Chapter1
セキュリティ

1 情報セキュリティ

1. 情報セキュリティの目的と考え方

1）情報セキュリティの概念

JIS Q 27000:2019（情報セキュリティマネジメントシステム－用語）では、情報セキュリティは、「情報の機密性，完全性及び可用性を維持すること。」と定義しています。また、注記として、「さらに，真正性，責任追跡性，否認防止，信頼性などの特性を維持することを含めることもある。」と記述しています。

そして、**機密性**（confidentiality）は、「認可されていない個人，エンティティ又はプロセスに対して，情報を使用させず，また，開示しない特性。」と定義しています。これは、「不正アクセスや情報漏えいから情報資産を守ること」を意味します。

さらに、**完全性**（integrity）は、「正確さ及び完全さの特性。」と定義しています。これは、「許可されていない者によって情報が改ざんされたり、破壊されたりしないこと」を意味します。

可用性（availability）は、「認可されたエンティティが要求したときに，アクセス及び使用が可能である特性。」と定義しています。これは、「正規の利用者が情報を利用しようとしたときには、いつでも情報にアクセスできること」を意味します。

真正性（authenticity）は、「エンティティは，それが主張するとおりのものであるという特性。」と定義しています。これは、「利用者、システム、プロセス、情報が本物であること」を意味します。

否認防止（non-repudiation）は、「主張された事象又は処置の発生，及びそれを引き起こしたエンティティを証明する能力。」と定義しています。これは、「利用者がシステムを利用したという事実を証明可能にすること」を意味します。

信頼性（reliability）は、「意図する行動と結果とが一貫しているという特性。」と定義しています。これは、「意図する行動と結果が一貫性をもつこと」を意味します。

なお、責任追跡性（accountability）については、JIS X 25010:2013 において、「実体の行為がその実体に一意的に追跡可能である度合い。」と定義しています。これは、「システム、プロセス、情報に対する利用者の行動を追跡できること」を意味します。

例題

情報の“完全性”を脅かす攻撃はどれか。

ア Web ページの改ざん
イ システム内に保管されているデータの不正コピー
ウ システムを過負荷状態にする DoS 攻撃
エ 通信内容の盗聴

イ、エ 機密性を脅かす攻撃です。
ウ 可用性を脅かす攻撃です。

情報セキュリティマネジメント 平成28年度秋 問21 [出題頻度:★★★]

解答－ア

別冊演習ドリル 1-1～4

2）OECD セキュリティガイドライン

OECD セキュリティガイドラインは、OECD（経済協力開発機構）が加盟各国の情報システム及びネットワークのセキュリティ確保のための枠組み作りの指針として採択したガイドラインで次の9つの原則から構成されています。

①認識（Awareness）の原則

参加者は、情報システム及びネットワークのセキュリティの必要性並びにセキュリティを強化するために自分達にできることについて認識すべきである。

②責任（Responsibility）の原則

すべての参加者は、情報システム及びネットワークのセキュリティに責任を負う。

③対応（Response）の原則

参加者は、セキュリティの事件に対する予防、検出及び対応のために、時宜を得たかつ協力的な方法で行動すべきである。

④倫理（Ethics）の原則

参加者は、他者の正当な利益を尊重するべきである。

⑤民主主義（Democracy）の原則

情報システム及びネットワークのセキュリティは、民主主義社会の本質的な価値に適合すべきである。

⑥リスクアセスメント（Risk assessment）の原則

参加者は、リスクアセスメントを行うべきである。

⑦セキュリティの設計及び実装（Security design and implementation）の原則

参加者は、情報システム及びネットワークの本質的な要素としてセキュリティを組み込むべきである。

⑧セキュリティマネジメント（Security management）の原則

参加者は、セキュリティマネジメントへの包括的アプローチを採用するべきである。

⑨再評価（Reassessment）の原則

参加者は、情報システム及びネットワークのセキュリティのレビュー及び再評価を行い、セキュリティの方針、実践、手段及び手続に適切な修正をすべきである。

2. 情報セキュリティの重要性

社会のネットワーク化に伴い、企業にとって情報セキュリティの水準の高さが企業評価の向上につながり、情報システム関連の事故が事業の存続を脅かすことになります。

1）情報資産

情報セキュリティ事故は、情報資産に、脅威と脆弱性が組み合わさることで発生します。

JIS Q 27002:2006（情報セキュリティマネジメント実践のための規範）では、**情報資産**に関連付けた資産として次のような項目を例としてあげています。

資産の種類	例示
情報	データベース及びデータファイル、契約書及び同意書、システムに関する文書、調査情報、利用者マニュアル、訓練資料、運用手順又はサポート手順、事業継続計画、代替手段の取決め、監査証跡、保存情報
ソフトウェア資産	業務用ソフトウェア、システムソフトウェア、開発用ツール、ユーティリティソフトウェア
物理的資産	コンピュータ装置、通信装置、取外し可能な媒体、その他の装置
サービス	計算処理サービス、通信サービス、一般ユーティリティ（例えば、暖房、照明、電源、空調）
人	保有する資格、技能、経験
無形資産	組織の評判、イメージ

情報資産

2）サイバー空間

サイバー空間は、コンピュータシステムと通信ネットワークから構築された仮想的な空間で、インターネットの急速な進展により、国民生活に欠かせないものとなっています。したがって、サイバー空間に不正に侵入して情報を不正取得、改ざん、破壊する**サイバー攻撃**によって、安定的なサイバー空間の利用が妨げられた場合には、その被害は甚大なものとなります。そこで、わが国では2015年1月に、前年11月に成立したサイバーセキュリティ基本法に基づき、内閣に「サイバーセキュリティ戦略本部」を、内閣官房に「内閣サイバーセキュリティセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity）」を設置し、安定的なサイバー空間の利用を可能にすべく対策に当たっています。

3．脅威

JIS Q 27000:2019では、**脅威**(threat)を、「システム又は組織に損害を与える可能性がある，望ましくないインシデントの潜在的な原因。」と定義しています。これは、「情報資産や組織に損失や損害をもたらす要因で、不測の事態において発生し、潜在的に存在するもの」を意味します。

1）脅威の種類

内閣府が主催する情報セキュリティ対策推進会議が公表した「情報セキュリティポリシーに関するガイドライン」では、脅威を物理的脅威、技術的脅威、人的脅威に大別しています。

物理的脅威には、事故、災害、故障、破壊、盗難、不正侵入などがあります。

技術的脅威には、不正アクセス、盗聴、マルウェア、なりすまし、改ざん、エラーなどがあります。なお、悪意をもってコンピュータに不正侵入しデータを盗み見たり、破壊などを行う**クラッキング**も技術的脅威に該当します。また、受信者の承諾なしに無差別に送付される **SPAM**（迷惑メール）や、インターネットを介して不特定多数の者とファイルのやり取りを行うための**ファイル共有ソフト**も技術的脅威に該当します。

人的脅威には、誤操作、紛失、破損、不正利用などがあります。なお、本人を装って電話をかけてパスワードを聞き出す、パスワードを入力しているところを後ろから近づいて覗き見る（ショルダハッキング、ショルダサーフィン）、ゴミ箱に捨てられた資料からIPアドレスの一覧や利用者名、パスワードといった情報を探す（トラッシング、スキャベンジング）などの、電子的な方法を用いないで組織内部の人間からパスワードや機密情報などを不正に入手する**ソーシャルエンジニアリング**も人的脅威に該当します。

IPAが2007年11月に公表した「リモートアクセス環境におけるセキュリティ」では、脅威を、地震、台風、雷、火事などの環境的脅威、事故、故障、停電、誤動作、過失などの偶発的脅威、不正アクセス、盗聴・盗視、盗難、ウイルス、アクセス不能攻撃、情報持ち出しなどの意図的脅威に大別しています。

例題

緊急事態を装って組織内部の人間からパスワードや機密情報を入手する不正な行為は，どれに分類されるか。

ア ソーシャルエンジニアリング　　イ トロイの木馬
ウ 踏み台攻撃　　エ ブルートフォース攻撃

イ トロイの木馬は、正体を偽ってコンピュータへ侵入し、特定の日時や実行要件などの一定の条件が満たされるまで潜伏して、データ消去やファイルの外部流出、他のコンピュータの攻撃などの活動を行うプログラムです。
ウ 踏み台攻撃は、セキュリティ対策の甘いサイトに不正侵入し、他サイトへの攻撃の中継サイトとして利用することです。
エ ブルートフォース攻撃は、適当に文字を組み合わせて作成したパスワードでログインを繰り返すことで、力ずくでパスワードを探し出そうとすることです。

情報セキュリティマネジメント　平成28年度秋　問25［出題頻度：★★☆］

解答－ア

別冊演習ドリル　1-5～7

2）マルウェア・不正プログラム

マルウェア（malicious software）とは、コンピュータウイルス（computer virus）やスパイウェア（spyware）、ランサムウェア、キーロガーなどの不正プログラムの総称です。

①コンピュータウイルス

コンピュータウイルスは、第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムです。コンピュータウイルスのうち、マクロと呼ばれる簡易プログラムで作成されたウイルスで、ワープロソフトの文書ファイルや表計算ソフトのワークシートに潜伏し、ファイルを開いたときに他の同一形式のファイルに感染するものを**マクロウイルス**（macro virus）と呼びます。

また、コンピュータシステムまたはネットワークを介して自分自身を繁殖させることができるものを**ワーム**（worm）、ネットワーク（インターネット）を介して感染したコンピュータを外部から操ることを目的として作成されたものを**ボット**（bot）、ボットを送り込み乗っ取ったコンピュータで構成されるネットワークを**ボットネット**と呼びます。

なお、ボットネットに対して指令（command）を出したり、制御（control）するサーバを **C&C サーバ**と呼びます。

ボットネットへの対策の一つに、C&Cサーバへのアクセスを遮断する方法が考えらます。

例題

ボットネットにおける C&C サーバの役割はどれか。

ア Web サイトのコンテンツをキャッシュし，本来のサーバに代わってコンテンツを利用者に配信することによって，ネットワークやサーバの負荷を軽減する。
イ 遠隔地からインターネットを経由して社内ネットワークにアクセスする際に，CHAP などのプロトコルを用いることによって，利用者認証時のパスワードの盗聴を防止する。
ウ 遠隔地からインターネットを経由して社内ネットワークにアクセスする際に，チャレンジレスポンス方式を採用したワンタイムパスワードを用いることによって，利用者認証時のパスワードの盗聴を防止する。
エ 侵入して乗っ取ったコンピュータに対して，他のコンピュータへの攻撃などの不正な操作をするよう，外部から命令を出したり応答を受け取ったりする。

