問題

問 1

正解 完璧 直前CHECK

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，認証対象の各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，認証対象の各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1　エ

シングルサインオン（SSO）：1回のID／パスワード入力で，認証が必要な複数のアプリケーションを利用可能とすること．Webのシングルサインオンの場合，一度認証をするとアクセス権を有する他のWebサーバへのアクセス時にID／パスワード入力することなくアクセスできる．**リバースプロキシ方式**とWebサーバに**エージェント**（SSOモジュール）をインストールする方式がある．

クッキー（Cookie）：WebサーバからWebブラウザを通じて，訪問者のコンピュータに一時的にデータを書き込んで保存させる仕組み．シングルサインオンを利用する場合，クッキーには有効期間を設定し，認証結果，セッション情報，ユーザに関する情報などを記録しておく．

リバースプロキシ：特定のサーバの代理として，サーバへの要求を中継するプロキシサーバ．代行されているサーバへのアクセスは，すべてリバースプロキシを経由する．

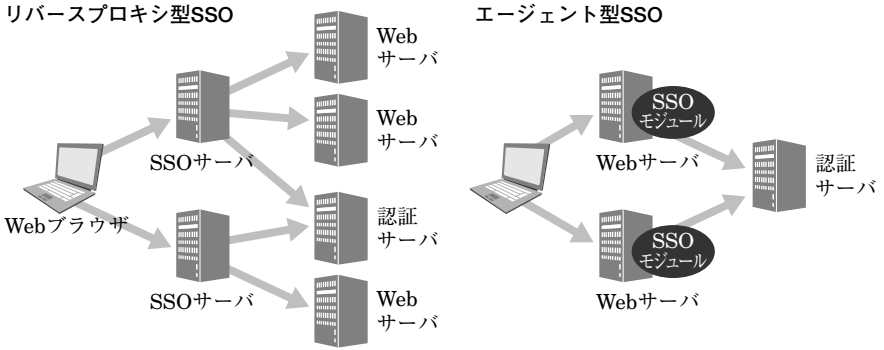


図　リバースプロキシ型とエージェント型

ア：クッキーはクライアントに保存される．

イ：クッキーは同じドメインでの読取りが可能なため，認証対象の各サーバは同じインターネットドメインに配置する．

ウ：リバースプロキシを使ったシングルサインオンでは，仕組み上，同じインターネットドメインにWebサーバが配置される．

問2

正解 完璧 直前CHECK

作成者によってディジタル署名された電子文書に，タイムスタンプ機関がタイムスタンプを付与した．この電子文書を公開する場合のタイムスタンプの効果のうち，適切なものはどれか．

ア　タイムスタンプを付与した時刻以降に，作成者が，電子文書の内容をほかの電子文書へコピーして流用することを防止する．
イ　タイムスタンプを付与した時刻以降に，第三者が，電子文書の内容をほかの電子文書へコピーして流用することを防止する．
ウ　電子文書が，タイムスタンプの時刻以前に存在したことを示し，作成者が，電子文書の作成を否認することを防止する．
エ　電子文書が，タイムスタンプの時刻以前に存在したことを示し，第三者が，電子文書を改ざんすることを防止する．

問3

正解 完璧 直前CHECK

FIPS 140-2を説明したものはどれか．

ア　暗号モジュールのセキュリティ要求事項
イ　情報セキュリティマネジメントシステムに関する認証基準
ウ　ディジタル証明書や証明書失効リストの標準仕様
エ　無線LANセキュリティ技術

問4

正解 完璧 直前CHECK

米国NISTが制定したAESにおける鍵長の条件はどれか．

ア　128ビット，192ビット，256ビットから選択する．
イ　256ビット未満で任意に指定する．
ウ　暗号化処理単位のブロック長より32ビット長くする．
エ　暗号化処理単位のブロック長より32ビット短くする．

問2　ウ

タイムスタンプ：単にタイムスタンプといった場合，ファイルなどの電子データにおいて，その作成や更新などが行われた日時を示す情報を意味する．**タイムスタンプ機関**によるタイムスタンプは，電子データに対して正確な日時情報を付与し，その時点での電子データの**存在証明**と**非改ざん証明**を行う仕組みあるいは技術を意味することがある．タイムスタンプは**電子公証**，**電子署名法**において利用され，知的財産やプレスリリースといった新規性の証明や発行日時の証明が必要な電子文書に付与する．タイムスタンプ技術の国際標準として**IETF RFC 3161**（Time Stamp Protocol）という規格がある．

