第6回 IDF講習会

https://digitalforensic.jp/home/act/lecture/lecture-6-2016/　検索☞「IDF講習会」

開催日時　2016年　9月　7日(水)～9月　9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)

実際のフォレンジック技術のセミナーコースと
ハンズオン形式のコースがございます。

ご興味をお持ちの方は、是非ご参加下さい！

各コース受講の際に前提とされる
知識等につきましては、ウェブサイトで
公開しておりますので、ご確認下さい。

開催概要 (日時･会場)　※各コース内容の詳細は裏面をご覧下さい

9月7日(水)	簡易	9:30～16:30	Vコース 定員20名 会場:(株)フォーカスシステムズ トレーニングルーム(五反田)
		10:00～17:00	Wコース定員10名 会場:(株)FRONTEO トレーニングルーム (品川)
9月8日(木)	通常	9:30～12:30	Aコース ／ Bコース ／ Cコース ／ Dコース
		13:30～16:30	Eコース ／ Fコース ／ Gコース ／ Hコース ※Hのみ官公庁限定
		通常コース会場:TKP市ヶ谷カンファレンスセンター(TEL:03-5227-6911) 〒162-0844 東京都新宿区市谷八幡町8番地 JR総武線 市ケ谷駅 徒歩2分	
	簡	9:30～16:30	Xコース 定員15名 会場:AOSリーガルテック(株) 浜松町会場 (浜松町･大門)
9月9日(金)	通常	9:30～12:30	Iコース ／ Jコース ／ Kコース ／ Lコース
		13:30～16:30	Mコース ／ Nコース ／ Oコース ／ Pコース
		通常コース会場:TKP市ヶ谷カンファレンスセンター(TEL:03-5227-6911) 〒162-0844 東京都新宿区市谷八幡町8番地 JR総武線 市ケ谷駅 徒歩2分	
	簡易	9:30～16:30	Yコース 定員15名 会場:AOSリーガルテック(株) 浜松町会場 (浜松町･大門)
		10:00～17:00	Zコース 定員16名 会場:ストーンビートセキュリティ(株) 赤坂会場 (赤坂)

受講費

◆通常コース

IDF会員	￥3,000－／コース
JASA･JNSA･DRAJ会員	￥5,000－／コース
一般	￥7,000－／コース

◇簡易トレーニングコース

Vコース	￥50,000－／名
Wコース	￥35,000－／名
X、Yコース	￥50,000－／名
Zコース	￥59,000－／名

お申込み

申込方法　WEBフォーム　：当研究会HPにございます「受講申込フォーム」よりお申込み下さい。
https://digitalforensic.jp/lecture-6
FAX　：当研究会ウェブサイトにある「受講申込用紙」をダウンロードして頂き、
必要事項をご記入の上、事務局までお送り下さい。

申込締切　2016年　8月　31日　(水)

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　　HP　：　https://digitalforensic.jp/
TEL　：　03-5420-1805　　FAX　：　03-5420-3634

通常コース詳細

A・I

実践で学ぶサイバー攻撃対応のためのフォレンジック
(株) フォーカスシステムズ

本コースでは、各種サイバー攻撃対応で必要になるフォレンジックの技術を概観します。調査の際に必要になるPC上の様々な痕跡（アーティファクト）について基礎的な背景をご説明した後に、攻撃を再現した環境を用いて、調査解析を疑似体験して頂きます。

B・J

国際訴訟案件を事例とした人工知能搭載ツールによる、より効果的な解析手法
(株) FRONTEO（(株) UBICから社名変更）

国際訴訟案件を例に、FRONTEOで独自開発した人工知能搭載の解析ツール「Lit i View XAMINER」による、大量のメールデータの解析手法をご紹介します。増大する調査対象のデータの中から、効率良く証拠を見つけ出すために有効です。

C・K

標的型攻撃対策サービス「Lastline」入門編 SCSK (株)

標的型攻撃対策サービス「Lastline」の概要と本サービスを用いた不正通信、及びマルウェアの基礎的な解析方法を説明致します。また、Lastlineの導入構成や実際の運用イメージについても合わせて紹介致します。

D

CSIRT構築入門 ストーンビート セキュリティ (株)

本コースは、これから新規に社内CSIRTを構築することを検討されているご担当者様向けに、CSIRTの役割や体制の確立、規程類の整備、訓練の実施などのポイントを分かりやすく解説します。

