基本情報対策 8/18
「セキュリティ」

山岸　拓

もくじ

はじめに

セキュリティとは…？

(例)部屋の戸締まり(鍵をかける)

スマホのロック(パスワードや指紋認証で解除)

不審なファイルやメールを開かない

→資産や情報を守る

本日のゴール

セキュリティの大切さを知る
セキュリティ分野に興味を持って学習できるようになる

→ 用語を覚える、テストの点数を伸ばす、とは直結しません…ごめんなさい

テーマ①

パスワードリスト攻撃

テーマ①

パスワードリスト攻撃：参考書 P426

あるサイトに対する攻撃などによって得られたIDとパスワードのリストを用いて、別のサイトへの不正ログインを試みる攻撃

パスワードリスト攻撃


Abema news/
なぜ？「セブンペイ」9月末で廃止
攻撃方法は“リスト型”？
リスト型アカウントハッキング
SNSなど
何かの
インターネットサービスの
アカウント情報を
不正に入手
同一のID・パスワードを
使用する他のサービス
不正アクセス可能
ショッピング
サイト
オンライン
ゲーム
ブログ

パスワードリスト攻撃

実例

セブンペイ事件(2019/07)：
被害額 5500万円、
3ヶ月後サービス終了

パスワードリスト攻撃

午前問題での出題例(平成28年秋期 問44)

問44　別のサービスやシステムから流出したアカウント認証情報を用いて，アカウント認証情報を使い回している利用者のアカウントを乗っ取る攻撃はどれか。

ア　パスワードリスト攻撃　　イ　ブルートフォース攻撃

ウ　リバースブルートフォース攻撃　　エ　レインボー攻撃

テーマ②

ハッシュ関数

テーマ②

ハッシュ関数：(参考書 P451)

任意の長さのデータを入力すると固定長のビット列(ハッシュ値，メッセージダイジェスト)を返す関数

- **入力データが同じであれば、常に同じメッセージダイジェストが生成される。**
- メッセージダイジェストから元の入力データを再現することが困難である。
- 異なる入力データから同じメッセージダイジェストが生成される可能性が非常に低い。

ハッシュ化

（参考）平成30年春期 午後問題 問1の問題文より引用

同じ
パスワード

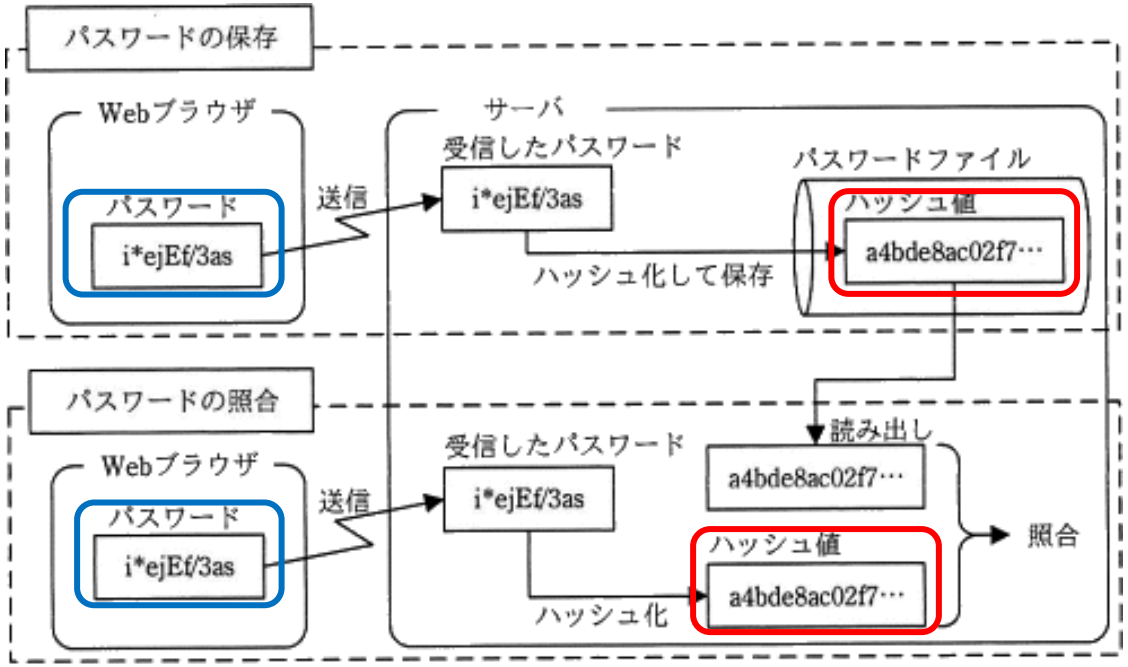

図1　パスワードの保存の流れと，照合の流れ

一致した！

ハッシュ化

実例

宅ふぁいる便(2019/01)：

パスワードをハッシュ化せず平文で保存
→ 約480万人分のメールアドレスとパスワード、生年月日、氏名、性別などが流出

ハッシュ化

午前問題での出題例(平成31年春期 問37)

問38　ディジタル署名などに用いるハッシュ関数の特徴はどれか。

ア　同じメッセージダイジェストを出力する二つの異なるメッセージは容易に求められる。

イ　メッセージが異なっていても，メッセージダイジェストは全て同じである。

ウ　メッセージダイジェストからメッセージを復元することは困難である。

エ　メッセージダイジェストの長さはメッセージの長さによって異なる。

最後に

+ おまけ

おまけ

（時間に余裕があるとき）

何かリクエストがあれば対応します （質問など）

午前問題なら過去問道場がオススメ
https://www.fe-siken.com/fekakomon.php

ありがとうございました！