サイバー犯罪と戦う捜査機関／CSIRT向けトレーニングのご案内

EY新日本有限責任監査法人
Forensics事業部

近年、WindowsやMacといった従来のPC型デバイスに加えて、スマートフォンやタブレットなどの携帯型デバイス、これらと連携するクラウドなどのWebサービスの台頭により、人々のIT機器の利用方法・形態が劇的に変化しています。

さらに、IT機器の多様化に伴い、デバイス固有のOSやプライバシー保護を目的としたセキュリティの強化、複数人でデータを共有するアプリケーションなど、さまざまなテクノロジーが絶え間なく開発されています。それに加えて、サイバー攻撃の巧妙化・複雑化も加わり、フォレンジック調査やインシデント対応においては、広範な視点・技術が求められているのが現状です。

上述のような状況を踏まえ、当法人が提供するトレーニングでは、現代において主に使用されているデバイスの構成やOS、ファイルシステムに関連する基礎、サイバー攻撃のトレンド、実際に調査を実施する際の観点、ならびに保全・解析手法を中心に解説いたします。

トレーニングコースおよび開催日程（予定）

現在、下記の日程にて当法人パートナー企業の株式会社ワイ・イー・シー主催でオンサイト研修を実施予定です。お申込み、お問い合わせは、株式会社ワイ・イー・シーまでご連絡ください。

Tel：042 796 8511
URL：https://www.kk-yec.co.jp/products/forensic/training.html

コース名	日程（予定）
Windows® Forensics※3	東京：2024年1月24日～26日、2024年10月頃 大阪：2024年11月頃
Mac® Forensics※3	東京：2024年2月7日～9日、2024年10月頃 大阪：2024年11月頃
File System Forensics※3	東京：2024年2月20日~21日、2024年10月頃
マルウェア解析基礎	東京：2024年1月31日

※3：該当のトレーニングは情報処理安全確保支援士の特定講習となります。
https://www.meti.go.jp/policy/it_policy/jinzai/tokutei_file/koushu/itiran.pdf

- **日　程**※1
  順次開催（予定）
- **東 京 会 場**※1
  東京ミッドタウン日比谷
  日比谷三井タワー セミナールーム
  または外部のセミナールーム
- **大 阪 会 場**※1
  阪急梅田　大阪梅田ツインタワーズ・ノース セミナールーム
  または外部のセミナールーム
- **対 象 者**
  サイバー犯罪対策や不正調査でフォレンジック技術を利用される官公庁のご担当者様や一般事業会社のCSIRTご担当者様
- **ご持参いただくもの**
  筆記用具、お名刺1枚、受講証※2
- **主　催**
  EY新日本有限責任監査法人
  Forensics事業部または
  株式会社ワイ・イー・シー

※1 日程・会場・プログラム内容は都合により変更となる場合がございます。また、地震・停電などの影響により、開催を中止させていただく場合がございます。予めご了承ください。

※2 お申込み後にお送りいたします。

サイバーインシデントに対峙する
CSIRT担当者向けカスタマイズトレーニング

日程・カリキュラム・実施形態(オンサイト／オンライン開催):カリキュラムはご要望に応じてカスタマイズ可能です（下記カリキュラムは一例）。カスタマイズトレーニングの参加費は別途お見積りいたします。

日程	時間	内容（予定）
1日目	10:00～17:30 （1時間の昼食休憩含む）	▸ サイバー攻撃の概要／サイバーセキュリティキーワード ▸ ログ解析（解析対象ログの種別および概要、主要なログの解析）
2日目		▸ OS（Windows／Linux）が出力するログの解析 ▸ パケットキャプチャデータの解析 ▸ サイバースレットインテリジェンス
3日目		▸ デジタルフォレンジック概要とFast Forensics ▸ Windowsの主要なアーティファクトのタイムライン解析 ▸ メモリ解析（プロセス情報、ネットワーク情報などの調査） ▸ マルウェア解析（表層解析、動的解析、静的解析）

