

講義録レポート

講義録コード

04-29-1-301-02

講 座	情報処理安全確保支援士	科目①	模試編
目標年	2022年春期合格目標	科目②	公開模試解説 後編
コース	本科生(プラス/午前Ⅰ免除) 上級コース	回 数	1 回
用 途	ビデオブース ・ テープレクチャー ・ 集合ビデオ WEB ・ DVD通信 ・ 資料通信		

講師名	根岸 良征 先生	講義録枚数	8 枚	※レポート 含まず サイズ (B5)
		補助レジュメ枚数	0 枚	
		その他	0 枚	

講義構成	解説1 (39分) → 解説2 (98分) → 解説3 (42分)		
使用教材	公開模試 午後Ⅰ問題		
	公開模試 午後Ⅱ問題		
	公開模試 解答・解説		
配布教材			
備考			

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。

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 後
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

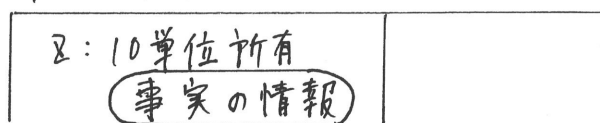
先生

黒 板 内 容

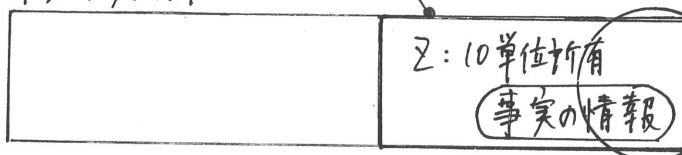
PMI 問3

- ・ セキュアプログラミング
- ・ Webアプリへの攻撃
- ・ OS コマンドインジェクション
- ・ バッファオーバーフロー
- ・ サンドボックス
→ 制限された動作環境
- ・ ハッシュ関数
- ・ 公開鍵暗号方式

トランザクション2

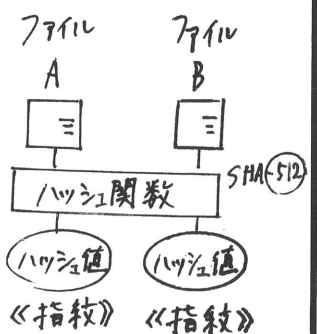


トランザクション1



↑
 使う
 Tさんの秘密鍵で復号してから...
 書き写す = 通貨を所有している
 本人にだけ出来る

← Tさんの公開鍵で
 暗号化されている



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 後編	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

PMII 問1

・暗号化ZIP 添付ファイルの問題点

- × 実際上、機密性は保てない
- × メールサーバでのウイルスチェックに影響

公開鍵方式を
利用して
・暗号化
・署名
する

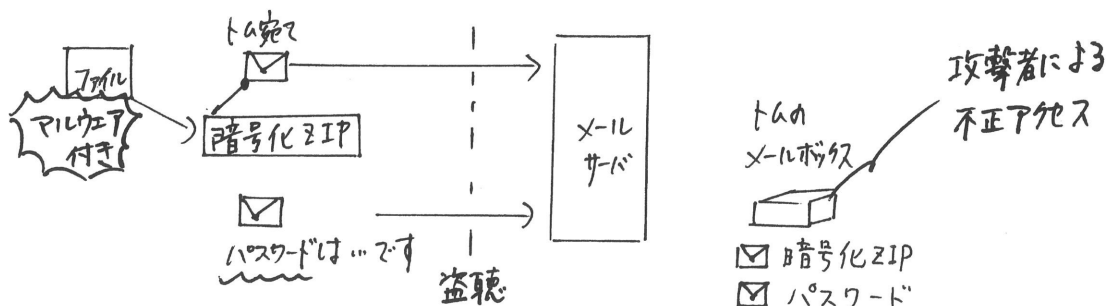
● X-11の場合
S/MIME

● ファイル交換用サイト
Webベースで提供
(HTTPS, ユーザ認証)

・言認可制御 : アクセス権の言認定, アクセス制限 アクセスコントロール

・P社ルール

- ・ ... 公開されている ... 各種の資料ファイル ...
- 公開されている ファイル名と同じ ファイル名にする ...

