gzn030402 「暗号化と電子署名」解答解説

問１　ア

傍受や盗聴と暗号化に関する問題である。

傍受・盗聴は、通信回線上を転送されているデータを相手に知られないように入手する犯罪の１つである。高度な技術と機器が必要であり、探知は難しい。

アの暗号化は、傍受や盗聴されても直ちに内容が把握されることにならないため、被害を避ける対策としては効果がある。求める答えはアとなる。

イのデジタル署名は、発信者の認証である。

ウのファイアフォールは、システムへの不正アクセスの防止である。

エのメッセージ認証は、通信上での情報の改変やエラーの検査のために有効な手段であり、傍受や盗聴防止には役立たない。

問２　イ

公開鍵暗号方式の鍵に関する問題である。

公開鍵暗号方式は送信元は受信先（Ｎさん）の公開鍵を利用して暗号化し、受信先は（Ｎさん）秘密鍵を利用して復号する。求める答えはイである。

問３　ウ

公開鍵暗号方式に関する問題である。

送信者は受信者の公開鍵で暗号化し、受信者は自分の秘密鍵で復号する。求める答えはウとなる。

アの暗号化は送信者の自分の公開鍵が誤りで、受信者の公開鍵である。

イの暗号化は送信者の秘密鍵ではなく、受信者の公開鍵で行い、復号は受信者の秘密鍵になる。

エの暗号化は受信者の秘密鍵ではなく、受信者の公開鍵で行い、復号は自分の秘密鍵で行う。

問４　イ

公開鍵暗号方式の鍵に関する問題である。

公開鍵暗号方式は暗号化鍵と復号鍵は等しくなく、暗号化鍵は公開で、復号鍵は秘密であり、求める答はイとなる。

問５　ウ

電子メールの公開鍵暗号化方式による暗号化の問題である。

送信者はＸさん、受信者はＹさんであるから、Ｘさんが使用する鍵はＹさんの公開鍵である。求める答えはウとなる。

問６　ウ

公開鍵暗号方式に関する問題である。

顧客から注文内容の秘密を商店が守ることであり、商店の関係者以外に秘密にしなければなら

ないため、商店は秘密鍵、顧客は公開鍵を使用する必要がある。求める答えはウとなる。

問７　ウ

暗号方式に関する問題である。

アの公開鍵暗号方式は送信者は受信者の公開鍵を利用して暗号化し、受信者は自分の秘密鍵で復号する。暗号鍵は公開されている。秘密時に配信する必要はない。

イの公開鍵暗号方式は秘密鍵暗号方式と比べて処理方法が複雑なため処理速度も速くはない。単純で高速であるは誤りである。

ウの内容は秘密鍵暗号化方式の鍵管理の方法として実用化されており正しい。求める答えはウとなる。

エの同一の秘密鍵を多数の通信相手に使用すると秘密鍵でなくなるため安全でない。

問８　エ

公開鍵暗号方式に関する問題である。

アは、暗号化鍵、暗号化アルゴリズムは公開であり、復号鍵が秘密である。

イは、暗号化アルゴリズムも公開でよい。

ウは、暗号化鍵は公開で、復号鍵が秘密である。

エの復号鍵は秘密、暗号化鍵は公開は適切である。求める答えはエとなる。

問９　エ

暗号化に関する問題である。

アのＤＥＳは、秘密鍵暗号方式であり、ＲＳＡは公開鍵暗号方式である。

イの公開鍵暗号方式では暗号化鍵を公開する。復号鍵の公開ではない。

ウのデジタル署名に利用するのは公開鍵暗号方式である。秘密鍵方式ではない。

エの秘密鍵暗号方式は暗号化の鍵と復号の鍵は同じである。求める答えはエとなる。

問10　イ

暗号に関する問題である。

アのＤＥＳは秘密鍵暗号方式であり、公開鍵暗号方式ではない。

イのＲＳＡは素因数分解を利用した公開鍵暗号方式である。求める答えはイとなる。

ウの鍵の管理が問題になるのは秘密鍵暗号方式であり、公開鍵暗号方式ではない。

エの公開する鍵は受信者の暗号化鍵であり、復号鍵ではない。

問11　ア

ＤＥＳの暗号化方式に関する問題である。

アのアルゴリズムが公開されている秘密の共通鍵暗号方式である。ＤＥＳの内容であり、求める答えはアである。

イの暗号化鍵を公開し復号鍵を秘密にするのは公開鍵暗号方式であり、ＲＳＡ方式である。

ウの処理に時間がかかり認証機能に優れているのは公開鍵暗号化方式のＲＳＡ方式である。

