ITコンサルタント：佐藤豊史（さとうとよし）のブログ

情報セキュリティマネジメント試験受験編

私が2020年2月から4月まで情報セキュリティマネジメント試験の受験勉強をしてきた過程についてブログをまとめました。

目次

情報セキュリティマネジメント試験受験編

IT入門お役立ち情報：情報セキュリティマネジメント試験受験編（その1）

情報セキュリティマネジメント試験を受験することにしました
昨今情報セキュリティに対する注目は増すばかりで、情報セキュリティのエキスパートを求める声が高まっています。特に組織などで情報システムを利用する立場でありながら、情報セキュリティの確保や改善を統率できる能力を持つ人材が必要とされています。

「情報処理技術者試験」については、私自身過去にいくつかの試験にチャレンジしてきましたし、情報セキュリティ関連の「情報セキュリティアドミニストレータ試験」もかなり昔に受験しました。しかし、その後各試験区分や資格名などは年を経るとともに変化していき、情報セキュリティに関する試験も近年大幅に変わってきました。

私自身は「情報セキュリティアドミニストレータ試験」に合格した後に、管理的な仕事が増えてきたことや、数年前にシステム部門からユーザ部門に異動になったこともあり、システム部門でのセキュリティの現場での実務的な業務から、ユーザ部門でのセキュリティを確保していく業務に移っていき、情報処理技術者試験はしばらく意識をしていませんでした。

ところが、最近自分の部署での仕事に役立てるために、同僚や後輩とIT関連の基礎知識を勉強する機会があったので、改めて情報処理技術者試験に関する参考書などに触れることになりました。すると、私が受験した頃とは技術も進歩・変化していますので、インターネットをベースにした内容に変わっていたり、セキュリティに関しても次々と新たな技術が出てきていました。

そこで、私自身のこれまでのシステム部門やユーザ部門での仕事で習得した情報セキュリティに関する知識や経験などを整理するのと同時に新しい技術も習得する目的で、ITの専門家ではなくITを利用する立場で、情報処理技術者試験の「情報セキュリティマネジメント試験」を受験することにしました。これから、試験勉強を始めて今年の春期の試験には受験したいと考えています。具体的には、「ニュースペックテキスト情報セキュリティマネジメント、TAC出版（著）」という参考書をもとに、次のとおり、各分野を順番に勉強していき試験を迎えたいと思います。

1. 情報セキュリティ技術（1）
2. 情報セキュリティ技術（2）
3. 情報セキュリティ管理
4. 関連法規
5. テクノロジー系
6. マネジメント系
7. ストラテジー系
8. 午後対策：事例
9. まとめ
10. 受験（2020年4月）

今後、自分の受験勉強についての進捗などを順次書いていきたいと思います。

情報セキュリティマネジメント試験受験編

IT入門お役立ち情報：情報セキュリティマネジメント試験受験編（その２）

情報セキュリティ技術について勉強しました（1）
情報セキュリティ技術の基礎知識として、次のような項目について学習しました。

- 情報セキュリティの基本概念

情報セキュリティのCIA＝C：機密性、I：完全性、A：可用性
脅威：情報資産に発生すると損害を与える事象
脆弱性：セキュリティ上の弱点、セキュリティホール
リスク：脅威が脆弱性を利用して情報資産に損害を生じる可能性

- サイバー攻撃と情報セキュリティ対策

マルウェア：悪意のあるソフトウェア、不正で有害な動作を行うプログラム
セキュリティパッチ：OSやアプリ上のセキュリティ上の問題を修正するためのプログラム
不正アクセス：アクセス権を持たないものがシステムに侵入する行為
ソーシャルエンジニアリング：IT技術を使わずに重要な情報（パスワードなど）を盗み出す手口
標的型攻撃：特定の企業や組織をターゲットにしたサイバー攻撃
WAF（ウェブアプリケーションファイアウォール）：ウェブアプリケーションへの不正なアクセスを遮断する装置
ランサムウェア：データを勝手に暗号化したりして、金銭を要求するマルウェア
ログ管理：発生したイベント（事象）やエラーを記録して、分析・レビューする
内部不正：「動機」「機会」「正当化」の3つの要素である不正のトライアングルが揃うと不正行為が行われる

