講義録レポート

講義録コード　04-52-1-301-01

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	2025年春期(上期)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	2　枚
			補助ﾚｼﾞｭﾒ枚数	6　枚
			その他	0　枚

講義構成	解説1 (67分) → 休憩 (10分) → 解説2 (89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	三ッ矢 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6, 8～12, 14, 16, 19, 21, 22, 24, 26, 27

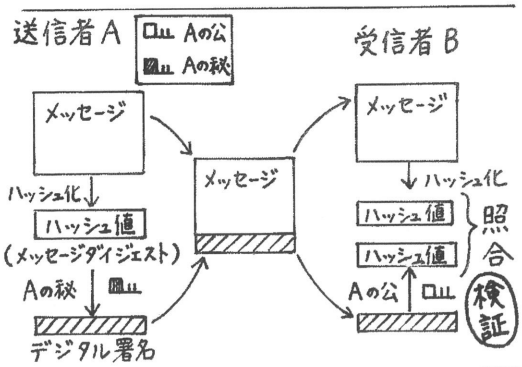
29, 32, 33 34, 43, 47

- 科目B

問50～53 56, 58～60

問12関連 デジタル署名

メッセージ認証＋秘密鍵による本人認証



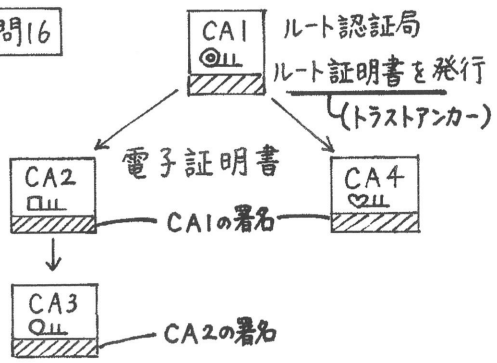
問14 FIDO認証 (配) P3 Lesson6

エ：リスクベース認証

イ：3Dセキュア

ア：トランザクション署名 (配) P3 Lesson7

問16



問19 (エ)

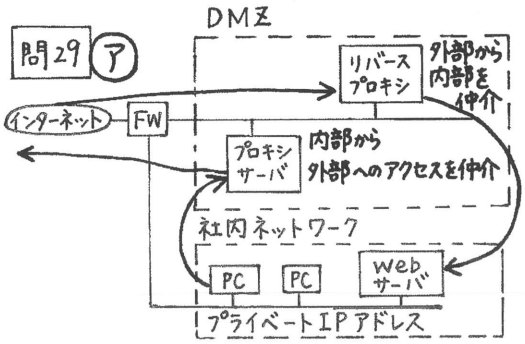
	営 3ビット	開 3ビット	削 3ビット
8進数	7	6	6
↓			
2進数	1 1 1	1 1 0	1 1 0
		読 書 削	
	7	⑦	6

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	三ッ矢 先生

黒板内容

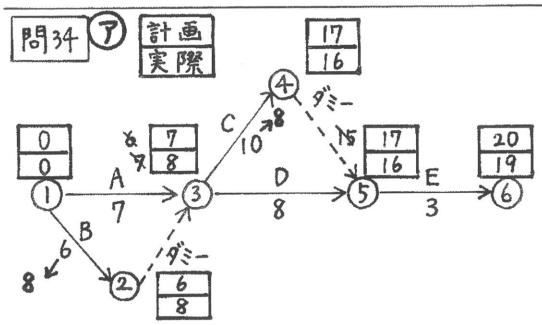
問29 ア



問32 オープンデータ

三要件
- ①営利目的・非営利目的を問わずに、二次利用が可能なルールが適用されたもの
- ②機械判読に適したもの
- ③無償で利用できるもの

問34 ア



問43

- 地政学的リスク
  国の立地や政治情勢などに起因するリスク
- レピュテーションリスク
  評判リスク・風評リスク
- ソブリンクラウド
  自国の法律に準拠して運用を行えるようなクラウド環境

