Payment Card Industry

# データセキュリティ基準

## 変更点のまとめ

## PCI DSS のバージョン 3.2.1 から 4.0

改訂 1

2022 年 5 月

# ドキュメント変更

| 日付 | 改訂 | 商品説明 |
|---|---|---|
| 2022 年 3 月 | | PCI DSS v3.2.1 から v4.0 への初期リリース 変更点の概要 |
| 2022 年 5 月 | 1 | PCI DSS v4.0 要件 8.3.9 の変更点の説明を修正するために正誤表を更新しました。 |

*免責事項：本文書の英語版は、PCI SSC ウェブサイト上で利用可能になっており、全ての目的において、これらの文書の正規版と見做される。本記述と英語版記述との間に曖昧もしくは不一致がある限りにおいては該当部分に相当する英語版が優先される。*

# 目次


1 イントロダクション ..... 1

2 変更の種類 ..... 2

3 PCI DSS 導入部の変更点まとめ ..... 3

4 PCI DSS 要件の全般的な変更点の概要 ..... 6

5 要件ごとの追加変更点 ..... 7

6 新規要件の概要 ..... 31

# 1 イントロダクション

この文書は、*PCI DSS v3.2.1* から *PCI DSS v4.0* までの変更点を大まかにまとめて説明しており、すべての文書の改訂を詳述しているわけではありません。変更点の範囲が広いため、この要約文書だけに注目するのではなく、基準書全体を見直す必要があります。

この変更点の概要は、次のように構成されています:

- *変更の種類* - 変更の種類の概要
- *PCI DSS 導入部の変更点まとめ* - 影響を受ける各セクションの変更点の説明 。
- *PCI DSS 要件の全般的な変更点の概要* - 要件、テスト手順、およびガイダンス全体を通して行われた変更点についての説明 。
- *要件ごとの追加変更点* - 要件 1 ～ 12 および付録で行われた追加変更点の説明 。
- *新規要件の概要* - すべての新規要件、新規要件が適用される事業体（つまり、すべての事業体またはサービスプロバイダのみ）、および新規要件の発効日の一覧 。

# 2 変更の種類

| 変更の種類 | 定義 |
|---|---|
| 新規追加／変更 | 新たな脅威や技術、決済業界の変化に対応し、基準を最新のものにするための変更。 例としては、要件やテスト手順の新規追加や変更、要件の削除などがあります。 |
| 明確化またはガイダンス | 特定のトピックに関する理解を深めるため、またはさらなる情報やガイダンスを提供するために、言葉遣い、説明、定義、追加のガイダンス、および／または指示を更新します。 |
| 内容の再編成 | 要件の内容を揃えるための結合、分離、番号の付け直しなど、内容の再編成。 |

# 3 PCI DSS 導入部の変更点まとめ

| セクション | | 変更内容 | 変更の種類 |
|---|---|---|---|
| PCI DSS v3.2.1 | PCI DSS v4.0 | | |
| 概論および PCI データセキュリティ基準の概要 | 導入と PCI データセキュリティ基準の概要 | 「制限事項」の小見出しを追加し、PCI DSS が郡、州、または地域の法律に優先しないことを明確にしました。<br>PCI DSS リソースのリストを拡張しました。 | 明確化またはガイダンス |
| PCI DSS 適用性情報 | PCI DSS 適用情報 | 読みやすくするため、小見出しを追加しました。<br>プライマリアカウント番号（PAN）を保存、処理、または送信しない事業体には、一部の PCI DSS 要件が適用される場合があることを明確化しました。<br>アカウントデータ、機密認証データ（SAD）、カード会員データ、および PAN という用語は互換性がなく、PCI DSS では意図的に使用されていることを明確化しました。<br>カード会員データおよび機密認証データ（SAD）の全般的に使用される要素の表、保存が許可されているかどうか、およびデータを読み取り不可能にする必要があるかどうかを明確化しました。 | 明確化またはガイダンス |
| PCI DSS と PA-DSS との関係 | PCI DSS と PCI SSC ソフトウェア基準との関係 | PCI DSS と PCI SSC のソフトウェア標準の関係についてのセクションを再フォーカスし、PA-DSS（2022 年 10 月に引退）についても言及。 | 新規追加／変更 |
| PCI DSS 要件の適用範囲 | PCI DSS の要件の範囲 | PCI DSS 要件の適用範囲とカード会員データ環境（カード会員データ環境（CDE））の定義を明確化。<br>PCI DSS が適用されるシステムコンポーネントの例を拡張し、クラウドおよびその他のシステムコンポーネントを追加しましました。<br>「PCI DSS の適用範囲を理解する」ダイアグラムを追加。 | 明確化またはガイダンス |
| PCI DSS 要件の適用範囲 | PCI DSS 要件の適用範囲年次 PCI DSS 適用範囲確認 | 小見出しを追加し、既存の内容を明確化しました。 | 明確化またはガイダンス |
| 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 | PCI DSS 要件の範囲:セグメンテーション | 以前付録 D にあったセグメンテーション図を移動し、若干の編集を加えました。<br>サブセクションのタイトルを変更し、より広範なセグメンテーション管理をサポートするために、「ネットワークセグメンテーション」から「セグメンテーション」へと参照を更新しました。 | 明確化またはガイダンス |
| PCI DSS 要件の適用範囲:ワイヤレス | PCI DSS 要件の適用範囲:ワイヤレス | 不正無線検知（要件 11.2.1）は、カード会員データ環境（CDE）で無線が使用されていなくても、また、事業体がその使用を禁止するポリシーを持っ | 明確化またはガイダンス |

| セクション | | 変更内容 | 変更の種類 |
|---|---|---|---|
| PCI DSS v3.2.1 | PCI DSS v4.0 | | |
| | | ていても、実施しなければならないことを明確化しました。 | |
| | PCI DSS 要件の適用範囲:暗号化されたカード会員データと PCI DSS の適用範囲への影響 | サブセクションと関連コンテンツを追加。 | 明確化またはガイダンス |
| | PCI DSS 要件の適用範囲:第三者サービスプロバイダのカード会員データの暗号化と PCI DSS 適用範囲への影響 | 新しいサブセクションと関連コンテンツを追加。 | 明確化またはガイダンス |
| PCI DSS 要件の適用範囲:第三者サービスプロバイダ／アウトソーシングの使用 | PCI DSS 要件の適用範囲:サードパーティサービスプロバイダの使用 | サブセクションのタイトルを変更し、新しい内容を追加し、既存の内容を新しい小見出しの下に再編成しました。 | 明確化またはガイダンス |
| PCI DSS を日常業務のプロセスに導入するためのベストプラクティス | PCI DSS をビジネス・アズ・ユース・プロセスに導入するためのベストプラクティス | ガイダンスと明確化した内容を全体に追加しました。 | 明確化またはガイダンス |
| 評価期間: 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 | 評価者向け: PCI DSS アセスメントのためのサンプリング | セクションのタイトルを変更し、ガイダンスと明確化を追加して全体を更新しました。<br>評価者がテストされる集団に適したサンプルを選択することを支援するために、テスト手順からサンプリングに関する言及が削除されたことを明確にしました。 | 明確化またはガイダンス |
| 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 | 評価者向け: PCI DSS アセスメントのためのサンプリング | 付録 D にあったサンプリング図を移動し、若干の編集を加えました。 | 明確化またはガイダンス |
| | PCI DSS 要件で使用されるタイムフレームの説明 | PCI DSS および関連する期待事項で指定されている頻度およびタイムフレームを明確にするための新しいセクション。<br>"大幅な変更"の説明を追加。 | 明確化またはガイダンス |
| | PCI DSS の実施と確認のためのアプローチ | PCI DSS を実施および確認するための 2 つのアプローチ（定義されたアプローチおよびカスタマイ | 新規追加／変更 |

| セクション | | 変更内容 | 変更の種類 |
|---|---|---|---|
| PCI DSS v3.2.1 | PCI DSS v4.0 | | |
| | | ズアプローチ）を説明および図解するセクションを新設しました。 | |
| 代替コントロール | PCI DSS の実施と確認のためのアプローチ | このセクションの「定義されたアプローチ」の小見出しに内容を移しました。 | 内容の再編成 |
| | 事業体のセキュリティ態勢に関する情報の保護 | 新しいセクションでは、事業体が PCI DSS 評価から得た機密性の高い成果物をどのように扱うことができるかを説明します。 | 明確化またはガイダンス |
| | PCI DSS 要件のテスト方法 | 各 PCI DSS テスト手順で使用されるテスト方法と、それに対応する評価者が行うべき期待されるアクティビティを説明するセクションを新設しました。 | 明確化またはガイダンス |
| PCI DSS 評価プロセス | PCI DSS 評価プロセス | 細かな説明を含みます。<br>以前は「PCI DSS 要件とセキュリティ評価手順の詳細」に記載されていた「PCI DSS 要件は実施されているとはみなされない...」から始まる注記をここに移動しました。 | 明確化またはガイダンス |
| | 参考文献の追加 | PCI DSS 要件またはガイダンスの中で参照される外部事業体をリストアップする新しいセクション。 | 明確化またはガイダンス |
| PCI DSS 要件とセキュリティ評価手順の詳細 | 詳細な PCI DSS 要件とセキュリティ評価手順 | セクションの最初のページの内容を、要件欄、テスト手順欄、ガイダンス欄のすべての要素を説明する図解に差し替えました。<br>セクションの最初のページに、「サービスプロバイダのみに対する追加要件」と記載されました「要件」の説明を追加しました。<br>セクションの最初のページに、異なる種類の事業体に対する追加の PCI DSS 要件を含む付録の概要を追加しました。 | 明確化またはガイダンス |

