応用情報技術者

午前対策問題集

無料体験入学者用

TAC

はじめに

この問題集は, 弊社刊「応用情報技術者試験対策テキストⅠ・Ⅱ・Ⅲ」の各学習項目に対応させて作成された問題集です。

本書は，過去の情報処理技術者試験において出題された午前問題で構成されています。実際の応用情報技術者試験の出題内容に合わせ，テーマごとに問題を集めて掲載しています。

本書では，日本産業規格をはじめとした各種の規格や基準に関する問題も掲載しています。規格や基準の改訂に伴って旧版となった規格や基準に関する問題も含まれますが，これらは最新版の規格でも通用する普遍的な概念や技法を問う問題であり，試験対策として問題なく活用できます。

試験に合格するためには，テキストによる知識のインプットだけではなく, 問題演習によるアウトプット(力試し)が非常に重要になります。問題を解き，間違えた問題のジャンルについては学習しなおして再度挑戦するという学習サイクルを身に付けましょう。

本書が，応用情報技術者試験の合格のお役に立てることを願ってやみません。

TAC情報処理講座

目　次

〔出典表記について〕

本書では，各問題の出典を問番号の下に略記形式で記載しています。

試験区分は以下の表記を用いています。

AP	応用情報技術者
SW	ソフトウェア開発技術者 (旧)
FE	基本情報技術者
IP	IT パスポート
AD	初級システムアドミニストレータ (旧)
AU	システム監査技術者
SD	上級システムアドミニストレータ (旧)
ST	IT ストラテジスト
DB	データベーススペシャリスト
NW	ネットワークスペシャリスト
SC	情報セキュリティスペシャリスト
PM	プロジェクトマネージャ
SM	IT サービスマネージャ
SA	システムアーキテクト

区分名の下には，年度と春／秋の別，問番号を記しています。たとえば“H22 秋問 54”ならば平成 22 年春期の問 54，“R01 秋問 2”ならば令和元年秋期の問 2 になります。また，高度区分は午前Ⅱの問番号を記しています。

問題編

4. 情報セキュリティ

問259
AP
H24秋問40

完全性を脅かす攻撃はどれか。

ア　Web ページの改ざん
イ　システム内に保管されているデータの持出しを目的とした不正コピー
ウ　システムを過負荷状態にする DoS 攻撃
エ　通信内容の盗聴

問260
AP
R1秋問40

JIS Q 27000:2019（情報セキュリティマネジメントシステム－用語）では，情報セキュリティは主に三つの特性を維持することとされている。それらのうちの二つは機密性と完全性である。残りの一つはどれか。

ア　可用性　　イ　効率性　　ウ　保守性　　エ　有効性

問261
AP
R3秋問39

JIS Q 27000:2019（情報セキュリティマネジメントシステム－用語）において定義されている情報セキュリティの特性に関する説明のうち，否認防止の特性に関するものはどれか。

ア　ある利用者があるシステムを利用したという事実が証明可能である。
イ　認可された利用者が要求したときにアクセスが可能である。
ウ　認可された利用者に対してだけ，情報を使用させる又は開示する。
エ　利用者の行動と意図した結果とが一貫性をもつ。

問262
AP
H25秋問40

ISMSにおいて定義することが求められている情報セキュリティ基本方針に関する記述のうち，適切なものはどれか。

ア　重要な基本方針を定めた機密文書であり，社内の関係者以外の目に触れないようにする。

イ　情報セキュリティの基本方針を述べたものであり，ビジネス環境や技術が変化しても変更してはならない。

ウ　情報セキュリティのための経営陣の方向性及び支持を規定する。

エ　特定のシステムについてリスク分析を行い，そのセキュリティ対策とシステム運用の詳細を記述する。

問263
AP
H23春問43

あるコンピュータセンタでは，インシデントを六つのタイプに分類した。

Scan：　プローブ，スキャン，そのほかの不審なアクセス

Abuse：　サーバプログラムの機能を悪用した不正中継

Forged：　送信ヘッダを詐称した電子メールの配送

Intrusion：システムへの侵入

DoS：　サービス運用妨害につながる攻撃

Other：　その他

このとき，次の三つのインシデントに対するタイプの組合せのうち，適切なものはどれか。

インシデント1：ワームの攻撃が試みられた形跡があるが，侵入されていない。

インシデント2：ネットワークの輻輳（ふくそう）による妨害を受けた。

インシデント3：DoS用の踏み台プログラムがシステムに設置されていた。

	インシデント1	インシデント2	インシデント3
ア	Abuse	DoS	Intrusion
イ	Abuse	Forged	DoS
ウ	Scan	DoS	Intrusion
エ	Scan	Forged	DoS

