Digital Life

Journal of Digital Life 2022,2,9

Article

Proposal of Rubric for Information Security Education Materials

Daisuke Saito [1], Shumon Masuda [1], Hironori Washizaki [1], Yoshiaki Fukazawa [1], Toshiharu Nishizawa [2]

[1] Waseda University, School of Fundamental Science and Engineering, 3-4-1 Okubo, Shinjuku-ku, Tokyo 169-8555, Japan
[2] Dennou Shokai Inc., 5-4-8 Shimo-takaido, Suginami-ku, Tokyo 168-0073, Japan

Abstract

This study proposes a generic rubric that can be used as an assessment axis for information security educational materials regarding existing computer science education evaluation standards to assess the learning effectiveness of information security educational materials aimed at young people. The proposed rubric includes items such as “understanding of cyber security” and “understanding why passwords are necessary,” and five-level learning objectives are defined for these items. Furthermore, the proposed rubric was used to assess the existing information security educational material “Hajimete no Joho Security (Learning First Information Security in a Different World)” using Minecraft. The proposed rubric was mapped to the learning contents of the teaching material as an assessment method, and the learning effectiveness of the teaching material was measured using Minecraft with the cooperation of a community center project in Sayama City in Japan. Therefore, we were able to evaluate the learning effects using the proposed rubric.

Keywords: Security Education; Evaluation of teaching materials; Rubric

1. Introduction

This study proposed a rubric for assessing the usefulness and learning effectiveness of information security educational materials for young people. Information security education has been studied for companies, working professionals, and university students (Ahmed, Lundqvist, Watterson, Baghaei, 2020; Yngström, Björck, 1999). In addition, the Information-Technology Promotion Agency of Japan (IPA) has proposed a Common Criteria for Information-Technology Security Evaluation (Information-technology Promotion Agency, 2017) to evaluate information security. However, these evaluation criteria are primarily useful for assessing the level of information security in businesses, and they are difficult to apply to the evaluation of educational materials and education for young people. To address this issue, this study looked at the following RQs for evaluating educational materials.

RQ1: Can we create a rubric to evaluate information security education materials?
RQ2: Can the proposed rubric be used to evaluate information security education materials?

To respond to RQ1, we proposed an evaluation index for information security education in the form of a rubric, which is a learning achievement goal, based on the Computer Science Teachers Association (CSTA) K-12 Computer Science Standards (Computer Science Teachers Association, 2017), which is a computer science education standard. As a method to answer RQ2, we investigate the possibility of using the proposed rubric as an evaluation axis by mapping it to the existing information security education material for young people “First Information Security in a Different World”(Internet-rating observation institute 2021) created by the Internet Content Review and Inspection Organization (I-ROI). The answers to these RQs are expected to contribute to the

Received: 20 April 2022, Revised: 17 May 2022, Accepted: 2 June 2022, Published: 10 June 2022
* Correspondence: d.saito@fuji.waseda.jp;
Publisher’s Note: JOURNAL OF DIGITAL LIFE. stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

evaluation of information security education for young people. Furthermore, the proposed rubric will facilitate the use and development of teaching materials.

The remainder of this article is structured as follows. The background of this study is described in Section 2. The proposed rubric is presented in Section 3. Section 4 describes the evaluation of information security education materials using the proposed rubric. Section 5 presents an experiment in a security education course to demonstrate the usefulness of rubric evaluation. Section 6 discusses the results of the evaluation. Section 7 presents related studies. Finally, Section 8 concludes this study and provides future perspectives.

2. Background

2.1. Information Security Education

Information security education for young people has been the subject of much research and is important worldwide. In Japan, the Ministry of Education, Culture, Sports, Science, and Technology's Guide to the Informatization of Education (Ministry of education, culture, sports, science, and technology, 2019) also cites information morality education as a means of fostering the ability to utilize information, an ability that is required in an information society.

Furthermore, numerous studies on information security education and the development of teaching materials have been conducted. First, we will look at a case study from Japan. Web-based information security educational materials for upper elementary school students were developed in a study by Oguma et al (Oguma, & Yamamoto, 2021).

Furthermore, in a study conducted by Shiota et al (Shiota, Takase, Sakai, Kobayashi, Yabuuch, 2019). The goal of this educational material was to allow students to assess the “suspiciousness” of problems in information security for themselves. The teaching m.od that used this material was shown to be beneficial for students in judging their own “suspiciousness.”

Second, we present examples of studies from around the world. Reid et al. demonstrate learning effects in an information security study using games (Reid, Van Niekerk, 2014). Rahman et al (Rahman, Sairi, Zizi, Khalid, 2020) showed the importance of cybersecurity education in schools through a comprehensive literature review. In particular, they raised the lack of knowledge and resources for cybersecurity education as a challenge, and stated that teachers, families, and others should work together on cybersecurity education. In a research by Geary et al (Geary, Ronke, Geary, 2019) the authors reported on the effectiveness of a 3D sandbox-type game called Minecraft in teaching information security. The results revealed that all aspects of information security can be taught in a fun way by utilizing the 3D space in Minecraft.

