広島市立大学の模擬問題A　第2問・第4問解説　「データの活用と情報通信ネットワーク」分野

情報処理学会・学会誌「情報処理」
2024年10月28日 08:53

稲垣俊介（山梨大学 教育学部）

広島市立大学は2023年3月24日に，「情報（情報I）模擬問題の公開と解説」説明会を開催[1]し，模擬問題を公開[2]しました．

2024年度（令和6年度）に実施される情報科学部一般選抜後期日程個別学力検査では，「情報（情報I）」が出題されます．広島市立大学のウェブサイトには，「『情報』が好き！」な高校生に，その学びの成果を入試で存分に発揮してほしいと記載されています[1]．ぜひ，「情報」を受験予定の生徒や指導をされる先生方に，この記事を読んでいただければと思います．

今回は，模擬問題Aの第2問と第4問の解説をいたします．第2問は「データの活用」分野，第4問は「情報通信ネットワーク」の分野に該当します．

目次

問2：シーザー暗号

問3: 共通鍵暗号システムにおける鍵の必要な数の計算

問4：電子認証のしくみ

すべて表示

模擬問題A 第2問

模擬問題Aの第2問は，「情報I」の「データの活用」分野をどれだけ理解しているかを見る問題です．天気や気温，来客数，売上高などのデータを使って，これらのデータがどんな性質を持っているかを理解し，どのように分析するかを学びます．特に，数値データと分類データの違い，足りないデータの扱い方，データをどう分析するかに焦点を当てています．

表1は，ある店舗の3月3日から3月12日までの10日間の気象情報（天気と最高気温），来客数および売上高のデータである。このとき，以下の問いに答えよ。

表1　ある店舗の売上データ

No.	日付	天気	最高気温（℃）	来客数（人）	売上高（千円）
1	3月3日	晴れ	10	5	900
2	3月4日	雨	8	4	300
3	3月5日	晴れ	15	9	2,000
4	3月6日	雨	6	8	600
5	3月7日	曇り	9	10	950
6	3月8日	晴れ	12	9	1,800
7	3月9日	晴れ	10	12	2,500
8	3月10日	曇り	8	8	800
9	3月11日	晴れ	12	10	1,800
10	3月12日	雨	5	15	–

問1：データの分類

問1　(ア) 量的データ，(イ) 質的データおよび (ウ) 欠損データについてそれぞれ説明せよ。さらに，表1の表頭にある項目「天気」，「最高気温（℃）」，「来客数（人）」，「売上高（千円）」を (ア) 量的データ と (イ) 質的データに分類せよ。

- **量的データ**
  「最高気温」や「来客数」「売上高」のような，数で表されるデータです．これらは足し算や引き算ができるので，比較や計算に使います．

- **質的データ**
  「天気」のように，データをグループに分けるときに使う言葉です．晴れ，雨，曇りなどのグループに分けて，どのグループにどれくらいデータがあるかを見るときに使います．

- **欠損データ**
  何らかの理由でデータが記録されていない場合です．たとえば，ある日の売上が記録されていないと，そのデータは足りないことになります．このようなデータは無視するか，推測して埋める必要があります．

ポイント
　この問題で大切なのは，データが何を表しているかをしっかりと理解し，どのように使うかを学ぶことです．量的データは計算に使え，質的データは情報を整理するのに役立ちます．また，データが足りないときの対応方法を知ることも大切です．これらの知識は，データを使った調査や問題解決に直接役立ちます．

問2：天気ごとの売上データの計算

問2　表2は，天気ごとに表1のNo. 1からNo. 9までの売上高の合計，平均，標準偏差の値をまとめたものである。このとき，（エ）～（カ）の空欄に入る数値を答えよ。なお，表1のNo. 10の売上高が欠損値のため，表2ではNo. 10は除外されていることに注意すること。

表2　ある店舗の売上データ

天気	合計	平均値	標準偏差
晴れ	9,000	（オ）	517.7
曇り	（エ）	875.0	75.0
雨	900	（カ）	150.0

　この問題では，異なる天気の日における売上を計算します．以下のように売上を合計したり，平均を出したりする計算を行います．

- **曇りの売上合計**
  - 3月7日の売上が950千円，3月10日の売上が800千円です．
  - 合計：950千円 + 800千円 = 1750千円

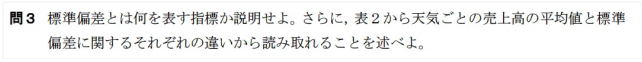
- **晴れの日の平均売上**
  - 5日間（3月3日，5日，6日，9日，11日）の売上合計が9000千円です．
  - 平均：9000千円 ÷ 5日 = 1800.0千円

