情報処理学会論文誌　教育とコンピュータ　Vol.6　No.1　40–51 (Feb. 2020)

論　文

IoT・ポリー：動機づけおよび能力獲得のための IoTセキュリティゲーム演習ツールの提案

近江谷 旦[1,a)]　門林 雄基[1,b)]

受付日 2019年3月23日，再受付日 2019年8月19日，
採録日 2019年11月13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．学習者がセキュリティ教育に関心を持てていないこと，セキュリティ担当者がセキュリティ疲れを抱いていることを受けてセキュリティ人材に必要な能力の獲得と学習者のモチベーションの維持が大きな課題であるといえる．本稿では，上記の課題を克服するため，既存のサイバーセキュリティ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セキュリティゲーム演習ツール，IoT・ポリーを提案する．IoT・ポリーではIoT システムのリスクアセスメントのプロセスを通して，セキュリティ人材に必要な能力の獲得を目指す．IoT・ポリーを用いた演習を 3 回実施し，カークパトリックの 4 段階評価のうち，学習者の反応と学習の効果を評価した．MEEGA+と呼ばれる教育ゲームの評価指標を活用し，IoT・ポリーを含む 4 つの演習ツールで学習者の反応を比較した．IoT・ポリーの結果は ARCS 動機づけモデルの項目において，平均値で比較すれば，他の演習と同等以上の値となったが，有意差は認められなかった．学習の効果はIoT・ポリーでカード化したコンテンツの理解度を質問したアンケート結果と演習で記録したワークシートの分析により評価した．評価の結果，IoT・ポリーは学習者に動機づけを与えつつ，セキュリティ人材に必要な能力を獲得させるうえで有用なツールであることを示した．

キーワード：IoT セキュリティ，ゲーム演習，リスクアセスメント，CAPEC，ENISA

IoT-Poly: An IoT Security Game Practice Tool for Learners Motivation and Skills Acquisition

Tan Omiya[1,a)]　Youki Kadobayashi[1,b)]

Received: March 23, 2019, Revised: August 19, 2019,
Accepted: November 13, 2019

Abstract: The current shortage of cybersecurity personnel is a serious issue that is exacerbated by the increase of damage caused by cyber attacks. The said personnel faces several challenges for acquiring the necessary abilities to perform well due to a lack of learner's motivation in security education and a general security fatigue. In this paper, we propose a cyber game exercise tool, IoT-Poly, which focuses on areas that are hitherto unsupported by the existing cyber game exercises. IoT-Poly aims to help cybersecurity personnel acquire the necessary skills to handle security issues that are related to the Internet of Things (IoT) through risk assessment. We conducted three experiments using IoT-Poly to evaluate the reaction and the learning effect of the learners with the Kirkpatrick's four grades evaluation. We compared the results of learners' reactions of IoT-Poly with three other exercise tools by using the evaluation index of the educational game called MEEGA+. The results of IoT-Poly were rated as equal to or higher than the results of the other exercise tools in the ARCS motivation model but there was no significant difference. We evaluated the effects of learning by analyzing the results of the questionnaires asking the degree of understanding of the content of IoT-Poly, and the worksheets recorded in the exercises. The evaluation results showed that IoT-Poly is a useful tool for cybersecurity personnel to acquire the necessary abilities while keeping their learners' motivation high.

Keywords: IoT security, game exercise, risk assesment, CAPEC, ENISA

1. はじめに

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．フロスト&サリバンの調査 [1] によると世界のセキュリティ人材は 2020 年で 150 万人，2022 年で 180 万人，不足すると推計されている．経済産業省の調査によると日本国内においては 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 [2]．セキュリティ人材の育成が重要となるが，適切に実施されていない問題がある．MOTEX 社の調査 [3] によると調査に回答した組織の約 50%がセキュリティ教育や研修を実施していないと回答している．また，80%以上がセキュリティ教育を改善する必要があると回答している．セキュリティ教育実施時に困っていることとして約 30%の組織が予算がないこと，および，学習者がセキュリティに興味・関心を持ってくれないことをあげている．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 [4]．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．以上から，セキュリティ人材の育成および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．

これまで，我々はセキュリティ人材の不足とセキュリティ担当者のモチベーション低下の課題を克服するためゲーム演習ツールを開発し，その有用性を確認してきた [5]．Capture The Flag（CTF）のような技術面の焦点を当てたゲーム演習は世界中で数多く実施されていること [6] から管理面に焦点を当てたゲーム演習ツールを開発した．本稿では，これまでの管理面に焦点を当てたゲーム演習では未対応領域に対応するゲーム演習ツール，IoT・ポリーを新たに開発した．IoT・ポリーの特徴はリスクアセスメントのプロセスをゲーム化していることと IoT システムに焦点を当てていることである．IoT システムに対するサイバー攻撃の脅威は情報処理推進機構（IPA）が毎年，公表している 10 大脅威 [7] において近年ランクインしている．また，米国国土安全保障省が作成した「IoT の安全性確保のための戦略的原則」[8] において，「確立されたセキュリティ対策の採用」や「想定される影響に応じて対策を優先付け」といったリスクアセスメントに関連する項目が原則としてあげられている．IoT システムは IT システムと比べて，システムごとに特徴が大きく異なっており，IoT システムごとの考慮すべき脅威や脅威への対策方法もその特徴を考慮し，変える必要がある．さらに，IPA は IoT システムや制御システムに対するリスクアセスメントに関連する資料を作成・公開している [9], [10]．上記の現状をふまえ，IoT・ポリーではリスクアセスメントのプロセスをゲーム演習内で体験するとともに，IoT システムへの脅威や適切な対策手法を学習できるようにしている．

本稿の以降の構成は下記のとおりである．2 章で関連研究と IoT・ポリーの新規性について示す．3 章および 4 章では，IoT・ポリーに教授設計（ID）[11] の改善サイクルである ADDIE モデル [12] を適用し，それぞれのプロセスの内容を詳述する．5 章で本稿のまとめとする．

2. 関連研究と IoT・ポリーの新規性

本章では，関連研究として本稿で活用した ID のモデルの概要とサイバーセキュリティゲーム演習のうち管理面に焦点を当てたゲーム演習について示した後，提案ツールである IoT・ポリーの新規性について示す．

2.1 教授設計：Instructional Design（ID）

インストラクションとは目的を持って学習を促進するために実施するすべてのことと定義される．インストラクションのアプローチは各種存在するが，本稿では「教育とゲーム」のアプローチに着目している．教育とゲームとは，インストラクションの対象として定めた知識，スキル，能力をその目的のために考案されたゲームを通して習得させる教授方法と定義される．ID とは効果的かつ効率的に特定のインストラクション（知識や技能など）を習得させるための方法論である．本稿で参考にした ID のモデルは以下のとおりである．

