問題

問 1

正解 □ 完璧 □ 直前CHECK □

DNSSEC（DNS Security Extensions）の機能はどれか．

ア　DNSキャッシュサーバの設定によって再帰的な問合せの受付範囲が最大限になるように拡張する．

イ　DNSサーバから受け取るリソースレコードに対するディジタル署名を利用して，リソースレコードの送信者の正当性とデータの完全性を検証する．

ウ　ISPなどのセカンダリDNSサーバを利用してDNSコンテンツサーバを二重化することで名前解決の可用性を高める．

エ　共通鍵暗号技術とハッシュ関数を利用したセキュアな方法で，DNS更新要求が許可されているエンドポイントを特定し認証する．

問 2

正解 □ 完璧 □ 直前CHECK □

セキュアハッシュ関数SHA-256を用いて，32ビット，256ビット，2,048ビットの三つの長さのメッセージからハッシュ値を求めたとき，それぞれのメッセージのハッシュ値の長さはどれか．

単位 ビット

メッセージの長さ	32	256	2,048
ア	32	256	256
イ	32	256	2,048
ウ	256	256	256
エ	256	256	2,048

問 3

正解 □ 完璧 □ 直前CHECK □

A社のWebサーバは，認証局で生成したWebサーバ用のディジタル証明書を使ってSSL/TLS通信を行っている．PCがA社のWebサーバにSSL/TLSを用いてアクセスしたときにPCが行う処理のうち，サーバのディジタル証明書を入手した後に，認証局の公開鍵を利用して行うものはどれか．

ア　暗号化通信に利用する共通鍵を生成し，認証局の公開鍵を使って暗号化する．

イ　暗号化通信に利用する共通鍵を認証局の公開鍵を使って復号する．

ウ　ディジタル証明書の正当性を認証局の公開鍵を使って検証する．

エ　利用者が入力して送付する秘匿データを認証局の公開鍵を使って暗号化する．

問1　イ

DNSSEC（DNS Security Extensions）：DNSサーバから送られてくるIPアドレスとホスト名の対応情報の信頼性を証明するセキュリティ拡張機能．応答を送信するDNSサーバが秘密鍵を使って応答に署名し，受信する側が公開鍵で検証する．秘密鍵で正しい署名を付けるので，署名の検証によって偽の応答を検知できる．DNSキャッシュポイズニングを防ぐことができる．

ア：再帰的な問合せの受付範囲を最大限にすると，**DDoS攻撃の踏み台**にされる危険性がある．

問2　ウ

SHA-256は2002年に米国家安全保障局（NSA）が設計し，NISTが規格化した米国政府標準ハッシュ関数である．ハッシュ長は256ビットである．

SHA-256は，メッセージの長短とは無関係に256ビットのハッシュ値が求められる．

問3　ウ

A社のWebサーバにSSL/TLSを用いてアクセスしたとき，サーバのディジタル署名を入手後に認証局の公開鍵を利用してPCが行う処理は，**ディジタル証明書の正当性を認証局の公開鍵を使って検証すること**である．その後，PC側で乱数を生成して証明書から取り出したサーバの公開鍵で暗号化し，A社のWebサーバへ送信する．PCとWebサーバは乱数を基に共通鍵を生成して，A社とPCは相互に暗号化通信を行う．

問4

正解 完璧 直前CHECK

SSLを使用して通信を暗号化する場合，SSL-VPN装置に必要な条件はどれか．

ア　SSL-VPN装置は，FQDN又はIPアドレスを含むディジタル証明書を組み込む必要がある．

イ　SSL-VPN装置は，装置メーカが用意した機種固有のディジタル証明書を組み込む必要がある．

ウ　SSL-VPN装置は，装置メーカから提供される認証局を利用する必要がある．

エ　同一ドメイン内で複数拠点にSSL-VPN装置を設置する場合は，同一のディジタル証明書を利用する必要がある．

問5

正解 完璧 直前CHECK

ISP“A”管理下のネットワークから別のISP“B”管理下の宛先へSMTPで電子メールを送信する．電子メール送信者がSMTP-AUTHを利用していない場合，スパムメール対策OP25Bによって遮断される電子メールはどれか．

