ITコンサルタント：佐藤豊史（さとうとよし）のブログ

情報処理安全確保支援士試験受験編

私が2020年4月から情報処理安全確保支援士試験の受験勉強を始めて、2020年10月に受験をして合格するまでのブログをまとめました。

目次

情報処理安全確保支援士試験受験編

IT入門お役立ち情報：情報処理安全確保支援士試験受験編（その１）

情報処理安全確保支援士試験を受験することにしました
昨今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。そして、そのような人材を育成、指導できる、または経営層に助言、提案して支援する情報セキュリティ分野のエキスパートを求める声が高まっています。
そこで、私自身がそのようなエキスパートになるべく、また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も兼ねて、情報処理技術者試験の「情報処理安全確保支援士試験」を受験することにしました。

これまで私はITの専門家という立場からだけではなく、ITを利用する現場で情報セキュリティについて対応する立場でもあったので、実際の現場での情報セキュリティへの対応というものが、容易ではないことは身につまされてきました。また、日進月歩のセキュリティの世界では立ち止まることは許されないため、日々自分の知識も更新しなければなりません。そのため、近年の情報セキュリティに関する動向や対応についても関心があります。

当初は、この４月に「情報セキュリティマネジメント試験」を受験して、その次のステップとして「情報処理安全確保支援士試験」を受験するつもりでした。しかし、残念ながら令和2年度春期試験が取りやめ（中止）になったために、「情報セキュリティマネジメント試験」の受験を待たずに、「情報処理安全確保支援士試験」を受験することにしました。
これから、受験勉強を始めて今年の秋期の試験には受験したいと考えています。具体的には、「情報処理教科書 情報処理安全確保支援士 2020年版、上原 孝之（著）」という参考書をもとに、次のとおり、勉強を進めていき試験を迎えたいと思います。

1. 序盤：基礎知識固め
2. 中盤：記述式試験に向けてトレーニング
3. 終盤：重要分野と最新トレンドの把握・整理
4. まとめ：過去問題で最終チェック
5. 受験（2020年10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。

情報処理安全確保支援士試験受験編

IT入門お役立ち情報：情報処理安全確保支援士試験受験編（その２）

序盤：基礎知識固めとして参考書を勉強しました（1）
参考書の章立てに沿って、次の内容について勉強しました。そこで、気づいたことや感じたことを少し述べてみます。

- 情報セキュリティの基本的な考え方

セキュリティとは何かに始まり、情報セキュリティのCIAや基本的な対策の考え方を改めて学習できました。ここでは、そもそもセキュリティはなぜ必要か、あるいはどのような考え方で対策するべきかなど、抽象的な概念の整理ができました。セキュリティ担当者としては、普段はあまりこのようなことは意識していないと思うのですが、振り返るとこれらの基本的な考え方に則って仕事をしていることに気づかされます。

- ISMSに関する規格と制度

ISMSの元になっているISO／JIS規格の役割や内容とその認証制度について学習しました。27000シリーズがベースになっていて、その概要を知る機会になりました。ISMSはセキュリティ対策を実装するだけではなく、PDCAサイクルを導入することが重要なようです。また、認証のプロセスは、一般的な監査手順と似ていますので、監査対応などの経験があれば、理解しやすいと思われます。

- TCP/IPの仕組み

現代のネットワークの基本的なプロトコルであるTCP/IPの仕組みに関する基礎的な内容について学習しました。純粋にネットワークの学習で、セキュリティに関する詳細ではありませんが、昨今のセキュリティではネットワークが重要な役割を果たしており、また基本的な仕組みはほとんど変わらないので、それらを理解しておくことはとても大切です。今回は、自分の知識の整理になりましたし、新たな知識の習得にもなりました。

- クラウドと仮想化技術

近年活用が進んでいるクラウドサービスに関する学習です。サービスの提供形態の違いやセキュリティ上の留意点が学習のポイントです。仮想化技術については、サーバの仮想化だけではなく、クライアント端末の様々な仮想化技術についても学びました。このあたりは、日々進歩している領域だと思いますので、新しい技術についてもチェックしておく必要がありそうです。

- 脅威の分類と概要

情報セキュリティを脅かし、損失を発生させる原因となるものが脅威ですが、まずは脅威にどのようなものがあるのかを知らずして、セキュリティ対策を考えても万全とは言えません。脅威といえば、悪意のある攻撃など意図的な人の脅威を真っ先に思い浮かべがちですが、操作ミスなどの偶発的な人の脅威も考慮する必要があります。また、災害や人為的な脅威だけではなく、障害も脅威の一つとして考えることも大切だと改めて認識しました。

