問 1 正解 完璧 直前チェック

CRL（Certificate Revocation List）に掲載されるものはどれか。

ア　有効期限切れになったディジタル証明書の公開鍵
イ　有効期限切れになったディジタル証明書のシリアル番号
ウ　有効期限内に失効したディジタル証明書の公開鍵
エ　有効期限内に失効したディジタル証明書のシリアル番号

問 2 正解 完璧 直前チェック

次の攻撃において，攻撃者がサービス不能にしようとしている標的はどれか。

〔攻撃〕
(1)　A社ドメイン配下のサブドメイン名を，ランダムに多数生成する。
(2)　(1)で生成したサブドメイン名に関する大量の問合せを，多数の第三者のDNSキャッシュサーバに分散して送信する。
(3)　(2)で送信する問合せの送信元IPアドレスは，問合せごとにランダムに設定して詐称する。

ア　A社ドメインの権威DNSサーバ
イ　A社内の利用者PC
ウ　攻撃者が詐称した送信元IPアドレスに該当する利用者PC
エ　第三者のDNSキャッシュサーバ

問 3 正解 完璧 直前チェック

PKIを構成するOCSPを利用する目的はどれか。

ア　誤って破棄してしまった秘密鍵の再発行処理の進捗状況を問い合わせる。
イ　ディジタル証明書から生成した鍵情報の交換がOCSPクライアントとレスポンダの間で失敗した際，認証状態を確認する。
ウ　ディジタル証明書の失効情報を問い合わせる。
エ　有効期限が切れたディジタル証明書の更新処理の進捗状況を確認する。

春

問1　エ

解説　CRLは，有効期限内に失効した公開鍵証明書を記載したリストである。認証局から発行され，公開鍵証明書が失効しているかどうかを確認できる。

公開鍵証明書の有効期限内に秘密鍵の紛失や漏えいが発生した場合には，該当する証明書の廃棄手続きが行われ，公開鍵証明書のシリアル番号がCRLに記載される。

ア，イ：有効期限切れではなく，有効期限内に失効した証明書のシリアル番号が登録される。
ウ：有効期限内に失効した公開鍵ではなく，シリアル番号が登録される。

問2　ア

解説　攻撃(1)～(3)は，**DNSリフレクター攻撃**の説明である。
(1)　サブドメイン名をランダムに多数生成することは，ドメインを詐称した攻撃であると読み取ることができる。
(2)　詐称したサブドメイン名に対する大量の問合せを，多数の第三者DNSキャッシュサーバに分散して送信することで，詐称したIPアドレスを大量に送ることができる。
(3)　送信元IPを詐称し，多数送付する。

攻撃(1)～(3)で，A社ドメインの権威DNSサーバが大量の問合せによってCPU高負荷やメモリ不足となり，サービス不能となる。

イ：DNSの問合せを詐称した攻撃であるため，利用者のPCは関係しない。
ウ：詐称した送信元IPアドレスへの通信は，ほぼないため関係ない。
エ：第三者のDNSキャッシュサーバへの通信は，詐称したサブドメインに対する問合せのみであるため影響ない範囲といえる。

問3　ウ

解説　**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確認するためのプロトコルである。OCSPはCRL（証明書失効リスト）の代替として策定され，CRLをもたなくてもリアルタイムで失効情報を確認することが可能である。RFC 2560によって規定されている。

問 4 正解 完璧 直前チェック

標準化団体OASISが，Webサイト間で認証，属性及び認可の情報を安全に交換するために策定したフレームワークはどれか。

ア　SAML　　イ　SOAP　　ウ　XKMS　　エ　XML Signature

問 5 正解 完璧 直前チェック

ハッシュ関数の性質の一つである衝突発見困難性に関する記述のうち，適切なものはどれか。

ア　SHA-256の衝突発見困難性を示す，ハッシュ値が一致する二つのメッセージの探索に要する最大の計算量は，256の2乗である。
イ　SHA-256の衝突発見困難性を示す，ハッシュ値の元のメッセージの探索に要する最大の計算量は，2の256乗である。
ウ　衝突発見困難性とは，ハッシュ値が与えられたときに，元のメッセージの探索に要する計算量の大きさによる，探索の困難性のことである。
エ　衝突発見困難性とは，ハッシュ値が一致する二つのメッセージの探索に要する計算量の大きさによる，探索の困難性のことである。

