Vol.2023-CE-169 No.29
2023/3/12

# ゲーミフィケーションを活用した児童・生徒向け情報セキュリティ学習プログラムの開発

津田敦哉[1]　松崎和賢[1]

**概要**：本稿では，ビデオゲームを活用した児童・生徒向けの情報セキュリティ学習プログラムを開発し，評価を行った結果を報告する．セキュリティ教育をめぐっては，学習者のセキュリティ行動に及ぼす効果が限定的であることや，COVID-19 の感染拡大に伴いアナログゲームや CTF(ハッキング競技)を利用した対面での活動を行うことが困難であること等の課題がある．そこで，サイバーリスクについて「自分ごと」として捉える機会を提供することで，学習者のセキュリティ意識を向上せしめる効果的なオンライン学習プログラムを開発することが本研究の狙いである．開発したプログラムを模擬授業により評価した結果，開発したプログラムが事前に定めた要件を充足し，学習者の動機付けに寄与しうることや，学習に対して有効性を示すことなどが確認された．

**キーワード**：情報セキュリティ，教育ゲーム，デジタルゲーム，ゲーミフィケーション

# Developing an InfoSec Learning Program for K-12 Education using Gamification

ATSUYA TSUDA[†1]　KAZUTAKA MATSUZAKI[†1]

## 1. はじめに

本稿では，児童・生徒向けの情報セキュリティ学習プログラム開発の一環として，ビデオゲーム等を制作し，評価を行った結果を報告する.セキュリティ教育をめぐっては，学習者のセキュリティ行動に及ぼす効果が限定的であることや，新型コロナウイルスの感染拡大に伴いアナログゲームや CTF(ハッキング競技)を利用した対面での活動を行うことが困難であること等の課題がある．そこで，サイバーリスクについて「自分ごと」として捉える機会を提供することで，学習者のセキュリティ意識を向上せしめる効果的なオンライン学習プログラムを開発することが本研究の狙いである．

近年，国内では子どものスマートフォン所持の低年齢化が進んでいる．2022 年に行われた調査によれば，子どもにスマートフォンを持たせた時期について「小学生から」と回答した親が 51.6%にのぼった[1] ．また，小学校学習指導要領(平成 29 年告示)・中学校学習指導要領(平成 29 年告示)・高校学習指導要領(平成 30 年告示)ではいずれも，情報セキュリティや情報モラルを含む情報活用能力は，各教科の学びの基盤となる資質・能力であるとして，教科横断的に育成すべき旨が示されている[2]–[4]．これらのことから，児童・生徒に対して早期に効果的な情報セキュリティ教育を行う重要性は増している．

## 2. 研究の背景

前述のような社会的要請に対して，従前のセキュリティ教育は効果が限定的であり，学習者が実際にセキュリティを確保する行動につながっていないとの課題も指摘されている[5]．セキュリティ強化行動を阻害する要因として，諏訪らは，コスト感を挙げており，具体的な対策手順や実施方法を伝えることが重要であると分析した[6]．また，越智らは，コストに対する割高感の低さ・知識の多さ・社会認識(セキュリティリスクの社会的な深刻さの認識)の高さ・周囲の熱心さ・自己効力感の高さ等が，セキュリティ強化行動を促進することを示した[7]．すなわち，学習プログラムの開発にあたっては，先行研究で示されているこれらのセキュリティ強化行動に関連するファクターを考慮することが肝要であると考えられる．

そのような中で，情報セキュリティ導入教育の実践としても，知識教授型のものに加えて，「内容のゲーミフィケーション《ゲーム要素やゲームメカニズム，およびゲーム的思考を適用し，コンテンツ内容をよりゲームらしくするための方法[8], [9]》」を取り入れたものも出現し始めている．実際に先行研究では，教育用シミュレーションゲームを用いてトレーニングを受けた受講者が，従来的な方法で指導を受けた受講者に比べて，自己効力感（トレーニングに関連した課題を遂行できるという自信）や記憶の定着率が高くなる効果があることも明らかになっている[10]．国内に限っても，ボードゲームやカードゲーム等のアナログゲー

1 中央大学国際情報学部
Faculty of Global Informatics, Chuo University

ムを使用したものやCTF（ハッキング競技）を取り入れたものなど，児童から社会人まで幅広い対象に対する様々な試みが存在する[11]–[14].

