研究論文

鳴門教育大学情報教育ジャーナル No.19 pp.43-47 2022

Scratch を用いた小学校高学年における安全なパスワードを考えるための体験型教材開発

西脇勇斗*，阪東哲也**

情報技術の浸透により，ICT の理解に基づく，ICT の適切な利活用が一層求められている。ICT に関するリテラシーの育成に向けて，パスワードに関する教育（以下，パスワード教育）の実施が考えられる。しかし，小学校学習指導要領（平成 29 年告示）には，パスワード教育に関する取り扱いについて明記されておらず，初等教育でのパスワード教育の教材開発は急務である。本論文では，小学校高学年が安全なパスワードを考えるための体験型教材を Scratch で開発した。安全なパスワードの特徴として 3 点を取り上げ，パスワードの安全性を確認する体験を通して，取り上げた安全なパスワードの特徴に気づかせられるように教材を設計した。

[**キーワード**：情報セキュリティ，小学校高学年，パスワード，Scratch]

1. はじめに

スマートフォンやタブレット端末が一般家庭に飛躍的に普及しており，誰もがインターネットを介して情報を扱う時代となった。IoT やビッグデータ，AI といった情報技術の一層の浸透による社会変化に対応できるように，平成 29 年度告示の学習指導要領では，情報活用能力が学習の基盤となる資質・能力として位置づけられており[1]，ICT の理解に基づく，ICT の適切な利活用が一層求められている。

ICT に関するリテラシーの育成に向けて，パスワード教育の実施が考えられる。しかし，現行の小学校学習指導要領[2]には，パスワードに関する取扱い（指針）については明記されていない。坪根らは，パスワード教育が各校に任されるために，パスワード教育の扱いに差が生じる可能性を指摘している[3]。初等教育におけるパスワード教育の水準を担保しつつ，より充実したものとするために，パスワード教育に関する教材開発は喫緊の課題といえる。

そこで，初等教育におけるパスワード教育の足掛かりとして，小学校高学年で使用できるビジュアル型プログラミング言語 Scratch を用いた，安全なパスワードについて考えさせる体験型教材を開発することとした。

2. 安全なパスワードの特徴

2.1 パスワードの被害状況

IPA(情報処理推進機構)が公開している情報セキュリティ 10 大脅威 2021 個人編[4]には，「インターネット上のサービスへの不正ログイン」がランクインしており，不正ログインによって出金機能が悪用され，金銭的被害を招いている。この攻撃手口として，パスワードリスト攻撃やパスワード推測攻撃による不正ログインが報告されている。特に後者の攻撃では，利用者が使いそうなパスワードや名前，誕生日を使ってパスワードを推測し攻撃していることが示されている。

2.2 安全なパスワードのガイドライン

我が国における情報セキュリティ対策の普及啓発を行っている IPA，JPCERT/CC では，パスワード作成時に用いる文字の種類，文字の数，使用する文字についてガイドラインを提供している。

パスワード作成時に用いる文字の種類については，できる限り多く使うことが推奨されており，大小英字，数字及び記号を混在させて作るべきとしている[5]。パスワード作成時に用いる文字の数については，できる限り長くなるようにすることが推奨されている。IPA では最低でも 8 文字以上[5]，JPCERT/CC では 12 文字以上で作るべきとしている[6]。使用するパスワードについては，簡単に想像できる単語を含まないことが推奨されている。JPCERT/CC には，推測されやすい文字の並びを避けて作るべきとしている[6]。

* 鳴門教育大学 大学院高度学校教育実践専攻 自然・生活系教科実践高度化コース(技術・工業・情報科教育実践分野) 大学院生
** 鳴門教育大学大学院 高度学校教育実践専攻 自然・生活系教科実践高度化コース(技術・工業・情報科教育実践分野)

3. 教材開発

3.1 概要

学習者がパスワードの安全性を確認し，安全なパスワードについて考えられるようにするための体験型教材として，ビジュアル型プログラミング言語 Scratch を用いた「パスワードチェッカーズ」を開発した[8]。図 1 に「パスワードチェッカーズ」を示す。

