情報処理学会論文誌 Vol.59 No.12 2232–2245 (Dec. 2018)

サイバーセキュリティゲーム演習ツール セキュ・ワンの提案

近江谷 旦[1,a)] 宮本 大輔[1,b)] 門林 雄基[1,c)]

受付日 2018年5月12日, 採録日 2018年9月7日

概要：サイバー攻撃による被害が増加していることを受け，セキュリティ人材の不足が問題視されている．セキュリティ担当者はつねに変化・進化するサイバー攻撃に適切に対応するため，モチベーションの維持が重要な課題である．本稿では，上記の課題を克服するため，既存のサイバーゲーム演習では着目していない領域に焦点を当てたサイバーゲーム演習ツール，セキュ・ワンを提案する．既存のサイバーゲーム演習ツールでは着目していないシステムの運用時のセキュリティ管理策について，学習できるように設計方針を明示している．課題であるモチベーションの維持を克服するため，学習者の動機付けに効果があることが報告されているゲーミフィケーションの仕組みを活用している．また，サイバー攻撃の手法と対策を学習できるようにサイバー攻撃の手法を辞書化した攻撃ライブラリとセキュリティ管理策のベストプラクティスである “The Critical Controls for Effective Cyber Defense（CSC)” を活用している．セキュ・ワンを用いた全 3 回のサイバーゲーム演習を実施し，参加者のアンケート結果を分析することで設計方針の達成度を評価した．評価の結果，セキュ・ワンによりセキュリティ人材の現状の能力を把握し，能力を向上させるうえで有用なツールであることを示す．

キーワード：サイバーセキュリティ，重点管理策，ATT&CK，CAPEC，ゲーミフィケーション

Proposal of Cyber Security Game Practice Tool Secure-One

Tan Omiya[1,a)] Daisuke Miyamoto[1,b)] Youki Kadobayashi[1,c)]

Received: May 12, 2018, Accepted: September 7, 2018

Abstract: The shortage of cybersecurity personnel is a major problem which is exacerbated by the increasing number of cyber attacks and the possible demotivation of the said personnel. While the lack of personnel could be fixed by training more people, in the meantime, it is important to maintain motivation among the cybersecurity team members of a given organization in order for them to appropriately respond to the changing and evolving cyber attacks. In order to overcome the above problems, we propose a cyber game exercise tool, Secure-One, which focuses on areas hitherto uncovered on existing cyber game exercises. Secure-One is comprised of a gamification mechanism that is known to be effective for learners' motivation and a design policy that leverages security control measures that are not used in existing cyber game exercises. We also make use of the Critical Controls for Effective Cyber Defense (CSC) which summarizes the best practices of security controls, and the attack libraries which are dictionaries of cyber attack methods. To validate Secure-One, we conducted cyber game exercises in three different occasions and evaluated the achievement of the design policy by analyzing the participants questionnaire results. The analysis showed that Secure-One is a useful tool for grasping the actual capabilities of cybersecurity personnel and for improving their abilities as well.

Keywords: cyber security, the critical security controls, ATT&CK, CAPEC, gamigication

1. はじめに

サイバー攻撃の脅威に適切に対抗するため，セキュリティの知識および技術を持った人材が必要とされる．また，攻撃者によりつねに新しいサイバー攻撃の手法が開発

[1] 奈良先端科学技術大学院大学先端科学技術研究科
Graduate School of Science and Technology, Nara Institute of Science and Technology, Ikoma, Nara 630–0192, Japan
[a)] omiya.tan.ol1@is.naist.jp
[b)] daisu-mi@is.naist.jp
[c)] youki-k@is.naist.jp

されており，そのトレンドも変化していることから特にセキュリティ担当者はつねに脅威の動向を注視し対応を継続することに留意しなければならない．

しかし，昨今，サイバーセキュリティ人材の不足が懸念されている．経済産業省の調査によると 2016 年時点で約 13.2 万人のセキュリティ人材が不足しており，2020 年には約 19.3 万人の不足が推計されている [1]．このような状況を受け，情報処理推進機構が毎年，作成・公開している 10 大脅威 2018 年版において，「脅威に対応するためのセキュリティ人材不足」が組織への脅威第 5 位に初めてランクインした [2]．また，ソフトバンクコマース&サービス株式会社の調査によると調査に参加した組織の 72.8%が「セキュリティ疲れ」を抱いていると回答した [3]．サイバー攻撃のトレンドや手法が毎年のように変化・進化するため，動向の確認や対応を繰り返し実施しなければならないことが要因であると考えられる．

現状を受け，セキュリティ人材を育成することおよびセキュリティ担当者のモチベーションを維持・向上させることが大きな課題であるといえる．本稿では上記の課題解決のため，カードゲーム形式でセキュリティ教育を実施するためのサイバーゲーム演習ツール（セキュ・ワン）を開発した．サイバーゲーム演習では，技術的な能力向上を目指す演習は数多く実施されているが，管理面の知識習得を目指す演習の機会は前者と比較して非常に少ない．さらに，管理面に関する知識の習得を目指すゲーム演習ツールはシステム開発時やインシデント発生後の対応に焦点を当てており，システム運用中の対策には焦点を当てていない．このため，セキュ・ワンではセキュリティ担当者・技術者に学習の動機付けを与えるとともにシステム運用中の管理面に関する知識を習得させることを目的とした．セキュ・ワンは学習者の動機付けに有効性が確認されているゲーミフィケーションの手法を取り入れている．また，最新のサイバー攻撃の手法と対策を学習するため，サイバー攻撃手法の辞書にあたる攻撃ライブラリとセキュリティ標準である “The CIS Critical Security Controls for Effective Cyber Defense（CSC）” [4] を用いている．

本稿の以降の構成は以下のとおりである．2 章で関連技術であるゲーミフィケーションおよびサイバー演習を説明し，サイバーセキュリティ分野における既存ゲーム演習の未対応領域を明示する．3 章で提案するセキュ・ワンの設計方針および設計方針を達成するためのセキュ・ワンの詳細について示す．4 章でセキュ・ワンを用いた演習とアンケート評価の分析結果によりセキュ・ワンの有用性を示す．最後に 5 章で本稿のまとめとする．

2. 関連技術

本章では関連技術であるゲーミフィケーションとサイバー演習について示す．また，これらの手法を取り入れた既存のサイバーセキュリティ教育用ツールをまとめ，既存の演習ツールでは未対応な領域を明らかにし，セキュ・ワンの適用領域を示す．

2.1 ゲーミフィケーション

ゲーミフィケーションとは課題の解決や顧客ロイヤリティの向上に，ゲームデザインの技術やメカニズムを利用する活動全般のことである．ゲーミフィケーションは様々な分野で活用されており，学習者の学習意欲を維持・向上できることが報告されている [5], [6]．被教育者の学習意欲を維持・向上させるゲーミフィケーションのフレームワークとしてゲーミフィケーション・フレームワーク [7] が作成されている．このフレームワークを用いたツールにより，学習意欲を向上できることが報告されている [8], [9]．セキュリティ分野では主にセキュリティ意識の啓発にゲーミフィケーションを取り入れた演習ツールが存在する [10], [11]．セキュリティ啓蒙だけでなくセキュリティ担当者・技術者向けのサイバー演習においても学習意欲向上のためにゲーミフィケーションの仕組みを活用できるものと考えられる．

2.2 サイバー演習

米国国土安全保障省は局地的な緊急事態から国家安全保障上の緊急事態までを適切に対処するため，「国土安全保障省演習評価プログラム（HSEEP）」[12] を作成した．

HSEEP では演習の種類を議論型の演習と実働型の演習に大別し，**表 1** のように定義している．昨今，サイバーセキュリティの分野において，HSEEP を参考にしたサイバー演習が実施されている．国内で実施されているサイバー演習の例として，内閣サイバーセキュリティセンター（NISC）による「分野横断的演習」[13] や総務省による「実践的なサイバー防御演習（CYDER）」[14] が知られている．これらは表 1 に示す演習種類の機能演習に当たるものと考えられる．本稿ではサイバー演習の中でも議論型演習のゲーム演習に焦点を当てている．議論型の演習は参加者が計画，政策，合意事項および手順等に習熟すること，または，それらを新たに開発することを目的としている．ゲーム演習では現実または仮想的な環境を模擬するデータ，規則および

表 1 演習の分類
Table 1 A classification of execise.

