第９回ＩＤＦ講習会

開催日時　２０１９年９月３日（火）～９月１３日（金）
主催　特定非営利活動法人デジタル・フォレンジック研究会
会場　TKP市ヶ谷カンファレンスセンター（東京都新宿区）　他

レクチャーを主とする通常コース（表面）と実機・実ソフトを操作する簡易トレーニングコース（裏面）があります。
ご注意：各コースの詳細や、受講の際に前提とされる知識等の受講条件、PC持参の有無等をWEBサイトに掲載しておりますので、お申し込みの際は必ずWEBサイトをご確認下さい。

通常コース

９／５（木）、９／６（金）

受講費(１コース)：会員　￥３，０００－
提携団体会員　￥５，０００－
一般　￥７，０００－

※提携団体は以下
JASA、JNSA、DRAJ、ADEC、CIKF

９／５（木）

午前（09：30～12：30）

A　メディア・フォレンジックの必要性
IDF　上原 哲太郎 氏（立命館大学）
画像における改ざん技術の現状をお伝えするとともに、オープンソースを用いた古典的なフォレンジックを起点に、画像の分析を行う手法について概要を解説します。

B　モバイルフォレンジックの基礎習得
リーガルテック株式会社
Androidスマートフォンからのデータ抽出およびデータ解析手法について解説・実演します。UFED、AndrExを活用した解析事例も紹介します。

C　NUIXとモバイルフォレンジックのMSABによる大規模データの調査・解析ラボのご紹介
Nuix Japan
急増するデータ、デバイスやデータタイプの多様化により、デジタル調査は日増しに困難となっています。MSABとNUIXとの連携により、効率的なワークフローとチームでの協業を実現し、事案を素早く解明する方法を解説します。

D　CyCraft社 CyCraft AIRを用いたファストフォレンジック調査の実演
株式会社スプラウト
模擬的な攻撃を行った複数の端末に対し、CyCraft AIRを用いたファストフォレンジック調査を実演します。その結果から、インシデント対応や将来的な予防の知見をどのように得るかをディスカッションします。

午後（13：30～16：30）

E　Autopsyを用いたデジタル・フォレンジックの実務
ベイシス・テクノロジー株式会社
デジタル・フォレンジックの実務の流れを、オープンソースツールAutopsyのDemoを用いて説明します。

F　画像解析フォレンジックの動画復元と画像鮮明化の解説
リーガルテック株式会社
画像解析フォレンジックツールを用いて防犯カメラ、ドライブレコーダーで撮られた動画データのフレーム復元技術と画像の鮮明化技術について初心者にも分かりやすく解説・実演します。

G　デジタル・フォレンジックと刑事法
IDF　石井 徹哉 氏（独立行政法人大学改革支援・学位授与機構）
サイバーセキュリティ対策を行う上で問題となる刑法上の犯罪の成立要件について、詳しく解説します。その際、攻撃者に対する積極的な対応策を講じることが犯罪となりうるかどうかについても検討し現行の法令上の限界と今後の展望について検討します。

H　X-Ways ForensicsによるWindowsフォレンジックの紹介
株式会社ディアイティ
X-Ways Forensicsの紹介と本製品を使用したWindowsマシンのフォレンジック調査要領を説明します。

９／６（金）

午前（09：30～12：30）

I　モバイルフォレンジック入門
株式会社フォーカスシステムズ／Cellebrite Japan
企業・組織において想定される仮想シーンを元にCellebrite UFEDやMagnet AXIOMなどのツールを駆使して、モバイル端末のデータをどのように取り扱っていくかを解説していきます。

J　人工知能を活用した大量データレビュー手法
株式会社FRONTEO
メールやドキュメント等の大量データのレビュー作業において、人工知能を搭載したデータ解析ツール「Lit i View XAMINER」を用い、従来のキーワード検索とは異なる観点でのデータレビュー手法を紹介します。

K　EnCaseのリモートフォレンジック技術を活用したファストフォレンジック入門
オープンテキスト株式会社
OpenText EnCaseのソリューション概要とフォレンジックにおける主な機能をご紹介します。またEnCaseを活用してネットワーク越しに証拠データを収集・保全・解析する方法について初心者向けに解説します。

