Vol.2026-CE-183 No.2
2026/2/7

鍵暗号方式を学ぶ Web アプリケーション「Picleis」の開発と評価

山﨑愛乃[1]　石井幹大[2]　伊藤一成[1]

概要：デジタル社会の進展に伴い，情報セキュリティに対する理解の重要性が高まっている．特に鍵暗号方式はセキュリティを支える基盤技術であり，高等学校教科「情報 I 」においてもその必要性が明示されているが，学習者にとって理解が困難な分野である．そこで我々は，メッセージ交換を通して鍵暗号方式を体験的に学習できる Web アプリケーション「Picleis」を開発した．「Picleis」は，鍵の受け渡しなど鍵の流れに学習者の意識が向くよう設計した点に特徴があり，学習者が一人で共通鍵暗号方式と公開鍵暗号方式の双方を学習できる．さらに，「Picleis」を用いた実践授業では，鍵暗号方式に対する理解の向上がみられ，アプリケーションの導線やインタフェースが概ね良好であることが示唆された．本稿では，「Picleis」の概要と機能，および実践授業を通して得られた評価について報告する．

キーワード：共通鍵暗号方式，公開鍵暗号方式，情報 I ，体験的学習

1. はじめに

デジタル社会の進展に伴い，デジタルトランスフォーメーション (DX) が加速し，社会全体で情報システムへの依存度が増大している[1]．一方，情報システムに対するサイバー攻撃の発生頻度は増加し，攻撃の手口も高度化していることから[2][3]，情報セキュリティに関する知識や理解を得る重要性は高まっていると言える．

情報セキュリティを支える基盤技術の 1 つが暗号化であり，暗号化を実現するための具体的な技術的手法が鍵暗号方式である．高等学校必履修科目「情報 I 」の教科書では，共通鍵暗号方式と公開鍵暗号方式の 2 つが主に取り上げられ，図を用いた解説が行われている．しかし，我々は，図や文章だけではなく，体験を通して学習することで，理解度の向上が図れると考えている．

体験的学習手法の 1 つにコンピュータサイエンスアンプラグド（以降，CS アンプラグドと表記）があり[4]，セキュリティや暗号方式に関する報告も行われている[5][6]．しかし，CS アンプラグドでは，専用の教材を用意する必要がある場合が多く，教授者にかかる経済的負担や時間的負担が大きいという課題も存在する[7]．

そのため我々は，特定の URL にアクセスするだけで共通鍵暗号方式と公開鍵暗号方式を体験的に学習できる「BOUCHO [8]」およびその改善版である「BOUCHO2 [9][10]」を開発・公開している．今回，「BOUCHO2」の実践や評価を踏まえ，新たに「Picleis」を開発し，実践授業を通して評価したので，本稿で報告する．

本稿の以降の構成は次の通りである．2 章では，我々の先行アプリケーション「BOUCHO」および「BOUCHO2」の概要や評価を概説し，今回「Picleis」の開発に至った経緯を述べる．3 章では，鍵暗号方式の学習を題材とした既存のツールを取り上げ，我々のアプリケーションとの差異を述べる．4 章で「Picleis」の機能や特徴についてまとめ，5 章で実践授業を通した「Picleis」の評価・考察を述べたのち，最後に 6 章でまとめを述べる．

[1] 青山学院大学 社会情報学部
[2] 青山学院大学 理工学部

2. 先行アプリケーション

我々の先行アプリケーションである「BOUCHO」および「BOUCHO2」は，学習者が複数人でメッセージ交換を行う中で，共通鍵暗号方式と公開鍵暗号方式の仕組みを体験的に学習できる点に特徴がある．「共通鍵モード」では「送信者」と「受信者」の役割に，「公開鍵モード」では「質問者」と「回答者」の役割に分かれ，パスフレーズの設定や二次元コードの共有などの手順を踏むことで，送信内容の暗号化や受信内容の復号を体験することができる．

