gzn030402 「暗号化と電子署名」演習問題

問１

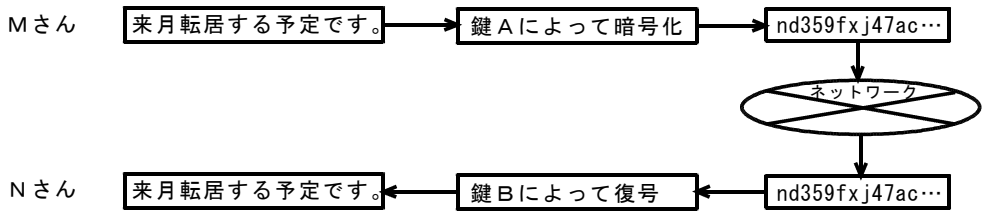
通信の“傍受や盗聴”の被害を避ける対策として，正しいものはどれか。

ア　暗号化　　イ　デジタル署名

ウ　ファイアウオール　　エ　メッセージ認証

問２

公開鍵暗号方式を用いて、図のようにＭさんからＮさんに他人に秘密にしておきたい文章を送るとき、暗号化と復号に用いる鍵として、適切な組合せはどれか。



	鍵Ａ	鍵Ｂ
ア	Ｍさんの秘密鍵	Ｍさんの公開鍵
イ	Ｎさんの公開鍵	Ｎさんの秘密鍵
ウ	共通の公開鍵	Ｎさんの秘密鍵
エ	共通の秘密鍵	共通の公開鍵

問３

公開かぎ暗号方式で，送信者が受信者に暗号文を送る場合の手順はどれか。

ア　送信者は自分の公開かぎで暗号化し，受信者は自分の秘密かぎで復号する。

イ　送信者は自分の秘密かぎで暗号化し，受信者は送信者の公開かぎで復号する。

ウ　送信者は受信者の公開かぎで暗号化し，受信者は自分の秘密かぎで復号する。

エ　送信者は受信者の秘密かぎで暗号化し，受信者は自分の公開かぎで復号する。

問４

公開かぎ暗号方式の暗号化かぎと復号かぎの関係として，適切なものはどれか。

	暗号化鍵と復号鍵の関係	暗号化鍵	復号鍵
ア	暗号化鍵≠復号鍵	公開	公開
イ	暗号化鍵≠復号鍵	公開	秘密
ウ	暗号化鍵＝復号鍵	秘密	公開
エ	暗号化鍵＝復号鍵	秘密	秘密

問５

Ｘさんは，Ｙさんにインターネットを使って電子メールを送ろうとしている。電子メールの内容は秘密にする必要があるので，公開かぎ暗号方式を使って暗号化して，送信したい。電子メールの内容を暗号化するのに使用するかぎとして，適切なものはどれか。

ア　Ｘさんの公開かぎ　　イ　Ｘさんの秘密かぎ
ウ　Ｙさんの公開かぎ　　エ　Ｙさんの秘密かぎ

問６

ある商店が、顧客からネットワークを通じて注文を受けるために、公開鍵暗号方式を利用して、注文の内容が第三者に分からないようにした。商店、顧客それぞれが利用する鍵の適切な組合せはどれか。

	商店	顧客
ア	公開鍵	秘密鍵
イ	公開鍵	公開鍵と秘密鍵
ウ	秘密鍵	公開鍵
エ	秘密鍵	公開鍵と秘密鍵

問７

暗号方式に関する記述のうち、正しいものはどれか。

ア　公開かぎ暗号方式では、暗号かぎを通信相手へ秘密裡に配信する必要がある。
イ　公開かぎ暗号方式では、秘密かぎ暗号方式よりも後で考案され、数学的に巧みな理論を応用しているので、秘密かぎ暗号方式に比べ復号処理が単純で高速なものとなっている。
ウ　秘密かぎ暗号方式のかぎを通信の開始時に公開かぎ暗号方式を使って送り、データの暗号化をそのかぎで行うという方法が実用化されている。
エ　秘密かぎ暗号方式は、多数の相手との通信の際、同一の暗号かぎを用いても安全である。