- ADDIE モデル：ADDIE モデルは ID のプロセスをモデル化したもので ID の改善サイクルに該当する．Analysis（分析），Design（設計），Develop（開発），Implement（実施），Evaluate（評価）のサイクルを実施後，各項目を改善させることで演習をより良くしていくものである．本稿では ADDIE モデルの改善サイクルを繰り返すことで演習の改善を実施した．
- カークパトリックの 4 段階評価モデル：カークパトリックの 4 段階評価モデルは研修評価のモデルとして知られている [13]．このモデルでは研修効果をレベル 1 からレベル 4 の 4 段階（Reactions：反応，Learning：学習，Behavior：行動，Results：結果）に分けて測定するものである．本稿ではカークパトリックの 4 段階評価モデルのうち，レベル 1（反応），レベル 2（学習）に焦点を当て評価を行った．
- ARCS 動機づけモデル：ARCS 動機づけモデル [14] はケラーによって提案された学習者の動機づけ効果を高めるための方法である．ケラーは高い学習意欲を引き出し，継続的に学ばせるためのアプローチを研究した

[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) youki-k@is.naist.jp

表 1　演習の分類
Table 1　A classfication 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・仮想状況下での手順などを体験
	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，手順などに精通

結果，ARCS に該当する 4 つの分類項目（Attention（注意），Relevance（関連性），Confidence（自信），Satisfaction（満足））で学習意欲が飛躍的に高まることを実証した．本稿では反応に該当する演習の評価に ARCS 動機づけモデルを活用した．

2.2　サイバーセキュリティゲーム演習

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）」[15] 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** にように定義している．本稿では，ゲーム演習に焦点を当てて，IoT・ポリーの開発を実施した．

サイバーセキュリティの分野においても HSEEP を適用した演習が実施されている．このうち，管理面に焦点を当てたゲーム演習に該当するツールを下記に示す．

- Elevation of Privilege（EoP）[16]：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などにおける脅威を洗い出すための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．
- セキュ・ワン [5]：我々が作成・公開したサイバーキルチェーンの攻撃段階ごとのサイバー攻撃手法と主にシステム運用中の対策との関連を議論を通じて確認・学習するための演習ツールである．攻撃カードに対応可能なシステム運用時の対策が記載された防御カードを迅速に提出し，有効性を他プレイヤに口頭で説明することで議論を誘発する．議論を通して，サイバー攻撃手法とその対策の理解を深めることができる．
- インシデント対応ボードゲーム [17]：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プロセスを体感できる演習ツールである．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などについて話し合い，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．

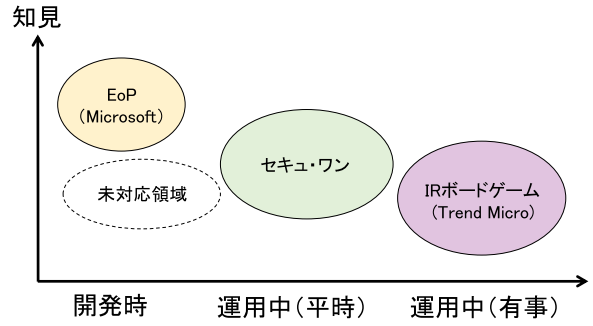


図 1　既存ゲーム演習の適用領域
Fig. 1　Scope of existing game exercises.

2.3　IoT・ポリーの新規性

図 1 に既存のゲーム演習ツールの適用範囲を示す．図の横軸はシステム開発からインシデント発生までの時間軸を表している．縦軸は参加者に必要な知見のレベルを表している．単一のゲーム演習ツールでは広範囲な領域を網羅することが困難であり，未対応領域を埋めるゲーム演習ツールを新たに開発することが重要がある．複数の演習ツールを組み合わせて活用することで様々な領域における必要な知識やプロセスを網羅的に学習することができる．本稿では図の破線に示した未対応領域を埋めるために IoT・ポリーを開発した．IoT・ポリーの時間軸（横軸）は既存研究で示した EoP の領域を包含している．EoP はリスクアセスメントの脅威の洗い出しプロセスをゲーム化した内容となっている．EoP のカード内容は STRIDE [16] に基づく抽象的な内容になっており，高度な知見を有する参加者がいた場合，システムに存在する新たな脅威を発見できる可能性がある．一方で高度な知見を有していない参加者がカードの記載事項から想定される脅威を連想することが困難な場合がある．また，EoP では脅威の洗い出しまでは実施可能であるが，低減策を検討するプロセスまではゲーム内で実施することができない．IoT・ポリーでは EoP よりも比較的容易に脅威の洗い出しができるようにカードの記載内容を具体化している．また，脅威の洗い出し以降のプロセスも体験できるような内容となっている．

セキュ・ワンは IT システム運用中の脅威と対策を理解するために開発されているが，カードの内容を開発時の対策に変更することで，未対応領域を埋められる可能性がある．しかし，セキュ・ワンで使用するカードは脅威カードと対策カードの 2 種類のみであり，脅威に対応する対策を検討することしかできない．特に IoT システムは IT システムとは異なり，システムの特性は防護対象により大きく異なる．このため，IoT・ポリーでは脅威カードと対策カードに，IoT カードとアタックサーフェスカードを加えて 4 種類のカードセットとすることで，IoT システムの特性を

考慮し，そのIoTシステムに対する重大な脅威や効果的な対策について，リスクアセスメントプロセスのなかで学習できるようにしている．我々は，セキュ・ワンでは学習することができなかったリスクアセスメントの他プロセスも学習できるようにすること，および，ITシステムとはまったく異なる特性を持つ様々なIoTシステムへのリスクアセスメントを実施できるようにIoT・ポリーを開発した．また，セキュ・ワンで作成したカードセットを使用することで，学習者が管理または利用するITシステムへのリスクアセスメントもできるようになっている．

3. 提案するゲーム演習について

演習開発にあたってはADDIEモデル [12] を活用した．本章ではADDIEモデルの分析から開発までの内容をまとめた．

3.1 分析：リスクアセスメントの概要

IoT・ポリーではリスクアセスメントの3つのプロセス（リスク特定，リスク分析，リスク評価）をゲーム化する．

リスク特定ではシステムに対するリスクを洗い出し，記述する．IoTシステムはその特性によりリスクの内容が変化する．IoT・ポリーでは様々なIoTシステムでリスク特定プロセスを体験できるようにする．

リスク分析では特定したリスクをリスク値として定量化し，低減策を講じることで許容値まで値を低減させる．特にIoTシステムにおいてはその特徴に応じてリスク値の算定過程における要素やその比重が変わるため，システムに対応したリスク値の算定手法を作成する必要がある．IoT・ポリーでは特定のリスク値算定手法への固執を避けるため，リスク値算定を実施せず，IoTシステムの特徴や脅威の影響度を議論できるような仕組みとすることでリスク分析の過程を体験できるようにする．

リスク評価では，想定されるリスクから低減策を講じたとしても残留するリスクを明らかにし，残留リスクの許容の可否を判定する．残留リスクはリスク分析の結果からリスク値が基準値以下であれば許容されるが，IoT・ポリーでは特定の算定手法を用いず，参加者間の議論により判断する．

