「マルチメディア，分散，協調とモバイル
(DICOMO2018)シンポジウム」 平成30年7月

サイバーセキュリティ演習システムにおける柔軟な制御のためのフレームワーク設計

山口 礼央[1]　知念 賢一[1]　篠田 陽一[2]

概要：高まるサイバー攻撃の脅威を背景として，ますます高まるサイバーセキュリティの必要性に対し，セキュリティ人材の育成は急務となっている．セキュリティ人材の育成には，座学による学習だけでなく，演習による実践的な経験を積む必要がある．コンピュータ上に特別に構築する仮想空間（サイバーレンジ）上で行われるサイバーセキュリティ演習における，受講者に合った演習を実現するためには，受講者の回答を踏まえた出題を実現するようなフィードバック機能が必要である．本研究では，フィードバック機能を実現し，さらに演習実施者が自由に演習を設計することが可能なフレームワークを検討する．本稿では，サイバーセキュリティ演習における既存システムを比較し，演習とは何かを整理し，必要な要素・技術を明らかにした上で，柔軟な制御を実現するフレームワークの設計を行う．

キーワード：セキュリティ演習，サイバーレンジ，セキュリティ教育，フレームワーク

Design of Framework for Flexible Control in Cyber Security Exercises

Reo YAMAGUCHI[1]　Ken-ichi CHINEN[1]　Yoichi SHINODA[2]

1. はじめに

クラウドサービスなどの普及に伴い，サイバー攻撃の手口は多様化し，その被害は増加の一途を辿っている．個人としての被害だけでなく，企業や官公庁などにとって，組織におけるインシデントは社会的信用の失墜や事業の停止につながり，結果として組織活動の継続が困難となるリスクを孕んでおり，サイバーセキュリティの必要性はますます高まっている．そうした中で，各大学や企業，研究所においてインシデントに対応する能力を養うために，サイバー攻撃や防御の演習が実施されている．サイバーセキュリティ演習の環境として，サイバーレンジと呼ばれる，コンピュータ上に特別に構築する仮想空間が用いられる．本研究では，サイバーレンジを用いた演習システムについて検討する．

サイバーセキュリティ演習受講者の熟練度や経験，受講目的などは様々であり，実施者はそれぞれの受講者に合わせた演習を行う必要がある．本研究では，サイバーセキュリティ演習実施者が自由に演習を設計できるようにすることを目的とする．そのために演習とは何かを整理し，必要な要素・技術を明らかにした上で，柔軟な制御を実現するフレームワークの設計を行う．

[1] 北陸先端科学技術大学院大学 先端科学技術研究科
Graduate School of Advanced Science and Technology, Japan Advanced Institute of Science and Technology

[2] 北陸先端科学技術大学院大学 情報社会基盤研究センター
Research Center for Advanced Computing Infrastructure, Japan Advanced Institute of Science and Technology

2. 既存システム

2.1 CyTrONE

CyTrONE[1] は北陸先端科学技術大学院大学（JAIST）の Cyber Range Organization and Design（CROND）NEC 寄付講座によって開発された，サイバーセキュリティ演習フレームワークであり，トレーニングコンテンツとトレーニング環境管理を統合するアプローチを通じて，トレーニング環境構築のプロセスを簡素化することが目指されている．トレーニング主催者の入力とトレーニングデータベースに基づいて，CyLMS というヘルパーツールを介してコンテンツ記述処理を行い，トレーニングコンテンツを学習管理システム:LMS(Learning Management System) にアップロードする．また CyRIS[2] というサイバーレンジインスタンシエーションシステムを介してトレーニング

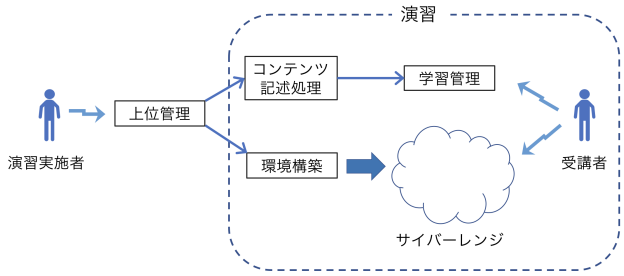

図 1　現行フレームワーク

環境を構築する．受講者は LMS にアクセスしてトレーニングコンテンツを参照し，サイバーレンジに接続して必要な演習を行い，LMS を介して回答をすることができる．問題のレベルや種類を設定し，確定することで自動的にそのサイバーレンジを生成してくれる機能に強みを持つシステムである．図 1 に現行フレームワークとして CyTrONE のフレームワークを示す．