E

AndrExとフォレンジックサービスによるモバイルフォレンジックの基礎習得 AOSリーガルテック (株)

AOS AndrEx（アンドレックス）によるAndroidスマートフォンからの通常データ抽出、Excelへの展開の説明・実演及び、捜査機関向けAOSモバイルフォレンジックサービスの紹介を致します。

F・N

インシデント発生時における実践的証拠保全手法
(株) FRONTEO（(株) UBICから社名変更）

フォレンジック調査において重要性の高い証拠保全について、HDDデュプリケーター「Image MASSter Solo-4 G3」を使った証拠保全手法をご説明します。インシデント発生時における、適切な初動対応や注意点と併せて解説します。

G

HDDの上書き消去の限界と、残留するデータ・領域（PARADAIS等）へのアクセスによるデータ復旧・消去に関する解説 (株) DD-RESCUE & 大阪データ復旧 (株)

1. 「証拠保全ガイドライン」の要求する「無データ状態の複製先」実現の難しさについて「『データ消去』分科会の結論」を解説
2. HDDのPARADAIS（余剰領域等）対策の信頼性とデータ復旧・消去について
3. DDRH（プラッタダメージ対処用データ復旧装置）の使用法と効能、その他

H

デジタル・フォレンジックの基礎※官公庁の方限定コース
NPOデジタル・フォレンジック研究会 白濱 直哉

東京電機大学（CySec）でのデジタル・フォレンジックの講義（全15回）を凝縮し、フォレンジック調査を実施するにあたっての重要なポイントや基礎的な事項について解説します。

L

HDD、メモリ、スマートフォンのこれまでの保全とこれからの保全
(株) くまなんピーシーネット

HDDレスパソコンの証拠保全と問題点、新技術HDDに対する証拠保全とその有効性、破損したメモリ製品のワイヤリング解析、スマートフォンのChip-Off解析などの講演と実演、Simple SEIZURE TOOLを使ったパソコンとスマートフォンの証拠保全実習を予定しています。

M

X-WaysForensicsによるWindowsフォレンジック入門
(株) ディアイティ

X-WaysForensics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致します。

O

標的型攻撃対策サービス「Lastline」応用編 SCSK (株)

標的型攻撃対策サービス「Lastline」の機能の詳細な紹介及び、サンプルを用いたマルウェア解析の解説を行います。また、実際にLastlineを用いた解析を体験いただくため、本コース受講者の方にはノートPC及びモバイルwifi環境を準備頂くことを推奨しています。

P

誰でもできる高度なフォレンジック、膨大なデータからすばやく証拠を探すテクニック (株) くまなんピーシーネット

【前半】「Belkasoft」を使って初心者でも熟練者並みの結果を簡単に出すフォレンジック手順。【後半】「Intella」を使った膨大なデータから証拠を探し出す手順。「Intella Connect」を使った調査とレビュー体験（各自PC、タブレット持ち込み必要）を予定しています。

簡易トレーニングコース詳細

V

Cloud Forensics - **端末に記録されているデータの検知と解析**
(株) フォーカスシステムズ

当社取扱い製品『IEF（Internet Evidence Finder）』を始めとする、様々なツールを活用して、PC端末に記録されているクラウドサービス利用時のデータを検知し解析するコースです。ますますニーズの高まる、クラウドサービスの利用実態を解明するための、実習も用意しております。

W

多様性を持つモバイル端末へのフォレンジック調査手法
(株) FRONTEO（(株) UBICから社名変更）

常に変化し続けるモバイル端末へのフォレンジック調査手法を、実践形式で学習します。世界100ヶ国以上の法執行機関、国防機関等で導入されているモバイル端末データ取得ツール「XRY」によるデータ取得方法や解析手法の基礎を、注意事項を交えて紹介します。

X・Y

ファイナルフォレンジック 基礎研修1日コース
AOSリーガルテック (株)

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、基本的な使用方法（データの復元・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。

Z

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)

セキュリティ対策を考える上で、攻撃者の思考や手口に対する理解は欠かせません。ターゲットシステムの偵察行為からシステムの脆弱性探索、システムへの侵入、情報探索など、実際に発生しているハッキングの手口や技術を実践的な演習を通して学習します。