問 6 正解 完璧 直前チェック

情報セキュリティにおけるエクスプロイトコードに該当するものはどれか。

ア　同じセキュリティ機能の製品に乗り換える場合に，CSVなど他の製品が取り込め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(ぜいじゃく)性を利用するために作成されたプログラム

春

問4　ア

解説

SAML（Security Assertion Markup Language）：標準化団体OASISによって策定された，IDやパスワードなどの認証情報を安全に交換するための仕様。SAMLを用いることで，一度の認証で複数のWebサイトやサービスの利用が可能となる**シングルサインオン**（SSO：Single Sign-On）を実現できる。WebサイトがSAMLに対応していれば，異なるドメインのサイトへ移動したときに，移動元のサイトと移動先のサイトがSAMLプロトコルで通信し，自動的に認証情報を引き継ぐことができる。

SOAP（Simple Object Access Protocol）：SOAPによる通信では，XML文書にエンベロープと呼ばれる付帯情報がついたメッセージをHTTPなどでやり取りする。

XKMS（XML Key Management Specification）：XMLを利用して公開鍵基盤（PKI）の鍵情報を効率よく管理するためのプロトコルである。

XML Signature：W3C（World Wide Web Consortium）によって勧告された規格。XMLにおいてディジタル署名を利用するための規格である。

問5　エ

解説　**衝突発見困難性**は，ハッシュ値が一致する二つのメッセージを探索するための計算量が大きいことによって，探索が困難となり解読されにくいことを意味する。ハッシュ値はあらかじめわかっていない状態から解析を行う。

問6　エ

解説　**エクスプロイトコード**（exploit code）とは，ソフトウェアのセキュリティホールを利用して，不正な動作を再現するプログラムである。例えば，OSのセキュリティホールを利用して，特権アカウントを搾取するプログラムなどが該当する。

ア：CSVなど他の製品が取り込める形式でのファイル出力は，**エクスポート**と呼ばれる。
イ：エクスプロイトコードは，暗号化を解除するものではない。
ウ：試作品を作成し，利用者の反応を見ながら完成形に近づける開発手法は，**プロトタイプモデル**となる。

問 7 正解 □ 完璧 □ 直前チェック □

DoS攻撃の一つであるSmurf攻撃はどれか。

ア　ICMPの応答パケットを大量に送り付ける。
イ　TCP接続要求であるSYNパケットを大量に送り付ける。
ウ　サイズが大きいUDPパケットを大量に送り付ける。
エ　サイズが大きい電子メールや大量の電子メールを送り付ける。

問 8 正解 □ 完璧 □ 直前チェック □

ディジタル証明書に関する記述のうち，適切なものはどれか。

ア　S/MIMEやTLSで利用するディジタル証明書の規格は，ITU-T X.400で標準化されている。
イ　ディジタル証明書は，TLSプロトコルにおいて通信データの暗号化のための鍵交換や通信相手の認証に利用されている。
ウ　認証局が発行するディジタル証明書は，申請者の秘密鍵に対して認証局がディジタル署名したものである。
エ　ルート認証局は，下位の認証局の公開鍵にルート認証局の公開鍵でディジタル署名したディジタル証明書を発行する。

問7 ア

解説 **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。

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がネットワークの全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8 イ

解説 **ディジタル証明書**は，ITUが公開鍵証明書の標準として，1988年に勧告したX.509によって標準化されている。ディジタル証明書には，シリアル番号，発行者名，有効期間，所有者名，所有者の公開鍵などの情報が含まれており，認証局の秘密鍵で電子署名が付与されている。

ア：S/MIMEやTLSで利用するディジタル証明書の規格は，ITU-TのX.500ディレクトリシリーズのX.509で規定されている。
ウ：ディジタル証明書には，申請者の公開鍵に対して認証局の電子署名が付与されている。
エ：下位認証局の証明書は，ルート認証局の秘密鍵で電子署名されている。