リスクアセスメントのプロセスを通じて**表2**に示す能力の獲得が期待できる．この表の「獲得を目指す能力」は日本ネットワークセキュリティ協会（JNSA）が公開したセキュリティ知識分野（SecBoK）人材スキルマップ [18] を参照した．

3.2 設計：リスクアセスメントプロセスの簡易化

リスクアセスメントのプロセスをモデル化したものは各種存在する．リスク合理化プロセス [19] は特定分野のリスクアセスメントに焦点を当てたものではなく，汎用的に活用できるモデルである．ICSリスクアセスメントのモデル [20] はOTシステムのうち産業制御システムに焦点を当てたリスクアセスメントのモデルである．IoT・ポリーにおけるリスクアセスメントのモデルでは汎用性があるモデルと特定のOTのモデルを参照し，様々なIoTシステムでより平易にプロセスを進捗できるように簡単化した．また，IoTシステムのアタックサーフェスごとに焦点を絞って，リスクアセスメントを実施できるようにしている．演習ではカードを使用し，配布されたカードの範囲内でリスクアセスメントを実施することができる．参加者の思考は手持ちのカードの範囲内に制限されるため，専門家以外であっても容易に演習に参加することができる．実際のリスクアセスメントのプロセスを簡易化していることに加え，カードを用い，参加者の焦点を絞ることで，仮想的な環境下において短時間でリスクアセスメントプロセスを体験できるようになっている．さらに，参加者は議論を通して他参加者の知見など，新たな気づきを得ることができるようにもなっている．以下に平易化した3つのプロセスを示す．

表2　IoT・ポリーで獲得を目指す能力
Table 2　Ability acquired using IoT-Poly.

区分	獲得を目指す能力
知識	利用者が学習すべき知識
	リスク管理のため情報保証の原理
	リスク評価手順・手法を含むリスク管理
	リスク受容・リスク管理のアプローチ
	リスク脅威の評価
	サイバー攻撃の脅威と対策
スキル	コミュニケーションスキル
	セキュリティ管理策を識別
	脆弱性の種類と関連攻撃の認知・分類
	特定したセキュリティリスクの対策の設計

3.2.1 状況付与

IoTシステムの特徴をカードとシステム構成図で表現し，脅威カードとプレイヤ間の議論により，そのIoTシステムのリスクを導出する．アタックサーフェス（IoTシステムの構成要素）ごとの議論に焦点を絞るため，プレイヤにアタックサーフェスカードを選択させる．

3.2.2 リスクシナリオ作成

状況付与を受けて，IoTシステムのアタックサーフェスへの脅威を順位付けする．議論の焦点を絞り，プレイヤの選択肢を制限するため，事前にプレイヤに配布する脅威カードの枚数を制限する．プレイヤは配布された脅威カードの中から最もリスクが大きいと考えられるカードを選択し，提示する．それぞれのプレイヤが提示した脅威カードを議論を通してリスクの大きさ順に順位付けする．議論により最もリスクが大きいと判定された脅威カードを用いて想定される攻撃をリスクシナリオの形で文書化する．

3.2.3　残存リスクの評価

プレイヤ間の議論により表現されたリスクシナリオを受けて対策を検討する．事前に枚数を制限した対策カードをプレイヤに配布することで，プレイヤの検討する思考の範囲を制限する．プレイヤは配布された対策カードから最も効果的な対策カードを選択し，提示する．議論により各プレイヤが提示した対策カードの効果順に順位付けする．また，プレイヤ間の議論により提示された全防御カードにより防ぐことができない残留リスクの有無と追加の対策を議論する．

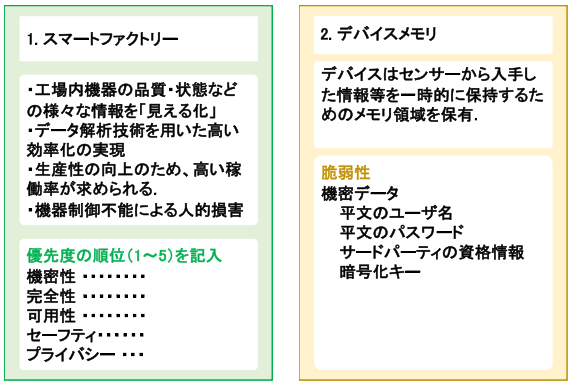
3.3　開発：演習ルールと演習資材

設計のプロセスを実現するため，演習ルールと演習資材（カード，ワークシート，脅威の詳細リスト）を開発した．以下のそれぞれの細部を示す．

3.3.1　カード

ゲームではIoTカード，アタックサーフェスカード，脅威カード，対策カードを開発した．以下にそれぞれのカードの概要を示す．

- IoTカード：様々な特性を持つIoTシステムへのリスクアセスメントを演習できるようにIoTシステムをカードとシステム構成図で表現した．また，リスクアセスメント時に参加者へ共通の評価軸を提供するため，IoTシステムの特性に優先順位付けができるようにした．
- アタックサーフェスカード：IoTの代表的なアタックサーフェスをまとめた．ここではOWASP IoT Projectによって定義された代表的な18個のアタックサーフェス[21]をカード化した．OWASP IoT ProjectではIoTの脆弱性Top10を定義しているとともに，アタックサーフェスごとの対応する脆弱性を紐付けしている．プレイヤはIoTカードとシステム構成図からアタックサーフェスに該当する要素を発見し，アタックサーフェスの脆弱性から脅威を連想する．
- 脅威カード：脅威カードはMITRE社が作成・公開しているサイバー攻撃の辞書にあたる攻撃ライブラリの一種であるCAPEC[22]を活用した．CAPECは攻撃手法の抽象度に応じて，メタ抽象化，標準抽象化，詳細抽象化に分類される．カード枚数を制限することおよび参加者間の議論の中で攻撃手法を具体化させることを狙いとしてカード化する内容はメタ抽象化の分類に該当する項目をまとめた．これにより，61枚のカードを作成した．
- 対策カード：対策カードにはENISAのBaseline Security Recommendations for IoT[23]のGood Practiceを活用した．IoTシステムのセキュリティ対策はIoTシステムの特徴に応じて，様々な標準が作成されているが，Baseline Security Recommendations for IoTはIoTシステムのセキュリティ対策を包括的にまとめた項目となっている．このため，IoTシステムのセキュリティ対策を適用する際はこの包括的なリストの中から適当な対策を選ぶ必要がある．IoT・ポリーでは様々なIoTシステムにおけるリスクアセスメントのプロセスの過程を演習するため，Baseline Security Recommendations for IoTの対策をまとめることとした．Baseline Security Recommendations for IoTの対策はさらに方針，組織・担当者・プロセス，技術の3つに分類される．このうち，方針の内容は包括的な脅威の対策に該当する内容が多かったため，組織・担当者・プロセスと技術に該当する71個の対策をカード化することとした．



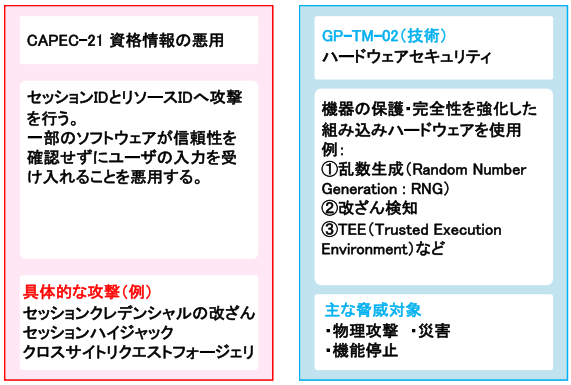
(a) IoTカード　　(b) サーフェスカード

図2　IoTカードとアタックサーフェスカード

Fig. 2　Examples of an IoT card and an attack-surface card.

