# 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 1.2**

2008 年 10 月

# 目次

# 概論および PCI データセキュリティ基準の概要

Payment Card Industry（PCI）データセキュリティ基準（DSS）は、カード会員のデータ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。この文書『PCI データセキュリティ基準の要件とセキュリティ評価手順』では、12 PCI DSS 要件を基盤として使用し、これらの要件と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、PCI DSS への準拠を確認する必要のある加盟店とサービスプロバイダのために、オンサイトレビューを実施する評価担当者を対象に作成されています。以下に、12 PCI DSS 要件を概説します。その後、数ページに渡って、PCI DSS 評価の準備作業、実施、レポートについて説明します。PCI DSS 要件の詳細については、13 ページから説明します。

## 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こと |
| 要件 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、ベンダ提供のデフォルト値を使用しないこと |
| **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の保護 |
| 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、暗号化すること |
| **脆弱性管理プログラムの整備** | |
| 要件 5 | アンチウィルスソフトウェアを使用し、定期的に更新すること |
| 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、保守すること |
| **強固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こと |
| 要件 8 | コンピュータにアクセスできる各ユーザに一意の ID を割り当てる |
| 要件 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** | |
| 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 |
| 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 |
| **情報セキュリティにポリシーの整備** | |
| 要件 12 | 情報セキュリティポリシーを整備する |

# PCI DSS 適用性情報

次の表は、カード会員とセンシティブ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。

| | データ要素 | 保存の許可 | 保護の必要性 | PCI DSS 要件 3.4 |
|---|---|---|---|---|
| **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 | はい |
| | カード会員名 [1] | はい | はい [1] | いいえ |
| | サービス コード [1] | はい | はい [1] | いいえ |
| | 有効期限 [1] | はい | はい [1] | いいえ |
| **センシティブ認証データ** [2] | 完全な磁気ストライプデータ [3] | いいえ | N/A | N/A |
| | CAV2/CVC2/CVV2/CID | いいえ | N/A | N/A |
| | PIN/PIN ブロック | いいえ | N/A | N/A |

1 *これらのデータ要素は、PAN と共に保存される場合は保護が必要です。この保護は、カード会員データ環境の全般的な保護に関する PCI DSS 要件に従います。さらに、他の法律（消費者の個人データ保護、プライバシ、ID 盗難、またはデータセキュリティに関連するものなど）により、このデータの特定の保護、または取引過程で消費者関連の個人データが収集される場合は会社の実施方法の適切な開示が必要になる可能性があります。ただし、PCI DSS は、PAN が保存、処理、または伝送されない場合は適用されません。*

2 *センシティブ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 *磁気ストライプのすべてのトラックのデータ、チップなどに存在する磁気ストライプイメージ。*

# PCI DSS 要件への準拠の評価範囲

PCI DSS セキュリティ要件は、すべてのシステムコンポーネントに適用されます。システムコンポーネントとは、カード会員データ環境に含まれる、またはこれに接続するすべてのネットワークコンポーネント、サーバ、またはアプリケーションとして定義されます。カード会員データ環境とは、カード会員データまたはセンシティブ認証データを保有するネットワークの一部です。ネットワークコンポーネントにはファイアウォール、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などが含まれますが、これらに限定されるわけではありません。 サーバタイプには、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)、ドメインネームサーバ(DNS)などが含まれますが、これらに限定されるわけではありません。アプリケーションには、内部および外部(インターネット)アプリケーションなど、すべての市販およびカスタムアプリケーションが含まれます。

### *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企業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 コントロールの実装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、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持つルーターによって実現できます。

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。不必要な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によって大きく左右されます。

*付録 F: PCI DSS レビュー – サンプルの範囲設定および選択に*、評価時の範囲設定の効果について詳しく説明されています。

### *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、伝送する場合（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（LAN）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（ファイアウォールによって明確に分離されていない場合など）、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実装する前に、企業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センシティブ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/アウトソーシング*

年 1 回オンサイト評価を受ける必要のあるサービスプロバイダは、カード会員データを保存、処理、伝送するすべてのシステムコンポーネントに対して準拠確認を行う必要があります。

サービスプロバイダまたは加盟店は第三者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。

カード会員データの保存、処理、伝送を第三者サービスプロバイダにアウトソースする事業体は、準拠に関するレポート（ROC）に各サービスプロバイダの役割を記述し、レビュー対象の事業体に適用する要件とサービスプロバイダに適用する要件を明確に区別する必要があります。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）自ら PCI DSS 評価を受け、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）独自の PCI DSS 評価を受けない場合、顧客の各 PCI DSS 評価コース中にサービスのレビューを受ける必要があります。詳細については、「準拠に関するレポートについての指示と内容」セクションの第 3 部の「管理サービスプロバイダ（MSP）のレビューの場合」で始まる箇条書きを参照してください。

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。*

### *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*

評価担当者は、PCI DSS 要件を評価するために、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選択できます。サンプルには、ビジネス設備とシステムコンポーネントの両方が含まれている必要があります。また、ビジネス設備のすべてのタイプと場所、および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、評価担当者がコントロールが予定どおりに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、フランチャイズ加盟店、さまざまな場所のビジネス設備などが挙げられます。サンプリングには、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。たとえば、各ビジネス設備に、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。各ビジネス設備で、評価担当者は Apache WWW 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 サーバなどを選択できます。すべてのアプリケーションが単一 OS（Windows、Sun 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。*(「付録 F: PCI DSS レビュー - サンプルの範囲設定および選択」を参照してください。)*

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

- 各設備が従うべき標準の必須 PCI DSS プロセスがある場合、各設備が標準プロセスに合わせて構成されていることを適切に保証するためのサンプルは、標準プロセスがない場合に必要とされる量より少なくて済みます。
- 複数タイプの標準プロセスがある場合（さまざまなタイプのシステムコンポーネントまたは設備など）、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システムコンポーネントまたは設備を含む十分な量でなければなりません。
- 標準の PCI DSS プロセスがなく、各設備がそれぞれのプロセスの責任を担っている場合、各設備で PCI DSS 要件を正しく理解し、実装していることを保証するため、サンプルの量は多くなければなりません。

*「付録 F: PCI DSS レビュー - サンプルの範囲設定および選択」も参照してください。*

### *代替コントロール*

毎年、代替コントロールを文書化し、レビューし、評価担当者が検証し、「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、準拠に関するレポートの PCI DSS 要件セクションに記載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についての指示と内容

この文書は、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。レポート要件と手順については、各ペイメントブランドに問い合わせてください。

### *レポートの内容と形式*

準拠に関するレポートを作成する際、レポートの内容と形式については次の指示に従ってください。

1. **概要**

   以下の内容を含めます。

   - 事業体のペイメントカード業務について記述します。
     - ペイメントカードに関して実行する業務。カード会員データの保存、処理、伝送方法およびその理由。

       *注: 事業体の Web サイトからカットアンドペーストするのではなく、評価担当者がペイメントおよび事業体の役割を理解していることを示す記述を行う必要があります。*
     - 支払の処理方法（直接、間接など）
     - 使用する支払チャネルのタイプ。カードを提示しないチャネル（mail-order-telephone-order （MOTO）、電子商取引など）、またはカードを提示するチャネルなど。
     - プロセッサ関係を含め、支払伝送または処理のために接続する事業体
   - 以下を含む、事業体のネットワーク構成の概要ネットワーク図（事業体から入手または評価担当者が作成）。
     - ネットワークへの、またはネットワークからの接続
     - POS デバイス、システム、データベース、Web サーバなど、カード会員データ環境内の重要なコンポーネント
     - 他の必要なペイメントコンポーネント

## 2. 作業範囲および実行するアプローチの説明

この文書の評価範囲に関するセクションに従って、以下を含む範囲を記述します。

- 評価の対象となった環境（クライアントのインターネットアクセスポイント、内部企業ネットワーク、接続処理など）
- 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 レビューの対象範囲が狭められている場合、セグメンテーションについて簡単に説明し、評価担当者がセグメンテーションの有効性をどのように検証したかを説明します
- 両方の事業体（店舗、設備など）に使用されたサンプリング、および選択したシステムコンポーネントの根拠を示し、文書化します
  - 母集団の合計
  - サンプル抽出数
  - 選択したサンプルの論理的根拠
  - サンプルの量が、事業体全体において、レビューしたコントロールが対応済コントロールであると評価担当者が信頼できるだけの十分な量である理由。
  - レビュー範囲から除外された、カード会員データを保存、処理、伝送する場所または環境、およびこれらの場所/環境が除外された理由
- PCI DSS 準拠を必要とする 100% 子会社、およびこれらの子会社を別個にレビューするか、この評価の一部としてレビューするか
- PCI DSS 準拠を必要とする海外事業体、およびこれらの事業体を別個にレビューするか、この評価の一部としてレビューするか
- カード会員データ環境に接続している、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可能性がある、ワイヤレス LAN およびワイヤレスペイメントアプリケーション（POS 端末など）、およびこれらのワイヤレス環境のセキュリティ
- 評価を実施する際に使用する『PCI DSS 要件およびセキュリティ評価手順』文書のバージョン
- 評価期間

## 3. レビュー環境の詳細

このセクションでは、以下について詳しく説明します。

- LAN、WAN、インターネットなど、各通信リンクの図
- カード会員データ環境についての説明
  - 承認、キャプチャ、決済、チャージバック、その他のフローを含め、カード会員データの伝送と処理の文書化

  - カード会員データを保存するファイルとテーブルのリスト。評価担当者が作成（またはソフトウェアベンダから入手）して報告書に記録されているインベントリによって裏付けます。このインベントリには、カード会員データストア（ファイル、テーブルなど）ごとに、以下を含めます。
    - 保存されているカード会員データのすべての要素のリスト
    - データのセキュリティ保護方法
    - データストアへのアクセスのログ方法
- カード会員データ環境で使用されているハードウェアおよび重要なソフトウェアのリストと、それぞれの機能/用途の説明
- 企業がカード会員データを共有するサービスプロバイダと他の事業体のリスト（注意: これらの事業体は PCI DSS 要件 12.8 に準拠する事業体です）
- 使用する第三者ペイメントアプリケーション製品とバージョン番号のリスト。各ペイメントアプリケーションが PA-DSS に従って検証されているかを含みます。ペイメントアプリケーションが PA-DSS 検証済であっても、評価担当者はそのアプリケーションが PCI DSS に準拠した方法および環境で、ペイメントアプリケーションベンダの PA-DSS 実装ガイドに従って実装されたことを確認する必要があります。*注: PA-DSS 検証済アプリケーションの使用は、PCI DSS 要件ではありません。それぞれの PA-DSS 準拠要件を把握するには、各ペイメントブランドに個別に問い合わせてください。*
- インタビューした個人とその肩書きのリスト
- レビューされる文書の一覧
- 管理サービスプロバイダ（MSP）のレビューの場合、評価担当者はこの文書のどの要件が MSP に適用され、どれがレビューに含まれず、MSP の顧客がレビューを担当するか、を明確に識別する必要があります。MSP のどの IP アドレスを MSP の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 MSP の顧客の独自の四半期スキャンに含めるかを記述します。

### 4. 連絡先情報とレポート日

以下を記述します。

- 加盟店またはサービスプロバイダと評価担当者の連絡先情報
- レポートの日付

### 5. 四半期ごとのスキャンの結果

- 要件 11.2 だけでなく、「概要」でも最新の 4 回の四半期ごとのスキャンの結果について簡単に記述します。

  *注: 1）最新のスキャン結果が過去のスキャンだった、2）事業体が今後の四半期ごとのスキャンに必要なポリシーと手順を文書化している、3）初期スキャンで記録された脆弱性が再スキャンで修正されている、ことを評価担当者が確認する場合、初回 PCI DSS 準拠で過去 4 回の四半期ごとのスキャンを調査する必要ありません。以降は、初回 PCI DSS レビュー後に、過去 4 回の四半期ごとのスキャンを調査する必要があります。*

- 「PCI DSS Security Scanning Procedures」に従って、スキャンでは、事業体に存在する外部アクセス可能なすべての（インターネットに露出している）IP アドレスを対象に含める必要があります。

**6. 発見内容と所見**

- 「概要」に、標準の「準拠に関するレポート」テンプレートフォーマットに適合しない事項を要約します。
- すべての評価担当者は、詳細な「PCI DSS 要件およびセキュリティ評価手順」テンプレートを使用して、各要件とサブ要件に関する、詳しいレポート記述および発見した事項を提供する必要があります。
- 評価担当者は、この代替コントロールによってコントロールが対応済になったと判断した、すべての代替コントロールをレビューして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、上の「代替コントロール」セクションと付録 B と C を参照してください。

### *未解決項目の再確認*

準拠確認には、「コントロール対応」レポートが必要です。未解決項目が含まれる場合、または将来日付に終了する項目が含まれる場合、レポートは非準拠とみなされます。加盟店/サービスプロバイダは、確認を終了する前に、これらの項目に対処する必要があります。加盟店/サービスプロバイダがこれらの項目に対処した後、評価担当者は、改善が施され、すべての要件が満たされていることを再評価します。再評価後、評価担当者はカード会員データ環境が完全準拠であることを確認して、新しい準拠に関するレポートを発行し、指示に従って提出します（以下を参照）。