区分	種類	概要
実働型	総合演習	最も複雑かつ資源集約型の演習
	機能演習	複数機能の検証・評価
	ドリル	単一機関の一機能・能力を検証
議論型	ゲーム	現実・仮想状況下でのデータ・手順を体験
	机上演習	種々の問題への議論，手順の確認
	ワークショップ	参加相互作用の拡大，成果物の生成
	セミナー	戦略，計画，手順等に精通

手順等を活用し，参加者の競争心を煽る環境を構築する．参加者の決心，行動および手順等を検証し，評価することができる．ゲーム演習はさらに技術面と管理面のどちらかに焦点を当てているかにより大別できる．技術面に焦点を当てているものとして，Capture The Flag（CTF）がある．CTF の競技内容として代表的なものにサイバー攻撃で利用されている技術等を点数配分された問題として提示し，取得した点数を競うものがある．国内の代表的な CTF としては SECCON [15] があり，国内外のセキュリティ技術者の能力向上に貢献している．CTF のような技術面の能力取得を目的としたゲーム演習は国内外で頻繁に実施されている．一方で管理面の能力取得を目的とするゲーム演習は演習ツールが少なく，実施の機会も技術面のゲーム演習より少ないのが現状である．このため，本稿では管理面の知識や能力の向上を目的とするゲーム演習に焦点を当てることとした．管理面の知識は資産管理，人的セキュリティ，物理セキュリティ，運用管理，アクセス制御，システムの開発・保守，脆弱性管理，インシデント管理等に関連する広範囲な領域に及ぶ．それぞれの領域に関連する用語の意味，それらの特性に加えて，効果的に組織をサイバー攻撃から防御するための方法論等が具体的な管理面の知識として考えられる．管理面の能力にはリスク分析（システム開発時），対策の妥当性と効果の確認（システム運用時），インシデントハンドリング（インシデント発生時）を適切に実施できること等があげられる．ゲーム演習は広範囲の領域から特定の領域に焦点を当て，知識・能力の向上を図るように設計されている．次節に管理面に焦点を当てた既存のサイバーセキュリティゲーム演習をまとめ，セキュ・ワンの新規性について示す．

2.3 演習ツール（セキュ・ワン）の新規性

ゲーミフィケーションおよびゲーム演習をサイバーセキュリティに取り入れた演習ツールが作成されている．

Kaspersky Interactive Protection Simulation（KIPS）[16] はカスペルスキー社で作成された重要インフラに対するサイバー攻撃の影響をゲーム形式で体験しながら，その対策を学習できるゲーム演習ツールである．サイバー攻撃を受けている企業や組織の運用上のリスクや投資に見合った有効な対策をゲーム形式で演習する．参加者はグループに分かれ，条件や指示が書かれた複数枚のカードと決められた予算，作業時間を有効に使い，発生するインシデントに対応しつつ 5 週間という仮想期間内での生産高を競う．

インシデント対応ボードゲーム [17] はトレンドマイクロ社により作成・公開されたセキュリティインシデント発生時の対応を体感できるゲーム演習ツールである．ゲーム内で発生する架空のインシデントに対して，調査方法，復旧方法，対外的なコミュニケーション戦略等について話し合い，インシデント対応プランを決定することで自組織の対応要領の確認や問題点を見つけ出すことができる．

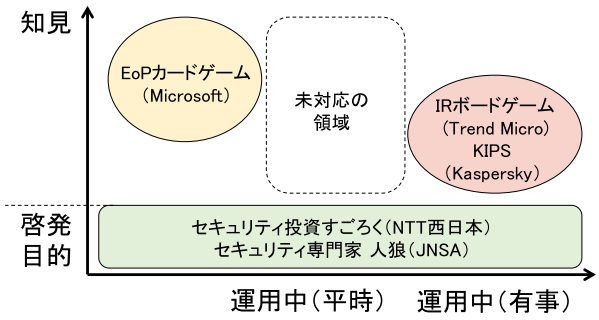

図 1 既存演習ツールの適用領域
Fig. 1 Applicable domain of existing educational tools.

The Elevation of Privilege（EoP）[18] は Microsoft 社により作成・公開されているカードゲーム形式で自組織の開発システム等における脅威を洗い出すためのゲーム演習用ツールである．演習ツールとしてだけではなく，実際にシステムへの脅威モデリングを実施するためにも用いられる．システム設計の段階で様々なメンバにより EoP を使用し，議論することで製品のリリース前に潜在的な脆弱性を修正することができる．

図 1 に既存の演習ツールと対応領域をマッピングした．グラフの横軸はシステムの開発時からセキュリティインシデント発生（運用中（有事））までの時間経過を示している．グラフの縦軸は演習ツール対象者が必要とされる知見のレベルを示している．啓発目的でゲーミフィケーションを取り入れた演習ツールはセキュリティの知見を有していない初級者を対象としている．既存のゲーム演習ツールは時系列的にはシステムの設計段階および運用中のインシデント発生時の対応を演習することができる．一方で，システム開発後の運用要領やセキュリティインシデント発生を防止するための対策について議論することが限定的である．これは既存のゲーム演習は特にシステム開発段階やインシデント対応に焦点を当てているためである．システム開発後の運用要領には導入したセキュリティ機能の設定内容の維持や妥当性の確認方法，機器やログの監視要領，運用中に生じる脆弱性の対応要領の他，教育・インシデント管理要領といった組織的な体制の強化方法があげられる．従来の演習ツールでは未対応の領域であるシステム運用中の対策に焦点を当てて議論を実施するための演習ツールが望まれる．このため，本稿では特に既存のゲーム演習ツールでは未対応の領域を議論できるツールを新規に開発することとした．

3. セキュ・ワンの詳細

前章で，既存のサイバーセキュリティ演習ツールでは十分に議論ができていない領域を明らかにした．本章では，セキュ・ワンにより既存の演習ツールの未対応領域を十分

に参加者間で議論させるためのゲームメカニズムや脅威・対策として参照したコンテンツの詳細について示す．また，ゲームの進行役にあたるゲームマスタを補助するための判定基準表について示す．

3.1 設計方針

前章までの分析をふまえ，以下にセキュ・ワンの設計方針を示す．

(1) 情報システムの運用中におけるサイバー攻撃への対策を重点的に議論することにより理解を図る．
(2) プレイヤ間での議論を通して，他プレイヤから新たなサイバーセキュリティの知見を取得する．
(3) プレイヤがゲームに没入するため，ゲームの公平性を確保する．
(4) プレイヤのモチベーションを向上させるため，競争心の高揚を図る．
(5) 最終的な取得ポイントでサイバー攻撃の脅威と対策の理解度および判断力を定量的に確認できるようにする．

上記の設計方針をどのようにセキュ・ワンに反映させたかについて，次節以降で示す．

3.2 ゲーミフィケーション・フレームワークの活用

被教育者の学習意欲を維持・向上させるため，セキュ・ワンに以下のようにゲーミフィケーション・フレームワーク [7] を適用した．

プレイヤの分類：プレイヤはセキュリティの実務担当者の他，セキュリティ分野に関心を持っている利用者も含む．サイバー攻撃および対策について専門的な用語等を使用するため，プレイヤに加えてゲームマスタの役割を追加した．ゲームマスタはセキュリティ分野に知見を有する者が担当する．

目的・ゲームコンセプト：様々なサイバー攻撃手法とそれに有効な対策をプレイヤ間の議論により理解する．

目標：攻撃を防ぐための防御カードを迅速・的確に選択し，高ポイントを得る．

可視化・フィードバック：攻撃・防御手法をカードにより可視化する．カードに付加されたポイントに応じた加減算をスコア表に記録し，プレイヤの取得ポイントの優劣を可視化する．知見を有するゲームマスタが，カードの内容について解説することにより提出したカードに対するフィードバックを行う．

