0001 情報資産・リスク事例 > 情報資産の特定・価値評価 ｜ 難易度：基礎

A社の人事部は、従業員1,200名の給与計算を社内システムで行っている。
給与DBには氏名、住所、銀行口座、給与額、扶養情報が保存され、給与明細は従業員ポータルから閲覧する。
最近、人事部から営業部へ異動した社員の旧権限が一部残っていることが分かった。

この状況で、機密性の観点から最も高い保護優先度を付けるべき情報資産はどれか。

ア：従業員の銀行口座や給与額などを含む給与DB

イ：採用サイトで公開済みの会社案内PDF

ウ：社内研修で使う架空データだけの操作マニュアル

エ：一般公開している本社代表電話番号の一覧

答え・解説 正答：ア

ア：給与DBには個人情報や金銭に関わる非公開情報が含まれ、漏えい時の本人・組織への影響が大きいため高い機密性が必要です。

イ：既に公開されている会社案内は機密性の要求が低い情報です。

ウ：架空データだけの操作マニュアルは、給与DBそのものより機密性の影響が小さい情報です。

エ：一般公開している代表電話番号は秘密情報ではなく、給与DBより機密性の優先度は低くなります。

総合解説：情報資産の価値は、単にデータ量でなく、漏えい・改ざん・利用不能になったときの事業、法令、本人への影響から評価します。

対象：2026年度 / 基準日 2026-09-05

0002 情報資産・リスク事例 > 脅威・脆弱性・リスク分析 ｜ 難易度：基礎

A社の人事部は、従業員1,200名の給与計算を社内システムで行っている。
給与DBには氏名、住所、銀行口座、給与額、扶養情報が保存され、給与明細は従業員ポータルから閲覧する。
最近、人事部から営業部へ異動した社員の旧権限が一部残っていることが分かった。

旧権限が残っている事実を踏まえたリスク分析として、最も適切なものはどれか。

ア：異動そのものが脅威なので、アクセス権の設定状況を確認する必要はない。

イ：異動者が不要となった人事権限を利用できることが脆弱性となり、給与情報の不正閲覧・持出しにつながるリスクがある。

ウ：給与DBが重要資産であること自体が脆弱性なので、利用者権限はリスクに影響しない。

エ：営業部への異動が完了しているため、旧権限が残っていてもリスクは発生しない。

答え・解説 正答：イ

ア：異動は組織上のイベントであり、それ自体を脅威と断定するより、権限残存などの管理上の弱点を評価する必要があります。

イ：不要権限の残存はアクセス制御上の弱点であり、内部者による不正利用や誤操作の機会を増やします。

ウ：情報資産の重要性は影響評価に関係しますが、脆弱性そのものではありません。

エ：異動後に不要権限が残ることこそがリスク要因であり、異動完了はリスク消滅を意味しません。

総合解説：リスク分析では、資産、脅威、脆弱性、発生可能性、影響を区別して因果関係を整理します。

対象：2026年度 / 基準日 2026-09-05

0003 情報資産・リスク事例 > 対策選択・優先順位・リスク対応計画 ｜ 難易度：基礎

A社の人事部は、従業員1,200名の給与計算を社内システムで行っている。
給与DBには氏名、住所、銀行口座、給与額、扶養情報が保存され、給与明細は従業員ポータルから閲覧する。
最近、人事部から営業部へ異動した社員の旧権限が一部残っていることが分かった。

このリスクへの最初の対応として、最も適切なものはどれか。

ア：給与DBを廃止し、全従業員の給与情報を紙だけで管理する。

イ：異動者本人に注意喚起メールを送るだけで、権限は残しておく。

ウ：異動者の不要権限を速やかに削除し、人事異動時の権限変更手順と定期レビューを改善する。

エ：問題が起きた後に対応できるよう、現在の権限設定は変更せず監視もしない。

答え・解説 正答：ウ

ア：業務要件を無視してシステムを廃止するのは過剰で、別のリスクや非効率を生みます。

イ：注意喚起だけでは技術的に利用可能な不要権限を除去できません。

ウ：現在存在する高リスクの不要権限を除去し、再発防止として権限ライフサイクル管理を改善するのが適切です。

エ：既知の高リスクを放置するのは適切なリスク対応ではありません。

総合解説：リスク対応では、現存するリスクを速やかに低減しつつ、原因となった管理プロセスも見直して再発を防ぎます。

対象：2026年度 / 基準日 2026-09-05

0004 情報資産・リスク事例 > 情報資産の特定・価値評価 ｜ 難易度：基礎

B社は新製品の設計データを開発部のファイルサーバで管理している。
発売前のCAD図面と原価表は競争力に直結する。設計サーバは夜間に自動バックアップされるが、バックアップ装置は同じサーバ室にあり、最近その部屋で漏水が発生した。

情報資産の評価として、最も適切なものはどれか。

ア：CAD図面はファイルサイズが大きいだけなので、価値は低い。

イ：原価表は数字だけのデータなので、漏えいしても事業影響はない。

ウ：バックアップがあるため、設計データの可用性を評価する必要はない。

エ：発売前のCAD図面は機密性が高く、消失すれば開発遅延にもつながるため、機密性と可用性の両面で重要度が高い。

答え・解説 正答：エ

ア：データ量やファイルサイズだけで資産価値は決まりません。

イ：原価情報は競争条件や価格戦略に影響し得る重要情報です。

ウ：バックアップが存在しても、同時被災や復元失敗の可能性を含め可用性評価は必要です。

エ：発売前の設計情報は競争上の秘密であり、漏えい・消失の双方が大きな事業影響を生み得ます。

総合解説：情報資産の価値評価は、機密性・完全性・可用性と事業への影響を組み合わせて行います。

対象：2026年度 / 基準日 2026-09-05

0005 情報資産・リスク事例 > 脅威・脆弱性・リスク分析 ｜ 難易度：基礎

B社は新製品の設計データを開発部のファイルサーバで管理している。
発売前のCAD図面と原価表は競争力に直結する。設計サーバは夜間に自動バックアップされるが、バックアップ装置は同じサーバ室にあり、最近その部屋で漏水が発生した。

漏水を踏まえたバックアップのリスク分析として、最も適切なものはどれか。

ア：原本とバックアップが同じサーバ室にあるため、漏水や火災で両方を同時に失う可能性がある。

イ：毎晩バックアップしているため、物理災害による同時消失は起こり得ない。

ウ：漏水は可用性だけの問題なので、バックアップ配置はリスク評価に含めない。

エ：バックアップ装置が別機器なら、同じ部屋でも災害リスクは完全に分離されている。

答え・解説 正答：ア

ア：同一場所への集中は共通原因故障のリスクを残します。

イ：バックアップ頻度だけでは、同一拠点での災害による同時消失を防げません。

ウ：漏水は重要情報の利用不能に直結するため可用性リスクとして評価します。

エ：機器が別でも、同じ室内の災害に同時に巻き込まれる可能性があります。

総合解説：リスク分析では、個々の装置の冗長性だけでなく、共通の障害要因や保管場所の分離も確認します。

対象：2026年度 / 基準日 2026-09-05

0006 情報資産・リスク事例 > 対策選択・優先順位・リスク対応計画 ｜ 難易度：基礎

B社は新製品の設計データを開発部のファイルサーバで管理している。
発売前のCAD図面と原価表は競争力に直結する。設計サーバは夜間に自動バックアップされるが、バックアップ装置は同じサーバ室にあり、最近その部屋で漏水が発生した。

優先すべき対応として、最も適切なものはどれか。

ア：バックアップ装置のラベルを目立つ色に変更するだけでよい。

イ：バックアップの世代管理に加え、原本と同時被災しない別拠点又は適切に分離された保管先を確保し、復元試験も行う。

ウ：毎晩のバックアップを毎週に減らし、装置への書込み回数を減らす。

エ：漏水対策は施設部門の問題なので、情報セキュリティ側では何も変更しない。

答え・解説 正答：イ

ア：ラベル変更は同時被災リスクを低減しません。

イ：バックアップは同時被災を避ける配置と、実際に復元できることの確認が重要です。

ウ：バックアップ頻度を下げると失われるデータ量が増える可能性があります。

エ：施設リスクも情報資産の可用性に影響するため、部門横断で対応する必要があります。

総合解説：高価値の設計情報では、バックアップの存在ではなく、災害時にも利用できることまで含めてリスク対応を設計します。

対象：2026年度 / 基準日 2026-09-05

0007 情報資産・リスク事例 > 情報資産の特定・価値評価 ｜ 難易度：基礎

C社は取引先向けWebポータルで見積書と契約書を提供している。
取引先ごとにログインIDを発行しているが、URLの末尾にある文書番号を変更すると、
別会社の見積書が表示されることがテストで判明した。

最も重要な情報資産の評価として適切なものはどれか。

ア：URL自体は短い文字列なので、表示される文書の価値は考慮しなくてよい。

イ：ポータルに掲載した時点で全て公開情報になる。

ウ：取引先別の見積書・契約書は、価格条件や契約内容を含むため、取引先間の機密性を確保すべき重要資産である。

エ：契約書は締結済みであれば改ざんや漏えいの影響はない。

答え・解説 正答：ウ

ア：URLの長さではなく、そのURLからアクセスできる情報の価値を評価します。

イ：認証済みポータルに置かれていることは一般公開を意味しません。

ウ：見積・契約情報は取引条件や機密事項を含み、誤開示は信用・契約・競争上の問題を生みます。

エ：締結済み文書でも漏えい・改ざんは重大な影響を及ぼします。

総合解説：情報資産は保存場所ではなく、内容と利用目的、漏えい・改ざん・利用不能時の影響で評価します。

対象：2026年度 / 基準日 2026-09-05

0008 情報資産・リスク事例 > 脅威・脆弱性・リスク分析 ｜ 難易度：基礎

C社は取引先向けWebポータルで見積書と契約書を提供している。
取引先ごとにログインIDを発行しているが、URLの末尾にある文書番号を変更すると、
別会社の見積書が表示されることがテストで判明した。

この事象のリスク分析として、最も適切なものはどれか。

ア：利用者がログインできているため、認可に関する脆弱性は存在しない。

イ：文書番号を変更する行為だけが脆弱性であり、システム側のアクセス制御は関係しない。

ウ：TLSを利用すれば、利用者が別会社の文書を見る問題も自動的に防げる。

エ：認証後の文書アクセスで利用者と文書所有者の対応を確認していないことが脆弱性で、他社文書の不正閲覧につながる。

答え・解説 正答：エ

ア：利用者の操作を想定して、システム側で不正なアクセスを拒否する必要があります。

イ：TLSは通信の保護に有効ですが、アプリケーションの認可不備を修正するものではありません。

ウ：認証済みであることだけでは、他社文書へのアクセスを許可してよい根拠になりません。

エ：認証と認可は別の管理です。ログイン済みでも、対象文書へのアクセス権確認が必要です。

総合解説：Webシステムのリスク分析では、利用者認証だけでなく、個々の資源への認可判定が正しく実装されているかを確認します。

対象：2026年度 / 基準日 2026-09-05

0009 情報資産・リスク事例 > 対策選択・優先順位・リスク対応計画 ｜ 難易度：基礎

C社は取引先向けWebポータルで見積書と契約書を提供している。
取引先ごとにログインIDを発行しているが、URLの末尾にある文書番号を変更すると、
別会社の見積書が表示されることがテストで判明した。

本番公開前の対応として、最も適切なものはどれか。

ア：サーバ側で利用者が閲覧権限を持つ文書だけを返す認可チェックを実装し、同種のアクセス制御不備をテストする。

イ：文書番号を長い乱数に変更するだけで、権限確認は実装しない。

ウ：利用規約に「他社文書を見ないこと」と追記し、システムは変更しない。

エ：発見したテスト担当者だけに文書番号を秘密にする。

答え・解説 正答：ア

ア：根本対策は、利用者と資源の権限関係をサーバ側で検証することです。

イ：推測しにくい番号は補助策にはなっても、認可の代替にはなりません。

ウ：利用規約だけでは技術的に閲覧できる状態を防止できません。

エ：特定の担当者に情報を秘匿しても脆弱性は残ります。

総合解説：高い機密性を持つ顧客文書の認可不備は、公開前に修正し、横展開で同じ設計不備がないか確認するのが適切です。

対象：2026年度 / 基準日 2026-09-05

0010 情報資産・リスク事例 > 情報資産の特定・価値評価 ｜ 難易度：標準

D社の研究部では、新材料の実験結果をクラウドストレージに保存している。
研究者は社外からもアクセスする。共有リンク機能が便利なため、一部フォルダでは
「リンクを知っている人は閲覧可」の設定が使われている。

資産価値評価として、最も適切なものはどれか。

ア：研究者しか理解できない専門データなので、漏えいしても価値はない。

イ：未公開の実験結果は研究開発上の競争力に直結するため、機密性と完全性を高く評価する。

ウ：クラウドに保存した情報はサービス事業者の資産となるため、自社では評価しない。

エ：未公開データはまだ製品化されていないため、完全性を考慮する必要はない。

答え・解説 正答：イ

ア：専門性が高いことは情報価値の低さを意味しません。

イ：未公開研究データは知的価値が高く、漏えいや改ざんが競争力や研究判断に大きく影響します。

ウ：クラウド利用でも情報の業務上の所有・管理責任が消えるわけではありません。

エ：誤った実験結果は研究判断を誤らせるため完全性も重要です。

総合解説：研究情報の価値評価では、現在の売上だけでなく、将来の競争力、知的財産、研究判断への影響も考慮します。

対象：2026年度 / 基準日 2026-09-05

0011 情報資産・リスク事例 > 脅威・脆弱性・リスク分析 ｜ 難易度：標準

D社の研究部では、新材料の実験結果をクラウドストレージに保存している。
研究者は社外からもアクセスする。共有リンク機能が便利なため、一部フォルダでは「リンクを知っている人は閲覧可」の設定が使われている。

「リンクを知っている人は閲覧可」の設定に関するリスク分析として、最も適切なものはどれか。

ア：リンク文字列が十分長ければ、アクセス制御の検討は不要である。

イ：クラウド側で暗号化されていれば、共有リンクの拡散による閲覧リスクはなくなる。

ウ：リンクが誤送信・転送・漏えいすると、本来の利用者以外が研究データへアクセスできる可能性がある。

エ：共有リンクは研究者が作成したものなので、組織としてのリスク評価対象ではない。

答え・解説 正答：ウ

ア：URLの長さは適切なアクセス制御の代替ではありません。

イ：保存時暗号化があっても、正規の共有機能経由で第三者が閲覧できれば漏えいは起こります。

ウ：共有リンクは認証を弱める場合があり、リンクの転送・誤送信による意図しない共有を考慮する必要があります。

エ：業務利用するクラウド設定は組織の情報セキュリティ管理対象です。

総合解説：クラウド利用では、サービス機能が便利でも、情報の重要度に応じて共有範囲・認証・期限・監査可能性を評価します。

対象：2026年度 / 基準日 2026-09-05

0012 情報資産・リスク事例 > 対策選択・優先順位・リスク対応計画 ｜ 難易度：標準

D社の研究部では、新材料の実験結果をクラウドストレージに保存している。
研究者は社外からもアクセスする。共有リンク機能が便利なため、一部フォルダでは「リンクを知っている人は閲覧可」の設定が使われている。

優先する対策として、最も適切なものはどれか。

ア：研究者の利便性を優先し、全フォルダを匿名リンクで共有する。

イ：リンク漏えいが起きた場合だけパスワードを変更し、平時の設定基準は設けない。

ウ：クラウド利用を全面禁止し、研究者には私物USBメモリで持ち運ばせる。

エ：重要フォルダは組織アカウントで認証された利用者だけに共有し、共有期限・権限レビュー・ログ確認を組み合わせる。

答え・解説 正答：エ

ア：匿名共有の拡大は重要研究情報の漏えいリスクを高めます。

イ：事故後対応だけでなく平時の共有基準が必要です。

ウ：全面禁止で私物媒体へ移行すると別の重大リスクを生みます。

エ：重要情報では認証された利用者への限定、権限レビュー、ログなど複数の管理策を組み合わせるのが適切です。

総合解説：リスク対応は利便性をゼロにすることではなく、情報価値に見合う共有制御を設計し、運用可能な形で継続することが重要です。

対象：2026年度 / 基準日 2026-09-05

0013 情報資産・リスク事例 > 情報資産の特定・価値評価 ｜ 難易度：標準

E社の工場では、生産設備の設定値を管理用PCから変更できる。
設定ファイルが誤って書き換わると不良品が大量発生する。管理用PCは工場ネットワークに接続されているが、
担当者間で共通アカウントを使っている。

情報資産の価値評価として、最も適切なものはどれか。

ア：生産設備の設定値と設定ファイルは、改ざんや誤変更が品質・停止損失に直結するため、完全性と可用性が特に重要である。

イ：設定ファイルは個人情報を含まないので、情報資産として評価する必要はない。

ウ：製造設備は物理資産なので、その設定情報の完全性は情報セキュリティと無関係である。

エ：不良品が出ても再製造できるため、設定情報の価値は常に低い。

答え・解説 正答：ア

ア：設定情報の完全性が製品品質や安全、生産継続へ直接影響するため重要資産です。

イ：個人情報でなくても、事業上重要な情報は情報資産です。

ウ：物理設備を制御するデータも情報セキュリティ管理の対象です。

エ：再製造可能でも、損失・納期・信用への影響を評価する必要があります。

総合解説：情報資産の価値は機密性だけでなく、改ざんや利用不能が業務へ与える影響から評価します。

対象：2026年度 / 基準日 2026-09-05

0014 情報資産・リスク事例 > 脅威・脆弱性・リスク分析 ｜ 難易度：標準

E社の工場では、生産設備の設定値を管理用PCから変更できる。
設定ファイルが誤って書き換わると不良品が大量発生する。管理用PCは工場ネットワークに接続されているが、
担当者間で共通アカウントを使っている。

共通アカウント利用に伴うリスクとして、最も適切なものはどれか。

ア：同じ部署の担当者だけが使うため、共通アカウントでも追跡性に問題はない。

イ：設定変更者を個人単位で追跡しにくく、不正変更や誤操作の原因究明が困難になる。

ウ：共通アカウントはパスワード共有を減らすので、個別IDより常に安全である。

エ：ログを取得していれば、共通アカウントでも誰が操作したか必ず特定できる。

答え・解説 正答：イ

ア：部署内利用でも個人単位の責任追跡性は必要です。

イ：共通IDでは操作主体の識別性が低く、説明責任や事故調査に支障が出ます。

ウ：共通パスワードは複数人で共有されるため管理上のリスクが増えます。

エ：共通IDのログだけでは実操作者を一意に特定できない場合があります。

総合解説：重要な設定変更では、個人識別、最小権限、変更記録、レビューを組み合わせて不正・誤操作リスクを低減します。

対象：2026年度 / 基準日 2026-09-05

0015 情報資産・リスク事例 > 対策選択・優先順位・リスク対応計画 ｜ 難易度：標準

E社の工場では、生産設備の設定値を管理用PCから変更できる。
設定ファイルが誤って書き換わると不良品が大量発生する。管理用PCは工場ネットワークに接続されているが、
担当者間で共通アカウントを使っている。

優先すべきリスク対応として、最も適切なものはどれか。

ア：共通アカウントのパスワードだけを長くし、利用者はそのまま共有する。

イ：設定変更を自由化し、問題が起きたときだけ原因を調べる。

ウ：個人IDへ切り替え、必要な担当者だけに設定変更権限を付与し、重要変更は記録・レビューする。

エ：ログ取得を止め、担当者が萎縮しないよう変更履歴を残さない。

答え・解説 正答：ウ

ア：強いパスワードでも共通IDの追跡性問題は残ります。

イ：自由な変更は品質・可用性リスクを増やします。

ウ：個人識別、最小権限、変更記録を組み合わせることで予防と追跡性を高められます。

エ：ログをなくすと原因究明や不正検知が困難になります。

総合解説：重大な業務影響を持つ設定変更は、本人識別と権限管理、変更管理、ログを組み合わせて統制します。

対象：2026年度 / 基準日 2026-09-05

0016 情報資産・リスク事例 > 情報資産の特定・価値評価 ｜ 難易度：標準

F社の営業担当者は顧客先を訪問する際、会社支給ノートPCに顧客名簿と提案書を保存している。ある担当者が出張中にPCを置き忘れた。端末にはログインパスワードはあるが、ディスク暗号化は有効化されていなかった。

この事例で優先して保護すべき情報資産の評価として、最も適切なものはどれか。

ア：ノートPC本体の購入価格だけを資産価値として評価し、保存データは考慮しない。

イ：提案書は顧客に見せる予定なので、紛失しても機密性はない。

ウ：顧客名簿は営業担当者が日常利用するため、重要情報ではない。

エ：端末内の顧客名簿と非公開提案書は、紛失時に顧客情報や営業情報が漏えいするため機密性が高い。

答え・解説 正答：エ

ア：特定顧客向けの非公開提案は一般公開情報ではありません。

イ：日常利用する情報でも漏えい時の影響が大きければ重要資産です。

ウ：情報資産価値は媒体価格と同一ではありません。

エ：端末の物理価格以上に、保存された顧客情報や営業情報の漏えい影響を評価する必要があります。

総合解説：モバイル端末のリスク評価では、端末自体と端末内に保存された情報を分けて考え、漏えい・利用不能時の影響を評価します。

対象：2026年度 / 基準日 2026-09-05

0017 情報資産・リスク事例 > 脅威・脆弱性・リスク分析 ｜ 難易度：標準

F社の営業担当者は顧客先を訪問する際、会社支給ノートPCに顧客名簿と提案書を保存している。ある担当者が出張中にPCを置き忘れた。端末にはログインパスワードはあるが、ディスク暗号化は有効化されていなかった。

端末紛失に関するリスク分析として、最も適切なものはどれか。

ア：端末紛失という脅威に対し、ディスク暗号化未実施が脆弱性となり、保存データを第三者に読み取られるリスクが高まる。

イ：ログインパスワードがあるため、ストレージを取り外して読む攻撃も必ず防げる。

ウ：紛失は物理資産の問題だけであり、情報漏えいリスクにはつながらない。

エ：ディスク暗号化は可用性対策なので、機密性とは関係しない。

答え・解説 正答：ア

ア：端末を取得した第三者が別環境からストレージを読む可能性があり、保存データ暗号化は機密性保護に有効です。

イ：OSログインだけではストレージ直接読取りへの耐性が不十分な場合があります。

ウ：端末紛失は保存情報の漏えいにもつながります。

エ：ディスク暗号化は主に保存データの機密性保護に有効です。

総合解説：モバイル端末では、紛失・盗難を前提に、保存データ暗号化、認証、遠隔管理などの対策を組み合わせます。

対象：2026年度 / 基準日 2026-09-05

0018 情報資産・リスク事例 > 対策選択・優先順位・リスク対応計画 ｜ 難易度：標準

F社の営業担当者は顧客先を訪問する際、会社支給ノートPCに顧客名簿と提案書を保存している。ある担当者が出張中にPCを置き忘れた。端末にはログインパスワードはあるが、ディスク暗号化は有効化されていなかった。

再発防止として最も適切な対応はどれか。

ア：端末を紛失した社員だけに口頭注意し、端末設定は変更しない。

イ：会社支給端末でディスク暗号化を標準化し、画面ロック、遠隔管理、紛失時の報告手順を併せて整備する。

ウ：顧客情報を個人の私物USBメモリへコピーして持ち歩く。

エ：パスワードを全員同じ強固な文字列に統一する。

答え・解説 正答：イ

ア：個人への注意だけでは同じ構造的リスクが残ります。

イ：技術対策と運用手順を組み合わせ、組織全体で同じリスクを低減することが重要です。

ウ：私物媒体への移行は管理外の新たなリスクを生みます。

エ：共有パスワードは本人識別と管理の面で不適切です。

総合解説：個別事故を契機に、端末標準設定と紛失対応プロセスを組織全体へ横展開するのが適切です。

対象：2026年度 / 基準日 2026-09-05

0019 情報資産・リスク事例 > 情報資産の特定・価値評価 ｜ 難易度：標準

G社はECサイトを運営しており、注文DBに氏名、配送先、購入履歴を保存している。
DBサーバは24時間稼働しているが、テスト環境を作る際に本番DBのコピーをそのまま利用している。
テスト担当者は本番運用担当者より広い人数である。