ア プロキシサーバに関する記述です。
イ RAS サーバに関する記述です。
ウ RADIUSサーバに関する記述です。

情報セキュリティマネジメント 平成28年度秋 問12［出題頻度:★★☆］

解答ーエ

別冊演習ドリル 1-8～11

②スパイウェア

スパイウェアは、有用なプログラムやツールを装うことで、利用者に気付かれずにコンピュータに侵入し、不正に個人情報などを収集するプログラムで、代表的なスパイウェアに**トロイの木馬**(Trojan horse)があります。スパイウェアによる被害を防ぐにはスパイウェア対策ソフトを導入し、怪しいサイトに近づかず、不用意なダウンロードは行わず、添付ファイルは開かない、などの注意が必要です。

例題

不正プログラムの一種であるトロイの木馬の特徴はどれか。

ア アプリケーションソフトのマクロ機能を利用してデータファイルに感染する。
イ 新種ウイルスの警告メッセージなどの偽りのウイルス情報をチェーンメールで流す。
ウ ネットワークを利用して，他のコンピュータに自分自身のコピーを送り込んで自己増殖する。
エ 有用なソフトウェアに見せかけて配布された後，システムの破壊や個人情報の詐取など悪意ある動作をする。

ア マクロウイルスに関する記述です。
イ デマウイルスに関する記述です。
ウ ワームに関する記述です。

ITパスポート 平成24年度春 問54 [出題頻度:★☆☆]

解答ーエ

別冊演習ドリル 1-12

③ランサムウェア

ランサムウェアは、感染すると勝手にファイルやデータの暗号化などを行って、正常にデータにアクセスできないようにし、元に戻すための代金を利用者に要求するプログラムです。

例題

ランサムウェアに分類されるものはどれか。

ア 感染したPCが外部と通信できるようプログラムを起動し，遠隔操作を可能にするマルウェア
イ 感染したPCに保存されているパスワード情報を盗み出すマルウェア
ウ 感染したPCのキー操作を記録し，ネットバンキングの暗証番号を盗むマルウェア
エ 感染したPCのファイルを暗号化し，ファイルの復号と引換えに金銭を要求するマルウェア

ア ボットに分類されます。
イ 様々なマルウェアが作られていますが、特別な総称はありません。
ウ キーロガーに分類されます。

情報セキュリティマネジメント 平成28年度秋 問27 [出題頻度:★☆☆]

解答ーエ

別冊演習ドリル 1-13

④キーロガー

キーロガーは、キーボードからの入力情報を監視するソフトウェアやハードウェアのことで、単に入力された文字だけでなく、使用したアプリケーションなども記録できるものもあります。

利用者 ID やパスワードなどの情報を不正に入手するために、不特定多数の利用者が利用するパソコンに、秘かにキーロガーを仕掛ける事例が増えています。

例題

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 ブ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 ブラウザの起動時に，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。

ア 中間者攻撃(Man-in-the-middle)に関する記述です。
ウ アドウェアに関する記述です。
エ ブラウザ・ハイジャッカーに関する記述です。

基本情報 平成27年度春 問37 [出題頻度:★☆☆]

解答ーイ

別冊演習ドリル 1-14

⑤ルートキット

ルートキット(rootkit)は、攻撃者が不正侵入後に利用するために、マルウェアなどの攻撃ツールをパッケージ化して隠蔽するプログラムです。

例題

サーバにバックドアを作り，サーバ内での侵入の痕跡を隠蔽するなどの機能をもつ不正なプログラムやツールのパッケージはどれか。

ア RFID　　イ rootkit　　ウ TKIP　　エ web beacon

ア RFID は、タグと呼ばれる微小な IC チップに商品情報などを埋め込み、対象を識別・管理するシステムです。
ウ TKIP は、無線 LAN において暗号化通信を行うためのプロトコルです。
エ web beacon は、目に見えない画像を Web ページや HTML メールに埋め込み、これを閲覧した時に画像ファイルが置かれたサーバに読出し要求が来ることを利用して、利用者のアクセス動向などの情報を収集する仕組みです。

情報セキュリティマネジメント 平成28年度秋 問14 [出題頻度:★☆☆]

解答ーイ

別冊演習ドリル 1-15

⑥バックドア

バックドアは、攻撃者が不正な行為に利用するため、企業内情報ネットワークやサーバに設置した通常以外の侵入経路です。

例題

バックドアに該当するものはどれか。

ア 攻撃を受けた結果，ロックアウトされた利用者アカウント
イ システム内に攻撃者が秘密裏に作成した利用者アカウント
ウ 退職などの理由で，システム管理者が無効にした利用者アカウント
エ パスワードの有効期限が切れた利用者アカウント

バックドアは、攻撃者が不正行為に利用するために、企業内ネットワークやサーバに設置した通常以外の侵入経路です。

情報セキュリティマネジメント 平成28年度春 問27 [出題頻度:★☆☆]

解答ーイ

別冊演習ドリル 1-16

⑦偽セキュリティ対策ソフト型ウイルス

偽セキュリティ対策ソフト型ウイルスは、セキュリティ機能を有しているように偽装したマルウェアで、偽のセキュリティ上の警告メッセージを表示して不安をあおり、これを購入させて、金銭を搾取します。

4. 脆弱性

脅威の発生を誘発する弱点を情報システムの**脆弱性**と呼びます。JIS Q 27000:2019 では、脆弱性を、「一つ以上の脅威によって付け込まれる可能性のある，資産又は管理策の弱点。」と定義しています。具体的には、情報システムの情報セキュリティに関する欠陥、企業、組織、個人に対する行動規範の不徹底、未整備などです。

また、ハードウェアを含めたシステム全体の欠陥や弱点を脆弱性と呼ぶのに対して、ソフトウェアの**バグ**（欠陥、欠陥が原因となって発生する誤動作）によって発生するセキュリティ上の欠陥や弱点を特に**セキュリティホール**と呼びます。

なお、攻撃者は、事前に利用可能なサービス（ポート）を調査する**ポートスキャン**を行い、攻撃対象を決定します。

例題

攻撃者がシステムに侵入するときにポートスキャンを行う目的はどれか。

ア 事前調査の段階で，攻撃できそうなサービスがあるかどうかを調査する。
イ 権限取得の段階で，権限を奪取できそうなアカウントがあるかどうかを調査する。
ウ 不正実行の段階で，攻撃者にとって有益な利用者情報があるかどうかを調査する。
エ 後処理の段階で，システムログに攻撃の痕跡が残っていないかどうかを調査する。

ポートスキャンは、コンピュータやルータのアクセス可能な通信ポートを外部から調査することです。攻撃者がシステムに侵入するときに、攻撃できそうなサービスがあるかどうか事前に調査する場合に、行います。

情報セキュリティマネジメント 平成28年度春 問29 [出題頻度:★★☆]

解答ーア

別冊演習ドリル 1-17～19

5. 不正のメカニズム

不正のメカニズムについて、アメリカの犯罪学者であるドナルド. R. クレッシーは、「不正行為は、機会、動機、正当化の3要素がそろったときに初めて行われる」という「**不正のトライアングル**（機会、動機、正当化）理論」を唱えました。

機会は、不正行為を容易に実行できる客観的環境です。

動機は、不正行為の実行に対する主観的欲求です。

正当化は、不正行為の実行を肯定する主観的事情です。

例題

“不正のトライアングル”理論において，全てそろったときに不正が発生すると考えられている3要素はどれか。

ア 機会，動機，正当化　　イ 機密性，完全性，可用性
ウ 顧客，競合，自社　　エ 認証，認可，アカウンティング

機会、動機、正当化の3要素のうち1つでも欠ければ不正は発生しないと考えられます。

情報セキュリティマネジメント 平成28年度春 問9 [出題頻度:★☆☆]
解答ーア

別冊演習ドリル 1-20

6. 攻撃者の種類、攻撃の動機

コンピュータやネットワークに関して高度な技術をもつ者をハッカーと呼び、その技術を利用して、コンピュータやネットワークに不正に侵入して破壊・改ざんなど（クラッキング）を行う者をクラッカーと呼びます。

クラッカーは愉快犯である場合が多いですが、クラッキングにより詐欺や恐喝などを行う詐欺犯や故意犯もいます。その中で、ボットネットを指揮して犯罪を行うクラッカーを特に**ボットハーダー**と呼びます。また、興味本位で他のクラッカーが制作した不正プログラムを利用してクラッキングを行う**スクリプトキディ**と呼ばれる者もいます。

攻撃には様々な動機がありますが、最も一般的な動機は金銭奪取です。また、社会的・政治的主張が攻撃の動機となる場合もあります。社会的・政治的主張のためにクラッキングを行うことを**ハクティビズム**と呼びます。

なお、国民生活や社会・経済基盤を標的にした大規模なクラッキングを**サイバーテロリズム**と呼びます。

例題

スクリプトキディの典型的な行為に該当するものはどれか。

ア PC の利用者が Web サイトにアクセスし，利用者 ID とパスワードを入力するところを後ろから盗み見して，メモをとる。
イ 技術不足なので新しい攻撃手法を考え出すことはできないが，公開された方法に従って不正アクセスを行う。
ウ 顧客になりすまして電話でシステム管理者にパスワードの再発行を依頼し，新しいパスワードを聞き出すための台本を作成する。
エ スクリプト言語を利用してプログラムを作成し，広告や勧誘などの迷惑メールを不特定多数に送信する。

ア ショルダハッキングに関する記述です。
ウ ソーシャルエンジニアリングに関する記述です。
エ スパムメール（迷惑メール）に関する記述です。

情報セキュリティマネジメント 平成28年度秋 問24 [出題頻度:★☆☆]
解答ーイ

7. 攻撃手法

システムの脆弱性を悪用する攻撃手法には様々な種類があります。

1）不正ログイン

コンピュータやネットワークに不正ログインする代表的な攻撃手法は次のとおりです。

①パスワードクラック

他人のパスワードを見破ることを**パスワードクラック**と呼び、代表的な方法に総当たり攻撃、辞書攻撃、レインボー攻撃があります。

総当たり（ブルートフォース）攻撃は、文字を組み合わせてあらゆるパスワードでログインを何度も試みて、力ずくでパスワードを取得する攻撃手法です。

辞書攻撃は、利用者がパスワードとして使いそうな文字列をあらかじめ辞書ファイルとして登録しておき、その辞書ファイルにある言葉を片っ端から入力し、力ずくでパスワードを取得する攻撃手法です。

