

# 特集 数学が守る 私たちの秘密

## わかと面白いパスワードや 暗証番号のしくみ

当たり前のように設定し、使っているパスワードや暗証番号。私たちの個人情報を守る上で今や欠かせませんが、みなさんはどのように設定していますか？

数字、アルファベット、記号などさまざまなものを組み合わせるべく長く複雑なものにしたほうが解読されにくいことはわかっているけど、覚えておくことを考えると悩む方もいらっしゃるのではないのでしょうか。

だれがどう足掻いても解読されないパスワード、暗証番号はどういうふうにとよいのでしょうか。

インターネットでよく使われているのはRSA暗号という暗号方式で、セキュリティ上とても重要な役割を担っています。

RSA暗号以外では、アルファベットを数字に置き換えたり、文字の並べ替えにより暗号化する方法があります。

### 例

A⇒26、B⇒25、……Z⇒1、  
CAT⇒ACT⇒TAC

難しいセキュリティのことを抜きに考えるとパズルのようで面白くありませんか？

## 暗号を題材にした映画

2015年に日本で公開された映画『イミテーション・ゲーム エニグマと天才数学者の秘密』をご覧になった方がいらっしゃるかもしれませんね。暗号の解読者であるイギリスのアラン・チューリングを描いた映画です。その映画で扱っているエニグマ暗号というのは、第二次世界大戦でドイツ軍が使用していた暗号システムです。

## 奥が深い素数や素因数分解

素数とは2以上の自然数（正の整数）で、1と自分自身以外に約数を持たない数です。その素数は暗号の仕組みを考える上で肝になってきます。

素数の積（かけ算）に表し難い数＝

解読されにくい数

ということになります。

1977年にRSA暗号の発明者の1人であるリベスト博士は2つの素数を掛け合わせた次のような129桁の数を出題しました。

114381625757888867669235779976  
146612010218296721242362562561  
842935706935245733897830597123  
563958705058989075147599290026  
879543541

懸賞金も懸けられた問題でしたが、1994年に解かれてしまいました。

中学校で必ず習う素因数分解ですが、実は奥がとっても深く、実用面では重要な役割を果たしているのです。

## 暗号に興味を持った方にお薦めの書籍

知りたい!サイエンス

中学数学からはじめる

暗号入門 現代の暗号は  
どのようにして作られたのか

関根 章道◎著

四六判・176頁 予定定価(本体価格1680円+税)

