4．平成 21 年度春期の試験に向けて

4-1　新試験について

インターネットの利用が日常生活に利便をもたらす一方で，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開発に移行しており，Web サーバなどの脆弱性を狙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。

これまでのテクニカルエンジニア（情報セキュリティ）試験と，情報セキュリティアドミニストレータ試験の内容を内包したものになる，と発表され，1 年に 2 回実施されます。セキュリティの重要性が高まる今，取得しておきたい資格です。

4-2　出題予想

(1)　午前Ⅰ試験，午前Ⅱ試験

新試験制度でも，出題内容に関しては平成 20 年度までの午前試験と，大きな変化はないと予想されますが，高度試験に共通の午前Ⅰ試験（出題数 30 問，試験時間 50 分），専門の午前Ⅱ試験（出題数 25 問，試験時間 40 分）というように出題形式が変わっています。これによって，共通問題の午前Ⅰ試験で基準点に達しないと，専門の午前Ⅱ試験の採点も行われずに不合格になってしまいます。このことをしっかりと頭に入れておきましょう。

午前Ⅰ試験では，出題分野もテクノロジ系（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）の全分野に渡ります。技術レベルは 4 段階の中のレベル 3 であるため，幅広い分野に関する知識が要求されます。しかも，基準点は 60%（18 問の正解）であり，日頃から情報処理技術全般に関する知識を修得するとともに，過去に出題された問題を確実に解いておくことが要求されます。基礎理論，システム戦略，経営戦略，企業

と法務など，新たに追加された分野も学習しておく必要があります。

午前Ⅱ試験の基準点も 60%（15 問の正解）です。出題の重点分野は，ネットワークとセキュリティです。このほかには，データベース，システム開発技術，ソフトウェア開発管理技術，サービスマネジメント，システム監査の 7 分野です。

ネットワークとセキュリティは重点分野であり，最も高いレベル 4 からも出題されます。出題の中心になるはずです。しかも，これらの技術知識は，午後試験においても必要とされるものです。基礎知識からしっかり固め，午後試験の技術に対応できるレベルまで発展させていくとよいでしょう。

(2) 午後Ⅰ試験，午後Ⅱ試験

午後Ⅰ試験の試験時間は 90 分，4 問の中から 2 問を選択して解答します。テクニカルエンジニア（情報セキュリティ）試験，情報セキュリティアドミニストレータ試験では 4 問中 3 問を解答していたため，1 問少なくなります。この影響はどのようなものになるかわかりません。しかし，午後Ⅰ試験の出題内容は，穴埋め問題が一部ありますが，記述式で解答する問題が多いと考えられます。

午後Ⅱ試験の試験時間は 120 分，2 問の中から 1 問選択して解答します。100 点満点で基準点は 60%です。午後Ⅱ試験は，平成 20 年春の試験とほぼ同様と考えてよいでしょう。

4-3 学習方法

学習方法について説明しておきましょう。

情報セキュリティスペシャリスト試験では，セキュリティとネットワークを中心とし，データベースやセキュリティマネジメントの知識が最も重要になると思います。

セキュリティの基本技術については，十分に修得しておくことが必要です。例えば，セキュリティの問題としては，暗号化方式，認証技術，ディジタル署名，電子証明書の検証方法のほか，SQL インジェクション，クロスサイトスクリプティング，ブルートフォース攻撃などのさまざまな攻撃手法，ファイアウォールの設定，IDS や IPS，セキュリティプロトコルなどの問題が重要です。さらに，情報セキュリティポリシやリスク分析などのマネジメント系の問題に加えて，フィッシングやフォレンジックなど最新のトピックも含めて出題されるので，幅広く知識を吸収していくことが必要です。また，JIS Q 27001 や JIS X 5070 などの

標準化動向の把握も忘れないようにしましょう。

午後Ⅰ試験，午後Ⅱ試験に関しては，セキュリティでは，Web アプリケーションなどに対するセキュアプログラミングをはじめ，メッセージ認証，本人認証，暗号化技術，ネットワークやデータベースに対するさまざまな攻撃とその対策，セキュリティプロトコル，VPN 技術，ファイアウォールの設定，IDS や IPS，迷惑メール対策など，多くの技術知識を吸収していくことが必要です。

ネットワークでは，TCP/IP（HTTP，HTTPS，IPsec，SSL など）やインターネット利用・接続技術，DNS の仕組み，電子メールの配送の仕組みなど，データベースでは，SQL 文，RDB，データベースに対するアクセス制御方式，データベースの排他制御やリカバリなど，リスク分析など，幅広い技術を修得していく必要があります。