レインボー攻撃は、パスワードとして使いそうな文字列のハッシュ値のリスト（レインボーリスト）を、あらかじめ用意しておき、攻撃目標のハッシュ値を比較して、パスワードを推測する攻撃手法です。

なお、ネットワーク上のデータを盗聴して ID やパスワードを不正に取得する方法を**スニッフィング**と呼びます。

例題

サーバへのログイン時に用いるパスワードを不正に取得しようとする攻撃とその対策の組合せのうち，適切なものはどれか。

	辞書攻撃	スニッフィング	ブルートフォース攻撃
ア	推測されにくいパスワードを設定する。	パスワードを暗号化して送信する。	ログインの試行回数に制限を設ける。
イ	推測されにくいパスワードを設定する。	ログインの試行回数に制限を設ける。	パスワードを暗号化して送信する。
ウ	パスワードを暗号化して送信する。	ログインの試行回数に制限を設ける。	推測されにくいパスワードを設定する。
エ	ログインの試行回数に制限を設ける。	推測されにくいパスワードを設定する。	パスワードを暗号化して送信する。

辞書攻撃は、利用者がパスワードに使いそうな言葉をあらかじめ登録した辞書ファイルに記載の言葉を先頭から順に入力することでパスワードを探し出そうとするため、推測されにくいパスワードを設定することで被害を防ぐことができます。

スニッフィングは、ネットワーク上のデータを盗聴して、IDやパスワードを不正取得するので、パスワードを暗号化することで被害を防ぐことができます。

ブルートフォース攻撃は、適当に文字を組み合わせて作成したパスワードでログインを繰り返すことで、力ずくでパスワードを探し出そうとするため、推測しにくいパスワードを設定する、ログインの試行回数に制限を設けるなどの方法で被害を防ぐことができます。

情報セキュリティマネジメント　平成29年度春　問16［出題頻度:★☆☆］

解答ーア

別冊演習ドリル　1-21

②パスワードリスト攻撃

パスワードリスト攻撃は、あらかじめ何らかの方法で取得した ID とパスワードをリスト化し、これを用いて不正ログインする攻撃手法です。

例題

パスワードリスト攻撃に該当するものはどれか。

ア 一般的な単語や人名からパスワードのリストを作成し，インターネットバンキングへのログインを試行する。
イ 想定し得るパスワードとそのハッシュ値との対のリストを用いて，入手したハッシュ値からパスワードを効率的に解析する。
ウ どこかの Web サイトから流出した利用者 ID とパスワードのリストを用いて，他の Web サイトに対してログインを試行する。
エ ピクチャパスワードの入力を録画してリスト化しておき，それを利用することでタブレット端末へのログインを試行する。

ア 辞書攻撃に関する記述です。
イ レインボー攻撃に関する記述です。
エ ピクチャパスワードハッキングに関する記述です。

情報セキュリティマネジメント 平成28年度秋 問26 [出題頻度:★★☆]
解答ーウ

別冊演習ドリル 1-22、23

2）Web アプリケーションの脆弱性

Web アプリケーションの脆弱性を利用した代表的な攻撃手法は次のとおりです。

①クロスサイトスクリプティング

クロスサイトスクリプティングは、悪意をもったスクリプトを、標的となるサイト経由で利用者のブラウザに送り込み、その標的にアクセスした利用者のクッキー（Cookie）にある個人情報を盗み取る攻撃手法です。

②クロスサイトリクエストフォージェリ

クロスサイトリクエストフォージェリは、Web サイトに不正なスクリプトや HTTP リダイレクト（自動転送）などを埋め込むことで、閲覧者の意図に関わらず別の Web サイトを不正に操作させる攻撃手法です。

③クリックジャッキング

クリックジャッキングは、Web サイトのコンテンツ上に透明化した標的サイトのコンテンツを配置し、利用者が気づかないうちに標的サイト上で意図に反した操作を実行させる攻撃手法です。

④ドライブバイダウンロード

ドライブバイダウンロードは、Web サイトにアクセスした利用者に気付かれないように、自動的にマルウェアなどをダウンロードし実行する攻撃手法です。

⑤SQL インジェクション

SQL インジェクションは、Web ページ上で利用者がデータを入力する欄（入力フォーム）に、SQL 文を閉じる区切り文字と不正なコマンドを埋め込むことで、データベース内のレコードを不正に操作して、レコードに含まれる情報の改ざん、消去、盗聴などを行う攻撃手法です。

⑥ディレクトリトラバーサル

ディレクトリトラバーサルは、ファイルを Web アプリケーションが使用する場合に、相対パス指定を悪用し、サーバ内の想定外のファイル名を直接指定することによって、本来は許されないファイルを不正に閲覧する攻撃手法です。

⑦SEO ポイズニング

SEO ポイズニングは、Web 検索サイトの順位付けアルゴリズムを悪用して、検索結果の上位に、悪意のある Web サイトを意図的に表示させる攻撃手法です。

例題

クロスサイトスクリプティングの手口はどれか。

ア Web アプリケーションに用意された入力フィールドに，悪意のある JavaScript コードを含んだデータを入力する。
イ インターネットなどのネットワークを通じてサーバに不正にアクセスしたり，データの改ざんや破壊を行ったりする。
ウ 大量のデータを Web アプリケーションに送ることによって，用意されたバッファ領域をあふれさせる。
エ パス名を推定することによって，本来は認証された後にしかアクセスが許可されていないページに直接ジャンプする。

イ 不正アクセスに関する記述です。
ウ バッファオーバフロー攻撃に関する記述です。
エ ディレクトリトラバーサル攻撃に関する記述です。

情報セキュリティマネジメント 平成28年度秋 問22 [出題頻度:★★★]
解答ーア

別冊演習ドリル 1-24～29

3)ネットワークの脆弱性

ネットワークの脆弱性を利用した代表的な攻撃手法は次のとおりです。

①中間者攻撃

中間者攻撃（**Man-in-the-middle attack**）は、送信者と受信者の間に介在し、当事者に成りすまして通信内容を横取りする攻撃手法です。

②第三者中継

第三者中継は、自分とは無関係の第三者のメールサーバを不正に中継することで、送信者が身元を偽ってメールを送信する攻撃手法です。

③IP スプーフィング

IP スプーフィングは、偽の IP アドレスを使いファイアウォールを突破してネットワークに侵入する攻撃手法です。

④DNS キャッシュポイズニング

DNS キャッシュポイズニングは、DNS サーバの情報を不正に書き換えることで、インターネットの閲覧者を偽の Web サイトに誘導する攻撃手法です。

⑤セッションハイジャック

セッションハイジャックは、セッション ID やセッションクッキーを盗んで、利用者になりすまして不正アクセスする攻撃手法です。

⑥リプレイ攻撃

リプレイ攻撃は、正当な利用者のログインシーケンスを記録して盗聴することで、利用者になりすまして不正アクセスする攻撃手法です。ログインシーケンスとは、ログインするための一連の手続きを指します。

例題

DNS キャッシュポイズニングに分類される攻撃内容はどれか。

ア DNS サーバのソフトウェアのバージョン情報を入手して，DNS サーバのセキュリティホールを特定する。
イ PC が参照する DNS サーバに偽のドメイン情報を注入して，利用者を偽装されたサーバに誘導する。
ウ 攻撃対象のサービスを妨害するために，攻撃者が DNS サーバを踏み台に利用して再帰的な問合せを大量に行う。
エ 内部情報を入手するために，DNS サーバが保存するゾーン情報をまとめて転送させる。

ア 攻撃する前の事前調査であるバナーチェックに関する記述です。
ウ DDoS攻撃に関する記述です。
エ ゾーン転送を利用した攻撃をする前の事前調査です。

情報セキュリティマネジメント 平成29年度秋 問22 [出題頻度:★☆☆]
解答ーイ

別冊演習ドリル 1-30～32

4)サービス妨害

CPU やサーバ、ネットワークに過大な負荷をかけることで利用者へのサービスの提供を妨害する代表的な攻撃手法は次のとおりです。

①DoS 攻撃

DoS 攻撃は、攻撃目標のサーバに大量のデータを送信して過大な負荷をかけることで、サービスの低下や停止に追い込む攻撃手法です。

②DDoS 攻撃

DDoS 攻撃は、複数の全く関係のない第三者のコンピュータに攻撃プログラムを仕掛けて踏み台にすることで、標的とするサーバに一斉にデータを送信し、過大な負荷をかけて、サービスの低下や停止に追い込む攻撃手法です。

③メールボム

メールボム(電子メール爆弾)は、サイズが大きい電子メールや大量の電子メールを送り付ける攻撃手法です。

例題

DoS(Denial of Service)攻撃の説明として，適切なものはどれか。

ア 他人になりすまして，ネットワーク上のサービスを不正に利用すること
イ 通信経路上で他人のデータを盗み見ること
ウ 電子メールや Web リクエストなどを大量に送りつけて，ネットワーク上のサービスを提供不能にすること
エ 文字の組合せを順に試すことによって，パスワードを解読しようとすること

ア なりすましに関する記述です。
イ 盗聴に関する記述です。
エ ブルートフォース攻撃に関する記述です。

ITパスポート 平成25年度春 問52 [出題頻度:★☆☆]
解答ーウ

別冊演習ドリル 1-33

5）標的型攻撃

特定の企業や組織を狙った**標的型攻撃**の代表的な攻撃手法は次のとおりです。

①APT

APT（Advanced Persistent Threats：持続的標的型攻撃）は、特定の企業や組織に狙いを定め、複数の手段を組み合わせてシステムに侵入・潜伏し、データの盗聴や改ざんなどの攻撃を長期間継続して行う攻撃手法です。

②水飲み場型攻撃

水飲み場型攻撃（Watering Hole Attack）は、標的となる企業や組織の構成員が頻繁にアクセスするWebサイトを改ざんし、当該構成員がアクセスした時だけマルウェアに感染するようにした攻撃手法です。