エの暗号文は必ず解読が可能なものであり、平文に戻すことができないは誤りである。ＤＥＳ

方式は鍵の管理が的確に行われると安全性の高い方式である。

問12　ウ

公開鍵暗号方式の暗号化鍵に関する問題である。

アの復号鍵を暗号化鍵から計算によって求めることができるのなら、暗号化鍵が公開されているからもともと暗号化の意味がなくなる。

イの復号鍵を事前に暗号化鍵から計算によって求めることができるなら、暗号化鍵が公開されていることから、暗号化の意味がなくなる。

ウの受信側が暗号化の鍵を知っていることは、受信側しか知らなければ公開鍵で暗号化しても暗号化の意味があることになる。求める答えはウとなる。

エの暗号鍵から算出した復号鍵を受信側に渡しても、暗号鍵が公開されているから、暗号化の意味がなくなる。

問13　ア

共通鍵暗号化方式の名称に関する問題である。

アのＤＥＳは米国の商務省標準局によって制定された共通鍵暗号方式である。求める答えはアとなる。

イのＲＳＡは大きな数の素因数分解の困難性を利用したもので、公開鍵暗号方式である。

ウのエルガマル暗号は離散対数問題の困難性を利用したもので、公開鍵暗号方式である。

エの楕円曲線暗号は楕円曲線上の離散対数問題の困難性を利用したもので、公開鍵暗号方式である。

問14　イ

公開鍵暗号方式に関する問題である。

ア、ウ、エの内容は秘密鍵暗号方式であり、イの内容が公開鍵暗号方式である。求める答えはイとなる。

問15　イ

デジタル署名に関する問題である。

公開かぎ暗号方式で、送信者を保証する方式は、送信者が自分の秘密かぎで暗号化し、受信者が送信者の公開かぎで復号する場合である。求める答えはイとなる。

問16　ウ

暗号文に関する問題である。

ＤＥＥＲ→ＥＲＤＥ　　ＤＩＤＤ→ＩＤＤＤ　　ＲＥＡＭ→ＥＭＲＡ　　ＤＥＥＰ→ＥＰＤＥ

従って、ＥＲＤＥＩＤＤＤＥＭＲＡＥＰＤＥとなり、求める答えはウである。

問17　イ

排他的論理和の論理演算によって暗号化する問題である。

元のデータとかぎの１０１０との排他的論理和が００１０となる元のデータを求めればよいこ

とになる。答は１０００となり、求める答えはイとなる。

問18　ウ

シーザ暗号に関する問題である。

ｃ→ｇ、ａ→ｅ、ｓ→ｗ、ｈ→ｌであるからＮ＝４である。求める答えはウである。

問19　エ

デジタル署名に関する問題である。

デジタル署名は電子メールの送信者が間違いなく本人であることや、文書やデータが改ざんされていないことを確認するための方法である。文書の送信者が文書をハッシングと呼ばれる手法でダイジェストという短いコードに変換し、このダイジェストを送信者の秘密鍵で暗号化したものがデジタル署名となり、これを元の文書とともに受信者に送付する。受信者はデジタル署名を送信者の公開鍵で復号し、ダイジェストを作成する。送信者のダイジェストと受信者が再作成したダイジェストが一致すれば、送信者本人からのメールであることを確認できる仕組みである。

アは受信者の公開鍵と秘密鍵であり、誤りである。

イは受信者の公開鍵が誤りである。

ウは受信者の秘密鍵が誤りである。

エの送信者の秘密鍵と公開鍵が正しい。求める答えはエとなる。

問20　イ

公開鍵暗号方式に関する問題である。

公開鍵暗号方式は通信文を送信する場合、送信元で公開鍵により暗号化し、受信先で専用の秘密鍵で復号する方式である。暗号化する鍵と復号する鍵が異なり、片方の鍵を公開し、もう一方の鍵は秘密にした暗号化方式である。代表的なものにＲＳＡ方式がある。公開鍵から秘密鍵を発見することは不可能であり、公開鍵を管理する必要がない。秘密鍵は自分だけが持てばよいので、鍵管理が簡単で安全度が高い。論理が複雑なため処理時間が長くなり、処理速度は共通鍵方式よりも遅い。公開鍵暗号を守秘に使う場合、送信者は受信者の公開鍵を用いて暗号化し、暗号文を送る。受信者は自分だけが知っている秘密鍵を用いて復号し、元の平文を得ることができる。鍵の配布やデジタル署名に利用される。

