目　　次

平成 30 年度秋期　問題と解答･解説編

＜出題分析＞

3. 第５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 29 年度秋期から平成 30 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。支援士試験になってからの合格率は 16～17%程度に向上し，今回の合格率は過去最高に並ぶ結果になりました。そして，IPA の発表によりますと，平成 30 年 10 月 1 日現在，“登録セキスペ”の登録者数は 17,360 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 29 年度秋期	23,425（-6.8%）	16,218（69.2%）	2,767（17.1%）
平成 30 年度春期	23,180（-1.0%）	15,379（66.3%）	2,596（16.9%）
平成 30 年度秋期	22,447（-3.2%）	15,257（68.0%）	2,818（18.5%）

（ ）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 29 年度秋期から平成 30 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 29 年度秋期	47.9%	76.8%
平成 30 年度春期	58.2%	78.2%
平成 30 年度秋期	51.7%	71.2%

図表 11　午前Ⅰ試験と午前Ⅱ試験の合格率の比較

平成 30 年度秋期の午前Ⅰ試験の合格率は，平成 30 年度春期に比べると 6.5 ポイント低下しましたが，1 年前に実施された平成 29 年度秋期に比較すると約 4 ポイント向上しています。このように，午前Ⅰ試験の合格率は，変動幅が大きいことが特徴ですが，今回の 51.7%という数字は，やや低めの合格率といえます。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とも一

●平成 30 年度秋期
午前Ⅰ問題 解答・解説

問1 ア

排他的論理和の相補演算（H30 秋-高度 午前Ⅰ問 1）

演算 A の相補演算とは，演算 A の演算結果（真偽）と結果が否定関係，つまり，全く逆となる演算のことなので，演算 A の否定と等価（演算結果が同じ）となる。

二つのオペランド（演算対象）A，B に対して，“・”(論理積)，“＋”(論理和)，“¯”(論理否定)を用いて排他的論理和を表すと，$\overline{A}\cdot B+A\cdot\overline{B}$ となる。これをベン図で表すと次の左図の部分になる。この演算の否定を考えると右図の部分になり，（ア）が正解であることが分かる。

図 排他的論理和とその否定

参考までに，排他的論理和の否定を次のように変形しても相補演算の式を得ることができる。

$$
\begin{aligned}
\text{排他的論理和の否定}&=\overline{\overline{A}\cdot B\ +\ A\cdot\overline{B}}\\
&=\overline{\overline{A}\cdot B}\ \cdot\ \overline{A\cdot\overline{B}} \quad \text{（ド・モルガンの法則）}\\
&=(\overline{\overline{A}}+\overline{B})\cdot(\overline{A}+\overline{\overline{B}}) \quad \text{（ド・モルガンの法則）}\\
&=(A+\overline{B})\cdot(\overline{A}+B) \quad \text{（二重否定を外す）}\\
&=A\cdot\overline{A}\ +\ A\cdot B\ +\ \overline{B}\cdot\overline{A}\ +\ \overline{B}\cdot B \quad \text{（分配法則）}\\
&=A\cdot B\ +\ \overline{B}\cdot\overline{A} \quad (A\cdot\overline{A}\text{ と }B\cdot\overline{B}\text{ は 0 なので，省略可})
\end{aligned}
$$

問2 イ

平均待ち時間が平均処理時間以上となる利用率（H30 秋-高度 午前Ⅰ問 2）

問題の伝票データをためる待ち行列の特徴は，この待ち行列が平均サービス時間 T秒の M/M/1 待ち行列モデルに従うことを示している。一般に，M/M/1 待ち行列モデルでは，対象となる資源の利用率をρで表すことが多いので，この記号を用いて平均待ち時間を表すと，$\{\rho/(1-\rho)\}\times T$（秒）となる。この式の前半にある$\rho/(1-\rho)$の部分に注目すると，利用率$\rho$が大きくなるほど，分子が大きくなり，分母は小さくなる。そして，全体としてはρが大きくなるほど大きくなり，平均待ち時間も大きくなる。これは，忙しいほど（利用率大）窓口で待たさ

●平成 30 年度秋期
午前Ⅱ問題 解答・解説

問1 ア

AES の特徴（H30 秋-SC 午前Ⅱ問 1）

AES（Advanced Encryption Standard）は，ブロック長 128 ビットのブロックと呼ばれる固定長のデータを単位として暗号化／復号を行う暗号化方式である。鍵長を 128，192，256 ビットの三つの中から選択することができる。暗号化の段数は鍵長によって，それぞれ 10，12，14 となっている。したがって，（ア）が正しい。なお，AES の基となった“Rijndael”では，ブロック長と鍵長はともに可変である。

その他の記述には，次のような誤りがある。

イ：鍵長は選択できるが，段数は選択できない。

ウ：トリプル DES（3DES）の説明である。

エ：AES は共通鍵暗号方式であるので，公開鍵は使用しない。

問2 ウ

CVE 識別子の説明（H30 秋-SC 午前Ⅱ問 2）

CVE（Common Vulnerabilities and Exposures；共通脆弱性）識別子は，個別製品中の脆弱性を識別するために，米国政府の支援を受けた非営利団体の MITRE 社が採番している識別子である。CVE 識別番号は「CVE-西暦-連番」という形式で，セキュリティベンダや製品開発ベンダ，研究者などのセキュリティ専門家が，報告のあった脆弱性を評価し割当て作業を行っている。したがって，（ウ）が正しい。

JVN（Japan Vulnerability Notes）は，日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供する脆弱性対策ポータルサイトで，JPCERT/CC と IPA が共同で運営している。JVN では独自の脆弱性識別番号に加えて，CVE 識別子も採用して情報を提供している。

