gzn030403 「認証システムとファイアウォール」演習問題

問１

認証局（ＣＡ）の役割に関する記述のうち、適切なものはどれか。

ア　相手の担保能力を確認する。
イ　公開鍵暗号方式を用いて、データの暗号化を行う。
ウ　転送すべきデータのダイジェスト版を作成し、電子署名として提供する。
エ　ユーザの公開鍵の正当性を保証する証明書を発行する。

問２

パスワードを用いて利用者を認証する方法のうち，適切なものはどれか。

ア　パスワードに対応する利用者ＩＤのハッシュ値を登録しておき，認証時に入力されたパスワードをハッシュ関数で変換して比較する。
イ　パスワードに対応する利用者ＩＤのハッシュ値を登録しておき，認証時に入力された利用者ＩＤをハッシュ関数で変換して比較する。
ウ　パスワードをハッシュ値に変換して登録しておき，認証時に入力されたパスワードをハッシュ関数で変換して比較する。
エ　パスワードをハッシュ値に変換して登録しておき，認証時に入力された利用者ＩＤをハッシュ関数で変換して比較する。

問３

ＰＫＩ（公開鍵基盤）の認証局が果たす役割はどれか。

ア　共通鍵を生成する。
イ　公開鍵を利用しデータの暗号化を行う。
ウ　失効したディジタル証明書の一覧を発行する。
エ　データが改ざんされていないことを検証する。

問４

公開かぎ暗号方式を採用した電子商取引において，取引当事者から独立した第三者機関である認証局（ＣＡ）が作成するものはどれか。

ア　取引当事者の公開かぎに対する電子証明書
イ　取引当事者のディジタル署名
ウ　取引当事者のパスワード
エ　取引当事者の秘密かぎに対する電子証明書

問５

入力パスワードと登録パスワードを用いて利用者を認証する方法において，パスワードファイルへの不正アクセスによる登録パスワードの盗用防止策はどれか。

ア　パスワードに対応する利用者ＩＤのハッシュ値を登録しておき，認証時に入力された利用者ＩＤをハッシュ関数で変換して参照した登録パスワードと入力パスワードを比較する。
イ　パスワードをそのまま登録したファイルを圧縮しておき，認証時に復元して，入力されたパスワードと比較する。
ウ　パスワードをそのまま登録しておき，認証時に入力されたパスワードと登録内容をともにハッシュ関数で変換して比較する。
エ　パスワードをハッシュ値に変換して登録しておき，認証時に入力されたパスワードをハッシュ関数で変換して比較する。

問６

送信者からメール本文とそのハッシュ値を受け取り，そのハッシュ値と，受信者がメール本文から求めたハッシュ値とを比較して実現できることはどれか。ここで，送信者からのハッシュ値は保護されているものとする。

ア　改ざんの有無の検出　　イ　盗聴の防止
ウ　なりすましの防止　　エ　メールの送達の確認

問７

手順に示す処理を実施したとき，メッセージの改ざんの検知の他に，受信者Ｂがセキュリティ上できることはどれか。

〔手順〕
送信者Ａの処理
（１）　メッセージから，ハッシュ関数を使ってダイジェストを生成する。
（２）　秘密に保持していた自分の署名生成鍵を用いて，（１）で生成したダイジェストからメッセージの署名を生成する。
（３）　メッセージと，（２）で生成したデータを受信者Ｂに送信する。
受信者Ｂの処理
（４）　受信したメッセージから，ハッシュ関数を使ってダイジェストを生成する。
（５）　受信したデータ，（４）で生成したダイジェスト及び送信者Ａの署名検証鍵を用いて，署名を検証する。