図2に完成したカードの例としてIoTカードとアタックサーフェスカードを示す．IoTカードは名称，概要，優先順位（機密性，完全性，可用性，セーフティ，プライバシー）の3つの項目を記載した．優先順位はプレイヤ間の議論の中で決定し，プレイヤが記載する．アタックサーフェスカードはアタックサーフェス名，概要，アタックサーフェスが含む脆弱性を記載した．プレイヤは脆弱性の内容から脅威を連想することができる．

図3に完成したカードの例として脅威カードと対策カードを示す．脅威カードはCAPECメタ抽象化に該当する手法とその概要および具体的な攻撃例を記載した．具体的な攻撃手法にはCAPEC標準化に該当する攻撃手法の名称を記載した．脅威カードとは別に具体的な攻撃手法のリストをまとめた表を作成し，必要に応じ，プレイヤが閲覧できるようにした．これにより，脅威カードを補完し，カードの情報だけで具体的な攻撃手法の連想が困難なプレイヤを補助できるようにした．対策カードは対策名とその概要および主な脅威対象を記載した．主な脅威対象を記載することで，プレイヤがリスクシナリオに対応する対策カードを提示する際にヒントとすることができる．



(a) 脅威カード　　(b) 対策カード

図 3　脅威カードと対策カード

Fig. 3　Examples of a threat card and a countermeasure card.

3.3.2　ワークシート

ゲームの進行を通して議論した内容を記録し，プレイヤにフィードバックができるようにワークシートを作成した．ワークシートの内容を他グループに発表し，意見交換するなどの方法でさらに理解を深めることもできる．ワークシートで記録する項目と内容は下記のとおり．

- IoT カードと優先順位：IoT カードと IoT システムの特徴をふまえ議論により導出した特性の優先順位を記載する．
- アタックサーフェスカード：任意のプレイヤが選択したアタックサーフェスカードの番号を記載する．
- 脅威カード：プレイヤが提出した脅威カードを深刻度と提出者が分かるように記載する．
- リスクシナリオ：最も深刻度が高いと識別された脅威カードを使用し，リスクシナリオを文章として書き出す．
- 対策カード：プレイヤが提出した対策カードを効果の順位と提出者が分かるように記載する．
- 残留リスク許容可否：対策カードでは防ぎきれない残留リスクと許容の可否を記録する．
- 追加の対策：残留リスクが許容できない場合の追加の対策を記録する．

3.3.3　脅威の詳細リスト

IoT・ポリーでは CAPEC を用いて IoT システムの脅威を思考する．脅威カードの内容は CAPEC メタ抽象化の内容をまとめているが，カードだけでは具体的な攻撃手法の連想が難しいプレイヤも存在すると考えられる．このため，メタ抽象化よりも具体的な内容が記載され，一般的に使われている攻撃手法名を多く含む標準抽象化の内容を参照できるように詳細リストを作成した．詳細リストはメタ抽象化の内容と標準抽象化の内容の親子関係が分かるように作成した．プレイヤは脅威カードの内容から具体的な脅威を連想できない場合，詳細リストにより具体的な攻撃手法を確認することができる．

3.3.4　演習ルール

IoT・ポリーは IoT システムのリスクアセスメントプロセスを抽象化したものであり，仮想的な状況下でリスクアセスメントを体験できるようにゲームルールを開発した．カードと参加者間の議論だけで，リスクアセスメントプロセスを実際よりも短時間で体験することができるようにした．また，参加者間の協調作業により，ゲームを進行させるため，参加者個人を評価する競争の仕組みを排除したルールとしている．協調作業により，導出した結果は，演習後の専門家による解説や今後，作成予定の解説書などを用い評価することができる．以下に演習のルールを示す．

(1) プレイヤに脅威カードと対策カードを 10 枚ずつ配布する．カードの枚数を制限することでプレイヤの思考範囲を制限し，適切な意思決定ができるようにしている．枚数を 10 枚にしたのは，ゲームのプレイヤ数は最大で 6 人を想定しているため，配布するカードに不足が発生しないようにするためである．ゲームの状況によっては配布枚数を 10 枚以下にし，思考の範囲をさらに制限することもできる．

(2) 任意のプレイヤが IoT カードを引き，提示する（または，プレイヤ間で相談し，任意の IoT カードを選択する）．

(3) IoT カードとシステム構成図を使用し，プレイヤ間の議論により以降の議論で焦点となる特性（機密性，完全性，可用性，セーフティ，プライバシ）の優先順位を決定する．

(4) 任意のプレイヤがアタックサーフェスカードセットから 1 枚のカードを引き，提示する．

(5) プレイヤは，提示されたアタックサーフェスカードと IoT カード，システム構成図から決定した特性の優先順位を考慮し想定される最も深刻な脅威を手持ちの脅威カードから 1 枚選択し，提出する．手持ちの脅威カードから選択できない場合，脅威カードセットから最大で 5 枚のカードを追加で引くことができるが，必ずしも脅威カードを提出する必要はない．追加で引けるカード数を制限しているのは，脅威の思考に制限をかけるためである．

(6) プレイヤ間の議論により，提出されたカードを脅威の深刻度順に順位付けする．順位付けの過程で議論を生じさせ，脅威への深い洞察と理解を与えることを狙いとしている．

(7) 最も深刻な脅威に選ばれた脅威カードから想定されるリスクシナリオをワークシートに記載する．グループ内でシナリオを作成することで，より具体的で実現可能な脅威を理解させる．

(8) プレイヤは記載された 1 つのリスクシナリオから，最も効果的であると考えられる対策を手持ちの対策カードから提出する．手持ちの対策カードから選択できな

表 3　演習の概要
Table 3　Summary of the exercise.