ア　ISP“A”管理下の固定IPアドレスから送信されたが，受信者の承諾を得ていない広告の電子メール

イ　ISP“A”管理下の固定IPアドレスから送信されたが，送信元IPアドレスがDNSで逆引きできなかった電子メール

ウ　ISP“A”管理下の動的IPアドレスからISP“A”のメールサーバを経由して送信された電子メール

エ　ISP“A”管理下の動的IPアドレスからISP“A”のメールサーバを経由せずに送信された電子メール

問6

正解 完璧 直前CHECK

100人の送受信者が共通鍵暗号方式で，それぞれが相互に暗号化通信を行うときに必要な共通鍵の総数は幾つか．

ア　200　　イ　4,950　　ウ　9,900　　エ　10,000

問4　ア

SSL-VPNは，インターネット網をあたかも専用回線であるかのように利用する**VPN**（Virtual Private Network）を構築する暗号通信方式である．トランスポート層のデータを暗号化して送受信する暗号通信プロトコルである**SSL**（Secure Socket Layer）を用いる．

イ：SSL-VPN装置のディジタル証明書は，メーカが用意したものではなく認証局から装置に対して発行されたディジタル証明書を用いる．

ウ：装置メーカから提供される認証局を利用する必要はない．

エ：SSL-VPN装置は，異なるディジタル証明書を利用する．

問5　エ

SMTP-AUTHとはユーザ認証機能（authentication）をSMTPに追加したものである．送信者の認証を実施することでスパムメールの送信を遮断する効果を持つ．この問題ではSMTP-AUTHが利用されていないので，送信時の認証が行われていない．

OP25Bは，ISPの会員が他のメールサーバを利用してスパムメールを送信することを防ぐ機能を持つ．

ア，イ：OP25Bは受信者の承諾の有無や送信元IPアドレスの正否を監視するスパムメール対策ではないので，遮断されない．

ウ：OP25Bは，異なるISPのメールサーバを利用して送信される電子メールを遮断する．同じISPのメールサーバを経由する電子メールであれば遮断されない．

エ：異なるISPのメールサーバを経由してるので，遮断される．

問6　イ

共通鍵暗号方式でn人の送受信者が相互に暗号を使って秘密の通信を行うとき，n人の中のある人が他の$n-1$人と通信するためには$n-1$個の鍵が必要である．n人全体では$n(n-1)$個の鍵を必要とする．ただし，送信者と受信者で使う鍵は共通なので，全体では$n(n-1)/2$個になる．

100人の場合は，$100(100-1)/2 = 4{,}950$の鍵が必要である．

問 7

正解 □ 完璧 □ 直前CHECK □

IPアドレスに対するMACアドレスの不正な対応関係を作り出す攻撃はどれか.

ア　ARPスプーフィング攻撃
イ　DNSキャッシュポイズニング攻撃
ウ　URLエンコーディング攻撃
エ　バッファオーバフロー攻撃

問 8

正解 □ 完璧 □ 直前CHECK □

DNSサーバに格納されるネットワーク情報のうち，第三者に公開する必要のない情報が攻撃に利用されることを防止するための，プライマリDNSサーバの設定はどれか.

ア　SOAレコードのシリアル番号を更新する.
イ　外部のDNSサーバにリソースレコードがキャッシュされる時間を短く設定する.
ウ　ゾーン転送を許可するDNSサーバを限定する.
エ　ラウンドロビン設定を行う.