アのＡＥＳは共通鍵暗号方式である。

イのＲＳＡは素因数分解の計算の困難さを利用した公開鍵暗号方式である。求める答はイとなる。

ウの公開鍵暗号方式の利用者が増加しても、鍵は公開されているので煩雑にはならない。

エの公開するのは受信者の暗号化鍵である。

問21　エ

公開鍵暗号方式に関する問題である。

アのＡＥＳは、アメリカ合衆国の新暗号規格（Advanced Encryption Standard）として規格化された共通鍵暗号方式である。

イのＤＳＡは、離散対数問題に基づく公開鍵暗号を応用して開発された、デジタル署名方式の

一つである。

ウのＩＤＥＡは、ＰＧＰやＳＳＨなどで使用される秘密鍵暗号方式である。

エのＲＳＡは、桁数が大きい合成数の素因数分解問題が困難であることを安全性の根拠とした公開鍵暗号の一つである。求める答えはエとなる。

問22　エ

ディジタル署名の鍵に関する問題である。

ディジタル署名の作成には発信者の秘密鍵を使用し、ディジタル署名の検証には発信者の公開鍵を使用する。求める答えはエとなる。

問23　エ

電子署名に関する問題である。

電子署名は送信元は送り手の秘密鍵を用いて署名文(暗号文)にし、受信先は送り手の公開鍵を用いて平文にする。通常、平文を署名文に変換することを復号、署名文を平文に変換することを暗号化という。

ａは送り手の秘密鍵、ｂは送り手の公開鍵であり、求める答えはエである。

問24　エ

デジタル署名に関する問題である。

署名が意味があるのは署名者しか署名できないからである。署名の内容を暗号化する場合に署名者しか暗号化の方法が判らないようにする必要がある。デジタル署名は公開鍵暗号方式を利用して署名者が秘密鍵をもち、署名を受信する人が署名者の公開鍵でメッセージを平文に復号するので、信頼性と公開性の上で意味のあるものになる。

アの受信者が署名鍵で平文に戻しても、多くの人が署名鍵を持つことになると署名の意味がなくなってしまうことになる。

イの送信者が署名の意味を関係者以外に分からないようにすると、関係者以外は署名の内容を把握することができない。関係者のみが知るための手段が問題になる。

ウの平文の冗長性のみで署名が可能になるならば暗号化の意味がない。もともと暗号化は冗長性を加えて意味不明のメッセージに一定のルールによって行う手段であり、他人がそれを実行できないところに価値がある。署名の信頼度を高める技術が問題になる。

エは公開鍵暗号方式の仕組みであり、正しい。求める答えはエとなる。

問25　エ

デジタル署名のメッセージの暗号化の方法に関する問題である。

発信者は自分の秘密鍵でメッセージのハッシュ値を暗号化する方法で行う。求める答えはエとなる。

アは相手の公開鍵でなく、自分の秘密鍵である。

イは相手の秘密鍵でなく、自分の秘密鍵である。

ウは自分の公開鍵でなく、自分の秘密鍵である。

問26　ウ

ディジタル署名に用いるハッシュ関数の特徴に関する問題である。

ドキュメントや数字などの文字列の羅列から一定長のデータに要約するための関数・手順のことをハッシュ関数という。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。１方向関数による生成であるので、ハッシュ値を変更しないまま元データを改ざんすることはできないため、認証と完全性検査に用いられる。

メッセージダイジェストからメッセージを復元することは困難である。求める答えはウとなる。

問27　ウ

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、本人確認ともいわれ、相手が確かに本当の相手であることを確認する手段である。単純な方式ではパスワードを使用する。第三者のなりすましに対する対策である。

メッセージ認証には、データの完全性と否認防止がある。データの完全性は、通信途上で、内容が改ざんされていないことを検査し、保証する手段であり、第三者の不正に対する対策である。否認防止は、送信側は、送ったことを否定できないことの保証であり、受信側は、受け取ったことを否定できないことの保証である。

相手認証以外の目的であるから、メッセージ認証である。ウの署名が行われた後で、メッセージに変更が加えられていないかどうかを確認することである。求める答えはウとなる。

