

数学教育におけるリスク対応を意図した教材開発と授業実践 —中学校第3学年「『安全』で『使いやすい』パスワードはどんなパスワード?」の分析—

笹瀬 大輔
(菊川市立菊川東中学校)

裕元 新一郎
(静岡大学)

Developing Teaching Materials and Classes Intended to Address Risks in Mathematics Education:

9th grade "What makes a password "secure" and "easy to use"?"

Sasase Daisuke Matsumoto Shinichiro

要旨

本研究の目的は、中学校数学科におけるリスクを扱った教材研究と授業実践を通して、リスクを数学科で扱う際の教材の要件と授業で扱う上での留意点を導出することである。中3を対象として「日常生活における情報漏洩のリスク」を題材として、教材開発及び授業実践と分析を行った。生徒は、情報化社会の中でパスワードがどのように作られ、活用されているか、どんなパスワードが推測されやすいかなどを学び、社会の意思決定や問題解決、については、リスク回避に数学がどのように貢献しているかを感じることができた。考察の結果、リスクを数学科で扱う際の教材の要件として、生徒に身近で数学的根拠のある題材を取り上げること、トレードオフの関係があるリスク分析をすることを挙げた。また、リスクを数学科の授業で扱う留意点として、身近で緊急性のある「避けられないリスク」を数学的に分析し、リスクを減らす行動をとれる気づきが得られる授業を構想すること、主観的リスクから客観的リスクに変換することの2点が得られた。

キーワード： リスク、いろいろな関数、パスワード、情報漏洩、トレードオフ

1. 研究の背景と研究の目的・方法

現代においては、新型コロナウイルス感染症(COVID-19)などの社会の根幹を揺るがすリスクだけでなく、交通事故による怪我、危険生物による被害、誤情報・偽情報によるトラブルなど、身近に起きる新旧のリスクが生まれ、私たちは様々な不安感に囲まれながら生活している。筆者らの研究グループでは、このようなリスク社会において、認知したリスクに対する確に判断・行動するためには算数・数学を用いることが重要であるという立場に立ち、小中高での指導のあり方を追究して研究を進めている。

裕元(2021)は、数学教育がリスク社会に貢献することの重要性を指摘し、小中高を通した多様な教材例を開発して授業実践を行い、児童・生徒の実態を分析・考察することの必要性を述べている。そこで、本研究では、中学校数学科におけるリスクを扱った教材研究と授業実践を通して、リスクを数学科で扱う際の教材の要件と授業で扱う上での留意点を導出することを目的とする。

リスクを扱った中学校の先行実践例として、「焼きそばの単価を決めよう(中3)」(藤原, 2024)、「そのメール開きますか(中3)」(菊野, 2024)、「あなたの買い物で温暖化を止める!?(中1)」(菊野, 2025)、「夏の外での活動はいつまで実施できそうか

(中2)」(笹瀬, 2025)がある。異なるリスクに対する教材研究や実践を積み重ねて、中学校数学科におけるリスクに関わる指導のあり方を深める必要がある。

筆者(第1著者)は、生徒が技術科の授業の情報セキュリティを学ぶ単元で、パスワードを題材に、情報漏洩リスクを学んでいることを知った。生徒は、校内で配布されている1人一台端末にパスワードを入力して使用していたり、個人のスマートフォンでもパスワードを使ってアカウントの管理をしていたりして、パスワード・パスワードは身近な存在である。一方で、そのパスワードが解析され、情報漏洩により起こるリスクへの認知は不十分であると考えた。そこで、パスワードが解析されることによって起こるリスクを学んだ上で、パスワードの「安全性」と「使いやすさ」について、生徒自らが、数学的な思考で冷静に分析することで、情報漏洩のリスクと向き合う態度を育てたいと考えた。

そこで、以下の方法で、本研究を進めることにした。

- ① 中3関数領域において教材を開発する。
- ② 授業実践を行って授業の様子を明らかにする。
- ③ リスクを数学科で扱う際の教材の要件及び授業で扱う上での留意点を考察する。
- ④ 今後の課題をまとめる。