問８

文書の内容を秘匿して送受信する場合の公開鍵暗号方式における鍵の取扱いのうち，適切なものはどれか。

ア　暗号化鍵と復号鍵は公開してもよいが，暗号化のアルゴリズムは秘密にしなければならない。
イ　暗号化鍵は公開してもよいが，暗号化のアルゴリズムは秘密にしなければならない。
ウ　暗号化鍵は秘密にしなければならないが，復号鍵は公開する。
エ　復号鍵は秘密にしなければならないが，暗号化鍵は公開する。

問９

暗号化に関する記述のうち，正しいものはどれか。

ア　ＤＥＳは公開かぎ暗号方式，ＲＳＡは秘密かぎ暗号方式の代表例である。
イ　公開かぎ暗号方式では，必ず暗号化かぎを秘密にして，復号かぎを公開する。
ウ　デジタル署名に利用するには，公開かぎ暗号方式よりも秘密かぎ暗号方式の方がよい。
エ　秘密かぎ暗号方式では，暗号化かぎと復号かぎは同じである。

問10

暗号に関する記述のうち，適切なものはどれか。.

ア　ＤＥＳは，公開かぎ暗号方式の一種である。
イ　ＲＳＡは，素因数分解の計算の複雑さを利用した公開かぎ暗号方式の一種である。
ウ　公開かぎ暗号方式の難点は，かぎの管理が煩雑になることである。
エ　公開かぎ暗号方式は，暗号化と復号とに異なるかぎを用い，受信者の復号かぎを公開する方式である。

問11

代表的な暗号方式の一つであるＤＥＳについて、正しいものはどれか。

ア　アルゴリズムが公開されている共通鍵方式である。
イ　暗号化鍵だけを公開し、復号鍵を秘密にする方式である。
ウ　処理に時間がかかるが、認証機能に優れインターネットでの利用に適した方式である。
エ　米国政府の標準方式で、盗聴者はもちろん、作成者も暗号文を平文に戻すことはできない安全性の高い方式である。

問12

平文を公開かぎ暗号方式を用いて暗号化するときの“かぎ”に関する記述として，正しいものはどれか。

ア　暗号文を受信した時に，暗号化かぎから計算によって復号かぎを算出する。
イ　事前に，暗号化かぎから計算によって復号かぎを算出しておく。
ウ　受信側は，暗号化かぎを知っている。
エ　送信側は，暗号化かぎから算出した復号かぎを，暗号化されたメッセージ本文とは別に受信側へ渡す。

問13

暗号化方式の名称に関する記述のうち，共通かぎ方式に分類されるものはどれか。

ア　ＤＥＳ　　イ　ＲＳＡ　　ウ　エルガマル暗号　　エ　だ円曲線暗号

問14

公開鍵暗号方式に関する記述として，適切なものはどれか。

ア　ＡＥＳなどの暗号方式がある。
イ　ＲＳＡや楕円曲線暗号などの暗号方式がある。
ウ　暗号化鍵と復号鍵が同一である。
エ　共通鍵の配送が必要である。

問15

公開かぎ暗号方式の用法に関する記述のうち，送信者が間違いなく本人であることを受信者が確認できるのはどれか。

ア　送信者は自分の公開かぎで暗号化し，受信者は自分の秘密かぎで復号する。
イ　送信者は自分の秘密かぎで暗号化し，受信者は送信者の公開かぎで復号する。
ウ　送信者は受信者の公開かぎで暗号化し，受信者は自分の秘密かぎで復号する。
エ　送信者は受信者の秘密かぎで暗号化し，受信者は自分の公開かぎで復号する。

問16

平文を４文字ずつのブロックに分け、それぞれのブロック内の文字の位置を、１番目を３番目に、２番目を１番目に、３番目を４番目に、４番目を２番目に置き換える転置式暗号がある。このとき、平文“ＤＥＥＲＤＩＤＤＲＥＡＭＤＥＥＰ”の暗号文として、正しいものはどれか。

