講義録レポート

講義録コード　04-32-1-301-01

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	2023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	5　枚
			その他	0　枚

講義構成	解説1 (75分) → 休憩 (10分) → 解説2 (83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：[ ]	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

Web模試解説

解説予定の問題

・科目A

問3, 5, 8, 9

11~15, 19

~~21~~, 34

~~44~~ ~~45~~

・科目B

問 ~~49~~~52

~~56~~, ~~57~~ ~~58~~, ~~60~~

問に関連

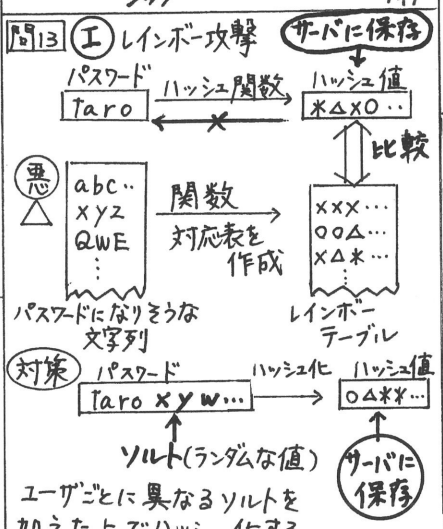
ウェルノウンポート番号

- HTTP = 80
- HTTPS = 443
- SMTP = 25
- POP = 101
- TELNET = 23
- SSH = 22

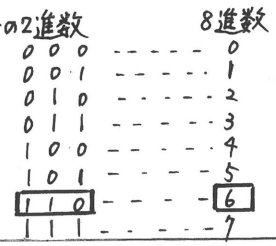
問5 イ CVSS：共通脆弱性評価システム

ウ = J-CSIP：サイバー情報共有イニシアティブ

問13 エ レインボー攻撃



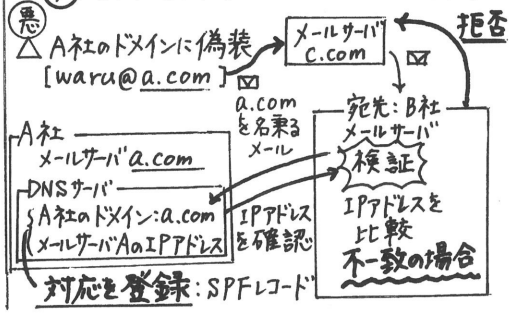
問14



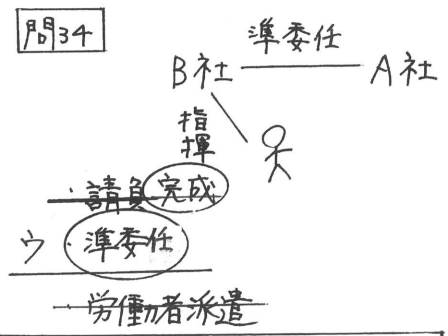
問25 エ FRR：本人拒否率, FAR：他人受入率

問29 ウ ・DKIM：メールのヘッダーにデジタル署名を付加

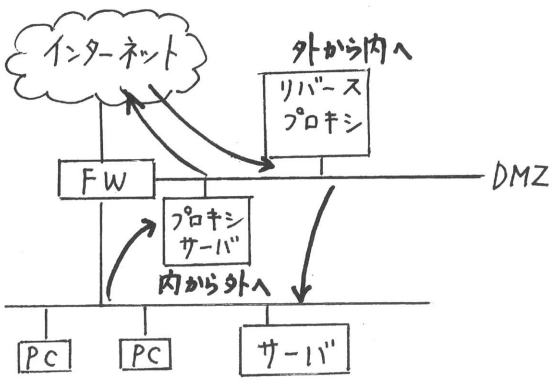
・SPF：DNSサーバにSPFレコードを登録



問34



問44



問45

・ROE：$\frac{\text{利益}}{\text{自己資本}} \times 100\%$

・ROA：$\frac{\text{利益}}{\text{総資本}} \times 100\%$

ウ ・ROI：$\frac{\text{利益}}{\text{投資額}} \times 100\%$

イ：BPM (P229) ← BPR

エ：RPA

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49 ク

	重要度	脅威	脆弱性		リスク値
表1より				表2より	(c×e)
a, b	c	d		e	f
2 2	2	2	1	1	2×1 =2

問56

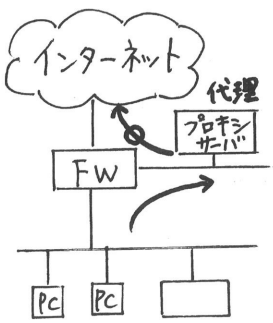
2進	10進	16進
0000	0	0
	⋮	⋮
	9	9
	10	A
	11	B
	12	C
	13	D
	14	E
1111	15	F