ソーシャルアクション：プレイヤはサイバー攻撃への対策の有効性を口頭で説明することで他プレイヤに理解させる．

プレイサイクルデザイン：初級者でも分かりやすいルールを設定し，ターンごとに手持ちの防御カード枚数が増減する仕組みとする．

改善・運用：難易度の異なる攻撃カードセットを 2 種類用意し，プレイヤの能力に応じて攻撃カードセットを選択する．必要に応じ，カード枚数を間引きし，難易度を調整する．セキュ・ワンを用いたゲーム演習実施後，参加者からのフィードバックを分析し，ルールおよびコンテンツを改善する．

3.3 基本的なルール

攻撃および防御の 2 種類のカードセットを使用する．ゲーム参加者の人数はプレイヤ 3〜6 名，防御カードの有効性を判断するゲームマスタ 1 名を基準とする．ゲームはターン制として，一定時間経過するか攻撃カードがなくなるまでターンを繰り返す．ゲーム終了時のポイントの優劣により，勝者を決定する．1 ターンごとのゲームの進行は以下のとおり．

(1) 任意のプレイヤがゲームのリーダとなり攻撃カードセットから 1 枚カードを引き，全プレイヤが閲覧できるように攻撃カードを提示する．
(2) プレイヤは提示された攻撃カードに有効と考えられる手持ち防御カードを早いもの順で提出する．
(3) プレイヤは提出した防御カードの攻撃への有効性を他プレイヤに説明し，他プレイヤから合意が得られた場合は得点を獲得する．
(4) プレイヤ間で有効性の判断ができない場合はゲームマスタが有効性の判断を実施する．
(5) 防御カードを提出できなかったプレイヤおよび提出したが有効性を示すことができなかったプレイヤは攻撃カードに応じたポイントを減算する．
(6) 防御カードを提出したが，有効性を示すことができなかった場合はお手つきとして，次のターンは参加できない．
(7) スコア表に得点の加減算を記録する．
(8) 前ターンで最初に防御カードを提出したプレイヤがリーダとなり (1)〜(7) を繰り返す．

攻撃および防御カードに応じたポイント加減算の仕組みは下記のとおり．優先順位の高い防御カードを素早く提出したプレイヤに高いインセンティブ（ポイント）を与えることで，サイバー攻撃の脅威と対策の理解度と判断力を定量的に測ることを狙いとしている．

(A) 防御カードを提出する速度に応じて高いポイントを与える．
(B) 防御カードの種類（優先度）に応じて (A) のポイントの倍率を決定する．
(C) 攻撃カードの種類（攻撃段階）に応じて，ポイントを減算する．

図 2 にゲームターンのイメージを示す．ここではゲーム参加者は 4 名（A〜D）で防御カードを提出し，有効性を示すことができた順に 4〜1 点のポイントを得ることができるものとする．A は一番最初に防御カードを提出し，有効性を示すことができたので 4 点取得する．B は優先度の

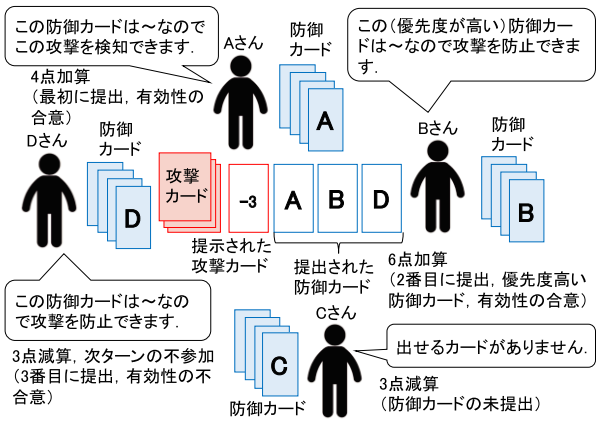

図 2 ゲームターンのイメージ
Fig. 2 Image of a game round.

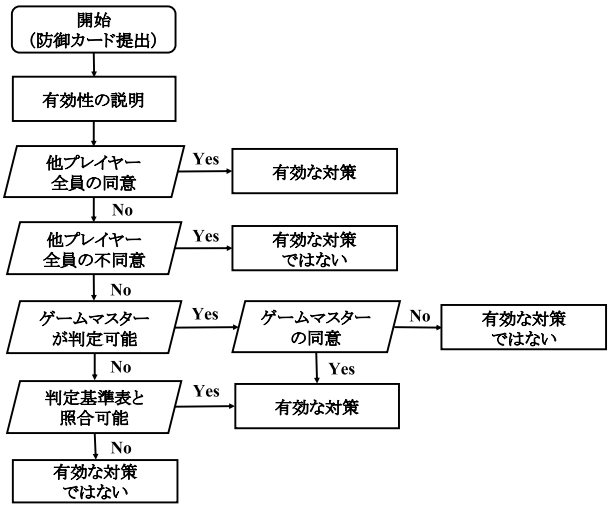

図 3 有効性判定プロセス
Fig. 3 Process of a judgement.

高い防御カードを 2 番目に提出し，有効性を示すことができたので $3 \times 2 = 6$ 点取得する．C は防御カードを提出できなかったので，攻撃カードに記載されたポイント（−3）を失う．D は防御カードを 3 番目に提出したが有効性の合意を得られなかったため，攻撃カードに記載されたポイント（−3）を失い，次のターンへの参加ができなくなる．

プレイヤは得点を取得するためには他プレイヤおよびゲームマスタに提出した防御カードの有効性を説明する必要があり，他プレイヤは説明内容に異議や補足を行うことができる．プレイヤ間で議論を誘発し，知識の共有や誤って理解している知識を是正させることを狙いとしている．プレイヤ間の議論により，サイバー攻撃手法とその対策について詳細な知識を習得することができる．

図 3 にプレイヤによって提出された防御カードの有効性判定プロセスを示す．提出された防御カードとプレイヤによる説明を他プレイヤ全員が理解し，合意した場合は有効であると判定される．他プレイヤとの議論により，意見が割れた場合はゲームマスタの知見により有効性が判定される．ゲームマスタが知見を有していない等により，有効性の判定が困難な場合は判定基準表を確認し，有効性を判定する．参加者の議論が割れた場合にゲームマスタの知見と判定基準表に頼ることで，判定の公平性が保てるようにした．

3.4 攻撃カード内容の詳細

攻撃カードは一般的な攻撃手法（Type A）およびサイバーキルチェーン [19] に基づく攻撃手法（Type B）の 2 種類のカードセットにまとめた．Type A は CSC Appendix B の内容をカード内に収まるように記載し，23 枚のカードにまとめた．Type A の攻撃手法は，CSC 開発時に CSC 管理策が様々なサイバー攻撃の脅威に適切に対応可能か確認するために使用された．Type A のカードは抽象化された内容が記述されているため，対応可能な防御カードが多く存在する．プレイヤは手持ち防御カードから適切なカードを選択しやすく，ゲームの難易度は低く設定できる．

Type B に用いるサイバーキルチェーンはサイバー攻撃の目的を達成するまでの段階を定義している．CSC ではサイバーキルチェーンの攻撃段階を横軸，NIST サイバーセキュリティフレームワーク [20] の防御段階を縦軸のマトリックスとした CIS コミュニティ脅威モデル [21] を定義し，サイバー攻撃の脅威に対する管理策の有効性を評価している．このため，CSC の管理策がサイバーキルチェーンのどの攻撃段階で有効な対策であるか考察が容易である．Type B のカードに記載する内容は MITRE 社が作成・公開している攻撃ライブラリである ATT&CK [22] と CAPEC [23] を参照した．ATT&CK はサイバーキルチェーンの初期侵害から任務目的遂行までの段階における具体的な攻撃をまとめた攻撃ライブラリである．CAPEC は攻撃の仕組みに応じて攻撃手法を辞書化した攻撃ライブラリであり，ATT&CK では定義されていないサイバーキルチェーンの初期段階から配送までの攻撃手法も辞書化している．以上のことから Type B にはサイバーキルチェーンの初期段階から配送までは CAPEC，初期侵害から任務目的実行までは ATT&CK を活用し，合計で 52 枚のカードにまとめた．**表 2** に CIS コミュニティ脅威モデルで定義された攻撃段階と ATT&CK および CAPEC で活用した項目の関係を示す．なお，攻撃段階「ツールの開発・取得」は該当する項目がなかったため，攻撃ライブラリを活用していない．「ツールの開発・取得」はそれ以降の攻撃段階を効果的に実行するための攻撃者の行為であり，ツール化される具体的な攻撃手法は他の攻撃段階における攻撃ライブラリの項目で定義されている．このため，「ツールの開発・取得」の内容は攻撃者の行為と意図が分かるように 1 枚のカードにまとめた．

図 4 に攻撃カード Type B のイメージを示す．攻撃カード内には防御カードを提示できなかった場合の減算ポイ

表 2 サイバーキルチェーン攻撃段階および活用した攻撃ライブラリの項目
Table 2 Cyber kill chain attack stages and attack libraries utilized.

