PCISSC.Assessor_New_V4.v2024-02-22.q29

試験コード:	Assessor_New_V4
試験名称:	Assessor_New_V4 Exam
認定資格:	PCI SSC
無料問題数:	29
バージョン:	v2024-02-22
アクセス数:	387
ページビュー数:	290
https://www.jpnpdf.com/PCISSC.Assessor_New_V4.v2024-02-22.q29-mondaishu.html	

最新問題: **1**
暗号化キーが廃止され、新しいキーに置き換えられる場合に当てはまるのは、次のどれですか?
A. 廃止されたキーは暗号化操作に使用してはなりません
B. 廃止されたキーの暗号化キー コンポーネントは、廃棄する前に 3 か月間保持する必要があります
C. 新しいキー管理者を割り当てる必要があります
D. 廃止されたキーで暗号化されたすべてのデータは安全に破棄する必要があります
Answer: A (メーッセージを残す**)**
説明
PCI DSS 要件 3.6.4 では、キーが暗号化期間の終わりに達した場合、エンティティはキーを廃棄または交換する必要があると規定しています。暗号化期間とは、特定のキーを暗号化操作に使用できる期間です1。廃止されたキーは暗号化操作に使用しないでください。暗号解析によって侵害または弱化されている可能性があり、データを適切に保護できない可能性があります。廃止されたキーは、必要に応じて、廃止されたキーで暗号化された履歴データにアクセスするための復号化操作に引き続き使用できます2。
したがって、正解は選択肢Aです。
暗号キーの廃止と置換に関しては、他のオプションは当てはまりません。選択肢 B は当てはまりません。PCI DSS では、ビジネス上または法的理由で不要になった暗号素材を安全に削除することがエンティティに求められていますが、PCI DSS では、廃止されたキーの暗号キー コンポーネントの保存期間が指定されていません。オプション C は当てはまりません。PCI DSS では、すべてのキー管理者の役割、責任、説明責任を定義し文書化することがエンティティに求められますが、PCI DSS では新しいキー管理者を割り当てる必要はありません。選択肢 D は当てはまりません。PCI DSS では、ビジネス上または法的な理由でカード会員データが不要になった場合、エンティティはカード会員データを読み取り不能

にする必要がありますが、廃止されたキーで暗号化されたすべてのデータを安全に破棄する必要はありません。参考文献:
PCI DSS v3.2.1
暗号化キー ブロック - PCI セキュリティ標準評議会

最新問題: **2**
部分評価は新たな評価結果です。 部分評価」とは何ですか？
A. どの要件をテストする必要があるかを決定するために SAQ を使用した後に完了した ROC。
FAQ 1331 による。(事業体が SAQ の資格基準を満たしている限り)
B. 最終的な ROC が完了する前の中間結果
C. 複数の支払いチャネルを持ち、各チャネルが独自の評価を持つ事業体を表すために、支払いブランドおよびアクワイアラによって使用される用語。
D. 少なくとも 1 つの要件が 未テスト」とマークされている評価*
Answer: D (メーッセージを残す)
説明
要件 3.1.2 によると、少なくとも 1 つの要件が 未テスト」とマークされている評価は部分的な評価とみなされます。これは、PCI DSS v3.2.1 クイック リファレンス ガイド 1 の付録 E で定義されているすべての要件と管理を満たしていないことを意味します。これは、PCI DSS に従って評価が確実に実施されるようにするための要件の 1 つです。

最新問題: **3**
用語集によると、オーダーメイドおよびカスタム ソフトウェアはどのタイプのソフトウェアを表していますか?
A. サードパーティによって開発されたソフトウェア
B. サードパーティによって開発され、エンティティによってカスタマイズできるソフトウェア。
C. エンティティが独自に使用するためにエンティティによって開発されたソフトウェア
D. 仮想決済端末
Answer: C (メーッセージを残す)
説明
用語集によると、オーダーメイドおよびカスタム ソフトウェアは、企業が独自に使用するために開発したソフトウェアを指します。つまり、他の企業と共有したり、適切な許可なしに販売または譲渡したりしてはならないことを意味します。これは、オーダーメイドおよびカスタム ソフトウェアが、PCI DSS v3.2.1 クイック リファレンス ガイド 1 の付録 E で定義されているすべてのセキュリティ標準と管理を確実に満たすための要件の 1 つです。

最新問題: **4**
ある小売業者には、暗号化された PAN データを保存するシステムを備えたサーバー ルームがあります。販売者は、誰が何日何時に部屋に出入りしたかを識別するバッジ アクセス

