0001 個人情報・プライバシー > 個人情報保護法・安全管理措置 ｜ 難易度：基礎

個人情報保護法上の「個人情報」の説明として、最も適切なものはどれか。

ア：生存する個人に関する情報で、氏名等の記述により特定の個人を識別できるものや、個人識別符号が含まれるもの。

イ：法人そのものの売上高や所在地だけを記録した情報は、必ず個人情報に該当する。

ウ：暗号化された情報は、復号鍵を事業者が保有していても必ず個人情報ではない。

エ：死亡した個人に関する情報は、どのような場合でも個人情報保護法上の個人情報である。

答え・解説 正答：ア

ア：個人情報保護法では、生存する個人に関する情報で特定個人を識別できるもの等を個人情報として扱います。

イ：法人に関する情報であることだけでは個人情報にはなりません。ただし、担当者氏名など生存する個人を識別できる情報を含めば個人情報となり得ます。

ウ：暗号化していても、事業者が特定個人を識別できる状態であれば個人情報性が直ちに失われるわけではありません。

エ：個人情報保護法上の個人情報は「生存する個人」に関する情報が基本です。ただし遺族など生存者を識別できる情報を含む場合は別途検討が必要です。

総合解説：個人情報かどうかは、単に氏名があるかではなく、生存する個人を識別できるか、個人識別符号を含むか等で判断します。暗号化や社内ID化だけで自動的に個人情報でなくなるわけではありません。

対象：2026年度 / 基準日 2026-09-05

0002 個人情報・プライバシー > 個人情報保護法・安全管理措置 ｜ 難易度：基礎

個人情報保護法上の「個人データ」に該当するものとして、最も適切なものはどれか。

ア：個人情報であれば、整理・検索可能性に関係なく必ず個人データになる。

イ：個人情報データベース等を構成する個人情報。

ウ：匿名加工情報は、常に元の本人を容易に識別できるので個人データである。

エ：企業秘密であれば、個人と無関係でも個人データになる。

答え・解説 正答：イ

ア：すべての個人情報が個人データになるわけではなく、個人情報データベース等を構成するかがポイントです。

イ：個人データは、個人情報データベース等を構成する個人情報を指します。

ウ：匿名加工情報は所定の加工により特定個人を識別できず復元できないようにされた情報で、通常の個人データとは異なる規律が適用されます。

エ：営業秘密かどうかと、個人データ該当性は別の概念です。

総合解説：試験では「個人情報」「個人データ」「保有個人データ」の違いが狙われます。安全管理措置、第三者提供、開示等の義務は、どの区分に対する規律かを区別して理解します。

対象：2026年度 / 基準日 2026-09-05

0003 個人情報・プライバシー > 個人情報保護法・安全管理措置 ｜ 難易度：基礎

個人データの安全管理措置について、個人情報保護委員会のガイドラインが示す分類の組合せとして、最も適切なものはどれか。

ア：安全管理措置は技術的対策だけを指し、教育や入退室管理は含まれない。

イ：物理的対策だけを講じれば、アクセス制御や従業者教育は不要である。

ウ：組織的・人的・物理的・技術的安全管理措置に加え、外国で個人データを取り扱う場合には外的環境の把握も考慮する。

エ：安全管理措置は個人データの漏えいが発生した後にだけ必要となる。

答え・解説 正答：ウ

ア：安全管理措置は技術だけではなく、組織・人・物理面を含む多層的なものです。

イ：物理対策だけでは個人データの安全管理として不十分です。

ウ：通則ガイドラインは、基本方針・規律整備に加え、組織的、人的、物理的、技術的安全管理措置と外的環境の把握を示しています。

エ：安全管理措置は漏えい等を防止するため平常時から講じる必要があります。

総合解説：安全管理措置は一つの製品導入で完結しません。組織ルール、教育、機器・媒体管理、アクセス制御、外部環境の把握などを事業規模・取扱状況に応じて組み合わせます。

対象：2026年度 / 基準日 2026-09-05

0004 個人情報・プライバシー > 個人情報保護法・安全管理措置 ｜ 難易度：標準

ECサイト運営会社が、商品発送のために取得した顧客住所を、本人への説明や法的根拠の確認をせず別会社の営業リストとして利用しようとしている。最も適切な考え方はどれか。

ア：一度取得した個人情報は企業の所有物なので、どの目的でも自由に利用できる。

イ：住所は秘密情報ではないため、利用目的を考慮する必要はない。

ウ：社内で利用する限り、利用目的の制限は一切適用されない。

エ：当初特定した利用目的との関係を確認し、利用目的の達成に必要な範囲を超える取扱いになる場合は、法令上認められる場合を除き本人同意等が必要となる。

答え・解説 正答：エ

ア：個人情報保護法は利用目的による制限を設けており、自由利用ではありません。

イ：公知かどうかだけで利用目的の規律が消えるわけではありません。

ウ：社内利用でも、利用目的の達成に必要な範囲を超える取扱いには規律があります。

エ：個人情報の利用は、特定した利用目的の達成に必要な範囲内で行うのが原則です。別目的利用は適法性を確認する必要があります。

総合解説：個人情報の取扱いでは「何のために取得したか」と「何に使うか」を対応させます。新たな利用が当初目的から合理的に関連する範囲か、本人同意等が必要かを確認します。

対象：2026年度 / 基準日 2026-09-05

0005 個人情報・プライバシー > 個人情報保護法・安全管理措置 ｜ 難易度：標準

顧客データを扱う従業者に対する安全管理として、最も適切なものはどれか。

ア：取扱規程を整備し、必要な教育を行い、権限に応じたアクセスを設定し、遵守状況を確認する。

イ：採用時に誓約書を1回提出させれば、その後の教育や権限見直しは不要である。

ウ：業務効率を優先し、全従業者へ顧客データの管理者権限を付与する。

エ：退職者のアカウントは引継ぎに便利なので無期限に残す。

答え・解説 正答：ア

ア：個人データの安全管理には、従業者に対する必要かつ適切な監督が含まれます。

イ：継続的な教育・権限管理・監督が必要で、誓約書だけでは十分ではありません。

ウ：必要以上の権限付与は漏えい・不正利用リスクを高めます。

エ：不要アカウントの残存は不正利用リスクとなるため、速やかな無効化が必要です。

総合解説：人的安全管理では教育だけでなく、役割・権限・退職や異動時の処理、違反時対応などを含めて監督します。

対象：2026年度 / 基準日 2026-09-05

0006 個人情報・プライバシー > 個人情報保護法・安全管理措置 ｜ 難易度：標準

個人データを含む顧客管理業務を外部事業者へ委託する場合の対応として、最も適切なものはどれか。

ア：委託した時点で個人データに関する責任はすべて委託先へ移るため、委託元は監督不要である。

イ：委託先を適切に選定し、契約等で安全管理に必要な事項を定め、取扱状況を把握するなど必要かつ適切な監督を行う。

ウ：価格だけで委託先を選び、安全管理体制を確認しない。

エ：委託先の再委託や事故報告条件を一切確認しない。

答え・解説 正答：イ

ア：委託元には委託先に対する必要かつ適切な監督が求められます。

イ：個人情報取扱事業者には、個人データの取扱いを委託する場合の委託先監督が求められます。

ウ：個人データを扱う委託では、安全管理能力を含めた選定が重要です。

エ：再委託や事故対応はリスク管理上の重要事項であり、契約・運用で把握すべきです。

総合解説：委託先管理は「契約したから終わり」ではありません。選定、契約、定期確認、インシデント時の連絡、終了時の返却・削除まで含めて管理します。

対象：2026年度 / 基準日 2026-09-05

0007 個人情報・プライバシー > 個人情報保護法・安全管理措置 ｜ 難易度：標準

個人データを保存したノートPCの紛失が判明した。まず行うべき対応として最も適切なものはどれか。

ア：紛失を隠すため資産台帳から端末を削除する。

イ：暗号化の有無や保存データを確認せず、必ず影響ゼロと判断する。

ウ：事実関係と影響範囲を確認し、被害拡大防止を行い、報告・本人通知の要否を法令・ガイドラインに基づき判断する。

エ：担当者個人で対応し、組織の報告ルートへ上げない。

答え・解説 正答：ウ

ア：事故を隠しても法的・事業上のリスクは解消せず、適切な対応を妨げます。

イ：影響評価には保存内容や保護措置、アクセス可能性などの確認が必要です。

ウ：漏えい等事案では、内部報告、事実関係調査、被害拡大防止、報告・本人通知等を適切に進めます。

エ：適切な判断や法令対応が遅れるため、定めた報告・エスカレーションが必要です。

総合解説：個人データの漏えい等は、事案の種類や影響により個人情報保護委員会への報告・本人通知が必要となる場合があります。まず正確な事実把握と被害拡大防止が重要です。

対象：2026年度 / 基準日 2026-09-05

0008 個人情報・プライバシー > 個人情報保護法・安全管理措置 ｜ 難易度：標準

人事部の個人データを全社員が閲覧できる共有フォルダに保存している。安全管理上の改善として最も適切なものはどれか。

ア：閲覧ログを取得しているため、全社員が閲覧できても問題ない。

イ：ファイル名を分かりにくくすればアクセス制御は不要である。

ウ：共有フォルダに置く代わりに、全社員へメール添付で配布する。

エ：業務上必要な者だけが閲覧できるようアクセス権を限定し、権限付与・変更・削除を管理する。

答え・解説 正答：エ

ア：ログ取得だけでは不要なアクセスを防げません。

イ：隠蔽によるセキュリティでは適切な権限制御の代替になりません。

ウ：複製範囲が広がり、管理がさらに困難になります。

エ：個人データへのアクセス制御は技術的安全管理措置の重要な要素です。

総合解説：個人データは「必要な人が必要な範囲だけ」アクセスできるようにすることが基本です。アクセス権の定期レビューや退職・異動時の更新も重要です。

対象：2026年度 / 基準日 2026-09-05

0009 個人情報・プライバシー > 個人情報保護法・安全管理措置 ｜ 難易度：応用

小規模事業者が顧客の氏名・連絡先を扱っている。大企業と同一の高価な製品を導入できないため、安全管理義務を果たせないと考えている。この判断への対応として最も適切なものはどれか。

ア：事業規模、取扱う個人データの性質・量、リスク等に応じて必要かつ適切な安全管理措置を設計し、組織・人・物理・技術面で実施する。

イ：高価な製品を導入できなければ、安全管理措置は一切不要になる。

ウ：小規模事業者は個人情報保護法の安全管理規律の対象外である。

エ：対策費を抑えるため、顧客データのバックアップを公開クラウドへ誰でも閲覧可能な状態で置く。

答え・解説 正答：ア

ア：安全管理措置は特定製品の導入義務ではなく、事業者の状況に応じた必要かつ適切な対策を講じることが重要です。

イ：事業規模にかかわらず、個人データの安全管理に必要かつ適切な措置が求められます。

ウ：規模だけを理由に当然に対象外となるわけではありません。

エ：漏えいリスクを高める不適切な運用です。

総合解説：安全管理措置はリスクに応じて合理的に設計します。例えば、権限管理、端末ロック、施錠保管、教育、バックアップ、委託先確認など、費用対効果を考えながら多層化します。

対象：2026年度 / 基準日 2026-09-05

0010 個人情報・プライバシー > 個人情報保護法・安全管理措置 ｜ 難易度：応用

国外のクラウド事業者のサーバで個人データを取り扱うことになった。安全管理上の対応として最も適切なものはどれか。

ア：クラウド事業者が有名企業であれば、保存国や制度を一切確認しなくてよい。

イ：データが取り扱われる外国の個人情報保護制度等を把握し、その環境を踏まえて安全管理措置を講じる。

ウ：データを国外に置いた時点で、日本の個人情報保護法上の安全管理責任は必ず消滅する。

エ：暗号化さえしていれば、契約・アクセス権・ログ・委託先管理は不要である。

答え・解説 正答：イ

ア：事業者名だけで外的環境の確認を省略できるとは限りません。

イ：通則ガイドラインは、外国で個人データを取り扱う場合に、当該外国の制度等の外的環境を把握した上で安全管理措置を講じることを示しています。

ウ：国外処理であっても、個人情報取扱事業者としての義務が直ちに消えるわけではありません。

エ：暗号化は一つの技術的対策であり、他の管理策を不要にするものではありません。

総合解説：海外クラウド利用では、第三者提供に該当するかという論点と、安全管理上の外的環境把握の論点を分けて確認します。契約、保存場所、法制度、アクセス制御などを総合評価します。

対象：2026年度 / 基準日 2026-09-05

0011 個人情報・プライバシー > マイナンバー・GDPR・第三者提供 ｜ 難易度：基礎

マイナンバー制度における「特定個人情報」の説明として、最も適切なものはどれか。

ア：法人番号を含む企業情報は、すべて特定個人情報である。

イ：本人の氏名だけが記載され、個人番号を含まない情報は必ず特定個人情報である。

ウ：個人番号をその内容に含む個人情報である。

エ：個人番号を削除した統計情報は、必ず特定個人情報のままである。

答え・解説 正答：ウ

ア：特定個人情報は個人番号を含む個人情報であり、法人番号とは区別されます。

イ：個人情報にはなり得ますが、個人番号を含まなければ特定個人情報とは限りません。

ウ：特定個人情報は、個人番号を含む個人情報を指し、通常の個人情報より利用・提供等に厳格な制限があります。

エ：個人番号を含むか、個人情報に該当するかなど具体的な状態で判断します。

総合解説：マイナンバーを扱う問題では「個人情報」と「特定個人情報」を区別します。特定個人情報には番号法による利用・提供・収集保管等の追加規律があります。

対象：2026年度 / 基準日 2026-09-05

0012 個人情報・プライバシー > マイナンバー・GDPR・第三者提供 ｜ 難易度：基礎

GDPRにおける個人データ処理の原則として、最も適切なものはどれか。

ア：取得できる個人データは将来使う可能性があれば無制限に収集する。

イ：一度取得した個人データは、当初目的と無関係な用途へ常に自由に転用できる。

ウ：保存期間は長いほど望ましく、不要になっても削除を検討しない。

エ：目的制限やデータ最小化などを踏まえ、目的に必要な範囲で適正に処理する。

答え・解説 正答：エ

ア：データ最小化の原則に反する考え方です。

イ：目的制限や適法性の検討が必要です。

ウ：保存制限の原則に反します。

エ：GDPR第5条は、適法性・公正性・透明性、目的制限、データ最小化、正確性、保存制限、完全性・機密性、説明責任等の原則を定めています。

総合解説：GDPRでは、データを多く持つこと自体が目的ではありません。処理目的と法的根拠を明確にし、必要なデータ・保存期間・アクセス範囲を最小化する考え方が重要です。

対象：2026年度 / 基準日 2026-09-05

0013 個人情報・プライバシー > マイナンバー・GDPR・第三者提供 ｜ 難易度：基礎

個人情報保護法における個人データの第三者提供の原則として、最も適切なものはどれか。

ア：法令上の例外等を除き、あらかじめ本人の同意を得ずに第三者へ提供してはならない。

イ：第三者提供は社外への提供であれば、本人同意の有無にかかわらず常に自由である。

ウ：第三者提供の規律は紙の名簿だけに適用され、電子データには適用されない。

エ：提供先が営利企業でなければ、第三者提供の規律は一切適用されない。

答え・解説 正答：ア

ア：個人データの第三者提供は本人同意が原則で、法令に基づく場合など一定の例外があります。

イ：個人データの第三者提供には原則として本人同意が必要です。

ウ：媒体が紙か電子かだけで規律の有無が決まるわけではありません。

エ：第三者かどうかは営利・非営利だけで決まりません。

総合解説：第三者提供では、本人同意の有無だけでなく、委託・事業承継・共同利用など「第三者に該当しない場合」や、法令上の例外を区別して判断します。

対象：2026年度 / 基準日 2026-09-05

0014 個人情報・プライバシー > マイナンバー・GDPR・第三者提供 ｜ 難易度：標準

企業が給与事務で従業員の個人番号を取得した。マーケティング部門が本人の同意を得れば顧客分析にも利用できると提案した。最も適切な判断はどれか。

ア：本人が同意すれば、個人番号は広告配信や購買分析など任意目的に利用できる。

イ：個人番号の利用は番号法で認められた事務の範囲に制限されるため、本人同意があっても自由にマーケティングへ利用できるわけではない。

ウ：社内利用なら番号法の利用制限は適用されない。

エ：個人番号をハッシュ化すれば、法定事務以外への利用が常に可能になる。

答え・解説 正答：イ

ア：個人番号には利用目的の法定制限があり、本人同意だけで任意利用できるわけではありません。

イ：個人番号は、本人の同意があればどの用途でも使える情報ではなく、法令で定められた利用範囲に従う必要があります。

ウ：社内か社外かにかかわらず、個人番号の利用範囲は番号法に従います。

エ：単なる加工で法定の利用制限を当然に回避できるわけではありません。

総合解説：マイナンバーは一般の個人情報より利用・提供・収集保管が厳格に制限されます。「本人同意があるからよい」とは限らない点が試験上重要です。

対象：2026年度 / 基準日 2026-09-05

0015 個人情報・プライバシー > マイナンバー・GDPR・第三者提供 ｜ 難易度：標準

退職者の個人番号を含む書類について、法定保存期間を経過し、番号を利用する必要もなくなった。対応として最も適切なものはどれか。

ア：将来使うかもしれないので、目的を定めず永久に保存する。

イ：廃棄記録を残す必要はなく、誰でもごみ箱へ捨てればよい。

ウ：個人番号を利用する必要がなくなり、保存義務もないのであれば、復元できない方法で速やかに廃棄・削除する。

エ：退職した本人の同意があれば、広告目的で個人番号を保存し続けてよい。

答え・解説 正答：ウ

ア：必要性のない保管は適切ではありません。

イ：廃棄は安全管理措置に従い、復元防止や取扱状況の確認が必要です。

ウ：特定個人情報は必要なくなった後も無期限に保管するのではなく、保存義務等を確認した上で適切に廃棄・削除します。

エ：本人同意だけで番号法の利用・保管制限を超えられるわけではありません。

総合解説：マイナンバー管理では、取得から利用、保管、廃棄までのライフサイクルを管理します。不要になった個人番号を漫然と残さないことが重要です。

対象：2026年度 / 基準日 2026-09-05

0016 個人情報・プライバシー > マイナンバー・GDPR・第三者提供 ｜ 難易度：標準

企業が給与計算を外部事業者へ委託し、その業務遂行に必要な範囲で従業員の個人データを渡す。個人情報保護法上の考え方として、最も適切なものはどれか。

ア：委託先へ渡す場合は必ず第三者提供であり、委託先監督という概念はない。

イ：委託であれば、利用目的と無関係なデータも自由に渡してよい。

ウ：委託先へ渡した後は、委託元の安全管理責任はすべて消滅する。

エ：利用目的の達成に必要な範囲での委託は、一定の要件の下で「第三者への提供」に該当しないが、委託先の監督は必要である。

答え・解説 正答：エ

ア：委託は法上「第三者に該当しない場合」として扱われることがあります。

イ：委託の目的に必要な範囲で取り扱う必要があります。

ウ：委託元には委託先監督が求められます。

エ：委託は第三者提供の例外的扱いですが、委託元には委託先を必要かつ適切に監督する義務があります。

総合解説：「外部へ渡す＝すべて第三者提供」と単純化しないことが重要です。委託、事業承継、共同利用は法上の取扱いが異なるため、要件を確認します。

対象：2026年度 / 基準日 2026-09-05

0017 個人情報・プライバシー > マイナンバー・GDPR・第三者提供 ｜ 難易度：標準

GDPRにおいて、個人データ処理の目的と手段を決定する主体に最も近い用語はどれか。

ア：controller（管理者）

イ：processor（処理者）は、常に自ら処理目的を自由に決める主体である。

ウ：data subjectは、個人データを保管するクラウド事業者だけを指す。

エ：supervisory authorityは、企業内のシステム管理者を指す。

答え・解説 正答：ア

ア：controllerは個人データ処理の目的と手段を決定する主体です。

イ：processorは原則としてcontrollerの指示に基づいて処理する主体です。

ウ：data subjectは個人データによって識別される本人を指します。

エ：supervisory authorityはGDPRに基づく独立監督機関を指します。

総合解説：GDPR問題ではcontroller、processor、data subjectの役割を区別します。委託契約上の名称だけでなく、実際に誰が目的・手段を決めているかが重要です。

対象：2026年度 / 基準日 2026-09-05

0018 個人情報・プライバシー > マイナンバー・GDPR・第三者提供 ｜ 難易度：標準

EU域内の利用者向けニュースレター登録で、配信に必要なのはメールアドレスだけである。GDPRのデータ最小化の観点から最も適切な設計はどれか。

ア：将来使う可能性だけを理由に、可能な限り多くの属性を必須で収集する。

イ：目的に必要な項目を中心に収集し、不要な生年月日や家族情報等を必須にしない。

ウ：収集項目を増やすほどGDPRへの適合性が高まる。

エ：一度収集したデータは、目的が終了しても永久保存する。

答え・解説 正答：イ

ア：目的との必要性がない過剰収集はデータ最小化に反します。

イ：データ最小化は、処理目的に照らして適切・関連性があり必要な範囲に限定する考え方です。

ウ：GDPRは必要最小限のデータ処理を重視します。

エ：保存制限の原則にも反する可能性があります。

総合解説：GDPRでは「取れるから取る」ではなく「目的に必要だから取る」が原則です。設計段階で項目、アクセス、保存期間を見直すことがプライバシー保護につながります。

