

【応用\_午前\_過去問】セキュリティ④

情報システムへの脅威とセキュリティ対策の組合せのうち、適切なものはどれか。

平成18年春期 問75

151問目／選択範囲の問題数237問

	脅威	セキュリティ対策
ア	地震と火災	フォールトトレラント方式のコンピュータによるシステムの二重化
イ	データの物理的な盗難と破壊	ディスクアレイやファイアウォール
ウ	伝送中のデータへの不正アクセス	HDLC プロトコルの CRC
エ	メッセージの改ざん	公開鍵暗号方式を応用したデジタル署名

ア

イ

ウ

エ

## □分類

テクノロジ系 » セキュリティ » 情報セキュリティ対策

## □正解

**エ** “あなたの解答：エ”

## □解説

- ア** 地震と火災の規模が大きいとシステムが物理的に破壊されてしまう可能性があるので、コンピュータ内での二重化は有効な対策ではありません。
- イ** ディスクアレイは複数の磁気ディスク装置を組み合わせることで大容量化、信頼性の向上、アクセス速度の向上などを図る技術、ファイアウォールは、ネットワーク外からの不正パケットを遮断する技術ですが、両方とも盗難や物理的破壊などが発生したデータを復元することはできません。データを物理的な破壊から守るには、別の媒体へのバックアップ、盗難から守るには媒体に保存されているデータの暗号化やコンピュータにセキュリティワイヤを取り付けるなどの方法が有効です。
- ウ** HDLC(High-Level Data Link Control)は、高効率・高信頼性の伝送制御手順です。CRCはHDLCに採用されている誤り検出方式なので不正アクセスの対策にはなりません。
- エ** 正しい。デジタル署名は、公開鍵暗号方式を使ってデジタル文書の正当性を保証する技術で、「発信元が正当であるか」と「改ざんの有無」の2点を確認することができます。

JIS Q 27000:2019(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。

令和4年春期 問43

152問目／選択範囲の問題数237問

- 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

## □分類

テクノロジ系 » セキュリティ » 情報セキュリティ管理

## □正解

**イ** “あなたの解答：エ”

## □解説

**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”

脆弱性の定義です。

**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”

**正しい**。リスクレベルの定義です。リスクは影響度と発生確率の積で大きさを見積もります。

**ウ** “対応すべきリスクに付与する優先順位”

この記述に対応する用語はありません。

**エ** “リスクの重大性を評価するために目安とする条件”

リスク基準の定義です。

公開鍵基盤とハッシュ関数を使用したメッセージ認証の手法はどれか。

平成18年秋期 問73

153問目／選択範囲の問題数237問

- ア 受信者は、送信者の公開鍵とハッシュ関数を用いてハッシュ値を復号し、メッセージを得る。
- イ 受信者は、ハッシュ関数を用いてメッセージからハッシュ値を生成し、送信者の公開鍵で復号したハッシュ値と比較する。
- ウ 送信者は、自分の公開鍵とハッシュ値を用いてメッセージからハッシュ値を生成し、メッセージとともに送信する。
- エ 送信者は、ハッシュ関数を用いて送信者の秘密鍵のハッシュ値を生成し、メッセージとともに送信する。

## □分類

テクノロジ系 » セキュリティ » 情報セキュリティ

## □正解

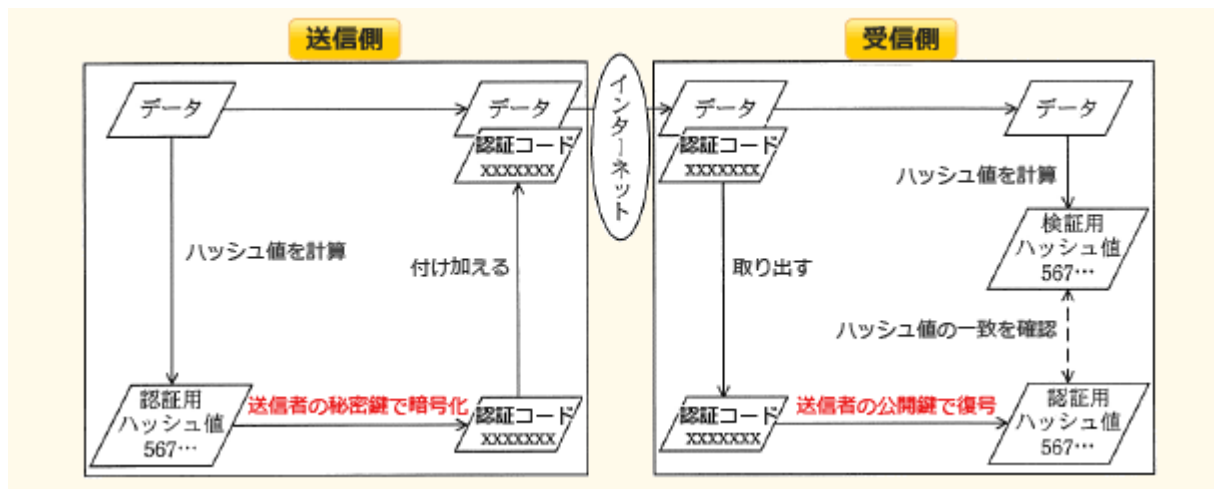
イ “あなたの解答：イ”

## □解説

ハッシュ関数を利用したメッセージ認証の手順は以下の通りです。

1. 送信者は、メッセージにハッシュ関数を適用してハッシュ値を生成する。
2. 送信者は、自分の**秘密鍵**でハッシュ値を暗号化しメッセージ認証コードを得る。
3. 送信者は、メッセージと認証コードを合わせて受信者に送信する。
4. 受信者は、送信者の公開鍵に付された認証局の公開鍵を用いて、その正当性を確認する。**(送信者の正当性を確認)**
5. 受信者は、送信者の**公開鍵**を用いてメッセージ認証コードを復号する。
6. 受信者は、受け取ったメッセージに(送信者と同じ)ハッシュ関数を適用してハッシュ値を生成する。
7. 受信者は、復号された認証コードと自分が生成したハッシュ値を比較し、同一であれば改ざんがないと判断する。**(改ざんの検知)**

以上の手順で受信したメッセージに改ざんがないこと、および送信者の正当性を確認します。



**ア** “受信者は、送信者の公開鍵とハッシュ関数を用いてハッシュ値を復号し、メッセージを得る。”

ハッシュ値は一方方向性の関数なので、ハッシュ値から元のメッセージを得ることはできません。

**イ** “受信者は、ハッシュ関数を用いてメッセージからハッシュ値を生成し、送信者の公開鍵で復号したハッシュ値と比較する。”

正しい手順です。

**ウ** “送信者は、自分の公開鍵とハッシュ値を用いてメッセージからハッシュ値を生成し、メッセージとともに送信する。”

ハッシュ値の生成には送信者の秘密鍵を使用します。

**エ** “送信者は、ハッシュ関数を用いて送信者の秘密鍵のハッシュ値を生成し、メッセージとともに送信する。”

ハッシュ値は元のメッセージをハッシュ化したものです。

ディレクトリトラバーサル攻撃に該当するものはどれか。

平成21年春期 問42

154問目／選択範囲の問題数237問

- ア Webアプリケーションの入力データとしてデータベースへの命令文を構成するデータを入力し、想定外のSQL文を実行する。
- イ Webサイトに利用者を誘導して、Webサイトの入力データ処理の欠陥を悪用し、利用者のブラウザで悪意のあるスクリプトを実行する。
- ウ 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。
- エ セッションIDによってセッションが管理されるとき、ログイン中の利用者のセッションIDを不正に取得し、その利用者に成りすましてアクセスする。



## □分類

テクノロジ系 » セキュリティ » 情報セキュリティ

## □正解

ウ “あなたの解答：ウ”

## □解説

ディレクトリトラバーサル攻撃は、ユーザーが入力したファイル名をパラメータとして受け取り、それをもとに処理を行うアプリケーションに対して行われる攻撃行為です。相対パス指定において親ディレクトリを表す(..)など、システムが想定外のファイル名を指定することで、本来秘匿にされているファイルを不正に閲覧及び取得することを目的としています。

ア “Webアプリケーションの入力データとしてデータベースへの命令文を構成するデータを入力し、想定外のSQL文を実行する。”

SQLインジェクションの説明です。

イ “Webサイトに利用者を誘導して、Webサイトの入力データ処理の欠陥を悪用し、利用者のブラウザで悪意のあるスクリプトを実行する。”

XSS(クロスサイトスクリプティング)の説明です。

ウ “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。”

正しい。ディレクトリトラバーサル攻撃の説明です。

エ “セッションIDによってセッションが管理されるとき、ログイン中の利用者のセッションIDを不正に取得し、その利用者に成りすましてアクセスする。”

セッションハイジャックの説明です。

ISMS適合性評価制度における詳細管理策の基となった国際規格はどれか。

平成17年春期 問78

155問目／選択範囲の問題数237問

ア ISO 9001

イ ISO 14001

ウ ISO/IEC 15408

エ ISO/IEC 17799

## □分類

テクノロジー系 » セキュリティ » 情報セキュリティ管理

## □正解

**エ** “あなたの解答：ウ”

## □解説

ISO/IEC 17799は、情報セキュリティ対策を行う際の実践規範を記したものであり、ベストプラクティスとして様々な管理策が記載されています。ISO/IEC17799:2000は、JIS X 5080:2002としてJIS化され、ISMS適合性評価制度におけるISMS認証基準のベースになりました。その後JIS Q 27002としてJIS規格化されています。

**ア** “ISO 9001”

ISO 9001は、組織の品質マネジメントシステムの要求事項を定めた国際標準規格です。

**イ** “ISO 14001”

ISO 14001は、組織の環境マネジメントシステムの要求事項を定めた国際標準規格です。

**ウ** “ISO/IEC 15408”

ISO/IEC 15408は、情報技術の製品及びシステムのセキュリティ特性を評価するための標準を定めた国際規格です。

**エ** “ISO/IEC 17799”

正しい。

受信した電子メールの送信元ドメインが詐称されていないことを検証する仕組みであるSPF (Sender Policy Framework)の特徴はどれか。

平成28年秋期 問43

156問目／選択範囲の問題数237問

- ア 受信側のメールサーバが、受信メールの送信元IPアドレスから送信元ドメインを検索してDNSBLに照会する。
- イ 受信側のメールサーバが、受信メールの送信元IPアドレスと、送信元ドメインのDNSに登録されているメールサーバのIPアドレスとを照合する。
- ウ 受信側のメールサーバが、受信メールの送信元ドメインから送信元メールサーバのIPアドレスを検索してDNSBLに照会する。
- エ メール受信者のPCが、送信元ドメインから算出したハッシュ値と受信メールに添付されているハッシュ値とを照合する。

## □分類

テクノロジ系 » セキュリティ » セキュリティ実装技術

## □正解

イ

“あなたの解答：エ”

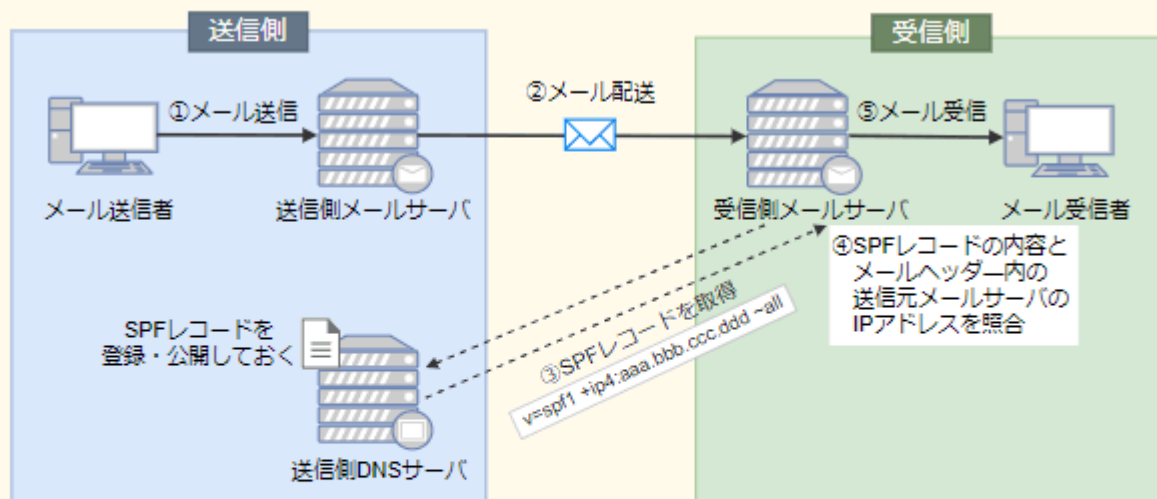
## □解説

SPF(Sender Policy Framework)は、メールを送信しようとしてきたメールサーバのIPアドレス情報を検証することで、正規のサーバからのメール送信であるかどうか確認することができる技術です。受信メールサーバ側がメールの送信元ドメインを管理するDNSサーバに問い合わせ、返されたIPアドレスが送信元メールサーバのIPアドレスと一致するかどうかでなりすましを検知します。