ア　ＤＩＤＤＤＥＥＰＤＥＥＲＲＥＡＭ　　イ　ＥＤＲＥＤＤＤＩＡＲＭＥＥＤＰＥ
ウ　ＥＲＤＥＩＤＤＤＥＭＲＡＥＰＤＥ　　エ　ＩＤＤＤＥＰＤＥＥＲＤＥＥＭＲＡ

問17

共通かぎ方式の暗号として，ビット列のデータにかぎとの排他的論理和(Å)を適用する方式がある。排他的論理和とは，次のとおりの結果になる演算である。

０Å０＝０　０Å１＝１　１Å０＝１　１Å１＝０

例えば，１１００というデータに対して，１０１０というかぎを使って暗号化すると，暗号データは０１１０となり，同じかぎとの排他的論理和をとることによって復号もできる。

データ	1	1	0	0
かぎ	1	0	1	0
暗号データ	0	1	1	0

↓暗号化　↑復号

１０１０というかぎを使って００１０という暗号データを得た。元のデータはどれか。

ア　００１０　　イ　１０００　　ウ　１０１０　　エ　１１００

問18

シーザ暗号はアルファベットをＮ文字分ずらす暗号方式である。例えば、ａｂｃｄをＮ＝２で暗号化するとｃｄｅｆとなる。シーザ暗号で暗号化された結果得られた文ｇｅｗｌを復号したところｃａｓｈであることが分かった。Ｎの値で正しいものはどれか。

ア　２　　イ　３　　ウ　４　　エ　５

問19

電子メールの送信者が正当な相手かどうかを確認するために，公開かぎ暗号方式を用いたディジタル署名を利用する場合，必要となるかぎの組合せはどれか。

ア　受信者の公開かぎと受信者の秘密かぎ
イ　受信者の公開かぎと送信者の秘密かぎ
ウ　送信者の公開かぎと受倍者の秘密かぎ
エ　送信者の公開かぎと送信者の秘密かぎ

問20

公開鍵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，ＮＩＳＴが公募した公開鍵暗号方式である。
イ　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。
ウ　公開鍵暗号方式に参加する利用者の数が増えると鍵の配送が煩雑になる。
エ　通信文の内容の秘匿に公開鍵暗号方式を使用する場合は，受信者の復号鍵を公開する。

問21

非常に大きな数の素因数分解が困難なことを利用した公開鍵暗号方式はどれか。

ア　ＡＥＳ　　イ　ＤＳＡ　　ウ　ＩＤＥＡ　　エ　ＲＳＡ

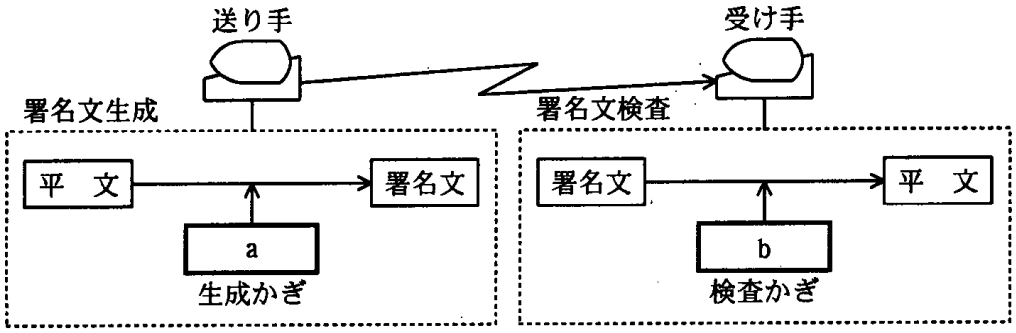
問22

ディジタル署名に用いる鍵の種別に関する組合せのうち，適切なものはどれか。

	ディジタル署名の作成に用いる鍵	ディジタル署名の検証に用いる鍵
ア	共通鍵	秘密鍵
イ	公開鍵	秘密鍵
ウ	秘密鍵	共通鍵
エ	秘密鍵	公開鍵

問23

図は，公開かぎ暗号方式による電子署名の構成を示している。ａ，ｂに該当する適切な組合せはどれか。



	a	b
ア	受け手の公開鍵	受け手の秘密鍵
イ	送り手の公開鍵	送り手の秘密鍵
ウ	送り手の秘密鍵	受け手の公開鍵
エ	送り手の秘密鍵	送り手の公開鍵

問24

デジタル署名の説明として、最も適切なものはどれか。

ア　受信者が署名鍵を使って暗号文を元の平文に戻す。
イ　送信者が、送信する平文の意味を関係者以外に分からないようにする。
ウ　送信者は平文に冗長性を付加し、暗号化する。受信者は復号したとき、予め定められた冗長性が入っていれば正しいメッセージと判断する。
エ　送信者は平文に署名鍵を使って署名することによって、受信者が送信者を確認できるようにする。

