講義録レポート

講義録コード　04-42-2-301-01

講　座	情報セキュリティマネジメント	科目①	模試編
目標年	2024年下期合格目標	科目②	模試解説
コース	本科生　本科生Ｂ	回　数	1　回

講師名	三ッ矢 眞紀　講師	内訳	板書枚数	4　枚
			補助ﾚｼﾞｭﾒ枚数	6　枚
			その他	0　枚

講義構成	解説1 (81分) → 休憩 (10分) → 解説2 (80分)
使用教材	
配付教材・資料	
備考	※Webで実施された方の問題・解答解説につきましては、模試実施後に表示される「結果画面」にてご確認ください。

ＴＡＣ情報処理講座

情報処理 講義録	コース・講義等	情報セキュリティマネジメント	科目	模試解説	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	三ツ矢 先生

黒板内容

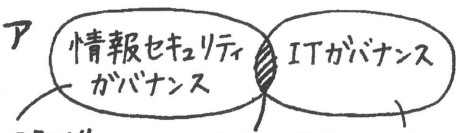
情報セキュリティマネジメント

模試解説講義

解説予定の問題

- 科目A
  - 問1, 3, 9～11
    13～15, 18～20
    23, 24, 26
    29, 34, 36
    37, 38, 41
- 科目B
  - 問49, 51～53
    55, 58～60

問3 ア



JIS Q 27014

重複する

JIS Q 38500（情報技術－ITガバナンス）

JIS Q 27017

クラウド固有の情報セキュリティ管理策

問10 ア 無線LANのセキュリティ

プライバシーセパレータ機能

イ：WPA2, WPA3
- エンタープライズモード（認証サーバを使用）
- パーソナルモード（PSKを使用）

事前共有鍵

例）WPA2-PSK(AES)
[規格][認証方式][暗号化方式]

ウ：MACアドレスフィルタリング
エ：SSIDステルス（ESSID）← 隠す

} 部外者の接続を防止

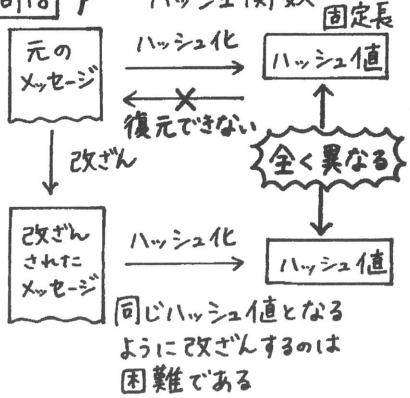
問11 エ E D R
端末 検出 対応

ア：SPF：送信元ドメインの偽装を防止する

イ：APT：高度かつ持続的な攻撃

ウ：CWE：共通脆弱性タイプ一覧

問18 ア ハッシュ関数



同じハッシュ値となるように改ざんするのは困難である

情報処理 講義録	コース・講義等	情報セキュリティマネジメント	科目	模試解説	回数	1

配布物	★テスト類：[ ]	講師	三ツ矢 先生
	★その他の配布物1：[ ]		
	★その他の配布物2：[ ]		

黒板内容

問19 ウ OCSP (Online Certificate Status Protocol)

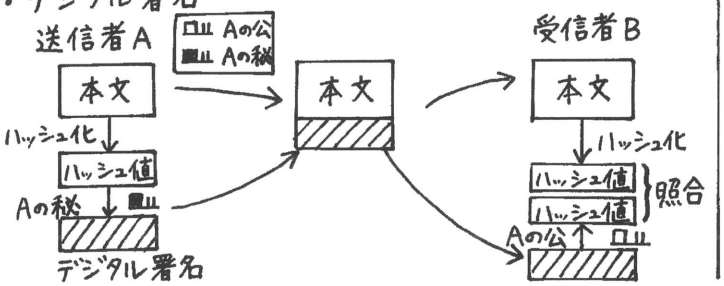
電子証明書の失効情報の問合せに用いるプロトコル

イ：CAPTCHA（キャプチャ） ~~FAC~~ 利用者が人間であることを確認するしくみ

問20 ウ FIDO（ファイド）(First IDentity Online)