ISBN 978-4-297-10337-8

2019年2月中旬発売予定

※最新情報は弊社ホームページ(<https://gihyo.jp/>)にてご確認ください。



# 親子で楽しむプログラミング

第7回

## リストと変数を使って 合否判定を作ってみよう!

文 松下 孝太郎 / 山本 光

### リストと変数を扱おう!!

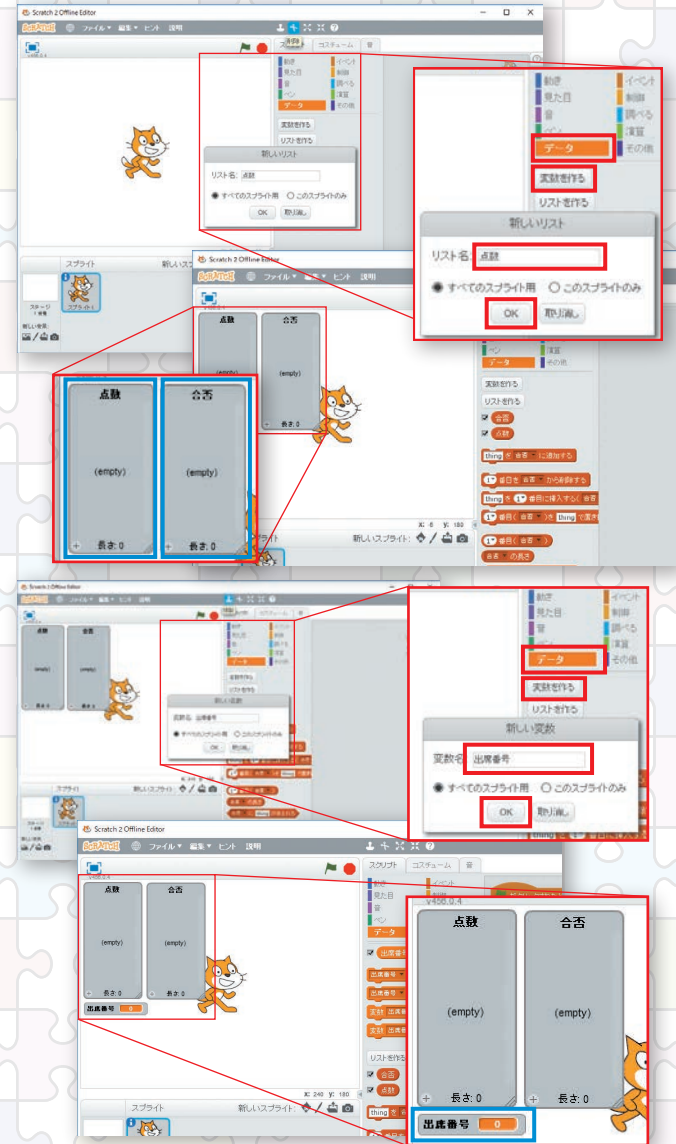
今回は、リストと変数について学びました。今回はこれらを使った基本例として合否判定を作成してみます。

### 合否判定

テストの成績で50点以上を合格、50点未満を不合格とするプログラムを作成します。

### リストと変数を準備しましょう!

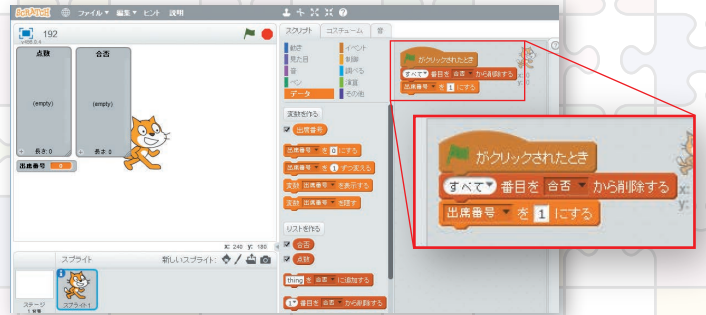
まず、リストと変数を準備します。リストはテストの点数を入れるリストと合否判定結果を入れる2つを用意します。2つのリストの名前はそれぞれ「点数」「合否」とします。変数名は「出席番号」とします。



### 合否判定を作成しましょう!!

まず、初期化を行います。初期化はプログラムを複数回実行させる場合に必要な処理となります。「合否」のリストをクリアします。また、「出席番号」の変数も「1」にします。

次に、合否判定部分を作成します。まず、繰り返し部分を配置します。繰り返し回数はデータ数に応じて入力します。繰り返しループの中に条件判断のブロックを配置します。



### 点数を入力して実行してみましょう!!

「点数」のリストに点数を入力して、緑旗をクリックします。「合否」のリストに結果が表示されます。なお、データ数が5つなので繰り返し回数を「5」にしています。



**親子でかんたん スクラッチ  
プログラミングの図鑑**

オールカラー / B5判 / 192頁  
定価(本体価格2580円+税)  
ISBN 978-4-7741-9387-8

松下 孝太郎 (まつした・こうたろう)  
(学)東京農業大学 東京情報大学総合情報学部教授。  
山本 光 (やまもと・こう)  
横浜国立大学教育学部学校教育課程数学教育講座准教授。



