修士論文

サイバーセキュリティマネジメント能力獲得のための利用者及びセキュリティ人材向けゲーム演習ツール

近江谷 旦

2019 年 3 月 15 日

奈良先端科学技術大学院大学
情報科学研究科 情報科学専攻

本論文は奈良先端科学技術大学院大学情報科学研究科に
修士（工学）授与の要件として提出した修士論文である．

近江谷 旦

審査委員：

門林 雄基 教授	（主指導教員）
笠原 正治 教授	（副指導教員）
林 優一 教授	（副指導教員）
妙中 雄三 准教授	（副指導教員）

サイバーセキュリティマネジメント能力獲得のための利用者及びセキュリティ人材向けゲーム演習ツール*

近江谷 旦

内容梗概

昨今，サイバー攻撃の高度化，広範囲化に伴いサイバーセキュリティ人材の不足が大きな問題となっている．また，多くの組織では教育が不十分であること，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が問題解決の障害となっている．モチベーションを維持，向上させながらサイバーセキュリティの能力を獲得させることが課題であると言える．上記の課題を克服するため，サイバーセキュリティ演習のゲーム演習に分類されるツールが開発されている．しかしながら，多くのゲーム演習ツールはセキュリティ啓発を目的に開発されており，ゲーム演習から多くの知識を取得することやセキュリティ人材向けの高度な知識とスキルの獲得を目指す内容となっていない．また，既存のセキュリティ人材向けに開発されたゲーム演習ツールはシステム開発やインシデント対応のプロセスに着目したものとなっているが，セキュリティ活動の全般を網羅できていない．このため，既存のゲーム演習ツールでは対応していない領域をカバーするためのサイバーセキュリティゲーム演習ツールを提案する．本稿では利用者の知識獲得，システム運用中の領域，リスクアセスメントのプロセス（システム開発時）に焦点を当て 3 つの演習ツールを開発する．提案するゲーム演習ツールと既存の演習ツールをあわせて活用することでセキュリティマネジメント能力を総合的に向上させることができる．すなわち，提案ツールは既存ツールの代替ツールではなく，既存ツールと共に強固なセキュリティ態勢を構築することを目指している．評価は提案したツールを実際に演習で使用し，参加者のアンケートを分析することで実施した．アンケートには教育ツールの評価で使用実績が豊富な既知の評価指標を用いた．有用性が確認されている既存ツールのアンケート結果と比較し，提案ツールは動機づけ効果，ゲームデザイン，

*奈良先端科学技術大学院大学 情報科学研究科 修士論文, 2019 年 3 月 15 日.

学習効果の評価項目において同程度以上の結果が得られた．特に動機づけ効果および学習効果においては，5 段階評価で平均点が 4 点以上になっている項目が多くあり，効果があることを確認した．また，事前・事後テストの平均点の結果を比較し 100 点満点中 7.63 点の向上が得られ，学習の効果があることを確認した．さらに学習記録を分析し，演習で取得するポイントから参加者の現状の能力を推定できる可能性を示した．以上から，提案ツールは学習者のモチベーションを維持・向上させつつ，サイバーセキュリティマネジメント能力を獲得させる上で有用であることを示した．

キーワード

ゲーム演習，インストラクショナルデザイン，ゲーミフィケーション，攻撃ライブラリ，重点管理策

Game Practice Tools to Acquire Cybersecurity Management Capability for Users and Security Personnel*

Tan Omiya

Abstract

In recent years, the shortage of cybersecurity personnel has become a big problem with the advancement and broadening of cyber attacks. In addition, there are obstacles to problem-solving as many organizations are not sufficiently educated and security officers suffer from security fatigue. It is a challenge to acquire cybersecurity management capabilities while maintaining and improving motivation. Cybersecurity game exercise tools were introduced in order to overcome the above challenge. However, many game exercise tools have been developed for the purpose of security enlightenment, and are not intended for acquiring knowledge (basic to advanced) and skills for security personnel. Furthermore, although the existing game exercise tools for security personnel focus on the process of system development and incident response, they cannot cover the entire security domain. For these reasons, we propose cybersecurity game exercise tools to cover the domains that are not supported by existing game exercise tools. In this thesis, we propose three game exercise tools that focus on knowledge acquisition for the users, risk assessment process, and the domain(s) under the system operation. It is possible to comprehensively improve security management capabilities by combining the proposed game exercise tools and existing exercise tools. In other words, the proposed tools are not alternatives to existing tools, but they rather complement them, and their combination pro-

*Master's Thesis, Graduate School of Information Science, Nara Institute of Science and Technology, March 15, 2019.

vides a stronger security posture. We evaluated our proposed tools by using them in game exercises and by analyzing the participants' questionnaires. We utilized an existing evaluation indicator, with abundant use record in the evaluation of the educational tools, to evaluate the questionnaires. The analysis of the participants' questionnaires showed that our tools performed as well as existing tools in the evaluation classes *motivation effect*, *game design*, and *learning effect*. There were effectivenesses since there were many items with an average score of 4 or more in a 5-grades evaluation system, especially in the *motivation effect* and the *learning effect* classes. There was also a *learning effect* because we compared the results of the average points of pre/post-tests and confirmed that there was an improvement of 7.63 points out of the 100 points. The analyzed results of learning records showed the possibility that a participant's current ability could be measured. From the above, we showed that our proposed tools are useful for maintaining and improving the motivation of the learner while helping them to acquire cybersecurity management capabilities.

Keywords:

Game Exercise, Instructional Design, Gamification, Attack Library, The Critical Security Controls

目次

図目次

第 1 章　はじめに

本章ではセキュリティ教育とセキュリティ人材の現状を把握し，それぞれの課題を明らかにする．明らかにした課題を受け，解決のための提案の概要と本稿の以降の構成を示す．

1.1　セキュリティ教育の現状と課題

組織のセキュリティ対策をまとめた様々なセキュリティ標準において，セキュリティ教育の重要性が記述されている．“The Critical Controls for Effective Cyber Defense (CSC)”[1] はセキュリティ対策の中でもっとも効果的な管理策を 20 個にまとめたセキュリティ標準であり，20 個のセキュリティ管理策を適切に実施することで既知の攻撃の 85 % 以上を防ぐことができると言われている．CSC の各管理策は基礎（Basic），基本（Foundational），組織（Organizational）の 3 つに分類され，組織的な管理策の 1 つにセキュリティ教育が挙げられている．

上記にようにセキュリティ教育の重要性は認知されているが，適切に実施されていない現状がある．MOTEX 社の調査 [2] によると調査に回答した対象の約 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．一方で 75 % 以上の回答者はセキュリティ知識を向上させる意欲を持っていると回答している．セキュリティ教育において学習者と実施者の間に大きなギャップが存在することがわかる．同じ調査によると，セキュリティ教育実施時に困っていることとして，約 30 % の調査対象が，予算がないこと，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挙げている．以上から，セキュリティ教育では学習者に動機づけを与え，セキュリティの知識を向上させることが課題であると言える．

1.2　セキュリティ人材の現状と課題

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スキルを持った人材が必要とされる．また，攻撃者により常に新しいサイバー攻撃の手法が

表 1.1: 情報セキュリティに関わる業務上の役割の分類（6 分類）

役割	定義	職種例	
		自社向け人材	社外向け人材
①統括的情報セキュリティ管理者	組織全体の情報セキ ュリティ対策を統括・管理する人材	・CSO/CISO ・全社の情報セキュリティ管理者 ・プライバシーオフィサー	ー
②部署内情報セキュリティ管理者	統括的情報セキュリティ管理者の指示のもとで部署内の情報セキュリティ対策の実施を主導する人材	・部門の情報セキュリティ管理者 ・情報セキュリティマネジメント人材 ・情報セキュリティアドミニストレータ	ー
③開発系業務従事者	情報セキュリティ対策製品・サービス等の設計、開発関連業務に従事する人材	・情報セキュリティスペシャリスト人材 ・自社の製品 ・サービスにセキュリティを実装する技術者	・セキュリティ製品・ツールの開発者 ・製品・サービスにセキュリティを実装する技術者 ・アプリケーションスペシャリスト
④運用系業務従事者	監視・インシデント対応等のサービス提供に関する業務に従事する人材	・情報セキュリティスペシャリスト人材 ・インシデントハンドラー	・情報セキュリティスペシャリスト人材 ・インシデントハンドラー ・セキュリティ監視・運用サービ ス技術者
⑤検査・監査系業務従事者	分析，検査，監査等のサービス提供に関する業務に従事する人材	・情報セキュリティスペシャリスト人材 ・セキュリティ監査者（社内）	・情報セキュリティスペシャリスト人材 ・セキュリティアナリスト ・脆弱性診断士 ・セキュリティ監査者（外部）
⑥コンサルティング系業務従事者	情報セキュリティマネジメント関連サービスの提供に関する業務に従事する人材	・セキュリティ講師	・セキュリティコンサルタント ・プロフェッショナルセールス ・セキュリティ講師

開発されており，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．フロスト&サリバンの調査 [3] によると，世界中で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 万人の人材が不足すると推計されている [4]．上記報告によると情報セキュリティに関わる業務上の役割は表 1.1 により大きく 6 つに分類される．図 1.1 にはそれぞれの分類における量的な人材の不足感，図 1.2 には質的な人材の不足感を示している．すべての役割で量的および質的に人材が不足していることがわかる．

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 [5]．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 [6]．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

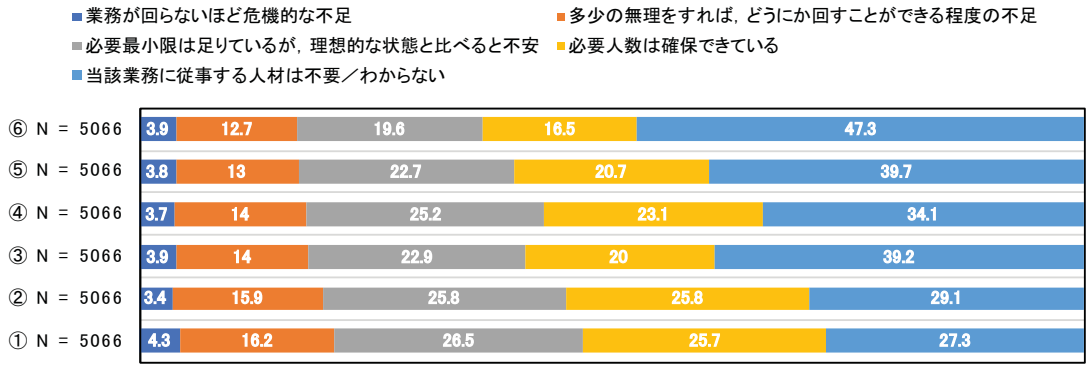


図 1.1: セキュリティ人材の量的不足感

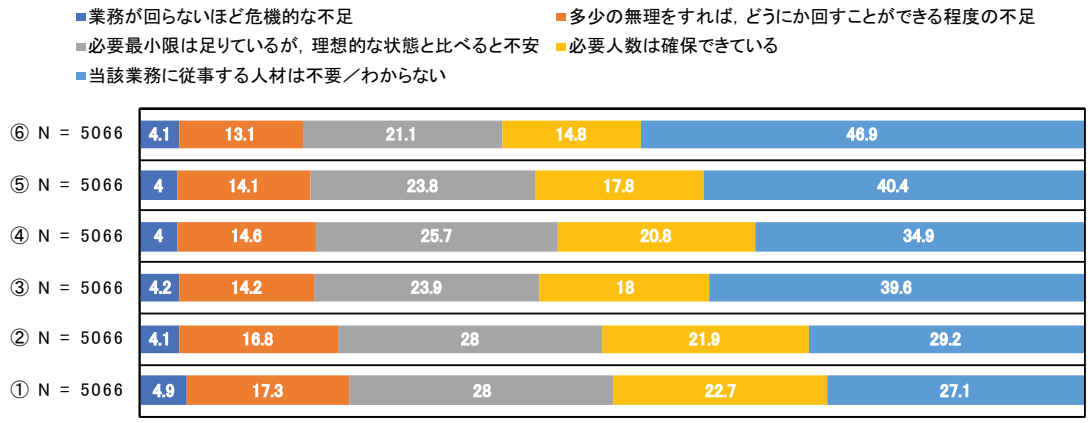


図 1.2: セキュリティ人材の質的不足感

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言える．

1.3　課題解決の提案と本稿の構成

前項を受け，セキュリティ教育，セキュリティ人材の育成および学習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言える．本稿では上記の課題解決のため，ゲーム形式でセキュリティ教育を実施するための 3 つのサイバー

ゲーム演習ツールを提案する．サイバーゲーム演習においては，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，管理面の能力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，管理面に関する能力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などの特定の領域に焦点を当てている．これは，セキュリティ管理の領域は広範囲で 1 つの演習ツールだけでは網羅できないためである．このため，本稿では学習者（利用者・セキュリティ人材）に学習の動機づけを与えるとともに既存演習ツールでは未対応の管理面に関する能力を習得させることを目的とした．この目的を達成するため，学習者の動機づ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，最新の体系的に整備された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様々なセキュリティ標準を活用している．既存ツールと 3 つの提案ツールを合わせることですべての領域を網羅的に学習できることを目指している．

本稿の以降の構成は以下のとおりである．第 2 章では，関連知識として教授設計 [7]，ゲーミフィケーション，ゲーム演習の関係を整理し本稿が焦点を当てている領域を明確にする．第 3 章では，関連研究としてサイバーセキュリティの分野におけるゲーム演習の先行研究を示し，既存の管理面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の未対応領域を明示する．第 4 章～第 6 章では，教授設計のモデルの 1 つである ADDIE モデル [8] を適用した上で，3 つのゲーム演習について詳述する．第 7 章では本研究を踏まえた上で議論を行う．最後に第 8 章で本稿を総括する．

第 2 章　関連知識

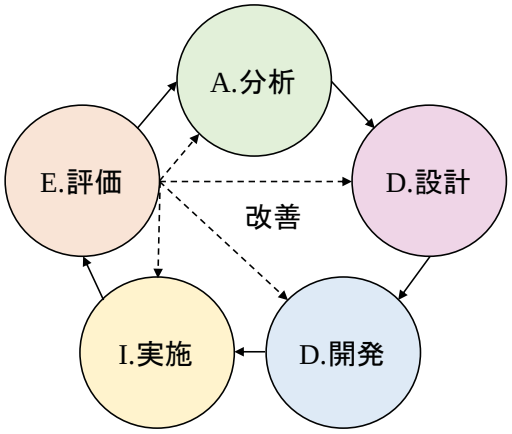
本章では，本研究を進める上で重要である関連知識（教授設計（2.1 節），ゲーミフィケーション（2.2 節），サイバーセキュリティゲーム演習（2.3 節））を整理した．また，それぞれの関連知識がどのような関係になっているかを明示している．教授設計とゲーミフィケーションには重なり合う領域があり，その中にゲーム演習が含まれる．本稿ではゲーム演習の領域のうち，サイバーセキュリティ分野の管理面の知識・スキルを獲得するための領域に焦点を当てている．2.4 節では本稿が焦点に当てているサイバーセキュリティマネジメント能力について定義する．

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．ID はもともと米軍で兵士教育のコース設計のために開発されたが，その後米国の企業内教育の教育設計手法として普及した．昨今，日本においても ID を用いた教育が普及してきている．ID には様々なモデルがあるが，以下に本稿を作成するにあたり，参考にしたモデルを示す．

2.1.1　ADDIE モデル

ADDIE[8] 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．図 2.1 に ADDIE モデルの概要を示す．本稿では 3 つの提案ツールに ADDIE モデルの改善サイクルを適用し，開発を行っている．



A 分析:学習者の特性，教育内容を分析

D 設計:目標を設計し，教授手法を決定

D 開発:教材の作成

I 実施:実際に教授を実施

E 評価:教材が目標を達成するのに役立ったかどうかを評価

改善:それぞれのプロセスを改善

図 2.1: ADDIE モデル

2.1.2 ARCS 動機づけモデル

ARCS 動機づけモデル [9] 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結果，ARCS に該当する 4 つの分類項目（注意，関連性，自信，満足）で学習意欲が飛躍的に高まることを実証している．図 2.2 はケラーの動機づけとパフォーマンスのマクロモデルであり，ARCS のそれぞれの分類の関係を示している．ARCS のそれぞれの分類はさらに 3 つの下位分類により定義される．以下に ARCS の主分類と下位分類の内容を示す．

- Attention:注意
  学習者の関心を獲得し，学ぶ好奇心を刺激する．
  - A1　知覚的喚起：彼らに興味を持たせるために何をしたらよいだろうか．
  - A2　探究心の喚起：どうしたら探究の態度を刺激できるだろうか．
  - A3　変化性：どうしたら彼らの注意を維持できるだろうか．
- Relevance:関連性
  学習者の肯定的な態度に作用する個人的ニーズやゴールを満たす．
  - R1　目的指向性：どうしたら学習者のニーズを最も満たすことができ

るだろうか（私は彼らのニーズを知っているか）.
  - R2　動機の一致：いつどのようにして，妥当な選択・責任・影響を学習者に提供できるか.
  - R3　親しみやすさ：どうしたら学習者の経験にインストラクションを結びつけることができるか.
- Confidence:自信

  学習者が成功できること，また，成功は自分たちの工夫次第であることを確信・実感するための助けとなる.
  - C1　学習要件：ポジティブな成功への期待感を形成するために，どういう支援をすることができるか.
  - C2　成功の機会：どのような学習体験にすれば，学習者が自分の能力を信じることを支援して高めることができるだろうか.
  - C3　個人的なコントロール：学習者に，自分の成功が自分の努力と能力の結果であることをどのようにして知らせることができるだろうか.
- Satisfaction:満足

  （内的と外的）報酬によって達成を強化する.
  - S1　自然な結果：どうしたら学習者が新たに習得した知識やスキルを使用する意味ある機会を提供できるだろうか.
  - S2　肯定的な結果：何が学習者の成功を強化するだろうか.
  - S3　公平さ：達成に関する肯定的な感情をつなぎとめるには，どのように支援することができるだろうか.

本稿では，学習者の動機づけ効果を与えることを 1 つの目的としていることから，動機づけの設計には次節のゲーミフィケーションを活用し，動機づけ効果の測定には ARCS 動機づけモデルに基づいて作成された指標を活用している.

2.1.3　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 [10]．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

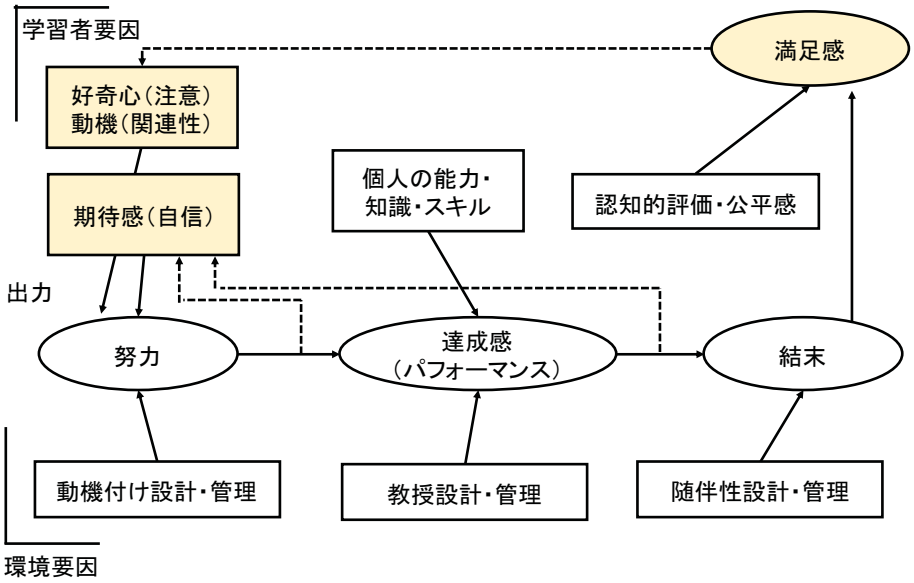


図 2.2: ケラーの動機付けとパフォーマンスのマクロモデル

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）に焦点を当てて評価を行っている．カークパトリックの 4 段階評価モデルの各レベルの概要は下記のとおりである．

- レベル 1（反応）: 受講者は教育に対して，どのような反応を示したかを確認する．研修後のアンケートで受講者の反応を確認し，受講者の理解度や満足度を測定する．
- レベル 2（学習）: どのような知識やスキルを習得したかを確認する．研修で学習した内容について，理解度テスト，検定試験，実技試験などで習得度合いを測定する．
- レベル 3（行動）: 受講者がどのように知識とスキルを仕事に活かしたかを確認する．研修後に日常業務でどのような行動変容が現われたかを評価する．受講者へのヒアリング（フォローアップ調査）や仕事への取り組み方など，職場で観察可能なものは上司などが評価（上長アンケート）する．
- レベル 4（結果）: 教育は組織と組織の目標にどのような効果をもたらしたかを確認する．その研修を実施したことで，どれだけ売上を上がったのか，利

益を得たのかなどの業績を確認する．レベル 3 の行動変容が「組織全体」としてプラスになったかどうかに着目している．

2.2 ゲーミフィケーション

ゲーミフィケーション [11] 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単に学習を促進するだけなく，消費者向け商品やマーケティングの中にも取り込まれ，活用事例は増加している．Karl M. Kapp はゲーミフィケーションには以下の特長があると述べている [11].

- ゲーミフィケーション設計のプロセスは ADDIE モデルとスクラムモデル（ソフトウェア開発の一手法）を用いることが最も効果的である．
- ゲーミフィケーション設計には ARCS 動機づけ理論の他，認知心理学などの多くの理論が用いられている．
- インストラクショナルゲームは宣言的な知識，手続き的知識を提供し，学習者に効果的な学習を提供することができる．

ゲーミフィケーションを取り入れたゲーム教材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 [12, 13]．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 [14] が報告されている．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 [15, 16]．以下にゲーミフィケーション・フレームワークの項目を示す．

- プレイヤーの分類
- 目的・ゲームコンセプト
- 目標
- 可視化・フィードバック
- ソーシャルアクション
- プレイサイクルデザイン

- 改善・運用

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 [17, 18]. 以上から，ゲーミフィケーション・フレームワークを提案ツールの 1 つであるセキュ・ワンに適用した.

2.3 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)」[19] 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 2.1 に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」[20] や総務省による「実践的なサイバー防御演習 (CYDER)」[21] が知られている．これらは表 2.1 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，規則および手順等を活用し，参加者間の競争や協調を構築する．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.

図 2.3 に教授設計，ゲーミフィケーション，ゲーム演習の関係を示す．文献 [19, 22] では演習の準備から評価の方法の具体例を示しているが，これは ADDIE モデルの各プロセスを詳述していることがわかる．また，参加者間の競争や協調を構築し，学習者に動機づけ効果を与えるためにはゲーミフィケーションを活用できることがわかる．文献 [23] では教育や学習にゲーミフィケーションを取り込む方法論が示されている．ここでは，ゲーム演習の起源である War Game をゲーミフィケーションと関連するゲーム教材として記述している．War Game は軍事目的のために開発されたものであるが，経営学，経済学などの分野における戦略や意思決定の学習，企業における事業戦略の計画策定と評価にも使用されている．また，教材の開発に ADDIE モデルを活用することや教授設計者の役割についても示してい

表 2.1: 演習の分類

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

る．すなわち，ゲーム演習は ID とゲーミフィケーションの要素を組み合わせたものと言える．以上から，本稿のゲーム演習は ID とゲーミフィケーションの理論を融合させた内容となっている．

表 2.2 にサイバーセキュリティゲーム演習の概要を示す．サイバーセキュリティ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[24] 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．

2.4 サイバーセキュリティマネジメント能力

JNSA（日本ネットワークセキュリティ協会）ではセキュリティ知識分野（SecBoK）人材スキルマップ [25] を公開し，16 のセキュリティ人材の役割（文献 [4] で定義した 6 分類を細分化した役割）に必要なスキル・知識を定義した．この人材スキルマップによると，必要な能力の中にはテクニカルスキル以外の項目が多

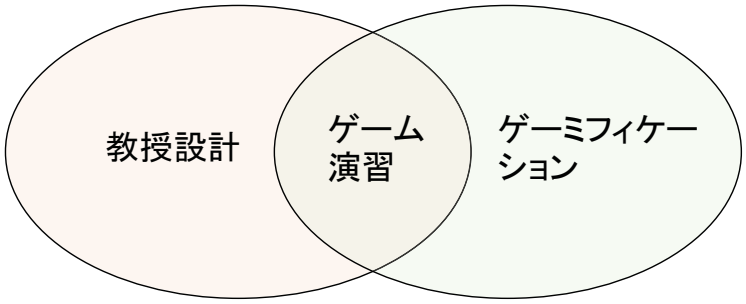


図 2.3: 教授設計，ゲーミフィケーション，ゲーム演習の関係

表 2.2: サイバーセキュリティゲーム演習の概要

	技術	管理
分野（例）	パケット解析	脅威モデリング
	フォレンジック	インシデント対応
具体例	CTF	KIPS Championship
実施頻度	多	少

数含まれていることがわかる．表 2.3 に代表的なテクニカルスキル以外のスキルをまとめた．テクニカルスキル以外のスキルを適切に実施するためにはテクニカルな知識も含め多くの知識が必要となる．本稿ではテクニカルスキル以外のスキルと関連する知識をサイバーセキュリティマネジメント（管理面）の能力と定義する．表 2.3 に含まれるセキュリティマネジメントを包含した意味となっている．図 2.4 にテクニカル（技術面）の能力とサイバーセキュリティマネジメント（管理面）の能力の関係を示す．技術スキルと管理スキルは関連する知識を有することで適切な実施が可能となる．情報処理推進機構が年 2 回実施する情報セキュリティマネジメント試験 [26] は情報セキュリティマネジメントの計画・運用・評価・改善を通して組織の情報セキュリティ確保に貢献し，脅威から継続的に組織を守るための基本的なスキルを認定する試験である．情報セキュリティマネジメント試験の出題範囲はマネジメント（管理）知識だけでなく，テクノロジ（技術）知識も含まれている．管理スキルを適切に実施するためには関連する管理面の知識に加えて，技術面の知識を必要であると言える．すなわち，本稿で定義するサイバーセキュリティマネジメ

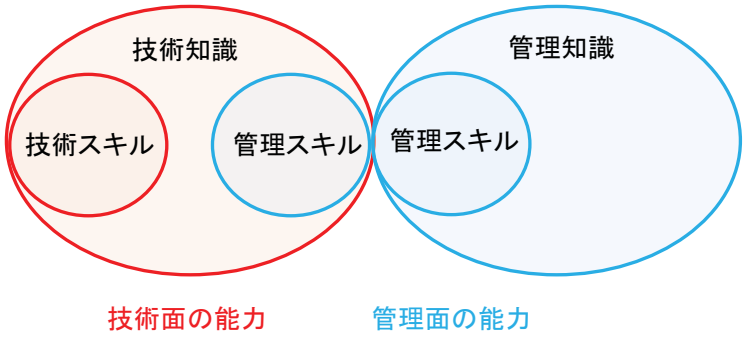


図 2.4: 技術面の能力と管理面の能力の関係

ント能力とは図 2.4 の青色の領域に該当する．

現状のサイバーセキュリティゲーム演習の多くはテクニカルな能力に焦点を当てており，セキュリティ人材に必要な能力を網羅的に学習することができない．このため，テクニカルな能力に該当しないサイバーセキュリティマネジメント（管理面）の能力に焦点を当てた演習ツールの開発が必要であり，本稿では管理面の能力獲得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挙げられる．管理面のスキルにはリスク分析（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挙げられる．ゲーム演習は広範囲の領域から特定の領域に焦点をあて，知識・スキルの獲得を図るように設計されている．

表 2.3: 代表的なテクニカルスキル以外のスキル（SecBoK より一部抜粋）

分野	大項目	小項目
基礎	ICT 基礎	ナレッジマッピングの実施に関するスキル システム開発のコンセプトに関するスキル システム運用のコンセプトに関するスキル サーバの計画、管理及び保守の実施に関するスキル 問い合わせとレポートの生成に関するスキル
	ビジネス基礎	企業の知的資産をアセスメントできるスキル 課題解決のための科学的規則と手法の利用に関するスキル 損失評価の実施に関するスキル 情報を効率的に伝達するための他者とのコミュニケーションに関するスキル
セキュリティ基礎	総論	機密性、完全性及び可用性の原則の適用に関するスキル
セキュリティ マネジメント	総論	システムセキュリティの目的を反映したポリシーの作成に関するスキル 情報保証の原理と信条に基づくセキュリティ管理策の設計に関するスキル 情報システムとネットワークの保護の必要性の識別に関するスキル 供給者および/または製品の信頼性に関する評価に関するスキル
セキュアシステム	総論	容量と要求の分析の実施に関するスキル
設計・構築		セキュリティ設計の適切性の評価に関するスキル
セキュティ運用	総論	セキュリティ運用と事業の衝突回避に関するスキル
	インシデント 対応	インシデントハンドリング手法の利用に関するスキル インシデントの根本原因分析の実施に関するスキル
サイバー攻撃手法	総論	脆弱性の種類と関連する攻撃の認知とカテゴライズに関するスキル
法・制度・標準	総論	活動に影響を及ぼす技術的及び法的なトレンドの追跡と解析に関するスキル

第 3 章　関連研究

本章では管理面に焦点を当てた既存のゲーム演習をまとめ，提案ツールの新規性について示す．図 3.1 は本章で紹介するゲーム演習ツールの対応領域をまとめたものである．図の横軸はシステム開発からインシデント発生後までの時間軸，縦軸は学習者が必要とするスキルレベルを表している．ゲーム演習ツールは広範囲の領域の中から特定の領域に焦点を当てた内容になっている．

3.1　利用者向けのゲーム演習

ここでは利用者向けのゲーム演習ツールをまとめた．利用者向けの演習ツールは啓発や利用者に関連する特定スキルに焦点を当てている．

- サイバーセキュリティ専門官　人狼
  サイバーセキュリティ専門官　人狼 [18] ではカードゲーム形式で「CSIRT（Computer Security Incident Response Team）」陣営と「サイバー犯罪者」陣営に分かれた攻防戦を通してサイバーセキュリティの概念を学ぶことができる．サイバーセキュリティ専門官　人狼の目的はセキュリティ啓発を促す

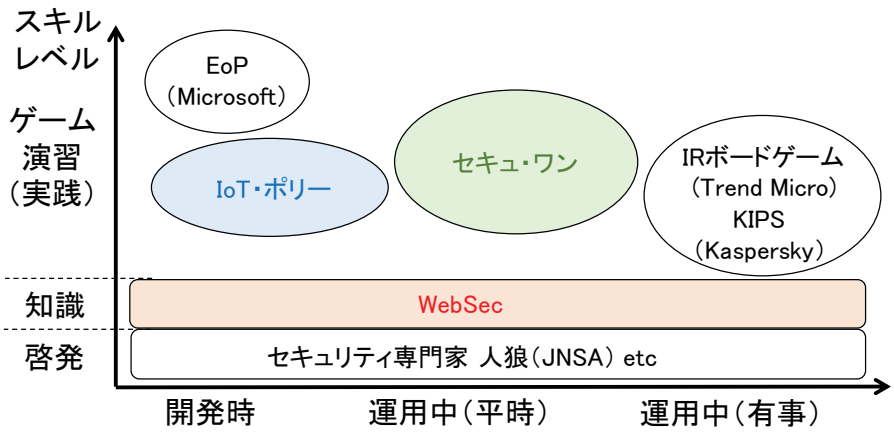


図 3.1: ゲーム演習ツールの対応領域

ことである．CSIRT の職務や内部不正対策について，参加者に演習後の発展学習を促すことで詳細な知識の獲得を期待している．

- Control-Alt-Hack
  Control-Alt-Hack[27] はフィッシング，ソーシャルエンジニアリングなどのサイバー攻撃手法の概念を学習するためボードゲームである．学習者はカードに記述されたサイバー攻撃の手法をゲーム中に意識することができる．Control-Alt-Hack の目的はセキュリティ啓発を促すことである．Control-Alt-Hack には技術的知識はほとんどなく，サイバーセキュリティ教育を開始するためのはじめの段階と位置付けている．
- What.Hack
  What.Hack[28] は標的型メールの特徴を理解するための Web ベースの教育ゲームである．学習者は示された正規メールと標的型メールの特徴から制限時間内に受信するメールを正規メールと標的型メールに振り分けなければならない．学習者が 1 つのステージをクリアすると，付与される特徴に関する情報が追加され，振り分けの難易度が高くなる．What.Hack の目的は標的型メールの特徴を理解し，標的型メールを適切に見分けるスキルを向上させることである．

3.2 セキュリティ人材向けのゲーム演習

ここではセキュリティ人材向けのゲーム演習ツールをまとめた．図 3.1 の特定の時間軸に焦点を当てた内容となっている．

- Elevation of Privilege
  Elevation of Privilege (EoP)[29] 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ーにより 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．

- KIPS
  Kaspersky Interactive Protection Simulation (KIPS)[30] 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
  インシデント対応ボードゲーム [31] 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．