本人確認を利用者の端末で行い、その結果にデジタル署名を付けてサーバに送信する方式

・デジタル署名



問24 ⑦ ✕ ア：SMTP-AUTH → S/MIME を用いることで

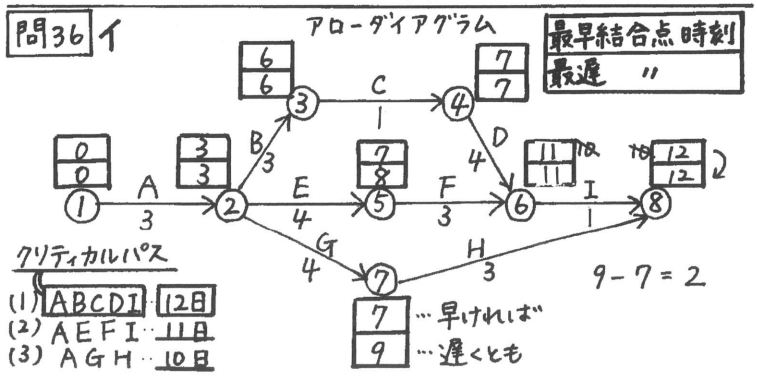
SSH ✕ イ：SPF → DKIM では デジタル署名を付与

✕ エ：TLS(SSL/TLS)：サーバ認証が先

公開鍵認証も利用できる

問29 イ
- ディスインフォメーション：意図的なニセ情報
- ミス 〃：勘違いなどによる誤情報
- マル 〃：内容は正しいが悪意のある〃

問36 イ

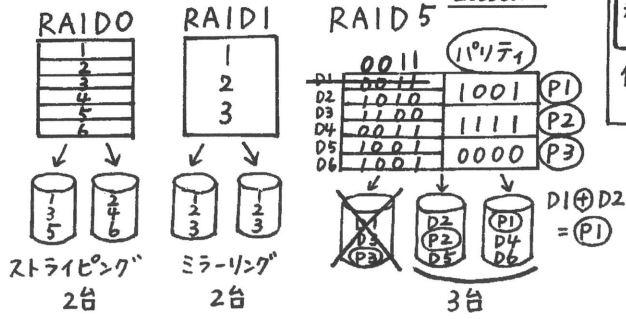


情報処理 講義録	コース・講義等	情報セキュリティマネジメント	科目	模試解説	回数	1

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	三ツ矢 先生

黒板内容

問37 イ RAID



(再2) P3 Lesson 5

問38 ウ

$$稼働率 = \frac{MTBF}{MTBF+MTTR}$$

保守後 $\frac{96}{96+4} = 0.96$ (比率)

保守前

MTBF：$96 \div 1.6 = 60$

MTTR $4 \div 0.6 = 6.66 = \frac{40}{6} = \frac{20}{3}$

保守前の稼働率

$$\frac{60}{60+\frac{20}{3}} = \frac{180}{180+20} = 0.9$$

問41 (イ)

IPアドレス 192．168．1．0

32ビット [8ビット][8ビット][8ビット][8ビット]

サブネットマスク 255．255．255．0

2進数 11111111 11111111 11111111 00000000

ネットワーク部 / ホスト部

問49 3原則のポイント

(1) 経営者のリーダーシップのもとで対策を進める

(2) サプライチェーン全体にわたるサイバーセキュリティ対策の目配りが必要

(3) 関係者との積極的なコミュニケーションが必要

問51 b……(ニ)

絞る イ．(オ)．ク

a…1，3，4

問55 FQDN

www.tac-school.co.jp

ホスト名 / ドメイン名

FQDN

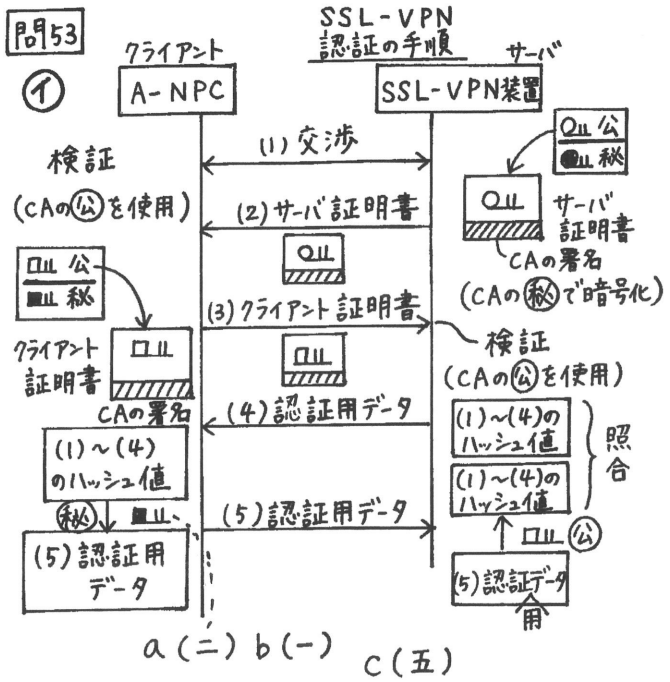
問58 最大値↓

対策	機	完	可	重	脅	脆	被	リスク値
暗号化なし	a [2]	b [2]	0	c [2]	3	2		
暗号化あり	a [2]	b [2]	0	c [2]	3	d [1]	e [2]	f [4]

情報処理 講義録	コース・講義等	情報セキュリティマネジメント	科目	模試解説	回数	1

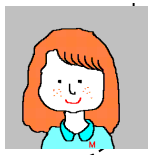
配布物	★テスト類：[ ]	講師	三ッ矢 先生
	★その他の配布物1：[ ]		
	★その他の配布物2：[ ]		

