G-27

デジタルフォレンジック演習システムの開発 ～演習進行管理機能の実装と動作確認～

A Digital Forensics Training System on Security Incident ～Implementation and Verification of the Training Progress Management Function～

輿水　基秀†　福田　洋治‡　井口　信和‡
Motohide Koshimizu　Youji Fukuta　Nobukazu Iguchi

1. はじめに

組織が直面するセキュリティ上の脅威に対して，自らの役割に応じて能動的な対応ができるようなスキルを備えた人材で構成され，関連部署同士が緊密に連携できるようなセキュリティ体制の構築が求められており，CSIRT はその 1 つである．

CSIRT 人材には，初動対応で必要となる基本的な手順，操作やそこで収集したデジタル痕跡への簡易的な調査，被害拡大の防止，被害範囲の確認等でフォレンジック調査に関する知識やスキルが求められるが，それらを学ぶことができる無料の演習システムや教育用コンテンツは不足している．

豊田らは，情報工学系の大学院を想定した高等教育機関や中小企業を対象に，演習プログラムの共同開発が可能なサイバー攻撃と防御演習システムを提案している[1]．VirtualBox，Docker といった仮想化技術を利用した演習環境上に，演習プログラムを実装するシステムを構築することで，高等教育機関や中小企業において導入が容易で演習プログラムが共同開発可能なエコシステムの考え方に基づいている．

著者らは，特定の人や組織に対して，メールや Web など間接的な方法で，悪意ある第三者が仕掛けた罠に誘導するという誘導型攻撃に注目して，標的型メールによる誘導型攻撃の訓練を行うための方法，これを無料のソフトウェアを組み合わせ実現する方法を与えている[2]．VirtualBox，Vagrant を用いた仮想環境上に攻撃メールを用いた Web を介した誘導型攻撃のインシデントの訓練シナリオを用意し，Java 言語によりシナリオ作成補助，訓練内容提示と操作・状況提示の機能を試作し，動作確認を行っている．

本研究では，情報系の初学者を対象にマルウェア感染，不正アクセス，DoS・DDoS 攻撃，記憶媒体等の紛失・盗難，メールの誤送信などのセキュリティインシデントにおけるフォレンジック調査の過程の知識やスキルを学ぶための VirtualBox，Vagrant などの無料の仮想化技術に基づく学習者の PC 上で動作させる演習システムを開発している[3]．

この演習システムでは，閉じた仮想ネットワーク上に標的ホスト，攻撃ホスト等を配置し，攻撃ツールやコマンドを実行，セキュリティインシデントを発生させ，適切なロガーの配置，その設定を検討する演習や，実際にロガーを配置，設定した上でのエビデンスの収集，保存，保護，解析の演習を想定している．

著者らはこれまで，演習シナリオとその演習資料，それに合わせた VirtualBox，Vagrant による演習環境のファイルセットを作成し，演習環境管理機能と演習進行管理機能の実装を進めており，本稿では，演習進行管理機能の実装とその動作確認について報告する．

2. デジタルフォレンジック演習システム

本研究では，セキュリティインシデントにおけるフォレンジック調査の過程の知識やスキルを学ぶための VirtualBox，Docker などの無料の仮想化技術に基づく学習者の PC 上で動作させる演習システムを開発する．

演習システムの要件は，以下のとおりである．

要件 1　・・・　ロガーの配置と設定の後，攻撃を体験する．次に取得したログに対してフォレンジック調査を行い，調査内容をフォレンジックレポートにまとめるという一連の過程をエミュレータ上で体験，演習ができる．