問25

デジタル署名に関する記述のうち，適切なものはどれか。

ア　発信者は相手の公開かぎでメッセージのハッシュ値を暗号化することによってデジタル署名を生成する。
イ　発信者は相手の秘密かぎでメッセージのハッシュ値を暗号化することによってデジタル署名を生成する。
ウ　発信者は自分の公開かぎでメッセージのハッシュ値を暗号化することによってデジタル署名を生成する。
エ　発信者は自分の秘密かぎでメッセージのハッシュ値を暗号化することによってデジタル署名を生成する。

問26

ディジタル署名などに用いるハッシュ関数の特徴はどれか。

ア　同じメッセージダイジェストを出力する二つの異なるメッセージは容易に求められる。
イ　メッセージが異なっていても，メッセージダイジェストは全て同じである。
ウ　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。
エ　メッセージダイジェストの長さはメッセージの長さによって異なる。

問27

ディジタル署名を利用する主な目的は二つある。一つは，受信者がメッセージの発信者を確認することである。もう一つの目的はどれか。

ア　受信者が，発信者のＩＤを確認すること
イ　受信者が，秘密かぎを返送してよいかどうかを確認すること
ウ　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
エ　送信の途中で，メッセージが不当に解読されていないことを確認すること

問28

インターネットで公開されているソフトウェアにディジタル署名を添付する目的はどれか。

ア　ソフトウェアの作成者が保守責任者であることを告知する。
イ　ソフトウェアの使用を特定の利用者に制限する。
ウ　ソフトウェアの著作権者が署名者であることを明示する。
エ　ソフトウェアの内容が改ざんされていないことを保証する。

問29

暗号を利用したデジタル署名に関する記述のうち、正しいものはどれか。

ア　発信者は自分の公開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い、受信者は自分の公開鍵で復号し確認する。
イ　発信者は自分の公開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い、受信者は自分の秘密鍵で復号し確認する。
ウ　発信者は相手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、自分の公開鍵でさらに暗号化する。
エ　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。

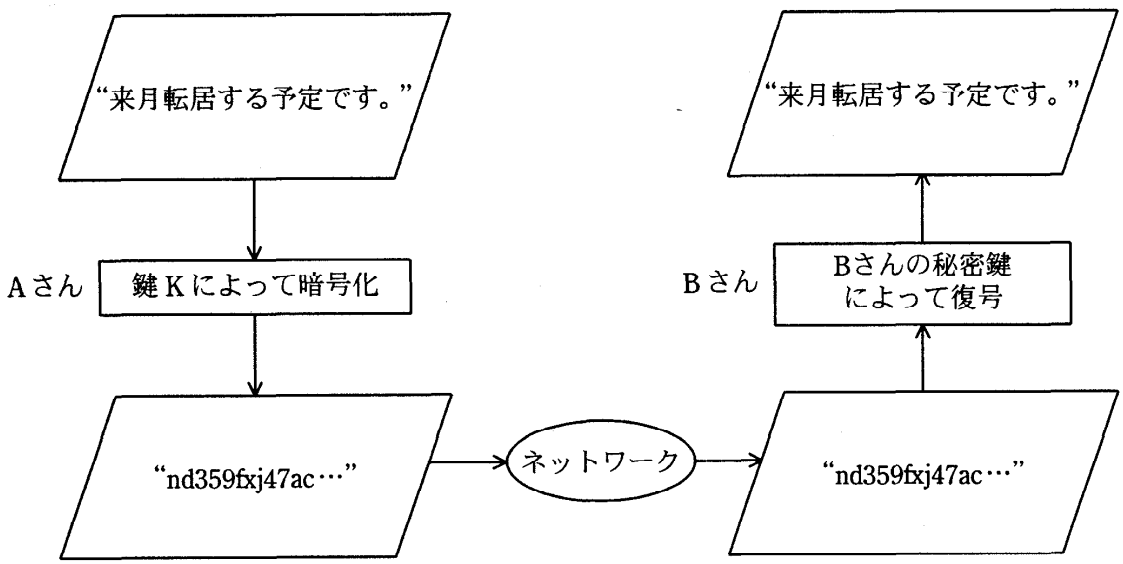
問30

ディジタル証明書をもつA氏が，B商店に対して電子メールを使って商品の注文を行うときに，A氏は自分の秘密鍵を用いてディジタル署名を行い，B商店はA氏の公開鍵を用いて署名を確認する。この事法によって確認できることはどれか。ここで，A氏の秘密鍵はA氏だけが使用できるものとする。