II. 授業の構想

牧之段 (2023) と富田 (2024) は、小学校・高校の実践をもとに、対象のリスクを児童・生徒が自分事として捉えることのできる教材開発を行うことの重要性を指摘している。本実践も、中学生が日常生活のリスクを自分事として捉え、より深いリスクの分析になるように授業を構想した。

なお、栢元他 (2023) の数学教育においてリスクを扱う際の枠組みの観点に基づき、本時におけるリスクを扱う際の枠組みとの対応を表 1 のように整理した。

表 1 本実践の「リスクを扱う際の枠組み」との対応

・ 観点 1 リスクの場面	情報漏洩
・ 観点 2 リスクの文脈のレベル	C 社会的
・ 観点 3 リスクの内容	⑩高度技術リスク
・ 観点 4 行動の種類	②身の回りの用事
・ 観点 5 モデルをつくる目的	
① 現象のしくみを理解する	
・ 観点 6 算数・数学の内容(領域)	C 解析
・ 観点 7 リスクを算数・数学で考察する力	
② 変数を選択する力(計画を立てる:定量的)	
③ リスクを数学的に捉える力(数学化する)	
④ 算数・数学のきまりに従って処理する力(算数・数学内)	
⑥ 算数・数学でリスクを予測・推測する力	
⑧ 場面に戻ってリスクを検討したり、リスクに対応したりする力(リスクの評価)	
・ 観点 8 リスクリテラシー	
③リスクに関わる意思決定や行動につなげる力	

本実践は、中 3「2 乗に比例する関数」の単元後半の「いろいろな関数」の学習内容と関連付けて 2 時間授業として行う。

(1) 第 1 時 リスク認識とパスワードの組み合わせ

<数学科に関わる目標>

・パスワードに使用できる文字の種類が増えると、組み合わせの数が爆発的に増えることがわかる。

<リスクに関わる目標>

・パスワードに使用できる文字の種類により、パスワード解析の時間の差異があることがわかる。

① 導入 リスク認識

日常生活におけるリスクを数学科の授業で扱う場合、生徒自身のリスクの認知は欠かせない。そこで、「あなたのパスワード、大丈夫?」という問いかけから始め、身近な事例から情報セキュリティの重要性を認識できる導入をする。「なぜパスワードが必要な?」「どんなパスワードが危険だと思う?」といった問いと、有名人のアカウント乗っ取り事件や、なりすましアカウントから生まれた金銭トラブルの事例を取り上げ、リスクを認識する導入が必要であると考える。

② 展開 A 推測されやすいパスワードを知る

アカウントが乗っ取られた理由は、パスワードが流

出してしまった、または、推測されてしまったためである。種類や桁数が多くても、推測されやすいパスワードがある。以下のような例を生徒に示し、推測されやすいパスワードの注意を促す(表 2 も参照)。

- ・ 氏名やニックネーム、生年月日、電話番号、家族やペットの名前、辞書掲載英単語
- ・ キーボードの配列(例:qwerty, asdfgh)、連続した文字や数字、同じ文字の繰り返し

これらのパスワードは、プログラムを使えば短時間で解読されてしまうため、避けるべきであると言われている。文字数が多ければよいのではなく、推測されやすいパスワードがあることも理解して、第 2 時のパスワード作成の授業につなげたい。

表 2 日本の漏洩アカウントのパスワードトップ 10¹⁾

順位	日本人のパスワード	
	2024 年	前回(2021)
1 位	123456	123456
2 位	password	password
3 位	123123	000000
4 位	qwerty	1qaz2wsx
5 位	111111	12345678
6 位	000000	123456789
7 位	abc123	111111
8 位	1q2w3e4r	Sakura
9 位	xxxxxx	dropbox
10 位	1qaz2wsx	12345

③ 展開 B パスワードの組み合わせ数の理解

次に、パスワードの組み合わせの数の確認をする。簡単な例で「組み合わせの数」の仕組みと組み合わせの数(何通りできるか)を確認する。ここでは、パスワードで使う文字の種類と桁数を複数提示し、類推することを通して、パスワードの組み合わせ数が爆発的に増えることが理解できるような展開にした。

