複雑って？

～最強のパスワードを考える～

神奈川県立藤沢総合高等学校　田澤諭子

概要

「パスワードは複雑にしなければいけない」ということは知っているが、具体的にどうしたら「複雑」になるのだろうか。
自分が使っているパスワードが適切なものなのか見直し、情報セキュリティを高めるための方法を考える。

今年夏のニュース

あのパスワード規則、実は失敗作だった

数字・記号・大文字の組み合わせ、2003年に考案した人物が後悔

By Robert McMillan

2017 年 8 月 9 日 10:33 JST

パスワード管理に関する有名な冊子の執筆者ビル・バー氏（72）は、あれは失敗作だったと告白している。

2003年、米国の業界規格設定を手掛ける国立標準技術研究所（NIST）の中間管理職だったバー氏は「NISTスペシャルパブリケーション800-63 別表A」を作成した。8ページのこの文書は、インターネットで使うアカウントを守る方法として、パスワードに記号や大文字や数字を盛り込み、定期的に変更するよう勧めていた。

THE WALL STREET JOURNAL

授業案

授業案

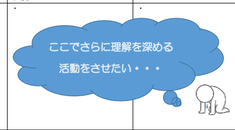
（１）研究実施校：神奈川県立藤沢総合高等学校
（２）科目：社会と情報　学年：１年
（３）教科・科目　　：情報・社会と情報
（４）単元名　　：情報セキュリティの確保
（５）単元のねらい　：個人認証と暗号化などの技術的対策など情報セキュリティを高めるための様々な方法を理解する。
（６）単元の評価規準：

関心・意欲・態度	思考・判断・表現	技能	知識・理解
積極的に授業に参加し、授業で学んだことを成果物として残そうとしている。	情報セキュリティについて、自分の考えを適切に表現できている。	情報セキュリティの技術的対策の基礎を理解し、活用することができる。	情報セキュリティの基礎を理解し、的確に活用することができる。

（７）単元の指導と評価の計画：
【評価規準の記号】ａ：関心・意欲・態度、ｂ：思考・判断・表現、ｃ：技能、ｄ：知識・理解
○：指導・評価した観点

時	学習内容	学習活動	ねらい	評価の観点 a	b	c	d	評価方法
1（本時）	効果のあるパスワード設定について検証する。	効果のあるパスワードについて検証する。	パスワードの設定によりセキュリティが高まることを理解する。	○	○			・観察 ・ｽｷﾙｼｰﾄ ・ﾜｰｸｼｰﾄ
2	情報セキュリティを高めるための技術的対策について理解する。	情報セキュリティを高めるための技術的対策のひとつである暗号化について学ぶ。暗号化・復号を実際に行う。	暗号化のしくみについての基礎的な知識を身につける。			○	○	・観察 ・ﾜｰｸｼｰﾄ

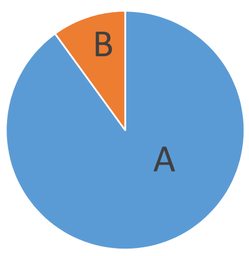
（８）指導内容：
本時のねらい：適切なパスワードはどのようなものか理解する。

授業展開	学習活動	指導上の留意点	評価方法
導入（5分）	・最新のスマートフォンで実装されているセキュリティについて考える。	・生体認証が今後も増えていくと予想されるが、パスワードを設定しなければいけない場面は当面なくならないことを確認する。	
展開１（25分）	・２つのパスワード案を出し、どちらがより複雑で強いパスワードなのか予想する。 ・パスワード強度メーターを使って、２つのパスワードが解読されるまでにかかる時間を確認する。 ・それぞれのパスワードが何パターンあるか計算し、確認する。 ・情報セキュリティは安全性と利便性の両立が大切であることを確認する。	・まずは直感で答えさせる。 ・２つのパスワードが確認できたら、いろいろ入力してみて、どのようなパスワードだと解読されるまでにかかる時間が長くなるのか考えさせる。	【知・理】 ・定期試験
展開２（15分）	・ 	・	
まとめ（5分）	・振り返り	・本時で気づいたこと、考えたことを記述させる。	【思・判・表】 ・ﾜｰｸｼｰﾄ

