Chapter11

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

学習のポイント

✅ 機密性、完全性、可用性は重要用語！しっかり覚えよう！

### 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（エンティティは、情報セキュリティの文脈においては、情報を使用する組織及び人、情報を扱う設備、ソフトウェア及び物理的媒体などを意味します）。これは、「許可された者だけが許可された方法でのみ情報にアクセスできるようにする」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、「情報の利用者、利用する際のシステムや手順（プロセス）、また情報そのものが本物であること」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、「利用者が意図する結果を求めて動作を行うと、障害などによって結果が得られなかったり、正しくない結果が出ることなく、利用者が意図したとおりの結果が得られること」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  JIS Q 27000:2014（情報セキュリティマネジメントシステム－用語）において，“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”と定義されているものはどれか。  ア　真正性 イ　信頼性 ウ　責任追跡性 エ　否認防止  イ　信頼性は、JIS Q 27000において、“意図する行動と結果とが一貫しているという特性”と定義されています。  ウ　責任追跡性は、改訂された情報の履歴をたどることができるようにすることで、誰がいつ情報を更新したかが分かることを意味します。  エ　否認防止は、JIS Q 27000において、“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”と定義されています。  基本情報　平成30年度春　問39　[出題頻度：★★★]  解答－ア |

別冊演習ドリル 》 1-672～676

🏋プラスアルファ

**●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、各国における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**

全ての参加者は、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べきである。

**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。リスクアセスメントとは、セキュリティ上の脅威と脆弱性を識別し、リスクの許容でき  
　　るレベルの決定やリスクを管理するための措置の選択を支援するもの。

**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 | 例えば、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。そのため、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。そのため、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。

|  |
| --- |
| 例題　🏋プラスアルファ  サイバー攻撃の例ではないものはどれか。  ア　機密情報の取得を目的として，オフィスから廃棄された記録メディアをあさる。  [イ](https://www.itpassportsiken.com/kakomon/30_haru/q67.html#ans)サーバの脆弱性を利用して，Webサイトに侵入してデータを改ざんする。  [ウ](https://www.itpassportsiken.com/kakomon/30_haru/q67.html#ans)大量のアクセスを集中させて，サービスを停止させる。  [エ](https://www.itpassportsiken.com/kakomon/30_haru/q67.html#ans)バックドアを利用して，他人のPCを遠隔操作する。  サイバー攻撃は、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、破壊する行為です。  選択肢アは、通信ネットワークや他者のPCに侵入していないので、サイバー攻撃には該当しません。  ITパスポート　平成30年度春　問67　[出題頻度：★☆☆]  解答－ア |

## 3. 脅威

学習のポイント

✅ 全ての用語に出題の可能性あり！用語の意味を覚えよう！

脅威とは、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です。

### 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。

|  |
| --- |
| 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　パスワードクラック エ　踏み台攻撃  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　パスワードクラックは、辞書攻撃や総当たり攻撃などにより、他人のパスワードを解析し、探り当てる行為です。  エ　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。  基本情報　平成26年度春　問41　[出題頻度：★★☆]  解答－ア |

別冊演習ドリル 》 1-677

### 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。

|  |
| --- |
| 例題  マルウェアについて，トロイの木馬とワームを比較したとき，ワームの特徴はどれか。  ア　勝手にファイルを暗号化して正常に読めなくする。  イ　単独のプログラムとして不正な動作を行う。  ウ　特定の条件になるまで活動をせずに待機する。  エ　ネットワークやリムーバブルメディアを媒介として自ら感染を広げる。  ア　ランサムウェアに関する記述です。  イ　ワームはネットワークを介して感染を広げます。  ウ　コンピュータウイルスの潜伏機能に関する記述です。  基本情報　平成29年度秋　問41　[出題頻度：★★☆]  解答－エ |

別冊演習ドリル 》 1-678,679

#### 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や添付ファイルを開く操作は行わない、などの注意が必要です。

|  |
| --- |
| 例題  スパイウェアに該当するものはどれか。  ア　Webサイトへの不正な入力を排除するために，Webサイトの入力フォームの入力データから，HTMLタグ，JavaScript，SQL文などを検出し，それらを他の文字列に置き換えるプログラム  イ　サーバへの侵入口となり得る脆弱なポートを探すために，攻撃者のPCからサーバのTCPポートに順番にアクセスするプログラム  ウ　利用者の意図に反してPCにインストールされ，利用者の個人情報やアクセス履歴などの情報を収集するプログラム  エ　利用者のパスワードを調べるために，サーバにアクセスし，辞書に載っている単語を総当たりで試すプログラム  ア　サニタイジングに関する記述です。  イ　ポートスキャンに関する記述です。  エ　辞書攻撃に関する記述です。  基本情報　平成28年度春　問38　[出題頻度：★☆☆]  解答－ウ |

#### 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　コンピュータウイルスの一種ですが、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－エ |

#### 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 attack）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－イ |

#### ⑤ルートキット（rootkit）

ルートキットは、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。

#### 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  企業内ネットワークやサーバに侵入するために攻撃者が組み込むものはどれか。  ア　シンクライアントエージェント イ　ストリクトルーティング  ウ　ディジタルフォレンジックス エ　バックドア  ア　シンクライアントエージェントは、必要最低限の機能だけを備えたシンクライアントシステムで動作する自律的なソフトウェアです。  イ　ストリクトルーティングは、TCP/IPの経路選択において、途中の経路をすべて送信者が指定する方法です。  ウ　ディジタルフォレンジックスは、コンピュータ犯罪の被害に備えて、不正アクセスなどのコンピュータに関する犯罪の法的な証拠を明らかにするために、原因究明に必要な情報を収集して分析するための手段や技術です。  基本情報　平成26年度春　問43　[出題頻度：★☆☆]  解答－エ |

別冊演習ドリル 》 1-680,681

#### ⑦偽セキュリティ対策ソフト

偽セキュリティ対策ソフトは、セキュリティ機能を有しているように偽装したソフトウェアです。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、偽セキュリティ対策ソフトを購入させて、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。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。

|  |
| --- |
| 例題  不正アクセスなどに利用される，コンピュータシステムやネットワークに存在する弱点や欠陥のことを何というか。  ア　インシデント イ　セキュリティホール  ウ　ハッキング エ　フォレンジック  ア　インシデントは、システムの脆弱性によって脅威が誘発されて損失が発生している状態です。  ウ　ハッキングは、他人のコンピュータシステムに不正に侵入する行為です。  エ　フォレンジック（ディジタルフォレンジクス）は、コンピュータ犯罪の被害に備えて、不正アクセスなどのコンピュータに関する犯罪の法的な証拠を明らかにするために、原因究明に必要な情報を収集して分析するための手段や技術です。  ITパスポート　平成26年度秋　問58　[出題頻度：★☆☆]  解答－イ |

## 5. 不正のメカニズム　🏋プラスアルファ

学習のポイント

✅ 出題頻度を参考に効率よく学習しよう！

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　🏋プラスアルファ  “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－ア |

別冊演習ドリル 》 1-682

## 6. 攻撃者の種類、攻撃の動機　🏋プラスアルファ

学習のポイント

✅ 出題頻度を参考に効率よく学習しよう！

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　🏋プラスアルファ  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－イ |

## 7. 攻撃手法

学習のポイント

✅ 全ての用語に出題の可能性あり！用語の意味を覚えよう！

システムの脆弱性を悪用する攻撃手法にはさまざま種類があります。

### 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り攻撃、辞書攻撃、レインボー攻撃があります。

**総当たり攻撃**（**ブルートフォース**）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。

#### 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。

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、パスワードをランダムな文字列で作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、データ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－ア |

別冊演習ドリル 》 1-683～688

### 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）にある個人情報など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リンクやボタンを配置し、悪意のあるWebサイトに誘導したり、意図に反した操作を実行させたりする攻撃手法です。

#### 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**（Search Engine Optimization）とは、Webサイトの検索サイトなどで、検索サイトの順位付けのアルゴリズムを解析し、対象のWebサイトを検索上位に表示されるようにする技術や手法の総称です。SEOポイズニングは、このSEO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  SQLインジェクション攻撃の説明はどれか。  ア　Webアプリケーションに問題があるとき，悪意のある問合せや操作を行う命令文をWebサイトに入力して，データベースのデータを不正に取得したり改ざんしたりする攻撃  イ　悪意のあるスクリプトを埋め込んだWebページを訪問者に閲覧させて，別のWebサイトで，その訪問者が意図しない操作を行わせる攻撃  ウ　市販されているDBMSの脆弱性を利用することによって，宿主となるデータベーサーバを探して自己伝染を繰り返し，インターネットのトラフィックを急増させる攻撃  エ　訪問者の入力データをそのまま画面に表示するWebサイトに対して，悪意のあるスクリプトを埋め込んだ入力データを送ることによって，訪問者のブラウザで実行させる攻撃  イ　クロスサイトリクエストフォージェリに関する記述です。  ウ　ワームに関する記述です。  エ　クロスサイトスクリプティングに関する記述です。  基本情報　平成29年度秋　問39　[出題頻度：★★★]  解答－ア |

別冊演習ドリル 》 1-689～693

### 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、当事者にな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ドメイン名ハイジャック

ドメイン名ハイジャックは、何らかの方法でドメイン名を乗っ取り、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。誘導する手段の一つにDNSキャッシュポイズニングがあります。

#### ⑥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。

#### ⑦リプレイ攻撃

リプレイ攻撃は、正当な利用者による、パスワードの入力などのログインするための一連の手続きを盗聴して記録し、それを用いて、利用者になりすまして不正アクセスする攻撃手法です。

|  |
| --- |
| 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。  基本情報　平成29年度秋　問37　[出題頻度：★★☆]  解答－イ |

別冊演習ドリル 》 1-694～697

### 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（Denial of Service attack）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。

#### ②EDoS（Economic DoS）攻撃

EDoS攻撃は、クラウドサービスなど、利用量に応じて料金を支払う（従量課金制）サービスの契約者である攻撃目標に対して、外部から当該サービスに関する不要なリクエストを大量に送信することで、経済的な損失を与えることを目的としたDoS攻撃です。

#### ③DDoS（Distributed DoS）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。

#### ④メールボム

メールボムは、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  従量課金制のクラウドサービスにおけるEDoS(Economic Denial of Service，又はEconomic Denial of Sustainability)攻撃の説明はどれか。  ア　カード情報の取得を目的に，金融機関が利用しているクラウドサービスに侵入する攻撃  イ　課金回避を目的に，同じハードウェア上に構築された別の仮想マシンに侵入し，課金機能を利用不可にする攻撃  ウ クラウドサービス利用者の経済的な損失を目的に，リソースを大量消費させる攻撃  エ　パスワード解析を目的に，クラウドサービス環境のリソースを悪用する攻撃  DoS（Denial of Service）攻撃は、攻撃目標のサーバに大量のデータを送信し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行為で、EDoS（Economic DoS）攻撃は、これを応用し、クラウドサービスを利用する企業の経済的な損失を目的に、リソースを大量消費させる攻撃です。  情報セキュリティマネジメント　平成30年度秋　問23　[出題頻度：★☆☆]  解答－ウ |

### 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（Advanced Persistent Threats：持続的標的型攻撃）

APT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（Watering Hole Attack）

水飲み場型攻撃は、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　攻撃者がDoS攻撃及びDDoS攻撃を繰り返し，長期間にわたり特定組織の業務を妨害すること  イ　攻撃者が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こと  ウ　攻撃者が特定の目的をもち，標的となる組織の防御策に応じて複数の攻撃手法を組み合わせ，気付かれないよう執拗に攻撃を繰り返すこと  エ　攻撃者が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こと  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30年度秋　問21　[出題頻度：★☆☆]  解答－ウ |

別冊演習ドリル 》 1-698

### 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、ソフトウェアやハードウェアに内在するセキュリティ上の欠陥（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、エクスプロイト（脆弱性を標的とするスクリプトやプログラムなどの攻撃ツール）を使いセキュリティホールに対して行われる攻撃手法で、ゼロデイ・エクスプロイト攻撃とも呼ばれます。

#### 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**テンペスト攻撃**（電磁波解析攻撃）と呼ぶこともあります。

|  |
| --- |
| 例題  手順に示すセキュリティ攻撃はどれか。  〔手順〕  (1)　攻撃者が金融機関の偽のWebサイトを用意する。  (2)　金融機関の社員を装って，偽のWebサイトへ誘導するURLを本文中に含めた電子メールを送信する。  (3)　電子メールの受信者が，その電子メールを信用して本文中のURLをクリックすると，偽のWebサイトに誘導される。  (4)　偽のWebサイトと気付かずに認証情報を入力すると，その情報が攻撃者に渡る。  ア　DDoS攻撃 イ　フィッシング ウ　ボット エ　メールヘッダインジェクション  フィッシングは、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です。  ア　DDoS攻撃は、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行為です。  ウ　ボット（bot）は、ネットワーク（インターネット）を通じて、感染したコンピュータを外部から操ることを目的に作成されたマルウェアです。  エ　メールヘッダインジェクションは、第三者のWebサイトの問合せ用電子メール送信フォームなどに特殊なコードを入力することで、送信メール内容や宛先を改ざんし、迷惑メール送信などに悪用する行為です。  基本情報　平成25年度春　問38　[出題頻度：★★★]  解答－イ |

別冊演習ドリル 》 1-699～701

### ７）攻撃の準備

攻撃者は次のような方法で事前に攻撃対象の情報を収集します。

#### ①ポートスキャン

ポートスキャンは、攻撃者がアクセス可能なサービス（ポート番号）があるか外部から調査する行為で、検査対象の通信ポートに信号を送るツールをポートスキャナと呼びます。

#### ②フットプリンティング

フットプリンティングは、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です。

|  |
| --- |
| 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　後処理の段階において，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。  イ　権限取得の段階において，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　事前調査の段階において，攻撃できそうなサービスがあるかどうかを調査する。  エ　不正実行の段階において，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。  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（サービス）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を事前に調査する場合に行います。  基本情報　平成30年度春　問37　[出題頻度：★☆☆]  解答－ウ |

別冊演習ドリル 》 1-702

## 8. 情報セキュリティに関する技術

学習のポイント

✅ 重要項目！暗号化方式（共通鍵暗号方式・公開鍵暗号方式）をはじめ、登場する用語をしっかり覚えよう！

### 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。

来月転居する予定です。

Nd359fxj47ac･･･

Nd359fxj47ac･･･

来月転居する予定です。

送信者

受信者

Nd359fxj47ac･･･

※仮に第三者にデータを盗まれても、変換ルールを知らなければ元に戻せない。（盗聴することができない）

🏋プラスアルファ

**●CRYPTREC**（クリプトレック）**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、電子政府における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-256など（P344～345,347参照）がリストに掲載されています。

|  |
| --- |
| 例題　🏋プラスアルファ  CRYPTRECの活動内容はどれか。  ア　暗号技術の安全性，実装性及び利用実績の評価・検討を行う。  イ　情報セキュリティ政策に係る基本戦略の立案，官民における統一的，横断的な情報セキュリティ対策の推進に係る企画などを行う。  ウ　組織の情報セキュリティマネジメントシステムについて評価し認証する制度を運用する。  エ　認証機関から貸与された暗号モジュール試験報告書作成支援ツールを用いて暗号モジュールの安全性についての評価試験を行う。  イ　内閣官房情報セキュリティセンターに関する記述です。  ウ　情報マネジメントシステム推進センタに関する記述です。  エ　JCMVP（Japan Cryptographic Module Validation Program）に関する記述です。  情報セキュリティスペシャリスト　平成28年度秋Ⅱ　問8　[出題頻度：★☆☆]  解答－ア |

別冊演習ドリル 》 1-703

#### ①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－イ |

#### ②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は、**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。





**復号**

**暗号化**

平文

平文

暗号文



**受信者**

**送信者**

**同じ鍵を利用**

C:\Users\情報処理講座本部\AppData\Local\Microsoft\Windows\INetCache\Content.Word\AdobeStock_52324192_01.png

**Point**

共通鍵暗号方式

|  |
| --- |
| 例題  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  イ　PKI（公開鍵基盤）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を守るための仕組み全体のことです。  ウ　RSAは公開鍵暗号方式の一つで、桁数の多い数の素因数分解が困難であることを利用しています。公開鍵暗号方式では、暗号化と復号のための鍵は同じではなく、内容を秘匿する場合、復号のための鍵は公開しません。  エ　SHA-256は、改ざんの検知や、なりすましの防止に利用されるハッシュ値を導くハッシュ関数に採用されているアルゴリズムで、264以下の長さのデータから256ビットのハッシュ値を生成します。  基本情報　平成27年度春　問39　[出題頻度：★★☆]  解答－ア |

別冊演習ドリル 》 1-704,705

#### ③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**や、RSAに比べて、短い鍵長で同レベルの安全性が実現できることでTLS（P401参照）にも採用されている暗号化アルゴリズムである**楕円曲線暗号**があります。





**復号**

**暗号化**

平文

平文

暗号文



**受信者**

**送信者**

**受信者の秘密鍵**

**受信者の公開鍵**

C:\Users\情報処理講座本部\AppData\Local\Microsoft\Windows\INetCache\Content.Word\AdobeStock_52324192_01.pngC:\Users\情報処理講座本部\AppData\Local\Microsoft\Windows\INetCache\Content.Word\AdobeStock_52324192_01.png

**Point**

**Point**

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。  “来月転居する予定です。”  “nd359fxj47ac…”  鍵Ｋによって暗号化  Ａさん  “nd359fxj47ac…”  “来月転居する予定です。”  Bさんの秘密鍵  によって復号  Ｂさん  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  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う方式です。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。  基本情報　平成27年度春　問40　[出題頻度：★★★]  解答－ウ |

別冊演習ドリル 》 1-706～712

#### ④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は後述するS/MIME（P348参照）やSSL/TLS（P401参照）があります。

データ

送信者と受信者

の共通鍵

送信者

(暗)データ

(暗)送信者と受信者

の共通鍵

受信者の公開鍵

(暗)送信者と受信者

の共通鍵

(暗)データ

受信者の秘密鍵

送信者と受信者

の共通鍵

データ

受信者

①暗号化

②暗号化

③送信

④受信

⑤復号

⑥復号

※ (暗)は暗号化されたデータを表す

ハイブリッド暗号方式

|  |
| --- |
| 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化方式で復号し，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－エ |

別冊演習ドリル 》 1-713,714

#### ⑤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  ワームの検知方式の一つとして，検査対象のファイルからSHA-256を使ってハッシュ値を求め，既知のワーム検体ファイルのハッシユ値のデータベースと照合することによって，検知できるものはどれか。  ア　ワーム検体と同一のワーム  イ　ワーム検体と特徴あるコード列が同じワーム  ウ　ワーム検体とファイルサイズが同じワーム  エ　ワーム検体の亜種に当たるワーム  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。そのため、既知のワーム検体ファイルのハッシュ値のデータベースと照合することによって、ワーム検体と同一のワームを検知できます。  基本情報　平成27年度秋　問43　[出題頻度：★★☆]  　解答－ア |

別冊演習ドリル 》 1-715,716

#### ⑥S/MIME（Secure MIME）

S/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を使っ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、メッセージ本文の暗号化に共通鍵暗号方式を用い、共通鍵の受渡しには公開鍵暗号方式を用いるので、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  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  S/MIMEは、MIMEに共通鍵暗号方式、公開鍵暗号方式、ハッシュ関数を組み合わせて暗号化機能を加えたプロトコルです。S/MIMEを使うことで送信者のなりすまし、メールの盗聴、改ざんを防ぐことができます。  基本情報　平成20年度春　問67　[出題頻度：★☆☆]  解答－イ |