ア　メッセージが送信者Ａからのものであることの確認
イ　メッセージの改ざん部位の特定
ウ　メッセージの盗聴の検知
エ　メッセージの漏えいの防止

問８

二つの通信主体Ｘ，Ｙ間で，次の手順で情報をやり取りしたときの認証に関する記述のうち，正しいものはどれか。

手順１：Ｙは任意の情報を織り込んだ文字列(チャレンジコード)をＸへ送信する。

手順２：Ｘは，あらかじめＸ，Ｙ間で定めたルールに基づき，受け取った文字列から新たな文字列(レスポンスコード)を生成しＹへ返送する。

手順３：Ｙは返送されてきたレスポンスコードが正しいことを確認する。

ア　ＸがＹを認証し，ＹがＸを認証する。
イ　ＸがＹを認証する。
ウ　Ｘがチャレンジコードを認証する。
エ　ＹがＸを認証する。

問９

ＥＣ(電子商取引)における認証の役割に関する記述のうち、最も適切なものはどれか。

ア　受信側で、送信者の正当性を証明することである。
イ　送信側及び受信側で、トランザクションの内容が正しいことを証明することである。
ウ　第三者機関によって、トランザクションの内容が正しいことを証明することである。
エ　第三者機関によって、取引相手の正当性を証明することである。

問10

メッセージ認証符号におけるメッセージダイジェストの利用目的はどれか。

ア　メッセージが改ざんされていないことを確認する。
イ　メッセージの暗号化方式を確認する。
ウ　メッセージの概要を確認する。
エ　メッセージの秘匿性を確保する。

問11

セキュリティプロトコルＳＳＬの特徴はどれか。

ア　ＳＳＬはＷｅｂサーバだけで使用されるセキュリティ対策用のプロトコルで，ネットワーク層に位置するものである。
イ　ＳＳＬを利用するＷｅｂサーバでは，そのＦＱＤＮをディジタル証明書に組み込む。
ウ　個人認証用のディジタル証明書は，ＰＣごとに固有のものを作成する必要がある。
エ　日本国内では，政府機関に限り１２８ビットの共通鍵長のディジタル証明書を取得申請できる。

問12

インターネット経由で、WWWサーバにアクセスして商取引をしたい。このWWWサーバの提供者が、商取引上、信頼できる相手であるかどうかを判断するのに有効な情報を与えてくれる仕組みはどれか。

ア　ＩＰパケットフィルタリング　　イ　ＩＰポート番号
ウ　ＳＳＬ　　エ　クッキーヘッダ

問13

ＳＳＬ／ＴＬＳを利用することによって実現できるものはどれか。

ア　クライアントサーバ間の通信の処理時間を短縮する。
イ　クライアントサーバ間の通信を暗号化する。
ウ　ブラウザとＷｅｂサーバの通信の証跡を確保する。
エ　メールソフトからＷｅｂサーバへのＳＭＴＰ接続を可能にする。

問14

無線ＬＡＮやＶＰＮ接続などで利用され，利用者を認証するためのシステムはどれか。

ア　ＤＥＳ　　イ　ＤＮＳ　　ウ　ＩＤＳ　　エ　RADIUS

問15

バイオメトリクス認証システムの判定しきい値を変化させるとき，ＦＲＲ(本人拒否率)とＦＡＲ(他人受入率)との関係はどれか。

ア　ＦＲＲとＦＡＲは独立している。
イ　ＦＲＲを減少させると，ＦＡＲは減少する。
ウ　ＦＲＲを減少させると，ＦＡＲは増大する。
エ　ＦＲＲを増大させると，ＦＡＲは増大する。

問16

生体認証システムを導入するときに考慮すべき点として，最も適切なものはどれか。

ア　システムを誤作動させるデータを無害化する機能をもつライブラリを使用する。
イ　パターンファイルの頻繁な更新だけでなく，ヒューリスティックなど別の手段を組み合わせる。
ウ　本人のディジタル証明書を信頼できる第三者機関に発行してもらう。
エ　本人を誤って拒否する確率と他人を誤って許可する確率の双方を勘案して装置を調整する。

問17

バイオメトリクス認証には身体的特徴を抽出して認証する方式と行動的特徴を抽出して認証する方式がある。行動的特徴を用いているものはどれか。

ア　血管の分岐点の分岐角度や分岐点間の長さから特徴を抽出して認証する。
イ　署名するときの速度や筆圧から特徴を抽出して認証する。
ウ　どう孔から外側に向かって発生するカオス状のしわの特徴を抽出して認証する。
エ　隆線によって形作られる紋様からマニューシヤと呼ばれる特徴点を抽出して認証する。