- ・ 4 桁の数字(10 種類)のみのパスワードの組み合わせ数

$$10^4 \text{通り} = 1,000 \text{通り}$$

- ・ 8 桁の小文字アルファベットのみ(26 種類)のパスワードの組み合わせ数

$$26^8 \text{通り} = 208,827,064,576 \text{通り}$$

- ・ 8 桁の小文字、大文字のアルファベット(52 種類)のパスワードの組み合わせ数

$$52^8 \text{通り} = 53,459,728,531,456 \text{通り}$$

- ・ 8 桁の数字、小文字、大文字を全て使ったパスワード(62 種類)の組み合わせ数

$$62^8 \text{通り} = 218,340,105,584,896 \text{通り}$$

もし、9 桁すると、

$$62^9 \text{通り} = 13,537,086,546,263,552 \text{通り}$$

このように、種類と桁数が 1 つでも増えただけで、組み合わせの数が「爆発的に」増える。なお、生徒自らが素早く実感できるように、筆者らは指数の計算が簡単にできるアプリ「累乗計算機」を作成し(図 1)、生徒が自由に使用できるように web に公開した²⁾。

図1 累乗計算機

(62^9 の場合)

④ 終末 パスワード解析にかかる時間の予想

パスワードの文字数ごとに解析にかかる時間の調査結果が、web で公開されている (巻末の資料 2) ³⁾。

生徒に、「パスワード解析にかかる時間はどれくらい?」と問いかけ、解析時間の予想をする活動を取り入れる。なお、この活動がスムーズにいくように、筆者らは秒数を年日時分秒に変換 (逆も可能) するアプリ「時間の変換」を作成し (図 2)、生徒が自由に使用できるように web に公開した ²⁾。この活動を通して、種類と桁数を増やすことで、パスワード解析に時間がかかり、安全性が高まるパスワードになるという理解が深まると考えた。

図2 時間の変換 (資料1のワークシートで利用)

(7×52^4 (=51181312) 秒を年日時分秒に変換の場合)

(2) 第2時 「安全性」と「使いやすさ」の両立

<数学科に関わる目標>

- ・組み合わせの数と解析時間の学びを活かし、「安全」と「使いやすい」を両立したパスワードを作成し、その根拠を説明することができる。

<リスクに関わる目標>

- ・情報セキュリティ (情報漏洩リスク) とパスワード

の利便性の両立を考察することができる。

第2時は、個人やチームでパスワードを実際に作りながら、「安全」で「使いやすい」パスワードを考察する授業である。

① 導入 パスワード作成の条件の確認

第2時の導入時に、以下のような問いを設定した。

卒業アルバム作成する。クラスの仲間と一緒に撮った写真フォルダにクラス全員で保存や編集をするためアクセスする。そのフォルダにパスワードをかける。「安全」で「使いやすい」パスワードは、どんなパスワードがいいだろうか。

作成したパスワードをクラス全員が使い、外部の人に分からないように個人情報を守るという条件設定を把握できるように、場面の想定を詳細に確認する。また、文字の種類や桁数、推測されやすいか、されにくい、パスワードの入力時間など様々な観点から、パスワードの分析ができるよう、複数のパスワードを積極的に作成するよう呼びかける。次の展開場面で生徒の議論が広がり、さらに、深まるようにする。

図3 パスワード入力時間測定

(表3の最初のパスワードの場合)

② 展開 個人・チームで、「安全」で「使いやすい」パスワードの作成し、考察する

- ・個人で実際にパスワードを複数作成する。
- ・4, 5人の学習班 (チーム) でそれぞれが作ったパスワードを持ち寄り「安全」で「使いやすい」か議論する。
- ・実際に作成したパスワードをキーボードを使って、入力し、入力時間を計測して、「使いやすさ」の

根拠とする。

なお、筆者らは、生徒のパスワードの入力時間が計測できるアプリ「パスワード入力時間測定」を作成し（図 3）、授業の中で生徒が随時入力時間を計測できるように web に公開した²⁾。