## 3. 研究の目的

先に述べたように，ゲーミフィケーションを取り入れた様々な実践が行われるようになっているが，一方で現在のところ，セキュリティを初めて学ぶ児童・生徒がオンラインで利用可能な，ビデオゲームを活用した学習プログラムは，調べた限り見当たらなかった．また，従前の学習コンテンツの中には，技術的な詳細に特化し，モラルや法律に関しては対象としない難解なものや，組織におけるインシデント対策に限定して焦点を当てているものなど，初学者には適さないものも少なくない．さらに，2023 年時点では，COVID-19 の感染拡大の影響により，対面での CTF やアナログゲームを用いた教育の実施は依然容易とはいえない．

そこで本研究では，ビデオゲームを用いて，インターネット利用時の身近なトラブルを擬似的に体感してもらうことにより，サイバーリスクについて「自分ごと」として捉える機会を提供し，もって学習者のセキュリティ意識を向上せしめる効果的な学習プログラムを開発することを目指す．

### 3.1 要件

前述の目的を達するため，本研究において開発する学習プログラムは以下の要件を満たすよう設計する．

I. ストーリーテリング
II. キャラクターの存在
III. 自律性
IV. 関係性
V. コンピテンス

I のストーリーテリングは，物語の文脈を学習に追加することで，特定の学習内容をいつ適用するべきかを学習者に知らせたい場合に用いられる．ストーリーを通して「なぜこれを学ぶのか」「どう役立つのか」が明確になることで学習者の興味をひき[9]，学習後のセキュリティ意識の向上にもつながる可能性があると考えられる．

II のキャラクターの存在は，学習者をより深く関与させる効果を持つ．先行研究により，画面にアバターが表示されると，学習者はコンピュータに対してよりも，その「人」に対して責任があると感じるため，学習者の動機づけになることが分かっている[9], [15].

III の自律性は，学習者が自分で行動の結果を決定できると思える内容であることを指す[9]．この実現の方法としては，学習プログラムにインタラクティブ性（学習者の選択による内容の変化）を持たせることが考えられる．

IV の関係性は，人が他者とのつながりを感じたときに経験されるものである[9]．学習者を小グループに分け，チーム間の競争やチーム内の協働を促すことが効果的であると考えられる．

V のコンピテンスとは，チャレンジしたいという思いと完全習得したという感覚を指す[9]．これを得るためには，実際に日常生活で役立つ新しいスキルを習得する機会や適切な挑戦を受ける機会が肝要であり，身近なセキュリティインシデントを題材として用いることやレベル別の課題設定などが有効であると考えられる．

## 4. 研究の方法

### 4.1 学習プログラムの概要

開発する学習プログラムの全体図を図 1 に示す．教員は全体のコーディネートと講義を担う．学習者はいくつかのチームに分かれて，チームごとに提供されるゲームをプレイし，そのシナリオを通して，チャプター毎に疑似的なセキュリティインシデントに直面する．各チャプターのプレイ終了後に，教員は「登場人物はどのような対策をしていれば情報を盗まれずに済んだか？」「怪しいと思ったらどのような行動をとるべきか？」などのゲームの内容に関連する発問を行う．学習者は，オンラインコラボレーションツールを利用したワークを行い，チーム内でそれらの課題について数分間話し合う．このワークの結果はクラス全体でも共有を行い，さらに議論を深める．その後，教員が当該チャプターで取り扱ったインシデントについて解説を行う．これらをゲームのチャプターの数だけ繰り返すことで授業が進行する．

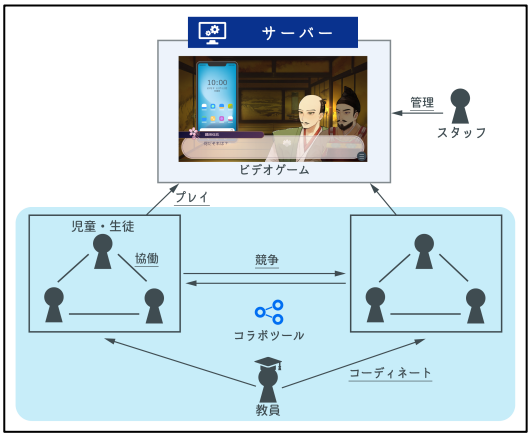


図 1 学習プログラムの全体像

### 4.2 予備調査

コンテンツの開発に着手するあたり，筆者は 2022 年 6 月に WEB 上で 2 度にわたる予備調査を実施した．調査の目的は，若年層のデジタルデバイスへの接触・所有経験や，デバイスを使用するにあたってのトラブル経験，学校教育

の中で情報セキュリティを学んだ経験など，シナリオ作成の基礎となるデータを収集することである．なお，アンケートは，セルフ型アンケートツールである「Freeasy」を利用して収集した．はじめに行った調査(以下，アンケート A とする)と，その結果をもとに，さらに詳細な情報セキュリティ関連トラブルのエピソードを集める目的で行った追加調査（以下，アンケート B とする）の概要を以下に示す．

#### 4.2.1 アンケート A

(1) **調査概要**

**回収期間**

2022 年 6 月 8 日～2022 年 6 月 9 日

**調査の対象**

全国の 15～20 歳の学生

**サンプル数**

1000 人 (男性: 500 人，女性: 500 人)

