

## 情報処理安全確保支援士試験の 勉強法と合格のコツ

情報処理安全確保支援士の試験は、合格率が20%前後の難関試験です。しかも、レベル1~4の4段階に区分された情報処理技術者試験のなかで、最も高い「レベル4」に位置付けられています。レベル2の基本情報技術者試験や、レベル3の応用情報技術者試験をクリアしてからこの試験を受ける人も多く、受験者のレベルが高いなかでの20%という合格率です。そう簡単には合格できません。

ではどうやって勉強すればいいのでしょうか。合格のコツはあるのでしょうか。本章では、この試験の勉強方法について解説します。

### 1 最初にやるべきこと

どこかの国の童話（だと聞きました）をご紹介します。

さて、皆さんに質問です。

木こりさんは、1日に10本の木を切ります。しかし、最近、斧の刃がボロボロになりました。その結果、1日に7本しか切れなくなりました。

それを見た旅人（あなた）は、なんと声をかけますか？



おそらく旅人（あなた）は、「木こりさん、斧を研いだらどうですか？」と声をかけることでしょう。

すると木こりさんは、「1日に7本しか切れないから忙しいんだ。斧を研いでいる時間はないよ」と言いました。

この話を初めて聞いたのが、中小企業診断士の勉強の真っ最中のときでした。まさに私が、この童話に出てくる木こりさんと同じだったのです。合格への青写真を描かず、自分の実力も理解せず、「人の3倍勉強すれば受かるだろう」と考え無謀なチャレンジをしてしまったのです。別の本でも書きましたが、その結果、莫大な勉強を6年間続けたにもかかわらず不合格を重ねました（今も合格していません）。

なんと無駄な時間を費やしたことが……。

リンカーン元アメリカ大統領は、「木を切る時間が8時間あるなら、最初の6時間は斧を研ぐ」と言ったそうです。

そうです。試験に合格するために最初にすべきことは、いきなり勉強を始めることではありません。この試験は難関で、がむしゃらにやれば合格するような甘い試験ではないのです。

最初にやるべきことは、試験を知ることです。そして、合格のコツを探し、合格までの青写真を描くことが大事です。

### 2 この試験の合格に必要なもの

p.18ページに、経験年数別の合格率を掲載しています。見ていただくとわかるように、経験年数が増えるごとに、合格率が下がっていきます。（なんてことだ！）

そして、学生と社会人の合格率を見ても、学生のほうが6%も合格率が高いのです。（なんてことだ！）

▼学生と社会人の合格率

	合格率
社会人	14.8%
学生	20.8%
合計	15.1%

出典：[https://www.ipa.go.jp/shiken/reports/nq6ept00000015c9-at/houkei\\_r06a.pdf](https://www.ipa.go.jp/shiken/reports/nq6ept00000015c9-at/houkei_r06a.pdf)

つまり、この試験に必要なものは、「①莫大な技術や知識」でも「②実務での卓越した経験」でもありません。必要なのは、「③この試験に順応した対策」です。

- ①莫大な技術や知識 ———— ✕
- ②実務での卓越した経験 ———— ✕
- ③この試験に順応した対策 ———— ○

ですから、この試験をよく知り、この試験に則した対策をするようにしましょう。

### 3 合格者の勉強法

では、合格者はどんな勉強をしているのでしょうか。経験年数が浅いほうが合格率が高いということは、画期的な勉強方法があるのではと勘違いされたかもしれませんが、さすが、合格するための勉強の流れは、次の3STEPです。計画を立て、基

APIに関するセキュリティ設計およびWAFを題材にした設問です。採点講師は、「正答率は平均的であった」とあります。ですが、Web APIの経験がない人には難しい問題だったと思います。

問1 APIセキュリティに関する次の記述を読んで、設問に答えよ。

G社は、ヘルスケアサービス新興企業である。利用者が食事、体重などを入力してそのデータを管理したり、健康リスクの判定や食事メニューのアドバイスを受けたりできるサービス（以下、サービスYという）を計画している。具体的には、クラウドサービス上にサービスY用のシステム（以下、Sシステムという）を構築して、G社が既に開発しているスマートフォン専用アプリケーションプログラム（以下、G社スマホアプリという）からアクセスする。Sシステムの要件を図1に示す。

