セキュリティ

スマホ・パソコン・インターネットを
安全に使うって、どういうこと？

合同会社Q³
ゴウドウガイシャキュービック

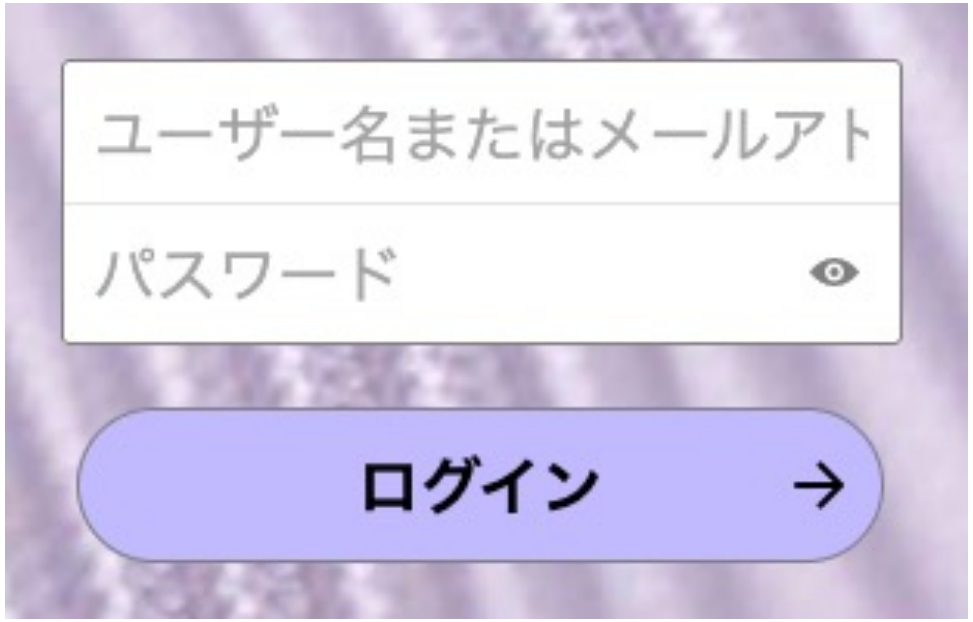
qube cafe
キューブカフェ

詐欺をする理由

- お金を直接手に入れたい
- お金を間接的に手に入れたい
  - 情報を売る
  - モノ

ユーザ名とパスワード

- ユーザ名：　　あなたが誰なのかを識別する
- パスワード：　　あなた以外が使えないようにするための暗証番号



例）ショッピングサイトに不正ログインする

- Amazon、楽天、Yahoo!ショッピング・オークション、メルカリ、ZOZOTOWN、ヨドバシ・ドットコムなど、買い物ができるサイト

利用者（ユーザ）は、クレジットカードや引き落とし銀行口座などの支払い方法を登録している

- あなたのユーザ名とパスワードが攻撃者に知られてしまったら？
  ▶ あなたのお金で買い物し放題

銀行のオンラインバンキングに不正ログインする

不正ログインを防ぐには？

- パスワードを複雑にする

よくある
「パスワードは◯文字以上にしてください」
「パスワードには大文字・小文字を含めてください」
「推測されにくいパスワードを使用してください」

なぜ？

総当り攻撃とは？

- 別名、ブルートフォース攻撃

- 自転車のダイヤルロックに例えると、**0000** から **9999** まで
  全部試したらいつかは解錠できてしまいます。

- 4桁のダイヤルなら、
  10 x 10 x 10 x 10
  = 10^4
  = 1万通り

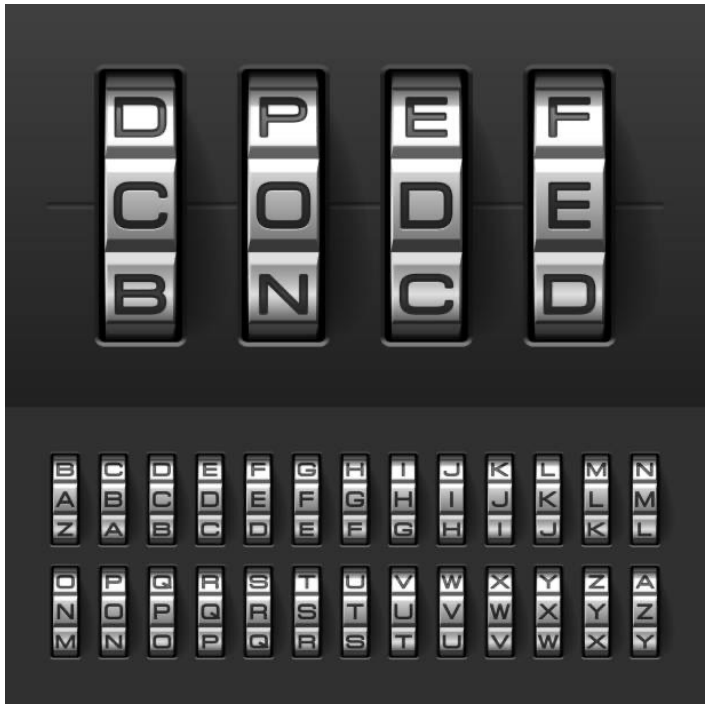
パスワードの総当り攻撃

- パスワードに当てはめると
- **小文字のアルファベットだけ使う： a ～ z の26文字**
- パスワードが8文字なら 26^8 = 208,827,064,576通り（約2千億通り）
- 問題は、コンピュータは人の手よりも速く攻撃できる
- ダイヤルを大きくすると、安全度が増します

A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P
Q	R	S	T
U	V	W	X
Y	Z		

26文字

- **大文字・小文字：　52文字**
