講義録レポート

講義録コード　04-49-1-301-02

講　座	情報処理安全確保支援士	科目①	模試編
目標年	2024年春期(上期)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

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 (56分) → 解説2 (42分) → 解説3 (54分)
使用教材	公開模試 午後問題 公開模試 解答・解説
配付 教材・資料	
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

PM 問2

PW暗号化ZIPファイル

- 後からメールでパスワードを送る → 機密性を保つことは困難
- 受信したメールサーバでのウイルス検査が困難

○ 導入当初 ① PW暗号化ZIPファイルを添付したメールを送信 ⚠ 手作業
② パスワードメールを送信

○ メールアプライアンス製品 …→ ①, ② を自動化

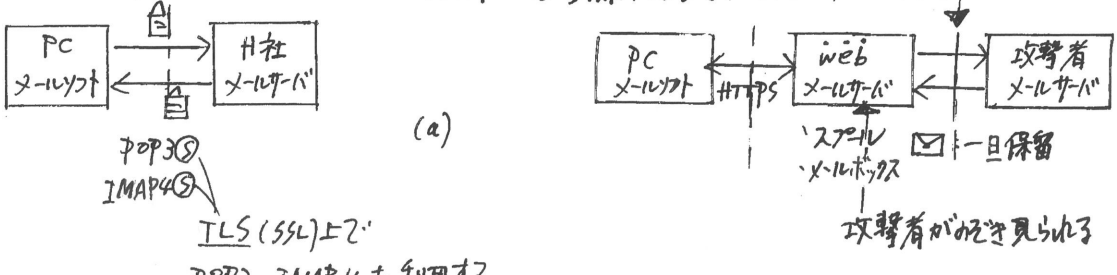
宛先を間違えるとパスワードもそこに届く ← この宛先に、自動的に② パスワード が届く

パスワードへの攻撃

- オンライン攻撃 … アカウントロックアウトで しめだせる
- ○ オフライン攻撃 … 攻撃者のPCで試すので、パスワード試行回数に上限なし

→ PW暗号化ZIPファイルには、オフライン攻撃が使える

図4 SMTPS ------ ① TLSでセッション確立 ② SMTP
SMTP(STARTTLS) ① SMTP ② STARTTLSで、TLSセッション確立



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

(事前鍵交換)