本教材を通じて，実際に学習者は入力したパスワードの安全性を確認する体験ができる。本教材上で表示される結果から安全なパスワードの特徴について考え，パスワードの安全性を確保するために必要な条件を理解できるようになることをねらいとする。

3.2 本教材で学習する 3 つの特徴

学習者に理解させる安全なパスワードの特徴として，次の 3 つを選定した。①文字の種類が多いこと，②文字の数が多いこと，③簡単に想像できる単語を含まないことである。

3.3 教材の構成

3.3.1 安全なパスワード：文字の種類

数字とアルファベット小文字を使用し，3 つの文字パターンで総当たり攻撃を行う。表 1 に，文字パターン別の割り当てられる文字一覧を示す。

表 1 の文字パターン(3)のように，数字のみやアルファベット小文字のみよりも，2 種類以上の文字の種類を混合してパスワードを作成することで，攻撃用パスワード生成時に，より多くの文字を割り当てる必要が生じる。割り当てる文字が増えることで，総当たり攻撃にかかる時間も増加し，パスワードの安全性も向上すると考えられる。

図 1　パスワードチェッカーズ

3.3.2 安全なパスワード：文字の数

表 2 に，数字とアルファベット小文字をパスワードに用いる際の攻撃用パスワードの候補数を示す。利用できる文字の数が多いほど，膨大な数の攻撃用パスワードを全て確認する必要があるため，総当たり攻撃にかかる時間も増加し，安全性も向上すると考えられる。

3.3.3 安全なパスワード：使用する単語

例えば「happy12345」は，数字とアルファベット小文字の混合かつ 10 文字のパスワードである。「happy12345」の総当たり攻撃にかかる時間は，10 文字であることから IPA のガイドラインに示された 8 文字より長くなると想定されるが，実際にパスワードとして使用するのは危険である。このパスワードは誰もが容易に想像できる単語のみで構成されているからである。誰もが容易に想像できる単語のみで構成されたパスワードは安全でない判断されることで，より的確にパスワードの安全性を確認できると考えられる。

3.4 パスワードの安全性の判定方法

パスワードを判定する時間は，授業時間内での活用を考慮して，総当たり攻撃は 10 秒間と設定した。

10 秒間の総当たり攻撃時に効率良くパスワードの安全性の判定を行うために，2 つの攻撃アルゴリズムを採用した。1 つ目は一般的な総当たり攻撃である。学習者が入力したパスワードに対して，攻撃用パスワードを次々に生成し，一致するかどう

表 1　文字パターン別の割り当てられる文字

文字パターン	割り当てられる文字	数
(1) 数字	0123456789	10
(2) アルファベット小文字	abcdefghijklm nopqrstuvwxyz	26
(3) 数字・アルファベット小文字	0123456789 abcdefghijklm nopqrstuvwxyz	36

表 2　文字の数別の攻撃用パスワードの候補数

文字の数	攻撃用パスワードの候補数
1	36
2	1,296
3	46,656
4	1,679,616
8	2,821,109,907,456
12	4,738,381,338,321,620,000

かを確認する。2 つ目は総当たり攻撃にパスワードリスト攻撃を掛け合わせた攻撃である。これまでに漏洩されたことが報告されているパスワードのうち，「12345678」や「password」，「qwerty」といった上位 10 万のパスワードを用意し[7]，次々に一致するかどうかを確認する。

3.5 攻撃用パスワード生成のアルゴリズム

図2に，攻撃用パスワード生成のアルゴリズムを示す。攻撃用パスワードは，3 つの文字パターンで同時並行に生成され，学習者が入力したパスワードへの総当たり攻撃を行う。3 つの文字パターンとは，表 1 に示した(1)数字，(2)アルファベット小文字，(3)数字・アルファベット小文字である。

総当たり攻撃は，10 秒が経過するまで，或いは学習者が入力したパスワードが発見されるまで行う。生成される攻撃用パスワードの文字の数は1から始まり，その文字の数で考えられる全ての攻撃用パスワードの総当たり攻撃が終了すると，文字の数は2に増え，同様の処理が繰り返し行われる。