問50 キ

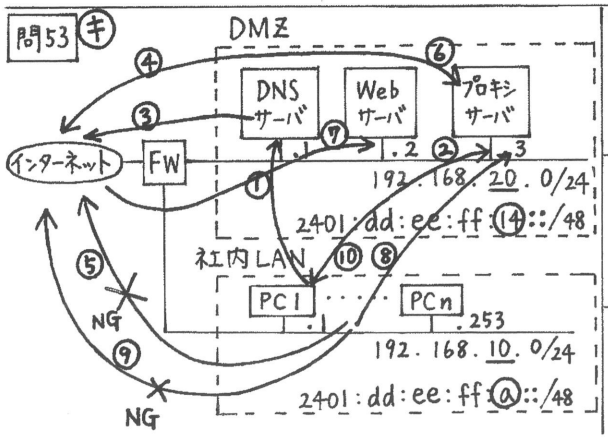
表2 情報資産のリスク値

対策	機	完	可	重要度	脅威	脆弱性	被害発生可能性	リスク値 (キ)or ク
暗号化していない	2	2	1	a 2	2	b 3	2	c 4 (2×2)
暗号化している	2	2	1	a 2	d 2	1	e 1	f 2 (2×1)

表1 被害発生可能性決定

脅威＼脆弱性	③	2	1
3	3	2	2
2	②	1	① e
1	1	1	1

問53 キ



問51 オ

- 氏名は削除すべき
  - ① → ア, ウ, オ に絞る
  - 利用日時・利用店舗はカエ不要 → (ハイフン) → オ に絞る

問52 エ

- 3-2-1ルール(バックアップ方法)
  - データは3つ用意(オリジナルとコピー2つ)
  - 2つのコピーは異なる媒体に保存
  - コピーのうち1つは遠隔地に保存

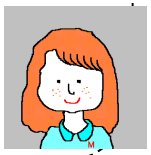
問60 キ

クライアント証明書のしくみ (配)P4
- 機能4：有効 オ or キ

Lesson 12

●令和 7 年度春期 Web 模擬解説〔テスト区分：E5A1〕

- 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 6, 8, 9, 10, 11, 12, 14, 16,
19, 21, 22, 24, 26, 27,
29, 32, 33, 34, 43, 47

