目　　次

平成 23 年度秋期　問題と解答･解説編

＜出題分析＞

3．出題範囲と試験の概要

3-1　情報セキュリティスペシャリストの対象者像

情報セキュリティスペシャリストの対象者像は,次のように規定されています。業務と役割，期待する技術水準，レベル対応も示されています。

対象者像	高度 IT 人材として確立した専門分野をもち，情報システムの企画・要件定義・開発・運用・保守において，情報セキュリティポリシに準拠してセキュリティ機能の実現を支援し，又は情報システム基盤を整備し，情報セキュリティ技術の専門家として情報セキュリティ管理を支援する者
業務と役割	セキュリティ機能の企画・要件定義・開発・運用・保守を推進又は支援する業務，若しくはセキュアな情報システム基盤を整備する業務に従事し，次の役割を主導的に果たすとともに，下位者を指導する。 ① 情報システムの脅威・脆弱性を分析，評価し，これらを適切に回避，防止するセキュリティ機能の企画・要件定義・開発を推進又は支援する。 ② 情報システム又はセキュリティ機能の開発プロジェクトにおいて，情報システムへの脅威を分析し，プロジェクト管理を適切に支援する。 ③ セキュリティ侵犯への対処やセキュリティパッチの適用作業など情報システム運用プロセスにおけるセキュリティ管理作業を技術的な側面から支援する。 ④ 情報セキュリティポリシの作成，利用者教育などに関して，情報セキュリティ管理部門を支援する。
期待する技術水準	情報セキュリティ技術の専門家として，他の専門家と協力しながら情報セキュリティ技術を適用して，セキュアな情報システムを企画・要件定義・開発・運用・保守するため，次の知識・実践能力が要求される。 ① 情報システム又は情報システム基盤のリスク分析を行い，情報セキュリティポリシに準拠して具体的な情報セキュリティ要件を抽出できる。 ② 情報セキュリティ対策のうち，技術的な対策について基本的な技術と複数の特定の領域における応用技術をもち，これらの技術を対象システムに適用するとともに，その効果を評価できる。 ③ 情報セキュリティ対策のうち，物理的・管理的な対策について基本的な知識と適用場面に関する技術をもつとともに，情報セキュリティマネジメントの基本的な考え方を理解し，これを適用するケースについて具体的な知識をもち，評価できる。 ④ 情報技術のうち，ネットワーク，データベース，システム開発環境について基本的な知識をもち，情報システムの機密性，責任追跡性などを確保するために必要な暗号，認証，フィルタリング，ロギングなどの要素技術を選択できる。 ⑤ 情報システム開発における工程管理，品質管理について基本的な知識と具体的な適用事例の知識，経験をもつ。 ⑥ 情報セキュリティポリシに関する基本的な知識をもち，ポリシ策定，

	利用者教育などに関して，情報セキュリティ管理部門を支援できる。 ⑦　情報セキュリティ関連の法的要求事項などに関する基本的な知識をもち，これらを適用できる。
レベル対応	共通キャリア・スキルフレームワークの 人材像：テクニカルスペシャリストのレベル 4 の前提要件

図表 10　情報セキュリティスペシャリストの対象者像

3-2　試験時間と出題形式

情報セキュリティスペシャリスト試験の試験時間と出題形式は次のとおりです。

	午前 I	午前 II	午後 I	午後 II
試験時間	9:30～10:20 (50 分)	10:50～11:30 (40 分)	12:30～14:00 (90 分)	14:30～16:30 (120 分)
出題形式	多肢選択式 (四肢択一)	多肢選択式 (四肢択一)	記述式	記述式
出題数と解答数	30 問出題 30 問解答	25 問出題 25 問解答	4 問出題 2 問解答	2 問出題 1 問解答

図表 11　情報セキュリティスペシャリスト試験

3-3　出題範囲

(1)　午前の試験

図表 4「試験区分別出題分野一覧表」で示されているように，情報セキュリティスペシャリストの午前の試験では，大分類の「3 技術要素」,「4 開発技術」,「6 サービスマネジメント」の出題分野から，主に出題されることになっています。しかし，午前 I 試験の出題分野は「1 基礎理論」～「9 企業と法務」であるため，まんべんなく学習する必要があります。