攻撃段階	活用した攻撃ライブラリの項目	枚数
初期段階	情報の収集と分析（CAPEC）	6
ツールの開発・取得	—	1
配送	なりすまし（CAPEC）	5
初期侵害	実行（ATT&CK）	3
	防衛回避（ATT&CK）	6
誤用・特権昇格	権限昇格（ATT&CK）	5
内部偵察	資格情報アクセス（ATT&CK）	4
	発見（ATT&CK）	3
侵入拡大	侵入拡大（ATT&CK）	4
持続性確立	持続性（ATT&CK）	6
任務目的実行	収集（ATT&CK）	3
	情報流出（ATT&CK）	3
	遠隔操作（ATT&CK）	3

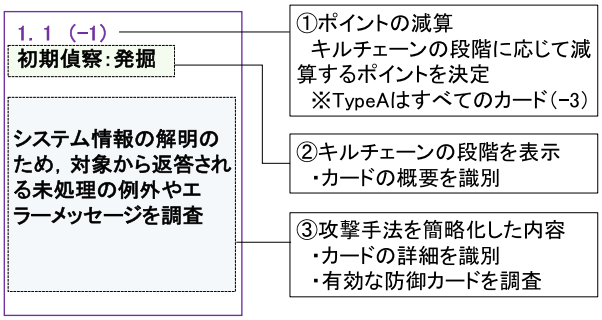

図 4 攻撃カードのイメージ
Fig. 4 Image of attack cards.

ントを明記している．減算ポイントはサイバーキルチェーンの段階により大きくなるように付加した．カードにはサイバーキルチェーンの段階および攻撃内容を簡略化し，記載した．プレイヤは攻撃カードの内容を考察し，対応可能な防御カードを選択する必要がある．攻撃カードの内容は Type A よりも具体的であり対応可能な防御カードが限定されるため，ゲームの難易度が高くなる．

攻撃カードは Type A および Type B いずれも一定の抽象度を持った内容になっている．プレイヤは攻撃カードの内容から解釈される具体的な攻撃手法を他プレイヤに説明することで，提出した防御カードの有効性を理解させることができる．プレイヤの説明により攻撃カードが具体化され，プレイヤ間の議論により攻撃カードの解釈が深化されることで，各プレイヤは詳細かつ分別された攻撃手法の理解が可能となる．

3.5 防御カード内容の詳細

自システムへのサイバー攻撃の脅威に対応するために情報セキュリティの管理策をまとめた標準は複数存在する．CSC は既知のサイバー攻撃から効果的に資産を防御するために，20 個の管理策に絞った内容になっている．管理策は最初に実施しなければならない管理策（CSC 1〜5）とそれ以外（CSC 6〜20）に分類され，管理策の優先順位が分かるようになっている．20 個の管理策はさらに 149 個のサブ管理策に細分化されており，具体的な内容が記述されている．CSC の管理策の有効性確認等の整備は CIS コミュニティにより実施されている．管理策の有効性確認には CIS コミュニティ脅威モデルとセキュリティベンダーが公表する脅威レポート（ベライゾン社 [24] およびシマンテック社 [25] 等）が活用されている．報告された新たな脅威に対し，CSC の各管理策が CIS コミュニティ脅威モデルのマトリックス上のいずれか 1 つ以上のセルに対応可能か分析する．分析により，有効性の確認および管理策の改善を実施することで最新の脅威にも適切に対応できるように整備されている．CSC は 20 個の他標準に比べて少ない優先順位付けされた管理策により最大のリスク低減効果を得られる．以上のことから防御カードは CSC のサブ管理策の内容を簡略化し，カード内に記載することとした．**表 3** に防御カードの内訳を示す．防御カードは 149 個の CSC サブ管理策のうち，高度なサブ管理策 24 個以外の 125 個のサブ管理策をカード化した．高度な対策は高度な知見を有する人材が必要条件となっており，標準的な対策ではないため，カード化しなかった．カード化したサブ管理策は NIST サイバーセキュリティフレームワークの防御段階（特定，防御，検知，反応，復旧）に対応付けできる．サブ管理策の大部分はシステム運用中の対策に焦点を当てているが，一部のサブ管理策においてはシステム開発時やインシデント

表 3 防御カードの内訳
Table 3 Breakdown of defense cards.

番号	管理策	枚数
1	許可，無許可のデバイスのインベントリ	5
2	許可，無許可のソフトウェアのインベントリ	3
3	ハードウェア，ソフトウェアのセキュアな設定	7
4	継続的な脆弱性診断および修復	8
5	管理者権限のコントロールされた使用	8
6	監査ログの保守，監視，分析	6
7	電子メールと Web ブラウザの保護	8
8	マルウェア対策	5
9	サービス等の制限，コントール	4
10	データ復旧能力	4
11	ネットワーク機器のセキュアな設定	6
12	境界防御	7
13	データ保護	2
14	Need-to-Know によるアクセスコントロール	6
15	無線アクセスコントロール	7
16	アカウントの監視，コントロール	13
17	セキュリティスキル評価，適切なトレーニング	4
18	アプリケーションソフトウェアセキュリティ	9
19	インシデントレスポンスと管理	7
20	ペネトレーションテスト，レッドチーム訓練	6

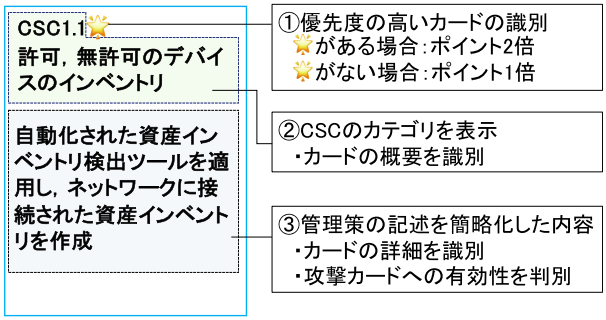

図 5 防御カードのイメージ
Fig. 5 Image of defense cards.

発生後も考慮した内容となっている．CSC18「アプリケーションソフトウェアセキュリティ」の一部のサブ管理策はセキュアコーディング等のシステム開発時に該当する内容となっており，システム開発時の対策について議論に発展する場合が考えられる．CSC10「データ復旧能力」のサブ管理策は防御段階の復旧，CSC19「インシデントレスポンスと管理」のサブ管理策は防御段階の反応に該当する内容となっており，インシデント発生後を想定しているため，インシデント発生後の対策について議論になる場合が考えられる．ただし，CSC10 および CSC19 はインシデント発生を想定して，システム運用時から実施すべき対策となっている．上述のように一部の防御カードにおいてはシステム開発時およびインシデント発生後の対策についての議論に発展する可能性があるが，そのほかの防御カードにおいてはシステム運用中の対策について重点を置いた議論ができるものと考えられる．

図 5 に防御カードのイメージを示す．CSC の管理策のうち，優先順位が高い管理策である CSC 1〜5 の防御カードを提出した場合はそれ以外の管理策 CSC 6〜20 の防御カードを提出した場合よりも 2 倍の得点を獲得できることとした．優先度が識別できるように，優先度の高いカードに識別子を付加した．カードには CSC の管理策とサブ管理策の記述を簡略化して表記した．プレイヤは防御カードの記載内容から攻撃カードへの対応の可否を判断する．

