第6回IDF講習　通常コース内容
（1／2）

Aコース Iコース	コース名	**実践で学ぶサイバー攻撃対応のためのフォレンジック**
	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
	概要	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コース Jコース	コース名	**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**
	実施社	株式会社FRONTEO （株式会社UBICから社名変更）
	前提知識等	デジタル・フォレンジックの基本的な知識をお持ちの方
	概要	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コース Kコース	コース名	**標的型攻撃対策サービス「Lastline」入門編**
	実施社	SCSK株式会社
	前提知識等	どなたでも受講可能 （ネットワーク、セキュリティに関する基礎的な知識があればなお可）
	概要	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コース	コース名	**CSIRT構築入門**
	実施社	ストーンビート セキュリティ株式会社
	前提知識等	CSIRTの構築を検討されているご担当者様
	概要	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。
	その他	IDF講習会のために特別に編集し、通常3日間で構成する弊社トレーニングをダイジェストでご紹介します。

Eコース	コース名	**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**
	実施社	AOSリーガルテック株式会社
	前提知識等	どなたでも受講可能 フォレンジック製品の導入検討もしくは導入をされている方 デジタル・フォレンジックの基礎知識をお持ちでWindowsシステムの操作の基本を習得されている方
	概要	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・実演および捜査機関向け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コース Nコース	コース名	**インシデント発生時における実践的証拠保全手法**
	実施社	株式会社FRONTEO （株式会社UBICから社名変更）
	前提知識等	PC（特にWindows）の基本的なオペレーションを理解している方
	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。

第6回IDF講習　通常コース内容
（2／2）

Gコース	コース名	**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**
	実施社	株式会社DD-RESCUE　大阪データ復旧株式会社
	前提知識等	どなたでも受講可能
	概要	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コース 官公庁の方限定コース	コース名	**デジタル・フォレンジックの基礎**
	実施社	NPOデジタル・フォレンジック研究会
	前提知識等	省庁オブザーバー及び官公庁での現場対応者等
	概要	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コース	コース名	**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**
	実施社	株式会社くまなんピーシーネット
	前提知識等	パソコン、スマートフォンの証拠物に携わる司法機関の方を歓迎します。
	概要	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。
	その他	実習用のパソコンは数台用意いたしますが、お持込のパソコンでも対応できます。

Mコース	コース名	**X-WaysForensics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
	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致します。

Oコース	コース名	**標的型攻撃対策サービス「Lastline」応用編**
	実施社	SCSK株式会社
	前提知識等	本コースの受講に先立って開催される入門編（Cコース又はKコース）を受講されることをお勧めします。
	概要	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環境を準備いただくことを推奨しています。

Pコース	コース名	**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**
	実施社	株式会社くまなんピーシーネット
	前提知識等	どなたでも受講可能
	概要	【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。
	その他	当日紹介するソフトウェアを一定期間フル機能で使用できるデモ版を配布いたします。