

講義録レポート

講義録コード

04-39-2-301-01

講 座	情報処理安全確保支援士	科目①	模試編
目標年	2023年秋期(下期)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

講師名	根岸 良征 講師	内 訳	板書 枚数	9 枚
			補助ビジュアル 枚数	0 枚
			その他	0 枚

講義構成	解説1 (81分) → 解説2 (67分)		
使用教材	公開模試 午前Ⅱ問題		
	公開模試 午後問題		
	公開模試 解答・解説		
配付 教材・資料			
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。

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 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

支援士模試解説

AMⅡ

- ・ セキュリティ 問 1 ~ 17
 - ・ ネットワーク 問 18, 19, 20
 - ・ 開発 問 22, 23
 - ・ ITサービス
マネジメント 問 24
 - ・ システム監査 問 25
- } 専門分野
DB 問 21

＊ 15 問 正 解 で 合 格 点

問 2 OCSP ステージング

- ・ OCSP: オンラインでサーバに証明書の失効情報を問い合わせる
- ・ CRL: 失効リスト OCSPレスポンス

有効期間内の証明書について、失効の申請が出ていないかを調べる。

- ・ 秘密鍵がバレた。/ 秘密鍵を紛失した。
- ・ 秘密鍵を使えなくなった。など

公開鍵証明書を失効させる。

◎ HTTPS, (TLS) — サーバ認証が必須。

サーバ証明書で、サーバ認証を行う

- ・ サーバに署名させて、…サーバは、サーバの秘密鍵で署名
クライアント側で署名を…サーバの公開鍵で署名を検証
検証する。

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 前
編

回
数

1

配布物

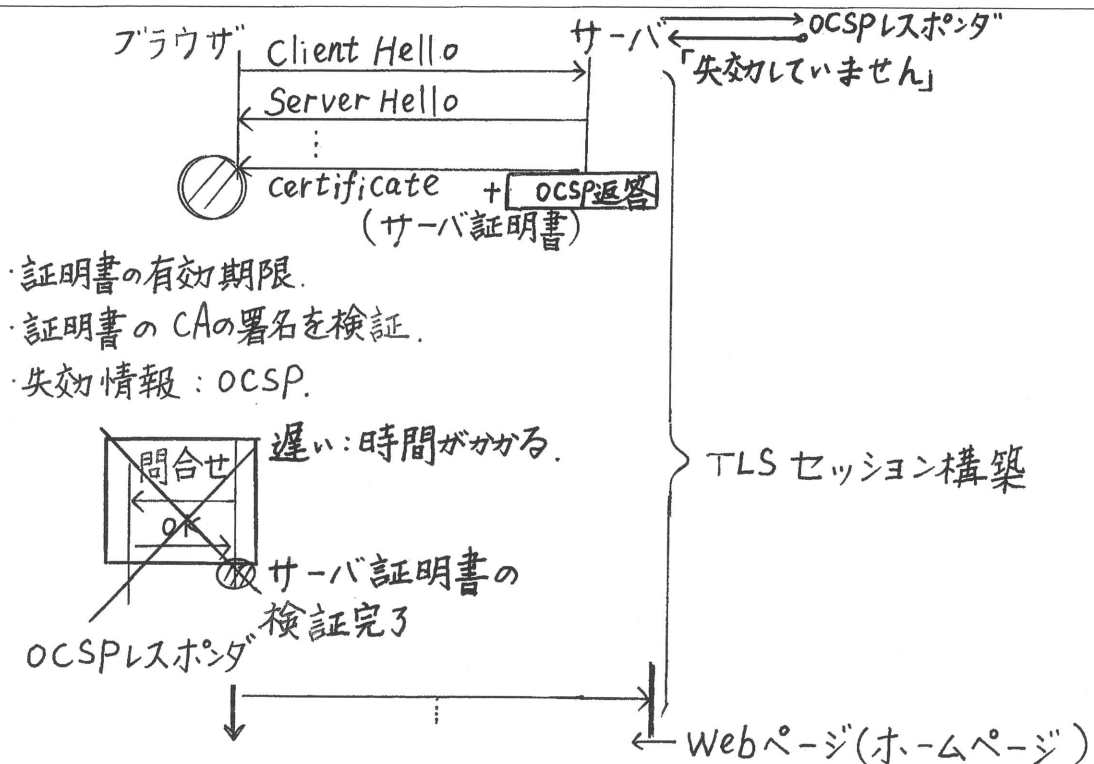
- ★ テ ス ト 類 : []
★ その他の配布物 1 : []
★ その他の配布物 2 : []

講
師

根岸

先生

黒 板 内 容



問3 パスワードへの攻撃.