攻撃用パスワード生成には，攻撃用カウントが使用される。0 から始まり，新たな攻撃用パスワードを生成する度に1ずつ増加する。この変数はカウントとして使用するため，計算用に計算用カウントが用意され，攻撃用カウントの値が代入される。

計算用カウントは，各パターンに割り当てられる文字の数（以下，割当文字数という）で剰余され，0～(割当文字数-1)の整数を得る。この整数が各パターンの文字のリスト番号として，対応した文字が攻撃用パスワードに結合される。計算用カウントは0になるまで割当文字数で切り捨て除算される。ここまでで生成される攻撃用パスワードの文字の数が，変数で定義される文字の数に満たない場合がある。この場合，各パターンの文字リストの1番目が，足りない文字の数の分だけ結合される。

この段階で攻撃用パスワードは学習者が入力したパスワードと比較される。一致時はパスワード発見となり，不一致時は最初の判定前へ戻る。

3.6 判定結果による表示の変化

学習者が入力したパスワードが3.4の判定にて発見された場合と発見されなかった場合で，画面遷移が変化するようにした。図3に総当たり攻撃時の本教材の画面遷移を示す。

10 秒以内に発見された場合，入力したパスワードが発見されたこと及びそのパスワードが安全でないことを表示し，その後発見までにかかった時間を表示する。少なくとも 10 秒以内に発見されたパスワードには「あなたのパスワードは安全ではありません」と明確なフィードバックを返すようにした。

一方，10 秒以内に発見されなかった場合，入力したパスワードが発見されなかったことを表示し，その後一致するまでにかかる時間を試算して表示する。なお，発見されなかった場合に入力したパスワードが安全と表示しないのは，10 秒間の総当たり攻撃で発見されないパスワードが全て安全とは言い切れないためである。