SPFでは以下の手順で送信元IPアドレスの検証を行います。

- ① 送信側は、送信側ドメインのDNSサーバのSPFレコード(またはTXTレコード)に正当なメールサーバのIPアドレスやホスト名を登録し、公開しておく。
- ② 送信側から受信側へ、SMTPメールが送信される。
- ③ 受信側メールサーバは、受信側ドメインのDNSサーバを通じて、MAIL FROMコマンドに記載された送信者メールアドレスのドメインを管理するDNSサーバに問い合わせ、SPF情報を取得する。
- ④ SPF情報との照合でSMTP接続してきたメールサーバのIPアドレスの確認に成功すれば、正当なドメインから送信されたと判断する。

### SPF (Sender Policy Framework)



したがって正しい記述は「イ」です。

【参考】

A社のWebサーバは、サーバ証明書を使ってTLS通信を行っている。PCからA社のWebサーバへのTLSを用いたアクセスにおいて、当該PCがサーバ証明書を入手した後に、認証局の公開鍵を利用して行う動作はどれか。

平成29年春期 問37

157問目／選択範囲の問題数237問

- ア 暗号化通信に利用する共通鍵を生成し、認証局の公開鍵を使って暗号化する。
- イ 暗号化通信に利用する共通鍵を、認証局の公開鍵を使って復号する。
- ウ サーバ証明書の正当性を、認証局の公開鍵を使って検証する。
- エ 利用者が入力して送付する秘匿データを、認証局の公開鍵を使って暗号化する。

## □分類

テクノロジ系 » セキュリティ » 情報セキュリティ

## □正解

ウ “あなたの解答：ウ”

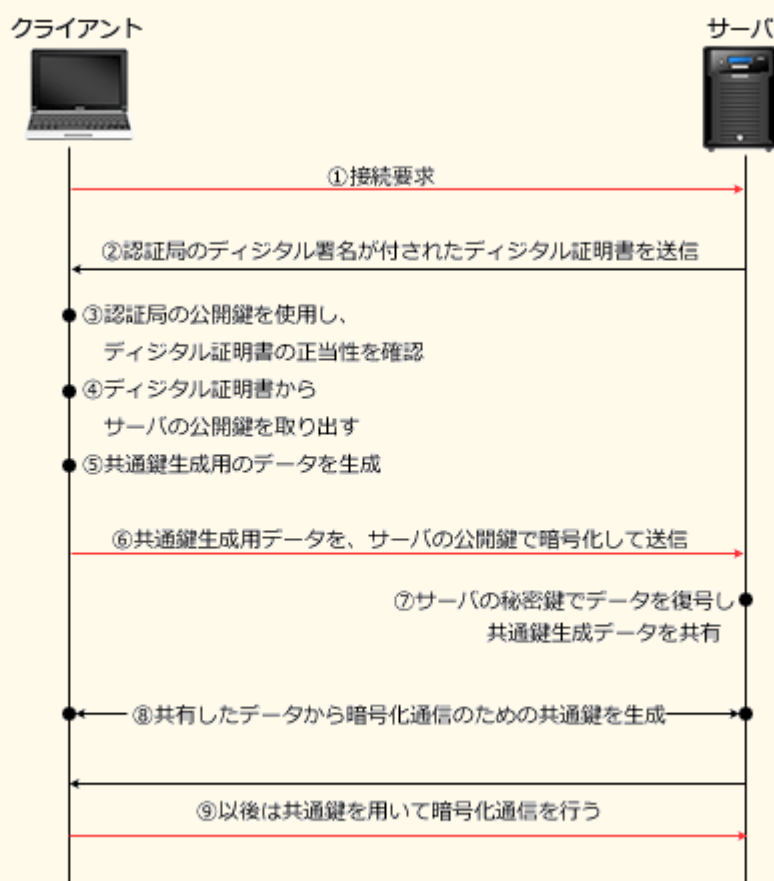
## □解説

サーバ証明書は、TLS暗号化通信の開始に先立ち、サーバからクライアントに送られる公開鍵に対する電子式の証明書で、認証局(CA)と呼ばれる第三者機関によって発行されています。サーバ証明書には、認証を受けた公開鍵が含まれていて、その信頼性を担保するために認証局のデジタル署名が付されています。

サーバ証明書を提示された利用者は、暗号化通信の開始に際し「認証局の公開鍵」を使用してサーバ証明書に付された「認証局のデジタル署名」を検証します。デジタル署名の検証に成功したならば、同封されている公開鍵が正当であり、かつ、改ざんされていないことが保証されます。

したがって正しい動作は「ウ」です。

SSL/TLSでは公開鍵の検証後、その公開鍵を使って通信相手と共通鍵を共有します（RSA方式の鍵交換の場合）。そして、以降はその共通鍵を使用して暗号化通信を行います。



経済産業省“個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン”の物理的安全管理措置に該当するものはどれか。

平成20年秋期 問77

158問目／選択範囲の問題数237問

- ア 個人情報の安全管理にかかわる従業員の役割及び責任についての教育・訓練を実施する。
- イ 個人データの漏えいなどの事故が発生した場合の、代表者などへの報告連絡体制を整備する。
- ウ 個人データを取り扱う情報システムへのアクセスの成功と失敗の記録を取得する。
- エ 個人データを取り扱う情報システムを、ICカードによる入退出管理を実施している室内に配置する。



## □分類

テクノロジ系 » セキュリティ » 情報セキュリティ対策

## □正解

**エ** “あなたの解答：エ”

## □解説

**個人情報の保護に関するガイドライン**は、個人情報保護法を踏まえ経済産業分野における事業者等が行う個人情報の適正な取扱いの確保に関する活動を支援する具体的な指針として定められたものです。

個人情報保護法第20条に「個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない」と定められているように、個人情報取扱事業者は安全管理措置を講じる必要があります。

ガイドラインでは、安全管理措置を「組織的」「人的」「物理的」および「技術的」の4つに分類して望まれる管理措置を記述しています。

**ア** “個人情報の安全管理にかかわる従業員の役割及び責任についての教育・訓練を実施する。”

人的安全管理措置です。

**イ** “個人データの漏えいなどの事故が発生した場合の、代表者などへの報告連絡体制を整備する。”

組織的安全管理措置です。

**ウ** “個人データを取り扱う情報システムへのアクセスの成功と失敗の記録を取得する。”

技術的安全管理措置です。

**エ** “個人データを取り扱う情報システムを、ICカードによる入退出管理を実施している室内に配置する。”

**正しい**。物理的安全管理措置です。

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)、そのデジタル署名を生成し、デジタル署名と結合データの組(デ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。

平成27年秋期 問37

159問目／選択範囲の問題数237問

- 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

## □分類

テクノロジ系 » セキュリティ » 情報セキュリティ

## □正解

**エ** “あなたの解答：エ”

## □解説

設問の手順は「タイムスタンプ」の仕組みを説明したものです。

**タイムスタンプ**は、対象とする電子文書に対して、信頼できる第三者機関である時刻認証局(TSA:Time Stamp Authority)が発行する時刻情報を含んだ電子データです。タイムスタンプは、付与時点での**存在性**、およびその時刻以後の**完全性**を証明することを目的としています。

結合データに付されたデジタル署名が正当なものであるということは「結合データが第三者機関によって作成され、改ざんされていないこと」を意味するため、結合データ内のハッシュ値に対応するファイルがその日時に存在し、その日時以降に改ざんされていないことが証明されます。

したがって「エ」が正解です。

タイムビジネス推進協議会ガイドラインではタイムスタンプを「特定の電子情報と時刻情報を結合する事により、その時刻以前にその電子データが存在していたことの証明（存在証明）とその時刻までの間にその電子情報が変更・改ざんされていないことの証明（非改ざん証明）することができる手段、およびその証拠に結びつく情報」と定義しています。

デ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。

平成27年秋期 問43

160問目／選択範囲の問題数237問

- 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の法的な証拠性を確保できるように、原因究明に必要な情報の保全、収集、分析をすること

## □分類

テクノロジ系 » セキュリティ » 情報セキュリティ対策

## □正解

**エ** “あなたの解答：エ”

## □解説

デジタルフォレンジックスは、不正アクセスや情報漏えいなどのセキュリティインシデントの発生時に、原因究明や法的証拠を保全するために対象となる電子的記録を収集・解析することです。分析の結果は、訴訟や内部懲戒に至った場合の証拠となったり、運用上の問題を是正するための活動に役立てたりします。

したがって「エ」が適切な記述です。

**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”

電子メールフィルタリングの説明です。

**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”

ファイアウォールなどの説明です。

**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”

上書きによる物理フォーマットの説明です。

**エ** “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確保できるように、原因究明に必要な情報の保全、収集、分析をすること”

**正しい。** デジタルフォレンジックスの説明です。

公開鍵暗号方式の暗号アルゴリズムはどれか。

平成27年秋期 問40

161問目／選択範囲の問題数237問

ア AES

イ KCipher-2

ウ RSA

エ SHA-256

## □分類

テクノロジ系 » セキュリティ » 情報セキュリティ

## □正解

ウ

“あなたの解答：ウ”

## □解説

ア “AES”

Advanced Encryption Standardの略。アメリカ合衆国の次世代暗号方式として規格化された共通鍵暗号方式です。

イ “KCipher-2”

ケーサイファー・ツーと読みます。2007年に九州大学とKDDI研究所により共同開発された共通鍵暗号方式です。

ウ “RSA”

**正しい。** RSA(Rivest Shamir Adleman)は、桁数が大きい合成数の素因数分解が困難であることを安全性の根拠とした公開鍵暗号の一つです。数字の桁数がそのまま安全強度につながるため、実際のRSAでは合成数の元となる2つの素数に150～300もの桁数の数を使用します。

エ “SHA-256”

Secure Hash Algorithm 256の略。入力データから256ビットのハッシュ値を出力するハッシュ関数です。

自社製品の脆弱性に起因するリスクに対応するための社内機能として、最も適切なものはどれか。

令和6年春期 問39

162問目／選択範囲の問題数237問

ア CSIRT

イ PSIRT

ウ SOC

エ WHOISデータベースの技術連絡担当



## □分類

テクノロジ系 » セキュリティ » 情報セキュリティ管理

## □正解

**イ** “あなたの解答：ア”

## □解説

### **ア** “CSIRT”

CSIRTは、対象とする範囲でセキュリティ上の問題が起きていないかどうかを監視するとともに、発生したセキュリティインシデントについて対応するチームや組織の総称です。

### **イ** “PSIRT”

**正しい。** PSIRTは、製品セキュリティインシデント対応チームです。P = Product、すなわち自社が開発・販売する製品、ソリューション、コンポーネント、サービスなどを対象として、脆弱性リスクの特定や評価を行い、発生したセキュリティインシデントについて対応するチームや組織の総称です。いわば自社製品版のCSIRTです。

### **ウ** “SOC”

SOCは、システムが発するアラートやセキュリティインシデントの予兆を専門のスタッフが24時間365日体制で監視し、インシデント発生時にはCSIRTへ報告を行うとともに支援を行う機関、または組織内の部署です。

### **エ** “WHOISデータベースの技術連絡担当”

WHOISデータベースの技術連絡担当は、co.jpやor.jpなどの属性型ドメインに関する技術的な問い合わせ先としてWhoIsデータベースで公開されている担当者情報です。脆弱性情報の受付窓口としては機能しますが、リスク対応にはなりません。

デジタル署名に用いる鍵の組合せのうち、適切なものはどれか。

平成26年秋期 問36

163問目／選択範囲の問題数237問

	デジタル署名の 作成に用いる鍵	デジタル署名の 検証に用いる鍵
ア	共通鍵	秘密鍵
イ	公開鍵	秘密鍵
ウ	秘密鍵	共通鍵
エ	秘密鍵	公開鍵

ア

イ

ウ

エ

## □分類

テクノロジ系 » セキュリティ » 情報セキュリティ

## □正解

エ “あなたの解答：エ”

## □解説

デジタル署名は、公開鍵暗号方式の技術を使って通信内容が改ざんされていないことと、送信者の正当性を確認する技術です。デジタル署名の作成と検証の手順は以下のとおりです。