情報資産管理の観点から最も適切な評価はどれか。

ア：テスト環境に置いた時点でデータは架空データとみなせる。

イ：本番システムではないため、テスト環境のデータは情報資産台帳に載せる必要がない。

ウ：本番DBのコピーも顧客情報を含むため本番データと同様に重要な情報資産として管理対象に含める。

エ：同じデータのコピーは新しい情報資産ではないので、保存場所や利用者を把握しなくてよい。

答え・解説 正答：ウ

ア：環境名がテストでもデータ内容は実データです。

イ：非本番環境も情報資産管理の対象です。

ウ：本番データの実コピーであれば、保存場所がテスト環境でも顧客情報としての価値・義務は変わりません。

エ：コピーの所在と利用者を把握しないと、漏えい経路を管理できません。

総合解説：情報資産管理では、元データだけでなく複製・バックアップ・テスト利用などの派生コピーも把握する必要があります。

対象：2026年度 / 基準日 2026-09-05

0020 情報資産・リスク事例 > 脅威・脆弱性・リスク分析 ｜ 難易度：標準

G社はECサイトを運営しており、注文DBに氏名、配送先、購入履歴を保存している。
DBサーバは24時間稼働しているが、テスト環境を作る際に本番DBのコピーをそのまま利用している。
テスト担当者は本番運用担当者より広い人数である。

リスク分析として最も適切なものはどれか。

ア：テスト環境はインターネット公開していなければ、内部者による漏えいリスクは存在しない。

イ：本番DBが安全なら、そのコピーのアクセス制御が弱くても全体リスクは変わらない。

ウ：テスト担当者は開発目的で利用するため、個人情報へのアクセス範囲を制限する必要はない。

エ：実顧客データを広い人数が利用するテスト環境へ複製しているため、不必要な閲覧や漏えいの可能性が高まる。

答え・解説 正答：エ

ア：非公開ネットワークでも内部不正や誤操作のリスクはあります。

イ：コピー側の統制が弱ければ、そこが漏えい経路になります。

ウ：業務目的に必要な範囲へアクセスを限定することが重要です。

エ：複製先の利用者増加と統制低下は、漏えいの発生可能性を高めます。

総合解説：リスクは最も弱い取扱場所から顕在化することがあるため、非本番環境を含めて情報のライフサイクル全体を評価します。

対象：2026年度 / 基準日 2026-09-05

0021 情報資産・リスク事例 > 対策選択・優先順位・リスク対応計画 ｜ 難易度：標準

G社はECサイトを運営しており、注文DBに氏名、配送先、購入履歴を保存している。
DBサーバは24時間稼働しているが、テスト環境を作る際に本番DBのコピーをそのまま利用している。
テスト担当者は本番運用担当者より広い人数である。

リスク低減策として最も適切なものはどれか。

ア：テスト目的に実データが不要なら匿名化・マスキングしたデータを用い、必要な場合も利用者と期間を最小限に制限する。

イ：本番データをそのまま配布し、各担当者に自己責任で管理させる。

ウ：テスト環境のログ取得を停止して、作業効率を優先する。

エ：テスト完了後も将来使う可能性があるため、実データのコピーを無期限に残す。

答え・解説 正答：ア

ア：テスト目的に必要な最小限のデータへ変換し、アクセスと保管期間を制限するのが適切です。

イ：実データの広範な配布は漏えいリスクを高めます。

ウ：ログ停止は追跡性を下げます。

エ：不要な実データを長期保管すると露出期間が延びます。

総合解説：情報資産の利用目的に応じて、データ最小化、マスキング、アクセス制御、削除を組み合わせることが有効です。

対象：2026年度 / 基準日 2026-09-05

0022 情報資産・リスク事例 > 情報資産の特定・価値評価 ｜ 難易度：標準

H社の経理部では月次決算ファイルを共有フォルダで管理している。
部門長が最終確認する前に、担当者が誤って前月のファイルを上書きしてしまい、
一部の集計値を再計算する必要が生じた。

月次決算ファイルの情報資産価値の評価として、最も適切なものはどれか。

ア：社内だけで利用するため、完全性は重視しなくてよい。

イ：経営判断や報告に使うため、数値の完全性と必要時に参照できる可用性が重要である。

ウ：機密性が確保されていれば、誤った集計値でも問題はない。

エ：月次ファイルは翌月に更新されるため、過去版の保持価値はない。

答え・解説 正答：イ

ア：社内利用でも誤情報は重大な影響を与えます。

イ：財務情報は正確性が経営判断や報告に直結し、完全性が重要です。

ウ：機密性だけでなく完全性が必要です。

エ：過去版は差異確認や復旧、監査証跡として価値があります。

総合解説：情報資産の評価では、利用目的から必要なセキュリティ特性を特定します。財務情報では完全性の重要度が高くなります。

対象：2026年度 / 基準日 2026-09-05

0023 情報資産・リスク事例 > 脅威・脆弱性・リスク分析 ｜ 難易度：標準

H社の経理部では月次決算ファイルを共有フォルダで管理している。
部門長が最終確認する前に、担当者が誤って前月のファイルを上書きしてしまい、
一部の集計値を再計算する必要が生じた。

この事故のリスク分析として最も適切なものはどれか。

ア：誤操作した担当者だけが脅威なので、システム側の管理策は必要ない。

イ：ファイルが消えず上書きされただけなので、情報セキュリティ事故ではない。

ウ：共有フォルダで版管理や復旧手段が不十分なことが脆弱性となり、誤操作で正しい決算データを失うリスクがある。

エ：部門長が最終確認するため、途中データの完全性は評価しなくてよい。

答え・解説 正答：ウ

ア：人のミスだけに責任を帰すのではなく、誤操作が重大損失につながる弱点を評価します。

イ：上書きでも正しいデータの消失という完全性・可用性の問題が生じます。

ウ：誤操作は想定すべき事象であり、版管理やバックアップで影響を低減する必要があります。

エ：最終確認前でも復旧不能なら業務影響が発生します。

総合解説：リスク分析では、人のミスを前提に、誤操作が重大事故へ発展しない管理策があるかを確認します。

対象：2026年度 / 基準日 2026-09-05

0024 情報資産・リスク事例 > 対策選択・優先順位・リスク対応計画 ｜ 難易度：標準

H社の経理部では月次決算ファイルを共有フォルダで管理している。
部門長が最終確認する前に、担当者が誤って前月のファイルを上書きしてしまい、
一部の集計値を再計算する必要が生じた。

再発防止策として最も適切なものはどれか。

ア：ファイル名の色を変えて注意を促すだけでよい。

イ：全員に削除・上書き権限を付け、操作ミスは教育だけで防ぐ。

ウ：過去版は容量を使うので、更新のたびに即時削除する。

エ：世代保存やバージョン管理を有効にし、重要ファイルの更新権限を限定し、復元手順を確認する。

答え・解説 正答：エ

ア：視覚的注意だけでは上書き自体を防げません。

イ：過大な権限と教育依存は再発リスクを残します。

ウ：過去版の即時削除は復旧可能性を下げます。

エ：版管理と権限制御、復元確認を組み合わせることで、誤操作の予防と復旧の両方を改善できます。

総合解説：重要業務ファイルでは、人の注意だけでなく、版管理、最小権限、バックアップなど技術・運用両面の統制が必要です。

対象：2026年度 / 基準日 2026-09-05

0025 情報資産・リスク事例 > 情報資産の特定・価値評価 ｜ 難易度：応用

I社は大規模災害時に使用する取引先・従業員の緊急連絡網を作成している。
連絡網には携帯電話番号と代替連絡先が含まれるが、更新は年1回だけで、
最近の組織変更や退職者が反映されていない。

緊急連絡網の価値評価として、最も適切なものはどれか。

ア：個人情報を含むため機密性が必要である一方、災害時に正しく連絡できるよう完全性と可用性も重要である。

イ：電話番号だけなので、情報資産として管理する必要はない。

ウ：災害時だけ使う情報なので、平時の更新は不要である。

エ：機密性だけ確保すれば、古い番号が残っていても問題はない。

答え・解説 正答：ア

ア：連絡網は個人情報であり、同時に緊急時の業務継続に使うため、複数のセキュリティ特性が重要です。

イ：電話番号も個人に結び付けば管理対象となります。

ウ：非常時に使う情報ほど、平時の整備が必要です。

エ：古い情報は必要時に連絡できないため完全性・可用性を損ないます。

総合解説：情報資産の価値は一つの特性だけでなく、利用目的に応じて機密性・完全性・可用性を総合評価します。

対象：2026年度 / 基準日 2026-09-05

0026 情報資産・リスク事例 > 脅威・脆弱性・リスク分析 ｜ 難易度：応用

I社は大規模災害時に使用する取引先・従業員の緊急連絡網を作成している。
連絡網には携帯電話番号と代替連絡先が含まれるが、更新は年1回だけで、
最近の組織変更や退職者が反映されていない。

現在の運用に関するリスク分析として、最も適切なものはどれか。

ア：連絡網が存在するだけでBCP要件は満たされるため、内容の正確性はリスクに影響しない。

イ：更新頻度が低く退職者や組織変更が未反映であるため、災害時に重要連絡が届かないリスクがある。

ウ：年1回更新していれば、異動や退職の発生時期に関係なく十分である。

エ：古い電話番号は機密性だけの問題で、事業継続には影響しない。

答え・解説 正答：イ

ア：文書の存在ではなく、実際に機能することが重要です。

イ：情報が古いと、災害時の意思決定や安否確認が遅れる可能性があります。

ウ：人員変動が多い場合は年1回更新では不十分なことがあります。

エ：古い連絡先は可用性・完全性の問題として継続計画へ影響します。

総合解説：BCP関連情報は、作成時点の正確さだけでなく、変化へ追随できる更新プロセスまで評価する必要があります。

対象：2026年度 / 基準日 2026-09-05

0027 情報資産・リスク事例 > 対策選択・優先順位・リスク対応計画 ｜ 難易度：応用

I社は大規模災害時に使用する取引先・従業員の緊急連絡網を作成している。
連絡網には携帯電話番号と代替連絡先が含まれるが、更新は年1回だけで、
最近の組織変更や退職者が反映されていない。

最も適切な改善策はどれか。

ア：毎年の更新日まで変更を反映せず、災害時に担当者が個別に調べる。

イ：利便性を優先して連絡網を社外公開Webに掲載する。

ウ：人事異動・退職などのイベントに連動して更新し、定期確認と緊急時の利用テストを行う。

エ：古い情報を残したまま、ファイル名だけを「最新版」に変更する。

答え・解説 正答：ウ

ア：災害時の即時対応に必要な情報を事前に整備するのがBCPの考え方です。

イ：個人情報を無制限に公開するのは不適切です。

ウ：組織変更に連動した更新と定期確認、利用テストによって実効性を高められます。

エ：名称変更だけでは情報の正確性は改善しません。

総合解説：継続計画に必要な情報は、平時から更新責任と確認方法を定め、実際に使えることをテストします。

対象：2026年度 / 基準日 2026-09-05

0028 情報資産・リスク事例 > 情報資産の特定・価値評価 ｜ 難易度：応用

J社は複数の外部サービスと連携するため、APIキーを設定ファイルに保存している。
開発者がトラブル調査のため設定ファイルを社内チャットに添付し、そのチャットには委託先メンバーも参加していた。
APIキーには本番環境のデータ取得権限がある。

APIキーの情報資産価値の評価として、最も適切なものはどれか。

ア：APIキーは短い文字列なので、通常の文書より価値が低い。

イ：設定ファイルの一部なので、単独では情報資産とみなさない。

ウ：社内チャットに貼れる情報は全て公開情報として扱える。

エ：本番データへアクセスできるAPIキーは認証情報であり、漏えいすると権限悪用につながるため高い機密性が必要である。

答え・解説 正答：エ

ア：文字列の長さでは価値は決まりません。

イ：設定ファイル内の秘密情報も個別に保護対象です。

ウ：社内チャットは公開情報の保管場所を意味しません。

エ：APIキーはアクセス権を行使できる秘密情報であり、漏えい時の影響が大きい重要資産です。

総合解説：パスワード、秘密鍵、トークン、APIキーなどの認証情報は、情報システムへの権限そのものに近い価値を持つため厳格に管理します。

対象：2026年度 / 基準日 2026-09-05

0029 情報資産・リスク事例 > 脅威・脆弱性・リスク分析 ｜ 難易度：応用

J社は複数の外部サービスと連携するため、APIキーを設定ファイルに保存している。
開発者がトラブル調査のため設定ファイルを社内チャットに添付し、そのチャットには委託先メンバーも参加していた。
APIキーには本番環境のデータ取得権限がある。

この事象のリスク分析として、最も適切なものはどれか。

ア：本番権限を持つAPIキーを閲覧範囲の広いチャットへ添付したことで、不要な利用者がキーを取得・悪用できるリスクが生じた。

イ：社内チャットなので、委託先を含め誰が見ても機密性リスクはない。

ウ：APIキーが設定ファイルに書かれている以上、どこへ送信してもリスクは変わらない。

エ：APIアクセスは自動処理用なので、人がキーを知っても悪用できない。

答え・解説 正答：ア

ア：認証情報の共有範囲が必要以上に広がると、不正利用や漏えいの可能性が高まります。

イ：社内ツールでも参加者や権限範囲を確認する必要があります。

ウ：保存場所や共有先によって露出リスクは変わります。

エ：APIキーを取得した人が正規APIを利用できる場合があり、人による悪用も可能です。

総合解説：認証情報は最小限の利用者・システムだけが扱えるようにし、誤共有を前提とした失効・ローテーション手順も必要です。

対象：2026年度 / 基準日 2026-09-05

0030 情報資産・リスク事例 > 対策選択・優先順位・リスク対応計画 ｜ 難易度：応用

J社は複数の外部サービスと連携するため、APIキーを設定ファイルに保存している。
開発者がトラブル調査のため設定ファイルを社内チャットに添付し、そのチャットには委託先メンバーも参加していた。
APIキーには本番環境のデータ取得権限がある。

最初に実施すべき対応として、最も適切なものはどれか。

ア：チャットの投稿を削除するだけで、APIキーはそのまま利用し続ける。

イ：漏えいした可能性のあるAPIキーを速やかに失効・再発行し、アクセスログを確認した上で秘密管理の方法を改善する。

ウ：委託先メンバーに口頭で「使わないで」と依頼し、キーは変更しない。

エ：次回の定期保守まで何もせず、悪用が確認された場合だけキーを変更する。

答え・解説 正答：イ

ア：投稿削除後も既にコピーされている可能性があり、秘密の有効性は回復しません。

イ：一度閲覧された可能性がある秘密情報は回収できないため、失効・ローテーションと利用状況確認が必要です。

ウ：注意依頼だけでは技術的な利用可能性を除去できません。

エ：本番権限を持つキーの漏えいは待たずに対応すべき高リスク事象です。

総合解説：秘密情報の漏えい時は、秘密を無効化する即時対応と、秘密管理・共有手順の是正を分けて実施します。

対象：2026年度 / 基準日 2026-09-05

0031 システム利用・管理策事例 > アクセス・パッチ・ログ・バックアップ ｜ 難易度：基礎

K社では社内ポータルをLinuxサーバで運用している。
ベンダから重要度の高い脆弱性修正パッチが公開されたが、業務部門は「停止が怖い」として適用延期を希望している。
テスト環境はあり、夜間の保守時間帯も確保できる。

最も適切な対応はどれか。

ア：停止リスクをゼロにするため、サーバ廃止までパッチを適用しない。

イ：重要度に関係なく全パッチを公開当日に本番へ無検証で適用する。

ウ：脆弱性の深刻度と自社への影響を評価し、テスト環境で検証した上で優先度に応じて保守時間帯に適用する。

エ：業務部門が延期を希望しているため、セキュリティ側では脆弱性評価を行わない。

答え・解説 正答：ウ

ア：無期限延期は既知脆弱性を放置します。

イ：緊急性が高くても、利用可能な検証環境があるなら必要な確認を行うべきです。

ウ：パッチ管理は脆弱性の深刻度、露出状況、業務影響を評価し、検証・適用・結果確認まで計画的に行います。

エ：業務部門の要望だけでなく、セキュリティリスクを含めて意思決定します。

総合解説：パッチ管理では、適用しないリスクと適用に伴う変更リスクの両方を評価し、優先順位と手順を決めます。

対象：2026年度 / 基準日 2026-09-05

0032 システム利用・管理策事例 > メール・Web・モバイル・媒体管理 ｜ 難易度：基礎

K社では社内ポータルをLinuxサーバで運用している。
ベンダから重要度の高い脆弱性修正パッチが公開されたが、業務部門は「停止が怖い」として適用延期を希望している。
テスト環境はあり、夜間の保守時間帯も確保できる。

保守作業に関する利用者対応として、最も適切なものはどれか。

ア：停止を知らせると苦情が増えるので、利用者には事前通知しない。

イ：脆弱性の技術詳細と攻撃手順を全社員へ無制限に配布する。

ウ：保守中も通常どおり利用できると案内し、実際の停止可能性は伝えない。

エ：停止時間と影響範囲を事前周知し、利用者が回避策や代替手段を取れるようにする。

答え・解説 正答：エ

ア：事前通知なしの停止は業務混乱を招きます。

イ：必要以上に攻撃手順まで広く配布する必要はありません。

ウ：実際の影響を正確に伝えることが重要です。

エ：計画停止は利用者へ適切に周知し、業務影響を低減することが重要です。

総合解説：セキュリティ対策は技術だけでなく、利用者への適切な連絡と業務調整を含めて運用します。

対象：2026年度 / 基準日 2026-09-05

0033 システム利用・管理策事例 > クラウド利用・セキュリティ要求事項 ｜ 難易度：基礎

K社では社内ポータルをLinuxサーバで運用している。
ベンダから重要度の高い脆弱性修正パッチが公開されたが、業務部門は「停止が怖い」として適用延期を希望している。
テスト環境はあり、夜間の保守時間帯も確保できる。

このポータルをIaaSへ移行した場合のセキュリティ要求として、最も適切なものはどれか。

ア：クラウド事業者が基盤を管理する範囲と、自社がOS・アプリのパッチを管理する範囲を明確にする。

イ：IaaSへ移行すれば、OSやアプリの脆弱性管理も全てクラウド事業者の責任になる。

ウ：クラウド事業者の認証取得を確認すれば、自社の設定やパッチ管理は不要になる。

エ：クラウドは自動的に安全なので、責任分界を契約や設計で確認しなくてよい。

答え・解説 正答：ア

ア：IaaSでは利用者側がOSやアプリを管理する部分が残るため、責任分界を明確にすることが重要です。

イ：IaaSで利用者が管理するOS等まで全て事業者責任になるわけではありません。

ウ：第三者認証は有用ですが、自社側の管理責任を消しません。

エ：クラウド利用でも責任範囲の明確化が必要です。

総合解説：クラウドではサービスモデルによって責任分界が変わるため、脆弱性管理や設定管理の担当を明確にします。

対象：2026年度 / 基準日 2026-09-05

0034 システム利用・管理策事例 > アクセス・パッチ・ログ・バックアップ ｜ 難易度：基礎

L社の会員サイトで、深夜に同一IDへ数百回のログイン失敗が記録された後、正常ログインが1回発生している。
現在、ログは各サーバに保存されるだけで、日常的な集約・分析はしていない。

最初の対応として、最も適切なものはどれか。

ア：ログイン成功が1回あるので正常利用と判断し、失敗ログは削除する。

イ：該当IDの認証ログ、接続元、ログイン後の操作を確認し、必要に応じてアカウント保護やインシデント対応へ移行する。

ウ：ログ件数が多いので分析を諦め、全ログ取得を停止する。

エ：該当利用者へ確認せず、全会員アカウントを永久停止する。

答え・解説 正答：イ

ア：成功があることは正常の証拠ではなく、侵害成功の可能性もあります。

イ：大量失敗後の成功は認証攻撃の可能性があるため、関連ログを確認し影響を評価します。

ウ：ログ停止は検知・調査能力を失わせます。

エ：全利用者を無条件に永久停止するのは過剰で、影響評価に基づく対応が必要です。

総合解説：ログ監視では単一イベントではなく、失敗・成功・接続元・後続操作を関連付けて判断します。

対象：2026年度 / 基準日 2026-09-05

0035 システム利用・管理策事例 > メール・Web・モバイル・媒体管理 ｜ 難易度：基礎

L社の会員サイトで、深夜に同一IDへ数百回のログイン失敗が記録された後、正常ログインが1回発生している。
現在、ログは各サーバに保存されるだけで、日常的な集約・分析はしていない。

該当IDが不正利用された可能性が高い場合の利用者対応として、最も適切なものはどれか。

ア：利用者に知られると不安になるため、侵害の可能性を一切伝えない。

イ：利用者へパスワードをメール本文で送るよう依頼する。

ウ：利用者へ状況を連絡し、認証情報の変更やセッション無効化など必要な保護措置を案内・実施する。

エ：調査前から利用者に損害賠償責任があると断定する。

答え・解説 正答：ウ

ア：通知しないことで被害が継続する可能性があります。

イ：パスワードを平文メールで収集するのは不適切です。

ウ：利用者保護のため、必要な事実と対応を適切に案内し、アカウントを保護します。

エ：事実確認前に責任を断定するのは適切ではありません。

総合解説：インシデント対応では、技術調査だけでなく、影響を受ける利用者への適切な連絡と保護措置が重要です。

対象：2026年度 / 基準日 2026-09-05

0036 システム利用・管理策事例 > クラウド利用・セキュリティ要求事項 ｜ 難易度：基礎

L社の会員サイトで、深夜に同一IDへ数百回のログイン失敗が記録された後、正常ログインが1回発生している。
現在、ログは各サーバに保存されるだけで、日常的な集約・分析はしていない。

会員サイトをPaaSへ移行する際のログ要件として、最も適切なものはどれか。

ア：PaaSでは全ログが自動的に永久保存されるため、契約前の確認は不要である。

イ：クラウド事業者だけがログを見られれば、自社は事故調査にアクセスできなくてよい。

ウ：ログは容量を使うので、認証成功だけを残し失敗ログは取得しない。

エ：認証・管理操作など必要なログを取得できるか、保管期間・アクセス方法・時刻同期・エクスポート可否を事前に確認する。

答え・解説 正答：エ

ア：永久保存が自動で保証されるわけではありません。

イ：自社が調査・監査に必要なログへアクセスできることが重要です。

ウ：失敗ログは攻撃検知に重要な情報です。

エ：クラウドでは利用可能なログ種類や保持期間がサービスによって異なるため、必要要件を事前確認します。

総合解説：クラウド選定では、機能だけでなく監査・調査に必要なログ取得能力をセキュリティ要求事項として確認します。

対象：2026年度 / 基準日 2026-09-05

0037 システム利用・管理策事例 > アクセス・パッチ・ログ・バックアップ ｜ 難易度：基礎

M社のファイルサーバがランサムウェアに感染し、共有ファイルが暗号化された。毎日バックアップを取得していたが、バックアップ領域は常時サーバから書込み可能で、同時に暗号化されていた。

再発防止として最も適切なバックアップ管理はどれか。

ア：本番から常時書込みできないオフライン又はイミュータブルなコピーを含め、複数世代を保持し復元確認を行う。

イ：バックアップ回数だけを増やし、全コピーを常時同じ権限で接続する。

ウ：容量節約のため、最新1世代だけを本番サーバ内に保存する。

エ：バックアップがあることだけを確認し、復元テストは行わない。

答え・解説 正答：ア

ア：ランサムウェアからバックアップを守るには、本番と分離したコピー、世代管理、復元確認が重要です。

イ：常時同じ権限で接続されると一括暗号化されるリスクが残ります。

ウ：最新1世代だけでは感染後のバックアップで上書きされる可能性があります。

エ：バックアップは復元できて初めて有効です。

総合解説：バックアップは取得頻度だけでなく、攻撃・災害からの分離、世代、復元可能性まで設計します。

対象：2026年度 / 基準日 2026-09-05

0038 システム利用・管理策事例 > メール・Web・モバイル・媒体管理 ｜ 難易度：基礎

M社のファイルサーバがランサムウェアに感染し、共有ファイルが暗号化された。毎日バックアップを取得していたが、バックアップ領域は常時サーバから書込み可能で、同時に暗号化されていた。

