講義録レポート

講義録コード　04-22-2-301-01

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	2022年秋期(下期)合格目標	科目②	公開模試解説
コース	本科生　本科生Ｂ	回　数	1　回
用　途	ビデオブース　・　テープレクチャー　・　集合ビデオ (ＷＥＢ)　・　DVD通信　・　資料通信		

講師名	三ッ矢 眞紀 先生	講義録枚数	2　枚	※レポート含まず
		補助ﾚｼﾞｭﾒ枚数	4　枚	サイズ(B5)
		その他	0　枚	

講義構成	解説1(56分)　→　休憩(10分)　→　解説2(89分)
使用教材	公開模試　午前/午後問題 公開模試　解答・解説
配付教材(※ビデオブース生)	
備考	

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：[ ]	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

模擬試験解説講義

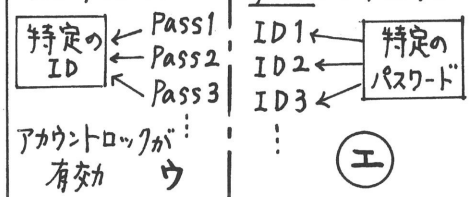
解説予定の問題
- 午前
  - 問1, 2, 5, 6, 7, 8, 11, 13, 19, 22, 24, 26, 27, 28, 36, 37, 40, 42
- 午後
  - 問3
  - 問2 設問1

午前問題

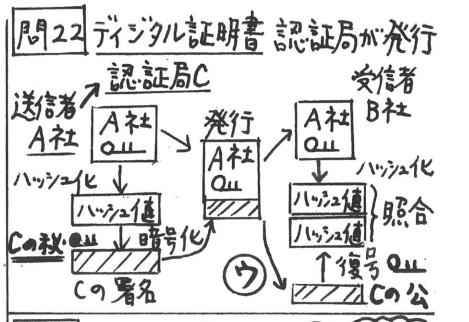
問7 情報セキュリティ監査のガイドライン
- 情報セキュリティ監査基準：監査人の行為規範
- 情報セキュリティ管理基準：監査上の判断尺度

エ
- a マネジメント：基本的な実施事項（JISQ27001（要求事項））
- b 管理策：具体的な管理項目（JISQ27002（具体的な管理策））

問13 リバースブルートフォース攻撃



問22 ディジタル証明書 認証局が発行



問26 フィルタリングテーブル イ 通過

送元IP	あて先IP	送元ポート	あて先ポート	
*	公開Webサーバ	*	443	タ→Webサーバ
公開Webサーバ	*	443	*	Webサーバ→タ

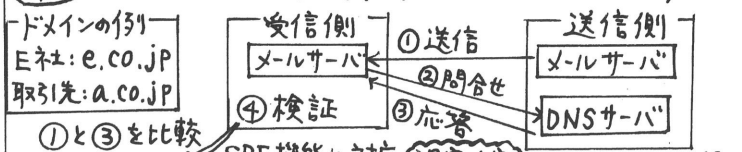
問42 毎日8~22時, 22-8=14時間
1年間では, 14×360日=5040時間
停止は1%未満 5040×0.01=50.4 ア

午後問題

問3 P24~【標的型攻撃メール】
- インシデントの発生
  - P29 設問1(1)a：オ 不自然な通信 ③⑥⑦
- 初動対応
  - P29設問1(2)b：オ 2つを選択 (iii)→(i)
  - (i)○ (ii)× (iii)○ (iv)×
  - (i) ネットワークから切り離す
  - (iii) 証拠を取得
- 調査 P30設問1(3)C：エ
  - Emotet：ワープロ文書などのマクロを悪用
- 対策 P30設問2(1)
  - キ～d：ゼロデイ e：ソーシャル攻撃 ク エンジニアリング

- 対策
  - P31 設問2(2)f：ウ---【管理上の問題点】
  - 〃 (3)g：ウ---【不審なメールへの対処】
  - 〃 (4)h：ウ---【ポート80宛を遮断. 業務に支障あり】
  - j：エ---【 〃 〃 支障なし】
  - j：カ---【より細やかな制御】URLフィルタリング

SPF：送信元ドメインを確認する（ドメイン名の偽装を検知する）しくみ



P32 設問2(5)

k	パターン1の検知	E社 (ii)	取引先 (iii)	k：エ
l	パターン2の検知	取引先 (iv)	E社 (i)	l：ウ

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

午後問題

問2 P13～〔事業継続計画〕とバックアップ〕

・事業継続計画（BCP）〔設問1〕 → ・バックアップの検討〔設問2〕 → ・バックアップデータ移行作業の評価試験〔設問3〕

P19 設問1(1) a：キ 選択しない理由
- ・インターネットVPN：品質・安全性で不安(iii)(iv)
- ・専用線：利用コスト大(ii)