ア. パスワードリスト攻撃: 他のサイトから流出したID/パスワードをそのまま利用して、ログインを試みる

イ. レインボーテーブル攻撃: パスワードのハッシュ値からパスワードを推測する.

ウ. 辞書攻撃

エ. リバースブルートフォース攻撃: パスワード固定、IDを変化させる

・ブルートフォース攻撃: 総当たり、ID → 様々なパスワードを試す.
(全通り)

・アカウントロックアウト

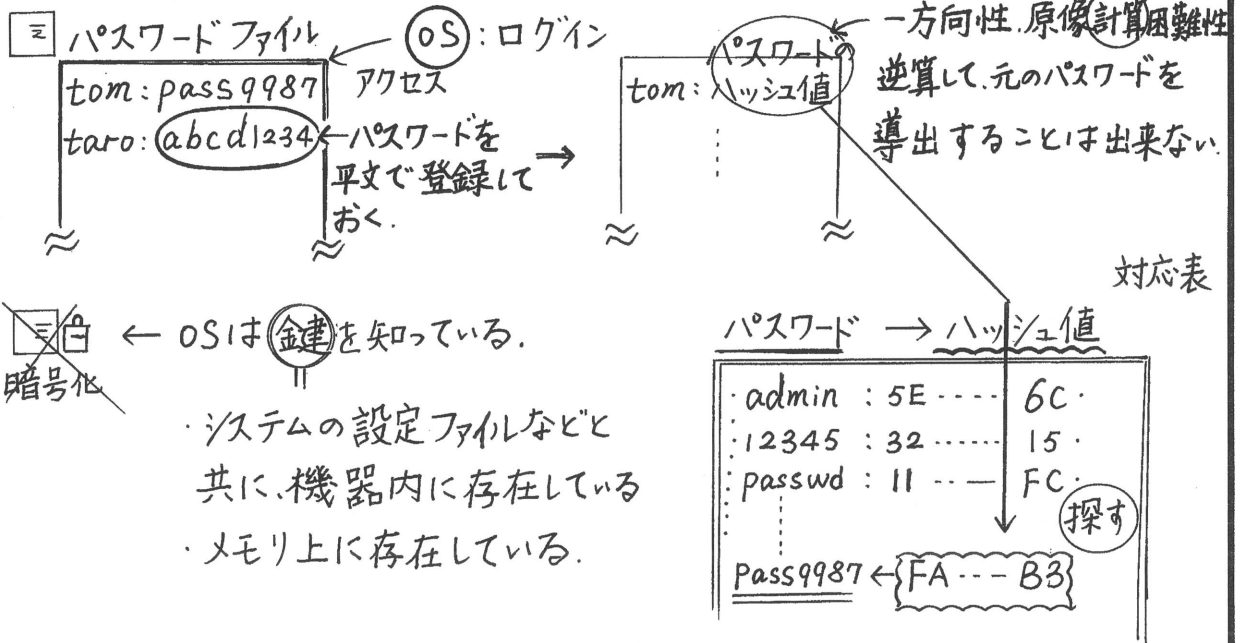
・パスワードスプレー攻撃.

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
----------	---------	-------------	----	-----------	----	---