- **大文字・小文字・数字：　62 文字**
- **大文字・小文字・数字・記号：　もっと**



使用する文字の種類を増やすと、より安全

使用する文字の種類	使用可能文字数	4桁	6桁	8桁	10桁
数字（0〜9）	10	10,000	1,000,000	100,000,000	10,000,000,000
英字（小文字a〜zのみ）	26	456,976	308,915,776	208,827,064,576	141,167,095,653,376
英字（小文字a〜zのみ）＋数字	36	1,679,616	2,176,782,336	2,821,109,907,456	3,656,158,440,062,980
英字（大小あり）＋数字	62	14,776,336	56,800,235,584	218,340,105,584,896	839,299,365,868,340,000
英字（大小あり）＋数字＋記号31文字	93	74,805,201	646,990,183,449	5,595,818,096,650,400	48,398,230,717,929,300,000
英字（大小あり）＋数字＋記号32文字	94	78,074,896	689,869,781,056	6,095,689,385,410,820	53,861,511,409,490,000,000
英字（大小あり）＋数字＋記号34文字	96	84,934,656	782,757,789,696	7,213,895,789,838,340	66,483,263,599,150,100,000

それじゃ、
パスワードを長くしたら
安心なの？

答え：

- 残念ながら、

いいえ

辞書型攻撃

- 自転車の鍵の例に戻ってみましょう
- 銀行のキャッシュカードの暗証番号でも同じ

4桁の数字に覚えやすい番号を使っていませんか？

- 自分に関連のある数字
- 身内の誕生日、記念日、住所、電話番号、

- S47年10月生まれ　→　4710　とか。

辞書型攻撃（パスワードの場合）

- 辞書型攻撃とは、
  よく使われる言葉や数字などから順番に試して鍵を開けようとする攻撃です。

- ごく一部の例
  「password」
  「abc123」
  「iloveyou」
- .,
- よく使われる単語や数字を膨大な辞書として、はじめから試していくのが辞書型攻撃です。