(2) b：カ リスクを洗い出した後 各リスクが事業に与える影響度を分析
c：オ 復旧時間目標〔RTO〕〔ビジネスインパクト分析〕

P20 設問1(3) d：ア e：ア

P16表3より
・代替なし
大＝レベル1
中＝レベル2
・代替あり
大＝レベル2
中＝レベル3

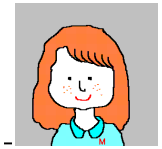
	影響度	代替手段	レベル
案件管理サーバ	大	無し	レベル1
Webサーバ	大	無し	レベル1
メール〃	中	有り f1	レベル3
総務〃	中	有り f2	レベル3
経理〃	大	有り f3	レベル2

P21 設問1(4) 代替手段の内容
f：ク キor⑦絞り込む
- f1：メールサーバの代替手段（v）
- f2：総務〃 (iv)
- f3：経理〃 (iii)

設問1(5) 案件管理サーバ g：オ
2つを選択 (iii)(iv)

●令和４年度 下期試験向　模擬試験解説講義

●午前試験、午後試験の各 90 分間、集中力を持続できましたか？
●午前問題では、易しい問題・定番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！）
●午後問題では、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。）
★模試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予定の問題

●**午前問題**　…　**重点分野**：問 1，2，5，6，7，8，11，13，19，22，24，26，27，28，36
関連分野：問 37，40，42

●**午後問題**　…問 3，　問 2（設問 1）

Lesson1　午前 問６：SECURITY ACTION　**********

IPA が創設した、「中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度」のこと。安全・安心な IT 社会を実現するために創設された。

・1 つ星(★)：「**情報セキュリティ５か条**」への取組みを宣言した場合
・2 つ星(★★)：「中小企業の情報セキュリティ対策ガイドライン」付録の「**5 分でできる！情報セキュリティ自己診断**」で自社の現状を把握した上で、自社の情報セキュリティポリシ（基本方針）を定めて公開したことを宣言した場合

IPA に申し込むことにより、取組み段階に応じたロゴマークを使用することができる（名刺や Web サイト等にロゴを表示して、自社の取組みをアピールできる）。➡

Lesson2　午前 問 24：ＣＷＥ　**********

CWE(Common Weakness Enumeration)は、ソフトウェアにおけるセキュリティ上の弱点（脆弱性）の種類を識別するための共通の脆弱性タイプの一覧である。

CWE では、SQL インジェクション、クロスサイト・スクリプティング、バッファオーバーフローなど、多種多様な脆弱性の種類を脆弱性タイプとして分類し、それぞれに CWE 識別子（CWE-ID）を付与して階層構造で体系化している。

利用者は、脆弱性を識別し、脆弱性の低減を行い、再発を防止するための辞書として、これを活用することができる。

●参 考：TPM とは？　午前 問 24　選択肢“ア”　**********

TPM（Trusted Platform Module）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）、及びその仕様である。

TPM は高い耐タンパ性をもっており，内部データの不正な読取りや改ざんを物理的に防御することができる。 TPM には、データの暗号化と復号，鍵ペアの生成，ハッシュ値の計算，ディジタル署名の生成・検証などの機能が含まれており、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る。 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となる。

Lesson3　午前 問 28：IPsec(IP Security 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る。

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）：自動的な鍵交換を行う**

●**参考：** IPsec には、次の 2 つのモードがある。
(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、新ヘッダを付与する

