

講義録レポート

講義録コード

04-39-1-301-02

講 座	情報処理安全確保支援士	科目①	模試編
目標年	2023年春期(上期)合格目標	科目②	公開模試解説 後編
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
			補助レジュメ 枚数	0 枚
			その他	0 枚

講義構成	解説1 (50分) → 解説2 (58分) → 解説3 (34分) → 解説4 (26分)			
使用教材	公開模試 午後Ⅰ問題			
	公開模試 午後Ⅱ問題			
	公開模試 解答・解説			
配付 教材・資料				
備考				

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

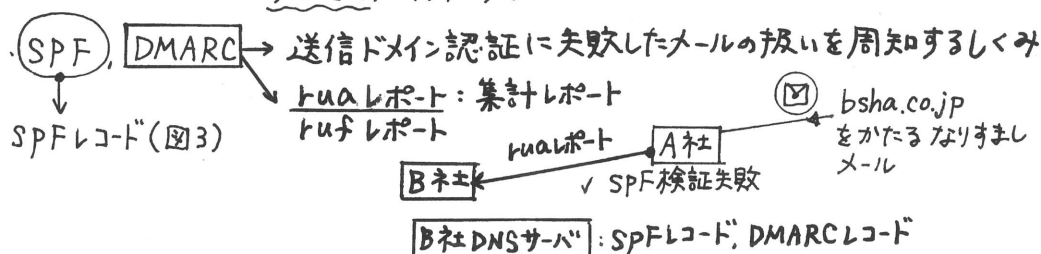
情報処理 講義録	コース・講義等	情報処理安全確保 支援士	科目	公開模試解説 後編	回数	1
----------	---------	--------------	----	-----------	----	---

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

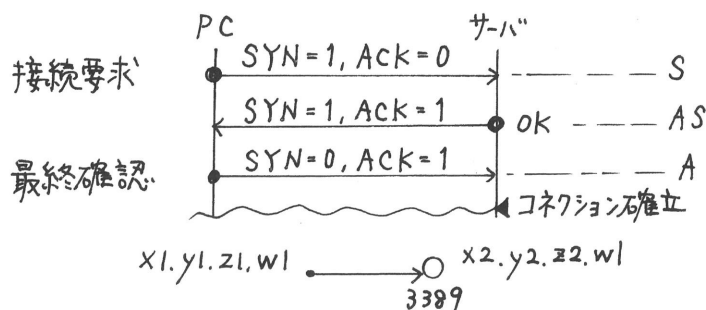
問2

- ・ログを分析する
- ・メールヘッダなどのヘッダの内容を分析する
- ・事前調査の手法 : ポートスキャン
 - 3ウェイハンドシェーク
 - 実際に接続してみても反応があるかを調べる
 - TCPスキャン ... 反応があるかを調べる
 - UDPスキャン ... ICMP port unreachable ポート到達不能
 - 開いているポートを探す
 - 当該のポートで待ち受けているプロセスが存在する



TCPヘッダのフラグビット

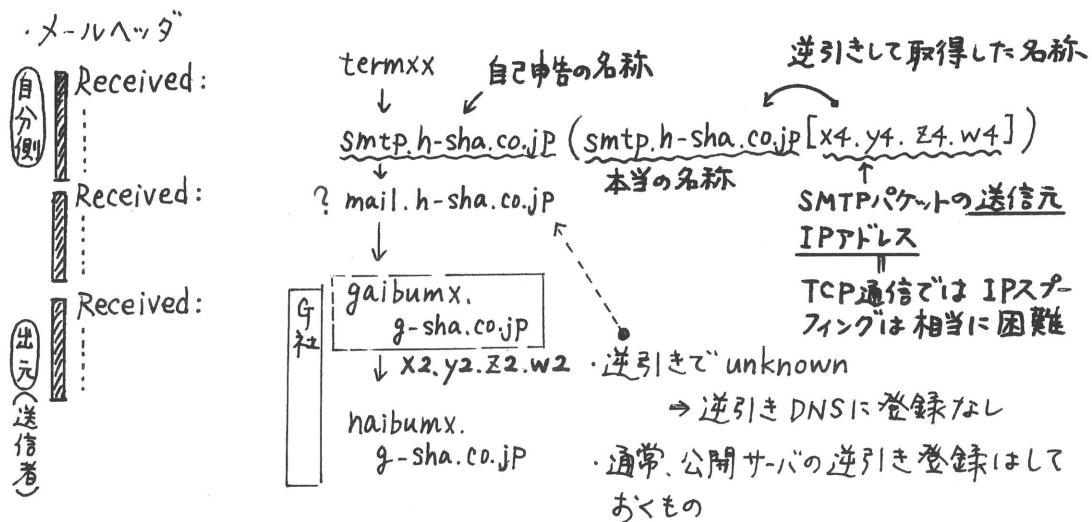
- ・3ウェイハンドシェーク : コネクションをつくるためのやりとり



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 後編	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



