２．コンピュータの技術要素

２．３情報セキュリティ（アクセス制御）

問題１

パスワードに関する記述のうち、適切なものはどれか。

ア．パスワードには、英単語など意味のある言葉を使用する。

イ．パスワードは必ずメモしておき、誰からも見やすい場所に貼っておく。

ウ．パスワード漏えいの事実が発覚した場合、速やかに管理者に報告する。

エ．忘れないようにするために、できるだけ短いパスワードを設定する。

問題２

一度の認証で、許可されている複数のサーバやアプリケーションなどを利用できる仕組みを何というか。

ア．シングルサインオン　　イ．ディジタルフォレンジックス

ウ．バイオメトリクス認証　　エ．ワンタイムパスワード

問題３

ネットワークにおいて、外部からの不正アクセスを防ぐために内部ネットワークと外部ネッワークの間に置かれるものはどれか。

ア．DNS サーバ　　イ．サーチエンジン

ウ．スイッチングハブ　　エ．ファイアウォール

問題４

セキュリティに問題がある PC を社内ネットワークなどに接続させないことを目的とした仕組みであり、外出先で使用した PC を会社に持ち帰った際に、ウイルスに感染していないことなどを確認するために利用するものはどれか。

ア．DMZ　　イ．IDS

ウ．検疫ネットワーク　　エ．ファイアウォール

問題５

システムの利用者認証技術に関する記述のうち、適切なものはどれか。

ア．一度の認証で、許可されている複数のサーバやアプリケーションなどを利用できる仕組みをチャレンジレスポンス認証という。

イ．指紋や声紋など、身体的な特徴を利用して本人認証を行う仕組みをシングルサインオンという。

ウ．特定の数字や文字の並びではなく、位置についての情報を覚え、認証時には画面に表示された表の中で、自分が覚えている位置に並んでいる数字や文字をパスワードとして入力する方式をバイオメトリクス認証という。

エ．認証のために一度しか使えないパスワードのことを、ワンタイムパスワードという。

問題６

企業内ネットワークからも、外部ネットワークからも論理的に隔離されたネットワーク領域であり、そこに設定されたサーバが外部から不正アクセスを受けたとしても、企業内ネットワークには被害が及ばないようにするためのものはどれか。

ア．DMZ　　イ．DNS　　ウ．DoS　　エ．SSL

問題７

無線 LAN のセキュリティにおいて、アクセスポイントが接続要求を受け取ったときに、端末固有の情報固有の情報を基にアクセス制御を行う仕組みはどれか。

ア．ESSID　　イ．MAC アドレスフィルタリング

ウ．WEP　　エ．WPA

２．３情報セキュリティ（暗号化／ディジタル署名）

問題１

共通鍵暗号方式に関する記述のうち、適切なものはどれか。

ア．暗号化に用いる鍵を第三者に公開しても、第三者は暗号文を復号できない。

イ．公開鍵暗号方式よりも、暗号化処理と復号処理の計算量は少ない。

ウ．通信経路で改ざんされた暗号文を復号処理で訂正し、元の暗号文に復元する機能をもつ。

エ．複数の相手ごとに通信内容を秘密にしたい場合でも、暗号化に用いる鍵は一つである。

問題２

無線 LAN で利用される暗号方式の規格はどれか。

ア．AES　　イ．DES　　ウ．RSA　　エ．WPA2

問題３

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。電子メールの内容を秘密にする必要があるので、公開鍵暗号方式を用い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鍵はどれか。

ア．X さんの公開鍵　　イ．X さんの秘密鍵

ウ．Y さんの公開鍵　　エ．Y さんの秘密鍵

問題４

公開鍵基盤（PKI）における認証局（CA）が果たす役割はどれか。

ア．SSL を利用した暗号化通信で使用する認証プログラムを提供する。

イ．Web サーバに不正な仕組みがないことを示す証明書を発行する。

ウ．公開鍵が被認証者のものであることを示す証明書を発行する。

エ．被認証者のディジタル署名を安全に送信する。

問題５

セション鍵暗号方式で用いられるハイブリッド方式に関する記述のうち、適切なものはどれか。

ア．共通鍵と公開鍵で二重に暗号化するので、改ざんが難しい。

イ．共通鍵と公開鍵を併用するので、高速な暗号通信には向かない。

ウ．公開鍵暗号方式を使って、共通鍵を暗号化して通信相手に送信する。

エ．使用する鍵の数は、全体で単独方式の 2 乗倍必要となる。

問題６

受信した電子メールに PKI（公開鍵基盤）を利用してディジタル署名を付与した場合に関する記述①～④のうち、判断可能な記述だけをすべて挙げたものはどれか。

①電子メールの添付ファイルはウイルスに感染していない。

②電子メールの内容は通信途中において、他の誰にも盗み見られていない。

③電子メールの発信者は、なりすましされていない。

④電子メールは通信途中で改ざんされていない。

ア．①，②　　イ．①，③　　ウ．②，④　　エ．③，④

問題 7

小文字の英字からなる文字列の暗号化を考える。次表の英字を文字番号に変換し、変換後の文字番号について 1 文字目には 1 を、2 文字目には 2 を、…、n 文字目には n を加える。それぞれの数を 26 で割った余りを新たに文字番号とみなし、表から対応する英字に変換する。

例　fax → 6、24 → 6+1、1+2、24+3 → 7、3、27 → 7、3、27 → 7、3、27 → 7、3、1 → gca

この手続きで暗号化した結果が”tmb”であるとき、元の文字列はどれか。

文字番号	1	2	3	4	5	6	7	8	9	10	11	12	13
英字	a	b	c	d	e	f	g	h	i	j	k	l	m
文字番号	14	15	16	17	18	19	20	21	22	23	24	25	26
英字	n	o	p	q	r	s	t	u	v	w	x	y	z

ア．she　　イ．shy　　ウ．ski　　エ．sky