3.3 提案ゲーム演習ツールの新規性と対象

サイバーセキュリティの領域は非常に広範囲であることから 1 つのゲーム演習ですべての領域を網羅することは不可能である．既存ツールは学習者に動機づけを与え，関連する知識を獲得させる上で非常に有用であると考えられる．既存ツールで対応できていない領域においてはゲーム演習とは別の手段を用いる必要があり，学習者が動機づけ効果などのゲーム演習のメリットを享受できないことになる．上記の課題を克服するため，既存ゲーム演習では未対応の領域を埋める形で 3 つのゲーム演習ツールを提案する．

3.3.1 提案ゲーム演習ツール（利用者向け）

利用者向けの演習ツールは啓発目的または特定のスキルに焦点を当てている．しかし，サイバー攻撃の被害は組織だけでなく利用者にも及ぶことから利用者であっ

てもサイバー攻撃と対策を理解しておく必要がある．啓発の次の段階として，サイバー攻撃に対抗するために利用者として身につけておくべき知識を網羅的に学習できるゲーム演習ツールが望まれる．このため，新たにゲーム演習ツールである WebSec を提案する．第 4 章に WebSec の提案内容を詳述する．

3.3.2 提案ゲーム演習ツール（セキュリティ人材向け）

セキュリティ人材向けの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の脅威の洗い出し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．このため，新たなゲーム演習ツールとして，IoT・ポリーとセキュ・ワンを提案する．第 5 章に IoT・ポリー，第 6 章にセキュ・ワンの内容を詳述する．提案するゲーム演習ツールの新規性は既存演習ツールでは未対応の領域に焦点を当て，必要な知識とスキルを獲得できる点である．

図 3.2 にゲーム演習ツールの対応領域と対象者を示す．利用者と経産省が定義した 6 種類のセキュリティ人材が図 3.1 のどの領域に含まれるか明示している．WebSec は利用者を対象に作成，評価したが，コンテンツを入れ替えることで，セキュリティ人材も対象とすることができる．IoT・ポリーはすべてのセキュリティ人材を対象としている．セキュ・ワンは開発系業務従事者を除くすべてのセキュリティ人材を対象としている．

3.3.3 提案ゲーム演習ツールで獲得を目指す能力

表 3.1 に本稿で獲得を目指す能力の一覧を示す．WebSec で獲得を目指す「利用者が学習すべき知識」以外の項目は SecBoK で定義されたセキュリティ人材が必要なスキル・知識から該当するものをリストアップした．本稿では 3 つの提案ツールにより，幅広い知識とスキルの獲得を目指す．

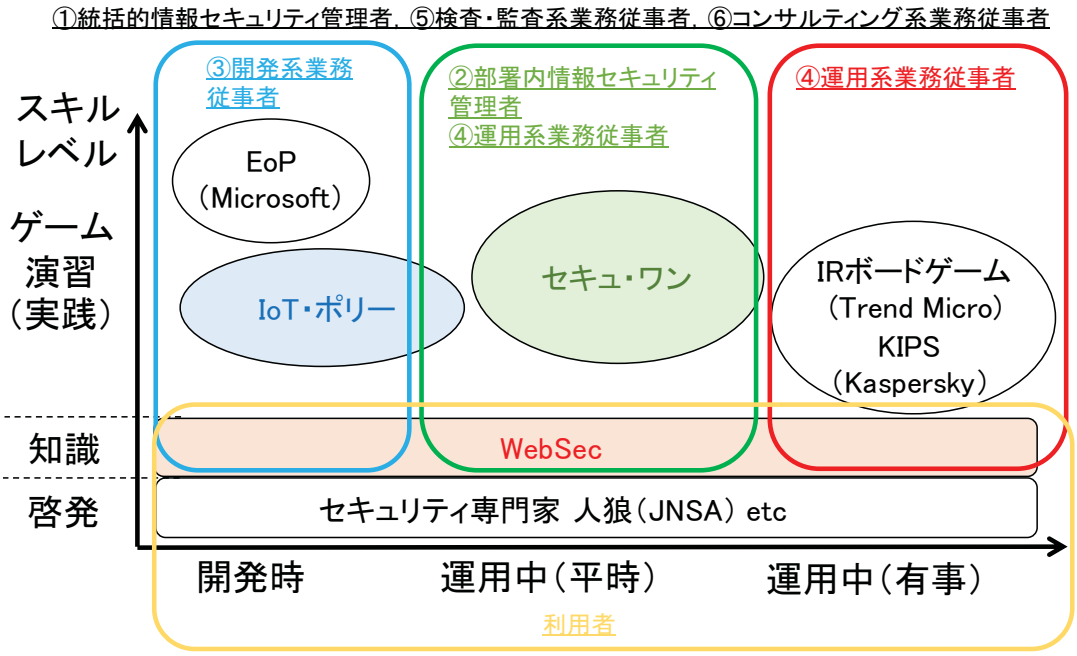


図 3.2: ゲーム演習ツールの対応領域と対象者

表 3.1: 提案ゲーム演習ツールで獲得を目指す能力

区分	獲得を目指す能力	WebSec	IoT・ポリー	セキュ・ワン
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	-	○	○

第 4 章　WebSec

本章では提案ゲーム演習ツールの 1 つである WebSec について詳述する．WebSec はサイバー攻撃に対抗するため，利用者として身につけておくべき知識を網羅的に学習することおよび学習者に動機づけを与えることを目的としている．また，セキュリティ教育実施時に困っていることとして約 30 % の対象が予算がないこと [2] からツールを容易に配布ができるようにした．以降の各節は ADDIE モデルのプロセスごと，内容をまとめている．

4.1　分析：教育コンテンツとシステム要件

本節では学習コンテンツおよび WebSec のシステム要件を分析した．

4.1.1　コンテンツ

セキュリティ教育の対象者は IT システムの利用者とセキュリティ人材に大別できる．効果的にセキュリティ教育を実施するためには学習者の立場に応じてセキュリティ教育のコンテンツを変更する必要がある．WebSec は学習者の立場やレベルにあった内容を提供する．

4.1.2　システム要件

以下にシステム要件をまとめた．

- 配布の容易性: WebSec は企業におけるセキュリティ教育での活用を想定している．集合教育や個別学習には組織のイントラネット内で実施されるため，配布の容易性を確保したシステムを構築する．
- 管理者による理解度・進捗の把握: 管理者が学習者の学習状況を把握できるようにする必要がある．また，コンテンツやツールの改善に役立てるため，学習状況を分析できるようにする．

- ゲーム性: 動機付け効果に有効性が確認されているゲーミフィケーションの仕組みを活用する．

4.2 設計：教育コンテンツ，システム設計，ゲーム設計

本節では，分析結果を反映させる形でシステムの設計を実施した．

4.2.1 コンテンツ

WebSec では難易度および対象に応じて 3 つのをコンテンツ群を作成する．

- レベル 1：利用者向けの内容とする．コンテンツは内閣サイバーセキュリティセンター（NISC）[32] および総務省の資料 [33] を参照する．
- レベル 2：多くの組織にはユーザのシステム利用に関して権限を持った管理者が存在する．ここでは，システムのセキュリティ管理について学習できる管理者向けの内容とする．コンテンツは CSC[1] を参照する．
- レベル 3：セキュリティ人材は自組織のセキュリティ対策を検討し，インシデント発生時に迅速に対応できるようにサイバー攻撃手法の特徴を知っておく必要がある．コンテンツはサイバー攻撃手法の辞書に当たる CAPEC[34] の内容を参照する．
- 被害事例の学習：レベル 1〜3 のコンテンツとは別に，セキュリティ対策を怠った場合の被害事例を学習できるようにする．被害事例の学習は学習者の進捗に併せて，学習している内容と関連するコンテンツを提示する．被害事例は学習した内容を理解していれば正しい解答できるが，やや応用力が必要とされる．コンテンツは verizon 社の公表資料 [35][36] の内容を参照する．

4.2.2 システム設計

図 4.1 にシステム構成図を示す．システムは配布が容易なように Docker コンテナ上に構築する．また，管理者が学習者の状況を容易に把握できるようにデータ

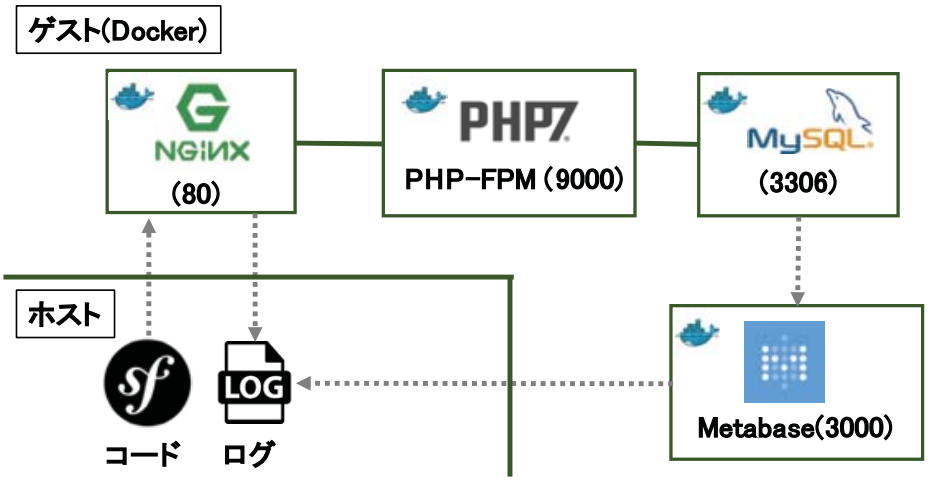


図 4.1: システム構成図

ベースの BI（ビジネスインテリジェンス）ツールである Metabase を活用する．システムから得られるログは教育終了後に確認できるようにホストとの共有ボリュームに保存することで，永続化している．データベースは学習者の進捗，問題の正解・不正解の記録などを管理する．

4.2.3 ゲーム設計

学習者の進捗に応じてポイントを付与し，他学習者と競争することで学習者に動機づけを与えることを狙いとする．セキュリティトピック毎に知識の学習と問題の解答を実施し，正解だった場合に新たな知識を提供することを繰り返すことで段階的に学習できるようにする．問題には難易度を定義し，正しい解答ができた場合には難易度に応じたポイントを付与する．誤った解答の場合は難易度に応じてポイントを減算する．

4.3 開発：Web アプリケーション開発，システム開発

設計に基づき WebSec を開発した．図 4.2 と図 4.3 に WebSec のイメージを示す．図 4.2 は知識の学習画面であり，図の左側に項目，右側に選択した項目の細部

内容が表示される．図 4.3 は知識事項を学習した後に表示される問題画面である．問題は多肢選択形式と自由記載形式の 2 種類あり，正解しなければ，関連する新しい知識事項の学習には進めない．解答が不正解の場合，学習者は再度，関連する知識事項について確認を行う必要がある．学習の進捗に応じて画面上部の 3 つのポイントが推移する．それぞれのポイントの詳細は下記のとおりである．

- セキュリティ満足度：ゲーム内で学習者がどれくらい信頼できる人なのかを数値で表現している．学習者が問題を適切に解答することで値が増加するが，誤った解答や長時間何もしなかった場合，この値は減少する．この値が 0 になった場合，ゲームオーバーとなる．すなわち，学習者の継続的な学習へのインセンティブとなっている．
- 許容トークン：学習者が解答を誤った場合，セキュリティ満足度は低下するが，許容トークンの値が高ければ満足度の減少は小さくなる．一方で許容トークンの値が低ければ，満足度の低下が大きくなる．すなわち，セキュリティ満足度と許容トークンの変化量を任意に設定することでゲームオーバーのなりやすさを調整することができる．
- スコア：学習者の取得スコアを表す．問題の正解・不正解を受け，難易度に応じて値が変化する．ランキングボードでこの値を競うことで参加者の競争心を煽ることができる．

図 4.4 は学習者の学習状況をまとめたステータス画面である．学習者の学習継続時間，進捗，スコアの他，他の学習者のスコアと比較した成績を表示している．学習状況を数字化することで学習意欲の維持・向上を狙いとしている．

図 4.5 に Metabase による学習者のポイント推移の表示画面を示す．Metabase によりリアルタイムで学習者のポイントの推移を確認することができる．この図では学習者のスコア値の推移を例として表示している．集合教育時に Metabase をランキングボードとして用いることで学習者間で競争を促し，学習意欲を高める際に活用できる．また，教育実施後にデータの加工や表示が可能で管理者は学習状況などの管理も容易に実施できる．

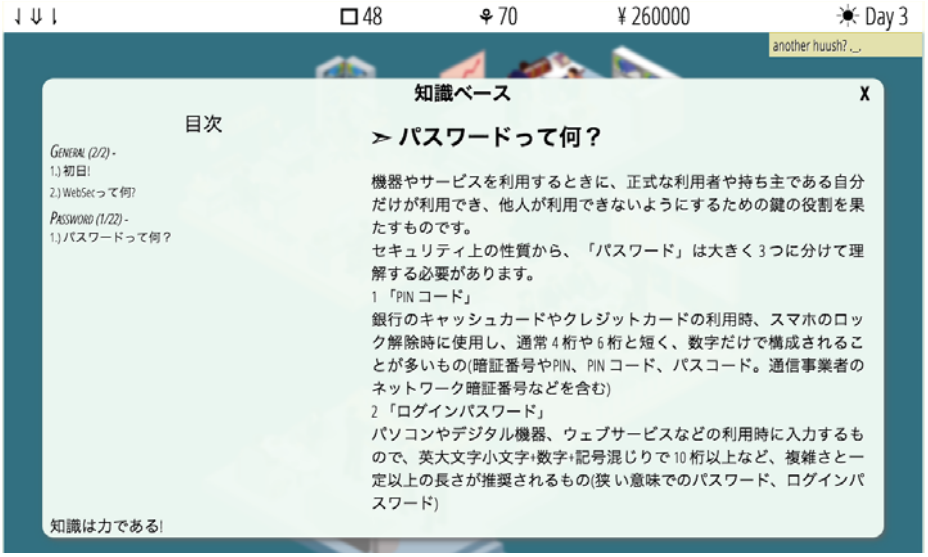


図 4.2: WebSec のイメージ 1（知識の学習画面）

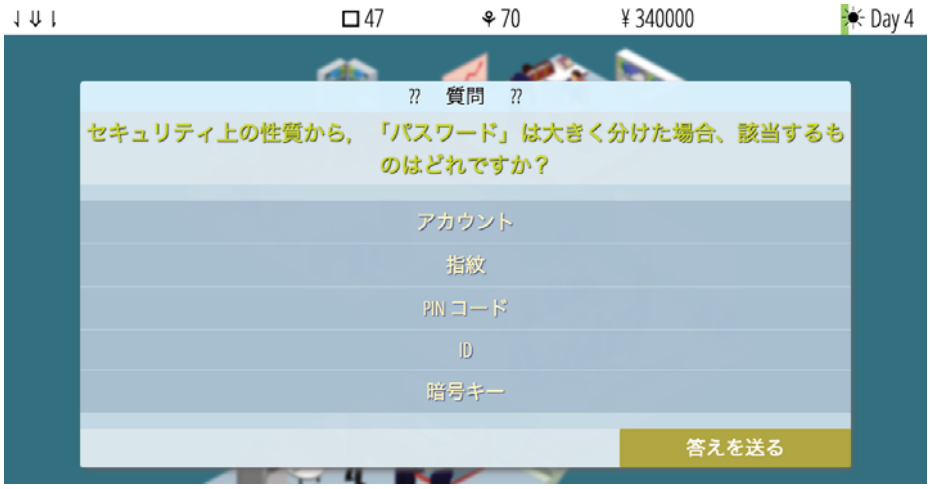


図 4.3: WebSec のイメージ 2（問題画面）

4.4 実施：ゲーム演習の実施

WebSec の有用性を確認するため，SecCap[37] の受講生を対象に演習を実施した．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

図 4.4: WebSec のイメージ 3（学習状況のステータス画面）

ある．実施した演習の概要は下記のとおりである．

実施日時：H30.9.15(金) 10:30 - 12:00(約 90 分間)

対象：大学院生 (SecCap 受講生)

人数：16 名

実施したゲームレベル：レベル 1

また，セキュリティ教育受講に関する情報は下記のとおり．

セキュリティ研修の経験：ある 8 名，ない 8 名

研修頻度：年 1 回 7 名，年 1 回以上 1 名

研修方法：集合教育 7 名，e-learning 1 名

4.5 評価：評価方法と評価結果

本節ではゲーム演習の評価方法と演習実施後の評価結果を示す．

図 4.5: Metabase の画面例：学習者のポイント推移（X 軸：時間経過，Y 軸：学習者の取得スコア）

4.5.1 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．

レベル 1（反応）

演習直後のアンケート調査により参加者に演習ツールのユーザ評価を実施してもらう．アンケートの項目には既存の指標と独自で作成した内容を用いる．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+[38]，EGameFlow[39]，RETAIN[40] がある．表 4.1 にそれぞれの特徴をまとめた．3 つの評価指標は教育ゲームなどで活用されている．MEEGA+ はデジタル・アナログの教育ゲームの両方に対応しているため，本稿の他の 2 つのアナログゲーム演習（IoT・ポリー，セキュ・ワン）でも活用できる．また，ARCS 動機づけモデルに加えてユーザ体験（ゲームのデザインなど），学習効果に基づき，アンケート項目を作

表 4.1: 既存教育ツールの評価指標

	MEEGA+	EGameFlow	RETAIN
評価対象	教育ゲーム （デジタル・アナログ）	e ラーニングゲーム	シリアルゲーム
指標	ARCS ユーザ体験 学習	フロー 動機づけ 学習	ARCS の R のみ ゲーム設計 学習（フロー，没入）
特徴	分類毎の相関等の分析	分類毎の相関等の分析	分類ごとの重み （専門家により決定）
評価方法	アンケート（5 段階）	アンケート（8 段階）	アンケート（1 - 3 点） 記述毎に該当する点数

成しており，教育ゲームとして必要な項目を網羅できている．特にプロジェクトマネジャー向けの教育ゲームの評価指標で使用されており，活用事例が多いことや統計的な手法を用いてアンケート項目の分類などについて分析していることから本稿でも MEEGA+ を 1 つの評価指標として活用することとした．

評価項目には MEEGA+ に加えて，目的の達成を確認するための独自アンケートを作成して使用した．アンケートの回答はすべて 5 段階評価で実施できるように作成している．また，自由記載形式で意見等を回答してもらい，定性的な分析を実施した．

- MEEGA+

  表 4.2 に MEEGA+ のアンケート項目の一覧を示す．文献 [38] では学習者の体験と学習効果の 2 つの分類となっている．学習者の体験の内容が ARCS 動機づけモデルに関連する内容とゲームデザインに関連する内容となっていたことからこれらを分割し，3 つの主分類（動機づけ効果，ゲームデザイン，学習効果）に大別し，評価を実施することとした．以上から MEEGA+ のアンケートで，学習者の動機づけ効果，ゲームデザイン，学習効果を確認する．3 つの主分類はさらに 14 つの項目に分類（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，エラー防止・回復，短時間学習効果，学習目標の達成度）されており，全 36 問の質問から構成される．なお，学習目標の項目は演習ツールに該当する内容を記

述する必要があるため，「サイバーセキュリティにおける利用者としての注意事項の理解に貢献した」に修正した．

- 独自のアンケート内容
  WebSec と既存のセキュリティ教育との比較を実施するために以下に示す 2 つの質問を回答してもらう．これにより，利用者として身につけておくべき知識を網羅的に学習することができ，既存のセキュリティ教育の代替または補完が可能であるか分析する．
  - ツールの活用：WebSec をあなたの所属組織のセキュリティ研修でも活用したいか？
  - 教育内容の合致：WebSec はあなたの所属組織のセキュリティ研修で教えたい（教えてもらった）内容と合致しているか？

レベル 2（学習）

学習者の学習到達度の評価を確認するため，以下の 2 つの手法により効果を測定した．

- 事前・事後テスト：演習前後で参加者の理解度を測定し，演習により理解度の変化を確認する．事前・事後テストではゲーム中に学習する 20 個の問題をランダムに選択した．ただし，事前・事後テストは同一の問題とした．
- ゲーム演習の進捗・正誤の記録：演習の進捗や正誤の記録を用いて参加者の理解度との関連性を調査する．

4.5.2 評価結果

前節の評価方法を用いた評価結果を以下に示す．

レベル 1（反応）

表 4.3 に MEEGA+ の結果を示す．平均 (Avg.) と標準偏差 (SV) をまとめている．相互作用，可用性，エラー防止と回復の分類は低い値になっているのは，関連する機能が実装されていないためである．標準偏差の値は 1 前後となっており，バ

表 4.2: MEEGA+ のアンケート内容

No.	分類	アンケート内容
動機づけ効果		
1		ゲームの始めに注意を引く面白いことがあった.
2	注意	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		自分にとって適切なレベルの課題であった.
7	挑戦	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		ゲーム中に他のプレイヤーと対話することができた.
10	相互作用	ゲームはプレイヤー間の協力または競争を促した.
11		ゲーム中に他プレイヤー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		ゲームの内容はあなたの興味に関係していた.
15	関連性	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		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	満足	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.
ゲームデザイン		
22	美的感覚	ゲームデザインは魅力的だった（インターフェイス，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		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	学習可能性	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		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	可用性	ゲームで使用される色は意味があったと感じた.
31		このゲームでは好みに応じて外観（フォントや色）をカスタマイズできた.（デジタルのみ）
32	エラー防止	このゲームはあなたの間違った操作を防いでくれた.（デジタルのみ）
33	と回復	あなたが間違った操作した際に容易に回復することができた.（デジタルのみ）
学習効果		
34	短時間学習	このゲームはあなたの学びに貢献した.
35		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.
36	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.

ラツキが小さいことがわかる．

各分類を定量的に比較し，事前知識による結果の差異を分析するため，事前テストの結果上位グループ（8 名）と下位グループ（8 名）の結果をグラフにより比較する．グラフでは分類ごとの各項目を平均した値を比較している．

図 4.6 に MEEGA+ の動機づけ効果の結果を示す．上位グループと下位グループの結果を比較するとすべての項目で下位グループの値が高くなっていることがわかる．今回の演習ではコンテンツが利用者向けの内容になっており，上位グループの参加者にとっては既知の内容が多かったため，動機づけ効果が低くなったものと考えられる．相互作用の項目が他項目に比べて低い値になっているのは WebSec では参加者間に相互作用を与える機能を実装していなかったためである．

図 4.7 に MEEGA+ のゲームデザインの結果を示す．ゲームデザインについては実施可能性を除くすべての項目で下位グループの方が値が高くなっていることがわかった．上位グループは下位グループに比べて動機づけが得られなかったため，否定的な感情により値を低く評価された可能性がある．実施可能性の値が高かったのは，上位グループにとって難易度が低かったため，容易にゲームを進捗することができたためと考えられる．

図 4.8 に MEEGA+ の学習効果の結果を示す．学習効果も動機づけ効果およびゲームデザインの評価と同様に下位グループの方がツールの評価が高くなっている．以上のことから，参加者の知識に基づき，適切なレベルのコンテンツを学習できれば，動機づけ効果を与え，高い学習効果が期待できる．

図 4.9 に独自の質問内容の結果を示す．ツールの活用については学習者の好みが別れる結果になった．アンケートの定性的な分析を実施した結果，否定的な回答をした参加者の多くはツールの操作性に不満を持っていることがわかった．操作性を改善することで，ツールを活用したい参加者が増える可能性がある．教育内容の合致については，合致していると回答する参加者が多かった．これは WebSec がセキュリティ教育で実施されている知識を網羅的に包含できているためと考えられる．

表 4.3: MEEGA+ のアンケート結果

No.	分類	Avg.	SV	No.	分類	Avg.	SV
動機づけ効果							
1		3.31	1.10	12	自信	3.25	0.97
2	注意	3.19	1.24	13		3.50	1.06
3		3.56	1.17	14		3.56	1.17
4	面白さ	3.56	1.27	15	関連性	3.69	1.21
5		3.13	1.36	16		3.06	1.25
6		4.00	1.12	17		3.31	1.26
7	挑戦	3.25	1.35	18		2.94	1.25
8		2.31	1.16	19	満足	3.00	1.12
9		1.38	0.78	20		3.44	1.00
10	相互作用	1.75	0.97	21		2.94	1.39
11		1.31	0.59				
ゲームデザイン							
22	美的感覚	3.25	1.39	29		3.50	1.12
23		3.25	1.30	30	可用性	2.75	1.15
24		2.63	1.41	31		1.69	1.16
25	学習可能性	3.50	1.12	32	エラー防止	1.50	0.87
26		3.25	1.03	33	と回復	1.81	1.01
27	実施可能性	4.25	0.75				
28		3.56	1.37				
学習効果							
34	短時間学習	3.75	1.15	36	学習目標	3.75	0.90
35		3.44	1.12				

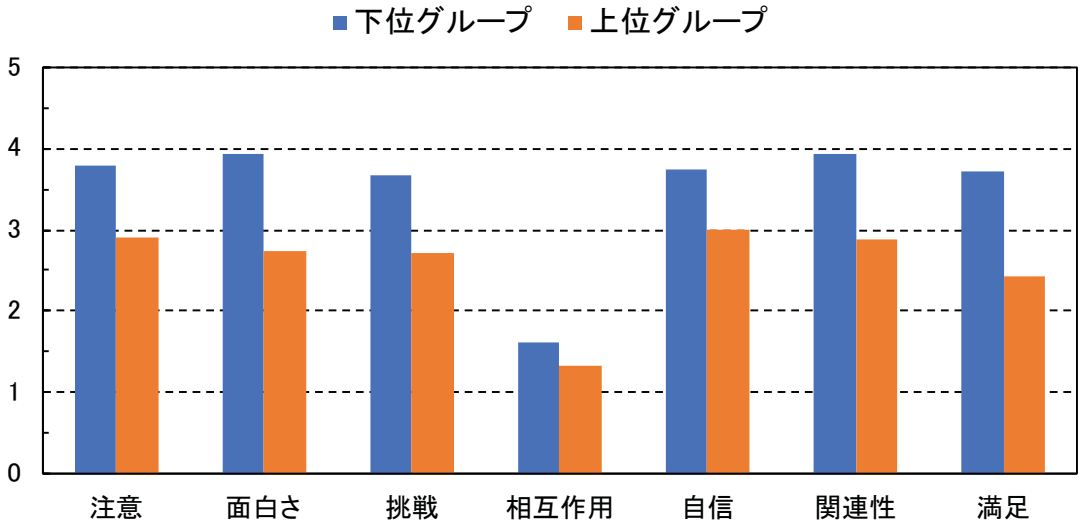


図 4.6: 動機づけ効果の結果（MEEGA+）

レベル 2（学習）

ここでは，事前・事後テストの結果の比較とゲーム演習の進捗・正誤の記録の結果をまとめた．

- 事前・事後テスト
  図 4.10 に事前テストと事後テストの結果を示す．事後テストは事前テストよりも平均点が 7.63 点も向上しており，知識の定着が図れたものと考えられる．図 4.11 に事前テストと事後テストの各問題ごとの結果を示す．問題 1〜11 は演習中に比較的学習できた問題である．学習者によっては事前・事後テストに関連する知識の学習まで至っていない者もおり，学習ができた問題に限ってみるとさらなる向上が確認できていることがわかる．
- ゲーム演習の進捗・正誤の記録
  図 4.12 に学習の進捗を示す．114 問の問題があり，正解数と不正解数を確認することで進捗を確認することができる．出現する問題は最初の問題のみが固定で他の問題は学習者が学習した知識項目に基づき，提示される．最初の問題で正解・不正解数が多くなっているのは，WebSec の操作方法に慣れ

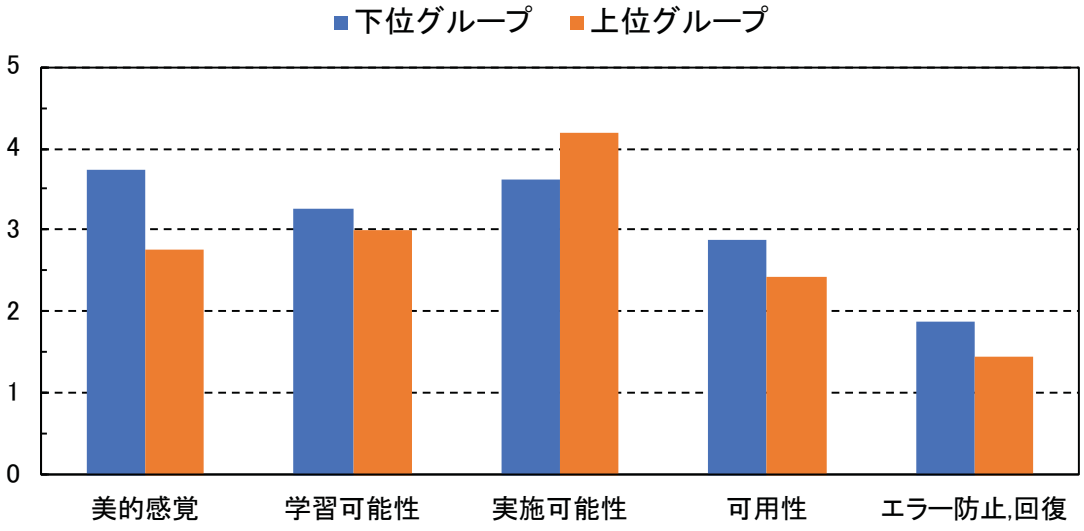


図 4.7: ゲームデザインの結果（MEEGA+）

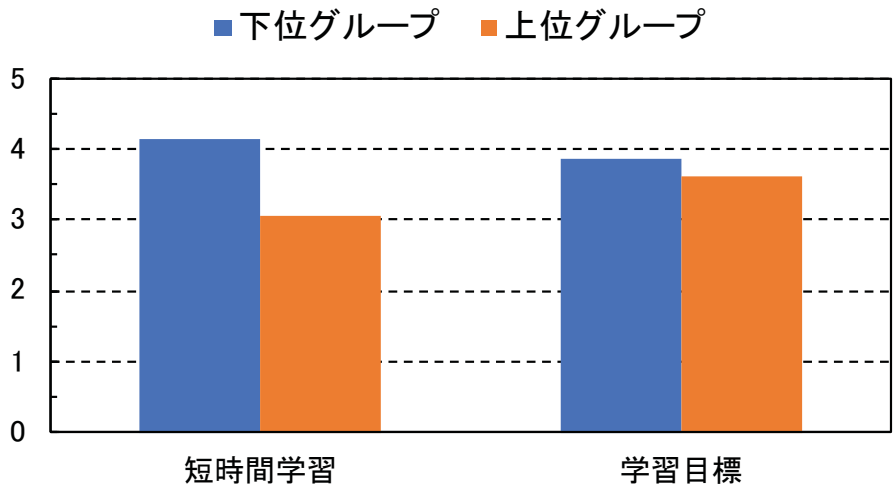
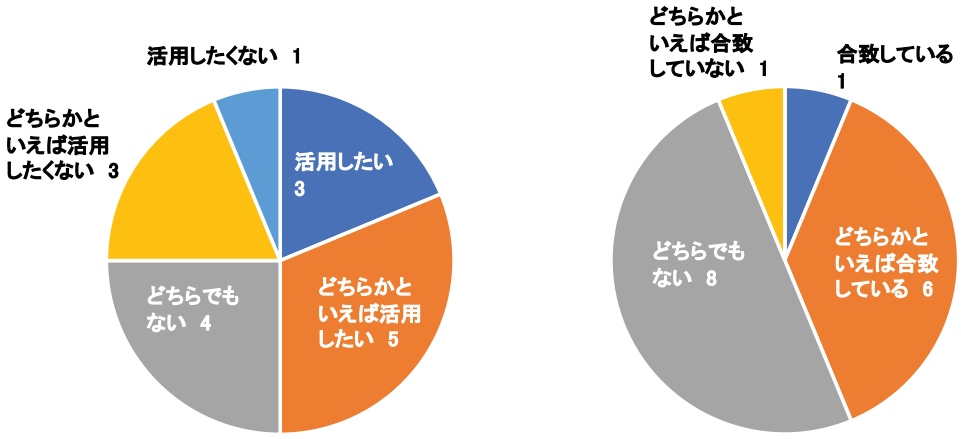


図 4.8: 学習効果の結果（MEEGA+）

ていなかったためと考えられる．約 90 分間の演習であったが，多くの問題が確認されていることがわかる．また，不正解数が多かった問題は難易度が高い問題であるか，問題文または解答に不具合があると考えられる．このため，問題文や解答を見直すとともに，問題の難易度にラベルを付け直す必要



(a) ツールの活用　　(b) 教育内容の合致

図 4.9: 独自アンケートの結果 ($n = 16$)