2.3. Rubrics

Rubrics are indicators of educational perspectives graded by learning objectives (Reddy, Andrade, 2010; Stegeman, Barendsen, Smetsers,2016). This rubric has been proposed in many educational studies (Fegely, Cherner, 2021; Saito, Kaieda, Washizaki, Fukazawa, 2020; Akram, Min, Wiebe, Navied, Mott, Boyer, Lester, 2020). A rubric based on Bloom's Taxonomy (Krathwohl, 2002) is proposed in a study by Ramsoonder et al(Ramsoonder, Kinnoo, Griffin, Valli, Johnson, 2020) for the evaluation of SQL-related cybersecurity education

2.3. Computer Science Standards for Education

Learning objectives such as information security are included in computer science educational standards such as the CSTA K-12 Computer Science Standards and the ISTE Standard (ISTE, 2016). The CSTA K-12 Computer Science Standards are the focus of this research.

> The CSTA developed the CSTA K-12 Computer Science Standards, which are standards for computer science education. These standards include several computer science assessments as well as a section on information security. The following items, for example, are included: Explain what passwords are and why we use them and use strong passwords to protect devices and information from unauthorized access (Computer Science Teachers Association, 2017).
>
> Recommend security measures to address various scenarios based on factors such as efficiency, feasibility, and ethical impacts (Computer Science Teachers Association, 2017).

As a result, this standard can be used to assess information security education. However, the goals of these items include many learning perspectives, making it difficult to evaluate teaching materials and learning using this standard. As a result, in this study, these learning perspectives are divided and the learning objectives are divided into phases to facilitate evaluation.

3. Proposal for an Information Security Education Evaluation Rubric

We proposed an evaluation index for information security education in this study, based on a rubric that divides perspectives into stages based on learning objectives. The CSTA K-12 Computer Science Standards were utilized to create the proposed rubric, and the seven elements of cybersecurity, a sub-item of the standards, were divided into 12 perspectives by referring to Networks & the internet, an item of the standards. The proposed rubric is shown in Table 1. This rubric includes 12 evaluation perspectives: “Need for Passwords,” “Understanding Cybersecurity,” “Personal Information,” “Understanding Physical Security,” “Understanding Digital Security,” “Encryption,” “Communicating Information,” “Information Ethics,” Security Measures,” “Cyber Security Measures,” “Applications of Security Measures,” and “Understanding Unauthorized Access and Attack Techniques,” were designed to allow evaluation of several information security education programs. We also divided the rubric's perspectives into five levels of learning objectives. These learning objectives were designed so that Stage 1 would be the least proficient and Stage 5 would be the most proficient. Examples are shown below:

Learning Perspective: Understand why passwords are necessary (Need for passwords)
- **Stage1:** Can explain what a password is
- **Stage2:** Can devise and set passwords
- **Stage3:** Able to analyze simple passwords hung on files.
- **Stage4:** Can set passwords that are virtually impossible to guess or analyze.
- **Stage5:** Can set and manage passwords for critical information in an organization.

Learning Perspective: Understand the cybersecurity issues that are currently occurring around the world and what to do about them (Understanding of cyber security)
- **Stage1:** Have heard of incidents related to cyber security.
- **Stage2:** Have installed anti-virus software.
- **Stage3:** Understand firewalls and be able to configure them appropriately.
- **Stage4:** Can set up a network and create their own environment to prevent unauthorized access.
- **Stage5:** Be able to gather information about current security issues and discuss security measures with the networked community.

As a problem, the seven items in the CSTA K-12 Computer Science Standards do not cover all possible assessment items for all information security education.

4. Evaluation of Information Security Education Materials

4.1. Selection of teaching materials

The proposed rubric was used to target existing information security education materials in this section, and the items were mapped to the rubric. We used the Internet Content Review and Inspection Organization’s “First Information Security in a Different World” (Internet-rating observation institute 2021) as a mapping target (I-ROI). Minecraft is a game with a high degree of freedom in which students can create various objects (large and small), raise animals, and fight against enemy characters. Minecraft also has a proven track record of being used for security education (Markman, 2020; Geary et al, 2019). Using these characteristics, “First Information Security in a Different World” aims to teach students about security measures and cyberattacks through the experience of playing a game and seeing how security measures are implemented. The “First Information Security in a Different World” program includes seven tests divided by theme as well as tests to assess the level of understanding of these tests. Figure 1 depicts an example of this material. Additionally, this material is provided in Japanese. Further, the following is an overview of what will be learned in this material:

Trial 1: Phishing
Trial 2: Protecting Files During Cyber Attacks
Trial 3: Virus (malware) countermeasures
Trial 4: Incident Countermeasures
Trial 5: How firewalls work
Trial 6: Packet Management
Trial 7: Web server port management