ア，イ：タイムスタンプでは文書のコピーを防止することはできない．

エ：改ざんすることは防止できない．タイムスタンプによる効果は改ざんされていないことの証明である．

問3　ア

FIPS 140-2：暗号モジュールに関するセキュリティ要件仕様を規定する米国連邦標準規格．

イ：**BS 7799-2**や国内規格の**ISMS認証基準Ver.2.0**の後継として開発された国際規格および国内規格として，**ISO 27001**，**JIS Q 27001**がある．

ウ：インターネットのための**X.509 公開鍵基盤**（PKI）に対する標準がある．

エ：**IEEE 802.11**無線LANの国際規格の中では，セキュリティ技術として**SSID**（Service Set Identifier），**MACアドレスフィルタリング**，**WEP**（Wired Equivalent Privacy），**WPA2**（Wi-Fi Protected Access 2）などがある．

問4　ア

AES：米国国立標準技術研究所（NIST）が制定した共通鍵暗号方式．ブロック長は128ビットで鍵長は128ビット，192ビット，256ビットの三つが利用できる．DESに代わる暗号標準規格の公募で採用された．

問 5

正解 完璧 直前CHECK

JIS Q 27001:2006における情報システムのリスクとその評価に関する記述のうち，適切なものはどれか．

ア　脅威とは，脆弱性が顕在化する確率のことであり，情報システムに組み込まれた技術的管理策によって決まる．

イ　脆弱性とは，情報システムに対して悪い影響を与える要因のことであり，自然災害，システム障害，人為的過失及び不正行為に大別される．

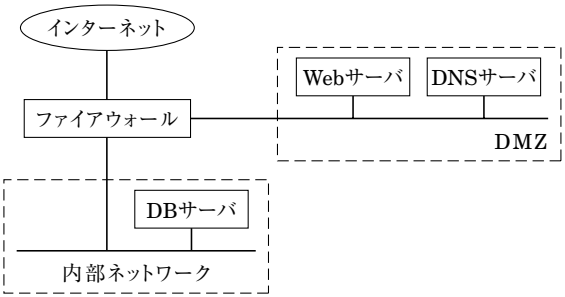
ウ　リスクの特定では，脅威が情報資産の脆弱性に付け込み，情報資産に与える影響を特定する．

エ　リスク評価では，リスク回避とリスク低減の二つに評価を分類し，リスクの大きさを判断して対策を決める．

問 6

正解 完璧 直前CHECK

DMZ上に公開しているWebサーバで入力データを受け付け，内部ネットワークのDBサーバにそのデータを蓄積するシステムがある．インターネットからDMZを経由してなされるDBサーバへの不正侵入対策の一つとして，DMZと内部ネットワークとの間にファイアウォールを設置するとき，最も有効な設定はどれか．



ア　DBサーバの受信ポート番号を固定し，WebサーバからDBサーバの受信ポート番号への通信だけをファイアウォールで通す．

イ　DMZからDBサーバへの通信だけをファイアウォールで通す．

ウ　Webサーバの発信ポート番号は任意のポート番号を使用し，ファイアウォールでは，いったん終了した通信と同じ発信ポート番号を使った通信を拒否する．

エ　Webサーバの発信ポート番号を固定し，その発信ポート番号からの通信だけをファイアウォールで通す．

問5　ウ

JIS Q 27001:2006：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）の確立，導入，運用，監視，レビュー，維持及び改善のための要求事項が規定されている．

ア：**脅威**とは，システムまた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または資産グループが持つ弱点である．

エ：**リスク対応**の選択肢については，リスクの回避，リスクの最適化，リスクの移転，リスクの保有の四つがある．

問6　ア

DMZ：インターネット（組織の外部）とイントラネット（組織の内部）の間にある隔離された区画のネットワーク領域．外部に公開するサーバやプロキシサーバなどが置かれる．停戦した地域に設定される「非武装地帯」をもとにした用語．

不正侵入：脆弱性（セキュリティホール）を突いて，本来は外部からのアクセスが許されていないイントラネット上のホストへアクセスすること．組織内のパソコンやサーバにアクセスされると，データの改ざんや破壊，個人情報や企業秘密の盗難の恐れがある．

