

講義録レポート

講義録コード

04-59-1-301-02

講 座	情報処理安全確保支援士	科目①	模試編
目標年	2025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	7 枚
			補助ビジュアル 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 (49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			

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： []	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 シングルサインオンシステム

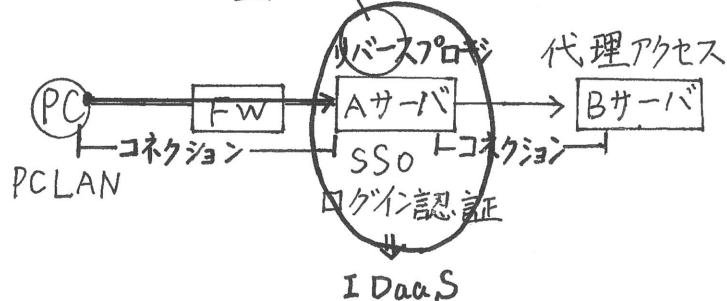
- ・業務Bシステム；Bサーバ
- ・業務Cシステム；Cサーバ
- ・業務Dシステム；Dサーバ

社内システムLAN

現状

※社員が
B、C、Dサーバに
直接アクセス
することはない

- ・業務用PC ⇒ 3システム用 URL がブックマークされている。
- ・Aサーバ；リバースプロキシ型SSOシステム



ディレクトリサーバ

- ・ディレクトリサービス；LDAP
- ・アカウント情報
- ・ホスト情報 など

情報共有サービス

- ・参照の頻度が多い
- ・追加・削除更新はあまり行わない

P.13 A社 部長 が……

表2・Bシステム用URL；部長用

表3

P.14 表4 認可機能

現状

表3：URL単位

SPの FQDN 単位で アクセスの可否 を判定する

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 : []		

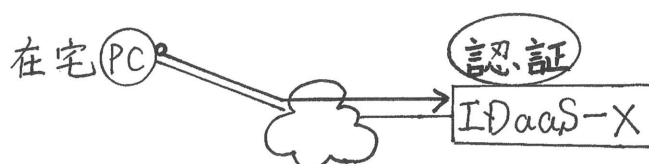
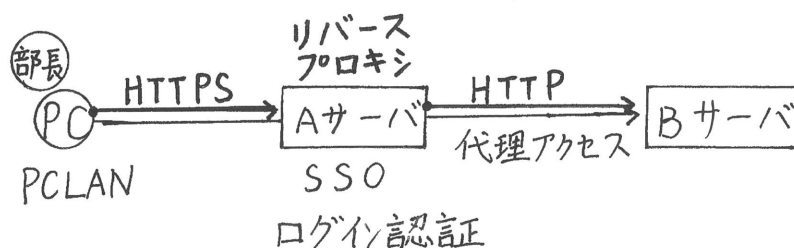
黒 板 内 容

