第8回IDF講習会　通常コース内容
(1／3)

Aコース	コース名	**オープンソースツールを用いたForensic**
	実施社	デジタル･フォレンジック研究会　上原　哲太郎　氏
	前提知識等	ファイルとファイルシステムに関する基礎的知識 (「デジタル･フォレンジックの基礎と実践」2章および3章を読んでおくと理解が早まると思います。)
	概要	オープンソースを用いたフォレンジックを実践します。Autopsy / The Sleuth Kitを用いて、基本的なファイルシステム内のファイル調査やスラック領域の検索などを行います。
	その他	Windowsの動作するパソコンを持ち込んで下さい。フォレンジック練習に用いるディスクイメージは当日配布します。

Bコース Jコース	コース名	**最先端のデュプリケーターによる証拠保全概論**
	実施社	株式会社フォーカスシステムズ
	前提知識等	どなたでも受講可能です。
	概要	新型ユニットForensic Falcon NEOによる証拠保全方法について説明します。証拠保全の基礎から分解が困難な薄型ノートＰＣからネットワーク経由でのデータ取得など現場の厳しい要求により激変しつつあるデュプリケーターの新しい基準も併せて説明します。

Cコース	コース名	**サイバー攻撃の世界動向とレジリエンス向上のための備え**
	実施社	株式会社ブロードバンドセキュリティ
	前提知識等	どなたでも受講可能です。
	概要	刻々と変わっていくサイバー攻撃の最新動向と、フォレンジックからわかる被害の最小化を目指す備えについて2名で講演します。

Dコース	コース名	**事例から見る民間におけるデジタル･フォレンジックの活用と課題**
	実施社	ＭＹＫアドバイザリー株式会社
	前提知識等	どなたでも受講可能です。
	概要	民間調査におけるデジタル･フォレンジック活用の実態と、その更なる活用のための現実的な課題について、デジタル･フォレンジックサービス提供事業者の立場から、事例に基づく考察を交えて紹介します。

Eコース	コース名	**クラウドの証拠保全(AWS編)**
	実施社	株式会社ラック
	前提知識等	どなたでも受講可能です。
	概要	AWSの証拠保全に初めて取り組む方を対象に、AWSの技術要素や証拠保全の各工程をわかりやすく解説します。また、日本におけるクラウドの利用状況やインシデント事例も紹介します。

第8回IDF講習会　通常コース内容
(2／3)

Fコース	コース名	インシデント発生時における様々な証拠保全手法
	実施社	株式会社FRONTEO
	前提知識等	どなたでも受講可能です。
	概要	フォレンジック調査において重要性の高い証拠保全作業について、インシデント発生後の適切な初動対応や注意点を紹介します。また、HDDデュプリケーター「Image MASSter Solo-4 G3」を用い、実演を交えたHDDデータの証拠保全手法を説明します。

Gコース	コース名	不正調査ツールNuixの紹介とデモ
	実施社	AOSリーガルテック株式会社
	前提知識等	フォレンジックの基礎知識
	概要	Nuix社の製品ラインナップの紹介と世界の多くの捜査機関で利用されている大量データ処理向けのNuix Investigation and responseの製品説明･デモを行います。

Hコース	コース名	X-Ways Forensics によるWindows フォレンジック入門
	実施社	株式会社ディアイティ
	前提知識等	どなたでも受講可能です。
	概要	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。

Iコース	コース名	インシデントレスポンスに関連する法制度
	実施社	デジタル･フォレンジック研究会　北條　孝佳　氏
	前提知識等	CSIRTに所属する方々、経営者層を対象とした内容になります。
	概要	情報漏えい事案から様々なサイバー攻撃等、インシデントレスポンスへの対応における法制度面の理解の必要性について説明し、インシデントレスポンスに関連する法律及び企業が直面する事案について解説します。

Kコース	コース名	AndrExによるモバイルフォレンジックの基礎習得
	実施社	AOSリーガルテック株式会社
	前提知識等	フォレンジックの基礎知識
	概要	AOS AndrEx (アンドレックス) シリーズ (*)によるAndroidスマートフォンからのデータ抽出の説明･実演を致します。 (*) 実際に説明するソフトウエア 1) AndrEx、2) AndrEx SS、3) AndrEx LB、4) AndrEx for Images

第8回IDF講習会　通常コース内容
(3／3)

Lコース	コース名	**新たな保全対象とデータ解析アプローチ（前編）　～コンピュータ、特殊装置編～**
	実施社	株式会社くまなんピーシーネット
	前提知識等	コンピュータなどの証拠物に携わる官公庁の方限定
	概要	HDDを搭載せず、I/F接続概念がないフラッシュストレージ実装PCが当たり前となった現在。これからの証拠保全とフォレンジックについて危機感を持ち、従来型の方法に囚われない新しい手段を学びます。近年のストレージアーキクチャやその特性についての座学と、保全方法や解析アプローチの実践を予定しています。
	その他	実際の鑑定事例等を交えるため官公庁の方限定となります。

Mコース	コース名	**デジタル･フォレンジックと刑事法**
	実施社	デジタル･フォレンジック研究会　石井　徹哉　氏
	前提知識等	どなたでも受講可能です。
	概要	本コースでは、デジタル･フォレンジックに関係する刑事法上の規制を解説し、広狭様々なインシデントレスポンスで投入される手法の法的意味、限界を確認したいと思います。

Nコース	コース名	**複数拠点間での人工知能を使った解析ノウハウの共有手法**
	実施社	株式会社FRONTEO
	前提知識等	どなたでも受講可能です。
	概要	人工知能搭載データ解析ツール「Lit i View XAMINER」を用いたメール等の大量電子データの解析ノウハウを複数拠点間で共有する手法をご紹介します。

Oコース	コース名	**AOS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**
	実施社	AOSリーガルテック株式会社
	前提知識等	フォレンジックの基礎知識
	概要	AOS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。

Pコース	コース名	**新たな保全対象とデータ解析アプローチ（後編）　～モバイル、IoTデバイス編～**
	実施社	株式会社くまなんピーシーネット
	前提知識等	スマートフォンなどの証拠物に携わる官公庁の方限定
	概要	モバイル端末はグローバル化、身近な機器はIoT化で何かと繋がっている現在。これら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学びます。破壊された端末、電源を切るとデータが消えるメモリ搭載機器など、今後どのように解析すべきなのかを座学を交え説明。これらの保全手段と解析アプローチの実践を予定しています。
	その他	実際の鑑定事例等を交えるため官公庁の方限定となります。