**同意**

回答者に対しては，データの取扱方法について事前に説明し，研究に使用する旨を告知した上で，同意を得た．

(2) **調査結果（抜粋）**

**デジタルデバイスへの接触・所有経験**

図 2 に結果を示す．小学生時点で 16%，中学生時点で全体の半数を超える回答者がスマートフォンを所有していたことが明らかとなった．

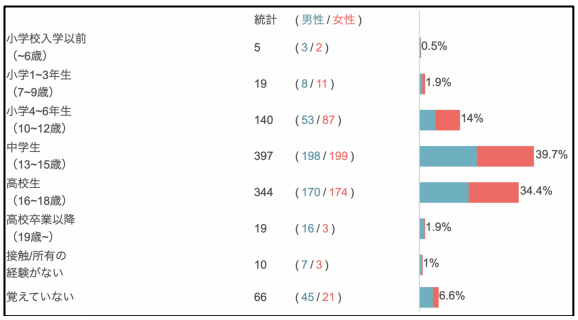


図 2　スマートフォンを初めて所有した時期(択一)

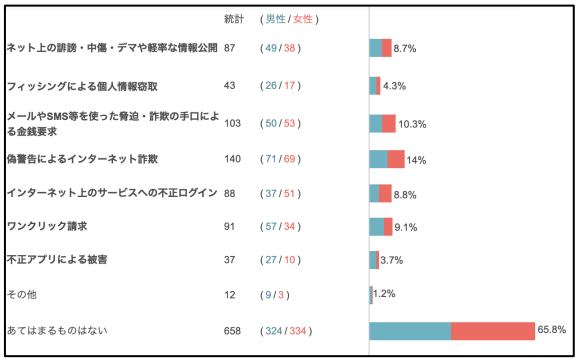


図 3　過去に遭遇したセキュリティトラブル(複数選択)

**デバイスを使用するにあたってのトラブル経験**

図 3 に結果を示す．回答者全体のおよそ 34%が，デジタルデバイスを使用する上で何らかのセキュリティにまつわるトラブルを経験したことがあることが明らかになった．また，遭遇率が高いトラブルの上位としては，偽警告によるインターネット詐欺・メールや SMS を使った脅迫や詐欺の手口による金銭要求･ワンクリック請求などが並んだ．

**情報セキュリティ教育の経験**

図 4 と図 5 に結果を示す．情報セキュリティ教育を受けた時期としては，授業のスタイルや用いた教材にかかわらず，中学校時代という回答が最も多かった．授業の進め方については，図 4 より，一方向型の授業(教員による講義スタイル)が最も多かった．また，用いた教材については，図 5 より教科書やテキストを利用した割合・啓発/資料映像を利用した割合が高かった．一方で，ゲームや実際の端末を使った学習経験がある者はどの年齢層でも 20%に満たなかった．また，どの形式でも教育を受けたことがないと回答した者は 12.5%にのぼった．

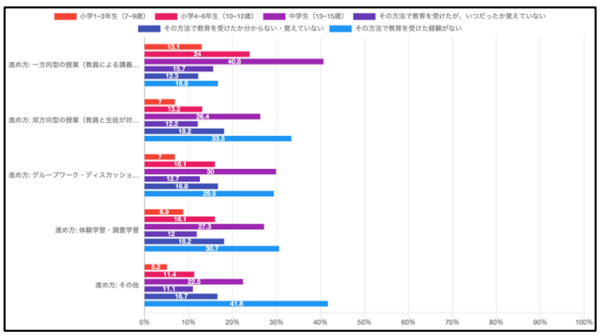

図 4　情報セキュリティ教育の経験（授業形式別）

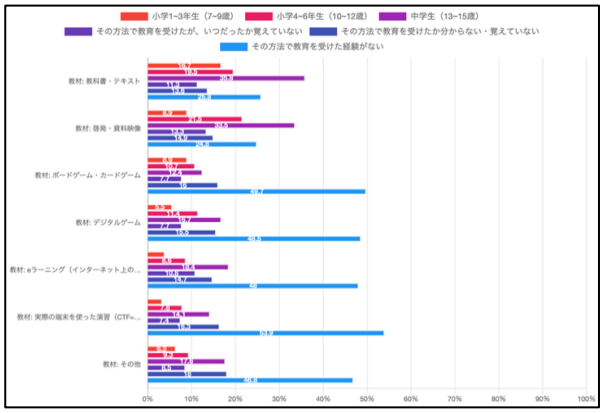

図 5　情報セキュリティ教育の経験（教材別）

#### 4.2.2 アンケート B

(1) **調査概要**

**回収期間**

2022 年 6 月 14 日

**調査の対象**

アンケート A でトラブルに遭遇した経験・遭遇しそうになった経験の少なくともいずれか一方があると回答した 521 人のうち，不正回答であると思われる者を除いた計 501 人

