

講義録レポート

講義録コード

04-59-2-301-01

講 座	情報処理安全確保支援士	科目①	模試編
目標年	2025年秋期合格目標	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	8 枚
			補助ビジュアル 枚数	0 枚
			その他	0 枚

講義構成	解説1 (69分) → 解説2 (72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

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

AM II

問1 EMV 3-Dセキュア

(当初) 購入 → カード会社の
認証画面 → 購入完了

(EMV 3-Dセキュア) ; リスクベース認証をとり入れた

問2 OSコマンドインジェクション Webアプリの攻撃の1つ

HTTPヘッダインジェクション

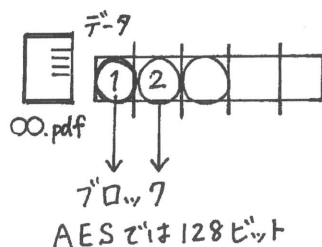
クリックジャッキング

Smurf

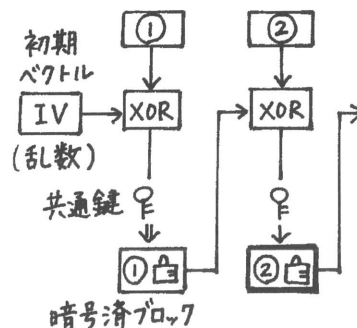
↓
WAF

問3

共通鍵暗号方式 $\left\{ \begin{array}{l} \text{ブロック暗号 : AES : 運用モード } \begin{array}{l} \text{CBC, (CTR)} \\ \text{GCM} \\ \text{CCM} \end{array} \\ \text{ストリーム暗号 : ChaCha20} \end{array} \right.$



CBC



認証暗号
(認証付き暗号)
↓
メッセージ認証

*CRYPTREC暗号リストも
確認しておいて下さい

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

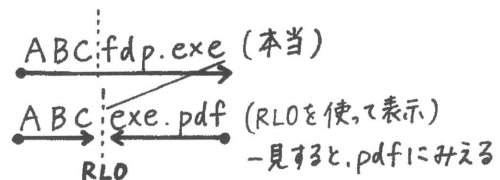
配布物	★テスト類 : [] ★その他の配布物1 : [] ★その他の配布物2 : []	講師	根岸 先生
-----	---	----	-------

黒板内容

問4 サイドチャネル攻撃

- 電力解析攻撃
 - タイミング攻撃
 - テンペスト
- など
- 機器の物理的な動きなどをもとに、秘密の情報(鍵など)を得る

- プロンプトインジェクション
- 中間者攻撃
- RLOを用いたファイル名の偽装



問5

SAMLアサーション

- SAML : XMLを用いて 認証情報 をやりとりする
- 異なるドメインのサイト間で SSO を実現する
 - SP: サービスプロバイダ,
 - IdP: IDプロバイダ

ケルベロス認証 : KDC (鍵 配布センター), チケット交付チケット: TGT
共通鍵 チケット交付サーバ: TGS

OAuth2.0: 複数のサイト間で認可制御を行う

LDAP: ディレクトリ サービス ... アカウント情報の共有などに使う

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

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6

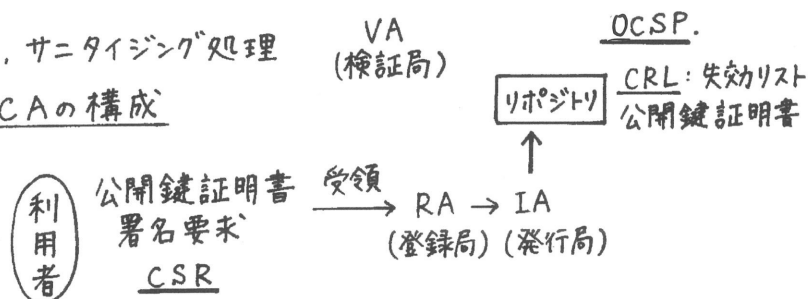
Webアプリへの攻撃 → 問2 OSコマンドインジェクション

- ・ XSS
- ・ SQLインジェクション
- ・ CSRF
- ・ セッションハイジャック
- ・ HTTPヘッダインジェクション

※ 攻撃の手法、被害の内容
対策法を復習して下さい。

※ エスケープ処理、サニタイジング処理

問7 PKI, CAの構成



問8 サイバーキルチェーン；標的型攻撃

- ・ 偵察
- ・ 武器化
- ・ デリバリー
- ・ エクスプロイト
- ・ インストール
- ・ C&C
- ・ 目的の実行
- ・ APT
- ・ カスタマイズしたマルウェア
- ・ やりとり型攻撃
- ・ 水飲み場型攻撃/ドライブバイダウンロード
- ・ サプライチェーン攻撃
- ・ パスワードリスト攻撃

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

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9 NOTICE 問10 ・ J-CSIP ・ J-CRAT ・ JPCERT/CC ・ CRYPTREC ・ NISC 問11 SOAR CSPM SIEM	・ SECURITY ACTION ・ JC-STAR など セキュリティの取組み体制 支援体制、ガイドライン ・ CVSS ・ KEV ・ EPSS 問12 SBOM 問13 ・ Wi-Fi Enhanced Open ・ Easy Connect ・ WPA3 パーソナルモード ; SAE 問14 (TLS) 1.3 ・ Client Hello ・ Server Hello ・ 暗号スイート ・ DHE ・ ECDHE } 鍵交換 → PFS対策 問15 DNSSEC … DNS回答に、DNSサーバが署名を付ける DNSキャッシュポイズニング対策 ○DNS通信の暗号化 PC → DNS キャッシュサーバ DNS通信 DNS over TLS : DoT DNS over HTTPS : DoH