調査の結果、感染開始は不審メールの添付ファイル実行だった。利用者向け対策として最も適切なものはどれか。

ア：不審メールを見つけたら、添付ファイル付きのまま全社員へ転送して注意喚起する。

イ：不審メールの報告手順を整備し、添付ファイルやURLを安易に開かない教育と技術的対策を組み合わせる。

ウ：メールを完全禁止し、業務連絡は私物SNSだけで行う。

エ：教育だけで十分なので、メールフィルタや端末対策は不要とする。

答え・解説 正答：イ

ア：危険な添付やURLをそのまま転送すると被害を拡大させる可能性があります。

イ：不審メールは安全な報告経路で扱い、教育とメール・端末側の技術対策を組み合わせます。

ウ：私物SNSへの移行は新たな管理外リスクを生みます。

エ：人的対策だけに依存せず多層的に防御することが重要です。

総合解説：科目Bでは、利用者行動と技術的管理策を組み合わせて現実的な運用を選ぶ判断が重要です。

対象：2026年度 / 基準日 2026-09-05

0039 システム利用・管理策事例 > クラウド利用・セキュリティ要求事項 ｜ 難易度：基礎

M社のファイルサーバがランサムウェアに感染し、共有ファイルが暗号化された。
毎日バックアップを取得していたが、バックアップ領域は常時サーバから書込み可能で、同時に暗号化されていた。

クラウドバックアップサービスを導入する際のセキュリティ要求として、最も適切なものはどれか。

ア：クラウドならランサムウェアの影響を絶対に受けないので、管理者認証は不要である。

イ：サービス料金だけを比較し、復元方法や保持仕様は導入後に確認する。

ウ：保存データの暗号化、管理者認証、削除・保持制御、復元性能、事業者側障害時の対応を確認する。

エ：バックアップ先をクラウドにすれば、自社の復元訓練は不要になる。

答え・解説 正答：ウ

ア：クラウドも認証情報侵害や誤削除などのリスクがあります。

イ：復元要件は選定前に確認すべき重要条件です。

ウ：クラウドバックアップでも認証、データ保護、保持、復元、責任分界を確認する必要があります。

エ：事業者機能があっても、自社の復旧手順が実際に機能するか確認が必要です。

総合解説：クラウド利用では、サービスの可用性だけでなく、自社が必要な復旧目標を満たせるかを要求事項として評価します。

対象：2026年度 / 基準日 2026-09-05

0040 システム利用・管理策事例 > アクセス・パッチ・ログ・バックアップ ｜ 難易度：標準

N社では、退職者のSaaSアカウントを人事担当者が月末にまとめて削除している。
月初に退職した社員のアカウントが約4週間有効なまま残ることがある。
複数のSaaSには顧客情報や社内資料が保存されている。

最も適切な改善策はどれか。

ア：月末まで利用されないことを信頼し、現行運用を続ける。

イ：退職者のパスワードを管理者が知っていれば、アカウントは残してよい。

ウ：削除漏れを防ぐため、全社員のアカウントを毎月一度削除して再作成する。

エ：退職日と連動してアカウントを無効化し、定期的に有効アカウントと在籍者を照合する。

答え・解説 正答：エ

ア：利用されないという期待だけではリスクを除去できません。

イ：管理者がパスワードを知っていても不要アカウントの残存リスクは変わりません。

ウ：全員のアカウント再作成は過剰で、業務影響も大きくなります。

エ：退職時に不要権限を速やかに停止し、定期レビューで漏れを検知することが重要です。

総合解説：アクセス管理では、入社・異動・退職などの人事イベントとアカウント変更を連携させます。

対象：2026年度 / 基準日 2026-09-05

0041 システム利用・管理策事例 > メール・Web・モバイル・媒体管理 ｜ 難易度：標準

N社では、退職者のSaaSアカウントを人事担当者が月末にまとめて削除している。
月初に退職した社員のアカウントが約4週間有効なまま残ることがある。
複数のSaaSには顧客情報や社内資料が保存されている。

人的・運用面の対策として最も適切なものはどれか。

ア：退職時に秘密保持・データ持出し禁止・会社データの返却又は削除手順を確認し、必要な教育と誓約を行う。

イ：退職者はもう社員ではないため、退職前の説明や手続は不要である。

ウ：退職前に本人へ全顧客データをバックアップとして渡す。

エ：アカウント削除だけで十分なので、秘密保持やデータ返却は確認しない。

答え・解説 正答：ア

ア：退職時はアクセス停止に加え、秘密情報・会社資産の扱いを明確にし、返却・削除を確認します。

イ：退職前の手続こそ重要です。

ウ：会社データを個人へ渡すのは不適切です。

エ：技術的なアカウント停止と契約・運用上の秘密保持は補完関係です。

総合解説：退職者対策はアカウント削除だけでなく、情報持出し、媒体・機器返却、秘密保持を含めて管理します。

対象：2026年度 / 基準日 2026-09-05

0042 システム利用・管理策事例 > クラウド利用・セキュリティ要求事項 ｜ 難易度：標準

N社では、退職者のSaaSアカウントを人事担当者が月末にまとめて削除している。
月初に退職した社員のアカウントが約4週間有効なまま残ることがある。
複数のSaaSには顧客情報や社内資料が保存されている。

新たなSaaSを導入する際、退職者アカウント残存を減らすために有効な要求事項はどれか。

ア：SaaSごとに個人メールアドレスで登録し、退職後も本人が管理する。

イ：組織のID基盤との連携やアカウント自動停止、管理者向け利用者一覧・監査機能を確認する。

ウ：利用者一覧を出力できないサービスを選び、各部署の記憶だけで管理する。

エ：アカウント削除機能がなくても、契約が安ければ問題ない。

答え・解説 正答：イ

ア：個人メールでの登録は組織管理を困難にします。

イ：ID連携や利用者棚卸し機能は、複数SaaSのアカウントライフサイクル管理に有効です。

ウ：利用者一覧がないと棚卸しが難しくなります。

エ：削除・無効化機能はアクセス管理上の重要要件です。

総合解説：クラウドサービス選定では、認証方式だけでなく、利用者の追加・変更・削除を組織が管理できる機能も確認します。

対象：2026年度 / 基準日 2026-09-05

0043 システム利用・管理策事例 > アクセス・パッチ・ログ・バックアップ ｜ 難易度：標準

O社では製造現場の装置へ設定ファイルを渡すためUSBメモリを使用している。
現場では私物USBも利用可能で、利用記録は取っていない。
最近、マルウェア感染した私物USBが持ち込まれた。

最も適切な対策はどれか。

ア：私物USBも含め自由利用を認め、問題が起きた場合だけ回収する。

イ：USBを使う担当者の名前だけ覚えておき、媒体識別や記録はしない。

ウ：許可された媒体だけを使用し、貸出・返却を記録し、接続前のマルウェア検査と必要な書込み制御を行う。

エ：マルウェア対策ソフトがあるので、媒体管理は不要とする。

答え・解説 正答：ウ

ア：私物媒体の自由利用は管理外の感染経路になります。

イ：人の記憶だけでは追跡性が不足します。

ウ：許可媒体、利用記録、検査、必要な制御を組み合わせることで媒体経由のリスクを低減できます。

エ：マルウェア対策だけでは紛失・不正持出し等の媒体リスクをカバーできません。

総合解説：可搬媒体では、マルウェアだけでなく、持出し、紛失、改ざん、追跡性も含めて管理します。

対象：2026年度 / 基準日 2026-09-05

0044 システム利用・管理策事例 > メール・Web・モバイル・媒体管理 ｜ 難易度：標準

O社では製造現場の装置へ設定ファイルを渡すためUSBメモリを使用している。
現場では私物USBも利用可能で、利用記録は取っていない。
最近、マルウェア感染した私物USBが持ち込まれた。

製造機密の設定ファイルをUSBへ保存する場合の運用として、最も適切なものはどれか。

ア：USB容量に余裕があるため、関連しない機密ファイルもまとめて保存する。

イ：持出し先が工場内なら、承認や返却確認は不要である。

ウ：紛失時の影響を減らすため、USBのラベルにパスワードを記載する。

エ：業務上必要なファイルだけを保存し、持出し承認、暗号化、返却・消去を管理する。

答え・解説 正答：エ

ア：不要な情報を載せると漏えい時の影響を拡大します。

イ：工場内でも紛失や不正利用は起こり得ます。

ウ：パスワードを媒体へ記載すると暗号化の保護効果を弱めます。

エ：必要最小限のデータ、承認、暗号化、返却・消去を組み合わせるのが適切です。

総合解説：媒体管理では、保存する情報の最小化と媒体のライフサイクル管理が重要です。

対象：2026年度 / 基準日 2026-09-05

0045 システム利用・管理策事例 > クラウド利用・セキュリティ要求事項 ｜ 難易度：標準

O社では製造現場の装置へ設定ファイルを渡すためUSBメモリを使用している。
現場では私物USBも利用可能で、利用記録は取っていない。
最近、マルウェア感染した私物USBが持ち込まれた。

USB利用を減らすためクラウド経由のファイル受渡しを検討する。必要な要求事項として最も適切なものはどれか。

ア：認証・権限制御、通信と保存の保護、操作ログ、共有期限、対象装置への安全な取込み方法を確認する。

イ：クラウドなら媒体紛失がないため、アクセス権やログは不要である。

ウ：共有URLを永久有効にし、誰でもアクセスできる設定にする。

エ：アップロード後のファイルは削除できないサービスを選び、履歴を残さない。

答え・解説 正答：ア

ア：媒体リスクが減っても、クラウドでは認証、共有、ログ、データ保護など別の管理が必要です。

イ：匿名・無期限共有は漏えいリスクを高めます。

ウ：削除・保持要件を管理できることは重要です。

エ：安全な取込み方法まで含めて全体のデータフローを設計します。

総合解説：媒体からクラウドへ手段を変えてもリスクが消えるわけではなく、リスクの種類が変わるため、新しい管理策を設計します。

対象：2026年度 / 基準日 2026-09-05

0046 システム利用・管理策事例 > アクセス・パッチ・ログ・バックアップ ｜ 難易度：標準

P社の公開Webサイトで、入力欄に不正な文字列を送る試行が多数観測された。
WAFは導入済みだが、アプリケーションは数年前から大きな改修がなく、
脆弱性診断も長期間実施していない。

最も適切な対応はどれか。

ア：WAFがあるのでアプリケーションに脆弱性があっても修正しない。

イ：WAFログを確認しつつ、アプリケーションの脆弱性診断と修正を行い、WAFだけに依存しない。

ウ：攻撃試行があるため公開サイトを永久停止し、原因調査は行わない。

エ：WAFのログ量を減らすため、検知機能を無効化する。

答え・解説 正答：イ

ア：WAFだけでは全ての攻撃を防げるとは限りません。

イ：WAFは補完策であり、アプリケーション自体の脆弱性を修正することが重要です。

ウ：永久停止は過剰で、影響評価と改善が必要です。

エ：検知を無効にすると攻撃状況の把握が困難になります。

総合解説：Webセキュリティは、アプリ修正、WAF、ログ監視、パッチなどの多層防御で考えます。

対象：2026年度 / 基準日 2026-09-05

0047 システム利用・管理策事例 > メール・Web・モバイル・媒体管理 ｜ 難易度：標準

P社の公開Webサイトで、入力欄に不正な文字列を送る試行が多数観測された。
WAFは導入済みだが、アプリケーションは数年前から大きな改修がなく、
脆弱性診断も長期間実施していない。

運用担当者が攻撃試行の急増を確認した場合の対応として、最も適切なものはどれか。

ア：ブロックされているように見えるため、ログを見ず誰にも報告しない。

イ：攻撃元IPを確認せず、全インターネット通信を遮断する。

ウ：定めた基準に従ってセキュリティ担当へ報告し、攻撃対象URLや送信元、成功兆候を分析する。

エ：ログをSNSへ公開し、外部の誰かに分析を依頼する。

答え・解説 正答：ウ

ア：WAFで一部ブロックされても回避や成功の可能性を確認する必要があります。

イ：全通信遮断は業務影響が大きく、状況に応じた判断が必要です。

ウ：攻撃の急増はインシデント兆候として、報告基準に従い分析・エスカレーションします。

エ：ログには機密情報が含まれる可能性があり、無制限公開は不適切です。

総合解説：科目Bでは、検知した事象を放置せず、組織の手順に沿って情報を集め、必要な関係者へ連携する判断が重要です。

対象：2026年度 / 基準日 2026-09-05

0048 システム利用・管理策事例 > クラウド利用・セキュリティ要求事項 ｜ 難易度：標準

P社の公開Webサイトで、入力欄に不正な文字列を送る試行が多数観測された。
WAFは導入済みだが、アプリケーションは数年前から大きな改修がなく、
脆弱性診断も長期間実施していない。

クラウドWAFサービスへ移行する場合、最も適切な確認事項はどれか。

ア：クラウドWAFを導入すれば、アプリケーションの脆弱性は自動的に修正される。

イ：サービス事業者がログを保持するなら、自社はアクセスできなくてもよい。

ウ：WAFがクラウドにあるため、障害時の連絡・復旧条件は契約で定めなくてよい。

エ：検知・遮断ルールの管理主体、ログ提供範囲、障害時の対応、アプリ側で残る脆弱性修正責任を明確にする。

答え・解説 正答：エ

ア：WAFはアプリのソースコードを自動修正するものではありません。

イ：自社の調査や監査に必要なログへのアクセスが重要です。

ウ：障害時の対応条件もサービス要件として確認します。

エ：サービス利用後も、WAF運用とアプリ修正の責任分界、ログ、可用性を明確にする必要があります。

総合解説：クラウド型セキュリティサービスでも、責任を丸投げせず、自社が担う管理と事業者が担う管理を明確にします。

対象：2026年度 / 基準日 2026-09-05

0049 システム利用・管理策事例 > アクセス・パッチ・ログ・バックアップ ｜ 難易度：標準

Q社では営業担当者が顧客一覧をメール添付で送付することがある。
最近、宛先のオートコンプリートで別会社の担当者を選び、顧客一覧を誤送信する事故が発生した。
添付ファイルには多数の顧客連絡先が含まれていた。

再発防止として最も適切な対策はどれか。

ア：大量・機密データのメール送信を必要最小限にし、宛先確認、承認又は安全な共有手段を組み合わせる。

イ：誤送信は人の注意不足だけが原因なので、システムや手順は変更しない。

ウ：全メールを暗号化すれば、誤った宛先へ送信しても漏えいにはならない。

エ：オートコンプリートを使う社員だけ処分し、データ送付方法はそのままにする。

答え・解説 正答：ア

ア：誤送信しやすい業務プロセス自体を見直し、データ量の最小化や安全な共有方式を含めて多層的に対策します。

イ：人の注意だけに依存すると再発しやすくなります。

ウ：誤った受信者が復号できる形なら暗号化だけでは誤送信を防げません。

エ：個人処分だけでは構造的な原因が残ります。

総合解説：人的ミスを前提に、誤操作が重大な漏えいへ発展しにくい仕組みを設計することが重要です。

対象：2026年度 / 基準日 2026-09-05

0050 システム利用・管理策事例 > メール・Web・モバイル・媒体管理 ｜ 難易度：標準

Q社では営業担当者が顧客一覧をメール添付で送付することがある。
最近、宛先のオートコンプリートで別会社の担当者を選び、顧客一覧を誤送信する事故が発生した。
添付ファイルには多数の顧客連絡先が含まれていた。

誤送信に気付いた直後の対応として、最も適切なものはどれか。

ア：本人だけで解決しようとして上司やセキュリティ担当へ報告しない。

イ：社内の報告手順に従って速やかに連絡し、送信内容・宛先・件数を確認し、受信者への削除依頼など必要な措置を行う。

ウ：送信済みメールを自分の送信済みフォルダから削除すれば事故は解消する。

エ：誤送信した事実を隠すため、受信者へ別メールを大量送信して埋もれさせる。

答え・解説 正答：イ

ア：本人だけで処理すると組織として必要な対応が遅れる可能性があります。

イ：早期報告により影響範囲の把握、受信者対応、法的・契約上の判断を迅速に行えます。

ウ：自分のフォルダから削除しても相手に届いたメールは消えません。

エ：隠蔽行為は被害や信頼問題を拡大します。

総合解説：メール誤送信も情報セキュリティインシデントとして、事実確認・報告・影響低減・再発防止を行います。

対象：2026年度 / 基準日 2026-09-05

0051 システム利用・管理策事例 > クラウド利用・セキュリティ要求事項 ｜ 難易度：標準

Q社では営業担当者が顧客一覧をメール添付で送付することがある。
最近、宛先のオートコンプリートで別会社の担当者を選び、顧客一覧を誤送信する事故が発生した。
添付ファイルには多数の顧客連絡先が含まれていた。

メール添付を減らすため法人向けファイル共有SaaSを導入する。最も重要な要求事項の組合せはどれか。

ア：匿名リンクを永久有効にでき、管理者は共有状況を確認できないこと

イ：個人メールアドレスで自由登録でき、会社側では利用者を削除できないこと

ウ：利用者認証、共有相手の制限、共有期限、ダウンロード制御、操作ログ、管理者による失効機能

エ：共有後は権限変更できず、ログも取得できないこと

答え・解説 正答：ウ

ア：匿名・永久リンクは漏えい時の制御が難しくなります。

イ：個人管理では退職・異動時の統制が困難です。

ウ：安全な共有には、誰が誰へ何をいつまで共有するかを組織が制御・追跡できる機能が重要です。

エ：失効やログがないと誤共有時の影響低減と調査が難しくなります。

総合解説：SaaS選定では、利便性だけでなく、誤共有時に組織が権限を取り消し、利用状況を追跡できることを確認します。

対象：2026年度 / 基準日 2026-09-05

0052 システム利用・管理策事例 > アクセス・パッチ・ログ・バックアップ ｜ 難易度：標準

R社では営業担当者へスマートフォンを支給し、メール、チャット、CRMを利用させている。
一部端末ではOS更新が長期間行われておらず、紛失時の遠隔ワイプも設定されていない。
端末には顧客とのチャット履歴が残る。

最も適切な端末管理はどれか。

ア：端末は携帯電話なので、PCと異なり更新や暗号化は不要である。

イ：利用者ごとに任意設定とし、組織は端末状態を把握しない。

ウ：紛失時は新品を支給すればよいので、保存データ対策はしない。

エ：MDM等でOS更新状況、画面ロック、暗号化、遠隔ロック・ワイプを組織的に管理する。

答え・解説 正答：エ

ア：スマートフォンも脆弱性やデータ漏えいのリスクがあります。

イ：個人任せでは基準の統一と確認が困難です。

ウ：端末代替だけでは保存情報の漏えいを防げません。

エ：企業利用のモバイル端末では、更新、暗号化、認証、遠隔管理などを組織的に統制することが有効です。

総合解説：モバイル端末は常時持ち出されるため、紛失と脆弱性の両方を前提に集中管理します。

対象：2026年度 / 基準日 2026-09-05

0053 システム利用・管理策事例 > メール・Web・モバイル・媒体管理 ｜ 難易度：標準

R社では営業担当者へスマートフォンを支給し、メール、チャット、CRMを利用させている。
一部端末ではOS更新が長期間行われておらず、紛失時の遠隔ワイプも設定されていない。
端末には顧客とのチャット履歴が残る。

CRMの顧客データを端末へ保存する際の運用として、最も適切なものはどれか。

ア：業務上必要な範囲だけを端末へ保持し、可能ならサーバ側参照を優先し、ローカル保存期間を制限する。

イ：通信できない場合に備え、全顧客データを全端末へ常時保存する。

ウ：便利なので、会社端末から私物クラウドへ顧客一覧を同期する。

エ：端末暗号化があれば、保存するデータ量や保持期間は考慮しなくてよい。

答え・解説 正答：ア

ア：端末紛失時の影響を抑えるため、保持する情報を最小化することが有効です。

イ：全顧客データを全端末へ持つと露出範囲が大きくなります。

ウ：私物クラウドへの同期は組織管理外となります。

エ：暗号化は重要ですが、データ最小化を不要にはしません。

総合解説：モバイル利用では、端末保護に加えて、端末へ何をどれだけ保存するかも重要な管理点です。

対象：2026年度 / 基準日 2026-09-05

0054 システム利用・管理策事例 > クラウド利用・セキュリティ要求事項 ｜ 難易度：標準

R社では営業担当者へスマートフォンを支給し、メール、チャット、CRMを利用させている。
一部端末ではOS更新が長期間行われておらず、紛失時の遠隔ワイプも設定されていない。
端末には顧客とのチャット履歴が残る。

新しいCRM SaaSのモバイル機能を選定する際、最も適切な要求事項はどれか。

ア：スマートフォンの電話番号だけで本人確認できれば、他の認証は不要である。

イ：多要素認証、端末制御、セッション失効、アクセスログ、管理者による利用停止などを確認する。

ウ：モバイルアプリではログを残さず、利用者のプライバシーだけを優先する。

エ：退職者のアプリ利用を管理者が停止できなくても、パスワード変更を本人に任せればよい。

答え・解説 正答：イ

ア：電話番号だけでは本人確認として十分でない場合があります。

イ：モバイルSaaSでも、強い認証、端末・セッション管理、ログ、アカウント停止が重要です。

ウ：監査・不正検知に必要なログを適切に取得します。

エ：退職時に組織がアクセスを停止できることが必要です。

総合解説：クラウドサービスのモバイル利用では、組織が利用者・端末・セッションを管理できるかを事前に確認します。

対象：2026年度 / 基準日 2026-09-05

0055 システム利用・管理策事例 > アクセス・パッチ・ログ・バックアップ ｜ 難易度：応用

S社ではDB管理者が本番データベースへ直接アクセスできる。
管理者操作ログは取得しているが、ログファイルはDB管理者自身が削除できる場所に保存されている。
最近、顧客レコードが削除されたが、操作主体を特定できなかった。

最も適切な改善策はどれか。

ア：ログを同じDB内だけに保存し、管理者には全削除権限を与える。

イ：管理者を信頼してログ取得を停止する。

ウ：特権操作ログを管理対象サーバとは分離した保管先へ転送し、DB管理者が容易に改ざん・削除できないようアクセスを分離する。

エ：ログファイル名を複雑にすれば、同じ権限で削除できても十分である。

答え・解説 正答：ウ

ア：同一権限で削除できると不正の隠蔽が可能です。

イ：ログ停止は追跡性を失います。

ウ：ログの証拠価値を保つには、監視対象者が容易に消せないよう分離・保護することが重要です。

エ：ファイル名の難読化はアクセス制御の代替ではありません。

総合解説：特権ユーザの活動は高リスクであるため、ログの完全性と独立したレビューを確保します。

対象：2026年度 / 基準日 2026-09-05

0056 システム利用・管理策事例 > メール・Web・モバイル・媒体管理 ｜ 難易度：応用

S社ではDB管理者が本番データベースへ直接アクセスできる。
管理者操作ログは取得しているが、ログファイルはDB管理者自身が削除できる場所に保存されている。
最近、顧客レコードが削除されたが、操作主体を特定できなかった。

DB管理者による内部不正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：管理者は専門職なので、特権の定期レビューや監視は行わない。

イ：不正を疑うと士気が下がるため、特権操作の記録を禁止する。

ウ：全開発者へ同じDB管理者権限を付け、相互に監視させる。

エ：特権付与を必要最小限にし、重要操作を定期レビューし、必要に応じて承認や職務分掌を設ける。

答え・解説 正答：エ

ア：専門性の高さは統制不要の理由になりません。

イ：記録をなくすと不正検知と説明責任が困難です。

ウ：権限の拡大は不正・誤操作リスクを高めます。

エ：最小権限、職務分掌、独立レビュー、ログは内部不正の機会を低減します。

総合解説：内部不正対策では、個人の信頼だけでなく、権限・証跡・相互牽制を組織的に設計します。

対象：2026年度 / 基準日 2026-09-05

0057 システム利用・管理策事例 > クラウド利用・セキュリティ要求事項 ｜ 難易度：応用

S社ではDB管理者が本番データベースへ直接アクセスできる。
管理者操作ログは取得しているが、ログファイルはDB管理者自身が削除できる場所に保存されている。
最近、顧客レコードが削除されたが、操作主体を特定できなかった。