**サンプル数**

200 人(男性:100 人，女性: 100 人)

**同意**

回答者に対しては，データの取扱方法について事前に説明し，研究に使用する旨を告知した上で，同意を得た．

(2) **調査結果（抜粋）**

表 1 に一部抜粋した回答を示す．なお，個人の特定を避けるため，回答は一部修正を加えている．記述式のアンケート B では，偽警告やフィッシングに関するエピソードが目立った．ゲームアプリや SNS など，児童・生徒にとって身近なサービス上で被害に遭うケースも少なくないことが本調査で明らかになった．学校でインシデントへの対処法を習っていなかった者・習った知識と実際のインシデントの状況が乖離していたと感じる者も一定数認められた．

表 1　これまでに遭遇した/しかけたトラブルの詳細

| 年齢 | 性別 | 回答 |
|---|---|---|
| 16 歳 | 女性 | SNS の自分のアカウントを乗っ取られ，知らない投稿をされたり共有されたりした．自分では気づかず，フォロワーから教えてもらい気づいた．その後，そのフォロワーにパスワードを変えた方がいいと言われ変えた．しかし，その後も何度も乗っ取りが続き，ついにアカウントを凍結された． |
| 18 歳 | 男性 | SNS を閲覧していたところ，アプリゲームの課金アイテムをプレゼントする旨の広告が表示され，タップした．移動先の WEB サイトで，キャンペーンへの応募のためゲームの ID とパスワードを入力したが，このサイトは偽サイトであり，入力した情報からアカウントを乗っ取られてしまった．ゲーム会社に問い合せても解決できなかった． |
| 15 歳 | 女性 | スマートフォンに携帯電話会社のようなメールアドレスから通信容量の補充に関するメールが届いた． その月の残量がほぼなかったため，リンクからサイトに飛んでしまった．後で親がそのメールアドレスをネットで調べたため，詐欺だと分かった．学校で習った知識よりもリアルな状況であり，学んだことを役立てられなかった． |

## 5. 設計と実装

### 5.1 ノベルゲーム（Visual Nobel）

本節では，学習プログラムの内容のひとつであるビデオゲームの開発について述べる．ノベルゲーム(Visual Novel)とは，テキストやキャラクター画像，背景画像などの要素を用いて対話を可視化し，プレイヤーにストーリーを語りかけるビデオゲームの一種である．ノベルゲームはアクション性が少なく，高度なプレイヤースキルを必要としない上に，時間的・ハードウェア的な制約も比較的受けない．そのため，日常的にゲームをプレイしない学習者も楽しむことができるという特徴がある．また，教材作成者にとっても，開発に要するコストを比較的抑えることができ，内容の更新が容易であるという利点がある．これらの観点から，本研究ではこのゲームジャンルを選択した．

#### 5.1.1 ゲームの概要

開発するゲームの舞台設定は，戦国時代とした．これは，戦国時代は様々な創作物で頻繁に用いられ，学校の授業等で取り扱われることも多いために，児童・生徒が親しみを感じやすく，理解が困難でないと思われるためである．以下に，シナリオのあらすじを示す．

> *時は戦国時代．主人公・織田信長は天下統一まであと一歩に迫るも，足利義昭に苦戦を強いられていた．そんな中で，信長の家臣・明智光秀は南蛮渡来の「あいてい (IT)」の導入を提案する．スマホを配備した信長軍は，チャットやマップで連携を図って戦を有利に進めるが，ひょんなことからセキュリティトラブルに巻き込まれていく．*

#### 5.1.2 教育の内容

ゲームに含める情報セキュリティ関連トラブルの内容については，前述のアンケート A・B の結果を踏まえ，作劇上の面白さを勘案した上で選定した．検討の結果，最終的 4 つの類型をシナリオに含めることとした．各類型とその概要，シナリオの具体的な連関を表 2 に示す．

表 2　インシデントとシナリオの対応

| トラブル類型 | トラブル概要 | シナリオの内容 |
|---|---|---|
| フィッシング | 実在する組織を装った WEB サイトなどに誘導し，個人情報や認証情報を盗まれる類型 | 織田信長は，ネットショッピングで格安の茶器を購入しようと，よく確かめずに ID やパスワードを入力する．しかし，WEB サイトは足利軍が仕掛けた罠であり，ログイン情報を奪われてしまう． |
| 不正ログイン | 認証情報の窃取・推測などにより，WEB サービスに不正にログインされる類型 | 織田信長は妻・帰蝶に，クラウドストレージサービスの ID やパスワードをつい教えてしまう．ある日，帰蝶が興味本位でアカウントにログインしたところ，家臣・明智光秀の暗殺計画らしき文書を見つける． |
| ソーシャルエンジニアリング | ショルダーハッキング(キー操作などを肩越しに見て情報を盗む)など，人間の心理的な弱点を利用されて被害に遭う類型 | 柴田勝家は，城下町の茶屋でテレワークに勤しんでいた．その最中，使っていた PC をロックせずそのままトイレに立ったために，足利軍の差し向けた忍者によって作戦情報などが漏洩してしまう． |
| SNS 投稿からの情報流出 | SNS 上での投稿から，個人情報や行動履歴等が特定される類型 | 帰蝶は，戦火を避けようと避難する道中で撮影した写真を，写真共有 SNS に投稿する．アカウントは非公開だったが，「友だち」に足利軍の関係者が紛れ込んでいたために，居場所が筒抜けになってしまう． |