その他の記述が示すものは，次のとおりである。

ア：CCE（Common Configuration Enumeration；共通セキュリティ設定一覧）のことである。

イ：多種多様な脆弱性の種類を脆弱性タイプとして分類し，それらを識別するための CWE（Common Weakness Enumeration；共通脆弱性タイプ一覧）という識別子は存在するが，脆弱性が悪用されて改ざんされた Web サイトのスクリーンショットを識別するような共通の識別子はない。

エ：CPE（Common Platform Enumeration；共通プラットフォーム一覧）のこ

●平成 30 年度秋期
午後Ⅰ問題 解答・解説

問1 ソフトウェア開発

(H30 秋-SC 午後Ⅰ問 1)

【解答例】

［設問1］ (1) a：キ　b：カ　c：ウ　d：ア

(2) あ：㋒

(3) shell コードが DEP で実行禁止にされているスタック領域にあるから。

［設問2］ (1) e：canary　f：ASLR

(2) g：strcpy

［設問3］ (1) 行番号：16 行目

排除できない理由：ポインタを使って直接メモリを操作しているから。

(2) 問題：メモリ破壊攻撃を防げないこと

開発環境：SSP を適用できないコンパイラを利用する開発環境

【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ある。C++の問題として，定番テーマといえるメモリ破壊脆弱性であるスタックバッファオーバフロー脆弱性対策が出題されている。対策技術の DEP（データ実行防止）機能や ASLR（アドレス空間配置のランダム化）機能は，過去問題でも複数回出題されており，本文中でも説明されているので，全体としては解答しやすい設問が多いといえる。設問3 (2)は設問の主旨を理解することがポイントになると思われる。

［設問1］

(1) 空欄 a は，「図 2 は Vuln 内の関数 foo が呼び出された後のメモリマップである。プログラム実行時に，変数 b が指し示すデータが不正な場合，そのデータによって，［ a ］が［ あ ］に書き換えられると，関数 foo の終了時に shell コードへ処理が遷移する」などといった記述の中にある。ここでは，空欄 a と(2)の空欄あを合わせて解説する。

図 1（スタックバッファオーバフロー脆弱性のあるプログラム Vuln）のプログラムのうち，関数 foo の主要部までのコードを抜粋して図 A に示す。

●平成 30 年度秋期
午後Ⅱ問題 解答・解説

問1　クラウド環境におけるセキュリティ対策　(H30 秋-SC 午後Ⅱ問 1)

【解答例】

［設問１］　GDPR

［設問２］　(1) R&D 情報は，物理的な入退室管理が行われているプロジェクトルーム内に配置されたプロジェクト専用サーバに保管する。

(2) 満たせなくなる基本要件の具体的内容：

① 生産関連サーバは，X 社の工場及びデータセンタに配置する。

② 生産関連サーバのバックアップを他の工場又はデータセンタに配置する。

③ 同じ重要インフラ設備を製造する工場及び生産関連サーバは同一の国又は地域内の 2 か所以上に配置する。

IaaS C のサービス仕様の内容：日本国内のデータセンタが被災した場合はシンガポールのデータセンタでサービスが継続される。

(3) X 社のシステムの機器に割り当てている IP アドレスが，IaaS C で予約されているプライベートアドレスと重複する可能性があるという問題

［設問３］　(1) 一度のログインで全システムにアクセスできるという利便性

(2) 業務サーバ：㋑，㋒

構成要素：㋖，㋗，㋘，㋙

［設問４］　(1) ティア 1：イ　　ティア 2：ウ　　ティア 3：ア

(2) 標準ソフトウェア以外のソフトウェアは，脆弱性管理がされないという不都合

(3) ① 正確である。

② 作業が速くできる。

［設問５］　(1)

		クライアント	業務サーバ
案 A	①	Ⓗ	Ⓓ
	②	Ⓘ	Ⓓ
案 B	①	Ⓖ	Ⓑ
	②	Ⓗ	Ⓑ
	③	Ⓘ	Ⓑ

情報処理安全確保支援士試験

平成 29 年度秋期，平成 30 年度春期，平成 30 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 29 年度秋期　高度午前Ⅰ（共通知識）試験
平成 29 年度秋期　情報処理安全確保支援士 午前Ⅱ試験
平成 30 年度春期　高度午前Ⅰ（共通知識）試験
平成 30 年度春期　情報処理安全確保支援士 午前Ⅱ試験
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

・高度午前Ⅰ（共通知識）試験の出題範囲順
（平成 29 年度秋期，平成 30 年度春期，平成 30 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 29 年度秋期，平成 30 年度春期，平成 30 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

(3) 午後Ⅰ，午後Ⅱ問題　予想配点表

■平成 29 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	3	3	50
	2	(1)a，b	2	3	6	
		(2)	1	4	4	
		(3)営業用 PC の設定，ランサムウェア X の特徴	2	4	8	
		(4)	1	6	6	
	3	(1)c～h	6	1	6	
		(2)	1	6	6	
		(3)	1	5	5	
	4		1	6	6	
問 2	1	(1)ア，イ	2	2	4	50
		必要な全てのコードの並び	1	6	6	
		(2)	1	3	3	
		(3)	1	3	3	
	2	(1)a，b	2	3	6	
		(2)	1	8	8	
	3	(1)	1	6	6	
		(2)	1	6	6	
		(3)	1	8	8	
問 3	1	(1)a～d	4	2	8	50
		(2)	1	6	6	
		(3)	1	2	2	
	2	(1)ア，イ	2	2	4	
		(2)①，②	2	4	8	
		(3)	1	3	3	
	3	(1)	1	6	6	
		(2)	2	2	4	
		(3)	1	3	3	
		(4)	1	6	6	
					合計	100