gzn030403 「認証システムとファイアウォール」解答解説

問１　エ

ＣＡに関する問題である。

ＣＡはインターネットのメールやWWWページなどにデジタル署名するときに付与する電子印鑑証明書を発行するシステムである。求める答えはエである。

問２　ウ

パスワードを用いた利用者認証に関する問題である。

利用者認証は、相手が本当の相手であることを確認する手段であり、単純な方式では、利用者ＩＤとパスワードを組み合わせて利用する。その際、パスワードの盗難防止の目的で、パスワードをハッシュ値に変化して使用する。

ハッシュ関数は、あるデータが与えられた場合にそのデータを代表する数値を得る操作、または、その様な数値を得るための関数のことである。ハッシュ関数から得られた数値のことをハッシュ値または単にハッシュという。通信における暗号化やユーザ認証、ディジタル署名などでは、不可逆的な関数で処理を行い、ハッシュ値から原文を再現することができないようにする。これを利用することによって、改ざん防止やパスワードの盗難防止を図る。

アの利用者ＩＤをハッシュ関数で変換して登録し、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しても利用者認証にはならない。

イの利用者ＩＤをハッシュ関数で変換して登録し、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も、本人の確認は不十分である。

ウのパスワードをハッシュ関数で変換して登録し、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、比較すると本人の確認は可能である。求める答えはウとなる。

エのパスワードをハッシュ関数で変換して登録し、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も、本人の確認は不十分である。

問３　ウ

認証局の役割に関する問題である。

認証局は公開鍵とその所有者を対応づけるために電子証明書を発行する機関である。認証局では、各ユーザからの電子証明書の発行依頼を受けると、そのユーザの本人確認を行った後に、正しいユーザである場合にのみ電子証明書を発行する。電子証明書には所有者の識別情報や公開鍵などが記載されている。

認証局の主な役割には次のものがある。

①　申請者の公開鍵にディジタル署名を付したディジタル証明書を発行する
②　ＣＲＬ(証明書失効リスト)を発行する
③　ＣＰＳ(認証局運用規定)を公開する
④　ディジタル証明書を検証するための認証局の公開鍵を公開する
⑤　認証局の秘密鍵を厳重に管理する

失効した(効力をなくした)ディジタル証明書の一覧を発行する内容が適切である。求める答え

はウとなる。

問４　ア

認証局に関する問題である。

電子商取引（ＥＣ）は、コンピュータとネットワークを利用して企業間の商取引や企業と消費者の直接取引を行う。ＥＣを実現するために各企業はインターネットを活用したプライベートのポータルサイトを構築したり、業界共通のパブリックなポータルサイトに接続するなどして、顧客からのアクセス機会を増やすことを行う。

電子認証システムは、デジタル署名技術と認証局、電子証明書を用いることにより、取引者間の相互認証を実現する仕組みである。電子証明書は、インターネットを利用する電子決済などのために、利用者の正当性を保証する証明書で、この証明書は第３者の認証機関が発行する。電子証明書の技術は、公開鍵暗号方式を利用し、公開鍵のデータが正当であることを証明するために、認証機関はこのデータにデジタル署名をする。デジタル署名を使用するシステムでは、各ユーザとそのユーザの公開鍵との対比関係が第三者機関によって保証されていなければならない。

認証局は公開鍵とその所有者を対応づけるために電子証明書を発行する機関である。認証局では、各ユーザからの電子証明書の発行依頼を受けると、そのユーザの本人確認後に正しいユーザであることを保証する所有者の識別情報や公開鍵などを記載した電子証明書を発行する。

認証局が発行するのは、取引当事者の公開かぎに対する電子証明書である。求める答えはアとなる。

問５　エ

パスワードの盗難防止に関する問題である。

ハッシュ関数は、あるデータが与えられた場合にそのデータを代表する数値を得る操作、または、その様な数値を得るための関数のことである。ハッシュ関数から得られた数値のことをハッシュ値または単にハッシュという。通信における暗号化やユーザ認証、ディジタル署名などでは、不可逆的な関数で処理を行い、ハッシュ値から原文を再現することができないようにする。これを利用することによって、改ざん防止やパスワードの盗難防止を図る。

アの利用者ＩＤをハッシュ関数で変換して、登録パスワードをそのまま保管していると、盗難時には、パスワードがそのまま使用されることになる。

イのパスワードファイルを圧縮して保管していても、復元すればパスワードを知ることができるため無意味である。

ウのパスワードをそのまま登録していると、ファイルの盗難時にパスワードの内容がそのまま相手に知られてしまう。

エのパスワードをハッシュ関数を使用して、ハッシュ値を求めていると、ファイルを盗まれても直ちに内容が相手に分かることがない。

問６　ア

メッセージ認証に関する問題である。

認証には相手認証とメッセージ認証がある。相手認証はある人が他の人に自分が確かに本人であると納得させる事をいう。本人固有の情報（名前、所属、住所、電話番号）を伝えたり、指紋、

