



Payment Card Industry (PCI) データセキュリティ基準

要件とセキュリティ評価手順

バージョン 3.2.1

2018 年 5 月

この文書について

この文書（「公式日本語訳」）は、https://www.pcisecuritystandards.org/document_library , © 2006-2018 PCI Security Standards Council, LLC（「審議会」）で入手可能な PCI DSS と記される文書の公式の日本語訳です。この公式日本語訳は、JCDSC（「団体」）の承認と支援により情報提供のみを目的として、審議会と団体間の契約に基づいて提供されるものです。この翻訳に関して、本文書に記述された仕様を実装する権利は認められません。そのような権利は、https://www.pcisecuritystandards.org/document_library で入手可能な使用許諾契約書の条項に同意することによってのみ確保されます。本文書の英語版は、https://www.pcisecuritystandards.org/document_library で入手できるもので、本文書の完全版であるとみなされます。不明瞭な点および日本語訳と英語版における不一致については英語版が優先され、日本語訳はいかなる目的であっても依拠することはできません。審議会も団体も、本文書に含まれるいかなる誤りや不明瞭さにも責任を負いません。

About this document

This document (the "Official Japanese Translation") is the official Japanese language translation of the document described as PCI DSS, available at https://www.pcisecuritystandards.org/document_library , © 2006-2018 PCI Security Standards Council, LLC (the "Council"). This Official Japanese Translation is provided with the approval and support of JCDSC ("the Company"), as an informational service only, under agreement between the Council and the Company. No rights to implement the specification(s) described in this document are granted in connection with this translation; such rights may only be secured by agreeing to the terms of the license agreement available at https://www.pcisecuritystandards.org/document_library . The English text version of this document is available at https://www.pcisecuritystandards.org/document_library and shall for all purposes be regarded as the definitive version of this document. To the extent of any ambiguities or inconsistencies between this version and such English text version of this document, the English text version shall control, and accordingly, this version shall not be relied upon for any purpose whatsoever. Neither the Council nor the Company assume any responsibility for any errors or ambiguities contained herein.

文書の変更

日付	バージョン	説明	ページ
2008年 10月	1.2	PCI DSS v1.2 を『PCI DSS 要件とセキュリティ評価手順』として紹介するために、ドキュメント間の重複を削除し、『PCI DSS セキュリティ監査手続き v1.1』からの一般的な変更および固有の変更を行った。詳細については、『PCI データセキュリティ基準: PCI DSS バージョン 1.1 から 1.2 への変更点のまとめ』を参照してください。	
2009年 7月	1.2.1	PCI DSS v1.1 と v1.2 で間違って削除された文を追加。	5
		テスト手順 6.3.7.a と 6.3.7.b の「then」を「than」に修正。	32
		テスト手順 6.5.b の「対応」と「未対応」のグレイアウトのマーキングを削除。	33
		「代替コントロールワークシート - 完成例」の、ページの一番上の文を「このワークシートを使用して、代替コントロールにより『対応』と記載された要件について代替コントロールを定義します。」に修正。	64
2010年 10月	2.0	v1.2.1 からの変更点を更新および反映。詳細については、『PCI DSS - PCI DSS バージョン 1.2.1 から 2.0 への変更点のまとめ』を参照してください。	
2013年 11月	3.0	v2.0 から更新。詳細については、『PCI DSS - PCI DSS バージョン 2.0 から 3.0 への変更点のまとめ』を参照してください。	
2015年 4月	3.1	PCI DSS v3.0 から更新。『PCI DSS - PCI DSS バージョン 3.0 から 3.1 への変更点の詳細のまとめ』を参照してください。	
2016年 4月	3.2	PCI DSS v3.1 から更新。『PCI DSS - PCI DSS バージョン 3.1 から 3.2 への変更点の詳細のまとめ』を参照してください。	
2018年 5月	3.2.1	PCI DSS v3.2 から更新。『PCI DSS - PCI DSS バージョン 3.2 から 3.2.1 への変更点の詳細のまとめ』を参照してください。	

目次

文書の変更	2
概論および PCI データセキュリティ基準の概要	5
PCI DSS リソース	6
PCI DSS 適用性情報	7
PCI DSS と PA-DSS との関係	9
PA-DSS アプリケーションに対する PCI DSS 適用性	9
ペイメントアプリケーションベンダに対する PA-DSS 適用性	9
PCI DSS 要件の適用範囲	10
ネットワークセグメンテーション	11
ワイヤレス	12
第三者サービスプロバイダ/アウトソーシングの使用	12
PCI DSS を日常業務のプロセスに導入するベストプラクティス	13
評価機関：ビジネス設備とシステムコンポーネントのサンプリング	15
代替コントロール	16
準拠に関するレポートの指示と内容	17
PCI DSS 評価プロセス	17
PCI DSS バージョン	18
PCI DSS 要件およびセキュリティ評価手順の詳細	19
安全なネットワークとシステムの構築と維持	20
要件 1: カード会員データを保護するために、ファイアウォールをインストールして構成を維持する	20
要件 2: システムパスワードおよび他のセキュリティパラメータにベンダ提供のデフォルト値を使用しない	29
カード会員データの保護	35
要件 3: 保存されるカード会員データを保護する	35
要件 4: オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化する	47

脆弱性管理プログラムの維持	50
要件 5: すべてのシステムをマルウェアから保護し、ウイルス対策ソフトウェアまたはプログラムを定期的に更新する	50
要件 6: 安全性の高いシステムとアプリケーションを開発し、保守する	53
強力なアクセス制御手法の導入.....	67
要件 7: カード会員データへのアクセスを、業務上必要な範囲内に制限する	67
要件 8: システムコンポーネントへのアクセスを識別・認証する.....	70
要件 9: カード会員データへの物理アクセスを制限する	81
ネットワークの定期的な監視およびテスト	90
要件 10: ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する.....	90
要件 11: セキュリティシステムおよびプロセスを定期的にテストする。	99
情報セキュリティポリシーの維持	109
要件 12: すべての担当者の情報セキュリティに対応するポリシーを維持する。	109
付録 A: 追加の PCI DSS 要件	119
付録 A1: 共有ホスティングプロバイダ向けの PCI DSS 追加要件.....	120
付録 A2: カード提示 POS POI 端末接続用に SSL / 初期の TLS を使用する事業体向けの PCI DSS 追加要件.....	122
付録 A3: PCI DSS 指定事業体向けの追加検証.....	125
付録 B: 代替コントロール	140
付録 C: 代替コントロールワークシート	141
付録 D: ビジネス設備とシステムコンポーネントのセグメンテーションとサンプリング	143

概論および PCI データセキュリティ基準の概要

Payment Card Industry データセキュリティ基準 (PCI DSS) は、カード会員データのセキュリティを強化し、均一なデータセキュリティ評価基準の採用をグローバルに推進するために策定されました。PCI DSS はアカウントデータを保護するために規定された技術面および運用面の要件のベースラインとして利用できます。PCI DSS は加盟店、プロセサー、アクワイアラー、イシュア、サービスプロバイダに適用されます。また PCI DSS は、カード会員データ (CHD) や機密認証データ (SAD) を保存、処理、または送信するすべての事業体に適用されます。以下に、12 の PCI DSS 要件を概説します。

PCI データセキュリティ基準 - 概要

安全なネットワークとシステムの構築と維持	1. カード会員データを保護するために、ファイアウォールをインストールして構成を維持する 2. システムパスワードおよびその他のセキュリティパラメータにベンダー提供のデフォルト値を使用しない
カード会員データの保護	3. 保存されるカード会員データを保護する 4. オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化する
脆弱性管理プログラムの維持	5. すべてのシステムをマルウェアから保護し、ウイルス対策ソフトウェアまたはプログラムを定期的に更新する 6. 安全性の高いシステムとアプリケーションを開発し、保守する
強力なアクセス制御手法の導入	7. カード会員データへのアクセスを、業務上必要な範囲内に制限する 8. システムコンポーネントへのアクセスを識別・認証する 9. カード会員データへの物理アクセスを制限する
ネットワークの定期的な監視およびテスト	10. ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する 11. セキュリティシステムおよびプロセスを定期的にテストする
情報セキュリティポリシーの維持	12. すべての担当者の情報セキュリティに対応するポリシーを維持する

この文書『PCI データセキュリティ基準要件とセキュリティ評価手順』では、12 項目の PCI DSS 要件と、これらの要件に該当するテスト手順をセキュリティ評価ツールに統合しました。この文書は、事業体の検証プロセスの一部としての PCI DSS 準拠の評価作業において使用するために作成されています。以下のセクションには、PCI DSS 評価の準備作業、実施、結果のレポート作成を行う事業体をサポートするための詳細なガイドラインとベストプラクティスが記載されています。PCI DSS 要件とテスト手順については、19 ページで説明します。

PCI DSS はアカウントデータを保護するための必要最小限の要件で構成され、リスクを軽減する追加の規制や慣行、さらには地元、地域、セクターの法規制によって強化される場合があります。さらに、法律または規制上の要件により、個人情報またはその他のデータ要素（カード会員名など）の特定の保護が必要になる場合があります。PCI DSS は地元や地域の法律、政府規制などの法的要件に取って代わるものではありません。

PCI DSS リソース

PCI Security Standards Council (PCI SSC) の Web サイト (www.pcisecuritystandards.org) には、組織が自社の PCI DSS の評価と検証を行うために利用できる、以下を含むその他のリソースが掲載されています。

- 以下を含む文書ライブラリ：
 - [PCI DSS - PCI DSS バージョン 3.1 から 3.2 への変更点のまとめ](#)
 - [PCI DSS クイックリファレンスガイド](#)
 - PCI DSS と PA-DSS の用語集（用語、略語、および頭字語）
 - [補足情報とガイドライン](#)
 - [PCI DSS の優先的なアプローチ](#)
 - [準拠に関するレポート \(ROC\) レポートテンプレートおよびレポートの手引き](#)
 - [自己問診 \(SAQ\) と SAQ の手引きとガイドライン](#)
 - [準拠証明書 \(AOC\)](#)
- よくある質問 (FAQ)
- 小規模加盟店の Web サイト
- PCI トレーニングコースと情報ウェビナー
- 認定セキュリティ評価機関 (QSA) と認定スキヤニングベンダ (ASV) のリスト。
- PTS 認定デバイスと PA-DSS 検証済みペイメントアプリケーションのリスト

注: 「補足情報」は PCI DSS を補足し、PCI DSS 要件を満たすための追加の考慮事項と推奨事項を指定します。PCI DSS またはその要件に優先したり、取って代わったり、拡張したりするものではありません。

これらおよびその他のリソースの詳細については、www.pcisecuritystandards.org を参照してください。

PCI DSS 適用性情報

PCI DSS はペイメントカードの処理を行うすべての事業体に適用されます—これには加盟店、プロセサー、アクワイアラー、イシュア、サービスプロバイダが含まれます。また PCI DSS は、カード会員データや機密認証データを保存、処理、または送信するその他のすべての事業体に適用されます。

カード会員データと機密認証データの定義は次のとおりです。

アカウントデータ	
カード会員データには、以下の情報が含まれます。	機密認証データには、以下の情報が含まれます。
<ul style="list-style-type: none">■ プライマリーアカウント番号 (PAN)■ カード会員名■ 有効期限■ サービスコード	<ul style="list-style-type: none">■ フルトラックデータ (磁気ストライプデータまたはチップ上の同等データ)■ CAV2/CVC2/CVV2/CID■ PIN または PIN ブロック

プライマリーアカウント番号はカード会員データを定義する要素です。カード会員名、サービスコード、および有効期限が PANとともに保存、処理、または送信される場合、またはカード会員データ環境 (CDE) に存在する場合、それらは適用される PCI DSS 要件に従って保護される必要があります。

PCI DSS 要件はアカウントデータ（カード会員データや機密認証データ）が保存、処理、または送信される組織に適用されます。一部の PCI DSS 要件は支払業務や CDE 管理をアウトソースしている組織にも適用されます¹。CDE や支払業務を第三者にアウトソースする組織はまた、アカウントデータが第三者により PCI DSS 要件に従って保護されていることを確認する責任があります。

次のページの表は、カード会員データと機密認証データの一般的な構成要素、各データ要素の保存が許可されるか禁止されるか、各データ要素を保護する必要があるかどうかを示したものです。この表は完全なものではありませんが、各データ要素に適用されるさまざまな種類の要件を示しています。

¹ペイメントブランド準拠プログラムに従う

		データ要素	保存の許可	要件 3.4 に従って、保存されたデータを読み取り不能にする
アカウントデータ	カード会員データ	プライマリアカウント番号 (PAN)	はい	はい
		カード会員名	はい	いいえ
		サービスコード	はい	いいえ
		有効期限	はい	いいえ
機密認証データ ²	機密認証データ ²	フルトラックデータ ³	いいえ	要件 3.2 に従って保存できない
		CAV2/CVC2/CVV2/CID ⁴	いいえ	要件 3.2 に従って保存できない
		PIN/PIN ブロック ⁵	いいえ	要件 3.2 に従って保存できない

PCI DSS 要件 3.3 と 3.4 は PAN にのみ適用されます。PAN がカード会員データの他の要素とともに保存された場合、PCI DSS 要件 3.4 に従って PAN のみを読み取り不能にする必要があります。

機密認証データは承認後、たとえ暗号化していても保存してはなりません。これは環境内に PAN がない場合にも当てはまります。組織はそのアクワイアラーや個々のペイメントブランドに直接連絡し、承認前に SAD を保存することが許可されているか、どれだけの期間ほど許可されるか、関連した使用・保存要件について確認してください。

² 機密認証データは承認後、(たとえ暗号化していても) 保存してはなりません。

³ 磁気ストライプのフルトラックデータ、チップ上の同等のデータなど

⁴ ペイメントカードの前面または裏面に印字された 3 枠または 4 枠の数字

⁵ 取引中にカード会員によって入力される個人識別番号、または取引メッセージ内に存在する暗号化された PIN ブロック、あるいはその両方

PCI DSS と PA-DSS との関係

PA-DSS アプリケーションに対する PCI DSS 適用性

ペイメントアプリケーションデータセキュリティ基準 (PA-DSS) 準拠アプリケーションを単独で使用しても、事業体の PCI DSS 準拠は確立されません。これは、そのアプリケーションが PCI DSS 準拠環境に導入され、ペイメントアプリケーションベンダが提供する『PA-DSS 実装ガイド』に従っている必要があるためです。

カード会員データを保存、処理、または送信するすべてのアプリケーションは、PA-DSS に対して検証されたアプリケーションも含めてを含み、事業体の PCI DSS 評価の範囲に入ります。PCI DSS 評価では、PA-DSS 検証済みのペイメントアプリケーションが PCI DSS 要件に従って正しく設定されており、セキュアに実装されていることを確認する必要があります。ペイメントアプリケーションのカスタマイズが行われている場合には、そのアプリケーションは PA-DSS で検証済みのバージョンとは異なっている可能性があるため、PCI DSS 評価中により詳細なレビューが必要になります。

PA-DSS の要件は、『PCI DSS 要件とセキュリティ評価手順』（この文書で定義）から派生したものです。PA-DSS には、顧客の PCI DSS 準拠を容易にするためにペイメントアプリケーションが満たす必要のある要件が詳しく記述されています。セキュリティ脅威は常に進化を続けるので、もはやベンダによってサポートされない（例. ベンダによって「サポート期限切れ」と識別された）アプリケーションは、サポートバージョンのものと同じセキュリティレベルが提供されないかもしれません。

安全なペイメントアプリケーションは、PCI DSS 準拠の環境にインストールされることで、PAN、フルトラックデータ、カード検証コードと値 (CAV2、CID、CVC2、CVV2) 、PIN と PIN ブロックの侵害につながるセキュリティ侵害、およびこれらの侵害から生じる有害な不正行為の可能性を最小限に抑えます。

特定のペイメントアプリケーションに PA-DSS が適用されるかどうかについては、www.pcisecuritystandards.org にある『PA-DSS プログラムガイド』を参照してください。

ペイメントアプリケーションベンダに対する PA-DSS 適用性

ペイメントアプリケーションベンダが顧客のカード会員データを保存、処理、または送信する場合（サービスプロバイダなど）、PCI DSS を適用することができます。

PCI DSS 要件の適用範囲

PCI DSS のセキュリティ要件は、カード会員データ環境に含まれる、または接続されるすべてのシステムコンポーネントに適用されます。カード会員データ環境（CDE）は、カード会員データまたは機密認証データを保存、処理、または送信する人、処理、およびテクノロジで構成されます。「システムコンポーネント」には、ネットワークデバイス、サーバ、コンピュータ、アプリケーションが含まれます。システムコンポーネントの例には、次のものが含まれますが、これらに限定されるわけではありません。

- セキュリティサービス（認証サーバなど）を提供する、セグメンテーションを促進する（内部ファイアウォールなど）、または CDE のセキュリティに影響を及ぼす（名前解決や Web リダイレクションなど）システム。
- 仮想マシン、仮想スイッチ/ルーター、仮想機器、仮想アプリケーション/デスクトップ、ハイパーテザなどの仮想化コンポーネント。
- ファイアウォール、スイッチ、ルーター、ワイヤレスアクセスポイント、ネットワーク機器、その他のセキュリティ機器を含むが、これらに限定されないネットワークコンポーネント。
- Web、アプリケーション、データベース、認証、メール、プロキシ、ネットワークタイムプロトコル（NTP）、ドメインネームシステム（DNS）などを含むが、これらに限定されないサーバタイプ。
- 内部および外部（インターネットなど）アプリケーションを含む、すべての市販およびカスタムアプリケーション。
- CDE 内にあるか CDE に接続されている他のコンポーネントまたはデバイス

PCI DSS 評価の最初の手順は、レビューの範囲を正確に決定することです。少なくとも年に一度、毎年の評価前に、評価対象の事業体はカード会員データの場所とフローをすべて特定し、さらにすべての接続されている、または CDE に影響を与える可能性のある（例えば、認証サーバ）安全でないシステムを識別し、それらが PCI DSS の範囲に含まれていることを確認することによって、PCI DSS の範囲の正確性を確認する必要があります。対象範囲定義プロセスの一環として、バックアップ/リカバリサイトやフェイルオーバーシステムを含むすべてのシステムおよび拠点の種類を考慮すべきです。CDE の定義の正確性と適用性を確認するには、以下を実行します。

- 評価対象の事業体は環境内に存在するすべてのカード会員データを識別および文書化して、現在定義されている CDE の外部にカード会員データが存在していないことを確認します。
- カード会員データのすべての場所を識別および文書化したら、事業体はその結果を使用して PCI DSS の範囲が適切であることを確認します（例えば、結果はカード会員データの場所を表す図やインベントリである場合があります）。
- 事業体は、見つかったすべてのカード会員データを PCI DSS 評価範囲内にあり、CDE の一部であるものと見なします。事業体が現在 CDE に含まれていないデータを見つけた場合、そのようなデータは完全に削除するか、現在定義されている CDE に移行するか、このデータを含むように CDE を再定義する必要があります。

事業体は PCI DSS の範囲がどのように決められたかを示す文書を保持します。この文書は、評価担当者のレビューのためか、翌年の PCI DSS の範囲確認作業で参照するために保持されます。

それぞれの PCI DSS 評価で、評価者は、評価が正確に定義されていて、文書化されていることを検証する必要があります。

ネットワークセグメンテーション

カード会員データ環境のネットワークセグメンテーション、またはカード会員データ環境の残りの事業体ネットワークからの隔離（セグメント化）は、PCI DSS 要件ではありません。ただし、ネットワークセグメンテーションは以下を引き下げる方法として強く推奨されます。

- PCI DSS 評価の対象範囲
- PCI DSS 評価のコスト
- PCI DSS コントロールの実施と維持に関するコストおよび難易度
- 組織のリスク（カード会員データをコントロールが強化された少数の場所に統合することで、低減します）

ネットワークセグメンテーションが適切に設定されていない場合（「フラットネットワーク」とも呼ばれます）、ネットワーク全体が PCI DSS 評価の対象範囲になります。ネットワークセグメンテーションは、適切に構成された内部ネットワークファイアウォール、ネットワークの特定セグメントへのアクセスを制限する強力なアクセス制御リストまたは他のテクノロジをもつルーターなどのいくつかの物理的または論理的な手段を通じて実現できます。PCI DSS の範囲外と見なされるシステムコンポーネントは、範囲外のシステムコンポーネントが侵害された場合にも CDE のセキュリティに影響しないように CDE から適切に分離（セグメンテーション）する必要があります。

カード会員データ環境の範囲を狭めるための重要な前提条件は、カード会員データの保存、処理または伝送に関するビジネスニーズおよびプロセスを明確にすることです。不必要的データの削除および必要なデータの統合により、カード会員データをできるだけ少ない場所に制限するには、長期にわたるビジネスプラクティスのリエンジニアリングが必要になる可能性があります。

データフロー図を使用してカード会員データフローを文書化することによって、すべてのカード会員データフローを把握し、すべてのネットワークセグメンテーションがカード会員データ環境を効果的に隔離していることを確認できます。

ネットワークセグメンテーションが設定されていて、PCI DSS 評価範囲の縮小に使用されている場合、評価担当者はネットワークセグメンテーションが評価範囲の縮小に適していることを確認する必要があります。ネットワークを適切にセグメント化することによって、カード会員データを保存、処理、伝送するシステムはそれ以外のシステムから高いレベルで隔離されます。ただし、ネットワークセグメンテーションの特定の実装が適切であるかどうかは、特定ネットワークの構成、導入されているテクノロジ、および実装されている他のコントロールなどのいくつかの要因によって大きく左右されます。

「付録 D: ビジネス設備とシステムコンポーネントのセグメンテーションとサンプリング」には、ネットワークセグメンテーションの有効性と PCI DSS 評価範囲のサンプリングに関するより多くの情報が記載されています。

ワイヤレス

ワイヤレステクノロジを使用してカード会員データを保存、処理、送信する場合（POS トランザクション、ラインバスティング「line-busting」など）、またはワイヤレスローカルエリアネットワーク（WLAN）がカード会員データ環境に接続されている場合またはその一部となっている場合、ワイヤレス環境に関する PCI DSS 要件とテスト手順も適用され、これらを実行する必要があります（要件 1.2.3、2.1.1、4.1.1 など）。ワイヤレステクノロジを導入する前に、事業体はテクノロジの必要性をリスクと照らし合わせて注意深く評価する必要があります。ワイヤレステクノロジは機密でないデータを伝送するためだけに導入することも検討してください。

第三者サービスプロバイダ/アウトソーシングの使用

サービスプロバイダまたは加盟店は第三者サービスプロバイダを使用して、カード会員データを保存、処理、伝送したり、ルーター、ファイアウォール、データベース、物理セキュリティ、サーバなどのコンポーネントを管理できます。この場合、カード会員データ環境のセキュリティに影響する可能性があります。

関係者は、サービスプロバイダの PCI DSS 評価範囲、サービスプロバイダが受け持つ特定の PCI DSS 要件、およびサービスプロバイダの顧客が自社の PCI DSS レビューに含める責任を担う要件など、サービスとシステムコンポーネントを明確に指定する必要があります。例えば、管理下のホスティングプロバイダは、どの IP アドレスを四半期ごとの脆弱性スキャンの一部としてスキャンするか、どの IP アドレスをその顧客自身による四半期スキャンに含めるかを明確に記述する必要があります。

サービスプロバイダは、PCI DSS に準拠していることを示す責任があり、ペイメントブランドからそうすることを要求される可能性があります。サービスプロバイダはそのアクワイアラーおよび/またはカードブランドに連絡し、適切な準拠確認方法について確認してください。

第三者サービスプロバイダの準拠確認には 2 つのオプションがあります。

- 1) **年次評価:**サービスプロバイダが自ら年次の PCI DSS 評価を行い、その証拠を顧客に提出して準拠していることを示すことができます。または、
- 2) **複数のオンデマンド評価:**自ら年次の PCI DSS 評価を行わない場合は、サービスプロバイダは顧客の要求に応じて評価を受ける、および/または各顧客に提供されるレビューの結果を伴う、顧客ごとの PCI DSS レビューに参加する必要があります。

第三者サービスプロバイダが自らの PCI DSS 評価を行う場合、自社による PCI DSS 評価の範囲がその顧客に該当するサービスを含んでおり、関連する PCI DSS 要件が審査され、満たされていることが確認されたことを十分に実証する証拠を顧客に提供する必要があります。サービスプロバイダが顧客に提供する証拠の種類は、当事者間で締結された契約によって異なります。例えば、AOC やサービスプロバイダの ROC（機密情報を保護するために改訂）の関連セクションは、その情報の一部またはすべてを提供するのに役立ちます。

また、加盟店とサービスプロバイダは、カード会員データへのアクセス権を持つ関連するすべての第三者サービスプロバイダの PCI DSS 準拠を管理および監視する必要があります。詳細については、この文書の要件 12.8 を参照してください。

PCI DSS を日常業務のプロセスに導入するベストプラクティス

セキュリティコントロールが適切に実施されていることを確認するには、PCI DSS を事業体の総合セキュリティ戦略の一環として日常業務（BAU）に組み込む必要があります。これにより、事業体が自社のセキュリティコントロールの有効性を継続的に監視し、PCI DSS 評価間の PCI DSS 準拠環境を維持できます。PCI DSS を BAU 活動に組み込む方法の例には次のようなものがありますが、これらに限定されません。

1. セキュリティコントロールの監視 - ファイアウォール、侵入検知システム/侵入防止システム（IDS/IPS）、ファイル整合性監視（FIM）、アンチウイルス、アクセス制御など - により効果的かつ意図された運用を確実にします。
 2. セキュリティコントロールのすべての障害が、タイムリーに検出され、対処されていることを確認する。セキュリティコントロールの障害に対処するためのプロセスには以下のようないります。
 - セキュリティコントロールの復旧
 - 障害原因の特定
 - セキュリティコントロールの障害中に発生したセキュリティ問題を特定し、対処する
 - 低減策の実施（プロセスやテクニカルコントロールなど）により、障害原因の再発を防止する
 - 一定期間監視を強化してセキュリティコントロールの監視を再開し、コントロールが効果的に行われていることを確認する
 3. 変更（新しいシステムの追加、システムまたはネットワーク設定の変更など）を完了する前に環境への変更を確認し、以下を行う。
 - PCI DSS の範囲に対する潜在的な影響を特定する（例えば、CDE 内のシステムと別のシステム間の接続を許可するという新しいファイアウォールルールにより、追加のシステムまたはネットワークが PCI DSS の範囲内に含まれるようになるなど）
 - 変更の影響を受けるシステムとネットワークに適用される PCI DSS 要件を特定する（例えば、新しいシステムが PCI DSS の範囲内にある場合、それを FIM、アンチウイルス、パッチ、監査ログなどのシステム構成基準に従って設定し、四半期ごとの脆弱性スキャンスケジュールに追加する必要がある）
 - 必要に応じて PCI DSS の範囲を更新し、セキュリティコントロールを導入する
 4. 組織構造への変更（会社の合併や買収など）があった場合は、PCI DSS の範囲と要件への影響の正式なレビューをする必要があります。
 5. 定期的なレビューと連絡により、PCI DSS の要件が引き続き満たされており、担当者がセキュアプロセスに従っていることを確認する必要があります。これらの定期レビューは、小売店、データセンターなどを含むすべての施設や場所を対象とし、システムコンポーネント（またはシステムコンポーネントのサンプル）のレビューにより PCI DSS の要件が引き続き満たされていること、構成基準が適用されていること、パッチやアンチウイルスが最新のものであること、監査ログがレビューされていることなどを確認する必要があります。定期レビューの頻度は、事業体によってその環境のサイズと複雑さに応じて決定されます。
- これらのレビューはまた、事業体による次回の準拠評価の準備において、監査ログ、脆弱性スキャンレポート、ファイアウォールレビューなど、適切な証跡が保持されていることの保証として使用することもできます。

6. ハードウェアとソフトウェアのテクノロジーを少なくとも年に一度レビューして、引き続きベンダによりサポートされており、PCI DSS などの事業体のセキュリティ要件を満たしていることを確認します。テクノロジーがベンダによりサポートされなくなったか、事業体のセキュリティニーズを満たすことができなくなった場合、事業体は必要に応じてテクノロジーの置き換えに至るまでの修正計画を準備する必要があります。

上記の実践に加え、組織は、セキュリティおよび/または監査部門が運用部門から独立するよう、セキュリティ部門の責任分離を実施することを考慮する場合があります。個人が複数の役割を担うような環境では（管理者とセキュリティ運用など）、独立したチェックポイントを利用せずに、個人がエンドツーエンドのプロセスコントロールを持たないよう、責任を割り当てる必要があります。例えば、構成の責任と変更を承認する責任は、別々の個人に割り当てます。

注:いくつかの事業体では、これらのベストプラクティスが既存の PCI DSS 準拠要件となります。例えば、PCI DSS はこれらの原則をいくつかの要件内に含んでおり、指定事業体補足検証 (PCI DSS 付録 A3) で指定された事業体はこれらの原則を検証する必要があります。

すべての組織は、これらのベストプラクティスの検証を求められていない場合でも、環境内に導入されているかを考慮すべきです。

評価機関：ビジネス設備とシステムコンポーネントのサンプリング

サンプリングは、ビジネス設備および/またはシステムコンポーネントの数が多い場合に評価プロセスの実行を容易にするため、評価機関が使用できるオプションのひとつです。

評価機関が事業体の PCI DSS 準拠レビューの一環としてビジネス設備/システムコンポーネントをサンプルすることは問題ありませんが、事業体がその環境（例えば、四半期ごとの脆弱性スキャンの要件がすべてのシステムコンポーネントに適用される）のサンプルのみに PCI DSS 要件を適用することはできません。同様に、評価機関が PCI DSS 要件のサンプルのみの準拠をレビューすることはできません。

評価対象となる環境全体の範囲と複雑さを考慮した後で、評価担当者は PCI DSS 要件に関する事業体の準拠状態を評価するために、ビジネス設備とシステムコンポーネントの代表的なサンプルを個別に選択できます。最初にビジネス設備のサンプルを定義し、次に、選択した各ビジネス設備のシステムコンポーネントを定義する必要があります。ビジネス設備のすべてのタイプと場所、および選択されたビジネス設備内のシステムコンポーネントのすべてのタイプから代表的なものを選択する必要があります。評価担当者が、予定どおりにコントロールが実装されていると確信できるほど十分な量でなければなりません。

ビジネス設備の例として、会社のオフィス、店舗、フランチャイズ場所、処理設備、データセンター、さまざまな場所のビジネス設備などがあげられます。サンプリングには、選択された各ビジネス設備のシステムコンポーネントが含まれている必要があります。例えば、選択された各ビジネス設備について、レビュー対象領域で使用されるさまざまなオペレーティングシステム、機能、アプリケーションを含めます。

例として、評価担当者は各ビジネス設備で、Apache を実行する Sun サーバ、Oracle を実行する Windows サーバ、従来のカード処理アプリケーションを実行するメインフレームシステム、HP-UX を実行するデータ転送サーバ、MySQL を実行する Linux サーバなどを含むサンプルを定義できます。すべてのアプリケーションが単一 OS (Windows 7 や Solaris 10 など) 上で実行されている場合も、サンプルには各種のアプリケーション (データベースサーバ、Web サーバ、データ転送サーバなど) が含まれている必要があります。

ビジネス設備とシステムコンポーネントのサンプルを個別に選択する場合、評価担当者は以下を考慮する必要があります。

- 整合性を確保し、各ビジネス設備/システムコンポーネントが従うべき標準的な一元化された PCI DSS セキュリティおよび運用プロセス/コントロールがある場合、サンプルは標準プロセス/コントロールがない場合に必要とされる量より少なくて済みます。サンプルは、すべてのビジネス設備/システムコンポーネントが標準プロセスに合わせて構成されていると評価担当者が確信できるほど十分な量でなければなりません。評価担当者は、標準化された一元管理が実装されており、効果的に機能していることを確認する必要があります。
- 複数タイプの標準のセキュリティおよび運用プロセスがある場合 (さまざまなタイプのビジネス設備/システムコンポーネントなど) 、サンプルは各プロセスタイプでセキュリティ保護されたビジネス設備/システムコンポーネントを含む十分な量でなければなりません。
- 標準の PCI DSS プロセス/コントロールがなく、各ビジネス設備/システムコンポーネントが標準以外のプロセスによって管理されている場合、サンプルは各ビジネス設備/システムコンポーネントにおいて PCI DSS 要件が適切に実装されていると評価担当者が確信できるほど十分な量でなければなりません。

- システムコンポーネントのサンプリングには、使用中のすべての種類と組み合わせを含む必要があります。例えば、アプリケーションをサンプリングするとき、各種類のアプリケーションのすべてのバージョンとプラットフォームを含める必要があります。

サンプリングを使用する状況ごとに、評価担当者は以下を実行する必要があります。

- サンプリング方法とサンプルサイズの根拠を文書化する。
- サンプルサイズの決定に使用した標準的な PCI DSS プロセスとコントロールを文書化および検証する。
- サンプルが母集団全体を代表する適切なものであることを説明する。

関連項目：付録 D: ビジネス設備とシステムコンポーネントのセグメンテーションとサンプリング

評価担当者はサンプリングの根拠を評価ごとに再検証する必要があります。サンプルを使用する場合は、ビジネス設備/システムコンポーネントのさまざまなサンプルを評価ごとに選択する必要があります。

代替コントロール

年に一度、評価担当者は代替コントロールをすべて文書化、レビュー、検証し、「付録 B: 代替コントロール」および「付録 C: 代替コントロールワークシート」に従って、準拠に関するレポートに含める必要があります。

代替コントロールごとに、代替コントロールワークシート（付録 C）を記入する必要があります。また、代替コントロールの結果を、対応する PCI DSS 要件セクション内の ROC に文書化する必要があります。

代替コントロールの詳細については、上述の付録 B と C を参照してください。

準拠に関するレポートの指示と内容

準拠に関するレポート（ROC）の指示と内容は『*PCI DSS ROC レポートテンプレート*』にて提供されています。

『*PCI DSS ROC レポートテンプレート*』は、準拠に関するレポートを作成するためのテンプレートとして使用する必要があります。評価対象の事業体は、各ペイメントブランドが事業体の準拠状況を認識できるように、ペイメントブランドごとのレポート要件に従う必要があります。レポート要件と作成手順については、各ペイメントブランドまたはアクワイアラーに問い合わせてください。

PCI DSS 評価プロセス

PCI DSS 評価プロセスには以下のステップの完了を含みます。

1. PCI DSS 評価の対象範囲を確認します
2. 各要件のテスト手順に従って環境の PCI DSS 評価を行います
3. すべての代替コントロールの記録を含む、該当するレポート（自己問診「SAQ」または準拠に関するレポート「ROC」）を、該当する PCI ガイダンスと指示書に従って作成します。
4. サービスプロバイダまたは加盟店に対する、準拠証明書を完成させます。準拠証明書は PCI SSC Web サイトから入手可能です。
5. SAQ または ROC、準拠証明書を他の必須文書とともに、アクワイアラー（加盟店の）またはペイメントブランドまたは他の要求者（サービスプロバイダの）に提出します。
6. 必要に応じて、未対応の要件に対する修正を行い、更新されたレポートを提供します。

PCI DSS バージョン

この文書の発行日から、PCI DSS v3.2 は 2018 年 12 月 31 日まで有効であり、以降は無効となります。この日 [訳注：2018 年 12 月 31 日] 以降のすべての PCI DSS 検証は PCI DSS v3.2.1 またはそれ以降で行わなければなりません。

次の表は、PCI DSS バージョンと有効期限のまとめを示したものです。⁶

バージョン	公開日	有効期限
PCI DSS v3.2.1 (この文書)	2018 年 5 月	未定
PCI DSS v3.2	2016 年 4 月	2018 年 12 月 31 日

⁶PCI DSS の新バージョンのリリースに伴い、変更することがあります。

PCI DSS 要件およびセキュリティ評価手順の詳細

以下に、PCI DSS 要件およびセキュリティ評価手順に関する表の列見出しを定義します。

- **PCI DSS 要件** - この列では、データセキュリティ基準要件を定義します。これらの要件に照合して PCI DSS 準拠が検証されます。
- **テスト手順** - この列には、PCI DSS 要件に「対応」していることを検証するために、評価担当者が行うプロセスが表示されています。
- **ガイダンス** - この列には、各 PCI DSS 要件の意図とセキュリティ目標が表示されています。この列には、ガイダンスのみ表示され、各要件の意図を理解しやすくすることを目的としています。この列のガイダンスは、PCI DSS 要件およびテスト手順を置き換えるものではありません。

注: コントロールがまだ導入されていないか、将来の日付に完了する予定の場合には、PCI DSS 要件に未対応と見なされます。事業体が未解決または未対応項目に対処した後、評価担当者は、対策が施され、すべての要件が満たされていることを再評価します。

PCI DSS 評価の文書化については、以下のリソース (PCI SSC Web サイトで入手可) を参照してください。

- 準拠に関するレポート (ROC) の作成手順については、『PCI DSS ROC レポートテンプレート』を参照してください。
- 自己問診 (SAQ) の記入方法については、『PCI DSS SAQ に関する指示およびガイドライン』を参照してください。
- PCI DSS 準拠の検証レポートの提出手順については、『PCI DSS 準拠証明書』を参照してください。

安全なネットワークとシステムの構築と維持

要件 1: カード会員データを保護するために、ファイアウォールをインストールして構成を維持する

ファイアウォールは事業体のネットワーク（社内）と信頼できないネットワーク（外部）とのコンピュータトラフィック、および事業体の信頼できる内部ネットワーク内の機密性の高い領域へのトラフィックを制御するデバイスです。事業体の信頼できるネットワーク内の非常に機密性の高いエリアの例として、カード会員データ環境があげられます。

ファイアウォールはすべてのネットワークトラフィックを調べて、指定されたセキュリティ基準を満たさない伝送をブロックします。

すべてのシステムは、電子商取引、従業員のデスクトップブラウザからのインターネットアクセス、従業員の電子メールによるアクセス、B2B 接続などの専用接続、ワイヤレスネットワーク、その他のソースを介したシステムへのアクセスなど、信頼できないネットワークからの不正なアクセスから保護されなければなりません。しばしば、信頼できないネットワークへの（からの）問題ないように思われるアクセス経路が、重要なシステムへの侵入経路になっていることがあります。ファイアウォールは、すべてのコンピュータネットワークのための、重要な保護メカニズムです。

要件 1 に記載されているファイアウォールの最小要件を他のシステムコンポーネントが満たしている場合は、それらのファイアウォール機能を利用できます。カード会員データ環境内の他のシステムコンポーネントのファイアウォール機能を使用している場合は、要件 1 の評価範囲にそれらのデバイスが含まれている必要があります。

PCI DSS 要件	テスト手順	ガイダンス
1.1 以下を含むファイアウォールとルーターの構成基準を確立し、実施する:	1.1 ファイアウォール/ルーター構成基準および以下で指定されたその他の文書を検査し、標準が完全であり、以下のように実施されていることを確認する：	ファイアウォールとルーターは、ネットワークへの出入りを管理するアーキテクチャの重要なコンポーネントです。これらのデバイスは、不要なアクセスをブロックし、ネットワークに出入りする承認済みアクセスを管理するソフトウェアまたはハードウェアデバイスです。 構成基準と手順は、データを保護するための組織における防御の第一線の強度を維持するのに役立ちます。
1.1.1 すべてのネットワーク接続およびファイアウォール/ルーター構成への変更を承認およびテストする正式なプロセス	1.1.1.a 文書化された手順を調べて、すべてをテストし承認するための正式なプロセスがあることを確認する。 <ul style="list-style-type: none"> • ネットワーク接続および • ファイアウォール/ルーター構成の変更 1.1.1.b ネットワーク接続のサンプルでは、責任者をインタビューし、記録を検査してネットワーク接続が承認されてテストされていることを確認する。	ファイアウォールとルーターへのすべての接続と変更を承認およびテストするために文書化されて実施されているプロセスは、ネットワーク、ルーター、またはファイアウォールの誤った構成により発生するセキュリティ上の問題を防ぐのに役立ちます。

PCI DSS 要件	テスト手順	ガイダンス
1.1.2 ワイヤレスネットワークなど、カード会員データ環境とその他のネットワーク間のすべての接続を示す最新ネットワーク図	<p>1.1.1.c ファイアウォールおよびルーター構成に実際に加えられた変更のサンプルを特定し、変更記録と比較して、責任者をインタビューして変更が承認されテストされたことを確認する。</p> <p>1.1.2.a ネットワーク図を検査してネットワーク構成を観察し、現在のネットワーク図が存在すること、また、その文書がワイヤレスネットワークを含む、カード会員データへの全接続を含んでいることを確認する。</p> <p>1.1.2.b 責任者をインタビューして、図が最新のものであることを確認する。</p>	変更の正式な承認とテストなしでは、変更の記録が更新されず、ネットワーク文書と実際の構成間に不整合が生じる原因となります。
1.1.3 システムとネットワーク内でのカード会員データのフローを示す最新図	<p>1.1.3.a データフロー図を調べ、担当者をインタビューして図を確認する。</p> <ul style="list-style-type: none"> • システムとネットワーク内でのすべてのカード会員データのフローを示す • 最新状態に保たれており、環境に変化があれば必要に応じて更新されている 	<p>カード会員データフロー図は、ネットワーク内で保存、処理、または送信されたすべてのカード会員データの場所を示します。</p> <p>ネットワーク図とカード会員データフロー図は、ネットワーク内および個々のデバイス間のカード会員データのデータフローを示すことで、組織がカード会員データ環境の範囲を理解し、追跡することができるようになります。</p>
1.1.4 各インターネット接続、およびDMZ (demilitarized zone) と内部ネットワークゾーンとの間のファイアウォール要件	<p>1.1.4.a ファイアウォール構成基準を調べて、各インターネット接続、およびDMZと内部ネットワークゾーンとの間のファイアウォール要件が含まれていることを確認する。</p> <p>1.1.4.b 現在のネットワーク図が、ファイアウォール構成基準と一致していることを確認する。</p> <p>1.1.4.c 文書化されている構成基準とネットワーク図に基づき、ネットワーク構成を見て、各インターネット接続、および非武装地帯 (DMZ) と内部ネットワークゾーンとの間にファイアウォールがあることを確認する。</p>	ネットワークへの（およびネットワークからの）すべての接続に対してファイアウォールを使用することで、組織はアクセスを監視および管理し、悪意のある者が内部ネットワークにアクセスする可能性を最小限に抑えることができます。
1.1.5 ネットワークコンポーネントを管理するためのグループ、役割、責任に関する記述	<p>1.1.5.a ファイアウォールおよびルーター構成基準に、ネットワークコンポーネントの管理のためのグループ、役割、責任に関する記述が含まれていることを確認する。</p> <p>1.1.5.b ネットワークコンポーネントの管理責任者をインタビューし、文書通りに役割と責任が割り当てられていることを確認する。</p>	この役割と責任の割り当ての記述により、スタッフがすべてのネットワークコンポーネントについて、各コンポーネントのセキュリティの責任者は誰かを知り、コンポーネントの管理を任せられた責任者が各自の責任を認識できるようになります。役割と責任が正式に割り当てられないと、デバイスは管理されないままになる可能性があります。

PCI DSS 要件	テスト手順	ガイダンス
<p>1.1.6 安全でないと見なされているプロトコルに実装されているセキュリティ機能の文書化などを含む、使用が許可されているすべてのサービス、プロトコル、ポートの使用に対する業務上の正当な理由および承認の文書化</p>	<p>1.1.6.a ファイアウォール/ルーター構成基準に、業務上の正当な理由と承認を含む、すべてのサービス、プロトコル、ポートを文書化したリストが含まれていることを確認する。</p> <p>1.1.6.b 使用が許可されているが安全でないサービス、プロトコル、ポートを特定する。かつ、各サービスについてセキュリティ機能が文書化されていることを検証する。</p> <p>1.1.6.c ファイアウォールとルーターの構成を検査し、文書化されているセキュリティ機能が安全でない各サービス、プロトコル、ポートに実装されていることを確認する。</p>	<p>未使用または安全でないサービスとポートには、多くの既知の脆弱性があるため、多くの場合、侵害はこれらが原因で発生します。多くの組織は、(その脆弱性がいまだに存在するにもかかわらず) 使用しないサービス、プロトコル、ポートのセキュリティ脆弱性のパッチ処理を行いません。各組織は、どのサービス、プロトコル、ポートがビジネスにとって必要かを明確に決定し、文書化することで、その他のサービス、プロトコル、ポートはすべて無効にするか削除する必要があります。</p> <p>承認は、構成を管理する要員とは異なる独立した担当者によって与えられる必要があります。</p> <p>安全でないサービス、プロトコル、またはポートが業務上必要な場合、これらのプロトコルの使用によってもたらされるリスクが組織によって明確に理解および承認され、プロトコルの使用が正当化され、さらにこれらのプロトコルを安全に使用できるようにするセキュリティ機能が文書化されて実装されている必要があります。これらの安全でないサービス、プロトコル、またはポートがビジネスにとって不要な場合は、無効にするか削除する必要があります。</p> <p>安全でないと見なされているサービス、プロトコル、またはポートのガイダンスについては、業界の標準やガイダンス（例、NIST、ENISA、OWASPなど）を参照してください。</p>
<p>1.1.7 ファイアウォールおよびルーターのルールセットは少なくとも 6 カ月ごとにレビューされる必要がある</p>	<p>1.1.7.a ファイアウォール/ルーター構成基準で、ファイアウォールおよびルーターのルールセットを少なくとも 6 カ月ごとにレビューするように要求していることを確認する。</p> <p>1.1.7.b ルールセットのレビューに関連した文書を検査し、担当者をインタビューすることで、ルールセットが少なくとも 6 カ月ごとにレビューされていることを確認する。</p>	<p>このレビューにより、組織は少なくとも 6 カ月ごとに不要、期限切れ、または不正なルールを取り除くことができ、すべてのルールセットで業務上の正当な理由に一致する承認済みのサービスとポートのみが許可されていることを確認できます。</p> <p>ファイアウォールおよびルーターのルールセットへの変更が多い組織は、レビュー頻度を増やしてルールセットが継続的にビジネスニーズを満たすようにすることが推奨されます。</p>