2.2　Alfons

NICT の安田らによって開発された Alfons[3] はサイバーセキュリティ実験における，模擬ネットワーク環境を構築するための，テンプレートとなる OS ディスクイメージに個々のノードの差分となる実行バイナリや設定ファイル，ドキュメントファイルといったコンテンツを挿入することで，ビルディングブロック式にノードを生成し，構築コストを削減するシステムである．

2.3　CABIN

CABIN[4] は NICT の太田らによって開発された，サイバー演習に必要なリアリティを維持しながら監視/観測する統合サイバー演習環境であり，雛型となるトポロジを利用したサイバー演習環境の構築をサポートする．リアリティの支援や監視/観測機能による評価支援，ロールバックにより，主催者の運用の簡便化を実現する．CABIN は複数の物理サーバーを 1 つの大きな仮想環境として，サイバー演習環境用にそれぞれリソースを提供する．実線で区切られているのは独立している様子を表しており，他のサイバー演習環境からの影響は受けない．各主催者は，提供されたリソース上でサイバー演習環境を構築する．各主催者は，CABIN 上で提供されている雛型トポロジを用いてサイバー演習環境を構築できる．CABIN が提供するリアリティ支援機能や監視/観測機能は，主催者の選択によって利用が可能である．

2.4　CYDERANGE

NICT ナショナルサイバートレーニングセンターによって開発された CYDERANGE[5] は，演習シナリオの自動生成，演習環境の自動構築等を可能とする演習自動化システムシミュレーター等でも用いられる次世代の演習データ記録方式の世界規格である Experience API に準拠しており，演習環境における受講者のあらゆる操作情報を記録し，分析することで，演習の質の向上を可能とした．CYDERANGE は，受講者のプロファイル（スキルレベルや業務領域等）に合わせて，最新事例を踏まえたサイバー演習シナリオを自動的に生成することができるほか，生成されたシナリオの舞台となる演習環境を自動的に構築することができる．これらの機能の自動化により，演習の運営に係るコストを大幅に削減することが可能となった．さらに，受講者のプロファイルに合わせた効果的な演習プログラムを短時間で作成することができるようになった．また演習環境上では，演習効果の向上を目的として，データ収集エージェントが演習環境での受講者のあらゆる行動（キー入力，マウス操作，ウィンドウ操作等）をパーソナルデータの適切な取扱いに配慮しつつ収集し，データベースに蓄積する．

2.5　セキュリティ演習 (SECCON，Hardening)

SECCON[6] は情報セキュリティのコンテストである．競技としていくつか種目があるが，その中に，自チームサーバーを守りながら相手チームサーバーの脆弱性を攻める“Attack and Defense”方式のサイバー演習がある．

Web Application Security Forum（WAS Forum）[7] が開催する Hardening[8] は，基本的にチーム対抗の競技であり，脆弱性のあるビジネスシステム（EC サイト）へのハードニング（堅牢化）力の強さを総合的に競うコンペティションの形を取る．競技内容は，セキュリティを扱う人が貢献する，現実的な問題をどのように扱うかに焦点があてられる．e コマースの運用という実践的なテーマのもとで，リアルタイムで発生する複数のインシデントを克服する．Hardening には Alfons が導入されており，インスタンスの展開作業，ネットワーク設定における構築といった負荷が軽減されている．

3.　要件

サイバーセキュリティ演習を実施する際，多くの場合，演習実施者が管理する機構として，以下の三つの機能が利用されている。

- 演習の進行を管理する機能（進行管理機能）
- 演習環境を生成・管理する機能（演習管理機能）
- 受講者の学習状況の管理や問題の提示を行う機能（学習管理機能）

今回，演習環境はサイバーレンジを指す．現行ではサイバーレンジは一括生成されており，演習中に同一のサイバーレンジにおけるホストやネットワークの構成を変形させたり，受講者の挙動によって問題を変更させるといった柔軟性に欠けるといった課題がある．またそのような動作を強引に行う場合には，サイバーレンジの初期構築からや

り直さなければならず，あまり現実的な方法とは言えない．

3.1 理想とする機能

サイバーセキュリティ演習に限らず，さまざまな分野において，教育における理解度や達成度の効率化は演習受講者にとって重要である．例えば，初心者に対して難易度の高い問題を提示したり，上級者に対して難易度の低い問題の提示をする割合が多い場合，学習における無駄が多く，効率的な演習とは言えないばかりか，その学習分野への興味の低減，学習そのものに対しての意欲低下の恐れがある．受講者にとって演習における無駄の少ない，効率的な演習を行うためには，演習環境上での受講者の挙動を監視・評価し，よりマンツーマン形式に近いような，受講者のレベルに適した問題提示を逐次行うようなフィードバック機能が必要だと考える．フィードバック機能を実現するために，柔軟な制御機構を検討する．

