G-05

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 ～学習者操作ログ収集機能の実装～

A Digital Forensics Training System on Security Incident ～Implementation of a Function to Collect Learners Operation Logs～

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，設定した上でのインシデントに関係するログの収集，保存，保護，解析の演習を想定している．

これまで著者らは，演習環境管理機能と演習進行管理機能を実装し，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てきた．

本稿では，演習システムにおける学習者のキーボード，マウスの操作情報を記録する学習者操作ログ収集機能，学習者の操作ログを用いて学習者の演習を評価する演習結果表示機能を新たに実装したので報告する．

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．

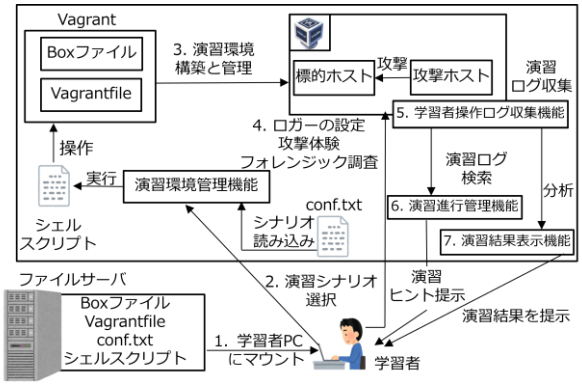

図 1 演習システムの構成と動作

† 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

要件 5　・・・　演習終了後の学習者に対して演習結果を提示し，演習理解度の確認や復習の補助ができ，セキュリティの観点からログファイルが削除されること．

従来の要件 1～4 に新たに要件 5 を加えて，これらを満たすように，図 1 のような演習システムを構築することを考える．

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．

学習者操作ログ収集機能は，学習者のキーボード入力とマウス操作を記録しログファイルとして出力する機能であり，収集したログファイルを分析することで個々の事象に対して学習者への説明ができることから要件 4 に対応すると考えられる．

演習結果表示機能は，学習者操作ログ収集機能で収集したログファイルを分析し，演習内容の正誤判定と演習時間をテキストファイルに出力後，学習者の操作ログファイルが自動で削除されることから，要件 5 に対応すると考えられる．

3. 学習者操作ログ収集機能

学習者操作ログ収集機能と演習結果表示機能の実装に使用した技術を，図 2 に示す．

学習者操作ログ収集機能は，キーボード操作ログとマウス操作ログを収集してログファイルに出力する機能である

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．

標的ホストと攻撃ホストの起動後，学習者操作ログ収集機能を標的ホストと攻撃ホストの仮想マシン上で実行し，学習者は演習シナリオに従って演習する．学習者が，演習中に標的ホストと攻撃ホストの仮想マシン上で行うキーボード操作とマウス操作のログをログファイルとして収集する．

収集されたログファイルは，物理マシンと仮想マシンの間にある共有フォルダに保管する．

学習者操作ログ収集機能で収集されたログファイルは，演習進行管理機能を用いてリアルタイムにコメントや説明を提示する際や演習終了後に演習結果表示機能を用いて演習の正誤判定と演習時間を学習者に提示する際に活用できる．

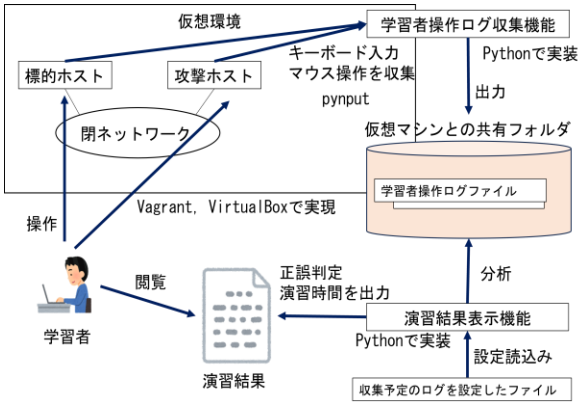

図 2 学習者操作ログ収集機能と
演習結果表示機能の実装

3.1　キーボード操作のログ収集

キーボード操作のログ収集では，キーボードの入力を監視し，その入力された文字列とキーボード入力開始時のウィンドウタイトルのテキストをログファイルに記録する方法を示す．

キーボード入力の監視は，Python ライブラリの pynput を使用して，学習者のキーボード操作をキャプチャしている．pynput は，Python でキーボードやマウスの入力を制御および監視するためのライブラリである[4]．学習者操作ログ収集機能では，キーボードから Enter キーまたは tab キーが押下された場合に，キーボードから入力中の文字列がログファイルに出力される． SPACE キーが押下された場合は，入力中の文字列を保持する変数に対して半角空白を加え，BackSpace キーが押下された場合は，入力中の最後の文字を削除することでタイプミスの際に，キーボード入力された文字列が判読不能になることを防いでいる．ESC キーが押下された場合は，学習者操作ログ収集機能を終了し演習結果表示機能を実行する．また，学習者操作ログ収集機能では CTRL キーや SHIFT キーなどの特殊キーは，ログの分析に必要がないため，ログファイルには出力されない．