●科目 B 問題 … 問 50, 51, 52, 53, 56, 58, 59, 60

Lesson 1　問 8：二重脅迫（ダブルエクストーション）とは　***

二重脅迫型ランサムウェアとは、次のように、二重に身代金を要求するタイプのランサムウェアのことです。

(1) 他人のデータを勝手に暗号化するなどして使用できなくし、復旧させてほしかったら、そのための費用を支払うことを要求する。

(2) さらに、あらかじめ盗んでおいたデータを外部に公開されたくなかったら、費用を支払うことを要求する。

Lesson 8　問 24：WORM（Write Once Read Many）とは　***

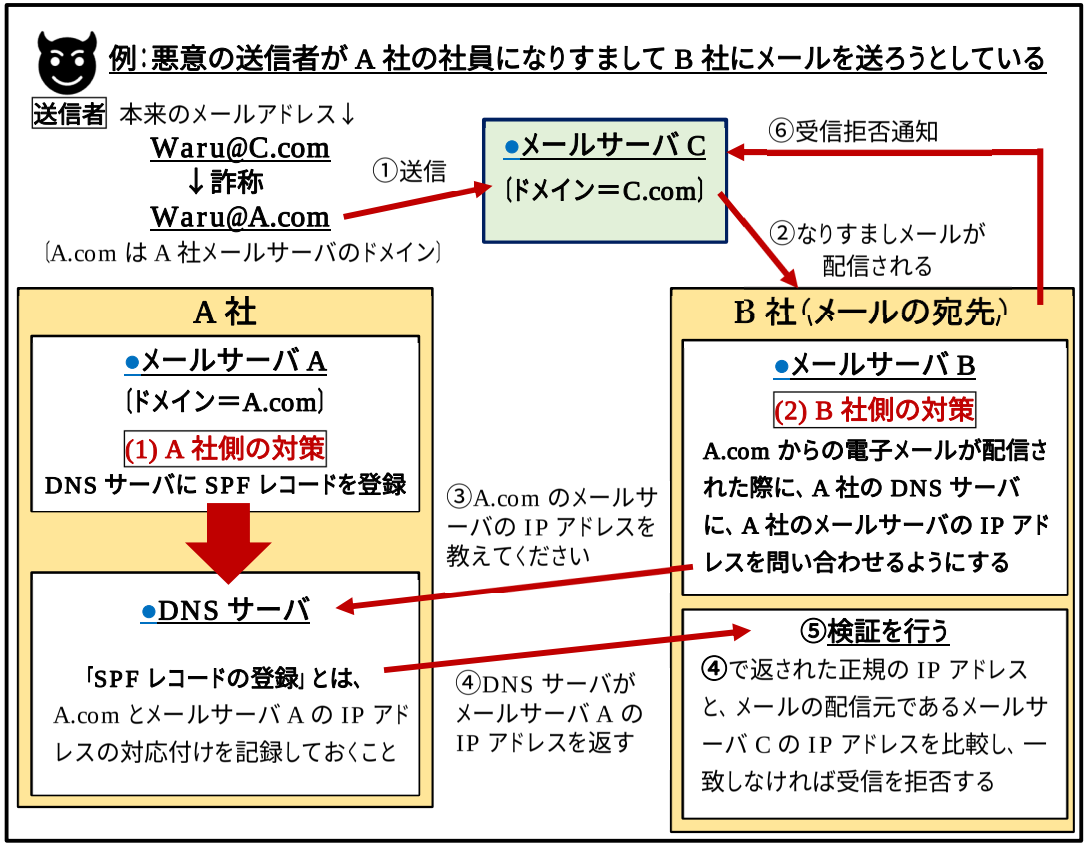
WORM とは、一度書き込んだデータを後から変更したり、消去したりすることができないようにする機能のことです。データの改ざんや、**ランサムウェア**などへの対策として有効です。（データの読出しが可能なため、記憶媒体の廃棄手段としては不適切です。）

Lesson 9　問 27：ベイジアンフィルタリングとは　**********

ベイジアンフィルタリングとは、迷惑メールのフィルタリングに用いられる手法の一つです。大量のメールを学習データとして使用し、統計理論の一つであるベイズの定理を用いて、各単語が迷惑メールに含まれる確率などを計算し、迷惑メールの判定を行います。

Lesson10　問 27 関連：SPF（Sender Policy Framework）とは　*

SPF は、電子メールの送信元ドメインが偽装されていないかを検証する仕組みです。
DNS サーバにメールサーバの IP アドレスを登録しておき、照合することで検証を行います。



Lesson11　問 27 関連：DKIM（DomainKeys Identified Mail）　*

DKIM は、電子メールの送信元ドメインの認証と、**改ざんの検知**を行う仕組みです。送信元のメールサーバでメールにデジタル署名を付けて送信し、受信側でそれを検証します。

送信サーバは自身の秘密鍵を用いて送信メールにデジタル署名を付加し、受信サーバは、送信元ドメインの DNS サーバに問い合わせて公開鍵を取得し、署名を検証します。認証結果は、メールヘッダーに記述されるため、受信者はメールの正当性を確認できます。

Lesson2　問 10 関連：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。

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：〇〇△▽※
・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	〇〇△▽※	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