#### 5.1.3 開発環境と実行環境

ゲームの開発には，STRIKE WORKES が提供する GUI ベースのノベルゲーム制作ソフトウェアである「ティラノビルダー PRO (Ver2.04b)」を使用した．開発画面の例を図 6 に，開発したゲームのシーンの一部を図 7 にそれぞれ示す．作成したゲームは，本ソフトウェアの書き出し機能を用いて，HTML5 環境で動作するブラウザゲームとして出力し，サーバー上に配置することで，学習者は PC・タブレット・スマートフォンなど任意の端末でプレイ可能である．

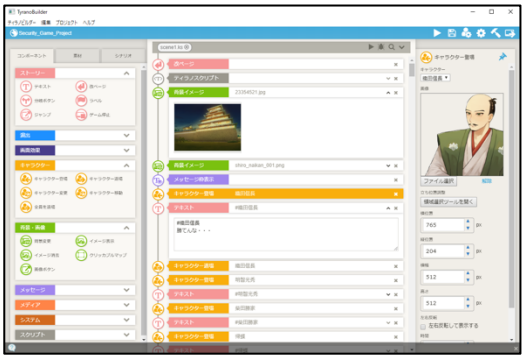

図 6　開発画面の例

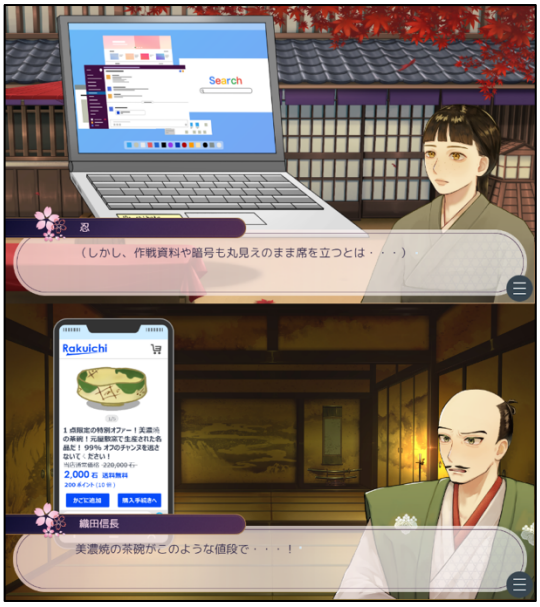


図 7　ゲーム画面の例

### 5.2 授業資料

本節では，学習プログラムの実施に用いる授業資料の作成について述べる．本研究では，情報セキュリティの学習経験が少ない教員であっても円滑に授業を実施できるよう，授業用のスライド資料を Microsoft PowerPoint を使用して作成した．資料には，ゲームに関連する発問や，インシデントの内容や対処法に関する解説，教員向けの詳細な台本などが含まれる．図 8 に，作成した資料の一部を示す．


図 8　授業資料の例

## 6. 評価

### 6.1 模擬授業の実施

学習プログラムの評価のため，模擬授業を実施した．模擬授業を行うにあたっては，事前に，情報セキュリティに関する習熟度などを問う目的で，参加者に WEB アンケートを行った．その後は，原則として 4.1 節の手順に則り，研究協力者に対して模擬授業を実施する．ただし，今回の実験では，時間の都合上，参加者は模擬授業を受講する前に各自でゲームプレイを行うこととした．授業中は参加者を 2 つのグループに分け，筆者が教員の役を務めた．また，授業の実施後には，本教育プログラムに対するフィードバックなどを収集するため，参加者に対して WEB アンケートを行った．模擬授業の実施概要を以下に示す．

#### 6.1.1 概要

**実施日時**

2023 年 2 月 6 日　19 時～21 時

**参加者の平均年齢**

22.6 歳（SD 3.05）

**参加者の属性**

学生（80%），サービス業従事者（20%）

**サンプル数**

5 人（男性：2 人，女性：3 人）

**同意**

回答者に対しては，データの取扱方法について事前に説明し，研究に使用する旨を告知した上で，同意を得た．

### 6.2 評価方法

#### 6.2.1 学習到達度

学習プログラムによる到達度の評価は，学習者の自己評価によって行う．これに先立ち，表 2 に示した各項目について，5 段階の到達度（理解の度合い）を示したルーブリックを作成した（表 3 に示す）．この作成したルーブリックに基づいて，模擬授業の実施前と実施後に参加者にアンケートを実施し，回答時点に最も当てはまると感じる到達度を回答してもらった．