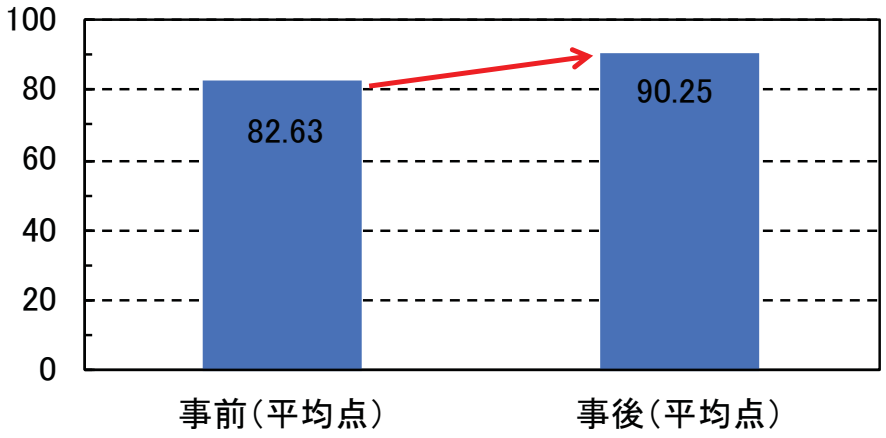


図 4.10: 事前・事後テストの結果

がある．

図 4.13 に事前テストの結果と参加者の進捗（問題の正答数）の散布図を示す．事前テストの結果と参加者の進捗の相関を計算すると $r = 0.58$ で中程度の正の相関が確認された．学習者の進捗をモニタすることで進捗速度に応じて学習者の知識レベルを把握することができる可能性がある．学習の進捗

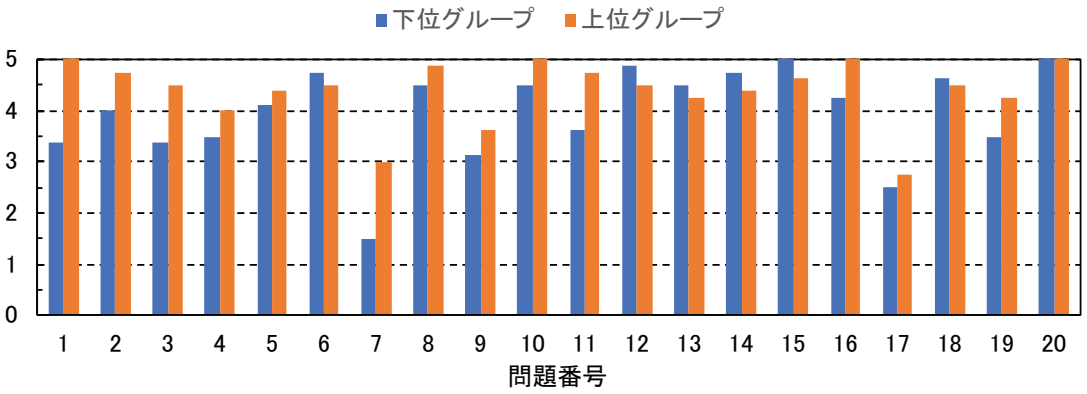


図 4.11: 事前・事後テストの結果 （細部）

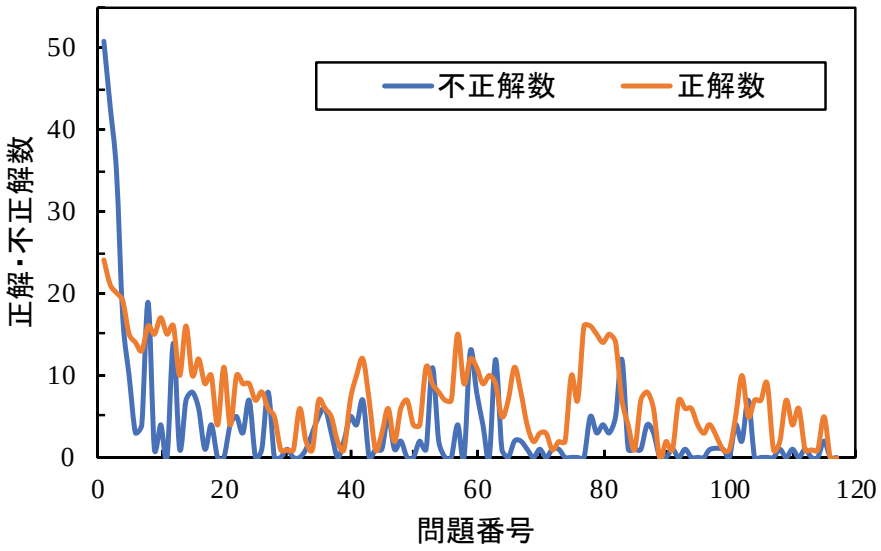


図 4.12: 学習の進捗

をシステムでモニタすることで学習者の知識レベルを判断し，学習者に知識レベルに合致する難易度の問題を提供することができる可能性がある．

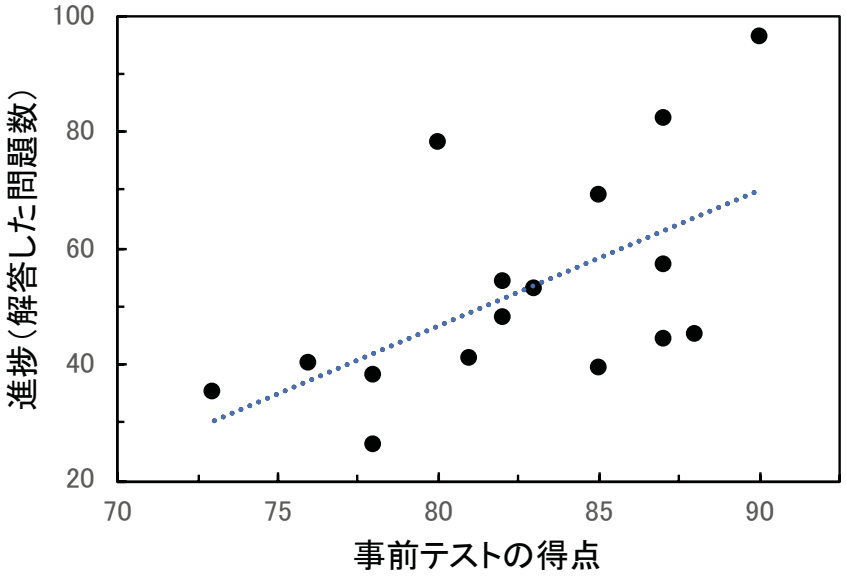


図 4.13: 事前テストと学習の進捗の散布図

4.6　改善：定性的分析結果に基づくアプリケーションの改善

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他に自由記載形式で意見を記載してもらった．以下に定性的分析から改善すべき内容をまとめた．

意見 1:操作要領をわかるようにしてほしい．

改善 1:ゲーム内に操作方法や表示画面を説明する画面を追加する．

意見 2:ゲームを記録し，途中から始められる機能を追加してほしい．

改善 2:ゲームの記憶機能を追加する．

意見 3:項目が多く，知識の確認画面が見難い．

改善 3:知識の分類ごとに異なる知識確認画面を作成する．

意見 4:フリーテキストを入力して解答する問題でエンターキーに反応し，解答が提出されてしまった．

改善 4:提出ボタンの選択で解答するように修正する．

表 4.4: アンケート内容と結果 ($n = 33$)

項目	質問	Avg.	SD
注意	このゲームはおもしろかったですか？	4.60	0.83
関連性	あなたにも関係がある内容でしたか？	4.15	1.03
自信	インターネット利用時の注意事項がわかりましたか？	4.70	0.73
満足	やれてよかったですか？	4.76	0.56

4.7 その他のユースケース

WebSec のコンテンツを小学生向けのアレンジし，奈良先端科学技術大学院大学のオープンキャンパス（H30.11.11(日) 10:00 - 15:00 実施）で来場者に体験してもらった．コンテンツは内閣府の「青少年のインターネット利用環境実態調査」の結果 [41] を受けて，ゲーム，動画視聴，情報検索，コミュニケーションに焦点を当てている．コンテンツの細部はシマンテック社 [42] およびトレンドマイクロ社 [43] の資料を参照し，インターネットの正しい利用方法を学習できる内容となっている．

WebSec 体験後に ARCS 動機づけモデル [9] の各項目に関連する簡単なアンケートに回答してもらうことで，効果を確認した．アンケートの回答者数は 33 人で幼稚園生から成人まで含まれるが，多くの参加者は小学生であった．また，アンケートは 5 段階評価で回答してもらっている．表 4.4 にアンケート内容と結果を示す．ARCS の注意，自信，満足に該当する 3 つの質問の結果は非常に高い値になっていることがわかる．関連性は他の項目に比べると若干，低い値になっている．これは，参加者によってはインターネットで学習コンテンツに該当する行為を行なった経験がなかったためと考えられる．簡単なアンケートではあるが，動機づけ効果を確認できた．以上から，コンテンツの入れ替えのみで，WebSec を多くのケースで活用できるものと考えられる．

4.8　4 章のまとめ

本稿では，教授設計モデルの ADDIE モデルに従って組織へのセキュリティ教育のためのゲーム演習ツールを開発し，評価を行った．演習ツールは利用者向けの学習コンテンツを用いた演習後に参加者の反応を評価するため，MEEGA+ と呼ばれる指標を活用してアンケートを回答してもらった．アンケート結果を分析することで，学習コンテンツに関する知識を十分に備えていない参加者の評価が高く，コンテンツの内容が学習者のレベルに合っている場合は有効であることがわかった．独自のアンケートにより，WebSec は好みが分かれるがセキュリティ研修の代替ツールとなる可能性と学習内容の網羅性を満たしていることを確認した．また，学習到達度については事前・事後テストの結果を確認することで知識の習得ができていることがわかった．ゲーム演習の参加者の進捗と事前テストの結果からゲームの進捗速度をモニタすることで学習者の知識レベルを推定できる可能性を示した．WebSec のコンテンツを小学生向けに修正し，ユーザ評価をしたところ，動機づけ効果で良好な結果を得ることができた．コンテンツを対象や利用状況に応じて最適なものに変更することで，多くの場面で活用できる可能性を示すことができた．以上から，本章のはじめに示した WebSec の目的は学習者の知識レベルに応じて適切なコンテンツを提供した場合に達成できたとものと考える．

本章の制約事項としては，学習者コンテンツは利用者を対象としたもの（レベル 1）のみを評価しており，レベル 2 および 3 のコンテンツを用いた場合の評価は実施していない．今後の課題はシステム的に学習者の知識レベルを判断し，適切なレベルの学習コンテンツを提供できるようにすることが挙げられる．これにより参加者の知識量に依存せず，高い学習効果が期待できるものと考えられる．また，レベル 2，3 のコンテンツを用いた演習を実施し，他のレベルでも WebSec が活用できることを確認する必要がある．

第 5 章　IoT・ポリー

本章では 2 つ目の提案するゲーム演習ツールである IoT・ポリーについてまとめる．IoT・ポリーの目的は動機づけを与えることに加えて，リスクアセスメントのプロセスの概要を理解すること，IoT システムへの脅威と対策の知識を獲得することである．

5.1　分析：教育コンテンツ

昨今，IoT システムへのサイバー攻撃が増加している．情報処理推進機構（IPA）が公表している情報セキュリティ 10 大脅威 2018 年版 [5] では「個人」向けの脅威の第 9 位に「IoT 機器の不適切な管理」，「組織」向け脅威の第 7 位に「IoT 機器の脆弱性の顕在化」がランクインした．IoT システムは IT システムと比べて，システム毎に特徴が大きく異なっており，IoT システム毎の考慮すべき脅威の対象や脅威への対策方法もその特徴を考慮する必要がある．このため，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 [44, 45]．現状，脅威の洗い出しのためのゲーム演習ツールとして EoP が存在するが，リスクアセスメントのプロセスを体験できるゲーム演習ツールは存在しない．上記から IoT・ポリーではリスクアセスメントのプロセスを体験するとともに，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する．

3 章の関連研究で示した EoP はリスクアセスメントの脅威の洗い出しをゲーム化した内容となっている．EoP のカード内容は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未知の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．このため，EoP は非常に高度な知識を持っている学習者向けのゲーム演習ツールであると言える．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する必要がある．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する必要がある．

図 5.1 にサイバー攻撃の脅威をまとめたツールとその抽象度の関係を示す．脅威の抽象度が高いツールを使用した場合，未知の攻撃を発見できる可能性があるが，上級者向けである．最も抽象度が高い STRIDE は EoP のカード内で用いられている．本稿ではより具体的な脅威を学習者の知識として獲得させることを目的としているため，図 5.1 で黄色いハイライトをつけた攻撃ライブラリを活用する．IoT・ポリーでは，攻撃の仕組みに着目し幅広い攻撃手法を定義していることから CAPEC を用いることとした．CAPEC は 2 種類の方法で攻撃手法を分類（仕組みによる分類と領域による分類）している．領域による分類ではメタ抽象化の項目を 6 つの分類にクラス分けしている．仕組みによる分類ではメタ抽象化の項目を 9 つの分類にクラス分けし，さらに攻撃手法を標準抽象化（159 個の手法）と詳細抽象化（299 個の手法）に詳細化している．

リスクアセスメント内の一つのプロセスであるリスク分析ではリスク値を定量化し，低減策を講じることで許容値までリスクを低減させる．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，IoT 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．リスク値の算定に用いられる代表的なものとして CVSS[46] や NIST SP800-30[47] などがある．IoT・ポリーでは特定のリスク値算定手法を使用せず，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．また，想定されるリスクから低減策を講じたとしてもリスクが残留するため，残留リスクを明らかにする必要がある．残留リスクを分析し，追加の対策を検討するプロセスは，IoT・ポリーにも組み込んだ．

5.2　設計：リスクアセスメントの簡易モデル

IoT・ポリーでは，ゲームによりリスクアセスメントのプロセスを体験させ，様々な IoT における脅威と対策を議論を通して獲得させる．従来，OT システムのリスクアセスメントは安全性（セーフティ）を確保するために実施されている [48]．文献 [48] ではソフトウェアのセーフティに関連するリスクアセスメントのプロセスとリスク分析の手法が詳述されている．サイバー攻撃へのリスクアセスメントのアプローチは上記の手法と基本的には同じである．このようなリスクアセスメントのプ

ツール	概　要
STRIDE	6つに分類(S:なりすまし, T改ざん, R:否認, I:情報漏洩, D:サービス不能, E:特権昇格)により脅威の連想するためのもの
OWASP Top 10	OWASPによって公開されている脆弱性のトップ10
10大脅威	流行りの脅威をランキング化したもの
文献レビュー	セキュリティベンダーのレポートなどから脅威を分析すること
攻撃ライブラリ	システムの脅威を効率的に発見するために具体的な手法をまとめたツール

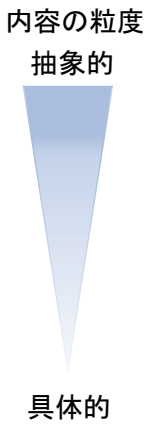


図 5.1: サイバー攻撃の脅威をまとめたツールとその抽象度の関係

ロセスは様々な文献においてモデル化されている [49, 50]．本稿ではこのうち，リスク合理化プロセス [49] および ICS リスクアセスメントのモデル [50] を参考にし，より平易な 3 つのプロセスとなるように簡単化した．リスク合理化プロセスは特定の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，汎用性があるモデルである．ICS リスクアセスメントのモデルは 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簡易モデルでは汎用性があるモデルと特定の OT のモデルを包含し，様々な IoT システムのリスクアセスメントでも適用できるようにした．図 5.2 に IoT・ポリーの 3 つのプロセスとリスク合理化プロセス，ICS リスクアセスメントのモデルの対応を示す．また，以下に平易化した 3 つのプロセスを示す．

- 状況付与：IoT システムの特徴をカードと簡易なシステム構成図で表現し，脅威カードとプレイヤー間の議論により，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毎の議論に焦点を絞るため，プレイヤーにアタックサーフェスカードを選択させる．
- 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毎の脅威を順位付けする．議論の焦点を絞り，プレイヤーの選択肢を制限するため，事前にプレイヤーに配布する脅威カードの枚数を制限する．プレイヤー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

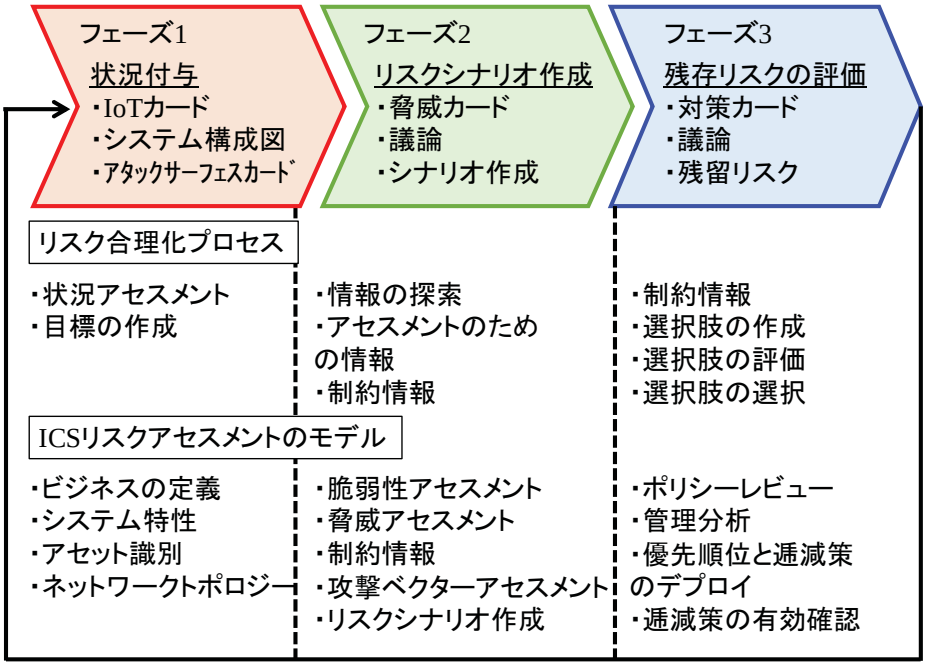


図 5.2: IoT・ポリーとリスクアセスメントプロセスの関係

カードを選択し，提示する．それぞれのプレイヤーが提示した脅威カードと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．

- 残存リスクの評価：プレイヤー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ーに配布することで，プレイヤーの検討する範囲を制限する．プレイヤー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ーが提示した対策カードの効果順に順位付けする．また，プレイヤー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．

5.3 開発：演習ルールと演習資材

開発のプロセスでは，演習ルールと演習資材を作成した．本節ではルールと演習資材の細部について示す．

5.3.1 演習ルール

ルールおよび進行は以下のとおりである．

1. プレイヤー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ー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，ゲームのプレイヤー数は最大で 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，プレイヤー間で相談し，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，プレイヤー間の議論により以降の議論で焦点となる特性（IoT カード内に記載）の優先順位を決定する．
4. 任意のプレイヤー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. プレイヤーは，提示されたアタックサーフェスカード，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. プレイヤー間の議論により，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. プレイヤーは記載された 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. プレイヤー間の議論により，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. プレイヤー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を講じても残留する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．

5.3.2 演習資材

本項では演習で使用する資材についてまとめる．演習資材としてカード，IoT システムのシステム構成図，ワークシート，脅威の詳細リストを作成した．

カード

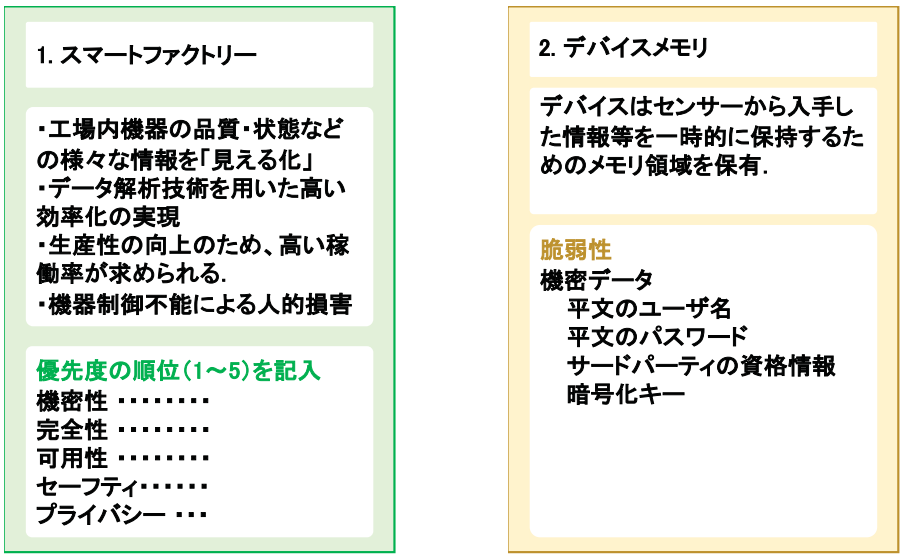
以下にカードの種類と概要を示す．

- 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有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 システム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 18 個のアタックサーフェスをカード化した [51].
- 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 CAPEC[34] 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[52] 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 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 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．

図 5.3 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ー間の議論の中で決定し，プレイヤーが記載する．アタックサーフェスカードはサーフェス名，概要，サーフェスが含む脆弱性を記載した．プレイヤーは脆弱性の内容から脅威を連想することができる．

図 5.4 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



(a) IoT カード　　(b) サーフェスカード

図 5.3: IoT カードとアタックサーフェスカード

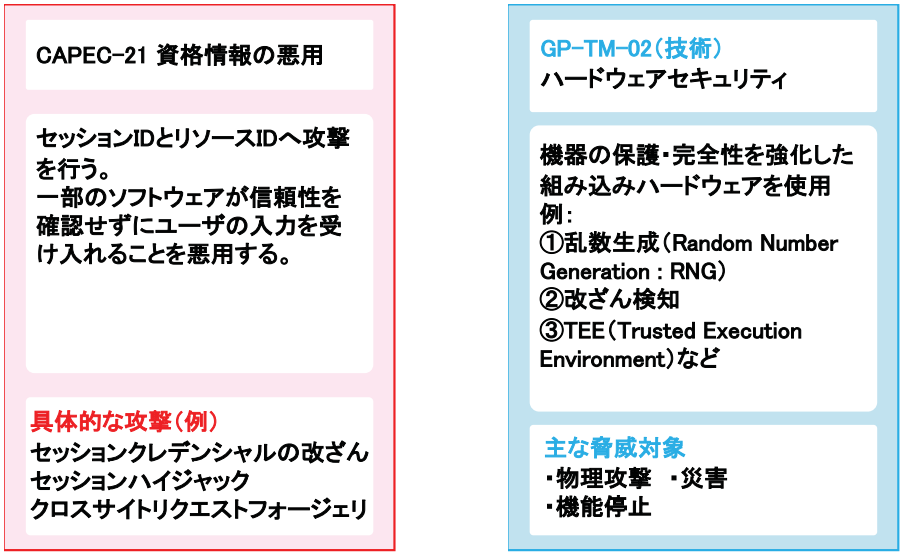
た．具体的な攻撃手法には CAPEC 標準化に該当する攻撃手法の名称を記載した．脅威カードとは別に具体的な攻撃手法のリストをまとめたリストを作成し，必要に応じ，プレイヤーが閲覧できるようにした．これにより，脅威カードを補完し，カードの情報だけで具体的な攻撃手法の連想が困難なプレイヤーを補助できるようにした．対策カードは対策名とその概要及び主な脅威対象を記載した．主な脅威対象を記載することで，プレイヤーがリスクシナリオに対応する対策カードを提示する際にヒントとすることができる．

IoT システムのシステム構成図

IoT カードに記載された IoT システムの構成は簡易化したシステム構成図としてまとめた．

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，プレイヤー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，



(a) 脅威カード　　(b) 対策カード

図 5.4: 脅威カードと対策カード

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 システムの特徴を踏まえ，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：任意のプレイヤー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：プレイヤーが提出した脅威カードを深刻度と提出者がわ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：プレイヤーが提出した対策カードを効果の順位と提出者がわかるように記載する．
- 残留リスクの許容可否：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．

脅威の詳細リスト

IoT・ポリーでは CAPEC を用いて IoT 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ー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．表 5.1 は作成した詳細リストの一部抜粋である．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わかるように作成した．プレイヤー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．

5.4　実施：3 回のゲーム演習の実施

IoT・ポリーの目的の達成度を確認するため，3 回の演習を実施した．演習は SecCap[37] および ICS-CoE 中核人材育成プログラム [53] の受講生を対象として実施した．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ゲーム演習の対象としては適正である．表 5.2 に実施した演習の概要を示す．2 回目演習では参加者の人数が少なかったことから定性的な分析に留めている．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レジリエンス構成学研究室に所属する学生である．

5.5　評価：評価方法と評価結果

本節では，評価方法と評価結果をまとめた．

表 5.1: 攻撃手法の詳細リスト（一部抜粋）

CAPEC ID	タイトル	関連する攻撃手法	概要
212	機能の悪用		攻撃者はアプリケーションの正当な能力を悪用する．システムの機能は変更もされていないが，意図されていない方法で使用される．これは，特定の機能の過度な使用，機密データへのアクセスが可能な設計上の欠陥がある機能を活用することによって実現される．
2	アカウントロックアウトの誘導	機能の悪用	攻撃者は攻撃を阻止しようとするシステムのセキュリティ機能を利用し，正当なユーザへのサービス拒否攻撃を実行する．たとえば，一定回数の不正なログイン試行後にアカウントをロックするパスワード調整メカニズムの実装を悪用して正当なユーザのアカウントをロックすることができる．
50	パスワードリカバリの悪用	機能の悪用	攻撃者はパスワードの忘失からユーザが回復できるようにする機能を利用する．たとえば，システムは忘失からの回復に 1 つの質問のみ（例：母親の旧姓）使用する．特に攻撃者が正当なユーザを知っている場合は，この情報を知ることは容易である．
620	暗号化レベルの低下	機能の悪用	攻撃者は暗号化レベルを下げるよう強制し，暗号化されたデータに対する攻撃を成功させることができる．

5.5.1 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．また，上記とは別に自由記載形式で IoT・ポリーへの感想・意見を聴取した．以下に反応と学習の評価方法について示す．

表 5.2: 演習の概要（IoT・ポリー）

演習	実施日	対象	特記事項
1 回目	H30.9.15(金)	SecCap 受講生 16 名	
2 回目	H30.10.22(火)	ICS-CoE 受講生 5 名	定性的分析のみ
3 回目	H30.12.11(火)	ICS-CoE 受講生 6 名 + 留学生 6 名	英語コンテンツ

レベル 1（反応）

演習直後のアンケート調査を行い，参加者に演習ツールを評価してもらう．評価指標には WebSec で用いた MEEGA+[38] を使用する．MEEGA+ は表 4.2 からデジタルツールのみに使用できる 3 つの評価項目を除外した項目を用いる．すなわち，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．なお，学習目標の項目は演習ツールに該当する内容を記述する必要があるため，「リスクアセスメントの理解およびスキル向上に貢献した」に修正した．1 回目演習では 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の結果を比較した．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．

レベル 2（学習）

学習者の学習到達度を確認するため，参加者にコンテンツの理解度についてアンケートによる主観評価を実施してもらった．表 5.3 に理解度の確認に用いたアンケートの質問内容を示す．

5.5.2 評価結果（1 回目）

以下に第 1 回目演習の結果を示す．

表 5.3: コンテンツの理解度についてのアンケート内容

理解度の確認内容	質問内容
IoT システムの特徴	IoT カード，システム構成図を理解できたか
アタックサーフェスの特徴	アタックサーフェスカードを理解できたか
脅威の内容	脅威カードを理解できたか
対策の内容	対策カードを理解できたか

レベル 1（反応）

表 5.4 に MEEGA+ の評価結果を示す．IoT・ポリーの結果は他の 3 つのゲーム演習ツールと比較してもすべての項目で他ツールの最も高い値と同程度の値になっていることがわかる．

図 5.5 に MEEGA+ の動機づけ効果の結果を示す．MEEGA+ のそれぞれの項目の平均をグラフ化している．セキュ・ワンが総じて高い値になっていることがわかる．セキュ・ワンはゲーミフィケーション・フレームワークを適用し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．セキュ・ワン以外の既存演習ツールは IoT・ポリー同様，特定のプロセスをゲーム化した内容となっている．IoT・ポリーは既存の演習ツールと同程度以上の値となっていることから，既存ツールと同程度以上の動機づけ効果があるものと考えられる．

図 5.6 に MEEGA+ のゲームデザインの結果を示す．図 5.5 と同様に MEEGA+ のそれぞれの分類の平均をグラフ化している．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，ゲームデザインの改善プロセスが組織的に実施でき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・サイズ等のバランスが悪化してしまった可能性がある．IoT・ポリーは他演習ツールと比べても同程度の評価になっており，ゲームデザインにおいても優れた結果であることがわかる．

図 5.7 に MEEGA+ の学習効果の結果を示す．上記 2 つの結果と同様に

表 5.4: MEEGA+ のアンケート結果

		IoT・ポリー		セキュ・ワン		ツール X		ツール Y	
No.	分類	Avg.	SV	Avg.	SV	Avg.	SV	Avg.	SV
動機づけ効果									
1		3.44	1.00	3.69	0.92	3.25	0.97	2.69	0.85
2	注意	3.81	0.95	4.25	0.83	3.88	0.86	3.63	1.17
3		3.81	1.01	4.06	0.75	3.88	1.05	3.63	1.17
4	面白さ	4.06	0.83	4.38	0.78	4.13	0.86	3.56	1.12
5		3.38	1.05	4.25	0.75	3.50	0.79	3.25	1.15
6		3.56	0.93	3.81	1.01	3.56	0.93	2.69	1.16
7	挑戦	3.44	1.00	4.19	0.63	3.50	1.12	3.56	0.61
8		3.44	1.00	3.88	0.86	4.06	0.83	3.13	0.99
9		4.69	0.58	4.81	0.39	4.75	0.43	4.50	0.61
10	相互作用	4.19	1.01	4.69	0.46	4.06	1.03	4.00	0.94
11		4.19	0.73	4.13	0.78	3.88	0.86	3.31	1.16
12	自信	2.81	0.88	2.56	0.93	2.44	0.93	1.56	0.61
13		3.44	0.93	3.63	0.99	2.81	0.95	2.63	0.99
14		4.00	0.87	3.81	0.81	3.44	0.79	3.38	0.99
15	関連性	3.63	0.78	3.31	0.92	3.44	1.06	3.56	0.61
16		3.63	0.86	3.81	0.92	3.56	0.70	3.31	0.85
17		3.50	0.87	3.94	0.90	3.31	1.10	2.75	1.09
18		3.56	0.86	3.81	0.88	3.38	1.22	3.06	1.20
19	満足	3.56	0.79	3.69	0.77	3.38	0.86	2.94	1.09
20		3.69	0.77	3.75	0.75	3.56	0.79	3.38	0.86
21		3.31	1.10	3.44	1.00	3.44	0.79	2.56	1.06
ゲームデザイン									
22	美的感覚	3.63	0.99	3.31	1.04	3.69	1.04	2.88	1.22
23		3.69	0.98	3.06	0.97	4.00	0.79	3.06	0.97
24		3.69	0.85	4.06	0.75	4.06	0.83	4.44	0.70
25	学習可能性	3.13	1.17	3.13	0.99	3.25	1.25	2.19	1.07
26		3.25	1.03	2.81	0.88	2.69	0.77	2.19	1.01
27	実施可能性	3.69	1.16	3.31	1.31	3.19	1.33	1.88	0.99
28		3.69	1.04	3.25	1.31	3.06	1.30	2.00	1.22
29	可用性	3.94	1.14	3.75	1.20	4.25	1.09	3.25	1.20
30		3.50	1.22	2.94	1.20	3.63	1.11	3.13	1.36
学習効果									
34	短時間学習	3.81	0.73	4.00	0.71	3.81	0.81	3.63	0.70
35		3.75	0.75	3.88	0.86	3.44	0.93	3.00	1.00
36	学習目標	4.00	0.61	3.56	0.70	3.44	0.79	3.75	0.66

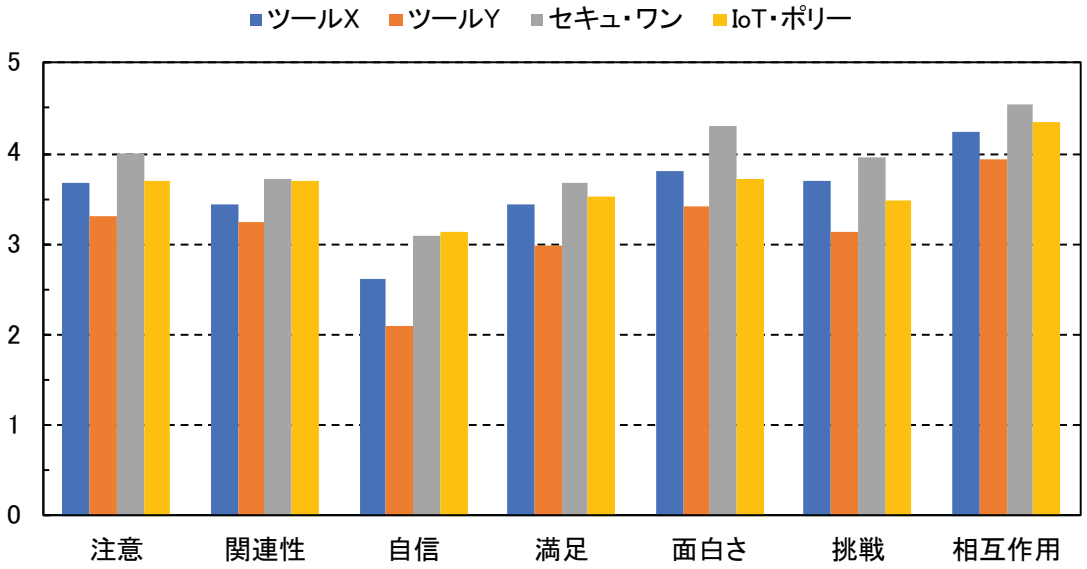


図 5.5: 動機づけ効果

MEEGA+ のそれぞれの分類の平均をグラフ化している．IoT・ポリーは他ツールに比べても高い値になっていることがわかる．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，高い学習効果を得ることができたものと考えられる．