問7　ア

ARPスプーフィング攻撃：ARPはIPアドレスからMACアドレスを求めるプロトコルであるが，これを悪用した攻撃手法．誤ったMACアドレスを返すことで偽のPCや機器にデータが転送されるようになる．

DNSキャッシュポイズニング攻撃：DNSサーバに偽ドメイン情報をキャッシュさせる攻撃手法である．DNSサーバに偽ドメイン情報がキャッシュされると，DNSサーバはクライアントに偽ドメインのアドレスを返してしまい，クライアントは偽装されたWebサーバに誘導されてしまう

URLエンコーディング攻撃：URLエンコーディングとは，URLに含まれる字句がシステムコードなどと認識されて発生することで予期しない動作命令をコンピュータに与えることを防ぐ機能である．その機能を利用して，不正なURLを読み込ませてブラウズを以上動作させる攻撃手法がURLエンコーディング攻撃である．

バッファオーバフロー攻撃：システムが想定しているサイズよりも大きなサイズのデータを送信することでバッファオーバフローを発生させて，システムの暴走や意図しない動作をさせる攻撃手法．

問8　ウ

選択肢ア，イ，エは，本問の攻撃の防止とは無関係である．

ア：**SOA**（Start Of Authority）**レコード**のシリアル番号の更新は，**ゾーンデータ**が変更されていることを示す．

イ：ホストのIPアドレスの変更を予定している場合は，キャッシュが適切に更新されるように事前に**セカンダリDNSサーバ**が**プライマリDNSサーバ**に問合せを行う時間間隔（更新間隔）を短くする．

ウ：第三者に公開する必要がない情報をゾーン転送してしまわないように，ゾーン転送を許可したDNSサーバを登録する．

エ：**DNSラウンドロビン**は，一つのドメイン名に複数のIPアドレスを割り当てる負荷分散技術の一つである．トラフィックを複数のIPアドレスのホストに分散させるために用いられる．

問題

問 9

正解 □ 完璧 □ 直前CHECK □

サービス不能攻撃（DoS）の一つであるSmurf攻撃の特徴はどれか．

ア　ICMPの応答パケットを大量に発生させる．
イ　TCP接続要求であるSYNパケットを大量に送信する．
ウ　サイズの大きいUDPパケットを大量に送信する．
エ　サイズの大きい電子メールや大量の電子メールを送信する．

問 10

正解 □ 完璧 □ 直前CHECK □

表に示すテーブルX，Yへのアクセス要件に関して，JIS Q 27001:2006（ISO/IEC 27001:2005）が示す“完全性”の観点からセキュリティを脅かすおそれのあるアクセス権付与はどれか．

テーブル	アクセス要件
X（注文テーブル）	① 調達課の利用者Aが注文データを入力するために，又は内容を確認するためにアクセスする． ② 管理課の利用者Bはアクセスしない．
Y（仕入先マスタテーブル）	① 調達課の利用者Aが仕入先データを照会する目的だけでアクセスする． ② 管理課の利用者Bが仕入先データのマスタメンテナンス作業を行うためにアクセスする．

ア　`GRANT INSERT ON Y TO A`　　イ　`GRANT INSERT ON Y TO B`
ウ　`GRANT SELECT ON X TO A`　　エ　`GRANT SELECT ON X TO B`

問9　ア

Smurf攻撃とはネットワークに大量のパケットを発生させてサービス不能状態を作り出す攻撃手法である．攻撃の手法は次の通り．

ICMPではICMP Echo Requestが送信されるとEcho Replayが返信される．攻撃者は送信元を攻撃対象のサイトに偽造して，Echo Requestをブロードキャストアドレス宛に送信する．Echo Replyがネットワークのすべてのコンピュータから返信され，この大量のReplyによりサービス不能となる．

問10　ア

JIS Q 27001は，情報セキュリティマネジメントシステム（**ISMS**）の国際規格であるISO/IEC 27001をベースとして，その内容や構成をそのまま日本語化し，日本工業規格としたものである．**完全性**とは，情報及び処理方法が正確であり，完全であることを保証することである．

選択肢はSQLのスキーマを表しており，それぞれ，GRANT：アクセス権限，INSERT：データの挿入，SELECT：データの選択を意味している．

解答を選択するには，まず選択肢と，表のテーブルとアクセス要件の内容の整合性を確認する．そして，不整合が発生していて完全性を脅かすものを選択すればよい．

ア：“AはYにおいてデータ挿入可能”となっているが，表：Yの①より，Aはデータ照会のみ許可されており，データ挿入はできないため，不整合である．また，Aはデータを書き換えることが可能であるため，完全性の観点からも脅威となる．