表 3　ルーブリック

| 項目 / 到達度 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|
| ショルダーハッキング | ショルダーハッキングとは何かを理解し，具体例などを用いてある程度説明できる． | 聞いたことがあり，なぜ危険なのか理解している． | 聞いたことがあり，危険だということだけは知っている． | 聞いたことはあるが，どのようなものなのか知らない． | その言葉を聞いたことがない． |
| フィッシング | フィッシングとは何かを理解し，具体例などを用いてある程度説明できる． | 聞いたことがあり，なぜ危険なのか理解している． | 聞いたことがあり，危険だということだけは知っている． | 聞いたことはあるが，どのようなものなのか知らない． | その言葉を聞いたことがない． |
| SNS 投稿からの情報漏洩 | SNS 投稿からの情報漏洩とは何かを理解し，具体例などを用いてある程度説明できる． | 聞いたことがあり，なぜ危険なのか理解している． | 聞いたことがあり，危険だということだけは知っている． | 聞いたことはあるが，どのようなものなのか知らない． | その言葉を聞いたことがない． |
| 不正ログイン | 不正ログインとは何かを理解し，具体例などを用いてある程度説明できる． | 聞いたことがあり，なぜ危険なのか理解している． | 聞いたことがあり，危険だということだけは知っている． | 聞いたことはあるが，どのようなものなのか知らない． | その言葉を聞いたことがない． |

#### 6.2.2 学習プログラムに対する反応

学習プログラムに対する参加者の反応や 3.1 節に示した要件との適合性を，模擬授業実施後のアンケートで評価する．アンケートは全 12 問で構成され，回答者は各項目について「全く当てはまらない」から「非常によく当てはまる」の 5 段階のリッカート尺度で回答する．

#### 6.2.3 ゲームに対する反応

参加者のゲームに対する反応を評価するため，本研究では，教育用ビデオゲームの評価指標として実績のある MEEGA+を用いた．MEEGA+では，ゲームのユーザビリティとプレイヤー体験に関する学習者の反応ついて，35 個の設問を用いてアンケートを行い，5 段階のリッカート尺度で評価する．本実験では，[16]で提案された質問票を筆者らの手で日本語訳し，使用した．

### 6.3 評価結果

#### 6.3.1 学習到達度に対する評価結果

表 4 に集計結果を示す．表中の MD（Mean Difference）は，授業後の平均スコアと授業前の平均スコアの差分を取ることにより得られるものである．模擬授業の前後で比較すると，全ての項目で平均到達度に上昇が見られた．最も上昇量が大きかった項目は「ショルダーハッキング」であり，平均で 2 ポイント上昇した．また，授業後の到達度の平均は全て 4 ポイントを超え，開発したプログラムの学習に対する有効性が示唆された．

表 4　到達度の評価結果

| 項目 | 授業前 | | 授業後 | | MD |
|---|---|---|---|---|---|
| | Avg. | SD | Avg. | SD | |
| ショルダーハッキング | 2.6 | 1.67 | 4.6 | 0.89 | 2.0 |
| フィッシング | 3.2 | 1.30 | 4.8 | 0.45 | 1.6 |
| SNS 投稿からの情報漏洩 | 4.4 | 0.55 | 4.8 | 0.45 | 0.4 |
| 不正ログイン | 4.6 | 0.55 | 4.8 | 0.45 | 0.2 |

#### 6.3.2 学習プログラムに対する評価結果

表 5 に設問と集計結果を示す．3.1 節に示した要件に対応した設問 ID3, 4, 6, 11, 12 の全てで平均が 4 ポイントを上回っていることから，本研究で開発した学習プログラムは，事前に定めた要件を一定のレベルで充足するものであると考えられる．また，教材に関連する設問 ID8, 9, 10 より，ゲームを除き最も学習に寄与したと評価された教材は，スライド資料であった．全ての項目で，参加者の反応の平均が 4 ポイントを下回る項目は見られなかった．

#### 6.3.3 ゲームに対する評価結果

表 6 に設問と集計結果を示す．ユーザビリティの項目では，ID10（見た目のカスタマイズ）以外の設問の全てで，平均スコアが 4 ポイント以上となった．とりわけ，学習可能性に関するスコアが高くなり，開発したゲームが学習者にとってプレイしやすいものであることが示された．一方で，プレイヤー体験の項目では，社会的交流や集中に関する評価が比較的低くなった．これらは，本実験では参加者がゲームプレイを個人で行ったこと，ゲーム内の交流や対戦機能が存在しないこと，また，ゲームデザインが選択肢を持たないノベルゲーム形式であることによるものであると考えられるため，今後の改良を要する．