学習をしての気づき
情報セキュリティの基本概念や具体的なサイバー攻撃の手口およびそれらに対する対策などを一通り学習できました。サイバー攻撃の手口および対策についてはかなりの種類が紹介されていますので、それらをひとつひとつ丁寧に理解していくことが必要ですが、しっかりと違いを学習しておけば、試験では慌てることはないかと思います。
また、問題を解くときは、問題文をよく読む必要があります。実際私もある問題で文意を取り違えてしまうことがあり、しっかりと文意を理解していれば解けた問題を間違ってしまったこともありました。ただし、そのような点を注意していれば、関連用語とその内容を十分に理解していれば問題ないと思います。もし万一、知らない用語が出てきてもある程度消去法で推測できることがありますので、回答できる場合もあるかと思います。しかしながら、やはり一通り学習して理解しておいたほうが安心ですね。

情報セキュリティマネジメント試験受験編

IT入門お役立ち情報：情報セキュリティマネジメント試験受験編（その３）

情報セキュリティ技術について勉強しました（2）
情報セキュリティ技術の基礎知識として、次のような項目について学習しました。

- 情報セキュリティを確保する技術

暗号化：誰にでも内容を判読できるデータである平文を、鍵を持っている人だけが内容を判読できるデータである暗号文に変換すること
共通鍵暗号方式：暗号化と復号に同一の鍵（共通鍵）を用いる
公開鍵暗号方式：暗号化と復号に2個1組の異なる鍵（公開鍵と秘密鍵）を用いる
ディジタル署名：メッセージを作成した本人と内容が改ざんされていないことを保証する仕組み
認証局：公開鍵証明書を発行する機関
パスワード認証：ユーザIDとパスワードの組み合わせで本人であることを確認
バイオメトリクス認証：生体情報（身体的特徴、行動的特徴）を利用した認証方式
ファイアウォール（防火壁）：パケットフィルタリングなどで通信の遮断と許可を制御する仕組み
DMZ（非武装セグメント）：外部へ公開するサーバを設置するネットワークセグメント
IDS（侵入検知システム）：アクセス状況を監視して不正侵入を検知する仕組み
SSL：Webサーバとのやり取りを安全に行うために利用される（HTTPS通信）
VPN：インターネットなどに仮想的な専用網を構築する仕組み
WPA/WPA2：無線LANにおける暗号通信の仕組み
デジタルフォレンジックス：不正アクセスの追跡や証拠データ保全などの捜査活動
UPS（無停電電源装置）：停電時などにバッテリーにより電力を供給する装置

- 情報セキュリティ教育、普及啓発活動

サイバーセキュリティ基本法：サイバーセキュリティに関する教育、学習の振興などを定めた法律

学習をしての気づき
暗号化に関する技術問題が多かったです。その中でも特に公開鍵暗号方式はしっかりと学習する必要があると思います。具体的な過去問題としては、ディジタル署名に関してよく出題されているようです。私自身もそうですが、普段実務をしていても暗号化についてはあまり意識せずに利用していたので、今回の学習を通して改めて勉強になりました。
また、認証方式の問題とネットワークに関するセキュリティについても重要であると思います。これらに関しては、どのような認証方式を採用するかとか、どのようなネットワーク構成にするかについて、私自身これまで実務でよく経験していたので、ある程度容易に学習を進めることができました。しかしながら、試験ではおそらくより技術的に詳しい理解が求められると思うので、しっかりと学習する必要あるかと思います。

情報セキュリティマネジメント試験受験編

IT入門お役立ち情報：情報セキュリティマネジメント試験受験編（その４）

情報セキュリティ管理について勉強しました
情報セキュリティ管理の基礎知識として、次のような項目について学習しました。

- 情報セキュリティ管理とISMS

ISMS（情報セキュリティマネジメントシステム）：情報セキュリティに対して組織的な取り組みを行うための体系
PDCAサイクル：計画（Plan）→実行（Do）→点検（Check）→改善（Act）を繰り返す基本的な管理サイクル
ISO/JISQ 27001：ISMSが満たすべき事項（要求事項）を定めた規格、ISMSを構築する際のチェックリストとして用いられる
リスクアセスメント：リスクを洗い出して特定し、分析・評価する一連の活動
情報セキュリティポリシー：情報セキュリティに対する方針を定めたもの
リスク対応（リスクコントロール）：次のような選択肢がある