# 4 PCI DSS 要件の全般的な変更点の概要

| PCI DSS 要件全体に実施されました全般的な変更点 | 変更の種類 |
|---|---|
| 概要のセクションを再フォーマットし、各主要要件の冒頭にセクションの概要を追加。 | 内容の再編成 |
| 概要部分を更新し、各要件部分の冒頭にガイダンスを追加。 | 明確化またはガイダンス |
| 各要件に該当する要件を整理して説明するために、各要件全体に番号付きの要件説明見出しを追加しました。 | 内容の再編成 |
| 要件とテスト手順の番号を変更し、要件の説明の見出しに番号を付けたため、要件を整理しました。 | 内容の再編成 |
| 指令的要件を目的型に言い換えました。 | 新規追加／変更 |
| 要件やテスト手順の例をガイダンス欄に移動しました。 | 内容の再編成 |
| テスト手順からサンプリングへの言及を削除。 | 明確化またはガイダンス |
| 要件とテスト手順の重複を最小限にするため、テストは「この要件に規定されているすべての要素に従って」行われることを明確にし、テスト手順を短縮しました。 | 明確化またはガイダンス |
| 整合性と一貫性を保つため、要件および／または対応するテスト手順の文言を更新しました。 | 明確化またはガイダンス |
| 各要件に期待されるバリデーションのレベルを明確にするため、テスト手順を強化しました。 | 明確化またはガイダンス |
| 要件とテスト手順を再フォーマットし、読みやすさのために文言を若干変更しました。 | 内容の再編成 |
| 同じ意図をサポートする要件を組み合わせ、異なる意図をサポートする要件を分離しました。 | 内容の再編成 |
| 複雑な要件／テスト手順を分離し、冗長または重複するテスト手順を削除しました。 | 内容の再編成 |
| テスト手順のみに記載されていた必須要素を要件に移し、要件の明確化とテスト手順の短縮を図りました。 | 明確化またはガイダンス |
| ポリシーと手順に関する要件を、各主要要件の最後から最初に移動し、文言を変更しました。 | 内容の再編成 |
| SSL／Early TLS を参照している要件について、ガイダンス欄から SSL／Early TLS に関する注記を削除しました。 | 明確化またはガイダンス |
| 用途や意図に合わせ、必要に応じて「カード会員データ」を「アカウントデータ」に変更しました。 | 明確化またはガイダンス |
| *PCI DSS 要件で使用されるタイムフレームの説明*に従い、要件全体で頻度を参照するために使用される用語を変更しました。 | 明確化またはガイダンス |
| ガイダンス欄のタイトルを追加し、内容を整理して理解を助け、類似の情報を統合しました。 | 内容の再編成 |

# 5 要件ごとの追加変更点

| 要件 | | 変更内容 | 変更の種類 |
|---|---|---|---|
| PCI DSS v3.2.1 | PCI DSS v4.0 | | |
| **要件 1** | | | |
| 要件 1 - 全般 | | 「ネットワークセキュリティコントロール」に焦点を当てるため、主要な要件のタイトルを更新しました。<br>「ファイアウォール」と「ルーター」を「ネットワークセキュリティコントロール」に置き換え、従来ファイアウォールが満たしていたセキュリティ目標を満たすために使用される、より広範な技術をサポートするようにしましました。 | 新規追加／変更 |
| 1.1.5 | 1.1.2 | 「ネットワークコンポーネントの管理に関するグループ、役割、責任の記述」の要件を、要件 1 の役割と責任に関する全般的な要件に置き換えましました。 | 新規追加／変更 |
| 1.1 | 1.2.1 | ネットワークセキュリティコントロールルールセットの構成基準を定義、実装、維持することについて、以前の「null」要件（すべての内容は他の要件を指しています）に焦点を当て直しました。 | 明確化またはガイダンス |
| 1.1.1 | 1.2.2 | 要件 6.5.1 で定義された変更管理プロセスに従って、変更が管理されることを明確化しました。 | 明確化またはガイダンス |
| 1.1.4 | | 冗長な要件を削除しました。 | 明確化またはガイダンス |
| 1.1.6 | 1.2.5<br>1.2.6 | 2 つの要件に分離し、それぞれの意図を明確にしました。 | 明確化またはガイダンス |
| 1.1.7 | 1.2.7 | ネットワークセキュリティコントロールの構成を少なくとも 6 カ月に 1 回見直すという趣旨を明確化しました。 | 明確化またはガイダンス |
| 1.2 | | 「null」要件を削除しました（すべての内容は他の要件を指しています）。 | 内容の再編成 |
| 1.2.2 | 1.2.8 | 設定ファイルのセキュリティ確保の意図を明確にしました。 | 明確化またはガイダンス |
| 1.2.1<br>1.3.4 | 1.3.1<br>1.3.2 | 要件 1.2.1.を 2 つの要件に分離し、それぞれの意図を明確にしました。<br>冗長な要件 1.3.4 を削除しました。 | 明確化またはガイダンス |
| 1.2.3 | 1.3.3 | 無線ネットワークとカード会員データ環境（CDE）間のネットワークセキュリティコントロールの実装の意図を明確にしました。 | 明確化またはガイダンス |

| 要件 | | 変更内容 | 変更の種類 |
|---|---|---|---|
| **PCI DSS v3.2.1** | **PCI DSS v4.0** | | |
| 1.3 | 1.4.1 | 以前は無効であった要件に焦点を当てました（すべての内容は他の要件を指しています）。<br>信頼できるネットワークと信頼できないネットワークの間でコントロールを実装することを意図していることを明確にしました。 | 明確化またはガイダンス |
| 1.3.1<br>1.3.2<br>1.3.5 | 1.4.2 | 信頼できないネットワークからのインバウンドトラフィックを制限する意図があることを明確にするため、要件を統合しました。 | 明確化またはガイダンス |
| 1.3.6 | 1.4.4 | カード会員データを格納するシステムコンポーネントが信頼されていないネットワークから直接アクセスできないようにすることを目的としていることを明確にしましました。 | 明確化またはガイダンス |
| 1.4 | 1.5.1 | 信頼されないネットワークとカード会員データ環境（CDE）の両方に接続するコンピューティングデバイスにセキュリティ管理を実装することを意図していることを明確にしました。 | 明確化またはガイダンス |
| **要件 2** | | | |
| 要件 2 - 全般 | | ベンダが提供するデフォルトの設定だけでなく、全般的な安全な設定に重点を置いていることを反映するため、主要な要件のタイトルを更新しました。 | 明確化またはガイダンス |
| | 2.1.2 | **新規：**役割と責任に関する新しい要件を追加しました。<br>*この要件は、すべての **v4.0** アセスメントに即時適用されます。* | 新規追加／変更 |
| 2.1 | 2.2.2 | ベンダのデフォルトアカウントが使用されているかどうかを把握し、それに応じた管理を行うことを意図していることを明確にしました。 | 明確化またはガイダンス |
| 2.2.1 | 2.2.3 | 異なるセキュリティレベルを必要とする主要機能を管理するための要件の意図を明確にしました。 | 明確化またはガイダンス |
| 2.2.2<br>2.2.5 | 2.2.4 | 類似のトピックを揃えるために要件を統合しました。 | 内容の再編成 |
| 2.2.3 | 2.2.5 | 要件の意図が、安全でないサービス、プロトコル、またはデーモンが存在する場合、であることを明確にしました。 | 明確化またはガイダンス |
| 2.1.1 | 2.3.1<br>2.3.2 | 無線ベンダのデフォルトを変更するためのすべての要件を 2 つに分割し、それぞれでフォーカスする点を明確にしました。 | 明確化またはガイダンス |
| 2.4 | 12.5.1 | 関連する内容を揃えるため、要件を移動しました。 | 内容の再編成 |
| 2.6 | | 「null」要件を削除しました（すべての内容は他の要件を指しています）。 | 内容の再編成 |

