# 講義録レポート

講義録コード　04-32-2-301-01

| | | | |
|---|---|---|---|
| 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 | 2023年秋期(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 | 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 (86分) → 休憩 (10分) → 解説2 (72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 | 三ツ矢 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, 7, 10～12, 15～17, 19, 23, 24, 31, 35, 38, 39, 40, 42, 47, 48
- 科目B
  - 問50, 52, 54～56, 58～60

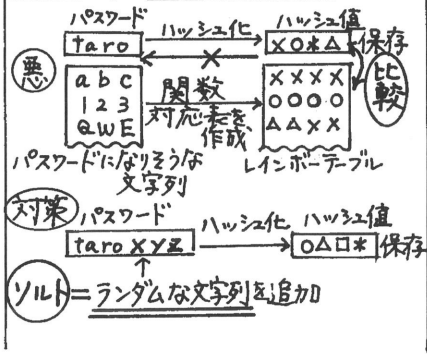
### 問12 イ SEOポイズニング

Search Engine Optimization
検索エンジン最適化

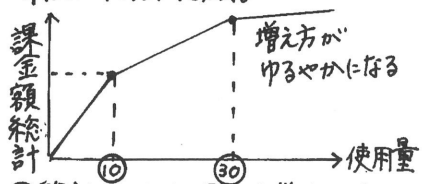
### 問15 ウ EDR

Endpoint Detection and Response
端末 ← 挙動を観察

### 問24 イ レインボー攻撃



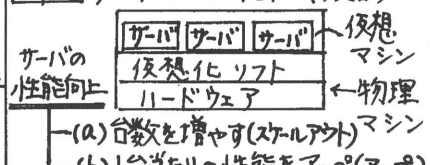

### 問39 ア 逓減課金方式



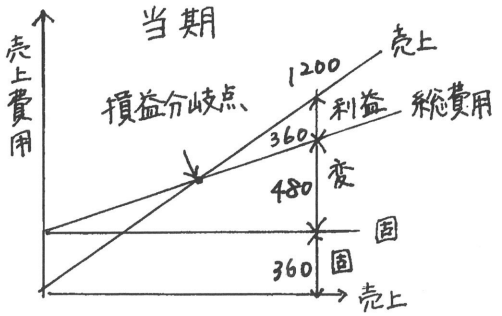

### 問40 ウ 設計工程の要員数

工数：400人月×32%＝128人月
期間：20か月×40%＝8か月
128人月÷8か月＝16人

### 問42 ア サーバの仮想化（復習）

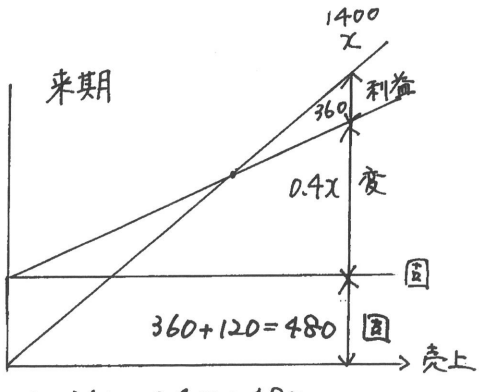



### 問48 イ 損益分析：利益図表




利益＝1200－(480＋360)
＝360

変動費率＝$\frac{480}{1200}$＝0.4




$X = 360 + 0.4X + 480$

$X - 0.4X = 360 + 480$

$(1 - 0.4)X = 360 + 480$

公式 $X = \frac{360 + 480}{1 - 0.4}$

$X = \frac{840}{0.6} = 1,400$

| 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

### Web模試解説

解説予定の問題

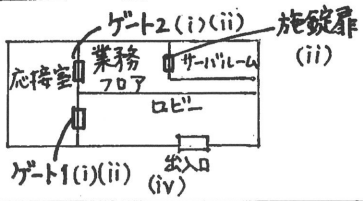
- 科目A

問3～5, 7, 10～12, 15～17, 19, 23, 24, 31, 35, 38, 39, 40, 42, 47, 48

- 科目B