BOUCHO を用いた実践授業では，アプリケーションが体験を通じた鍵暗号方式の理解に寄与できる可能性を示した．しかし，「全体の流れやどの段階の処理が実施されているのかが分かりづらい」「暗号化処理あるいは復号処理に用いられる鍵の種類に対して意識が向きにくい」といった課題も観察された．そこで，これらの課題の改善を目的とした BOUCHO2 を開発し，実践授業を行ったところ，アプリケーションの使用感や鍵暗号方式の理解に関して良好な結果が得られた．一方，BOUCHO および BOUCHO2 は，複数人での利用や，二次元コードを読み込むためのスマートフォンの利用を前提とした設計となっていたため，授業運営上の柔軟性の観点から，今回，学習者個々人が PC のみで使用できるアプリケーションを開発するに至った．

ⓒ2026 Information Processing Society of Japan

3. 関連研究

長瀧，白井が開発した Web ツール[11]も鍵暗号方式の基本概念を学習できるツールとして公開されており，生徒の学習意欲や理解度の向上に寄与したことが報告されている[12]．ただし，このツールで扱う対象は公開鍵暗号方式のみであり，共通鍵暗号方式と公開鍵暗号方式の双方を対象としている我々のアプリケーションとは差異がある．また，このツールでは，ファイルのダウンロードやアップロード，ステップごとのページスクロールが必須となっており，学習者の PC 操作スキル等によっては，認知的負荷の増大[13][14]およびそれに伴う授業参加意欲の低下[15]につながる可能性も考えられる．

他には，「Visual CryptoEd」も暗号方式の基本概念を学習できるツールとして報告されているが[16]，2025 年 12 月時点では一般に公開されていない．

4. Picleis

2 章および 3 章で述べた背景を踏まえ，次の 3 点を Picleis の設計指針とした．

設計指針1 共通鍵暗号方式および公開鍵暗号方式を対象とした，学習者個々人での体験的学習の支援

設計指針2 暗号化処理および復号処理における鍵の受け渡しや利用関係を中心とした，全体プロセスの明確化

設計指針3 学習操作の簡素化や操作負荷の低減

設計指針に基づき，Picleis では，先行アプリケーションと同様に，「共通鍵モード」と「公開鍵モード」を実装した．学習においては身近なテーマを用いることが重要とされており[17][18]，1 人の学習者が役割を切り替えて，メッセージをやり取りすることで，鍵暗号方式の体験を支援する（設計指針 1）．また，体験学習の支援にあたり，ファイルのダウンロードやアップロードといった操作を取り入れない（設計指針 3）．さらに，知識の定着を図るためには，学習に必要な情報やフローは統合して可視化する必要があるとされているため[19]，鍵暗号方式の一連の流れを明示し，視覚化する（設計指針 2）．

本章では，4.1 節で共通鍵モードについて，4.2 節で公開鍵モードについて，それぞれ述べる．

4.1 共通鍵モード

共通鍵モードは，共通鍵暗号方式を体験するモードである．共通鍵モードでは，1 人の学習者が，メッセージを送信する「送信者」と，メッセージを受け取る「受信者」の役割を切り替えて操作することで，暗号化から復号に至る一連の処理を 1 人で体験できる．共通鍵モードでは，「送信者によるメッセージの暗号化」，「受信者による暗号文の復号」の順で操作を行う．各手順について，4.1.1 項，4.1.2 項で解説する．

4.1.1 送信者によるメッセージの暗号化

共通鍵モードにアクセスすると，図 1 に示す画面に遷移する．画面は 4 つの領域に大別され，上部が説明領域，左部が送信者領域，中央部がチャット画面領域，右部が受信者領域である．説明領域に示される指示に従い，学習者が送信者領域もしくは受信者領域で操作を行うことで，チャット画面領域に，メッセージのやり取りや鍵の受け渡しといった履歴が表示される．

図 1　初期画面（共通鍵モード）

はじめに，学習者は，画面内の指示に従って，共通鍵となる文字列を入力し，共通鍵を生成する（手順 1）．次に，手順 2 では，暗号化したいメッセージを入力し，「暗号化」ボタンを押下することで，AES を用いた暗号化処理が実行される．その後，「送信」ボタンを押下することで，暗号化されたメッセージを「チャット画面」に表示するとともに，次手順から「受信者」として操作する必要があることをモーダルウィンドウで伝える（図 2）．