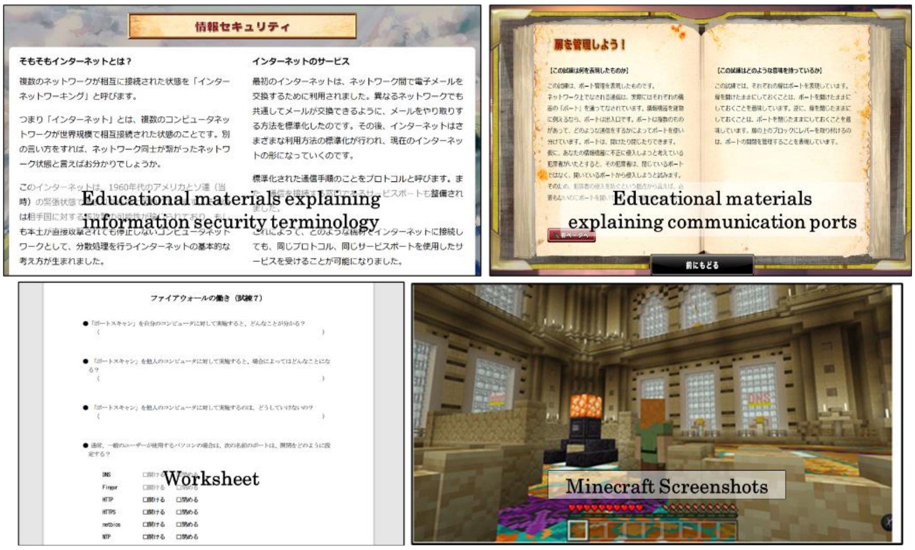
Table 1. Rubric for security education

Item No.	Learning Perspectives	Stage				
		1	2	3	4	5
1	Understanding the reason you need a password (Necessity of password)	Can explain what password.	Device and set password.	Analysis of a simple password multiplied by the file.	Can set a password that can be virtually impossible to guess and analyze.	The password can be set and managed and operated in the organization .
2	Aware of the current cybersecurity issues that are affecting the world, as well as the measures that are being taken to address them (Understanding Cyber Security)	Have heard the case related to cyber security.	Have introduced antivirus software.	Can understand the firewall and make appropriate settings.	The network can be launched, and an environment can be created to prevent unauthorized access.	Communities on the network can collect information about current security issues and consult security measures.
3	Understand how to protect personal information (Personal information)	What personal information can explain?	There is an understanding of the risk of personal information on the Internet.	Management of its personal information can be performed.	Data can be examined from data such as photos and moving images from data.	Understand the method for protecting personal information as well as the methods for keeping notes and managing information in organizational operations.
4	Understand physical security measures (Understanding Physical Security)	Understand the need for data backup.	Data is distributed and stored and corrupted.	Data storage can be used online and offline, and the method is appropriate.	Security measures can be made on physical devices.	Can determine the delivery guidelines of data in your organization and try to protect data.
5	Digital security measures are understood (Understanding Digital Security)	Understand the need for encrypted communication.	Encrypted communication and other communication can be distinguished.	Safe communication environments can be used.	Can set up a private network and build an environment where you can get attacked.	Data server operation and port can be managed, and external attacks can be prevented.
6	Understanding multiple encryption methods (Encryption)	What can be explained by encryption?	Can encrypt files.	Can use appropriate encryption properly.	Understand the calculation principle of encryption.	Can understand the vulnerability in encryption and encrypt and manage important information.
7	Understanding the safety transmission method of information (Transmission of information)	Information can be sent on the Internet.	Encryption information can be sent on the Internet.	From among the plurality of transmission methods to the scene can be used properly.	Can model paths until the information reaches the other party.	Unless environmentally dependent can communicate information safely.
8	Understand the factors such as efficiency, feasibility, ethical effects (Information ethics)	Have heard about information ethics.	Can discuss information ethics.	When operating personal information and important information, you can consider ethical issues in management.	Can be resolved quickly and efficiently for operational problems that occur.	It is possible to manage and operate high ethics and manage information.
9	Can take security measures in various cases (Security measures)	Who has heard of security measures?	There is an experience that worked on security by itself.	Understand the authentication method in security measures and know the weaknesses.	Can send and receive data after knowing the attack method.	There is an understanding of the potential problem, and its response can be discussed and supported.
10	Cyber Security can discuss recommended measures in various positions (Cyber Security Countermeasures)	Security measures can be explained anymore.	Security measures can be systematically illustrated and described.	Can build security measures and create a report on the contents of construction.	Countermeasures can be explained about report results of security measures.	Security measures are made, and their evaluation and measures can be performed and documented.
11	Understanding security measures and practical trade-off (Application of security measures)	The relationship between security measures and practicality can be described.	Can explain the specific proposal of security measures.	A specific proposal of security measures can be performed.	Security measures can be made while limiting practicality.	While maintaining practicality, security measures that meet your organization can be taken.
12	Understanding the method and measures of unauthorized access (Understanding of unauthorized access and attack method)	Have heard of news and incidents about unauthorized access.	Know how to prevent unauthorized access.	An unauthorized access can be modeled for any method.	It can be recognized that it has received unauthorized access.	Correspondence when receiving unauthorized access and identification of the attack method can be performed.