- すべての組み合わせを試す総当り攻撃よりも早くパスワードを見つけてしまう可能性があります。

辞書型攻撃の対策

- 脈絡のない文字列にする
- 例

```
YRHde*&Vd2b6rhGd
```

安全ですね。

でも、、、

YRHde*&Vd2b6rhGd

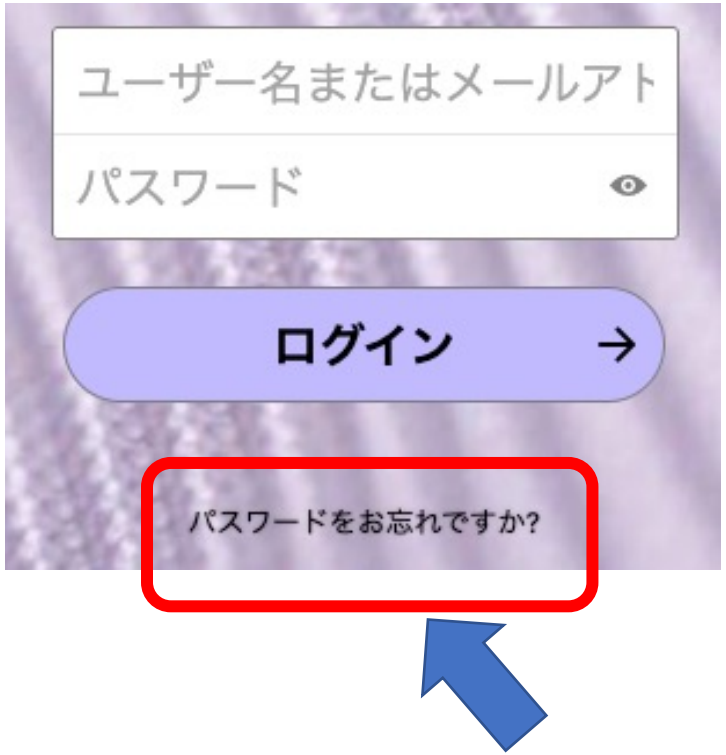
そんなの覚えていられない！

また、問題はそれだけじゃありません

「パスワードを忘れた」問題

- パスワードを忘れたとき、多くのサービスでは「パスワードを忘れた場合」という対処ができます。

- 「パスワードを忘れた」を使うと、
  - 登録されたメールアドレスや電話番号に、パスワードを再登録するためのリンク（URL）が届きます。
  - 送られてきたリンクをクリックすると、新しいパスワードの設定画面にジャンプします。



そのメール、本物ですか？

偽装

メールが既に盗み見されていたら？

赤の他人があなたのメールのパスワードを既に知っていたら、
あなたの成り代わって「パスワードを忘れた場合」を実行できてしまいます。
そして届いたメールのリンクをクリックして、好きなパスワードに変更できてしまう。

偽装問題

- パスワード再設定のメール偽装は、あなたのメールアドレスさえ知られていれば可能です。
- 送られてきたメールは、本物ですか？

パスワードリセットの仕組み

あなた

パスワードを忘れた

パスワード再設定のリンクをメール送信

リンクからパスワードを再設定

新しいパスワードを承認

利用サービス

パスワードリセットの仕組み

あなた

攻撃者

パスワードを忘れた

パスワード再設定のリンクをメール送信

不正に閲覧

リンクからパスワードを再設定

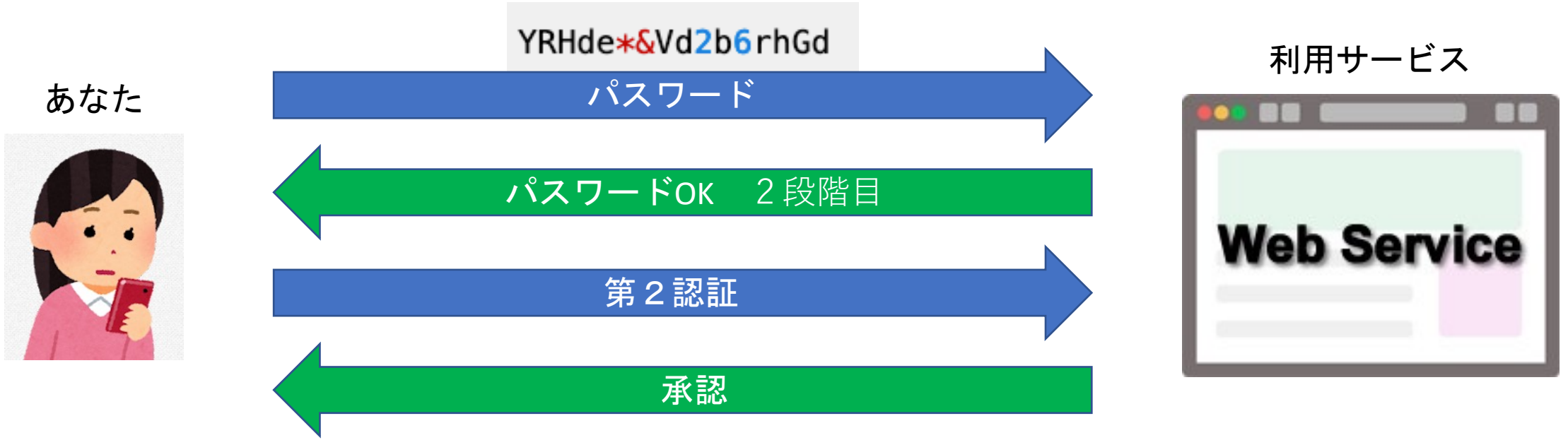
新しいパスワードを承認

利用サービス

新しい安全の仕組み

多要素認証

- 二段階認証、多段階認証、2FA（2-Factor Authentication）、MFA（Multi-Factor Authentication）とも呼ばれています。



定期的なパスワード変更は必要？

Google Play と App Store の審査の違い