図 2　メッセージ送信時の画面

4.1.2 受信者による暗号文の復号

「チャット画面」に暗号文が表示されると，受信者領域でもメッセージを受信したことが表示される（手順 3）．次に，手順 4「共通鍵を聞く」にて「聞く」ボタンを押下す

ⓒ2026 Information Processing Society of Japan

ると，「共通鍵を教えてください」というテキストが「チャット画面」に送信される．これに対し，送信者側から共通鍵が自動で回答され，「チャット画面」に表示される．

手順 5 では，送信者から受け取った共通鍵を正しく入力し，「復号」ボタンを押下することで，AES を用いた復号処理が実行される．その結果が図 3 であり，復号されたメッセージが「チャット画面」に表示される．なお，誤った共通鍵を入力した場合，「復号に失敗しました。共通鍵を確認してください」というメッセージが表示され，正しい共通鍵が入力されるまでメッセージは復号されない．

図 3　メッセージ復号時の画面

4.2　公開鍵モード

公開鍵モードは，公開鍵暗号方式を体験するモードである．公開鍵モードでは，1 人の学習者が，質問文を作成・送信し，回答文の復号をする「質問者」と，質問文を受け取り，回答を暗号化した後，回答文を送信する「回答者」の役割を切り替えて操作することで，暗号化から復号に至る一連の処理を 1 人で体験できる．公開鍵モードでは，「質問者による秘密鍵・公開鍵の設定と質問文の作成」，「回答者による回答文の作成と回答文の暗号化」，「質問者による回答文の復号」の手順で操作が行われる．各手順について，4.2.1 項から 4.2.3 項で解説する．

4.2.1 質問者による秘密鍵・公開鍵の設定と質問文の作成

公開鍵モードにアクセスすると，共通鍵モードと同様の構成を有する画面に遷移する．公開鍵モードでは，上部が説明領域，左部が質問者領域，中央部がチャット画面領域，右部が回答者領域である．

はじめに，学習者は，画面内の指示に従って，秘密鍵となる文字列を入力し，秘密鍵を生成する（手順 1）．次に，手順 2 では，「生成」ボタンを押下することで，手順 1 で生成した秘密鍵をもとに，RSA アルゴリズムを用いて公開鍵が生成される．続いて，手順 3 で，質問文を入力し，「鍵選択」ボタンを押下すると，「公開鍵」と「秘密鍵」が表示される（図 4）．適切な「公開鍵」を選択し，「送信」ボタンを押下することで，「チャット画面」に，「質問文」と「公開鍵」が表示され，質問文と公開鍵が送信されたことを示す．また，公開鍵モードと同様に，次手順から「回答者」として操作する必要があることをモーダルウィンドウで伝える．なお，「鍵選択」にて誤った鍵（本場面では「秘密鍵」）が選択された場合は，図 5 のようにポップアップを表示し，適切な鍵が選択されるまで次手順には遷移しない．

図 4　質問文送信時の鍵選択画面

図 5　質問文送信時の鍵選択で誤答した際の画面

4.2.2 回答者による回答文の作成と回答文の暗号化

「チャット画面」に質問文と公開鍵が表示されると，回答者領域でも質問文と公開鍵を受信したことが示される（手順 4）．次に，手順 5「回答文を作成し，暗号化」では，質問に対する回答を入力後，「鍵選択」ボタンを押下すると，「公開鍵」と「秘密鍵」が表示される．適切な「公開鍵」を選択し，「暗号化」ボタンを押下すると，RSA を用いた暗号化が行われ，作成した回答文が暗号化される．そして，手順 6「暗号化された回答文を送信」で，「送信」ボタンを押下することで，「チャット画面」に，暗号化された回答が表示される．また，次手順から「質問者」として操作する必要があることをモーダルウィンドウで伝える．

4.2.3 質問者による回答文の復号

「チャット画面」に暗号化された回答が表示されると，質問者領域で暗号化された回答文を受信したことが示される（手順 7）．次に，手順 8「受信した回答文を復号」で，

ⓒ2026 Information Processing Society of Japan

手順 1 で作成した「秘密鍵」を正しく入力し，「復号」ボタンを押下することで，復号された回答文が，「チャット画面」に表示される（図 6）．復号に失敗した場合，「復号に失敗しました。鍵を確認してください」というメッセージが表示され，正しい「秘密鍵」が入力されるまで回答文は復号されない．