- リスク低減：リスクを小さくする、損失予防（発生確率を下げる）と損失軽減（被害を少なくする）がある
- リスク保有：リスクをあえて受け入れる
- リスク回避：リスクそのものの存在をなくす
- リスク共有・移転：リスクを他社と分担する

- セキュリティインシデントの管理

セキュリティインシデント対応手順：対応の手順を確立、文書化して定期的に見直しする
CSIRT：セキュリティに関する問題に対応するための組織
サイバーレスキュー隊：標的型サイバー攻撃の被害低減と攻撃を拡大させないための支援をする

学習をしての気づき
とにかくISMSが基本です。ISMSではPDCAのプロセスがしっかりと繰り返されていることが重要ですので、それぞれのプロセスでするべきことを理解する必要があります。
特に、リスクアセスメントからリスク対応までの詳細を学習する必要があります。私自身はリスクアセスメントの経験があり、その結果に基づいてのリスク対応も結構悩みながら検討および実施したこともありますので、これらのプロセスを学習することは改めてこれまでの理解の整理になりました。
また、セキュリティインシデント管理も重要です。事前の準備から実際に発生してからの対応などについて理解しておく必要があります。私自身セキュリティインシデントも実際に経験したことがあり、その際の経験から対応手順や対応チームの重要性も身にしみて感じていましたので、こちらの学習も知識の整理に役に立ちました。

情報セキュリティマネジメント試験受験編

IT入門お役立ち情報：情報セキュリティマネジメント試験受験編（その５）

関連法規について勉強しました
関連法規の基礎知識として、次のような項目について学習しました。

- セキュリティ関連法規

サイバーセキュリティ基本法：サイバーセキュリティ（情報の漏洩や改ざんなどから情報システムやネットワークを守ること）の基本理念を定め、国や地方公共団体の責務を明らかにしている。サイバーセキュリティ戦略本部が設置され施策を推進する。
不正アクセス禁止法：アクセス制御機能をもつコンピュータに、ネットワーク経由での不正アクセス行為（他人の権限で不正にシステムを利用すること）や、それを助長する行為（他人のID・パスワードを無断で提供すること）を禁止する。
個人情報保護法：個人情報（生存する個人に関する情報で、特定の個人を識別できるもの）の取扱事業者（個人情報データベースなどの運用者）に対して遵守すべき義務を定めている。
特定電子メール法：オプトイン（事前に同意）を得ていない受信者への電子メール送信を禁止する。

- 知的財産権関連法規

知的財産権：著作権または営業秘密や特許権、実用新案権、意匠権、商標権などを指す。
著作権法：プログラムなどのソフトウェアは著作物として保護される。ソフトウェアの開発を委託した場合は、委託先に著作権がある。また、海賊版と知りながら入手した場合は、著作権の侵害になる。
不正競争防止法：営業秘密（秘密として管理された有用な情報、トレードシークレット）やドメイン名を保護する。

- 労働関連・取引関連法規

労働者派遣：労働者が他社のもとで労務を提供する。労働者と派遣先には指揮命令関係がある。
請負：請負業者が他社作業の完成を請け負う。
労働基準法：１日あたり、１週間あたりの労働時間や休日の基準を定めている。これを超える場合は、３６協定と呼ばれる労使協定を結ぶ。
ソフトウェアライセンス契約：あらかじめ許可された台数までインストールして利用できるなどの契約形態
オープンソースソフトウェア（OSS）：プログラムのソースコードが公開され、改良や再配布が自由にできるソフトウェア
標準化団体：ISO（国際標準化機構）、IEEE（米国電気電子学会）、JISC（日本工業標準調査会）など

学習をしての気づき
関連法規の詳細についてはあまり理解できていなかったところもあったので、勉強になりました。普段の実務では、法規上してはいけないことを単にしないように指示はされますが、その根拠となる法規についてはあまり意識していないことが多いと思います。今回の学習を通して、その根拠についてしっかりと理解ができたので、大変参考になりました。
また、各法規の対象となる範囲もそれぞれ微妙に異なるので、しっかりと理解をしておいたほうが良いと思います。コンピュータを使用した不正行為でも、様々な法規で規定がされており、不正行為の内容によって対象となる法規が違うことが理解できました。
そして、自分が知らないうちに他人の権利を侵害したり、不正行為に加担したりしてしまう可能性があることも整理できたので、大変勉強になりました。