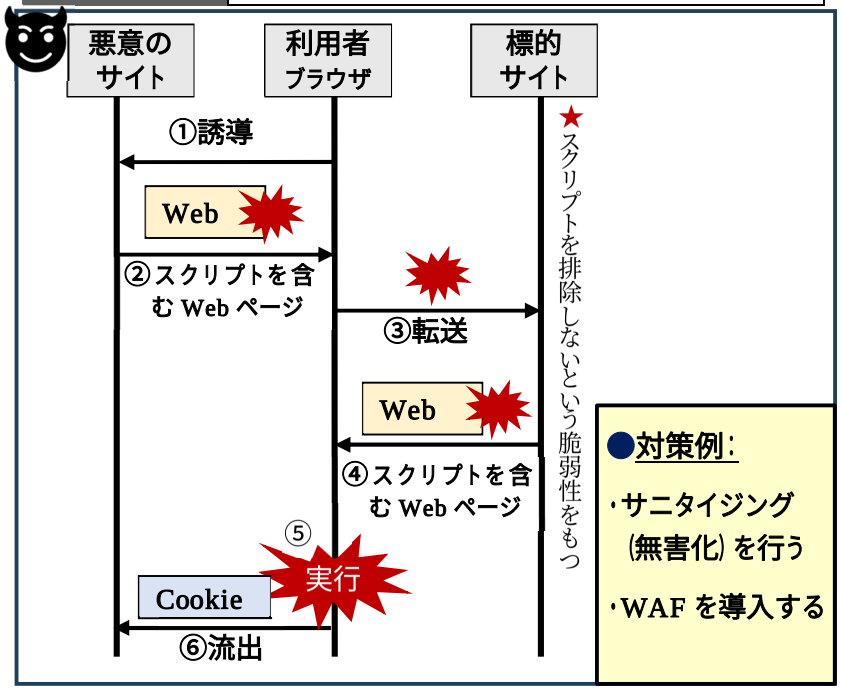
SQL 文のひな型にプレースホルダ（変数の場所を示す？などの記号）を置いておき、？以外の部分の解析をあらかじめ済ませておく。

例：次のような SQL 文のひな型を用意しておく

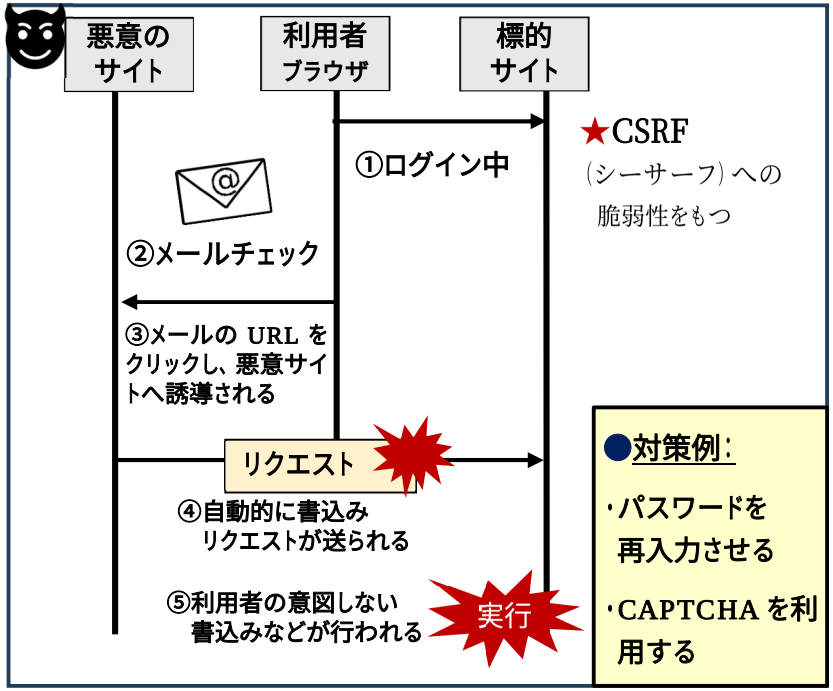
```
SELECT *
    FROM   社員表
    WHERE  社員名＝？
```

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。

Lesson3　クロスサイトスクリプティング（XSS） **



Lesson4　クロスサイトリクエストフォージェリ **



Lesson5　問 12：メッセージダイジェスト **

メッセージダイジェストとは、ハッシュ関数によって変換された値であり、ハッシュ値とも呼ばれます。デジタル署名やメッセージ認証において、メッセージの改ざんの有無を確認する（改ざんの検知の）ために用いられます。