午前 I 試験が合格点に達しない場合は，専門知識が問われる午前 II 試験以降は採点されないので，特に注意が必要です。平成 23 年度秋期試験における午前 I 試験の合格率は 69.1%と，これまでの試験に比べると向上したものの，平成 23 年度春期試験では 50.4%，平成 22 年度秋期では 37.1%というように，かなり低い合格率でした。このため，初めて情報セキュリティスペシャリスト試験にチャレンジされる受験者の方は，午前 I 試験の対策を含め，十分な準備を行っておくことが必要です。

4．平成 24 年度春期の試験に向けて

4-1　情報セキュリティスペシャリスト試験について

インターネットの利用が，日常生活に利便をもたらした半面，ウイルス感染をはじめとし，数多くのセキュリティ問題が指摘されています。例えば，アプリケーションの多くが Web ベースのソフトウェアに移行しており，Web サーバなどの脆弱性をねらった攻撃が大きな問題になっています。こうしたセキュリティ問題に対し，適切に対応していくには，セキュリティ全般に関する技術知識が広く求められ，情報セキュリティ技術者に対する社会の期待も大きくなっています。この情報セキュリティ技術者としての実力を証明する公的な資格が，情報セキュリティスペシャリスト試験です。この資格は，ぜひ取得しておきたいものです。

参考までに，平成 22 年度秋期から平成 23 年度秋期までの受験者数，合格者数などの推移を図表 13 に示します。なお，合格率については，平成 21 年度秋期の合格率（18.5%）をピークに，その後，徐々に低下してきています。このため，情報セキュリティスペシャリスト試験を受験するに当たっては，受験対策を十分に行って試験に臨む必要があると考えられます。

年　度	応募者数	受験者数	合格者数
平成 22 年度秋期	28,989　(-4.3%)	19,391（66.9%）	2,759（14.2%）
平成 23 年度春期	30,704　(5.9%)	19,445（63.3%）	2,712（13.9%）
平成 23 年度秋期	26,539（−13.6%）	17,753（66.9%）	2,398（13.5%）

（　）内は，それぞれ対前期比増減率，受験率，合格率を示す。

図表 13　応募者数・受験者数・合格者数の推移

4-2　出題予想

(1)　午前Ⅰ試験，午前Ⅱ試験

平成 22 年度秋期から平成 23 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，その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試験の合格率を比較すると，図表 14 のようになります。なお，午前Ⅰ試験の合格率が，午前Ⅱ試験の合格率を上回ったのは，平成 23 年度秋期が初めてです。

年　度	午前Ⅰ試験	午前Ⅱ試験
平成 22 年度秋期	37.1%	72.5%
平成 23 年度春期	50.4%	74.9%
平成 23 年度秋期	69.1%	67.1%

図表 14　午前Ⅰ試験と午前Ⅱ試験の合格率の比較

平成 23 年度秋期の午前Ⅰ試験の合格率は，前回（平成 23 年度春期），前々回（平成 22 年度秋期）と比較すると大きく向上しています。特に，1 年前の試験に比べると，32 ポイントも向上し，約 2 倍弱の合格率となっています。これに対し，午前Ⅱ試験の合格率は，ここ 3 期の試験の合格率は，おおむね 70%前後で推移しています。このため，平成 23 年度秋期試験で，初めて午前Ⅰ試験の合格率が，午前Ⅱ試験の合格率を上回るという結果になりました。これは，午前Ⅰ試験から受験する必要のある受験者が，少なくとも午前Ⅰ試験に合格し，次回の試験からは，専門分野の情報セキュリティ分野に絞った学習に専念して，次回の試験以降で合格をかち取りたいという意識などが強く働いたものと思われます。なお，午前Ⅰ試験の免除制度を利用できない受験者にとっては，午前Ⅰ試験の出題範囲が極めて広範囲にわたることから，十分に準備して受験することが必要です。そこで，前述したように，初回の試験では手堅く午前Ⅰ試験だけに合格し，2 回目以降の試験で午前Ⅱ試験以降をすべて合格するという方法もよいでしょう。あるいは，午前Ⅰ試験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よいでしょう。