黒板内容



●令和 6 年度秋期 Web 模擬解説〔テスト区分：E4AA〕

- 120 分間、集中力を持続できましたか？
- 解きやすい問題を優先できましたか？
  （判断に迷う問題、時間のかかりそうな問題は後回しにしましょう！）
- 科目 B の問題では、効率よく問題文や設問のポイントをつかめましたか？
- 時間は足りましたか？　時間配分は適切でしたか？
- 早とちりや、うっかりミスはありませんでしたか？
  （解けるはずの問題でミスをしたらもったいないですね。）
- ★ 模擬試験を通してご自身の弱点などを発見し、
  今後の試験対策に活かしていきましょう。



解説講義で取り上げる問題

●科目 A 問題 … 問 1, 3, 9, 10, 11, 13, 14, 15,
18, 19, 20, 23, 24, 26, 29,
34, 36, 37, 38, 41

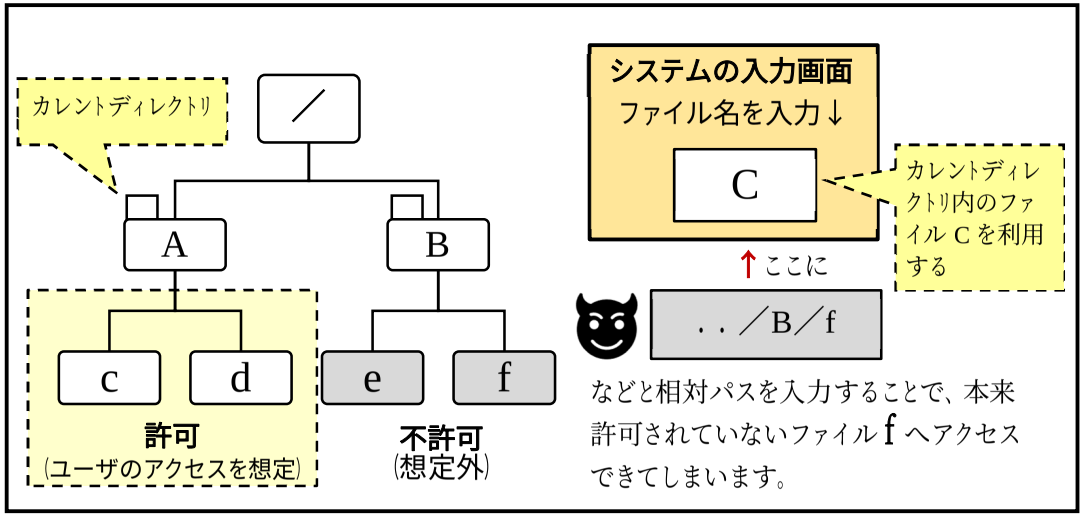
●科目 B 問題 … 問 49, 51, 52, 53, 55, 58, 59, 60

Lesson1　問 9：TPM（Trusted Platform Module）とは　****

TPM とは、コンピュータのプロセッサ内、またはマザーボード上に搭載されているセキュリティチップ（半導体部品）のことです。データの暗号化と復号、鍵ペアの生成、ハッシュ値の計算、デジタル署名の生成・検証などの機能をもっています。
また、従来は補助記憶装置上に格納していた暗号鍵などの情報を安全に格納・管理することができます。 例えば、ハードディスクのデータを暗号化したとき、復号鍵を同じハードディスク内に保存するのではなく、TPM に保存することで、万一ハードディスクが盗難にあった場合でも安全です。

Lesson2　問 14：ディレクトリトラバーサル攻撃　**********

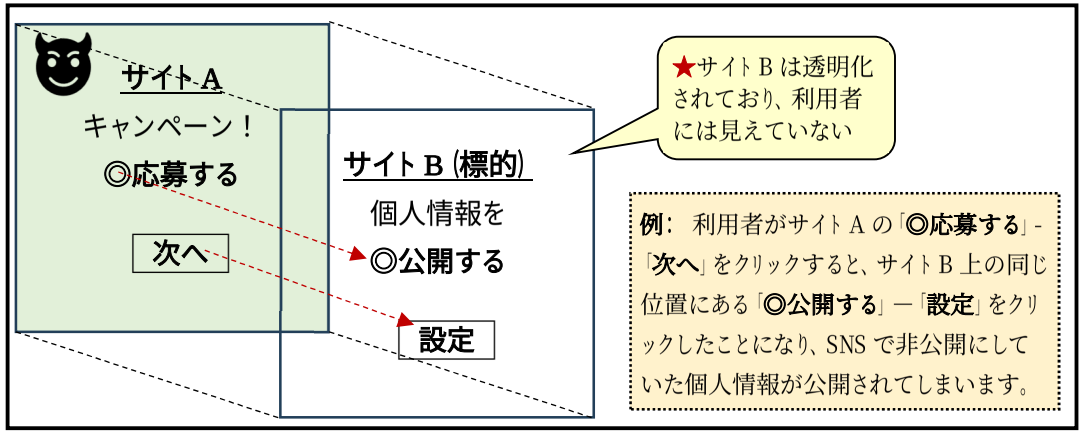
ディレクトリトラバーサル攻撃とは、パス付きのファイル名を指定することで，許可されていない（想定外の）ファイルへアクセスする攻撃です。