ア、イは相手認証、ウはメッセージ認証である。

エは盗聴であり、認証では対応できない。

問28　エ

ディジタル署名に関する問題である。

ディジタル署名が使用される認証には、相手認証とメッセージ認証がある。相手認証は、本人確認ともいわれ、相手が確かに本当の相手であることを確認する手段である。メッセージ認証は、データの完全性と否認防止がある。データの完全性は、通信途上で内容が改ざんされていないことを検査し、保証する手段であり、第三者の不正に対する対策である。否認防止は、送信側は送ったことを否定できないことの保証であり、受信側は受け取ったことを否定できないことの保証である。

ディジタル署名は、ソフトウェアの作成者を認証するものであり、署名後変更されていないことを証明するものである。従って、インターネットで公開されているソフトウェアの署名はデータの完全性を保証するものである。求める答えはエとなる。

問29　エ

デジタル署名に関する問題である。

デジタル署名は、電子メールの送信者が間違いなく本人であることや、文書やデータが改ざんされていないことを確認するための方法である。

デジタル署名は秘密鍵と公開鍵を組み合わせた個人認証システムである。

送信元の秘密鍵を用いて復号し、受信先で送信元の公開鍵を用いて暗号化し、元の平文としての署名を得る。文書の送信者が文書をハッシングと呼ばれる手法でダイジェストという短いコードに変換し、このダイジェストを送信者の秘密鍵で暗号化したものがデジタル署名となり、これを文書とともに受信者に送付する。受信者はデジタル署名を送信者の公開鍵で復号し、ダイジェストを作成する。送信者のダイジェストと受信者が再作成したダイジェストが一致すれば、送信者本人からのメールであることを確認できる仕組みである。

発信者は自分の秘密鍵でメッセージを暗号化することによってデジタル署名を行った上で、相手の公開鍵でさらに暗号化することになる。求める答えはエとなる。

問30　ウ

ディジタル署名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。送信者はメッセージのデータに、秘密鍵で作成した署名データを付けて送信する。受信者は公開鍵を使って署名を確認する。

アの第三者に情報が漏れるかどうかはディジタル署名では確認できない。

イの発信された注文がＢ商店についてかどうかは確認できない。

ウの発信者がＡさんであることは確認できる。求める答はウとなる。

エのＡ氏に商品を売ることの許可は確認できない。

問31　ウ

公開鍵暗号方式に関する問題である。

ＡからＢに通信文を送信する時に、暗号化に使用する鍵は受信者Ｂの公開鍵である。ＡはＢの公開鍵で暗号化し、ＢはＢの秘密鍵で復号する。求める答えはウとなる。

問32　ウ

ディジタル署名に関する問題である。

ディジタル署名が使用される認証には、相手認証とメッセージ認証がある。相手認証は、本人確認ともいわれ、相手が確かに本当の相手であることを確認する手段である。メッセージ認証は、データの完全性と否認防止がある。データの完全性は、通信途上で内容が改ざんされていないことを検査し、保証する手段であり、第三者の不正に対する対策である。否認防止は、送信側は送ったことを否定できないことの保証であり、受信側は受け取ったことを否定できないことの保証である。

ディジタル署名は、ソフトウェアの作成者を認証するものであり、署名後変更されていないことを証明するものである。従って、インターネットで公開されているソフトウェアの署名はデータの完全性を保証するものであり、メッセージが改ざんされていないことを保証する。求める答えはウとなる。

問33　エ

暗号化技術の利用目的に関する問題である。

アの否認防止はメッセージ認証によって実現できる。公開鍵暗号方式の利用である。

イの相手認証は公開鍵暗号方式を利用すれば実現する。

ウの守秘は暗号化によって実現できる。

エの通信途中での喪失は防止することができない。途中で情報が失われても、内容が理解できないとか理解に時間がかかる場合には対策を講じることが可能になる。そのために暗号化は意味のあることになる。求める答えはエとなる

問34　ア

盗聴防止対策に関する問題である。

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子である。ログインに必要なＩＤとパスワード、クレジットカード番号、銀行口座番号なとが対象になる。盗聴には電話盗聴、室内盗聴、電子盗聴などがある。盗聴を防止する手段としては暗号化がある。