イ：“BはYにおいてデータ挿入可能”となっており，表：Yの②より，Bはデータのマスタメンテナンス作業が可能であり，データ挿入可能であるため，整合的である．

ウ：“AはXにおいてデータ選択可能”となっており，表：Xの①より，Aはデータ確認が許可されており，データ選択可能であるため，整合性がとれている．

エ：“BはXにおいてデータ選択可能”となっており，表：Xの②より，Bはデータアクセスできないため不整合である．しかし，データを書き換えることができないため，完全性の観点から脅威とならない．

問題

問 11

正解 □ 完璧 □ 直前CHECK □

テンペスト（TEMPEST）攻撃を説明したものはどれか．

ア　故意に暗号化演算を誤動作させて正しい処理結果との差異を解析する．
イ　処理時間の差異を計測し解析する．
ウ　処理中に機器から放射される電磁波を観測し解析する．
エ　チップ内の信号線などに探針を直接当て，処理中のデータを観測し解析する．

問 12

正解 □ 完璧 □ 直前CHECK □

ダウンローダ型ウイルスがPCに侵入した場合に，インターネット経路で他のウイルスがダウンロードされることを防ぐ対策のうち，最も有効なものはどれか．

ア　URLフィルタを用いてインターネット上の不正Webサイトへの接続を遮断する．
イ　インターネットから内部ネットワークに向けた要求パケットによる不正侵入行為をIPSで破棄する．
ウ　スパムメール対策サーバでインターネットからのスパムメールを拒否する．
エ　メールフィルタで他サイトへの不正メール発信を遮断する．

問 13

正解 □ 完璧 □ 直前CHECK □

ルートキット（rootkit）を説明したものはどれか．

ア　OSの中核であるカーネル部分の脆弱(ぜい)性を分析するツール
イ　コンピュータがウイルスやワームに感染していないことをチェックするツール
ウ　コンピュータやルータのアクセス可能な通信ポートを外部から調査するツール
エ　不正侵入してOSなどに不正に組み込んだものを隠蔽する機能をまとめたツール

問11　ウ

テンペスト（TEMPEST）**攻撃**とは，コンピュータやディスプレイ，ケーブル等から放射される電磁波を受信・解析することで，キー入力情報の収集や表示画面の復元などを行う攻撃（盗聴）手法である．

テンペスト攻撃の対策としては，周辺機器やケーブル等をシールドして電波の放射を防ぐ方法が有効である．具体的には，回線設計の段階で信号の漏えいを防ぎつつ，ケーブル等を被覆して電磁波をシールドすることが基本的な対策である．また，コンピュータの設置された部屋全体をシールドする手段もある．

問12　ア

ダウンローダ型ウイルスとは**トロイの木馬型ウイルス**の一種で，コンピュータのOSやアプリケーションソフトの脆弱性を利用して感染した後，別のPCへの感染活動だけでなく，別のウイルスをインターネットからダウンロードするという特徴がある．

ア：ダウンロード先の不正WebサイトのURLが判明している場合，URLフィルタを用いて不正Webサイトへの接続を遮断する．

イ：ダウンローダ型ウイルスは内部ネットワークから外部ネットワークであるインターネットへアクセスするように動作するため，このIPSではウイルスのダウンロード防止の効果はない．

ウ：スパムメールの中にはウイルスが添付されていたり，ウイルスをダウンロードさせるWebサイトへ誘導したりするものもある．ダウンローダ型ウイルスの感染予防にはなる．

エ：不正メールの発信防止であり，ダウンローダ型ウイルスの対策とは無関係である．

問13　エ

ルートキットとは，**クラッカ**が**セキュリティホール**等を利用して不正侵入した後に用いる，侵入の隠ぺい，バックドアの確保，踏み台による攻撃等の機能をまとめたツール群のことである．