虹彩等のバイオメトリクス情報を伝えたり、パスワードを入力したり、合言葉を認証者に言ったり、ＩＣカードを認証機械に通すことによって行われる。メッセージ認証はメッセージの同一性の保証であり、コンピュータウイルス、不正侵入等を使った破壊行為によりメッセージが変更されていない事を保証する為の手続きである。メッセージmに対しそのハッシュ値Ｘ＝Ｈ(m)を計算し、Ｘを安全なな場所に保管する。mが改竄されて別のメッセージMになっていた場合、Ｘ≠Ｈ(M)なのでメッセージが改竄された事が分かる。

アの改ざんの有無を検出するはメッセージ認証である。メール本文をハッシュ値と比較するのはメッセージ認証の方法である。求める答えはアとなる。

イの盗聴は電話回線上の通話や通信ネットワーク上で送受信されているデータを不正に傍受することである。

ウのなりすましは他者のユーザＩＤやパスワード、ＩＰアドレスなどを使用して、他者であるふりをしてシステムに進入して不正行為を行うことである。

エのメールの送達確認はメールが目的の相手に無事送られたかどうかを確認することである。

問７　ア

ハッシュ関数を使用した認証システムの問題である。

ハッシュ関数は、あるデータが与えられた場合にそのデータを代表する数値を得る操作、または、その様な数値を得るための関数のことである。ハッシュ関数から得られた数値のことをハッシュ値または単にハッシュという。通信における暗号化やユーザ認証、ディジタル署名などでは、不可逆的な関数で処理を行い、ハッシュ値から原文を再現することができないようにする。これを利用することによって、改ざん防止やパスワードの盗難防止、メッセージ送信者の確認などを図る。

メッセージが送信者Ａからのものであることを確認するとなり、求める答えはアとなる。

問８　エ

Ｘ、Ｙの２者間での認証に関する通信の問題である。

ＹがチャレンジコードをＸに送信し、Ｘはレスポンスコードを返信し、Ｙが確認する仕組みであるから、ＹがＸを認証することになる。求める答えはエとなる。

問９　エ

電子商取引における認証の役割に関する問題である。

電子認証システムは、デジタル署名技術と認証局(ＣＡ)、電子証明書を用いることにより、取引者間の相互認証を実現する仕組みである。

電子証明書は、インターネットを利用する電子決済などのために、利用者の正当性を保証する証明書で、この証明書は第３者の認証機関が発行する。電子証明書の技術としては公開鍵暗号方式を利用するのが一般的である。公開鍵のデータが正当であることを証明するために、認証機関はこのデータにデジタル署名をする。

商取引における取引相手の確認やデータ改ざんの有無の確認は、メッセージ認証やデジタル署名の技術を利用することによって実現できる。署名の検証者は署名者の正しい公開鍵を用いることによって可能となる。デジタル署名を使用するシステムでは、各ユーザとそのユーザの公開鍵

との対比関係が第三者機関によって保証されていなければならない。

エの第三者機関によって、取引相手の正当性の証明が電子証明書で、求める答えはエとなる。

問10　ア

メッセージダイジェストに関する問題である。

メッセージダイジェストは、元のメッセージから任意の長さのメッセージを演算処理して特徴的なパターンを生成し、データ通信のメッセージが正しいことを証明する技術である。インターネットの標準技術であるＭＤ５（Message Digest Algorithm 5）では、一方向ハッシュ関数を使った演算により、元のデータの長さに関係なく128ビットのデータを生成する。

メッセージ認証は、受信したメッセージが途中で改ざんされていないかを確認することである。ハッシュ関数の一種であるメッセージダイジェスト関数を用いて求めるメッセージダイジェストを比較して改ざんの有無を確認する。送信メッセージのメッセージダイジェストと受信メッセージのメッセージダイジェストが異なる場合、伝送途中で改ざんがあったと判断する。

メッセージダイジェストは電子署名の基礎技術であり、電子署名ではダイジェストデータをさらに暗号化する。通信回線を通じてデータを送受信する際に、経路の両端でデータのハッシュ値を求めて両者を比較すれば、データが通信途中で改ざんされていないか調べることができる。求める答えはアとなる。

問11　イ

ＳＳＬに関する問題である。

ＳＳＬは、インターネット上で情報を暗号化して送受信するプロトコル。現在インターネットで広く使われているWWWやＦＴＰなどのデータを暗号化し、プライバシーに関わる情報やクレジットカード番号、企業秘密などを安全に送受信することができる。

ＦＱＤＮは、インターネットやイントラネットなどのＴＣＰ／ＩＰネットワーク上で、ドメイン名・サブドメイン名・ホスト名を省略せずにすべて指定した記述形式のことである。

