【応用_午前_過去問】セキュリティ①

☆☆

オープンリダイレクトを悪用した攻撃に該当するものはどれか。

令和3年秋期　問44
1問目／選択範囲の問題数237問

ア　HTMLメールのリンクを悪用し，HTMLメールに，正規のWebサイトとは異なる偽のWebサイトのURLをリンク先に指定し，利用者がリンクをクリックすることによって，偽のWebサイトに誘導する。

イ　Webサイトにアクセスすると自動的に他のWebサイトに遷移する機能を悪用し，攻撃者が指定した偽のWebサイトに誘導する。

ウ　インターネット上の不特定多数のホストからDNSリクエストを受け付けて応答するDNSキャッシュサーバを悪用し，攻撃対象のWebサーバに大量のDNSのレスポンスを送り付け，リソースを枯渇させる。

エ　設定の不備によって，正規の利用者以外からの電子メールやWebサイトへのアクセス要求を受け付けるプロキシを悪用し，送信元を偽った迷惑メールの送信を行う。

❑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

オープンリダイレクトは、URLパラメータやフォームデータなどの外部パラメータによって指定されたWebページに遷移するようにしているWebアプリケーションが、実装不備により、無制限にURLを受け入れてしまう状態です。攻撃者がこの脆弱性を悪用することで、利用者は、気付かないうちに信頼できるWebサイトから悪意のあるWebサイトに誘導されてしまい、誘導した先でフィッシングなどの被害に遭う危険があります。

ア “HTMLメールのリンクを悪用し，HTMLメールに，正規のWebサイトとは異なる偽のWebサイトのURLをリンク先に指定し，利用者がリンクをクリックすることによって，偽のWebサイトに誘導する。”

標的型攻撃メールやフィッシングの例です。
HTMLでは、表示上のURLと実際のリンク先URLを異なるものにすることができるのを悪用した攻撃です。
例）https://www.ap-siken.com/ は、当サイトのトップページのURLですがITパスポート試験ドットコムに遷移します。

イ “Webサイトにアクセスすると自動的に他のWebサイトに遷移する機能を悪用し，攻撃者が指定した偽のWebサイトに誘導する。”

正しい。オープンリダイレクトを利用した攻撃です。

ウ “インターネット上の不特定多数のホストからDNSリクエストを受け付けて応答するDNSキャッシュサーバを悪用し，攻撃対象のWebサーバに大量のDNSのレスポンスを送り付け，リソースを枯渇させる。”

DNSアンプ攻撃（DNSリフレクタ攻撃）です。

エ “設定の不備によって，正規の利用者以外からの電子メールやWebサイトへのアクセス要求を受け付けるプロキシを悪用し，送信元を偽った迷惑メールの送信を行う。”

踏み台攻撃の説明です。

☆☆☆

ソフトウェア製品の脆弱性を第三者が発見し，その脆弱性をJPCERTコーディネーションセンターが製品開発者に通知した。その場合における製品開発者の対応のうち，"情報セキュリティ早期警戒パートナーシップガイドライン(2019年5月)"に照らして適切なものはどれか。

令和3年秋期　問38
2問目／選択範囲の問題数237問

ア　ISMS認証を取得している場合，ISMS認証の停止の手続をJPCERTコーディネーションセンターに依頼する。

イ　脆弱性関連の情報を集計し，統計情報としてIPAのWebサイトで公表する。

ウ　脆弱性情報の公表に関するスケジュールをJPCERTコーディネーションセンターと調整し，決定する。

エ　脆弱性の対応状況をJVNに書き込み，公表する。

❑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

ウ　“あなたの解答：ア”

❑解説

情報セキュリティ早期警戒パートナーシップガイドラインは、IPAやJPCERTコーディネーションセンター(JPCERT/CC)等が共同で策定しているガイドラインで、脆弱性関連情報の適切な流通により、コンピュータ不正アクセス、コンピュータウイルス等による被害発生を抑制するために、関係者に推奨する行為をとりまとめたものです。具体的には、IPAが受付機関、JPCERT/CCが調整機関という役割を担い、発見者、製品開発者、ウェブサイト運営者と協力をしながら脆弱性関連情報に対処するための、その発見から公表に至るプロセスを詳述しています。

本ガイドラインにおいて、ソフトウェア製品に係る脆弱性関連情報取扱の概要は、以下のようになっています。

① 発見者は、IPAに脆弱性関連情報を届け出る

② IPAは、受け取った脆弱性関連情報を、原則としてJPCERT/CCに通知する

③ JPCERT/CCは、脆弱性関連情報に関係する製品開発者を特定し、製品開発者に脆弱性関連情報を通知する

④ 製品開発者は、脆弱性検証を行い、その結果をJPCERT/CCに報告する

⑤ JPCERT/CCと製品開発者は、対策方法の作成や海外の調整機関との調整に要する期間、当該脆弱性情報流出に係るリスクを考慮しつつ、脆弱性情報の公表に関するスケジュールを調整し決定する

⑥ 製品開発者は、脆弱性情報の公表日までに対策方法を作成するよう努める

⑦ 製品開発者は、製品利用者に生じるリスクを低減できると判断した場合、JPCERT/CCと調整した上で、公表日以前に製品利用者に脆弱性検証の結果、対策方法および対応状況について通知することができる

⑧ IPAおよびJPCERT/CCは、脆弱性情報と、③にてJPCERT/CCから連絡したすべての製品開発者の脆弱性検証の結果、対策方法および対応状況を公表する

⑨ IPAは統計情報を、原則、四半期ごとに公表する

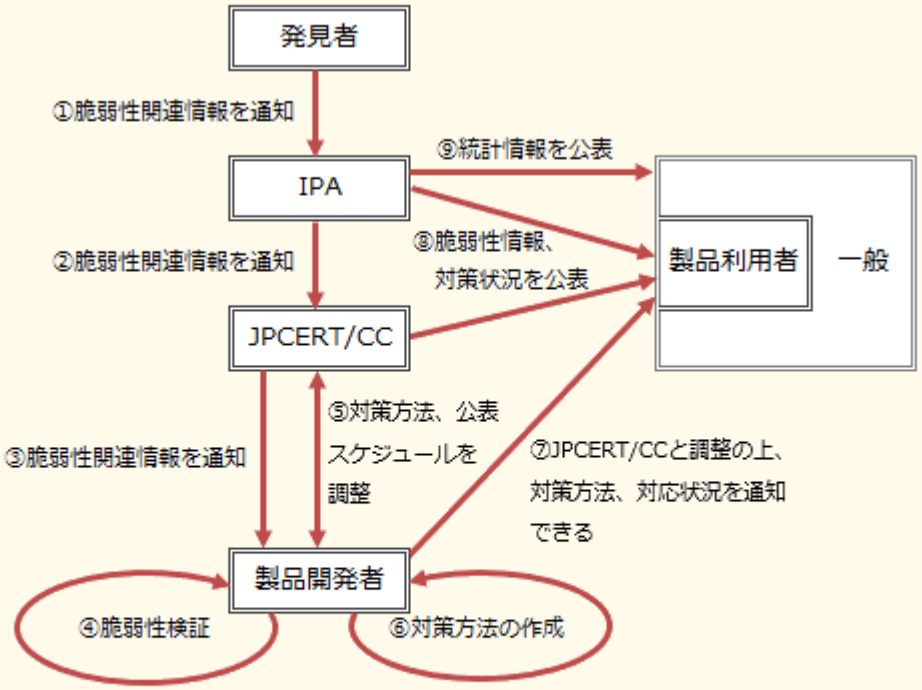


図　ソフトウエア製品に係る脆弱性関連情報取扱の概要

なお、ウェブアプリケーションに係る脆弱性関連情報の場合には、JPCERT/CCを介さずに、IPAからウェブサイト運営者に対して直接通知される取扱い手順となっています。

ア “ISMS認証を取得している場合，ISMS認証の停止の手続をJPCERTコーディネーションセンターに依頼する。”

ISMS認証の停止の手続きは本ガイドラインに規定されていません。ソフトウェアに脆弱性情報が見つかったとしても、それが直ちにISMS認証の停止につながるわけではありませんので誤りです。

イ “脆弱性関連の情報を集計し，統計情報としてIPAのWebサイトで公表する。”

統計情報の公開は、IPAが行います（⑨）。

ウ “脆弱性情報の公表に関するスケジュールをJPCERTコーディネーションセンターと調整し，決定する。”

正しい。製品開発者の役割です（⑤）。

エ “脆弱性の対応状況をJVNに書き込み，公表する。”

JVN(Japan Vulnerability Notes)への書込みは、IPAとJPCERTコーディネーションセンターが行います（⑧）。

☆☆☆

サイト運営者に不特定の利用者が電子メールで機密データを送信するに当たって，機密性を確保できる仕組みのうち，適切なものはどれか。

平成24年春期　問41
3問目／選択範囲の問題数237問

ア　サイト運営者はサイト内のSSLで保護されたWebページに共通鍵を公開し，利用者は電子メールで送信するデータをその共通鍵で暗号化する。

イ　サイト運営者はサイト内のSSLで保護されたWebページにサイト運営者の公開鍵を公開し，利用者は電子メールで送信するデータをその公開鍵で暗号化する。

ウ　サイト運営者はサイト内のSSLで保護されたWebページに利用者の公開鍵を公開し，利用者は電子メールで送信するデータをその公開鍵に対応する秘密鍵で暗号化する。

エ　サイト運営者はサイト内の認証局で利用者の公開鍵を公開し，利用者は電子メールで送信するデータをその公開鍵に対応する秘密鍵で暗号化する。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

イ　“あなたの解答：ウ”

❑解説

1対nの暗号化通信を行うのに適しているのが**公開鍵暗号方式**です。暗号化と復号に異なる鍵を使用し、暗号化鍵は誰もが使用できるように公開し(公開鍵)、復号鍵は受信者が厳重に管理します。(秘密鍵)

ア “サイト運営者はサイト内のSSLで保護されたWebページに共通鍵を公開し，利用者は電子メールで送信するデータをその共通鍵で暗号化する。”

共通鍵暗号方式では暗号化と復号に同じ鍵を使用します。Webページ上に共通鍵を公開してしまうと、送信されたデータを不特定多数の人が復号できるようになってしまうので誤りです。

イ “サイト運営者はサイト内のSSLで保護されたWebページにサイト運営者の公開鍵を公開し，利用者は電子メールで送信するデータをその公開鍵で暗号化する。”

正しい。暗号化はWebページ上の公開鍵を用いて誰でも行えますが、復号できるのは秘密鍵をもつサイト運営者だけです。

ウ “サイト運営者はサイト内のSSLで保護されたWebページに利用者の公開鍵を公開し，利用者は電子メールで送信するデータをその公開鍵に対応する秘密鍵で暗号化する。”

秘密鍵で暗号化したデータは対をなす公開鍵で復号が可能です。公開鍵がWebページに公開されている場合、不特定多数の人が電子メールを復号できてしまうので誤りです。(SSLで保護されたページはサーバ－クライアント間の通信が暗号化されるだけで、ページへのアクセスが制限されるわけではありません。)

エ “サイト運営者はサイト内の認証局で利用者の公開鍵を公開し，利用者は電子メールで送信するデータをその公開鍵に対応する秘密鍵で暗号化する。”

「ウ」と同じ理由で誤りです。

☆☆

迷惑メールのメールヘッダーから送信元又は中継元のISP又は組織を特定する手がかりのうち，最も信頼できるものはどれか。

Return-Path: <ユーザー名@ホスト名・ドメイン名①>
Received: from ホスト名・ドメイン名②(ホスト名・ドメイン名③[IPアドレス])
　　by 受信メールサーバ名 with SMTP id ...
From: <ユーザー名@ホスト名・ドメイン名④>

平成19年秋期　問74
4問目／選択範囲の問題数237問

ア	SMTPのMAIL FROMコマンドで通知されたホスト・ドメイン名①
イ	SMTPのHELOコマンドで通知されたホスト・ドメイン名②
ウ	送信元又は中継元のIPアドレスから逆引きされたホスト・ドメイン名③及びIPアドレス
エ	電子メールのFromヘッダーに設定されたホスト・ドメイン名④

❑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

ア “SMTPのMAIL FROMコマンドで通知されたホスト・ドメイン名①”

SMTPのMAIL FROMコマンドは、送信者が任意のアドレスを指定できるので詐称されている可能性があります。

イ “SMTPのHELOコマンドで通知されたホスト・ドメイン名②”

SMTPのHELOコマンドは、送信者が任意のアドレスを指定できるので詐称されている可能性があります。

ウ “送信元又は中継元のIPアドレスから逆引きされたホスト・ドメイン名③及びIPアドレス”

正しい。ホスト名・ドメイン名②は、送信者が任意のアドレスを指定できますが、ホスト名・ドメイン名③およびIPアドレスの部分は、送信元・中継元のIPアドレスから逆引きされたものなので詐称できません。この情報をもとに迷惑メールに使用される中継元やISPを特定し対策を依頼することもできます。

エ “電子メールのFromヘッダーに設定されたホスト・ドメイン名④”