1. 送信者は、平文をハッシュ関数で圧縮したメッセージダイジェストを**送信者の秘密鍵**で暗号化し、平文と一緒に送信する。
2. 受信者は、受信したメッセージダイジェストを**送信者の公開鍵**で復号し、受信した平文をハッシュ関数で圧縮したものと比較する。
3. 送信者から送られてきたメッセージダイジェストと、受信側でハッシュ化したメッセージダイジェストが同じなら、通信内容が改ざんされていないことが証明される。

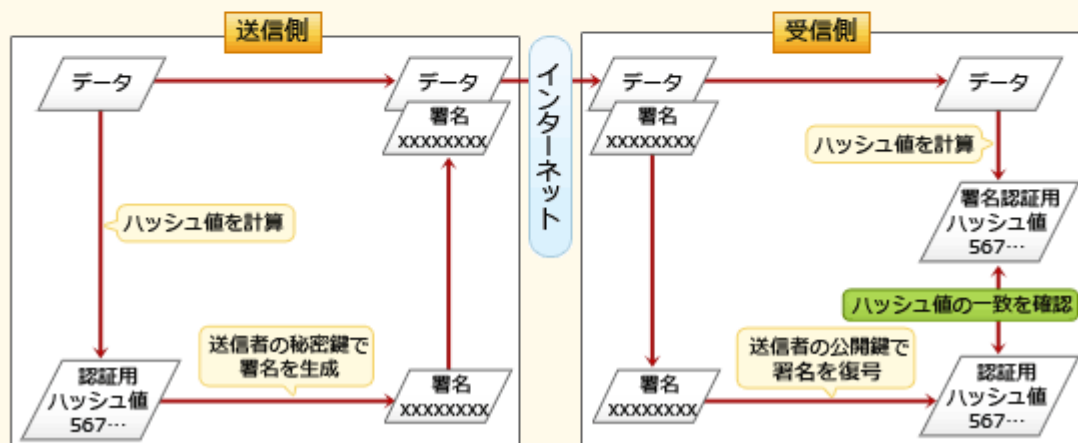


図 デジタル署名の生成～検証の手順

公開鍵暗号方式における暗号化通信では、送信者が公開鍵で暗号化、受信者が秘密鍵で復号を行います。デジタル署名では逆に送信者がメッセージダイジェストを**秘密鍵で暗号化**し、受信者がメッセージダイジェストを**公開鍵で復号**することになっているのがポイントです。

デジタル署名の作成に用いるのは**秘密鍵**、検証に用いるのは**公開鍵**なので、適切な組合せは「エ」です。

公開鍵暗号方式を使った暗号通信をn人が相互に行う場合、全体で何個の異なる鍵が必要になるか。ここで、一組の公開鍵と秘密鍵は2個と数える。

令和6年春期 問38

164問目／選択範囲の問題数237問

ア  $n+1$

イ  $2n$

ウ  $\frac{n(n-1)}{2}$

エ  $\log_2 n$

## □分類

テクノロジ系 » セキュリティ » 情報セキュリティ

## □正解

**イ** “あなたの解答：イ”

## □解説

公開鍵暗号方式を使った暗号通信では、復号鍵(秘密鍵)を正規の受信者が保持し、暗号化鍵(公開鍵)を複数の送信者に向けて公開します。暗号化は誰でもできますが、正しく復号できるのは正規の受信者のみなので通信内容を秘匿にすることができます。

この方式では、一組の秘密鍵と公開鍵を用意するだけで、受信者1人が不特定多数の送信者と暗号通信を行うことができます。n人が相互に暗号通信する場合、秘密鍵を保持する受信者はn人なので必要となる秘密鍵はn個です。さらに、n個の秘密鍵に対応する公開鍵がn個必要になるため、鍵の総数は「 $n + n = 2n$ 個」となります。したがって「イ」が正解です。

なお、共通鍵暗号方式でn人が相互に暗号化通信を行うには、 $\frac{n(n-1)}{2}$ 個（n人から2人を選ぶ組合せと同数）の鍵が必要となります。

	共通鍵暗号方式	公開鍵暗号方式
暗号化と復号の鍵	同じ	異なる
鍵の配送	手間が掛かる	必要なし
処理速度（計算量）	速い（少ない）	遅い（多い）
秘密に管理する鍵	両方	秘密鍵のみ
代表的なアルゴリズム	AES、DES、RC4	RSA、楕円曲線暗号、エルガマル暗号
n人相互の暗号化通信で必要な鍵数	$\frac{n(n-1)}{2}$	$2n$

3Dセキュア2.0(EMV 3-Dセキュア)は、オンラインショッピングにおけるクレジットカード決済時に、不正取引を防止するための本人認証サービスである。3Dセキュア2.0で利用される本人認証の特徴はどれか。

令和6年春期 問35

165問目／選択範囲の問題数237問

- ア 利用者がカード会社による本人認証に用いるパスワードを忘れた場合でも、安全にパスワードを再発行することができる。
- イ 利用者の過去の取引履歴や決済に用いているデバイスの情報から不正利用や高リスクと判断される場合に、カード会社が追加の本人認証を行う。
- ウ 利用者の過去の取引履歴や決済に用いているデバイスの情報にかかわらず、カード会社がパスワードと生体認証を併用した本人認証を行う。
- エ 利用者の過去の取引履歴や決済に用いているデバイスの情報に加えて、操作しているのが人間であることを確認した上で、カード会社が追加の本人認証を行う。

## □分類

テクノロジー系 » セキュリティ » 情報セキュリティ対策

## □正解

イ

“あなたの解答：イ”

## □解説

3Dセキュアは、ネットショッピングなどの非対面でクレジットカードを利用するときに、不正利用を防ぐために本人確認を行う仕組みです。カード決済の際、カード番号や有効期限、セキュリティコード以外に、事前に登録したパスワードの入力を求められることがあります。これが3Dセキュアです。“3D”とは加盟店、カード発行会社とカード会員、国際カードブランドの三者を指します。

従来の3Dセキュア(3Dセキュア1.0)では全ての取引においてパスワード入力が必要でしたが、3Dセキュア2.0ではリスクベース認証が導入され、過去の利用履歴や利用端末などから“リスクが高い”と判断された取引だけに、本人認証を要求するように変更されています。これにより利用者にとっては入力軽減、加盟店にとっては「カゴ落ち（決済時の離脱）」の防止というメリットがあります。また、認証方法としてよりセキュアなワンタイムパスワード・生体認証・QRコードスキャンの採用、クレジットカード以外のモバイルアプリ上での決済にも対応したなどの変更もあります。クレジットカードの不正利用が増加していることを受けて、3Dセキュア2.0は、2025年3月末までに全てのEC事業者で導入が義務化されることになっています。

**ア** “利用者がカード会社による本人認証に用いるパスワードを忘れた場合でも、安全にパスワードを再発行することができる。”

パスワード再発行の仕組みは提供しません。

**イ** “利用者の過去の取引履歴や決済に用いているデバイスの情報から不正利用や高リスクと判断される場合に、カード会社が追加の本人認証を行う。”

**正しい。** リスクベース認証が導入されたのが3Dセキュア2.0の特徴です。

**ウ** “利用者の過去の取引履歴や決済に用いているデバイスの情報にかかわらず、カード会社がパスワードと生体認証を併用した本人認証を行う。”

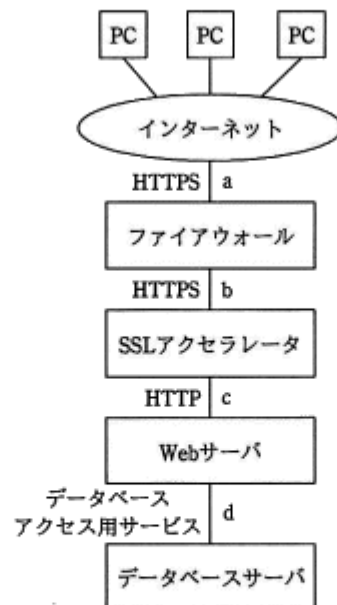
リスクベース認証なので、リスクが低いと判断された取引では追加の本人認証は行われません。

**エ** “利用者の過去の取引履歴や決済に用いているデバイスの情報に加えて、操作しているのが人間であることを確認した上で、カード会社が追加の本人認証を行う。”

リスクの評価に使われるのは、カード保有者情報・請求先情報・配送先情報・インターネット利用環境に関する情報などです。操作しているのが人間であるかどうかの情報は、リスクの評価に含まれません。なりすましやボットによる取引には別途対応する必要があります。



図のような構成と通信サービスのシステムにおいて、Webアプリケーションの脆弱性対策のためのWAFの設置場所として、最も適切な箇所はどこか。ここで、WAFには通信を暗号化したり復号したりする機能はないものとする。



平成29年春期 問43

166問目／選択範囲の問題数237問

ア a

イ b

ウ c

エ d

## □分類

テクノロジ系 » セキュリティ » 情報セキュリティ対策

## □正解

ウ

“あなたの解答：ウ”

## □解説

WAF(Web Application Firewall)は、通過するパケットのIPアドレスやポート番号だけでなくペイロード部(データ部分)をチェックすることで、Webアプリケーションに対する攻撃を検知し、攻撃と判断した通信をブロックするファイアウォールです。

WAFは、“シグネチャ(パターン)マッチング”や“HTTPヘッダーの検証”などによって不正なパケットを検知しますが、HTTPS通信が行われている経路上のパケットは暗号化されておりペイロード部分を見ることができないため、これらの検知手法が使えません。すなわちHTTPS通信が行われている「a」と「b」は設置場所として不適切です。

また、WAFによる不正アクセスの検知・遮断は、Webアプリケーションによって処理が実行される前に行われる必要があるので「d」は不適切です。

したがって適切な設置場所は「c」しかありません。

### 【参考】

SSLアクセラレータは、SSL/TLS通信におけるパケットの暗号化と復号を高速に行う専用のハードウェアで、Webサーバの処理負荷を軽減する目的で設置されます。

マルウェア対策ソフトでのフォールスネガティブに該当するものはどれか。

平成31年春期 問41

167問目／選択範囲の問題数237問

- ア マルウェアに感染していないファイルを，マルウェアに感染していないと判断する。
- イ マルウェアに感染していないファイルを，マルウェアに感染していると判断する。
- ウ マルウェアに感染しているファイルを，マルウェアに感染していないと判断する。
- エ マルウェアに感染しているファイルを，マルウェアに感染していると判断する。

## □分類

テクノロジ系 » セキュリティ » 情報セキュリティ対策

## □正解

**ウ** “あなたの解答：ウ”

## □解説

フォールスネガティブは、対をなすフォールスポジティブとともにマルウェア対策ソフトやIDS/IPSにおける誤検知の性質を表す言葉です。

### フォールスネガティブ（False Negative）

本来は検知すべき悪意のある活動を、誤って害のないものとして分類すること。いわゆる検知漏れ。多くなるほどコンピュータに影響を与え得る攻撃を通過させてしまう可能性が高くなる。

### フォールスポジティブ（False Positive）

本来は通過させるべき害のない活動を、誤って悪意のあるものとして分類すること。いわゆる過剰検知。多くなるほど正常な操作の阻害回数や管理者の負担が増える。

2つの発生数にはトレードオフの傾向がありますが、フィルタリングルールの調整によってどちらも最小になるように改善し続けることが求められます。

上記の性質を踏まえると、「ウ」がフォールスネガティブに該当すると判断できます。

**ア** “マルウェアに感染していないファイルを、マルウェアに感染していないと判断する。”

適切な処理であり、誤検知とは関係ありません。

**イ** “マルウェアに感染していないファイルを、マルウェアに感染していると判断する。”

フォールスポジティブに該当します。

**ウ** “マルウェアに感染しているファイルを、マルウェアに感染していないと判断する。”

**正しい。**フォールスネガティブに該当します。

**エ** “マルウェアに感染しているファイルを、マルウェアに感染していると判断する。”

適切な処理であり、誤検知とは関係ありません。

ダークネットは、インターネット上で到達可能であるが、使われていないIPアドレス空間を示す。このダークネットにおいて観測されるものはどれか。

令和元年秋期 問43

168問目／選択範囲の問題数237問

- ア インターネット上で公開されているWebサイトに対してWebブラウザから送信するパケット
- イ インターネットにつながっており、実在するIoT機器から実在するサーバに送信されるパケット
- ウ マルウェアがIoT機器やサーバなどの攻撃対象を探すために送信するパケット
- エ 有効な電子メールアドレスに対して攻撃者が標的型攻撃メールを送信するSMTPのパケット

## □分類

テクノロジー系 » セキュリティ » 情報セキュリティ

## □正解

ウ “あなたの解答：ウ”