アのＳＳＬはＷｅｂだけで使用されるプロトコルではない。

イは適切な記述である。求める答えはイとなる。

ウのディジタル証明書は、各ユーザからの電子証明書の発行依頼を受け、そのユーザの本人確認を行った後に、正しいユーザである場合にのみ電子証明書を発行する。電子証明書には所有者の識別情報や公開鍵などが記載されている。ＰＣ単位ではない。

エのディジタル証明書は、共通鍵ではなく公開鍵暗号方式を使用する。

問12　ウ

商取引に関係する認証の問題である。

アのＩＰパケットフィルタリングは、ルーター、ゲートウエイ、ファイア・ウオールなどで、パケットのあて先アドレス、あるいは送信元アドレスとあて先アドレスの組み合わせを調べて、通過させて良いパケットと阻止すべきパケットを区別すること及びその機能である。パケット・フィルタリングは、余分なトラフィックが生じることの抑制と、セキュリティ機能を実現するための方法である。

イのＩＰポート番号はパソコンと周辺機器を接続するインターフェースのコネクタ部分の番号

で、ポート番号を通してＩＰパケットは入出力される。ファイアウォールなどで利用される。

ウのＳＳＬは、WWWのブラウザやサーバ間でサーバの認証に利用されたり、通信データを暗号化したりする技術である。求める答えはウである。

エのクッキーヘッダは、WWWサーバーがユーザーを識別・管理するための仕組みである。

問13　イ

ＳＳＬ／ＴＬＳに関する問題である。

ＳＳＬ／ＴＬＳはウェブブラウザとサーバ間の通信を暗号化して安全にデータをやり取りするプロトコルである。

クライアントサーバ間の通信を暗号化するが正しい答である。求める答はイとなる。

問14　エ

RADIUSに関する問題である。

RADIUSは、ネットワーク資源の利用の可否の認証と利用の事実の記録を、ネットワーク上のサーバコンピュータに一元化することを目的とした、ＩＰ上のプロトコルである。常時接続方式のインターネット接続サービス、無線ＬＡＮ、ＶＬＡＮ、コンテンツ提供サービスなどのサービス提供者側設備において、認証とアカウンティングを実現するプロトコルとして幅広く利用されている。

アのＤＥＳは、米国の商務省が標準暗号化方式として制定した共通鍵暗号方式である。

イのＤＮＳは、インターネットに接続されたコンピュータのドメイン名とＩＰアドレスの対応付けや、両者を置き換える機能などを提供する仕組みである。

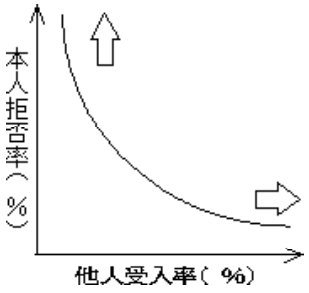
ウのＩＤＳは、ネットワークやコンピュータに対する不正行為を検出し、知らせるためのシステムである。

エのRADIUSは、無線ＬＡＮやＶＰＮ等で利用され、利用者を認証するシステムである。求める答えはエとなる。

問15　ウ

バイオメトリック認証に関する問題である。

ＦＲＲ(本人拒否)は本人同士のデータの照合で不一致と判定されることことである。ＦＡＲ(他人受入)は本人と他人のデータの照合で一致と判定されることである。ＦＲＲとＦＡＲは相関関係にあり、片方の比率を上げるともう片方の比率が下がる。安全性を重視すると、ＦＡＲを小さくする必要があるが、その場合ＦＲＲが上がり、使い勝手に影響がでる。逆に利便性を重視するためにＦＲＲを下げると、ＦＡＲが上がってしまい、安全性が低下してしまう特徴がある。



アのＦＲＲとＦＡＲは相関関係にある。

イのＦＲＲを減少するとＦＡＲが増大する。

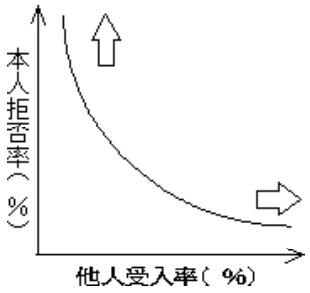
ウのＦＲＲを減少するとＦＡＲが増大する内容は適切である。求める答えはウとなる。

エのＦＲＲを増大するとＦＡＲは減少する。

問16　エ

生体認証システムに関する問題である。

ＦＲＲ(本人拒否)は本人同士のデータの照合で不一致と判定されることことである。ＦＡＲ(他人受入)は本人と他人のデータの照合で一致と判定されることである。



ＦＲＲとＦＡＲは相関関係にあり、片方の比率を上げるともう片方の比率が下がる。安全性を重視すると、ＦＡＲを小さくする必要があるが、その場合ＦＲＲが上がり、使い勝手に影響がでる。逆に利便性を重視するためにＦＲＲを下げると、ＦＡＲが上がってしまい、安全性が低下してしまう特徴がある。