Fromヘッダーは、メール発信者の送信エージェントに設定された内容が記載されるので詐称されている可能性があります。

☆

メッセージにRSA方式のデジタル署名を付与して2者間で送受信する。そのときのデジタル署名の検証鍵と使用方法はどれか。

令和5年春期　問38
5問目／選択範囲の問題数237問

ア　受信者の公開鍵であり，送信者がメッセージダイジェストからデジタル署名を作成する際に使用する。

イ　受信者の秘密鍵であり，受信者がデジタル署名からメッセージダイジェストを算出する際に使用する。

ウ　送信者の公開鍵であり，受信者がデジタル署名からメッセージダイジェストを算出する際に使用する。

エ　送信者の秘密鍵であり，送信者がメッセージダイジェストからデジタル署名を作成する際に使用する。

❑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：エ”

❑解説

デジタル署名の生成と検証の手順は次のとおりです。

1. 送信者は、メッセージをハッシュ関数にかけてメッセージダイジェスト(ハッシュ値)を得る
2. 送信者は、メッセージダイジェストを**送信者の秘密鍵で暗号化**することでデジタル署名を生成し、メッセージと一緒に送信する
3. 受信者は、デジタル署名を**送信者の公開鍵で復号**し、メッセージダイジェストを得る
4. 受信者は、受信したメッセージを送信者と同じハッシュ関数でハッシュ化したものと、3.で復号したメッセージダイジェストを比較する
5. 一つのメッセージからハッシュ関数によって生成されるメッセージダイジェストは常に同じになるため、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

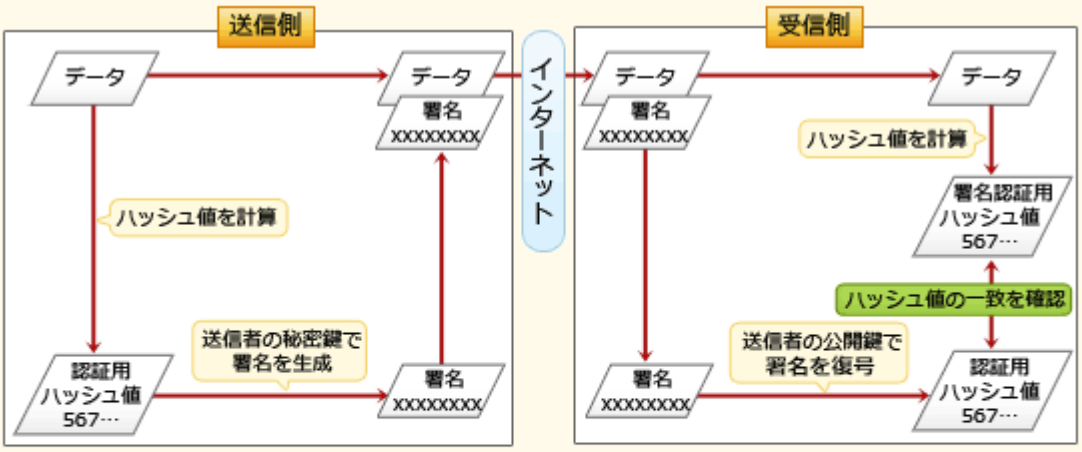


図　ディジタル署名の生成～検証の手順

デジタル署名の検証鍵は「送信者の公開鍵」であり、その使用方法は「受信者がデジタル署名からメッセージダイジェストを算出する」ことです（上記の3.の手順が該当します）。

したがって「ウ」の記述が適切です。

システム運用管理者による機密ファイルの不正な持出しを牽制するための対策はどれか。

平成26年秋期　問44
6問目／選択範囲の問題数237問

ア　運用管理者のPCの定期的なウイルス検査

イ　運用管理者のPCへのクライアントファイアウォールの導入

ウ　監視者の配置

エ　機密ファイルのバックアップ

❑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

ア “運用管理者のPCの定期的なウイルス検査”

ウイルス検査をしても、不正な持ち出しを防ぐことはできません。

イ “運用管理者のPCへのクライアントファイアウォールの導入”

ファイアウォールでは、外部記憶媒体にコピーして持ち出す行為への抑止力にはなりません。

ウ “監視者の配置”

正しい。監視によって持ち出しを完全に防げるわけではありませんが、常駐する警備員や設置された監視カメラに常に見られているという意識を持たせ、不正行為を実行する気を失くさせることが効果的です。

エ “機密ファイルのバックアップ”

不正な持ち出しにより業務に影響が出ることは防げますが、持ち出しへの対策にはなりません。

☆☆

サイバーレスキュー隊(J-CRAT)は，どの脅威による被害の低減と拡大防止を活動目的としているか。

平成30年春期　問40
7問目／選択範囲の問題数237問

ア	クレジットカードのスキミング	イ	内部不正による情報漏えい
ウ	標的型サイバー攻撃	エ	無線LANの盗聴

❑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

ウ　“あなたの解答：ウ”

❑解説

サイバーレスキュー隊(J-CRAT)は、「標的型サイバー攻撃特別相談窓口」にて受け付けた相談や情報に対して調査分析を実施し、JPCERT/CCやセキュリティベンダー等と連携して助言や支援および情報共有を行うことで被害の低減と攻撃の拡大防止を図るIPAの取り組みです。**標的型サイバー攻撃の被害低減と拡大防止**を活動目的としています。

したがって「ウ」が適切です。

参考URL: サイバーレスキュー隊J-CRAT（ジェイ・クラート）
https://www.ipa.go.jp/security/J-CRAT/index.html

https://www.ipa.go.jp/security/j-crat/about.html

☆☆

ISMSにおいて定義することが求められている情報セキュリティ基本方針に関する記述のうち，適切なものはどれか。

平成25年秋期　問40
8問目／選択範囲の問題数237問

ア　重要な基本方針を定めた機密文書であり，社内の関係者以外の目に触れないようにする。

イ　情報セキュリティの基本方針を述べたものであり，ビジネス環境や技術が変化しても変更してはならない。

ウ　情報セキュリティのための経営陣の方向性及び支持を規定する。

エ　特定のシステムについてリスク分析を行い，そのセキュリティ対策とシステム運用の詳細を記述する。

❑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

ウ　"あなたの解答：ウ"

❑解説

組織が情報セキュリティのために定める文書は、一般的に情報セキュリティ基本方針、情報セキュリティ対策基準、情報セキュリティ実施手順の3階層の文書で構成されます。この3つを合わせて**情報セキュリティポリシー**と言います。

情報セキュリティ基本方針

組織の経営者が「セキュリティの最高責任者として、情報セキュリティに本格的に取り組む」という姿勢を示し、情報セキュリティの目標と、その目標を達成するために企業がとるべき行動を組織内外に宣言する文書

情報セキュリティ対策基準

基本方針の目標を達成するために必要な規則を記述した文書。企業の構成員が守るべきセキュリティ関連規程類に相当する

情報セキュリティ実施手順

対策基準を実践するために必要な手続きを記述した文書。作業手順書やマニュアルなどに相当する

情報セキュリティ基本方針には、情報資産をどのような脅威から、どのようにして守るのかについての基本的な考え方と、情報セキュリティを確保するための体制、組織および運用などの枠組みが包括的に規定されます。策定した情報セキュリティ基本方針には、有効性・妥当性を維持するために定期的な改善をすること、全ての従業員に対して周知させることが求められます。

ア “重要な基本方針を定めた機密文書であり，社内の関係者以外の目に触れないようにする。”

情報セキュリティ基本方針は、組織のセキュリティ方針を経営者が組織内外に宣言するものなので機密文書としては取り扱いません。組織内に広く伝達するとともに、Webサイト上に公開するなどして必要に応じて社外を含む利害関係者が入手可能であることが求められます。

イ “情報セキュリティの基本方針を述べたものであり，ビジネス環境や技術が変化しても変更してはならない。”

情報セキュリティ基本方針は、事業環境・法改正・技術などの変化に適合するように、必要に応じて変更することが求められます。

ウ “情報セキュリティのための経営陣の方向性及び支持を規定する。”

正しい。情報セキュリティ基本方針には、組織が情報セキュリティの要求事項を満たすことへの経営者の責任(コミットメント)を含めなければなりません。

エ “特定のシステムについてリスク分析を行い，そのセキュリティ対策とシステム運用の詳細を記述する。”

情報セキュリティ基本方針には、具体的なセキュリティ対策は記述しません。対策と運用の詳細は、対策基準と実施手順に記述します。

☆☆☆

DKIM(DomainKeys Identified Mail)に関する記述のうち，適切なものはどれか。

令和5年秋期　問44
9問目／選択範囲の問題数237問

ア　送信側のメールサーバで電子メールにデジタル署名を付与し，受信側のメールサーバでそのデジタル署名を検証して送信元ドメインの認証を行う。

イ　送信者が電子メールを送信するとき，送信側のメールサーバは，送信者が正規の利用者かどうかの認証を利用者IDとパスワードによって行う。

ウ　送信元ドメイン認証に失敗した際の電子メールの処理方法を記載したポリシーをDNSサーバに登録し、電子メールの認証結果を監視する。

エ　電子メールの送信元ドメインでメール送信に使うメールサーバのIPアドレスをDNSサーバに登録しておき，受信側で送信元ドメインのDNSサーバに登録されているIPアドレスと電子メールの送信元メールサーバのIPアドレスとを照合する。

❑分類

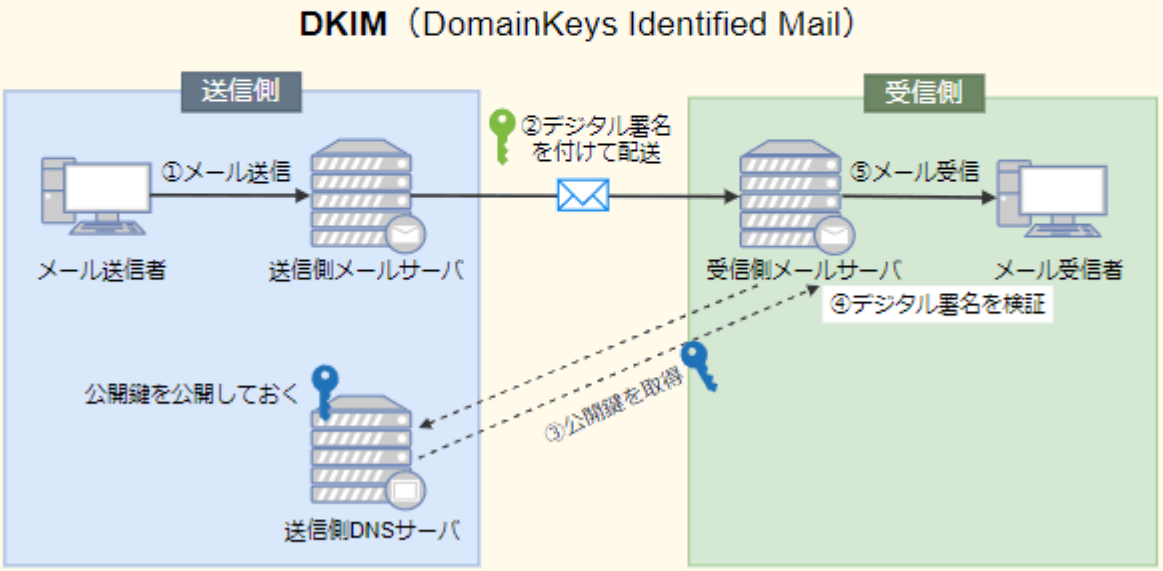
テクノロジ系 » セキュリティ » セキュリティ実装技術

❑正解

ア　“あなたの解答：エ”

❑解説

DKIM(DomainKeys Identified Mail)は、送信する電子メールのヘッダーと本文から生成されたデジタル署名を送信側メールサーバで付加し、受信側メールサーバが、送信側ドメインのDNSサーバに登録されている公開鍵を使用してデジタル署名の検証を行うことで、正当なメールサーバから送られてきたメールであることを確認する仕組みです。スパムメール対策の技術のひとつとして利用されています。



したがって「ア」が正解です。

ア “送信側のメールサーバで電子メールにデジタル署名を付与し，受信側のメールサーバでそのデジタル署名を検証して送信元ドメインの認証を行う。”

正しい。DKIMの説明です。

イ “送信者が電子メールを送信するとき，送信側のメールサーバは，送信者が正規の利用者かどうかの認証を利用者IDとパスワードによって行う。”

SMTP-AUTHの説明です。

ウ “送信元ドメイン認証に失敗した際の電子メールの処理方法を記載したポリシーをDNSサーバに登録し、電子メールの認証結果を監視する。”

DMARC(ディーマーク)の説明です。

エ “電子メールの送信元ドメインでメール送信に使うメールサーバのIPアドレスをDNSサーバに登録しておき，受信側で送信元ドメインのDNSサーバに登録されているIPアドレスと電子メールの送信元メールサーバのIPアドレスとを照合する。”