| 要件 | | 変更内容 | 変更の種類 |
|---|---|---|---|
| PCI DSS v3.2.1 | PCI DSS v4.0 | | |
| **要件 3** | | | |
| 要件 3 - 全般 | | アカウントデータに焦点を当てるため、主要要件のタイトルを更新しました。 | 明確化またはガイダンス |
| | 3.1.2 | **新規：**役割と責任に関する新しい要件を追加しました。<br>*この要件は、すべての v4.0 アセスメントに即時適用されます。* | 新規追加／変更 |
| 3.1 | 3.2.1 | **新規：**データ保持および廃棄の方針、手順、およびプロセスの実施を通して、オーソリゼーション完了前に保存されました機密認証データ（SAD）に対処するための新しい要件の箇条書きを追加しました。<br>*この箇条書きは、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| | 3.3.2 | **新規：**オーソリゼーションが完了する前に電子的に保管される機密認証データ（SAD）を暗号化するための新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| 3.2.a<br>3.2.b | 3.3.3 | イシュアによる機密認証データ（SAD）の保管は、正当な発行業務に必要なものに限定され、安全が確保されることを、従来の試験手順で対応するための要件を追加しました。 | 明確化またはガイダンス |
| 3.3 | 3.4.1 | 業務上必要な担当者のみが PAN の BIN／下 4 桁以上を確認できるよう、PAN を表示する際にマスキングすることを明確化しました。 | 新規追加／変更 |
| 12.3.10 | 3.4.2 | **新規：**リモートアクセス技術を使用する場合、PAN のコピーおよび／または再配置を防止するための技術的なコントロールに関する新しい要件を追加しました。旧要件 12.3.10 から拡張されたものです。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| 3.4 | 3.5.1 | PAN を読み取り不能にする手法の「インデックストークンおよびパッド」の箇条書きから、「パッド」を削除しました。 | 新規追加／変更 |
| | 3.5.1.1 | **新規：**ハッシュを使用して PAN を読み取り不能にする場合の、鍵付き暗号ハッシュに関する新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |

| 要件 | | 変更内容 | 変更の種類 |
|---|---|---|---|
| **PCI DSS v3.2.1** | **PCI DSS v4.0** | | |
| | 3.5.1.2 | **新規：**ディスクレベルまたはパーティションレベルの暗号化は、リムーバブル電子メディア上の PAN を読み取り不能にするためにのみ使用されるか、リムーバブルでない電子メディアで使用する場合は、要件 3.5.1 を満たすメカニズムで PAN も読み取り不能にするという新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| 3.5.1 | 3.6.1.1 | **新規：**サービスプロバイダのみ、暗号アーキテクチャの文書化された記述に、本番環境とテスト環境で同一の暗号鍵を使用しないことを含めることを新しい要件の箇条書きを追加しました。<br>*この箇条は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| **要件 4** | | | |
| 要件 4 - 全般 | | カード会員データの送信を保護するための「強力な暗号」に焦点を当て、主要要件のタイトルを更新しました。 | 明確化またはガイダンス |
| | 4.1.2 | **新規：**役割と責任に関する新しい要件を追加しました。<br>*この要件は、すべての v4.0 アセスメントに即時適用されます。* | 新規追加／変更 |
| 4.1 | 4.2.1 | **新規：**オープンな公共ネットワークでの PAN 送信に使用される証明書が有効であり、期限切れまたは失効していないことを確認するための新しい要件の箇条書きを追加しました。<br>*この箇条は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| | 4.2.1.1 | **新規：**信頼できる鍵および証明書のインベントリを維持するための新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |

| 要件 | | 変更内容 | 変更の種類 |
|---|---|---|---|
| PCI DSS v3.2.1 | PCI DSS v4.0 | | |
| **要件 5** | | | |
| 要件 5 - 全般 | | すべてのシステムとネットワークを悪意のあるソフトウェアから保護することに重点を置き、主要な要件のタイトルを更新しました。 | 明確化またはガイダンス |
| | | 従来、アンチウイルスソフトウェアによって満たされていたセキュリティ目標を満たすために使用される、より幅広い技術をサポートするために、全体を通して「アンチウイルス」を「アンチマルウェア」に置き換えました。 | 新規追加／変更 |
| | 5.1.2 | **新規：**役割と責任に関する新しい要件を追加しました。<br>*この要件は、すべての **v4.0** アセスメントに即時適用されます。* | 新規追加／変更 |
| 5.1.2 | 5.2.3 | 「マルウェアのリスクがないシステムコンポーネント」に焦点を当て、要件を明確にしました。 | 明確化またはガイダンス |
| | 5.2.3.1 | **新規：**マルウェアのリスクがないシステムコンポーネントの定期的な評価の頻度を、事業体のターゲットリスク分析で定義する新しい要件を追加しました。<br>*この要件は、**2025** 年 **3** 月 **31** 日まではベストプラクティスです。* | 新規追加／変更 |
| 5.2 | 5.3.1<br>5.3.2<br>5.3.4 | 1 つの要件を 3 つに分割し、各要件を 1 つのエリアにフォーカスしました。<br>• 自動更新により、マルウェアソリューションを最新の状態に保つこと<br>• 定期的なスキャンとアクティブスキャンまたはリアルタイムスキャンを実行すること（継続的な行動分析の新しいオプション付き）<br>• マルウェアソリューションによる監査ログを生成すること | 明確化またはガイダンス |
| | 5.3.2.1 | **新規：**事業体のターゲットリスク分析において、定期的なマルウェアスキャンを行う頻度を定義する新しい要件を追加しました。<br>*この要件は、**2025** 年 **3** 月 **31** 日まではベストプラクティスです。* | 新規追加／変更 |
| | 5.3.3 | **新規：リムーバブル電子メディア用マルウェアソリューションの新要件。**<br>*この要件は、**2025** 年 **3** 月 **31** 日まではベストプラクティスです。* | 新規追加／変更 |
| | 5.4.1 | **新規：**フィッシング攻撃を検知し、担当者を保護するための新しい要件を追加しました。*この要件は、**2025** 年 **3** 月 **31** 日まではベストプラクティスです。* | 新規追加／変更 |

| 要件 | | 変更内容 | 変更の種類 |
|---|---|---|---|
| PCI DSS v3.2.1 | PCI DSS v4.0 | | |
| **要件 6** | | | |
| 要件 6 - 全般 | | 主要要件のタイトルを更新し、「アプリケーション」ではなく「ソフトウェア」を含むようにしました。<br>要件 6.2 が特注ソフトウェアおよびカスタムソフトウェアにのみ適用されることを除き、要件 6 がすべてのシステムコンポーネントに適用されることを明確にしました。 | 明確化またはガイダンス |
| | 6.1.2 | **新規：**役割と責任に関する新しい要件を追加しました。<br>*この要件は、すべての v4.0 アセスメントに即時適用されます。* | 新規追加／変更 |
| 6.3 | 6.2.1 | ソフトウェアを安全に開発するための要件を移動し、すべてのソフトウェア開発の内容を要件 6.2 に合わせました。 | 内容の再編成 |
| | | 「内部および外部」を「特注およびカスタム」ソフトウェアに置き換えました。<br>この要件は、事業体のためにまたは事業体が事業体自身の使用のために開発したソフトウェアに適用され、第三者のソフトウェアには適用されないことを明確化しました。 | 明確化またはガイダンス |
| 6.5 | 6.2.2 | ソフトウェア開発者のトレーニングに関する要件 6.5 の要素を移動し、すべてのソフトウェア開発の内容を要件 6.2 に揃えました。<br>ソフトウェア開発担当者の教育要件を明確化しました。 | 明確化またはガイダンス |
| 6.3.2 | 6.2.3<br>6.2.3.1 | リリース前のカスタムソフトウェアのレビューに関する要件を移動し、すべてのソフトウェア開発内容を要件 6.2 に合わせましました。<br>全般的なコードレビューの実施方法と、手動コードレビューを実施する場合に必要な方法を分離するために、要件を分割しました。 | 明確化またはガイダンス |
| 6.5.1 – 6.5.10 | 6.2.4 | 全般的なコーディングの脆弱性に対処するための要件を移動し、要件 6.2 の下ですべてのソフトウェア開発内容を整合させました。<br>全般的なソフトウェア攻撃を防止または軽減する方法を 1 つの要件にまとめ、各攻撃の種類を説明する言語を一般化しました。 | 明確化またはガイダンス |
| 6.1<br>6.2 | 6.3 | セキュリティの脆弱性を特定し、パッチ適用によりシステムコンポーネントを脆弱性から保護するための要件を要件 6.3 に移しました。 | 内容の再編成 |

