

講義録レポート

講義録コード

04-49-1-301-01

講 座	情報処理安全確保支援士	科目①	模試編
目標年	2024年春期(上期)合格目標	科目②	公開模試解説 前編
コース	本科生(プラス/午前Ⅰ免除) 上級コース	回 数	1 回

講師名	根岸 良征 講師	内 訳	板書 枚数	6 枚
			補助ビジュアル 枚数	0 枚
			その他	0 枚

講義構成	解説1 (71分) → 解説2 (70分)	
使用教材	公開模試 午前Ⅱ問題	
	公開模試 午後問題	
	公開模試 解答・解説	
配付 教材・資料		
備考	※午前Ⅰの解説講義はありません。午前Ⅰ解答解説冊子でご確認ください。	

この講義録の著作権は、TAC株式会社または権利者に帰属しており、当社に無断で複製、改変、転載、転用、インターネット上にアップロードする等の著作権を侵害する行為は法律によって禁止されております。

T A C 情報処理講座

情報処理 講義録	コース・講義等	情報処理安全確保 支援士	科目	公開模試解説 前 編	回数	1
----------	---------	-----------------	----	---------------	----	---

配布物	★テスト類： []	講師	根岸 先生
	★その他の配布物1： []		
	★その他の配布物2： []		

黒板内容

問1

CRYPTREC

共通鍵暗号方式 ... ブロック長：128ビット/鍵長 128/192/256

ブロック暗号：AES, Camellia
ストリーム暗号：KCipher-2

認証付き暗号：AEAD ... TLS1.3で登場する!

メッセージ認証

AES-GCM
AES-CCM

DHE 前方秘匿性(PFS)
ECDHE

鍵共有アルゴリズム：DH, ECDH

鍵交換

共通鍵

問2 MAC：メッセージ認証符号 完全性

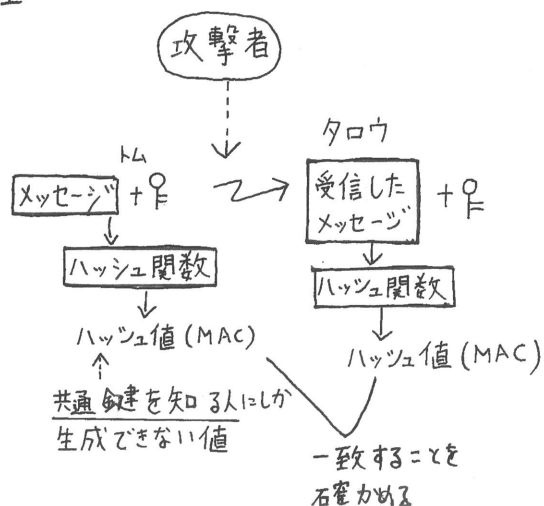
HMAC ... 鍵付きハッシュ関数

共通鍵

CBCMAC ... ブロック暗号方式を利用
改良版 CMAC

※デジタル署名の役割

・メッセージ認証 ... 己が有無の石印
・エンティティ認証 ... 本人石印



情報処理 講義録	コース講義等	情報処理安全確保支援士	科目	公開模試解説 前編	回数	1
----------	--------	-------------	----	-----------	----	---

配布物	★テスト類 : []	講師	根岸 先生
	★その他の配布物1 : []		
	★その他の配布物2 : []		

黒板内容

ドメインをまたいだ
問4 SAML : SSOを実現するしくみ
シングルサインオン

言認証情報をXML形式でやりとりする

アクション — (言認証) (認可) (属性)