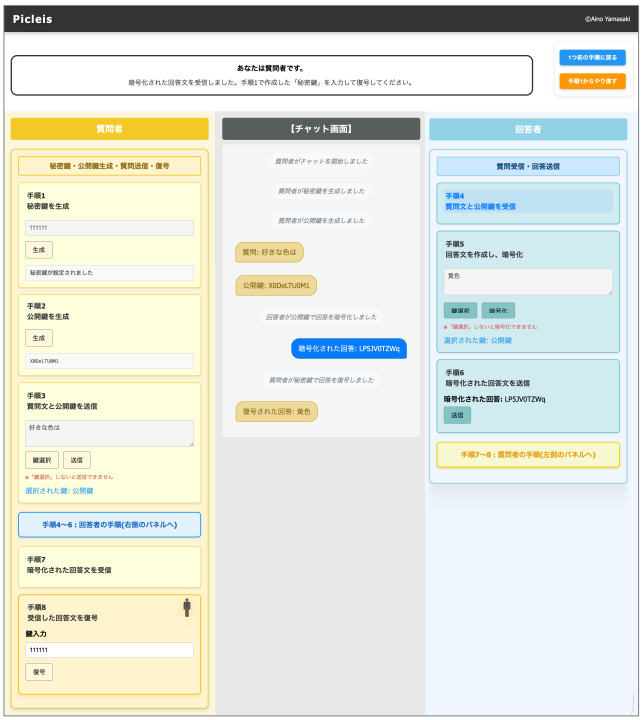

図 6　回答文復号時の画面

5.　実践・評価

5.1　実践

4 章で述べた実装指針を踏まえ，「教授者の細かな指示がなくとも，学習者個々人で Picleis を円滑に利用できるか」「Picleis を利用することで鍵暗号方式の流れを理解できるか」の 2 点を評価するために，Picleis を用いた実践授業を，青山学院大学 2025 年度秋学期科目「ウェブテクノロジー演習」の中で行った．「ウェブテクノロジー演習」は，社会情報学部 2 年生以上が対象の選択科目であり，金曜 2 限に設定されている．履修者には各週の月曜日に事前課題が課され，履修者は事前課題を済ませた状態で授業に出席する．

はじめに，2025 年 12 月 1 日に，第 11 回授業（2025 年 12 月 5 日）の事前課題を公開した．事前課題の内容は，Picleis を自由に体験し，履修者個々人で鍵暗号方式を学習することである．履修者には，Picleis の使い方を説明する 3 分程度の動画も併せて提示したほか，第 11 回授業で鍵暗号方式に関する出題を行うことも予告した．

次に，第 11 回授業内で，3 分間のミニテストおよび 5 分間のアンケートを行った．質問項目は，5.2 節で示す．

5.2　評価・考察

本節では，5.1 節で述べた実践授業の結果をまとめる．実践授業で行ったミニストの質問項目を表 1，アンケートの質問項目を表 2 に示し，ミニテストの結果を図 7，アンケートの結果を図 8, 9 に，それぞれ示す．ミニテスト，アンケートはどちらも 59 名の履修者から回答があった．

表 1　ミニテストでの質問項目

Q.	質問内容	回答形式
1-1	共通鍵暗号方式についての質問です。共通鍵は、以下の選択肢のうち、どの操作で用いますか？	三者択一
1-2	共通鍵暗号方式についての質問です。共通鍵は、どのような状態で送信者から受信者に渡されましたか？	三者択一
1-3	公開鍵暗号方式についての質問です。あなたは回答者です。質問者のピク美さんから受け取った平文の質問に対して、暗号化した回答を送信しようとしています。このとき、暗号化に使う鍵はどれですか？	二者択一
1-4	公開鍵暗号方式についての質問です。あなたは質問者です。回答者のピク子さんから暗号化された回答を受け取りました。この回答を復号に使う鍵はどれですか？	二者択一