マネージドDBへ移行する場合の監査要件として、最も適切なものはどれか。

ア：管理操作とデータアクセスのログ取得範囲、事業者側管理者の統制、ログ保持・出力方法を確認する。

イ：マネージドサービスなら管理者不正は起こらないので、監査ログは不要である。

ウ：ログは事業者だけが閲覧できればよく、自社の監査要件は考慮しない。

エ：サービス仕様に監査ログがなくても、価格が安ければ選定する。

答え・解説 正答：ア

ア：マネージドDBでも自社・事業者双方の管理操作に関する監査可能性を確認する必要があります。

イ：外部委託で内部不正リスクが消えるわけではありません。

ウ：自社の監査・調査に必要なログへアクセスできることが重要です。

エ：監査ログは重要なセキュリティ要求事項です。

総合解説：クラウド利用では、見えなくなる管理領域が増えるため、事業者の統制とログ提供能力を契約前に確認します。

対象：2026年度 / 基準日 2026-09-05

0058 システム利用・管理策事例 > アクセス・パッチ・ログ・バックアップ ｜ 難易度：応用

T社は在宅勤務者向けにVPNを提供している。
利用者はIDとパスワードだけで接続でき、私物PCからの接続も許可されている。
ある利用者の認証情報がフィッシングで窃取され、不審な海外IPからVPN接続があった。

再発防止として最も適切な対策はどれか。

ア：パスワードを1文字だけ長くし、他の対策は行わない。

イ：VPNに多要素認証を導入し、接続端末の要件を定め、異常な接続元や時間帯を監視する。

ウ：認証情報が盗まれてもVPNは暗号化されるので問題ない。

エ：全利用者で同じVPNアカウントを使い、個別IDを廃止する。

答え・解説 正答：イ

ア：パスワード強化だけではフィッシングで窃取された場合のリスクが残ります。

イ：認証情報窃取への耐性を高める多要素認証と、端末・ログの管理を組み合わせます。

ウ：VPN暗号化は通信保護であり、盗まれた認証情報の不正利用を防ぎません。

エ：共有IDは本人識別と追跡性を低下させます。

総合解説：リモートアクセスでは、強い認証、端末の信頼性、接続ログ監視を組み合わせて不正接続を防ぎます。

対象：2026年度 / 基準日 2026-09-05

0059 システム利用・管理策事例 > メール・Web・モバイル・媒体管理 ｜ 難易度：応用

T社は在宅勤務者向けにVPNを提供している。
利用者はIDとパスワードだけで接続でき、私物PCからの接続も許可されている。
ある利用者の認証情報がフィッシングで窃取され、不審な海外IPからVPN接続があった。

利用者教育として最も適切な内容はどれか。

ア：一度入力したパスワードは変更すると覚えにくくなるため、被害後も使い続ける。

イ：不審メールは確認のため同僚へそのまま転送し、全員でリンクを開く。

ウ：不審な認証要求に資格情報を入力しないこと、誤入力した場合は直ちに報告して認証情報を変更することを周知する。

エ：フィッシングは技術部門だけの問題なので、一般利用者への教育は行わない。

答え・解説 正答：ウ

ア：漏えいした認証情報を使い続けるのは危険です。

イ：不審なリンクの共有は被害を拡大する可能性があります。

ウ：利用者が早期に気付き、報告・変更できることは被害拡大防止に重要です。

エ：利用者が攻撃対象になるため、教育は重要です。

総合解説：フィッシング対策は、技術的な防御だけでなく、利用者が不審事象を認識し迅速に報告できる運用が必要です。

対象：2026年度 / 基準日 2026-09-05

0060 システム利用・管理策事例 > クラウド利用・セキュリティ要求事項 ｜ 難易度：応用

T社は在宅勤務者向けにVPNを提供している。
利用者はIDとパスワードだけで接続でき、私物PCからの接続も許可されている。
ある利用者の認証情報がフィッシングで窃取され、不審な海外IPからVPN接続があった。

VPNの代替としてクラウド型リモートアクセスサービスを選定する際、最も適切な要求事項はどれか。

ア：クラウドサービスなら認証機能の確認は不要である。

イ：接続ログを利用者が削除できることを必須要件にする。

ウ：障害時は全社員が個人用リモート操作ソフトを使えるようにする。

エ：多要素認証、利用者・端末ごとのアクセス制御、接続ログ、可用性、障害時の代替手段を確認する。

答え・解説 正答：エ

ア：クラウド利用でも認証の強度は重要です。

イ：利用者がログを削除できると監査・調査能力が低下します。

ウ：管理外の個人用ツールは新たなリスクを生みます。

エ：クラウド型アクセスでも認証、端末、ログ、可用性を要件化することが重要です。

総合解説：リモートアクセス方式を変更するときは、セキュリティ機能だけでなく、可用性と障害時運用も含めて評価します。

対象：2026年度 / 基準日 2026-09-05

0061 委託・継続事例 > 委託先評価・契約・要求事項 ｜ 難易度：基礎

U社は給与計算を外部SaaSへ切り替える予定である。
委託先には従業員の氏名、住所、銀行口座、給与額を預ける。
候補サービスの一つは低価格だが、事故時の連絡時間やデータ返却方法が契約書に明記されていない。

委託先選定時の対応として、最も適切なものはどれか。

ア：セキュリティ体制、アクセス制御、事故対応、データ保護、再委託などを事前評価し、必要事項を契約で明確にする。

イ：価格が最安ならセキュリティ評価を省略する。

ウ：SaaSなので委託先へ預けたデータの管理責任は全て消滅する。

エ：契約締結後に問題が起きてから要求事項を決める。

答え・解説 正答：ア

ア：重要な個人情報を扱う委託では、事前評価と契約による要求事項の明確化が必要です。

イ：価格だけではリスクを評価できません。

ウ：外部委託しても自社側の委託管理責任がなくなるわけではありません。

エ：重要条件は契約前に確認する必要があります。

総合解説：委託先管理では、選定前の評価、契約、運用中の確認、終了時のデータ処理まで一連で管理します。

対象：2026年度 / 基準日 2026-09-05

0062 委託・継続事例 > 委託先監督・更新・終了 ｜ 難易度：基礎

U社は給与計算を外部SaaSへ切り替える予定である。
委託先には従業員の氏名、住所、銀行口座、給与額を預ける。
候補サービスの一つは低価格だが、事故時の連絡時間やデータ返却方法が契約書に明記されていない。

契約更新又は終了に備えて、あらかじめ定めておく事項として最も適切なものはどれか。

ア：契約終了後も委託先が自由にデータを保持できるようにする。

イ：データの返却形式、移行支援、契約終了後の削除時期・削除確認、アカウント無効化を定める。

ウ：終了時の移行は必ず即日できると仮定し、手順や期間を定めない。

エ：アカウントは将来再契約する可能性があるため無期限に残す。

答え・解説 正答：イ

ア：利用目的を失ったデータを無期限保持させるのは不適切です。

イ：終了時のデータ返却・移行・削除・アクセス停止は、委託管理の重要事項です。

ウ：移行には時間や形式上の制約があるため事前設計が必要です。

エ：不要アカウントの残存は不正アクセスの機会を残します。

総合解説：委託は契約締結時だけでなく、更新・終了まで含めたライフサイクルで管理します。

対象：2026年度 / 基準日 2026-09-05

0063 委託・継続事例 > BCP・障害・災害時の継続判断 ｜ 難易度：基礎

U社は給与計算を外部SaaSへ切り替える予定である。
委託先には従業員の氏名、住所、銀行口座、給与額を預ける。
候補サービスの一つは低価格だが、事故時の連絡時間やデータ返却方法が契約書に明記されていない。

SaaS障害が給与支払日前に発生する場合を想定した継続策として、最も適切なものはどれか。

ア：給与業務は月1回なので、障害時の代替手順は不要である。

イ：SaaSの可用性は委託先だけの責任なので、自社BCPでは扱わない。

ウ：給与支払の重要期限を踏まえて復旧目標を決め、代替手順や必要データの確保、連絡体制を準備する。

エ：障害時は復旧時刻を確認せず、従業員への連絡もしない。

答え・解説 正答：ウ

ア：頻度が低くても期限を逃す影響は大きくなり得ます。

イ：委託サービスの停止も自社事業継続へ影響します。

ウ：重要期限のある業務は、許容停止時間と代替手順を事前に設計する必要があります。

エ：関係者への連絡も継続計画の一部です。

総合解説：外部サービスを使う重要業務では、委託先の復旧能力と自社の代替手段を組み合わせてBCPを設計します。

対象：2026年度 / 基準日 2026-09-05

0064 委託・継続事例 > 委託先評価・契約・要求事項 ｜ 難易度：基礎

V社は顧客サポート業務をコールセンター会社へ委託する。
委託先オペレータはV社の顧客管理システムを閲覧する必要がある。
候補会社からは「従業員教育は実施している」と説明されたが、具体的な証跡はまだ確認していない。

委託先評価として、最も適切な対応はどれか。

ア：口頭で「教育している」と説明されたので、それ以上確認しない。

イ：有名企業であればセキュリティ対策の確認は不要である。

ウ：委託開始後に事故が起きるまで証跡確認を延期する。

エ：教育記録、アクセス管理手順、監査結果など客観的な証跡を確認し、必要に応じて追加質問や改善要求を行う。

答え・解説 正答：エ

ア：口頭説明だけでは実効性を十分に確認できません。

イ：企業規模や知名度だけでリスクは判断できません。

ウ：開始前に重要な管理状況を確認する必要があります。

エ：委託先評価では自己申告だけでなく、必要な証跡を確認して実施状況を評価します。

総合解説：委託先のセキュリティ評価は、質問票だけでなく、証跡や第三者評価などを用いて実効性を確認します。

対象：2026年度 / 基準日 2026-09-05

0065 委託・継続事例 > 委託先監督・更新・終了 ｜ 難易度：基礎

V社は顧客サポート業務をコールセンター会社へ委託する。
委託先オペレータはV社の顧客管理システムを閲覧する必要がある。
候補会社からは「従業員教育は実施している」と説明されたが、具体的な証跡はまだ確認していない。

委託開始後の監督として最も適切なものはどれか。

ア：委託先の在籍者と発行アカウントを定期照合し、異動・退職時の停止状況やアクセスログを確認する。

イ：契約時にアカウント一覧を確認したので、以後は契約終了まで確認しない。

ウ：委託先の人事異動は委託元に関係ないため、アカウント削除状況を確認しない。

エ：利便性のため委託先全員へ同じ共有IDを付与する。

答え・解説 正答：ア

ア：委託先の要員は変化するため、アカウントの継続的な棚卸しとログ確認が必要です。

イ：契約時の確認だけでは退職者権限の残存を検知できません。

ウ：委託先要員の変更はアクセス権に直結します。

エ：共有IDは追跡性を下げます。

総合解説：委託先監督では、契約時に定めた要求事項が運用中も維持されているかを確認します。

対象：2026年度 / 基準日 2026-09-05

0066 委託・継続事例 > BCP・障害・災害時の継続判断 ｜ 難易度：基礎

V社は顧客サポート業務をコールセンター会社へ委託する。
委託先オペレータはV社の顧客管理システムを閲覧する必要がある。
候補会社からは「従業員教育は実施している」と説明されたが、具体的な証跡はまだ確認していない。

委託先拠点が災害で停止した場合の継続策として、最も適切なものはどれか。

ア：コールセンターが停止したら、復旧するまで顧客からの連絡を全て拒否する。

イ：重要な問い合わせの優先順位を定め、代替拠点・在宅対応・自社での暫定受付など複数の代替手段を準備する。

ウ：委託先がBCPを持っていると聞いたので、自社側の連絡方法や代替策は考えない。

エ：災害時は全ての問い合わせを通常時と同じSLAで処理するとだけ決め、資源配分は検討しない。

答え・解説 正答：イ

ア：全停止は顧客影響を拡大します。

イ：重要業務を優先し、代替チャネルや拠点を事前に準備するのが適切です。

ウ：委託先BCPだけでなく自社側の連携・代替策も必要です。

エ：限られた資源では重要業務の優先順位が必要です。

総合解説：委託業務のBCPでは、委託先の計画と自社の顧客対応・意思決定を接続して設計します。

対象：2026年度 / 基準日 2026-09-05

0067 委託・継続事例 > 委託先評価・契約・要求事項 ｜ 難易度：基礎

W社は新しい会員アプリの開発をベンダへ委託する。
要件定義書には機能要件は詳しく書かれているが、認証強度、ログ、脆弱性対応、データ削除などの
セキュリティ要求は「適切に対応する」としか書かれていない。

契約前に行うべき対応として、最も適切なものはどれか。

ア：「適切に対応する」という表現があれば、具体的要件は不要である。

イ：セキュリティは開発完了後に考えるため、要件定義では扱わない。

ウ：認証、権限、ログ、脆弱性修正期限、テスト、データ取扱いなどを検証可能な要求事項として具体化する。

エ：ベンダの一般的な実績だけを確認し、今回システム固有の要求は定めない。

答え・解説 正答：ウ

ア：曖昧な表現では合否判断や責任分界が困難です。

イ：セキュリティは設計初期から考慮する必要があります。

ウ：検収や運用時に確認できるよう、セキュリティ要求を具体的・検証可能にする必要があります。

エ：システム固有のデータ・リスクに応じた要求が必要です。

総合解説：開発委託では、セキュリティ要求を要件・契約へ明示し、受入れ時に確認できる形にします。

対象：2026年度 / 基準日 2026-09-05

0068 委託・継続事例 > 委託先監督・更新・終了 ｜ 難易度：基礎

W社は新しい会員アプリの開発をベンダへ委託する。
要件定義書には機能要件は詳しく書かれているが、認証強度、ログ、脆弱性対応、データ削除などの
セキュリティ要求は「適切に対応する」としか書かれていない。

開発途中でベンダが再委託先を追加したいと申し出た。最も適切な対応はどれか。

ア：ベンダの判断に全て任せ、再委託先の名称も確認しない。

イ：再委託は必ず危険なので、理由に関係なく全て禁止する。

ウ：再委託先が海外企業でなければ、セキュリティ評価は不要とする。

エ：契約上の再委託条件を確認し、再委託先の役割・データアクセス・セキュリティ対策を評価して承認判断する。

答え・解説 正答：エ

ア：丸投げするとサプライチェーンリスクを把握できません。

イ：一律禁止では業務上合理的な再委託まで排除します。

ウ：所在地だけでリスクの有無は決まりません。

エ：再委託ではデータや権限の範囲が変わるため、契約条件とリスクを確認して判断します。

総合解説：委託先の変更・再委託は、当初のリスク評価が変化するイベントとして管理します。

対象：2026年度 / 基準日 2026-09-05

0069 委託・継続事例 > BCP・障害・災害時の継続判断 ｜ 難易度：基礎

W社は新しい会員アプリの開発をベンダへ委託する。
要件定義書には機能要件は詳しく書かれているが、認証強度、ログ、脆弱性対応、データ削除などの
セキュリティ要求は「適切に対応する」としか書かれていない。

開発ベンダが倒産・事業停止した場合に備えた対策として、最も適切なものはどれか。

ア：ソースコード、設計書、構成情報、アカウント管理情報の引渡し条件と、自社又は代替ベンダが保守を継続できる体制を準備する。

イ：ベンダが存続することを前提にし、成果物の引渡し条件は定めない。

ウ：ソースコードはベンダだけが保持し、自社は実行ファイルだけ受け取る。

エ：事業停止時にはシステムを直ちに廃止するとだけ決め、顧客影響は評価しない。

答え・解説 正答：ア

ア：重要システムでは、委託先停止時にも保守・復旧できるよう必要な成果物と権限を確保します。

イ：単一ベンダへの過度な依存は継続リスクになります。

ウ：実行ファイルだけでは修正・保守が困難な場合があります。

エ：廃止による事業影響を評価せず決めるのは不適切です。

総合解説：外部開発では、契約終了や委託先事業停止を想定した移行可能性・保守継続性も重要な要求です。

対象：2026年度 / 基準日 2026-09-05

0070 委託・継続事例 > 委託先評価・契約・要求事項 ｜ 難易度：標準

X社は購買履歴データの分析を外部会社へ委託する。
分析会社は「精度向上のため全顧客データが必要」と説明しているが、
実際の分析では顧客氏名や住所を直接使わない。

委託時のデータ提供方法として、最も適切なものはどれか。

ア：委託先が希望するなら目的に関係なく全顧客情報を提供する。

イ：分析目的に不要な氏名・住所などを除外又は仮名化し、必要最小限のデータだけを提供する。

ウ：分析業務なので契約上のデータ利用目的は定めなくてよい。

エ：データ量が多いほど安全性も高まるので、可能な限り多く渡す。

答え・解説 正答：イ

ア：委託先の希望だけで不要情報を渡すのは不適切です。

イ：委託目的に必要な範囲へデータを限定すると、漏えい時の影響を低減できます。

ウ：利用目的・取扱条件を契約で明確にする必要があります。

エ：データ量が増えるほど漏えい時の影響が大きくなる可能性があります。

総合解説：委託では、必要性を基準に提供データを最小化し、利用目的とアクセス範囲を明確にします。

対象：2026年度 / 基準日 2026-09-05

0071 委託・継続事例 > 委託先監督・更新・終了 ｜ 難易度：標準

X社は購買履歴データの分析を外部会社へ委託する。
分析会社は「精度向上のため全顧客データが必要」と説明しているが、
実際の分析では顧客氏名や住所を直接使わない。

委託中の確認として最も適切なものはどれか。

ア：契約締結後は委託先を信頼し、データ利用状況は一切確認しない。

イ：分析結果が良ければ、元データを別目的で使っても問題ない。

ウ：契約で定めた目的外利用の禁止、アクセス権、保管場所、再委託、削除期限の順守状況を定期的に確認する。

エ：委託先の再委託は自社に関係ないので確認しない。

答え・解説 正答：ウ

ア：成果品質とデータ利用の適法・適切性は別です。

イ：目的外利用を許すと管理できません。

ウ：委託中も、契約した条件が守られているかを継続的に確認する必要があります。

エ：再委託はデータ流通範囲を変えるため重要な確認事項です。

総合解説：委託先監督は一度の審査ではなく、運用状況や変更を継続的に把握する活動です。

対象：2026年度 / 基準日 2026-09-05

0072 委託・継続事例 > BCP・障害・災害時の継続判断 ｜ 難易度：標準

X社は購買履歴データの分析を外部会社へ委託する。
分析会社は「精度向上のため全顧客データが必要」と説明しているが、
実際の分析では顧客氏名や住所を直接使わない。

分析会社のシステム障害で月次分析ができなくなった。業務影響を抑えるための事前対策として最も適切なものはどれか。

ア：分析業務は外部委託なので、自社では停止影響を評価しない。

イ：障害時は必ず完全復旧まで全ての意思決定を停止する。

ウ：代替手順を作ると本番手順と混乱するため、何も準備しない。

エ：分析結果の必要期限と停止許容時間を明確にし、必要なら前回結果の暫定利用や代替分析手順を準備する。

答え・解説 正答：エ

ア：外部委託は事業影響を消しません。

イ：完全停止より、許容される暫定手段があれば活用できます。

ウ：平時に代替手順を明確にしておくことで混乱を減らせます。

エ：委託業務でも自社の経営判断へ影響するため、許容停止時間と代替手段を準備します。

総合解説：事業継続では、外部サービス停止時に何をどこまで暫定運用できるかを事前に決めます。

対象：2026年度 / 基準日 2026-09-05

0073 委託・継続事例 > 委託先評価・契約・要求事項 ｜ 難易度：標準

Y社は24時間のセキュリティ監視をMSPへ委託する。
MSPはY社のFW・EDR・クラウドログを閲覧し、重大アラート時に連絡する。
候補契約には「重大」の定義と連絡期限が明確に書かれていない。

契約で明確にすべき事項として最も適切なものはどれか。

ア：重大度の判定基準、監視時間、連絡期限、連絡先、エスカレーション、ログ取扱いと責任分界を定める。

イ：監視を委託するので、自社のCSIRTや連絡先は定めなくてよい。

ウ：重大度は担当者の感覚で毎回決めればよい。

エ：連絡期限を決めるとMSPの負担になるため、無期限とする。

答え・解説 正答：ア

ア：監視サービスの品質と初動速度を確保するには、判定基準と連絡条件を具体化する必要があります。

イ：委託後も自社側の受け手と意思決定体制が必要です。

ウ：曖昧な重大度では対応の一貫性が保てません。

エ：連絡期限は重大インシデントの対応速度に直結します。

総合解説：監視委託では、何を検知し、どの条件で、誰へ、何分以内に連絡するかを検証可能なサービス条件として定めます。

対象：2026年度 / 基準日 2026-09-05

0074 委託・継続事例 > 委託先監督・更新・終了 ｜ 難易度：標準

Y社は24時間のセキュリティ監視をMSPへ委託する。
MSPはY社のFW・EDR・クラウドログを閲覧し、重大アラート時に連絡する。
候補契約には「重大」の定義と連絡期限が明確に書かれていない。

委託開始後の監督として最も適切なものはどれか。

ア：契約を締結したので、サービス実績を確認する必要はない。

イ：月次で検知件数、通知遅延、未処理アラート、誤検知、改善事項をレビューし、契約条件との差異を確認する。

ウ：通知件数が少なければ安全と判断し、ログや検知ルールは確認しない。

エ：MSPが自己評価で満点なら、自社側のレビューは不要とする。

答え・解説 正答：イ

ア：契約後の監督は継続的に必要です。

イ：サービス実績を定量・定性の両面から確認し、要求との差異を改善します。

ウ：通知件数の少なさは検知漏れの可能性もあり、安全の証拠ではありません。

エ：自己評価だけでなく自社の要求に照らした確認が必要です。

総合解説：委託先監督では、SLAやKPIだけでなく、実際の検知品質・改善状況を継続評価します。

対象：2026年度 / 基準日 2026-09-05

0075 委託・継続事例 > BCP・障害・災害時の継続判断 ｜ 難易度：標準

Y社は24時間のセキュリティ監視をMSPへ委託する。
MSPはY社のFW・EDR・クラウドログを閲覧し、重大アラート時に連絡する。
候補契約には「重大」の定義と連絡期限が明確に書かれていない。

MSP側の障害で監視サービスが停止した場合に備えた対策として、最も適切なものはどれか。

ア：MSP停止中は攻撃も発生しないとみなし、監視を完全に停止する。

イ：障害時の連絡先は通常窓口だけとし、緊急連絡先は設けない。

ウ：自社で最低限確認するログ・アラート、代替連絡先、復旧見込みの確認手順を決め、必要なら代替監視手段を用意する。

エ：復旧するまでログ保存も止め、容量を節約する。

答え・解説 正答：ウ

ア：サービス停止は攻撃停止を意味しません。

イ：緊急時の連絡経路を準備する必要があります。

ウ：監視委託が停止しても攻撃リスクは継続するため、最低限の代替監視やログ保存が必要です。

エ：ログ停止は後日の検知・調査能力を失わせます。

総合解説：重要なセキュリティサービス自体もBCPの対象であり、停止時の代替能力を設計します。

対象：2026年度 / 基準日 2026-09-05

0076 委託・継続事例 > 委託先評価・契約・要求事項 ｜ 難易度：標準

Z社は基幹サーバを外部データセンターへ設置している。
契約には電源冗長化の記載があるが、復旧時間の目標や災害時の連絡方法は曖昧である。
Z社の受注業務は長時間停止すると大きな損失が出る。

委託先との契約で追加すべき事項として最も適切なものはどれか。

ア：電源冗長化の記載だけで全ての可用性リスクをカバーできる。

イ：災害は不可抗力なので、連絡や復旧条件を契約に定める意味はない。

ウ：停止損失は自社側の問題なので、委託先の復旧条件を確認しない。

エ：サービス停止時の連絡、復旧目標、保守計画、冗長化範囲、障害報告と責任分界を明確にする。

答え・解説 正答：エ

ア：電源だけで全障害を防げません。

イ：不可抗力でも連絡・復旧手順は重要です。

ウ：自社の事業影響に合わせて委託条件を確認します。

エ：可用性は電源以外にも通信、設備、運用、復旧体制など複数要因で決まるため、具体的なサービス条件が必要です。

総合解説：重要業務を支える外部インフラでは、技術仕様だけでなく、障害時のサービス条件と連絡体制を契約へ反映します。

対象：2026年度 / 基準日 2026-09-05

0077 委託・継続事例 > 委託先監督・更新・終了 ｜ 難易度：標準

Z社は基幹サーバを外部データセンターへ設置している。
契約には電源冗長化の記載があるが、復旧時間の目標や災害時の連絡方法は曖昧である。
Z社の受注業務は長時間停止すると大きな損失が出る。