共通鍵(PW) … 鍵の配送問題が生じる　※S/MIMEでは

PW暗号化ZIPファイル ×

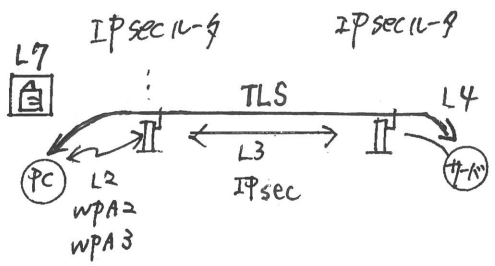
S/MIME L7　公開鍵 … 〃 が生じない　公開鍵証明書で扱う

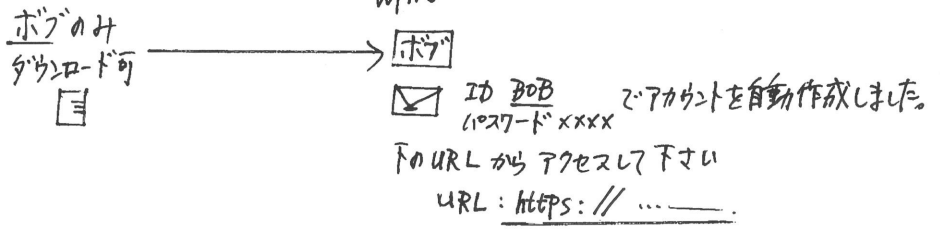
↑ メール受信者から入手する

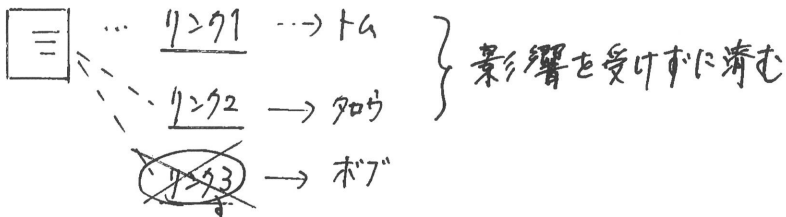
TLS … L4

IPsec … L3

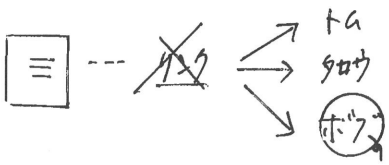
WPA2 WPA3 … L2

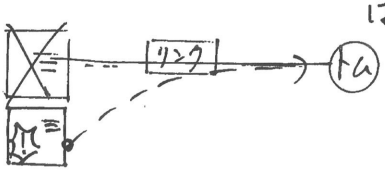






はれてしまった
はれてしまったリンクだけを無効にする



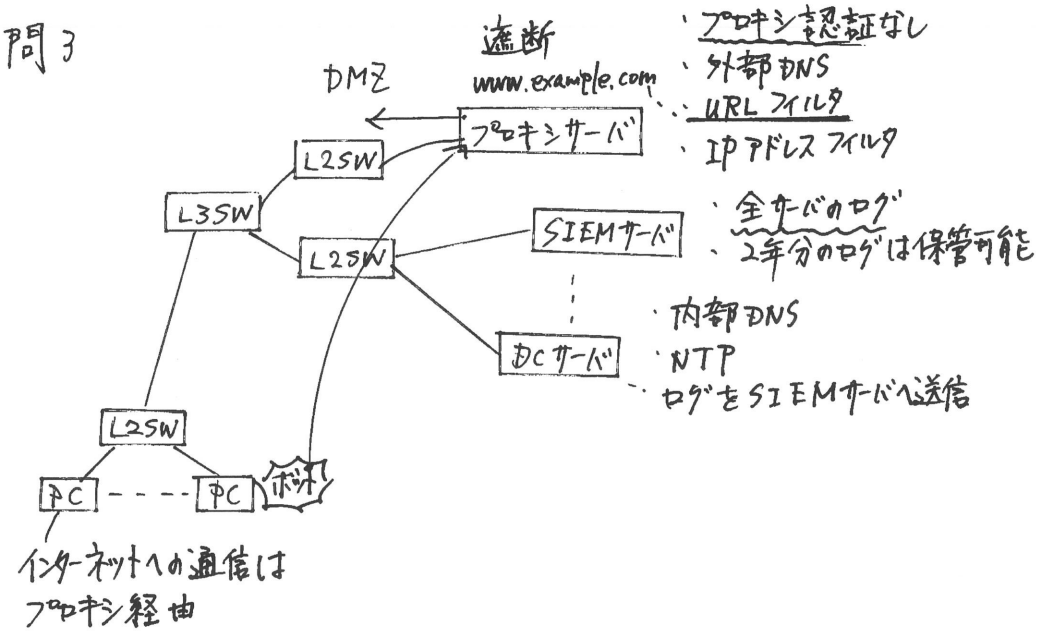


情報処理 講義録	コース・講義等	情報処理安全確保支援士	科目	公開模試解説 後編	回数	1

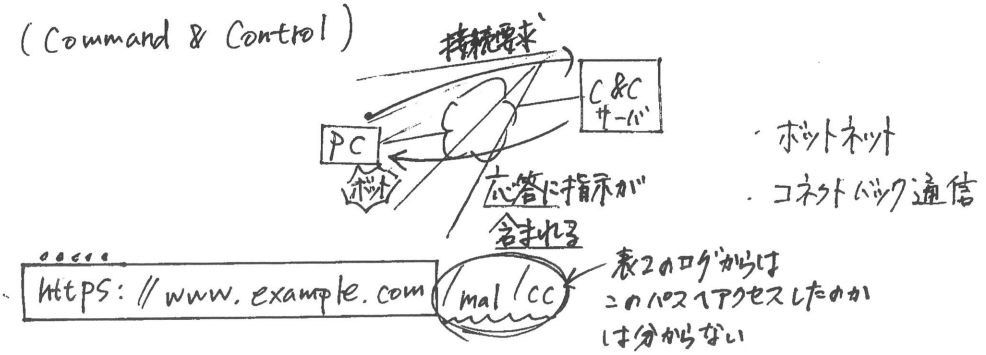
配布物	★テスト類：[ ]	講師	根岸 先生
	★その他の配布物1：[ ]		
	★その他の配布物2：[ ]		

黒板内容

PM問3



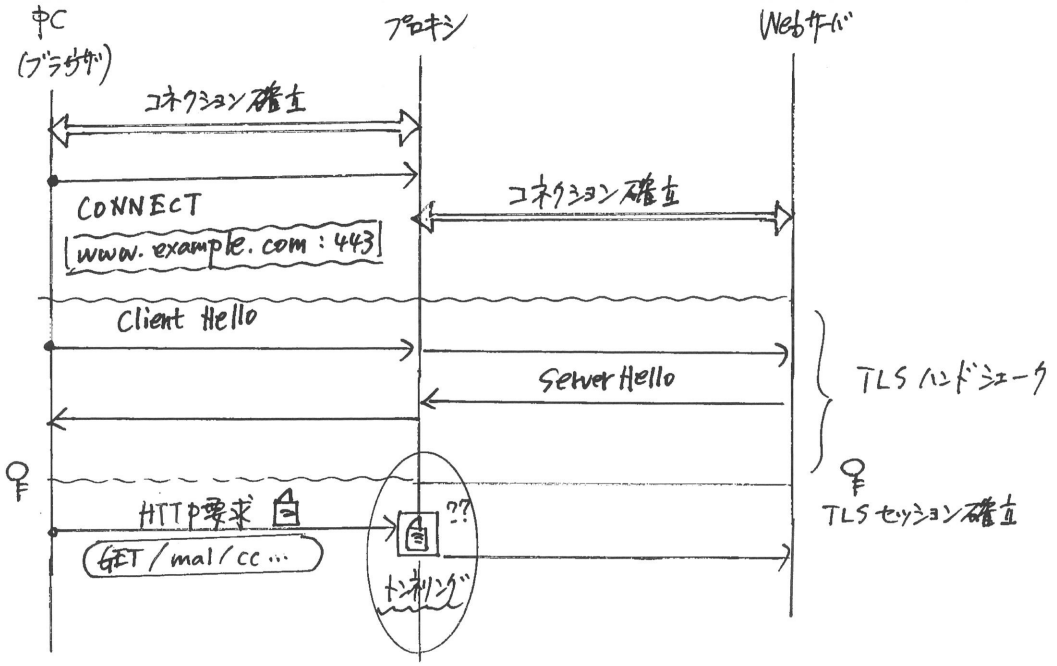
・…管理者アカウントによってログイン … 作業報告書 …
・各サーバとPCのシステムバックアップ … 3世代分 … 保存 …
・データバックアップ … 1週間分保存 …
・C&Cサーバ … ボットウイルスなどでの指令塔サーバ
(Command & Control)