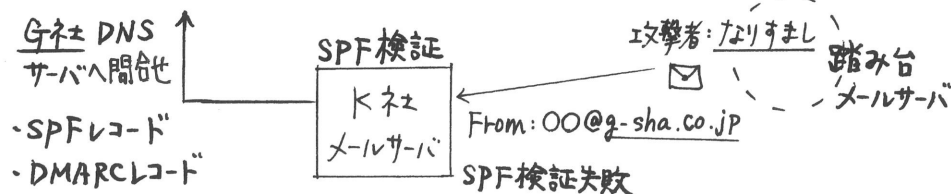
G社 権威 DNSサーバに 設定する SPFコード
 (DMZ上の DNSサーバ)

DMZ上の 外部メールサーバ

⇒ G社ドメインを 送信元とするメールを西に信するメールサーバの IP アドレスを指定する

図 3

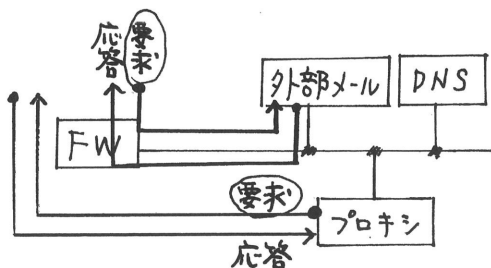
IN TXT "V=spf1 +ip4: X2.y2.z2.w2 -all"



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 後編	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： []		

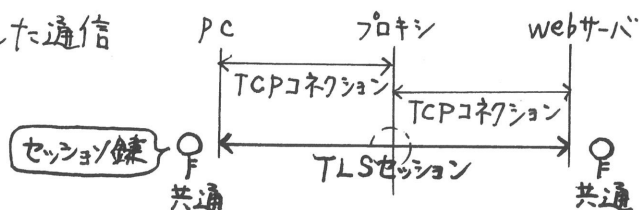
黒板内容



問3

- DNSサーバの役割
 - DNSコンテンツサーバ / 権威サーバ
 - DNSキャッシュサーバ / フォルサービスリゾルバー
- プライマリサーバ / セカンダリサーバ
- ランダムサブドメイン
- DNS水責め (Dos攻撃)
- DNSキャッシュポイズニング
- 再帰問合せ

- ゾーン情報：権威サーバが管理する当該ドメインの情報
- ゾーン転送
- プロキシサーバを介した通信



情報処理 講義録

情報処理安全確保
支援士

科
目

公開模試解説 後
編

回
数

1

配布
物

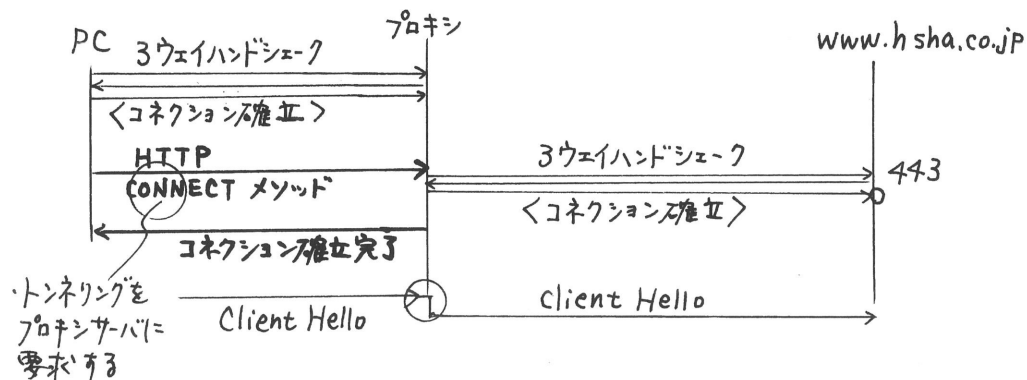
- ★ テ ス ト 類 : []
- ★ その他の配布物 1 : []
- ★ その他の配布物 2 : []