- 要件1：利用者が入力したデータを蓄積する。
- 要件2：蓄積したデータを機械学習で学習し、その結果を利用して健康リスクの判定や食事メニューのアドバイスを利用者に提供する。
- 要件3：利用者のステータス（以下、利用者ステータスという）として、“有償利用者”と“無償利用者”を定義する。有償利用者の場合、全ての機能を利用できる。無償利用者の場合、機能の利用に一部制限がある。
- 要件4：可能な限り、既存のサービスライブラリを使って構築する。

図1 Sシステムの要件（抜粋）

G社は、Sシステムの構築をITベンダーF社に委託した。F社との協議の結果、クラウドサービスプロバイダE社のクラウドサービス上にSシステムを構築する方針にした。

【APIの設計】

Sシステムには、将来的には他社が提供するスマートフォン専用アプリケーションプログラムからもアクセスすることを想定し、RESTful API方式のAPI（以下、SシステムのAPIをS-APIという）を用意する。RESTful APIの設計原則の一つ

このあとに記載がありますが、有償利用者かどうかはパラメータstatusで管理します。設問2(4)にも関連します。

印刷機能やログ出力機能など、よく利用する機能を商品化したものです。

クラウドサービスの詳細は、表1に記載があります。

API(Application Programming Interface)は、アプリケーションやプログラムをつなぐインターフェースという意味で、異なるアプリケーションが連携できるようにする機能です。たとえば、Google Maps APIを使用することで、自分のWebサイトにGoogle Mapsの機能を埋め込むことができます。

言葉の意味は設問1で詳しく解説します。この方式を実現するために、このあと登場するJWTというトークンを使います。

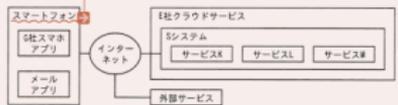
にセッション管理を行わないという性質がある。この性質をaという。

E社が提供するクラウドサービスのサービス一覧を表1に、サービスYのシステム構成を図2に、S-API呼出し時の動作概要を図3に、S-APIの仕様を表2に、Sシステムの仕様を図4に、それぞれ示す。

表1 E社が提供するクラウドサービスのサービス一覧（抜粋）

サービス名	サービス概要
サービスK	APIゲートウェイサービスである。当該サービスは、APIへのリクエストを受信し、その内容に基づき、サービスを呼び出す。
サービスL	イベント駆動型のコンピューティングサービスである。サービスKからの呼出しがあったとき、又は指定された日時に、事前に定義された処理を実行する。また、外部サービスと連携する。
サービスM	マネージド型のデータベースサービスである。
サービスN	マネージド型のWAFサービスである。サービスKが受信したAPIへのリクエストを検査して、許可・検知・遮断を行う。

注記 Sシステムの構築時点では、サービスNを導入しない計画である。



注記 サービスK及びサービスLからインターネットへの通信は許可されている。

図2 サービスYのシステム構成

G社スマホアプリからS-APIが呼び出された場合の動作は次のとおりである。

- S-APIが呼び出されると、S-APIへのリクエストは、サービスKが一元的に受ける。サービスKは、そのリクエスト内容に基づき、サービスLを呼び出す。サービスLは、事前に定義された処理を実行してレスポンスをサービスKに返し、サービスKは、G社スマホアプリにレスポンスを返す。
- サービスLでは、データベースのデータの読み取り又は書き込みが必要な場合は、事前に定義された処理からサービスMを呼び出す。