3.6 判定基準表

セキュ・ワンは知見を有するゲームマスタが重要である．知見を有するゲームマスタが参加できない場合に参加者により提出された防御カードの有効性を判定する手段が必要である．また，公平性を確保するために，ゲームマスタが参照可能な判定基準表を作成した．判定基準表には攻撃カードに対応する防御カードの一覧に加えて，防御カードがなぜ有効であるのか解説を加えた．判定基準表は以下の 3 つの要領で作成した．

・攻撃ライブラリを参照

ATT&CK および CAPEC には攻撃手法の他に低減策や検出手法が明記されている．それぞれの攻撃ライブラリを参照し，判定基準表をまとめた．

・CIS コミュニティ脅威モデルによる分析

CIS コミュニティ脅威モデルのマトリックスを使用し，攻撃カードに有効な防御カードを分析することで攻撃ライブラリに記載されていない有効な対策を考察し，判定基準表にまとめた．

・実際の演習により，有効であると判定された結果の分析

上記 2 つの要領で判定基準表を作成後，演習を実施し，判定基準表によらず，有効であるとプレイヤ間およびゲームマスタに判定された結果を分析し，判定基準表にまとめた．

上記の要領により作成した判定基準表は，攻撃カード Type A に含まれる 289 個のリスト，Type B に含まれる 507 個のリスト，合計 796 個のリストとなった．

4. セキュ・ワンを用いた演習と評価

前章でセキュ・ワンの設計意図や具体的な内容を明記した．本章では実際に，セキュ・ワンを活用した演習を実施し，参加者にアンケート形式で評価してもらうことで有用性を示す．

4.1 演習概要

セキュ・ワンの有用性を確認するため，3 回の演習を実施した．演習は SecCap [26] および ICS-CoE 中核人材育成プログラム [27] の受講生を対象として実施した．SecCap は「セキュリティ実践力のある IT 人材」を増やすことを目的に複数の大学により専門的なセキュリティ技術および知識を教育するためのプロジェクトである．ICS-CoE 中核人材育成プログラムは情報処理推進機構で実施されている社会インフラ・産業基盤のサイバーセキュリティ対策の強化をテーマに，テクノロジー（OT・IT），マネジメント，ビジネス分野を総合的に学ぶ 1 年程度のトレーニングプロジェクトである．

これらは大学院生および企業におけるサイバーセキュリティのスペシャリストを育成するためのプロジェクトであり，セキュ・ワンを含むサイバーゲーム演習の対象としては適正である．実施した演習の概要を下記にまとめた．

〈1 回目〉
実施日：H29.9.13（水）
対象：大学院生（SecCap 受講生）
人数：19 名
ゲームマスタ：知見を有する者（大学教員および CISSP 有資格者）
評価項目：他演習ツールと動機付け効果を比較

〈2 回目〉
実施日：H29.10.24（火）
対象：社会人（ICS-CoE 中核人材育成プログラム受講生）
人数：15 名

ゲームマスタ：知見を有する者（大学教員および CISSP 有資格者）
評価項目：動機付け効果の詳細
〈3 回目〉
実施日：H30.2.26（火）
対象：社会人（ICS-CoE 中核人材育成プログラム受講生）
人数：66 名
ゲームマスタ：参加者（2 回目演習の参加者でゲームルールを把握している者）
評価項目：他演習ツールと動機付け効果の詳細を比較，その他設計方針の達成度

4.2 評価項目

セキュ・ワンの有用性は動機付け効果と 3.1 節で示した設計方針の達成度を確認することにより示す．ゲーム演習は参加者の動機付けの効果を意図して作成されていることから，設計方針のうち，動機付け効果の評価はセキュ・ワンと他の演習ツールの評価を比較することとした．動機付けの効果を測定するための指標に ARCS 動機付けモデル [28] を用い，セキュ・ワンと他演習ツールを共通の指標で評価した．ARCS 動機付けモデルは 4 つの項目（注意，関連性，自信，満足）に分類される．ARCS の各項目を高めることにより，高い動機付け効果が得られるとされている．

第 1 回目の演習では，ARCS の項目に関連する 4 つの質問を 5 段階評価で回答するアンケートを作成した．セキュ・ワンを含む 3 つの演習ツールについて評価し，結果を比較した．**表 4** にアンケート内容を示す．

第 2 回目の演習では，第 1 回目の質問項目に加え，動機付け効果を詳細に分析できるように熊本大学大学院で作成・公表されている ARCS 動機付けモデル評価シート [29] を活用した．ARCS の 4 つの項目をさらに 4 つの内容に詳細化し，合計で 16 個の質問で構成される．評価シートの項目ごとの質問内容は相関があり，他の項目から独立している．**表 5** にアンケート内容を示す．

第 3 回目の演習では，動機付け効果に加えて，設計方針の達成度を確認するための質問を作成した．動機付け効果の確認は ARCS 動機付けモデル評価シートを活用し，セキュ・ワンを含む 2 つの演習ツールを比較した．動機付け効果以外の設計方針の達成度を確認するため，5 段階評価で回答可能な質問を作成した．**表 6** に設計方針に対応する質問内容を示す．なお，設計方針のうち「最終的な取得ポイントでサイバー攻撃の脅威と対策の理解度および判断力を定量的に確認できるか」については次節の評価結果を分析することで確認を行う．

そのほか，第 1 回目から第 3 回目演習において，自由記載形式で感想・意見を聴取し，定性的な評価を実施した．

表 4 ARCS に関連するアンケート内容
Table 4 Questionnaire related to ARCS.

項目	質問
注意	ゲーム時間は適切だったか
関連性	興味を持てたか
自信	ルールは理解できたか
満足	ゲーム趣旨は理解できたか

4.3 評価

セキュ・ワンを含む演習ツールを使用した演習を実施後，参加者に前節のアンケートを回答してもらった．アンケートの回答結果を分析することでセキュ・ワンを評価した．

4.3.1 動機付け効果の評価

表 7 に第 1 回目演習における表 4 のアンケート結果を示す．セキュ・ワンを含む 3 つの演習ツールの平均値（Avg.）と標準偏差（SD）の結果を比較した．セキュ・ワンの評価は他の 2 つの演習ツールに比べ，同程度以上の評価になっていることが分かる．

表 8 に第 1 回目および第 2 回目演習のセキュ・ワンにおける表 4 のアンケート結果（平均値（Avg.）と標準偏差

表 5 ARCS 動機付けモデル評価シートのアンケート内容
Table 5 Content of questionnaire on ARCS motivational model evaluation sheet.

項目	質問
1 注意	1-1（このゲーム演習は）面白かったか
	1-2（このゲーム演習は）眠くならなかったか
	1-3（このゲーム演習は）好奇心をそそられたか
	1-4（このゲーム演習は）変化に富んでいたか
2 関連性	2-1（このゲーム演習は）やりがいがあったか
	2-2（このゲーム演習は）自分に関係があったか
	2-3（このゲーム演習は）身につけたい内容だったか
	2-4（このゲーム演習は）途中の過程が楽しかったか
3 自信	3-1（このゲーム演習で）自信がついたか
	3-2（このゲーム演習は）目標がはっきりしていたか
	3-3（このゲーム演習で）学習を着実に進められたか
	3-4（このゲーム演習を）自分なりに工夫しながら進められたか
4 満足	4-1（このゲーム演習を）やれてよかったか
	4-2（このゲーム演習は）すぐに使えそうか
	4-3（このゲーム演習で）できたら認めてもらえたか
	4-4（このゲーム演習は）評価に一貫性があったか

表 6 設計方針の達成度確認のためのアンケート内容
Table 6 Questionnaire for confirming the achievement of design policy.

設計方針	質問
サイバー攻撃への対策の理解	攻撃と防御カードは理解できたか
他プレイヤの知見を共有	他プレイヤから知見が得られたか
ゲームの公平性確保	判定基準表は理解できたか
	判定基準表は役立ったか
競争心の高揚	迅速に防御カードを提出したか

表 7 アンケート結果 1（$n = 19$）
Table 7 A result of questionnaire #1.

	セキュ・ワン		ツール X		ツール Y	
項目	Avg.	SD	Avg.	SD	Avg.	SD
注意	4.05	1.19	4.05	1.50	3.21	1.34
関連性	4.63	0.74	4.53	0.75	3.89	0.72
自信	4.68	0.46	4.37	0.94	3.32	0.98
満足	3.95	0.89	4.58	0.59	3.89	0.79

表 8 アンケート結果 2
Table 8 A result of questionnaire #2.