PM 問 2 シングルサインオンシステム

- ・ 業務B システム ; Bサーバ
 - ・ 業務C システム ; Cサーバ
 - ・ 業務D システム ; Dサーバ
- 社内システム LAN

現状

※社員が
B,C,Dサーバに
直接アクセス
することはない



P.13 A社(部長)が……

表2・Bシステム用URL ; 部長用

表3

P.14 表4 認可機能

Aシステム

現状

表3: URL単位

SPのFQDN単位でアクセスの可否を判定する

情報処理 講義録

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

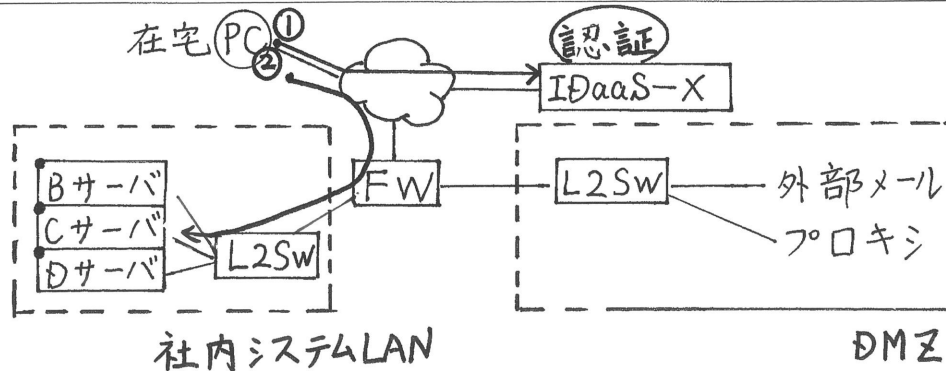
★ テ ス ト 類 : []
★ その他の配布物 1 : []
★ その他の配布物 2 : []

講
師

根岸

先生

黒 板 内 容

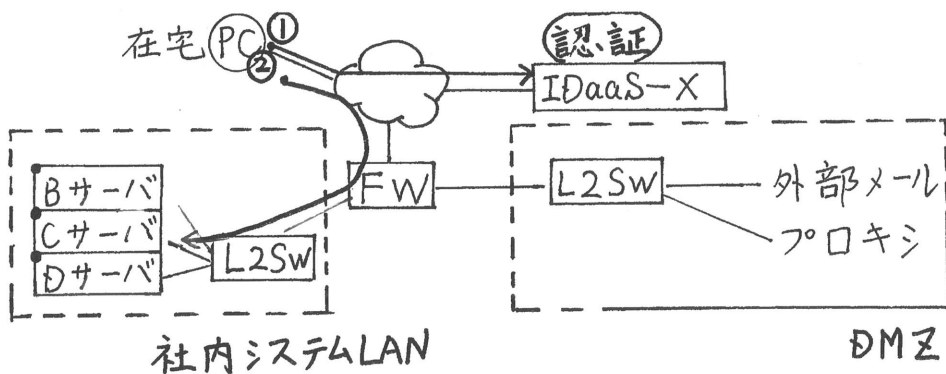


◎ 証明書のグレード

DV: ドメイン認証型... CN(SAN)のみ・ドメインの所有のみを証明する
OV: 組織認証型
EV: EV型

① コモンネーム; サーバ証明書の場合, サーバのFQDNを記載する

*
Webサーバ: www.a-sha.co.jp cn=*.a-sha.co.jp
web.a-sha.co.jp
gogocamp.a-sha.co.jp



◎ 証明書のグレード

DV: ドメイン認証型... CN(SAN)のみ・ドメインの所有のみを証明する
OV: 組織認証型
EV: EV型

① コモンネーム; サーバ証明書の場合, サーバのFQDNを記載する

*
Webサーバ: www.a-sha.co.jp cn=*.a-sha.co.jp
web.a-sha.co.jp
gogocamp.ak.ne.jp

サブジェクト代替名 → マルチドメイン証明書

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

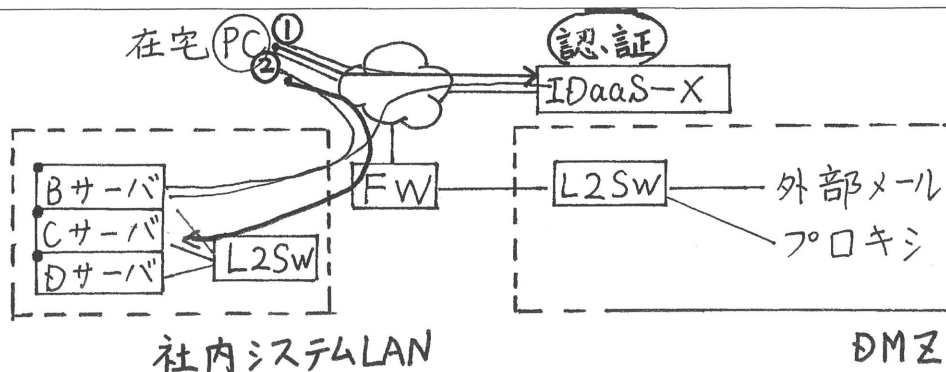
- ★ テ ス ト 類 : []
★ その他の配布物 1 : []
★ その他の配布物 2 : []