イ：ウイルス対策ソフトの説明である．

ウ：ポートスキャンツールの説明である．

問題

問 14

正解 □ 完璧 □ 直前CHECK □

スパムメールの対策であるDKIM（DomainKeys Identified Mail）の説明はどれか．

ア　送信側メールサーバでディジタル署名を電子メールのヘッダに付与して，受信側メールサーバで検証する．

イ　送信側メールサーバで利用者が認証されたとき，電子メールの送信が許可される．

ウ　電子メールのヘッダや配送経路の情報から得られる送信元情報を用いて，メール送信元のIPアドレスを検証する．

エ　ネットワーク機器で，内部ネットワークから外部のメールサーバのTCPポート25番への直接の通信を禁止する．

問 15

正解 □ 完璧 □ 直前CHECK □

IPsecのAHに関する説明のうち，適切なものはどれか．

ア　IPパケットを暗号化する対象部分によって，トランスポートモード，トンネルモードの方式がある．

イ　暗号化アルゴリズムや暗号化鍵のライフタイムが設定される管理テーブルで，期間を過ぎると新しいデータに更新される．

ウ　暗号化アルゴリズムを決定し，暗号化鍵を動的に生成する鍵交換プロトコルで，暗号化通信を行う．

エ　データの暗号化は行わず，SPI，シーケンス番号，認証データを用い，完全性の確保と認証を行う．

問 16

正解 □ 完璧 □ 直前CHECK □

Webアプリケーションの脆弱(ぜい)性を悪用する攻撃手法のうち，Perlのsystem関数やPHPのexec関数など外部プログラムの呼出しを可能にするための関数を利用し，不正にシェルスクリプトや実行形式のファイルを実行させるものはどれに分類されるか．

ア　HTTPヘッダインジェクション

イ　OSコマンドインジェクション

ウ　クロスサイトリクエストフォージェリ

エ　セッションハイジャック

問14　ア

DKIMは，送信者が正当な団体であるかどうかを認証する送信者認証技術である．メールを送信するときに自分が持っている秘密鍵でディジタル署名を行い，メールを受け取る受信者側では送信情報を元にDNSを管理しているサーバに問い合わせて，公開鍵を取得する．

イ：**SMTP-AUTH**の説明である．

ウ：**ブラックリスト**の説明である．スパムメール送信元IPアドレスのブラックリスト照合する．

エ：**OBP25**（Outbound Port 25 Blocking）の説明である．

問15　エ

IPsecはネットワーク層で動作するプロトコルで，暗号技術を用いてデータの改ざん防止機能や秘匿機能を提供している．その機能は，AH（Authentication Header），ESP（Encapsulated Security Payload），IKE（Internet Key Exchange protocol）などにより構成されている．

AHは，データの完全性（改ざんされていないこと）を確認して認証を行う機能を持つ．

ア：暗号化範囲の違いによってトランスポートモードとトンネルモードが異なるのは，**ESP**パケットである．

イ，ウ：**IKE**の機能に関する説明である．

エ：AHの機能に関する説明である．

問16　イ

HTTPヘッダインジェクション：動的にHTTPヘッダが生成されるHTTP通信の機能を利用した攻撃手法．HTTPヘッダに改行コードを生成させることで不正な動作を実行させる．

OSコマンドインジェクション：サーバ内のOSコマンドを外部から実行させることでサーバに不正な動作を実行させる攻撃手法．

クロスサイトリクエストフォージェリ：Webサイトに埋め込まれているスクリプトや命令が，利用者がそのWebサイトにアクセスすることによって自動的に実行させられてしまう攻撃手法．掲示板への書き込みやオンラインショップでの買い物などが，意図せずに行われてしまう．

セッションハイジャック：セッションIDを盗み出すことでセッションを乗っ取り，あたかもそのセッションの参加者であることを装う攻撃手法．セッションの参加者でなければ見ることのできない情報を盗み出すことができる．

問題

問 17

正解 □ 完璧 □ 直前CHECK □

DNSのMXレコードで指定するものはどれか.

ア　エラーが発生したときの通知先のメールアドレス
イ　送信先ドメインのメールサーバ
ウ　複数のDNSサーバが動作しているときのマスタDNSサーバ
エ　メーリングリストを管理しているサーバ

問 18

正解 □ 完璧 □ 直前CHECK □

コンピュータとスイッチングハブの間，又は2台のスイッチングハブの間を接続する複数の物理回線を論理的に1本の回線に束ねる技術はどれか.