次に，午前Ⅰ試験の出題分野についてです。出題分野は，テクノロジ系（基礎理論，コンピュータシステム，技術要素，開発技術），マネジメント系（プロジェクトマネジメント，サービスマネジメント），ストラテジ系（システム戦略，経営戦略，企業と法務）の全分野にわたりますので，幅広い分野に関する知識が要求されます。平成 22 年度秋期から平成 23 年度秋期試験までの分野別の出題数は，図表 15 に示すとおりです。なお，午前Ⅰで出題される 30 問は，応用情報技術者

●平成 23 年度秋期
午前Ⅰ問題 解答・解説

問1 ウ

逆ポーランド表記法による表現（H23 秋-高度 午前Ⅰ問 1）

数式を表現する方法には，次の三つがある。

・前置記法（ポーランド表記法）：演算子を演算数の前に置く表記法である。
（例：×ab）

・中置記法（一般的な表記法）：演算子を演算数の中央に置く表記法である。
（例：a×b）

・後置記法（逆ポーランド表記法）：演算子を演算数の後に置く表記法である。
（例：ab×）

逆ポーランド表記法で表現された数式は，数式を左から順に参照し，演算数ならスタックにプッシュする。また，演算子ならスタックのトップにある二つの演算数をポップして演算し，結果をスタックにプッシュするという簡単な方法で処理できる。

問題で問われているのは，式 A＋B×C を逆ポーランド表記法で表現した内容である。A＋B×C の計算では，B×C の部分を最初に行い，その結果を A に加えるが，逆ポーランド表記法に書き変えるときもこれと同じ順序で行う。まず，最初に計算する B×C の部分を BC×と書き換えると，式は A＋(BC×)となる。そして，(BC×)の部分を一つのまとまり（オペランド）と見れば，これは A(BC×)＋と書き換えることができる。そして，“( )”を取った ABC××＋が逆ポーランド表記法による表現となるので，（ウ）が正解である。

ア：C×B＋A のポーランド表記法による表現である。

イ：(A＋B)×C のポーランド表記法による表現である。

エ：C×(B＋A)の逆ポーランド表記法による表現である。

問2 エ

ハミング符号による誤り訂正（H23 秋-高度 午前Ⅰ問 2）

受信した符号語が“1000101”なので，x_1＝1，x_2＝0，x_3＝0，x_4＝0，x_5＝1，x_6＝0，x_7＝1 となる。まず，c_0，c_1，c_2 を mod 2 で計算すると，それぞれ次のようになる。

$c_0 = x_1 + x_3 + x_5 + x_7 = 1 + 0 + 1 + 1 = 1$

$c_1 = x_2 + x_3 + x_6 + x_7 = 0 + 0 + 0 + 1 = 1$

$c_2 = x_4 + x_5 + x_6 + x_7 = 0 + 1 + 0 + 1 = 0$

更に，i は次式によって計算するので，

●平成 23 年度秋期
午前Ⅱ問題 解答・解説

問1 イ

DNSSEC の機能（H23 秋-SC 午前Ⅱ問 1）

DNSSEC（DNS Security Extensions）は，DNS キャッシュポイズニング攻撃などの対策として，権威 DNS サーバ（コンテンツサーバともいう）に登録するリソースレコードにディジタル署名を付与し，リソースレコードの送信者の真正性と，その内容の完全性を保証しようとするための規格である。このため，キャッシュサーバが DNS 問合せパケットをコンテンツサーバに送信した後，その回答パケットを受け取ると，リソースレコードに付加されているディジタル署名を用いて，リソースレコードの送信者の正当性とデータの完全性を検証することができる。したがって，（イ）が正しい。

なお，DNSSEC に関する RFC には，RFC 4033（DNS Security Introduction and Requirements），RFC 4034（Resource Records for the DNS Security Extensions）などがある。

問2 ウ

SHA-256（H23 秋-SC 午前Ⅱ問 2）

セキュアハッシュ関数（単にハッシュ関数ともいう）は，可変長の入力データから固定長のビット列を出力する関数である。SHA-256 は，256 ビットのハッシュ値（ダイジェストなどともいう）を出力するので，入力メッセージが 32 ビット，256 ビット，2,048 ビットのいずれの場合でも，そのハッシュ値は 256 ビットとなる。したがって，（ウ）が正しい。