問50, 52, 54～56, 58～60

**問50** エ 図1 エリア管理




**問52** (ウ) or エ リスクの分析と評価

重要度＝影響度×脅威×脆弱性

| 商品データ | a：機 1 | b：完 3 | c：可 2 | 10以上 |
|---|---|---|---|---|
| (甲) | 1×3×2＝6 | 3×3×2＝(18) | 2×3×2＝(12) | 2つ |
| 乙 | 1×2×2＝4 | 3×2×2＝(12) | 2×2×2＝8 | 1つ |
| 丙 | 1×3×1＝3 | 3×3×1＝9 | 2×3×1＝6 | なし |

[表2より] 甲：3 乙：2 丙：3

[表3より] 甲：2 乙：2 丙：1

**問54** ケ 全体36Gバイト

① 36000Mバイト÷4Mバイト/秒÷60秒 ＝150分

② 毎日更新 … 全体の$\frac{1}{30}$, $150\times\frac{1}{30}=5$分 / 各曜日当たり 〃 〃 5分

例）月曜の差分バックアップ：5分＋5分＝10分

(配) P4 Lesson7へ (土) … 35分

**問55** コ 表1

(二)(ホ)A社スタッフ (六)

| 利用者 | C社（B社に委託） | | | D社（A社が担当） | | |
|---|---|---|---|---|---|---|
| | 関 | 記 | タグ | 関 | 記 | タグ |
| a | ○ | α(なし) | ○ | β(なし) | | |
| b | | | | ○ | γ○ | ○ |

・電話での対応を記録

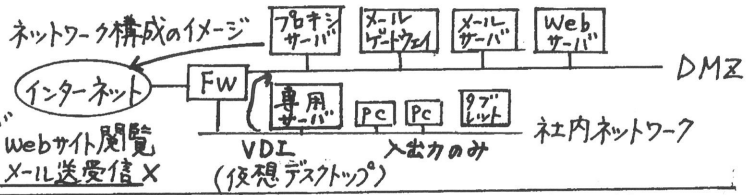
**問56**

シンクライアント化によって 絞る

a：有効なこと オor カ

b：困難になること (カ)

ネットワーク構成のイメージ




**問58** カ

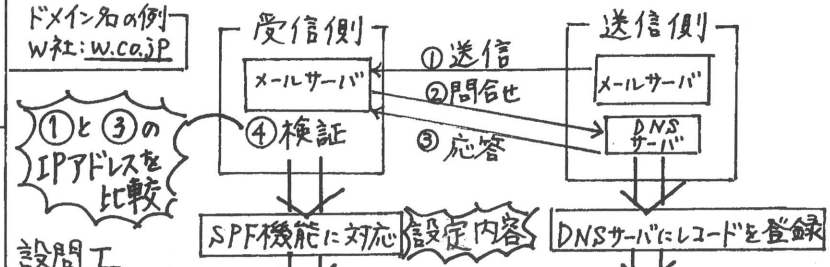
不自然な通信 ③ ⑥ ⑦

**問59** キ

絞る a (b)

| | a | b |
|---|---|---|
| (キ) | 項番4 | 項番1 |
| ク | 〃4 | 〃3 |
| ケ | 〃4 | 〃5 |

**問60** 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

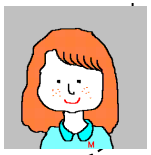



設問エ

| | | |
|---|---|---|
| パターン1の検知 | W社 (ii) | 取引先 (iii) |
| パターン2の検知 | 取引先 (iv) | W社 (i) |

# ●令和 5 年度秋期 Web 模擬解説〔テスト区分：E3AA〕

- 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問題

●科目 A 問題 … 問 3, 4, 5, 7, 10, 11, 12, 15,
16, 17, 19, 23, 24, 31,
35, 38, 39, 40, 42, 47, 48