- **雨の日の平均売上**
  - 2日間（3月4日と6日）の売上合計が900千円です.
  - 平均：900千円 ÷ 2日 = 450.0千円

ポイント
合計の計算
　同じ天気の日の売上を全部足します．これで，その天気の日の全部の売上を知ることができます.
平均の計算
　合計した売上をその天気の日数で割ります．これにより，一日あたりの平均売上がどれくらいかが分かります.

　この計算を通じて，晴れ，曇り，雨の日では売上がどれくらい違うかを比較できます．また，どの天気の日に売上が多かったか，少なかったかを知ることができます．このような分析は，データをもとにした判断や計画を立てるときに役立つ基本的な方法です.

問3：標準偏差と天気ごとの売り上げのばらつき


問3　標準偏差とは何を表す指標か説明せよ。さらに，表2から天気ごとの売上高の平均値と標準偏差に関するそれぞれの違いから読み取れることを述べよ。

　標準偏差とは，データが平均値からどれだけ散らばっているかを示す数値です．この問題では，曇り，晴れ，雨のそれぞれの天気での売上データのばらつきを標準偏差を使って調べ，どんな意味があるかを考えます.

ポイント

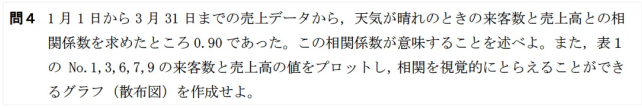
- **標準偏差の計算法**
  - 最初に，曇り，晴れ，雨の各天気ごとに売上の平均値を出します.
  - 次に，各売上がその平均値からどれだけ離れているか（偏差）を計算します.
  - これらの偏差を二乗し，その平均値（これが分散です）を求めます.
  - 最後に，分散の平方根を取ることで，標準偏差を求めます.

- **データの解釈**
  - 標準偏差が小さいと，その売上データは平均値に近い値で集中しており，売上が安定していると考えられます.

- 逆に標準偏差が大きいと，売上データが平均値から大きく離れており．売上が不安定であると言えます．

この計算を通じて．天気ごとに売上がどれだけ安定しているか，または不安定かを把握できます．たとえば，晴れの日には売上が平均的に高いですが，そのばらつきが大きい場合，晴れの日に非常に高い売上を記録することもあれば，意外と低い日もあるということが分かります．このような情報を深く理解することで，売上の予測や計画に役立てることができます．

問4：相関係数とその解釈


問4 1月1日から3月31日までの売上データから，天気が晴れのときの来客数と売上高との相関係数を求めたところ0.90であった。この相関係数が意味することを述べよ。また，表1の No. 1, 3, 6, 7, 9 の来客数と売上高の値をプロットし，相関を視覚的にとらえることができるグラフ（散布図）を作成せよ。

相関係数は，2つの事項（たとえば来客数と売上高）がどれだけ密接に関連しているかを数値で示します．この問題では，来客数と売上高の間の相関係数が0.90と計算されており，これは非常に強い正の関連があることを意味しています．

ポイント

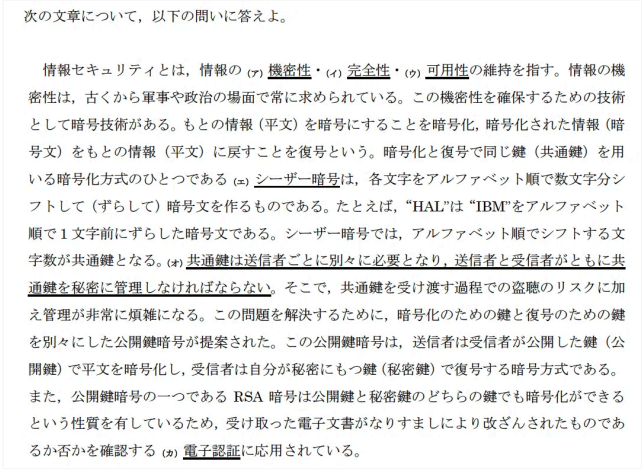
- **相関係数の範囲**
  - 相関係数は-1から+1までの値を取ります．プラスは正の相関（一方が増えるともう一方も増える），マイナスは負の相関（一方が増えるともう一方は減る）を意味しており，+1に近づくほど，-1に近づくほど強い相関であることを示しています．0は相関がないことを示します．