●午後問題のテーマ・難易度と解答に必要な知識 **********

問	出題テーマ ・ 難易度	解答に必要な知識
1	**顧客情報の管理** 問題文の状況がつかみやすく、比較的素直なインシデント対応の問題である。 個人情報の第三者提供等に関する知識などが必要であるが、難易度は中程度～やや易しいレベル。	顧客情報漏えいの際の初動対応 電子メールの送信先指定〔TO, CC, BCC の使い分け〕 パスワードの（不適切な）管理 オプトイン、オプトアウトの違いについて 個人情報保護法における第三者提供について 情報提供先（業務委託先）との守秘契約など 【★出題のポイント：子会社への個人情報の提供は第三者提供に当たること、通知はオプトアウトでも可】
2	**事業継続計画とバックアップ** 災害時の事業継続計画(BCP)の策定に関して、業務への影響度の評価、業務データのバックアップ計画、非常時対応の評価試験の実施計画など、盛りだくさんの内容が含まれている。 関連分野の知識（コンピュータ共通の前提知識）が必要な設問も多い。 難易度は中程度。	ハウジングサービス、IP-VPN、インターネット VPN ビジネスインパクト分析 RTO（復旧時間目標）、業務への影響度の評価 バックアップサイト〔ホットサイト・コールドサイト〕 バックアップの方法と復旧について〔フルバックアップ、差分バックアップ、増分バックアップの違い〕 【★出題のポイント：問題の背景に応じたリスクの評価、現状を踏まえたバックアップ運用の検討など】 業務委託の際のリスク低減策
3	**標的型攻撃メール** 標的型攻撃メールによるマルウェア感染に関して、初動対応→原因の調査・分析→対応策の検討といった流れの中で、通信ログの分析、マルウェア感染時の措置、セキュリティ管理上の問題点、ファイアウォールの設定による対策、なりすましメールへの対策等についてが、ひととおり問われている。 判断力が必要な設問もあり、難易度は中程度～やや難しいレベル。	DMZ、パケットフィルタリング HTTP（ポート 80）、SMTP（ポート 25）など プロキシサーバ パターンマッチング バックドア 標的型攻撃メールの特徴、 Emotet（エモテット） ゼロデイ攻撃、ソーシャルエンジニアリング C＆C サーバ、SPF、DNS サーバ 【★出題のポイント：攻撃手法の知識を踏まえた上での各種対策の検討、なりすましメール検知のために SPF を利用する際の、送信側・受信側の設定など】

●本試験に向けて

（1）本試験の配点と合格基準点

●午前試験（90 分）：1 問 2 点×50 問　合格基準点＝100 点満点中 60 点
●午後試験（90 分）：1 問 34 点×3 問　合格基準点＝100 点満点中 60 点
〔午後試験は各 34 点×3 問ですが、得点上限は 100 点なので、100 点満点〕

（2）午後試験　解答の導き方【参考です】 ↓

①問題文を効率よく読む

午後試験の長文問題は CBT 方式ですが、ページ数に換算すると、3 問で 40 ページ前後のボリュームになります。

試験当日は、各問に最大 30 分の制限時間を設けて行うとよいです。時間を節約するために「まず設問から読む」という人もいますが、その方法では、本文中の重要な条件を読み飛ばしてしまい、勘違いによるミスが発生する可能性もあります。ストーリーは順番どおりに展開していくので、本文を順番に読み進めて、状況を正しくつかむようにしましょう。 次のような手順で問題を解くと効率が良いと思います。〔注：ハイライトは本試験(CBT)で使用できます〕

【1】本文を最初から読み、背景となる業務システム等の状況を把握する。
【2】管理上の不備や、気になる点にハイライトを設定しながら読み進める。
【3】空欄や下線部が出てきたら、対応する設問を表示し、解答群を見る。
【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。
【5】➡【2】に戻り、問題本文の続きを読み進める。

★この手順を繰り返して、最後の設問まで解いていきます。
★空欄を埋める問題では、空欄に入れるべき字句をある程度予想しておくと、解答群の中から短時間で選ぶことができます。
★1 問当たり 25 分～30 分で解けるよう、繰り返し練習しましょう。

②解答群をヒントにする

設問の内容がわかりにくくても、解答群を見れば出題の意図をつかめることがあります。また、絞り込み法や、消去法で解答を導くこともできます。

③過去問題・練習問題をたくさん解き、問題に慣れること！

解答を導くための材料は、問題文や設問文の中に必ず記述されています。午後問題に慣れてくると、そのような材料をすばやく見つけることができるようになりますよ。

（3）CBT 方式の試験について

●令和 4 年度下期試験までの情報セキュリティマネジメント試験では、上期と下期にそれぞれ 1 か月程度の試験実施期間が設けられ、その期間内で（午前試験）と（午後試験）を 1 回ずつ受験（予約）することができます。

●試験名の（午前試験）（午後試験）は試験名称であり、予約可能な時間帯を示すものではありません。（午前試験）を午後の時間帯、（午後試験を）午前の時間帯に予約することが可能です。また、午後試験を先に受験することも可能です。
だたし、予約は（午前試験）→（午後試験）の順に個別に行います。

●試験実施期間の最終日終了時点において、午前試験、午後試験のどちらか一方しか受験していない場合、その結果を次回に持ち越すことはできず、不合格となります。（実施期間内に午前試験、午後試験の両方を受験する必要があります。）

●CBT 試験実施の詳細は、情報処理推進機構（IPA）の下記サイトをご参照ください。
https://www.jitec.ipa.go.jp/1_02annai/r02sg_exam.html