例題

APTの説明はどれか。

ア　攻撃者はDoS攻撃及びDDoS攻撃を繰り返し組み合わせて，長期間にわたり特定組織の業務を妨害する。
イ　攻撃者は興味本位で場当たり的に，公開されている攻撃ツールや脆弱性検査ツールを悪用した攻撃を繰り返す。
ウ　攻撃者は特定の目的をもち，標的となる組織の防御策に応じて複数の手法を組み合わせ，気付かれないよう執拗に攻撃を繰り返す。
エ　攻撃者は不特定多数への感染を目的として，複数の攻撃方法を組み合わせたマルウェアを継続的にばらまく。

特定の個人や組織に対する攻撃を標的型攻撃と呼びます。その中で、複数の手法を組み合わせて持続的に行われるものは、APTと呼ばれます。

情報セキュリティマネジメント　平成28年度春　問19［出題頻度：★☆☆］

解答－ウ

別冊演習ドリル　1-34

6）近年深刻化する脅威

上記以外に、近年深刻化する脅威には次のようなものがあります。

①フィッシング

偽のメールやWebサイトを用いて、個人情報やクレジットカード番号、パスワードなどの情報を不正に入手する行為を**フィッシング**と呼び、代表例にワンクリック詐欺やスミッシングがあります。

ワンクリック詐欺は、メールやWebサイトに記載されているURLを一度クリックしただけで一方的に契約を了承したことにされて代金を請求する手法です。

スミッシングは、携帯電話のショートメッセージサービスを利用したフィッシングです。

②ゼロデイ攻撃

ゼロデイ攻撃は、セキュリティの脆弱性が公表される（セキュリティパッチが提供される）前にセキュリティホールに対して行われる攻撃手法です。

③サイドチャネル攻撃

サイドチャネル攻撃は、暗号化機能を有する機器が暗号化の際に生ずる処理時間や消費電力、電磁波などのサイドチャネル情報を観察することで、暗号化鍵などの情報を取得する攻撃手法です。なお、処理時間に注目したものを**タイミング攻撃**、消費電力に注目したものを電力解析攻撃、電磁波に注目したものを電磁波解析攻撃（**テンペスト攻撃**）と呼ぶこともあります。

④フットプリンティング

フットプリンティングは、攻撃前に攻撃対象の情報を収集することで、DNSサーバのソフトのバージョン情報を入手して、DNSサーバのセキュリティホールを特定するなどの行為が、これに当たります。

例題

フィッシングの説明として，最も適切なものはどれか。

ア ウイルスに感染したコンピュータを，そのウイルスの機能を利用することによってインターネットなどのネットワークを介して外部から不正に操作する。
イ 偽の電子メールを送信するなどして，受信者を架空の Web サイトや実在している Web サイトの偽サイトに誘導し，情報を不正に取得する。
ウ 利用者が入力したデータをそのままブラウザに表示する機能が Web ページにあるとき，その機能の脆弱性を突いて悪意のあるスクリプトを埋め込み，そのページにアクセスした他の利用者の情報を不正に取得する。
エ 利用者に気づかれないように PC にプログラムを常駐させ，ファイルのデータや PC 操作の情報を不正に取得する。

ア ボットに関する記述です。
ウ クロスサイトスクリプティングに関する記述です。
エ スパイウェアに関する記述です。

ITパスポート 平成23年度秋 問87 [出題頻度:★☆☆]
解答ーイ

別冊演習ドリル 1-35～38

8. 情報セキュリティに関する技術

1）暗号技術

データを権限なしの照会や使用から保護する方法に、暗号化技術があります。通信データの漏えいや改ざんといった犯罪を防止するためには暗号化は欠かせません。

①CRYPTREC 暗号リスト

CRYPTREC 暗号リスト（電子政府推奨暗号リスト）は、総務省と経済産業省が共同で運営する暗号技術検討会及び関連委員会（CRYPTREC）が、安全性と実装性能が確認された暗号技術のうち、電子政府の調達時に利用することを推奨する暗号技術のリストです。

後述する AES や RSA の一種や、SHA-246 などがリストに掲載されています。

例題

CRYPTREC の役割として，適切なものはどれか。

ア 外国為替及び外国貿易法で規制されている暗号装置の輸出許可申請を審査，承諾する。
イ 政府調達において IT 関連製品のセキュリティ機能の適切性を評価，認証する。
ウ 電子政府での利用を推奨する暗号技術の安全性を評価，監視する。
エ 民間企業のサーバに対するセキュリティ攻撃を監視，検知する。

ア 外為法（外国為替及び外国貿易法）に関する記述です。
イ IT セキュリティ評価及び認証制度（Japan Information Technology Security Evaluation and Certification Scheme、JISEC）に関する記述です。
エ IDS（Intrusion Detection System：侵入検知システム）やIPS（Intrusion Prevention System：侵入防止システム）に関する記述です。

情報セキュリティマネジメント 平成29年度秋 問4 [出題頻度:★☆☆]
解答ーウ

別冊演習ドリル 1-39、40

②暗号方式

データを第三者が解読できないように一定のルールで変換することを**暗号化**といい、暗号化する前のデータを平文、暗号化されたデータを暗号文と呼びます。また、暗号文を平文に戻すことを**復号**といいます。

暗号化の代表的な方法には、共通鍵暗号方式と公開鍵暗号方式があります。

例題

電子メールを暗号化することによる効果はどれか。

ア 暗号化かぎの紛失を防止できる。
イ 電子メールの内容の漏えいを防止できる。
ウ メールサーバの送信記録を改ざんから保護できる。
エ メールサービスの妨害攻撃を防止できる。

暗号化の目的は、通信中にデータを盗聴されても、内容が分からないようにすることです。
これにより、重要なデータの漏えいを防ぐことができます。

基本情報 平成17年度秋 問64 [出題頻度:★☆☆]

解答ーイ

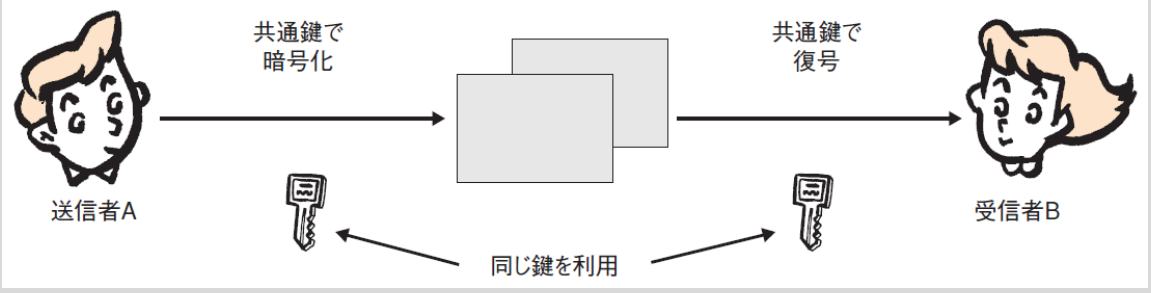
別冊演習ドリル 1-41

③共通鍵暗号方式

共通鍵暗号方式は、暗号化も復号も共通の鍵を用いる方式です。そのため、鍵情報は公開せずに秘密にします。この方式では、仮にN人の相手とデータのやり取りをする場合にはN個の鍵を必要とするため、鍵の管理が問題となります。また、鍵情報を安全に相手方に渡す方法を工夫する必要があります。

代表的な暗号化アルゴリズムに、**AES**(Advanced Encryption Standard)があります。

なお、共通鍵暗号方式には、データを一定の大きさ(ブロック)に分割して、ブロックごとに暗号化するブロック暗号利用モードとビット単位やバイト単位で行うストリーム暗号利用モードの2つがあります。

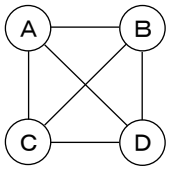


①送信者Aは、受信者Bとの間で持ち合う共通の鍵を用いて、データを暗号化する。
②暗号化したデータを受信者Bに送信する。
③受信者Bは、送信者Aから送られた暗号化データを自分が持つ送信者Aとの共通の鍵で復号する。

共通鍵暗号方式

例題

共通鍵暗号方式では通信の組合せごとに鍵が1個必要となる。例えばA～Dの4人が相互に通信を行う場合は，AB，AC，AD，BC，BD，CDの組合せの6個の鍵が必要である。10 人が相互に通信を行うためには何個の鍵が必要か。



ア 15　　イ 20　　ウ 45　　エ 50

共通鍵暗号方式では、平文を暗号化、暗号データを復号するために、同一の鍵を使用します。

例えば、3人のグループ(A、B、C)で共通鍵暗号方式を行った場合、Aは、BとCに対し、別々の鍵を渡すことによって「AとB」「AとC」の送受信を行うことになります。また、同様にBとCに関しても、自分以外のメンバ分だけ異なる鍵を配布する必要があります。

つまり、各人がもっている鍵の総和は「(人数－1)×人数」となります。ただし、鍵の種類で考えると、Aが渡したBの鍵と、BのAに対する鍵は同一のものとなるため、共通鍵の総数としては「(人数－1)×人数÷2」となります。

したがって、必要な鍵の個数は「(10－1)×10÷2＝45 個」となります。

ITパスポート　平成22年度春　問70 [出題頻度:★☆☆]

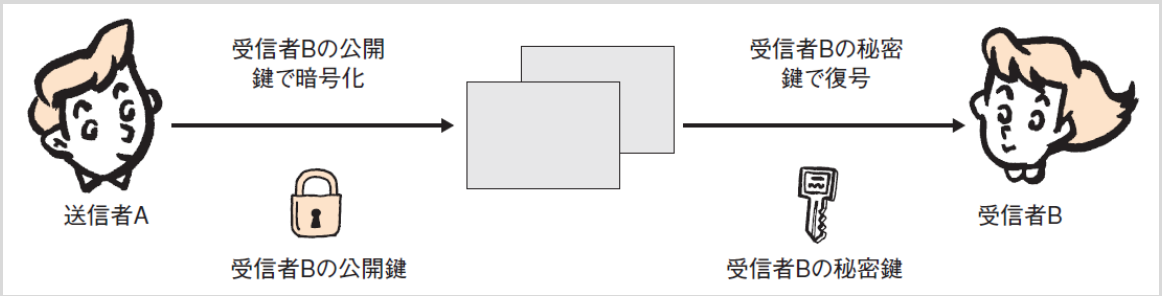
解答－ウ

別冊演習ドリル　1-42～44

④公開鍵暗号方式

公開鍵暗号方式は、データ受信者の**公開鍵**(暗号化のための鍵情報と暗号化アルゴリズムを不特定多数の者に公開)を使ってデータを暗号化する方式です。暗号化と復号のための鍵情報は共通でなく、復号のための鍵情報は**秘密鍵**として公開しません。暗号文の受信者は、公開鍵と対の秘密鍵で復号します。この方式は、暗号化の鍵を公開できるため、不特定多数との通信に向いています。ただし、共通鍵暗号方式に比べて、鍵情報を複雑にする必要があり、暗号化に多くの時間が必要となります。