要件 2　・・・　学習者のノート PC でいつでも，どこでも，多種多様な攻撃に対するフォレンジック調査のシナリオの演習が無料で実施できる．

要件 3　・・・　学習者は演習環境（仮想環境）の使用，設定と管理等の複雑なコマンドや GUI の操作を必要としない．

要件 4　・・・　学習者のノート PC 上の演習環境（仮想環境）で起こった個々の事象について，学習者に説明やヒント，コメントが提示できること．

上記の要件 1～4 を満たすように演習システムを考案した．本演習の構成と動作を図 1 に示す．

学習者は，演習シナリオに従って，標的ホストと攻撃ホストを操作し，ロガーの配置や設定をした後，攻撃を体験，取得したログに対して，フォレンジック調査するところま

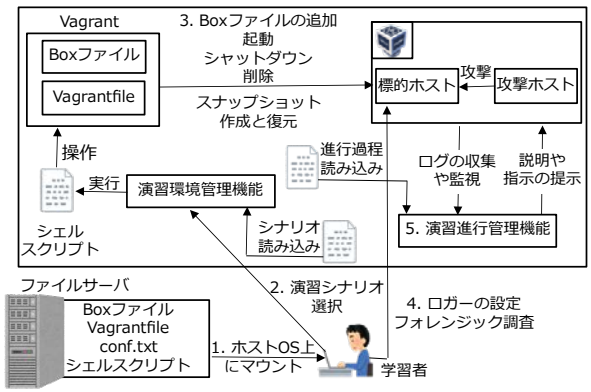

図 1 演習システムの構成と動作

† 近畿大学大学院総合理工学研究科, Graduate School of Science and Engineering，Kindai University

‡ 近畿大学情報学部/情報学研究所, Faculty of Informatics, Kindai University / Cyber Informatics Research Institute，Kindai University

で，仮想環境上で演習を行うことができるので，要件 1 に対応すると考えられる．

デジタルフォレンジック演習は，学習者の PC 上で，Vagrant，VirtualBox を用いた仮想環境を動作させ，仮想マシンの挙動をエミュレートすることで実現しているため，要件 2 を満たすと考えられる．

学習者は，演習環境管理機能の GUI からボタン操作することで，ファイルサーバから Box ファイルの追加，標的ホストと攻撃ホストの起動，標的ホストと攻撃ホストのスナップショットの作成と復元，標的ホストと攻撃ホストのシャットダウン，Box ファイルと標的ホスト，攻撃ホストの削除ができる．以上のことから，要件 3 に対応すると考えられる．

演習進行管理機能は，仮想環境上の標的ホストと攻撃ホストのユーザ操作やシステム，サービス，アプリケーションなどのログを取得，監視・分析することで，学習者が行った操作やシステム，サービス，アプリケーションで起こった事象に対して，説明や指示，ヒントを提示する機能であり，要件 4 に対応すると考えられる．

3. 演習進行管理機能の実装と動作確認

3.1 機能の実装

演習進行管理機能の実装に使用した技術を，図 2 に示す．

演習シナリオに合わせて Vagrant により標的ホストや攻撃ホストの仮想 OS の Box ファイルを展開し，VirtualBox に追加，設定し，起動させる．

標的ホストや攻撃ホストでは，システムやサービス，アプリケーションのログを残す設定を行い，さらにユーザ操作を取得，記録するロガーを動作させる．各ホストのログファイルは，仮想マシンと物理マシンの間で共有フォルダを用意し，ホスト毎に分けて保管するように設定する．

用意した演習シナリオでは，Windows の標的ホストできいろがぁ[4]を，Linux の攻撃ホストで script コマンドを動作させ，ログファイルを更新するバッチファイル，シェルスクリプトをそれぞれ書いた．

共有フォルダに保管される各種ログファイルは，Java の WatchService により作成，追加のイベントを監視し，その都度，ファイルに新たに書き込まれた部分に対して，文字列の検索を行い，イベントの有無を検出する．決まったイベントを検出した場合，Java の Swing で作成した GUI を介してメッセージを学習者に提示する．