問264
AP
R2問42

暗号方式に関する記述のうち，適切なものはどれか。

ア　AES は公開鍵暗号方式，RSA は共通鍵暗号方式の一種である。

イ　共通鍵暗号方式では，暗号化及び復号に同一の鍵を使用する。

ウ　公開鍵暗号方式を通信内容の秘匿に使用する場合は，暗号化に使用する鍵を秘密にして，復号に使用する鍵を公開する。

エ　ディジタル署名に公開鍵暗号方式が使用されることはなく，共通鍵暗号方式が使用される。

問265
AP
H30秋問37

楕円曲線暗号に関する記述のうち，適切なものはどれか。

ア　AES に代わる共通鍵暗号方式として NIST が標準化している。

イ　共通鍵暗号方式であり，ディジタル署名にも利用されている。

ウ　公開鍵暗号方式であり，TLS にも利用されている。

エ　素因数分解問題の困難性を利用している。

問266
AP
H25春問39

公開鍵暗号を使って n 人が相互に通信する場合，全体で何個の異なる鍵が必要になるか。ここで，一組の公開鍵と秘密鍵は 2 個と数える。

ア　$n+1$　　イ　$2n$　　ウ　$\dfrac{n(n-1)}{2}$　　エ　$\log_2 n$

問267
AP
H29秋問39

パスワードに使用できる文字の種類の数を M，パスワードの文字数を n とするとき，設定できるパスワードの理論的な総数を求める数式はどれか。

ア　M^n　　イ　$\dfrac{M!}{(M-n)!}$

ウ　$\dfrac{M!}{n!\,(M-n)!}$　　エ　$\dfrac{(M+n-1)!}{n!\,(M-1)!}$

問268
AP
H30秋問42

ブルートフォース攻撃に該当するものはどれか。

ア　Web ブラウザと Web サーバの間の通信で，認証が成功してセッションが開始されているときに，Cookie などのセッション情報を盗む。

イ　コンピュータへのキー入力を全て記録して外部に送信する。

ウ　使用可能な文字のあらゆる組合せをそれぞれパスワードとして，繰り返しログインを試みる。

エ　正当な利用者のログインシーケンスを盗聴者が記録してサーバに送信する。

問269
AP
H27春問39

パスワードリスト攻撃に該当するものはどれか。

ア　一般的な単語や人名からパスワードのリストを作成し，インターネットバンキングへのログインを試行する。

イ　想定され得るパスワードとそのハッシュ値との対のリストを用いて，入手したハッシュ値からパスワードを効率的に解析する。

ウ　どこかの Web サイトから流出した利用者 ID とパスワードのリストを用いて，他の Web サイトに対してログインを試行する。

エ　ピクチャパスワードの入力を録画してリスト化しておき，それを利用することでタブレット端末へのログインを試行する。

問270
AP
R3春問39

リスクベース認証の特徴はどれか。

ア　いかなる利用条件でのアクセスの要求においても，ハードウェアトークンとパスワードを併用するなど，常に二つの認証方式を併用することによって，不正アクセスに対する安全性を高める。

イ　いかなる利用条件でのアクセスの要求においても認証方法を変更せずに，同一の手順によって普段どおりにシステムにアクセスできるようにし，可用性を高める。

ウ　普段と異なる利用条件でのアクセスと判断した場合には，追加の本人認証をすることによって，不正アクセスに対する安全性を高める。

エ　利用者が認証情報を忘れ，かつ，Web ブラウザに保存しているパスワード情報を使用できないリスクを想定して，緊急と判断した場合には，認証情報を入力せずに，利用者は普段どおりにシステムを利用できるようにし，可用性を高める。

問271
AP
R4春問42

パスワードクラック手法の一種である，レインボー攻撃に該当するものはどれか。

ア　何らかの方法で事前に利用者 ID と平文のパスワードのリストを入手しておき，複数のシステム間で使い回されている利用者 ID とパスワードの組みを狙って，ログインを試行する。