対象：2026年度 / 基準日 2026-09-05

0019 個人情報・プライバシー > マイナンバー・GDPR・第三者提供 ｜ 難易度：応用

GDPRの適用を受ける組織で個人データ侵害が発生し、自然人の権利・自由にリスクを生じる可能性がある。監督機関への通知について最も適切な考え方はどれか。

ア：調査が完全に終わるまで何か月でも通知を待ち、期限は存在しない。

イ：どのような侵害でも必ず72時間以内に全データ主体へ同一内容を通知することだけが求められる。

ウ：原則として侵害を認識してから72時間以内に、可能な限り監督機関へ通知し、遅れた場合は理由を示す。

エ：72時間を過ぎたら通知義務は消滅する。

答え・解説 正答：ウ

ア：GDPRには原則72時間という通知期限があります。完全調査終了まで待つことを前提としていません。

イ：監督機関への通知とデータ主体への通知は要件が異なり、リスクの程度などに応じて判断します。

ウ：GDPR第33条は、リスクを生じる可能性がある個人データ侵害について、原則72時間以内の監督機関通知を定めています。

エ：期限を超えた場合でも必要な通知を行い、遅延理由を説明することが求められます。

総合解説：GDPRの侵害対応では、監督機関への通知とデータ主体への連絡を区別します。最初の段階で全情報が揃っていなくても、法的要件と追加情報の提出方法を確認します。

対象：2026年度 / 基準日 2026-09-05

0020 個人情報・プライバシー > マイナンバー・GDPR・第三者提供 ｜ 難易度：応用

日本企業がEU域内の顧客向けサービスを提供し、個人データを日本の外部事業者へ処理委託する。法令確認として最も適切な進め方はどれか。

ア：日本企業なのでGDPRはどのような場合も絶対に適用されない。

イ：GDPRに対応すれば日本の個人情報保護法の確認は不要である。

ウ：委託先が日本国内なら、個人データの国際的な取扱いに関する確認は一切不要である。

エ：日本の個人情報保護法上の委託・第三者提供等の整理に加え、GDPRの適用可能性、controller/processor関係、越境移転等の要件を別々に確認する。

答え・解説 正答：エ

ア：GDPRには域外適用の規定があり、EU域内の個人への商品・サービス提供等で適用される場合があります。

イ：適用される各法令・契約をそれぞれ確認する必要があります。

ウ：サービス提供地域や処理主体、移転経路等により複数の規律が関係し得ます。

エ：複数法域の規律が関係する場合、一方の法令に適合しただけで他方への適合が自動的に保証されるわけではありません。

総合解説：国際的な個人データ取扱いでは、適用法令、処理主体、委託関係、移転先、契約・安全管理を整理します。「国内企業だから国内法だけ」と決めつけないことが重要です。

対象：2026年度 / 基準日 2026-09-05

0021 個人情報・プライバシー > 匿名加工・仮名加工・PIA・プライバシー保護 ｜ 難易度：基礎

仮名加工情報と匿名加工情報の違いに関する説明として、最も適切なものはどれか。

ア：仮名加工情報は、他の情報と照合しない限り特定個人を識別できないよう加工した情報であり、匿名加工情報は特定個人を識別できず、かつ元の個人情報を復元できないよう加工した情報である。

イ：仮名加工情報と匿名加工情報は法律上まったく同じ定義である。

ウ：仮名加工情報は必ず第三者へ自由に提供できるが、匿名加工情報は提供できない。

エ：匿名加工情報は、加工後も本人を容易に識別できることを前提とする。

答え・解説 正答：ア

ア：両者は加工水準と法的取扱いが異なります。仮名加工情報は内部分析等での利活用を想定し、匿名加工情報はより強い匿名化を前提とします。

イ：両者は定義・義務・利用場面が異なります。

ウ：仮名加工情報には原則として第三者提供の制限があり、匿名加工情報には一定の公表・表示等の義務の下で第三者提供の仕組みがあります。

エ：匿名加工情報は特定の個人を識別できず、元の個人情報を復元できないようにすることが要件です。

総合解説：「仮名」と「匿名」は名称が似ていますが、法的な加工要件と利用ルールが異なります。試験では、本人識別可能性、第三者提供、識別行為の禁止などを区別して理解することが重要です。

対象：2026年度 / 基準日 2026-09-05

0022 個人情報・プライバシー > 匿名加工・仮名加工・PIA・プライバシー保護 ｜ 難易度：基礎

匿名加工情報を作成・提供する場合の取扱いとして、最も適切なものはどれか。

ア：氏名だけ削除すれば必ず匿名加工情報となり、追加の加工は不要である。

イ：所定の加工基準や安全管理措置を守り、第三者提供時には含まれる情報項目や提供方法を公表するなど、法令上の義務に従う。

ウ：匿名加工情報は作成者が自由に元の本人を再識別してよい。

エ：匿名加工情報は第三者へ提供する場合でも、提供する情報項目や提供方法の公表は一切不要である。

答え・解説 正答：イ

ア：氏名削除だけで再識別可能性を十分に下げられるとは限らず、所定の加工基準を満たす必要があります。

イ：匿名加工情報には、加工方法、安全管理、第三者提供時の公表・明示、識別行為の禁止等の規律があります。

ウ：匿名加工情報を取り扱う者には、本人を識別する目的で他情報と照合すること等が禁止されています。

エ：第三者提供時には所定の公表等が必要です。

総合解説：匿名加工情報は「個人名を消しただけ」のデータではありません。再識別や復元を防ぐための加工と、取扱い上の義務を一体として理解します。

対象：2026年度 / 基準日 2026-09-05

0023 個人情報・プライバシー > 匿名加工・仮名加工・PIA・プライバシー保護 ｜ 難易度：基礎

PIA（Privacy Impact Assessment）の目的として、最も適切なものはどれか。

ア：インシデント発生後に損害額だけを算出する会計手続である。

イ：システムの処理速度だけを測定する性能試験である。

ウ：新たなシステムやサービス等がプライバシーへ及ぼす影響・リスクを事前に評価し、必要な低減策を設計へ反映する。

エ：個人情報を大量に収集するためのマーケティング手法である。

答え・解説 正答：ウ

ア：PIAは主として事前のプライバシーリスク評価です。

イ：性能試験とは目的が異なります。

ウ：PIAは、個人情報等の取扱いによるプライバシー上のリスクを事前に評価し、回避・低減するための取組です。

エ：PIAは収集拡大ではなく、プライバシー影響を評価し低減するために行います。

総合解説：PIAは設計・企画の早い段階で実施するほど、データ最小化やアクセス制御、保存期間などを組み込みやすくなります。

対象：2026年度 / 基準日 2026-09-05

0024 個人情報・プライバシー > 匿名加工・仮名加工・PIA・プライバシー保護 ｜ 難易度：標準

顧客行動を社内で統計分析するため、氏名等を削除し、別管理の対応表がないと本人を識別できない状態に加工した。仮名加工情報の取扱いとして最も適切なものはどれか。

ア：仮名加工した時点で、利用目的や安全管理の検討は一切不要になる。

イ：対応表が別に存在するなら、分析担当者が本人を突き止めるため自由に照合してよい。

ウ：仮名加工情報は必ずインターネット上で公開しなければならない。

エ：法令上の仮名加工情報に該当するかを確認し、本人を識別する目的で他情報と照合しないなど、仮名加工情報に関する規律に従って利用する。

答え・解説 正答：エ

ア：仮名加工情報にも法令上の取扱義務が残ります。

イ：本人識別を目的とする照合は制限されます。

ウ：公開義務はなく、むしろ内部利用を想定する場面が多い仕組みです。

エ：仮名加工情報は内部分析等の利活用を促進する仕組みですが、識別行為の禁止や安全管理などの義務があります。

総合解説：仮名加工情報は個人データの安全な利活用を広げる制度ですが、「仮名化したから何でも自由」ではありません。加工後の用途と識別禁止などの義務を確認します。

対象：2026年度 / 基準日 2026-09-05

0025 個人情報・プライバシー > 匿名加工・仮名加工・PIA・プライバシー保護 ｜ 難易度：標準

購買履歴から氏名だけを削除したが、会員番号・詳細な購入日時・店舗情報を組み合わせれば容易に本人を特定できる可能性が高い。最も適切な判断はどれか。

ア：氏名削除だけで匿名加工情報になるとは限らず、特定個人を識別できず元情報を復元できないよう、必要な加工を行う必要がある。

イ：氏名を削除すれば、残りの項目に関係なく必ず匿名加工情報になる。

ウ：会員番号が残っていても、本人を特定できる可能性は評価しなくてよい。

エ：匿名加工情報を作る場合は元データを一切変更してはならない。

答え・解説 正答：ア

ア：匿名加工情報は、単純な氏名削除ではなく、識別・復元を防ぐための加工基準を満たす必要があります。

イ：組合せによる識別可能性などを考慮する必要があります。

ウ：識別につながる識別子等は加工対象として検討が必要です。

エ：匿名加工情報は所定の加工を行って作成します。

総合解説：匿名加工はラベル変更ではなく、再識別リスクを下げる加工です。どの項目を削除・置換・一般化するかを、データの組合せも含めて判断します。

対象：2026年度 / 基準日 2026-09-05

0026 個人情報・プライバシー > 匿名加工・仮名加工・PIA・プライバシー保護 ｜ 難易度：標準

匿名加工情報を外部の研究機関へ提供することになった。提供者の対応として最も適切なものはどれか。

ア：匿名加工情報なので、提供に際して一切の手続や表示は不要である。

イ：法令で定める方法により、匿名加工情報に含まれる個人に関する情報の項目と提供方法をあらかじめ公表し、提供先に匿名加工情報である旨を明示する。

ウ：提供先に元の本人を識別するよう依頼しなければならない。

エ：匿名加工情報は法律上、第三者へ一切提供できない。

答え・解説 正答：イ

ア：匿名加工情報にも第三者提供時の義務があります。

イ：匿名加工情報の第三者提供には、公表・明示に関する義務があります。

ウ：本人識別を目的とする照合等は禁じられています。

エ：一定の義務を履行した上で第三者提供する仕組みがあります。

総合解説：匿名加工情報は利活用を可能にする一方、透明性と再識別防止を確保するためのルールが設けられています。

対象：2026年度 / 基準日 2026-09-05

0027 個人情報・プライバシー > 匿名加工・仮名加工・PIA・プライバシー保護 ｜ 難易度：標準

位置情報を常時取得する新機能を開発している。PIAの進め方として最も適切なものはどれか。

ア：サービス公開後に問題が起きるまでPIAは実施しない。

イ：位置情報を扱う場合でも、プライバシーへの影響は評価不要である。

ウ：本番稼働前の設計段階から、取得項目・利用目的・保存期間・第三者提供・安全管理等を評価し、必要な対策を設計へ反映する。

エ：PIAではセキュリティ対策だけを見ればよく、利用目的や保存期間は検討しない。

答え・解説 正答：ウ

ア：事前評価というPIAの目的に反します。

イ：位置情報は行動把握につながり得るため、目的・必要性・リスクを慎重に評価します。

ウ：PIAは事後説明だけでなく、設計段階でプライバシーリスクを評価し、対策を組み込むことに価値があります。

エ：PIAはプライバシー全体の影響を評価し、データ最小化や透明性なども含めて検討します。

総合解説：PIAはPrivacy by Designと相性がよく、仕様が固まる前に行うほど改善余地が大きくなります。

対象：2026年度 / 基準日 2026-09-05

0028 個人情報・プライバシー > 匿名加工・仮名加工・PIA・プライバシー保護 ｜ 難易度：標準

健康管理アプリが歩数表示だけを提供する機能について、氏名、住所、勤務先、家族構成、詳細な位置履歴をすべて必須入力にしようとしている。プライバシー保護の観点で最も適切な対応はどれか。

ア：取得できるデータは将来利用する可能性があるため、可能な限り必須化する。

イ：同意文を長くすれば、不要なデータを無制限に集めても問題ない。

ウ：取得後のアクセス制御を強化すれば、収集項目の必要性は考えなくてよい。

エ：機能の目的達成に本当に必要なデータを精査し、不要な項目は取得しない又は任意化する。

答え・解説 正答：エ

ア：目的との必要性がない過剰収集はプライバシーリスクを高めます。

イ：同意の有無だけでなく、目的・必要性・透明性等を検討する必要があります。

ウ：安全管理とデータ最小化は別の対策で、両方が重要です。

エ：データ最小化は、必要な情報だけを取得することでプライバシーリスクを低減します。

総合解説：プライバシー保護は「集めた後に守る」だけでなく、「そもそも必要以上に集めない」ことが重要です。

対象：2026年度 / 基準日 2026-09-05

0029 個人情報・プライバシー > 匿名加工・仮名加工・PIA・プライバシー保護 ｜ 難易度：応用

小売企業が、店内カメラ映像と会員IDを組み合わせて来店者の行動を分析する新サービスを企画した。プライバシーリスク管理として最も適切なものはどれか。

ア：導入前にPIAを実施し、目的の必要性、データ項目、識別可能性、保存期間、アクセス権、本人への説明、代替手段等を評価してリスク低減策を決める。

イ：技術的に実現可能なら、プライバシー影響を確認せずすぐ本番導入する。

ウ：会員規約に「データを利用する」と一文書けば、収集範囲や保存期間は評価不要である。

エ：映像を取得した後で問題が起きた場合だけアクセス権を検討する。

答え・解説 正答：ア

ア：複数データの結合や行動追跡はプライバシー影響が大きくなり得るため、事前評価と設計改善が有効です。

イ：技術可能性と法令・プライバシー適切性は別問題です。

ウ：透明性だけでなく必要性・比例性・安全管理等の評価が必要です。

エ：アクセス権や保護策は事前に設計へ組み込むべきです。

総合解説：高リスクなデータ活用では、法令適合だけでなく利用者の期待、識別・追跡の程度、漏えい時影響も含めてPIAで評価します。

対象：2026年度 / 基準日 2026-09-05

0030 個人情報・プライバシー > 匿名加工・仮名加工・PIA・プライバシー保護 ｜ 難易度：応用

研究部門で仮名加工した顧客データを分析する。仮名IDと実名を対応付ける情報を同じ共有フォルダに置き、研究者全員が閲覧できる状態になっている。最も適切な改善はどれか。