### *PA-DSS 準拠 - 完了手順*

1. 上述の「検証レポートに関する指示と内容」セクションに従って、準拠に関するレポート（ROC）を完成させます。
2. 過去の脆弱性スキャンが PCI SSC Approved Scanning Vendor（ASV）によって実行されたことを確認し、ASV から過去のスキャンの証拠を入手します。
3. 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。準拠証明書については、付録 D と E を参照してください。
4. ROC、過去のスキャンの証拠、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。

# 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ヘッダーを定義します。

- **PCI DSS 要件** - この列では、データセキュリティ標準を定義し、PCI DSS 準拠を達成するための要件を表示します。これらの要件への準拠が検証されます。
- **テスト手順** - この列では、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を表示します。
- **対応** - この列は、代替コントロールの結果として対応されているコントロールを含め、評価担当者が対応されているコントロールを簡単に説明するために使用します。(注: この列は、まだ対応されていない項目または将来日付に終了する未解決項目には使用しないでください。)
- **未対応** - この列は、評価担当者が未対応のコントロールを簡単に説明するために使用します。特に要求された場合を除き、非準拠レポートをペイメントブランドまたはアクワイアラーに提出しないでください。 非準拠レポートの詳細については、付録 D と付録 E: 準拠証明書を参照してください。
- 目標期日/コメント - 評価担当者は「未対応」コントロールに、加盟店またはサービスプロバイダがコントロールが「対応」になるのを期待する目標期日を記載する必要があります。その他の注記またはコメントも記載できます。

# 安全なネットワークの構築と維持

## *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こと*

ファイアウォールは企業のネットワーク（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、および企業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コンピュータ装置です。企業の信頼できるネットワーク内の非常に機密性の高い領域の例として、カード会員データ環境が挙げられます。

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査して、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。

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **1.1** 以下を含むファイアウォールおよびルーター構成基準を確立する | **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文書を入手および検査し、標準が完全であることを確認する。次の各項目に記入する。 | | | |
| **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** 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、正式なプロセスがあることを確認する。 | | | |
| **1.1.2** ワイヤレスネットワークを含む、カード会員データへのすべての接続を示す最新ネットワーク図 | **1.1.2.a** 最新のネットワーク図（ネットワーク上のカード会員データフローを示す図など）が存在し、ワイヤレスネットワークを含む、カード会員データへのすべての接続が記載されていることを確認する。 | | | |
| | **1.1.2.b** 図が最新のものであることを確認する。 | | | |
| **1.1.3** 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 | **1.1.3** ファイアウォール構成基準に、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。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。 | | | |
| **1.1.4** ネットワークコンポーネントの論理的管理のためのグループ、役割、責任に関する記述 | **1.1.4** ファイアウォール/ルーター構成基準に、ネットワークコンポーネントの論理的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。 | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **1.1.5** 使用が許可されているすべてのサービス、プロトコル、ポートの文書化。および使用が許可されている業務上の理由（安全でないとみ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） | **1.1.5.a** ファイアウォール/ルーター構成基準に、業務に必要なサービス、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（HTTP、SSL、SSH、VPN プロトコルなど）。 | | | |
| | **1.1.5.b** 許可されている安全でないサービス、プロトコル、ポートを識別し、それらが必要であり、セキュリティ機能が文書化されており、審査されたファイアウォール/ルーター構成基準および各サービスの設定によって実装されていることを確認する。安全でないサービス、プロトコル、ポートの例として、ユーザー資格情報をクリアテキストで渡す FTP が挙げられる。 | | | |
| **1.1.6** 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 | **1.1.6.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。 | | | |
| | **1.1.6.b** 文書を入手および調査して、ルールセットが少なくとも 6 カ月ごとにレビューされることを確認する。 | | | |
| **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との接続を制限する、ファイアウォール構成を構築する。 | **1.2** ファイアウォール/ルーター構成を調査して、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。 | | | |
| *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。* | | | | |
| **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制限する。 | **1.2.1.a** 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おり、制限が文書化されていることを確認する。 | | | |
| | **1.2.1.b** たとえば明示の「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。 | | | |
| **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。 | **1.2.2** ルーター構成ファイルがセキュリティ保護され同期化されていることを確認します。たとえば、実行構成ファイル（ルーターの標準実行に使用）とスタートアップ構成ファイル（マシンの再起動時に使用）が同じセキュリティ保護構成であることを確認する。 | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **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、ワイヤレス環境からカード会員データ環境へのすべてのトラフィックを拒否または制御（そのようなトラフィックが業務上必要な場合）するようにファイアウォールを構成する。 | **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を保存するシステムの間に、境界ファイアウォールがインストールされ、ワイヤレス環境からカード会員データ環境へのすべてのトラフィックを拒否または制御（そのようなトラフィックが業務上必要な場合）するようにファイアウォールが構成されていることを確認する。 | | | |
| **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/ルーター構成を以下に説明するとおりに調査し、インターネットと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。 | | | |
| **1.3.1** DMZ を実装し、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制限する。 | **1.3.1** DMZ が実装され、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。 | | | |
| **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。 | **1.3.2** 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。 | | | |
| **1.3.3** インターネットとカード会員データ環境間トラフィックの、すべての直接経路（着信/発信）を使用不可にする。 | **1.3.3** インターネットとカード会員データ環境間トラフィックの、直接経路（着信/発信）がないことを確認する。 | | | |
| **1.3.4** インターネットから DMZ 内へ通過できる内部インターネットアドレスを禁止する。 | **1.3.4** 内部アドレスがインターネットから DMZ 内へ通過できないことを確認する。 | | | |
| **1.3.5** 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、DMZ 内の IP アドレスにのみアクセス可能なように制限する。 | **1.3.5** 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、DMZ 内の IP アドレスにのみアクセス可能であることを確認する。 | | | |
| **1.3.6** 動的パケットフィルタリングとも呼ばれる、ステートフルインスペクションを実装する。（ネットワーク内へは、「確立された」接続のみ許可される。） | **1.3.6** ファイアウォールがステートフルインスペクション（動的パケットフィルタリング）を実行することを確認する。[確立された接続のみ許可され、前に確立されたセッションに関連付けられている場合にのみ許可される必要がある（すべての TCP ポートで “syn reset” または ”syn ack” ビットを設定してポートスキャナを実行する。レスポンスがあった場合、前に接続されたセッションの一部でないにも関わらず、パケットが許可されていることになる。）] | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **1.3.7** DMZ から分離された内部ネットワークゾーンに、データベースを配置する。 | **1.3.7** DMZ から分離された内部ネットワークゾーンに、データベースが配置されていることを確認する。 | | | |
| **1.3.8** RFC 1918 アドレス領域を使用して、IP マスカレードを実装し、内部アドレスが変換されインターネット上で露出することを防ぐ。ポート アドレス変換(PAT)などのネットワークアドレス変換(NAT)テクノロジを使用する。 | **1.3.8** ファイアウォールおよびルーターコンポーネントのサンプルについて、RFC 1918 アドレス領域を使用する NAT などのテクノロジを使用して内部ネットワークからインターネットへの IP アドレスのブロードキャストが制限されていることを確認する(IP マスカレード)。 | | | |
| **1.4** インターネットに直接接続するすべてのモバイルコンピュータまたは従業員所有のコンピュータ(あるいはその両方)で、企業ネットワークへのアクセスに使用されるものに(従業員が使用するラップトップなど)、パーソナルファイアウォールソフトウェアをインストールする。 | **1.4.a** インターネットに直接接続するモバイルコンピュータまたは従業員所有のコンピュータ(あるいはその両方)で、企業ネットワークへのアクセスに使用されるものに(従業員が使用するラップトップなど)、パーソナルファイアウォールソフトウェアをインストールされ、有効になっていることを確認する。 | | | |
| | **1.4.b** パーソナルファイアウォールソフトウェアが企業固有の基準で構成され、その構成がモバイルコンピュータユーザーによって変更可能でないことを確認する。 | | | |

## *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こと*

（社内外の）悪意のある人々は多くの場合、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 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **2.1** システムをネットワーク上に導入する**前に**、ベンダ提供のデフォルト値を必ず変更する（パスワード、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変更、不必要なアカウントの削除など）。 | **2.1** システムコンポーネント、重要なサーバ、ワイヤレスアクセスポイ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）、デフォルトのアカウントとパスワード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。） | | | |
| **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**、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キー、パスワード、SNMP コミュニティ文字列が含まれる（ただし、これらに限定されない）。認証および伝送のために、強力な暗号化技術のワイヤレスデバイスセキュリティ設定が有効になっていることを確認する。 | **2.1.1** ワイヤレス環境のベンダデフォルト設定について、次の事項を確認し、すべてのワイヤレスネットワークに強力な暗号化メカニズム（AES など）が実装されていることを確認する。<br>▪ 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。また、キーの知識を持つ人物が退社または異動するたびに、キーが変更されていること。<br>▪ 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変更されてること。<br>▪ アクセスポイントのデフォルトのパスワード/パスフレーズが変更されてること。<br>▪ ワイヤレスデバイスのファームウェアが更新され、ワイヤレスネットワーク経由の認証および伝送用の強力な暗号化をサポートしていること（WPA/WPA2 など）。<br>▪ その他、セキュリティに関連するワイヤレスベンダのデフォルト値 | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **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。 | **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査し、システム構成基準が SysAdmin Audit Network Security（SANS）、National Institute of Standards Technology（NIST）、Center for Internet Security（CIS）など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。 | | | |
| | **2.2.b** システム構成基準に、次の項目（2.2.1 ～ 2.2.4）が含まれていることを確認する。 | | | |
| | **2.2.c** 新しいシステムを構成する際に、システム構成基準が適用されていることを確認する。 | | | |
| **2.2.1** 1 つのサーバには、主要機能を 1 つだけ実装する。 | **2.2.1** システムコンポーネントのサンプルについて、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。たとえば、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。 | | | |
| **2.2.2** 安全性の低い不必要なサービスおよびプロトコルはすべて無効にする（デバイスの特定機能を実行するのに直接必要でないサービスおよびプロトコル）。 | **2.2.2** システムコンポーネントのサンプルについて、有効なシステムサービス、デーモン、プロトコルを検査する。不要なまたは安全性の低いサービスおよびプロトコルが無効になっていること、またはサービスの適切な使用の根拠が示され、文書化されていることを確認する。（たとえば、FTP が使用されていない、または SSH などの技術によって暗号化されているなど。） | | | |
| **2.2.3** システムの誤用を防止するためにシステムセキュリティパラメータを構成する。 | **2.2.3.a** システム管理者またはセキュリティマネージャ（あるいはその両方）にインタビューし、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に関する知識があることを確認する。 | | | |
| | **2.2.3.b** システム構成基準に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。 | | | |
| | **2.2.3.c** システムコンポーネントのサンプルについて、一般的なセキュリティパラメータが適切に設定されていることを確認する。 | | | |
| **2.2.4** 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。 | **2.2.4** システムコンポーネントのサンプルについて、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。有効な機能が文書化され、セキュリティ構成をサポートし、文書化された機能のみがサンプルマシンに存在することを確認する。 | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **2.3** すべてのコンソール以外の管理アクセスを暗号化する。Web ベースの管理やその他のコンソール以外の管理アクセスについては、SSH、VPN、または SSL/TLS などのテクノロジを使用する。 | **2.3** システムコンポーネントのサンプルについて、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。<br>▪ 各システムへの管理者ログオンを見て、管理者パスワードが要求される前に、強力な暗号化方式が実行されていることを確認する。<br>▪ システム上のサービスおよびパラメータファイルを確認して、Telnet などのリモートログインコマンドが内部で使用不可になっていることを確認する。<br>▪ Web ベース管理インターフェイスへの管理者アクセスが、強力な暗号化技術で暗号化されていることを確認する。 | | | |
| **2.4** 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。*「付録 A: 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要件を満たす必要がある。* | **2.4** 共有ホスティングプロバイダの PCI DSS 評価について、「付録 A: 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 **A.1.1** ～ **A.1.4** 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。 | | | |

# カード会員データの保護

## *要件 3: 保存されたカード会員データを保護すること*

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。侵入者が他のネットワーク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、正しい暗号化キーがなければ、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。たとえば、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、暗号化されていない電子メールで 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 Glossary of Terms, Abbreviations, and Acronyms」を参照してください。