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

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16 S/MIME

問17 HSTS

午後問1

○送信ドメイン認証

- ・SPF ; IPアドレスベース
- ・DKIM ; メールサーバの署名 → ARC : 送信ドメイン認証できる
- ・DMARC ; SPF, DKIM認証失敗時の対応を 情報提供する
集計レポート(rua)

↓
必要な情報は
DNSサーバで
提供する

・ARC

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

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

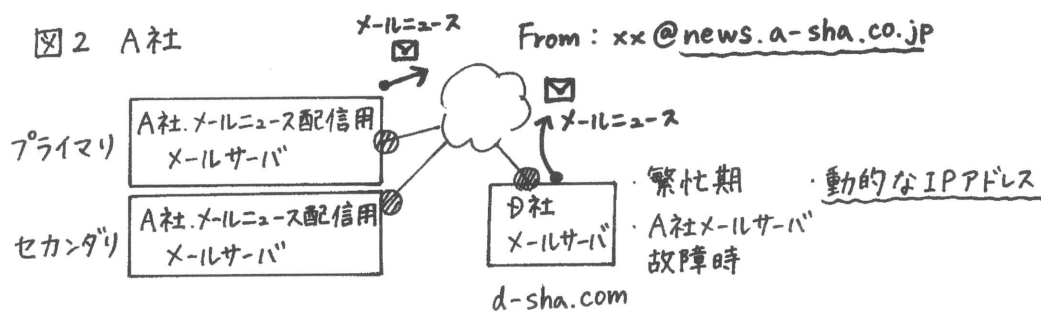
・ A社 メールニュースを配信

[P社の迷惑メール対策方針とA社の現状の …]

図1. P社

- ・ SPF未設定 → 迷惑メールスコア上昇
- ・ DKIM未設定
- ・ SPF, DKIMで認証失敗 → ブロック又は隔離

図2 A社



[SPFの設定変更]

(ゾーンファイルの内容)

news.a-sha.co.jp. IN TXT "v=spf1 +ip4:203.0.113.10

+ip4:203.0.113.11 ~all"

softfail

"v=spf1 +ip4:203.0.113.10/31 ~all"

【訂正】講義内の板書は「203.0.113.10/23」となっておりますが、
正しくは講義録のとおり、「203.0.113.10/31」です。お詫びして訂正いたします。

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

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 : []		

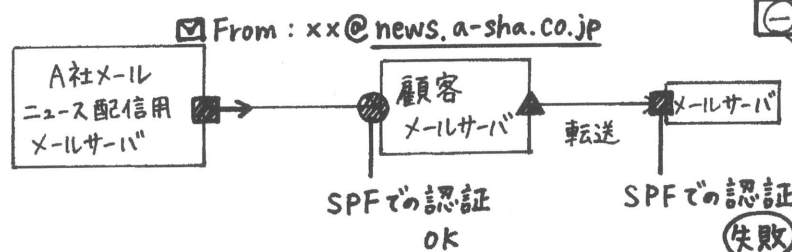
黒 板 内 容

[SPFの設定変更]
(ゾーンファイルの内容)

news.a-sha.co.jp. IN TXT "V=spf1 +ip4:203.0.113.10

+ip4:203.0.113.11 +ip4: 自社メールサーバ"

+ip4:203.0.113.11
include = d-sha.com ~all"
fail



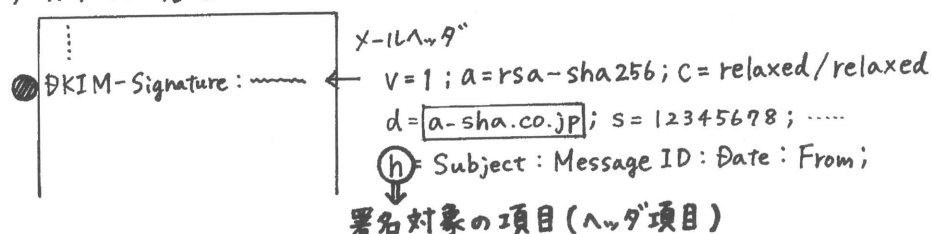
[DKIMの設定]

・メールサーバが署名する → 検証用の公開鍵はDNSサーバで配布する

セレクト

12345678. _domainkey. news.a-sha.co.jp. IN TXT "...公開鍵(旧)..."
12345679. _domainkey. news.a-sha.co.jp. IN TXT "...公開鍵(新)..."
並行運用する

メールサーバの署名



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

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

[DMARCの設定]

- DMARC
 - SPF, DKIMの認証に失敗したメールの取り扱い情報を提供
 - quarantine ; 隔離
 - reject ; 拒否
 - none ; 何もしない
 - 認証に失敗した情報 ⇒ 集計レポート

- SPF ... MAIL FROM → インベロープ FROM → SMTPのやりとりを復習
- DKIM ... DKIM-Signature
 - MAIL FROM
 - RCPT TO
- ※ DMARC ... from
 - ↓ 認証結果
 - Authentication-Results

[メール転送への高度な対応]

- ARC
 - ARC-Authentication-Results
 - ARC-Message-Signature
 - ARC-Seal