- **データの解釈**
  - 相関係数が0.90という高い値は，来客数が増えると売上も同じように増える傾向が強いということを示しています．これは，多くの人が来店するほど，売上が良くなることが多いと解釈できます．

この問題を通じて，相関係数を用いることで，2つの異なる事項がどのように連動しているかを数値で理解できます．来客数と売上の間に強い関連があることを知ることで，店のマーケティング戦略や顧客サービスを改善する際に，どのように計画を立てるかの手がかりになります．たとえば，特定の日に多くの顧客が来店することが予想される場合，それに合わせて特別な販売戦略を用意することが有効ですね．

模擬問題A 第4問

模擬問題Aの第4問は，「情報I」の「情報通信ネットワーク」分野の理解を深めるための問題です．ここでは，情報を守るために必要な基本的な安全対策や，暗号技術の使い方について学びます．この問題では，情報セキュリティの3要素（機密性，完全性，可用性）について理解し，シーザー暗号の使い方，共通鍵暗号システムでの鍵の管理方法，電子認証の手順を学びます．



次の文章について，以下の問いに答えよ。

情報セキュリティとは，情報の (ア) 機密性・(イ) 完全性・(ウ) 可用性の維持を指す。情報の機密性は，古くから軍事や政治の場面で常に求められている。この機密性を確保するための技術として暗号技術がある。もとの情報（平文）を暗号にすることを暗号化，暗号化された情報（暗号文）をもとの情報（平文）に戻すことを復号という。暗号化と復号で同じ鍵（共通鍵）を用いる暗号化方式のひとつである (エ) シーザー暗号は，各文字をアルファベット順で数文字分シフトして（ずらして）暗号文を作るものである。たとえば，“HAL”は “IBM”をアルファベット順で 1 文字前にずらした暗号文である。シーザー暗号では，アルファベット順でシフトする文字数が共通鍵となる。(オ) 共通鍵は送信者ごとに別々に必要となり，送信者と受信者がともに共通鍵を秘密に管理しなければならない。そこで，共通鍵を受け渡す過程での盗聴のリスクに加え管理が非常に煩雑になる。この問題を解決するために，暗号化のための鍵と復号のための鍵を別々にした公開鍵暗号が提案された。この公開鍵暗号は，送信者は受信者が公開した鍵（公開鍵）で平文を暗号化し，受信者は自分が秘密にもつ鍵（秘密鍵）で復号する暗号方式である。また，公開鍵暗号の一つである RSA 暗号は公開鍵と秘密鍵のどちらの鍵でも暗号化ができるという性質を有しているため，受け取った電子文書がなりすましにより改ざんされたものであるか否かを確認する (カ) 電子認証に応用されている。

問1：情報セキュリティの三大要素

問 1 上の文章中にある (ア) 機密性，(イ) 完全性および (ウ) 可用性をそれぞれ説明せよ。

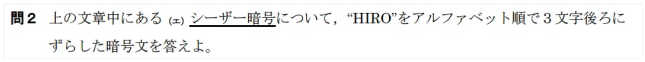
情報セキュリティは，情報を安全に保つために必要な「機密性」，「完全性」，「可用性」という3つの基本要素から成り立っています．

- **機密性（Confidentiality）：**機密性は，許可された人だけが情報にアクセスできるようにすることです．たとえば，パスワードが必要なサイトには，パスワードを知っている人だけがログインできます．
- **完全性（Integrity）：**完全性は，情報が正確であり，勝手に変更されないように保護することです．文書やデータが変更された場合，誰がいつどのように変更したかが記録されることが一例です．
- **可用性（Availability）：**可用性は，必要なときに情報が利用できる状態を保つことです．たとえば，重要なデータを保存しているサーバーが壊れた場合，すぐに修理や対応が行われるようにすることが含まれます．

ポイント

情報セキュリティのこれらの要素は，個人情報や学校の成績表など，私たちが普段から接している重要な情報を守る上できわめて重要です．機密性，完全性，可用性がしっかりと保たれているかを常に確認し，日常生活での情報保護に活かすことが大切です．これにより，不正アクセスやデータ漏洩のリスクを減らし，安全に情報を扱うことができます．