問18

ＨＴＴＰＳを用いて実現できるものはどれか。

ア　Ｗｅｂサーバ上のファイルの改ざん検知
イ　クライアント上のウイルス検査
ウ　クライアントに対する侵入検知
エ　電子証明書によるサーバ認証

問19

画像などのディジタルコンテンツが，不正にコピーされて転売されたものであるかを判別できる対策はどれか。

ア　タイムスタンプ　　イ　電子透かし　　ウ　電子保存　　エ　配達証明

問20

ＨＴＴＰＳ(HTTP over SSL/TLS)の機能を用いて実現できるものはどれか。

ア　ＳＱＬインジエクションによるＷｅｂサーバへの攻撃を防ぐ。
イ　ＴＣＰポート８０番と４４３番以外の通信を遮断する。
ウ　Ｗｅｂサーバとブラウザの間の通信を暗号化する。
エ　Ｗｅｂサーバへの不正なアクセスをネットワーク層でのパケットフィルタリングによって制限する。

問21

ネットワークを通してデータ交換を行う場合，ユーザを認証する方法として，適切なものはどれか。

ア　受信データが改ざんされていないかどうかを調べる。
イ　送信データを暗号化する。
ウ　データを発信しているコンピュータを特定する。
エ　パスワードの一致を調べる。

問22

Ｗｅｂサーバのコンテンツの改ざんを検知する方法のうち，最も有効なものはどれか。

ア　Ｗｅｂサーバのコンテンツの各ファイルの更新日を保管しておき，定期的に各ファイルの更新日と比較する。
イ　Ｗｅｂサーバのコンテンツの各ファイルのハッシュ値を保管しておき，定期的に各ファイルから生成したハッシュ値と比較する。
ウ　Ｗｅｂサーバのメモリ使用率を定期的に確認し，バッファオーバフローが発生していないことを確認する。
エ　Ｗｅｂサーバへの通信を監視し，ＨＴＴＰ，ＨＴＴＰＳ以外の通信がないことを確認する。

問23

ファイアウォールのパケットフィルタリング機能に関する記述のうち，適切なものはどれか。

ア　インターネットから受け取ったパケットに改ざんがある場合は修正し，改ざんが修正できない場合には，ログを取って内部ネットワークへの通過を阻止する。
イ　インターネットから受け取ったパケットのヘッダ部分及びデータ部分に，改ざんがあるかどうかをチェックし，改ざんがあった場合にはそのパケットを除去する。
ウ　動的に割り振られたＴＣＰポート番号をもったパケットを，受信側で固定値のＴＣＰポート番号をもったパケットに変更して，内部ネットワークへの通過を許可する。
エ　特定のＴＣＰポート番号をもったパケットだけに，インターネットから内部ネットワークへの通過を許可する。

問24

ディレクトリに，読取り，更新，配下のファイル作成のアクセス権を設定できるＯＳがある。この３種類のアクセス権は，それぞれに１ビットを使って許可，不許可を設定する。この３ビットを８進数表現０～７の数字で設定するとき，次の試行結果から考えて，適切な記述はどれか。

〔試行結果〕
①　０を設定したら，一切のアクセスができなくなってしまった。
②　３を設定したら，読取りと更新はできたが，作成ができなかった。
③　７を設定したら，すべてのアクセスができるようになった。

ア　２を設定すると，読取りと作成ができる。
イ　４を設定すると，作成だけができる。
ウ　５を設定すると，更新だけができる。
エ　６を設定すると，読取りと更新ができる。

問25

利用者情報を管理するデータベース(利用者データベース)がある。利用者データベースを検索し，検索結果を表示するアプリケーションに与えるデータベースのアクセス権限として，セキュリティ管理上適切なものはどれか。ここで，権限の範囲は次のとおりとする。

〔権限の範囲〕

参照権限：　利用者データベースのレコードの参照が可能

更新権限：　利用者データベースへのレコードの登録，変更，削除が可能

管理者権限：利用者データベースのテーブルの参照，登録，変更，削除が可能

ア　管理者権限　　イ　更新権限

ウ　参照権限　　エ　参照権限と更新権限

問26

１台のファイアウォールによって，外部セグメント，ＤＭＺ，内部ネットワークの三つのセグメントに分割されたネットワークがある。このネットワークにおいて，Ｗｅｂサーバと，重要なデータをもつＤＢサーバから成るシステムを使って，利用者向けのサービスをインターネットに公開する場合，インターネットからの不正アクセスから重要なデータを保護するためのサーバの設置方法のうち，最も適切なものはどれか。ここで，ファイアウォールでは，外部セグメントとＤＭＺ間及びＤＭＺと内部ネットワーク間の通信は特定のプロトコルだけを許可し，外部セグメントと内部ネットワーク間の通信は許可しないものとする。