アの通信の暗号化は盗聴防止に効果がある。求める答えはアとなる。

イのＩＰアドレスの制限、ウのパスワードの設定、エのポート番号の変更などはアクセス制御の役割は果たすが盗聴防止には役立たない。

問35　ウ

ディジタル署名に関する問題である。

アのウィルスチェックは、コンピュータウィルスを発見・駆除するための処理である。

イのジャンクメールフィルタは、迷惑メールを仕分けし、取り除くフィルタである。

ウのデジタル署名は、受発注情報の改ざん、なりすまし、否認の防止に役立つ。求める答えはウとなる。

エのファイアフォールは、システムへの不正アクセスの防止である。

問36　エ

通信文の共通鍵を用いた暗号化方式の問題である。

通信文は共通鍵方式で暗号化し、共通鍵の送信を受信者の公開鍵を用いて暗号化し、受信者は自分の秘密鍵で共通鍵を得て、その共通鍵を使用して通信文を平文に復号する。

セキュリティ上の効果は電子メールの本文の内容の漏洩の防止である。求める答えはエとなる。

問37　エ

Ｓ／ＭＩＭＥに関する問題である。

アのＢＡＳＥ６４は、電子メールに画像などのバイナリデータを添付する際に、中身を文字列データに置換する方式の一つである。

イのＧＺＩＰは、ファイル圧縮形式の一つである。

ウのＰＮＧは、画像フォーマットの一つである。

エのＳ／ＭＩＭＥは、電子メールを暗号化するための方式である。求める答えはエとなる。

問38　イ

Ｓ／ＭＩＭＥに関する問題である。

Ｓ／ＭＩＭＥは電子メールの暗号化と電子署名に関する規格である。インターネット電子メールの標準仕様であるＭＩＭＥを拡張したプロトコルである。なりすまし、盗聴、改ざんといった電子メールに関する不正行為を防ぐための機能を提供している。Ｓ／ＭＩＭＥではＰＫＩを用いるため、認証局で発行する公開鍵証明書を用いて電子署名の正当性を保証している。

Ｓ／ＭＩＭＥの機能は内容の暗号化と署名である。求める答えはイとなる。

問39　ア

ＩＰsecに関する問題である。

ＩＰsecは、暗号技術を用いて、ＩＰパケット単位でデータの改竄防止や秘匿機能を提供するプロトコルである。ＩＰsecはネットワーク層のプロトコルを保護するので、暗号化がサポートされていない上位層やアプリケーションでもセキュリティの確保が可能になる。ＩＰｖ４ではオプションとして使用することができるが、次世代のＩＰｖ６では標準で実装される。

アのＩＰsecは、ネットワーク層でＩＰによる通信を暗号化するためのプロトコルである。求める答えはアとなる。

イのＰＰＰは、２地点間で回線をつなぎリンクを確立するためのプロトコルである。パソコンからプロバイダのルータまでの間を電話回線でつなぐ場合に利用する。

ウのＳＳＨは、暗号や認証の技術を利用して、安全にリモートコンピュータと通信するためのプロトコルで、ＰＯＰ３やＦＴＰなどネットワーク上に平文のパスワードが流れてしまう既存のプロトコルを安全に使用する技術として広く利用される。

エのＳＳＬは、Ｗｅｂブラウザと Ｗｅｂ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ためのプロトコルである。

問40　エ

コンピュータ不正アクセス対策基準に関する問題である。

コンピュータ不正アクセス対策基準は、コンピュータ不正アクセスによる被害の予防、発見及び復旧並びに拡大及び再発防止について、企業等の組織及び個人が実行すべき対策をとりまとめたものである。システムユーザ基準、システム管理者基準、ネットワークサービス事業者基準及びハードウェア・ソフトウェア供給者基準から構成される。

この基準で考えられている「不正アクセス」とは、システムを利用する者が、その者に与えられた権限によって許された行為以外の行為をネットワークを介して意図的に行うことである。

「システムユーザ」が実施すべき対策として、パスワード及びユーザＩＤ管理、情報管理、コンピュータ管理、事後対応、教育及び情報収集、監査ついてまとめられている。

アの監視効率向上のため単純にネットワーク相互接続したり、ファイルを共有することは、セキュリティ上問題がある。

イの利用者ユーザＩＤの共有は問題がある。ユーザＩＤは個人単位に設定するのが原則である。

ウのシステム管理者が全ての権限をもつ利用者ＩＤを常に使用するのは不適合である。システム管理者が不正を働く危険性がある。

エのセキュリティ方針の文書化、定期的な研修は適合している。

問41　エ

利用資格の正当性チェックと利用状況の把握に関する問題である。

ユーザＩＤはユーザの識別子で、そのユーザがそのシステムを使う権利があるかどうかを判断するのに利用する。ユーザＩＤとパスワードの差異の認識が重要である。

アのＩＰアドレスはＴＣＰ／ＩＰで通信する場合に通信元や通信先を識別するためのアドレスである。

イのアクセス権はデータやプログラムを読み書きし、それを利用することを認めた権利である。

ウのパスワードは正当なユーザかどうかを確認するための合い言葉である。

エのユーザＩＤはコンピュータの利用時にユーザを認識するために、個々のユーザに与えられた番号であり、英字と数字が用いられる。システムへのアクセス権を判断するのに利用したり、使用実績の把握に用いる。求める答えはエとなる。