生体認証システムを導入する場合、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必要がある。求める答えはエとなる。

問17　イ

バイオメトリクス認証の問題である。

身体的特徴を利用しているのは、アの血管の分岐点の分岐角度や分岐点間の長さの特徴を用いるもの、ウの瞳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用いるもの、エの隆線によって形作られる紋様からマニューシャと呼ばれる特徴点を抽出して認証するものがある。

行動的特徴を用いるものには、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ものがある。求める答えはイとなる。

問18　エ

ＨＴＴＰＳに関する問題である。

ＨＴＴＰＳは、ＳＳＬ／ＴＬＳプロトコルを用いて、サーバの認証、通信内容の暗号化、改竄検出などを行い、なりすましや盗聴などの攻撃を防ぐことができる。Ｗｅｂブラウザとｗｅｂサーバの間の通信を暗号化して、盗聴や改竄を防ぐ。

アのサーバ上のファイルの改ざんの検知ではない。

イのウィルス検査の役割はない。

ウのクライアントへの侵入検知はしない。

エの電子証明書を用いてサーバ認証に使用する。求める答えはエとなる。

問19　イ

電子透かしに関する問題である。

アのタイムスタンプは、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である。

イの電子透かしは、音声や画像などの電子化されたコンテンツに対して、品質を落とさず利用者に分からない方法で著作権情報を記録する仕組みである。求める答えはイとなる。

ウの電子保存は、情報を電子媒体に保存することである。

エの配達証明は、一般書留とした郵便物や荷物を配達した事実を証明するサービスである。

問20　ウ

ＨＴＴＰＳに関する問題である。

ＨＴＴＰＳは、ＳＳＬ／ＴＬＳプロトコルを用いて、サーバの認証、通信内容の暗号化、改竄検出などを行い、なりすましや盗聴などの攻撃を防ぐことができる。Ｗｅｂブラウザとウｅｂサーバの間の通信を暗号化して、盗聴や改竄を防ぐ。

アのＳＱＬインジェクションは、ＳＱＬ文を利用して、ＤＢの改ざんや不正に情報を入手することである。

イのＴＣＰポート８０は、ＨＴＴＰを利用してアプリケーションにデータを渡す場合に利用するポートで、ＨＴＴＰＳはそれ以外のデータ通信を遮断することではない。

ウのサーバとブラウザ間の通信の暗号化は適切な内容である。求める答えはウとなる。

エのパケットフィルタリングは、ネットワーク層型ファイアウォールの機能である。

問21　エ

ユーザ認証に関する問題である。

アの受信データの改ざんの調査を行っても、ユーザ認証にはならない。

イの送信データの暗号化はデータの守秘は守れるが、ユーザ認証にはならない。

ウのデータを発信するコンピュータを特定しても、ユーザを特定することはできない。ユーザ認証にはならない。

エのパスワードはユーザ特有のものであり、ユーザ認証になる。求める答えはエとなる。

問22　イ

コンテンツの改ざんに関する問題である。

何らかの理由でファイルが破損していないか、オリジナルから変更されていないかをチェックする場合には、ファイルの「ハッシュ値」を比較する方法が広く使われている。フリーソフトウェアやシェアウェアでは、配布サイト上にＭＤ５やＳＨＡ１方式によるハッシュ値を掲載し、ダウンロード中にファイルが破損するなどの理由でオリジナルと違ってしまっていないかを確認できるようにしているサイトも多い。求める答えはイとなる。

問23　エ

ファイアウォールに関する問題である。

パケットフィルタリングは、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、接続を開始する方向性、プロトコルに基づき、転送パケットを通過させるかさせないかのアクセス制御を実現することである。パケットフィルタリングによって、あらかじめ設定されていない不正なパケットの流出入を防止する。ルータなどの経路情報を有する装置を利用する。

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。求める答えはエとなる。

問24　イ

アクセス権設定に関する問題である。

３ビットで読取り、更新、作成のアクセス権を設定する。

① ０００はすべてのアクセス権を許可しない。

② ０１１は読取り、更新ができ、作成ができない。

③ １１１はすべてのアクセスが可能になる。

④ 以上の内容からアクセス権の設定は、作成・読取り・更新、または作成・更新・読取りになる。

アは、０１０となり、作成はできない。

イは、１００となり、作成だけができる。求める答えはイとなる。

ウは、１０１となり、作成と更新、または作成と読取りになる。

エは、１１０となり、作成と更新、または作成と読取りになる。

問25　ウ

権限の範囲に関する問題である。

アプリケーションは、利用者が必要としている情報をデータベースから検索して、その結果を表示する処理であるから、権限のうち登録や変更、削除などは必要でない。アプリケーションに必要な権限は参照権限であり、更新権限、管理者権限は必要がない。求める答えはウとなる。