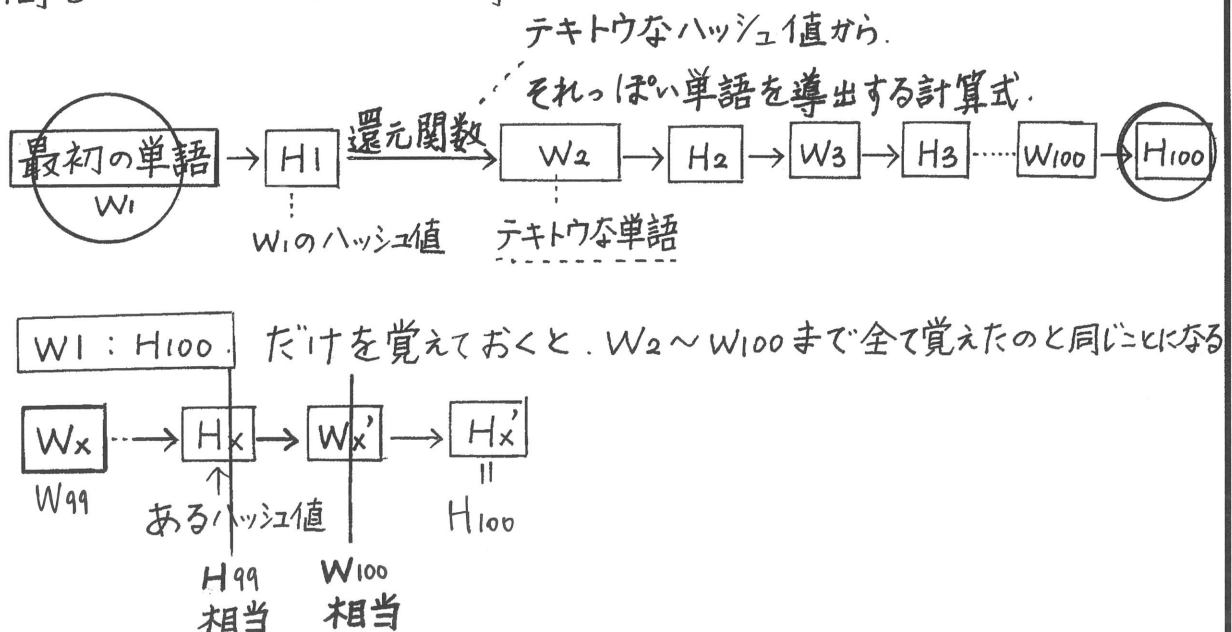
配布物	★テスト類： []	講師	根岸 先生
	★その他の配布物1： []		
	★その他の配布物2： []		

黒板内容

◎サーバでのパスワード管理



問3 パスワードへの攻撃



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

問 4 FIDO . Webauthn

ア. トランザクション署名 : MITB (Man In The Browser)

中間者攻撃 : ブラウザと利用者間に立って
やりとりしているデータを改ざんしたりする

対策

イ. 3D セキュア

エ. リスクベース認証 : 通常とは異なる環境からアクセスすると
追加で認証を行う。

問 6 SAML

シングルサインオン

・ 異なるドメイン間での SSO を実現する

・ IdP, SP, アサーション

↑
認証する
所

↙
サービス
を提供する
サイト

↑
認証情報
(XML形式)

・ 言証アサーション

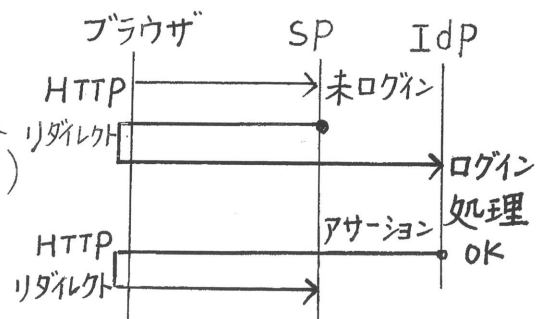
・ 属性アサーション

・ 認可アサーション

・ OAuth

・ Open ID

オンラインショップ



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

問 8 XSS

I: 反射型 XSS

II: 格納型 XSS

III: DOMベースXSS ... 悪意のあるスクリプトが クライアント(Webブラウザ)側では込まれる

↓
(Javascript)

↓
悪意のあるスクリプトを
利用者に実行させる。

問 9.10

- ・ J-CSIP : サイバー情報共有イニシアチブ
- ・ J-CRAT : サイバーレスキュー隊
- ・ JPCERT/cc
- ・ CRYPTREC
- ・ JVN
- ・ NISC : 内閣サイバーセキュリティセンター
- ・ CSIRT

問 13

- ・ HSTS

問 14

- ・ CAAレコード : ドメインの証明書を発行するCAを指定する
- ・ SOAレコード
- ・ TXTレコード
- ・ MXレコード
- ・ NSレコード
- ・ A, AAAAレコード
- ・ PTRレコード