問 9 正解 完璧 直前チェック

暗号に関連するデータのうち，次に示す処理で出力可能なものはどれか。

〔処理〕
(1) カウンタを初期化する。
(2) その時点に得た時刻データを共通鍵で暗号化する。
(3) カウンタの値と(2)の結果のXORをとり，さらに共通鍵で暗号化する。
(4) (3)の結果を出力する。
(5) (3)の結果と(2)の結果のXORをとり，さらに共通鍵で暗号化する。
(6) (5)の結果をカウンタの新しい値とする。
(7) (4)の出力について，必要とする分の数を得るまで(2)～(6)を繰り返す。

ア 擬似乱数　　イ ディジタル証明書
ウ ハッシュ値　　エ メッセージ認証コード

問 10 正解 完璧 直前チェック

“サイバー情報共有イニシアティブ(J-CSIP)”の説明はどれか。

ア 暗号技術の調査を行い，電子政府における調達のために参照すべき暗号のリストを公表するためのプロジェクト
イ 検知したサイバー攻撃の情報を公的機関に集約し，高度なサイバー攻撃対策につなげていく取組み
ウ 制御システムにおけるセキュリティマネジメントシステムの認証制度
エ 脆弱性関連情報の発見から公表に至るまでの対処プロセス

春

問9 ア

解説 処理(1)～(7)において出力可能なものは，擬似乱数である。**擬似乱数**とは，乱数列に見えるが実際には，計算によって求められる乱数であるため，厳密には再現や予測が可能となる。本来乱数とは，規則性，再現性がないものを表す。
イ：**ディジタル証明書**は，認証局が発行するデータである。
ウ：**ハッシュ値**は，元となるデータから一定の計算によって求められた，規則性のない固定長の値である。
エ：**メッセージ認証コード**(MAC：Message Authentication Code)は，データの作成元と受信者によってデータの改ざんがないことを確認するための手法である。メッセージ認証コードは，データの作成元がハッシュ関数を利用してハッシュ値を生成する。その後，受信者と共有している共通鍵で暗号化し，受信者に送る。受信者では，共通鍵でデータを復号し，ハッシュ関数を利用してデータが改ざんされていないことを確認する。

問10 イ

解説 **サイバー情報共有イニシアティブ**(J-CSIP：Initiative for Cyber Security Information sharing Partnership of Japan：ジェイシップ)は，2011年に重工，重電など重要インフラで利用される機器の製造業者を中心に，参加組織間で情報共有を行い，高度なサイバー攻撃対策に繋げていく取組みである。

具体的には，IPA(情報処理推進機構)と各参加組織(あるいは参加組織を束ねる業界団体)間で締結した秘密保持契約(NDA)のもと，参加組織およびそのグループ企業において検知されたサイバー攻撃等の情報をIPAに集約する。そして情報提供元に関する情報や機微情報の匿名化を行い，IPAによる分析情報を付加した上で，情報提供元の承認を得て共有可能な情報とし，参加組織間での情報共有を行っている。
ア：**CRYPTREC**(Cryptography Research and Evaluation Committees)の説明である。
ウ：**IEC 62443-2-1**(CSMS：Cyber Security Management System)の説明である。
エ：**ソフトウェア等脆弱性関連情報取扱基準**に示されている，脆弱性関連情報の取扱いプロセスの内容である。

問 11 正解 完璧 直前チェック

JIS Q 27000における情報セキュリティリスクに関する定義のうち，適切なものはどれか。

ア　脅威とは，一つ以上の要因によって悪用される可能性がある，資産又は管理策の弱点のことである。
イ　脆弱性とは，望ましくないインシデントを引き起こし，システム又は組織に損害を与える可能性がある潜在的な原因のことである。
ウ　リスク対応とは，リスクの大きさが，受容可能か又は許容可能かを決定するために，リスク分析の結果をリスク基準と比較するプロセスのことである。
エ　リスク特定とは，リスクを発見，認識及び記述するプロセスのことであり，リスク源，事象，それらの原因及び起こり得る結果の特定が含まれる。

問 12 正解 完璧 直前チェック

DNSキャッシュポイズニング攻撃に対して有効な対策はどれか。

ア　DNSサーバで，マルウェアの侵入をリアルタイムに検知する。
イ　DNS問合せに使用するDNSヘッダ内のIDを固定せずにランダムに変更する。
ウ　DNS問合せに使用する送信元ポート番号を53番に固定する。
エ　外部からのDNS問合せに対しては，宛先ポート番号53のものだけに応答する。

