G-08

インシデントの仕組みの体験学習を可能とするセキュリティ訓練システムの開発 -情報収集作業を支援する訓練シナリオ作成機能の検討-

Development of Security Training System Enabling to Learn Mechanism and Experience of Incident - A Function of Creating Training Scenario For Supporting Information Gathering –

清時 耀†　　福田 洋治‡　　井口 信和‡
Akira Kiyotoki　Youji Fukuta　　Nobukazu Iguchi

1. 序論

インシデントの再発予防では，組織の内部者は，情報や情報システムにアクセスする権限を持つ者の場合が多く，ID 管理やアクセス制御等の技術的な対策では限界がある事から，不正行為を低減するための管理や制限，教育の強化徹底等が主に行われる 1).

著者らは，組織内で起こるセキュリティインシデントの再発防止において，実施されるセキュリティ訓練の円滑な実行の支援をするため，起こった事を分かりやすく伝える，組織内で起こった Web を介した攻撃を学習，体験できるセキュリティ訓練システム(以下，本システム)の開発を進めている 2).

訓練シナリオを作成するにあたって，あるインシデントを完全または部分的に再現するために，インシデントレポート，攻撃パターン，脆弱性や設定不備等の情報を収集する作業が発生する．しかしながら，各種の公開情報のデータベースから，これらの情報を集めて来る作業は，手間がかかり，シナリオ作成者の負担となっている．

本稿では，著者らのセキュリティ訓練システムの訓練シナリオの作成において，インシデントレポート，攻撃パターン，脆弱性や設定情報に関する情報収集の作業を支援する機能の追加を検討する．

2. セキュリティ訓練システム

発生するインシデントは，組織によって異なるため，デジタルフォレンジックの技術や手法に基づいて起こった事象を再現，訓練に使用することが望ましく，特に組織の内部者を狙った Web を介した誘導型攻撃は深刻 3)で対応が求められていることから，要件 1 を設定する．

PMT4)，ELM5)の議論に基づけば，個人をインシデントの関係者と同じ状況におき，自身の判断，行動の結果として何が起こるのかを体験でき，かつ危機感を喚起するメッセージを分かりやすく伝えることが，個人の態度変容に影響を与えると考え，要件 2，要件 3 を設定する．

要件 1 … 組織で起こった Web を介した誘導型攻撃を含むインシデントを再現できること．

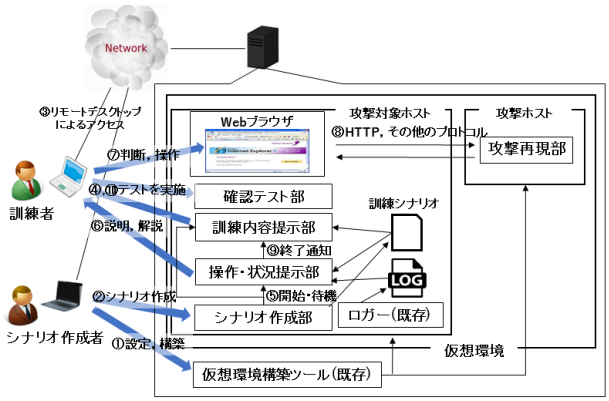

図 1　Web を介した誘導型攻撃の訓練システムの構成

要件 2 … 個人に状況を判断，端末を操作させてその結果として何が起こるか体験できること．

要件 3 … 個人の端末操作の結果，起こった個々の事象について説明できること．

要件 1～3 を満たすシステムの構成を図 1 に示す．シナリオ作成者は，組織で起こったインシデントに基づいて，仮想環境構築ツールを用いて，訓練のための攻撃対象ホスト，攻撃ホストの OS，アプリケーションを設定し，シナリオ作成部を操作して，訓練シナリオを作成，登録する．

訓練者は，使用している Windows PC から攻撃対象ホストへネットワークを経由してリモートデスクトップ接続し攻撃対象ホストを操作することでインシデントに関わる事象を体験し，周辺の情報に基づき行動を選択，判断し，妥当な行動がとれるかどうかの訓練を行う．

攻撃再現部は，ペネトレーションテストに用いられる Metasploit Framework で実際にあった攻撃を再現する．攻撃を再現する際には，Metasploit Framework で予め用意されているエクスプロイトを使用する．

攻撃を行う環境を用意するために，シェルスクリプト等を用意しており，操作・状況提示部などがシナリオファイルを読み込んだ際に，シェルスクリプトが実行され，攻撃を行う環境を用意する．攻撃再現部は，被攻撃ホストからのアクセスを待ち受ける．仮想環境上に，攻撃再現部を稼働させた攻撃ホストと，攻撃対象ホストを配置して，訓練者にリモートデスクトップで攻撃対象ホストを操作させることにより，要件 1 と要件 2 に対応すると考えられる．

