

講義録レポート

講義録コード

04-59-1-301-01

講 座	情報処理安全確保支援士	科目①	模試編
目標年	2025年春期(上期)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	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 (79分) → 解説2 (73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

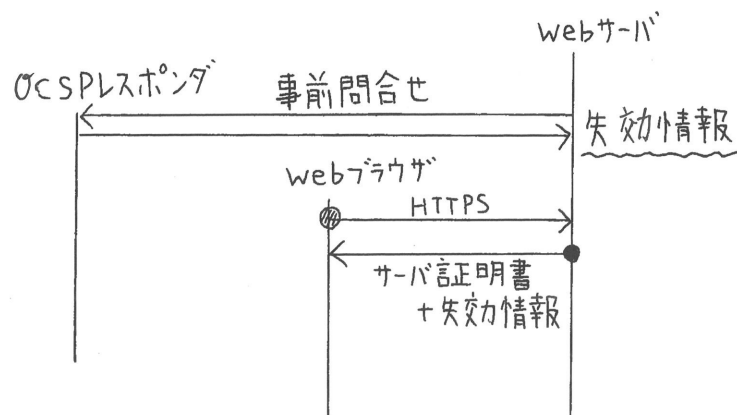
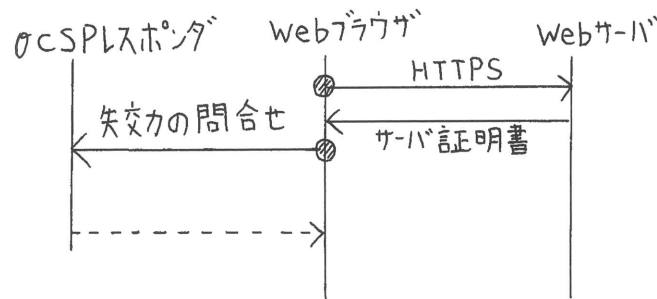
AMⅡ

問1~17 セキュリティ

問18,19,20 NW

問1 OCSPステッピング; 証明書と一緒に、
失効情報も渡す

- ・証明書の失効情報をサーバ(OCSPレスポンド)から取得するしくみ
- ・CRL:失効カリスト



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 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2 サイドチャネル攻撃

- ・ タイミング攻撃
- ・ 電力解析攻撃
- ・ テンペスト、電磁波解析攻撃

3 Smurf ICMPエコー要求/ICMPエコー応答
送元IPアドレスを偽る → IPスプーフィング

ウ. サプライチェーン攻撃

エ. ディレクトリトラバーサル, パストラバーサル

問4 DR DoS

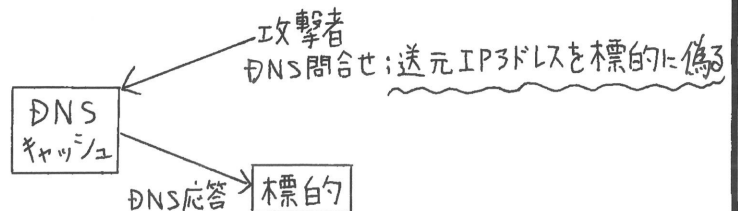
↓
Distributed ; (分散型) DDoS

→ ボットウィルスなどを用いて、様々な機器からDoS攻撃を行う

- ・ C&Cサーバ; ボットウィルスに指示を出すサーバ
- ・ コネクトバック通信

リフレクション
Reflection: 反射攻撃

↓
DNSリフレクション攻撃



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

- ・HTTP flood
- ・SYN flood
- 問6 SAML ; 異なるドメイン間でSSOを実現する
- 問7
 - ・SP ; サービスプロバイダ... サービスを提供するサイト
 - ・IdP ; IDプロバイダ ... 認証サーバ → IDaaS
 - ・3セッション ; 認証 認可 属性 情報, XML形式
 - ・3セッションを HTTPリダイレクト を用いて, SP ↔ ブラウザ ↔ IdP間で交換する
 - ・ケルベロス認証
 - ・OAuth, OpenID
 - ↓
 - 認可のしくみ
- 問9
 - ・FIRST
 - ・CSIRT
 - ・NISC ; 内閣サイバーセキュリティセンター
 - ・JPCERT/CC
 - ・CRYPTREC , CRYPTREC暗号リスト
 - 記載されている 暗号を見格ハッシュ関数 復習する!
 - 「電子政府における言語達のために参照すべき暗号のリスト」
 - ・J-CSIP ; サイバー情報共有インシデント
 - ・J-CRAT ; サイバーレスキュー隊
- 問10. NOTICE