問2：シーザー暗号


問2　上の文章中にある (エ) シーザー暗号について，“HIRO”をアルファベット順で3文字後ろにずらした暗号文を答えよ。

シーザー暗号の基本

シーザー暗号は，アルファベットを決められた数だけシフトして文字を置き換える暗号化方法です．この方法は非常に古く，元の文字列を少し変えるだけで，ほかの人が内容を読むことを難しくします．

問題の説明

この問題では，「HIRO」という文字列を3文字ずつアルファベット順にずらして暗号化します．具体的な手順は以下のとおりです．

- 'H' はアルファベット順で3つ後ろの 'K' になります．
- 'I' は 'L' に，
- 'R' は 'U' に，
- 'O' は 'R' に変換されます．

したがって，「HIRO」は「KLUR」に暗号化されます．

ポイント

シーザー暗号は，その単純さから，暗号学の基礎を学ぶ際によく使われます．元の情報を簡単に隠すこの方法は，基礎的な教育や趣味で楽しむ範囲で特に役立ちますが，現代ではもっと高度な暗号が一般的に使用されています．

問3: 共通鍵暗号システムにおける鍵の必要な数の計算

問3 上の文章中にある（オ）について，同じ人同士で送受信する際は同一の共通鍵を使うことにした場合，機密性を確保しつつ４人の間で相互に送受信するには６個の共通鍵が必要である。一般に，n $(n \geq 2)$人の間では何個の共通鍵が必要か答えよ。なお，その答えの導出過程も述べること。

共通鍵暗号システムとは，通信する双方が同じ鍵を使って暗号化と復号を行うシステムです．このシステムの課題は，鍵を安全に共有することです．人数が増えると，通信者間で秘密を守るために必要な鍵の数が増え，管理が難しくなります．

鍵の数の計算

n 人が相互に通信を行うためには，各ペア間で共通鍵が必要です．ペアを作る組合せの数を計算するために，組合せの公式を使います．n 人の中から2人を選んで通信するペアの数は，組合せの数で表され，公式は以下のとおりです．

$$\frac{n(n-1)}{2}$$

これは，n 人の中で2人を選んで通信を行うために必要な共通鍵の数です．

導出過程

1. n人がいる場合，まず1人目が他のn-1人全員と通信するためにはn-1個の共通鍵が必要です．
2. 2人目はすでに1人目との通信に共通鍵を使用しているため，残りのn-2人との通信のためにn-2個の共通鍵が必要です．
3. このように続けていくと，合計で

$$(n-1)+(n-2)+\ldots+1=\frac{n(n-1)}{2}$$

という数式が得られます．

例(n=4)を使った説明

n = 4 の場合，4人がそれぞれペアを組むために必要な共通鍵の数を考えます．

1. 1人目は，残りの3人（4-1=3）とペアを組むので，まず3個の共通鍵が必要です．
2. 2人目は，残りの2人（4-2=2）とペアを組むので，さらに2個の共通鍵が必要です．

3. 3人目は，残りの1人（4-3=1）とペアを組むので，最後に1個の共通鍵が必要です.

これらをすべて足すと，

$$3 + 2 + 1 = 6$$

これが，4人の場合に必要な共通鍵の数です.

一般化

n人の場合として一般化すると，n人が相互に通信するために必要な共通鍵の数は次のように計算できます.

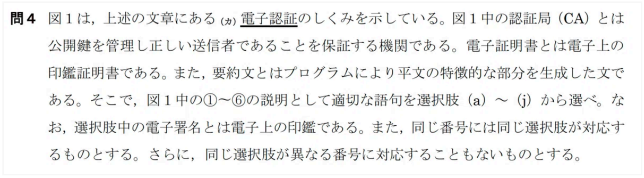
$$\frac{n(n-1)}{2}$$

このように，任意の人数に対して必要な共通鍵の数を簡単に求めることができます.

ポイント

この計算は，情報セキュリティがどのように機能するかを理解するのに役立ちます．多くの人がかかわる通信システムでは，鍵の数が多くなりがちですが，鍵の管理を効率的に行うことが非常に重要です.