レベル 2（学習）

図 5.8 に学習コンテンツの理解度を示す．平均の値をグラフ化している．アンケートによる参加者の主観評価ではあるが，各種コンテンツの内容を概ね理解することができていることがわかる．脅威カードと対策カードの理解度が他のコンテンツより低くなっているのはカード内の記載事項が多いためと考えられる．

5.5.3 評価結果（2 回目）

第 2 回目の演習では，それぞれのゲーム演習ツールごとに参加者の入れ替わりが発生したため，定量的なゲーム演習ツールの比較ができないと判断した．このため，自由記載形式によるコメントと演習後のヒアリングによる改善事項の分析に留

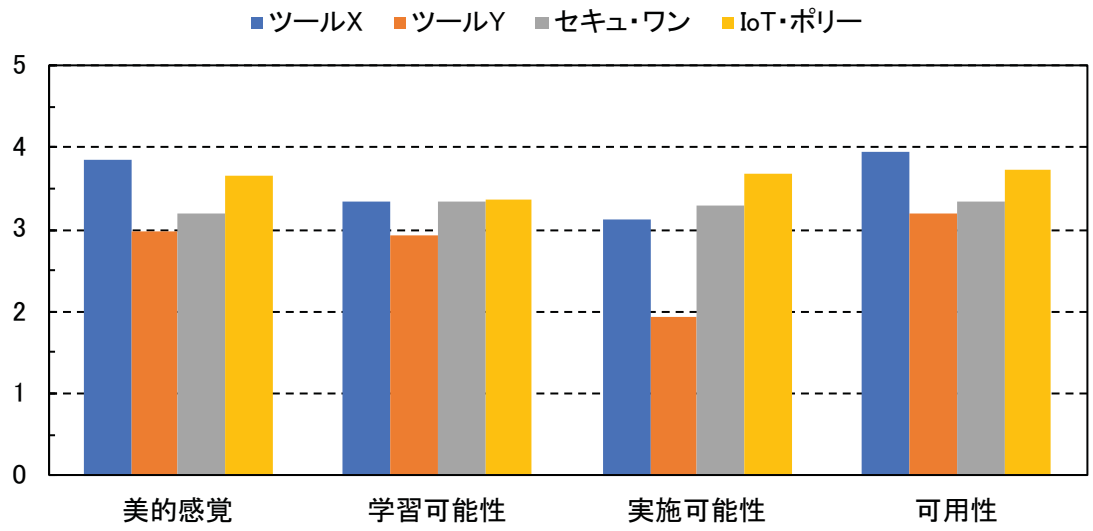


図 5.6: ゲームデザイン

めている．

5.5.4 評価結果（3 回目）

以下に第 3 回目演習の結果を示す．第 3 回目演習ではコンテンツを英語化し，演習を実施した．IoT・ポリーとセキュ・ワンの結果を比較した．また，第 1 回目演習と第 3 回目演習の結果を比較した．

レベル 1（反応）

表 5.5 に第 1 回目演習と第 3 回目演習の IoT・ポリーとセキュ・ワンの結果を示す．特に動機づけ効果の項目において，大きな改善があった．また，1 回目ではセキュ・ワンの方が評価が高かった項目のうち 3 回目で IoT・ポリーの評価が逆転した項目が複数あった．これは 1，2 回目のフィードバックを受け，ゲームルールの改善を図ったこと，コンテンツが英語だったこと，参加者が社会人およびセキュリティ研究に従事している留学生でありセキュリティ知識が高かったことが要因として考えられる．

図 5.9 に MEEGA+ 動機づけ効果の項目別平均値の結果を示す．セキュ・ワンと

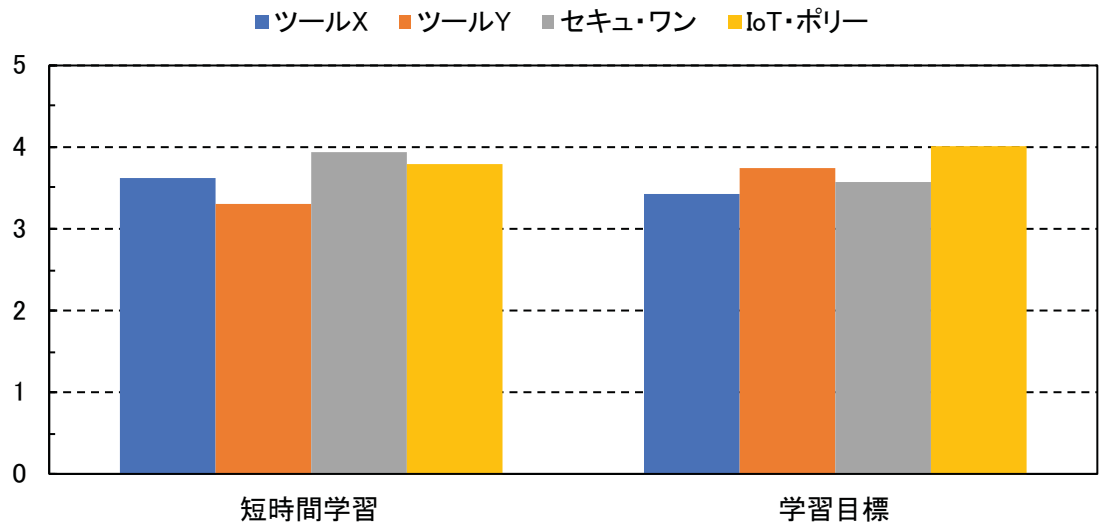


図 5.7: 学習効果

同程度の値になっていることがわかる．自信は他の項目と比較すると低い値になっている．演習終了後にプレイヤーの判断についてのフィードバックを与える仕組みを加えることで達成感と自信を与えることができるものと考える．システム的または人的な手段を活用し，フィードバックを与える仕組みを構築するのが課題と考えられる．

図 5.10 に MEEGA+ ゲームデザインの項目別平均値の結果を示す．セキュ・ワンと比べても同程度かそれ以上の値となっている．このことからセキュ・ワンよりもゲームデザインが優れていることがわかる．

図 5.11 に MEEGA+ 学習効果の項目別平均値の結果を示す．IoT・ポリーはセキュ・ワンに比べても同程度以上の値になっていることから高い学習効果を得ることができたものと考えられる．

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．

表 5.5: MEEGA+ のアンケート結果（第 1 回目と第 3 回目）

		IoT・ポリー				セキュ・ワン			
		1 回目		3 回目		1 回目		3 回目	
No.	分類	Avg.	SV	Avg.	SV	Avg.	SV	Avg.	SV
動機づけ効果									
1		3.44	1.00	4.17	0.55	3.69	0.92	4.08	0.86
2	注意	3.81	0.95	4.25	0.92	4.25	0.83	4.33	0.85
3		3.81	1.01	4.17	0.90	4.06	0.75	3.58	0.76
4	面白さ	4.06	0.83	4.33	1.03	4.38	0.78	4.75	0.43
5		3.38	1.05	4.08	0.76	4.25	0.75	4.42	0.64
6		3.56	0.93	3.92	0.64	3.81	1.01	3.83	0.80
7	挑戦	3.44	1.00	4.25	0.83	4.19	0.63	4.12	0.69
8		3.44	1.00	4.17	1.07	3.88	0.86	4.17	0.90
9		4.69	0.58	4.75	0.43	4.81	0.39	4.92	0.27
10	相互作用	4.19	1.01	4.75	0.60	4.69	0.46	4.42	0.76
11		4.19	0.73	4.50	0.76	4.13	0.78	4.50	0.50
12	自信	2.81	0.88	2.83	1.07	2.56	0.93	2.92	0.86
13		3.44	0.93	3.75	0.92	3.63	0.99	3.92	0.86
14		4.00	0.87	4.33	0.94	3.81	0.81	4.00	1.08
15	関連性	3.63	0.78	4.33	0.75	3.31	0.92	4.33	0.75
16		3.63	0.86	4.58	0.49	3.81	0.92	4.50	0.50
17		3.50	0.87	4.42	0.64	3.94	0.90	3.92	0.76
18		3.56	0.86	4.17	0.80	3.81	0.88	4.25	0.72
19	満足	3.56	0.79	3.83	0.90	3.69	0.77	4.00	0.71
20		3.69	0.77	4.33	0.94	3.75	0.75	4.25	0.60
21		3.31	1.10	4.08	1.11	3.44	1.00	4.33	0.75
ゲームデザイン									
22	美的感覚	3.63	0.99	4.00	1.00	3.31	1.04	3.75	0.92
23		3.69	0.98	3.83	1.14	3.06	0.97	3.83	0.99
24		3.69	0.85	3.75	0.83	4.06	0.75	3.33	1.18
25	学習可能性	3.13	1.17	3.25	1.09	3.13	0.99	3.50	0.87
26		3.25	1.03	3.33	1.03	2.81	0.88	3.83	1.07
27	実施可能性	3.69	1.16	3.42	1.11	3.31	1.31	3.33	0.85
28		3.69	1.04	3.92	0.86	3.25	1.31	3.83	1.21
29	可用性	3.94	1.14	3.00	1.29	3.75	1.20	3.00	1.41
30		3.50	1.22	4.08	0.86	2.94	1.20	3.33	1.11
学習効果									
34	短時間学習	3.81	0.73	4.33	0.75	4.00	0.71	4.25	0.60
35		3.75	0.75	4.42	0.49	3.88	0.86	3.92	0.76
36	学習目標	4.00	0.61	4.17	0.69	3.56	0.70	4.08	0.64

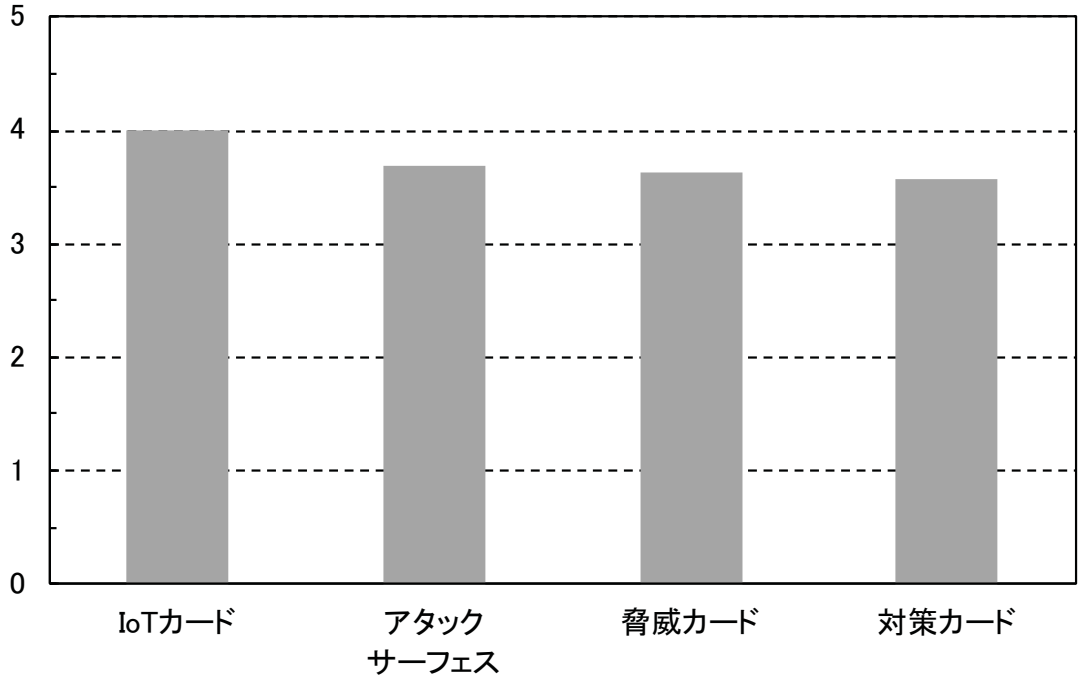


図 5.8: 学習コンテンツの理解度

レベル 2（学習）

図 5.12 に学習コンテンツの理解度を示す．第 1 回目演習に比べて総じて高い結果になっている．これは，演習参加者が社会人とセキュリティ研究に従事する留学生が含まれており，参加者の知識レベルが第 1 回目演習に比べて高かったためと考えられる．主観評価であるが，多くの参加者が学習コンテンツの内容を理解できており，IoT システムの脅威や対策などの知識を獲得する目的は達成することができたものと考える．しかし，ここでは理解度の確認を参加者の主観評価だけに頼っている．事前・事後テストや別の手段で参加者の知識向上を定量的に測り，知識の獲得を証明することが今後の課題と言える．

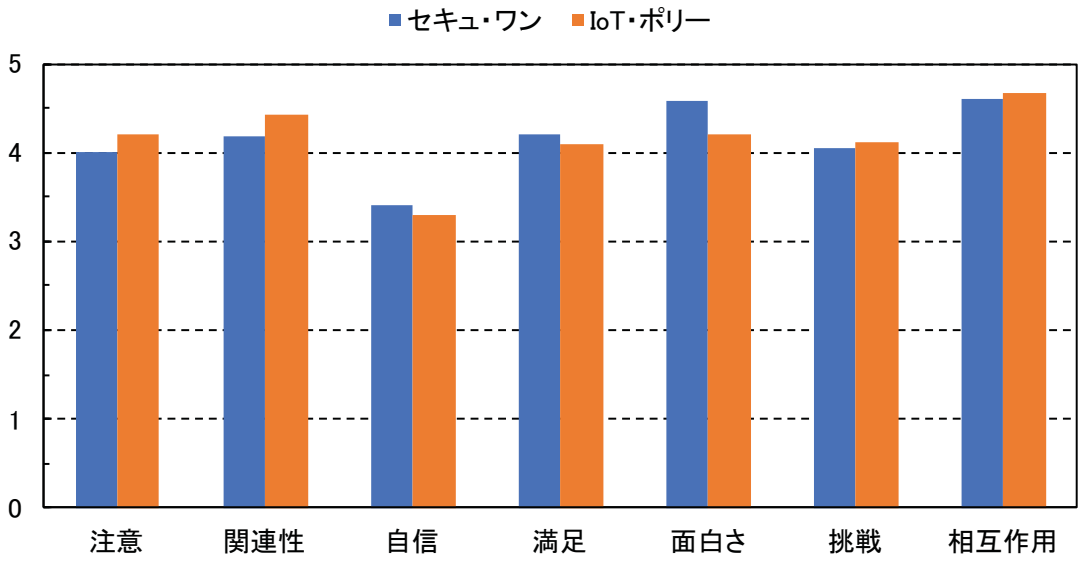


図 5.9: 動機づけ効果（3 回目演習）

5.6　改善：定性的な分析に基づくツールの改善

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他に自由記載形式で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．

5.6.1　1 回目

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．

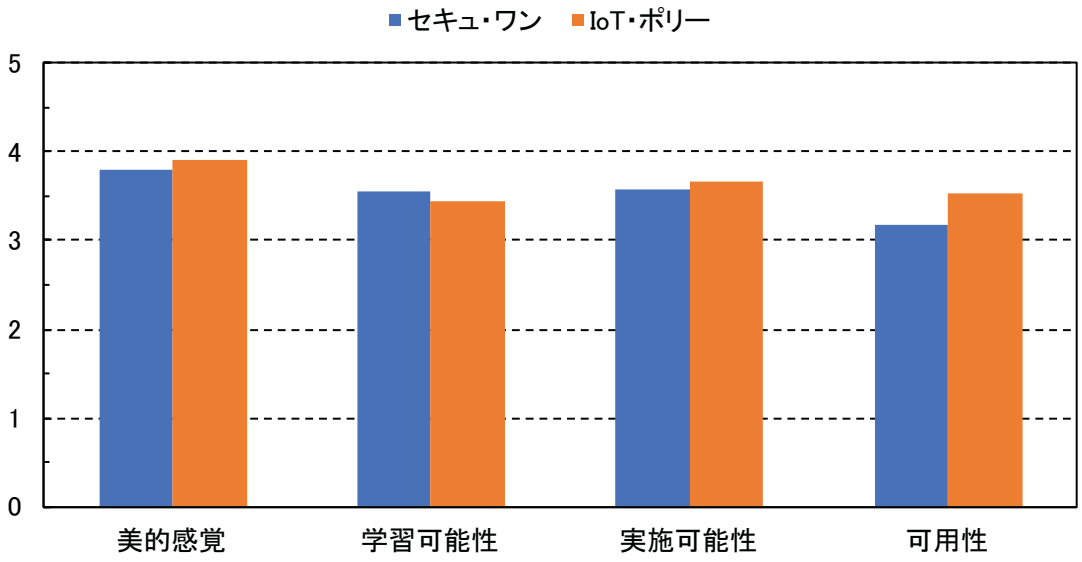


図 5.10: ゲームデザイン（3 回目演習）

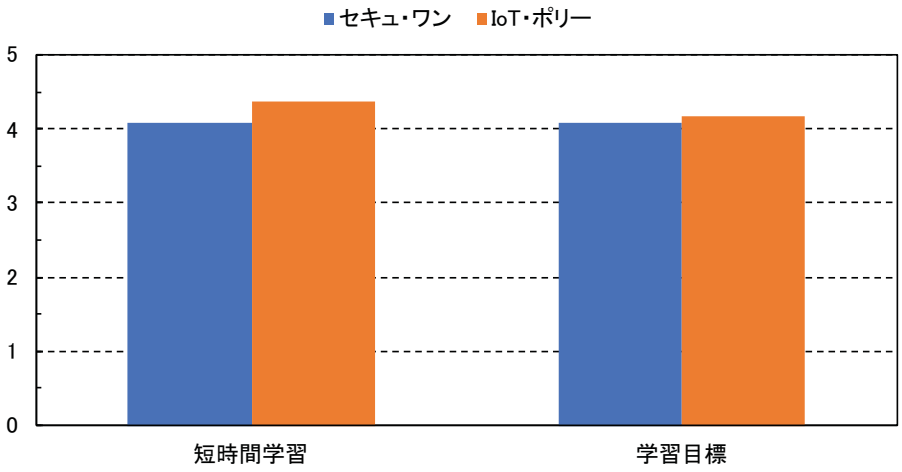


図 5.11: 学習効果（3 回目演習）

5.6.2　2 回目

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．

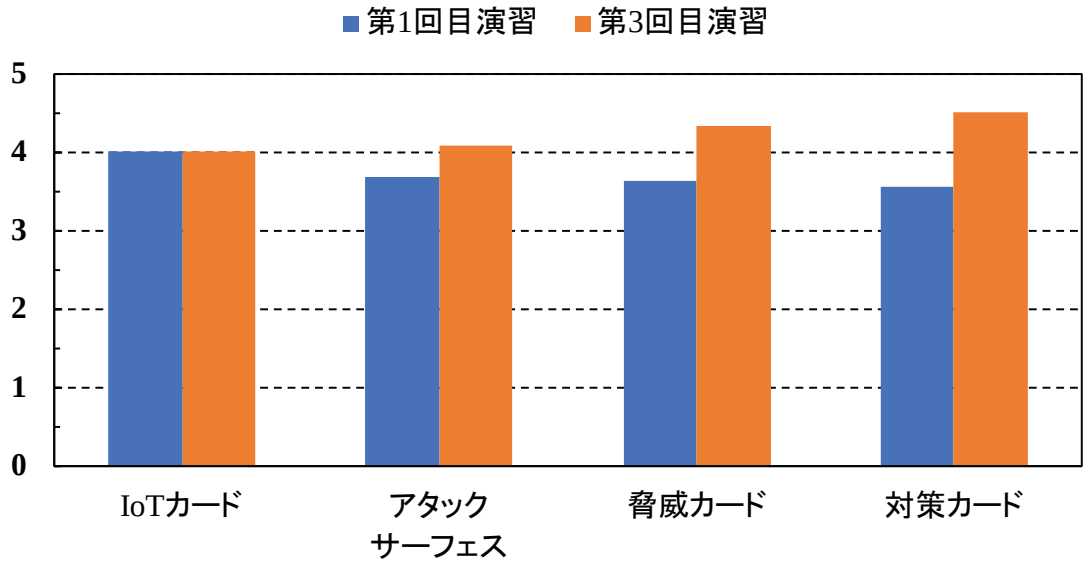


図 5.12: 学習コンテンツの理解度

意見 4:カード内の情報量が多い.

改善 4:不要な情報を除去した.

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明記）した.

3 回目演習では 1，2 回目の意見を反映したため，特に大きな改善意見はなかった.

5.7　5 章のまとめ

本章では，動機づけを与えること，リスクアセスメントのプロセスの概要を理解すること，IoT システムへの脅威と対策の知識を獲得することを目的に教授設計モデルの 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．ゲーム演習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 の特徴，アタックサーフェス，脅威，対策についての知識を獲得できるように設計した．実際の演習において IoT・ポリーを含む 4 つの演習を

実施し，参加者の反応を評価するため，同一指標（MEEGA+）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，他ツールと同等またはそれ以上の評価となっていることを確認した．以上から，動機づけ効果を与えることやリスクアセスメントのプロセスを理解させる目的が達成できたものと考える．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を分析することで，ゲーム内のコンテンツを通して必要な知識の獲得を確認した．今後の課題はさらなる評価の向上のため，参加者が選択したカードに対するフィードバックを与えることが挙げられる．選択されたカードの組み合わせ毎の模範解答を作成し，システム的または人的に参加者に提示する．また，理解度の確認を参加者の主観評価だけでなく別の側面から評価することも課題である．事前・事後テストや別の手段で参加者の知識向上を定量的に測り，知識の獲得を証明する必要がある．

第 6 章　セキュ・ワン

本章では既存演習ツールの未対応領域のうち，運用中の対策について重点的に議論できるゲーム演習ツールであるセキュ・ワンを提案する．セキュ・ワンは動機づけ効果に加えて，サイバーキルチェーン [54] の攻撃段階に応じた攻撃手法と効果的な対策に関する知識を獲得することを目的としている．また，演習中に取得したポイントにより，参加者の能力を定量的に測ることができるか検討を実施した．

6.1　分析：教育コンテンツ

第 3 章では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．セキュ・ワンにより既存の演習ツールの未対応領域である運用中の対策を十分に参加者間で議論させる．既存のゲーム演習はセキュリティ活動のプロセスをゲーム化しているものが多い．IoT・ポリーはリスクアセスメントのプロセスを簡易化したものをゲーム化している．IR ボードゲームはインシデント発生の対応プロセスをゲーム化している．システム運用中の対策を議論できる演習ツールが存在しなかった理由として，セキュリティ活動のプロセスをゲーム化することが困難であったためと考えられる．セキュ・ワンではセキュリティ活動のプロセス自体をゲーム化せず，ゲーミフィケーション・フレームワークを用いてゲームのルールを検討し，必要な知識（攻撃手法とシステム運用中の対策）を獲得できるようにする．企業への脅威のモデルにはサイバーキルチェーンの攻撃段階が用いられる場合が多い．このため，セキュ・ワンではサイバーキルチェーンの攻撃段階ごとの詳細な攻撃手法をまとめた攻撃ライブラリである ATT&CK [55] を活用することとした．ATT&CK の細部特徴は「攻撃カード内容の詳細」の項で示す．また，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挙げられる．上記のような対策は様々な組織・団体によりセキュリティ標準としてまとめられ，公開されている．セキュ・ワンではその中から，CSC [1] を活用することにした．CSC の細部特徴は「防御カード内容の詳細」の項で示す．攻撃手法と対策の知識（カード）

にインセンティブを設けることで，参加者の能力を定量的に測れるか検討を行った．

6.2 設計：システム設計とゲーミフィケーション・フレームワークへの適用

分析を踏まえ，以下にセキュ・ワンの設計要件をまとめた．

1. 学習者に動機づけ効果を与えるため，ゲーミフィケーションの仕組みを適用する．
2. 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．
3. 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．

設計要件を反映できるようにセキュ・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 [14] を適用した．

1. プレイヤーの分類：プレイヤー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，プレイヤーに加えてゲームマスターの役割を追加した．ゲームマスターはセキュリティ分野に知見を有する者が担当する．
2. 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に関する知識をプレイヤー間の議論により獲得する．
3. 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．
4. 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，プレイヤー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ーが，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．
5. ソーシャルアクション：プレイヤー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ーに理解させる．

6. プレイサイクルデザイン：初級者でもわかりやすいルールを設定し，ターン毎に手持ちの防御カード枚数が増減する仕組みとする．
7. 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，プレイヤー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．

6.3 開発：演習ルールと演習資材

設計を受け，演習を実施するためのルールとコンテンツを作成した．コンテンツの内容として攻撃・防御カードと判定基準表の細部について示す．

6.3.1 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ー 3〜6 名，防御カードの有効性を判断するゲームマスター 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 ターン毎のゲームの進行は以下のとおり．

1. 任意のプレイヤーがゲームのリーダーとなり攻撃カードセットから 1 枚カードを引き，全プレイヤーが閲覧できるように攻撃カードを提示する．
2. プレイヤー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. プレイヤーは提出した防御カードの攻撃への有効性を他プレイヤーに説明し，他プレイヤーから合意が得られた場合は得点を獲得する．
4. プレイヤー間で有効性の判断ができない場合はゲームマスター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ー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ー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ーがリーダーとなり 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ー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. 防御カードの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 6.1 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．図の説明には該当するゲーム進行の項番，ポイント加減算の項番，下記の説明に該当する項番がわかるように下線付き数字，アルファベット大小文字で表記している．

a. 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 点を取得する．
b. B は優先度の高い防御カードを 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. 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. 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．

プレイヤーは得点を取得するためには他プレイヤーおよびゲームマスターに提出

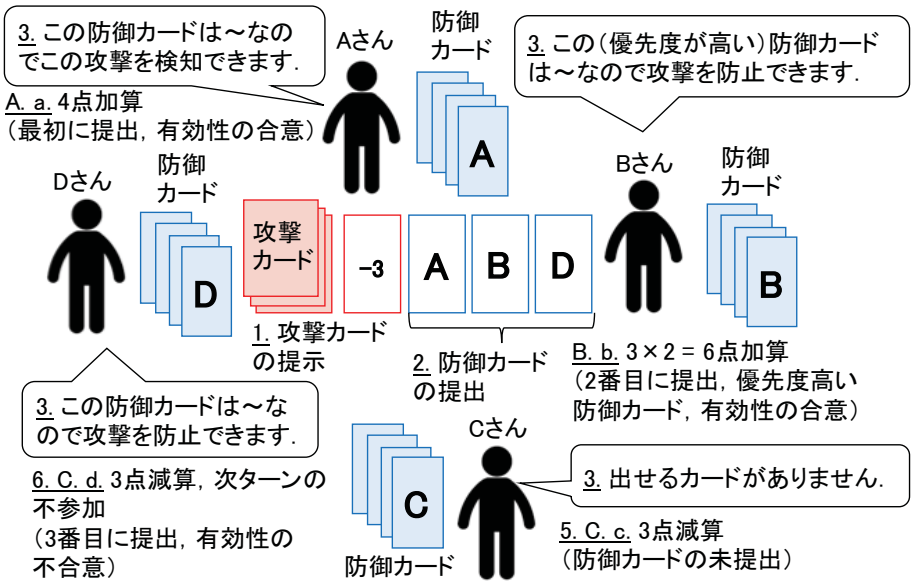


図 6.1: ゲームのターンのイメージ

した防御カードの有効性を説明する必要があり，他プレイヤーは説明内容に異議や補足を行うことができる．プレイヤー間で議論を誘発し，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．プレイヤー間の議論により，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 6.2 にプレイヤー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ーによる説明を他プレイヤー全員が理解し，合意した場合は有効であると判定される．他プレイヤーとの議論により，意見が割れた場合はゲームマスターの知見により有効性が判定される．ゲームマスター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ー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．

6.3.2 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 [54] 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

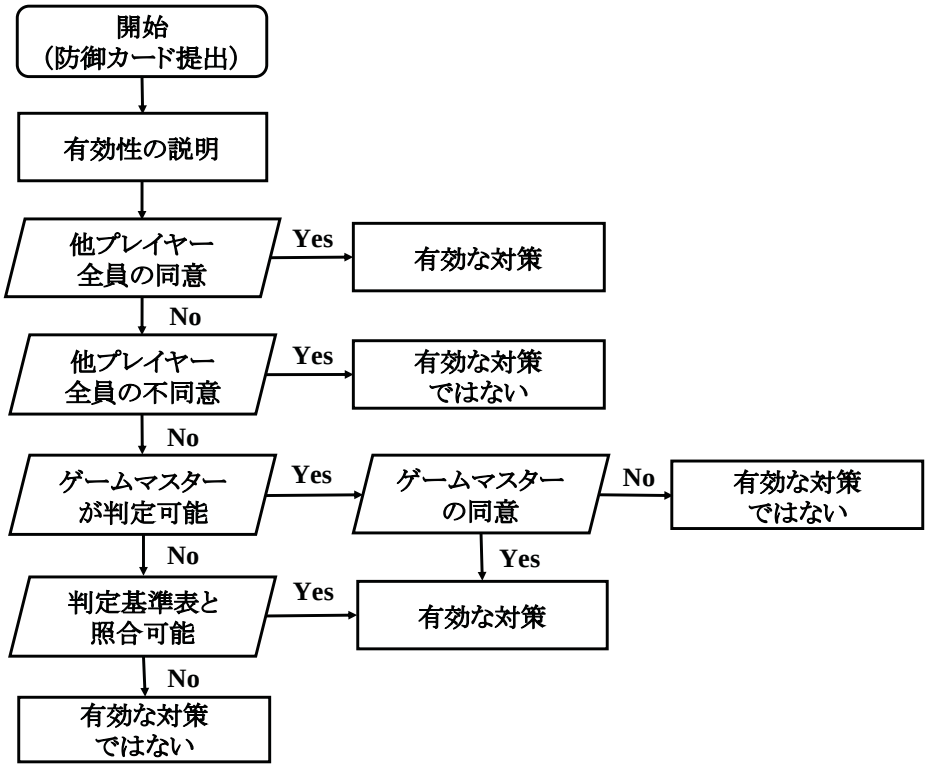


図 6.2: 判定フロー

Version 6.1 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．プレイヤーは手持ち防御カードから適切なカードを選択し易く，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 [56] 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 [57] 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[55] と CAPEC[34] を参照した．ATT&CK はサイバーキルチェーンの初期アクセス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 を活用した．ATT&CK の内容は都度，更新されており，2018 年 4 月に大きな変更として初期アクセスの項目が追加された．この変更に併せて，攻撃カードの配送段階にカードを追加した．その他，ATT&CK の修正に併せて攻撃カードの内容を更新し，最終的に合計で 81 枚のカードにまとめた．表 6.1 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わかるように 1 枚のカードにまとめた．

図 6.3 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．プレイヤー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．プレイヤー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ーに説明することで，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．プレイヤーの説明により攻撃カードが具体化され，プレイヤー間の議論により攻撃カードの解釈が深化されることで，各プレイヤーは詳細かつ分別された攻撃手法の理解が可能となる．

表 6.1: 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

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
	初期アクセス (ATT&CK)	7
初期侵害	実行 (ATT&CK)	3
	防衛回避 (ATT&CK)	11
誤用・特権昇格	権限昇格（ATT&CK）	6
内部偵察	資格情報アクセス（ATT&CK）	6
	発見（ATT&CK）	4
侵入拡大	侵入拡大（ATT&CK）	6
持続性確立	持続性（ATT&CK）	7
任務目的実行	収集 (ATT&CK)	5
	情報流出 (ATT&CK)	3
	遠隔操作 (ATT&CK)	11

6.3.3 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 Basic（CSC 1〜6），Foundational (CSC 7-16)，Organizational（CSC 17〜20）に分類され，管理策の優先順位がわかるようになっている．20 個の管理策はさらに 171 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 [58] およびシマンテック社 [59] 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

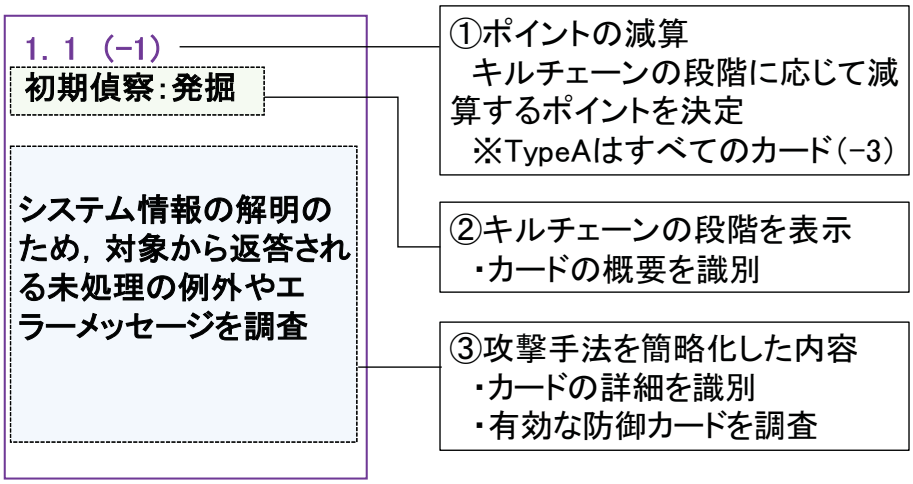


図 6.3: 攻撃カードのイメージ

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が得られる．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 6.2 に防御カードの内訳を示す．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発生後も考慮した内容となっている．CSC 18「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．CSC 10「データ復旧能力」のサブ管理策は防御段階の復旧，CSC 19「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，CSC 10 および CSC 19 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，その他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