SPF(Sender Policy Framework)の説明です。

デジタル署名において，発信者がメッセージのハッシュ値からデジタル署名を生成するのに使う鍵はどれか。

平成25年秋期　問39
10問目／選択範囲の問題数237問

ア	受信者の公開鍵	イ	受信者の秘密鍵
ウ	発信者の公開鍵	エ	発信者の秘密鍵

❑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

デジタル署名の手順は、

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、平文と一緒に送信します。
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します。
3. 一つの平文からハッシュ関数によって生成されるメッセージダイジェストは常に同じになるため、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ます。

したがって発信者がメッセージのハッシュ値をデジタル署名に変換するのに使う鍵は「発信者の秘密鍵」が適切です。

☆☆

家庭内で，PCを無線LANとブロードバンドルータを介してインターネットに接続するとき，期待できるセキュリティ上の効果の記述のうち，適切なものはどれか。

令和4年秋期　問43
11問目／選択範囲の問題数237問

ア	IPマスカレード機能による，インターネットからの不正侵入に対する防止効果
イ	PPPoE機能による，経路上の盗聴に対する防止効果
ウ	WPA機能による，不正なWebサイトへの接続に対する防止効果
エ	WPS機能による，インターネットからのマルウェア感染に対する防止効果

❑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

ア　“あなたの解答：エ”

❑解説

ブロードバンドルータは、家庭内の複数内の端末が同時にインターネットに接続できるように、**IPマスカレード**(NAPT)の機能を備えています。

ブロードバンドルータは、LAN内のPCがインターネットに接続する際に、①PCのプライベートIPアドレスとポート番号の組合せをグローバルIPアドレスとポート番号の組合せに変換し、その対応を変換テーブルに記録しておきます。その後、インターネットから応答パケットを受け取ると、②変換テーブルの中から応答パケットの宛先ポート番号を探し、適切なプライベートIPアドレスとポート番号の組合せに戻して送信元PCに応答パケットを届けます。この一連のアドレスとポート番号の変更がIPマスカレードの動作です。

②の動作において該当するポート番号が変換テーブル内に存在しないときは、適切な変換先が見つからないのでルータは応答パケットを破棄することになります。つまり、外部から適当なパケットを送り付けても内部LANには到達しないということです。この仕組みにより、外部からポートスキャンや不正侵入を試みる攻撃が来たとしても、PCが守られるセキュリティ効果が期待できます。

ア “IPマスカレード機能による，インターネットからの不正侵入に対する防止効果”

正しい。

イ “PPPoE機能による，経路上の盗聴に対する防止効果”

PPP over EthernetはPPPをイーサネット上で利用できるようにしたものです。ブロードバンドルータからプロバイダの認証と接続を行うときに使用されていますが、通信経路の暗号化機能は持っていません。

ウ “WPA機能による，不正なWebサイトへの接続に対する防止効果”

WPA(Wi-Fi Protected Access)は、無線LANの暗号化規格です。コンテンツフィルタリング機能やURLフィルタリング機能はありません。

エ “WPS機能による，インターネットからのマルウェア感染に対する防止効果”

WPS(Wi-Fi Protected Setup)は、無線LANの親機と子機の接続設定やセキュリティ設定を容易に行うために策定された規格です。マルウェア感染を防止する機能はありません。

☆☆☆

デジタルフォレンジックスの手順は収集，検査，分析及び報告から成る。このとき，デジタルフォレンジックスの手順に含まれるものはどれか。

令和5年春期　問42
12問目／選択範囲の問題数237問

ア　サーバとネットワーク機器のログをログ管理サーバに集約し，リアルタイムに相関分析することによって，不正アクセスを検出する。

イ　ディスクを解析し，削除されたログファイルを復元することによって，不正アクセスの痕跡を発見する。

ウ　電子メールを外部に送る際に，本文及び添付ファイルを暗号化することによって，情報漏えいを防ぐ。

エ　プログラムを実行する際に，プログラムファイルのハッシュ値と脅威情報を突き合わせることによって，プログラムがマルウェアかどうかを検査する。

❑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

イ　“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明らかにするために対象となる電子的記録を収集し、保全し、分析する一連のプロセスです。

IPAが公開している「インシデント対応へのフォレンジック技法の統合に関するガイド」によれば、デジタルフォレンジックスの手順は、収集・検査・分析・報告の4つのフェーズから成ります。

収集

特定の事象に関連するデータの識別、ラベル付け、記録、および収集を行い、その完全性を保護する

検査

収集されたデータの種類に適したフォレンジックツールやフォレンジック技法を実行することにより、データの完全性を保護しながら、収集されたデータから関連する情報を識別し、抽出する

分析

検査結果を分析することにより、収集と検査を行う契機となった疑問を解決するのに役立つ情報を導き出す

報告

分析フェーズによって得られた結果を報告する

選択肢のうちセキュリティインシデントの痕跡を収集している「イ」が、デジタルフォレンジックスの手順である「収集・検査」に該当します。

☆

APT(Advanced Persistent Threats)の説明はどれか。

平成26年秋期　問35
13問目／選択範囲の問題数237問

ア　攻撃者はDoS攻撃及びDDoS攻撃を繰り返し組み合わせて，長期間にわたって特定組織の業務を妨害する。

イ　攻撃者は興味本位で場当たり的に，公開されている攻撃ツールや脆弱性検査ツールを悪用した攻撃を繰り返す。

ウ　攻撃者は特定の目的をもち，特定組織を標的に複数の手法を組み合わせて気付かれないよう執拗(よう)に攻撃を繰り返す。

エ　攻撃者は不特定多数への感染を目的として，複数の攻撃を組み合わせたマルウェアを継続的にばらまく。

❑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

APT攻撃(Advanced Persistent Threats)は、複数の攻撃方法を組み合わせて、特定の組織や個人に対して長期間にわたり持続的に行われるサイバー攻撃の総称です。

単なる標的型攻撃と異なる点は、準備や攻撃が長い期間を通じて持続的に行われる点です。最初にメールや外部メディア等で組織内部の従業員（組織の幹部を含む）の端末への不正侵入を試み、そこから組織の内部へ更に入り込んでいくなど目的達成のために数か月から数年にわたって攻撃が継続します。最終的には組織にとって非常に重要な情報（知財情報や個人情報）を盗み出すことなどを目的としています。

「APT」というのは海外での呼び名で、日本では**持続的標的型攻撃**と呼ばれています。

ア “攻撃者はDoS攻撃及びDDoS攻撃を繰り返し組み合わせて，長期間にわたって特定組織の業務を妨害する。”

過負荷によるサービス停止を引き起こすタイプの攻撃ではありません。

イ “攻撃者は興味本位で場当たり的に，公開されている攻撃ツールや脆弱性検査ツールを悪用した攻撃を繰り返す。”

場当たり的ではなく、特定の目的をもって攻撃を繰り返します。

ウ “攻撃者は特定の目的をもち，特定組織を標的に複数の手法を組み合わせて気付かれないよう執拗(よう)に攻撃を繰り返す。”

正しい。情報窃取やシステムへの不正侵入などの目的で行われる攻撃です。

エ “攻撃者は不特定多数への感染を目的として，複数の攻撃を組み合わせたマルウェアを継続的にばらまく。”

攻撃対象となるのは特定の組織や個人です。

☆☆☆

IDS(Intrusion Detection System)の特徴のうち，適切なものはどれか。

平成18年春期　問73
14問目／選択範囲の問題数237問

ア　ネットワーク型IDSでは，SSLを利用したアプリケーションを介して行われる攻撃を検知できる。

イ　ネットワーク型IDSでは，通信内容の解析によって，ファイルの改ざんを検知できる。

ウ　ホスト型IDSでは，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る。

エ　ホスト型IDSでは，到着する不正パケットの解析によって，ネットワークセグメント上の不正パケットを検知できる。

❑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

ウ　“あなたの解答：ア”

❑解説

IDS(Intrusion Detection System，侵入検知システム)は、ネットワークやホストをリアルタイムで監視し、異常を検知した場合に管理者に通知するなどの処置を行うシステムです。IDSには、ネットワークセグメントに接続しネットワークを流れる通信を監視する**NIDS**(Network-Based IDS)と、監視対象のサーバ(ホスト)にインストールしてそのサーバで発生するイベントを監視する**HIDS**(Host-Based IDS)の2つに分類することができます。

ア “ネットワーク型IDSでは，SSLを利用したアプリケーションを介して行われる攻撃を検知できる。”

一般的なネットワーク型IDS(NIDS)は、通信内容を復号するSSLアクセラレータ機能をもっていないため、暗号化された攻撃を検知することができません。(ただし一部の高機能NIDSはSSLアクセラレータの機能をもつ機器も存在します)

イ “ネットワーク型IDSでは，通信内容の解析によって，ファイルの改ざんを検知できる。”

NIDSは、ネットワークに接続して通信内容の監視を行う機器のため、ホスト上に存在するファイルの異常を検知することはできません。

ウ “ホスト型IDSでは，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る。”

正しい。ホスト型IDS(HIDS)では、パターンマッチングだけでなく、ログインや特定ファイルへのアクセスなども検知項目とするため、これらを監視することで不正パケットを検知することが可能です。

エ “ホスト型IDSでは，到着する不正パケットの解析によって，ネットワークセグメント上の不正パケットを検知できる。”

HIDSは、対象ホストのみを監視するのでネットワークに流れる不正パケットのすべての検知はできません。

☆☆☆

VBScript(Visual Basic Script)で作られたコンピュータウイルスの特徴はどれか。

平成19年春期　問74
15問目／選択範囲の問題数237問

ア	HTML形式の電子メール本文などに埋め込まれたスクリプトによって動作する。
イ	感染対象が実行形式ファイルであるか文書ファイルであるかにかかわらず，すべてのOSで動作する。
ウ	実行ファイルはなくワープロの文書ファイルなどに感染し，関連するアプリケーションソフトを利用して動作する。
エ	ブートセクタに感染して，通常のプロセス起動前にウイルスが呼び出されて動作する。

❑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：イ”

❑解説

VBScriptは、プログラム言語Visual Basicの簡易版でありMicrosoft Windows上で動作するスクリプト言語です。VBScriptで作られたコンピュータウィルスは、メール本文やWebページなどのHTML形式の文書に埋め込まれ、閲覧したと同時に実行されるスクリプトによってコンピュータを感染させるという特徴を持っています。

ア “HTML形式の電子メール本文などに埋め込まれたスクリプトによって動作する。”

正しい。

イ “感染対象が実行形式ファイルであるか文書ファイルであるかにかかわらず，すべてのOSで動作する。”

感染対象はMicrosoft Windowsがインストールされたコンピュータのみです。

ウ “実行ファイルはなくワープロの文書ファイルなどに感染し，関連するアプリケーションソフトを利用して動作する。”

マクロウィルスの特徴です。

エ “ブートセクタに感染して，通常のプロセス起動前にウイルスが呼び出されて動作する。”

ブートセクタウィルスの特徴です。

☆☆☆

経済産業省とIPAが策定した"サイバーセキュリティ経営ガイドライン(Ver2.0)"の説明はどれか。

令和3年春期　問41
16問目／選択範囲の問題数237問

ア　企業がIT活用を推進していく中で，サイバー攻撃から企業を守る観点で経営者が認識すべき3原則と，情報セキュリティ対策を実施する上での責任者となる担当幹部に，経営者が指示すべき重要10項目をまとめたもの

イ　経営者が情報セキュリティについて方針を示し，マネジメントシステムの要求事項を満たすルールを定め，組織が保有する情報資産をCIAの観点から維持管理し，継続的に見直すためのプロセス及び管理策を体系的に規定したもの

ウ　事業体のITに関する経営者の活動を，大きくITガバナンス(統制)とITマネジメント(管理)に分割し，具体的な目標と工程として40のプロセスを定義したもの

エ　世界的規模で生じているサイバーセキュリティ上の脅威の深刻化に関して，企業の経営者を支援する施策を総合的かつ効果的に推進するための国の責務を定めたもの

❑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

ア　“あなたの解答：ア”

❑解説

サイバーセキュリティ経営ガイドラインは、サイバー攻撃から企業を守る観点で、経営者が認識する必要のある「3原則」、及び経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部(CISO等)に指示すべき「重要10項目」をまとめたものです。具体的には、経営者のリーダーシップの下での体制整備と対策の進め方、社会やステークホルダに対する情報開示のあり方などが取りまとめられています。

したがって適切な説明は「ア」です。

ア “企業がIT活用を推進していく中で，サイバー攻撃から企業を守る観点で経営者が認識すべき3原則と，情報セキュリティ対策を実施する上での責任者となる担当幹部に，経営者が指示すべき重要10項目をまとめたもの”

正しい。サイバーセキュリティ経営ガイドラインの説明です。

イ “経営者が情報セキュリティについて方針を示し，マネジメントシステムの要求事項を満たすルールを定め，組織が保有する情報資産をCIAの観点から維持管理し，継続的に見直すためのプロセス及び管理策を体系的に規定したもの”

情報セキュリティ方針の説明です。

ウ “事業体のITに関する経営者の活動を，大きくITガバナンス(統制)とITマネジメント(管理)に分割し，具体的な目標と工程として40のプロセスを定義したもの”