4.2. Associating rubrics with teaching materials

To confirm the usefulness of this rubric as an evaluation axis for teaching materials, the study will evaluate the learning effectiveness of “First Information Security in a Different World,” created by I-ROI. As a result, in this paper, we map our rubric to the learning contents of “First Information Security in a Different World.” This mapping makes it easier to assess the learning effectiveness of this material.

To begin with, as a premise, our proposed rubric does not cover all aspects of information security education, so we have limited the rubric to perspectives that correspond to the learning content of “First Information Security in a Different World.” We used “First Information Security Learned in Another World” as a mapping method and applied it to the rubric's perspectives. As a result, 9 out of the 12 perspectives were matched. Table 2 displays the corresponding points of view and teaching materials. However, not all of the learning contents of this material could be applied.


Educational materials explaining information security terminology
Educational materials explaining communication ports
Worksheet
Minecraft Screenshots
前ページへ
前にもどる

情報セキュリティ

そもそもインターネットとは？

複数のネットワークが相互に接続された状態を「インターネットワーキング」と呼びます。

つまり「インターネット」とは、複数のコンピュータネットワークが世界規模で相互接続された状態のことです。別の言い方をすれば、ネットワーク同士が繋がったネットワーク状態と言えばお分かりでしょうか。

このインターネットは、1960年代のアメリカとソ連（当時）の緊張状態で [illegible] は相手国に対する核攻撃の可能性が論じられており、もし [illegible] も本土が直接攻撃されても停止しないコンピュータネットワークとして、分散処理を行うインターネットの基本的な考え方が生まれました。

インターネットのサービス

最初のインターネットは、ネットワーク間で電子メールを交換するために利用されました。異なるネットワークでも共通してメールが交換できるように、メールをやり取りする方法を標準化したのです。その後、インターネットはさまざまな利用方法の標準化が行われ、現在のインターネットの形になっていくのです。

標準化された通信手順のことをプロトコルと呼びます。また、通信を接続する窓口であるサービスポートも整備されました。

これによって、どのような機材でインターネットに接続しても、同じプロトコル、同じサービスポートを使用したサービスを受けることが可能になりました。

扉を管理しよう！

【この試練は何を表現したものか】

この試練は、ポート管理を表現したものです。ネットワーク上でなされる通信は、実際にはそれぞれの機器の「ポート」を通ってなされています。情報機器を建物に例えるなら、ポートは出入口です。ポートは複数のものがあって、どのような通信をするかによってポートを使い分けています。ポートは、開けたり閉じたりできます。仮に、あなたの情報機器に不正に侵入しようと考えている犯罪者がいたとすると、その犯罪者は、閉じているポートではなく、開いているポートから侵入しようと試みます。そのため、犯罪者の侵入を防ぐという観点から言えば、必要もないのにポートを開い [illegible]

【この試練はどのような意味を持っているか】

この試練では、それぞれの扉はポートを表現しています。扉を開けたままにしておくことは、ポートを開けたままにしておくことを意味しています。逆に、扉を閉じたままにしておくことは、ポートを閉じたままにしておくことを意味しています。扉の上のブロックにレバーを取り付けるのは、ポートの開閉を管理することを表現しています。

ファイアウォールの働き（試練7）

● 「ポートスキャン」を自分のコンピュータに対して実施すると、どんなことが分かる？
（　　　　）

● 「ポートスキャン」を他人のコンピュータに対して実施すると、場合によってはどんなことになる？
（　　　　）

● 「ポートスキャン」を他人のコンピュータに対して実施するのは、どうしていけないの？
（　　　　）

● 通常、一般のユーザーが使用するパソコンの場合は、次の名前のポートは、開閉をどのように設定する？

DNS	□開ける	□閉める
Finger	□開ける	□閉める
HTTP	□開ける	□閉める
HTTPS	□開ける	□閉める
netbios	□開ける	□閉める
NTP	□開ける	□閉める

Fig.1. First Information Security in a Different World. This is a teaching material provided in Japanese. Learn the basics of information security through Minecraft (All materials are provided in Japanese)

Table 2. Correspondence between rubric and teaching materials

Learning Perspectives	Trail Number
Understanding Cyber Security	1 , 2, 3, 4, 5, 6, 7
Personal Information	1
Understanding Digital Security	1 , 2, 3, 4, 5, 7
Transmission Of Information	5, 6, 7
Information Ethics	1 , 2, 3, 4, 5, 6, 7
Security Measures	1 , 2, 3, 4, 5, 6, 7
Cyber Security Countermeasures	1 , 2, 3, 4, 5, 6, 7
Application Of Security Measures	2, 3, 4
Understanding Of Unauthorized Access And Attack Method	5, 6, 7

5. Experiments

We evaluated and investigated whether the learning material “First Information Security in a Different World” created by I-ROI could satisfy the corresponding rubric perspectives as a learning effect. In this study, we selected the “Web Server Port Management” Section of Trial 7 from the study material “Information Security for Beginners in Another World” and conducted a security education course for elementary school students in November 2021. Participants in this course were recruited from elementary school students in cooperation with the community center in Sayama City, Saitama Prefecture, Japan. Four elementary school students applied through this recruitment. Consequently, there were four participants (L1–L4) in the security education course in this experiment. Table 3 shows the gender and grade of the participants. In addition, the participants were informed that they would be given a short quiz before and after the course. The quizzes were administered anonymously. The participants were also informed that they would not be evaluated in a manner that would be detrimental to them. Details of the quiz are given in the next section.