などと相対パスを入力することで、本来許可されていないファイル f へアクセスできてしまいます。

Lesson3　問 14 関連：クリックジャッキング攻撃　**********

クリックジャッキングとは、利用者が開いた Web ページのコンテンツ上に標的サイトの Web ページのコンテンツを透明な状態で重ねて読み込ませ、標的サイト上で利用者の意図しない操作を行わせる攻撃です。



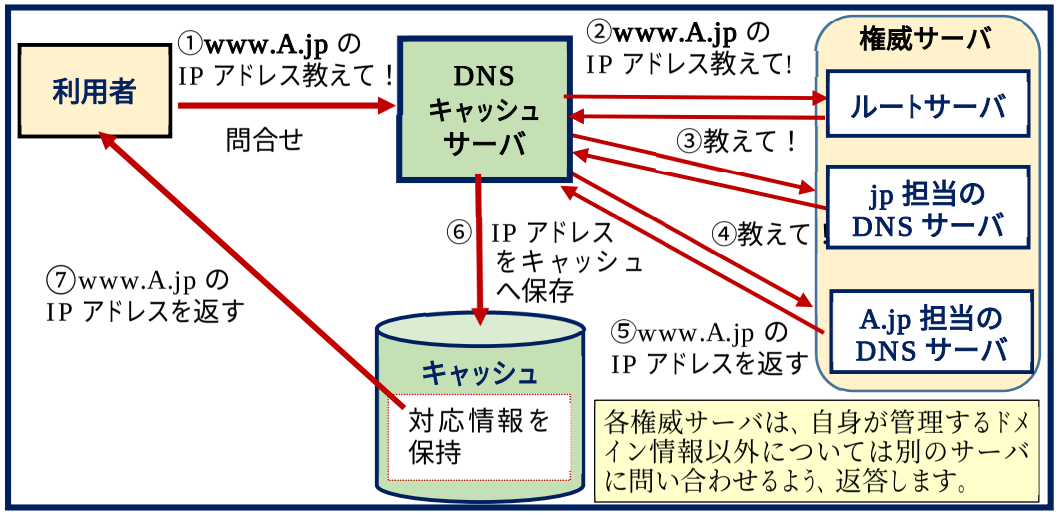
問 14 のその他の選択肢 ↓

●**クリプトジャッキング攻撃**：他人のコンピュータをマルウェアに感染させ、他人のコンピュータの CPU 能力を勝手に利用して、暗号資産を稼ぐ（マイニングを行う）ことです。

●**プロンプトインジェクション攻撃**：生成 AI に対し、悪意のある質問や指示を与えることにより、不適切な回答を出力させたり、意図しない動作をさせたりする攻撃のことです。

Lesson4　問 15 関連：DNS の仕組み（知識の確認）

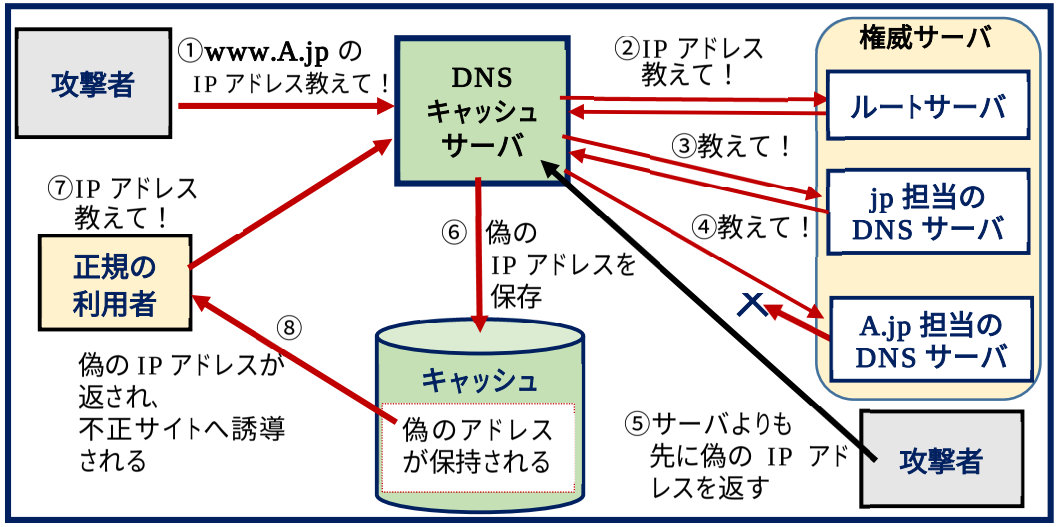
DNS では、ドメイン名と IP アドレスの対応情報を階層ごとに分散して保持しています。DNS キャッシュサーバが利用者からの新しい問合せに対応する IP アドレスを得るときには、ルートサーバから順番にたどっていくことで、必要な情報を得ることができます。