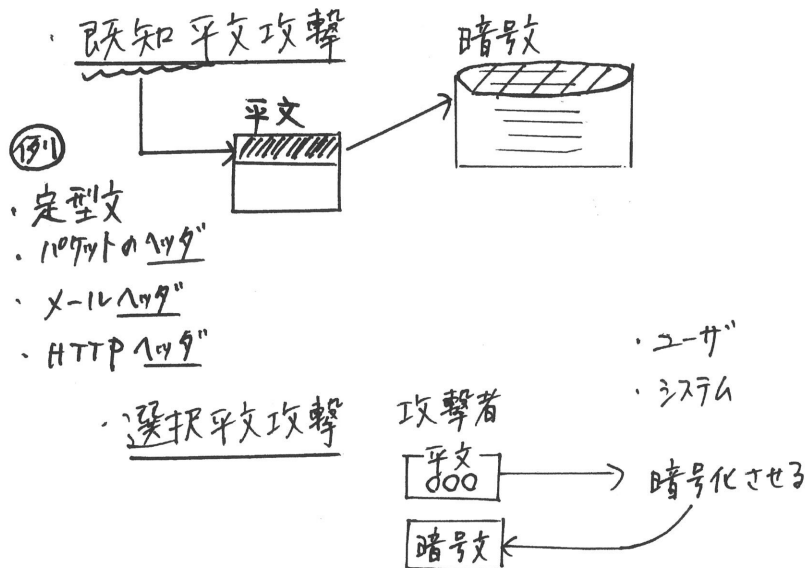


情報処理 講義録	コース講義等	情報処理安全確保支援士	科目	公開模試解説 後編	回数	1
----------	--------	-------------	----	-----------	----	---

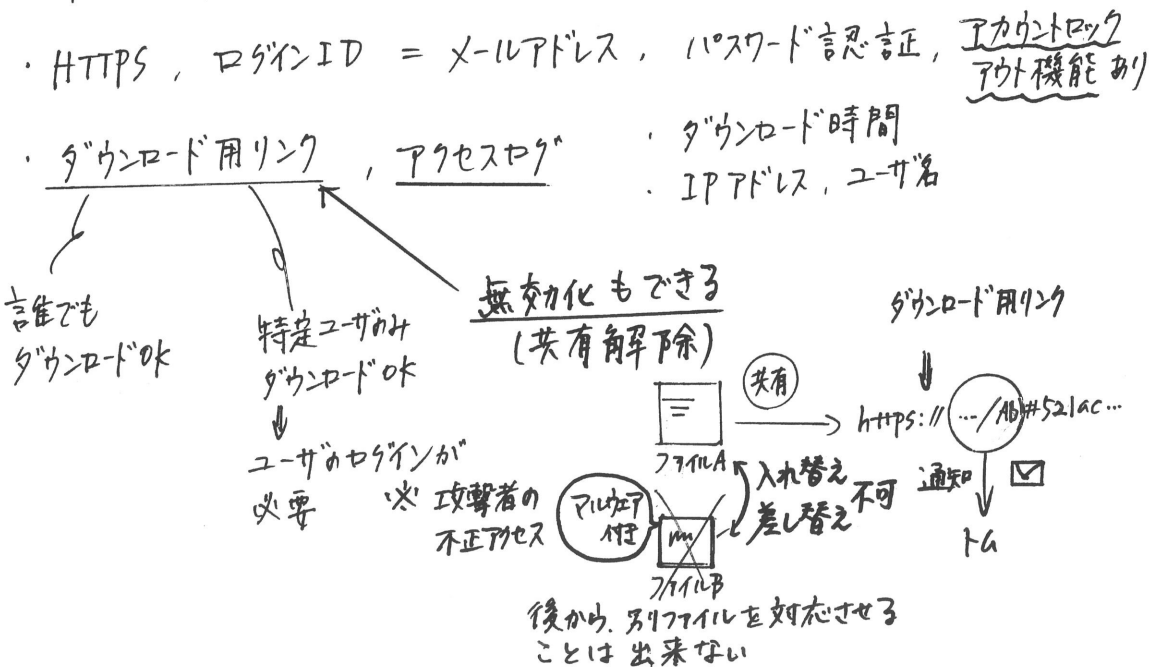
配布物	★テスト類： []	講師	根岸 先生
	★その他の配布物1： []		
	★その他の配布物2： []		