ア：仮名加工情報という名称を付ければ、対応表の管理方法は問われない。

イ：対応付けに必要な情報を分析データから分離し、アクセス権を必要最小限に制限するなど、識別リスクを低減する。

ウ：研究者が便利に使えるよう、実名対応表を全員へ配布する。

エ：再識別可能な状態でも、外部へ公開しなければ安全管理は不要である。

答え・解説 正答：イ

ア：名称ではなく実際の加工と管理が重要です。

イ：仮名加工情報を活用する場合も、容易な再識別を招かない管理が必要です。

ウ：本人識別につながる情報の広範な共有はリスクを高めます。

エ：内部利用でも必要な安全管理・識別防止が求められます。

総合解説：仮名化の効果を得るには、識別子や対応表を分離し、アクセス可能者を限定することが重要です。加工と運用をセットで設計します。

対象：2026年度 / 基準日 2026-09-05

0031 セキュリティ関連法規 > サイバーセキュリティ基本法・不正アクセス禁止法 ｜ 難易度：基礎

サイバーセキュリティ基本法の説明として、最も適切なものはどれか。

ア：不正アクセスを行った個人の具体的な構成要件と刑罰だけを定める刑事特別法である。

イ：電子署名の技術方式だけを定める法律である。

ウ：サイバーセキュリティに関する基本理念や国等の責務、施策の基本的事項などを定める基本法である。

エ：著作物の複製権だけを定める法律である。

答え・解説 正答：ウ

ア：不正アクセスの禁止・罰則は主に不正アクセス禁止法等で扱われ、基本法の役割とは異なります。

イ：電子署名に関する法律とは別です。

ウ：サイバーセキュリティ基本法は、国全体のサイバーセキュリティ政策の基本的枠組みを定めます。

エ：著作権法とは目的が異なります。

総合解説：「基本法」は政策の理念・責務・推進体制を定める性格が中心です。具体的な禁止行為や罰則を定める個別法と区別します。

対象：2026年度 / 基準日 2026-09-05

0032 セキュリティ関連法規 > サイバーセキュリティ基本法・不正アクセス禁止法 ｜ 難易度：基礎

不正アクセス禁止法が禁止する「不正アクセス行為」に最も近いものはどれか。

ア：自分の正規アカウントで許可された画面を閲覧する行為。

イ：インターネットに公開された企業の公式Webページを閲覧するだけの行為。

ウ：自分のPCでオフライン文書を編集する行為。

エ：アクセス制御機能を有する特定電子計算機に対し、他人の識別符号を無断で入力するなどして、本来制限されている利用を可能にする行為。

答え・解説 正答：エ

ア：適法に付与された権限内の利用は、不正アクセス行為とは通常異なります。

イ：公開情報の通常閲覧は不正アクセスとは異なります。

ウ：アクセス制御された他者システムへの不正な侵入とは無関係です。

エ：不正アクセス禁止法は、他人の識別符号の無断入力等によりアクセス制御を回避して利用する行為などを禁止しています。

総合解説：試験では「アクセス制御を回避して利用する行為」と「公開情報の閲覧」「正規権限内利用」を区別します。

対象：2026年度 / 基準日 2026-09-05

0033 セキュリティ関連法規 > サイバーセキュリティ基本法・不正アクセス禁止法 ｜ 難易度：基礎

不正アクセス禁止法に関する説明として、最も適切なものはどれか。

ア：不正アクセス行為だけでなく、不正アクセスに用いる目的で他人の識別符号を取得・保管したり、一定の場合に第三者へ提供したりする行為も規制対象となる。

イ：実際に不正ログインが成功しない限り、他人のID・パスワードに関する行為は一切規制されない。

ウ：パスワードをだまし取るための偽ログイン画面を公開する行為は、法律上まったく問題にならない。

エ：アクセス管理者には識別符号の適切な管理を行う必要はない。

答え・解説 正答：ア

ア：同法は侵入行為だけでなく、識別符号の不正取得・助長・保管や不正な入力要求なども規制しています。

イ：不正アクセスの準備・助長に関わる一定の識別符号関連行為も規制対象です。

ウ：識別符号の不正な入力要求も規制対象となり得ます。

エ：アクセス管理者には不正アクセス防御に関する措置を講ずる努力義務等があります。

総合解説：不正アクセス禁止法は、侵入そのものだけでなく、認証情報を不正に集める・提供する・保管するといった周辺行為も対象にしています。

対象：2026年度 / 基準日 2026-09-05

0034 セキュリティ関連法規 > サイバーセキュリティ基本法・不正アクセス禁止法 ｜ 難易度：標準

退職した同僚のIDとパスワードがまだ有効だったため、上司の許可なくその情報で社内システムへログインした。最も適切な判断はどれか。

ア：パスワードが有効なまま残っていたので、誰が使っても合法である。

イ：他人の識別符号を無断で用いてアクセス制御を突破しているため、不正アクセス行為に該当し得る。

ウ：社内システムであれば不正アクセス禁止法は関係しない。

エ：閲覧だけでデータを変更していないなら、他人のID利用は常に問題ない。

答え・解説 正答：イ

ア：認証情報が技術的に有効でも、利用権限があるとは限りません。

イ：識別符号の有効・無効ではなく、正当な権限なく他人の識別符号を用いてアクセスする点が問題になります。

ウ：要件を満たすアクセス制御機能を有するシステムであれば、社内外だけで単純に区別できません。

エ：不正アクセス行為はデータ改ざんの有無だけで決まりません。

総合解説：認証情報の有効性と利用権限は別です。退職者アカウントを速やかに無効化する運用対策も重要です。

対象：2026年度 / 基準日 2026-09-05

0035 セキュリティ関連法規 > サイバーセキュリティ基本法・不正アクセス禁止法 ｜ 難易度：標準

企業が外部業者へWebシステムの脆弱性診断を依頼した。診断行為を適法・適切に行うための対応として最も適切なものはどれか。

ア：診断契約が一つあれば、同社が所有する全システムへ無制限に侵入してよい。

イ：インターネットから到達できるシステムは、誰でも自由に侵入試験してよい。

ウ：対象システム、期間、試験手法、許可される行為、連絡方法等を事前に合意し、明確な権限の範囲内で実施する。

エ：診断では認証情報や個人データが見えても、報告や保護は一切不要である。

答え・解説 正答：ウ

ア：許可範囲は対象・方法・期間等で限定されるため、範囲外実施は不適切です。

イ：公開されていることと侵入試験の許可は別です。

ウ：脆弱性診断は正当な権限の下で実施することが重要です。範囲外への侵入は別の法的問題を生じ得ます。

エ：診断中に取得した情報の取扱いも契約・安全管理上の重要事項です。

総合解説：セキュリティ診断では「善意」だけでは足りず、権限・スコープ・実施条件を明確にします。

対象：2026年度 / 基準日 2026-09-05

0036 セキュリティ関連法規 > サイバーセキュリティ基本法・不正アクセス禁止法 ｜ 難易度：標準

銀行を装った偽サイトを作り、利用者にID・パスワードを入力するよう求めた。最も適切な説明はどれか。

ア：まだ実際にログインしていないので、偽サイトで認証情報を求めても法的問題はない。

イ：メールではなくWebサイトを使えば規制されない。

ウ：取得したID・パスワードを第三者へ売却しても、実際に使われなければ常に合法である。

エ：不正アクセスに用いる目的で識別符号の入力を要求する行為として、不正アクセス禁止法上の規制対象となり得る。

答え・解説 正答：エ

ア：識別符号の不正な入力要求自体が規制対象となり得ます。

イ：媒体だけで規制を免れるものではありません。

ウ：識別符号の不正取得・提供等にも規制があります。

エ：不正アクセス禁止法は、アクセス管理者になりすますなどして識別符号を不正に入力させる行為も規制します。

総合解説：不正アクセス対策では、侵入後だけでなく認証情報を盗むフィッシング段階から法的リスクがあります。

対象：2026年度 / 基準日 2026-09-05

0037 セキュリティ関連法規 > サイバーセキュリティ基本法・不正アクセス禁止法 ｜ 難易度：標準

アクセス管理者が不正アクセスを防ぐために行う対応として、最も適切なものはどれか。

ア：識別符号を適切に管理し、アクセス制御機能の有効性を検証し、必要に応じて機能の高度化その他の措置を講じる。

イ：全利用者に同じ共有パスワードを永久に使わせる。

ウ：脆弱性情報が公表されてもアクセス制御を一切見直さない。

エ：退職者のIDを削除せず、誰でも引継ぎに使えるようにする。

答え・解説 正答：ア

ア：不正アクセス禁止法はアクセス管理者に対して、防御措置を講ずる努力を求めています。

イ：共有パスワードは追跡性や認証強度を低下させ、不正アクセス防止上不適切です。

ウ：防御機能の有効性を継続的に評価・改善することが重要です。

エ：不要アカウントの残存は不正アクセスの機会を増やします。

総合解説：法律上の努力義務に加えて、実務ではMFA、権限レビュー、ログ監視、パッチ適用など複数の対策を組み合わせます。

対象：2026年度 / 基準日 2026-09-05

0038 セキュリティ関連法規 > サイバーセキュリティ基本法・不正アクセス禁止法 ｜ 難易度：標準

企業Webサイト上で誰でも閲覧できる公開資料を、通常のブラウザ操作で閲覧した。最も適切な説明はどれか。

ア：企業が運営するサイトを閲覧しただけで、必ず不正アクセスになる。

イ：アクセス制御を回避していない通常の公開情報閲覧であり、それだけで不正アクセス行為とは通常いえない。

ウ：公開資料を見つけた後、その同じURLの末尾を変更してアクセス制御された管理画面へ侵入しても同じ扱いである。

エ：検索エンジンで表示された情報は、認証回避をしても常に自由に利用できる。

答え・解説 正答：イ

ア：通常の公開ページ閲覧は不正アクセスとは異なります。

イ：不正アクセス禁止法の中心は、アクセス制御を不正に回避して利用する行為です。

ウ：アクセス制御を回避する行為は別途評価が必要です。

エ：検索結果への表示とアクセス権限は別です。

総合解説：不正アクセス該当性は「公開されていたか」だけでなく、アクセス制御の有無と回避行為、権限の有無などを確認します。

対象：2026年度 / 基準日 2026-09-05

0039 セキュリティ関連法規 > サイバーセキュリティ基本法・不正アクセス禁止法 ｜ 難易度：応用

退職者Aのアカウントが削除されず残っていた。Aは退職後、そのIDで顧客管理システムへログインし名簿を閲覧した。会社側の再発防止として最も適切なものはどれか。

ア：退職者がログインできたのは会社の設定ミスなので、Aの行為に法的問題は絶対に生じない。

イ：Aを処分すれば、退職者アカウントを残す運用は変更しなくてよい。

ウ：Aの行為について不正アクセス等の法的問題を検討するとともに、会社は退職時のアカウント無効化、権限棚卸し、ログ監視を徹底する。

エ：ログを削除すれば事故はなかったことになる。

答え・解説 正答：ウ

ア：設定不備があっても、正当な権限のないアクセス行為の評価は別問題です。

イ：再発防止にはアカウントライフサイクル管理の改善が必要です。

ウ：利用者の不正行為と、アクセス管理者側の予防措置は別々に評価し、双方へ対応する必要があります。

エ：証拠や監査記録を消すことは適切な対応ではありません。

総合解説：法務問題でも技術・運用を分離せず、禁止行為と管理者側の防御措置を合わせて考えるのが実務的です。

対象：2026年度 / 基準日 2026-09-05

0040 セキュリティ関連法規 > サイバーセキュリティ基本法・不正アクセス禁止法 ｜ 難易度：応用

外部業者が「example.jp配下のテスト用Webサーバ1台」だけを対象として侵入試験の許可を得たが、追加承認なく同社の本番メールサーバへも侵入を試みた。最も適切な対応はどれか。