訓練内容提示部は，訓練シナリオに基づいて，訓練者の立場・状況・仕事といった訓練内容のメッセージを提示す

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

‡ 近畿大学理工学部,Faculty of Science and Engineering, Kindai University

る．シナリオ作成部は，1 つのインシデントに関する原因，事象の関係性と，各ノードで提示するメッセージ，訓練内容のメッセージから成る訓練シナリオの作成を支援する．

操作・状況提示部は，訓練者の操作に応じて攻撃対象ホストの OS，アプリケーションの挙動を，ロガーの出力をモニタしながら訓練シナリオに基づいて未成立の事象の有無を判断し，各ノードのメッセージを提示する．これにより要件 3 に対応すると考えられる．

3. 訓練シナリオ作成支援機能の追加

訓練シナリオを作成するにあたって，あるインシデントを完全または部分的に再現するために，インシデントレポート，攻撃パターン，脆弱性や設定不備等の情報を収集する作業がシナリオ作成者の負担となっている．

訓練者が本システムを使用して得られる訓練の効果を高めるために著者らが必要と考えた要件 1〜3 の他に，シナリオ作成者の負担を小さくし，多種多様な訓練シナリオを用意できるように，新たに要件 4 を設定する．

要件 4 …訓練シナリオを作成する際，あるインシデントを再現するための情報収集が容易であること．

今回シナリオ作成部に，入力されたキーワードに応じて，脆弱性や攻撃パターン，設定情報に関する情報を収集する事ができる訓練シナリオ作成支援機能を追加した．訓練シナリオ作成支援機能の構成を図 2，訓練シナリオ作成支援機能の画面を図 3 に示す．脆弱性や攻撃パターン，設定情報に関する情報の収集元として，JVN や CVE，CWE，CAPEC，CCE が挙げられる．

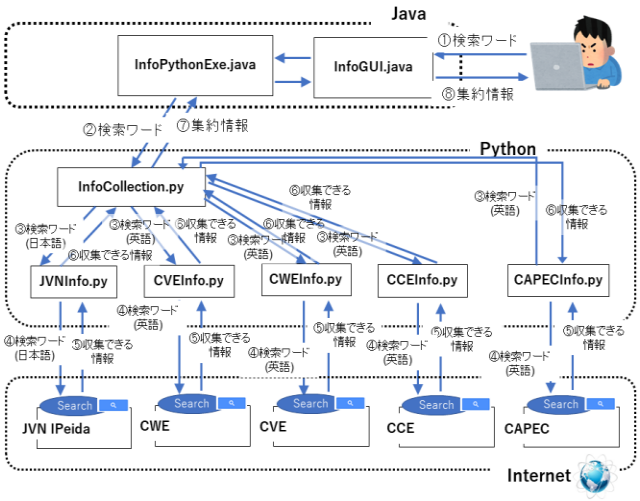

図 2 訓練シナリオ作成支援機能

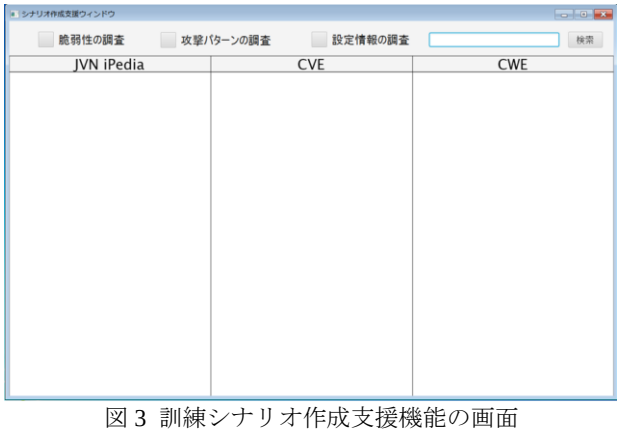

図 3 訓練シナリオ作成支援機能の画面

JVN(Japan Vulnurability Notes)は，日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供し，情報セキュリティ対策に資することを目的とする脆弱性対策情報ポータルサイトである．脆弱性が確認された製品とバージョン，脆弱性の詳細や分析結果，製品開発者によって提供された対策や関連情報へのリンクなどが掲載されている．

CVE(Common Vulnerabilities and Exposures)は，個別製品中の脆弱性を対象として，米国政府の支援を受けた非営利団体の MITRE 社が採番している識別子である．脆弱性検査ツールや脆弱性対策情報提供サービスの多くが CVE を利用している．その CVE 識別番号の管理サイトには，プログラム上のどこの部分にセキュリティの問題があるか等を記載した脆弱性の概要(Descpription)や製品開発ベンダサイトの URL がリストアップされている参考 URL(Referenc-es)が記載されている．