講
師

根岸

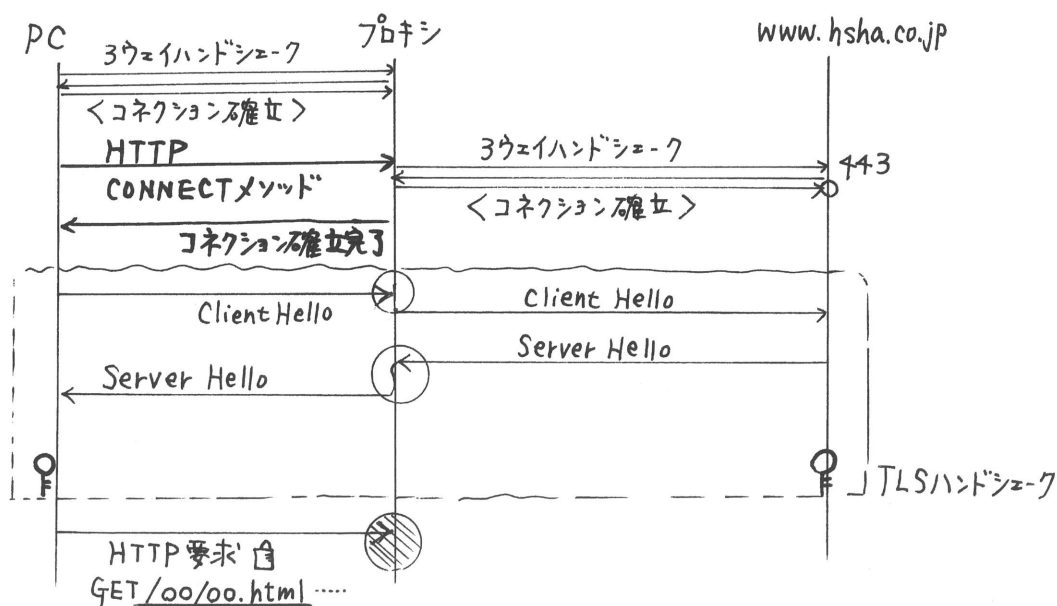
先生

黒 板 内 容



CONNECT www.hsha.co.jp:443 -----

接続先ホスト名 : ポート番号
(IPアドレスでもOK)