# 瀬山士郎先生の 数学よもやま話

連載⑩ ..... 電卓を使うということ

一人でパソコン家計簿をつけ始めて数年になる。男やもめ暮らしだから、大した出費があるわけではなく、ましてや毎月の定期収入があるわけでもない。だから家計簿の計算は暗算で済ますことも多かった。一応縦横で項目を分け、月末に縦横の和が一致すればいい。ところが一致しないのですね。となるともう一度計算をし直し。まあ、数百円単位なら合わなくても仕方がない。と言いつつ、しばらく前から、家計簿をエクセルに変えた。金額を入れれば瞬時に和が計算される。これで間違いはなくなったが、なんとなく元の手計算や暗算が懐かしい。あっ、これが世にいう脳活なのか、などと思っています。

小学校や中学校の教科書に電卓マークが入るようになってからもうしばらく経つ。桁数の多い面倒な計算は電卓でやった方が間違いがないし、早い。では3桁程度の四則演算を手計算でやる意味はどこにあるのだろうか。

2018年10月14日の毎日新聞の漫画「ぐうたらママ」(古谷三敏とファミリー企画)にこんな話題が載った。

グズオ君が算数の宿題をしている。「めんどくさいな」「電卓つかっちゃおっと」途端にパパの怒鳴り声「それじゃーなんの意味もないだろ!! 電卓なんか使うな」わかったよ、としぶしぶ計算をするグズオ君。

私たちが普通行う計算は、10進記数法という数の表し方に基づき、その構造を使って計算している。位取りの原理や小数点の移動などもその構造から分かる計算技術である。小学生がすぐに電卓を使わず、なぜ筆算を学ぶのか。それはこの構造を学ぶためである。電卓は完全なブラックボックスで、確かに計算の答は分かるが、なぜその答になるのかという疑問には答えてくれない。やはりパパの「何の意味もないだろ」には意味があったのです。

profile .....

瀬山士郎 (せやま しろう)

1946年群馬県生まれ。1970年東京教育大学大学院理学研究科終了。専門は位相幾何学、グラフ理論。1970年群馬大学教員となり、2011年定年退職。群馬大学名誉教授。数学教育協議会会員。

主な著書に「バナッハ・タルスキの密室」(日本評論社、2013年)、「読む数学」(角川ソフィア文庫、2014年)、「はじめての現代数学」(ハヤカワ文庫、2009年)、「幾何物語」(ちくま学芸文庫、2007年)「無限と連続の数学」(東京図書、2005年)、「トポロジー：柔らかな幾何学」(日本評論社、2003年)、「計算のひみつ—考え方の練習帳」(さ・え・ら書房、2004年)、「数学 想像力の科学」(岩波書店、2014年)などがある。

技術評論社

話題の新刊

## しくみと働きが理解できる

電気回路の基本をさまざまな観点から掘り下げながらわかりやすく解説!



## 電気回路が 一番わかる

有馬良知◎著  
A5判・176頁  
定価(本体価格1880円+税)  
ISBN 978-4-297-10255-5

## この1冊で、目指せ 予選突破!

過去問題の中から絶対におさえたい100問+著者オリジナルの12問の合計112問で対策はバッチリ!



## 数学オリンピックの 表彰台に立て!

予選100問+  
オリジナル12問で突破

数理哲人◎著 A5判・176頁  
定価(本体価格1980円+税)  
ISBN 978-4-297-10285-2





# 確定申告、お早めに!

## ◎サラリーマンでも確定申告が必要な場合がある

確定申告の季節がやってきました。確定申告は「納めるべき正しい額の所得税を納める」ための手続きで1年に1回行います。確定申告をすることによって、所得税の払いすぎや不足を確認するわけです。提出期間は2月18日(月)から3月15日(金)までです。

確定申告の対象となる所得は毎年1月1日から12月31日までの1年分です。サラリーマンは、年末調整で、控除や所得の状況を確認する手続きを行っているので、通常、確定申告をする必要はありません。しかし、サラリーマンでも確定申告が必要な場合があります。