制御システムを導入しています。サーバー ルームにはビデオ カメラが設置されていません。この情報に基づくと、PCI DSS の物理的セキュリティ要件に関して正しいのはどれですか?
A. バッジ アクセス制御システムは、改ざんや無効化から保護する必要があります。
B. 販売者は既存のアクセス制御システムに加えてビデオ カメラを設置する必要があります
C. アクセス制御システムからのデータは毎月安全に削除する必要があります
D. 販売者は、既存のアクセス制御システムに加えて、モーション検知アラームを設置する必要があります
Answer: (解答を表示する**)**
説明
PCI DSS 要件 9.1.1 では、カード所有者データ環境 (CDE)1 内のシステムへの物理的アクセスを制限および監視するために、適切な施設入場制御を使用することが事業体に求められています。バッジ アクセス制御システムは、サーバー ルームに誰がいつ出入りしたかを識別できるため、そのような制御の一例です。ただし、この制御は、PCI DSS 要件 9.1.2 に記載されているように、権限のない人物による改ざんや無効化から保護されている場合にのみ有効です1。そうしないと、アクセス制御システムがバイパスまたは侵害され、暗号化された PAN データを保存するシステムへの不正アクセスが許可される可能性があります。したがって、オプション A に記載されているように、バッジ アクセス制御システムは改ざんまたは無効化から保護する必要があります。
サーバー ルームの PCI DSS 物理セキュリティ要件に関しては、他のオプションは当てはまりません。オプション B は当てはまりません。推奨されるベスト プラクティスではありますが、PCI DSS では既存のアクセス制御システムに加えてビデオ カメラの使用を義務付けていないからです2。PCI DSS ではアクセス制御システムのデータ保存期間が指定されていないため、オプション C は当てはまりません。ただし、PCI DSS では、監査証跡履歴を少なくとも 1 年間保存し、少なくとも 3 か月はすぐに分析に利用できるようにする必要があります3。オプション D は当てはまりません。PCI DSS では、既存のアクセス制御システムに加えてモーション センシング アラームを使用する必要がありませんが、これも推奨されるベスト プラクティスです2。参考文献:
PCI DSS v3.2.1
PCI DSS 要件 9: 物理的セキュリティの強化
PCI DSS 要件 10: ネットワーク リソースとカード所有者データへのすべてのアクセスを追跡および監視する

最新問題**: 5**
PCI DSS 評価中にビジネス施設のサンプルがレビューされます。評価者はサンプルについて何を検証する必要がありますか?
A. すべての評価についてレビューされる一貫した一連の機能が含まれています。
B. サンプル内の施設の数は、施設の総数の少なくとも 10% です
C. カード会員データが保管されているすべての施設が検査されます

D. 施設のすべてのタイプと場所が表されます
Answer: (解答を表示する**)**
説明
PCI DSS では、評価者は、ビジネス施設のサンプルが評価の対象となる施設全体を代表していることを検証する必要があります。PCI DSS 要件に準拠
12.8.5、どの PCI DSS 要件が各サービス プロバイダーによって管理され、どの PCI DSS 要件がエンティティによって管理されるかに関する情報を維持する。」さらに、PCI DSS 要件 12.9.1 によれば、「サービス プロバイダーの場合、要件に指定されているとおり、書面による同意/承認を顧客に提供する必要があります。」
したがって、ビジネス施設のサンプルを検証するための PCI DSS 要件を満たすシナリオは、評価がカード製造環境の多様性と複雑さを確実にカバーするように、施設のすべての種類と場所が代表されるシナリオです。他のシナリオは、施設の変動性を考慮していないか、PCI DSS によって定義されたサンプリング方法論に従っていません。参考資料: PCI DSS v3.2.1、Card Production Security Assessor - Physical - Credly

最新問題**: 6**
PCI DSS 要件 10 に準拠しています。監査ログはどのくらいの期間保持する必要がありますか?
A. 少なくとも 1 年、最新の 3 か月はすぐに利用可能
B. 少なくとも 2 年、最新の 3 か月はすぐに利用可能
C. 少なくとも 2 年間、最新の月がすぐに利用可能
D. 少なくとも 3 か月 (最新の月はすぐに利用可能)
Answer: (解答を表示する**)**
説明
PCI DSS v3.2.1 クイック リファレンス ガイド1 によると、監査ログは少なくとも 1 年間保持し、最新の 3 か月はすぐに利用できるようにする必要があります。これは、監査ログをレビューと分析に確実に利用できるようにするための要件の 1 つです。

最新問題**: 7**
脆弱性にリスクランクを割り当てる目的は何ですか?
A. すべての脆弱性が 30 日以内に解決されるようにします
B. 四半期ごとの ASV スキャンの必要性を置き換えます。
C. より迅速に対処できるように、最もリスクの高い項目に優先順位を付けます。
D. 重要なセキュリティ パッチが少なくとも四半期ごとにインストールされていることを確認します。
Answer: (解答を表示する**)**
説明
PCI DSS v3.2.1 クイック リファレンス ガイド 1 によると、脆弱性にリスク ランクを割り当てる目的は、すべての脆弱性が 30 日以内に対処されることを保証したり、必要な問題を