PCI DSS 要件	テスト手順	ガイダンス
<p>1.2 信頼できないネットワークとカード会員データ環境内のすべてのシステムコンポーネントの接続を制限する、ファイアウォール構成を構築する。</p> <p>注: 「信頼できないネットワーク」とは、レビュー対象の事業体に属するネットワーク外のネットワーク、または事業体の制御または管理が及ばないネットワーク（あるいはその両方）のことである。</p>	<p>1.2 ファイアウォール/ルーター構成を調べて、信頼できないネットワークとカード会員データ環境内のシステムコンポーネント間で接続が制限されていることを確認する。</p>	<p>内部の信頼できるネットワークと、外部にある、または事業体の制御または管理が及ばない信頼できないネットワークとの間にネットワーク保護をインストールすることは不可欠です。この手段を正しく実装しないと、事業体は悪意のある者やソフトウェアによる不正アクセスに対して脆弱になります。</p> <p>ファイアウォールの機能が効果的であるためには、事業体のネットワークに出入りするトラフィックを適切に制御または制限する必要があります。</p>
<p>1.2.1 着信および発信トラフィックを、カード会員データ環境に必要なトラフィックにし、それ以外のすべてのトラフィックを特定的に拒否する</p>	<p>1.2.1.a ファイアウォール/ルーター構成基準を調べて、カード会員データ環境に必要な着信および発信トラフィックが特定されていることを確認する。</p> <p>1.2.1.b 着信および発信トラフィックが、カード会員データ環境に必要なトラフィックに制限されていることを確認する。</p> <p>1.2.1.c ファイアウォール/ルーター構成を検査して、例えば明示の「すべてを拒否」、または許可文の後の暗黙の拒否を使用することで、他のすべての着信および発信トラフィックが明確に拒否されていることを確認する。</p>	<p>すべての着信および発信接続を調査することは、発信元および/または宛先アドレスに基づくトラフィックの制限および検査を可能にし、信頼されない環境と、信頼できる環境の間でフィルタリングされていないアクセスを防止します。これは、悪意のある者が不正な IP アドレス経由で事業体のネットワークにアクセスしたり、不正な方法でサービス、プロトコル、またはポートを使用（例えば、組織のネットワーク内から取得したデータを信頼できないサーバに送出する）することを防止します。</p> <p>特に必要でない発信および着信トラフィックをすべて拒否するルールを実装することにより、意図しない、有害の可能性があるトラフィックの着信または発信を可能にするセキュリティホールが不用意に開かれるのを防ぐことができます。</p>
<p>1.2.2 ルーター構成ファイルをセキュリティ保護および同期化する</p>	<p>1.2.2.a ルーター構成ファイルを調べて、不正アクセスからセキュリティ保護されていることを確認する。</p>	<p>実行中（またはアクティブな）ルーター構成ファイルには最新のセキュア設定が入っていますが、</p>

PCI DSS 要件	テスト手順	ガイダンス
	<p>1.2.2.b ルーター構成を調べて、同期化されていることを確認する。例えば、実行（アクティブ）構成ファイルが起動構成（マシンの再起動時に使用）に一致することを確認する。</p>	<p>起動ファイル（ルーターの再起動またはブート時に使用）は同じセキュア設定で更新して、起動時構成が実行されるときにこれらの設定が適用されるようにする必要があります。</p> <p>起動構成ファイルはあまり実行されることがないため、更新を忘れがちになります。ルーターが起動され、実行中の構成ファイルと同じ安全な設定で更新されていない起動構成ファイルを読み込んだ場合、より脆弱なルールが適用され、悪意のある者がネットワークに侵入できる可能性があります。</p>
<p>1.2.3 すべてのワイヤレスネットワークとカード会員データ環境の間に境界ファイアウォールをインストールし、ワイヤレス環境とカード会員データ環境間のトラフィックを業務上必要な場合に拒否または承認されたトラフィックのみを許可するようにファイアウォールを構成する</p>	<p>1.2.3.a ファイアウォール/ルーター構成を調べて、すべてのワイヤレスネットワークとカード会員データ環境間に境界ファイアウォールがインストールされていることを確認する。</p> <p>1.2.3.b ファイアウォールが、ワイヤレス環境とカード会員データ環境間のすべてのトラフィックを拒否または、業務上必要な場合、承認されたトラフィックのみ許可することを確認する。</p>	<p>ネットワーク内のワイヤレステクノロジの既知の（または不明な）実装および利用は、悪意のある者がネットワークとカード会員データにアクセスするための一般的な経路となります。ワイヤレスデバイスまたはネットワークが事業体の知らない間にインストールされた場合、悪意のある者はネットワークに容易に、かつ「認識されずに」侵入できます。ファイアウォールがワイヤレスネットワークから CDE へのアクセスを制限していない場合、ワイヤレスネットワークへの不正アクセスを得た悪意のある者は、容易に CDE に接続し、アカウント情報を侵害することができます。</p> <p>ワイヤレスネットワークが接続されている環境の目的に関係なく、すべてのワイヤレスネットワークと CDE の間にファイアウォールをインストールする必要があります。これには企業ネットワーク、小売店、倉庫などの環境も含まれますがこれらに限定されません。</p>

PCI DSS 要件	テスト手順	ガイダンス
1.3 インターネットとカード会員データ環境内のすべてのシステムコンポーネント間の、直接的なパブリックアクセスを禁止する。	1.3 ファイアウォールおよびルーター構成を以下に説明するとおりに調査し、以下の詳細に従って、インターネットと内部のカード会員ネットワークセグメントのシステムコンポーネント間に直接アクセスがないことを確認する。システムコンポーネントには、インターネットのチョークルーター、 DMZ ルーターおよびファイアウォール、 DMZ カード会員セグメント、境界ルーター、内部のカード会員ネットワークセグメントなどが含まれるが、これらに限定されない。	DMZ 上のシステムに対して信頼できない接続を許可する正当な理由（例、Web サーバへのパブリックアクセスの許可）があったとしても、そのような接続は内部ネットワーク内のシステムに対しては、決して許可すべきではありません。ファイアウォールの目的は、公共システムと内部システム、特にカード会員データを保存、処理、または伝送するシステムとの間のすべての接続を管理および制御することです。公共システムと CDE との間で直接のアクセスが許可されている場合、ファイアウォールが提供する保護が迂回され、カード会員データを保存するシステムコンポーネントが侵害にさらされる可能性があります。
1.3.1 DMZ を実装し、承認された公開サービス、プロトコル、ポートを提供するシステムコンポーネントのみへの着信トラフィックに制限する。 1.3.2 着信インターネットトラフィックを DMZ 内の IP アドレスに制限する。	1.3.1 ファイアウォール/ルーター構成を検査し、 DMZ が実装され、承認された公開サービス、プロトコル、ポートを提供するシステムコンポーネントのみへの着信トラフィックに制限していることを確認する。 1.3.2 ファイアウォール/ルーター構成を検査し、着信インターネットトラフィックが、 DMZ 内の IP アドレスに制限されていることを確認する。	DMZ は、インターネット（またはその他の信頼できないネットワーク）と組織が公開する必要があるサービス（Web サーバなど）との間の接続を管理するネットワークの一部です。 この機能は、悪意のある者がインターネットから組織の内部ネットワークにアクセスしたり、不正な方法でサービス、プロトコル、またはポートを使用したりするのを防止することを目的としています。
1.3.3 アンチスプーフィング対策を実施し、偽の送信元 IP アドレスを検出して、ネットワークに侵入されないようにブロックする。 (例えば、内部送信元アドレスをもつインターネットからのトラフィックをブロックするなど)	1.3.3 ファイアウォールおよびルーター構成を検査し、例えば、内部アドレスがインターネットから DMZ 内へ通過できないなど、スプーフィング対策が実装されていることを確認する。	通常、パケットには、最初にそのパケットを送信したコンピュータの IP アドレスが含まれ、ネットワーク上の他のコンピュータでパケットがどこから来たかがわかるようになっています。悪意を持つユーザは、送信元 IP アドレスをスプーフ（詐称）して、宛先システムにパケットが信頼されている送信元から来たと信じさせようと試みます。ネットワークに入ってくるパケットをフィルタリングすることにより、パケットが内部ネットワークから送信されたものであるかのように「スプーフィング」されていないことを確認できます。

PCI DSS 要件	テスト手順	ガイダンス
1.3.4 カード会員データ環境からインターネットへの未承認の発信トラフィックを禁止する。	1.3.4 ファイアウォール/ルーター構成を検査し、カード会員データ環境からインターネットへの発信トラフィックが明示的に承認されていることを確認する。	カード会員データ環境から発信されるすべてのトラフィックを評価して、発信トラフィックが確立・承認されたルールに確實に従うようにする必要があります。接続を検査して、許可された通信のみにトラフィックを制限する必要があります（送信元/宛先のアドレス/ポートの制限やコンテンツのブロックなど）。
1.3.5 ネットワーク内へ「確立された」接続のみを許可する。	1.3.5 ファイアウォール/ルーター構成を検査し、ファイアウォールが内部ネットワーク内への確立された接続のみ許可し、予め確立されたセッションによらない着信接続は拒否することを確認する。	通過する各接続の「状態」（またはステータス）を維持するファイアウォールは、以前への応答であるように見える接続が実際に有効で承認済みの応答（各接続の状態を保持しているため）か、またはファイアウォールをだまして接続の許可を得ようとしている悪意のあるトラフィックかどうか判断できます。
1.3.6 DMZ やその他の信頼できないネットワークから隔離されている内部ネットワークゾーンで、カード会員データを保存するシステムコンポーネント（データベースなど）を配置する。	1.3.6 ファイアウォール/ルーター構成を検査し、カード会員データを保存するシステムコンポーネントは、DMZ やその他の信頼できないネットワークから隔離されている内部ネットワークゾーンにあることを確認する。	カード会員データが DMZ 内に配置されている場合、侵入する層の数がより少ないため、この情報へのアクセスは外部の攻撃者にとって容易になります。DMZ などの信頼できないネットワークからファイアウォールで分離された内部ネットワークゾーンに、カード会員データを保存する安全なシステムコンポーネントを配置してシステムコンポーネントからの不正ネットワークトラフィックを防止する必要があります。 注: この要件は、揮発性メモリ内におけるカード会員データの一時記憶には適用されません。
1.3.7 プライベート IP アドレスとルーティング情報を許可されていない第三者に開示しない。 注: IP アドレスを開示しない方法には、以下のものが含まれるが、これらに限定されるわけではない：	1.3.7.a ファイアウォール/ルーター構成を検査し、プライベート IP アドレスおよび内部ネットワークからインターネットへのルーティング情報を開示しない方法が導入されていることを確認する。	インターネットまたはプライベート IP アドレスの開示を制限することは、ハッカーに内部ネットワークの IP アドレスを「知られ」て、この情報をネットワークへのアクセスに使用されることを防ぐために不可欠です。

PCI DSS 要件	テスト手順	ガイダンス
<ul style="list-style-type: none"> ■ ネットワークアドレス変換 (NAT) ■ カード会員データを保持するサーバをプロキシサーバ/ファイアウォールの背後に配置する。 ■ 登録されたアドレス指定を使用するプライベートネットワークのルートアドバタイズを削除するか、フィルタリングする。 ■ 登録されたアドレスの代わりに RFC1918 アドレス空間を内部で使用する。 <p>1.4 ネットワークの外側ではインターネットに接続され（従業員が使用するラップトップなど）、また CDE へのアクセスにも使用されるすべてのポータブルコンピューティングデバイス（会社および/または従業員所有を含む）に、パーソナルファイアウォールソフトウェアまたは同等の機能をインストールする。ファイアウォール（または同等の構成）には以下が含まれます。</p> <ul style="list-style-type: none"> • 専用の構成設定が定義されていること • パーソナルファイアウォール（または同等の機能）がアクティブに実行中であること • パーソナルファイアウォール（または同等の機能）がポータブルコンピューティングデバイスのユーザによって変更されていないこと 	<p>1.3.7.b 担当者のインタビューや文書の調査により、どのプライベート IP アドレスおよび外部事業体へのルーティング情報開示にも許可が必要であることを確認する。</p> <p>1.4.a ポリシーと構成基準を調べて以下を確認する：</p> <ul style="list-style-type: none"> • ネットワークの外側ではインターネットに接続され、また CDE へのアクセスにも使用されるすべてのポータブルコンピューティングデバイス（会社および/または従業員所有を含む）にパーソナルファイアウォールソフトウェアまたは同等の機能が要求されている • パーソナルファイアウォール（または同等の機能）専用の構成設定が定義されている • パーソナルファイアウォール（または同等の機能）がアクティブに実行するために構成されている • パーソナルファイアウォール（または同等の機能）の構成がポータブルコンピューティングデバイスのユーザによって変更できないようになっている <p>1.4.b 会社または従業員所有デバイス（またはその両方）を検査して、以下を確認する。</p> <ul style="list-style-type: none"> • パーソナルファイアウォール（または同等の機能）がインストールされており、組織の構成設定に従って設定されている • パーソナルファイアウォール（または同等の機能）がアクティブに実行中である • パーソナルファイアウォール（または同等の機能）がポータブルコンピューティングデバイスのユーザによって変更されていない 	<p>この要件の目的を満たすための手段は、使用しているネットワークテクノロジによって異なる場合があります。例えば、この要件を満たすために使用するコントロールは、IPv4 ネットワークの場合と IPv6 ネットワークの場合とで異なる可能性があります。</p> <p>企業ファイアウォールの外部からインターネットに接続できるポータブルコンピューティングデバイスは、インターネットベースの脅威に対してより脆弱です。ファイアウォール機能（例、パーソナルファイアウォールソフトウェアまたはハードウェア）を使用すると、デバイスがシステムに再接続された時点での組織のシステムとデータにアクセスできる、インターネットベースの攻撃からデバイスを保護するのに役立ちます。</p> <p>特定のファイアウォール構成設定は、組織によって決定されます。</p> <p>注: この要件は、従業員所有および会社所有のポータブルコンピューティングデバイスを適用対象とします。会社のポリシーで管理できないシステムは弱点をもたらし、悪意のある者により攻撃される可能性があります。信頼できないシステムが組織の CDE に接続することを許可すると、攻撃者やその他の悪意のあるユーザにアクセスが付与されることにつながります。</p>

PCI DSS 要件	テスト手順	ガイダンス
1.5 ファイアウォールの管理に関するセキュリティポリシーと操作手順が文書化および使用されており、影響を受ける関係者全員に知らされていることを、確実にする。	<p>1.5 文書を調べ、関係者をインタビューすることで、ファイアウォールの管理に関するセキュリティポリシーと操作手順が以下の要件を満たしていることを確認する。</p> <ul style="list-style-type: none"> • 文書化されている • 使用されている • 影響を受ける関係者全員に知らされている 	ファイアウォールとルーターが継続的に管理されてネットワークへの不正アクセスが確実に防止されるように、関係者はセキュリティポリシーと操作手順を認識・順守する必要があります。

要件2: システムパスワードおよび他のセキュリティパラメータにベンダ提供のデフォルト値を使用しない

(社内外の) 悪意のある者は多くの場合、ベンダのデフォルトパスワードおよびベンダのその他のデフォルト設定を使用して、システムを脅かします。これらのパスワードと設定はハッカーの間でよく知られており、公開情報を通じて容易に特定できます。

PCI DSS 要件	テスト手順	ガイダンス
<p>2.1 システムをネットワークに導入する前に、必ずベンダ提供のデフォルト値を変更し、不要なデフォルトアカウントを無効にする。</p> <p>これは、オペレーティングシステム、セキュリティサービスを提供するソフトウェア、アプリケーション、システムアカウント、ポイントオブセールス(POS)端末、ペイメントアプリケーション、簡易ネットワーク管理プロトコル(SNMP)コミュニティ文字列で使用されるものを含むがこれらに限定されない、すべてのデフォルトパスワードに適用されます。</p>	<p>2.1.a システムコンポーネントのサンプルを選択し、ベンダ提供のデフォルトのアカウントとパスワードを使用してデバイスへのログオンを試み（システム管理者の協力を得て）、すべてのデフォルトパスワード（オペレーティングシステム、セキュリティサービスを提供するソフトウェア、アプリケーション、システムアカウント、POS端末、簡易ネットワーク管理プロトコル(SNMP)コミュニティ文字列で使用されるものを含む）が変更されていることを確認する。（ベンダのマニュアルおよびインターネット上のソースを使用して、ベンダ提供のアカウント/パスワードを探す。）</p> <p>2.1.b システムコンポーネントのサンプルで、すべての不要なデフォルトアカウント（オペレーティングシステム、セキュリティソフトウェア、アプリケーション、システム、POS端末、SNMPなどで使用されているアカウントを含む）が削除または無効化されていることを確認する。</p> <p>2.1.c 担当者をインタビューし、関係文書を調べて、以下を確認する。</p> <ul style="list-style-type: none"> • システムをネットワークにインストールする前にすべてのベンダデフォルト（オペレーティングシステム、セキュリティサービスを提供するソフトウェア、アプリケーション、システムアカウント、POS端末、簡易ネットワーク管理プロトコル(SNMP)コミュニティ文字列のデフォルトパスワード）が変更されている • システムがネットワークにインストールされる前にすべての不要なデフォルトアカウント（オペレーティングシステム、セキュリティソフトウェア、アプリケーション、システム、POS端末、SNMPなどで使用されているアカウントを含む）が削除または無効化されている 	<p>悪意のある者（組織の内外にかかわらず）は多くの場合、ベンダのデフォルト設定、アカウント名、およびパスワードを使用して、それがインストールされているオペレーティングシステムソフトウェア、アプリケーション、システムを侵害します。これらのデフォルト設定は公開されることが多く、ハッカーの間でよく知られていますが、設定を変更することで攻撃に対するシステムの脆弱性を軽減することができます。</p> <p>デフォルトアカウントを使う予定がない場合にも、デフォルトパスワードを強力で一意なパスワードに変更してからそのアカウントを無効にすることで、悪意のある者がそのアカウントを再び有効にしてデフォルトパスワードを使ってアクセスすることを防止できます。</p>

PCI DSS 要件	テスト手順	ガイダンス
2.1.1 カード会員データ環境に接続されている、またはカード会員データを伝送するワイヤレス環境の場合、インストール時にすべてのワイヤレスベンダのデフォルト値を変更する。これには、デフォルトのワイヤレス暗号化鍵、パスワード、SNMP コミュニティ文字列が含まれるが、これらに限定されない。	<p>2.1.1.a 担当者をインタビューし、関係文書を調べて、以下を確認する。</p> <ul style="list-style-type: none"> 暗号化キーがインストール時のデフォルトから変更されていること。 暗号化キーの知識を持つ人物が退社または異動するたびに、そのキーが変更されていること。 <p>2.1.1.b 担当者をインタビューし、ポリシーと手順を調べることで、以下を確認する。</p> <ul style="list-style-type: none"> デフォルトの SNMP コミュニティ文字列をインストール後に変更する必要があること。 アクセスポイントのデフォルトのパスワード/パスフレーズをインストールごとに変更する必要があること。 <p>2.1.1.c システム管理者の協力を得て、ベンダ文書を調べ、ワイヤレスデバイスにログインして、以下を確認する。</p> <ul style="list-style-type: none"> ワイヤレスデバイスのデフォルトの SNMP コミュニティ文字列が使われていないこと。 アクセスポイントのデフォルトのパスワード/パスフレーズが使用されていないこと。 <p>2.1.1.d ベンダ文書を調べ、ワイヤレス構成設定を観察して、ワイヤレスデバイスのファームウェアが、以下の強力な暗号化をサポートするために更新されていることを確認する。</p> <ul style="list-style-type: none"> ワイヤレスネットワーク経由での認証 ワイヤレスネットワーク経由での送信 <p>2.1.1.e ベンダ文書を調べ、ワイヤレス構成設定を観察することで、必要に応じて、他のセキュリティに関するワイヤレスベンダのデフォルトが変更されたことを確認する。</p>	ワイヤレスネットワークが十分なセキュリティ構成（デフォルト設定の変更を含む）で実装されていない場合、盗聴者はワイヤレストラフィックを傍受し、データとパスワードを容易にキャプチャしてネットワークに容易に侵入して攻撃することができます。 さらに、古いバージョンの 802.11x 暗号化（Wired Equivalent Privacy 「WEP」）用の鍵交換プロトコルは破られており、暗号化が役に立たなくなっている可能性があります。デバイスのファームウェアが安全性の高いプロトコルをサポートするように更新されていることを確認します。
2.2 すべてのシステムコンポーネントについて、構成基準を作成する。この基準は、すべての既知のセキュリティ脆弱性をカバーし、また業界で認知されたシステム強化基準と一致している必要がある。	<p>2.2.a すべてのタイプのシステムコンポーネントについて企業のシステム構成基準を調べ、システム構成基準が、業界で認知されたシステム強化基準と一致していることを確認する。</p> <p>2.2.b ポリシーを調べ、担当者をインタビューすることで、システム構成基準が、新たな脆弱性の問題が見つかったときに、要件 6.1 で規定されているように更新されていることを確認する。</p>	多くのオペレーティングシステム、データベース、エンタープライズアプリケーションには既知の弱点があります。また、セキュリティの脆弱性を修正するようにこれらのシステムを構成する既知の方法もあります。セキュリティの専門家でない人々のために、多数のセキュリティ組織がシス

PCI DSS 要件	テスト手順	ガイダンス
<p>業界で認知されたシステム強化基準のソースには以下が含まれる（これらに限定されない）。</p> <ul style="list-style-type: none"> ▪ Center for Internet Security (CIS) ▪ 国際標準化機構 (ISO) ▪ SysAdmin Audit Network Security (SANS) Institute ▪ 米国国立標準技術研究所 (NIST) 	<p>2.2.c ポリシーを調べ、担当者をインタビューすることで、新しいシステムが構成されたときにシステム構成基準が適用され、ネットワークにシステムがインストールされる前にその実装が検証されたことを確認する。</p> <p>2.2.d システム構成基準に、すべての種類のシステムコンポーネントに対する以下の手順が含まれていることを確認する。</p> <ul style="list-style-type: none"> • すべてのベンダ提供デフォルト値を変更し、不要なデフォルトアカウントを削除する • 同じサーバに異なったセキュリティレベルを必要とする機能が共存しないように、1つのサーバには、主要機能を1つだけ実装する • システムの機能に必要な安全性の高いサービス、プロトコル、デーモンなどのみを有効にする • 安全でないと見なされている必要なサービス、プロトコル、またはデーモンに追加のセキュリティ機能を実装する • システムセキュリティのパラメータが、悪用を防ぐために設定されている • スクリプト、ドライバ、機能、サブシステム、ファイルシステム、不要な Web サーバなど、不要な機能をすべて削除する 	<p>システム強化に関するガイドラインと推奨事項を確立し、これらの弱点を修正する方法についてアドバイスしています。</p> <p>構成基準に関するガイドラインは、www.nist.gov、www.sans.org、www.cisecurity.org、www.iso.org、製品ベンダなどから入手できます。</p> <p>システムをネットワーク上にインストールする前に、新たに発見された弱点を確実に修正するためには、システム構成基準を最新状態に保つ必要があります。</p>
<p>2.2.1 同じサーバに異なったセキュリティレベルを必要とする機能が共存しないように、1つのサーバには、主要機能を1つだけ実装する。（例えば、Web サーバ、データベースサーバ、DNS は別々のサーバに実装する必要がある。）</p> <p>注:仮想化テクノロジを使用している場合は、1つの仮想システムコンポーネントに主要機能を1つだけ実装する。</p>	<p>2.2.1.a システムコンポーネントのサンプルを選択し、システム構成を調べて1つのサーバに主要機能が1つだけ実装されていることを確認する。</p> <p>2.2.1.b 仮想化テクノロジが使用されている場合は、システム構成を調べて、1つの仮想システムコンポーネントまたはデバイスに主要機能が1つだけ実装されていることを確認する。</p>	<p>同じサーバ上に異なるセキュリティレベルが必要なサーバ機能がある場合、より高いセキュリティレベルを必要とする機能のセキュリティレベルはより低いセキュリティレベルの機能の存在によって低下する場合があります。さらに、セキュリティレベルが低い方のサーバ機能が同じサーバ上の他の機能に対し、セキュリティの脆弱性をもたらす可能性があります。システム構成基準と関連プロセスの一部として、異なるサーバ機能のセキュリティの必要性を考慮することで、組織は、同じサーバ上に異なるセキュリティレベルを必要とする機能を共存させないことを保証できます。</p>

PCI DSS 要件	テスト手順	ガイダンス
2.2.2 システムの機能に必要なサービス、プロトコル、デーモンなどのみを有効にする。	2.2.2.a システムコンポーネントのサンプルを選択し、有効なシステムサービス、デーモン、プロトコルを検査して、必要なサービスまたはプロトコルだけが有効になっていることを確認する。	要件 1.1.6 に記述されているとおり、悪意のある者によりネットワークを侵害するために一般的に使用される多くのプロトコルが業務上必要となる（またはデフォルトで有効になっている）場合があります。組織の構成基準と関連プロセスの一部としてこの要件を含めることで、必要なサービスとプロトコルのみを有効にしていることを保証できます。
	2.2.2.b 有効になっているが安全でないサービス、デーモン、プロトコルを特定し、担当者をインタビューして、それらが文書化された構成基準に従って正当化されていることを確認する。	
2.2.3 安全でないと見なされている必要なサービス、プロトコル、またはデーモンにセキュリティ機能を実装する。	2.2.3 構成設定を調べて、安全でないすべてのサービス、デーモン、プロトコルに対するセキュリティ機能が文書化および反映されていることを確認する。	新しいサーバを導入する前にセキュリティ機能を有効にすることで、サーバが安全でない構成で環境にインストールされることを防止できます。 すべての安全でないサービス、プロトコル、デーモンが適切なセキュリティ機能によって十分にセキュリティ保護されるようにすることで、悪意のある者がネットワーク内で一般的に使用される侵害ポイントを利用にくくなります。 強力な暗号化や安全なプロトコルに関する業界標準やベストプラクティスを参照します。（例えば、NIST SP 800-52 や SP 800-57、OWASPなど） 注: SSL / 初期の TLS は強力な暗号化とはみなされず、付録 A2 で定義されるように、既知の攻撃手法に対して耐性があると検証された POS POI 端末、およびこれらが接続する SSL / TLS の終端箇所を除いて、セキュリティ対策として使用することはできません。
2.2.4 システムセキュリティのパラメータが、悪用を防ぐために設定されている。	2.2.4.a システム管理者やセキュリティ管理者のインタビューを行い、システムコンポーネントの一般的なセキュリティパラメータ設定に関する知識があることを確認する。 2.2.4.b システム構成基準を調べて、一般的なセキュリティパラメータ設定が含まれていることを確認する。 2.2.4.c システムコンポーネントのサンプルを選択し、一般的なセキュリティパラメータ設定を調べて、それらが構成基準に従って正しく設定されていることを確認する。	組織のシステム構成基準と関連プロセスによって、セキュリティへの影響があることが明らかであるセキュリティ設定およびパラメータを確実に設定する必要があります。 システムを安全に設定するためには、システムの構成と管理の責任者が、そのシステムに適用する特定のセキュリティパラメータと設定に精通している必要があります。

PCI DSS 要件	テスト手順	ガイダンス
2.2.5 スクリプト、ドライバ、機能、サブシステム、ファイルシステム、および不要な Web サーバなど、すべての不要な機能を削除する。	<p>2.2.5.a システムコンポーネントのサンプルを選択し、構成を調べ、不要な機能（スクリプト、ドライバ、機能、サブシステム、ファイルシステムなど）がすべて削除されていることを確認する。</p> <p>2.2.5.b 文書とセキュリティパラメータを調べて、有効な機能が文書化されていて、セキュリティ保護された構成をサポートしていることを確認する。</p> <p>2.2.5.c 文書とセキュリティパラメータを調べて、文書化された機能だけがサンプリングされたシステムコンポーネントに存在していることを確認する。</p>	不要な機能は、悪意のある者がシステムにアクセスする機会を与える可能性がある。不要な機能を削除することで、組織は必要な機能の安全を保護し、不明な機能が悪用されるリスクを軽減できます。 サーバ強化基準とプロセスを含めることで、不要な機能に関連したセキュリティ上の影響に対処する（サーバがこの機能を実行していない場合、FTP または Web サーバを削除/無効化するなど）。
2.3 強力な暗号化を使用して、すべてのコンソール以外の管理アクセスを暗号化する。	<p>2.3 システムコンポーネントのサンプルを選択し、コンソール以外の管理アクセスが、以下によって暗号化されていることを確認する。</p> <p>2.3.a 各システムへの管理者ログオンを観察し、システム構成を調べて、管理者のパスワードが要求される前に、強力な暗号化メソッドが実行されていることを確認する。</p> <p>2.3.b システム上のサービスおよびパラメータファイルシステムをレビューし、Telnet やその他の安全でないリモートログインコマンドがコンソール外からのアクセスに使用できないことを確認する。</p> <p>2.3.c 管理者の各システムへのログオンを観察し、Web ベースの管理インターフェースへの管理者アクセスが、強力な暗号方式で暗号化されていることを確認する。</p> <p>2.3.d ベンダ文書を調べ、担当者をインタビューすることで、使用テクノロジの強力な暗号化が業界のベストプラクティスとベンダの推奨事項に従って導入されていることを確認する。</p>	コンソール外（リモートを含む）からの管理が安全な認証と暗号化された通信を使用して行われない場合、管理または運用レベルの機密情報（管理者の ID やパスワードなど）が盗聴者に知られてしまう可能性があります。悪意のある者は、この情報を使用してネットワークにアクセスし、管理者となってデータを盗むことができます。 平文プロトコル（HTTP、Telnet など）はトランザクションやログオン情報を暗号化しないため、この情報が盗聴されやすいという欠点があります。 「強力な暗号化」と見なされるためには、適切な鍵強度と鍵管理機能を持ち、業界で認識されているプロトコルを使用テクノロジの種類に合わせて導入する必要があります。（『PCI DSS と PA-DSS の用語集（用語、略語、および頭字語）』の「強力な暗号化技術」や、NIST SP800-52 や SP800-57、OWASPなどの業界標準やベストプラクティスを参照してください。） 注: SSL / 初期の TLS は強力な暗号化とはみなされず、付録 A2 で定義されるように、既知の攻撃手法に対して耐性があると検証された POS POI 端末、およびこれらが接続する SSL / TLS の終端箇所を除いて、セキュリティ対策として使用することはできません。

PCI DSS 要件	テスト手順	ガイダンス
2.4 PCI DSS の適用範囲であるシステムコンポーネントのインベントリを維持する	2.4.a システムのインベントリを調べて、ハードウェアとソフトウェアのコンポーネントリストが維持されており、それぞれの機能/使用に関する説明が含まれていることを確認する。	すべてのシステムコンポーネントの最新リストを維持することで、組織は PCI DSS コントロールを導入するための環境範囲を正確かつ効率的に定義できる。インベントリなしでは、一部のシステムのコンポーネントが忘れられたり、組織の構成基準から誤って除外されたりすることがあります。
	2.4.b 担当者をインタビューして、文書化されたインベントリが最新状態に保たれていることを確認する。	
2.5 ベンダデフォルト値およびその他のセキュリティパラメータの管理に関するセキュリティポリシーと操作手順が文書化されて使用されており、影響を受ける関係者全員に知られていることを、確実にする。	2.5 文書を調べ、関係者をインタビューすることで、ベンダデフォルトとその他のセキュリティパラメーターの管理に関するセキュリティポリシーと操作手順が以下の要件を満たしていることを確認する。 <ul style="list-style-type: none"> • 文書化されている • 使用されている • 影響を受ける関係者全員に知らされている 	ベンダデフォルト値およびその他のセキュリティパラメータが継続的に管理されて安全でない構成が防止されるように、関係者はセキュリティポリシーと毎日の操作手順を認識・順守する必要があります。
2.6 共有ホスティングプロバイダは、各事業体のホスト環境およびカード会員データを保護する必要がある。これらのプロバイダは、「付録 A1: 共有ホスティングプロバイダ向けの追加 PCI DSS 要件」に示されているように、特定の要件を満たす必要がある。	2.6 共有ホスティングプロバイダの PCI DSS 評価について、「付録 A1: 共有ホスティングプロバイダ向けの PCI DSS 追加要件」に詳しく説明されているテスト手順 A1.1 ~ A1.4 を実行し、共有ホスティングプロバイダが事業体（加盟店およびサービスプロバイダ）のホスト環境およびデータを保護していることを確認する。	これは、同じサーバ上で複数のクライアント向けの共有ホスティング環境を提供するホスティングプロバイダを対象としています。すべてのデータが同じサーバ上にあり、単一の環境の管理下にあると、多くの場合、これらの共有サーバの設定が個々のクライアントから管理できません。このため、クライアントはその他のすべてのクライアント環境のセキュリティに影響を及ぼす安全でない機能やスクリプトを追加できるので、悪意のある者はあるクライアントのデータを容易に侵害でき、さらにその他のすべてのクライアントのデータにアクセスすることができます。要件の詳細については、付録 A1 を参照してください。

カード会員データの保護

要件 3: 保存されるカード会員データを保護する

暗号化、トランケーション、マスキング、ハッシュなどの保護方式は、カード会員データ保護のための重要な要素です。侵入者が他のセキュリティコントロールを回避し、暗号化されたデータにアクセスできても、正しい暗号化鍵がなければ、そのデータを読み取り、使用することはできません。保存したデータを保護するための効果的な別の方法として考えられるのは、リスクを軽減する方法です。例えば、リスクを最小限にする方法として、カード会員データが絶対的に必要でない限り保存しない、完全な PAN が不要ならカード会員データを切り捨てる、電子メールやインスタントメッセージングなどのエンドユーザーメッセージング技術を使用して保護されていない PAN を送信しない、などがあります。

「強力な暗号化技術」および他の PCI DSS 用語については、『PCI DSS と PA-DSS の用語集（用語、略語、および頭字語）』を参照してください。

PCI DSS 要件	テスト手順	ガイダンス
<p>3.1 すべてのカード会員データ (CHD) の保存について少なくとも以下のものを含むデータ保存および廃棄ポリシー、手順、プロセスを実装することで、保存するカード会員データを最小限に抑える。</p> <ul style="list-style-type: none"> ▪ 保存するデータ量と保存期間を、法律上、規則上、および/または業務上必要な範囲に限定する。 ▪ 必要性がなくなった場合のデータを安全に削除するためのプロセス ▪ カード会員データの特定のデータ保存要件 ▪ 定義された保存要件を超えるカード会員データを安全に廃棄する四半期ごとのプロセス。 	<p>3.1.a すべてのカード会員データ (CHD) ストレージについて、データの保存および廃棄ポリシー、手順、プロセスを調べ、以下のことが含まれていることを確認する。</p> <ul style="list-style-type: none"> • 法律上、規制上、および/または業務上の要件で必要なデータのストレージ容量と保持期限の制限 • カード会員データの保存についての特定の要件（カード会員データは、X の期間、Y という業務上の理由で保存する必要がある、など）。 • 法律上、規制上、または業務上の理由で不要になったカード会員データの安全な削除のためのプロセス • 定義された保存要件を超えるカード会員データを安全に廃棄する四半期ごとのプロセス。 <p>3.1.b 担当者をインタビューして、以下を確認する。</p> <ul style="list-style-type: none"> • 保存されているカード会員データの場所すべてがデータ保存および破棄プロセスに含まれている。 • カード会員データを見つけて安全に廃棄する四半期ごとの自動または手動プロセスが含まれている。 • カード会員データのすべての場所に対して四半期ごとの自動または手動プロセスが実施されている。 	<p>正式なデータ保存ポリシーで、保存する必要があるデータとそのデータの保存場所を識別し、不要になった場合は即座に安全な方法で破棄または削除できるようにしておきます。</p> <p>承認後に保存できるカード会員データは、プライマリーアカウント番号 (PAN)（読み取り不能に処理したもの）、有効期限、カード会員名、サービスコードのみです。</p> <p>カード会員データを正しく保存し、必要なくなったときに破棄するためには、それがどこにあるかを知っていることが必要です。適切な保存要件を定義するには、まず、事業体は固有のビジネスニーズと、業界または保存するデータの種類（あるいはその両方）に適用される法律上または規則上の義務を理解する必要があります。</p> <p>特定の保存期間を過ぎて保存されているデータを特定して削除することで、不要になったデータの不要な保存を防止できます。このプロセスは、自動的でも手動でも、あるいはその組み合わせでもできます。例えば、プログラムされた手順（自動または手動）を使ってデータを見つけて削除した</p>

PCI DSS 要件	テスト手順	ガイダンス
	<p>3.1.c カード会員データを保存するシステムコンポーネントのサンプルについて</p> <ul style="list-style-type: none"> ファイルとシステムレコードを調べて、保存されているデータがデータ保存ポリシーで定義された要件を超えていないことを確認する。 削除方法を観察して、データが安全に削除されることを確認する。 	<p>り、データストレージエリアを手動でレビューしたりすることなどが可能です。</p> <p>安全な削除方法を実装することにより、不要になつたデータを確実に取得できなくします。</p> <p>必要ない場合は、保存してはいけません。</p>
<p>3.2 承認後に機密認証データを保存しない（暗号化されている場合でも）。機密認証データを受け取った場合、認証プロセスが完了し次第すべてのデータを復元不可能にする。</p> <p>以下の場合に、イシュアとイシューイングサービスをサポートする企業は機密認証データを保存することが可能である。</p> <ul style="list-style-type: none"> 業務上の正当な理由がある データが安全に保存されている <p>機密認証データには、以降の要件 3.2.1 ~ 3.2.3 で言及されているデータを含む。</p>	<p>3.2.a イシュアまたはイシューイングサービスをサポートし機密認証データを保存する会社について、ポリシーを調べ、担当者をインタビューすることで、機密認証データを保存する発行者または会社について、機密認証データの保存に関して文書化された業務上の理由があることを確認する。</p>	<p>機密認証データは、フルトラックデータ、カード検証コードまたは値、PIN データから構成されます。承認後の機密認証データの保存は禁止されています。このデータからペイメントカードを偽造し、不正トランザクションを作成することができるため、このデータは悪意のある者にとって非常に貴重です。</p>
	<p>3.2.b イシュアまたはイシューイングサービスをサポートし、機密認証データを保存する会社について、データストアとシステム構成を調べて、機密認証データがセキュアに保存されていることを確認する。</p>	<p>ペイメントカードを発行するか、発行サービスを実施するかサポートする事業体は、発行機能の一部として機密認証データを作成・制御することがよくあります。サービスの発行を実施、推進、またはサポートする会社は、業務上の正当な理由がある場合に限り、機密認証データを保存できます。イシュアにはすべての PCI DSS 要件が適用されますが、イシュアとイシューイングサービスにとって唯一の例外は、業務上の正当な理由がある場合は機密認証データを保存できるということです。正当な理由とは、イシュアが提供する機能の遂行に必要で、単なる利便性を目的としない理由のことです。これらのデータは PCI DSS および個別のペイメントブランド要件に従って安全に保存する必要があります。</p>
	<p>3.2.c その他のすべての事業体では、機密認証データを受信した場合、ポリシーと手順をレビューし、システム構成を調べて、認証後にデータが保存されていないことを確認します。</p>	<p>発行しない事業体では、承認後機密認証データを保存することは許可されません。</p>
	<p>3.2.d その他のすべての事業体では、機密認証データを受け取った場合、手順をレビューしてデータを安全に削除するプロセスを調べ、データが回復不能であることを確認する。</p>	

PCI DSS 要件	テスト手順	ガイダンス
<p>3.2.1 (カードの裏面やチップ上の同等のデータなどにある磁気ストライプの) トラックデータの完全な内容を承認後に保存しない。このデータは、フルトラック、トラック、トラック 1、トラック 2、磁気ストライプデータとも呼ばれます。</p> <p>注: 通常の取引過程では、磁気ストライプからの以下のデータ要素を保存する必要が生じる場合があります。</p> <ul style="list-style-type: none"> ▪ カード会員名 ▪ プライマリアカウント番号 (PAN) ▪ 有効期限 ▪ サービスコード <p>リスクを最小限に抑えるため、取引に必要なデータ要素のみを保存します。</p>	<p>3.2.1 システムコンポーネントのサンプルで、データソースを調べる。これには、以下の項目が含まれるがこれらに限定されない。また、カード裏面の磁気ストライプまたはチップの同等データから得られたトラック内容が、承認後、保存されていないことを確認する。</p> <ul style="list-style-type: none"> ▪ 受信トランザクションデータ ▪ すべてのログ（トランザクション、履歴、デバッグ、エラーなど） ▪ 履歴ファイル ▪ トレースファイル ▪ データベーススキーマ ▪ データベースコンテンツ 	<p>フルトラックデータが保存されると、そのデータ入手した悪意のある者はそのデータを使ってペイメントカードを複製し、不正なトランザクションを行うことができます。</p>
<p>3.2.2 カードを提示しない取引を検証するために使用された、カード検証コードまたは値（ペイメントカードの表面または裏面に印字されている 3 桁または 4 桁の数字）を承認後に保存しない。</p>	<p>3.2.2 システムコンポーネントのサンプルについて、カード表面または署名欄に印字されている 3 桁または 4 桁のカード検証コードまたは値 (CVV2、CVC2、CID、CAV2 データ) を含む（ただし、これらに限定されない）データソースを調べて、これらが、承認後、保存されないことを確認する。</p> <ul style="list-style-type: none"> ▪ 受信トランザクションデータ ▪ すべてのログ（トランザクション、履歴、デバッグ、エラーなど） ▪ 履歴ファイル ▪ トレースファイル ▪ データベーススキーマ ▪ データベースコンテンツ 	<p>カード検証コードの目的は、消費者とカードを対面で取引しない、「カードを提示しない」取引（インターネットまたは通信販売「MO/TO」取引）を保護することです。</p> <p>このデータが盗まれた場合、悪意のある者はインターネットおよび MO/TO 取引を偽造できます。</p>

PCI DSS 要件	テスト手順	ガイダンス
<p>3.2.3 個人識別番号 (PIN) または暗号化された PIN ブロックを承認後に保存しない。</p>	<p>3.2.3 システムコンポーネントのサンプルについて、データソースを調べる。これには PIN および暗号化された PIN ブロックが、承認後、保存されないこの確認も含まれる（ただし、これらに限定されない）。</p> <ul style="list-style-type: none"> ▪ 受信トランザクションデータ ▪ すべてのログ（トランザクション、履歴、デバッグ、エラーなど） ▪ 履歴ファイル ▪ トレースファイル ▪ データベーススキーマ ▪ データベースコンテンツ 	<p>これらの値を知っている必要があるのは、カード所有者またはカードを発行した銀行のみです。このデータが盗まれた場合、悪意のある者は PIN ベースの引き落とし取引（ATM での引き出しなど）を偽造することができます。</p>
<p>3.3 表示時に PAN をマスクして（先頭 6 枠と末尾 4 枠が最大表示桁数）、業務上の正当な理由がある関係者だけが先頭 6 枠/末尾 4 枠を超える PAN を見ることができるようとする。</p> <p>注: カード会員データの表示（法律上、またはペイメントカードブランドによる POS レシート要件など）に関するこれより厳しい要件がある場合は、その要件より優先されることはありません。</p>	<p>3.3.a PAN の表示をマスクするための、明文化されたポリシーと手順を調べて、以下を確認する。</p> <ul style="list-style-type: none"> • 先頭 6 枠/末尾 4 枠を超える PAN（PAN 全体を含む）の表示へのアクセスを必要とする役割の一覧が、アクセス権を持つ正当な業務上の理由とともに文書化されていること。 • PAN を表示する際は、正当な業務上の理由のある担当者のみが先頭 6 枠/末尾 4 枠を超える PAN を見ることができるようにマスクする必要がある。 • PAN 全体を表示する承認のない役割の者はすべて、マスクされた PAN しか見えなくする。 <p>3.3.b システム構成を調べて、文書化された業務上の必要性のあるユーザー/役割に対してのみ PAN 全体が表示され、他のすべての表示要求に対しては PAN はマスクされることを確認する。</p> <p>3.3.c PAN の表示（画面、紙のレシートなど）を調べて、業務上の正当な必要性により先頭 6 枠/末尾 4 枠を超える PAN を見る必要のある場合を除き、カード会員データを表示する際に PAN がマスクされることを確認する。</p>	<p>コンピュータ画面、ペイメントカードの領収書、FAX、または紙の計算書などのアイテムに PAN 全体が表示されると、このデータが権限のない人々によって取得され、不正に使用される可能性があります。業務上の正当な理由により PAN 全体を見る必要がある者に対してのみ PAN 全体を表示すると、承認されていない者が PAN にアクセスするリスクを最小限に抑えることができます。</p> <p>マスキング方法は、特定業務機能の実行に必要な最低限の桁数のみが表示されることを常に確実にするべきです。例えば、ある業務機能を実施するために末尾 4 枠のみが必要となる場合は、その業務を実行する個人が末尾 4 枠のみを参照できるように PAN をマスクします。その他の例として、ある業務がルーティング目的⁷で銀行識別番号（BIN）にアクセスする必要がある場合、業務中は BIN 枠（一般的に先頭 6 枠）のみ表示します。</p> <p>この要件は画面、紙の領収書や印刷物などに表示された PAN の保護に関連します。ファイルやデータベースなどに保存された PAN の保護に関する要件 3.4 と混同しないよう注意してください。</p>