データセンター事業者から設備構成変更の通知があった。最も適切な対応はどれか。

ア：自社サービスへの影響、冗長性、保守時間、契約要件への適合を確認し、必要なテストや計画更新を行う。

イ：委託先の設備変更は自社に関係ないため、通知を破棄する。

ウ：変更後に障害が起きるまで影響を確認しない。

エ：設備構成が変わったら必ず契約を解除し、評価は行わない。

答え・解説 正答：ア

ア：委託先の変更が自社リスクや可用性へ影響するかを評価し、必要な対応を行います。

イ：外部設備でも自社システムを支えるなら影響があります。

ウ：事後だけでなく変更前の評価が重要です。

エ：変更＝即解約ではなく、リスクと契約適合性を判断します。

総合解説：委託先監督では、契約時の状態だけでなく、サービスや設備の変更を継続的に管理します。

対象：2026年度 / 基準日 2026-09-05

0078 委託・継続事例 > BCP・障害・災害時の継続判断 ｜ 難易度：標準

Z社は基幹サーバを外部データセンターへ設置している。
契約には電源冗長化の記載があるが、復旧時間の目標や災害時の連絡方法は曖昧である。
Z社の受注業務は長時間停止すると大きな損失が出る。

大規模災害でデータセンターが長時間利用不能になる場合に備え、最も適切な対策はどれか。

ア：災害は頻度が低いので、復旧戦略は作らない。

イ：業務のRTO・RPOを基に代替サイトやクラウド復旧などの復旧戦略を決め、切替訓練を行う。

ウ：バックアップがあれば、復旧先や切替手順は考えなくてよい。

エ：RTOを決めず、復旧できた時点を目標時刻とする。

答え・解説 正答：イ

ア：低頻度でも影響が大きい災害は評価対象です。

イ：重要業務ではBIAに基づきRTO・RPOを定め、それを満たす復旧戦略と訓練が必要です。

ウ：バックアップだけでは稼働環境や切替手順を確保できません。

エ：目標がなければ必要な復旧能力を設計できません。

総合解説：災害復旧は、データのバックアップだけでなく、代替処理環境、通信、要員、切替手順まで含めます。

対象：2026年度 / 基準日 2026-09-05

0079 委託・継続事例 > 委託先評価・契約・要求事項 ｜ 難易度：標準

AA社は物流倉庫業務を外部企業へ委託している。
委託先はAA社の受注システムへ接続し、配送先情報を取得する。
委託先から、作業効率化のため個人所有タブレットからの接続を認めてほしいと要望があった。

この要望への対応として、最も適切なものはどれか。

ア：委託先の端末なので、自社システムへの接続条件は定めない。

イ：私物端末は必ず安全なので、端末状態の確認をせず許可する。

ウ：必要な端末要件、認証、暗号化、紛失対策、管理方法を評価し、基準を満たす端末だけ接続を許可する。

エ：効率化の要望がある場合は、情報の重要度に関係なく無条件で許可する。

答え・解説 正答：ウ

ア：私物か会社支給かだけで安全性は判断できません。

イ：業務効率と情報リスクを評価して条件を決めます。

ウ：委託先端末でも自社情報へアクセスするなら、接続条件と保護要件を定める必要があります。

エ：配送先情報を扱うため、認証・端末保護・紛失対策が重要です。

総合解説：委託先の利用環境も自社情報の処理環境の一部として捉え、必要なセキュリティ要求を契約・技術設定へ反映します。

対象：2026年度 / 基準日 2026-09-05

0080 委託・継続事例 > 委託先監督・更新・終了 ｜ 難易度：標準

AA社は物流倉庫業務を外部企業へ委託している。
委託先はAA社の受注システムへ接続し、配送先情報を取得する。
委託先から、作業効率化のため個人所有タブレットからの接続を認めてほしいと要望があった。

BYOD接続を条件付きで認めた後の監督として、最も適切なものはどれか。

ア：一度許可した端末は、OSが古くなっても契約終了まで使わせる。

イ：端末紛失は委託先だけの問題なので、自社への報告は不要とする。

ウ：アクセスログは委託先のプライバシー保護のため一切取得しない。

エ：許可端末一覧、OS更新状況、紛失報告、アクセスログなどを定期確認し、基準違反端末の接続を停止できるようにする。

答え・解説 正答：エ

ア：脆弱な端末の継続利用は自社情報へのリスクになります。

イ：紛失は顧客情報漏えいへつながる可能性があり、報告が必要です。

ウ：必要な範囲のアクセスログは監査・事故調査に重要です。

エ：端末状態は時間とともに変化するため、継続的な確認と接続停止手段が必要です。

総合解説：条件付き許可では、条件が継続して満たされているかを監督できる仕組みが必要です。

対象：2026年度 / 基準日 2026-09-05

0081 委託・継続事例 > BCP・障害・災害時の継続判断 ｜ 難易度：標準

AA社は物流倉庫業務を外部企業へ委託している。
委託先はAA社の受注システムへ接続し、配送先情報を取得する。
委託先から、作業効率化のため個人所有タブレットからの接続を認めてほしいと要望があった。

受注システム障害で委託倉庫が配送先を取得できなくなった場合の継続策として、最も適切なものはどれか。

ア：優先注文を定義し、必要最小限の配送情報を安全に代替連携する手順と、復旧後の差分反映手順を準備する。

イ：障害中は全出荷を停止し、復旧見込みや優先度を確認しない。

ウ：非常時は個人メールで全顧客データを委託先へ送る。

エ：代替手順は平時に試すと手間なので、災害当日に考える。

答え・解説 正答：ア

ア：重要業務を優先し、安全な代替連携と復旧後の整合を事前に設計することが適切です。

イ：全停止が必要かは事業影響に基づいて判断します。

ウ：個人メールで全顧客データを送るのは漏えいリスクが高い方法です。

エ：非常時手順は平時の訓練・確認が重要です。

総合解説：BCPでは、可用性だけでなく、非常時の情報セキュリティ水準を必要以上に低下させない代替手段を設計します。

対象：2026年度 / 基準日 2026-09-05

0082 委託・継続事例 > 委託先評価・契約・要求事項 ｜ 難易度：標準

AB社はメール配信業務をマーケティング会社へ委託している。
配信リストは毎月CSVで委託先へ渡している。
契約終了が決まり、委託先は「過去の配信分析のためデータを残したい」と申し出た。

委託開始時に契約で定めておくべき事項として、最も適切なものはどれか。

ア：配信件数だけ合えばよいので、データ取扱条件は定めない。

イ：利用目的、取扱担当者、再委託、保管期間、事故報告、契約終了時の返却・削除を明確にする。

ウ：顧客データは委託先へ渡した時点で自由利用を認める。

エ：契約終了時のデータ処理は委託先の裁量に任せる。

答え・解説 正答：イ

ア：成果だけでなくデータ管理も重要です。

イ：顧客データを委託する場合、利用目的から終了時削除までの条件を具体化する必要があります。

ウ：目的外利用を無制限に認めるのは不適切です。

エ：終了時の扱いは事前に定めるべき重要事項です。

総合解説：データ委託では、データの受渡しから廃棄までのライフサイクルを契約に反映します。

対象：2026年度 / 基準日 2026-09-05

0083 委託・継続事例 > 委託先監督・更新・終了 ｜ 難易度：標準

AB社はメール配信業務をマーケティング会社へ委託している。
配信リストは毎月CSVで委託先へ渡している。
契約終了が決まり、委託先は「過去の配信分析のためデータを残したい」と申し出た。

契約終了時の対応として、最も適切なものはどれか。

ア：委託先が分析に使いたいなら、期間を定めず保持を認める。

イ：自社からCSVを送らなくなれば、委託先に残るコピーは管理対象外とする。

ウ：契約で認めた保管期間と利用目的を確認し、不要な顧客データの削除を要求して削除完了の証跡を確認する。

エ：削除したという口頭説明だけを必ず十分な証拠とみなす。

答え・解説 正答：ウ

ア：委託先の希望だけで目的外・無期限保管を認めるのは不適切です。

イ：委託先保有コピーも自社データの委託管理対象です。

ウ：契約終了後に不要となるデータは、定めた条件に従って削除し、必要に応じて証跡で確認します。

エ：重要データでは削除報告や証明など客観的確認が有効です。

総合解説：委託終了時のデータ残存は見落とされやすいため、返却・削除・アカウント停止を明示的に確認します。

対象：2026年度 / 基準日 2026-09-05

0084 委託・継続事例 > BCP・障害・災害時の継続判断 ｜ 難易度：標準

AB社はメール配信業務をマーケティング会社へ委託している。
配信リストは毎月CSVで委託先へ渡している。
契約終了が決まり、委託先は「過去の配信分析のためデータを残したい」と申し出た。

委託先サービスが長時間停止した場合の継続策として、最も適切なものはどれか。

ア：全てのメール配信を同じ重要度として扱い、停止時の優先順位は決めない。

イ：サービス停止時は顧客連絡を全て中止し、復旧後にまとめて送る。

ウ：代替チャネルは個人SNSだけとし、会社管理の手段は準備しない。

エ：緊急性の高い顧客連絡について代替チャネルと対象者を定め、配信停止時の判断基準を準備する。

答え・解説 正答：エ

ア：全配信が同じ重要度とは限りません。

イ：緊急連絡まで一律中止すると影響が拡大します。

ウ：管理外の個人SNSは機密性や記録性の問題があります。

エ：重要な連絡を識別し、代替チャネルを事前に準備することで事業影響を抑えられます。

総合解説：事業継続では、業務を一括して考えるのではなく、重要度に応じて優先順位と代替手段を定めます。

対象：2026年度 / 基準日 2026-09-05

0085 委託・継続事例 > 委託先評価・契約・要求事項 ｜ 難易度：応用

AC社はバックアップ保管をクラウド事業者へ委託している。
バックアップは暗号化されているが、復元試験は2年間実施していない。
契約上の復元所要時間も明確ではない。

サービス要件として最も重要なものはどれか。

ア：必要なRTO・RPOに対応できるバックアップ頻度、保持世代、復元時間、復元手順、サポート条件を確認する。

イ：暗号化されていれば復元時間は何時間でもよい。

ウ：保存容量だけを比較し、復元機能は障害後に確認する。

エ：バックアップ取得の成功表示があれば、復元能力の確認は不要である。

答え・解説 正答：ア

ア：バックアップサービスは復元できて初めて事業継続に役立つため、RTO/RPOと復元能力を要件化します。

イ：暗号化は機密性対策で、復旧時間を保証しません。

ウ：復元機能は選定前に確認すべき主要要件です。

エ：取得成功と復元成功は同じではありません。

総合解説：バックアップ委託では、保存することより、必要な時点・時間で復元できることを中心に評価します。

対象：2026年度 / 基準日 2026-09-05

0086 委託・継続事例 > 委託先監督・更新・終了 ｜ 難易度：応用

AC社はバックアップ保管をクラウド事業者へ委託している。
バックアップは暗号化されているが、復元試験は2年間実施していない。
契約上の復元所要時間も明確ではない。

委託中の監督として最も適切なものはどれか。

ア：2年前に一度成功しているので、今後は復元試験を行わない。

イ：定期的にバックアップ成功状況を確認し、実際の復元試験でデータと手順が利用可能か検証する。

ウ：バックアップ容量が増えていれば正常と判断し、エラー内容は確認しない。

エ：復元試験は本番障害時だけ実施する。

答え・解説 正答：イ

ア：過去の成功は現在の復元可能性を保証しません。

イ：バックアップと復元手順は環境変更で劣化する可能性があるため、定期的な復元試験が必要です。

ウ：容量増加だけではバックアップの完全性は判断できません。

エ：障害時に初めて試すと復旧遅延のリスクがあります。

総合解説：バックアップ運用の有効性は、定期的な復元試験と結果の改善で維持します。

対象：2026年度 / 基準日 2026-09-05

0087 委託・継続事例 > BCP・障害・災害時の継続判断 ｜ 難易度：応用

AC社はバックアップ保管をクラウド事業者へ委託している。
バックアップは暗号化されているが、復元試験は2年間実施していない。
契約上の復元所要時間も明確ではない。

クラウド事業者自身が広域障害で利用不能になる場合に備えた対策として、最も適切なものはどれか。

ア：大手クラウドは停止しないと仮定し、代替先を考えない。

イ：全データを同じクラウドの同じ場所へ複製すれば広域障害対策になる。

ウ：重要データについて別の障害ドメインや代替保管先を検討し、単一サービスへの依存度をRTO/RPOから評価する。

エ：復旧できなくても保険で損失補填できれば、データ復元策は不要である。

答え・解説 正答：ウ

ア：どのサービスにも障害可能性があります。

イ：同じ障害範囲内の複製では共通障害を避けられない場合があります。

ウ：単一障害ドメインへの依存がRTO/RPOを満たさない場合、別拠点・別方式などの対策を検討します。

エ：金銭補填と業務データの復元は別問題です。

総合解説：事業継続では、外部サービスを含む単一障害点を把握し、許容停止時間に見合う冗長化・代替戦略を設計します。

対象：2026年度 / 基準日 2026-09-05

0088 委託・継続事例 > 委託先評価・契約・要求事項 ｜ 難易度：応用

AD社のECサイトは外部決済サービスのAPIに依存している。
決済事業者から、来月APIの認証方式を変更する通知が届いた。
AD社は変更対応の担当者をまだ決めておらず、未対応だと決済が停止する可能性がある。

外部サービス選定・契約時に確認しておく事項として、最も適切なものはどれか。

ア：API仕様は将来変わらないと仮定し、変更通知条件は不要とする。

イ：変更は全て利用者責任なので、事業者の通知期限は確認しない。

ウ：料金だけを契約に定め、技術仕様変更は口頭連絡で十分とする。

エ：仕様変更の通知方法・猶予期間、サポート、互換性、セキュリティ変更への対応責任を明確にする。

答え・解説 正答：エ

ア：外部サービスは更新・廃止される可能性があります。

イ：利用者責任があっても、通知の十分性は重要です。

ウ：重要変更は記録可能な方法で管理する必要があります。

エ：外部APIへ依存する場合、変更管理と通知条件は継続性に直結する重要な契約事項です。

総合解説：外部サービスの委託・利用では、通常時の性能だけでなく、仕様変更・終了時の影響も事前に評価します。

対象：2026年度 / 基準日 2026-09-05

0089 委託・継続事例 > 委託先監督・更新・終了 ｜ 難易度：応用

AD社のECサイトは外部決済サービスのAPIに依存している。
決済事業者から、来月APIの認証方式を変更する通知が届いた。
AD社は変更対応の担当者をまだ決めておらず、未対応だと決済が停止する可能性がある。

今回の通知を受けた対応として、最も適切なものはどれか。

ア：影響範囲を確認して担当者と期限を定め、テスト環境で新認証方式を検証し、本番切替とロールバック手順を計画する。

イ：変更日まで何もせず、決済停止後に対応を開始する。

ウ：通知を受け取った担当者だけが私的に対応し、組織として進捗管理しない。

エ：本番環境で初めて新認証方式を試し、失敗時の戻し方は考えない。

答え・解説 正答：ア

ア：外部サービス変更も変更管理の対象とし、影響評価、担当、期限、テスト、切替手順を管理します。

イ：事後対応ではサービス停止リスクが高まります。

ウ：個人任せでは進捗・責任が不明確です。

エ：本番初回試験とロールバック未準備は変更リスクを高めます。

総合解説：委託先・クラウドの変更通知は、自社システムの変更管理プロセスへ取り込みます。

対象：2026年度 / 基準日 2026-09-05

0090 委託・継続事例 > BCP・障害・災害時の継続判断 ｜ 難易度：応用

AD社のECサイトは外部決済サービスのAPIに依存している。
決済事業者から、来月APIの認証方式を変更する通知が届いた。
AD社は変更対応の担当者をまだ決めておらず、未対応だと決済が停止する可能性がある。

変更対応が間に合わず決済APIが停止した場合のBCPとして、最も適切なものはどれか。

ア：決済できない場合はサイト全体を無期限に停止し、代替案は検討しない。

イ：注文受付と決済を分離できるか、代替決済手段を使えるかを事前に検討し、顧客への案内と復旧優先順位を定める。

ウ：障害中も決済成功と表示して商品を出荷する。

エ：顧客への説明は不要とし、復旧後に自動的に解決すると考える。

答え・解説 正答：イ

ア：全停止が最善とは限らず、影響を比較する必要があります。

イ：重要機能の停止時に、業務を部分継続できるか、代替手段があるかを事前に判断します。

ウ：決済未完了なのに成功表示・出荷するのは整合性と信用の問題になります。

エ：顧客への適切な案内は混乱・苦情を抑えるため重要です。

総合解説：外部サービス依存のBCPでは、機能停止時に残せる業務、代替手段、顧客対応を具体化します。

対象：2026年度 / 基準日 2026-09-05

0091 インシデント事例 > 発見・初動・報告・エスカレーション ｜ 難易度：基礎

製造業A社で、共有ファイルサーバ上の複数ファイルの拡張子が突然変わり、開けなくなった。同時刻に端末のEDRから不審な暗号化処理のアラートが発生している。生産計画ファイルも共有サーバに置かれている。

最初の対応として最も適切なものはどれか。

ア：感染拡大を防ぐため影響端末・サーバを必要に応じてネットワークから隔離し、CSIRT等へ直ちに報告する。

イ：業務を止めないよう、そのまま利用を継続し翌日の定例会で報告する。

ウ：暗号化されたファイルを確認するため、他の端末から同じ共有フォルダを開き続ける。

エ：原因が確定するまで関係者へ連絡せず、担当者だけで様子を見る。

答え・解説 正答：ア

ア：ランサムウェアの可能性が高い兆候があるため、拡大防止と速やかなエスカレーションが優先です。

イ：継続利用は暗号化範囲や被害を広げる可能性があります。

ウ：他端末からアクセスを続けると感染経路や被害範囲を拡大するおそれがあります。

エ：原因確定を待たず、インシデントの疑い段階で定めた連絡経路へ報告する必要があります。

総合解説：科目Bでは、完全な原因究明より前に、被害拡大防止と組織的な初動を選べることが重要です。

対象：2026年度 / 基準日 2026-09-05

0092 インシデント事例 > 分析・証拠保全・復旧 ｜ 難易度：基礎

製造業A社で、共有ファイルサーバ上の複数ファイルの拡張子が突然変わり、開けなくなった。同時刻に端末のEDRから不審な暗号化処理のアラートが発生している。生産計画ファイルも共有サーバに置かれている。

分析・復旧の進め方として最も適切なものはどれか。

ア：早く復旧するため、影響端末を直ちに初期化しログも削除する。

イ：必要なログや端末情報を保全し、感染経路と影響範囲を確認した上で、安全が確認されたバックアップから復旧する。

ウ：暗号化ファイルだけを消し、感染端末はそのまま業務へ戻す。

エ：バックアップが存在することだけ確認し、復元可能性や感染時点を確認せず上書き復旧する。

答え・解説 正答：イ

ア：初期化前に必要な証拠を失うと、侵入経路や被害範囲の特定が困難になります。

イ：調査に必要な証拠を保全しつつ、侵害原因を除去してから復旧するのが基本です。

ウ：原因が残ったまま業務へ戻すと再感染する可能性があります。

エ：感染後のバックアップや復元不能なバックアップを使うと、復旧に失敗する可能性があります。

総合解説：証拠保全、根絶、復元は順序と目的を意識して進め、復旧を急ぐあまり原因調査や証拠を失わないことが重要です。

対象：2026年度 / 基準日 2026-09-05

0093 インシデント事例 > 再発防止・情報公開・関係者対応 ｜ 難易度：基礎

製造業A社で、共有ファイルサーバ上の複数ファイルの拡張子が突然変わり、開けなくなった。同時刻に端末のEDRから不審な暗号化処理のアラートが発生している。生産計画ファイルも共有サーバに置かれている。

復旧後の対応として最も適切なものはどれか。

ア：復旧できたため原因分析は行わず、事故記録も残さない。

イ：再発防止はEDR製品の交換だけに限定し、人的・運用面は確認しない。

ウ：侵入原因と統制上の弱点を分析し、パッチ・認証・バックアップ・教育等を改善するとともに、影響を受けた関係者へ事実に基づき説明する。

エ：外部説明では混乱を避けるため、確認できていない原因や被害件数も断定して発表する。

答え・解説 正答：ウ

ア：復旧だけで終了すると同じ弱点が残る可能性があります。

イ：単一製品の変更だけでは侵入経路や運用上の問題を解消できない場合があります。

ウ：再発防止は根本原因と複数の管理策を見直し、説明も確認済み事実に基づいて行います。

エ：未確認情報の断定は誤情報となり、信用や対応をさらに悪化させます。

総合解説：インシデント後は教訓を組織へ反映し、技術・運用・教育を横断して是正し、関係者対応も正確性を優先します。

対象：2026年度 / 基準日 2026-09-05

0094 インシデント事例 > 発見・初動・報告・エスカレーション ｜ 難易度：基礎

B社のクラウドストレージで、管理者アカウントが通常は利用しない深夜帯に海外IPからログインした。直後に大量のファイルダウンロードが記録されている。管理者本人はその時間に利用していないと回答した。

初動として最も適切なものはどれか。

ア：本人が利用していないならログの誤記とみなし、何もしない。

イ：海外IPを全て永久遮断するだけで、管理者アカウントはそのまま使わせる。

ウ：大量ダウンロードが完了するまで証拠収集のため接続を維持する。

エ：管理者アカウントのセッションを無効化し認証情報を再設定するとともに、インシデント対応責任者へエスカレーションする。

答え・解説 正答：エ

ア：本人否認はむしろ不正利用を疑う重要情報です。

イ：IP遮断だけでは窃取された認証情報や別経路の利用を防げません。

ウ：被害拡大を許してまで接続を維持する必要はなく、まず封じ込めを行います。

エ：不正利用の可能性が高いため、アカウント保護と組織的対応を直ちに開始します。

総合解説：不審な認証と大量操作が組み合わさった場合、単なる異常ログではなく高優先度のインシデントとして扱います。

対象：2026年度 / 基準日 2026-09-05

0095 インシデント事例 > 分析・証拠保全・復旧 ｜ 難易度：基礎

B社のクラウドストレージで、管理者アカウントが通常は利用しない深夜帯に海外IPからログインした。
直後に大量のファイルダウンロードが記録されている。管理者本人はその時間に利用していないと回答した。

被害範囲を確認するため、優先して確認すべきものはどれか。

ア：認証ログ、ダウンロード対象ファイル、操作時刻、接続元、権限変更、他アカウントへの操作履歴を相関して確認する。

イ：管理者本人の記憶だけを聞き取り、クラウド側ログは確認しない。

ウ：大量ダウンロードの件数だけを確認し、どのファイルかは調べない。

エ：ログ保存期間を短縮し、調査対象を減らす。

答え・解説 正答：ア

ア：複数ログを相関して、いつ・誰の権限で・何が操作されたかを明らかにする必要があります。

イ：本人の記憶だけでは客観的な被害範囲を確定できません。

ウ：対象ファイルの重要度により影響評価が変わるため内容確認が必要です。

エ：ログ削減は証拠を失わせ、調査を困難にします。

総合解説：クラウドインシデントでは、事業者が提供する監査ログを活用し、操作履歴と対象情報を時系列で整理します。

対象：2026年度 / 基準日 2026-09-05

0096 インシデント事例 > 再発防止・情報公開・関係者対応 ｜ 難易度：基礎

B社のクラウドストレージで、管理者アカウントが通常は利用しない深夜帯に海外IPからログインした。
直後に大量のファイルダウンロードが記録されている。管理者本人はその時間に利用していないと回答した。