## 7. まとめ

本研究では，児童・生徒向けにビデオゲームを活用した学習プログラムを開発し，模擬授業による評価を行った．その結果，開発したプログラムが要件を充足して学習者の動機付けに寄与しうることや学習に有効性を示すこと，ゲームが高いユーザビリティを持つことなどが確認された．

今後は，アンケートのフィードバックをもとに，追加の開発等を行い，学習プログラムの構成やゲームのプレイヤー体験をさらに改善することが課題である．また，本学習プログラムの主なターゲットとして想定される中学生等を対象に，さらに評価を行うことを予定している．

表 5　学習プログラムの評価結果

| ID | 設問 | Avg. | SD |
|---|---|---|---|
| 1 | この学習プログラムは，楽しめるものだった | 4.2 | 0.84 |
| 2 | この学習プログラムで学んだ内容は，今後の日常生活に生かせるものだった | 4.6 | 0.55 |
| 3 | この学習プログラムの中で，課題にチャレンジする意欲や，習った内容を身につけられたという感覚が得られた | 4.4 | 1.34 |
| 4 | この学習プログラムでは，グループワークなどを通じて他の学習者とのつながりが感じられた | 4.4 | 0.55 |
| 5 | 学習プログラムを受講する中で，「情報セキュリティ」に対する心理的なハードルが下がった | 4.8 | 0.45 |
| 6 | 学習プログラムは，インタラクティブ（自らの選択や発言によって内容が変化する）なつくりになっていた | 4.0 | 1.00 |
| 7 | 授業の中で出された課題の内容やレベルは，適切だった | 4.2 | 1.10 |
| 8 | グループワークは，学習の役に立った | 4.6 | 0.55 |
| 9 | 授業スライドは，学習の役に立った | 5.0 | 0.00 |
| 10 | 投影した動画は，学習の役に立った | 4.6 | 0.89 |
| 11 | ゲームのキャラクターは魅力的だった | 4.4 | 0.89 |
| 12 | ゲームのストーリーは魅力的だった | 4.6 | 0.55 |

表 6　MEEGA+の評価結果

| 品質因子 | 特質 | ID | 設問 | Avg. | SD |
|---|---|---|---|---|---|
| ユーザビリティ | 美的感覚 | 1 | ゲームの視覚的なデザインは魅力的だった | 4.2 | 0.84 |
| | | 2 | 文字のフォントや色がマッチしていて統一感がある | 4.8 | 0.45 |
| | 学習可能性 | 3 | ゲームをプレイする前に身につけておく必要のある知識は少なかった | 4.6 | 0.55 |
| | | 4 | ゲームの遊び方を覚えるのは簡単だった | 5.0 | 0.00 |
| | | 5 | ほとんどの人が，すぐにこのゲームをプレイできると思う | 5.0 | 0.00 |
| | 操作性 | 6 | このゲームはプレイしやすいと思う | 4.2 | 1.10 |
| | | 7 | ゲームのルールは明確でわかりやすい | 5.0 | 0.00 |
| | アクセス可能性 | 8 | ゲーム内の文字は読みやすい | 4.0 | 1.00 |
| | | 9 | ゲーム内の色の使い方に意図が感じられる | 4.0 | 0.71 |
| | | 10 | ゲームの見た目を自分好みにカスタマイズできる | 2.4 | 0.89 |
| プレイヤー体験 | ユーザーの誤り防止 | 11 | このゲームのシステムはプレイヤーのミスを未然に防いでくれる | 4.0 | 1.00 |
| | | 12 | このゲームのシステムはミスしてもすぐ復帰できるようになっている | 3.0 | 0.00 |
| | 信頼性 | 13 | 最初にゲームを見たとき，簡単そうだという印象を受けた | 3.6 | 1.14 |
| | | 14 | 内容や構成を見て，このゲームで学べそうという気持ちになった | 4.4 | 0.55 |
| | 挑戦 | 15 | このゲームは適切な難易度だった | 4.8 | 0.45 |
| | | 16 | 適切なペースで新しいチャレンジ(新しい課題や状況など)が訪れる | 3.6 | 0.55 |
| | | 17 | ゲームが進むにつれて単調(くり返しや退屈な作業)にならない | 3.0 | 1.00 |
| | 満足度 | 18 | ゲームの課題をクリアすることで，満足のいく達成感が得られた | 3.0 | 0.71 |
| | | 19 | ゲームを進めることができたのは，自分自身の努力によるものである | 3.2 | 0.84 |
| | | 20 | ゲームから学んだ内容に満足している | 4.4 | 0.55 |
| | | 21 | このゲームを周りの人にもすすめたい | 3.8 | 0.84 |
| | 社会的交流 | 22 | ゲーム中に他のプレイヤーと交流できた | 1.8 | 1.30 |
| | | 23 | ゲーム内で協力したり，競争したりするのが楽しかった | 1.6 | 0.89 |
| | | 24 | ゲーム中に他のプレイヤーと交流できて良かった | 1.6 | 0.89 |
| | 楽しみ | 25 | ゲームを楽しめた | 4.0 | 1.00 |
| | | 26 | ゲーム中に笑顔になるできごと(ゲーム要素など)があった | 3.2 | 0.84 |
| | 集中 | 27 | ゲームの始めに興味をひかれるできごとがあった | 3.6 | 0.55 |
| | | 28 | ゲームに夢中になり，時間が経つのを忘れた | 2.4 | 0.89 |
| | | 29 | ゲーム中，周囲のことを忘れて遊べた | 2.4 | 1.14 |
| | 関連性 | 30 | ゲームの内容は自分の興味に合っていた | 2.8 | 1.30 |
| | | 31 | ゲームの内容が学習プログラム全体とどのように関連しているか分かりやすかった | 4.8 | 0.45 |
| | | 32 | このゲームは，この学習プログラムに適した教育方法だと思う | 4.0 | 1.00 |
| | | 33 | 他の教え方よりもこのゲームでの学習の方が好ましい | 4.0 | 1.00 |
| | 学習効果 | 34 | ゲームは，この学習プログラムの中での自らの学習に役立った | 4.4 | 0.89 |
| | | 35 | このゲームは，学習プログラムの他の活動に比べて，効率的に学習することができた | 3.8 | 1.30 |