置き換えたりするのではなく、リスクの最も高い項目を優先してより迅速に対処できるようにすることです。四半期ごとの ASV スキャン、または重要なセキュリティ パッチが少なくとも四半期ごとにインストールされていることを確認します。これは、脆弱性をできるだけ早く特定して軽減するための要件の 1 つです。

最新問題: **8**
PCI DSS 要件で使用される時間枠の説明に示されている 四半期」の定義を満たすのは次のうちどれですか?
A. 年の各四半期のある時点で発生します
B. 少なくとも 95 ～ 97 日に 1 回。
C. 毎月 3 か月の 15 日
D. 各 4 月 1 日
Answer: C (メーッセージを残す**)**
説明
PCI DSS v3.2.1 クイック リファレンス ガイド 1 によると、四半期とは、少なくとも 95 日または 97 日に 1 回ではなく、1 年の各四半期のある時点で発生することを意味します。これは、PCI DSS 評価が定期的に実施されるようにするための要件の 1 つです。

最新問題: **9**
ある小売業者には、暗号化された PAN データを保存するシステムを備えたサーバー ルームがあります。販売者は、何日何時に部屋に出入りしたのかを識別するバッジ アクセス制御システムを導入しています。サーバー ルームにはビデオ カメラが設置されていません。この情報に基づくと、PCI DSS の物理的セキュリティ要件に関して正しいのはどれですか?
A. バッジ アクセス制御システムは、改ざんや無効化から保護する必要があります。
B. 販売者は既存のアクセス制御システムに加えてビデオ カメラを設置する必要があります
C. アクセス制御システムからのデータは毎月安全に削除する必要があります
D. 販売者は、既存のアクセス制御システムに加えて、モーション検知アラームを設置する必要があります
Answer: (解答を表示する**)**
説明
PCI DSS v3.2.1 クイック リファレンス ガイド1 によると、この情報に基づいて、PCI DSS の物理的セキュリティ要件に関して正しいのはどれですか? サーバー ルームにはビデオ カメラがないため、販売者は既存のアクセス制御システムに加えてビデオ カメラを設置する必要があります。この情報に基づくと、PCI DSS の物理的セキュリティ要件に関して正しいのはどれですか? サーバー ルームにはビデオ カメラがないため、販売者は既存のアクセス制御システムに加えてモーション センシング アラームを設置する必要があります。この情報に基づくと、PCI DSS の物理的セキュリティ要件に関して正しいのはどれですか? サーバー ルームにはビデオ カメラがないため、販売者は既存のアクセス制御システムに加

えてビデオ カメラを設置する必要があります。この情報に基づくと、PCI DSS の物理的セキュリティ要件に関して正しいのはどれですか? サーバー ルームにはビデオ カメラがないため、販売者は既存のアクセス制御システムに加えてモーション センシング アラームを設置する必要があります。この情報に基づくと、PCI DSS の物理的セキュリティ要件に関して正しいのはどれですか? 加盟店にはビデオ カメラが設置されていないため、既存のアクセス制御システムに加えてビデオ カメラを設置する必要があります。

最新問題: **10**
要件 1 によると、「ネットワーク セキュリティ管理」の目的は何ですか?
A. CDE 全体でマルウェア対策を管理します。
B. 2 つ以上の論理または物理ネットワーク セグメント間のネットワーク トラフィックを制御します。
C. 脆弱性を発見し、ランク付けします。
D. 保存時に PAN を暗号化する
Answer: B (メーッセージを残す**)**
説明
要件 1 によると、ネットワーク セキュリティ制御は、2 つ以上の論理または物理ネットワーク セグメント間のネットワーク トラフィックを制御することを目的としています。つまり、ネットワーク上のカード所有者のデータやトランザクションの不正なアクセス、変更、開示を防止する必要があります。これは、PCI DSS に従ってネットワーク セキュリティ制御が実装および維持されることを保証するための要件の 1 つです。