情報処理安全確保支援士試験受験編

IT入門お役立ち情報：情報処理安全確保支援士試験受験編（その３）

序盤：基礎知識固めとして参考書を勉強しました（2）
参考書の章立てに沿って、次の内容について勉強しました。そこで、気づいたことや感じたことを少し述べてみます。

- ネットワークを介した攻撃手法

- ポートスキャン自体は、攻撃そのものではないですが、この対策を怠ると攻撃の対象になるので、疎かにできないです。
- バッファーオーバーフロー攻撃は、システムやサービスの停止を引き起こすだけかと思っていましたが、システムへの侵入や管理者権限の取得までされるような攻撃であることが理解できました。
- パスワードを破ろうとするパスワードクラッキング行為は、典型的な攻撃です。パスワードを破られた場合は、そのアカウントのユーザに影響を与えるだけではなく、特に管理者権限のアカウントの場合は、システム全体に影響を及ぼします。しかし、昨今は一人のユーザがいくつもシステムやアプリのアカウントを保有して、それらのパスワードを管理しなければならないので、対策が大変な攻撃の一つです。
- セッションハイジャックは、攻撃者がサーバやクライアントになりすまして、不正行為を働きます。なりすましでは、いろいろな被害が想定されますので、とても危険です。
- DNSサーバに対する攻撃では、DNSサーバや攻撃対象のサーバを過負荷にして、サービス不能状態を引き起こしたりしますが、キャッシュに偽情報を登録して、偽サイトに誘導するファーミングという手法も脅威です。
- DoS攻撃は、攻撃対象が正常動作できないサービス不能状態に陥れる行為ですが、これらを根本的に防ぐのはとても困難な攻撃です。
- クロスサイトスクリプトやSQLインジェクションのようなウェブアプリケーションに不正なスクリプトや命令を実行させる攻撃は、いろいろな種類があります。私自身は普段はスクリプトなどコードに触れる機会は少ないので、それぞれの攻撃の内容を理解するのは、少し苦労をしましたが、代表的なものはしっかりと理解しておくほうが良いでしょう。
- ユーザの意図に反する不正な振る舞いをするように作られたマルウェアは、多種多様なものがあり、代表的なものについては、それぞれ仕組みや対策を理解する必要があると思います。マルウェアは代表的な攻撃手法の一つでもあり、年々新しいものが出てきているので、最新の情報にもチェックをしておくべきでしょう。近年特に、標的型攻撃といって特定の組織や団体などをターゲットにした攻撃が行われているようで、一部の企業などで大きな被害が出て問題となっているので、出題される可能性が高いのではと思います。

情報処理安全確保支援士試験受験編

IT入門お役立ち情報：情報処理安全確保支援士試験受験編（その４）

序盤：基礎知識固めとして参考書を勉強しました（3）
参考書の章立てに沿って、次の内容について勉強しました。そこで、気づいたことや感じたことを少し述べてみます。

- 情報セキュリティにおける脆弱性

情報セキュリティにおいてリスクが発生する要因の一つが脆弱性ですが、様々な種類の脆弱性があります。この脆弱性に対していかに対策を講じていくかが、リスクを発生させないために大変重要ですし、脅威と違って自分たちでコントロールが可能です。つまり、脆弱性への対策が、情報セキュリティの要だと改めて認識しました。

- ネットワーク構成における脆弱性と対策

ネットワーク構成での対策は、可能な限り使用目的に応じたセグメントに分けることに尽きます。攻撃が標的に及ばないように、または被害を拡大しないようにも、VLANを構築して、接続口も必要最小限に抑えることが肝心です。

- TCP/IPプロトコルの脆弱性と対策

プロトコルの仕様が公開されているからこそ、世界標準のプロトコルとして普及していますが、裏を返せばそれを悪用もされやすいということです。特にIPv4は暗号化機能が標準装備されていないので、盗聴による漏洩のリスクが高いです。しかし、これだけ普及しているプロトコルを容易に変えるわけにはいかないので、それらへの対策を施す必要があります。そして、このTCP/IPプロトコルの基本的なところを理解しておくことは、後の学習にも役立つと思います。

- 電子メールの脆弱性と対策

古くから普及して使用されている電子メールに関するプロトコルは、シンプルであるが故に、数多くの脆弱性が指摘されています。電子メールにおいて大きな問題は、やはり膨大な迷惑メールですが、これらはメールサーバにおける脆弱性が原因となっています。それらへの対策として、代表的なSMTPとPOPに関しては、様々な対策が取られていますが、なかなか根本的な対策はないように思われます。なお、電子メールはよく使われるツールなので、出題されやすい分野でもあると思います。

- DNSの脆弱性と対策

名前解決を行うDNSにもいくつか脆弱性があり、これらを悪用されると悪意のあるサイトに誘導されたりして大変危険です。DNSSECなどいくつかの対策が講じられているようですが、そのためにシステムにも負荷が高くなってきているようです。