代表的な暗号化アルゴリズムに、開発者の頭文字(Rivest、Shamir、Adleman)を取って命名された **RSA** があります。

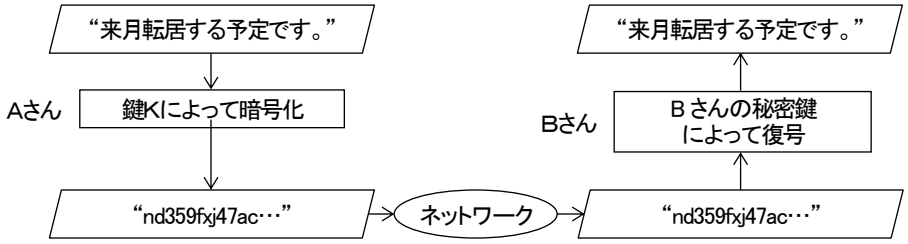


①送信者Aは、公開されている受信者Bの公開鍵を入手し、その鍵を用いてデータを暗号化する。
②暗号化したデータを受信者Bに送信する。
③受信者Bは、自分しか持たない復号用の鍵(秘密鍵)を用いてデータを復号する。

公開鍵暗号方式

例題

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 共通鍵

公開鍵暗号方式は、暗号化と復号に別の鍵を用い、暗号化には受信者側の公開鍵を使用し、復号には受信者側の秘密鍵を使用する方式です。本問では、送信者がA、受信者がBとなっているので選択肢ウが適切です。

情報セキュリティマネジメント　平成29年度秋　問28［出題頻度:★★★］

解答ーウ

別冊演習ドリル　1-45～48

⑤ハイブリッド暗号方式

共通鍵暗号方式は、公開鍵暗号方式に比べ処理は高速ですが、鍵情報を安全に配布することが難しいという問題があります。これに対して、公開鍵暗号方式は、鍵情報の管理は容易ですが、処理に時間がかかるという問題があります。この2つの相反する性質をもつ暗号方式を組み合わせることで互いの問題点を解決したのが、ハイブリッド暗号方式です。

ハイブリッド暗号方式では、まずデータを共通鍵で暗号化します。次に、受信者の公開鍵でデータを暗号化するために使った鍵情報（共通鍵）を暗号化し、暗号化したデータとともに受信者に送信します。受信者は、送信者から送られてきた鍵情報（共通鍵）を自分の秘密鍵を用いて復号し、復号された共通鍵を使って暗号化されたデータを復号します。

なお、ハイブリッド暗号方式を用いる代表的なプロトコルに後述するS/MIMEやPGPがあります。。

例題

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

データの暗号化と復号に共通鍵暗号方式を用い、その際の共通鍵を公開鍵暗号方式で暗号化して相手に送る方法を、ハイブリッド暗号方式と呼びます。
ア 電子メールの送達を確認するには、受信者に送達の事実を知らせてもらいます。
イ 送信者のなりすましの検出には、公開鍵暗号方式を応用したディジタル署名を用います。
ウ 電子メールの本文の改ざんの有無の検出には、メッセージ認証符号を用います。

基本情報 平成22年度秋 問41 [出題頻度:★☆☆]
解答ーエ

別冊演習ドリル 1-49、50

⑥ハッシュ関数

データ(メッセージ)をそのサイズに関わらず128から512ビット程度の一定のサイズに変換する関数を**ハッシュ関数**と呼び、ハッシュ関数によって演算した結果をハッシュ値(**メッセージダイジェスト**)と呼びます。ハッシュ関数から得られたハッシュ値は、異なるデータが同じ値になることがほとんどありません。

代表的なハッシュ関数に、可変長のデータから256ビットのハッシュ値を生成する**SHA-256**があります。

例題

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。

ア メッセージダイジェストから元のメッセージを求めることはできません。
イ メッセージが異なればメッセージダイジェストも異なります。
エ ハッシュ関数が生成するメッセージダイジェストの長さは一定になります。

情報セキュリティマネジメント 平成29年度春 問20[出題頻度:★☆☆]
解答ーウ

別冊演習ドリル 1-51

⑦S/MIME

S/MIME(Secure MIME)は、画像や音声などのマルチメディアデータをメールで送信するためのプロトコルであるMIMEに暗号化機能を加えたプロトコルです。S/MIMEを用いてメッセージを送信することで、盗聴、改ざんを防ぐことができます。なお S/MIME では、共通鍵暗号方式によりメッセージ本文を暗号化し、共通鍵の受渡しに公開鍵暗号方式を用いるハイブリッド暗号方式を採用しているので、受信者はあらかじめ自身の公開鍵が本物であることを証明する公開鍵証明書を取得しておく必要があります。

例題

Aさんが Bさんに暗号化メールを送信したい。S/MIME(Secure/Multipurpose Internet Mail Extensions)を利用して暗号化したメールを送信する場合の条件のうち，適切なものはどれか。

ア Aさん，Bさんともに，あらかじめ，自身の公開鍵証明書の発行を受けておく必要がある。
イ Aさん，Bさんともに，同一の ISP(Internet Service Provider)に属している必要がある。
ウ Aさんが属している ISP が S/MIME に対応している必要がある。
エ Bさんはあらかじめ，自身の公開鍵証明書の発行を受けておく必要があるが，Aさんはその必要はない。

S/MIME は、ハイブリッド暗号方式を用いて電子メールを暗号化するプロトコルです。送信者(A さん)は、暗号化に使用する受信者(B さん)の公開鍵が本物であるか判断するために、受信者の公開鍵証明書を確認します。

ITパスポート 平成24年度秋 問56 [出題頻度:★★☆]
解答ーエ

別冊演習ドリル 1-52

⑧PGP

PGP(Pretty Good Privacy)は、S/MIME と同様に、共通鍵暗号方式によりメッセージ本文を暗号化し、共通鍵の受渡しに公開鍵暗号方式を用いるハイブリッド暗号方式を採用していますが、事前に当事者間で公開鍵を交換することを前提としているため、公開鍵の所有者を保証する仕組みは必要としません。また、入手した公開鍵の有効性を確認する仕組みもありません。

⑨危殆化

危殆化とは、「危険な状態になる」という意味で、コンピュータの処理能力の向上や暗号解読技術の進歩は、既存の暗号化技術の危殆化を招いています。

例題

暗号の危殆化に該当するものはどれか。

ア 暗号化通信を行う前に，データの伝送速度や，暗号の設定情報などを交換すること
イ 考案された当時は容易に解読できなかった暗号アルゴリズムが，コンピュータの性能の飛躍的な向上などによって，解読されやすい状態になること
ウ 自身が保有する鍵を使って，暗号化されたデータから元のデータを復元すること
エ 元のデータから一定の計算手順に従って疑似乱数を求め，元のデータをその疑似乱数に置き換えること

コンピュータの処理能力の向上や暗号解読技術の進歩は、既存の暗号化技術の危殆化を招いています。

情報セキュリティマネジメント 平成29年度春 問9 [出題頻度:★☆☆]
解答ーイ

別冊演習ドリル 1-53

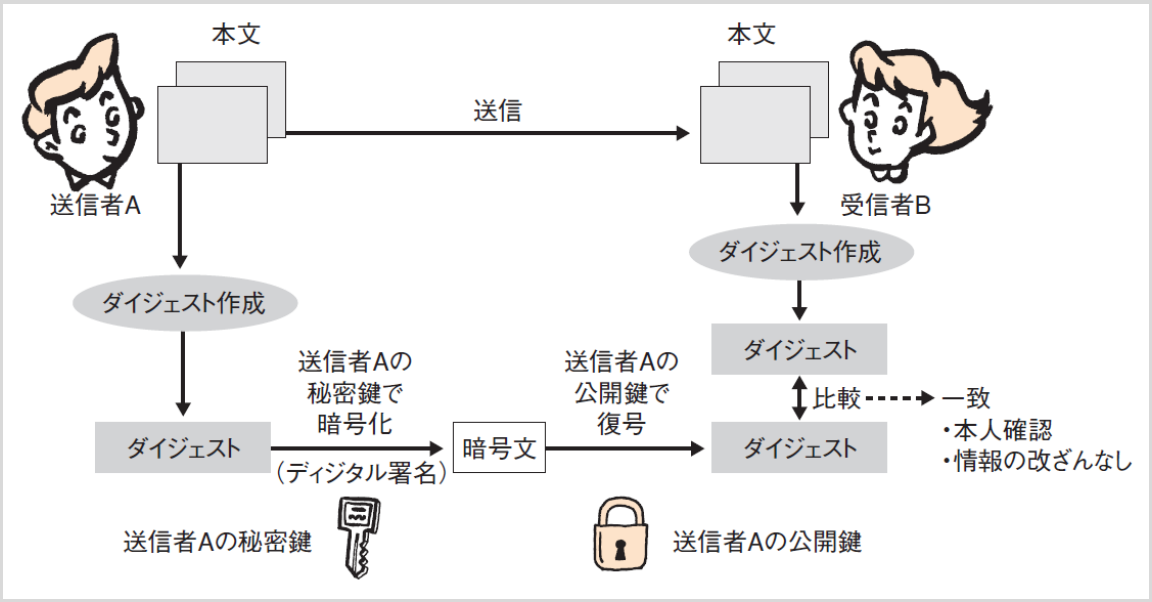
2）認証技術

対象物の正当性を証明する方法を認証技術と呼びます。代表的な認証技術に、ディジタル署名、タイムスタンプ、メッセージ認証、チャレンジレスポンス認証があります。

①ディジタル署名

ディジタル署名（電子署名）は、データが正当な送り手からのものであることを証明する（送信者認証）と同時に、改ざんされていないことを証明する（メッセージ認証）方法です。

ディジタル署名は、公開鍵暗号方式を応用した方法で、公開鍵暗号方式が受信者の公開鍵で暗号化するのに対して、ディジタル署名は送信者の秘密鍵で暗号化する点が異なります。これは、「送信者の秘密鍵で暗号化したデータは、送信者の公開鍵のみで復号できる」ということから、データの送り手を証明するものです。なお、送信者の秘密鍵を**署名鍵**、送信者の公開鍵を**検証鍵**と呼ぶことがあります。