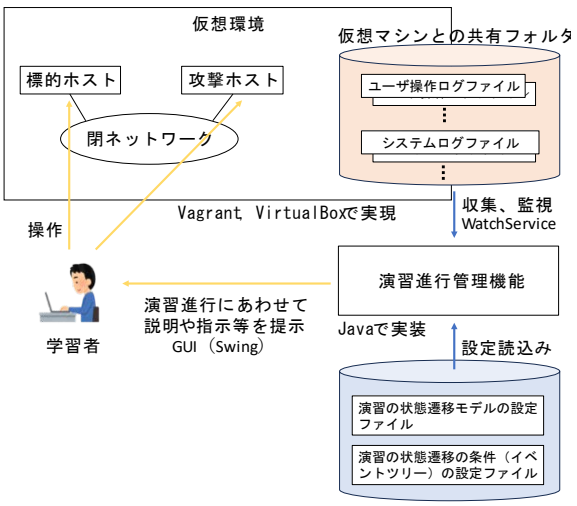

図 2 演習進行管理機能の実装

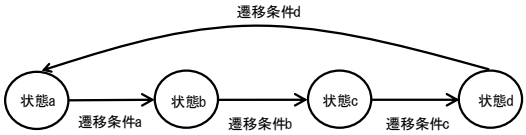

図 3 演習シナリオの進行過程に合わせた状態遷移モデルの例

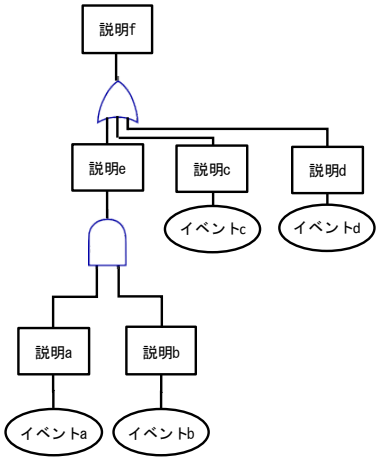

図 4 状態遷移モデルにおける各状態への遷移条件となるイベントツリーの例

演習進行管理機能では，図 3 のように，演習シナリオの進行過程に合わせた状態遷移モデルの設定ファイルを用意しておき，演習時にこれを読み込む．

各状態への遷移条件は，図 4 のように，イベントツリーのかたちで設定ファイルを用意しておき，演習時にこれらを読み込み，各種ログファイルを監視する．

イベントツリーにあるイベントの有無を，各種ログファイルの中に決まった文字列が出力されたかどうかで判断し，イベントを検出した場合，予め用意した説明や指示，ヒントのメッセージを学習者に提示する．

3.2 設定ファイルの作成

ドライブバイダウンロード（DBD）攻撃に対するフォレンジック調査の演習シナリオに合わせて，状態遷移モデルの設定ファイルと状態遷移条件のイベントツリーの設定ファイルを作成する．

DBD 攻撃に対するフォレンジック調査の演習シナリオでは，図 5 のような，事前準備，攻撃体験，フォレンジック調査，終了の 4 つの状態を持つ状態遷移モデルが考えられる．遷移条件 a，b，c，d は，それぞれの状態で，必要とされるユーザ操作が行われたことを，イベントツリーのかたちで表したものである．

事前準備では，Windows Event Log と Tshark のログ取得設定を行う．Windows Event Log の設定は，監査ポリシーサブカテゴリの設定を有効にして監査ポリシーのサブカテゴリ設定を上書きできるようにする．詳細な監査ポリシーのオブジェクトアクセスカテゴリからサブカテゴリのファイル

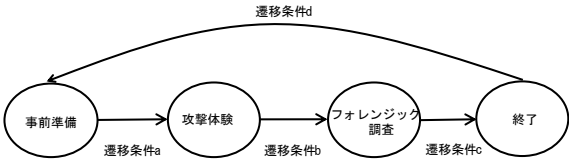

図 5 DBD 攻撃に対するフォレンジック調査の
演習シナリオの状態遷移モデル

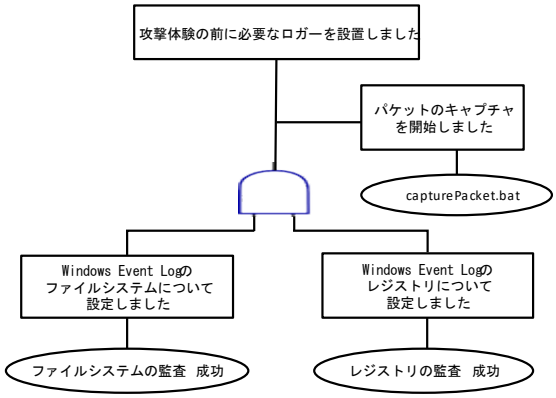

図 6 遷移条件 a のイベントツリー

システムの監査とレジストリの監査を有効にして操作が成功したときに Windows Event Log に残るようにする．Tshark の設定では，capturePacket.bat を実行することでネットワークパケットのキャプチャを開始する．イベントツリーは図 6 のように作成した．

