の準備
 - 1.2.4 役割・サービスの周知
 - 1.2.5 セキュリティインシデント対応訓練
- 1.3 インシデント対応の手順
 - 1.3.1 インシデント対応のプロセス
 - 1.3.2 セキュリティインシデント対応の流れ
- 1.4 サイバー犯罪捜査
- 1.5 デジタルフォレンジック
 - 1.5.1 デジタルフォレンジックの対象となるデジタルデータ
 - 1.5.2 デジタルフォレンジックの分類

第2章 初動対応

- 2.1 セキュリティインシデント発生時の初動対応
- 2.2 現況確認
- 2.3 被害拡大防止
- 2.4 情報収集と分析
- 2.5 ライブフォレンジック
- 2.6 レベル判定

第3章 保全

- 3.1 証拠保全
- 3.2 保全対象の決定
- 3.3 保全用デバイスの準備
- 3.4 保全用ツールの準備
- 3.5 メモリイメージの保全
 - 3.5.1 Windowsのメモリイメージ保全
 - 3.5.2 Linuxのメモリイメージ保全(1)
 - 3.5.2 Linuxのメモリイメージ保全(2)
 - 3.5.3 揮発性データの保全
- 3.6 ハードディスクの保全
 - 3.6.1 オンラインでのハードディスク保全(Windows)2/1
 - 3.6.1 オンラインでのハードディスク保全(Windows)2/2
 - 3.6.2 オンラインでのハードディスク保全(Linux)
 - 3.6.3 オフラインでのハードディスク保全(Windows/Linux)2/1
 - 3.6.3 オフラインでのハードディスク保全(Windows/Linux)2/2

第4章

メモリーイメージ解析

- 4.1 メモリーイメージ解析の概要
- 4.2 メモリーイメージ解析用ツール
- 4.3 volatilityによるメモリーイメージ解析
 - 4.3.1 volatilityの実行形式
 - 4.3.2 メモリーイメージのバナー情報出力(imageinfo)
 - 4.3.3 ソケット情報(通信状態)の出力(netscan)
 - 4.3.4 実行中プロセス一覧の出力(pslist/pstree)
 - 4.3.5 隠ぺいされたプロセスの出力(psscan)
 - 4.3.6 セッション情報の出力(sessions)
 - 4.3.7 タイムライン情報の出力(timuliner)
 - 4.3.8 コマンド実行履歴の出力(userassist)
 - 4.3.9 マルウェア情報の出力(malfind)

第5章

ハードディスクイメージ解析

- 5.1 ハードディスクイメージ解析の概要
- 5.2 ハードディスクイメージ解析用ツール
- 5.3 OSFrensicによる調査(ケース作成)
 - 5.3.1 OSFrensicによる調査(ディスクイメージの登録)
 - 5.3.2 ファイルシステム参照
 - 5.3.3 ファイル検索
 - 5.3.4 ユーザーの操作履歴の調査(UserAssist/MRU/ブラウザ/デバイス)
 - 5.3.5 ユーザ操作の調査(Prefetch)
 - 5.3.6 ファイルの完全性確認
 - 5.3.7 メール解析1/2
 - 5.3.7 メール解析2/2