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **3.1** 保存するカード会員データは最小限に抑える。データの保存と廃棄に関するポリシーを作成する。データ保存ポリシーに従って、保存するデータ量と保存期間を、業務上、法律上、規則上必要な範囲に限定する。 | **3.1** データの保存と廃棄に関する会社のポリシーおよび手順を入手して検討し、以下を実行する。<br>▪ ポリシーと手順にデータ保存に関する法律上、規則上、業務上の要件が含まれていることを確認する。これにはカード会員データの保存に関する具体的な要件が含まれる(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)。<br>▪ ポリシーと手順に、法律上、規則上、業務上の必要性がなくなった場合のデータの廃棄(カード会員データの廃棄を含む)に関する措置が含まれていることを確認する。<br>▪ ポリシーと手順で、カード会員データの保存に関するすべてがカバーされていることを確認する。<br>▪ ポリシーと手順に、業務上の保存要件を超えて保存されているカード会員データを少なくとも四半期ごとに削除する自動プロセス、または保存されたカード会員データが業務上の保存要件を超えていないかを確認するために少なくとも四半期ごとに実施するレビュー要件が含まれていることを確認する。 | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **3.2** 承認後にセンシティブ認証データを保存しない（暗号化されている場合でも）。<br>センシティブ認証データには、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。 | **3.2** センシティブ認証データを受け取ったり削除したりする場合、データを確実に復元不可能にするための削除手順を入手してレビューする。<br>センシティブ認証データの各項目に対して、以下の手順を実行する。 | | | |
| **3.2.1** 磁気ストライプのいかなるトラックのいかなる内容も保存しない（カードの裏面、チップ内、その他に存在する）。このデータは、全トラック、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る。<br>*注: 通常の業務範囲では、磁気ストライプの以下のデータ要素を保存する必要が生じる場合がある。*<br>▪ *カード会員名*<br>▪ *プライマリアカウント番号（PAN）*<br>▪ *有効期限*<br>▪ *サービスコード*<br>*リスクを最小限に抑えるため、業務上必要なデータ要素のみを保存する。*<br>*注:* 詳細については、「PCI DSS Glossary of Terms, Abbreviations, and Acronyms」を参照。 | **3.2.1** システムコンポーネントのサンプルを調査し、以下の項目について、カード裏面の磁気ストライプから得られたトラック内容が、いかなる状況においても保存されていないことを確認する。<br>▪ 受信トランザクションデータ<br>▪ 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）<br>▪ 履歴ファイル<br>▪ トレースファイル<br>▪ データベーススキーマ<br>▪ データベースコンテンツ | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **3.2.2** カードを提示しない取引の確認に使用されるカード検証コードまたは値(ペイメントカードの前面または裏面に印字された 3 桁または 4 桁の数字)を保存しない。<br>*注:* 詳細については、『PCI DSS Glossary of Terms, Abbreviations, and Acronyms』を参照。 | **3.2.2** システムコンポーネントのサンプルについて、カード前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)がいかなる状況においても保存されていないことを確認します。<br>▪ 受信トランザクションデータ<br>▪ 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)<br>▪ 履歴ファイル<br>▪ トレースファイル<br>▪ データベーススキーマ<br>▪ データベースコンテンツ | | | |
| **3.2.3** 個人識別番号(PIN)または暗号化された PIN ブロックを保存しない。 | **3.2.3** システムコンポーネントのサンプルを調査し、以下の各項目について、PIN および暗号化された PIN ブロックがいかなる状況においても保存されていないことを確認する。<br>▪ 受信トランザクションデータ<br>▪ 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)<br>▪ 履歴ファイル<br>▪ トレースファイル<br>▪ データベーススキーマ<br>▪ データベースコンテンツ | | | |
| **3.3** 表示する際に PAN をマスクする(最大でも最初の 6 桁と最後の 4 桁のみを表示)。<br>*注:*<br>▪ *従業員およびその他の関係者が、業務上の合法的なニーズにより PAN 全体を見る必要がある場合、この要件は適用されない。*<br>▪ *カード会員データの表示に関するこれより厳しい要件(POS レシートなど)がある場合は、そちらに置き換えられる。* | **3.3** 文書化されたポリシーを入手および検討し、PAN の表示(画面、紙のレシートなど)を調査して、業務上の合法的なニーズにより PAN 全体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。 | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **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)。<br>▪ 強力な暗号化技術をベースにしたワンウェイハッシュ<br>▪ トランケーション<br>▪ 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)<br>▪ 関連するキー管理プロセスおよび手順を伴う、強力な暗号化<br>アカウント情報のうち、少なくとも PAN は読み取り不能にする必要がある。<br>*注:*<br>▪ *何らかの理由で PAN を読み取り不能にできない場合は、「付録 B: 代替コントロール」を参照。*<br>▪ 強力な暗号化技術は、「PCI DSS Glossary of Terms, Abbreviations, and Acronyms」で定義されています。 | **3.4.a** 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入手して検討する。次のいずれかの方法により、PAN が読み取り不能になっていることを確認する。<br>▪ 強力な暗号化技術をベースにしたワンウェイハッシュ<br>▪ トランケーション<br>▪ 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)<br>▪ 関連するキー管理プロセスおよび手順を伴う、強力な暗号化 | | | |
| | **3.4.b** データリポジトリのサンプルからいくつかのテーブルまたはファイルを調査し、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)。 | | | |
| | **3.4.c** リムーバブルメディア(バックアップテープなど)のサンプルを調査し、PAN が読み取り不能になっていることを確認する。 | | | |
| | **3.4.d** 監査ログのサンプルを調査し、PAN の不適切な部分が削除されているか、PAN がログから削除されていることを確認する。 | | | |
| **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を使用しないなどの方法で)。 | **3.4.1.a** ディスク暗号化を使用している場合、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を使用しないなどの方法で)。 | | | |
| | **3.4.1.b** 暗号化キー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)。 | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| 暗号解除キーをユーザアカウントに結合させてはいけない。 | **3.4.1.c** 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。<br>*注: ディスク暗号化では、しばしばリムーバブルメディアを暗号化できないことがあるため、リムーバブルメディアに保存されたデータは別個に暗号化する必要がある。* | | | |
| **3.5** カード会員データの暗号化に使用される暗号化キーを、漏洩と誤使用から保護する。 | **3.5** 以下の項目を確認して、カード会員データの暗号化に使用されているキーを、漏洩と誤使用から保護するためのプロセスを確認する。 | | | |
| **3.5.1** 暗号化キーへのアクセスを、必要最小限の管理者に制限する。 | **3.5.1** ユーザーアクセスリストを調査し、キー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。 | | | |
| **3.5.2** 暗号化キーの保存場所と形式を最小限にし、安全に保存する。 | **3.5.2** システム構成ファイルを調査し、キーが暗号化された形式で保存され、キー暗号化キーがデータ暗号化キーとは別個に保存されていることを確認する。 | | | |
| **3.6** カード会員データの暗号化に使用されるキー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。 | **3.6.a** カード会員データの暗号化に使用するキーの管理手順が存在することを確認する。<br>*注: キー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。* | | | |
| | **3.6.b** サービスプロバイダのみ: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キーを顧客と共有している場合、顧客のキー(顧客とサービスプロバイダの間でデータを伝送するために使用される)を安全に保存および変更する方法が記述された文書を、サービスプロバイダが顧客に提供していることを確認する。 | | | |
| | **3.6.c** キー管理手順を調査し、以下を実行する。 | | | |
| **3.6.1** 強力な暗号化キーの生成 | **3.6.1** キー管理手順で、強力なキーの生成が要求されていることを確認する。 | | | |
| **3.6.2** 安全な暗号化キーの配布 | **3.6.2** キー管理手順で、安全なキーの配布が要求されていることを確認する。 | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **3.6.3** 安全な暗号化キーの保存 | **3.6.3** キー管理手順で、安全なキーの保存が要求されていることを確認する。 | | | |
| **3.6.4** 定期的な暗号化キーの変更<br>▪ 関連するアプリケーションで必要とされる場合、自動的に行われることが望ましい(再キー入力など)。<br>▪ 少なくとも年 1 回 | **3.6.4** キー管理手順で、定期的なキーの変更が要求されていることを確認する(少なくとも年 1 回)。 | | | |
| **3.6.5** 古いキーまたは危険にさらされた疑いのあるキーの破棄または取替 | **3.6.5.a** キー管理手順で、古いキーの破棄が要求されていることを確認する(アーカイブ、廃棄、廃止など)。 | | | |
| | **3.6.5.b** キー管理手順で、危険にさらされされたことが分かっている、またはその疑いがあるキーの取替が要求されていることを確認する。 | | | |
| **3.6.6** 暗号化キーの知識分割と二重管理 | **3.6.6** キー管理手順で、キーの知識分割と二重管理が要求されていることを確認する(例: キー全体を再構築するには、2 ～ 3 人を必要とし、各自がキーの一部のみを知っている)。 | | | |
| **3.6.7** 暗号化キーの不正置換の防止 | **3.6.7** キー管理手順で、キーの不正置換の防止が要求されていることを確認する。 | | | |
| **3.6.8** 暗号化キー管理者が自身の責務を理解し、それを受諾したことを示す書面への署名 | **3.6.8** キー管理手順で、キー管理者が自身の責務を理解し、それを受諾したことを示す書面への署名が要求されていることを確認する。 | | | |

## 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、暗号化すること

ネットワークには悪意のある人々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、悪意のある人々の標的となります。

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **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、強力な暗号化と SSL/TLS または IPSEC などのセキュリティプロトコルを使用する。<br>*PCI DSS では、オープンな公共ネットワークの例として以下が挙げられる。*<br>▪ *インターネット*<br>▪ *ワイヤレステクノロジ*<br>▪ *Global System for Mobile communications（GSM）*<br>▪ *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合、暗号化（SSL/TLS または IPSEC など）が使用されていることを確認する。<br>▪ データ伝送時に強力な暗号化が使用されていることを確認する。<br>▪ SSL を実装する場合:<br>– サーバが最新のパッチバージョンをサポートしていることを確認する。<br>– ブラウザの URL に HTTPS が表示されることを確認する。<br>– URL に HTTPS が表示されない場合、カード会員データが要求されないことを確認する。<br>▪ 受信時のトランザクションのサンプルを選択してトランザクションを監視し、カード会員データが送信時に暗号化されていることを確認する。<br>▪ 信頼できる SSL/TLS キー/証明書のみが受け付けられていることを確認する。<br>▪ 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。） | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **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しているワイヤレスネットワークには、業界のベストプラクティス（IEEE 802.11i など）を使用して、認証および伝送用に強力な暗号化を実装する。<br>▪ *新しいワイヤレス実装において、2009 年 3 月 31 日以降は WEP を実装できない。*<br>▪ *現在のワイヤレス実装において、2010 年 6 月 30 日以降は WEP を使用できない。* | **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しているワイヤレスネットワークで、業界のベストプラクティス（IEEE 802.11i など）を使用して認証および伝送用に強力な暗号化が実装されていることを確認する。 | | | |
| **4.2** 暗号化されていない 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、チャットなど）で送信しない。 | **4.2.a** エンドユーザメッセージングテクノロジでカード会員データを送信する場合、常に強力な暗号化が使用されていることを確認する。 | | | |
| | **4.2.b** 暗号化されていない PAN をエンドユーザメッセージングテクノロジで送信しないことを規定したポリシーが存在することを確認する。 | | | |

# 脆弱性管理プログラムの整備

## 要件 5: アンチウィルスソフトウェアまたはプログラムを使用し、定期的に更新すること

一般に「マルウェア」と呼ばれる悪意のあるソフトウェア（ウィルス、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、アンチウィルスソフトウェアを使用して、最新の進化するマルウェア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。

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **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、アンチウィルス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、適用可能なアンチウィルステクノロジが存在する場合は、アンチウィルスソフトウェアが導入されていることを確認する。 | | | |
| **5.1.1** すべてのアンチウィルスプログラムは、すべての既知のタイプの悪意のあるソフトウェアに対して検知、駆除、保護が可能でなければならない。 | **5.1.1** システムコンポーネントのサンプルについて、すべてのアンチウィルスプログラムが、すべての既知のタイプの悪意のあるソフトウェア（ウィルス、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）に対して検知、駆除、保護が可能であることを確認する。 | | | |
| **5.2** すべてのアンチウィルスメカニズムが最新で、有効に実行されており、監査ログが生成できる。 | **5.2** すべてのアンチウィルスメカニズムが最新で、有効に実行されており、監査ログが生成できることを確認するために、以下の項目を確認する。 | | | |
| | **5.2.a** ポリシーを入手して検討し、アンチウィルスソフトウェアおよび定義の更新が要求されていることを確認する。 | | | |
| | **5.2.b** ソフトウェアのマスターインストールが自動更新と定期スキャンに対して有効になっていることを確認する。 | | | |
| | **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、自動更新と定期スキャンが有効になっていることを確認する。 | | | |
| | **5.2.d** システムコンポーネントのサンプルについて、アンチウィルスソフトウェアログ生成が有効になっており、ログが PCI DSS 要件 10.7 に従って保存されていることを確認する。 | | | |