顧客情報が含まれるファイルの持出しが確認された場合の対応として最も適切なものはどれか。

ア：顧客に不安を与えないため、社外への報告義務があっても通知しない。

イ：法令・契約・社内手順に基づき報告・通知の要否を判断し、対象者や取引先へ確認済みの影響と必要な対応を説明する。

ウ：全顧客へ同じ内容を一斉送信し、対象かどうかの確認は行わない。

エ：調査が継続中でも推測を含む被害内容を確定情報として公表する。

答え・解説 正答：イ

ア：法令・契約上必要な通知を意図的に避けるのは不適切です。

イ：漏えい時は適用される要求事項と実際の影響に基づいて報告・通知を判断します。

ウ：影響範囲を特定し、必要な対象へ適切に連絡することが重要です。

エ：調査中は判明済み事実と未確定事項を区別して説明します。

総合解説：情報公開では迅速性と正確性の両立が重要で、推測や隠蔽のどちらも避けます。

対象：2026年度 / 基準日 2026-09-05

0097 インシデント事例 > 発見・初動・報告・エスカレーション ｜ 難易度：基礎

C社の経理担当者に、取引先社長を名乗るメールで「振込口座が変更になった。今日中に支払ってほしい」と連絡があった。
担当者は通常と異なる手順で500万円を送金した後、取引先へ電話して詐欺だと判明した。

発覚直後の対応として最も適切なものはどれか。

ア：担当者の評価を守るため、月末まで事故を報告しない。

イ：メールを削除して証拠を残さず、送金先へ自分で連絡する。

ウ：上司・セキュリティ・経理責任者へ直ちに報告し、金融機関へ組戻し等の相談を行い、関連メールを保全する。

エ：詐欺メールは情報システム障害ではないため、セキュリティ部門には連絡しない。

答え・解説 正答：ウ

ア：報告遅延は資金回収や追加被害防止の機会を失います。

イ：メール削除は調査に必要な証拠を失わせます。

ウ：金銭被害の抑制には早期の金融機関連携が重要で、同時に組織内報告と証拠保全を行います。

エ：BECは認証・メール・人的対策を含む情報セキュリティインシデントです。

総合解説：金銭被害を伴うBECでは、技術対応だけでなく経理・法務・金融機関など関係者への迅速なエスカレーションが必要です。

対象：2026年度 / 基準日 2026-09-05

0098 インシデント事例 > 分析・証拠保全・復旧 ｜ 難易度：基礎

C社の経理担当者に、取引先社長を名乗るメールで「振込口座が変更になった。今日中に支払ってほしい」と連絡があった。
担当者は通常と異なる手順で500万円を送金した後、取引先へ電話して詐欺だと判明した。

原因分析で優先して確認すべき事項はどれか。

ア：メール本文の日本語が自然かどうかだけで原因を確定する。

イ：送金済みなのでメール関連ログは全て不要と判断する。

ウ：担当者がだまされたことだけを原因とし、技術的侵害の有無は調べない。

エ：メールヘッダ、送信元ドメイン、認証ログ、メールボックスの転送ルール、取引先側の侵害有無などを確認する。

答え・解説 正答：エ

ア：文章の自然さだけで送信経路は判断できません。

イ：関連ログは侵害範囲や追加被害の確認に必要です。

ウ：人的要因だけに限定すると、アカウント侵害等を見落とす可能性があります。

エ：BECは偽装ドメイン、メールアカウント侵害、転送ルール悪用など複数経路があるため、証拠を確認します。

総合解説：インシデント分析では「人がミスした」で終わらせず、攻撃者がどの情報・経路を利用したかを客観的に確認します。

対象：2026年度 / 基準日 2026-09-05

0099 インシデント事例 > 再発防止・情報公開・関係者対応 ｜ 難易度：基礎

C社の経理担当者に、取引先社長を名乗るメールで「振込口座が変更になった。今日中に支払ってほしい」と連絡があった。
担当者は通常と異なる手順で500万円を送金した後、取引先へ電話して詐欺だと判明した。

再発防止策として最も適切なものはどれか。

ア：振込先変更は既知の連絡先で別経路確認し、一定額以上は複数承認とし、メール認証・教育も組み合わせる。

イ：経理担当者に『今後気を付ける』と注意するだけにする。

ウ：メールを使わないため、全ての振込指示を個人SNSで受ける。

エ：迷惑メールフィルタを導入すれば、振込手順の見直しは不要とする。

答え・解説 正答：ア

ア：BECは業務手続そのものを狙うため、技術・教育・承認統制を組み合わせる必要があります。

イ：注意喚起だけでは巧妙な攻撃への耐性が不足します。

ウ：個人SNSは管理外の新たなリスクを生みます。

エ：フィルタだけでは正規アカウント侵害や巧妙な詐欺を完全には防げません。

総合解説：再発防止では、攻撃メールを見抜く能力だけでなく、偽メールが届いても不正送金が成立しにくい業務統制を作ります。

対象：2026年度 / 基準日 2026-09-05

0100 インシデント事例 > 発見・初動・報告・エスカレーション ｜ 難易度：標準

D社のコーポレートサイトが突然改ざんされ、トップページに不審なメッセージが表示された。
Webサーバの管理画面には、直前に管理者アカウントでログインした記録があるが、担当者は操作していない。

初動として最も適切なものはどれか。

ア：表示だけの問題なので、通常どおり公開を続け原因は後日調べる。

イ：改ざん拡大や閲覧者被害を防ぐため必要に応じて公開を一時制限し、管理者アカウントを保護してインシデント対応を開始する。

ウ：担当者が操作していないためログを誤記とみなし削除する。

エ：改ざんページを手作業で元に戻すだけで、認証情報や侵入経路は確認しない。

答え・解説 正答：イ

ア：改ざんサイトが不正プログラム配布等に利用される可能性があります。

イ：閲覧者への影響と再改ざんを防ぐため封じ込めとアカウント保護を優先します。

ウ：本人否認は不正アクセスを疑う材料でありログ削除は不適切です。

エ：表面だけ戻しても侵入経路が残れば再発します。

総合解説：Web改ざんは外観の問題に見えても、管理者権限侵害や他システム侵害の兆候である可能性があるため、正式なインシデントとして扱います。

対象：2026年度 / 基準日 2026-09-05

0101 インシデント事例 > 分析・証拠保全・復旧 ｜ 難易度：標準

D社のコーポレートサイトが突然改ざんされ、トップページに不審なメッセージが表示された。Webサーバの管理画面には、直前に管理者アカウントでログインした記録があるが、担当者は操作していない。

復旧手順として最も適切なものはどれか。

ア：最新ファイルで上書きすればよいので、改ざん時のログは保存しない。

イ：改ざんされたサーバをそのまま複製し、別環境で公開する。

ウ：Web・OS・認証ログ等を保全し、侵入経路と不正変更を確認して脆弱性を除去した後、既知の正常状態から復旧する。

エ：管理者パスワードだけ変更し、未修正の脆弱性や不審ファイルは残す。

答え・解説 正答：ウ

ア：ログを捨てると侵入経路や影響範囲の特定が困難になります。

イ：侵害状態を複製すると不正要素も引き継ぐ可能性があります。

ウ：証拠を保全し、原因を除去してから正常な状態へ戻すことが必要です。

エ：認証情報変更だけでは脆弱性やバックドアが残る場合があります。

総合解説：復旧は見た目を戻すことではなく、侵害要因を取り除き、安全性を確認した状態へ戻すことです。

対象：2026年度 / 基準日 2026-09-05

0102 インシデント事例 > 再発防止・情報公開・関係者対応 ｜ 難易度：標準

D社のコーポレートサイトが突然改ざんされ、トップページに不審なメッセージが表示された。Webサーバの管理画面には、直前に管理者アカウントでログインした記録があるが、担当者は操作していない。

公開サイト利用者への説明として最も適切なものはどれか。

ア：原因が未確定でも『個人情報漏えいは絶対にない』と断定する。

イ：信用低下を避けるため、改ざんが広く確認されていても一切説明しない。

ウ：技術用語だけを大量に並べ、利用者が何をすべきかは示さない。

エ：利用者影響がある場合は、発生事実、確認済みの影響範囲、利用者に求める対応、今後の更新方法を整理して公表する。

答え・解説 正答：エ

ア：未確定事項を断定すると後の訂正で信用を損なう可能性があります。

イ：影響がある場合に説明を避けると混乱や不信を高める場合があります。

ウ：技術詳細より、影響・対応・問い合わせ先など利用者に必要な情報を示すべきです。

エ：対外説明は確認済み事実と利用者が必要とする行動を分かりやすく伝えることが重要です。

総合解説：情報公開では、事実性、対象者への有用性、更新性を重視し、未確定事項は未確定と区別します。

対象：2026年度 / 基準日 2026-09-05

0103 インシデント事例 > 発見・初動・報告・エスカレーション ｜ 難易度：標準

E社の営業社員が出張先で会社支給ノートPCを紛失した。
端末には顧客との商談資料が保存されており、ディスク暗号化は有効である。
MDMで最終接続時刻は確認できるが、まだ端末はオンラインになっていない。

紛失判明時の対応として最も適切なものはどれか。

ア：社内の紛失報告手順に従い速やかに報告し、アカウント・端末の状態確認や遠隔ロック等の措置を準備する。

イ：暗号化済みなので情報漏えいは絶対にないと判断し、報告しない。

ウ：端末がオンラインになるまで社内報告を待つ。

エ：社員個人の持ち物ではないため、警察や関係部門への連絡要否を検討しない。

答え・解説 正答：ア

ア：暗号化は重要な保護策ですが、紛失事故として状態確認と組織的対応が必要です。

イ：暗号化があっても認証情報や端末設定等の確認が必要です。

ウ：報告遅延は遠隔操作やアカウント保護の機会を失います。

エ：物理紛失は必要に応じて警察・管理部門等への連携も検討します。

総合解説：インシデント初動では、対策が有効だから報告不要とはせず、事実を早期共有して影響を評価します。

対象：2026年度 / 基準日 2026-09-05

0104 インシデント事例 > 分析・証拠保全・復旧 ｜ 難易度：標準

E社の営業社員が出張先で会社支給ノートPCを紛失した。
端末には顧客との商談資料が保存されており、ディスク暗号化は有効である。
MDMで最終接続時刻は確認できるが、まだ端末はオンラインになっていない。

漏えい可能性の評価で確認すべき事項として最も適切なものはどれか。

ア：暗号化という一点だけで漏えい有無を確定する。

イ：端末暗号化の状態、ログイン方式、保存データ、最終接続、クラウドセッション、遠隔管理ログを確認する。

ウ：端末がないため調査不能として、記録を残さない。

エ：保存データの内容を確認せず、全顧客情報が漏えいしたと断定する。

答え・解説 正答：イ

ア：暗号化の実装状態や認証強度によってリスクは異なります。

イ：複数の事実を組み合わせて、第三者がデータへアクセスできた可能性を評価します。

ウ：端末がなくてもMDMやクラウド側に調査可能な証拠があります。

エ：対象情報を確認せず最大範囲を断定するのは不正確です。

総合解説：紛失事故の影響評価では、端末内情報とクラウド側セッションの双方を確認し、証拠に基づいて判断します。

対象：2026年度 / 基準日 2026-09-05

0105 インシデント事例 > 再発防止・情報公開・関係者対応 ｜ 難易度：標準

E社の営業社員が出張先で会社支給ノートPCを紛失した。
端末には顧客との商談資料が保存されており、ディスク暗号化は有効である。
MDMで最終接続時刻は確認できるが、まだ端末はオンラインになっていない。

再発防止として最も適切なものはどれか。

ア：紛失した社員だけに始末書を書かせ、他の端末運用は確認しない。

イ：今後は全顧客データを端末へ保存し、紛失時に一括で確認しやすくする。

ウ：端末持出しルール、ディスク暗号化、画面ロック、MDM、保存データ最小化、紛失訓練を見直す。

エ：端末紛失を防ぐため、暗号化を解除して端末追跡を優先する。

答え・解説 正答：ウ

ア：保存データを増やすと紛失時の影響が拡大します。

イ：暗号化解除は保存データの機密性を低下させます。

ウ：個別責任だけでなく、全社の端末管理と利用方法を見直す必要があります。

エ：技術・人的・運用対策を組み合わせるのが適切です。

総合解説：再発防止は、事故を起こした人だけでなく、同種端末を利用する全組織へ横展開することが重要です。

対象：2026年度 / 基準日 2026-09-05

0106 インシデント事例 > 発見・初動・報告・エスカレーション ｜ 難易度：標準

F社のDLPが、退職予定者のPCから深夜に大量の設計ファイルが外部クラウドストレージへアップロードされたことを検知した。
本人は翌週退職予定で、通常業務ではそのクラウドサービスを使用しない。

最初の対応として最も適切なものはどれか。

ア：退職予定者なので、退職日まで自由にデータを持ち出せると判断する。

イ：本人へDLP検知内容を即座に全て伝え、証拠保全前にファイル削除を依頼する。

ウ：DLPは誤検知があり得るため、退職後まで調査を延期する。

エ：セキュリティ責任者へ報告し、人事・法務等と連携して必要なアクセス制限と証拠保全を行う。

答え・解説 正答：エ

ア：雇用中でも会社情報の持出しが自由になるわけではありません。

イ：証拠保全前に本人へ詳細を伝えると、証拠消去等につながる可能性があります。

ウ：高リスクな兆候は誤検知の可能性があっても速やかに確認すべきです。

エ：内部不正の疑いでは、証拠を失わないようにしつつ、関係部門と連携して被害拡大を防止します。

総合解説：内部不正対応では、技術部門だけで判断せず、人事・法務・経営を含む適切な権限者へエスカレーションします。

対象：2026年度 / 基準日 2026-09-05

0107 インシデント事例 > 分析・証拠保全・復旧 ｜ 難易度：標準

F社のDLPが、退職予定者のPCから深夜に大量の設計ファイルが外部クラウドストレージへアップロードされたことを検知した。
本人は翌週退職予定で、通常業務ではそのクラウドサービスを使用しない。

分析のために最も適切な証拠保全はどれか。

ア：DLPログ、端末・クラウドのアクセスログ、対象ファイル一覧、時刻情報を改ざんされにくい形で保全する。

イ：本人のPCを通常利用させたまま、数週間後に残っているログだけを見る。

ウ：ファイル名だけをメモし、元ログは容量削減のため削除する。

エ：本人の私物端末へ無断で侵入し、会社と無関係な全データを収集する。

答え・解説 正答：ア

ア：業務上必要な範囲の客観的証拠を保全し、完全性と取扱いを管理することが重要です。

イ：通常利用を継続するとログや証拠が上書き・変更される可能性があります。

ウ：元ログを失うと操作時刻や送信先等の検証が困難になります。

エ：調査は法令・社内規程・権限の範囲で行い、必要性を超える私的情報収集は避けます。

総合解説：内部不正調査では、証拠の有用性だけでなく、適法性・必要性・完全性を考慮して保全します。

対象：2026年度 / 基準日 2026-09-05

0108 インシデント事例 > 再発防止・情報公開・関係者対応 ｜ 難易度：標準

F社のDLPが、退職予定者のPCから深夜に大量の設計ファイルが外部クラウドストレージへアップロードされたことを検知した。
本人は翌週退職予定で、通常業務ではそのクラウドサービスを使用しない。

再発防止として最も適切なものはどれか。

ア：退職予定者は全員危険とみなし、退職申出直後に全業務アクセスを無条件で停止する。

イ：退職・異動時の権限見直し、外部クラウド利用制御、ログ監視、秘密保持教育を組み合わせて改善する。

ウ：DLPを導入済みなので、権限管理や教育は不要とする。

エ：事故を公表しないため、同様の兆候を今後はログに残さない。

答え・解説 正答：イ

ア：一律の全アクセス停止は業務上必要な引継ぎ等を妨げる可能性があり、リスクに応じた権限管理が必要です。

イ：内部不正は技術・人的・組織的要因が関係するため、複数の対策を組み合わせます。

ウ：DLPだけで全ての持出し経路や動機を抑えられるわけではありません。

エ：ログ削除は検知・抑止能力を低下させます。

総合解説：再発防止では、不正の機会を減らし、早期検知し、退職時の情報管理を確実にする仕組みを整えます。

対象：2026年度 / 基準日 2026-09-05

0109 インシデント事例 > 発見・初動・報告・エスカレーション ｜ 難易度：標準

G社のオンライン予約サービスでアクセス数が急増し、応答が極端に遅くなった。
監視では多数の異なる送信元から短時間に大量リクエストが届いている。
予約サービスは売上に直結し、長時間停止は大きな影響がある。

初動として最も適切なものはどれか。

ア：アクセス増加は人気上昇の可能性もあるため、サービス停止まで何もしない。

イ：全利用者のアクセスを永久に遮断して攻撃を終わらせる。

ウ：インシデント対応担当へ報告し、回線・クラウド・CDN等の事業者と連携して緩和策を実施する。

エ：攻撃元が多数なので調査不能と判断し、監視を停止する。

答え・解説 正答：ウ

ア：通常アクセスとの識別は必要ですが、障害が進行している状況では対応を開始すべきです。

イ：全利用者の永久遮断はサービス目的を失わせます。

ウ：可用性への重大影響が出ているため、事業者と連携したDDoS緩和とエスカレーションが必要です。

エ：監視停止は状況把握と緩和効果の確認を困難にします。

総合解説：DDoSでは自社設備だけで対処できないことがあるため、回線事業者やクラウド事業者を含む連絡体制が重要です。

対象：2026年度 / 基準日 2026-09-05

0110 インシデント事例 > 分析・証拠保全・復旧 ｜ 難易度：標準

G社のオンライン予約サービスでアクセス数が急増し、応答が極端に遅くなった。
監視では多数の異なる送信元から短時間に大量リクエストが届いている。
予約サービスは売上に直結し、長時間停止は大きな影響がある。

分析・復旧として最も適切なものはどれか。

ア：応答が戻った瞬間に全ての緩和策を解除し、再攻撃を監視しない。

イ：攻撃中のトラフィック記録は容量を使うため全て削除する。

ウ：送信元IPが多いので、分析せず原因を『海外からの攻撃』と断定する。

エ：トラフィックの送信元・宛先・プロトコル・時間帯を分析し、緩和策の効果を確認しながら段階的に通常運用へ戻す。

答え・解説 正答：エ

ア：攻撃が継続・再開する可能性があるため段階的な復旧が安全です。

イ：ログは攻撃特性と対策評価に役立ちます。

ウ：送信元数や地域だけでは攻撃主体や原因を断定できません。

エ：攻撃パターンと緩和効果を確認し、再発に注意しながら復旧します。

総合解説：DDoS対応では、サービス復旧と並行して攻撃特性を記録し、今後の容量設計や緩和ルール改善に活かします。

対象：2026年度 / 基準日 2026-09-05

0111 インシデント事例 > 再発防止・情報公開・関係者対応 ｜ 難易度：標準

G社のオンライン予約サービスでアクセス数が急増し、応答が極端に遅くなった。
監視では多数の異なる送信元から短時間に大量リクエストが届いている。
予約サービスは売上に直結し、長時間停止は大きな影響がある。

サービス復旧後の対応として最も適切なものはどれか。

ア：停止時間・影響範囲・復旧状況を整理して利用者へ案内し、DDoS対策容量や事業者連携手順を見直す。

イ：復旧したので、利用者から問い合わせが来ても障害の事実を否定する。

ウ：攻撃者を特定できていなくても、特定企業からの攻撃だと公表する。

エ：今後のために常時サービスを低速化し、業務要件は見直さない。

答え・解説 正答：ア

ア：利用者へ必要な事実を伝え、技術・運用面の改善を行うのが適切です。

イ：障害事実の否定は信頼を損ねます。

ウ：根拠のない攻撃主体の断定は避けるべきです。

エ：恒常的な性能低下ではなく、事業要件とリスクに応じた容量・緩和策を設計します。

総合解説：可用性インシデントでも、利用者への説明と継続計画の改善が必要です。

対象：2026年度 / 基準日 2026-09-05

0112 インシデント事例 > 発見・初動・報告・エスカレーション ｜ 難易度：標準

H社が利用する業務ソフトの正規アップデート後、複数端末で不審な外部通信が発生した。
同じ製品を利用する他社からも類似報告があり、ベンダは更新ファイルの侵害可能性を調査中である。

最も適切な初動はどれか。

ア：正規アップデート経由なので安全と判断し、通信を許可し続ける。

イ：影響製品・端末を特定し、不審通信を制限しながらベンダ・CSIRT等と情報共有して対応を開始する。

ウ：ベンダの最終発表まで全ての調査を停止する。

エ：同じ製品を利用する端末数を把握せず、1台だけ初期化する。

答え・解説 正答：イ

ア：署名付き・正規配布であっても供給元が侵害される可能性があります。

イ：正規経路でもサプライチェーン侵害は起こり得るため、自社の影響範囲を把握し封じ込めます。

ウ：ベンダ調査と並行して自社側で可能な保護を行う必要があります。

エ：影響製品の利用範囲を特定しないと侵害端末を見落とします。

総合解説：サプライチェーンインシデントでは、外部情報を待つだけでなく、自社資産の影響確認と一時的な緩和策を行います。

対象：2026年度 / 基準日 2026-09-05

0113 インシデント事例 > 分析・証拠保全・復旧 ｜ 難易度：標準

H社が利用する業務ソフトの正規アップデート後、複数端末で不審な外部通信が発生した。同じ製品を利用する他社からも類似報告があり、ベンダは更新ファイルの侵害可能性を調査中である。

分析・復旧で最も適切な方法はどれか。

ア：不審通信端末を全て初期化し、更新適用履歴は不要として削除する。

イ：ベンダが調査中なので、自社ログは保存しなくてよい。

ウ：更新適用履歴、ハッシュ・配布時刻、不審通信・プロセスを保全し、安全が確認された版や回避策へ切り替える。

エ：原因がアップデートと推定できるため、個別端末の影響確認は省略する。

答え・解説 正答：ウ

ア：初期化前に証拠を失うと侵害範囲の確認が困難になります。

イ：ベンダ調査と自社証拠は補完関係にあります。

ウ：更新経路と端末挙動を追跡できる証拠を保全し、信頼できる復旧状態へ戻す必要があります。

エ：同じ更新を適用しても端末ごとに侵害状況が異なる可能性があります。

総合解説：サプライチェーン侵害では、どのバージョンをいつ適用したかを追跡できる資産・変更管理が重要です。

対象：2026年度 / 基準日 2026-09-05

0114 インシデント事例 > 再発防止・情報公開・関係者対応 ｜ 難易度：標準

H社が利用する業務ソフトの正規アップデート後、複数端末で不審な外部通信が発生した。同じ製品を利用する他社からも類似報告があり、ベンダは更新ファイルの侵害可能性を調査中である。

再発防止として最も適切なものはどれか。

ア：正規ベンダの製品は今後一切更新しない。

イ：今回のベンダだけを信用しないと決め、他ベンダの評価は行わない。

ウ：更新によるリスクを避けるため、脆弱性修正も含め全てのパッチを停止する。

エ：重要ソフトの資産台帳・更新管理、ベンダの脆弱性連絡、代替手段、更新前後の監視を見直す。

答え・解説 正答：エ

ア：更新停止は既知脆弱性の放置につながります。

イ：一社だけでなく重要な供給者をリスクに応じて管理します。

ウ：全パッチ停止は別の重大リスクを生みます。

エ：特定事故を受けて、供給者管理と変更監視を体系的に改善するのが適切です。

総合解説：サプライチェーン対策は、取引先選定だけでなく、変更通知・脆弱性情報・代替性・監視まで継続的に行います。

対象：2026年度 / 基準日 2026-09-05

0115 インシデント事例 > 発見・初動・報告・エスカレーション ｜ 難易度：応用

I社の地方支店で、複数PCとNASがマルウェア感染し業務ファイルが利用できなくなった。本社ネットワークとはVPN接続されている。支店担当者は業務再開を急ぎ、感染PCをそのままVPNへ再接続したいと申し出た。