最新問題: **11**
カード会員データを含むデータベースへのアクセスを制限するための PCI DSS 要件を満たすシナリオはどれですか?
A. データベースへのユーザー アクセスはプログラムによる方法のみを使用します。
B. データベースへのユーザー アクセスはシステム管理者とネットワーク管理者に制限されています
C. データベース アプリケーションのアプリケーション ID はデータベース管理者のみが使用できます
D. データベースへの直接クエリは共有データベース管理者アカウントに制限されます
Answer: A (メーッセージを残す**)**
説明
PCI DSS では、カード会員データを含むデータベースへのアクセスを許可されたユーザーおよびアプリケーションに制限し、そのようなデータベースへの直接アクセスを禁止することが求められています。PCI DSS 要件に準拠
7.1.2、「特権ユーザー ID へのアクセスを、職務の遂行に必要な最小限の権限に制限する。」
さらに、PCI DSS 要件 8.3.1 によれば、「管理アクセスを持つ担当者のカード会員データ環境へのコンソール以外のすべてのアクセスに対して多要素認証を実装する」とされていま

す。したがって、カード所有者データを含むデータベースへのアクセスを制限するための PCI DSS 要件を満たすシナリオは、データベースへのユーザー アクセスが、認証、承認、暗号化を強制するアプリケーション インターフェイスなどのプログラム的な方法のみを介して行われるシナリオです。他のシナリオでは、データベースへの直接アクセスを許可するか、アクセスを必要最小限の権限に制限しないか、管理アクセスに多要素認証を使用しません。参考文献: [PCI DSS v3.2.1]、カード製造セキュリティ評価者 - 論理 - Credly

最新問題: **12**
支払い取引プロセスのどの段階で、加盟店の銀行は加盟店に購入代金を支払い、カード所有者の銀行はカード保有者に請求を行いますか?
A. 認可
B. クリアリング
C. 決済
D. チャージバック
Answer: C (メーッセージを残す**)**
説明
PCI DSS v3.2.1 クイック リファレンス ガイド 1 によると、決済は、加盟店が完了した取引に対してカード発行会社から支払いを受け取り、両当事者が事前に合意したとおり、顧客またはその他の当事者に商品またはサービスを提供するときに発生します。配達または支払いの際にいずれかの当事者によって課される条件。これには、配達または支払いの際にいずれかの当事者による受諾、拒否、返品、交換、返金、キャンセル、変更、一時停止、終了または取り消しが含まれますが、これらに限定されません。または、配送時または支払い時にいずれかの当事者によって課されるその他の条件。または、配送時または支払い時にいずれかの当事者によって課されるその他の条件。または、配送時または支払い時にいずれかの当事者によって課されるその他の条件。

最新問題: **13**
企業は、評価中にソフトウェア セキュリティ フレームワークを利用できるかどうかを知りたいと考えています。これは次のソフトウェア タイプのどれに適用されますか?
A. CDE 内の任意の支払いソフトウェア
B. PCI PTS デバイス上で実行されるソフトウェアのみ
C. PCI SSC によってリストされ、PA-DSS 評価を受けている検証済みの支払いアプリケーション
D. Secure SLC 標準に従って事業体によって開発されたソフトウェア
Answer: A (メーッセージを残す**)**
説明
ソフトウェア セキュリティ フレームワーク (SSF) は、決済ソフトウェアの安全な設計と開発のための標準とプログラムの集合です1。SSF は、Payment Application Data Security Standard (PA-DSS) を、より幅広い種類の支払いソフトウェア、テクノロジ、および開発手法をサポートする最新の要件に置き換えます2。SSF は、カード会員データ環境 (CDE) の

一部であるあらゆる支払いソフトウェアに適用されます。CDE とは、カード会員データや機密認証データを保存、処理、送信する人、プロセス、およびテクノロジーです3。したがって、正解は選択肢Aです。
他のオプションは、さまざまな種類のソフトウェアに対する SSF の適用性に関しては当てはまりません。オプション B は当てはまりません。SSF は、やり取りの時点で支払いカード データを受け入れるハードウェア デバイスである PCI PTS デバイス上で実行されるソフトウェアに限定されないからです。SSF は、Web サーバー、モバイル デバイス、クラウド サービス、組み込みシステムなど、さまざまなプラットフォームやデバイス上で実行されるソフトウェアをカバーしています。オプション C は当てはまりません。SSF は、PCI SSC によってリストされ、PA-DSS 評価を受けている検証済みの支払いアプリケーション、つまり PA-DSS 評価機関によって検証され、PA-DSS 要件を満たしている支払いアプリケーションに限定されないためです。。SSF は、加盟店やサービス プロバイダーが独自に使用するために開発したソフトウェア、または第三者に販売、配布、またはライセンス供与されていないソフトウェアなど、PA-DSS 検証の対象とならない可能性のある支払いソフトウェアを対象としています。選択肢 D は当てはまりません。SSF は、Secure SLC Standard に従って企業が開発したソフトウェアに限定されないからです。Secure SLC Standard は、SSF の一部であり、ソフトウェア ベンダーにセキュリティ要件と評価手順を提供する 2 つの標準のうちの 1 つです。ソフトウェア開発ライフサイクルに統合します。SSF は、セキュア ソフトウェア標準のセキュリティ要件と検証手順を満たしている限り、ソフトウェア ベンダー、マーチャント、サービス プロバイダー、サードパーティなど、あらゆる主体によって開発された決済ソフトウェアを対象としています。もう 1 つは SSF の一部であり、決済ソフトウェア製品のセキュリティ要件と評価手順を規定する標準です。参考文献:
PCI ソフトウェア セキュリティ フレームワークを理解する: 新しい教育リソース PCI ソフトウェア セキュリティ フレームワークは、決済ソフトウェア セキュリティへの最新のアプローチを提供します PCI DSS v3.2.1
[PCI PTS POI セキュリティ要件]
【ソフトウェアセキュリティフレームワークセキュアソフトウェア標準】
【決済アプリケーションデータセキュリティ基準】
【ソフトウェアセキュリティフレームワークセキュアソフトウェアライフサイクル セキュアSLC）規格】
[PCI DSS v4.0: カスタマイズされたアプローチはあなたの組織に適していますか?]