図3 S-API呼出し時の動作概要（抜粋）

APIの作成や管理を、サービスとして提供します。実際のサービス例としてAmazon API Gatewayなどがあります。

APIへの接続などのイベントが発生した場合に、任意の処理を実行できる仕組みを提供します。実際のサービス例として、Amazon Lambdaなどがあります。

データベース機能を提供するサービスです。AWSの場合、Amazon RDSがあります。

WAF(Web Application Firewall)をサービスとして提供する仕組みです。AWS WAFなどがあります。

利用者のスマートフォンです。ここから、インターネットを経由してSシステムにアクセスします。

なぜサービスKかという点、表1より、APIゲートウェイサービスの機能がサービスKだからです。

あとに出てくる共通ジョーブルPのことです。

#### 設問4 (1)

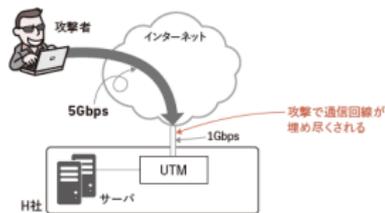
本文中の下線⑤について、利用する外部のサービスを、20字以内で具体的に答えよ。

#### 解説

問題文の該当部分は以下のとおりです。

まず、通信回線については、DDoS攻撃で大量のトラフィックが発生すると、使えなくなる。これについては、通信回線の帯域を大きくするという方法のほか、⑤外部のサービスを利用するという方法があることが分かった。

この部分の攻撃について、以下の図で説明します。たとえば、H社が1Gbpsのインターネット回線契約を結んでいたとします。ここに、攻撃者からの5Gbpsのトラフィックがきたらどうなるでしょうか。1Gbpsの回線は埋め尽くされ、正常な通信ができなくなります。



#### ▲DDoS攻撃により回線が使用不能になる

対策としては、問題文に記載があるように、「通信回線の帯域を大きくするという方法」があります。つまり、回線帯域をたとえば10Gbpsにします。ただし、回線帯域を大きくすると、高額な費用がかかります。

この設問では、それ以外の対策を考えます。



でも、H社の通信回線を埋め尽くされたら、対策なんてできませんよね

はい。回線を埋め尽くされていますから、自社でDDoS対策の装置を置いたとしても有効な対策をすることは難しいでしょう。

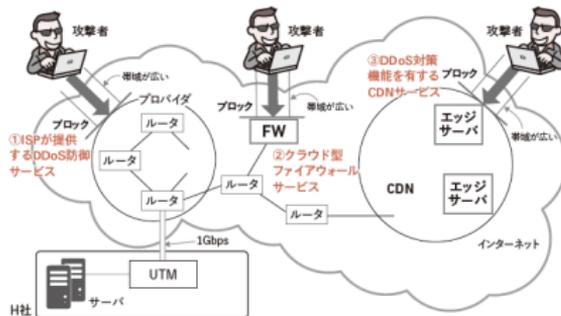
ではどうするかというと、下線⑤にあるように「外部のサービス」を利用します。DDoS対策の考え方は、H社に大量のパケットが届く前に防御することです。そのためには、外部のクラウドサービスやISPのサービスを利用します。

解答例を見てみましょう。

#### 解答例：

- DDoS対策機能を有するCDNサービス (19字)
- クラウド型ファイアウォールサービス (17字)
- ISPが提供するDDoS防御サービス (18字)

上記の解答例のイメージを以下の図に示します。プロバイダが持っている回線帯域は1Gbpsどころではなく、100Gbpsや200Gbpsという帯域を持っています。その帯域を埋め尽くすことは簡単ではありません。そこで、広い帯域を持つISPやクラウドサービス、CDNサービスにて攻撃トラフィックを拒否してもらうのです。そうすれば、H社の1Gbpsの回線帯域まで攻撃トラフィックが届くことはありません。



#### ▲DDoS攻撃に対する外部のサービス

では、解答例を順に確認していきます。

参考 ディレクトリに実行権限がないとファイルにアクセスできないのか、実際にやってみました

解説で述べたことを実際に試してみました。

- ① webappuserでログインし、ディレクトリのオーナーはwebappuserで、パーミッションを774に設定。

```
[webappuser@xxx log]$ pwd
/var/log ← 現在のディレクトリは/var/log
[webappuser@xxx log]$ chmod 774 serverlog ← serverlogディレクトリのパーミッションを774に設定
[webappuser@xxx log]$ ls -la | grep serverlog ← パーミッションの確認
drwxr-xr-x. 2 webappuser webappuser 23 Oct 27 01:59 serverlog
```