直感的にどちらのパスワードが複雑か？

A　Tr0u4d&3

B　dongurikorokorodongurikooikeniha



授業の導入で聞いてみると、ほとんどの生徒がAのパスワードの方が複雑だと感じていた。

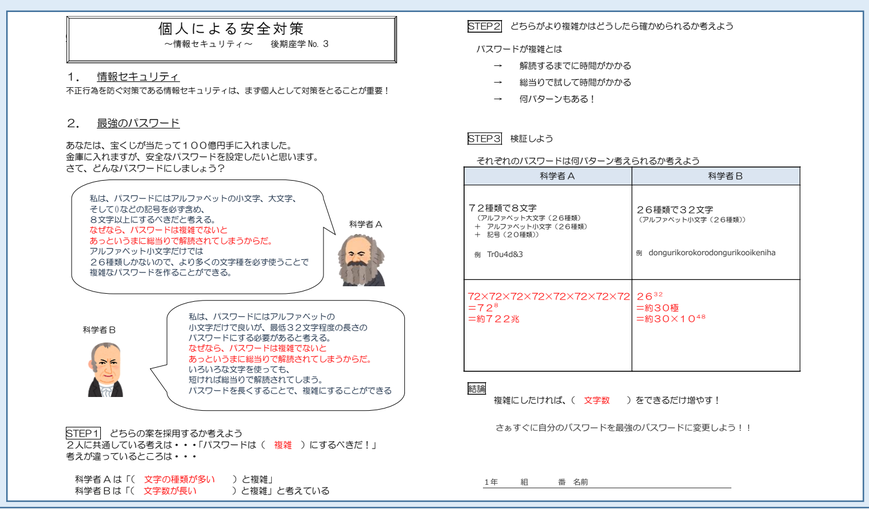
授業で使ったスライド

解読されるまでにかかる時間は？

Tr0u4d&3	dongurikorokorodongurikooikeniha
46日	24穣年 (24×10^{28})

how secure is my passwordのサイト

授業で使ったプリント



個人による安全対策
～情報セキュリティ～　後期座学 No. 3

1．　情報セキュリティ
不正行為を防ぐ対策である情報セキュリティは、まず個人として対策をとることが重要！

2．　最強のパスワード
あなたは、宝くじが当たって１００億円手に入れました。
金庫に入れますが、安全なパスワードを設定したいと思います。
さて、どんなパスワードにしましょう？

科学者Ａ：私は、パスワードにはアルファベットの小文字、大文字、そして!などの記号を必ず含め、８文字以上にするべきだと考える。なぜなら、パスワードは複雑でないとあっというまに総当りで解読されてしまうからだ。アルファベット小文字だけでは２６種類しかないので、より多くの文字種を必ず使うことで複雑なパスワードを作ることができる。

科学者Ｂ：私は、パスワードにはアルファベットの小文字だけで良いが、最低３２文字程度の長さのパスワードにする必要があると考える。なぜなら、パスワードは複雑でないとあっというまに総当りで解読されてしまうからだ。いろいろな文字を使っても、短ければ総当りで解読されてしまう。パスワードを長くすることで、複雑にすることができる

STEP１　どちらの案を採用するか考えよう
２人に共通している考えは・・・「パスワードは（　複雑　）にするべきだ！」
考えが違っているところは・・・
科学者Ａは「（　文字の種類が多い　）と複雑」
科学者Ｂは「（　文字数が長い　）と複雑」と考えている

STEP２　どちらがより複雑かはどうしたら確かめられるか考えよう
パスワードが複雑とは
→　解読するまでに時間がかかる
→　総当りで試して時間がかかる
→　何パターンもある！

STEP３　検証しよう
それぞれのパスワードは何パターン考えられるか考えよう

科学者Ａ	科学者Ｂ
７２種類で８文字 （アルファベット大文字（２６種類） ＋　アルファベット小文字（２６種類） ＋　記号（２０種類）） 例　Tr0u4d&3	２６種類で３２文字 （アルファベット小文字（２６種類）） 例　dongurikorokorodongurikooikeniha
$72\times72\times72\times72\times72\times72\times72\times72$ $=72^8$ ＝約７２２兆	26^{32} ＝約３０極 $=約30\times10^{48}$

結果
複雑にしたければ、（　文字数　）をできるだけ増やす！
さぁすぐに自分のパスワードを最強のパスワードに変更しよう！！

１年　　組　　番　名前

それぞれ何パターンある？

Tr0u4d&3	dongurikorokorodongurikooikeniha
７２種類で８文字 （アルファベット大文字（２６種類） ＋　アルファベット小文字（２６種類） ＋　記号（２０種類））	２６種類で３２文字 （アルファベット小文字（２６種類））
72^8 ＝約７２２兆パターン	26^{32} ＝約３０極パターン

考察

総当り攻撃に対して有効な方法しか伝えなかったが、辞書攻撃も防御できないといけない。
パスワード強度メーターはあくまで参考程度にしかならず、最新のパスワードクラッキング能力はどんどん上がっていることも認識しなければならない。
しかし、複雑にしすぎることで、利便性が下がってしまうのも問題だ。
見破られるまでにかかる時間が長く、かつ覚えていることができるパスワードを考える必要がある。