問 13 正解 完璧 直前チェック

スパムメールの対策として，宛先ポート番号25の通信に対してISPが実施するOP25Bの説明はどれか。

ア　ISP管理外のネットワークからの通信のうち，スパムメールのシグネチャに該当するものを遮断する。
イ　動的IPアドレスを割り当てたネットワークからISP管理外のネットワークへの直接の通信を遮断する。
ウ　メール送信元のメールサーバについてDNSの逆引きができない場合，そのメールサーバからの通信を遮断する。
エ　メール不正中継の脆弱性をもつメールサーバからの通信を遮断する。

問11　エ

解説 **JIS Q 27000**は，組織の事業リスク全般に対する考慮のもとで文書化した**ISMS**（Information Security Management System）の規格である。
ア：**脅威**とは，システム又は組織に損害を与える可能性があるインシデントの潜在的な原因である。
イ：**脆弱性**とは，一つ以上の脅威が付け込むことのできる資産又は資産グループがもつ弱点である。
ウ：**リスク対応**とは，リスクを修正するプロセスである。リスク対応の選択肢については，リスクの回避，リスクの低減，リスクの移転，リスクの保有の四つがある。

問12　イ

解説 **DNSキャッシュポイズニング攻撃**とは，URLなどのDNSを利用したIPアドレス検索を行う際に，正しいIPアドレスを検索できなくすること。攻撃者が不正なIPアドレスを返すようDNSのキャッシュ（一定期間IPアドレス情報を記憶している仕組み）を汚染させることである。そのため，汚染されたキャッシュ上のWebサーバにアクセスしようとすると本来とは異なるサーバに誘導される。
　対策としては，DNS問合せに対するDNSヘッダのIDを，ランダムに変更することである。
ア：DNSキャッシュポイズニング攻撃は，キャッシュ内容が不正になるため，マルウェアの進入とは関連しない。
ウ：ポート番号の53番は，一般的にDNSで利用されるポートであるため，固定してもDNSキャッシュポイズニング攻撃を防ぐことはできない。
エ：ポート番号の53番は，一般的にDNSで利用されるポートであるため誤りである。

問13　イ

解説 **OP25B**（Outbound Port 25 Blocking）は，内部ネットワークから外部ネットワークへのポート番号25の通信（SMTP）を遮断する手法である。例えば，ISPがOP25Bを用いることで，会員がISPの外部ネットワークに存在するメールサーバを使用して，スパムメールを送信することを防止することが可能となる。

問 14 正解 完璧 直前チェック

ディジタルフォレンジックスに該当するものはどれか。

ア　画像や音楽などのディジタルコンテンツに著作権者などの情報を埋め込む。
イ　コンピュータやネットワークのセキュリティ上の弱点を発見するテスト手法の一つであり，システムを実際に攻撃して侵入を試みる。
ウ　ネットワークの管理者や利用者などから，巧みな話術や盗み聞き，盗み見などの手段によって，パスワードなどのセキュリティ上重要な情報を入手する。
エ　犯罪に関する証拠となり得るデータを保全し，その後の訴訟などに備える。

問 15 正解 完璧 直前チェック

DMZ上のコンピュータがインターネットからのpingに応答しないようにしたいとき，ファイアウォールのルールで“通過禁止”に設定するものはどれか。

ア　ICMP　　イ　TCPのポート番号21
ウ　TCPのポート番号110　　エ　UDPのポート番号123

問 16 正解 完璧 直前チェック

認証にクライアント証明書を用いるプロトコルはどれか。

ア　EAP-FAST　　イ　EAP-MD5　　ウ　EAP-TLS　　エ　EAP-TTLS

春

問14　エ

解説　**ディジタルフォレンジックス**は，パソコンやサーバなどのコンピュータ機器が犯罪や裁判での証拠となり得るときに，データを保全し賠償などに備えることや，内容を分析，鑑定するための手段や技術を指す。
ア：**電子透かし**の説明である。
イ：**擬似アタックテスト**の説明である。
ウ：**ソーシャルエンジニアリング**の説明である。

