SHEET12 セキュリティ

レベル１

R2 第 10 問

近年、情報ネットワークが発展・普及し、その重要性はますます高まっている。

安全にネットワーク相互間の通信を運用するための記述として、最も適切なものの組み合わせを下記の解答群から選べ。

a　SSL/TLS は、インターネットを用いた通信においてクライアントとサーバ間で送受信されるデータを暗号化する際に使われる代表的なプロトコルである。

b　IDS は、大切な情報を他人には知られないようにするために、データを見てもその内容が分からないように、定められた処理手順でデータを変換する仕組みである。

c　VPN は、認証と通信データの暗号化によってインターネット上に構築された仮想的な専用ネットワークである。

d　DMZ は、LAN に接続するコンピュータやデバイスなどに対して、IP アドレス、ホスト名やDNS サーバの情報といった通信に必要な設定情報を自動的に割り当てるプロトコルである。

〔解答群〕

ア　ａとｂ　　イ　ａとｃ　　ウ　ｂとｄ　　エ　ｃとｄ

R1 第 8 問

中小企業診断士のあなたは、あるメールを開封したところ、次のような URL に接続するように指示が出てきた。

https://News.Fishing.jp/test

この URL から分かることとして、最も適切なものはどれか。

ア　SSL を用いて暗号化されたデータ通信であることが確認できる。

イ　大文字と小文字を入れ替えた偽サイトであることが確認できる。

ウ　参照先ホストのサーバが日本国内に設置されていることが確認できる。

エ　ホスト名の WWW が省略されていることが確認できる。

R1 第 19 問

情報ネットワーク社会を支えるセキュリティ技術の 1 つに暗号化技術がある。

暗号化方式に関する記述として、最も適切なものの組み合わせを下記の解答群から選べ。

a　共通鍵暗号方式は、暗号化と復号に共通鍵を用いる方式である。この方式では、送信者と受信者はあらかじめ共通鍵を共有しておく必要がある。

b　公開鍵暗号方式では、送信者は送信データを受信者の公開鍵で暗号化し、それを受け取った受信者は、ペアとなる送信者の秘密鍵で復号する。

c　公開鍵暗号方式は、暗号化と復号に 2 個 1 組の異なる鍵を用いる方式である。

この方式では、データを送信する時には送信者の公開鍵を使う。

d　セッション鍵方式は、共通鍵暗号方式の長所と公開鍵暗号方式の長所を組み合わせた方式である。

〔解答群〕

ア　ａとｂ　　イ　ａとｄ　　ウ　ｂとｃ　　エ　ｃとｄ

H30 第 10 問

社外から、機密情報を持つ社内ネットワーク内の DB サーバへ安全にアクセスする仕組みに関する以下の文章の空欄Ａ～Ｄに入る語句の組み合わせとして、最も適切なものを下記の解答群から選べ。

自宅や出張先から社内ネットワークに安全に接続するには[Ａ]を利用する方法がある。別のやり方として、[Ｂ]によって社内ネットワークを内部セグメントと[Ｃ]に分ける方法もある。この場合、機密情報を持つ DB サーバは内部セグメントに設置し、[Ｃ]に設置する Web サーバを経由してアクセスする。[Ｂ]のパケットフィルタリングは、[Ｄ]において通信データに含まれる情報を検査し、フィルタリング設定にそぐわないパケットを遮断する。

〔解答群〕

ア　A：VPN　B：SSH　C：LAN　D：ハブ

イ　A：VPN　B：ファイアウォール　C：DMZ　D：ルータ

ウ　A：イントラネット　B：SSH　C：LAN　D：ルータ

エ　A：イントラネット　B：ファイアウォール　C：DMZ　D：ハブ

H30 第 24 問

情報システムに対するコンティンジェンシープランに関する記述として、最も適切なものはどれか。

ア　災害などにより情報システムの運用が困難になることを想定して行う、情報システム部門に対する教育・訓練計画である。

イ　情報システムに障害が起きて損失が発生した後に、直ちに作成される、被害の調査と復旧のための計画である。

ウ　情報システムに障害が発生しても業務を中断することなく処理を継続できるために行う、フォールトトレラント・システムの構築計画である。

エ　情報システムに不測の事態が発生することを想定し、事前に対応策や手順などを定める緊急時対応計画である。

H29 第 22 問

ATM を使った金融取引や PC へのログインの際など、本人確認のための生体認 証技術が広く社会に普及している。認証の精度は、他人受入率(FAR：False Acceptance Rate)と本人拒否率(FRR：False Rejection Rate)によって決まる。この 2 つはトレードオフ関係にあり、一般に片方を低く抑えようとすると、もう片方 は高くなる。