以上のほか，ハッシュ関数は，次のような特徴をもつ。

① 入力メッセージが少しでも異なれば，出力されるダイジェストは大きく異なる。

② ダイジェストから元のメッセージを算出することは困難である（一方向性）。

③ 同じダイジェストを出力する二つの入力メッセージを見つけることは困難である。

なお，SHA-256 は，SHA-2（Secure Hash Algorithm 2）の一つである。SHA-1（160 ビットのハッシュ値を出力する）については，衝突を見つける理論的な攻撃手法が発表されたことを受け，米国国立標準技術研究所（NIST）では，2010 年末までに SHA-2 に移行することが望ましいとしている。

●平成 23 年度秋期
午後Ⅰ問題 解答・解説

問1　セキュアプログラミング

(H23 秋-SC 午後Ⅰ問 1)

【解答例】

［設問 1］　(1) user，day
(2) a：プレースホルダ
(3) b：prepareStatement
(4) ア
(5) c：HTML における特別な記号　　d：エスケープ
(6) user，day，rep

［設問 2］　e：ポインタ　　f：バッファオーバフロー　　g：ガーベジコレクション

［設問 3］　アドレスを計算対象にできないから。

【解説】

本問では C++と Java の二つのプログラミング言語が取り上げられているが，SQL インジェクションやクロスサイトスクリプティング，バッファオーバフローなどの定番テーマが中心であることから，比較的取り組みやすいといえる。一方，変数名を選ぶ設問やメソッド名を答える設問などについては，正確な解答が要求されるためにやや難しい。しかし，この問題の選択者は，C++や Java を理解している受験者が多いと考えられるので，難易度を総合的に評価すると，標準レベルといえる。

なお，情報セキュリティスペシャリスト試験で出題されるプログラミング言語は，これまでは Perl，C++，Java の 3 種類であったが，平成 24 年度春期試験からは C++，Java，ECMAScript の三つになるので，気を付けるようにしたい。

［設問 1］

(1) 図 2（SQL インジェクション対策前の C++コード）のコードの中で，SQL インジェクションの原因となる変数名を選ぶ問題である。

コードの 2 行目で `SELECT` 文を組み立てて，`string` 型（文字列型）の変数 `query` に代入している。図 1（getReport の仕様（抜粋））に書かれているように，変数 `user` には利用者画面からの入力を基にした値がセットされる。図 2 の 3 行目では `SELECT` 文に `" AND day "` を連結しているが，この変数 `day` も利用者画面からの入力を基にした値である。そして，組み立てられた SQL 文は，9 行目の `executeQuery` 関数で実行される。利用者画面からの入力値である変数 `user` や `day` に不正な文字列があると，9 行目でそのまま実行され，SQL インジェクションが成立するリスクがあ

●平成２３年度秋期
午後Ⅱ問題 解答・解説

問１　医療情報システムの要件定義と設計　(H23 秋-SC 午後Ⅱ問 1)

【解答例】

［設問１］ (1) 作成責任者以外の者による電子カルテへの署名
(2) 耐タンパ性

［設問２］ (1) 医療行為に必要な範囲を超えて患者の医療情報にアクセスすることを抑止する効果
(2) a：A，R，U，D，P
(3) 個別の利用者ごとに，電子カルテのデータ項目ごとに行うアクセス制御

［設問３］ (1) ① (J)　② (K)
(2) 電子カルテのディジタル署名の有効期限が切れる前に，署名検証に必要な情報を含むアーカイブタイムスタンプを付与する。
(3) b：ディジタル署名
(4) バックアップから改ざん前の電子カルテを復旧する機能

［設問４］ (1) 日々行うべき業務：患者ごとに，見読可能な画像データを電子カルテから生成し，USB ディスクに書き出しておく。
災害時に行うべき業務：電子カルテの画像データを保管した USB ディスクを端末に接続して，患者の電子カルテの画像データを医師に配布する。
(2) ① 本人確認の方法と，認証に用いる IC カードの貸与及び利用者 ID の付与の方法
② 応援者の資格の確認方法と，応援者に付与するアクセス権限の内容と付与方法