最新問題**: 14**
企業は、評価中にソフトウェア セキュリティ フレームワークを利用できるかどうかを知りたいと考えています。これは次のソフトウェア タイプのどれに適用されますか?
A. CDE 内の任意の支払いソフトウェア
B. PCI PTS デバイス上で実行されるソフトウェアのみ

C. PCI SSC によってリストされ、PA-DSS 評価を受けている検証済みの支払いアプリケーション
D. Secure SLC 標準に従って事業体によって開発されたソフトウェア
Answer: D (メーッセージを残す**)**
説明
要件 12.3.2 によると、Secure SLC Standard に従ってエンティティによって開発されたソフトウェアは、エンティティが CDE で使用する前に、Qualified Security Assessor (QSA) によって検証される必要があります。これは、Secure SLC 標準に従って企業によって開発されたソフトウェアが、PCI DSS v3.2.1 クイック リファレンス ガイド 1 の付録 E で定義されているすべてのセキュリティ標準と管理を確実に満たすための要件の 1 つです。

最新問題**: 15**
デフォルトのアカウントとデフォルトの管理者アカウントのパスワードは次のようにすべきですか?
A. ネットワーク上にシステムをインストールしてから 30 日以内に変更されました。
B. ネットワークにシステムをインストールする前にデフォルトのパスワードにリセットします。
C. ネットワークにシステムをインストールする前に変更されました
D. 30 日で期限切れになるように構成されています
Answer: C (メーッセージを残す**)**
説明
PCI DSS v3.2.1 クイック リファレンス ガイド1 によると、ネットワーク上にシステムをインストールする前に、デフォルト アカウントとデフォルトの管理者アカウントのパスワードを変更する必要があります。これは、カード会員データへの不正アクセスを防ぐための要件の 1 つです。

最新問題**: 16**
カード会員データを含むメディアを分類する目的は何ですか?
A. メディアに含まれるデータの機密性に応じてメディアの財産が保護されていることを確認します。
B. カード所有者データを含むメディアが四半期ごとに安全なエリアから移動されていることを確認する
C. メディアにカード所有者のデータが含まれていることをすべての担当者が認識できるように、メディアに明確かつ目に見えるラベルが付けられていることを確認します。
D. 内容に関係なく、すべてのメディアが同じスケジュールで一貫して破棄されるようにします。
Answer: A (メーッセージを残す**)**
説明
カード会員データを含むメディアの分類は、含まれるデータの機密性に応じてメディアの財産が確実に保護されるようにすることを目的としています。つまり、機密性または完全

性のレベルを示すラベルまたはタグをメディアに付ける必要があります。これは、カード所有者のデータを含むメディアに適切なラベルが付けられていることを確認するための要件の 1 つです。

最新問題: **17**
監査ログ ファイルの表示を制限する必要がありますか?
A. 記録されたアクティビティを実行した個人
B. 読み取り/書き込みアクセス権を持つ個人
C. 管理者権限を持つ個人
D. 仕事に関連したニーズがある個人
Answer: D (メーッセージを残す**)**
説明
要件 4 によると、監査ログ ファイルの閲覧は、職務に関連する必要がある個人に限定される必要があります。つまり、監査ログ ファイルには、職務に関連する正当な目的でのみアクセスする必要があります。
これは、監査ログ ファイルが無許可の担当者または不要な担当者によってアクセスされないようにするための要件の 1 つです。