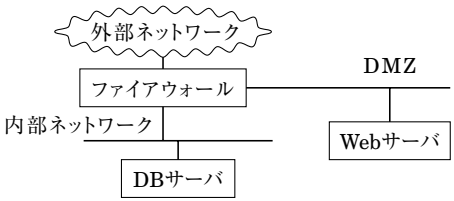
不正侵入対策：ファイアウォールを設置して外部からの通信を遮断する，OSやソフトへパッチを適用して最新の状態にしておくなどの対策がある．不正侵入を試みる特有の攻撃パターンの検知および防御の技術が開発されており，**不正侵入検知**（IDS）や**不正侵入防御**（IDP・IPS）と呼ばれている．

ファイアウォールは，内部ネットワークと外部ネットワークの間に設置される．内部ネットワークの情報システムを保護するために，内部ネットワークと外部ネットワークの間を通過しようとするパケットをセキュリティポリシに従った設定ルールに従って制御する．

問題文から，内部ネットワークのDBサーバを外部ネットワークから保護し，DBサーバと連携するDMZ上のWebサーバからの通信を許可する設定を選択すればよい．

イ，ウ：Webサーバの発信ポートではなく，DBサーバの受信ポートの設定でなければ，DBサーバを保護する設定とならない．

エ：この設定では，外部ネットワークからDBサーバにパケットが到達してしまう．



問題

問 7

正解 完璧 直前CHECK

ファイアウォールにおいて，自ネットワークのホストへの侵入を防止する対策のうち，IPスプーフィング（spoofing）攻撃に有効なものはどれか．

ア　外部から入るTCPコネクション確立要求パケットのうち，外部へのインターネットサービスの提供に必要なもの以外を阻止する．

イ　外部から入るUDPパケットのうち，外部へのインターネットサービスの提供や利用したいインターネットサービスに必要なもの以外を阻止する．

ウ　外部から入るパケットのあて先IPアドレスが，インターネットとの直接の通信をすべきでない自ネットワークのホストのものであれば，そのパケットを阻止する．

エ　外部から入るパケットの送信元IPアドレスが自ネットワークのものであれば，そのパケットを阻止する．

問 8

正解 完璧 直前CHECK

SQLインジェクション攻撃を防ぐ方法はどれか．

ア　入力から，上位ディレクトリを指定する文字列（../）を取り除く．

イ　入力中の文字がデータベースへの問合せや操作において特別な意味をもつ文字として解釈されないようにする．

ウ　入力にHTMLタグが含まれていたら，解釈，実行できないほかの文字列に置き換える．

エ　入力の全体の長さが制限を超えていたときは受け付けない．

問 9

正解 完璧 直前CHECK

通信を要求したPCに対し，ARPの仕組みを利用して実現できる通信の可否の判定方法のうち，最も適切なものはどれか．

ア　PCにインストールされているソフトウェアを確認し，登録されているソフトウェアだけがインストールされている場合に通信を許可する．

イ　PCのMACアドレスを確認し，事前に登録されているMACアドレスをもつ場合だけ通信を許可する．

ウ　PCのOSのパッチ適用状況を確認し，最新のパッチが適用されている場合だけ通信を許可する．

エ　PCのマルウェア対策ソフトの定義ファイルを確認し，最新になっている場合だけ通信を許可する．

問7　エ

ファイアウォール：自ネットワークへの外部ネットワークからの侵入を防ぐシステム．**パケットフィルタリング型ファイアウォール**では，パケットのヘッダに記述された送信元IPアドレス，宛先IPアドレス，送信元ポート番号，宛先ポート番号に基づいて，そのパケットの内部もしくは外部への通過を制御（**フィルタリング**）する．

IPスプーフィング：攻撃元を隠すために，偽の送信元IPアドレスを装ったパケットを作成して送ること．

外部から内部へ向かうパケットの送信元IPアドレスは外部のネットワークアドレスであるはずなので，送信元が自ネットワークのIPアドレスである場合，そのIPアドレスは詐称されていると考えて，そのパケットの通過を阻止する．

問8　イ

SQLインジェクション攻撃：データベースと連動したWebサイトにおいて，データベースへの問合せや操作を行うプログラムにパラメータとしてSQL文の断片を入力することで，データベースの改ざんや不正な情報の入手を実行する攻撃．

ア：**ディレクトリトラバーサル**の攻撃を防ぐ方法の説明である．ディレクトリトラバーサルはOSや言語処理系に依存する脆弱性を突く攻撃である．ファイル名やディレクトリ名に相対パスを使用することで，プログラムが意図していないファイルやディレクトリへのアクセスを実行する．