⁷ BIN 枠を使用して、使用されたペイメントカードが所属するイシュアを特定するなど。

PCI DSS 要件	テスト手順	ガイダンス
<p>3.4 以下の手法を使用して、すべての保存場所で PAN を少なくとも読み取り不能にする（ポータブルデジタルメディア、バックアップメディア、ログを含む）。</p> <ul style="list-style-type: none"> ▪ 強力な暗号化技術をベースにしたワンウェイハッシュ（PAN 全体をハッシュする必要がある） ▪ トランケーション（PAN の切り捨てられたセグメントの置き換えにはハッシュを使用できない） ▪ インデックストークンとパッド（パッドは安全に保存する必要がある） ▪ 関連する鍵管理プロセスおよび手順を伴う、強力な暗号化 <p>注:悪意のある個人がトランケーションされた PAN とハッシュ化された PAN の両</p>	<p>3.4.a 以下の方法を用いて、ベンダ、システム/プロセスのタイプ、暗号化アルゴリズム（該当する場合）などが記載された、PAN の保護に使用されているシステムに関する文書を調べる。</p> <ul style="list-style-type: none"> ▪ 強力な暗号化技術をベースにしたワンウェイハッシュ ▪ トランケーション ▪ インデックストークンとパッド（パッドは安全に保存する必要がある） ▪ 関連する鍵管理プロセスおよび手順を伴う、強力な暗号化 <p>3.4.b データリポジトリのサンプルから複数のテーブルまたはファイルを検査し、PAN が読み取り不能になっていることを確認する（平文で保存されていない）。</p> <p>3.4.c リムーバブルメディア（バックアップテープなど）を検査し、PAN が読み取り不能であることを確認する。</p> <p>3.4.d ペイメントアプリケーションログを含む監査ログのサンプルを検査し、PAN が読み取り不能か、ログ中に存在しないことを確認する。</p>	<p>主な保管場所（データベース、またはテキストファイルスプレッドシートなどのフラットファイル）およびそれ以外の保管場所（バックアップ、監査ログ、例外またはトラブルシューティングログ）に保存される PAN はすべて保護する必要があります。</p> <p>強力な暗号化技術をベースにしたワンウェイハッシュ関数を使用して、カード会員データを読み取り不能にすることができます。ハッシュ関数は元の数値を取得する必要がない場合に適しています（ワンウェイハッシュは復元できません）。攻撃者がデータを事前に計算されたハッシュ値のテーブルと比較（して PAN を導出）する可能性を低減するために、ハッシュする前にカード会員データに追加のランダム入力値を追加することが推奨されていますが、現時点では要求されていません。</p> <p>トランケーションの目的は、PAN の断片化したデータの一部を永続的に削除したうえで（一般的</p>

PCI DSS 要件	テスト手順	ガイダンス
<p>方を取得した場合、元の PAN を比較的容易に再現することができます。ハッシュ化およびトランケーションされた PAN の同じバージョンが事業体の環境に存在する場合、元の PAN を再構築するために、ハッシュ化およびトランケーションされたバージョンを関連付けることはできないことを確実にする追加コントロールを導入する必要があります。</p> <p>3.4.1 (ファイルまたは列レベルのデータベース暗号化ではなく) ディスク暗号化が使用される場合、論理アクセスはネイティブなオペレーティングシステムの認証およびアクセス制御メカニズムとは別に管理する必要がある (ローカルユーザーアカウントデータベースや一般的なネットワークログイン資格情報を使用しないなどの方法で)。復号鍵がユーザーアカウントと関</p>	<p>3.4.e 同じ PAN のハッシュ化および切り捨てられたバージョンが環境に存在する場合、導入されているコントロールを調べて、元の PAN を再構築するためにハッシュ化およびトランケーションされたバージョンを関連付けできることを確認する。</p> <p>3.4.1.a ディスク暗号化を使用している場合、構成を調べて、認証プロセスを観察し、暗号化されたファイルシステムへの論理アクセスが、ネイティブなオペレーティングシステムのメカニズムとは別のメカニズムで実装されていることを確認する (ローカルユーザーアカウントデータベースや一般的なネットワークログイン資格情報を使用しないなどの方法で)。</p> <p>3.4.1.b プロセスを観察し、担当者をインタビューすることで、暗号化鍵が安全に保存されていることを確認する (強力なアクセス制御で適切に保護されているリムーバブルメディアに保存されているなど)。</p>	<p>に先頭 6 衔と末尾 4 衔を超えないようにする) PAN を保存することです。</p> <p>インデックストークンは、指定のインデックスをベースに PAN を予測不能な値に置き換える暗号トークンです。ワンタイムパッドは、ランダム生成の秘密鍵を 1 回だけ使用してメッセージを暗号化し、一致するワンタイムパッドと鍵を使用して復号するシステムです。</p> <p>強力な暗号化技術 (『PCI DSS と PA-DSS の用語集 (用語、略語、および頭字語)』で定義) の意図は、業界がテスト済みの認められたアルゴリズム (専用または「内製」のアルゴリズムではなく) と強力な暗号化鍵を基にした暗号化技術を利用することです。</p> <p>悪意のある個人は、特定の PAN をハッシュ化したものとトランケーションしたものと関連付けて元の PAN を容易に再現することができます。このデータの関連付けを防ぐコントロールを実施することで、元の PAN を読み取り不能の状態に保つことが可能になります。</p> <p>この要件の目的は、カード会員データを読み取り不能にするためのディスクレベルでの暗号化の許容基準を設定することです。ディスクレベルの暗号化は、コンピュータ上のディスク/パーティション全体に保存されているデータを暗号化し、権限のあるユーザが要求したときに情報を自動的に復号します。ディスク暗号化ソリューションの多くは、オペレーティングシステムの読み取り/書き込み操作を遮断し、システム起動時またはセッション開始時のパスワードまたはパスフレーズの入力</p>

PCI DSS 要件	テスト手順	ガイダンス
<p>連付けられていない。</p> <p>注: この要件は他のすべての暗号化および鍵管理に関する PCI DSS 要件に加えて適用されます。</p>	<p>3.4.1.c 構成を調べて、プロセスを観察することで、どこに保存されている場合でも、リムーバブルメディアのカード会員データが暗号化されていることを確認する。</p> <p>注: ディスク暗号化がリムーバブルメディアの暗号化に使用されていない場合は、この媒体に保存されるデータを、他の方法を使って、読み取り不能にする必要があります。</p>	<p>以外、ユーザによる特別な操作を一切必要とせずに適切な暗号化変換を実行します。ディスクレベルの暗号化のこれらの特性に基づいてこの要件に準拠するためには、この方式で以下をしないようにする必要があります。</p> <ol style="list-style-type: none"> 1) オペレーティングシステムと同じユーザアカウント認証文字列を使用する 2) システムのローカルユーザアカウントデータベースまたは一般的なネットワークログイン資格情報に関連付けられているか、これらから派生した復号鍵を使用する <p>ディスク全体の暗号化は、ディスクが物理的に紛失した場合のデータの保護に役立つため、カード会員データを保存している携帯デバイスに適しています。</p>
<p>3.5 カード会員データを漏洩と悪用から保護するために使用される鍵を保護するための手順を文書化し、実施する。</p> <p>注: この要件は、保存されているカード会員データを暗号化する鍵に適用され、またデータ暗号化鍵の保護に使用する鍵暗号化鍵にも適用される。つまり、鍵暗号化鍵は、少なくともデータ暗号化鍵と同じ強度をもつ必要がある。</p>	<p>3.5 鍵管理ポリシーと手順を調べて、プロセスがカード会員データを暗号化した鍵を漏洩と悪用から保護するよう規定されており、少なくとも以下を含むことを確認する。</p> <ul style="list-style-type: none"> • 暗号化鍵へのアクセスが必要最小限の管理者に制限されている • 鍵暗号化鍵が少なくとも保護対象データの暗号化鍵と同じ強度をもつ • 鍵暗号化鍵がデータ暗号化鍵とは別に保存されている • 鍵の保存場所と形式を最小限にし、安全に保存する 	<p>暗号化鍵へのアクセスを取得するとデータを復号できるため、暗号化鍵は厳重に保護する必要があります。鍵暗号化鍵を使用する場合、データを暗号化する鍵とその鍵で暗号化されたデータを適切に保護するには、少なくともデータ暗号化鍵と同じ強度をもつ必要があります。</p> <p>鍵を漏洩と悪用から保護するための要件は、データ暗号化鍵と鍵暗号化鍵の両方に適用されます。1つの鍵暗号化鍵で複数のデータ暗号化鍵へのアクセスが付与される場合があるため、鍵暗号化鍵には強力な保護手段が必要です。</p>

PCI DSS 要件	テスト手順	ガイダンス
<p>3.5.1 サービスプロバイダに対する追加の要件：以下を含む文書化された暗号化アーキテクチャの詳細を維持する：</p> <ul style="list-style-type: none"> ▪ カード会員データの保護に使われるすべてのアルゴリズム、プロトコル、および鍵の強度と有効期限を含む鍵の詳細 ▪ 各鍵の使用方法の詳細 ▪ 鍵管理で使用される任意の HSM および他の SCD のインベントリ 	<p>3.5.1 責任者をインタビューし、文書をレビューすることで、暗号化アーキテクチャを説明する文書が存在することを確認する。これには以下を含む：</p> <ul style="list-style-type: none"> ▪ カード会員データの保護に使われるすべてのアルゴリズム、プロトコル、および鍵の強度と有効期限を含む鍵の詳細 ▪ 各鍵の使用方法の詳細 ▪ 鍵管理で使用される任意の HSM および他の SCD のインベントリ 	<p>注：この要件は評価される事業体がサービスプロバイダである場合のみ適用されます。</p> <p>暗号化アーキテクチャの文書を最新の状態に保つことで、カード会員データを保護するためのアルゴリズム、プロトコル、および暗号化鍵だけではなく、鍵の生成、使用、保護するデバイスを、事業体が理解することが可能となります。これによって、事業体は異なるアルゴリズム/鍵の強度の変更により提供される保証レベルなどの計画の見直しをすすめることができます。このような文書を維持することで、事業体は鍵または鍵管理デバイスの消失または紛失を検知し、その暗号化アーキテクチャに対する無許可の追加を識別することもできます。</p>
<p>3.5.2 暗号化鍵へのアクセスを、必要最小限の管理者に制限する。</p>	<p>3.5.2 ユーザのアクセスリストを調べて、鍵へのアクセスがごく少数の管理者に制限されていることを確認する。</p>	<p>暗号化鍵にアクセスできる人物はごく少数にするべきです（カード会員データが無許可の人々から見られる可能性を減らすために）、通常、鍵管理者のみにします。</p>
<p>3.5.3 カード会員データの暗号化に使用される秘密暗号化鍵は、以下のいずれかの形式（複数可）で常時保存する。</p> <ul style="list-style-type: none"> • 少なくともデータ暗号化鍵と同じ強度の鍵暗号化鍵で暗号化されており、データ暗号化鍵とは別の場所に保存されている • 安全な暗号化デバイス（ハードウェア（ホスト）セキュリティモジュール（HSM）または PTS 承認の加盟店端末装置など）内 	<p>3.5.3.a 文書化された手順を調べて、カード会員データの暗号化に使用される暗号化鍵が常に以下のいずれかの形式でのみ存在することを確認する。</p> <ul style="list-style-type: none"> • 少なくともデータ暗号化鍵と同じ強度の鍵暗号化鍵で暗号化されており、データ暗号化鍵とは別の場所に保存されている • 安全な暗号化デバイス（ハードウェア（ホスト）セキュリティモジュール（HSM）または PTS 承認の加盟店端末装置など）内 • 業界承認の方式に従う、鍵コンポーネントまたは鍵共有として 	<p>暗号化鍵は、承認されていないまたは不必要的カード会員データへのアクセスを防止するため、安全に保存する必要があります。</p> <p>鍵の暗号化鍵を暗号化する必要はありませんが、要件 3.5 で定義されているように、漏洩や悪用に対する保護が必要です。鍵暗号化鍵を用いる場合、鍵暗号化鍵を物理的または論理的（あるいはその両方）にデータ暗号化鍵とは別の場所に保存することで、2つの鍵に不正アクセスされるリスクが軽減されます。</p>

PCI DSS 要件	テスト手順	ガイダンス
<ul style="list-style-type: none"> 業界承認の方式に従う、少なくとも 2 つの全長鍵コンポーネントまたは鍵共有として <p>注:公開鍵がこれらの形式で保存されていることは要求されていません。</p>	<p>3.5.3.b システム構成と鍵の保存場所を調べて、カード会員データの暗号化に使用される暗号化鍵が常に次のいずれかの形式（複数可）で存在していることを確認する。</p> <ul style="list-style-type: none"> 鍵暗号化鍵による暗号化 安全な暗号化デバイス（ハードウェア（ホスト）セキュリティモジュール（HSM）または PTS 承認の加盟店端末装置など）内 業界承認の方式に従う、鍵コンポーネントまたは鍵共有として <p>3.5.3.c 鍵暗号化鍵を使用する場合、システム構成と鍵の保存場所を調べて、以下を確認する。</p> <ul style="list-style-type: none"> 鍵暗号化鍵が少なくとも保護対象データの暗号化鍵と同じ強度をもつ 鍵暗号化鍵がデータ暗号化鍵とは別に保存されている 	
3.5.4 暗号化鍵を最小限の場所に保存する。	3.5.4 鍵の保存場所を調べ、プロセスを観察し、必要最小限の場所に鍵が保存されていることを確認する。	暗号化鍵を最小限の場所にのみ保存することで、組織はすべての鍵保存場所を追跡・監視し、鍵が無許可のユーザにさらされる危険を最小限にできます。
3.6 カード会員データの暗号化に使用される暗号化鍵の管理プロセスおよび手順をすべて文書化し、実装する。これには、以下が含まれる。 <p>注:鍵管理には多数の業界標準があり、NIST (http://csrc.nist.gov を参照) などさまざまなリソースから入手可能です。</p>	<p>3.6.a サービスプロバイダ評価のための追加のテスト手順：サービスプロバイダがカード会員データの伝送に使用する鍵を顧客と共有している場合、サービスプロバイダが顧客に提供する文書を調べて、以下の要件 3.6.1～3.6.8 に従って、顧客の鍵（顧客とサービスプロバイダ間でデータを伝送するために使用される）を安全に伝送、保存、変更する方法が記述されていることを確認する。</p> <p>3.6.b カード会員データの暗号化に使用される暗号化鍵の管理手順とプロセスを調べて、以下を行う。</p>	<p>暗号化鍵の管理方法は、暗号化ソリューションのセキュリティを継続させるための重要な要素です。適切な鍵管理プロセスは、手動、または暗号化製品の一部として自動化されている場合のいずれも、業界標準に基づき、すべての鍵要素を 3.6.1～3.6.8 に対応させます。</p> <p>顧客に暗号化鍵を安全に送信、保存、更新するためのガイダンスを提供することは、鍵の管理上のミスや無許可の事業体への漏洩の防止に役立ちます。</p> <p>この要件は、保存されたカード会員データの暗号化に使用する鍵および個々の鍵暗号化鍵を適用対象とします。</p> <p>注：テスト手順 3.6.a はサービスプロバイダを評価する場合のみに適用される追加の手順です。</p>
3.6.1 強力な暗号化鍵の生成	3.6.1.a 鍵管理手順に、強力な鍵の生成方法が指定されていることを確認する。	暗号化ソリューションは、『PCI DSS と PA-DSS の用語集（用語、略語、および頭字語）』の「暗

PCI DSS 要件	テスト手順	ガイダンス
	3.6.1.b 鍵の生成方法を観察して、強力な鍵が生成されることを確認する。	号化鍵の生成」に定義されている強力な鍵を生成する必要があります。強力な暗号化鍵の使用により、暗号化されたカード会員データの安全レベルが著しく向上します。
3.6.2 安全な暗号化鍵の配布	3.6.2.a 鍵管理手順に、鍵の安全な配布方法が指定されていることを確認する。 3.6.2.b 鍵を配布する方法を観察し、鍵が安全に配布されることを確認する。	暗号化ソリューションは鍵を安全に配布する必要があります。つまり、鍵を要件 3.5.2 で指定されている管理者にのみ配布し、決して平文で配布しないことを意味します。
3.6.3 安全な暗号化鍵の保存	3.6.3.a 鍵管理手順に、鍵の安全な保存方法が指定されていることを確認する。 3.6.3.b 鍵を保存する方法を観察して、鍵が安全に保存されることを確認する。	暗号化ソリューションは鍵を安全に保存する必要があります（鍵暗号化鍵で暗号化するなど）。適切な保護なしで鍵を保存すると、攻撃者にアクセスを許し、カード会員データの復号、および漏洩をもたらす危険があります。
3.6.4 関連アプリケーションベンダまたは鍵の所有者が定義し、業界のベストプラクティスおよびガイドライン（例えば、NIST Special Publication 800-57）に基づいた、暗号化期間の終了時点に到達した暗号化鍵の鍵変更。暗号化期間の終了時点とは、例えば、定義された期間が経過した後、または付与された鍵で一定量の暗号化テキストを作成した後（またはその両方）である。	3.6.4.a 鍵管理手順に、使用されている各鍵の種類ごとの暗号化期間の定義が含まれており、定義された暗号化期間の終わりに行う鍵変更のプロセスが定義されていることを確認する。 3.6.4.b 担当者をインタビューすることで、定義された暗号化期間の終わりに鍵が変更されていることを確認する。	暗号化期間とは、定義された目的で特定の暗号化鍵を使用できる期間のことです。暗号化期間を定義する場合には、基盤アルゴリズムの強度、鍵のサイズまたは鍵長、鍵が危険にさらされるリスク、暗号化するデータの機密性などを考慮する必要がありますが、これらに限りません。 鍵の暗号化期間の終わりに暗号化鍵の定期的な変更を行うことは、暗号化鍵が取得され、データが復号されるリスクを最小限に抑えるために必須です。
3.6.5 （平文暗号化鍵の知識を持つ従業員が離職したなど、）鍵の整合性が脆弱になっている場合、または鍵が侵害された疑いがある場合に必要な、鍵の破棄または取り替え（アーカイブ、破壊、無効化など）。	3.6.5.a 鍵管理手順に、以下のプロセスが指定されていることを確認する。 <ul style="list-style-type: none"> • 鍵の整合性が脆弱になったときの鍵の破棄または取り替え。 • 侵害されたことがわかっているまたは疑われる鍵の取り替え。 • 破棄された、または取り替えられた鍵を保持する場合、その鍵が暗号化操作に使用されていないこと。 	使われなくなった、または不要になった鍵、および脆弱であることがわかっているまたは疑われる鍵は、破棄するか破壊して使用できないようにする必要があります。（アーカイブされた暗号化データをサポートするなどのために）そのような鍵を保管しておく必要がある場合は、厳重に保護する必要があります。

PCI DSS 要件	テスト手順	ガイダンス
<p>その鍵を（例えば、鍵暗号化鍵を使用することにより）安全にアーカイブする必要がある。アーカイブされた暗号化鍵は、復号/検証の目的のためにのみ使用できます。</p> <p>3.6.6 平文暗号化鍵の管理を手動で操作する場合、鍵の知識分割とデュアルコントロールを使用する必要がある。</p> <p>注: 手動の鍵管理操作の例には、鍵の生成、伝送、読み込み、保存、破棄などが含まれますが、これらに限定されません。</p>	<p>3.6.5.b 担当者をインタビューすることで、以下のプロセスが実施されていることを確認する。</p> <ul style="list-style-type: none"> 鍵の知識を持つ従業員が退職した場合など、鍵の整合性が脆弱になったときに必要に応じて鍵を破棄する、または取り替える。 侵害されたことがわかっているまたは疑われる鍵が取り替えられている。 破棄された、または取り替えられた鍵を保持する場合、その鍵が暗号化操作に使用されていないこと。 <p>3.6.6.a 手動の平文暗号化鍵の管理手順に、以下のプロセスが指定されていることを確認する。</p> <ul style="list-style-type: none"> 鍵知識の分割により、鍵コンポーネントが 2 人以上の管理下に置かれ、各人は自分の鍵コンポーネントに関する知識しか持たないようにする。および 鍵のデュアルコントロールにより、いかなる鍵管理操作を行う場合にも 2 人以上を必要とし、どちらも他方の認証情報（パスワードや鍵など）にアクセスできないようにする。 <p>3.6.6 b 担当者をインタビューするかプロセスを観察して、手動の平文暗号化鍵が次の方法で管理されていることを確認する。</p> <ul style="list-style-type: none"> 知識分割、および デュアルコントロール 	<p>また、暗号化ソリューションでは、侵害されたことがわかっている、またはその疑いがある鍵を取り替えるプロセスを提供し、使いやすくする必要があります。</p> <p>鍵の知識の分割とデュアルコントロールは、1 人の人物が鍵全体にアクセスできる可能性を排除するために使用されます。この管理は通常、手動の鍵管理操作に、または鍵管理が暗号化製品によって実装されていない場合に適用されます。</p> <p>鍵の知識分割方法では、2 人以上が別々に鍵コンポーネントを持っており、個々の知識では暗号化鍵を生成できないようにした状態を指します。各人は、自分の鍵コンポーネントしか知りません。</p> <p>デュアルコントロールでは、2 人以上が 1 つの機能を実行し、どの 1 人も他方の認証情報にアクセスもできなくなっています。</p>
3.6.7 暗号化鍵の不正置換の防止。	<p>3.6.7.a 鍵管理手順で、鍵の不正置換を防止するプロセスが指定されていることを確認する。</p> <p>3.6.7.b 担当者をインタビューするかプロセスを観察して、鍵の不正置換が防止されていることを確認する。</p>	<p>暗号化ソリューションでは、不正なソースまたは予期しないプロセスからの鍵の置換を許可してはいけません。</p>
3.6.8 暗号化鍵の管理者が自身の責務を理解し、鍵管理者としての責務を受諾する。	<p>3.6.8.a 鍵管理手順に、鍵管理者が自身の責務を理解し、鍵管理者としての責務を受諾したことを示す書面または電子ファイルへの署名を要求するプロセスが指定されていることを確認する。</p> <p>3.6.8.b 鍵管理者が鍵管理者としての責務を理解して（書面または電子的に）受諾したことを示す文書または他の証拠を観察する。</p>	<p>このプロセスは、個人が鍵管理者としての役割を果たし、自身の責務を理解し、受諾することを確実にするために役立ちます。</p>

PCI DSS 要件	テスト手順	ガイダンス
<p>3.7 保存されているカード会員データを保護するためのセキュリティポリシーと操作手順が文書化および使用されており、影響を受ける関係者全員に知られていることを、確実にする。</p>	<p>3.7 文書を調べ、関係者をインタビューすることで、保存されているカード会員データを保護するためのセキュリティポリシーと操作手順が以下の要件を満たしていることを確認する。</p> <ul style="list-style-type: none"> • 文書化されている • 使用されている • 影響を受ける関係者全員に知らされている 	カード会員データの安全な保存の継続的な管理を行うために、関係者はセキュリティポリシーと文書化されている操作手順を認識・順守する必要があります。

要件 4: オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化する

ネットワークには悪意のある者が容易にアクセスできるため、機密情報をネットワーク経由で伝送する場合は暗号化する必要があります。誤って構成されたワイヤレスネットワーク、および従来の暗号化や認証プロトコルの脆弱性は、こうした脆弱性につけこんでカード会員データ環境への特権アクセスを取得する、悪意のある者の標的となります。

PCI DSS 要件	テスト手順	ガイダンス
4.1 オープンな公共ネットワーク経由で機密性の高いカード会員データを伝送する場合、以下のような、強力な暗号化とセキュリティプロトコルを使用して保護する。 <ul style="list-style-type: none"> • 信頼できる鍵と証明書のみを受け入れる • 使用されているプロトコルが、安全なバージョンまたは構成のみをサポートしている • 暗号化の強度が使用中の暗号化方式に適している オープンな公共ネットワークの例として以下があげられるが、これらに限定されない。 <ul style="list-style-type: none"> ▪ インターネット ▪ 802.11 と Bluetooth を含むワイヤレステクノロジ ▪ Global System for Mobile communications (GSM) や Code division multiple access (CDMA) などの携帯端末テクノロジ ▪ General Packet Radio Service (GPRS) 	4.1.a カード会員データがオープンな公共ネットワーク経由で送受信される場所をすべて特定する。文書化された基準を調べ、システム構成を比較して、すべての場所でセキュリティプロトコルと強力な暗号化が使用されていることを確認する。 4.1.b 文書化されたポリシーと手順を調べて、以下のプロセスが規定されていることを確認する。 <ul style="list-style-type: none"> • 信頼できる鍵または証明書（あるいはその両方）のみが受け付けられている • 使用されているプロトコルが安全なバージョンと構成のみをサポートしており、安全でないバージョンや構成がサポートされない • 使用中の暗号化手法に、適切な強度の暗号化が実装されている 4.1.c 発信・着信の発生時（例えば、システムプロセスまたはネットワークトラフィックの観察によって）の選択および観察し、カード会員データが転送中に強力な暗号化技術で暗号化されていることを確認する。 4.1.d 鍵および証明書を調べて、信頼できる鍵および/または証明書のみが受け付けられていることを確認する。 4.1.e システム構成を調べて、プロトコルの安全な構成のみが使用され、安全でないバージョンまたは構成がサポートされないことを確認する。 4.1.f システム構成を調べて、使用中の暗号化手法に、適切な強度の暗号化が実装されていることを確認する（ベンダの推奨事項/ベストプラクティスを確認する）。	悪意のある者が伝送中にデータを傍受したり宛先を変更させたりすることは容易で一般的であるため、機密情報を公共ネットワーク経由で伝送する場合は暗号化する必要があります。 カード会員データの安全な送信には、信頼されている鍵/証明書、トランスポート用の安全なプロトコル、適切な強度の暗号化の使用が必要です。必要な暗号化の強度をサポートせず、そのため接続が安全でないシステムからの接続要求は受け付けないでください。 一部のプロトコルの実装（SSL、SSH v1.0、初期の TLS のバージョンなど）では、攻撃者がシステムの制御を得るために使用できる、脆弱性が存在することに注意してください。どのセキュリティプロトコルを使用する場合も、安全なバージョンと構成のみが使用され、安全でない接続の使用が防止されることを確認してください。例えば、信頼済み証明書のみを使用すること、または強力な暗号化のみをサポートする（弱い、安全でないプロトコルまたは手法をサポートしない） 証明書が信頼されている（例えば、期限が切れておらず、発行元が信頼されているなど）ことの検証は、安全な接続の整合性を確保するのに役立ちます。

PCI DSS 要件	テスト手順	ガイダンス
<ul style="list-style-type: none"> ▪ 衛星通信 	<p>4.1.g TLS 実装の場合：システム構成を調べて、カード会員データの送受信時に TLS が有効になっていることを確認する。</p> <p>例えば、ブラウザベースの実装の場合：</p> <ul style="list-style-type: none"> ▪ ブラウザの URL プロトコルとして HTTPS が表示される ▪ カード会員データは、URL に HTTPS が表示される場合にのみ要求される 	<p>通常、Web ページの URL は、https で始まり、ブラウザウィンドウ内のどこかに南京錠のアイコンが表示されます。また、SSL 証明書ベンダーの多くは、目立つ検証マーク（「セキュリティシール」または「セキュリティ信頼シール」ともいう）も提供し、このシールをクリックするとその Web サイトについての情報が表示されます。</p> <p>強力な暗号化や安全なプロトコルに関する業界標準やベストプラクティスを参照します。（例えば、NIST SP 800-52 や SP 800-57、OWASP など）</p> <p>注: SSL / 初期の TLS は強力な暗号化とはみなされず、付録 A2 で定義されるように、既知の攻撃手法に対して耐性があると検証された POS POI 端末、およびこれらが接続する SSL / TLS の終端箇所を除いて、セキュリティ対策として使用することはできません。</p>
<p>4.1.1 カード会員データを伝送する、またはカード会員データ環境に接続されているワイヤレスネットワークが、認証および伝送用に強力な暗号化を実装するため、業界のベストプラクティスを使用していることを確実にする。</p>	<p>4.1.1 カード会員データを伝送する、またはカード会員データ環境に接続されているすべてのワイヤレスネットワークを識別する。文書化されている基準を調べ、システム構成設定と比較して、識別されたすべてのワイヤレスネットワークについて以下を確認する。</p> <ul style="list-style-type: none"> • 業界のベストプラクティスを使用して認証および伝送用の強力な暗号化が実装されている。 • 認証や送信のセキュリティ対策に弱い暗号化（WEP、SSL など）が使用されていない。 	<p>悪意のある者は、入手が容易な無料のツールを使用して、ワイヤレス通信を傍受します。強力な暗号化を使用すると、ワイヤレスネットワーク上で機密情報の開示を制限することができます。</p> <p>悪意のある者がワイヤレスネットワークにアクセスしたり、ワイヤレスネットワークを利用して他の内部ネットワークまたはデータにアクセスするのを防ぐには、カード会員データの認証と伝送に対する強力な暗号化が必要です。</p>
<p>4.2 保護されていない PAN をエンドユーザメッセージングテクノロジ（電子メール、インスタントメッセージング、SMS、チャットなど）で送信しない。</p>	<p>4.2.a エンドユーザメッセージングテクノロジを使用してカード会員データを送信する場合は、PAN を送信するプロセスを観察し、送信内容のサンプルを調査して、PAN を読み取り不能にするか、強力な暗号化で保護していることを確認する。</p>	<p>電子メール、インスタントメッセージング、SMS、チャットは、内部および公共ネットワーク上の配信中にパケットスニッフィングによって容易に傍受することができます。強力な暗号化を</p>

PCI DSS 要件	テスト手順	ガイダンス
	<p>4.2.b 文書化されているポリシーを調べ、保護されていない PAN がエンドユーザメッセージングテクノロジを介して送信されないことを記したポリシーの存在を確認する。</p>	<p>提供する構成になっている場合を除き、これらのメッセージングツールを利用して PAN を送信してはいけません。</p> <p>追加の情報として、企業がエンドユーザメッセージング技術を介して PAN を要求する場合、伝送前に強力な暗号化または読み取り不能な状態に変換するような PAN を保護するためのツールや手法を提供するべきです。</p>
4.3 カード会員データの伝送を暗号化するためのセキュリティポリシーと操作手順が文書化されて使用されており、影響を受ける関係者全員に知られていることを、確実にする。	<p>4.3 文書を調べ、関係者をインタビューすることで、カード会員データの伝送を暗号化するためのセキュリティポリシーと操作手順が以下の要件を満たしていることを確認する。</p> <ul style="list-style-type: none"> • 文書化されている • 使用されている • 影響を受ける関係者全員に知らされている 	<p>カード会員データの安全な伝送の継続的な管理を行うために、関係者はセキュリティポリシーと操作手順を認識・順守する必要があります。</p>

脆弱性管理プログラムの維持

要件 5: すべてのシステムをマルウェアから保護し、ウイルス対策ソフトウェアまたはプログラムを定期的に更新する

一般に「マルウェア」と呼ばれる悪意のあるソフトウェア（ウイルス、ワーム、トロイの木馬など）は、従業員の電子メール、インターネット、モバイルコンピュータ、ストレージデバイスの使用など、業務上承認された活動を通じて、システムの脆弱性を利用してネットワークに侵入します。マルウェアの影響を受けやすいすべてのシステムで、ウイルス対策ソフトウェアを使用して、最新の進化する悪意のあるソフトウェアの脅威からシステムを保護する必要があります。追加のウイルス対策ソリューションの使用をウイルス対策ソフトウェアの補助として考慮することはできますが、このようなウイルス対策ソリューションで、必要なウイルス対策ソフトウェア実装の必要性を置き換えるものではありません。

PCI DSS 要件	テスト手順	ガイダンス
5.1 悪意のあるソフトウェアの影響を受けやすいすべてのシステム（特にパーソナルコンピュータとサーバ）に、ウイルス対策ソフトウェアを導入する。	5.1 悪意のあるソフトウェアの影響を受けやすいすべてのオペーレーティングシステムタイプを含む、システムコンポーネントのサンプルについて、適用可能なウイルス対策テクノロジが存在する場合は、ウイルス対策ソフトウェアが導入されていることを確認する。	広く報道されているセキュリティ上の弱点を使った「0 day」（これまでに知られていなかった脆弱性を狙った攻撃）と呼ばれる、それ以外の攻撃に対しては安全なシステムを狙う攻撃が次々に出現しています。定期的にウイルス対策ソフトウェアを更新しないと、これらの新しい形式の悪意あるソフトウェアにより、ネットワークが攻撃され、使用できなくなる恐れがあります。
5.1.1 ウイルス対策プログラムが、既知の悪意のあるソフトウェアの全タイプに対して、検出、削除、保護が可能であることを、確実にする。	5.1.1 ベンダ文書を読み、ウイルス対策構成を調べて、ウイルス対策プログラムが以下を行うことを確認する <ul style="list-style-type: none"> 既知の悪意のあるソフトウェアの全タイプを検出する。 既知の悪意のあるソフトウェアの全タイプを削除する。 既知の悪意のあるソフトウェアの全タイプから保護する。 例として、ウイルス、トロイの木馬、ワーム、スパイウェア、アドウェア、ルートキットなどがあります。	すべての種類および形式の、悪意のあるソフトウェアから保護することが重要です。
5.1.2 一般的に悪意のあるソフトウェアに影響されないと見なされているシステムでは、定期的に評価を行って、進化を続けるマルウェアの脅威を特定して評価することで、システムにウイルス対策ソフトウェアが依然として必要ないかどうか	5.1.2 担当者をインタビューすることで、システムにウイルス対策ソフトウェアが依然として必要ないかどうかを判断するために、進化を続けるマルウェアの脅威の、一般的に悪意のあるソフトウェアに影響されないと見なされているシステムに対する影響が監視されていることを確認する。	現在では、通常、メインフレーム、ミッドレンジコンピュータ（AS/400など）、その他の類似システムは、マルウェアに狙われたり、侵害されることはありません。しかしながら、悪意のあるソフトウェアの傾向は急変する可能性があるため、組織は自社のシステムを侵害する可能性のある新

PCI DSS 要件	テスト手順	ガイダンス
を判断する		しいマルウェアについて常に警戒していることが重要です。これには、例えばベンダセキュリティ通知やウイルス対策ニュースグループの動きを継続的に監視し、自社のシステムが新しいマルウェアや進化を続ける脅威の影響を受けるか判断することなどが可能です。 悪意のあるソフトウェアの傾向を、新しいセキュリティの脆弱性の識別に含め、必要に応じて、新しい傾向への対応方法を企業の構成基準および保護メカニズムに組み込む必要があります。
5.2 すべてのウイルス対策メカニズムが以下のように維持されていることを確実にする。 <ul style="list-style-type: none">• 最新の状態である• 定期的にスキャンを行う• PCI DSS 要件 10.7 に従って監査ログを生成・保持する	<p>5.2.a ポリシーと手順を調べて、ウイルス対策ソフトウェアおよび定義を最新状態に保つことが要求されていることを確認する。</p> <p>5.2.b ソフトウェアのマスタインストールを含め、ウイルス対策構成を調べることで、ウイルス対策メカニズムが以下を満たすことを確認する。</p> <ul style="list-style-type: none">• 自動更新を行うように構成されている• 定期的にスキャンを行うように構成されている <p>5.2.c 悪意のあるソフトウェアの影響を受けやすいすべてのオペレーティングシステムタイプを含む、システムコンポーネントのサンプルについて、以下を確認する。</p> <ul style="list-style-type: none">• ウイルス対策ソフトウェアと定義が最新である。• 定期的なスキャンが実行される。 <p>5.2.d ソフトウェアのマスタインストールを含め、ウイルス対策構成を調べることで、ウイルス対策メカニズムが以下を満たすことを確認する。</p> <ul style="list-style-type: none">• ウイルス対策ソフトウェアログの生成が有効になっている• ログが PCI DSS 要件 10.7 に従って保持されている	どのように優れたウイルス対策ソリューションでも、最新のセキュリティ更新、署名ファイル、マルウェアからの保護に合わせて保守管理されていないと、その効果は制限されます。 監査ログで、ウイルスやマルウェアの活動とアンチマルウェアの対応を監視することができます。監査ログを生成するようにアンチマルウェアソフトウェアを構成し、ログを要件 10 に従って管理することが不可欠です。
5.3 ウイルス対策メカニズムがアクティブに実行されており、経営管理者からケースバイケースで期間を限って特別に許可されない限り、ユーザが無効にしたり変更でき	<p>5.3.a ソフトウェアのマスタインストールとシステムコンポーネントのサンプルを含め、ウイルス対策構成を調べることで、ウイルス対策ソフトウェアがアクティブに実行されていることを確認する。</p>	連続的に実行され、変更できないウイルス対策は、マルウェアに対する持続的なセキュリティを提供します。

PCI DSS 要件	テスト手順	ガイダンス
<p>ないことを、確実にする。</p> <p>注:ウイルス対策ソリューションは、ケースバイケースで経営管理者により許可されたことを前提に、正当な技術上のニーズがある場合に限り、一時的に無効にすることができます。特定の目的でアンチウイルス保護を無効にする必要がある場合、正式な許可を得る必要があります。アンチウイルス保護が無効になっている間、追加のセキュリティ手段が必要になる場合があります。</p>	<p>5.3.b ソフトウェアのマストインストールとシステムコンポーネントのサンプルを含め、ウイルス対策構成を調べることで、ウイルス対策ソフトウェアがユーザによって無効化・変更できないことを確認する。</p> <p>5.3.c 責任者をインタビューし、プロセスを観察することで、ウイルス対策ソフトウェアは、経営管理者からケースバイケースで期間を限って特別に許可されない限り、ユーザが無効化・変更できることを確認する。</p>	<p>すべてのシステムでポリシーベースの制御を使用してアンチマルウェア保護の変更や無効化ができないことは、システムの弱点から悪意のあるソフトウェアが侵害するのを防ぐのに役立ちます。</p> <p>ウイルス対策保護が無効になっている間、例えば、ウイルス対策が無効になったときにインターネットから非保護のシステムを切り離して、再び有効にした後フルスキャンを実行するなど、追加のセキュリティ手段が必要になる場合があります。</p>
<p>5.4 マルウェアからシステムを保護するためのセキュリティポリシーと操作手順が文書化されて使用されており、影響を受ける関係者全員に知られていることを、確実にする。</p>	<p>5.4 文書を調べ、関係者をインタビューすることで、マルウェアからシステムを保護するためのセキュリティポリシーと操作手順が以下の要件を満たしていることを確認する。</p> <ul style="list-style-type: none"> • 文書化されている • 使用されている • 影響を受ける関係者全員に知らされている 	<p>システムが継続的にマルウェアから保護されるようにするために、関係者はセキュリティポリシーと操作手順を認識・順守する必要があります。</p>

要件 6: 安全性の高いシステムとアプリケーションを開発し、保守する

悪意のある者は、セキュリティの脆弱性を利用して、システムへの特権アクセスを取得します。このような脆弱性の多くは、ベンダが提供するセキュリティパッチによって修正されます。システムを管理する事業体はこうしたパッチをインストールする必要があります。すべてのシステムは、適切なソフトウェアパッチを適用することにより、悪意のある者および不正なソフトウェアによるカード会員データの不正使用および侵害から保護される必要があります。

注:適切なソフトウェアパッチとは、既存のセキュリティ構成と競合しないことが十分に評価およびテストされたパッチを指します。自社開発アプリケーションの場合、標準のシステム開発プロセスと安全なコーディング技術を使用することで、多くの脆弱性を回避できます。

PCI DSS 要件	テスト手順	ガイダンス
<p>6.1 セキュリティ脆弱性情報の信頼できる社外提供元を使ってセキュリティの脆弱性を特定し、新たに発見されたセキュリティの脆弱性にリスクのランク（「高」、「中」、「低」など）を割り当てるプロセスを確立する。</p> <p>注: リスクのランク分けは、業界のベストプラクティスおよび考えられる影響の程度に基づいています。例えば、脆弱性をランク分けする基準は、CVSS ベーススコア、ベンダによる分類、影響を受けるシステムの種類の考察などを含む場合があります。</p> <p>脆弱性を評価し、リスクのランクを割り当てる方法は、組織の環境とリスク評価戦略によって異なります。リスクのランクは、最小限、環境に対する「高リスク」と見なされるすべての脆弱性を特定するものである必要があります。リスクのランク分けに加えて、環境に対する差し迫った脅威をもたらす、重要システムに影響を及ぼす、対処しないと侵害される危険がある場合、脆弱性は「重大」と見なされます。重要システムの例としては、セキュリティシステム、一般公開のデバイスやシステム、データベース、およびカード会員データを保存、処理、送信するシステムなどがあります。</p>	<p>6.1.a ポリシーと手順を調べ、以下のプロセスが定義されていることを確認する。</p> <ul style="list-style-type: none"> • 新しいセキュリティの脆弱性の識別 • すべての「高リスク」と「重大」な脆弱性の識別を含む脆弱性のランク分けの割り当て • セキュリティ脆弱性情報の信頼できる外部情報源の使用 <p>6.1.b 担当者をインタビューするかプロセスを観察して、以下を確認する。</p> <ul style="list-style-type: none"> • 新しいセキュリティの脆弱性が識別されている • すべての「高リスク」と「重大」な脆弱性の識別を含む脆弱性のランク分けが割り当てられている • 新しいセキュリティの脆弱性を特定するプロセスに、セキュリティ脆弱性情報を得るための外部情報源の使用が含まれている 	<p>この要件の目的は、組織の環境に影響を及ぼす可能性がある新しい脆弱性に関する情報を最新状態に保つことです。</p> <p>脆弱性情報の情報源は信頼できるものでなければならず、ベンダの Web サイト、業界ニュースグループ、メーリングリスト、RSS フィードなどがあります。</p> <p>組織の環境に影響を及ぼす可能性がある脆弱性を特定したら、その脆弱性のリスクを評価およびランク分けする必要があります。このため、組織が継続的に脆弱性を評価し、リスクをランク分けするための方法を設ける必要があります。これは、ASV スキャンや内部脆弱性スキャンによっては達成できず、脆弱性情報の業界情報源をアクティブに監視するプロセスを必要とします。</p> <p>リスクの分類（「高」、「中」、「低」など）により、組織は優先順位のもっとも高いリスク項目をより迅速に特定して対処し、もっともリスクが高い脆弱性を利用される可能性を低下させることができます。</p>

PCI DSS 要件	テスト手順	ガイダンス
<p>6.2 すべてのシステムコンポーネントとソフトウェアに、ベンダ提供のセキュリティパッチがインストールされ、既知の脆弱性から保護されている。重要なセキュリティパッチは、リリース後 1 カ月以内にインストールする。</p> <p>注:要件 6.1 で定義されているリスクのランク分けプロセスに従って、重要なセキュリティパッチを識別する必要があります。</p>	<p>6.2.a セキュリティパッチのインストールに関連したポリシーと手順を調べて、以下のプロセスが定義されていることを確認する。</p> <ul style="list-style-type: none"> 該当する、ベンダ提供の重要セキュリティパッチは、リリース後 1 カ月以内にインストールする。 該当する、ベンダ提供のセキュリティパッチをすべて、適切な時間枠内（3 カ月以内など）にインストールする。 <p>6.2.b システムコンポーネントおよび関連ソフトウェアのサンプルについて、各システムにインストールされたセキュリティパッチのリストと、ベンダの最新のセキュリティパッチのリストを比較して、以下を確認する。</p> <ul style="list-style-type: none"> 該当する、ベンダ提供の重要セキュリティパッチは、リリース後 1 カ月以内にインストールする。 該当するすべてのベンダが提供するセキュリティパッチは、適切な時間枠（例えば 3 カ月以内）内にインストールされている。 	<p>広く報道されているセキュリティ上の弱点を使った「0 day」（これまでに知られていなかった脆弱性を狙った攻撃）と呼ばれる、それ以外の攻撃に対しては安全なシステムを狙う攻撃が次々に出現しています。可能な限り迅速に重要なシステムに最新のパッチを実装しないと、悪意のある者によりこれらの弱点が使用され、ネットワークが攻撃されて使用不可になる可能性があります。</p> <p>重要なインフラ用のパッチを優先することで、高優先度のシステムとデバイスは、<u>パッチがリリースされ次第脆弱性から保護されるようになります</u>。重要なシステムまたは危険な状態にあるシステムへのセキュリティパッチを 30 日以内にインストールされ、その他の危険度の低いパッチは 2 ~ 3 カ月内にインストールするよう、パッチのインストールに優先順位を付けることを検討してください。</p> <p>この要件は、インストールされているペイメントアプリケーション（PA-DSS 検証済み、未検証の両方）を含む、すべてのソフトウェアの該当するパッチに適用されます。</p>
<p>6.3 内部および外部ソフトウェアアプリケーション（アプリケーションへの Web ベースの管理アクセスを含む）を次のように開発する。</p> <ul style="list-style-type: none"> PCI DSS（安全な認証やロギングなど）に従って。 業界基準やベストプラクティスに基づいて。 ソフトウェア開発ライフサイクル全体に情報セキュリティを組み込む。 <p>注: これは、社内開発ソフトウェアすべて、および第三者によって開発されたカスタムソフトウェアにも当てはまります。</p>	<p>6.3.a 文書化されたソフトウェア開発プロセスを調べて、プロセスが業界標準またはベストプラクティス（あるいはその両方）に基づいていることを確認する。</p> <p>6.3.b 記述されたソフトウェア開発プロセスを検査し、ライフサイクル全体に情報セキュリティが組み込まれていることを確認する。</p> <p>6.3.c 記述されたソフトウェア開発プロセスを検査し、PCI DSS に従って、ソフトウェアアプリケーションが開発されていることを確認する。</p> <p>6.3.d ソフトウェア開発者のインタビューから、文書化されたソフトウェア開発プロセスが実装されていることを確認する。</p>	<p>ソフトウェア開発の要件定義、設計、分析、およびテスト段階にセキュリティを含めないと、セキュリティの脆弱性が過失または故意によって本番環境にもたらされる可能性があります。</p>