本来演習とは，教育の場では，講義で得た知識の理解・定着の深化，暗黙知の獲得，不足し獲得すべき知識領域の自覚などを目的とした，講義形式とは対照をなす重要なものである [9]．特に情報工学における演習は他の分野での演習と比較しても出題，回答の双方で独自性，独創性が意識されるべき分野であると，長きに渡って議論されてきた [10]．実施者が受講者の能力向上に向けて設計した演習のコンテンツと，環境構築に用いられる記述ファイルが別々であるということが，そもそも演習の意に即した方法であるのか，演習のコンテンツと環境構築に用いる記述言語の統一の必要性を検討する必要がある．実施者が意図した演習を実現する上で，環境構築にはサイバーレンジを途中から生成する機能，作りかけのサイバーレンジを直すといった機能が求められる．

3.2 追加項目

既存のシステムにおいて，演習の問題生成および環境構築は分けて記述されており，パッケージとしてそれぞれの機構に入力されている．また，実施者は演習ごとに問題および演習環境の記述ファイルを用意しなければならない．サイバーセキュリティ演習において柔軟な制御が実現できれば，演習中の同一サイバーレンジにおけるホストやネットワーク構成の変形や，受講者の回答を反映した上での出題の変更といったことが可能になる．また，実施者の負担を低減させるとともに，受講者の挙動を評価し，演習実施者へ報告，その結果を基に次の演習内容を変化させるといったフィードバックが可能となる．このことにより，受講者の熟練度や経験に合わせた適切な演習の実施が可能になり，演習における受講者の効率的な能力向上が期待できる．

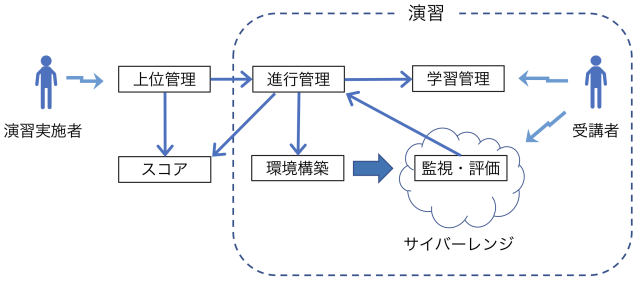

図 2 提案フレームワーク

4. 設計

4.1 全体像

本研究では柔軟な演習の制御を行うために，演習中での変更をサイバーレンジ構築システムへ命令する進行管理機構を作成する．また，演習管理機能として，一度作成したサイバーレンジの実行中における再生成，継続的な変更を追加するなどといった，サイバーレンジを逐次生成するような機能を実装する．さらに，受講者に対してより柔軟な出題ができるように，サイバーレンジ上におけるホストやネットワークの状態や，受講者の挙動を監視・評価する機能を実装する．以上のような，柔軟な制御の実現の上で必要となる，それぞれの機能の実装，図 2 のようなフレームワークを提案とする．現行フレームワークである図 1 と比較して，一方通行ではなく逐次演習を変更するような制御が可能となる．

4.2 進行管理

進行管理サブシステムは，学習管理と連携して進捗管理を行い，演習シナリオの進行を司る権限を持ったシステムとする．演習実施者は進行管理サブシステムにアクセスし，演習を開始する．また，演習における受講者の挙動を監視・評価サブシステムから報告を受け，学習管理サブシステムの変更を行い，環境構築サブシステムにサイバーレンジの変更を指示する．

4.3 学習管理

学習管理サブシステムでは，受講者が問題の閲覧や回答を行ったり，環境構築システムにサイバーレンジの生成を指示する．現行システムである CyTrONE では Moodle 等の学習管理機構において進行の機能も実装されているが，ここでは主に問題提示のみを行うことで，フィードバックを行うために柔軟に制御するべく，進行管理と機能を分離する．学習管理サブシステムにおいて問題提示を簡略化することで，進行管理サブシステムによる一括での管理が容易となる．

4.4 環境構築

環境構築サブシステムでは，VM(virtual machine) を起動し，構成要素のインストール，サイバーレンジの生成などといった環境構築を行う．現行システムである CyRIS に沿ったシステムを設計するため，サイバーレンジの作成については，YAML 形式の記述ファイルとして作成されたサイバーレンジの構成や内容を元に，手動または自動化ツールで生成することを検討する．記述ファイルは以下の三つの要素からなるものとする．