③ 終末 チームで検討したパスワードを発表し、意見交換とまとめをする

パスワードの強度は解析時間を目安として、数学的に分析できることや桁数、種類、推測されないようランダムな文字列が重要であることと、安全性と使いやすさは一方を犠牲にするトレードオフの関係にあるが、工夫次第で両立できることをまとめとして、情報漏洩リスクと向き合う態度を育てていきたい。

Ⅲ. 授業の実際

対象生徒は静岡県内公立中学校の3年生1クラス(28名)である。実施時期は、2025年10月の実践である(授業者は第1著者)。

(1) 第1時の授業の実際

① 導入 「リスク認識」の様子

授業の冒頭、有名人の SNS が乗っ取り被害にあったことを取り上げた。生徒の反応は、様々であったが、普段からスマートフォンが身近である生徒たちには、アカウント乗っ取りの意味とそこから生まれる被害や危険性、情報漏洩のリスクを、理解している様子であった。

② 展開 A 「推測されやすいパスワード」の様子

漏洩アカウントのランキング(表 2)を生徒に示したときには、「これではバレて当然」という反応があった。一方で「qwerty」「1q2w3e4r」というキーボード配列の左から右を連打するというパスワード作成について、知らなかった生徒がいたようで、気づいた生徒からの説明を聞き、「なるほど」という納得の声が聞こえた。

③ 展開 B 「パスワードの組み合わせ数の理解」の様子

生徒がタブレットで使っている4桁の数字(0~9の10種類)から組み合わせ数を確認した。0000~9999までの10000通りが 10^4 通りになる確認からはじめ、8桁のアルファベット小文字(a~zの26種類)になれば、 26^8 通りになる。それでは、8桁のアルファベット小文字と大文字(a~zの26種類×2倍=52種類)ではどうなると問いかけると、「 52^8 通り」という反応は一部の生徒からすぐに返ってきた。全体での確認から近隣の生徒間の確認を促したが、「基数が種類、指数が桁数」という類推から、多くの生徒が組み合わせ数の仕組みを理解できた。

累乗で表された表現では、実際の桁数をつかみづらいので、 52^8 通りこの累乗をどれくらいの桁数になりそうかという生徒の予想を近隣の生徒同士で対話させた。その後、「累乗計算機」のアプリを紹介し(図 1)、

各自で入力して計算してみると、兆を超え、京までになることを知り、その桁数の多さと増え方にとっても驚いている様子が見られた。

④ 終末「パスワード解析にかかる時間の予想」の様子

授業の後半では、「今、あなたのスマホにサイバー犯罪者(ハッカー)がパスワード解析中!どれくらいの時間がかかると思う?」と問いかけた。生徒は自分のパスワードの種類と桁数を基に、大体の予想を立てていたが、資料1の表を見た途端、「うわ、ヤバすぎじゃん」という声が聞こえた。生徒が使うタブレットのパスコードの多くは数字4桁のパスコードであり、それは1秒未満で解析されることを知った反応である。

資料1の下部の空欄時を埋める際、上部の秒数を参考にしながら、予想を立てていたが、大体の生徒は、解析時間を短く予想を立てていた。一方で、秒数が「文字の種類」倍(26倍や52倍など)で増えていくことに気付いた生徒も数名いた。秒の表記があることで、解析時間の推測がしやすくなったと思われる。秒数を年日時分秒に変換する「時間の変換」のアプリを活用し(図 2)、予想を立てることができていた。その生徒の気づきを全体で取り上げ、解析時間の仕組みの共通理解を図った。授業の最後には、資料2の解析時間一覧を配布すると、144兆年という解析時間に笑いが起きるぐらいの驚きを示していた。次時(第2時)の「安全」なパスワード作成のための基礎となる情報漏洩リスクの知識を学級全体で確認できた授業となった。