FAR と FRR に関する以下の文章の空欄Ａ～Ｄに入る語句の組み合わせとして、最も適切なものを下記の解答群から選べ。

ａ［ Ａ ］が低いと安全性を重視したシステムになり、［ Ｂ ］が低いと利 用者の利便性を重視したシステムになる。

ｂ ATM での生体認証では、［ Ｃ ］が十分低くなるように設定されている。

ｃ なりすましを防止するには、［ Ｄ ］を低く抑えることに重点をおけばよい。

［解答群］

ア　A：FAR　B：FRR　C：FAR　D：FAR

イ　A：FAR　B：FRR　C：FRR　D：FRR

ウ　A：FRR　B：FAR　C：FAR　D：FAR

エ　A：FRR　B：FAR　C：FRR　D：FRR

H28 第 6 問

業務において各種のサービスを各々異なるサーバ機能で運用する場合、各サービスを利用するごとに、それぞれの ID、パスワードを入力して認証を受けなければならないのは、運用者・利用者の双方にとって ID 管理の負担が大きく非効率的である。この状況を解決するための方法に関する以下の文章の空欄Ａ～Ｄに入る語句の組み合わせとして、最も適切なものを下記の解答群から選べ。

複数のサーバ機能による各サービスの利用者認証を、利用者ごとにひとつの ID とパスワードの組み合わせで行う仕組みが[A]である。

この仕組みは、サーバ機能によるサービスの利用時だけではなく、社内の[B]に[C]を接続して利用する際の認証にも利用することができる。この仕組みを社内で導入するには、[D]をサーバマシン上で運用する必要がある。

[解答群]

ア	A：シングルサインオン	B：LAN	C：プリンタ	D：Linux と Apache
イ	A：シングルサインオン	B：無線 LAN	C：PC やスマートフォン	D：RADIUS と LDAP
ウ	A：マルチセッション	B：VPN	C：プリンタ	D：Linux と LDAP
エ	A：マルチログイン	B：無線 LAN	C：POS 端末	D：Apache と RADIUS

H24 第 21 問

近年、多くの情報漏洩被害をもたらしている「新しいタイプの攻撃」(Advanced Persistent Threats：APT)への対策としては、入口対策だけでなく、出口対策も重要になる。

出口対策として最も適切なものはどれか。

ア　IDS(Intrusion Detection System)の導入

イ　RAT(Remote Access Trojan/Remote Administration Tool)による内部 proxy 通信いわゆる CONNECT 接続の検知遮断

ウ　パッチファイルの適用による脆弱性対策

エ　ファイアウォールによるステルス機能の導入

H24 第 22 問

インターネット利用が普及して、インターネット上で取引情報やプライバシーにかかわる情報を扱う場面が多くなっている。従って情報セキュリティについて、その基礎事項を把握しておくことは重要である。

情報セキュリティにかかわる記述として最も適切なものはどれか。

ア　インターネットを介して、顧客情報を収集してそれをデータベース化した場合、それが漏洩しないようにするにはウイルス対策を行えばよい。

イ　インターネットを介して、顧客に送り先等の他に年齢、家族構成などを入力してもらう場合、その用途については顧客に知らせる必要はない。

ウ　取引企業、顧客との情報のやりとりは、暗号化することが好ましいが、その場合に用いる公開鍵暗号方式とは、関係者の間で共通鍵を設定して、情報を暗号化する方式である。

