

フォレンジックトレーニング

最新技術、実践的な調査手法を学べるトレーニングです

☐ 特徴

最新の技術を学べます

メモリ・フォレンジック、Windows 7の調査項目など最新技術や、ログ/タイムスタンプの調査、IM（インスタントメッセージ）の調査などの実践的なフォレンジック技術を習得することができます。

実践的な内容

EnCaseを日頃から調査に利用されている経験者、またはガイダンスソフトウェア社のCF I+IIコースを受講済みの方向けの内容となっています。EnCaseユーザー様がさらに専門的で実践的な調査技術を学ぶことができる最適なトレーニング内容です。

受講者の方のニーズに合わせて

トレーニングは全7つの講座から構成されており、興味のある技術、必要な講座のみを受講することができます。
また、トレーニングは一人1台のパソコンを利用したハンズオン形式です。



☐ 講座一覧

Windows 7 フォレンジック調査	Web/Mail フォレンジック調査
タイムライン/ログ調査	IMのフォレンジック調査
Windows メモリフォレンジック I	レジストリのフォレンジック調査
Windows メモリフォレンジック II	EDSモジュールを利用した調査

※詳細は別紙をご覧ください。

☐ 価格/定員/会場について

	価格	定員/最低催行人数	会場
全コース共通	49,350円（税込）	定員10名 最低催行人数5名	株式会社Ji2オフィス内 セミナールーム

※官公庁または法執行機関の方だけが受講いただけます。一般企業の方は受講いただけません。
※定員に達した時点で受付を締め切らせていただきます。受講をご希望の方はお早めにお申し込みください。

☐ 株式会社Ji2について

株式会社Ji2はコンピューターフォレンジックツールの世界標準EnCaseの日本総代理店です。
官公庁・法執行機関を対象としたフォレンジックトレーニングの分野において、多数の実績を持ちます。

株式会社Ji2

〒160-0022 東京都新宿区新宿1-9-5 大台ビル3F
TEL 03-6228-0163 / FAX 03-6228-0164 / MAIL seminar@ji2.co.jp

<http://www.ji2.co.jp/>

フォレンジックトレーニング

講座概要

コース名	概要	コース内容	開催日/ 時間
Windows7 フォレンジック調査	Windows 7に搭載されている特徴的な機能や、アーティファクトの解析方法について学びます。	1.Windows 7の特徴 2.VSS機能 3.VSSデータの解析 4.検索インデックス 5.その他のアーティファクト 6.演習	2010/09/28 AM 09:30～ PM 17:30
タイムライン/ログ調査	Windowsシステムにおける各種タイムスタンプと、イベントログの解析を通じて、時系列に情報を追跡する方法について学びます。	1.タイムスタンプの基本 2.イベントログの解析 3.タイムラインの作成 4.タイムラインの調査 5.タイムスタンプの改ざん 6.演習	2010/09/29 AM 09:30～ PM 17:30
Windows メモリアレンジック I	Windowsシステムの揮発性データを収集・分析するメモリアレンジックの手法について学びます。	1.メモリアレンジック概要 2.演習 (RAWイメージの取得) 3. Windowsメモリデータ構造 4.解析手法の分類 5.演習 (RAWイメージの解析①) 6.演習 (RAWイメージの解析②)	2010/09/30 AM 09:30～ PM 17:30
Windows メモリアレンジック II	演習を中心にマルウェアの発見や攻撃の分析、ユーザが使用するIMの解析などを行い、メモリアレンジックの実践的なスキルを学びます。	1.メモリアレンジックの注意点 2.演習 (イメージフォーマットの変換) 3.演習 (RAWイメージ取得・解析) 4.演習 (クラッシュダンプ取得・解析) 5.演習 (IMソフトの解析) 6.演習 (標的型攻撃の解析)	2010/10/01 AM 09:30～ PM 17:30
WEB/Mail フォレンジック調査	IEとFirefoxをベースに、Webの履歴とキャッシュ管理の調査、Webメールの痕跡と、通常の電子メールの解析方法について学びます。	1.IE履歴とキャッシュ管理 2.Firefox履歴とキャッシュ管理 3.Webメールの痕跡① 4.Webメールの痕跡② 5.電子メール (Windows Liveメール) 6.演習	2011/02/21 AM 09:30～ PM 17:30
IMフォレンジック調査	メッセージングアプリケーションが保管している情報の解析方法、それらのデータ痕跡の取り扱いについて学びます。	1.Skype 2.Skype (メモリアレンジック) 3.Windows Liveメッセージ 4.Yahooメッセージ 5.その他のメッセージングアプリ 6.演習	2011/02/22 AM 09:30～ PM 17:30
レジストリ フォレンジック調査	Windowsのレジストリファイルの構造と、保存されている情報の役割と解析方法について学びます。	1.レジストリファイルのパス 2.削除キーと値 3.Protected Storage 4.プロセス実行の痕跡 (UserAssist) 5.USBデバイスの接続痕跡 6.演習	2011/02/23 AM 09:30～ PM 17:30
EDS モジュール を利用した調査	認証パスワードや暗号化ファイルシステムなど、システムを保護する機能への対応方法について学びます。	1.SAMファイルとSYSKEY 2.暗号化ファイルシステム (EFS) 3.レジストリ保護領域 4.BitLocker (Vista) 5.その他の保護機能への対応 6.演習	2011/02/24 AM 09:30～ PM 17:30