DNS 関連の主な攻撃手法

(1) DNS キャッシュポイズニング

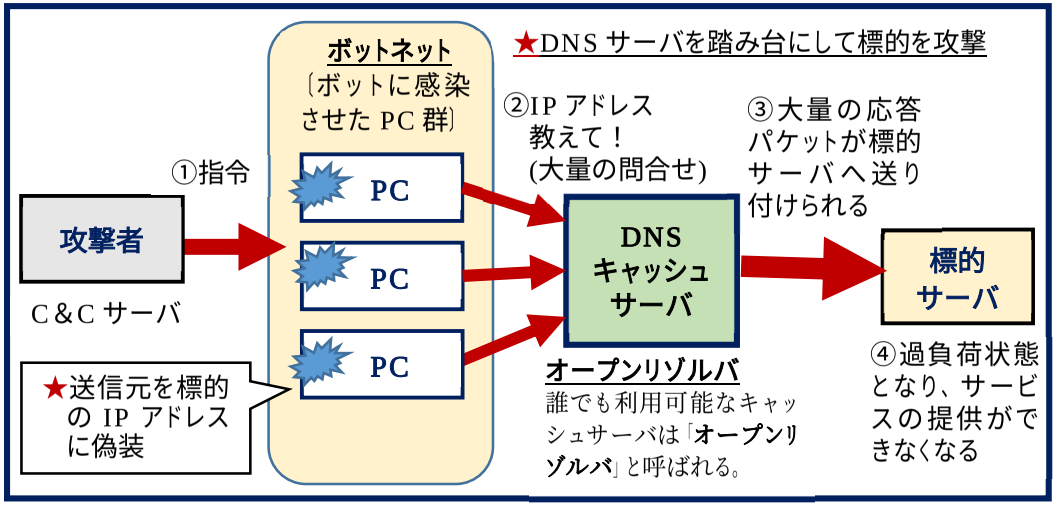
ドメイン情報を管理する DNS キャッシュサーバに偽の情報を記録させる攻撃です。



★DNS サーバのキャッシュが汚染され、偽の IP アドレスが返されることにより、正規の利用者が不正サイトへ誘導されてしまいます。（直接の被害を受けるのは、**利用者**です。）

(2) DNS リフレクタ攻撃（DNS リフレクション攻撃 ・ DNS amp 攻撃ともいう）

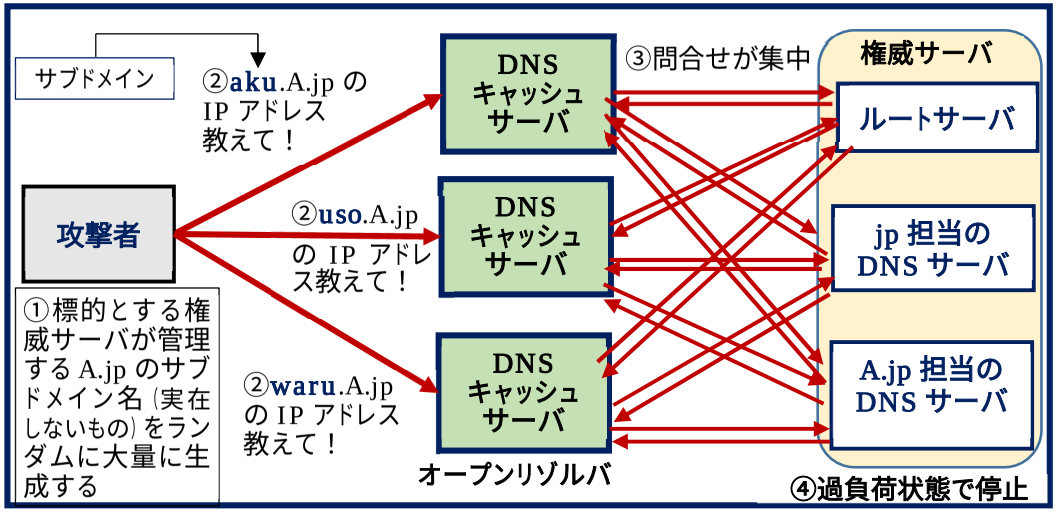
標的とするサーバからの問合せに偽装した問合せパケットを**オープンリゾルバ**（誰でも利用可能となっている DNS キャッシュサーバ）に大量に送信し、DNS サーバからの応答パケットを標的サーバに一斉に送り付けてサービスを停止させる攻撃です。



★DNS リフレクタ攻撃で直接の被害を受ける対象となるのは、**標的サーバ**です。

(3) DNS 水責め攻撃（ランダムサブドメイン攻撃）…権威サーバに対する DDoS 攻撃

標的とする権威 DNS サーバが管理するドメインのサブドメイン名をランダムに大量に生成し、多数の**オープンリゾルバ**（誰でも利用可能な DNS キャッシュサーバ）に問い合わせることで、権威 DNS サーバに問合せを集中させて過負荷状態にし、処理を停止させる攻撃です。



★上記の DNS 水責め攻撃で直接の被害を受けるのは、**権威 DNS サーバ**です。

Lesson5　問 23：SQL インジェクション攻撃の例とその対策 **********

SQL インジェクションとは、入力した文字列をそのまま SQL 文に埋め込むような脆弱性をもつサイトに対し、不正な文字列を入力して任意の SQL 文を実行させ、データの不正取得や改ざんを行う攻撃です。