●ハッシュ関数の特徴：

・元のメッセージが少しでも改ざんされると、ハッシュ値は全く異なるものになる。
・異なるメッセージから同じハッシュ値が得られる確率は極めて低い。
・ハッシュ値から元のメッセージを復元することはできない（一方向である）。

Lesson6　問 14：FIDO（ファイド）認証とは

FIDO（Fast Identity Online）認証とは、パスワードに代わる本人認証技術です。生体認証や公開鍵認証を組み合わせて利用することで、安全なパスワードレス認証を可能にしています。

●FAID 認証の主な手順：

事前準備　・利用者がスマートフォンや PC 内の認証器で生体認証などによる本人認証を行うと、秘密鍵と公開鍵のペアが生成される。
・事前の利用者登録によって、サーバ側には公開鍵が保持され、利用者側の認証器には秘密鍵が保持される。

ログイン時　・利用者は認証器で本人認証を行った結果を秘密鍵で暗号化したデータ（**デジタル署名**）をサーバに送信する。
・サーバは事前に登録されている認証器の公開鍵で署名の検証を行い、検証結果が正しければログインを許可する。

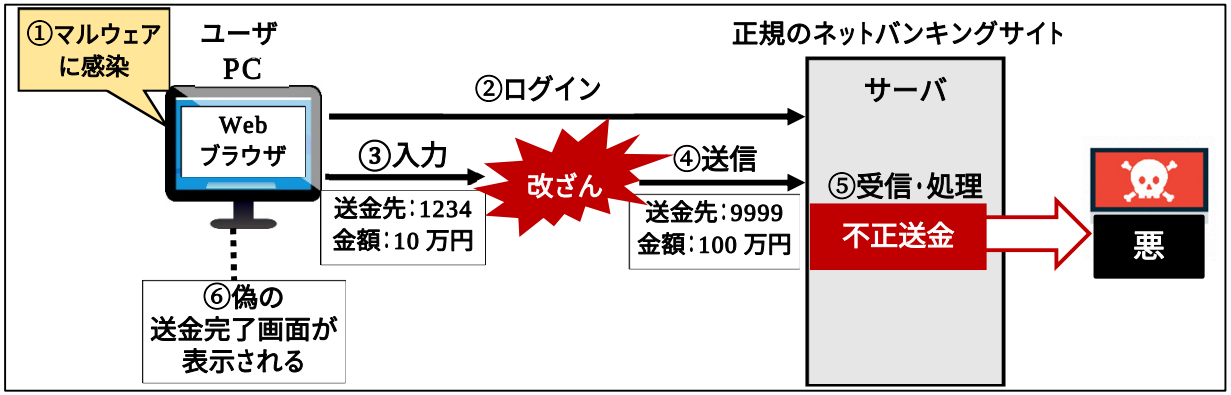
●FIDO 認証の利点：

FIDO 認証では、生体認証などの認証は利用者の端末（認証器）上で完結しており、その確認結果だけを暗号化して送るので、利用者の生体情報などの秘密情報がネットワーク上に流れることもなく、第三者に情報を盗まれるといったリスクを低減できます。

現在では、Web ブラウザ上で FIDO 認証が可能な、FIDO2（ファイドツー）も利用されています。

Lesson7　問 14 関連：MITB（Man-In-The-Browser）とその対策 *********

MITB は、マルウェアに感染した PC が正規のネットバンキングサイトのサーバにアクセスした際に、通信セッションが乗っ取られ、送金先の口座番号や送金金額の改ざんなどが行われてしまう攻撃です。