ア：同じ会社のサーバなので、どこまで侵入しても最初の許可で当然に認められる。

イ：技術力の確認になるため、事前承認なしの範囲拡大が望ましい。

ウ：結果を報告すれば、許可範囲外へのアクセスは常に正当化される。

エ：許可範囲を逸脱しているため直ちに試験を停止し、契約・法的観点を含めて事実関係を確認する。

答え・解説 正答：エ

ア：テスト対象・範囲は契約や承認で限定されます。

イ：無断の範囲拡大は法的・運用上の重大リスクです。

ウ：事後報告だけで事前の権限欠如が解消されるとは限りません。

エ：正当なセキュリティ試験は明示された許可範囲で実施する必要があります。

総合解説：脆弱性診断やペネトレーションテストでは、対象IP・ドメイン、時間帯、禁止手法、データ取扱い、緊急連絡先などを明確化します。

対象：2026年度 / 基準日 2026-09-05

0041 セキュリティ関連法規 > 刑法上のサイバー犯罪・電子署名法 ｜ 難易度：基礎

刑法上の不正指令電磁的記録に関する罪が主に対象とするものとして、最も適切なものはどれか。

ア：正当な理由なく、人が電子計算機を使用する際の意図に反する動作をさせるべき不正な指令を与える電磁的記録を作成・提供等する行為。

イ：すべてのソフトウェアの作成行為を禁止するもの。

ウ：OSの正規アップデートを配布する行為を一律に禁止するもの。

エ：公開Webページを閲覧する行為を処罰するもの。

答え・解説 正答：ア

ア：いわゆるコンピュータ・ウイルス等に関する犯罪類型であり、不正な指令を与える電磁的記録の作成・供用等を一定の要件で処罰します。

イ：通常のソフトウェア開発を禁止する規定ではありません。

ウ：正規更新は通常、利用者の意図に反する不正な指令を与えるものではありません。

エ：閲覧行為そのものを対象とする規定ではありません。

総合解説：刑法上のサイバー犯罪は、単に「コンピュータを使った」というだけで成立するものではなく、各犯罪類型の構成要件を確認します。

対象：2026年度 / 基準日 2026-09-05

0042 セキュリティ関連法規 > 刑法上のサイバー犯罪・電子署名法 ｜ 難易度：基礎

電子署名法に関する説明として、最も適切なものはどれか。

ア：電子署名があれば文書内容が必ず事実として正しいことを国が保証する。

イ：一定の要件を満たす本人による電子署名が行われた電磁的記録について、真正に成立したものと推定する規定などを設けている。

ウ：電子署名を行うと、文書の秘密性が自動的に確保される。

エ：電子契約は必ず紙に印刷して押印しなければ効力を持たないと定める。

答え・解説 正答：イ

ア：電子署名は作成者・改ざん検知等に関係しますが、記載内容の真実性そのものを保証する制度ではありません。

イ：電子署名法は、電子取引等の円滑化に向け、電子署名の法的効果や認証業務の制度を定めています。

ウ：電子署名と暗号化による機密性確保は目的が異なります。

エ：電子署名法は電子的な取引を支える法制度であり、そのような一律の紙・押印義務を定めるものではありません。

総合解説：電子署名では「誰が作成したか」と「署名後に改ざんされていないか」を技術的に確認する考え方と、その法的効果を区別して理解します。

対象：2026年度 / 基準日 2026-09-05

0043 セキュリティ関連法規 > 刑法上のサイバー犯罪・電子署名法 ｜ 難易度：基礎

電子署名で用いられる電子証明書の役割として、最も適切なものはどれか。

ア：署名対象文書の内容が社会的に正しいことを保証する。

イ：文書を必ず暗号化して第三者から読めなくする。

ウ：公開鍵とその利用者との結び付きを確認できるようにし、署名検証時の本人性確認を支援する。

エ：秘密鍵をインターネット上で誰でも取得できるよう公開する。

答え・解説 正答：ウ

ア：証明書は文書内容の真実性を保証するものではありません。

イ：署名と暗号化は別機能です。

ウ：電子証明書は公開鍵と主体の対応関係を証明し、PKIにおける署名検証等を支えます。

エ：秘密鍵は署名者が厳重に管理すべき情報です。

総合解説：認証局・電子証明書・公開鍵・秘密鍵の関係は、技術と法務の両方で頻出です。証明書が保証する範囲を過大評価しないことが重要です。

対象：2026年度 / 基準日 2026-09-05

0044 セキュリティ関連法規 > 刑法上のサイバー犯罪・電子署名法 ｜ 難易度：標準

セキュリティ研究者が隔離された検証環境で、マルウェアの挙動を分析するため検体を保有している。最も適切な考え方はどれか。

ア：マルウェアを保有しただけで、目的や事情に関係なく必ず犯罪が成立する。

イ：研究目的と名乗れば、第三者へ無断で感染させても常に合法である。

ウ：隔離環境での検証では安全管理や権限制御は不要である。

エ：不正指令電磁的記録に関する罪は目的や正当な理由等の要件を含むため、研究目的の適法性は具体的事情に基づいて判断する必要がある。

答え・解説 正答：エ

ア：犯罪成立には条文上の要件があり、単純な所持だけで一律には判断できません。

イ：正当な研究目的でも、他者システムへ無断で被害を与える行為は正当化されません。

ウ：検体の流出や誤実行を防ぐため、隔離・権限制御等が重要です。

エ：同じプログラムを扱っていても、保有・作成の目的、正当な理由、利用態様などによって法的評価が異なり得ます。

総合解説：法務問題では、用語だけでなく「正当な理由」「目的」「他者への影響」など具体的要件を確認する必要があります。

対象：2026年度 / 基準日 2026-09-05

0045 セキュリティ関連法規 > 刑法上のサイバー犯罪・電子署名法 ｜ 難易度：標準

取引先から「電子署名したPDFなら第三者には内容を読まれない」と説明された。最も適切な指摘はどれか。

ア：電子署名は主に署名者確認や改ざん検知に用いられ、内容の機密性を確保するには別途暗号化等が必要である。

イ：電子署名を付けると、必ず文書全体が暗号化される。

ウ：暗号化と電子署名は完全に同じ処理なので区別する必要はない。

エ：電子署名は改ざん検知には一切利用できない。

答え・解説 正答：ア

ア：電子署名と暗号化は異なるセキュリティ機能を提供します。

イ：署名だけで機密性が自動的に確保されるわけではありません。

ウ：目的・鍵の使い方・効果が異なります。

エ：適切に検証すれば、署名後の改ざん検知に役立ちます。

総合解説：CIAの観点では、電子署名は真正性・完全性等、暗号化は主に機密性に関係します。目的に応じて組み合わせます。

対象：2026年度 / 基準日 2026-09-05

0046 セキュリティ関連法規 > 刑法上のサイバー犯罪・電子署名法 ｜ 難易度：標準

電子署名に使う秘密鍵が漏えいした疑いがある。最も適切な対応はどれか。

ア：秘密鍵が漏えいしても、公開鍵が変わらなければ問題ない。

イ：該当する証明書の失効手続等を行い、新しい鍵・証明書へ切り替え、影響した署名の扱いを確認する。

ウ：証明書の有効期限まで何もせず使い続ける。

エ：秘密鍵を社内全員へ配布して本人確認を簡単にする。

答え・解説 正答：イ

ア：秘密鍵漏えいは署名者になりすまされる重大なリスクです。

イ：秘密鍵漏えい時は、第三者によるなりすまし署名の可能性があるため証明書失効等が重要です。

ウ：漏えい疑いがある場合は速やかな失効等が必要です。

エ：秘密鍵は署名者のみが管理すべきで、共有すると本人性が失われます。

総合解説：電子署名の信頼性は秘密鍵管理に依存します。証明書の有効期限だけでなく、失効情報を確認する運用も重要です。

対象：2026年度 / 基準日 2026-09-05

0047 セキュリティ関連法規 > 刑法上のサイバー犯罪・電子署名法 ｜ 難易度：標準

他人の決済アカウントを不正に操作し、虚偽の情報をシステムへ与えて財産上の利益を得る行為を検討している。最も適切な考え方はどれか。

ア：コンピュータを使った犯罪はすべて不正アクセス禁止法だけで処理され、刑法は適用されない。

イ：金銭的利益を得ても、画面上の操作だけなら刑法上の問題にはならない。

ウ：不正アクセス禁止法だけでなく、行為態様によっては刑法上の電子計算機使用詐欺など複数の犯罪類型を検討する必要がある。

エ：ID・パスワードが正しければ、利用権限の有無にかかわらずすべて適法である。

答え・解説 正答：ウ

ア：刑法にも電子計算機を利用した犯罪類型があります。

イ：電子的な操作でも財産犯罪等の対象になり得ます。

ウ：一つのサイバー行為が複数の法令・犯罪類型に関係することがあります。構成要件ごとに整理します。

エ：認証情報が正しいことと、正当な利用権限があることは別です。

総合解説：サイバー犯罪では、不正アクセス、詐欺、業務妨害、マルウェア等の論点が重なることがあります。事実関係を分解して検討します。

対象：2026年度 / 基準日 2026-09-05

0048 セキュリティ関連法規 > 刑法上のサイバー犯罪・電子署名法 ｜ 難易度：標準

電子署名付き契約書の署名検証が正常であった。そこから直接確認できる事項として最も適切なものはどれか。

ア：契約内容が法的・経済的に必ず妥当であると保証される。

イ：契約相手が履行能力を持つことが保証される。

ウ：署名対象文書が一度も第三者に閲覧されていないことが保証される。

エ：使用した証明書等が適切であることを前提に、署名者との結び付きと署名後に文書が改変されていないことを確認する手掛かりになる。

答え・解説 正答：エ

ア：署名検証は契約内容の妥当性までは保証しません。

イ：信用力や履行能力は別途確認が必要です。

ウ：署名は機密性や閲覧履歴を保証するものではありません。

エ：電子署名検証は署名者と文書の完全性を確認するための重要な手段です。

総合解説：電子署名の「保証範囲」を正確に理解することが重要です。真正性・完全性に関する確認と、内容の正当性・機密性は別問題です。

対象：2026年度 / 基準日 2026-09-05

0049 セキュリティ関連法規 > 刑法上のサイバー犯罪・電子署名法 ｜ 難易度：応用

電子署名済みの契約PDFを受領後、第三者が金額欄を書き換えた。署名検証で異常が表示された場合の説明として最も適切なものはどれか。

ア：署名対象データが署名後に変更された可能性があり、改ざんされた文書を正当な署名済み原本として扱うべきではない。

イ：署名者の秘密鍵が変わっていない限り、文書改ざんは検知できない。

ウ：金額欄だけなら署名検証には影響しない。

エ：電子署名が付いている文書は技術的に一切編集できない。

答え・解説 正答：ア

ア：電子署名は署名対象データの完全性確認に利用でき、署名後の変更を検知する手掛かりになります。

イ：署名検証では署名対象データの変更も検出できます。

ウ：署名対象範囲に含まれる変更であれば検証結果に影響します。

エ：編集自体が物理的に不可能になるわけではなく、変更を検知できることが重要です。

総合解説：署名は「編集不能化」ではなく、「署名後に変更されたかを検証できる」仕組みと理解します。

対象：2026年度 / 基準日 2026-09-05

0050 セキュリティ関連法規 > 刑法上のサイバー犯罪・電子署名法 ｜ 難易度：応用

社内教育担当者が、実物のランサムウェア検体を一般社員へメール添付し、各自のPCで実行して学習させようとしている。最も適切な対応はどれか。

ア：教育目的と記載すれば、社員PCへ実物マルウェアを配布しても常に安全かつ適法である。

イ：実害や拡散の危険が高いため実施せず、必要な教育は無害化した教材や隔離検証環境で行い、マルウェアの作成・提供等に関する法的要件も確認する。

ウ：社内メールならマルウェアは感染しないため問題ない。

エ：検体を配布した後にバックアップを取れば十分である。

答え・解説 正答：イ

ア：目的だけで実害・法的リスクが消えるわけではありません。

イ：教育目的でも実環境へ危険な検体を配布することは重大なリスクです。目的だけで危険行為が当然に正当化されるわけではありません。

ウ：社内でも実行・拡散・暗号化等の被害は発生し得ます。

エ：被害を前提とするのではなく、安全な教育方法を採用すべきです。

総合解説：サイバー教育は安全なシミュレーションで行うのが基本です。法的要件と運用上の安全性を両方確認します。

対象：2026年度 / 基準日 2026-09-05

0051 セキュリティ関連法規 > 情報流通プラットフォーム対処法・特定電子メール法 ｜ 難易度：基礎

情報流通プラットフォーム対処法の主な内容として、最も適切なものはどれか。

ア：広告メールの送信だけを全面的に禁止する法律である。

イ：個人番号の利用範囲だけを定める法律である。

ウ：特定電気通信による情報流通で権利侵害が生じた場合の役務提供者の損害賠償責任の制限や発信者情報開示、大規模プラットフォーム事業者の対応義務等を定める。

エ：著作権の保護期間だけを定める法律である。

答え・解説 正答：ウ

ア：広告メールは主に特定電子メール法の対象です。

イ：マイナンバー法制とは別です。

ウ：旧プロバイダ責任制限法が改正・改題され、大規模プラットフォーム事業者に関する削除対応の迅速化・透明化等も規定されています。

エ：著作権法とは異なります。

総合解説：IPAシラバスVer.4.1では旧称のプロバイダ責任制限法から情報流通プラットフォーム対処法へ更新されています。旧名称だけで覚えないことが重要です。

対象：2026年度 / 基準日 2026-09-05

0052 セキュリティ関連法規 > 情報流通プラットフォーム対処法・特定電子メール法 ｜ 難易度：基礎

情報流通プラットフォーム対処法で大規模な特定電気通信役務提供者に求められる対応の趣旨として、最も適切なものはどれか。

ア：利用者のすべての投稿を行政機関が公開前に検閲する。

イ：すべての申出があれば内容確認なしに即時削除する。

ウ：プラットフォーム上の投稿者の氏名を常に一般公開する。

エ：権利侵害情報への削除申出に関する手続の迅速化や運用状況の透明化を図る。

答え・解説 正答：エ

ア：事前検閲制度を定めるものではありません。

イ：削除の要否は権利侵害等を踏まえて判断し、手続の迅速化・透明化を図る制度です。

ウ：そのような一律の公開義務ではありません。

エ：大規模プラットフォームに対して、削除申出窓口・調査・通知・運用状況公表等の義務が設けられています。

総合解説：「迅速化」と「必ず削除」は同じではありません。申出への適切な調査・判断と透明性確保がポイントです。

対象：2026年度 / 基準日 2026-09-05

0053 セキュリティ関連法規 > 情報流通プラットフォーム対処法・特定電子メール法 ｜ 難易度：基礎

特定電子メール法における広告宣伝メール送信の原則として、最も適切なものはどれか。

ア：一定の例外を除き、あらかじめ送信を求め又は送信に同意した者に対して送信する。

イ：受信者が拒否するまで、本人の意思に関係なく無制限に送信できる。

ウ：送信者名を隠せば事前同意は不要になる。

エ：広告メールは法律上すべて禁止されている。

答え・解説 正答：ア

ア：特定電子メール法は広告宣伝メールについて原則オプトイン方式を採用しています。

イ：原則として事前同意が必要です。

ウ：送信者情報を偽ることは適切ではなく、同意原則も変わりません。

エ：所定の要件を満たせば広告宣伝メールの送信自体が全面禁止されているわけではありません。

総合解説：オプトインは「事前に受信意思を確認する」方式です。例外、表示義務、受信拒否後の取扱いも合わせて整理します。

対象：2026年度 / 基準日 2026-09-05

0054 セキュリティ関連法規 > 情報流通プラットフォーム対処法・特定電子メール法 ｜ 難易度：標準

大規模SNS上の投稿について、利用者が「自分の権利を侵害している」と削除を申し出た。プラットフォーム側の対応として最も適切なものはどれか。

ア：申出があれば内容を確認せず必ず即時削除する。

イ：法令上の手続に従い申出を受け付け、必要な調査・判断を迅速に行い、所定の通知等を行う。

ウ：削除申出の窓口を設けず、利用者からの連絡を一切受け付けない。

エ：削除しない場合は理由を一切示さず、結果も通知しない。

答え・解説 正答：イ

ア：申出だけで機械的に削除が義務付けられるわけではありません。

イ：大規模プラットフォームには、削除申出への迅速な対応や透明性確保に関する義務があります。

ウ：大規模事業者には申出手続の整備等が求められます。

エ：法令上、申出者への通知等が求められる場合があります。

総合解説：権利侵害情報対応では、投稿者の表現の利益と申出者の権利保護を踏まえ、制度に沿った調査・判断を行います。

対象：2026年度 / 基準日 2026-09-05

0055 セキュリティ関連法規 > 情報流通プラットフォーム対処法・特定電子メール法 ｜ 難易度：標準

匿名投稿による権利侵害の被害者が、投稿の削除だけでなく投稿者を特定して損害賠償請求を検討している。最も適切な考え方はどれか。

ア：投稿が削除されれば、発信者情報は自動的に一般公開される。

イ：匿名投稿について発信者情報を開示する制度は存在しない。

ウ：削除申出と発信者情報開示は目的・手続が異なるため、必要に応じて発信者情報開示制度の要件と手続を確認する。

エ：被害者が希望すれば、法的要件を確認せず必ず全個人情報を開示できる。

答え・解説 正答：ウ

ア：削除と発信者情報開示は別手続です。

イ：法令に発信者情報開示に関する制度があります。

ウ：投稿削除は情報流通を止めること、発信者情報開示は権利行使のため発信者を特定することが主な目的で、別の手続です。

エ：開示には法律上の要件・手続があります。

総合解説：プラットフォーム法務では「削除」「発信者情報開示」「事業者の責任制限」を区別することが重要です。

対象：2026年度 / 基準日 2026-09-05

0056 セキュリティ関連法規 > 情報流通プラットフォーム対処法・特定電子メール法 ｜ 難易度：標準

事業者が同意を得た相手へ広告メールを送る場合の対応として、最も適切なものはどれか。

ア：同意を得ていれば、送信者を偽装してもよい。

イ：同意があれば、受信拒否の手段を一切用意しなくてよい。

ウ：メール本文に広告であることが分からないようにすることが法の目的である。

エ：法令で求められる送信者情報や受信拒否のために必要な事項等を適切に表示する。

答え・解説 正答：エ

ア：送信者情報を偽ることは認められません。

イ：受信拒否に関する表示・対応が必要です。

ウ：法は適正な送信と利用者保護を目的としています。

エ：事前同意を得た場合でも表示義務等は別途存在します。

総合解説：メール法務では「事前同意」と「表示義務」「拒否後の送信停止」を別々の要件として確認します。

対象：2026年度 / 基準日 2026-09-05

0057 セキュリティ関連法規 > 情報流通プラットフォーム対処法・特定電子メール法 ｜ 難易度：標準

利用者から広告メールの受信拒否が明確に通知された後も、同じ広告メールを送り続けている。最も適切な対応はどれか。

ア：受信拒否の意思を反映して送信を停止し、配信リストや配信システムを適切に更新する。

イ：最初に同意を得ていれば、その後の受信拒否は無視してよい。

ウ：件名だけ変えれば同じ広告を送り続けてよい。

エ：別の配信システムを使えば受信拒否情報を引き継がなくてよい。

答え・解説 正答：ア

ア：特定電子メール法は、受信拒否の通知を受けた後の広告宣伝メール送信を制限しています。

イ：受信拒否後は適切に停止する必要があります。

ウ：内容や送信者を変装しても受信拒否の意思を無視できるわけではありません。

エ：組織として受信拒否を反映する運用が必要です。

総合解説：同意管理は取得時だけでなく撤回・拒否までライフサイクルで管理する必要があります。

対象：2026年度 / 基準日 2026-09-05

0058 セキュリティ関連法規 > 情報流通プラットフォーム対処法・特定電子メール法 ｜ 難易度：標準

営業部が外部業者からメールアドレス一覧を購入し、「本人同意の有無は不明だが全員に広告メールを送ろう」としている。最も適切な対応はどれか。

ア：リストを有償購入したので、本人同意は自動的に成立する。

イ：送信対象ごとに法令上の同意又は例外の要件を確認できない限り、一律送信を避け、取得経緯・同意記録を確認する。

ウ：メールアドレスは文字列なので、特定電子メール法の対象にならない。

エ：送信者名を海外企業名にすれば日本法を確認しなくてよい。

答え・解説 正答：イ

ア：購入契約と受信者の同意は別です。

イ：広告宣伝メールは原則オプトインのため、リストを購入しただけで送信の適法性が当然に確保されるわけではありません。

ウ：広告宣伝メールの送信には同法の規律があります。

エ：送信の態様や対象等に応じて法令適用を確認する必要があります。

総合解説：マーケティングでは、リストの入手経路だけでなく、受信者の同意記録や適用除外の有無を確認します。

対象：2026年度 / 基準日 2026-09-05

0059 セキュリティ関連法規 > 情報流通プラットフォーム対処法・特定電子メール法 ｜ 難易度：応用

匿名SNS投稿で企業秘密だと主張する情報と担当者への中傷が拡散している。企業は投稿の流通停止と投稿者特定の双方を検討している。最も適切な進め方はどれか。

ア：投稿者特定を望む場合でも、投稿のURLや画面記録などの証拠は残さなくてよい。

イ：SNSへ削除申出をすれば、投稿者の氏名・住所が必ず自動通知される。

ウ：権利侵害の具体的内容と証拠を整理し、削除申出と発信者情報開示の各要件・手続を分けて検討し、必要に応じて法的専門家へ相談する。

エ：中傷投稿はすべて同法により即時削除され、個別判断は一切ない。

答え・解説 正答：ウ

ア：後の手続に備えて適切に証拠を保全することが重要です。

イ：削除と発信者情報開示は別です。

ウ：削除と発信者特定は別目的・別手続です。権利侵害の根拠と証拠保全を行った上で適切な制度を利用します。

エ：権利侵害の成否や手続に応じた判断が必要です。

総合解説：インターネット上の権利侵害では、まず証拠保全、流通停止、発信者特定、損害回復など目的を分けて対応します。

対象：2026年度 / 基準日 2026-09-05

0060 セキュリティ関連法規 > 情報流通プラットフォーム対処法・特定電子メール法 ｜ 難易度：応用

EC事業者が広告メールを運用している。申込画面では広告配信への同意が他の規約に埋もれ、送信メールには配信停止方法も記載していない。改善として最も適切なものはどれか。

ア：一度でもサービスを利用した人には、同意確認や受信拒否対応なしで永久に広告を送れる。

イ：配信停止リンクを隠すほど法令順守になる。

ウ：広告送信を外部委託すれば、委託元は法令順守を一切確認しなくてよい。

エ：広告配信への同意を適切に取得・記録し、送信時の表示義務や受信拒否手段を整備し、拒否後は確実に停止する。

答え・解説 正答：エ

ア：原則オプトインや受信拒否対応を確認する必要があります。

イ：受信拒否に必要な情報を適切に表示することが求められます。

ウ：外部委託しても自社の法令・契約上の責任確認は必要です。

エ：特定電子メール法への対応は、同意取得、記録、表示、拒否処理を一連の運用として設計することが重要です。

総合解説：広告メール運用はマーケティングシステムの設定と法務要件を結び付けます。同意証跡や停止リストの一元管理が有効です。

対象：2026年度 / 基準日 2026-09-05

0061 知的財産・契約・労働 > 著作権・不正競争防止法・営業秘密 ｜ 難易度：基礎

日本の著作権に関する説明として、最も適切なものはどれか。

ア：著作物を創作した時点で原則として著作権が発生し、権利発生のための登録を一般的な要件とはしない。

イ：著作権は特許庁への登録が完了した時点でのみ発生する。

ウ：著作権は出版物に限って発生し、プログラムには生じない。

エ：著作権は法人だけが取得でき、個人の創作者には生じない。

答え・解説 正答：ア

ア：日本の著作権制度は無方式主義を採り、著作物の創作により権利が発生します。

イ：著作権の発生に一般的な登録は必要ありません。

ウ：プログラムも著作物となり得ます。

エ：個人も著作者となり得ます。

総合解説：著作権と特許権・商標権などの産業財産権では権利取得の仕組みが異なります。登録の要否を混同しないことが重要です。

対象：2026年度 / 基準日 2026-09-05

0062 知的財産・契約・労働 > 著作権・不正競争防止法・営業秘密 ｜ 難易度：基礎

ソフトウェアと著作権の関係として、最も適切なものはどれか。

ア：アルゴリズムの考え方を知っただけで、他者は同じ処理目的のソフトウェアを一切作れない。

イ：創作性のあるプログラムの具体的な表現は著作物として保護され得るが、単なるアイデアやアルゴリズムそのものとは区別して考える。

ウ：プログラムは著作権法の保護対象になり得ない。

エ：ソースコードをWebで公開すると、著作権は自動的に放棄される。

答え・解説 正答：イ

ア：著作権はアイデア自体を一般に独占するものではありません。

イ：著作権は創作的な表現を保護し、アイデアそのものを独占する制度ではありません。

ウ：プログラムは著作物の一類型です。

エ：公開しただけで著作権が自動消滅するわけではなく、利用条件はライセンス等で定められます。

総合解説：情報系資格では「プログラムの表現」と「アルゴリズム・アイデア」の区別が重要です。OSSでも著作権が存在し、ライセンスに基づいて利用許諾されるのが通常です。

対象：2026年度 / 基準日 2026-09-05

0063 知的財産・契約・労働 > 著作権・不正競争防止法・営業秘密 ｜ 難易度：基礎

不正競争防止法上の営業秘密として保護されるための三要件の組合せとして、最も適切なものはどれか。

ア：機密性・完全性・可用性。

イ：新規性・進歩性・産業上の利用可能性。

ウ：秘密管理性・有用性・非公知性。

エ：真正性・責任追跡性・否認防止。

答え・解説 正答：ウ

ア：これは情報セキュリティのCIAであり、営業秘密の三要件ではありません。

イ：これは主に特許要件に関する用語です。

ウ：経済産業省は営業秘密の三要件として秘密管理性、有用性、非公知性を示しています。

エ：情報セキュリティ上の特性であり、営業秘密の三要件ではありません。

総合解説：営業秘密は「社内で秘密と呼んでいる」だけでは足りません。秘密として管理され、事業上有用で、公然と知られていないことが必要です。

対象：2026年度 / 基準日 2026-09-05

0064 知的財産・契約・労働 > 著作権・不正競争防止法・営業秘密 ｜ 難易度：標準

開発者が前職で作成したソースコードを無断で持ち出し、新しい勤務先の製品へそのまま組み込もうとしている。最も適切な対応はどれか。

ア：自分が書いたコードなら、職務上作成したものでも必ず自由に持ち出せる。

イ：ソースコードは物ではないので、無断利用しても知的財産上の問題は生じない。

ウ：変数名を数個変更すれば、元コードの権利関係は必ず消滅する。

エ：著作権の帰属や利用許諾、営業秘密該当性等を確認し、権利関係が明確でないコードは使用しない。

答え・解説 正答：エ

ア：職務著作や契約、営業秘密等により権利関係が異なり得ます。

イ：プログラムは著作権法の保護対象となり得ます。

ウ：表面的な変更だけで著作権等の問題が当然に解消するわけではありません。

エ：前職で作成したコードには著作権・営業秘密・契約上の守秘義務など複数の論点があり得ます。

総合解説：業務で他社・前職のコードを利用する場合は、著作権、ライセンス、秘密情報、雇用契約などを横断的に確認します。

対象：2026年度 / 基準日 2026-09-05

0065 知的財産・契約・労働 > 著作権・不正競争防止法・営業秘密 ｜ 難易度：標準

企業が「営業秘密」と主張する顧客リストを、社内外から誰でも認証なしで閲覧できる公開URLに置いていた。最も適切な判断はどれか。

ア：秘密として管理されていたと認められるかに重大な問題が生じ、営業秘密の秘密管理性を満たさない可能性が高まる。

イ：ファイル名に「secret」と付けていれば、公開状態でも必ず秘密管理性を満たす。

ウ：顧客リストは価値があるため、管理方法に関係なく必ず営業秘密になる。

エ：一度営業秘密と指定した情報は、インターネット公開後も永遠に非公知性を失わない。

答え・解説 正答：ア

ア：営業秘密として保護を受けるには、情報を秘密として管理する意思が従業者等に認識可能な形で示されていることが重要です。

イ：名称だけでなく実際の管理状況が重要です。

ウ：有用性だけでなく秘密管理性・非公知性も必要です。

エ：公知となれば非公知性にも影響します。

総合解説：営業秘密保護には、アクセス制御、秘密表示、規程、教育などにより秘密として管理していることを客観的に示す必要があります。

対象：2026年度 / 基準日 2026-09-05

0066 知的財産・契約・労働 > 著作権・不正競争防止法・営業秘密 ｜ 難易度：標準

競合企業と同様の機能を持つシステムを、自社の技術者が公開情報と独自研究だけを用いて開発した。競合の営業秘密を不正取得・使用した事実はない。最も適切な考え方はどれか。