ア　ＷｅｂサーバとＤＢサーバをＤＭＺに設置する。

イ　ＷｅｂサーバとＤＢサーバを内部ネットワークに設置する。

ウ　ＷｅｂサーバをＤＭＺに，ＤＢサーバを内部ネットワークに設置する。

エ　Ｗｅｂサーバを外部セグメントに，ＤＢサーバをＤＭＺに設置する。

問27

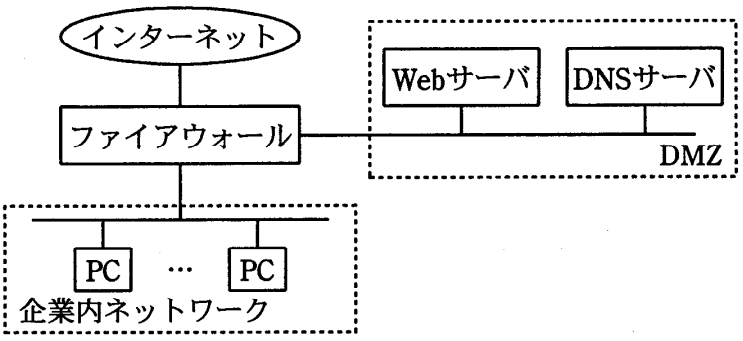
図に示すネットワーク構成で，Ｗｅｂページの閲覧だけを社外に提供する。攻撃を防止するためにファイアウォールのＩＰパケットフィルタリングを設定する場合，フィルタリングルールでインターネットからＤＭＺへのパケットの通過を禁止できないプロトコルはどれか。

ア　ＦＴＰ

イ　ＨＴＴＰ

ウ　ＳＭＴＰ

エ　ＳＮＭＰ



問28

パケットフィルタリング型ファイアウォールがルール一覧に基づいてパケットを制御する場合，パケットＡに対する制御はどれか。ここで，ファイアウォールでは，ルール一覧に示す番号の１から順にルールの適用判断を行い，一つのルールが適用されたときには残りのルールは適用しない。

〔ルール一覧〕

番号	送信元アドレス	宛先アドレス	プロトコル	送信元ポート番号	宛先ポート番号	動作
1	10.1.2.3	*	*	*	*	通過禁止
2	*	10.2.3.*	TCP	*	25	通過許可
3	*	10.1.*	TCP	*	25	通過許可
4	*	*	*	*	*	通過禁止

注記　＊は任意のパターンを表す。

〔パケット A〕

送信元アドレス	宛先アドレス	プロトコル	送信元ポート番号	宛先ポート番号
10.1.2.3	10.2.3.4	TCP	2100	25

ア　番号１によって，通過を禁止する。
イ　番号２によって，通過を許可する。
ウ　番号３によって，通過を許可する。
エ　番号４によって，通過を禁止する。

問29

複数の業務システムがある場合のアクセス管理の方法として，最も適切なものはどれか。

ア　業務の担当変更に迅速に対応するために，業務グループごとに共通の利用者ＩＤを使用する。
イ　人事異動が頻繁に発生する場合には，年初にまとめてアクセス権限の変更を行う。
ウ　新入社員の名簿に基づいて，あらかじめ全業務システムに全員の利用者登録を実施しておく。
エ　利用者の職位権限にかかわらず，業務システムごとに適切なアクセス権限の設定を行う。

問30

Ｗｅｂビーコンに該当するものはどれか。

ア　ＰＣとＷｅｂサーバ自体の両方に被害を及ぼす悪意のあるスクリプトによる不正な手口
イ　Ｗｅｂサイトからダウンロードされ ＰＣ上で画像ファイルを消去するウイルス
ウ　Ｗｅｂサイトで用いるアプリケーションプログラムに潜在する誤り
エ　Ｗｅｂページなどに小さい画像を埋め込み，利用者のアクセス動向などの情報を収集する仕組み