CWE では，SQL インジェクション，クロスサイト・スクリプティング，バッファオーバーフローなど，多種多様にわたるソフトウェアの脆弱性を識別するための，脆弱性の種類（脆弱性タイプ）の一覧を体系化して提供している．CWE には，脆弱性のタイプが書かれたビュー(View)や共通の特性を持つ脆弱性タイプをグループ化したカテゴリー(Category)や個々の脆弱性の属性が書かれた脆弱性(Weakness)のセクションが記載されている．

この三つからは脆弱性に関する多くの情報を取得する事が可能なので，これらから脆弱性を攻撃される事による被害，攻撃される原因や脆弱性の対象に関する情報を収集する．

CAPEC(Common Attack Pattern Enumeration and Classification)は，セキュリティ攻撃パターンを網羅的に分類・カタログ化したものである．CAPEC の情報を用いれば攻撃手法に関する情報共有をスムーズに行うために利用でき，インシデントの攻撃タイプ分類の参考とすることができる．CAPEC からは，攻撃パターンに関する情報に加えて，攻撃の分類や攻撃手法に関する情報を収集する．

CCE(Common Configuration Enumeration)は，「設定上のセキュリティ問題」を解決するために，コンピュータセキュリティの設定項目に，一意の番号を付与している．CCE 識別番号管理サイトには，セキュリティ設定項目に付与された識別番号である CCE 識別番号やセキュリティを確保するために必要な設定項目が書かれている設定項目の概要，設定項目に設定する値のタイプが記載されている．CCE からは，攻撃を成功させるか否かが決まるセキュリティの設定に関する情報を収集する．これらから情報を収集すれば，このユーザに脆弱性や攻撃パターン，設定情報に関する情報を提供できる．

訓練シナリオ作成支援機能を用いて，訓練シナリオを作成する際の様子を説明する．まず，シナリオ作成部を立ち上げると，状態遷移表と訓練シナリオ作成支援機能の二つのウィンドウが立ち上がる．訓練シナリオ作成支援機能には，脆弱性の調査か，攻撃パターンの調査か，設定情報の調査か，を決めるチェックボックスがある．チェックを付けた後，訓練シナリオ作成支援機能のウィンドウの検索ウィンドウに文字を打ち込み，検索のボタンがクリックされると，チェックされた調査項目に応じた情報収集を開始する．

脆弱性の調査が選択されれば，シナリオ作成支援機能がJVNで検索し，JVNのサイトから，脆弱性の概要・詳細情報，想定される影響，CVEの識別子の情報，CVEのサイトに繋がる情報を収集する．そして，情報の収集が完了すれば，作成支援ウィンドウに，情報が表示される．CVEやCWEで該当するインシデントが存在すれば，情報をウィンドウで表示する．CVEの情報であれば，DescriptionとReferenceの情報を表示し，攻撃の対象・攻撃による被害等に関する情報を利用者に表示する．CWEの情報であれば，CWE識別子の情報も記載されている場合，CWEの分類項目(CWE-400 Uncontrolled Resource Consumptionなど)の情報もウィンドウで表示する．

これらの受け取った情報を FT 図に追加していく，そして調べたい項目があれば，訓練シナリオ作成支援機能のウィンドウの検索ウィンドウに文字を打ち込み，検索のボタンがクリックし，情報を取得するという流れを繰り返す．

攻撃パターンの調査が選択されていれば，シナリオ作成支援機能が CAPEC のサイト内を調査し，攻撃の手順や内容・対象などが書かれた Descrpition(概要)や比較的攻撃パターンが似ている攻撃パターンの一覧が記載された RelationShips(関連項目)等の識別子の詳細情報を表示する．また，設定情報の調査が選択されていれば，シナリオ作成支援機能が CCE のサイト内の Excel ファイルがダウンロードし，Excel ファイル内の Description 内の文字を検索し，キーワードに当てはまる文章，項目を表示する．

これらの調査でも，訓練シナリオ作成支援機能のウィンドウの検索ウィンドウに文字を打ち込み，検索のボタンがクリックし，情報を取得するという流れを繰り返す．この訓練シナリオ作成支援機能により，脆弱性や攻撃パターン，設定情報に関する調査の作業を支援できる．

4. 動作確認

PC(CPU: Intel Core i5-4460 3.2GHz，Main Memory:16GB，OS: Windows 10 Education 64bit)上に，VirtualBox を用いて Windows7 32bit SP1 を配置し，Windows7 内でシナリオ作成支援機能を追加したシナリオ作成部の実行ファイルを動作させる．