問4：電子認証のしくみ



問4 図1は，上述の文章にある(ア)電子認証のしくみを示している。図1中の認証局（CA）とは公開鍵を管理し正しい送信者であることを保証する機関である。電子証明書とは電子上の印鑑証明書である。また，要約文とはプログラムにより平文の特徴的な部分を生成した文である。そこで，図1中の①～⑥の説明として適切な語句を選択肢（a）～（j）から選べ。なお，選択肢中の電子署名とは電子上の印鑑である。また，同じ番号には同じ選択肢が対応するものとする。さらに，同じ選択肢が異なる番号に対応することもないものとする。

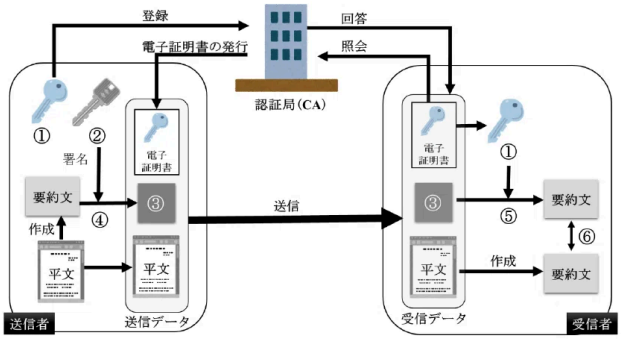


図1 電子認証のしくみ

選択肢

(a)	暗号化	(b)	復号	(c)	送信者の公開鍵	(d)	受信者の公開鍵
(e)	電子署名	(f)	電子文書	(g)	送信者の秘密鍵	(h)	受信者の秘密鍵
(i)	比較	(j)	複写				

この問題では，RSA暗号を用いた電子認証の仕組みを確認します．RSA暗号は公開鍵暗号方式の一つで，公開鍵と秘密鍵の2つの鍵を使ってメッセージの暗号化や**RSAを用いた電子署名**の検証を行います．ここでは，暗号化やRSAを用いた電子署名の手順において，どの鍵が使用されるかを正確に判断することが求められています．

RSA暗号には，次の2つの主要な機能があります．

1. メッセージの暗号化と復号

送信者は，受信者の公開鍵を使ってメッセージを暗号化します．この暗号化されたものを暗号文と言います．受信者は，送られてきた暗号文を自分の秘密鍵を使って復号し，メッセージの内容を確認します．

ただし，暗号文は通信回線を用いて送信されるため，悪意のある人はこの暗号文を盗聴できます．また，復号に使う鍵は，公開鍵から計算できます．しかし，その計算には数百年以上かかるように公開鍵が設定されています．したがって，悪意のある人が，暗号文を現実的な時間で解読することは難しく，送信者は受信者にメッセージを安全に伝えることができます．

2. 電子署名と署名の検証

送信者は，自分の秘密鍵を使ってメッセージにRSAを用いた電子署名を行います．これにより，メッセージが送信者によって作成されたものであり，改ざんされていないことを証明します．受信者は，送信者の公開鍵を使ってこの署名を検証し，メッセージが正当なものであるかどうかを確認します．ここでの署名は，RSA暗号を利用した特定の電子署名方式であることに注意してください．

RSA暗号のしくみ

RSA暗号の流れは次のように進みます.

1. メッセージの暗号化

- **暗号化**：送信者は，受信者の公開鍵を使ってメッセージを暗号化します．たとえば，送信者が「秘密のメッセージ」を送信したい場合，受信者の公開鍵でこのメッセージを暗号化します.
- **送信**：暗号化されたメッセージを受信者に送ります.
- **復号**：受信者は，自分の秘密鍵を使って受け取った暗号文を復号し，元のメッセージを取得します.

2. 電子署名の生成

- **署名**：送信者は，自分の秘密鍵を使ってメッセージにRSAを用いた電子署名を行います．たとえば，送信者が「重要な文書」を送る際に，自分の秘密鍵で署名を生成します.
- **送信**：署名付きのメッセージを受信者に送ります.
- **検証**：受信者は，送信者の公開鍵を使って署名を検証し，メッセージが送信者からのものであり，改ざんされていないことを確認します.

問題の説明

①：c［送信者の公開鍵］

受信者は，送信者の公開鍵を使ってRSAを用いた電子署名を検証します．送信者がメッセージにRSAを用いた電子署名を行った後，受信者はこの公開鍵を使って署名を検証し，メッセージが正当であるか確認します.

②：g［送信者の秘密鍵］

送信者は，自分の秘密鍵を使ってメッセージにRSAを用いた電子署名を行います．この秘密鍵を使うことで，メッセージが送信者から送られたものであることを証明します.