上記のような技術的なカリキュラム以外にも、経営層向けのサイバーセキュリティやインシデント対応などを大局的に捉える際に有用な研修、非IT人材などを対象としたサイバーセキュリティの知識の向上、初動対応の迅速化・被害拡大の防止などを目的とした研修も提供することも可能です。なお、取り扱うトピックや内容などについては、ご要望に応じて柔軟に調整可能です。詳細につきましては、お気軽にお問い合わせください。

フォレンジック・トレーニングの提供実績

当法人が提供するフォレンジック・トレーニングは、2014年10月のサービス開始から2023年11月末までに、のべ1,250名以上の方が受講されております。
EY Japanは、世界的なプロフェッショナルファームである EY のメンバーファームとして「Building a better working world（より良い社会の構築を目指して）」をパーパス（存在意義）に掲げ、サイバー犯罪捜査にあたる捜査機関やサイバーインシデントに対峙するCSIRTの支援に取り組んでいます。

お問い合わせ先

開催日、申し込み以外の個社向けトレーニング等については、下記宛てにお気軽にお問い合せください。

EY新日本有限責任監査法人　Forensicsセミナー担当　事務局
Tel: 03 3503 3292　Email: forensics.cyber@jp.ey.com

- 個人でのご参加はご遠慮願います。また、当法人が競合他社であると判断したご法人担当者様は受講をお断りさせていただきます。予めご了承ください。
- 録音・録画は固くお断りしております。

※ お申し込みによってお知らせいただいた皆様の個人情報につきましては、当セミナーの運営にかかわる事務に利用させていただく他、EY新日本有限責任監査法人およびEY Japan*1 で共有させていただき、今後実施する説明会、セミナー勉強会、研究会発刊書籍および業務内容などのご案内をさせていただく目的以外には使用いたしません。個人情報の管理は、当法人プライバシーポリシー*2 に則って、EY新日本有限責任監査法人が責任をもって行います。
＊1 https://www.ey.com/ja_jp/people/ey-japan　＊2 https://www.ey.com/ja_jp/legal-and-privacy/ey-shinnihon-privacy-policy

Forensics / Cyber Security / Incident Response Training

EY Japan Forensic & Integrity Servicesが提供するトレーニングの特徴

EY Japan Forensic & Integrity Servicesのトレーニングは、各種アーティファクトの内部構造および調査における活用方法に関する講義と、実機を用いたハンズオン形式の演習を通じて、特定のフォレンジックツールに依存しない実践的なデジタルフォレンジックスキルの習得を目指します。

さまざまなセキュリティインシデントの実務経験を有する講師陣

- 日常業務においてインシデント対応や不正調査におけるデジタルフォレンジックを行う実務者が講師を担当します
- トレーニング受講後も適宜質問を受けつけ、トレーニング内容の十分な理解をサポートします

特定のフォレンジックツールに依存しないスキルの習得

- 各コースでは、特定のフォレンジックツールに依存した内容ではなく、フォレンジックで最も大事な「再現性」を重視し、各種アーティファクトの生成メカニズムや内部構造を中心的に説明します
- 各コースでは、OS標準コマンドや入手が容易なオープンソースなどのツールを中心に使用して解説します

調査に利活用可能な豊富な情報が記載されたテキスト

- 各コースとも1日あたり200ページを超える豊富な情報量
- 各種アーティファクトの保存場所や解析手法などを記載
- トレーニング受講後の復習や調査を支援する参考情報として利活用可能です

Mac Forensics

Macの保全から解析までフォレンジックの基礎を学ぶ

日程：3日間、定員：12名、参加費（1名あたり）：300,000円（税抜き）

日程	時間	内容（予定）
1日目～2日目	10:00～17:30 10:00～13:00 （1時間の昼食休憩含む）	▸ macOS®基礎 　▸ macOSの機能・特徴など 　▸ macOSのファイルシステム ▸ Macのデータ保全 　▸ データ保全手法 　▸ データ保全における注意点 　▸ ディスクイメージのマウント方法 ▸ APFSの概要 ▸ 演習
2日目～3日目	13:00～17:30 10:00～17:30 （1時間の昼食休憩含む）	▸ macOS解析 　▸ ログファイル・システムファイル 　▸ macOSのシステム設定 　▸ macOSシステムアーティファクト（Spotlight®、Time Machine®など） 　▸ ユーザーアクティビティの調査（ファイル閲覧履歴、過去のバージョンなど） 　▸ Apple標準のアプリケーション解析（Safari®、Mail、写真アプリ など） ▸ 演習