攻撃体験では，まず擬似マルウェアをダウンロードするサーバの起動，悪性 Web サイトの作成，リバースシェル接続を行うためのポート開け待ち受ける．次に標的ホストから悪性 Web サイトにアクセスし擬似マルウェアがダウンロード，実行されることで攻撃ホストから標的ホストを遠隔操作する．その後，攻撃ホストから標的ホストに永続的なバックドアを設置し攻撃体験を終了する．事前準備で設定した Windows Event Log と Tshark を用いて取得した攻撃体験のログはフォレンジック調査で使用する．イベントツリーは図 7 のように作成した．

フォレンジック調査演習では，初めに Wireshark で攻撃体験時にダウンロードされた擬似マルウェアの抽出を行う．Tshark で収集したネットワークパケットの pcap ファイルを Wireshark で開く．送信元：192.168.56：102，プロトコル：TCP，Length：1514 のパケットを右クリックし，TCP ストリーム，追跡の順でクリックして名前を付けて Raw 形式で保存する．擬似マルウェアは，悪性 Web サイトに閲覧したときにダウンロード，実行されたので送信元は攻撃ホストとなる．また，Length：1514 は大きいファイルをダウンロードしたとき，連続する複数のパケットに分けられるため，そのうちの一つを選択することで複数のパケットが一つのファイルとして保存される．次にバイナリエディタで抽出した擬似マルウェアを開き，余分なヘッダの削除と拡張子の確認を行う．ASCII コードのマジックナンバーより前のヘッダを削除することでファイルの抽出が完了し，マジックナンバーから拡張子 exe がわかる．次に，Windows Event Log のファイルシステムとレジストリに対して行われた操作を調査する．攻撃体験で取得した Windows Event Log を

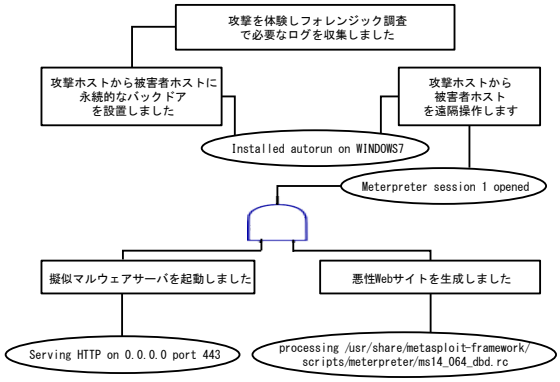

図 7 遷移条件 b のイベントツリー

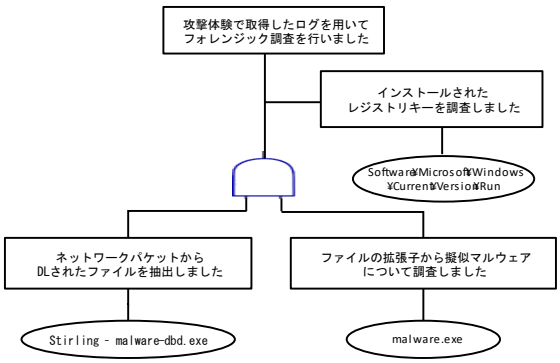

図 8 遷移条件 c のイベントツリー

Event Log Explorer で開く．ファイルシステムと拡張子 exe でフィルタリング，時間を昇順で表示してイベントログを見ていくと，デスクトップ上になかった malware.exe というファイルが確認できる．次に，デスクトップ上に作成されていた malware.exe でフィルタリングすることで，その malware.exe によって新しいレジストリキーがインストールされていることが確認できる．イベントツリーは図 8 のように作成した．

3.3 機能の動作確認

著者らはこれまでに，演習環境管理機能の実装のほか，ドライブバイダウンロード攻撃（CVE-2014-6332）に対するフォレンジック調査の演習シナリオ，演習の資料，演習環境のファイルセット（標的ホスト：Windows7 32bit SP1(Internet Explorer8)と攻撃ホスト；Kali Linux　v2021.2 の仮想 OS）を作成している．

ここで新たに，演習進行管理機能を Java（eclipse 2022-09, java sdk 8）で実装し，演習シナリオに合わせて，状態遷移モデルの設定ファイルと状態遷移条件のイベントツリーの設定ファイルを作成したので，その動作確認を行うことにした．

