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
			補助ﾚｼﾞｭﾒ 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	

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 ← TCPスキャン … 3ウェイハンドシェーク 実際に接続してみて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 が返ってこないかを調べる

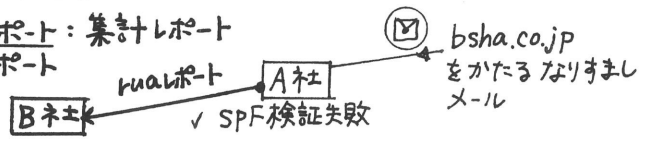
開いているポートを探す = 当該のポートで待ち受けているプロセスが存在する

・SPF, DMARC → 送信ドメイン認証に失敗したメールの扱いを周知するしくみ

SPFレコード(図3)

rua レポート：集計レポート

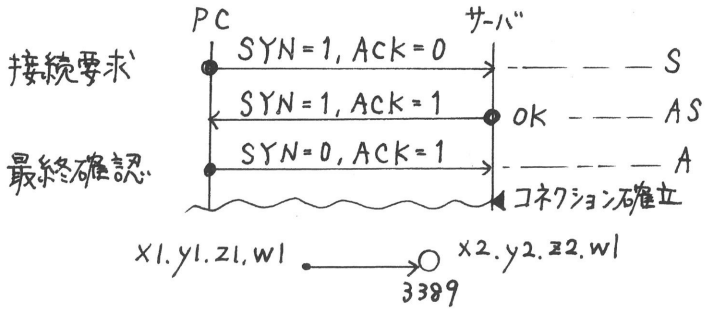
ruf レポート



B社DNSサーバ：SPFレコード, DMARCレコード

TCPヘッダのフラグビット

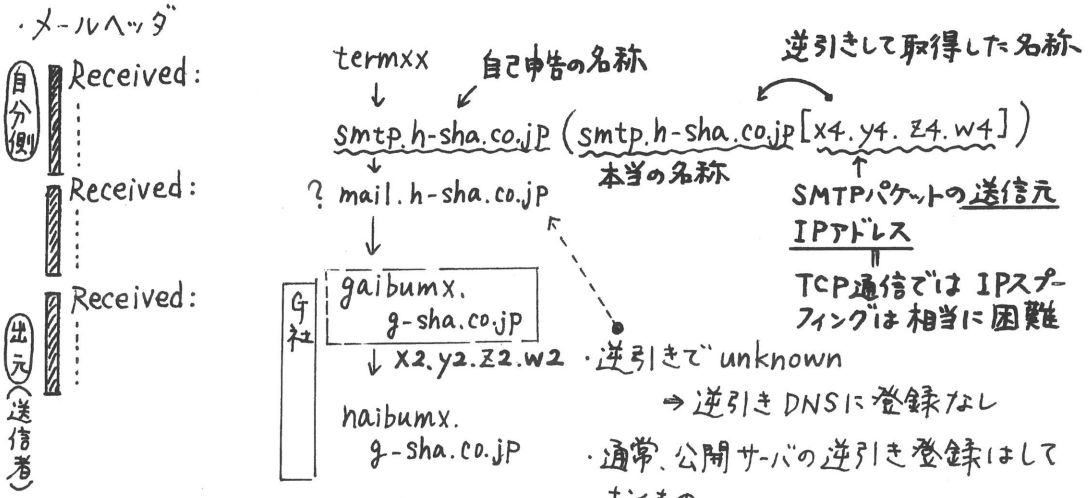
・3ウェイハンドシェーク：コネクションをつくるためのやりとり



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

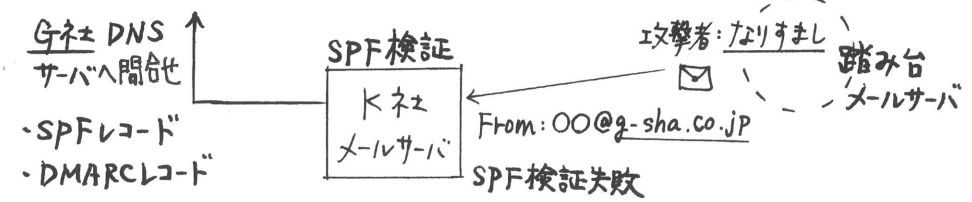
黒板内容



G社 権威DNSサーバに設定するSPFレコード
(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配信するメールサーバのIPアドレスを指定する

図3

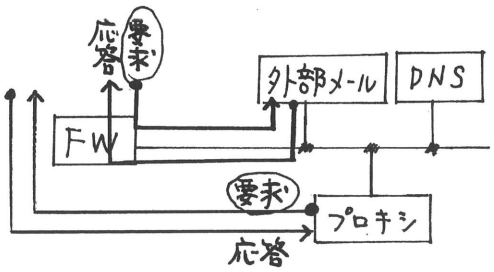
```
---- IN TXT "v=spf1 +ip4:x2.y2.z2.w2 -all"
```