セキュアプログラミングに関する問題は，Perl 言語，C++言語，Perl 言語と続いており，C++言語や Java が出題される可能性もあります。しかし，セキュアプログラミングについては，プログラムのコーディングが出題の対象外になっているので，データベースに対するアタックである SQL インジェクション，Web サーバで利用される CGI に対するコマンドインジェクションのほか，クロスサイトスクリプティング，ディレクトリトラバーサルなどの攻撃と，それらに対する対策との関係をよく理解しておくことが必要です。なお，セキュアプログラミングについては，IPA セキュリティセンターから，セキュアプログラミング講座や，安全な Web サイトの作り方などの資料が公開されているので，これらの資料を事前に学習しておくことも効果的です。

午後試験の特徴は，一つの技術に絞った問題よりも，複合的な観点から出題されることです。この傾向は，午後Ⅱ試験では特に顕著になります。そこで，セキュリティと，ネットワークあるいはデータベースの相互に関連した総合問題に対応できる技術力を養っていくことが必要になります。しかし，幅が広いこれらの技術を十分に修得するには，かなりの時間が必要です。試験の直前になってあせらないように，あらかじめ多くの学習時間を見込んでおき，計画的に学習することが必要です。また，一度，理解しても繰り返し技術知識をインプットしていかないと，すぐに忘れてしまいます。工夫をしながら継続的に学習していく姿勢を確立してください。試験問題では，単なる技術的な知識から解答する問題はそれほど多くありません。問題文に記述された内容に従って解答する問題のほうが多いので，記述内容を正しく理解し，その範囲内で考えていくようにしましょう。

このため，問題文の内容を理解できるだけの基本的な技術力をまず確保することが必要です。

また，午後Ⅰ試験，午後Ⅱ試験は数十字の記述式で解答するものが多く，記述内容については，考え方や根拠を明確に示すほか，キーワードをしっかりと押さえた解答を作成することがポイントです。

以上のように，情報セキュリティスペシャリストの資格を取得するためには，努力が必要です。したがって，この資格を保有することは，それだけ価値が高いということになります。学習計画をしっかり立てて，合格するように努力していきましょう。

4-4　平成 20 年春の試験のデータ

平成 20 年春のテクニカルエンジニア（情報セキュリティ）試験を分析します。平成 21 年春から実施される情報セキュリティスペシャリスト試験を受験する際の参考にしてください。

(1)　午前問題

午前問題 55 問の出題分野を見ていきましょう。

基本ソフトウェアが 2 問，システムの構成と方式が 3 問でした。初めて待ち行列の計算問題が出題されました。過去に出題された問題の類似問題では，稼働率の計算問題とフェールソフトの内容を問うもので，いずれも基本的な問題でした。

システムの開発と運用からは，ソフトウェア開発のリポジトリ，プロセス成熟度モデル，オブジェクト指向のインヘリタンスの問題が新しく出題されました。その反面，OSS（Open Source Software），ITIL（IT Infrastructure Library）に関する問題が，平成 19 年春に続いて出題されました。

ネットワーク技術の出題数は 15 問です。TCP/IP プロトコルやインターネット，LAN 関連技術などの出題が中心で，これらの問題は 12 問ありました。そのほかは，CRC，トラフィック計算，ウィンドウ制御の問題です。新規の問題としては H.323 の内容を問う問題が出題されました。これは技術の細部を問うものでしたから，15 問の中で最も難しいといえます。

データベース技術の 10 問の内訳は，データベースモデルが 2 問，言語が 1 問，データベースに関する制御が 7 問です。平成 19 年春に引続き，データベースに関する制御の問題が大半を占めています。

セキュリティから 16 問（技術系が 13 問，マネジメント系が 3 問），標準化から 4 問という割合でした。標準化の出題が多かったことのほか，マネジメント系が 3 問（平成 19 年春は 1 問）に増加したことが特徴です。セキュリティでは，過去問題からの流用は少なく，新しい問題が多く見られました。内容的には，基本的な技術を十分に理解しているかどうかを問うものが多く，出題傾向としては望ましいといえます。

平成 19 年春，平成 20 年春のテクニカルエンジニア（情報セキュリティ）試験の出題内容を，新しく発表された共通キャリア・スキルフレームワークに沿ってまとめると，次のようになります。

