講義録レポート

講義録コード　04-29-2-301-02

講　座	情報処理安全確保支援士	科目①	模試編
目標年	2022年秋期合格目標	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	7　枚	※レポート含まず
		補助レジュメ枚数	0　枚	サイズ(B5)
		その他	0　枚	

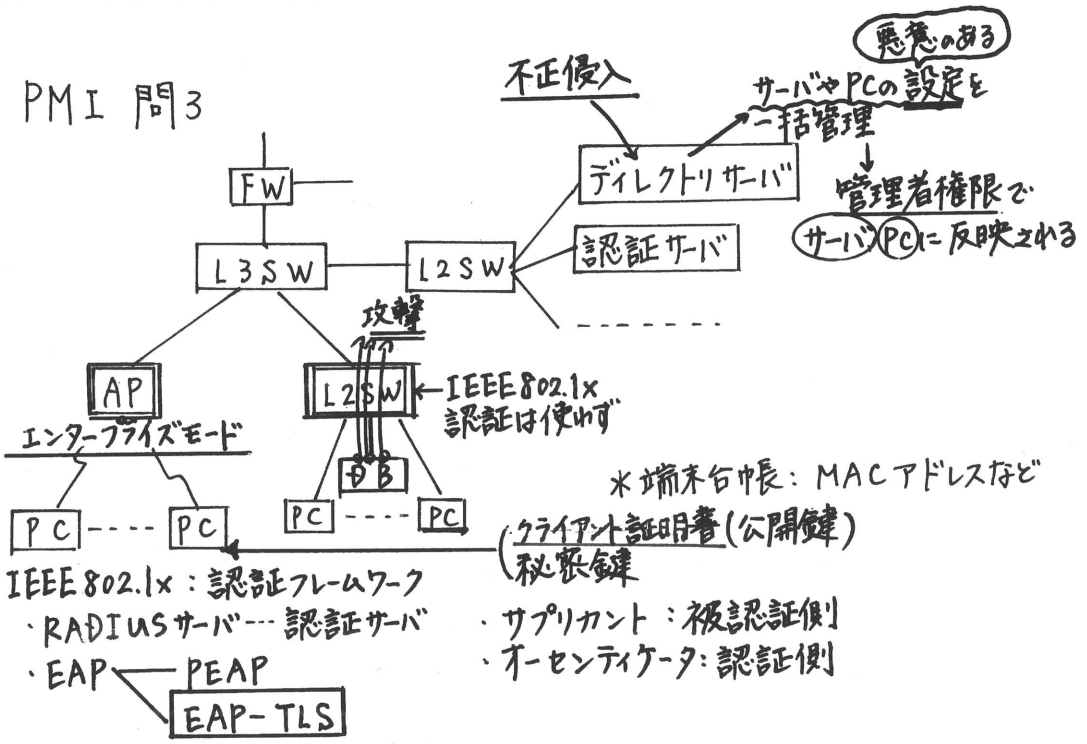
講義構成	解説1 (54分) → 解説2 (65分) → 解説3 (29分)
使用教材	公開模試 午後Ⅰ問題 公開模試 午後Ⅱ問題 公開模試 解答・解説
配布教材	
備考	