最も適切な判断はどれか。

ア：感染端末・NASを隔離し、本社との接続経路も確認して、全社CSIRTへエスカレーションする。

イ：支店だけの事故なので、本社へ報告せずVPN接続を再開する。

ウ：業務再開を優先し、感染端末から本社共有サーバへ直接データをコピーする。

エ：支店ネットワークを隔離すれば十分なので、認証情報の悪用可能性は確認しない。

答え・解説 正答：ア

ア：拠点感染はVPN経由で本社へ波及する可能性があり、全社インシデントとして評価します。

イ：支店内に限定されている保証がないため報告が必要です。

ウ：感染端末を本社へ接続するのは被害拡大につながります。

エ：侵害された認証情報が他拠点でも使われる可能性を確認する必要があります。

総合解説：拠点単位の事故でも、ネットワーク・アカウント・共有サービスを通じた全社波及を考えて初動します。

対象：2026年度 / 基準日 2026-09-05

0116 インシデント事例 > 分析・証拠保全・復旧 ｜ 難易度：応用

I社の地方支店で、複数PCとNASがマルウェア感染し業務ファイルが利用できなくなった。本社ネットワークとはVPN接続されている。支店担当者は業務再開を急ぎ、感染PCをそのままVPNへ再接続したいと申し出た。

支店業務の復旧方法として最も適切なものはどれか。

ア：感染PCを再起動して動作すれば、そのまま本番利用へ戻す。

イ：クリーンな端末環境を用意し、感染原因を除去した上で、検証済みバックアップから必要データを復元する。

ウ：感染NASのファイルを新NASへ全て無検査でコピーする。

エ：バックアップの取得日や感染時点を確認せず、最新世代だけを必ず使う。

答え・解説 正答：イ

ア：再起動で正常に見えてもマルウェアが残る場合があります。

イ：安全な実行環境と検証済みデータから段階的に業務を戻すのが適切です。

ウ：不正ファイルやマルウェアを新環境へ移す可能性があります。

エ：最新バックアップが既に感染後である可能性があるため時点確認が必要です。

総合解説：復旧では『早く戻す』だけでなく、侵害状態を新環境へ持ち込まないことが重要です。

対象：2026年度 / 基準日 2026-09-05

0117 インシデント事例 > 再発防止・情報公開・関係者対応 ｜ 難易度：応用

I社の地方支店で、複数PCとNASがマルウェア感染し業務ファイルが利用できなくなった。本社ネットワークとはVPN接続されている。支店担当者は業務再開を急ぎ、感染PCをそのままVPNへ再接続したいと申し出た。

復旧後の改善として最も適切なものはどれか。

ア：事故が起きた支店だけ改善し、同じ構成の他拠点は確認しない。

イ：支店担当者の責任として処理し、全社のネットワーク設計は見直さない。

ウ：支店だけでなく全拠点のパッチ、端末保護、権限、バックアップ、VPN分離、教育を横断的に点検する。

エ：今後は支店からのインシデント報告を減らすため、軽微な兆候は記録しない。

答え・解説 正答：ウ

ア：一拠点だけの是正では同じ原因が残る可能性があります。

イ：個人責任だけにすると構造的な問題を改善できません。

ウ：共通構成・共通運用の弱点が他拠点にも存在する可能性があるため横展開が必要です。

エ：兆候の記録を減らすと早期検知が難しくなります。

総合解説：インシデントの教訓は、同じ資産・運用を持つ他部署・拠点へ反映することで組織全体のリスク低減につながります。

対象：2026年度 / 基準日 2026-09-05

0118 インシデント事例 > 発見・初動・報告・エスカレーション ｜ 難易度：応用

J社の担当者がクラウドストレージの設定を変更したところ、社内限定の顧客資料フォルダがインターネットから認証なしで閲覧できる状態になった。外部の研究者から連絡を受けて発覚した。公開状態が何日続いたかは不明である。

初動として最も適切なものはどれか。

ア：外部研究者が見ただけなので、設定はそのままにして翌月修正する。

イ：公開設定を直した後、事故が知られないよう変更履歴を削除する。

ウ：原因が担当者の操作ミスと分かった時点で、アクセスログの確認は不要とする。

エ：公開設定を直ちに安全な状態へ戻し、変更履歴とアクセスログを保全して責任者へ報告する。

答え・解説 正答：エ

ア：公開状態を継続すると被害が拡大します。

イ：変更履歴は原因分析と説明に必要な証拠です。

ウ：設定ミスが原因でも、実際に誰がアクセスしたかは別途確認が必要です。

エ：まず追加閲覧を止め、証拠を保全して影響調査を開始します。

総合解説：クラウド誤設定は、誤操作の是正と外部アクセスの影響評価を並行して行います。

対象：2026年度 / 基準日 2026-09-05

0119 インシデント事例 > 分析・証拠保全・復旧 ｜ 難易度：応用

J社の担当者がクラウドストレージの設定を変更したところ、社内限定の顧客資料フォルダがインターネットから認証なしで閲覧できる状態になった。
外部の研究者から連絡を受けて発覚した。公開状態が何日続いたかは不明である。

被害範囲を特定するため最も重要な確認はどれか。

ア：設定変更時刻、公開期間、アクセス元、閲覧・ダウンロードされたオブジェクト、対象資料の内容をログから確認する。

イ：公開期間が不明なので、全顧客資料が必ず漏えいしたと断定する。

ウ：設定を直したので、過去のアクセス状況は調べない。

エ：研究者から連絡があった1件だけを確認し、他アクセスの有無は見ない。

答え・解説 正答：ア

ア：公開期間とアクセス履歴、対象情報を組み合わせて実際の影響を評価します。

イ：不明な点は不明として調査し、最大被害を事実として断定しません。

ウ：設定修正後も過去ログは影響評価に必要です。

エ：発見者以外のアクセスが存在する可能性を確認する必要があります。

総合解説：漏えい可能性の評価では、設定状態だけでなく、公開期間中の実アクセスと対象情報の重要度を確認します。

対象：2026年度 / 基準日 2026-09-05

0120 インシデント事例 > 再発防止・情報公開・関係者対応 ｜ 難易度：応用

J社の担当者がクラウドストレージの設定を変更したところ、社内限定の顧客資料フォルダがインターネットから認証なしで閲覧できる状態になった。
外部の研究者から連絡を受けて発覚した。公開状態が何日続いたかは不明である。

再発防止と関係者対応として最も適切なものはどれか。

ア：設定変更を全社員に許可し、問題があれば後で戻す運用にする。

イ：公開設定変更の権限・承認・自動検知を見直し、影響調査結果に基づいて必要な報告・通知を行う。

ウ：誤設定は人的ミスなので、技術的な予防・検知策は設けない。

エ：漏えい可能性があっても、会社の信用を守るため関係者への説明は一律に行わない。

答え・解説 正答：イ

ア：広い変更権限は誤設定リスクを高めます。

イ：権限制御・変更管理・設定監視で誤公開を予防・早期検知し、影響に応じて関係者対応を判断します。

ウ：人的ミスを前提に技術・運用の多層対策を設けるべきです。

エ：必要な報告・通知は法令・契約・影響に基づいて判断します。

総合解説：クラウド事故の再発防止では、設定変更を個人の注意に依存せず、予防・検知・レビューの仕組みへ改善します。

対象：2026年度 / 基準日 2026-09-05

0121 教育・監査・総合判断 > 教育・訓練・内部不正防止 ｜ 難易度：基礎

K社は全社員500名に標的型メール訓練を実施した。
結果は次のとおりだった。

【訓練結果】
・訓練メール開封：180名
・訓練URLクリック：60名
・模擬ログイン画面へ資格情報入力：18名
・不審メール報告ボタンで報告：35名

前年はURLクリック80名、報告20名だった。

教育施策として最も適切なものはどれか。

ア：クリックした社員だけを公開して処罰し、教育は行わない。

イ：前年よりクリック数が減ったので、今後の訓練を全て中止する。

ウ：資格情報を入力した社員を含む高リスク層へ追加教育を行い、全社員には不審メールの見分け方と報告手順を継続訓練する。

エ：報告者が35名いるため、資格情報入力18名は問題ないと判断する。

答え・解説 正答：ウ

ア：処罰中心では報告をためらう文化を生み、学習効果を下げる可能性があります。

イ：改善傾向があっても、資格情報入力など重大な弱点が残っています。

ウ：訓練結果から弱点を特定し、対象別教育と報告行動の定着を図るのが適切です。

エ：報告者増加は良い傾向ですが、資格情報入力リスクを相殺するものではありません。

総合解説：教育は一度実施して終わりではなく、行動指標を使って弱点を特定し、内容・対象・頻度を改善します。

対象：2026年度 / 基準日 2026-09-05

0122 教育・監査・総合判断 > コンプライアンス・監査・是正 ｜ 難易度：基礎

K社は全社員500名に標的型メール訓練を実施した。
結果は次のとおりだった。

【訓練結果】
・訓練メール開封：180名
・訓練URLクリック：60名
・模擬ログイン画面へ資格情報入力：18名
・不審メール報告ボタンで報告：35名

前年はURLクリック80名、報告20名だった。

内部監査で確認する事項として最も適切なものはどれか。

ア：訓練を実施したという担当者の口頭説明だけで適合とする。

イ：クリック率だけを確認し、未受講者や改善措置は監査対象外とする。

ウ：監査担当者が教育内容を自ら作成・実施し、その同じ活動だけを自己監査する。

エ：教育計画・受講記録・訓練結果・未受講者フォロー・改善措置が定めた方針どおり実施されているかを証拠で確認する。

答え・解説 正答：エ

ア：口頭説明だけでは実施状況の裏付けが不十分です。

イ：教育の網羅性や改善も有効性評価に重要です。

ウ：自己監査は独立性を損ないやすいため、可能な範囲で役割を分けます。

エ：監査では計画から実施・評価・改善までを客観的な証拠で確認します。

総合解説：教育統制の監査では、実施件数だけでなく、対象者の網羅性と改善サイクルが機能しているかを確認します。

対象：2026年度 / 基準日 2026-09-05

0123 教育・監査・総合判断 > 表・ログ・規程読解・複数論点の実務判断 ｜ 難易度：基礎

K社は全社員500名に標的型メール訓練を実施した。
結果は次のとおりだった。

【訓練結果】
・訓練メール開封：180名
・訓練URLクリック：60名
・模擬ログイン画面へ資格情報入力：18名
・不審メール報告ボタンで報告：35名

前年はURLクリック80名、報告20名だった。

表の結果から読み取れる判断として最も適切なものはどれか。

ア：URLクリックは前年より25%減少し報告者は増えたが、資格情報入力者が18名いるため、改善傾向と残存リスクの両方を評価すべきである。

イ：URLクリックが20名減ったので、リスクは完全に解消した。

ウ：不審メール報告が15名増えたので、クリック・資格情報入力の結果は無視できる。

エ：訓練メール開封者180名は全員インシデントを起こしたと判断できる。

答え・解説 正答：ア

ア：80名から60名への減少は25%ですが、資格情報入力者が残るため継続改善が必要です。

イ：一つの良い指標だけで他のリスク指標を無視してはいけません。

ウ：報告者の増加は望ましいものの、入力行動の危険性は別に評価します。

エ：メール開封だけで実被害が発生したとは限らず、行動段階を区別して評価します。

総合解説：科目Bでは、単一の数字だけで結論を出さず、複数の指標から改善と残存リスクを同時に判断することが重要です。

対象：2026年度 / 基準日 2026-09-05

0124 教育・監査・総合判断 > 教育・訓練・内部不正防止 ｜ 難易度：基礎

L社の四半期アクセス権棚卸しで、次の状況が判明した。

【特権アカウント】
A：情報システム部長／在籍／利用あり
B：元DB担当／2か月前に営業部へ異動／直近1週間に利用あり
C：退職者／3週間前退職／利用なし
D：外部保守会社共有ID／5名で利用／利用あり

規程では、異動・退職時に不要権限を速やかに削除し、特権操作は個人単位で追跡可能にすると定めている。

教育・訓練として最も適切なものはどれか。

ア：管理者は専門知識があるため、情報セキュリティ教育の対象外とする。

イ：特権利用者へ権限の目的外利用禁止、共有禁止、操作記録、異動・退職時の申告手順を具体的事例とともに教育する。

ウ：特権利用者には一般社員より強い権限があるため、規程の例外を自由に判断させる。

エ：内部不正防止のため、特権利用者にはログ取得の存在を一切知らせない。

答え・解説 正答：イ

ア：専門知識と規程順守は別であり、教育は必要です。

イ：特権利用者は高い権限を持つため、責任・禁止事項・証跡・変更時手続きを明確に教育する必要があります。

ウ：強い権限ほど統制が重要で、自由な例外判断を認めるべきではありません。

エ：監視の存在や利用ルールを適切に周知することは抑止にもつながります。

総合解説：内部不正防止教育では、一般論だけでなく、特権利用者の具体的な責任と違反例を示します。

対象：2026年度 / 基準日 2026-09-05

0125 教育・監査・総合判断 > コンプライアンス・監査・是正 ｜ 難易度：基礎

L社の四半期アクセス権棚卸しで、次の状況が判明した。

【特権アカウント】
A：情報システム部長／在籍／利用あり
B：元DB担当／2か月前に営業部へ異動／直近1週間に利用あり
C：退職者／3週間前退職／利用なし
D：外部保守会社共有ID／5名で利用／利用あり

規程では、異動・退職時に不要権限を速やかに削除し、特権操作は個人単位で追跡可能にすると定めている。

監査指摘として最も優先すべきものはどれか。

ア：退職者Cは利用記録がないため、アカウント残存を適合とする。

イ：共有ID Dは保守会社が利用するため、個人追跡不可でも規程違反ではないとする。

ウ：異動者Bの旧特権が残り実際に利用されていることを重大な不適合として扱い、利用内容確認と権限是正を直ちに行う。

エ：部長Aは役職が高いので、特権利用のレビュー対象外とする。

答え・解説 正答：ウ

ア：退職者アカウントの残存自体が規程違反であり、未利用でも是正が必要です。

イ：共有IDは個人単位追跡の規程に反します。

ウ：異動後の不要特権が実利用されているため、規程違反と不正利用の可能性を同時に確認すべき高優先度事項です。

エ：役職にかかわらず特権は適切にレビューします。

総合解説：監査指摘の優先度は、単なる形式違反ではなく、実際の利用状況と影響を含むリスクで判断します。

対象：2026年度 / 基準日 2026-09-05

0126 教育・監査・総合判断 > 表・ログ・規程読解・複数論点の実務判断 ｜ 難易度：基礎

L社の四半期アクセス権棚卸しで、次の状況が判明した。

【特権アカウント】
A：情報システム部長／在籍／利用あり
B：元DB担当／2か月前に営業部へ異動／直近1週間に利用あり
C：退職者／3週間前退職／利用なし
D：外部保守会社共有ID／5名で利用／利用あり

規程では、異動・退職時に不要権限を速やかに削除し、特権操作は個人単位で追跡可能にすると定めている。

規程と表を照合した対応として最も適切なものはどれか。

ア：Bは在籍中なのでそのまま、Cだけ削除し、Dは共有IDを継続する。

イ：B・Cは削除するが、Dは5名全員が同じ会社なので追跡不要とする。

ウ：A〜Dを全て削除し、業務に必要な管理作業も停止する。

エ：Bの利用内容を調査して不要特権を停止し、Cを無効化し、Dは個人識別可能な方式へ改める。

答え・解説 正答：エ

ア：異動者Bの不要特権は在籍中でも問題です。

イ：共有ID Dは個人追跡性の要求を満たしません。

ウ：必要な権限まで全削除するのではなく、最小権限と業務継続を両立させます。

エ：規程に照らすとB・C・Dにそれぞれ異なる是正が必要です。

総合解説：複数の不適合がある場合、各事実を規程へ対応付け、リスクと業務必要性に応じて是正します。

対象：2026年度 / 基準日 2026-09-05

0127 教育・監査・総合判断 > 教育・訓練・内部不正防止 ｜ 難易度：基礎

M社のテレワーク規程には次の記載がある。
①会社支給端末を利用する。
②機密資料は承認なく端末へ保存しない。
③離席時は画面をロックする。
④公共Wi-Fi利用時は会社指定VPNを使用する。

自己点検では、20名中5名が私物PCを利用し、3名がVPNを使わず公共Wi-Fiへ接続したと回答した。

教育内容として最も適切なものはどれか。

ア：規程の各ルールが防ぐリスクを説明し、公共Wi-Fi、画面ロック、データ保存、端末紛失時の具体的行動を訓練する。

イ：規程PDFを配布するだけで、内容の理解確認は行わない。

ウ：テレワークは自宅勤務が中心なので、物理・通信・端末のリスク教育は不要とする。

エ：違反者名を全社員へ公開することを教育の中心にする。

答え・解説 正答：ア

ア：具体的な場面とリスクを結び付けて教育することで、規程を実際の行動へつなげられます。

イ：配布だけでは理解や実践を確認できません。

ウ：自宅や公共空間でも覗き見、端末紛失、不安全な通信等のリスクがあります。

エ：羞恥を与えることより、正しい行動と報告文化を定着させることが重要です。

総合解説：教育は規程の暗記ではなく、利用場面で正しい判断を選べるようにすることが目的です。

対象：2026年度 / 基準日 2026-09-05

0128 教育・監査・総合判断 > コンプライアンス・監査・是正 ｜ 難易度：基礎

M社のテレワーク規程には次の記載がある。
①会社支給端末を利用する。
②機密資料は承認なく端末へ保存しない。
③離席時は画面をロックする。
④公共Wi-Fi利用時は会社指定VPNを使用する。

自己点検では、20名中5名が私物PCを利用し、3名がVPNを使わず公共Wi-Fiへ接続したと回答した。

自己点検後の対応として最も適切なものはどれか。

ア：自己申告なので証拠価値がないとして結果を全て無視する。

イ：私物PC利用とVPN未使用の実態・原因を確認し、是正期限を定めて端末配備・設定・教育など必要な改善を行う。

ウ：違反者が少数なので、規程を実態に合わせて無条件に廃止する。

エ：自己点検の点数だけ保存し、具体的な是正は行わない。

答え・解説 正答：イ

ア：自己申告には限界がありますが、無視せず必要に応じて証拠確認を行います。

イ：自己点検は実態把握の手段として活用し、原因を確認して是正へつなげます。

ウ：実態に合わせるだけでなく、リスクと業務要件から規程・設備の妥当性を判断します。

エ：点検は改善につなげて初めて意味があります。

総合解説：コンプライアンス管理では、違反を発見したら個人の注意不足だけでなく、設備不足やルールの実行可能性も確認します。

対象：2026年度 / 基準日 2026-09-05

0129 教育・監査・総合判断 > 表・ログ・規程読解・複数論点の実務判断 ｜ 難易度：基礎

M社のテレワーク規程には次の記載がある。
①会社支給端末を利用する。
②機密資料は承認なく端末へ保存しない。
③離席時は画面をロックする。
④公共Wi-Fi利用時は会社指定VPNを使用する。

自己点検では、20名中5名が私物PCを利用し、3名がVPNを使わず公共Wi-Fiへ接続したと回答した。

規程と自己点検結果から、最も適切な判断はどれか。

ア：私物PC利用者が25%なので、規程は自動的に無効になる。

イ：VPN未使用者が3名だけなら規程不適合にはならない。

ウ：私物PC利用とVPN未使用はいずれも規程不適合であり、特に公共Wi-FiでVPN未使用は通信保護の観点から速やかな是正が必要である。

エ：会社支給端末であれば、公共Wi-FiでVPNを使わなくても規程に適合する。

答え・解説 正答：ウ

ア：違反割合が高いことは規程無効ではなく、実行可能性や教育の見直し材料です。

イ：少人数でも違反は違反であり、リスク評価が必要です。

ウ：規程に明確な要求があるため、件数にかかわらず不適合です。影響や危険性で是正優先度を付けます。

エ：会社支給端末でも④のVPN要件は別途適用されます。

総合解説：複数の規程条項を分けて読み、違反件数とリスクの大きさを混同しないことが重要です。

対象：2026年度 / 基準日 2026-09-05

0130 教育・監査・総合判断 > 教育・訓練・内部不正防止 ｜ 難易度：標準

N社の購買部は新規クラウドサービスを選定する。
候補3社の状況は次のとおり。

A社：価格○、MFA○、監査ログ○、障害連絡4時間以内
B社：価格◎、MFA×、監査ログ×、障害連絡条件なし
C社：価格△、MFA○、監査ログ○、障害連絡1時間以内

対象サービスでは機密情報を扱い、障害時は2時間以内の初報が必要である。

購買部への教育として最も適切なものはどれか。

ア：価格が最安のサービスを選べば経営上正しいため、セキュリティ評価は不要と教える。

イ：クラウド事業者の知名度だけを確認すればよいと教える。

ウ：契約後に不足機能を知ればよいので、選定時のチェックは省略するよう教える。

エ：価格だけでなく、扱う情報の重要度、認証、ログ、可用性、事故連絡などを要求事項として比較する方法を教育する。

答え・解説 正答：エ

ア：価格だけでは情報漏えい・業務停止等のリスクを評価できません。

イ：知名度は具体的な管理策の代替ではありません。

ウ：導入後に変更できない条件もあるため事前確認が必要です。

エ：調達担当者が事業・セキュリティ要求を理解して比較できるようにすることが重要です。

総合解説：セキュリティはIT部門だけでなく、調達・契約を行う部門にも役割があるため、役割別教育が有効です。

対象：2026年度 / 基準日 2026-09-05

0131 教育・監査・総合判断 > コンプライアンス・監査・是正 ｜ 難易度：標準

N社の購買部は新規クラウドサービスを選定する。
候補3社の状況は次のとおり。

A社：価格○、MFA○、監査ログ○、障害連絡4時間以内
B社：価格◎、MFA×、監査ログ×、障害連絡条件なし
C社：価格△、MFA○、監査ログ○、障害連絡1時間以内

対象サービスでは機密情報を扱い、障害時は2時間以内の初報が必要である。

監査で最も重視すべき確認はどれか。

ア：定めたセキュリティ要求がRFP・評価表・契約へ反映され、選定理由と例外承認が証拠として残っているか確認する。

イ：最終的な契約金額だけ確認し、評価過程は監査しない。

ウ：サービスが現在動いていれば、選定時の要求確認は不要とする。

エ：監査人が自分の好みで候補会社を再選定し、その結果を唯一の基準にする。

答え・解説 正答：ア

ア：監査では、組織が定めたプロセスと要求に沿って合理的に選定されたかを証拠で確認します。

イ：価格だけでは選定統制の有効性を確認できません。

ウ：現在稼働していても、重要なセキュリティ要求が欠けている可能性があります。

エ：監査は個人的好みではなく、基準と証拠に基づきます。

総合解説：委託先選定の監査では、結果だけでなく、要求設定・評価・承認・契約のプロセスを確認します。

対象：2026年度 / 基準日 2026-09-05

0132 教育・監査・総合判断 > 表・ログ・規程読解・複数論点の実務判断 ｜ 難易度：標準

N社の購買部は新規クラウドサービスを選定する。
候補3社の状況は次のとおり。

A社：価格○、MFA○、監査ログ○、障害連絡4時間以内
B社：価格◎、MFA×、監査ログ×、障害連絡条件なし
C社：価格△、MFA○、監査ログ○、障害連絡1時間以内

対象サービスでは機密情報を扱い、障害時は2時間以内の初報が必要である。

表と要件だけを前提とした判断として最も適切なものはどれか。

ア：B社は価格が最良なので、MFAと監査ログがなくても最も適切である。

イ：C社はMFA・監査ログを満たし、障害初報1時間で2時間以内要件も満たすため、3社の中では要求への適合度が最も高い。

ウ：A社は障害連絡4時間以内なので、2時間以内の初報要件を満たす。

エ：3社とも価格が異なるため、セキュリティ要求への適合比較はできない。

答え・解説 正答：イ

ア：価格だけで必須要求の欠落を補うことはできません。

イ：提示条件ではC社が必要なセキュリティ・連絡要件を満たしています。

ウ：A社の4時間以内は2時間以内という要求を満たしません。

エ：価格と要求適合性を分けて評価することが可能です。

総合解説：調達の実務判断では、必須条件と評価項目を区別し、価格だけで安全上の最低要件を覆さないようにします。

対象：2026年度 / 基準日 2026-09-05

0133 教育・監査・総合判断 > 教育・訓練・内部不正防止 ｜ 難易度：標準

O社は四半期ごとに重要システムの復旧訓練を行っている。
今回の結果は次のとおり。

【目標】RTO：4時間、RPO：1時間
【実績】復旧完了：5時間20分、復元データ：障害発生の45分前
【備考】手順書に古いサーバ名が残り、切替作業で50分迷った。

