講義録レポート

講義録コード　04-69-1-301-02

講　座	情報処理安全確保支援士	科目①	模試編
目標年	2026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/科目A-1試験免除） 上級コース	回　数	1　回

講師名	根岸 良征　講師	内訳	板書枚数	8　枚
			補助ﾚｼﾞｭﾒ枚数	0　枚
			その他	0　枚

講義構成	解説1（86分）→ 解説2（37分）→ 解説3（38分）→ 解説4（10分）
使用教材	公開模試 科目B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	

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

科目B 問2

- 認証．SSO
- 無線LANアクセスポイントのセキュリティ
- クラウド環境へのセキュリティ対策

科目B 問2

- 会社のPCを勝手に持ち出して紛失
- 一部の従業員 → スマホ，それ以外 → 携帯TEL（通話，SMSのみ）

〔システム環境〕

- 社内LAN → プロキシサーバ → インターネット（不審な通信を検出したら自動的に遮断）
- プロキシ．FW．メール → 毎日1回ログ管理サーバにログを集約．VPN通信
  毎月1回分析，1年分のログを保管
- 端末 ←HTTPS→ 社内LANのサーバ
  サーバ証明書：プライベート証明書 ← CAサーバ（サーバLAN）で発行する
- 検疫LAN（検疫ネットワーク）
- 端末FWは認証も行う
  → 接続先の指定．IPアドレス／FQDN
  ・FW：VPN機能：~~利用せず~~ 利用
  → 社内LANのサーバとの通信
  クラウドサービス利用時は使わない

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	

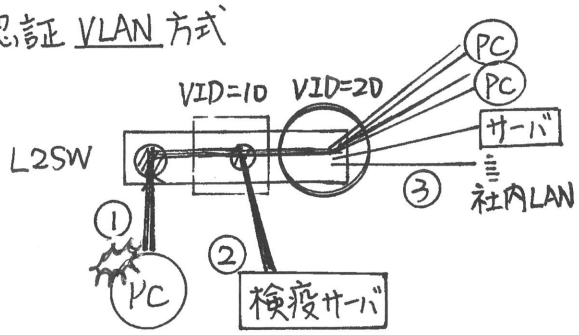
配布物	★テスト類：[ ]	講師	根岸 先生
	★その他の配布物1：[ ]		
	★その他の配布物2：[ ]		

黒板内容

⑥ 検疫ネットワーク

機能：・隔離 …社内LANと通信できないエリアに隔離する
・検査 …マルウェア検査、セキュリティパッチ、アプリ/OSのバージョンなどを検査
・治療 …マルウェア駆除、セキュリティパッチ、最新バージョンをインストール
許可されていないアプリをアンインストールする など

認証VLAN方式



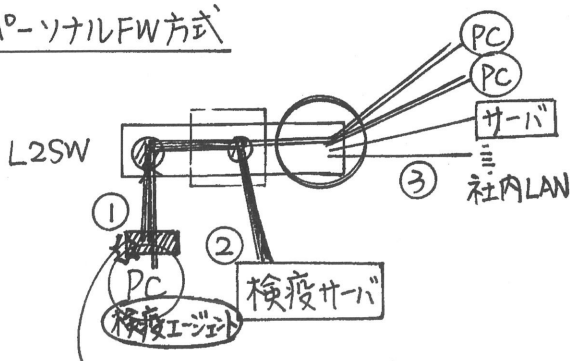
① IEEE 802.1x認証
・RADIUSサーバ
・EAP ⟶ PEAP、EAP-TLS
② 検疫エリア
③ 社内LAN

① 802.1x認証前：どこも通信不能
② 802.1x認証完了：検疫エリアに隔離性 → VID=10
③ 検疫完了：社内LANエリアに参加 → VID=20

⑥ 検疫ネットワーク

機能：・隔離 …社内LANと通信できないエリアに隔離する
・検査 …マルウェア検査、セキュリティパッチ、アプリ/OSのバージョンなどを検査
・治療 …マルウェア駆除、セキュリティパッチ、最新バージョンをインストール
許可されていないアプリをアンインストールする など

パーソナルFW方式



① IEEE 802.1x認証
・RADIUSサーバ
・EAP ⟶ PEAP、EAP-TLS
② 検疫エリア
③ 社内LAN

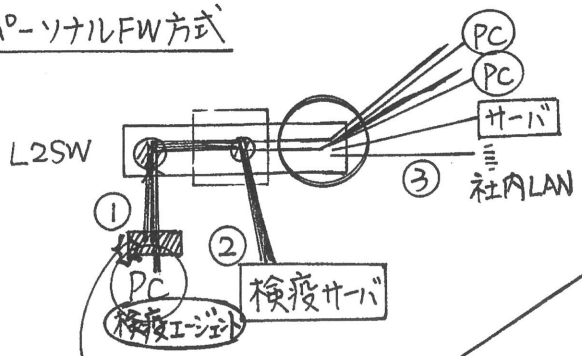
PCのパーソナルFW機能 → 当初は検疫サーバとだけ通信可能
↘ 検疫完了したら、社内LANと通信可能