COBITの説明です。アメリカの情報システムコントロール協会(ISADA)とITガバナンス協会(ITGI)が策定しているIT管理についてのフレームワークです。

エ “世界的規模で生じているサイバーセキュリティ上の脅威の深刻化に関して，企業の経営者を支援する施策を総合的かつ効果的に推進するための国の責務を定めたもの”

サイバーセキュリティ基本法の説明です。

参考URL: サイバーセキュリティ経営ガイドライン
http://www.meti.go.jp/policy/netsecurity/mng_guide.html

☆

デジタル署名における署名鍵の使い方と，デジタル署名を行う目的のうち，適切なものはどれか。

平成24年春期　問40
17問目／選択範囲の問題数237問

ア　受信者が署名鍵を使って，暗号文を元のメッセージに戻すことができるようにする。

イ　送信者が固定文字列を付加したメッセージを，署名鍵を使って暗号化することによって，受信者がメッセージの改ざん部位を特定できるようにする。

ウ　送信者が署名鍵を使って署名を作成し，それをメッセージに付加することによって，受信者が送信者を確認できるようにする。

エ　送信者が署名鍵を使ってメッセージを暗号化することによって，メッセージの内容を関係者以外に分からないようにする。

❑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、この仕組みによって「発信者が正当であるか」と「改ざんの有無」の2点を確認できます。また改ざんの検知はできますが、改ざん部位の特定および訂正機能はもちません。

以下はデジタル署名の手順です。

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. 一つの平文からハッシュ関数によって生成されるメッセージダイジェストは常に同じになるため、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ば、通信内容が改ざんされていないことが証明される。

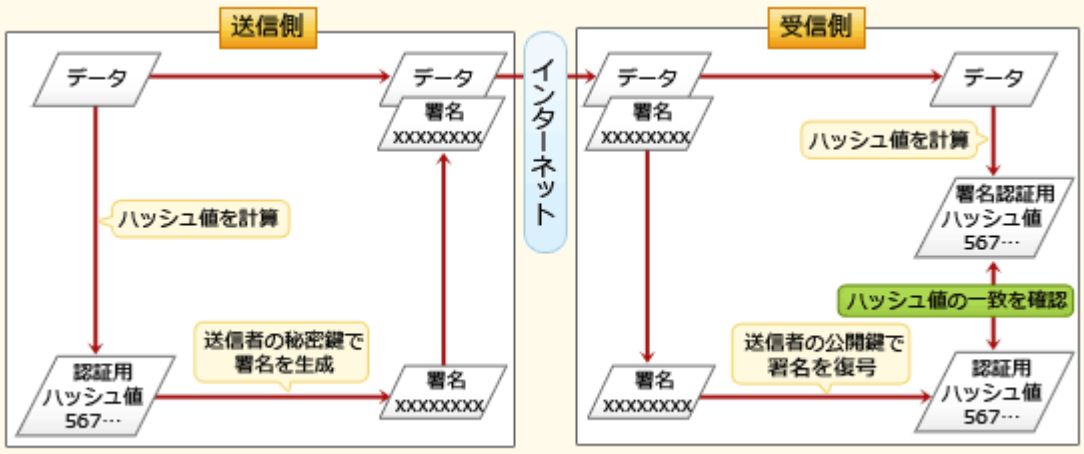


図　ディジタル署名の生成～検証の手順

ア “受信者が署名鍵を使って，暗号文を元のメッセージに戻すことができるようにする。”

署名鍵は、メッセージダイジェストを暗号化してデジタル署名を生成するために使用されます。

イ “送信者が固定文字列を付加したメッセージを，署名鍵を使って暗号化することによって，受信者がメッセージの改ざん部位を特定できるようにする。”

メッセージダイジェストの復号に使われるのは送信者の公開鍵です。またデジタル署名には改ざん部位を特定する機能はありません。

ウ “送信者が署名鍵を使って署名を作成し，それをメッセージに付加することによって，受信者が送信者を確認できるようにする。”

正しい。ある秘密鍵で暗号化された署名は、それと対になる公開鍵でしか復号できません。送信者の公開鍵で署名が復号できたという事実から、送信元の真正性を確認できます。

エ “送信者が署名鍵を使ってメッセージを暗号化することによって，メッセージの内容を関係者以外に分からないようにする。”

デジタル署名はメッセージ本文の暗号化を行いません。

☆

手順に示すハッシュ関数とメッセージダイジェストの処理を行うことで得られるセキュリティ上の効果はどれか。ここで，メッセージダイジェストは安全な方法で保護され，改ざんや破壊がされていないものとする。

〔手順〕

(1) 送信者Aは，電子メールの本文からハッシュ関数を用いて，メッセージダイジェストを作成する。電子メールの本文とメッセージダイジェストを別々に受信者Bに送信する。

(2) 受信者Bは受信した電子メールの本文からハッシュ関数を用いて，メッセージダイジェストを作成する。その作成したメッセージダイジェストと，受信したメッセージダイジェストを比較する。

平成24年秋期　問38
18問目／選択範囲の問題数237問

ア	電子メールの改ざんの有無の確認	イ	電子メールの誤送信の防止
ウ	電子メールの送達確認	エ	電子メールの盗聴の防止

❑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

この問題文で説明されている、ハッシュ関数とメッセージダイジェストを用いた手順は「メッセージ認証」と呼ばれているものです。

ハッシュ関数には、

- 入力データが同じであれば、常に同じメッセージダイジェストが生成される。
- 入力データが少しでも異なっていれば生成されるメッセージダイジェストは大きく異なったものになる。
- メッセージダイジェストから元の入力データを再現することが困難である。
- 異なる入力データから同じメッセージダイジェストが生成される可能性が非常に低い。

という特徴があるため、受信したメッセージダイジェストと、受信したメール本文から（送信者と同じハッシュ関数を用いて）作成したメッセージダイジェストが同じであれば、メール本文の改ざんが行われていないと判断することができます。なお、メッセージ認証を行う際に、本文に添付されるメッセージダイジェストをメッセージ認証符号（MAC: Message Authentication Code）といいます。

ア “電子メールの改ざんの有無の確認”

正しい。メッセージ認証により改ざんの有無を確認できます。

イ “電子メールの誤送信の防止”

誤送信の防止はできません。

ウ “電子メールの送達確認”

送達確認がとれるような仕組みはありません。

エ “電子メールの盗聴の防止”

電子メール本文は暗号化されていないため盗聴を防止することはできません。

☆

公開鍵暗号方式を用いて送信者が文書にデジタル署名を行う場合，文書が間違いなく送信者のものであることを受信者が確認できるものはどれか。

平成21年秋期　問38
19問目／選択範囲の問題数237問

ア　送信者は自分の公開鍵を使用して署名処理を行い，受信者は自分の秘密鍵を使用して検証処理を行う。

イ　送信者は自分の秘密鍵を使用して署名処理を行い，受信者は送信者の公開鍵を使用して検証処理を行う。

ウ　送信者は受信者の公開鍵を使用して署名処理を行い，受信者は自分の秘密鍵を使用して検証処理を行う。

エ　送信者は受信者の秘密鍵を使用して署名処理を行い，受信者は自分の公開鍵を使用して検証処理を行う。

❑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

デジタル署名の手順としては、

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、平文と一緒に送信します。
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します。
3. 一つの平文からハッシュ関数によって生成されるメッセージダイジェストは常に同じになるため、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ます。

ただしデジタル署名では、第三者が正当な送信者になりすまして送信をする行為までは防ぐことはできません。

☆☆☆
※解答なし

認証局が発行するCRLに関する記述のうち，適切なものはどれか。

平成29年秋期　問36
20問目／選択範囲の問題数237問

ア　CRLには，失効したデジタル証明書に対応する秘密鍵が登録される。

イ　CRLには，有効期限内のデジタル証明書のうち失効したデジタル証明書と失効した日時の対応が提示される。

ウ　CRLは，鍵の漏えい，失効申請の状況をリアルタイムに反映するプロトコルである。

エ　有効期限切れで失効したデジタル証明書は，所有者が新たなデジタル証明書を取得するまでの間，CRLに登録される。

☆☆

重要情報の取扱いを委託する場合における，委託元の情報セキュリティ管理のうち，適切なものはどれか。

平成28年春期　問38
21問目／選択範囲の問題数237問

ア　委託先が再委託を行うかどうかは委託先の判断に委ね，事前報告も不要とする。

イ　委託先の情報セキュリティ対策が確認できない場合は，短期間の業務に限定して委託する。

ウ　委託先の情報セキュリティ対策が適切かどうかは，契約開始前ではなく契約終了時に評価する。

エ　情報の安全管理に必要な事項を事前に確認し，それらの事項を盛り込んだ上で委託先との契約書を取り交わす。

❑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

エ　“あなたの解答：エ”

❑解説

委託元組織は、委託先による組織の情報へのアクセスに具体的に対処するため、適切な情報セキュリティ管理策を定め、委託先に義務付けることが重要です。

ア “委託先が再委託を行うかどうかは委託先の判断に委ね，事前報告も不要とする。”

重要情報にアクセスする組織や要員の範囲が変更される場合は、委託元の認可を得る様な手順を定めるべきです。

イ “委託先の情報セキュリティ対策が確認できない場合は，短期間の業務に限定して委託する。”

情報セキュリティの要求事項について委託先と合意できない場合は契約すべきではありません。

ウ “委託先の情報セキュリティ対策が適切かどうかは，契約開始前ではなく契約終了時に評価する。”

委託先との間に誤解がないことを確実にするために、情報セキュリティ対策の評価は契約開始前に行うべきです。

エ “情報の安全管理に必要な事項を事前に確認し，それらの事項を盛り込んだ上で委託先との契約書を取り交わす。”

正しい。JIS Q 27001:2014では、「組織の資産に対する供給者のアクセスに関連するリスクを軽減するための情報セキュリティ要求事項について，供給者と合意し，文書化しなければならない」としています。

☆☆☆

クライアント証明書で利用者を認証するリバースプロキシサーバを用いて，複数のWebサーバにシングルサインオンを行うシステムがある。このシステムに関する記述のうち，適切なものはどれか。

令和4年春期　問41
22問目／選択範囲の問題数237問

ア　クライアント証明書を利用者のPCに送信するのは，Webサーバではなく，リバースプロキシサーバである。

イ　クライアント証明書を利用者のPCに送信するのは，リバースプロキシサーバではなく，Webサーバである。

ウ　利用者IDなどの情報をWebサーバに送信するのは，リバースプロキシサーバではなく，利用者のPCである。

エ　利用者IDなどの情報をWebサーバに送信するのは，利用者のPCではなく，リバースプロキシサーバである。

❑分類

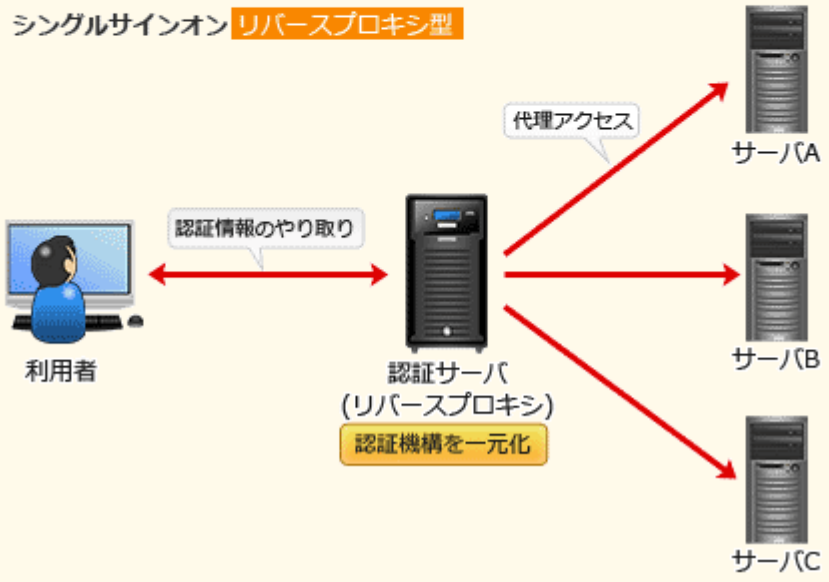
テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

エ　“あなたの解答：エ”

❑解説

リバースプロキシ型SSOは、複数のWebサーバと利用者PCとの間にリバースプロキシサーバを配置し、すべてのWebサーバへのアクセスをリバースプロキシサーバに集約することでシングルサインオンを実現する構成です。リバースプロキシサーバはアクセスしてきた利用者を認証し、認証に成功すればリバースプロキシサーバはWebサーバに代理アクセスして、結果を利用者に返します。



ア “クライアント証明書を利用者のPCに送信するのは，Webサーバではなく，リバースプロキシサーバである。”

クライアント証明書は利用者の認証に使うので、利用者のPCからリバースプロキシサーバに送信されます。

イ “クライアント証明書を利用者のPCに送信するのは，リバースプロキシサーバではなく，Webサーバである。”

クライアント証明書は、PCからリバースプロキシサーバに送信されます。

ウ “利用者IDなどの情報をWebサーバに送信するのは，リバースプロキシサーバではなく，利用者のPCである。”