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（プライマリサーバ セカンダリサーバ） / 権威サーバ

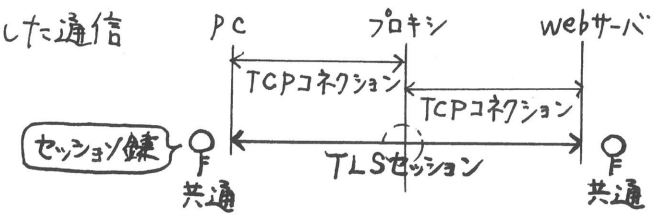
・DNSキャッシュサーバ（再帰問合せ） / フルサービスリゾルバー

<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

＊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

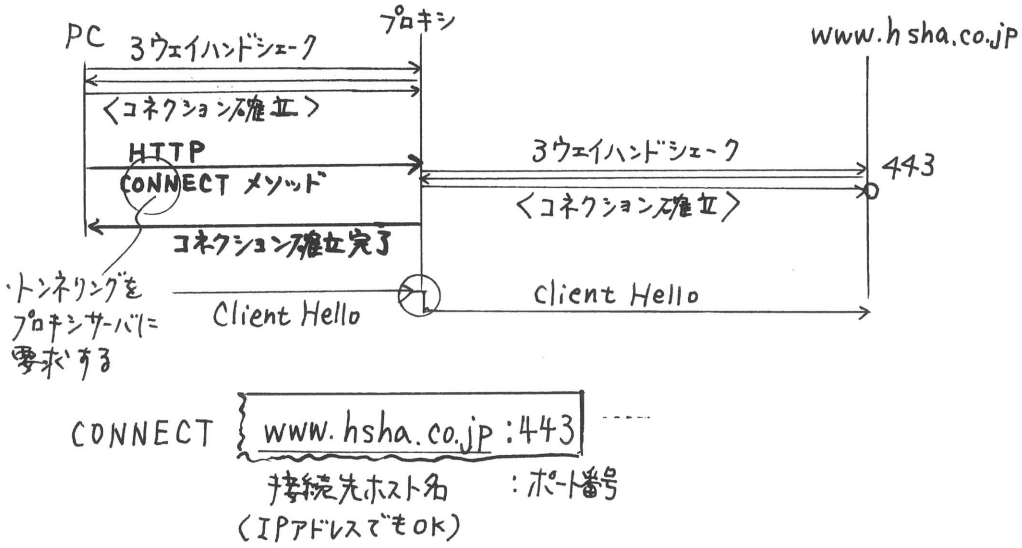
・プロキシサーバを介した通信



情報処理 講義録	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

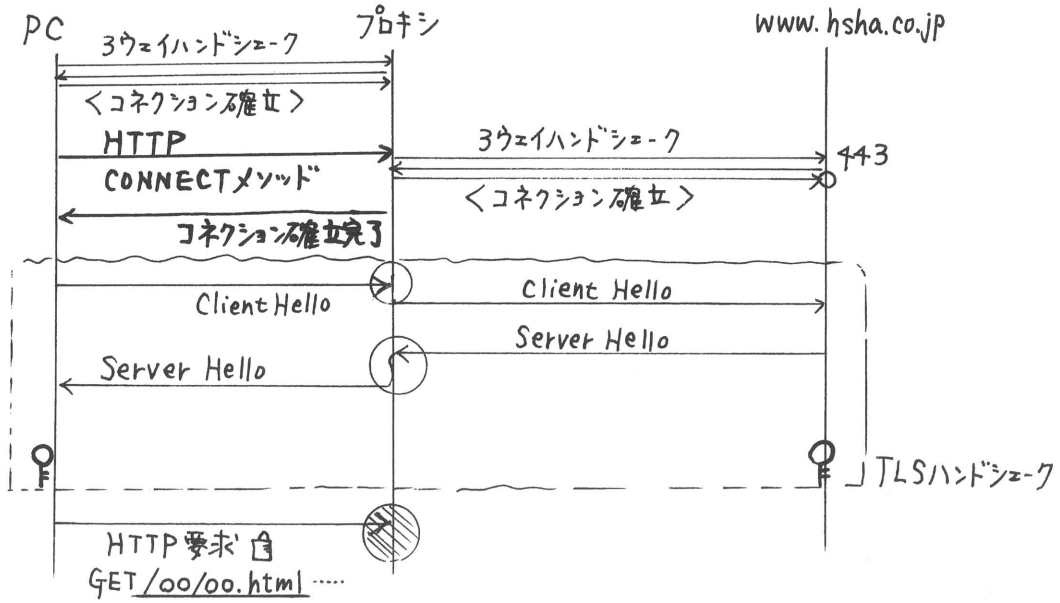
配布物	★テスト類：[ ]	講師	根岸 先生
	★その他の配布物1：[ ]		
	★その他の配布物2：[ ]		