アクセス権は、`rwX (=7)`、`rwX (=7)`、`r-- (=4)`であり、その他のグループにいるシステム運用担当者 (operator) には、ディレクトリの読み込み権限があるように見えます。

- ② 配下にあるerror.logファイルのアクセス権を664に設定。

```
[webappuser@xxx log]$ chmod 664 ./serverlog/error.log ← 配下にあるerror.logファイルのアクセス権を664に設定
[webappuser@xxx log]$ ls -la serverlog ← error.logファイルのパーミッションの確認
-rw-rw-r--. 1 webappuser webappuser 132 Oct 27 01:59 error.log
```

- ③ operatorでログインし、serverlogディレクトリに移動しようとしても、Permission deniedのエラーになります。また、ファイルを直接開こうとしてもエラーです。つまり、ファイルへのアクセス権がありません。

```
[operator@xxx log]$ pwd
/var/log ← 現在のディレクトリは/var/log
[operator@xxx log]$ cd serverlog/ ← serverlogディレクトリに移動
bash: cd: serverlog/: Permission denied
[operator@xxx log]$ cat /var/log/serverlog/error.log ← 配下のファイルをcatで開く
cat: /var/log/serverlog/error.log: Permission denied
```

- ④ webappuserでログインし、ディレクトリのパーミッションを775に設定します。

```
[webappuser@xxx log]$ chmod 775 serverlog ← serverlogディレクトリのパーミッションを775に設定
[webappuser@xxx log]$ ls -ld serverlog ← パーミッションの確認
drwxr-xr-x. 2 webappuser webappuser 23 Oct 27 01:59 serverlog
```

`rwX (=7)`、`rwX (=7)`、`r-x (=5)`であり、その他のグループにいるシステム運用担当者 (operator) にはディレクトリに対する実行権限も付与されました。

- ⑤ operatorでログインします。serverlogディレクトリに移動したり、ファイルの内容を表示できます。

```
[operator@xxx log]$ cd serverlog/ ← serverlogディレクトリに移動
[operator@xxx serverlog]$ ls ← エラーは出ず、lsコマンドでディレクトリの中身も確認可能
error.log
[operator@xxx serverlog]$ cat error.log ← 配下のファイルを開くことも可能
aaaaaaaaaaaaaaaaaaaaaaaaaaaa (ファイルの中身)
```

つまり、ファイルを読み取るには、ファイルへの読み取り権限だけでなく、ディレクトリへの実行権限も必要であることがわかりました。

設問 2 (4)

図4中の  に入れる適切な字句を答えよ。

解説

空欄fは、E氏が指摘したソースコードの修正内容が問われています。どんな指摘かは、空欄fのソースコードを見てみましょう。

修正前	5: MessageDigest mdObj = MessageDigest.getInstance("SHA-1");
修正後	5: MessageDigest mdObj = MessageDigest.getInstance(" <input type="text" value="f"/> ");

ここで、MessageDigestという文字があることから、ハッシュ関数に関する以下の指摘だと想定できます。

E氏は、図3のソースコードについて、次のように指摘した。

- ・パスワードからハッシュ値を得るためのハッシュ関数が、表1の要件を満たしていない。

続いて、表1の要件は何かというと、表1の項番19にハッシュ関数に関する要件があります。

19	パスワードの保存	パスワードは、CRYPTREC暗号リスト(令和5年3月30日版)の電子政府推奨暗号リストに記載されているハッシュ関数でハッシュ化してDBに保存する。
----	----------	--