最新問題: **18**
訪問者を管理するための組織の手順に含める必要があるもの9
A. 訪問者ログには、訪問者の名前、住所、連絡先電話番号が含まれます
B. 訪問者バッジは、オンサイト担当者が使用するバッジと同じです。
C. 訪問者は、カード所有者のデータが処理または維持されるエリア内に常に付き添われます。
D. 訪問者は訪問完了後 30 日間、身分証明書 (訪問者バッジなど) を保持します。
Answer: (解答を表示する**)**
説明
PCI DSS v3.2.1 クイック リファレンス ガイド 1 によると、訪問者はカード所有者データが処理または維持されるエリア内では常に付き添われ、訪問者バッジはオンサイト担当者が使用するバッジと同一であり、訪問者ログには訪問者の名前、住所、連絡先電話番号が含まれます。に基づき、訪問者は訪問終了後 30 日間、身分証明書 (訪問者バッジなど) を保持

します。これらは、カード所有者データが処理または維持される範囲内のシステムにアクセスする訪問者を管理する組織の手順に含める必要がある手順の例です。

最新問題: **19**
PCI DSS コンプライアンス レポート (ROC) に関して正しいのはどれですか?
A. PCI SSC によって提供される ROC レポート テンプレートと手順は、すべての ROC に使用する必要があります。
B. 評価者は独自のテンプレートまたは PCI SSC が提供する ROC レポート テンプレートのいずれかを使用できます。
C. 評価者は評価レポートごとに独自の ROC テンプレートを作成する必要があります
D. PCI SSC によって提供される ROC レポート テンプレートは、サービス プロバイダーの評価にのみ必要です
Answer: A (メーッセージを残す**)**
説明
PCI DSS v3.2.1 クイック リファレンス ガイド1 によると、評価者は独自のテンプレートまたは PCI SSC が提供する ROC レポート テンプレートのいずれかを使用できます。これは、ROC の一貫性と正確性を確保するための要件の 1 つです。

最新問題: **20**
環境内に同じ PAN のハッシュされたバージョンと切り捨てられたバージョンの両方が存在することに関して正しいのはどれですか?
A. ハッシュ化および切り詰められたバージョンによって元の PAN が公開されるのを防ぐための制御が必要です
B. PAN のハッシュ バージョンも、強力な暗号化のための PCI OSS 要件に従って切り詰める必要があります。
C. ソース PAN を識別できるように、ハッシュされたバージョンと切り捨てられたバージョンを相関させる必要があります。
D. PAN のハッシュされたバージョンと切り捨てられたバージョンは同じ環境に存在してはなりません
Answer: A (メーッセージを残す**)**
説明
ハッシュは、ハッシュ値から元のデータ要素を取得する方法を使用せずに、データ要素を一意の固定サイズのデータ要素 (ハッシュ値) に変換する一方向暗号化の形式です1。トランケーションは、PAN データのセグメントを永久に削除することで、PAN 全体を読み取り不能にする方法です2。PCI DSS 要件 3.4 では、エンティティは、強力な暗号化、切り捨て、インデックス トークンとパッドに基づく一方向ハッシュ、関連するキー管理プロセスを使用した強力な暗号化、および手順３.ただし、PCI DSS 要件 3.4e では、同じ PAN のハッシュされたバージョンと切り捨てられたバージョンが環境内に存在する場合、元の PAN3 を再構築するためにハッシュされたバージョンと切り捨てられたバージョンが相関できないことを保証するための追加の制御を導入する必要があるとも述べています。これは、攻

撃者が同じ PAN のハッシュされたバージョンと切り捨てられたバージョンの両方を取得した場合、ブルート フォース攻撃または辞書攻撃を使用して、一致する 4 が見つかるまで異なる PAN 値をハッシュおよび切り詰めることにより、元の PAN を推測できる可能性があるためです。したがって、正解は選択肢Aです。
他のオプションは、環境内に同じ PAN のハッシュされたバージョンと切り捨てられたバージョンの両方が存在する場合には当てはまりません。オプション B は当てはまりません。PCI DSS では PAN のハッシュ バージョンも切り詰める必要がありませんが、元の PAN5 が公開されるリスクをさらに減らすために推奨されるベスト プラクティスです。オプション C は当てはまりません。PCI DSS では、ハッシュ化されたバージョンと切り捨てられたバージョンを相関付ける必要がありません。これにより、PAN を読み取り不能にするという目的が無効になり、元の PAN が公開されるリスクが高まるからです。オプション D は当てはまりません。元の PAN の再構築を防ぐための追加の制御が行われている限り、PCI DSS は同じ環境内に同じ PAN のハッシュされたバージョンと切り捨てられたバージョンの両方が存在することを禁止していないからです。参考文献:
PCI DSS 3.4 に従ってハッシュ化されたカード所有者データを保護 - Advantio
PCI DSS 切り捨てルールとガイドライン - Truvantis
PCI DSS v3.2.1
ハッシュ化および切り詰められたバージョンの PAN を使用したカード番号の保存
pci dss - クレジットカードデータのセキュリティ - ハッシュ、切り捨て、暗号化 - スタック オーバーフロー