株式会社 Ji2 セミナー受付担当宛て
送信先FAX :03-6228-0164 / 送信先eMail :seminar@ji2.co.jp

【フォレンジックトレーニング】申し込み用紙
(官公庁・法執行機関専用 ※一般企業の方は受講頂けません)

本セミナーの受付確認につきましては「申込書」のメールアドレスに「セミナー受付」を2営業日以内にお送りし完了とさせていただきます。「セミナー受付」が届かない場合はJi2までお問い合わせください。

以下の項目にご記入ください

組織名		
部署名		
申込者氏名		
住所		
メールアドレス		
連絡先電話番号		内線番号
参加希望コース	<p>コース内容・開催日をご確認のうえ 参加を希望するコースにチェックしてください</p> <p><input type="checkbox"/> Windows7 フォレンジック調査 開催日：2010/09/28</p> <p><input type="checkbox"/> タイムライン/ログ調査 開催日：2010/09/29</p> <p><input type="checkbox"/> Windows メモリフォレンジック I 開催日：2010/09/30</p> <p><input type="checkbox"/> Windowsメモリフォレンジック II 開催日：2010/10/01</p> <p><input type="checkbox"/> WEB/MAIL フォレンジック調査 開催日：2011/02/21</p> <p><input type="checkbox"/> IM フォレンジック調査 開催日：2011/02/22</p> <p><input type="checkbox"/> レジストリフォレンジック調査 開催日：2011/02/23</p> <p><input type="checkbox"/> EDSモジュールを利用した調査 開催日：2011/02/24</p>	
請求関連情報 (申込者と異なる場合にご記入ください)		
請求先部門/担当者		
請求先部門連絡先		
請求書送付先住所		
<p>【お支払条件】・申込確認後、請求書を発行いたします。講習実施月の翌月末日までに現金でお支払いください。 ・事前にお見積り書が必要な場合はお申し付けください。 <input type="checkbox"/> 見積り書希望</p>		

私（申込者）は上記の内容でセミナーへの参加を申し込みます。

申し込み日 年 月 日

申込者署名



●お申込みキャンセルはトレーニング開催日の1週間前までにお知らせください。それ以降のキャンセルについては費用をお支払頂きます。●最低催行人数5名に達しない場合は中止となる場合があります。●ご記入いただきました個人情報は次の目的の範囲内にて使用し、ご本人の同意なく第三者に提供することはありません。（本トレーニングに関するご送付先やご連絡用/各種セミナーのご案内/製品に関するご案内/ニュースレター）