読み	参(8)	更(4)	追(2)	削(1)	10進	16進	
a	1	1	1	0	14	E	カ
b	1	0	0	0	8	8	
c	1	1	0	0	12	C	

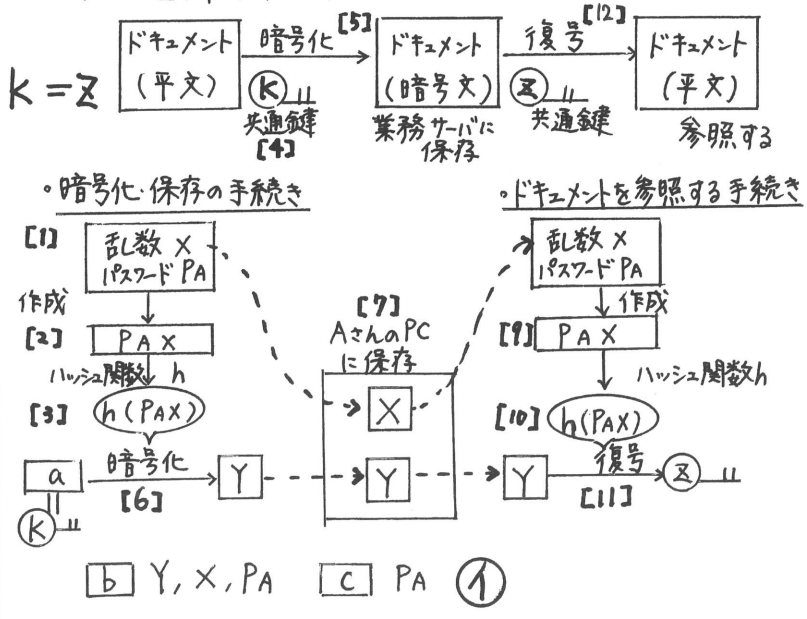
問57 ア

		実際の在室者	システム上の在室者
9:30	Aさん (i)により入室拒否 ツーパーソンルール		
10:00	AとB入室	A, B	
11:00	C入室	A, B, C	
11:30	B退室	A, C	
12:00	D入室 E共入	A, C, D E	A, C, D
12:30	D退室 A共退	C, E	A, C
13:00	Cさん (ii)により退室拒否	ツーパーソンルール	
14:00	F入室	C, E, F	A, C, F
15:00	Eさん (iii)により退室拒否	アンチパスバック	
15:30	Aさん (iv)により再入室拒否	アンチパスバック	

問59 ク



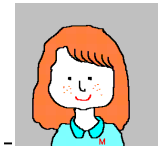
問60 共通鍵暗号方式



b Y, X, PA　c PA　(イ)

●令和 5 年度春期 Web 模擬解説〔テスト区分：E3A1〕

- 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 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予定の問題

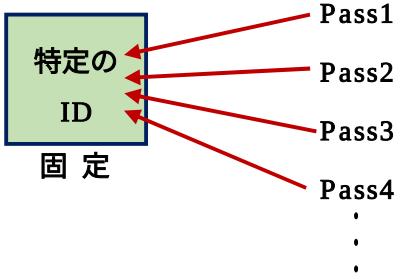
●科目 A 問題　…問 2, 5, 6, 9, 11, 12, 13, 14, 15, 19, 24, 25, 26, 27, 28, 29, 30, 31, 34, 44, 45