- HTTPおよびWebアプリケーションの脆弱性と対策

インターネット上で最も使用されるHTTPプロトコルとWebアプリケーションには、その仕様や特性からセッション管理に関する脆弱性が大きな問題です。これらに対しては様々な対策が必要となりますが、脆弱性が適切に対策されているかどうかはなかなかわかりません。したがって、Webアプリケーションを新規開発するときには、それらの脆弱性に対する考慮をした設計をする必要がありますし、本番運用する前は、必ず脆弱性検査を実施することが必要です。このセキュリティを考慮した設計は、システム開発に関する問題としても出題されるでしょう。

情報処理安全確保支援士試験受験編

IT入門お役立ち情報：情報処理安全確保支援士試験受験編（その５）

序盤：基礎知識固めとして参考書を勉強しました（4）
参考書の章立てに沿って、次の内容について勉強しました。そこで、気づいたことや感じたことを少し述べてみます。

- リスクアセスメント

組織や情報システムに内在する情報リスクを洗い出し、その大きさや影響度を評価することによって、初めてセキュリティ対策を計画することができます。やみくもにセキュリティ対策を検討しても、それが効果的かどうかはリスクアセスメントをベースにして考えないといけないと改めて認識しました。そして、その対策を実施して、対応方法を適宜見直すことまで行うリスクマネジメントを、継続的に繰り返すことが肝心です。

- 情報セキュリティポリシー

情報セキュリティに対する組織の基本的な考え方や方針を示すもので、これが組織内で周知徹底されていないと、セキュリティレベルを向上できなかったり、全社的に効率的なセキュリティ対策を取れなくなる可能性があるので、策定するだけでは十分ではありません。また、情報セキュリティに対する責任の所在を明確にした管理組織体制も重要です。

- 情報資産の管理

リスクアセスメントでも基本となる情報資産を洗い出して、それらを分類して管理のレベルを決めることによって、情報の機密度や重要度に応じた対策を施して、情報資産を適切に取り扱うことが可能になります。近年は、情報資産を保存できるクライアントPCの管理も同様に重要です。いずれにせよ、まずは情報資産を管理するための資産台帳を整備することが肝心だと思います。

- 物理的・環境的・人的セキュリティ

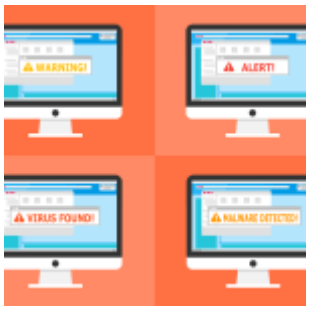
技術面のセキュリティ対策だけではなく、災害や障害の脅威および不正行為などについては、物理環境面や人的資源に対するセキュリティの確保が必要になります。セキュリティと言うとつい技術面だけを注目しがちですが、こちらも大切です。

- インシデント管理や事業継続計画（BCP）

何か問題が発生した場合や何らかの危機や災害が発生した場合に、どのように対応するかについては、予め計画や準備をしておく必要があります。これらが準備されていれば、いざというときでも慌てることはないですね。

- 情報セキュリティ監査及びシステム監査

情報セキュリティを向上させるためには、定期的にチェックをすることが効果的です。そのための監査として、これらはもっと活用されるべきだと思います。その際には、単なる現状の評価にとどまらずに、どのようにすれば改善できるかにもっと注力するべきでしょう。



情報処理安全確保支援士試験受験編

IT入門お役立ち情報：情報処理安全確保支援士試験受験編（その６）

序盤：基礎知識固めとして参考書を勉強しました（5）
参考書の章立てに沿って、次の内容について勉強しました。そこで、気づいたことや感じたことを少し述べてみます。

- ホストの要塞化

OSやソフトウェアのセキュリティ上の問題をなくして堅牢な状態にすることで、ハードニングとも呼ばれています。ホストの堅牢さを維持するには、随時点検が必要です。

- 脆弱性検査

実際にOSやアプリケーションに脆弱性がないか検査をすることは重要です。システムやサイトを本番稼働する前には、この検査が必須だと思います。

- ファイアウォール

ネットワークからの不正アクセスや攻撃を防御するための代表的な対策が、ファイアウォールです。また、不要なパケットを遮断することによって、ネットワークの利用効率を高めることが可能になることも、私にとっては新たな視点でした。

- Webアプリケーションファイアウォール（WAF）

ファイアウォールだけでは防御できないWebアプリケーションに対する攻撃に対応します。ただし、セッションハイジャックなどのWebアプリケーションのロジックの脆弱性を突いた攻撃などに、対応することは容易ではありませんので、決して万能ではないです。また、誤検知やWAF自体の処理能力の問題で、サービスに影響が出る可能性があるので、設計や構築においては十分な考慮が必要です。

