Deloitte.
デロイト トーマツ

デジタル フォレンジック トレーニング基礎編

初動調査を自組織で実施できることを目的としたトレーニング

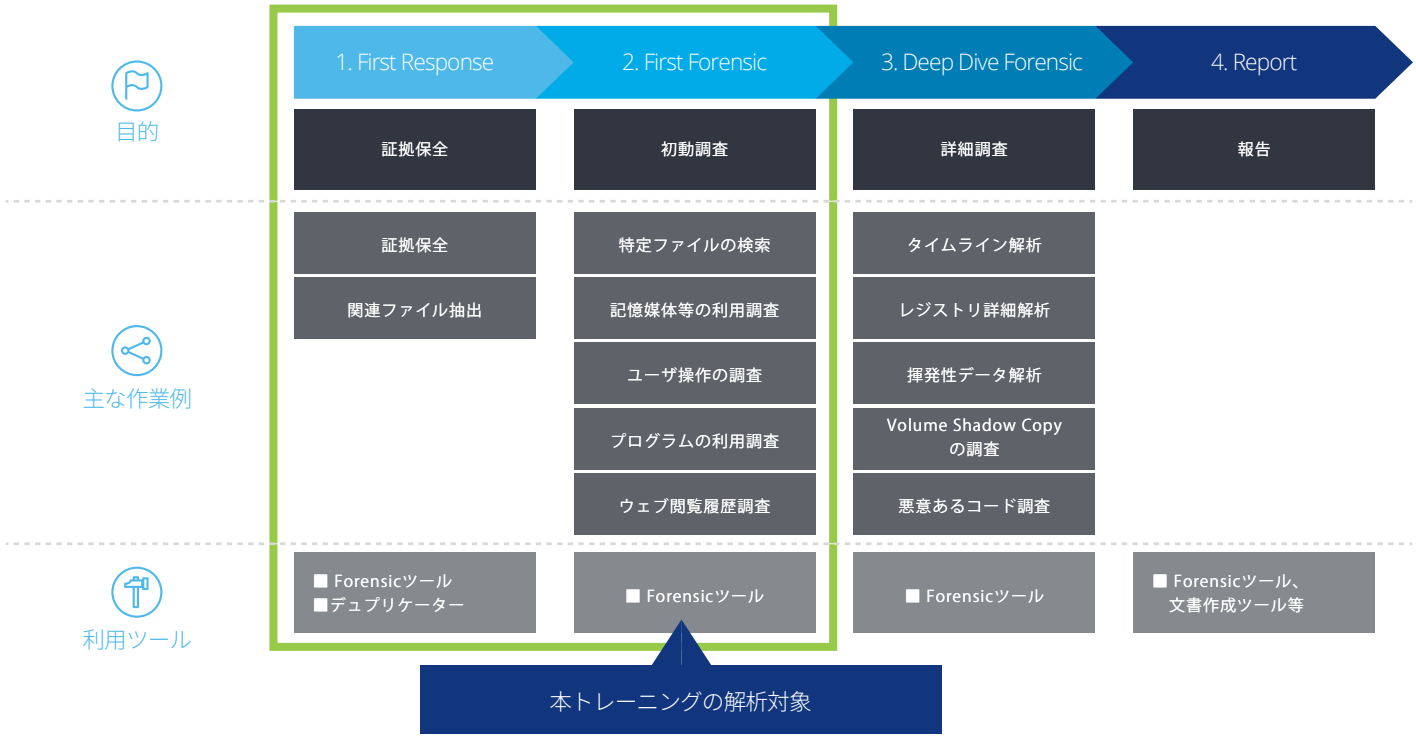
デジタルフォレンジック技術習得の必要性

昨今の標的型サイバー攻撃に代表される高度な攻撃は、従来型の予防対策（入口・出口対策）だけでは限界を迎えています。実際にインシデントが発生した場合、被害原因や影響範囲の把握、拡大防止、回復、社内外のステークホルダーへの報告等、担当者は様々な対応に迫られることになります。
インシデント発生時に特に重要となるのが、インシデント内容を解明し、被害原因や影響範囲を特定するフォレンジックと呼ばれる作業です。
インシデントが発生した際には、組織内のメンバーである程度の初動対応を行うことが求められます。その対応方法に誤りがあったために、詳細な調査に支障が出るケースも少なくありません。そのため、組織内でインシデント対応に携わる方は、フォレンジックに関する必要最低限の知識を習得しておく必要があります。

サービス概要

デロイト トーマツ グループは、グローバルレベルでの長年の経験に基づく独自の方法論を活用し、フォレンジックトレーニングを策定しています。本トレーニングは初動調査を自組織で実施できることを目的としています。証拠保全の手順や初動対応の基礎手順、初動調査を実施するためのスキルを習得し、事案の白黒判定ができるようになることが目標です。