別冊演習ドリル 》 1-717,718

🏋プラスアルファ

**●PGP（**Pretty Good Privacy）

S/MIMEと同様に、メッセージ本文の暗号化に共通鍵暗号方式を用い、共通鍵の受渡しには公開鍵暗号方式を用いる暗号方式ですが、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。

**●危殆化**（きたいか）

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　プラスアルファ  暗号アルゴリズムの危殆化を説明したものはどれか。  ア　外国の輸出規制によって，十分な強度をもつ暗号アルゴリズムを実装した製品が利用できなくなること  イ　鍵の不適切な管理によって，鍵が漏えいする危険性が増すこと  ウ　計算能力の向上などによって，鍵の推定が可能になり，暗号の安全性が低下すること  エ　最高性能のコンピュータを用い，膨大な時間とコストを掛けて暗号強度をより確実なものにすること  危殆化とは、セキュリティ上の安全が脅かされ得る状態になることです。コンピュータの計算能力の向上などにより、暗号化アルゴリズムのうちいくつかは安全性が低下しつつあります。  情報セキュリティマネジメント　平成30年度春　問26　[出題頻度：★☆☆]  解答－ウ |

別冊演習ドリル 》 1-719

### 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。



平文

平文

**受信者**

**送信者**

「平文」と

「暗号化したダイジェスト」を

セットで送信



**ダイジェスト作成**

**ダイジェスト作成**

**ダイジェスト**



**ダイジェスト**

暗号文

**暗号化**

**復号**

**ダイジェスト**



C:\Users\情報処理講座本部\AppData\Local\Microsoft\Windows\INetCache\Content.Word\AdobeStock_52324192_01.png

**一致すれば・・・**

**・本人確認**

**・情報の改ざんなし**

**Point**

**Point**

**送信者の公開鍵**

**送信者の秘密鍵**

C:\Users\情報処理講座本部\AppData\Local\Microsoft\Windows\INetCache\Content.Word\AdobeStock_52324192_01.png

ディジタル署名

**●登録時**

利用者



認証局



②発行依頼

③審査

④認証局の秘密鍵で

暗号化（ディジタル署名）

⑤発行



⑥公開

①公開鍵作成

**●利用時**



①受信者の

公開鍵入手



②認証局の

公開鍵で復号

③認証局の公開鍵で復号できた

→認証局の秘密鍵で暗号化した

→この鍵は認証局が認めた鍵

→間違いなく受信者の公開鍵

送信者

|  |
| --- |
| 例題  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  ディジタル署名は、公開鍵暗号方式を応用した方法で、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。  基本情報　平成22年度春　問40　[出題頻度：★★★]  解答－ウ |

別冊演習ドリル 》 1-720～724

🏋プラスアルファ

**●タイムスタンプ（時刻認証）**

タイムスタンプは、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　🏋プラスアルファ  手順に示す処理を行ったとき，検証できることはどれか。  〔手順〕  (1) 送信者Ａはファイルのハッシュ値を計算して，信頼できる第三者機関に送信する。  (2) 第三者機関は，信頼できる日時を保持しており，受信したハッシュ値とその受信日時を結合し（結合データ），そのディジタル署名を生成し，ディジタル署名と結合データの組（ディジタル署名済みの結合データ）を送信者Ａに返信する。  (3) 送信者Ａはファイルと第三者機関から送られてきたディジタル署名済みの結合データを受信者Ｂに送信する。  (4) 受信者Ｂは第三者機関のディジタル署名を確認し，ファイルから計算したハッシュ値と，ディジタル署名済みの結合データから取り出されたハッシュ値を照合する。そして，結合データから取り出された日時を確認する。  ア　当該日時に受信者Ｂにファイルが到達したこと  イ　当該日時に送信者Ａが受信者Ｂにファイルを送信したこと  ウ　当該日時にファイルが作成されたこと  エ　当該日時にファイルが存在し，それ以降改ざんされていないこと  この問題はタイプスタンプ付与の手順を示しています。  ファイルから計算したハッシュ値と、ディジタル署名済みの結合データから取り出されたハッシュ値が一致すれば、受信日時にファイルが存在していたことと、ファイルは改ざんされていないことが証明されます。  応用情報　平成27年度 秋　問37　[出題頻度：★☆☆]  解答－エ |

別冊演習ドリル 》 1-725

#### ②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 |

#### ③メッセージ認証符号（MAC：Message Authentication Code）

メッセージ認証符号は、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。

**🕮 さらに詳しく**

**●メッセージダイジェスト**

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。

異なるデータが同じハッシュ値になることはほとんどありません。（一方向性関数）

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  メッセージ認証符号の利用目的に該当するものはどれか。  ア　メッセージが改ざんされていないことを確認する。  イ　メッセージの暗号化方式を確認する。  ウ　メッセージの概要を確認する。  エ　メッセージの秘匿性を確保する。  受信者は、送信者から受け取ったメッセージ（データ）から作成したメッセージダイジェストと、送信者から受け取ったメッセージダイジェストが一致すれば、メッセージが改ざんされていないことを確認できます。  基本情報　令和4年度サンプル　問32　[出題頻度：★☆☆]  解答－ア |

別冊演習ドリル 》 1-726

#### ④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。

クライアント

サーバ

①チャレンジ生成

②チャレンジ送信

④レスポンス送信

③送信されてきたチャレンジと利用者のパスワードを使ってレスポンス生成

⑤送信したチャレンジと登録されている利用者のパスワードを使ってレスポンスを生成し、④で受信したレスポンスと照合

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－ウ |

別冊演習ドリル 》 1-727

🏋プラスアルファ

**●リスクベース認証**

リスクベース認証は、利用者のIPアドレスなどの環境を分析し、いつもと異なるネットワークからのアクセスに対して追加の認証を行うことで、不正アクセスに対抗して安全性を高める認証技術です。例えば、普段はPCでサービスを利用している契約者が、同じID、パスワードを用いてスマートフォンでサービスにアクセスした際、本人でない恐れがあるため、サービス企業から契約者が登録した電子メールに一時的なパスワードを送り、これをスマートフォン側で入力することで、本人であることを認証します。

|  |
| --- |
| 例題　プラスアルファ  リスクベース認証の特徴はどれか。  ア　いかなる環境からの認証の要求においても認証方法を変更せずに，同一の手順によって普段どおりにシステムが利用できる。  [イ](https://www.ap-siken.com/kakomon/31_haru/q37.html#ans)　ハードウェアトークンとパスワードを併用させるなど，認証要求元の環境によらず常に二つの認証方式を併用することによって，安全性を高める。  ウ　普段と異なる環境からのアクセスと判断した場合，追加の本人認証をすることによって，不正アクセスに対抗し安全性を高める。  エ　利用者が認証情報を忘れ，かつ，Webブラウザに保存しているパスワード情報も使用できない場合でも，救済することによって，利用者は普段どおりにシステムを利用できる。  ア　統合サーバ認証に関する記述です。  イ　２要素認証に関する記述です。  エ　パスワードリマインダに関する記述です。  応用情報　平成31年度春　問37　[出題頻度：★☆☆]  解答－ウ |

別冊演習ドリル 》 1-728

### 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恐れがあるため、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、Ｍｎ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を使用して一定期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  利用者IDとパスワードの適切な運用管理方法はどれか。  ア　管理作業を簡素化するために，現在使用されていない利用者IDとパスワードを再利用する。  イ　トラブル処理を迅速化するために，利用者IDとパスワードの一覧表を作成し，管理者が保管する。  ウ　パスワードを他人に悪用されるのを防止するために，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。  エ　利便性を向上させるために，利用者登録申請書が届く前に，人事異動速報を見て新任者の利用者IDと仮のパスワードを登録する。  ア　使用しなくなったIDやパスワードは利用を停止し、再利用しないことが望ましいです。  イ　パスワードの一覧表を作成していた場合、万が一その一覧表が流出すると、多くの人のパスワードが一度に流出することになり、被害が大きくなる危険性があります。  エ　新任者に配布するIDに過不足が生じたり、誤ったアクセス権を設定してしまったりする危険があるため、正しい手順を踏んで登録すべきです。  基本情報　平成17年度秋　問66　[出題頻度：★★☆]  解答－ウ |

別冊演習ドリル 》 1-729～732

#### ②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、パスワードの盗難による不正アクセスを避けることができます。

携帯用パソコンを用いて外部からアクセスする場合には、盗難や紛失を考えて、認証にワンタイムパスワードを使用することが有効です。

なお、ワンタイムパスワードは、利用者が毎回直接変更して憶えておくことは難しいため、専用のソフトウェアやハードウェアを使って自動生成することが一般的です。ワンタイムパスワードを表示するためのハードウェアの一種に**セキュリティトークン**があります。

#### ③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。一般的な方式では、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おき、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することで、パスワードを再設定するサイトへのURLをあらかじめ設定しておいたメールアドレスに送付してもらい、再設定を行います。

|  |
| --- |
| 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ヘ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ヘ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－イ |

#### ④IC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。  基本情報　平成28年度秋　問40　[出題頻度：★☆☆]  解答－エ |

#### ⑤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、危険性は増大します。

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）（P405参照）に認証・許可の機能をも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として、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パスポート　平成23年度秋　問85　[出題頻度：★☆☆]  解答－ア |

#### ⑥CAPTCHA

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困難なため、ボットによる被害を抑止することができます。



CAPTCHAの例

|  |
| --- |
| 例題  CAPTCHAの目的はどれか。  ア　Webサイトなどにおいて，コンピュータではなく人間がアクセスしていることを確認する。  イ　公開鍵暗号と共通鍵暗号を組み合わせて，メッセージを効率よく暗号化する。  ウ　通信回線を流れるパケットをキャプチャして，パケットの内容の表示や解析，集計を行う。  エ　電子政府推奨暗号の安全性を評価し，暗号技術の適切な実装法，運用法を調査，検討する。  イ　ハイブリッド暗号に関する記述です。  ウ　パケットキャプチャに関する記述です。  エ　CRYPTRECに関する記述です。  基本情報　平成31年度春　問36　[出題頻度：★☆☆]  解答－ア |

別冊演習ドリル 》 1-733

#### ⑦マトリクス認証

マトリクス認証は、認証ごとにランダムに生成されるマトリクス表と利用者の記憶している位置・順序情報をもとにパスワードを生成する方法です。

①

②

③

④

①

②

③

④

初回登録時、①～④の位置をパスワードに使用

パスワード 4397

次回認証時、①～④の位置にある値を

パスワードに使用

パスワード 3510



マトリクス認証の例

|  |
| --- |
| 例題  システムの利用者を認証するための方式に関する記述のうち，適切なものはどれか。  ア　一度しか使えないパスワードを用いて認証する方式を，シングルサインオンという。  [イ](https://www.itpassportsiken.com/kakomon/30_aki/q69.html#ans)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方式を，ワンタイムパスワードという。  [ウ](https://www.itpassportsiken.com/kakomon/30_aki/q69.html#ans)　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などをパスワードとして入力する方式を，マトリクス認証という。  [エ](https://www.itpassportsiken.com/kakomon/30_aki/q69.html#ans)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方式を，チャレンジレスポンス認証という。  ア　ワンタイムパスワードの説明です。  イ　シングルサインオンの説明です。  エ　バイオメトリクス認証の説明です。  ITパスポート　平成30年度秋　問69　[出題頻度：★☆☆]  解答－ウ |

#### ⑧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。特に２種類の組合せで認証するものを、**２要素認証**と呼ぶ場合もあります。

|  |
| --- |
| 例題  ２要素認証に該当するものはどれか。  ア　２本の指の指紋で認証する。  イ　虹彩とパスワードで認証する。  ウ　異なる２種類の特殊文字を混ぜたパスワードで認証する。  エ　異なる二つのパスワードで認証する。  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。  基本情報　平成27年度秋　問45　[出題頻度：★☆☆]  解答－イ |

別冊演習ドリル 》 1-734

#### ⑨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・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  ある会社では，技術部，開発部，検査部のそれぞれのパソコンをLANで接続し，各部のデータベースにアクセス制御設定を行った。次の設定にしたとき，Ａ，Ｂ，Ｃはどの部に該当するか。  〔アクセス制御設定〕  (1)　各部の社員には，自分の所属する部のデータベースの読み書きを許可する。  (2)　技術部のデータベースは，開発部の社員に読出しを許可する。  (3)　検査部のデータベースは，技術部と開発部の社員に読出しを許可する。   |  |  |  |  | | --- | --- | --- | --- | | データベース | Ａ部 | Ｂ部 | Ｃ部 | | データベース１ | 読み書き可能 | 読出しだけ可能 | 読出しだけ可能 | | データベース２ | アクセス不可 | 読み書き可能 | アクセス不可 | | データベース３ | アクセス不可 | 読出しだけ可能 | 読み書き可能 |  |  |  |  |  | | --- | --- | --- | --- | |  | Ａ部 | Ｂ部 | Ｃ部 | | ア | 開発部 | 技術部 | 検査部 | | イ | 開発部 | 検査部 | 技術部 | | ウ | 検査部 | 開発部 | 技術部 | | エ | 検査部 | 技術部 | 開発部 |   開発部は、(2)と(3)により自分以外の２つのデータベースを読み出す事ができます。したがって該当するのはＢ部です。技術部は、(3)により検査部のデータベースは読み出す事ができます。したがって該当するのはＣ部です。検査部は、問題文中に指定がないので、自分のデータベース以外はアクセスできないと考えます。したがってＡ部です。  基本情報　平成14年度春　問33　[出題頻度：★★★]  解答－ウ |

別冊演習ドリル 》 1-735～737

### ４）生体認証技術

生体認証技術は、**バイオメトリクス認証技術**とも呼ばれ、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。

・指紋の隆線によって形作られる紋様による**指紋認証**

・掌（てのひら）の血管（静脈）の特徴（角度や長さなど）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**

・眼球の網膜の毛細血管の特徴による**網膜認証**

・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**

なお、静脈パターン認証や眼球による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  認証デバイスに関する記述のうち，適切なものはどれか。  ア　IEEE 802.1Xでは，ディジタル証明書や利用者ID，パスワードを格納するUSBキーは，200kバイト以上のメモリを内蔵することを規定している。  イ　安定した大容量の電力を必要とする高度な処理には，接触型ICカードよりも非接触型ICカードの方が適している。  ウ　虹彩認証では，成人には虹彩の経年変化がないので，認証デバイスでのパターン更新がほとんど不要である。  エ　静電容量方式の指紋認証デバイスでは，LED照明を設置した室内において正常に認証できなくなる可能性がある。  アIEEE802.1Xは、LANスイッチや無線LANアクセスポイントからLANを利用可能にする前に利用者を認証するための規格です。ディジタル証明書や利用者ID、パスワードを格納するUSBキーの内蔵メモリに関する規定はありません。  イ　安定した大容量の電力を必要とする高度な処理には、非接触型ICカードよりも接触型ICカードの方が適しています。  エ　静電容量方式の指紋認証デバイスは、指の凹凸に応じてたまるとセンサの間の電荷の量をもとに認証する非光学式の認証装置です。  基本情報　平成23年度春　問43　[出題頻度：★☆☆]  解答－ウ |

#### 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－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マッチング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など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、類似度に基づくしきい値の設定は、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　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。  [イ](https://www.fe-siken.com/kakomon/30_haru/q45.html#ans)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。  [ウ](https://www.fe-siken.com/kakomon/30_haru/q45.html#ans)マルウェア定義ファイルの更新が頻繁な製品を利用することによって，本人を誤って拒否する確率の低下を防ぐ。  [エ](https://www.fe-siken.com/kakomon/30_haru/q45.html#ans)容易に推測できないような知識量と本人が覚えられる知識量とのバランスが，認証に必要な知識量の設定として重要となる。  生体認証では、あらかじめ登録された特徴情報と、認証時に入力される情報をマッチング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、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、類似度に基づくしきい値として、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）を考慮しなければなりません。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が高くなり、安全性を重視した認証となります。  基本情報　平成30年度春　問45　[出題頻度：★★☆]  解答－イ |

別冊演習ドリル 》 1-738

### ５）PKI（Public Key Infrastructure：公開鍵基盤）

PKI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を守るための仕組み全体のことです。

具体的には、公開鍵暗号方式、ディジタル署名、登録局、認証局、ディジタル証明書、CRL、検証局などの認証技術と、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－イ |

🏋プラスアルファ

**●GPKI（Government Public Key Infrastructure：政府認証基盤）**

GPKI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。

#### ①ディジタル証明書（公開鍵証明書、電子証明書）

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限られ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](https://www.sg-siken.com/kakomon/29_haru/q19.html#ans)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信者からのものであることを確認する（送信者認証）と同時に、改ざんされていないことを確認する（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－ウ |

別冊演習ドリル 》 1-739,740

🏋プラスアルファ

**●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、認証局運用規定を公開して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。

|  |
| --- |
| 例題　プラスアルファ  ディジタル証明書に関する記述のうち，適切なものはどれか。  ア　S/MIMEやTLSで利用するディジタル証明書の規格は，ITU-T X.400で規定されている。  イ　ディジタル証明書は，SSL/TLSプロトコルにおいて通信データの暗号化のための鍵交換や通信相手の認証に利用されている。  ウ　認証局が発行するディジタル証明書は，申請者の秘密鍵に対して認証局がディジタル署名をしたものである。  エ　ルート認証局は，下位の認証局の公開鍵にルート認証局の公開鍵でディジタル署名したディジタル証明書を発行する。  ア　ITU-T X.400は電子メールについての標準を定めた規定です。  ウ　認証局が発行するディジタル証明書は、申請者の公開鍵に対して認証局がディジタル署名したものです。  エ　すべての認証局は、秘密鍵でディジタル署名したディジタル証明書を発行します。  情報セキュリティスペシャリスト　平成26年度秋Ⅱ　問4　[出題頻度：★☆☆]  解答－イ |

別冊演習ドリル 》 1-741

#### ②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。

#### ③CRL（Certificate Revocation List：証明書失効リスト）

CRLは、期限切れや紛失により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  セキュリティ対策で利用するCRLに記載されるデータはどれか。  ア　スパムメールの発信元及びメールの不正中継を行うドメインの名前  イ　ディジタル証明書の有効期間内に認証局の廃止などによって失効した自己署名証明書及び相互認証証明書  ウ　有効期間内に失効したディジタル証明書のシリアル番号  エ　利用者に対して与えられた情報資源へのアクセス権限リスト  ア　非営利組織「ORDB.org」がブラックリストとして2006年12月まで情報を提供していました。  イ　ARL（Authority Revocation List：認証機関失効リスト）に関する記述です。  エ　ACL（Access Control List：アクセス制御リスト）に関する記述です。  応用情報　平成22年度秋　問38　[出題頻度：★☆☆]  解答－ウ |

別冊演習ドリル 》 1-742～744

# 2. 情報セキュリティ管理

## 1. 情報セキュリティ管理

学習のポイント

✅ 出題頻度を参考に効率よく学習しよう！

組織の情報セキュリティ対策を包括的かつ継続的に実施するために、情報セキュリティ管理は重要です。

### １）情報セキュリティポリシに基づく情報の管理

情報セキュリティポリシは組織の情報セキュリティに対する姿勢を明文化したもので、組織は情報セキュリティポリシに基づき情報の管理を行う必要があります。

対象となる情報は、組織が活動するに当たり入手及び知り得た情報、並びに組織が活動する上で保有する全ての情報です。

🏋プラスアルファ

**●情報資産**

情報のうち、組織にとって価値のあるものを情報資産と呼びます。具体的には、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、保存情報などが例として挙げられます。