【解説】

本問では，IC カードに格納する秘密鍵の保護やディジタル署名，タイムスタンプなどの技術的な内容のほかに，アクセス制御の検討，医療情報の機密性・真正性・可用性保護の考え方，非常時の業務継続や BCP に盛り込む内容の検討などが取り上げられている。ディジタル署名に関する一部の設問（タイムスタンプのアーカイブなどの設問）を除いて高度な知識は要求されていない。このため，合格基準点をクリアするには，情報セキュリティの基本的な考え方を踏まえた上で，問題文の記述に沿って，一つ一つ丹念に解答を作成していくことができるかどうかがポイントになると思われ

（1）午前問題出題分析

・問題番号順

平成 22 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	後置表記法（逆ポーランド表記法）	イ	T	1	1	3	3
2	符号化に要するビット列の長さ	ウ	T	1	1	3	4
3	表の構成法と探索手法の組合せ	ア	T	1	2	2	3
4	平均アクセス時間を表す式	イ	T	2	3	2	2
5	システムの信頼性向上技術	エ	T	2	4	2	3
6	ページサイズを半分にしたときに予想される事象	ウ	T	2	5	1	3
7	デュアルライセンスのソフトウェア利用条件	イ	T	2	5	5	3
8	論理回路と等価な回路	ウ	T	2	6	1	2
9	システム状態の視認性	イ	T	3	7	1	3
10	コンピュータグラフィックス	ウ	T	3	8	2	3
11	データベースの参照制約	ウ	T	3	9	2	3
12	パケット送信におけるあて先	ウ	T	3	10	3	2
13	データやサービスを呼び出すためのプロトコル	エ	T	3	10	3	3
14	公開鍵暗号方式の鍵の総数	イ	T	3	11	1	2
15	プログラムの正当性検証手法	ア	T	4	12	5	3
16	マッシュアップ	エ	T	4	13	1	3
17	特許権	ア	T	4	13	2	2
18	WBS の構成要素であるワークパッケージ	ウ	M	5	14	2	3
19	アローダイアグラムの所要日数の短縮	ウ	M	5	14	3	2
20	パックアップに必要な磁気テープの本数	ウ	M	6	15	4	3
21	可用性の計算	エ	M	6	15	4	2
22	システム管理基準の説明	ウ	M	6	16	1	3
23	エンタープライズアーキテクチャの説明	ウ	S	7	17	1	3
24	SOA の説明	エ	S	7	17	3	3
25	サプライチェーンマネジメントの改善指標	ウ	S	7	18	3	3
26	類似性で分類し分析する手法	ア	S	8	19	2	3
27	フラッシュメモリを採用する理由	イ	S	8	20	1	3
28	EDI の情報表現規約での規定	エ	S	8	21	3	3
29	売上高増加額の計算	ウ	S	9	22	3	2
30	プログラム著作権の原始的帰属	エ	S	9	23	1	2

■平成 23 年度秋期 情報セキュリティスペシャリスト試験
午後Ⅰの問題（問 1～問 4 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)	1	4	4	50
		(2) a	1	4	4	
		(3) b	1	4	4	
		(4)	1	4	4	
		(5) c	1	6	6	
		(5) d	1	4	4	
		(6)	1	4	4	
	2	e，f，g	3	4	12	
	3		1	8	8	
問 2	1	a	1	2	2	50
	2	b，c，d，e	4	4	16	
	3	(1)	1	8	8	
		(2)	1	8	8	
	4		1	8	8	
	5		1	8	8	
問 3	1	(1)	1	6	6	50
		(2)	1	6	6	
		(3)	1	3	3	
	2	(1) a	1	3	3	
		(2) ①，②	2	6	12	
	3	(1) b	1	8	8	
		(2)	1	6	6	
		(3)	1	6	6	
問 4	1	a	1	4	4	50
	2	b，c	2	3	6	
		d，e	2	5	10	
	3	(1)	1	3	3	
		(2)	1	8	8	
		(3)	1	8	8	
	4	(1) f	1	3	3	
		(2)	1	8	8	
					合計	100