第 1 回目：H30.9.15（金），SecCap 受講生 16 名		
順番	ツール名	演習時間（分）
1	ツール X	90
2	ツール Y	90
3	セキュ・ワン	90
4	IoT・ポリー	90
第 2 回目：H30.10.22（火），ICS-CoE 受講生 5 名		
順番	ツール名	演習時間（分）
1	ツール X	90
2	ツール Y	90
3	セキュ・ワン	90
4	IoT・ポリー	90
第 3 回目：H30.12.11（火），ICS-CoE 受講生 6 名，留学生 6 名		
順番	ツール名	演習時間（分）
1	セキュ・ワン	90
2	IoT・ポリー	90

い場合，対策カードセットから最大で 5 枚のカードを追加で引くことができる．追加で引けるカード数を制限しているのは，対策の思考に制限をかけるためである．

(9) プレイヤ間の議論により，提出されたカードを対策の効果順に順位付けする．順位付けの過程で議論を生じさせ，対策への深い洞察と理解を与えることを狙いとしている．

(10) プレイヤは提出したカードから残留リスクを議論する．最悪リスクシナリオにおいて提出された対策カードによる残留リスクの許容可否をワークシートに記載する．残留リスクを許容できない場合は追加の対策についてさらに議論し，ワークシートに記載する．

(11) (3)〜(10) を異なるアタックサーフェスカードで任意の回数，繰り返す．

(12) 以上でゲームは終了となるが別の IoT カードを使って，(1)〜(11) を再度繰り返し，ゲームを継続することもできる．

4. 演習の実施と評価

本章では ADDIE モデルの実施，評価と評価結果を受けて改善した内容について示す．

4.1 実施：演習の概要

IoT・ポリーの有用性を確認するため，**表 3** に示す 3 回の演習を実施した．演習は SecCap [24] および ICS-CoE 中核人材育成プログラム [25] 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 IPA 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，IoT・ポリーを含むサイバーセキュリティゲーム演習の対象としては適正である．第 2 回目演習は人数が少なかったこと，および，演習中に参加者の入れ替わりが発生したため，定性的な分析のみを実施した．第 3 回目演習ではコンテンツを英語化したものを評価するため，留学生と社会人（日本人）を混合させたグループにより演習を実施した．留学生は奈良先端科学技術大学院大学のサイバーセキュリティ関連の研究室に所属する学生とした．

4.2 評価方法

演習の評価はカークパトリックの 4 段階評価法のうち，レベル 1（反応）とレベル 2（学習）のみに着目した．レベル 3（行動）とレベル 4（業績）については長期的な研修と確認が必要となるため，本演習評価で対象としていない．以下に反応と学習の評価方法について示す．

4.2.1 評価方法：レベル 1（反応）

演習直後のアンケートにより，参加者の反応を調査した．アンケート調査に用いる代表的な教育ゲームの評価指標には MEEGA+ [26]，EGameFlow [27]，RETAIN [28] がある．このうち，アナログ教育ゲームに適用可能で多くの活用事例があることから MEEGA+を用いることにした．MEEGA+は主にソフトウェア開発のための教育ツールの評価指標として活用された実績がある．プロジェクトマネジメントの分野における管理事項を学習するツールを評価する際にも活用されており，サイバーセキュリティゲーム演習においても活用できるものと考察した．**表 4** に MEEGA+のアンケート内容を示す．MEEGA+はアンケートにより，学習者の反応を 5 段階で評価することができる．13 個の項目に分類（注意，面白さ，挑戦，相互作用，自信，関連性，満足，美的感覚，学習可能性，実施可能性，可用性，短時間学習効果，学習目標の達成度）された全 33 問の質問から構成される．ARCS 動機づけモデルの注意，関連性，自信，満足を包含する内容となっていることから動機づけ効果も確認することができる．演習では MEEGA+を用いて IoT・ポリーを含む 4 つのセキュリティゲーム演習ツールの結果を比較した．

4.2.2 評価方法：レベル 2（学習）

学習者の学習到達度を確認するため，参加者にカード化したコンテンツの理解度を問うアンケートを 5 段階評価で回答してもらった．また，演習後に記載されたワークシートを確認することで議論で導出した結果の分析を行った．

表 4　MEEGA+のアンケート内容
Table 4　Contents of questionnaire in MEEGA+.

No.	分類	アンケート内容
1	注意	ゲームの始めに注意を引く面白いことがあった.
2		時間を忘れるくらいゲームのタスクに没頭した.
3		ゲームを実施している間，周囲を気にならなかった.
4	面白さ	このゲーム演習は面白かった.
5		ゲーム中に発生したことが（ゲーム要素，競技など）が楽しかった.
6	挑戦	自分にとって適切なレベルの課題であった.
7		ゲームは適切なペースで新しい課題（障害，状況，バリエーション）を提供していた.
8		ゲームの進行で単調（退屈な作業）になることはなかった.
9	相互作用	ゲーム中に他のプレイヤと対話することができた.
10		ゲームはプレイヤ間の協力または競争を促した.
11		ゲーム中に他プレイヤとのやりとりがうまくできている感じがした.
12	自信	最初にゲームを見たとき，簡単そうなに感じた.
13		ゲームで内容や構造を学ぶことで自信を持てた.
14	関連性	ゲームの内容はあなたの興味に関係していた.
15		ゲームの内容がどのくらい学習すべき内容に関連しているのかは明白だった.
16		このゲームは学習すべき内容における適切な教授方法だった.
17		他の方法で学習するよりもこのゲームで学習する方を好みだった.
18	満足	ゲームのタスクが終わると満足のいく達成感が得られた.
19		自分の努力により，ゲーム内で成長することができた.
20		ゲームから学んだことに満足している.
21		同僚や友人にこのゲームをお勧めするだろう.
22	美的感覚	ゲームデザインは魅力的だった（インタフェース，グラフィックス，ボード，カードなど）
23		テキストのフォントと色はゲームに溶け込んでおり，一貫性があった.
24	学習可能性	ゲームを実施する前にいくつかのことを学ぶ必要があった.
25		このゲームを使って学習することは簡単だった.
26		すぐに多くの人がこのゲームを使って学ぶことになると思う.
27	実施可能性	このゲームは簡単に実施できたと思う.
28		ゲームのルールは明確で分かりやすかった.
29	可用性	ゲームで使用されるフォント（サイズとスタイル）は読みやすかった.
30		ゲームで使用される色は意味があったと感じた.
31	短時間学習	このゲームはあなたの学びに貢献した.
32		このゲームを使うことで他の学習方法と比較して効率的な学習ができたと思う.
33	学習目標	ゲームは学習目標（各演習ツールに該当する内容を記述）の達成に貢献した.

