

選考問題例

過去に出題された問題を掲載しています。

※ 出題された専門考査、経験小論文、論文の問題については、一定期間、警視庁情報公開センター（警視庁本部庁舎 1 階）及び都民情報ルーム（都庁第一本庁舎 3 階）にて閲覧することができます。

◎ 財務捜査官

【専門考査】

[設問] 粉飾決算が疑われる一般事業会社の過去 3 期分の決算書等の資料を入手した。当該資料を用いて分析を行ったところ、以下のような結果が出た。想定される粉飾方法をそれぞれ答えなさい。

- (1) 棚卸資産回転期間が長期化している。
- (2) 売上債権回転期間及び棚卸資産回転期間に顕著な変動は見られないが、1 人当たりの売上高が顕著に増加している。なお、新製品の販売は行われていない。
- (3) 固定資産が顕著に増加しているが、投資活動によるキャッシュ・フローは増加していない。

【経験小論文】

[課題]

過去の犯罪事例をとりあげ、今後財務捜査官としてあなたが当該犯罪事例に対してどのように対応すべきと考えるか、経験も踏まえて述べなさい。

◎ 科学捜査官（化学）

【専門考査】

[設問] 次の化学物質の構造式を記しなさい。また、主要な用途、人体に与える影響（作用・中毒症状など）、適用法令について知るところを記載しなさい。

- (1) 亜硝酸イソブチル
- (2) 塩化ベンザルコニウム
- (3) ケタミン（ただし塩酸塩のもの）
- (4) メチルメルカプタン
- (5) ジクロロフルオロメタン（別名 フロン 21）

【経験小論文】

[課題]

あなたが今まで経験、蓄積してきた技術、知識等を警視庁でどのように役立てられるか、あなたの考えを述べなさい。

◎ サイバー犯罪捜査官

【専門考査】

[設問] 脆弱性に関する次の記述を読んで、[No.1] [No.2] の問いに答えよ。

A 君は中小企業に勤務し、前任者の退職に伴い情報システム担当になった。自社のシステムの構成を学びつつ、情報セキュリティの基礎を座学で学び始めた。CIAという3要素(a)が基本であり、それぞれの観点に則ったセキュリティ管理に取り組む必要を確認した。

担当して早々に、経営層から2つの課題に急いで取り組むように指示を受けた。

1つは、社内システムには知財情報や、顧客情報などが保存されており、外部からの侵入や攻撃は重大なリスクとなるため、このセキュリティをどのようにすればよいかについてであった。

もう1つは、在宅勤務がトレンドとなり、テレワークができることを打ち出さないと人材の採用が立ち行かないが、これをどのようにすればよいかについてであった。

A 君はそれぞれについて検討を開始した。社内システムへの外部からの侵入・攻撃は、一般的に事前調査、権限取得、不正実行、後処理の4段階に分けて行われ、事前調査段階で侵入を防ぐことが最も大切と知った。侵入者は糸口をつかむために、まずターゲットのシステムについて詳しく調べ、システム情報を収集する。具体的には、IP アドレス、サーバ名、サーバソフトウェア、OSの種類・バージョン、提供されているサービス、侵入検知・防御システム(b)などに関する情報である。システム情報を入手するには、手がかりとして、公開されている Web サイトなどを使い、通信に使用するポートの状態を調べ、開かれているポートや提供されているポートサービスを調べる(c)のが常套手段であり、これはセキュリティ上重要なポイントであった。またファイアウォールに関しては、プライベートアドレスをグローバルアドレスに変換(d)し内部情報を隠蔽、DMZ(e)を設け Web サーバ、Mail サーバ、DNS サーバ(f)などを内部ネットワークではなく、DMZ に置くようにすべきと理解し対応を始めた。

次にテレワークについて調べてみたところ、総務省からテレワークセキュリティガイドラインが策定・公表されており、その方式と、脅威に対する「脆弱性」などが示されていた。

以下のとおり、テレワーク方式として7つ例示されていた。

- VPN 方式(g)
- リモートデスクトップ方式(h)
- 仮想デスクトップ方式(i)
- セキュアコンテナ方式
- セキュアブラウザ方式
- クラウドサービス方式(j)
- スタンドアロン方式