利用者のPCとWebサーバが直接通信することはありません。

エ “利用者IDなどの情報をWebサーバに送信するのは，利用者のPCではなく，リバースプロキシサーバである。”

正しい。利用者がリバースプロキシサーバで認証を受けた場合、リバースプロキシサーバからWebサーバへ利用者IDなどの情報が送信されます。

☆☆

SPF(Sender Policy Framework)の仕組みはどれか。

令和6年春期　問43
23問目／選択範囲の問題数237問

ア　電子メールを受信するサーバが，電子メールに付与されているデジタル署名を使って，送信元ドメインの詐称がないことを確認する。

イ　電子メールを受信するサーバが，電子メールの送信元のドメイン情報と，電子メールを送信したサーバのIPアドレスから，送信元ドメインの詐称がないことを確認する。

ウ　電子メールを送信するサーバが，電子メールの宛先のドメインや送信者のメールアドレスを問わず，全ての電子メールをアーカイブする。

エ　電子メールを送信するサーバが，電子メールの送信者の上司からの承認が得られるまで，一時的に電子メールの送信を保留する。

❑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

イ　“あなたの解答：イ”

❑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。

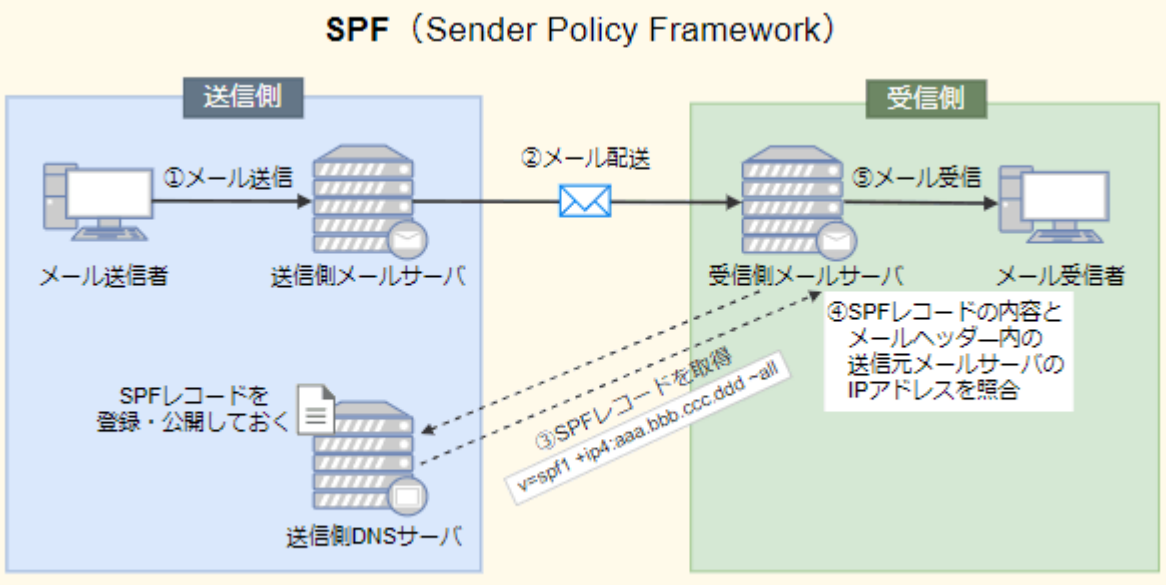
SPFでは以下の手順で電子メールの送信元IPアドレスの検証を行います。

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。



この仕組みを踏まえて各選択肢の正誤を判断します。

ア “電子メールを受信するサーバが，電子メールに付与されているデジタル署名を使って，送信元ドメインの詐称がないことを確認する。”

SPFではデジタル署名を使用しません。記述はDKIM(DomainKeys Identified Mail)の仕組みです。

イ “電子メールを受信するサーバが，電子メールの送信元のドメイン情報と，電子メールを送信したサーバのIPアドレスから，送信元ドメインの詐称がないことを確認する。”

正しい。SPFの仕組みです。

ウ “電子メールを送信するサーバが，電子メールの宛先のドメインや送信者のメールアドレスを問わず，全ての電子メールをアーカイブする。”

メールアーカイブシステムの仕組みです。

エ “電子メールを送信するサーバが，電子メールの送信者の上司からの承認が得られるまで，一時的に電子メールの送信を保留する。”

メール誤送信防止システムの仕組みです。

☆☆☆

SSLの利用に関する記述のうち，適切なものはどれか。

平成19年秋期　問75
24問目／選択範囲の問題数237問

ア　SSLで使用する個人認証用のデジタル証明書は，ICカードなどに格納できるので，格納場所を特定のPCに限定する必要はない。

イ　SSLは特定利用者間の通信のために開発されたプロトコルであり，Webサーバ提供者への事前の利用者登録が不可欠である。

ウ　デジタル証明書にはIPアドレスが組み込まれているので，SSLを利用するWebサーバのIPアドレスを変更する場合は，デジタル証明書を再度取得する必要がある。

エ　日本国内では，SSLで使用する共通鍵の長さは，128ビット未満に制限されている。

❑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

ア　“あなたの解答：ア”

❑解説

SSL(Secure Sockets Layer)は、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です。主にWebブラウザとWebサーバ間でデータを安全にやり取りするための業界標準プロトコルとして使用されています。

ア “SSLで使用する個人認証用のデジタル証明書は，ICカードなどに格納できるので，格納場所を特定のPCに限定する必要はない。”

正しい。デジタル証明書の内容はデジタルデータなので様々な媒体に格納することができます。
個人認証用のデジタル証明書は電子証明書と呼ばれ、公的認証サービスなどを利用すると電子証明書が記録されたICカードの発行をうけることができます。

イ “SSLは特定利用者間の通信のために開発されたプロトコルであり，Webサーバ提供者への事前の利用者登録が不可欠である。”

SSLはインターネット上で安全に情報をやり取りするために開発されたプロトコルで、事前の利用者登録は必要ありません。

ウ “デジタル証明書にはIPアドレスが組み込まれているので，SSLを利用するWebサーバのIPアドレスを変更する場合は，デジタル証明書を再度取得する必要がある。”

デジタル証明書では、証明書が有効なサーバ(コモンネーム)を記述するのにIPアドレスだけでなくFQDNも使用できます。FQDNで指定した場合にはIPアドレスが変わっても再発行の必要はありません。

エ “日本国内では，SSLで使用する共通鍵の長さは，128ビット未満に制限されている。”

SSLでは鍵長40～256ビットの共通鍵で暗号化通信を行います。日本国内においても256ビットまでの鍵長を制限なく選択できます。

JIS Q 27000:2019(情報セキュリティマネジメントシステム－用語)では，情報セキュリティは主に三つの特性を維持することとされている。それらのうちの二つは機密性と完全性である。残りの一つはどれか。

令和元年秋期　問40
25問目／選択範囲の問題数237問

ア	可用性	イ	効率性	ウ	保守性	エ	有効性

❑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

ア　“あなたの解答：エ”

❑解説

JIS Q 27000:2019では、情報セキュリティを「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。この定義に集約されているように、情報セキュリティマネジメントにおいては、主に「機密性」「完全性」および「可用性」の3つの特性を維持・管理することが肝要です。

機密性（Confidentiality）

許可された正規のユーザーだけが情報にアクセスできる特性を示す

完全性（Integrity）

情報が完全で、改ざん・破壊されていない特性を示す

可用性（Availability）

システムが正常に稼働し続けることの度合い。ユーザーが必要な時にシステムが利用可能である特性を示す

したがって残り1つは「可用性」になります。

☆☆☆

公開鍵基盤とハッシュ関数を利用したメッセージのデジタル署名の手法はどれか。

平成20年秋期　問72
26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符号を復号し，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符号を生成し，送信者の公開鍵で復号したハッシュ符号と比較する。

ウ　送信者は，自分の公開鍵とハッシュ関数を用いてメッセージからハッシュ符号を生成し，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符号を生成し，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：ア”

❑解説

デジタル署名の生成および検証の手順は次のとおりです。

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（ハッシュ符号）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. 一つの平文からハッシュ関数によって生成されるメッセージダイジェストは常に同じになるため、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

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符号を復号し，メッセージを得る。”

送信されてきたデジタル署名は、送信者の秘密鍵で暗号化されているので、それと対になる送信者の公開鍵で復号して、ハッシュ符号を取り出します。ハッシュ関数は一方向性なので、ハッシュ符号にハッシュ関数をかけても元のメッセージに戻すことはできません。

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符号を生成し，送信者の公開鍵で復号したハッシュ符号と比較する。”

正しい。デジタル署名は、①メッセージ ⇒ ②ハッシュ化 ⇒ ③送信者の秘密鍵で暗号化、の手順で生成され、受信者はデジタル署名を公開鍵で復号し、メッセージのハッシュ値と比較することで検証を行います。

ウ “送信者は，自分の公開鍵とハッシュ関数を用いてメッセージからハッシュ符号を生成し，メッセージとともに送信する。”

送信者が、メッセージのハッシュ符号を生成するときに使用するのはハッシュ関数です。メッセージとともに送信するのは、ハッシュ符号を自身の秘密鍵で暗号化したデジタル署名です。

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符号を生成し，メッセージとともに送信する。”

ハッシュ符号は、メッセージをハッシュ関数で固定長の文字列に圧縮したものであり、秘密鍵をハッシュ化したものではありません。また、ハッシュ符号を平文のまま送ることもありません。

☆

ISMS適合性評価制度における情報セキュリティポリシーに関する記述のうち，適切なものはどれか。

平成19年秋期　問76
27問目／選択範囲の問題数237問

ア　重要な基本方針を定めた機密文書であり，社内の関係者以外の目に触れないようにする。

イ　情報セキュリティの方針は，事業，組織，所在地，資産及び技術の特徴を考慮して策定する。

ウ　セキュリティの基本方針を述べたものであり，ビジネスの環境や技術が変化しても変更してはならない。

エ　特定のシステムについてリスク分析を行い，そのセキュリティ対策とシステム運用の詳細を記述したものである。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ管理

❑正解

イ　“あなたの解答：イ”

❑解説

情報セキュリティポリシーは、組織の経営者(トップマネジメント)が最終的な責任者となり「組織が情報セキュリティに本格的に取り組む」という姿勢を示し、情報セキュリティの目標と、その目標を達成するために企業・組織がとるべき行動を社内外に宣言する文書です。情報資産をどのような脅威から、どのようにして守るのかについての基本的な考え方と、情報セキュリティを確保するための体制、組織および運用などの枠組みが包括的に規定されます。
策定した情報セキュリティポリシーには、有効性・妥当性を維持するために定期的な改善をすること、及び、全ての従業員に対して周知させることが求められます。

ア “重要な基本方針を定めた機密文書であり，社内の関係者以外の目に触れないようにする。”

文書の要件として必要に応じて利害関係者が入手可能であることが求められます。

イ “情報セキュリティの方針は，事業，組織，所在地，資産及び技術の特徴を考慮して策定する。”

正しい。

ウ “セキュリティの基本方針を述べたものであり，ビジネスの環境や技術が変化しても変更してはならない。”

環境や状況の変化に適合するように、常に改訂することが求められます。

エ “特定のシステムについてリスク分析を行い，そのセキュリティ対策とシステム運用の詳細を記述したものである。”

特定のシステムだけでなく、ISMSの適用範囲のすべてのシステムに対してリスクアセスメントを行います。

インターネットで公開するソフトウェアにデジタル署名を添付する目的はどれか。

平成19年秋期　問71
28問目／選択範囲の問題数237問

ア　ソフトウェアの作成者が保守責任者であることを告知する。

イ　ソフトウェアの使用を特定の利用者に制限する。

ウ　ソフトウェアの著作権が署名者であることを明示する。

エ　ソフトウェアの内容が改ざんされていないことを確認できるようにする。

❑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：エ”

❑解説

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、デジタル署名を利用して確認できることは「発信元が正当であるか」と「改ざんの有無」の2点です。また改ざんの検知はできますが、改ざん部位の特定および訂正機能はもちません。

したがって「エ」が適切な目的です。

JIS Q 2001:2001に規定されたリスク算定の定量的評価を，組織のセキュリティ対策の優先度を検討するリスク分析に適用したものはどれか。

平成21年秋期　問41
29問目／選択範囲の問題数237問

ア　過去に発生した被害件数と対策の難易度で評価する。

イ　攻撃に対する対処時間と被害の顕在性で評価する。

ウ　攻撃もとの特定可否と攻撃手法の新しさで評価する。

エ　被害が発生する確率と被害額で評価する。

❑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

エ　“あなたの解答：エ”

❑解説

定量的評価とは、リスクの大きさを金額(数値)で表す評価手法です。これに対して**定性的評価**はランク付けやレベルなどの金額以外で表す手法になります。

ア “過去に発生した被害件数と対策の難易度で評価する。”

定性的評価です。

イ “攻撃に対する対処時間と被害の顕在性で評価する。”

定性的評価です。

ウ “攻撃もとの特定可否と攻撃手法の新しさで評価する。”