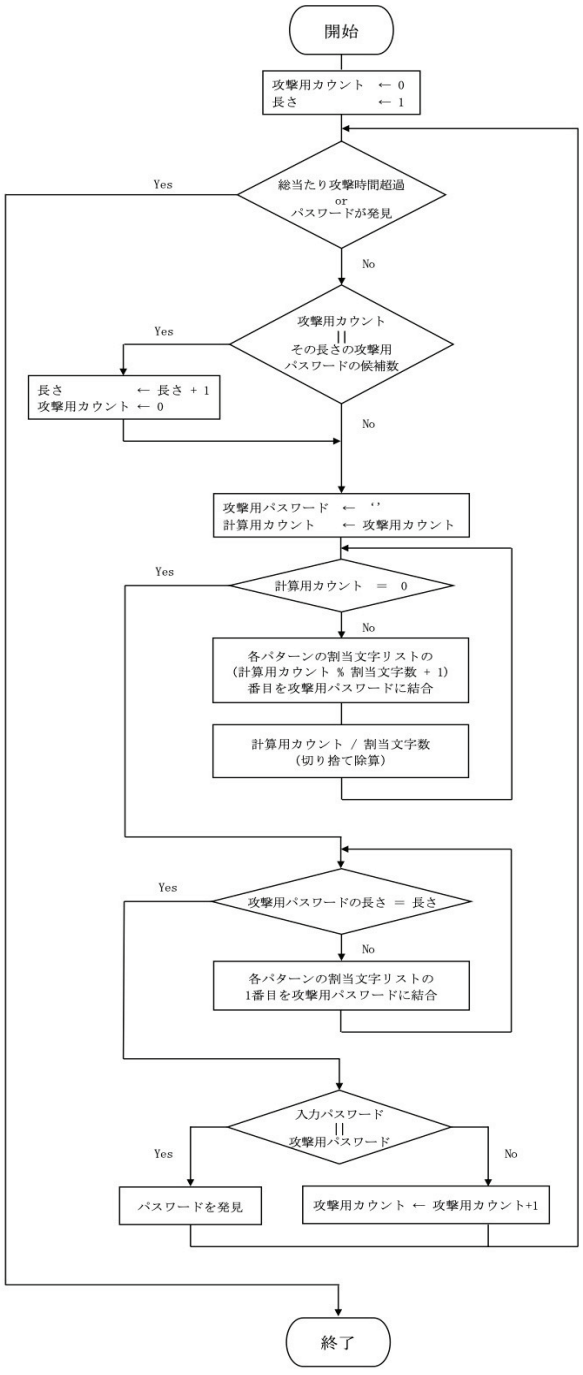

図 2　攻撃用パスワード生成のフローチャート

4. 本教材の発展的活用

本教材は Scratch で作成しているため，学習者が自由にプログラム部分を改変できることに，利点がある。プログラム部分を改変する活動を授業に取り入れることで，より実感をもって，安全なパスワードへの理解を深める効果が期待できる。改変例として次の 3 点を取り上げる。

4.1 総当たり攻撃時間の変更

総当たり攻撃時間は，プログラム中の変数「制限時間[秒]」を変更することで，学習者が任意の時間に設定できる。例えば，総当たり攻撃時間を 10 秒から 1 日に変更することで，より多くのパスワードが発見できてしまうことを実感させることができる。

4.2 総当たり攻撃に用いる文字の追加

表1に示した各文字パターンに割り当てられている文字を学習者が追加できる。例えば，デフォルトで設定している数字とアルファベットに加えて，記号も総当たり攻撃の対象とすることができる。記号を追加したい場合は，本教材のプログラム中の定義「～リスト準備」に含まれるリスト「～リスト」上に追加したい記号を1つずつ入力すればよい。なお，Scratch は仕様上，アルファベット大文字と小文字は区別できないことは留意する必要がある。

4.3 パスワードリストに単語の追加

3.4 に示した 2 つ目の攻撃アルゴリズムで使用するパスワードリストに，新たな単語を追加できる。追加する手順は，Scratch で本教材のプログラムを開き，Scratch のブロックパレットの「変数」にある「パスワードリスト」のチェックボックスにチェックを入れる。Scratch のステージ上に「パスワードリスト」のリストの中身が表示されるようになる。「パスワードリスト」上の「＋ボタン」をクリックすることで，新たな単語を追加できる。例えば，先生が学級で流行している言葉をパスワードリストに追加することで，児童により馴染みのある単語を含めて，パスワードの安全性を判定させることができる。

また，児童同士で単語を追加して，どちらが先にパスワードが発見されるかといったゲーム性をもたせた学習に取り組ませることも考えられる。

5. まとめ

本論文では，小学校高学年が安全なパスワードを考えるための体験型教材を Scratch で開発した。安全なパスワードの特徴について3つを選定し，児童がパスワードの安全性を確認する体験を通して，

