目　　次

平成 30 年度春期　問題と解答･解説編

＜出題分析＞

0. 国家資格　情報処理安全確保支援士とは

情報処理安全確保支援士試験（以下，支援士試験という）とはどのような制度・試験なのでしょうか。本章では，2016 年 10 月 21 日に，独立行政法人情報処理推進機構（以下，IPA という）から公表された試験概要をまとめています。なお，試験内容の詳細については，「1. 情報処理安全確保支援士試験の概要」をご確認ください。

0-1　“情報処理安全確保支援士試験”制度創設の背景

社会全体として早急な情報セキュリティ人材の確保が求められているなか，独立行政法人情報処理推進機構（以下，IPA という）が実施する国家試験「情報処理技術者試験」においては，次のような取組みがなされてきました。

・情報セキュリティスペシャリスト（SC）試験の実施
・SC 以外の全ての試験区分における，情報セキュリティ関連の出題強化・拡充（平成 26 年度～）。
・「情報セキュリティマネジメント試験」の創設（平成 27 年 10 月），実施（平成 28 年度春期試験～）。

しかしながら，情報処理試験に関しては，一度試験に合格すると，その後のフォローがなく，最新の動向を踏まえて専門的な知識・技能が維持されているか確認できないといった指摘もありました。新設される支援士試験制度は，情報セキュリティの専門的な知識・技能を有する人材を登録・公表するもので，更新制度を伴うものとなっています。

3. 第3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。このため，これまでの情報セキュリティスペシャリスト試験の傾向を分析し，その結果に基づいて，受験対策を行うことは有効であるといえます。

平成 28 年度秋期から平成 29 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，平成 21 年度秋期試験の合格率（18.5%）をピークに，その後，徐々に低下し，おおむね 13%台ないしは 14%台で推移してきました。支援士試験としては，これまでに 2 回実施されましたが，平成 29 年度秋期試験の合格率は，第 1 回の 16.3%を超える 17.1%になりました。

●平成 30 年度春期
午前 I 問題 解答・解説

問1 ア

ハミング符号の誤りビット訂正（H30 春・高度 午前 I 問 1）

ハミング符号 1110011 から，情報ビット，冗長ビットは次のようになる。

$X_1=1$，$X_2=1$，$X_3=1$，$X_4=0$，$P_1=1$，$P_2=1$，$P_3=0$

これらを与えられた式に当てはめる。

$X_1 \oplus X_3 \oplus X_4 \oplus P_1 = 1 \oplus 1 \oplus 0 \oplus 1 = 1$

$X_1 \oplus X_2 \oplus X_4 \oplus P_2 = 1 \oplus 1 \oplus 0 \oplus 1 = 1$

$X_1 \oplus X_2 \oplus X_3 \oplus P_3 = 1 \oplus 1 \oplus 1 \oplus 0 = 1$

誤りがなければ，全ての式が 0 になるが，誤りビットを含んでいる式は 1 になる。したがって，三つの式の全てに誤りビットを含んでいることを示している。そして，この三つの式に共通して含まれているのは X_1 だけなので，誤りは X_1 の 1 であることが分かる。これを 0 に訂正すると，正しいハミング符号は，0110011 となり，（ア）が正解となる。

問2 ウ

定義された再帰関数の実行結果（H30 春・高度 午前 I 問 2）

非負の整数 m, n に対して定義された関数 Ack(m, n)は，$m>0$ かつ $n>0$ のとき，再帰的に呼出しが行われている。

再帰呼出し

$$\mathrm{Ack}(m, n)=\begin{cases}\mathrm{Ack}(m-1, \mathrm{Ack}(m, n-1)) & (m>0 \text{ かつ } n>0 \text{ のとき}) \quad \cdots① \\ \mathrm{Ack}(m-1, 1) & (m>0 \text{ かつ } n=0 \text{ のとき}) \quad \cdots② \\ n+1 & (m=0 \text{ のとき}) \quad \cdots③\end{cases}$$

$\mathrm{Ack}(1, 3)=\mathrm{Ack}(0, \mathrm{Ack}(1, 2))$ （①の呼出し）

$=\mathrm{Ack}(0, \mathrm{Ack}(0, \mathrm{Ack}(1, 1)))$ （①の呼出し）

$=\mathrm{Ack}(0, \mathrm{Ack}(0, \mathrm{Ack}(0, \mathrm{Ack}(1, 0))))$ （①の呼出し）

$=\mathrm{Ack}(0, \mathrm{Ack}(0, \mathrm{Ack}(0, \mathrm{Ack}(0, 1))))$ （②の呼出し）

$=\mathrm{Ack}(0, \mathrm{Ack}(0, \mathrm{Ack}(0, 2)))$ （③の呼出し）

$=\mathrm{Ack}(0, \mathrm{Ack}(0, 3))$ （③の呼出し）

$=\mathrm{Ack}(0, 4)$ （③の呼出し）

$=5$

したがって，（ウ）が正解である。

●平成 30 年度春期
午前Ⅱ問題 解答・解説

問1 ア

CVSS v3 の基本評価基準の説明（H30 春-SC 午前Ⅱ問 1）

CVSS（Common Vulnerability Scoring System；共通脆弱性評価システム）は，IT 製品の脆弱性の深刻度を評価する手法である。CVSS では，次の三つの基準で脆弱性を評価する。なお，v3 は現在（2018 年 6 月時点）の最新バージョンである。