●科目 B 問題　…問 49, 50, 51, 52, 56, 57, 59, 60

Lesson1　問 13 関連：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）

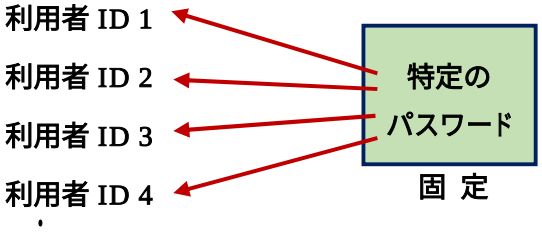
パスワードとして次々に文字列を入力



★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

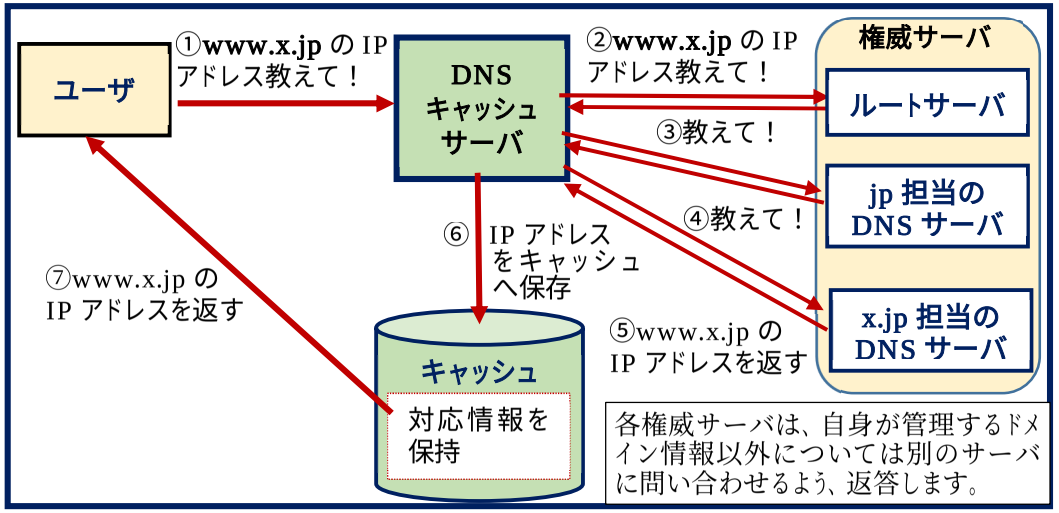
パスワードを一つ選び、利用者 ID として次々に文字列を用意して総当たりにログインを試行する



★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。

Lesson2　問 19 関連：DNS の仕組み **********

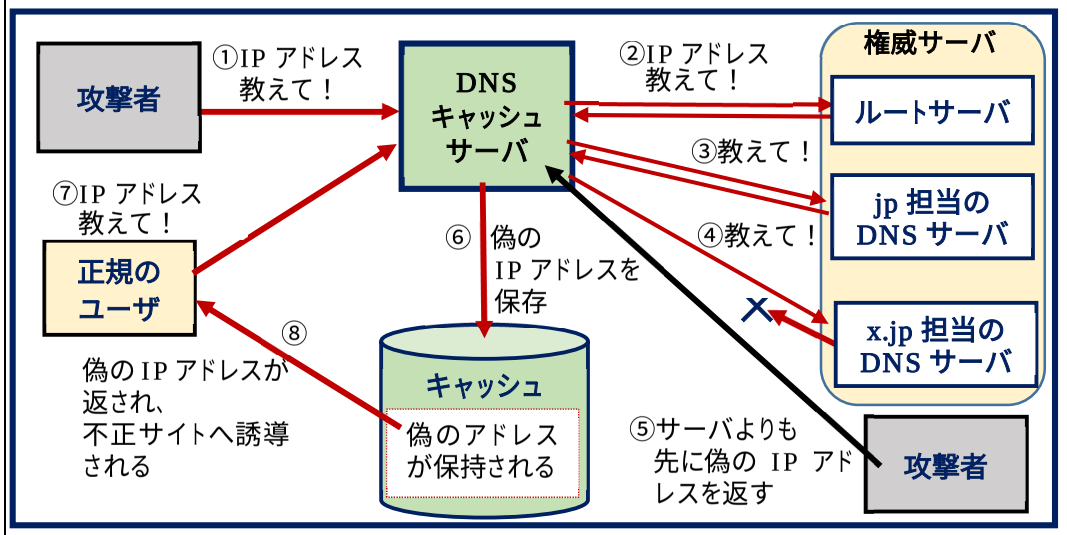
DNS では、特定のサーバ 1 台がドメイン名の情報を全て持っているわけではなく、データを階層ごとに分散化して保持しています。ユーザがドメイン名に対応する IP アドレスを得るときは、ルートサーバから順次たどっていくことで、最終的に必要な情報を得ます。