## □解説

ダークネットは、インターネット上で到達可能かつ未使用のIPアドレス空間のことを指します。

通常のインターネット利用を考えれば特定のホストに割り当てられていない未使用のIPアドレス宛にパケットが送信されることは稀なはずですが、実際にダークネットを観測すると相当数のパケットが未使用のIPアドレス宛に送信されているようです。

これらは、

- マルウェアが次の感染対象を探すためのスキャン
- マルウェアが脆弱性を攻撃するためのパケット
- 送信元IPアドレスが詐称されたパケットへの応答パケット

などの不正な活動を目的とするパケットに因るものです。

ダークネットで観測されるパケットは、実際には使用されていないIPアドレスが宛先に設定されています。よって、マルウェアが総当たり的に次の攻撃対象を探すためのパケットが観測されます。

社内のセキュリティポリシーで、利用者の事故に備えて秘密鍵を復元できること、及びセキュリティ管理者の不正防止のための仕組みを確立することが決められている。電子メールで公開鍵暗号方式を使用し、鍵の生成はセキュリティ部門が一括して行っている場合、秘密鍵の適切な保管方法はどれか。

平成18年秋期 問72

169問目／選択範囲の問題数237問

- ア 1人のセキュリティ管理者が、秘密鍵を暗号化して保管する。
- イ 暗号化された秘密鍵の一つ一つを分割し、複数のセキュリティ管理者が分担して保管する。
- ウ セキュリティ部門には、秘密鍵を一切残さず、利用者本人だけが保管する。
- エ 秘密鍵の一覧表を作成し、セキュリティ部門内に限り参照できるように保管する。

## □分類

テクノロジー系 » セキュリティ » 情報セキュリティ管理

## □正解

**イ** “あなたの解答：エ”

## □解説

**ア** “1人のセキュリティ管理者が、秘密鍵を暗号化して保管する。”

鍵の生成はセキュリティ部門が一括して行っているので、セキュリティ管理者による不正の可能性あります。

**イ** “暗号化された秘密鍵の一つ一つを分割し、複数のセキュリティ管理者が分担して保管する。”

正しい。認証局などの特に重要なセキュリティが要求される機関は、秘密鍵の保管方法に記述のような秘密分散技術を用いています。

**ウ** “セキュリティ部門には、秘密鍵を一切残さず、利用者本人だけが保管する。”

事故が起こった場合の復元方法が考慮されていないので不適切です。

**エ** “秘密鍵の一覧表を作成し、セキュリティ部門内に限り参照できるように保管する。”

セキュリティ管理者による不正の可能性があるので不適切です。



化学製品を製造する化学プラントに、情報ネットワークと制御ネットワークがある。この二つのネットワークを接続し、その境界に、制御ネットワークのセキュリティを高めるためにDMZを構築し、制御ネットワーク内の機器のうち、情報ネットワークとの通信が必要なものをこのDMZに移した。DMZに移した機器はどれか。

令和3年秋期 問45

170問目／選択範囲の問題数237問

- ア 温度，流量，圧力などを計測するセンサー
- イ コントローラーからの測定値を監視し，設定値(目標値)を入力する操作端末
- ウ センサーからの測定値が設定値に一致するように調整するコントローラー
- エ 定期的にソフトウェアをアップデートする機器に対して，情報ネットワークから入手したアップデートソフトウェアを提供するパッチ管理サーバ

## □分類

テクノロジ系 » セキュリティ » 情報セキュリティ対策

## □正解

**エ** “あなたの解答：エ”

## □解説

近年の制御システムのオープン化、ネットワーク化に伴い、制御システムのセキュリティ脅威は増大しています。情報ネットワークで発生したマルウェア被害の影響を制御ネットワークに与えないために、情報ネットワークと制御ネットワークはできるだけ分離しておき、必要最小限の接続に留めることが大切です。

DMZに移すのは「情報ネットワークとの通信が必要なもの」です。選択肢のうち「エ」のパッチ管理サーバは、アップデートソフトウェアを情報ネットワークから入手するとありますから、これがDMZに移す機器であると判断できます。

公開鍵暗号方式に関する記述として、適切なものはどれか。

平成20年秋期 問71

171問目／選択範囲の問題数237問

- ア DESやAESなどの暗号方式がある。
- イ RSAや楕(だ)円曲線暗号などの暗号方式がある。
- ウ 暗号化鍵と復号鍵が同一である。
- エ 共通鍵の配送が必要である。

## □分類

テクノロジ系 » セキュリティ » 情報セキュリティ

## □正解

**イ** “あなたの解答：イ”

## □解説

公開鍵暗号方式は、暗号化と復号に異なる鍵を使用する暗号方式です。暗号化鍵は誰もが使用できるように公開しておき(公開鍵)、復号鍵は受信者が厳重に管理します(秘密鍵)。暗号化鍵と復号鍵は一对のペアとして生成され、1つの暗号化鍵で暗号化されたデータは、その鍵のペアである復号鍵でしか元のデータに戻せないため、復号を行えるのは正当な受信者のみであることが保証されています。

非常に大きな数の素因数分解が困難であることを利用した「RSA暗号」が公開鍵暗号の代表的存在ですが、この他にも楕円曲線上の演算規則を利用した「楕円曲線暗号」や、離散対数問題を応用した「エルガマル暗号」などがあります。

**ア** “DESやAESなどの暗号方式がある。”

DESやAESは共通鍵暗号方式の一種です。

**イ** “RSAや楕(だ)円曲線暗号などの暗号方式がある。”

**正しい。**

**ウ** “暗号化鍵と復号鍵が同一である。”

公開鍵暗号方式では、暗号化と復号に異なる鍵を使用します。

**エ** “共通鍵の配送が必要である。”

公開鍵暗号方式では、共通鍵は使用しません。

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。

平成27年春期 問37

172問目／選択範囲の問題数237問

- 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、偽装されたサーバにPCの利用者を誘導する。
- 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。

## □分類

テクノロジ系 » セキュリティ » 情報セキュリティ

## □正解

**イ** “あなたの解答：イ”

## □解説

**DNSキャッシュポイズニング**は、DNSサーバからの名前解決要求があった場合に正常な応答に加えて偽の名前解決情報（ドメイン情報）を付加して送信することで、そのサーバのキャッシュに偽の情報を登録させるという攻撃手法です。この汚染されたDNSサーバを利用したユーザーが、偽のキャッシュ情報をもとに悪意のあるサイトに誘導され、機密情報を盗まれるなどの被害が発生する可能性があります。

**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。”

攻撃のための情報を事前に収集するフットプリンティングの説明です。サーバソフトウェアのバージョン情報等の収集には、ポートスキャンツールが用いられることがあります。

**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、偽装されたサーバにPCの利用者を誘導する。”

**正しい。** DNSキャッシュポイズニング攻撃です。

**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。”

反射型DoS攻撃の一種であるDNSリフレクション攻撃の説明です。

**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。”

ゾーン転送を悪用した登録情報の収集です。

JIS X 9401:2016(情報技術－クラウドコンピューティング－概要及び用語)の定義によるクラウドサービス区分において、パブリッククラウドのクラウドサービスカスタマのシステム管理者が、仮想サーバのゲストOSに対するセキュリティパッチの管理と適用を実施可か実施不可かの組合せのうち、適切なものはどれか。

平成30年秋期 問38

173問目／選択範囲の問題数237問

	IaaS	PaaS	SaaS
ア	実施可	実施可	実施不可
イ	実施可	実施不可	実施不可
ウ	実施不可	実施可	実施不可
エ	実施不可	実施不可	実施可

ア

イ

ウ

エ

## □分類

テクノロジ系 » セキュリティ » 情報セキュリティ対策

## □正解

イ “あなたの解答：イ”

## □解説

JIS X 9401:2016では、クラウドコンピューティングのサービスモデル「SaaS」「PaaS」「IaaS」について次のように区分しています。

### SaaS (Software as a Service)

サービス利用者が、クラウドサービス提供者のアプリケーションを利用することができる形態

### PaaS (Platform as a Service)

サービス利用者が、クラウドサービス提供者によってサポートされる一つ以上のプログラミング言語と一つ以上の実行環境とを使って利用者が作った又は利用者が入手したアプリケーションを配置し、管理し、及び実行することができる形態

### IaaS (Infrastructure as a Service)

サービス利用者が、クラウドサービス提供者の演算リソース、ストレージリソース又はネットワークリソースを供給及び利用することができる形態

SaaS	事業者はアプリケーション以下を提供。利用者は機能を使い、アプリケーションにおける設定(カスタマイズ)も可能。
PaaS	事業者はミドルウェア以下を提供。利用者はアプリケーションを用意し、ミドルウェアにおける設定(カスタマイズ)も可能。
IaaS	1.事業者はOS以下を提供。利用者はミドルウェア以上を用意し、OSにおける設定(カスタマイズ)も可能。 2.事業者はハードウェア、ネットワークを提供。利用者はOS以上を用意。





3つのモデルのうち"OSに対する管理権限"を持つのはIaaSだけなので、IaaSだけがゲストOSに対するセキュリティパッチの管理と適用を実施可能です。したがって適切な組合せは「イ」になります。

なお、パブリッククラウドとクラウドサービスカスタマについては次のように定義されています。

### パブリッククラウド

クラウドサービスが任意のクラウドサービスカスタマに対して潜在的に利用可能であり、リソースはクラウドサービスプロバイダによって制御されているクラウド配置モデル  
 →つまり、資源を複数の利用者で共有する形態

### クラウドサービスカスタマ

クラウドサービスを使うためにビジネス関係にある自然人又は法人  
 →つまり、サービス利用者のこと

ペネトレーションテストの目的はどれか。

平成27年秋期 問45

174問目／選択範囲の問題数237問

- ア 暗号化で使用している暗号方式と鍵長が，設計仕様と一致することを確認する。
- イ 対象プログラムの入力に対する出力結果が，出力仕様と一致することを確認する。
- ウ ファイアウォールが単位時間あたりに処理できるセッション数を確認する。
- エ ファイアウォールや公開サーバに対して侵入できないかどうかを確認する。

## □分類

テクノロジー系 » セキュリティ » セキュリティ技術評価

## □正解

**エ** “あなたの解答：エ”

## □解説

ペネトレーションテスト(Penetration Test)は、ネットワークに接続されているシステムに対して、実際に様々な方法で侵入や攻撃を試みることで脆弱性の有無を検査するテストです。侵入テストとも呼ばれます。

システムの稼働開始時点では脆弱性がなくとも、システムの変更や更新の際の作業抜けや設定ミスによりセキュリティホールが内在している可能性があるため、定期的にテストを実施する必要があります。

**ア** “暗号化で使用している暗号方式と鍵長が、設計仕様と一致することを確認する。”

暗号モジュール試験の目的です。

**イ** “対象プログラムの入力に対する出力結果が、出力仕様と一致することを確認する。”

ブラックボックステストの目的です。

**ウ** “ファイアウォールが単位時間あたりに処理できるセッション数を確認する。”

負荷テストの目的です。

**エ** “ファイアウォールや公開サーバに対して侵入できないかどうかを確認する。”

**正しい。** ペネトレーションテストの目的です。

あるコンピュータセンターでは、インシデントを六つのタイプに分類した。

Scan：      プローブ、スキャン、そのほかの不審なアクセス

Abuse：     サーバプログラムの機能を悪用した不正中継

Forged：    送信ヘッダーを詐称した電子メールの配送

Intrusion： システムへの侵入

DoS：       サービス運用妨害につながる攻撃

Other：      その他

このとき、次の三つのインシデントに対するタイプの組合せのうち、適切なものはどれか。

インシデント1：ワームの攻撃が試みられた形跡があるが、侵入されていない。

インシデント2：ネットワークの輻輳(ふくそう)による妨害を受けた。

インシデント3：DoS 用の踏み台プログラムがシステムに設置されていた。

平成23年特別 問43

175問目／選択範囲の問題数237問

	インシデント1	インシデント2	インシデント3
ア	Abuse	DoS	Intrusion
イ	Abuse	Forged	DoS
ウ	Scan	DoS	Intrusion
エ	Scan	Forged	DoS

ア

イ

ウ

エ

## □分類

テクノロジ系 » セキュリティ » 情報セキュリティ

## □正解

ウ “あなたの解答：エ”

## □解説

[インシデント1について]

AbuseとScanのどちらかですが、インシデント1の内容はネットワーク内部への侵入を許したわけではなく「サーバの機能を悪用した不正中継」でもないので、不審なアクセスの項目がある**Scan**に分類されます。

[インシデント2について]

DoSとForgedのどちらかですが、Forgedは「送信ヘッダーを詐称した電子メールの配送」なので誤りであることがわかります。インシデント2「ネットワークの輻輳(ふくそう)による妨害を受けた」は、ネットワークの混雑がひどくなるとサービス提供に支障をきたす可能性もあるので**DoS**に分類されます。