●科目 B 問題 … 問 50, 52, 54, 55, 56, 58, 59, 60

---

## Lesson1　問 4 関連：IPA が提供している機能・取組み　*****

●**JVN と My JVN**:

JVN(Japan Vulnerability Notes)は、脆弱性対策情報のポータルサイトであり、国内外の脆弱性情報を収集してデータベース化し、JVN iPedia として公開している。

My JVN は、JVN iPedia を利用者が効率よく活用するための機能を提供する仕組み（フレームワーク）である。ツールとして、PC にインストールされているソフトウェアのバージョンが最新かどうかをチェックする機能（**バージョンチェッカ**）などが提供されている。

●**icat for JSON**（アイキャット フォー ジェイソン）:

IPAが提供するサイバーセキュリティ注意喚起サービス。Webページに所定のタグを埋め込んでおくことで、その部分にIPAから発信されるセキュリティ情報がリアルタイムに表示される。

●**J -CRAT**（ジェイ クラート）: **サイバーレスキュー隊**

標的型サイバー攻撃の被害拡大防止のための支援体制。

●**J -CSIP**（ジェイ シップ）: **サイバー情報共有イニシアティブ**

IPAにサイバー攻撃などの情報を集約し、組織間で情報共有を行うことによって、高度なサイバー攻撃対策につなげていく取組み。

●**ICS CoE**: **産業サイバーセキュリティセンター**

模擬プラントを用いた演習や、攻撃防御の実戦経験、最新のサイバー攻撃情報の調査･分析等を通じて、社会インフラ･産業基盤へのサイバーセキュリティリスクに対する人材･組織･システム･技術を生み出すことを目的としている。

●**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社診断**」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

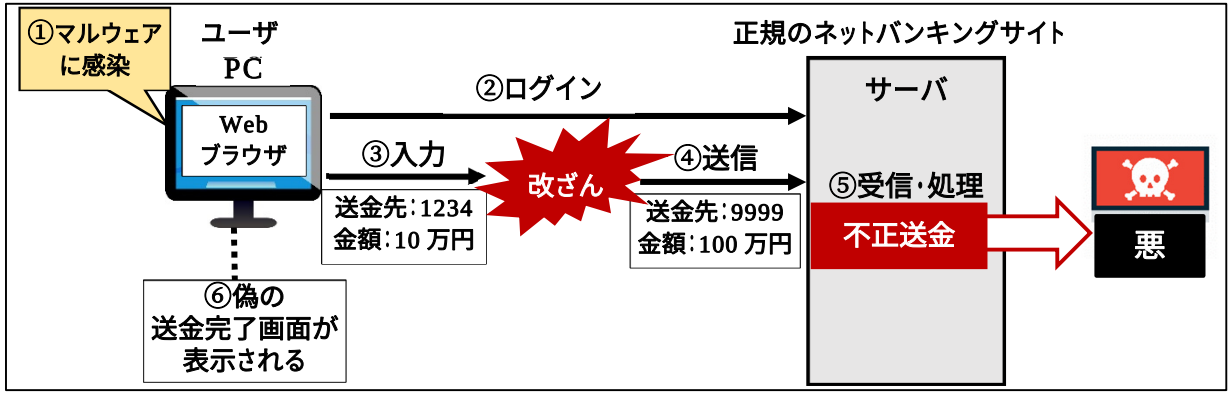
IPA に申し込むことにより、取組み段階に応じたロゴマークを使用することができる（名刺やWeb サイト等にロゴを表示して、自社の取組みをアピールできる）。➡➡➡➡➡➡➡➡➡➡➡➡


●**情報セキュリティ 5 か条**

①OS やソフトウェアは常に最新の状態にしよう！
②ウイルス対策ソフトを導入しよう！
③パスワードを強化しよう！
④共有設定を見直そう！（共有範囲を限定するなど）
⑤脅威や攻撃の手口を知ろう！（最新の手口を知り、注意喚起を確認する）

