講義録レポート

講義録コード　04-69-1-301-01

講　座	情報処理安全確保支援士	科目①	模試編
目標年	2026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/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	11　枚
			補助ﾚｼﾞｭﾒ枚数	0　枚
			その他	0　枚

講義構成	解説1（79分）　→　解説2（83分）
使用教材	公開模試 科目A-2問題 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	※科目A-1の解説講義はありません。科目A-1解答解説冊子でご確認ください。

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：[ ]	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1~15 セキュリティ

16~20 ネットワーク

21~25 その他分野

問1. セキュリティ・バイ・デザイン

問2. ゼロデイ攻撃：脆弱性の存在が知られていない
セキュリティパッチ、対策法もない
攻撃者だけが、その脆弱性を知っている状況で、
攻撃を行う

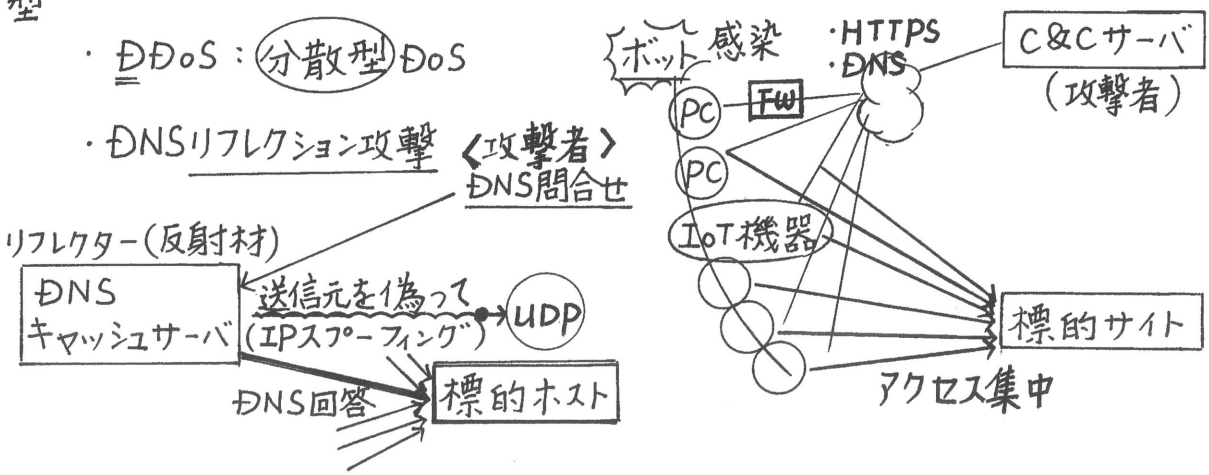
エクスプロイット
exploitコード：脆弱性を利用して、攻撃するプログラム
→多くの場合は、管理者権限(特権)を奪取する
権限昇格

問3. DRDoS

分散型 リフレクション(反射) 過負荷をかけて本来提供しているサービスの提供を妨害する

・DDoS：分散型DoS

・DNSリフレクション攻撃 〈攻撃者〉DNS問合せ



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：[　　]		

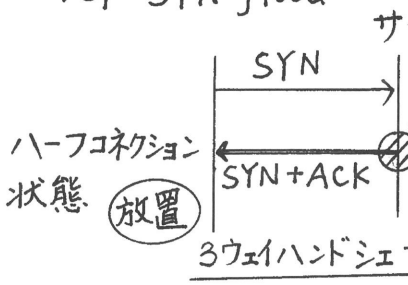
黒板内容

・ARPキャッシュポイズニング

ARPキャッシュテーブルの情報を汚染して、中間者攻撃を行う

〈IPアドレス：MACアドレス〉

・TCP SYN flood



を何度も、くり返す

・DNSキャッシュポイズニング

対策

・DNSキャッシュサーバが、DNS問合せに用いる、送信元ポート番号をランダム化

・オープンリゾルバ状態にしない

・根本的な対策→DNSSEC

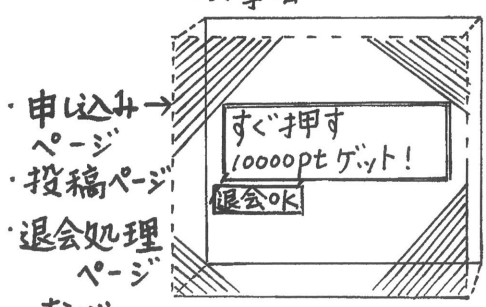
DNSサーバが、DNS回答に署名を付ける

問4．クリプトジャッキング

問6→サイドチャネル攻撃→耐タンパ性

クリックジャッキング

攻撃者



・申し込みページ
・投稿ページ
・退会処理ページ
など

透明で表示
(透明度100%)

