目　　次

平成 31 年度春期　問題と解答･解説編

＜出題分析＞

3. 第６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 年度春期から平成 31 年度春期までの受験者数，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 回で 18.5%に向上しました。今回の試験では過去最高の 18.9%になり，約 5.3 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，平成 31 年 4 月 1 日現在，“登録セキスペ”の登録者数は 18,330 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%）
平成 31 年度春期	22,447（-3.2%）	14,556（65.6%）	2,774（18.9%）

（　）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 年度春期から平成 31 年度春期までの 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 年度春期	58.2%	78.2%
平成 30 年度秋期	51.7%	71.2%
平成 31 年度春期	50.8%	79.8%

図表 11　午前Ⅰ試験と午前Ⅱ試験の合格率の比較

平成 31 年度春期の午前Ⅰ試験の合格率は，平成 30 年度秋期に比べると約 1 ポイント，1 年前に実施された平成 30 年度春期に比較すると 7.4 ポイント低下しています。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 50.8%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

●平成 31 年度春期
午前 I 問題 解答・解説

問1　ア

定義された関数と等しい式（H31 春-高度 午前 I 問 1）

next(n)と等しい式の結果は，0≦n＜255 のとき n＋1，n＝255 のとき 0 となる。したがって，まず n＝0 のときは 1 となり，n＜255 の間は n に 1 加算した答えが求められるものでなくてはいけない。選択肢の論理式は全て，論理演算子（AND や OR）の左側が (n＋1)であり，0≦n＜255 のときには，この左側の値がそのまま演算結果となる論理式である必要がある。一方，論理演算子の右側は 255，256 であるが，これらは，2 進数表現でそれぞれ 011111111，100000000 であり，AND や OR を取ったときに左側の値（0≦n＜255）がそのまま演算結果となるのは，x AND 255 としたときだけである。

255 を 9 ビットで表現すると 011111111 で，先頭の 0 に続いて 1 が 8 ビット並んでいる。よって，n＋1 が 8 ビットで表現できる（すなわち n＋1 が 255 以下である）間は(n＋1) AND 255＝n＋1 となり，n＋1 が 256 になると(n＋1) AND 255＝0 となる。したがって，（ア）の(n＋1) AND 255 は，0≦n＜255 のとき n＋1，n＝255 のとき 0 となり，正解であることが分かる。

この問題は n として代表的な値を選んで，255（＝$(011111111)_2$）と 256（＝$(100000000)_2$)に対する論理積や論理和を計算しても正解を求めることができる。

① n＝0 のとき，n＋1＝1 となるような論理式を選ぶ。
ア：$(000000001)_2$ AND $(011111111)_2$＝$(000000001)_2$＝$(1)_{10}$
イ：$(000000001)_2$ AND $(100000000)_2$＝$(000000000)_2$＝$(0)_{10}$
ウ：$(000000001)_2$ OR $(011111111)_2$＝$(011111111)_2$＝$(255)_{10}$
エ：$(000000001)_2$ OR $(100000000)_2$＝$(100000001)_2$＝$(257)_{10}$

② n＝255 のとき，0 となることも確認する。
ア：$(100000000)_2$ AND $(011111111)_2$＝$(000000000)_2$=$(0)_{10}$
イ：$(100000000)_2$ AND $(100000000)_2$＝$(100000000)_2$=$(256)_{10}$
ウ：$(100000000)_2$ OR $(011111111)_2$＝$(111111111)_2$＝$(511)_{10}$
エ：$(100000000)_2$ OR $(100000000)_2$＝$(100000000)_2$＝$(256)_{10}$

以上からも，（ア）が正解であることが確認できる。

●平成 31 年度春期

午前Ⅱ問題 解答・解説

問1　エ

CRL に掲載されるもの（H31 春-SC 午前Ⅱ問 1）

ディジタル署名については，署名を行う秘密鍵（署名鍵ともいう）が極めて重要な役割を担っている。例えば，秘密鍵が漏えいしたり，危殆化したりすると，その秘密鍵を使ってなりすまされる危険性がある。こうした事態になると，秘密鍵に対応するディジタル証明書を失効させて，秘密鍵を無効にする必要がある。そのために利用されるものが CRL（Certificate Revocation List；ディジタル証明書の有効期間内に失効したディジタル証明書のリスト）である。この CRL では，有効期間内に失効したディジタル証明書のシリアル番号を掲載し，そのシリアル番号によってどのディジタル証明書が失効しているかを識別できるようにしている。したがって，（エ）が正しい。