ア　A氏からB商店に送られた注文の内容は，第三者に漏れない。
イ　A氏から発信された注文は，B商店に届く。
ウ　B商店に届いたものは，A氏からの注文である。
エ　B商店は，A氏に商品を売ることの許可が得られる。

問31

公開鍵暗号方式を用いて，図のようにAさんからBさんへ，他人に秘密にしておきたい文章を送るとき，暗号化に用いる鍵Kとして，適切なものはどれか。



ア　Aさんの公開鍵　　イ　Aさんの秘密鍵
ウ　Bさんの公開鍵　　エ　共通の秘密鍵

問32

ディジタル署名付きのメッセージをメールで受信した。受信したメッセージのディジタル署名を検証することによって，確認できることはどれか。

ア　メールが，不正中継されていないこと
イ　メールが，漏えいしていないこと
ウ　メッセージが，改ざんされていないこと
エ　メッセージが，特定の日時に再送信されていないこと

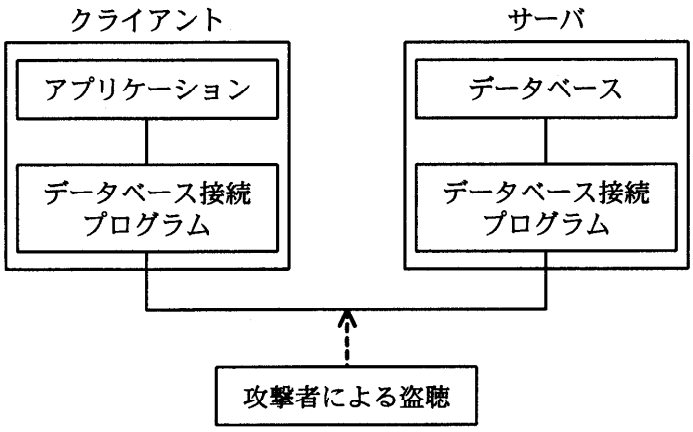
問33

ネットワークを使用するシステムで，暗号化技術を利用しても実現できないものはどれか。

ア　いったん受信したメッセージを，後で送信元から送信した覚えはないといって否定されることを防止する。
イ　受信メッセージが，正当な送出者からのものであることを確認する。
ウ　データの第三者への漏えいを防止する。
エ　メッセージが途中で失われることを防止する。

問34

図のように，クライアント上のアプリケーションがデータベース接続プログラム経由でサーバ上のデータベースのデータにアクセスする。データベース接続プログラム間で送受信されるデータが，通信経路上で盗聴されることに対する対策はどれか。



ア　クライアント側及びサーバ側にあるデータベース接続プログラム間の通信を暗号化する。
イ　サーバ側のデータベース接続プログラムにアクセスできるクライアントのＩＰアドレスを必要なものだけに制限する。
ウ　サーバ側のデータベース接続プログラムを起動・停止するときに必要なパスワードを設定する。
エ　データベース接続プログラムが通信に使用するポート番号をデータベース管理システムによって提供される初期値から変更する。

問35

通信販売の電子商取引では，受発注における改ざん，なりすまし，否認によって販売業者又は利用者に被害が及ぶ危険性がある。この三つの防止に適用できるセキュリティ技術はどれか。