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12

○ SSPM 姿勢
SaaS Security Posture Management

○ CSPM
Cloud

・サイバーセキュリティ経営ガイドライン

問13 HSTS: 2回目以降(次回以降), httpsアクセスをさせるしくみ
http://...でアクセスしても、HTTPSアクセスになる

3. CookieのSecure属性

7. Content-Security-Policy

問14 DNS, CAAコード ← 当該ドメインの(サーバ)証明書を発行する
CAを表す

ゾーンファイル {
・ Aコード
・ NSコード
・ MXコード
・ TXTコード
・ CNAMEコード

問17 TLS 1.3



メッセージ認証
↑
● AEAD; 認証 暗号
・ AES-GCM
- CCM
・ Chacha20-Poly1305

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： []		

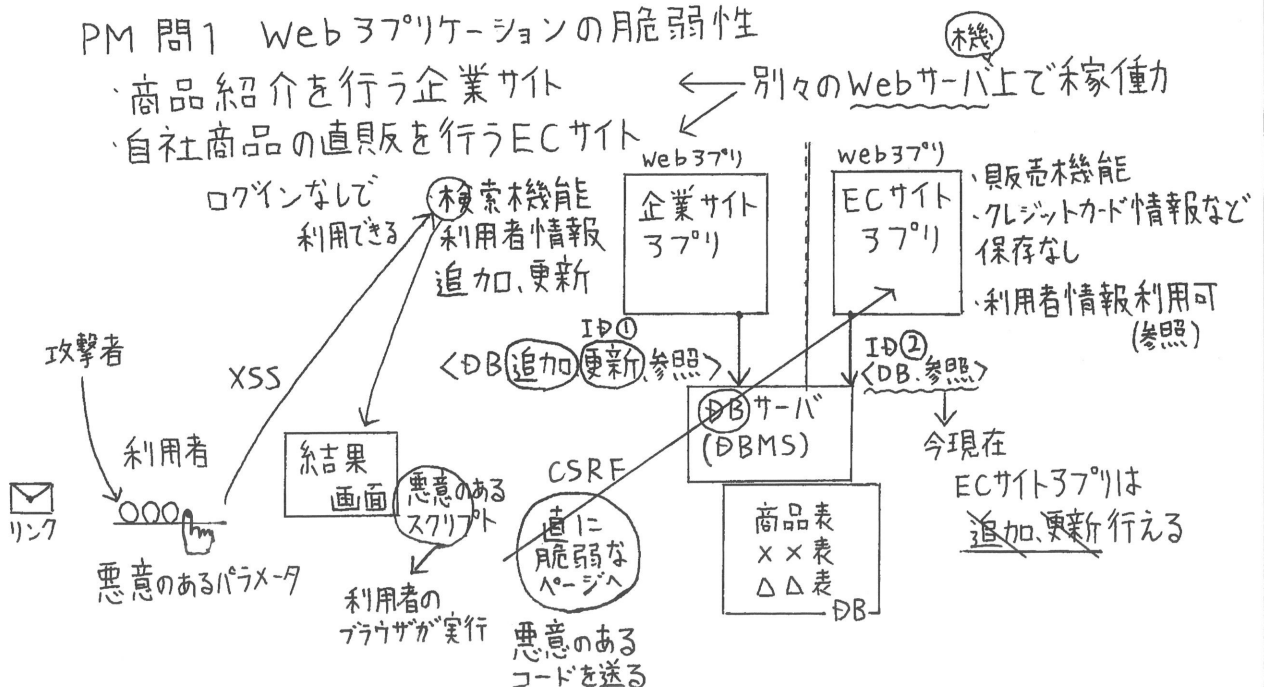
黒板内容

- ・金鍵交換；DHE, EC DHE
 ↓
 楕円曲線暗号に基づく
 ×RSA
 PFSの観点から
 女子ましくない

問20 IEEE 802.1x 認証フレームワーク

- ・RADIUSサーバ；認証サーバ
- ・オーセンティケータ
- ・サブリカント
- ・EAP；認証プロトコル
 EAPoL；EAP over LAN
 └ PEAP…ID.パスワードで認証
 └ EAP-TLS…利用側も証明書による認証

PM 問1 Webアプリケーションの脆弱性



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

〔セキュリティインシデントの発生〕

図2 通常とは異なるSQL文の実行 = SQL文インジェクション

```
sql.Statement = "SELECT 商品名 ...  
WHERE 商品コード = " + inputParam + " " ;
```

↑
検索機能画面で
入力された商品コード

〔セキュリティインシデントの発生〕

図2 通常とは異なるSQL文の実行 = SQLインジェクション

```
sql.Statement = "SELECT 商品名 ...  
WHERE 商品コード = " + "00" + "; INSERT ... --" ;  
sql.execute()
```

データ
コメントアウト
あ

* バインド機能

・プレースホルダ ... 置き換え場所を指定する文字
・アプレースホルダステートメント ... SQL文のひな形

⇒ 埋めこむデータと
SQL文本体が
明確に区別できる
様になる

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