| 要件 | | 変更内容 | 変更の種類 |
|---|---|---|---|
| PCI DSS v3.2.1 | PCI DSS v4.0 | | |
| 6.1 | 6.3.1 | 特注／カスタムおよびサードパーティ製ソフトウェアの脆弱性への適用を明確にするため、箇条書きを追加しました。 | 明確化またはガイダンス |
| | 6.3.2 | **新規：**特注ソフトウェアおよびカスタムソフトウェアのインベントリを維持するための新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| 6.6 | 6.4.1 | 公開用 Web アプリケーションの新たな脅威と脆弱性への対応に関する要件を要件 6.4 に移しました。 | 内容の再編成 |
| | 6.4.2 | **新規：**公開用ウェブアプリケーションに対して、ウェブベースの攻撃を継続的に検出し、防止する自動化された技術的ソリューションを展開するための新しい要件を追加しました。この新しい要件では、手動または自動のアプリケーション脆弱性評価ツールまたは方法によって Web アプリケーションをレビューするという要件 6.4.1 のオプションが削除されます。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| | 6.4.3 | **新規：**消費者のブラウザに読み込まれ、実行されるすべての決済ページスクリプトの管理に関する新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| 6.3.1<br>6.4<br>6.4.1 – 6.4.6 | 6.5.1 – 6.5.6 | システムコンポーネントの変更に関する要件を要件 6.5 に移動・統合しました。 | 内容の再編成 |
| 6.4 | 6.5.3<br>6.5.4<br>6.5.5<br>6.5.6 | 特定の文書化された手順の要件を削除し、関連する各要件に方針と手順を確認するための試験手順を追加しました。 | 明確化またはガイダンス |
| 6.4.1 | 6.5.3 | 「開発／テストおよび本番」環境から「本番およびプレ本番」環境へ用語を変更しました。 | 明確化またはガイダンス |
| 6.4.2 | 6.5.4 | 「開発／テストおよび本番」環境から「本番およびプレ本番」環境へ用語を変更しました。<br>「職務の分離」という用語を変更し、本番環境とプレ本番環境における役割と機能の分離は、承認された変更のみが配備されるように説明責任を果たすことを目的としていることを明確にしました。 | 明確化またはガイダンス |

| 要件 | | 変更内容 | 変更の種類 |
|---|---|---|---|
| **PCI DSS v3.2.1** | **PCI DSS v4.0** | | |
| 6.4.3 | 6.5.5 | 「テストまたは開発」環境から「プレ本番」環境へ用語を変更しました。<br>適用されるすべての PCI DSS 要件に対応されている場合を除き、プレ本番環境ではライブ PAN を使用しないことを明確化しました。 | 明確化またはガイダンス |
| **要件 7** | | | |
| 要件 7 - 全般 | | システムコンポーネントとカード会員データを含むように、主要要件のタイトルを更新しました。 | 明確化またはガイダンス |
| | 7.1.2 | **新規：**役割と責任に関する新しい要件を追加しました。<br>*この要件は、すべての v4.0 アセスメントに即時適用されます。* | 新規追加／変更 |
| 7.1 | 7.2.1<br>7.2.2<br>7.2.3 | 特定の文書化された手順の要件を削除し、関連する各要件に方針と手順を確認するための試験手順を追加しました。 | 明確化またはガイダンス |
| 7.1.1 | 7.2.1 | アクセス制御モデルの定義に関する要件を明確化しました。 | 明確化またはガイダンス |
| 7.1.2<br>7.1.3 | 7.2.2 | 職務分類と機能に基づくアクセス権の割り当てと、最小限の権限に関する要件をまとめました。 | 内容の再編成 |
| 7.1.4 | 7.2.3 | 権限ある担当者による必要な権限の承認に関する要件であることを明確化しました。 | 明確化またはガイダンス |
| | 7.2.4 | **新規：**すべてのユーザアカウントと関連するアクセス権限のレビューに関する新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| | 7.2.5 | **新規：**すべてのアプリケーションとシステムアカウント、および関連するアクセス権の割り当てと管理に関する新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| | 7.2.5.1 | **新規：**アプリケーションおよびシステムアカウントによるすべてのアクセス、および関連するアクセス権限のレビューに関する新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| 8.7 | 7.2.6 | 要件 7 の内容との整合性を高めるため、要件を移動しました。 | 内容の再編成 |
| 7.2 | | 「null」要件を削除しました（すべての内容は他の要件を指しています）。 | 内容の再編成 |

| 要件 | | 変更内容 | 変更の種類 |
|---|---|---|---|
| PCI DSS v3.2.1 | PCI DSS v4.0 | | |
| **要件 8** | | | |
| 要件 8 - 全般 | | 「認証要素」および「認証クレデンシャル」の用語を統一しました。<br>「非消費者ユーザ」を削除し、消費者（カード保持者）が使用するアカウントには要件が適用されないことを概要で明確化しました。 | 明確化またはガイダンス |
| | | 単一の取引を促進するために一度に 1 つのカード番号のみにアクセスできるユーザアカウントには適用されない要件を列挙した概要の注記を削除し、関連する各要件にその注記を追加しました。 | 内容の再編成 |
| | 8.1.2 | **新規：**役割と責任に関する新しい要件を追加しました。<br>*この要件は、すべての v4.0 アセスメントに即時適用されます。* | 新規追加／変更 |
| 8.1.1 | 8.2.1 | この要件は、単一の取引を促進するために一度に 1 つのカード番号のみにアクセスできる POS 端末のユーザアカウントに適用することを意図していない旨の注記を追加しました。 | 明確化またはガイダンス |
| 8.5 | 8.2.2 | 要件のフォーカスを変更し、共有認証クレデンシャルの使用を許可するが、例外的にのみ使用できるようにした。 | 新規追加／変更 |
| | | この要件は、単一の取引を促進するために一度に 1 つのカード番号のみにアクセスできる POS 端末のユーザアカウントに適用することを意図していない旨の注記を追加しました。 | 明確化またはガイダンス |
| 8.5<br>8.5.1 | 8.2.2<br>8.2.3 | グループアカウント、共有アカウント、汎用アカウント、および顧客施設にリモートアクセスするサービスプロバイダに関する要件を要件 8.2 に移動しました。 | 内容の再編成 |
| 8.1.8 | 8.2.8 | この要件は、単一の取引を促進するために一度に 1 つのカード番号のみにアクセスできる POS 端末のユーザアカウントに適用することを意図していない旨の注記を追加しました。 | 内容の再編成 |
| 8.2 | 8.3.1 | この要件は、単一の取引を促進するために一度に 1 つのカード番号のみにアクセスできる POS 端末のユーザアカウントに適用することを意図していない旨の注記を追加しました。 | 内容の再編成 |
| 8.1.6<br>8.1.7 | 8.3.4 | 要件を統合し、要件 8.3 の下に移動しました。<br>この要件は、単一の取引を促進するために一度に 1 つのカード番号のみにアクセスできる POS 端末のユーザアカウントに適用することを意図していない旨の注記を追加しました。 | 内容の再編成 |

| 要件 | | 変更内容 | 変更の種類 |
|---|---|---|---|
| PCI DSS v3.2.1 | PCI DSS v4.0 | | |
| | | ユーザ ID をロックアウトするまでの無効な認証の試行回数を 6 回から 10 回に増やしました。 | 新規追加／変更 |
| 8.2.6 | 8.3.5 | 要件 8.3.1 を満たす認証要素としてパスワード／パスフレーズを使用する場合のみ、この要件が適用されることを明確化しました。 | 明確化またはガイダンス |
| 8.2.3 | 8.3.6 | **新規：**パスワードの長さを最低 7 文字から最低 12 文字（システムが 12 文字に対応していない場合は最低 8 文字）に増やすという新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。*<br>2025 年 3 月 31 日までは、v3.2.1 の要件 8.2.3 に従って、パスワードは最低 7 文字でなければならないことを明確にしました。<br>要件 8.3.1 を満たす認証要素としてパスワード／パスフレーズを使用する場合のみ、この要件が適用されることを明確にしました。<br>この要件は、単一の取引を促進するために一度に 1 つのカード番号のみにアクセスできる POS 端末のユーザアカウントに適用することを意図していない旨の注記を追加しました。 | 新規追加／変更 |
| 8.2.5 | 8.3.7 | この要件は、単一の取引を促進するために一度に 1 つのカード番号のみにアクセスできる POS 端末のユーザアカウントに適用することを意図していない旨の注記を追加しました。 | 内容の再編成 |
| 8.4 | 8.3.8 | ユーザ認証のポリシーと手順の伝達に関する内容を要件 8.3 に移動しましました。 | 内容の再編成 |
| 8.2.4 | 8.3.9 | この要件は、パスワード／パスフレーズがユーザーアクセスの唯一の認証要素として使用される場合（すなわち、一要素認証の実装において）に適用されることを明確にした。<br>この要件は、単一の取引を促進するために一度に 1 つのカード番号のみにアクセスできる POS 端末のユーザアカウントに適用することを意図していない旨の注記を追加しました。<br>要件は、サービスプロバイダの顧客アカウントには適用されないが、サービスプロバイダ担当者のアカウントには適用されるという注釈を追加しました。 | 明確化またはガイダンス |
| 8.2.4 | 8.3.9 | 90 日に 1 回以上パスワード／パスフレーズを変更する代わりに、アカウントのセキュリティ状態を動的に分析し、リソースへのアクセスを自動的に決定するオプションを追加しました。 | 新規追加／変更 |