ア　ウィルスチェック
イ　ジャンクメールフィルタ
ウ　ディジタル署名
エ　ファイアウォール

問36

手順に示す電子メールの送受信によって得られるセキュリティ上の効果はどれか。

〔手順〕

（１）送信者は，電子メールの本文を共通鍵暗号方式で暗号化し(暗号文)，その共通鍵を受信者の公開鍵を用いて公開鍵暗号方式で暗号化する(共通鍵の暗号化データ)。

（２）送信者は，暗号文と共通鍵の暗号化データを電子メールで送信する。

（３）受信者は，受信した電子メールから取り出した共通鍵の暗号化データを，自分の秘密鍵を用いて公開鍵暗号方式で復号し，得た共通鍵で暗号文を復号する。

ア　送信者による電子メールの送達確認

イ　送信者のなりすましの検出

ウ　電子メールの本文の改ざんの有無の検出

エ　電子メールの本文の内容の漏えいの防止

問37

電子メールを暗号化するために使用される方式はどれか。

ア　ＢＡＳＥ６４　　イ　ＧＺＩＰ

ウ　ＰＮＧ　　エ　Ｓ／ＭＩＭＥ

問38

電子メールに用いられるＳ／ＭＩＭＥの機能はどれか。

ア　内容の圧縮　　イ　内容の暗号化と署名

ウ　内容の開封通知　　エ　内容の再送

問39

ＰＣからサーバに対し，ＩＰｖ６を利用した通信を行う場合，ネットワーク層で暗号化を行うのに利用するものはどれか。

ア　ＩＰsec　　イ　ＰＰＰ　　ウ　ＳＳＨ　　エ　ＳＳＬ

問40

“コンピュータ不正アクセス対策基準”に適合しているものはどれか。

ア　監視効率を向上させるためにすべてのネットワークを相互接続する。

イ　業務上必要な場合は，利用者ＩＤを個人間で共有して使用できる。

ウ　システム管理者が，すべての権限をもつ利用者ＩＤを常に使用できる。

エ　組織のセキュリティ方針を文書化し，定期的に研修を開催する。

問41

コンピュータシステムに対する利用者の利用資格の正当性チェックと利用状況の把握を行う目的で，利用者に付与される情報を表す用語として，適切なものはどれか。

ア　ＩＰアドレス　　イ　アクセス権
ウ　パスワード　　エ　ユーザＩＤ

問42

インターネット利用時のセキュリティ確保に関する記述のうち，適切なものはどれか。

ア　インターネットを経由してデータベースサーバを利用する場合，データベースへの不正アクセスやデータの改ざんを防止する対策も必要となる。
イ　インターネットを利用して電子メールを送る場合，暗号化を行えば，電子メールの到達確認ができる。
ウ　インターネットを利用するには，利用者認証システムに登録する必要がある。
エ　社内電子メールシステムをインターネットで社外と接続しても，ファイアウォールを導入すれば，社内からの重要情報の流出は自動的に防止できる。

問43

セキュリティ技術に関する記述のうち、適切なものはどれか。

ア　地震や火災に対しては、フォールトトレラント方式のコンピュータによるシステムの二重化が有効である。
イ　データの物理的な盗聴や破壊に対しては、ディスクアレイシステムやファイアフォールが有効である。
ウ　伝送中のデータへの不正アクセスに対して、ＨＤＬＣプロトコルのＣＲＣ方式が有効である。
エ　メッセージの改ざんやなりすましによる不正アクセスに対しては、公開鍵暗号方式を応用したディジタル署名が有効である。

問44

公衆回線を利用しているコンピュータシステムで、セキュリティの面から適切な運用方法はどれか。

ア　あらかじめ定められたパスワードの変更を禁止する。
イ　接続要求があった場合、特定の電話番号にコールバックして接続する。
ウ　パスワードはユーザが確認できるように、ログイン時に端末に表示する。
エ　パスワードをあらかじめ定めた回数間違えて入力した場合、パスワードを通知する。

問45

ユーティリティプログラムの不正な実行によるデータの改ざんや破壊を防止する上で，効果的な管理手段として，最も適切なものはどれか。

ア　システムログの採取
イ　ソースプログラムと実行プログラムの比較
ウ　データのバックアップ
エ　ファイルへのアクセス権限の設定

問46

ユーザＩＤの管理について、最も適切なものはどれか。

ア　同じプロジェクトに参加している利用者は、みな同じユーザＩＤを用いる。
イ　複数のユーザＩＤをもつ利用者は、すべてのＩＤに対して同じパスワードを設定する。
ウ　ユーザＩＤに権限を設定する場合は、必要最小限なものにする。
エ　ユーザＩＤの抹消は、廃止の届出後、十分な期間をおいてから行う。

