# 目　　次

**令和元年度秋期　問題と解答･解説編**



**＜出題分析＞**

# 3. 第７回情報処理安全確保支援士試験に向けて

## 3-1　情報処理安全確保支援士試験について

平成 28 年 10 月 21 日，経済産業省からサイバーセキュリティ分野において初の国家資格となる「情報処理安全確保支援士」制度を開始する旨の発表が行われました。それによりますと，情報処理安全確保支援士制度は，「近年，情報技術の浸透に伴い，サイバー攻撃の件数は増加傾向にあり，企業等の情報セキュリティ対策を担う実践的な能力を有する人材も不足する中，情報漏えい事案も頻発しています。このため，サイバーセキュリティの対策強化に向け情報処理の促進に関する法律の改正法が本日（平成 28 年 10 月 21 日）施行され，我が国企業等のサイバーセキュリティ対策を担う専門人材を確保するため，最新のサイバーセキュリティに関する知識・技能を備えた高度かつ実践的な人材に関する新たな国家資格制度を開始しました」とされています。また，情報処理安全確保支援士は，「サイバーセキュリティに関する知識・技能を活用して企業や組織における安全な情報システムの企画・設計・開発・運用を支援し，また，サイバーセキュリティ対策の調査・分析・評価を行い，その結果に基づき必要な指導・助言を行う者です。サイバーセキュリティの確保に取り組む政府機関，重要インフラ事業者，重要な情報保有する企業等のユーザー側及びこれら組織に専門的・技術的なサービスを提供するセキュリティ関連企業等のいわゆるベンダー側の双方において活躍が期待されます」と説明されています。

こうした背景の基に，平成 29 年 4 月から情報処理安全確保支援士試験（以下，支援士試験という）が実施されるようになりました。この支援士試験は，これまでの情報セキュリティスペシャリスト試験の流れをそのまま受け継ぐものですから，午前Ⅰ，午前Ⅱ，午後Ⅰ，午後Ⅱという四つの試験が行われることには変わりありません。

平成 30 年度秋期から令和元年度秋期までの受験者数，合格者数などの推移を図表 10 に示します。なお，合格率については，第 1 回から第 3 回までは 16%から 17%程度で推移し，第 4 回，第 5 回とも 18%台に向上しました。さらに，今回の試験では過去最高の 19.4%になり，約 5.2 人に 1 人の割合で合格者が生まれることになりました。そして，IPA の発表によりますと，令和元年 10 月 1 日現在，“登録セキスペ”の登録者数は 19,417 名に達し，登録することの有効性が意

識されるようになっています。

| 年　度 | 応募者数 | 受験者数 | 合格者数 |
|---|---|---|---|
| 平成 30 年度秋期 | 22,447（-3.2%） | 15,257（68.0%） | 2,818（18.5%） |
| 平成 31 年度春期 | 22,175（-1.2%） | 14,556（65.6%） | 2,774（18.9%） |
| 令和元年度秋期 | 21,237（-4.2%） | 13,964（65.8%） | 2,703（19.4%） |

（　）内は，それぞれ対前期比増減率，受験率，合格率を示す。

**図表 10　応募者数・受験者数・合格者数の推移**

## 3-2　出題予想

### (1)　午前Ⅰ試験，午前Ⅱ試験

平成 30 年度秋期から令和元年度秋期までの 3 期にわたる試験から判断すると，午前試験については，次のようにいえます。まず，午前Ⅰ（共通知識）と午前Ⅱ（専門知識）を比較すると，午前Ⅰの出題範囲が広範囲にわたることなどから，合格基準点をクリアすることが難しく，午前Ⅱは，午前Ⅰがクリアできれば，比較的多くの受験者はクリアできるレベルのものと考えられます。ちなみに，午前Ⅰ試験と午前Ⅱ試験の合格率を示すと，図表 11 のようになります。

| 年　度 | 午前Ⅰ試験 | 午前Ⅱ試験 |
|---|---|---|
| 平成 30 年度秋期 | 51.7% | 71.2% |
| 平成 31 年度春期 | 50.8% | 79.8% |
| 令和元年度秋期 | 51.9% | 86.1% |