Lesson3　問 19 関連：DNS 関連の攻撃手法 **********

(1) DNS キャッシュポイズニング

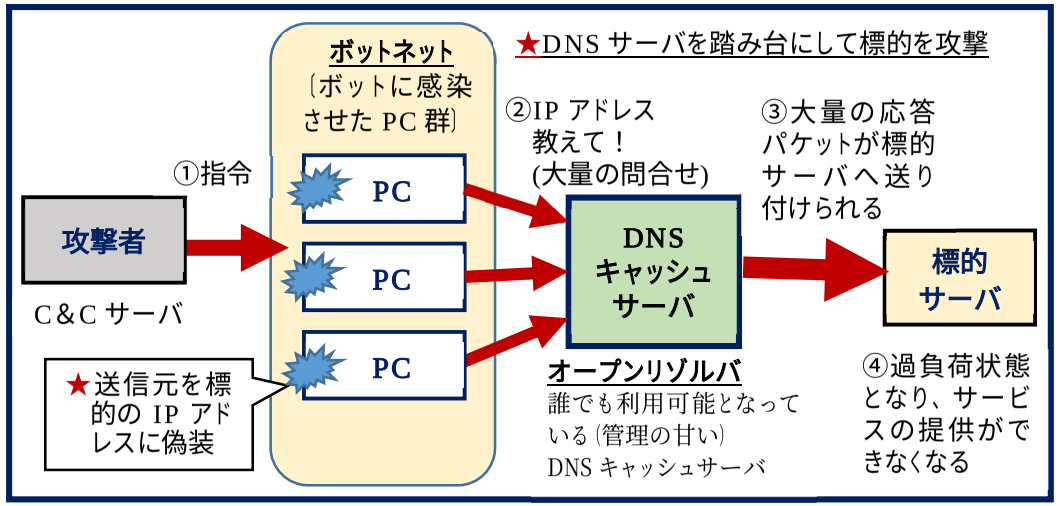
ドメイン情報を管理する DNS キャッシュサーバに偽の情報を記録させる攻撃です。



★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，ユーザが不正サイトへ誘導されてしまいます。

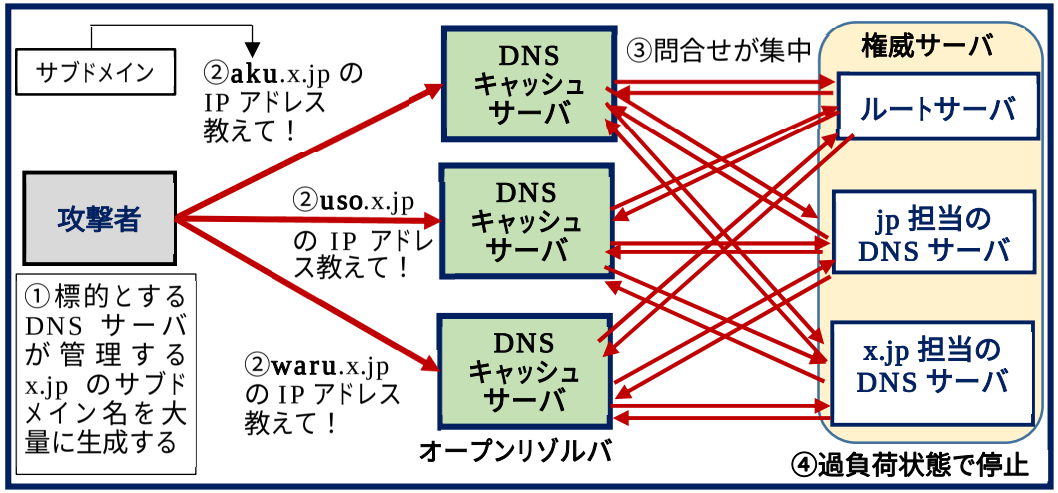
(2) DNS リフレクタ攻撃 (DNS リフレクション攻撃 ・ DNS amp 攻撃ともいう)

標的サーバの IP アドレスに偽装した問合せパケットを DNS 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。



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

標的 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 DNS キャッシュサーバに問い合わせ、標的 DNS サーバに問合せを集中させて停止させます。



