講義録レポート

講義録コード　04-42-1-301-01

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	2024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	4　枚
			補助ﾚｼﾞｭﾒ枚数	5　枚
			その他	0　枚

講義構成	解説1(84分) → 休憩(10分) → 解説2(74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4～6, 9
    12～14, 17, 19,
    20, 22～25
    27～30, 39, 40
- 科目B 44, 48
  - 問50, 51
    54, 55, 56, 57
    59, 60

問4 イ　ISMAP（イスマップ）
ア SECURITY ACTION
ウ CRYPTREC
エ JVN

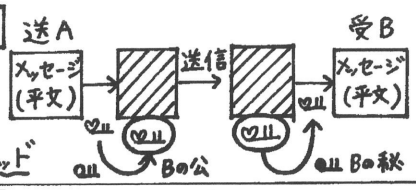
問5 イ JISQ 27017
クラウドサービス固有の情報セキュリティ管理策

問6 ウ
検知(②) → 順位付け(③) → 対処(①) → 報告(④)

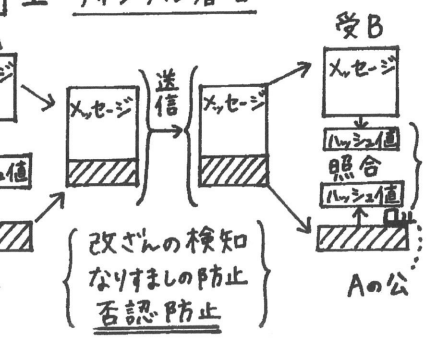
問14 イ
読 書 実
1 1 0

8進	2進
0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

問10 ウ　ハイブリッド



問22 エ　ディジタル署名



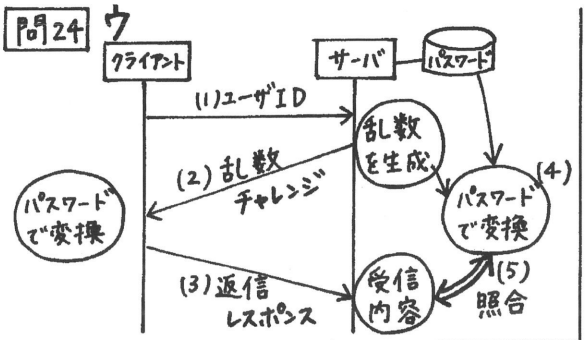
情報処理 講義録	コース・講義等	情報セキュリティマネジメント	科目	模試解説	回数	1

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24 ウ



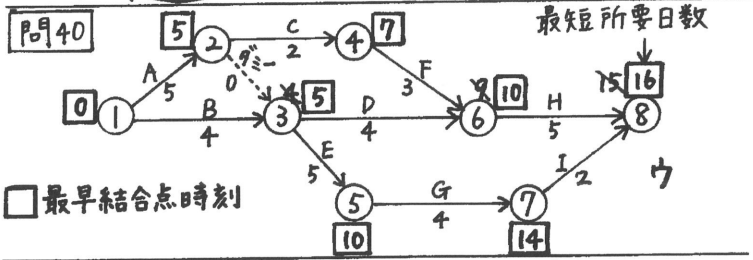
問25 生体認証の測定誤差
工 ・FRR(本人拒否率) 高 低
・FAR(他人受入率) 低 高

問27 ㋑ IPsec 配 P1 Lesson 2
ウ：SPF 配 P1 〃 3

問30 ㋑・SQLインジェクション 配 P2 Lesson 4
ウ・クリックジャッキング 配 P2 〃 5

問39 イ
RTO：復旧時間の目標
RPO：復旧時点の〃

問40



□最早結合点時刻

問48 工 減価償却 配 P2 Lesson 7 定額法
取得原価 $x=100$万円
耐用年数 $S=5$年
使用年数 t → 残存価額
$t=1$：$100-(20\times1)=80$
$t=2$：$100-(20\times2)=60$
$t=3$：$100-(20\times3)=40$
⋮ ⋮