平成 20 年度までの出題分野	平成 19 年春	平成 20 年春	共通キャリア・スキルフレームワーク（中分類）
基本ソフトウェア	1 問	2 問	基本ソフトウェア
システムの構成と方式	4 問	3 問	システム構成要素
システムの開発と運用	5 問	5 問	ヒューマンインタフェースなど
ネットワーク技術	15 問	15 問	ネットワーク
データベース技術	10 問	10 問	データベース
セキュリティ	16 問	16 問	セキュリティ
標準化	4 問	4 問	法務

図表 14　分野別出題傾向

(2)　午後 I の問題

平成 20 年春の試験では，セキュアプログラミングが全く出題されなかったほか，認証技術がほとんど出題されませんでした。こうした背景から，ネットワーク系分野からの出題が大半を占めました。また，出題内容としては，技術中心の問題であったといえるので，出題傾向としては望ましいといえます。このような問題に対応していくためには，セキュリティ技術の本質を十分に理解している必要があり，技術知識を十分に把握して試験に臨むことが要求されます。

次に，各問の特徴を簡単に述べておきます。

問 1　ボット感染とその対策

迷惑メール対策とウイルス対策の問題です。メールヘッダの見方，ファイアウォールに適用するルール，ボット対策，rootkit の機能などを熟知している必要が

あります。問題文の内容を十分に確認していけば，設問 1，2 の多くは正解できます。しかし，設問 3 の記述式問題は，かなりの専門知識が要求されるので，難易度を全体的に評価すると，やや難といえます。

問２　ネットワークのセキュリティ

TCP の SYN Flood 攻撃に特化した問題です。SYN Flood 攻撃の基本的な仕組みを十分に把握していれば，容易であったといえます。

問３　通信データの保護

通信データの保護というテーマの問題です。通信データの盗聴対策，適用する暗号化方式の検討などが主な出題項目です。通信データの盗聴対策は，少し考えにくいところもありますが，光通信の特質を十分に理解していれば，解答を作成できると思います。適用する暗号化方式の検討は，問題の条件をよく確認することが必要です。問題自体の難易度は中レベルと思いますが，思ったように得点できないかもしれません。

問４　ISMS 構築時のリスクマネジメント

リスクマネジメントの基礎用語，ノート PC の紛失時などにおける情報漏えい対策，パスワードの安全な運用などに関する問題です。穴埋め問題は語句選択，記述式の問題は比較的基本的な内容を解答する問題であったため，全体的な難易度は標準的といえます。ただし，設問数が多いので，思うように得点できない可能性もあります。

(3)　午後Ⅱの問題

「Web アプリケーションシステムの脆弱性対策」,「認証システムの企画・設計」というテーマは，平成 19 年春の出題内容とは，基本的に異なる内容です。問 1 では，Perl 言語によるセキュアプログラミングが出題されました。この出題は，隔年現象があるといえます。また，午後Ⅰで認証技術がほとんど出題されなかったので，午後Ⅱで出題されたものと考えられます。

応用能力や実務能力に重点が置かれた問題が出題される傾向にあります。このため，問題文を把握しながら，問題に取り組むことが基本です。問題文の条件を十分に確認しながらそれぞれの設問を解いていけば,正解できるものがあります。

したがって，問題をよく読みながら設問で問われている内容に，的確に答えていくという姿勢で試験に臨んでください。

問１　Web アプリケーションシステムの脆弱性対策

脆弱性対策，SQL インジェクション対策，DB サーバに対する運用上の問題とインシデント対応策に関する設問が設定されています。設問 1，設問 2 については，IPA セキュリティセンターが公開しているセキュアプログラミング講座に記載されている内容から出題されています。この講座の内容を十分に学習していれば，難しくなかったでしょう。また，設問 3 は問題文に従って考えていけば，正解を導くことができます。なお，全体的な難易度を評価すれば，セキュアプログラミングについては必ずしも十分に準備できているとは限らないので，中レベルといえます。

問２　認証システムの企画・設計

Web サイトの認証手法，情報システムの認証方式，SSO（Single Sign-On）の実現方式，無線 LAN と利用者認証方式，共通認証システムの設計という設問が設定されていました。認証技術に関する専門知識が要求されますが，技術の本質さえ理解できていれば，かなりの設問に正解できると思われます。全体的な難易度を評価すると，やや易と思われます。なお，技術的には，IEEE 802.1X/EAP，SSO を構築したときの注意点などに関するものが出題されています。