The course lasted 3 h, including the preparation and a quiz. The topic focused on webserver port management, as mentioned above. The learning objective of the course is “to understand the fundamentals of port.” The main lecture content included a 1-h-long explanation of what a port is at the beginning. We explained to the participants that there are certain rules for communication, such as “HTTP” for web pages. In addition, we explained that these rules, “HTTP,” etc., have their dedicated passageways, with numbers such as “80” at the entrance and exit. We also taught them about port scanning, which allows them to find out which ports are “open” and “closed.” Further, we explained closing unused ports as a countermeasure against port scanning. Second, the participants learned about opening and closing ports through Minecraft to better understand ports. The learning content in Minecraft was first presented to participants with ports that should be opened and closed. Moreover, the goal was to open and close a door that looked like a port according to that goal. If it had to be closed and if the door was open, an enemy posing as a malicious communication would enter that door and the goal would fail. This Minecraft activity lasted approximately 1.5 h.

Table 3. Students Detail

ID	Grade	Gender
L1	5th	Male
L2	6th	Male
L3	5th	Male
L4	6th	Male

Table 4. Quiz details

No.	Question Content	Question Format	Possible Answers	Rubric Item Number
1	Explain with examples what a port is.	Description	Door to connect your PC to the Internet	7
2	What cannot be done if the port is closed?	Description	The relevant application is unable to communicate	7
3	You have found evidence of a port scan on your PC. What do you do first?	Description	Disconnect from the Internet and check for viruses	9
4	The home PC is not attacked because there is no important information on it.	"o" or "x" choice	x	2
5	The only way to check the port scan is manual.	"o" or "x" choice	x	9
6	It is not possible to do http communication from the main port.	"o" or "x" choice	o	7
7	http and https communicate using the same port.	"o" or "x" choice	x	7

5.1. About the Quiz

To investigate the level of understanding of web server port management, a quiz was administered before and after the course to measure the effectiveness of the course. Table 4 below shows the quizzes that were submitted. The quiz consisted of 7 questions in total, two types of questions: "o" and "x" choice type questions, and "write-in" type questions. This quiz corresponds to the rubric evaluation perspectives of "understanding of cyber security," "information communication," and "security measures."

5.2. Experimental Results

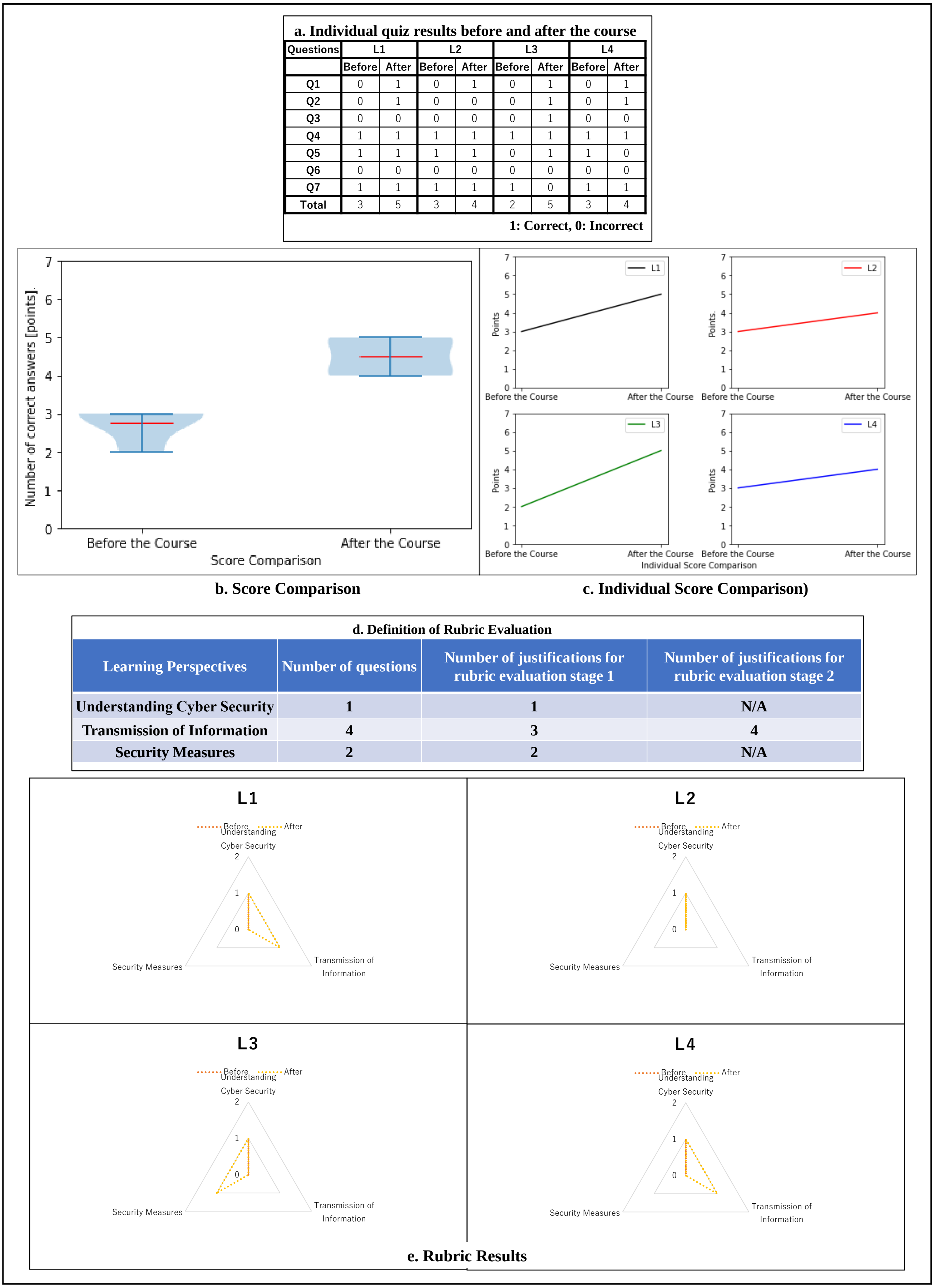
This section describes the experiment. The figure 2 shows the results of the experiment. Figure 2 shows the results of correct and incorrect answers to the quiz (a. Individual quiz results before and after the course).