⊙タイミング攻撃　・テンペスト
⊙電力解析
・エラー回復処理を利用する　など

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

・Smurf　ICMPエコー要求を用いたDoS攻撃

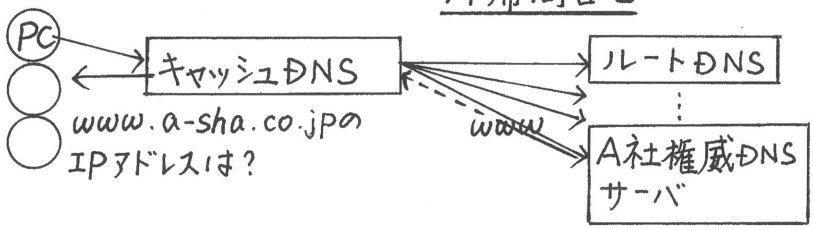
問5　失効リスト(CRL)：有効期間内であるが、使えない公開鍵証明書の一覧

問6　・ディレクトリトラバーサル/パストラバーサル

・サプライチェーン攻撃

問7　・オープンリゾルバー：外部からの問い合わせに応じるDNSキャッシュサーバ

⇓再帰問合せ



問8　ハッシュ関数

ハッシュ値のビット数

SHA-256　SHA3-256

SHA-512　SHA3-512

SHA2　SHA3

・Cryptrecの暗号リスト

- SHA-512/256

①まず512ビットのハッシュ値を作る

②一部切り出して、256ビットのハッシュ値として扱う

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：[ ]	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9. CPS：CAの運用を規定した文書

問10・ISMAP

・FIPS140-3：暗号モジュールに求められるセキュリティ要件の仕様

・JIS Q15001：個人情報保護マネジメントシステム

・サイバーセキュリティ経営ガイドライン

問11 CSF

問12 ISO/IEC 15408 ‥‥ 個別製品のセキュリティ

JISQ27001：ISMS

問13 IoC：マルウェアの活動こん跡 などの情報のこと
不正アクセスのこん跡

問14 イミュータブルバックアップ
変更不能

・WORMデバイス ：一旦書き込んだら上書きなどの
Write Once Read Many 変更は出来ない

問15・DKIM …メールサーバの署名

・SPF ‥‥ IPアドレスを検証

・DMARC…DKIM/SPFでの認証失敗時の扱いを伝える
集計レポート(rua)の送り先(メールアドレス)を伝える

・ARC ‥‥ 署名のチェーン(連鎖)を用いることで、SPF.DKIMがうまく機能しない場面を補う

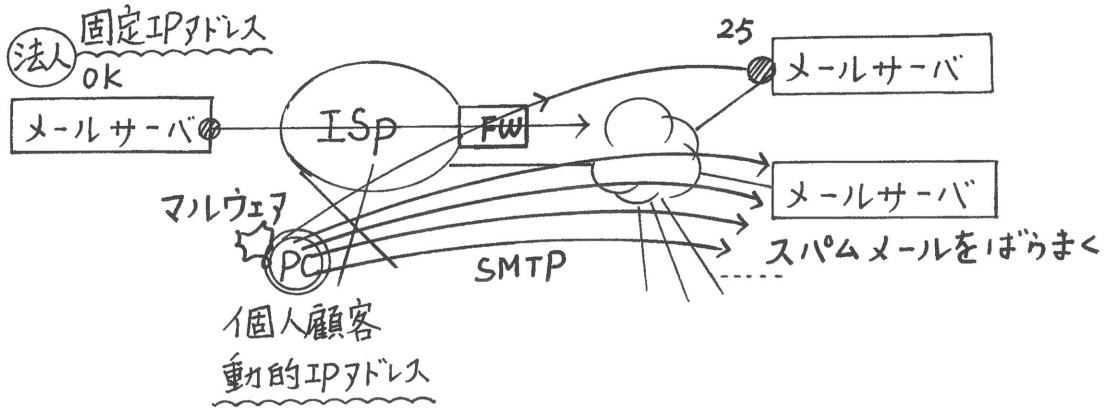
情報処理 講義録	コース・講義等	情報処理安全確保支援士	科目	公開模試解説 前編	回数	