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

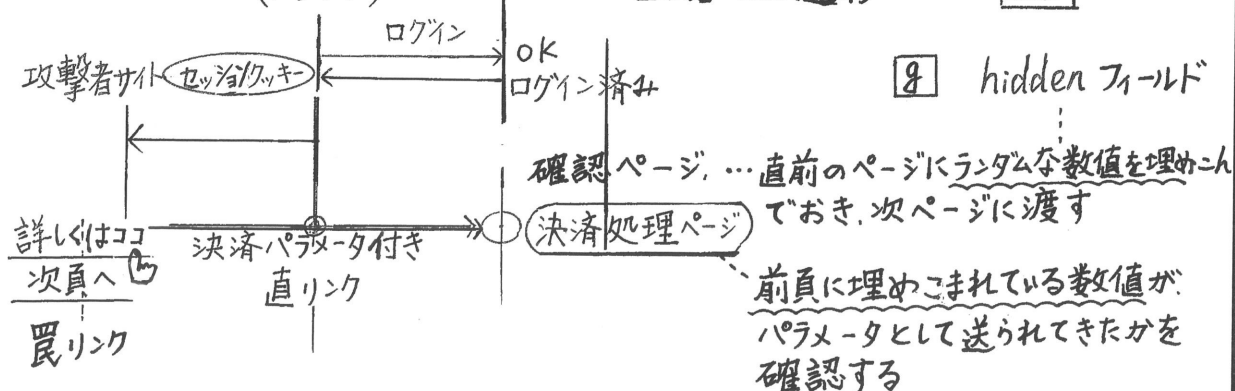
PM 問1 目標解答時間: 70分

設問2 [Webサイトの脆弱性とその対策]について...

PM 問1 目標解答時間: 70分

[Webサイトの脆弱性とその対策]

CSRF
クロスサイト
リクエストフォージェリ
オンラインショップ
利用者
(ブラウザ)



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
----------	---------	-------------	----	-----------	----	---

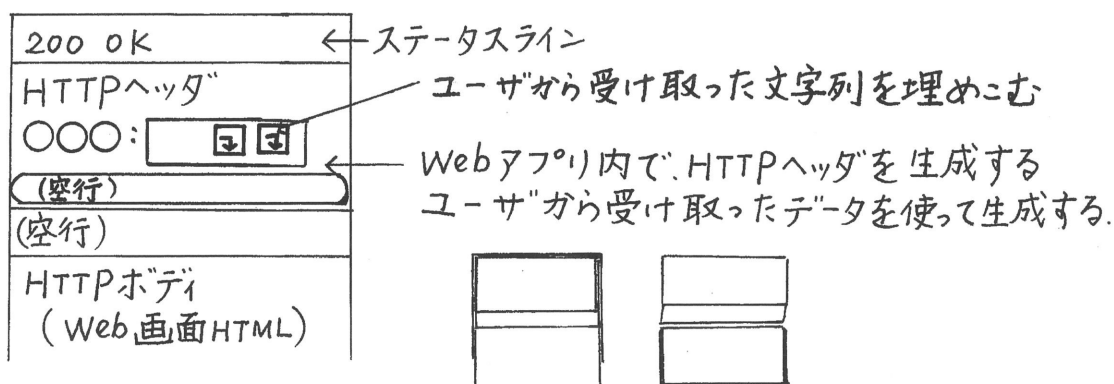
配布物	★ テ ス ト 類 : [] ★ その他の配布物 1 : [] ★ その他の配布物 2 : []	講師	根岸 先生
-----	---	----	-------

黒 板 内 容

HTTPヘッダインジェクション

HTTPヘッダ、HTTPボディ

◎ HTTP応答



◎ クッキーの属性

- ・ Secure属性: HTTPS通信の時だけ、当該クッキーを送る
- ・ http only属性: Java Scriptでクッキーを読み出せなくする

HTTP応答: Set-Cookie: サーバ → ブラウザ クッキーを設定

HTTP要求: Cookie: ブラウザ → サーバ クッキーを送信

※ クッキーを設定したドメインと
異なるドメインには、クッキーは送信
しない。

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 前編	回数	1
----------	---------	-------------	----	-----------	----	---