5.2.1. Quizzes Results

The quiz results are presented in this section. First, the violin plot diagram in Fig.2 shows a comparison of the results across participants (b. Score Comparison). When the results were compared before and after the course, the lowest score was 2 and the highest score was 3. The lowest score after the course was 4 and the highest score was 6. The mean quiz score before the course was 2.75, and it was 4.5 after the course. The difference was 1.78 points, indicating that scores improved after the course. We now turn to the individual results. The changes in individual scores are shown in Fig.2(c. Individual Score Comparison). Fig. 2 (c. Individual Score Comparison) also shows the responses of learners from L1 to L4; all learners from L1- to L4 showed an improvement in their scores. Individual scores have risen from 3 to 4 points for L1 and L2, from 2 to 5 points for L3, and from 3 to 4 points for L4. Thus, based on these overall findings, it is possible to conclude that the port's understanding was deepened throughout the course.

5.2.2. Rubric Evaluation Results

The results of the rubric evaluation based on the quiz results are discussed in this section. The relationship between the number of justifications for the quiz and the rubric's rating levels was defined as shown in Fig.2 (d. Definition of Rubric Evaluation). If the number of justifications did not meet the definition in Fig.2 (d. Definition of Rubric Evaluation), the evaluation viewpoint was rated as "not understood" with a rating level of 0. Furthermore, the N/A locations were not evaluated because the results of this quiz indicated that they were difficult to evaluate. Fig.2 depicts the evaluation results based on this definition (e. Rubric Results). As a result, except for L2, the evaluation stages improved: L1 and L4 improved from 0 to 1 in the "communication of information" stage; L3 improved from 0 to 1 in the "security measures" stage; L4 improved from 0 to 1 in the "security measures" stage; and L4 improved from 0 to 1 in the "security measures" stage.



a. Individual quiz results before and after the course

Questions	L1		L2		L3		L4	
	Before	After	Before	After	Before	After	Before	After
Q1	0	1	0	1	0	1	0	1
Q2	0	1	0	0	0	1	0	1
Q3	0	0	0	0	0	1	0	0
Q4	1	1	1	1	1	1	1	1
Q5	1	1	1	1	0	1	1	0
Q6	0	0	0	0	0	0	0	0
Q7	1	1	1	1	1	0	1	1
Total	3	5	3	4	2	5	3	4

1: Correct, 0: Incorrect

b. Score Comparison

c. Individual Score Comparison)

d. Definition of Rubric Evaluation

Learning Perspectives	Number of questions	Number of justifications for rubric evaluation stage 1	Number of justifications for rubric evaluation stage 2
Understanding Cyber Security	1	1	N/A
Transmission of Information	4	3	4
Security Measures	2	2	N/A

e. Rubric Results

Fig.2. Experimental results

6. Discussion

This section discusses this study and presents the responses to the RQs.

6.1. Discussion of Rubric

In this study, we proposed a rubric to evaluate educational materials in information security education and to assess the extent to which these materials can achieve learning in information security education. Teaching materials and evaluation rubrics have been proposed in previous security education research, but in many cases, the teaching materials and rubrics were proposed as a set, and the rubrics are not very versatile. The learning perspectives for our proposed rubric were established using the existing CSTA K-12 Computer Science Standards for computer science education. Furthermore, we proposed a versatile learning perspective for information security education based on the CSTA K-12 Computer Science Standards. To validate the usefulness of the proposed rubric, the learning perspectives of an existing information security teaching material, "First Information Security in a Different World," were mapped to the rubric's learning perspectives. However, some items in the teaching materials were difficult to map and the rubric did not cover all items of information security education. As a result, the rubric should be expanded by referring to more existing indicators to improve its versatility.