いずれのトレーニングも最低開講人数は5名となります。トレーニングはオンライン（Teams／ご指定のオンライン会議サービスなど）で実施することも可能です。また、本資料に記載されたカリキュラムはご要望に応じて組み合わせて、カスタマイズすることも可能です。詳細には、 お気軽にForensicsセミナー担当者にお問い合わせください。

- Microsoft、Windows、BitLocker、Surface、Internet Explore、OneDrive、Microsoft Edge、Cortanaは、米国 Microsoft Corporation の、米国およびその他の国における登録商標または商標です。
- Macintosh、macOS、OS X、Spotlight、Time Machine、Safariは、Apple Inc.の商標です。AndroidはGoogle Inc.の商標です。
- 本トレーニングは、独立のセミナーであり、マイクロソフト コーポレーションと提携しているものではなく、また、マイクロソフト コーポレーションが許諾、後援、その他の承認をするものではありません。
- 本トレーニングは、独立したセミナーであり、Apple Inc.が認定、後援、その他承認したものではありません。

Windows Forensics

Windows がインストールされた端末のフォレンジックを学ぶ

日程：3日間、定員：15名、参加費（1名あたり）：300,000円（税抜き）

日程	時間	内容（予定）
1日目～2日目	10:00～17:30 10:00～13:00 （1時間の昼食休憩含む）	▸ Windows® に導入された機能概要およびWindowsのデータ保全 　▸ Secure Boot、BitLocker®、Surface®などのタブレット端末のデータ保全 ▸ Windowsを解析するための前提知識 　▸ SQLiteデータベース、ESEデータベース、レジストリ ▸ Live ForensicsとFast Forensics 　▸ Live Forensics（揮発性情報およびFast Forensics用データの取得）、Fast Forensics（プログラム実行、ブラウザアクセス、イベントログ、メモリダンプなどの基本的な解析）
2日目～3日目	13:00～17:30 10:00～17:30 （1時間の昼食休憩含む）	▸ Windows Deep Forensics 　▸ システム情報、アカウント情報の解析、ユーザーの挙動の解析（プログラム実行、ファイル操作、ブラウザアクセス、RDPの解析など）、Microsoftストアアプリの解析 　▸ その他のアーティファクトの解析（日本語IME入力、回復、Windowsバックアップ、ファイル履歴など） ▸ Windowsの新機能関連の解析（Cortana®、タイムライン、近距離共有など）、演習

File System Forensics

フォレンジックの観点でファイルシステムの構造を基礎から学ぶ

日程：2日間、定員：15名、参加費（1名あたり）：250,000円（税抜き）

日程	時間	内容（予定）
1日目	10:00～17:30 （1時間の昼食休憩含む）	▸ ファイルシステムの基礎 　▸ File System Fundamental、パーティション ▸ Windowsファイルシステム編 　▸ FAT・exFATの構造、演習
2日目	10:00～17:30 （1時間の昼食休憩含む）	▸ Windowsファイルシステム編 　▸ NTFSの構造（前半）、演習 ▸ Windowsファイルシステム編 　▸ NTFSの構造（後半）、演習 ▸ EXTファイルシステム 　▸ EXT2/EXT3/EXT4の構造、演習

マルウェア解析基礎

マルウェア解析基礎

日程：1日、定員：15名、参加費（1名あたり）：150,000円（税抜き）

時間	内容（予定）
10:00～17:30 （1時間の昼食休憩含む）	▸ マルウェア解析の基礎知識 　▸ マルウェアとは、マルウェアの解析概要 ▸ 基本的な静的解析 　▸ ハッシュ値の活用、Win32アプリケーションの構造、文字列情報などの解析、演習 ▸ マルウェアの動的解析 　▸ 動的解析環境の構築、マルウェアのモニタリング、モニタリング結果の解析、演習