①送信者Aは、本文データからハッシュ値（メッセージダイジェスト）を生成し、それを自分の秘密鍵で暗号化する。
②本文データと①の暗号化されたハッシュ値を送信する。
③受信者Bは、本文データからハッシュ値を生成し、さらに②の暗号化されたハッシュ値を送信者Aの公開鍵で復号する。
④③で生成したハッシュ値と復号したハッシュ値が一致すれば、送信者がA本人であること、改ざんがなされていないことが証明される。

ディジタル署名

例題

送信者Aが文書ファイルと，その文書ファイルのディジタル署名を受信者Bに送信したとき，受信者Bができることはどれか。ここで，受信者Bは送信者Aの署名検証鍵Xを保有しており，受信者Bと第三者は送信者Aの署名生成鍵Yを知らないものとする。

ア ディジタル署名，文書ファイル及び署名検証鍵Xを比較することによって，文書ファイルに改ざんがあった場合，その部分を判別できる。
イ 文書ファイルがウイルスに感染していないことを認証局に問い合わせて確認できる。
ウ 文書ファイルが改ざんされていないこと，及びディジタル署名が署名生成鍵Yによって生成されたことを確認できる。
エ 文書ファイルとディジタル署名のどちらかが改ざんされた場合，どちらが改ざんされたかを判別できる。

ディジタル署名は、データが正当な送り手からのものであることを証明すると同時に、改ざんされていないことを証明する方法です。

ディジタル署名は、公開鍵暗号方式を応用した方法で、「送信者の秘密鍵で暗号化したデータは、送信者の公開鍵のみで復号できる」ということから、送信者の正当性を証明する方法です。なお、送信者の秘密鍵を署名鍵、送信者の公開鍵を検証鍵と呼ぶことがあります。

情報セキュリティマネジメント　平成28年度春　問23［出題頻度:★★★］

解答ーウ

別冊演習ドリル　1-54～57

②タイムスタンプ

タイムスタンプ（**時刻認証**）は、データが存在していた日時を記録した情報です。第三者機関（タイプスタンプ機関）がタイムスタンプを付与したデータにディジタル署名することで、タイムスタンプの正当性と完全性を保証します。ディジタル署名されたデータを公開する場合、タイムスタンプを利用すると、公開されたデータがまさしく本人のものであることと同時に、公開以前にデータが存在していたことを示し、データの作成を否認することを防ぎます。

例題

情報セキュリティにおけるタイムスタンプサービスの説明はどれか。

ア 公式の記録において使われる全世界共通の日時情報を，暗号化通信を用いて安全に表示するWebサービス
イ 指紋，声紋，静脈パターン，網膜，虹彩などの生体情報を，認証システムに登録した日時を用いて認証するサービス
ウ 電子データが，ある日時に確かに存在していたこと，及びその日時以降に改ざんされていないことを証明するサービス
エ ネットワーク上のPCやサーバの時計を合わせるための日時情報を途中で改ざんされないように通知するサービス

タイムスタンプの付与は、付与した時点で電子データが存在していたこと、改ざんされていないことを証明します。

情報セキュリティマネジメント　平成29年度春　問10［出題頻度:★☆☆］

解答ーウ

別冊演習ドリル　1-58

③メッセージ認証

メッセージ認証は、受け取ったデータ(メッセージ)が改ざんされていないことを確認する方法です。

ハッシュ値は、異なるデータが同じ値になることがほとんどありません。そのため、送信者はデータと共にそのハッシュ値を送信し、受信者は受け取ったデータからハッシュ値を生成し、これと送信者から受け取ったハッシュ値との一致を確認することで、データが改ざんされていないことを確認できます。

例題

送信者から電子メール本文とそのハッシュ値を受け取り，そのハッシュ値と，受信者が電子メール本文から求めたハッシュ値とを比較することで実現できることはどれか。ここで，受信者が送信者から受け取るハッシュ値は正しいものとする。

ア 電子メールの送達の確認　　イ 電子メール本文の改ざんの有無の検出
ウ 電子メール本文の盗聴の防止　　エ なりすましの防止

ア 電子メールの送達の確認は、受信者側から受信の旨を返信してもらうことで確認します。
ウ 電子メール本文の盗聴の防止は、暗号化によって行います。
エ 送信者へのなりすましの防止は、送信者が自身の情報を認証機関に登録し、受信者がこれを利用することで行います。

基本情報　平成24年度春　問40［出題頻度:★☆☆］

解答－イ

④メッセージ認証符号

メッセージ認証符号(**MAC**:Message Authentication Code)は、送信データに共通鍵をつけてハッシュ化したデータ(メッセージダイジェスト)です。

送信者はデータ(メッセージ)とともにメッセージ認証符号を送信し、受信者は受け取ったデータからメッセージ認証符号を作成し、これと送信者から受け取ったメッセージ認証符号との一致を確認することによって、データの正当性を証明します(メッセージ認証)。

例題

次のようなAからBへの公開鍵暗号方式に基づく通信モデルがある。このモデルに関する記述のうち，適切なものはどれか。

Aが送信するメッセージからメッセージ認証符号を生成する。それをAの秘密鍵で暗号化したビット列を生成し，元のメッセージとともに電子メールを利用してBへ送信する。
Bは，Aの公開鍵を信頼できる機関から入手し，受信したビット列を復号してメッセージ認証符号を得るとともに，受信したメッセージからメッセージ認証符号を生成し，両者の合致を確認した上でメッセージを利用する。

ア Aは，メッセージがBに届いたことを確認できる。
イ Aは，メッセージの内容が盗聴されないことをBに対して保証できる。
ウ Bは，Aからのメッセージを確実に受信できる。
エ Bは，メッセージの送信者がAであり，内容の改ざんがないことを確認できる。

メッセージ認証符号が一致したということは、メッセージが途中で改ざんされていないことを示しています。

初級システムアドミニストレータ　平成15年度秋　問51［出題頻度:★☆☆］

解答－エ

別冊演習ドリル　1-59

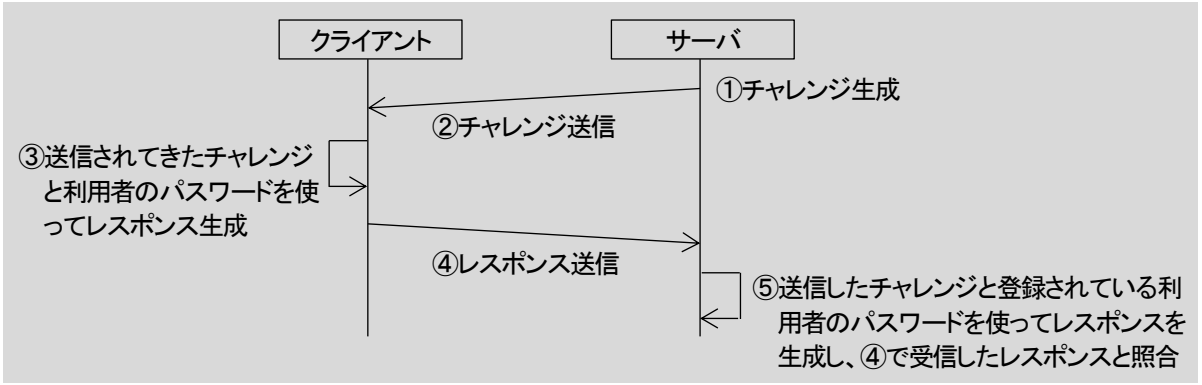
⑤チャレンジレスポンス認証

チャレンジレスポンス認証は、ネットワークにおける利用者認証の方式です。

クライアントは、利用者が入力したパスワードと、サーバから送られてきたランダムなデータであるチャレンジからレスポンスと呼ばれるデータを生成し、サーバに送り返します。

サーバは送信したチャレンジと利用者があらかじめ登録したパスワードからレスポンスを生成し、利用者から送られてきたレスポンスと照合します。両者の一致を確認することで利用者の正当性を確認します。

なお、チャレンジレスポンス認証を用いることで、パスワード自体が通信されないため、ネットワーク上でのパスワードの漏えいと、リプレイ攻撃を防ぐことができます。



チャレンジレスポンス認証の手順

例題

二つの通信主体XとYの間で，次の手順で情報交換を行う認証はどれか。

〔手順〕
(1) Yは，任意の情報を含む文字列(チャレンジ)をXへ送信する。
(2) Xは，あらかじめX，Y間で定めた規則に基づき，受け取った文字列から新たな文字列(レスポンス)を生成し，Yへ返送する。
(3) Yは，返送されてきた文字列(レスポンス)が正しいことを確認する。

ア XがYを認証する。
イ XがYを認証することによって，結果としてYがXを認証する。
ウ YがXを認証する。
エ YがXを認証することによって，結果としてXがYを認証する。

問題文に示された手順で、仮に悪意の第三者がXになりすましてYから文字列を受け取ったとします。ところが、この者はあらかじめX、Y間で定めた規則を知らないので、(2)で新たな文字列を作成し、Yへ返送したとしても、(3)の段階でYは、返送された文字列が正しくないと認識します。返送されてきた文字列が正しければ、Xが正当な通信相手であることが証明されることになります。

基本情報 平成19年度春 問65 [出題頻度:★☆☆]

解答ーウ

別冊演習ドリル 1-60

3）利用者認証

利用者認証は、システムの正当な利用者であるか否かを確認することです。不正アクセスを防ぐためにも、システムの正当な利用者であるか否かを識別することは重要です。

①利用者 ID とパスワード

利用者認証の手段として一般的に用いられるのが、利用者 ID とパスワードです。

利用者 ID（ユーザ ID）はシステムにアクセスする利用者を識別するために使用し、**パスワード**は利用者認証に使われます。パスワードは本人のみが知っているので、正しく入力されれば、本人の認証になります。なお、パスワードはそのままの状態で登録しておくと、情報が漏れてしまった場合に二次災害のおそれがあるため、ハッシュ値に変換して登録しておき、第三者にわからないようにすることが肝要です。

パスワードは推測されやすいものは避ける必要があります。また退職や人事異動、担当業務の変更に伴って、システム管理者は各人の利用者 ID やパスワードを抹消、更新する必要があります。