6.2. Discussion of Experiments

In this study, a course was performed to verify whether the learning perspectives addressed by the rubric could be met by using the teaching materials. The course implemented the contents of "Trial 7" of the material presented in subsection 7.1. The validation was evaluated by a 7-point test on the communication port. The learning perspectives evaluated were "Understanding Cyber Security," "Transmission of information," and "Security measures." As a result of the course, the average score improved, as shown in Fig. 2 (b. Individual Score Comparison).

Individual results show that all students improved their scores from L1 to L4, indicating that the materials are effective for port-related items. However, there was no change in the learning achievement stage of L2. In the L2 responses, Q1 was answered incorrectly before the course and correctly after the course. Q1 was a descriptive question that described the port with an example. This question corresponds to the "Transmission of information" learning perspective of the rubric. The other questions corresponding to "Transmission of information" are Q2, Q6, and Q7; L2 correctly answered Q6 before the course but was assigned a learning achievement level of 0 based on the rubric's definition of learning achievement level. L2 correctly answered two questions after the course, Q1 and Q6. However, to reach achievement Stage 1, L2 had to correctly answer three questions. As a result, the L2 achievement level was 0. Furthermore, L3 correctly answered Q7 before the course and L4 correctly answered Q5. However, they answered incorrectly after the course. Since both questions were multiple-choice, it can be said that the students responded intuitively before the course. The learning perspectives for L3, "Transmission of information, " and L4, "Security measures," were 0 both before and after the course, by definition of the rubric's assessment of the learning achievement stage. Furthermore, L1 and L4 improved their learning achievement in the learning perspective of "information transfer." As a result, it is suggested that the materials used were effective in improving the achievement level of "information communication" from a learning standpoint. l3 increased the level of achievement in the learning perspective of "security measures."

As a result, the materials used may improve the achievement level of the learning perspective of "security measures." However, the teaching materials may be ineffective in terms of improving the achievement of the learning perspective of "understanding cyber security." These results suggest that the proposed rubric can be used to evaluate security education materials and identify areas for improvement. However, additional data collection is required due to the small number of participants and the possibility that the rubric's effectiveness may be dependent on teaching methods.

6.3. Answer to Research Questions

6.3.1. RQ1: Can we create a rubric to evaluate information security education materials?

Using the CSTA K-12 Computer Science Standards and dividing the learning perspectives required for security education into stages, the responses to RQ1 were able to create a rubric. However, the proposed rubric does not cover all aspects of information security learning. As a result, it must be expanded to include indicators other than the CSTA K-12 Computer Science Standards, as described in Section 6.1.

6.3.2. RQ2: Can the proposed rubric be used to evaluate information security education materials?

In response to RQ2, the proposed rubric can be used to evaluate information security education materials by mapping the learning items of the materials to the learning perspectives of the rubric as shown in Table 2.

Furthermore, we ran and evaluated a course using the mapped instructional materials. As a result, as illustrated in Fig.2 (Rubric Results), the learning perspectives in information security based on the rubric can be easily grasped in terms of the participants' achievement stage. However, due to the small number of participants in this course, additional verification is required.

6.4. Threats of validity

Threats of validity in this study include: (1) Only CSTA was used to create the rubric, which does not cover all information security learning perspectives; (2) Only certain items in existing security education materials were evaluated; (3) The number of participants in the course is small and statistical analysis is not available.
These validity threats will be addressed through modification of the rubric and further experimentation.

7. Related Works

In this Section, we highlight relevant studies and demonstrate the benefits of our research. Many studies have addressed information security education activities for young people(Oguma et al 2021; Shiota et al, 2019; Geary et al, 2019). Learning effects have been assessed in these studies. However, the evaluations used in these studies are limited in their applicability. Furthermore, the evaluation methods must be reviewed each time new teaching materials are developed. Ramsoonder et al. conducted another study (Ramsoonder et al, 2020). This study used Bloom's taxonomy to map a cybersecurity education curriculum. A rubric was also proposed in this study. The proposed rubric is SQL-related, which is still a limitation in terms of versatility.
In our study, we proposed a rubric that is versatile enough to avoid the need to design new assessments due to changes in teaching materials.

8. Conclusion and Future

We proposed a rubric to assess the learning effects of using information security education materials. The proposed rubric is based on the security items of CSTA K-12 Computer Science Standards, and the learning perspectives are defined. We also divided the learning perspectives into five levels of learning objectives. Furthermore, we assessed an existing educational material on information security, “First Information Security in a Different World,” to show whether the proposed rubric can be used for evaluation. As a result of the evaluation, it became easier to understand the points to be enhanced in the said educational material. However, as an issue, not all items were statistically evaluated. As a result, for future research, we plan to reconsider and verify whether the range of the step-by-step evaluation of learning perspectives in the rubric is even, to verify the learning effects of “First Information Security in Another World” and other information security educational materials, and to improve the method of measuring learning effects.