問42　ア

インターネットのセキュリティに関する問題である。

アのデータベースサーバを利用する場合に不正アクセスの防止やデータの改ざん対策が必要になる。求める答えはアとなる。

イの暗号化は、第三者へ内容が漏洩しないようにするために、ある一定の規則に従ってデータを変換することである。暗号化は電子メールの到達確認とは異なる。

ウの利用者認証システムは、ネットワーク経由でコンピュータにアクセスしてくるユーザーが登録済みか否かを信頼できる方法で確認するソフトウエアである。中心部分は認証サーバと呼ぶソフトウエアで、ユーザーの名前やパスワードなどを一括管理する。インターネットを利用するためには必ずしも必要としない。個人ユーザがプロバイダーと契約してインターネットを利用する場合には、プロバイダーのシステムを経由するために認証が必要になるだけである。

エのファイアウォールは、インターネットとＬＡＮとの間に置くことでデータ通信を管理し、外部からの攻撃や不正アクセスから内部ネットワークを守る仕組みである。ファイアウォールを設置しても社内からの重要情報の流出を自動的に防止できない。

問43　エ

セキュリティ技術に関する問題である。

アのフォルトトレラント技術は、システムの一部に障害が起きても全体を停止させずに稼働を続け、その間に復旧を図る考え方である。この技術は地震や火災に対しては意味がない。

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り、ファイアフォールやディスクアレイシステムで防ぐことはできない。

ウのＣＲＣ方式は、バーストエラーやランダムエラーなどの通信上の誤りを検出する方式であり、データの不正アクセス防止の対策にはならない。

エのメッセージの改ざんやなりすまし防止にディジタル署名は効果的である。求める答えはエとなる。

問44　イ

ユーザ認証の問題である。

パスワードは正当なユーザを確認するための合い言葉であり、設定上次のことに留意する。

① パスワード入力の際にパスワード自体の表示や印字を抑止する。

② パスワードの有効期限を設定する。

③ パスワードを暗号化してファイル上に格納する。

④ パスワードを保存するパスワードファイルのアクセスを制限する。

⑤ 高度パスワードを適用し、類推できるようなパスワードの使用を制限する。

⑥ 初期パスワードの設定をする。

⑦ 初期パスワードは、初回だけ仮パスワードで情報処理システムへアクセスを許し、ファイルアクセス前にユーザ側で正式のパスワードに変更しなければならない方法にする。

アのパスワードの変更は、有効期限を設定し、絶えず変更する必要がある。変更を禁止するのは誤りである。

イのコールバックは本人であるかどうかの認証方法の一つて、折り返し電話をすることで本人確認をする方法である。求める答えはイとなる。

ウのユーザがパスワードを確認できるように端末に表示するのは誤りで、パスワードの表示や印字は行ってはならない。

エの一定回数間違ったからといって、親切に相手に通知するのは誤りである。

問45　エ

データの改ざんや破壊防止に関する問題である。

災害や情報セキュリティのシステム的対策として次のことが考えられる。

① システム・回線の多重化等のフォルトトレラント技術、

② バックアップ技術、無停電電源などの信頼性技術、

③ 暗号、ユーザ認定、アクセス制御などの情報セキュリティ技術

データの改ざんや破壊を防止する最も効果的な方法はセキュリティ技術であり、ファイルへのアクセス権限の設定が効果的である。

ア、ウの内容は障害発生時の回復処理には必要であるが、改ざんや破壊防止には役立たない。

イは改ざんの検出には役立つが防止にはならない。

エのファイルへのアクセス権限の設定はデータの改ざんや破壊防止に効果的である。求める答えはエとなる。

問46　ウ

ユーザＩＤ管理に関する問題である。

あるコンピュータをユーザーが使う時に、コンピュータはユーザーＩＤを使って、そのユーザーがそのコンピュータを使う権利があるかどうかを識別する。ＩＤは各ユーザーの識別子であり、このＩＤを管理することをユーザＩＤ管理という。