黒板内容

暗号文の解読のための手法



ファイル交換システム

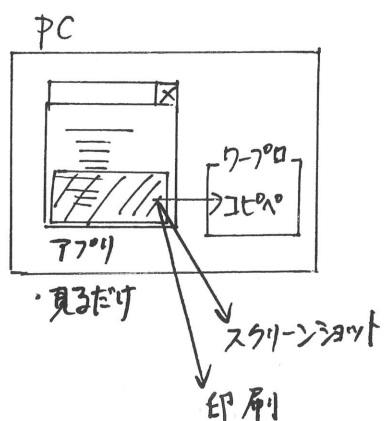
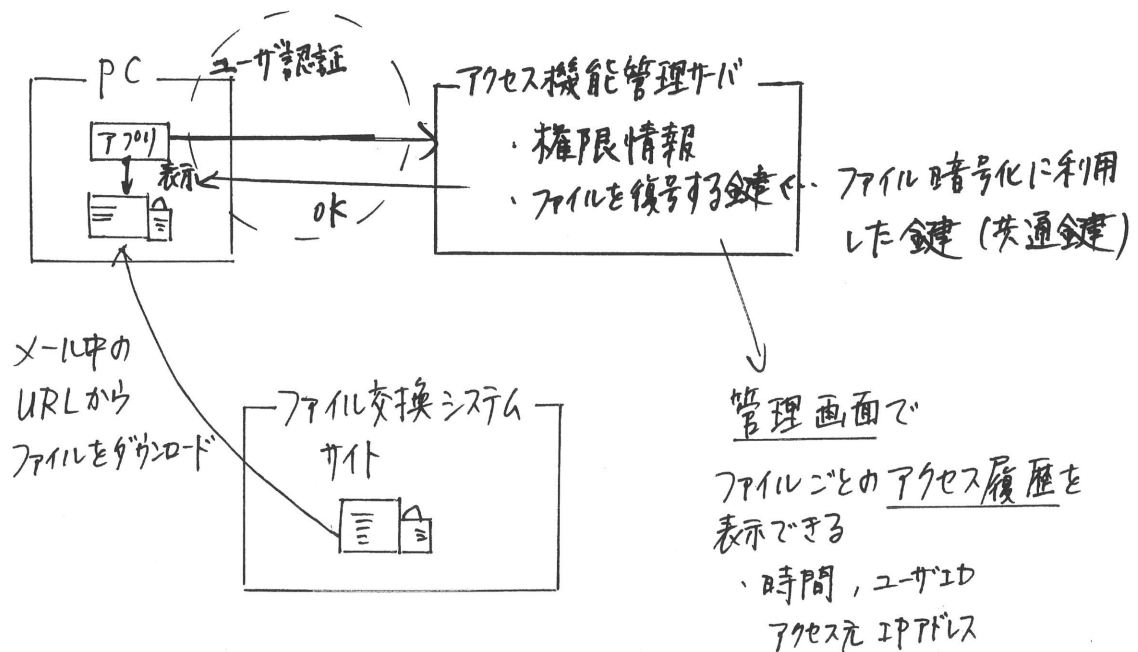


先生

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 後 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