**図表 11　午前Ⅰ試験と午前Ⅱ試験の合格率の比較**

令和元年度秋期の午前Ⅰ試験の合格率は，平成 31 年度春期に比べると約 1 ポイント向上し，1 年前に実施された平成 30 年度秋期とほぼ同じ水準といえます。このように，午前Ⅰ試験の合格率は，支援士試験になって以来，一度も 60%を超えたことはありませんが，今回の 51.9%という数字は，低めの合格率になっています。このため，午前Ⅰ試験を受験する必要のある方は，図表 4 で示した，幅広い情報処理技術分野の知識を十分に把握して試験に臨むことが必要です。なお，午前Ⅰ試験には免除制度がありますので，この制度を利用できるように，応用情報技術者試験に合格するか，いずれかの高度試験の午前Ⅰ試験に合格しておくこ

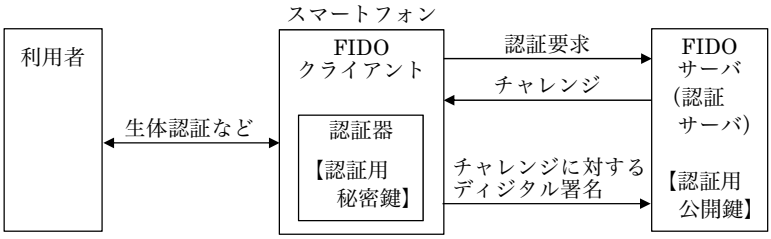
# ●令和元年度秋期

# 午前Ⅱ問題 解答・解説

## 問1　イ

FIDO UAF 1.1 に基づく認証処理（R1 秋-SC 午前Ⅱ問 1）

FIDO（ファイド）（Fast IDentity Online）は，パスワードに依存しない，あるいはパスワードへの依存を少なくすることを目的とする認証方式の規格である。現在，FIDO には FIDO UAF（Universal Authentication Framework）1.1，FIDO U2F（Universal Second Factor）1.2，FIDO2 の三つの規格がある。これらのうち，FIDO UAF 1.1 と FIDO2 は，パスワードを使わないパスワードレス認証方式である。FIDO UAF 1.1 は，主にスマートフォンによる利用を想定した規格で，その概要を次に示す。




FIDO サーバ（認証サーバ）には，認証器（オーセンティケータ；Authenticator）の情報と認証用公開鍵を事前に登録しておく。認証は次の手順で行われる。

① FIDO クライアントが FIDO サーバへ認証要求を行うと，FIDO サーバはチャレンジを応答する。

② FIDO クライアントでは，認証器を用いて利用者に認証操作を要求し，生体認証や PIN コード（暗証コード）認証などの方法で利用者を認証する。

③ 利用者の認証に成功すると，認証器は認証用秘密鍵を用いてチャレンジに対するディジタル署名を計算し，FIDO サーバへ送信する。

④ FIDO サーバでは，認証用公開鍵で署名を検証して利用者の認証を行う。

FIDO UAF 1.1 では，以上のような手順によって認証を行う。したがって，SaaS 接続時の認証において，スマートフォンで顔認証を行った後，スマートフォン内の秘密鍵でディジタル署名を生成して，そのディジタル署名を認証サーバに送信したと記述された（イ）が正しい。