Forensicの主な流れとトレーニングの関係



トレーニング内容例

本トレーニングは、2つのカリキュラムで構成されます。証拠保全を目的としたカリキュラムでは、証拠保全の流れや考え方、実施方法を学習します。初動調査を目的としたカリキュラムでは、フォレンジックを行う上での基本的な確認ポイントとなるレジストリや削除ファイル等の調査方法を学習します。各トレーニング項目において、受講者自身が手を動かして対応するハンズオンが含まれており、実践的な研修を提供します。

目的	研修項目	研修内容	
証拠保全	証拠保全	✓ 証拠保全のプロセス ✓ 証拠保管の一貫性（Chain of Custody）の考え方 ✓ 保全対象に応じた対応方法 ✓ 物理複製やイメージファイルの概要 ✓ 複製ツールを用いた証拠保全の実施（ハンズオン）	
	関連ファイル抽出	✓ 初動調査時の重要ファイルについて ✓ ファイルの抽出方法 ✓ 複製した証拠物のマウント（ハンズオン） ✓ マウントした証拠物からの関連ファイル抽出（ハンズオン）	
初動調査	特定ファイルの検索	✓ 現存するファイル内での検索 ✓ ゴミ箱内の検索	✓ 削除済みファイルの検索 未割当領域 スラックスペース
	記憶媒体等の利用調査 （外部記憶媒体、ファイル共有）	✓ レジストリ解析 › 接続日時 › 接続デバイス情報 › ファイル共有情報	✓ デバイス接続ログ解析 ✓ イベントログ解析 ✓ ショートカットファイル （.LNKファイル）解析
	ユーザ操作の調査	✓ レジストリ解析 › 検索キーワード抽出 › 最近利用したファイル › オープン、セーブしたファイル情報	✓ ショートカットファイル （.LNKファイル）解析 ✓ ブラウザ履歴ファイル解析 ✓ Jump Lists解析
	プログラムの利用調査	✓ レジストリ解析 › ファイルの実行履歴 › ファイルの実行回数	✓ ショートカットファイル （.LNKファイル）解析 ✓ Prefecthファイル解析 ✓ Jump Lists解析
	ウェブ閲覧履歴調査	✓ Internet Explorerの閲覧履歴分析 ✓ Firefoxの閲覧履歴分析	

デロイト トーマツ リスクサービス株式会社

本　社　〒100-0005　東京都千代田区丸の内3-3-1 新東京ビル　Tel:03-6213-1300
名古屋　〒450-6337　愛知県名古屋市中村区名駅1-1-1 JPタワー名古屋　Tel:052-565-5950

デロイト トーマツ グループは日本におけるデロイト トウシュ トーマツ リミテッド（英国の法令に基づく保証有限責任会社）のメンバーファームおよびそのグループ法人（有限責任監査法人トーマツ、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザリー合同会社、デロイト トーマツ税理士法人およびDT弁護士法人を含む）の総称です。デロイト トーマツ グループは日本で最大級のビジネスプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査、税務、法務、コンサルティング、ファイナンシャルアドバイザリー等を提供しています。また、国内約40都市に約8,700名の専門家（公認会計士、税理士、弁護士、コンサルタントなど）を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループWebサイト（www.deloitte.com/jp）をご覧ください。

Deloitte（デロイト）は、監査、コンサルティング、ファイナンシャルアドバイザリーサービス、リスクマネジメント、税務およびこれらに関連するサービスを、さまざまな業種にわたる上場・非上場のクライアントに提供しています。全世界150を超える国・地域のメンバーファームのネットワークを通じ、デロイトは、高度に複合化されたビジネスに取り組むクライアントに向けて、深い洞察に基づき、世界最高水準の陣容をもって高品質なサービスをFortune Global 500®　の8割の企業に提供しています。“Making an impact that matters”を自らの使命とするデロイトの約225,000名の専門家については、Facebook、LinkedIn、Twitterもご覧ください。

Deloitte（デロイト）とは、英国の法令に基づく保証有限責任会社であるデロイト トウシュ トーマツ リミテッド（“DTTL”）ならびにそのネットワーク組織を構成するメンバーファームおよびその関係会社のひとつまたは複数を指します。DTTLおよび各メンバーファームはそれぞれ法的に独立した別個の組織体です。DTTL（または“Deloitte Global”）はクライアントへのサービス提供を行いません。Deloitteのメンバーファームによるグローバルネットワークの詳細は www.deloitte.com/jp/about をご覧ください。

Member of
Deloitte Touche Tohmatsu Limited

© 2016. For information, contact Deloitte Tohmatsu Risk Services Co., Ltd.

2016.10_0067