イ　パスワードに成り得る文字列の全てを用いて，総当たりでログインを試行する。

ウ　平文のパスワードとハッシュ値をチェーンによって管理するテーブルを準備しておき，それを用いて，不正に入手したハッシュ値からパスワードを解読する。

エ　利用者の誕生日や電話番号などの個人情報を言葉巧みに聞き出して，パスワードを類推する。

問272
AP
H24秋問36

シングルサインオンの説明のうち，適切なものはどれか。

ア　クッキーを使ったシングルサインオンの場合，サーバごとの認証情報を含んだクッキーをクライアントで生成し，各サーバ上で保存，管理する。

イ　クッキーを使ったシングルサインオンの場合，認証対象のサーバを，異なるインターネットドメインに配置する必要がある。

ウ　リバースプロキシを使ったシングルサインオンの場合，認証対象の Web サーバを，異なるインターネットドメインに配置する必要がある。

エ　リバースプロキシを使ったシングルサインオンの場合，利用者認証においてパスワードの代わりにディジタル証明書を用いることができる。

問273
AP
R4春問38

チャレンジレスポンス認証方式に該当するものはどれか。

ア　固定パスワードを，TLS による暗号通信を使い，クライアントからサーバに送信して，サーバで検証する。

イ　端末のシリアル番号を，クライアントで秘密鍵を使って暗号化し，サーバに送信して，サーバで検証する。

ウ　トークンという機器が自動的に表示する，認証のたびに異なる数字列をパスワードとしてサーバに送信して，サーバで検証する。

エ　利用者が入力したパスワードと，サーバから受け取ったランダムなデータとをクライアントで演算し，その結果をサーバに送信して，サーバで検証する。

問274
AP
H28秋問41

アクセス制御に用いる認証デバイスの特徴に関する記述のうち，適切なものはどれか。

ア　USB メモリにディジタル証明書を組み込み，認証デバイスとする場合は，利用する PC の MAC アドレスを組み込む必要がある。

イ　成人には虹彩の経年変化がなく，虹彩認証では，認証デバイスでのパターン更新がほとんど不要である。

ウ　静電容量方式の指紋認証デバイスでは，LED 照明を設置した室内において正常に認証できなくなる可能性がある。

エ　認証に利用する接触型 IC カードは，カード内のコイルの誘導起電力を利用している。

問275
AP
H24春問38

ディジタル署名などに用いるハッシュ関数の特徴はどれか。

ア　同じメッセージダイジェストを出力する異なる二つのメッセージが，容易に求められる。

イ　メッセージが異なっていても，メッセージダイジェストは同じである。

ウ　メッセージダイジェストからメッセージを復元することは困難である。

エ　メッセージダイジェストの長さはメッセージの長さによって異なる。

問276
AP
H24秋問38

手順に示すハッシュ関数とメッセージダイジェストの処理を行うことで得られるセキュリティ上の効果はどれか。ここで，メッセージダイジェストは安全な方法で保護され，改ざんや破壊がされていないものとする。

〔手順〕

(1) 送信者 A は，電子メールの本文からハッシュ関数を用いて，メッセージダイジェストを作成する。電子メールの本文とメッセージダイジェストを別々に受信者 B に送信する。

(2) 受信者 B は受信した電子メールの本文からハッシュ関数を用いて，メッセージダイジェストを作成する。その作成したメッセージダイジェストと，受信したメッセージダイジェストを比較する。

ア　電子メールの改ざんの有無の確認
イ　電子メールの誤送信の防止
ウ　電子メールの送達確認
エ　電子メールの盗聴の防止

問277
AP
H26秋問36

ディジタル署名に用いる鍵の組合せのうち，適切なものはどれか。

	ディジタル署名の作成に用いる鍵	ディジタル署名の検証に用いる鍵
ア	共通鍵	秘密鍵
イ	公開鍵	秘密鍵
ウ	秘密鍵	共通鍵
エ	秘密鍵	公開鍵

問278
AP
H24春問40

ディジタル署名における署名鍵の用い方と，ディジタル署名を行う目的のうち，適切なものはどれか。

ア　受信者が署名鍵を使って，暗号文を元のメッセージに戻すことができるようにする。

イ　送信者が固定文字列を付加したメッセージを，署名鍵を使って暗号化することによって，受信者がメッセージの改ざん部位を特定できるようにする。

ウ　送信者が署名鍵を使って署名を作成し，それをメッセージに付加することによって，受信者が送信者を確認できるようにする。

エ　送信者が署名鍵を使ってメッセージを暗号化することによって，メッセージの内容を関係者以外に分からないようにする。

問279
AP
H27秋問37

手順に示す処理を行ったとき，検証できることはどれか。

〔手順〕

(1) 送信者 A はファイルのハッシュ値を計算して，信頼できる第三者機関に送信する。

(2) 第三者機関は，信頼できる日時を保持しており，受信したハッシュ値とその受信日時を結合し（結合データ），そのディジタル署名を生成し，ディジタル署名と結合データの組（ディジタル署名済みの結合データ）を送信者 A に返信する。

(3) 送信者 A はファイルと第三者機関から送られてきたディジタル署名済みの結合データを受信者 B に送信する。

(4) 受信者 B は第三者機関のディジタル署名を確認し，ファイルから計算したハッシュ値と，ディジタル署名済みの結合データから取り出されたハッシュ値を照合する。そして，結合データから取り出された日時を確認する。

ア 当該日時に受信者 B にファイルが到達したこと

イ 当該日時に送信者 A が受信者 B にファイルを送信したこと

ウ 当該日時にファイルが作成されたこと

エ 当該日時にファイルが存在し，それ以降改ざんされていないこと

問280
AP
H26春問39

認証局が侵入され，攻撃者によって不正な Web サイト用のディジタル証明書が複数発行されたおそれがある。どのディジタル証明書が不正に発行されたものか分からない場合，誤って不正に発行されたディジタル証明書を用いた Web サイトにアクセスしないために利用者側で実施すべき対策はどれか。

