

講義録レポート

講義録コード

04-29-1-301-01

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 前編
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 サイズ (B5)
		補助ビジュアル枚数	0 枚	
		その他	0 枚	

講義構成	解説1 (59分) → 解説2 (80分) → 解説3 (39分)		
使用教材	公開模試 午前Ⅱ問題		
	公開模試 午後Ⅰ問題		
	公開模試 解答・解説		
配布教材			
備考	※午前Ⅰの解説講義はありません。午前Ⅰ解答解説冊子でご確認ください。		

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。

T A C 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 前 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

AMⅡ

Q1 ~ 17 セキュリティ分野 } 専門分野

Q18, 19, 20 ネットワーク分野 }

Q21 ~ 25 その他 ... 応用情報レベル

不正なデータ

Q1 OS コマンド インジェクション
SQL インジェクション
HTTP ヘッダ インジェクション

みな形
ユーザーからの入力
を補って、全体を
完成させる

(定番) Smurf

Q2 SAML (必須)

- ・ SSO (シングル・サイン・オン)
- ・ 異なるサイト (ドメイン) 間で SSO を実現する
- ・ XML の形式で: 認証 情報などをやりとりする
アサクション
- ・ IdP, SP
IDプロバイダ, サービスプロバイダ
- ・ ケルバロス認証 KDC, チケット, チケット交付チケット (TGT)
- ・ OAuth
- ・ OpenID

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 前 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： []		

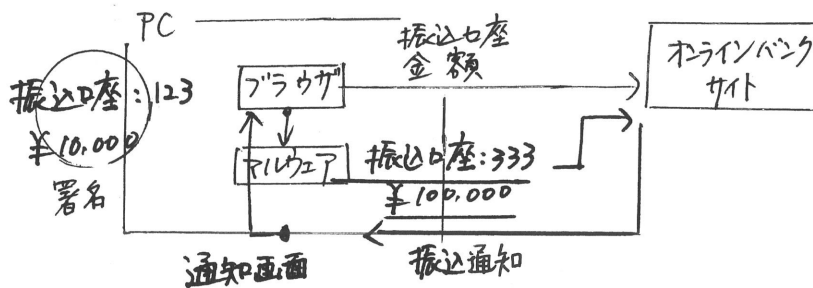
黒板内容

Q3 サイドチャネル攻撃

Q4 サプライチェーン攻撃

- ・ BEC : ビジネスメール詐欺
- ・ ランサムウェア

Q5 MITB → トランザクション署名



Q6

- ・ CVE
- ・ CVSS
- ・ CWE

Q7 J-CSIP

- ・ CRYPTREC
- ・ CSIRT
- ・ JPCERT/CC
- ・ NISC

Q8 CRYPTREC 暗号リスト

SHA2 ~~SHA256~~ SHA512

SHA3 ~~SHA3-256~~ SHA3-512

ハッシュ関数 ハッシュ値のビット数

Q9 ブロックチェーン

Q10 CASB

CDLP

OSIEM

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 前 編	回数	1
----------	---------	-----------------	----	---------------	----	---

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

黒板内容

- Q11 デジタルフォレンジックス 監理者
- Q12 エクスプロイトコード 権限昇格 (権限を奪取)
ゼロデイ攻撃
- Q13 クッキー (Cookie) 必須
↑ セッションクッキー, Secure 属性
- Q14 FW 外向き 25番ポート宛て通信はブロック
- Q15 DNS SEC 必須
DNS キャッシュポイズニング対策
- Q16 SMTP-AUTH
DKIM } 送信ドメイン認証 必須
SPF }
- Q17 OP25B
-

PMI 問1

- 問題 本文の事例の状況を正しく把握できるか?
- 解答 ← 本文を読んだ証拠を含む解答とすること!

- 本文中の用語を使っている
- 本文の表現にならって表現している
- 図、表中の機器の名称を明確に示している

(30~40字で述べよ) 主語を書く!

解答を書く

設問文をもう一度読む
もう一度、解答を読む] 文章の表現をうまくする

空欄は前後の表現に注目!

文脈から専門用語を埋める

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 前
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： []