- サイバーレンジが配置されているホストに関する情報．ID，管理アドレス，管理アカウントなどを示す．
- ベースイメージに関する情報．タグタスクは，CyRIS が準備する必要があるサイバーレンジのすべてのコンテンツを定義する．例として，サイバーレンジは，wireshark のインストール，DDoS 攻撃のエミュレート，トラフィックの捕捉，エミュレートされたマルウェアの計算モードでの展開など，いくつかの設定で構成されていると想定する．
- クローニングフェーズの詳細．固有のレンジ ID，管理ネットワーク，および仮想マシンアドレスのリストを持つ．

また，一度作成したサイバーレンジの実行中における再生成，継続的な変更を追加するなどといった，サイバーレンジを逐次生成するような機能を検討する．

4.5 監視・評価

本研究では，受講者のレベルに合わせた出題を可能にするべく，監視・評価サブシステムでは，サイバーレンジ上での演習者の挙動を監視する．ネットワーク上のトラフィックを監視し，演習における評価を行うことで，受講者の挙動と演習出題の間のフィードバックが可能となる．監視・評価サブシステムにおいて，サイバーレンジ上の受講者の挙動を把握するために，キーロガーなどを用いて，ログ情報を取得する．このログ情報から，演習シナリオにおいて参加者の挙動を判断するために，各種サーバへのログイン情報やファイル等へのアクセス情報，入力コマンドのヒストリ情報などを取得する．ここで取得する情報については，演習の出題に対し，回答する上で必要となる動作情報をあらかじめ用意しておくことで，評価に必要な情報の抽出を検討する．また，取得した情報はプロセス間通信によって進行管理サブシステムに渡すことを検討する．

4.6 サブシステム間の連携

演習開始までの事前準備から演習開始，演習終了までのサブシステム間の連携を図 3 に示す．まず，実施者が上位管理システムおよびスコアシステムを起動し，2 つのシステムを演習終了まで作動させる．起動した上位管理システムは，進行管理サブシステムを起動し，起動の応答を受け取る．さらに起動した進行管理サブシステムは，環境構築サブシステムを起動し，演習の環境構築を行う．環境構築からの応答を受けた進行管理は，学習管理に対し，問題の提示を指示する．受講者は学習管理にアクセスし，提示された問題に対する回答を行う．学習管理は，進行管理に回答情報を報告する．一方，環境構築の際にサイバーレンジ上に生成された監視評価サブシステムは，進行管理からの問い合わせに対し，受講者の挙動が判断できる情報を報告する．進行管理は，報告をもとに，回答の正誤を判定し，判定の結果をスコアに反映させる．演習終了の際，上位管理は進行管理に対し終了の指示をし，進行管理は各サブシステムに対して順に終了を指示する．このときの上位管理の制御を，タイムドリブン型もしくはイベントドリブン型にするかについては検討が必要である．

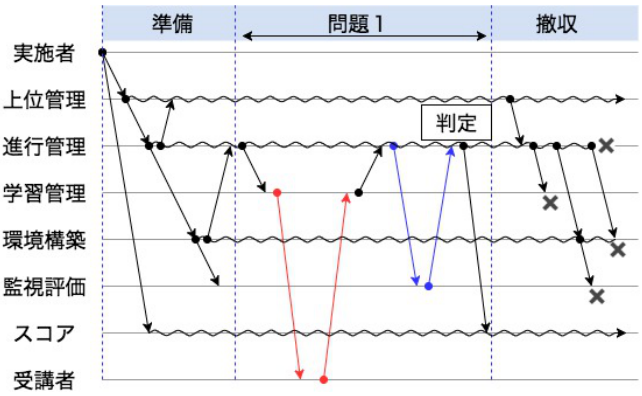

図 3　サブシステム間の連携フロー

4.7 さまざまな進行に対するサブシステム間の連携の例

サブシステム間通信の例として，一つの問題におけるヒント表示までのフローを図 4 に示す．1 周目の回答に対し，監視評価の報告から進行管理が不正解と判定した場合，進行管理はスコアを更新した後に，2 周目として学習管理にヒントの表示を指示する．この際のヒントはあらかじめ実施者によって用意されるか，受講者の回答および監視評価からの報告に基づいて提示される必要がある．また，問題 1 を終え，問題 2 に進む際の例として，図 5 のように問題の間に進行管理から環境構築に対して変更が指示され，サイバーレンジの変更が行われる．