(2) 第2時の授業の実際

① 導入「パスワード作成の条件の確認」の様子

第2時は、第1時の翌日に実施した。前時の組み合わせ数や桁数など、簡単な振り返りから、「本時は、前時の学びを活かし、パスワードを作成すること。」を伝えた。次に、「卒業アルバム作成のフォルダにパスワードをかける。『安全』で『使いやすい』パスワードは、どんなパスワードがいいだろうか。」とパスワード作成の条件を確認した。「自分だけが使うものではなくみんなで使うものであるため、覚えやすいことも条件になる。しかし、推測されやすいパスワードでは、情報漏洩のリスクもある。」などの確認をした。

また、入力しやすさの視点として、「パスワード入力時間測定」のアプリを紹介した(図 3)。生徒は「安全」で「使いやすい」というパスワードの条件に納得できた様子で、個別にパスワード作成に取り組むことができた。

② 展開 「個人で、『安全』で『使いやすい』パスワードの作成し、考察する」の様子

個人でのパスワード作成には、戸惑いを見せる生徒が多かった。10分程度の作成の時間を設けたが、1つか2つ程度の作成にとどまる生徒が多く見られた。個人で取り組んだワークシートの記述を読み取ると、以下の図4のようなパスワードが見られた。

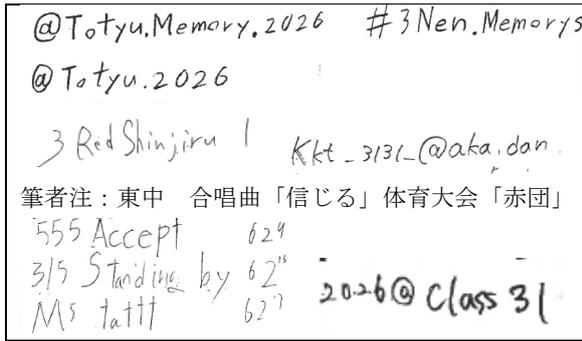


図4 個人で作成したパスワード(例)

③ 展開 「チームで、『安全』で『使いやすい』パスワードの作成し、考察する」の様子

個別に作成されたパスワードを4人から5人のチームで発表し合い、安全性と使いやすさの検討を重ねていた(写真1)。使いやすさの視点として、入力時間を示したが、個人のタイピング能力の差により、入力時間が異なることから、1つのパスワードを「パスワード入力時間測定」のアプリを使ってチームのメンバーの複数で入力し、入力時間の平均を比べていた。覚えやすさや入力時間の短いものを評価する生徒が現れ、長いパスワードは入力時間がかかることから、チーム内検討で、否定される様子が見られた。15分ほど、チームで検討した結果、全体共有の場面で取り上げられたパスワードの主なものは、表3の通りである。



写真1 チームでの検討の様子

表3 全体発表されたパスワードと入力時間調査

パスワード	入力時間調査 (複数回実施あり)
Aoharu@jin31	54秒 20秒 103秒
@Kikuto3omoide1	10.619秒
Omoide@31	2秒
@Kikugawaschoooooooooo131	(未記入)
W0a9_v0E1	43秒 32秒 23秒
Otonanokaidan31.com	10秒



写真2 全体での意見交換の様子

全体での意見交換の場面では、パスワード作成の理由や話し合いの様子を発表した(写真2)。授業者は、「@Kikugawaschoooooooooo131」を取り上げ、作成し、検討をしたチームから説明してもらった。「文字数を多くすると覚えにくくなるが、oの数を10個として、覚えておくと、入力しやすくなる。」という説明を受け、感嘆する生徒の反応が見られた。

④ 終末 生徒の感想

生徒は、第2時終了時に感想を聞いた。これらを整理すると、以下のように、「リスクの実感」「安全性と使いやすさの両立」「リスクを減らす行動」に分類することができる。

(ア) リスクを実感している記述

- ・ 機械の発展が進んでいる今、パスワードの授業はとても面白かった。1桁増えるだけで、数百年、数千年とかかる時間が変わっていくことにすごく驚かされた。自分と友達とで予想した数字が全く違うのが面白かった。
- ・ 私は、数字のみの4桁だから、一瞬でバレてしまうことがすごく驚きました。一番印象に残ったことは、何年か予想するときです。分からなすぎて、勘で書いたら、実際の年が違いすぎて、それも、何億年とか何兆年など、使わない数でびっくりしました。
- ・ パスワードの組み合わせによって、144兆年かかることにびっくりしました。また、組み合わせを複雑にするほど、安全だけど、パスワードを覚え方や、管理(メモに残しておくなど)の仕方も工夫しないといけないと思いました。
- ・ (入力に)どのくらいかかるのかの計算なども、仲間と話して教えてもらったり、実際に作ったパスワードを打つのに、何秒かかるのかを検証したりして、みんなで話している時が楽しくて、印象に残った。