問31

ＰＣへの侵入に成功したマルウェアがインターネット上の指令サーバと通信を行う場合に，宛先ポートとしてＴＣＰポート番号８０が多く使用される理由はどれか。

ア　ＤＮＳのゾーン転送に使用されるので，通信がファイアウォールで許可されている可能性が高い。

イ　ＷｅｂサイトのＨＴＴＰＳ通信での閲覧に使用されることから，侵入検知システムで検知される可能性が低い。

ウ　Ｗｅｂサイトの閲覧に使用されることから，通信がファイアウォールで許可されている可能性が高い。

エ　ドメイン名の名前解決に使用されるので，侵入検知システムで検知される可能性が低い。

問32

社内ネットワーク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て，社内ネットワーク上のＰＣからインターネット上のＷｅｂサーバの８０番ポートにアクセスできるようにするとき，フィルタリングで許可するルールの適切な組合せはどれか。

ア

送信元	宛先	送信元 ポート番号	宛先 ポート番号
PC	Web サーバ	80	1024 以上
Web サーバ	PC	80	1024 以上

イ

送信元	宛先	送信元 ポート番号	宛先 ポート番号
PC	Web サーバ	80	1024 以上
Web サーバ	PC	1024 以上	80

ウ

送信元	宛先	送信元 ポート番号	宛先 ポート番号
PC	Web サーバ	1024 以上	80
Web サーバ	PC	80	1024 以上

エ

送信元	宛先	送信元 ポート番号	宛先 ポート番号
PC	Web サーバ	1024 以上	80
Web サーバ	PC	1024 以上	80

問33

認証デバイスに関する記述のうち，適切なものはどれか。

ア　ＩＥＥＥ８０２．１Ｘでは，ディジタル証明書や利用者ＩＤ，パスワードを格納するＵＳＢキーは，２００ｋバイト以上のメモリを内蔵することを規定している。
イ　安定した大容量の電力を必要とする高度な処理には，接触型ＩＣカードよりも非接触型ＩＣカードの方が適している。
ウ　虹彩認証では，成人には虹彩の経年変化がないので，認証デバイスでのパターン更新がほとんど不要である。
エ　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。

問34

２要素認証に該当するものはどれか。

ア　２本の指の指紋で認証する。
イ　虹彩とパスワードで認証する。
ウ　異なる２種類の特殊文字を混ぜたパスワードで認証する。
エ　異なる二つのパスワードで認証する。

問35

社員が利用するスマートフォンにディジタル証明書を導入しておくことによって，当該スマートフォンから社内システムへアクセスがあったときに，社内システム側で確認できるようになることはどれか。

ア　当該スマートフォンがウイルスに感染していないこと
イ　当該スマートフォンが社内システムへのアクセスを許可されたデバイスであること
ウ　当該スマートフォンのＯＳに最新のセキュリティパッチが適用済みであること
エ　当該スマートフォンのアプリケーションが最新であること

問36

Ｗｅｂシステムのパスワードを忘れたときの利用者認証において合い言葉を使用する場合，合い言葉が一致した後の処理のうち，セキュリティ上最も適切なものはどれか。

ア　あらかじめ登録された利用者のメールアドレス宛てに，現パスワードを送信する。
イ　あらかじめ登録された利用者のメールアドレス宛てに，パスワード再登録用ページへアクセスするための，推測困難なＵＲＬを送信する。
ウ　新たにメールアドレスを入力させ，そのメールアドレス宛てに，現パスワードを送信する。
エ　新たにメールアドレスを入力させ，そのメールアドレス宛てに，パスワード再登録用ページへアクセスするための，推測困難なＵＲＬを送信する。

問37

公開鍵暗号を利用した電子商取引において，認証局（ＣＡ）の役割はどれか。

ア　取引当事者間で共有する秘密鍵を管理する。
イ　取引当事者の公開鍵に対するディジタル証明書を発行する。
ウ　取引当事者のディジタル署名を管理する。
エ　取引当事者のパスワードを管理する。

問38

人間には読み取ることが可能でも，プログラムでは読み取ることが難しいという差異を利用して，ゆがめたり一部を隠したりした画像から文字を判読して入力させることによって，プログラムによる自動入力を排除するための技術はどれか。