★なお、CBT 試験実施業務は IPA から「プロメトリック株式会社」に委託されています。

（4）受験申込みについて

★令和 4 年度下期の試験実施期間：

試験科目	申込期間	試験実施期間
午前試験	2022 年 11 月 1 日～12 月 19 日	2022 年 12 月 1 日～12 月 22 日
午後試験	2022 年 11 月 1 日～12 月 20 日	2022 年 12 月 1 日～12 月 25 日

★受付期間中に、プロメトリック株式会社の下記ページにアクセスし、予約を行います。
http://pf.prometric-jp.com/testlist/sg/index.html

●試験会場ごとに試験日が異なるので、ご自身の都合の良い日時に開催予定の試験会場を選んでいただきますが、座席に空きがない場合は予約できません。

●予約は（午前試験）→（午後試験）の順に個別に行う必要があります。

●受験手数料(7,500 円)の支払いは(午前試験)の予約時にのみ必要となります。

●午前試験の予約完了後に午後試験の予約が可能となります。

●支払い方法：クレジットカード、コンビニエンスストア払い、Pay-easy 払いが可能です。（Pay-easy 払いの支払手数料（242 円）は払込人の負担となります。）

●支払い方法がコンビニエンスストア払い・Pay-easy 払いの場合、午前試験の予約の入金確認後に、午後試験の予約が可能です。支払い方法がクレジットカードの場合、午前試験の予約完了後に午後試験の予約が可能です。

●Web 領収証の発行は、受験後にオンライン上から印刷できます。受理した受験手数料は理由のいかんにかかわらず、返還できません。

（5）試験当日の主な留意事項

●試験当日は、試験開始の 15 分前までに必ず試験会場へ行き、受付で「**本人確認書類**（顔写真付きの運転免許証や学生証など）」を提示してください。

●着席する番号が記された「**ID 番号票**」を受け取って、PC ルームに入室します。
〔なお、試験中、電卓は使用できません。時計、スマホ、筆記用具などの所持品も全てかばんへしまって、入室前に試験会場のロッカー等に預けてください。〕

●机上にシャープペンシルとメモ用紙が用意されているので、メモをとることはできます。ただし、このメモ用紙を持ち帰ることはできません。試験終了後、メモ用紙は、シャープペンシル、「ID 番号票」とともに、試験監督員に返却します。

（6）成績照会と合格発表

●試験受験後、「スコアレポート」の確認用 URL が記載されたメールが登録済みのメールアドレスに届きますので、「スコアレポート」より、成績照会が可能です。

●「スコアレポート」には、得点等が記載されます。

●「午前試験：60 点以上」かつ「午後試験：60 点以上」で合格となります。

●正式な合格発表は、午前試験、午後試験の両方の受験が完了した翌月下旬に、合格者の受験番号（プロメトリック ID）が IPA のホームページに掲載されます。なお、後日、合格者の受験番号が官報に公示されます。

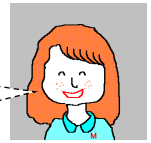
●合格者には、経済産業大臣から「情報処理技術者試験合格証書」が交付されます。

●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。合格証書は午後試験の予約時に登録した住所に簡易書留で送付されます。

※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。

★試験についての問い合わせ先：
（1）試験の予約、受験手数料の支払い、試験当日の手続等に関するお問い合わせ：
プロメトリック株式会社　TEL：03-6204-9830（電話受付時間：9：00～18：00）
問合せフォーム：**https://w1.prometric-jp.com/contact/agree0010.html**
（2）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.jitec.ipa.go.jp/**