これらについて、オフィス業務の再現性についての評価をみると、(g)～(i)が相対的に優れていることがわかった。スタンドアロン方式以外は社内システムやクラウドサービスへイ

インターネットを用いて接続して利用するが、利用場所は、自宅(k)、テレワークオフィス、カフェや交通機関(1)に至るまで多岐にわたっており、それぞれの場所でのセキュリティレベルに配慮する必要がある。またクラウドサービスは、情報を預け、システム運用の一部を担うことになるため、クラウドサービス事業者について、その信頼性を確認する(m)ことが重要と理解し、テレワーク環境の構築検討を進めることとした。

[No.1] 社内システムの話題に関して以下の問いに答えよ。

- ① (a)に示す CIA は、それぞれ英単語 C・・・、Integrity、Availability の頭文字をとった略語である。この C を頭文字とする適切な英単語を記述せよ。
- ② (b)に示す侵入検知・防御システムとして知られる IDS と IPS について、それぞれの概要を 50 字以内で記述せよ。
- ③ (c)に示すポートサービスのうち、以下の 2 つの用途を記述せよ。
 - (i) 80 番
 - (ii) 110 番
- ④ (c)に示すポートサービスのうち、445 番ポートは、インターネット側から内部ネットワークへ向かって接続できないような設定が推奨されている。このポートはどのような用途であるか、またそのような設定にする理由を簡潔に記述せよ。
- ⑤ (d)をアルファベット 3 文字で記述せよ。
- ⑥ (e)に示す DMZ について 40 字以内で説明せよ。
- ⑦ (f)に示す DNS サーバの脆弱性を利用して、偽の情報を DNS サーバに記憶させ、ユーザーに対して影響を与える攻撃の名称を記述せよ。

[No.2] リモートワークに関して以下の問いに答えよ。

- ① (g)に示す VPN 方式は、暗号化、完全性検査、トンネル化の機能によって仮想的な専用ネットワークを構築するが、トンネル化の概要を 60 字以内で記述せよ。
- ② (h)に示すリモートデスクトップ方式の概要を 70 字以内で記述せよ。
- ③ (i)に示す仮想デスクトップ方式で用いられる、個別のデータ保存やアプリケーション機能を持たない端末の名称を記述せよ。
- ④ (j)に示すクラウドサービスには、事業者が提供する資源の範囲(レベル)によって、「SaaS」「PaaS」「IaaS」という分類があるが、サーバや記録領域(ストレージ)等のハードウェアレベルの資源を提供するサービスは、3 つのうちどの分類に該当するか記述せよ。
- ⑤ (g) (h) (i)に示した 3 つの方式でセキュリティ統制の容易性を比較したとき、容易な順に左から記号を並べて記述せよ。
- ⑥ (k)に示す自宅で利用する Wi-Fi ルーターの暗号化方式には「WEP」「WPA」「WPA2」「WPA3」が一般的に用いられているが、このうち最も推奨されている暗号化方式はどれか記述せよ。
- ⑦ (l)に示すような、カフェや公共機関などのフリー Wi-Fi では が不十分で、悪意ある第三者に容易に内容が漏れてしまう可能性がある。この空白に当てはまる適切な語句を記述せよ。
- ⑧ (m)に示すような ISMS クラウドセキュリティの ISO 認証として適切なものを以下の(ア)～(エ)の中から 1 つ選び記号を記述せよ。
 - (ア) ISO 9001 (イ) ISO 14001 (ウ) ISO 27001 (エ) ISO 50001

【経験小論文】

[課題]

サイバー空間では、ランサムウェア被害が依然として高水準で推移するとともに、クレジットカード不正利用被害が急増し、インターネットバンキングに係る不正送金被害が過去最多となるなど、極めて深刻な情勢が続いている。

このような情勢を踏まえ、次の設問1～3に答えなさい(必要があれば、図、表を使用してもよい)。

設問1 あなたがこれまでに開発、保守又は運用した経験のある情報処理システムについて、代表的なものを1つ選び、システムの概要及びそのシステムにおけるサイバーセキュリティ上のリスクを述べなさい。

設問2 設問1で述べたリスクへの対策(ウイルス対策ソフトによるものを除く。)について述べなさい。

設問3 あなたがこれまでに得た知識、経験を警察のサイバー犯罪捜査にどのように役立てられるか、あなたの考えを述べなさい。