情報セキュリティマネジメント試験受験編

IT入門お役立ち情報：情報セキュリティマネジメント試験受験編（その６）

関連分野のテクノロジー系について勉強しました
テクノロジー系の基礎知識として、次のような項目について学習しました。

- システム構成

クライアントサーバシステム：クライアントがサーバに処理を依頼し、サーバがその処理をして応える形態。代表例としては、Webアプリケーションシステムがある。
クラウドコンピューティング：インターネット上にデータを置き、どのデバイスからも利用できるようにする処理形態。
MIPS：CPUの性能を表す指標で、1秒間に実行できる命令数を表す。
スループット：単位時間に処理できる仕事量を表す。
RASIS：信頼性、可用性、保守性、完全性、安全性のシステムを評価する概念。
フォールトトレランス：システム障害が発生しても、システムが停止しないようにする考え方。

- データベース

関係データベース：データを表形式で管理するデータベース
SQL（Structured Query Language）：関係データベースを操作するための言語。必要な情報を取り出すことをクエリ（問合せ）とよび、SELECT文が用いられる。
トランザクション：いくつかの処理をまとめた一連の処理単位。

- ネットワーク

LAN（Local Area Network）：敷地内や建物内などに敷設したネットワーク
WAN（Wide Area Network）：地理的に離れた場所をつなぐネットワーク
通信プロトコル：通信に際して制御のための取り決め（ルール）を定めた規約
インターネット：通信にTCP/IPプロトコルを用い、WWWや電子メール、ファイル転送などの様々なサービスを利用できる。
IPアドレス：TCP/IPネットワーク中で機器（ホスト）を識別するための番号
ポート番号：アプリケーションがデータ通信を行うために割り振られた接続用の番号

学習をしての気づき
この分野は、コンピュータの基礎知識に関する学習です。
情報セキュリティを考える上で、最低限必要な知識が網羅できるように、基礎的な内容が出題されていると思います。
情報セキュリティの技術的な脅威を理解する上では、その前提となる知識を習得しておくことは必要不可欠です。特にネットワーク関連の知識は、情報セキュリティ技術と関連が深いので、しっかりと学習する必要あります。つまり、コンピュータがネットワークに接続されていると、脅威にさらされる機会が随分と増えますので、ネットワークに関する十分な理解が必要です。
私自身は過去にネットワーク構築の仕事にも携わっていたので、これらの学習を通じて自分の知識の復習及び整理になりました。

IT入門お役立ち情報：情報セキュリティマネジメント試験受験編（その７）

関連分野のマネジメント系について勉強しました
マネジメント系の基礎知識として、次のような項目について学習しました。

- プロジェクトマネジメント

ステークホルダ：プロジェクトの利害関係者。顧客やスポンサーだけではなくプロジェクトマネジャー・メンバーも含む。
WBS（Work Breakdown Structure）：プロジェクトで必要な作業（タスク）を洗い出した図
クリティカルパス：作業日程上、全く余裕のない作業の工程
アーンド・バリュー・マネジメント：進捗を金銭的な価値に換算して管理する手法

- サービスマネジメント

SLA（Service Level Agreement）：サービス内容、提供レベルなどについて、顧客とプロバイダ間で取り決めた合意書
サービスデスク：顧客やユーザからの質問や相談、インシデント（障害）の報告を受け付け、一次対応およびサポートチームにエスカレーションする
問題管理：インシデントの根本原因を探り、それを排除するための活動
サービス復旧：復旧対策における指標として、RTO（Recovery Time Objective：復旧時間目標）とRPO（Recovery Point Objective：復旧時点目標）がある

- システム監査

ITガバナンス：情報戦略の策定や実行をコントロール（統制）して、企業をあるべき方向へ導くこと
コントロール：ものごとを正常・適切な状態とするための仕組みや環境
システム監査人：外観上と精神上の独立が求められる
システム監査実施：予備調査でコントロールの有無を確認して、本調査でコントロールが正しく機能していることを確認する
監査報告書：指摘事項、改善勧告、監査人の意見などが記されている
フォローアップ：改善状況を監視して、改善活動に関してアドバイスを行う