**●情報資産に関連付けた資産**

JIS Q 27002:2006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挙げています。

**①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

**②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など

**③人的資産**

保有する資格、技能、経験

**④無形資産**

例えば、組織の評判、イメージ

**⑤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（暖房、照明、電源、空調）

**●リスクマネジメント（JIS Q 31000）**

ISOは、企業等組織のリスクに焦点を絞り、組織経営のための取組みプロセスを明確にする指針として、2009年11月にISO 31000を公表しました。

2010年９月に発行されたJIS Q 31000「リスクマネジメント－原則及び指針」は、ISO 31000を翻訳したもので、リスクマネジメントにおける論理的考え方及び行うべき原則「リスクマネジメントの原則」、リスクマネジメントにおける組織体制「リスクマネジメントの枠組み」、リスクを認識して対処する過程「リスクマネジメントプロセス」から構成されています。

なお、JIS Q 31000では、**リスク**を「目的に対する不確かさの影響」と定義し、**リスクマネジメント**を「リスクについて、組織を指揮統制するための調整された活動」と定義しています。

JIS Q 31000は、全ての組織に適用でき、かつ、全てのリスクに適用できますが、適用は任意であり、強制力はありません。

|  |
| --- |
| 例題　プラスアルファ  JIS Q 31000：2010（リスクマネジメント－原則及び指針）において，リスクマネジメントを効果的なものにするために，組織が順守することが望ましいこととして挙げられている原則はどれか。  ア　リスクマネジメントは，静的であり，変化が生じたときに終了する。  イ　リスクマネジメントは，組織に合わせて作られる。  ウ　リスクマネジメントは，組織の主要なプロセスから分離した単独の活動である。  エ　リスクマネジメントは，リスクが顕在化した場合を対象とする。  JIS Q 31000:2010（リスクマネジメント－原則及び指針）の「3 原則」に「リスクマネジメントを効果的なものにするために，組織は，次の原則をすべての階層で順守することが望ましい。」と記述されており、その中に、「g) リスクマネジメントは，組織に合わせて作られる。」と記述されています。  ア　「j) リスクマネジメントは，動的で，繰り返し行われ，変化に対応する。」と記述されています。  ウ　「b) リスクマネジメントは，組織のすべてのプロセスにおいて不可欠な部分である。リスクマネジメントは，組織の主要な活動及びプロセスから切り離された単独の活動ではない。」と記述されています。  エ　「k) リスクマネジメントは，組織の継続的改善を促進する。」と記述されており、リスクが顕在化した場合を対象とするわけではありません。  情報セキュリティマネジメント　平成29年度春　問5　[出題頻度：★☆☆]  解答－イ |

🏋プラスアルファ

**●情報セキュリティ事象と情報セキュリティインシデント**

情報セキュリティマネジメントに関する国際規格であるISO 27001では、情報セキュリティ事象を「システム、サービス又はネットワークにおける特定の状態の発生。特定の状態とは、情報セキュリティ基本方針への違反若しくは管理策の不具合の可能性、又はセキュリティに関連するかもしれない未知の状況を示しているものをいう」と定義し、情報セキュリティインシデントを「望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの」と定義しています。

IPAは、情報セキュリティ事象の例として「セキュリティポリシ違反」、「情報セキュリティの発見」、「メールの誤送信」を、情報セキュリティインシデントの例として「ウイルス感染」、「不正アクセスを受ける」、「情報媒体（USBメモリなど）の紛失」、「パソコンなどの盗難」を挙げています。

|  |
| --- |
| 例題　プラスアルファ  JIS Q 27000:2014(情報セキュリティマネジメントシステム－用語)及びJIS Q 27001:2014(情報セキュリティマネジメントシステム－要求事項)における情報セキュリティ事象と情報セキュリティインシデントの関係のうち，適切なものはどれか。  ア　情報セキュリティ事象と情報セキュリティインシデントは同じものである。  イ　情報セキュリティ事象は情報セキュリティインシデントと無関係である。  ウ　単独又は一連の情報セキュリティ事象は，情報セキュリティインシデントに分類され得る。  [エ](https://www.sg-siken.com/kakomon/30_haru/q5.html#ans)単独又は一連の情報セキュリティ事象は，全て情報セキュリティインシデントである。  JIS Q 27000：2014（情報セキュリティマネジメントシステム－用語）では、「2.36 情報セキュリティインシデント（information security incident）」として、「望まない単独若しくは一連の情報セキュリティ事象，又は予期しない単独若しくは一連の情報セキュリティ事象であって，事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。」と記述されています。  情報セキュリティマネジメント　平成30年度春　問5　[出題頻度：★☆☆]  解答－ウ |

## 2. リスク分析と評価

学習のポイント

✅ リスク基準、リスクレベル、リスクアセスメントを中心に用語を覚えておこう！

🏋プラスアルファ

**１）情報資産の調査**

リスクを分析するに当たっては、まず、関係者の話や、成果物のレビューなどをもとに、情報資産の調査を行い、どのようなリスクがプロジェクトに影響を与えるかを把握します。

**２）情報資産の重要性による分類**

情報資産を保護するための判断基準を作成するために、用途、管理者、利用者、利用場所、利用期間を調査し、機密性、完全性、可用性の３つの側面から重要性を検討し、分類します。

この分類に基づいて、情報資産台帳を作成し、管理の方法を決定します。

**３）リスクの種類**

**①リスクの種類**

リスクには、様々な種類があります。

オペレーションリスクは、従業員の不正や業務ミスによるリスクから地震や台風などによる自然災害によるリスクまで、通常業務に係るリスクの総称です。

サプライチェーンリスクは、自然災害やシステムトラブルなので、原材料が製品となって顧客に届くまでのサプライチェーンが分断されることによるリスクです。2011年３月11日に発生した東日本大震災後、特に注目されるようになりました。

外部サービス利用のリスクは、クラウドサービスの利用を含む外部サービスを利用することによる、データの保管場所が不明であったり、バックアップの方法が不明であったりすることに伴うリスクです。

SNSによる情報発信のリスクは、SNSを利用することで発生する可能性があるリスクで、SNS 上での不適切な発言によるリスク、位置情報が特定されることによるリスク、ウイルス感染などが挙げられます。

規律や倫理観の欠如などによるモラルハザードもリスクの一つです。

**②損失の分類**

リスクに伴って発生する可能性がある損失は、データやシステムの破壊などによって発生する財産損失、情報漏洩や誤動作などによって発生する損害賠償責任による責任損失、代替システムを用意するための費用、正常に動作していた場合に得られた利益を失うことによる機会損失などの純収益の損失、役員や従業員の傷害や疾病、死亡による人的損失の４つに分けられます。

**③年間予想損失額**

年間予想損失額は、損失発生の予想頻度（ｆ）と１回当たりの予想損失額（ｉ）から計算できます。

米国商務省標準局（NBS：National Bureau of Standard）が、連邦政府の標準として発表した計算式は次のとおりです。

年間予想損失額 ＝ 10 f＋ｉ－３ ÷ ３

### ４）情報セキュリティリスクアセスメント

情報セキュリティリスクアセスメントとは、情報セキュリティリスクを分析し、評価することです。具体的には、組織が保有する情報資産を対象に、どのような脅威が存在するか、その脅威はどの程度発生する可能性があるか、脅威が顕在化した場合にはどの程度の影響を受けるか、評価します。

#### ①リスク基準

リスク受容基準と情報セキュリティリスクアセスメントを実施するための基準を総称してリスク基準と呼びます。

**リスク受容基準**は、存在するリスクに対策を実施するかどうか判断する基準です。組織がリスクを受け入れることができないと判断した場合に対策を実施します。

情報セキュリティリスクアセスメントでは、繰り返し実施した情報セキュリティリスクアセスメントが、一貫性及び妥当性があり、かつ、比較可能な結果を生み出すことを確実にするために、まず、情報セキュリティのリスク基準を確立し、維持します。

#### ②リスクレベル

リスクレベル（リスクの大きさ）は、資産価値、脅威、脆弱性の大きさによって決まります。

リスクレベルは、広く受け入れ可能なリスクレベル、受け入れ可能なリスクレベル、やむを得ず受け入れ可能なリスクレベル、広く受け入れ不可能なリスクレベルに分けられます。

なお、JIS Q 27000：2019では、リスクレベルを「結果とその起こりやすさの組合せとして表現される、リスクの大きさ。」と定義しています。

|  |
| --- |
| 例題  JIS Q 27000：2014（情報セキュリティマネジメントシステム－用語）における“リスクレベル”の定義はどれか。  ア　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  イ　結果とその起こりやすさの組合せとして表現される，リスクの大きさ  ウ　対応すべきリスクに付与する優先順位  エ　リスクの重大性を評価するために目安とする条件  ア　JIS Q 27000：2014に「2.89 ぜい弱性（vulnerability）　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。」と記述されており、“ぜい弱性”の定義です。  ウ　JIS Q 27000：2014には該当する定義はありません。  エ　JIS Q 27000：2014に「2.73 リスク基準（risk criteria）　リスクの重大性を評価するための目安とする条件。」と記述されており、“リスク基準”の定義です。  基本情報　平成31年度春　問41　[出題頻度：★☆☆]  解答－イ |

別冊演習ドリル 》 1-745

#### ③リスクアセスメントのプロセス

リスクアセスメントのプロセスは、リスク特定、リスク分析、リスク評価、リスク対応から構成されています。

**リスク特定**では、保有する情報資産を対象に、存在する脅威を特定します。

**リスク分析**では、特定した脅威はどの程度発生する可能性があるか分析します。

**リスク評価**では、脅威が顕在化した場合にはどの程度の影響を受けるか評価します。また、対応すべきリスクか否かを判断するために、予め定められた基準と比較します。

**リスク対応**では、リスクアセスメントによって判明したリスクに対しての対応方法を決定します。

なお、JIS Q 27000：2019では、リスクアセスメントを、「リスク特定、リスク分析及びリスク評価のプロセス全体。」と定義しています。

🏋プラスアルファ

**●定性的リスク分析と定量的リスク分析**

識別されたリスク全てに対応することは時間と費用の面から難しいので、その影響と発生確率から、定性的に優先順位付けをします。これを定性的リスク分析と呼びます。

その後、個々のリスクの発生確率とその影響を、数量的に分析します。これを定量的リスク分析と呼びます。

最後に、分析結果に基づいて、リスクが発生した場合に影響を最小限にするための対応計画を個々のリスクごとにまとめます。

なお、日本情報処理開発協会（JIPDEC）が開発した定性的リスク分析の手法に、**JRAM**（JIPDEC Risk Analysus Method）があります。これは、「JRAM質問票」に対する回答結果をもとに脆弱性の分析を行い、「業務日報・障害報告など」の分析シートに基づいてリスクの実態分析を行います。

|  |
| --- |
| 例題  JIS Q 27000:2014（情報セキュリティマネジメントシステム－用語）におけるリスク評価についての説明として，適切なものはどれか。  ア　対策を講じることによって，リスクを修正するプロセス  イ　リスクとその大きさが受容可能か否かを決定するために，リスク分析の結果をリスク基準と比較するプロセス  [ウ](https://www.sg-siken.com/kakomon/30_haru/q3.html#ans)リスクの特質を理解し，リスクレベルを決定するプロセス  エ　リスクの発見，認識及び記述を行うプロセス  ア　リスク対応の説明です。  ウ　リスク分析の説明です。  エ　リスク特定の説明です。  情報セキュリティマネジメント　平成30年度春　問3　[出題頻度：★★★]  解答－イ |

別冊演習ドリル 》 1-746～752

🏋プラスアルファ

**●リスクマトリックス**

リスクマトリックスは、縦軸に強度（一定期間の総損失額や一件当たりの損失額など）、横軸に頻度（一定期間の総損失件数や確率など）をとった４象限マトリックスで、保有するリスクをリスクマトリックス上にマッピングすることで、対策の優先順位を決定します。

Ⅱ

Ⅰ

Ⅲ

Ⅳ

高

低

少

多

強度

頻度

Ⅰ、Ⅱ、Ⅲ、Ⅳの順に、対策を行います。

**●リスク所有者**

リスク所有者は、リスクを運用管理する責任と権限をもつ人及び主体です。リスク所有者が示すリスクの評価指針や対策基準に従って、情報資産の管理者はリスクの評価と対策を検討します。

**●リスク源**

リスク源は、それ自体又は他と組み合わせによってリスクを生じさせる力を潜在的にもつものです。リスク源こそがリスクの根本原因です。

**●リスク選好とリスク忌避**

リスク選好は、ある機会を追求するために、そのリスクをとる又は増加させることを意味します。

リスク忌避は、リスクを避けることを意味します。

情報セキュリティリスクマネジメントでは、リスク選好ではなく、リスク忌避を選択すべきです。

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 例題　プラスアルファ  システムの改善に向けて提出された４案について，評価項目を設定して採点した結果を，採点結果表に示す。効果及びリスクについては５段階評価とし，それぞれの評価項目の重要度に応じて，重み付け表に示すとおりの重み付けを行った上で次の式で総合評価点を算出したとき，総合評価点が最も高い改善案はどれか。  〔総合評価点の算出式〕  総合評価点＝効果の総評価点－リスクの総評価点  採点結果表   |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | 案  評価項目 | | 案１ | 案２ | 案３ | 案４ | | 効果 | セキュリティ強化 | ３ | ４ | ５ | ２ | | システム運用品質向上 | ２ | ４ | ２ | ５ | | 作業コスト削減 | ５ | ４ | ２ | ４ | | リスク | スケジュールリスク | ２ | ４ | １ | ５ | | 技術リスク | ４ | １ | ５ | １ |   重み付け表   |  |  |  | | --- | --- | --- | | 評価項目 | | 重み | | 効果 | セキュリティ強化 | ４ | | システム運用品質向上 | ２ | | 作業コスト削減 | ３ | | リスク | スケジュールリスク | ８ | | 技術リスク | ３ |   ア　案１ イ　案２ ウ　案３ エ　案４  各選択肢の総合評価点を計算すると、次にようになります。  ア　案１＝３×４＋２×２＋５×３－（２×８＋４×３）＝12＋４＋15－16－12＝３  イ　案２＝４×４＋４×２＋４×３－（４×８＋１×３）＝16＋８＋12－32－３＝１  ウ　案３＝５×４＋２×２＋２×３－（１×８＋５×３）＝20＋４＋６－８－15＝７  エ　案４＝２×４＋５×２＋４×３－（５×８＋１×３）＝８＋10＋12－40－３＝－13  情報セキュリティスペシャリスト　平成26年度春Ⅱ　問24　[出題頻度：★☆☆]  解答－ウ |

別冊演習ドリル 》 1-753,754

### ５）情報セキュリティリスク対応

リスク対応は、リスクアセスメントの結果に基づき、リスク対策の方法を選択することです。リスク対策の方法には、リスクコントロールとリスクファイナンシングがあります。

#### ①リスクコントロール

リスクコントロールは、リスク発生による損失を未然に防ぐための対策で、おもなものに、リスク回避とリスク低減があります。

**リスク回避**は、リスクを発生させる設備や情報との関係を絶つことで、リスク自体の発生をゼロにすることです。

**リスク低減**（**リスク軽減**）は、設備の安全性向上やセキュリティ管理の強化などにより、リスク自体を低減させることです。

#### ②リスクファイナンシング

リスクファイナンシングは、リスクが現実化した場合に損失を最小にするために行う資金的対策で、リスクの発生を予測し体制を整えるリスクヘッジの一種で、おもなものに、リスク保有とリスク共有があります。

**リスク保有**（**リスク受容**）は、リスクが許容できる（損失の発生に対し、積立金・引当金などの自己の資金で対応できる）範囲内にある場合、当面は現在の状態を継続させることです。

**リスク共有**（**リスク移転**、**リスク分散**）は、リスクを事前に予測して、それに対する保険等で担保するなど、リスクが発生した場合に、リスクに見合うプラスの効果を得るようにバランスさせることです。

なお、リスク対応後に残るリスクを**残留リスク**と呼び、残留リスクが最小になるように**リスク対応計画**を立てる必要があります。

|  |
| --- |
| 例題  リスク対応のうち，リスクの回避に該当するものはどれか。  ア　リスクが顕在化する可能性を低減するために，情報システムのハードウェア構成を冗長化する。  イ　リスクの顕在化に伴う被害からの復旧に掛かる費用を算定し，保険を掛ける。  ウ　リスクレベルが大きいと評価した情報システムを用いるサービスの提供をやめる。  エ　リスクレベルが小さいので特別な対応をとらないという意思決定をする。  ア　リスク軽減（リスク低減）に該当します。  イ　リスク共有（リスク移転、リスク分散）に該当します。  エ　リスク保有（リスク受容）に該当します。  情報セキュリティマネジメント　平成30年度春　問2　[出題頻度：★★★]  解答－ウ |

別冊演習ドリル 》 1-755～759

🏋プラスアルファ

**●リスク登録簿**

リスク登録簿は、リスク特定、リスク分析、リスク評価、リスク対応における全ての活動を記録したリスク管理台帳で、常に更新され、リスクマネジメントのために活用されます。

**●リスクコミュニケーション**

リスクコミュニケーションは、リスクに関して、利害関係者が情報を共有し、意見を交換することで、理解を深め、良い対応ができるようにする活動で、リスクマネジメントの最適化のために重要な役割を担います。

## 3. 情報セキュリティ継続

学習のポイント

✅ 出題頻度を参考に効率よく学習しよう！

緊急事態に備えて、継続した情報セキュリティを組織の事業継続マネジメントシステムに組み込む必要があります。

#### ①緊急事態の区分

リスクが顕在化し、万が一に緊急事態が発生した場合に備えて、低（影響の程度が小さい、影響が及ぶ範囲が狭いなど）、高（影響の程度が大きい、影響が及ぶ範囲が広いなど）のように緊急事態の区分を決めて、それぞれの区分に沿った対応計画を立てておく必要があります。

#### ②緊急時対応計画（コンティンジェンシープラン）

緊急時対応計画は、組織が潜在的に抱える脅威が万が一発生した場合に、その被害や損失を最小限にとどめるために立案される対策のことです。

米国海軍省発行のComputer Incident Response Guidebookでは、コンピュータシステムのコンティンジェンシープランを策定する目的として次の７項目を挙げています。

・緊急事態からの迅速で効果的な復旧をサポートすること。

・リスクによるダメージを最小化すること。

・整然とした計画的な対応を規定すること。

・システムを守ること。

・システムに関係する人々を守ること。

・復旧のためのリソースを効果的に使用すること。

・適切な法的手続きをとること。

なお、障害復旧までの見込み時間の長さによって、幾つかの対応方法を盛り込んだコンティンジェンシープランを策定します。

|  |
| --- |
| 例題  コンティンジェンシープランにおける留意点はどれか。  ア　企業の全てのシステムを対象とするのではなく，システムの復旧の重要性と緊急性を勘案して対象を決定する。  イ　災害などへの対応のために，すぐに利用できるよう，バックアップデータをコンピュータ室内又はセンタ内に保存しておく。  ウ　バックアップの対象は，機密情報の中から機密度を勘案して選択する。  エ　被害のシナリオを作成し，これに基づく“予防策策定手順”を策定する。  コンティンジェンシープランは、組織が潜在的に抱える脅威が万が一発生した場合に、その被害や損失を最小限にとどめるために立案される対策のことです。発生頻度と発生時の損失額を想定し、費用対効果を考慮に入れて立案します。  情報セキュリティスペシャリスト　平成24年度春Ⅱ　問5　[出題頻度：★☆☆]  解答－ア |

別冊演習ドリル 》 1-760,761

#### ③復旧計画

復旧計画は、災害や障害の発生によって中断したシステムやサービスを通常の状態に戻すための計画です。復旧計画を立案する際に重要なことは、コストと目標復旧時点（RPO：Recovery Point Objective）及び目標復旧時間（RTO：Recovery Time Objective）のバランスです。目標復旧時点をどこに設定するか、目標復旧時間をいつに設定するかによって**バックアップ対策**が異なります。例えば、目標復旧時点を中断直前（RPO＝０）とした場合には、データレプリケーション（複製）が必要です。また、目標復旧時間を24時間以内（RTO≦24）とした場合には、直ちに通常稼働できるホットサイトを用意する必要があります。コストとRPO及びRTOはトレードオフの関係にあるため、システムやサービスが停止した場合に自社が被る業務上や財務上の影響を**ビジネスインパクト分析**の結果に基づいて測定し、最適な復旧計画を立てる必要があります。