(イ) 安全性と使いやすさの両立を考えている記述

- ・ 数字+英語+記号でも、桁も大きくして、安全性

がばっちりでも、打ちづらいパスワードだと実用性が低いから、自分や仲間だけに、わかりやすい合言葉をパスワードに変えるなど、安全性と使いやすさの両立が大事だと思った。パスワードを設定するときには、「安全性」と「使いやすさ」の割合を時と場合（使う頻度）によって、変えるといいと思った。

- ・ Aさんが考えた School の o を 10 個にするのが印象に残り、普通に見たら、ふざけている様だけど、ハッカーから見たら、かなりの嫌がらせになる。
- ・ 文字数が多ければ多いほど、いいことがわかった。自分にとってわかる安全なパスワードを作るとは難しいと思った。この授業をして、自分のパスワードは安全で使いやすいのか見直すきっかけになった。

(ウ) リスクを減らす行動を考えている記述

- ・ これからは、数字と大文字、小文字を使うのは当たり前前として、文字数をできるだけ増やしたいと思いました。バレやすいパスワードは使わないようにします。
- ・ 今、自分が使っているパスワードは、小文字+数字であまり安全ではないから、これからは最低でも、大文字小文字の 8 桁以上で、解読するのに、1 年以上はかかる安全なパスワードを使っていきたい。

IV. 教材の要件・留意点の考察

(1) リスクを数学科で扱う際の教材の要件

今後、様々なリスクと向き合うには、「正しく恐れる」ことが必要であると考えます。数学科の授業でリスクを扱う教材の要件として、以下の 2 点を挙げる。

① 生徒が身近なリスクとして実感でき、それに関わる数学的根拠があること

この授業実践では、生徒にとって、身近な情報端末に係わるパスワードの実践である。また、客観的に判断できるように、パスワードの解析時間を計算し、分析する場面を設定した。さらに、パスワードの入力時間を可視化できるようにした。授業後の感想の記述にも驚きを示してリスクを実感する記述があった。笹瀬(2025)における暑さリスクに係わる気温や暑さ指数 WBGT を題材とした実践でも、信頼できる気象庁の気象データがあったように、情報漏洩のリスクは、生徒自身に身近なリスクである理解の上で、そのリスクが数学的に分析できる根拠があることが数学科の授業でリスクを扱う教材の要点になると考える。

② トレードオフの関係があるリスク分析をすること

本研究では、「安全」で「使いやすい」パスワードを作り、情報セキュリティ（情報漏洩リスク）とパス

ワードの利便性の両立（トレードオフ）を考察する授業実践をした。

実際の授業での生徒の様子やワークシートの記述、授業後の感想より、この両立に悩み、議論する姿が読み取ることができた。この授業実践では、明確な解はなく、オープンエンドな議論となった。このように、むやみに「絶対的な安全性」を追求するのではなく、「どのような脅威から守るべきか」を明確にし、そのレベルに見合った利便性も考慮するという「安全」で「使いやすい」トレードオフの関係を取り入れた授業展開にすることが、リスクを数学科の授業で扱う上での要件になると考える。

トレードオフの関係は、価格（安さ）と品質（耐久性・機能）の関係のように、低価格な製品を選ぶと初期費用は抑えられるが、すぐに壊れ、機能が不十分で満足度が低くなるような例が挙げられる。このような関係がオープンエンドの議論を生み出し、リスクと向き合いつつ、数学的な考え方を使い、冷静に根拠を示して、リスクを分析したくなる授業を構想したい。