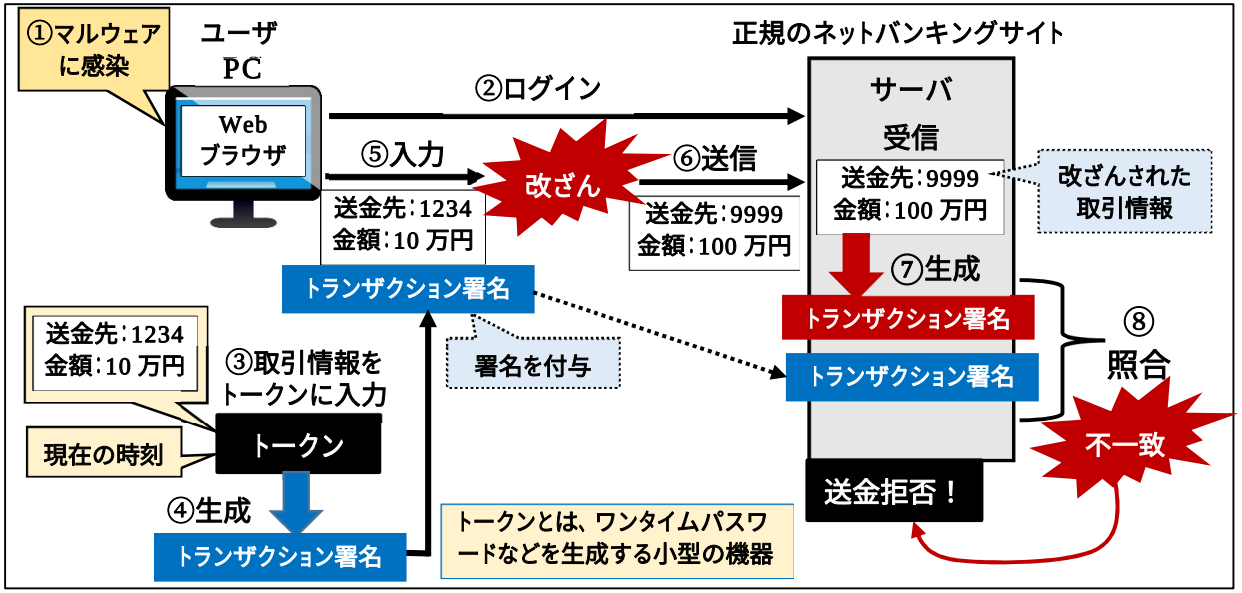


★**ポイント：**　フィッシングとは違って、偽サイトではなく正規のサイトにログインした後に通信セッションを乗っ取るので、攻撃者はパスワードを盗む必要もなく、認証機能を強化しても効果が得られません。

↓

MITB 攻撃への対策・・・トランザクション署名 **********

ユーザが入力する取引情報（送金先の口座番号や金額など）から「トランザクション署名」を生成して付与することにより、サーバ側で「改ざんの検知」と「送信者本人の確認」を行う仕組み。



★**ポイント：**　PC に感染したマルウェアによって偽の署名が作成される危険性もあるため、PC とは別のデバイス（トークン）で安全に署名を作成し、これを Web ブラウザ上で入力しています。

●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	**インターネット経由でのシステム利用の検討** 〔★難易度：易しい〕	ワンタイムパスワード、IDS、アカウントロック、リモートワイプ機能
50	**リスク分析** 〔★難易度：中程度〕	脅威と脆弱性の評価値、被害発生の可能性、リスクの算出
51	**匿名加工情報への加工手法** 〔★難易度：中程度〕	匿名加工情報の加工手法と加工すべき項目との適切な組合せを考える
52	**ランサムウェアによるサイバー攻撃** 〔★難易度：中程度〕	仮想化ソフト、SPF、DKIM、ランサムウェア、3-2-1 ルール
53	**不自然な通信形跡の判定** 〔★難易度：やや難しい〕	IPv4 と IPv6 とのデュアルスタック、DMZ、プロキシサーバ、ポート番号
54	**貸出ロッカーでの盗難事故** 〔★難易度：やや易しい〕	入退室管理、アカウントロック、ログへの記録、防犯カメラによる録画
55	**社内セキュリティ規程への対応** 〔★難易度：やや易しい〕	VPN 経由の社内 LAN へのアクセス、ルートキット
56	**文書ファイルのアクセス管理** 〔★難易度：中程度〕	アクセス制御、文書の管理 見過ごし･確認ミス
57	**内部不正チェックシートの修正点** 〔★難易度：やや易しい〕	組織における内部不正防止ガイドライン、各部門の責任範囲の見直し
58	**マルウェアによる不正な通信** 〔★難易度：中程度〕	C&C サーバ マルウェアの活動隠蔽の手口
59	**ドメイン名の切替えによるリスク** 〔★難易度：中程度〕	ドメイン名の切替え、フィッシング ドメイン名の有効期限と適切な更新
60	**不正ログイン防止のための設定** 〔★難易度：やや難しい〕	認証機能等の見直し、クライアント証明書、安全なパスワードの設定･管理