#### ④被害状況の調査手法

災害復旧や障害復旧を最適に行うには被害状況の調査が必要です。被害状況の調査手法には、IPAが公表する「情報セキュリティ事象被害状況調査票」を活用する方法などがあります。

## 4. 情報セキュリティ諸規定

学習のポイント

✅ 例題を解くことができるように用語を覚えておこう！

**情報セキュリティポリシ**は、組織の情報セキュリティに対する姿勢を明文化したもので、情報セキュリティ基本方針、情報セキュリティ対策基準（基本規定）、情報セキュリティ実施手順（運用手順）の３つから構成されています。

**・情報セキュリティ基本方針**

各組織の情報セキュリティに関する考え方や、取り組みを明らかにします。

**・情報セキュリティ対策基準**

基本方針で定められた情報セキュリティを確保するために、遵守すべき行為や行動を示したものです。具体的な基準として、情報の適正管理の方法を定めた**情報管理規程**、各種機密情報を保護するための**機密管理規程**、文書の保存及び管理の方法を定めた**文書管理規程**、**情報セキュリティインシデント対応規程**（コンピュータウイルス感染時の対応ほか）、個人情報の適正な取扱い方法を定めた**プライバシポリシ**（**個人情報保護方針**）などがあります。

**・情報セキュリティ実施手順**

対策基準に定められた内容を具体的な業務において、どのような手順に従って実行していくのかを示したものです。

🏋プラスアルファ

IPA“中小企業の情報セキュリティ対策ガイドライン（第2.1版）”では、中小企業などの規模の小さい組織を対象に、対策基準と実施手順とを１階層に簡素化した情報セキュリティポリシの策定を紹介しています。

|  |
| --- |
| 例題  企業の情報セキュリティポリシの基本方針策定に関する記述のうち，適切なものはどれか。  ア　業種ごとに共通であり，各企業で独自のものを策定する必要性は低い。  イ　システム管理者が策定し，システム管理者以外に知られないよう注意を払う。  ウ　情報セキュリティに対する企業の考え方や取り組みを明文化する。  エ　ファイアウォールの設定内容を決定し，文書化する。  ア　情報セキュリティポリシは、企業全体の情報セキュリティに関する基本方針です。各企業が、自社のセキュリティに対する取り組みや姿勢を示す必要があります。  イ　情報セキュリティポリシを策定し公開することによって、責任の所在や判断基準、実施すべき対策が明らかになり、その結果、社員の１人ひとりの情報セキュリティに対する意識や、企業の対外的なイメージや信頼性が向上します。  エ　ファイウォールの設定など、個別のセキュリティ対策は、実施手順で示します。  基本情報　平成15年度春　問72　[出題頻度：★☆☆]  解答－ウ |

別冊演習ドリル 》 1-762

## 5. 情報セキュリティマネジメントシステム（ISMS）

学習のポイント

✅ 例題を解くことができるように用語を覚えておこう！

ISMS（Information Security Management System：情報セキュリティマネジメントシステム）の目的は、情報資産の喪失、流出、外部からの不正アクセスなどの脅威からシステムを守り、情報の機密性、完全性、可用性を継続的に確保・維持するシステムを確立することです。

#### ①ISMS適用範囲

ISMSを構築する際には、最初に、事業、組織、所在地、資産、技術の特徴の観点から、ISMS適用範囲を決める必要があります。基本的には、事業所名、部署名、所在地を明示します。

#### ②リーダシップとコミットメント

経営者は、組織の事業プロセスをISMSの要求事項に沿うようするために、ISMSに必要な経営資源が利用可能であることを確実にし、有効なISMS要求事項への適合の重要性を伝達する必要があります。そのため、情報セキュリティ方針と情報セキュリティ目的を確立し、ISMSの構築に関してリーダシップとコミットメントを実証する必要があります。

#### ③PDCAモデル

ISMSの構築には、PDCA（Plan→Do→Check→Act）モデルの導入は不可欠です。

**・計画（Plan）**

まず、ISMSの適用範囲及び基本方針を経営陣のコミットメントを得て確立します。次に、リスクアセスメントに基づいて管理目的と管理策を選択します。最後にリスク対応後に残っているリスクについて経営陣の承認を得ます。

**・運用（Do）**

リスク対応計画を策定し、これに従い優先順位の高い管理策から実施します。そして、管理策の有効性を測定します。また、教育・訓練及び意識向上のためのプログラムを実施します。ISMSの運用を管理し、ISMSのための経営資源を管理します。迅速にセキュリティ事象を抽出し、セキュリティインシデントに対応できるための手順及びその他の管理策を実施します。

**・パフォーマンス評価（Check）**

セキュリティ活動が期待通り行われているか、セキュリティ違反やインシデントが発生していないかを内部監査すると同時に、ISMSの有効性について定期的に確認しながら継続的な改善を行います。これをマネジメントレビューといいます。そして、内部監査やマネジメントレビューから得られた事項を考慮するために、セキュリティ計画を更新します。また、ISMSの有効性やパフォーマンスに影響を及ぼす可能性がある活動及び事象を記録します。

**・改善（Act）**

特定した改善策をISMSに導入し、適切な是正処置及び予防処置をとります。また、利害関係者に、処置と改善策を伝え、合意を得ることで、継続的改善を行い改善策が目的を達成することを確実にします。

なお、JIS Q 27000：2019では、是正処置を「不適合の原因を除去し、再発を防止するための処置」、継続的改善を「パフォーマンスを向上するために繰り返し行われる活動」と定義しています。

PDCAモデル

|  |
| --- |
| 例題　プラスアルファ  ISMSプロセスのPDCAモデルにおいて，PLANで実施するものはどれか。  ア　運用状況の管理 イ　改善策の実施  ウ　実施状況に対するレビュー エ　情報資産のリスクアセスメント  ア　Doの段階で実施します。  イ　Actの段階で実施します。  ウ　Checkの段階で実施します。  基本情報　平成19年度秋　問69　[出題頻度：★☆☆]  解答－エ |

別冊演習ドリル 》 1-763

#### ④ISMS適合性評価制度

ISMS適合性評価制度は、ISMSの体制が整備されているかを認証する制度で、企業のISMSがJIS Q 27001（ISO/IEC 27001）に準拠しているかどうかを、管轄機関であるJIPDEC（(財)日本情報処理開発協会）が認定する第三者登録機関が審査し、JIPDECが認証する制度です。実施すべき管理策としては、「セキュリティポリシ」、「セキュリティ組織」、「情報資産の分類及び管理」、「人的セキュリティ」、「物理的及び環境的セキュリティ」、「通信及び運用管理」、「アクセス制御」、「システムの開発及びメンテナンス」、「事業継続管理」、「準拠」の10項目があります。

ISMS適合性評価制度は、「国際的にも信頼を得られる情報システムのセキュリティ管理に対する第三者適合性評価制度を確立し、我が国の情報セキュリティレベル全体の向上を図ること」を目的としています。この制度に基づいて**ISMS認証**を取得した場合には、年１回以上の内部監査が必要になります。ただし外部監査を受ける必要はありません。

|  |
| --- |
| 例題  ISMS適合性評価制度の説明はどれか。  ア　ISO/IEC 15408に基づき，IT関連製品のセキュリティ機能の適切性・確実性を評価する。  イ　JIS Q 15001に基づき，個人情報について適切な保護措置を講じる体制を整備している事業者などを認定する。  ウ　JIS Q 27001に基づき，組織が構築した情報セキュリティマネジメントシステムの適合性を評価する。  エ　電子政府推奨暗号リストに基づき，暗号モジュールが適切に保護されていることを認証する。  ア　コモンクライテリア（Common Criteria）に関する記述です。  イ　個人情報保護マネジメントシステム‐要求事項に関する記述です。  エ　CRYPTRECに関する記述です。  基本情報　平成27年度秋　問40　[出題頻度：★☆☆]  解答－ウ |

別冊演習ドリル 》 1-764,765

#### ⑤JIS Q 27001（ISO/IEC 27001）

JIS Q 27001は、情報セキュリティマネジメントの国際規格であるISO/IEC 27001をJIS規格化したもので、組織の事業リスク全般を考慮して、文書化したISMSを確立、導入、運用、監視、レビュー、維持及び改善するための要求事項を規定しており、次に示すような項目で構成されています。

・情報セキュリティマネジメントシステム（ISMSの確立及び運営管理、文書化、記録）

・経営者の責任（経営者のコミットメント、経営資源の提供、教育訓練）

・内部監査

・マネジメントレビュー

・ISMSの改善（継続的改善、是正処置、予防処置）

・管理目的及び管理策

🏋プラスアルファ

**●JIS Q 27002（ISO/IEC 27002）**

JIS Q 27002は、ISO/IEC 27002をJIS規格化したもので、情報セキュリティマネジメントの導入、実施、維持及び改善に関するベストプラクティス（最も効果的な適用事例）をまとめた規格で、ISO/IEC 27001のためのガイドラインです。これに従い、情報セキュリティに関するPDCA（リスクの評価、セキュリティポリシの策定（Plan）→改善策の実施、セキュリティ教育（Do）→運用状況の管理、内部監査（Check）→有効性の確認、重要な不適合部分の是正（Act））モデルを確立することで、新たな脅威の発見が容易になり、セキュリティ事故の発生を減少させ損失を抑えることができます。

なお、JIS Q 27002に規定する指針に、クラウドサービスの提供及び利用に適用できる情報セキュリティ管理策のための指針を追加したものに、**JlS Q 27017：2016**（JIS Q 27002に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範）があります。

|  |
| --- |
| 例題  JIS Q 27001:2006におけるISMSの確立に必要な事項①～③の順序関係のうち，適切なものはどれか。  ①適用宣言書の作成  ②リスク対応のための管理目的及び管理策の選択  ③リスクの分析と評価  ア　①→②→③ イ　①→③→② ウ　②→③→① エ　③→②→①  ISMSの確立に必要な事項の順序は次のとおりです。  ①リスクの識別  ②リスクの分析と評価  ③リスク対応  ④管理目的と管理策の選択  ⑤経営陣による残留リスクの承認  ⑥適用宣言書の作成  基本情報　平成22年度春　問80　[出題頻度：★☆☆]  解答－エ |

別冊演習ドリル 》 1-766～772

🏋プラスアルファ

**●情報セキュリティガバナンス**

情報セキュリティガバナンスは、経済産業省開催の「企業における情報セキュリティガバナンスのあり方に関する研究会」の報告書において、「コーポレート・ガバナンスと、それを支えるメカニズムである内部統制の仕組みを、情報セキュリティの観点から企業内に構築・運用すること」と定義されています。

なお、経済産業省が2009年に公表した「情報セキュリティガバナンス導入ガイダンス」を元に、組織における情報セキュリティガバナンスの概念や原則、活動に関するガイダンスとして発行された国際標準にISO/IEC 27014が、これをJIS規格化したものに**JIS Q 27014**があります。

## 6. 情報セキュリティ組織・機関

学習のポイント

✅ 出題頻度を参考に効率よく学習しよう！

不正アクセスによる被害受付の対応、再発防止のための提言、情報セキュリティに関する啓発活動などを行う主な情報セキュリティ組織・機関は次のとおりです。

🏋プラスアルファ

**①情報セキュリティ委員会**

情報セキュリティ委員会は、「企業における情報セキュリティガバナンスのあり方に関する研究会」の報告書において、「情報セキュリティに係る企業のビジョンやポリシーの決定・承認、情報セキュリティ推進計画の承認や評価結果の承認などの役割を担う情報セキュリティ管理責任者をはじめとした経営層の意思決定組織」と定義されています。

**②SOC（Security Operation Center）**

SOCは、セキュリティ対策用装置やシステムのログなどを監視して、インシデントを発見する組織の総称です。

**③サイバーセキュリティ戦略本部**

サイバーセキュリティ戦略本部は、サイバーセキュリティ基本法に基づき内閣に設置された組織で、内閣官房長官を本部長に、日本におけるサイバーセキュリティ戦略の司令塔として、サイバーセキュリティ戦略案の作成及び実施の推進、国の行政機関などにおける対策の実施状況に関する監査、重大事象に対する原因究明のための調査等を行います。

|  |
| --- |
| 例題　プラスアルファ  サイバーセキュリティ基本法において定められたサイバーセキュリティ戦略本部は，どの機関に置かれているか。  ア　経済産業省 イ　国家安全保障会議 ウ　国会 エ　内閣  サイバーセキュリティ戦略本部は、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、内閣官房長官を本部長として、内閣官房に設置されました。  情報セキュリティマネジメント　平成30年度秋　問31　[出題頻度：★☆☆]  解答－エ |

🏋プラスアルファ

**④内閣サイバーセキュリティセンター（NISC）**

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）は、内閣官房に設置された組織で、内閣官房副長官補（事態対処・危機管理担当）をセンター長に、サイバーセキュリティ戦略本部の事務の処理を行い、日本におけるサイバーセキュリティの司令塔機能を担っています。

|  |
| --- |
| 例題　プラスアルファ  サイバーセキュリティ基本法に基づき，内閣官房に設置された機関はどれか。  ア　IPA イ　JIPDEC ウ　JPCERT/CC エ　NISC  ア　IPAは、情報処理システムの信頼性・安全性に関する基盤整備、ソフトウェア開発などの技術発展と人材育成などを目的とした経済産業省所管の独立行政法人です。  イ　JIPDECは、情報化環境整備の促進、情報信頼性確保の推進、電子商取引の推進、情報技術開発の促進、情報化人材の育成などを目的とする経済産業省所管の一般財団法人です。  ウ　JPCERT/CCは、国内外の関連組織と連携して、コンピュータセキュリティインシデントに係わる報告の受付、対応の支援などを行う組織（調整機関）です。  応用情報　平成30年度秋　問36　[出題頻度：★☆☆]  解答－エ |

🏋プラスアルファ

**⑤IPAセキュリティセンター（Information-technology Security Center）**

IPAセキュリティセンターは、経済産業省の告示に基づき、コンピュータウイルス・不正アクセス・脆弱性情報に関する発見・被害の届出を受け付ける組織（受付機関）です。集められた情報は、定期的に集計・公表され、被害の拡大・再発の防止、情報セキュリティ対策の向上に利用されています。なお、IPAは、次の各種制度に関する届出機関として指定されています。

・コンピュータ不正アクセス対策基準に基づくコンピュータ不正アクセス届出制度

・コンピュータウイルス対策基準に基づくコンピュータウイルス届出制度

・ソフトウェア等脆弱性関連情報取扱基準に基づくソフトウェア等の脆弱性関連情報に関する届出制度

**⑥JPCERT/CC**

JPCERT（ジェーピーサート）/CC（Japan Computer Emergency Response Team Coordination Center）は、国内外の関連組織と連携して、コンピュータセキュリティインシデントに係わる報告の受付、対応の支援などを行う組織（調整機関）です。集められた情報は、インシデントごとに分類し、届出者のプライバシーを侵害することがないように配慮した上で、四半期毎の活動概要、及びインシデント対応四半期レポートとして公開されています。

また、組織的なインシデント対応体制である「組織内CSIRT（組織内の情報セキュリティ問題を専門に扱う、インシデント対応チーム）」の構築を支援する目的で、組織内CSIRTの必要性や役割とその範囲、構築プロセス、運用などを、「構想」「構築」「運用」のそれぞれのフェーズごとの資料としてまとめたCSIRTマテリアルを公表しています。

なお、JPCERT/CCが報告を受け付けているコンピュータセキュリティインシデントは、「情報システムの運用におけるセキュリティ上の問題として捉えられる事象」であり｢実際には影響が発生していない事象であっても何らかの影響を受けた疑いがある、もしくは放置しておくとセキュリティ上の影響が生じるおそれがある場合であれば、コンピュータセキュリティインシデントと捉える｣と定義されています。

|  |
| --- |
| 例題　プラスアルファ  JPCERT/CCの説明はどれか。  ア　工業標準化法に基づいて経済産業省に設置されている審議会であり，工業標準化全般に関する調査・審議を行っている。  イ　電子政府推奨暗号の安全性を評価・監視し，暗号技術の適切な実装法・運用法を調査・検討するプロジェクトであり，総務省及び経済産業省が共同で運営する暗号技術検討会などで構成される。  ウ　特定の政府機関や企業から独立した組織であり，国内のコンピュータセキュリティインシデントに関する報告の受付，対応の支援，発生状況の把握，手口の分析，再発防止策の検討や助言を行っている。  エ　内閣官房に設置され，我が国をサイバー攻撃から防衛するための司令塔機能を担う組織である。  ア　日本工業標準調査会に関する記述です。  イ　国立研究開発法人情報通信研究機構に関する記述です。  エ　内閣サイバーセキュリティセンターに関する記述です。  情報セキュリティマネジメント　平成28年度秋　問3　[出題頻度：★☆☆]  解答－ウ |

別冊演習ドリル 》 1-773,774

#### ⑦CSIRT（Computer Security Incident Response Team：シーサート）

CSIRTは、日本シーサート協議会によって、「インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動を行うコンピュータセキュリティにかかるインシデント（事故）に対処するための組織の総称」と定義されています。

なお、JPCERT/CCが2015年11月に公表した“CSIRTガイド”では、CSIRTを活動とサービス対象によって、組織にかかわるインシデントに対応する“組織内CSIRT”、国を代表するインシデント対応のための連絡窓口として活動する“国際連携CSIRT”、CSIRT間の情報連携、調整を行なう“コーディネーションセンター”、インシデントの傾向分析やマルウェアの解析や侵入等攻撃の痕跡の分析を行ない必要に応じて注意喚起を行なう“分析センター”、自社製品の脆弱性に対応してパッチを作成したり注意喚起をしたりする“ベンダチーム”、組織内CSIRTの機能の一部又は全部を有償で請け負う“インシデントレスポンスプロバイダ”の６つに分類しています。

|  |
| --- |
| 例題  CSIRTの説明として，適切なものはどれか。  ア　IPアドレスの割当て方針の決定，DNSルートサーバの運用監視，DNS管理に関する調整などを世界規模で行う組織である。  イ　インターネットに関する技術文書を作成し，標準化のための検討を行う組織である。  ウ　企業内・組織内や政府機関に設置され，情報セキュリティインシデントに関する報告を受け取り，調査し，対応活動を行う組織の総称である。  エ　情報技術を利用し，宗教的又は政治的な目標を達成するという目的をもつ者や組織の総称である。  ア　ICANN（The Internet Corporation for Assigned Names and Numbers）に関する記述です。  イ　IETF（Internet Engineering Task Force）に関する記述です。  エ　ハクティビスト（hacktivist）に関する記述です。  基本情報　平成29年度秋　問42　[出題頻度：★☆☆]  解答－ウ |

🏋プラスアルファ

**⑧情報セキュリティ早期警戒パートナーシップ**

情報セキュリティ早期警戒パートナーシップは、ソフトウェア等脆弱性関連情報取扱基準に基づき、国内におけるソフトウェア等の脆弱性関連情報を適切に流通させるために作られた枠組みです。

IPA、JPCERT/CC、JEITA（一般社団法人電子情報技術産業協会）、CSAJ（一般社団法人コンピュータソフトウェア協会）、JISA（一般社団法人情報サービス産業協会）、JNSA（特定非営利活動法人日本ネットワークセキュリティ協会）などが参加しています。