- 侵入検知システム（IDS）

リアルタイムでネットワークやホストコンピューターを監視して、侵入や攻撃を検知します。検知した後は、管理者に通知をするなどのアクションを実行しますが、アプリケーションの脆弱性を突いた攻撃などはほとんど検知できません。また、ある程度の誤検知は避けられないので、その対応を考慮しておく必要があります。

- 侵入防御システム（IPS）

ネットワークのIDSと同等の侵入検知機能と、その防御機能を備えたシステムです。IDSのように検知することだけではなく、不正なパケットを遮断することができます。IDSの機能が強化されたシステムですが、IDSと同様に誤検知などのリスクがあるので、それらの課題に対する考慮が必要です。
検知・防御については、万能の対策はないので、最大限の防御ができるような対策の検討を、考えて実行し続けるしかないのだろうと思います。

情報処理安全確保支援士試験受験編

IT入門お役立ち情報：情報処理安全確保支援士試験受験編（その７）

序盤：基礎知識固めとして参考書を勉強しました（6）
参考書の章立てに沿って、次の内容について勉強しました。そこで、気づいたことや感じたことを少し述べてみます。

- アクセス制御

情報資産の機密性を確保するための最も基本的かつ重要な技術が、アクセス制御です。情報資産に対して権限のある者にのみ、アクセスを許可する仕組みです。アクセスする利用者を何らかの情報に基づいて識別して、認証します。そして、誰にどのようなアクセス権限を与えるかというルールを、慎重に検討する必要があります。これらに問題があると、セキュリティ上の問題につながりますので、アクセス制御は重要なセキュリティ対策の一つだと思います。

- 認証技術

情報資産にアクセスを要求する者の正当性や真正性を確認することが、認証という技術です。正しい権限を保持しているのか、またはその本人に間違いがないのかなどを、正しく確認できなければ、セキュリティ上の問題になります。また、認証の強度を高めるために、一度の認証だけではなく、複数の要素や二段階で認証することが広く普及しており、私自身も近年よく経験をします。

➢ パスワード認証

予め登録された利用者本人しか知らないパスワードで、本人を認証する非常にシンプルで実装が容易な、そして古くから用いられてきたシステムです。このシステムが機能するためには、本人しか知らない、そして他人に推測しづらいパスワードであることが前提ですが、現実には容易ではなく、私自身も運用に苦労した経験があります。

➢ ワンタイムパスワード方式

認証を行うたびに毎回異なるパスワードを使用する方式で、使い捨てパスワード方式とも呼ばれます。たとえパスワードを盗聴されても、そのパスワードは二度と使用されないために、なりすましによる不正アクセスの可能性はとても低くなります。

➢ バイオメトリクス認証

人間の身体的な特徴や行動面での特性などを利用して、本人の認証をします。これらは、本人以外には保持できないために、非常に有効な認証方式です。しかし、確実に本人を認証するための技術が必要で、導入もまだまだ高価な点が課題だと思います。

➢ 様々な認証技術

その他に、認証システムを実現する技術として、RADIUS、TACACS、Kerberos、ディレクトリサービス、EAPなどがあります。認証のための情報を一元管理して、役割分担を明確にして、様々なシステムで利用できます。

➢ シングルサインオン

一回の認証で複数のシステムについて利用できるようにする技術で、認証を必要とするシステムが増えたために、昨今導入がされています。シングルサインオンを実現するための様々な仕組みがありますが、十分なセキュリティが確保することが求められます。

情報処理安全確保支援士試験受験編

IT入門お役立ち情報：情報処理安全確保支援士試験受験編（その８）

序盤：基礎知識固めとして参考書を勉強しました（7）
参考書の章立てに沿って、次の内容について勉強しました。そこで、気づいたことや感じたことを少し述べてみます。

- 暗号化技術

情報資産の機密性を高めるために有効な手段が、情報そのものを暗号化することです。特に情報を受け渡すときに使用される、ネットワーク環境での暗号化技術には様々な技術があります。私自身は、それぞれの技術の概要については知っていましたが、その詳細については、あまり知らなかったので、大変勉強になりました。試験でもよく出題される分野のようですので、十分な準備が必要そうです。