例：社員名を入力すると、データベースから社員の情報を検索して表示する Web システムを悪用する

(1) Web システム

社員名　田中　一郎　← 入力欄に社員名を入力

・住　所：○○△▽※
・ＴＥＬ：03-****-****
・基本給：28,000

(2) 関係データベースの表

社員表

社員名	住所	TEL	基本給
田中　一郎	○○△▽※	03-****-****	28,000
山田　英司	＊＊＊＊＊	047-***-****	30,000
佐藤　優理	＊＊＊＊＊	03-****-****	22,000
⋮	⋮	⋮	⋮

(3) システムに用意された SQL 文 ↓

```
SELECT *          //*は全ての列を表示する場合//
    FROM   社員表
    WHERE  社員名＝ ’ 田中　一郎 ’
```

★注記 1：Web システム上で入力した文字列がここ（’と’の間）に差し込まれ、SQL 文が実行されます。
★注記 2：’(シングルクォーテーション)は、SQL 文において、検索条件の文字列を囲むために使用する特殊文字です。

(4) ここで、悪意の攻撃者が社員名の入力欄に下記の文字列を入力すると ↓

太田　学’ OR ’X’ ＝ ’X

SQL 文の WHERE 句に上記の文字列が埋め込まれ、

WHERE 社員名＝ ’太田　学’ OR ’X’ ＝ ’X ’

が実行される。（二つの条件が OR で結ばれている）
社員名＝’太田　学’は社員表に存在しないので「**偽**」となるが、**’X’ ＝ ’X’**は常に成立するため「**真**」となる（偽 OR 真 ＝ 真となる）。よって、この SQL 文が実行されると、社員表の全ての行が表示されてしまう。

(5) 対策 1：サニタイジング（無害化）を行う

・入力画面から、’(シングルクォーテーション)などの特殊文字を入力できないようにする。
・特殊文字が現れた場合、処理を中断する。
・特殊文字を無効化する（エスケープ処理）。

★サニタイジングは、**WAF** (Web Application Firewall) の設置などによって、実現できます。

(6) 対策 2：バインド機構を利用する

SQL 文のひな型にプレースホルダ（変数の場所を示す？などの記号）を置いておき、？以外の部分の解析をあらかじめ済ませておく。

例：次のような SQL 文のひな型を用意しておく

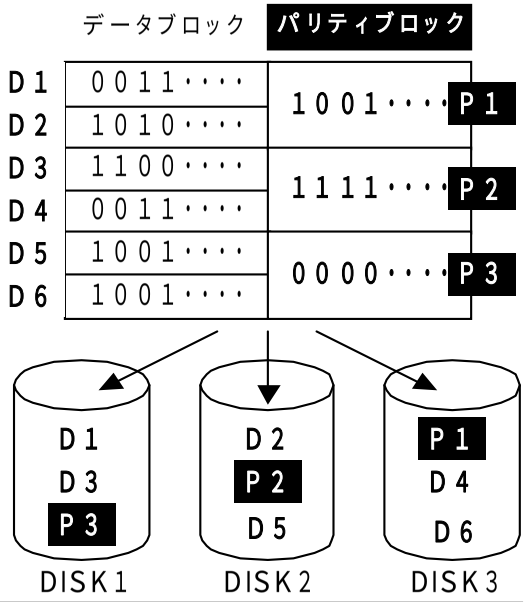
```
SELECT *
    FROM   社員表
    WHERE  社員名＝？
```

Web システムの入力欄に社員名が入力されると、？の部分にその社員名が埋め込まれ、結果が返される。これにより、SQL 文中の’が SQL の特殊文字として解釈されず、攻撃者が入力した文字列全体が「社員名」であると解釈されるため、エラーが返される。

Lesson6　問 37 関連：RAID5 **********

RAID5 とは、1 台の**ハードディスク**が故障しても、残りのデータブロックとパリティブロックから失われたデータを復旧できるしくみです。
ハードディスクは少なくとも 3 台用意しておく必要があります。

3 台構成の RAID5 の場合



例）DISK1 が故障した場合

```
   D2    1010
⊕  P1    1001
   D1    0011
```

D2 と P1 の排他的論理和を求めることにより、D1 が復旧できる！

3 台構成の場合
パリティブロックは、2 つのデータブロックの**排他的論理和**で求める。
片方が 1 のときのみ 1 を返す
（例：D1 ⊕ D2＝**P1**）

```
   D1   0011
⊕  D2   1010
  ------------
   P1   1001
```

排他的論理和では

D1 ⊕ D2＝**P1**
D2 ⊕ **P1**＝D1
P1 ⊕ D1＝D2

となる。

●ポイント：実際にデータを格納できる容量と、パリティの容量の関係

1 組の台数	データの容量	パリティの容量
3 台 1 組	全容量の 3 分の 2	全容量の 3 分の 1
4 台 1 組	全容量の 4 分の 3	全容量の 4 分の 1
5 台 1 組	全容量の 5 分の 4	全容量の 5 分の 1