学習をしての気づき
この分野は、私がこれまで経験してきた仕事に大いに関連していたので、特に問題なく理解できました。
私自身実際にシステム構築のプロジェクトに携わったり、システムオペレーションのサービスを担当したり、またシステム監査の対応に追われたりしてきましたので、それぞれの内容をこれまでの経験と照らし合わせながら、学習することができました。
例えば、問題管理については、私が社会人になりたての頃に、会社で徹底的に教え込まれたのを思い出しました。つまり、問題に対して応急処置だけで終わらさずに、必ず予防処置までを考えることが重要であるということです。
また、システム監査のフォローアップについては、現場の責任者として、改善勧告に対して必ず何らかのアクションを取っていなければならないことが、結構なプレッシャーになったりしましたね。

情報セキュリティマネジメント試験受験編

IT入門お役立ち情報：情報セキュリティマネジメント試験受験編（その８）

関連分野のストラテジー系について勉強しました
ストラテジー系の基礎知識として、次のような項目について学習しました。

- システム戦略・企画

全体最適化計画：個々の戦略を部分的に最適化するのではなく、全体として最適な状態を目指す。
CIO（Chief Information Officer）：組織における情報システムに関する最高責任者。情報戦略の策定と情報システムの計画・実行を統括する。
BPR（Business Process Re-engineering）：ビジネスプロセスや業務フローを根本的に見直し、業務の再構築を行う。
共通フレーム：ソフトウェアの構想から開発、運用、保守、廃棄までの各段階で、どのような作業が必要か、作業の役割は何かを規定。
ASP（Application Service Provider）：インターネットなどを利用して、アプリケーションサービスを提供する事業者
SOA（Service Oriented Architecture）：業務システム全体を個々の業務プロセス（ソフトウェア部品）の集合とみなす考え方。

- 企業活動

BCP（Business Continuity Plan）：災害発生時の事業継続計画
QC七つ道具：特性要因図（ある特性の要因を分析するのに用いる魚の骨のような図）、散布図（２変数間にどのような関係があるかを分析する図）、管理図（工程に異常があるかどうかを検証するために用いられる）、パレート図（ABC分析などで使用する棒グラフと折れ線グラフからなる図）など
データマイニング：大量のデータを分析し、データ間の規則性や関係性を見つける技法
財務諸表：貸借対照表（決算日などにおける財務状態を表す）、損益計算書（会計期間における経営成績を表す）、キャッシュフロー計算書（会計期間中の現金の流れを表す）など。
減価償却：固定資産の費用を複数年に割り振って費用化すること。

学習をしての気づき
企業での情報システムの役割や戦略的な活用について、改めて意識をするような問題です。また、そのシステム戦略をどのように構築していくかについて、具体的な手法などを問われます。
この分野では基本的に各用語の意味を理解していれば、解ける問題が多いと思いますので、各用語を覚えることができればよいかと思います。
私自身は、ASP、BCPやQC七つ道具から財務関連用語まで、これまでの業務で携わってきた用語が多かったので、比較的容易に学習を進めることができましたが、それぞれの用語の復習・整理になりました。

追記：2020年3月24日に、令和2年度春期情報処理技術者試験・情報処理安全確保支援士試験の取りやめ（中止）が発表されました。この試験に向けて勉強してきたので、受験できないのは大変残念ですが、今後の試験や自身のスキルアップのためにも受験勉強は継続していきます。

情報セキュリティマネジメント試験受験編

IT入門お役立ち情報：情報セキュリティマネジメント試験受験編（その９）

午後問題対策のために用意された事例集について勉強しました
午後問題対策のために用意された事例集を通して、次のような項目について学習しました。

- 標的型攻撃の対策

「不審なメールや添付ファイルは開かない」、「疑わしいメールのURLはクリックしない」などの基本的なルールをユーザに周知する。
コンピュータのOSやアプリケーション、ウィルス対策ソフトを最新の状態に保つ。
ウィルス感染や情報漏えいが発覚した場合の報告手順を定め、周知する。
フィッシング詐欺等に関する最新情報を周知する。