問26　ウ

ＤＭＺを使用したサーバ設置法に関する問題である。

ＤＭＺは、インタネットなどの外部ネットワークと社内ネットワークの中間につくられるネットワーク上のセグメントで、外部ネットワークからも内部ネットワークからもファイアウォールなどによって隔離されている。社内ネットワークをインターネットに接続する際に、Ｗｅｂサーバやメールサーバなどインターネットに公開しなければならないサーバは、ＤＭＺセグメントに設置しセキュリティ強化を図ることができる。外部に公開するＷｅｂサーバは、常にリスクに晒されているため、Ｗｅｂサーバーを社内ネットワークに置くとリモートハッキングやマルウェアなどを組み込まれたりした場合、社内ネットワークに接続されているその他のサーバやパソコンがすべて被害を受ける可能性がある。ＤＭＺ内に公開用のＷｅｂサーバを設置して、社内ネットワークと隔離することで、不正侵入された後のマルウェアの感染拡大を防ぐことができ、業務システムなどへの侵入による機密情報の漏洩を防止することが可能になる。

ＤＭＺの構成は、２台のファイアウォールを設置して、インターネット／ファイアウォール／ＤＭＺ／ファイアウォール／社内ネットワークとする方法がセキュリティ強度を高くすることになるが、ファイアウォール1台だけで構成する方法も可能で、１台のファイアウォールが外部セグメントとＤＭＺの間、およびＤＭＺと内部セグメントとの間を特定の通信プロトコルで通信許可の処理を行い対応する。

ＷｅｂサーバはＤＭＺに、データベースサーバは内部セグメントに設置する。求める答えはウとなる。

問27　イ

ＨＴＴＰプロトコルに関する問題である。

アのＦＴＰは、ファイル転送プロトコルである。ファイルを転送する場合、ユーザアカウント

とパスワードを用いてユーザ認証を行い、認証後に転送を利用できる。

イのＨＴＴＰは、ＨＴＭＬで記述されたファイルを転送するプロトコルである。WWWクライアントとWWWサーバ間で、クライアントからのコンテンツ転送要求に応じて、サーバに格納されているＨＴＭＬファイル、画像、音声、動画像などのコンテンツを転送し、表示する。Ｗｅｂページの閲覧が目的であるからインターネットからの通過を禁止できない。

ウのＳＭＴＰは、インターネット上で電子メールを送信または転送するためのプロトコルである。ＴＣＰのポート番号２５を利用して行う。ユーザの確認、メールボックスの有無、容量の不足などをチェックしながら通信が行われる。

エのＳＮＭＰは、ＴＣＰ／ＩＰのネットワーク管理プロトコルで、ルータやハブなどのネットワーク機器のネットワーク管理情報を管理システムに送る場合の標準プロトコルである。ネットワーク情報の収集に必要なパケットのみを通過させる。

問28　ア

パケットフィルタリング型ファイアウォールに関する問題である。

ファイアウォールのルールは次のように適用される。

① 番号１で、送信元アドレスをチェックし、一致すれば通過禁止にする。

② 番号２で、宛先アドレス、プロトコル、宛先ポート番号をチェックし、一致すれば通過許可する。

③ 番号３で、宛先アドレス、プロトコル、宛先ポート番号をチェックし、一致すれば通過許可する。

④ 番号１～３で、ルールが適用されなかったものは、通過禁止にする。

パケットＡは、ルール番号１の送信元アドレスで一致するため、番号１によって通過を禁止する。求める答えはアとなる。

問29　エ

アクセス管理に関する問題である。

アクセス管理はファイルやネットワークなどへのアクセスに関して、ユーザごとにアクセス権を与え、アクセス状況を管理することである。アクセス権は、ユーザがコンピュータのファイルやネットワークなどの共有資源を利用するための権利のことであり、アクセスの禁止や読み取りの許可、書換・削除の許可など、ユーザごとに権利の設定を行う。

ユーザ管理は情報システムの利用者をユーザＩＤなどの識別子を用いて、ユーザの資源利用の実態把握やユーザの不当アクセス防止などの管理を行うことである。ユーザ管理を利用して、ユーザごとにファイルなどの共有資源へのアクセス権を設定し、管理する。

アの利用者ＩＤは利用者個人に対して発行するものであって、原則として業務グループごとに共通のＩＤを使用しない。

イのアクセス権の設定は人事異動など必要が発生する度に変更し、年初にまとめて発行してはならない。

ウの利用者ＩＤの発行は本人の申請に基づいて、担当の業務に関連して発行するものであり、あらかじめ登録しておくものではない。

エの利用者の職務権限に関係なく、業務システムごとにアクセス権を設定するは適切である。

求める答えはエとなる。

問30　エ

Ｗｅｂビーコンに関する問題である。

Ｗｅｂビーコンは、Ｗｅｂページに埋め込まれた情報収集用の極めて小さい画像のことで、利用者のアクセス動向などを収集するために用いられる。大手サイトを中心に利用されている。求める答えはエとなる。