➢ 暗号方式
共通鍵暗号方式と公開鍵暗号方式が基本ですが、それぞれの暗号化の仕方についても理解が必要です。
➢ ハッシュ関数
一方向性の関数で、出力結果から入力データを逆算できないので、暗号化技術では非常に重要な役割を果たしており、改ざん検知に有効な技術です。
➢ VPN
パブリックネットワーク上に、仮想的なプライベートネットワークを構築する技術です。カプセル化とトンネリングという技術が用いられています。
➢ IPsec
IP（Internet Protocol）のセキュリティを高めたプロトコルで、暗号化通信が可能です。IPsecには、様々なプロトコルや機能があり、いろいろと進化しています。
➢ SSL/TLS
Webサーバとブラウザ間でデータを安全にやり取りするために、使用されているプロトコルです。古くから業界標準として使用されてきましたが、過去に重大な脆弱性が発見されて、都度バージョンアップしています。
➢ その他の通信技術
セキュアな通信を実現する技術としては、SSH、S/MIME、PGPなどがあり、これらも理解をしておく必要がありそうです。
➢ 無線LAN環境でのセキュリティ対策
当初の無線LAN環境でのセキュリティについては、脆弱性があるということで、WEPという暗号化方式が、WPA、WPA2、WPA3と改善されてきています。
➢ PKI（公開鍵基盤）
公開鍵暗号方式では、公開鍵や秘密鍵の正当性を保証することが重要ですが、これを実現するために、ディジタル証明書に関する機関や技術があります。これらを利用して、データの作成者の正当性や改ざんの確認ができます。タイムスタンプ技術により、データ作成された時刻情報の確認もできます。これらの技術は電子文書の保存にも重要な役割を果たしています。

情報処理安全確保支援士試験受験編

IT入門お役立ち情報：情報処理安全確保支援士試験受験編（その９）

序盤：基礎知識固めとして参考書を勉強しました（8）
参考書の章立てに沿って、次の内容について勉強しました。そこで、気づいたことや感じたことを少し述べてみます。

- システム開発におけるセキュリティ対策

各システム開発工程にて、それぞれ推奨されるセキュリティ対策があります。つまり、システム開発終了後にセキュリティ対策を検討するのではなく、システム開発当初からセキュリティ対策を検討しておく必要があります。特に、要件定義フェーズから、セキュリティ対策の基本方針を決定することが重要だと思います。

- C++言語のプログラミング上の留意点

C++言語には、バッファーオーバーフロー攻撃の標的となりやすい言語仕様上の問題があるので、これに対する留意点や対策が多く解説されています。

- Javaのプログラミング上の留意点

Javaは他の言語と比べて、セキュアな開発を行うのに適した言語といえるようです。サンドボックスモデルのように、セキュリティが確保された環境が提供されていますが、それでもいくつか留意点があります。

- ECMAScriptのプログラミング上の留意点

ECMAScriptとは、JavaScriptなどを標準化したスクリプト言語です。これに関連した技術として、AjaxやJSONなどがあり、これらを利用する上での留意点があります。

- 情報セキュリティに関する規格・制度

ISOなどの国際標準化機関で策定された情報セキュリティに関する様々な規格があります。多くは、日本のJIS規格にも策定されており、それに関する認証制度などもあります。IT関連製品や情報システムそのもののセキュリティレベルを評価するものと、組織自体のセキュリティレベルを評価するものに分かれます。

- 情報セキュリティに関する法律・制度

コンピュータ犯罪を取り締まるために、これまで様々な法律が施行・改正されてきました。そして、著作権などの知的財産権を保護するための法律についても理解が必要です。また、個人情報保護やマイナンバーに関する法律・ガイドラインおよびプライバシーマーク制度もあります。これらは正しく理解をして、自分が意識せず違法行為をしていないか注意することも大切だと思います。

- 電子文書に関する法令・制度

企業などが事業活動で作成する法定文書について、電子文書による保存が容認されてきています。そのための法令や、それを可能にするためのタイムスタンプに関する制度なども理解が必要です。

- 内部統制に関する法制度

組織内に違法行為や不正行為などが発生しないように、活動全般を適切にコントロールすることを内部統制といいますが、それを維持するための法律があります。本来は、このような法律がなくても、企業としてこのようなことが発生しないようにするべきですが、現実はさにあらず、残念なことです。

情報処理安全確保支援士試験受験編

IT入門お役立ち情報：情報処理安全確保支援士試験受験編（その１０）

中盤：記述式試験に向けてトレーニングとして問題集を勉強しました（1）
「2020　情報処理安全確保支援士「専門知識＋午後問題」の重点対策、三好康之（著）」という問題集の章立てに沿って、次の内容について勉強しました。そこで、気づいたことや感じたことを少し述べてみます。

- 認証とアクセスコントロール

セキュリティの基本中の基本であり、認証技術はほぼ毎年出題されているテーマです。その中でも、シングルサインオンに関する出題が目立ってきているようです。昨今はクラウドサービスの利用も増えてきているので、この技術が重要になってきている背景があると思います。また、業務上様々なシステムにアクセスする必要がある場合は、そのシステムを統合して利用できるようにするためにも必要な技術です。