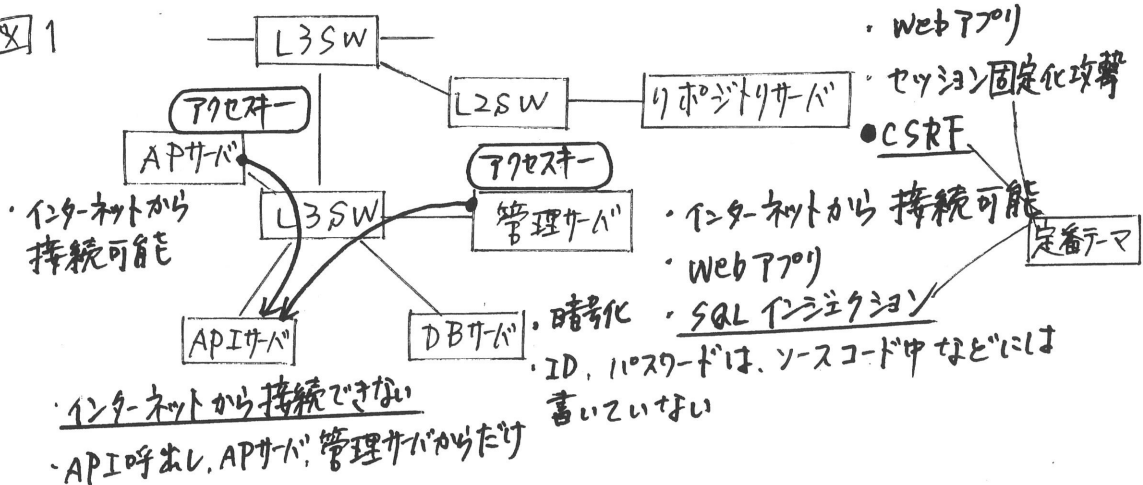
講
師

根岸

先生

黒板 内 容

図1

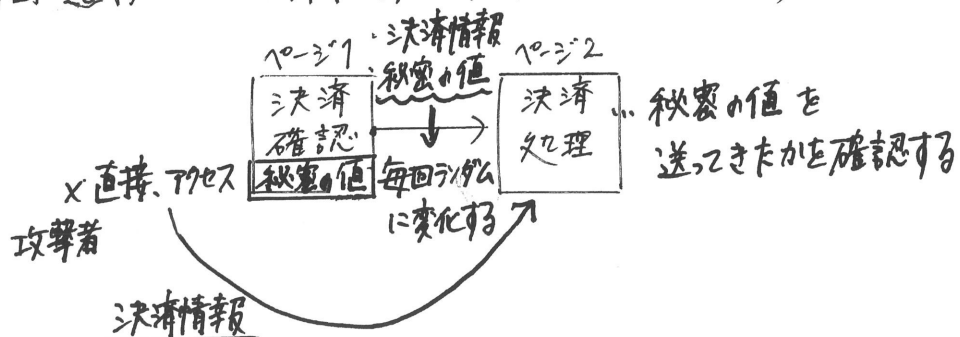


・リポジトリサーバ

ログイン前 ... セッションIDを付与 ...
X ログイン後 ... ユーザ情報をひもつける ...) X セッション固定化攻撃

にセッションIDはつけ直す

画面遷移 → CSRF (クロスサイトリクエストフォージェリ)?



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 前
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

図2

SQL文のひな形

\$sql = "SELECT ... WHERE id = ' " . id . " '

↓
組み立てた結果の SELECT 文

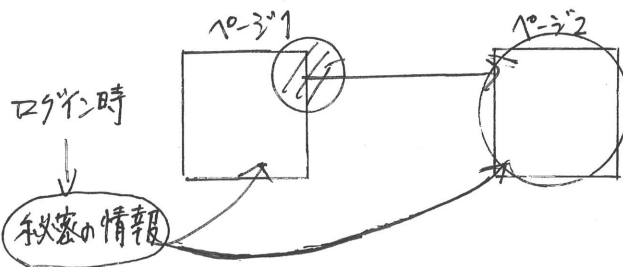
SELECT ... WHERE id = ' /// ' AND password = ' /// ' ;

↑
ユーザーが入力した ID

ユーザーの入力をそのまま
利用して SQL 文を組み
立ててはいけない

- ・水飲み場型攻撃
- ・ドライブ・バイ・ダウンロード

↓
バインド機構を利用
・フリースホルダ
・ポリバートステートメント



HTTPヘッダ

Referer ← ・Referer をヘッダに
含めるのは任意
・(攻撃者)

Referer の値を 不正な
値に改変する

図2

SELECT * FROM users

WHERE id = ' id ' AND

password = ' ' OR 'abcdool' = 'abcdoollo'
OR 'password' = 'password'

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 前
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2

バックアップ機能/復旧機能

・ 予約管理システム、予約管理パッケージを導入

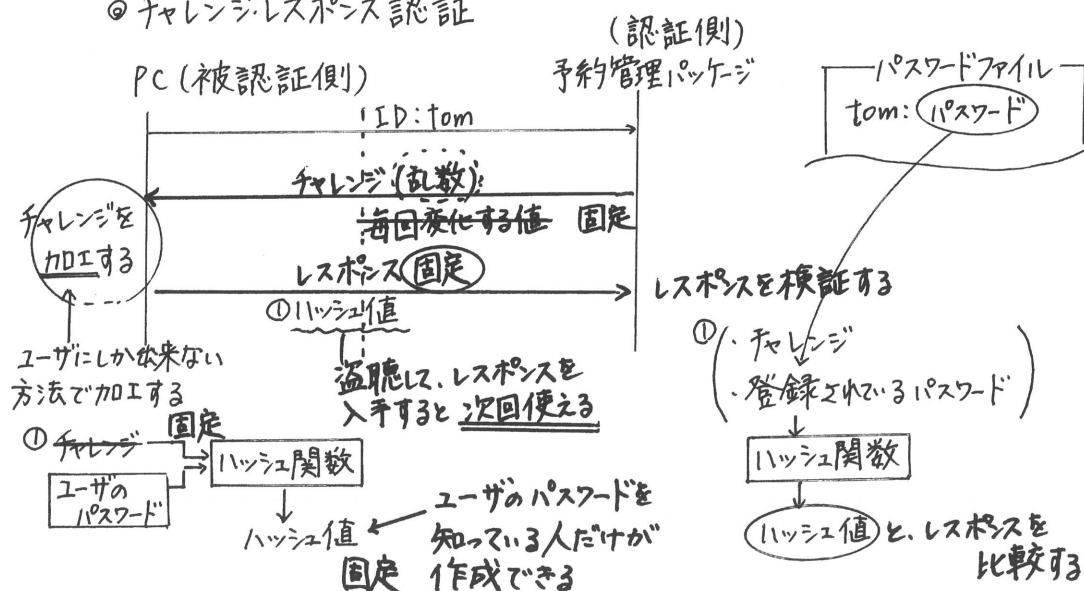
[他社でのセキュリティ事故事例]

・ ----- データ復旧を断念するという事態 -----

・ DBサーバ：来店予約データ ← システム管理者は参照してはならない

↓
特権アカウントではアクセスできてしまう↓
不用意に特権アカウントを利用しない・ アクセスログ... 記録されない設定

◎ チャレンジレスポンス認証



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 目	公開模試解説 前 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