## 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、保守すること

悪意のある人々は、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。すべての重要なシステムは、最新リリースの適切なソフトウェアパッチを適用することにより、悪意のある人々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 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **6.1** すべてのシステムコンポーネントとソフトウェアに、ベンダ提供の最新セキュリティパッチを適用する。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。<br>*注: 組織は、パッチインストールの優先順位を付けるために、リスクに基づくアプローチの適用を検討できる。たとえば、重要なインフラストラクチャ(一般に公開されているデバイス、システム、データベースなど)に重要性の低い内部デバイスよりも高い優先順位を付けることで、優先順位の高いシステムおよびデバイスは 1 カ月以内に対処し、重要性の低いシステムおよびデバイスは 3 カ月以内に対処するようにする。* | **6.1.a** 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、最新のベンダパッチがインストールされていることを確認する。 | | | |
| | **6.1.b** セキュリティパッチのインストールに関するポリシーを調査し、すべての重要な新規セキュリティパッチを 1 カ月以内にインストールすることが要求されていることを確認する。 | | | |
| **6.2** 新たに発見された脆弱性を特定するためのプロセスを確立する(インターネット上で無料で入手可能な警告サービスに加入するなど)。新たな脆弱性の問題に対処するために、PCI DSS 要件 2.2 で要求されているとおりに構成基準を更新する。 | **6.2.a** 責任者にインタビューして、新たなセキュリティ脆弱性を特定するためのプロセスが実装されていることを確認する。 | | | |
| | **6.2.b** 新たなセキュリティ脆弱性を特定するためのプロセスに、セキュリティ脆弱性情報に外部ソースを使用すること、および新たな脆弱性の問題が見つかったときに要件 2.2 でレビューしたシステム構成基準を更新すること、が含まれていることを確認する。 | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **6.3** PCI DSS（安全な認証やロギングなど）に従い、業界のベストプラクティスに基づいてソフトウェアアプリケーションを開発し、ソフトウェア開発ライフサイクル全体を通して情報セキュリティを実現する。これらのプロセスには、以下を含める必要がある。 | **6.3.a** 文書化されたソフトウェア開発プロセスを入手して検討し、プロセスが業界標準に基づいていること、ライフサイクル全体にセキュリティが取り込まれていること、およびソフトウェアアプリケーションが PCI DSS に従って開発されていることを確認する。 | | | |
| | **6.3.b** 文書化されたソフトウェア開発プロセスの調査、ソフトウェア開発者のインタビュー、関連データ（ネットワーク構成文書、本番環境データ、テストデータなど）の調査から、以下を確認する。 | | | |
| **6.3.1** 導入前にすべてのセキュリティパッチ、システムとソフトウェア構成の変更をテストする（以下のテストが含まれるが、これらに限定されない）。 | **6.3.1** すべての変更（パッチを含む）が、本番環境への導入前にテストされていること。 | | | |
| **6.3.1.1** すべての入力の検証（クロスサイトスクリプティング、インジェクションの不具合、悪意のあるファイル実行などを防止するため） | **6.3.1.1** すべての入力の検証（クロスサイトスクリプティング、インジェクションの不具合、悪意のあるファイル実行などを防止するため） | | | |
| **6.3.1.2** 適切なエラー処理の検証 | **6.3.1.2** 適切なエラー処理の検証 | | | |
| **6.3.1.3** 暗号化による安全な保存の検証 | **6.3.1.3** 暗号化による安全な保存の検証 | | | |
| **6.3.1.4** 安全な通信の検証 | **6.3.1.4** 安全な通信の検証 | | | |
| **6.3.1.5** 適切な役割ベースのアクセス制御（RBAC）の検証 | **6.3.1.5** 適切な役割ベースのアクセス制御（RBAC）の検証 | | | |
| **6.3.2** 開発/テスト環境と本番環境の分離 | **6.3.2** 開発環境/テストが、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。 | | | |
| **6.3.3** 開発/テスト環境と本番環境での責務の分離 | **6.3.3** 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。 | | | |
| **6.3.4** 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 | **6.3.4** 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、または使用する前に不適切な部分を削除する。 | | | |
| **6.3.5** 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を削除する | **6.3.5** 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。 | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **6.3.6** 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、カスタムアプリケーションアカウント、ユーザー ID、パスワードを削除する | **6.3.6** システムが実稼動になる前、または顧客にリリースされる前に、カスタムアプリケーションアカウント、ユーザー ID、パスワードを削除する。 | | | |
| **6.3.7** コーディングの脆弱性がないことを確認するために、本番または顧客へのリリースの前に、カスタムコードをレビューする<br>*注: このコードレビュー要件は、PCI DSS 要件 6.3 で要求される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。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。* | **6.3.7.a** ポリシーを入手してレビューし、内部アプリケーションのすべてのカスタムアプリケーションコードの変更に対して、レビューが要求されていることを確認する(手動または自動プロセスで)。<br>▪ コード変更は、コード作成者以外の、コードレビュー技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。<br>▪ リリース前に、適切な修正を実装する必要がある。<br>▪ 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。 | | | |
| | **6.3.7.b** ポリシーを入手してレビューし、Web アプリケーションのすべてのカスタムアプリケーションコードの変更に対して、レビューが要求されていることを確認する(手動または自動プロセスで)。<br>▪ コード変更は、コード作成者以外の、コードレビュー技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。<br>▪ コードレビューにより、コードが「Open Web Security Project Guide」などの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)。<br>▪ リリース前に、適切な修正を実装する必要がある。<br>▪ 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。 | | | |
| | **6.3.7.c** 最新のカスタムアプリケーション変更のサンプルを選択し、カスタムアプリケーションコードが上述の 6.3.7a と 6.3.7b に従ってレビューされていることを確認する。 | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **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、変更管理手順に従う。手順には以下を含める必要がある。 | **6.4.a** セキュリティパッチとソフトウェア変更に関する会社の変更管理手順を入手して検討し、手順で項目 6.4.1 ～ 6.4.4 が要求されていることを確認する。 | | | |
| | **6.4.b** システムコンポーネントと最新の変更/セキュリティパッチのサンプルについて、変更内容に関連する変更管理文書を確認します。確認した変更内容について、以下を実行します。 | | | |
| **6.4.1** 影響の文書化 | **6.4.1** 各変更のサンプルについて、顧客への影響に関する記述が、変更管理文書に記載されていることを確認する。 | | | |
| **6.4.2** 適切な管理者による承認 | **6.4.2** 各変更のサンプルについて、適切な管理者による承認が行われていることを確認する。 | | | |
| **6.4.3** 運用機能のテスト | **6.4.3** 各変更のサンプルについて、運用機能のテストが実施されたことを確認する。 | | | |
| **6.4.4** 回復手順 | **6.4.4** 各変更のサンプルについて、回復手順が用意されていることを確認する。 | | | |
| **6.5** すべての Web アプリケーション（内部、外部、アプリケーションへの Web 管理アクセス）を、「Open Web Application Security Project Guide」などの安全なコーディングガイドラインに基づいて開発する。ソフトウェア開発プロセスに共通するコーディングの脆弱性の防止に対応して、以下を含める。<br>*注: PCI DSS v1.2 が発行されたときに 6.5.1 ～ 6.5.10 に挙げられている脆弱性は、現在 OWASP ガイドに掲載されている。ただし、OWASP ガイドが更新されている場合、これらの要件には現在のバージョンを使用する必要がある。* | **6.5.a** すべての Web ベースアプリケーションのソフトウェア開発プロセスを入手してレビューする。このプロセスで、開発者に安全なコーディング技法に関するトレーニングが要求されていて、OWASP ガイド（http://www.owasp.org）などのガイダンスに基づいていることを確認する。 | | | |
| | **6.5.b** サンプル抽出した開発者にインタビューして、安全なコーディング技法に関する知識を持っているという確証を得る。 | | | |
| | **6.5.c** Web アプリケーションに以下の脆弱性が存在しないことを保証するプロセスが存在することを確認する。 | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **6.5.1** クロスサイトスクリプティング（XSS） | **6.5.1** クロスサイトスクリプティング（XSS）（取り込む前にすべてのパラメータを検証） | | | |
| **6.5.2** インジェクションの不具合（特に SQL インジェクション）LDAP と 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。 | **6.5.2** インジェクションの不具合（特に SQL インジェクション）（入力を検証し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）。 | | | |
| **6.5.3** 悪意のあるファイル実行 | **6.5.3** 悪意のあるファイル実行（入力を検証してアプリケーションがユーザからファイル名またはファイルを受け付けないことを確認する） | | | |
| **6.5.4** 安全でないオブジェクトの直接参照 | **6.5.4** 安全でないオブジェクトの直接参照（内部オブジェクト参照をユーザーに公開しない） | | | |
| **6.5.5** クロスサイトリクエスト偽造（CSRF） | **6.5.5** クロスサイトリクエスト偽造（CSRF）（ブラウザから自動的に送信される承認資格情報とトークンを使用しない） | | | |
| **6.5.6** 情報漏洩と不適切なエラー処理 | **6.5.6** 情報漏洩と不適切なエラー処理（エラーメッセージまたはその他の手段で情報を漏洩しない） | | | |
| **6.5.7** 不完全な認証管理とセッション管理 | **6.5.7** 不完全な認証管理とセッション管理（ユーザを適切に認証し、アカウント資格情報とセッショントークンを保護する） | | | |
| **6.5.8** 安全でない暗号化保存 | **6.5.8** 安全でない暗号化保存（暗号化の欠陥を防ぐ） | | | |
| **6.5.9** 安全でない通信 | **6.5.9** 安全でない通信（認証されたすべてのセンシティブ通信を適切に暗号化する） | | | |
| **6.5.10** URL アクセスの制限失敗 | **6.5.10** URL アクセスの制限失敗（プレゼンテーション層とビジネスロジックですべての URL に対するアクセス制御を一貫して実施する） | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **6.6** 一般公開されている Web アプリケーションは、常時、新しい脅威と脆弱性に対処し、以下のいずれかの手法によって既知の攻撃から保護する必要がある。<br>▪ 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<br>▪ 一般公開されている Web アプリケーションの手前に、Web アプリケーションファイアウォールをインストールする | **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。<br>▪ 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/自動で評価する以下のツールまたは手法を使用してレビューされていることを確認する。<br>– 少なくとも年 1 回<br>– 何らかの変更を加えた後<br>– 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<br>– 脆弱性がすべて修正されていること<br>– 修正後、アプリケーションが再評価されていること<br>▪ 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 アプリケーション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。<br><br>*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かまわない。* | | | |

# 強固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こと

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 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **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。アクセス制限には以下を含める必要がある。 | **7.1** データ管理に関する文書化されたポリシーを入手して検討し、ポリシーに以下が含まれていることを確認する。 | | | |
| **7.1.1** 特権ユーザー ID に関するアクセス権が、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 | **7.1.1** 特権ユーザー ID に関するアクセス権が、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を確認する。 | | | |
| **7.1.2** 特権の付与は、個人の職種と職能に基づくこと | **7.1.2** 特権の付与が、個人の職種と職能に基づいていることを確認する(「役割ベースのアクセス制御」(RBAC)とも呼ばれる)。 | | | |
| **7.1.3** 管理職により署名され、必要な特権を特定する承認フォームが要求される | **7.1.3** すべてのアクセスに対して、管理職により署名された、必須権限を指定する承認フォームが要求されることを確認する。 | | | |
| **7.1.4** 自動アクセス制御システムを実装する | **7.1.4** 自動アクセス制御システムによるアクセス制御が実装されていることを確認する。 | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **7.2** 複数のユーザーを持つシステムコンポーネントに対して、ユーザーの必要な範囲に基づいてアクセスを制限し、特に許可されていない限り「すべてを拒否」に設定した、アクセス制御システムを確立する。<br>アクセス制御システムには以下を含める必要がある。 | **7.2** システム設定とベンダ文書を調査して、アクセス制御システムが次のように実装されていることを確認する。 | | | |
| **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。 | | | |
| **7.2.2** 職種と職能に基づく、個人への特権の付与 | **7.2.2** 職種と職能に基づいて個人に特権を付与するように、アクセス制御システムが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に「すべてを拒否」がデフォルト設定されていることを確認する。<br>*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。* | | | |