ウィンドウタイトルのテキストは，Google Chrome のタブ上に表示されている文字列や Power Point でファイルを開いた際に画面中央上に表示されるファイル名などのことであり，どのウィンドウやタブを開いているのか表すものである．

ウィンドウタイトルのテキストは，キーボード入力時に，ウィンドウハンドルとプロセス ID を取得し，これを引数として GetWindowTextW 関数を使用することで取得している．GetWindowTextW 関数は，指定されたウィンドウタイトルのテキストを取得するための API である[5]．ウィンドウハンドルは，Windows OS において ウィンドウを一意に識別するための値であり，ウィンドウタイトルの変更などに使われる．また，プロセス ID は，実行中のプログラムを一意に識別するためのものである．

キーボード操作のログ収集手順としては，キーボード入力の開始時に GetWindowTextW 関数を使用して，ウィンドウタイトルのテキストをログファイルに出力する．その後，

pynput ライブラリを使用してキーボード入力の内容を出力することで学習者がどのウィンドウでキーボード操作をしているのか，把握することができる．

学習者操作ログ収集機能は，学習者が入力したコマンドやテキストとそのウィンドウを詳細に記録することで演習手順の分析や演習後の学習者に対してフィードバックを提供する際に活用することができる．

例えば，演習として学習者がターミナルでコマンドを入力している場合，コマンド入力時にウィンドウタイトルを取得した後，その入力されたコマンドが全てログとして記録されます．これらのログを収集することによって，演習中の学習者に対してターミナル上で特定のコマンドを実行した場合に説明やヒントを提示することができる．また，演習終了後に，演習時間や実行コマンドの正誤を提供する際に活用できる．

3.2 マウス操作のログ収集

マウス操作のログ収集は，マウスのクリックイベントを監視し，クリックが発生したウィンドウタイトルのテキストとその座標を収集しログファイルに記録する方法を示す．

マウス操作の監視は，Python ライブラリの pynput を使用してマウスのクリックイベントをキャプチャしている．pynput は，Python でキーボードやマウスの入力を制御および監視するためのライブラリである[4]．pynput を使用してマウスのクリックイベントを監視することでマウスクリック時の座標を取得することができる．マウスクリックの座標を収集することでウィンドウの中でどの機能やボタンを使用しているのか分析することができる．

ウィンドウタイトルのテキストは，マウスのクリック時にウィンドウハンドルとプロセス ID を取得し，これを引数として GetWindowTextW 関数を使用することで取得している． GetWindowTextW 関数は，指定されたウィンドウタイトルのテキストを取得するための API である[5].

マウス操作のログ収集手順として，マウスクリック時に GetWindowTextW 関数と pynput ライブラリを使用して，ウィンドウタイトルのテキストと座標をログファイルに出力する．

この機能は，学習者が演習を行う際，GUI の画面操作のみの場合に，ウィンドウタイトルのテキストとマウスのクリック座標を記録することで演習手順の分析や演習後の学習者に対してフィードバックを提供する際に活用できる．

例えば，演習シナリオに従い，学習者がフォレンジックツールを使用して GUI 操作で攻撃の痕跡を調査する場合，そのフォレンジックツールのウィンドウタイトルとＧＵＩ操作中にクリックした座標を収集することができる．これらのログは，演習終了後に学習者が演習シナリオに沿って意図した演習がＧＵＩ操作で行われたのか分析する際に活用できる．

3.3 機能の使用例

学習者操作ログ収集機能の使用例として Google Chrome から kindai unipa と検索し，検索結果から Web サイトの UNIVERSAL PASSPORT EX へのログインを試す一連の流れを演習として想定する．

上記の演習を行い，学習者操作ログ収集機能を使用してログを収集した場合，収集したログファイルは以下の図 3 のようになった．図 3 は収集したログファイルを表として見やすくしたものである．

1 行目　Mouse Click at (2391, 1062) - PID:23900 [Code.exe] [keylogger.py - 学習操作ログ収集機能 - Visual Studio Code]
2 行目　Mouse Click at (2272, 326) - PID:25208 [chrome.exe] [新しいタブ - Google Chrome]
3 行目　kindai unipa
4 行目　Mouse Click at (2233, 487) - PID:25208 [chrome.exe] [kindai unipa - Google 検索 - Google Chrome]
5 行目　Mouse Click at (2447, 353) - PID:25208 [chrome.exe] [UNIVERSAL PASSPORT EX - Google Chrome]
6 行目　kindai
7 行目　taro