黒板内容



CONNECT { www.hsha.co.jp :443 }

接続先ホスト名（IPアドレスでもOK）　：ポート番号



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

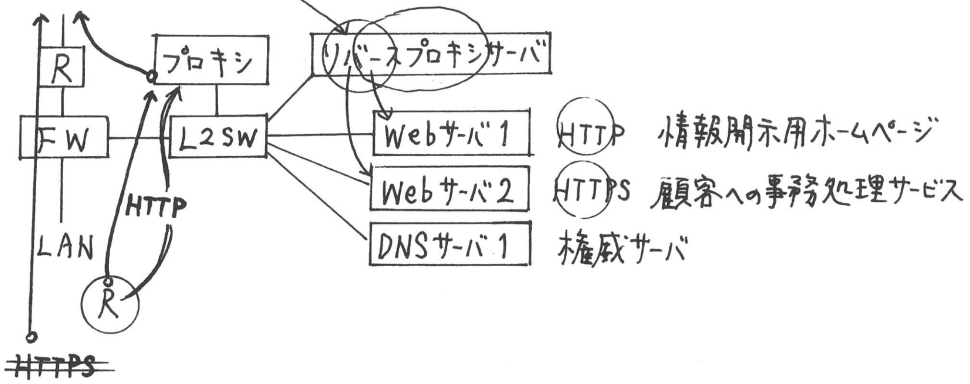
配布物	★テスト類：[ ]	講師	根岸 先生
	★その他の配布物1：[ ]		
	★その他の配布物2：[ ]		

黒板内容

・（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

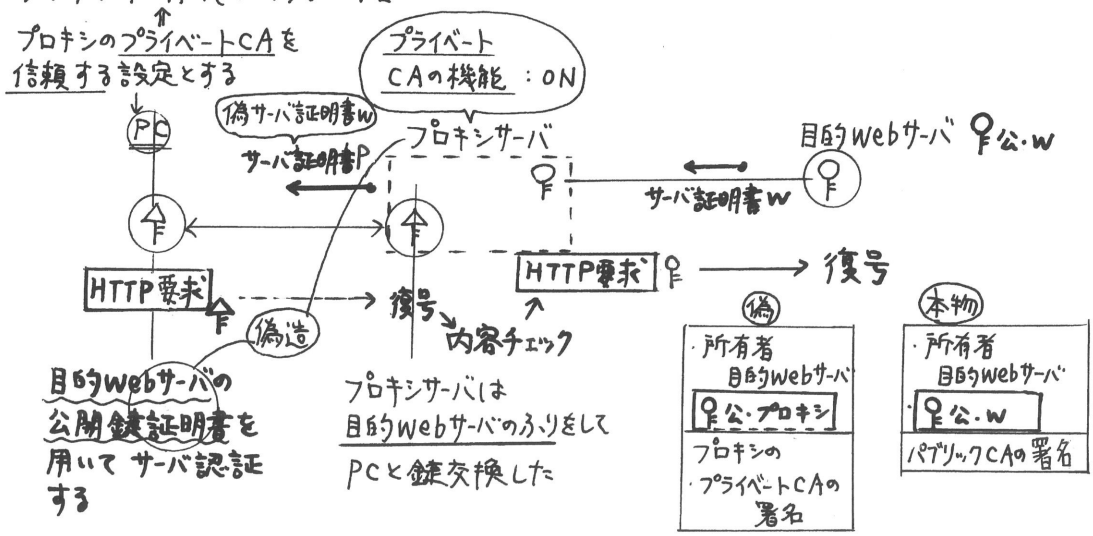
プロキシ認証：プロキシサーバ利用時に利用者認証を行う



・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



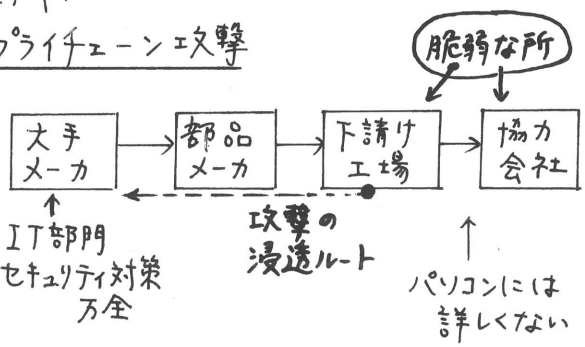
情報処理 講義録	コース・講義等	情報処理安全確保支援士	科目	公開模試解説 後編	回数	1

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

PM II 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：脆弱性がもつそもそもの深刻度

【訂正】問1設問3(2)の解説について、講師は正答を「オ(防御的アプローチ)」としておりますが、正しくは解説冊子に記載のとおり「イ(サイバーハイジーン)」となります。

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：[ ]	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

・ディレクトリサーバ：(例) LDAPサーバ

・情報を共有するためのしくみ

↓

・ホスト情報（hostsファイル）

・ユーザ情報（IDなど）

・----

PMⅡ 問2

標的型攻撃

・標的組織・個人を定める

・APT：長期間、ばれない様に攻撃を続ける（目的を達成するまで）

→徐々に中枢部に到達する

・カスタマイズしたマルウェア，ゼロデイ攻撃

↳パターンマッチング方式のウィ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

・メール添付ファイルでのマルウェア配布

↳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：[ ]	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

・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サーバから指令を受けとる
コネクトバック

・ウィルス検出の方式（設問3. e, f. g）
・パターンマッチング↔難読化
・ルールベース
・ヒューリスティック／ビヘイビア … 実際に動かしてみて不審な動作をしないかを調べる
サンドボックス：隔離された環境