ウ：**クロスサイトスクリプティング**の攻撃を防ぐ方法の説明である．クロスサイトスクリプティングは，入力値を基に動的にHTML文書を作成することができるWebサイトの弱点を利用した攻撃である．入力に含まれている**HTMLタグ**をほかの文字列に置換（**サニタイジング**）する対策が有効である．

エ：**バッファオーバフロー**攻撃を防ぐ方法の説明である．バッファオーバフローは，プログラムが確保したメモリサイズを越えた文字列の入力が領域のあふれ（オーバフロー）を引き起こし，予期しない動作を発生させる攻撃である．

問9　イ

ARP：あて先の**IPアドレス**から**MACアドレス**を求めるためのプロトコル．

ARP認証は，ネットワークに流れるARPフレームを監視し，認証サーバに登録されているMACアドレスであれば正しいARP情報を送信して通信を可能にし，未登録のMACアドレスを発見すると偽のARP情報を送信して通信不能にする．

MACアドレス認証は，ネットワークカード（ポート）に固有のMACアドレスを用いてアクセス制御を行う認証方式である．

問 10

正解 完璧 直前CHECK

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，暗号化及び復号に使用する鍵が同一である．

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

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 11

正解 完璧 直前CHECK

社内とインターネットの接続点にパケットフィルタリング型ファイアウォールを設置したネットワーク構成において，社内のPCからインターネット上のSMTPサーバに電子メールを送信するとき，ファイアウォールで通過許可とするTCPパケットのポート番号の組合せはどれか．

		送信元	あて先	送信元 ポート番号	あて先 ポート番号
ア	発信	PC	SMTPサーバ	25	1024以上
	応答	SMTPサーバ	PC	1024以上	25
イ	発信	PC	SMTPサーバ	1024以上	25
	応答	SMTPサーバ	PC	25	1024以上
ウ	発信	SMTPサーバ	PC	110	1024以上
	応答	PC	SMTPサーバ	1024以上	110
エ	発信	SMTPサーバ	PC	1024以上	110
	応答	PC	SMTPサーバ	110	1024以上

問10　イ

ア：**AES**は共通鍵暗号方式，**RSA**は公開鍵暗号方式の一種である．

ウ：鍵の使い方が逆である．公開鍵暗号方式を通信内容の秘匿に使用する場合には，送信者は暗号化鍵として通信相手の公開鍵を用い，受信者は復号鍵として自分の秘密鍵を用いる．

エ：**ディジタル署名**には公開鍵暗号が使用されている．

問11　イ

パケットフィルタリング型ファイアウォール：OSI参照モデル第3層のIPパケットや第4層のTCP/UDPパケットのヘッダの情報（IPアドレス，ポート番号）に基づいてパケットを通過させるか廃棄するかの判断を行うタイプのファイアウォール．

社内のPCからインターネット上の**SMTPサーバ**に電子メールを送信するということは，発信時の送信元はPC，あて先はSMTPサーバであり，SMTPの送信元ポート番号は**25/TPC**である．それに対して応答時の送信元はSMTPサーバであり，あて先はPCとなる．

なお，1024以上のポート番号は，使用するアプリケーションよって設定されるポート番号である．

表　よく利用されるポート番号とプロトコル

ポート番号	アプリケーション	用途
20	ftp-data	ファイル転送(データ本体)
21	ftp	ファイル転送(コントロール)
22	ssh	シェル：SSH(セキュア)
23	telnet	シェル：telnet
25	smtp	メール送受信：SMTP
53	domain	DNS
80	http	WWW
110	pop3	メール受信(POP)
143	imap	メール(IMAP)
443	https	WWW(セキュア)

問 12

正解 □ 完璧 □ 直前CHECK □

送信元を詐称した電子メールを拒否するために，SPF（Sender Policy Framework）の仕組みにおいて受信側が行うことはどれか．

ア　Resent-Sender:，Resent-From:，Sender:，From:などのメールヘッダ情報の送信者メールアドレスを基に送信メールアカウントを検証する．
イ　SMTPが利用するポート番号25の通信を拒否する．
ウ　SMTP通信中にやり取りされるMAIL FROMコマンドで与えられた送信ドメインと送信サーバのIPアドレスの適合性を検証する．
エ　付加されたディジタル署名を受信側が検証する．