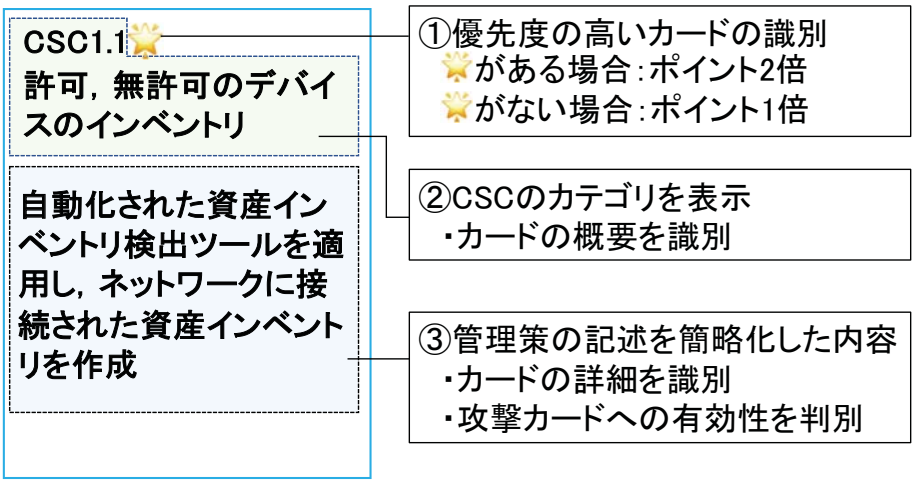


図 6.4: 防御カードのイメージ

きるものと考えられる．

図 6.4 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 1〜6 の防御カードを提出した場合はそれ以外の管理策 CSC 7〜20 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．プレイヤー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．

6.3.4 判定基準表

セキュ・ワンは知見を有するゲームマスターが重要である．知見を有するゲームマスター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，ゲームマスター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

表 6.2: 防御カードの内訳

番号	管理策	枚数
1	ハードウェア資産のインベントリと管理	8
2	ソフトウェア資産のインベントリ管理	10
3	継続的な脆弱性管理	7
4	管理者特権の管理された使用	9
5	ハードウェアとソフトウェアのセキュアな構成	5
6	監査ログの保守，監視，分析	8
7	電子メールと Web ブラウザの保護	10
8	マルウェア対策	8
9	サービス等の制限と管理	5
10	データ復旧能力	5
11	ネットワーク機器のセキュアな設定	7
12	境界防御	12
13	データ保護	9
14	知る必要性に基づくアクセスコントロール	9
15	無線アクセスコントロール	10
16	アカウントの監視，管理	13
17	セキュリティ意識啓発プログラムの実施	9
18	アプリケーションソフトウェアセキュリティ	11
19	インシデントレスポンスと管理	8
20	ペネトレーションテスト，レッドチーム訓練	8

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，判定基準表に依らず，有効であるとプレイヤー間およびゲームマスター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．

表 6.3 にセキュ・ワンにおいてゲームマスター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．

6.4 実施：6 回のゲーム演習の実施

セキュ・ワンの有用性を確認するため，6 回の演習を実施した．表 6.4 に演習の概要を示す．演習は SecCap[37] および ICS-CoE 中核人材育成プログラム [53] の受講生を対象として実施した．ゲームマスターの中で「知見を有する者」は大学教員および CISSP 有資格者のことである．3 回目演習におけるゲームマスターは 2 回目演習の参加者でゲームルールを把握している者が担当している．それぞれの演習の評価方法は次節に示す．

6.5 評価：評価指標と評価結果

本節では評価指標と評価結果をまとめる．

6.5.1 評価指標

評価はアンケートによるユーザ評価を活用した．既存の演習ツールと同一の指標を用いることで結果を比較できるようにした．また，ゲーム演習中に取得したポイントから測定可能な参加者の能力を分析した．

ARCS 動機づけモデル

ゲーム演習は参加者の動機づ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，動機づ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

表 6.3: 判定基準表 (一部抜粋)

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．

ることとした．動機づけの効果を測定するための指標に ARCS 動機づけモデル [9] 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．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

表 6.4: 演習の概要（セキュ・ワン）

演習	実施日	対象	ゲームマスター
1 回目	H29.9.13(水)	SecCap 受講生 19 名	知見を有する者
2 回目	H29.10.24(火)	ICS-CoE 受講生 15 名	知見を有する者
3 回目	H30.2.26(火)	ICS-CoE 受講生 66 名	参加者
4 回目	H30.9.13(木)	SecCap 受講生 16 名	知見を有する者
5 回目	H30.10.22(火)	ICS-CoE 受講生 5 名	知見を有する者
6 回目	H30.12.11(火)	ICS-CoE 受講生 6 名 + 留学生 6 名	知見を有する者

表 6.5: ARCS に関連するアンケート内容

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

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 6.5 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，動機づ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 動機づけモデル評価シート [60] 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 6.6 にアンケート内容を示す．

MEEGA+

第 4 回目の演習では動機づけ効果に加えて，ゲームデザインや学習効果を測定できるように MEEGA+ を活用する．表 4.2 の MEEGA+ のアンケート項目からデジタルゲームの項目を除いた質問を用いた．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，

表 6.6: ARCS 動機づけモデル評価シートのアンケート内容

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

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．なお，学習目標の項目は演習ツールに該当する内容を記述する必要があるため，「CSC の理解・標的型攻撃の理解に貢献した.」に修正した．演習では MEEGA+ を用いてセキュ・ワンを含む 4 つのセキュリティゲーム演習の結果を比較した．

独自のアンケート

コンテンツ理解度の確認および取得得点から参加者能力の定量評価ができるようにするために独自の質問を作成した．表 6.7 に質問内容を示す．第 4，6 回目の質問内容は第 3 回目の質問内容よりも詳細化している．

表 6.7: 独自アンケートの内容

項目	質問
3 回目演習	
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
取得得点	総得点は何点だったか
4，6 回目演習	
サイバー攻撃への対策の理解	攻撃カードは理解できたか
	防御カードは理解できたか
取得得点	攻撃カード Type A の取得得点
	攻撃カード Type B の取得得点

その他，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．

6.5.2 評価結果

セキュ・ワンを含む演習ツールを使用した演習を実施後，参加者に前項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．

ARCS 動機づけモデルの評価

表 6.8 に第 1 回目演習における表 6.5 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わかる．

表 6.9 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 6.5 のアンケート結果（平均値 (Avg.) と標準偏差 (SD)）を示す．学生・社会人の結果が類似していることがわかる．セキュ・ワンが学生や社会人の違いに依らず，同程度の動機づけ効果を与えられることを示している．

表 6.10 に第 3 回目演習における表 6.6 のアンケート結果を示す．セキュ・ワン

表 6.8: 第 1 回目演習アンケート結果 1($n = 19$)

	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 6.9: 第 1，2 回目演習アンケート結果の比較

	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

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わかる．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づけ効果が得られることがわかる．

MEEGA+ の評価

図 6.5 に第 4 回目演習の MEEGA+ 動機づけ効果の結果を示す．セキュ・ワンが総じて高い値になっていることがわかる．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．

図 6.6 に第 4 回目演習の MEEGA+ ゲームデザインの結果を示す．セキュ・ワンは他演習ツールと比べても低い評価になっており，フォントやデザインの改善が必要である．

表 6.10: 第 3 回目演習アンケート結果 ($n = 66$)

		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

図 6.7 に第 4 回目演習の MEEGA+ 学習効果の結果を示す．セキュ・ワンは他ツールに比べても同程度の値になっていることがわかる．演習の中でカードに記載された各種コンテンツの内容を議論を通して学習することができたため，高い学習効果を得ることができたものと考えられる．

MEEGA+ の評価（英語コンテンツ）

図 6.8 に第 6 回目演習の MEEGA+ 動機づけ効果の結果を示す．図 6.9 に第 6 回目演習の MEEGA+ ゲームデザインの結果を示す．図 6.10 に第 6 回目演習の MEEGA+ 学習効果の結果を示す．IoT・ポリーの結果と比較しても同程度の値に

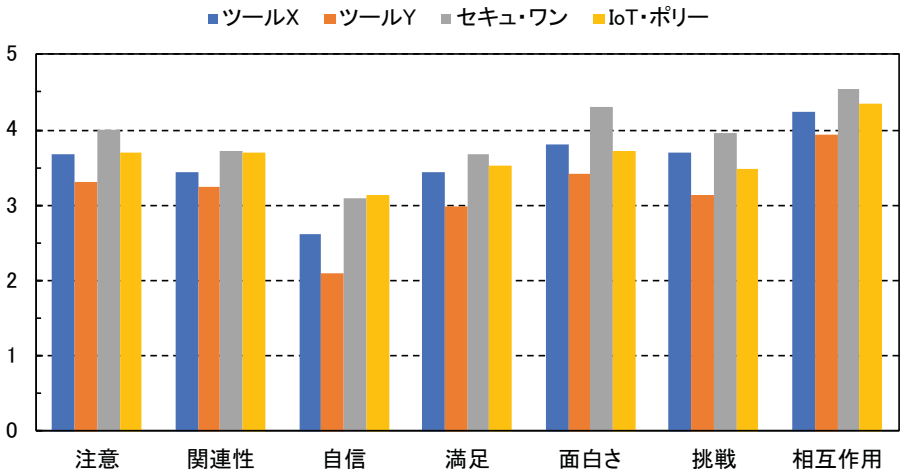


図 6.5: 第 4 回演習 MEEGA+ 動機づけ効果の結果（再掲）

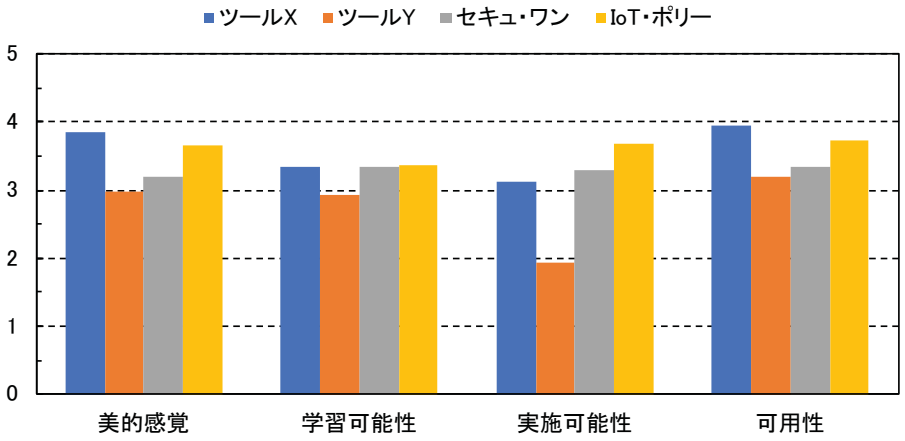


図 6.6: 第 4 回目演習 MEEGA+ ゲームデザインの結果（再掲）

なっていることがわかる．以上から英語コンテンツとしても演習ツールとしての有用性を確認することができた．

独自アンケートの評価

表 6.11 に第 3，4，6 回目演習における表 6.7 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

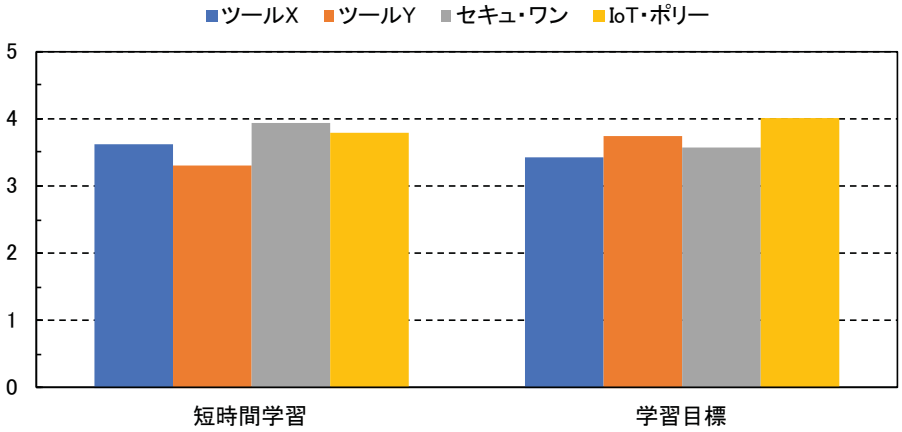


図 6.7: 第 4 回目演習 MEEGA+ 学習効果の結果（再掲）

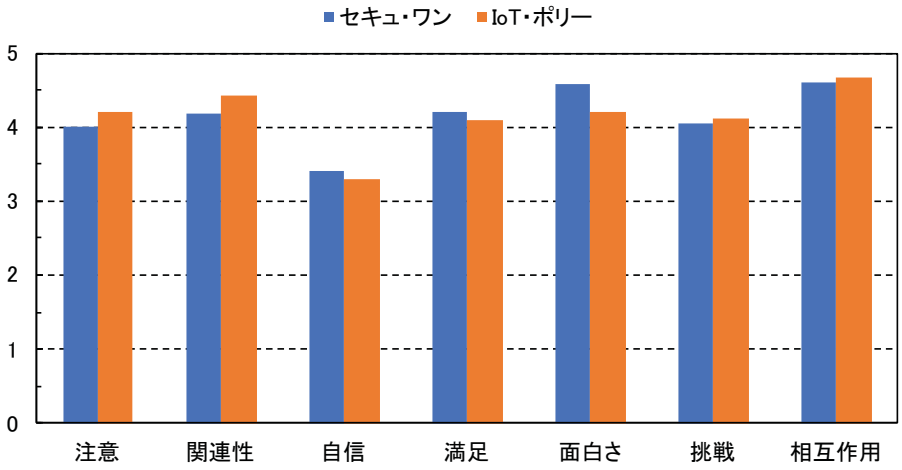


図 6.8: 第 6 回演習 MEEGA+ 動機づけ効果の結果（再掲）

量的には概ねコンテンツの理解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コンテンツの理解の達成度の考察を示す．

プレイヤー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，他プレイヤーやゲームマスターの説明を聞き，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

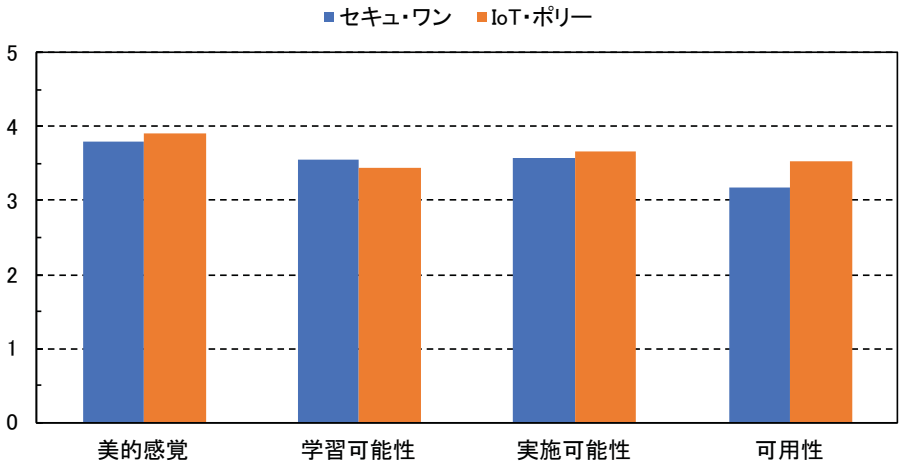


図 6.9: 第 6 回目演習 MEEGA+ ゲームデザインの結果（再掲）

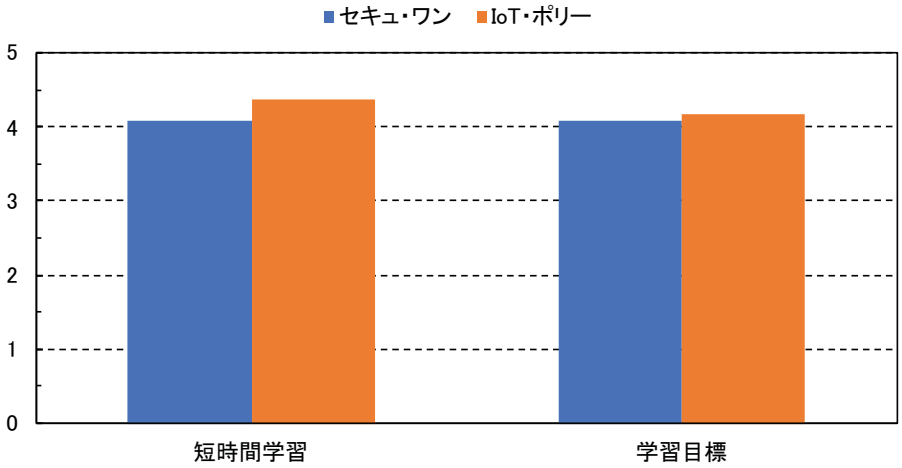


図 6.10: 第 6 回目演習 MEEGA+ 学習効果の結果（再掲）

め，コンテンツの理解は概ね達成できたものと考える．

参加者能力の定量的な測定の可能性

図 6.11 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 6.7 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

表 6.11: 第 3，4，6 回目演習における独自アンケートの結果

質問	Avg.	SD
第 3 回目演習		
攻撃と防御カードは理解できたか	3.35	0.84
迅速に防御カードを提出したか	3.65	1.07
第 4 回目演習		
攻撃カード Type A は理解できたか	3.93	0.75
攻撃カード Type B は理解できたか	3.06	1.09
防御カードは理解できたか	3.06	0.97
迅速に防御カードを提出したか	3	1.17
第 6 回目演習		
攻撃カード Type A は理解できたか	4.08	0.95
攻撃カード Type B は理解できたか	3.92	1.04
防御カードは理解できたか	4.08	0.64
迅速に防御カードを提出したか	4.25	0.72

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．

図 6.12 に第 4 回目演習における「カード内容を理解し，迅速な提出」の値と攻撃カード Type A の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 6.7 のアンケート項目「攻撃カード Type A は理解できたか」,「防御カードは理解できたか」,「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」の値と攻撃カード Type A の得点の相関係数は $r = 0.75$ となり，第 4 回目の演習では高い正の相関を認められた．参加者は 4 人のグループを形成し演習を実施していたことから，第 3 回演習に比べて同一条件で演習を実施することができた．一方で攻撃カード Type B の得点との相関が認められなかった．これは，攻撃カード Type B はより具体的な攻撃手法が記載されているため，

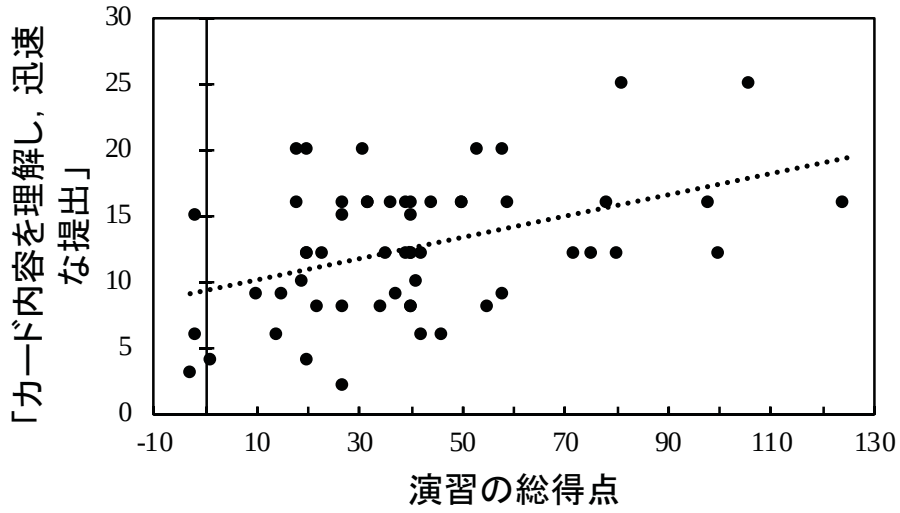


図 6.11: 第 3 回目演習「カード内容を理解し，迅速な提出」の値と総得点の散布図 ($n = 56$)

提出可能な防御カードが制限されており，参加者能力よりも配布される防御カード運の依存が高くなるためと考えられる．

図 6.13 に第 6 回目演習における「カード内容を理解し，迅速な提出」の値と攻撃カード Type A の得点の散布図を示す．「カード内容を理解し，迅速な提出」の値と攻撃カード Type A の得点の相関係数は $r = 0.41$ となり，第 6 回回の演習では中程度の正の相関を認められた．一方で攻撃カード Type B の得点では $r = 0.34$ となり，弱い正の相関が認められた．参加者は 6 人のグループを形成し演習を実施していた．第 4 回目演習に比べて Type A 使用時の相関係数の値が低くなった要因は参加者の元々の知識レベルに大きな差がなかったことが考えられる．

以上のことから若干の条件の不均一があるものの，セキュ・ワンは，攻撃カード Type A を活用した場合「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．今後は配布されるカード運によらず，攻撃カード Type B でも参加者能力を測定できるようにすることが課題である．

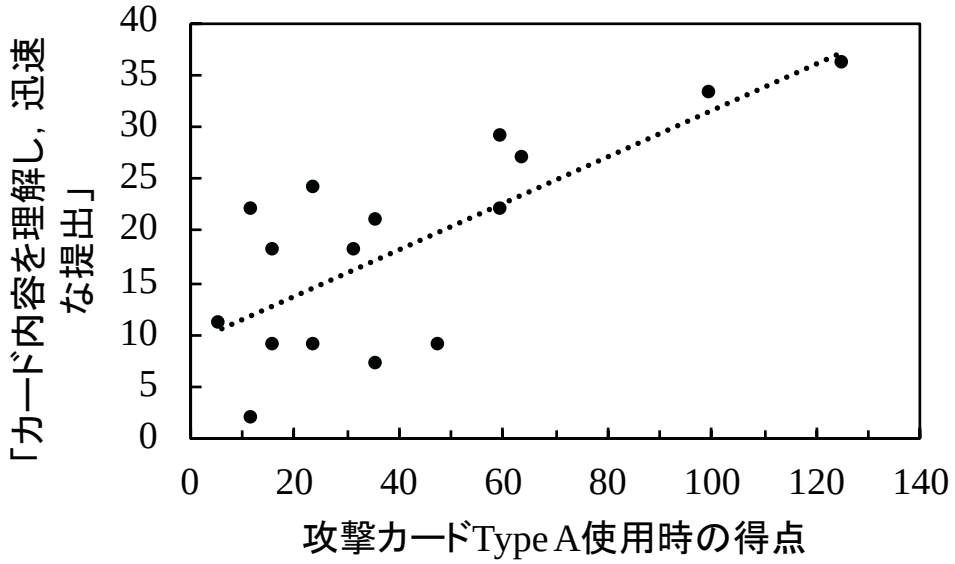


図 6.12: 第 4 回目演習「カード内容を理解し，迅速な提出」の値と Type A 使用時の得点の散布図 ($n = 16$)

6.6 改善：定性的な分析に基づくツールの改善

第 1 回目から第 6 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．本節では，定性的なアンケート結果の分析結果を示す．次項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．

6.6.1 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．

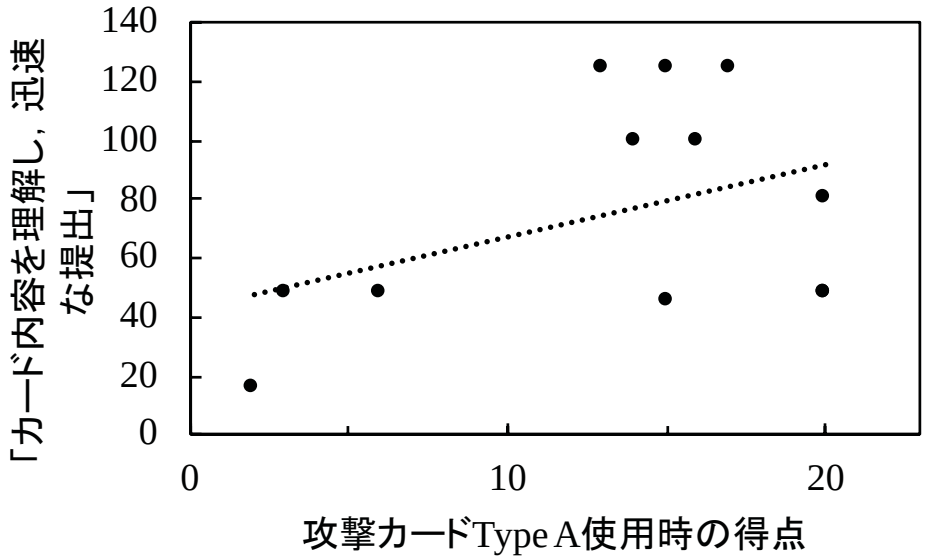


図 6.13: 第 6 回目演習「カード内容を理解し，迅速な提出」の値と Type A 使用時の得点の散布図 ($n = 12$)

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．

6.6.2 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ーを補助できるようにした．

6.6.3 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わかるように修正した．

6.6.4　4 回目

意見 8：改行が多く文章が読み難い．

改善 8：文字フォントサイズを小さくして改行を減らした．

6.6.5　5 回目

意見 9：競争を促すルールではない方が良い．

改善 9：基本ルールに加えて参加者によるルールのアレンジや拡張を許可することとした．

6.6.6　6 回目

意見 10：ポイント付与の方法をグループ内でアレンジした．

改善 10：演習のルールの記載に参加者によるアレンジを可とする旨を追記した．

6.7　6 章のまとめ

本章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．

本章では参加者による 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．動機づ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．

ゲームデザインと学習目標の達成度は MEEGA+ を使用して確認した．ゲームデザインは他ツールよりも評価が低かったため，文字サイズ・フォントの修正により，改善する必要がある．学習目標の達成度は他プレイヤーおよびゲームマスターとの議論を通して，コンテンツの理解を深めることで概ね達成できた．他プレイヤー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．演習後にプレイヤー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」を測れる可能性を示した．特に攻撃カード Type A でその傾向を確認することができた．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，プレイヤー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，ゲームマスター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．

第 7 章　議論

近年，各団体，組織などで様々なセキュリティ人材育成の取り組みが実施されている．本章では，セキュリティ人材の取り組みをまとめ，提案するゲーム演習ツールの活用先についても議論する．また，提案ツールの今後のあり方について議論する．

7.1　提案ツールの活用先

7.1.1　日本国内のセキュリティ人材育成の取り組み内での活用

表 7.1 に日本国内における代表的なセキュリティ人材育成の取り組みをまとめた．本稿ではこのうち，SecCap および ICS-CoE の活動の中で演習を実施した．SecCap と ICS-CoE の対象者は大学院生と企業の中核人材に該当する社会人であるため，本稿で実施できた対象者の範囲が限定的であった．取り組みの趣旨を考慮すると表 7.1 で示すほとんどの取り組みにおいて提案ツールは活用できるものと考えられる．また，表 7.1 で示した取り組み以外にも非営利なセキュリティ勉強会やインベントが多く存在するため，そのような活動の中で活用できるものと考えられる．

7.1.2　サイバー演習としての活用

本節では国内外のサイバーセキュリティマネジメント能力の獲得を目指すサイバー演習をまとめた．表 7.2 に代表的なサイバー演習を示す．表の上段が海外のサイバー演習，下段が国内のサイバー演習になっている．多くのサイバー演習はインシデント対応や事業継続の観点からの演習となっている．また，演習は定期的に実施され，担当者の能力の維持・向上に寄与している．Hardening Project などの一部の演習ではチームを作り，チームごとの得点を競うゲーム演習と機能演習を複合した内容となっている．また，本稿第 3 章の関連研究で示した KIPS を使用し，チームで得点を競うゲーム演習も定期的に実施されている．本稿で提案するセ

表 7.1: 代表的なサイバー演習

名称	概要
Basic SecCap	大学学部生を対象として実践的なセキュリティ人材を育成するプログラム
SecCap	大学院生を対象としたセキュリティエキスパート人材の育成プログラム
ProSec	社会人を対象とした情報セキュリティプロ人材育成短期集中プログラム
SecHack365	25 歳以下の学生や社会人を対象とした若手セキュリティイノベーター育成プログラム
CySec	東京電機大学の後援により約 4 か月でサイバーセキュリティの専門家を育成するプログラム
ICS-CoE	セキュリティの観点から経営層と現場担当者を繋ぐ中核人材を対象とした人材育成プログラム
セキュリティキャンプ	22 歳以下の学生を対象とした IT セキュリティ技術を学ぶ合宿形式の勉強会

キュ・ワンは適切な対策を迅速に提出することで高いインセンティブ（ポイント）を付加しているため，KIPS と同様に競技会形式として活用できる可能性がある．IoT・ポリーはポイントを競うものではなかったが，Hardening Project や KIPS と同様にチームの活動のどこかにインセンティブを与えることでチーム制の競技会用ツールとして発展できる可能性がある．WebSec は表 7.2 には含んでいないが CTF のようなオンラインの競技会として活用できる可能性がある．

7.1.3 企業内セキュリティ研修での活用

CSC をはじめ多くのセキュリティ標準において，組織のセキュリティ対策としてセキュリティ教育を実施する旨が明記されている．第 1 章に示したとおりセキュリティ教育が適切に実施できていない要因として，時間がない，予算がない，社員の興味・関心がないことが挙げられている [2]．本稿の提案ツールは上記の課題の克服を目指して開発されており，第 4 章〜第 6 章にかけてその有効性を示してきた．

利用者向けの演習ツールである WebSec は第 4 章で示したように集合教育の一環として活用できることに加え，オンライン化することにより通勤時間や隙間時間に学習する用途としても活用できるものと考えている．学習の進捗は教育者により容易に管理できるため，コンテンツの見直しや人的な脆弱性（進捗が遅い学習者）へ

のフォローアップも可能となる．

セキュリティ人材向けの演習ツールである IoT・ポリーとセキュ・ワンは企業内のセキュリティ担当者に対する集合研修の機会に実施できるものと考えられる．これらの演習ではグループ内での競争または協調作業による議論を誘発し，部署間の意識の格差や知識の誤認識を改善することができる．

提案ツールを企業内セキュリティ研修内で活用することにより，従来のセキュリティ教育におけるマンネリを打破するとともに，より高度な知識とスキルの獲得が期待できるものと考えている．

7.2　提案ツールの今後のあり方

本節では本稿で提案した 3 つ演習ツールのあり方について議論を行う．提案ツールはサイバーセキュリティマネジメント能力の向上を目指すすべての学習者に実際に使って頂き，その能力の進展を図ることで価値が生じるものと考えられる．以上から提案ツールの配布と更新の要領について以下に示す．

7.2.1　提案ツールの配布

第 1 章で示したとおり国内だけでなく全世界的にセキュリティ人材は不足している．上記の社会的な問題を解決するため，国内外で前節で示した様々な活動が実施されている．前節のような活動は非常に有効な手段であるが，運営側の負担のため地理的および時間的な制限された条件で一定数の人員を集合させて演習する必要がある．また，これらの演習はインシデント対応能力に焦点を当てているものが多く，インシデント対応以外のセキュリティ活動の能力を獲得することに重点を置いていない．本稿で提案した IoT・ポリーおよびセキュ・ワンは同一組織内の仲間で気軽に始めることができるとともに，インシデント対応以外の能力を獲得することができる．セキュリティ人材を目指す多くの学習者にセキュリティ活動の包括的な能力を獲得することの重要性を気づいてもらい，サイバーセキュリティマネジメント能力の伸展を期待して IoT・ポリーおよびセキュ・ワンを GitHub[61, 62] 上にアップロードし，誰でも使用できるようにした．IoT・ポリーおよびセキュ・ワン

をゲーム演習で活用したい学習者はこれらのコンテンツをダウンロード，印刷し，使用することができる．

7.2.2　ゲーム演習ツールの定期的な更新

攻撃者により常に新たなサイバー攻撃手法が開発されていることから提案ツールのコンテンツは新たな脅威に追従する必要がある．提案ツールの元となるコンテンツの多くは様々な組織で整備されており，適時，内容の更新が実施されている．提案ツールのコンテンツは上記の更新に合わせて，更新する必要がある．すべての提案ツールで参照した攻撃ライブラリ（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．IoT・ポリーおよびセキュ・ワン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カードで解釈できない場合は新たなカードを追加する必要がある．WebSec およびセキュ・ワンで用いた 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コンテンツを更新する必要がある．