問2　ウ

OCSP を利用する目的（H31 春-SC 午前Ⅱ問 2）

OCSP（Online Certificate Status Protocol）は，PKI（Public Key Infrastructure；公開鍵基盤）において，ディジタル証明書の失効情報をオンラインで問い合わせるためのプロトコルである。したがって，（ウ）が正しい。ブラウザやメールソフトなどの OCSP クライアントは，検証したいディジタル証明書のシリアル番号や発行者，公開鍵のハッシュ値などを OCSP リクエストとして OCSP サーバ（OCSP レスポンダ）に送信する。レスポンダでは，ディジタル証明書の状態を確認し，“有効”，“失効”あるいは“不明”のいずれかを回答する。なお，ディジタル証明書の失効情報を確認するためには，CRL（Certificate Revocation List；証明書失効リスト）をダウンロードする方法もあるが，OCSP を利用すると，CRL 利用と比較して，迅速かつリアルタイムに失効情報を確認できるというメリットがある。また，レスポンダは，一般に VA（Validation Authority；検証局）がその役割を担う。

その他の記述には，次のような誤りがある。

ア：OCSP には，秘密鍵の再発行処理の進捗状況を問い合わせる機能はない。

イ：OCSP には，認証状態を確認する機能はない。

エ：OCSP には，ディジタル証明書の更新処理の進捗状況を確認する機能はない。

●平成 31 年度春期

午後Ⅰ問題 解答・解説

問1　Web サイトのセキュリティ

(H31 春-SC 午後Ⅰ問 1)

【解答例】

［設問 1］　(1) a：Same-Origin
　　(2) b：イ　　c：キ　　d：ク（順不同）
　　(3) Web サイト B へのログイン

［設問 2］　e：(v)

［設問 3］　(1) f：https://site-a.m-sha.co.jp
　　(2) g：売れ筋商品情報配信の申込ページのオリジン
　　(3) h：Origin ヘッダフィールドの値
　　i：許可するオリジンのリスト
　　j：一致

【解説】

本問は，Web サイト間の情報連携機能の実装におけるセキュリティ対策を題材として，Web サイトのリソースへのアクセス制限の仕様，不正なクロスオリジンへのアクセスの手口，CORS（Cross-Origin Resource Sharing）の仕組みや動作，複数のオリジンからの情報連携の実現方法などについて出題されている。Web セキュリティ分野として頻出テーマといえる“オリジン”の考え方の基礎知識を有していれば，かなりの設問には本文の説明を基に解答することができるだろう。

［設問 1］

(1) 空欄 a は，「スクリプト Z は，［ a ］ポリシによって，［ b ］，［ c ］，［ d ］のいずれかが異なるリソースへのアクセスが制限される」という記述の中にある。スクリプト Z は，図 1（Web サイト B から Web サイト A への情報連携機能）から分かるように，情報連携機能のうち，API-Y を利用する会員情報の取得のために用いられる。図 1 のうち，(X-1) と (X-2) の売れ筋商品情報の取得を除いた，(Y-1) ～ (Y-7) の会員情報の取得におけるメッセージングを抜粋した情報連携を，図 A に示す。なお，注記については(3)の解説のために，注 2) だけを抜粋している。

●平成 31 年度春期
午後Ⅱ問題 解答・解説

問1　マルウェア感染と対策

(H31 春-SC 午後Ⅱ問 1)

【解答例】

［設問1］　a：FW1　　b：プロキシサーバ

［設問2］　内容：削除されたファイルの内容
手段：空きセクタの情報からファイルを復元する。

［設問3］　(1) MAC アドレスが平文の状態で送信されるから。
(2) 端末の無線 LAN ポートの MAC アドレスを，総務部の W-AP に登録済みの MAC アドレスに変更する。

［設問4］　(1) IP ヘッダ部及び TCP ヘッダ部は，同一のバイト列であることが多いこと
(2) c：同一の暗号ブロック　　d：平文ブロック　　e：カウンタ値を暗号化した値

［設問5］　(1) f：読み取る
(2) g：カ　　h：オ
(3) ① 攻撃者が用意した W-AP に接続し，情報を送信する。
② 内部メールサーバを利用して攻撃者にメールを送信する。

［設問6］　(1) i：信頼する CA のディジタル証明書
(2) j：クライアント証明書の提示が必要な外部 Web サーバにアクセスする。
(3) k：FW1 の製造元によって安全性が確認されていない CA が発行したサーバ証明書を使用した外部 Web サーバにアクセスする。

【解説】

本問は，マルウェア感染と対策をテーマとしたものであるが，出題内容としては，設問 1 でマルウェア感染を特定するために必要なログをもつ機器名，設問 2 でファイル単位ではなくセクタ単位でコピーする理由，設問 3 で無線 LAN 通信の特徴，設問 4 で ECB モードと CTR モードによる暗号化処理の問題，設問 5 で HTTP 通信と HTTPS 通信で取得できるログの内容及びマルウェアが窃取した情報を社内 PC から社外へ送信する経路，設問 6 でプロキシサーバにおいて HTTPS 通信を復号する機能をもたせた場合に発生する制約などを答えるものが出題されている。設問 1 から設問 5 は比較的技術要素の強い問題であり，設問 6 はディジタル証明書の検証に関する条件を答えることが必要となる。

情報処理安全確保支援士試験

平成 30 年度春期，平成 30 年度秋期，平成 31 年度春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
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

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

・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 年度春期，平成 30 年度秋期，平成 31 年度春期）

（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 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	3	2	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