定性的評価です。

エ “被害が発生する確率と被害額で評価する。”

正しい。被害想定を数値で表しているので定量的評価です。

☆☆☆

認証局が発行するCRLに関する記述のうち，適切なものはどれか。

令和2年秋期　問36
30問目／選択範囲の問題数237問

ア　CRLには，失効したデジタル証明書に対応する秘密鍵が登録される。

イ　CRLには，有効期限内のデジタル証明書のうち失効したデジタル証明書のシリアル番号と失効した日時の対応が提示される。

ウ　CRLは，鍵の漏えい，失効申請の状況をリアルタイムに反映するプロトコルである。

エ　有効期限切れで失効したデジタル証明書は，所有者が新たなデジタル証明書を取得するまでの間，CRLに登録される。

❑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：ア”

❑解説

CRL(証明書失効リスト)は、有効期限内であるにもかかわらず、秘密鍵の漏えい、紛失、証明書の被発行者の規則違反などの理由により失効したデジタル証明書が列挙されたリストです。CRLには、失効した証明書のシリアル番号と失効日時が登録されています。

ア “CRLには，失効したデジタル証明書に対応する秘密鍵が登録される。”

CRLに登録されるのはシリアル番号と失効日時です。

イ “CRLには，有効期限内のデジタル証明書のうち失効したデジタル証明書のシリアル番号と失効した日時の対応が提示される。”

正しい。CRLには、失効したデジタル証明書のシリアル番号とその証明書が失効した日時が登録されています。

ウ “CRLは，鍵の漏えい，失効申請の状況をリアルタイムに反映するプロトコルである。”

OCSP(Online Certificate Status Protocol)に関する記述です。

エ “有効期限切れで失効したデジタル証明書は，所有者が新たなデジタル証明書を取得するまでの間，CRLに登録される。”

CRLに登録されている証明書は、有効期限の満了時点でCRLから抹消されます。有効期限を過ぎたデジタル証明書は無効とみなされ使用できないので、その情報を公表しなくても問題ないからです。

☆☆

インターネットに接続された利用者のPCから，DMZ上の公開Webサイトにアクセスし，利用者の個人情報を入力すると，その個人情報が内部ネットワークのデータベース(DB)サーバに蓄積されるシステムがある。このシステムにおいて，利用者個人のデジタル証明書を用いたTLS通信を行うことによって期待できるセキュリティ上の効果はどれか。

平成30年秋期　問4(
31問目／選択範囲の問題数237問

ア　PCとDBサーバ間の通信データを暗号化するとともに，正当なDBサーバであるかを検証することができるようになる。

イ　PCとDBサーバ間の通信データを暗号化するとともに，利用者を認証することができるようになる。

ウ　PCとWebサーバ間の通信データを暗号化するとともに，正当なDBサーバであるかを検証することができるようになる。

エ　PCとWebサーバ間の通信データを暗号化するとともに，利用者を認証することができるようになる。

❑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

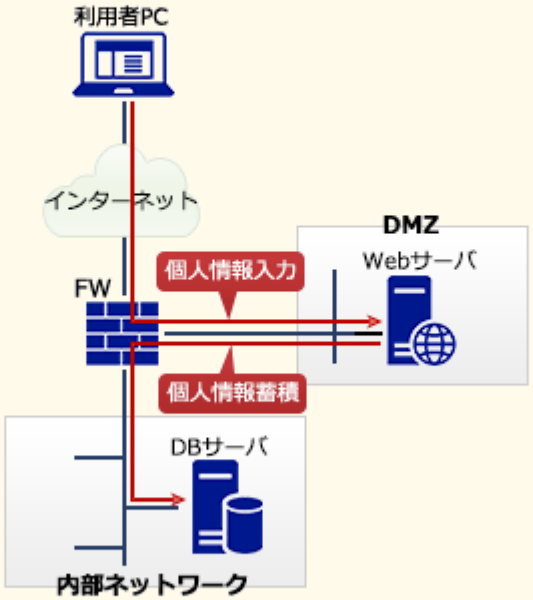
エ　“あなたの解答：エ”

❑正解

エ　“あなたの解答：エ”

❑解説

設問の関係を図示すると次のようになります。



設問の事例はDMZを介した通信になっているので、コネクションを確立するのは利用者PCとWebサーバ、WebサーバとDBサーバの組みになります。そして、デジタル証明書は利用者個人のものですので利用者認証のために使用します。

したがって適切な説明は「エ」です。

TLS通信では、必須のサーバ認証とは別にオプションでクライアント認証を行うこともできます。利用者PCと通信を行うWebサーバは、利用者個人のデジタル証明書に付された認証局の署名を検証することで、デジタル証明書の正当性を確認します。デジタル証明書が正当なものならば、利用者(クライアント)の真正性が証明されます。

ア “PCとDBサーバ間の通信データを暗号化するとともに，正当なDBサーバであるかを検証することができるようになる。”

利用者PCと通信を行うのはWebサーバです。また、利用者個人のデジタル証明書は利用者の認証に使用します。

イ “PCとDBサーバ間の通信データを暗号化するとともに，利用者を認証することができるようになる。”

DMZを介した通信なので利用者PCとDBサーバは通信を行いません。利用者PCと通信を行うのはWebサーバです。

ウ “PCとWebサーバ間の通信データを暗号化するとともに，正当なDBサーバであるかを検証することができるようになる。”

利用者個人のデジタル証明書は利用者の認証に使用します。

エ “PCとWebサーバ間の通信データを暗号化するとともに，利用者を認証することができるようになる。”

正しい。

☆☆

ディレクトリトラバーサル攻撃はどれか。

平成30年春期　問38
32問目／選択範囲の問題数237問

ア　OSコマンドを受け付けるアプリケーションに対して，攻撃者が，ディレクトリを作成するOSコマンドの文字列を入力して実行させる。

イ　SQL文のリテラル部分の生成処理に問題があるアプリケーションに対して，攻撃者が，任意のSQL文を渡して実行させる。

ウ　シングルサインオンを提供するディレクトリサービスに対して，攻撃者が，不正に入手した認証情報を用いてログインし，複数のアプリケーションを不正使用する。

エ　入力文字列からアクセスするファイル名を組み立てるアプリケーションに対して，攻撃者が，上位のディレクトリを意味する文字列を入力して，非公開のファイルにアクセスする。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

エ　“あなたの解答：エ”

❑解説

ディレクトリトラバーサル攻撃は、ファイル名を要求するプログラムに対してサーバ内の想定外のファイル名(親ディレクトリの移動「../」など)を直接指定することによって、本来許されないファイルの不正な閲覧・取得を狙う攻撃方法です。

したがって正しい記述は「エ」です。

ア　“OSコマンドを受け付けるアプリケーションに対して，攻撃者が，ディレクトリを作成するOSコマンドの文字列を入力して実行させる。”

OSコマンドインジェクション攻撃の説明です。

イ　“SQL文のリテラル部分の生成処理に問題があるアプリケーションに対して，攻撃者が，任意のSQL文を渡して実行させる。”

SQLインジェクション攻撃の説明です。

ウ　“シングルサインオンを提供するディレクトリサービスに対して，攻撃者が，不正に入手した認証情報を用いてログインし，複数のアプリケーションを不正使用する。”

不正アクセスの事例です。

エ　“入力文字列からアクセスするファイル名を組み立てるアプリケーションに対して，攻撃者が，上位のディレクトリを意味する文字列を入力して，非公開のファイルにアクセスする。”

正しい。ディレクトリトラバーサル攻撃の説明です。

☆

虹彩認証に関する記述のうち，最も適切なものはどれか。

令和元年秋期　問45
33問目／選択範囲の問題数237問

ア　経年変化による認証精度の低下を防止するために，利用者の虹彩情報を定期的に登録し直さなければならない。

イ　赤外線カメラを用いると，照度を高くするほど，目に負担を掛けることなく認証精度を向上させることができる。

ウ　他人受入率を顔認証と比べて低くすることが可能である。

エ　本人が装置に接触したあとに残された遺留物を採取し，それを加工することによって認証データを偽造し，本人になりすますことが可能である。

❑分類

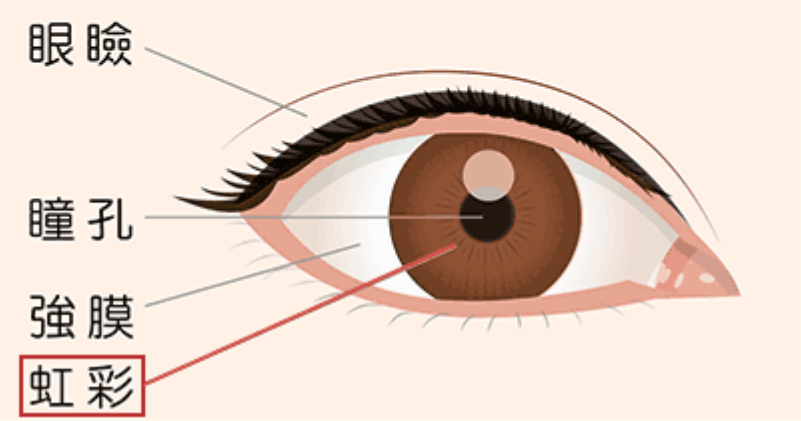
テクノロジ系 » セキュリティ » 情報セキュリティ対策

❑正解

ウ　“あなたの解答：ウ”

❑解説

虹彩認証とは、眼球の特徴で本人認証を行うバイオメトリクス認証技術です。**虹彩**とは、眼球の黒目部分、瞳孔の外側にある円状の部分のことで、その部分のしわのパターンが個人ごとに異なることを認証に利用します。



ア “経年変化による認証精度の低下を防止するために，利用者の虹彩情報を定期的に登録し直さなければならない。”

虹彩は、満2歳以降は経年変化しないので虹彩情報を更新する必要はありません。

イ “赤外線力メラを用いると，照度を高くするほど，目に負担を掛けることなく認証精度を向上させることができる。”

虹彩情報を得るためには、一般的に赤外線力メラを用いて静脈内を流れる血液中のヘモグロビンに近赤外線を照射しますが、照度を高くすると精度の高い像が得られる反面、目に負担が掛かります。

ウ “他人受入率を顔認証と比べて低くすることが可能である。”

正しい。顔認証よりも高精度な認証が可能です。顔認証では判別が難しい一卵性双生児も判別可能です。またマスクや眼鏡の着脱も関係ありません。

エ “本人が装置に接触したあとに残された遺留物を採取し，それを加工することによって認証データを偽造し，本人になりすますことが可能である。”

センサー部に触れずに認証できるので指紋認証のように遺留物が残ることがありません。また衛生面も優れています。

☆☆☆

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。

平成30年秋期　問36
34問目／選択範囲の問題数237問

ア	IPA	イ	JIPDEC	ウ	JPCERT/CC	エ	NISC

❑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

エ　“あなたの解答：エ”

❑解説

NISC(内閣サイバーセキュリティセンター)は、内閣官房に設置され、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政策の推進に係る企画などを行う機関です。

サイバーセキュリティ基本法では、内閣への「サイバーセキュリティ戦略本部」の設置と行うべき事務を規定しており、その事務については内閣官房で処理することと定めています。この事務を行うために内閣官房に置かれている組織がNISCです。

したがって「エ」が正解です。

ア　“IPA”

IPA(情報処理推進機構)は、経済産業省所管の独立行政法人です。産業サイバーセキュリティセンターが設置されています。

イ　“JIPDEC”

JIPDEC(一般財団法人日本情報経済社会推進協会)は、プライバシーマーク制度などを運用する一般財団法人です。

ウ　“JPCERT/CC”

JPCERT/CCは、インターネットを介して発生する侵入やサービス妨害等のコンピュータセキュリティインシデントについて、日本国内のサイトに関する報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行う一般社団法人です。

エ　“NISC”

正しい。NISCは、内閣官房に設置されている機関です。

☆☆☆

無線LANのセキュリティプロトコル，暗号アルゴリズム，暗号鍵の鍵長の組合せのうち，適切なものはどれか。

平成30年秋期　問45
35問目／選択範囲の問題数237問

	セキュリティプロトコル	暗号アルゴリズム	暗号鍵の鍵長
ア	WPA（TKIP）	AES	128，192又は256ビット
イ	WPA（TKIP）	RC4	64ビット
ウ	WPA2（CCMP）	AES	128ビット
エ	WPA2（CCMP）	RC4	64ビット

ア　イ　ウ　エ

❑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

WPAとWPA2のセキュリティプロトコル、暗号アルゴリズム、暗号鍵の鍵長をまとめると次のようになります。

	方式	暗号アルゴリズム	暗号化鍵の鍵長
WPA	WPA-TKIP	RC4	128ビット
	WPA-AES	AES	128/192/256ビット
WPA2	WPA2-TKIP	RC4	128ビット
	WPA2-AES	CCMP(AES)	128/192/256ビット

ア　WPAでは WPA-TKIP または WPA-AES を選択可能ですが、TKIPのときは必ずRC4を使用することになります。

イ　WPAのRC4暗号鍵の鍵長は128ビットです。

ウ　正しい。WPA2-AESではCCMモードのAES(CCMP)に基づいて暗号化を行います。また、AESの鍵長は128ビット、192ビット、256ビットから選択します。