$t=3$のときに結果が40となる式を選ぶ
ア：$100\times5/(5+3)=62.5$
イ：$100\times(5+3)/5=160$
ウ：$100\times5/(5-3)=250$
㋓：$100\times(5-3)/5=$㊵

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

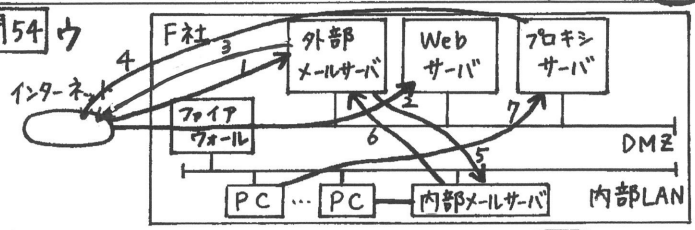
問51 イ a:(−) or (×)

・利用者IDでログイン →(切替え)→ 特権ID →(切替え)→ 利用者ID
(利用者固有) (4名で共有)

→ ・ログファイルに保存
・他のサーバ管理者が特権IDに切り替えて使用している間は切替コマンドは使用できない.
→ 4名のうち誰かを特定可能

b: (×) or (四) or (×)

問54 ウ



項番1 → (5)
項番6 → 3
項番7 → 4
(配) P3 Lesson 8

(ウ): 外部メールサーバ → 内部メールサーバ (ポート25)
×エ: 外部メールサーバ → 内部メールサーバ ポート110

×イ: 項番4の応答パケット, ×カ: 内部LAN内同士のやりとり

問55 図1の1のリスク低減案
=
(バックアップデータが盗まれて外部に流出)

力

(×), (二), (×) (四) (×)

問56 ウ ① 電子メールによる不正送金の手口

(−) BEC (二) SET※ (三) UTM

② 発覚を遅らせる手口とは?

(×) (×) (六)

関連用語: 3Dセキュア2.0
※ クレジットカード決済時に本人確認のために ワンタイムパスワードを入力させるなどして、不正利用を防ぐしくみ

問59関連 ウ
アライアンス型: ネットワークを流れるデータを監視するタイプ

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57 ウ　規則違反に該当するもの

(i) PCを放置し離席　~~申請せず~~　~~推測できる単語~~　(iv) 製品情報の持ち出し　~~フィルタ不使用~~　(vi) パスワードの文字種

問60 ○(一)DBの脆弱性診断の実施 OK

イ ○(二)アプリの 〃 OK

(三)結果の報告

	診断月	報告期限	報告日	
DB	7月	2か月以内	7月末	OK
アプリ	4月	1か月以内	7月末	NG

NG

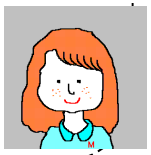
(四)結果の対応

	検出月	脆弱性	対応期限	対応日	申請
NG アプリ	4月	21件(軽微)	発見後1か月以内	8/1	なし
? DB	7月	1件(緊急)	〃 1週間以内	8/1	なし

NG

●令和 6 年度春期 Web 模擬解説〔テスト区分：E4A1〕

- 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

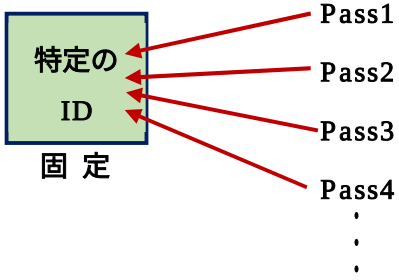
●科目 A 問題 … 問 4, 5, 6, 9, 12, 13, 14, 17,
19, 20, 22, 23, 24, 25, 27,
28, 29, 30, 39, 40, 44, 48