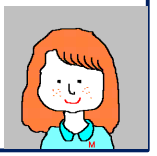
★N 台 1 組の場合、N－1 台分のデータを格納できます。

●科目 B　各問のテーマ・難易度と出題のポイント

***** **********

問	出題テーマ ・ 難易度	出題のポイント
49	**情報セキュリティ基本方針の再検討** 〔★難易度：中程度〕	サイバーセキュリティ経営ガイドライン(Ver.3.0) 経営者が認識すべき 3 原則
50	**脅威とインシデント発生時の初動対応** 〔★難易度：中程度〕	CSIRT 従業員の適切な初動対応 (CSIRT への連絡、証拠保全など)
51	**ファームウェアの脆弱性による不正アクセスの可能性** 〔★難易度：中程度〕	ブロードバンドルータの機能(パケットフィルタリング、NAPT、DNS プロキシ、DHCP サーバ)、ファームウェア
52	**EC サイトの会員登録処理に関する脆弱性調査** 〔★難易度：やや難しい〕	パスワードリスト攻撃 会員登録処理の脆弱性 スクリーニング
53	**SSL-VPN を利用したリモートアクセスの認証手順** 〔★難易度：難しい〕	テレワーク SSL-VPN の認証における通信手順 サーバ証明書、クライアント証明書
54	**ノート PC の盗難による情報漏洩、及びランサムウェア対策** 〔★難易度：やや易しい〕	2 要素認証 ハードディスク全体の暗号化 業務データのバックアップ
55	**パケットフィルタリングを困難にする不正通信の手口** 〔★難易度：中程度〕	プロキシサーバ FQDN の使用によるパケットフィルタリングの回避
56	**IC カードによる入退室管理** 〔★難易度：やや易しい〕	セキュリティレベルと利便性を考慮した入退室管理機能の設定
57	**アクセス権グループごとのアクセス権の判定** 〔★難易度：易しい〕	アクセス権テーブル 流れ図による判定
58	**リスクアセスメントの実施** 〔★難易度：中程度〕	機密性・完全性・可用性の評価値による重要度、脅威と脆弱性による被害可能性、リスク値の算出
59	**BYOD 導入の際の検討事項** 〔★難易度：中程度〕	BYOD アプリが要求する携帯端末のアクセス権限
60	**ビジネスメール詐欺による不正送金の被害** 〔★難易度：中程度〕	ビジネスメール詐欺(BEC) 電子メール偽装の手口 From ヘッダフィールド、Reply-To ヘッダフィールド

MEMO：



●本試験に向けて

問題数と試験時間	・科目 A：48 問と、科目 B：12 問の合計 60 問を、120 分間で解く	
時間配分の目安	・科目 A（小問）： 60 分 60 分／48 問＝1 問当たり 75 秒 （できれば 1 問平均 60～70 秒）	・科目 B（事例問題）： 60 分 60 分／12 問＝1 問当たり 5 分
合格基準点	・総合評価点（科目 A・B の総合点）： 600 点／1,000 点満点	

●「科目 B」問題の解き方　（参考）**********

①問題を解く手順について（一例です）：

【1】 問題文の冒頭を読み、出題テーマや業務の背景（状況や条件）をつかみます。

【2】 設問と解答群を眺め、解答の形式（文章を選択する問題、適切な答えの組合せを選択する問題、空欄を埋める問題など）を把握しておきます。

【3】 解答を導くための詳細部分（図や表の中の細かな内容）に目を通します。

【4】 解答群の中から正しいと思う答えを選び、解答欄の記号をクリックします。

②設問解答のテクニック ：

【1】 計算問題は、紙に書いて計算しましょう。（計算ミスの防止、及び見直しのため）

【2】 空欄を埋める形式の問題などでは、中に入れる字句をある程度予想しておくと効率がよいです。予想できなければ、解答群をヒントにして考えます。（選択肢の中であきらかに問題文の状況に合わないものから消去していくなど。）

【3】 適切な答えの組合せを選択する問題では、一つの答えが見つかるたびに解答を絞り込んでいくと効率が良いです。（解答時間の短縮ができます。）

【4】 適切な解決策を選択する問題などでは、自身の経験や一般的な対応を選ぶと失敗してしまうことがあります。あくまでも、問題の舞台となっている部署の状況に合致する対応を選択すること（条件や状況を踏まえた上で判断すること）を、忘れないようにしましょう。

●今後の対策 **********

①科目 A について：

問題集の問題を解き、必ず解説を読みます。なぜ、その解答になるのか、他の選択肢がなぜ間違いなのかをしっかり理解しておきましょう。

新しい用語や、セキュリティ関連のガイドラインなどについては、テキストやインターネットで調べ、周辺知識もまとめておきましょう。また、最近猛威を振るっているマルウェアの名称や、不正攻撃の最新の手口なども調べておくとベストです。