VirtualBox（6.1.38）と Vagrant（2.3.4）を PC（CPU：Intel Core i7-6700K 4．0GHz，Main Memory：32GB，OS：Ubuntu 22．04．1 LTS）上に導入し，ドライブバイダウンロード攻撃に対するフォレンジック調査の演習シナリオ，演習の資料，演習環境のファイルセットを用いて，演習進行管理機能を動作させる．

ドライブバイダウンロード攻撃シナリオに対するフォレンジック調査でレジストリキーを調査したときの操作画面を図 9 に示す．図 9 では画面上が演習進行管理機能の表示

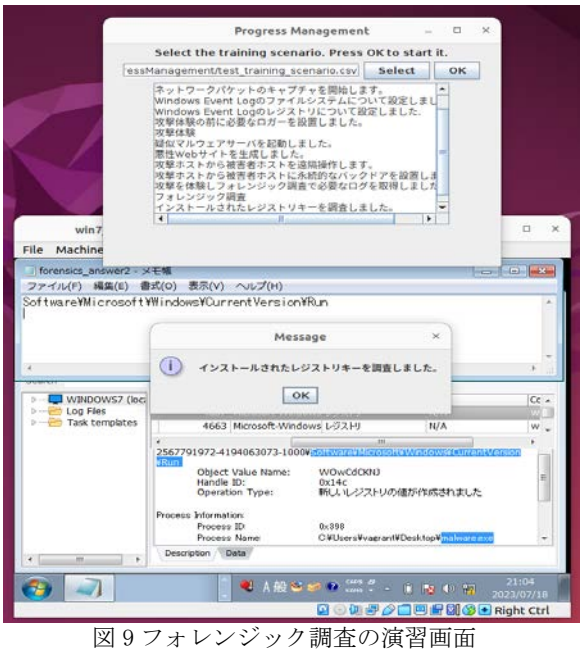

図 9 フォレンジック調査の演習画面
（上：演習進行管理機能
中央：操作に対してメッセージを表示
下：フォレンジック調査を行う被害者ホスト）

ウィンドウ, 中央がイベント完了時に表示されるメッセージ, 下がフォレンジック調査を実施する被害者ホストとなっている. 演習進行管理機能の表示ウィンドウで演習シナリオの CSV ファイルを選択することにより演習進行管理機能を開始できる．演習進行管理機能の表示ウィンドウから現在の状態を表示し各状態遷移モデルに定義されたイベントを満たすことで操作内容が提示できていることがわかる. 画面下では，攻撃体験時に収集したログを使用して被害者ホスト上でフォレンジック調査を行なっている．図 5 のイベントツリーで定義されているイベントが指定したファイルに入力または出力されると説明が表示される. Windows Event Log の調査から発見したレジストリキーを forensics_answer2.txt に入力することでフォレンジック調査のイベントを満たし画面中央に現在の操作内容についてリアルタイムで表示できていることが確認できる.

4. まとめ

著者らはこれまで，演習シナリオやその演習資料，それに合わせた VirtualBox，Vagrant による演習環境のファイルセットを作成し，演習環境管理機能と演習進行管理機能の実装を進めており，本稿では，演習進行管理機能の実装とその動作確認について報告した.

今後の課題として，他の攻撃に対するフォレンジック調査の演習シナリオ，演習資料，設定ファイルも含めた演習環境のファイルセットの作成，演習システムとしての学習効果や使い易さ、運用の手間等の評価，実験の実施が挙げられる.

参考文献

[1] 豊田真一，中田亮太郎，長谷川久美ほか，”エコシステムで構成するサイバー攻撃と防御演習システム CyExec の提案，” コンピュータセキュリティシンポジウム 2018 論文集，Vol.2018，No.2，pp.1301-1306（2018）

[2] 清時耀，福田洋治，井口信和，”インシデントの仕組み学習と体験を可能とするセキュリティ訓練システムの開発-web を介した誘導型攻撃の訓練の検討-，” 2018 年度電気関係学会関西連合大会，pp.330-331（2018）

[3] 輿水基秀，福田洋治，井口信和，”セキュリティインシデントにおけるデジタルフォレンジック演習システムの開発，” 情報処理学会第 85 回全国大会，6ZC-04（2023）

[4] Vector，”きいろがぁ，” https://www.vector.co.jp/soft/win95/util/se322072.html，ref. July 20th，2023.