## *要件 8: コンピュータにアクセスできる各ユーザに一意の ID を割り当てる。*

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。

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **8.1** 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** 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。 | | | |
| **8.2** 一意の ID の割り当てに加え、以下の方法の少なくとも 1 つを使用してすべてのユーザを認証する。<br>▪ パスワードまたはパスフレーズ<br>▪ 2 因子認証(トークンデバイス、スマートカード、生体認証、公開鍵など) | **8.2** カード会員データ環境にアクセスする際にユーザが一意の ID および追加認証(パスワードなど)を使用して認証されることを確認するために、以下を実行する。<br>▪ 使用される認証方法について記述した文書を入手して調査する。<br>▪ 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、認証を調査し、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。 | | | |
| **8.3** 従業員、管理者、および第三者によるネットワークへのリモートアクセス(ネットワーク外部からのネットワークレベルアクセス)には 2 因子認証を組み込む。RADIUS(Remote Authentication and Dial-In Service)、TACACS(Terminal Access Controller Acceess Control System)とトークン、または VPN(SSL/TLS または IPSEC ベース)と個々の証明書などのテクノロジを使用する。 | **8.3** すべてのリモートネットワークアクセスに 2 因子認証が実装されていることを確認するために、ネットワークにリモート接続する従業員(管理者など)を観察し、パスワードと追加認証アイテム(スマートカード、トークン、PIN など)の両方が要求されていることを確認する。 | | | |
| **8.4** (「PCI DSS Glossary of Terms, Abbreviations, and Acronyms」で定義されている)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の伝送および保存中にすべてのパスワードを読み取り不能にする。 | **8.4.a** 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査して、パスワードが伝送および保存中に読み取り不能であることを確認する。 | | | |
| | **8.4.b** サービスプロバイダの場合のみ、パスワードファイルを調査して、顧客パスワードが暗号化されていることを確認する。 | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **8.5** すべてのシステムコンポーネントで、以下のように、消費者以外のユーザおよび管理者に対して適切なユーザ認証とパスワード管理を確実に行う。 | **8.5** 手順を確認し、担当者にインタビューして、以下を実行することによってユーザ認証とパスワード管理のための手順が実施されていることを確認する。 | | | |
| **8.5.1** ユーザ ID、資格情報、およびその他の識別子オブジェクトの追加、削除、変更を管理する。 | **8.5.1.a** 管理者と一般ユーザの両方を含め、ユーザ ID のサンプルを選択する。以下を実行して、会社のポリシーに従って各ユーザにシステムの使用が承認されていることを確認する。<br>▪ 各 ID の承認フォームを入手して調査する。<br>▪ 承認フォームからシステムへと情報を追跡して、サンプルユーザ ID が承認フォームに従って実装されていること(指定されたとおりの権限を持っているか、すべての署名が取得されているかなど)を確認する。 | | | |
| **8.5.2** パスワードのリセットを実行する前にユーザ ID を確認する。 | **8.5.2** パスワード手順を調査し、セキュリティ担当者を観察して、ユーザがパスワードのリセットを電話、電子メール、Web、またはその他の対面以外の方法で要求した場合、パスワードがリセットされる前にユーザ ID が確認されていることを確認する。 | | | |
| **8.5.3** 初期パスワードをユーザごとに一意の値に設定し、初回使用後に直ちに変更する。 | **8.5.3** パスワード手順を調査し、セキュリティ担当者を観察して、新規ユーザの初期パスワードがユーザごとに一意の値に設定され、初回使用後に変更されていることを確認する。 | | | |
| **8.5.4** 契約終了したユーザのアクセスは直ちに取り消す。 | **8.5.4** 過去 6 カ月間に契約終了した従業員のサンプルを選択し、現在のユーザアクセスリストを調査して、これらの従業員の ID が無効化または削除されていることを確認する。 | | | |
| **8.5.5** 少なくとも 90 日ごとに非アクティブのユーザアカウントを削除/無効化する。 | **8.5.5** 90 日以上非アクティブなアカウントが削除または無効化されることを確認する。 | | | |
| **8.5.6** リモート保守のためにベンダが使用するアカウントは、必要な期間のみ有効にする。 | **8.5.6** システムコンポーネントをサポートおよび保守するためにベンダが使用するアカウントが無効になっていて、ベンダが必要とする場合のみ有効になり、使用中は監視されていることを確認する。 | | | |
| **8.5.7** パスワード手順およびポリシーを、カード会員データにアクセスできるすべてのユーザに伝達する。 | **8.5.7** ユーザ ID のサンプルに含まれるユーザにインタビューして、パスワード手順およびポリシーを理解していることを確認する。 | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **8.5.8** グループ、共有、または汎用のアカウントおよびパスワードを使用しない。 | **8.5.8.a** システムコンポーネントのサンプルに対して、ユーザ ID リストを調査して以下を確認する。<br>▪ 汎用ユーザ ID およびアカウントが無効化または削除されている。<br>▪ 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。<br>▪ 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。 | | | |
| | **8.5.8.b** パスワードポリシー/手順を調査して、グループパスワードおよび共有パスワードが明示的に禁止されていることを確認する。 | | | |
| | **8.5.8.c** システム管理者にインタビューして、たとえ要求された場合でも、グループパスワードおよび共有パスワードは配布されていないことを確認する。 | | | |
| **8.5.9** 少なくとも 90 日ごとにユーザパスワードを変更する。 | **8.5.9** システムコンポーネントのサンプルに対して、システム構成設定を入手して調査し、ユーザパスワードのパラメータが少なくとも 90 日ごとにパスワードの変更をユーザに要求するように設定されていることを確認する。<br>サービスプロバイダの場合のみ、内部プロセスおよび顧客/ユーザ文書を確認して、顧客パスワードの定期的な変更が要求されていること、およびパスワードを変更する必要がある時期や状況についてのガイダンスが顧客に提供されていることを確認する。 | | | |
| **8.5.10** パスワードに 7 文字以上が含まれることを要求する。 | **8.5.10** システムコンポーネントのサンプルに対して、システム構成設定を入手して調査し、パスワードのパラメータが 7 文字以上のパスワードを要求するように設定されていることを確認する。<br>サービスプロバイダの場合のみ、内部プロセスおよび顧客/ユーザ文書を確認して、顧客パスワードが最小長に関する要件を満たすことが要求されていることを確認する。 | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **8.5.11** 数字と英文字の両方を含むパスワードを使用する。 | **8.5.11** システムコンポーネントのサンプルに対して、システム構成設定を入手して調査し、パスワードのパラメータが数字と英文字の両方を含むパスワードを要求するように設定されていることを確認する。<br>サービスプロバイダの場合のみ、内部プロセスおよび顧客/ユーザ文書を確認して、数字と英文字の両方を含む顧客パスワードが要求されていることを確認する。 | | | |
| **8.5.12** ユーザが新しいパスワードを送信する際、最後に使用した 4 つのパスワードと同じものを使用できないようにする。 | **8.5.12** システムコンポーネントのサンプルに対して、システム構成設定を入手して調査し、パスワードのパラメータが、新しいパスワードを以前の 4 つのパスワードと同じにすることができないように設定されていることを確認する。<br>サービスプロバイダの場合のみ、内部プロセスおよび顧客/ユーザ文書を確認して、新しい顧客パスワードを以前の 4 つのパスワードと同じものにできないことを確認する。 | | | |
| **8.5.13** 最大 6 回の試行後にユーザ ID をロックアウトして、アクセス試行の繰り返しを制限する。 | **8.5.13** システムコンポーネントのサンプルに対して、システム構成設定を入手して調査し、パスワードのパラメータが、最大 6 回の無効なログオン試行の後でユーザのアカウントがロックアウトされるように設定されていることを確認する。<br>サービスプロバイダの場合のみ、内部プロセスおよび顧客/ユーザ文書を確認して、最大 6 回の無効なアクセス試行の後、顧客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。 | | | |
| **8.5.14** ロックアウトの期間を、最小 30 分または管理者がユーザ ID を有効にするまで、に設定する。 | **8.5.14** システムコンポーネントのサンプルに対して、システム構成設定を入手して調査し、パスワードのパラメータが、ユーザがロックアウトされた場合、最小 30 分間またはシステム管理者がアカウントをリセットするまでロックされたままになるように設定されていることを確認する。 | | | |
| **8.5.15** セッションが 15 分を超えてアイドル状態の場合、端末を再有効化するためにユーザにパスワードの再入力を要求する。 | **8.5.15** システムコンポーネントのサンプルに対して、システム構成設定を入手して調査し、システム/セッションのアイドルタイムアウト機能が 15 分以下に設定されていることを確認する。 | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **8.5.16** 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を認証する。これには、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が含まれる。 | **8.5.16.a** データベースおよびアプリケーションの構成設定を確認し、データベースに対するユーザ認証およびアクセスに以下が含まれていることを確認する。<br>▪ すべてのユーザはアクセス前に認証される。<br>▪ 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（移動、コピー、削除など）はすべて、プログラムによる方法（ストアドプロシージャなど）によってのみ行われる。<br>▪ 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に制限される。 | | | |
| | **8.5.16.b** データベースアプリケーションおよび関連アプリケーション ID を確認して、アプリケーション ID を使用できるのはアプリケーションのみである（個々のユーザやその他のプロセスは使用できない）ことを確認する。 | | | |

## *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。

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **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。 | **9.1** カード会員データ環境内のコンピュータルーム、データセンター、およびシステムを含むその他の物理エリアのそれぞれに、物理的なセキュリティ管理が存在することを確認する。<br>▪ バッジ読み取り機または承認済みバッジ、ロック、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。<br>▪ システム管理者がカード会員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。 | | | |
| **9.1.1** ビデオカメラやその他のアクセス管理メカニズムを使用して、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。<br>*注: "機密エリア" とは、データセンタ、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す。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ません。* | **9.1.1** 機密エリアへの出入りを監視するためのビデオカメラやその他のアクセス管理メカニズムが設置されていることを確認する。ビデオカメラまたはその他のメカニズムは、改ざんまたは無効化から守られている必要がある。ビデオカメラまたはその他のメカニズムが監視されていて、カメラまたは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。 | | | |
| **9.1.2** 誰でもアクセス可能なネットワークジャックへの物理アクセスを制限する。 | **9.1.2** ネットワーク管理者へのインタビューおよび観察により、ネットワークジャックが承認された従業員が必要とする場合のみ有効化されることを確認する。たとえば、訪問者に対応するための会議室では、ネットワークポートの DHCP を有効にしないようにする必要がある。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がいることを確認する。 | | | |
| **9.1.3** 無線アクセスポイント、ゲートウェ | **9.1.3** 無線アクセスポイント、ゲートウェイ、およびハンドヘ | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| イ、およびハンドヘルドデバイスへの物理アクセスを制限する。 | ルドデバイスへの物理アクセスが適切に制限されていることを確認する。 | | | |
| **9.2** カード会員データにアクセス可能なエリアでは特に、すべての担当者が従業員と訪問者を容易に区別できるような手順を開発する。<br>*この要件において、"従業員" とは、フルタイムおよびパートタイムの従業員、一時的な従業員および要員、事業体の敷地内に "常駐" してい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、従業員の客、サービス要員、または短時間（通常は 1 日以内）施設に入る必要がある人として定義されます。* | **9.2.a** 従業員および訪問者にバッジを割り当てるためのプロセスと手順を確認して、これらのプロセスに以下が含まれていることを確認する。<br>▪ 新しいバッジの許可、アクセス要件の変更、および契約終了した従業員と期限切れの訪問者バッジの取り消し<br>▪ バッジシステムへのアクセスの制限 | | | |
| | **9.2.b** 施設内の人々を観察して、従業員と訪問者を容易に区別できることを確認する。 | | | |
| **9.3** すべての訪問者が次のように処理されることを確認する。 | **9.3.** 次のような従業員/訪問者管理が存在することを確認する。 | | | |
| **9.3.1** 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前に承認が行われる | **9.3.1** 訪問者を観察して、訪問者 ID バッジの使用を確認する。データセンターへのアクセスを試みて、訪問者 ID バッジではカード会員データを格納す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。 | | | |
| **9.3.2** 有効期限があり、訪問者を非従業員として識別する物理トークン（バッジ、アクセスデバイスなど）が与えられる | **9.3.2** 従業員バッジと訪問者バッジを調査して、ID バッジによって従業員と訪問者/部外者が明確に区別されること、および訪問者バッジに有効期限があることを確認する。 | | | |
| **9.3.3** 施設を出る前、または期限切れの日に物理トークンの返却を求められる | **9.3.3** 施設から出る訪問者を観察して、訪問者が退去時または期限切れのときに ID バッジの返却を求められていることを確認する。 | | | |
| **9.4** 訪問者ログを使用して、訪問者の行動の物理的な監査証跡を保持する。訪問者の名前、所属会社、物理アクセスを承認した従業員をログに記録する。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。 | **9.4.a** カード会員データが保存または伝送されるコンピュータルームやデータセンターだけでなく、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。 | | | |
| | **9.4.b** ログに訪問者の名前、所属会社、物理アクセスを承認した従業員が含まれていて、少なくとも 3 カ月間保管されていることを確認する。 | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **9.5** メディアバックアップ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。 | **9.5** バックアップ媒体の保管が安全であることを判断するために保管場所の再検証が少なくとも年に一度行われていることを確認する。 | | | |
| **9.6** カード会員データを含むすべての紙および電子媒体を物理的にセキュリティで保護する。 | **9.6** カード会員データを保護するための手順に、紙および電子媒体(コンピュータ、リムーバブル電子メディア、ネットワーク、通信ハードウェア、通信回線、紙の受領書、紙のレポート、FAX を含む)を物理的にセキュリティで保護するための管理が含まれていることを確認する。 | | | |
| **9.7** カード会員データを含むあらゆる種類の媒体の内部または外部での配布に関して、以下を含め、厳格な管理を維持する。 | **9.7** カード会員データを含む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。 | | | |
| **9.7.1** 秘密であると識別できるように、媒体を分類する。 | **9.7.1** "秘密" であると識別できるように、すべての媒体が分類されていることを確認する。 | | | |
| **9.7.2** 安全な配達業者または正確に追跡できるその他の配送方法によって媒体を送付する。 | **9.7.2** 施設の外部に送付されるすべての媒体が管理者によってログに記録されて承認され、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。 | | | |
| **9.8** 安全なエリアから移動されるカード会員データを含むすべての媒体を管理者が承認するようにする(特に媒体が個人に配布される場合)。 | **9.8** カード会員データを含む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、追跡の詳細および適切な管理者承認がログに含まれていることを確認する。 | | | |
| **9.9** カード会員データを含む媒体の保管およびアクセスに関して厳格な管理を維持する。 | **9.9** ハードコピーおよび電子媒体の保管と維持を管理するためのポリシーを入手して調査し、ポリシーで定期的なメディアの在庫調査が要求されていることを確認する。 | | | |
| **9.9.1** すべての媒体の在庫ログを適切に保持し、少なくとも年に一度メディアの在庫調査を実施する。 | **9.9.1** 媒体の在庫ログを入手して確認し、少なくとも年に一度、定期的なメディアの在庫調査が実施されていることを確認する。 | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **9.10** 次のように、ビジネスまたは法律上の理由で不要になったカード会員データを含む媒体を破棄する。 | **9.10** 定期的な媒体破棄に関するポリシーを入手して調査し、カード会員データを含むすべての媒体に対応していることを確認し、以下を確認する。 | | | |
| **9.10.1** 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。 | **9.10.1.a** ハードコピー資料が、再現できないことを合理的に保証するように、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。 | | | |
| | **9.10.1.b** 破棄される情報に使用される保管コンテナを調査して、コンテナが安全であることを確認する。たとえば、"裁断予定" のコンテナに、中身にアクセスするのを防止する鍵が付けられていることを確認する。 | | | |
| **9.10.2** カード会員データを再現できないように、電子媒体上のカード会員データを回復不能にする。 | **9.10.2** 電子媒体上のカード会員データが、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って、またはそれ以外の場合は媒体の物理的な破壊（消磁など）によって、回復不能になっていることを確認する。 | | | |