問 13

正解 □ 完璧 □ 直前CHECK □

ISP管理下の動的IPアドレスを割り当てられたPCからのスパムメール送信を防止する対策OP25Bはどれか．

ア　管理下の動的IPアドレスから，管理外のグローバルIPアドレスへのPOP通信を拒否する．
イ　管理下の動的IPアドレスから，管理外のグローバルIPアドレスへのSMTP通信を拒否する．
ウ　メールサーバで，受信メールのあて先電子メールアドレスが管理外のドメインを指す場合，電子メールの受信を拒否する．
エ　メールサーバで，スパムメール受信時に送信元の電子メールアドレスをブラックリストに登録しておき，スパムメール送信元からの電子メールの受信を拒否する．

問 14

正解 □ 完璧 □ 直前CHECK □

無線LANにおける通信の暗号化の仕組みに関する記述のうち，適切なものはどれか．

ア　EAPは，クライアントPCとアクセスポイントとの間で，あらかじめ登録した共通鍵による暗号化通信を実現する．
イ　ESS-IDは，クライアントPCごとの秘密鍵を定めたものであり，公開鍵暗号方式による暗号化通信を実現する．
ウ　WEPでは，クライアントPCとアクセスポイントとの間で公開鍵暗号方式による暗号化通信を実現できる．
エ　WPA2では，IEEE802.1Xの規格に沿って機器認証を行い，動的に更新される暗号化鍵を用いて暗号化通信を実現できる．

問12　ウ

SPF（Sender Policy Framework）：差出人のメールアドレスが他のドメインになりすましていないかどうかを検出する，電子メールにおける送信ドメイン認証の仕組み．

ア：**スパムメール**は実在しないドメインのメールアカウントを使用することが多いことから，スパムメールの判定に利用されることがある．メールヘッダ情報の送信者メールアドレスが実在するメールアカウントに詐称されているとチェックできない．

イ：**OP25B**（Outbound Port 25 Blocking）の説明である．外部のSMTPサーバへの通信を遮断することによって，スパムメールの送信やウイルスの拡散を防ぐために，主にISPで行われる．

エ：**DKIM**（Domain Keys Identified Mail）の説明である．送信元メールサーバがメールに付加したディジタル署名を受信側がチェックすることで送信元の正当性を確認する．

問13　イ

OP25B（Outbound Port 25 Blocking）は，管理下の動的IPアドレスからの**SMTP通信**（TCP 25番ポート）を拒否することでスパムメールの送信を防止する対策である．ウイルス感染者や迷惑メール送信業者が，自分のPCまたはサーバから故意あるいは無意識に行うメール送信を阻止できる．

問14　エ

EAP（Extensible Authentication Protocol）：PPP接続を拡張した認証プロトコル．ユーザID／パスワード以外にも，**スマートカード**（ICカード）や**ディジタル証明書**など様々な認証方式をサポートしている．**EAP-TLS**，**EAP-TTLS**などがある．

ESS-ID：同じ**SSID**を登録した無線LAN端末およびアクセスポイントだけが相互に通信できる．IEEE 802.11におけるアクセスポイントに付ける識別子である．

WEP：無線LANで使われる通信の暗号化技術．暗号化に64ビットもしくは128ビットの共通鍵が使用される．WEPには脆弱性が発見されている．

WPA2：米国のNISTが定めた暗号化標準のAESを採用し，128～256ビットの可変長鍵を利用した強力な暗号化が可能である．IEEE 802.11i規格により機器認証を行い，エンタープライズモードでは動的セッション鍵を使用する．

問題

問 15

正解 □ 完璧 □ 直前CHECK □

SSLの利用に関する記述のうち，適切なものはどれか．

ア　SSLで使用する個人認証用のディジタル証明書は，IC力ードなどに格納できるので，格納場所を特定のPCに限定する必要はない．

イ　SSLはWebサーバを経由した特定の利用者間の通信のために開発されたプロトコルであり，Webサーバ提供者への事前の利用者登録が不可欠である．

ウ　SSLを利用するWebサーバのディジタル証明書にはIPアドレスの組込みが必須なので，WebサーバのIPアドレスを変更する場合は，ディジタル証明書を再度取得する必要がある．