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	

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

パーソナルFW方式



PCのパーソナルFW機能 → 当初は検疫サーバとだけ通信可能
→ 検疫完了したら、社内LANと通信可能

・ステートフルパケットインスペクション
・動的パケットフィルタリング

端末FW
認証も可能

表1

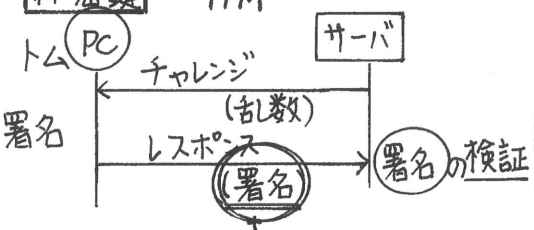
PC → RADIUSサーバ；DNS
＝
認証サーバ

指紋リーダー
クライアント証明書
C-Certificate
S-

リモートデスクトップ(RDP)で接続
10.10.1.10 からの接続のみok
ヘルプデスク端末

・認証 → 指紋認証
クライアント証明書による認証

・クライアント証明書
・秘密鍵 …… TPM



設問1(2) 公開鍵証明書
(クライアント証明書)

・指紋認証がダメ 内線 でサポート窓口へ → 代替パスワードを口頭で伝える
→ SMSで伝える

・クラウドサービス → 従業員はクラウドサービスごとに個別のアカウント
→ 接続元IPアドレス制限 (~~D社からのみ~~) クライアント証明書
サーバのIPアドレスは変わることもある
アクセスログの取得はしていない

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	

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

表1

PC → RADIUSサーバ；DNS ⟷ 認証サーバ

指紋リーダー
クライアント証明書

リモートデスクトップ(RDP)で接続
10.10.1.10 からの接続のみOK
ヘルプデスク端末

認証前・RADIUS
・DNS
追加 FWのVPNサーバ
HTTP/HTTPS全て …クラウドサービス用
SMTPS/POPS …メールの送受信
・RDPで接続受け付け

・認証 → 指紋認証
クライアント証明書による認証
} 設問1(2)

・指紋認証がダメ ~~内線~~ 外線も でサポート窓口へ → 代替パスワードを ~~口頭~~ で伝える
↓
SMSで伝える

・クラウドサービス → ~~従業員はクラウドサービスごとに個別のアカウント~~ ⇒ SSO(SAML, OpenIDconnect)
接続元IPアドレス制限 ~~(D社からのみ)~~
サーバのIPアドレスは変わることもある
アクセスログの取得はしていない

認証
認可
属性
} アサーション

ToTP：時刻ベース OTP

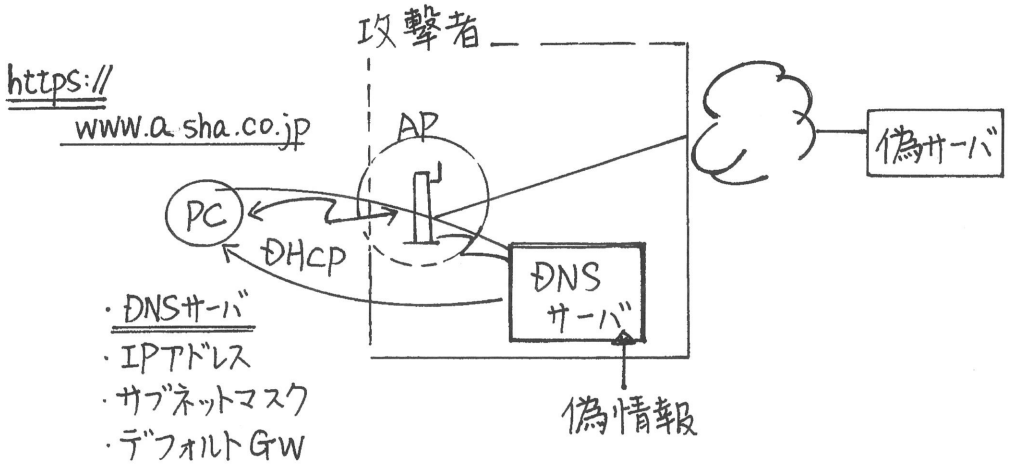
時刻　秘密の番号
↓
ハッシュ値

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	

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

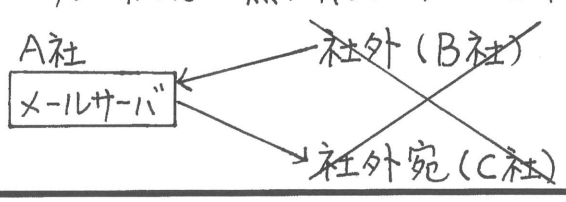
科目B 問2



科目B 問3

・オープンリレー対策／第三者中継
・SPF：IPアドレスを利用
・DKIM：署名を利用
} 送信ドメイン認証
・DMARC：SPF，DKIM 失敗時のメールの扱いを伝える
rua：集計レポートの送り先メールアドレスを伝える