(2) リスクを数学科の授業で扱う上での留意点

今後の日常生活の中で、感情や偏見に流されずにリスクを客観的に評価し、適切な対応をとらなくてはならない。リスクを数学科の授業で扱う上での留意点として、以下の 2 点を挙げる。

① 身近で緊急性のある「避けられないリスク」を数学的に分析し、リスクを減らす行動をとれる気づきが得られる授業を構想すること

先行実践の「暑さリスク」（笹瀬、2025）と本実践「情報漏洩リスク」は、我々の生活の中で身近で、緊急性のある避けられないリスクである。このほかにも、「感染症リスク」や「交通事故リスク」なども挙げられる。これらの避けられないリスクを数学科の授業であえて扱うことが大切である。そして、緊急性があるが、自分のできる範囲でコントロールできるリスクであるという認識と、数学的に冷静にリスク分析し、発生確率を下げられる行動をとれる気づきが得られる授業を構想することが留意点として挙げられる。一方で、すぐに結果が出ないため、緊急性が低いと判断され、対応が後回しになりやすい「生活習慣病リスク」や「経済問題リスク」は、生徒のリスクとしての実感が伴わず、数学科の授業で扱うリスクとしては扱いにくい事例になる。

② 主観的リスクから客観的リスクに変換すること

個人の感情や経験に基づく主観的なリスク認知は社会の混乱を生み出す。数学科の授業において、リスクを扱う時には、データや統計に基づく冷静な分析をして、対話をする態度を育成することで、客観的なリスク評価へと移行できる。数学科の授業を通して、仲間と一緒に「避けられないリスク」に向き合い、これからの生活に活かすため、生徒目線の主観的で具体的な

事例を基に、数学科の授業で取り上げることで、主観的リスクから客観的リスクとしてとらえる力につながるだろう。例えば、SNS 利用時の書き込みに対して、デジタルタトゥーリスクや炎上リスクを取り上げ、「誰も見てないだろう」「私の意見は正しいから大丈夫」という過信や楽観の主観的リスクを「情報の拡散速度（富田，2024）」や「コメント炎上の発生確率」のデータ分析を通して、客観的リスクへの変換などが考えられる。

V. 今後の課題

本実践は、中学校 3 年生において高校で学ぶ数学II「指数関数」と数学 A「場合の数と確率」につながる授業になった。この題材で、高校での授業実践を構想し、中高の生徒の様相を比較・分析することで、発達段階に合わせたカリキュラムの構想ができる。さらに、本研究グループでの小中高の実践を振り返り、その実践の共通項を分析し、カリキュラム構想の要点と留意点をまとめていきたい。

注

- 1) 株式会社ソリトンシステムズ（本論文の表 2 の掲載を承認済）
<https://www.soliton.co.jp/products/csa/WP-CSA-2410B.pdf>
- 2) 作成したアプリ「累乗計算機」「時間の変換」「パスワード入力時間測定」は、以下の URL にある。なお、Gemini や ChatGPT を参考に作成した。
<https://wvp.shizuoka.ac.jp/matsugen/%e3%83%aa%e3%83%b3%e3%82%af/>
- 3) NTT インテグレーション株式会社（旧日本情報通信株式会社）「今後のパスワードは複雑さにプラスして長さも必要」（2024 年 11 月 13 日更新：本論文巻末の資料 2 の掲載を承認済）
https://www.niandc.co.jp/tech/20241113_55911/
なお、この表は、Hive Systems 社の 2024 年の Are Your Passwords in the Green? の情報（www.hivesystems.com/password）を基に、NTT インテグレーション株式会社（旧日本情報通信株式会社）が編集・作成したものである。

付記

本研究は JSPS 科研費 22K02518（代表者：裕元新一郎）「リスク社会に対応した数学教育のあり方に関する研究」の助成を受けて行ったものである。

引用・参考文献

藤原大樹（2024）．中学校数学科におけるリスク対応を意図した授業の教材開発の視点，日本科学教育学会年会論文集，48，221-224.
https://doi.org/10.14935/jssep.48.0_221

菊野慎太郎（2024）．リスク社会に対応した数学教育における教材開発と授業実践—中学第 3 学年「そのメール開きますか」の分析—，日本科学教育学会年会論文集，48，221-224.