その他の記述は，次のように UAF 1.1 に基づいた認証処理ではない。

ア：UAF 1.1 の特徴は，認証器を用いて利用者認証をローカルで行うことであり，PIN コードのような利用者の認証情報は認証サーバに送信されない。

## 問1　電子メールのセキュリティ対策　(R1 秋-SC 午後Ⅰ問 1)

**【解答例】**

［設問1］　a：MAIL FROM

［設問2］　(1) b：×　c：×　d：×　e：×　f：×　g：○　h：×　i：×

(2) j：x1.y1.z1.1

(3) 送信側の DNS サーバに設定された IP アドレスと SMTP 接続元の IP アドレスが一致しないから。

(4) メール本文及びメールヘッダの改ざんの有無

［設問3］　k：mail.x-sha.co.jp.　l：x2.y2.z2.1　m：quarantine　n：r

［設問4］　N 社の取引先と似たメールアドレスから送信ドメイン認証技術を利用してメールを送信する。

**【解説】**

本問は，電子メールのセキュリティのうち，送信ドメイン認証技術の SPF（Sender Policy Framework），DKIM（DomainKeys Identified Mail），DMARC（Domain-based Message Authentication, Reporting, and Conformance）を中心とした問題である。DNS サーバのゾーンファイルや，DNS の名前解決の仕組みなどに関する知識が必要とされるが，これらの専門知識を有していれば，設問 1 から設問 3 までの多くの小問に正解できると考えられる。これに対し，設問 4 は，問題文の記述内容を基にしただけでは解答を導くことが難しいと思われるので，比較的難度の高い設問といえる。

［設問1］

空欄 a は，「送信者メールアドレスには，SMTP の［ a ］コマンドで指定されるエンベロープの送信者メールアドレス（以下，Envelope-FROM という）と，メールデータ内のメールヘッダで指定される送信者メールアドレス（以下，Header-FROM という）がある」という記述の中にある。

SMTP（Simple Mail Transfer Protocol）を使って，メールを送信する際には，メールの送信者のメールアドレスのほか，受信者のメールアドレス，メールデータ（メールヘッダとメール本文）などの情報をそれぞれ指定する必要がある。そのために，幾つかのコマンドが規定されており，エンベロープの送信者メールアドレスを指定するためのコマンドが MAIL コマンドである。この MAIL コマンドは，“MAIL FROM：<メールアドレス>”という形式で用いられることから，一般に MAIL FROM コマンドと呼ばれている。したがって，空欄 a には“MAIL FROM”が入る。

なお，Header-FROM で指定されるメールアドレスは，メールデータ内の情報なので，メールクライアントが DATA コマンドを投入後，メールサーバから OK 応答があると，メールデータの一部として送信される。また，メールの受信者のメールアドレ

## 問1　ソフトウェア開発におけるセキュリティ対策　(R1 秋-SC 午後Ⅱ問 1)

**【解答例】**

［設問１］
(1) DBMS-R における同じ脆弱性を悪用されて，別のマルウェア X またはほかのマルウェアに再度感染してしまい，マルウェア X の動作が阻害される。
(2) α：カ　β：ク　γ：ア
(3) マルウェア X には，暗号資産の採掘プログラムによる採掘演算結果以外の情報を外部に送信する機能はなく，マルウェア X 以外による遠隔コマンド実行及び SSH サービスへの接続がなかったから。

［設問２］
(1) 対策 1：(イ)　対策 2：(イ)　対策 3：(ア)，(エ)
対策 4：(ウ)，(エ)，(オ)
(2) あ：22/tcp　い：6379/tcp　う：a2.b2.c2.d2
(3) a：curl　b：iptables
(4) え：オ　お：カ　か：キ

［設問３］
(1) ア，ウ
(2) S 社のシステムを構成する実行環境のバージョン情報を把握して，その情報を常に最新にしておくこと
(3) き：ア　く：ウ
(4) け：レビュー　こ：第三者

［設問４］ c：オ　d：ア　e：エ　f：カ　g：キ　h：ウ

**【解説】**

本問は，開発と運用を一体的に行う DevOps にセキュリティ対策の考え方を取り入れた，DevOpsSec（DevSecOps なども使われる）をテーマとして，マルウェアの活動や機能，ルートキットの動作，インシデント被害の影響，多層的なマルウェア対策方法，FW ルールの見直し，ファイルの改ざん検知方法，開発・運用プロセスの見直し，開発・運用におけるコンテナ技術の活用などに関する問題である。