メールリレー：メールを中継する
オープンリレー状態：無制限にメールを中継する状態



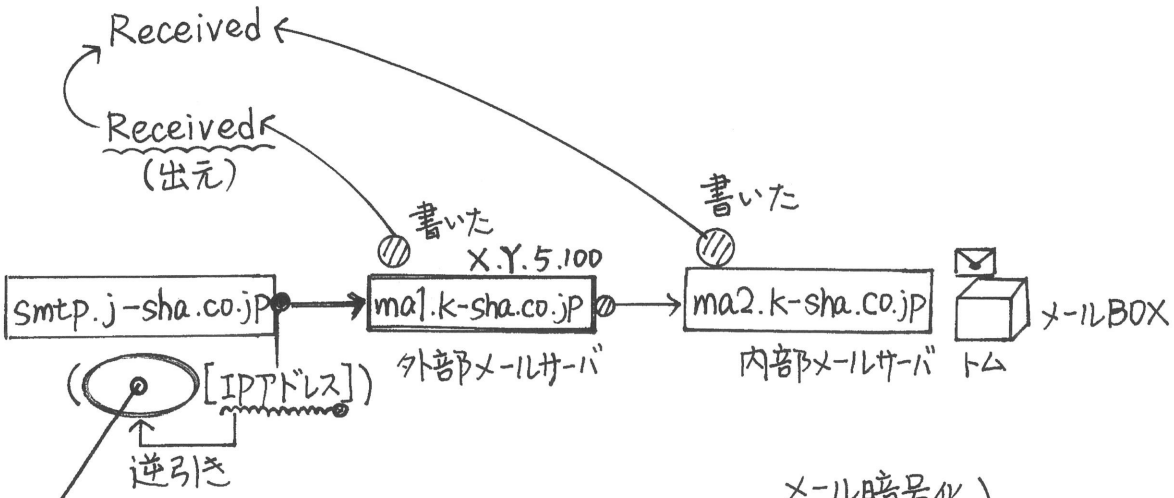
rua
ruf

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	

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

メールヘッダ



メール暗号化
メール署名
) S/MIME

科目B 問3

・K社DNSサーバ：SPFレコード K社メールを配送するサーバのIPアドレスを記載する

図3

SPFレコード

K-sha.co.jp. IN TXT "V=spf1 +ip4:X.Y.5.100 -all"

・K社DNSサーバ：DKIMレコード K社のメールを配送するサーバの公開鍵

p=公開鍵 ○Selector1._domainkey.k-sha.co.jp. …… P=公開鍵1 …… 令和1

○Selector2._domainkey.k-sha.co.jp …… P=公開鍵2 … 令和2

DKIM利用時のメールヘッダがDKIM-Signature

S=セレクタ名、Selector1

h=署名対象とするメールヘッダの項目名

d=ドメイン名

(本試験) Ro1.秋.PM1.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	

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

A社　　攻撃者が取得したドメイン

a-sha.co.jp　　a-sha.com

asha.com

↑

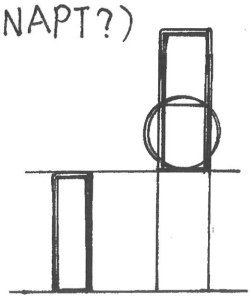
A社のドメインに似たドメイン

科目B 問4

・クラウドサービス：メール.予定表.Web会議　：送信元IPアドレスでログイン制限

・本社 ↔ 拠点：IPsec VPN　　Y社本社のFWのIPアドレスのみ

・インターネット接続は全て本社経由　　（NAPT?）



・パスワードリスト攻撃

⊙Y社のノートPC：機内モードスイッチ　ON…電波出さない　OFF…電波出す

⊙二重窃盗型.ダブルエクストーション

・サプライチェーン攻撃

・CSIRT

⊙暗号化して.使えなくする

・ファイルを（全て）盗みとる

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	

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

〔現存する脆弱性の洗い出し〕

・アタックサーフェス

・CSPM

〔防御体制の整備〕

・サイバーハイジーン

〔ランサムウェアの活動の検出〕

・EDR …プロセスの動作
通信状態　を監視，ロギング，不審なプロセスを強制終了
マルウェア

・SIEM

・ディレクトリサーバ：ディレクトリサービス：（簡易的な）情報共有サービス
（LDAP）　◎ユーザアカウント　・ホスト情報（hosts ファイル）　など
・メーラーのアドレス帳

〔ランサムウェア検出後の対応〕

〔バックアップ取得体制の検討〕

・3-2-1ルール

バックアップは3つ

異なる2つの媒体に保管

オフサイト．遠隔地に保管

被災したことを踏まえて