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起き、だれからも見やすい場所に貼っておく。

ウ：　パスワード漏洩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

　ネットワークにいて、外部からの不正アクセスを防ぐために内部のネットワークと外部のネット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、ウィ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：　指紋や音声など、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、一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、そこに設置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、端末固有の情報をもと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．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【解答：ウ】

　パスワードは、利用者本人しか知らない文字列（キーワード）である。利用者が入力したIDとパスワードを使用して、システムがアクセスを許可した本人かどうか確認（利用者認証）する。パスワードの運用では、パスワードが推測されないことと、第三者に漏洩しないことに注意する。

ア：　パスワードは、英数字などを組み合わせた、意味のない文字列にすべきである。英単語などを利用すると、辞書攻撃で簡単に解読されてしまう。

イ：　パスワードを書いたメモなどは、人目に触れるところに空いておくべきではない。メモしたい場合には、その管理方法に十分配慮する必要がある。

ウ：　パスワード漏洩の事実が明らかになった場合は、速やかに管理者に連絡すべきである。また、漏洩したパスワードはすぐに変更するか、管理者が無効にする。（正解）

エ：　パスワードは、必要十分な長さ（最低６から８文字）にすべきである。短いパスワードは、総当たり攻撃で解読されやすい。

問題２【解答：ア】

・シングルサインオン

・ディジタルフォレンジックス

・バイオメトリクス認証

・ワンタイムパスワード

問題３【解答：エ】

・DNS（Domain Name System）

：URLやメールアドレスをIPアドレスに変換するサービスを提供するサーバである。

・サーチエンジン

：Webサービスの一つである、情報検索サイトで処理を行うプログラムである。

・スイッチングハブ

：MACアドレスによるフィルタリング機能（ストアアンドフォワード）を持った接続装置である。LAN内のPCから発信されたパケットは、転送する必要のないLANには伝送されない。

・ファイアウォール

：内部ネットワークと外部ネットワークの間に設置して、通信が許可されていないパケットの侵入（不正アクセス）を防ぐ仕組みである。（正解）

問題４【解答：ウ】

・DMZ（DeMilitarized Zone；非武装地帯）

：内部ネットワークと外部ネットワークの間にファイアウォールを設置し、社外に公開するWebサーバ、メールサーバなどを社内ネットワークから隔離するためのセグメントである。

ファイアウォールによって、通信が許可されていないパケットの侵入（不正アクセス）を防ぐことができる。

・IDS（Intrusion Detection System；侵入検知システム）

：ネットワーク接続機器などへの不正侵入を検知し、ログの収集・解析を行うシステムである。

あらかじめ登録してある侵入パターンに該当するアクセスパターンや、通常の運用におけるアクセスパターンと異なるものなどを検知する。  
・検疫ネットワーク

：内部ネットワークに接続するPCを、独立したネットワークにいったん接続して検査し、問題があれば対処する仕組みである。外出先で使用したPCを会社に持ち帰った際に、ウィルスに感染していないかなどを確認するために利用する。（正解）

・ファイアウォール

：内部ネットワークと外部ネットワークの間に設置して、通信が許可されていないパケットの侵入（不正アクセス）を防ぐ仕組みである。

問題５【解答：エ】

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は、シングルサインオンである。チャレンジレスポンス認証とは、受信したチャレンジコードから一定のルールに従って求めたレスポンスコードを送信することで、一定のルールを知っている正当な利用者であることを認証する仕組みである。

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は、バイオメトリクス認証である。

ウ：　画面に表示された表の中で、自分が覚えている位置にならなんでいる数字や文字をパスワードとして入力する方式は、マトリックス認証である。

エ：　認証のために一度しか使えないパスワードは、ワンタイムパスワードである。ログインのたびに異なるパスワードを使用することで、外出先などで第三者にパスワードの入力を盗み見られても、そのパスワードを再利用することはできないので安全性が高い。（正解）

問題６【解答：ア】

・DMZ（DeMilirarized Zone;非武装地帯）

：内部ネットワークと外部ネットワークの間にファイアウォールを設置し、内部ネットワークから隔離するネットワーク領域である。ＤＭＺには、Ｗｅｂサーバやメールサーバなど、社外に公開したいサーバを設置する。（正解）

・DNS（Domain Name System）

：URLやメールアドレスをIPアドレスに変換するプロトコル又は仕組みの事である。

・DoS（Denial of Service）

：標的のサーバに大量のデータを送信し続け、サーバのCPU、メモリなどに過剰な負荷をかけて、サービスをボおう害する攻撃である。

・SSL（Security Sockets Layer）

：データの暗号化機能や、電子証明書などを使用した利用者（又はWebサーバ）認証機能を備えたセキュリティプロトコルである。

問題７【解答：イ】

・ESSID（Extended SSID；ネットワーク識別子）

：無線LANのアクセスポイントを識別するネットワーク識別子である。

・MACアドレスフィルタリング

：接続を許可する端末のMACアドレス（端末固有の情報）をアクセスポイントにあらかじめ登録しておき、登録されていないＭＡＣアドレスを持つ端末からの接続を拒否する機能である。（正解）

・WEP（Wired Equivalent Privacy）

：WEPパスワードとSSIDを利用して、無線LANの暗号化を行う方式である。

・WPA（Wi-Fi Protected Access）

：ＷＥＰを改良した方式で、一定時間ごとに鍵を生成／更新する暗号化プロトコルTKIP（Temporal Key Integrity Protocol）を利用して無線LANの暗号化を行う。