## Lesson2　問 10 関連：MITB（Man-In-The-Browser）攻撃 **********

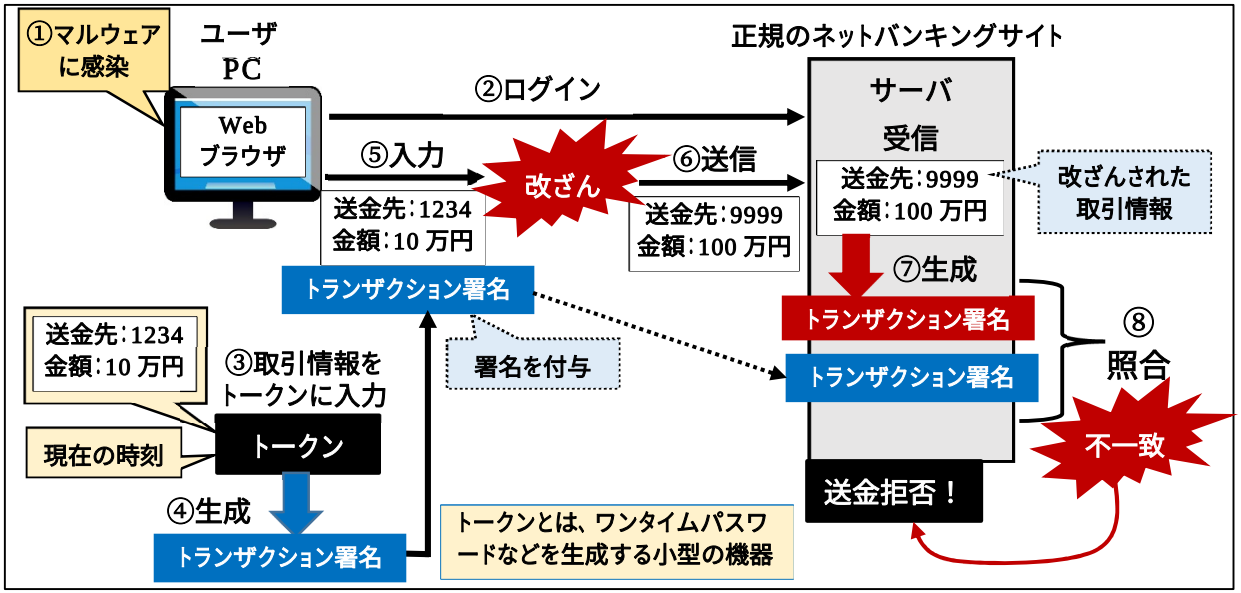
マルウェアに感染した PC が正規のネットバンキングサイトのサーバにアクセスした際に、通信セッションが乗っ取られ、送金先の口座番号や送金金額の改ざんなどが行われてしまう攻撃。