**⑨JVN（Japan Vulnerability Notes）**

JVNは、JPCERT/CCとIPAが共同で管理している脆弱性対策情報提供サイトです。

|  |
| --- |
| 例題　プラスアルファ  JVN（Japan Vulnerability Notes）はどれか。  ア　情報システムに存在する脆弱性の深刻度を評価する手法  イ　製品に存在する脆弱性に対して採番された識別子  ウ　脆弱性対策情報などを提供するポータルサイト  エ　組織内の情報セキュリティ問題を専門に扱うインシデント対応チーム  ア　CVSS(Common Vulnerability Scoring System：共通脆弱性評価システム)に関する記述です。  イ　CVE(Common Vulnerabilities and Exposures：共通脆弱性識別子)に関する記述です。  エ　CSIRT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4　[出題頻度：★☆☆]  解答－ウ |

🏋プラスアルファ

**⑩サイバーレスキュー隊（J-CRAT）**

サイバーレスキュー隊（J-CRAT：Cyber Rescue and Advice Team against targeted attack of Japan）は、標的型サイバー攻撃の被害拡大防止のため、経済産業省の協力のもと、IPAが相談を受けた組織の被害の低減と攻撃の連鎖の遮断を支援する活動を行うために2014年7月に発足させました。

**⑪ホワイトハッカー**

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ハッカーの中で善意の活動を行う者をホワイトハッカーと呼ぶことがあります。

情報セキュリティ組織や機関の中には、ホワイトハッカーの力を積極的に活用しようという動きも出てきています。

# 3. 情報セキュリティ技術評価

## 1. セキュリティ評価基準

学習のポイント

✅ 出題頻度を参考に効率よく学習しよう！

🏋プラスアルファ

**１）ISO/IEC 15408**

ISO/IEC 15408は、情報システムのセキュリティレベルを評価するための評価基準であり、**コモンクライテリア**(CC：Common Criteria for Information Technology Security Evaluation）と呼ばれます。具体的には、情報技術を用いた製品やシステムが備えるべきセキュリティ機能に関する要件（**セキュリティ機能要件**）と、設計から製品化に至る過程でセキュリティ機能が実現されていることを確認する要件（**セキュリティ保証要件**）の基準が網羅されており、情報技術に関連した製品や情報システムに対して、情報セキュリティを評価し認証するための**評価保証レベル**を定めています。なお、日本ではISO/IEC 15408の完全翻訳版として**JIS X 5070**を定めています。

|  |
| --- |
| 例題　プラスアルファ  ISO/IEC 15408を評価基準とする“ITセキュリティ評価及び認証制度”の説明として，適切なものはどれか。  ア　暗号モジュールに暗号アルゴリズムが適切に実装され，暗号鍵などが確実に保護されているかどうかを評価及び認証する制度  イ　主に無線LANにおいて，RADIUSなどと連携することで，認証されていない利用者を全て排除し，認証された利用者だけの通信を通過させることを評価及び認証する制度  ウ　情報技術に関連した製品のセキュリティ機能の適切性，確実性を第三者機関が評価し，その結果を公的に認証する制度  エ　情報セキュリティマネジメントシステムが，基準にのっとり，適切に組織内に構築，運用されていることを評価及び認証する制度  ア　JCMVP（暗号モジュール試験及び認証制度）に関する記述です。  イ　WPA（Wi-Fi Protected Access）に関する記述です。  エ　ISMS適合性評価制度に関する記述です。  情報セキュリティスペシャリスト　平成27年度秋Ⅱ　問6　[出題頻度：★☆☆]  解答－ウ |

別冊演習ドリル 》 1-775,776

🏋プラスアルファ

**２）セキュリティ評価認証制度**

現在日本で運用されている代表的なセキュリティの評価認証制度は次のとおりです。

**①JISEC（ITセキュリティ評価及び認証制度）**

ISEC（Japan Information Technology Security Evaluation and Certification Scheme）は、IT関連製品のセキュリティ機能に関して、ISO/IEC 15408に基づいて、IPAが評価認証する制度で、主に政府調達において活用されています。なお、同様の制度をもつ他の国々と認証製品を相互に受け入れる協定に参加しているため、国内で認証を受けた製品は、協定に参加している各国においても認証された製品とみなされます。

**②JCMVP（暗号モジュール試験及び認証制度）**

JCMVP（Japan Cryptographic Module Validation Program）は、IPAが運用する暗号モジュールのセキュリティ機能等に関する認証制度で、「政府機関向けセキュリティシステムの調達に際して、供給者は、本制度に基づく認証を取得することにより、選択された暗号アルゴリズムが適切に実装され、鍵等の重要情報のセキュリティが確保された暗号モジュールである」ことを証明するものです。

**③PCI DSS**

PCI DSSは、クレジットカード情報および取引情報を保護するために2004年12月、AmericanExpress、Discover、JCB、MasterCard、VISAの５社が共同で策定したクレジット業界におけるグローバルセキュリティ基準で、次の12の要件を規定しています。

安全なネットワークの構築・維持

要件１：データを保護するためにファイアウォールを導入し、最適な設定を維持すること

要件２：システムまたはソフトウェアの出荷時の初期設定値をそのまま利用しないこと

カード会員情報の保護

要件３：保存されたデータを安全に保護すること

要件４：公衆ネットワーク上でカード会員情報およびセンシティブ情報を送信する場合、暗号化すること

脆弱性を管理するプログラムの維持

要件５：アンチウイルスソフトを利用し、定期的にソフトを更新すること

要件６：安全性の高いシステムとアプリケーションを開発し、保守すること

強固なアクセス制御手法の導入

要件７：業務目的別にデータアクセスを制限すること

要件８：コンピュータにアクセスする際、利用者ごとに識別ID を割り当てること

要件９：カード会員情報にアクセスする際、物理的なアクセスを制限すること

定期的なネットワークの監視およびテスト

要件10：ネットワーク資源およびカード会員情報に対するすべてのアクセスを追跡し、監視すること

要件11：セキュリティシステムおよび有事の対応手順を定期的にテストすること

情報セキュリティポリシの保有

要件12：情報セキュリティポリシを保持すること

|  |
| --- |
| 例題　プラスアルファ  クレジットカードなどのカード会員データのセキュリティ強化を目的として制定され，技術面及び運用面の要件を定めたものはどれか。  ア　ISMS適合性評価制度 イ　PCI DSS  ウ　特定個人情報保護評価 エ　プライバシーマーク制度  ア　ISMS適合性評価制度は、JIS Q 27001に基づき，組織が構築した情報セキュリティマネジメントシステムの適合性を評価する制度です。  ウ　特定個人情報保護評価は、特定個人情報ファイルを保有しようとする又は保有する国の行政機関や地方公共団体等が、個人のプライバシー等の権利利益に与える影響を予測した上で特定個人情報の漏えいその他の事態を発生させるリスクを分析し、そのようなリスクを軽減するための適切な措置を講ずることを宣言するものです。  エ　プライバシーマーク制度は、一般財団法人日本情報経済社会推進協会（JIPDEC）が付与する個人情報の取扱いに関する認定制度です。  情報セキュリティマネジメント　平成29年度春　問26　[出題頻度：★☆☆]  解答－イ |

🏋プラスアルファ

**④CVSS（共通脆弱性評価システム）**

CVSS（Common Vulnerability Scoring System）は、情報システムの脆弱性に対するベンダに依存しないオープンで汎用的な評価手法です。次の３つの基準を基にIT製品のセキュリティ脆弱性の深刻度を評価します。

・脆弱性そのものの特性を評価する基本評価基準

・脆弱性の現在の深刻度を評価する現状評価基準

・製品利用者の利用環境も含め最終的な脆弱性の深刻度を評価する環境評価基準

|  |
| --- |
| 例題　プラスアルファ  共通脆弱性評価システム（CVSS）の特徴として，適切なものはどれか。  ア　CVSSv2とCVSSv3は，脆弱性の深刻度の算出方法が同じであり，どちらのバージョンで算出しても同じ値になる。  イ　情報システムの脆弱性の深刻度に対するオープンで汎用的な評価手法であり，特定ベンダに依存しない評価方法を提供する。  ウ　脆弱性の深刻度を0から100の数値で表す。  エ　脆弱性を評価する基準は，現状評価基準と環境評価基準の二つである。  ア　CVSSv2とCVSSv3では、脆弱性の深刻度の算出方法が異なります。CVSSv3は、CVSSv2に比べて脆弱性の影響範囲を拡大しました。  ウ　脆弱性の深刻度を0（低）から10.0（高）の数値で表します。  エ　脆弱性を評価する基準は、基本評価基準と現状評価基準と環境評価基準の三つです。  情報セキュリティマネジメント　平成30年度秋　問28　[出題頻度：★☆☆]  解答－イ |

別冊演習ドリル 》 1-777

🏋プラスアルファ

**３）脆弱性検査**

脆弱性検査は、IPAが公表した「脆弱性検査と脆弱性対策に関するレポート」では、「ソフトウェアやシステムに対して、脆弱性がないかどうかを検査するもの」と定義されています。

**４）IT製品の調達におけるセキュリティ要件リスト**

IT製品の調達におけるセキュリティ要件リストは、IT製品を調達する際に、想定される脅威に対抗できる製品の調達を可能にするために、経済産業省がIPAと共同で、製品分野ごとに考慮すべきセキュリティ上の脅威とそれに対抗するためのセキュリティ要件をまとめたものです。

### ５）ペネトレーションテスト

ペネトレーションテスト（penetration test）は、外部からネットワークに不正侵入できないか実際に試してみることで、セキュリティ上の弱点を評価する方法です。

|  |
| --- |
| 例題  コンピュータやネットワークのセキュリティ上の脆弱性を発見するために，システムを実際に攻撃して侵入を試みる手法はどれか。  ア　ウォークスルー イ　ソフトウェアインスペクション  ウ　ペネトレーションテスト エ　リグレッションテスト  ペネトレーションテストとは、外部からネットワークに不正侵入できないかどうかを実際に試みることで、セキュリティ上の弱点を評価する方法です。次に示すようなテスト項目があります。  ・ファイアウォールや公開サーバに対するセキュリティホールや設定ミスの有無  ・DoS攻撃を受けた場合にどの程度耐えられるのかの確認  ・他のコンピュータを攻撃する踏み台にされないかどうかの確認　　など  基本情報　平成29年度秋　問45　[出題頻度：★★☆]  解答－ウ |

別冊演習ドリル 》 1-778,779

### ６）耐タンパ性

耐タンパ性は、物理的および論理的に情報を読まれることを防ぐ機能です。ICチップなどの情報の不正解読や偽造に対して有効な対策です。

|  |
| --- |
| 例題  ICカードの情報の解読や偽造に対して，物理的に情報を保護するための機能を示すものはどれか。  ア　SECE イ　インターロック ウ　インボリューション エ　耐タンパ性  ア　SECE（Secure Electronic Commerce Environment）は、インターネットを利用して安全に決済ができるようにするための技術仕様のことです。  イ　インターロックは、誤った操作や誤動作による事故を防ぐための仕組みです。  ウ　インボリューション（involution）は、複雑化、内側に向かう、などの意味をもっています。Feistelの開発した暗号では、インボリューションと呼ばれる1：1変換のデータランダム化処理テクニックが用いられています。  ソフトウェア開発　平成19年度春　問75　[出題頻度：★★☆]  解答－エ |

別冊演習ドリル 》 1-780,781

# 4. 情報セキュリティ対策

## 1. 情報セキュリティ対策の種類

学習のポイント

✅ 例題を解くことができるように用語を覚えておこう！

情報セキュリティ対策は、その対象が情報システムの利用者である人間か、装置や設備、施設の管理方法か、情報システムそのものかという観点から、大きく３つに分けられます。

### １）人的セキュリティ対策

人的セキュリティ対策は、組織を構成するすべての人間に対して行うべきセキュリティ対策です。

🏋プラスアルファ

**①組織における内部不正ガイドライン**

組織における内部不正ガイドラインは、IPAセキュリティセンターが設置した「組織における内部不正ガイドライン検討委員会」が「企業やその他の組織において必要な内部不正対策を効果的に実施可能とすること」を目的に作成したもので、内部不正防止の重要性や対策の体制、関連する法律などの概要を説明しています。

また、組織における内部不正の在り方について、基本方針、資産管理、技術的管理、証拠確保、コンプライアンス、職場環境、事後管理などの観点のもと、具体的な対策を示しています。

現在、IPAのWebサイト（https://www.ipa.go.jp/security/fy24/reports/insider/）で第４版が公開されています。

|  |
| --- |
| 例題　プラスアルファ  IPA“組織における内部不正防止ガイドライン”にも記載されている，組織の適切な情報セキュリティ対策はどれか。  ア　インターネット上のWebサイトへのアクセスに関しては，コンテンツフィルタ（URLフィルタ）を導入して，SNS，オンラインストレージ，掲示板などへのアクセスを制限する。  イ　業務の電子メールを，システム障害に備えて，私用のメールアドレスに転送するよう設定させる。  ウ　従業員がファイル共有ソフトを利用する際は，ウイルス対策ソフトの誤検知によってファイル共有ソフトの利用が妨げられないよう，ウイルス対策ソフトの機能を一時的に無効にする。  エ　組織が使用を許可していないソフトウェアに関しては，業務効率が向上するものに限定して，従業員の判断でインストールさせる。  IPA“組織における内部不正防止ガイドライン”の「4-4.技術・運用管理」の「(12) ネットワーク利用のための安全管理」に、「組織のネットワーク利用では、PC等の情報機器から重要情報が漏えいしないように、ファイル共有ソフト及びソーシャル・ネットワーク・サービス(SNS)、外部のオンラインストレージ等の使用を制限して安全なネットワーク環境を整えなければならない。」と記述されています。  イ　業務の電子メールを私用のメールアドレスに転送するように設定した場合、業務上重要な情報が漏えいするリスクが高くなるので、望ましい設定ではありません。  ウ　ファイル共有ソフトの利用は、意図しない重要情報の外部流出や、マルウェア感染のリスクが高くなるので、避けるべきです。仮に利用する場合は、必ずウイルス対策ソフトを使用します。  エ　組織内で許可されたソフトウェア以外のものをインストールして利用することを禁止します。利用を許可するソフトウェアは、組織内で決定します。  情報セキュリティマネジメント　平成28年度春　問7　[出題頻度：★☆☆]  解答－ア |

別冊演習ドリル 》 1-782～784

🏋プラスアルファ

**②情報セキュリティ啓発**

適切な情報セキュリティ対策が実施されるために、情報セキュリティの重要性を認識させる情報セキュリティ啓発は重要です。

情報セキュリティ啓発の一つの手段に、組織の情報セキュリティポリシを周知させるために行う教育があります。具体的には、コンピュータウイルスの脅威、インターネットの危険性、個人情報保護の重要性、情報資産の保護などについて学びます。なお、派遣社員を含む組織を構成する全ての人間に対して実施する必要があります。

また、組織の情報セキュリティを脅かす事態が起きた場合に備えて計画された対応策に沿って、事前に訓練を行っておくことは、組織構成員の情報セキュリティ意識を向上させるためにも重要です。

なお、国の情報セキュリティ啓発の一環として、情報セキュリティ上のさまざまな脅威と対策を学ぶための資料配布をIPAが実施しています。また、テレビや新聞、政府広報などのメディア活用による情報セキュリティ啓発も行われています。

#### ③利用者アクセスの管理

システムやサービスにアクセスする権利をアカウントと呼び、システム管理者は、利用者IDやパスワードを用いて**アカウント管理**を行います。システム管理者はアカウントに適切なアクセス権（P359参照）を付与する必要があります。

システム管理者が使用するシステムやサービスに関する特権的アクセス権（特権アカウント、特権ID）の漏えいは、重大な事故や犯罪につながる危険性が高いため、特権的アクセス権の管理は重要です。

なお、必要以上にアクセス権を付与すると不正や事故の確率が増えるので、利用者に付与するアクセス権は必要最小限にします。これを、アクセス権のneed-to-know（最小権限）の原則と呼びます。

#### ④ログ管理

ログ管理を行い、アクセス状況を監視して異常が発生した場合に状況を確認できる仕組みを作ることで、不正の発生を抑制できます。

|  |
| --- |
| 例題  利用者情報を格納しているデータベースから利用者情報を検索して表示する機能だけをもつアプリケーションがある。このアプリケーションがデータベースにアクセスするときに用いるアカウントに与えるデータベースへのアクセス権限として，情報セキュリティ管理上，適切なものはどれか。ここで，権限の名称と権限の範囲は次のとおりとする。  〔権限の名称と権限の範囲〕  参照権限： レコードの参照が可能  更新権限： レコードの登録，変更，削除が可能  管理者権限： テーブルの参照，登録，変更，削除が可能  ア　管理者権限 イ　更新権限 ウ　更新権限と参照権限 エ　参照権限  セキュリティ管理上適切なのは、need-to-know（最小権限）のアクセス権です。このアプリケーションは利用者データベースを検索し、検索結果を表示するだけでよいので、need-to-knowのアクセス権は参照権限のみです。  基本情報　平成30年度春　問43　[出題頻度：★☆☆]  解答－エ |

別冊演習ドリル 》 1-785

### ２）技術的セキュリティ対策

技術的セキュリティ対策は、情報システム自体に対して行うべきセキュリティ対策です。

#### ①クラッキング対策

クラッキング（P332参照）対策には、DoS（P340参照）攻撃対策、DDoS攻撃対策、ソーシャルエンジニアリング（P332参照）対策などがあります。

**DoS攻撃対策**では、攻撃元のIPアドレスを特定し、当該IPアドレスからのアクセスを制限します。また、同一のIPアドレスからのアクセス回数を制限します。

**DDoS攻撃対策**では、攻撃元が複数でIPアドレスを特定できないので、同一のIPアドレスからのアクセス回数を制限します。また、国内の利用者を対象にするサービスであれば、海外からのアクセスを禁止します。

**ソーシャルエンジニアリング対策**では、手段がのぞき見の場合には、不在時にはディスプレイをロックし、重要な情報はメモに残さない、机上に放置しないようにします。また、重要な情報が記載された紙媒体を処分する場合には必ずシュレッダーにかけます。ハードディスクを廃棄する場合には、一切復元できないようにデータを消去します。

|  |
| --- |
| 例題　プラスアルファ  機密ファイルが格納されていて，正常に動作するPCの磁気ディスクを産業廃棄物処理業者に引き渡して廃棄する場合の情報漏えい対策のうち，適切なものはどれか。  ア　異なる圧縮方式で，機密ファイルを複数回圧縮する。  イ　専用の消去ツールで，磁気ディスクのマスタブートレコードを複数回消去する。  ウ　ランダムなビット列で，磁気ディスクの全領域を複数回上書きする。  エ　ランダムな文字列で，機密ファイルのファイル名を複数回変更する。  ア　圧縮しても伸長されれば、情報漏えいの可能性があります。  イ　マスタブートレコードは、OSの起動情報などが記録される領域ですので、ここを消去しても、機密ファイルの情報はそのまま残ります。  エ　ファイル名を変更しても機密ファイルの情報に影響はありません。  情報セキュリティマネジメント　平成28年度春　問17　[出題頻度：★☆☆]  解答－ウ |

#### ②不正アクセス対策

外部からの不正アクセスを防ぐ代表的な不正アクセス対策には、ファイアウォール、IDS、IPS、WAF、SIEM（シーム）などがあります。

**ファイアウォール**は、あらかじめ決めておいた条件に合致したものだけにアクセスを許可することによって、不正アクセスを防ぐ仕組みです。

なお、ファイアウォールの設置により、外部ネットワークからも内部ネットワークからも隔離された場所を、**DMZ**（DeMilitarized Zone：非武装地帯）と呼びます。