[インシデント3について]

IntrusionとDoSのどちらかですが、不正なプログラムがシステムに設置されていたということは、システムへの侵入を許したことを示していますので**Intrusion**に分類されます。

認証局が侵入され、攻撃者によって不正なWebサイト用のデジタル証明書が複数発行されたおそれがある。どのデジタル証明書が不正に発行されたものか分からない場合、誤って不正に発行されたデジタル証明書を用いたWebサイトにアクセスしないために利用者側で実施すべき対策はどれか。

平成26年春期 問39

176問目／選択範囲の問題数237問

- ア Webサイトのデジタル証明書の有効期限が過ぎている場合だけアクセスを中止する。
- イ Webサイトへのアクセスログを確認し、ドメインがWhoisデータベースに登録されていない場合だけアクセスする。
- ウ 当該認証局のCP(Certificate Policy)の内容を確認し、セキュリティを考慮している内容である場合だけアクセスする。
- エ ブラウザで当該認証局を信頼していない状態に設定し、Webサイトのデジタル証明書に関するエラーが出た場合はアクセスを中止する。

## □分類

テクノロジ系 » セキュリティ » 情報セキュリティ

## □正解

**エ** “あなたの解答：ウ”

## □解説

攻撃された認証局から発行されたデジタル証明書は、正当か不正かの区別がつかない状態になってしまいます。

ブラウザには認証局について設定するオプションがあるので、攻撃された認証局を信頼できる機関から一旦除外します。これによって証明書が攻撃された認証局で発行されたものであった場合に、ブラウザはエラーメッセージを表示するようになるため、利用者に不正サイトへのアクセスを踏みとどまらせることができます。

**ア** “Webサイトのデジタル証明書の有効期限が過ぎている場合だけアクセスを中止する。”

不正なデジタル証明書の有効期限が切れているわけではないため、有効期限の検証に意味はありません。

**イ** “Webサイトへのアクセスログを確認し、ドメインがWhoisデータベースに登録されていない場合だけアクセスする。”

Whoisデータベースは、ドメイン名の登録時に入力された所有者や連絡先などの情報が登録されているデータベースです。ドメイン登録の有無とデジタル証明書の正当性には関連性がありません。

**ウ** “当該認証局のCP(Certificate Policy)の内容を確認し、セキュリティを考慮している内容である場合だけアクセスする。”

CP(Certificate Policy, 証明書ポリシー)は認証局が証明書を発行するときのポリシーです。ポリシーの内容と発行された証明書の正当性には関連がありません。

**エ** “ブラウザで当該認証局を信頼していない状態に設定し、Webサイトのデジタル証明書に関するエラーが出た場合はアクセスを中止する。”

**正しい。**

ドライブバイダウンロード攻撃の説明はどれか。

平成29年秋期 問40

177問目／選択範囲の問題数237問

- ア PCにUSBメモリが接続されたとき、USBメモリに保存されているプログラムを自動的に実行する機能を用いてマルウェアを実行し、PCをマルウェアに感染させる。
- イ PCに格納されているファイルを勝手に暗号化して、復号することと引換えに金銭を要求する。
- ウ 不正にアクセスする目的で、建物の外部に漏れた無線LANの電波を傍受して、セキュリティの設定が脆弱な無線LANのアクセスポイントを見つけ出す。
- エ 利用者がWebサイトを閲覧したとき、利用者に気付かれないように、利用者のPCに不正プログラムを転送させる。



## □分類

テクノロジ系 » セキュリティ » 情報セキュリティ

## □正解

**エ** “あなたの解答：エ”

## □解説

ドライブバイダウンロードは、Webサイトに悪意のあるプログラムを埋め込み、Webブラウザを通じて利用者が気付かないようにそのプログラムをダウンロードさせたり、自動的に実行させる攻撃です。脆弱性のある利用環境だとWebページを閲覧ただけでマルウェアの被害に遭うおそれがあります。ドライブバイダウンロードは、単独で攻撃に使用されることもありますし、また標的型攻撃や水飲み場攻撃などで補助的に使用されることもあります。

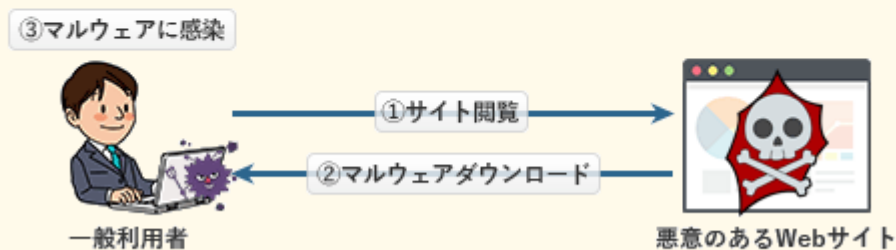


図 ドライブバイダウンロード攻撃

**ア** “PCにUSBメモリが接続されたとき、USBメモリに保存されているプログラムを自動的に実行する機能を用いてマルウェアを実行し、PCをマルウェアに感染させる。”

autorun.inf※を悪用して感染を試みるマルウェアの説明です。

※コンピュータにCDやUSBメモリが接続されたときに、自動起動するファイル名を記述するための設定ファイル

**イ** “PCに格納されているファイルを勝手に暗号化して、復号することと引換えに金銭を要求する。”  
ランサムウェアの説明です。

**ウ** “不正にアクセスする目的で、建物の外部に漏れた無線LANの電波を傍受して、セキュリティの設定が脆弱な無線LANのアクセスポイントを見つけ出す。”  
ウォードライビング(War Driving)の説明です。

**エ** “利用者がWebサイトを閲覧したとき、利用者に気付かれないように、利用者のPCに不正プログラムを転送させる。”  
**正しい。**ドライブバイダウンロード攻撃の説明です。

システム及び製品に関する情報技術セキュリティ評価基準の国際規格はどれか。

平成17年秋期 問79

178問目／選択範囲の問題数237問

ア ISO/IEC 13335

イ ISO/IEC 14516

ウ ISO/IEC 15408

エ ISO/IEC 17799

## □分類

テクノロジ系 » セキュリティ » セキュリティ技術評価

## □正解

ウ “あなたの解答：エ”

## □解説

ISO/IEC 15408は、情報技術の製品及びシステムのセキュリティ特性を評価するための国際規格です(JIS版は JIS X 5070)。評価対象はソフトウェアだけでなく、ハードウェア、ファームウェア、あるいは、システム全体も含まれます。また、製品の形態としては、ファイアウォールのように、直接セキュリティに関係する機能を提供する製品に限らず、オペレーティングシステム、データベース、あるいはグループウェアなど、保護すべき資源を保有する製品はすべて評価対象となります。

日本では ISO/IEC 15408に基づいて第三者機関が評価する「ITセキュリティ評価及び認証制度(JISEC)」がIPAにより運営されています。また、製品やシステムのセキュリティ特性は評価保証レベル(EAL: Evaluation Assurance Level)により7段階(EAL1～EAL7)に分類されています。

ア “ISO/IEC 13335”

ISO/IEC 13335は、情報通信技術セキュリティマネジメントの概念及びモデルに関する国際規格です。

イ “ISO/IEC 14516”

ISO/IEC 14516は、電子認証、電子公証、タイムスタンプ、暗号機能の鍵管理など、信頼できる第三者によるサービスに対しての利用と管理を規定した国際規格です。

ウ “ISO/IEC 15408”

正しい。

エ “ISO/IEC 17799”

ISO/IEC 17799は、情報セキュリティマネジメントにおける管理策のための国際規格です。

公開鍵暗号方式に関する記述のうち、適切なものはどれか。

平成22年秋期 問40

179問目／選択範囲の問題数237問

- ア AESは、NISTが公募した公開鍵暗号方式の一種である。
- イ RSAは、素因数分解の計算の困難さを利用した公開鍵暗号方式である。
- ウ 公開鍵暗号方式では利用者の数が増えると秘密鍵の配送先が増加する。
- エ 通信の秘匿に公開鍵暗号方式を使用する場合は、受信者の復号鍵を公開する。

## □分類

テクノロジ系 » セキュリティ » 情報セキュリティ

## □正解

**イ** “あなたの解答：イ”

## □解説

**ア** “AESは、NISTが公募した公開鍵暗号方式の一種である。”

AES(Advanced Encryption Standard)は、アメリカ合衆国の次世代暗号方式として規格化された**共通鍵**暗号方式です。旧国家暗号規格のDES(Data Encryption Standard)では鍵長が56ビットであったのに対して、AESでは鍵長が最大256ビットとなり暗号強度が高められています。

**イ** “RSAは、素因数分解の計算の困難さを利用した公開鍵暗号方式である。”

正しい。RSAは、桁数が大きい合成数の素因数分解が困難であることを安全性の根拠とした**公開鍵**暗号方式です。

**ウ** “公開鍵暗号方式では利用者の数が増えると秘密鍵の配送先が増加する。”

通信を行う人数が増えるにつれて鍵の管理が煩雑になるのは共通鍵暗号方式の特徴です。

**エ** “通信の秘匿に公開鍵暗号方式を使用する場合は、受信者の復号鍵を公開する。”

公開鍵暗号方式を使った暗号化通信において、平文の暗号化に使うのは公開鍵です。同じ公開鍵暗号の原理を利用するデジタル署名では、この場合とは逆に送信者が秘密鍵で署名を作成し、受信者が公開鍵で正当性を確認するので両者の違いを確認しておきましょう。

HTTPS通信において、暗号化とサーバ認証に使用されるものはどれか。

平成25年春期 問36

180問目／選択範囲の問題数237問

ア Cookie

イ S/MIME

ウ SSL/TLS

エ ダイジェスト認証

## □分類

テクノロジ系 » セキュリティ » セキュリティ実装技術

## □正解

ウ “あなたの解答：ウ”

## □解説

HTTPS(HTTP over SSL/TLS)は、WebサーバとWebブラウザがデータを安全に送受信するために、SSL/TLSプロトコルによって生成されるセキュアな接続上でデータのやり取り(HTTP通信)を行う方式です。

HTTPは、平文のままで情報をやり取りする仕様のため、個人情報の送信や電子決済などセキュリティが重要となる通信に使うことは危険が伴います。HTTPS通信では、SSL/TLSから提供される通信の暗号化、**ノードの認証**、改ざん検出などの機能を使用することで「なりすまし」や「盗聴」による攻撃から通信を保護することができるようになっています。

**ア** “Cookie”

Cookie(クッキー)は、Webサーバに対するアクセスがどのPCからのものであるかを識別するために、WebサーバやWebページの指示によってWebブラウザにユーザー情報などを保存する仕組みです。

**イ** “S/MIME”

Secure MIMEの略。暗号技術を使用して「認証」「改ざん検出」「暗号化」などの機能を電子メールソフトに提供する技術で、電子メールを盗聴や改ざんなどから守るために米国RSA Data Security社によって開発されました。

**ウ** “SSL/TLS”

**正しい。** HTTPS通信の暗号化とサーバ認証はSSL/TLSによって提供されます。

**エ** “ダイジェスト認証”

ダイジェスト認証は、ユーザー名とパスワードをMD5でハッシュ(ダイジェスト)化して送るHTTPの認証方法の1つです。

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

令和2年秋期 問40

181問目／選択範囲の問題数237問

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



## □分類

テクノロジ系 » セキュリティ » 情報セキュリティ

## □正解

**イ** “あなたの解答：イ”

## □解説

デジタル署名は、公開鍵暗号の技術を応用してデジタル文書の正当性を保証する仕組みです。送信するデジタル文書にデジタル署名を付けると、受信側で「発信元が正当であるか」と「改ざんの有無」の2点を確認することができます。ただし、改ざん部位の特定、および訂正の機能は有しません。

デジタル署名の生成には「送信者の秘密鍵」を使用し、受信側での検証には「送信者の公開鍵」を使用するため、設問中の署名検証鍵Xは「送信者の公開鍵」、署名生成鍵Yは「送信者の秘密鍵」に相当します。