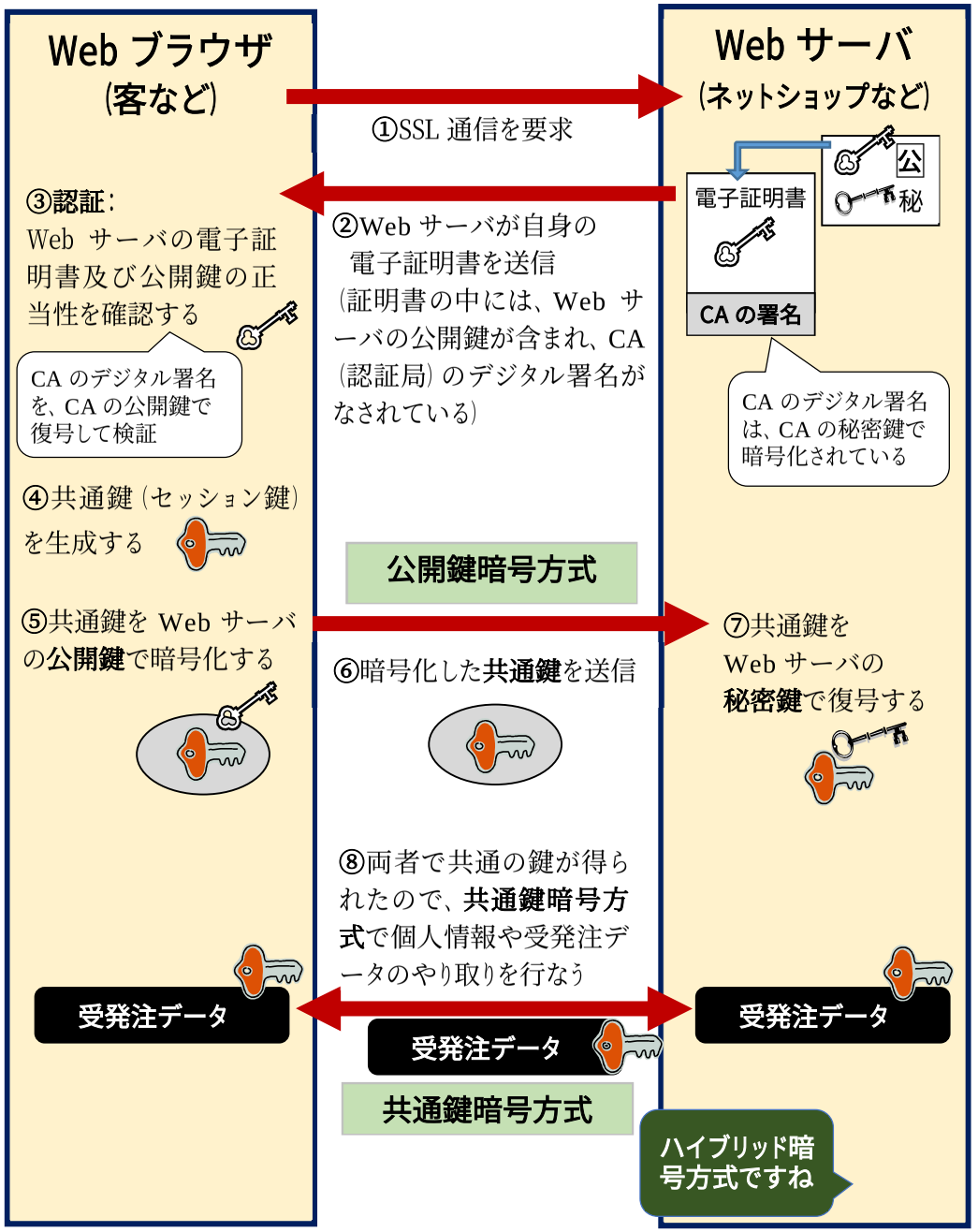
(4) DNS トンネリング (不正な遠隔操作のために DNS プロトコルを悪用する)

手順：①攻撃者が遠隔操作のための C&C サーバとして、不正な権威 DNS サーバを用意しておく。②ボットに感染させた PC から DNS キャッシュサーバに対し、(不正な権威 DNS サーバが管理するドメインについて) 問合せを送るように仕向けられる。③DNS キャッシュサーバから不正な権威 DNS サーバに対して問合せが送られ、これに返答することで通信を確立させる。