配布物	★テスト類：[ ]	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 OP25B

Outbound Part 25 Block



・オープンリレー，第三者中継

科目B 問1

- Webサイトへの攻撃
  - ・SQLインジェクション
  - ・CSRF
- ・パスワードへの攻撃
- ・WAF

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

科目B 問1

・顧客情報が流出する事故　ID，パスワードの(ハッシュ値)が流出

・不正アクセスが多数発生した

・一方向性→直ちにパスワード漏えいにはならない

・レインボーテーブル攻撃

単語：ハッシュ値(SHA-256)

admin　xxxxxx

password　△△△△△

⋮

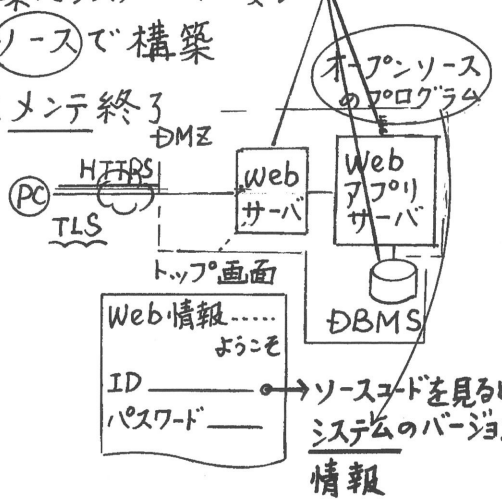
↑この表を効率よく扱うレインボーテーブル攻撃

〔Web情報案内システムの概要〕

仮想サーバ(コンテナ)

・オープン(ソース)で構築

・数年前にメンテ終了



Webサーバ．Webアプリ．DBMS → 専用ユーザ権限（≒一般ユーザ権限）

一般ユーザ権限

Webサーバプロセス ←攻撃 悪意のあるプログラム

実行 ↓ 送りこむ

悪意のあるプロセス

一般ユーザ権限で実行される

× 管理者権限 root スーパーユーザ

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	

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1

- 顧客情報が流出する事故　ID, パスワードのハッシュ値が流出
- 不正アクセスが多数発生した

〔Web情報案内システムの概要〕

- オープンリースで構築
- 数年前にメンテ終了
- EXPORT → ユーザ単位で権限設定：初期 → どのユーザもEXPORTの実行可能

〔SQLインジェクションによる流出ファイルの生成〕

↳SQL文の一部をデータとして流しこみ、システムの設計者が想定していなかったSQL文を実行させる

× 入力されたデータをそのまま使ってSQL文を組み立てるとダメ

○ DBMSのバインド機構を使う

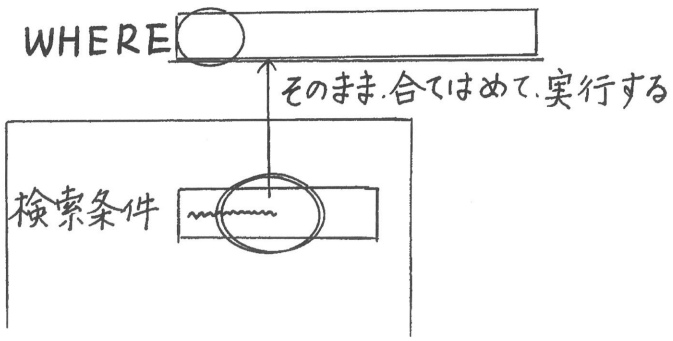
プリペアードステートメント(SQL文のひな型)を作り、それにデータを入れる。

EXPORT [SELECT * FROM USER] OUTPUT [/var/web/data/xyz123]