★**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ない。

## Lesson3　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。

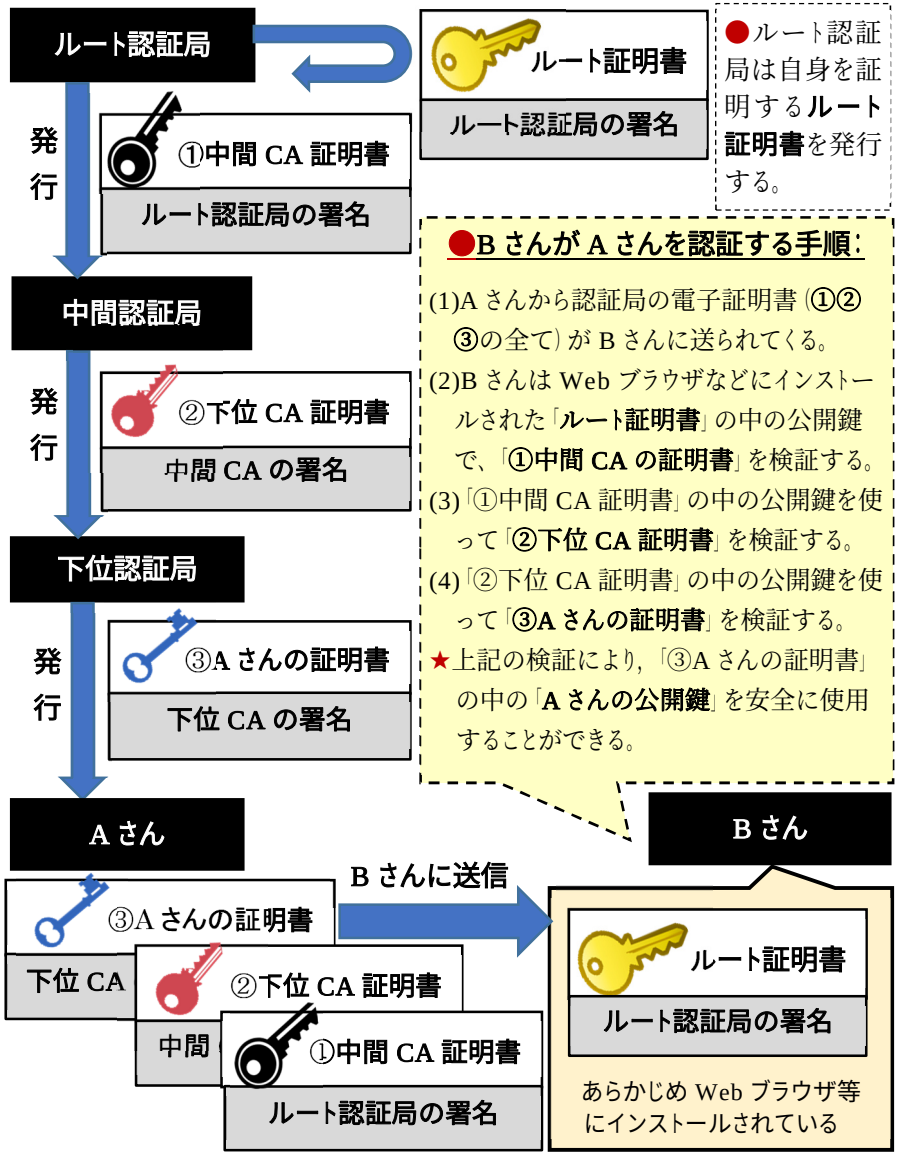



★**ポイント**：PC に感染したマルウェアによって偽の署名が作成される危険性もあるため、PC とは別のデバイス（トークン）で安全に署名を作成し、これを Web ブラウザ上で入力している。