# 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 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **10.1** システムコンポーネントへのすべてのアクセス（特に、ルートなどの管理権限を使用して行われたアクセス）を各ユーザにリンクするプロセスを確立する。 | **10.1** システム管理者の観察とインタビューを通じて、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を確認する。 | | | |
| **10.2** 以下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** 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。 | | | |
| **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個人アクセスがログ記録されることを確認する。 | | | |
| **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** ルート権限または管理権限を持つ個人によって行われたアクションがログ記録されることを確認する。 | | | |
| **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。 | | | |
| **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ログ記録されることを確認する。 | | | |
| **10.2 5** 識別および認証メカニズムの使用 | **10.2 5** 識別および認証メカニズムの使用がログ記録されることを確認する。 | | | |
| **10.2.6** 監査ログの初期化 | **10.2.6** 監査ログの初期化がログ記録されることを確認する。 | | | |
| **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。 | | | |
| **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。 | | | |
| **10.3.1** 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。 | | | |
| **10.3.2** イベントの種類 | **10.3.2** イベントの種類がログエントリに含まれることを確認する。 | | | |
| **10.3.3** 日付と時刻 | **10.3.3** 日付および時刻スタンプがログエントリに含まれることを確認する。 | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **10.3.4** 成功または失敗を示す情報 | **10.3.4** 成功または失敗を示す情報がログエントリに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** イベントの発生元がログエントリに含まれることを確認する。 | | | |
| **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** すべての重要なシステムクロックおよび時間を同期する。 | **10.4** 組織内で正しい時刻を取得して配布するプロセス、およびシステムコンポーネントのサンプルに対する時刻関連のシステムパラメータ設定を入手して確認する。以下がプロセスに含まれ、実装されていることを確認する。 | | | |
| | **10.4.a** PCI DSS 要件 6.1 および 6.2 に従って最新に保たれている、既知の安定したバージョンの NTP（Network Time Protocol）または同様のテクノロジが時刻同期に使用されていることを確認する。 | | | |
| | **10.4.b** 内部サーバが必ずしもすべて外部ソースから時刻信号を受け取っていないことを確認する。[組織内の 2 ～ 3 の中央のタイムサーバは、[国際原子時および UTC（以前は GMT）を基にした特別なラジオ、GPS 衛星、またはその他の外部ソースから直接] 外部時刻信号を受信し、連携して正確な時刻を維持し、他の内部サーバと時間を共有します。] | | | |
| | **10.4.c** （悪意のある個人が時計を変更するのを防ぐために）タイムサーバが NTP 時刻更新を受け付ける特定の外部ホストが指定されていることを確認する。（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キーで暗号化し、NTP サービス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。<br>詳細については、www.ntp.orgを参照 | | | |
| **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。 | **10.5** システム管理者にインタビューし、アクセス権限を調査して、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。 | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **10.5.1** 監査証跡の表示を、仕事関連のニーズを持つ人物のみに制限する。 | **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ことを確認する。 | | | |
| **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ことを確認する。 | | | |
| **10.5.3** 監査証跡ファイルを、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が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ことを確認する。 | | | |
| **10.5.4** 外部に公開されているテクノロジのログを内部 LAN 上のログサーバに書き込む。 | **10.5.4** 外部に公開されているテクノロジ（無線、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オフロードまたはコピーされることを確認する。 | | | |
| **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査して、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。 | | | |
| **10.6** 少なくとも日に一度、すべてのシステムコンポーネントのログを確認する。ログの確認には、侵入検知システム（IDS）や認証、認可、アカウンティングプロトコル（AAA）サーバ（RADIUS など）のようなセキュリティ機能を実行するサーバを含める必要がある。<br>*注: 要件 10.6 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。* | **10.6.a** セキュリティに関するポリシーと手順を入手して調査し、セキュリティログを少なくとも日に一度確認する手順が含まれていること、および例外への対応が要求されていることを確認する。 | | | |
| | **10.6.b** 観察とインタビューを通じて、すべてのシステムコンポーネントに対して定期的なログの確認が実行されていることを確認する。 | | | |
| **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）。 | **10.7.a** セキュリティに関するポリシーと手順を入手して調査し、監査ログの保存期間に関するポリシーが含まれていること、および監査ログの保存期間として少なくとも 1 年を要求していることを確認する。 | | | |
| | **10.7.b** 監査ログが少なくとも 1 年間利用できること、およびすぐ分析できるように少なくとも過去 3 カ月間のログを復元するプロセスが整えられていることを確認する。 | | | |

## *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 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **11.1** 無線アナライザを少なくとも四半期に一度使用して、または使用中のすべての無線デバイスを識別するための無線 IDS/IPS を導入して、無線アクセスポイントの存在をテストする。 | **11.1.a** 無線アナライザが少なくとも四半期に一度使用されていること、または無線 IDS/IPS が実装され、すべての無線デバイスを識別するように構成されていることを確認する。 | | | |
| | **11.1.b** 無線 IDS/IPS が実装されている場合は、担当者へ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。 | | | |
| | **11.1 c** 組織のインシデント対応計画（要件 12.9）に、不正な無線デバイスが検出された場合の対応が含まれていることを確認する。 | | | |
| **11.2** 内部および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、ネットワークトポロジの変更、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。<br>*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* | **11.2.a** 内部ネットワーク、ホスト、およびアプリケーションの脆弱性スキャンの最新の 4 四半期の出力を調査して、カード会員データ環境内でデバイスのセキュリティテストが定期的に行われていることを確認する。スキャンプロセスに、合格結果が取得される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。<br>*注: ネットワーク変更後に実施される外部スキャン、および内部スキャンは、会社が資格を与えた内部担当者または第三者によって実行することができます。* | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| 与えられた Approved Scanning Vendor(ASV)によって実行される必要があります。ネットワーク変更後に実施されるスキャンは、会社の内部スタッフによって実行することができます。 | **11.2.b** 外部の脆弱性スキャンの最新の 4 四半期の出力を調査して以下のことを確認することで、PCI セキュリティスキャン手順に従って四半期ベースで外部スキャンが行われていることを確認する。<br>▪ 過去 12 カ月間に四半期に一度のスキャンが 4 回行われた<br>▪ スキャンの結果は、PCI セキュリティスキャン手順を満たしている(緊急、重大、または高い脆弱性がない、など)<br>▪ スキャンは PCI SSC によって資格を与えられた Approved Scanning Vendor(ASV)が完了した<br>*注: 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再スキャンにおいて示されているとおりに修正されたことを確認した場合、初回の PCI DSS 準拠のために、4 つの四半期に一度のスキャンに合格する必要はありません。初回の PCI DSS レビュー以降の年は、4 つの四半期に一度のスキャンに合格している必要があります。* | | | |
| | **11.2.c** 昨年のスキャン結果を調査することで、ネットワークへの大幅な変更後に内部スキャンや外部スキャンが実行されていることを確認する。スキャンプロセスに、合格結果が取得される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。 | | | |
| **11.3** 外部および内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。これらのペネトレーションテストには以下を含める必要がある。 | **11.3.a** 最新のペネトレーションテストの結果を入手して調査し、ペネトレーションテストが少なくとも年に一度および環境への大幅な変更後に実行されていることを確認する。判明した脆弱性が修正され、テストが繰り返されたことを確認する。 | | | |
| | **11.3.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ター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。 | | | |
| **11.3.1** ネットワーク層のペネトレーションテスト | **11.3.1** ペネトレーションテストにネットワーク層のペネトレーションテストが含まれることを確認する。これらのテストには、ネットワーク機能および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。 | | | |
| **11.3.2** アプリケーション層のペネトレーションテスト | **11.3.2** ペネトレーションテストにアプリケーション層のペネトレーションテストが含まれることを確認する。Web アプリケーションの場合、テストには要件 6.5 に記載されている脆弱性を最低限含める必要がある。 | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **11.4** 侵入検知システムや侵入防止システムを使用して、カード会員データ環境内の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。すべての侵入検知および防止エンジンを最新状態に保つ。 | **11.4.a** 侵入検知システムや侵入防止システムが使用されていて、カード会員データ環境内の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。 | | | |
| | **11.4.b** IDS や IPS が侵害の疑いを担当者に警告するように構成されていることを確認する。 | | | |
| | **11.4.c** IDS/IPS 構成を調査し、IDS/IPS デバイス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。 | | | |
| **11.5** ファイル整合性監視ソフトウェア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。<br><br>*注: ファイル整合性監視において、重要なファイルとは通常、定期的に変更されないが、その変更がシステムの侵害や侵害のリスクを示す可能性があるファイルのことです。ファイル整合性監視製品では通常、関連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構成されています。カスタムアプリケーション用のファイルなど、その他の重要なファイルは、事業体(つまり、加盟店またはサービスプロバイダ)による評価および定義が必要です。* | **11.5** システム設定と監視対象ファイルを調査し、監視作業からの結果を確認して、カード会員データ環境内でファイル整合性監視製品が使用されていることを確認する。<br><br>監視する必要があるファイルの例:<br>▪ システム実行可能ファイル<br>▪ アプリケーション実行可能ファイル<br>▪ 構成およびパラメータファイル<br>▪ 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 | | | |

# 情報セキュリティポリシーの整備

## *要件 12: 従業員および派遣社員向けの情報セキュリティポリシーを整備する。*

強力なセキュリティポリシーは、会社全体でのセキュリティの方向性を設定し、従業員に対して期待される内容を示します。すべての従業員は、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。この要件において、"従業員" とは、フルタイムおよびパートタイムの従業員、一時的な従業員および要員、会社の敷地内に "常駐" している派遣社員やコンサルタントのことです。