●科目 B 問題 … 問 50, 51, 54, 55, 56, 57, 59, 60

Lesson 1　問 13：リバースブルートフォース攻撃 **********

● ブルートフォース攻撃（総当たり）

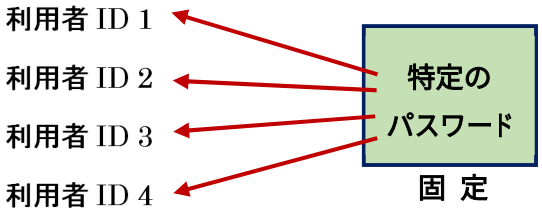
パスワードとして次々に文字列を入力



★有効な対策：アカウントロック

● リバースブルートフォース攻撃

パスワードを一つ選び、利用者 ID として次々に文字列を用意して総当たりにログインを試行する



★各利用者 ID に対しては、1 回ずつ試行するだけなので、アカウントロックでは不正ログインを防ぐことができない。

Lesson 2　問 27：IPsec（Security Architecture for Internet Protocol）

IPsec は、OSI 基本参照モデルの**第 3 層**(ネットワーク層)で動作する **IP** にセキュリティ機能を付加したプロトコルであり、次のような複数のプロトコルで構成されています。

IPsec
- **AH（認証ヘッダ）：メッセージの認証を行う**
- **ESP（暗号化ペイロード）：メッセージの認証と暗号化を行う**
- **IKE（鍵交換方式）：自動的に鍵の交換を行う**

●**参考**：IPsec には、次の 2 つのモードがあります。

(1) **トランスポートモード**：パケットの IP ヘッダを除いたデータ部分を暗号化する

(2) **トンネルモード**：IP ヘッダも含めた全体を暗号化し、新たに IP ヘッダを付与する

Lesson 3　問 27：SPF（Sender Policy Framework）とその対策 *

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。

例：悪意の送信者が A 社の社員になりすまして B 社にメールを送ろうとしている

送信者　本来のメールアドレス↓
Waru@C.com
↓詐称
Waru@A.com
〔A.com は A 社メールサーバのドメイン〕

①送信

●メールサーバ C
〔ドメイン＝C.com〕

⑥受信拒否通知

②なりすましメールが配信される

A 社

●メールサーバ A
〔ドメイン＝A.com〕
(1) A 社側の対策
DNS サーバに SPF レコードを登録

●DNS サーバ
「SPF レコードの登録」とは、A.com とメールサーバ A の IP アドレスの対応付けを記録しておくこと

③A.com のメールサーバの IP アドレスを教えてください

④DNS サーバがメールサーバ A の IP アドレスを返す

B 社（メールの宛先）

●メールサーバ B
(2) B 社側の対策
A.com からの電子メールが配信された際に、A 社の DNS サーバに、A 社のメールサーバの IP アドレスを問い合わせるようにする

⑤検証を行う
④で返された正規の IP アドレスと、メールの配信元であるメールサーバ C の IP アドレスを比較し、一致しなければ受信を拒否する

Lesson4　問 30：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などを行う攻撃です。

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：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  '
```

(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。

★**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。

(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)。

※なお、サニタイジングは、**WAF**(Web Application Firewall)などの設置によって、行われます。

(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。

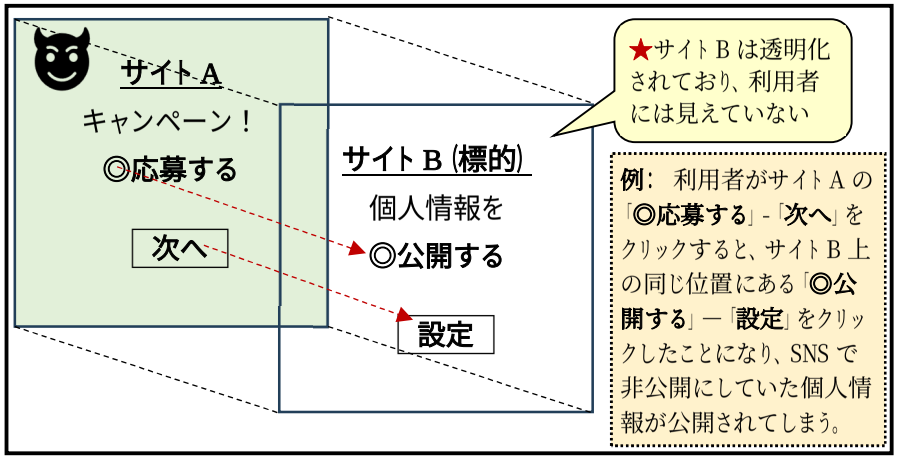
例：　次のような SQL 文のひな型を用意しておく

