



情報セキュリティ 実践トレーニング

インシデント調査トレーニングの決定版!!
実践力で差をつけよう!!
現場で役立つ即戦力の養成!!



我々の情報システムは、Web ページの改ざんやマルウェアの感染に代表されるサイバー攻撃の危険性に常にさらされています。また意図的／偶発的な情報漏えいなど、組織内部に起因するセキュリティ侵害も後を絶ちません。ひとたびセキュリティ・インシデント（事故）が発生すると、情報システムを運営する組織には適切な対応と再発防止のための改善が求められます。そのためには速やかなインシデント調査を実施することでインシデントの発生事象と影響範囲を明らかにし、攻撃／感染などの経路を特定するとともに、根本的な原因の解明を行う必要があります。本トレーニングではフリーで入手可能なさまざまなツールを使用しハンズオン実習を行いますので、インシデント調査に必要な知識はもとより、現場ですぐに役立つ実用的な技術を身につけることができます。

| | | | |
|-------------|------------------------------------|------------|-------------|
| 主催 | 合同会社セキュリティ・プロフェッショナルズ・ネットワーク | | |
| 日程 | トレーニング導入セミナー | 10月20日 | 13:00～16:00 |
| | ネットワークパケット解析コース | 10月22日～23日 | 9:30～18:00 |
| | ファイルシステム解析コース | 10月24日～25日 | 9:30～18:00 |
| | Windows インシデント調査コース | 10月26日～27日 | 9:30～18:00 |
| 会場 | ヒートウェーブITアカデミー恵比寿校(JR恵比寿駅西口から徒歩1分) | | |
| 募集人数 | 各コース 18名 | | |
| 受講料 | 各コース 105,000円 (税込み) | | |
| 応募締切 | 10月10日 (水) | | |

※ トレーニング導入セミナーは各コースの受講者に限り参加できます (参加費無料)

<http://www.Sec-Pro.Net/training.html>



▶ ネットワークパケット解析コース

本コースではトラブルシューティングやインシデント調査で必要とされるパケットのキャプチャや解析を行う方法を解説するとともに、トラブルやインシデントを再現してキャプチャしたパケットを実際に解析することで、実務で役立つパケット解析技術を習得します。

- 1) パケット解析とは
- 2) 使用するツールの説明
- 3) パケットをキャプチャする場所
- 4) パケットをキャプチャする方法
- 5) キャプチャしたパケットの解析

▶ ファイルシステム解析コース

本コースではファイルシステム解析用のフリーツールとして代表的な TSK (The Sleuth Kit) およびその GUI フロントエンドである Autopsy を主に使用することで、より深くファイルシステムを理解するとともに、実用的なファイルシステム解析手法に関する知識と技能を習得します。

- 1) ハードディスクとファイルシステム
- 2) TSK : The Sleuth Kit
- 3) Autopsy
- 4) 非使用領域とスラックスペース
- 5) キーワード検索
- 6) イメージデータをマウントした調査
- 7) タイムライン解析

▶ Windows インシデント調査コース

本コースではインシデント調査に必要とされる Windows OS の技術情報を解説すると同時に、各種のフリーツールを用いた Windows システムの解析を実習することにより、幅広い Windows インシデント調査技法を習得します。

- 1) レジストリ解析
- 2) イベントログ解析
- 3) パスワード解析
- 4) ファイル解析
- 5) メモリ解析
- 6) タイムライン解析
- 7) EFS と BitLocker

講師略歴



吉田英二

1999年から情報セキュリティ系のベンチャー企業にてネットワーク・セキュリティの調査や研究に従事し、今までに数多くの企業や省庁のペネトレーション・テストを担当。個人活動として penetration technique research site というペネトレーション・テストに用いる技術について調査や開発を行うサイトを開設して、脆弱性や侵入技術の研究結果を公開している。2007年独立、セキュリティ監査や講演・教育・執筆活動を行う。2008年、合同会社セキュリティ・プロフェッショナルズ・ネットワークを設立。セキュリティキャンプ講師(2006年～2012年)



塩月誠人

1985年鹿児島大学理学部地学科卒業。1996年よりWindows NTを利用したISP環境の構築・運用管理に参画した後、情報セキュリティ系ベンチャー企業にてセキュリティ監査や各種セキュリティコンサルティング業務に従事。その後、中央大学における実践的セキュリティ人材育成に携わり、2008年、合同会社セキュリティ・プロフェッショナルズ・ネットワークを設立。情報セキュリティ大学院大学客員講師、セキュリティキャンプ講師(2005年～2009年)、セキュリティキャンプ実行委員(2004年、2008年～2009年)、IPA情報セキュリティセミナー講師(2009年)。

※本資料に掲載されている社名、団体名、製品名等は、それぞれ各社・各団体の商標または登録商標です。

お申し込み／お問合せ：

ヒートウェーブITアカデミー TEL:03-5725-2920

東京都渋谷区恵比寿南 1-1-1 ヒューマックス恵比寿ビル 4F

FAX:03-3791-0390 E-Mail:tokyo@heatwavenet.co.jp