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **12.1** 以下を実現するセキュリティポリシーを確立、公開、維持、および周知する。 | **12.1** 情報セキュリティポリシーを調査し、ポリシーが公開され、すべての関連システムユーザ(ベンダ、派遣社員、ビジネスパートナーを含む)に周知されていることを確認する。 | | | |
| **12.1.1** すべての PCI DSS 要件に対応する。 | **12.1.1** ポリシーがすべての PCI DSS 要件に対応していることを確認する。 | | | |
| **12.1.2** 脅威、脆弱性、結果を識別する年に一度のプロセスを正式なリスク評価に含める。 | **12.1.2** 情報セキュリティポリシーにおいて、脅威、脆弱性、結果を識別する年に一度のリスク評価プロセスが正式なリスク評価に含まれていることを確認する。 | | | |
| **12.1.3** レビューを少なくとも年に一度含め、環境の変化に合わせて更新する。 | **12.1.3** 情報セキュリティポリシーが少なくとも年に一度レビューされ、必要に応じてビジネス目標やリスク環境の変化を反映するように更新されることを確認する。 | | | |
| **12.2** この仕様の要件と整合する日常的な運用上のセキュリティ手順を作成する(たとえば、ユーザアカウント保守手順、ログレビュー手順)。 | **12.2.a** 日常的な運用上のセキュリティ手順を調査する。この仕様と整合していること、および各要件に対する管理および技術手順が含まれていることを確認する。 | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **12.3** 従業員に公開されている重要なテクノロジ(リモートアクセステクノロジ、無線テクノロジ、リムーバブル電子メディア、ラップトップ、携帯情報端末(PDA)、電子メールの使用、インターネットの使用など)に関する使用ポリシーを作成して、すべての従業員および派遣社員向けにこれらのテクノロジの適切な使用を定義する。これらの使用ポリシーでは以下を要求します。 | **12.3** 従業員に公開されている重要なテクノロジに関するポリシーを入手して調査し、以下を実行する。 | | | |
| **12.3.1** 管理者による明示的な承認 | **12.3.1** 使用ポリシーでテクノロジの使用に関する管理者の明示的な承認が要求されていることを確認する。 | | | |
| **12.3.2** テクノロジの使用に対する認証 | **12.3.2** 使用ポリシーで、すべてのテクノロジの使用をユーザ ID とパスワードまたはその他の認証アイテム(トークンなど)によって認証することが要求されていることを確認する。 | | | |
| **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 | **12.3.3** 使用ポリシーで、すべてのデバイスとデバイスを使用する権限がある担当者のリストが要求されていることを確認する。 | | | |
| **12.3.4** デバイスへの所有者、連絡先情報、目的を記載したラベルの添付 | **12.3.4** 使用ポリシーで、デバイスに所有者、連絡先情報、目的を記載したラベルを添付することが要求されていることを確認する。 | | | |
| **12.3.5** テクノロジの許容される利用法 | **12.3.5** 使用ポリシーで、テクノロジの許容される利用法が要求されていることを確認する。 | | | |
| **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** 使用ポリシーで、テクノロジの許容されるネットワーク上の場所が要求され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** 使用ポリシーで、会社が承認した製品のリストが要求されていることを確認する。 | | | |
| **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** 使用ポリシーで、非アクティブ状態が特定の期間続いた後、リモートアクセステクノロジのセッションを自動切断することが要求されていることを確認する。 | | | |
| **12.3.9** ベンダ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ことが要求されていることを確認する。 | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **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場合、ローカルハードドライブおよびリムーバブル電子メディアへのカード会員データのコピー、移動、保存を禁止する。 | **12.3.10** 使用ポリシーで、リモートアクセステクノロジ経由でのアクセス時に、ローカルハードドライブおよびリムーバブル電子メディアへのカード会員データのコピー、移動、または保存が禁止されていることを確認する。 | | | |
| **12.4** セキュリティポリシーおよび手順に、すべての従業員および派遣社員の情報セキュリティに対する責任を明確に定義する。 | **12.4** 情報セキュリティポリシーおよび手順に、従業員と派遣社員の両方の情報セキュリティに対する責任が明確に定義されていることを確認する。 | | | |
| **12.5** 個人またはチームに以下の情報セキュリティ管理責任を割り当てる。 | **12.5** 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そ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ことを確認する。情報セキュリティポリシーおよび手順を入手して調査し、以下の情報セキュリティ責任が明確かつ正式に割り当てられていることを確認する。 | | | |
| **12.5.1** セキュリティポリシーおよび手順を確立、文書化、および周知する。 | **12.5.1** セキュリティポリシーおよび手順を作成して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。 | | | |
| **12.5.2** セキュリティに関する警告および情報を監視して分析し、該当する担当者に通知する。 | **12.5.2** セキュリティに関する警告を監視して分析し、該当する情報セキュリティおよび事業単位の管理担当者に通知する責任が正式に割り当てられていることを確認する。 | | | |
| **12.5.3** 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、および周知して、あらゆる状況をタイムリーかつ効果的に処理する。 | **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作成および周知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、ユーザアカウントを管理する | **12.5.4** ユーザアカウントの管理および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** データへのすべてのアクセスを監視および管理する。 | **12.5.5** データへのすべて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。 | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **12.6** 正式なセキュリティに関する認識を高めるプログラムを実施して、すべての従業員がカード会員データセキュリティの重要性を認識するようにする。 | **12.6.a** すべての従業員を対象にした正式なセキュリティに関する認識を高めるプログラムが存在することを確認する。 | | | |
| | **12.6.b** セキュリティに関する認識を高めるプログラムの手順と文書を入手して調査し、以下を実行する。 | | | |
| **12.6.1** 雇用時および少なくとも年に一度従業員を教育する。 | **12.6.1.a** セキュリティに関する自己啓発プログラムが、複数の方法で認識を伝え、従業員を教育していることを確認する(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)。 | | | |
| | **12.6.1.b** 従業員が雇用時および少なくとも年に一度、自己啓発トレーニングに出席していることを確認する。 | | | |
| **12.6.2** 会社のセキュリティポリシーおよび手順に目を通して理解したことについての同意を、少なくとも年に一度従業員に求める。 | **12.6.2** セキュリティに関する自己啓発プログラムで、会社の情報セキュリティポリシーに目を通して理解したことについての同意(書面上、電子的など)を、少なくとも年に一度従業員に求めていることを確認する。 | | | |
| **12.7** 雇用する前に、可能性のある従業員(上述の 9.2 の "従業員" の定義を参照)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。<br>*トランザクションを進めるときに一度に 1 つのカード番号にしかアクセスできない、店のレジ係などの従業員については、この要件は推奨のみです。* | **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従業員については、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。(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、経歴照会があります。) | | | |
| **12.8** カード会員データをサービスプロバイダと共有する場合は、サービスプロバイダを管理するためのポリシーと手順を維持および実施して、以下を含める。 | **12.8** 評価される事業体がカード会員データをサービスプロバイダ(バックアップテープ保管施設、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管理対象サービスプロバイダ、または不正モデリング目的でデータを受信するサービスプロバイダなど)と共有する場合は、観察、ポリシーと手順のレビュー、および関連文書のレビューを通じて、以下を実行する。 | | | |
| **12.8.1** サービスプロバイダのリストを維持する。 | **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を確認する。 | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **12.8.2** サービスプロバイダが自社の所有するカード会員データのセキュリティに対して責任を負うことに同意した、書面での契約を維持する。 | **12.8.2** 書面による契約に、カード会員データのセキュリティに対して責任を負うことへのサービスプロバイダの同意が含まれていることを確認する。 | | | |
| **12.8.3** 契約前の適切なデューディリジェンスを含め、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。 | **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ィリジェンスを含め、ポリシーと手順が文書化されていて、それに従って契約が実施されていることを確認する。 | | | |
| **12.8.4** 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。 | **12.8.4** 評価される事業体が、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していることを確認する。 | | | |
| **12.9** インシデント対応計画を実施する。システム違反に直ちに対応できるよう準備する。 | **12.9** インシデント対応計画および関連手順を入手して調査し、以下を実行する。 | | | |

*(12.9 は次のページに続く)*

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **12.9.1** システム違反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。<br>▪ 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<br>▪ 具体的なインシデント対応手順<br>▪ ビジネスの復旧および継続手順<br>▪ データバックアッププロセス<br>▪ 侵害の報告に関する法的要件の分析<br>▪ 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<br>▪ 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 | **12.9.1** 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。<br>▪ 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<br>▪ 具体的なインシデント対応手順<br>▪ ビジネスの復旧および継続手順<br>▪ データバックアッププロセス<br>▪ 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）<br>▪ 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<br>▪ 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 | | | |
| **12.9.2** 計画を少なくとも年に一度テストする。 | **12.9.2** 計画が少なくとも年に一度テストされることを確認する。 | | | |
| **12.9.3** 警告に 24 時間体制で対応できる担当者を指定する。 | **12.9.3** 観察およびポリシーのレビューを通じて、承認されていない活動、承認されていない無線アクセスポイントの検出、重要な IDS 警告、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重要な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 時間行われていることを確認する。 | | | |
| **12.9.4** セキュリティ違反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。 | **12.9.4** 観察とポリシーのレビューを通じて、セキュリティ違反への対応を担当する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。 | | | |

| PCI DSS 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **12.9.5** 侵入検知、侵入防止、およびファイル整合性監視システムからの警告を含める。 | **12.9.5** 観察とプロセスのレビューを通じて、承認されていない無線アクセスポイントの検出を含め、セキュリティ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。 | | | |
| **12.9.6** 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、産業の発展を組み込むプロセスを作成する。 | **12.9.6** 観察とポリシーのレビューを通じて、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、産業の発展を組み込むプロセスがあることを確認する。 | | | |

# 付録 A:　共有ホスティングプロバイダ向けの PCI DSS 追加要件

### *要件 A.1: 共有ホスティングプロバイダはカード会員データ環境を保護する必要がある*

要件 12.8 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 2.4 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。

| 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **A.1**　A.1.1 ～ A.1.4 に従い、各事業体（つまり、加盟店、サービスプロバイダ、またはその他の事業体）のホストされている環境およびデータを保護する。<br>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。<br>*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。* | **A.1**　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 A.1.1 ～ A.1.4 を実行する。 | | | |
| **A.1.1** 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。 | **A.1.1** 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:<br>▪ 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。<br>▪ 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。 | | | |

| 要件 | テスト手順 | 対応 | 未対応 | 目標期日/コメント |
|---|---|---|---|---|
| **A.1.2** 各事業体のアクセスおよび権限をその事業体のカード会員データ環境のみに制限する。 | **A.1.2.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。 | | | |
| | **A.1.2.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。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。 | | | |
| | **A.1.2.c** 事業体のユーザが共有システムバイナリへの書き込みアクセス権を持たないことを確認する。 | | | |
| | **A.1.2.d** ログエントリの表示が所有事業体に制限されることを確認する。 | | | |
| | **A.1.2.e** 各事業体がサーバリソースを独占して脆弱性（たとえば、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。<br>▪ ディスク領域<br>▪ 帯域幅<br>▪ メモリ<br>▪ CPU | | | |
| **A.1.3** ログ記録および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固有であり、PCI DSS 要件 10 と整合性を保つようにする。 | **A.1.3.a** 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。<br>▪ 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。<br>▪ ログはデフォルトでアクティブである。<br>▪ 所有事業体がログをレビューできる。<br>▪ ログの場所が所有事業体に明確に伝えられている。 | | | |
| **A.1.4** ホストされた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。 | **A.1.4** 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。 | | | |

# 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を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、「Navigating PCI DSS」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既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。たとえば、コンソール以外の管理アクセス用のパスワードは、クリアテキスト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、その他の 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クリアテキスト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、その他のパスワード管理は、（パスワードについて）レビュー中の項目の PCI DSS 要件に既になっています。

   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。たとえば、2 因子認証はリモートアクセスの PCI DSS 要件です。内部ネットワーク内からの 2 因子認証も、暗号化パスワードの伝送をサポートできない場合、コンソール以外の管理アクセスの代替コントロールと見なすことができます。2 因子認証は、（1）クリアテキストの管理用パスワードの傍受リスクに対応することで元の要件の目的を満たし、（2）安全な環境で適切に設定されている場合、代替コントロールとして許容することができます。

   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。たとえば、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）内部ネットワークからの 2 因子認証。
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。*

**要件番号および定義:**

| | 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の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、「はい」にチェックが付けられ、「Special」列で代替コントロールについて言及されている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—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 "ルート" ログインを必要とします。XYZ 社が "ルート" ログインを管理することは管理することは不可能であり、各ユーザによるすべての "ルート" 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。 | *一意のログインの要求の目的は 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 人の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、SU コマンドを使用してデスクトップからサーバにログインすることをすべてのユーザに要求する予定です。SU により、ユーザは「ルート」アカウントにアクセスし、「ルート」アカウントの下でアクションを実行できますが、SU-log ディレクトリにログを記録することが可能です。この方法で、各ユーザのアクションを SU アカウントを通じて追跡できます。* |
| **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、SU コマンドの実行、およびコマンドを利用する個人がログに記録され、その個人がルート権限の下でアクションを実行していることが識別されることを、評価者に実際に示します。* |
| **6. 維持** | 代替コントロールを維持するためのプロセスおよび管理を定義する。 | *XYZ 社は、SU 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追跡またはログ記録されることなくルートコマンドを実行できるようにならないようにするためのプロセスおよび手順を文書化します。* |

付録 D:　準拠証明書 - 加盟店

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

---

## オンサイト評価の準拠証明書
## – 加盟店

**バージョン 1.2**

2008 年 10 月

### *提出に関する指示*

認定セキュリティ評価機関（QSA）または加盟店（加盟店の内部監査で検証を実行する場合）は、PCI データセキュリティ基準（PCI DSS）に対する加盟店の準拠状況を明らかにするものとして、この文書を完成させる必要があります。すべての該当するセクションを完成させて、アクワイアラーまたは要求元のペイメントブランドに提出します。

### パート 1. 認定セキュリティ評価機関の会社情報

| | | | | | |
|---|---|---|---|---|---|
| 会社名: | | | | | |
| QSA リーダーの名前: | | 役職: | | | |
| 電話番号: | | 電子メール: | | | |
| 会社住所: | | 市区町村: | | | |
| 都道府県: | | 国: | | 郵便番号: | |
| URL: | | | | | |