※ 各問いの選択肢は次のとおり
- Q.1-1:「暗号化と復号」「暗号化のみ」「復号のみ」
- Q.1-2:「暗号化されていない状態で渡された」「暗号化された状態で渡された」「暗号化されたメッセージの一部として自動的に含まれていた」
- Q.1-3, Q.1-4:「秘密鍵」「公開鍵」

表 2　アンケートでの質問項目

Q.	質問内容	回答形式
2-1	ミニテストの質問に回答する際、実際にアプリケーション「Picleis」を用いて実習した場面を思い浮かべながら回答した。	六者択一
2-2	アプリケーションを使用する中で、共通鍵暗号方式と公開鍵暗号方式における鍵の受け渡しの安全性の違い（どちらが安全かなど）について、意識する場面があった。	六者択一
2-3	アプリケーションは使いやすいと感じた。	六者択一
2-4	アプリケーション内の説明を読みながら、学習を進めることができた。	六者択一
2-5	体験的に学習をすることができた。	六者択一
2-6	鍵の流れを意識しながら学習することができた。	六者択一
2-7	Picleisを使用した感想について教えてください。	自由記述

※ 六者択一の選択肢：「とてもそう思う」「そう思う」「ややそう思う」「ややそう思わない」「そう思わない」「全くそう思わない」

ミニテストの正答率は，Q.1-1 が 86.4%，Q.1-3 が 91.5%，Q.1-4 が 84.7%と高い値を示した．アンケートでは，体験的に学習できたかを尋ねた Q.2-5，学習時に鍵の流れを意識したかを尋ねた Q.2-6，ミニテストの回答時に Picleis を思い浮かべたかを尋ねた Q.2-1 で「ややそう思う」以上の回答を選択した履修者が 85%以上であった．さらに，自由記述の Q.2-7 においても，図 9 (a), (b), (c)のような回答があり，履修者は，本アプリケーションを通して鍵暗号方式を体験