エ　WPA2では WPA2-TKIP または WPA2-AES(CCMP) を選択可能ですが、CCMPはAESベースの暗号化アルゴリズムですのでCCMPのときには必ずAESを使用することになります。

※WPA（Wi-Fi Protected Access）
：線 LAN 機器が Wi-Fi Alliance が策定したセキュリティプロトコルに準拠していることを示す認証プログラム、あるいはセキュリティプロトコル

☆☆☆

クレジットカードの対面決済時の不正利用に対して，カード加盟店が実施する対策のうち，最も有効なものはどれか。

令和3年春期　問43
36問目／選択範囲の問題数237問

ア　ICチップを搭載したクレジットカードによる決済時の本人確認のために，サインではなくオフラインPINを照合する。

イ　クレジットカードのカード番号を加盟店で保持する。

ウ　クレジットカードの決済ではICチップではなく磁気ストライプの利用を利用者に促す。

エ　利用者の取引履歴からクレジットカードの不正利用を検知するオーソリモニタリングを実施する。

❑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

ア　“あなたの解答：エ”

❑解説

ア “ICチップを搭載したクレジットカードによる決済時の本人確認のために，サインではなくオフラインPINを照合する。”

正しい。オフラインPINとは、クレジットカードのICチップ内に保存されている暗証番号で、決済時にICチップ対応決済端末に入力することで本人確認を行います。サインはマネできてしまいますし、カード偽造、紛失・盗難カードによる不正利用を防げないので、オフラインPINによる認証の方が有効です。

イ “クレジットカードのカード番号を加盟店で保持する。”

カード情報を保護するため、カード加盟店に対しては、カード情報を保持しない「非保持化」またはカード情報を保持する場合はPCI DSSに準拠することが求められています。PCI DSS準拠するためには12の要件に基づく400以上の要求事項に対応する必要があるので、普通のカード加盟店は「非保持化」を選択することになります。したがって、カード番号を加盟店で保持するのは逆にリスクを高める行為となります。
※非保持化とは、自社で保有する機器・ネットワークにおいてカード情報を「保存」「処理」「通過」しないことを意味します。

ウ “クレジットカードの決済ではICチップではなく磁気ストライプの利用を利用者に促す。”

磁気ストライプで情報を記録するクレジットカードは、スキミング等による情報の盗み取りに対して脆弱なので、セキュリティ面で優れるICチップタイプの利用を促すべきです。2021年現在において対面取引のクレジットカードにおける不正利用対策としては、IC取引が最も効果的です。本肢はどちらかと言えばカード会社が実施する対策と言えます。

エ “利用者の取引履歴からクレジットカードの不正利用を検知するオーソリモニタリングを実施する。”

オーソリモニタリングとは、カード会社がオーソリゼーション情報（決済可能か検証するための情報）等により不正利用を検知する仕組みです。本問ではカード加盟店が実施する不正利用対策が問われているため不適切です。

参考URL: クレジットカード・セキュリティガイドライン
https://www.j-credit.or.jp/security/safe/plan.html

☆

OpenPGPやS/MIMEにおいて用いられるハイブリッド暗号方式の特徴はどれか。

平成28年秋期　問42
37問目／選択範囲の問題数237問

ア　暗号通信方式としてIPsecとTLSを選択可能にすることによって利用者の利便性を高める。

イ　公開鍵暗号方式と共通鍵暗号方式を組み合わせることによって鍵管理コストと処理性能の両立を図る。

ウ　複数の異なる共通鍵暗号方式を組み合わせることによって処理性能を高める。

エ　複数の異なる公開鍵暗号方式を組み合わせることによって安全性を高める。

❑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

ハイブリッド暗号方式は、公開鍵暗号方式を用いて共通鍵を通信相手へ安全に配送し、以後はその共通鍵を使用して暗号化通信を行う方式です。TLSやS/MIMEで採用されています。

それぞれの暗号方式を他方と比較すると次のような短所があります。

共通鍵暗号方式

安全に鍵を配送するのに手間が掛かる
通信相手が増えると必要な鍵数が多くなる

公開鍵暗号方式

暗号化・復号に要する計算量が多いため処理に時間が掛かる

ハイブリッド暗号方式は、両者を組み合わせることで、当事者間で鍵を安全に共有しつつ、低い処理負荷での暗号化・復号を可能にしています。したがって「イ」が適切な記述です。

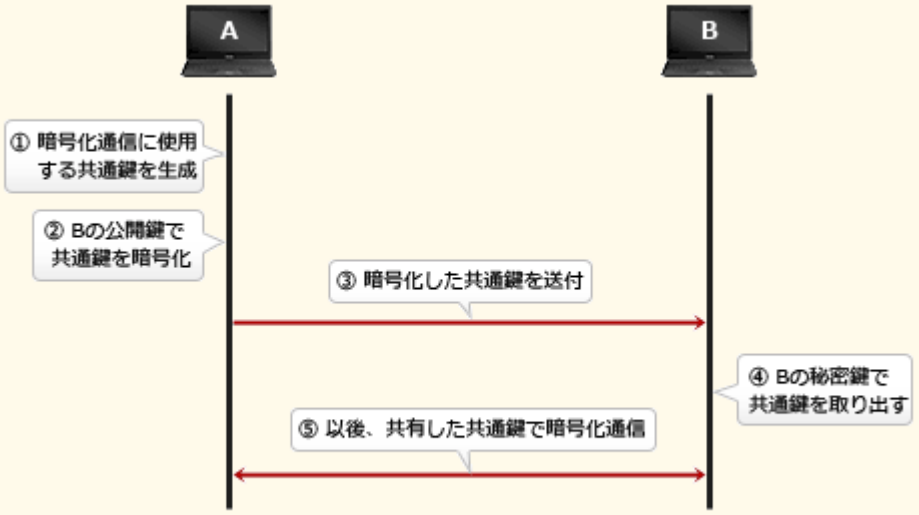


図　ハイブリッド暗号方式

☆☆☆

HTTPSを用いて実現できるものはどれか。

平成19年春期　問76
38問目／選択範囲の問題数237問

ア　Webサーバ上のファイルの改ざん検知

イ　クライアント上のウイルス検査

ウ　クライアントに対する侵入検知

エ　電子証明書によるサーバ認証

❑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

エ　“あなたの解答：エ”

❑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通信経路上でデータのやり取り(HTTP通信)を行う方式です。HTTPプロトコルは、平文のままで情報をやり取りするため、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には危険が伴います。TLSから提供される通信の暗号化、デジタル証明書を用いたノードの認証、改ざん検出などの機能を使用することで、HTTPS通信を「なりすまし」や「盗聴」による攻撃から通信を保護できるようになっています。

SSL/TLSでは、クライアントがサーバに接続を要求すると、サーバはクライアントに対してデジタル証明書(公開鍵証明書，サーバ証明書)を提示することになっています。クライアントはこのデジタル証明書を検証することで、これから暗号化通信を行おうとするサーバの正当性を確認できます。

したがって答えは「電子証明書によるサーバ認証」になります。

☆☆☆☆

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その効果の組みとして，適切なものはどれか。

令和5年春期　問43
39問目／選択範囲の問題数237問

	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，悪意の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アクセスポイント経由の通信を遮断する。	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アクセスすることを防止する。

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：ア”

❑解説

ア MACアドレスフィルタリングは、無線LANのアクセスポイントに正当な機器のMACアドレスを登録しておくことで、正当な機器以外からのアクセスを拒否する機能です。しかし、MACアドレスを正当なものに偽装している端末からの接続を遮断することはできません。

イ SSIDを暗号化することはできません。SSIDを秘匿にするためにはアクセスポイントにSSIDステルスの設定を行います。これにより、アクセスポイントから発せられるビーコンにSSIDの情報が含まれなくなるため、第三者にアクセスポイントのSSIDを知られてしまう危険性を低くできます。

ウ ドメイン名は公開されていて、悪意のあるアクセスポイントのSSIDとして他者のドメインを設定することも可能なので、対策として意味がありません。不正なアクセスポイントの設置に対しては、SSIDや暗号化キーを類推できないものにすることがある程度の対策になります。

エ 正しい。無線LANのプライバシーセパレータ機能(アクセスポイントアイソレーション)についての記述です。
プライバシーセパレータは、同一の無線LANに接続された子機同士の通信を禁止する機能です。店舗内Wi-fiや公衆無線LANサービスのように見知らぬ他人同士が同じ無線LANに接続する場面で、利用者のセキュリティ保護のために設定されます。

図　プライバシーセパレータ機能

☆

暗号アルゴリズムの危殆(たい)化を説明したものはどれか。

平成25年春期　問37
40問目／選択範囲の問題数237問

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，膨大な時間やコストを掛けて暗号強度をより確実なものにすること

❑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：ウ”

❑解説

素因数分解問題を応用したRSAや離散対数問題を応用したエルガマル暗号など、解読に膨大な量の計算が必要になることを安全性の根拠にしている暗号アルゴリズムが多くなっています。
暗号アルゴリズムの危殆化とは、技術の進歩によってコンピュータの計算性能が高まり、解読に要する計算を現実的な時間で行うことができる可能性が生じることで暗号アルゴリズムの安全性が低下してしまう状況をいいます。実際に2010年には、

- 2-key Triple DES
- 鍵長1,024ビットのRSA
- 鍵長1,024ビットのDSA
- 鍵長160ビットのECDSA
- ハッシュ関数 SHA-1

の5つが安全性低下の理由で米国政府標準暗号から廃止されています。

したがって適切な記述は「計算能力の向上などによって，鍵の推定が可能となり，暗号の安全性が低下すること」となります。

☆☆☆

ステガノグラフィを説明したものはどれか。

平成24年春期　問44
41問目／選択範囲の問題数237問

ア　データをコピーできないようにする技術のことをいう。

イ　データを第三者に盗み見られても解読できないようにするために，決まった規則に従ってデータを変換することをいう。

ウ　文書の正当性を保証するために付けられる暗号化された署名情報のことをいう。

エ　メッセージを画像データや音声データなどに埋め込み，メッセージの存在を隠す技術のことをいう。

❑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

ステガノグラフィ(Steganography)とは、音声や画像などのデータの中に、別のデータ(多くの場合文字列)を秘密裏に埋め込む技術や考え方のことです。デジタルデータの世界では著作物に著作者名や利用者の情報などを埋め込む「電子透かし技術」として応用されています。

ア “データをコピーできないようにする技術のことをいう。”

コピーガードの説明です。

イ “データを第三者に盗み見られても解読できないようにするために，決まった規則に従ってデータを変換することをいう。”

クリプトグラフィ(暗号化)の説明です。

ウ “文書の正当性を保証するために付けられる暗号化された署名情報のことをいう。”

デジタル署名の説明です。

エ “メッセージを画像データや音声データなどに埋め込み，メッセージの存在を隠す技術のことをいう。”

正しい。ステガノグラフィの説明です。

☆☆

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(ポート番号80)にアクセスできるようにするとき，パケットフィルタリングルールで許可するものの適切な組合せはどれか。

平成19年秋期　問73
42問目／選択範囲の問題数237問

		送信元	あて先	送信元 ポート番号	あて先 ポート番号
ア	発信	PC	Web サーバ	80	1024 以上
	応答	Web サーバ	PC	1024 以上	80
イ	発信	PC	Web サーバ	1024 以上	80
	応答	Web サーバ	PC	80	1024 以上
ウ	発信	Web サーバ	PC	80	1024 以上
	応答	PC	Web サーバ	80	1024 以上
エ	発信	Web サーバ	PC	1024 以上	80
	応答	PC	Web サーバ	80	1024 以上

ア　イ　ウ　エ

❑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

パケットフィルタリングでは、パケットのヘッダー情報内のIPアドレス及びポート番号を基準にパケット通過の可否を決定します。

ポート番号は、通信をする際にあて先のプログラムを特定するための0から65535(16ビット符号無し整数)の番号です。IPアドレスが建物の住所だとすれば、ポート番号は部屋番号ということになります。0～1023までは「WELL KNOWN PORT NUMBERS」と言い、よく利用されるアプリケーション用に予約されています。
(HTTP:TCP/80、FTP:20/TCP、SMTP:25/TCPなど)

インターネット通信に使われるプロトコルは**HTTP**(HyperText Transfer Protocol)で、ポート番号は80です。このため、インターネット上のWebサーバにアクセスできるようにするには、内部からWebサーバの80番ポートに向けた発信パケット(HTTPリクエスト)、および逆向きの、Webサーバのポート80からクライアントPCの1024番以上に向けた応答パケット(HTTPレスポンス)の通過を許可する必要があります。

したがって正しいルール設定は「イ」です。

☆☆☆

ピヘイビア法のウイルス検出手法に当たるものはどれか。

平成25年秋期　問41
43問目／選択範囲の問題数237問

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。

❑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

ビヘイビア法は、ウイルスの実際の感染・発病動作を監視して検出する手法です。
感染・発病動作として「書込み動作」「複製動作」「破壊動作」等の動作そのものの異常を検知するだけでなく、感染・発病動作によって起こる環境の様々な変化を察知してウイルスを見い出すこともあります。例えば「例外ポート通信・不完パケット・通信量の異常増加・エラー量の異常増加」「送信時データと受信時データの量的変化・質的変化」等がそれに該当します。