③：e［電子署名］

送信者が自分の秘密鍵を使って生成したRSAを用いた電子署名です．これが受信者に送られ，受信者が送信者の公開鍵を使って署名を検証します.

④：a［暗号化］

⑤：b［復号］

送信者の持つ秘密鍵を第三者が送信者の公開鍵から，現実的な時間では計算することはできません．したがって，送信者の秘密鍵は送信者以外が使うことができず，その暗号文（要約文）は送信者自身から送られたものであることが受信者は確認できます．
送信者の秘密鍵で暗号化されたものは，その送信者の公開鍵でしか復号できないという性質があります．ですから，送信者の公開鍵で復号できたなら，それは送信者の秘密鍵で暗号化されたものだということになります．送信者の秘密鍵は送信者自身しか持っていないものです．つまり，送信者の持つ秘密鍵を第三者が送信者の公開鍵から，現実的な時間では計算することはできません．つまり，その暗号文（要約文）は送信者自身から送られたものであることが受信者は確認できます．

⑥：i［比較］
最後に，受信者はメッセージの内容を確認し，元の署名されたメッセージと一致するかどうかを比較します．この比較によって，メッセージが正しく送信されたことが確認されます．

ポイント
RSA暗号では，通常，公開鍵で暗号化し，秘密鍵で復号します．また，RSAを用いた電子署名の際には秘密鍵で署名し，公開鍵で署名を検証します．

RSA暗号は，大きな整数の素因数分解が計算量的に困難であるという性質に基づいています．公開鍵と秘密鍵はこの性質を利用して作られており，秘密鍵を知らない第三者がメッセージを復号したり，偽の署名を作成したりすることは現実的な時間内では困難です．この性質を**「計算量的安全性」**といいます．

RSA暗号は歴史的に重要なもので教科書でも解説されていますが，いつか効率的な素因数分解アルゴリズムが発見されたり，量子コンピュータが実用化されれば，RSA暗号はその安全性を失う（「危殆化」といいます）可能性があります．そのことを予想して，暗号方式の見直しが進んでいます．

TLS1.3という2024年現在のWebで採用されている方式では，RSAは電子署名に選択できる手段の一つとされ，RSAを使用することは必須ではありません．また，メッセージ本体の暗号化・復号には，RSA に限らず公開鍵暗号は採用されていません．

まとめ

広島市立大学が公開した模擬問題Aの第2問と第4問は，高校の「情報I」における「データの活用」と「情報通信ネットワーク」の理解を深めることができる問題です．これらの問題を通じて，生徒たちは情報科学の基本的な概念をどれだけ理解し，実際に使いこなせるかが問われています．情報科学の知識は，将来の学びや日常生活での情報活用に役立つでしょう．

広島市立大学が「情報」科目の入試を導入するにあたって，「覚悟」したそうです[3]．同大学は，「情報科学部」老舗という節義のために，「情報」の個別入試導入を決断しました．この「覚悟」をも

って，新しい時代にふさわしい学生を育成するという姿勢は非常に意義深く，情報科教育にかかわる私としては素直に応援をしたいと思います．

この「覚悟」に共鳴するように，高校生の皆さんも自分の「覚悟」を持って，この新しい挑戦に臨んでください．広島市立大学の決断を支える一助として，皆さんが一生懸命に取り組む姿勢が求められています．その努力が，新たな未来を切り拓く一歩となることを心から期待しています．

参考文献

1）広島市立大学：[3月24日 開催]「『情報（情報I）』模擬問題の公開と解説」説明会の開催について
https://www.hiroshima-cu.ac.jp/news/c00038544/
2）広島市立大学：2025年度入学者選抜「情報」模擬問題
https://www.hiroshima-cu.ac.jp/guide/category0001/c00038636/
3）石光俊介：ぺた語義：「情報」個別入試への道，情報処理，Vol.64，No.9，pp.462-466 (Sep. 2023).
http://doi.org/10.20729/00227207

（2024年8月31日受付）
（2024年10月28日note公開）

■稲垣俊介（正会員）
山梨大学教育学部准教授．博士（情報科学）．東北大学大学院情報科学研究科博士後期課程修了．高等学校にて情報科教諭等の学校現場を約20年経験し，2024年度より現職．主な著書および監修は，教科書『情報I 図解と実習』（日本文教出版），『思考力アップ大学入学共通テスト「情報I」』（翔泳社），『情報I 大学入学共通テスト対策』（インプレス）等がある．