- パスワードに関する攻撃の対策

パスワードに関する基本的なルールを設定し、周知徹底する。
使われなくなったユーザIDは速やかに削除する。
複数のサービスで同じパスワードの使い回しをしない。

- ソフトウェアの脆弱性対策

脆弱性に関する情報収集を欠かさず、セキュリティパッチが公表されたら迅速に適用する。
サポート終了に備えて、別製品や後継製品への移行を計画し、実施する。

- クラウドサービス利用における対策

サービス提供事業者のセキュリティ対策を確認する。
クラウドに保存したデータについてバックアップを取る。
クラウドサービスの停止時や障害発生時の対応について対策する。

- スマートデバイス利用における対策

個人所有のモバイル機器を業務上で利用する場合は、適切なセキュリティ対策を利用者に義務付ける。
モバイル機器のOSやアプリケーション、ウィルス対策ソフトを最新の状態に保つ。
信頼できるアプリのみをインストールし、業務とは関係のないアプリをインストールしない。

- 内部不正防止のための対策

システム管理者の適切な権限設定と監視
サーバールームや情報機器および記録媒体などの物理的な保護と管理
内部不正防止のための従業員教育
公平な人事評価や適正な労働環境の整備

学習をしての気づき
具体的な事例に基づき問題がなされるので、実務経験があれば取り組みやすいと思います。
事例はインシデント対応やシステム運用に関する有りがちなケースが元になっているため、私自身は実際に似たような事例を経験したことがあるので、臨場感があって理解しやすかったです。
ただし、攻撃の手口やそれに関連するIT技術については最新のものを理解しておく必要があります。
また、関連法案が実際の現場でどのように適用されているかについての事例についても学習が必要です。
そして、情報セキュリティポリシーの導入なども現場の抵抗にあうことが多いので、その対策も問われることが多いと思います。