PCI DSS 要件	テスト手順	ガイダンス
<p>6.3.1 アプリケーションがアクティブになる前、または顧客にリリースされる前に、テスト/カスタムアプリケーションアカウント、ユーザ ID、パスワードを削除する</p>	<p>6.3.1 文書化されたソフトウェア開発手順を調べ、責任者をインタビューすることで、本番前テスト/カスタムアプリケーションアカウント、ユーザ ID/パスワードが、システムが本番環境に導入される、または顧客にリリースされる前に削除されることを確認する。</p>	<p>開発、テスト/カスタムアプリケーションアカウント、ユーザ ID、パスワードは、アプリケーションがアクティブになる前、または顧客にリリースされる前に本番環境コードから削除する必要があります。これらのアイテムは、アプリケーションの機能に関する情報を漏洩する場合があるためです。このような情報を保持していると、アプリケーションおよび関連するカード会員データの侵害を容易にする可能性があります。</p>
<p>6.3.2 コーディングの潜在的な脆弱性を識別するために、本番または顧客にリリースする前に、（手動または自動化されたプロセスのいずれかを使用して）カスタムコードをレビューする。少なくとも以下を含む。</p> <ul style="list-style-type: none"> ■ コード変更は、コード作成者以外の、コードレビュー手法と安全なコーディング手法の知識のある人がレビューする。 ■ コードレビューにより、コードが安全なコーディングガイドラインに従って開発されたことが保証される 	<p>6.3.2.a 文書化されたソフトウェア開発手順を調べ、責任者をインタビューすることで、すべてのカスタムアプリケーションコードの変更は、次のように（手動または自動化されたプロセスのいずれかを使用して）レビューする必要があることを確認する。</p> <ul style="list-style-type: none"> ■ コード変更は、コード作成者以外の、コードレビュー手法と安全なコーディング手法の知識のある人がレビューする。 ■ コードレビューにより、コードが安全なコーディングガイドラインに従って開発されたことが保証される（PCI DSS 要件 6.5 を参照）。 ■ リリース前に、適切な修正を実装している。 ■ コードレビュー結果は、リリース前に管理職によってレビューおよび承認される。 	<p>カスタムコードのセキュリティの脆弱性は、悪意のある者によってネットワークにアクセスし、カード会員データを侵害するために一般的に悪用されます。</p> <p>コードレビュー技術の知識と経験のある人がレビューのプロセスに関与する必要があります。コードレビューをコードの開発者以外の担当者に割り当てるにより、独立した客観的なレビューを実施できます。手動レビューの代わりに自動ツールやプロセスを使用することができますが、自動ツールがコーディング上の問題を特定することは困難あるいは不可能な場合があります。</p> <p>コードが本番環境に導入される、または顧客にリリースされる前にコードエラーを訂正すること</p>

PCI DSS 要件	テスト手順	ガイダンス
<ul style="list-style-type: none"> ▪ リリース前に、適切な修正を実装している。 ▪ コードレビュー結果は、リリース前に管理職によってレビューおよび承認される。 <p>注:このコードレビュー要件は、システム開発ライフサイクルの一環として、すべてのカスタムコード（内部および公開）に適用される。</p> <p>コードレビューは、知識を持つ社内担当者または第三者が実施できる。一般に公開されている Web アプリケーションは、実装後の脅威および脆弱性に対処するために、PCI DSS 要件 6.6 に定義されている追加コントロールの対象となる。</p> <p>6.4 システムコンポーネントへのすべての変更において、変更管理のプロセスおよび手順に従う。これらのプロセスには、以下を含める必要がある。</p>	<p>6.3.2.b 最近のカスタムアプリケーションの変更についてサンプルを選択し、そのカスタムアプリケーションコードが上記 6.3.2.a に従ってレビューされていることを確認する。</p>	<p>で、コードが環境を潜在的な侵害にさらすことを防止できます。コードエラーは、本番環境に導入またはリリースした後に対処する場合、その前に比べてずっと難しく、高価な代償を支払う結果になります。</p> <p>リリース前に経営管理者の正式なレビューと承認を含めることにより、コードが承認され、ポリシーと手順に従って開発されていることが確認できます。</p>
<p>6.4.1 開発/テスト環境を本番環境から分離し、分離を実施するためのアクセス制御を行う。</p>	<p>6.4 ポリシーと手順を調べ、以下が定義されていることを確認する。</p> <ul style="list-style-type: none"> • 開発/テスト環境が、本番環境から分離されていて、分離を実施するためのアクセス制御が行われていること • 開発/テスト環境に割り当てられている担当者と本番環境に割り当てられている担当者との間で責務が分離されていること • テストまたは開発に本番環境データ（実際の PAN）を使用しないこと。 • 本番環境システムがアクティブになる前にテストデータとテストアカウントが削除されること • セキュリティパッチやソフトウェアの変更の実装に関する変更管理手順が文書化されていること <p>6.4.1.a ネットワーク文書とネットワークデバイス構成を調べて、開発/テスト環境が本番環境から分離されていることを確認する。</p> <p>6.4.1.b アクセス制御設定を調べて、開発/テスト環境と本番環境の分離を強制するためのアクセス制御が行われていることを確認する。</p>	<p>適切に文書化されて実施されている変更管理がないと、セキュリティ機能が過失または故意によって省略あるいは動作不能にされたり、処理の不規則性が発生したり、悪意のあるコードが取り込まれる可能性があります。</p>

PCI DSS 要件	テスト手順	ガイダンス
6.4.2 開発/テスト環境と本番環境での責務の分離	6.4.2 プロセスを観察し、開発/テスト環境に割り当てられている担当者と本番環境に割り当てられている担当者をインタビューすることで、開発/テスト環境と本番環境の責務が分離されていることを確認する。	本番環境およびカード会員データにアクセスできる担当者の数を少なくすることにより、リスクは最小限に抑えられ、アクセスは業務上必要とするユーザのみに制限できます。 この要件の目的は、開発/テスト機能を本番機能から確実に分離することです。例えば、開発者は、開発環境では権限を昇格して管理者レベルのアカウントを使用し、本番環境では別のユーザレベルアカウントでアクセスするという方法があります。
6.4.3 テストまたは開発に本番環境データ（実際の PAN）を使用しない	6.4.3.a テストプロセスを観察し、担当者をインタビューすることで、本番環境データ（実際の PAN）がテストまたは開発に使用されていないことを確認する。	セキュリティコントロールは、通常、開発環境ではそれほど厳しくありません。本番環境データを使用すると、悪意のある者に本番環境データ（カード会員データ）に不正にアクセスする機会を与えることになります。
	6.4.3.b テストデータのサンプルを観察して、本番環境データ（実際の PAN）がテストまたは開発に使用されていないことを確認する。	
6.4.4 テストデータとテストアカウントは、システムがアクティブになる前、または本番稼働の前にシステムコンポーネントから削除する	6.4.4.a テストプロセスを観察し、担当者をインタビューすることで、本番環境システムがアクティブになる前にテストデータとアカウントが削除されることを確認する。 6.4.4.b 最近インストールされたか更新された本番システムからのデータとアカウントのサンプルを調べて、本番環境システムがアクティブになる前にテストデータとアカウントが削除されることを確認する。	アプリケーションまたはシステムの機能に関する情報漏洩を防止するために、テストデータおよびテストアカウントをシステムコンポーネントがアクティブになる（本番稼働）前に削除する必要があります。これらのアイテムは、アプリケーションまたはシステムの機能に関する情報を漏洩する場合があるためです。このような情報を保持していると、システムおよび関連するカード会員データの侵害を容易にする可能性があります。

PCI DSS 要件	テスト手順	ガイダンス
6.4.5 変更管理手順は以下を含む必要がある。	<p>6.4.5.a 文書化された変更管理手順を調べて、以下の手順が定義されていることを確認する。</p> <ul style="list-style-type: none"> • 影響の文書化 • 適切な権限を持つ関係者による文書化された変更承認。 • 変更がシステムのセキュリティに悪影響を与えていないことを確認するための機能テスト • 回復手順 <p>6.4.5.b システムコンポーネントのサンプルについて、責任者をインタビューすることで、最新の変更を確認する。それらの変更内容に関する変更管理文書を確認する。確認した変更内容について、以下を実行する。</p>	適切な変更管理が実施されないと、ハードウェアまたはソフトウェアの更新とセキュリティパッチのインストールなどのシステム変更完全に実施されず、意図しない結果を招く可能性があります。
6.4.5.1 影響の文書化。	6.4.5.1 サンプリングした変更で、影響の文書化が変更管理文書に含まれていることを確認する。	変更の影響を文書化して、影響を受けるすべての関係者が処理の変更に対して適切に計画できるようにする必要があります。
6.4.5.2 適切な権限を持つ関係者による文書化された変更承認。	6.4.5.2 サンプリングした変更で、適切な権限を持つ関係者による文書化された変更承認が存在していることを確認する。	適切な権限を持つ関係者による承認は、変更が組織によって許可された正当な承認済みの変更であることを示します。
6.4.5.3 変更がシステムのセキュリティに悪影響を与えないことを確認するための機能テスト。	<p>6.4.5.3.a サンプリングした各変更で、変更がシステムのセキュリティに悪影響を与えないことを確認するため、機能テストが実施されたことを確認する。</p> <p>6.4.5.3.b カスタムコードの変更では、すべての更新を本番環境に導入する前に、PCI DSS の要件 6.5 に従って準拠がテストされていることを確認する。</p>	徹底的なテストを実施して、変更の実装によって環境のセキュリティが低下しないことを確認する必要があります。テストでは、環境の変更後に、すべての既存のセキュリティコントロールが元どおりに保たれ、同等の強力なコントロールに置き換えられているか、強化されていることを検証する必要があります。
6.4.5.4 回復手順。	6.4.5.4 サンプリングした各変更で、回復手順が準備されていることを確認する。	変更ごとに、変更が失敗したか、アプリケーションまたはシステムに悪影響を及ぼした場合に以前の状態に復元するための回復手順が存在する必要があります。

PCI DSS 要件	テスト手順	ガイダンス
<p>6.4.6 大幅な変更の完了時、すべての関連する PCI DSS 要件が新規または変更されたシステムおよびネットワークに実装され、該当する場合は文書が更新される必要がある。</p>	<p>6.4.6 大幅な変更のサンプルについて、変更履歴を検査し、担当者をインタビュー、および影響を受けたシステム/ネットワークを観察することで、適切な PCI DSS 要件が実装され、変更箇所に応じて文書が更新されていることを確認する。</p>	<p>大幅な変更を分析するためのプロセスは、対象範囲内の追加または変更されたすべてのシステムに PCI DSS コントロールを確実に適用するために役立ちます。</p> <p>この変更管理プロセス内にこの検証を構築することで、デバイスインベントリおよび構成基準が最新化され、必要に応じてセキュリティ対策が適用されることを確実にするために役立ちます。</p> <p>変更管理プロセスは、PCI DSS 要件が実装されている証拠、または反復プロセスを通じて維持されていることを裏付ける証拠を含める必要があります。PCI DSS 要件に影響を与える例としては以下を含みますが、これらに限りません：</p> <ul style="list-style-type: none"> 変更を反映するためのネットワーク図の更新 システムが各構成基準に従って構成され、すべてのデフォルトパスワードを変更および不要なサービスを無効化する 必要な対策によりシステムが保護されている - 例、ファイル整合性監視 (FIM)、アンチウイルス、パッチ、監査ログ。 機密認証データ (SAD) は保存せず、すべてのカード会員データ (CHD) 保管場所が文書化され、データ保管ポリシーと手順に組み込まれている 新しいシステムが四半期ごとの脆弱性スキャンプロセスの対象に含まれる
<p>6.5 ソフトウェア開発プロセスにおいて次のようにして一般的なコーディングの脆弱性に対応する。</p> <ul style="list-style-type: none"> 開発者に対して一般的なコーディングの脆弱性を回避する方法を含む安全なコーディング技法について少なくとも年1回のトレーニングを実施する。 	<p>6.5.a ソフトウェア開発ポリシーと手順を調べ、業界のベストプラクティスとガイダンスに基づき、少なくとも年に一度開発者のための安全なコーディング技法について最新のトレーニングを要求していることを確認する。</p> <p>6.5.b トレーニング記録を調べて、少なくとも年に一度ソフトウェア開発者が、一般的なコーディングの脆弱性を避けることを含め、安全なコーディング技法についての最新のトレーニングを受けたことを確認する。</p>	<p>アプリケーション層はリスクが高く、内部と外部の両方の脅威の標的となる可能性があります。</p> <p>要件 6.5.1 ~ 6.5.10 は必要最小限の制御であり、組織は環境内の個々のテクノロジに適用可能な適切で安全なコーディング手法を採用する必要があります。</p> <p>アプリケーション開発者は、これら（および他の）一般的なコードの脆弱性に関する問題を識別</p>

PCI DSS 要件	テスト手順	ガイダンス
<p>くとも年に一度トレーニングを実施する</p> <ul style="list-style-type: none"> 安全なコーディングガイドラインに基づいてアプリケーションを開発する <p>注:要件 6.5.1～6.5.10 にあげられている脆弱性は、このバージョンの PCI DSS が発行された時点の最新の業界ベストプラクティスを踏襲しているが、しかし、脆弱性管理のための業界のベストプラクティスは更新されているため (OWASP ガイド、SANS CWE Top 25、CERT Secure Coding など)、現在のベストプラクティスは、これらの要件を使用する必要がある。</p>	<p>6.5.c アプリケーションを少なくとも以下の脆弱性から保護するためのプロセスが存在することを確認する。</p>	<p>して解決するための適切なトレーニングを受ける必要があります。安全なコーディングガイドラインの知識を持つスタッフを有することにより、稚拙なコーディング方法によりもたらされるセキュリティの脆弱性を最小限に抑えることができます。開発者のトレーニングは、社内で行うことも第三者によって行うこともでき、使用テクノロジに該当するものでなければなりません。</p> <p>業界で認知された安全なコーディング手法が変化した場合は、メモリのスクレーピング攻撃などの新しい脅威に対応するため、組織のコーディング手法および開発者のトレーニングを更新する必要があります。6.5.1 から 6.5.10 で指定される脆弱性は、最低限のベースラインを示します。最新の脆弱性の傾向に精通し、コーディングの実践に適切な対策を組み入れることは組織の責任です。</p>
<p>注:以下の要件 6.5.1 から 6.5.6 は、すべてのアプリケーション（内部または外部）に適用されます。</p> <p>6.5.1 インジェクションの不具合（特に SQL インジェクション）。OS コマンドインジェクション、LDAP および Xpath のインジェクションの不具合、その他のインジェクションの不具合も考慮する。</p>	<p>6.5.1 ソフトウェア開発ポリシーと手順を調べ、責任者をインタビューすることで、以下を含め、コーディング技法によってインジェクションの不具合が対処されていることを確認する。</p> <ul style="list-style-type: none"> 入力を調べて、ユーザデータがコマンドとクエリの意味を変更できないことを確認する パラメータ化クエリを使用する 	<p>インジェクションの不具合（特に SQL インジェクション）は、アプリケーションの侵害に使用される一般的な方法です。インジェクションは、ユーザ入力データがコマンドまたはクエリの一部としてインタプリタに送信されるときに発生します。攻撃者の悪意をもったデータはインタプリタに意図しないコマンドを実行したりデータを変更したりするよう仕向けて、攻撃者が、アプリケーションを通じてネットワーク内部のコンポーネントを攻撃したり、バッファオーバーフローなどの攻撃を開始したり、機密情報とサーバアプリケーション機能の両方を露出させたりすることを可能にします。</p> <p>情報は、アプリケーションに送信する前に、すべての英字、英字と数字の混合をチェックするなどして検証する必要があります。</p>

PCI DSS 要件	テスト手順	ガイダンス
6.5.2 バッファオーバーフロー	<p>6.5.2 ソフトウェア開発ポリシーと手順を調べ、責任者をインタビューすることで、以下を含め、コーディング技法によってバッファオーバーフローが対処されていることを確認する。</p> <ul style="list-style-type: none"> • バッファ境界を検証する • 入力文字列をトランケーションする 	バッファオーバーフローは、アプリケーションにバッファ領域での適切なバインドチェック機能がない場合に発生します。これにより、バッファ内の情報がバッファのメモリ領域から押し出され、実行可能メモリ領域に移動する可能性があります。その場合、攻撃者は悪意のあるコードをバッファの最後に挿入し、バッファをオーバーフローさせることによって、そのコードを実行可能メモリ領域に押し出すことができます。この方法で悪意のあるコードが実行され、多くの場合、攻撃者はアプリケーションや感染したシステムにリモートアクセスできます。
6.5.3 安全でない暗号化保存	<p>6.5.3 ソフトウェア開発ポリシーと手順を調べ、責任者をインタビューすることで、以下を含め、コーディング技法によって安全でない暗号化保存が対処されていることを確認する。</p> <ul style="list-style-type: none"> • 暗号化の不具合を防止する • 強力な暗号化アルゴリズムと鍵を使用する 	データの保存に強力な暗号化機能を適切に利用していないアプリケーションは、侵害されて認証情報やカード会員データが漏洩するリスクが高くなります。攻撃者が脆弱な暗号化プロセスを利用して、暗号化されたデータに平文アクセスすることも可能になります。
6.5.4 安全でない通信	<p>6.5.4 ソフトウェア開発ポリシーと手順を調べ、責任者をインタビューすることで、安全でない通信がすべての機密情報の通信を適切に認証して暗号化するコーディング技法によって対処されていることを確認する</p>	ネットワークトラフィックを強力な暗号化によって適切に暗号化していないアプリケーションは、侵害されてカード会員データが漏洩するリスクが高くなります。攻撃者が弱い暗号化プロセスを利用して、アプリケーションを制御したり、暗号化されたデータに平文アクセスすることも可能になります。

PCI DSS 要件	テスト手順	ガイダンス
6.5.5 不適切なエラー処理	6.5.5 ソフトウェア開発ポリシーと手順を調べ、責任者をインタビューすることで、不適切なエラー処理が、エラーメッセージを通して情報を漏洩しないコーディング技法によって対処されていることを確認する（例えば、具体的なエラー情報ではなく汎用エラーメッセージを返すなど）	アプリケーションは、不適切なエラー処理方法によって構成、内部動作、特権情報に関する情報を意図せずに漏洩したり、プライバシーを侵害したりする可能性があります。攻撃者は、この弱点を利用して、機密データを盗んだり、システムを侵害したりします。悪意のある者は、アプリケーションが正しく処理しないエラーを作成して、詳細なシステム情報を取得したり、サービス拒否割り込みを作成したり、セキュリティを失敗させたり、サーバをクラッシュさせたりすることができます。例えば、「提供されたパスワードが正しくありません」というメッセージは、提供されたユーザ ID は正確であり、パスワードにのみ焦点を合わせればよいことを攻撃者に伝えてしまします。「データを確認できませんでした」など、より汎用的なエラーメッセージを使用します。
6.5.6 脆弱性特定プロセス（PCI DSS 要件 6.1 で定義）で特定された、すべての「高リスク」脆弱性。	6.5.6 ソフトウェア開発ポリシーと手順を調べ、責任者をインタビューすることで、コーディング技法により、アプリケーションを侵害する可能性のある、PCI DSS 要件 6.1 で特定されたすべての「高リスク」脆弱性に対処する。	組織の脆弱性リスクのランク分けプロセス（要件 6.1 で定義）で「高リスク」に特定され、アプリケーションを侵害する可能性があるすべての脆弱性は、アプリケーション開発中に特定・対処する必要がある。
注: 以下の要件 6.5.7～6.5.10 は、Web アプリケーションとアプリケーションインターフェース（内部または外部）に適用されます。		内部および外部（公開）の Web アプリケーションにはアーキテクチャに応じて特有のセキュリティリスクがあり、侵害が比較的容易で発生しやすいという特徴があります。
6.5.7 クロスサイトスクリプティング（XSS）	6.5.7 ソフトウェア開発ポリシーと手順を調べ、責任者をインタビューすることで、以下を含め、コーディング技法によってクロスサイトスクリプティング（XSS）が対処されていることを確認する。 <ul style="list-style-type: none"> • 取り込む前にすべてのパラメータを検証 • コンテキスト依存エスケープの使用 	XSS の不具合は、アプリケーションがユーザ入力データを取り入れ、検証したりコンテンツをエンコードしたりする前に Web ブラウザに送信するたびに発生します。XSS により、攻撃者は、被害者のブラウザでスクリプトを実行して、ユーザセッションを乗っ取ったり、Web サイトを書き換えたり、ワームを取り込んだりすることができます。

PCI DSS 要件	テスト手順	ガイダンス
6.5.8 不適切なアクセス制御（安全でないオブジェクトの直接参照、URL アクセス制限の失敗、ディレクトリトランザクション、機能へのユーザアクセス制限の失敗など）	<p>6.5.8 ソフトウェア開発ポリシーと手順を調べ、責任者をインタビューすることで、不適切なアクセス制御（安全でないオブジェクトの直接参照、URL アクセス制限の失敗、ディレクトリトランザクション、機能へのユーザアクセス制限の失敗など）が以下を含むコーディング技法によって対処されていることを確認する。</p> <ul style="list-style-type: none"> ● ユーザの適切な認証 ● 入力値の削除 ● 内部オブジェクト参照をユーザに公開しない ● ユーザインターフェースで無許可の機能へのアクセスを許可しない 	<p>オブジェクトの直接参照は、開発者が内部実装オブジェクト（ファイル、ディレクトリ、データベースレコード、キーなど）を URL または form 形式) パラメータとして公開するときに発生します。攻撃者は、これらの参照を操作して、承認を受けずにその他のオブジェクトにアクセスできます。</p> <p>すべての URL に対してプレゼンテーション層とビジネスロジックでアクセス制御を一貫して実施します。多くの場合、アプリケーションが機密機能を保護する唯一の方法は、権限のないユーザにリンクまたは URL を表示しないことです。攻撃者は、この弱点を使用してアクセスし、これらの URL に直接アクセスすることで不正な操作を実行できます。</p> <p>攻撃者は Web サイトのディレクトリ構造（ディレクトリトランザクション）を列挙してナビゲートすることで、情報に不正アクセスし、後から攻撃するためにサイトの動作を詳細に調べることができます。</p> <p>ユーザインターフェースで無許可の機能へのアクセスが許可されると、このアクセスは無許可のユーザが特権情報やカード会員データにアクセスできるようになります。許可を持つユーザのみが機密リソースの直接オブジェクト参照へのアクセスを許可されるようになります。データリソースへのアクセスを制限することは、カード会員データが無許可のリソースに提示されることを防止するために役立ちます。</p>
6.5.9 クロスサイトリクエスト偽造 (CSRF)	<p>6.5.9 ソフトウェア開発ポリシーと手順を調べ、責任者をインタビューすることで、クロスサイトリクエスト偽造 (CSRF) は、アプリケーションがブラウザから自動的に送信された認証情報とトークンに依存しないコーディング技法によって対処されていることを確認する。</p>	<p>CSRF 攻撃は、ログオン済みの被害者のブラウザを使用して未認証の要求を脆弱な Web アプリケーションへ送信させ、攻撃者が被害者に実行が許可されているステート変更操作（アカウント情報の更新、購入、さらにはアプリケーションの認証などさえも）を行えるようにします。</p>

PCI DSS 要件	テスト手順	ガイダンス
6.5.10 不完全な認証管理とセッション管理	<p>6.5.10 ソフトウェア開発ポリシーと手順を調べ、責任者をインタビューすることで、以下を含め、コーディング技法によって不完全な認証管理とセッション管理が対処されていることを確認する。</p> <ul style="list-style-type: none"> • セッショントークン（クッキーなど）を「secure」としてフラグ付けする • URL にセッション ID を含めない • ログイン後の適切なタイムアウトとセッション ID の巡回 	安全な認証とセッション管理は、無許可ユーザによる合法的なアカウントの資格情報、鍵、またはセッショントークンの侵害を防止し、侵入者が許可されているユーザの ID を盗用できなくなる。

PCI DSS 要件	テスト手順	ガイダンス
<p>6.6 一般公開されている Web アプリケーションで、継続的に新たな脅威や脆弱性に対処し、これらのアプリケーションが、次のいずれかの方法によって、既知の攻撃から保護されていることを確実にする。</p> <ul style="list-style-type: none"> ▪ 一般公開されている Web アプリケーションは、アプリケーションのセキュリティ脆弱性を手動/自動で評価するツールまたは手法によって、少なくとも年 1 回および何らかの変更を加えた後にレビューする 注: この評価は、要件 11.2 で実施する脆弱性スキャンとは異なる。 ▪ Web ベースの攻撃を検知および回避するために、一般公開されている Web アプリケーションの手前に、Web ベースの攻撃を自動的に検出・防止する技術的な解決策 (Web アプリケーションファイアウォールなど) をインストールする。 	<p>6.6 一般公開されている Web アプリケーションについて、以下のいずれかの手法がとられていることを確認する。</p> <ul style="list-style-type: none"> ▪ 文書化されているプロセスを調べ、担当者をインタビューして、アプリケーションセキュリティ評価記録を見ることで、一般公開されている Web アプリケーションが (セキュリティ脆弱性を手動/自動で評価するツールまたは手法を使用して) 以下のようにレビューされていることを確認する。 <ul style="list-style-type: none"> - 少なくとも年に一度実施する - 何らかの変更を加えた後 - アプリケーションのセキュリティを専門とする組織によって - 評価に少なくとも要件 6.5 に記載されている脆弱性を含める - 脆弱性がすべて修正されている - 修正後、アプリケーションが再評価されている ▪ システム構成設定を調べ、責任者をインタビューすることで、Web ベースの攻撃を自動的に検出・防止する技術的な解決策 (Web アプリケーションファイアウォールなど) が以下のとおり備わっていることを確認する。 <ul style="list-style-type: none"> - Web ベースの攻撃を検知および防止するために、一般公開されている Web アプリケーションの手前にインストールされている - アクティブに実行されており、最新状態である (該当する場合) - 監査ログを生成する - 即時調査可能にするために Web ベースの攻撃をブロックするか、アラートを生成する 	<p>一般公開 Web アプリケーションは攻撃者の主要ターゲットで、拙いコーディングの Web アプリケーションは攻撃者が機密データやシステムにアクセスできる容易な経路を提供することになります。アプリケーションのレビューまたは Web アプリケーションファイアウォールのインストールに関するこの要件の目的は、拙いコーディングやアプリケーション管理方法による一般公開されている Web アプリケーションへの侵害の数を削減することです。</p> <ul style="list-style-type: none"> ▪ アプリケーションの脆弱性をレビューまたはスキャンする手動/自動の脆弱性セキュリティ評価ツールまたは手法 ▪ Web アプリケーションファイアウォールは、アプリケーション層で不要なトラフィックをフィルタリングおよびブロックします。適切に構成された Web アプリケーションファイアウォールをネットワークベースのファイアウォールと組み合わせて使用することで、アプリケーションが正しくコーディングまたは構成されていない場合にアプリケーション層への攻撃が防止されます。これは、技術、プロセスの組み合わせによって達成ができる。プロセスベースのソリューションは、この攻撃を防ぐための要件の意図を満たすために、アラートへのタイムリーな対応を促進する仕組みをもっている必要があります。 <p>注: レビュー担当者がアプリケーションのセキュリティに精通していて、開発チームからの独立性を実証できる人物であれば、「アプリケーションのセキュリティを専門とする組織」は、第三者の企業でも内部組織でも構いません。</p>

PCI DSS 要件	テスト手順	ガイダンス
<p>6.7 安全性の高いシステムとアプリケーションを開発・保守するためのセキュリティポリシーと操作手順が文書化されて使用されており、影響を受ける関係者全員に知られていることを、確実にする。</p>	<p>6.7 文書を調べ、関係者をインタビューすることで、安全性の高いシステムとアプリケーションを開発・保守するためのセキュリティポリシーと操作手順が以下の要件を満たしていることを確認する。</p> <ul style="list-style-type: none"> • 文書化されている • 使用されている • 影響を受ける関係者全員に知らされている 	<p>システムとアプリケーションが安全に開発され、継続的に脆弱性から保護されるようするために、関係者はセキュリティポリシーと操作手順を認識・順守する必要があります。</p>

強力なアクセス制御手法の導入

要件 7: カード会員データへのアクセスを、業務上必要な範囲内に制限する

権限を与えられた担当者のみが重要なデータにアクセスできるように、システムおよびプロセスでは、職責に応じて必要な範囲にアクセスを制限する必要があります。

「必要な範囲」とは、アクセス権が職務の実行に必要な最小限のデータ量および特権にのみ付与されることを示します。

PCI DSS 要件	テスト手順	ガイダンス
7.1 システムコンポーネントとカード会員データへのアクセスを、業務上必要な人に限定する。	<p>7.1.a アクセス制御に関する文書化されたポリシーを入手して検討し、ポリシーが以下のように 7.1.1~7.1.4 を含んでいることを確認する。</p> <ul style="list-style-type: none"> 各役割のアクセスニーズと特権割り当てを定義する 特権ユーザ ID に与えるアクセス権が、職務の実行に必要な最小限の特権に制限されていること 特権の付与は、個人の職種と職務に基づくこと すべてのアクセスに対して、権限を持つ関係者による、許可された特権のリストを含む、文書化された承認（書面または電子的） 	カード会員データにアクセスする人が増えるほど、ユーザのアカウントが不正に使用されるリスクが高まります。アクセスを、業務上必要とする正当な理由がある人に限定すると、組織での経験不足や悪意によるカード会員データの不適切な処理を防ぐことができます。
7.1.1 以下を含む、各役割のアクセスニーズを定義する <ul style="list-style-type: none"> 各役割が職務上アクセスする必要のあるシステムコンポーネントとデータリソース リソースへのアクセスに必要な特権レベル（ユーザ、管理者など） 	<p>7.1.1 役割のサンプルを選択し、各役割のアクセスニーズが定義されており、以下を含むことを確認する。</p> <ul style="list-style-type: none"> 各役割が職務上アクセスする必要のあるシステムコンポーネントとデータリソース 各役割が職務を遂行するために必要な特権の特定 	カード会員データへのアクセスをそのアクセスを必要とするユーザに限定するためには、まず、各役割のアクセスニーズ（システム管理者、コールセンタースタッフ、店員など）、各役割がアクセスする必要のあるシステム/デバイス/データ、各役割が割り当てられたタスクを効果的に遂行するために必要な特権レベルを定義する必要があります。役割が定義されたら、その役割に応じて各人のアクセス権を付与できます。
7.1.2 特権ユーザ ID に与えるアクセス権を職務の実行に必要な最小限の特権に制限する。	<p>7.1.2.a アクセス権の割り当ての責任者をインタビューすることで、特権ユーザ ID へのアクセスが以下を満たしていることを確認する。</p> <ul style="list-style-type: none"> そのようなアクセス権を特に必要とする役割にのみ割り当てる 職務の実行に必要な最小限の特権に制限されている 	特権 ID を割り当てるとき、各人が仕事を遂行するために必要な特権を割り当てることが重要です（「必要最小限の特権」）。例えば、データベース管理者やバックアップ管理者には、システム全体の管理者と同じ特権を割り当てないことが必要です。必要最小限の特権を割り当てることで、ア

PCI DSS 要件	テスト手順	ガイダンス
	<p>7.1.2.b アクセス権を持つユーザ ID のサンプルを選択し、管理責任者をインタビューすることで、割り当てられた特権が以下を満たすことを確認する。</p> <ul style="list-style-type: none"> ● そのユーザの職務に必要 ● 職務の実行に必要な最小限の特権に制限されている 	プリケーションについて十分な知識のないユーザが間違って、または知らないでアプリケーションの構成を変更したり、セキュリティ設定を変更することを防止できます。必要最小限の特権を割り当てるとはまた、無許可の人物があるユーザ ID にアクセスできた場合の損害範囲を最小限にとどめるためにも役立ちます。
7.1.3 個人の職種と職務に基づくアクセス権を割り当てる。	7.1.3 ユーザ ID のサンプルを選択し、管理責任者をインタビューすることで、割り当てられた特権がその個人の職種と職務に基づいていることを確認する。	ユーザ役割のニーズが定義されたら（PCI DSS 要件 7.1.1 に従って）、すでに作成されている役割を使用し、各人の職種と職務に基づき簡単にアクセス権を付与することができます。
7.1.4 適切な権限を持つ関係者による文書化された変更承認を必要とする。	<p>7.1.4 ユーザ ID を選択し、文書化された承認と比較することで、以下を確認する。</p> <ul style="list-style-type: none"> ● 割り当てられた特権に対する文書化された承認が存在する ● その承認は権限のある関係者によるものである ● 指定された特権がその個人に割り当てられた役割に一致している 	文書化された承認（書面または電子的）により、アクセス権を持つ個人が管理責任者に知られており、許可されていること、およびそのアクセスが職務上必要であることが確認できます。
7.2 システムコンポーネントのアクセス制御システムを確立することで、ユーザの必要性に基づいてアクセスを制限し、特に許可のない場合は「すべてを拒否」に設定する。 アクセス制御システムには以下の項目を含める必要がある。	7.2 システムの設定とベンダの文書を検査し、アクセス制御システムが以下のように実装されていることを確認する。	ユーザが必要とする範囲に基づいてアクセスを制限するメカニズムがないと、ユーザは知らないうちにカード会員データへのアクセスを付与される場合があります。アクセス制御システムは、アクセスの制限と特権の割り当てプロセスを自動化します。さらに、デフォルトの「すべてを拒否」設定により、そのアクセス権を特に付与するルールが確立されるまで、誰にもアクセス権が付与されないようになっています。 事業体はユーザアクセスを管理するため、一つ以上のアクセス制御システムを持っているかもしれません。
7.2.1 すべてのシステムコンポーネントを対象に含む	7.2.1 アクセス制御システムがすべてのシステムコンポーネントに実装されていることを確認する。	注: 一部のアクセス制御システムはデフォルトで「すべてを許可」が設定されており、個別に拒否するためのルールを記述しない限り、または記述するまでは、アクセスが許可される。
7.2.2 職種と職務に基づく、個人への特権の付与	7.2.2 アクセス制御システムが、職種と職務に基づいて個人に割り当てられる特権を強制するよう構成されていることを確認する。	
7.2.3 デフォルトでは「すべてを拒否」の設定	7.2.3 アクセス制御システムがデフォルトで「すべて拒否」が設定されていることを確認する。	

PCI DSS 要件	テスト手順	ガイダンス
7.3 カード会員データへのアクセスを制限するためのセキュリティポリシーと操作手順が文書化されて使用されており、影響を受ける関係者全員に知られていることを、確実にする。	<p>7.3 文書を調べ、担当者をインタビューすることで、カード会員データへのアクセスを制限するためのセキュリティポリシーと操作手順が以下の要件を満たしていることを確認する。</p> <ul style="list-style-type: none"> • 文書化されている • 使用されている • 影響を受ける関係者全員に知らされている 	担当者はセキュリティポリシーと操作手順を認識・順守して、アクセスが、知る必要性と必要最小限の特権に基づいて継続的に制御されるようになります。

要件 8: システムコンポーネントへのアクセスを識別・認証する

アクセスが可能な各ユーザに一意の ID を割り当てて、各ユーザが自身の行動に独自に説明責任を負うようにします。このような説明責任に対応している場合、重要なデータおよびシステムに対するアクションは既知の承認されたユーザやプロセスによって実行され、そのユーザを追跡することが可能です。

パスワードの有効性は、主として認証システムのデザインと実装方法、特に、攻撃者がどれだけの頻度でパスワードを試すことが許されるか、および入力中、送信中、および保存中におけるユーザパスワードを保護するセキュリティ方式によって決まります。

注:これらの要件は、管理機能をもつすべてのアカウント (POS アカウントを含む)、およびカード会員データの閲覧またはアクセス、あるいはカード会員データを保存するシステムへのアクセスに使用されるすべてのアカウントに適用可能です。これには、ベンダーその他の第三者 (サポートやメンテナンスのためなど) によって使用されるアカウントも含まれます。これらの要件は消費者によって使用されるアカウントには適用されません (例、カード会員)

ただし、要件 8.1.1、8.2、8.5、8.2.3 ~ 8.2.5、8.1.6 ~ 8.1.8 は、1 つのトランザクションを行うために一度に 1 つのカード番号にしかアクセスできない、POS ペイメントアプリケーション内のユーザアカウント (レジ係のアカウントなど) に適用することは意図していません。

PCI DSS 要件	テスト手順	ガイダンス
8.1 ポリシーと手順を定義して実装することで、次のように、すべてのシステムコンポーネントで、非消費者ユーザと管理者のための適切なユーザ識別管理が行われるようにする。	8.1.a 手順を調べて、以下の 8.1.1 ~ 8.1.8 の各項目についてのプロセスが定義されていることを確認する。 8.1.b 以下を実行することによって、ユーザ識別管理のための手順が実施されていることを確認する。	複数の従業員が 1 つの ID を使用するのではなく、各ユーザが一意に識別されるようにすることで、組織はアクションに対する個人の責任と従業員ごとの有効な監査証跡を保持することができます。これは、悪用や悪意のある意図が発生した場合に、問題を迅速に解決および抑制するのに役立ちます。
8.1.1 システムコンポーネントまたはカード会員データへのアクセスを許可する前に、すべてのユーザに一意の ID を割り当てる。	8.1.1 管理責任者をインタビューすることで、すべてのユーザに、システムコンポーネントまたはカード会員データにアクセスするための一意の ID が割り当てられていることを確認する。	
8.1.2 ユーザ ID、資格情報、および他の識別オブジェクトの追加、削除、変更を管理する。	8.1.2 特権ユーザ ID と一般ユーザ ID について、関連付けられている権限を調べ、システム設定を観察して、各ユーザ ID と特権ユーザ ID に、文書化されている承認内容で指定されている特権のみが実装されていることを確認する。	システムへのアクセス権が付与されているユーザアカウントがすべて有効で認識されているユーザであることを確認するためには、強力なプロセスを用いて、新しいユーザ ID の追加や既存のものの変更と削除を含む、ユーザ ID および他の認証情報のすべての変更を管理する必要があります。
8.1.3 契約終了したユーザのアクセスを直ちに取り消す。	8.1.3.a 過去 6 カ月間に契約終了したユーザのサンプルを選択し、現在のユーザアクセリストを調べて、ローカルとリモートアクセス両方につき - これらのユーザの ID が無効化または削除されていることを確認する。	従業員の退職後も彼らのユーザアカウント経由でネットワークへのアクセスが可能な場合、元従業員または、古いアカウントや未使用のアカウントを利用する悪意のある者によって、カード会員

PCI DSS 要件	テスト手順	ガイダンス
	8.1.3.b スマートカード、トークンなど、すべての物理的認証方法が返還されたか、無効にされたことを確認する。	データへの不要な、または悪意のあるアクセスが発生する可能性があります。不正なアクセスを防ぐには、ユーザの資格情報やその他の認証方法が、退職時にできるだけ速やかに破棄される必要があります。
8.1.4 90 日以内に非アクティブなユーザアカウントを削除/無効にする。	8.1.4 ユーザアカウントを観察することで、90 日間を超える非アクティブなアカウントが削除または無効になっていることを確認する。	日常的に使用されていないアカウントでは変更（パスワードの変更など）に気づかれる危険性が少ないので、攻撃の対象となることが多くなります。そのため、これらのアカウントは侵害しやすく、カード会員データへのアクセスに使用されることになります。
8.1.5 第三者がリモートアクセス経由でシステムコンポーネントのアクセス、サポート、メンテナンスに使用するユーザ ID を以下のように管理する。 <ul style="list-style-type: none"> • 必要な期間内だけ有効になり、使用されていないときは無効になっている。 • 使用時に監視されている。 	8.1.5.a 担当者をインタビューし、第三者がシステムコンポーネントのアクセス、サポート、メンテナンスに使用するアカウントを管理するためのプロセスを観察して、リモートアクセスに使用するアカウントが以下を満たしていることを確認する。 <ul style="list-style-type: none"> • 使用されていないときに無効になっている • 第三者が必要なときにのみ有効になり、使用されていない場合は無効になる 8.1.5.b 担当者をインタビューし、プロセスを観察することで、使用中に第三者のリモートアクセスアカウントが監視されていることを確認する。	システムをサポートする必要がある場合に備えて第三者がネットワークに 24 時間 365 日アクセスできるようにすると、ネットワークへのこの常時使用可能な外部エントリポイントを見つけて使用する、第三者環境内のユーザ、または悪意のある者からの不正なアクセスが行われる可能性が増加します。必要な期間にのみアクセスを有効にし、必要なくなった時点で無効にすると、これらの接続の悪用防止に役立ちます。 第三者のアクセス監視は、第三者が必要なときだけ、および承認された時間内でのみシステムにアクセスすることを保証できます。
8.1.6 6 回以下の試行で、ユーザ ID をロックアウトすることによって、アクセス試行の繰り返しを制限する。	8.1.6.a システムコンポーネントのサンプルで、システム構成設定を検査することで、無効なログイン試行後に、ユーザアカウントのロックアウトを要求する認証パラメータが 6 回以下に設定されていることを確認する。 8.1.6.b サービスプロバイダの評価のみの追加のテスト手順：内部プロセスと顧客/ユーザ文書をレビューし、実装されたプロセスを観察することで、6 回以下の無効なアクセス試行後に、非消費者の顧客ユーザアカウントが一時的にロックアウトされることを確認する。	アカウントロックアウトメカニズムがないと、攻撃者は、手動または自動ツール（パスワード解読ツールなど）を使用し、推測に成功してユーザアカウントへのアクセスを得るまで、継続してパスワードの推測を試みることができます。 注：テスト手順 8.1.6.b は企業がサービスプロバイダを評価する場合の追加の手順です。

PCI DSS 要件	テスト手順	ガイダンス
8.1.7 最低 30 分間、または管理者がユーザ ID を有効にするまでのロックアウト期間を設定する。	8.1.7 システムコンポーネントのサンプルで、システム構成設定を調べ、ユーザアカウントがロックアウトされたら、最低 30 分間、または管理者がユーザ ID を有効にするまでロックアウト状態が続くことを要求するよう、認証パラメータが設定されていることを確認する。	パスワードの推測が絶えず試みられたためにアカウントがロックアウトされる場合、アカウント再有効化の遅延管理により、悪意のある者がこれらのロックされたアカウントのパスワードを継続して推測することを防ぐことができます（アカウントが再有効化されるまで少なくとも 30 分待つ必要があります）。さらに、再有効化を要求する必要がある場合、管理者またはヘルプデスクは、実際にアカウント所有者が再有効化をリクエストしていることを検証できます。
8.1.8 セッションのアイドル状態が 15 分を超えた場合、ターミナルまたはセッションを再度アクティブにするため、ユーザの再認証が必要となる。	8.1.8 システムコンポーネントのサンプルで、システム構成設定を調べ、セッションのアイドル状態が 15 分を超えた場合、ターミナルまたはセッションを再度アクティブにするため、ユーザの再認証が必要となることを確認する。	重要なシステムコンポーネントまたはカード会員データにアクセス可能なオープンマシンからユーザが離れるとき、そのマシンがユーザの不在時に他の者によって使用され、権限のないアカウントアクセスや悪用が発生する可能性があります。 再認証は、そのマシン上で実行されているすべてのセッションを保護するために、システムレベルで適用するか、アプリケーションレベルで適用できます。
8.2 一意の ID を割り当てることに加え、すべてのユーザを認証するため、次の方 法の少なくとも 1つを使用することで、すべてのシステムコンポーネント上での非消費者のユーザと管理者の適切なユーザ認証管理を確実にする。 <ul style="list-style-type: none">• ユーザが知っていること（パスワードやパスフレーズなど）• トーカンデバイスやスマートカードなど、ユーザが所有しているもの• ユーザ自身を示すもの（生体認証など）	8.2 ユーザがカード会員データ環境にアクセスするための一意の ID と追加の認証（パスワード/パスフレーズなど）を使用して認証されることを確認するため、次の項目を実行する。 <ul style="list-style-type: none">• 使用される認証方法について記述した文書を調べる。• 使用される認証方法の各種類およびシステムコンポーネントの各種類について、認証を調べて、文書に記述された認証方法に従って認証が機能していることを確認する。	これらの認証方法を一意の ID に加えて使用すると、侵害を試みようとする人物は一意の ID に加えてパスワード（またはその他の認証アイテム）を知る必要があるため、ユーザの ID が侵害されるのを防ぐことができます。デジタル証明書は、そのユーザに一意である限り、「ユーザが所有しているもの」での認証形式として有効なオプションであることに留意してください。 悪意のある者がシステムを侵害するために最初に行うステップの 1つが弱いまたは存在しないパスワードを利用することであるため、認証管理のための適切なプロセスを実装することが重要です。
8.2.1 強力な暗号化を使用して、すべてのシステムコンポーネントで、送信と保存中に認証情報（パスワード/パスフ	8.2.1.a ベンダ文書とシステム構成設定を調べて、送信および保存中にパスワードが強力な暗号化によって保護されていることを確認する。	多くのネットワークデバイスおよびアプリケーションは、ネットワーク内で暗号化されていない読み取り可能なパスワードを伝送し、パスワード