```
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。

Lesson5　問 30 関連：クリックジャッキング *****

クリックジャッキングは、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。



Lesson6　問 44：主な無線 LAN の種類 **********

規格	使用周波数帯	最大通信速度	呼称
IEEE802.11b	2.4GHz	11M ビット／秒	
IEEE802.11a	5GHz	54M ビット／秒	
IEEE802.11g	2.4GHz	54M ビット／秒	
IEEE802.11n	2.4GHz　5GHz	600M ビット／秒	Wi-Fi 4
IEEE802.11ac	5GHz	6.9G ビット／秒	Wi-Fi 5
IEEE802.11ax	2.4GHz　5GHz	9.6G ビット／秒	Wi-Fi 6

Lesson7　問 48：減価償却（定額法）の例 **********

●取得原価 100 万円、耐用年数 5 年、残存価額 0 の場合：
各年の減価償却費は、100 万円 ÷ 5 年 ＝ **20 万円** となります。

使用年数	減価償却費	残存価額 (未償却残高)
1 年	20 万円	100 － (20 × 1) ＝ 80 万円
2 年	20 万円	100 － (20 × 2) ＝ 60 万円
3 年	20 万円	100 － (20 × 3) ＝ 40 万円
4 年	20 万円	100 － (20 × 4) ＝ 20 万円
5 年	20 万円	100 － (20 × 5) ＝ 0 円

※本問では、t 年間使用した後の残存価額を表す式を求めます。

●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	**メール添付によるファイル共有の問題点** 〔★難易度：やや易しい〕	ZIP ファイルと ZIP パスワード パスワードメールの運用 メール受信拒否の設定
50	**秘密保持契約の見直し** 〔★難易度：中程度〕	秘密保持契約取り交わしのタイミング 転職者採用時の留意点など
51	**ファイルサーバの運用管理** 〔★難易度：中程度〕	リモートログイン 特権 ID 共有時の運用方法
52	**不正ログイン試行の形跡** 〔★難易度：やや易しい〕	パスワード運用規定の強化 ブルートフォース攻撃 リバースブルートフォース攻撃
53	**文書ファイルの管理における現状の問題点** 〔★難易度：やや易しい〕	アクセス権限の設定 運用時のリスク特定
54	**ファイアウォールのフィルタリングルール** 〔★難易度：やや難しい〕	外部メールサーバと内部メールサーバ、プロキシサーバ パケットフィルタリング ウェルノウンポート番号
55	**バックアップシステムへの不正アクセス対策** 〔★難易度：中程度〕	クラウドサービス上のデータ流出に関するリスク対策
56	**電子メールを用いた不正送金の手口** 〔★難易度：中程度〕	BEC（ビジネスメール詐欺） 詐欺の発覚を遅らせるための手口
57	**ノート PC 紛失のインシデントに関する調査** 〔★難易度：中程度〕	機密情報、及びパソコンの取扱いについての規則 違反行為によるリスク
58	**リスクアセスメントの実施** 〔★難易度：易しい〕	機密性・完全性・可用性のリスク値の算出 リスクの評価
59	**機密情報の管理の現状と改善策** 〔★難易度：中程度〕	機密情報を記録したメディア（媒体）の取扱い 不正コピーの防止策
60	**脆弱性診断の実施・報告・対応** 〔★難易度：中程度〕	社内のセキュリティ基準に基づいた自己点検の実施 点検結果の検証

Lesson 8　問 54 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。

ポート番号	プロトコル	用　途
80	HTTP	Web サイトの閲覧
443	HTTPS	SSL/TLS を利用した Web サイトの閲覧
25	SMTP	電子メールの送信・メールサーバ間の転送
110	POP3	電子メールのダウンロード
587	SMTP	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
23	Telnet	リモートログイン・遠隔操作（暗号化・認証機能なし）
22	SSH	リモートログイン・遠隔操作（暗号化・認証機能あり）

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！！**