ア：競合と同じ機能を実現しただけで、必ず営業秘密侵害となる。

イ：類似した成果になったことだけで直ちに営業秘密侵害となるわけではなく、不正な取得・使用・開示等の事実を具体的に検討する。

ウ：営業秘密は特許と同じなので、独自開発でも必ず使用禁止となる。

エ：公開情報を調査する行為自体が営業秘密の不正取得に該当する。

答え・解説 正答：イ

ア：機能の類似だけで営業秘密の不正取得等が当然に認定されるわけではありません。

イ：営業秘密制度は秘密情報の不正取得等を規制するもので、独自開発まで一律に禁止するものではありません。

ウ：営業秘密と特許は保護の仕組みが異なります。

エ：公知情報の通常利用は営業秘密の不正取得とは異なります。

総合解説：営業秘密は「秘密だから守られる」制度であり、独占権として公開技術まで広く排除する特許とは性質が異なります。

対象：2026年度 / 基準日 2026-09-05

0067 知的財産・契約・労働 > 著作権・不正競争防止法・営業秘密 ｜ 難易度：標準

GitHub上でソースコードが公開されているライブラリを見つけた。利用前の対応として最も適切なものはどれか。

ア：インターネットで閲覧できるコードには著作権が存在しない。

イ：URLが公開されていれば、ライセンス条件を無視して商用製品へ組み込める。

ウ：公開されているだけで自由利用できるとは限らないため、著作権表示とライセンス条件を確認する。

エ：コードを一行でも改変すれば元の著作権は必ず消える。

答え・解説 正答：ウ

ア：公開コードにも著作権は存在し得ます。

イ：利用はライセンス許諾の範囲で行う必要があります。

ウ：ソースコードが閲覧可能であることと、任意条件で利用・改変・再配布できることは別です。

エ：改変しても元著作物の権利関係が残る場合があります。

総合解説：OSS利用では「無料」「公開」「自由」を同一視しないことが重要です。各ライセンスの条件を確認します。

対象：2026年度 / 基準日 2026-09-05

0068 知的財産・契約・労働 > 著作権・不正競争防止法・営業秘密 ｜ 難易度：標準

未公開の自社ソースコードを、退職予定者が秘密保持規程に反して外部へ持ち出した。最も適切な考え方はどれか。

ア：著作権があれば営業秘密や契約上の検討は一切不要である。

イ：ソースコードは営業秘密にはなり得ない。

ウ：退職予定者なら持出しを自由に行える。

エ：著作権だけでなく、秘密管理性等を満たす場合は不正競争防止法上の営業秘密や契約上の守秘義務も問題となり得る。

答え・解説 正答：エ

ア：複数の法制度・契約が同時に適用され得ます。

イ：要件を満たせば技術上の情報として営業秘密となり得ます。

ウ：在職・退職にかかわらず、権限や契約、法律に従う必要があります。

エ：同一の情報について複数の法的保護が重なることがあります。

総合解説：実務では「著作権か営業秘密か」の二者択一ではなく、複数の保護根拠を整理します。

対象：2026年度 / 基準日 2026-09-05

0069 知的財産・契約・労働 > 著作権・不正競争防止法・営業秘密 ｜ 難易度：応用

営業担当者が、アクセス制限と秘密表示がされた顧客名簿を退職直前に私物クラウドへコピーし、転職先で営業に利用した。最も適切な対応はどれか。

ア：顧客名簿が営業秘密の三要件を満たすか確認し、不正取得・使用等の該当性、契約違反、証拠保全を含めて対応する。

イ：顧客名簿は営業情報なので、どのような管理状態でも自動的に営業秘密である。

ウ：退職前にコピーしたので、退職後の利用は常に自由である。

エ：社内規程違反だけを確認すればよく、不正競争防止法は検討不要である。

答え・解説 正答：ア

ア：適切に秘密管理された有用かつ非公知の顧客情報は営業秘密となり得ます。持出し・転用の事実を証拠とともに整理します。

イ：営業秘密には三要件が必要です。

ウ：権限ある閲覧と私的な持出し・転用は別です。

エ：要件を満たす場合は法令上の営業秘密侵害も問題となり得ます。

総合解説：内部不正事案では、営業秘密該当性、アクセスログ、持出し経路、利用状況、契約・規程を整理し、技術・法務の両面で対応します。

対象：2026年度 / 基準日 2026-09-05

0070 知的財産・契約・労働 > 著作権・不正競争防止法・営業秘密 ｜ 難易度：応用

開発者が匿名掲示板に流出した競合製品のソースコードをダウンロードし、自社製品へ多数の部分をコピーしようとしている。最も適切な対応はどれか。

ア：ネット上に流出した時点で著作権は消滅するため自由利用できる。

イ：利用を止め、著作権侵害や営業秘密の不正取得・使用等に該当する可能性を法務部門と確認する。

ウ：匿名掲示板から取得したので、出所を確認する必要はない。

エ：自社製品の一部にだけ使えば、知的財産上の問題は必ずなくなる。

答え・解説 正答：イ

ア：無断流出で著作権が消滅するわけではありません。

イ：流出物であることを認識しながら利用する行為は、著作権・営業秘密等の重大なリスクがあります。

ウ：不正取得された情報である可能性や権利関係を確認すべきです。

エ：利用量だけで適法性が決まるわけではありません。

総合解説：出所不明・流出疑いのコードは、法的クリーンルームを汚染するリスクがあります。採用前に権利と出所を確認する運用が重要です。

対象：2026年度 / 基準日 2026-09-05

0071 知的財産・契約・労働 > ライセンス・コピーレフト・契約類型 ｜ 難易度：基礎

ソフトウェアライセンスの説明として、最も適切なものはどれか。

ア：ライセンス契約を結ぶと、著作権そのものが必ず利用者へ移転する。

イ：ソフトウェアを購入すれば、著作権者の条件に関係なく無制限に再配布できる。

ウ：著作権等を保有する者が、一定の条件の下でソフトウェアの利用・複製・改変・再配布等を許諾する仕組みである。

エ：無料ソフトウェアにはライセンス条件が存在しない。

答え・解説 正答：ウ

ア：利用許諾と著作権譲渡は別です。

イ：購入した利用権の範囲はライセンス条件に従います。

ウ：ライセンスは権利の全面放棄ではなく、利用条件を定める許諾です。

エ：無償でも利用条件が定められていることがあります。

総合解説：「所有権」「著作権」「利用許諾」を区別することが重要です。パッケージやクラウド利用でも契約条件を確認します。

対象：2026年度 / 基準日 2026-09-05

0072 知的財産・契約・労働 > ライセンス・コピーレフト・契約類型 ｜ 難易度：基礎

コピーレフト型OSSライセンスの一般的な考え方として、最も適切なものはどれか。

ア：コピーレフトとは、著作権が一切存在しない状態をいう。

イ：コピーレフト型ソフトウェアは商用利用が法律で一律禁止されている。

ウ：すべてのOSSライセンスは同じ条件であり、区別する必要がない。

エ：著作権を放棄するのではなく、改変物や派生物を配布する際に同じ又は互換するライセンス条件の継承等を求めるものがある。

答え・解説 正答：エ

ア：著作権を前提にライセンス条件を設定する仕組みです。

イ：商用利用可能なコピーレフト型OSSもあります。

ウ：ライセンスごとに義務や許諾範囲が異なります。

エ：コピーレフトは著作権を利用して、一定の自由や条件を派生物へ継承させる考え方です。具体的義務は各ライセンス本文で確認します。

総合解説：OSSでは「オープンソース」という共通性があっても、コピーレフトの強さや通知義務などはライセンスごとに異なります。

対象：2026年度 / 基準日 2026-09-05

0073 知的財産・契約・労働 > ライセンス・コピーレフト・契約類型 ｜ 難易度：基礎

情報システム開発契約で、請負と準委任を区別する観点として最も適切なものはどれか。

ア：請負は仕事の完成を目的とするのに対し、準委任は一定の事務処理を善良な管理者の注意をもって遂行することが中心となる。

イ：請負も準委任も、常に同一の成果完成義務を負う。

ウ：準委任では作業を一切行わなくても報酬請求が必ず認められる。

エ：契約書の題名だけで法的性質が必ず決まり、実際の合意内容は無関係である。

答え・解説 正答：ア

ア：契約類型により受託者の義務の性質や成果物・検収等の考え方が異なります。実際の契約では個別条項を確認します。

イ：契約類型により義務の性質が異なります。

ウ：適切な事務処理の遂行義務等があります。

エ：契約の内容・実態を確認する必要があります。

総合解説：システム開発では工程ごとに請負・準委任が使い分けられることがあります。名称だけでなく、完成責任や役割分担を確認します。

対象：2026年度 / 基準日 2026-09-05

0074 知的財産・契約・労働 > ライセンス・コピーレフト・契約類型 ｜ 難易度：標準

無償で入手できるOSSライブラリを商用製品へ組み込みたい。最初に行うべき対応として最も適切なものはどれか。

ア：無料なので、ライセンス文を確認せず自由に再配布する。

イ：対象ライブラリのライセンスを特定し、商用利用・改変・再配布・著作権表示・ソースコード提供等の条件を確認する。

ウ：OSSであれば著作権表示を削除して自社著作物として表示してよい。

エ：ソースコードを閲覧できれば、そのソフトウェアは必ずOSI認定OSSである。

答え・解説 正答：イ

ア：無償性と無条件利用は別です。

イ：OSSは無償で入手できても、利用条件がないわけではありません。

ウ：ライセンスや著作者表示に従う必要があります。

エ：単なるソース公開とオープンソースライセンスは区別されます。

総合解説：OSS管理ではSBOM等と連携し、採用ライブラリの名称・版・ライセンス・義務を継続的に把握すると有効です。

対象：2026年度 / 基準日 2026-09-05

0075 知的財産・契約・労働 > ライセンス・コピーレフト・契約類型 ｜ 難易度：標準

コピーレフト型OSSを改変して製品とともに配布する計画がある。対応として最も適切なものはどれか。

ア：コピーレフト型なら、製品の販売自体が必ず禁止される。

イ：社内で一度改変しただけで、外部配布の有無に関係なく必ず全社のソースコード公開義務が生じる。

ウ：該当するライセンス本文を確認し、ソースコード提供やライセンス条件継承等、配布時に求められる義務を満たす。

エ：ライセンス名を確認せず「OSSだから大丈夫」と判断する。

答え・解説 正答：ウ

ア：商用販売そのものが一律禁止されているわけではありません。

イ：義務発生条件は各ライセンスと利用・配布形態に依存します。

ウ：コピーレフト型ライセンスでは配布時に一定の義務が生じる場合があります。具体的範囲はライセンスごとに確認します。

エ：具体的ライセンス条件の確認が必要です。

総合解説：OSS問題では断定し過ぎず、「各ライセンス本文で義務を確認する」が重要です。特に結合方法や配布形態で影響が変わります。

対象：2026年度 / 基準日 2026-09-05

0076 知的財産・契約・労働 > ライセンス・コピーレフト・契約類型 ｜ 難易度：標準

開発会社へソフトウェア開発を委託し、代金を全額支払った。発注者が「代金を払ったので著作権も当然すべて自社へ移った」と判断している。最も適切な考え方はどれか。

ア：委託契約では、どのような契約条項でも著作権は必ず発注者へ自動移転する。

イ：著作権の帰属は契約で定めることができない。

ウ：著作権を移転すれば、第三者ライブラリのライセンス条件もすべて消滅する。

エ：著作権の帰属・譲渡範囲は契約や法令に基づいて確認し、代金支払だけで当然に全著作権が移転すると決めつけない。

答え・解説 正答：エ

ア：契約内容や法令上の規定を確認する必要があります。

イ：契約で帰属・利用許諾等を定めることが一般的です。

ウ：第三者権利は別途残ります。

エ：成果物の所有・利用許諾と著作権の帰属は別に定める必要があります。

総合解説：委託開発では、成果物、知的財産権、既存ソフトウェア、第三者ソフトウェアの取扱いを契約で明確化します。

対象：2026年度 / 基準日 2026-09-05

0077 知的財産・契約・労働 > ライセンス・コピーレフト・契約類型 ｜ 難易度：標準

複数のOSSライブラリを一つの配布製品に組み込みたいが、それぞれ異なるライセンスである。最も適切な対応はどれか。

ア：各ライセンスの義務と相互の互換性、結合・配布形態を確認し、両立しない条件があれば構成やライブラリを見直す。

イ：OSS同士ならライセンス条件は必ず互換なので確認不要である。

ウ：最も緩いライセンスだけ守れば、他のライセンスは無視できる。

エ：製品名を変更すればライセンス条件は消滅する。

答え・解説 正答：ア

ア：異なるOSSライセンスを組み合わせる場合は、同時に満たすべき条件が矛盾しないか確認が必要です。

イ：OSSライセンス間でも条件が異なり、互換性問題が生じることがあります。

ウ：利用する各コンポーネントの条件を満たす必要があります。

エ：名称変更で権利・義務が消えるわけではありません。

総合解説：ライセンス管理は採用時だけでなく、バージョン更新や依存ライブラリ変更時にも再確認します。

対象：2026年度 / 基準日 2026-09-05

0078 知的財産・契約・労働 > ライセンス・コピーレフト・契約類型 ｜ 難易度：標準

要件が固まっていない探索的なアジャイル開発の初期工程で、一定期間チームが専門的作業を行う契約を検討している。最も適切な考え方はどれか。

ア：要件が未確定でも、請負契約なら仕様を一切決めずに完成責任だけ負わせればよい。

イ：成果完成の確約が難しい工程では準委任型を含む契約類型を検討し、役割・作業範囲・成果の確認方法を明確にする。

ウ：準委任では作業内容や責任分担を契約に書く必要がない。

エ：契約類型はプロジェクトリスクと無関係なので、常に同じひな型を使えばよい。

答え・解説 正答：イ

ア：完成基準が不明確だと紛争リスクが高まります。

イ：工程の性質に応じて契約類型を選び、責任分担や検収方法を設計することが重要です。

ウ：準委任でも役割、期間、報告、成果物等を明確にすることが重要です。

エ：工程特性と責任分担に応じて設計すべきです。

総合解説：IT契約では法律上の名称だけでなく、実際の開発手法・不確実性・検収・変更管理と整合させます。

対象：2026年度 / 基準日 2026-09-05

0079 知的財産・契約・労働 > ライセンス・コピーレフト・契約類型 ｜ 難易度：応用

自社製品へOSSを組み込んだ後、発売直前に「ライセンス文書を一度も確認していない」ことが判明した。最も適切な対応はどれか。

ア：OSSは無料なので、どのライセンスでも確認不要である。

イ：自社製品が有料ならOSSを使うこと自体が必ず禁止される。

ウ：出荷を急いで無視せず、使用OSSとバージョンを特定し、ライセンス条件、著作権表示、ソース提供等の義務を確認してから出荷可否を判断する。

エ：製品の利用規約に「すべて自社所有」と書けば第三者OSSの条件を上書きできる。

答え・解説 正答：ウ

ア：無料であってもライセンス条件があります。

イ：商用利用の可否・条件はライセンスごとに確認します。

ウ：発売後のライセンス違反は差止め・信用低下等のリスクにつながるため、出荷前に確認すべきです。

エ：自社規約だけで第三者の権利・ライセンス条件を消すことはできません。

総合解説：OSSコンプライアンスでは、部品表、ライセンス一覧、通知文、ソース提供義務などをリリースゲートで確認すると有効です。

対象：2026年度 / 基準日 2026-09-05

0080 知的財産・契約・労働 > ライセンス・コピーレフト・契約類型 ｜ 難易度：応用

開発チームが、作者もライセンスも不明なコード片をインターネットから取得し、商用サービスの中核機能へ組み込もうとしている。最も適切な対応はどれか。

ア：作者不明なら著作権者も存在しないため自由に使える。

イ：コードが短ければ必ず著作物ではなく、確認は一切不要である。

ウ：インターネット検索で見つかったコードはすべてパブリックドメインである。

エ：権利者と利用条件を確認できるまで採用を保留し、必要なら自社実装や権利関係が明確な代替ライブラリへ置き換える。

答え・解説 正答：エ

ア：作者が分からないことと著作権がないことは同じではありません。

イ：創作性や利用範囲は個別に評価され、短さだけで一律に判断できません。

ウ：公開されていることと権利放棄は別です。

エ：ライセンス不明のコードは、利用許諾の範囲を確認できず、法務リスクが高い状態です。

総合解説：開発のスピードより、ソフトウェアサプライチェーンの権利情報を追跡できる状態を優先します。

対象：2026年度 / 基準日 2026-09-05

0081 知的財産・契約・労働 > 守秘契約・委託契約・労働／派遣の基礎 ｜ 難易度：基礎

新製品の共同検討に先立ち、相手企業へ未公開仕様を開示することになった。この場面でNDA（秘密保持契約）を締結する主な目的として、最も適切なものはどれか。

ア：開示する秘密情報の範囲や利用目的、第三者開示の制限、返還・廃棄等の取扱いを当事者間で定める。

イ：相手方へ開示した情報の著作権を必ず相手へ譲渡する。

ウ：契約締結後は技術的アクセス制御が一切不要になる。

エ：秘密情報をインターネットへ公開することを義務付ける。

答え・解説 正答：ア

ア：NDAは秘密情報の取扱条件を契約で明確化し、情報開示に伴うリスクを管理するために用いられます。

イ：秘密保持と著作権譲渡は別の契約事項です。

ウ：契約と技術的・組織的対策は補完関係です。

エ：NDAは通常、秘密情報の不適切な開示を防ぐための契約です。

総合解説：NDAでは秘密情報の定義、除外情報、利用目的、開示可能者、期間、事故時対応、返還・廃棄などを具体化します。

対象：2026年度 / 基準日 2026-09-05

0082 知的財産・契約・労働 > 守秘契約・委託契約・労働／派遣の基礎 ｜ 難易度：基礎

情報システム運用を外部委託する契約に盛り込むセキュリティ事項として、最も適切なものはどれか。

ア：委託価格だけを定め、セキュリティ責任は一切書かない。

イ：安全管理要求、アクセス権、再委託条件、事故報告、監査・確認、契約終了時のデータ返還・削除等を明確にする。

ウ：再委託は無条件で何層でも自由とし、委託元は把握しない。

エ：契約終了後も顧客データを委託先が自由に保有できるようにする。

答え・解説 正答：イ

ア：事故時の責任や要求事項が不明確になり、リスクが高まります。

イ：委託契約では、業務内容だけでなくセキュリティ上の責任分担とライフサイクルを明確化することが重要です。

ウ：サプライチェーン管理の観点から再委託条件・把握が重要です。

エ：返還・削除・保存義務等を明確にする必要があります。

総合解説：委託管理は選定から契約、運用確認、再委託、終了まで一貫して行います。

対象：2026年度 / 基準日 2026-09-05

0083 知的財産・契約・労働 > 守秘契約・委託契約・労働／派遣の基礎 ｜ 難易度：基礎

労働者派遣と請負の違いに関する説明として、最も適切なものはどれか。

ア：請負でも注文主が請負労働者へ日常的に直接指揮命令することが制度の前提である。

イ：派遣労働者は派遣先と雇用契約を結び、派遣元とは無関係である。

ウ：労働者派遣では派遣先が派遣労働者に指揮命令するが、請負では注文主と請負事業者の労働者との間に直接の指揮命令関係を生じさせない。

エ：契約書の題名が「請負」であれば、実態がどうであっても必ず請負になる。

答え・解説 正答：ウ

ア：請負では注文主と請負労働者の間に指揮命令関係を生じさせないことが基本です。

イ：派遣労働者は派遣元と雇用関係を持ち、派遣先から指揮命令を受けます。

ウ：厚生労働省は、派遣と請負の重要な区別として指揮命令関係を示しています。

エ：派遣・請負の区分は契約形式だけでなく実態に即して判断されます。

総合解説：情報システム現場では、常駐委託者への指示方法が偽装請負の問題につながり得ます。契約形式だけでなく実態を確認します。

対象：2026年度 / 基準日 2026-09-05

0084 知的財産・契約・労働 > 守秘契約・委託契約・労働／派遣の基礎 ｜ 難易度：標準

委託先全員とNDAを締結したため、顧客データベースを委託先の全従業員へ管理者権限で開放しようとしている。最も適切な判断はどれか。

ア：NDAがあれば、アクセス権は無制限でよい。

イ：アクセスログを取れば、権限管理は一切不要である。

ウ：委託先社員はすべて同じ業務をするため、個別の役割確認は不要である。

エ：NDAは重要だが安全管理の代替ではないため、業務上必要な者だけに最小権限を付与し、ログ・教育等も組み合わせる。

答え・解説 正答：エ

ア：秘密保持契約だけで不要なアクセスを防止できません。

イ：予防的なアクセス制御と事後追跡の両方が重要です。

ウ：役割に応じた必要最小限の権限が基本です。

エ：契約上の義務とアクセス制御などの管理策は補完関係にあります。

総合解説：法的対策と技術的対策を一方だけに依存しないことが、情報セキュリティ管理の基本です。

対象：2026年度 / 基準日 2026-09-05

0085 知的財産・契約・労働 > 守秘契約・委託契約・労働／派遣の基礎 ｜ 難易度：標準

クラウド運用委託契約が終了した。委託先には顧客データの複製が残っている。最も適切な対応はどれか。

ア：法令上の保存義務等を確認した上で、契約に従いデータを返還・削除し、必要に応じて削除完了を確認する。

イ：契約終了後は委託先が自由に顧客データを利用してよい。

ウ：本番データだけ削除すれば、バックアップや複製の扱いは確認不要である。

エ：契約が終了したので、委託元は削除状況を確認する必要がない。

答え・解説 正答：ア

ア：契約終了時はアカウント無効化、データ返還・廃棄、媒体・バックアップの扱いまで確認することが重要です。

イ：委託目的終了後の利用は契約・法令に反する可能性があります。

ウ：複製・バックアップを含むデータライフサイクルを確認すべきです。

エ：終了時の管理も委託元の重要な確認事項です。

総合解説：外部委託では「入口」だけでなく「出口」の管理が重要です。データ残存やアカウント残存を防ぎます。

対象：2026年度 / 基準日 2026-09-05

0086 知的財産・契約・労働 > 守秘契約・委託契約・労働／派遣の基礎 ｜ 難易度：標準

契約上は請負だが、注文主の社員が請負会社の個々の作業者へ毎日直接、作業手順・開始時刻・担当割当てを指示している。最も適切な考え方はどれか。

ア：契約書に「請負」と書いてあれば、実態は一切考慮しない。

イ：契約名が請負でも実態が派遣に該当する可能性があるため、指揮命令関係を含めて派遣・請負の区分基準に照らして見直す。

ウ：注文主からの直接指揮命令は請負に必須である。

エ：偽装請負は情報システム業務では問題にならない。

答え・解説 正答：イ

ア：実態に即した判断が必要です。

イ：厚生労働省は契約形式ではなく実態に即して派遣・請負を判断するとしています。

ウ：請負では請負事業者が自己の労働者を指揮命令することが基本です。

エ：業種を問わず実態に応じて区分が問題となり得ます。

総合解説：常駐型IT委託では、日々のタスク指示が誰から誰へ行われているかを確認することが重要です。

対象：2026年度 / 基準日 2026-09-05

0087 知的財産・契約・労働 > 守秘契約・委託契約・労働／派遣の基礎 ｜ 難易度：標準

個人データを扱う外部委託で、契約書にセキュリティ事故時の報告期限や連絡経路がない。改善として最も適切なものはどれか。

ア：事故時はその場で考えればよいので、契約・手順は不要である。

イ：委託先が事故を公表しない限り、委託元へ報告しなくてよい。

ウ：事故の定義、初報期限、連絡先、必要報告事項、証拠保全、原因分析・再発防止への協力などを契約・手順で明確にする。

エ：事故情報は証拠になり得るため、ログを直ちに削除するよう契約する。

答え・解説 正答：ウ

ア：重大事案では迅速な法令・顧客対応が必要なため事前定義が重要です。

イ：委託元が影響評価や法令対応を行えるよう速やかな報告が必要です。

ウ：事故対応の役割と時間軸を事前に合意しておくことで、発生時の混乱と報告遅延を減らせます。

エ：ログや証拠は適切に保全すべきです。

総合解説：委託契約は「平常時の業務」だけでなく「異常時の共同対応」まで設計します。

対象：2026年度 / 基準日 2026-09-05

0088 知的財産・契約・労働 > 守秘契約・委託契約・労働／派遣の基礎 ｜ 難易度：標準

派遣労働者が契約終了日を迎える。システムアクセス管理として最も適切な対応はどれか。

ア：派遣元が別会社なので、派遣先のシステムアカウントは無期限に残してよい。

イ：将来また派遣されるかもしれないため、管理者権限を残す。

ウ：貸与PCを返却すれば、クラウドアカウントは残してよい。

エ：業務終了時点に合わせて不要なアカウント・権限を速やかに無効化し、貸与機器・媒体の返却も確認する。

答え・解説 正答：エ

ア：アクセス権は業務上の必要性に応じて管理します。

イ：不要権限の残存は不正アクセスリスクを高めます。

ウ：物理機器と論理アカウントの両方を終了処理する必要があります。

エ：雇用・契約形態にかかわらず、業務上の必要性がなくなった権限は速やかに削除します。

総合解説：人の入社・異動・退職・契約終了に合わせた権限ライフサイクル管理は、内部不正と不正アクセスの予防に直結します。

対象：2026年度 / 基準日 2026-09-05

0089 知的財産・契約・労働 > 守秘契約・委託契約・労働／派遣の基礎 ｜ 難易度：応用

SOC運用を委託したA社が、契約で事前承認を求められているにもかかわらず、顧客ログを扱う業務を海外のB社へ無断再委託していた。最も適切な対応はどれか。

ア：契約違反とデータ取扱リスクを確認し、再委託を停止又は是正させ、B社の安全管理・所在地・アクセス範囲・データ残存等を調査する。

イ：A社と契約しているので、その先の再委託先は一切把握しなくてよい。

ウ：海外再委託なら日本側の契約条件は自動的に無効になる。

エ：ログは個人情報になり得ないため、どの再委託先に渡しても安全管理は不要である。

答え・解説 正答：ア

ア：再委託はサプライチェーンを広げるため、契約上の承認と安全管理状況の確認が重要です。

イ：再委託先での取扱いも委託元のリスクに影響します。

ウ：契約・適用法・データ取扱いを個別に確認する必要があります。

エ：ログにも個人データや機密情報が含まれる場合があり、適切な管理が必要です。

総合解説：再委託管理では、承認、再委託先一覧、セキュリティ要求のフローダウン、監査権、事故報告、終了時削除まで確認します。

対象：2026年度 / 基準日 2026-09-05

0090 知的財産・契約・労働 > 守秘契約・委託契約・労働／派遣の基礎 ｜ 難易度：応用

自社オフィスに常駐する外部技術者について、契約は「請負」だが、自社の課長が各技術者の残業、休暇、作業順序を直接指示している。最も適切な対応はどれか。

ア：情報セキュリティ業務であれば、労働者派遣法上の区分は考慮しなくてよい。

イ：契約名称ではなく実態を確認し、請負の区分基準に適合するよう指揮命令関係や業務運営を見直す。必要なら適法な派遣契約等へ変更する。

ウ：契約書の表紙に「請負」と印刷されているので、現場運用を変える必要はない。

エ：外部技術者が同意していれば、注文主の直接指揮命令は常に請負として適法である。

答え・解説 正答：イ

ア：業務内容だけで派遣・請負の区分が消えるわけではありません。

イ：注文主が請負労働者を直接指揮命令する実態は、偽装請負と評価されるリスクがあります。

ウ：実態に即して判断されます。

エ：本人同意だけで派遣・請負の区分基準を回避できるわけではありません。

総合解説：IT現場ではセキュリティ上の権限設計に加え、誰が誰へ業務指示を出すかという労務面の統制も重要です。

対象：2026年度 / 基準日 2026-09-05

0091 規格・ガイドライン > ISO/IEC 27000・JIS Q 27000規格群 ｜ 難易度：基礎

ISO/IEC 27000の説明として、最も適切なものはどれか。

ア：ISO/IEC 27000は、ISMS規格群の基本概念や各規格の関係を理解するための概要を示す。

イ：ISO/IEC 27000は、組織を認証するための審査手順だけを規定する。

ウ：ISO/IEC 27000は、カード会員データだけを対象とする業界規格である。

エ：ISO/IEC 27000は、特定の暗号アルゴリズムだけを認定する規格である。

答え・解説 正答：ア

ア：2026年版ISO/IEC 27000は、ISMSの基本概念と27000ファミリの関係を示す概要規格です。

イ：認証の要求事項の中心はISO/IEC 27001であり、27000自体は認証審査手順だけを定める規格ではありません。

ウ：カード会員データ保護を主対象とするのはPCI DSSです。

エ：暗号アルゴリズムの認定だけを目的とする規格ではありません。

総合解説：ISO/IEC 27000ファミリでは、規格ごとの役割を区別することが重要です。27000は全体像の理解、27001はISMS要求事項、27002は管理策の実施指針という関係で整理すると混同しにくくなります。

対象：2026年度 / 基準日 2026-09-05

0092 規格・ガイドライン > ISO/IEC 27000・JIS Q 27000規格群 ｜ 難易度：基礎

ISMS認証の準備を進める企業が、要求事項の確認と管理策の具体化に用いる規格の組合せとして、最も適切なものはどれか。

ア：JIS Q 27001は管理策の実施例だけを示し、JIS Q 27002は認証要求事項を規定する。

イ：JIS Q 27001はISMSの要求事項を規定し、JIS Q 27002は情報セキュリティ管理策の実施の手引を示す。

ウ：両規格は名称だけが異なり、規定内容は同一である。

エ：JIS Q 27002は個人情報保護法の罰則だけを解説する法令集である。

答え・解説 正答：イ

ア：役割が逆です。認証要求事項の中心は27001です。

イ：JIS Q 27001はISMSを確立・実施・維持・継続的改善するための要求事項、27002は一般的な管理策と実施の手引です。

ウ：両者は関連しますが、目的と規定内容は同一ではありません。

エ：JIS Q 27002は情報セキュリティ管理策に関する規格であり、法令集ではありません。

総合解説：試験では「要求事項」と「管理策の手引」の区別が重要です。組織がISMSを構築する際、27001の要求事項を満たしつつ、27002などを参考に管理策を具体化します。