4.3　評価結果：レベル 1（反応）

本節では評価結果のうち，学習者の反応の結果を示す．**表 5** に MEEGA+のアンケート結果を示す．5 段階評価による平均（Avg.）と標準偏差（SV）をまとめた．第 1 回目演習では IoT・ポリーを含む 4 つの演習ツールを用いて結果を比較した．第 3 回目演習では IoT・ポリーとセキュ・ワンの結果を比較した．

本稿ではセキュリティ教育におけるモチベーションを維持・向上させることが目的であるため，アンケート結果のうち，動機づけ効果（ARCS 動機づけモデル）に該当する分類に着目する．**図 4** に第 1 回目演習の動機づけ効果の分類別平均値の結果を示す．平均値で比較すればセキュ・ワンが総じて高い値になっているが，有意差は認められなかった．セキュ・ワンはゲーミフィケーションの仕組みを用いて作成された演習ツールで，他ツールに比べてゲーム性が高い内容となっているためと考えられる．一方で IoT・ポリーは平均値で比較すれば，セキュ・ワン以外の既存演習ツールに比べて，高い値になっているが，有意差は認められなかった．セキュ・ワン以外の既存演習ツールは IoT・ポリーと同様に特定のセキュリティ活動のプロセスをゲーム化した内容となっている．**図 5** に第 3 回目演習の動機づけ効果の項目別平均値の結果を示す．平均値で比較すれば，セキュ・ワンと同程度の値になっているが，有意差は認められなかった．第 1 回および第 2 回演習をふまえ，ルールの一部を修正し，ゲームサイクルが改善できたことが要因と考えられる．日本語版コンテンツで実施した第 1 回目演習の結果と比べても同程度の結果となっていることからコンテンツを英語化したツールの有効性を確認することができた．

以下に動機づけ効果以外の分類における結果の考察をま

表 5　MEEGA+のアンケート結果
Table 5　Results of questionnaire in MEEGA+.

No.	分類	第 1 回目演習								第 3 回目演習			
		IoT・ポリー		セキュ・ワン		ツール X		ツール Y		IoT・ポリー		セキュ・ワン	
		Avg.	SD	Avg.	SD	Avg.	SD	Avg.	SD	Avg.	SD	Avg.	SD
1	注意	3.44	1.00	3.69	0.92	3.25	0.97	2.69	0.85	4.17	0.55	4.08	0.86
2		3.81	0.95	4.25	0.83	3.88	0.86	3.63	1.17	4.25	0.92	4.33	0.85
3		3.81	1.01	4.06	0.75	3.88	1.05	3.63	1.17	4.17	0.90	3.58	0.76
4	面白さ	4.06	0.83	4.38	0.78	4.13	0.86	3.56	1.12	4.33	1.03	4.75	0.43
5		3.38	1.05	4.25	0.75	3.50	0.79	3.25	1.15	4.08	0.76	4.42	0.64
6	挑戦	3.56	0.93	3.81	1.01	3.56	0.93	2.69	1.16	3.92	0.64	3.83	0.80
7		3.44	1.00	4.19	0.63	3.50	1.12	3.56	0.61	4.25	0.83	4.17	0.69
8		3.44	1.00	3.88	0.86	4.06	0.83	3.13	0.99	4.17	1.07	4.17	0.90
9	相互作用	4.69	0.58	4.81	0.39	4.75	0.43	4.50	0.61	4.75	0.43	4.92	0.28
10		4.19	1.01	4.69	0.46	4.06	1.03	4.00	0.94	4.75	0.60	4.42	0.76
11		4.19	0.73	4.13	0.78	3.88	0.86	3.31	1.16	4.5	0.76	4.50	0.5
12	自信	2.81	0.88	2.56	0.93	2.44	0.93	1.56	0.61	2.83	1.07	2.92	0.86
13		3.44	0.93	3.63	0.99	2.81	0.95	2.63	0.99	3.75	0.92	3.92	0.86
14	関連性	4.00	0.87	3.81	0.81	3.44	0.79	3.38	0.99	4.33	0.94	4.00	1.08
15		3.63	0.78	3.31	0.92	3.44	1.06	3.56	0.61	4.33	0.75	4.33	0.75
16		3.63	0.86	3.81	0.92	3.56	0.70	3.31	0.85	4.58	0.49	4.50	0.50
17		3.50	0.87	3.94	0.90	3.31	1.10	2.75	1.09	4.42	0.64	3.92	0.76
18	満足	3.56	0.86	3.81	0.88	3.38	1.22	3.06	1.20	4.17	0.80	4.25	0.72
19		3.56	0.79	3.69	0.77	3.38	0.86	2.94	1.09	3.83	0.90	4.00	0.71
20		3.69	0.77	3.75	0.75	3.56	0.79	3.38	0.86	4.33	0.94	4.25	0.60
21		3.31	1.10	3.44	1.00	3.44	0.79	2.56	1.06	4.08	1.11	4.33	0.75
22	美的感覚	3.63	0.99	3.31	1.04	3.69	1.04	2.88	1.22	4.00	1.00	3.75	0.92
23		3.69	0.98	3.06	0.97	4.00	0.79	3.06	0.97	3.83	1.14	3.83	0.99
24	学習可能性	3.69	0.85	4.06	0.75	4.06	0.83	4.44	0.70	3.75	0.83	3.33	1.18
25		3.13	1.17	3.13	0.99	3.25	1.25	2.19	1.07	3.25	1.09	3.50	0.87
26		3.25	1.03	2.81	0.88	2.69	0.77	2.19	1.01	3.33	1.03	3.83	1.07
27	実施可能性	3.69	1.16	3.31	1.31	3.19	1.33	1.88	0.99	3.42	1.11	3.33	0.85
28		3.69	1.04	3.25	1.31	3.06	1.30	2.00	1.22	3.92	0.86	3.83	1.21
29	可用性	3.94	1.14	3.75	1.20	4.25	1.09	3.25	1.20	3.00	1.29	3.00	1.41
30		3.50	1.22	2.94	1.20	3.63	1.11	3.13	1.36	4.08	0.86	3.33	1.11
31	短時間学習	3.81	0.73	4.00	0.71	3.81	0.81	3.63	0.70	4.33	0.75	4.25	0.60
32		3.75	0.75	3.88	0.86	3.44	0.93	3.00	1.00	4.42	0.49	3.92	0.76
33	学習目標	4.00	0.61	3.56	0.70	3.44	0.79	3.75	0.66	4.17	0.69	4.08	0.64

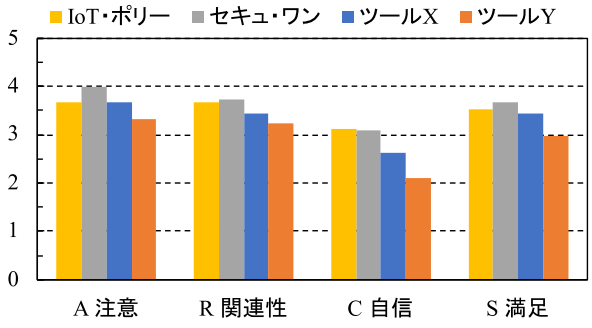


図 4　動機づけ効果の結果（第 1 回目演習）
Fig. 4　Results of motivation in 1st exercise.

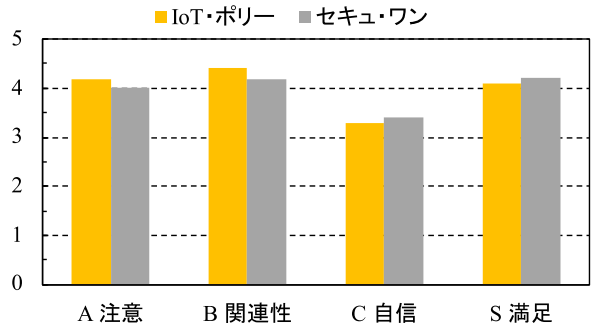


図 5　動機づけ効果の結果（第 3 回目演習）
Fig. 5　Results of motivation in 3rd exercise.