Lesson4　問 27 関連：SSL／TLS のしくみ **********

●**Web ブラウザと Web サーバ間で認証と暗号化通信を行う仕組み**

〔★実際には、双方のソフトウェアが全自動で下記のやりとりを行ってくれています。〕



●科目 B　各問のテーマ・解答に必要な知識など ********

問	出題テーマ ・ 難易度	解答に必要な知識･要素
49	**リスクアセスメント** （与えられた評価基準に従って評価値とリスク値を求める） ★難易度：中程度	機密性、完全性、可用性の評価 被害発生可能性の評価 リスク値の計算
50	**セキュリティ要件を満たすサービスの選択** ★難易度：やや易しい	オンラインストレージサービス データセンタ、操作ログ 権限制御
51	**目的に合致した情報セキュリティ対策の検討** ★難易度：やや易しい	クラウドサービス 2 要素認証 暗号化、クライアント証明書 バックアップ
52	**情報セキュリティ監査における指摘事項と対応策** ★難易度：やや難しい	共有 ID の運用 共有パスワード変更のタイミング 操作ログの取得 状況に応じた対応策の選択
53	**情報セキュリティ対策情報のヒアリング** ★難易度：易しい	情報セキュリティ 5 か条 OS、ソフトウェアの更新
54	**ビジネスメール詐欺の手口と対策** ★難易度：やや易しい	BEC（ビジネスメール詐欺）の特徴 電子メールのヘッダフィールド （From＝送信元、Reply-To＝返信先）
55	**Web サーバに対する不正ログインの分析** ★難易度：やや易しい	認証処理ログ ブルートフォース攻撃 アカウントロック パスワードの強化（桁数の増加）
56	**アクセス要件に沿ったアクセス権限の設定** ★難易度：中程度	2 進数と 16 進数の対応 権限の種類と設定（参照／更新／追加／削除）
57	**サーバルームの入退室管理** ★難易度：やや難しい	ツーパーソンルール（TPMOR） アンチパスバック 入室拒否／退室拒否の要因分析
58	**内部不正防止のためのチェックシート作成** ★難易度：中程度～やや易しい	IPA 組織における内部不正防止ガイドライン 各対策項目の主担当部門とサポート部門の決定
59	**ファイアウォールのフィルタリングルールの設定** ★難易度：やや難しい	ファイアウォール パケットフィルタリング プロキシサーバ ウェルノウンポート番号〔SMTP＝25、HTTP＝80、HTTPS＝443 など〕
60	**ドキュメントの暗号化と保存、及び参照の手続き** ★難易度：難しい	共有鍵暗号方式 ハッシュ関数 ハッシュ値を利用した共通鍵の暗号化と復号、復号に必要な情報

Lesson5　問 57 関連：内部不正牽制のための入退出管理策 ***

(1) ツーパーソンルール（TPMOR：Two Person Minimum Occupancy Rule）

室内に 1 人だけでいることを防止するためのルール。「最初に入室する者は 2 人以上で同時に入室し、最後に退室する者は 2 人以上で同時に退出しなければならない（1 人だけを残して退室することを許さない）」とすることで、犯行の抑止が期待できる。

(2) アンチパスバック･･･共連れ（1 人の認証で複数名が入退出すること）の防止策

「入室記録のない者は退出を許可しない、退室記録のない者は再入室を許可しない」とする仕組み。システムとしてこの仕組みを有効にすることで、共連れで入室した不審者による情報の持出しなどのリスクを抑えることができる。

●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：

【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、勘違いした内容や不足していた知識を正しくつかみましょう。

IPA が公開しているサンプル問題も活用しましょう。

- **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。

③サンプル問題について：

★IPA が公開しているサンプル問題も、必ず解いておきましょう。

サンプル問題（60 問）、及び解答ページへのリンク ↓

https://www.jitec.ipa.go.jp/1_00topic/topic_20221226.html

●試験の申込みについて　〔2023 年 4 月以降の CBT 試験〕

〔1〕**申込み受付開始日：　2023 年 3 月 15 日 (水) 10 時**

〔2〕**試験開始日：　2023 年 4 月 5 日 (水)**　〔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、申込受付開始後に受験申込みを行っていただきます。 なお、受験申込みする月から起算して 3 ヶ月後までの試験日時が選択可能です。

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。)

●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

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。
  〔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。**

〔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.jitec.ipa.go.jp/**

〔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
受験サポートセンター (専用窓口)　**TEL 03-4500-7862**

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！！