① 基本評価基準（Base Metrics）

脆弱性そのものの特性を評価する基準で，攻撃元区分，攻撃条件の複雑さ，攻撃に必要な特権レベル，利用者の関与の要否，影響の想定範囲，機密性への影響，完全性への影響，可用性への影響の 8 種類の特性で評価する。基本評価基準による評価結果は固定していて，時間の経過や利用環境の違いによって変化しない。IPA が運営している JVN iPedia（脆弱性対策情報データベース）では，脆弱性の深刻度の基準値として，この基本評価基準の数値を公表している。

② 現状評価基準（Temporal Metrics）

評価時点における脆弱性の特性を評価する基準で，攻撃される可能性，利用可能な対策のレベル，脆弱性情報の信頼性の 3 種類の特性で評価する。現状評価基準による評価結果は，脆弱性への対応状況に応じて，時間が経過すると変化することが特徴である。

③ 環境評価基準（Environmental Metrics）

製品利用者の利用環境や緩和策の実施状況を再評価して，脆弱性の最終的な深刻度を評価する基準で，機密性の要求度，完全性の要求度，可用性の要求度，緩和策後の攻撃元区分，緩和策後の攻撃条件の複雑さ，緩和策後の攻撃に必要な特権レベル，緩和策後の利用者の関与の要否，緩和策後の影響の想定範囲，緩和策後の機密性への影響，緩和策後の完全性への影響，緩和策後の可用性への影響の 11 種類の特性で評価する。環境評価基準による評価結果は，脆弱性に対して想定される脅威に応じ，製品利用者ごとに変化することが特徴である。

これらの内容を踏まえて解答群を検討すると，次のようになる。

ア：基本評価基準に該当する。

イ：現状評価基準に該当する。

ウ：機会，正当化，動機の三つの観点は，内部不正が発生する際に働く不正のトライアングルにおける 3 要素であり，CVSS の基準ではない。

エ：環境評価基準に該当する。

したがって，（ア）が正しい。

●平成 30 年度春期

午後Ⅰ問題 解答・解説

問1　ソフトウェアの脆弱性

(H30 春-SC 午後Ⅰ問 1)

【解答例】

［設問1］　a：カ　　b：ウ
［設問2］　785634120a
［設問3］　c：(エ)
［設問4］　d：0x0b123400
［設問5］　e：ヒープ
［設問6］　ライブラリ関数はデータ実行防止の対象ではないメモリ領域に配置されているから。
［設問7］　f：(ア)
［設問8］　g：DisplayNote
［設問9］　h：m_note = NULL;

【解説】

プログラム言語として C++を対象とするセキュアプログラミング問題で，Use-After-Free の脆弱性などに関して出題されている。C++のセキュアプログラミング問題では，バッファオーバフローをテーマとする出題が多いが，Use-After-Free が初めて取り上げられた。本問では，Use-After-Free の前提知識がなくても，本文の記述に従って脆弱性を理解しながら解答できるようになっている。後半のデータ実行防止機能や ASLR（アドレス空間配置ランダマイゼーション）機能は，過去問題でも出題されている。C++の知識に加え，制限時間内で記述内容を正確に読み取れるかどうかという理解力がポイントになると思われる。

［設問1］

空欄 a は，T 主任の「確保済みメモリ領域を超えてデータを書き込んでしまう［ a ］と呼ばれる脆弱性の報告が以前から多かった」という発言の中にある。解答群の中で，確保済みメモリ領域を超えてデータを書き込むという特徴に整合する脆弱性は，バッファオーバフロー（BOF；Buffer Overflow）（カ）である。したがって，空欄 a には“カ”が入る。BOF 脆弱性には，スタック領域を超えてデータを書き込んでしまうスタック BOF や，ヒープ領域を超えてデータを書き込んでしまうヒープ BOF などがある。BOF 脆弱性がある場合，プログラムが確保したサイズを超える入力データを書き込むと，メモリ領域があふれて隣接するメモリ領域を上書きしてしま

●平成 30 年度春期
午後Ⅱ問題 解答・解説

問1　セキュリティ対策の評価

(H30 春-SC 午後Ⅱ問 1)