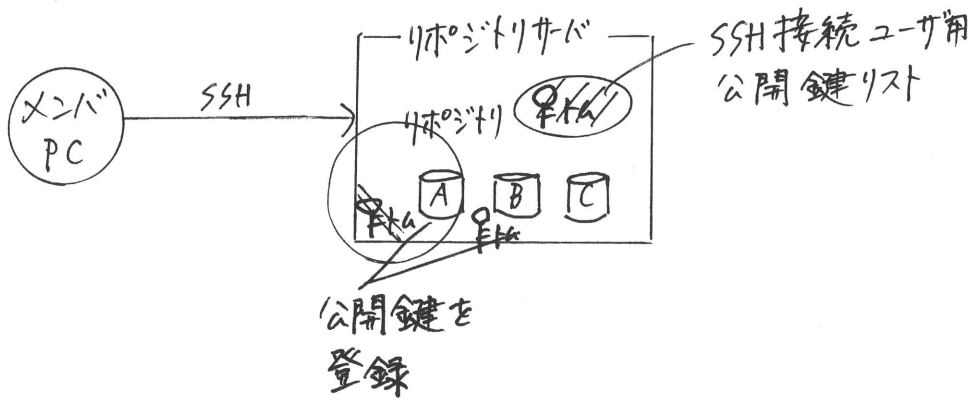


情報処理 講義録	コース講義等	情報処理安全確保支援士	科目	公開模試解説 後編	回数	1
----------	--------	-------------	----	-----------	----	---

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

図6



PMⅡ 問2

- IoT 機器におけるセキュリティ
 - 量が多い = 攻撃者 (踏み台) 手下にできる機器が多い
 - 設置したらそのまま、あまり頻繁に保守されない → ハードウェア性能が高くなっている (近年)
 - ファームウェアの脆弱性 → ファームウェアが更新されず 長期間放置 コードサイン プログラムコードに開発者がデジタル署名を付ける
 - パスワード設定が初期値のまま
 - IoT 機器にボットを感染させて、ボットネットに組み込む
 - 耐タンパ性

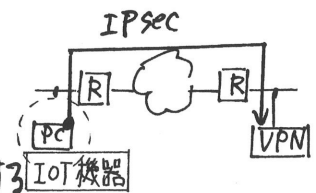
情報処理 講義録	コース講義等	情報処理安全確保支援士	科目	公開模試解説 後編	回数	1
----------	--------	-------------	----	-----------	----	---

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

IPsec による VPN

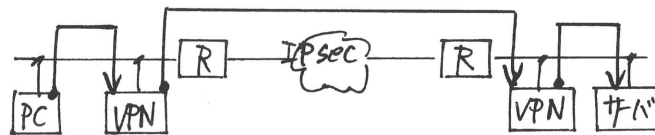
- ESP : 暗号化 / 認証
- AH : 認証 (エンティティ認証)
- IKE : 鍵交換プロトコル, ユーザ認証, 暗号化 / 復号をする



運用モード

- トランスポートモード : 端末が直接 IPsec パケットを送出する
- トンネルモード : LAN 間の接続に利用

IPsec VPN 装置を LAN 内に設置して、
IPsec VPN 装置がパケットの暗号化 / 復号をする

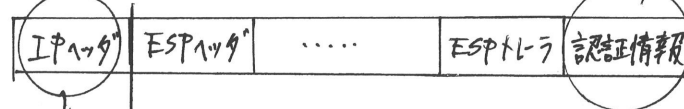


IPsec 通信と NAT

NAT トラバース

NAPT → IP アドレス / ポート番号を書きかえる

IPsec パケット



NAT トラバース
では、

UDPヘッダを NAPT ルータで挿入する

UDP エンカプレーション

ハッシュ値と
考えるべき

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 後 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

p.16 (6) 初期設定では 99回でロック ...

全ての管理用エロがロック ... ハードリセット ...

・ あえて、アカウントロックアウト
させて、使えなくする

(DOS攻撃)

5秒間リセットボタンを押します...

↑ IOT機器の設置現場へ
人が向かう必要がある

(7) ... 自動設定 サービス ... デフォルトで 起動 ...

(デモン)

... 利用していない

サーバプロセス

p.18上 ... 外出先 から タブレットで 社内システムに接続 ...

VPNを利用 ... 接続元IPアドレス ... F社本社の
ファイアウォールのもの ...