講師

根岸

先生

黒 板 内 容



◎ 証明書のグレード

- ①
~~DN~~: ドメイン認証型... CM(SAN)のみ、ドメインの所有のみを証明する
OV: 組織認証型... 会社名(O), 住所(都道府県, 市区町村)
x EV: EV型... 最も厳密な審査

コモンネーム; サーバ証明書の場合, サーバのFQDNを記載する

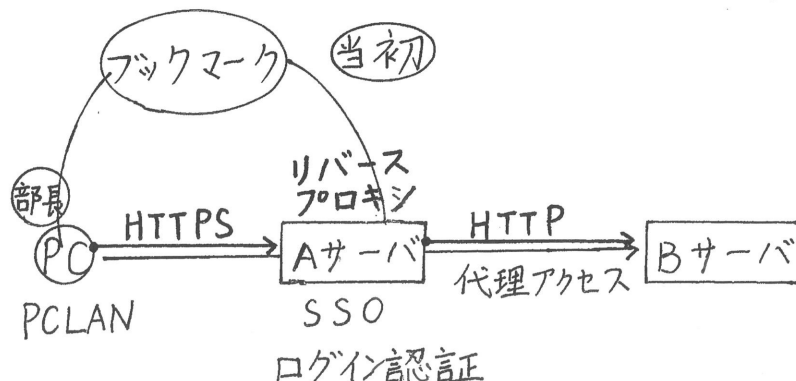
cn = (*). a-sha.co.jp

PM 問2 シングルサインオンシステム

- ・ 業務Bシステム ; Bサーバ
 - ・ 業務Cシステム ; Cサーバ
 - ・ 業務Dシステム ; Dサーバ
- 社内システムLAN

現状

※ 社員が
B, C, Dサーバに
直接アクセス
することはない



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

PM問3 情報セキュリティインシデントへの対応

- ・情報の入力・報告 → インターネットを介して行う ; 入力用PC
- ・集計・分析 → 社内ネットワークの 業務用PC ↔ 業務サーバ
- ・社員用PC ; インターネット・Web , メール送受信