5. おわりに

本研究ではサイバーセキュリティ演習における重要な要素としてフィードバック機能を取り上げ，そのために必要であると考えられる柔軟な制御を検討した．フレームワークを構成する各サブシステムについて，現行システムでの役割に加え，フィードバック機能を実現するために，機能を検討した．特に，進行管理サブシステムを独立して設け，各サブシステムに命令を発するような機能を検討した．また，環境構築サブシステムについては一度作成した

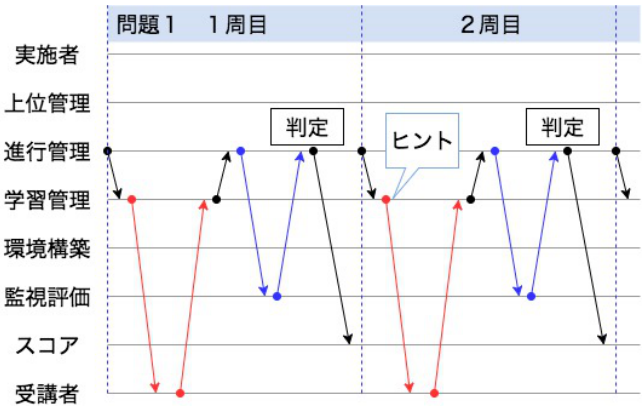

図 4　不正解の際のヒント表示

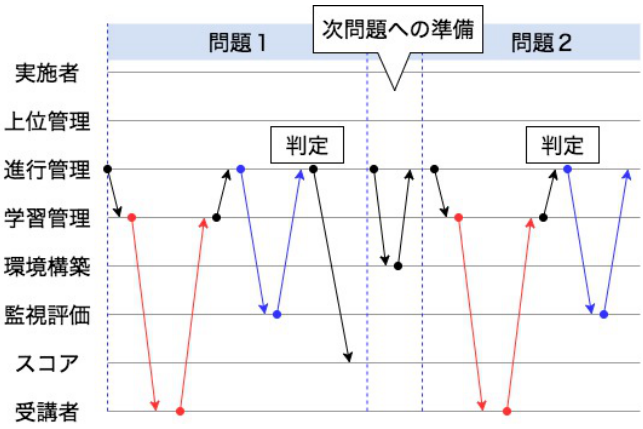

図 5　次問題に進む際の準備

サイバーレンジの実行中における再生成，継続的な変更を追加するなどといった，サイバーレンジを逐次生成するような機能を考え，監視・評価サブシステムを設けることで，進行を司る機能に演習環境上における受講者の挙動を報告し，次の動作につながるような機能を検討した．

参考文献

[1] Razvan Beuran, Pham Cuong, Tang Thanh Dat, Ken ichi Chinen, Yasuo Tan, and Yoichi Shinoda. CyTrONE: An Integrated Cybersecurity Training Framework. In *International Conference on Information Systems Security and Privacy (ICISSP 2017)*, pp. 157–166, February 2017.

[2] Razvan Beuran, Pham Cuong, Tang Thanh Dat, Ken ichi Chinen, Yasuo Tan, and Yoichi Shinoda. Cybersecurity Education and Training Support System: CyRIS. *IEICE Transactions on Information and Systems*, Vol. E101-D, No. 3, March 2018.

[3] Shingo Yasuda, Ryosuke Miura, Satoshi Ohta, Yuki Takano, and Toshiyuki Miyachi. Alfons: A Mimetic Network Environment Construction System. In *Testbeds and Research Infrastructures for the Development of Networks and Communities (TridentCom 2016)*, pp. 59–69, November 2016.

[4] 太田悟史, 安田真悟, 湯村翼, 高野祐輝. 次世代サイバー演習環境に向けて. マルチメディア，分散協調とモバイルシンポジウム 2016 論文集, pp. 1776–1782, jul 2016.

[5] サイバー演習自動化システム CYDERANGE の開発と実運用の開始. <https://www.nict.go.jp/press/2018/03/08-1.html>（2018.05.14）.

[6] SECCON:SECURITY CONTEST 2017. <https://2017.seccon.jp/about/>（2018.05.14）.

[7] Web Application Security Forum WASForum. <https://wasforum.jp>（2018.05.14）.

[8] Hardening Project 2018. <https://wasforum.jp/hardening-project/>（2018.05.14）.

[9] 小林真也, 黒田久泰, 遠藤慶一. 座学と演習の反復による教育の効果を最大化する実課題 PBL. *ISECON2015*, March 2016.

[10] 都倉信樹ほか. 情報処理専門教育について: 情報処理教育における実験・演習. 情報処理, Vol. 32, No. 10, 1991.