とめた．美的感覚および可用性の評価はツール X は比較的高い値になっている．これは企業により作成・公開されたツールであるため，デザインや文字フォントなどの可読性が高かったためと考えられる．同様にツール Y も企業によって作成・公開されたものであるが，英語の内容を日本語化し活用したため，文字フォント・サイズなどのバラン

表 6　学習コンテンツの理解度
Table 6　Understanding of learning content.

	第 1 回目演習		第 3 回目演習	
カードの種類	Avg.	SD	Avg.	SD
IoT カード	4.00	0.61	4.00	1.00
アタックサーフェスカード	3.69	1.04	4.08	0.86
脅威カード	3.63	1.11	4.33	0.47
対策カード	3.56	1.12	4.50	0.50

スが悪化してしまった可能性がある．IoT・ポリーはツール X を参考にし，デザインなどを改善する必要があると考えられる．短時間学習や学習目標については，IoT・ポリーの評価は比較的高い値となっており，良好な反応を得ることができた．リスクアセスメントのプロセスの中で，体系化された各種コンテンツの内容を学習することができたため，効果的な学習に貢献できたものと考えられる．平均値で比較すれば，総じて，IoT・ポリーは他演習ツールと比べても同程度以上の値になっているが有意差は認められなかった．

4.4　評価結果：レベル 2（学習）

本節では評価結果のうち，学習の結果を示す．**表 6** に学習コンテンツの理解度を示す．それぞれのカードコンテンツの理解度を 5 段階評価で回答していただいた．平均値で比較すれば，第 3 回目演習は第 1 回演習に比べて総じて高い値になっているが，有意差は認められなかった．これは，演習参加者に社会人が含まれており，参加者の知識レベルが第 1 回目に比べて高かったためと考えられる．別に調査した定性的な分析結果から，議論により他参加者からカード内の知識を補足できたと回答する参加者が多く，第 1 回目においてもカードと議論を組み合わせることで参加者は十分な知識を得ることができたものと考えられる．

次に参加者が記載したワークシートを確認し，議論の適正性について確認した．脅威カードで活用した CAPEC はサイト内に攻撃手法における低減策が明記されており，サイト内の記載内容と参加者が提出したカードの内容を突合することでおおむねの議論の妥当性を判断できるものと考察した．ただし，CAPEC のなかには低減策が記載されていないものも多くあるため，文献調査などにより示された一般的な対策から議論の妥当性を判断した．以下にワークシートの妥当性確認の結果の概要をまとめた．

4.4.1　ワークシートの分析（第 1 回目演習）

第 1 回目演習のうち，記載されたワークシートの結果を 1 つ例示する．

- IoT カード：スマートハウス
- アタックサーフェスカード：デバイスの Web インタフェース
- 最も深刻な脅威カード：ブルートフォース
- 最も効果が高い対策カード：認証（弱い，無効な，空のパスワードの使用を禁止する）
- 残留リスク許容可否：否
- 追加の対策：ログイン試行数の制限

ここでは，学習者によりスマートハウス内に設置されたセンサの Web インタフェースがブルートフォース攻撃を受けて，不正アクセスさせるリスクシナリオが導出された．CAPEC 内に示された低減策は，大きな秘密の空間（パスワードの場合は文字長）を与えることがあげられている．参加者の議論の中で得られた最も効果が高い対策カードは，CAPEC の低減策を包含した内容となっていることが分かる．また，参加者は追加の対策の検討により，ログイン試行数に制限を設けることをあげており，CAPEC に示されていない対策を導出できていることが分かる．

4.4.2　ワークシートの分析（第 2 回目演習）

第 2 回目演習のうち，記載されたワークシートの結果を 1 つ例示する．

- IoT カード：制御システム
- アタックサーフェスカード：ネットワーク通信
- 最も深刻な脅威カード：プロトコル操作
- 最も効果が高い対策カード：安全性および信頼性の高い通信（データ暗号化により，リプレイ，傍受，パケット盗聴，通信傍受，盗聴などのネットワーク脅威を最小化する）
- 残留リスク許容可否：可
- 追加の対策：なし

ここでは，学習者により標的型マルウェアの制御系ネットワークへの感染を受けて，PLC の設定が書き換えられ，プラントの異常状態が生起し，作業員の安全を侵害するというリスクシナリオが導出された．CAPEC では，プロトコル操作に該当する低減策は示されていない．参加者の議論の中で得られた最も効果が高い対策カードは，データの暗号化を施すというものである．また，他の提出されたカードには暗号化コード署名などが含まれていた．PLC の設定を書き換える攻撃として脆弱なプロトコル（Modbus など）が送信元データを検証せずに受け入れる仕組みを悪用するもの [20] があるため，暗号化技術を活用し，データの信頼性を判断することは妥当な対策であると考えられる．

4.4.3　ワークシートの分析（第 3 回目演習）

第 3 回目演習のうち，記載されたワークシートの結果を 1 つ例示する．

- IoT カード：スマートファクトリー
- アタックサーフェスカード：管理インタフェース
- 最も深刻な脅威カード：接続リセット
- 最も効果が高い対策カード：ロギング（ユーザ認証，アカウント/アクセス権管理，ルールの変更，システム機能に関するイベントを記録するロギングシステムを導入する）

- 残留リスク許容可否：否
- 追加の対策：セキュア・ソフトウェア，セキュアなインタフェースとネットワークサービス

ここでは，学習者によりスマートファクトリー内の管理インタフェースに接続リセットを送ることでネットワークを混乱させるというリスクシナリオが導出された．最も効果が高い対策カードにはロギングが選択されたが，ロギング以外にも監視・監査などの他分類のカードも幅広く提出された．ロギングと監視により，攻撃元を早急に検知し，追加の対応を試みることを意図していると考えられる．文献 [29] によると，この攻撃は仕様の問題となるため，実装により緩和は可能であるが，回避はできないことからロギングし監視する対応には妥当性をあるものと考えられる．ここでは議論にあがっていなかったが，IPSec による下位レイヤの暗号化保護も有効な対策であると考えられる [29]．

3 回の演習のワークシートの結果と CAPEC で定義された攻撃の低減策と文献調査で得られた対策からおおむねの議論の妥当性を確認することができた．これは，学習者がグループを形成し，議論を通してリスクアセスメントを行った効果であると考えられる．ただし，一部のグループにおいては議論内で見逃してしまった対策もあったため，即時のフィードバックを与えることが重要である．現在の演習では参加者に議論の適正性を示す即時のフィードバックを与えることができていないため，CAPEC の記載事項やその他の文献などから議論のアウトプットに対する推奨する解答（リファレンス）をまとめることが今後の課題であるといえる．

