メモリフォレンジック

～ メモリ情報からプロセスや通信履歴を迅速解析 ～【２日間】

揮発性データであるメモリ情報を保全し、解析することで、実行プロセスや通信履歴を迅速に把握することが可能です。また、近年、HDDに痕跡を残さないファイルレスマルウェアなどの増加やファストフォレンジックの必要性から、メモリフォレンジックの技術が注目されています。メモリ情報の保全から解析まで、実践的な演習を通して、メモリフォレンジックについて学習します。

研修のゴール

・メモリ情報の保全方法及び手順を理解し、適切にメモリ保全ができるようになる
・メモリ情報の解析ツールの使い方を理解し、適切に使用できるようになる
・メモリ情報から確認できた痕跡情報から、適切に情報の解析ができるようになる

受講対象者

・デジタルフォレンジック担当者
・セキュリティ担当者、CSIRT/SOC担当者
・システム管理者

前提知識/望ましいスキルなど

・ネットワークに関する基礎知識
・OS（Windows/Linux）に関する基礎知識
・デジタルフォレンジックの基礎知識

研修内容

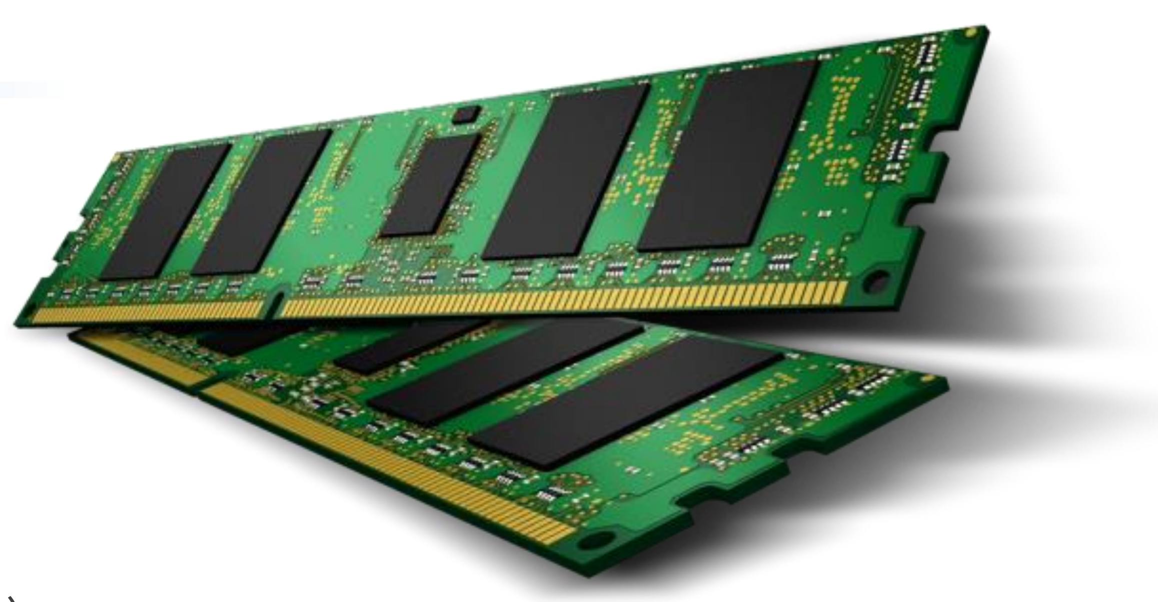
【１日目】

１．デジタルフォレンジック基礎
２．システムの全体像
　１）コンピュータシステム概要
　２）メモリの基礎、データ構造
３．メモリ保全
　１）メモリ保全の考え方
　２）メモリダンプ/保全基礎
　３）メモリイメージの変換
４．メモリ解析ツール
　１）Volatility Framework
　２）その他ソフトウェア、ツール群
５．メモリ解析基礎
　１）アーティファクト解析
　２）メモリ上のデータ解析/データカービング

【２日目】

６．Windowsシステムのメモリ解析
　１）ネットワーク
　２）Windows オブジェクト
　３）プロセス、ハンドル、トークン
　４）プロセスメモリ
　５）Windowsマルウェア解析
　６）イベントログ
　７）レジストリ情報
　８）Windows サービス
７．パスワード解析 / 暗号化解析
８．イベントの再構成
９．タイムライン作成
１０．総合演習

開催要項



・コース名：メモリフォレンジック
・開催日数：２日間（ 9:30-17:30 ）
・実施方法：オンライン、または、集合研修
・研修形式：座学、実機を使った演習
・研修費用：200,000円（税別）／人　（最少催行人数：4名）

当社の定期開催は1名様からお申込みいただけます。定期開催の実施スケジュールは、
弊社営業へお問い合わせください。また、個別開催も可能です。随時お問い合わせ下さい。

お問い合わせ・お申込み

・ストーンビートセキュリティ株式会社
・TEL 050-6877-5988　メール：training@stonebeat.co.jp
・https://www.stonebeat.co.jp#training

Stonebeat Security
Your Trusted Security Advisor