ア　スパニングツリー　　イ　ブリッジ
ウ　マルチホーミング　　エ　リンクアグリゲーション

問 19

正解 □ 完璧 □ 直前CHECK □

電源オフ時にIPアドレスを保持することができない装置が，電源オン時に自装置のMACアドレスから自装置に割り当てられているIPアドレスを知るために用いるデータリンク層のプロトコルで，ブロードキャストを利用するものはどれか.

ア　ARP　　イ　DHCP　　ウ　DNS　　エ　RARP

問17　イ

DNS（Domain Name System）では，利用されるデータをリソースレコード（RR）と呼ぶ．主なリソースレコードの役割は以下のとおりである．

MXレコード （Mail Exchengerレコード）	電子メールの送信に利用される．DNS上で電子メールの配送先ホスト名を指定する際に利用する．
NSレコード （Name Serverレコード）	ドメインの委任を行うときに指定するレコード．例えばxxx.co.jpというドメインを立ち上げたときにco.jpから各種レコードを参照するため，co.jp側にてxxx.co.jpのNSレコードを設定する必要がある．
PTRレコード （逆引きレコード）	IPアドレスからドメイン名を問い合わせるためのレコード．
SOAレコード （Start Of Authorityレコード）	DNSで指定するゾーン（xxx.co.jp）の基本的な設定を行うレコード．シリアル，リフレッシュ等を指定する．
Aレコード （正引きレコード）	ドメイン名からIPアドレスを問い合わせるためのレコード．
CNAMEレコード （Canonical Nameレコード）	ホスト名に別名をつけるレコード．

問18　エ

スパニングツリー：リング型のネットワークでデータが永久に循環するのを防ぐための方式の一つ．スイッチングハブで利用される．

ブリッジ：データリンク層でデータを中継するための装置．

マルチホーミング：複数の経路を選択して同時に使用することで冗長化すること．論理的に1本の回線として扱っているわけではない．

リンクアグリゲーション：複数の物理回線を論理的に1本に束ねて高速の回線として利用する．

問19　エ

ARP（Address Resolution Protocol）：IPアドレスからイーサネットアドレス（MACアドレス）を得るプロトコルである．

DHCP（Dynamic Host Configuration Protocol）：端末に対して動的にIPアドレスを割り当てるためのプロトコルである．

DNS（Domain Name System）：IPアドレスとホスト名の相互変換サービスである．

RARP（Reverse Address Resolution Protocol）：MACアドレスからIPアドレスを問い合わせるプロトコルである．

問 20

正解 完璧 直前CHECK

TCPヘッダに含まれる情報はどれか.

ア　宛先ポート番号　　イ　パケット生存時間（TTL）

ウ　発信元IPアドレス　　エ　プロトコル番号

問 21

正解 完璧 直前CHECK

次数がnの関係Rには，属性なし（ϕ）も含めて異なる射影は幾つあるか.

ア　n　　イ　2n　　ウ　n^2　　エ　2^n

問 22

正解 完璧 直前CHECK

バグ埋込み法において，埋め込まれたバグ数をS，埋め込まれたバグのうち発見されたバグ数をm，埋め込まれたバグを含まないテスト開始前の潜在バグ数をT，発見された総バグ数をnとしたとき，S，T，m，nの関係を表す式はどれか.

ア　$\frac{m}{S} = \frac{n-m}{T}$　　イ　$\frac{m}{S} = \frac{T}{n-m}$

ウ　$\frac{m}{S} = \frac{n}{T}$　　エ　$\frac{m}{S} = \frac{T}{n}$

問20　ア

TCPヘッダは下記のような構造となっている．

送信元ポート番号								**宛先ポート番号**
シーケンス番号								
ACK番号								
データオフセット	予約領域	URG	ACK	PSH	RST	SYN	FIN	ウィンドウサイズ
チェックサム								緊急ポインタ

問21　エ

次数がnの関係Rにはn個の属性が含まれる．実際に次数を設定して射影の数を数えてみる．

・次数n＝2のとき：(a，b)