	学生（$n = 19$）		社会人（$n = 15$）	
項目	Avg.	SD	Avg.	SD
注意	4.05	1.19	4.20	0.98
関連性	4.63	0.74	4.60	0.49
自信	4.68	0.46	4.33	0.47
満足	3.95	0.89	3.86	0.50

表 9 アンケート結果 3（$n = 66$）
Table 9 A result of questionnaire #3.

		セキュ・ワン		ツール Y	
項目	質問	Avg.	SD	Avg.	SD
1	1-1	3.94	0.80	2.97	1.01
	1-2	4.08	1.02	3.68	1.23
	1-3	3.82	0.76	3.03	1.01
	1-4	3.48	0.94	2.64	0.86
2	2-1	3.68	0.82	2.91	0.90
	2-2	3.65	0.91	3.46	0.97
	2-3	3.55	0.82	3.33	0.89
	2-4	3.74	0.89	3.15	0.96
3	3-1	2.91	0.77	2.57	0.78
	3-2	3.03	0.89	2.38	0.94
	3-3	3.29	0.75	2.95	0.93
	3-4	3.55	0.78	3.20	0.96
4	4-1	3.52	0.97	3.03	0.90
	4-2	3.00	1.04	2.48	0.87
	4-3	3.44	0.82	3.50	0.87
	4-4	3.15	0.91	2.95	0.89

（SD））を示す．学生・社会人の結果が類似していることが分かる．セキュ・ワンが学生や社会人の違いによらず，同程度の動機付け効果を与えられることを示している．

表 9 に第 3 回目演習における表 5 のアンケート結果を示す．セキュ・ワンとツール Y の結果（平均値（Avg.）と標準偏差（SD））を比較している．ツール Y と比較してもセキュ・ワンの評価が同等以上になっていることが分かる．

表 10 に第 2 回目および第 3 回目演習のセキュ・ワンにおける表 5 のアンケート結果（平均値（Avg.）と標準偏差（SD））を示す．すべての項目において，第 3 回目の結果が第 2 回目よりも低い値となっている．第 2 回目の演習ではゲームマスタに知見を有する者が担当していたが，第 3 回目では参加者が判定基準表を用いてゲームマスタを実施していたため，全体的に評価が下がったものと考えられる．

表 10 アンケート結果 4
Table 10 A result of questionnaire #4.

		2 回目演習（$n = 15$）		3 回目演習（$n = 66$）	
項目	質問	Avg.	SD	Avg.	SD
1	1-1	4.67	0.47	3.94	0.80
	1-2	4.80	0.54	4.08	1.02
	1-3	4.80	0.40	3.82	0.76
	1-4	4.40	0.88	3.48	0.94
2	2-1	4.60	0.49	3.68	0.82
	2-2	4.87	0.34	3.65	0.91
	2-3	4.47	0.62	3.55	0.82
	2-4	4.67	0.47	3.74	0.89
3	3-1	3.40	1.02	2.91	0.77
	3-2	4.00	0.89	3.03	0.89
	3-3	4.20	0.89	3.29	0.75
	3-4	4.13	0.88	3.55	0.78
4	4-1	4.40	1.02	3.52	0.97
	4-2	4.00	0.89	3.00	1.04
	4-3	4.47	0.72	3.44	0.82
	4-4	3.67	1.19	3.15	0.91

表 11 アンケート結果 5（$n = 66$）
Table 11 A result of questionnaire #5.

質問	Avg.	SD
攻撃と防御カードは理解できたか	3.35	0.84
他プレイヤから知見が得られたか	3.84	0.86
判定基準表は理解できたか	3.19	0.81
判定基準表は役立ったか	3.37	0.92
迅速に防御カードを提出したか	3.65	1.07

第 1 回目から 3 回目までの演習により，被学習者の動機付け効果の評価を実施した．既存の演習ツールと同じ指標による評価結果からセキュ・ワンは他演習ツールと同程度以上の動機付け効果が得られることが分かった．また，高い動機付けの効果を与えるためにはゲームマスタが重要であることが分かった．ゲームマスタの知見により，動機付け効果に影響を与えることが分かった．

4.3.2 設計方針の達成度の確認

表 11 に第 3 回目演習における表 6 のアンケート結果（平均値（Avg.）と標準偏差（SD））を示す．すべての項目で平均が 3 点以上の値になっており，定量的にはおおむね設計方針 (1)〜(4) を達成できたものと考える．以下に自由記載形式の回答と合わせて分析した設計方針 (1)〜(4) の達成度の考察を示す．

設計方針 (1) サイバー攻撃への対策の理解：質問「攻撃と防御カードは理解できたか」の平均値は設計方針 (2)，(4) に関連する質問への回答と比較すると低かった．プレイヤ間の議論を活性化させるため，カードの内容から具体的な攻撃手法を連想できるように工夫したことに加えてカード内に専門用語が記述されており，一部の記載内容の理解が

困難であったと回答する参加者が複数いた．しかし，他プレイヤやゲームマスタの説明を聞き，不明な用語や自分とは異なるカードの解釈を理解することで，新たな知見を取得できたと回答する参加者が多かった．このため，設計方針 (1) はおおむね達成できたものと考える．

設計方針 (2) 他プレイヤの知見を共有：質問「他プレイヤから知見が得られたか」に多くの参加者が「得られた」と回答していたことから，達成できたものと考える．

設計方針 (3) ゲームの公平性確保：設計方針 (3) は動機付け効果の評価に用いた表 5 の質問 4-4「(このゲーム演習は) 評価に一貫性があったか」と関連している．4.3.1 項で示したように表 10 から第 2 回目演習は第 3 回目演習の質問 4-4 の平均値より高く，ゲームマスタの能力により影響を受けていることが分かる．ゲームの公平性の確保はゲームマスタが知見を有している場合は十分に達成できるが，知見を有していない場合は判定基準表に依存する．質問「判定基準表は理解できたか」,「判定基準表は役立ったか」の平均値は設計方針 (2), (4) に関連する質問への回答と比較すると低かった．これは一部の判定基準表の内容にプレイヤが納得がいかない判定が含まれていたためであり，3.6 節で示した「実際の演習により，有効であると判定された結果の分析」をすることで，判定基準表の精度を高める必要性がある．上記からゲームマスタと判定基準表を組み合わせることで設計方針 (3) はおおむね達成できたが，さらなる公平性の確保のために判定基準表の精度改善が課題であるといえる．

設計方針 (4) 競争心の高揚：質問「迅速に防御カードを提出したか」に多くの参加者が迅速に防御カードを提出したと回答していたことからおおむね達成できたものと考える．

設計方針 (5) の達成度は参加者の総得点と表 6 の結果を分析することで確認した．

設計方針 (5) 理解度および判断力を定量的に確認：図 **6** に第 3 回目演習における「カード内容を理解し，迅速な提出」の値と総得点の散布図を示す．「カード内容を理解し，迅速な提出」は表 6 のアンケート項目「攻撃と防御カードは理解できたか」と「迅速に防御カードを提出したか」の回答を乗算した値である．「カード内容を理解し，迅速な提出」の値と総得点の相関係数は $r = 0.43$ となり，今回の演習では中程度の正の相関を認められた．参加者は 4〜8 人程度のグループを形成し，演習を実施していたことから，ターンの回数や点数配分等，一部異なる条件で演習を実施していた．若干の条件の不均一があるものの，セキュ・ワンにより,「サイバー攻撃を理解し，迅速に最適な対策を判断する能力」を定量的に測定可能であると考えられる．

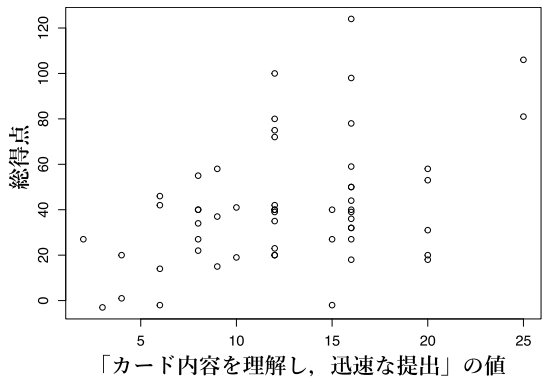

図 6 「カード内容を理解し，迅速な提出」の値と総得点の散布図 ($n = 56$)

Fig. 6 Scatter plot of the values of 'understand card contents and submission promptly' and the total scores.