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！！

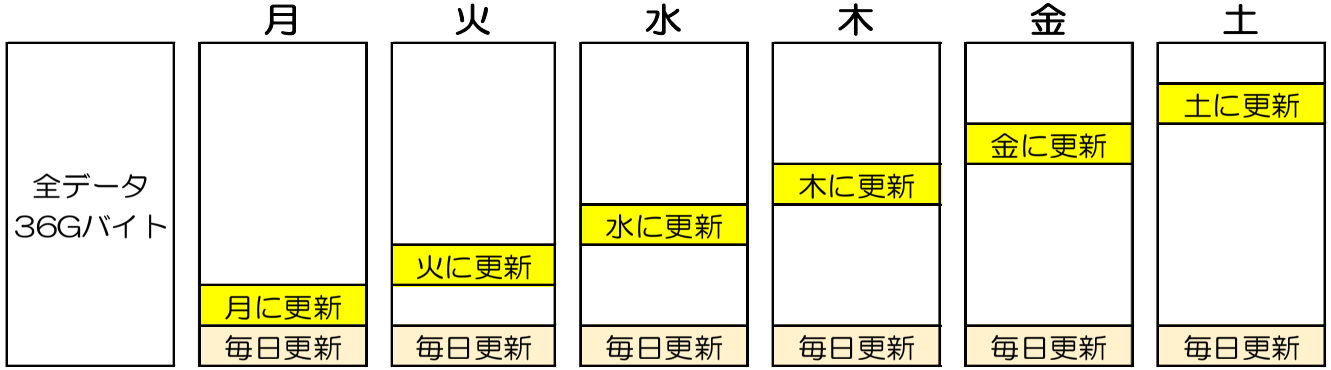


●参考　午後 問２　設問２（３）　バックアップの検討について

●各曜日のバックアップは個別の磁気テープに保存する。サーバから磁気テープへのバックアップ速度は 4M バイト／秒。　**★ポイント：毎日使用するデータは、毎日更新される。**

（１）全データと月曜～土曜に更新するデータ

●毎日更新されるデータは全データの1／30、各曜日に更新されるデータも全データの1／30



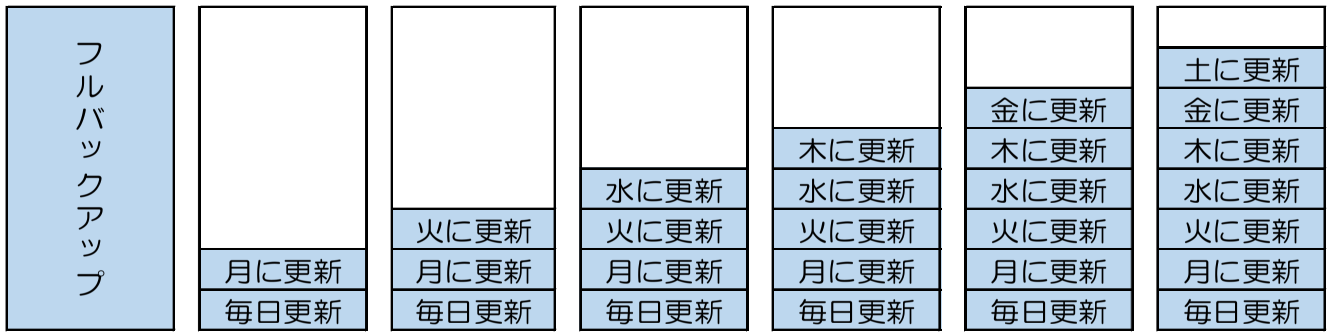
※p17の記述より、フルバックアップは**150分**
●念のため、計算してみると、↓

$$\frac{\text{全データ量}}{\text{バックアップ速度}} = \frac{36\text{Gバイト}}{4\text{Mバイト／秒}}$$

$$= \frac{36{,}000\text{Mバイト}}{4\text{Mバイト／秒}} = 9{,}000[\text{秒}] = 150[\text{分}]$$

（２）バックアップの方式

●毎週日曜はフルバックアップ、月～土曜は**差分バックアップ**（フルバックアップ以降に更新されたデータを全て取得）



（３）バックアップに要する時間

日	月	火	水	木	金	土
フル 150分※	5分×2 ＝10分	5分×3 ＝15分	5分×4 ＝20分	5分×5 ＝25分	5分×6 ＝30分	5分×7 ＝35分

●毎日更新されるデータと各曜日に更新されるデータは、それぞれ全データの1／30なので、
$\frac{150\text{分}}{30}$＝5分　●月曜は、5分＋5分＝10分

●土曜は、毎日更新されるデータと月～土に更新されるデータを全て取得するので、
5分×7＝35分（空欄ｋ）

（４）障害発生と復旧について

●例えば、土曜日の深夜に障害が発生したとします。このとき、土曜日のバックアップ取得直後の状態にまで復旧するために必要なバックアップ分について考えてみましょう。

・左記のように、毎週日曜はフルバックアップ、月曜～土曜は差分バックアップで運用していた場合、
日曜のフルバックアップと障害直近の（土曜の）差分バックアップの二つ（2本の磁気テープ）を使用すれば全データを復旧することができます。（空欄ｌ）

・毎週日曜はフルバックアップ、月～土曜は増分バックアップ（前日のバックアップ以降に更新されたデータだけを取得）で運用していた場合、復旧のためには、
日曜のフルバックアップと月曜～土曜のすべてのバックアップ（7本の磁気テープ）が必要になります。（空欄ｍ）