**ア** “デジタル署名、文書ファイル及び署名検証鍵Xを比較することによって、文書ファイルに改ざんがあった場合、その部分を判別できる。”

改ざん部位を特定することはできません。

**イ** “文書ファイルが改ざんされていないこと、及びデジタル署名が署名生成鍵Yによって生成されたことを確認できる。”

**正しい。** デジタル署名の検証によって、改ざんの有無とデジタル署名が正当な署名生成鍵によって作成されたかどうかを確認できます。

**ウ** “文書ファイルがマルウェアに感染していないことを認証局に問い合わせて確認できる。”

デジタル署名はマルウェアに感染しているか否かを確認する仕組みではありません。

**エ** “文書ファイルとデジタル署名のどちらかが改ざんされた場合、どちらが改ざんされたかを判別できる。”

この場合、デジタル署名の検証が失敗に終わりますが、どちらが改ざんされたかを判別することはできません。

☆☆☆☆

シングルサインオンの説明のうち、適切なものはどれか。

平成24年秋期 問36

182問目／選択範囲の問題数237問

- ア クッキーを使ったシングルサインオンの場合、サーバごとの認証情報を含んだクッキーをクライアントで生成し、各サーバ上で保存、管理する。
- イ クッキーを使ったシングルサインオンの場合、認証対象のサーバを、異なるインターネットドメインに配置する必要がある。
- ウ リバースプロキシを使ったシングルサインオンの場合、認証対象のWebサーバを、異なるインターネットドメインに配置する必要がある。
- エ リバースプロキシを使ったシングルサインオンの場合、利用者認証においてパスワードの代わりにデジタル証明書を用いることができる。

## □分類

テクノロジ系 » セキュリティ » 情報セキュリティ

## □正解

**エ** “あなたの解答：ウ”

## □解説

シングルサインオン(Single Sign-On, SSO)は、ユーザー認証を一度受けるだけで許可された複数のサーバへのアクセスについても認証する技術です。実装方式としては、Cookieを使うもの、リバースプロキシ型などがあります。

### クッキーを使うSSO

1. 最初のログインの際には、Webサーバにインストールされたエージェントが認証サーバにアクセスで認証を行う。
2. その認証・識別情報をクッキーに含めクライアントに返す。
3. 別のWebサーバにアクセスがあった場合には、エージェントが認証サーバにアクセスしクッキー情報をもとに認証を行う。

### リバースプロキシ型SSO

1. すべてのWebサーバへのアクセスをリバースプロキシに集約する。
2. リバースプロキシはアクセスしてきたユーザーを認証する。
3. ログインに成功すると、リバースプロキシはWebサーバに代理アクセスし結果をユーザーに返す。

### SAML(Security Assertion Markup Language)を使うSSO

認証情報に加え、属性情報とアクセス制御情報を異なるドメインに伝達するためのWebサービスプロトコル。これを用いてほかのドメインとの間で認証情報を交換することで、同一ドメインに留まらない大規模なサイトにおいてもシングルサインオンの仕組みやセキュアな認証情報管理を実現できる。

- ア** “クッキーを使ったシングルサインオンの場合、サーバごとの認証情報を含んだクッキーをクライアントで生成し、各サーバ上で保存、管理する。”

クッキーはサーバで生成され、クライアントのコンピュータに保存されます。

- イ** “クッキーを使ったシングルサインオンの場合、認証対象のサーバを、異なるインターネットドメインに配置する必要がある。”

クッキーの有効範囲は同ドメイン内のページに限られています。異なるドメインに配置されたシステムは他のドメインで生成されたクッキーにアクセスすることができないので認証を行うことはできません。

- ウ** “リバースプロキシを使ったシングルサインオンの場合、認証対象のWebサーバを、異なるインターネットドメインに配置する必要がある。”

Webサーバには認証を行わないとアクセスできないようにしたいので、リバースプロキシと同ドメインに配置しなくてはなりません。

- エ** “リバースプロキシを使ったシングルサインオンの場合、利用者認証においてパスワードの代わりにデジタル証明書を用いることができる。”

**正しい。** IDとパスワードの組合せのほかにデジタル証明書が使用可能です。

☆☆☆☆☆

Webブラウザのcookieに関する設定と、それによって期待される効果の記述のうち、最も適切なものはどれか。

令和4年春期 問40

183問目／選択範囲の問題数237問

- ア サードパーティcookieをブロックする設定によって、当該Webブラウザが閲覧したWebサイトのコンテンツのキャッシュが保持されなくなり、閲覧したコンテンツが当該Webブラウザのほかの利用者に知られないようになる。
- イ サードパーティcookieをブロックする設定によって、当該Webブラウザが複数のWebサイトを閲覧したときにトラッキングされないようになる。
- ウ ファーストパーティcookieを承諾する設定によって、当該WebブラウザがWebサイトの改ざんをcookieのハッシュ値を用いて検知できるようになる。
- エ ファーストパーティcookieを承諾する設定によって、当該Webブラウザがデジタル証明書の失効情報を入手でき、閲覧中のWebサイトのデジタル証明書の有効性を確認できるようになる。

## □分類

テクノロジー系 » セキュリティ » セキュリティ実装技術

## □正解

**イ** “あなたの解答：ア”

## □解説

現在訪問しているWebサイトのドメインから発行されるクッキーがファーストパーティcookie、閲覧しているページ内の広告等の要素の配信とともに別ドメインから発行されるのがサードパーティcookie(第三者配信クッキー)です。

広告配信会社は、利用者の嗜好を把握して効果が高いと思われるターゲティング広告を配信するために、サードパーティcookieを利用して閲覧したWebサイトの情報を収集しています。クッキーによりWebサイトの閲覧履歴が収集されると、個人の興味や趣味、家族構成、住んでいる場所、年収や信条などが推測されてしまうことになり、これが行き過ぎた情報収集であるとしてプライバシー保護の観点から問題となっています。このような背景があり、Webブラウザの開発会社はサードパーティcookieを規制する動きを強めています。

**ア** “サードパーティcookieをブロックする設定によって、当該Webブラウザが閲覧したWebサイトのコンテンツのキャッシュが保持されなくなり、閲覧したコンテンツが当該Webブラウザのほかの利用者に知られないようになる。”

Webブラウザのシークレットモードやプライベートモードに関する記述です。cookieのブロックとWebブラウザ内の閲覧履歴の記録は無関係です。

**イ** “サードパーティcookieをブロックする設定によって、当該Webブラウザが複数のWebサイトを閲覧したときにトラッキングされないようになる。”

**正しい。** サードパーティcookieをブロックすることで、サイトを横断したトラッキングをさせないようにできます。

**ウ** “ファーストパーティcookieを承諾する設定によって、当該WebブラウザがWebサイトの改ざんをcookieのハッシュ値を用いて検知できるようになる。”

cookieとWebサイトの改ざん検知は無関係です。

**エ** “ファーストパーティcookieを承諾する設定によって、当該Webブラウザがデジタル証明書の失効情報を入手でき、閲覧中のWebサイトのデジタル証明書の有効性を確認できるようになる。”

cookieとデジタル証明書の失効情報とは無関係です。失効情報は、WebブラウザがCRLを確認することによって自動的に行われています。

●サードパーティ Cookie

：第三者ドメインが発行する Cookie

訪問したサイト以外の「第三者」ドメインが発行し、 これを使うと、ドメインをまたいだ広告出稿や  
トラッキングが可能

●トラッキング

：特定のユーザーが、サイト内でどこを閲覧しているのかを追跡、分析すること

クライアントとWebサーバの間において、クライアントからWebサーバに送信するデータを  
検査して、SQLインジェクションなどの攻撃を遮断するためのものはどれか。

平成23年秋期 問40

184問目／選択範囲の問題数237問

ア SSL-VPN機能

イ WAF

ウ クラスタ構成

エ ロードバランシング機能



## □分類

テクノロジー系 » セキュリティ » セキュリティ実装技術

## □正解

**イ** “あなたの解答：イ”

## □解説

パケットフィルター型ファイアウォールは、通過するパケットのIPアドレスとポート番号を見て通過の可否を決めます。しかしXSSやSQLインジェクションなどのWebアプリケーションに対する攻撃パケットは、正規のHTTP通信に則り、HTTPポート(80/TCP)宛てに送信されるため、パケットのヘッダー情報だけでは通常のHTTP通信との区別が付きません。このためパケットフィルター型ファイアウォールで、これらの攻撃を遮断することは困難です。

WAF(Web Application Firewall)は、Webアプリケーションの防御に特化したファイアウォールで、パケットのヘッダー部に含まれるIPアドレスやポート番号だけでなくペイロード部(データ部分)をチェックし、攻撃の兆候の有無を検証します。これによりWebアプリケーションに対する攻撃を検知し、遮断することが可能です。

### **ア** “SSL-VPN機能”

SSL-VPNは、VPN(Virtual Private Network)の一形態で、SSL技術による暗号化を行いWebブラウザ(https)を用いてVPN環境を構築する技術です。

### **イ** “WAF”

正しい。

### **ウ** “クラスタ構成”

クラスタ構成は、複数台のコンピュータを結合することで、1台のコンピュータでは得られない処理性能や可用性を得るものです。

### **エ** “ロードバランシング機能”

ロードバランシング機能は、複数台のサーバに処理を分散することで、負荷分散やサーバの利用効率の向上を行う機能です。

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。

令和3年春期 問44

185問目／選択範囲の問題数237問

- ☐ ア WebサーバにおいてセッションIDを内蔵ストレージに格納する。
- ☐ 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を内蔵ストレージに格納する。

## □分類

テクノロジ系 » セキュリティ » セキュリティ実装技術

## □正解

**イ** “あなたの解答：イ”

## □解説

IPAで公開されているセキュアプログラミング講座では、セッション乗っ取りの機会を低減させるための予防策として「セッションタイムアウト」と「明示的なログアウト機能」を挙げています。

### セッションタイムアウト

Webアプリケーションにはセッションタイムアウト機能を設ける。ユーザーはログアウト操作をすることを忘れてしまうことがある。

### 明示的なログアウトの機能

Webアプリケーションには明示的なログアウトの機能を設ける。できれば、各ページでログアウト操作が行えると良い。

そして利用者がログアウトを要求した場面では、Webアプリケーションは次のような操作を行うべきとしています。

- Webサーバ側でセッションIDを確実に無効にする。その後同じセッションIDがクライアントから送られてきても受け付けない
- Webブラウザ側のセッションIDを消去する

一般的なWebページのセッション管理方式では、WebブラウザとWebサーバでセッションIDを共有することで同じ利用者かどうかを判断しています。セッションIDさえ一致すれば、第三者からのアクセスを正規のアクセスとして判断してしまう可能性があるということです。不要なセッションIDを有効なままにしておくのはセキュリティ上のリスクになります。

セッションIDを必要とするのはログイン中だけです。ログアウトが要求された（セッションIDが不要になった）時点でWebサーバ側（可能であればWebブラウザも）のセッションIDを無効化し、それ以降は無効化されたセッションIDを拒否することで、セッション乗っ取りの機会を最小限に減らせます。

したがって適切な処理は「イ」です。

楕円曲線暗号に関する記述のうち、適切なものはどれか。

平成30年秋期 問37

186問目／選択範囲の問題数237問

- ア AESに代わる共通鍵暗号方式としてNISTが標準化している。
- イ 共通鍵暗号方式であり、デジタル署名にも利用されている。
- ウ 公開鍵暗号方式であり、TLSにも利用されている。
- エ 素因数分解問題の困難性を利用している。

## □分類

テクノロジ系 » セキュリティ » 情報セキュリティ

## □正解

**ウ** “あなたの解答：ウ”

## □解説

楕円曲線暗号は、楕円曲線の点の演算を用いた公開鍵暗号方式です。楕円曲線によって定義された有限可換群上の離散対数問題を解く際の計算量の多さを安全性の根拠とし、同じ強度を想定した場合、RSAより鍵長を短くできる利点があります。

**ア** “AESに代わる共通鍵暗号方式としてNISTが標準化している。”

楕円曲線暗号は公開鍵暗号方式です。

**イ** “共通鍵暗号方式であり、デジタル署名にも利用されている。”

楕円曲線暗号はデジタル署名のアルゴリズム“ECDSA”として利用されています。しかし、共通鍵暗号方式ではないので記述は誤りです。

**ウ** “公開鍵暗号方式であり、TLSにも利用されている。”

**正しい。** 認証及び鍵交換のアルゴリズムとしてTLSで利用されています。

**エ** “素因数分解問題の困難性を利用している。”

RSAの説明です。

ボットネットにおいてC&Cサーバが担う役割はどれか。

令和5年春期 問36

187問目／選択範囲の問題数237問

- ア 遠隔操作が可能なマルウェアに、情報収集及び攻撃活動を指示する。
- イ 攻撃の踏み台となった複数のサーバからの通信を制御して遮断する。
- ウ 電子商取引事業者などへの偽のデジタル証明書の発行を命令する。
- エ 不正なWebコンテンツのテキスト、画像及びレイアウト情報を一元的に管理する。