一例として，動作実験も兼ねて，標的型メール攻撃のシナリオを作っている様子を述べる．最初に，シナリオ作成部の実行ファイルをクリックし，シナリオ作成部を起動させる．

図 4 のようにシナリオ作成部のウィンドウが表示される事を確認した．ウィンドウ内にある脆弱性の調査，攻撃パターンの調査，設定情報の調査のチェックボックスのいずれかを，クリックし，チェックをつける．JVN や CVE，CWE から正しく情報が取得できているかを確認する為，脆弱性の調査のチェックボックスをクリックし，ウィンドウ内の検索ウィンドウに，「標的型メール攻撃」，「Adobe Flash」のキーワードを入力し，検索ボタンをクリックする．

図 5 のように，JVN，CVE，CWE 内のフィールドに，単語に関係する識別子やタイトル名，公表日，CVE・CWE の識別子，Description 等の情報が表示されている事を確認した．単語に関係する識別子やタイトル名，公表日，CVE・CWE の識別子，Description 等の情報や一部 Web ブラウザで調査した情報を基に，FT図を基に作られたシナリオを作成し，シナリオファイルに書き込んだ．

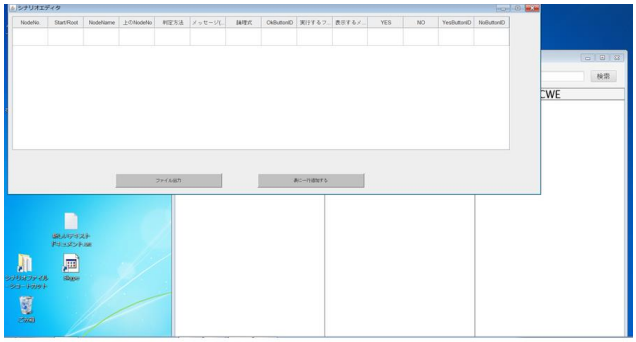

図 4 シナリオ作成部の起動画面

図 5 検索後の訓練シナリオ作成支援機能の画面

5. 関連研究

浅井氏らの研究では，技術的攻撃対策を回避して，インシデントが発生した場合に，円滑にインシデント対応をするには訓練を実施する必要があり，訓練実施の準備に必要な，訓練シナリオの作成作業を支援するシステムが開発されている 6).

豊田氏らの研究では，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が提案されている 7).

八代氏らの研究では，インシデントレスポンスにおける技術要員としての初期段階の学習機会の提供を目標として，体験型のセキュリティ学習システムの提案と構築を行っている 8).

増山氏らの研究では，高校生に対する将来における情報セキュリティへの備えの必要性から，シナリオに基づいて標的型メールの判別と対応を学習させる教材の開発をしている 9).

本システムは，組織に属していてかつ IT 技術に精通していない人物を対象とし，クライアントの端末で実際に発生したインシデントを再現，セキュリティ訓練を行うことを想定している．

6. 結論

著者らは，組織内で起こるセキュリティインシデントの再発防止において，実施されるセキュリティ訓練の円滑な実行の支援する目的で，起こった事を分かりやすく伝える，組織内で起こった Web を介した攻撃を学習，体験できるセキュリティ訓練システムの開発を進めている 2).

本稿では，訓練シナリオを作成するにあたって，あるインシデントを完全または部分的に再現するために，攻撃パターン，脆弱性や設定情報に関する情報収集を支援する機能を検討，シナリオ作成部の機能を拡張するかたちで試作し，動作を確認した．

参考文献

1)jstage:組織のセキュリティー文化を反映するシーサート活動, jstage(オンライン)，入手先 <https://www.jstage.jst.go.jp/article/johokanri/59/2/59_96/_pdf>(参照 2017-11-14)

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，電子情報通信学会関西支部学生会, vol.23，pp.14(2018)

3)NEC:企業を狙う標的型攻撃の動向とサイバーセキュリティ対策ソリューション， NEC(オンライン)，入手先 <http://jpn.nec.com/techrep/journal/g15/n01/pdf/150122.pdf>(参照 2017-10-20)

4)Rogers, R.W.: A protection motivation theory of fear appeals and attitude change,Journal of Psychology,vol.91,pp.93-114(1975).

5)Petty, R.E. and Cacioppo, J.T.: The elaborative likelihood model of persuasion,Advances in Experimental Social Psychology, vol. 19, pp. 123-205(1985).

6)浅井健志，河内清人，祢宜知孝：サイバー攻撃訓練システムにおける訓練シナリオ生成方法の提案，CSEC，Vol.2016，No.10，pp.1-7(2016).

7)豊田真一，中田亮太郎，長谷川久美ら: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，no.22-25，pp.1301-1306(2018)

8) 八代 哲， 高橋 和司，渡辺 亮平ら：体験型サイバーセキュリティ学習システムの提案と構築，コンピュータセキュリティシンポジウム，no.23-25 pp.1453-1460(2015)

9) 増山一光：シナリオによる標的型メール対策教材を用いた情報セキュリティ教育の実践， 教育情報研究，Vol.33，No.1，pp.25-32(2017).