4.3.3 定性的なアンケート結果の分析

第 1 回目から第 3 回目の演習で，自由記載形式で参加者にアンケートを記載してもらった．本項では，定性的なアンケート結果の分析結果を示す．以下にはアンケートの改善意見とそれを受けて修正した点のみをまとめた．アンケートの分析によりセキュ・ワンを改善し，以降の演習では改善した状態のセキュ・ワンを活用し，演習を実施している．

〈1 回目〉

意見 1：カードの日本語が冗長なものがあった．

改善 1：カードの記載内容を見直し，簡潔な文章に修正した．

意見 2：攻撃カードによるインセンティブがあると良い．

改善 2：防御カードによる有効性を示せなかった場合の減算ポイントを攻撃カードに付与した．

意見 3：防御カードが多すぎる．

改善 3：防御カードの事前配布枚数を制限するルールに修正した．

〈2 回目〉

意見 4：防御カードの有効性判定にブレがあった．

改善 4：判定基準表を作成し，判定が難しい場合にゲームマスタを補助できるようにした．

〈3 回目〉

意見 5：カードの内容が抽象的で具体的な攻撃方法の想像が難しかった．

改善 5：必要に応じ，攻撃カードの抽象度を下げた内容に修正した．

意見 6：知らない用語が含まれている．

改善 6：用語集を作成した．

意見 7：判定基準表の粒度が粗く，納得いかない場合があった．

改善 7：判定基準表において，有効な管理策に CSC の管理策を標記していた部分をサブ管理策まで粒度を細かくし，攻撃カードと防御カードの対応が分かるように修正した．

5. まとめと今後の展望

本稿ではサイバーセキュリティゲーム演習ツールである

セキュ・ワンを開発，評価した．既存のサイバーゲーム演習ツールでは十分な議論が難しいと考えられるインシデント発生前のシステム運用中の対策について，議論ができるように設計した．既存の演習ツールとセキュ・ワンを合わせて使用することで，システム設計時からインシデント発生後の対応まで総合的にゲーム演習で学習できるものと考えられる．すなわち，セキュ・ワンは既存演習ツールの代替ツールではなく，既存演習ツールとともに強固なセキュリティ体制を構築するための助けとなる．

本稿では設計意図の達成度を5段階評価のアンケートを分析することで定量的に評価した．動機付け効果は既存演習ツールと同程度以上の評価となっており，有効性を確認することができた．これは，ゲーミフィケーションの仕組みおよびCSCや攻撃ライブラリのような体系的に整備されたコンテンツを上手く活用できたためと考えられる．すなわち，最新のサイバー攻撃の手法と効果的な対策を楽しみながら学習することが可能であると考えられる．動機付け効果以外の設計方針も他プレイヤおよびゲームマスタとの議論を通して，おおむね達成できた．他プレイヤから単に知識を得るだけではなく，単独学習では困難であったサイバー攻撃手法や対策の解釈の幅を広げることが可能となった．演習後にプレイヤの総得点を確認することで，「サイバー攻撃を理解し，迅速に最適な対策を判断する能力」を測ることができる可能性を示した．セキュ・ワンは単に知識習得のために使用されるものではなく，プレイヤの現状の能力を定量的に把握する場合にも有用であると考えられる．

セキュ・ワンの課題は，ゲームマスタの能力への依存が大きいことが考えられる．この課題の克服には，判定基準表の役割が重要となるため，セキュ・ワンを用いた演習結果の分析を重ねることで判定基準表の精度を改善していく必要がある．

また，攻撃者によりつねに新たなサイバー攻撃手法が開発されていることから最新のサイバー攻撃とそれらへの効果的な防御方法をセキュ・ワンの攻撃・防御カードに反映する必要がある．攻撃カードで用いた攻撃ライブラリ（ATT&CKとCAPEC）は最新のサイバー攻撃手法が発見されると随時データを更新している．攻撃カードは攻撃ライブラリを抽象化した内容となっているため，発見された攻撃手法が既存の攻撃カードで解釈できない場合は新たな攻撃カードを追加する必要がある．防御カードで用いたCSCは現在のサイバー攻撃の傾向と近未来に予測されるサイバー攻撃に対する効果的な管理策となっている．CSCは定期的なバーションアップにより管理策およびサブ管理策が変更されているため，CSCのバージョンアップに合わせて防御カードを更新する必要がある．このため，セキュ・ワンの電子データをGitHubに公開[30]し，攻撃カード更新時はマイナーバージョン更新，防御カード更新時はマスタバージョン更新することで最新のサイバー攻撃手法およびその対策を反映することとした．セキュ・ワンをサイバーゲーム演習で活用したい利用者は更新されたセキュ・ワンをダウンロード，印刷し，使用することができる．

今後の展望としては，セキュ・ワンのアプリ化や単独で学習可能なナレッジベースのツールを開発する．サイバーゲーム演習は複数名のプレイヤの参加が必須である．ゲーム演習と単独学習ツールを組み合わせることにより，効果的なサイバーセキュリティ教育が可能になると考える．

謝辞 セキュ・ワンは平成29年度大学院生向けSecCapおよび産業サイバーセキュリティセンター中核人材育成プログラムの演習において活用および評価していただいた．ここに記して感謝の意を表する．

参考文献

[1] 経済産業省：IT人材の最新動向と将来推計に関する調査報告書，入手先 ⟨http://www.meti.go.jp/press/2016/06/20160610002/20160610002.html⟩（参照 2018-04-18）．
[2] 情報処理推進機構：情報セキュリティ10大脅威2018〜引き続き行われるサイバー攻撃，あなたは守りきれますか？，入手先 ⟨https://www.ipa.go.jp/files/000065376.pdf⟩（参照 2018-04-18）．
[3] SoftBank C&S：調査：「底なし沼」のセキュリティ—兼務現場で求められる効率化，コストとの兼ね合いは？，入手先 ⟨https://japan.zdnet.com/paper/30001014/30002470/⟩（参照 2018-04-18）．
[4] Center for Internet Security: The CIS Critical Security Controls for Effective Cyber Defense Version6.1, available from ⟨https://www.cisecurity.org/⟩ (accessed 2017-08-14).
[5] 山内藍雅，島田英昭：カードゲーム化によるカテゴリー教材の学習，信州大学教育学部研究論集，No.10，pp.91–103 (2017).
[6] 川村ひとみ，岸本桂子，松田俊之，福島紀子：感染対策に関するボードゲームと講義による学習効果の比較に関する検討，YAKUGAKU ZASSHI, Vol.134, No.7, pp.839–849 (2014).
[7] 深田浩嗣：ソーシャルゲームはなぜハマるのか，Softbank Creative (2011).
[8] 杉浦さや，大平茂輝，長尾　確：研究活動へのゲーミフィケーションの導入とその評価，情報処理学会第78回全国大会講演論文集，Vol.2016, No.1, pp.704–704 (2016).
[9] 川西康介，小林尚弥，大平茂輝，長尾　確：ディスカッションマイニングへのゲーミフィケーションの導入，情報処理学会研究報告，Vol.2013-DCC-3, No.9 (2013).
[10] NTT西日本：セキュリティ投資すごろく，入手先 ⟨https://www.ntt-west.co.jp/solution/solution/category/ntt_sugoroku.html⟩（参照 2018-04-20）．
[11] 日本ネットワークセキュリティ協会：セキュリティ専門家　人狼，入手先 ⟨http://www.jnsa.org/edu/secgame/secwerewolf/secwerewolf.html⟩（参照 2018-04-20）．
[12] Federal Emergency Management Agency: Homeland Security Exercise and Evaluation Program, available from ⟨https://preptoolkit.fema.gov/documents/1269813/1269861/HSEEP_Revision_Apr13_Final.pdf⟩ (accessed 2018-04-23).
[13] 内閣官房内閣サイバーセキュリティセンター（NISC）：2017年度「分野横断的演習」について，入手先 ⟨https://www.nisc.go.jp/conference/cs/ciip/dai14/pdf/14shiryou08.pdf⟩（参照 2018-04-20）．
[14] 総務省：実践的サイバー防御演習「CYDER」，入手先