## □分類

テクノロジー系 » セキュリティ » 情報セキュリティ

## □正解

**ア** “あなたの解答：ア”

## □解説

C&Cサーバ(コマンド・コントロール・サーバ)は、マルウェアが侵入に成功したコンピュータ群(ボットネット)の動作を制御するために用いられる外部の指令サーバです。

マルウェアはC&Cサーバからの指令を受けて、乗っ取ったコンピュータで悪意のある活動を行います。単純に外部から内部ネットワークに存在するマルウェアに対して通信を試みてもFWなどで遮断されてしまうため、マルウェア側からC&Cサーバに対して定期的に問い合わせを行い、その応答を使って指令を行う仕組みが用いられています。この仕組みを「コネクトバック通信」といいます。

したがって、C&Cサーバの役割を説明した記述は「ア」です。

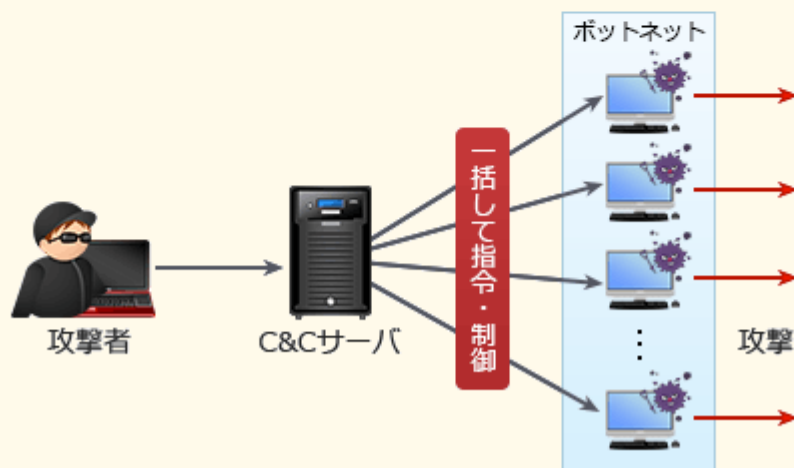


図 C&Cサーバ

SEOボイズニングの説明はどれか。

令和2年秋期 問39

188問目／選択範囲の問題数237問

- ア Web検索サイトの順位付けアルゴリズムを悪用して、検索結果の上位に、悪意のあるWebサイトを意図的に表示させる。
- イ 車などで移動しながら、無線LANのアクセスポイントを探し出して、ネットワークに不正侵入する。
- ウ ネットワークを流れるパケットから、侵入のパターンに合致するものを検出して、管理者への通知や、検出した内容の記録を行う。
- エ マルウェア対策ソフトのセキュリティ上の脆弱性を悪用して、システム権限で不正な処理を実行させる。



## □分類

テクノロジ系 » セキュリティ » 情報セキュリティ

## □正解

**ア** “あなたの解答：ア”

## □解説

SEO(Search Engine Optimization)とは、Webサイトを制作するときに、Googleなどの検索エンジンの検索結果において上位に表示されるようにページやサイト全体を最適化することをいいます。

上位表示を狙うサイトが普通のサイトであれば問題ないのですが、**SEOボイズニング**では、フィッシングサイトやマルウェアなどを仕込んだ悪意のあるページ（または悪意のあるページに移動させることを目的とするページ）に様々なSEO対策を施して検索結果の上位に表示させようとします。このような悪質なページが検索結果の上位に表示されると、何も知らずキーワード検索から訪れた利用者が、マルウェアのダウンロードや不正サイトへのリダイレクトなどの攻撃を受けることがあります。

**ア** “Web検索サイトの順位付けアルゴリズムを悪用して、検索結果の上位に、悪意のあるWebサイトを意図的に表示させる。”

**正しい。** SEOボイズニングの説明です。

**イ** “車などで移動しながら、無線LANのアクセスポイントを探し出して、ネットワークに不正侵入する。”

**ウォードライビング(War Driving)**の説明です。

**ウ** “ネットワークを流れるパケットから、侵入のパターンに合致するものを検出して、管理者への通知や、検出した内容の記録を行う。”

**IDSやIPSの説明です。**

**エ** “マルウェア対策ソフトのセキュリティ上の脆弱性を悪用して、システム権限で不正な処理を実行させる。”

**セキュリティホールを悪用した攻撃ですが、SEOボイズニングとは関係ありません。**

SIEM(Security Information and Event Management)の特徴はどれか。

平成29年秋期 問38

189問目／選択範囲の問題数237問

- ア DMZを通過する全ての通信データを監視し、不正な通信を遮断する。
- イ サーバやネットワーク機器のMIB(Management Information Base)情報を分析し、中間者攻撃を遮断する。
- ウ ネットワーク機器のIPFIX(IP Flow Information Export)情報を監視し、攻撃者が他者のPCを不正に利用したときの通信を検知する。
- エ 複数のサーバやネットワーク機器のログを収集分析し、不審なアクセスを検知する。

## □分類

テクノロジ系 » セキュリティ » 情報セキュリティ対策

## □正解

**エ** “あなたの解答：エ”

## □解説

SIEM(Security Information and Event Management)は、OS、データベース、アプリケーション、ネットワーク機器など多様なソフトウェアや機器が出力する大量のログデータを分析し、異常があった場合に管理者に通知したり対策を知らせたりする仕組みです。日本語ではセキュリティ情報およびイベント管理と訳されます。

したがって「エ」が適切な説明です。

**ア** “DMZを通過する全ての通信データを監視し、不正な通信を遮断する。”

ファイアウォールやIPSなどの特徴です。

**イ** “サーバやネットワーク機器のMIB(Management Information Base)情報を分析し、中間者攻撃を遮断する。”

SNMP(Simple Network Management Protocol)の特徴です。SNMPにはRMON(Remote network MONitoring)という通信状況を監視するMIBがあります。

**ウ** “ネットワーク機器のIPFIX(IP Flow Information Export)情報を監視し、攻撃者が他者のPCを不正に利用したときの通信を検知する。”

Cisco社のNetFlowの特徴です。

**エ** “複数のサーバやネットワーク機器のログを収集分析し、不審なアクセスを検知する。”

正しい。SIEMの特徴です。

100人の送受信者が共通鍵暗号方式で、それぞれ秘密に通信を行うときに必要な共通鍵の総数は幾つか。

平成18年秋期 問71

190問目／選択範囲の問題数237問

ア 200

イ 4,950

ウ 9,900

エ 10,000

## □分類

テクノロジー系 » セキュリティ » 情報セキュリティ

## □正解


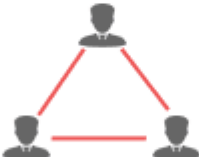


**イ** “あなたの解答：イ”

## □解説

共通鍵暗号方式では、送信者と受信者で共有している同じ鍵を使用するので、通信の組合せの数だけ異なる鍵が必要になります。

相互に通信を行う人数が2人の場合は1個、3人の場合は3個、4人の場合は6個、5人の場合は10個というように増えていきます。

n人が相互に共通鍵暗号通信を行う場合に必要となる鍵数

人数	2人	3人	4人	5人
鍵数	 1	 3	 6	 10

一般に共通鍵暗号方式においてn人が相互に通信を行う場合に必要となる鍵数は、

$$n(n-1)/2$$

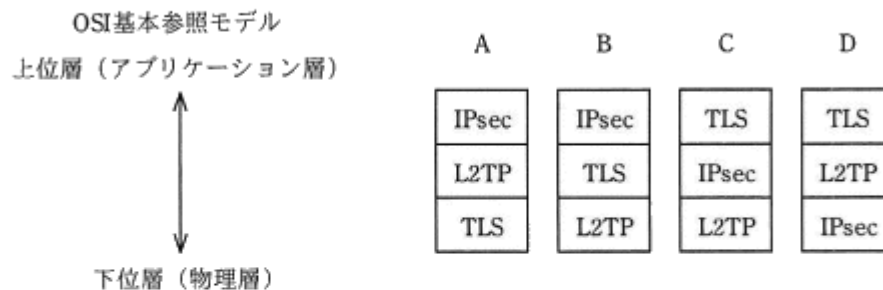
の公式で求めることができます。

nに100を当てはめると、

$$\begin{aligned} & 100(100-1)/2 \\ &= (100 \times 99)/2 \\ &= 9900/2 = 4950 \end{aligned}$$

**4950個**であることがわかります。

VPNで使用するセキュアなプロトコルであるIPsec, L2TP, TLSの, OSI基本参照モデルにおける相対的な位置関係はどれか。



平成31年春期 問42

191問目／選択範囲の問題数237問

ア A

イ B

ウ C

エ D

## □分類

テクノロジ系 » セキュリティ » セキュリティ実装技術

## □正解

ウ “あなたの解答：ウ”

## □解説

それぞれのセキュアプロトコルの特徴と位置する階層は次のとおりです。

### IPsec (IP Security)

IP(Internet Protocol)を拡張してセキュリティを高めたプロトコルで、改ざんの検知、通信データの暗号化および送信元の認証などの機能を、OSI基本参照モデルのネットワーク層レベル(TCP/IPモデルではIP層)で提供する。認証プロトコルAHや認証／暗号化プロトコルESPを含む

### L2TP (Layer 2 Tunneling Protocol)

PPPなどのフレームをIPヘッダーでカプセル化することで、ルータを越えた複数の拠点間でフレームのやり取りを実現するトンネリングプロトコル。暗号化の機能はないため必要に応じてIPsecと併用する必要がある。“レイヤ2”の名称どおり、OSI基本参照モデルの第2層のデータリンク層で動作する

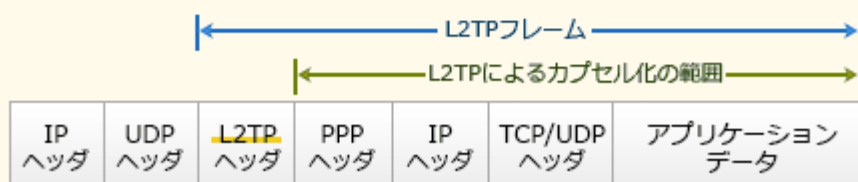


図 L2TPトンネリング

### TLS (Transport Layer Security)

通信の暗号化、デジタル証明書を利用した改ざん検出、ノード認証を含む統合セキュアプロトコル。その名のとおりOSI基本参照モデルのトランスポート層で動作する

IPsecはIPが属するネットワーク層(第3層)、L2TPはデータリンク層(第2層)、TLSはトランスポート層(第4層)にするので、適切な位置関係は上層から TLS→IPsec→L2TP の順です。したがって「C」が正解です。

ファジングに該当するものはどれか。

令和4年春期 問45

192問目／選択範囲の問題数237問

- 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ー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。



## □分類

テクノロジ系 » セキュリティ » セキュリティ技術評価

## □正解

ウ “あなたの解答：ア”

## □解説

ファジング(fuzzing)とは、検査対象のソフトウェア製品に「ファズ（英名：fuzz）」と呼ばれる問題を引き起こしそうなデータを大量に送り込み、その応答や挙動を監視することで(未知の)脆弱性を検出する検査手法です。

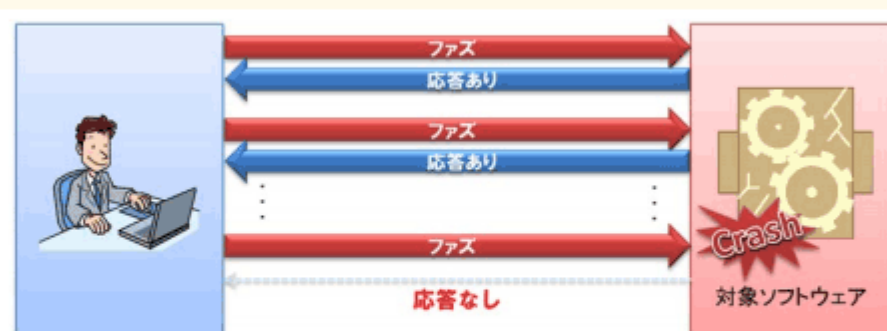


図 21-1 ファジングによる脆弱性検出イメージ

IPA資料「ファジング活用の手引き」より引用  
<http://www.ipa.go.jp/files/000051628.pdf>

ファジングは、ファズデータの生成、検査対象への送信、挙動の監視を自動で行うファジングツール(ファザー)と呼ばれるソフトウェアを使用して行います。開発ライフサイクルにファジングを導入することで「バグや脆弱性の低減」「テストの自動化・効率化によるコスト削減」が期待できるため、大手企業の一部で徐々に活用され始めています。