出力結果を格納するファイル

・Webページで表示する画像データの置き場所

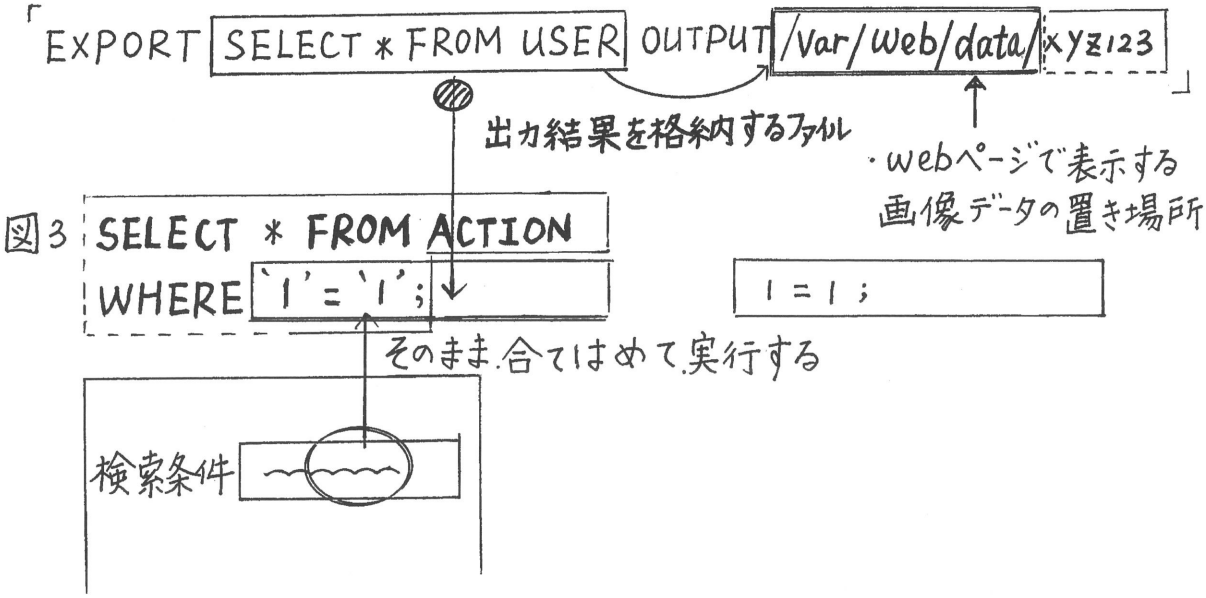
図3 SELECT * FROM ACTION

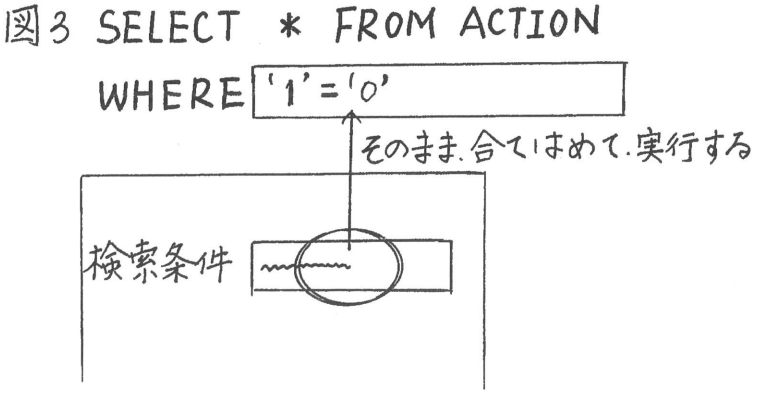


情報処理 講義録	コース・講義等	情報処理安全確保支援士	科目	公開模試解説 前編	回数	

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





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

「EXPORT [SELECT * FROM USER] OUTPUT [/var/web/date/] [xyz123]」

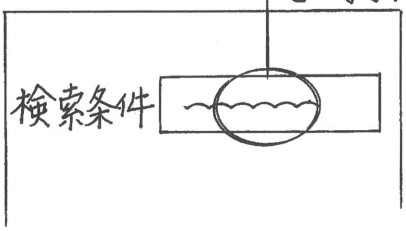
出力結果を格納するファイル

・webページで表示する画像データの置き場所

図3 [SELECT * FROM ACTION WHERE %1]