- PKI

SSL/TLSやディジタル証明書に関する問題は、コンスタントに出題されているようです。暗号技術やディジタル証明書については、日頃利用はしているのですが、その仕組みについて普段あまり意識したことはなく、いざ問題を解くとなると結構苦戦をしましたが、自分の知識の整理にはとても役立ったと思います。また、電子文書に関する証明書についての知識も習得できました。

- ファイアウォール・IDS・IPS・UTM

ネットワークからの攻撃を防御するための技術ですので、ネットワークが関連する問題では必ず登場してくると思います。ここでは、とにかくどのネットワーク経路を通って、通信が行われているかを理解することが、いちばん大切で、そのネットワーク図が正しく描ければ、容易に解答にたどり着けると思います。

- サーバセキュリティ

サーバを要塞のように構築・設定をして、脅威への対策をすることが基本になります。そして、個別にWebサーバとDNSサーバに対する対策なども必要です。代表的な攻撃に対する対策を理解するために、各サーバの個別の技術を理解しなければならないので、私にとっては改めて勉強になりました。

- 電子メールのセキュリティ

まずは、電子メールそのものの仕組みをしっかりと理解する必要があります。電子メール自体は古くからある技術ですが、それ故にセキュリティ的には脆弱なところが多々あり、それに対する仕組みが色々追加されてきたような感じです。業務上も大変良く使われるシステムだと思いますので、しっかりと学習したいと思います。

- リモートアクセス

今やリモートアクセスは日常になってきていると思いますが、ここでもそれ相応のセキュリティが必要になります。接続する機器やユーザを正しく認証することと、通信を暗号化することがポイントになると思います。リモートアクセスで使用する機器については、運用上のルールなども重要なポイントではないかと思います。

情報処理安全確保支援士試験受験編

IT入門お役立ち情報：情報処理安全確保支援士試験受験編（その１０）

- セキュアプログラミング

必ず出題されているテーマです。ある程度ソースコードを理解できる知識が必要になりますが、問われている知識はプログラミング自体というよりも、脆弱性に対してどのようなロジックで対応するかが重要なのだと思います。私自身は日常プログラミングに携わっているわけではないので、少し難しいところがありますが、基本的な考え方は身につけたいと思います。

- 物理的セキュリティ対策

システムを物理的にどのようにして守るかというテーマです。情報機器が設置されている作業区画に対して、どのような対策を講じるかが基本的な問題ですが、近年のクラウドサービスの活用に伴い、それらのサービスでどのような対策が取られているかを問われることも増えてきています。

- ログ

セキュリティ上の問題について、検知をしたり、原因を追求したりするときに、重要な役割を担うのがログです。どのような場合にログを取得するのか、また取得する場合はどのように取得・保存するかなどが問題となります。また、ログが改ざんされないようにすることも大切になってきています。

- インシデント対応

セキュリティ上の問題、すなわちインシデントが発生した場合の、その対応方法について習得する必要があります。昨今の標的型攻撃が増えてきていることや、その対応のためのCSIRTチームの立ち上げが重要視されてきていることなどから、重要なテーマの一つだと思います。

情報処理安全確保支援士試験受験編

IT入門お役立ち情報：情報処理安全確保支援士試験受験編（その１１）

中盤：記述式試験に向けてトレーニングとして問題集を勉強しました（2）
「2020　情報処理安全確保支援士「専門知識＋午後問題」の重点対策、三好康之（著）」という問題集で、各章で理解を深めるために紹介されている午後の過去問題について、IPAのサイトからダウンロードして勉強しました。

各章で特にお勧めの過去問題は、問題を読むだけでも、それらの技術に関する基本的なことを学習することができることがわかりました。問題文の中に関連する技術の説明がされていたり、重要な語句は空欄で設問になっていたりしていますので、それらを読んだり解いたりすることで学習できるようになっています。また、問題のタイトルで、どの技術について問いているかがわかりますので、ある程度同じような技術に関する問題をまとめて解くことによって、その技術に対して重点的に学習ができます。

問題を問いたあとに、解答例と自分の解答と答え合わせをしますが、その時には、解答例のキーワードについて注目するようにしました。表現は異なっていても、必要なキーワードが含まれていれば、正解に近づくと思います。また、自分の解答全体の文意も、解答例の文意に沿っているかも合わせて確認をしました。

そして、問題に対する講評がある場合は、それも参照しました。そこには、出題者の意図や解答者に期待していたことが述べられていますので、その問題に対してどのようなことを解答するべきであったかがわかります。それらを読むと、期待する解答については、ヒントが問題文中に記載されていることが、改めてわかりますので、問題文は何度もじっくりと読み込むことが重要だと気づきました。