最新問題**: 21**
PCI DSS では、POS でカード読み取りデバイスを保護するためにどのようなプロセスが必要ですか?
A. デバイスは定期的に検査され、不正なカードのスタマーが検出されます。
B. 各デバイスのシリアル番号は、デバイスの製造元によって定期的に確認されます。
C. デバイス識別子とセキュリティラベルは定期的に置き換えられます
D. 侵害の疑いがある場合、デバイスは物理的に破壊されます
Answer: A (メーッセージを残す**)**
説明
PCI DSS v3.2.1 クイック リファレンス ガイド 1 によると、物理的な検査や、ソフトウェアベースのツールやネットワーク ベースのツール (ファイアウォールなど) などのその他の方法を使用して、デバイスが定期的に検査され、不正なカードのスタマーが検出されます。これは、カード所有者のデータを侵害する可能性のあるカード スキミング攻撃を防ぐための要件の 1 つです。

最新問題**: 22**
組織は、システムに変更検出メカニズムを実装しました。重要なファイルの比較はどのくらいの頻度で実行する必要がありますか?
A. 少なくとも毎週

B. エンティティの定義に従って定期的に
C. 有効な変更がインストールされた後のみ
D. 少なくとも毎月
Answer: A (メーッセージを残す**)**
説明
PCI DSS 要件 11.5 では、重要なシステム ファイル、構成ファイル、またはコンテンツ ファイルの不正な変更を担当者に警告するために、企業は変更検出メカニズム (ファイル整合性監視ツールなど) を導入する必要があると規定しています。重要なファイルの比較を少なくとも毎週実行するようにソフトウェアを設定します1。これは、ファイルに対する不正または悪意のある変更が検出され、適時に報告され、ファイルの整合性とセキュリティが維持されるようにするためです。重要なファイルとは、システム ファイル、アプリケーション実行可能ファイル、構成ファイル、データベース ファイル、ログ ファイルなど、カード会員データ環境 (CDE) のセキュリティに影響を与えるファイルです2。したがって、正解は選択肢Aです。
他のオプションは、変更検出メカニズムの重要なファイル比較の頻度に関しては当てはまりません。PCI DSS では少なくとも毎週 1 という最小頻度が指定されているため、PCI DSS ではファイル比較の周期を定義することが許可されていないため、選択肢 B は当てはまりません。オプション C は当てはまりません。PCI DSS では、変更ステータスに関係なく、少なくとも毎週ファイル比較を実行する必要があるため、ファイル比較を有効な変更がインストールされた後のみに制限していません1。オプション D は当てはまりません。PCI DSS では、少なくとも毎週 1 という高い頻度でファイル比較を実行する必要があるため、ファイル比較を少なくとも毎月実行することが許可されていません。参考文献:
PCI DSS v3.2.1
PCI DSS 用のファイル整合性監視ツール

最新問題**: 23**
重要なシステムが正確で一貫した時刻を取得するための PCI DSS 要件を満たすシナリオはどれですか?
A. 各内部システムは、独自のタイム サーバーとして構成されます。
B. 時間構成設定へのアクセスは、システムのすべてのユーザーが利用できます。
C. 中央タイムサーバーは特定の承認された外部ソースから時刻信号を受信します。
D. 各内部システムはディレクトリを外部ソースとピアリングして、時刻更新の精度を確保します。
Answer: C (メーッセージを残す**)**
説明
重要なシステムは正確で一貫した時刻を持っている必要があります。つまり、信頼できるタイム ソースを使用し、クロックを他のシステムと同期する必要があります。これは、重要なシステムが正確な時刻を取得できるようにするための要件の 1 つです。

最新問題**: 24**

AES 128 ビット データ暗号化キー (DEK) を保護するために使用されるキー暗号化キー (KEK) の適切な強度はどれくらいですか?
A. DES256
B. RSA512
C. AES 128
D. ROT 13
Answer: A (メーッセージを残す**)**
説明
暗号キーが廃止され、新しいキーに置き換えられる場合、新しいキーはその用途に適した強度を持っている必要があります。つまり、ブルート フォース攻撃に耐えられる十分な長さと複雑さが必要です。これは、暗号キーが安全で効果的であることを保証するための要件の 1 つです。