PCI DSS 要件	テスト手順	ガイダンス
レーズなど) をすべて読み取り不能とする。	<p>8.2.1.b システムコンポーネントのサンプルに対して、パスワードファイルを調べて、パスワードが保存中に読み取り不能であることを確認する。</p> <p>8.2.1.c システムコンポーネントのサンプルに対して、データ伝送を調べて、パスワードが伝送中に読み取り不能であることを確認する。</p> <p>8.2.1.d サービスプロバイダの評価のみの追加のテスト手順：パスワードファイルを観察して、保存中に非消費者の顧客のパスワードが読み取れないことを確認する。</p> <p>8.2.1.e サービスプロバイダの評価のみの追加のテスト手順：データの送信を観察して、送信中に非消費者の顧客のパスワードが読み取れないことを確認する。</p>	を暗号化せずに保存します。悪意のある者は、暗号化されていないパスワードを「スニッファー（Sniffer）」を使用して伝送中に容易に傍受したり、保存されているファイル内の暗号化されていないパスワードに直接アクセスしたりして、このデータを使用して不正にアクセスすることができます。 注：テスト手順 8.2.1.d および 8.2.1.e は企業がサービスプロバイダを評価する場合の追加の手順です。
8.2.2 パスワードのリセット、新しいトークンの準備、新しい鍵の生成など、認証情報を変更する前に、ユーザの身元を確認する。	8.2.2 認証情報を変更するための認証手順を調べて、セキュリティ担当者を観察して、ユーザが、電話、電子メール、Web、または他の非対面法でパスワードのリセットを要求した場合、パスワードがリセットされる前に、ユーザの身元が確認されていることを確認する。	多くの悪意のある者は「ソーシャルエンジニアリング」（ヘルプデスクに電話して正当なユーザを装うなど）を使用してパスワードを変更させて、ユーザ ID を利用できるようにします。管理者が認証情報をリセットまたは変更する前にユーザを識別できるよう、正しいユーザのみが答えることができる「秘密の質問」を使用することを検討してください。
8.2.3 パスワード/パスフレーズは以下を満たす必要がある。 <ul style="list-style-type: none"> • パスワードに 7 文字以上が含まれる • 数字と英文字の両方を含む あるいは、上記のパラメータに等しい	<p>8.2.3.a システムコンポーネントのサンプルについて、システム構成設定を調べて、少なくとも以下の強度/複雑さを必要とするようにユーザパスワード/パスフレーズのパラメータが設定されていることを確認する。</p> <ul style="list-style-type: none"> • パスワードに 7 文字以上が含まれる • 数字と英文字の両方を含む 	悪意のある者は最初に弱いパスワードをもつ、またはパスワードが存在しないアカウントを見つけるとするため、強力なパスワード/パスフレーズはネットワーク防御にとって最初の手段です。パスワードが短く、あるいは単純で推測しやすい場合、悪意のある者がこれらの脆弱なアカウントを

PCI DSS 要件	テスト手順	ガイダンス
複雑さと強度をもつパスワード/パスフレーズ	<p>8.2.3.b サービスプロバイダの評価のみの追加のテスト手順：内部プロセスおよび顧客/ユーザ文書を確認して、非消費者顧客のユーザのパスワード/パスフレーズが少なくとも次の強度/複雑さを満たすことが要求されていることを確認する。</p> <ul style="list-style-type: none"> • パスワードに 7 文字以上が含まれる • 数字と英文字の両方を含む 	<p>見つけ、有効なユーザ ID を装ってネットワークを侵害することは比較的簡単です。</p> <p>この要件では、パスワード/パスフレーズに 7 文字以上の数字と英字を両方含むことを指定しています。技術的な制限上、この最小限を満たせない場合、事業体は「等価強度」を使用してその代替値を評価します。異なるフォーマットのパスワード/パスフレーズのためのパスワードの変動性および強度の同等性（またエントロピーとも呼ばれる）に関する情報については、業界標準を参照してください（例、NIST SP 800-63 の現行バージョン）。</p> <p>注：テスト手順 8.2.3.b は事業体がサービスプロバイダを評価する場合のみの追加の手順です。</p>
8.2.4 ユーザパスワード/パスフレーズは、少なくとも 1 回は 90 日ごと変更する。	<p>8.2.4.a システムコンポーネントのサンプルについて、システム構成設定を調べて、少なくとも 1 回は 90 日ごとにパスワード/パスフレーズを変更することを要求するようにユーザパスワードのパラメータが設定されていることを確認する。</p> <p>8.2.4.b サービスプロバイダの評価のみの追加のテスト手順。内部プロセスおよび顧客/ユーザ文書を調べて、以下を確認する。</p> <ul style="list-style-type: none"> • 非消费者的顧客ユーザパスワード/パスフレーズを定期的に変更することが要求されている • 非消费者的顧客ユーザに、いつどのような状況下でパスワード/パスフレーズを変更する必要があるかについてのガイダンスが与えられている 	<p>長期間変更せずに有効なままになっているパスワード/パスフレーズは、悪意のある者がパスワード/パスフレーズを解読する行為により長い時間を与えることになります。</p> <p>注：テスト手順 8.2.4.b は事業体がサービスプロバイダを評価する場合のみの追加の手順です。</p>
8.2.5 これまでに使用した最後の 4 つのパスワード/パスフレーズのいずれかと同じである新しいパスワード/パスフレーズを許可しない。	<p>8.2.5.a システムコンポーネントのサンプルで、システム構成設定を入手して調べ、新しいパスワード/パスフレーズとして、これまでに使用した最後の 4 つのパスワード/パスフレーズのいずれかと同じパスワード/パスフレーズを指定できないことを要求するユーザパスワードパラメータが設定されていることを確認する。</p> <p>8.2.5.b サービスプロバイダの評価のみの追加のテスト手順：内部プロセスと顧客/ユーザマニュアルを調べて、非消费者的顧客ユーザのパスワード/パスフレーズがこれまでに使用した 4 つのパスワード/パスフレーズのいずれかにすることはできなくなっていることを確認する。</p>	<p>パスワード履歴が保持されていない場合、以前のパスワードが何度も再使用されることがあるため、パスワードを変更することの効果が低減します。一定期間ほどパスワードを再使用できないことを要求することで、推定されたか総当たり攻撃で見つけられたパスワードが今後使用される可能性が低減されます。</p> <p>注：テスト手順 8.2.5.b は事業体がサービスプロバイダを評価する場合のみの追加の手順です。</p>

PCI DSS 要件	テスト手順	ガイダンス
8.2.6 初期パスワード/パスフレーズとリセットパスワード/パスフレーズをユーザごとに一意の値にリセットし、初回の使用後直ちに変更する。	8.2.6 パスワード手順を調べて、セキュリティ担当者を観察して、新しいユーザの初期パスワード/パスフレーズと既存ユーザのリセットパスワード/パスフレーズが、各ユーザで一意の値に設定され、初回の使用後に変更されていることを確認する。	新規ユーザに同じパスワードを使用すると、内部ユーザ、元従業員、または悪意のある者により、このパスワードが知られ、または容易に発見されて、それを使用してアカウントへのアクセスが可能になります。

8.3CDE に対する、すべての非コンソール管理アクセス、ならびにすべてのリモートアクセスについて、多要素認証を使用して安全に保護する。

注:多要素認証は、3つの認証方法のうち最低2つを認証に使用する必要がある（認証方法については、要件8.2を参照）。1つの要素を2回使用すること（例えば、2つの個別パスワードを使用する）は、多要素認証とは見なされない。

多要素認証は、アクセスが許可される前に、個人の認証に最低二つ以上の別の形式（要件8.2に記載されているように）の提示を要求します。

多要素認証は、権限を得ようとアクセスを試行する個人が、本人の主張するとおりの人物であるという付加的な保証を提供します。多要素認証において、攻撃者は少なくとも二つの異なる認証メカニズムを侵害する必要があり、侵害の難易度を高めることでリスク軽減になります。

多要素認証は、特定のシステムコンポーネントのシステムレベルおよびアプリケーションレベルの両方で必要とされているわけではありません。多要素認証は、特定のネットワークへの認証、またはシステムコンポーネントへの認証の際のいかで実施することができます。

多要素認証方式の例としては、トークン使用のRADIUS（Remote Authentication and Dial-In Service）、トークン使用のTACACS（Terminal Access Controller Access Control System）、および多要素認証を促進する他の方式が含まれますが、これらに限りません。

PCI DSS 要件	テスト手順	ガイダンス
<p>8.3.1 CDE への管理者のアクセス権を持つ担当者によるすべての非コンソールアクセスに多要素認証を組み込む。</p>	<p>8.3.1.a 該当するネットワークおよび/またはシステム構成を調べ、多要素認証が CDE に対するすべての非コンソール管理アクセスの際に要求されていることを確認する。</p> <p>8.3.1.b CDE にログインする管理者のサンプルを観察することで、3つの認証方式のうちの少なくとも 2つが使用されていることを確認する。</p>	<p>この要件は CDE に対する管理アクセス権限を持つすべての担当者に適用することを意図します。この要件は管理アクセス権を持つ担当者による CDE に対する非コンソールアクセスのみに適用されます。自動機能を実行するためのアプリケーションまたはシステムアカウントには適用されません。事業体が CDE と他のネットワークを分離するためのセグメンテーションを使用していない場合、管理者は CDE ネットワークへログインする際、またはシステムへログインする際のいずれかで多要素認証を使用することができます。</p> <p>CDE が事業体の他のネットワークからセグメンテーションされている場合、管理者は非 CDE ネットワークから CDE システムへ接続する際に多要素認証の使用が必要です。多要素認証は、ネットワークレベルまたはシステム/アプリケーションレベルに対して多要素認証を実装することができます。両方に実装する必要はありません。管理者が CDE ネットワークにログインする際に多要素認証を使用する場合、CDE 内の特定のシステムやアプリケーションへのログインに、再度多要素認証を使用する必要はありません。</p>
<p>8.3.2 事業体のネットワーク外からのすべてのリモートネットワークアクセス（ユーザと管理者の両方、サポートやメンテナンスのための第三者のアクセスを含む）に多要素認証を組み込む。</p>	<p>8.3.2.a リモートアクセスサーバとシステムのシステム構成を調べて、以下に対して多要素認証が要求されていることを確認する：</p> <ul style="list-style-type: none"> • ユーザ権限および管理者権限を有する担当者によるすべてのリモートアクセス、および • すべての第三者/ベンダリモートアクセス（サポートやメンテナンス目的でのアプリケーションやシステムコンポーネントへのアクセスを含む） 	<p>この要件は、リモートアクセスによって CDE にアクセスされる可能性があるネットワークにリモートアクセスする、一般ユーザ、管理者、およびベンダ（サポートやメンテナンス用）を含むすべての関係者が適用対象です。リモートアクセスの接続先が、適切なセグメンテーションを使用し、リモートユーザがカード会員データ環境にアクセスしたり、影響を及ぼしたりすることができないよ</p>

PCI DSS 要件	テスト手順	ガイダンス
8.4 以下を含む認証のポリシーと手順を文書化し、すべてのユーザーに通達する。 <ul style="list-style-type: none"> ・ 強力な認証情報を選択するためのガイダンス ・ ユーザが自分の認証情報を保護する方法についてのガイダンス ・ 前に使用していたパスワードを再使用しないという指示 ・ パスワードが侵害された疑いがある場合にはパスワードを変更するという指示 	<p>8.3.2.b ネットワークにリモート接続する従業員（ユーザや管理者など）のサンプルを観察し、3つの認証方法のうち2つが使用されていることを確認する。</p> <p>8.4.a 手順を調べ、担当者をインタビューすることで、認証のポリシーと手順がすべてのユーザに配布されていることを確認する。</p> <p>8.4.b ユーザに配布された認証のポリシーと手順を調べることで、以下を確認する。 <ul style="list-style-type: none"> ・ 強力な認証情報を選択するためのガイダンス ・ ユーザが自分の認証情報を保護する方法についてのガイダンス ・ 前に使用していたパスワードを再使用しないという指示 ・ パスワードが侵害された疑いがある場合にはパスワードを変更するという指示 </p> <p>8.4.c ユーザのサンプルのインタビューを行い、認証のポリシーと手順に精通していることを確認する。</p>	<p>うになっている事業体のネットワークである場合、そのネットワークへのリモートアクセスに多要素認証を組み込むことは要件ではありませんが、カード会員データ環境にアクセスできるネットワークへのリモートアクセスには多要素認証が必要であり、事業体のネットワークへのすべてのリモートアクセスに多要素認証を使用することが推奨されます。</p> <p>パスワード/認証のポリシーと手順をすべてのユーザに伝達すると、ユーザのポリシーの理解および準拠に役立ちます。</p> <p>例えば、強力なパスワードの選択に関するガイダンスには、辞書にある単語、ユーザに関する情報（ユーザ ID、姓などの人名、生年月日など）を含まない推測しにくいパスワードを選ぶための提案を含みます。認証情報の保護についてのガイダンスには、パスワードを書き下ろさない、安全でないファイルに保存しない、（例えば、従業員に電話して「トラブルシューティングのため」を装ってパスワードを聞き出そうとするなど）パスワードを侵害しようとする悪意のある者について警告する、などを含むことができます。</p> <p>パスワードが安全でなくなった可能性がある場合にはパスワードを変更するようにユーザに指示することで、悪意のある者が合法的なパスワードを使って不正なアクセスを行うことを防止できます。</p>
8.5 次のように、グループ、共有、または汎用の ID やパスワード、または他の認証方法が使用されていない。 <ul style="list-style-type: none"> ・ 汎用ユーザ ID が無効化または削除されている ・ システム管理作業およびその他の重要な機能に対する共有ユーザ ID が存在しない 	<p>8.5.a システムコンポーネントのサンプルについて、ユーザ ID リストを調べて、以下を確認する。</p> <ul style="list-style-type: none"> ・ 汎用ユーザ ID が無効化または削除されている ・ システム管理作業およびその他の重要な機能のための共有ユーザ ID が存在しない ・ システムコンポーネントの管理に共有および汎用ユーザ ID が使用されていない 	<p>複数のユーザが同じ認証資格情報（アカウントとパスワードなど）を共有すると、システムアクセスやアクションを誰が行ったかを追跡することは不可能になります。特定の活動を行ったユーザが、認証資格情報を知っているグループ内の誰であるかを特定できないため、個人のアクションに責任を割り当てる、個人のアクションの有効な</p>

PCI DSS 要件	テスト手順	ガイダンス
<p>しない</p> <ul style="list-style-type: none"> システムコンポーネントの管理に共有および汎用ユーザ ID が使用されていない <p>8.5.1 サービスプロバイダのみの追加要件: 顧客環境へのリモートアクセス権を持つサービスプロバイダは（例: POS システムやサーバのサポートで）、各顧客に一意な認証情報（パスワード/パスフレーズなど）を使用する必要がある。</p> <p>注:この要件は、複数の顧客環境がホストされている、独自のホスティング環境にアクセスする共有ホスティングプロバイダに適用することを意図していません。</p>	<p>8.5.b 認証のポリシーと手順を調べて、グループおよび共有 ID やパスワードまたは他の認証方法が明示的に禁止されていることを確認する。</p> <p>8.5.c システム管理者のインタビューを行い、グループおよび共有 ID やパスワード、または他の認証方法が、要求があっても配布されないことを確認する。</p> <p>8.5.1 サービスプロバイダの評価のみの追加のテスト手順：認証ポリシーと手順を調べ、担当者をインタビューすることで、各顧客環境にリモートアクセスするために異なる認証情報が使用されていることを確認する。</p>	<p>ログを記録したりすることができなくなります。</p> <p>注:この要件は事業体がサービスプロバイダを評価する場合のみの追加の手順です。</p> <p>サービスプロバイダが各顧客で異なる認証情報を使用すると、複数の顧客が单一の資格情報を使用することによる悪用を防ぐのに役立ちます。</p> <p>各接続で一意の資格情報（例えば、单一使用パスワードを経由して）を提供する、多要素メカニズムなどのテクノロジを使用して、この要件の目的を満たすこともできます。</p>
<p>8.6 その他の認証メカニズムが使用されている（例えば、物理的または論理的セキュリティトークン、スマートカード、証明書など）これらのメカニズムの使用は、以下のように割り当てる必要がある。</p> <ul style="list-style-type: none"> 認証メカニズムは、個々のアカウントに割り当てなければならず、複数アカウントで共有することはできない 物理/論理制御により、意図されたアカウントのみがアクセスできるようになる 	<p>8.6.a 認証ポリシーと手順を調べ、物理セキュリティトークン、スマートカード、証明書などを使用する手順が定義されており以下を含むことを確認する。</p> <ul style="list-style-type: none"> 認証メカニズムが、個々のアカウントに割り当てられており、複数アカウントで共有されていない 物理/論理制御により、意図されたアカウントのみがアクセスできるようになっている 	<p>トークン、スマートカード、証明書などのユーザ認証メカニズムが複数のアカウントによって使用できる場合は、認証メカニズムを使用して個人を特定することが不可能になる場合があります。アカウントのユーザを一意に特定するために物理的および/または論理制御（PIN、生体認証データ、パスワードなど）を使うと、共有認証メカニズムの使用による不正ユーザのアクセスを防止できます。</p>

PCI DSS 要件	テスト手順	ガイダンス
	<p>8.6.b セキュリティ担当者をインタビューすることで、認証メカニズムが、個々のアカウントに割り当てられており、複数アカウントで共有されていないことを確認する。</p> <p>8.6.c システム構成設定や該当する場合は物理制御を調べて、物理/論理制御により、意図されたアカウントのみがそのメカニズムを使ってアクセスできるようにする制御が実装されていることを確認する。</p>	
<p>8.7 カード会員データを含むデータベースへのすべてのアクセス（アプリケーション、管理者、およびその他のすべてのユーザによるアクセスを含む）が以下のように制限されている。</p> <ul style="list-style-type: none"> データベースへのユーザアクセス、データベースのユーザクエリ、データベースに対するユーザアクションはすべて、プログラムによる方法によってのみ行われる。 データベースへの直接アクセスまたはクエリはデータベース管理者のみに制限される。 データベースアプリケーション用のアプリケーション ID を使用できるのはそのアプリケーションのみである（個々のユーザやその他の非アプリケーションプロセスは使用できない）。 	<p>8.7.a データベースおよびアプリケーションの構成設定を調べ、すべてのユーザがアクセスする前に認証されていることを確認する。</p> <p>8.7.b データベースおよびアプリケーションの構成設定を調べて、データベースでのすべてのユーザアクセス、ユーザのクエリ、およびユーザのアクション（例えば、移動、コピー、削除）が、プログラムを使用する方法（ストアドプロシージャを介してなど）によってのみ実行されることを確認する。</p> <p>8.7.c データベースアクセス制御設定とデータベースアプリケーション構成設定を調べて、ユーザの直接アクセスまたはデータベースへのクエリがデータベース管理者に制限されていることを確認する。</p> <p>8.7.d データベースアクセス制御設定、データベースアプリケーション設定、および関連アプリケーション ID を調べて、アプリケーション ID がアプリケーションによってのみ使用できることを確認する（個々のユーザまたはその他のプロセスでは使用できない）。</p>	データベースおよびアプリケーションへのアクセス時にユーザ認証を行わないと、権限のないアクセスまたは悪意のあるアクセスが発生する可能性が増え、さらにユーザが認証されていないためシステムに認識されず、このようなアクセスをログに記録できません。また、データベースアクセスは、エンドユーザによるデータベースへの直接アクセスではなく、プログラムによる方法（ストアドプロシージャなど）を通じてのみ許可される必要があります（管理職務のためにデータベースに直接アクセスする必要のある DBA を除きます）。
<p>8.8 識別と認証に関するセキュリティポリシーと操作手順が文書化されて使用されており、影響を受ける関係者全員に知られていることを、確実にする。</p>	<p>8.8 文書を調べ、関係者をインタビューすることで、識別と認証に関するセキュリティポリシーと操作手順が以下の要件を満たしていることを確認する。</p> <ul style="list-style-type: none"> 文書化されている 使用されている 影響を受ける関係者全員に知らされている 	識別と認証の継続的な管理を行うために、関係者はセキュリティポリシーと操作手順を認識・順守する必要があります。

要件 9: カード会員データへの物理アクセスを制限する

データまたはカード会員データを格納するシステムへの物理アクセスは、デバイスまたはデータにアクセスし、システムまたはハードコピーを削除する機会をユーザに提供するため、適切に制限する必要があります。要件 9において、「オンサイト要員」とは、フルタイムおよびパートタイムの従業員、一時的な従業員、事業体の施設内に物理的に存在する請負業者やコンサルタントのことです。「訪問者」は、ベンダー、オンライン要員の客、サービス要員、または短期間（通常は 1 日以内）施設に入る必要がある人のことです。「媒体」は、カード会員データを含むすべての紙および電子媒体のことです。

PCI DSS 要件	テスト手順	ガイダンス
<p>9.1 適切な施設入館管理を使用して、カード会員データ環境内のシステムへの物理アクセスを制限および監視する。</p> <p>9.1.1 ビデオカメラやアクセス制御メカニズム（または両方）を使用して、機密エリアへの個々の物理アクセスを監視する。収集されたデータを確認し、その他のエントリと相関付ける。法律によって別途定められていない限り、少なくとも 3 カ月間保管する。</p> <p>注: 「機密エリア」とは、データセンター、サーバルーム、またはカード会員データを保存、処理、または伝送するシステムが設置されているエリアのことである。これには、小売店のレジなど、POS 端末のみが存在するエリアは含まれない。</p>	<p>9.1 各コンピュータルーム、データセンター、およびカード会員データ環境内のシステムを備えた物理的なエリアで、物理的なセキュリティコントロールが存在することを確認する。</p> <ul style="list-style-type: none"> ■ パッジ読み取り機または承認済みパッジ、施錠、鍵などのその他のデバイスによってアクセスが管理されていることを確認する。 ■ システム管理者がカード会員データ環境内のランダムに選択したシステムのコンソールにログインするのを観察して、コンソールが不正使用を防止するように「ロック」されていることを確認する。 <p>9.1.1.a ビデオカメラやアクセス制御メカニズム（または両方）を使用して、機密エリアへの入退場ポイントを監視する。</p> <p>9.1.1.b ビデオカメラやアクセス制御メカニズム（または両方）が改ざんや無効化から保護されていることを確認する。</p> <p>9.1.1.c ビデオカメラやアクセス制御メカニズムのデータをレビューし、カメラやその他のメカニズムからのデータが少なくとも 3 カ月間保管されていることを確認する。</p>	<p>バッジシステムや入室の管理などの物理的なアクセス制御がないと、権限のないユーザが施設に容易に入り、重要なシステムやカード会員データを盗用、無効化、中断、または破壊することができます。コンソールのログイン画面をロックすることで、権限のない人々が機密情報にアクセスしたり、システム構成を変更したり、ネットワークに脆弱性を導入したり、記録を破壊したりすることができます。</p> <p>物理的な侵入の調査時、これらの管理は、機密エリアに物理的にアクセスした個人およびその侵入と退出時刻を特定するのに役立ちます。</p> <p>機密エリアへの物理的なアクセスを試みる犯罪者は、監視制御装置を無効にしたりバイパスすることを試みようとしています。これらの制御装置の改ざんを防止するために、改ざんが必ず検出されるような位置にビデオカメラを設置します。同様に、アクセス制御メカニズムを監視するか、物理的な保護を施し、悪意のある者が破損したり無効にしたりすることを阻止できます。</p> <p>機密エリアの例として、社内データベースサーバルーム、カード会員データが保存されている小売店舗のバックオフィスルーム、大量のカード会員データの保管エリアなどがあります。各組織で機密エリアを特定し、適切な物理監視制御が実施されていることを確認します。</p>

PCI DSS 要件	テスト手順	ガイダンス
<p>9.1.2 物理/論理制御を実施することで、誰でもアクセス可能なネットワークジャックへのアクセスを制限する。</p> <p>例えば、公共の場や訪問者がアクセス可能なエリアにあるネットワークジャックは、無効にしておき、ネットワークへのアクセスが明示的に承認されている場合にのみ有効にすることができる。または、アクティブなネットワークジャックがあるエリアでは訪問者に常に同行者をつけるプロセスを実施できる。</p>	<p>9.1.2 責任者をインタビューし、誰でもアクセスできる場所にあるネットワークジャックの場所を観察して、物理/論理制御が備わっており、誰でもアクセスできる場所にあるネットワークジャックへのアクセスを制限していることを確認する。</p>	<p>ネットワークジャック（またはネットワークポート）へのアクセスを制限すると、悪意のある者が差し込み可能なネットワークジャックを利用して内部ネットワークリソースにアクセスするのを防ぐことができます。</p> <p>論理制御か物理制御か、またはその組み合わせいかかわらず、明示的な許可を持つ個人がデバイスをネットワークに接続するのを防止できるものでなければなりません。</p>
<p>9.1.3 ワイヤレスアクセスポイント、ゲートウェイ、ハンドヘルドデバイス、ネットワーク/通信ハードウェア、および電気通信回線への物理アクセスを制限する。</p>	<p>9.1.3 ワイヤレスアクセスポイント、ゲートウェイ、ハンドヘルドデバイス、ネットワーク/通信ハードウェア、および電気通信回線への物理的なアクセスが適切に制限されていることを確認する。</p>	<p>ワイヤレスコンポーネントおよびデバイスへのアクセスに対するセキュリティがないと、悪意のある者は、組織の無人ワイヤレスデバイスを使用してネットワークリソースにアクセスしたり、さらには自身のデバイスをワイヤレスネットワークに接続して不正アクセスしたりすることができます。また、ネットワークと通信ハードウェアをセキュリティ保護することにより、悪意のある者がネットワークトラフィックを傍受したり、自身のデバイスをワイヤード（有線）ネットワークリソースに物理的に接続したりすることを防止できます。</p>
<p>9.2 次のようにオンサイト要員と訪問者を容易に区別できるような手順を開発する。</p> <ul style="list-style-type: none"> ▪ オンサイト要員と訪問者を識別する（バッジの使用など） ▪ アクセス要件を変更する ▪ 契約が終了したオンサイト要員や期限切れの訪問者の ID（バッジなど）を無効にする 	<p>9.2.a 文書化されたプロセスを調べて、オンサイト要員と訪問者を識別し、区別する手順が定義されていることを確認する。</p> <p>手順に以下が含まれていることを確認します。</p> <ul style="list-style-type: none"> • オンサイト要員と訪問者を識別する（バッジの使用など） • アクセス要件を変更する • 契約が終了したオンサイト要員や期限切れの訪問者の ID（バッジなど）を無効にする <p>9.2.b 識別方法（ID バッジなど）を実施し、オンサイト要員と訪問者を識別し、区別するプロセスを観察し、以下を確認する。</p> <ul style="list-style-type: none"> • 訪問者が明確に識別される • オンサイト要員と訪問者を容易に区別できる 	<p>承認された訪問者を識別し、オンサイト要員と容易に区別できるようにすることで、カード会員データが存在するエリアに不正な訪問者が出入りを許可されることを防止します。</p>

PCI DSS 要件	テスト手順	ガイダンス
9.3 オンサイト要員の機密エリアへの物理アクセスを次のように制御する。 <ul style="list-style-type: none"> • アクセスが個々の職務に基づいて許可される • 職務の終了後直ちにアクセスを無効とし、鍵、アクセスカードなどすべての物理アクセスメカニズムを返還するか無効にする 	<p>9.2.c 識別プロセス（バッジシステムなど）へのアクセスが、許可された担当者に制限されていることを確認する。</p> <p>9.3.a 機密エリアへの物理アクセス権を持つオンサイト要員のサンプルに対して、責任者をインタビューし、アクセス制御リストを見て、以下を確認する。 <ul style="list-style-type: none"> • 機密エリアへのアクセスが許可されている • アクセスがその個人の職務に必要 </p> <p>9.3.b 関係者による機密エリアへのアクセスを観察して、すべての関係者は、アクセスを許可される前に、承認が必要であることを確認する。</p> <p>9.3.c 最近退職した従業員のサンプルを選択し、アクセス制御リストを調べ、その従業員が機密エリアへの物理アクセスを持たないことを確認する。</p>	<p>機密エリアへの物理アクセスの制御により、業務上、正当な必要性のある承認された者だけがアクセスを許可されるようにすることができます。</p> <p>担当者が組織を離れるとき、すべての物理アクセスメカニズムを、退職後できるだけ速やかに返すか無効にして、退職後に機密エリアに物理的にアクセスできなくなる必要があります。</p>
9.4 訪問者を識別し、承認する手順を実施する。 手順には、以下を含める必要がある。	<p>9.4 訪問者の承認とアクセス制御が次のように行われていることを確認する。</p> <p>9.4.1.a 手順を観察し、担当者をインタビューすることで、訪問者は、カード会員データが処理または保守されているエリアに入ることに許可される前に承認が行われ、そのエリアにいる間ずっと同行者に付き添われていることを確認する。</p> <p>9.4.1.b 訪問者 ID バッジまたは他の ID の使用を観察して、物理トークンのバッジがカード会員データの処理または保守がされている物理エリアに同行者なしでアクセスできないことを確認する。</p> <p>9.4.2.a 施設内にいる人を観察し、訪問者バッジが使用されていて、訪問者とオンサイト要員を明確に区別できることを確認する。</p> <p>9.4.2.b 訪問者のバッジその他の ID が有効期限を過ぎると無効になることを確認する。</p> <p>9.4.3 施設を出る前、または期限が切れる日にバッジその他の ID の返還を求められる</p>	<p>訪問者管理は、権限のない人々や悪意のある者が施設（さらにカード会員データ）にアクセスするリスクを削減するために重要です。</p> <p>訪問者管理により、訪問者が入室を認められているエリアにのみ入室できること、担当者が行動を監視できるように訪問者として識別可能であること、およびアクセスが正当な訪問時間内のみに制限されることを確実にできます。</p> <p>期限が切れたか訪問が完了した時点で訪問者バッジが確実に返還されるようにすることで、悪意のある者が前に承認されたパスを使って訪問が終わった後に建物に侵入することを防止できます。</p> <p>訪問者に関する最小限の情報を文書化する訪問者ログは、容易に低成本で維持できます。また、建物または部屋への物理アクセス、およびカード会員データへのアクセスの可能性の識別に役立ちます。</p>

PCI DSS 要件	テスト手順	ガイダンス
<p>9.4.4 訪問者ログを使用して、コンピュータルームやデータセンターだけでなく、カード会員データの保存または送信が行われている施設への訪問者の行動の物理的監査証跡を保持する。</p> <p>訪問者の名前、所属会社、物理アクセスを承認したオンサイト要員をログに記録する。</p> <p>法律によって別途定められていない限り、このログを少なくとも 3 カ月間保管する。</p>	<p>9.4.4.a コンピュータルームやデータセンターだけでなく、カード会員データが保存または伝送される施設への物理アクセスの記録にも訪問者ログが使用されていることを確認する。</p> <p>9.4.4.b ログに以下が含まれていることを確認する。</p> <ul style="list-style-type: none"> • 訪問者名 • 所属会社 • 物理アクセスを承認したオンサイト要員 <p>9.4.4.c ログが 3 カ月以上保持されることを確認する。</p>	
<p>9.5 すべての媒体を物理的にセキュリティ保護する。</p>	<p>9.5 カード会員データを保護する手順に、すべての媒体（コンピュータ、リムーバブル電子媒体、紙の受領書、紙のレポート、FAX を含むがこれらに限定されない）のセキュリティを物理的に保護するための管理が含まれていることを確認する。</p>	<p>媒体を物理的にセキュリティ保護するための管理は、無許可の者がいかなる種類の媒体上にあるカード会員データへのアクセスもできなくすることを意図しています。カード会員データは、リムーバブルメディアまたはポータブルメディア上、印刷時、または誰かの机の上などに置かれ保護されていない場合、不正に表示、コピー、またはスキャンされやすくなります。</p>
<p>9.5.1 バックアップの入った媒体を安全な場所に保管する（代替またはバックアップサイト、商用ストレージ施設などのオフサイト施設が望ましい）。保管場所のセキュリティを少なくとも年に一度確認する。</p>	<p>9.5.1 バックアップメディアの保管が安全であることを確認するため、保管場所のセキュリティが少なくとも年に一度レビューされていることを確認する。</p>	<p>セキュリティで保護されていない施設に保存されている場合、カード会員データを含むバックアップは、紛失、盗難、または悪意のある目的でコピーされる可能性があります。</p> <p>保管場所を定期的にレビューすることにより、組織は検出されたセキュリティ上の問題をタイムリーに解決し、潜在的なリスクを最小限に抑えることができます。</p>
<p>9.6 次の項目を含め、あらゆるタイプの媒体を内部または外部に配布する際の厳格な管理を維持する。</p>	<p>9.6 媒体の配布を管理するためのポリシーが存在し、そのポリシーが、個人に配布されるものを含め、すべての配布媒体に対応していることを確認する。</p>	<p>手順とプロセスによって内部および外部ユーザに配布される媒体上のカード会員データを保護します。このような手順がないと、データが紛失または盗難に遭い、偽造目的で使用される可能性があります。</p>

PCI DSS 要件	テスト手順	ガイダンス
9.6.1 データの機密性を識別できるように、媒体を分類する。	9.6.1 データの機密性を決定することができるよう、すべての媒体が分類されていることを確認する。	分類ステータスを容易に識別できるように媒体を分類することが重要です。媒体を機密であることを識別しないと、適切な保護ができないことや、盗難または紛失が発生することがあります。 注：これは、媒体に「機密」というラベルが貼付される必要があるというわけではなく、組織が機密データを保存している媒体を識別して保護できるようすることを意味します。
9.6.2 安全な配達業者または正確に追跡することができるその他の方法によって媒体を送付する。	9.6.2.a 担当者をインタビューし、記録を調べて、施設の外部に送付されるすべての媒体がログに記録され、安全な配達業者または追跡可能なその他の配送方法によって送付されることを確認する。	通常郵便などの追跡不可能な方法で送付された場合、媒体が紛失または盗難に遭う可能性があります。カード会員データを格納した媒体の配送には安全な配達業者のサービスを使用し、組織が追跡システムを使用して配送品の在庫と場所を維持管理できるようにします。
	9.6.2.b すべての媒体の数日分のオフサイト追跡ログの最新サンプルを選択し、追跡の詳細がログに記録されていることを確認する。	
9.6.3 安全なエリアから移動されるすべての媒体を管理者が承認していることを確認する（媒体が個人に配布される場合を含む）。	9.6.3 すべての媒体の数日分のオフサイト追跡ログの最新サンプルを選択する。ログを調べ、責任者をインタビューすることで、媒体が安全なエリアから移動（媒体が個人に配達される場合を含む）されるたびに適切な管理者の承認が得られていることを確認する。	媒体の移動時にはすべて、媒体が安全なエリアから取り出される前に必ず承認されるという厳しいプロセスなしでは、媒体の追跡や適切な保護ができず、その場所が不明となり、媒体の紛失や盗難につながります。
9.7 媒体の保管およびアクセスについて、厳密な管理を維持する。	9.7 すべての媒体の保管と維持を管理するためのポリシー入手して調べ、ポリシーで定期的な媒体の在庫調査が要求されていることを確認する。	慎重な在庫管理方法と保管管理がないと、媒体の盗難または紛失に無限に気付かない可能性があります。
9.7.1 すべての媒体の在庫ログを保持し、少なくとも年に一度、媒体の在庫調査を実施する。	9.7.1 媒体の在庫ログを調べて、媒体の在庫調査が少なくとも年に一度行われていることを確認する。	媒体の在庫が管理されていない場合、媒体の盗難または紛失に長い間、またはまったく気付かない可能性があります。

PCI DSS 要件	テスト手順	ガイダンス
9.8 次のように、ビジネスまたは法律上不要になった媒体を破棄する。	9.8 定期的な媒体破棄ポリシーを調べて、すべての媒体が対象になっており、以下の要件が定義されていることを確認する。 <ul style="list-style-type: none"> • ハードコピー資料は再現できないことの合理的な保証が得られるように、クロスカット裁断、焼却、またはパルプ化する必要がある。 • 破棄する資料を保管する容器は安全でなければならない。 • 電子媒体上のカード会員データが、回復不能になっている必要がある。（例えば、安全な削除に関して業界が承認した標準に従った安全なワイププログラムによるか、または媒体の物理的な破壊によって） 	ハードディスク、ポータブルドライブ、CD/DVD、または紙面に含まれている情報を破棄するための手順が事前に講じられていない場合、破棄された媒体から悪意のある者が情報を取得し、データを侵害する可能性があります。例えば、悪意のある者は、「ダンプスターダイビング」と呼ばれる技法を使用して、ゴミ箱をあさり、見つけた情報を使用して攻撃を開始することができます。 破棄する予定の資料の保管に使用する容器を安全に保護することで、資料を収集するときに機密情報が盗みとられることを防止できます。例えば、「裁断予定」の容器に施錠し、中身にアクセスされるのを物理的に防止することができます。 電子媒体を安全に破棄する方法の例として、安全な消去、消磁、物理的な破壊（ハードディスクの粉碎や裁断など）などがあります。
9.8.1 カード会員データを再現できないよう、ハードコピー資料を裁断、焼却、またはパルプ化する。破棄する資料を保管する容器を安全に保護する。	9.8.1.a 担当者をインタビューし、手順を調べて、ハードコピーの資料が再現できないことの合理的な保証が得られるように、クロスカット裁断、焼却、またはパルプ化されていることを確認する。	
	9.8.1.b 破棄される情報を含む資料の保管に使用されるコンテナを調べて、コンテナが安全に保護されていることを確認する。	
9.8.2 カード会員データを再現できないよう、電子媒体上のカード会員データを回復不能にする。	9.8.2 電子媒体上のカード会員データが、回復不能になっていることを確認する。（例えば、安全な削除に関して業界が承認した標準に従った安全なワイププログラムか、または媒体の物理的な破壊によって）	

PCI DSS 要件	テスト手順	ガイダンス
<p>9.9 カードの物理的な読み取りによってペイメントカードデータを取り込む装置を改ざんや不正置換から保護する。</p> <p>注: これには、カード（カードのスワイプやディップ）によるトランザクションに使用されるカード読み取り装置も含まれる。この要件は、コンピュータのキーボードやPOSのキーパッドのような手動キー入力コンポーネントには適用されない。</p>	<p>9.9 文書化されたポリシーと手順を調べ、以下が含まれていることを確認する。</p> <ul style="list-style-type: none"> デバイスのリストの管理 デバイスを定期的に検査して改ざんや不正置換がないか調べる 関係者にトレーニングを受けさせて、怪しい行動を識別し、デバイスの改ざんや不正置換を報告できるようにする 	<p>犯罪者は、カード読み取り装置や端末を盗難および/または操作することでカード会員データを盗み取ろうとします。例えば、カード読み取り装置や端末を盗んで持ち帰り、それに侵入する方法を見つけ出したり、合法的な装置を偽の装置で置き換えてカードが挿入されるたびにペイメントカード情報を送信させたりします。犯罪者はまた、装置の外側に「スキミング」コンポーネントを付けて、ペイメントカードが装置に挿入される前にその詳細を取り込まれます。例えば、追加のカードリーダーを合法的なカードリーダーの上に取り付けてペイメントカードの詳細が一度犯罪者の取り付けたカードリーダーで、2度目は合法的なカードリーダーで、合計2度取り込まれるようにするという手をとります。この方法では、犯罪者がペイメントカードの情報を「スキミング」してもトランザクションは中断なく完了します。</p> <p>この要件は推奨されますが、コンピュータのキーボードやPOSのキーパッドのような手動キー入力コンポーネントには必須ではありません。</p> <p>スキミングの防止に関する追加のベストプラクティスは PCI SSC の Web サイトをご覧ください。</p>
<p>9.9.1 装置のリストを保持する。リストには以下を含める必要がある。</p> <ul style="list-style-type: none"> 装置のメーカーと型式 装置の場所（装置が設置されている店舗の住所など） 装置の連番や他の一意識別方法 	<p>9.9.1.a 装置のリストを見て、以下が含まれていることを確認する。</p> <ul style="list-style-type: none"> 装置のメーカーと型式 装置の場所（装置が設置されている店舗の住所など） 装置の連番や他の一意識別方法 <p>9.9.1.b リストから装置のサンプルを選択して、装置本体および装置の場所を観察し、リストが正確で最新のものであることを確認する。</p> <p>9.9.1.c 担当者をインタビューすることで、装置が追加、移動、廃棄された場合に装置のリストが更新されることを確認する。</p>	<p>装置の最新リストを保持することで、組織は装置の設置場所を追跡でき、装置の紛失・損失があった場合に、迅速に特定できます。</p> <p>装置のリストを保持する方法は自動化（装置管理システムなど）することも手動で行うことも（電子的または紙面で文書化）できます。移動式装置の場合、装置の場所はその装置が割り当てられている関係者の名前にできます。</p>

PCI DSS 要件	テスト手順	ガイダンス
<p>9.9.2 定期的に装置の表面を検査して改ざん（カードスキマーの取り付けなど）や不正置換（連番など装置の特性を調べて偽の装置に差し替えられていないことを確認する）を検出する。</p> <p>注：装置が改ざんされたり不正置換されたりする兆候の例としては、予期していない付着物やケーブルが装置に差し込まれている、セキュリティラベルが無くなっていたり、変更されている、ケースが壊れていたり色が変わっている、あるいは連番その他の外部マーキングが変更されているなどがある。</p>	<p>9.9.2.a 文書化された手順を調べて、プロセスに以下が含まれるように定義されていることを確認する。</p> <ul style="list-style-type: none"> • 装置を検査する手順 • 検査の頻度 <p>9.9.2.b 責任者をインタビューし、検査プロセスを観察して、以下を確認する。</p> <ul style="list-style-type: none"> • 関係者が装置を検査する手順を知っている • すべての装置が改ざんや不正置換の形跡がないことを定期的に検査されている 	<p>装置を定期的に検査することで、装置の改ざんや不正置換をより早期に検出でき、偽の装置の使用による被害を最小限に抑えることができます。</p> <p>検査の種類は装置によって異なり、例えば、安全であることがわかっている装置の写真と比較して装置の現在の外観が元のものから変更されているかを調べることができます。他の方法として、セキュアなマーカーペン（紫外線マーカーなど）を使って、装置の表面と入口をマークして、装置の置換や改ざんされた場合にわかるようにします。犯罪者は装置の外側のケースを取り替えて改ざんを隠すことがよくあり、そのような場合にはこの方法は効果があります。装置ベンダも、装置が改ざんされているかを調べるためのセキュリティに関するガイダンスや「ハウツー」ガイドを提供できる場合があります。</p> <p>検査の頻度は、装置の場所や装置が接続されているか接続されていないかなどによって異なります。例えば、装置が公共の場にあり組織の関係者による監視がない場合には、装置が安全な場所に置かれている場合や一般からのアクセスが監視されている場合より頻繁に検査をすることになります。検査の種類および頻度は、年1回のリスク評価プロセスによって定義されているように、加盟店によって決定されます。</p>

PCI DSS 要件	テスト手順	ガイダンス
<p>9.9.3 関係者が装置の改ざんや不正置換の試みを認識できるようにトレーニングを実施する。トレーニングには以下を含める必要がある。</p> <ul style="list-style-type: none"> 第三者の修理・保守要員を名乗っている者に装置へのアクセスを許可する前に、身元を確認する。 検証なしで装置を設置、交換、返品しない。 装置の周辺での怪しい行動（知らない人が装置のプラグを抜いたり装置を開けたりする）に注意する 怪しい行動や装置が改ざんや不正置換された形跡がある場合には適切な関係者（マネージャーやセキュリティ要員など）に報告する 	<p>9.9.3.a販売場所の関係者用トレーニング材料を調べて、以下のトレーニングが含まれていることを確認する。</p> <ul style="list-style-type: none"> 第三者の修理・保守要員を名乗っている者に装置への変更、トラブルシューティングのためのアクセスを許可する前に、身元を確認する。 検証なしで装置を設置、交換、返品しない 装置の周辺での怪しい行動（知らない人が装置のプラグを抜いたり装置を開けたりする）に注意する すべての怪しい行動を適切な関係者（マネージャーやセキュリティ要員など）に報告する 怪しい行動や装置が改ざんや不正置換された形跡がある場合には適切な関係者（マネージャーやセキュリティ要員など）に報告する <p>9.9.3.b販売場所の関係者のサンプルをインタビューすることで、彼らがトレーニングを受けており、以下の手順を知っていることを確認します。</p> <ul style="list-style-type: none"> 第三者の修理・保守要員を名乗っている者に POS 装置への変更、トラブルシューティングのためのアクセスを許可する前に、身元を確認する。 検証なしで装置を設置、交換、返品しない POS 装置の周辺での怪しい行動（知らない人が装置のプラグを抜いたり装置を開けたりする）に注意する 怪しい行動や POS 装置が改ざんや不正置換された形跡がある場合には適切な関係者（マネージャーやセキュリティ要員など）に報告する 	<p>犯罪者は装置にアクセスするために、認定メンテナンス担当者を装うことがあります。装置へのアクセスを求めるすべての第三者にアクセスを許可する前に、必ず検証する必要があります。例えば、管理者への問合せや、メンテナンス会社（ベンダーやアクワイアラーなど）に電話して検証することなど。多くの犯罪者は、部分的な変装（工具入れの所持や、作業服を着用する）によって担当者をだまそうしたり、装置の場所についてよく知っていたりするため、関係者が常に手順に従うようにトレーニングを受ける必要があります。</p> <p>犯罪者がよく使用するもうひとつの手は、「新しい」システムを送り込んで、合法的なシステムと交換し、合法的なシステムを指定した住所宛てに「返品」するように指示してくることがあります。犯罪者は、装置を手に入れたいために返送料金を前払いすることさえあります。担当者は、装置の取り付け前や業務に使用する前に、必ず装置が正規品であることや、信頼できる場所から送付されていることを管理者やサプライヤに確認する必要があります。</p>
<p>9.10 カード会員データへの物理的アクセスを制限するためのセキュリティポリシーと操作手順が文書化されて使用されており、影響を受ける関係者全員に知られていることを、確実にする。</p>	<p>9.10 文書を調べ、担当者をインタビューすることで、カード会員データへの物理的アクセスを制限するためのセキュリティポリシーと操作手順が以下の要件を満たしていることを確認する。</p> <ul style="list-style-type: none"> 文書化されている 使用されている 影響を受ける関係者全員に知らされている 	<p>カード会員データと CDE システムへの物理的アクセスを継続的に制限するために、関係者はセキュリティポリシーと文書化されている操作手順を認識・順守する必要があります。</p>

ネットワークの定期的な監視およびテスト

要件 10: ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する

ログ記録メカニズムおよびユーザの行動を追跡する機能は、データへの侵害を防ぐ、検出する、またはその影響を最小限に抑えるうえで不可欠です。すべての環境でログが存在することにより、何か不具合が発生した場合に徹底的な追跡、警告、および分析が可能になります。侵害の原因の特定は、システムアクティビティログなしでは非常に困難です。