エ　日本国内では，SSLで使用する共通鍵の長さは，128ビット未満に制限されている．

問 16

正解 □ 完璧 □ 直前CHECK □

WAF（Web Application Firewall）のブラックリスト又はホワイトリストの説明のうち，適切なものはどれか．

ア　ブラックリストは，脆弱(ぜい)性のあるサイトのIPアドレスを登録したものであり，該当する通信を遮断する．

イ　ブラックリストは，問題のある通信データパターンを定義したものであり，該当する通信を遮断するか又は無害化する．

ウ　ホワイトリストは，脆弱性のないサイトのFQDNを登録したものであり，該当する通信を遮断する．

エ　ホワイトリストは，問題のある送信データをどのように無害化するかを定義したものであり，該当するデータを無害化する．

問 17

正解 □ 完璧 □ 直前CHECK □

1台のサーバと複数台のクライアントが，100Mビット／秒のLANで接続されている．業務のピーク時には，クライアント1台につき1分当たり600kバイトのデータをサーバからダウンロードする．このとき，同時使用してもピーク時に業務を滞りなく遂行できるクライアント数は何台までか．ここで，LANの伝送効率は50％，サーバ及びクライアント内の処理時間は無視できるものとし，1Mビット／秒＝10^6ビット／秒，1kバイト＝1,000バイトとする．

ア　10　　イ　625　　ウ　1,250　　エ　5,000

問15　ア

SSL：インターネット上でデータを暗号化して送受信する方法の一つ．公開鍵暗号や秘密鍵暗号，ディジタル証明書，ハッシュ関数などのセキュリティ技術を組み合わせ，データの盗聴や改ざん，なりすましを防ぐことができる．

イ：特定の利用者間の通信ではないので，事前の利用者登録は不要である．Webサーバと利用者間の通信を暗号化することで情報漏えいを防ぐ．

ウ：**ディジタル証明書**にIPアドレスの組込みは不要である．

エ：現在は，共通鍵の長さは128ビット未満に制限されていない．1998年12月以前，アメリカ合衆国からアメリカ合衆国およびカナダ以外へ輸出する場合には，合衆国政府から特別な輸出許可を受けない限り，利用可能な鍵長は40ビットまでという制限があった．

問16　イ

WAF（Web Application Firewall）：Webアプリケーションのやり取りを把握・管理することによって不正侵入を防御するファイアウォール．プログラムに渡される入力内容などを直接に検査することによって，不正と見なされたアクセス要求を遮断する仕組みが採用されている．クライアントの操作するWebブラウザとWebサーバ間に介在し，ブラウザとの直接的なやり取りをWAFが受け持つ．**SQLインジェクション**や**クロスサイトスクリプティング**，**強制ブラウジング**といった要求はWAFが遮断する．

ブラックリストには問題のある通信データパターンが定義され，**ホワイトリスト**には問題のない正規の通信データパターンが定義されている．それ以外の通信はいわばグレーゾーンであり，ホワイトリストで許可してそれ以外のグレーゾーンを含む通信を拒否するか，ブラックリストのみ拒否してそれ以外のグレーゾーンを含む通信を許可するのかを考えなければならない．

日々新しいWebアプリケーションは増えており，新しい攻撃もあるため，運用まで考慮すると，ブラックリストとホワイトリストの優劣はつけ難い．

問17　イ

クライアント数は，（1秒間の実効データ転送速度）÷（クライアント1台の1秒間のデータ量）で求められる．

$$(0.5 \times 100 \times 10^6 \div 8) \div (600 \times 10^3 \div 60) = (6.25 \times 10^6) \div (1 \times 10^4) = 625$$

伝送効率：ネットワーク回線の単位時間あたりに転送できるデータ量の比率．通信量が増えると，衝突が発生して低下することがある．

問題

問 18

正解 □ 完璧 □ 直前CHECK □

LANの制御方式に関する記述のうち，適切なものはどれか．

ア　CSMA/CD方式では，単位時間当たりの送出フレーム数が増していくと，衝突の頻度が増すので，スループットはある値をピークとして，その後下がる．

イ　CSMA/CD方式では，一つの装置から送出されたフレームが順番に各装置に伝送されるので，リング状のLANに適している．

ウ　TDMA方式では，伝送路上におけるフレームの伝搬遅延時間による衝突が発生する．

エ　トークンアクセス方式では，トークンの巡回によって送信権を管理しているので，トラフィックが増大すると，CSMA/CD方式に比べて伝送効率が急激に低下する．

問 19

正解 □ 完璧 □ 直前CHECK □

DNSSECの説明として，適切なものはどれか．

ア　DNSサーバへのDoS攻撃を防止できる．

イ　IPsecによる暗号化通信が前提となっている．

ウ　代表的なDNSサーバの実装であるBINDの代替として使用する．

エ　ディジタル署名によってDNS応答の正当性を確認できる．

問18　ア

CSMA/CD方式：LANの通信状況を監視して，ネットワークが空いたタイミングで送信を開始する方式．複数のノードが同時に送信を開始すると，ケーブル内でデータが衝突して壊れるので，両者は送信を中止し，ランダムな時間を待ってから送信を再開する．トラフィックが増大すると伝送効率が急激に低下する．