CRYPTREC暗号リストに記載されているハッシュ関数は次のとおりです。

設問	IPAの解答例・解答の要点	予想 配点
設問1	a ステートレス	3
	b 500	3
設問2	(1) データ JWT ヘッダ内のalgに指定された値 内容 NONEでないことを検証する。	2
	(2) JWTに含まれる利用者IDがmidの値と一致するかどうかを検証する処理	3
	(3) c 共通モジュールP	5
	(4) d 連続失敗回数がかきい値を超えたらアカウントをロックする 処理	3
	(5)	5
設問3	(1) テストサーバのindex.htmlへのアクセスを記録し、確認する仕組み	5
	(2) e Header	3
	(3) f Header	3
	(4) ・YW(jj)[nN][dD][iI]YW ・YW(jj)(nN)(dD)(iI)YW	5
(4)	利点 誤検知による遮断を防ぐことができる。	5
	内容 アラートを受信したら攻撃かどうかを精査する。	5
※予想配点は著者による		合計 50

### IPAの出題趣旨

多くのシステムにおいて、スマートフォンのアプリケーションプログラムを利用したAPI連携が行われる中、APIの脆弱性を作り込むケースが増えている。

本問では、APIセキュリティを題材として、指摘された脆弱性に対して対策を立案する能力を問う。

### IPAの採点講評

問1では、APIセキュリティを題材に、セキュリティ設計及び脆弱性対応について出題した。全体として正答率は平均的であった。

設問2(2)は、正答率がやや低かった。JSON Web Token (JWT) 改ざんにおける検証方法を問うたが、既に実装されている対策を解答するなど、脆弱性を正しく理解していないと思われる解答が散見された。図4に示す仕様と表3に示す脆弱性を正しく理解してほしい。

設問3(1)は、正答率がやや低かった。脆弱性の存在を判断するための仕組みについて問うたが、図6に示す攻撃の流れに合っていない解答が散見された。脆弱性対策では、脆弱性を悪用する攻撃の流れの理解が重要であることから、正確に理解してほしい。

設問3(4)の利点については、正答率が高かった。WAFの利点と課題は正確に理解していると思われる。セキュリティ施策は導入前にトレードオフを検討してほしい。

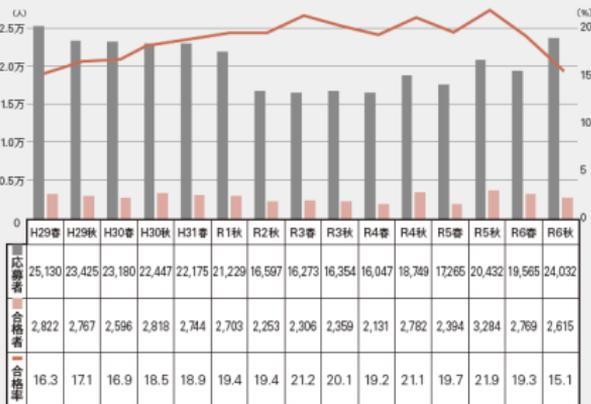
### 出典

『令和6年度 春期 情報処理安全確保支援士試験 解答例』  
[https://www.ipa.go.jp/shiken/mondai-kaietu/m420bm000000afqx-att/2024/06h\\_sc\\_gm\\_ana.pdf](https://www.ipa.go.jp/shiken/mondai-kaietu/m420bm000000afqx-att/2024/06h_sc_gm_ana.pdf)  
 『令和6年度 春期 情報処理安全確保支援士試験 採点講評』  
[https://www.ipa.go.jp/shiken/mondai-kaietu/m420bm000000afqx-att/2024/06h\\_sc\\_gm\\_crmt.pdf](https://www.ipa.go.jp/shiken/mondai-kaietu/m420bm000000afqx-att/2024/06h_sc_gm_crmt.pdf)

# データで見る 情報処理安全確保支援士

その2

## 応募者・合格者・合格率の推移



令和6年度は応募者数が増えました。  
でも、秋期の合格率がとても低いんですね。

令和6年度を通して、応募者の平均年齢は38.2歳、  
合格者の平均年齢は34.0歳でした。  
最年少合格者は14歳(4人)、最年長合格者は66歳(3人)です。



受験者は10歳以下(!)から75歳以上  
までと、幅広い層に渡っています。