Linux のコマンドや DevOps に関する用語などは，今回が初めての出題であり，これらの分野の知識がなければ難しいといえる。また，設問 1 (1)や(3)のように解答する字数が多い設問は，本文の記述内容をうまく引用するなどして分かりやすく表現することが必要である。そして，開発・運用プロセスのうち，脆弱性対応や検証作業に関する考察問題は，一般的な知識に加えて本文の記述内容を確認しながら要点をまとめていくとよいだろう。

［設問１］

(1) この設問は，下線①について，挿入されなかった場合，攻撃者の意図に反して，どのようなことが起こると想定できるかを述べるものである。なお，下線①は，次

# 情報処理安全確保支援士試験

平成 30 年度秋期, 平成 31 年度春期, 令和元年度秋期に行われた高度午前Ⅰ（共通知識）試験，情報処理安全確保支援士午前Ⅱ試験を分析し，問題番号順と，3 回分を合わせた「午前の出題範囲」の出題分野順にまとめた表を掲載します。

また，出題分野の基になっている「午前の出題範囲」の詳細も掲載します。

情報処理安全確保支援士試験を受験する際に，過去の SC 試験の出題分析は重要な資料になります。

## （1）午前問題出題分析

・問題番号順

平成 30 年度秋期　高度午前Ⅰ（共通知識）試験
平成 30 年度秋期　情報処理安全確保支援士 午前Ⅱ試験
平成 31 年度春期　高度午前Ⅰ（共通知識）試験
平成 31 年度春期　情報処理安全確保支援士 午前Ⅱ試験
令和元年度秋期　高度午前Ⅰ（共通知識）試験
令和元年度秋期　情報処理安全確保支援士 午前Ⅱ試験