**謝辞** ゲームの素材作成にあたっては，國生まりあさん（イラスト担当・横浜美術大学)，齊藤飛廉さん（制作進行・横浜美術大学)，本庄勇史さん（シナリオ担当・デジタルハリウッド大学)のご協力を賜りました.感謝申し上げます.

## 参考文献

[1] 日本経済新聞社: “スマホデビュー、「小学生から」５１％、民間調査、低年齢化進む,” 日本経済新聞 夕刊, p. 11, Mar. 23, 2022.
[2] 文部科学省: “小学校学習指導要領（平成 29 年告示）解説 総則編.” 2017.
[3] 文部科学省: “中学校学習指導要領（平成 29 年告示）解説 総則編.” 2017.
[4] 文部科学省: “高等学校学習指導要領（平成 30 年告示）解説 総則編.” 2018.
[5] 坂本倫子, 喜入暁, 越智啓太: “セキュリティ教育はセキュリティ対策行動を促進しない,” 日本心理学会大会発表論文集, vol. 79, no. 0, pp. 3EV – 123, 2015.
[6] 諏訪博彦, 原賢, 関良明ほか: “情報セキュリティ行動モデルの構築―人はなぜセキュリティ行動をしないのか,” 情報処理学会論文誌, vol. 53, no. 9, pp. 2204–2212, 2012.
[7] 越智啓太: “情報セキュリティ行動を促進・抑制する要因,” 法政大学文学部紀要, vol. 77, pp. 77–104, 2018.
[8] Kapp, K. M., Blair, L., and Mesch, R.: *The gamification of learning and instruction fieldbook: ideas into practice*. Wiley, 2013.
[9] Reigeluth, C. M., Beatty, B. J., and Myers, R. D.: インストラクショナルデザイン理論とモデル: 学習者中心の教育を実現する. 北大路書房, 2020.
[10] Sitzmann, T.: “A meta-analytic examination of the instructional effectiveness of computer-based simulation games,” *Personnel psychology*, vol. 64, no. 2, pp. 489–528, 2011.
[11] 中矢誠, 富永浩之: “初心者への情報セキュリティの教育機会としてのハッキングゲーム CTF,” 電子情報通信学会技術研究報告.ET, 教育工学, vol. 112, no. 66, pp. 45–50, 2012.
[12] 会田和弘, 佐々木良一: “双六をつかった情報セキュリティ教育の試み,” デジタルプラクティス, vol. 9, no. 3, pp. 716–737, 2018.
[13] 花田経子: “ICT 機器の安全利用を促すための小学校高学年向けアナログゲーム教材の開発,” 日本デジタル教科書学会発表予稿集, vol. 8, no. 0, Art. no. 0, 2019.
[14] 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. 59, no. 12, pp. 2232–2245, 2018.
[15] Clark, R. C. and Mayer, R. E.: *E-learning and the science of instruction: proven guidelines for consumers and designers of multimedia learning*, 3rd ed. Pfeiffer, 2011.
[16] Petri, G., von Wangenheim, C. G., and Borgatto, A. F.: “MEEGA+: a method for the evaluation of educational games for computing education,” *INCoD–Brazilian Institute for Digital Convergence*, pp. 1–47, 2018.