### パート 2. 加盟店の組織情報

| | | | | | |
|---|---|---|---|---|---|
| 会社名: | | DBA: | | | |
| 名前: | | 役職: | | | |
| 電話番号: | | 電子メール: | | | |
| 会社住所: | | 市区町村: | | | |
| 都道府県: | | 国: | | 郵便番号: | |
| URL: | | | | | |

### パート 2a. 加盟店のビジネスの種類（該当するものすべてにチェック）

☐ 小売　☐ 情報通信　☐ 食料雑貨およびスーパーマーケット

☐ 石油　☐ 電子商取引　☐ 通信販売

☐ 旅行およびエンターテインメント　☐ その他（指定してください）:

PCI DSS レビューに含まれる施設および場所のリスト:

### パート 2b. 関係

1 つ以上の第三者の代理店と関係がありますか（ゲートウェイ、Web ホスティング企業、航空券予約代理店、ロイヤルティプログラム代理店など）?　☐ はい ☐ いいえ

複数のアクワイアラーと関係がありますか?　☐ はい ☐ いいえ

### パート 2c. 取引処理

使用中のペイメントアプリケーション:　ペイメントアプリケーションのバージョン:

## パート 3. PCI DSS 検証

(date of ROC) 付の準拠に関するレポート("ROC")で言及されている結果を基に、(QSA Name/Merchant Name) は、本書のパート 2 に記載されている事業体について (date) 現在で以下の準拠状態を証明します(1 つチェック):

☐ **準拠:** ROC 内のすべての要件が "対応[4]" になっていて、合格スキャンが PCI SSC Approved Scanning Vendor (ASV) (ASV Name) によって完了されています。これにより、(Merchant Company Name) は、PCI DSS (insert version number) に完全に準拠していることを示しました。

☐ **非準拠:** ROC 内のいくつかの要件が "未対応" であるために全体的な評価が**非準拠**になっている、**または**合格スキャンが PCI SSC Approved Scanning Vendor(ASV)によって完了されていません。これにより、(Merchant Company Name) は、PCI DSS への完全な準拠を示しませんでした。

準拠の**目標期日**:

状態が非準拠で、このフォームを提出する事業体は、本書のパート 4 にあるアクションプランを完了しなければならない場合があります。すべてのペイメントブランドがこのセクションを要求するわけではないため、パート 4 を完成させる前にアクワイアラーまたはペイメントブランドに確認してください。

## パート 3a. 準拠状態の確認

**QSA/加盟店は以下を確認します:**

| | |
|---|---|
| ☐ | ROC は、PCI DSS 要件およびセキュリティ評価手順、バージョン (insert version number) の指示に従って完了されました。 |
| ☐ | 上記で参照されている ROC およびこの証明書のすべての情報は、評価の結果をすべての重要な点において公平に表しています。 |
| ☐ | 加盟店は、ペイメントアプリケーションが承認後にセンシティブな認証データを保存しないことをペイメントアプリケーションベンダに確認しました。 |
| ☐ | 加盟店は、PCI DSS に目を通し、常に完全な PCI DSS 準拠を維持する必要があることを認識しています。 |
| ☐ | 取引承認の後の磁気ストライプ(つまり追跡)データ[5]、CAV2、CVC2、CID、または CVV2 データ[6]、または PIN データ[7] が保存されているという証拠は、この評価でレビューされたすべてのシステムで見つかりませんでした。 |

## パート 3b. QSA および加盟店による確認

| | |
|---|---|
| ***QSA リーダーの署名 ↑*** | ***日付:*** |
| ***QSA リーダーの名前:*** | ***役職:*** |

| | |
|---|---|
| ***加盟店役員の署名 ↑*** | ***日付:*** |
| ***加盟店役員名:*** | ***役職:*** |

[4] 「対応」という結果には、QSA/加盟店の内部監査によってレビューされる代替コントロールも含める必要があります。代替コントロールが要件に関連するリスクを十分に軽減すると判断された場合、QSA はその要件を「対応」とする必要があります。

[5] カードを提示する取引中に、承認のために使用される磁気ストライプにエンコードされたデータ。取引承認の後、事業体は磁気ストライプデータ全体を保持してはいけません。保持できる追跡データの要素は、アカウント番号、有効期限、名前のみです。

[6] カードを提示しない取引を検証するために使用される、署名欄またはペイメントカードの前面に印字されている 3 または 4 桁の値。

[7] カードを提示する取引中に、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。

## パート 4. 非準拠状態のアクションプラン

要件ごとに該当する「準拠状態」を選択してください。要件に対して「いいえ」を選択した場合は、会社が要件に準拠する予定である日付と、要件を満たすために講じられるアクションの簡単な説明を記入する必要があります。*すべてのペイメントブランドがこのセクションを要求するわけではないため、パート 4 を完成させる前にアクワイアラーまたはペイメントブランドに確認してください。*

| PCI 要件 | 説明 | 準拠状態<br>（1 つ選択） | 改善日およびアクション<br>（準拠状態が "いいえ" の場合） |
|---|---|---|---|
| 1 | カード会員データを保護するために、ファイアウォール構成をインストールして維持する。 | ☐ はい<br>☐ いいえ | |
| 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提供のデフォルト値を使用しない。 | ☐ はい<br>☐ いいえ | |
| 3 | 保存されるカード会員データを保護する。 | ☐ はい<br>☐ いいえ | |
| 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。 | ☐ はい<br>☐ いいえ | |
| 5 | アンチウィルスソフトウェアを使用し、定期的に更新する。 | ☐ はい<br>☐ いいえ | |
| 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。 | ☐ はい<br>☐ いいえ | |
| 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。 | ☐ はい<br>☐ いいえ | |
| 8 | コンピュータにアクセスできる各ユーザに一意の ID を割り当てる。 | ☐ はい<br>☐ いいえ | |
| 9 | カード会員データへの物理アクセスを制限する。 | ☐ はい<br>☐ いいえ | |
| 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。 | ☐ はい<br>☐ いいえ | |
| 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。 | ☐ はい<br>☐ いいえ | |
| 12 | 情報セキュリティポリシーを整備する。 | ☐ はい<br>☐ いいえ | |

付録 E:　準拠証明書 - サービスプロバイダ

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

## オンサイト評価の準拠証明書
## – サービスプロバイダ

**バージョン 1.2**

2008 年 10 月

### *提出に関する指示*

認定セキュリティ評価機関（QSA）およびサービスプロバイダは、PCI データセキュリティ基準（PCI DSS）に対するサービスプロバイダの準拠状態を明らかにするものとしてこの文書を完成させる必要があります。すべての該当するセクションを完成させて、要求元のペイメントブランドに提出します。

| **パート 1. 認定セキュリティ評価機関の会社情報** | | | | | |
|---|---|---|---|---|---|
| 会社名: | | | | | |
| QSA リーダーの名前: | | | 役職: | | |
| 電話番号: | | | 電子メール: | | |
| 会社住所: | | | 市区町村: | | |
| 都道府県: | | 国: | | 郵便番号: | |
| URL: | | | | | |

| **パート 2. サービスプロバイダの組織情報** | | | | | |
|---|---|---|---|---|---|
| 会社名: | | | DBA: | | |
| 名前: | | | 役職: | | |
| 電話番号: | | | 電子メール: | | |
| 会社住所: | | | 市区町村: | | |
| 都道府県: | | 国: | | 郵便番号: | |
| URL: | | | | | |

**パート 2a. 提供されるサービス（該当するものすべてにチェック）**

| | | |
|---|---|---|
| ☐ 承認 | ☐ ロイヤルティプログラム | ☐ 3-D の安全なアクセス制御サーバ |
| ☐ スイッチング | ☐ IPSP（電子商取引） | ☐ 磁気ストライプ取引の処理 |
| ☐ ペイメントゲートウェイ | ☐ 清算および決済 | ☐ MO/TO 取引の処理 |
| ☐ ホスティング | ☐ 発行処理 | ☐ その他（指定してください）: |

PCI DSS レビューに含まれる施設および場所のリスト:

**パート 2b. 関係**

1 つ以上の第三者のサービスプロバイダと関係がありますか（ゲートウェイ、Web ホスティング企業、航空券予約代理店、ロイヤルティプログラム代理店など）? ☐ はい ☐ いいえ

**パート 2c. 取引処理**

*カード会員データをどのように、またどのような機能で、保存、処理、伝送していますか?*

*使用中のペイメントアプリケーション:* *ペイメントアプリケーションのバージョン:*

## パート 3. PCI DSS 検証

(date of ROC) 付の準拠に関するレポート("ROC")で言及されている結果を基に、(QSA Name) は、本書のパート 2 に記載されている事業体について (date) 現在で以下の準拠状態を証明します(1 つチェック):

☐ **準拠:** ROC 内のすべての要件が "対応 [8]" になっていて、合格スキャンが PCI SSC 指定スキャンベンダ (ASV Name) によって完了されています。これにより、(Service Provider Name) は、PCI DSS (insert version number) に完全に準拠していることを示しました。

☐ **非準拠:** ROC 内のいくつかの要件が "未対応" であるために全体的な評価が**非準拠**になっている、**または**合格スキャンが PCI SSC 指定スキャンベンダによって完了されていません。これにより、(Service Provider Name) は、PCI DSS への完全な準拠を示しませんでした。

準拠の**目標期日**:

状態が非準拠で、このフォームを提出する事業体は、本書のパート 4 にあるアクションプランを完了しなければならない場合があります。*すべてのペイメントブランドがこのセクションを要求するわけではないため、パート 4 を完成させる前にペイメントブランドに確認してください。*

## パート 3a. 準拠状態の確認

**QSA およびサービスプロバイダは以下を確認します:**

| | |
|---|---|
| ☐ | ROC は、PCI DSS 要件およびセキュリティ評価手順、バージョン (insert version number) の指示に従って完了されました。 |
| ☐ | 上記で参照されている ROC およびこの証明書のすべての情報は、評価の結果をすべての重要な点において公平に表しています。 |
| ☐ | サービスプロバイダは、PCI DSS に目を通し、常に完全な PCI DSS 準拠を維持する必要があることを認識しています。 |
| ☐ | 取引承認の後の磁気ストライプ(つまり追跡)データ[9]、CAV2、CVC2、CID、または CVV2 データ[10]、または PIN データ[11] が保存されているという証拠は、この評価でレビューされたすべてのシステムで見つかりませんでした。 |

## パート 3b. QSA およびサービスプロバイダの確認

| | |
|---|---|
| ***QSA リーダーの署名*** ↑ | ***日付:*** |
| ***QSA リーダーの名前:*** | ***役職:*** |

| | |
|---|---|
| ***サービスプロバイダ役員の署名*** ↑ | ***日付:*** |
| ***サービスプロバイダ役員名:*** | ***役職:*** |

[8] "対応" という結果には、QSA によってレビューされる代替コントロールも含める必要があります。代替コントロールが要件に関連するリスクを十分に軽減すると判断された場合、QSA はその要件を "対応" とする必要があります。

[9] カードを提示する取引中に、承認のために使用される磁気ストライプにエンコードされたデータ。取引承認の後、事業体は磁気ストライプデータ全体を保持してはいけません。保持できる追跡データの要素は、アカウント番号、有効期限、名前のみです。

[10] カードを提示しない取引を検証するために使用される、署名欄またはペイメントカードの前面に印字されている 3 または 4 桁の値。

[11] カードを提示する取引中に、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。

## パート 4. 非準拠状態のアクションプラン

要件ごとに該当する "準拠状態" を選択してください。要件に対して "いいえ" を選択した場合は、会社が要件に準拠する予定である日付と、要件を満たすために講じられるアクションの簡単な説明を記入する必要があります。*すべてのペイメントブランドがこのセクションを要求するわけではないため、パート 4 を完成させる前にペイメントブランドに確認してください。*

| PCI 要件 | 説明 | 準拠状態<br>（1 つ選択） | 改善日およびアクション<br>（準拠状態が "いいえ" の場合） |
|---|---|---|---|
| 1 | カード会員データを保護するために、ファイアウォール構成をインストールして維持する。 | ☐ はい<br>☐ いいえ | |
| 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提供のデフォルト値を使用しない。 | ☐ はい<br>☐ いいえ | |
| 3 | 保存されるカード会員データを保護する。 | ☐ はい<br>☐ いいえ | |
| 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。 | ☐ はい<br>☐ いいえ | |
| 5 | アンチウィルスソフトウェアを使用し、定期的に更新する。 | ☐ はい<br>☐ いいえ | |
| 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。 | ☐ はい<br>☐ いいえ | |
| 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。 | ☐ はい<br>☐ いいえ | |
| 8 | コンピュータにアクセスできる各ユーザに一意の ID を割り当てる。 | ☐ はい<br>☐ いいえ | |
| 9 | カード会員データへの物理アクセスを制限する。 | ☐ はい<br>☐ いいえ | |
| 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。 | ☐ はい<br>☐ いいえ | |
| 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。 | ☐ はい<br>☐ いいえ | |
| 12 | 情報セキュリティポリシーを整備する。 | ☐ はい<br>☐ いいえ | |

# 付録 F:　PCI DSS レビュー – サンプルの範囲指定および選択