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。”

チェックサム法/インテグリティチェック法の説明です。

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。”

コンペア法の説明です。

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。”

ハッシュ値を使用した検出手法です。

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。”

正しい。ビヘイビア法の説明です。

☆☆☆

無線LAN環境におけるWPA2-PSKの機能はどれか。

令和元年秋期　問39
44問目／選択範囲の問題数237問

ア　アクセスポイントに設定されているSSIDを共通鍵とし，通信を暗号化する。

イ　アクセスポイントに設定されているのと同じSSIDとパスワード(Pre-Shared Key)が設定されている端末だけに接続を許可する。

ウ　アクセスポイントは，IEEE 802.11acに準拠している端末だけに接続を許可する。

エ　アクセスポイントは，利用者ごとに付与されたSSIDを確認し，無線LANへのアクセス権限を識別する。

❑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

WPA2-PSK(WPA2 Pre-Shared Key)は、無線LANの暗号化方式の規格であるWPA2のうち個人宅やスモールオフィスなどの比較的小規模なネットワークで使用されることを想定したパーソナルモードです。このモードではアクセスポイントと端末間で事前に8文字から63文字から成る**パスフレーズ**(PSK:Pre-Shared Key)を共有しておき、そのパスフレーズとSSIDによって端末の認証を行います。

したがって「イ」が適切です。

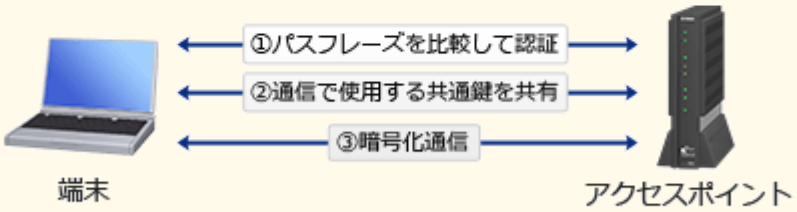


図　WPA2-PSK

なお、認証にパスワードでなくIEEE802.1Xに準拠した認証サーバを使用する方式は「WPA2 エンタープライズモード」と呼ばれます。

ア “アクセスポイントに設定されているSSIDを共通鍵とし，通信を暗号化する。”

SSIDはアクセスポイントの識別子であり暗号化鍵としては使用されません。

イ “アクセスポイントに設定されているのと同じSSIDとパスワード(Pre-Shared Key)が設定されている端末だけに接続を許可する。”

正しい。

ウ “アクセスポイントは，IEEE 802.11acに準拠している端末だけに接続を許可する。”

端末の認証はパスワードによって行われます。

エ “アクセスポイントは，利用者ごとに付与されたSSIDを確認し，無線LANへのアクセス権限を識別する。”

無線LANではアクセスポイントと同じSSIDをもつ端末としか通信できないようになっていますが、これはWPA2ではなく無線LANの規格IEEE 802.11の機能です。

☆☆

セキュアブートの説明はどれか。

令和5年秋期　問42
45問目／選択範囲の問題数237問

ア　BIOSにパスワードを設定し，PC起動時にBIOSのパスワード入力を要求することによって，OSの不正な起動を防ぐ技術

イ　HDD又はSSDにパスワードを設定し，PC起動時にHDD又はSSDのパスワード入力を要求することによって，OSの不正な起動を防ぐ技術

ウ　PCの起動時にOSのプログラムやドライバのデジタル署名を検証し，デジタル署名が有効なものだけを実行することによって，OS起動完了前のマルウェアの実行を防ぐ技術

エ　マルウェア対策ソフトをスタートアッププログラムに登録し，OS起動時に自動的にマルウェアスキャンを行うことによって，マルウェアの被害を防ぐ技術

❑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：ア”

❑解説

セキュアブートとは、コンピュータの起動時にOS起動ファイルやドライバのデジタル署名を検証し、起動プロセスを認証することで、OS起動前に不正なプログラムが実行されることを未然に防止する仕組みです。BIOSに代わる新仕様であるUEFI(Unified Extensible Firmware Interface)で規定されていて、WindowsではWindows8以降が対応しています。セキュアブートを行うことで、HDDのブートセクタに感染するタイプのマルウェアの実行も防止できます。

ア “BIOSにパスワードを設定し，PC起動時にBIOSのパスワード入力を要求することによって，OSの不正な起動を防ぐ技術”

BIOSパスワードの説明です。

イ “HDD又はSSDにパスワードを設定し，PC起動時にHDD又はSSDのパスワード入力を要求することによって，OSの不正な起動を防ぐ技術”

HDDパスワードの説明です。

ウ “PCの起動時にOSのプログラムやドライバのデジタル署名を検証し，デジタル署名が有効なものだけを実行することによって，OS起動完了前のマルウェアの実行を防ぐ技術”

正しい。セキュアブートの説明です。

エ “マルウェア対策ソフトをスタートアッププログラムに登録し，OS起動時に自動的にマルウェアスキャンを行うことによって，マルウェアの被害を防ぐ技術”

セキュアブートはOS起動前のマルウェア実行を防ぐ技術です。

☆

JIS Q 27000で定義された情報セキュリティの特性に関する記述のうち，否認防止の特性に該当するものはどれか。

平成28年春期　問39
46問目／選択範囲の問題数237問

ア　ある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。

イ　意図する行動と結果が一貫性をもつ。

ウ　認可されたエンティティが要求したときにアクセスが可能である。

エ　認可された個人，エンティティイ又はプロセスに対してだけ，情報を使用させる又は開示する。

❑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

ア　“あなたの解答：ア”

❑解説

否認防止(Non-Repudiation)は、情報セキュリティマネジメントの付加的な要素で、行った操作や発生した事象を後になって否認されないように証明することができる能力のことです。ログの取得で必要な項目を確実に記録するとともに、完全性が損なわれてないように保存することで確保できます。デジタル署名やタイムスタンプは否認防止に活用される技術です。
JIS Q 27000では「主張された事象又は処理の発生，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。

ア “ある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。”

正しい。否認防止の説明です。

イ “意図する行動と結果が一貫性をもつ。”

信頼性の説明です。

ウ “認可されたエンティティが要求したときにアクセスが可能である。”

可用性の説明です。

エ “認可された個人，エンティテイ又はプロセスに対してだけ，情報を使用させる又は開示する。”

機密性の説明です。

☆☆☆

ネットワーク障害の原因を調べるために，ミラーポートを用意して，LANアナライザーを使用するときに留意することはどれか。

平成25年春期　問41
47問目／選択範囲の問題数237問

ア　LANアナライザーがパケットを破棄してしまうので，測定中は測定対象外のコンピュータの利用を制限しておく必要がある。

イ　LANアナライザーにはネットワークを通過するパケットを表示できるので，盗聴などに悪用されないように注意する必要がある。

ウ　障害発生に備えて，ネットワーク利用者にLANアナライザーの保管場所と使用方法を周知しておく必要がある。

エ　測定に当たって，LANケーブルを一時的に切断する必要があるので，利用者に対して測定日を事前に知らせておく必要がある。

❑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

イ　“あなたの解答：イ”

❑解説

LANアナライザーは、LAN上を通過するパケットを監視したり記録するためのハードウェアまたはソフトウェアのことです。LANアナライザーが悪用されると盗聴などの被害をもたらす危険があるので慎重な管理が求められます。

ア “LANアナライザーがパケットを破棄してしまうので，測定中は測定対象外のコンピュータの利用を制限しておく必要がある。”

パケットは破棄されません。

イ “LANアナライザーにはネットワークを通過するパケットを表示できるので，盗聴などに悪用されないように注意する必要がある。”

正しい。

ウ “障害発生に備えて，ネットワーク利用者にLANアナライザーの保管場所と使用方法を周知しておく必要がある。”

保管場所が知られると不正利用される危険性が高まるので不適切です。

エ “測定に当たって，LANケーブルを一時的に切断する必要があるので，利用者に対して測定日を事前に知らせておく必要がある。”

ハブやスイッチのミラーポートに接続するので切断の必要はありません。

☆☆

攻撃者が行うフットプリンティングに該当するものはどれか。

令和3年春期　問38
48問目／選択範囲の問題数237問

ア　Webサイトのページを改ざんすることによって，そのWebサイトから社会的・政治的な主張を発信する。

イ　攻撃前に，攻撃対象となるPC，サーバ及びネットワークについての情報を得る。

ウ　攻撃前に，攻撃に使用するPCのメモリを増設することによって，効率的に攻撃できるようにする。

エ　システムログに偽の痕跡を加えることによって，攻撃後に追跡を逃れる。

❑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：ア”

❑解説

フットプリンティングは、特定のコンピュータにサイバー攻撃を行う前の事前準備として、攻撃対象を下調べする行為です。コンピュータやWebページ内の脆弱性の有無を調査したり、検索エンジン、公開データベースおよびツールを用いて個人や組織の情報を収集したりするなど、攻撃の足掛かりとなる情報を得る行為が該当します。

したがって「イ」が正解です。

ア “Webサイトのページを改ざんすることによって，そのWebサイトから社会的・政治的な主張を発信する。”

ハクティビズムの説明です。情報技術を高度に利用し、信教や政治的な目標を達成しようとする行為や行動思想のことを言います。

イ “攻撃前に，攻撃対象となるPC，サーバ及びネットワークについての情報を得る。”

正しい。フットプリンティングの説明です。

ウ “攻撃前に，攻撃に使用するPCのメモリを増設することによって，効率的に攻撃できるようにする。”

フットプリンティングと同じく攻撃の事前準備ですが、特に該当する用語はありません。

エ “システムログに偽の痕跡を加えることによって，攻撃後に追跡を逃れる。”

ルートキットの機能に関する記述です。

☆

セキュリティ対策の"予防"に該当するものはどれか。

平成17年秋期　問75
49問目／選択範囲の問題数237問

ア　アクセスログをチェックし，不正なアクセスがないかどうかを監視する。

イ　コンティンジェンシープランを策定し，訓練を実施する。

ウ　重要ファイルのバックアップ処理を定期的に行う。

エ　セキュリティに関する社内教育を実施し，個人の意識を高める。

❑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

セキュリティ対策における"予防"とは、物理的環境、人、情報システムなどの脆弱な部分に対して、事前にセキュリティ対策を行うことで被害が発生しにくい強固な状態を作り出すことです。

ア　“アクセスログをチェックし，不正なアクセスがないかどうかを監視する。”

異常を検知し被害を最小限に抑える対策なので、セキュリティ対策の"検知・追跡"に該当します。

イ　“コンティンジェンシープランを策定し，訓練を実施する。”

被害が発生した場合に正常な状態に復旧させるための対策なので、セキュリティ対策の"回復"に該当します。

ウ　“重要ファイルのバックアップ処理を定期的に行う。”

「イ」と同じくセキュリティ対策の"回復"に該当します。

エ　“セキュリティに関する社内教育を実施し，個人の意識を高める。”

正しい。セキュリティに関する社内教育には、犯罪や不正行為を思いとどまらせる抑止効果を期待することができます。問題を未然に防ぐための対策なので"予防"に該当します。

☆☆

電子メールをスマートフォンで受信する際のメールサーバとスマートフォンとの間の通信をメール本文を含めて暗号化するプロトコルはどれか。

令和2年秋期　問45
50問目／選択範囲の問題数237問

ア	APOP	イ	IMAPS
ウ	POP3	エ	SMTP Submission

❑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

IMAPS(IMAP over SSL/TLS)は、メール受信プロトコルであるIMAP(Internet Message Access Protocol)にTLSを組み合わせ、TLSによって暗号化された通信コネクション上でメール受信を行うプロトコルです。バージョン番号を付けてIMAP4Sと表記されることもあります。

既存のプロトコル名の後ろに"S"が付いているものは、TLSにより暗号化されたものであることが多いです。HTTPSもその1つです。POP3にもTLS版であるPOP3Sというプロトコルがあります。

ア　“APOP”

Authenticated POPの略。メール受信前の認証におけるパスワード送信を暗号化(MD5ハッシュ化)することで安全性を高めたプロトコルです。暗号化されるのはパスワードだけなので、メール本文は暗号化されず平文のまま通信経路上を流れます。

イ　“IMAPS”

正しい。IMAPSは認証やメール本文の受信など、IMAP通信の全てをTLSによって暗号化するプロトコルです。

ウ　“POP3”

POP3は、認証やメール本文の通信を平文で行うメール受信プロトコルです。

エ　“SMTP Submission”

SMTP Submissionは、ユーザー(メールソフト)からのメール送信を専門に受け付けるサブミッションポート(587/TCP)を用意し、SMTP-AUTH認証を経たユーザーからのメールだけを送信する仕組みです。メール受信用途ではなく、OP25Bの影響を受けずに外部のメールサーバを使用したメール送信を可能にする仕組みなので誤りです。