最新問題**: 25**
AES 128 ビット データ暗号化キー (DEK) を保護するために使用されるキー暗号化キー (KEK) の適切な強度はどれくらいですか?
A. DES256
B. RSA512
C. AES 128
D. ROT 13
Answer: (解答を表示する**)**
説明
キー暗号化キー (KEK) は、データ暗号化キー (DEK) を不正なアクセスや開示から保護するために使用されます。暗号化チェーン内のリンクが弱くなるのを防ぐために、KEK は DEK と同等以上の強度を持つ必要があります。PCI カード製造論理セキュリティ要件のセクション 4.1.1 によると、
「キー暗号化キー (KEK) は、保護するデータ暗号化キー (DEK) と少なくとも同じくらい強力でなければなりません。」さらに、セクション 4.1.2 には、「KEK は、NIST SP 800-90A または同等の要件を満たす安全な乱数生成器 (RNG) を使用して生成する必要がある」と記載されています。AES 128 は、128 ビット キーを使用する対称暗号化アルゴリズムであり、NIST 標準に準拠しています。したがって、これは、AES 128 ビット DEK を保護するために使用される KEK にとって適切な強度となります。他のオプションは、弱い暗号化アルゴリズムまたは非対称暗号化アルゴリズムであり、KEK には適していません。参考資料: PCI カード製造の論理セキュリティ要件、[NIST SP 800-90A]

最新問題**: 26**
エンティティは電子商取引の支払いカード取引を受け入れ、アカウント データをデータベースに保存します。データベース サーバーと Web サーバーはどちらもインターネットからアクセスできます。データベース サーバーと Web サーバーは、別個の物理サーバー上にあります。企業が PCI DSS 要件を満たすために必要なもの7

A. Web サーバーとデータベース サーバーは同じ物理サーバーにインストールする必要があります
B. データベース サーバーは、信頼できないネットワークからアクセスできないように再配置する必要があります。
C. Web サーバーを内部ネットワークに移動する必要があります
D. より多くの同時接続を可能にするために、データベース サーバーを Web サーバーとは別のセグメントに移動する必要があります。
Answer: B (メーッセージを残す**)**
説明
PCI DSS v3.2.1 クイック リファレンス ガイド1 によると、信頼できないネットワークからアクセスできないようにデータベース サーバーを再配置する必要があります。これは、転送中および保存中のカード会員データを保護するための要件の 1 つです。

最新問題**: 27**
どのシステムにマルウェア対策ソリューションが必要か
A. すべての CDE システム、接続されたシステム。NSC。およびセキュリティ提供システム
B. すべてのポータブル電子ストレージ
C. PAN を保存するすべてのシステム
D. マルウェアの危険にさらされていないと特定されたシステムを除く、対象範囲内のシステム
Answer: (解答を表示する**)**
説明
PCI DSS v3.2.1 クイック リファレンス ガイド 1 によると、マルウェアの危険がないと特定されたシステムを除き、対象となるシステムにはマルウェア対策ソリューションがインストールされ、ベスト プラクティスに従って構成されている必要があります。これは、カード会員データを侵害する可能性のあるマルウェア感染を防ぐための要件の 1 つです。

最新問題**: 28**
カード会員データを含むデータベースへのアクセスを制限するための PCI DSS 要件を満たすシナリオはどれですか?
A. データベースへのユーザー アクセスはプログラムによる方法のみを使用します。
B. データベースへのユーザー アクセスはシステム管理者とネットワーク管理者に制限されています
C. データベース アプリケーションのアプリケーション ID はデータベース管理者のみが使用できます
D. データベースへの直接クエリは共有データベース管理者アカウントに制限されます
Answer: C (メーッセージを残す**)**
説明
データベース アプリケーションのアプリケーション ID はデータベース管理者のみが使用できます。つまり、データベース管理者はすべてのデータベース アプリケーションとその

設定にアクセスできる必要があります。これは、データベース管理者がデータベース アプリケーションを完全に制御できるようにするための要件の 1 つです。

最新問題: **29**
組織は、ユーザーの個別のパスワードとデジタル証明書を使用して、リモート アクセス用の多要素認証を実装したいと考えています。次のシナリオのうち、多要素認証の PCI DSS 要件を満たすのはどれですか?
A. 証明書は管理グループにのみ割り当てられ、通常のユーザーには割り当てられません。
B. 個別のユーザー アカウントごとに異なる証明書が割り当てられ、証明書は共有されません。
C. 証明書は記録されるため、従業員が退職するときに取得できます。
D. 証明書が 90 日ごとに変更されるように、変更管理プロセスが導入されています。
Answer: (解答を表示する**)**
説明
PCI DSS v3.2.1 クイック リファレンス ガイド1 によれば、個々のユーザー アカウントには異なる証明書が割り当てられ、証明書は共有されません。これは、デジタル証明書を使用してカード所有者データへの不正アクセスを防止するための要件の 1 つです。