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

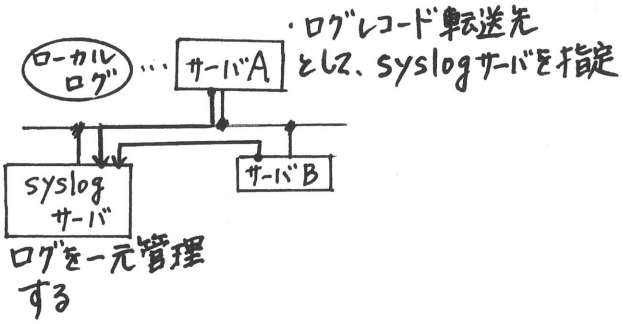
PMI 問3



IEEE802.1x：認証フレームワーク
・RADIUSサーバ…認証サーバ
・EAP — PEAP
EAP-TLS

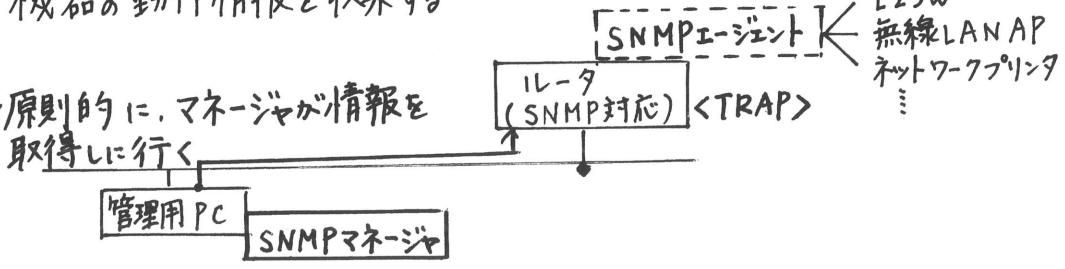
・サプリカント：被認証側
・オーセンティケータ：認証側

・Syslog
ログサーバ：syslogサーバ



◎ログを一元管理する

・SNMP
Simple Network Management Protocol
機器の動作情報を収集する



×原則的に，マネージャが情報を取得しに行く

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

・シャドーIT

・DHCPサーバ：IPアドレスの払い出し時に、MACアドレスを検証する

MACアドレス
↑
端末台帳

指摘点
・手動設定
・MACアドレスを偽る

・検疫ネットワークシステム

機能
・隔離
・検疫（検査）
・治療

検疫ネットワーク（隔離されたネットワーク）

VID=1 検疫サーバ

VLAN

VID=2 社内LAN

PC

・ウイルス感染の有無
・許可されていないソフトの有無
・セキュリティパッチ
・ウイルス定義ファイル
・・・・など

VID=1
VID=2

社内LAN

社内LAN

PC

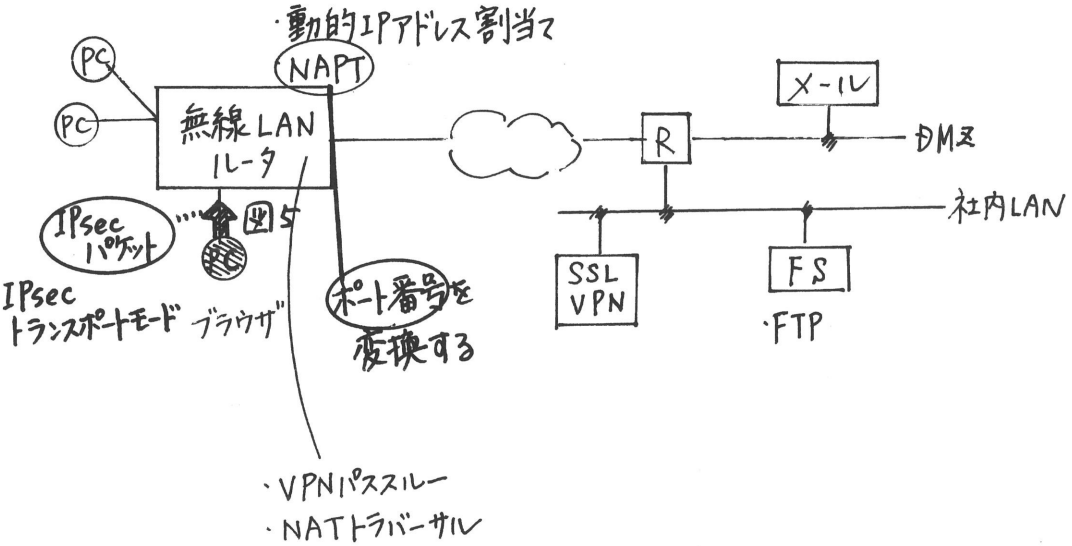
OK

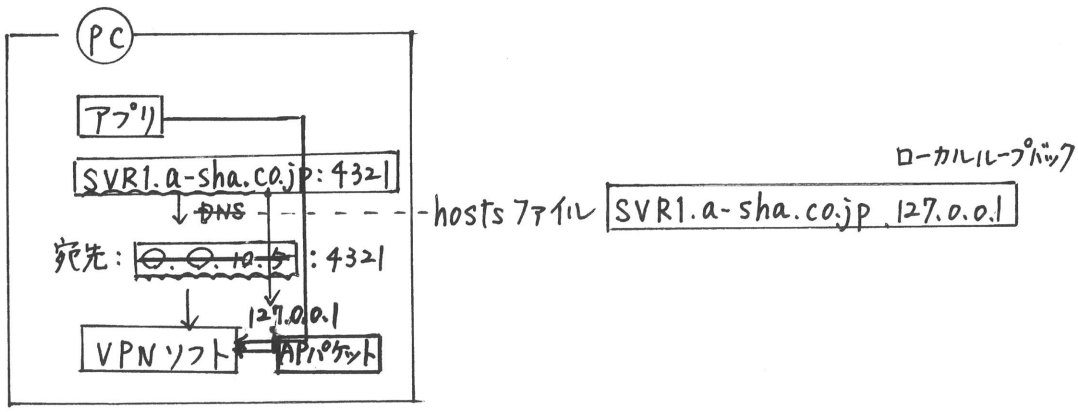
情報処理 講義録	コース・講義等	情報処理安全確保支援士	科目	公開模試解説 後編	回数	1