表 7.2: 代表的なサイバー演習

名称	概要
海外	
Cyber Storm	米国国土安全保障省（DHS）が隔年で実施するサイバー演習である．政府が主導でサイバーセキュリティ演習のフレームワークを提供している．
GridEx	北米電力信頼度協議会により開催され，電力セキュリテ演習である．政府が主導でサイバーセキュリティ演習のィの緊急事態への対応，パートナー間のコミュニケーションの向上，特定の能力のテストを実施している．
Cyber Coalition	NATO や加盟国内ネットワークを防御するための能力として同盟国全域から集まった技術者をテスト・訓練している．
Cyber Europe	ENISA によりサイバー危機演習であり，作成されたシナリオに基づき事業継続計画と危機管理手順をテストしている．
国内	
分野横断的演習	重要インフラ事業者における事業継続計画や官民・分野横断的な情報共有体制に関する実効性の検証などを実施している．
CYDER	国の行政機関，地方公共団体，重要社会基盤事業者等を対象とする実践的なサイバー防御演習を開発・実施している．
Hardening Project	各チームごと仮想的な組織 (会社) となり，自社の EC サイトの売り上げの最大化することを目標に EC サイトの堅牢化技術を競い合う．
サイバークエスト	金融 ISAC により実施されている架空の金融機関を狙った「同時多発的なサイバー攻撃」に対して調査から対応，報告までを訓練している．
CAE2014	テレコム・アイザック推進会議による通信インフラへのサイバー攻撃発生時への対応能力の向上などを目的とした演習である．
KIPS Championship	KIPS を用いて業務継続性や生産性を維持しながらのサイバーセキュリティ確保しチームごとに得点を競い合う．

第 8 章　総括

本稿では，動機づけ効果を与えることおよびこれまで既存のゲーム演習ツールでは考慮されていなかった領域の知識・スキルを獲得することに焦点を当て，3 つのゲーム演習ツールを提案した．本章では本稿のまとめと今後の課題について述べる．

8.1　まとめ

本稿ではセキュリティ教育が適切に実施できていないこと，セキュリティ人材が不足していること，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サイバーセキュリティ演習のゲーム演習に焦点を当て 3 つのゲーム演習ツールを提案した．既存のゲーム演習ツールはテクニカルな能力に焦点を当てたものが多い反面，サイバーセキュリティマネジメント能力に焦点を当てた演習ツールが少なく，実施の機会も十分ではなかった．既存のサイバーセキュリティマネジメント能力に焦点を当てた演習ツールは広範なセキュリティ領域の特定領域に焦点を当てているため，全領域で網羅的にゲーム演習を適用することができていなかった．提案ツールではこれまで，既存の演習ツールでは焦点を当てていなかったサイバーセキュリティマネジメントの領域に焦点を当てた．既存の演習ツールと合わせて活用することでセキュリティ人材が必要とする知識やスキルを網羅的に獲得するこを目指した．演習ツールの開発にあたっては ID の改善プロセスである ADDIE モデルを適用し，改善サイクルを複数回，回した．学習者の動機づけ効果が確認されているゲーミフィケーションの仕組みを取り入れることでセキュリティ教育とセキュリティ疲れの課題の克服を狙った．体系的な知識を獲得するためにサイバー攻撃手法の辞書にあたる攻撃ライブラリ（CAPEC，ATT&CK）とセキュリティ標準である CSC などを演習ツールに適用することで，セキュリティ人材に必要な知識の獲得を目指した．IoT・ポリーでは，リスクアセスメントのプロセスを簡易化したプロセスを通してリスクアセスメントに必要なスキルの獲得を目指した．セキュ・ワンではゲーム化した演習のプロセスを通して，必要なスキルの獲得を目指した．提案ツールの評価にはカークパトリックの 4 段階評価のうち，レベル 1（反応），レベ

ル 2（学習）に着目した．反応では参加者のアンケート結果を分析することで，提案ツールが参加者に動機づけ効果を与えられる可能性を示した．学習ではカード化したコンテンツと参加者間の議論により，コンテンツに関する知識を獲得できる可能性を示した．WebSec では事前・事後テストの結果から，知識の獲得を確認した．また，セキュ・ワンでは演習で獲得する得点により参加者のスキルを定量化できる可能性を示した．

本稿では特性が異なる 3 つのゲーム演習ツールを提案した．WebSec は Web アプリケーションであり，セキュリティ研修だけでなく単独学習にも活用が可能である．コンテンツの内容を IoT・ポリーやセキュ・ワンで活用したものに入れ替えることでカードゲーム演習の復習や予習にも活用できるものと考えられる．IoT・ポリーとセキュ・ワンはカードゲーム演習であり，単独学習では困難であった他の参加者やゲームマスターなどの他者から知見が得られる内容となっている．一方で，カード化したすべてのコンテンツを学習することは困難であり，WebSec のような単独学習が可能なシステムを活用し，補完する必要がある．また，IoT・ポリーは参加者で協調し，演習を進捗させるのに対し，セキュ・ワンは参加者間でポイントを競争する形で演習を進捗させる必要がある．本稿では，IoT・ポリーは IoT システム，セキュ・ワンは IT システムを意識した内容となっているが，IoT・ポリーとセキュ・ワンのカードを入れ替えることで，協調作業で IT システムのリスクアセスメントを演習することや競争により IoT システムの脅威と対策を学習することも可能であると考えている．参加者グループによっては協調より競争を好む場合やその逆もありうる．特性の異なるカードゲーム演習を開発したことで，参加者の好みにあった演習の選択が可能となった．あえて，特性が異なる 3 つのゲーム演習ツールを開発したことで，相互に欠点を補い，柔軟な演習の提供が可能になったものと考える．

以上のことから，本稿で提案した 3 つのゲーム演習ツールを既存のゲーム演習ツールと合わせて活用することで，学習者のモチベーションを維持・向上させつつ，広範なサイバーセキュリティマネジメント能力を獲得させることに貢献できたものと考える．

8.2 今後の課題

本稿では利用者向けの演習ツールとセキュリティ人材向け演習ツールを開発し，主にアンケートによるユーザ評価を用いてそれぞれの演習ツールを評価した．アンケート評価は学習者の主観評価に基づくもので非常に有効な手法である反面，実際に効果があるのかを証明することが難しい．演習ツールによる効果や有用性を示すためにはアンケート評価以外の評価方法を追求する必要があると考えられる．アンケート評価以外の考えられる評価方法は以下のとおり．

- 教育工学のアプローチを追求：本稿の評価はカークパトリック 4 段階評価のうち，主にレベル 1 の段階である反応と一部レベル 2 の段階である学習のみであった．以下にレベル 2 からレベル 4 までの評価方法の適用について考察する．
  - レベル 2 学習：第 4 章において WebSec の評価で実施した事前事後テストは短期的な知識の獲得を評価する上で有効であると考えられる．ただし WebSec では WebSec 実施前後の結果比較のみを示しただけであり，他の演習分類であるセミナー，ワークショップ，机上演習（または，その他の教授手法）を同じ時間実施し，どれだけ効果に差があったのかを比較する必要がある．奈良先端科学技術大学院大学の場合，集合教育としてセキュリティ研修（セミナー）は毎年実施されているので，これを統制群にし，WebSec を使った演習を実験群として効果の差を確認することができるものと考えられる．
  - レベル 3 行動：演習で獲得した知識・スキルが仕事で活かされているか確認するものである．ゲーム演習を定期的に実施しているグループとそうでないグループを比較し，それぞれの対象の行動を確認することで効果を確認する．本稿のように演習の計画者と学習者が別の所属である場合には行動の確認は困難である．企業内研修などで演習ツールを活用した場合には演習計画者が学習者の行動を直接確認することに加えて，学習者の上長を活用し，チェックリストなどで行動の変化の差を確認することができるものと考えられる．
  - レベル 4 業績：学習者や職場の業績の向上を確認するものである．レベ

ル 3（学習）と同じで演習の計画者と学習者が別の所属である場合には確認が困難である．企業内研修などで演習ツールを活用する場合には学習者が所属する部署のセキュリティインシデント数が減少した，インシデント発生後の対応速度が早くなった，脆弱性診断の結果が改善したなどのセキュリティ活動の改善を確認することができるものと考える．

- ラーニングアナリティクスの改善：第 4 章において WebSec の学習ログを活用し，学習者の事前知識と演習速度の相関があること示した．第 6 章においてセキュ・ワンによる取得スコアとアンケート結果を分析し，取得スコアから学習者の能力に相関がある可能性を示した．上記の結果はラーニングアナリティクスによる成果であると考えられる．WebSec は BI ツールを用いることで容易に学習ログを分析できた反面，セキュ・ワンではスコア表を人的に確認し，結果をまとめたことで作業コストが増大した．また，IoT・ポリーではワークシートに議論の過程を記述したが，ワークシートから有効な分析結果を導出することができなかった．上記の反省を踏まえ，演習ツールの効果および有用性を迅速的確に示すには以下の改善が望まれる．
  - 仮説と学習記録の測定項目：演習実施前にゲーム演習ツールが与える効果の仮説を立て，仮説を立証するための測定項目を決定する．IoT・ポリーの場合，提出および順位付けされた脅威カードと対策カードの模範解答を正しく導出するための学習者の行動に仮説をたてる．例えば，模範解答の導出には意思決定にかかる時間に因果関係がある，または，模範解答の導出にはグループ内の各学習者の発言回数に因果関係があるなどが考えられる．

    上記の仮説を受けて，必要な測定項目を決定する．上記の例の場合，時間や発言回数が測定項目になると考えられる．
  - 測定方法：IoT・ポリーおよびセキュ・ワンの学習記録は紙面への記録であり，分析の作業コストが増大した．アナログゲーム演習であっても記録方法は可能な限りシステム化することが望ましいと考える．また，極力，学習者に学習事項とは無関係な操作に意識が向かないように測定要領も考慮することが重要であると考える．例えば，Web インターフェースを作成し，学習者に演習の記録を入力させ，サーバに学習ログ

として保存するシステムを構築できる．または，アナログゲームに使用するカード内に読み取り可能なバーコードまたは QR コードを付加し，使用されたカードを読み取り，情報をサーバに送信することもできる．加えて，学習者の発言内容や動作を確認するためには動画の撮影が必要となる場合が考えられる．ここでは音声認識技術などの最新の研究成果も活用可能であると考えられる．

謝辞

本研究を取り組むにあたり，ご指導を頂きました本学情報科学領域の門林雄基教授, 笠原正治教授, 林優一教授, 妙中雄三准教授に深く感謝致します．また, サイバーレジリエンス構成学研究室の樫原茂助教, Doudou Fall 助教, 東京大学の宮本大輔准教授にも多大なるご指導を賜りましたことここに厚く御礼申し上げます．WebSec の共同開発者である Balazs Barna 氏 (Corvinus University of Budapest)，および同氏の日本留学を支援していただいた Erasmus Mundus TEAM プロジェクトに感謝申し上げます．演習の実施の際にご支援いただいた IPA 産業サイバーセキュリティセンター (ICS-CoE)，および演習ツールの翻訳をご支援いただいた稲田陽子様に感謝申し上げます．SecCap における IR ボードゲームの無償利用を許諾いただいたトレンドマイクロ株式会社様に感謝申し上げます．演習コンテンツで活用した CAPEC, ATT&CK を無償公開して頂いた MITRE 社，および Baseline Security Recommendations for IoT を無償公開して頂いた ENISA にも感謝しております．サイバーレジリエンス構成学研究室の秘書，学生の皆様をはじめ，博士前期課程の期間に様々な活動を通して知り合ったすべての皆様にこの場を借りて感謝申し上げます．

参考文献

[1] Center for Internet Security, The CIS Critical Security Controls for Effective Cyber Defense Version 7.1, available from <https://www.cisecurity.org/> (accessed 2018-10-31).

[2] 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).

[3] 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).

[4] 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）.

[5] 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）.

[6] 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).

[7] 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.

[8] 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.

[9] J. M. ケラー, 「学習意欲をデザインする」, 北大路書房, 2010.

[10] 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.

[11] Karl M. Kapp, “The Gamification of Learning and Instruction: Game-based Methods and Strategies for Training and Education”, Pfeiffer, 2012

[12] 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).
[13] 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).
[14] 深田浩嗣：ソーシャルゲームはなぜハマるのか，Softbank Creative(2011).
[15] 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誌，Vol.2016, No.1，pp.704-704(2016).
[16] 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)
[17] 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).
[18] 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).
[19] 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).
[20] 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).
[21] 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).
[22] Regina Phelps, “Emergency Management Exercises”, Chandi Media, 2010
[23] Sangkyun Kim, Kibong Song, Barbara Lockee, John Burton, “Gamification

in Learning and Education", Springer, 2018

[24] 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).

[25] 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).

[26] 情報処理推進機構:情報セキュリティマネジメント試験, 入手先<https://www.jitec.ipa.go.jp/sg/index.html> (参照 2019-2-24).

[27] Tamara Denning, Adam Shostack, and Tadayoshi Kohno "Practical Lessons From Creating the Control-Alt-Hack Card Game and Research Challenges for Games In Education and Research", 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14), 2014.

[28] Zikai Alex Wen, Yiming Li, Reid Wade, Jeffrey Huang, Amy Wang "What.Hack: Learn Phishing Email Defence the Fun Way ", CHI EA '17 Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems, 2017, pp.234-237.

[29] Adam Shostack, "threat modeling designing for security", WILEY, 2014

[30] 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).

[31] 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).

[32] 内閣サイバーセキュリティセンター:"ネットワークビギナーのための情報セキュリティハンドブック", 入手先<https://www.nisc.go.jp/security-site/files/handbook-all.pdf> (参照 2018-10-31).

[33] 総務省:"国民のための情報セキュリティサイト", 入手先<http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/> (参照 2018-10-31).

[34] MITRE: CAPEC^{TM} A Community Resource for Identifying and Understanding Attacks, available from <https://capec.mitre.org/> (accessed 2018-04-23).

[35] VERIZON: Data Breach Digest, available from <http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf> (accessed 2019-01-21).

[36] VERIZON: Data Breach Digest, available from <http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest-2017-perspective-is-reality_xg_en.pdf> (accessed 2019-01-21).

[37] 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).

[38] Giani Petri, Christiane Gresse von Wangenheim, Adriano Ferreti Borgatto, "A large-scale evaluation of a model for the evaluation of games for teaching software engineering", in Proceedings of the 39th International Conference on Software Engineering: Software Engineering and Education Track, 2017.

[39] Fu, F., Su, R., Yu, S, "EGameFlow: A scale to measure learners' enjoyment of e-learning games", Computers & Education, 52(1), 101-112, 2009.

[40] Gunter, A. G., Kenny, F. R., Vick, H. E, "Taking educational games seriously: using the RETAIN model to design endogenous fantasy into standalone educational games", Education Tech Research Dev, 56, pp.511-537, 2008.

[41] 内閣府："平成 29 年度 青少年のインターネット利用環境実態調査 調査結果（速報）", 入手先<http://www8.cao.go.jp/youth/youth-harm/chousa/h29/net-jittai/pdf/sokuhou.pdf> (参照 2018-10-31).

[42] Symantec："インターネットをあんぜんにたのしく使おう", 入手先 <https://japan.norton.com/edu/?inid=jp_hho_NortonLP_banner _discoverychannel> (参照 2018-11-13).

[43] Trend Micro："小・中学生向け インターネットあんしんガイド", 入手先<https://is702.jp/download/partner/12_t/?cm_mmc=Corp-

_-DL-_-702> (参照 2018-11-13).
[44] IPA : “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).
[45] 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).
[46] 情報処理推進機構 : “共通脆弱性評価システム CVSS 概説”, 入手先 <https://www.ipa.go.jp/security/vuln/CVSS.html> (参照 2018-12-19).
[47] 情報処理推進機構 : “NIST SP800-30 : リスクアセスメント実施の手引き”, 入手先<https://www.ipa.go.jp/files/000025325.pdf> (参照 2018-12-19).
[48] ナンシー・G・レブソン, セーフウェア 安全・安心なシステムとソフトウェアを目指して, 翔泳社, 2009.
[49] Andrew M’Manga, Shamal Faily, John Mcalaney, Chris Williams, Youki Kadobayashi, Daisuke Miyamoto, “Eliciting Persona Characteristics for Risk Based Decision Making”, in Proceedings of 32nd British Computer Society Human Computer Interaction Conference, 2018.
[50] Clint Bodungen, Bryan Singer, Aaron Shbeeb, Kyle Wilhoit, Stephen Hilt, “Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions”, McGraw-Hill Education, 2016.
[51] 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).
[52] ENISA: Baseline Security Recommendations for IoT, available from <https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport> (accessed 2018-10-17).
[53] 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).

[54] Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin: 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).

[55] MITRE: Finding Cyber Threats with ATT&CK^{TM}-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).

[56] 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, available from <https://www.ipa.go.jp/security/keihatsu/videos/ index.html> (accessed 2017-08-21).

[57] 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).

[58] Verizon: The Verizon Data Breach Investigations Report. Available (with registration), available from <http://www.verizonenterprise.com/DBIR/> (accessed 2017-08-16).

[59] Symantec: 2017 年インターネットセキュリティ脅威レポート (with registration), available from <https://www.symantec.com/ja/jp/security-center/threat-report> (accessed 2017-08-16).

[60] 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, available from <http://www2.gsis.kumamoto-u.ac.jp/arcsguidebook/html/aboutheet.html> (accessed 2017-10-16).

[61] GitHub : secure-one, available from <https://github.com/nabetan/secure-one> (accessed 2018-07-19).

[62] GitHub : IoT-Poly, available from <https://github.com/nabetan/IoT-

Poly> (accessed 2019-01-31).

業績

学術論文

[1] 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.12，2018，pp.2264-2271.

国際学会

[1] Tan Omiya, Youki Kadobayashi, “Secu-One: A Proposal of Cyber Security Exercise Tool for Improving Security Management Skill”, in Proceedings of 2019 7th International Conference on Information and Education.

国内研究会

[1] 近江谷旦, 宮本大輔, 門林雄基, “サイバー攻撃の脅威に対応する具体的な管理策を学ぶための教育ツールの検討” 電子情報通信学会 ICSS 研究会, 2017 年 11 月.
[2] 近江谷旦, Doudou Fall，樫原茂, “機械学習を用いたベビーモニターの試作と評価” 電子情報通信学会 MoNA 研究会, 2018 年 2 月.
[3] 近江谷旦, 門林雄基, “IoT・ポリー：IoT セキュリティゲーム演習ツールの開発と評価” 2019 年　暗号と情報セキュリティシンポジウム（SCIS2019), 2019 年 1 月.
[4] 近江谷旦, 門林雄基, “WebSec：セキュリティ研修のためのゲーム演習ツールの提案と評価” 電子情報通信学会 教育工学研究会, 2019 年 1 月.

付録

A　IoT・ポリー：IoT カード一覧

No.	タイトル	概要
1	スマートファクトリー	-工場内機器の品質・状態などの様々な情報を「見える化」，-データ解析技術を用いた高い効率化の実現，-生産性の向上のため高い稼働率が求められる，-機器制御不能による人的損害
2	制御システム	-製造寿命は 10 年以上で継続的なサポートが必要，-24 時間 365 日連続稼働が必須，-リアルタイムの情報交換，-（システムによっては）人命・設備・製品の喪失や環境負荷のリスク
3	スマートハウス	-電力需給を制御する HEMS を中心に対応機器を一元管理することで省エネを実現，-取得データにより家主の不在を判断可能，-金銭的被害（エネルギーの浪費）や物理的被害（火災等）
4	スマートシティ	-生活の質の向上と都市の運用とサービス効率向上を図る都市，-収集されたデータへの市民のプライバシー保護が必要，-交通等においては人的な被害を与える可能性がある．
5	スマートカー	-ICT 端末の機能を持つ自動車，-車両の状態や周囲の道路状況等のデータをセンサーにより取得し NW を介して集積・分析，-不正操作による重大事故や収集データと GPS 等を組み合わて個人を特定できる可能性
6	スマートファーム	-環境状態のデータを収集し管理・分析など行うシステム，-24 時間継続的なデータ管理，-センサーデータの改ざんにより農作物の損害リスク，-飼料や薬品の過剰投与による健康被害のリスク
7	スマート家電	-製造寿命は 10 年以上で継続的なサポートが必要，-外部メディア・NW に接続可能，-十分にセキュリティ対策のコストをかけることができない，-踏み台（スパム，DDoS 攻撃）で悪用された事例がある．
8	ヘルスケア機器	-個々のヘルスケアデータを一元管理するシステム，-データ解析等により高付加価値のあるサービスを提供可能，-（医療機器によっては）患者の人命に影響，データは取り扱い注意を要する機微な情報
9	POS システム	-売上を単商品の単位で集計し集計結果により売上げや在庫を管理・分析するシステム，-カードリーダの物理的な入れ替えや細工が可能，-RAM スクレーパーによるクレジットカード情報の漏洩
10	Web カメラ，見守りシステム等	-Web 経由等で撮影された画像にリアルタイムにアクセス可能，-低価格で取得可能，-不正利用された場合，プライバシー侵害のリスク，-踏み台（スパム，DDoS 攻撃）で悪用された事例がある．

B　IoT・ポリー：アタックサーフェスカード一覧

No.	タイトル	概要	脆弱性
1	エコシステムのアクセス制御	エコシステムの構築によりデバイスにより収集された情報をビッグデータ解析等で利用が可能	-コンポーネント間の暗黙の信頼関係，-セキュリティ設定，-廃棄されたシステム，-アクセス手順の無効化
2	デバイスメモリ	デバイスはセンサーから入手した情報等を一時的に保持するためのメモリ領域を保有	機密データ（平文のユーザ名，平文のパスワード，サードパーティの資格情報，暗号化キー）
3	デバイスの物理的なインターフェース	外部デバイスを接続可能な物理的なインターフェースを保有	-ファームウェアの抽出，-ユーザ CLI , -管理者 CLI , -特権昇格，-脆弱な状態にリセット，-記憶媒体の取り外し，-耐タンパー性，-デバックポート，-デバイス ID/シリアル番号の公開
4	デバイスの Web インターフェース	デバイス情報の閲覧等をネットワーク経由で Web ブラウザから実現するための機能を提供	-一般的な Web アプリケーションの脆弱性，-資格情報管理の脆弱性（ユーザ名の列挙，脆弱なパスワード，アカウントロック，既知の資格情報，脆弱なパスワード復旧メカニズム）
5	デバイスファームウェア	デバイスを制御するため，デバイス内の ROM やフラッシュメモリに記録された組み込みのソフトウェアを保有	-ハードコードされた資格情報，-機密情報の漏洩，-機密 URL の漏洩，-暗号化鍵，-ファームウェアバージョンや最終更新日の表示，-セキュリティに関わる API の公開，-ファームウェアのダウングレード，-セキュリティ関連 API の公開

次ページに続く

前ページからの続き

No.	タイトル	概要	脆弱性
6	デバイスのネットワークサービス	操作性の向上等のため，ユーザに提供するネットワーク経由のサービスを保有	-情報漏洩，-ユーザ CLI，-管理 CLI，-インジェクション，-サービスの停止・ DoS，-非暗号サービス，-実装が適切でない暗号化，-テスト/開発サービス，-バッファオーバフロー，-UPnP， 脆弱な UDP サービス
7	管理インターフェース	デバイスを直接または遠隔から管理するためのインターフェースを提供．操作性の向上により容易なデバイスの管理を実現	-SQL インジェクション，-クロスサイトスクリプティング，-クロスサイトリクエストフォジュリー，-ユーザ名の列挙，-アカウントロック，-脆弱なパスワード，-二要素認証，-既知の資格情報，-セキュリティ/暗号化オプション，-ロギングオプション，-デバイスの消去が不能
8	ローカルデータストレージ	デバイスは過去のセンサー情報等を蓄積するためにローカルデータストレージ領域を保有	-非暗号データ，-公開された鍵でデータを暗号化，-不十分なデータ完全性検査，-静的な同一暗号化 / 復号鍵の使用
9	クラウド Web インターフェース	デバイスからクラウドに送信された情報を閲覧等が可能なクラウド Web インターフェースを保有	一般的な Web アプリケーションの脆弱性，-資格情報管理の脆弱性（ユーザ名の列挙，脆弱なパスワード，アカウントロック，既知のデフォルトな資格情報，脆弱な PW 回復メカニズム），-トランスポートの暗号化
10	サードパーティバックエンド API	デバイスから入力した情報からデータ処理，保存，結果の出力等を実行するため，サードパーティバックエンド API を利用	-非暗号 PII の送信，-暗号化 PII の送信，-デバイス情報の漏洩，-位置情報の漏洩

次ページに続く

前ページからの続き

No.	タイトル	概要	脆弱性
11	アップデートの仕組み	デバイスの脆弱性の修正等のため，アップデートの仕組みを提供	-非暗号化で送られる更新，-署名がない更新，-書き込み可能な場所が更新，-更新の確認，-認証の更新,-悪意のある更新,-更新メカニズムがない，-手動の更新メカニズムがない
12	モバイルアプリケーション	スマートフォンやタブレット端末からデバイスを管理しセンサー情報を閲覧できるようにモバイルアプリ機能を提供	-デバイスやクラウドにより暗黙的に信頼,-ユーザ名の列挙,-アカウントロック，-二要素認証，-既知のデフォルトな資格情報，-脆弱なパスワード，-脆弱なデータストレージ，-トランスポートの暗号化，-脆弱なパスワード回復メカニズム
13	ベンダーバックエンド API	デバイスから入力した情報からデータ処理，保存，結果の出力等を実行するため，ベンダーバックエンド API を利用	-クラウドやモバイルアプリの本来の信頼，-脆弱な認証，-脆弱なアクセス制御，-インジェクション攻撃，-隠されたサービス
14	エコシステムの通信	デバイスの死活監視等を実現するための通信を実行	-ヘルスチェック，-ハートビート，-エコシステムコマンド，-プロビジョニングの解除，-更新を強制
15	ネットワーク通信	デバイスへの双方向な通信を実現するため，様々なネットワーク通信機能を保有	LAN ，インターネットに繋がった LAN ，短距離通信，非標準通信，無線 (WiFi，Z-wave，XBee，Zigbee，Bluetooth，LoRA) ，プロトコルファジング

次ページに続く

前ページからの続き

No.	タイトル	概要	脆弱性
16	認証/認可	正当なユーザやデバイス等との情報のやりとりを保証するため認証/認可機能を保有	-認証/許可関連の情報（セッション鍵，トークンなど）の開示，-セッション鍵，トークン等の再利用，-デバイスからデバイス，-デバイスからモバイルアプリ，-デバイスからクラウド，-モバイルアプリからクラウド，-Web アプリからクラウド，-動的認証の欠如
17	プライバシー	デバイスが取得する情報や保有する情報の中にユーザのプライバシー情報が含まれる．	-ユーザデータの開示，-ユーザ/デバイスの位置の開示，-プライバシーの区分
18	ハードウェア（センサー）	物理的にセンサーやその周辺環境にアクセスや操作が可能	-センシング環境の操作，-改ざん（物理的），-損害（物理的）

以上

C　IoT・ポリー：脅威カード一覧

ID	タイトル	概要	具体的な攻撃（例）
21	資格情報の悪用	セッション ID とリソース ID へ攻撃を行う．一部のソフトウェアが信頼性を確認せずにユーザの入力を受け入れることを悪用する．	セッションクレデンシャルの改ざん，セッションハイジャック，クロスサイトリクエストフォージェリ
22	クライアントへの信頼を悪用	クライアント/サーバ通信チャネル認証とデータ整合性の脆弱性を悪用する．攻撃者はクライアントとサーバ間の通信チャネルに自分自身を認識させる．	中間者攻撃，悪意のあるクライアントを作成，トークンの操作（クッキー，URL 等）
25	デッドロックの強制	標的ソフトウェアをデッドロック状態にし，サービス拒否状態にする．デッドロックは，2 つ以上の競合するアクションがお互いに完了するのを待っているときに発生する可能性がある．	なし

次ページに続く

前ページからの続き

ID	タイトル	概要	具体的な攻撃（例）
26	競合状態の悪用	複数のプロセスが同じリソースに同時にアクセスし操作するときに発生する競合状態を悪用する.	シンボリックリンクによる競合条件，チェックから使用までの間(TOCTOU)における競合条件
28	ファジング	ファジングによりシステムの弱点を特定する．ファジングはシステムにランダムな入力を与え，障害が生じた結果を調査するソフトウェアのセキュリティ・機能テストの手法である.	なし
74	ユーザの状態を操作	標的ソフトウェアにより保持される状態情報をユーザがアクセス可能な場所に変更する．成功すると，標的ソフトウェアは侵害された状態情報を使用し，意図しない方法で実行してしまう.	複数のフォームセット内の中間フォームのバイパス（ Web フォームの順序をバイパスなど）
112	ブルートフォース	アセットをロック解除する秘密等を発見するため，すべての可能な秘密値を探索するブルートフォースにより資産にアクセスする．秘密の例にはパスワード，暗号化キーなどがある.	暗号化鍵へのブルートフォース，パスワードへのブルートフォース，レインボーテーブルパスワードクラッキング
113	API の操作	アプリケーションプログラミングインターフェイス（API）の機能を悪用し，API を実装しているシステムを攻撃する．意図しない機能が実行され，API を実装するシステムが侵害される.	テスト API の悪用，未公開 API の悪用，スクリプトベースの API を悪用
114	認証の悪用	認証メカニズムの固有の弱点・認証スキームの実装の欠陥を悪用し，アプリケーション・サービス・デバイスに不正にアクセスする.	デバイスリソースの不正使用，認証プロトコルへのリフレクション攻撃

次ページに続く

前ページからの続き

ID	タイトル	概要	具体的な攻撃（例）
115	認証のバイパス	認証メカニズムを回避し，許可されたユーザ・特権ユーザ権限でアプリケーション・サービス・デバイスにアクセスする．攻撃者の予期しないアクセス手順が認証のための適切なチェックポイントを通過しないことが原因である．	強制的ブラウズ，ハッシュ関数拡張機能の弱点がある Web サービス API 署名偽造
116	発掘	標的の情報を収集するため，1. 通常のやりとりで標的を探索する，2. 所望のデータを含む応答を生成するため，構文的に無効・非標準のデータを送信する．	ゴミ箱あさり，共有・システムリソースからデータを収集
117	傍受	情報収集のため，標的のデータのやりとりを監視する．後に続く攻撃のための情報収集か，収集されたデータが攻撃の最終目標となる可能性がある．	スニッフィング攻撃，インテントの傍受，ビデオ周辺機器等を用いた盗聴
122	特権悪用	特権を持つユーザ・管理者が実行するべきであるが特権のないアカウントによって使用できてしまう機能を利用する．	ACL 制限がない機能にアクセス，ACL の誤った設定，WebView の公開
123	バッファの操作	バッファ攻撃の対象はバッファの内容を解釈するコードではなく，バッファ空間自体である．割り当てられたバッファに格納できる以上の入力を取得・送信し，意図しない他のプログラムメモリを読み書きする．	バッファオーバーフロー，バッファオーバーリード
124	共有データの操作	複数のアプリケーションで共有されるデータ構造を利用し，アプリケーション動作に影響を与える．データは複数のアプリケーション間，単一のアプリケーションの複数のスレッド間で共有できる．	なし

次ページに続く

前ページからの続き

ID	タイトル	概要	具体的な攻撃（例）
125	フラッディング	標的とのインタラクションの数を急激に増やすことで標的のリソースを消費させる．レート制限またはフローの弱点を突くことで正当なユーザがサービスにアクセスできなくなり，標的がクラッシュする可能性がある．	TCP Flood，UDP Flood，ICMP Flood，HTTP Flood，増幅攻撃，XML Flood
129	ポインタの操作	標的アプリケーション内のポインタを操作し，アプリケーションの意図しないメモリ位置にアクセスする．アプリケーションのクラッシュ，任意のコードの実行等の可能性がある．	なし
130	過度な割り当て	サービスの悪用・拒否のため，標的に過度のリソースを割り当てる．慎重にフォーマットされた 1 つまたは少数の要求により，標的に要求を処理するための過剰なリソースを割り当てさせる．	TCP，UDP フラグメンテーション，ICMP フラグメンテーション，SOAP 配列拡張
131	リソースのリーク	標的上のリソースリークを悪用し，正当な要求処理に利用可能なリソースの量を枯渇させる．割り当てられたメモリが処理後に解放されず，メモリリークを生起される手法が最も一般的.	なし
137	パラメータの注入	入力検証の弱点を悪用し要求されるパラメータの内容を操作する．分離文字であるテキスト文字列を操作できる場合，エンコーディングスキームで使用される特殊文字を挿入しパラメータを追加，変更できる．	書式文字列攻撃，コマンド区切り文字，メールヘッダーインジェクション
148	コンテンツスプーフィング	コンテンツの見かけのソースを変更せずに元のコンテンツ制作者が意図したものとは異なるものを含むようにコンテンツを変更する．	GPS 信号の偽装, インテントの偽装，UDDI/ebXML メッセージの偽装