・高度午前Ⅰ（共通知識）試験の出題範囲順
（平成 30 年度秋期，平成 31 年度春期，令和元年度秋期）

・情報処理安全確保支援士　午前Ⅱ試験の出題範囲順
（平成 30 年度秋期，平成 31 年度春期，令和元年度秋期）

## （2）午前の出題範囲

## （3）午後Ⅰ，午後Ⅱ問題　予想配点表

# （1）午前問題出題分析

・問題番号順

平成 30 年度秋期 高度午前 I （共通知識）試験

| 問 | 問 題 タ イ ト ル | 正解 | 分野 | 大 | 中 | 小 | 難易度 |
|---|---|---|---|---|---|---|---|
| 1 | 排他的論理和の相補演算 | ア | T | 1 | 1 | 1 | 3 |
| 2 | 平均待ち時間が平均処理時間以上となる利用率 | イ | T | 1 | 1 | 2 | 4 |
| 3 | 正規分布における得点者数の推定 | イ | T | 1 | 1 | 2 | 3 |
| 4 | 2 次元配列の要素数 | イ | T | 1 | 2 | 1 | 2 |
| 5 | メモリの誤り制御方式 | エ | T | 2 | 3 | 2 | 2 |
| 6 | 仮想記憶においてページインだけの処理の割合 | エ | T | 2 | 5 | 1 | 3 |
| 7 | 半加算器の論理回路 | ア | T | 2 | 6 | 1 | 2 |
| 8 | レンダリングの説明 | イ | T | 3 | 8 | 2 | 3 |
| 9 | 全てのハッシュ値が衝突する除数 | ウ | T | 3 | 9 | 2 | 3 |
| 10 | プログラムが並行実行できるアクセスモードの組合せ | エ | T | 3 | 9 | 4 | 3 |
| 11 | スイッチングハブに相当する装置 | イ | T | 3 | 10 | 2 | 2 |
| 12 | 利用者個人のディジタル証明書を用いた TLS 通信を行う効果 | エ | T | 3 | 11 | 5 | 4 |
| 13 | クロスサイトスクリプティング対策に該当するもの | ウ | T | 3 | 11 | 5 | 3 |
| 14 | ブルートフォース攻撃に該当するもの | ウ | T | 3 | 11 | 1 | 3 |
| 15 | 脆弱性検査手法のファジング | イ | T | 3 | 11 | 5 | 3 |
| 16 | 安全性と信頼性に関するプログラム設計の方針 | ア | T | 4 | 12 | 4 | 2 |
| 17 | アジャイル開発で“イテレーション”を行う目的 | ア | T | 4 | 13 | 1 | 3 |
| 18 | トレンドチャートの説明 | ウ | M | 5 | 14 | 6 | 2 |
| 19 | ファンクションポイント法の見積りで必要な情報 | イ | M | 5 | 14 | 7 | 2 |
| 20 | サービスライフサイクルの段階 | イ | M | 6 | 15 | 1 | 3 |
| 21 | サンプリング（試査）に関する用語の説明 | ア | M | 6 | 16 | 1 | 3 |
| 22 | 情報システムの可監査性 | ア | M | 6 | 16 | 1 | 3 |
| 23 | 業務プロセスの可視化における UML の活用シーン | ウ | S | 7 | 17 | 2 | 3 |
| 24 | IT 投資に対する KPI の例 | エ | S | 7 | 17 | 4 | 3 |
| 25 | システム化構想の立案プロセスで行うべきこと | ア | S | 7 | 18 | 1 | 3 |
| 26 | 類似性で集団を分類し分析する手法 | ア | S | 8 | 19 | 2 | 3 |
| 27 | IoT がもたらす効果の“自律化”の段階 | ウ | S | 8 | 21 | 2 | 3 |
| 28 | 生産計画における正味所要量の計算 | イ | S | 8 | 21 | 2 | 2 |
| 29 | 変動費の計算 | ウ | S | 9 | 22 | 3 | 3 |
| 30 | 下請代金支払遅延等防止法で禁止されている行為 | イ | S | 9 | 23 | 3 | 3 |

# (3) 午後Ⅰ，午後Ⅱ問題　予想配点表

■平成 30 年度秋期 情報処理安全確保支援士試験
午後Ⅰの問題（問 1～問 3 から 2 問選択）

| 問番号 | 設問 | 設問内容 | 小問数 | 小問点 | 配点 | 満点 |
|---|---|---|---|---|---|---|
| 問 1 | 1 | (1)a～d | 4 | 3 | 12 | 50 |
| | | (2) | 1 | 3 | 3 | |
| | | (3) | 1 | 6 | 6 | |
| | 2 | (1) e，f | 2 | 3 | 6 | |
| | | (2) g | 1 | 4 | 4 | |
| | 3 | (1)行番号 | 1 | 3 | 3 | |
| | | 排除できない理由 | 1 | 6 | 6 | |
| | | (2)問題 | 1 | 4 | 4 | |
| | | 開発環境 | 1 | 6 | 6 | |
| 問 2 | 1 | a～e | 5 | 2 | 10 | 50 |
| | 2 | (1) | 1 | 3 | 3 | |
| | | (2)(a)，(b) | 2 | 5 | 10 | |
| | 3 | (1) | 1 | 6 | 6 | |
| | | (2)イ，オ，カ | 3 | 2 | 6 | |
| | 4 | (1)①，② | 2 | 5 | 10 | |
| | | (2) | l | 5 | 5 | |
| 問 3 | 1 | | 1 | 5 | 5 | 50 |
| | 2 | | 1 | 4 | 4 | |
| | 3 | | 1 | 8 | 8 | |
| | 4 | 調査すべき機器 | 1 | 4 | 4 | |
| | | 調査すべき内容 | 1 | 8 | 8 | |
| | 5 | (1) b | 1 | 3 | 3 | |
| | | (2) | 1 | 8 | 8 | |
| | | (3) c，d | 2 | 5 | 10 | |
| | | | | | 合計 | 100 |