ア Web サイトのディジタル証明書の有効期限が過ぎている場合だけアクセスを中止する。

イ Web サイトへのアクセスログを確認し，ドメインが Whois データベースに登録されていない場合だけアクセスする。

ウ 当該認証局の CP（Certificate Policy）の内容を確認し，セキュリティを考慮している内容である場合だけアクセスする。

エ ブラウザで当該認証局を信頼していない状態に設定し，Web サイトのディジタル証明書に関するエラーが出た場合はアクセスを中止する。

問281
AP
R2問36

認証局が発行する CRL に関する記述のうち，適切なものはどれか。

ア　CRL には，失効したディジタル証明書に対応する秘密鍵が登録される。

イ　CRL には，有効期限内のディジタル証明書のうち失効したディジタル証明書と失効した日時の対応が提示される。

ウ　CRL は，鍵の漏えい，失効申請の状況をリアルタイムに反映するプロトコルである。

エ　有効期限切れで失効したディジタル証明書は，所有者が新たなディジタル証明書を取得するまでの間，CRL に登録される。

問282
AP
R4秋問38

デジタル証明書が失効しているかどうかをオンラインで確認するためのプロトコルはどれか。

ア　CHAP　　イ　LDAP　　ウ　OCSP　　エ　SNMP

問283
AP
R2問38

OCSP クライアントと OCSP レスポンダとの通信に関する記述のうち，適切なものはどれか。

ア　ディジタル証明書全体を OCSP レスポンダに送信し，その応答でディジタル証明書の有効性を確認する。

イ　ディジタル証明書全体を OCSP レスポンダに送信し，その応答としてタイムスタンプトークンの発行を受ける。

ウ　ディジタル証明書のシリアル番号，証明書発行者の識別名（DN）のハッシュ値などを OCSP レスポンダに送信し，その応答でディジタル証明書の有効性を確認する。

エ　ディジタル証明書のシリアル番号，証明書発行者の識別名（DN）のハッシュ値などを OCSP レスポンダに送信し，その応答としてタイムスタンプトークンの発行を受ける。

問284
AP
H27春問43

サーバにバックドアを作り，サーバ内で侵入の痕跡を隠蔽するなどの機能がパッケージ化された不正なプログラムやツールはどれか。

ア　RFID　　イ　rootkit　　ウ　TKIP　　エ　web beacon

問285
AP
H31春問36

情報セキュリティにおけるエクスプロイトコードの説明はどれか。

ア　同じセキュリティ機能をもつ製品に乗り換える場合に，CSV 形式など他の製品に取り込むことができる形式でファイルを出力するプログラム

イ　コンピュータに接続されたハードディスクなどの外部記憶装置や，その中に保存されている暗号化されたファイルなどを閲覧，管理するソフトウェア

ウ　セキュリティ製品を設計する際の早い段階から実際に動作する試作品を作成し，それに対する利用者の反応を見ながら徐々に完成に近づける開発手法

エ　ソフトウェアやハードウェアの脆弱性を検査するために作成されたプログラム

問286
AP
R1秋問42

エクスプロイトキットの説明はどれか。

ア　JPEG データを読み込んで表示する機能をもつ製品に対して，セキュリティ上の問題を発生させる可能性のある値を含んだ JPEG データを読み込ませることによって，脆弱性がないかをテストするツール

イ　JVN などに掲載された脆弱性情報の中に，利用者自身が PC 又はサーバにインストールした製品に関する情報が含まれているかどうかを確認するツール

ウ　OS やアプリケーションソフトウェアの脆弱性を悪用して攻撃するツール

エ　Web サイトのアクセスログから，Web サイトの脆弱性を悪用した攻撃を検出するツール

解答・解説編

テザリング：スマートフォンなどをモバイルルータとして機能させることで，PCや他の情報端末のインターネット接続を可能にする機能

フォールバック：縮退運転。障害発生の際に，機能や性能を落としたシステム運用に切り替える動作の総称。通信サービスにおいては，LTEなどのパケット通信網に障害が発生した際に3Gなどの回線交換方式へ切り替えることを“回線交換フォールバック(CSフォールバック)”と呼ぶ

ローミング：無線LANやモバイル通信サービスにおいて，ある通信事業者のサービス加入者が，別の事業者のサービスにも接続できるようにする技術

4. 情報セキュリティ

問259　ア

セキュリティにおける完全性(インテグリティ)とは，

「資産(情報)の内容が正確な状態である」

ことを保護する特性である。Webページの改ざんのように「不正に内容を変更する」攻撃は，完全性を脅かす脅威の一つである。

イ，エ　機密性を脅かす攻撃である。

ウ　可用性を脅かす攻撃である。

問260　ア

情報セキュリティには，主要な特性として機密性(Confidentiality)，完全性(Integrity)，可用性(Availability)の3要素があり，それぞれの頭文字をとってCIAと呼ばれることもある。この3要素に加えるオプション特性として，真正性(Authenticity)や信頼性(Reliability)などがある。それぞれの概要を，JIS Q 27000での定義とともに次に示す。