| 要件 | | 変更内容 | 変更の種類 |
|---|---|---|---|
| PCI DSS v3.2.1 | PCI DSS v4.0 | | |
| 8.2.4.b | 8.3.10 | 以前のテスト手順から、サービスプロバイダがパスワード／パスフレーズの変更に関するガイダンスを顧客に提供するための要件に内容を移しました。<br>要件 8.3.10.1 が有効になると、この要件は要件 8.3.10.1 に取って代わられることを追記しました。 | 内容の再編成 |
| | 8.3.10.1 | **新規（サービスプロバイダのみ）**：パスワード／パスフレーズが顧客ユーザアクセスの唯一の認証要素である場合、パスワード／パスフレーズは少なくとも 90 日に 1 回変更されるか、アカウントのセキュリティ状態を動的に分析することによってリソースへのアクセスが自動的に決定されることを記載しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。*<br>この要件は、ペイメントカード情報にアクセスする消費者ユーザのアカウントには適用されないという注釈を追加しました。<br>本要件は、要件 8.3.10 が発効された時点で要件 8.3.10 よりも優先され、それまではサービスプロバイダは要件 8.3.10 または 8.3.10.1 のいずれかを満たすことができることを追記しました。 | 新規追加／変更 |
| 8.6 | 8.3.11 | 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、証明書などの認証要素に関する要件を要件 8.3 の下に移動しました。 | 内容の再編成 |
| 8.3 | | 「null」要件を削除しました（すべての内容は他の要件を指しています）。 | 内容の再編成 |
| | 8.4.2 | **新規：**カード会員データ環境（CDE）へのすべてのアクセスに多要素認証（MFA）を実装する新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。*<br>要件 8.4.2 および 8.4.3 で指定された両方のタイプのアクセスに MFA が必要であること、および 1 つのタイプのアクセスに MFA を適用しても、他のタイプのアクセスに MFA の別のインスタンスを適用する必要性に代わるものではないことを明確にするための注記が追加されました。 | 新規追加／変更 |
| | 8.5.1 | **新規：**多要素認証システムの安全な実装に関する新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |

| 要件 | | 変更内容 | 変更の種類 |
|---|---|---|---|
| PCI DSS v3.2.1 | PCI DSS v4.0 | | |
| | 8.6.1 | **新規：**対話型ログインに使用できるシステムまたはアプリケーションアカウントの管理に関する新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| | 8.6.2 | **新規：**対話型ログインに使用できるアプリケーションおよびシステムアカウントについて、パスワード／パスフレーズをファイルまたはスクリプトにハードコーディングしてはならない新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| | 8.6.3 | **新規：**アプリケーションおよびシステムアカウントのパスワード／パスフレーズを悪用されないように保護するための新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| 8.7 | 7.2.6 | 要件 7 の内容との整合性を高めるため、要件を移動しました。 | 内容の再編成 |
| **要件 9** | | | |
| 要件 9 - 全般 | | 概要において、要件 9 の対象となる 3 つの異なる領域（機密エリア、カード会員データ環境（CDE）、施設）を明確化しました。<br>全体を通して、各要件がカード会員データ環境（CDE）、機密エリア、施設のいずれに適用されるかを明確にしました。 | 明確化またはガイダンス |
| | 9.1.2 | **新規：**役割と責任に関する新しい要件を追加しました。<br>*この要件は、すべての v4.0 アセスメントに即時適用されます。* | 新規追加／変更 |
| 9.1 | 9.2.4 | 非使用時にロックすることによって機密エリアのコンソールへのアクセスを制限するという、以前の試験手順の箇条書きに対応するための要件を追加しましました。 | 明確化またはガイダンス |
| 9.2 | 9.3.1<br>9.3.2 | 担当者および訪問者の識別に関する要件を、それぞれ要件 9.3.1 および 9.3.2 に分割しました。 | 内容の再編成 |
| 9.4<br>9.4.1<br>9.4.2 | 9.3.2 | 訪問者のアクセス許可と管理に関する要件を要件 9.3.2 にまとめました。 | 内容の再編成 |

| 要件 | | 変更内容 | 変更の種類 |
|---|---|---|---|
| PCI DSS v3.2.1 | PCI DSS v4.0 | | |
| 9.5<br>9.5.1 | 9.4.1<br>9.4.1.1<br>9.4.1.2 | 媒体を物理的に保護する手順の要件（9.5）を削除し、その手順を関連する要件に統合しました。<br>メディアのバックアップを安全な場所に保管し、オフラインのバックアップ場所のセキュリティを少なくとも 12 カ月ごとに見直すという要件を 2 つの要件に分割しました。 | 明確化またはガイダンス |
| 9.6<br>9.6.1<br>9.6.2<br>9.6.3 | 9.4.2<br>9.4.3<br>9.4.4 | 媒体の内部および外部配布の手順に関する要件（9.6）を削除し、その手順を関連する要件に統合しました。 | 明確化またはガイダンス |
| 9.7<br>9.7.1 | 9.4.5<br>9.4.5.1 | メディアの保管とアクセス性を厳密に管理するための手順に関する要件（9.7）を削除し、関連する要件へ統合しました。<br>メディアインベントリログの維持とメディアインベントリの年 1 回の実施に関する要件を 2 つの要件に分割しました。 | 明確化またはガイダンス |
| 9.8<br>9.8.1<br>9.8.2 | 9.4.6<br>9.4.7 | メディアが不要になった場合のメディア破棄の手順に関する要件（9.8）を削除し、その手順を関連する要件に統合しました。<br>不要になったメディアの破棄には、電子メディアの破棄またはカード会員データの回復不能のいずれかの選択肢であることを明確化しました。 | 明確化またはガイダンス |
| 9.9 | 9.5.1 | 要件の焦点が「ペイメントカードフォームファクタとの直接的な物理的相互作用によってペイメントカードデータをキャプチャする POI 端末」にあることを明確化しました。<br>カードを提示する取引で使用される配備された POI 端末に要件が適用されることを明確化しました。 | 明確化またはガイダンス |
| | 9.5.1.2.1 | **新規：**事業体のターゲットリスク分析に基づき、定期的な POI 端末の検査頻度を定義するための新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |

| 要件 | | 変更内容 | 変更の種類 |
|---|---|---|---|
| PCI DSS v3.2.1 | PCI DSS v4.0 | | |
| **要件 10** | | | |
| 要件 10 - 全般 | | 監査ログ、システムコンポーネント、カード会員データへのフォーカスを反映させるため、主要要件のタイトルを更新しました。<br>これらの要件は、消費者（カード保有者）のユーザ活動には適用されないことを明確化しました。<br>「監査証跡」を「監査ログ」に置き換えました。 | 明確化またはガイダンス |
| | 10.1.2 | **新規：**役割と責任に関する新しい要件を追加しました。<br>*この要件は、すべての v4.0 アセスメントに即時適用されます。* | 新規追加／変更 |
| 10.2 | | 「null」要件を削除しました（すべての内容は他の要件を指しています）。 | 内容の再編成 |
| 10.5 | | 「null」要件を削除しました（すべての内容は他の要件を指しています）。 | 内容の再編成 |
| 10.5.1 – 10.5.5 | 10.3.1 – 10.3.4 | 監査ログ保護要件を要件 10.3 に移しました。 | 内容の再編成 |
| 10.5.3<br>10.5.4 | 10.3.3 | 類似のトピックを揃えるために要件を統合しました。 | 内容の再編成 |
| 10.6 | | 「null」要件を削除しました（すべての内容は他の要件を指しています）。 | 内容の再編成 |
| 10.6.1 – 10.6.3 | 10.4.1 – 10.4.3 | 監査ログレビューの要件を要件 10.4 に移動しました。 | 内容の再編成 |
| | 10.4.1.1 | **新規：**監査ログレビューの実行に自動化されたメカニズムを使用するための新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| | 10.4.2.1 | **新規：**その他のすべてのシステムコンポーネント（要件 10.4.1 で定義されていない）に対する定期的なログレビューの頻度を定義するために、ターゲットリスク分析に関する新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| 10.7 | 10.5.1 | 監査ログ履歴の要件を 10.5.1 に移しました。 | 内容の再編成 |
| 10.4<br>10.4.1 – 10.4.3 | 10.6.1 – 10.6.3 | 時刻同期に関する要件を 10.6 に移し、再編成しました。 | 内容の再編成 |
| 10.8 | 10.7.1 | *サービスプロバイダ*が重要なコントロールシステムの障害を検出し、警告し、迅速に対処するための要件を要件 10.7.1 に移動しました。 | 内容の再編成 |