ⓒ2026 Information Processing Society of Japan

的に学べ，暗号化あるいは復号で利用される鍵の種類に関する理解を得られたと考えられる．

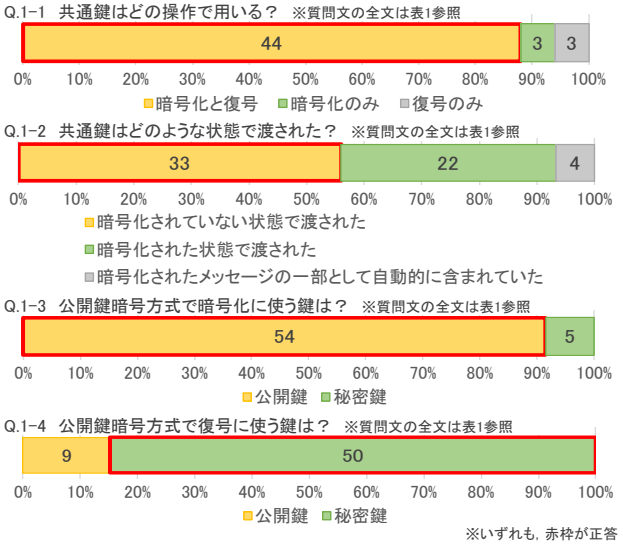

図 7　ミニテストの結果

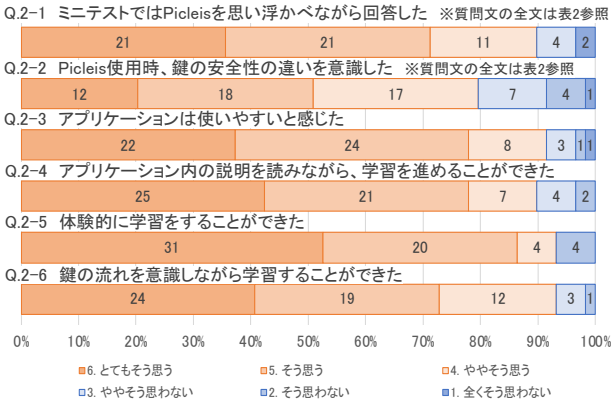

図 8　アンケート（Q.2-1 から Q.2-6）の回答分布

(a) 手順が案内されるので、進めやすかった。質問者と回答者で、パネルが離れているのがとても分かりやすく、操作しやすかった。
(b) 今まで、公開鍵や共通カギについて学んできたことはあったけれど、体験的に学んだことでイメージがすごくしやすくなり理解を深めることができた。また、安全性の差もとても意識しやすくなった。
(c) 送信者、受信者のどちらの立場も体験できたのでわかりやすかったです。実際にシミュレーションすることで記憶に残りやすかったため、とても良い教材だと感じました。
(d) どのように公開鍵や秘密鍵を使用しながら回答者と質問者でやり取りをすればよいかの流れが視覚的にわかりやすく、理解が深まった。実際に流れを体験したことで理解するまでのスピードが速くなった。
(e) 最初は公開鍵方式と共通鍵方式の違いがわかりませんでしたが、実習を通して使い分けが理解できました。チャット欄がとてもわかりやすくてよかったです。

図 9　自由記述 (Q.2-7) の回答抜粋

さらに，アプリケーションの操作性についても，アンケート Q.2-3, Q.2-4 で「ややそう思う」以上の回答を選択した履修者が 85%以上であった．また，自由記述の Q.2-7 においては，図 9 (d)のように“全体の流れが分かりやすかった”という旨の回答が 14 件 (23.7%)，図 9 (e)のように“チャット欄が分かりやすかった”という旨の回答が 7 件 (11.9%) あった．本アプリケーションの設計が概ね良好であることが示唆されたと言える．

一方で，共通鍵の安全性に関する理解を尋ねた Q.1-2 の正答率は 55.9%にとどまった．本アプリケーションでは，チャット画面で鍵の受け渡しを明示していたが，1 人で鍵暗号方式を体験することを特徴としているため，鍵の受け渡しに伴う安全性にまで学習者の注意が向きにくかったと考えられる．実際に，鍵の安全性について意識したかを尋ねた Q.2-2 では，「ややそう思う」以上の回答を選択した履修者は 80%未満，「そう思う」以上の回答を選択した履修者は約 50%となり，他の設問よりもその割合は低い結果となった．そのため，送信者と受信者といった役割に加え，サーバやクライアントといった，実際の通信環境を想像しやすい状態での体験を提供することも視野に入れる．鍵暗号方式は，ネットワークを介した通信で利用されるため，サーバ・クライアント間の通信を示すことで，学習者が暗号化の意義や安全性の重要性について意識しやすくなる可能性がある．

6. おわりに

本研究では，1 人で鍵暗号方式について体験的に学ぶことが可能なアプリケーション「Picleis」を開発し，その有用性について，実践授業を通して評価した．実践授業の結果，Picleis を利用することで，鍵暗号方式の暗号化・復号の一連の流れや，鍵の受け渡し，利用関係といった事項について理解を促進することが示唆された．一方で，鍵の安全性には履修者の意識や理解が向きにくいことが課題として示された．

今後は，二者間でのメッセージのやり取りを基本とする本アプリケーションの基本的な構成は維持しつつ，サーバ・クライアント間の通信を想定した体験を取り入れることで，暗号化の意義や安全性の重要性について意識を向けやすい環境をつくり，学習者の鍵暗号方式における安全性への理解をより高められるように発展させていくことを検討している．

謝辞　本研究は JSPS 科研費 23K21729 および 23K02718 の助成を受けたものです．

参考文献

[1] デジタル庁：デジタル社会推進実践ガイドブック DS-200 政府情報システムにおけるセキュリティ・バイ・デザインガイドライン，入手先 <https://www.digital.go.jp/assets