L　次世代の保全方法と証拠ファイルの解析アプローチ（前編）～コンピュータ、特殊装置編～
株式会社くまなんピーシーネット
HDDを搭載せず、I/F接続概念がないオールフラッシュPCだけの時代となり、これからの証拠保全についての危機感を持ち、従来の方法に囚われない新しい解析手段を提案します。近年のストレージアーキクチャについての座学と注意点、誰でもできる保全方法や仮想環境を使った新たな解析アプローチの実践を予定しています。

午後（13：30～16：30）

M　デジタル・フォレンジックと情報法
IDF　小向 太郎 氏（日本大学）
デジタル情報の法的位置づけについては、いまだに論点が多い。DFについても、係争等の法的背景、調査分析の法的評価、証拠としての有効性などが問題となり得ます。本講座では、情報に関する法的規律の性格とDFとの関係を概説します。

N　RECON Imager/LabによるMacフォレンジックの基礎
株式会社FRONTEO
RECON Imager/Labのご紹介とデモを交え、Macフォレンジックの基礎を解説します。

O　7つのサイクルから導きだす「サイバー犯罪」の最終処理
IDF　林 憲明 氏（サイバー犯罪捜査・調査ナレッジフォーラム）
『CIBOK：サイバー犯罪捜査・調査知識体系』に基づいて学習を進めます。サイバー犯罪の捜査・調査に関わる各メンバーの役割に対する理解を促し、円滑な情報共有を推進するための共通言語を身に付けることができます。

P　次世代の保全方法と証拠ファイルの解析アプローチ（後編）～モバイル、IoTデバイス編～
株式会社くまなんピーシーネット
5G通信時代を前に端末のグローバル化は加速し身近な機器は何かと繋がる時代になり、多種多様な機器に残された情報から証拠の手がかりを探す方法を提案します。近年のフラッシュメモリについての座学と注意点、今後スマートフォンやIoT機器をどのように解析すべきなのか少し踏み込んだ解析アプローチの実践を予定しています。

