講義録レポート

講義録コード　04-39-1-301-01

講　座	情報処理安全確保支援士	科目①	模試編
目標年	2023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
			補助ﾚｼﾞｭﾒ枚数	0　枚
			その他	0　枚

講義構成	解説1 (63分) → 解説2 (53分) → 解説3 (29分)
使用教材	公開模試 午前Ⅱ問題 公開模試 午後Ⅰ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。

ＴＡＣ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：[ ] ★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

AM Ⅱ

Q1～17　セキュリティ

Q18～20　ネットワーク

Q21～25　その他分野

問2　サイバーキルチェーン：主に標的型攻撃を想定して、攻撃の段階を7つに分類したもの

偵察
- ウォードライビング
- ポートスキャン、バナーチェック、スタックフィンガプリンティング
  OS、サーバプログラム、ライブラリなどの環境 …… などを調べる
- 組織：ソーシャルエンジニアリング

- 武器化　マルウェア作成
- デリバリー　メール添付、水飲み場型攻撃、ドライブバイダウンロード
- エクスプロイト　exploitコード（攻撃用プログラム）：管理者権限を奪取　権限昇格
- インストール
- C&C：Command & Control　PCやサーバを乗っ取って、遠隔操作する
  - ボット：C&Cサーバ：指令塔となるサーバ

- 目的を実行

コネクトバック通信

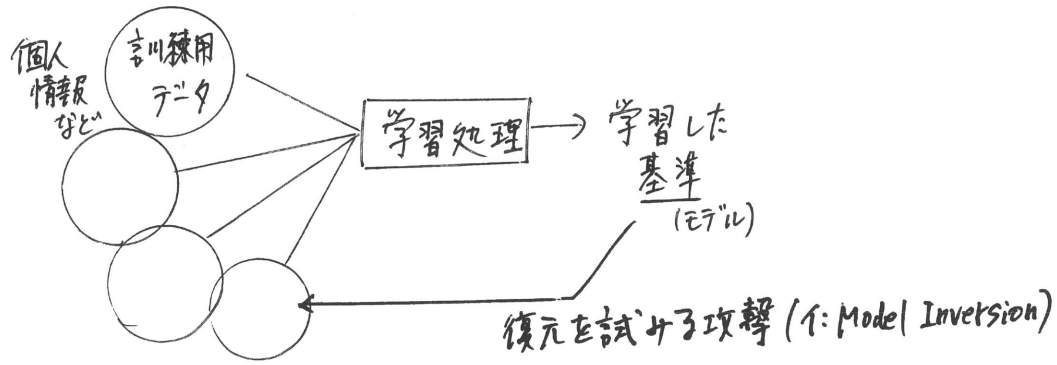
情報処理 講義録	コース・講義等	情報処理安全確保支援士	科目	公開模試解説 前編	回数	1

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

問3

AIアルゴリズムに対しての攻撃



AIの判断を意図的に誤らせる：(例) ある種(特殊な)の柄の服を着る → 人として認識されない

ア Adversarial Examples. 攻撃.

スミッシング：スマホ・携帯TELのSMS(ショートメール)を利用した、偽メール 偽サイトへ誘導する

問5 サイドチャネル攻撃

(例) テンペスト

・消費電力の変化から、暗号化・復元処理の内容を探る：電力解析攻撃 → 鍵を推測する

・タイミング攻撃

問6 量子コンピュータでも解読困難な暗号方式：PQC

・SAE：WPA3

・SPF：送信ドメイン認証

・PFS：TLS通信、鍵交換にDHEを使う

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7 SAML ：SSOの実現方式
Web技術と相性が良い

- IdP：IDプロバイダ (例) ユーザ認証を行うサイト
- SP：サービスプロバイダ (例) オンラインショップサイト
- SAML アサーション：HTTPリダイレクトを用いて、アサーションをIdPとSP間で受け渡す
  - 認証・属性
  - 認可
- ケルベロス認証：チケット TGS（チケット交付サーバ）
  TGT（チケット交付チケット）

問11 FIPS 140-3 ：暗号モジュール

問14 TLS 1.3

- (PFS)に対応している：DHE, ECDHE
  ~~RSAの鍵交換は~~ PFS対策とはならない
- 少ない回数でハンドシェークを完了できる
- ハンドシェークの途中から暗号通信できる
- 0-RTT セッション(再開)時に、あらかじめ決めた[共通鍵(PSK)]で最初から暗号通信できる

問17 AEAD：認証暗号 → CRYPTREC暗号リストを見ておく！
暗号化と共にメッセージ認証も行える方式

AES-GCM
AES-CCM

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

PM I 問1

・エンティティ(主体)認証：利用者認証，クライアント認証，サーバ認証 など 本人本物を確認(機器)