PCI DSS 要件	テスト手順	ガイダンス
10.1 システムコンポーネントへのすべてのアクセスを各ユーザにリンクする監査証跡を確立する	10.1 システム管理者の観察とインタビューを通じて、以下を確認する。 <ul style="list-style-type: none"> システムコンポーネントに対する監査証跡が有効になっていてアクティブであること システムコンポーネントへのアクセスを各ユーザにリンクする 	ユーザアクセスをアクセス先のシステムコンポーネントにリンクするプロセスまたはシステムを確立することが重要です。このシステムは、監査ログを生成し、疑わしいアクティビティを特定のユーザまで追跡する機能を提供します。
10.2 次のイベントを再現するために、すべてのシステムコンポーネントの自動監査証跡を実装する。	10.2 責任者のインタビュー、監査ログの調査、および監査ログ設定の調査を通じて、以下を実行する。	疑わしいアクティビティの監査証跡の生成は、システム管理者に警告を送信し、データを他の監視メカニズム（侵入検知システムなど）に送信し、インシデント後の追跡用の履歴証跡を提供します。次のイベントをログに記録することにより、組織は悪意のある行為の可能性を識別および追跡できます。
10.2.1 カード会員データへのすべての個人アクセス	10.2.1 カード会員データへのすべてのアクセスがログに記録されていることを確認する。	悪意のある者が CDE でシステムにアクセスできるユーザアカウント情報を取得することや、カード会員データにアクセスするために新しい不正なアカウントを作成する可能性があります。カード会員データへのすべての個人アクセスの記録から、侵害または悪用されている可能性があるアカウントを識別できます。
10.2.2 ルート権限または管理権限を持つ個人によって行われたすべてのアクション	10.2.2 ルートまたは管理者権限を持つ個人によって実施されたすべてのアクションが記録されていることを確認する。	高い権限を持つ「管理者」や「ルート」などのアカウントは、システムのセキュリティや本番環境機能に多大な影響を及ぼす可能性があります。実行されたアクティビティのログがなければ、組織は管理者権限の悪用によって生じた問題を追跡し、原因となる行為や個人を特定することができません。

PCI DSS 要件	テスト手順	ガイダンス
10.2.3 すべての監査証跡へのアクセス	10.2.3 すべての監査証跡へのアクセスがログ記録されることを確認する。	悪意のある者は、多くの場合、自身の行為を隠すために監査ログの変更を試みます。アクセスの記録があれば、組織はログの矛盾や改ざんの可能性を追跡して個人のアカウントを特定できます。ログにアクセスして変更、追加、削除を特定できることは、無許可の者が取ったステップを追跡するのに役立ちます。
10.2.4 無効な論理アクセス試行	10.2.4 無効な論理アクセス試行が記録されていることを確認する。	悪意のある者は、多くの場合、ターゲットとなるシステムに対する複数のアクセスを試みます。無効なログインが何度も試行された場合、不正ユーザが「総当たり」によるパスワードの推測を試行している可能性があります。
10.2.5 識別と認証メカニズムの使用および変更（新しいアカウントの作成、特権の昇格を含むがこれらに限定されない）、およびルートまたは管理者権限をもつアカウントの変更、追加、削除のすべて	10.2.5.a 識別および認証メカニズムの使用がログに記録されることを確認する。 10.2.5.b 特権の昇格がすべてログに記録されることを確認する 10.2.5.c ルートまたは管理者権限をもつアカウントの変更、追加、または削除がすべてログに記録されていることを確認する	インシデントの発生時点で誰がログオンしていたかがわからなければ、使用された可能性があるアカウントを特定できません。また、悪意のある者が認証をバイパスしたり、有効なアカウントになりますしたりする目的で認証管理の操作を試みる可能性もあります。
10.2.6 監査ログの初期化、停止、一時停止	10.2.6 以下がログに記録されていることを確認する。 <ul style="list-style-type: none"> • 監査ログの初期化 • 監査ログの停止と一時停止 	不正なアクティビティを実行する前に監査ログを停止する（または一時停止する）ことは、悪意のある者が検出から逃れるための一般的な手法です。監査ログの初期化は、ユーザが自身の行為を隠蔽するためにログ機能を無効にした可能性を示します。
10.2.7 システムレベルオブジェクトの作成および削除	10.2.7 システムレベルオブジェクトの作成および削除がログ記録されることを確認する。	マルウェアなどの悪意のあるソフトウェアは、多くの場合、システムの特定の機能や操作を制御するためにターゲットシステム上のシステムレベルオブジェクトを作成または置換します。データベーステーブルやストアドプロシージャなど、システムレベルのオブジェクトが作成または削除されるたびにログに記録することで、そのような変更が承認されたものであったかを判断しやすくなります。
10.3 イベントごとに、すべてのシステムコンポーネントについて少なくとも以下の監査証跡エントリを記録する。	10.3 インタビューと監査ログの観察を通じて、監査可能なイベント（10.2に記載）ごとに、以下を実行する。	10.2に記載されている監査可能なイベントに対してこれらの詳細を記録することにより、侵害の可能性を迅速に識別し、人物、内容、場所、

PCI DSS 要件	テスト手順	ガイダンス
10.3.1 ユーザ識別	10.3.1 ユーザ識別がログエントリに含まれることを確認する。	方法に関する十分な詳細を把握することができます。
10.3.2 イベントの種類	10.3.2 ログエントリにイベントの種類が含まれていることを確認する。	
10.3.3 日付と時刻	10.3.3 ログエントリに日付と時刻が含まれていることを確認する。	
10.3.4 成功または失敗を示す情報	10.3.4 ログエントリに成功または失敗を示す情報が含まれることを確認する。	
10.3.5 イベントの発生元	10.3.5 ログエントリにイベントの発生元が含まれていることを確認する。	
10.3.6 影響を受けるデータ、システムコンポーネント、またはリソースの ID または名前。	10.3.6 影響を受けるデータ、システムコンポーネント、またはリソースの ID または名前がログエントリに含まれることを確認する。	
10.4 時刻同期技術を使用してすべての重要なシステムクロックおよび時間を同期し、時間を取得、配布、保存するために以下の要件が実施されていることを確実にする。 注: ネットワークタイムプロトコル (NTP) は、時刻同期技術の一例である。	10.4 構成基準とプロセスを調べることで、時刻同期技術が実装され、PCI DSS の要件 6.1 と 6.2 に従って最新状態に保たれていることを確認する。	時刻同期技術は複数のシステムのクロックを同期するために使用されます。クロックが正しく同期されていない場合、他のシステムとのログファイルの比較および正確なイベント順序の設定が不可能にはならなくても、困難になります（これらは侵害が発生した場合のフォレンジック分析に不可欠です）。インシデント後のフォレンジックチームにとって、すべてのシステムの時刻の正確性と一貫性、および各アクティビティの時刻は、システムがどのように侵害されたかを判断するうえで重要です。
10.4.1 重要なシステムが正確で一貫性のある時刻をもっている。	10.4.1.a 組織内で正しい時刻を取得、配布、保存するプロセスを調べて、以下を確認する。 <ul style="list-style-type: none"> • 指定した中央タイムサーバが、外部ソースから時刻信号を受信し、外部ソースからの時刻信号は国際原子時または UTC に基づいている。 • 複数のタイムサーバがある場合、それらのタイムサーバが正確な時刻を保つためにお互いに通信する。 • システムは時刻情報を指定した中央タイムサーバからのみ受信する。 	

PCI DSS 要件	テスト手順	ガイダンス
	<p>10.4.1.b システムコンポーネントのサンプルに対して、時刻関係のシステムパラメータ設定を観察して、以下を確認する。</p> <ul style="list-style-type: none"> 指定した中央タイムサーバが、外部ソースから時刻信号を受信し、外部ソースからの時刻信号は国際原子時または UTCに基づいている 複数のタイムサーバが指定されている場合、指定した中央タイムサーバが正確な時刻を保つためにお互いに通信する システムは時刻情報を指定した中央タイムサーバからのみ受信する 	
10.4.2 時刻データが保護されている。	<p>10.4.2.a システム構成および時刻同期設定を調べて、時刻データへのアクセスは、業務上時刻データにアクセスする必要のある担当者のみに制限されていることを確認する。</p>	
	<p>10.4.2.b システム構成および時刻同期設定とプロセスを調べて、重要なシステムの時刻設定への変更が、ログ記録、監視、およびレビューされていることを確認する。</p>	
10.4.3 時刻設定は、業界で認知されている時刻ソースから受信されている。	<p>10.4.3 システム構成を調べて、タイムサーバが（悪意のある個人が時計を変更するのを防ぐために）業界で認知されている特定の外部ソースから時刻更新を受け付けることを確認する。（内部タイムサーバの不正使用を防ぐために）これらの更新を対称鍵で暗号化し、時刻更新が提供されるクライアントマシンの IP アドレスを指定するアクセス制御リストを作成することもできる。</p>	
10.5 変更できないよう監査証跡をセキュリティで保護する。	<p>10.5 システム管理者をインタビューし、システム構成とアクセス権限を調べて、次のように、監査証跡が変更できないようにセキュリティで保護されていることを確認する。</p>	多くの場合、ネットワークに侵入した悪意のある者は、監査ログを編集して自身の行動を隠そとします。監査ログを適切に保護しないことで、完全性、正確性、整合性が保証されず、侵害後の調査ツールとして役に立たないことがあります。

PCI DSS 要件	テスト手順	ガイダンス
10.5.1 仕事関連のニーズを持つ個人に監査証跡の表示を制限する。	10.5.1 仕事関連のニーズを持つ個人のみが監査証跡ファイルを表示できる。	監査ログの適切な保護には、強力なアクセス制御（ログへのアクセスを「必要な範囲」に基づいて制限する）と、ログを検索および変更しにくくするための物理的またはネットワーク分離の使用が含まれます。ログを変更するのが困難な一元管理のログサーバやメディアに即座にバックアップしておくと、システムが生成するログが悪用された場合でも、ログの保護を維持できます。
10.5.2 監査証跡ファイルを不正な変更から保護する。	10.5.2 アクセス制御メカニズム、物理的な分離、ネットワークの分離などによって、現在の監査証跡ファイルが不正な変更から保護されている。	
10.5.3 監査証跡ファイルは、変更が困難な一元管理ログサーバまたは媒体に即座にバックアップする。	10.5.3 現在の監査証跡ファイルは、変更が困難な一元管理ログサーバまたは媒体に即座にバックアップされる。	
10.5.4 外部に公開されているテクノロジのログを、安全な一元管理の内部ログサーバまたは媒体デバイス上に書き込む。	10.5.4 外部に公開されているテクノロジ（ワイヤレス、ファイアウォール、DNS、メールなど）のログが安全な一元管理される内部ログサーバまたは媒体に書き込まれる。	ワイヤレス、ファイアウォール、DNS、メールサーバなどの外部に公開されているテクノロジからのログを安全性がより高い内部ネットワーク内に書き込むことにより、これらのログは失われたり変更されたりするリスクが軽減されます。 ログは直接書き込むことも、外部システムから安全な内部システムまたは媒体にオフロードまたはコピーすることもできます。
10.5.5 ログに対してファイル整合性監視または変更検出ソフトウェアを使用して、既存のログデータを変更すると警告が生成されるようにする（ただし、新しいデータの追加は警告を発生させない）。	10.5.5 システム設定、監視対象ファイル、および監視作業からの結果を調べて、ログに対してファイル整合性監視または変更検出ソフトウェアが使用されていることを確認する。	ファイル整合性監視または検出システムは、重要なファイルへの変更を確認し、このような変更が検出されたときに通知します。ファイル整合性監視では、事業体は通常、定期的に変更されないが、変更される場合は侵害の可能性を示すファイルを監視します。

PCI DSS 要件	テスト手順	ガイダンス
<p>10.6 すべてのシステムコンポーネントのログとセキュリティイベントを調べ、異常や怪しい活動を特定する。</p> <p>注:この要件に準拠するために、ログの収集、解析、および警告ツールを使用することができます。</p>	<p>10.6 以下のことを実行します。</p>	<p>多くの侵害は、検出されるまでに数日または数カ月かけて行われています。担当者によるか自動化された日常的なログのレビューにより、カード会員データ環境への不正アクセスを特定し、未然に対処できるようになります。</p> <p>ログレビュープロセスは手動にする必要はありません。ログの収集、解析、および警告ツールの使用により、レビューを必要とするログイベントが特定されるため、プロセスを実施しやすくなります。</p>
<p>10.6.1 每日一度以上以下をレビューする</p> <ul style="list-style-type: none"> • すべてのセキュリティイベント • CHD や SAD を保存、処理、または送信するすべてのシステムコンポーネントのログ • すべての重要なシステムコンポーネントのログ • すべてのサーバとセキュリティ機能を実行するシステムコンポーネント（ファイアウォール、侵入検出システム/侵入防止システム（IDS/IPS）、認証サーバ、電子商取引リダイレクションサーバなど）のログ 	<p>10.6.1.a セキュリティポリシーと手順を調べて、手動またはログツールを用いて、以下を少なくとも毎日一度レビューする手順が定義されていることを確認する。</p> <ul style="list-style-type: none"> • すべてのセキュリティイベント • CHD や SAD を保存、処理、または送信するすべてのシステムコンポーネントのログ • すべての重要なシステムコンポーネントのログ • すべてのサーバとセキュリティ機能を実行するシステムコンポーネント（ファイアウォール、侵入検出システム/侵入防止システム（IDS/IPS）、認証サーバ、電子商取引リダイレクションサーバなど）のログ <p>10.6.1.b プロセスを観察し、担当者をインタビューすることで、以下が少なくとも毎日一度レビューされていることを確認する。</p> <ul style="list-style-type: none"> • すべてのセキュリティイベント • CHD や SAD を保存、処理、または送信するすべてのシステムコンポーネントのログ • すべての重要なシステムコンポーネントのログ • すべてのサーバとセキュリティ機能を実行するシステムコンポーネント（ファイアウォール、侵入検出システム/侵入防止システム（IDS/IPS）、認証サーバ、電子商取引リダイレクションサーバなど）のログ 	<p>ログを毎日確認することで、侵害の可能性が明らかになるまでの時間と露出を最小限に抑えることができます。</p> <p>セキュリティイベント（例えば、怪しいまたは異常な行動を特定する通知やアラート）や重要システムコンポーネントからのログ、セキュリティ機能を実行するシステムからのログ（ファイアウォール、IDS/IPS、ファイル整合性監視（FIM）システムなど）といったセキュリティイベントを毎日レビューすることは、発生する可能性がある問題を特定するのに欠かせません。</p>

PCI DSS 要件	テスト手順	ガイダンス
10.6.2 組織のポリシー、および年間リスク評価によって決定されたリスク管理戦略に基づいて他のすべてのシステムコンポーネントのログを定期的にレビューする	<p>10.6.2.a セキュリティポリシーと手順を調べて、組織のポリシーとリスク管理戦略に基づき定期的に、他のすべてのシステムコンポーネントのログを、手動またはログツールを用いて、レビューする手順が定義されていることを確認する。</p> <p>10.6.2.b 組織のリスク評価文書を調べ、担当者をインタビューして、レビューが組織のポリシーとリスク管理戦略に従って実施されていることを確認する。</p>	他のすべてのシステムコンポーネントのログも定期的にレビューして、潜在的な問題や機密性の低いシステムから機密システムにアクセスしようとする試みの兆候を識別することが必要です。レビュー頻度は、事業体の年間リスク評価によって決定します。
10.6.3 レビュープロセスで特定された例外と異常をフォローアップする。	<p>10.6.3.a セキュリティポリシーと手順を調べて、レビュープロセスで特定された例外と異常をフォローアップする手順が定義されていることを確認する。</p> <p>10.6.3.b プロセスを観察し、担当者をインタビューすることで、例外と異常のフォローアップが実施されていることを確認する。</p>	ログのレビュープロセスで特定された例外と異常をフォローアップしないと、事業体は無許可で潜在的に悪意のある行動が自社のネットワーク内で発生していることに気づかない可能性があります。
10.7 監査証跡の履歴を少なくとも 1 年間保持する。少なくとも 3 カ月はすぐに分析できる状態にしておく（オンライン、アーカイブ、バックアップから復元可能など）。	<p>10.7.a セキュリティポリシーと手順を調べ、以下が定義されていることを確認する。</p> <ul style="list-style-type: none"> • 監査ログ保存ポリシー • 監査ログを少なくとも 1 年間保持し、最低 3 カ月はすぐに使用できる状態にしておくための手順。 <p>10.7.b 担当者をインタビューし、監査ログを調べることで、監査ログが少なくとも 1 年間保持されていることを確認する。</p> <p>10.7.c 担当者をインタビューし、プロセスを観察することで、解析用に、少なくとも過去 3 カ月分のログが即座に利用可能であることを確認する。</p>	少なくとも 1 年間ログを保持することで、侵害が発生した、または発生していることに気付くまでにしばらくの間かかることが多いという事実に基づき、発生した可能性のある侵害と、システムが影響を受けた期間をより適切に判断するための十分なログ履歴を調査官に提供することができます。過去 3 カ月間のログをすぐに利用できるようにしておくことで、事業体はデータ侵害をすばやく識別し、影響を最小限に抑えることができます。ログをオフライン場所に保管すると、すぐに利用できず、ログデータの復元、分析の実行、および影響を受けたシステムまたはデータの識別に、より長い時間がかかる可能性があります。

PCI DSS 要件	テスト手順	ガイダンス
<p>10.8 サービスプロバイダのための追加要件: 重要なセキュリティ対策システムの障害のタイムリーな検出および報告のためのプロセスを実装する、障害には以下を含むがこれらに限定されない:</p> <ul style="list-style-type: none"> • ファイアウォール • IDS/IPS • ファイル整合性監視 • アンチウイルス • 物理アクセス制御 • 論理アクセス制御 • 監査ログメカニズム • セグメンテーション制御（使用している場合） 	<p>10.8.a 文書化されたポリシーと手順を調べ、重要なセキュリティ対策システムの障害のタイムリーな検出および報告のためのプロセスが定義されていることを確認する。障害には以下を含むがこれらに限定されない:</p> <ul style="list-style-type: none"> • ファイアウォール • IDS/IPS • ファイル整合性監視 • アンチウイルス • 物理アクセス制御 • 論理アクセス制御 • 監査ログメカニズム • セグメンテーション制御（使用している場合） <p>10.8.b 検出および警告のプロセスを調べ、担当者をインタビューし、すべての重要なセキュリティ対策のためのプロセスが実装されていること、および重要なセキュリティ対策の障害に対して警告が生成されることを確認する。</p>	<p>注：この要件は評価対象の事業体がサービスプロバイダである場合のみに適用されます。</p> <p>重要なセキュリティ対策の障害を検出し、警告するための正式なプロセスがなければ、障害が長期間検出されない可能性があり、攻撃者がシステムを侵害し、カード会員データ環境から機密データを盗むために十分な時間を提供することにつながります。</p> <p>特定の障害タイプは、使用中のデバイスおよび技術の機能に依存して変化します。典型的な障害は、セキュリティ機能の動作が停止した場合や意図する方法で機能していないシステムが含まれます。例えば、ファイアウォールの場合、すべてのルールを消去することや、オフラインになることです。</p>
<p>10.8.1 サービスプロバイダのための追加要件: すべての重要なセキュリティ対策の障害についてタイムリーに対応する。セキュリティ対策の障害に対応するためのプロセスには以下を含む:</p> <ul style="list-style-type: none"> • セキュリティ機能の復旧 • セキュリティ障害の期間（開始から終了までの日付時刻）の識別および文書化 • 根本原因を含む障害の原因の識別と文書化、および根本原因に対応する改善案の文書化 • 障害中に発生したすべてのセキュリティ問題の識別および対応 • セキュリティ障害の結果としてさらなる活動が必要かどうか判断するためのリスク評価の実施 • 再発防止策の実装 • セキュリティ対策の監視の再開 	<p>10.8.1.a 文書化されたポリシーおよび手順を調べ、担当者をインタビューすることで、以下を含むセキュリティ対策の障害に対応するプロセスが定義され、実装されていることを確認する:</p> <ul style="list-style-type: none"> • セキュリティ機能の復旧 • セキュリティ障害の期間（開始から終了までの日付時刻）の識別および文書化 • 根本原因を含む障害の原因の識別と文書化、および根本原因に対応する改善案の文書化 • 障害中に発生したすべてのセキュリティ問題の識別および対応 • セキュリティ障害の結果としてさらなる活動が必要かどうか判断するためのリスク評価の実施 • 再発防止策の実装 • セキュリティ対策の監視の再開 <p>10.8.1.b 記録を調べ、以下を含むセキュリティ対策の障害が文書化されていることを確認する:</p> <ul style="list-style-type: none"> • 根本原因を含む障害原因の識別 • セキュリティ障害の期間（開始から終了までの日付時刻） • 根本原因に対応するために必要な改善方法の詳細 	<p>注：この要件は評価対象の事業体がサービスプロバイダである場合のみに適用されます。</p> <p>重要なセキュリティ対策の障害に対する警告が迅速かつ効果的な応答でない場合、攻撃者はこの時間を利用して悪意のあるソフトウェアを入れ込み、システムの制御を奪う、または事業体の環境からデータを窃取するかもしれません。</p> <p>文書化された証跡（例、問題管理システムの記録）はプロセスと手順がセキュリティ障害に対して適切な対応であることを支援するべきです。さらに、担当者は障害発生時の責任について認識するべきです。障害に対する活動および対応は、文書化された証跡として収集するべきです。</p>

PCI DSS 要件	テスト手順	ガイダンス
10.9 ネットワークリソースとカード会員データへのすべてのアクセスを監視するためのセキュリティポリシーと操作手順が文書化され、使用されており、影響を受ける関係者全員に知られていることを、確実にする。	<p>10.9 文書を調べ、担当者をインタビューすることで、ネットワークリソースとカード会員データへのすべてのアクセスを監視するためのセキュリティポリシーと操作手順が以下の要件を満たしていることを確認する。</p> <ul style="list-style-type: none"> • 文書化されている • 使用されている • 影響を受ける関係者全員に知られている 	ネットワークリソースとカード会員データへのすべてのアクセスを継続的に監視するために、関係者はセキュリティポリシーと日常の操作手順を認識・順守する必要があります。

要件 11: セキュリティシステムおよびプロセスを定期的にテストする。

脆弱性は、悪意のある個人や研究者によって絶えず検出されており、新しいソフトウェアによって広められています。システムコンポーネント、プロセス、およびカスタムソフトウェアを頻繁にテストして、セキュリティ管理が変化する環境に継続的に対応できるようにする必要があります。

PCI DSS 要件	テスト手順	ガイダンス
11.1 四半期ごとにワイヤレスアクセスポイントの存在をテストし (802.11) 、すべての承認されているワイヤレスアクセスポイントと承認されていないワイヤレスアクセスポイントを検出し識別するプロセスを実施する 注: プロセスで使用される方法には、ワイヤレスネットワークのスキャン、システムコンポーネントおよびインフラストラクチャの論理的/物理的な検査、ネットワークアクセス制御 (NAC) 、無線IDS/IPSが含まれるがこれらに限定されるわけではない。 いずれの方法を使用する場合も、承認されているデバイスと承認されていないデバイスを両方検出および識別できる機能を十分に備えている必要がある。	<p>11.1.a ポリシーと手順を調べ、四半期ごとに承認されているワイヤレスアクセスポイントと承認されていないワイヤレスアクセスポイントを両方検出し識別するプロセスが定義されていることを確認する。</p> <p>11.1.b 方法が、少なくとも以下を含むすべての不正なワイヤレスアクセスポイントを検出して識別するのに十分であることを確認する。</p> <ul style="list-style-type: none"> ▪ システムコンポーネントに挿入された WLAN カード ▪ ワイヤレスアクセスポイントを作成するためにシステムコンポーネントに (USB などで) 接続したポータブルやモバイルデバイス ▪ ネットワークポートまたはネットワークデバイスに接続されたワイヤレスデバイス <p>11.1.c ワイヤレススキャナを使用する場合、最近のワイヤレススキャナの出力を調べて、以下を確認する。</p> <ul style="list-style-type: none"> • 承認されているワイヤレスアクセスポイントと承認されていないワイヤレスアクセスポイントが識別される • すべてのシステムコンポーネントおよび施設に対し、このスキャナが少なくとも四半期ごとに実施されている <p>11.1.d 自動監視 (ワイヤレス IDS/IPS や NAC など) が使用されている場合は、担当者に通知するための警告が生成されるように構成されていることを確認する。</p>	<p>ネットワーク内でのワイヤレステクノロジの実装と利用は、悪意のある者がネットワークとカード会員データにアクセスするために使用するもっとも一般的な経路の 1 つです。ワイヤレスデバイスまたはネットワークが企業の知らない間にインストールされた場合、攻撃者はネットワークに容易に、かつ「認識されずに」侵入できます。不正なワイヤレスデバイスはコンピュータまたは他のシステムコンポーネント内に隠れているか、接続している可能性があります。または、ネットワークポートや、スイッチやルーターなどのネットワークデバイスに直接接続している可能性もあります。このような不正デバイスは環境内への不正なアクセスポイントになる可能性があります。</p> <p>どのワイヤレスデバイスが承認されているかがわかっていると、管理者は承認されていないワイヤレスデバイスを素早く特定でき、承認されていないワイヤレスアクセスポイントの ID に対応することで、悪意のある者への CDE のそれ以上の開示を予防することで被害を最小限にとどめることができます。</p> <p>ワイヤレスアクセスポイントをネットワークに簡単に接続できること、その存在を検出するのが困難なこと、および権限のないワイヤレスデバイスがもたらすリスクの増加により、ワイヤレステクノロジの使用を禁止するポリシーが存在する場合でも、これらのプロセスを実行する必要がありま</p>

PCI DSS 要件	テスト手順	ガイダンス
11.1.1 文書化されている業務上の理由を含め、承認されているワイヤレスアクセスポイントのインベントリを維持する。	11.1.1 文書化されている記録を調べて、承認されているワイヤレスアクセスポイントのインベントリが維持されており、すべての承認されているワイヤレスアクセスポイントに対して業務上の理由が文書化されていることを確認する。	す。 環境内に不正なワイヤレスアクセスポイントがインストールされていないことを確実にするための適切なツールとプロセスは、環境の規模と複雑度によって決まります。
11.1.2 承認されていないワイヤレスアクセスポイントが検出された場合のインシデント対応計画を実装する。	<p>11.1.2.a 組織のインシデント対応計画（要件 12.10）を調べて、承認されていないワイヤレスアクセスポイントが検出された場合に要求される対応が定義されていることを確認する。</p> <p>11.1.2.b 責任者をインタビューし、最近のワイヤレススキャンと関連する対応を調べて、承認されていないワイヤレスアクセスポイントが見つかった場合に対処されていることを確認する。</p>	例えば、ショッピングモール内の単独の小売キオスクの場合、すべての通信コンポーネントを改ざん防止機能の付いたケースに収容し、キオスクの詳細な物理検査を行うことで、不正なワイヤレスアクセスポイントが接続またはインストールされていないことを十分に確認できますが、複数のノードをもつ環境（大規模な小売店、コールセンター、サーバルーム、データセンターなど）の場合、詳細な物理検査を行うことは困難です。この場合、物理的なシステム検査とワイヤレスアナライザの結果を組み合わせるなど、複数の方法を組み合わせることで要件を満たすことが可能になります。

PCI DSS 要件	テスト手順	ガイダンス
<p>11.2 内部と外部ネットワークの脆弱性スキャンを少なくとも四半期に一度およびネットワークでの大幅な変更（新しいシステムコンポーネントのインストール、ネットワークトポジの変更、ファイアウォール規則の変更、製品アップグレードなど）後に実行する。</p> <p>注:四半期ごとのスキャンプロセスの複数のスキャンレポートをまとめて、すべてのシステムがスキャンされ、すべての脆弱性に対処されたことを示すことができる。未修正の脆弱性が対処中であることを確認するために、追加の文書が要求される場合がある。</p> <p>初期の PCI DSS 準拠では、評価者が 1) 最新のスキャン結果が合格スキャンであったこと、2) 事業体で四半期に一度のスキャンを要求するポリシーと手順が文書化されていること、および 3) スキャン結果で判明した脆弱性が修正されたことが再スキャンで示されたことを確認した場合、初回の PCI DSS 準拠のために、四半期に一度のスキャンに 4 回合格することは要求されない。初回 PCI DSS レビュー以降は毎年、四半期ごとのスキャンに 4 回合格しなければならない。</p>	<p>11.2 スキャンレポートと関連文書を調べて、内部および外部脆弱性スキャンが、次のように実行されていることを確認する。</p>	<p>脆弱性スキャンは、外部および内部のネットワークデバイスとサーバに対して実行される自動化または手動のツール、技術、および/または手法の組合せで、悪意のある者により発見されて利用される可能性があるネットワーク内の脆弱性の可能性を明らかにするよう設計されています。</p> <p>PCI DSS には、3 種類の脆弱性スキャンが要求されます。</p> <ul style="list-style-type: none"> 四半期ごとの内部脆弱性スキャン（有資格者が実施する、PCI SSC 認定スキャニングベンダー (ASV) の使用は要求されない） 四半期ごとの外部脆弱性スキャン（ASV が実施することが必要） 大幅な変更後に行う内部と外部のスキャン これらの弱点が識別されたら、事業体はこれを修正し、すべての脆弱性が修正されるまでスキャンを繰り返します。 <p>脆弱性をタイムリーに特定して対処することで、脆弱性が利用されてシステムコンポーネントやカード会員データが侵害される可能性は低下します。</p>
<p>11.2.1 四半期ごとの内部脆弱性スキャンを実施する。脆弱性に対処し、再スキャンを実施して、事業体の脆弱性ランク付け（要件 6.1 に基づく）に従ったすべての「高リスク」脆弱性が解決されたことを確認する。スキャンは有</p>	<p>11.2.1.a スキャンレポートをレビューし、四半期ごとの内部スキャンが過去 12 カ月間で 4 回行われたことを確認する。</p> <p>11.2.1.b スキャンレポートをレビューし、すべての「高リスク」脆弱性が対応されたことと、スキャンプロセスに「高リスク」脆弱性（PCI DSS 要件 6.1 で定義された）が解決されたことを確認する再スキャンが含まれることを確認する。</p>	<p>インターネットシステム上の内部システムの脆弱性を特定するために確立されたプロセスでは、四半期ごとの脆弱性スキャンを実施する必要があります。環境に最大のリスクをもたらす脆弱性（要件 6.1 に従って「高」にランク分けされた脆弱性など）は、最優先で解決する必要があります。</p>

PCI DSS 要件	テスト手順	ガイダンス
資格者が実施する必要がある。	11.2.1.c 担当者をインタビューすることで、スキャンが資格のある内部リソースまたは資格のある外部の第三者によって行われたこと、該当する場合は、テスターの組織の独立性（QSA や ASV である必要はない）が存在することを確認する。	内部の脆弱性スキャンは、スキャン対象となるシステムコンポーネントから適切に独立し、資格を与えられた内部スタッフによって実行できます（例えば、ファイアウォールの管理者がファイアウォールのスキャンを担当することは不適切です）。または、事業体は内部の脆弱性スキャンを、脆弱性スキャンの専門企業に委託することもできます。
11.2.2 四半期に一度の外部の脆弱性スキャンは、PCI (Payment Card Industry) セキュリティ基準審議会 (PCI SSC) によって資格を与えられた認定スキャニングベンダ (ASV) によって実行される必要がある。スキャンに合格するまで、必要に応じて再スキャンする。 注: 四半期に一度の外部の脆弱性スキャンは、PCI (Payment Card Industry) セキュリティ基準審議会 (PCI SSC) によって資格を与えられた認定スキャニングベンダ (ASV) によって実行される必要がある。 スキャンにおける顧客の責任、スキャンの準備などについては、PCI SSC Web サイトで公開されている『ASV プログラムガイド』を参照してください。	11.2.2.a 四半期ごとに行われた最新の 4 回の外部スキャンからの結果をレビューし、過去 12 カ月間で四半期ごとのスキャンが 4 回行われたことを確認する。 11.2.2.b 四半期ごとの外部スキャンと再スキャンの結果をレビューし、『ASV プログラムガイド』の要件（例えば、CVSS による 4.0 以上のレートの脆弱性がなく、自動エラーがない）を満たすことを確認する。 11.2.2.c スキャンレポートをレビューし、PCI SSC 認定スキャニングベンダ (ASV) がスキャンを完了したことを確認する。	外部ネットワークは侵害されるリスクがより高いため、四半期に一度の外部の脆弱性スキャンは PCI SSC 認定スキャニングベンダ (ASV) が実施する必要があります。堅実なスキャンの取り組みは、スキャンが実行され、脆弱性がタイムリーに対応されたことを確実にします。
11.2.3 大幅な変更があった後の内部と外部脆弱性スキャンを必要に応じて繰り返す。スキャンは有資格者が実施す	11.2.3.a 変更管理文書とスキャンレポートを調べて相関させ、大幅な変更の対象となるシステムコンポーネントがスキャンされたことを確認する。	大幅な変更が何を意味するかは、環境の構成によって大きく左右されます。アップグレードまたは変更が、カード会員データへのアクセスを許可

PCI DSS 要件	テスト手順	ガイダンス
る必要がある。	<p>11.2.3.b スキャンレポートをレビューし、スキャンプロセスに、以下の要件を満たすまで再スキャンを実行することが含まれていることを確認する。</p> <ul style="list-style-type: none"> ▪ 外部スキャンの場合、CVSS スコアで 4.0 以上の脆弱性がないこと。 ▪ 内部スキャンの場合、PCI DSS 要件 6.1 で定義されたすべての「高リスク」脆弱性が解消されていること。 <p>11.2.3.c スキャンが資格のある内部リソースまたは資格のある外部の第三者によって行われたこと、該当する場合は、データの組織の独立性（QSA や ASV である必要はない）が存在することを確認する。</p>	<p>する、またはカード会員データ環境のセキュリティに影響を与える場合は、大幅の変更とることができます。</p> <p>大幅な変更を行った後に環境をスキャンすることにより、変更是適切に完了し、変更によって環境のセキュリティが損なわれていないことを確認できます。変更の影響を受けたすべてのシステムコンポーネントをスキャンする必要があります。</p>

PCI DSS 要件	テスト手順	ガイダンス
<p>11.3 少なくとも以下を含むペネトレーションテスト方法を開発し、実装する。</p> <ul style="list-style-type: none"> 業界承認のペネトレーションテスト方法(NIST SP800-115など)に基づいている CDE 境界と重要システム全体を対象とした対応を含める ネットワークの内部と外部からの侵入テスト セグメンテーションと範囲減少制御の有効性テストを含める アプリケーション層のペネトレーションテストは、少なくとも要件 6.5 に記載されている脆弱性を含める必要がある ネットワーク層のペネトレーションテストには、ネットワーク機能とオペレーティングシステムをサポートするコンポーネントを含める必要がある 過去 12 カ月にあった脅威と脆弱性のレビューと考慮を含める ペネトレーションテスト結果と修正実施結果の保持を指定する 	<p>11.3 ペネトレーションテスト方法を調べ、責任者をインタビューすることで、この方法が実装されており少なくとも以下を含むことを確認する。</p> <ul style="list-style-type: none"> 業界承認のペネトレーションテスト方法に基づいている CDE 境界と重要システム全体を対象とした対応 ネットワークの内部と外部からの侵入テスト セグメンテーションと範囲減少制御の有効性テスト アプリケーション層のペネトレーションテストは、少なくとも要件 6.5 に記載されている脆弱性を含める必要がある ネットワーク層のペネトレーションテストには、ネットワーク機能とオペレーティングシステムをサポートするコンポーネントを含める必要がある 過去 12 カ月にあった脅威と脆弱性のレビューと考慮 ペネトレーションテスト結果と修正実施結果の保持を指定する 	<p>ペネトレーションテストの目的は、攻撃者が環境にどの程度まで侵入できるかを特定することを目標に、実際の攻撃の状況をシミュレーションすることです。これにより、事業体は露出の可能性をより的確に把握し、攻撃から防御するための戦略を策定できます。</p> <p>脆弱性スキャンとは異なり、ペネトレーションテストは、特定された脆弱性を利用するなどのアクティブラ探査です。脆弱性スキャンの実行はペネトレーションテスト者が攻撃の戦略を立てるために最初に行う手順の 1 つですが、唯一の手順ではありません。脆弱性スキャンによって既知の脆弱性が検出されなかった場合でも、多くの場合、ペネトレーションテスト者はセキュリティアップの可能性を特定するため、システムに関する十分な情報が得られます。</p> <p>ペネトレーションテストは一般に手動操作主体のプロセスです。場合によっては自動化ツールも使用可能ですが、テスト者はシステムに関する自らの知識を利用して環境に侵入します。多くの場合、テスト者は防御の層を突破することを目標にして数種類の利用手段を連結します。例えば、テスト者は、アプリケーションサーバにアクセスする手段を見つけると、侵害されたサーバを、そのサーバがアクセスできるリソースに基づいて新しい攻撃を行うためのポイントとして使用します。このようにして、テスト者は環境内で弱点となる可能性がある領域を特定するために、攻撃者が行う方法をシミュレーションできます。</p> <p>ペネトレーションテストの手法は、異なる組織によって変わり、テストの種類、深度、複雑さは、特定の環境と組織のリスク評価によって異なります。</p>

PCI DSS 要件	テスト手順	ガイダンス
11.3.1 外部のペネトレーションテストを少なくとも年に一度および大幅なインフラストラクチャまたはアプリケーションのアップグレードや変更（オペレーティングシステムのアップグレード、環境へのサブネットワークの追加、環境への Web サーバの追加など）後に実行する。	<p>11.3.1.a 最新の外部ペネトレーションテストの対象範囲と結果を調べて、ペネトレーションテストが以下を満たしていることを確認する。</p> <ul style="list-style-type: none"> 定義された方法に従っている 少なくとも年に一度実施する 環境に対して重大な変更が行われた後実施する <p>11.3.1.b テストが認定された内部リソースまたは認定された外部の第三者によって実行されたこと、および該当する場合はテスト者が組織的に独立した立場であること（QSA または ASV である必要はない）を確認する。</p>	<p>ペネトレーションテストを定期的および環境に大きな変更があったときに実施することは、悪意のある者が CDE にアクセスする可能性を最小限にとどめるための予防的なセキュリティ手段です。</p> <p>大幅なアップグレードや変更が何を意味するかは、環境の構成によって大きく左右されます。アップグレードや変更がカード会員データのアクセスを許可する、またはカード会員データ環境のセキュリティに影響する場合は、大幅なアップグレードや変更と見なされます。ネットワークのアップグレードや変更後にペネトレーションテストを実行すると、アップグレードや変更後も、実装されているコントロールが動作していることを確認できます。</p>
11.3.2 内部ペネトレーションテストを少なくとも年に一度および大幅なインフラストラクチャまたはアプリケーションのアップグレードや変更（オペレーティングシステムのアップグレード、環境へのサブネットワークの追加、環境への Web サーバの追加など）後に実行する。	<p>11.3.2.a 最新の内部ペネトレーションテストの結果を調べて、ペネトレーションテストが以下のとおり実行されていることを確認する。</p> <ul style="list-style-type: none"> 定義された方法に従っている 少なくとも年に一度実施する 環境に対して重大な変更が行われた後に実施する <p>11.3.2.b テストが認定された内部リソースまたは認定された外部の第三者によって実行されたこと、および該当する場合はテスト者が組織的に独立した立場であること（QSA または ASV である必要はない）を確認する。</p>	
11.3.3 ペネトレーションテストで検出された悪用可能な脆弱性が修正され、修正が確認されるまでテストを繰り返し行う。	11.3.3 ペネトレーションテストの結果を調べて、検出された悪用可能な脆弱性が修正され、修正が認められるまでテストが繰り返されたことを確認する。	

PCI DSS 要件	テスト手順	ガイダンス
<p>11.3.4 セグメンテーションを用いて CDE を他のネットワークから分離した場合、少なくとも年に一度セグメンテーションの制御/方法が変更された後にペネトレーションテストを行って、セグメンテーション方法が運用可能で効果的であり、CDE 内のシステムから適用範囲外のシステムをすべて分離することを確認する。</p>	<p>11.3.4.a セグメンテーション制御を調べ、ペネトレーションテスト方法をレビューして、ペネトレーションテスト手順ですべてのセグメンテーション方法をテストし、ペネトレーションテストを行って、セグメンテーション方法が運用可能で効果的であり、CDE 内のシステムから適用範囲外のシステムをすべて分離することを確認する。</p> <p>11.3.4.b 最新のペネトレーションテストからの結果を調べて、以下を満たしていることを確認する。</p> <ul style="list-style-type: none"> セグメンテーション制御を確認するペネトレーションテストが少なくとも年 1 回およびセグメンテーション制御/方法に何らかの変更を加えた後に実施されている ペネトレーションテストが、利用中のすべてのセグメンテーション制御/方法を対象としている ペネトレーションテストにより、セグメンテーション方法が運用可能で効果的であり、CDE 内システムから対象範囲外システムを分離していることを確認している <p>11.3.4.c 認定された内部リソースまたは外部の第三者によってテストが実施されたこと、および該当する場合はテスターが組織的に独立した立場であること（QSA や ASV である必要はない）を確認する。</p>	<p>ペネトレーションテストは、他のネットワークから CDE を隔離する任意のセグメント化が有効であることを確認するための重要なツールである。ペネトレーションテストは、事業体ネットワークの外部、およびネットワーク内部だが CDE の外部の両方のセグメンテーション制御に焦点を当て、セグメンテーション制御を通過して CDE にアクセスできないことを確認する必要がある。例えば、ネットワークテスト/オープンポートのスキャンにより、対象範囲内外のネットワーク間に接続がないことを確認する。</p>
<p>11.3.4.1 サービスプロバイダのための追加要件：セグメンテーションを使用している場合、少なくとも 6 カ月ごと、およびセグメンテーション制御/方法の変更後にセグメンテーション制御に対してペネトレーションテストを実施することで PCI DSS 対象範囲を確認する。</p>	<p>11.3.4.1.a 最近のペネトレーションテストの結果を調べ、以下を確認する：</p> <ul style="list-style-type: none"> ペネトレーションテストが実行され、少なくとも 6 カ月ごと、および任意のセグメンテーション制御/方法の変更後にセグメンテーション制御を確認する。 ペネトレーションテストが、使用されているすべてのセグメンテーション制御/方法を対象としている。 ペネトレーションテストによりセグメンテーション方法が運用可能で効果的であり、CDE 内システムからすべての対象範囲外システムを分離していることを確認する。 	<p>注：この要件は評価対象の事業体がサービスプロバイダの場合のみ適用されます。</p> <p>サービスプロバイダの PCI DSS 対象範囲の検証は、PCI DSS 対象範囲が最新になっていることや、変化するビジネス目的に沿っていることを確実にするため、可能な限り頻繁に実施する必要があります。</p>

PCI DSS 要件	テスト手順	ガイダンス
<p>11.4 侵入検知システムや侵入防止手法を使用して、ネットワークへの侵入を検知および/または防止する。カード会員データ環境との境界およびカード会員データ環境内の重要なポイントを通過するすべてのトラフィックを監視し、侵害の疑いがある場合は担当者に警告する。</p> <p>すべての侵入検知および防止エンジン、ベースライン、シグネチャを最新状態に保つ。</p>	<p>11.3.4.1.b 認定された内部リソースまたは外部の第三者によってテストが実施されたこと、および該当する場合はテスターが組織的に独立した立場であること (QSA や ASV である必要はない) を確認する。</p> <p>11.4.a システム構成とネットワーク図を調べて、(侵入検知システムや侵入防止などの) 手法が使用されていて、すべてのトラフィックが監視されていることを確認する。</p> <ul style="list-style-type: none"> • カード会員データ環境の境界で • カード会員データ環境内の重要なポイントで <p>11.4.b システム構成を調べ、責任者をインタビューすることで、侵入検知や侵入防止が侵害の疑いを担当者に警告することを確認する。</p> <p>11.4.c 侵入検知や侵入防止手法の構成とベンダ文書を調べて、侵入検知や侵入防止手法が最適な保護を実現するためのベンダの指示に従って構成、保守、更新されていることを確認する。</p>	<p>侵入検知/侵入防止システム (IDS/IPS など) は、ネットワークに入って来るトラフィックを既知の「署名」や数千種類の侵害 (ハッカーツール、トロイの木馬、およびその他のマルウェア) と比較し、警告を送信し、侵害の試みが発生した場合は阻止します。これらのツールを使用する権限のないアクティビティを検出するためのプロアクティブな手法がないと、コンピュータリソースへの攻撃 (または悪用) についてリアルタイムで気付かない可能性があります。侵入の試みを阻止できるよう、これらの手法によって生成されるセキュリティに関する警告を監視する必要があります。</p>
<p>11.5 変更検出メカニズム (ファイル整合性監視ツールなど) を導入して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 (変更、追加、および削除を含む) を担当者に警告し、重要なファイルの比較を少なくとも週に一度実行するようにソフトウェアを構成する。</p> <p>注: 変更検知の目的において、通常重要なファイルは定期的に変更されないため、これらのファイルの変更は、システムの侵害や侵害のリスクの可能性を指し示し</p>	<p>11.5.a システム設定と監視されたファイルを観察し、監視活動の結果をレビューすることで、変更検出メカニズムが使用されていることを確認する。</p> <p>監視する必要があるファイルの例:</p> <ul style="list-style-type: none"> ▪ システム実行可能ファイル ▪ アプリケーション実行可能ファイル ▪ 構成およびパラメータファイル ▪ 集中的に保存されている、履歴またはアーカイブされた、ログおよび監査ファイル ▪ 事業体が指定した追加の重要ファイル (リスク評価その他の方法で) 	<p>ファイル整合性監視 (FIM) ツールなどの変更検出ソリューションは、重要なファイルへの変更、追加、および削除を調べ、このような変更が検出されたときに通知します。適切に実装されておらず、変更検出ソリューションの出力が監視されていない場合、悪意のある者により、構成ファイルの内容、オペレーティングシステムプログラム、またはアプリケーション実行可能ファイルが追加、削除、または変更される可能性があります。権限のない変更が検出されない場合、既存のセキュリティ管理が無効となり、通常の処理へ影響が認識されることなくカード会員データが盗まれ</p>