問15　ア

解説　**ping**は**ICMP**（Internet Control Message Protocol）を使用するため，ICMPを通過禁止にする。pingを使用することで，攻撃者はDMZ上のサーバの有無を知ることができる。
イ：TCPポート番号21は，**FTP**（File Transfer Protocol：ファイル転送プロトコル）の制御に使用される。FTPを禁止にする場合には，FTP（データ）のTCPポート番号20も通過禁止にする必要がある。
ウ：TCPポート番号110は，一般的に**POP3**（Post Office Protocol version3：メール受信用プロトコル）に使用される。
エ：UDPポート番号123は，**NTP**（Network Time Protocol）に使用される。

問16　ウ

解説　**EAP**（Extensible Authentication Protocol）は，PPP（Point to Point Protocol）用の認証プロトコルであり，認証にクライアント証明書を用いる方式である。EAPでは，各種の拡張認証方式を利用することができる。無線LANでは，Ether（データリンク層）のユーザ認証の規格であるIEEE 802.1xが採用されている。
ア，イ：認証にIDとパスワードを用いる方式である。証明書は使用しない。
エ：認証に証明書を用いるが，サーバ側でのみ証明書を用いる。

問 17

正解 □ 完璧 □ 直前チェック □

電子メールを暗号化する三つのプロトコルについて，公開鍵を用意する単位の適切な組合せはどれか。

	PGP	S/MIME	SMTP over TLS
ア	メールアドレスごと	メールアドレスごと	メールサーバごと
イ	メールアドレスごと	メールサーバごと	メールアドレスごと
ウ	メールサーバごと	メールアドレスごと	メールアドレスごと
エ	メールサーバごと	メールサーバごと	メールサーバごと

問 18

正解 □ 完璧 □ 直前チェック □

無線LANで用いられるSSIDの説明として，適切なものはどれか。

ア　48ビットのネットワーク識別子であり，アクセスポイントのMACアドレスと一致する。
イ　48ビットのホスト識別子であり，有線LANのMACアドレスと同様の働きをする。
ウ　最長32オクテットのネットワーク識別子であり，接続するアクセスポイントの選択に用いられる。
エ　最長32オクテットのホスト識別子であり，ネットワーク上で一意である。

問 19

正解 □ 完璧 □ 直前チェック □

IPv4ネットワークでIPアドレスを割り当てる際に，DHCPクライアントとDHCPサーバ間でやり取りされるメッセージの順序として，適切なものはどれか。

ア　DHCPDISCOVER，DHCPACK，DHCPREQUEST，DHCPOFFER
イ　DHCPDISCOVER，DHCPOFFER，DHCPREQUEST，DHCPACK
ウ　DHCPREQUEST，DHCPACK，DHCPDISCOVER，DHCPOFFER
エ　DHCPREQUEST，DHCPDISCOVER，DHCPOFFER，DHCPACK

問17　ア

解説

PGP（Pretty Good Privacy）：ファイルやメールを暗号化するためのソフトウェアである。メールアドレスごとに公開鍵を用意する。

S/MIME（Secure / Multipurpose Internet Mail Extensions）：MIME（電子メールの機能を拡張する規格）に暗号化とディジタル署名の機能を追加した規格のことである。メールアドレスごとに公開鍵を用意する。

SMTP over TLS：メールの送信・転送を行うSMTP（Simple Mail Transfer Protocol）に，転送路を暗号化するTLS（Transport Layer Security）を組み合わせたプロトコルである。SMTPはメールサーバ間のプロトコルであるため，メールサーバごとに公開鍵を用意する。

問18　ウ

解説

SSID（Service Set Identifier）：アクセスポイント内で同じグループ識別子をもつ端末同士だけが通信できるように，アクセスを制限するIDである。

ア：**BSSID**（Basic Service Set Identifier）の説明である。

イ：SSIDはアクセスポイントのグループであるため，有線LANのように自端末を識別するものではない。

エ：SSIDはホスト識別子ではない。**ネットワーク識別子**である。

問19　イ

解説

DHCP（Dynamic Host Configuration Protocol）：IPアドレスなど各種設定の自動割当てを行うプロトコルである。ほかに設定できる項目として，デフォルトゲートウェイ，サブネットマスク，DNSサーバなどがある。