## Lesson6　問 23 関連：認証局（CA）の認証の連鎖 **

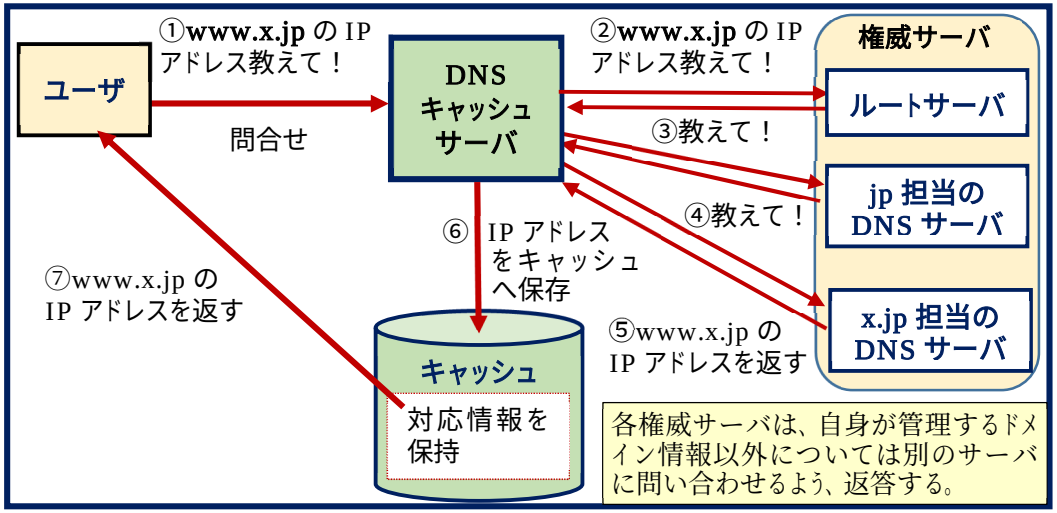
**●電子証明書発行の流れ**

- ルート認証局は，自身の公開鍵の証明書（**ルート証明書**）を発行する。
- ルート認証局は，「**①中間認証局の公開鍵の電子証明書**」を発行する。
- 中間認証局は，「**②下位認証局の公開鍵の電子証明書**」を発行する。
- 下位認証局は，「**③A さんの公開鍵の電子証明書**」を発行する。

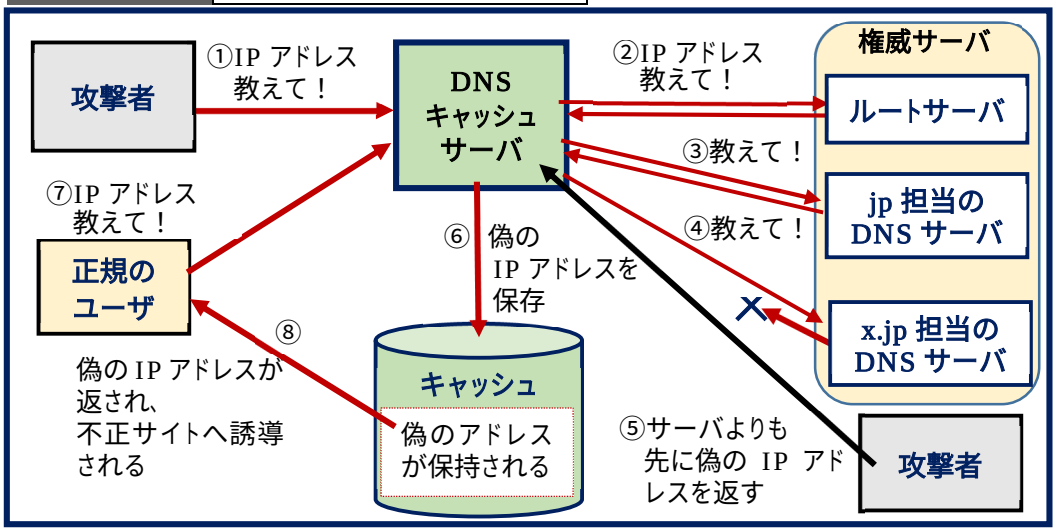


## Lesson4　問 19 関連：DNS の仕組み **********

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化して保持している。DNS キャッシュサーバがユーザ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次たどっていくことで、最終的に必要な情報を得ることができる。