| 要件 | | 変更内容 | 変更の種類 |
|---|---|---|---|
| **PCI DSS v3.2.1** | **PCI DSS v4.0** | | |
| | 10.7.2 | **新規：***すべての事業体*に対して、重要なセキュリティ管理システムの障害を検知し、警告し、迅速に対処するための新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。*<br>この新しい要件は、*すべての事業体*に適用されます。サービスプロバイダに対する要件 10.7.1 には含まれていない、2 つの追加の重要なセキュリティコントロールが含まれます。 | 新規追加／変更 |
| 10.8.1 | 10.7.3 | **新規：**重要なセキュリティ管理で障害が発生した場合、迅速に対応するための新しい要件を追加しました。<br>サービスプロバイダ向け:これは現行の PCI DSS v3.2.1 要件です。<br>その他のすべての事業体（サービスプロバイダ以外）：これは新しい要件です。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティス（非サービスプロバイダ向け）です。* | 新規追加／変更 |
| **要件 11** | | | |
| 要件 11 - 全般 | | 主要な要件のタイトルをマイナーアップデートしました。 | 明確化またはガイダンス |
| | 11.1.2 | **新規：**役割と責任に関する新しい要件を追加しました。<br>*この要件は、すべての v4.0 アセスメントに即時適用されます。* | 新規追加／変更 |
| 11.1 | 11.2.1 | 要件の意図が、許可および未許可の無線アクセスポイントの両方を管理することであることを明確にしました。<br>ワイヤレス技術の使用を禁止するポリシーが存在する場合でも、この要件が適用されることを明確にしました。 | 明確化またはガイダンス |
| | 11.3.1.1 | **新規：**内部の脆弱性スキャンで発見されたその他の該当する脆弱性（高リスクまたは重要としてランク付けされていないもの）をすべて管理するための新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| | 11.3.1.2 | **新規：**認証スキャンによって内部脆弱性スキャンを実行するための新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |

| 要件 | | 変更内容 | 変更の種類 |
|---|---|---|---|
| PCI DSS v3.2.1 | PCI DSS v4.0 | | |
| 11.2.3 | 11.3.1.3<br>11.3.2.1 | 内部および外部の脆弱性スキャンを実施し、大幅な変更があった場合は再スキャンを行うという要件を、内部スキャン（11.3.1.3）および外部スキャン（11.3.2.1）の要件として分離しました。 | 内容の再編成 |
| 11.3 | 11.4.1 | 以下を明確化しました。<br>• 方法論が定義され、文書化され、事業体により実施されている<br>• ペネトレーションテストの結果が、少なくとも 12 カ月間保持されている<br>• 方法論には、侵入テストで発見された悪用可能な脆弱性およびセキュリティ上の弱点によってもたらされるリスクを評価し、対処するための文書化されたアプローチが含まれている<br>• ネットワーク内部からのテスト（内部ペネトレーションテスト）およびネットワーク外部からのテスト（外部ペネトレーションテスト）の意味 | 明確化またはガイダンス |
| 11.3.3 | 11.4.4 | ペネトレーションテストの所見は、セキュリティ上の問題がもたらすリスクに関する事業体の評価に従って修正されることを明確化しました。 | 明確化またはガイダンス |
| | 11.4.7 | **マルチテナントサービスプロバイダー**が外部からの侵入テストのために顧客をサポートするための新しい要件。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| | 11.5.1.1 | **新規（サービスプロバイダ向け）：**サービスプロバイダが、侵入検知または侵入防止技術を使用して、マルウェアの秘密の通信経路を検知し、警告／防止し、対処するための新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| | 11.6.1 | **新規：**消費者ブラウザが受信した決済ページの HTTP ヘッダとコンテンツに対する不正な変更を警告する、変更と改ざんの検出メカニズムを導入するための新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| 11.2 | | 「null」要件を削除しました（すべての内容は他の要件を指しています）。 | 内容の再編成 |
| 11.1.2 | 12.10.5 | 不正な無線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手順の要件を移動し、他のインシデント対応項目と整合させました。 | 内容の再編成 |

| 要件 | | 変更内容 | 変更の種類 |
|---|---|---|---|
| **PCI DSS v3.2.1** | **PCI DSS v4.0** | | |
| 11.5.1 | 12.10.5 | 変更検出ソリューションによって生成されたアラートに対応するための要件を、他のインシデント対応項目と整合させるために移動しました。 | 内容の再編成 |
| **要件 12** | | | |
| 要件 12 - 全般 | | 情報セキュリティをサポートする事業体のポリシーとプログラムに焦点を当てていることを反映するために、主要な要件のタイトルを更新しました。 | 明確化またはガイダンス |
| 12.2 | | 正式な事業体全体のリスクアセスメントの要件を削除し、特定のターゲットリスク分析（12.3.1 および 12.3.2）に置き換えました。 | 新規追加／変更 |
| 12.4 | 12.1.3 | 担当者が自身の責任を正式に認識していることに関する内容を追加しました。 | 新規追加／変更 |
| 12.5<br>12.5.1 – 12.5.5 | 12.1.4 | 最高情報セキュリティ責任者または経営陣の知識のある他のメンバーに責任を正式に割り当てることを明確化しました。<br>情報セキュリティの責任を正式に割り当てるための要件を統合しました。 | 明確化またはガイダンス |
| 12.3<br>12.3.1 – 12.3.9 | 12.2.1 | エンドユーザ・テクノロジに対する許容使用ポリシーに関する要件の意図を明確にしました。<br>管理者の明示的な承認、技術の許容される使用方法、従業員が使用するために会社が承認したハードウェアおよびソフトウェア製品のリストに焦点を当てるために、要件を統合し削除しました。 | 明確化またはガイダンス |
| 12.3.10 | 3.4.2 | リモートアクセス技術を使用する際に、PAN のコピーや移転を防止するための技術管理に関する要件が削除され、新しい要件 3.4.2 が追加されました。 | 新規追加／変更 |
| | 12.3.1 | **新規：**実行頻度に柔軟性を持たせる PCI DSS 要件に対して、ターゲットリスク分析を実行するための新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| | 12.3.2 | **新規（カスタマイズアプローチを使用する事業体向け）：**カスタマイズアプローチを使用する事業体が、カスタマイズアプローチで満たす各 PCI DSS 要件についてターゲットリスク分析を実行するための新しい要件。<br>*この要件は、v4.0 評価を受けているすべての事業体で、カスタマイズアプローチを使用している場合に即時発効します。* | 新規追加／変更 |

| 要件 | | 変更内容 | 変更の種類 |
|---|---|---|---|
| PCI DSS v3.2.1 | PCI DSS v4.0 | | |
| | 12.3.3 | **新規：**少なくとも 12 カ月に一度、使用中の暗号スイートとプロトコルを文書化し、レビューするための新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| | 12.3.4 | **新規：**少なくとも 12 カ月に一度、使用中のハードウェアとソフトウェア技術を見直すための新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| 12.11<br>12.11.1 | 12.4.2<br>12.4.2.1 | 担当者による PCI DSS 作業がポリシーと手順に従って行われていることを確認するためのレビューに関する要件を要件 12.4 に移し、PCI DSS 準拠活動を管理するための他の要件と整合させました。 | 内容の再編成 |
| 2.4 | 12.5.1 | PCI DSS 範囲の文書化および確認に関する他の要件と整合さるため、要件 12.5 の下に移動しました。 | 内容の再編成 |
| | 12.5.2 | **新規：**少なくとも 12 カ月ごとに、また適用範囲の環境に大幅な変更があった場合に、PCI DSS の範囲を文書化し確認するための新しい要件を追加しました。<br>*この要件は、すべての v4.0 アセスメントに即時適用されます。* | 新規追加／変更 |
| | 12.5.2.1 | **新規（サービスプロバイダ向け）：**少なくとも 6 カ月に 1 回と、適用範囲の環境に大きな変更があった場合に、PCI DSS 範囲を文書化して確認するためのサービスプロバイダ向けの新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| | 12.5.3 | **新規（サービスプロバイダ向け）：**事業体構成の大幅な変更に伴う PCI DSS の範囲およびコントロールの適用性への影響の文書化されたレビューに関するサービスプロバイダ向けの新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| 12.6 | 12.6.1 | すべての担当者が、事業体の情報セキュリティポリシーおよびカード会員データの保護における各自の役割を認識することを意図していることを明確化しました。 | 明確化またはガイダンス |

| 要件 | | 変更内容 | 変更の種類 |
|---|---|---|---|
| PCI DSS v3.2.1 | PCI DSS v4.0 | | |
| | 12.6.2 | 少なくとも 12 カ月に一度、セキュリティ啓発プログラムを見直し、（必要に応じて）更新するための新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| 12.6.1<br>12.6.2 | 12.6.3 | セキュリティ意識向上トレーニングに関する要件を統合しました。 | 内容の再編成 |
| | 12.6.3.1 | **新規：**カード会員データ環境（CDE）のセキュリティに影響を与える可能性のある脅威や脆弱性についての認識を含む、セキュリティ啓発トレーニングの新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| | 12.6.3.2 | **新規：**要件 12.2.1 に従って、エンドユーザ・テクノロジの許容可能な使用に関する認識を含めるためのセキュリティ啓発トレーニングの新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| 12.8 | | 「null」要件を削除しました（すべての内容は他の要件を指しています）。 | 内容の再編成 |
| 12.8.1 – 12.8.5 | 12.8.1 – 12.8.5 | 「サービスプロバイダ」を「サードパーティサービスプロバイダ（TPSP）」に置き換えました。<br>PCI DSS 準拠の TPSP を使用することで事業体が PCI DSS 準拠になるわけではなく、事業体自身の PCI DSS 準拠に対する責任がなくなるわけでもないことを明確化しました。 | 明確化またはガイダンス |
| 12.8.2 | 12.8.2 | 「サービスプロバイダ」を「サードパーティサービスプロバイダ（TPSP）」に置き換えました。 | 明確化またはガイダンス |
| 12.8.3 | 12.8.3 | 「サービスプロバイダ」を「サードパーティサービスプロバイダ（TPSP）」に置き換えました。 | 明確化またはガイダンス |
| 12.8.4 | 12.8.4 | 「サービスプロバイダ」を「サードパーティサービスプロバイダ（TPSP）」に置き換えました。<br>事業体が事業体に代わって PCI DSS 要件を満たすために TPSP と契約している場合、事業体は TPSP と協力して該当する PCI DSS 要件が満たされるようにしなければならないことを明確にしました。TPSP が該当する PCI DSS 要件を満たしていない場合、それらの要件もその事業体に「適用されていない」ことになります。 | 明確化またはガイダンス |