訓練後の教育として最も適切なものはどれか。

ア：復旧に成功したので、訓練結果を担当者へ共有しない。

イ：訓練はシステム担当だけの仕事なので、業務部門の役割は教育しない。

ウ：実際に迷った手順を教材化し、担当者が手順書を使って役割分担・切替・連絡を実践できるよう再訓練する。

エ：手順書の誤りは訓練時だけの問題として修正せず、記憶で対応する。

答え・解説 正答：ウ

ア：成功・失敗双方の教訓を共有する必要があります。

イ：業務再開にはシステム担当以外の判断・連絡も関係します。

ウ：訓練で見つかった具体的な弱点を教育・再訓練へ反映することが有効です。

エ：手順書の誤りは本番障害でも遅延要因になるため修正が必要です。

総合解説：BCP訓練は合否だけでなく、手順・役割・連絡の弱点を発見して改善する教育機会です。

対象：2026年度 / 基準日 2026-09-05

0134 教育・監査・総合判断 > コンプライアンス・監査・是正 ｜ 難易度：標準

O社は四半期ごとに重要システムの復旧訓練を行っている。
今回の結果は次のとおり。

【目標】RTO：4時間、RPO：1時間
【実績】復旧完了：5時間20分、復元データ：障害発生の45分前
【備考】手順書に古いサーバ名が残り、切替作業で50分迷った。

監査・是正対応として最も適切なものはどれか。

ア：復旧できたため、RTO未達は指摘せず完了とする。

イ：RPOは達成しているので、RTOの評価は不要とする。

ウ：改善計画を作るだけで、次回の有効性確認は行わない。

エ：RTO未達の原因を分析し、手順書更新や作業改善の責任者・期限を定め、次回訓練で有効性を確認する。

答え・解説 正答：エ

ア：復旧した事実と目標時間内に復旧したかは別です。

イ：RTOとRPOは別の目標であり、それぞれ評価します。

ウ：計画だけでなく実装・有効性までフォローアップします。

エ：目標未達は原因と改善策を管理し、再訓練で効果を確認する必要があります。

総合解説：監査・是正では、目標値に対する実績差を証拠として扱い、根本原因と改善効果を確認します。

対象：2026年度 / 基準日 2026-09-05

0135 教育・監査・総合判断 > 表・ログ・規程読解・複数論点の実務判断 ｜ 難易度：標準

O社は四半期ごとに重要システムの復旧訓練を行っている。
今回の結果は次のとおり。

【目標】RTO：4時間、RPO：1時間
【実績】復旧完了：5時間20分、復元データ：障害発生の45分前
【備考】手順書に古いサーバ名が残り、切替作業で50分迷った。

訓練結果の評価として最も適切なものはどれか。

ア：RPOは1時間以内を満たすがRTOは1時間20分超過しており、古い手順書が復旧遅延の一因として是正対象になる。

イ：復元データが45分前なのでRPOは未達である。

ウ：復旧完了が5時間20分でも、最終的に復旧したためRTO達成である。

エ：手順書の古いサーバ名はデータ復元量にだけ影響し、RTOには関係しない。

答え・解説 正答：ア

ア：障害45分前まで復元できているためRPO 1時間以内です。一方、復旧5時間20分はRTO 4時間を超えています。

イ：45分は1時間以内なのでRPOを満たします。

ウ：RTOは目標復旧時間なので、5時間20分は未達です。

エ：切替時の50分遅延は復旧時間へ直接影響しています。

総合解説：RTOとRPOを混同せず、数値目標と実績を別々に比較して原因まで結び付けることが重要です。

対象：2026年度 / 基準日 2026-09-05

0136 教育・監査・総合判断 > 教育・訓練・内部不正防止 ｜ 難易度：標準

P社の顧客対応部では、問い合わせ対応のため顧客情報を扱う。
社内規程では「顧客情報を外部送信する場合、宛先・添付内容を確認し、必要に応じて上長承認を得る」と定めている。
監査で、担当者3名が承認対象の一覧ファイルを上長確認なしで送信していたことが分かった。

教育内容として最も適切なものはどれか。

ア：個人情報保護は法務担当だけの業務なので、顧客対応部には教育しない。

イ：誤送信や過剰送信の事例を用い、宛先確認・データ最小化・承認・事故時報告を具体的手順として訓練する。

ウ：規程違反を防ぐため、顧客情報を扱う全業務を停止する。

エ：承認が必要な理由は説明せず、『ルールだから守る』だけを伝える。

答え・解説 正答：イ

ア：実際に情報を扱う担当者への教育が必要です。

イ：実際の業務場面に沿って、なぜ確認・承認が必要かまで理解させることが有効です。

ウ：業務停止ではなく、適切な管理の下で必要な業務を継続します。

エ：理由を理解させることで例外的な場面でも適切な判断につながります。

総合解説：教育では、法令・規程の名称だけでなく、日常業務でどの行動を取るべきかまで落とし込むことが重要です。

対象：2026年度 / 基準日 2026-09-05

0137 教育・監査・総合判断 > コンプライアンス・監査・是正 ｜ 難易度：標準

P社の顧客対応部では、問い合わせ対応のため顧客情報を扱う。
社内規程では「顧客情報を外部送信する場合、宛先・添付内容を確認し、必要に応じて上長承認を得る」と定めている。
監査で、担当者3名が承認対象の一覧ファイルを上長確認なしで送信していたことが分かった。

監査後の対応として最も適切なものはどれか。

ア：違反者3名を処分すれば、手順やシステムの見直しは不要とする。

イ：情報漏えいが発生していないため、規程違反は監査指摘にしない。

ウ：違反の原因を確認し、承認手順の実行可能性や記録方法を見直し、未承認送信を防ぐ是正策を期限付きで実施する。

エ：監査結果を保存するだけで、改善責任者や期限を定めない。

答え・解説 正答：ウ

ア：処分だけでは手順の不備や運用上の障害が残る可能性があります。

イ：事故未発生でも統制逸脱は是正対象です。

ウ：違反の背景を分析し、個人対応とプロセス改善の両方を検討する必要があります。

エ：責任者・期限・完了条件を定めることで改善を管理できます。

総合解説：監査は事故の有無だけでなく、統制が設計どおり運用されているかを確認し、不備を是正へつなげます。

対象：2026年度 / 基準日 2026-09-05

0138 教育・監査・総合判断 > 表・ログ・規程読解・複数論点の実務判断 ｜ 難易度：標準

P社の顧客対応部では、問い合わせ対応のため顧客情報を扱う。
社内規程では「顧客情報を外部送信する場合、宛先・添付内容を確認し、必要に応じて上長承認を得る」と定めている。
監査で、担当者3名が承認対象の一覧ファイルを上長確認なしで送信していたことが分かった。

規程と監査結果から最も適切に判断できるものはどれか。

ア：実際の誤送信がなければ、承認なし送信は規程適合である。

イ：担当者本人が宛先確認したなら、上長承認要件は自動的に免除される。

ウ：3名だけの違反なので、規程の存在自体を無効と判断する。

エ：承認対象ファイルを上長確認なしで送信した3件は規程不適合であり、承認記録の仕組みも含めて是正すべきである。

答え・解説 正答：エ

ア：事故発生の有無と規程順守は別問題です。

イ：本人確認と上長承認は異なる統制です。

ウ：違反件数だけで規程の有効性を否定することはできません。

エ：規程に承認要件がある以上、対象送信を未承認で行った事実は不適合です。

総合解説：規程読解問題では、条文の条件と事実を一つずつ対応付けて判断します。

対象：2026年度 / 基準日 2026-09-05

0139 教育・監査・総合判断 > 教育・訓練・内部不正防止 ｜ 難易度：標準

Q社の研究所では、実験装置からデータを取り出すためUSBメモリを使用している。
規程では「会社貸与の暗号化USBのみ使用可」「利用前後に台帳記録」「紛失時は直ちに報告」と定めている。
自己点検では、10人中2人が私物USBを使ったことがあると回答した。

教育として最も適切なものはどれか。

ア：私物媒体利用がマルウェア感染・情報持出し・紛失追跡不能につながることを説明し、貸与媒体の利用と報告手順を訓練する。

イ：暗号化USBなら紛失しても必ず安全なので、紛失報告は不要と教える。

ウ：研究者は専門職なので、媒体管理ルールの教育対象外とする。

エ：私物USBの利用を黙認し、事故時だけ注意する。

答え・解説 正答：ア

ア：具体的リスクを理解させ、正規の利用手順を身に付けさせるのが適切です。

イ：暗号化は重要ですが、紛失事故の報告・回収対応は必要です。

ウ：専門職でも組織の情報資産を扱う以上ルール順守が必要です。

エ：黙認すると規程が形骸化し、管理外媒体が増えます。

総合解説：媒体管理教育では、禁止事項だけでなく、なぜ管理対象媒体を使うのかを理解させることが重要です。

対象：2026年度 / 基準日 2026-09-05

0140 教育・監査・総合判断 > コンプライアンス・監査・是正 ｜ 難易度：標準

Q社の研究所では、実験装置からデータを取り出すためUSBメモリを使用している。
規程では「会社貸与の暗号化USBのみ使用可」「利用前後に台帳記録」「紛失時は直ちに報告」と定めている。
自己点検では、10人中2人が私物USBを使ったことがあると回答した。

自己点検結果への対応として最も適切なものはどれか。

ア：違反者が2人だけなので、統制上の問題はないと判断する。

イ：私物USB利用の原因と対象データを確認し、貸与媒体の不足や手順上の問題を是正し、利用記録を再点検する。

ウ：自己申告した2人だけを処罰し、正規USBの配備状況は確認しない。

エ：規程を守れない社員がいるため、台帳記録も廃止する。

答え・解説 正答：イ

ア：少数でも機密研究データが関係すれば重大リスクになり得ます。

イ：違反の背景に設備不足や不便な手順がないか確認し、統制を実効的に改善します。

ウ：個人対応だけでは構造的な原因が残る可能性があります。

エ：台帳廃止は追跡性をさらに低下させます。

総合解説：是正では、人の順守だけでなく、必要な機器が提供されているか、手順が実行可能かも確認します。

対象：2026年度 / 基準日 2026-09-05

0141 教育・監査・総合判断 > 表・ログ・規程読解・複数論点の実務判断 ｜ 難易度：標準

Q社の研究所では、実験装置からデータを取り出すためUSBメモリを使用している。
規程では「会社貸与の暗号化USBのみ使用可」「利用前後に台帳記録」「紛失時は直ちに報告」と定めている。
自己点検では、10人中2人が私物USBを使ったことがあると回答した。

規程と自己点検結果から最も適切な判断はどれか。

ア：私物USBが暗号化されていれば、会社貸与でなくても規程適合である。

イ：自己申告で発覚した違反は監査対象にしてはいけない。

ウ：私物USBを利用した2人は規程不適合であり、利用データの確認とともに正規媒体の供給・台帳運用も点検すべきである。

エ：紛失事故が起きていないので、媒体管理の不適合は存在しない。

答え・解説 正答：ウ

ア：私物側の暗号化だけでは会社貸与要件を満たしません。

イ：自己申告も統制改善に利用できる情報です。

ウ：規程は会社貸与の暗号化USBに限定しているため、私物利用は不適合です。

エ：事故未発生でも規程違反は不適合として評価します。

総合解説：表面的な違反者確認だけでなく、正規手段が十分提供されているかまで見ると、実効的な改善につながります。

対象：2026年度 / 基準日 2026-09-05

0142 教育・監査・総合判断 > 教育・訓練・内部不正防止 ｜ 難易度：標準

R社は年1回、情報漏えいを想定した机上訓練を実施した。
訓練では、現場からCSIRTへの第一報に25分かかり、広報担当への連絡先が古くて15分遅延した。
規程上の目標は「重大インシデントは発見後10分以内にCSIRTへ第一報」である。

次回教育で重点化すべき内容として最も適切なものはどれか。

ア：訓練で遅延した担当者だけに規程を読ませ、組織訓練は中止する。

イ：連絡先は頻繁に変わるので、更新せず当日調べる方法を教育する。

ウ：第一報は詳細調査が完了してから行うよう教育する。

エ：重大度判断、10分以内の第一報、代替連絡先、部門間の役割分担を実際のシナリオで反復訓練する。

答え・解説 正答：エ

ア：個人だけでなく連絡網や役割設計にも問題があります。

イ：緊急連絡先は平時に更新・確認すべきです。

ウ：第一報は原因確定後ではなく、重大事象を早期共有するために行います。

エ：今回の遅延要因を具体的な訓練項目へ反映するのが適切です。

総合解説：インシデント訓練では、知識だけでなく時間制約の中で役割を実行できることを確認します。

対象：2026年度 / 基準日 2026-09-05

0143 教育・監査・総合判断 > コンプライアンス・監査・是正 ｜ 難易度：標準

R社は年1回、情報漏えいを想定した机上訓練を実施した。
訓練では、現場からCSIRTへの第一報に25分かかり、広報担当への連絡先が古くて15分遅延した。
規程上の目標は「重大インシデントは発見後10分以内にCSIRTへ第一報」である。

是正対応として最も適切なものはどれか。

ア：第一報遅延と連絡先不備を不適合として記録し、責任者・期限を決めて連絡網と手順を更新し再訓練する。

イ：実被害がなかったため、訓練上の不備は是正しない。

ウ：25分でも最終的に報告できたので、10分目標は評価しない。

エ：連絡先更新だけ実施し、第一報遅延の原因は分析しない。

答え・解説 正答：ア

ア：訓練で発見した不備は本番事故前に是正できる貴重な情報です。

イ：実被害がなくても訓練目的は統制の有効性確認です。

ウ：規程の10分目標と実績を比較する必要があります。

エ：複数の遅延原因をそれぞれ是正します。

総合解説：訓練は監査・改善の入力情報となり、発見した不備を再訓練で確認することで継続的改善が成立します。

対象：2026年度 / 基準日 2026-09-05

0144 教育・監査・総合判断 > 表・ログ・規程読解・複数論点の実務判断 ｜ 難易度：標準

R社は年1回、情報漏えいを想定した机上訓練を実施した。
訓練では、現場からCSIRTへの第一報に25分かかり、広報担当への連絡先が古くて15分遅延した。
規程上の目標は「重大インシデントは発見後10分以内にCSIRTへ第一報」である。

訓練結果の評価として最も適切なものはどれか。

ア：第一報は25分なので、10分目標を15分下回って達成している。

イ：第一報は目標10分に対し25分で15分超過しており、連絡先不備による追加遅延も含め、初動連絡プロセスの改善が必要である。

ウ：広報連絡の15分遅延があるため、CSIRT第一報25分は評価対象外である。

エ：机上訓練は実事故ではないため、規程目標との比較は行わない。

答え・解説 正答：イ

ア：25分は10分より長いため未達です。

イ：25分－10分＝15分の超過です。さらに別の連絡先不備も発見されています。

ウ：広報遅延とCSIRT第一報遅延は別の改善論点です。

エ：訓練こそ規程や目標が実行可能か確認する場です。

総合解説：科目Bでは、規程の目標値と実績を正しく比較し、複数の遅延要因を切り分けて改善判断する力が求められます。

対象：2026年度 / 基準日 2026-09-05

0145 教育・監査・総合判断 > 教育・訓練・内部不正防止 ｜ 難易度：応用

S社では本番システムの変更について、規程で次を定めている。
・変更申請者と承認者は原則として別人
・本番適用前にテスト結果を記録
・緊急変更は事後1営業日以内に責任者レビュー

監査対象10件のうち、通常変更1件で自己承認、2件でテスト記録なし、緊急変更1件で3営業日後にレビューされていた。

変更担当者への教育として最も適切なものはどれか。

ア：システムに詳しい担当者なら自己承認してよいと教育する。

イ：テストに成功したら記録は不要と教育する。

ウ：承認分離、テスト記録、緊急変更レビューが不正・誤変更の予防と事後検証にどう役立つかを具体例で教育する。

エ：緊急変更は急ぐため、事後レビューを省略してよいと教育する。

答え・解説 正答：ウ

ア：専門性が高くても自己承認は相互牽制を弱めます。

イ：テスト記録は実施事実と結果を後から確認するために必要です。

ウ：各統制の目的まで理解させることで、例外時にも適切な判断がしやすくなります。

エ：緊急時こそ事後レビューで妥当性を確認します。

総合解説：統制教育では『手続を守る』だけでなく、その手続が防ぐリスクを理解させることが有効です。

対象：2026年度 / 基準日 2026-09-05

0146 教育・監査・総合判断 > コンプライアンス・監査・是正 ｜ 難易度：応用

S社では本番システムの変更について、規程で次を定めている。
・変更申請者と承認者は原則として別人
・本番適用前にテスト結果を記録
・緊急変更は事後1営業日以内に責任者レビュー

監査対象10件のうち、通常変更1件で自己承認、2件でテスト記録なし、緊急変更1件で3営業日後にレビューされていた。

監査結果の扱いとして最も適切なものはどれか。

ア：10件中一部だけなので、全て監査上問題なしとする。

イ：変更後に障害が起きていないため、規程違反は指摘しない。

ウ：最も件数の多いテスト記録欠落だけを扱い、他の不適合は無視する。

エ：自己承認、テスト記録欠落、緊急レビュー遅延をそれぞれ規程不適合として原因・リスクを評価し是正する。

答え・解説 正答：エ

ア：少数でも重大な統制逸脱は評価対象です。

イ：障害の有無と統制順守は別です。

ウ：件数が少ない自己承認やレビュー遅延も重要なリスクになり得ます。

エ：規程上の要求ごとに適合性を判断し、発生件数とリスクを踏まえて是正します。

総合解説：監査では『何件違反したか』だけでなく、どの統制が破られ、どのリスクが生じたかを評価します。

対象：2026年度 / 基準日 2026-09-05

0147 教育・監査・総合判断 > 表・ログ・規程読解・複数論点の実務判断 ｜ 難易度：応用

S社では本番システムの変更について、規程で次を定めている。
・変更申請者と承認者は原則として別人
・本番適用前にテスト結果を記録
・緊急変更は事後1営業日以内に責任者レビュー

監査対象10件のうち、通常変更1件で自己承認、2件でテスト記録なし、緊急変更1件で3営業日後にレビューされていた。

規程と監査結果から最も適切な判断はどれか。

ア：通常変更では自己承認1件とテスト記録欠落2件、緊急変更ではレビュー期限超過1件があり、少なくとも三種類の統制不適合が存在する。

イ：テスト記録欠落が2件あるため、不適合の種類も2種類だけである。

ウ：緊急変更は例外なので、3営業日後レビューでも規程適合である。

エ：自己承認は1件だけなので、職務分掌の規程は満たしている。

答え・解説 正答：ア

ア：件数と不適合の種類を分けて読む必要があります。提示事実では三種類の統制違反があります。

イ：件数2はテスト記録欠落の発生件数であり、不適合種類数ではありません。

ウ：規程は緊急変更も1営業日以内の事後レビューを要求しています。

エ：1件でも原則に反する自己承認は不適合として評価対象です。

総合解説：複数論点問題では、件数・種類・例外条件を混同せず、規程の各条件へ事実を対応付けます。

対象：2026年度 / 基準日 2026-09-05

0148 教育・監査・総合判断 > 教育・訓練・内部不正防止 ｜ 難易度：応用

T社の月次セキュリティ会議で、次の指標が報告された。

【指標】
1. インターネット公開VPN装置：重大脆弱性あり、実悪用情報あり、未修正
2. 退職者アカウント：4件残存、うち1件に直近ログインあり
3. フィッシング訓練：資格情報入力率2%
4. バックアップ復元試験：成功、RTO目標内
5. 内部監査指摘：前月の「特権ログレビュー未実施」が今月も未完了

経営層は、限られた要員で優先対応を決める必要がある。

教育・訓練面で優先して行うべき対応として最も適切なものはどれか。

ア：バックアップ復元試験が成功した担当者だけを再教育する。

イ：フィッシングで資格情報を入力した層への追加訓練と、特権管理担当者へのログレビュー手順再教育を実施する。

ウ：重大脆弱性は教育だけで修正できるため、技術対応は不要とする。

エ：退職者アカウント残存は人事・IT連携の問題ではないため、手順教育は不要とする。

答え・解説 正答：イ

ア：復元試験は目標内で成功しており、提示情報上の優先教育対象ではありません。

イ：人的弱点が表れているフィッシングと、未実施統制が続く特権ログレビューには教育・手順改善が有効です。

ウ：脆弱性は技術的な修正・緩和が必要で、教育だけでは解消しません。

エ：退職者アカウントは人事・ITの役割と手順教育も改善対象になり得ます。

総合解説：総合判断では、教育で解決すべき問題と、技術・運用で直ちに対処すべき問題を分けて考えます。

対象：2026年度 / 基準日 2026-09-05

0149 教育・監査・総合判断 > コンプライアンス・監査・是正 ｜ 難易度：応用

T社の月次セキュリティ会議で、次の指標が報告された。

【指標】
1. インターネット公開VPN装置：重大脆弱性あり、実悪用情報あり、未修正
2. 退職者アカウント：4件残存、うち1件に直近ログインあり
3. フィッシング訓練：資格情報入力率2%
4. バックアップ復元試験：成功、RTO目標内
5. 内部監査指摘：前月の「特権ログレビュー未実施」が今月も未完了

経営層は、限られた要員で優先対応を決める必要がある。

監査・是正の観点から最も適切な対応はどれか。

ア：監査指摘は一度記録すれば、完了しなくても翌月以降は追跡しない。

イ：技術脆弱性がある月は、内部監査指摘の是正を全て停止する。

ウ：前月から未完了の特権ログレビュー指摘を再評価して期限・責任者を明確化し、退職者アカウント残存など関連統制も監査対象として確認する。

エ：退職者アカウントは運用担当者の問題なので、監査では扱わない。

答え・解説 正答：ウ

ア：監査指摘は完了と有効性が確認されるまで管理する必要があります。

イ：重大脆弱性対応と監査是正は優先順位を調整しつつ並行管理できます。

ウ：未完了指摘はフォローアップし、関連するアクセス管理統制も必要に応じて確認します。

エ：退職者アカウントはアクセス管理の統制不備として監査対象になり得ます。

総合解説：監査・是正では、未完了事項を放置せず、リスクの変化を踏まえて優先順位と期限を再設定します。

対象：2026年度 / 基準日 2026-09-05

0150 教育・監査・総合判断 > 表・ログ・規程読解・複数論点の実務判断 ｜ 難易度：応用

T社の月次セキュリティ会議で、次の指標が報告された。

【指標】
1. インターネット公開VPN装置：重大脆弱性あり、実悪用情報あり、未修正
2. 退職者アカウント：4件残存、うち1件に直近ログインあり
3. フィッシング訓練：資格情報入力率2%
4. バックアップ復元試験：成功、RTO目標内
5. 内部監査指摘：前月の「特権ログレビュー未実施」が今月も未完了

経営層は、限られた要員で優先対応を決める必要がある。

提示された指標だけを前提に、最も緊急性が高い対応として適切なものはどれか。

ア：バックアップ復元試験が成功したため、他の全リスク対応を翌月まで延期する。

イ：フィッシング入力率2%だけを最優先し、実悪用中の脆弱性は定例パッチ日まで放置する。

ウ：監査指摘が未完了なので、VPN脆弱性や退職者アカウントより監査文書の更新だけを優先する。

エ：実悪用情報のあるインターネット公開VPNの重大脆弱性を直ちに修正又は緩和し、同時に直近利用のある退職者アカウントを停止・調査する。

答え・解説 正答：エ

ア：バックアップ成功は良い状態ですが、他リスクを延期する根拠にはなりません。

イ：教育も必要ですが、現に悪用可能な重大脆弱性の緊急性が高いです。

ウ：監査文書の更新だけでは現在の技術・アクセスリスクを除去できません。

エ：外部公開・重大・実悪用ありという条件は侵害可能性が高く、退職者アカウントの実利用も進行中の不正利用を疑うため緊急です。

総合解説：科目Bの総合問題では、発生可能性、外部露出、実悪用、現在進行中の兆候、影響を組み合わせて優先順位を決めます。

対象：2026年度 / 基準日 2026-09-05