問47

あるコンピュータのログイン時に入力するパスワードの文字数は５文字である。英字の大文字２６字と数字が使えるものとする。一つのパスワードが使用できるかどうかを試みるのに０．５秒かかるとした場合、すべてのパスワードの組合せを試すためにはどの程度の期間を必要とするか。

ア　１０日　　イ　１０週間　　ウ　６か月　　エ　１年

問48

データベースの不正利用を防止する方法として有効なものはどれか。

ア　アクセス権の設定　　イ　一貫性維持の制御
ウ　データのカプセル化　　エ　ファイルの二重化

問49

利用者認証に用いられるＩＣカードの適切な運用はどれか。

ア　ＩＣカードによって個々の利用者を識別できるので，管理負荷を軽減するために全利用者に共通なＰＩＮを設定する。
イ　ＩＣカードの表面に刻印してある数字情報を組み合わせて，ＰＩＮを設定する。
ウ　ＩＣカード紛失時には，新たなＩＣカードを発行し，ＰＩＮを設定した後で，紛失したＩＣカードの失効処理を行う。
エ　ＩＣカードを配送する場合には，ＰＩＮを同封せず，別経路で利用者に知らせる。

問50

パスワードに使用する文字の種類をM，パスワードのけた数をｎとするとき，設定できるパスワードの個数Ｐを求める数式はどれか。

ア　$P=M^n$

イ　$P=\frac{M!}{(M-n)!}$

ウ　$P=\{\frac{M!}{(M-n)!}\}\times\frac{1}{n!}$

エ　$P=\{\frac{(M+n-1)!}{(M-1)!}\}\times\frac{1}{n!}$

問51

ＩＣカードとＰＩＮを用いた利用者認証における適切な運用はどれか。

ア　ＩＣカードによって個々の利用者を識別できるので，管理負荷を軽減するために全利用者に共通のＰＩＮを設定する。

イ　ＩＣカードの表面に刻印してある数字情報を組み合わせて，ＰＩＮを設定する。

ウ　ＩＣカード紛失時には，新たなＩＣカードを発行し，ＰＩＮを再設定した後で，紛失したＩＣカードの失効処理を行う。

エ　ＩＣカードを配送する場合には，ＰＩＮを同封せず，別経路で利用者に知らせる。

問52

コンピュータシステムにおけるパスワード運用管理方法として、適切なものはどれか。

ア　トラブル処理を迅速化するために、ユーザＩＤとパスワードの一覧表を作成し、管理者しか分からないように隠す。

イ　利用者が自分のパスワードをいつでも自由に変更できるようにする。

ウ　利用者管理作業を簡素化するために、現在使用されていないユーザＩＤとパスワードを再利用する。

エ　利用者登録申請書が届く前に、新任者の人事異動速報を見てユーザＩＤと仮のパスワードを登録する。

問53

キーロガーの悪用例はどれか。

ア　通信を行う２者間の経路上に割り込み，両者が交換する情報を収集し，改ざんする。

イ　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。

ウ　プラウザでの動画閲覧時に，利用者の意図しない広告を勝手に表示する。

エ　プラウザの起動時に，利用者がインストールしていないツールバーを勝手に表示する。

問54

ディジタル署名における署名鍵の用い方と，ディジタル署名を行う目的のうち，適切なものはどれか。

ア　受信者が署名鍵を使って，暗号文を元のメッセージに戻すことができるようにする。
イ　送信者が固定文字列を付加したメッセージを署名鍵を使って暗号化することによって，受信者がメッセージの改ざん部位を特定できるようにする。
ウ　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する。
エ　送信者が署名鍵を使ってメッセージを暗号化することによって，メッセージの内容を関係者以外に分からないようにする。

問55

データベースで管理されるデータの暗号化に用いることができ，かつ，暗号化と復号とで同じ鍵を使用する暗号化方式はどれか。

ア　ＡＥＳ　　イ　ＰＫＩ　　ウ　ＲＳＡ　　エ　ＳＨＡ-２５６

問56

公開鍵暗号方式の暗号アルゴリズムはどれか。

ア　ＡＥＳ　　イ　KCipher-2　　ウ　ＲＳＡ　　エ　ＳＨＡ-２５６