PCI DSS 要件	テスト手順	ガイダンス
ます。ファイル整合性監視製品などの変更検出メカニズムは通常、関連するオペレーティングシステム用の重要なファイルがあらかじめ設定されています。カスタムアプリケーションなどの他の重要なファイルは、事業体（加盟店、またはサービスプロバイダ）によって評価および定義されている必要があります。	11.5.b 重要なファイルの不正な変更（変更、追加、および削除を含む）を担当者に警告し、重要なファイルの比較を少なくとも週に1回実行するようにメカニズムが構成されていることを確認する。	る可能性があります。
11.5.1 変更検出ソリューションによって生成された警告に対応するプロセスを実装する。	11.5.1 担当者をインタビューすることで、すべての警告が調査され解決されたことを確認する。	
11.6 セキュリティ監視とテストに関するセキュリティポリシーと操作手順が文書化されて使用されており、影響を受ける関係者全員に知られていることを、確実にする。	11.6 文書を調べ、担当者をインタビューすることで、セキュリティ監視とテストに関するセキュリティポリシーと操作手順が以下の要件を満たしていることを確認する。 <ul style="list-style-type: none"> • 文書化されている • 使用されている • 影響を受ける関係者全員に知られている 	関係者は、セキュリティ監視とテストに関するセキュリティポリシーと操作手順を継続的に認識・順守する必要があります。

情報セキュリティポリシーの維持

要件 12: すべての担当者の情報セキュリティに対応するポリシーを維持する。

強力なセキュリティポリシーは、事業体全体でのセキュリティの方向性を設定し、担当者に対して期待される内容を示します。すべての担当者は、データの極秘性とその保護に関する自身の責任を認識する必要があります。要件 12において、「担当者」とは、フルタイムおよびパートタイムの従業員、一時的な従業員、事業体の敷地内に「常駐」しているか、またはカード会員データ環境にアクセスできる請負業者やコンサルタントのことです。

PCI DSS 要件	テスト手順	ガイダンス
12.1 セキュリティポリシーを確立、公開、維持、普及させる	12.1 情報セキュリティポリシーを調べて、ポリシーが公開され、すべての関係者（ベンダー、ビジネスパートナーを含む）に普及されていることを確認する。	企業の情報セキュリティポリシーは、もつとも貴重な資産を保護するセキュリティ手段を実装するためのロードマップを作成します。すべての担当者は、データの極秘性とその保護に関する自身の責任を認識する必要があります。
12.1.1 少なくとも年に一度セキュリティポリシーをレビューし、環境が変更された場合にポリシーを更新する。	12.1.1 情報セキュリティポリシーを少なくとも年に一度レビューし、ビジネス目標またはリスク環境への変更を反映するため、必要に応じて更新されていることを確認する。	セキュリティの脅威と保護方式は、急速に進化します。関連する変更を反映するようにセキュリティポリシーが更新されない場合、これらの脅威に対抗するための新しい保護方式が確立されません。
12.2 以下のリスク評価プロセスを実装する。 <ul style="list-style-type: none"> • 少なくとも年に一度と環境に大きな変更があった場合（買収、合併、移転など）に実施される • 重要なアセット、脅威、脆弱性を識別する • 正式な文書化されたリスク分析に至る (リスク評価方法の例としては、OCTAVE、ISO 27005、および NIST SP 800-30 があげられます、これらに限定されません。)	12.2.a 年に一度のリスク評価プロセスに以下の内容が文書化されていることを確認する： <ul style="list-style-type: none"> • 重要な資産、脅威、および脆弱性を識別する。 • 正式な文書化されたリスク分析に至る 12.2.b リスク評価文書をレビューし、リスク評価プロセスが少なくとも年に一度と大きな変更があった場合に実施されていることを確認する。	リスク評価によって、組織は業務に悪影響を及ぼす可能性がある脅威および関連する脆弱性を識別できます。異なるリスクの考慮事項の例として、サイバー犯罪、ウェブ攻撃、およびPOSのマルウェアが含まれます。さらに、リソースを効果的に割り当てて、認識された脅威の影響を受ける可能性を低下させるコントロールを実装できます。 リスク評価を少なくとも年に一度と大きな変更があった場合に実施することで、組織の変更、進化する脅威、傾向、テクノロジに関する情報を最新状態に保つことができます。

PCI DSS 要件	テスト手順	ガイダンス
<p>12.3 重要なテクノロジに関する使用ポリシーを作成して、これらのテクノロジの適切な使用を定義する</p> <p>注: 重要なテクノロジの例には、リモートアクセスおよびワイヤレステクノロジ、ノートパソコン、タブレット、リムーバブル電子メディア、電子メールの使用、インターネットの使用がありますが、これらに限定されません</p> <p>これらの使用ポリシーで以下を要求することを確認する。</p>	<p>12.3 重要なテクノロジに関する使用ポリシーを調べ、責任者をインタビューすることで、ポリシーが実装・順守されていることを確認する。</p>	<p>担当者の使用ポリシーでは、会社のポリシーである場合に特定のデバイスとその他のテクノロジの使用を禁止したり、正しい使用法と実装に関するガイダンスを担当者に提供したりすることができます。使用ポリシーがない場合、担当者は会社のポリシーに違反するテクノロジを使用する可能性があり、その結果、悪意のある者により重要なシステムとカード会員データへのアクセスが可能となります。</p>
12.3.1 権限を持つ関係者による明示的な承認	12.3.1 使用ポリシーが、テクノロジを使用するために、許可された当事者からの明示的な承認を要求していることを確認する。	これらのテクノロジの実装に対して適切な承認を要求しないと、担当者は、認識されたビジネスニーズに対するソリューションを実装し、知らずに重要なシステムとデータを悪意のある者にさらす大きなセキュリティホールを開いてしまう可能性があります。
12.3.2 テクノロジの使用に対する認証	12.3.2 使用ポリシーが、すべてのテクノロジの使用に、ユーザIDとパスワードまたはその他の認証項目（トークンなど）による認証を要求するプロセスを含んでいることを確認する。	テクノロジが適切な認証（ユーザIDとパスワード、トークン、VPNなど）なしで実装される場合、悪意のある者は、この保護されていないテクノロジを使用して、容易に重要なシステムとカード会員データにアクセスできます。
12.3.3 このようなすべてのデバイスおよびアクセスできる担当者のリスト	<p>12.3.3 使用するポリシーが、以下を定義していることを確認する：</p> <ul style="list-style-type: none"> • すべての重要なデバイスのリスト、および • デバイスの使用を許可された担当者のリスト 	悪意のある者は、物理セキュリティを侵害し、自身のデバイスをネットワーク上に「裏口」として配置する場合があります。従業員も、手順を無視してデバイスを設置する場合があります。デバイスへの適切なラベル添付を使用する正確な在庫管理により、未承認の設置をすばやく識別できます。

PCI DSS 要件	テスト手順	ガイダンス
12.3.4 デバイスの所有者、連絡先情報、目的を正確にその場で識別できる方法（ラベル付け、コーディング、デバイスのインベントリ）	12.3.4 使用ポリシーがデバイスの所有者、連絡先情報、目的を正確にその場で識別できる方法（ラベル付け、コーディング、デバイスのインベントリ）を定義することを確認する。	悪意のある者は、物理セキュリティを侵害し、自身のデバイスをネットワーク上に「裏口」として配置する場合があります。従業員も、手順を無視してデバイスを設置する場合があります。デバイスへの適切なラベル添付を使用する正確な在庫管理により、未承認の設置をすばやく識別できます。デバイスの正式な名前付け規則を確立することを検討し、確立された在庫管理に従ってすべてのデバイスをログに記録します。デバイスを所有者、連絡先情報、目的に関連付けられるコードなどの情報を記載した論理ラベルを使用することもできます。
12.3.5 テクノロジの許容される利用法	12.3.5 使用ポリシーが、テクノロジの許容される利用法を定義していることを確認する。	会社が承認したデバイスとテクノロジの許容されるビジネス用途と場所を定義することにより、会社は、悪意のある者が重要なシステムとカード会員データにアクセスするために利用する「裏口」が開かれないよう、構成と運用管理におけるギャップをより適切に管理および制御できます。
12.3.6 テクノロジの許容されるネットワーク上の場所	12.3.6 使用ポリシーが、テクノロジの許容されるネットワーク上の場所を定義していることを確認する。	
12.3.7 会社が承認した製品のリスト	12.3.7 使用ポリシーが、会社が承認した製品のリストを含むことを確認する。	
12.3.8 非アクティブ状態が特定の期間続いた後のリモートアクセステクノロジのセッションの自動切断	12.3.8.a 使用ポリシーが、非アクティブ状態が一定期間続いた後のリモートアクセステクノロジのセッションの自動切断を要求していることを確認する。 12.3.8.b リモートアクセステクノロジの構成を調べて、非アクティブ状態が一定期間続いた後にリモートアクセステクノロジのセッションが自動切断されることを確認する。	リモートアクセステクノロジは、重要なリソースとカード会員データへの「裏口」となることがあります。未使用時のリモートアクセステクノロジ（POS またはその他のベンダ、あるいはビジネスパートナーがシステムをサポートするために使用するテクノロジなど）を切断することで、ネットワークへのアクセスとリスクは最小限に抑えられます。
12.3.9 ベンダおよびビジネスパートナーには必要とする場合にのみリモートアクセステクノロジをアクティブ化し、使用後直ちに非アクティブ化する	12.3.9 使用ポリシーで、ベンダやビジネスパートナーが必要とする場合にのみリモートアクセステクノロジをアクティブ化し、使用後直ちに非アクティブ化することが要求されていることを確認する。	
12.3.10 リモートアクセステクノロジ経由でカード会員データにアクセスする担当者については、定義されたビジネスニーズのために明示的に承認されて	12.3.10.a 使用ポリシーで、リモートアクセステクノロジを介してカード会員データにアクセスする場合、このようなデータをローカルハードドライブやリムーバブル電子媒体にコピー、移動、保存することは禁止されていることを確認する。	カード会員データをローカルのパーソナルコンピュータやその他の媒体に保存したりコピーしたりしてはいけないという責任をすべての担当者に認識させるには、明示的に承認された担当者以外

PCI DSS 要件	テスト手順	ガイダンス
いない限り、ローカルハードドライブおよびリムーバブル電子媒体へのカード会員データのコピー、移動、保存を禁止する。承認されたビジネスニーズがある場合、使用ポリシーはデータが適用される PCI DSS 要件すべてに従って保護されることを要求する必要がある。	12.3.10.b 適切な承認を持つ担当者について、使用ポリシーが PCI DSS 要件に従って、カード会員データの保護を要求していることを確認する。	にこのような行動を明確に禁止するポリシーが必要です。カード会員データをローカルハードドライブその他の媒体に保存またはコピーする場合、適用されるすべての PCI DSS 要件に従うことが必要です。
12.4 セキュリティポリシーと手順が、すべての担当者に関する情報セキュリティ責任を明確に定義していることを確実にする。	12.4.a すべての担当者について、情報セキュリティを明確に定義する情報セキュリティポリシーを確認する。 12.4.b 責任者のサンプルをインタビューして、セキュリティポリシーを理解していることを確認する。	明確に定義されたセキュリティの役割と責任が割り当てられていないと、セキュリティグループとのやりとりが統一されず、テクノロジがセキュリティで保護されずに実装されたり、古くなったテクノロジや安全でないテクノロジが使用されたりします。
12.4.1 サービスプロバイダのための追加要件：経営層は以下を含むカード会員データの保護および PCI DSS 準拠プログラムのための責任を確立する： <ul style="list-style-type: none"> • PCI DSS 準拠の維持に関する全体的な責任 • PCI DSS 準拠プログラムおよび経営層とのコミュニケーションに関する憲章の定義 	12.4.1.a 文書を調べ、経営層が事業体の PCI DSS 準拠の維持に関する全体的な責任を割り当てていることを確認する。 12.4.1.b 会社の PCI DSS 憲章を調べ、PCI DSS 準拠プログラムの実施条件と経営層とのコミュニケーション条件を概説していることを確認する。	注：この要件は評価対象の事業体がサービスプロバイダの場合のみ適用されます。 経営層への PCI DSS 準拠の責任の割り当ては、経営レベルにおける PCI DSS 準拠プログラムの可視性を確実にし、プログラムの有効性と戦略的優先事項への影響を判断するための適切な質問の機会を与えます。PCI DSS 準拠プログラムの全体的な責任は、組織内の個々の役割および/またはビジネス部門に割り当てるこも可能です。 経営層は、執行役員、取締役会、または同等レベルが含まれます。具体的な職位は特定の組織構造に依存します。経営層に提供される詳細なレベルは、特定の組織や関係者に対して適切であるべきです。
12.5 個人またはチームに以下の情報セキュリティの責任を割り当てる。	12.5 情報セキュリティポリシーと手順を調べ、以下を確認する。 <ul style="list-style-type: none"> • 情報セキュリティが最高セキュリティ責任者またはマネージメントの他のセキュリティに詳しいメンバーに正式に割り当てられている。 • 以下の情報セキュリティ責任が明確かつ正式に割り当られている： 	情報セキュリティ管理について責任がある各個人またはチームは、特定のポリシーを通じて、その責任と関連タスクを明確に理解している必要があります。この説明責任がないと、プロセスにおけるギャップが重要なリソースまたはカード会員データへのアクセスを開放してしまう場合があります。
12.5.1 セキュリティポリシーおよび手続きを確立、文書化、配布する。	12.5.1 セキュリティポリシーと手順を確立、文書化、および配布する責任が、正式に割り当てられていることを確認する。	

PCI DSS 要件	テスト手順	ガイダンス
12.5.2 セキュリティの警告や情報を監視および分析し、適切な担当者に配布する。	12.5.2 セキュリティの警告を監視および分析し、情報を適切な情報セキュリティおよび部署管理担当者に配布する責任が、正式に割り当てられていることを確認する。	事業体は、セキュリティ任務の責任が割り当てられず遂行されない可能性を回避するために、主要な人員の配置および/または後継者育成計画を考慮する必要があります。
12.5.3 セキュリティインシデントの対応およびエスカレーション手順を確立、文書化、配布し、すべての状況にタイムリーかつ効率的に対処することを、確実にする。	12.5.3 セキュリティインシデントの対応およびエスカレーション手順を確立、文書化、および配布する責任が、正式に割り当てられていることを確認する。	
12.5.4 追加、削除、変更を含め、ユーザーアカウントを管理する	12.5.4 ユーザーアカウントの管理（追加、削除、変更）の責任と認証管理の責任が正式に割り当てられていることを確認する。	
12.5.5 すべてのデータへのアクセスを監視および管理する。	12.5.5 すべてのデータへのアクセスを監視および管理する責任が正式に割り当てられていることを確認する。	
12.6 カード会員データセキュリティポリシーおよび手順をすべての担当者が認識できるように正式なセキュリティ意識向上プログラムを実装する。	12.6.a 正式なセキュリティ意識向上プログラムを調べて、このプログラムがカード会員データセキュリティポリシーおよび手順をすべての担当者に認識させることができることを確認する。 12.6.b セキュリティ意識向上プログラム手順と文書を調べて、以下を実施する。	担当者がセキュリティ責任について教育されていない場合、実装されたセキュリティ対策およびプロセスが、ミスや意図的なアクションによって無効になる可能性があります。
12.6.1 担当者の教育を採用時および少なくとも年に一度行う。 注: 方法は、担当者の役割とカード会員データへのアクセスレベルに応じて異なる。	12.6.1.a セキュリティ意識向上プログラムが、担当者の意識向上と教育を図るため、複数の方法（例えば、ポスター、手紙、メモ、Webベースのトレーニング、会議、プロモーションなど）で提供されていることを確認する。 12.6.1.b 担当者が、採用時および少なくとも年に一度、セキュリティ意識向上トレーニングに参加していることを確認する。 12.6.1.c 担当者のサンプルをインタビューすることで、意識向上トレーニングを完了しており、カード会員データセキュリティの重要さを認識していることを確認する。	セキュリティに関する認識を高めるプログラムに定期的な再訓練セッションが含まれていないと、重要なセキュリティプロセスおよび手順が忘れられたり無視されたりして、重要なリソースおよびカード会員データの公開につながる可能性があります。
12.6.2 担当者は、少なくとも年に一度セキュリティポリシーおよび手順を読み、理解したことを書面または電子的に認める必要があることを、セキュリティ意識向上プログラムが要求していることを確認する。	12.6.2 担当者が、少なくとも年に一度セキュリティポリシーおよび手順を読み、理解したことを書面または電子的に認める必要があることを、セキュリティ意識向上プログラムが要求していることを確認する。	担当者の同意を書面または電子的に要求することは、担当者がセキュリティポリシー/手順に目を通して理解したこと、およびこれらのポリシーへの準拠を約束したこと、また今後も約束することを確認するのに役立ちます。

PCI DSS 要件	テスト手順	ガイダンス
<p>12.7 雇用する前に、可能性のある担当者を選別して、内部ソースからの攻撃リスクを最小限に抑える。（バックグラウンドチェックの例には、職歴、犯罪歴、信用履歴、経歴照会がある。）</p> <p>注:このような可能性のある担当者を、トランザクションの実施で一度に1つのカード番号にしかアクセスできないようなレジ係など、特定の役職に採用する場合は、この要件は推奨のみです。</p>	<p>12.7 人事部門の管理者に問い合わせて、カード会員データまたはカード会員データ環境にアクセスする可能性のある担当者については、雇用の前にバックグラウンドチェックが（地域法の制約内で）実施されることを確認する。</p>	<p>カード会員データへのアクセスを許可される予定の担当者を雇用する前に徹底的なバックグラウンドチェックを実行すると、不審な経歴または犯罪歴を持つ人々による PAN およびその他のカード会員データの不正使用のリスクが軽減されます。</p>
<p>12.8 カード会員データがサービスプロバイダと共有されるか、サービスプロバイダによってカード会員データのセキュリティに影響を及ぼされる可能性のある場合は、次の項目を含め、サービスプロバイダを管理するポリシーと手順を維持および実装する。</p>	<p>12.8 ポリシーと手順の観察とレビュー、関連文書のレビューを通して、カード会員データを共有するか、カード会員データのセキュリティに影響を及ぼす可能性のあるサービスプロバイダを次のように管理するプロセスが実装されていることを確認する。</p>	<p>加盟店またはサービスプロバイダがサービスプロバイダとカード会員データを共有する場合、特定の要件を適用して、このデータの保護がサービスプロバイダによって継続的に実施されることを確実にします。</p> <p>いくつかの異なる種類のサービスプロバイダの例としてバックアップテープの保管施設、Web ホスティング企業やセキュリティサービスプロバイダなどのマネージドサービスプロバイダ、不正行為事例の収集目的でデータを受信する事業体などがあります。</p>
<p>12.8.1 提供されるサービスの詳細を含むサービスプロバイダのリストを維持する。</p>	<p>12.8.1 サービスプロバイダのリストが維持されていること、提供されるサービスの詳細を含んでいることを確認する。</p>	<p>すべてのサービスプロバイダを追跡することで、リスクの可能性が組織の外部でどこまで広がるかを識別できます。</p>

PCI DSS 要件	テスト手順	ガイダンス
<p>12.8.2 サービスプロバイダが顧客に代わって所有、保存、処理、送信するカード会員データのセキュリティについて、または顧客のカード会員データのセキュリティに影響を与える範囲について、サービスプロバイダが責任を持つことを認める内容の書面による契約書を維持する。</p> <p>注: 同意の正確な言葉づかいは、提供されるサービスの詳細、各事業体に割り当てられる責任など、2つの事業体間の同意によって異なります。同意の正確な言葉づかいに、この要件で提供されているのと同じものを含める必要はありません。</p>	<p>12.8.2 書面による契約を調べて、サービスプロバイダが顧客に代わって所有、保存、処理、送信するカード会員データのセキュリティについて、または顧客のカード会員データのセキュリティに影響を与える範囲について、サービスプロバイダが責任を持つことを認める文面であることを確認する。</p>	<p>サービスプロバイダの同意は、クライアントから取得するカード会員データの適切なセキュリティを維持することに対するコミットメントの証拠となります。サービスプロバイダのカード会員データのセキュリティに関する責任範囲は特定のサービスやプロバイダと評価対象の事業体の間の合意に依存することになります。</p> <p>この要件は、要件 12.9 との関連で、両当事者に該当する PCI DSS 責任の理解の一貫したレベルを促進することを意図しています例えば、同意には、提供されるサービスの一部として維持される該当する PCI DSS 要件を含めることができます。</p>
<p>12.8.3 契約前の適切なデューデリジェンスを含め、サービスプロバイダとの契約に関するプロセスが確立されている。</p>	<p>12.8.3 サービスプロバイダとの契約前の適切なデューデリジェンスを含め、ポリシーと手順が文書化されて、実施されていることを確認する。</p>	<p>プロセスにより、サービスプロバイダの契約は組織によって内部で徹底的に精査されます。サービスプロバイダとの正式な契約関係を築く前のリスク分析を含める必要があります。</p> <p>具体的なデューデリジェンスプロセスと目標は各組織によって異なります。考慮事項の例としては、プロバイダのレポート方法、侵害通知、インシデント対応手順、PCI DSS 責任をどのように各当事者に割り当てるかについての詳細、プロバイダが PCI DSS への準拠を検証する方法、提供する証拠などがあります。</p>
<p>12.8.4 少なくとも年に一度、サービスプロバイダの PCI DSS 準拠ステータスを監視するプログラムを維持する。</p>	<p>12.8.4 事業体が、少なくとも年に一度そのサービスプロバイダの PCI DSS 準拠ステータスを監視するためのプログラムを維持していることを確認する。</p>	<p>サービスプロバイダの PCI DSS 準拠ステータスを知ることで、組織が従う要件と同じ要件にサービスプロバイダが準拠していることが確実となります。</p>

PCI DSS 要件	テスト手順	ガイダンス
<p>12.8.5 各サービスプロバイダに対し、どの PCI DSS 要件がサービスプロバイダによって管理され、どの PCI DSS 要件が事業体によって管理されるかについての情報を維持する。</p>	<p>12.8.5 各サービスプロバイダに対し、どの PCI DSS 要件がサービスプロバイダによって管理され、どの PCI DSS 要件が事業体によって管理されるかについての情報を事業体が維持していることを確認する。</p>	<p>す。サービスプロバイダがさまざまなサービスを提供している場合、この要件はクライアントに提供する、クライアントの PCI DSS 評価の範囲内にあるサービスに適用されます。</p> <p>事業体が維持する特定の情報は、サービスの種類など、プロバイダとの同意によって異なります。この意図は、評価される事業体が、どの PCI DSS 要件をプロバイダが満たすと同意しているかを理解することにあります。</p>
<p>12.9 サービスプロバイダのみの追加要件：顧客に代わって所有、保存、処理、送信するカード会員データのセキュリティについて、または顧客のカード会員データのセキュリティに影響を与える範囲について責任を持つことを認める内容の書面による契約書を維持する。</p> <p>注: 同意の正確な言葉づかいは、提供されるサービスの詳細、各事業体に割り当てられる責任など、2つの事業体間の同意によって異なります。同意の正確な言葉づかいに、この要件で提供されているのと同じものを含める必要はありません。</p>	<p>12.9 サービスプロバイダの評価のための追加のテスト手順：サービスプロバイダのポリシーと手順をレビューし、契約書に使用されるテンプレートを調べて、サービスプロバイダが、顧客のカード会員データを保持する、または他の方法で顧客の代わりに保存、処理、送信するか、顧客のカード会員データ環境のセキュリティに影響を与える業務範囲において該当するすべての PCI DSS 要件を順守することについて書面で同意していることを確認する。</p>	<p>注: この要件は、評価される事業体がサービスプロバイダである場合に適用されます。</p> <p>この要件は、要件 12.8.2 との関連で、両当事者に該当する PCI DSS 責任の理解の一貫したレベルを促進することを意図しています。サービスプロバイダの同意は、クライアントから取得するカード会員データの適切なセキュリティを維持することに対するコミットメントの証拠となります。</p> <p>サービスプロバイダの内部ポリシーとプロセスが顧客の契約プロセスと関連付けられており、契約書に使用されるテンプレートが、該当する PCI DSS 要件への同意の条項を含む必要があります。サービスプロバイダの応答文書を提供する方法は、プロバイダと顧客の間で合意する必要があります。</p>
<p>12.10 インシデント対応計画を実施する。システム侵害に直ちに対応できるよう準備する。</p>	<p>12.10 インシデント対応計画と関連手順を調べて、事業体がシステム侵害に対して以下を実施することで即時対応する用意があることを確認する。</p>	<p>責任を持つ関係者によって適切に周知され、読まれて、理解されている綿密なセキュリティインシデント対応計画がない場合、混乱や統一された対応の不足により、ビジネスのダウンタイム、公共メディアへの不要な公開、および新しい法的責任が増える可能性があります。</p>

PCI DSS 要件	テスト手順	ガイダンス
<p>12.10.1 システム侵害が発生した場合に実施されるインシデント対応計画を作成する。計画では、最低限、以下に対応する。</p> <ul style="list-style-type: none"> ▪ ペイメントブランドへの通知を最低限含む、侵害が発生した場合の役割、責任、および伝達と連絡に関する戦略 ▪ 具体的なインシデント対応手順 ▪ ビジネスの復旧および継続手順 ▪ データバックアッププロセス ▪ 侵害の報告に関する法的要件の分析 ▪ すべての重要なシステムコンポーネントを対象とした対応 ▪ ペイメントブランドによるインシデント対応手順の参照または包含 	<p>12.10.1.a インシデント対応計画に以下が含まれていることを確認する。</p> <ul style="list-style-type: none"> ▪ ペイメントブランドへの通知を最低限含む、侵害が発生した場合の役割、責任、および伝達に関する戦略 ▪ 具体的なインシデント対応手順 ▪ ビジネスの復旧および継続手順 ▪ データバックアッププロセス ▪ 侵害の報告に関する法的要件の分析（データベースにカリフォルニア在住者が含まれている企業に対し、実際の侵害または侵害の可能性が発生した場合に、影響を受ける消費者への通知を要求する California Bill 1386 など） ▪ すべての重要なシステムコンポーネントを対象とした対応 ▪ ペイメントブランドによるインシデント対応手順の参照または包含 <p>12.10.1.b 担当者をインタビューし、以前に報告されたインシデントや警告をレビューして、文書化されたインシデントレスポンス計画と手順に従っていることを確認する。</p>	インシデント対応計画は綿密で、カード会員データに影響を及ぼす可能性がある侵害が発生した場合に会社が効果的に対応できるようにするためのすべての主要要素が含まれている必要があります。
<p>12.10.2 少なくとも年に一度、要件 12.10.1 にあげられたすべての要素を含め、計画をレビューおよびテストする。</p>	<p>12.10.2 担当者をインタビューし、テスト文書をレビューすることで、少なくとも年に一度、計画がテストされていること、およびテストに要件 12.10.1 にあげられたすべての要素を含んでいることを確認する。</p>	適切なテストが行われないと、インシデント発生時の漏洩が増大する可能性がある主要な手順が見過ごされる場合があります。
<p>12.10.3 警告に 24 時間 365 日体制で対応できる担当者を指定する。</p>	<p>12.10.3 ポリシーの観察とレビュー、および責任者のインタビューを通じて、承認されていない活動、承認されていないワイヤレスアクセスポイントの検出、重要な IDS 警告、重要なシステムまたはコンテンツファイルの承認されていない変更の痕跡がないかどうかを調査するために、インシデント対応および監視が 24 時間体制で行われていることを確認する。</p>	訓練済みのすぐに対応できるインシデント対応チームがないと、ネットワークへの損害が拡大し、重要なデータとシステムが対象システムの不適切な処理によって「汚染」される可能性があります。これにより、インシデント後の調査が妨げられる可能性があります。
<p>12.10.4 セキュリティ侵害への対応を担当するスタッフに適切なトレーニングを提供する。</p>	<p>12.10.4 ポリシーの観察とレビュー、および責任者のインタビューを通じて、セキュリティ侵害への対応に責任を持つスタッフが定期的にトレーニングされていることを確認する。</p>	

PCI DSS 要件	テスト手順	ガイダンス
12.10.5 侵入検知、侵入防止、ファイア ウォール、ファイル整合性監視システムを含むがこれらに限定されない、セキュリティ監視システムからの警告を含める。	12.10.5 プロセスの観察とレビューを通じて、セキュリティ監視システムからの警告の監視および対応がインシデント対応計画に含まれていることを確認する。	これらの監視システムは、データへの可能性のあるリスクに焦点を合わせるように設計されており、侵害を防ぐための迅速な措置を講じるうえで重要で、インシデント対応プロセスに含める必要があります。
12.10.6 得られた教訓を踏まえてインシデント対応計画を変更および改善し、業界の動向を組み込むプロセスを作成する。	12.10.6 ポリシーの観察とレビュー、および責任者のインタビューを通じて、得られた教訓を踏まえてインシデント対応計画を変更および改善し、業界の動向を組み込むプロセスがあることを確認する。	インシデント後に「得られた教訓」をインシデント対応計画に組み込むことで、計画を最新状態に保ち、新たな脅威やセキュリティの傾向に対応することができます。
12.11 サービスプロバイダのための追加要件：担当者がセキュリティポリシーおよび運用手順に従っていることを確認するため、少なくとも四半期ごとにレビューを実施する。レビューでは以下のプロセスを対象に含む必要がある： <ul style="list-style-type: none"> • 日次のログレビュー • ファイアウォールのルールセットのレビュー • 新たなシステムへの構成基準の適用 • セキュリティ警告への対応 • 変更管理プロセス 	<p>12.11.a ポリシーおよび手順を調べ、担当者がセキュリティポリシーおよび運用手順に従っていることをレビューし、確認するプロセスが定義されていることを確認する。レビューには以下を対象に含む：</p> <ul style="list-style-type: none"> • 日次のログレビュー • ファイアウォールのルールセットのレビュー • 新たなシステムへの構成基準の適用 • セキュリティ警告への対応 • 変更管理プロセス <p>12.11.b 責任者をインタビューし、レビューの記録を調べることで、少なくとも四半期ごとにレビューが実施されていることを確認する。</p>	<p>注：この要件は評価対象の事業体がサービスプロバイダの場合のみ適用されます。 セキュリティポリシーおよび手順に従っていることを定期的に確認することで、期待する制御がアクティブで、かつ意図したとおりに機能していることの保証を提供します。 これらのレビューの目的は他の PCI DSS 要件を再評価することではなく、手順が期待するとおり、守られているかどうかを確認することです。</p>
12.11.1 サービスプロバイダのための追加要件：以下を含む四半期ごとのレビュープロセスの文書が維持されている： <ul style="list-style-type: none"> • レビュー結果の文書化 • PCI DSS 準拠プログラムに責任をもつ担当者による結果のレビューおよび承認 	12.11.1 四半期ごとのレビュー文書を調べ、以下が含まれていることを確認する： <ul style="list-style-type: none"> • レビュー結果の文書化 • PCI DSS 準拠プログラムに責任をもつ担当者による結果のレビューおよび承認 	<p>注：この要件は評価対象の事業体がサービスプロバイダの場合のみ適用されます。 これらの独立したチェックの意図は、セキュリティ活動が継続的に実施されているかどうかを確認することです。 これらのレビューは、事業体の次回の PCI DSS 評価の準備を支援するために、例えば、監査ログ、脆弱性スキャンレポート、ファイアウォールのレビューなどの適切な証拠が維持されていることの確認にも使用することができます。</p>

付録 A: 追加の PCI DSS 要件

この付録は異なる事業体の種類に対する追加の PCI DSS 要件が含まれています。この付録のセクションには以下が含まれています：

- 付録 A1: 共有ホスティングプロバイダ向けの PCI DSS 追加要件
- 付録 A2: カード提示 POS POI 端末接続用に SSL / 初期の TLS を使用する事業体向けの PCI DSS 追加要件
- 付録 A3: 指定事業体向け追加検証

ガイダンスおよび適用可能な情報は各セクションで提供されます。

付録 A1: 共有ホスティングプロバイダ向けの PCI DSS 追加要件

要件 12.8 と 12.9 に言及されているとおり、カード会員データにアクセスするすべてのサービスプロバイダ（共有ホスティングプロバイダを含む）は PCI DSS に従う必要があります。さらに、要件 2.6 には、共有ホスティングプロバイダは各事業体のホストされている環境およびデータを保護する必要があると記載されています。したがって、共有ホスティングプロバイダは、加えてこの付録に記載されている要件に従う必要があります。

A1 要件	テスト手順	ガイダンス
A1 各事業体（加盟店、サービスプロバイダ、またはその他の事業体）のホスト環境とデータを、A1.1～A1.4 に従って保護する。 ホスティングプロバイダは、これらの要件および PCI DSS のその他すべての関連セクションを満たす必要があります。 注: ホスティングプロバイダがこれらの要件を満たすことができたとしても、そのホスティングプロバイダを使用する事業体の準拠が保証されるわけではありません。各事業体は、PCI DSS に従い、準拠を適宜検証する必要があります。	A1 共有ホスティングプロバイダの PCI DSS 評価の場合、共有ホスティングプロバイダが事業体（加盟店およびサービスプロバイダ）のホストされている環境およびデータを保護していることを確認するために、ホストされている加盟店およびサービスプロバイダの代表サンプルからサーバのサンプル（Microsoft Windows および Unix/Linux）を選択し、以下の A1.1～A1.4 を実行する。	PCI DSS の付録 A は、顧客である加盟店やサービスプロバイダに PCI DSS 準拠のホスティング環境を提供することを希望する共有ホスティングプロバイダを対象としています。
A1.1 各事業体が、その事業体のカード会員データ環境にアクセスするプロセスのみを実行するようにする。 <ul style="list-style-type: none"> システム上のどの事業体も、共有 Web サーバユーザ ID を使用できない。 事業体が使用するすべての CGI スクリプトは、その事業体の一意のユーザ ID を使用して作成され実行される必要がある。 	A1.1 共有ホスティングプロバイダが事業体（加盟店やサービスプロバイダなど）に独自のアプリケーションの実行を許可する場合は、これらのアプリケーションプロセスが事業体の一意の ID を使用して実行されることを確認する。例: <ul style="list-style-type: none"> システム上のどの事業体も、共有 Web サーバユーザ ID を使用できない。 事業体が使用するすべての CGI スクリプトは、その事業体の一意のユーザ ID を使用して作成され実行される必要がある。 	加盟店またはサービスプロバイダが共有サーバ上で独自のアプリケーションを実行することを許可されている場合、これらのアプリケーションは特権ユーザではなく加盟店またはサービスプロバイダのユーザ ID を使用して実行する必要があります。

A1 要件	テスト手順	ガイダンス
A1.2 各事業体のアクセスおよび特権が、その事業体のカード会員データ環境のみに制限されている。	<p>A1.2.a アプリケーションプロセスのユーザ ID が、特権ユーザ（ルート/管理者）ではないことを確認する。</p> <p>A1.2.b 各事業体（加盟店、サービスプロバイダ）が、その事業体が所有するファイルおよびディレクトリに対して、または必要なシステムファイルに対してのみ、読み取り、書き込み、または実行許可を持つ（ファイルシステムアクセス権限、アクセス制御リスト、chroot、jailshellなどによって制限される）ことを確認する。</p> <p>重要:事業体のファイルをグループで共有することはできません。</p> <p>A1.2.c 事業体のユーザが共有されているシステムバイナリへの書き込みアクセス権がないことを確認する。</p> <p>A1.2.d ログエントリの閲覧が所有する事業に制限されていることを確認する。</p> <p>A1.2.e 各事業体がサーバリソースを独占して脆弱性（例えば、バッファオーバーフローなどを引き起こすエラー、競合、および再起動状況）を悪用できないようにするために、以下のシステムリソースの使用に関して制限が課せられていることを確認する。</p> <ul style="list-style-type: none"> ▪ ディスク領域 ▪ 帯域幅 ▪ メモリ ▪ CPU 	各加盟店またはサービスプロバイダが自身の環境のみにアクセスできるようにアクセスおよび権限を制限するには、以下を考慮します。 (1) 加盟店またはサービスプロバイダの Web サーバユーザ ID の権限、(2) ファイルを読み取り、書き込み、および実行するために付与される許可、(3) システムバイナリに書き込むために付与される許可、(4) 加盟店およびサービスプロバイダのログファイルへのアクセス権の付与、(5) 1 つの加盟店またはサービスプロバイダがシステムリソースを独占できないようにするための管理。
A1.3 ログ記録と監査証跡が有効になっていて、各事業体のカード会員データ環境に一意であり、PCI DSS 要件 10 と一致していることを、確実にする。	<p>A1.3 共有ホスティングプロバイダが、各加盟店およびサービスプロバイダ環境に対して、次のようにログ記録を有効にしていることを確認する。</p> <p>一般的なサードパーティアプリケーションでログが有効になっている。ログはデフォルトでアクティブである。</p> <p>所有事業体がログをレビューできる。</p> <p>ログの場所が所有事業体に明確に伝えられている。</p>	加盟店およびサービスプロバイダがカード会員データ環境に固有のログにアクセスして確認することができるよう、共有ホスティング環境でログを使用可能にする必要があります。
A1.4 ホストされている加盟店またはサービスプロバイダへの侵害が発生した場合に、タイムリーなフォレンジック調査を提供するプロセスを可能にする。	A1.4 共有ホスティングプロバイダが、侵害が発生した場合に、関連サーバのタイムリーなフォレンジック調査を提供するポリシーを作成していることを確認する。	共有ホスティングプロバイダは、侵害に対するフォレンジック調査が必要になった場合に、個別の加盟店またはサービスプロバイダの詳細を把握できるように、適切な詳細レベルまで、迅速かつ簡単に応答するためのプロセスを確立する必要があります。

付録 A2: カード提示 POS POI 端末接続用に SSL / 初期の TLS を使用する事業体向けの PCI DSS 追加要件

POS POI 端末接続用に SSL および初期の TLS を使用している事業体は、可能な限り早く強力な暗号化プロトコルへのアップグレードに向けて努力しなければなりません。さらに、SSL および/または初期の TLS は、これらのプロトコルが現状存在していない環境には導入してはいけません。発行時点では、POS POI 決済端末において、既知の脆弱性を攻撃することは困難です。しかし、新たな脆弱性は常に現れるものであり、組織として脆弱性の傾向を最新に維持することや、任意の既知の攻撃を受けやすいかどうかを判断することは、組織の責任です。

PCI DSS 要件で直接的に影響があるのは：

- | | |
|----------|---------------------------------------------------------------------------|
| 要件 2.2.3 | 安全でないと見なされている必要なサービス、プロトコル、またはデーモンに追加のセキュリティ機能を実装する。 |
| 要件 2.3 | 強力な暗号化を使用して、すべてのコンソール以外の管理アクセスを暗号化する。 |
| 要件 4.1 | オープンな公共ネットワーク経由で機密性の高いカード会員データを伝送する場合、以下のような、強力な暗号化とセキュリティプロトコルを使用して保護する。 |

本付録内で詳細が記載されている POS POI 端末接続を除き、SSL および初期の TLS はセキュリティ対策としてこれらの要件を満たすために使用してはなりません。POS POI 端末について SSL および初期の TLS から移行作業を行う際のサポートとして、以下の準備を含めます：

- 新規の POS POI 端末実装で、SSL または初期の TLS をセキュリティ対策として使用してはならない。
- すべての POS POI 端末サービスプロバイダは、安全なサービスを提供しなければならない。
- SSL および/または初期の TLS を使用する既存の POS POI 端末実装をサポートするサービスプロバイダは、正式なリスク低減策と移行計画を定めて実行している必要がある。
- SSL および初期の TLS の既知の攻撃手法に対して耐性があると検証できるカード提示環境の POS POI 端末および SSL / TLS の接続終端地点は、これらをセキュリティ対策として使用し続けることができる。

この付録は、POS POI 端末への接続を提供するサービスプロバイダを含め、POS POI 端末を保護するためのセキュリティ対策として SSL および初期の TLS を使用する事業体に適用されます。

A2 要件	テスト手順	ガイダンス
<p>A2.1 (加盟店または支払いを受け付ける場所の) POS POI 端末で SSL および/または初期の TLS を使用している事業体は、デバイスが既知の攻撃手法に対して耐性があることを検証する必要がある。</p> <p>注: この要件は、加盟店のような POS POI 端末を持つ事業体に対して適用されることを目的としています。この要件は、POS POI 端末の終端箇所または接続先としての役割を果たすサービスプロバイダに対して適用することを目的としていません。要件 A2.2 および A2.3 は、POS POI サービスプロバイダに適用されます。</p>	<p>A2.1 POS POI 端末で SSL および/または初期の TLS を使用している場合、事業体がデバイスについて SSL および初期の TLS に関する既知の攻撃手法に対して耐性があることを検証する文書（例えば、ベンダ文書、システム/ネットワーク構成の詳細など）をもっていることを確認する。</p>	<p>カード提示環境で使用される POS POI 端末は、現在の既知の攻撃手法に対して耐性があると示すことができる場合、SSL および初期の TLS を継続して利用することができます。</p> <p>しかし、SSL は古い技術であり将来的にさらなるセキュリティ脆弱性の対象となり得るため、POS POI 端末も可能な限り安全なプロトコルへアップグレードすることを強く推奨します。</p> <p>SSL および初期の TLS が環境に必要ない場合、これらのバージョンの使用とフォールバックを無効化する必要があります。</p> <p>さらなるガイダンスとして、現行の SSL/初期の TLS に関する PCI SSC 補足情報を参照してください。</p> <p>注: 現時点での攻撃手法に耐性がある POS POI 端末への容認は、現在の既知のリスクに基づくものです。POS POI 端末に対して影響がある新たな攻撃手法が現れた場合、その POS POI 端末を直ちに更新する必要があります。</p>

A2 要件	テスト手順	ガイダンス
A2.2 サービスプロバイダのための要件 : A2.1 で参照される POS POI 端末への既存の接続点で SSL および/または初期の TLS を使用しているサービスプロバイダは、正式なリスク低減策と移行計画を定めて実行している必要がある。	<p>A2.2 文書化されたリスク低減策と移行計画をレビューし、以下が含まれていることを確認する :</p> <ul style="list-style-type: none"> • 伝送されるデータ、SSL および初期の TLS を使用および/またはサポートするシステムの種類と数、環境の種類を含む使用方法の記述 • リスク評価の結果および実施されているリスク低減策 • SSL および初期の TLS を利用する新たな脆弱性を監視するためのプロセスの記述 • SSL および初期の TLS が新規環境に実装されないことを確実にする実装済み変更管理プロセスの記述 • 将來の移行プロジェクト計画の概要 	<p>アクワイアラやアクワイアラプロセッサなどのサービスプロバイダを含むがこれらに限定されない、POS POI 終端箇所は、サービスプロバイダがこれらの接続をサポートするリスクの低減策を実施済みであることを示す場合、SSL/初期の TLS を使用し続けることができます。</p> <p>リスク低減および移行計画は事業体によって整備される文書で、安全なプロトコルへの移行の計画の詳細、および事業体が移行完了までに SSL および初期の TLS に関するリスクを低減するために実行しているコントロールを説明します。</p> <p>サービスプロバイダは、SSL/初期の TLS を使用している顧客に対して、その使用に関連するリスクおよび安全なプロトコルへの移行について、通達すべきです。</p> <p>さらなる リスク低減策と移行計画に関するガイダンスとして、SSL/初期の TLS に関する現行の PCI SSC 補足情報を参照してください。</p>
A2.3 サービスプロバイダのための要件 : すべてのサービスプロバイダは安全なサービスを提供しなければならない。	A2.3 システム構成とサポート文書を調べ、サービスプロバイダのサービスが安全なプロトコルオプションを提供していることを確認する	<p>POS POI 端末への SSL/初期の TLS 接続をサポートするサービスプロバイダは、安全なプロトコルオプションを提供するべきです。</p> <p>さらなるガイダンスとして、SSL/初期の TLS に関する現行の PCI SSC 補足情報を参照してください。</p>

付録 A3: PCI DSS 指定事業体向けの追加検証

この付録はペイメントブランドまたはアクワイアラーによって PCI DSS 既存要件の追加検証が必要であると指定された事業体のみに適用されます。この付録が適用される事業体の例としては以下が含まれます：

- カード会員データを大量に保存、処理、および/または伝送している。
- カード会員データの集約場所を提供している。または
- カード会員データの重大な、または度重なる侵害を受けたことがある。

これらの補助的な検証ステップは、日常業務（BAU）プロセスの検証および強化された検証と評価範囲の考察を通じて、PCI DSS コントロールが効果的かつ継続的に維持されていることのさらなる保証を提供することを目的としています。

この文書に記載されている追加の検証の手順は、次の管理領域に分類されます：

- A3.1. PCI DSS 準拠プログラムの実装
- A3.2. PCI DSS 対象範囲の文書化と検証
- A3.3. PCI DSS が日常業務（BAU）の活動として組み込まれていることの検証
- A3.4. カード会員データ環境への論理アクセスに対する制御と管理
- A3.5. 疑わしいイベントの識別と対応

注：一部の要件は、特定の活動が実施されるための時間枠（例えば、少なくとも四半期ごとまたは6カ月ごと）を定義しています。

評価担当者が以下を検証する場合、この文書の初回の評価では、前年1年間に、前記の時間枠すべてにおいて活動が実施されることを認められません：

- 1) 適用される要件に従って直近の時間枠（直近の四半期ごと、または6カ月）で実施されている。および
- 2) 事業体が定義された時間枠内で活動の実施を継続するポリシーおよび手順を文書化している。