https://doi.org/10.14935/jssep.48.0_217

菊野慎太郎（2025）．数学教育におけるリスク対応を意図した教材開発と授業実践の視点—中学校第 1 学年「あなたの買い物で温暖化を止める！？」の分析—，日本科学教育学会年会論文集，49，223-225.

https://doi.org/10.14935/jssep.49.0_223

牧之段拓（2023）．リスク社会に対応した数学教育における教材開発と授業実践—小学校第 6 学年「生活習慣病にならないために」—，日本科学教育学会年会論文集，47，29-32.

https://doi.org/10.14935/jssep.47.0_29

裕元新一郎（2021）．リスク社会における数学教育の貢献のあり方，日本科学教育学会年会論文集，45，365-368. https://doi.org/10.14935/jssep.45.0_365

裕元新一郎・峰野宏祐・熊倉啓之（2023）．数学教育においてリスクを扱う際の枠組みの提案，日本科学教育学会年会論文集，47，17-20.

https://doi.org/10.14935/jssep.47.0_17

笹瀬 大輔（2025）．数学教育におけるリスク対応を意図した教材開発と授業実践の視点—中学校第 2 学年「夏の外での活動はいつまで実施できそうか」の分析—，日本科学教育学会年会論文集，49，227-230.

https://doi.org/10.14935/jssep.49.0_227

富田真永（2024）．数学教育におけるリスク社会に対応した教材を用いた授業実践—高等学校第 1 学年「情報拡散の脅威」の授業を通して—，日本科学教育学会年会論文集，48，225-228.

https://doi.org/10.14935/jssep.48.0_225

（すべての URL は、2025 年 11 月 30 日参照）

(資料1:ワークシート) 解析にかかる時間を予想しよう.空欄を予想して,埋めてみましょう.

	数字のみ 10種類	小文字のみ 26種類	大文字と小文字 26×2=52種類	数字大文字小文字 10+52=62種類	数字大文字小文字+記号8種類 62+8=70種類
組み合わせ数	10^n	26^n	52^n	62^n	70^n
文字数 4	1秒未満	1秒未満	7秒	14秒	23秒
文字数 5	1秒未満	11秒	6分4秒 (364秒)	14分28秒 (868秒)	26分50秒 (1610秒)
文字数 6	1秒	4分46秒 (286秒)	5時間15分28秒 (18928秒)	14時間56分56秒 (53816秒)	1日7時間23分20秒 (112700秒)
文字数 7	10秒	2時間3分56秒 (7436秒)	11日10時間37分 (984256秒) 約2週間	38日14時間49分52秒 (3336592秒) 約1か月	91日7時間23分20秒 (7889000秒) 約3か月
文字数 8	1分40秒 (100秒)	2日5時間42分16秒 (193336秒) 約2日	約 年	約 年	約 年
文字数 9	16分40秒 (1000秒)	約 月	約 年	約 年	約 年
文字数 10	約 時間	約 年	約 年	約 年	約 年

資料2

解析にかかる時間

文字数	数字のみ	小文字	大文字と小文字	数字、大文字、小文字	数字、大文字、小文字、記号
4	即時	即時	7秒	14秒	23秒
5	即時	11秒	6分	15分	27分
6	1秒	5分	5時間	15時間	1日
7	10秒	2時間	2週間	1ヶ月	3ヶ月
8	2分	2日	2年	7年	17年
9	16分	2ヶ月	84年	411年	1,000年
10	3時間	4年	4,000年	25,000年	85,000年
11	1日	111年	22.8万年	100万年	500万年
12	2週間	2,000年	1,100万年	9,700万年	4.19億年
13	4ヶ月	7,500年	6.16億年	60億年	290億年
14	3年	100万年	320億年	3,760億年	2兆年
15	30年	5,000万年	1兆年	23兆年	144兆年

Hive Systems 社にてパスワードの文字数ごとに解析にかかる時間の調査結果が報告されています。
この表は、A100 を 8 台、bcrypt でハッシュ化されたパスワードで計測した結果となります。