TDMA方式：一つの周波数を一定時間ごとに区切って，複数の発信者が短時間ずつ共有する方式．

イ：**トークンアクセス方式**（トークンパッシング方式）の説明である．トークンと呼ばれる送信権を持つ装置からのみ送信が行われる．

ウ：**CSMA/CD方式**の説明である．**TDMA方式**では，伝送遅延時間による衝突は発生しない．

エ：トークンアクセス方式ではCSMA/CDのような衝突は発生しない．したがって，トラフィックが増大しても，CSMA/CD方式に比べて伝送効率の低下は少ない．

問19　エ

DNSSEC（Domain Name System Security Extension）：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という，DNSサーバに一時的に保存（キャッシュ）してあるホスト名とIPアドレスの対応情報を偽の情報に書き換える攻撃があり，DNSSECはこの攻撃に対してDNS情報を正しく保つための方法の一つである．DNSキャッシュが不正な情報で汚染されると，クライアントのWebブラウザは偽のWebサイトに誘導されてしまうといったことが起こり，情報漏えいやウイルス感染などの2次的な被害を生じる恐れがある．

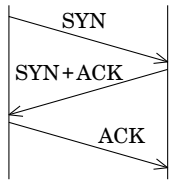
問題

問 20

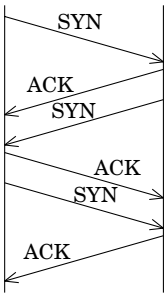
正解 完璧 直前CHECK

TCPのコネクション確立方式である3ウェイハンドシェイクを表す図はどれか.

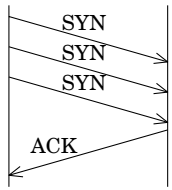
ア



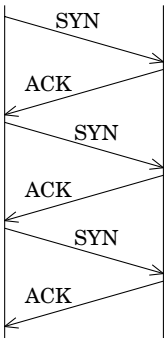
イ



ウ



エ



問 21

正解 完璧 直前CHECK

和両立である表R（ID，NAME），S（NO，NAMAE）がある．差集合R−Sを求めるSELECT文とするために，a に入れるべき適切な字句はどれか．ここで，下線部は主キーを表す．また，NAMEとNAMAEはNULL不可とする．

```
SELECT * FROM R WHERE [ a ]
    (SELECT * FROM S WHERE S.NO = R.ID AND S.NAMAE = R.NAME)
```

ア EXISTS　　イ NOT EXISTS　　ウ NOT IN　　エ R.ID NOT IN

問20　ア

TCPは，通信のコネクションの要求元と要求先で相互の状況を確認してからデータを送り，データの到着を確認してから次のデータを送るというコネクション確立方式の通信を行う．要求元は要求先に**SYN**（SYNchronization：同期）を送信する．要求先はそれを受けて，要求を受付けた**ACK**（ACKnowledgement：確認応答）とSYNを返信する．それを受けて要求元はACKを送る．この送信準備を**3ウェイハンドシェイク**という．要求先の確認を取ることを**ネゴシエーション**という．

ちなみに，**UDP**は**コネクションレス方式**であるので，送信元は送信先へ直ちにデータを送信する．UDPには再送機能やフロー制御機能はない．

問21　イ

EXISTS：副問合せによって返されたレコードが一つでもあれば真，一つもなければ偽を返す．

NOT EXISTS：副問合せによって返されたレコードがなければ真，一つでもあれば偽を返す．

NOT IN：副問合せによって返されたレコードが複数あり，その値のいずれとも同じではないという条件．

集合Rから集合Sと共通する要素を取り除いた行を選択する処理である．SQL文の（ ）内では集合RとSの共通要素を求めているので，それらとは異なる要素を条件とする句が空欄aには入る．

問題

問 22

正解 □ 完璧 □ 直前CHECK □

ソフトウェアの保守作業の効率向上施策として，最も適切なものはどれか．

ア　エンドユーザによる動作確認テスト
イ　コーディング規約に準拠したプログラムの作成
ウ　最適化コンパイルによる性能改善
エ　発生したバグの要因分類による傾向分析

問 23

正解 □ 完璧 □ 直前CHECK □

SOA（Service Oriented Architecture）でサービスを設計する際の注意点のうち，適切なものはどれか．

ア　可用性を高めるために，ステートフルなインタフェースとする．
イ　業務からの独立性を確保するために，サービスの命名は役割を表すものとする．
ウ　業務の変化に対応しやすくするために，サービス間の関係は疎結合にする．
エ　セキュリティを高めるために，一度開発したサービスは再利用しない方がよい．