- ・マイホームを購入した(住宅ローン控除)
- ・医療費が10万円を超えた(医療費控除)
- ・5団体より多くの自治体にふるさと納税を行った
- ・副業の収入が20万円以上ある
- ・株式の売買で譲渡損(売買損)がある など

このような場合は、確定申告をすると、払いすぎた所得税が戻ってくる可能性があります。

## ◎10年続く、住宅ローン控除

資金を銀行などの金融機関から借り入れて、マイホームを購入または増築したときには、住宅ローン控除を受けることができます。控除額の計算式は「平成30年末の住宅ローンの残高×1%」です。たとえば、住宅ローンの残高が平成30年末現在で2500万の場合、25万円がその年の所得税額から控除されます。住宅ローン減税は、税額控除なので、直接税金の額から引かれるわけです。これが10年間続きます。なお、住宅ローンを組んでマイホームを買った最初の年だけ確定申告を行えば、次の年からは年末調整で手続きができます。

## ◎医療費控除は、意外にあなどれない

また、病気やけがなどをして1年間に支払った医療費が、年間10万円を超えた場合には、医療費控除が受けられます(保険金等で支払われた分は差し引いて計算)。病院で払った治療費や薬代だけでなく、ドラッグストアで購入した胃腸薬や風邪薬、通院時の交通費なども医療費として認められます。扶養家族の医療費も合算できます。

たとえば、出産費用として60万円かかったとします。健康保険からの出産育児一時金42万円を差し引いて、さらに10万円を引いた残りの額8万円が医療費控除の対象となります。医療費控除は所得額からの控除です。住宅ローン控除のように直接税金から差し引かれるわけではありませんが、所得が低くなり、所得区分が変わることによって、児童手当や高額医療費なども変わってきます。もろもろを考慮すると、ちょっと手間ですが確定申告するのがベターです。

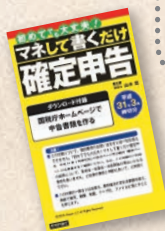
確定申告の手続きは、国税庁のホームページ (<http://www.nta.go.jp>) を活用すると、スムーズにできます。必要な情報を入力していくと、申告書類が作成できるので、あとは印刷して提出します。また、2019年1月からはID・パスワード方式でスマートフォンからも申告書を作成・提出(送信)できるようになるとのこと。ただし、ID・パスワード発行のために一度、運転免許証など本人確認のできる書類を持って税務署に行く必要があるようです。

### ↓確定申告を手っ取り早くやりたい人は



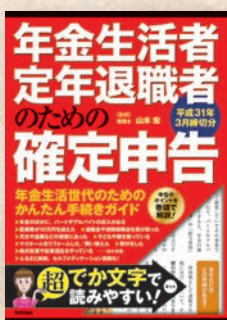
初めてでも大丈夫!  
マネして書だけ  
**確定申告**  
平成31年3月締切分

山本 宏◎監修 A4判・176頁  
定価(本体価格1380円+税)  
ISBN 978-4-297-10159-6



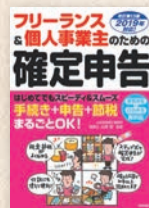
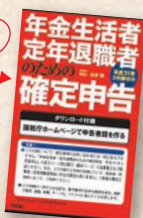
ダウンロード付録  
「国税庁ホームページで  
申告書類を作る」付き

### ↓フリーランス&個人事業主の人はこちら!



年金生活者・  
定年退職者のための  
**確定申告**  
平成31年3月締切分

山本 宏◎監修 A4判・144頁  
定価(本体価格1480円+税)  
ISBN 978-4-297-10170-1



フリーランス&個人事業主  
のための**確定申告**

山本 宏◎監修 A5判・256頁  
定価(本体価格1580円+税)  
ISBN 978-4-297-10127-5



フリーランス&個人事業主  
確定申告でお金を残す!  
元国税調査官のウラ技

大村 大次郎◎著 A5判・240頁  
定価(本体価格1580円+税)  
ISBN 978-4-297-10128-2