## Lesson5　DNS 関連の攻撃手法 **********



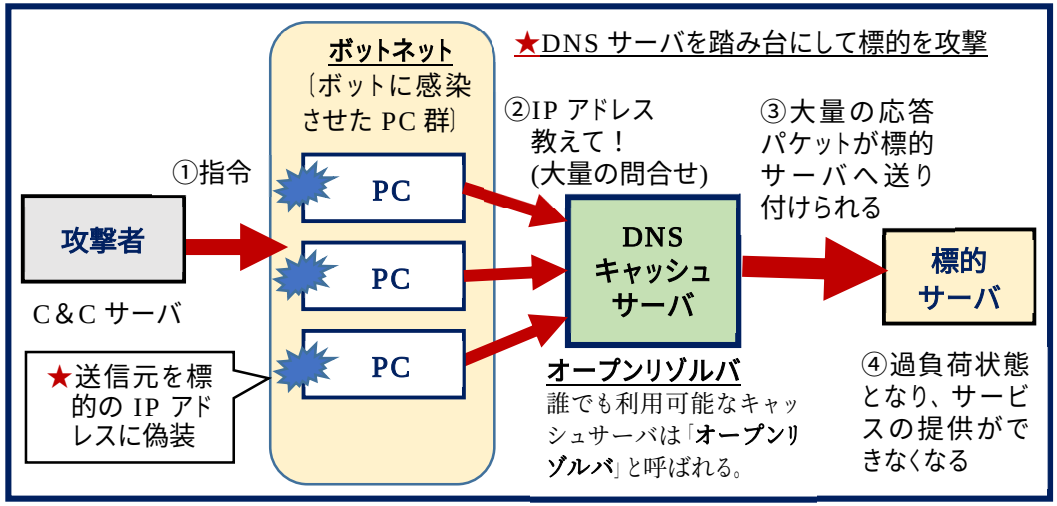

### (1) DNS キャッシュポイズニング

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。

★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う。

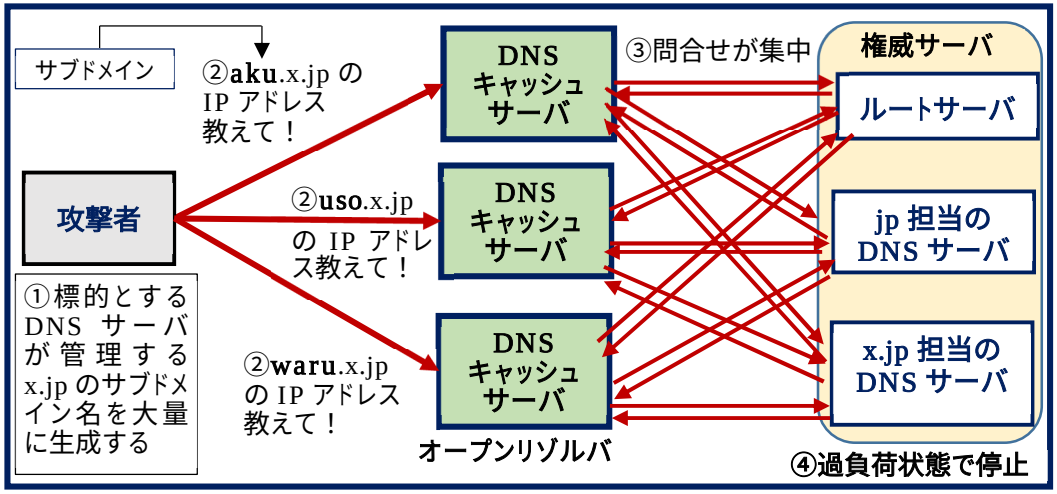
### (2) DNS リフレクタ攻撃 (DNS リフレクション攻撃 ・ DNS amp 攻撃ともいう) …DoS 攻撃