表　情報セキュリティの主な特性

特性	JIS Q 27000での定義	内容
機密性 (Confidentiality)	認可されていない個人，エンティティ又はプロセスに対して，情報を使用させず，また，開示しない特性	アクセスが必要であると認めた存在以外には，情報へのアクセスを許さないこと
完全性 (Integrity)	正確さ及び完全さの特性	情報の内容が矛盾しておらず，整合性を保っていること
可用性 (Availability)	認可されたエンティティが要求したときに，アクセス及び使用が可能である特性	正当な利用者が情報を使用したいときに使用できること
真正性 (Authenticity)	エンティティは，それが主張するとおりのものであるという特性	利用者や記録作成者などの，相手の身元主張の正当性が確保できる状態にしなければならないこと

信頼性 (Reliability)	意図する行動と結果とが一貫しているという特性	業務プロセスやシステムが不具合なく正常に機能し，矛盾したり，異常な結果に終わることが無い状態にしなければならないこと

問261　ア

JIS Q 27000 では，否認防止について

> 主張された事象又は処置の発生，及びそれを引き起こしたエンティティを証明する能力。

という定義を行っている。すなわち,ある事象(出来事)が起きたこと,及びその事象が誰によって引き起こされたのかを証明できるということが，否認防止の特性に該当する。

選択肢アは,「ある利用者があるシステムを利用した」という事実について証明することを述べているので，否認防止に該当する。

イ　可用性に関する記述である。
ウ　機密性に関する記述である。
エ　信頼性に関する記述である。

問262　ウ

ISMSの実践規範であるJIS Q 27002では，基本方針の目的について

「情報セキュリティのための経営陣の方向性及び支持を，
　事業上の要求事項，関連する法令及び規制に従って規定するため」

と記している。

ア　機密文書とすべきではない。経営陣によって承認され，全従業員に公表・通知すべきである。
イ　定期的に，また影響を及ぼす変化があった場合に，見直すべきである。
エ　セキュリティ対策やシステム運用の詳細を記述したものを，情報セキュリティの実施規程あるいは運用規程という。また，ISMSでは特定のシステムではなく，組織体が保有する情報資産を保護対象としてリスク分析を行い，情報セキュリティポリシを定める。

問263　ウ

ここで挙げられている分類は，コンピュータインシデントに関する支援活動を行う団体であるJPCERT/CC(JPCERTコーディネーションセンター)が，インシデント報告を分類するさいに用いる定義の一つに準拠している。各タイプについて具体的に説明すると次のようになる。

①Scan：プローブ，スキャン，そのほかの不審なアクセス
・弱点探索(サーバプログラムのバージョンのチェックなど)
・侵入行為の試み(未遂に終わったもの)
・ワームの感染の試み(未遂に終わったもの)

②Abuse：サーバプログラムの機能を使用した不正中継など
・管理者が意図しないような，メールサーバやプロキシサーバなどの第三者による使用
③Forged：送信ヘッダを詐称した電子メールの配送
・From:欄などの詐称
④Intrusion：システムへの侵入
・システムへの侵入や改ざん
・DDoS用プログラムの設置（踏み台）
・ワームの感染
⑤DoS(Denial of Service)：サービス運用妨害につながる攻撃
・ネットワークの輻輳（混雑）による妨害
・サーバプログラムの停止
・OSの停止や再起動
⑥Other：その他
・SPAMメールの受信
・コンピュータウィルスの感染

以上に従うと，問題で示された各インシデントは次のように分類できる。

インシデント1 …「ワームの感染の試み（未遂に終わったもの）」といえるので，Scanに該当する。
インシデント2 …「ネットワークの輻輳（混雑）による妨害」といえるので，DoSに該当する。
インシデント3 …「DDoS用プログラムの設置（踏み台）」といえるので，Intrusionに該当する。

問264　イ

共通鍵暗号方式は，暗号化と復号に同じ鍵を用いるのが特徴である。鍵の管理が難しいのが欠点であるが，公開鍵暗号方式と比較して暗号化や復号の処理が高速であるという利点がある。

ア　AESはDESの後継として位置付けられる共通鍵暗号方式の標準暗号規格であり，RSAは公開鍵暗号方式の代表例である。
ウ　公開鍵暗号方式を通信内容の秘匿に使用する場合，暗号化鍵を公開して復号鍵を秘密にする。
エ　ディジタル署名は，公開鍵暗号方式を利用して実現されていることが多い。

問265　ウ

楕円曲線暗号は，楕円曲線という3次元曲線上にある特殊な演算を用いて暗号化する公開鍵暗号方式の暗号規格である。RSA暗号に比べると鍵のサイズが小さく，高速処理が可能という特徴をもつ。

エ　素因数分解問題の困難性を利用しているのは，RSAである。

問266　イ

公開鍵暗号方式では，通信を行う各主体（利用者）ごとに，それぞれ秘密鍵と公開鍵のペア

を用意する。したがって，n 人の間で相互に暗号を使って通信する場合には，必要な鍵の数は 2n となる。

問267　ア

パスワードでは，文字の並びも区別の要素となる。たとえば，“ABA”と“BAA”は別々の文字列として区別される。つまり，2種類の文字を3個並べて作られるパスワードの個数は，