エ　ファイアウォールを自社コンピュータに対する不正アクセスの防止手段として利用する場合、どのような内容のアクセスを拒否するのかをあらかじめ設定する必要がある。

レベル２

R3 第 11 問

情報システムの利用において、利用者を認証する仕組みの理解は重要である。

それらに関する記述として、最も適切なものはどれか。

ア　生体認証では、ID とパスワードに加えてセキュリティトークンによって利用者を認証する。

イ　チャレンジレスポンス認証では、指紋認証、静脈認証、署名の速度や筆圧などによって利用者を認証する。

ウ　二要素認証では、パスワードだけではなく秘密の質問の答えの 2 つを組み合わせることによって利用者を認証する。

エ　リスクベース認証では、普段と異なる環境からログインする際、通常の認証に加えて合言葉などによって利用者を認証する。

オ　ワンタイムパスワードによる認証では、一度認証されれば、利用する権限を持つ各サーバやアプリケーションでの認証が不要となる。

R3 第 21 問

業務システムのクラウド化やテレワークの普及によって、企業組織の内部と外部の境界が曖昧となり、ゼロトラストと呼ばれる情報セキュリティの考え方が浸透してきている。

ゼロトラストに関する記述として、最も適切なものはどれか。

ア　組織内において情報セキュリティインシデントを引き起こす可能性のある利用者を早期に特定し教育することで、インシデント発生を未然に防ぐ。

イ　通信データを暗号化して外部の侵入を防ぐ VPN 機器を撤廃し、認証の強化と認可の動的管理に集中する。

ウ　利用者と機器を信頼せず、認証を強化するとともに組織が管理する機器のみを構成員に利用させる。

エ　利用者も機器もネットワーク環境も信頼せず、情報資産へのアクセス者を厳格に認証し、常に確認する。

オ　利用者を信頼しないという考え方に基づき認証を重視するが、一度許可されたアクセス権は制限しない。

H30 第 23 問

近年、機密情報への攻撃の手法が多様化している。機密情報を不正に入手する手法であるソーシャルエンジニアリングに関する記述として、最も**不適切**なものはどれか。

ア　シュレッダーで処理された紙片をつなぎ合わせて、パスワードを取得する。

イ　パソコンの操作画面を盗み見して、パスワードを取得する。

ウ　文字列の組み合わせを機械的かつ総当たり的に試すことで、パスワードを取得する。

エ　ユーザになりすまして管理者に電話し、パスワードを取得する。

H28 第 19 問

情報システムの利用においては、フィッシング詐欺や情報漏洩(ろうえい)事案などの増加に対応するために情報セキュリティをより高めなければならない。その一環としてユーザ認証の強化が叫ばれている。これに関する記述として最も適切なものはどれか。

ア　CHAP 認証とは、チャレンジ／レスポンスという方式で、Web サイトにアクセスしてきたユーザを認証するものである。

イ　二段階認証とは、同じパスワードを 2 回入力させてユーザの認証を行う方式のことである。

ウ　ハードウェアトークンとは、その機器を認証装置にかざすことで本人を認証する仕組みのことである。

エ　ワンタイムパスワードとは、サイトに登録した際に最初の認証に利用されるパスワードである。

H28 第 20 問

情報セキュリティへの脅威としてのクリックジャッキング攻撃およびその対策に関する記述として、最も適切なものはどれか。

ア　Web ページに出力するすべての要素に対して、エスケープ処理を実施することで、クリックジャッキング攻撃を防止することができる。

イ　Web ページの HTTP レスポンスヘッダに X-Frame-Options ヘッダフィールドを出力しないことが、クリックジャッキング攻撃への対策となる。

ウ　クリックジャッキング攻撃とクロスサイト・リクエスト・フォージェリに共通する対策がある。

エ　クリックに応じた処理を実行する直前のページで再度パスワードの入力を求め、再度入力されたパスワードが正しい場合のみ処理を実行することが、クリックジャッキング攻撃とクロスサイト・スクリプティングで共通の対策となる。

H26 第 21 問

インターネットが普及した現在においては、関係者以外に知られてはならないような情報を、インターネットを介してやり取りしなければならない状況も多い。そのような状況下では暗号化の技術が重要になる。

大阪の A さんが、東京にいる B さんに顧客名簿を送ってもらうように依頼した。

その場合に利用する暗号化方式に関する記述として最も適切なものはどれか。

ア　B さんは、顧客名簿のファイルを、暗号化鍵を管理する社内部署から鍵をひとつもらって暗号化した。A さんに送付後、その鍵で暗号化したことを鍵管理部署に連絡した。A さんは、その部署から B さんが使った鍵を聞き、送られたファイルを復号化した。この方式は SSL 方式のひとつである。

イ　B さんは、顧客名簿のファイルを A さんと B さんが共有する秘密鍵で暗号化して A さんに送付した。この方式はシーザー暗号方式のひとつである。

ウ　B さんは、顧客名簿のファイルを A さんの公開鍵で暗号化して送付した。A さんは、B さんの秘密鍵で復号化した。この方式は公開鍵方式のひとつである。

エ　B さんは、顧客名簿のファイルを任意に決めた鍵で暗号化して A さんに送付した。A さんは B さんから電話でその鍵を聞き、復号化した。この方式は共通鍵方式のひとつである。

解答

SHEET12 セキュリティ			
レベル 1	R2	10	イ
	R1	8	ア
	R1	19	イ
	H30	10	イ
	H30	24	エ
	H29	22	ア
	H28	6	イ
	H24	21	イ
	H24	22	エ
レベル 2	R3	11	エ
	R3	21	エ
	H30	23	ウ
	H28	19	ア
	H28	20	ウ
	H26	21	エ