午後の過去問題を解いていくと、最初は問題文を読み込むのにもかなり時間がかかったり、長文の問題文を読むこと自体が少し苦痛だったりしました。しかし、問題を重ねていくとそのうち慣れてくるもので、長文の問題文を読むこと自体も苦痛ではなくなり、問題文の流れや設問との関係もある程度わかってくるようになりました。つまり、各設問で関連のある重要な問題文の箇所はどのあたりかを、目処をつけることもできるようになりました。
やはり、時間の許す限り、できるだけ多くの過去問題をこなすことが、午後の問題の対策としては、当たり前のことでしょうが、一番大切なのではないかと思います。

情報処理安全確保支援士試験受験編

IT入門お役立ち情報：情報処理安全確保支援士試験受験編（その１２）

終盤：重要分野と最新トレンドの把握・整理をしました
仕上げとして、「ポケットスタディ　情報処理安全確保支援士、村山直紀（著）」で重要分野の復習と、午後対策のスペシャルテクニックを学習しました。

出題頻度から各分野で需要なキーワードを中心に解説がされていましたので、それらキーワードについて学習するだけでも、終盤の知識の整理としては有効だと思います。また、それらキーワードに関する問題に対しての解答の仕方について、重要なポイントが鉄則として説明がされていたり、暗記すべき重要な項目が明記されていたりするので、試験対策としては役立ちます。

午後対策のスペシャルテクニックについては、IPA公表の公式解答例をもとに、その回答例に沿うような解答を目指すようになっています。出題者が期待する解答を導き出せるように、問題の内容からパターン分けをして、それぞれのパターンの問題に対して、期待されている解答のポイントが記載されています。やはり、出題頻度の高い問題パターンもあるので、それらに対する解答例を覚えておけば、解答に迷うことはないと思いました。

また、期待される解答から考えていくと、問題文には必ずそれらの解答に関連する記述が記載されていることがわかります。すなわち、問題を読んでいて、これは何か引っかかる表現だなとか、この記述は何のために書かれているのだろうかと思ったところが、結構解答のヒントになっていることも分かってきました。やはり、試験なので出題者の意図を理解することが重要であることを、改めて感じました。

最後に、IPAのサイト（https://www.ipa.go.jp/security/index.html）などから、近年話題になっている次のような技術・運用に関するガイドラインなどに目を通して、最新トレンドの把握・整理をしました。

情報セキュリティ10大脅威 2020

『高度標的型攻撃』対策に向けたシステム設計ガイド

サイバーセキュリティ経営ガイドライン

中小企業の情報セキュリティ対策ガイドライン

テレワークを行う際のセキュリティ上の注意事項

安全なウェブサイトの作り方

IPA：Web Application Firewall 読本

TLS暗号設定ガイドライン～安全なウェブサイトのために（暗号設定対策編）～

IoT セキュリティガイドライン ver 1.0 – 総務省

情報処理安全確保支援士試験受験編

IT入門お役立ち情報：情報処理安全確保支援士試験受験編（その１３）

情報処理安全確保支援士試験に合格しました
令和2年度10月試験を受験しました。そして、合格することができました。
そこで、午前・午後のそれぞれ問題ごとに、その内容と自分の解答について振り返ってみます。

- 午前Ⅰ問題

これらの問題については、私自身の準備期間も限られていたので、今回は特に試験勉強は行いませんでした。これまで、いくつかの情報処理試験を受験してきて、その度に勉強してきた箇所なので、改めて勉強する必要もないだろうと考えていました。ところが、いざ試験が始まり問題をさっと眺めていると、簡単に解けそうにないと思われる問題があり、初めは内心少し焦りました。ただし、落ち着いて問題に取り組むと、これまでの知識を応用したりして、大抵は解くことができましたし、実際に8割以上の得点も取れていました。結果的には問題なかったのですが、以前に試験を受けたのが10年以上前だったので、今回もし時間に余裕があったのであれば、少しでも復習を兼ねて勉強をしておいたほうが安心だったかもしれません。