ϕ，(a)，(b)，(a，b)・・・射影：4個

・次数n＝3のとき：(a，b，c)

ϕ，(a)，(b)，(c)，(a，b)，(b，c)，(a，c)，(a，b，c)・・・射影：8個

上記の結果より，2^nとなる．

問22　ア

バグ埋込みにおいては，埋め込まれたバグ数とその中から発見されたバグ数の比率と，潜在バグ数とその中から発見されたバグ数の比率は，等しいものと考える．

埋め込まれたバグ数とその中から発見されたバグ数の比率は，問題より下記のように表記できる．

$$\frac{m}{S}$$

潜在的なバグ数とその中から発見されたバグ数の比率も，同様に下記のように表記できる．

$$\frac{n-m}{T}$$

これらが等しいことから，次のように表される．

$$\frac{m}{S}=\frac{n-m}{T}$$

問 23

正解 □ 完璧 □ 直前CHECK □

ソフトウェア開発組織の活動状態のうち，CMMIモデルにおける成熟度レベルが最も高いものはどれか．

ア　作業成果物の状況が，主要なタスクの完了時点で管理層に対して見える状態になっている．
イ　実績が定量的に把握されており，プロセスが組織的に管理されている．
ウ　プロセスが明文化されて，組織内の全ての人がそれを利用している．
エ　プロセスを継続的に改善していくための仕組みが機能している．

問 24

正解 □ 完璧 □ 直前CHECK □

情報システムの設計において，フェールソフトが講じられているのはどれか．

ア　UPS装置を設置することで，停電時に手順どおりにシステムを停止できるようにし，データを保全する．
イ　制御プログラムの障害時に，システムの暴走を避け，安全に運転を停止できるようにする．
ウ　ハードウェアの障害時に，パフォーマンスは低下するが，構成を縮小して運転を続けられるようにする．
エ　利用者の誤操作や誤入力を未然に防ぐことで，システムの誤動作を防止できるようにする．

問 25

正解 □ 完璧 □ 直前CHECK □

ISMSにおけるリスク分析手法の一つである“詳細リスク分析”で行う作業はどれか．

ア　情報セキュリティポリシの作成
イ　セーフガードの選択
ウ　リスクの評価
エ　リスクの容認

問23　エ

CMMI（Capability Maturity Model Integration）モデルは，能力成熟度モデル統合と呼ばれる．カーネギーメロン大学により開発されたCMMおよびその派生モデルを統合したもの．組織がプロセスを適切に管理できるように，プロセスを5段階で評価する構成tなっている．

ア：CMMIにおける評価のレベル2に該当する．
イ：CMMIにおける評価のレベル4に該当する．
ウ：CMMIにおける評価のレベル3に該当する．
エ：CMMIにおける評価のレベル5に該当する．

問24　ウ

フェールソフトとは，システムに障害が発生した場合に障害箇所を切り離して障害の影響の拡大を防ぎ，規模を縮小して稼働を継続するシステム構成技法である．

ア：**フォールトトレランス**に関する説明である．システム障害発生時にも正常な動作を維持できるようにシステムを構成する手法．
イ：**フェールセーフ**に関する説明である．システムに故障が発生した場合，生命や周辺の機器へ損害を及ぼすことのないように，常に安全な状態にシステムを維持するシステム構成手法．
ウ：**フェールソフト**に関する説明である．
エ：**フールプルーフ**に関する説明である．利用者の誤入力や誤操作を想定し，あらかじめそのような事象が発生しないようにシステムを構成する．

問25　ウ

ISMSにおける**詳細リスク分析**とは，組織の保有するすべての情報資産について綿密な評価を実施して，それらに対する脅威や脆弱性を分析するものである．

ア：**情報セキュリティポリシ**の作成は，ISMSの計画・目標の策定の段階で実施する．
イ：**セーフガード**は，詳細リスク分析によりリスクの評価が完了した後，そのリスクに対するリスク低減策として検討される．
ウ：リスクの評価は詳細リスク分析の中で実施する．
エ：評価されたリスクに対して，そのリスク値が許容できるものであれば容認する．したがって，詳細リスク分析の後に検討される．