表1

○ LANケーブルを抜いた

× 電源を切断してから → メモリ中にのみ存在していた・マルウェアの活動のこゝろ跡が消える、ファイルマルウェア
↓
メモリダンプ

× 緊急性はないと 独自に 判断し

・キーロガー ; 押したキーを記録して、外部へ記録を送出する
スパイウェア

・オートコンプリート機能

・二要素認証

— 知識

— 生体情報

— 所有物

第一パスワード

第二パスワード

→ 二段階認証

— 他人受入率: FAR

— 本人拒否率: FRR

デジタル署名

① エンティティ認証 ; 本人確認

・メッセージ認証 ; 改ざん有無の検証

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

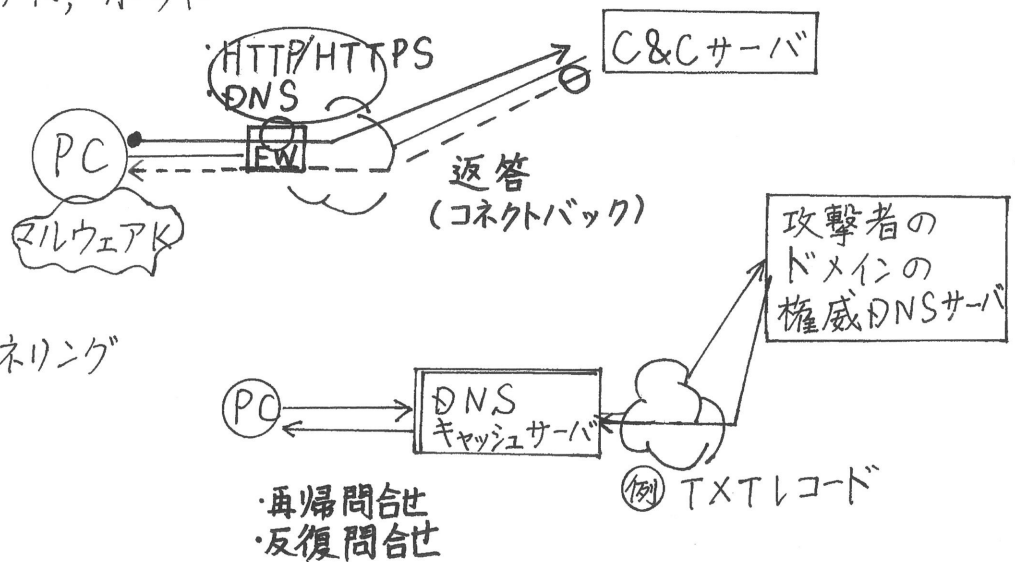
先生

黒 板 内 容

PM 問 3 情報セキュリティインシデントへの対応

- ・耐タンパ 性
- ・マルウェアK; ボット

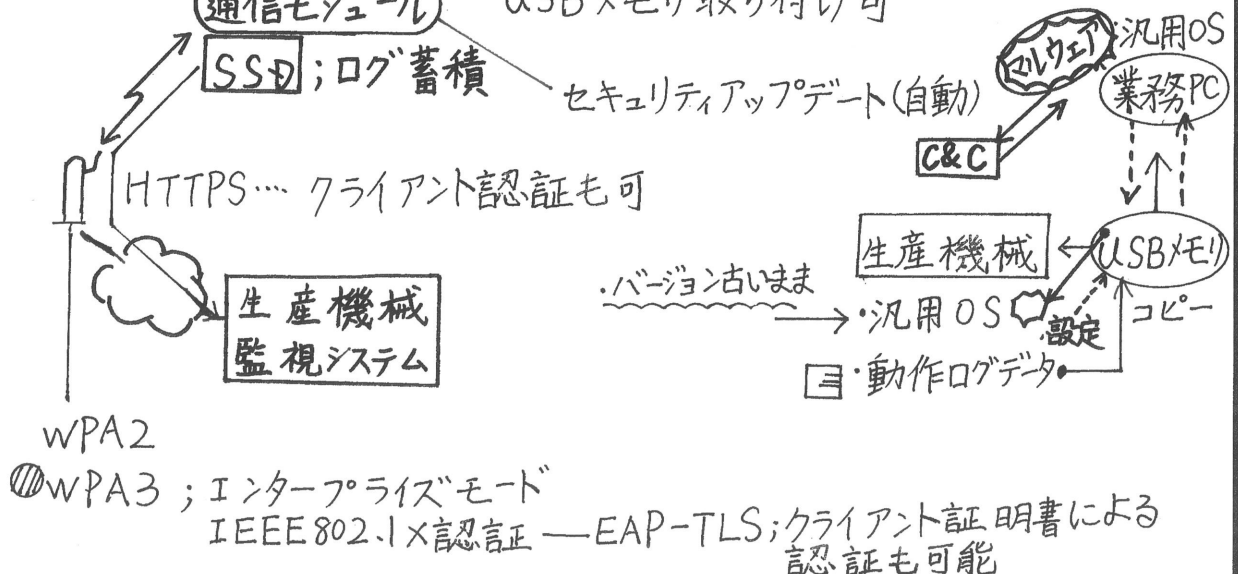
FWを通り抜けしやすいような
プロトコルを使う



- ・DNSトンネリング

PM 問 4

- ・工場の生産機械 → 社内ネットワークに接続されていない
通信モジュール USBメモリ取り付け可



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
標的型攻撃 ・APT ; <u>気付かれない様に</u>、長期間にわたって攻撃を続ける ・標的組織に特化した攻撃 → <u>カスタマイズしたマルウェア</u> ↓ <u>水飲み場型攻撃</u> など ドライブ・バイ・ダウンロード