簡易トレーニングコース

９／３（火）～９／１３（金）　全１５コース

※受講費はコース毎に異なります

９／３（火）	Ｃ１ 定員20 10:00～17:00	サイバー犯罪の解決と証拠収集・分析	（一社）サイバー犯罪捜査・調査ナレッジフォーラム 会場：トレンドマイクロ本社（新宿）　受講費：¥10,000- サイバー犯罪事件の被害者となった企業が、その事件にどのように対応し解決すべきかのフレームワークを理解するとともに、その解決の肝となる証拠収集と分析をどのような点に留意しながら実施すべきかをCIBOK（サイバー犯罪捜査・知識体系）を軸とした「心得」を座学とワークショップで学びます。
９／４（水）	Ｅ１ 定員12 10:00～17:30	マルウェア解析基礎	EY新日本有限責任監査法人 会場：TKPスター貸会議室日比谷（日比谷）　受講費：¥80,000- Windowsで動作するマルウェアを主体とした表層解析、動的解析の手法について実演、演習を交えて解説します。
９／５（木）	Ｆ１ 定員16 10:00～17:00	Windows 7～10フォレンジックの基礎	株式会社FRONTEO 会場：FRONTEO品川本社（品川）　受講費：¥55,000- Windows 7～10の代表的なアーティファクトを対象とした、Windowsフォレンジックの基礎を解説します。コースでは、フリーツールを用いたアーティファクト解析のハンズオントレーニングも実施します。
	Ｓ１ 定員16 10:00～17:00	ハッキング入門 ～攻撃者視点で思考できるホワイトハッカー入門コース～　ストーンビートセキュリティ株式会社 会場：ストーンビートセキュリティ株式会社　研修ルーム（麹町）　受講費：¥55,000- 実際のハッキングの手口や技術を実践的な演習を通して、攻撃者視点でセキュリティ対策を思考できるようになります。	
	Ｅ２ 定員12 10:00～17:30	Macintosh Forensics 保全編	EY新日本有限責任監査法人 会場：TKPスター貸会議室日比谷（日比谷）　受講費：¥80,000- 最新のmacOSであるMojaveを対象としたデータ保全に係るMacintosh特有のフォレンジックについて、Macintosh固有の機能とあわせて実演、演習を交えて解説します。
９／６（金）	Ｎ１ 定員20 09:30～16:30	Nuix Investigator 実践編	Nuix Japan 会場：Nuix Japan 会議室（六本木一丁目）　受講費：¥75,000- Nuix Workstationを活用しデータ処理、検索、分析、検証することを実践・説明するトレーニングとなります。電子証拠に対してのデータ処理、識別、重複排除、検索、分析方法などの一連の操作実践や詳細な説明が含まれます。
	Ｓ２ 定員10 10:00～17:00	メモリフォレンジック ～ハンズオントレーニング/ダイジェスト1日版～　ストーンビートセキュリティ株式会社 会場：ストーンビートセキュリティ株式会社　研修ルーム（麹町）　受講費：¥85,000- メモリフォレンジックについて、ハンズオンを通してメモリ取得や解析の知識と技術の習得ができます。	
	Ｅ３ 定員12 10:00～17:30	Macintosh Forensics 解析編	EY新日本有限責任監査法人 会場：TKPスター貸会議室日比谷（日比谷）　受講費：¥80,000- 最新のmacOSであるMojaveを対象とした解析に係るMacintosh 特有のフォレンジックについて、Macintosh固有のアーティファクトおよび解析プロセスを実演、演習を交えて解説します。
９／６（金） 09:30～12:30 13:30～16:30	Ｂ1、Ｂ2 （午前）（午後） 各定員8 ※同内容	Autopsyを用いたデジタル・フォレンジックの実務（ハンズオン）	ベイシス・テクノロジー株式会社 会場：ベイシス・テクノロジー株式会社（永田町）　受講費：¥30,000- デジタル・フォレンジックの実務の流れを、オープンソースツールAutopsy を用いて実際に体験して頂きます。
９／５（木） ９／６（金）	Ｌ1、Ｌ2 各定員16 09:00～16:30 ※同内容	ファイナルフォレンジック 基礎研修 1日コース	リーガルテック株式会社 会場：東芝総合人材開発研修センター（浜松町）　受講費：¥50,000- ファイナルフォレンジックを使用する際の基礎的知識の説明から使用方法（データ復元・分類、データの検索、メールデータの復元、システムレジストリの解析等）についてPCを使用した実習を行います。
９／11（水）	Ｅ４ 定員12 10:00～17:30	Windows 10 Forensics 初動対応編	EY新日本有限責任監査法人 会場：東京ミッドタウン日比谷（日比谷）　受講費：¥80,000- Windows 10を対象とした初動対応として、Windows 10の機能や特徴とあわせてデータ保全からFast Forensics（一般的なアーティファクトの解析等）について実演、演習を交えて解説します。
９／12（木）	Ｅ５ 定員12 10:00～17:30	Windows 10 Forensics 解析編	EY新日本有限責任監査法人 会場：東京ミッドタウン日比谷（日比谷）　受講費：¥80,000- Windows 10の解析手法について、各種アーティファクトの解析プロセスを中心にWindows 10で実装されたフォレンジックに係る機能・特徴等を実演、演習を交えて解説します。なお、本編で扱うアーティファクトは、初動対応編よりも広範になります。
９／13（金）	Ｅ６ 定員12 10:00～17:30	ファイルシステム解析 NTFS編	EY新日本有限責任監査法人 会場：東京ミッドタウン日比谷（日比谷）　受講費：¥80,000- WindowsでNTFSファイルシステムについて、 ファイルシステムの機能・特徴からフォレンジック調査における重要性、解析に有用な知識を実演、演習を交えて解説します。

申込方法　講習会WEBページの「受講申込フォーム」よりお申込み下さい。
「受講申込用紙」でのFAXのお申込も受け付けております。

申込締切　２０１９年８月２３日（金）

お問合せ　特定非営利活動法人デジタル・フォレンジック研究会　事務局
E-Mail：info@digitalforensic.jp　WEBサイト：https://digitalforensic.jp/
TEL　：03-5420-1805　FAX　：03-5420-3634