問31　ウ

ＷｅｂサーバとのＨＴＴＰ通信に関する問題である。

ＨＴＴＰ通信では、ＴＣＰのポート番号８０を使用して、Ｗｅｂサーバとの通信を行う。ＰＣに侵入したマルウェアは、業務上のＷｅｂ閲覧と同じ条件でサーバへのアクセスを行い、侵入を図る。

アのＤＮＳサーバのポート番号は５３、イのＨＴＴＰＳは４４３、ウのＨＴＴＰは８０、エのドメイン名の名前解決に使用されるのはＵＤＰの５３である。求める答えはウとなる。

問32　ウ

パケットフィルタリングに関する問題である。

通信を行う場合、通信前にポート番号を決める必要がある。通常、ポート番号はアプリケーションごとに標準で決められた番号があり、０～１０２３の番号が割り当てられている。インターネット上のＷｅｂサーバと通信を行う場合はサーバ側のポート番号は８０を用いる。

この問題では、社内のＰＣからインターネット上のＷｅｂサーバにアクセスする場合であるから、Ｗｅｂサーバでのポート番号は８０、ＰＣのポート番号は１０２４以上を用いる。

ＰＣからの発信は、送信元はＰＣ、あて先はＷｅｂサーバ、送信元ポート番号１０２４以上、あて先ポート番号８０であり、サーバからの応答は、送信元はＷｅｂサーバ、あて先はＰＣ、送信元ポート番号８０、あて先ポート番号１０２４以上となる。求める答えはウとなる。

問33　ウ

認証デバイスに関する問題である。

アのＩＥＥＥ８０２．１Ｘ(ＥＡＰ-ＴＬＳ)は、無線ＬＡＮなどで利用される認証プロトコルの１つである。ネットワークのセキュリティを高めるＥＡＰ(Extensible Authentication Protocol)に対応し、サーバ／クライアントの双方で電子証明書を利用する方式のためセキュリティが、より強化される。また、電子証明書の保管にＵＳＢ認証トークン、指紋認証トークンなどを用いることで、さらにセキュリティレベルを強化することができる。

イの確実な通信を行える接触型は主に、より堅牢なセキュリティが求められる決済や認証の分野で使われている。非接触型とは、カード内部にアンテナの役目を果たすコイルが内蔵されており、端末のリーダ／ライタから発生している磁界にカードをかざすと無線通信でデータのやりとりができる。鉄道改札や入退室管理など、より利便性を求められるジャンルで活用されている。

ウの虹彩認証は、眼球の黒目に現れる皺のパターンを識別して本人確認を行う認証方式であり、人体の特徴を利用するバイオメトリクス認証(生体認証)の一つである。カメラで眼の部分を撮影

し、コンピュータで虹彩のパターンを抽出して認証する。非接触式であるため衛生的で、心理的抵抗が少ない。顔や声のように年をとっても変化することがなく、指紋のような偽造も難しい。認証率も高く、処理するデータ量も少なくて済むという。求める答えはウとなる。

エの静電容量方式の指紋認証デバイスはＬＥＤ照明の下でも正常に認証でき、活用されている。

問34　イ

２要素認証に関する問題である。

２要素認証は、ユーザが知っているもの（ID・パスワード）とユーザが持っているもの（複製できない、もしくは複製しづらい機器）を組み合わせてセキュリティレベルを高める方法である。２つの要素が揃っていないと認証を完了することができないため、たとえＩＤ・パスワードが漏えいしてしまっても、もう1つの要素がない限りはログインすることができない仕組みである。

アの２本の指の指紋は、ユーザがもっているものの組合せであり、不適である。

イの虹彩とパスワードは、ユーザがもっているものと知っているものの組合せであるから、２要素認識となる。求める答えはイとなる。

ウの２種類のパスワードは、ユーザが知っているものの組合せであり、不適である。

エの異なる２つのパスワードは、ユーザが知っているものの組合せであり、不適である。

問35　イ

スマートフォーンのディジタル証明書に関する問題である。

デジタル署名は個人認証システムと通信文の暗号化システムの組み合わせで実現するシステムである。送信側は送信元の秘密鍵を用いて署名を復号し、署名を含んだ通信文を受信先の公開鍵で暗号化し伝送する。受信側では、その通信文を受信側の秘密鍵で復号し平文を得て、送信元の公開鍵を用いて暗号化することによって送信者のデジタル署名を得ることができる。メッセージの受信者が、そのメッセージは正当な送信者が署名したものであり、途中で改変されていないことを確認できるシステムである。