次ページに続く

前ページからの続き

ID	タイトル	概要	具体的な攻撃（例）
151	識別情報のなりすまし	ある他のエンティティ（人間・人間以外）の識別情報を仮定し，その識別情報を用いて目標達成を試みる．関係者から送られたように見えるメッセージを作成，盗まれた/偽装された認証資格を使用することがある．	署名の偽装，クロスフレームスクリプティング，プリンシパル・スプーフィング
153	入力データの操作	入力値検証の弱点を突き，入力処理インターフェースのデータフォーマット・構造を制御する．非標準・予期しない形式の入力を実行することで，攻撃者は標的のセキュリティに悪影響を与える．	ディレクトリトラバーサル，整数型攻撃，代替エンコーディングの利用
154	リソース位置のなりすまし	アプリケーションやユーザを欺いて，意図しない場所からリソースを要求するように誘導する．これにより，攻撃者は悪意のあるリソースを使用させることができる．	ライブラリアクセスをリダイレクト，類似した場所に悪意のあるバージョンを配置
161	インフラストラクチャの操作	ネットワークエンティティのインフラストラクチャの特性を悪用する．ネットワークオブジェクト上の攻撃や情報収集を行い，ネットワークオブジェクト間の通常の情報フローの変化を発生させる．	キャッシュポイズニング，監査ログの操作，中央リポジトリへのログを遮断
165	ファイルの操作	アプリケーションが誤った処理をするようにファイルの内容や属性（拡張子や名前など）を変更する．1. アプリケーションを不安定な状態にする，2. 機密情報を上書きする，3. 特権で任意のコードを実行することができる．	Web サーバーの誤ったファイルタイプを処理させる，代替データストリーム

次ページに続く

前ページからの続き

ID	タイトル	概要	具体的な攻撃（例）
169	フットプリンティング	スキャンにより，対象の構成要素と特性を特定する．攻撃の準備時によく利用され，収集される情報には，オープンポート，アプリケーションとそのバージョン，ネットワークトポロジなどの情報がある．	ポートスキャン，ネットワークトポロジマッピング，ホストの発見
173	アクションスプーフィング	攻撃者は，あるアクションを別のアクションに変えることができる．ユーザがある動作を開始しようとするときにユーザが意図した動作と別の動作を開始することでユーザを騙す．	クリックジャッキング，タップジャック攻撃
175	コードの包含	標的上の弱点を突き，任意のコードをローカル・リモートから実行する．コードファイルへの参照の追加・置換を伴い，コードファイルが標的によってロードされ，あるアプリケーションのコードの一部として使用される．	ローカルコードのインジェクション，リモートコードのインジェクション
176	構成/環境の操作	対象アプリケーションの外部にあるファイルや設定を操作し，動作に影響を与える．外部構成ファイル・ライブラリを変更し，アプリケーションがこれらを使用する能力に影響を与える．	アプリのレジストリ値を操作，スキーマポイズニング，セキュリティソフトウェアの無効化
184	ソフトウェアの完全性を攻撃	ソフトウェアコード，デバイスデータ構造，デバイスファームウェアの完全性を侵害することで標的の整合性を変更して安全性の低い状態にする．	悪意のあるソフトウェアのダウンロード，悪意のあるソフトウェアの更新
188	リバースエンジニアリング	分析対象のエンティティがどのように構築され動作するかを効果的に判定するため，様々な分析技術を使用してオブジェクト，リソース，システムの構造，機能，構成を探索する．	ホワイトボックス・ブラックボックスリバースエンジニアリング

次ページに続く

前ページからの続き

ID	タイトル	概要	具体的な攻撃（例）
192	プロトコル解析	パケット交換データネットワーク上に相互接続されたノード・システム間で情報を送信するために使用されるネットワーク・アプリケーション通信プロトコルのプロトコル情報を解読・復号する.	暗号解読（セルラ暗号の暗号解読，パディングオラクル攻撃）
212	機能の悪用	アプリケーションの正当な能力を悪用する．システムの機能が意図されていない方法で使用される．特定の機能を過度に使用，不正に機密データにアクセス可能な設計上の欠陥を悪用する.	アカウントロックアウトの誘導，パスワードリカバリの悪用，暗号化レベルの低下を強制
216	通信チャネルの操作	通信チャネル上の設定やパラメータを操作する．これは，情報漏洩，通信ストリームからの情報の挿入/除去，システムの侵害をもたらす可能性がある.	誤った設定された SSL の悪用，他のクライアントに割り当てられたメッセージ識別子の選択
224	フィンガープリント	標的システムからの出力と標的に関する特定の情報を一意に識別する既知のインジケータを比較する．これにより，攻撃者は標的の既存の弱点を発見することができる.	OS フィンガープリンティング，アプリケーションフィンガープリンティング
227	継続的なクライアントによる攻撃	リソースを可能な限り長く縛り続けるため，特定のリソースを継続的に関与させる．これにより，正当なユーザによるリソースへのアクセスを拒否する.	HTTP DoS
233	特権昇格	脆弱性を悪用してシステムの権限を昇格させ，実行権限のない処理を実行する.	クロスゾーンスクリプティング，特権プロセスの乗っ取り，特権実行スレッドのハイジャック
240	リソースインジェクション	入力検証の弱点を突き，リソースの意図しない変更・指定を可能にするリソース識別子を操作する.	モバイル技術のトラフィックにデータ（シグナリングデータ）を注入し，通信を中断

次ページに続く

前ページからの続き

ID	タイトル	概要	具体的な攻撃（例）
242	コードのインジェクション	標的上の入力検証の弱点を突き，現在実行中のコードに新しいコードを注入する．	クロスサイトスクリプティング, クロスドメイン窃取, スクリプト内にスクリプトの埋込
248	コマンドインジェクション	攻撃者が任意の命令を実行しようとする際，既存のコマンドに新しい項目を挿入し，意図されたものから解釈を変更する．信頼できない値を使用してこれらのコマンド文字列を作成する．	SQL インジェクション，OS コマンドインジェクション，XML インジェクション
272	プロトコル操作	通信プロトコルを悪用し，他人を偽装，機密情報の発見，セッションの制御などを実行する．プロトコル実装上の固有な前提，プロトコルの不正な実装，プロトコル自体の脆弱性を対象とする．	HTTP リクエストスマグリング攻撃，コンポーネント間・データ交換，Web サービスのプロトコル操作
390	物理的セキュリティのバイパス	施設で使用されるロック，電子的なカード入力システム，物理的なアラームなどによる検出を避けるため，監視の回避，エントリポイントを保護する電子的・物理的なロックをバイパスする．	磁気ストリップ・RFID カードへのブルートフォース攻撃・クローニング，RFID チップの無効化・破壊
391	物理的なロックをバイパス	建物や施設の物理的なセキュリティ対策を回避するための手法や方法を使用する．物理的なロックにはラップトップやサーバーを保護するために使用されるケーブルロック，サーバーケースのロックなど，さまざまなデバイスにまで及ぶ．	ピッキング，スナップガンによるロック強制
392	バンピング	バンプキーを使用しビルや施設の施錠・開錠を行う．バンピングとはロック内のピンを一時的な位置合わせに落としロックを開くことを可能にする特殊なタイプのキーを使用することである．	なし

次ページに続く

前ページからの続き

ID	タイトル	概要	具体的な攻撃（例）
410	情報の抽出	ソーシャルエンジニアリング手法の組み合わせを使用する．詳細な知識と組み合わせた信憑性のある偽装は，攻撃の成功確率を増加させる．	プリテキスティング（カスタマーサービスの偽装，宅配便の偽装など）
416	人間の行動を操作	人間の心理的性質を利用し，1. 標的となる個人・グループに影響を与え情報を取得，2. 標的を操作して攻撃者に役立つアクションを実行させる．標的が情報を直接共有するようにするか，重要な情報を意図せずに漏洩させる．	知覚･認知へ影響を与える，インセンティブ（金銭的な詐欺等），フレーミング技法
438	製造時の変更	サプライチェーンにおける一部のエンティティに対する攻撃を行う目的で製造段階の技術，製品，コンポーネントを変更する．	製品等のデザインの変更，開発中に製品等を変更
439	配布中の操作	流通経路のある段階で製品，ソフトウェア，技術の完全性を攻撃する．最終的に資産が提供される際に複数のサプライヤや企業を経由する可能性があるため，多くの流通段階から生起する．	悪意のあるハードウェアコンポーネントに交換，悪意のあるソフトウェアの埋込
440	ハードウェア完全性攻撃	標的に導入・使用されているハードウェアに攻撃を実行するため，テクノロジー，製品，コンポーネント，サブコンポーネントを変更する．	ハードウェアをハッキング，悪意のあるハードウェアの更新
441	悪意のあるロジックの挿入	悪意のあるロジックをシステムの一見正しいコンポーネントにインストール・追加する．このロジックはシステムのユーザから隠され，画面の裏で悪影響を与える動作を実行する．	製品ソフトウェア・ハードウェア・メモリに悪意のあるロジック（トロイ等）を挿入
466	同じ発信元ポリシーを迂回する中間者攻撃を活用	被害者のブラウザで同じ発信元ポリシーの保護をバイパスするため，中間者攻撃を利用する．この攻撃は，セッション固定化とキャッシュポイズニング攻撃を有効にするためにも使用できる．	なし

次ページに続く

前ページからの続き

ID	タイトル	概要	具体的な攻撃（例）
507	物理的な窃盗	物品の窃盗によってシステム・デバイスに物理的にアクセスする．システム・デバイスの所持は，多くの攻撃のを実行可能にし，攻撃者に長期の時間を提供する．	なし
548	情報資源の侵害	認可されていない分類/機密性の情報を取り扱わせることで，（デバイスやネットワークを含む）システムを侵害する．情報へのアクセスが未許可の個人に公開され，流出の調査中はシステムを利用できなくなる．	なし
549	コードのローカル実行	組織の情報テクノロジ環境における既知の脆弱性を利用する標的型マルウェアを開発する．標的型マルウェアは，特に，テクノロジ環境について収集された情報に基づいている．	標的型マルウェア（サービスなどのインストール，ログオン時に実行など）
554	機能のバイパス	システムを保護するために意図された機能の一部・全部をバイパスすることでシステムを攻撃する．多くの場合，システムユーザは保護が適切であると考えているが，攻撃者はその保護機能を無効にしている．	エバークッキー，マイクロサービスの悪用，透過的なプロキシの悪用
586	オブジェクトインジェクション	オブジェクトのシリアル化処理中に追加の悪質なコンテンツを注入する．開発者はデータや状態を静的なバイナリ形式に変換してディスクに保存，ネットワーク経由で転送するためにシリアル化を利用する．	なし
594	接続リセット	標的の接続の片方または両方に接続リセットパケットを注入する．攻撃者は標的サーバ・宛先サーバの間でトラフィックを直接フィルタリングする必要がなく，接続を切断することができる．	TCP RST インジェクション

次ページに続く

前ページからの続き

ID	タイトル	概要	具体的な攻撃（例）
607	妨害	システムコンポーネント間のやり取りを妨害する．システム間の相互作用を中断・無効にすることで，1. システムが劣化状態になる．2. 障害を引き起こす．	デバイス等の物理的破壊，ジャミング，ネットワークルートの無効化
624	フォルトインジェクション	破壊的な信号・イベント（電磁パルス，レーザパルス，クロックグリッチなど）を使用して，電子デバイスの誤動作を引き起こす．暗号操作を行うデバイスの場合，この誤動作により秘密鍵情報を導出することができる．	モバイルデバイスへのフォルトインジェクション

以上

D　IoT・ポリー：対策カード一覧

ID	タイトル	概要	主な脅威対象
TM-01	ハードウェアセキュリティ	ハードウェアベースの不変的な「Root of Trust ※」を導入．※ハードウェア／ソフトウェアのセキュリティ分野では，信頼性を実現する根幹となる部分を「Root of Trust」と呼ぶ.	物理攻撃，災害　，機能停止
TM-02		機器の保護・完全性を強化した組み込みハードウェアを使用例：1. 乱数生成（Random Number Generation：RNG），2. 改ざん検知，3.TEE（Trusted Execution Environment）など	物理攻撃，災害，機能停止
TM-03		他ソフトウェア・実行可能プログラムの信用 (Trust) 要求前にブート環境の信用を確立するため，セキュリティ侵害のない状態の検証・判定を行うブート環境を実装する.	障害/誤作動，　機能停止，　不正行為/不正使用

次ページに続く

前ページからの続き

ID	タイトル	概要	主な脅威対象
TM-04		以下の機能を有する暗号化コード署名を実装：1. 機器の安全性を証明する署名後に改ざんがないことの保証，2. 実行時の保護，3. 読込み後に悪意のある攻撃でコードの上書きがないことを確認するセキュアな実行後監視	不正行為/不正使用，盗聴/傍受/ハッキング
TM-05	信頼性および完全性管理	未承認ソフトウェアおよびその読込型ファイルの起動を防止するソフトウェアにインストール管理機能を実装，未認証ソフトウェアを許可する場合，制限付きアクセス権/サンドボックスのみで稼働	機能停止，不正行為/使用，盗聴/傍受/ハッキング
TM-06		セキュリティ違反の発生後・アップグレードの失敗時に既知の安全な状態までシステムを回復する機能を実装	機能停止，不正行為/使用，盗聴/傍受/ハッキング
TM-07		信頼性・信頼関係を管理可能なプロトコルやメカニズムを活用する．各通信チャンネルはサポートするセキュリティ要件と同等レベルまで信頼できるものでなければならない．	不正行為/不正使用，盗聴/傍受/ハッキング
TM-08	強固な初期設定セキュリティおよびプライバシー	適用可能なセキュリティ機能はデフォルトで有効にする．不使用または安全でない機能はデフォルトで無効にする．	機能停止，不正行為/使用，障害/誤作動
TM-09		解読困難な機器別初期設定パスワードを確立する．複数機器に同一のものを使用した場合，解読困難な初期設定パスワードであっても脆弱性が高くなる．	機能停止，不正行為/使用，障害/誤作動
TM-10		公平かつ合法的に個人データの収集および処理を行う．データの主体の合意がない状態でデータの収集，処理してはならない．	損害/損失 (IT 資産)，不正行為/不正使用

次ページに続く

前ページからの続き

ID	タイトル	概要	主な脅威対象
TM-11		収集した個人情報について以下の措置を確認する．1. 特定目的に沿ったデータ使用，2. 個人データの追加の処理に互換性がある，3. データ対象者に対する十分な情報の提供	損害/損失 (IT 資産)，不正行為/不正使用
TM-12	データ保護および適合性	収集･保有するデータを最小限にする．IoT 利害関係者は集約したデータのみを必要とし，IoT 機器が収集した生データは必要としないため，データ抽出後，早急に生データを削除する．	損害 / 損失 (IT 資産)
TM-13		IoT 利害関係者は EU 一般データ保護規則 (GDPR) を遵守する．関連する利害関係者は，単一の個人データ処理における法的責任の明確な分配を要求する．	損害 / 損失 (IT 資産)，不正行為 / 不正使用
TM-14		IoT 製品/ユーザが以下の権利を行使できるようにする．1. 情報のアクセス・消去・修正，データ可搬性，処理制限，2. 処理に対する異議申立権，3. 自動化処理上で評価されないようにする権利	損害/損失 (IT 資産)，不正行為/不正使用
TM-15		システム・運用の中断を考慮して設計を行う．システムが容認し難い怪我・物理的損害を防止し損害から環境を保護するため，誤作動がない状態を保証するフェイルセーフ設計を行う．	機能停止，障害/誤作動，災害
TM-16	システム安全性および信頼性	故障，誤作動，悪化した状態からの復旧のため，自己診断･自己修復/回復メカニズムを実装する．	機能停止，障害/誤作動
TM-17		スタンドアロン運用を実現する．重要な機能は通信の喪失状態でも機能し続け，侵害されたデバイスやクラウドベースのシステムによる悪影響を記録する．	機能停止　，障害/誤作動

次ページに続く

前ページからの続き

ID	タイトル	概要	主な脅威対象
TM-18		更新について以下を確認する．1. デバイスソフトウェア/ファームウェア，設定等に OTA をアップデートする機能があること，2. アップデートサーバの安全性，3. 安全な接続を介した送信，4. 重要データがないこと等	機能停止，障害/誤作動，不正行為/不正使用，盗聴/傍受/ハッキング
TM-19	安全性の高いソフトウェア・ファームウェア更新	自動ファームウェア更新メカニズムを提供する．機器のファームウェア更新の有無を頻繁に確認する設定とする．初期設定で自動ファームウェア更新を有効にする．	機能停止，障害/誤作動
TM-20		ファームウェア更新に下方互換性を持たせる．ユーザに無断でユーザ設定，セキュリティ・プライバシー設定を変更する自動ファームウェア更新を回避する．ユーザは更新を承認，認可，拒否できる．	機能停止，障害/誤作動
TM-21		システムレベルの脅威モデルに基づき認証・承認プログラムを設計する．デバイスにはバックエンドサービス・サポートアプリケーションを確実に認証するメカニズムを含める．	障害/誤作動，不正行為/不正使用，盗聴/傍受/ハッキング
TM-22		初期設定時に既定パスワード/既定ユーザー名が変更されていることを確認する．弱い，無効な，空のパスワードの使用を禁止する．	障害/誤作動，不正行為/不正使用，盗聴/傍受/ハッキング
TM-23		強固なパスワード・個人識別番号 (PIN) を使用した認証メカニズムを有する．スマートフォンのように二要素認証 (2FA) や多要素認証 (MFA)，生体認証，証明書の使用を検討する．	障害/誤作動，不正行為/不正使用，盗聴/傍受/ハッキング
TM-24	認証	認証証明書（パスワードに限定されない）はソルト化，ハッシュ化，暗号化されなければならない．	障害/誤作動，不正行為/不正使用，盗聴/傍受/ハッキング

次ページに続く

前ページからの続き

ID	タイトル	概要	主な脅威対象
TM-25		合理的回数の無効なログイン試行後にユーザや機器サポートアカウントを一時使用制限・無効化する．ログイン失敗後に再ログインまでの一定待機時間を設定し，不正ログイン攻撃から保護する．	障害/誤作動，不正行為/不正使用，盗聴/傍受/ハッキング
TM-26		パスワードの回復・リセットメカニズムが堅牢であることを確認し，攻撃者に有効なアカウントを示す情報を提供しない．主要な更新および回復メカニズムにも同様に適用する．	障害/誤作動，不正行為/不正使用，盗聴/傍受/ハッキング
TM-27	承認	指定されたシステムの認可された活動のみ実行できるようにアクセス制限を施す．(例：情報所有者がオンラインユーザグループによりアクセスされる共有ファイルの更新可能な人物を決定) 代表的な機能：ABAC，RBAC	障害/誤作動，不正行為/不正使用，盗聴/傍受/ハッキング
TM-28		アクセス権が不要なファームウェアから特権コード，プロセス，データを分離できるように機器のファームウェアを設計する．ハードウェアは特権がないユーザの機密コードへのアクセスを防ぐ分離機能を有する．	障害/誤作動，不正行為/不正使用，盗聴/傍受/ハッキング
TM-29		アクセス制御によりデータの完全性および機密性を強化する．アクセス権を要求する対象者に特定プロセスのアクセス権限を承認する際，明確なセキュリティ方針を強制する．	物理攻撃，障害/誤作動，不正行為/不正使用，盗聴/傍受/ハッキング
TM-30		様々な重要度に影響を及ぼすコンテキストベースのセキュリティ対策およびプライバシー対策を確保する．(例：非常事態，ホームオートメーション)	障害/誤作動，不正行為/不正使用，盗聴/傍受/ハッキング，損害 / 損失 (IT 資産)

次ページに続く

前ページからの続き

ID	タイトル	概要	主な脅威対象
TM-31	アクセス制御－物理的および環境的セキュリティ	遠隔から管理を必要とする機器，ゲートウェイ等の改ざん保護・検知の機能を実装する．ハードウェア改ざんの検知・対応はネットワーク接続に依存してはならない．	物理攻撃，不正行為/不正使用
TM-32		機器の容易な分解やデータ記憶媒体の容易な取り外しが困難であること，保存データの暗号化を確認する．機器の盗難時にデバイスのコンテンツを遠隔からロックまたは削除するなどの機能を有する．	物理攻撃，不正行為/不正使用
TM-33		機器は機能に必要な物理的外部ポート (USB など) のみを有していることを確認する．安全なテスト/デバッグモードの確保し，機器への不正なアクセスを不可能にする．	物理攻撃，障害/誤作動，盗聴/傍受/ハッキング
TM-34	暗号化	送信中・保存中のデータ・情報 の機密性，信頼性，完全性の保護のため適切・効果的な暗号化を適用する．標準化され，強力な暗号化アルゴリズムと強力な暗号鍵を適切に選択し，安全ではないプロトコルを無効にする．	不正行為/不正使用，盗聴/傍受/ハッキング
TM-35		暗号鍵を安全に管理する．暗号化鍵の管理は鍵の生成，配布，保管，保守管理を含む．	不正行為/不正使用，盗聴/傍受/ハッキング
TM-36		軽量な暗号化とセキュリティ技術 (セキュアな ID，設定など) に互換性がある機器を構築する．一方で管理作業を最小化し，ユーザビリティを最大化する．	不正行為/不正使用，盗聴/傍受/ハッキング
TM-37		拡張可能な鍵管理計画をサポートする．極小型センサノードには制限が多く，全セキュリティ機能の実装が不可能であることを考慮する．	不正行為/不正使用，盗聴/傍受/ハッキング

次ページに続く

前ページからの続き

ID	タイトル	概要	主な脅威対象
TM-38		ネットワーク上の送信中情報・IoT アプリケーションやクラウドの保存情報に対するセキュリティ要件を保証する．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．	障害/誤作動，不正行為/不正使用，盗聴/傍受/ハッキング
TM-39		暗号化用 TLS などの最新の標準化セキュリティプロトコルを利用し通信セキュリティを確保する．	盗聴/傍受/ハッキング，損害 / 損失 (IT 資産)
TM-40		認証情報が内部・外部ネットワーク通信上で漏洩しない状況を確保する．	盗聴/傍受/ハッキング，損害 / 損失 (IT 資産)
TM-41		信頼性の高い情報交換を実現化するため，データ認証を保証する (データ送受信，双方向)．1 対 1 のデータ送信だけでなく，複数ノードによりデータが処理等されるため，データの保存時，常時データを署名する．	盗聴/傍受/ハッキング，不正行為/不正使用
TM-42	安全性および信頼性の高い通信	受信データを信用することなく，常時全ての相互接続性を検証する．信頼関係の確立前にネットワーク接続機器の検出，特定，検証/認証を実施し，信頼性の高いサービスの完全性を維持する．	障害/誤作動，不正行為/不正使用，盗聴/傍受/ハッキング
TM-43		IoT 機器は通信を制限する機能が必要．可能な場合，初期設定でインバウンド接続を到達不可能にすべきである．	不正行為/不正使用，盗聴/傍受/ハッキング
TM-44		全プロトコルレベルで製品・製品に接続した機器への不正接続を防止する．他機器・基盤・サービスとの初期相互認証 (Paring)，接続する場合，IoT 機器による通知の提供およびユーザ承認を必要とする．	不正行為/不正使用，盗聴/傍受/ハッキング

次ページに続く

前ページからの続き

ID	タイトル	概要	主な脅威対象
TM-45		選択的な接続のための特定ポート・ネットワーク接続を無効にする．必要に応じ，最終的な実装時にユーザに本プロセスの実施の手引きを提供する．	不正行為/不正使用，盗聴/傍受/ハッキング
TM-46		レート制限，自動化された攻撃のリスクを低減するためにネットワークにより送受信トラフィックを管理する．	不正行為/不正使用，盗聴/傍受/ハッキング
TM-47		ネットワークコンポーネントを分割し，セキュリティ違反の探知・全体的なリスクの最小化を実現する．性能向上・セキュリティ強化のため，サブネットワークによりネットワークを分割する．	盗聴/傍受/ハッキング
TM-48		スマートオブジェクトを同一機器として展開するため，単一機器への不正アクセス時，装置全体に影響を及ぼすことのないプロトコルを設計する．	盗聴/傍受/ハッキング
TM-49		単一機器への不正侵入が製品群全体に拡大する可能性があるため，製品群全体における同一秘密鍵の設定を回避する．	盗聴/傍受/ハッキング
TM-50		必要ポートのみが公開され，利用可能な状態を確保する．	障害/誤作動，盗聴/傍受/ハッキング
TM-51	安全性の高いインターフェースおよびネットワークサービス	自機器，他機器，ローカルまたは他ネットワークユーザに影響を及ぼすサービスへの DDoS 攻撃から保護するため，DDoS 耐性型インフラ・負荷分散型インフラを導入する．	不正行為/不正使用
TM-52		Web インターフェースが機器からバックエンドサービスに至るユーザセッションを完全に暗号化し，XSS，CSRF，SQL インジェクションなどの影響を受けないことを確認する．	不正行為/不正使用

次ページに続く

前ページからの続き

ID	タイトル	概要	主な脅威対象
TM-53		エラーメッセージはユーザが必要とする簡潔な情報のみを提供/表示する．エラー ID，Web サーバのバージョンなど攻撃者が悪用可能な機密情報の公開を避ける．	不正行為/不正使用
TM-54	安全性の高い出入力処理	データ入力検証 (使用前にデータの安全性を保証) および出力のフィルタリング機能を実装する．	不正行為/不正使用，障害/誤作動
TM-55	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．ログは永続的に記憶装置に保存され，認証済み接続を経由して取得する．	損害 / 損失 (IT 資産)
TM-56	監視および監査	機器動作の検証，マルウェア検知，整合性エラーの検出のため，定期的に監視する．	損害 / 損失 (IT 資産)
TM-57		1. セキュリティ関連イベントの監査，システム異常の監視・追跡の実施，2. コントロールの有効性を確認するために定期的な監査・評価を実施，3. 少なくとも年 2 回の侵入テストの実施	損害/損失 (IT 資産)，不正行為/不正使用
OP-01	生産終了サポート	IoT 製品向け生産終了戦略を策定する．開発者は初期段階から製品終了プランを作成・通達し，製造業者・消費者が機器のサポート期間後のリスクを認識可能にする．	障害/誤作動
OP-02		存続期間，終了間近なセキュリティ，修正サポート (製品保証外) を開示する．上記の開示はデバイスの予想寿命に合わせ，購入前に消費者に通知する．	障害/誤作動
OP-03		製品ライフサイクル「サポート終了」期間まで性能を監視し，既知の脆弱性を修正する．	障害/誤作動，不正行為/使用，損害/損失 (IT 資産)

次ページに続く

前ページからの続き

ID	タイトル	概要	主な脅威対象
OP-04	実証済みソリューション	実証済みソリューション (例：科学界が承認した周知の通信プロトコル・暗号アルゴリズムなど) を使用する．カスタム暗号化アルゴリズムなど，特定の専用ソリューションの利用を回避する．	損害/損失 (IT 資産)，不正行為/不正使用
OP-05	セキュリティ脆弱性・インシデントの管理	セキュリティインシデントの分析手順/処理手順を確立する．セキュリティインシデント発生時に迅速・効果的に対応できるように管理基準を確立する．	障害/誤作動，損害 / 損失 (IT 資産)
OP-06		特定の脆弱性に対応するため，関連する対策を含んだ調整済みの脆弱性を開示する．開示方針は開発者，製造業者，サービス供給業者が関与し，CSIRT への報告済み脆弱性に関する情報も含む．	障害/誤作動，不正行為/使用，損害/損失 (IT 資産)
OP-07		情報共有プラットフォームに参加し，脆弱性報告・官民連携組織からの現行サーバへの脅威/脆弱性に関する重要情報を適時に受領する．	損害 / 損失 (IT 資産)
OP-08		脆弱性報告を目的とした公開メカニズムを構築する．例：企業独自の内部セキュリティチームによる捕捉が困難な脆弱性を特定するため，クラウドソーシング手法を用いたバグ報奨金プログラムを利用する．	損害/損失 (IT 資産)
OP-09		人的な訓練によりプライバシーとセキュリティの順守を促進する．技術的専門知識とセキュリティ知識が必ずしも同等ではないことを認識させる．	不正行為 / 不正使用

次ページに続く

前ページからの続き

ID	タイトル	概要	主な脅威対象
OP-10	人的資源セキュリティ訓練および認識	プライバシーおよびセキュリティ研修活動を文書化し監視する.	不正行為/不正使用
OP-11		全従業員に対するサイバーセキュリティの任務/責任を確立する．事業の特性・セキュリティの工学的な必要性に合致するように人員を割り当てる.	不正行為/不正使用
OP-12	第三者との関係性	第三者の処理データ (例：組織がクラウド電子メールプロバイダーを利用した場合) は第三者とのデータ処理契約による保護が必要	障害/誤作動
OP-13	第三者との関係性	製品機能/サービス運用の使用に必要で制限がない場合に限り，消費者の同意を得て第三者と消費者の個人情報のみを共有する．第三サービス提供業者に同一のセキュリティ方針の適用を要求する.	障害/誤作動，損害/損失 (IT 資産)
OP-14		IoT ハードウェア製造業者/IoT ソフトウェア開発者はサプライチェーンのリスク管理ポリシーを適用し，サプライヤー等にセキュリティ要件を報告する.	不正行為/使用，機能停止，盗聴/傍受/ハッキング

以上

E　セキュ・ワン：攻撃カード Type A 一覧

No.	概要
1	未保護の新規システムを継続的にスキャンし，脆弱性を悪用
2	パッチ処理が未完で，セキュリティ設定が不適切なクライアントソフトウェアの脆弱性を悪用
3	継続的に脆弱性の高いソフトウェアをスキャンし，脆弱性を利用して対象マシンを侵害

次ページに続く

前ページからの続き

No.	概要
4	マルウェア感染したマシンから他の脆弱なマシンを特定し，侵害
5	システムの脆弱なデフォルト設定を悪用
6	継続的な脆弱性評価や修正が未実施で，重要パッチが未適用のシステムの脆弱性を悪用
7	対策の有効性測定や継続的改善が未実施の標的を攻撃
8	悪意あるコードにより対象マシンを侵害し，機密データを取得
9	業務に不必要なリモートアクセス可能なサービスを詳細にスキャンし，攻撃ルートを用意することでセキュリティを侵害
10	SQL インジェクション，クロスサイトスクリプティングなどにより脆弱なアプリケーションソフトウェアを悪用
11	無線アクセスポイントや無線クライアントシステムの脆弱性を悪用し，内部ネットワークに侵入
12	ソーシャルエンジニアリングによりユーザやシステム管理者を欺く
13	一時的に例外を認めたが修正されず，セキュリティ設定が脆弱なネットワークデバイスを悪用
14	フィッシングメールにより対象マシン上で悪意あるコードを管理者権限で実行
15	インターネットからアクセス可能な DMZ 上のシステム経由で内部ネットワークの深部まで侵入
16	未保護の接続，脆弱なフィルタリング設定などの不適切なネットワークアーキテクチャの設定を悪用
17	ログ収集およびログレビューが未実施の標的システム上で，長時間，検知されることなく活動
18	機密情報を適切に特定せず未保護な組織の機密文書にアクセス
19	一時雇用者，請負業者，元従業員などが残した非アクティブアカウントを悪用
20	パスワード推測，パスワード解析，権限昇格の脆弱性を突く攻撃により管理者権限を取得し，他のマシンにも被害を拡大
21	システムの内部にアクセスし，検知されることなく機密情報を収集
22	システムを侵害し，重要データを改ざんすることで組織の信頼性を侵害
23	効果的対応能力を持たない組織内で検知されずに活動を継続

以上

F　セキュ・ワン：攻撃カード Type B 一覧

No.	タイトル	概要
1.1	初期偵察：発掘	システム情報の解明のため，標的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
1.2	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
1.3	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
1.4	初期偵察：プロトコル分析	システムが使用する通信プロトコルの情報を調査・解読
1.5	初期偵察：フィンガープリント	標的からの出力と既知のインジケータを比較し，標的の情報を特定
1.6	初期偵察：情報抽出	ソーシャルエンジニアリリングにより，標的組織および個人に関する重要な情報を取得
2.1	ツール開発/取得	攻撃の効率化を図るため，ツールを開発または取得し，使用
3.1	配送：コンテンツスプーフィング	フィッシングサイト等の偽装コンテンツを表示
3.2	配送：アイデンティティスプーフィング	窃取または，なりすました認証情報を使用し，メッセージや署名付きファイルを送付
3.3	配送：リソースロケーションスプーフィング	ブラウザに偽のアドレスを表示する等により利用者に意図しない場所からリソースを取得させる
3.4	配送：アクションスプーフィング	目に見えない（非表示の）インターフェースを利用して意図しない動作を実行
3.5	配送：人間の行動を操作	人間の心理につけこみ，標的から情報を収集または標的を操作して利益を獲得
3.6	配送：ドライブバイ攻撃	ユーザのブラウジング操作により Web サイトを介してシステムにアクセス
3.7	配送：公的なアプリケーションの悪用	インターネットに接続したシステムなどの脆弱性を突くソフトウェア，データ，コマンドにより意図しない動作を誘発
3.8	配送：ハードウェアの追加	初期アクセスのために悪意のあるハードウェアを追加
3.9	配送：リムーバブルメディアを介した複製	マルウェアに感染したリムーバブルメディアの挿入時に自動再生機能を悪用することでシステムに侵入