情報処理 講義録

情報処理安全確保
支援士

科
目

公開模試解説 後
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

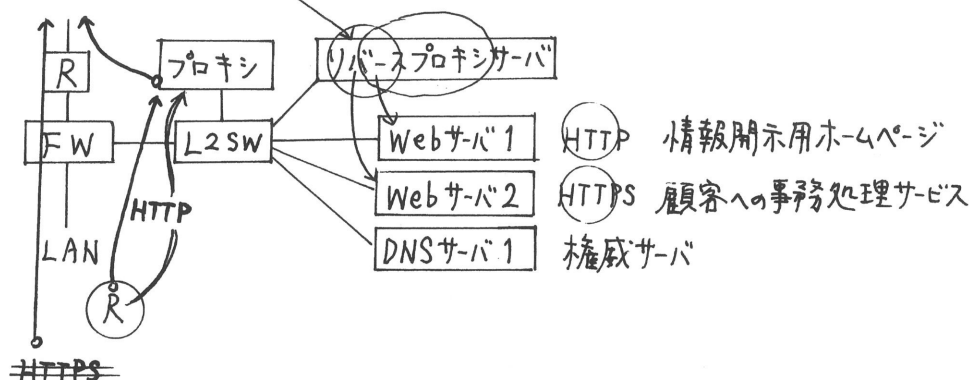
根岸

先生

黒 板 内 容

- ・ (フォワード) プロキシ 内部 → 外部
- ・ リバース プロキシ 外部 → 内部 : 社内LANのサーバに
外部から接続したい

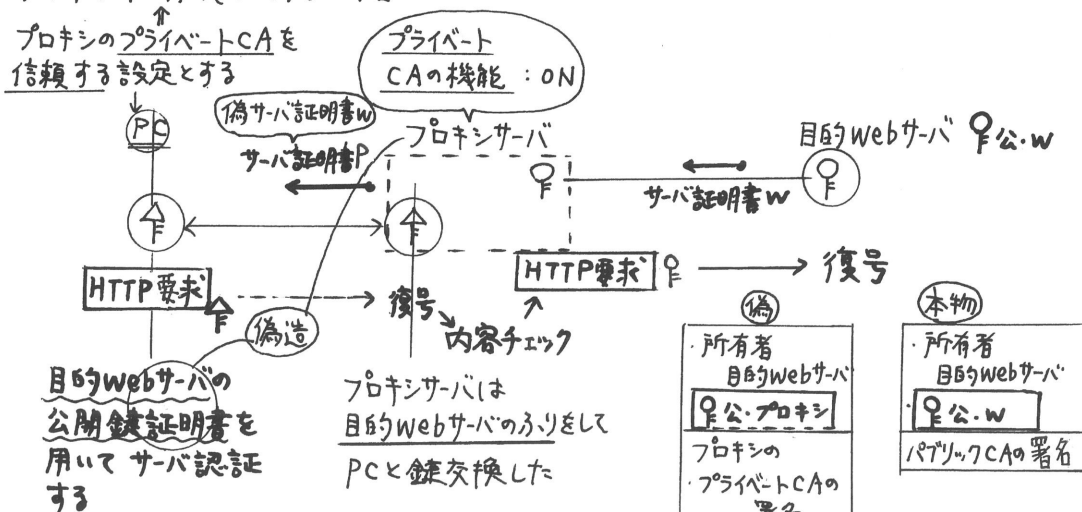
プロキシ認証 : プロキシサーバ利用時に利用者認証を行う



- ・ 透過型 プロキシ
- ・ 図4

プライベートCAの(ルート)証明書をインストールしておく

プロキシのプライベートCAを
信頼する設定とする



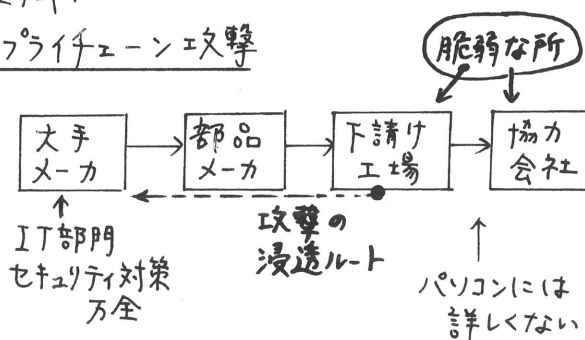
情報処理 講義録	コース・講義等	情報処理安全確保 支援士	科目	公開模試解説 後 編	回数	1
----------	---------	-----------------	----	---------------	----	---

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

PMⅡ問1

・ サプライチェーン攻撃



・ CSIRT

・ トリアージ

・ SOC : Security Operation Center

・ アタックサーフェステスト

・ ペネトレーションテスト

脆弱性の深刻度

・ CVSS

・ 現状値:

・ 環境値:

・ 基本値: 脆弱性があるものの深刻度

内部統制

・ 職務分離 の原則

・ 必要最小(権限)

・ EDR : Endpoint Detection and Response

・ SIEM: Security Information and Event Management

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 後編	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
・ ディレクトリサーバ: ^(例) LDAPサーバ ・ <u>情報を共有するためのしくみ</u> ↓ ・ ホスト情報 (hosts ファイル) ・ ユーザ情報 (ID など) ・ ----- PM II 問 2 標的型攻撃 ・ 標的組織・個人を定める 目的を達成するまで ・ APT: <u>長期間</u>、<u>ばれない様に攻撃を続ける</u> → 徐々に中枢部に到達する ・ <u>カスタマイズしたマルウェア</u>, ゼロデイ攻撃 ↳ パターンマッチング方式の ウイルス対策ソフトでは 検出できない ・ ソーシャルエンジニアリング ・ 水飲み場型攻撃 ・ BEC: ビジネスメール 詐欺 ・ <u>メール添付ファイルでのマルウェア配布</u> ↳ やりとり型攻撃

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 後編	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
・ ハクティビズム : ← 自らの情報は公表する / 名乗る ・ ボット, RAT (Remote Access Tool) C&C サーバから <u>指令を受け取る</u> / <u>コネクトバック</u> ・ ウィルス検出の方式 (説明 3. e, f, g) ・ パターンマッチング → <u>難読化</u> ・ ルールベース ・ ヒューリスティック / ビヘイビア ... <u>実際に動かしてみても</u> 不審な動作をしないかも 調べる サンドボックス : 隔離された環境