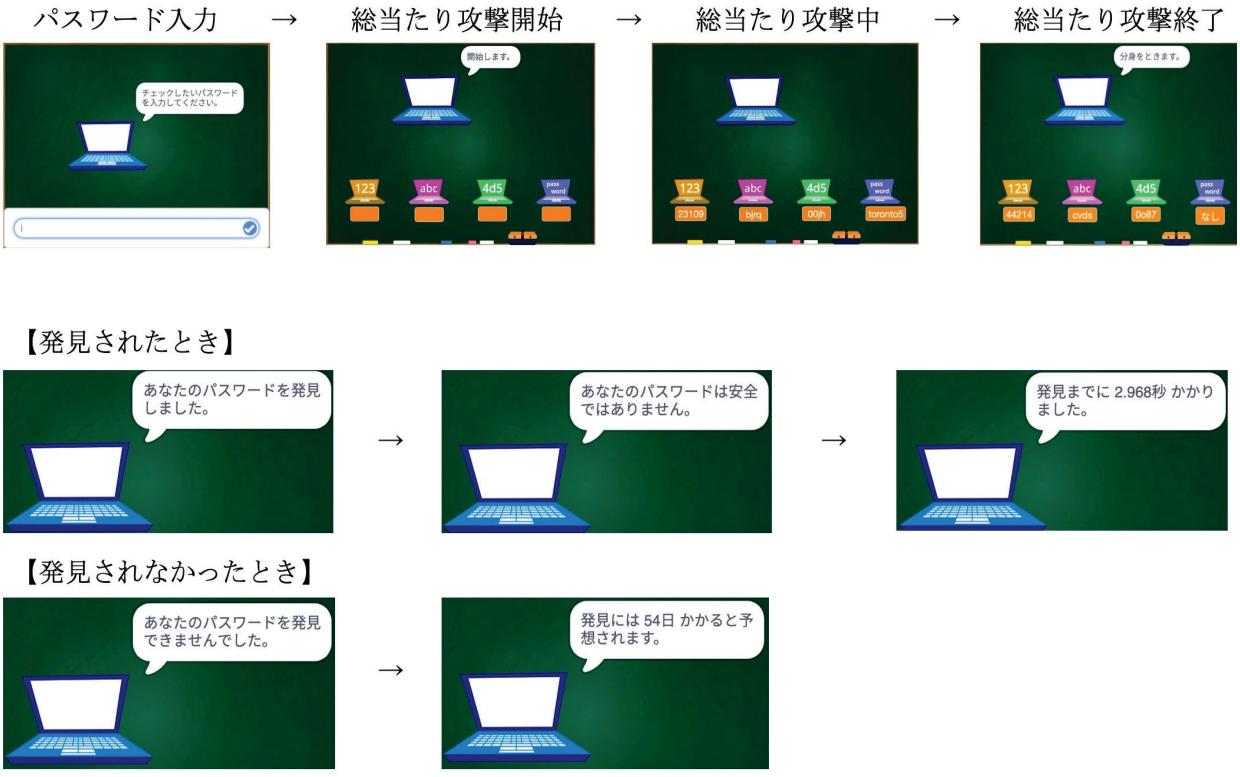

図 3　教材の画面遷移

実感を伴う理解につなげられるように教材開発を行った。

今後，本教材を用いた授業実践を行う予定である。授業後にアンケートを実施し，分析を通して，本教材を活用した教育的効果を検証する。Scratchを活用した教材は小学校高学年だけではなく，中学生を対象としても十分に機能すると考えられる。小学校高学年での検証結果を踏まえて，小学校高学年を対象とし，パスワードの安全性に関する実感をもった理解につなげられる機能を検討することに加えて，中学生でも使えるように改善を検討したい。

参考文献

[1] 文部科学省，学習の基盤となる資質・能力としての情報活用能力の育成，https://www.mext.go.jp/content/20201002-mxt_jogai01-100003163_1.pdf （最終閲覧日：2022 年 1 月 31 日）

[2] 文部科学省，小学校学習指導要領(平成29年告示)，東洋館出版社

[3] 坪根恵・長谷川彩子・秋山満昭・森達哉：日本国内における児童向けセキュリティ教材の実態調査．研究報告セキュリティ心理学とトラスト(SPT)，2021，43，pp.1-8.

[4] IPA(情報処理推進機構)，情報セキュリティ10大脅威[個人編]，https://www.ipa.go.jp/files/000089480.pdf（最終閲覧日：2022年1月31日）

[5] IPA，日常における情報セキュリティ対策，https://www.ipa.go.jp/security/measures/everyday.html（最終閲覧日：2022年1月31日）

[6] JPCERT/CC，STOP！パスワード使い回し!，jpcert.or.jp/pr/stop-password.html （最終閲覧日：2022年1月31日）

[7] NCSC(National Cyber Security Centre)，PwnedPasswordsTop100k，https://www.ncsc.gov.uk/static-assets/documents/PwnedPasswordsTop100k.txt（最終閲覧日：2022年1月31日）

[8] 西脇勇斗・阪東哲也(2021) 小学校高学年に向けた安全なパスワードを考えるための体験型教材開発，日本産業技術教育学会第 37 回四国支部大会講演趣旨集，B8