ア　CAPTCHA　　イ　ＱＲコード
ウ　短縮ＵＲＬ　　エ　トラックバックping

問39

社内ネットワークとインターネットの接続点に，ステートフルインスペクション機能をもたない，静的なパケットフィルタリング型のファイアウォールを設置している。この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できるようにするとき，ファイアウォールで通過を許可するＴＣＰパケットのポート番号の組合せはどれか。ここで，ＳＭＴＰ通信には，デフォルトのポート番号を使うものとする。

	送信元	宛先	送信元 ポート番号	宛先 ポート番号
ア	PC	SMTP サーバ	25	1024 以上
	SMTP サーバ	PC	1024 以上	25
イ	PC	SMTP サーバ	110	1024 以上
	SMTP サーバ	PC	1024 以上	110
ウ	PC	SMTP サーバ	1024 以上	25
	SMTP サーバ	PC	25	1024 以上
エ	PC	SMTP サーバ	1024 以上	110
	SMTP サーバ	PC	110	1024 以上

問40

ＰＫＩにおける認証局が，信頼できる第三者機関として果たす役割はどれか。

ア　利用者からの要求に対して正確な時刻を返答し，時刻合わせを可能にする。
イ　利用者から要求された電子メールの本文に対して，ディジタル署名を付与する。
ウ　利用者やサーバの公開鍵を証明するディジタル証明書を発行する。
エ　利用者やサーバの秘密鍵を証明するディジタル証明書を発行する。

問41

ＷＡＦの説明はどれか。

ア　Ｗｅｂサイトに対するアクセス内容を監視し，攻撃とみなされるパターンを検知したときに当該アクセスを遮断する。
イ　Ｗｉ－Ｆｉアライアンスが認定した無線ＬＡＮの暗号化方式の規格であり，ＡＥＳ暗号に対応している。
ウ　様々なシステムの動作ログを一元的に蓄積，管理し，セキュリティ上の脅威となる事象をいち早く検知，分析する。
エ　ファイアウォール機能を有し，ウイルス対策，侵入検知などを連携させ，複数のセキュリティ機能を統合的に管理する。

問42

ＣＳＩＲＴの説明として，適切なものはどれか。

ア　ＩＰアドレスの割当て方針の決定，ＤＮＳルートサーバの運用監視，ＤＮＳ管理に関する調整などを世界規模で行う組織である。
イ　インターネットに関する技術文書を作成し，標準化のための検討を行う組織である。
ウ　企業内・組織内や政府機関に設置され，情報セキュリティインシデントに関する報告を受け取り，調査し，対応活動を行う組織の総称である。
エ　情報技術を利用し，宗教的又は政治的な目標を達成するという目的をもつ者や組織の総称である。

問43

生体認証システムを導入するときに考慮すべき点として，最も適切なものはどれか。

ア　本人のディジタル証明書を，信頼できる第三者機関に発行してもらう。
イ　本人を誤って拒否する確率と他人を誤って許可する確率の双方を勘案して装置を調整する。
ウ　マルウェア定義ファイルの更新が頻繁な製品を利用することによって，本人を誤って拒否する確率の低下を防ぐ。
エ　容易に推測できないような知識量と本人が覚えられる知識量とのバランスが，認証に必要な知識量の設定として重要となる。

問44

電子メールの送信時に，送信者を送信側のメールサーバで認証するためのものはどれか。

ア　ＡＰＯＰ　　イ　ＰＯＰ３Ｓ　　ウ　Ｓ／ＭＩＭＥ　　エ　SMTP-AUTH

問45

情報セキュリティにおけるタイムスタンプサービスの説明はどれか。

ア　公式の記録において使われる全世界共通の日時情報を，暗号化通信を用いて安全に表示するＷｅｂサービス

イ　指紋，声紋，静脈パターン，網膜，虹彩などの生体情報を，認証システムに登録した日時を用いて認証するサービス

ウ　電子データが，ある日時に確かに存在していたこと，及びその日時以降に改ざんされていないことを証明するサービス

エ　ネットワーク上のＰＣやサーバの時計を合わせるための日時情報を途中で改ざんされないように通知するサービス