DHCPがIPアドレスを割り当てる際には，以下の順序でメッセージをやり取りする。

DHCPDISCOVER：DHCPクライアントがDHCPサーバに対して情報の取得要求を行う。送信先は，ブロードキャストアドレスである。

DHCPOFFER：DISCOVERメッセージを受信したDHCPサーバは，DHCPクライアントに対して，IPアドレスなどの情報を送信（OFFER）する。

DHCPREQUEST：DHCPクライアントはDHCPサーバから提示されたIPアドレスなどの情報に問題がなければ，正式に情報の要求（REQUST）を行う。

DHCPACK：DHCPサーバは，DHCPクライアントに対して応答（ACK）を返し，DHCPクライアントはACKを受信することで完了となる。

問 20 正解 完璧 直前チェック

TCPのサブミッションポート（ポート番号587）の説明として，適切なものはどれか。

ア　FTPサービスで，制御用コネクションのポート番号21とは別にデータ転送用に使用する。
イ　Webアプリケーションで，ポート番号80のHTTP要求とは別に，サブミットボタンをクリックした際の入力フォームのデータ送信に使用する。
ウ　コマンド操作の遠隔ログインで，通信内容を暗号化するためにTELNETのポート番号23の代わりに使用する。
エ　電子メールサービスで，迷惑メール対策としてSMTPのポート番号25の代わりに使用する。

問 21 正解 完璧 直前チェック

“アカウント”表に対して，SQL文を実行したとき，“アカウント”表の全ての行が取得される入力パラメタはどれか。ここで，入力パラメタのエスケープ処理は行わない。また，“;”はSQL文の終端として解釈されるものとする。

アカウント

ID	ユーザ名	メールアドレス
A001	TARO JOHO	t-joho@email.org.jp
A002	JIRO JOHO	j-joho@email.org.jp
A003	HANAKO JOHO	h-joho@email.org.jp

〔SQL文〕

```
SELECT ID,ユーザ名,メールアドレス FROM アカウント
   WHERE ユーザ名='入力パラメタ';
```

ア　'OR'--'='--
イ　'OR ユーザ名='ユーザ名
ウ　'--OR 1=1
エ　¥'OR 1=1';--

問20　エ

解説 **TCPのサブミッションポート**は，ポート番号587を使用したメール送信専用ポートのことである。従来利用されてきたSMTPのポート番号25の代わりに使用する。SMTPのポート番号25は迷惑メールで使用されるといったセキュリティ上のリスクが高くなってきている。そのためメールを送信するプロバイダは，サブミッションポートを使用し，認証技術などを組み合わせてメール送信を行い，迷惑メールの送信を回避している。

問21　ア

解説 **SQL**のSELECT文で，特定の行を選択するときにWHERE句を用いる。
ア：WHERE　ユーザ名＝'' OR '--'='--';となる。ORの右'--'が等しいため，全ての行が選択される。よって，正解。
イ：WHERE　ユーザ名＝'' OR ユーザ名＝'ユーザ名';となる。ユーザ名という文字列を比較しているため，ORの右が一致しない。よって，選択されない。
ウ：WHERE　ユーザ名＝'' -- OR 1＝1';となる。--とORが構文として扱われないため選択されない。
エ：WHERE　ユーザ名＝'¥' OR 1＝1'となる。¥'により，'が区切りではなく文字列として扱われ一致しないため，選択されない。

春

問 22 正解 完璧 直前チェック

フェールセーフの考えに基づいて設計したものはどれか。

ア　乾電池のプラスとマイナスを逆にすると，乾電池が装填できないようにする。
イ　交通管制システムが故障したときには，信号機に赤色が点灯するようにする。
ウ　ネットワークカードのコントローラを二重化しておき，故障したコントローラの方を切り離しても運用できるようにする。
エ　ハードディスクにRAID1を採用して，MTBFで示される信頼性が向上するようにする。

問 23 正解 完璧 直前チェック

アジャイルソフトウェア開発などで導入されている“ペアプログラミング”の説明はどれか。

ア　開発工程の初期段階に要求仕様を確認するために，プログラマと利用者がペアとなり，試作した画面や帳票を見て，相談しながらプログラムの開発を行う。
イ　効率よく開発するために，2人のプログラマがペアとなり，メインプログラムとサブプログラムを分担して開発を行う。
ウ　短期間で開発するために，2人のプログラマがペアとなり，作業と休憩を交代しながら長時間にわたって連続でプログラムの開発を行う。
エ　品質の向上や知識の共有を図るために，2人のプログラマがペアとなり，その場で相談したりレビューしたりしながら，一つのプログラムの開発を行う。