2×2×2　← 2を3回掛ける

と求められる。

よって，M種類の文字をn個並べて作られるパスワードの個数は，

M×M×…×M　← Mをn回掛ける

$= M^n$

となる。

問268　ウ

ブルートフォース攻撃は，「総当たり」で暗号文やパスワードなどを解読する攻撃手法のことである。ログイン時のユーザ認証において，パスワードの文字列の組合せをすべて試すために，何度もログインを試みる行為は，パスワードクラッキングにおけるブルートフォース攻撃に該当する。

ア　セッションハイジャックに関する記述である。

イ　キーロガーに関する記述である。キーロガーは，パスワードなどの機密情報を攻撃者サイトに不正送信する目的で仕掛けられる。

エ　リプレイアタック（再使用攻撃）に関する記述である。

問269　ウ

パスワードリスト攻撃とは，外部から入手した過去のパスワード使用履歴などをもとにして不正アクセスを試みる手法である。同じパスワードを繰り返し使用していると，過去のパスワードがそのまま通用する確率が高まってしまう。

ア　一般的なパスワードシステムに対する辞書攻撃に該当する。

イ　パスワードのハッシュ値を用いるシステムに対する攻撃手法に該当する。入手したハッシュ値をオフラインで（対象システムに入力試行せず，別の環境で）解析することが多く，その場合はオフライン総当たり攻撃やオフライン辞書攻撃などとよばれることもある。

エ　ピクチャパスワードとよばれる，画面へのタッチやジェスチャーなどのUI動作によって認識するシステムへの攻撃手法に該当する。

問270　ウ

リスクベース認証とは，アクセスごとにそのアクセスが不正である可能性を判断し，「不正のリスク」が高いと判断された場合に追加の認証措置によって安全性を高める仕組みである。例えば，アクセス要求が通常とは異なる機器や位置で発生した場合，“秘密の質問”を用いて本人であることの確証を高める仕組みなどがリスクベース認証に該当する。

ア　このような手法は2要素認証，あるいは多要素認証とよばれる。

問271　ウ

レインボー攻撃は，ハッシュ値に変換して保存されたパスワードを解読する攻撃である。パスワードになりそうな文字列をあらかじめハッシュ値に変換して対応表（レインボーテーブルという）に登録しておき，この表と入手したハッシュ値を比較して，元のパスワードを見つけ出す。

レインボー攻撃への対策の一つとして，登録したパスワードに“ソルト”と呼ばれるランダムな文字列を連結し，そのハッシュ値を保存する方法がある。ソルトが変わるとハッシュ値も変わるため，攻撃者はそれぞれ計算し直して一覧表を作成する必要があるが，その作業量は膨大なものになってしまう。

ア　パスワードリスト攻撃に関する記述である。
イ　ブルートフォース攻撃（総当たり攻撃）に関する記述である。
エ　ソーシャルエンジニアリングに関する記述である。

問272　エ

シングルサインオンとは，一組のユーザIDとパスワードで，複数のサーバにおける利用者認証を一括して安全に行えるようにする認証方法や仕組みのことである。利用者は1回のログインで複数のサーバの提供するサービスを利用できる。

シングルサインオンを実現する方法には，サーバごとの認証情報を含んだ認証クッキーをクライアント上で保存・管理する方法や，各サーバが行うべき利用者認証をリバースプロキシサーバが一括して行う方法などがある。

リバースプロキシを使ったシングルサインオンでは，認証情報を一元的に管理する認証サーバが各サーバに対するリクエストをチェックし，認証済みのリクエストだけをサーバに送信する。そのため，利用者認証においてパスワードの代わりにディジタル証明書を用いることができる。

ア　クッキーを使ったシングルサインオンでは，生成したクッキーはクライアント上で保存・管理される。
イ　クッキーを使ったシングルサインオンでは，認証対象の各サーバはクッキーの伝達範囲内（クッキードメイン内）であることが求められるが，認証対象の各サーバをそれぞれ異なるインターネットドメインにする必要はない。
ウ　リバースプロキシを使ったシングルサインオンでは，利用者認証をリバースプロキシサーバが一括して管理するので，認証対象の各Webサーバをそれぞれ異なるインターネットドメインにする必要はない。

問273　エ

チャレンジレスポンス方式は,認証主体（サーバ）が作成するチャレンジコード（要求文字列）をもとに，被認証主体（利用者）が暗号技術を適用してレスポンスコードを生成し，レスポンスコードを認証主体が検証することで被認証主体の実体の真正性を認証する方式である。パス

ワードをそのまま通信することがないため，パスワードを窃取されることを防止できる。また，チャレンジコードは毎回変わるので，リプレイアタックにも対抗できる。

問274　イ

認証デバイスとは，ユーザ認証を行うさいに使用する機器のことである。代表的なものに，認証用のディジタル証明書を格納したUSBトークンタイプ，ICカードタイプのものや，バイオメトリクス認証（生体認証）などがある。