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。




### (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る。




### (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) :参考

**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。

## ●科目 B　各問のテーマ・解答に必要な知識・要素 *****

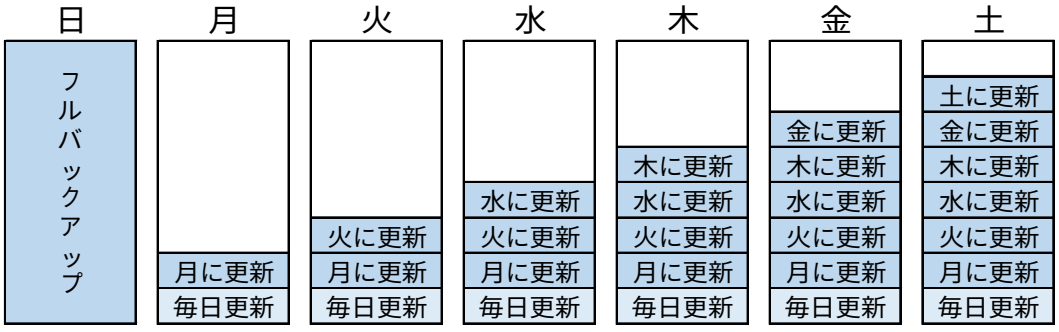
| 問 | 出題テーマ ・ 難易度 | 解答に必要な知識･要素 |
|---|---|---|
| 49 | **ログイン ID･パスワードによる認証の改善案**<br>〔★難易度：易しい〕 | ID･パスワード認証とアクセス権限<br>ログイン ID 共有のリスク |
| 50 | **入退出管理**<br>〔★難易度：易しい〕 | IC カードによる扉の開閉制御 |
| 51 | **USB ドロップテストの訓練**<br>〔★難易度：やや易しい〕 | USB デバイスの使用規定<br>USB ドロップテストの計画案 |
| 52 | **リスク分析と評価**<br>〔★難易度：中程度〕 | リスクの重要度の算出<br>影響度･脅威･脆弱性の評価 |
| 53 | **VPN 利用の在宅勤務環境**<br>〔★難易度：やや易しい〕 | VPN（仮想専用網）<br>2 要素認証、無線 LAN の暗号化通信<br>VDI（デスクトップ仮想化） |
| 54 | **バックアップ取得の所要時間**<br>〔★難易度：中程度〕 | フルバックアップと差分バックアップ<br>バックアップの所要時間 |
| 55 | **コールセンター業務における操作権限**<br>〔★難易度：やや難しい〕 | AI による対応<br>不具合報告･質問のタグ付け<br>従業員･委託先の操作権限 |
| 56 | **シンクライアント化計画の検討**<br>〔★難易度：中程度〕 | タブレット型端末による社外からの営業活動<br>シンクライアントの利点と問題点<br>仮想マシン |
| 57 | **セキュリティ対策の取組状況の調査結果と判断**<br>〔★難易度：中程度〕 | SECURITY ACTION<br>個人所有のデバイス使用に関する社内規定<br>OS、ウイルス対策ソフトの状態 |
| 58 | **不自然な通信の形跡**<br>〔★難易度：中程度〕 | DMZ<br>パケットフィルタリング、通信ログ<br>HTTP、SMTP、POP3、DNS<br>プロキシサーバ、ポート番号 |
| 59 | **インシデントの調査結果と原因の考察**<br>〔★難易度：中程度〕 | マルウェア自身による通信の隠蔽<br>インシデントの特徴と手口の分析 |
| 60 | **SPF（送信元ドメイン認証技術）の導入**<br>〔★難易度：難しい〕 | メールアドレスのドメイン偽装<br>SPF によるなりすましメール対策<br>DNS サーバ、SPF レコードの登録<br>SPF 機能への対応 |

## Lesson 7　問 54 関連：差分バックアップの所要時間 **********

●日曜のフルバックアップ分の所要時間は、36,000[M バイト] ÷ 4[M バイト／秒]
＝ 9,000[秒] ＝ 150[分]

●毎日更新するデータは全体の 30 分の 1 ＝ 所要時間は、150 ÷ 30 ＝ 5[分]
各曜日当たりの業務データも全体の 30 分の 1 ＝ 所要時間は 150 ÷ 30 ＝ 5[分]

●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




●バックアップに要する時間

| 日 | 月 | 火 | 水 | 木 | 金 | 土 |
|---|---|---|---|---|---|---|
| フル<br>**150分** | 5分×2<br>**＝10分** | 5分×3<br>**＝15分** | 5分×4<br>**＝20分** | 5分×5<br>**＝25分** | 5分×6<br>**＝30分** | 5分×7<br>**＝35分** |

## ●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<br>60 分／48 問＝1 問当たり 75 秒<br>（できれば 1 問平均 60～70 秒） | ・科目 B（事例問題）： 60 分<br>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。）

## ●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
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！！**