対象：2026年度 / 基準日 2026-09-05

0093 規格・ガイドライン > ISO/IEC 27000・JIS Q 27000規格群 ｜ 難易度：基礎

JIS Q 27002:2024の情報セキュリティ管理策の整理として、最も適切なものはどれか。

ア：管理策は財務・営業・製造・物流という四つの部門別に整理されている。

イ：管理策は予防策だけで構成され、検知や是正の観点は扱わない。

ウ：JIS Q 27002:2024は、管理策を組織的・人的・物理的・技術的という四つのテーマで整理している。

エ：管理策はクラウド事業者だけを対象とし、一般企業には適用できない。

答え・解説 正答：ウ

ア：部門別の整理ではありません。

イ：管理策は予防だけに限定されず、組織のリスクに応じて多様な目的で利用されます。

ウ：JIS Q 27002:2024はISO/IEC 27002:2022と整合し、93の管理策を四つのテーマで整理しています。

エ：業種や規模を限定したクラウド専用規格ではありません。

総合解説：管理策の分類は、人的・物理的・技術的対策を組織的な仕組みと一体で運用することを理解するための枠組みです。

対象：2026年度 / 基準日 2026-09-05

0094 規格・ガイドライン > ISO/IEC 27000・JIS Q 27000規格群 ｜ 難易度：標準

ある組織が情報セキュリティ管理策を選定する。規格・基準の活用方法として、最も適切なものはどれか。

ア：JIS Q 27002にある管理策を、理由を問わず全組織が同一方法で実施する。

イ：監査で指摘されないよう、費用対効果やリスクを考えず可能な管理策をすべて導入する。

ウ：一度選択した管理策は、組織や脅威の変化があっても変更しない。

エ：組織のリスクや事業特性を踏まえ、必要な管理策を選択・追加・具体化して適用する。

答え・解説 正答：エ

ア：規格は一律の実装方法をすべての組織へ強制するものではありません。

イ：過剰対策も経営資源の浪費につながるため、リスクベースで判断します。

ウ：リスクや環境の変化に応じて見直すことが必要です。

エ：管理策は組織の状況とリスクに応じて選択し、必要に応じて追加・統合・具体化します。

総合解説：情報セキュリティ管理基準も、包括的な参照基準をそのまま機械的に適用するのではなく、業界・事業特性等を考慮して取捨選択や具体化を行う考え方を示しています。

対象：2026年度 / 基準日 2026-09-05

0095 規格・ガイドライン > ISO/IEC 27000・JIS Q 27000規格群 ｜ 難易度：標準

JIS Q 27014の説明として、最も適切なものはどれか。

ア：JIS Q 27014は、情報セキュリティガバナンスの概念と原則に基づくガイダンスを示す。

イ：JIS Q 27014は、個人情報の匿名加工手順だけを規定する。

ウ：JIS Q 27014は、無線LANの暗号方式だけを規定する。

エ：JIS Q 27014は、PCI DSSの自己評価質問票そのものである。

答え・解説 正答：ア

ア：JIS Q 27014は、経営・統治の観点から情報セキュリティを方向付け、評価・監督するためのガイダンスです。

イ：匿名加工情報の法的取扱いを定める規格ではありません。

ウ：無線LAN暗号方式の規格ではありません。

エ：PCI DSSとは別の規格体系です。

総合解説：ISMSの運用管理と、経営レベルの情報セキュリティガバナンスは関連しますが同一ではありません。JIS Q 27014は後者の考え方を扱います。

対象：2026年度 / 基準日 2026-09-05

0096 規格・ガイドライン > ISO/IEC 27000・JIS Q 27000規格群 ｜ 難易度：標準

2026年9月時点のISO/IEC 27000とJIS Q 27000の版に関する説明として、最も適切なものはどれか。

ア：ISO/IEC 27000:2018だけが現行で、2026年版はまだ発行されていない。

イ：2026年9月時点ではISO/IEC 27000:2026が発行済みだが、JIS Q 27000:2019は引き続き有効である。

ウ：JIS Q 27000:2019はISO/IEC 27000:2026の発行と同時に自動的に廃止された。

エ：国際規格が改訂されると、対応JISも同日に同じ版へ自動改訂される。

答え・解説 正答：イ

ア：ISO/IEC 27000:2018は2026年版に置き換えられています。

イ：国際規格と国内JISは改訂時期が一致しない場合があります。2026年7月にISO/IEC 27000:2026が発行されましたが、JIS Q 27000:2019は有効です。

ウ：JISは別の制定・確認・改正手続を経るため自動廃止ではありません。

エ：対応関係があっても改訂は自動同期ではありません。

総合解説：規格問題では「ISO版」と「JIS版」を同一視せず、規格番号と版年を確認することが重要です。特に2026年はISO/IEC 27000が改訂された一方、JIS Q 27000は2019版が有効です。

対象：2026年度 / 基準日 2026-09-05

0097 規格・ガイドライン > ISO/IEC 27000・JIS Q 27000規格群 ｜ 難易度：標準

ISMSの継続的改善に関する説明として、最も適切なものはどれか。

ア：認証を一度取得すれば、以後はリスクアセスメントを行う必要はない。

イ：改善は重大事故が発生した場合だけ実施し、平常時の評価結果は利用しない。

ウ：リスクや組織の状況の変化を踏まえ、ISMSの適切性・十分性・有効性を継続的に改善する。

エ：ISMSでは技術的対策だけを改善対象とし、組織的・人的対策は対象外とする。

答え・解説 正答：ウ

ア：認証取得後も環境やリスクは変化するため、継続的な評価が必要です。

イ：内部監査やレビュー等の結果も改善に利用します。

ウ：JIS Q 27001はISMSの維持と継続的改善を要求事項として扱います。

エ：ISMSは組織的・人的・物理的・技術的な観点を含みます。

総合解説：ISMSは一回限りのセキュリティ対策プロジェクトではなく、リスクアセスメント、運用、評価、是正、改善を継続するマネジメントシステムです。

対象：2026年度 / 基準日 2026-09-05

0098 規格・ガイドライン > ISO/IEC 27000・JIS Q 27000規格群 ｜ 難易度：標準

組織がJIS Q 27001とJIS Q 27002を利用する方法として、最も適切なものはどれか。

ア：認証要求事項はJIS Q 27002だけを確認し、JIS Q 27001は参照しない。

イ：情報セキュリティガバナンスの原則だけで、具体的な管理策を一律に決定する。

ウ：PCI DSSを採用すれば、組織のISMS要求事項をすべて満たしたことになる。

エ：認証を目指すISMSの要求事項はJIS Q 27001で確認し、具体的な管理策の実施方法はJIS Q 27002を参考にする。

答え・解説 正答：エ

ア：27002は要求事項規格ではありません。

イ：ガバナンスの原則だけでは個々の管理策の具体化は不十分です。

ウ：PCI DSSはカード情報保護に特化した業界基準で、ISMS要求事項の代替ではありません。

エ：27001と27002の役割を組み合わせるのが適切です。

総合解説：規格の名称を覚えるだけでなく、「何を確認するためにどの規格を使うか」を判断できることが重要です。

対象：2026年度 / 基準日 2026-09-05

0099 規格・ガイドライン > ISO/IEC 27000・JIS Q 27000規格群 ｜ 難易度：応用

クラウド利用を拡大した企業が、既存の情報セキュリティ管理策を見直すことになった。最も適切な対応はどれか。

ア：自社のクラウド利用形態や法令上の義務を踏まえ、参照基準の管理策を具体化し、必要に応じて追加する。

イ：他社の認証取得時の管理策一覧をそのままコピーし、自社のリスク評価は省略する。

ウ：規格に例示がない独自リスクは、管理策の検討対象から除外する。

エ：監査で比較しやすくするため、事業特性にかかわらず全社で他社と同一の管理策に固定する。

答え・解説 正答：ア

ア：包括的な基準は組織固有の事情に合わせて具体化する必要があります。

イ：他社と自社では資産・脅威・法令・事業特性が異なるため、そのままの転用は不適切です。

ウ：独自リスクもリスクアセスメントで扱い、必要な対策を追加します。

エ：標準化と組織固有リスクへの適合を両立させる必要があります。

総合解説：規格準拠は「ひな形をそのまま採用すること」ではありません。リスクと組織の状況を根拠として、管理策を選択・具体化し、説明可能な状態にすることが重要です。

対象：2026年度 / 基準日 2026-09-05

0100 規格・ガイドライン > ISO/IEC 27000・JIS Q 27000規格群 ｜ 難易度：応用

経営層・ISMS担当・管理策設計担当がそれぞれ規格を参照する場合の使い分けとして、最も適切なものはどれか。

ア：すべての課題をJIS Q 27000の用語定義だけで解決する。

イ：経営層にはJIS Q 27014のガバナンス観点、ISMS担当にはJIS Q 27001の要求事項、管理策設計にはJIS Q 27002を使い分ける。

ウ：技術部門だけがJIS Q 27014を使い、経営層は情報セキュリティガバナンスに関与しない。

エ：管理策の設計にはJIS Q 27001を使わず、法令やリスクも考慮しない。

答え・解説 正答：イ

ア：27000は全体像や概念理解に役立ちますが、それだけでISMS要求事項や管理策実装を代替できません。

イ：各規格の役割に沿って使い分けるのが適切です。

ウ：情報セキュリティガバナンスは経営・統治の課題であり、経営層の関与が重要です。

エ：管理策はISMS要求事項、法令、リスク等と整合させて設計します。

総合解説：ISO/IEC 27000・JIS Q 27000ファミリは相互補完的です。受験上は規格番号と役割を対応付けて理解すると、事例問題でも判断しやすくなります。