- 午前Ⅱ問題

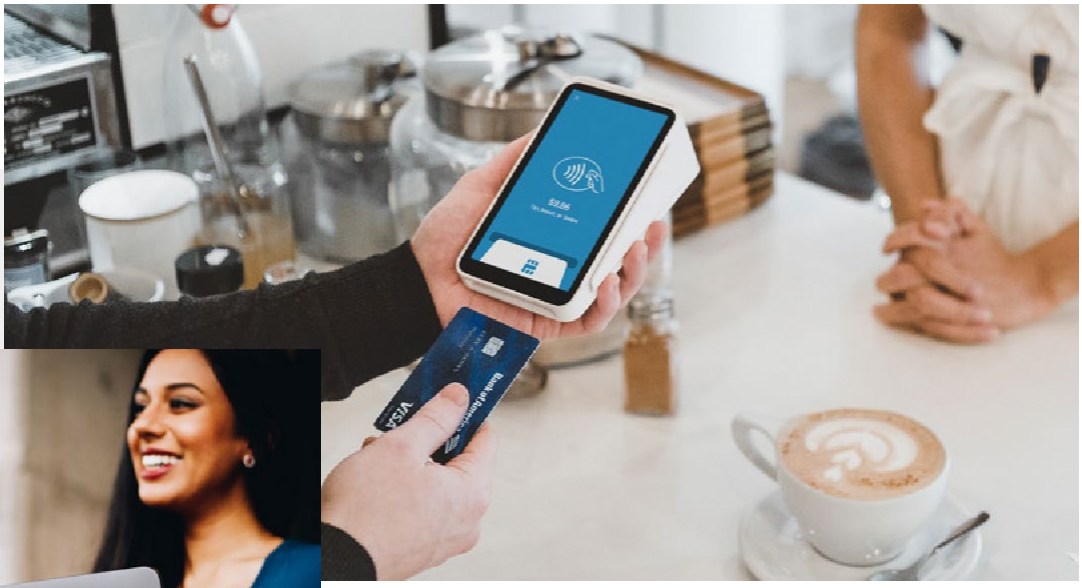
これらの問題については、参考書でじっくり時間をかけて学習しましたし、過去問題もいくつか解いていたので、およそ9割以上の得点を取ることができました。改めて実感したことですが、この領域は関連知識を習得すればするほど、得点に結びつきやすいので、比較的対策がしやすいと思います。しかし、別の言い方をすれば、学習していない問題は解答を推測することさえ難しいので、当てずっぽうで解答するしかないですね。

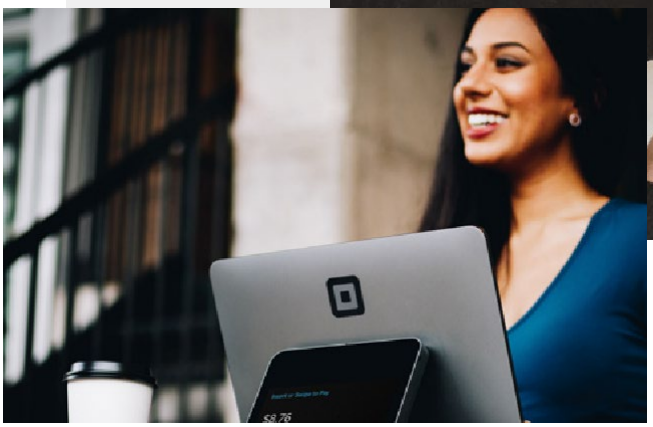
- 午後Ⅰ問題

まずは、解答する問題を3問中から2問選択しなければならないのですが、この問題選択も得点をする上では、重要だと思います。自分の得意な分野を選択するか、あるいは不得意な分野は選択しないという判断を、最初に少し時間をかけてしっかりとする必要があります。私の場合は、システム運用管理の経験が長く、システム開発については近年あまり深く経験していないので、プログラム開発をベースにした問題を除く選択をしました。
また、午後Ⅰの問題は記述式の解答で、なおかつ文字数も比較的少なめですので、キーワードを誤ったりしてしまうと得点が難しくなると思います。したがって、適切な字句を答える問題では、本文中にある字句や一般的な用語をなるべく使うようにしましたが、今回はあるプロトコル名を間違ってしまいました。これらは正しく覚えていれば、解答できたはずですので、もったいなかったと思います。しかし、結果として8割以上は得点できていましたので、今回は記述式問題の勉強を集中して実施した効果があったと思います。

- 午後Ⅱ問題

こちらも解答する問題を2問中1問選択しなければならないのですが、今回もプログラム開発の問題を避けて、クラウドサービスの問題を選択しました。予想通りに、昨今のテレワーク環境に関する題材が出題されたのですが、想定以上に問題が複雑で、何を解答として求められているのか見極めるのが難しくて、解答に苦労をしました。試験が終了した時点では、得点はかなり厳しいのではないかと思っていたのですが、結果としては8割ほど得点できていたので、なんとか出題者の意図を汲み取ることができたのではないかと思います。午後の記述式の問題については総体的に言えることですが、出題者の意図が何かということを読み取ることが、大変重要ではないかと思います。





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「**情報処理安全確保支援士試験**」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「**情報処理安全確保支援士試験**」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