下線② ○Webリソースフォルダ

そのまま合てはめて実行する



科目B 問1

・顧客情報が流出する事故　ID, パスワードのハッシュ値が流出

・不正アクセスが多数発生した

〔Web情報案内システムの概要〕

○ オープンソースで構築

○ 数年前にメンテ終了

○ EXPORT→ユーザ単位で権限設定：初期→どのユーザもEXPORTの実行可能

〔CSRFによる罠サイトからのコマンド投入〕

○ログインが必要なサイト

○ログインしたままの状態で罠サイトへ誘導された

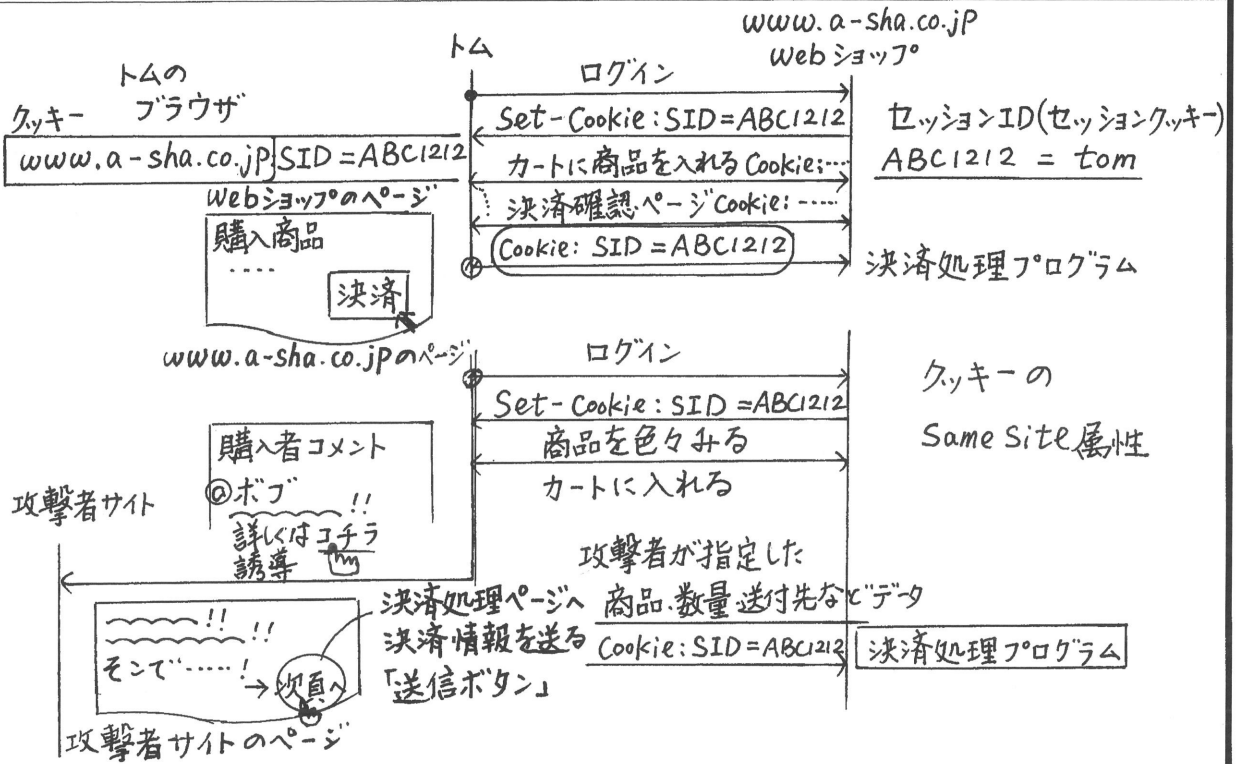
○罠サイト上で、フォーム送信ボタンを押すなどして、元のサイトの決済ページなどに直に移る

＊ユーザの知らない所でログイン後にしか出来ない処理をさせられる

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	

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



・画面遷移の確認

・手前のページ内に ランダムな値 を入れておき、手前ページから遷移してきた時に確かめる

= ・フォームデータとして送る
・画面上に表示させない → hidden 属性

・Referer：HTTPヘッダの1つ → https://www.b-sha.co.jp/pub/list.cgi?…

・Origin ：

スキーム（プロトコル） ホスト名 :443 パス パラメータ（URLクエリストリング）

・オリジン (スキーム.ホスト名.ポート番号) の情報のこと

https://www.a-sha.co.jp/index.html ← 同一オリジン
https://www.a-sha.co.jp/pub/OO.html
:443

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

科目B 問1

〔パスワードハッシュ値の適切な生成〕

・ハッシュ関数の性質
　・衝突困難性
　・原像計算困難性：一方向性
　・第二原像計算困難性

・ソルト値

・フォルスネガティブ

・フォルスポジティブ

・WAF