【解答例】

［設問１］ (1) 脆弱性の有無によってサーバからのレスポンスに違いがないから。
(2) スクリプトを分析し，フラグメント識別子の値の変化による挙動を確認する。
(3) R ポータルが利用しているスクリプトが Cookie の値を利用している場合

［設問２］ 踏み台サーバの操作記録機能によって，ログインした利用者のデスクトップ画面，実行したコマンド，及びキーボード入力を記録する。

［設問３］ (1) a：WebAP サーバ　b：DB サーバ　c：ODBC
ルール：項番 9
(2) 人事総務課の職員が踏み台サーバを経由して DB サーバに共通管理者アカウントでログインする行為
(3) d：2

［設問４］ (1) e：製作パートナに渡す CCI の数
(2) f：CC をインストールした PC を協力者宛てに輸送
(3) g：DRM サーバへの通信を製作パートナのグローバル IP アドレスからだけに制限する

【解説】

特定の取引先が利用するポータルサイトを題材として，Web アプリケーションのセキュリティ対策，共通アカウント利用時における証跡確保やリスクの考察，サーバのアクセス制御，ファイアウォールのフィルタリングルールの考察，取引先とのセキュアな図面データ交換方法の考察などの問題が出題されている。本問は，午後Ⅱ試験としては解答数が少ないので，一つ一つの設問に十分に時間をかけて，具体的に解答することがポイントといえる。なお，設問 1 は，頻出テーマの XSS に関する知識を十分に整理して試験に臨んだ受験者にとっては解答しやすいと思われる。

［設問１］

(1) この設問は，下線①（検知方法 1 では脆弱性 2 を検知できない）について，サーバからのレスポンスの内容を見て脆弱性を判断するツールを用いた場合，脆弱性 2 を検知できない理由を述べるものである。

・問題番号順

平成 30 年度春期 情報処理安全確保支援士 午前 II 試験

問	問 題 タ イ ト ル	正解	分野	大	中	小	難易度
1	CVSS v3 の基本評価基準の説明	ア	T	3	11	3	3
2	HTTP リクエストヘッダを悪用した脆弱性	イ	T	3	11	1	4
3	XML ディジタル署名の特徴	ア	T	3	11	1	3
4	エクスプロイトコードの説明	ア	T	3	11	1	3
5	シングルサインオンの実装方式	エ	T	3	11	1	3
6	ダイナミックパケットフィルタリングの特徴	ウ	T	3	11	4	3
7	ディジタル署名の生成に使用する鍵	エ	T	3	11	1	2
8	CRL に関する記述	エ	T	3	11	1	3
9	認証デバイスに関する記述	イ	T	3	11	1	3
10	サイバー情報共有イニシアティブの説明	エ	T	3	11	2	3
11	cookie の secure 属性の動作	ウ	T	3	11	5	3
12	DKIM の説明	ア	T	3	11	5	3
13	テンペスト攻撃の説明	ウ	T	3	11	1	3
14	マルウェアのダウンロードを防ぐ方策	イ	T	3	11	4	3
15	ルートキットの特徴	ア	T	3	11	5	3
16	DNSSEC で実現できること	ア	T	3	11	5	3
17	SQL インジェクション対策	エ	T	3	11	5	3
18	ICMP を識別するためのヘッダ情報	ア	T	3	10	3	4
19	VLAN 機能を有したスイッチのポートの種類	ウ	T	3	10	2	3
20	WebDAV の特徴	イ	T	3	10	5	3
21	コミット処理完了とみなすタイミング	エ	T	3	9	4	3
22	UML 2.0 の表記図法	ウ	T	4	12	3	3
23	XP におけるテスト駆動開発の特徴	エ	T	4	13	1	3
24	IT サービスの可用性計算	ウ	M	6	15	3	3
25	監査人が報告すべき指摘事項	ア	M	6	16	1	3

■平成 30 年度春期 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	a，b	2	3	6	50
	2		1	5	5	
	3	c	1	5	5	
	4	d	1	5	5	
	5	e	1	5	5	
	6		1	8	8	
	7	f	1	5	5	
	8	g	1	5	5	
	9	h	1	6	6	
問 2	1	(1)a	1	4	4	50
		(2)b～d	3	4	12	
	2	(1)e	1	8	8	
		(2)	2	6	12	
	3	(1)	1	6	6	
		(2)	1	8	8	
問 3	1	(1)a，b	2	2	4	50
		(2)c，d	2	2	4	
	2	(1)	1	6	6	
		(2)e～g	2	3	6	
		方法	1	6	6	
		(3)	1	6	6	
	3	h，j	2	2	4	
		i，k	4	2	8	
	4	l	1	6	6	
					合計	100