初回の評価後、その後の年度において、活動が必要とされている各時間枠に対して実行される必要があります。（例えば、四半期の活動は前年の各四半期で毎回実施されなければなりません）

注：事業体は、アクワイアラーまたはペイメントブランドによって指示された場合のみ、この付録による評価を行う必要があります。

A3 要件	テスト手順	ガイダンス
A3.1: PCI DSS 準拠プログラムの実装		
<p>A3.1.1 経営層は以下を含むカード会員データの保護および PCI DSS 準拠プログラムのための責任を確立する：</p> <ul style="list-style-type: none"> • PCI DSS 準拠の維持に関するすべての責任 • PCI DSS 準拠プログラムの憲章の定義 • PCI DSS 準拠の取り組みや改善活動を含む課題について経営層および取締役会へ少なくとも年に一回最新情報を提供する <p>PCI DSS 参照: 要件 12</p>	<p>A3.1.1.a 文書を調べ、経営層が事業体の PCI DSS 準拠の維持に関するすべての責任を割り当てていることを確認する。</p> <p>A3.1.1.b 会社の PCI DSS 憲章を調べ、PCI DSS 準拠プログラムを構成する条件を概説していることを確認する。</p> <p>A3.1.1.c 経営層と取締役会の議事録や議案を調べ、PCI DSS 準拠の取り組みや改善活動が、少なくとも年に一回コミュニケーションされていることを確認する。</p>	<p>経営層への PCI DSS 準拠の責任の割り当ては、経営レベルにおける PCI DSS 準拠プログラムの可視性を確実にし、プログラムの有効性と戦略的優先事項への影響を判断するための適切な質問の機会を与えます。</p> <p>PCI DSS 準拠プログラムの全体的な責任は、組織内の個々の役割およびまたはビジネス部門に割り当てることも可能です。</p>
<p>A3.1.2 正式な PCI DSS 準拠プログラムには以下を含める：</p> <ul style="list-style-type: none"> • 日常業務の活動を含む、全体的な PCI DSS 準拠を維持および監視する活動の定義 	<p>A3.1.2.a 情報セキュリティポリシーおよび手順を調べ、プロセスが具体的に以下を定義していることを確認する：</p> <ul style="list-style-type: none"> • 日常業務を含む、全体的な PCI DSS 準拠の維持および監視 • 年に一回の PCI DSS 評価 • PCI DSS 要件の継続的な検証 • 戰略的なビジネス上の意識決定に対する PCI DSS の潜在的な影響を判断するビジネス影響分析 	<p>正式な準拠プログラムは組織のセキュリティ対策の健全性を監視すること、制御の障害発生に対する積極的な対処、さらに組織全体の活動や準拠状態の効率的な共有を可能にします。PCI DSS 準拠プログラムは専用のプログラム、または包括的な準拠およびまたはガバナンスプログラムの一部としてもよいが、一貫性と効果的な</p>

A3 要件	テスト手順	ガイダンス
<ul style="list-style-type: none"> 年に一回の PCI DSS 評価プロセス PCI DSS 要件の継続的な検証プロセス（例えば：日次、週次、四半期ごと等。要件で該当する場合） 戦略的なビジネス上の意思決定に対する PCI DSS の潜在的な影響を判断するビジネス影響分析を実施するプロセス <p>PCI DSS 参照：要件 1-12</p>	<p>A3.1.2.b 担当者をインタビューし、準拠活動を観察することで、定義済プロセスが以下について実装されていることを確認する：</p> <ul style="list-style-type: none"> 日常業務の活動を含む、全体的な PCI DSS 準拠の維持および監視 年に一回の PCI DSS 評価管理 PCI DSS 要件の継続的な検証 戦略的なビジネス上の意思決定に対する PCI DSS の潜在的な影響を判断するビジネス影響分析 	<p>評価を実証する明確に定義された方法論を含める必要があります。方法論の例には以下が含まれます：計画-実行-評価-改善（PDCA）のデミングサークル、ISO 27001、COBIT、DMAIC、およびシックス SIGMA</p> <p>組織全体の PCI DSS 準拠の維持および監視は、日次、週次、月次、四半期ごと、または年に一回実施されるべき活動の識別と、これらの活動が適切に実施されていることの確認（例えば、セキュリティ自己評価または PDCA 手法を使用するなど）を含みます。</p> <p>PCI DSS の潜在的な影響が分析されるべき戦略的なビジネス上の意思決定の例には、合併および買収、新規技術の購入、または新たな支払を受け付けるチャネルが含まれます。</p>
<p>A3.1.3 PCI DSS 準拠の役割および責任は具体的に定義され、正式に一人以上の担当者が任命され、少なくとも以下を含んでいること：</p> <ul style="list-style-type: none"> 日常業務としての PCI DSS 管理 年に一回の PCI DSS 評価管理 PCI DSS 要件の継続的な検証の管理（例えば：日次、週次、四半期ごと等、要件で該当する場合） 戦略的なビジネス上の意思決定に対する PCI DSS の潜在的な影響を判断するビジネス影響分析の管理 <p>PCI DSS 参照：要件 12</p>	<p>A3.1.3.a 情報セキュリティポリシーおよび手順を調べ、担当者をインタビューすることで、役割と責任が明確に定義され、職務が少なくとも以下を含むように割り当てられていることを確認する：</p> <ul style="list-style-type: none"> 日常業務としての PCI DSS 管理 年に一回の PCI DSS 評価管理 PCI DSS 要件の継続的な検証の管理（例えば：日次、週次、四半期ごと等、要件で該当する場合） 戦略的なビジネス上の意思決定に対する PCI DSS の潜在的な影響を判断するビジネス影響分析の管理 <p>A3.1.3.b 責任者をインタビューし、指定された PCI DSS 準拠の責任を熟知し、実施していることを確認する。</p>	<p>具体的な PCI DSS 準拠の役割や責任の正式な定義は、継続中の PCI DSS 準拠の取り組みの説明責任や監視を確実にするために役立ちます。</p> <p>これらの役割は一人の主担当者、またはさまざまな局面のために複数の異なる主担当者として割り当てることができます。</p> <p>担当責任は、リスクベースの意思決定を行う権限があり、特定の機能について説明責任がある個人に対して割り当てられる必要があります。</p> <p>職務は正式に定義される必要があり、主担当者はその責任と説明責任の理解を実証可能である必要があります</p>

A3 要件	テスト手順	ガイダンス
<p>A3.1.4 最新の PCI DSS および/または情報セキュリティトレーニングを少なくとも年に一回 PCI DSS 準拠責任 (A3.1.3 で識別される) を持つ担当者に提供する。</p> <p>PCI DSS 参照: 要件 12</p>	<p>A3.1.4.a 情報セキュリティポリシーおよび手順を調べ、PCI DSS および/または情報セキュリティトレーニングが PCI DSS 準拠責任を持つ各役割に少なくとも年に一回要求されていることを確認する。</p> <p>A3.1.4.b 担当者をインタビューし、出席証明またはその他の記録を調べ、PCI DSS 準拠責任を持つ担当者が最新の PCI DSS および/または同様の情報セキュリティトレーニングを受講していることを確認する。</p>	<p>PCI DSS 準拠のための担当者の責任は、一般的なセキュリティ意識向上トレーニングによって提供されるものを超える特定のトレーニングを必要とします。</p> <p>PCI DSS 準拠責任を持つ個人は、個人が準拠責任を効果的に実施するために従うべき情報セキュリティの一般的な意識向上に加え、特定のセキュリティトピック、技術、プロセスや方法に焦点を当てた専門的なトレーニングを受講する必要があります。</p> <p>トレーニングは第三者が提供するもの—例えば、SANS または PCI SSC (PCI 意識向上、PCIP、および ISA) 、ペイメントブランド、およびアクワイアラー—または内部のトレーニングとすることができます。</p> <p>研修内容は、特定の職務機能に適用でき、最新のセキュリティ脅威および/または PCI DSS のバージョンを含めた最新の状態である必要があります。</p> <p>専門的な役割のための適切なセキュリティトレーニングコンテンツを開発する際の追加のガイダンスとして、PCI SSC の補足情報『セキュリティ意識向上プログラムを実装するためのベストプラクティス』を参照してください。</p>

A3 要件	テスト手順	ガイダンス
A3.2 PCI DSS 対象範囲の文書化および検証		
<p>A3.2.1 少なくとも四半期ごと、および対象範囲内の環境に大幅な変更の発生時に、PCI DSS 対象範囲の正確性を文書化し、確認する。最低でも、四半期ごとの対象範囲の検証には以下を含む必要がある：</p> <ul style="list-style-type: none"> • すべての対象範囲内のネットワークおよびシステムコンポーネントの識別 • すべての対象範囲外ネットワークの識別と、すべてのセグメンテーション制御の実装の詳細を含む対象範囲外となる正当な理由 • すべての接続事業体の識別一例、カード会員データ環境 (CDE) へアクセスする第三者事業体 <p>PCI DSS 参照：PCI DSS 要件の対象範囲</p>	<p>A3.2.1.a 文書化された対象範囲レビューの結果を調べ、担当者をインタビューすることで、レビューで以下のように実施されていることを確認する：</p> <ul style="list-style-type: none"> • 少なくとも四半期ごと • 対象範囲内の環境に対する大幅な変更後 <p>A3.2.1.b 文書化された四半期ごとの対象範囲のレビュー結果を調べ、以下を実施していることを確認する：</p> <ul style="list-style-type: none"> • すべての対象範囲のネットワークおよびシステムコンポーネントの識別 • すべての対象範囲外ネットワークの識別、およびすべてのセグメンテーション制御の実装の詳細を含むネットワークが対象外となる正当な理由 • すべての接続事業体の識別一例、CDE へアクセスする第三者事業体 	<p>PCI DSS 対象範囲の検証は PCI DSS 対象範囲が最新であり、変化するビジネス目標と整合していることを確実にするため可能な限り定期的に実施する必要があります。</p>

A3 要件	テスト手順	ガイダンス
<p>A3.2.2 新規システムの追加および新規ネットワークの接続を含む、システムまたはネットワークへのすべての変更による PCI DSS 対象範囲の影響を決定する。プロセスには以下を含む必要がある：</p> <ul style="list-style-type: none"> 正式な PCI DSS 影響評価の実施 システムまたはネットワークに適用される PCI DSS 要件の識別 適切な PCI DSS 対象範囲の更新 影響評価の結果に対する責任者（A3.1.3 で定義された方法で）による文書化された署名 <p>PCI DSS 参照：PCI DSS 要件の対象範囲; 要件 1-12</p>	<p>A3.2.2 変更文書を調べ、担当者をインタビューすることで、システムまたはネットワークへの各変更を確認する：</p> <ul style="list-style-type: none"> 正式な PCI DSS 影響評価が実施されていること システムまたはネットワークに適用される PCI DSS 要件が識別されていること 変更に対して適切な PCI DSS 対象範囲が更新されていること 責任者（A3.1.3 で定義された方法で）による署名が得られ、文書化されていること 	<p>システムまたはネットワークへの変更は PCI DSS 対象範囲に対して大幅な影響を与えます。例えば、ファイアウォールのルール変更は対象範囲内のネットワークセグメント全体へ影響をもたらし、または新規システムを CDE に追加する場合、適切に保護されている必要があります。</p> <p>事業体の PCI DSS 対象範囲上のシステムとネットワークへの変更がもたらす影響を判断するプロセスは、専用の PCI DSS 準拠プログラムの一部として実行することも、事業体の包括的な準拠および/またはガバナンスプログラムとして実行することもできます。</p>

A3 要件	テスト手順	ガイダンス
<p>A3.2.2.1 変更の完了時、すべての新規または変更されたシステム、ネットワークに対してすべての関連する PCI DSS 要件が検証され、文書が適切に更新されている。検証される必要がある PCI DSS 要件の例は以下を含むが、これらに限定されない：</p> <ul style="list-style-type: none"> • 変更を反映するためのネットワーク図の更新 • すべてのデフォルトパスワードを変更および不要なサービスを無効化を含め、システムが構成基準に従って構成されている • 必要な制御によりシステムが保護されている— 例、ファイル整合性監視 (FIM)、アンチウイルス、パッチ、監査ログ • 機密認証データ (SAD) は保存せず、すべてのカード会員データ (CHD) 保管場所が文書化され、データ保存ポリシーと手順に組み込まれている • 新しいシステムが四半期ごとの脆弱性スキャンプロセスの対象に含まれる <p>PCI DSS 参照 : PCI DSS 要件の対象範囲; 要件 1-12</p>	<p>A3.2.2.1 システムとネットワークの変更のサンプルに対して、変更履歴を検査し、担当者をインタビュー、および影響を受けたシステム/ネットワークを観察することで、適用される PCI DSS 要件が実装され、変更箇所に応じて文書が更新されていることを確認する。</p>	<p>PCI DSS 対象環境に追加されたシステムやネットワークに対してすべての適切な PCI DSS コントロールが適用されたことを確実にするため、実施されたすべての変更を分析するプロセスを持つことが重要です。</p> <p>この検証を変更管理プロセスに組み込むことは、デバイスのインベントリおよび構成基準が最新化されること、および必要に応じてセキュリティ対策が適用されていることを確認するのに役立ちます。</p> <p>変更管理プロセスは、PCI DSS 要件が実装されている証拠、または反復プロセスを通じて維持されていることを裏付ける証拠を含める必要があります。</p>

A3 要件	テスト手順	ガイダンス
<p>A3.2.3 組織構造の変更一例えば、会社の合併や買収、セキュリティコントロールに責任を持つ担当者の変更や配置転換において PCI DSS 対象範囲とコントロールの適用性への影響に関する正式な（内部）レビューを実施する。</p> <p>PCI DSS 参照: 要件 12</p>	<p>A3.2.3 ポリシーと手順を調べ、組織構造の変更において、PCI DSS 対象範囲とコントロールの適用性への影響に関する正式なレビューが実施されていることを確認する。</p>	<p>組織の構造と管理は、効果的で安全な運用のための要求事項と規約を定義します。この構造の変更は、これまで PCI DSS コントロールを担当していた人員の配置転換や削減、引き継いだ新たな責任者がコントロールを確立できていないことなどにより、既存のコントロールとフレームワークに悪影響を与える可能性があります。</p> <p>そのため、変更が発生した際に、コントロールが適用され有効であることを確実にするための PCI DSS 対象範囲とコントロールを再検討することが重要です。</p>
<p>A3.2.4 セグメンテーションを使用している場合、少なくとも 6 カ月ごと、およびセグメンテーションの制御/方法の変更後にセグメンテーション制御に対してペネトレーションテストを実施することで PCI DSS 対象範囲を確認する。</p> <p>PCI DSS 参照: 要件 11</p>	<p>A3.2.4 最近のペネトレーションテストの結果を調べ、以下を確認する：</p> <ul style="list-style-type: none"> ペネトレーションテストが実行され、少なくとも 6 カ月ごと、および任意のセグメンテーション制御/方法の変更後にセグメンテーション制御を確認する。 ペネトレーションテストが、使用されているすべてのセグメンテーション制御/方法を対象としている。 ペネトレーションテストによりセグメンテーション方法が運用可能で効果的であり、CDE 内システムからすべての対象範囲外システムを分離していることを確認する。 	<p>対象範囲外ネットワークから対象範囲内ネットワークを分離するためにセグメンテーションを使用する場合、ペネトレーションテストを用いて、セグメンテーション制御が運用可能で効果的に機能していることを確認します。</p> <p>ペネトレーションテストの技術は、PCI DSS 要件 11 で指定されている既存のペネトレーション手法に従う必要があります。</p> <p>効果的なペネトレーションテストの追加情報については、PCI SSC の補足情報『ペネトレーションテストガイド』を参照してください。</p>

A3 要件	テスト手順	ガイダンス
<p>A3.2.5 データ発見手法を実装し、少なくとも四半期ごと、およびカード会員環境またはプロセスの大幅な変更後に、PCI DSS 対象範囲、および平文の PAN の置かれているすべての出所と場所を確認する。</p> <p>データ発見手法は、平文の PAN が現在定義されている CDE の外側のシステムやネットワーク上に存在する可能性があることを考慮に入れる必要がある。</p> <p>PCI DSS 参照: PCI DSS 要件の適用範囲</p>	<p>A3.2.5.a 文書化されたデータ発見手法を調べ、以下を確認する：</p> <ul style="list-style-type: none"> データ発見手法が、平文の PAN のすべての出所と場所を識別するプロセスを含んでいる 平文の PAN が現在定義されている CDE の外側にあるシステムやネットワーク上に存在する可能性があることを考慮した手法である <p>A3.2.5.b 最近のデータ発見活動の結果を調べ、責任者にインタビューすることで、データ発見が少なくとも四半期ごと、およびカード会員環境やプロセスの大幅な変更後に実施されていることを確認する。</p>	<p>PCI DSS は、対象範囲特定の一環として、被審査事業体が環境内のすべての平文 PAN の存在を識別して、文書化する必要があることを要求します。</p> <p>平文 PAN のすべての出所と場所を識別し、現在定義されている CDE の外側にあるシステムやネットワークに存在する、あるいは定義された CDE 内の予期しない場所一例えは、エラーログやメモリダンプファイルの中一に存在する可能性を考慮に入れた、データ発見手法を実装することは、以前把握されていなかった平文 PAN の場所を検出し、適切に保護されていることを確認するのに役立ちます。</p> <p>データ発見プロセスは、次のような様々な方法によって実行することができますが、これらに限定されません：</p> <ol style="list-style-type: none"> (1) 市販の有効なデータ発見ソフトウェア (2) 自社開発のデータ発見プログラム、または (3) 手動検索 <p>使用する方法に関わらず、本取り組みの目的は、平文 PAN（定義された CDE 内に限らない）のすべての出所と場所を発見することです。</p>

A3 要件	テスト手順	ガイダンス
<p>A3.2.5.1 データ発見に使用される方法の有効性を確認する一例、方法が使用中のすべてのシステムコンポーネント（例えば、各オペレーティングシステムやプラットフォーム）の種類やファイルフォーマット上の平文 PAN を発見可能である。</p> <p>データ発見方法の有効性は、少なくとも年に一回確認する必要がある。</p> <p>PCI DSS 参照: PCI DSS 要件の適用範囲</p>	<p>A3.2.5.1.a 担当者にインタビューし、文書をレビューすることで以下を確認する：</p> <ul style="list-style-type: none"> 事業体が、データ発見で使用する方法の有効性をテストするプロセスをもっている 使用されている方法が、すべてのシステムコンポーネントの種類とファイルフォーマット上の平文の PAN を検出可能であることの検証を含むプロセスである 	<p>データ発見のために使用される方法の有効性テストのプロセスは、カード会員データ検出の完全性と正確性を確実にします。</p> <p>完全性のために、少なくとも対象範囲内と対象範囲外のネットワークの両方からシステムコンポーネントのサンプリングを、データ発見プロセスに含める必要があります。</p> <p>使用中のシステムコンポーネントとファイルフォーマットのサンプル上にテスト用の PAN を配置し、データ発見方法がテスト用 PAN の検出を確認することによって正確性をテストすることが可能です。</p>
	<p>A3.2.5.1.b 最近の有効性テストの結果を調べ、少なくとも年に一回、データ発見に使用された方法の有効性が検証されていることを確認する。</p> <p>A3.2.5.2.a 文書化された対応手順を調べ、CDE の外側で平文 PAN が検出された際の対応手順が定義され、以下を含むことを確認する：</p> <ul style="list-style-type: none"> CDE の外側で平文 PAN が発見された場合に修正、安全な削除、または必要に応じて現在定義されている CDE への移行を含む、実施るべきことを定義した手順 CDE の外側にあるデータが最終的にどのようにになるかを定義する手順 CDE の外側にデータが存在する結果に至った、データ漏えいやプロセスギャップの改善手順 データの出所を識別する手順 PAN とともにトラックデータが保存されているかどうかを識別する手順 	<p>文書化された対応手順の整備することは、CDE の外側で平文の PAN が発見された場合に従うべき必要な改善行動を識別し、将来の情報漏えいの防止に寄与します。</p> <p>例えば、PAN が CDE の外側で発見された場合、次のような分析が実施されるべきです。</p> <p>(1) 当該データが他のデータから独立して保存されたかどうか（またはフルトラックの一部として保存されたか）の判断。 (2) 当該データの出所の識別。 (3) 当該データが CDE の外側に存在する結果に至ったコントロールギャップの識別。</p>

A3 要件	テスト手順	ガイダンス
<p>なるかを定義する手順</p> <ul style="list-style-type: none"> • CDE の外側にデータが存在する結果に至った、データ漏えいやプロセスギャップの改善手順 • データの出所を識別する手順 • PANとともにトラックデータが保存されているかどうかを識別する手順 	<p>A3.2.5.2.b 担当者にインタビューし、対応活動の記録を調べることで、CDE の外側で平文 PAN が検出された場合に、改善策が実施されることを確認する。</p>	
<p>A3.2.6 平文 PAN が CDE から不正な経路、方法、プロセスを介して送信されることを検知し防止する監査ログや警告の生成を含むメカニズムを実装する。</p> <p>PCI DSS 参照: PCI DSS 要件の適用範囲</p>	<p>A3.2.6.a 文書を調べ、実装されているメカニズムを観察して、メカニズムが以下を備えていることを確認する :</p> <ul style="list-style-type: none"> • 実装されており、アクティブに実行中である • 不正な経路、方法、またはプロセスを介して CDE から送信される平文 PAN を検知し防止するように構成されている • 不正な経路や方法またはプロセスを介して CDE から送信される平文 PAN を検知するとログと警告を生成する <p>A3.2.6.b 監査ログと警告を調べ、責任者にインタビューすることで、警告が調査されていることを確認する。</p>	<p>不正な平文 PAN の流出を検知および防止するためのメカニズムはデータ損失防止 (DLP) ソリューションのような適切なツールおよび/または手動プロセスや手順を含むことができます。メカニズムの対象には、電子メール、リムーバブルメディアへのダウンロード、プリンターへの出力を含む必要がありますが、これらに限定されません。</p> <p>これらのメカニズムの使用により、組織はデータ損失につながる状況を検知および防止することができます。</p>
<p>A3.2.6.1 不正な経路や方法またはプロセスを介して、平文 PAN を CDE から取り出そうとする試みを検知した際に開始される対応手順を実装する。対応手順は以下の必要がある :</p> <ul style="list-style-type: none"> • 責任者によって、警告をタイムリーに調査する手順 • データ流出を防ぐための、データ漏えいやプロセスギャップを必要に応じて改善する手順 	<p>A3.2.6.1.a 文書化された対応手順を調べ、不正な経路や方法またはプロセスを介して、平文 PAN を CDE から取り出そうとする試みに対する対応手順に以下が含まれることを確認する :</p> <ul style="list-style-type: none"> • 責任者によって、警告をタイムリーに調査する手順 • データ流出を防ぐための、データ漏えいやプロセスギャップを必要に応じて改善する手順 <p>A3.2.6.1.b 担当者にインタビューし、不正な経路や方法、またはプロセスを介して、平文 PAN が CDE からの送信を検知した際の対応記録を調べ、改善策が実施されたことを確認する。</p>	<p>平文 PAN を不正な経路、方法、またはプロセスを介して取り出そうとする試みは、データを盗む悪意を示すか、あるいは適切な方法を知らない、または単に従わない正規の従業員の行動であるかもしれません。</p> <p>これらの発生時にタイムリーな調査を行うと、修正を行う必要のある箇所を識別すること、および価値のある情報を提供することができ、脅威がどこからもたらされたかを理解するのに役立ちます。</p>

A3.3 PCI DSS が日常業務 (BAU) の活動として組み込まれていることの検証

A3 要件	テスト手順	ガイダンス
A3.3.1 重要なセキュリティ対策システムの障害のタイムリーな検出および報告のためのプロセスを実装する。重要なセキュリティ障害の例には以下を含むがこれらに限定されない： <ul style="list-style-type: none"> • ファイアウォール • IDS/IPS • ファイル整合性監視 • アンチウイルス • 物理的アクセス制御 • 論理的アクセス制御 • 監査ログメカニズム • セグメンテーション制御 (使用している場合) <i>PCI DSS 参照：要件 1-12</i>	<p>A3.3.1.a 文書化されたポリシーと手順を調べ、重要なセキュリティ対策システムの障害のタイムリーな検出および報告のためのプロセスが定義されていることを確認する。</p> <p>A3.3.1.b 検出および警告のプロセスを調べ、担当者をインタビューし、すべての重要なセキュリティ対策のためのプロセスが実装されていること、および重要なセキュリティ対策の障害に対して警告が生成されることを確認する。</p>	重要なセキュリティ対策の障害を即座（出来る限り早く）検出し、警告するための正式なプロセスがなければ、障害が長期間検出されない可能性があり、攻撃者がシステムを侵害し、カード会員データ環境から機密データを盗むために十分な時間を提供することにつながります。
A3.3.1.1 すべての重要なセキュリティ対策の障害についてタイムリーに対応する。セキュリティ対策の障害に対応するためのプロセスには以下を含む： <ul style="list-style-type: none"> • セキュリティ機能の復旧 • セキュリティ障害の期間（開始から終了までの日付時刻）の識別および文書化 • 根本原因を含む障害の原因の識別と文書化、および根本原因に対応する改善案の文書化 • 障害中に発生したすべてのセキュリティ問題の識別および対応 • セキュリティ障害の結果としてさらなる活動が必要かどうか判断するためのリスク評価の実施 • 再発防止策の実装 • セキュリティ対策の監視の再開 	<p>A3.3.1.1.a 文書化されたポリシーおよび手順を調べ、担当者をインタビューすることで、以下を含むセキュリティ対策の障害に対応するプロセスが定義され、実装されていることを確認する：</p> <ul style="list-style-type: none"> • セキュリティ機能の復旧 • セキュリティ障害の期間（開始から終了までの日付時刻）の識別および文書化 • 根本原因を含む障害の原因の識別と文書化、および根本原因に対応する改善案の文書化 • 障害中に発生したすべてのセキュリティ問題の識別および対応 • セキュリティ障害の結果としてさらなる活動が必要かどうか判断するためのリスク評価の実施 • 再発防止策の実装 • セキュリティ対策の監視の再開 	文書化された証跡（例、問題管理システムの記録）はセキュリティ障害に対応するプロセスと手順が実施されていることを裏付けなければなりません。さらに、担当者は障害発生時の責任について認識するべきです。 障害に対する活動および対応は、文書化された証跡として保存するべきです。

A3 要件	テスト手順	ガイダンス
<p>び根本原因に対応する改善案の文書化</p> <ul style="list-style-type: none"> 障害中に発生したすべてのセキュリティ問題の識別および対応 セキュリティ障害の結果としてさらなる活動が必要かどうか判断するためのリスク評価の実施 再発防止策の実装 セキュリティ対策の監視の再開 <p>PCI DSS 参照: 要件 1-12</p>	<p>A3.3.1.1.b 記録を調べ、以下を含むセキュリティ対策の障害が文書化されていることを確認する：</p> <ul style="list-style-type: none"> 根本原因を含む障害原因の識別 セキュリティ障害の期間（開始から終了までの日付時刻） 根本原因に対応するために必要な改善方法の詳細 	
<p>A3.3.2 少なくとも年に一回、ハードウェアおよびソフトウェアのテクノロジーをレビューし、組織の PCI DSS 要件に合致しているかどうか確認する。（例えば、ベンダーによつてもはやサポートされないおよび/または組織のセキュリティニーズにもはや合致できないテクノロジーのレビュー）プロセスには、組織の PCI DSS 要件にもはや合致しないテクノロジーを改善する計画や、該当する場合、そのテクノロジーの更改も含まれる。</p> <p>PCI DSS 参照: 要件 2, 6</p>	<p>A3.3.2.a 文書化されたポリシーと手順を調べ、担当者にインタビューすることで、ハードウェアとソフトウェアのテクノロジーをレビューし、組織の PCI DSS 要件に合致し続けているかどうか確認するプロセスが定義され実装されていることを確認する。</p> <p>A3.3.2.b 最近のレビュー結果をレビューし、少なくとも年に一回レビューが実施されていることを確認する。</p> <p>A3.3.2.c 組織の PCI DSS 要件にもはや合致しないと判断されたテクノロジーに対し、テクノロジーを改善する計画が実施されていることを確認する。</p>	<p>ハードウェアとソフトウェアのテクノロジーは常に進化し、組織は利用しているテクノロジーの変化及びそれらに対する進化し続ける脅威を認識する必要があります。</p> <p>また、組織はテクノロジーベンダーによって製品やサポートプロセスに対して行われた変更を認識し、そのような変更によってテクノロジーを使用する組織にどのような影響があるか理解する必要があります。</p> <p>PCI DSS コントロールに影響を及ぼすテクノロジーを定期的にレビューすることは、購買、利用、実装戦略を支援することができ、テクノロジーに依存するコントロールが引き続き有効であることを確実にします。</p>

A3 要件	テスト手順	ガイダンス
<p>A3.3.3 少なくとも四半期ごとに、日常業務の活動が守られていることを確認するレビューを実施する。レビューは、PCI DSS 準拠プログラム（A3.1.3 で定められた）で割り当てられた担当者によって実施され、以下を含む必要がある：</p> <ul style="list-style-type: none"> すべての日常業務（例、A3.2.2、A3.2.6、A3.3.1）について実施されていることの確認 担当者がセキュリティポリシーと運用手順（例えば、日次のログレビュー、ファイアウォールのルールセットのレビュー、新規システムに対する構成基準など）に従っていることの確認 すべての日常業務で対応済みと確認したことを含む、レビューが完了した方法の文書化 年に一回の PCI DSS 評価で要求される文書化された証跡の収集 PCI DSS ガバナンスの責任を負った経営者による結果へのレビューと署名 すべての日常活動を対象とする、少なくとも 12 カ月の記録や文書の保存 <p>PCI DSS 参照: 要件 1-12</p>	<p>A3.3.3.a ポリシーと手順を調べ、日常業務をレビューし確認するプロセスが定義されていることを確認する。手順の確認には以下が含まれる：</p> <ul style="list-style-type: none"> すべての日常業務（例えは、A3.2.2、A3.2.6、A3.3.1）について実施されていることの確認 担当者がセキュリティポリシーと運用手順（例えは、日次のログレビュー、ファイアウォールのルールセットのレビュー、新規システムに対する構成基準など）に従っていることの確認 すべての日常業務で対応済みと確認したことを含む、レビューが完了した方法の文書化 年に一回の PCI DSS 評価で要求される文書化された証跡の収集 PCI DSS ガバナンスの責任を負った経営者による結果へのレビューと署名 すべての日常活動を対象とする、少なくとも 12 カ月の記録や文書の保存 <p>A3.3.3.b 責任者にインタビューし、レビューの記録を調べ、以下を確認する：</p> <ul style="list-style-type: none"> レビューは、PCI DSS 準拠プログラムを割り当てられた担当者によって実施されている レビューは少なくとも四半期ごとに実施されている 	<p>日常業務の活動の中に PCI DSS コントロールが導入されていることはセキュリティが継続的に通常の業務処理に含まれていることを確実にするために効果的な方法です。</p> <p>そのため、日常業務のコントロールがアクティブで意図したとおりに動作していることを確実にするため、独立したチェックを実施することが重要です。</p> <p>これらの独立したチェックの意図は、セキュリティ活動が継続的に実施されているかどうかを確認することです。</p> <p>これらのレビューは、事業体の次回の PCI DSS 評価の準備を支援するために、例えは、監査ログ、脆弱性スキャンレポート、ファイアウォールのレビューなどの適切な証拠が維持されていることの確認にも使用することができます。</p>

A3 要件	テスト手順	ガイダンス
A3.4 カード会員データ環境への論理アクセスに対する制御と管理		
A3.4.1 対象範囲内のシステムコンポーネントのユーザーアカウントとアクセス権限を少なくとも6ヶ月ごとにレビューし、ユーザーアカウントとアクセスが職務に基づき適切であり、承認されていることを確認する。 <i>PCI DSS 参照: 要件 7</i>	A3.4.1 責任者にインタビューし、サポートする文書を調べ、以下を確認する： <ul style="list-style-type: none"> ユーザーアカウントとアクセス権限が、少なくとも 6 ヶ月ごとにレビューされている アクセスが職務に基づいた適切なものであり、すべてのアクセスが承認されていることをレビューにより確認している 	アクセス要件は、個人の役割の変更や、退職、職務の変更によって、時間とともに変化します。管理者は、第三者やユーザの職務を含む担当者変更を反映するため、必要に応じてユーザーアクセスを定期的にレビュー、再評価、および更新する必要があります。
A3.5 疑わしいイベントの識別と対応		
A3.5.1 システムに対する攻撃パターンや望ましくない行動をタイムリーに特定する、少なくとも以下の手法を実装する—例えば、統合された手動レビューおよび/または一元管理または自動化ログ相関ツールの使用： <ul style="list-style-type: none"> 異常や疑わしい活動が発生したことの特定 疑わしい活動や異常を検知したときの、責任者へのタイムリーな警告の発行 文書化された対応手順に従った警告への対応 <i>PCI DSS 参照: 要件 10, 12</i>	A3.5.1.a 文書をレビューし、担当者にインタビューすることで、システムに対する攻撃パターンと望ましくない行動をタイムリーに特定する、以下を含む方法論が定義され、実装されていることを確認する： <ul style="list-style-type: none"> 異常や疑わしい活動が発生したことの特定 責任者へのタイムリーな警告の発行 文書化された対応手順に従った警告への対応 A3.5.1.b インシデント対応手順を調べ、責任者にインタビューすることで、以下を確認する： <ul style="list-style-type: none"> 対応の担当者は、タイムリーに警告を受ける 警告は、文書化された対応手順に従って対応される 	システムに対しての攻撃パターンと望ましくない行動を特定できる能力は、情報漏えいの影響を防止、検知、最小化するために重要です。すべての環境にログが存在することで、何か問題が発生した際に、完全な追跡、警告、分析することができます。 重要なシステムコンポーネントや、ファイアウォール、IDS/IPS およびファイル整合性監視 (FIM) システムのようなセキュリティ機能を実行するシステムからの情報を裏付けるプロセスがない場合、不可能ではないものの、侵害の原因を特定することは非常に困難です。 このため、すべての重要なシステムコンポーネントやセキュリティ機能を実行するシステムのログは、収集し、相関付けられ、維持される必要があります。 これには、セキュリティ情報イベント管理 (SIEM)、ファイル整合性監視 (FIM)、変更検知のようなリアルタイム分析、警告、レポート生成を提供するソフトウェア製品やサービス手法の利用が含まれます。

付録 B: 代替コントロール

事業体が正当な技術上の制約または文書化されたビジネス上の制約のために記載されているとおりに明示的に要件を満たすことができないが、その他の（つまり代替の）コントロールの実装を通じて要件に関連するリスクを十分に軽減している場合、ほとんどの PCI DSS 要件に対して代替コントロール検討することができます。

代替コントロールは、以下の条件を満たす必要があります。

1. 元の PCI DSS 要件の目的および厳密さを満たす。
2. 元の PCI DSS 要件で防御の対象とされているリスクを代替コントロールが十分に相殺するよう、元の PCI DSS 要件と同様のレベルの防御を提供する。（各 PCI DSS 要件の目的については、ガイダンス欄を参照。）
3. その他の PCI DSS 要件「以上」のことを実現する。（単なるその他の PCI DSS 要件への準拠は代替コントロールになりません。）

代替コントロールについてその他の要件「以上」であるかどうかを評価するときは、以下を考慮します。

注:以下の項目 a) ~ c) は例にすぎません。代替コントロールはすべて、PCI DSS レビューを実施する評価者によって、その十分性がレビューおよび検証される必要があります。代替コントロールの有効性は、コントロールが実装される環境、周囲のセキュリティコントロール、およびコントロールの構成の詳細によって異なります。企業は、特定の代替コントロールが必ずしもすべての環境において有効ではないことを認識する必要があります。

- a) 既存の PCI DSS 要件がレビュー中の項目に対してすでに要求されている場合、それらを代替コントロールと見なすことはできません。例えば、コンソール以外の管理アクセス用のパスワードは、平文の管理用パスワードが傍受されるリスクを軽減するために、暗号化して送信する必要があります。事業体は、他の PCI DSS パスワード要件（侵入者ロックアウト、複雑なパスワードなど）を使用して、暗号化パスワードの不足を補うことはできません。これらのパスワード要件は平文パスワードの傍受リスクを軽減するものではないためです。また、他のパスワード管理は、レビュー中の項目（パスワード）に対してすでに PCI DSS の要件になっています。
- b) 既存の PCI DSS 要件が別の領域で要求されているが、レビュー中の項目では要求されていない場合、それらを代替コントロールと見なすことは可能です。
- c) 既存の PCI DSS 要件を新しいコントロールと組み合わせて、代替コントロールにすることができます。例えば、企業が要件 3.4 に従って（暗号化などによって）カード会員データを読み取り不能にできない場合、デバイスを使用して、またはデバイス、アプリケーション、管理を組み合わせて、次のすべてに対応する代替コントロールを構成することができます。
(1) 内部ネットワークのセグメンテーション、(2) IP アドレスまたは MAC アドレスフィルタリング、(3) ワンタイムパスワード。

4. PCI DSS 要件に従わないことによって課せられるその他のリスクを考慮する。

評価者は、年に一度の PCI DSS 評価の際に代替コントロールを徹底的に評価して、上述の項目 1 ~ 4 に従い、代替コントロールのそれぞれが元の PCI DSS 要件が対象としているリスクに適切に対応していることを検証する必要があります。準拠を維持するには、評価の完了後も代替コントロールが有効性を保つためのプロセスと管理が整えられている必要があります。

付録 C: 代替コントロールワークシート

このワークシートを使用して、**PCI DSS** 要件を満たすために代替コントロールが使用される要件について代替コントロールを定義します。代替コントロールは、対応する **PCI DSS** 要件セクション内の準拠に関するレポートにも文書化する必要があります。

注: 準拠を実現するために代替コントロールの使用を検討できるのは、リスク分析を実施済みで、正当なテクノロジまたはビジネス上の制約がある企業のみです。

要件番号と定義:

	必要な情報	説明
1. 制約	元の要件への準拠を不可能にする制約を列挙する。	
2. 目的	元のコントロールの目的を定義し、代替コントロールによって満たされる目的を特定する。	
3. 特定されるリスク	元のコントロールの不足によって生じる追加リスクを特定する。	
4. 代替コントロールの定義	代替コントロールを定義し、元のコントロールの目的および追加リスク（ある場合）にどのように対応するかを説明する。	
5. 代替コントロールの検証	代替コントロールの検証およびテスト方法を定義する。	
6. 維持	代替コントロールを維持するために実施するプロセスおよび管理を定義する。	

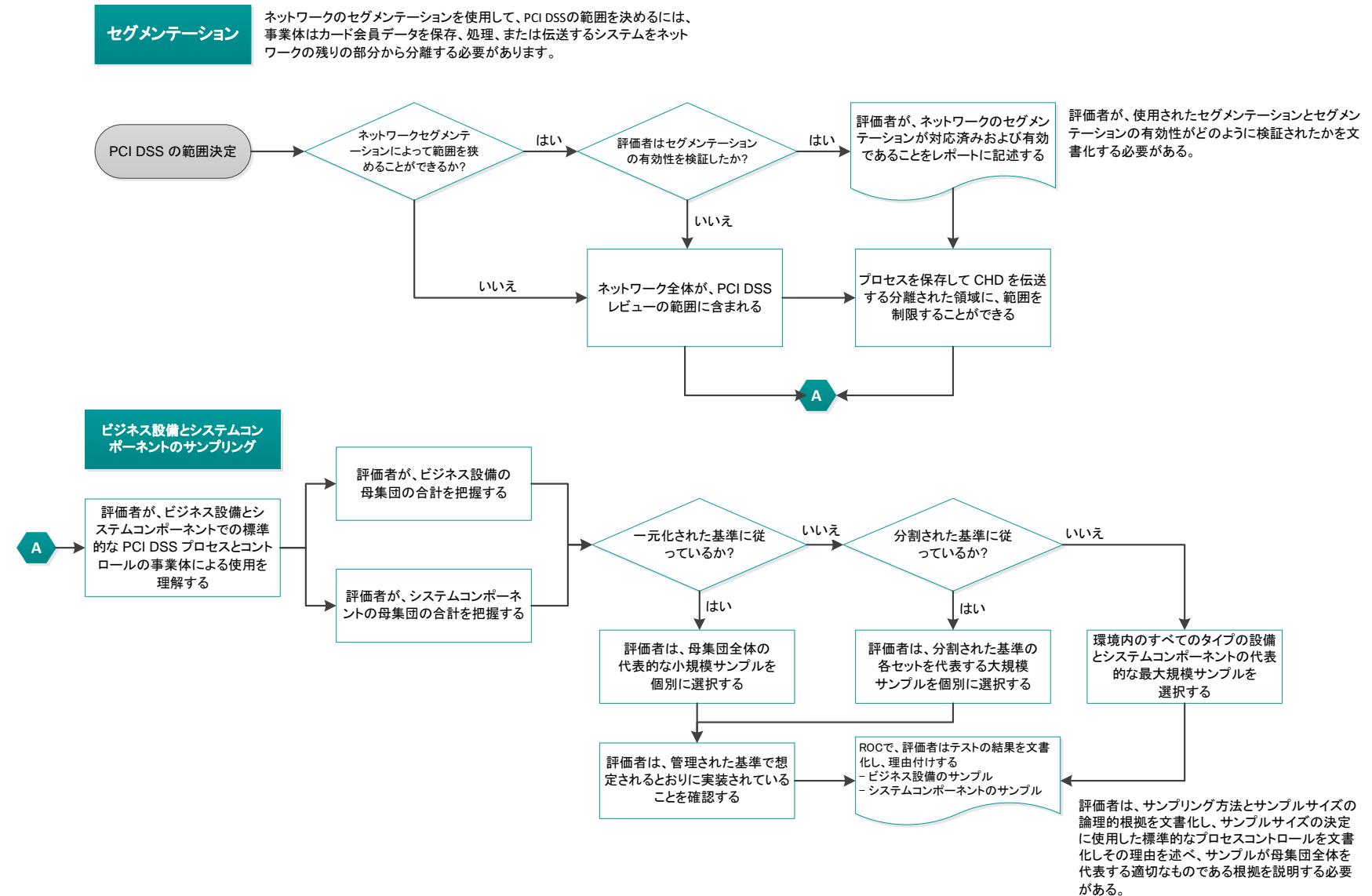
代替コントロールワークシート - 完成例

このワークシートを使用して、代替コントロールにより「対応」と記載された要件について代替コントロールを定義します。

要件番号:8.1.1 — システムコンポーネントまたはカード会員データへのアクセスを許可する前に、すべてのユーザに一意の ID が割り当てられているか?

	必要な情報	説明
1. 制約	元の要件への準拠を不可能にする制約を列挙する。	XYZ 社は、スタンドアロンの Unix サーバを LDAP なしで導入します。このため、それぞれのサーバが "root" ログインを必要とします。XYZ 社が "root" ログインを管理することは不可能であり、各ユーザによるすべての "root" アクティビティをログに記録することも不可能です。
2. 目的	元のコントロールの目的を定義し、代替コントロールによって満たされる目的を特定する。	一意のログインを要求する目的は 2 つあります。まず、ログイン資格情報を共有することはセキュリティの観点から許容されません。次に、共有ログインでは、1 人が特定のアクションの責任を負うことを断定できません。
3. 特定されるリスク	元のコントロールの不足によって生じる追加リスクを特定する。	すべてのユーザが一意の ID を持ち、すべてのユーザを追跡できることを確実にできないことにより、アクセス制御システムに追加リスクがもたらされます。
4. 代替コントロールの定義	代替コントロールを定義し、元のコントロールの目的および追加リスク（ある場合）にどのように対応するかを説明する。	XYZ 社は、標準のユーザアカウントを使用して、"sudo" コマンドを使用することでいくつかの管理用のコマンドを実行する予定です。sudo を使用すると、ユーザは "root" アカウント権限同様で事前定義のコマンドを実行でき、セキュリティログ内に sudo によって記録を残すことが可能です。この方法では、「ルート」パスワードをユーザと共有することなく、各ユーザのアクションを個々のユーザアカウントごとに追跡できます。
5. 代替コントロールの検証	代替コントロールの検証およびテスト方法を定義する。	XYZ 社は、sudo コマンドが "sudoers" ファイルの適切な構成によって、特定のユーザにのみ事前定義のコマンドを実行することができ、すべての活動が個々の sudo のログが識別でき、個々の "root" 権限のアクションが実行できることを評価者に示します。
6. 維持	代替コントロールを維持するために実施するプロセスおよび管理を定義する。	XYZ 社は、sudo 構成が変更されたり削除されたりして、個々のユーザが個々に識別、追跡またはログに記録されることなく特権コマンドを実行できるようにならないようにするためにのプロセスおよび手順を文書化します。

付録 D: ビジネス設備とシステムコンポーネントのセグメンテーションとサンプリング



翻訳協力会社

この翻訳文書は、日本カード情報セキュリティ協議会および以下の QSA 各社の協力により作成されました。

 JCDSC Japan Card Data Security Consortium	日本カード情報セキュリティ協議会
 Infosec	株式会社インフォセック
 NRI SECURE TECHNOLOGIES	NRI セキュアテクノロジーズ株式会社
 NTT DATA NTTデータ 先端技術株式会社	NTT データ先端技術株式会社
 国際マネジメントシステム認証機構 International Certificate Authority of Management System	国際マネジメントシステム認証機構株式会社
 net one	ネットワンシステムズ株式会社
 bsi.	BSI グループジャパン株式会社
 FUJITSU	富士通株式会社
 株式会社ブロードバンドセキュリティ BBSec	株式会社ブロードバンドセキュリティ