# デジタルフォレンジックトレーニング(基礎編)のご案内

**開催概要：**

| | |
|---|---|
| 開催日程 | 2016 年 12 月 5 日(月)～12 月 9 日(金)　5 日間<br>全日程：10:00 ～ 18:00 |
| 会場 | TKP 神田ビジネスセンターANNEX<br>カンファレンスルーム 8H<br>■　住所<br>〒101-0053<br>東京都千代田区神田美土代町 1<br>住友商事美土代ビル 8F<br>■　地図<br>http://www.kashikaigishitsu.net/facilitys/bc-kanda-annex/access/<br>  |
| 言語 | 英語、日本語同時通訳 |
| 持ち物 | 筆記用具 |
| 受講料 | 756,000 円 / 1 名(税抜) |
| お支払方法 | 別途ご案内申し上げます。 |
| お問い合わせ・<br>お申込み | 株式会社カスペルスキー<br>ビジネスデベロップメント<br>サイバーセキュリティトレーニング事務局<br>jp-sis@kaspersky.com |

## レベル２：デジタルフォレンジック

**概要：**

セキュリティインシデントが発生した際のインシデントレスポンスについて標準的なデジタルフォレンジック解析の手法を習得します。また、実際のマルウェアに感染した端末のイメージを使ってデジタルフォレンジックの演習を行います。

**受講の効果**

- ✓ 標準的なインシデントレスポンスができるようになります。
- ✓ インシデント発生端末からの証拠取得と適切な証拠の取り扱いができるようになります。
- ✓ 取得した証拠からインシデントの再現と標準的なフォレンジック解析ができるようになります。
- ✓ Windows コンポーネント、ブラウザー、メールクライアントの解析からインシデント発生原因、侵入経路、マルウェアを特定することができるようになります。

**１日目：**

フォレンジック調査で成果を出すためには、適切なインシデントレスポンスが必要です。インシデントレスポンスで最も重要となるメモリ、ハードディスクイメージなどの証拠を取得する方法を習得します。

また、実際のインシデントレスポンスでは証拠取得が出来ず、インシデントが現在発生している状態で調査しなければならないケースもあります。このようなケースに備えライブレスポンス(ライブ解析)の方法についても習得します。

| | |
|---|---|
| デジタルフォレンジック入門 | ● フォレンジック調査で使われる用語の解説<br>● フォレンジック調査のプロセスと進め方<br>● フォレンジック調査に必要なハードウェア、ソフトウェア |
| インシデントレスポンスの基礎 | ● インシデントレスポンスの概要と進め方<br>● インシデントレスポンスのシナリオ<br>● 事例 |
| 初動対応：<br>ライブレスポンスと証拠採取 | ● ライブレスポンス<br>➢ ライブレスポンス(Sysinternals)<br>● 証拠採取<br>➢ フォレンジック CDs(Helix, DEFT)<br>➢ メモリダンプの取得方法<br>➢ リモート証拠採取<br>➢ ディスクイメージの取得(FTK, dd, HDD)<br>➢ SSD ドライブからイメージ取得する際の注意点について<br>➢ 取得イメージのマウント |

**２日目、３日目：**

レジストリは採取した証拠のなかで一番重要な情報を含むコンポーネントとなります。レジストリを解析することでインシデント発生端末のシステム情報、スタートアップ設定、セキュリティポリシー、ウェブの閲覧履歴、ユーザー・システムの操作履歴などを確認することができます。また、マルウェアはユーザーのログオフ後、再起動後も活動が続けられるよう、レジストリに痕跡を残すケースがありマルウェアが残す痕跡の確認方法についても習得します。

３日目は Windows のイベントログ、link ファイル、タスク、prefetch ファイル、recycle bin ファイルの解析方法を習得します。

| | |
|---|---|
| レジストリ解析 | ● レジストリの構造<br>● ユーザプロファイル<br>● レジストリの確認項目(タイムゾーン、ネットワークアドレス、OS、autostart に登録されている実行ファイル、ブラウザーの履歴)<br>● レジストリ解析ツール(MiTec WRR)<br>● ユーザーとシステムのタイムライン解析(RegRipper) |
| Windows コンポーネントの解析 | ● イベントログ<br>● Link ファイル<br>● タスク<br>● Prefetch ファイル<br>● Recycle bin ファイル |

**４日目：**

ウェブから侵入するマルウェアによるインシデントの場合、ウェブの閲覧履歴、キャッシュファイル、ブックマーク、cookie などの解析が重要になります。ここでは取得したイメージからこのような情報を抽出し、解析する手法を習得します。

標的型メールによるインシデントの場合、メールデータの解析が必要になります。ここでは、Outlook、Lotus Notes、Web メール環境を利用した端末から取得したイメージからメールデータの抽出と解析方法を習得します。

| | |
|---|---|
| ブラウザーフォレンジック | ● ブラウザー毎のデータ保存領域の確認<br>● IE の解析方法<br>● Chrome の解析方法<br>● Firefox の解析方法 |
| E-Mail フォレンジック | ● クライアント-サーバの構成<br>● Outlook<br>● Lotus Notes<br>● Web メール |

**５日目：**

最終日は演習を実施し、これまでに修得した手法の理解を深めます。