参　考　問 53 関連：主なウェルノウンポート番号 **********

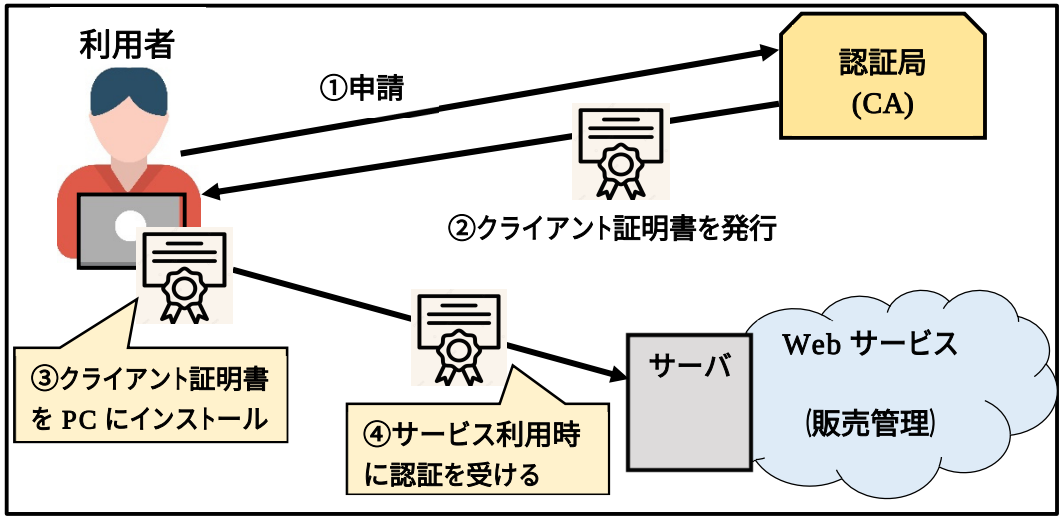
●ポート番号は、TCP で各プログラムを識別するための情報です。
主要なアプリケーションプログラム（アプリケーションプロトコル）に対しては、あらかじめ使用するポート番号が決められており、これらをウェルノウンポート番号と呼びます。

プロトコル	ポート番号	用　途
HTTP	80	Web サイトの閲覧
HTTPS	443	SSL/TLS を利用した Web サイトの閲覧
DNS	53	ドメイン名と IP アドレスの対応を管理･変換
SMTP	25	電子メールの送信･メールサーバ間の転送
POP3	110	電子メールのダウンロード
SMTP	587	電子メールの送信受付 （サブミッションポート） 一般に、SMTP-AUTH による利用者認証が行われる
Telnet	23	リモートログイン･遠隔操作（暗号化･認証機能なし）
SSH	22	リモートログイン･遠隔操作（暗号化･認証機能あり）

★プロキシサーバには「**8080 番**」が使用されることが多いですが、そのほかにも、「80 番」、「1080 番」、「3128 番」などが使用されることもあり、プロキシサーバによって異なります。

Lesson12　問 60 関連：クライアント証明書の仕組み **********

●クライアント証明書は、利用者やデバイスの身元を証明する電子証明書です。これを活用することで、クライアント証明書を持たない端末からのアクセスを遮断することができます。



●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、出題のテーマや業務の背景（状況や条件）をつかむ。

【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）をつかむ。

【3】 解答を導くための詳細部分（図や表の中の細かな内容）に目を通して解く。

【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する。

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

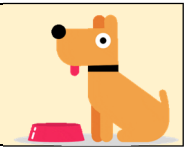
〔1〕**申込み：　随時、インターネットにて受付**

〔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！！