・SP : サービスプロバイダ

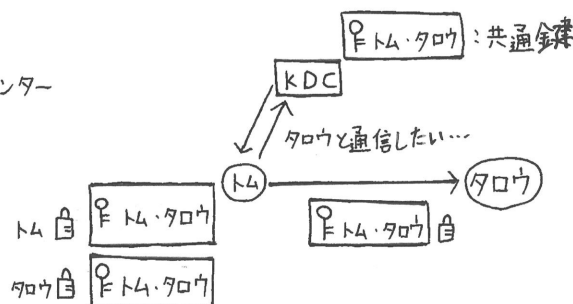
・IDP : IDプロバイダ ... 利用者言認証を行い言認証情報を発行する

・HTTPリダイレクトを用いてやりとりする

・ケルバロス言認証, KDC : (鍵) 配布センター
共通鍵

・OAuth

・LDAP



問5,6,7,8 : 攻撃手法

・クリプトジャッキング

・サイドチャネル攻撃

・クリックジャッキング

・Smurf

・DoS, DDoS

・SYN flood

・ICMP flood

問9 : セキュリティに関連する組織/取り組み

・J-CRAT : サイバレスキュー隊, 標的型攻撃

・J-CSIP : サイバース情報共有インフラ

・JVN

・XSS

・SSRF

・CSRF

・セッション固定化攻撃

・セッションフィックスセッション

・セッションハイジャック

なりすましてwebサイトを
利用する攻撃

・CSIRT : セキュリティインシデント
対応チーム

・CRYPTREC

・NISC : 内閣サイバー
セキュリティセンター

・JPCERT/CC

情報処理 講義録	コース・講義等	情報処理安全確保支援士	科目	公開模試解説 前編	回数	1
----------	---------	-------------	----	-----------	----	---

配布物	★テスト類 : []	講師	根岸 先生
	★その他の配布物1 : []		
	★その他の配布物2 : []		

黒板内容

問11

CVSS: 脆弱性の深刻度を評価する値

・基本評価基準

・現状評価基準 ... 攻撃用ツールが現状で利用可能か

情報が広く知られているか などに基つく値

・環境評価基準 ... 組織にとっての深刻度に基づく値

CVE: 共通脆弱性識別子 ... 製品に含まれる脆弱性を識別するための番号

問12 SQLインジェクション対策 → バインド木幾本書

・フリースホルダ

・プリparedステートメント

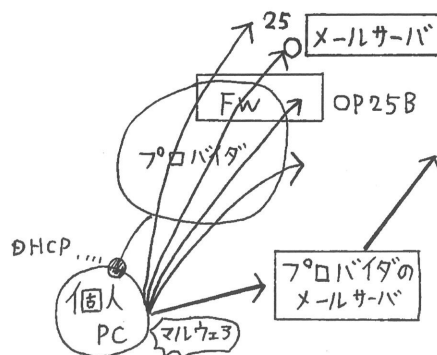
問13

OP25B ... outbound Port 25 Block

外向き 25番ポート宛ての通信をブロックする

SMTP

○サブミッションポート(587)
(代替)



情報処理 講義録	コース・講義等	情報処理安全確保 支援士	科目	公開模試解説 前 編	回数	1
----------	---------	-----------------	----	---------------	----	---

配布物	★テスト類 : []	講師	根岸 先生
	★その他の配布物1 : []		
	★その他の配布物2 : []		

黒板内容

問14 送信ドメイン認証

- ・SPF ... IPアドレスを利用する
- ・DKIM ... X-ルサーバが署名を付けて、署名を検証する
- ・DMARC
- ・DNSsec → DNSキャッシュポイズニング対策としてのしくみ
DNS応答に署名を付けることで偽応答でないことを保証する

問15 Wi-Fi Enhanced Open WPA3 ... SAE

問16 TLS 1.3

- ・認証暗号 (AEAD)
- ・鍵交換 (DHE, ECDHE) → PFSに対応
- ・少ない回数でハンドシェイクを完了できる

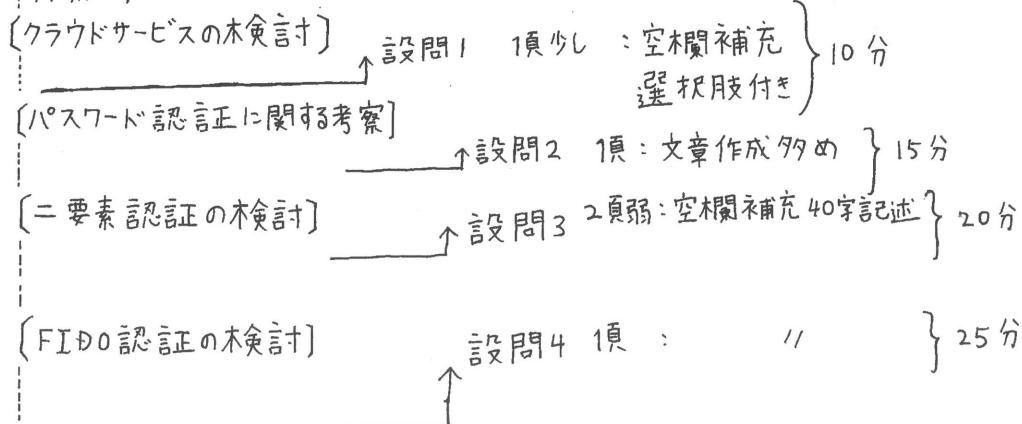
問17 HSTS

PM 問1

設問1 [クラウドサービスの検証] ... → P.4上まで

(70分)