…

PC

PC

ファイアウォール

Webサーバ

DNSサーバ

DMZ

企業内ネットワーク

ファイアウォールとDMZ

|  |
| --- |
| 例題  １台のファイアウォールによって，外部セグメント，DMZ，内部セグメントの三つのセグメントに分割されたネットワークがある。このネットワークにおいて，Webサーバと，重要なデータをもつデータベースサーバから成るシステムを使って，利用者向けのサービスをインターネットに公開する場合，インターネットからの不正アクセスから重要なデータを保護するためのサーバの設置方法のうち，最も適切なものはどれか。ここで，ファイアウォールでは，外部セグメントとDMZとの間及びDMZと内部セグメントとの間の通信は特定のプロトコルだけを許可し，外部セグメントと内部セグメントとの間の直接の通信は許可しないものとする。  ア　WebサーバとデータベースサーバをDMZに設置する。  イ　Webサーバとデータベースサーバを内部セグメントに設置する。  ウ　WebサーバをDMZに，データベースサーバを内部セグメントに設置する。  エ　Webサーバを外部セグメントに，データベースサーバをDMZに設置する。  DMZは、非武装地帯とも呼ばれ、外部セグメントと内部セグメントの中間に位置し、外部への接続のみ許可した領域です。  データベースサーバをDMZに設置した場合、重要なデータが改ざん・漏えいする恐れがあります。また、Webサーバを内部セグメントに設置した場合、許可したものしかWebサーバにアクセスできません。  基本情報　平成29年度春　問43　[出題頻度：★☆☆]  解答－ウ |

ファイアウォールの代表的な方式に**パケットフィルタリング**方式があります。パケットフィルタリングの機能をもつルータなどは、パケットがもつIPアドレスやポート番号といった情報を基に、ネットワーク間のパケットの通過の可否を決定します。パケットフィルタリング方式のファイアウォールでは、フィルタリングのルールをあらかじめ設定しておきます。例えば、許可する、又は許可しないパケットの送信元IPアドレス、送信元ポート番号、宛先IPアドレス、宛先ポート番号の組を設定します。このような、アクセスの可否を制御する情報を**ACL**（Access Control list）と呼びます（パケットフィルタリングの場合、フィルタリングテーブルと呼ぶ場合もある）。

なお、ACLの基本的な設定方式として代表的なものが二つあり、全ての通信を許可する前提で、ACLに許可しないパケットの通信パターン（ブラックリスト）を定義し、該当する通信を遮断する方式を、**ブラックリスト方式**、全ての通信を遮断する前提で、ACLに許可するパケットの通信パターン（ホワイトリスト）を定義し、該当しない通信は遮断する方式を、**ホワイトリスト方式**と呼びます。

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 例題  社内ネットワークとインターネットの接続点にパケットフィルタリング型ファイアウォールを設置して，社内ネットワーク上のPCからインターネット上のWebサーバの80番ポートにアクセスできるようにするとき，フィルタリングで許可するルールの適切な組みはどれか。   |  |  |  |  |  | | --- | --- | --- | --- | --- | | ア | 送信元 | 宛先 | 送信元ポート番号 | 宛先ポート番号 | |  | PC | Webサーバ | 80 | 1024以上 | |  | Webサーバ | PC | 80 | 1024以上 | |  |  |  |  |  | | イ | 送信元 | 宛先 | 送信元ポート番号 | 宛先ポート番号 | |  | PC | Webサーバ | 80 | 1024以上 | |  | Webサーバ | PC | 1024以上 | 80 | |  |  |  |  |  | | ウ | 送信元 | 宛先 | 送信元ポート番号 | 宛先ポート番号 | |  | PC | Webサーバ | 1024以上 | 80 | |  | Webサーバ | PC | 80 | 1024以上 | |  |  |  |  |  | | エ | 送信元 | 宛先 | 送信元ポート番号 | 宛先ポート番号 | |  | PC | Webサーバ | 1024以上 | 80 | |  | Webサーバ | PC | 1024以上 | 80 |   パケットフィルタリング型ファイアウォールでは、送信元IPアドレス、宛先IPアドレス、TCPやUDPといったプロトコル種別、ポート番号の情報を基に通信の可否をあらかじめファイウォールに設定し、そのルールに従ってパケットを選別し、許可／拒否といった処理を行います。  社内ネットワーク上のPCから、インターネット上のWebサーバにアクセスする場合、送信元はPC（ポート番号1024以上）、宛先はWebサーバ（ポート番号80）となります。  基本情報　平成29年度春　問42　[出題頻度：★★★]  解答－ウ |

別冊演習ドリル 》 1-786～788

**WAF**（Web Application Firewall）は、通常のファイアウォールでは防ぐことができない攻撃からWebアプリケーションを守るためのファイアウォールです。パケットの内容を解読してアクセスを制御することができます。

WAFでは、HTTPによる通信を、シグネチャ（攻撃パターン）やACL（Access Control List：アクセス制御リスト）に基づいて防御します。WAF は、SQLインジェクションなど、WebアプリケーションにHTTP通信でアクセスし、不正な命令を送り込もうとするような攻撃に対して有効です。

|  |
| --- |
| 例題  WAF（Web Application Firewall）を利用する目的はどれか。  ア　Webサーバ及びアプリケーションに起因する脆弱性への攻撃を遮断する。  イ　Webサーバ内でワームの侵入を検知し，ワームの自動駆除を行う。  ウ　Webサーバのコンテンツ開発の結合テスト時にアプリケーションの脆弱性や不整合を検知する。  エ　Webサーバのセキュリティホールを発見し，OSのセキュリティパッチを適用する。  イ　ウイルス対策ソフトに関する記述です。  ウ　ソフトウェア解析ツールに関する記述です。  エ　セキュリティチェックに関する記述です。  基本情報　平成26年度秋　問41　[出題頻度：★★★]  解答－ア |

別冊演習ドリル 》 1-789～791

**IDS**（Intrusion Detection System：**侵入検知システム**）は、不正アクセスを検知するためのシステムです。IDSは、監視対象によってホスト型IDSとネットワーク型IDSに分かれます。

**ホスト型IDS**（**HIDS**：Host base IDS）は、監視対象のホストごとにインストールされ、ホストのOSやアプリケーションのログを取得して不正アクセスを検知します。暗号化された通信にも有効であり、さらに、シグネチャとのパターンマッチングを失敗させるためのパケットが挿入された攻撃でも検知できます。

**ネットワーク型IDS**（**NIDS**：Network base IDS）は、企業ネットワークのDMZに配置され、対象ネットワークを流れる全てのパケットを監視します。パケットがシグネチャと一致したり、異常行動を監視したりすることによって不正アクセスを検知します。ただし、暗号化された通信については検知することが困難です。

なお、IDSはあくまでも検知できるシステムで、不正アクセスを防止することはできません。IDSの機能を拡張して不正アクセスを防止できるようにしたシステムを**IPS**（Intrusion Prevention System：**侵入防止システム**）と呼びます。IPSも、監視対象によってホスト型IPSとネットワーク型IPSに分かれます。

**ホスト型IPS**は、ホスト型IDSの機能を拡張して、不正アクセスの防止、ログの改ざん防止、自動シャットダウン機能などを備えています。

**ネットワーク型IPS**は、ネットワーク型IDSとファイアウォールを組み合わせたものです。

|  |
| --- |
| 例題  IDSの機能はどれか。  ア　PCにインストールされているソフトウェア製品が最新のバージョンであるかどうかを確認する。  イ　検査対象の製品にテストデータを送り，製品の応答や挙動から脆(ぜい)弱性を検出する。  ウ　サーバやネットワークを監視し，侵入や侵害を検知した場合に管理者へ通知する。  エ　情報システムの運用管理状況などの情報セキュリティ対策状況と企業情報を入力し，組織の情報セキュリティへの取組み状況を自己診断する。  ア　バージョンチェッカに関する記述です。  イ　ファジングに関する記述です。  エ　情報セキュリティ対策チェックリストに関する記述です。  基本情報　平成30年度秋　問42　[出題頻度：★☆☆]  解答－ウ |

別冊演習ドリル 》 1-792,793

**SIEM**（Security Information and Event Management）は、サーバやネットワーク機器などのログデータを一括管理、分析して、セキュリティ上の脅威を発見、通知するシステムです。

**DLP**(Data Loss Prevention)は、機密情報を判別し、機密情報の漏えいにつながる操作に対して警告を発令したり、その操作を自動的に無効化させたりするシステムです。

|  |
| --- |
| 例題  SIEM(Security Information and Event Management)の機能として，最も適切なものはどれか。  ア　隔離された仮想環境でファイルを実行して，C&Cサーバへの通信などの振る舞いを監視する。  イ　様々な機器から集められたログを総合的に分析し，管理者による分析を支援する。  ウ　ネットワーク上の様々な通信機器を集中的に制御し，ネットワーク構成やセキュリティ設定などを変更する。  エ　パケットのヘッダ情報の検査だけではなく，通信先のアプリケーションプログラムを識別して，通信を制御する。  ア　ビヘイビア法（サンドボックス）によるウイルス検出に関する記述です。  ウ　SDN（Software Defined Networking）に関する記述です。  エ　WAF（Web Application Firewall）に関する記述です。  基本情報技術者　令和元年度秋　問43　[出題頻度：★☆☆]  解答－イ |

別冊演習ドリル 》 1-794,795

#### ③マルウェア・不正プログラム対策

コンピュータウイルスなどのマルウェア・不正プログラム対策に**ウイルス対策ソフト**の導入があります。

**パターンマッチング方式**のウイルス対策ソフトは、既知のコンピュータウイルスの特徴を記録したパターンファイルである**ウイルス定義ファイル**（シグネチャコード）と検査対象のファイルを照らし合わせて、パターンの一致がみられた場合、そのファイルはコンピュータウイルスに感染していると判断する方法です。このとき問題となるのは、異常なファイルを検知できずに見逃してしまうことや、正常なファイルを誤って異常と検知してしまうことです。前者をフォールスネガティブ、後者をフォールスポジティブと呼びます。

なお、ウイルス定義ファイルは更新を欠かさず行い、常駐させておく必要があります。ただし、ウイルスは毎日のように新種が発生しており、コンピュータが最新のウイルス定義ファイルを保持していても、感染を防げない場合があります。また、データを暗号化した場合、ウイルスも暗号化されてしまうため、検出できません。

|  |
| --- |
| 例題  ウイルス対策ソフトのパターンマッチング方式を説明したものはどれか。  ア　感染前のファイルと感染後のファイルを比較し，ファイルに変更が加わったかどうかを調べてウイルスを検出する。  イ　既知ウイルスのシグネチャと比較して，ウイルスを検出する。  ウ　システム内でのウイルスに起因する異常現象を監視することによって，ウイルスを検出する。  エ　ファイルのチェックサムと照合して，ウイルスを検出する。  ア　コンペア法に関する記述です。  ウ　ビヘイビア法に関する記述です。  エ　チェックサム方式に関する記述です。  基本情報　平成26年度秋　問42　[出題頻度：★★☆]  解答－イ |

別冊演習ドリル 》 1-796,797

パターンマッチング方式では検出できないコンピュータウイルスの対応には、次のような方法を用います。

**ビヘイビア法**は、検査対象プログラムを動作させて、その挙動からコンピュータウイルスを検出する方法で、未知のウイルスでも検出することができます。実際の利用環境下で監視する方法と、主記憶装置上に**サンドボックス**と呼ばれる安全に隔離された仮想環境を用意して検査する方法があります。なお、異なるウイルスであっても同じような挙動をする場合があるため、必ずしもウイルス名を特定することはできません。

**逆アセンブル法**は、実行形式（バイナリコード）のファイルからソースコードを復元して、コンピュータウイルス特有のコードがないか確認する方法です。

**チェックサム法**は、コンピュータウイルスに感染していない状態での、検査対象のファイルを数値として合計した値（チェックサム）やハッシュ値などをあらかじめ記録しておき、検査時にそれらが一致するか否かによって感染を検出する方法です。

|  |
| --- |
| 例題  ウイルス検出におけるビヘイビア法に分類されるものはどれか。  ア　あらかじめ検査対象に付加された，ウイルスに感染していないことを保証する情報と，検査対象から算出した情報とを比較する。  イ　検査対象と安全な場所に保管してあるその原本とを比較する。  ウ　検査対象のハッシュ値と既知のウイルスファイルのハッシュ値とを比較する。  エ　検査対象をメモリ上の仮想環境下で実行して，その挙動を監視する。  ア　チェックサム法に関する記述です。  イ　コンペア法に関する記述です。  ウ　パターンマッチング法に関する記述です。  基本情報　平成28年度秋　問43　[出題頻度：★★☆]  解答－エ |

別冊演習ドリル 》 1-798～801

コンピュータウイルスに感染した場合には、他のパソコンへの感染を防止するために、感染したパソコンを速やかにネットワークから切り離し、セキュリティ管理者にその旨を伝えて指示に従います。また、コンピュータウイルスに感染したパソコンは、電源を切ると再度起動しない可能性があるので、セキュリティ管理者の指示があるまで電源は切らずにそのままにしておきます。なお、セキュリティ管理者は、コンピュータウイルス感染の情報を経済産業省が指定する者（独立行政法人情報処理推進機構（IPA））に届けなくてはなりません。

|  |
| --- |
| 例題  コンピュータウイルスを発見したときの適切な対処はどれか。  ア　ウイルス感染時の動作特性からウイルス名を特定するために，動作の再現性を確認する。  イ　短時間のうちに広範囲に感染するワームが発見されても，オンライン業務システムとして稼働中の場合は，そのままの状態でウイルス対策を進める。  ウ　ネットワークを経由してほかのコンピュータに感染する可能性があるので，まず感染したコンピュータをネットワークから切り離す。  エ　メモリ上にウイルスプログラムが展開されている可能性があるので，まずコンピュータの電源を切る。  ア　動作の再現性を確認することにより、被害が拡大する可能性があります。  イ　稼働を続けることにより、ウイルスが蔓延し被害が拡大することがあります。  エ　終了処理によってメモリ外に流出する可能性があるため、電源を落としても安全とは限りません。  基本情報　平成17年度秋　問65　[出題頻度：★☆☆]  解答－ウ |

#### ④脆弱性管理

脆弱性管理とは、脆弱性情報をもとにOSアップデートや脆弱性修正プログラム（修正パッチ、セキュリティパッチ）の適用を確実かつ適切に行うことです。

不正アクセス対策やマルウェア・不正プログラム対策に脆弱性管理は欠かせません。

|  |
| --- |
| 例題  クライアントPCで行うで行うマルウェア対策のうち，適切なものはどれか。  ア　PCにおけるウイルスの定期的な手動検査では，ウイルス対策ソフトの定義ファイルを最新化した日時以降に作成したファイルだけを対象にしてスキャンする。  イ　ウイルスがPCの脆弱性を突いて感染しないように，OS及びアプリケーションの修正パッチを適切に適用する。  ウ　電子メールに添付されたウイルスに感染しないように，使用しないTCPポート宛ての通信を禁止する。  エ　ワームが侵入しないように，クライアントPCに動的グローバルIPアドレスを付与する。  ア　PCにおけるウイルスの定期的な手動検査では、すべてのファイルを対象にスキャンします。  ウ　電子メールに添付されたウイルスに感染しないようにするためには、プレビュー表示機能を停止し、不審なメールは開かないようにします。  エ　動的グローバルIPアドレスとは、インターネットに接続する都度、異なるIPアドレスを割り当てる方法で、個人を対象にインターネット接続サービスを提供するプロバイダがIPアドレスを割り当てる際に用いられます。ワームの侵入を防ぐことに直接関係ありません。  基本情報　平成25年度秋　問42　[出題頻度：★☆☆]  解答－イ |

🏋プラスアルファ

**⑤入口対策と出口対策**

現在、多くの企業で採用されている不正アクセス対策やマルウェア・不正プログラム対策、脆弱性管理は、外部からのクラッカーの侵入やマルウェア・不正プログラムの侵入を防ぐ入口対策です。

しかし近年、ソーシャルエンジニアリングの手法を駆使した標的型攻撃などの攻撃手法の高度化によって、入口対策が破られる危険性が増しています。

そこで、入口対策が破られた場合も、外部への情報の漏えいや自社の設備を踏み台にさせない出口対策が重要になってきました。具体的には、通信内容を監視し、不審な動きがあった場合にはネットワークを切断して外部と通信できないようにしたり、情報を暗号化によって秘匿化します。

なお、入口対策と出口対策を組み合わせて、セキュリティ上の防御策を複数実行することを、**多層防護**と呼びます。

#### ⑥検疫ネットワーク

検疫ネットワークは、社内ネットワークに接続するクライアントPCにセキュリティ上の問題がないかを検査・修正するための仕組みです。社内ネットワークに接続する予定のクライアントPCを、事前に社内ネットワークから隔離された検査専用のネットワークに接続して（隔離）、セキュリティ上の問題がないか確認します（検査）。セキュリティ上問題があれば、これを修正し（治療）、問題解決後、安全なクライアントPCに限り接続を許可します。

クライアントPCのOSやアプリケーションの修正パッチの適用やウイルス対策ソフトのウイルス定義ファイルの更新が100％確実に行われているかどうかが疑わしい場合や、社外に持ち出されたクライアントPCを再び社内ネットワークに接続する場合などに有効です。

|  |
| --- |
| 例題　プラスアルファ  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  ア　DMZは、主に公開を目的としたサーバ等を設置するために、ファイアウォールなどによって内部ネットワークから隔離されたネットワークのことです。  イ　IDSは、インターネットから社内ネットワークへの不正侵入を検知する仕組みです。  エ　ファイアウォールは、あらかじめ決めておいた条件に合致したものだけにアクセスを許可することによって、不正アクセスを防ぐ仕組みです。  ITパスポート　平成26年度秋　問54　[出題頻度：★☆☆]  解答－ウ |

#### ⑦電子メール・Webのセキュリティ

電子メールの送信者が自分とは無関係の第三者のメールサーバ（SMTPサーバ）を不正に中継することで、身元を偽ってメールを送信することを、**第三者中継**と呼びます。第三者中継はスパムメールの送信に使われることが多く、正当な利用者のメールの配信の遅配にもつながることから、その対策が必要です。なお、代表的な第三者中継対策には、SPFやDKIM（ディーキム）、PbS、SMTP-AUTH（エスエムティーピーオース）などの認証プロトコル（P402参照）を使用する方法やOP25Bなどがあります。

🏋プラスアルファ

**●OP25B**（Outbound Port25 Blocking）

利用しているISPのメールサーバを経由せずに他のメールサーバへ直接送信されるメールを規制する方法です。なお、規制するのはポート番号が25番（SMTPサーバ宛）のメールのため、ポート番号110番（POPサーバ宛）を使用するメールの受信は問題なく行えます。

**●URLフィルタリング**

一般的なWebのセキュリティ対策の一つで、URLのブラックリストに基づきWebサイトの閲覧を制限することで、不正サイトへのアクセスや書込みを防止し、情報の漏えいやコンピュータウイルスの感染を防止する技術です。

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 例題  自社の中継用メールサーバで，接続元IPアドレス，電子メールの送信者のメールアドレスのドメイン名，及び電子メールの受信者のメールアドレスのドメイン名から成るログを取得するとき，外部ネットワークからの第三者中継と判断できるログはどれか。ここで，AAA.168.1.5とAAA.168.1.10は自社のグローバルIPアドレスとし，BBB.45.67.89とBBB.45.67.90は社外のグローバルIPアドレスとする。a.b.cは自社のドメイン名とし，a.b.dとa.b.eは他社のドメイン名とする。また，IPアドレスとドメイン名は詐称されていないものとする。   |  |  |  |  | | --- | --- | --- | --- | |  | 接続元IPアドレス | 電子メールの送信者の  メールアドレスのドメイン名 | 電子メールの受信者の  メールアドレスのドメイン名 | | ア | AAA.168.1.5 | a.b.c | a.b.d | | イ | AAA.168.1.10 | a.b.c | a.b.c | | ウ | BBB.45.67.89 | a.b.d | a.b.e | | エ | BBB.45.67.90 | a.b.d | a.b.c |   スパムメールの送信に使われる第三者中継は、自社に関係のない外部の第三者が自社のメールサーバを勝手に使ってメールの送受信を行う方法です。したがって、送信元のIPアドレスが社外のグローバルIPアドレスで、送信者のドメイン名と受信者のドメイン名の両方が自社のドメイン名でないメールは、第三者中継と判断できます。  基本情報　平成30年度秋　問45　[出題頻度：★☆☆]  解答－ウ |