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

　パスワードにするのうち、なものはどれか。

ア：　パスワードには、などのあるをする。

イ：　パスワードはずメモしてき、だれからもやすいにっておく。

ウ：　パスワードのがした、ににする。

エ：　れないようにするために、できるだけいパスワードをする。

問題２

　ので、されているのサーバやアプリケーションなどをできるみをというか。

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

エ：　ワンタイムパスワード

問題３

　ネットワークにいて、からのアクセスをぐためにのネットワークとのネットワークの間に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

　セキュリティにがあるPCをネットワークなどにさせないことをとしたみであり、でしたPCをにちったに、ウィルスにしていないことなどをするためにするものはどれか。

ア：　DMZ

イ：　IDS

ウ：　ネットワーク

エ：　ファイアウォール

問題５

システムのにするのうち、なものはどれか。

ア：　ので、されているのサーバやアプリケーションなどをできるみをチャレンジレスポンスという。

イ：　やなど、なをしてをみをシングルサインオンという。

ウ：　のやのびではなく、についてのを、にはにされたので、がえているにんでいるやをパスワードとしてするをバイオメトリクスという。

エ：　のためにしか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

　ネットワークからも、ネットワークからもにされたネットワークであり、そこにされたサーバがから不正アクセスをけたとしても、ネットワークにはが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

　LANのセキュリティにおいて、アクセスポイントがをけったときに、のをもとにアクセスをうみはどれか。

ア：　ESSID

イ：　MACアドレスフィルタリング

ウ：　WEP

エ：　WPA

２．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【解答：ウ】

　パスワードは、しからない（キーワード）である。がしたIDとパスワードをして、システムがアクセスをしたかどうか（利用者）する。パスワードのでは、パスワードがされないことと、にしないことにする。

ア：　パスワードは、などをみわせた、のないにすべきである。などをすると、でにされてしまう。

イ：　パスワードをいたメモなどは、にれるところにおいておくべきではない。メモしたいには、そのにするがある。

ウ：　パスワードのがらかになったは、やかに管理者にすべきである。また、したパスワードはすぐにするか、がにする。（正解）

エ：　パスワードは、なさ（６から８）にすべきである。いパスワードは、たり攻撃で解読されやすい。

問題２【解答：ア】

・シングルサインオン

：ので、されているのシステム（サービス、サーバ、アプリケーション）をできるみである。（正解）

・ディジタルフォレンジックス

：アクセスなどのコンピュータがきたとき、にするやデータをして、にとなるるかどうかをらかにするのである。

・バイオメトリクス

：のによってすることである。されていないを、がされているなどにれないようにするためにされる。

・ワンタイムパスワード

：しかえないパスワード（はしかえないパスワードでするみ）のである。

問題３【解答：エ】

・DNS（Domain Name System）

：URLやメールアドレスをIPアドレスにするサービスをするサーバである。

・サーチエンジン

：Webサービスの一つである、サイトでをうプログラムである。

・スイッチングハブ

：MACアドレスによるフィルタリング（ストアアンドフォワード）をったである。LANのPCからされたパケットは、するのないLANにはされない。

・ファイアウォール

：ネットワークとネットワークのにして、がされていないパケットの（アクセス）をぐ仕組みである。（正解）

問題４【解答：ウ】

・DMZ（DeMilitarized Zone；）

：ネットワークとネットワークのにファイアウォールをし、にするWebサーバ、メールサーバなどをネットワークからするためのセグメントである。

ファイアウォールによって、がされていないパケットの（アクセス）をぐことができる。

・IDS（Intrusion Detection System；システム）

：ネットワークなどへのをし、ログの・をうシステムである。あらかじめしてあるパターンにするアクセスパターンや、のにおけるアクセスパターンとなるものなどをする。

・ネットワーク

：ネットワークにするPCを、したネットワークにいったんしてし、があればするみである。でしたPCをにったに、ウィルスにしていないかなどをするためにする。（正解）

・ファイアウォール

：ネットワークとネットワークのにして、がされていないパケットの（アクセス）をみである。

問題５【解答：エ】

ア：　ので、されているのサーバやアプリケーションなどをできるみは、シングルサインオンである。チャレンジレスポンスとは、したチャレンジコードからのルールにってめたレスポンスコードをすることで、のルールをっているなであることをするみである。

イ：　やなど、なをしてをみは、バイオメトリクスである。

ウ：　にされたので、がえているにならなんでいるやをパスワードとしてするは、マトリックスである。

エ：　のためにしかえないパスワードは、ワンタイムパスワードである。ログインのたびになるパスワードをすることで、などでにパスワードのをられても、そのパスワードをすることはできないのでがい。（正解）

問題６【解答：ア】

・DMZ（DeMilirarized Zone;）

：ネットワークとネットワークのにファイアウォールをし、ネットワークからするネットワークである。ＤＭＺには、Ｗｅｂサーバやメールサーバなど、にしたいサーバをする。（正解）

・DNS（Domain Name System）

：URLやメールアドレスをIPアドレスにするプロトコルはのである。

・DoS（Denial of Service）

：のサーバにのデータをけ、サーバのCPU、メモリなどになをかけて、サービスをするである。

・SSL（Security Sockets Layer）

：データのや、などをした（又はWebサーバ）をえたセキュリティプロトコルである。

問題７【解答：イ】

・ESSID（Extended SSID；ネットワーク）

：LANのアクセスポイントをするネットワークである。

・MACアドレスフィルタリング

：をするのMACアドレス（の）をアクセスポイントにあらかじめしておき、されていないＭＡＣアドレスをつからのをするである。（正解）

・WEP（Wired Equivalent Privacy）

：WEPパスワードとSSIDをして、LANのをうである。

・WPA（Wi-Fi Protected Access）

：ＷＥＰをしたで、ごとにを／するプロトコルTKIP（Temporal Key Integrity Protocol）をしてLANのをう。