対象：2026年度 / 基準日 2026-09-05

0101 規格・ガイドライン > サイバーセキュリティ経営ガイドライン・内部不正防止 ｜ 難易度：基礎

サイバーセキュリティ経営ガイドラインの考え方として、最も適切なものはどれか。

ア：サイバーセキュリティはIT部門だけの技術課題なので、経営者は関与しない。

イ：事故発生後だけ経営者が関与し、平時の投資判断は担当者へ全面委任する。

ウ：経営者がリーダーシップを取り、サイバーセキュリティ対策を経営課題として推進する。

エ：経営者は対策状況を把握せず、外部委託先に責任をすべて移転する。

答え・解説 正答：ウ

ア：サイバーリスクは事業継続・信用・財務に影響する経営課題です。

イ：平時の資源配分や体制整備も経営判断です。

ウ：経済産業省のガイドラインは、経営者のリーダーシップを3原則の一つとして示しています。

エ：外部委託しても自社の経営上の責任が消えるわけではありません。

総合解説：サイバーセキュリティを単なるシステム部門の問題として扱うと、必要な予算・人員・優先順位付けが不十分になりやすいため、経営者の関与が重要です。

対象：2026年度 / 基準日 2026-09-05

0102 規格・ガイドライン > サイバーセキュリティ経営ガイドライン・内部不正防止 ｜ 難易度：基礎

サプライチェーンのサイバーセキュリティに関する経営者の対応として、最も適切なものはどれか。

ア：委託先のシステムで発生した事故は自社に影響しないため、評価対象外とする。

イ：契約を締結すれば、委託先のセキュリティ実施状況を確認する必要はない。

ウ：小規模な取引先は攻撃対象にならないので、セキュリティ要求を設けない。

エ：自社だけでなく、委託先や取引先を含むサプライチェーン全体のリスクにも目配りする。

答え・解説 正答：エ

ア：委託先の事故が自社データや業務停止に波及することがあります。

イ：契約後も必要な監督・確認が重要です。

ウ：規模だけで攻撃リスクがなくなるわけではありません。

エ：経営ガイドラインはサプライチェーン全体への目配りを原則として示します。

総合解説：サプライチェーンリスクでは、契約前の評価、要求事項の明確化、実施状況の確認、インシデント時の連携まで一連で考えます。

対象：2026年度 / 基準日 2026-09-05

0103 規格・ガイドライン > サイバーセキュリティ経営ガイドライン・内部不正防止 ｜ 難易度：基礎

サイバーセキュリティに関する社内外コミュニケーションとして、最も適切なものはどれか。

ア：平時・緊急時の双方で、社内外の関係者と適切にコミュニケーションできる体制を整える。

イ：緊急時は混乱防止のため、経営層にも情報を共有しない。

ウ：事故情報は技術担当者だけで保持し、法務・広報・取引先との連携は行わない。

エ：平時の連絡体制は不要で、事故が起きてから担当者を決める。

答え・解説 正答：ア

ア：経営ガイドラインの3原則には、平時・緊急時の積極的な社内外コミュニケーションが含まれます。

イ：経営判断に必要な情報共有を遮断するのは不適切です。

ウ：インシデントは技術だけでなく法務・広報・顧客対応等を伴います。

エ：事前に役割と連絡経路を整えることが重要です。

総合解説：重大インシデントでは、技術復旧だけでなく、経営判断、説明、届出、取引先連携が必要になるため、平時からコミュニケーション設計を行います。

対象：2026年度 / 基準日 2026-09-05

0104 規格・ガイドライン > サイバーセキュリティ経営ガイドライン・内部不正防止 ｜ 難易度：標準

経営者がCISO等へサイバーセキュリティ対策を指示する際の対応として、最も適切なものはどれか。

ア：担当者の善意に依存し、予算や権限を付与しない。

イ：事業リスクに基づいて必要な人材・予算を確保し、責任者と権限を明確にする。

ウ：全システムに同額の予算を配り、重要度やリスクは考慮しない。

エ：責任者を複数置くが、最終意思決定者は定めない。

答え・解説 正答：イ

ア：担当者任せでは組織的な実行力が不足します。

イ：実効的な対策には、経営判断による資源配分と責任・権限の明確化が必要です。

ウ：資源配分は事業影響やリスクに応じて優先順位付けします。

エ：責任の所在を曖昧にすると意思決定が遅れます。

総合解説：CISO等に責任だけを負わせるのではなく、経営者が必要な権限・資源を与え、経営リスクと整合した対策を指示・監督することが重要です。

対象：2026年度 / 基準日 2026-09-05

0105 規格・ガイドライン > サイバーセキュリティ経営ガイドライン・内部不正防止 ｜ 難易度：標準

内部不正の発生要因を説明する「不正のトライアングル」の考え方として、最も適切なものはどれか。

ア：内部不正は技術的脆弱性だけで決まり、職場環境や権限設計は関係しない。

イ：内部不正は退職者だけが行うため、在職者への対策は不要である。

ウ：内部不正の発生要因を、機会・動機・正当化の観点から捉えて対策する。

エ：内部不正は故意犯だけを対象とし、誤操作やルール不備は全て同じ対策で扱う。

答え・解説 正答：ウ

ア：権限過多や監視不足は「機会」を増やします。

イ：在職者も内部不正の主体になり得ます。

ウ：不正のトライアングルは、機会・動機・正当化の三要素で不正リスクを考える代表的な枠組みです。

エ：故意の内部不正と過失は区別しつつ、管理策を組み合わせます。

総合解説：内部不正防止では、技術対策だけでなく、権限管理、職場環境、教育、監視、退職時管理など複数の観点から不正の機会等を低減します。

対象：2026年度 / 基準日 2026-09-05

0106 規格・ガイドライン > サイバーセキュリティ経営ガイドライン・内部不正防止 ｜ 難易度：標準

内部不正の機会を低減するアクセス権管理として、最も適切なものはどれか。

ア：利便性を優先して全従業員に共有管理者IDを配布する。

イ：異動後も過去部門のアクセス権を残し、必要時にだけ利用者へ注意する。

ウ：ログ取得を止めれば従業員の不満が減るので、重要システムでも監視しない。

エ：業務上必要な範囲にアクセス権を限定し、定期的に見直す。

答え・解説 正答：エ

ア：共有管理者IDは責任追跡性を低下させます。

イ：不要権限を残すと内部不正や誤操作の機会が増えます。

ウ：重要システムでは適切なログ取得・監視が必要です。

エ：最小権限と定期的なアクセス権レビューは、不正の機会を減らす基本策です。

総合解説：内部不正対策では、誰が何にアクセスできるかを必要最小限にし、異動・退職等のライフサイクルに合わせて見直すことが重要です。

対象：2026年度 / 基準日 2026-09-05

0107 規格・ガイドライン > サイバーセキュリティ経営ガイドライン・内部不正防止 ｜ 難易度：標準

退職・異動時の内部不正防止策として、最も適切なものはどれか。

ア：退職・異動の時点に合わせてアクセス権を速やかに変更・削除し、機器や媒体を回収する。

イ：退職後1か月程度は引継ぎのため全権限を残しておく。

ウ：退職者が誓約書を提出した場合は、アカウント削除や機器回収を省略する。

エ：人事部門だけで退職処理を完了し、IT部門や資産管理部門には連絡しない。

答え・解説 正答：ア

ア：退職・異動時は不要権限を速やかに削除・変更し、貸与物や媒体を回収します。

イ：退職後の不要な権限残存は高リスクです。

ウ：誓約書は重要ですが、技術的・物理的な管理の代替ではありません。

エ：部門間で連携し、アクセス・資産・秘密保持等を一体で処理します。

総合解説：雇用の流動化に伴い、退職者・異動者のアクセス権や秘密情報の持出しリスクを管理することが内部不正防止で重要です。

対象：2026年度 / 基準日 2026-09-05

0108 規格・ガイドライン > サイバーセキュリティ経営ガイドライン・内部不正防止 ｜ 難易度：標準

内部不正対策として従業員の操作ログを監視する場合の考え方として、最も適切なものはどれか。

ア：内部不正対策なら、目的を示さず従業員の私的通信を無制限に収集してよい。

イ：監視の目的・範囲・取扱ルールを明確にし、必要性に応じたログ取得を行う。

ウ：監視によるプライバシー懸念を避けるため、重要操作のログも一切取得しない。

エ：ログは取得するだけでよく、アクセス権や保管期間の管理は不要である。

答え・解説 正答：イ

ア：必要性・相当性を無視した無制限監視は適切ではありません。

イ：内部不正対策では監視の有効性と個人情報・プライバシーへの配慮を両立させます。

ウ：重要操作の追跡可能性は不正抑止・検知に有効です。

エ：ログ自体も機密情報になり得るため、アクセス・保管・改ざん防止が必要です。

総合解説：内部不正防止ガイドライン第5版は、セキュリティ技術の活用と個人情報への配慮をともに重視しています。

対象：2026年度 / 基準日 2026-09-05

0109 規格・ガイドライン > サイバーセキュリティ経営ガイドライン・内部不正防止 ｜ 難易度：応用

テレワークで秘密情報を扱う従業員が増えた。内部不正防止の観点から最も適切な対応はどれか。

ア：在宅勤務では本人の自宅なので、機密情報の持出しや画面ののぞき見対策は不要である。

イ：VPNを使っていれば、端末の紛失やローカル保存のリスクは考慮しなくてよい。

ウ：社外での秘密情報取扱いルール、端末・媒体管理、アクセス制御を整備し、遵守状況を確認する。

エ：テレワークでは監視が難しいため、全従業員へ管理者権限を付与して自己管理させる。

答え・解説 正答：ウ

ア：自宅でも第三者閲覧や誤送信等のリスクがあります。

イ：通信保護だけで端末・保存データのリスクは消えません。

ウ：テレワークでは組織外で秘密情報を扱うため、技術・人的・物理的管理を組み合わせます。

エ：管理者権限の拡大はむしろ不正・誤操作リスクを高めます。

総合解説：第5版ではテレワーク等の新しい働き方を踏まえ、組織外で秘密情報を扱う場合のリスク低減策が強化されています。

対象：2026年度 / 基準日 2026-09-05

0110 規格・ガイドライン > サイバーセキュリティ経営ガイドライン・内部不正防止 ｜ 難易度：応用

内部不正防止ガイドラインのチェックシートを利用した自己点検後の対応として、最も適切なものはどれか。

ア：ガイドラインの全項目を確認せず、事故が起きた項目だけ対策する。

イ：チェックシートの点数を上げること自体を目的とし、実際の運用状況は確認しない。

ウ：内部不正は完全には防げないので、自己点検や改善を行わない。

エ：チェックシート等で自組織の対策状況を把握し、弱点を特定して改善計画へつなげる。

答え・解説 正答：エ

ア：内部不正対策は複数の観点で総合的に見る必要があります。

イ：形式的な点数ではなく、対策が実際に機能しているかを確認します。

ウ：完全防止が困難でも、発生可能性・影響を低減し、早期検知する価値があります。

エ：ガイドラインは対策状況を自己点検し、弱点を改善するためにも利用できます。

総合解説：内部不正対策は一度導入して終わりではなく、組織・働き方・技術の変化に応じて自己点検し、継続的に改善します。

対象：2026年度 / 基準日 2026-09-05

0111 規格・ガイドライン > CSF・PCI DSS・政府／中小企業向け基準等 ｜ 難易度：基礎

NIST Cybersecurity Framework（CSF）2.0の機能として、最も適切なものはどれか。

ア：CSF 2.0は、GOVERN・IDENTIFY・PROTECT・DETECT・RESPOND・RECOVERの六つの機能で整理される。

イ：CSF 2.0は、IDENTIFY・PROTECT・DETECTの三機能だけで構成される。

ウ：CSF 2.0ではGOVERNが廃止され、RECOVERに統合された。

エ：CSF 2.0はカード会員データの暗号化要件だけを規定する。

答え・解説 正答：ア

ア：CSF 2.0ではGOVERNを含む六つの機能でサイバーセキュリティ成果を整理します。

イ：三機能だけではありません。RESPONDやRECOVERなども含まれます。

ウ：GOVERNは廃止ではなく、CSF 2.0で独立した機能として明確化されました。

エ：カード会員データ保護に特化した基準はPCI DSSであり、CSFの説明ではありません。

総合解説：CSF 2.0では、統治から識別・防御・検知・対応・復旧までを一体のサイバーリスク管理として捉えます。

対象：2026年度 / 基準日 2026-09-05

0112 規格・ガイドライン > CSF・PCI DSS・政府／中小企業向け基準等 ｜ 難易度：基礎

NIST CSF 2.0におけるProfileの利用方法として、最も適切なものはどれか。

ア：Profileは脆弱性スキャンの実行回数だけを示す指標である。

イ：現在のサイバーセキュリティ成果と目標状態をProfileで比較し、改善の優先順位付けに使う。

ウ：Profileを作成すれば、組織固有のリスクアセスメントは不要になる。

エ：ProfileはPCI DSSの認証証明書と同じものである。

答え・解説 正答：イ

ア：Profileは単一の技術指標ではありません。

イ：Current ProfileとTarget Profileを比較することで、現状と目標の差を把握し、改善に活用できます。

ウ：Profileはリスク管理を支援するもので、リスクアセスメントの代替ではありません。

エ：PCI DSSの認証証明書ではありません。

総合解説：CSFのProfileは、組織固有の優先事項やリスクを反映して成果を整理するための手段です。単なるチェックリストの点数ではありません。

対象：2026年度 / 基準日 2026-09-05

0113 規格・ガイドライン > CSF・PCI DSS・政府／中小企業向け基準等 ｜ 難易度：基礎

NIST CSF 2.0でGOVERN機能が重視される理由として、最も適切なものはどれか。

ア：GOVERNは、マルウェアのパターンファイル更新だけを扱う。

イ：GOVERNは、事故発生後のデータ復元だけを扱う。

ウ：GOVERNは、リスク管理戦略・役割・方針・法的要求などを組織全体の統治と結び付ける。

エ：GOVERNは、ネットワーク機器の物理配置だけを扱う。

答え・解説 正答：ウ

ア：マルウェア対策は主にPROTECTやDETECTなどに関係します。

イ：データ復元は主にRECOVERの領域です。

ウ：GOVERNは、サイバーセキュリティを企業リスク管理、役割・責任、方針、法的要求などと結び付けます。

エ：物理配置だけに限定された機能ではありません。

総合解説：CSF 2.0ではサイバーセキュリティを技術部門だけの課題とせず、組織の統治と結び付ける点が強調されています。

対象：2026年度 / 基準日 2026-09-05

0114 規格・ガイドライン > CSF・PCI DSS・政府／中小企業向け基準等 ｜ 難易度：標準

PCI DSSの適用を検討する場面として、最も適切なものはどれか。

ア：PCI DSSは、全ての個人情報を扱う日本企業に法律上自動適用される。

イ：PCI DSSは、医療情報だけを保護するための政府規格である。

ウ：PCI DSSは、カード決済を扱わないシステムにも必ず同一範囲で適用する。

エ：カード会員データを保存・処理・伝送する環境に関係する組織は、PCI DSSの適用範囲を確認する。

答え・解説 正答：エ

ア：個人情報保護法とは別の枠組みで、全ての個人情報取扱事業者へ法律として自動適用されるものではありません。

イ：医療情報専用の政府規格ではありません。

ウ：適用範囲はカード会員データ環境との関係を踏まえて判断します。

エ：PCI DSSは決済カードデータの保護を目的とする業界セキュリティ基準です。

総合解説：PCI DSSでは、カード会員データ環境を適切に特定し、その範囲へ要求事項を適用する考え方が重要です。

対象：2026年度 / 基準日 2026-09-05

0115 規格・ガイドライン > CSF・PCI DSS・政府／中小企業向け基準等 ｜ 難易度：標準

PCI DSS v4.0.1の位置付けとして、最も適切なものはどれか。

ア：PCI DSS v4.0.1はv4.0の限定改訂で、要件の追加・削除ではなく明確化や修正が中心である。

イ：v4.0.1ではPCI DSSの全要件が廃止され、NIST CSFに一本化された。

ウ：v4.0.1はカード会員データ保護をやめ、個人情報一般だけを対象に変更した。

エ：v4.0.1で新しい要件が多数追加され、v4.0との互換性はない。

答え・解説 正答：ア

ア：PCI SSCはv4.0.1を限定改訂と位置付け、新規・削除要件はないと説明しています。

イ：PCI DSSは廃止されていません。

ウ：対象目的が個人情報一般へ変更されたわけではありません。

エ：v4.0.1は主に明確化や誤記修正などを行った版です。

総合解説：規格の版番号だけから大改訂と推測せず、公式の変更概要を確認することが重要です。

対象：2026年度 / 基準日 2026-09-05

0116 規格・ガイドライン > CSF・PCI DSS・政府／中小企業向け基準等 ｜ 難易度：標準

政府機関等のサイバーセキュリティ対策のための統一基準群の利用方法として、最も適切なものはどれか。

ア：民間のECサイトだけを対象とするカード決済規格として利用する。

イ：政府機関等が組織の規程や実施手順、情報システムのセキュリティ要件を整備する際の基礎として利用する。

ウ：政府機関では統一基準だけを読めばよく、個別マニュアルや組織内規程は不要である。

エ：統一基準群は技術製品の性能ランキングだけを示す。

答え・解説 正答：イ

ア：カード決済に特化したPCI DSSとは目的が異なります。

イ：統一基準群は政府機関等のサイバーセキュリティ対策を統一的に整備するための基準群です。

ウ：組織内の具体的な規程や手順へ落とし込むことが必要です。

エ：製品ランキングを目的とする資料ではありません。

総合解説：政府統一基準群は、政府機関等が具体的なルールや情報システムのセキュリティ要件を整備する際の基盤として利用されます。

対象：2026年度 / 基準日 2026-09-05

0117 規格・ガイドライン > CSF・PCI DSS・政府／中小企業向け基準等 ｜ 難易度：標準

IPA「中小企業の情報セキュリティ対策ガイドライン 第4.0版」の説明として、最も適切なものはどれか。

ア：上場企業だけが利用でき、中小企業や個人事業主は対象外である。

イ：技術者向けの暗号アルゴリズム仕様書なので、経営者は利用しない。

ウ：個人事業主や小規模事業者を含む中小企業等が、経営者の認識と実践手順の両面から対策を進めるために利用する。

エ：事故後の法的責任だけを解説し、予防対策は扱わない。

答え・解説 正答：ウ

ア：対象を上場企業に限定していません。

イ：経営者が認識・実施すべき指針も含みます。

ウ：第4.0版は個人事業主・小規模事業者を含む中小企業等の利用を想定し、経営者編と実践編で構成されています。

エ：予防や日常運用、インシデント対応など幅広い対策を扱います。

総合解説：中小企業向けガイドラインは、限られた経営資源の中でも段階的に情報セキュリティ対策を進めるための実践的な資料です。

対象：2026年度 / 基準日 2026-09-05

0118 規格・ガイドライン > CSF・PCI DSS・政府／中小企業向け基準等 ｜ 難易度：標準

カード決済を行う企業がCSFとPCI DSSを利用する方法として、最も適切なものはどれか。

ア：PCI DSSを採用したので、全社のサイバーガバナンスや非決済システムのリスク管理は不要とする。

イ：CSFを採用したので、カード業界で求められる具体的なPCI DSS対応は確認しない。

ウ：二つの枠組みは目的が異なるため、同じ組織で併用してはいけない。

エ：全社的なサイバーリスク管理にはCSFを活用し、カード会員データ環境にはPCI DSSの要求事項も適用する。

答え・解説 正答：エ

ア：PCI DSSはカード環境に重点があり、全社リスク管理の全てを代替するとは限りません。

イ：CSFを採用しても個別の業界要求を自動的に満たすわけではありません。

ウ：目的が異なる枠組みは、必要に応じて併用できます。

エ：CSFとPCI DSSは目的や粒度が異なるため、組織の状況に応じて補完的に利用できます。

総合解説：規格やフレームワークは一つを選べば他が不要になるとは限りません。適用対象と要求事項を整理して組み合わせます。

対象：2026年度 / 基準日 2026-09-05

0119 規格・ガイドライン > CSF・PCI DSS・政府／中小企業向け基準等 ｜ 難易度：応用

中小企業がIPAの情報セキュリティ自社診断を実施した。次の対応として、最も適切なものはどれか。

ア：自社診断で弱い対策を把握し、重要資産や脅威を踏まえて改善の優先順位を決める。

イ：診断の点数が前年より高ければ、重大な未対策脆弱性があっても放置する。

ウ：他社平均より高い点数なら、バックアップやインシデント対応計画は不要と判断する。

エ：自己診断は認証審査と同じなので、診断後は外部要求の確認を省略する。

答え・解説 正答：ア

ア：自己診断は現状把握と改善の入口として有効ですが、具体的なリスクを踏まえて優先順位を付けることが重要です。

イ：総合点だけでは重大な個別リスクを見落とす可能性があります。

ウ：他社平均は自社の重要資産や業務継続要求を代替しません。

エ：自己診断と認証審査・法的適合性評価は同一ではありません。

総合解説：IPAの中小企業向けガイドラインには自社診断ツールが用意されています。点数そのものより、弱点を発見し改善につなげることが重要です。

対象：2026年度 / 基準日 2026-09-05

0120 規格・ガイドライン > CSF・PCI DSS・政府／中小企業向け基準等 ｜ 難易度：応用

政府機関がカード決済を含むオンラインサービスを運用している。複数の基準・フレームワークの扱いとして、最も適切なものはどれか。

ア：政府機関ならPCI DSSだけで全てのセキュリティ要求を満たす。

イ：政府統一基準群を基礎にし、カード決済を扱う部分ではPCI DSSも確認し、全体リスク管理にはCSF等を参考にする。

ウ：CSFは米国発のため、日本の組織が参考にしてはいけない。

エ：中小企業向けガイドラインを使う場合、法令や取引先要求は確認しなくてよい。

答え・解説 正答：イ

ア：PCI DSSは決済カードデータに重点があり、政府統一基準群全体の代替ではありません。

イ：複数の規格・基準は適用対象が異なるため、組織の属性と業務に応じて組み合わせます。

ウ：NIST CSFは国や業種を限定せず活用できる汎用的フレームワークです。

エ：ガイドラインは法令や契約要求の代替ではありません。

総合解説：実務では、一つの規格ですべてを満たすと考えず、法令、業界基準、政府基準、一般フレームワークの適用範囲を整理します。

対象：2026年度 / 基準日 2026-09-05

0121 監査・内部統制 > システム監査・情報セキュリティ監査 ｜ 難易度：基礎

システム監査の目的として、最も適切なものはどれか。

ア：監査人が被監査部門の日常業務を代行し、統制の責任を引き受ける。

イ：監査は障害が発生したときだけ実施し、平時の評価は行わない。

ウ：情報システムの利活用に係る取組を独立・客観的な立場から検証・評価し、改善や信頼性向上に役立てる。

エ：システム監査は会計データの金額照合だけを目的とする。

答え・解説 正答：ウ

ア：統制の整備・運用責任は被監査側にあり、監査人が代行すると独立性を損ないます。

イ：計画的な監査も行われ、障害発生時だけに限定されません。

ウ：システム監査は、情報システムの利活用に関するリスクや管理の状況を独立・客観的に検証・評価する活動です。

エ：対象は会計数値だけでなく、情報システムの利活用を広く含みます。

総合解説：監査は運用の代行ではなく、独立した立場から証拠に基づいて検証・評価し、改善と信頼性向上に寄与するものです。

対象：2026年度 / 基準日 2026-09-05

0122 監査・内部統制 > システム監査・情報セキュリティ監査 ｜ 難易度：基礎

システム監査における独立性・客観性の確保として、最も適切なものはどれか。

ア：監査対象の責任者自身が監査結論を決める方が、業務を最も知っているので常に適切である。

イ：監査人は経営者が期待する結論に合わせて証拠を選ぶ。

ウ：監査の独立性は外部監査だけに必要で、内部監査では不要である。

エ：監査対象の業務について自ら意思決定・実施した担当者は、その同じ業務の監査を避けるなど独立性を確保する。

答え・解説 正答：エ

ア：自己監査は客観性に疑義が生じやすく、役割分離などが必要です。

イ：結論ありきで証拠を選ぶと客観性を失います。

ウ：内部監査でも、組織内で可能な範囲の独立性を確保する必要があります。

エ：監査対象から独立した立場と客観性を保つことが、監査品質の基礎です。

総合解説：システム監査基準は、精神的独立性だけでなく、監査対象から独立していると外部から見える外観的独立性にも配慮するよう求めています。

対象：2026年度 / 基準日 2026-09-05

0123 監査・内部統制 > システム監査・情報セキュリティ監査 ｜ 難易度：基礎

システム監査における監査証拠の扱いとして、最も適切なものはどれか。

ア：監査結論を裏付けるため、十分かつ適切な監査証拠を入手し評価する。

イ：担当者の口頭説明だけを必ず最終証拠とし、記録との照合は行わない。

ウ：監査人の経験が豊富なら、監査証拠を残さず結論を出してよい。

エ：監査対象が提出を拒んだ資料は、存在しないものとして扱う。

答え・解説 正答：ア

ア：監査結論は監査証拠に基づく必要があり、その十分性・適切性を評価します。

イ：口頭説明も情報源になり得ますが、必要に応じて記録や観察などで裏付けます。

ウ：経験は監査証拠の代替にはなりません。

エ：資料入手の制約自体が監査範囲や結論に影響する可能性があります。

総合解説：監査では、結論の根拠を第三者が追跡できるよう、入手した証拠と評価過程を適切に記録することが重要です。

対象：2026年度 / 基準日 2026-09-05

0124 監査・内部統制 > システム監査・情報セキュリティ監査 ｜ 難易度：標準

監査調書の作成・保管に関する説明として、最も適切なものはどれか。

ア：最終報告書があれば、監査手続や証拠の記録は全て破棄してよい。

イ：実施した手続、入手した証拠、判断過程を監査調書として記録し、適切に保管する。

ウ：監査調書には監査人の結論だけを書き、証拠との対応関係は記録しない。

エ：監査調書は被監査部門が自由に書き換えられる共有ファイルだけで管理する。

答え・解説 正答：イ

ア：最終報告書だけでは個々の手続や証拠を十分に再現できません。

イ：監査調書は、実施した監査手続・証拠・判断過程を追跡できるように作成し、適切に保管します。

ウ：結論と証拠の対応関係を残すことが重要です。

エ：監査調書自体の機密性・完全性も保護する必要があります。

総合解説：監査調書は、監査品質の確認、後日の説明、フォローアップなどの基盤となります。

対象：2026年度 / 基準日 2026-09-05

0125 監査・内部統制 > システム監査・情報セキュリティ監査 ｜ 難易度：標準

システム監査の計画を策定する際の考え方として、最も適切なものはどれか。

ア：全部門を毎年同じ時間だけ監査し、リスクの高低は考慮しない。

イ：監査開始後に目的を決めればよいので、事前の範囲設定は不要である。

ウ：重要なリスクや監査目的を踏まえて、対象範囲・時期・手続・必要資源を計画する。

エ：監査対象から要望された項目だけを監査し、組織の重要リスクは考慮しない。