別冊演習ドリル 》 1-802,803

#### ⑧携帯端末のセキュリティ

携帯電話、スマートフォン、タブレット端末などの携帯端末特有のセキュリティ対策に、盗難・紛失対策と安全に通信するための対策があります。

盗難・紛失対策の目的は情報の漏えい防止です。具体的には、パスワードやパターン入力、指紋などによる認証機能を備えた画面ロック機能の活用です。また、仮に、ロックが破られた場合に備えて、端末には必要最小限の情報しか置かない、重要な情報は暗号化するなどの対策が必要です。

盗聴を防ぎ安全に通信するには通信データを暗号化する必要があります。

会社や団体が、自組織の従業員に貸与するスマートフォンに対して、セキュリティポリシに従った一元的な設定をしたり、業務アプリケーションを配信したりして、スマートフォンの利用状況などを一元管理する仕組みを**MDM**（Mobile Device Management）と呼びます。

|  |
| --- |
| 例題  会社や団体が，自組織の従業員に貸与するスマートフォンに対して，セキュリティポリシに従った一元的な設定をしたり，業務アプリケーションを配信したりして，スマートフォンの利用状況などを一元管理する仕組みはどれか。  ア　BYOD（Bring Your Own Device） イ　ECM（Enterprise Content Management）  ウ　LTE（Long Term Evolution） エ　MDM（Mobile Device Management）  ア　BYODは、自分が所有するパソコンなどのデバイスを勤務先に持ち込んで業務で使用することです。  イ　ECMは、企業や組織における情報（データ）を統合的に管理する仕組みのことです。  ウ　LTEは、データ通信を高速化した規格のことです。  基本情報　平成26年度春　問40　[出題頻度：★★☆]  解答－エ |

別冊演習ドリル 》 1-804

#### ⑨無線LANセキュリティ

無線LANでは、盗聴、不正侵入によるLANの不正使用、なりすまし、データの改ざんや破壊に備えた対策を行う必要があります。盗聴の危険に備えて、無線LANの暗号化は必須です。無線LANの暗号化の規格には、後述するWPA2やWPA3など（P402参照）があります。

無線LANでは、接続グループの識別に最大32文字の英数字で表される**SSID**（Service Set IDentifier）を用います。SSIDを、無線LANへの接続要求を受け付けるアクセスポイントと無線LAN端末に設定し、アクセスポイントと同じSSIDを設定した無線LAN端末だけを接続可能とすることで、接続制限します。通常、接続を希望する無線LAN端末のためにアクセスポイントは自身のSSIDを公開します。そのため、無線が届く範囲内であれば、誰でもSSIDを知ることができます。そこで、接続者を制限するため、あらかじめSSIDを設定してある端末だけが接続できるように、SSIDを非公開にするアクセスポイントの機能を**SSIDステルス**と呼びます。

また、通常の無線LANでは、有線LANと同様、同じSSIDをもつ端末同士は通信が可能です。しかし、不特定多数の者が自由にアクセスすることができる公衆無線LANを利用する場合、関係のない者同士が、同じSSIDで接続するため、他者に接続している端末の情報を盗聴される危険性があります。そこで、公衆無線LANのアクセスポイントを設置する場合、設置者は接続する端末同士がアクセスポイント経由で互いに無断アクセスができないように設定する必要があります。この機能を**プライバシーセパレータ**（Privacy Separator）と呼びます。

なお、複数のアクセスポイントをもつネットワークで使用できるように機能を拡張したSSIDをESSID（Extended Service Set IDentifier）と呼びます。また、接続している端末がアクセスポイントの接続範囲をはずれても、移動先に同じESSIDをもつアクセスポイントがあれば、自動的に接続しなおし、通信を継続できる機能をローミングと呼びます。

さらに、無線LANへの不正アクセスを防ぐための技術として**MACアドレスフィルタリング**があります。MACアドレスフィルタリングは、各無線LAN端末がもつ固有の番号（MACアドレス）を識別子として用いるBSSID（Basic SSID）を無線LANへの接続要求を受け付けるアクセスポイントと無線LAN端末に設定し、アクセスポイントと同じBSSIDを設定した無線LAN端末だけを接続可能とする方法です。

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 例題  公衆無線LANのアクセスポイントを設置するときのセキュリティ対策と効果の組みのうち，適切なものはどれか。   |  |  |  | | --- | --- | --- | |  | セキュリティ対策 | 効果 | | ア | MACアドレスフィルタリングを設定する。 | 正規の端末のMACアドレスに偽装した攻撃者の端末からの接続を遮断し、利用者のなりすましを防止する。 | | イ | SSIDを暗号化する。 | SSIDを秘匿して，SSIDの盗聴を防止する。 | | ウ | 自社がレジストラに登録したドメインを，アクセスポイントのSSIDに設定する。 | 正規のアクセスポイントと同一のSSIDを設定した，悪意あるアクセスポイントの設置を防止する。 | | エ | 同一のアクセスポイントに無線で接続している端末同士の通信を，アクセスポイントで遮断する。 | 同一のアクセスポイントに無線で接続している他の端末に，公衆無線LANの利用者がアクセスポイントを経由して無断でアクセスすることを防止する。 |   ア　MACアドレスフィルタリングを設定するには、あらかじめ端末のMACアドレスをアクセスポイントに登録する必要があるため、不特定多数が利用する公衆無線LANには向いていません。  イ　SSIDステルス対策の効果です。SSIDを秘匿してしまうと、SSIDを知らない利用者が公衆無線LANを利用できません。  ウ　レジストラは、ドメインの登録を請け負う組織の総称です。この組織に登録することで、正規のドメインとなりますが、SSIDが正規のものであるかのチェック機能はないため、悪意あるアクセスポイントであるかどうかの判定はできません。  基本情報　平成30年度秋　問44　[出題頻度：★☆☆]  解答－エ |

別冊演習ドリル 》 1-805

#### ⑩クラウドサービスのセキュリティ

ネットワーク経由でコンピュータ資源の提供を受けるクラウドサービスを利用する際には、クラウドサービス提供事業者のセキュリティ環境を確認する必要があります。具体的には次のとおりです。

・通信経路は暗号化されているか

・利用者認証は多要素認証か

・データはバックアップされているか

・第三者機関のセキュリティ認証を受けているか

#### ⑪電子透かし

暗号化技術を応用してメッセージを画像データや音声データなどに埋め込み、その存在を隠す技術を**ステガノグラフィ**（steganography）と呼びます。

電子透かしは、著作権の保護を目的に、ステガノグラフィを応用した技術で、元のデータからの変化が一見してわからないように作成日や著作権情報などを埋め込みます。

|  |
| --- |
| 例題  画像などのディジタルコンテンツが，不正にコピーされて転売されたものであるかを判別できる対策はどれか。  ア　タイムスタンプ イ　電子透かし ウ　電子保存 エ　配達証明  ア　タイムスタンプは、データが存在していた日時を記録した情報です。  ウ　電子保存は、データを電子データとして保存することです。  エ　配達証明は、宛先に郵便物が配達されたことを証明するサービスです。  基本情報　平成23年度春　問45　[出題頻度：★☆☆]  解答－イ |

別冊演習ドリル 》 1-806,807

#### ⑫ディジタルフォレンジックス

ディジタルフォレンジックスは、不正アクセスなどコンピュータに関する犯罪の法的な証拠性を明らかにするために、原因究明に必要な情報を収集保全して分析することです。

|  |
| --- |
| 例題  ディジタルフォレンジックスの説明として，適切なものはどれか。  ア　あらかじめ設定した運用基準に従って，メールサーバを通過する送受信メールをフィルタリングすること  イ　外部からの攻撃や不正なアクセスからサーバを防御すること  ウ　磁気ディスクなどの書換え可能な記憶媒体を単に初期化するだけではデータを復元できる可能性があるので，任意のデータ列で上書きすること  エ　不正アクセスなどコンピュータに関する犯罪に対してデータの法的な証拠性を確保できるように，原因究明に必要なデータの保全，収集，分析をすること  ア　メールフィルタリングに関する記述です。  イ　ファイアウォールに関する記述です。  ウ　磁気ディスクを完全に初期化する方法に関する記述です。  応用情報　平成27年度秋　問43　[出題頻度：★☆☆]  解答－エ |

別冊演習ドリル 》 1-808

#### ⑬BYOD（Bring Your Own Device）とシャドーIT

従業員が私的に保有するパソコンなどの情報端末を勤務先に持ち込んで業務に使用することを、BYODと呼びます。コスト削減や効率向上の観点から近年増えていますが、情報漏えいやウイルス感染などに注意が必要です。特に、BYODを組織の許可を得ずに行うことをシャドーITと呼び、大きな脆弱性要因になります。

|  |
| --- |
| 例題  BYODの説明，及びその情報セキュリティリスクに関する記述のうち， 適切なものはどれか。  ア　従業員が企業から貸与された情報端末を，客先などへの移動中に業務に利用することであり，ショルダハッキングなどの情報セキュリティリスクが増大する。  イ　従業員が企業から貸与された情報端末を，自宅に持ち帰って私的に利用することであり，機密情報の漏えいなどの情報セキュリティリスクが増大する。  ウ　従業員が私的に保有する情報端末を，職場での休憩時間などに私的に利用することであり，セキュリティ意識の低下などに起因する情報セキュリティリスクが増大する。  エ　従業員が私的に保有する情報端末を業務に利用することであり，セキュリティ設定の不備に起因するウイルス感染などの情報セキュリティリスクが増大する。  ア　モバイルコンピューティングに関する記述です。  イ　逆BYODに関する記述です。  ウ　特別な名称はありません。  基本情報　平成28年度春　問42　[出題頻度：★★☆]  解答－エ |

別冊演習ドリル 》 1-809～811

🏋プラスアルファ

**●物理的セキュリティ対策**

物理的セキュリティ対策は、施設、設備、装置などに対して行うべきセキュリティ対策で、外部からの侵入、盗難、災害（水害、落雷、地震、火災）などから情報システムを保護し、信頼性と可用性を確保することです。

**①RASISとRAS技術**

既に「Chapter４．システム構成要素」（P140参照）で記述したように、RASISはコンピュータシステムの信頼性を表す言葉で、信頼性（Reliability）、可用性（Availability）、保守性（Serviceability）、保全性（完全性）（Integrity）、機密性（Security）の５つの言葉の頭文字を表しています。

なお、信頼性、可用性、保守性の３つを備えたシステムを実現するための技術を、その頭文字を取って特にRAS技術と呼びます。

RAS技術には、複数のハードディスクに同時に同じ内容を書込むことで信頼性を向上させる**ミラーリング**や、デュプレックスシステムやデュアルシステムのように可用性を向上させる**二重化技術**があります。

**②耐震耐火設備**

災害への対策として、耐震耐火設備や後述するUPSなどの電源設備にも配慮する必要があります（P506参照）。

**③入退出管理**

設備や情報の盗難、不正利用を防ぐために、施設をセキュリティレベルごとに区画分けし、区画ごとに入室資格を定め、入退室管理を行います。不審者の侵入を防ぐために監視カメラを設置したり、施錠管理を行うことも有用です。

なお、入退室管理システムが備える機能には、共連れを防止するために、入室後に入口と出口の両方を施錠して室内の人数を確定した後に出口を解錠可能にする**インターロックゲート**や本人認証を行わずに入室した場合には退室を認めず、本人認証を行わずに退室した場合には次回の入室を認めない**アンチパスバック**、最初の入室者と最後の退室者は２人同時でないと入退室不能とすることで常に２人以上の在室状態を維持する**TPMOR**（Two Person Minimum Occupancy Rule）などがあります。

**④クリアデスク・クリアスクリーン**

クリアデスクは、離席時に机上に書類等を放置しないことで、情報の紛失、盗難、漏えいを防ぐために必要です。また、クリアスクリーンは、離席時や作業中にディスプレイ画面の内容を見られないようにすることで、情報の漏えいを防ぐために必要です。クリアスクリーン徹底のためには、一定時間作業を中断する場合に必ずPCをログオフします。

**⑤遠隔バックアップ**

災害の発生でシステムやデータが使用不能になった場合に備えて、遠隔地にバックアップセンタを設けて複製を用意しておきます。

**⑥USBキー**

USBキーは、パソコンの不正利用を防ぐために、物理的な方法で利用者認証を行う装置です。

固有の認証情報が埋め込まれたUSBキーを対応するパソコンのUSBポートに挿入することで利用可能になります。パスワード漏えいの危険性はなくなりますが、USBキーを紛失した場合にはパソコンが使用不能になる危険があります。また、USBキーと対応するパソコンを同時に紛失した場合には情報漏えいの危険があります。

**⑦セキュリティワイヤ**

セキュリティワイヤは、オフィスでノートパソコンなどの持ち運びが可能な機器を使用する場合に盗難対策として用います。

|  |
| --- |
| 例題　プラスアルファ  情報セキュリティ対策のクリアデスクに該当するものはどれか。  ア　PCのデスクトップ上のフォルダなどを整理する。  イ　PCを使用中に離席した場合，一定時間経過すると，パスワードで画面ロックされたスクリーンセーバに切り替わる設定にしておく。  ウ　帰宅時，書類やノートPCを机の上に出したままにせず，施錠できる机の引出しなどに保管する。  エ　机の上に置いたノートPCを，セキュリティワイヤで机に固定する。  ア　デスクトップクリーンアップに関する記述です。  イ　クリアスクリーンに関する記述です。  エ　セキュリティワイヤロックに関する記述です。  情報セキュリティマネジメント　平成28年度春　問2　[出題頻度：★☆☆]  解答－ウ |

別冊演習ドリル 》 1-812

# 5. セキュリティ実装技術

## 1. セキュアプロトコル

学習のポイント

✅ 例題を解くことができるように用語を覚えておこう！

通信データの盗聴や不正接続を防ぐセキュアプロトコルには、IPsec、SSL/TLS、SSH、HTTPS（HTTP over TLS）、WPA2、WPA3などがあります。

#### ①IPsec

IPsec（Security Architecture for Internet Protocol/IP Security Protocol）は、データ認証と改ざんを検知するAH（Authentication Header）、暗号化機能を提供するESP（Encapsulating Security Payload）、暗号化アルゴリズムの情報や共通鍵を交換するためのIKE（Internet Key Exchange）などの暗号技術を用いてパケット単位で相手認証、盗聴や改ざんの防止などを行うネットワーク層のセキュアプロトコルです。そのため、暗号化に対応していないアプリケーションを用いても、盗聴や改ざんを防ぐことができます。

なお暗号化の形態には、ヘッダは暗号化せずにデータだけを暗号化するトランスポートモードと、ヘッダとデータの両方を暗号化し新たなヘッダを付加するトンネルモードの２つがあります。

インターネットVPN（P324参照）を実現するための技術としても用いられています。

|  |
| --- |
| 例題  OSI基本参照モデルのネットワーク層で動作し，"認証ヘッダ(AH)"と"暗号ペイロード(ESP)"の二つのプロトコルを含むものはどれか。  ア　IPsec イ　S/MIME ウ　SSH エ　XML暗号  イ　S/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アプリケーション層のセキュアプロトコルです。  ウ　SSHは、ディジタル署名や公開鍵暗号方式と共通鍵暗号方式、チャレンジレスポンス認証などを用いて安全にリモートコンピュータと通信するためのアプリケーション層のセキュアプロトコルです。  エ　XML暗号は、データを含む任意の情報に対する暗号文をXMLデータとして表現するためのアプリケーション層のセキュアプロトコルです。  基本情報　平成31年度春　問43　[出題頻度：★☆☆]  解答－ア |

#### ②SSL/TLS、HTTPS

SSL（Secure Sockets Layer）は、ディジタル署名や共通鍵暗号方式、公開鍵暗号方式を組み合わせ、インターネット上で安全に情報をやり取りするためのトランスポート層のセキュアプロトコルで、WebブラウザとWebサーバ間の信号を暗号化します。

SSLを用いた通信では、まず認証局が発行するディジタル証明書（サーバ証明書）がWebサーバからクライアントに送られます。なお、なりすましを防ぐため、ディジタル証明書には認証局によるディジタル署名が添付されます。次にクライアントではWebブラウザが通信で利用する共通鍵を生成し、ディジタル証明書が正当性を保証する公開鍵を用いて共通鍵を暗号化して、通信相手に送ります。以後、この共通鍵を用いて暗号化を行い、通信することになります。いわゆるハイブリッド暗号方式を採用しています。

なお、TLS（Transport Layer Security）は、SSLをインターネットの標準プロトコルとするために、IETF（Internet Engineering Task Force）がSSL3.0をもとに定めたプロトコルです。

HTTPS（Hypertext Transfer Protocol over SSL/TLS）は、SSL/TLS の機能を用いて、Webサーバとブラウザ間のデータを暗号化して転送するために使われるセキュアプロトコルです。

|  |
| --- |
| 例題  HTTPS（HTTP over SSL/TLS）の機能を用いて実現できるものはどれか。  ア　SQLインジェクションによるWebサーバへの攻撃を防ぐ。  イ　TCPポート80番と443番以外の通信を遮断する。  ウ　Webサーバとブラウザの間の通信を暗号化する。  エ　Webサーバへの不正なアクセスをネットワーク層でのパケットフィルタリングによって制限する。  ア　WAFによって実現します。   1. エ　パケットフィルタリング方式のファイアウォールによって実現します。   基本情報　平成26年度秋　問43　[出題頻度：★☆☆]  解答－ウ |

別冊演習ドリル 》 1-813

#### ③SSH

SSH（Secure Shell）は、ディジタル署名や共通鍵暗号方式、公開鍵暗号方式、チャレンジレスポンス認証などを組み合わせて、安全に遠隔にあるコンピュータ（リモートコンピュータ）と通信するためのアプリケーション層のセキュアプロトコルです。

|  |
| --- |
| 例題  SSHの説明はどれか。  ア　MIMEを拡張した電子メールの暗号化とディジタル署名に関する標準  イ　オンラインショッピングで安全にクレジット決済を行うための仕様  ウ　共通鍵暗号技術と公開鍵暗号技術を併用した電子メールの暗号化，復号の機能をもつ電子メールソフト  エ　リモートログインやリモートファイルコピーのセキュリティを強化したプロトコル，及びそのプロトコルを実装したコマンド  ア　S/MIMEに関する記述です。  イ　SET（Secure Electronic Transaction）に関する記述です。  ウ　PGP（Pretty Good Privacy）に関する記述です。  情報セキュリティマネジメント　平成30年度秋　問29　[出題頻度：★☆☆]  解答－エ |

別冊演習ドリル 》 1-814

#### ④WPA2、WPA3

WPA2（Wi-Fi Protected Access 2）は、無線LANに採用されているセキュアプロトコルで、利用者認証にIEEE802.1Xに沿った方法を、暗号化アルゴリズムに共通鍵暗号方式に使われるAESを採用しています。

なお、利用者が限定された無線LANでの使用を前提に、アクセスポイントと端末間で事前にPSK（Pre-Shared Key)と呼ばれる文字列を共通鍵として共有し、そのPSKとSSIDの組合せによって認証を行う方法にWPA2-PSKがあります。