春

問22　イ

解説　**フェールセーフ**とは，システムの障害や誤操作が発生することを想定し，発生した際の影響を最小限にするようにシステムを設計することである。踏み切りを例とすると，踏み切りが故障した場合には，電車との衝突事故を回避するため，自動的に遮断機を下ろし，事故を未然に防ぐ方向に動作することである。

ア：極を逆にした乾電池が入らないようにすることは，誤操作が発生しないようにする考え方（**フールプルーフ**）である。

ウ：故障した部分を切り離してシステムの運用を継続するという考え方は，**フォールトトレランス**の考え方である。

エ：RAID1（**ミラーリング**）することは，故障率を低下させる考え方である。

問23　エ

解説

アジャイルソフトウェア開発：ソフトウェア要求仕様の変更に対して機敏に対応し，顧客に価値あるソフトウェアを迅速に提供することを目的とするソフトウェア開発方法論。

ペアプログラミング：2人のプログラマがペアになって，コーディング担当とチェックやアドバイスをする担当に分かれて，相談したりレビューしたりしながら，一つのプログラムの開発を行うこと。

問 24 正解 完璧 直前チェック

ITサービスマネジメントの情報セキュリティ管理プロセスに対して，JIS Q 20000-1が要求している事項はどれか。

ア　CMDBに記録されているCIの原本を，物理的又は電子的にセキュリティが保たれた書庫で管理しなければならない。
イ　潜在的な問題を低減させるために，予防処置をとらなければならない。
ウ　変更要求が情報セキュリティ基本方針及び管理策に与える潜在的影響を評価しなければならない。
エ　変更要求の受入れについての意思決定では，リスク，事業利益及び技術的実現可能性を考慮しなければならない。

問 25 正解 完璧 直前チェック

組織体が情報システムにまつわるリスクに対するコントロールを適切に整備・運用する目的として，“システム管理基準”に示されているものはどれか。

ア　システム監査業務の品質を確保し，有効かつ効率的に監査を実施するため
イ　情報システムが，組織体の目的を実現するように安全，有効かつ効率的に機能するため
ウ　情報セキュリティに係るリスクのマネジメントが効率的に実施されるよう，リスクマネジメントに基づくコントロールの整備・運用の状況を評価するため
エ　リスクに対するコントロールをシステム監査人が評価し，保証又は助言を行い，ITガバナンスの実現に寄与するため

春

問24　ウ

解説

ア：JIS Q 20000-1 9.1 構成管理に要求事項が定義されている。
イ：JIS Q 20000-1 8.3 問題管理に要求事項が定義されている。
ウ：JIS Q 20000-1 6.6 情報セキュリティ管理に要求事項が定義されている。
エ：JIS Q 20000-1 9.2 変更管理に要求事項が定義されている。

問25　イ

解説　**システム管理基準**とは，組織体が情報システムにまつわるリスクに対するコントロールを適切に整備・運用する目的として経済産業省が策定したガイドラインである。具体的には以下がある。

・情報システムが，組織体の経営方針及び戦略目標の実現に貢献するため
・情報システムが，組織体の目的を実現するように安全，有効かつ効率的に機能するため
・情報システムが，内部又は外部に報告する情報の信頼性を保つように機能するため
・情報システムが，関連法令，契約又は内部規程等に準拠するようにするため

システム監査基準：情報システムを適切に管理・運用することを目的とした基準。具体的には以下がある。

・システム監査基準の品質を確保し，有効かつ効率的に監査を実施する
・リスクコントロールがリスクアセスメントに基づいて整備・運用されているかをシステム監査人が評価し，保証・助言を行い，ITガバナンスの実現に寄与するため

情報セキュリティ監査基準：情報資産を適切に管理・運用することを目的とした基準。具体的には以下がある。

・情報セキュリティに係るリスクマネジメントが効果的に実施されるように，リスクマネジメントに基づくコントロールの整備・運用の状況を評価する

ア，エ：システム監査基準に示されている。
ウ：情報セキュリティ監査基準に示されている。