4.5　改善：定性的な分析

演習の評価結果を受け，演習ツールの改善を実施した．アンケートには前節に示したアンケート項目のほかに自由記載形式で感想・意見を記載してもらった．演習実施ごとに改善し，次の演習時には改善された内容で演習を実施している．以下に定性的分析から改善した内容をまとめた．第 3 回目演習では大きな改善意見はなかった．

4.5.1　第 1 回目演習

意見 1：カードの文字が読み難い．

改善 1：簡潔な表現にし，文字数を少なくした．

意見 2：所持しているカードで提出できない場合があった．

改善 2：カードデッキから余りのカードを引くことを許容したルールに変更した．

4.5.2　第 2 回目演習

意見 3：優先順位が高いカードを提出した順にポイントが付与されたが，協調作業を阻害する．

改善 3：ルールを変更（ポイント付与を除去）した．

意見 4：カード内の情報量が多い．

改善 4：不要な情報の除去した．

意見 5：必ず手札を提出するルールとなっているため，ゲームの進捗が遅くなっている．

改善 5：ルールを変更（提出可能な手札がない場合はカードを提出しない旨を記載）した．

5.　まとめ

本稿では，教授設計モデルの ADDIE モデルに従って IoT セキュリティのためのゲーム演習ツール，IoT・ポリーを開発し，評価を行った．IoT・ポリーはリスクアセスメントを簡易化したプロセスを通じて，IoT システムの特徴，アタックサーフェス，脅威，対策について学習できるように設計した．IoT・ポリーを含む 4 つのゲーム演習ツールを使用した演習を実施し，参加者の反応を評価するため同一指標によるアンケートを回答してもらった．アンケート結果を分析し，既存のゲーム演習ツールと比較しても良好な結果が得られたことから IoT・ポリーの有用性を確認することができた．また，学習到達度についてはアンケートによる参加者の主観評価とワークシートを分析することで確認した．今後の課題は選択されたカードの組合せごとの推奨解答を作成し，参加者に即時にフィードバックを与えることなどがあげられる．なお，本稿で作成した IoT・ポリーは GitHub [30] 上に公開し，誰でもダウンロードし，活用できるようにしている．

謝辞　IoT・ポリーは平成 30 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] Center for Cyber Safety and Education: 2017 Global Information Security Workforce Study, available from ⟨https://iamcybersafe.org/wp-content/uploads/2017/06/europe-gisws-report.pdf⟩ (accessed 2018-12-25).
[2] 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）．
[3] MOTEX：調査レポート vol.05，入手先 ⟨https://www.motex.co.jp/nomore/report/5385/⟩（参照 2018-10-31）．
[4] 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）．
[5] 近江谷旦，宮本大輔，門林雄基：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，情報処理学会論文誌，Vol.41, No.12, pp.2264–2271 (2018).
[6] 2018 USENIX Workshop on Advances in Security Education: Git-based CTF: A Simple and Effective Approach to Organizing In-Course Attack-and-Defense Security Competit, available from ⟨https://www.usenix.org/sites/default/files/conference/protected-files/ase18_slides_wi.pdf⟩ (accessed 2019-03-11).
[7] 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）.
[8] Homeland Security: Strategic Principles for Securing the Internet of Things, available from ⟨https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf⟩ (accessed 2019-03-11).
[9] 情報処理推進機構：IoT 開発におけるセキュリティ設計の手引き，入手先 ⟨https://www.ipa.go.jp/files/000052459.pdf⟩（参照 2018-10-18）
[10] 情報処理推進機構：制御システムのセキュリティリスク分析ガイド 第 2 版，入手先 ⟨https://www.ipa.go.jp/security/controlsystem/riskanalysis.html⟩（参照 2018-10-18）.
[11] C.M. ライゲルース，A.A. カー=シェルマン：インストラクショナルデザインの理論とモデル，北大路書房 (2016).
[12] 鄭　仁星，鈴木克明，久保田賢一：最適モデルによるインストラクショナルデザイン，東京電機大学出版局 (2008).
[13] 鈴木克明：研修設計マニュアル：人材育成のためのインストラクショナルデザイン，北大路書房 (2015).
[14] J.M. ケラー：学習意欲をデザインする，北大路書房 (2010).
[15] 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 2018-11-14).
[16] Adam Shostack: Threat modeling designing for security, WILEY (2014).
[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] 日本ネットワークセキュリティ協会：セキュリティ知識分野（SecBoK）人材スキルマップ 2017 年版，入手先 ⟨https://www.jnsa.org/result/2017/skillmap/⟩（参照 2018-12-08）.
[19] M'Manga, A., Faily, S., Mcalaney, J., Williams, C., Kadobayashi, Y. and Miyamoto, D.: Eliciting Persona Characteristics for Risk Based Decision Making, *Proc. 32nd British Computer Society Human Computer Interaction Conference* (2018).
[20] Bodungen, C., Singer, B., Shbeeb, A., Wilhoit, K. and Hilt, S.: *Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions*, McGraw-Hill Education (2016).
[21] OWASP: IoT Attack Surface Areas Project, available from ⟨https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Attack_Surface_Areas⟩ (accessed 2018-10-17).
[22] MITRE: CAPEC™ A Community Resource for Identifying and Understanding Attacks, available from ⟨https://capec.mitre.org/⟩ (accessed 2017-09-19).
[23] 欧州 ネットワーク情報セキュリティ庁：Baseline Security Recommendations for IoT，入手先 ⟨https://2017.seccon.jp/⟩（参照 2018-04-20）.
[24] 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）.
[25] 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⟩（参照 2018-04-21）.
[26] Petri, G., von Wangenheim, C.G. and Borgatto, A.F.: A large-scale evaluation of a model for the evaluation of games for teaching software engineering, *Proc. 39th International Conference on Software Engineering: Software Engineering and Education Track* (2017).
[27] Fu, F., Su, R. and Yu, S.: EGameFlow: A scale to measure learners' enjoyment of e-learning games, Computers & Education, Vol.52, No.1, pp.101–112 (2009).
[28] Gunter, A.G., Kenny, F.R. and Vick, H.E.: Taking educational games seriously: Using the RETAIN model to design endogenous fantasy into standalone educational games, *Education Tech. Research Dev.*, Vol.56, pp.511–537 (2008).
[29] 情報処理推進機構：TCP/IP に係る既知の脆弱性に関する調査報告書，入手先 ⟨https://www.ipa.go.jp/security/vuln/documents/vuln_TCPIP.pdf⟩（参照 2019-03-16）.
[30] GitHub: IoT-Poly, available from ⟨https://github.com/nabetan/IoT-Poly⟩ (accessed 2019-03-14).

近江谷 旦

2006 年防衛大学校電気電子工学科卒業．2019 年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卒業．

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．

情報処理学会論文誌　教育とコンピュータ　Vol.6　No.1　40–51 (Feb. 2020)

正誤表

下記の箇所に誤りがございました．お詫びして訂正いたします．

訂正箇所	誤	正
40 ページ	再受付日 2019 年 8 月 19 日	再受付日 2019 年 8 月 18 日