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



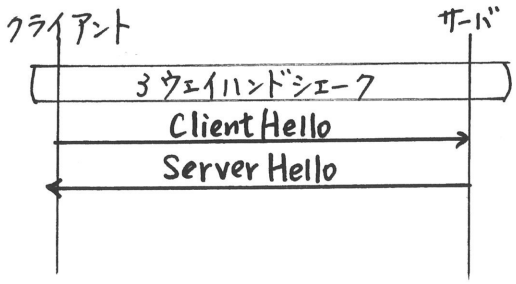


情報処理 講義録	コース・講義等	情報処理安全確保支援士	科目	公開模試解説 後編	回数	1

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：[ ]		

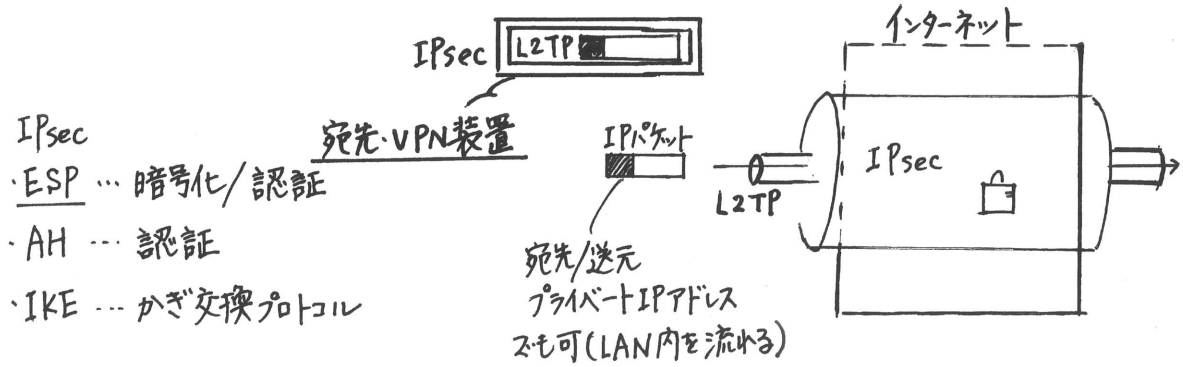
黒板内容

TLSのハンドシェーク



TLS 1.3 鍵交換 → DH法にもとづくもの
- DHE, ECDHE
- PSK

PFS ×RSA
×DH



IPsec
- ESP … 暗号化/認証
- AH … 認証
- IKE … かぎ交換プロトコル

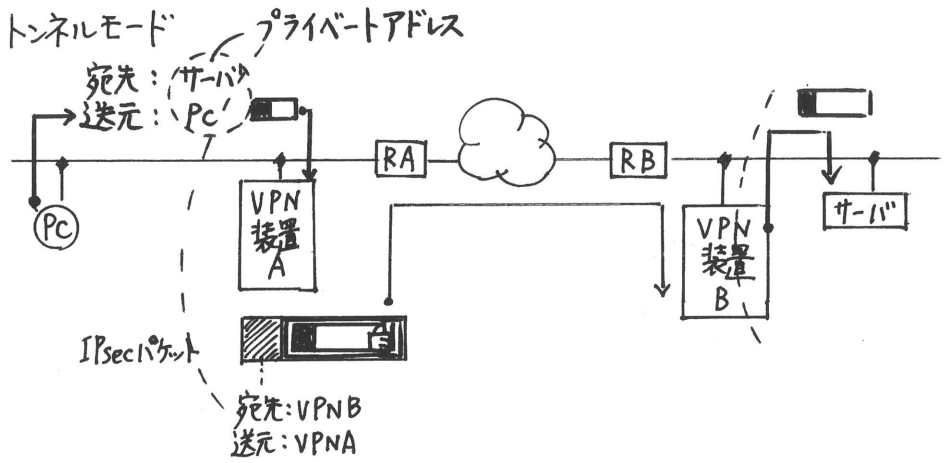
情報処理 講義録	コース・講義等	情報処理安全確保支援士	科目	公開模試解説 後編	回数	1

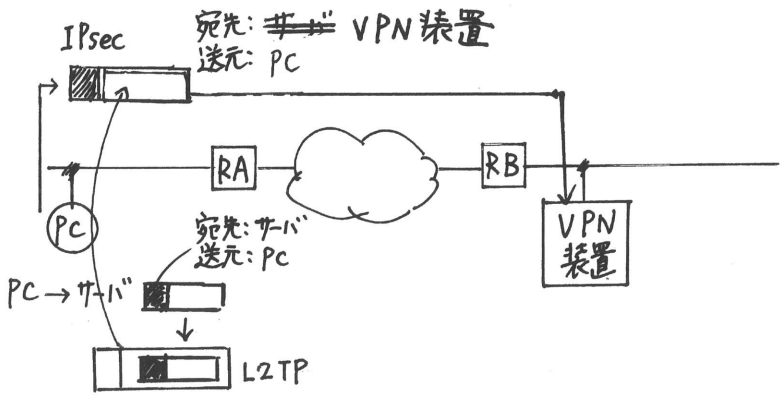
配布物	★テスト類：[ ]	講師	根岸 先生
	★その他の配布物1：[ ]		
	★その他の配布物2：[ ]		