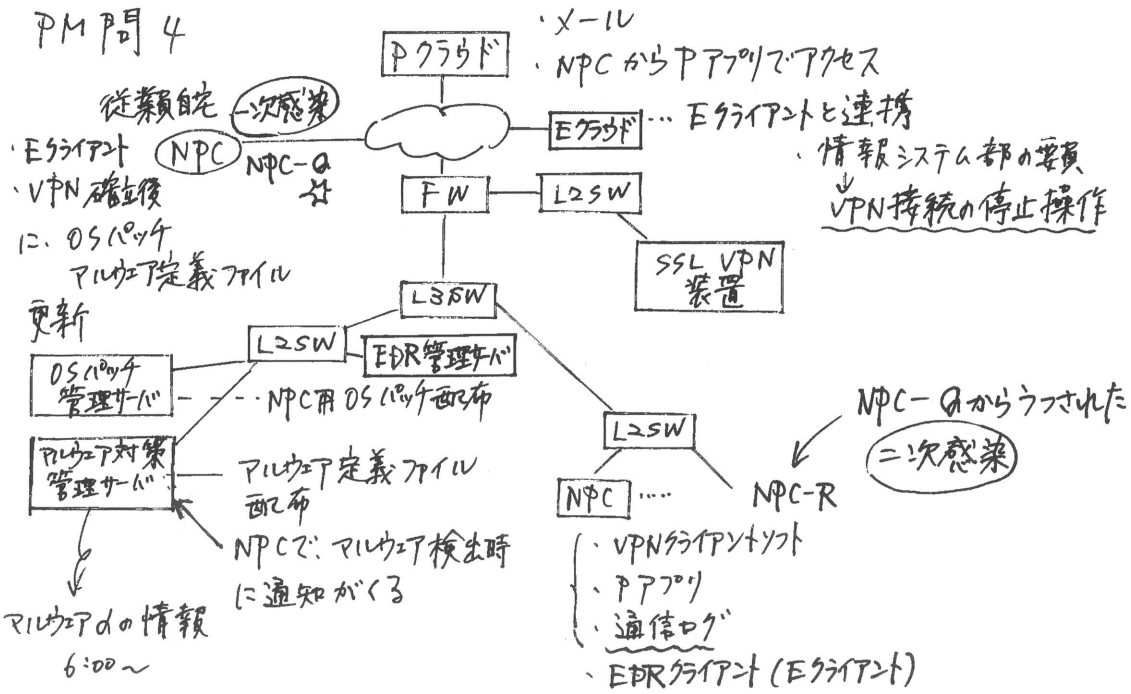


情報処理　講義録	コース・講義等	情報処理安全確保支援士	科目	公開模試解説 後編	回数	1

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





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

⑨ テレワーク用NPC

① NPC起動 ← 添付ファイル実行 → マルウェアに感染

② 手動でVPNクライアントを手動で起動 → VPNセッション確立

③ OSパッチ、マルウェア定義ファイル更新

・RPA … 新たなプロセスの生成 … 情報システム部への個々の報告は行われていない。

表2

#1：セキュリティインシデント発生時は
インシデント発生の当事者から
情報セキュリティ対策チームに報告する → インシデント発生の当事者の上長にも通知

・マルウェアα：C&Cサーバへの接続を試みる（私的）

・ゼロトラスト

マルウェア判定リスト

挙動不審な未知のプロセスを検出する … EDRクライアント（Eクライアント）

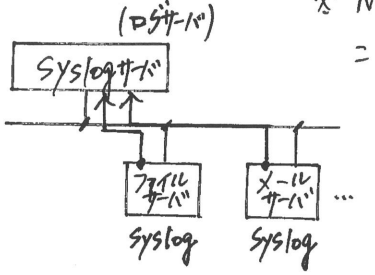
情報処理 講義録	コース・講義等	情報処理安全確保支援士	科目	公開模試解説 後編	回数	1

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

◎ RPA … 新たなプロセスの生成 … 情報システム部への個々の報告は行われていない。

・Syslog, Syslogサーバ



※ NTPで時刻同期しておくことが重要