②科目 B について：

- **主な出題テーマを把握しておく**

科目 B の主な出題範囲は次のとおりであり、これに基づいて技能が問われます。

1 情報セキュリティマネジメントの計画，情報セキュリティ要求事項に関すること

2 情報セキュリティマネジメントの運用・継続的改善に関すること

- **アウトプット学習（問題演習）を繰り返し行う**

問題演習を中心とした学習を行いましょう。

問題集の問題を解き、解説を読んで、勘違いしていた内容や不足していた知識があれば、正しく理解しておきましょう。

- **複数の事例に対応できるよう、知識をストックしておく**

科目 B では、問題ごとに業務の背景や出題テーマが異なるので、頭を切り替えて多くの事例に対応しなければなりません。各問の出題の趣旨を短時間で把握し、適切な解答を導くためにも、問題演習やニュースなどで様々な事例に触れ、知識をストックしておきましょう。

●学習の心得 **********

- 合格するまでの学習プロセスを十分に味わい、楽しみましょう。
  （一つひとつの学習項目と、ご自身の仕事や暮らしとの関わりとを確認しながら理解を深めていっていただければ、“合格”という結果もついてくると思います。）
- 通勤・通学の電車の中など、細切れの時間も有効に使うことを心がけましょう。

●本試験〔CBT 方式〕の申込みについて

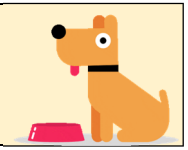
〔1〕**申込み：　随時、インターネットにて受付**

〔2〕**試験日時：**　試験会場によって開催する試験日時が異なります。各試験会場における試験日時は、申込時にご確認ください。

〔3〕**試験会場：**　株式会社シー・ビー・ティ・ソリューションズ（CBTS）が認定する全国の CBT テストセンター　〔最新のテストセンター一覧は申込時にご確認ください。〕

〔4〕**申込方法：**　利用者 ID（マイページアカウント）を作成の上、受験申込みを行っていただきます。受験申込みする月から起算して 3 か月先の月末までの試験日時が選択可能です。 なお、試験の申込みは遅くとも、試験日の 3 日前までに行っていただきます。（申込内容の変更も試験日の 3 日前までは可能です。）

利用者 ID（マイページアカウント）の作成については
下記のページをご参照ください。
https://itee.ipa.go.jp/ipa/user/public/entry/



★ **注意：**登録できる利用者 ID は、一人につき同時に一つのみとなりますので、作成した利用者 ID、パスワードは大切に保管しましょう。
作成した利用者 ID は、情報セキュリティマネジメント試験だけではなく、基本情報技術者試験、応用情報技術者試験、高度試験、情報処理安全確保支援士試験の受験申込みの際にも使用します。　（IT パスポート試験では使用できません。）

受験の流れ、CBT 方式の操作方法については、下記ページをご参照ください。
CBTS 受験者専用サイト：　https://cbt-s.com/examinee/examination/sg

●リテイクポリシー　（再受験についての規定）

〔1〕一度受験した試験区分の再申込みが可能になる日時：
申込み済の試験の終了時刻を過ぎたら、再申込みが可能になりますが、システム処理の都合上、再申込みが可能になるまでには数時間～1 日程度かかります。

〔2〕一度受験した試験区分の再申込み時に、受験日として指定が可能となる日：
前回の受験日の翌日から起算して 30 日を超えた日以降を、受験日として指定可能です。（受験日から 30 日を超えた日であれば、再受験が可能です。）

●試験当日の留意事項

本人確認書類（顔写真付き証明書）を必ず持参してください。

試験中にメモを取ることができますが、その際には会場受付で配布されたメモ用紙とボールペンを使用しなければなりません。追加のメモ用紙が必要な場合は試験監督者に合図をすれば、追加のメモ用紙を渡してもらえます。 なお、このメモ用紙は持ち帰ることができません。試験終了後、ボールペンとともに試験監督者へ返却します。

●評価点の確認と合格発表について

- 試験終了後、CBT の画面上に「総合評価点」が表示されます。
  〔この時点では“合否”は表示されませんが、総合評価点が 1,000 点満点中、600 点以上であれば、ご自身でも“合格”と判断することができます。〕
- 正式な合格発表は、受験月の翌月中旬を予定しています。
- 合格者には、経済産業大臣から「情報処理技術者試験合格証書」が交付されます。
- 合格証書の発送時期は、合格発表後、IPA のホームページに掲載されます。合格証書は試験申込時に登録した住所に簡易書留で送付されます。

★ **なお、試験の最新情報については、必ず IPA の Web サイト等をご確認くださいますよう、お願いいたします。**

〔1〕**試験制度、合格発表、合格証書等に関するお問い合わせ：**
独立行政法人　情報処理推進機構（IPA）：**https://www.ipa.go.jp/shiken/**

〔2〕**受験申込みに関するお問合せ：**
株式会社シー・ビー・ティ・ソリューションズ(CBTS)：　受験サポートセンター
TEL 03 - 4500 - 7862　（08:30～17:30　※年末年始を除く）

★ 一番大切なことは、最後まであきらめないことです。
1 問でも多く正解しよう　という気持ちで、あきらめずにベストを尽くせば、きっと良い結果が待っていますよ。 応援しています！

♪　**当日は、試験問題を楽しんで！！**