図 3　Google Chrome でキーワード検索後に Web サイトへのログイン試行を演習として想定し学習者操作ログ収集機能で収集したログファイル keylog.txt

2 行目の「Mouse Click at」と「新しいタブ - Google Chrome」のログからマウスのクリックで Google Chrome をクリックし新しいタブを開いていることが確認できる．3 行目は，「kindai unipa」と出力されていることから Google Chrome の検索バーから「kindai unipa」と検索していることが確認できる．4 行目の「Mouse Click at」と「kindai unipa - Google 検索 - Google Chrome」のログから Google Chrome の検索バーから「kindai unipa」と検索しページ遷移後のウィンドウをクリックしていることが確認できる．5 行目の「Mouse Click at」と「UNIVERSAL PASSPORT EX - Google Chrome」から 4 行目の検索結果の UNIVERSAL PASSPORT EX をクリックし，遷移後のページを開いていることが確認できる．6 行目と 7 行目から UNIVERSAL PASSPORT EX のページ上で「UserID:kindai」，「PassWord:taro」と入力していることがわかる．

4. 演習結果表示機能

演習結果表示機能は，学習者操作ログ収集機能で収集したログファイルを分析し，演習終了後に演習内容の正誤判定○×と演習時間を表示する．その後，学習者操作ログ収集機能で収集したログファイルを削除する．

演習結果表示機能は学習者操作ログ収集機能を実行中に Esc キーを押下することで学習者操作ログ収集機能が終了し，演習結果表示機能が実行される．

4.1 正誤判定

演習結果表示機能の正誤判定は，想定した演習で出力されるログ commandList.csv と分析対象のログファイル keylog.txt の二つのファイルを入力とし，演習結果が記載される result.txt が出力される．commandList.csv であらかじめ設定した文字列が keylog.txt に含まれている場合は，「文字列 - ○」と出力される．あらかじめ設定した文字列が含まれていない場合は，「文字列 - ×」と出力される．

図 4~6 で正誤判定の処理手順について説明する．図 4 のように正誤判定では，初めに commandList.csv の一行目 user で keylog.txt の一行目から順に文字列を検索する．3 行目で

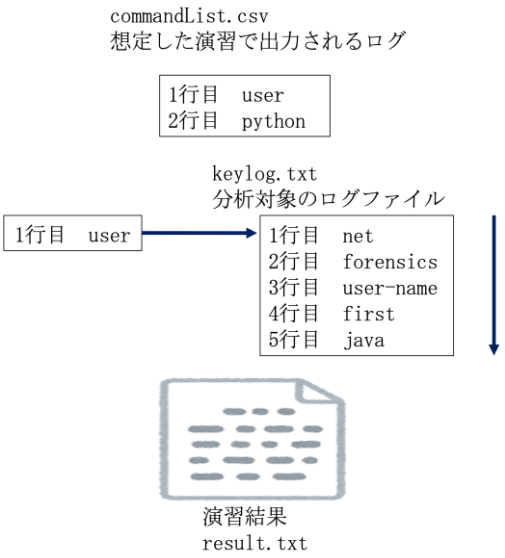

図 4 正誤判定例 1

検索対象の user が含まれている文字列 user-name が発見されると図 5 の result.txt に正誤判定として「user - ○」が出力される．検索対象の文字列が見つかった場合は，見つかった行の次の行から検索を開始し，文字列が見つからなかった場合，以前見つかった時の行から検索を開始する．次に commandList.csv の 2 行目 python で keylog.txt の 4 行目から順に文字列を検索する．図 6 のように，文字列 python で検索し最後の行まで見つからなかった場合，演習結果として「python - ×」と result.txt に出力される．

4.2 演習時間の計測

演習時間の計測は，python の time[6]モジュールを使用する．学習者操作ログ収集機能の開始時間と終了時間を収集して計算することで，演習結果表示機能の実行時に演習時間を出力している．学習者操作ログ収集機能の終了時間は，学習者操作ログ収集機能を Esc キーで終了した際の時間を取得している．演習時間は，「演習時間:○○時間○○分○○秒」の形式で出力される．