ⓒ2026 Information Processing Society of Japan

/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/7e3e30b9/20240131_resources_standard_guidelines_guidelines_01.pdf>（参照 2026-01-13）.
[2] 独立行政法人情報処理推進機構セキュリティセンター：情報セキュリティ 10 大脅威 2025 組織編，入手先 <https://www.ipa.go.jp/security/10threats/eid2eo0000005231-att/kaisetsu_2025_soshiki.pdf>（参照 2026-01-13）.
[3] 独立行政法人情報処理推進機構セキュリティセンター：情報セキュリティ 10 大脅威 2025 個人編，入手先 <https://www.ipa.go.jp/security/10threats/eid2eo0000005231-att/kaisetsu_2025_kojin.pdf>（参照 2026-01-13）.
[4] CS Unplugged: How do I teach CS Unplugged? <https://www.csunplugged.org/en/how-do-i-teach-cs-unplugged/>（参照 2026-01-13）.
[5] 駒野雄一，水木敬明：情報セキュリティアンプラグド ～計算機を用いない情報セキュリティ教育～，コンピュータセキュリティシンポジウム 2018 論文集，Vol.2018，No.2，pp.1101-1106 (2018).
[6] 布施泉，西田知博：一般情報教育での CS アンプラグドによる大学生の意識と知識の変化 ―公開鍵暗号に関わる教材を通して―，情報処理学会研究報告，Vol.2016-CE-134，No.24, pp.1-6 (2016).
[7] 御家雄一，米田貴，伊藤一成：ヒューマンピクトグラムアンプラグドにおける模倣学習を促す動画制作に関する一考察，2017 年度情報処理学会関西支部 支部大会 講演論文集 (E-02) (2017).
[8] 前田祐杜，御家雄一，伊藤一成：高等学校情報科における鍵暗号方式の理解を目的とした Web アプリケーションの評価，マルチメディア，分散，協調とモバイルシンポジウム 2023 (DICOMO2023) 論文集，pp.1693-1699 (2023).
[9] 山﨑愛乃，前田祐杜，石井幹大，伊藤一成：鍵暗号方式の理解を目的とした Web アプリケーション BOUCHO2 の開発，2024 年度情報処理学会関西支部 支部大会 論文集 (D-02) (2024).
[10] A. Yamasaki, M. Ishii and K. Ito: Web Based Application which Aims at Deepening Understanding of Key Cryptosystem, 2nd International Conference on Communication, Information and Digital Technologies (CIDT 2025) (2025).
[11] 大阪大学：Public-key encryption exercise， <https://oer.csedu-cme.org/tools/encrypt/index.php>（参照 2026-01-13）.
[12] 井手広康，白井詩沙香，長瀧寛之：公開鍵暗号を体験的に学習できる Web ツールを用いた教育実践，第 17 回全国高等学校情報教育研究会全国大会（愛知大会）大会冊子，p.53 (2024).
[13] X. Jiang, X. Wang, B. Wang and B. Deng: Research on Information Interaction Interface Optimization Based on Cognitive Load, 2024 4th International Conference on Computational Modeling, Simulation and Data Analysis (CMSDA 2024), pp.625-633 (2024).
[14] P. Ayres and J. Sweller: The Split-Attention Principle in Multimedia Learning, The Cambridge handbook of multimedia learning (published by Cambridge University Press), pp.135-146 (2005).
[15] Y. Zhang, Y. Tian, L. Yao, C. Duan, X. Sun and G. Niu: Teaching presence promotes learner affective engagement: The roles of cognitive load and need for cognition, Teaching and Teacher Education, Vol.129, p.104167 (2023).
[16] P. Rayavaram, S. C. Dindukuri, K. Vellamchety, J. Marward, M. Abbasalizadeh, C. S. Lee and S. Narain: Visual CryptoED: A Role-Playing and Visualization Tool for K-12 Cryptography Education, 55th ACM Technical Symposium on Computer Science Education V, Vol.1, pp.1105-1111 (2024).
[17] M. Papastergiou: Digital game-based learning in high school computer science education: Impact on educational effectiveness and student motivation, Computers & Education, Vol.52, No.1, pp.1-12 (2009).
[18] I. Jormanainen and M. Tukiainen: Attractive educational robotics motivates younger students to learn programming and computational thinking, 8th International Conference on Technological Ecosystems for Enhancing Multiculturality (TEEM), pp.54-60 (2020).
[19] Centre for Education Statistics and Evaluation: Cognitive load theory: Research that teachers really need to understand, Sydney: Centre for Education Statistics and Evaluation (2017).

ⓒ2026 Information Processing Society of Japan