| 要件 | | 変更内容 | 変更の種類 |
|---|---|---|---|
| PCI DSS v3.2.1 | PCI DSS v4.0 | | |
| 12.8.5 | 12.8.5 | 「サービスプロバイダ」を「サードパーティサービスプロバイダ（TPSP）」に置き換えました。<br>TPSP と事業体によって管理される PCI DSS 要件に関する情報には、TPSP と事業体の間で共有されるものを含めることを明確化しました。 | 明確化またはガイダンス |
| | 12.9.2 | **新規（サービスプロバイダ向け）：**要件 12.8.4 および 12.8.5 を満たすために、顧客からの情報要求をサポートするためのサービスプロバイダ向けの新しい要件を追加しました。<br>*この要件は、すべての v4.0 アセスメントに即時適用されます。* | 新規追加／変更 |
| 12.10 | | 「null」要件を削除しました（すべての内容は他の要件を指しています）。 | 内容の再編成 |
| 12.10.1 | 12.10.1 | 「システム違反」および「危殆化」を「セキュリティインシデントの疑いまたは確認」に置き換えました。 | 明確化またはガイダンス |
| 12.10.3 | 12.10.3 | 「警告」を「セキュリティインシデントの疑いまたは確認」に置き換えました。 | 明確化またはガイダンス |
| 12.10.4 | 12.10.4 | 「セキュリティ侵害」を「セキュリティインシデントの疑いまたは確認」に置き換えました。 | 明確化またはガイダンス |
| | 12.10.4.1 | **新規：**インシデント対応担当者の定期的な訓練の頻度を定義するために、ターゲットリスク分析を行う新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| 12.10.5<br>11.1.2<br>11.5.1 | 12.10.5 | 要件を統合し、インシデント対応計画の一部として監視および対応すべきセキュリティ監視システムを次のように更新しました。<br>• 不正な無線アクセスポイントの検出（旧 11.1.2）<br>• 重要ファイルの変更検出メカニズム（旧 11.5.1）<br>• **(新規項目)**決済ページの変更および改ざん検知メカニズムの使用に関する新しい要件項目（新しい要件 11.6.1 に関連する）<br>*この箇条書きは、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| | 12.10.7 | **新規：**想定外の場所で保存された PAN が検出された場合のインシデント対応手順を定め、開始されるための新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |

| 要件 | | 変更内容 | 変更の種類 |
|---|---|---|---|
| **PCI DSS v3.2.1** | **PCI DSS v4.0** | | |
| **付録 A1** | | | |
| 付録 A1 - 全般 | | マルチテナントサービスプロバイダに焦点を当て、主要要件のタイトルを更新しました。<br>マルチテナントサービスプロバイダとその環境について説明し、マルチテナントサービスプロバイダとその顧客との間の責任を明確にするために、要件の概要を更新しました。<br>全体を通して、「共有ホスティングプロバイダ」を「マルチテナントホスティングプロバイダ」に更新しましました。 | 明確化またはガイダンス |
| A1 | | 「null」要件を削除しました（すべての内容は他の要件を指しています）。 | 内容の再編成 |
| | A1.1.1 | **新規：**プロバイダ環境と顧客環境の論理的分離を実装するための新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| | A1.1.4 | 顧客環境を分離するために使用される論理的分離コントロールの有効性を、侵入テストを通じて確認するための新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| | A1.2.3 | **新規：**疑わしいまたは確認されたセキュリティインシデントおよび脆弱性を報告し、対処するためのプロセスおよび仕組みの導入に関する新しい要件を追加しました。<br>*この要件は、2025 年 3 月 31 日まではベストプラクティスです。* | 新規追加／変更 |
| A1.4 | A1.2.2 | 「侵害」を「疑いまたは確認されたセキュリティインシデント」に置き換えました。 | 明確化またはガイダンス |
| **付録 A2** | | | |
| 付録 A2 の変更は、A2.1 に要件の説明見出しを追加し、3 つの要件の番号を A2.1.1、A2.1.2、A2.1.3 に変更したのみです。 | | | 明確化またはガイダンス |

| 要件 | | 変更内容 | 変更の種類 |
|---|---|---|---|
| PCI DSS v3.2.1 | PCI DSS v4.0 | | |
| **付録 A3** | | | |
| 付録 A3 - 全般 | | 他の PCI 規準がこの付録の完成を参照する可能性があることを明確化しました。<br>すべての PCI DSS 要件が PCI DSS 評価を受けるすべての事業体に適用されるわけではないことを明確化し、そのため、一部の PCI DSS 要件はこの付録で重複していることを説明しました。この付録に関する質問は、アクワイアラーまたはペイメントブランドに問い合わせる旨を記載しました。 | 明確化またはガイダンス |
| A3.2.1 | A3.2.1 | PCI DSS 要件 12.5.2 と整合させるために、PCI DSS 範囲の文書化と確認に含まれる要素を更新しました。 | 新規追加／変更 |
| | A3.3.1 | 自動ログレビュー機構の障害を検出し、警告し、報告するための新しい要件の箇条書き。<br>自動化されたコードレビューツールの障害を検出し、警告し、報告するための新しい要件の箇条書き。<br>これらの箇条書きは、2025 年 3 月 31 日まではベストプラクティスです。 | 新規追加／変更 |
| 付録 B:代替コントロール | 付録 B:代替コントロール | 「正当かつ文書化された技術上またはビジネス上の制約」により、事業体が明示的に PCI DSS 要件を満たせない場合に、代替コントロールを考慮することができることを明確化しました。<br>項目 2 を更新し、多くの PCI DSS 要件の意図を理解するためにカスタマイズアプローチの目的およびその使用について言及しましました。<br>項目 4 の意図は、PCI DSS 要件を順守しないことによって課されるリスクに対処することであることを明確にしましました。<br>項目 6 を追加して、代替コントロールは現在および将来の要件に対処するために使用され、過去に見落とした要件に対処するために使用することはできないことを明確にしました。 | 明確化またはガイダンス |

| 要件 | | 変更内容 | 変更の種類 |
|---|---|---|---|
| PCI DSS v3.2.1 | PCI DSS v4.0 | | |
| 付録 C:代替コントロールワークシート | 付録 C:代替コントロールワークシート | 企業がワークシートを使用して代替コントロールを定義することが意図されていることを明確化しました。<br>項目 1 を「当初の要件への準拠を妨げる、技術上またはビジネス上の正当な制約を文書化する」に更新しました。<br>ワークシート項目の順序を変更し、項目 4 を項目 2 に移動しました。<br>項目 3 をカスタマイズアプローチの目的について言及するために更新し、項目を 2 つに分割して「オリジナルのコントロールの目的を定義する」と「代替コントロールが満たす目的を特定する」としました。<br>代替コントロールワークシート-完成例を削除しました。更新されました完成例は、別のガイダンス文書に含まれる予定です。 | 明確化またはガイダンス |
| | 付録 D:カスタマイズアプローチ | **新規：**カスタマイズアプローチの説明と解説を行うために、新しい付録を追加しました。 | 明確化またはガイダンス |
| | 付録 E:カスタマイズアプローチをサポートするサンプルテンプレート | **新規：**カスタマイズアプローチの一部として、企業が文書化するためのコントロールマトリックスとターゲットリスク分析のテンプレートの例について、新しい付録を追加しました。<br>事業体は特定のテンプレートのフォーマットに従う必要はなく、各テンプレートで定義されたすべての情報を提供しなければならないことを明確化しました。<br>2 つのテンプレートが含まれています。<br>• E1 コントロールマトリックスのテンプレート例<br>• E2 ターゲットリスク分析のテンプレート例 | 明確化またはガイダンス |
| | 付録 F:要件 6 をサポートするための PCI ソフトウェアセキュリティフレームワークの活用 | **新規：**PCI SSC の安全なソフトウェア基準の 1 つに従って開発および保守された特注またはカスタムソフトウェアを使用して、事業体が要件 6 のいくつかの要件を満たす方法について説明する新しい付録を追加しました。 | 明確化またはガイダンス |

| 要件 | | 変更内容 | 変更の種類 |
|---|---|---|---|
| PCI DSS v3.2.1 | PCI DSS v4.0 | | |
| | 付録 G:PCI DSS 用語集、略語、および頭字語 | **新規：**PCI DSS v4.0 用語集の新しい付録を追加しました。<br>用語集の全般的な更新内容は以下のとおりです。<br>• 更新された要件またはフィードバックに基づき、新しい用語を追加<br>• 他の資料で容易に検索できる一般的な用語を削除<br>• PCI DSS v4.0 では使用されていない用語を削除<br>• 略語の定義を短縮 | 明確化またはガイダンス |
| 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 | | 付録を削除し、従来の内容を「セグメンテーション」と「評価者向け」のセクションに移動しましました。PCI DSS 評価のためのサンプリング | 明確化またはガイダンス |