答え・解説 正答：ウ

ア：リスクを考慮しない一律配分では重要領域への監査が不足する可能性があります。

イ：目的・範囲を事前に明確にしないと、必要な証拠収集や結論形成が困難になります。

ウ：監査資源は有限なので、リスクや重要性を踏まえた計画が必要です。

エ：被監査側の要望だけでなく、監査目的や重要リスクとの整合が必要です。

総合解説：リスクベースの監査では、重要なリスク領域へ監査資源を重点配分し、監査目的に沿って手続を設計します。

対象：2026年度 / 基準日 2026-09-05

0126 監査・内部統制 > システム監査・情報セキュリティ監査 ｜ 難易度：標準

情報セキュリティ監査で用いる判断の尺度に関する説明として、最も適切なものはどれか。

ア：監査人の個人的な好みだけを判断尺度にする。

イ：判断尺度は監査終了後に結論に合うよう決める。

ウ：情報セキュリティ監査では、監査対象やリスクに関係なく必ず全管理策を同じ深さで監査する。

エ：監査目的に応じて判断の尺度を明確にし、必要に応じて情報セキュリティ管理基準等を具体化して用いる。

答え・解説 正答：エ

ア：個人の好みでは客観性を確保できません。

イ：結論に合わせた後付けの基準は監査の信頼性を損ないます。

ウ：監査目的やリスクに応じて対象範囲や監査深度を設定します。

エ：情報セキュリティ監査では、何をもって適切と判断するかを事前に明確化することが重要です。

総合解説：情報セキュリティ管理基準は代表的な判断尺度ですが、組織や監査目的に応じて個別管理基準へ具体化して用いることがあります。

対象：2026年度 / 基準日 2026-09-05

0127 監査・内部統制 > システム監査・情報セキュリティ監査 ｜ 難易度：標準

システム監査と情報セキュリティ監査の関係として、最も適切なものはどれか。

ア：システム監査は情報システムの利活用を広く対象とし、情報セキュリティ監査は情報セキュリティの適切性を中心に検証・評価する。

イ：両者は制度上完全に同一で、対象範囲も目的も常に同じである。

ウ：情報セキュリティ監査は財務諸表の金額だけを監査する。

エ：システム監査はセキュリティを一切対象にできない。

答え・解説 正答：ア

ア：両者は関連しますが、監査の焦点や用いる基準に違いがあります。

イ：完全に同一の制度ではありません。

ウ：情報セキュリティ監査はセキュリティマネジメントや管理策を中心に扱います。

エ：システム監査でもセキュリティは重要な評価対象になり得ます。

総合解説：名称が似ていても、監査の目的、対象、判断尺度を区別して理解することが重要です。

対象：2026年度 / 基準日 2026-09-05

0128 監査・内部統制 > システム監査・情報セキュリティ監査 ｜ 難易度：標準

監査報告後のフォローアップとして、最も適切なものはどれか。

ア：監査報告後は監査部門の仕事は終了なので、重大指摘でも改善状況を確認しない。

イ：監査結果を事実と根拠に基づいて報告し、改善計画の実施状況を必要に応じてフォローアップする。

ウ：指摘を受け入れやすくするため、根拠を示さず結論だけ通知する。

エ：改善提案の実施責任は監査人が負い、被監査部門の責任者は関与しない。

答え・解説 正答：イ

ア：重大指摘では対応状況の確認が重要です。

イ：監査報告は根拠を明確にし、必要に応じて改善計画の進捗や有効性を確認します。

ウ：根拠のない結論は監査の納得性・信頼性を損ないます。

エ：改善の実行責任は管理側にあり、監査人は独立性を保ってフォローアップします。

総合解説：監査は指摘を出して終わりではなく、改善が適切に実施されているかを確認することで組織の改善につながります。

対象：2026年度 / 基準日 2026-09-05

0129 監査・内部統制 > システム監査・情報セキュリティ監査 ｜ 難易度：応用

アクセス管理手順の有効性を内部監査する。監査の独立性を最も確保しやすい方法はどれか。

ア：アクセス管理手順を設計した本人が、自分の設計を唯一の監査人として評価する。

イ：被監査部門長が監査証拠を選別し、監査人は提示された資料だけで必ず適合とする。

ウ：アクセス管理手順を設計・承認した担当者とは別の監査担当者が、その運用の有効性を評価する。

エ：監査結論を事前に経営者から指定し、その結論に合う証拠だけを収集する。

答え・解説 正答：ウ

ア：自分の仕事を自分だけで監査すると自己レビューの脅威が高まります。

イ：被監査側に証拠選別を委ね切ると十分な監査ができません。

ウ：設計・実施と監査を分けることで、独立性と客観性を高められます。

エ：結論先行の監査は客観性を損ないます。

総合解説：内部監査でも、組織構造上可能な範囲で監査対象から独立し、監査人が自ら必要な証拠へアクセスできる体制が重要です。

対象：2026年度 / 基準日 2026-09-05

0130 監査・内部統制 > システム監査・情報セキュリティ監査 ｜ 難易度：応用

情報セキュリティ監査を受ける部門の対応として、最も適切なものはどれか。

ア：不都合なログは監査前に削除し、適合している記録だけを提示する。

イ：監査人へ口頭説明だけを行い、根拠資料の提示を拒否する。

ウ：指摘を受けても監査終了後に記録を廃棄し、改善計画は作成しない。

エ：要求された規程・記録を準備し、事実に基づいてインタビューへ回答し、指摘事項は改善計画へ反映する。

答え・解説 正答：エ

ア：証拠の隠蔽や削除は監査の信頼性を損ない、重大な問題です。

イ：説明だけでなく、必要な記録を提示できる状態にすることが重要です。

ウ：監査指摘は原因・リスクを評価して改善計画へ反映します。

エ：被監査部門は監査に協力し、必要な証拠を提示し、指摘を改善活動へつなげます。

総合解説：情報セキュリティマネジメント試験では、監査人の知識だけでなく、被監査部門として適切に監査へ対応する実務判断も重要です。

対象：2026年度 / 基準日 2026-09-05

0131 監査・内部統制 > 内部統制・職務分掌・統制活動 ｜ 難易度：基礎

内部統制の目的として、最も適切なものはどれか。

ア：業務の有効性・効率性、報告の信頼性、法令等の遵守、資産の保全の四つを目的とする。

イ：内部統制の目的は、利益を最大化することだけである。

ウ：内部統制は情報システムの稼働率だけを保証するための仕組みである。

エ：内部統制は従業員の不正を100%防止することだけを目的とする。

答え・解説 正答：ア

ア：日本の内部統制の基本的枠組みでは、この四つが内部統制の目的として示されています。

イ：利益最大化だけが目的ではありません。

ウ：ITは内部統制に関係しますが、目的はシステム稼働率だけではありません。

エ：内部統制は合理的な保証を目指すもので、あらゆる不正の完全防止だけを目的とするものではありません。

総合解説：内部統制は、経営目的を達成するため組織内の人々によって遂行されるプロセスであり、情報セキュリティや法令遵守も関係します。

対象：2026年度 / 基準日 2026-09-05

0132 監査・内部統制 > 内部統制・職務分掌・統制活動 ｜ 難易度：基礎

内部統制の基本的要素として、最も適切なものはどれか。

ア：計画、調達、開発、テスト、運用、廃棄の六つだけで構成される。

イ：統制環境、リスクの評価と対応、統制活動、情報と伝達、モニタリング、ITへの対応の六つで構成される。

ウ：機密性、完全性、可用性の三つだけで構成される。

エ：予防、検知、是正の三つだけで構成される。

答え・解説 正答：イ

ア：これはシステムライフサイクルに近い区分で、内部統制の基本的要素ではありません。

イ：金融庁・企業会計審議会の内部統制の基本的枠組みでは、この六つの基本的要素が示されています。

ウ：CIAは情報セキュリティの代表的な性質です。

エ：予防・検知・是正は統制の性格を表す分類で、六つの基本的要素そのものではありません。

総合解説：内部統制の六つの基本的要素は相互に関連し、四つの目的を達成するために組織の業務へ組み込まれます。

対象：2026年度 / 基準日 2026-09-05

0133 監査・内部統制 > 内部統制・職務分掌・統制活動 ｜ 難易度：基礎

職務分掌の目的として、最も適切なものはどれか。

ア：効率を高めるため、支払申請・承認・振込・照合を一人に集中させる。

イ：職務分掌は担当者の専門性を下げるため、セキュリティ上は行わない。

ウ：申請・承認・実行・記録・照合などの重要な役割を適切に分け、不正や誤りを一人で完結しにくくする。

エ：職務分掌をすれば、ログや承認記録は不要になる。

答え・解説 正答：ウ

ア：一人で全工程を完結できると相互牽制が働きにくくなります。

イ：職務分掌は組織的な統制として有効です。

ウ：職務分掌は権限集中を避け、不正や誤りの予防・発見可能性を高める代表的な統制活動です。

エ：職務分掌とログ・承認記録は補完関係にあります。

総合解説：重要な処理では、一人の担当者が申請から承認、実行、記録、照合まで全て行えないよう役割を分けることが基本です。

対象：2026年度 / 基準日 2026-09-05

0134 監査・内部統制 > 内部統制・職務分掌・統制活動 ｜ 難易度：標準

特権アクセス権の付与プロセスに職務分掌を適用する方法として、最も適切なものはどれか。

ア：システム管理者が自分で申請・承認・設定・レビューを全て行う。

イ：利用者本人が管理者権限を自由に追加し、事後確認は行わない。

ウ：全従業員に同じ管理者権限を付与して、申請手続きを不要にする。

エ：利用部門が申請し、権限管理責任者が承認し、システム管理者が設定し、別途定期レビューを行う。

答え・解説 正答：エ

ア：権限の自己承認では相互牽制が働きません。

イ：利用者が自由に特権を追加できる状態は統制上問題です。

ウ：一律の過大権限は職務分掌だけでなく最小権限の考え方にも反します。

エ：申請、承認、設定、レビューを適切に分けることで、不正な権限付与を抑制・検知しやすくなります。

総合解説：アクセス権管理は技術設定だけでなく、申請・承認・設定・レビューという業務プロセス全体で統制する必要があります。

対象：2026年度 / 基準日 2026-09-05

0135 監査・内部統制 > 内部統制・職務分掌・統制活動 ｜ 難易度：標準

重要な業務処理における統制活動として、最も適切なものはどれか。

ア：重要な処理は権限者の承認を経て実行し、処理結果を独立した記録と照合する。

イ：承認済みなら処理結果の照合は不要とし、誤処理を確認しない。

ウ：照合だけ行えば、重要取引の事前承認は不要である。

エ：担当者が自分で作成したデータを同じ画面で見直すだけで、十分な独立照合とする。

答え・解説 正答：ア

ア：承認は不適切な処理の予防、照合は誤りや不正の検知に役立ち、組み合わせることで統制が強化されます。

イ：承認後にも処理ミスは起こり得るため、必要な照合は有効です。

ウ：重要な処理では事前承認も重要です。

エ：独立性のある照合ほど検知力が高まります。

総合解説：統制活動は一つの仕組みに依存せず、承認、照合、アクセス制御、職務分掌などを組み合わせることが重要です。

対象：2026年度 / 基準日 2026-09-05

0136 監査・内部統制 > 内部統制・職務分掌・統制活動 ｜ 難易度：標準

内部統制における「合理的な保証」の説明として、最も適切なものはどれか。

ア：内部統制を導入すれば、共謀や経営者による無効化も含め全ての不正を完全に防止できる。

イ：内部統制は目的達成を絶対に保証するものではなく、一定の限界を踏まえながら合理的な水準の保証を得ることを目指す。

ウ：一件でも誤りが発生したら、内部統制は全て無意味である。

エ：合理的保証とは、統制の費用を無視して可能な限り多くの対策を実施することである。

答え・解説 正答：イ

ア：全ての不正を完全に防止できるわけではありません。

イ：内部統制には人為的誤り、共謀、経営者による無効化などの限界があるため、絶対的な保証ではなく合理的な保証を目指します。

ウ：不備があれば原因と影響を評価し、改善します。

エ：合理性には費用対効果やリスクも含めた判断が必要です。

総合解説：内部統制を「事故が絶対に起きない仕組み」と誤解しないことが重要です。限界を認識し、リスクに応じて継続的に改善します。

対象：2026年度 / 基準日 2026-09-05

0137 監査・内部統制 > 内部統制・職務分掌・統制活動 ｜ 難易度：標準

IT全般統制とIT業務処理統制の関係として、最も適切なものはどれか。

ア：IT全般統制は個々の売上計算式だけを確認し、アクセス管理は対象外である。

イ：IT業務処理統制はデータセンターの入退室管理だけを対象とする。

ウ：アクセス管理や変更管理などIT基盤全体に関わる統制と、個々の業務処理で入力・処理・出力の適切性を確かめる統制を区別する。

エ：両者は全く同じ意味なので、区別する必要はない。

答え・解説 正答：ウ

ア：個別の計算式や入力チェックは業務処理統制の例です。

イ：入退室管理は基盤的な統制に関係します。

ウ：IT全般統制はシステム開発・変更、アクセス、運用などの基盤的統制、IT業務処理統制は個別業務処理の正確性・完全性などに関わります。

エ：両者は相互に関連しますが、概念上区別されます。

総合解説：業務処理統制が適切でも、基盤となるアクセス管理や変更管理が弱ければ、その統制の信頼性が損なわれる可能性があります。

対象：2026年度 / 基準日 2026-09-05

0138 監査・内部統制 > 内部統制・職務分掌・統制活動 ｜ 難易度：標準

内部統制におけるモニタリングの役割として、最も適切なものはどれか。

ア：統制を一度導入したら、その後の有効性確認は不要である。

イ：モニタリングでは不備を記録せず、担当者の記憶だけで管理する。

ウ：モニタリングは事故発生後の損害額計算だけを目的とする。

エ：統制が設計どおり機能しているかを継続的又は個別に評価し、不備を把握して是正につなげる。

答え・解説 正答：エ

ア：環境や業務は変化するため、導入後も評価が必要です。

イ：不備や対応状況を記録することは改善管理に重要です。

ウ：事故後だけでなく、平時の継続的評価や個別評価を含みます。

エ：モニタリングは内部統制の基本的要素であり、統制の有効性を継続的に確認し改善へつなげます。

総合解説：内部統制は固定された仕組みではなく、モニタリングを通じて不備や環境変化を捉え、必要な改善を行うプロセスです。

対象：2026年度 / 基準日 2026-09-05

0139 監査・内部統制 > 内部統制・職務分掌・統制活動 ｜ 難易度：応用

従業員が少なく、完全な職務分掌が難しい企業での内部統制として、最も適切なものはどれか。

ア：人員上の制約で完全な職務分掌が難しい場合、経営者レビューや詳細ログ確認などの代替統制を設ける。

イ：人数が少ないので職務分掌は不可能と判断し、相互牽制を一切設けない。

ウ：一人に全権限を集中し、監査ログも無効化する。

エ：担当者を信頼しているため、重要取引の承認や事後レビューを全て省略する。

答え・解説 正答：ア

ア：小規模組織でも、リスクに応じて経営者レビュー、例外確認、ログ確認などの代替統制を設けることができます。

イ：制約があっても統制をゼロにするのは不適切です。

ウ：権限集中時ほど補完的な監視が必要です。

エ：個人への信頼だけでは組織的な統制になりません。

総合解説：職務分掌は重要ですが、組織規模に応じて実現方法を工夫し、代替統制でリスクを補完することが現実的です。

対象：2026年度 / 基準日 2026-09-05

0140 監査・内部統制 > 内部統制・職務分掌・統制活動 ｜ 難易度：応用

経営者や特権者による統制の無効化リスクを低減する方法として、最も適切なものはどれか。

ア：役員の操作は信頼できるので、特権ログの対象外とする。

イ：特権操作のログを独立した立場で確認し、例外承認にも理由・承認者・期間などの記録を残す。

ウ：経営者が指示した処理なら、規程違反でも承認記録を残さない。

エ：内部統制は経営者には適用されないため、経営者による例外処理は評価しない。

答え・解説 正答：イ

ア：役職が高いことは監視免除の理由にはなりません。

イ：経営者による統制の無効化は内部統制の限界の一つであり、重要操作の証跡や独立レビューでリスクを低減します。

ウ：例外処理は理由や承認者を記録し、追跡可能にすることが重要です。

エ：内部統制は経営者を含む組織全体で機能させる必要があります。

総合解説：内部統制の限界を認識したうえで、特権者や経営者の例外操作も追跡可能にし、独立したレビューを行うことが有効です。

対象：2026年度 / 基準日 2026-09-05

0141 監査・内部統制 > 順守状況の評価・CSA・改善対応 ｜ 難易度：基礎

法令・規格・社内規程の順守状況を評価する方法として、最も適切なものはどれか。

ア：規程を作成した時点で順守されているとみなし、実際の運用確認は行わない。

イ：順守状況は事故が発生した場合だけ確認する。

ウ：法令・規格・社内規程の要求事項と実際の運用を定期的に照合し、不適合を把握する。

エ：法令だけを確認し、契約や社内規程の要求事項は評価対象外とする。

答え・解説 正答：ウ

ア：規程の存在と、規程どおりに運用されていることは別です。

イ：事故の有無にかかわらず継続的な確認が必要です。

ウ：順守状況は、要求事項と実際の運用・証拠を照合して評価します。

エ：適用される法令だけでなく、規格、契約、社内規程なども評価対象になり得ます。

総合解説：情報セキュリティマネジメントでは、要求事項の特定、順守状況の確認、不適合の把握、改善までを一連の活動として管理します。

対象：2026年度 / 基準日 2026-09-05

0142 監査・内部統制 > 順守状況の評価・CSA・改善対応 ｜ 難易度：基礎

内部統制分野におけるCSAの説明として、最も適切なものはどれか。

ア：CSAはCyber Security Authenticationの略で、利用者認証方式を示す。

イ：CSAはCloud Service Agreementの略で、クラウド契約だけを意味する。

ウ：CSAは外部監査人だけが実施する法定監査であり、自己評価を含まない。

エ：CSAはControl Self Assessmentの略で、業務部門などが自ら統制の整備・運用状況を評価する統制自己評価である。

答え・解説 正答：エ

ア：この文脈で利用者認証方式を意味する略語ではありません。

イ：この文脈ではクラウドサービス契約の略語ではありません。

ウ：CSAは組織自身が統制を評価する自己評価の考え方です。

エ：IPAの試験シラバスでは、CSAをControl Self Assessment（統制自己評価）として挙げています。

総合解説：略語CSAは分野によって別の意味を持つ場合がありますが、本試験の内部統制分野ではControl Self Assessmentを指します。

対象：2026年度 / 基準日 2026-09-05

0143 監査・内部統制 > 順守状況の評価・CSA・改善対応 ｜ 難易度：基礎

CSAと独立した内部監査・外部監査の関係として、最も適切なものはどれか。

ア：CSAは現場の自己点検に有効だが、独立した監査とは役割が異なるため、必要に応じて併用する。

イ：CSAを実施すれば、独立性が必要な内部監査や外部監査は常に不要になる。

ウ：CSAは監査人が証拠を収集する手続だけを指し、現場の自己点検には使わない。

エ：CSAは統制を改善するためではなく、点数を社外へ公表することだけが目的である。

答え・解説 正答：ア

ア：CSAは業務部門自身の気付きや改善に有効ですが、自己評価ゆえのバイアスもあり得るため、独立監査と補完関係にあります。

イ：必要な独立監査を常に代替するものではありません。

ウ：CSAは現場などによる統制自己評価です。

エ：目的は統制の整備・運用状況を把握し、改善につなげることです。

総合解説：自己評価と独立評価は目的と独立性が異なります。組み合わせることで、日常的な気付きと客観的な検証を両立できます。

対象：2026年度 / 基準日 2026-09-05

0144 監査・内部統制 > 順守状況の評価・CSA・改善対応 ｜ 難易度：標準

CSAで複数の統制未実施が判明した。次の対応として、最も適切なものはどれか。

ア：評価結果を良く見せるため、根拠なく未実施項目を「実施済み」に変更する。

イ：未実施の統制がもたらすリスクを評価し、責任者・期限・対応内容を定めて改善する。

ウ：CSA結果は監査用に保存するだけで、改善計画には反映しない。

エ：全ての未実施項目をリスクに関係なく同じ優先順位で対応する。

答え・解説 正答：イ

ア：虚偽の自己評価では実態把握も改善もできません。

イ：CSAは改善のための自己評価です。不備は隠さず、リスクに基づいて対応計画へつなげます。

ウ：結果を保存するだけでは統制の改善につながりません。

エ：影響、発生可能性、法令・契約要求などを踏まえて優先順位を付けます。

総合解説：自己点検の価値は点数を高く見せることではなく、統制上の弱点を発見してリスク低減につなげることにあります。

対象：2026年度 / 基準日 2026-09-05

0145 監査・内部統制 > 順守状況の評価・CSA・改善対応 ｜ 難易度：標準

監査指摘に対する改善計画の内容として、最も適切なものはどれか。

ア：改善策として「今後注意する」だけを記載し、責任者や期限は設けない。

イ：指摘件数を減らすため、同じ原因の指摘を別々に処理して根本原因は分析しない。

ウ：指摘事項ごとに原因、リスク、改善策、責任者、期限、完了条件を明確にする。

エ：改善期限は全て無期限とし、優先順位を付けない。

答え・解説 正答：ウ

ア：注意喚起だけでは再発防止の実効性を確認しにくくなります。

イ：共通原因を分析すると、複数の指摘を横断的に改善できる場合があります。

ウ：実効的な改善計画では、誰が何をいつまでにどの状態へ改善するかを明確にします。

エ：リスクに応じた期限と優先順位を設定する必要があります。

総合解説：監査指摘は、原因分析と具体的な活動計画へ落とし込み、進捗と完了を確認して初めて改善につながります。

対象：2026年度 / 基準日 2026-09-05

0146 監査・内部統制 > 順守状況の評価・CSA・改善対応 ｜ 難易度：標準

複数の監査指摘について改善の優先順位を決める方法として、最も適切なものはどれか。

ア：指摘された順番だけで対応し、リスクの大きさは考慮しない。

イ：対応が簡単な軽微指摘だけを先に全て終え、重大指摘は後回しにする。

ウ：全指摘を同じ期限に設定し、業務影響や実現可能性は評価しない。

エ：法令違反や重大な情報漏えいにつながる高リスク指摘を、影響と緊急性に基づいて優先する。

答え・解説 正答：エ

ア：指摘された順番とリスクの大きさは一致するとは限りません。

イ：件数を減らすことより重大リスクの低減が重要です。

ウ：全件同一期限ではなく、リスクと対応可能性に応じた計画が必要です。

エ：改善の優先順位は、影響、発生可能性、法令要求、緊急性などのリスク観点で決めます。

総合解説：改善資源には限りがあるため、指摘件数ではなく、組織に与えるリスクを基準として優先順位を付けます。

対象：2026年度 / 基準日 2026-09-05

0147 監査・内部統制 > 順守状況の評価・CSA・改善対応 ｜ 難易度：標準

監査指摘を完了扱いにするための確認として、最も適切なものはどれか。

ア：改善策が実装され、有効に機能していることを示す証拠を確認してから指摘をクローズする。

イ：担当者が「対応済み」と口頭報告した時点で、証拠を確認せず必ず完了とする。

ウ：規程を改訂しただけで、システム設定や実際の運用が変わっていなくても完了とする。

エ：期限を過ぎた指摘は、自動的に完了扱いにする。

答え・解説 正答：ア

ア：改善完了は、設定記録、ログ、テスト結果、改訂規程と運用実績などの証拠で確認します。

イ：口頭報告だけでは実施状況や有効性を十分に確認できない場合があります。

ウ：文書だけでなく実運用まで変わっていることを確認します。

エ：期限超過は自動完了ではなく、エスカレーションや再計画の対象です。

総合解説：フォローアップでは、作業を実施した事実だけでなく、指摘の原因やリスクが適切に低減されたかを確認します。

対象：2026年度 / 基準日 2026-09-05

0148 監査・内部統制 > 順守状況の評価・CSA・改善対応 ｜ 難易度：標準

法令や情報セキュリティ規格が改訂された場合のコンプライアンス対応として、最も適切なものはどれか。

ア：改訂情報は次回事故まで確認せず、旧規程を継続使用する。

イ：改訂情報を収集し、自社に適用される変更を評価して、必要な規程・統制・教育を更新する。

ウ：規格番号が変わっていなければ内容も変わっていないとみなし、改訂履歴を確認しない。

エ：法令改正は法務部だけの問題として、システム設定や業務運用への影響を評価しない。

答え・解説 正答：イ

ア：旧ルールを放置すると不適合につながる可能性があります。

イ：法令・規格類の制定・改廃情報を収集し、自組織への適用性と影響を評価して必要な対応を実施します。

ウ：追補や一部改正もあるため、規格番号だけでなく公式改訂情報を確認します。

エ：法改正がシステム、契約、業務、教育などへ影響する場合があります。

総合解説：順守管理では、要求事項の変更を継続的に把握し、影響分析から実装・教育・証拠更新までつなげることが重要です。

対象：2026年度 / 基準日 2026-09-05

0149 監査・内部統制 > 順守状況の評価・CSA・改善対応 ｜ 難易度：応用

前年に是正したはずの監査指摘が再発した。次の対応として、最も適切なものはどれか。

ア：前回と同じ注意メールを送るだけで、原因分析は行わない。

イ：再発しても前回の改善計画をそのまま完了扱いにする。

ウ：表面的な修正だけでなく根本原因を分析し、必要に応じて管理プロセスそのものを見直す。

エ：指摘が多い部門の評価を守るため、再発指摘を監査記録から削除する。

答え・解説 正答：ウ

ア：注意喚起だけでプロセスが変わらなければ再発する可能性があります。

イ：再発時は前回改善の有効性を再検証します。

ウ：再発は前回の是正が不十分だった可能性を示すため、根本原因と統制の設計・運用を再評価します。

エ：監査記録の隠蔽は監査・コンプライアンス上重大な問題です。

総合解説：同じ不適合が繰り返される場合は、人の注意だけでなく、承認手順、権限、システム制御、教育、監視などを横断して根本原因を分析します。

対象：2026年度 / 基準日 2026-09-05

0150 監査・内部統制 > 順守状況の評価・CSA・改善対応 ｜ 難易度：応用

CSA・内部監査・改善活動を組み合わせた運用として、最も適切なものはどれか。

ア：CSAだけで十分として独立監査を廃止し、重大リスクの客観的検証を行わない。

イ：監査だけを年1回実施し、日常の自己点検や改善状況の確認を一切行わない。

ウ：改善計画を作成した時点で完了とし、実装や有効性確認は行わない。

エ：日常のCSAで弱点を早期把握し、独立監査で客観的に検証し、指摘を改善計画・フォローアップへつなげる。

答え・解説 正答：エ

ア：CSAと独立監査は補完関係であり、常に一方が他方を代替するわけではありません。

イ：日常の自己点検は弱点の早期発見に有効です。

ウ：計画だけでなく、実装と有効性確認まで行う必要があります。

エ：自己評価、独立評価、改善、フォローアップを組み合わせることで統制の継続的改善が機能しやすくなります。

総合解説：順守状況の評価は単発の監査イベントではありません。自己点検、独立監査、是正、フォローアップを循環させ、環境変化に応じて統制を改善します。

対象：2026年度 / 基準日 2026-09-05