なお、パスワードに使用する文字がM種類、パスワードの桁数をnとすると、M^n個のパスワードが設定可能であるため、システム管理者は利用者に一定以上の長さのパスワードを設定するように指導すべきです。

また、同じ利用者 ID を使用して一定時間内に一定回数以上ログインに失敗した場合には、パスワードを破るための総当り攻撃を受けていると判断して、その利用者 ID を無効にするロックアウトの設定をシステム管理者はしておくべきです。

例題

システム運用における利用者 ID とパスワードの管理に関する記述のうち，適切なものはどれか。

ア 希望者には利用者 ID を無条件で与え，パスワードを登録してもらう。
イ 定期的にパスワードを変更しなければ，ログインできない仕掛けを作る。
ウ パスワードは，辞書に載っている8文字以上の単語を使うように指導する。
エ 利用者が退職した場合でも，利用者 ID はそのまま残しておく。

利用者 ID とパスワードを設定する場合、パスワードは利用者本人が設定し、本人以外知り得ない状態にします。また、パスワードは他人に推測されにくいようなものを設定します。誕生日や電話番号などの他人が推測できるものは望ましくありません。

ア 希望者全てに無条件に利用者 ID を与えることは、不正アクセスにつながりやすく危険です。
ウ パスワードは、意味がある単語のような他人が想像可能なものは避け、全く無意味な文字列にするのが望ましいです。
エ 担当者が異動した場合や退職した場合には、速やかに利用者 ID を削除すべきです。

初級システムアドミニストレータ 平成15年度秋 問47 [出題頻度:★★☆]

解答ーイ

別冊演習ドリル 1-61～64

②アクセス管理

ファイルやデータベースなどのシステム資源を読み書きする権利を、アクセス権と呼びます。

アクセス管理は、セキュリティの観点から、経営者や管理者、システム担当者、一般利用者などの階層別にレベル分けしたり、営業部や人事部、製造部などの部署別にレベル分けして、利用者ごとにアクセス権を設定することです。不正なアクセスによるデータの改ざんや破壊を防止するためにも、アクセス管理は重要です。

例題

ファイル aaa は表のとおりにアクセス権が設定されている。ユーザBがファイル aaa をコピーしてファイル bbb を作成できるようにするとき，ファイル aaa へのアクセス権に関する記述のうち，適切なものはどれか。

ファイル所有者	アクセス権	
	ファイル所有者	ファイル所有者以外
ユーザA	R	ー

注記 アクセス権の意味
R:読込み可，W:書込み可，ー:読込み・書込みいずれも不可

ア アクセス権は変更しない。
イ “ファイル所有者以外”のアクセス権にR(読込み可)を追加する。
ウ “ファイル所有者以外”のアクセス権にW(書込み可)を追加する。
エ “ファイル所有者”のアクセス権にW(書込み可)を追加する。

ファイル所有者はユーザAなので、ユーザBは“ファイル所有者以外”ということになります。また、ファイルaaaをコピーするには、まず、読込む必要があります。したがって、ユーザBがファイルaaaをコピーするには、“ファイル所有者以外”のアクセス権にR(読込み可)を追加する必要があります。

ITパスポート 平成24年度春 問83 [出題頻度:★☆☆]

解答ーイ

別冊演習ドリル 1-65～67

③IC カード

IC カードは、情報を記録するための IC チップを組み込んだカードで、情報量が大きく、偽造や変造などの不正行為が困難です。利用者認証に使われるICカードには、利用者個人の秘密鍵と公開鍵証明書が厳重に保管されています。認証システムを利用する際には、自分の IC カードをシステムの IC カードリーダに挿入して、IC カードの暗証番号である**PIN コード**を入力します。これによって、利用者認証を行いICカード内の必要な情報を参照できるようになります。なお不正行為が困難であっても、IC カードを紛失した場合には速やかに失効手続きをする必要があります。

例題

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が識別できるので，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。
ウ PIN には，IC カードの表面に刻印してある数字情報を組み合わせたものを設定する。
エ PIN は，IC カードの配送には同封せず，別経路で利用者に知らせる。

ア 全利用者に共通な PIN が設定された場合、本人になりすまして不正に IC カードを利用される危険性が生じます。
イ IC カードが不正に利用される前に、まず紛失した IC カードの失効処理を行うべきです。
ウ IC カードの表面に刻印してある数字情報を総当たり方式で組み合わせることで、PIN を不正に取得することが可能になります。

情報セキュリティマネジメント 平成28年度秋 問1 [出題頻度:★☆☆]

解答ーエ

④ワンタイムパスワード

ワンタイムパスワードは、1度だけ使用可能なパスワードです。

パスワードを使い捨てにして、毎回異なるパスワードを使うワンタイムパスワードの仕組みを利用することで、パスワードの盗難を避けることができます。

なお、ワンタイムパスワードを表示するための機器に、**セキュリティトークン**があります。

例題

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。

ア シングルサインオンに関する記述です。
イ バイオメトリクス認証に関する記述です。
ウ マトリックス認証に関する記述です。

ITパスポート 平成25年度春 問58 [出題頻度:★☆☆]
解答ーエ

別冊演習ドリル 1-68

⑤多要素認証

利用者認証の手段は、本人しか知らない知識を認証の手段とする方法、本人しか所有していない物を認証の手段とする方法、本人の身体的特徴を認証の手段とする方法の3種類に分けられます。このうち、2種類以上を組み合わせることを**多要素認証**と呼び、認証の強度が高くなります。

例題

2要素認証に該当する組みはどれか。

ア クライアント証明書，ハードウェアトークン
イ 静脈認証，指紋認証
ウ パスワード認証，静脈認証
エ パスワード認証，秘密の質問の答え

利用者認証の手段は、パスワードなどの記憶(知識)による認証、IC カードなどの所有物による認証、指紋や虹彩などの身体的特徴による認証の3種類に分けられます。

2要素認証は、上記の3種類の認証手段のうち、2種類を組み合わせる方法です。

情報セキュリティマネジメント 平成29年度春 問18 [出題頻度:★★☆]
解答ーウ

別冊演習ドリル 1-69

⑥シングルサインオン

シングルサインオン（Single Sign-On）は、利用者が1回だけ認証を受けることで、許可されている複数の OS やアプリケーションを利用できるようにする方法です。

シングルサインオンを採用することで、利用者は複数の ID やパスワードを使い分ける必要がなくなり負担が軽減します。ただし、危険性も増大します。

なお、Web ブラウザを利用したシングルサインオンにおける利用者認証の仕組みとして、**クッキー**（**cookie**）を利用する方法があります。クッキーは、Web サイトを閲覧する際の足跡や入力した利用者名やパスワードなどの情報を、利用者のコンピュータに一時的に記録する仕組みです。

また、インターネットから受け取ったリクエストを Web サーバに中継する**リバースプロキシ**（Reverse proxy）に認証・許可の機能を持たせることでシングルサインオンを実現することもできます。この方法では利用者認証にパスワードの代わりにディジタル証明書を用いることもできます。

例題

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 スマートカード
ウ バイオメトリクス認証　　エ ワンタイムパスワード

イ スマートカードは、情報を記録するための IC チップを組み込んだ IC カードです。
ウ バイオメトリクス認証は、指紋、声紋、眼球の虹彩などの身体的特徴によって本人確認をする利用者認証方式です。
エ ワンタイムパスワードは、利用者認証に使われる1回だけの使い捨てのパスワードです。

ITパスワード　平成23年度秋　問85［出題頻度：★☆☆］

解答－ア

別冊演習ドリル　1-70、71

⑦CAPTCHA

CAPTCHA は、Web サイトなどにアクセスする場合などに、アクセス用のパスワードとしてサーバから送られてくるゆがんだ文字の画像です。CAPTCHA を用いると、プログラムによる自動アクセスが不可能なため、ボットによる被害を防ぐことができます。

例題

電子掲示板やブログに投稿するとき，図のようなゆがんだ文字の画像が表示され，それを読み取って入力するように求められることがある。その目的はどれか。

ア システムが想定する表示機能をブラウザがもっているかどうかを判断する。
イ 事前に投稿を許可された利用者であることを認証する。
ウ ディスプレイの表示機能に問題ないかを判別する。
エ プログラムによる自動投稿を防止する。

ゆがんだ文字などの画像データをサーバから送り、利用者にそれを読み取らせて入力させることによって認証する方法を、CAPTCHA 認証と呼びます。プログラムによる自動投稿を防止することで、ボットによる被害を防ぎます。

ITパスワード　平成22年度春　問75［出題頻度:★☆☆］
解答ーエ

別冊演習ドリル　1-72

⑧パスワードリマインダ

パスワードリマインダは、パスワードを忘れた利用者を救済するシステムです。利用者は、メールアドレスと特定の質問に対する回答を事前にシステムに登録して、パスワードを忘れた場合に特定の質問に対する回答をシステムに入力してパスワードの送付を受けます。なお、パスワードを再設定させるシステムもあります。

例題

Web システムのパスワードを忘れたときの利用者認証において合い言葉を使用する場合，合い言葉が一致した後の処理のうち，セキュリティ上最も適切なものはどれか。

ア あらかじめ登録された利用者のメールアドレス宛てに，現パスワードを送信する。
イ あらかじめ登録された利用者のメールアドレス宛てに，パスワード再登録用ページへアクセスするための，推測困難な URL を送信する。
ウ 新たにメールアドレスを入力させ，そのメールアドレス宛てに，現パスワードを送信する。
エ 新たにメールアドレスを入力させ，そのメールアドレス宛てに，パスワード再登録用ページへアクセスするための，推測困難な URL を送信する。

ア 現パスワードが盗聴されて、不正利用されるおそれがあります。
ウ、エ 正当な利用者になりすまして新たなメールアドレスを入力された場合に、パスワードが不正利用されるおそれがあります。

基本情報　平成28年度春　問40［出題頻度:★☆☆］
解答ーイ

4）生体認証技術

生体認証技術（**バイオメトリクス認証技術**）は、身体的特徴や行動的特徴によって本人確認する技術です。

①身体的特徴による認証

身体的特徴による認証技術には、次のような種類があります。

・掌の静脈パターンによる**静脈パターン認証**（掌認証）

・眼球の虹彩の模様による**虹彩認証**

・声の周波数の特徴である声紋による**声紋認証**

・顔の特徴による**顔認証**

・網膜のパターンによる**網膜認証**

なお、静脈パターン認証や網膜認証などは経年による変化が少ないため、認証に使用できる有効期間が他の方法に比べて長いです。

例題

バイオメトリクス認証に該当するものはどれか。

ア 顔写真を印刷した，IC チップ内蔵の ID カードの目視による認証
イ 個人ごとに異なるユーザ ID とパスワードによる認証
ウ てのひらを読取り機にかざすことによる認証
エ 人間には判別できるが機械的に判別できないような文字を正しく読み取ることができるかどうかによる認証