⟨https://cyder.nict.go.jp/⟩（参照 2018-04-20）.
[15] 日本ネットワークセキュリティ協会：SECCON，入手先 ⟨https://2017.seccon.jp/⟩（参照 2018-04-20）.
[16] カスペルスキー：Kaspersky Interactive Protection Simulation，入手先 ⟨http://www.kaspersky.co.jp/about/news/product/2017/pro22022017⟩（参照 2018-04-20）.
[17] トレンドマイクロ：インシデント対応ボードゲーム，入手先 ⟨http://www.trendmicro.co.jp/jp/security-intelligence/learning/index.html⟩（参照 2017-08-14）.
[18] Shostack, A.: *Threat modeling designing for security*, Wiley (2014).
[19] Hutchins, E.M., Cloppert, M.J. and Amin, R.M.: Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, available from ⟨https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf⟩ (accessed 2017-08-21).
[20] 情報処理推進機構：重要インフラのサイバーセキュリティを向上させるためのフレームワーク，入手先 ⟨https://www.ipa.go.jp/security/keihatsu/videos/index.html⟩（参照 2017-08-21）.
[21] Center for Internet Security: The Center for Internet Security Community Attack Model, available from ⟨https://www.cisecurity.org/white-papers/cis-community-attack-model/⟩ (accessed 2017-08-14).
[22] MITRE: Finding Cyber Threats with ATT&CK™-Based Analytics, available from ⟨https://www.mitre.org/sites/default/files/publications/16-3713-finding-cyber-threats with att&ck-based-analytics.pdf⟩ (accessed 2017-08-21).
[23] MITRE: CAPEC™ A Community Resource for Identifying and Understanding Attacks, available from ⟨https://capec.mitre.org/⟩ (accessed 2017-09-19).
[24] Verizon: The Verizon Data Breach Investigations Report, available from ⟨http://www.verizonenterprise.com/DBIR/⟩ (accessed 2017-08-16).
[25] Symantec：2017 年インターネットセキュリティ脅威レポート，入手先 ⟨https://www.symantec.com/ja/jp/security-center/threat-report⟩（参照 2017-08-16）.
[26] enPIT-Security：enPiT-Security【SecCap】分野・地域を越えた実践的情報教育協働ネットワーク（セキュリティ分野），入手先 ⟨https://www.seccap.jp/gs/index.html⟩（参照 2018-04-21）.
[27] 情報処理推進機構：中核人材育成プログラム：IPA 独立行政法人情報処理推進機構，入手先 ⟨https://www.ipa.go.jp/icscoe/program/core_human_resource/index.html⟩（参照 2018-04-21）.
[28] ケラー，J.M.：学習意欲をデザインする，北大路書房 (2010).
[29] 熊本大学大学院社会文化科学研究科：ARCS 動機モデル評価シート，入手先 ⟨http://www2.gsis.kumamoto-u.ac.jp/arcsguidebook/html/about_sheet.html⟩（参照 2017-10-16）.
[30] GitHub: secure-one, available from ⟨https://github.com/nabetan/secure-one⟩ (accessed 2018-07-19).

付　　録

A.1 判定基準表（一部抜粋）

表 A·1 にセキュ・ワンにおいてゲームマスタを補助するために作成した判定基準表の一部抜粋を示す.

表 A·1 判定基準表（一部抜粋）
Table A·1 Reference table for judgement (excerpt).

攻撃カード内容				有効な防御カード番号と解説	
No.	(PT)	タイトル	本文	防御カード番号	解説
1.1	(−1)	初期偵察：発掘	システム情報の解明のため，対象から返答される未処理の例外やエラーメッセージを調査	4.1, 4.4, 4.7, 4.8（防御）	事前に脆弱性スキャンを実施し，未処理の例外の有無を調査し，改善します．
				9, 11.1–11.3（防御）	不要なサービスへのアクセスを制御することで不必要な情報の開示を防止します．
				14.4（防御）	WSDL（Web Services Description Language）ファイルを保護またはWSDL ファイルへのアクセスを制限します．
				18.2（防御）	Web アプリケーションのエラーメッセージの調査を目的と考える攻撃通信を WAF により防御します．
				18.3, 18.5 (防御)	エラー/レスポンス出力を機能的な使用または訂正に必要なものだけの最小限のものにする必要があります．また，アプリケーションの機能に必要でない機密情報を削除，エラーの「コード化」とコードとの紐付けが可能なコードブックによる識別は具体的な対策です．空白の index.html を使用（空の index.html を置くだけでディレクトリのリストがサイト訪問者に表示されない）することも有効です．
				20.1, 20.3–20.6	ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．
1.2	(−1)	初期偵察：傍受	システムにアクセス可能な媒体を介してデータを傍受	1（特定）	ネットワークに接続したスニファ（デバイス）を検出します．このため，デバイスの適正な資産管理を実施し，不正なデバイスを検出する必要があります．
				8.3（防御）	未許可の外部デバイス経由により，情報の収集を防ぎます．
				14.1, 14.3, 14.4, 14.6, 15.7 (防御)	情報の重要度に応じてネットワークを分割しておくことで傍受可能となる情報を制限します．また，定期的にアクセスしないアーカイブデータ等への切り離すことで，リスクを低減できます．
				15.4（防御）	認証機能により，無線ネットワークによる不正利用を防ぎます．
				15.5, 15.6 (防御)	不要な無線アクセス機能を無効化します．
				20.1, 20.3–20.6	ペネトレーションテストは脆弱性によるシステムの影響や組織のセキュリティ能力を測る上で有用です．
1.3	(−1)	初期偵察：フットプリンティング	システムまたはアプリケーションが送信する識別可能な情報を調査	3.1, 3.2, 3.5–3.7（防御）	ファイルとフォルダに対する適切なアクセス許可を設定します．標準的なセキュア設定を確立し，この設定を反映，維持する必要があります．場合によっては，識別可能情報を送信しないように設定します．
				4（防御）	一般的なネットワーク脆弱性スキャンツールはシステム等から送信される識別情報とベースラインを比較し，既知の脆弱性を発見する場合があります．パッチを可能な限り毎週または毎日インストールして最新の状態に保ち，その後の攻撃段階への進行を防ぎます．
				5.3（防御）	ネットワーク機器に強力なパスワードを選択してデフォルトのパスワードを変更することで，ネットワーク機器の識別可能情報とデフォルトパスワードの紐付けを阻止します．その後の攻撃段階への進行を防ぎます．
				6.4–6.6（検知）	ネットワーク境界のログを定期的に調査することで，調査目的と思われる不審なアクセスを発見できる場合があります．
				7.1（防御）	ブラウザが送信する User Agent 等の情報により脆弱なブラウザが狙われる場合があります．最新のブラウザに保つことで，その後の攻撃段階への進行を防ぎます．
				9（防御）	不要なサービス/ポートを無効化し，識別可能な情報を制限します．不要なサービスの悪用のリスクを低減します．また，インターネットから接続できるサービスを制限します．

近江谷 旦

2006 年防衛大学校電気電子工学科卒業．2017 年より奈良先端科学技術大学院大学先端科学技術研究科博士前期課程在籍．

宮本 大輔

2000 年関西学院大学商学部卒業．2002 年奈良先端科学技術大学院大学情報科学研究科修士課程修了．2009 年同博士課程修了．博士（工学）．2011 年東京大学情報基盤センターネットワーク研究部門助教を経て，2017 年奈良先端科学技術大学院大学特任准教授．

門林 雄基 （正会員）

1997 年大阪大学にて博士（工学）．1996 年大阪大学大型計算機センター助手，1999 年同講師．2000 年奈良先端科学技術大学院大学情報科学研究科准教授を経て，2017 年より同大学教授．2008 年より国際電気通信連合（ITU-T）において，サイバーセキュリティ標準化に従事．電子情報通信学会，ACM，IEEE ComSoc 各会員．