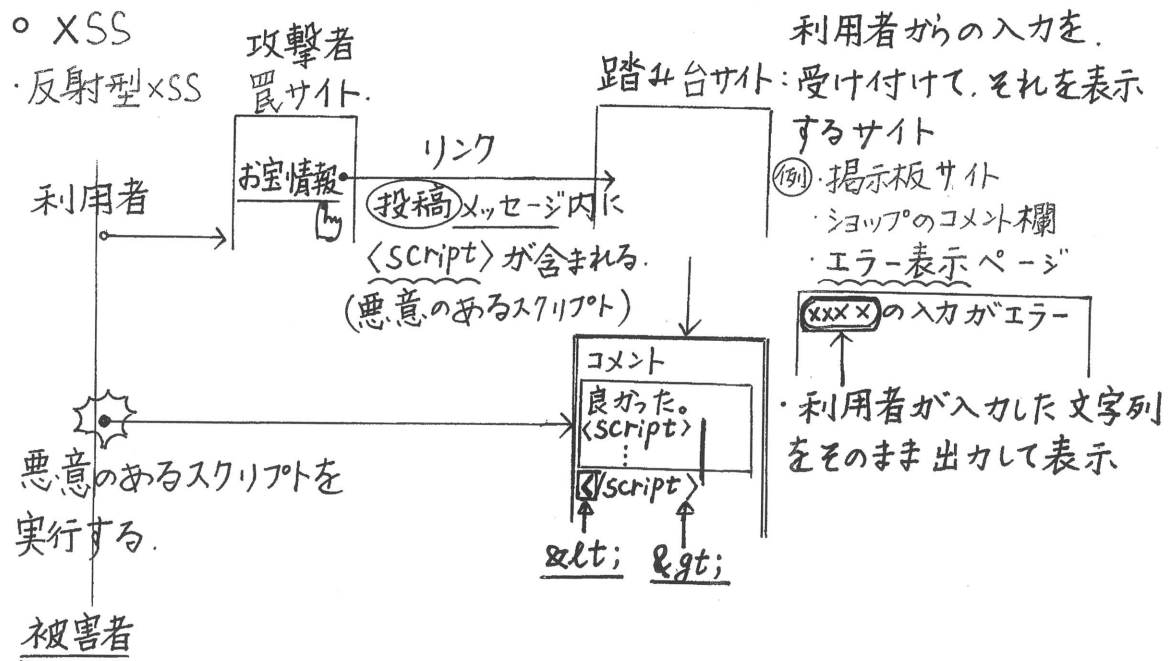
配布物	★テスト類： [] ★その他の配布物1： [] ★その他の配布物2： []	講師	根岸 先生
-----	--	----	-------

黒板内容

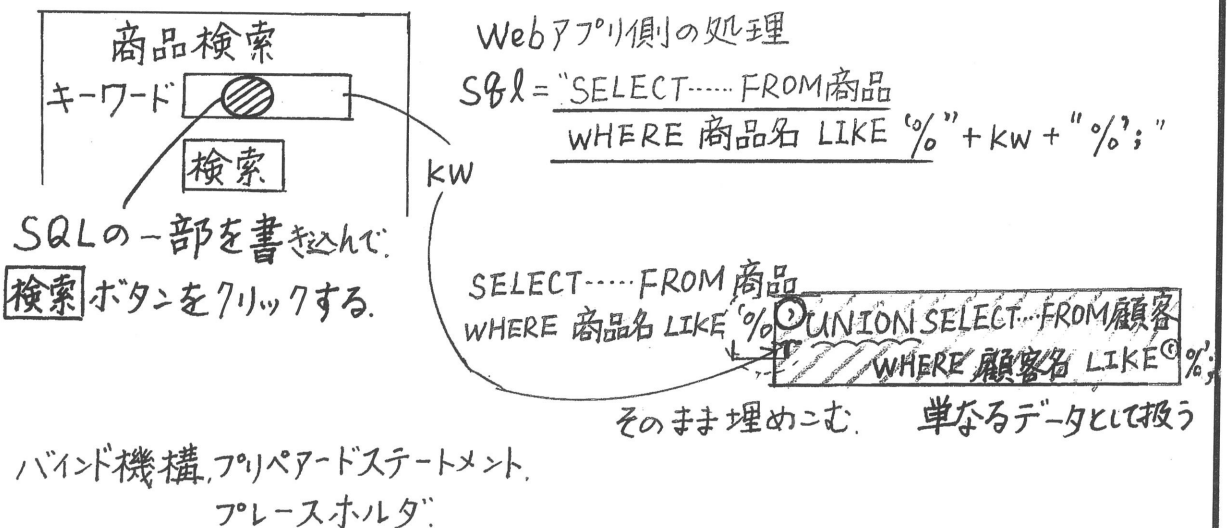
クロスサイトスクリプティング

○ XSS

・反射型XSS



⑥ SQLインジェクション



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

String sql = "SELECT ... FROM 商品 WHERE 商品名 = [?] ;"
データ

PreparedStatement ps = con.prepareStatement(sql); プリペアドステートメント

ps.setString(1, "おいしい水");

(" , UNION SELECT ... ")

String sql = "SELECT ... FROM 商品 WHERE 商品名 = [?] ;"
↑

プレースホルダ
(データを埋め込む箇所)

String sql = "SELECT ... FROM 商品 WHERE 商品名 = [?] ;"
データ

PreparedStatement ps = con.prepareStatement(sql); プリペアドステートメント

ps.setString(1, "おいしい水"); ... データ埋め込み

ResultSet rs = ps.executeQuery(); ... SQL文実行