ア IC カードという所有物による認証です。
イ パスワードという知識による認証です
エ CAPTCHA という知識による認証です。

ITパスポート 平成25年度秋 問50 [出題頻度:★☆☆]
解答ーウ

別冊演習ドリル 1-73～75

②行動的特徴による認証

行動的特徴による代表的な認証技術に、署名認証があります。

署名認証は、署名の速度や筆圧などの行動的特徴によって本人確認をする技術です。

例題

バイオメトリクス認証には，身体的特徴を抽出して認証する方式と行動的特徴を抽出して認証する方式がある。行動的特徴を用いているものはどれか。

ア 血管の分岐点の分岐角度や分岐点間の長さから特徴を抽出して認証する。
イ 署名するときの速度や筆圧から特徴を抽出して認証する。
ウ 瞳孔から外側に向かって発生するカオス状のしわの特徴を抽出して認証する。
エ 隆線によって形作られる紋様からマニューシャと呼ばれる特徴点を抽出して認証する。

ア 静脈パターン認証（身体的特徴）に関する記述です。
ウ 虹彩認証（身体的特徴）に関する記述です。
エ 指紋認証（身体的特徴）に関する記述です。

基本情報 平成27年度春 問41 [出題頻度:★☆☆]
解答ーイ

③本人拒否率と他人受入率

生体認証技術では、あらかじめ登録されている身体的特徴や行動的特徴のデータと、認証時に入力されたデータを照合して類似度が高い場合に本人と判定します。そこで、システムの運用者は、あらかじめ登録されているデータと認証時に入力されたデータの類似度に基づくしきい値を設定する必要があります。ただし、入力されたデータは湿度や気温等環境条件により異なってくるため、登録されているデータと完全に一致することはありません。そのため、類似度に基づく規定値の設定は、誤って本人を拒否する確率(**本人拒否率**)と、誤って他人を受け入れる確率(**他人受入率**)を考慮する必要があります。なお一般的には、不正アクセスを防ぐために、本人拒否率を高く、他人受入率を低く設定します。

例題

生体認証システムを導入するときに考慮すべき点として，最も適切なものはどれか。

ア システムを誤動作させるデータを無害化する機能をもつライブラリを使用する。
イ パターンファイルの頻繁な更新だけでなく，ヒューリスティックスなど別の手段と組み合わせる。
ウ 本人のディジタル証明書を信頼できる第三者機関に発行してもらう。
エ 本人を誤って拒否する確率と他人を誤って許可する確率の双方を勘案して装置を調整する。

生体認証システムは、あらかじめ登録された身体的特徴や行動的特徴の情報と、認証時に入力される情報を照合して類似度が高い場合に本人と判定します。入力される情報は、湿度や気温等環境条件により変化するため、事前に登録された情報と完全に一致することはありません。そのため、類似度に基づく規定値として、誤って本人を拒否する確率(本人拒否率)と誤って他人を受け入れる確率(他人受入率)を考慮する必要があります。なお、本人拒否率を低くすると他人受入率は高くなり、利便性を重視した認証となります。また、他人受入率を低くすると本人拒否率は高くなり、安全性を重視した認証となります。

基本情報 平成26年度春 問45 [出題頻度:★☆☆]
解答ーエ

別冊演習ドリル 1-76

5)公開鍵基盤

PKI(Public Key Infrastructure:**公開鍵基盤**)とは、インターネットの利用者を、なりすましや盗聴、改ざんなどの危険から守るための仕組み全体のことです。具体的には、ディジタル証明書、ルート証明書、サーバ証明書、クライアント証明書、CRL などの認証技術と、これらを適正に運用する仕組みのことです。

例題

所有者と公開鍵の対応付けをするのに必要なポリシや技術の集合によって実現される基盤はどれか。

ア IPsec　　イ PKI
ウ ゼロ知識証明　　エ ハイブリッド暗号

ア IPsecは、暗号技術を用いてパケットの改ざんを防止するためのプロトコルです。
ウ ゼロ知識証明(ZKIP)とは、利用者認証において、パスワードなどの適正な利用者だけが知っている情報について、その情報自体を送受信することなく、自分がその情報を知っていることを相手に伝える方法です。
エ ハイブリッド暗号は、共通鍵暗号方式と公開鍵暗号方式の両者を組み合わせて、安全に共通鍵暗号方式の鍵情報を相手方に渡す方式のことです。

応用情報 平成24年度春 問36 [出題頻度:★☆☆]
解答ーイ

①GPKI

GPKI(Government Public Key Infrastructure:**政府認証基盤**)は、政府(総務省行政管理局)が運営するPKIで、各省庁が運営する認証局(官職認証局)と、官職認証局相互間及び、官職認証局と政府認証基盤外の民間認証局を相互認証する**BCA**(Bridge Certification Authority:**ブリッジ認証局**)から構築されています。

電子署名法は、GPKIを前提とするものです。

②ディジタル証明書

公開鍵暗号方式では、鍵情報を不特定多数に公開します。その際、鍵情報が本当の公開鍵であることを保証する必要があります。仮に保証がなければ、悪意の第三者が本人になりすまして偽の鍵情報を公開鍵とすることも可能です。したがって、公開鍵暗号方式を有効に利用するには、第三者機関により公開鍵が正当なものである証明が必要です。

ディジタル証明書(**公開鍵証明書**、電子証明書)は、公開鍵が正当なものであることの証明として第三者機関が自らの秘密鍵でディジタル署名した証明書です。

なお、ディジタル証明書の登録申請の受付、本人の確認、登録までを担当し、ディジタル証明書の発行依頼者の資格審査を行う機関を登録局(RA:Registration Authority)と呼びます。また、登録完了後、ディジタル証明書の発行を行う機関を**認証局**(**CA**:Certification Authority)と呼びます。ただし、認証局が登録局をかねている場合も多いです。認証局には、第三者機関としての対外的な取引を行うパブリック認証局と、特定の組織内などの閉じた環境のみで機能するプライベート認証局があります。

例題

二者間で商取引のメッセージを送受信するときに，送信者のディジタル証明書を使用して行えることはどれか。

ア　受信者が，受信した暗号文を送信者の公開鍵で復号することによって，送信者の購入しようとした商品名が間違いなく明記されていることを確認する。
イ　受信者が，受信した暗号文を送信者の公開鍵で復号することによって，メッセージの盗聴を検知する。
ウ　受信者が，受信したディジタル署名を検証することによって，メッセージがその送信者からのものであることを確認する。
エ　送信者が，メッセージに送信者のディジタル証明書を添付することによって，メッセージの盗聴を防止する。

ディジタル署名は、公開鍵暗号方式を応用した方法で、「送信者の秘密鍵で暗号化したデータは、送信者の公開鍵のみで復号できる」ということから、データの送り手を証明するものです。

ディジタル証明書は、公開鍵が正当なものであることの証明として第三者機関が自らの秘密鍵でディジタル署名した証明書です。送信者のディジタル証明書を使用することで、受信者はメッセージが正当な送り手からのものであることを証明する(送信者認証)と同時に、改ざんされていないことを証明する(メッセージ認証)ことができます。

情報セキュリティマネジメント　平成29年度春　問19［出題頻度:★★★］

解答ーウ

別冊演習ドリル　1-77～79

③ルート証明書

認証局は、発行するディジタル証明書の正当性を証明するために、自身の正当性を証明する必要があります。**ルート証明書**は、認証局の正当性を証明するために発行されるディジタル証明書です。具体的には、認証局は階層構造になっており、より上位の認証局の証明するディジタル証明書を用いて正当性を証明します。なお、最上位の認証局のディジタル証明書は、WWW ブラウザにあらかじめインストールされているので、階層構造にある認証局のディジタル証明書を利用者が普段意識することはありません。このとき、上位の認証局による認証を受けずに自らの正当性を自ら証明する認証局をルート認証局、ルート認証局からディジタル証明書の発行を受け認証される認証局を中間認証局と呼びます。ルート認証局は、信頼される第三者機関として、認証局運用規定を公開しています。

④サーバ証明書とクライアント証明書

サーバ証明書は Web サーバの正当性を保証する証明書です。具体的には、サーバの運営者名、証明書を発行した認証局名、サーバの公開鍵、証明書の有効期間、認証局のディジタル署名から構成されています。サーバ証明書を確認することで、認証済の安全なサイトか、身元の確認が取れない危険なサイトかを判断します。

一方、**クライアント証明書**は、Web サーバに接続するクライアント PC の正当性を保証する証明書です。具体的には、クライアント名、証明書を発行した認証局名、サーバの公開鍵、証明書の有効期間、認証局のディジタル署名から構成されています。クライアント証明書を利用することで、なりすましを防ぐことができます。

⑤CRL

CRL(Certificate Revocation List:**証明書失効リスト**)は、何らかの理由で有効期間中に失効したディジタル証明書のシリアル番号の一覧で、失効したディジタル証明書のシリアル番号と失効した日時が記載されています。ディジタル証明書と同様に認証局が管理しています。ディジタル証明書を受け取った場合、CRL と照合することで、現在でも有効か確認できます。

なお、CRL の代わりにインターネット上でディジタル証明書の失効状態を問い合わせるプロトコルに **OCSP**(Online Certificate Status Protocol)があります。

例題

何らかの理由で有効期間中に失効したディジタル証明書の一覧を示すデータはどれか。

ア CA　　イ CP　　ウ CPS　　エ CRL

ア CA は、公開鍵暗号方式で使用される公開鍵が正当なものであることの証明として、ディジタル証明書(公開鍵証明書)を発行する機関です。

イ CP(Certificate Policy:証明書ポリシ)は、CA が発行するディジタル証明書の記載事項や本人確認方法等を明記した文書です。

ウ CPS(Certification Practice Statement:認証業務規定)は、CA の運用規定を定めた文書です。

情報セキュリティマネジメント　平成29年度春　問25 [出題頻度:★★★]

解答ーエ

別冊演習ドリル　1-80～83