Author Contributions

Conceptualization, D.S. and S.M.; methodology, D.S. and S.M.; validation, D.S., S.M. and T.N.; formal analysis, D.S.; investigation, D.S. and S.M.; writing—original draft preparation, D.S. and S.M.; writing—review and editing, D.S. and H.W.; visualization, D.S.; supervision, H.W. and Y.F.; project administration, D.S.; All authors have read and agreed to the published version of the manuscript.

Funding

This research received no external funding

Institutional Review Board Statement

This research complies with the Ethics Regulations related to Research with Human Subjects of Waseda University and was exempted from ethics review and approval as a result of checking the Application Guidelines for Ethics Review.

Informed Consent Statement

Not applicable

Acknowledgments

The authors would like to thank the people at the educational institutions who helped with the experiment. The authors would like to thank Enago (www.enago.jp) for the English language review.

Conflicts of Interest

The authors declare no conflict of interest

References:

Ahmed, A., Lundqvist, K., Watterson, C., & Baghaei, N. (2020, October). Teaching cyber-security for distance learners: A reflective study. In *IEEE frontiers in education conference (FIE), 2020* (pp. 1–7). IEEE Publications.

Akram, B., Min, W., Wiebe, E., Navied, A., Mott, B., Boyer, K. E., & Lester, J. (2020, February). A conceptual assessment framework for K-12 computer science rubric design. In *Proceedings of the 51st ACM Technical Symposium on Computer Science Education* (pp. 1328–1328).

Computer science teachers association. (2017). *Standards | Computer science teachers association. Computer science teachers association*. https://csteachers.org/Page/standards

Fegely, A., & S Cherner, T. S. (2021). A comprehensive rubric for evaluating EduVR. *Journal of Information Technology Education: Research*, *20*, 137–171. https://doi.org/10.28945/4737

Geary, J., Ronke, T., & Geary, M. (2019). Using Minecraft education edition to teach cybersecurity self-defense, annual Research symposium at Dakota State University.

Information-Technology Promotion Agency. (2017, April). Common criteria for Information Technology security evaluation. https://www.ipa.go.jp/security/jisec/cc/index.html. IPA Information-Technology Promotion Agency.

Internet-rating observation institute. (2021). *First Information Security in a Different World*. http://dcajr.jp/isekai/.

Iste. (2016). ISTE standards. *Students*. https://www.iste.org/standards/iste-standards-for-students.

Krathwohl, D. R. (2002). A revision of Bloom’s taxonomy: An overview. *Theory into Practice*, *41*(4), 212–218. https://doi.org/10.1207/s15430421tip4104_2

Markman, C. (2020). MetaMinecraft: Cybersecurity education through commercial video games. In *Cybersecurity for information professionals* (pp. 89–107). Auerbach Publications.

Ministry of Education, Culture, Sports, Science, and Technology. (2019). https://www.mext.go.jp/content/20200609-mxt_jogai01-000003284_001.pdf. Ministry of Education, Culture, Sports, Science, and Technology, Ministry of Education, Culture, Sports, Science, and Technology.

Oguma, R., & Yamamoto, R. (2021). Information security Web teaching material development and class practice in the upper grades of elementary school. *Journal of Educational Information Research*, *37*(1), 53–63. https://doi.org/10.20694/jjsei.37.1_53

Reddy, Y. M., & Andrade, H. (2010). A review of rubric use in higher education. *Assessment and Evaluation in Higher Education*, *35*(4), 435–448. https://doi.org/10.1080/02602930902862859

Ramsoonder, N. K., Kinnoo, S., Griffin, A. J., Valli, C., & Johnson, N. F. (2020, December). Optimizing Cyber Security Education: Implementation of Bloom’s Taxonomy for future Cyber Security workforce. In International Conference on Computational Science and Computational Intelligence (CSCI), *2020* (pp. 93–98). IEEE Publications.

Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5), 378–382. https://doi.org/10.18178/ijiet.2020.10.5.1393

Reid, R., & Van Niekerk, J. (2014). Snakes and ladders for digital natives: Information security education for the youth. *Information Management and Computer Security*, *22*(2), 179–190. https://doi.org/10.1108/IMCS-09-2013-0063

Saito, D., Kaieda, S., Washizaki, H., & Fukazawa, Y. (2020). Rubric for measuring and visualizing the effects of learning computer programming for elementary school students. *Journal of Information Technology Education: Innovations in Practice*, *19,* 203–227.

Shiota, S., Takase, K., Sakai, K., Kobayashi, K., & Yabuuch, S. (2019). Development and evaluation of information security teaching materials to encourage a sense of ownership in junior high school students: development of card teaching materials for judging “suspicious”. *Computers and Education*, *44(0)*, 85–90. https://doi.org/10.14949/konpyutariyoukyouiku.44.85

Stegeman, M., Barendsen, E., & Smetsers, S. (2016, November). Designing a rubric for feedback on code quality in programming courses. *Proceedings of the 16th Koli Calling International Conference on Computing Education Research* (pp. 160–164).

Yngström, L., & Björck, F. (1999, June). The value and assessment of information security education and training. In *Proceedings of the IFIP TC11 WG11*, *8*.