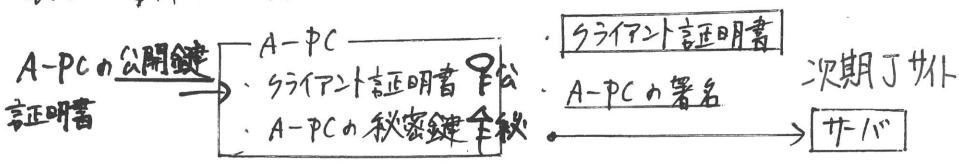
・TPM

・TLS：利用が推奨されるバージョン／TLS 1.2，TLS 1.3

・CRYPTREC 暗号リスト

・オンプレミス … 自組織に機器を設置して運用する ⟷ クラウドサービス

表1 要件3：クライアント認証 → クライアント証明書による認証



・知識 …. パスワード

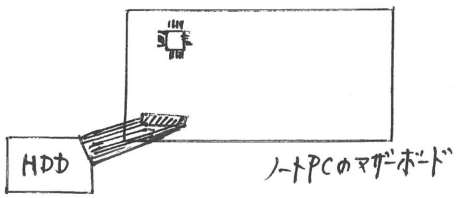
・生体情報 … 顔，指紋

・物 …… ICカード，セキュリティトークン

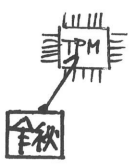
・多要素

・多段階 …. 第一段階 第一パスワード 知識

第二段階 第二パスワード



・TPM … セキュリティモジュール



・公開鍵，秘密鍵の生成

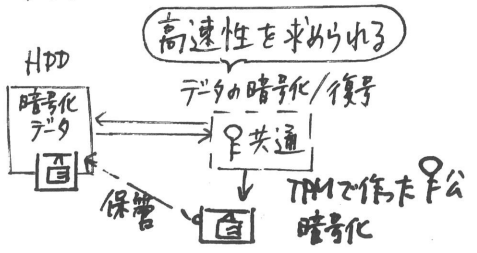
・署名処理，暗号化／復号処理

・データを安全に保管する

・ハッシュ値を生成

・乱数を生成 など

※耐タンパ性



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

・ブックマーク → URLを登録しておく

表2 現在のJサイト http://intra.a-sha.co.jp/ → HTTPリダイレクト

表3 次期Jサイト https://intra.a-sha.co.jp/

HSTS：次回以降、自動的にHTTPSでアクセスする
(ブラウザが覚えている)

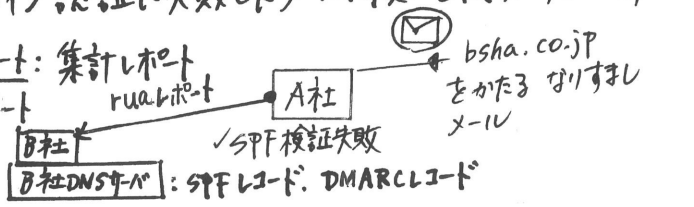
・TLS/SSLに対する攻撃 → TLS1.2, TLS1.3
- POODLE攻撃 BEAST攻撃
- バージョンロールバック攻撃
- ダウングレード攻撃

問2
- ログを分析する
- メールヘッダなどのヘッダの内容を分析する
- 事前調査の手法：ポートスキャン
  - TCPスキャン…3ウェイハンドシェーク 実際に接続してみて反応があるかを調べる
  - UDPスキャン…ICMP port unreachable ポート到達不能 が返ってこないかを調べる
- 開いているポートを探す
  = 当該のポートで待ち受けているプロセスが存在する

・SPF, DMARC → 送信ドメイン認証に失敗したメールの扱いを周知するしくみ

SPFレコード(図3)

ruaレポート：集計レポート
rufレポート



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

FW：静的パケットフィルタリング（スタティック） ⟷ 動的パケットフィルタリング（ダイナミック）

- 行き／帰り両方の通信についてあらかじめ設定しておく
- 接続方向の設定だけをしておく
- もどりのパケットに関する通過許可は自動で行われる

FWのフィルタリングルール

宛先	送元	動作	
IP DNS 53	インターネット側 ≧1024 ANY	許可	…… DMZ上のDNSサーバにDNS問合せパケット到着
インターネット側 ANY ≧1024	IP DNS 53	許可	…… DNS回答パケット

宛先	送元	動作	
IP DNS 53 ダイナミックパケットフィルタリング	インターネット側 ANY ≧1024	許可	… DMZ上のDNSサーバにDNS問合せパケット到着
インターネット側 ANY ≧1024	IP DNS 53	許可	… DNS回答パケット

スタティックパケットフィルタリング