問22　イ

ソフトウェア保守：ソフトウェアを改良，最適化していく作業．システムの使用開始後に発見された問題点やバグの修正および改善，機能追加を含む．作業時にはソースコードの修正作業が行われるため，コーディング規約に準拠したプログラムの作成が保守作業の効率向上施策として最も適切である．

ソフトウェア保守プロセスは**JIS X 0160**（ソフトウェアライフサイクルプロセス）でプロセスが規定されている．その詳細は，**JIS X 0161:2008**（ソフトウェアライフサイクルプロセス－保守）で規定されている．

ア：実際の現場で使用することによってユーザ視点での改良点の発見に役立つが，ソフトウェア保守作業そのものの効率向上とは直接関係ない．

ウ：ソフトウェア自体の性能改善であり，保守作業の効率向上とは直接の関係はない．

エ：未知のバグの推測に役立つが，保守作業そのものの効率向上とは直接の関係はない．

問23　ウ

SOA（Service Oriented Architecture，サービス指向アーキテクチャ）：問題では言及されていないが，「サービスは適切な粒度（オペレーションの数）を有すべき」「オペレーションは並行性を考慮して設計すべき」といったいくつもの原則がある．

ア：再利用を考慮して**ステートレス**なインターフェースとすべきである．業務の変化への対応を考慮して，**ステートフル**（状態と相互関係を重視する）インターフェースにはしない．

イ：サービスの命名はビジネス概念を表すものとする．サービス名には名詞，オペレーションには動詞が良いとされている．

エ：SOAにおいては，サービスを再利用することにより効率や利便性を得ることができる．

問 24

正解 □ 完璧 □ 直前CHECK □

レプリケーションが有効な対策となるものはどれか.

ア　悪意によるデータの改ざんを防ぐ.
イ　コンピュータウイルスによるデータの破壊を防ぐ.
ウ　災害発生時にシステムが長時間停止するのを防ぐ.
エ　操作ミスによるデータの削除を防ぐ

問 25

正解 □ 完璧 □ 直前CHECK □

請負契約でシステム開発を委託している案件について，委託元のシステム監査人の指摘事項に該当するものはどれか.

ア　委託した開発案件の品質を委託元の管理者が定期的にモニタリングしている
イ　委託元の管理者が委託先の開発担当者を指揮命令している.
ウ　契約書に機密保持のための必要事項が盛り込まれている.
エ　特定の委託先との契約が長期化しているので，その妥当性を確認している.

問24　ウ

レプリケーション：データベースシステムの管理機能の一つ．データベースの複製を維持する仕組み．マスタデータベースと複製（レプリカ）データベースが，常に同じ内容となるようにデータ更新が行われる．**同期複製**の場合には，すべてのデータベースで常に同じデータになる．**非同期複製**では一定の間隔で同期が行われるため，ある時点で見た場合は厳密には同じ内容とはならない．

　レプリケーションの構成は主に二つある．一つは，マスタサーバのみが更新系のクエリを受付けてスレーブはマスタから伝搬されたもの以外の更新処理は行わない**マスタスレーブ**である．もう一つは，どのサーバでも更新系のクエリを受付ける**マルチマスタ**である．

ア：データベースの更新権限があれば，悪意の有無に関係なく改ざんされたデータがレプリケーションにも反映される．

イ：コンピュータウイルスによるデータの破壊は防げないと考えたほうがよい．一般に，データベースのマスタとレプリカはほぼ同一構成のサーバであり，同一のネットワークか相互に通信可能なネットワークに配置されるため，両方感染する可能性がある．

ウ：地理的に離れた場所にレプリカがあれば，すぐに災害発生直前のデータでシステムの再開が可能である．

エ：誤った操作や誤ったSQL文など，ミスによる更新もレプリカに反映される．したがって，データの削除や変更を防ぐことはできない．

問25　イ

請負契約でシステム開発を行う場合，委託先の開発担当者は委託先の指揮命令にしたがって委託元の業務に従事する．委託先に業務の**完成責任**があり，委託元との間で**機密保持契約**が結ばれることもある．

　委託元の管理者が委託先の開発担当者に直接指揮命令することは禁じられているため，選択肢イについては法令順守の観点から，委託元のシステム監査人の指摘事項に該当する．