黒板内容

トンネルモード ----- LAN間の接続

トランスポートモード --- L2TP/IPsec



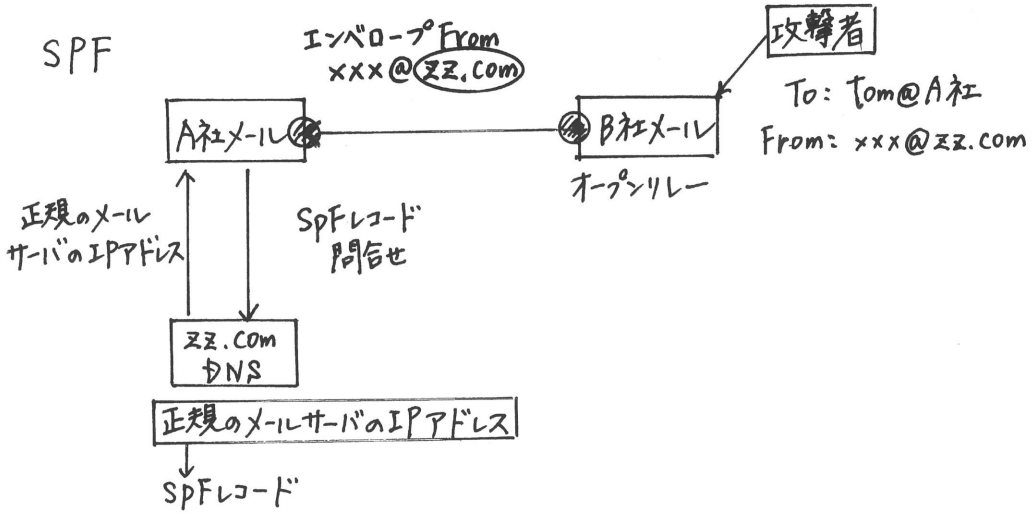


情報処理 講義録	コース・講義等	情報処理安全確保支援士	科目	公開模試解説 後編	回数	1

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：[ ]		

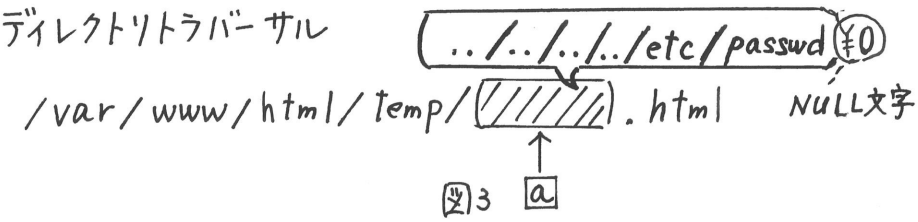
黒板内容

SPF



PMII 問2

・ディレクトリトラバーサル



@ /etc/passwd.

・ユーザID，パスワードのハッシュ値などが記録されている

・盗まれたくはないファイル

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

・OSコマンドインジェクション

・Referer ：HTTPヘッダ中の項目

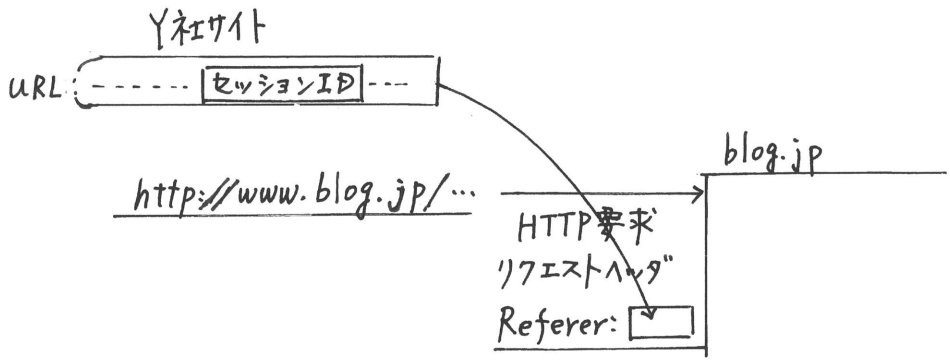


図7 セッションフィックセーション，セッション固定化攻撃
↑セッションハイジャック攻撃の一手法

図9 CSRF

・クリックジャッキング