次ページに続く

前ページからの続き

No.	タイトル	概要
3.10	配送：スピアフィッシング	ファイルまたはリンクをスピアフィッシング E メールに添付，または，さまざまな SNS，Web メール，企業が管理しないその他のサービスを介してメッセージを送信
3.11	配送：サプライチェーンの侵害	最終消費者が受領する前の製品または製品配送メカニズムを侵害
3.12	配送：有効なアカウント	ソーシャルエンジニアリングにより資格情報を取得
4.1	初期侵害：防御回避	シグネチャベースによる検出回避のため，バイナリパディングによりファイルハッシュを変更
4.2		形跡を消すため，レジストリ・コマンドヒストリ・イベントファイル・マルウェア自身等を削除（history –c，ファイル削除 (DEL コマンド)，ファイルの隠蔽 (attrib +h) ）
4.3		OS やアプリケーションの機能を利用し，セキュリティツールによる悪意のある動作の検出を防止（CMSTP.exe，Compiled HTML files (.chm)，DLL Search Order Hijacking，Extra Window Memory，DACLs）
4.4		悪意のあるコードを難読化・暗号化し，コードの分析から回避
4.5		悪意のあるプログラムのタイムスタンプを改ざんし，分析から回避
4.6		セキュリティツールを無効化し，悪意のあるアクティビティの検出を回避
4.7		コードサイニング証明書を使用してマルウェアやツールを正規のバイナリとして偽装
4.8		ログや隔離済みマルウェアなどのホストシステム上で生成されたアーティファクトを削除または変更
4.9		難読化されたファイルまたは情報により侵入のアーティファクトの分析を回避（Scripting，PowerShell，システム上に存在するユーティリティ）

次ページに続く

前ページからの続き

No.	タイトル	概要
4.10		ルートキットによりプログラム，ファイル，ネットワーク接続，サービス，ドライバ，その他のシステムコンポーネントの存在を隠蔽
4.11		開発，デバッグ，リバースエンジニアリングを支援するソフトウェア関連ユーティリティを悪用し，悪意のあるコードを実行（MSBuild，WinDbg / CDB，Tracker）
4.12		ネットワーク管理目的で使用するサードパーティアプリケーションやソフトウェア開発システムを悪用し，制御コードを実行
4.13		標的が使用する OS やアプリケーションの機能・仕組みを悪用し，標的を制御するコードを実行（CMSTP.exe, API, DLL, コマンドラインツール, .chm, タスクスケジューラ，Dynamic Data Exchange，PowerShell）
5.1	誤用/特権昇格	動的ライブラリの仕組みを利用し，他のプロセスに悪意のあるコードをロードさせ，実行（Windows DLL search order，AppInit DLLs value，AppCert DLLs，SID-History Injection）
5.2		不適切なファイルシステムのパーミッションを利用し，管理者権限で起動するプロセスをユーザ権限で改ざん
5.3		不適切なレジストリのパーミッションを利用し，管理者権限で起動するプロセスを登録
5.4		資格情報アクセス技術を使用して，特定アカウントの資格情報を窃取（アクセストークン操作，アカウント制御の回避，sudo キャッシング，有効なアカウントの悪用）
5.5		OS やアプリケーションの機能または脆弱性を悪用し，アカウントの権限を昇格（Web Shell，Extra Window Memory インジェクション，Application Shimming）

次ページに続く

前ページからの続き

No.	タイトル	概要
5.6		昇格した特権にアクセスするため，起動プロセスのアドレス空間で任意のコードを実行するプロセスインジェクションを実行
6.1	内部偵察：資格情報アクセス	アカウント情報が保存されているファイルや履歴を調査例）資格情報のダンプ: Mimikatz
6.2		ネットワークスニファにより，非暗号化通信で送信される資格情報を収集
6.3		アカウントへのアクセスのため，総当たり攻撃を使用
6.4		アクセス権限を持った攻撃者が攻撃に使用するアカウントを作成
6.5		端末に保存されている秘密鍵にアクセス
6.6	内部偵察：発見	認証メカニズムまたは OS の脆弱性を悪用し，資格情報とアクセス権を取得（SMB, Keychains, Hooking, LLMNR/NBT-NS Poisoning）
6.7		レジストリにアクセスし，システム情報またはインストールされているソフトウェアの情報を発見
6.8		追加攻撃またはシステム環境の詳細を知るため，端末に接続されている周辺機器を発見
6.9		コマンドを使用し情報を発見（アカウント: net user，ディレクトリ: dir，ネットワーク共有: net share，PW ポリシー: net accounts，プロセス: tasklist，遠隔システム: ping，システム時間: net time）
6.10		リモートホストで実行されている脆弱なサービスの一覧を入手
7.1	侵入拡大	システムの認証の仕組みを悪用し，ネットワーク上の別端末を侵害 (Login Scripts，Pass the Hash，Pass the ticket)
7.2		リムーバブルメディアの自動実行機能を悪用し，クローズドシステム等にマルウェアを拡散
7.3		ソフトウェアの脆弱性を突きリモートシステム上でコマンドやバイナリを実行し，システム侵害を拡大

次ページに続く

前ページからの続き

No.	タイトル	概要
7.4		標的が使用する OS やアプリケーションの機能・仕組みを悪用し，システム侵害を拡大 (AppleScript，DCOM，RDP，FTP，scp，SSH，RPC)
7.5		共有された感染コンテンツの実行によりリモートシステム上で攻撃者のコードを起動
7.6		Web サイトのディレクトリなどのファイル共有を介して，内部でアクセス可能な Web サイトに悪質なコンテンツの追加・ブラウザでの閲覧により悪質なコンテンツを実行
8.1		悪意のあるファイルに隠れファイル・ディレクトリ属性を付与し，利用者から隠蔽
8.2		OS，BIOS の外部で悪意のあるコードを実行する悪質なファームウェアをインストール
8.3		OS の起動時に動作するプロセス・スクリプト一覧に悪意のあるプログラム・スクリプトを追加（Startup Items，Logon Scripts，Office Application Startup，Login Item，Web Shell）
8.4	持続性確立	OS およびアプリケーションの機能を悪用（BITS，Browser Extensions，Loadable Kernel Modules，Scheduled Task）
8.5		OS の下層で動作するルートキットを悪用して，永続的にシステムにアクセス
8.6		リモートサービスを使用して持続的にネットワークにアクセス（VPNs，Citrix）
8.7		十分なアクセス権限を持つ攻撃者によりローカル・ドメインアカウントを作成
9.1		標的で使用可能な API により音声やクリップボード，スクリーンキャプチャなどの情報を収集
9.2		標的の内部情報を効率よく収集するために自動化技術を活用
9.3	任務目的実行：収集	標的内のローカルドライブ・リモートドライブ・リムーバブルメディアから情報を収集
9.4		脆弱性を有するブラウザの機能を悪用し，マン・イン・ザ・ブラウザ技術によりコンテンツの変更・挙動を改変，情報を傍受

次ページに続く

No.	タイトル	概要
9.5		データ抽出前にデータを集約：別々のファイルに保存，データ圧縮・データ暗号化などの手法で 1 つのファイルに集約
9.6	任務目的実行：情報流出	データの暗号化・圧縮・転送サイズ制限により，標的に気づかれないように情報を取得
9.7		任意の通信プロトコルを使用し，情報を収集
9.8		攻撃通信と通常のアクティビティを混在させるため，一日の特定の時間，特定の間隔でのみ実行
9.9	任務目的実行：遠隔操作	リムーバブルメディアによりクローズネットワークのホストを侵害し，コマンドおよび制御トラフィックを実行
9.10		コンピュータ上の通信ポートを介して，コマンドおよび制御トラフィックを送信
9.11		不適切に設定されているプロキシやファイアウォールを迂回するため非標準ポートを使用
9.12		異なるプロトコルにより通信を分割：受信コマンド・制御用のプロトコルと送信データ用プロトコル
9.13		データ転送しきい値を迂回するため，プライマリチャネルの代替通信チャネルを使用
9.14		カスタム暗号プロトコルまたはアルゴリズム，エンコーダー，難読化，プロキシを使用して，C2 トラフィックを隠蔽
9.15		既知の暗号化アルゴリズムを使用し，C2 トラフィックを隠蔽
9.16		侵入先のシステムへコマンドを中継する手段に既存の外部 Web サービスを悪用
9.17		正規のリモートアクセスソフトウェア（Team Viewer，Go2Assist，LogMein，AmmyyAdmin など）によりネットワーク内のシステムを標的とする対話型の C2 チャネルを確立
9.18		検出回避のため，プロキシにより C2 通信を管理し，同時アウトバウンドネットワーク接続の数を削減

以上

G　セキュ・ワン：対策カード一覧

No.	タイトル	防御段階	概要
1.1		特定	アクティブな検出ツールによりネットワークに接続されているデバイスを識別し，ハードウェア資産のインベントリを更新
1.2		特定	パッシブな検出ツールによりネットワークに接続されているデバイスを識別し，ハードウェア資産のインベントリを更新
1.3		特定	ハードウェア資産のインベントリを更新するため，DHCP サーバまたは IP アドレス管理ツールで DHCP ログを活用
1.4		特定	情報を保存・処理する可能性があるすべての資産の正確・最新の詳細なインベントリを更新
1.5	ハードウェア資産のインベントリと管理	特定	インベントリ更新に資産のネットワークアドレス，ハードウェアアドレス，マシン名，データ資産所有者，部門，資産のネットワーク接続の承認の有無を記録
1.6		反応	未許可の資産をネットワークから隔離，またはインベントリを適時に更新
1.7		防御	802.1x 規格に準拠したポートレベルのアクセス制御により，ネットワーク認証可能なデバイスを管理
1.8		特定	クライアント証明書により，組織の信頼されたネットワークに接続するハードウェア資産を認証
2.1		特定	ビジネス目的達成に必要なすべての認可されたソフトウェアの最新リストを維持
2.2		特定	ベンダーが現在サポートしているアプリケーションまたは OS のみが，組織の許可されたソフトウェアインベントリに含まれていることを確認

次ページに続く

前ページからの続き

No.	タイトル	防御段階	概要
2.3		特定	システム上の全ソフトウェアの一覧の取得を自動化するため，組織全体のソフトウェアインベントリツールを活用
2.4		特定	ソフトウェアインベントリシステムにより認可した OS を含む，すべてのソフトウェアの名前，バージョン，発行元，インストール日を追跡
2.5	ソフトウェア資産のインベントリ管理	特定	ソフトウェアインベントリシステムとハードウェア資産インベントリを統合するため，全デバイスと関連ソフトウェアを単一の機器で追跡
2.6		反応	承認されていないソフトウェアの削除，またはインベントリの適時更新
2.7		防御	承認されたソフトウェアのみが実行され，未承認のソフトウェアは実行されないようにアプリケーションのホワイトリスト技術を全資産に活用
2.8		防御	アプリケーションホワイトリストソフトウェアで承認されたソフトウェアライブラリ（* .dll，* .ocx，* .so 等）のみがシステムプロセスにロードされることを保証
2.9		防御	アプリケーションホワイトリストソフトウェアでデジタル署名済みの許可されたスクリプト（*.ps1，*.py，マクロ等）のみがシステム上で実行されることを保証
2.10		防御	物理的または論理的に分離されたシステムを使用して，業務に必要であるが組織へのリスクが大きいソフトウェアを切り離して実行
3.1		検知	最新の SCAP 準拠の脆弱性スキャンツールを使用し，週単位以上の頻度でネットワーク上の全システムを自動的にスキャンし，潜在的な脆弱性を特定

次ページに続く

前ページからの続き

No.	タイトル	防御段階	概要
3.2		検知	各システムのローカルで起動中のエージェント，または権限の昇格が設定されたリモートスキャナで認証された脆弱性スキャンを実行
3.3		防御	認証された脆弱性スキャンに使用する専用アカウントを他の管理者操作には使用せず，アカウントを特定の IP アドレスの特定のマシンに関連付ける
3.4	継続的な脆弱性管理	防御	OS がベンダーの提供する最新のセキュリティ更新プログラムを実行していることを確認するため，自動ソフトウェア更新ツールを展開
3.5		防御	サードパーティ製ソフトウェアがベンダーの提供する最新セキュリティ更新プログラムを実行していることを確認するため，自動化ソフトウェア更新ツールを展開
3.6		反応	繰り返し実施した脆弱性スキャンの結果を定期的に比較して，脆弱性が適時に修正されていることを確認
3.7		反応	リスク評価プロセスにより，発見された脆弱性の修正に優先順位を付ける
4.1		検知	自動化ツールにより，ドメインおよびローカルアカウントを含むすべての管理者アカウントを棚卸し
4.2		防御	新しい資産を展開する前に，全デフォルトパスワードを管理者レベルのアカウントと一致する値に変更
4.3		防御	管理者アカウントの権限を持つ全ユーザが昇格されたアクティビティに専用のアカウントまたはセカンダリアカウントを使用していることを確認

次ページに続く

前ページからの続き

No.	タイトル	防御段階	概要
4.4	管理者特権の管理された使用	防御	多要素認証がサポートされていない場合（ローカル管理者，ルート，サービスアカウントなど），アカウントには強力なパスワードを使用
4.5		防御	全管理者アカウントアクセスにマルチファクタ認証と暗号化されたチャネルを使用
4.6		防御	管理者は全管理タスクまたは管理アクセスを必要とする全タスクに専用マシンを使用
4.7		防御	スクリプティングツール（Microsoft PowerShell や Python など）へのアクセスをこれらの機能にアクセスする必要がある管理者または開発ユーザに制限
4.8		検知	管理者権限が割り当てられたグループに追加または削除があった場合，ログエントリと警告を発するようにシステムを設定
4.9		検知	管理者アカウントへのログイン失敗時にログエントリと警告を発するようにシステムを設定
5.1	ハードウェアとソフトウェアのセキュアな構成	防御	すべての認可された OS およびソフトウェアに関する標準化したセキュリティ構成基準を文書化し，維持
5.2		防御	組織の承認済みの構成基準に基づき，企業内の全システムのセキュアなイメージまたはテンプレートを維持
5.3		防御	イメージの許可された変更のみを確認するため，整合性を監視するツールで検証済みのセキュアなサーバにマスターイメージとテンプレートを格納
5.4		防御	スケジュールされた定期的な間隔で自動的にシステムに構成設定を強制し，再適用するシステム構成管理ツールを展開

次ページに続く

前ページからの続き

No.	タイトル	防御段階	概要
5.5		検知	全セキュリティ構成要素，承認された例外一覧，無許可の変更時の警告を検証するため，SCAP 準拠の構成監視システムを使用
6.1	監査ログの保守，監視，分析	検知	全サーバとネットワークデバイスが定期的に時刻情報を取得し，ログのタイムスタンプが一致するように，少なくとも 3 つの同期した時刻ソースを使用
6.2		検知	すべてのシステムとネットワークデバイスでローカルロギングが有効になっていることを確認
6.3		検知	イベントの情報源，日付，ユーザ，タイムスタンプ，送信元アドレス，宛先アドレス，その他の有用な要素など，詳細な情報をシステムログに記録
6.4		検知	ログを格納するすべてのシステムにログ用の十分な記憶領域があることを確認
6.5		検知	分析とレビューのため，適切なログが中央ログ管理システムに集約されていることを確認
6.6		検知	ログ相関と分析のため，SIEM またはログ解析ツールを導入
6.7		検知	定期的にログをレビューし，異常なふるまいや異常なイベントを特定
6.8		検知	使用可能なイベントをよりよく識別し，イベントノイズを減らすため，SIEM システムを定期的に調整
7.1		防御	完全にサポートされている Web ブラウザと電子メールクライアントのみが組織内で実行可能なことを確認
7.2		防御	ブラウザや電子メールクライアントの未許可なプラグイン，アドオンをアンインストールまたは無効化

次ページに続く

前ページからの続き

No.	タイトル	防御段階	概要
7.3		防御	すべての Web ブラウザと電子メールクライアントにおいて不必要なスクリプト言語の使用を制限
7.4		防御	未承認 Web サイトに接続するシステムの機能を制限するネットワークベースの URL フィルタを適用
7.5	電子メールと Web ブラウザの保護	防御	URL 分類サービスを用いて，利用可能な Web サイトカテゴリ定義が最新であることを確認し，未分類のサイトはデフォルトでブロックする
7.6		検知	インシデントハンドラが侵害されたシステムを特定するのを支援するため，オンサイト・モバイルデバイスに関わらず組織の各システムからの全 URL 要求を記録
7.7		防御	DNS フィルタリングサービスを使用し，既知の悪意のあるドメインへのアクセスをブロック
7.8		防御	有効なドメインを偽装または改ざんした電子メールを制限するため，SPF および DKIM 標準に基づく DMARC ポリシーおよび検証を実装
7.9		防御	ファイルの種類が組織のビジネスにとって不要な場合，組織の電子メールゲートウェイを通る電子メールの内，不要なファイル種類を含む添付ファイルをブロック
7.10		防御	サンドボックスを使用して，悪意のある行為を伴うインバウンド電子メールの添付ファイルを分析およびブロック
8.1		防御	集中管理されたマルウェア対策ソフトウェアを使用し，ワークステーションおよびサーバを継続的に監視および防御
8.2		防御	マルウェア対策ソフトウェアのスキャンエンジンおよびシグネチャデータベースを定期的に更新

次ページに続く

前ページからの続き

No.	タイトル	防御段階	概要
8.3		防御	OS で利用可能な DEP や ASLR などの不正使用防止機能を有効にするか，広範なアプリケーション等の保護が可能な適切なツールキットを展開
8.4	マルウェア対策	検知	挿入または接続時にリムーバブルメディアのマルウェア対策スキャンを自動的に実行するようにデバイスを設定
8.5		防御	リムーバブルメディアからコンテンツを自動実行しないようにデバイスを設定
8.6		検知	分析およびアラート通知のため，エンタープライズマルウェア対策管理ツールおよびイベントログサーバにすべてのマルウェア検出イベントを送信
8.7		検知	既知の悪意のあるドメインを含むホスト名のアクセスを検出するために DNS クエリのログを有効化
8.8		検知	Microsoft Powershell や Bash などのコマンドシェルのコマンドライン監査ログを有効化
9.1		特定	アクティブなポート，サービス，プロトコルを資産インベントリ内のハードウェア資産に関連付け
9.2		検知	検証され，ビジネスニーズがあるネットワークポート，プロトコル，サービスのみが各システムで実行されていることを確認
9.3	サービス等の制限と管理	検知	全システムに定期的に自動化されたポートスキャンを実行し，システム上で不正なポートの起動を検出した場合に警告する
9.4		検知	システムにホストベースのファイアウォールやポートフィルタリングツールを使用し，未許可のサービスやポートの全トラフィックを拒否するルールを適用

次ページに続く

前ページからの続き

No.	タイトル	防御段階	概要
9.5		検知	サーバに送信されるトラフィックを検証し正当性を確認するため，重要なサーバの前にアプリケーションファイアウォールを配置
10.1		防御	すべてのシステムデータが定期的に自動バックアップされることを確認
10.2		防御	システム全体を迅速に復旧できるように，主要なシステムのイメージングなどのプロセスを通じて完全なシステムとしてのバックアップを作成
10.3	データ復旧能力	防御	データの復元プロセスを実行することでバックアップの正常動作を確認し，定期的にバックアップメディアのデータ整合性をテストする
10.4		防御	バックアップの格納時およびネットワーク経由による移動時，物理セキュリティまたは暗号化によってバックアップが適切に保護されていることを確認
10.5		防御	全バックアップは少なくとも 1 つのバックアップ先があり，OS の呼び出しによって継続してアドレス指定できないようにする
11.1		特定	認可された全ネットワークデバイスに標準の文書化されたセキュリティ構成基準を維持
11.2		特定	トラフィックのネットワーク機器の通過を許可する全設定ルールは業務上の理由，業務の担当名，必要な期間とともに構成管理システムに文書化
11.3		検知	使用中のネットワーク機器ごとに定義されている承認されたセキュリティ構成と全ネットワークデバイス構成を比較し，変更が検出された場合，警告する

次ページに続く

前ページからの続き

No.	タイトル	防御段階	概要
11.4	ネットワーク機器のセキュアな設定	防御	すべてのネットワークデバイスに最新の安定版セキュリティ関連アップデートをインストール
11.5		防御	マルチファクタ認証と暗号化されたセッションを使用して，すべてのネットワークデバイスを管理
11.6		防御	ネットワークエンジニアがアクセスを必要とする全管理者タスクまたは権限昇格が必要なタスクに専用のマシンを使用
11.7		防御	ネットワーク機器の管理セッションに別々の VLAN，別の物理接続を用い，ビジネス使用とは別のネットワーク接続を介してネットワークインフラを管理
12.1	境界防御	特定	組織のすべてのネットワーク境界の最新インベントリを保持
12.2		検知	信頼可能な各ネットワーク境界の外側から定期的にスキャンを実行し，境界を越えてアクセスできる不正な接続を検出
12.3		防御	既知の悪意あるまたは未使用のインターネット IP アドレスとの通信を拒否し，各ネットワーク境界で信頼された IP アドレス範囲にのみアクセスを制限
12.4		防御	許可されていない TCP または UDP ポートまたはアプリケーショントラフィックに対する通信を拒否
12.5		検知	各組織のネットワーク境界を通過するネットワークパケットを記録するように監視システムを構成
12.6		検知	ネットワークベースの IDS センサーにより組織の各ネットワーク境界で異常な攻撃メカニズムを探索し，システムの侵害を検出

次ページに続く

前ページからの続き

No.	タイトル	防御段階	概要
12.7		防御	ネットワークベースの侵入防御システム（IPS）を展開して，各組織のネットワーク境界で悪意のあるネットワークトラフィックをブロック
12.8		検知	すべてのネットワーク境界デバイスでNetFlow およびロギングデータを収集できるようにする
12.9		検知	インターネットとの全ネットワークトラフィックが，未許可の接続をフィルタする認証済みアプリケーション層プロキシを通過することを確認
12.10		検知	境界プロキシで暗号化されたすべてのネットワークトラフィックを復号してから，コンテンツを分析
12.11		防御	組織のネットワークへアクセスするための全リモートログインアクセスは転送データを暗号化し，マルチファクタ認証を使用
12.12		防御	組織のセキュリティポリシーの強制を確認するため，ネットワークにアクセスする前にリモートログインを試みる全社内デバイスをスキャン
13.1		特定	オンサイトまたはリモートサービスプロバイダーに存在する情報を含む，システムによって保管，処理，送信される全機密情報のインベントリを管理
13.2		防御	組織から定期的にアクセスされない機密データやシステムをネットワークから削除
13.3		検知	機密情報の不正な転送を監視・転送を遮断・情報セキュリティの専門家に警告するネットワーク周辺機器に自動化ツールを導入

次ページに続く

前ページからの続き

No.	タイトル	防御段階	概要
13.4		防御	許可されたクラウドストレージまたは電子メールプロバイダにのみアクセスを許可
13.5	データ保護	検知	組織から出て行くすべてのトラフィックを監視し，暗号化の不正使用を検出
13.6		防御	承認されたディスク暗号化ソフトウェアを使用して，すべてのモバイルデバイスのハードディスクドライブを暗号化
13.7		防御	USB ストレージデバイスが必要な場合は，特定のデバイスのみを使用できるようにシステムを構成可能なエンタープライズソフトウェアを使用
13.8		防御	組織外のリムーバブルメディアをサポートするビジネス上の必要性がない場合，データを書き込まないようにシステムを設定
13.9		防御	USB ストレージデバイスが必要な場合は，そのデバイスに保存されているすべてのデータをセキュアに暗号化
14.1		防御	サーバに保存されている情報のラベルまたは分類レベルに基づいてネットワークを分割し，分離された VLAN 上にすべての機密情報を保存
14.2		防御	特定の目的のため，許可システムだけが必要な他システムと通信できることを保証するため，VLAN 間のファイアウォールフィルタリングを有効化
14.3		防御	隣接システムへ侵入拡大する攻撃者を制限するため，プライベート VLAN やマイクロセグメンテーション等によりワークステーションの相互通信を無効化
14.4		防御	転送中のすべての機密情報を暗号化

次ページに続く

前ページからの続き

No.	タイトル	防御段階	概要
14.5	知る必要性に基づくアクセスコントロール	検知	オンサイトやサービスプロバイダの情報を含むシステムが保存，処理，送信する全機密情報をアクティブ検出ツールで識別，インベントリを更新
14.6		防御	ファイルシステム，ネットワーク共有，アプリケーション，データベース固有のアクセス制御リストを用いてシステムに保存されている全情報を保護
14.7		防御	ホストベース Data Loss Prevention（DLP）等の自動ツールを使用し，データがシステムからコピーされてもコピーされたデータへのアクセス制御を強制
14.8		防御	情報にアクセスするため，OS に統合されていない二段階認証メカニズムを必要とするツールを使用して，全機密情報を保存時に暗号化
14.9		検知	機密データへのアクセスや機密データへの変更（ファイルの整合性監視，セキュリティ情報・イベント監視）の詳細な監査ログを適用
15.1		特定	有線ネットワークに接続されている許可された無線アクセスポイントのインベントリを管理
15.2		検知	有線ネットワークに接続されている不正ワイヤレスアクセスポイントを検出して警告を発するようにネットワーク脆弱性スキャンツールを構成
15.3		検知	ワイヤレス侵入検知システム（WIDS）を使用して，ネットワークに接続されている不正なワイヤレスアクセスポイントを検出し，警告する
15.4		防御	ワイヤレスアクセスのビジネス目的がない機器のワイヤレスアクセスを無効化

次ページに続く

前ページからの続き

No.	タイトル	防御段階	概要
15.5	無線アクセスコントロール	防御	ビジネス上必要なマシンに無線アクセスを設定し，承認済の無線ネットワークへのアクセスのみを許可し，他無線ネットワークへのアクセスを制限
15.6		防御	ワイヤレスクライアントでピアツーピア（アドホック）ワイヤレスネットワーク機能を無効化
15.7		防御	Advanced Encryption Standard（AES）を活用して，転送中のワイヤレスデータを暗号化
15.8		防御	ワイヤレスネットワークが相互認証，マルチファクタ認証を必要とする EAP/TLS などの認証プロトコルを使用
15.9		防御	ビジネス目的で必要とされる場合を除き，デバイスのワイヤレス周辺機器へのアクセス（Bluetooth や NFC など）を無効化
15.10		防御	個人用または信頼できないデバイス用に個別のワイヤレスネットワークを作成
16.1		特定	オンサイトまたはリモートサービスプロバイダに存在するものを含む，組織の認証システムのインベントリを管理
16.2		防御	ネットワーク，セキュリティ，クラウドシステムを含むすべてのアカウントのアクセスを可能な限り中央集中型の認証ポイントで構成
16.3		防御	オンサイトでの管理，サードパーティのプロバイダでの管理に依らず，全システム上の全ユーザアカウントに対してマルチファクタ認証を適用
16.4		防御	保存時にすべての認証資格情報を暗号化またはハッシュ化
16.5		防御	すべてのアカウントのユーザ名と認証資格情報が，暗号化されたチャネルを使用してネットワーク経由で送信されていることを確認

次ページに続く

前ページからの続き

No.	タイトル	防御段階	概要
16.6	アカウントの監視，管理	特定	認証システムにより，まとめられたすべてのアカウントのインベントリを管理
16.7		防御	従業員・請負業者の解雇・変更時に即時にアカウントを無効化しシステムアクセス権を取り消すための自動化されたプロセスを確立
16.8		反応	ビジネスプロセスやビジネスオーナーに関連付けられないアカウントをすべて無効化
16.9		反応	一定期間休止している休止状態のアカウントは自動的に無効化
16.10		防御	すべてのアカウントに監視および強制される有効期限が設定されていることを確認
16.11		防御	一定期間使用しないとワークステーションのセッションを自動的にロック
16.12		検知	監査ログを使用して非アクティブ化されたアカウントにアクセスする試みを監視
16.13		検知	時刻，ワークステーションの場所，ログイン間隔など，ユーザが通常のログイン動作から逸脱した場合に警告
17.1		-	スキルギャップ分析により，従業員が遵守していないスキルや行動を把握し，この情報を基にベースラインの教育ロードマップを構築
17.2		-	従業員のセキュリティ行動に積極的に影響を与えるため，特定されたスキルギャップに対処するための訓練を提供
17.3		-	組織のセキュリティを確保するために必要な行動やスキルを理解し発揮できるように，定期的に全従業員のセキュリティ意識向上プログラムを作成
17.4		-	新しい技術，脅威，標準，ビジネス要件に対応するため，組織のセキュリティ意識向上プログラムを頻繁に更新

次ページに続く

前ページからの続き

No.	タイトル	防御段階	概要
17.5		-	セキュアな認証を有効化し，利用することの重要性について，従業員を訓練
17.6	セキュリティ意識啓発プログラムの実施	-	フィッシング，電話詐欺，偽装電話などのさまざまな形態のソーシャルエンジニアリング攻撃を特定する方法について，従業員を訓練
17.7		-	機密情報を特定し，適切に保管，譲渡，破棄する方法について，従業員を訓練
17.8		-	モバイルデバイスの紛失や電子メールのオートコンプリートによる電子メール誤送信等，意図しないデータ漏洩の原因を認識するために従業員を訓練
17.9		-	従業員が最も一般的なインシデントのインジケータを特定し，インシデントを報告できるように従業員を訓練
18.1		-	使用するプログラミング言語および開発環境に適した安全なコーディングの履行を確立
18.2		-	社内で開発したソフトウェアはサイズ・データタイプ・許容範囲・フォーマット等，全入力に対してエラーチェックが実行され，文書化されていることを確認
18.3		-	外部から取得した全ソフトウェアのバージョンがサポートされていること，または開発者のセキュリティ推奨事項に基づき適切に強化されていることを確認
18.4		-	開発したソフトウェアには，最新の信頼できる第三者コンポーネントのみを使用
18.5		-	標準化され広範にレビューされた暗号化アルゴリズムのみを使用
18.6	アプリケーションソフトウェアセキュリティ	-	すべてのソフトウェア開発担当者が，安全なコードを書くトレーニングを受けていることを確認

次ページに続く

前ページからの続き

No.	タイトル	防御段階	概要
18.7		-	静的および動的分析ツールを適用して，内部開発されたソフトウェアのセキュリティ保護されたコーディング手法が遵守されていることを確認
18.8		-	セキュリティグループに連絡するための手段を提供するなど，ソフトウェア脆弱性の報告を受け入れて対処するプロセスを確立
18.9		-	生産システムと非生産システムを別々の環境で管理し，開発者に本番環境への監視されていないアクセス権を付与しないようにする
18.10		-	一般的な Web アプリケーション攻撃に備え Web アプリケーションに流れる全トラフィックを検査する WAF を実装して，Web アプリケーションを保護
18.11		-	データベースに依存するアプリケーションの場合は，標準のハードニング構成されたテンプレートを使用
19.1		-	人の役割とインシデントのハンドリング/管理のフェーズを定義するインシデント対応計画書が作成されていることを確認
19.2		-	特定個人にコンピュータとネットワークインシデントを処理するための職位と職務を割り当て，インシデント解決までの事案の追跡と文書化を実施
19.3		-	重要な意思決定の役割を果たす，インシデント対応プロセスをサポートする管理担当者とその代行者を指定
19.4	インシデントレスポンスと管理	-	システム管理者や他の従業員が異常なイベントを対応チームに報告可能な時間帯，報告の仕組み，通知に含める情報について組織全体の基準を作成

次ページに続く

前ページからの続き

No.	タイトル	防御段階	概要
19.5		-	法執行機関，関連する政府機関，ベンダー，ISAC パートナー等のセキュリティ問題を報告する必要がある第 3 者連絡先情報に関する情報を集め，管理
19.6		-	インシデントハンドリングチームに報告すべきコンピュータの異常やインシデントに関連する情報を全従業員に公開
19.7		-	現実の脅威に対応するための意識と能力を維持するため，インシデント対応に携わる人員の日常的なインシデント対応演習とシナリオを計画し，実施
19.8		-	組織への既知または潜在的な影響に基づくインシデントスコアリングおよび優先順位付けスキーマを作成
20.1	ペネトレーションテスト，レッドチーム訓練	-	ワイヤレス，クライアントベース，Web アプリケーションの攻撃など，あらゆる種類の複合型攻撃を含む侵入テストのプログラムを確立
20.2		-	定期的な外部および内部からの侵入テストを実施し，エンタープライズシステムの悪用可能な脆弱性および攻撃経路を特定
20.3		-	組織の準備状況をテストすることに加えて，迅速かつ効果的な攻撃の特定・阻止・対応のため，定期的なレッドチームの演習を実施
20.4		-	攻撃者にとって有用な未保護なシステム情報と成果物（ネットワーク構成図，設定ファイル，パスワード等）の存在を発見するためのテストを実施
20.5		-	実稼働環境を模擬したテストベッドを作成し，通常では実環境でテストできない機器に対してレッドチームによる攻撃を実施
20.6		-	脆弱性スキャンと侵入テストツールを連携して使用

次ページに続く

前ページからの続き

No.	タイトル	防御段階	概要
20.7		-	レッドチーム演習の結果は，コンピュータで読み取り可能なオープンな標準（SCAPなど）を使用して文書化されていることを確認
20.8		-	侵入テストに使用するユーザまたはシステムアカウントが，承認された目的でのみ使用されていることを確認し，テストの終了後には削除

以上