

第 21 回サイバー犯罪に関する白浜シンポジウム

セキュリティ道場のカリキュラム案

■カリキュラム案

※開催までに内容を一部変更する可能性があります。

<入門編>

1. テーマ

客観的な証拠を探すために必要となる電磁的記録媒体の証拠保全の方法を学び、フォレンジック（デジタル捜査）における初動捜査技術について習得します。初動捜査技術については、解析技法を講師による実機デモを通じて紹介いたします。

2. 内容

(1) サイバー捜査基礎

デジタルエビデンスの連鎖(環境保全、証拠の立証、時刻)による完全性の担保や、サイバーに係わる事案における迅速な証拠作成などについて

(2) ハンズオン演習

ツールを活用した効率的な保全技法や揮発性・不揮発性データの解析技法の実機デモ

<実践編>

1. テーマ

サイバー犯罪やサイバー攻撃等で行われる手口を学び、感染活動の手口、不正プログラムの痕跡調査の勘所を習得します。習得した攻撃者の手口に応じた模擬事案環境に対して、実機による揮発性・不揮発性データの解析技法の演習を行います。

2. 内容

(1) サイバー犯罪やサイバー攻撃等で行われる手口の解説

(2) 揮発性情報を活用した解析技法の演習

(3) 揮発性・不揮発性データを組み合わせた解析技法の演習

(4) 模擬事案分析演習

■講師

安田 良明（S & J 株式会社 執行役員 サイバーセキュリティ事業本部 本部長）