ディジタル証明書が導入されたスマートフォーンは社内システムへのアクセスが許可されたデバイスであること認証している。求める答えはイとなる。

問36　イ

パスワードリマインダに関する問題である。

パスワードリマインダはユーザがパスワードを忘れた際の救済措置である。本人しか知らない秘密情報をユーザに登録してもらい、パスワード忘れの際には、その情報をユーザ認証の代用とすることで、パスワードを再発行する仕組みである。パスワードリマインダは、認証の機会が増えることでセキュリティが弱くなるため、できればパスワードリマインダを設けない方がよい。

パスワード再設定/再発行手順

パスワードリマインダの「合言葉」が一致したら、パスワード再設定に次の手順を踏むことが推奨されている。

①　パスワードリマインダのＷｅｂページ上で１回限り有効なキーをユーザに発行する。

②　１回限り有効な別のキーを含むＵＲＬを、ユーザがあらかじめ登録している電子メールアドレス宛送信する。

③　ユーザにそのＵＲＬのＷｅｂページにアクセスしてもらい、先ほどのキーを入力してもらう。

④　キーが照合できたらパスワードの再設定あるいは再発行を行う。

⑤　一定回数以上照合に失敗したら２つのキーは無効にする。

アの場合、暗号化されていないと盗聴されてパスワードが盗まれる。

イの場合の一時的なパスワード再設定ページへのＵＲＬを送るのが安全な方法であり、キーが照合できたらパスワードの再設定あるいは再発行を行う。求める答えはイとなる。

ウ、エの場合、攻撃者が任意のメールアドレスを指定できてしまうため危険である。

問37　イ

認証局の役割に関する問題である。

認証局は公開鍵とその所有者を対応づけるために電子証明書を発行する機関である。認証局では、各ユーザからの電子証明書の発行依頼を受けると、そのユーザの本人確認を行った後に、正しいユーザである場合にのみ電子証明書を発行する。電子証明書には所有者の識別情報や公開鍵などが記載されている。

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。求める答えはイとなる。

問38　ア

CAPTCHAに関する問題である。

CAPTCHAは、Ｗｅｂページの入力フォームなどで、ロボットによる自動入力を防止するために人間であることを証明させるテストである。歪んだ文字や数字が埋め込まれた画像を表示して、何が書かれているかを入力させる方式がもっとも有名である。画像によるCAPTCHAは、コンピュータによる文字認識処理では読み取れないほど形を歪められたりノイズがかけられた文字や数字が並んでおり、正しい文字を読み取って入力できれば、人間が入力していると推測できる。CAPTCHAによる認証は、迷惑メール業者が無料メールサービスのアカウントを大量取得するのを防いだり、電子掲示板を巡回して広告を自動投稿するプログラムを拒否したり、オンライン投票で大量投票を行うプログラムをブロックしたりするのに使われる。

アのCAPTCHAは、ゆがめたり一部を隠したり画像から文字を判読させ入力させることで、人間以外による自動入力を排除する技術である。求める答えはアとなる。

イのＱＲコードは、自動で高速読み取りができるように開発された２次元コードである。

ウの短縮ＵＲＬは、Webサイトが使うＵＲＬを短く変換したもので、Webサービスとして運営されている短縮ＵＲＬサービスを使うことで、アルファベット数文字程度にする。

エのトラックバックpingは、あるブログからサーバーに対し、更新をしたこととその内容を伝えるためのメカニズムのことである。

問39　ウ

パケットフィルタリングに関する問題である。

通信を行う場合、通信前にポート番号を決める必要がある。通常、ポート番号はアプリケーションごとに標準で決められた番号があり、０～１０２３の番号が割り当てられている。インターネット上のＳＭＴＰサーバと通信を行う場合はサーバ側のポート番号は２５を用いる。

この問題では、社内のＰＣからインターネット上のＳＭＴＰサーバにアクセスする場合であるから、ＳＭＴＰサーバでのポート番号は２５、ＰＣのポート番号は１０２４以上を用いる。

ＰＣからの発信は、送信元はＰＣ、あて先はＳＭＴＰサーバ、送信元ポート番号１０２４以上、あて先ポート番号２５であり、サーバからの応答は、送信元はＳＭＴＰサーバ、あて先はＰＣ、送信元ポート番号２５、あて先ポート番号１０２４以上となる。求める答えはウとなる。

問40　ウ

認証局の役割に関する問題である。

認証局は公開鍵とその所有者を対応づけるために電子証明書を発行する機関である。認証局では、各ユーザからの電子証明書の発行依頼を受けると、そのユーザの本人確認を行った後に、正しいユーザである場合にのみ電子証明書を発行する。電子証明書には所有者の識別情報や公開鍵などが記載されている。

認証局の主な役割には次のものがある。

①　申請者の公開鍵にディジタル署名を付したディジタル証明書を発行する
②　ＣＲＬ(証明書失効リスト)を発行する
③　ＣＰＳ(認証局運用規定)を公開する
④　ディジタル証明書を検証するための認証局の公開鍵を公開する
⑤　認証局の秘密鍵を厳重に管理する