情報セキュリティマネジメント試験受験編

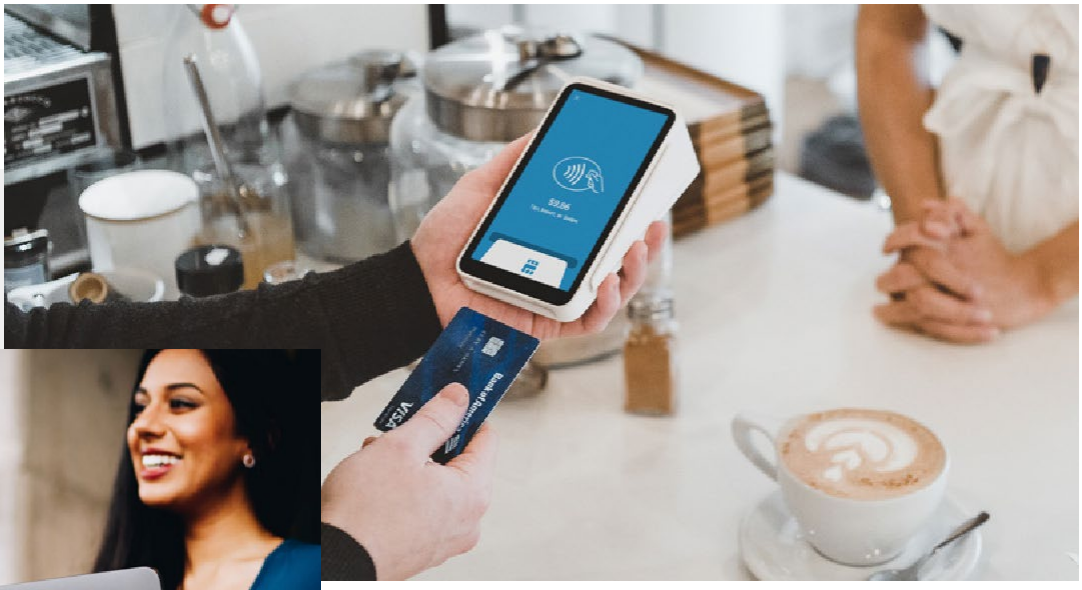
IT入門お役立ち情報：情報セキュリティマネジメント試験受験編（その１０）

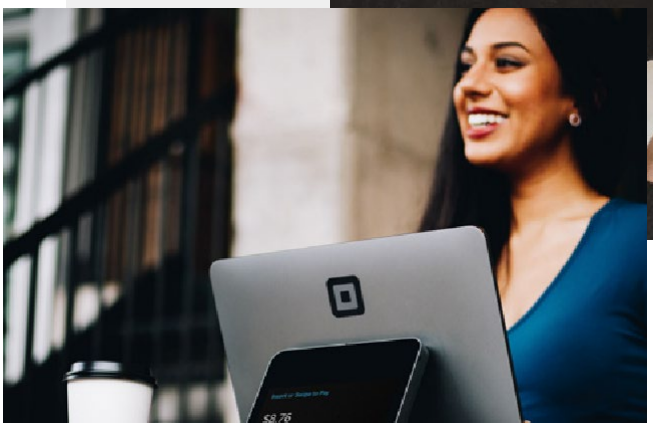
まとめとして過去問題を勉強しました

過去問題として、令和元年秋期試験問題を解いてみました。
午前問題は、90分間で50問出題されます。各問題については、4つの選択肢から一つの正解を選びます。
約6割はセキュリティ技術に関する問題で、残りは関連法規やマネジメント・ストラテジー系の問題でした。
セキュリティ技術に関する問題は、用語の意味や内容を問われる問題が多かったです。これらの問題に対しては、その用語について知らなければ、例えば消去法で正解を選択しようと思っても、なかなか難しいところがありました。また、リスクベース認証やPCIDSSなど、近年一般的に使われていたり、話題になっている新しい技術などについても出題がされています。
マネジメントやストラテジー系の問題は、比較的基本的な知識を問われることが多かったです。そして、関連法規に関する問題は、具体的な事例をもとにどの法規が関連するかなどが問われたりしていました。
午後問題は、90分で3問出題されます。長文形式で問題ごとに設問が複数ありますが、それぞれ選択肢から正解を選びます。また、一つの正しい選択肢を選ぶだけではなく、正しい選択肢の組み合わせを回答する問題もありました。
私が午後問題を解いてみた結果、3問解くのに90分でも時間的な余裕はあまりありませんでした。なぜなら、問題の本文や設問が長文なのでかなりの読解力が求められ、それもある程度の速度で読み解く必要があったからです。
それぞれの問題は事例をベースにして、セキュリティ上の問題やその対策について各事例の状況に応じて解答を求められます。したがって、一般的な解答を求められるのではなく、各事例に応じた具体的な解答を選択しなければならないので、本文の内容をよく理解する必要があります。
また、多くの人物やシステム機能・制限について本文に出てくるので、頭の中で整理するのも一苦労でした。そのために、設問を確認したあとに該当の本文部分に戻ったりと、何度も複数ページを行き来したので、このような問題の解き方に慣れていないと効率よく解答するのは難しいと思いました。

学習をしての気づき

セキュリティ技術に関する用語については、必ずしも全問正解する必要はありませんが、知らないと解けない問題が多いため、合格基準に達する程度解答するためには、各セキュリティ技術に関する概要だけではなく、ある程度詳細な技術内容についての学習が必要かもしれません。
関連法規については、個人情報保護法などの近年の法改正なども視野に入れる必要あると思います。
そして、午後問題に関しては、制限時間内で長文を読解することの訓練が必要だと思いました。設問をどのような順番で解いていくか、例えば全て本文を読んでから設問に取り掛かるのか、本文中で設問に関する箇所のたびに設問を解くのかなど、自分に適した自分なりの解き方を決めておいたほうが良いでしょうね。





おわりに

私自身のこれまでのシステム部門やユーザ部門での仕事で習得した知識や経験などを整理するのと同時に新しい技術も習得する目的で、ITの専門家ではなくITを利用する立場で、情報処理技術者試験の「情報セキュリティマネジメント試験」を受験することにしました。そして、私自身が実際に受験勉強や受験をしてきたなかで、私なりにこれは重要だと思うことや、これは改めて役に立ったと感じたことを書いてみましたが、いかがだったでしょうか。

これから「情報セキュリティマネジメント試験」を受験したいと考えている方の参考になればと思っています。

もし、何かご意見があれば、少しでもコメントいただければ幸いです。

お問い合わせ

ITコンサルタント：佐藤豊史（さとうとよし）のブログ