ユーザ管理の主な目的は次の通りである。

① 資源利用の把握に活用し、合わせて発生する費用の配賦に使用する。

② 資源の将来的な設備増強など設備計画に活用する。

③ 障害発生時に影響の及ぶユーザへ迅速な連絡に活用する。

④ 利用権を持たない利用者を制限し、情報処理システムの安全性や、信頼性、性能維持の

確保に利用する。

⑤　ユーザ支援の一貫として、情報処理システム広報作業など効率性向上のために利用する。

ユーザＩＤの付け方は次の通りである。

①　英数字の組合せで構成されたものが一般的である。

②　個人単位のユーザに付与する。ユーザがどのような利用者であるかも体系づける。

③　先頭に利用者の作業内容を示す英字を付ける。

④　ユーザＩＤによるアクセス権を設定する。

アのプロジェクトで皆同じユーザＩＤを用いるのは間違いで、個人単位に付与する。個人の識別子を用いて、ユーザの資源利用の実態把握と不当アクセス防止などの管理を行う。

イの同一人が複数のＩＤカードをもつのは管理上不合理になる。アクセス権の設定などのユーザＩＤに付与する権限か不明確になる。

ウのユーザＩＤの権限を設定する場合に権限は必要最小限のものにし、利用目的、利用期限を明確にする。求める答えはウとなる。

エのユーザＩＤの抹消は利用目的が完了した時点で直ちに抹消する必要がある。

問47　エ

パスワードの文字数と種類の数、その調査に必要な時間を求める問題である。

パスワードの文字数は５文字で、使用できる文字は英字２６文字、数字１０文字の計３６文字である。これらの文字でできるパターンの種別は36^5＝６０４６６１７６となる。

一つのパスーワードの調査に０．５秒必要であるから、全部のパスワードの検査には次の時間がかかることになる。

３０２３３０８８(秒)→８３９７(時間)→３５０(日)→１(年)

求める答えはエとなる。

問48　ア

データベースの不正利用防止の方法に関する問題である。

アのアクセス権の設定は正当な利用者のみにアクセスを許可するものであるから、不正な利用者のアクセスを防止することができる。求める答えはアとなる。

イの一貫性維持の制御は状態の変化が正しく反映されるとか矛盾を発生させない性質であり、複数のデータベースで論理矛盾を発生させないように、矛盾が発生する恐れがある場合には、すべてのデータベースを元の状態に戻すことによって回避する方法である。不正利用者のアクセス防止にはならない。

ウのデータのカプセル化は、データとその操作法を一体にすることによって独立性を保つことは可能になるが不正アクセスの防止にはならない。

エのファイルの二重化は故障時の停止を防止でき信頼性の向上にはなるが、不正利用者のアクセス防止にはならない。

問49　エ

ＩＣカードの暗証番号に関する問題である。

利用者認証を行うには、ＩＣカードのユーザＩＤとそのカードを使用しているのが本人である

ことを確認する暗証番号が必要である。

ＰＩＮコードは、クレジットカードやキャッシュカードの利用に際し持ち主の本人確認のために使われる、秘密の識別番号である。カードを提示した人物が所有者本人であることを確認するために照合される番号で、他人に知られると成りすまして悪用される恐れがあるため、秘密にして暗誦しなければならない。銀行のキャッシュカードなど、多くの場合に４桁の番号が使われる。

アの共通な暗証番号の設定では本人確認は不可能である。

イのＩＣカードの表面に印字している数字情報を組み合わせて暗証番号を作成すると、第三者が推測可能な番号となり、本人確認の機能にはならない。

ウの失効処理の順序が逆である。

エのＩＣカードを配送する場合には暗証番号は同封しない。暗証番号の配送が必要な場合は別経路で配送する。求める答えはエとなる。

問50　ア

パスワードに使用する文字の種類を問題にしている。

パスワードに使用する文字の種類をＭ、パスワードの桁数をｎとするとき、設定できるパスワードの個数は、場合の数の計算で求めると、各桁にＭ通りの文字が使用できるため、M^nとなる。求める答えはアである。