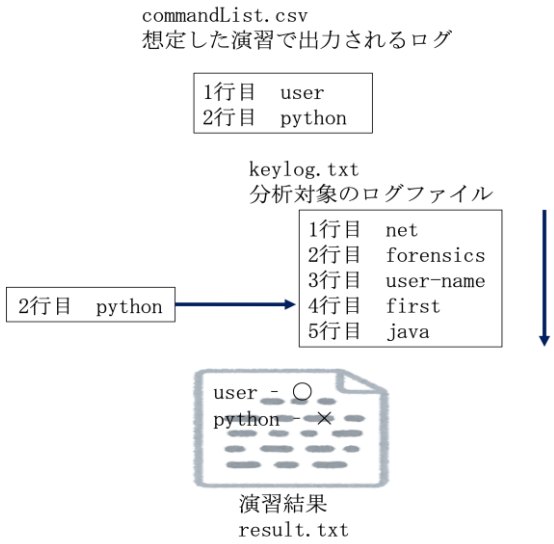

図 5 正誤判定例 2

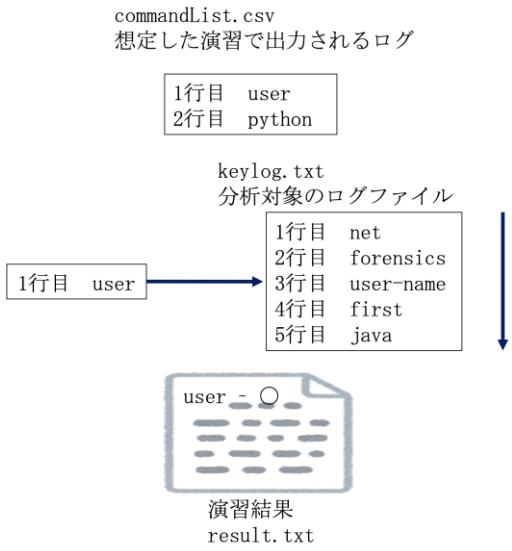

図 6 正誤判定例 3

4.3 機能の使用例

図 11 を演習として想定し取得するログをあらかじめ設定したファイル commandList.csv(図 7)と分析対象として学習者操作ログ収集機能で収集したログファイル keylog.txt(図 3)の二つのファイルを入力として演習結果表示機能を実行した実行結果を図 8 に示す．図 8 の演習結果表示機能の実行結果から 1～5 行目では演習として想定したログが収集できているのか「文字列 –○」で示されていることが確認できる．7 行目では「演習時間:○○時間○○分○○秒」の形式で出力できていることが確認できる

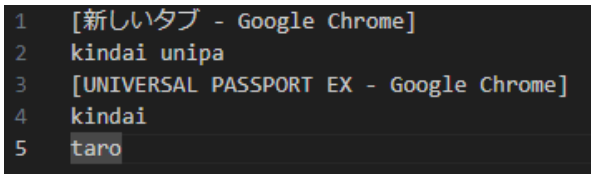

図 7 「3.3 機能の使用例」想定した演習で
取得するログを設定したファイル commandList.csv

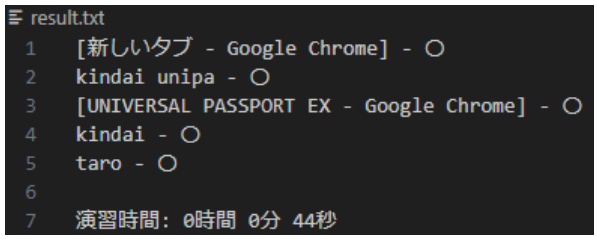

図 8 演習結果表示機能による
演習内容の正誤判定と演習時間の表示 result.txt

5. まとめ

本稿では，新たに作成した学習者操作ログ収集機能と演習結果表示機能について報告した． 学習者操作ログ収集機能によって，キーボード入力マウス操作を収集することで学習者に演習内容に応じた柔軟な説明を提示できる．また，演習結果表示機能によって演習終了後にフィードバックを提供することができる．これらの機能によって，理解度の補助やインストラクターの負担を軽減することが期待できる．

今後の課題として，演習システムを使用した際の学習者の教育効果，学習者の演習システムのセットアップと演習中の使い易さ，教員の演習システムの演習コンテンツの作成・準備の手間について利用評価実験を実施することが挙げられる．

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～Web ページ改ざんシナリオの設計～，” 情報処理学会第 86 回全国大会，2ZD-08（2024）

[4] Moses Palmér：pynput Package Documentation, 入手先<https://pynput.readthedocs.io/en/latest/>, （参照 2024-7-23）.

[5] Learn Microsoft：GetWindowTextW 関数 (winuser.h), 入手先<https://learn.microsoft.com/ja-jp/windows/win32/api/winuser/nf-winuser-getwindowtextw>, （参照 2024-7-23）.

[6] Python Docs： time - Time access and conversions, 入手先<https://docs.python.org/3/library/time.html>, （参照 2024-7-23）