また、WPA2で発見された脆弱性に対する対策を施し、セキュリティを強化したものにWPA3（Wi-Fi Protected Access 3）があります。

|  |
| --- |
| 例題  WPA3はどれか。  ア　HTTP通信の暗号化規格  イ　TCP/IP通信の暗号化規格  ウ　Webサーバで使用するディジタル証明書の規格  エ　無線LANのセキュリティ規格  WPA3は、無線LANのセキュリティ規格で、WPA2で発見された無線LANネットワークの公共通信についての脆弱性への対策などを施し、セキュリティを強化したバージョンです。  基本情報　令和元年度秋　問37　[出題頻度：★☆☆]  解答－エ |

別冊演習ドリル 》 1-815,816

## 2. 認証プロトコル

なりすましによる不正接続、サービスの不正利用を防ぐ**認証プロトコル**には、SPF、SMTP-AUTH、DKIM、OAuth（オーオース）、DNSSEC、EAP、EAP-TLS、PEAP（ピープ）、RADIUS（ラディウス）などがあります。

#### ①SPF

SPF（Sender Policy Framework）は、正当なメールサーバ以外からのメールの受信を拒否するプロトコルです。具体的には、メールサーバがメールを受信する際に、受信メールのドメイン名と送信元のIPアドレスとの関係が記述されたDNSサーバ内のSPFレコードを確認して、受信メールが正当なメールサーバから送信されたものかを認証します。そのため、送信元のIPアドレスを偽装していないスパムメールは検出できません。

|  |
| --- |
| 例題  SPF（Sender Policy Framework）を利用する目的はどれか。  ア　HTTP通信の経路上での中間者攻撃を検知する。  イ　LANへのPCの不正接続を検知する。  ウ　内部ネットワークへの侵入を検知する。  エ　メール送信者のドメインのなりすましを検知する。  SPFは、受信メールのドメイン名と送信元のIPアドレスとの関係が記述されたDNSサーバ内のSPFレコードを確認することで、メール送信のなりすましを検知する方法です。  情報セキュリティマネジメント　平成31年度春　問11　[出題頻度：★☆☆]  解答－エ |

別冊演習ドリル 》 1-817

#### ②SMTP-AUTH（SMTP Service Extension for Authentication）

SMTP-AUTHは、クライアントがSMTPサーバにアクセスしたときに利用者IDとパスワードを用いて利用者認証を行い、許可された利用者だけから電子メールを受け付けるプロトコルです。なお、この方法を利用するには、SMTPサーバもメールソフトも、ともにSMTP-AUTHに対応している必要があります。

🏋プラスアルファ

**●DKIM**（Domain Keys Identified Mail）

DKIMは、受信メールサーバがメールを受信する際に、ディジタル署名の仕組みを利用して正当な送信元であるかを確認するプロトコルです。具体的には、受信メールサーバがメールを受信する際に、送信情報を元にDNSサーバから公開鍵を取得して、受信メールに添付されているディジタル署名が正当な送信元のものであるかを認証します。

**●OAuth**

OAuthは、リソースごとに各利用者のアクセスが許されるか否かの判断を伝達することを目的としたプロトコルで、リソースの所有者からアクセストークンを受け取った利用者のみリソースへのアクセスが許可されます。

**●DNSSEC**（DNS Security Extensions）

DNSSECは、公開鍵暗号方式とディジタル署名の仕組みを利用して、DNS応答の正当性とメッセージが改ざんされていないことを確認するプロトコルです。

**●EAP-TLS**

EAP-TLSは、IEEE802.1Xで使われているディジタル証明書を使用した認証方式である**EAP**（Extensible Authentication Protocol：拡張認証プロトコル）の一種で、TLSを利用してサーバとクライアントの両方で相互にディジタル証明書を送って認証を行うプロトコルです。

**●PEAP**（Protected Extensible Authentication Protocol）

PEAPは、IEEE802.1Xで使われる認証方式の１つで、認証を行うサーバ側でディジタル証明書を発行し、クライアント側ではIDとパスワードを用いて、サーバとクライアント間で相互認証を行うプロトコルです。

|  |
| --- |
| 例題  SMTP-AUTH（SMTP Service Extension for Authentication）における認証の動作を説明したものはどれか。  ア　SMTPサーバは，クライアントがアクセスしてきた場合に利用者認証を行い，認証が成功したとき電子メールを受け付ける。  イ　サーバは認証局のディジタル証明書をもち，クライアントから送信された認証局の署名付きクライアント証明書の妥当性を確認する。  ウ　電子メールを受信した際にパスワード認証が成功したクライアントのIPアドレスは，一定時間だけSMTPサーバへの電子メールの送信が許可される。  エ　パスワードを秘匿するために，パスワードからハッシュ値を計算して，その値で利用者が電子メールを受信する際の利用者認証を行う。  イ　ディジタル署名に関する記述です。  ウ　PbS（POP before SMTP）に関する記述です。  エ　APOP（Authenticated POP）に関する記述です。  応用情報　平成26年度秋　問37　[出題頻度：★☆☆]  解答－ア |

別冊演習ドリル 》 1-818

## 3. ネットワークセキュリティ

学習のポイント

✅ パケットフィルタリングを中心に、用語の意味を覚えよう！

ネットワークセキュリティでは、ネットワークへの不正アクセス、不正利用、サービスの妨害などの脅威に対応するため、ファイアウォールで利用される**パケットフィルタリング**（P388参照）や、無線LANの**MACアドレスフィルタリング**（P396参照）以外に、次のような対策が取られています。

#### ①認証サーバ

認証サーバは、システムの正当な利用者であるか否かを判定する利用者認証に使用されるサーバです。

代表的な認証サーバに、**RADIUS**（Remote Authentication Dial In User Service）があります。

RADIUSは、無線LANやVPNに使用される認証サーバで、次の手順で利用者認証を行います。

ⅰ）利用者からの接続要求に応じてアクセスサーバが入力されたIDとパスワードを暗号化し、IDとパスワードを一元管理するRADIUSサーバに送ります。

ⅱ）RADIUSサーバは送られてきたIDとパスワードを確認し、正当な利用者であることが認められたら、アクセスサーバにその旨を返信します。

ⅲ）アクセスサーバは、RADIUSサーバからの返信内容を復号して結果を確認し、利用者の接続を許可します。

|  |
| --- |
| 例題  無線LANやVPN接続などで利用され，利用者を認証するためのシステムはどれか。  ア　DES イ　DNS ウ　IDS エ　RADIUS  ア　DESは、共通鍵暗号方式の代表的なアルゴリズムの１つでIBMが開発しました。  イ　DNSは、ドメインアドレスをIPアドレスに変換するシステムです。  ウ　IDSは、不正アクセスを検知するためのシステムです。  基本情報　平成21年度秋　問40　[出題頻度：★☆☆]  解答－エ |

#### ②VLAN（Virtual LAN：仮想LAN）

VLANは、LANスイッチ（スイッチングハブやレイヤ２スイッチ、レイヤ３スイッチ）がもつ機能を利用して、端末（ホスト）の物理的な接続形態とは別に、仮想的なグループを構成する方法です。ホストの物理的な位置にとらわれずLANを構成できるので、ホストを移動しても設定を変更する必要はありません。また、データが不要なLANに流れるというセキュリティ上の問題も防ぐことができます。

VLANの構成方法には、イーサネットのフレームのヘッダに格納されるプロトコルの情報を使用するプロトコルVLANや、LANで使用されるIEEE802.1xなどの認証機構を利用した認証VLANなどがあります。

#### ③VPN（Virtual Private Network）

Chapter10ネットワークで学習したVPNも、セキュリティ上で重要な技術の一つです（P324参照）。

#### ④セキュリティ監視

セキュリティ監視は、ネットワークのセキュリティログを監視し、不正アクセスを検知し対応します。

#### ⑤ハニーポット

ハニーポットは、クラッカーからの攻撃の内容を観察するために、ホストやシステムにわざと公開するセキュリティ上の脆弱性です。ハニーポットは必ずDMZに設置し、ファイアウォールなどの基本的なセキュリティ対策を整えて、侵入を検知したら速やかに警報を鳴らし、侵入者の行動記録（アクセスログ）をとります。

|  |
| --- |
| 例題  侵入者やマルウェアの挙動を調査するために，意図的に脆弱性をもたせたシステム又はネットワークはどれか。  ア　DMZ イ　SIEM ウ　ハニーポット エ　ボットネット  ア　DMZは、ファイアウォールの設置により、外部ネットワークからも内部ネットワークからも隔離された場所です。  イ　SIEMは、サーバやネットワーク機器などのログデータを一括管理、分析して、セキュリティ上の脅威を発見、通知するシステムです。  エ　ボットネットは、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です。  基本情報　平成31年度春　問44　[出題頻度：★☆☆]  解答－ウ |

#### ⑥リバースプロキシ

リバースプロキシは、特定のサーバへのリクエストを中継するプロキシサーバ（代理サーバ）です。

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に認証・許可の機能をもたせることでシングルサインオンを実現することができます。なお、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。

プロキシ

サーバ

Web

サーバ

クライアント

①リクエスト

②リクエスト

③データ

④データ

## 4. データベースセキュリティ

🏋プラスアルファ

**①データベースアクセス制御**

データベースアクセス制御は、「need-to-know（最小権限）」の原則に従って、利用者ごとにデータベースのアクセス権を与えることで、権限を越えたデータベースへの不正侵入を防ぐ仕組みです。

**②データベース暗号化**

データベース暗号化は、データベースへの不正侵入があった場合にも、データの盗聴を防ぐために行われます。

**③データベースバックアップ**

データベースバックアップは、事故や災害でデータベースに障害が発生したり、データベースへの不正侵入に伴いデータの破壊や改ざんが行われた場合に備えて、定期的に行う必要があります。

**④ログの取得**

ログの取得は、適切にデータベースアクセス制御が行われているかを確認し、万が一、障害が発生した場合の原因究明とデータベースの復旧のために必要です。

## 5. アプリケーションセキュリティ

学習のポイント

✅ 出題頻度を参考に効率よく学習しよう！

アプリケーションセキュリティでは、システムへの不正侵入、データの盗聴、破壊、改ざんなどの脅威に対応するために次のような対策が取られています。

🏋プラスアルファ

**①Webシステムのセキュリティ対策**

Webシステムのセキュリティ対策には、クロスサイトスクリプティングやSQLインジェクションなどのWebサイト内の情報の書き換えや漏えいといった攻撃への対策、DoS攻撃やDDoS攻撃などWebサイトへのアクセスを不可能にする攻撃への対策、フィッシングなどによるWebサイトの乗っ取り攻撃への対策などがあります。

具体的には、セキュリティパッチの適用、不要なサービスの停止、セキュアプログラミングの導入、ファイアウォールやWAFの導入、IDSやIPSの導入などが挙げられます。

**②セキュアプログラミング**

セキュアプログラミングは、アプリケーションを開発する際に、クラッカーなどの攻撃をあらかじめ想定し、対策を立てて攻撃されても正しく動作する脆弱でないプログラムを記述することです。また、システムの企画・設計段階からセキュリティを確保できるように考慮する方法を**セキュリティバイデザイン**と呼びます。

**③脆弱性低減技術**

脆弱性低減技術に、ソースコード静的検査、プログラムの動的検査、ファジング、エクスプロイトコードなどがあります。

**ソースコード静的検査**は、ソフトウェアの内部構造に注目し、ソースコードの構文を機械的にチェックするホワイトボックス検査を行うことで、脆弱性を見つける検査手法です。エクスプロイトコードは、ソフトウェアやハードウェアの脆弱性を検査するために作成されたプログラムです。

**プログラムの動的検査**は、一般に知られている攻撃パターンを送信し、プログラムの動きを観察することで、脆弱性を見つける検査手法です。

**ファジング**は、ソフトウェアのデータの入出力に注目し、問題を引き起こしそうなデータを大量に多様なパターンで入力して挙動を観察することで、脆弱性を見つける検査手法です。

|  |
| --- |
| 例題🏋プラスアルファ  ファジングに該当するものはどれか。  ア　サーバにFIN パケットを送信し，サーバからの応答を観測して，稼働しているサービスを見つけ出す。  イ　サーバのOS やアプリケーションソフトウェアが生成したログやコマンド履歴などを解析して，ファイルサーバに保存されているファイルの改ざんを検知する。  ウ　ソフトウェアに，問題を引き起こしそうな多様なデータを入力し，挙動を監視して，脆弱性を見つけ出す。  エ　ネットワーク上を流れるパケットを収集し，そのプロトコルヘッダやペイロードを解析して，あらかじめ登録された攻撃パターンと一致するものを検出する。  ア　ポートスキャンの説明です。  イ　ログ解析の説明です。  エ　パターンマッチングの説明です。  基本情報　令和4年度サンプル　問34　[出題頻度：★☆☆]  解答－ウ |

別冊演習ドリル 》 1-819,820

🏋プラスアルファ

**④パスワードクラック対策**

代表的なパスワードクラック対策に**ソルト**があります。

ソルトは、パスワードの推測を困難にする目的で、パスワードを暗号化する際に末尾に付加されるデータです。

**⑤バッファオーバフロー対策**

Ｃ言語などで記述したプログラムでは、プログラムが確保したメモリ領域（バッファ）のサイズを超えて文字列が入力されるとメモリ領域があふれ（オーバフロー）てしまい、予期しない動作が起こります。これがバッファオーバフロー（buffer overflow）です。

**バッファオーバフロー攻撃**は、特定のサーバに大量のデータを送信してメモリ領域をあふれさせて、システムを停止させる行為や、あふれ出たデータを実行させる行為です。

バッファオーバフロー対策を開発者側と利用者側でまとめると次のようになります。

・開発者側の対策

プログラミングに当たり、転記する文字列が転記先の領域に収まること、文字列の終端にナル文字が付加されること、ループカウンタの値が行き過ぎないことなどに注意します。

・利用者側の対策

バッファオーバフローは、プログラムのバグによって発生します。したがって、これを防ぐには、ソフトウェアメーカが用意するパッチ（修正プログラム）を当てるか、バージョンアップで対応します。また、ネットワーク経由での攻撃を防ぐためにも、ファイアウォールなどを導入して不要なネットワークアクセスを制限します。さらに、プログラムの脆弱性によるバッファオーバフローの危険性を少なくする意味から、不要なサービスプログラムを停止します。

#### ⑥SQLインジェクション対策

SQLインジェクション（P338参照）は、Webページ上の入力フォームに、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する行為です。

データベース内のレコードに含まれる情報の改ざん、消去、盗聴などの被害が考えられます。

SQLインジェクション対策には、入力フォームの入力データから、HTMLタグやJavaScript、SQL文などを検出し、その中に含まれる「＆」や「＜」などの特殊文字を一般の文字列に置き換える操作（**エスケープ処理**）を行うことで無害化（**サニタイジング**）することが有効です。また、これを自動的に行うデータベースの機能に**バインド機構**があります。

バインド機構とは、SQL文をあらかじめコンパイルしておき、そこに入力フォームからの入力データを値としてのみ組み入れる方式です。バインド機構を使用すると、Webアプリケーションから送られてくる値は必ず変数として扱うので、SQLに不正なコマンドが含まれていても、意図していない操作は実行されません。

|  |
| --- |
| 例題  SQLインジェクション攻撃による被害を防ぐ方法はどれか。  ア　入力された文字が，データベースへの問合せや操作において，特別な意味をもつ文字として解釈されないようにする。  イ　入力にHTML タグが含まれていたら，HTML タグとして解釈されない他の文字列に置き換える。  ウ　入力に上位ディレクトリを指定する文字列（../）が含まれているときは受け付けない。  エ　入力の全体の長さが制限を超えているときは受け付けない。  イ　クロスサイトスクリプティング対策に関する記述です。  ウ　ディレクトリトラバーサル対策に関する記述です。  エ　バッファオーバーフロー対策に関する記述です。  基本情報　令和4年度サンプル　問36　[出題頻度：★☆☆]  解答－ア |

別冊演習ドリル 》 1-821

🏋プラスアルファ

**⑦クロスサイトスクリプティング対策**

クロスサイトスクリプティング（P338参照）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行為です。

クロスサイトスクリプティング対策には、エスケープ処理を行うことでサニタイジングすることが有効です。

|  |
| --- |
| 例題🏋プラスアルファ  クロスサイトスクリプティング対策に該当するものはどれか。  ア　WebサーバでSNMPエージェントを常時稼働させることによって，攻撃を検知する。  イ　WebサーバのOSにセキュリティパッチを適用する。  ウ　Webページに入力されたデータの出力データが，HTMLタグとして解釈されないように処理する。  エ　許容量を超えた大きさのデータをWebページに入力することを禁止する。  ア　不正アクセス対策に関する記述です。  イ　OSコマンドインジェクションに関する記述です。  エ　バッファオーバーフロー対策に関する記述です。  応用情報　平成30年度秋　問41　[出題頻度：★☆☆]  解答－ウ |

🏋プラスアルファ

**⑧セッションハイジャック対策**

セッションハイジャック（P339参照）は、他人が確立したネットワークを横取りして使用する目的で、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、不正にアクセスする行為です。

セッションハイジャック対策には、類推が難しいセッションIDやセッションクッキーを使う、これらの有効期間を短くするなどの方法があります。また、個人情報の漏えいなどに被害が拡大しないようにするために、重要な情報を表示する画面の直前で追加的にパスワードによる利用者認証を行うようにします。

|  |
| --- |
| 例題🏋プラスアルファ  Webシステムにおいて，セッションの乗っ取りの機会を減らすために，利用者のログアウト時にWebサーバ又はWebブラウザにおいて行うべき処理はどれか。ここで，利用者は自分専用のPCにおいて，Webブラウザを利用しているものとする。  ア　WebサーバにおいてセッションIDをディスクに格納する。  イ　WebサーバにおいてセッションIDを無効にする。  ウ　WebブラウザにおいてキャッシュしているWebページをクリアする。  エ　WebブラウザにおいてセッションIDをディスクに格納する。  セッションハイジャックを防ぐには、類推が難しいセッションIDやセッションクッキーを使ったり、これらの有効期間を短くしたりします。また、利用者のログアウト時にはWebサーバにおいてセッションIDを無効にします。  応用情報　平成30年度春　問43　[出題頻度：★☆☆]  解答－イ |

🏋プラスアルファ

**⑨DNSキャッシュポイズニング対策**

DNSキャッシュポイズニング（P339参照）は、DNSにおいてドメイン情報を蓄積しているキャッシュDNSサーバに偽の情報を蓄積させる行為です。

DNSキャッシュポイズニング対策には、対応パッチを適応する、外部向けDNSサーバの台数を増やす、不特定多数のクライアントからの再帰的な名前解決問合せに応えるオープンリゾルバ設定を禁止し内部ネットワークからのものだけに応答するように設定する、問合せパケットのIDを固定せずにランダム化するなどの方法があります。

|  |
| --- |
| 例題🏋プラスアルファ  DNSキャッシュサーバに対して外部から行われるキャッシュポイズニング攻撃への対策のうち，適切なものはどれか。  ア　外部ネットワークからの再帰的な問合せにも応答できるように，コンテンツサーバにキャッシュサーバを兼ねさせる。  イ　再帰的な問合せに対しては，内部ネットワークからのものだけを許可するように設定する。  ウ　再帰的な問合せを行う際の送信元のポート番号を固定する。  エ　再帰的な問合せを行う際のトランザクションIDを固定する。  ア　外部からの再帰的な問合せには応答しない設定にします。  ウ　送信元のポート番号を固定しても対策にはなりません。  エ　トランザクションIDを固定しても対策にはなりません。  応用情報　平成30年度秋　問39　[出題頻度：★☆☆]  解答－イ |