バイオメトリクス認証は，個人の生体としての特徴を登録しておき，パスワードのように認証に利用する仕組みである。一般に下記のような情報を個人認証に利用可能である。

指紋：特徴点抽出方式やパターンマッチングにより照合する
声紋：事前収録した音声の周波数パターンを照合する
虹彩（こうさい）：目を撮影し，虹彩（瞳の模様）のパターンを照合する
掌静脈：手の平の静脈のパターンを照合する
顔：撮影した顔の画像を解析し，目や鼻の配置を照合する

このうち，指紋や虹彩は経年変化耐性（年齢を重ねても変化しにくい）があり，声紋や顔は経年変化耐性が弱いことで知られる。よって，虹彩認証では，認証デバイスのパターン更新はほとんど不要といってもよい。

ア　USBメモリにディジタル証明書を組み込む場合，保持者がそのUSBメモリをPCに接続しているときだけ，認証が有効になる。認証対象にPCを含めているわけではないので，利用するPCについてはMACアドレスなどの個別情報は組み込む必要はない。
ウ　静電容量方式の指紋認証デバイスは，光学式のように光によって読み取るのではなく，半導体技術を用いるので，LED照明などの影響は受けない。
エ　コイルの誘導起電力を利用するのは，非接触型ICカードの特徴である。接触型ICカードでは，カード表面に配置されたICモジュール端子部分を読取り装置に接触させることで直接読取りを行う。

問275　ウ

ディジタル署名で用いられるハッシュ関数は，改ざんの有無を検出するために用いられる。一般的に，ハッシュ値に求められる性質は次のとおりである。

・ハッシュ値から元のメッセージを生成できないこと（非可逆性）
・異なるメッセージから同じハッシュ値が生成される確率が極めて低いこと（衝突困難性）
・原則的に結果（ハッシュ値）が固定長となること
・元のメッセージが少しでも変われば，生成されるハッシュ値は大きく異なること（初期値敏感性）

問276　ア

問題に示されたような手順でメッセージダイジェストを処理することにより，メッセージダイジェストのもととなった電子メール本文の改ざんを検知できる。

ハッシュ関数は

・入力の内容が少しでも異なると，出力が異なる

・ハッシュ値からもとの入力内容を導き出すのは非常に困難である

という性質をもっている。仮に電子メール本文が改ざんされていた場合，受信者Bが改ざんされたメールから作成したダイジェストは，別に受け取ったダイジェストとは一致しなくなるので，改ざんに気付くことができる。

問277　エ

ディジタル署名は，公開鍵方式における“秘密鍵は鍵の所有者本人しかもち得ない”という性質を利用して，文書の作成者を証明し，かつその文書が改ざんされていないことを確認するための技術である。

ディジタル署名では，送信者は送信データ本体（メッセージ）のダイジェストを作成し，これを自らの秘密鍵で暗号化してディジタル署名とする。これを送信データ本体とともに受信者に対して送信する。受信者は，送信データ本体から作成したダイジェストと，ディジタル署名を送信者の公開鍵を用いて復号することで得られたダイジェストを比較する。適切に復号でき両者が一致すれば,メッセージは送信者が確かに作成したものであり（“なりすまし”ではない），かつ途中で改ざんを受けていないものと判断される。

問278　ウ

ディジタル署名は，メッセージ認証とエンティティ認証の両面をもち合わせる認証情報である。送信者は，メッセージダイジェストなどに対して署名鍵（通常は送信者の秘密鍵）を用いた暗号化を行い，送信者本人しか作成できないデータ（署名）を作成する。

受信者は,署名鍵に対応した復号鍵（通常は送信者の公開鍵）を使ってそれを復号する。もし，受信者が正しく復号できたのであれば，それは送信者本人のみが所有する鍵によって暗号化されたことを証明することになり，受信者が送信者を確認することができる。

エ　署名用の鍵ではなく暗号化鍵を使用して行う，メッセージの暗号化に関する記述である。

問279　エ

問題文に示された手順は，タイムスタンプを用いたディジタル署名によるファイルの存在証明を行う手順である。ディジタル署名の正当性と有効性を確保するために，送信者は第三者機関であるタイムスタンプオーソリティにハッシュ値を送る。タイムスタンプオーソリティは，それと時刻情報を組み合わせたもののディジタル署名を作成する。送信者は，結合されたデータとディジタル署名を受け取り，受信者に送信する。受信者は，ハッシュ値の照合を行い，ファイルが作成された日時と，それ以降でファイルが改ざんされていないことを確認できる。よって，正解は“エ”となる。

ア〔手順〕において結合データに含まれる日時は，第三者機関がファイルを受信した日時である。受信者Bにファイルが到達する日時は，それより後になる。

イ〔手順〕において結合データに含まれる日時は，第三者機関がファイルを受信した日時である。送信者Aが受信者Bにファイルを送信する日時は，それより後になる。

ウ 〔手順〕において結合データに含まれる日時は，第三者機関がファイルを受信した日時である。送信者Aが第三者機関にファイルを送る以前に，ファイルは作成されている。

問280 エ

認証局が侵入されて不正な証明書が複数発行され，どの証明書が不正に発行されたか分からないということは，その認証局の発行する証明書はすべて信頼できない状況といえる。このような状況では，「その認証局が発行する証明書をすべて信頼しない」としなければ，不正なWebサイトへのアクセスを防ぐことはできない。このためには，ブラウザの設定でその認証局を信頼していない状態にする（信頼できる認証局のリストから該当認証局を除外する）必要がある。