背景・導入



情報処理 講義録	コース 講義等	情報処理安全確保 支援士	科目	公開模試解説 前編	回数	1
----------	---------	--------------	----	-----------	----	---

配布物	★ テ ス ト 類 : [] ★ その他の配布物 1 : [] ★ その他の配布物 2 : []	講師	根岸 先生
-----	---	----	-------

黒 板 内 容

雇員客や取引先とのファイル共有 → パスワード付ZIP形式の添付
その後、パスワードをメールで送る

暗号化されたファイル

× PPAP

- パスワードメール・添付ファイル付きメールの両方を攻撃者が入手(盗聴)したら、復号して内容を見られる
- 受信メールサーバ側で添付ファイルのウイルスチェックが出来ない
(暗号化されている)

- Ⓐ ソフトウェアクラウド
- Ⓑ CLOUD Act
- Ⓒ GDPR
- Ⓓ クオリティクラウド

Ⓕ リバースブルートフォース

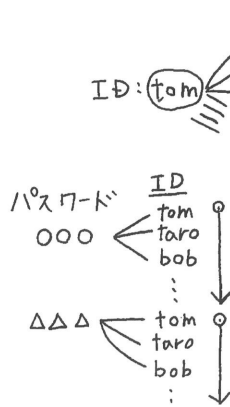
- ブルートフォース : 糸念あたり

Ⓖ パスワードリスト

- リバースブルートフォース
パスワードスプレー

○ 辞書攻撃

他のサイトで流出したID・パスワードを言式す



※同一ユーザIDに
対して矢旦時間に
何度も失敗すると
発重くなる

○ オンライン攻撃

実際に接続して、ID・パスワードを
入力し言式す

○ オフライン攻撃 (手元のPC上で言式す)

・ パスワードファイル中のパスワードの
ハッシュ値の解析

・ パスワード付きファイルのパスワード
を推測 (言式す)

tom@asha.com	1234567890
bob@bsha.co.jp	abcabcabc2

情報処理 講義録	コース講義等	情報処理安全確保支援士	科目	公開模試解説 前編	回数	1
----------	--------	-------------	----	-----------	----	---

配布物	★テスト類 : []	講師	根岸 先生
	★その他の配布物1 : []		
	★その他の配布物2 : []		

黒板内容

利用者認証に用いる要素

- 矢口言蔵 … パスワード認証 など
- 生体情報 … 指紋、顔、静脈パターン、虹彩パターン など
- 所有物 … スマホ (SIM)、ICカード など

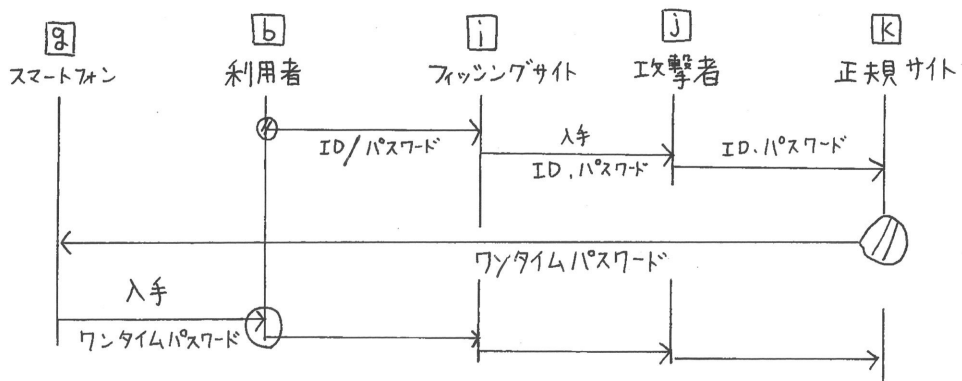
・二要素認証 (デュアルファクタ認証)

・多要素認証

第一パスワード → 第二パスワード
矢口言蔵 矢口言蔵

○ 二段階認証 / 多段階認証

× 二要素認証



◎ SMS インターセプト

◎ FIDO 認証 … パスワードレス認証

↓ スマホに搭載の生体認証を用いる

↓ スマホが署名を生成して Web サイトへ送る