ウの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。求める答えはウとなる。

アはＮＴＰ、イ、エは公開鍵を証明するディジタル証明である。

問41　ア

ＷＡＦに関する問題である。

ＷＡＦは、外部ネットワークからの不正アクセスを防ぐためのソフトウェアあるいはハードウェアであるファイアウォールの中でも、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ことのできるファイアウォールである。

ＷＡＦの特徴は、従来のファイアウォールがネットワークレベルで管理していたことに対して、アプリケーションのレベルで管理を行う。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という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サーバを仲介するかたちで存在し、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に対して、「攻撃」と見なして拒絶することができる。

アはＷＡＦ、イはＷＰＡ２、ウは総合ログ管理システム、エはＵＴＭである。求める答えはアとなる。

問42　ウ

ＣＳＩＲＴに関する問題である。

ＣＳＩＲＴ(シーサート)は、コンピュータセキュリティにかかるインシデントに対処するための組織の総称で、インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動をしいる。シーサートの活動は、目的、立場、活動範囲、法的規制

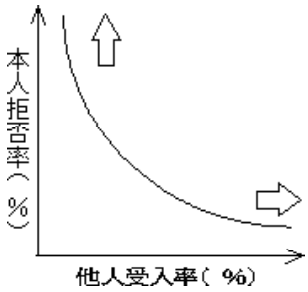
などの違いからそれぞれ独自で活動を行ってきた。 しかし、コンピュータセキュリティインシデントの攻撃が巧妙かつ複雑になり、迅速な対応には、単独のシーサートでは困難な状況になってきている。日本国内の企業事情を巧みに利用した攻撃手法などによるコンピュータセキュリティインシデントや、対応ノウハウの蓄積が難しい標的型攻撃などの存在があり、インターネットの発達、ビジネスにおけるＩＴへの依存度の高まりから、コンピュータセキュリティインシデントの発生リスクも大幅に高まり、攻撃が単なる愉快犯から、経済的利益を目的とした犯行へと移り変わっており、その手法も高度化、複雑化し、問題の把握がより難しくなる傾向にある。これらに適切に対処するためには、同じような状況や課題を持つシーサート同士による緊密な連携と、インシデント関連情報、脆弱性情報、攻撃予兆情報などを互いに収集し、積極的に共有する必要があり、互いに協調し、高いレベルでの緊密な連携体制の実現を目指し、共通の問題を解決する場を設けることを目的とした日本シーサート協議会が設立された。

アはＩＣＡＮＮ、イはＩＥＴＦ、ウはＣＳＩＲＴ、エはハクティビストである。求める答えはウとなる。

問43　イ

生体認証システムに関する問題である。

ＦＲＲ(本人拒否)は本人同士のデータの照合で不一致と判定されることことである。ＦＡＲ(他人受入)は本人と他人のデータの照合で一致と判定されることである。



ＦＲＲとＦＡＲは相関関係にあり、片方の比率を上げるともう片方の比率が下がる。安全性を重視すると、ＦＡＲを小さくする必要があるが、その場合ＦＲＲが上がり、使い勝手に影響がでる。逆に利便性を重視するためにＦＲＲを下げると、ＦＡＲが上がってしまい、安全性が低下してしまう特徴がある。

生体認証システムを導入する場合、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必要がある。求める答えはイとなる。

問44　エ

SMTP-AUTHに関する問題である。

アのAPOPは、POP3は利用者がメールサーバにユーザ名とパスワードをそのまま送信するため、通信途上に悪意の第三者がいる場合、容易にパスワードを盗まれてしまうという問題があったが、APOPではハッシュ関数などを用いてパスワードを暗号化して送受信することにより、容易に盗聴できないようにすることができる。

イのPOP3Sは、POP3による接続前にSSL/TLSで伝送路を暗号化するもので、メールや添付ファイルのデータだけでなくPOP3では平文で送受信されていたユーザ名とパスワードも暗号化されるため、盗聴によるアカウント乗っ取りなどの危険も低くなる。

ウのS/MIMEは、電子メールソフトのために暗号技術を使って、認証、通信文の完全性、発信元の否認防止、プライバシーとデータの機密保護などのセキュリティ機能を提供する。

エのSMTP-Authは、メールクライアントからSMTPサーバへメールの送信依頼を行う際に認証過程を導入し、クライアント側にアカウント名やパスワードを申告させて確かに正規の利用者であることを確認してから送信を受け付けるようにする認証方法である。求める答えはエとなる。

問45　ウ

タイムスタンプサービスに関する問題である。

タイムスタンプは、タイムスタンプに刻印されている時刻以前にその電子文書が存在していたこと（存在証明）と、その時刻以降、当該文書が改ざんされていないこと（非改ざん証明）を証明するものである。

アは標準時配信サービス、イはバイオメトリックス認証、ウはタイムスタンプサービス、エはＮＴＰである。求める答えはウとなる。