ア 証明書が不正に発行されたのであれば，有効期限にかかわらず証明書を無効化しなければならない。

イ 利用者がWebサイトのアクセスログを確認することはできない。また，ドメイン名登録情報の検索サービスであるWhoisデータベースを検索したとしても，そのWebサイトで使われている証明書が不正に発行されたものか否かは判断できない。

ウ その認証局から不正な証明書が発行されているので，認証局のCPは意味をもたない。

問281 イ

CRL(Certificate Revocation List：証明書失効リスト）は，有効期限内であっても，証明対象の公開鍵と対をなす秘密鍵の漏えい，紛失などの理由から無効となったディジタル証明書のリストである。無効となったディジタル証明書の発行元の認証局名や証明書シリアル番号，失効日時などが記載され，発行元の認証局の署名が付与される。

ア CRLには，失効されたディジタル証明書に対応する秘密鍵は登録されない。

ウ CMP(Certificate Management Protocol)に関する記述である。CMPを用いてディジタル証明書の登録申請者が証明書の破棄を認証局に要求すると，鍵の漏えいなどの破棄理由や破棄申請の状況がリポジトリ（データベース）にリアルタイムに反映される。

エ 有効期限の切れたディジタル証明書は，CRLの登録対象ではない。CRLに登録されるのは，有効期限内でありながら無効となったディジタル証明書である。

問282 ウ

OCSP(Online Certificate Status Protocol)は，証明書の失効情報問合せに用いるプロトコルである。OCSPを用いることで，各クライアントがCRL（失効リスト）を保持・検索する方法と比べ，リアルタイム性の向上，クライアント負荷の軽減などが期待できる。

CHAP(Challenge Handshake Authentication Protocol)：PPP接続で用いられるユーザ認証方式の一つ

LDAP(Lightweight Directory Access Protocol)：X.500に対応したディレクトリサービスにアクセスするためのプロトコル

SNMP(Simple Network Management Protocol)：ネットワーク上の機器を管理するためのプロトコル

問283　ウ

OCSP(Online Certificate Status Protocol)は，ディジタル証明書の失効情報をリアルタイムで問い合わせて確認するためのプロトコルで，RFC6960(旧RFC2560)でその仕様が規定されている。OCSPリクエスタ(OCSPクライアント)からOCSPレスポンダ(OCSPサーバ)にOCSPリクエスト(失効情報要求)が送信されると，OCSPレスポンス(失効情報応答)が返信される。

問284　イ

コンピュータに不正侵入した攻撃者が，自身の痕跡を隠蔽したり次回の侵入を容易にしたりするソフトウェアをまとめてパッケージ化したものをrootkit(ルートキット)という。rootkitには，ログを改ざんするツールや裏口(バックドア)を提供するツール，改ざんされたシステムコマンド群などが含まれることが多い。

RFID(Radio Frequency Identification)：ICタグ(RFタグ)に記録された情報を，無線通信によって読み書きすることで個々のタグを識別する仕組み。人や物品の管理などに多く用いられる。

TKIP(Temporal Key Integrity Protocol)：無線LANの暗号化通信において，一時的な暗号鍵を生成し，しばらくしたらそれを破棄して新たな鍵を生成する方式。WEPの脆弱性を補うために，WPA(Wi-Fi Protected Access)で採用されている。

web beacon：Webページの閲覧動向や閲覧者などを解析する仕組みや，そのために用いられる極めて小さな画像のこと。

問285　エ

エクスプロイトコード(exploit code)とは，ハードウェアやソフトウェアの脆弱性を利用するコードである。検証用コードを指す場合と，悪用した攻撃コードを指す場合がある。システムの脆弱性が発見されその存在が公開されると，その脆弱性を利用したエクスプロイトコードが作られ，ゼロデイ攻撃に利用されることがある。

ア　異なるシステム間でデータファイルを移行する際に用いる，データ変換プログラム(コンバータ)に該当する記述である。

イ　ファイルブラウザやファイルマネージャなどと呼ばれる管理用ソフトウェア，及びそれがもつ暗号化機能に該当する記述である。

ウ　プロトタイピングに該当する記述である。

問286　ウ

エクスプロイトキット(exploit kit)は，システムの脆弱性を攻撃する複数のスクリプトやプログラムなどをパッケージ化したものである。脆弱性を利用するツールであることから，逆に脆弱性の存在を検証する実証ツールとして利用されることもある。

ア　iFuzzMakerなどのファジング用ツールに関する記述である。

イ　MyJVNなどのチェックツールに関する記述である。

エ　ログ解析ツールに関する記述である。