問51　エ

ＩＣカードの暗証番号に関する問題である。

利用者認証を行うには、ＩＣカードのユーザＩＤとそのカードを使用しているのが本人であることを確認する暗証番号が必要である。

ＰＩＮコードは、クレジットカードやキャッシュカードの利用に際し持ち主の本人確認のために使われる、秘密の識別番号である。カードを提示した人物が所有者本人であることを確認するために照合される番号で、他人に知られると成りすまして悪用される恐れがあるため、秘密にして暗誦しなければならない。銀行のキャッシュカードなど、多くの場合に４桁の番号が使われる。

アの共通な暗証番号の設定では本人確認は不可能である。

イのＩＣカードの表面に印字している数字情報を組み合わせて暗証番号を作成すると、第三者が推測可能な番号となり、本人確認の機能にはならない。

ウの失効処理の順序が逆である。

エのＩＣカードを配送する場合には暗証番号は同封しない。暗証番号の配送が必要な場合は別経路で配送する。求める答えはエとなる。

問52　イ

パスワード運用方法に関する問題である。

パスワードは利用者の認証を行うために利用する数字や文字列である。利用制限をかけているコンピュータや共有資源では、ユーザＩＤとパスワードによって利用者であることを認証する。

パスワードは次の特徴をもっている。

①　正当な利用者以外に漏らしてはならない

②　推測しやすいパスワードを設定すると、悪意ある第三者による不正利用の恐れがある。

③　パスワードは数字や文字・記号を混在させた推測しづらいものを使用する。

④　パスワードは有効期限を設定し、適宜変更する。

⑤　パスワードは暗号化してファイルに格納する。

アの内容は、パスワードは本来、本人のみが認識でき変更できるものでなければならないため、管理者と言えども他人のユーザＩＤとパスワードの一覧表を作成し、いつでも確認できるようにすることは誤りである。

イの利用者がいつでも変更できるようにすることはパスワードの運用管理方法として適切である。求める答えはイとなる。

ウの現在利用されていないユーザＩＤとパスワードの再利用は、不正アクセスや情報処理システムの破壊などのトラブルの原因になる。従って、使用停止処理を必ず行う必要がある。

エの利用者登録申請書が到着する前に、ユーザＩＤや仮のパスワードを登録することは間違いである。

問53　イ

キーロガーに関する問題である。

キーロガーは、キーボードからの入力を監視して記録するソフトである。もともとデバッグなどに利用するツールだったが、複数の人間が利用するパソコンに仕掛けてパスワードやクレジットカード番号などを収集するなど、悪用されることがある。

イのネットバンキング利用時に、利用者が入力したパスワードを収集する。

アはプロキシサーバを悪用した中間者攻撃、イはキーロガーの悪用例、ウはアドウェアの悪用例、エはブラウザのアドオン悪用例である。求める答えはイとなる。

問54　ウ

ディジタル署名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。送信者はメッセージのデータに、秘密鍵で作成した署名データを付けて送信する。受信者は公開鍵を使って署名を確認する。

送信者が署名鍵を使って署名を作成し、それをメッセージに付加することによって、受信者が送信者を確認できるようになる。求める答えはウとなる。

アの署名鍵はメッセージダイジェストを暗号化するのに使用する。

イのメッセージダイジェクトの復号に使われるのは送信者の公開鍵であり、ディジタル署名には改ざん部位を特定する機能はない。

エのディジタル署名はメッセージ本文の暗号化を目的としない。

問55　ア

共通鍵暗号方式に関する問題である。

アのＡＥＳは、アメリカ合衆国の新暗号規格（Advanced Encryption Standard）として規格化された共通鍵暗号方式である。求める答えはアとなる。

イのＰＫＩは、公開鍵基盤で、公開鍵暗号を用いた技術・製品全般を指す。

ウのＲＳＡは、桁数が大きい合成数の素因数分解問題が困難であることを安全性の根拠とした公開鍵暗号の一つである。

エのＳＨＡ-２５６は、任意長の原文から固定長の特徴的な値であるハッシュ値を求める計算手順である。

問56　ウ

公開鍵暗号方式に関する問題である。

アのＡＥＳは、アメリカ合衆国の新暗号規格（Advanced Encryption Standard）として規格化された共通鍵暗号方式である。

イのKCipher-２は、九州大学とＫＤＤＩ研究所により共同開発されたストリーム暗号で、共通鍵暗号方式ある。

ウのＲＳＡは、桁数が大きい合成数の素因数分解問題が困難であることを安全性の根拠とした公開鍵暗号の一つである。求める答えはウとなる。

エのＳＨＡ-２５６は、任意長の原文から固定長の特徴的な値であるハッシュ値を求める計算手順である。