**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。”

ポートスキャンの説明です。

**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。”

ログ分析の説明です。

**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。”

**正しい。** ファジングの説明です。

**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ー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。”

パターンマッチングの説明です。

☆☆☆☆

クリプトジャッキングに該当するものはどれか。

令和2年秋期 問41

193問目／選択範囲の問題数237問

- ア PCにマルウェアを感染させ、そのPCのCPUなどが有する処理能力を不正に利用して、暗号資産の取引承認に必要となる計算を行い、報酬を得る。
- イ 暗号資産の取引所から利用者のアカウント情報を盗み出し、利用者になりすまして、取引所から暗号資産を不正に盗みとる。
- ウ カード加盟店に正規に設置されている、カードの磁気ストライプの情報を読み取る機器から、カード情報を窃取する。
- エ 利用者のPCを利用できなくし、再び利用できるようにするのと引換えに金銭を要求する。

## □分類

テクノロジ系 » セキュリティ » 情報セキュリティ

## □正解

**ア** “あなたの解答：ウ”

## □解説

クリプトジャッキングは、暗号資産を入手するために必要なマイニング作業（膨大な量のハッシュ値の計算）を、他人のコンピュータに秘密裏に行わせる行為です。コードを仕込んだマルウェアを感染させる方法、Webページのスクリプトにコードを仕込んでおき、訪れた利用者がページを閲覧している最中に計算させてしまう手法などがあります。計算資源や電気代の窃取であるとともに、過負荷による処理能力の低下やCPUの熱暴走を生じさせる点が問題となります。2017年に暗号資産が世界的に注目を浴びたことにより、クリプトジャッキングの被害が急増しました。

したがって「ア」が適切な記述です。

**ア** “PCにマルウェアを感染させ、そのPCのCPUなどが有する処理能力を不正に利用して、暗号資産の取引承認に必要となる計算を行い、報酬を得る。”

正しい。クリプトジャッキングの説明です。

**イ** “暗号資産の取引所から利用者のアカウント情報を盗み出し、利用者になりすまして、取引所から暗号資産を不正に盗みとる。”

クリプトジャッキングは、暗号資産を直接的に盗み取るわけではありません。

**ウ** “カード加盟店に正規に設置されている、カードの磁気ストライプの情報を読み取る機器から、カード情報を窃取する。”

スキミングの説明です。

**エ** “利用者のPCを利用できなくし、再び利用できるようにするのと引換えに金銭を要求する。”

ランサムウェアの説明です。

Webアプリケーションのセッションが攻撃者に乗っ取られ、攻撃者が乗っ取ったセッションを利用してアクセスした場合でも、個人情報の漏えいなどの被害が拡大しないようにするために、Webアプリケーションが重要な情報をWebブラウザに送信する直前に行う対策として、最も適切なものはどれか。

平成28年春期 問41

194問目／選択範囲の問題数237問

- ア Webブラウザとの間の通信を暗号化する。
- イ 発行済セッションIDをCookieに格納する。
- ウ 発行済セッションIDをURLに設定する。
- エ パスワードによる利用者認証を行う。

## □分類

テクノロジ系 » セキュリティ » セキュリティ実装技術

## □正解

**エ** “あなたの解答：ア”

## □解説

セッションハイジャック等によって、ログイン中のセッションが第三者に乘っ取られても、URLやCookieに格納されているセッションIDが正規のものである限り、Webアプリケーション側では「攻撃者によって乗っ取られたリクエスト」なのか「正規ユーザーによるリクエスト」なのかの区別が付きません。Webアプリケーション側で、このような不正処理を想定した対策がなされていないと、それを悪用した攻撃者によって正規ユーザーの意に反した処理が実行されてしまう恐れがあります。

特に「ログイン後に決済処理等の重要な処理を行うサイト」などでは、攻撃による被害が大きくなるため、セッション管理の堅牢性を高める必要があります。それに加えてセッションが乗っ取られた場合の不正処理を防ぐために、送金や購入確定、パスワード変更、秘密情報の表示、退会処理などの重要なリクエストをサーバに送信する前には、その**利用者が意図したリクエストであるかどうかを識別する仕組み**を設ける必要があります。

重要リクエストの送信直前に行われるパスワード認証には、現在のセッションの相手が正当なユーザーであることを確認し、セッションハイジャック等から生じた不正なリクエストを除外する効果があります。したがって適切な対策は「エ」です。

SQLインジェクション攻撃を防ぐ方法はどれか。

平成20年秋期 問73

195問目／選択範囲の問題数237問

- ア 入力値から、上位ディレクトリを指定する文字(../)を取り除く。
- イ 入力値から、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を解釈されないように保護する。
- ウ 入力値にHTMLタグが含まれていたら、解釈、実行できないほかの文字列に置き換える。
- エ 入力値の全体の長さが制限を超えていたときは受け付けない。

## □分類

テクノロジ系 » セキュリティ » セキュリティ実装技術

## □正解

**イ** “あなたの解答：イ”

## □解説

SQLインジェクション攻撃は、ユーザーからの入力をもとにSQL文を組み立てるウェブアプリケーションのセキュリティ上の不備を悪用して、データベースシステムを不正に操作するSQL文を発行させ、情報の不正取得やデータベースの破壊を行う攻撃です。SQLインジェクションを防ぐには、ユーザーの入力値の中でSQLにおいて特別な意味を持つ文字(単一引用符「'」やバックスラッシュ「\」など)を、無効化してからSQL文に組み込むことが重要かつ効果的な対策となります。

したがって「イ」が適切です。

**ア** “入力値から、上位ディレクトリを指定する文字(../)を取り除く。”

ディレクトリトラバーサル攻撃を防ぐ方法です。

**イ** “入力値から、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を解釈されないように保護する。”

**正しい。** SQLインジェクション攻撃を防ぐ方法です。

**ウ** “入力値にHTMLタグが含まれていたら、解釈、実行できないほかの文字列に置き換える。”

クロスサイトスクリプティング(XSS)を防ぐ方法です。

**エ** “入力値の全体の長さが制限を超えていたときは受け付けない。”

バッファオーバーフロー攻撃を防ぐ方法です。

暗号解読のための攻撃法のうち、ブルートフォース攻撃はどれか。

平成25年春期 問38

196問目／選択範囲の問題数237問

- ア 与えられた1組の平文と暗号文に対し、総当たりで鍵を割り出す。
- イ 暗号化関数の統計的な偏りを線形関数によって近似して解読する。
- ウ 暗号化装置の動作を電磁波から解析することによって解読する。
- エ 異なる二つの平文とそれぞれの暗号文の差分を観測して鍵を割り出す。



## □分類

テクノロジー系 » セキュリティ » 情報セキュリティ

## □正解

**ア** “あなたの解答：ア”

## □解説

ブルートフォース攻撃は、パスワード解析に用いられる手法の1つで、特定の文字数および文字種で設定される可能性のあるすべての組合せを試すことで不正ログインを試みる攻撃手法です。

パスワード長が短く、使用可能な文字種が少ない場合には、この手法によって破られる可能性が高くなってしまいます。

**ア** “与えられた1組の平文と暗号文に対し、総当たりで鍵を割り出す。”

**正しい。**

**イ** “暗号化関数の統計的な偏りを線形関数によって近似して解読する。”

暗号化関数の線形近似式を発見することを基本とした「線形解読法」の説明です。

**ウ** “暗号化装置の動作を電磁波から解析することによって解読する。”

サイドチャネル攻撃の説明です。

**エ** “異なる二つの平文とそれぞれの暗号文の差分を観測して鍵を割り出す。”

入力値の差分が出力値の差分にどのような影響を与えるかを分析して解読を試みる「差分解読法」の説明です。

JIS Q 31000:2019(リスクマネジメントー指針)におけるリスクアセスメントを構成するプロセスの組合せはどれか。

令和4年秋期 問41

197問目／選択範囲の問題数237問

ア リスク特定, リスク評価, リスク受容

イ リスク特定, リスク分析, リスク評価

ウ リスク分析, リスク対応, リスク受容

エ リスク分析, リスク評価, リスク対応

## □分類

テクノロジ系 » セキュリティ » 情報セキュリティ管理

## □正解

イ “あなたの解答：エ”

## □解説

リスクマネジメントの指針を示した規格であるJIS Q 31000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を網羅するプロセス全体を指す」と定義しています。

したがって、正しい組合せは「リスク特定、リスク分析、リスク評価」の3つです。

### リスク特定

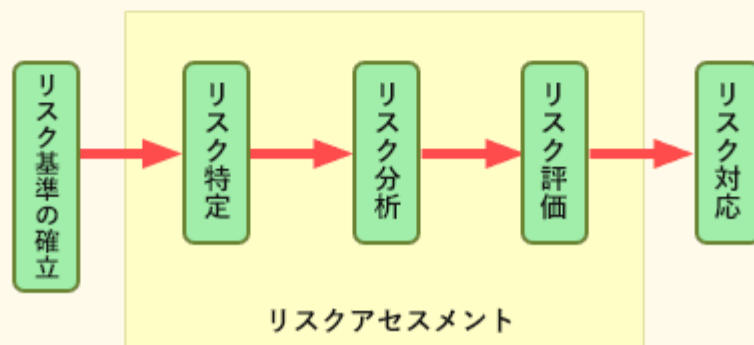
組織の目的の達成を助ける又は妨害する可能性のあるリスクを発見し、認識し、記述する

### リスク分析

必要に応じてリスクのレベルを含め、リスクの性質及び特徴を理解する

### リスク評価

リスク分析の結果と確立されたリスク基準との比較をし、追加する行為の決定を裏付ける



情報システムにおけるデータのオーナーに相当する部門として、適切なものはどれか。

平成17年春期 問73

198問目／選択範囲の問題数237問

- ア システム及びデータの維持管理を行っているシステム運用部門
- イ システム部門に開発，運用及び保守を委託している業務の主管部門
- ウ データのインテグリティを保証し，必要に応じてデータ内容の訂正を行う保守部門
- エ データを取り扱う画面や帳票のレイアウトを決定する利用部門

## □分類

テクノロジ系 » セキュリティ » 情報セキュリティ管理

## □正解

**イ** “あなたの解答：ア”

## □解説

データのオーナー部門とは、そのデータの管理や活用を主導し、データに対して監督責任をもつ部門のことです。

主管部門とは文字通り、主導的な立場に立ってその仕事の管理を行う部門のことなので、そのデータを用いた業務の主管部門と記述されている「イ」がデータのオーナーとして適切です。

クロスサイトスクリプティングによる攻撃へのセキュリティ対策はどれか。

平成18年秋期 問76

199問目／選択範囲の問題数237問

- ア OSのセキュリティパッチを適用することによって、Webサーバへの侵入を防止する。
- イ Webアプリケーションで、クライアントに入力データを再表示する場合、情報内のスクリプトを無効にする処理を行う。
- ウ WebサーバにSNMPプログラムを常駐稼働させることによって、攻撃を検知する。
- エ 許容範囲を超えた大きさのデータの書き込みを禁止し、Webサーバへの侵入を防止する。

## □分類

テクノロジ系 » セキュリティ » セキュリティ実装技術

## □正解

**イ** “あなたの解答：イ”

## □解説

クロスサイトスクリプティング(XSS)は、動的にWebページを生成するアプリケーションのセキュリティ上の不備を意図的に利用して、悪意のあるスクリプトを混入させることで、攻撃者が仕込んだ操作を実行させたり、別のサイトを横断してユーザーのクッキーや個人情報を盗んだりする攻撃手法です。

この攻撃に対する脆弱性は、ユーザーからの入力データ内に含まれる引用符やHTMLタグを無効せずにそのまま表示してしまうことが原因で生じるので、出力時にHTMLの特殊文字を適切にエスケープ(無効化)することで防ぐことができます。

米国で運用されたTCSECや欧州政府調達用のITSECを統合して、標準化が進められたCC(Common Criteria)の内容はどれか。

平成18年秋期 問79

200問目／選択範囲の問題数237問

- ☐ ア 暗号アルゴリズムの標準
- ☐ イ 情報技術に関するセキュリティの評価基準
- ☐ ウ 情報セキュリティ管理の実施基準
- ☐ エ セキュリティ管理のプロトコルの標準



## □分類

テクノロジ系 » セキュリティ » セキュリティ技術評価

## □正解

**イ** “あなたの解答：イ”

## □解説

CC(Common Criteria, 情報セキュリティ国際評価基準)は、IT製品やシステムのセキュリティ機能を評価し認証するための基準を定めた規格です。ほぼそのままの形でISO 15408(日本版では JIS X 5070)として国際標準化されています。

したがって適切な記述は「イ」です。

**ア** “暗号アルゴリズムの標準”

FIPS 140の説明です。

**イ** “情報技術に関するセキュリティの評価基準”

正しい。CCの説明です。

**ウ** “情報セキュリティ管理の実施基準”

情報セキュリティ管理基準の説明です。

**エ** “セキュリティ管理のプロトコルの標準”

IETFでRFCが発行されているSSL/TLS, IPsec, SSHなどの説明です。