# 6 新規要件の概要

下の表にあるように、PCI DSS v4.0に含まれる新しい要件は、以下のいずれかです:

- すべての PCI DSS v4.0 評価に対して直ちに発効。

オア

- 2025 年 3 月 31 日まではベストプラクティス その後、効力を発揮します。各要件は、以下でそのように記されています。

| 新要件 | | 適用範囲 | | 発効日 | |
|---|---|---|---|---|---|
| | | 全ての事業体 | サービスプロバイダのみ | すべての v4.0 アセスメントで即時実施 | 2025 年 3 月 31 日 |
| **2.1.2** | 要件 2 の活動を行うための役割と責任が文書化され、割り当てられ、理解されている。 | ✓ | | ✓ | |
| **3.1.2** | 要件 3 の活動を行うための役割と責任が文書化され、割り当てられ、理解されている。 | ✓ | | ✓ | |
| **3.2.1** | オーソリゼーション完了前に保存された機密認証データ（SAD）は、データ保持および廃棄の方針、手順、およびプロセスの実施により、最小限にとどめる。 | ✓ | | | ✓ |
| **3.3.2** | オーソリゼーションが完了する前に電子的に保管される機密認証データ（SAD）は、強力な暗号技術を使用して暗号化される。 | ✓ | | | ✓ |
| **3.3.3** | イシュアが保管する機密認証データ（SAD）は、強力な暗号技術を使用して暗号化される。 | | ✓[1] | | ✓ |
| **3.4.2** | リモートアクセス技術を使用する場合、明示的な許可を得た場合を除き、PAN のコピーおよび／または移動を防止するための技術的な管理が行われている。 | ✓ | | | ✓ |
| **3.5.1.1** | PAN を読み取り不能にするために使用するハッシュ（要件 3.5.1 の最初の箇条書きによる）は、関連する鍵管理プロセスおよび手順を備えた PAN 全体の鍵付き暗号ハッシュとする。 | ✓ | | | ✓ |
| **3.5.1.2** | PAN を読み取り不可能にするために使用する場合、ディスクレベルまたはパーティションレベルの暗号化を実装する。 | ✓ | | | ✓ |

[1] *イシュアおよび発行サービスをサポートし、機密認証データを保管する企業のみに適用される。*

| 新要件 | | 適用範囲 | | 発効日 | |
|---|---|---|---|---|---|
| | | 全ての事業体 | サービスプロバイダのみ | すべての v4.0 アセスメントで即時実施 | 2025 年 3 月 31 日 |
| **3.6.1.1** | 暗号アーキテクチャの文書化された説明には、実稼働環境およびテスト環境における暗号鍵の使用防止が含まれる。 | | ✓ | | ✓ |
| **4.1.2** | 要件 4 の活動を実行するための役割と責任が文書化され、割り当てられ、理解されている。 | ✓ | | ✓ | |
| **4.2.1** | オープンな公共ネットワークでの送信時に PAN を保護するために使用される証明書が有効であることが確認され、有効期限が切れていない、または失効していない。 | ✓ | | | ✓ |
| **4.2.1.1** | 事業体の信頼できる鍵および証明書のインベントリが維持されている。 | ✓ | | | ✓ |
| **5.1.2** | 要件 5 の活動を実行するための役割と責任が文書化され、割り当てられ、理解されている。 | ✓ | | ✓ | |
| **5.2.3.1** | マルウェアのリスクがないと識別されたシステムコンポーネントの定期的な評価の頻度を決定するために、ターゲットリスク分析が実施される。 | ✓ | | | ✓ |
| **5.3.2.1** | 定期的なマルウェアスキャンの頻度を決定するために、ターゲットリスク分析が実施される。 | ✓ | | | ✓ |
| **5.3.3** | リムーバブル電子メディアが使用されている場合、マルウェア対策スキャンが実施される。 | ✓ | | | ✓ |
| **5.4.1** | フィッシング攻撃を検知し、従業員を保護する仕組みがある。 | ✓ | | | ✓ |
| **6.1.2** | 要件 6 の活動を実施するための役割と責任が文書化され、割り当てられ、理解されている。 | ✓ | | ✓ | |
| **6.3.2** | 脆弱性およびパッチ管理を容易にするため、特注およびカスタムソフトのインベントリを維持する。 | ✓ | | | ✓ |
| **6.4.2** | 公開用 Web アプリケーションに対して、Web ベースの攻撃を継続的に検出・防止する自動化された技術的ソリューションを展開する。 | ✓ | | | ✓ |

| 新要件 | | 適用範囲 | | 発効日 | |
|---|---|---|---|---|---|
| | | 全ての事業体 | サービスプロバイダのみ | すべての v4.0 アセスメントで即時実施 | 2025 年 3 月 31 日 |
| **6.4.3** | 消費者のブラウザに読み込まれ、実行されるすべての決済ページスクリプトを管理する。 | ✓ | | | ✓ |
| **7.1.2** | 要件 7 の活動を実行するための役割と責任が文書化され、割り当てられ、理解されている。 | ✓ | | ✓ | |
| **7.2.4** | すべてのユーザアカウントと関連するアクセス権限を適切にレビューする。 | ✓ | | | ✓ |
| **7.2.5** | すべてのアプリケーションおよびシステムのアカウント、並びに関連するアクセス権を適切に割り当て、管理する。 | ✓ | | | ✓ |
| **7.2.5.1** | アプリケーションおよびシステムアカウントによるすべてのアクセス、並びに関連するアクセス権を適切にレビューする。 | ✓ | | | ✓ |
| **8.1.2** | 要件 8 の活動を実施するための役割と責任が文書化され、割り当てられ、理解されている。 | ✓ | | ✓ | |
| **8.3.6** | 認証要素として使用されるパスワードの最小限の複雑さのレベル。 | ✓ | | | ✓ |
| **8.3.10.1** | パスワード／パスフレーズが顧客ユーザアクセスの唯一の認証要素である場合、パスワード／パスフレーズは少なくとも 90 日ごとに変更されるか、アカウントのセキュリティ状態が動的に分析され、リソースへのリアルタイムのアクセスが決定される。 | | ✓ | | ✓ |
| **8.4.2** | カード会員データ環境（CDE）へのすべてのアクセスに多要素認証が適用される。 | ✓ | | | ✓ |
| **8.5.1** | 多要素認証システムが適切に実装されている。 | ✓ | | | ✓ |
| **8.6.1** | システムやアプリケーションで使用するアカウントの双方向ログインを管理する。 | ✓ | | | ✓ |
| **8.6.2** | アプリケーションやシステムのアカウントの対話型ログインに使用されるパスワード／パスフレーズが悪用されないよう保護されている。 | ✓ | | | ✓ |

| 新要件 | | 適用範囲 | | 発効日 | |
|---|---|---|---|---|---|
| | | 全ての事業体 | サービスプロバイダのみ | すべての v4.0 アセスメントで即時実施 | 2025 年 3 月 31 日 |
| **8.6.3** | アプリケーションおよびシステムアカウントのパスワード／パスフレーズが悪用されないように保護されている。 | ✓ | | | ✓ |
| **9.1.2** | 要件 9 のアクティビティを実行するための役割と責任が文書化され、割り当てられ、理解されている。 | ✓ | | ✓ | |
| **9.5.1.2.1** | 定期的な POI 装置の検査頻度を決定するために、ターゲットリスク分析が実施される。 | ✓ | | | ✓ |
| **10.1.2** | 要件 10 の活動を実行するための役割と責任が文書化され、割り当てられ、理解されている。 | ✓ | | ✓ | |
| **10.4.1.1** | 監査ログレビューが自動化されている。 | ✓ | | | ✓ |
| **10.4.2.1** | 他のすべてのシステムコンポーネントのログレビューの頻度を決定するために、ターゲットリスク分析が実施される。 | ✓ | | | ✓ |
| **10.7.2** | 重要なセキュリティコントロールシステムの障害が迅速に検出され、警告され、対処される。 | ✓ | | | ✓ |
| **10.7.3** | 重要なセキュリティコントロールシステムの障害が迅速に対応される。 | ✓ | | | ✓ |
| **11.1.2** | 要件 11 の活動を実施するための役割と責任が文書化され、割り当てられ、理解されている。 | ✓ | | ✓ | |
| **11.3.1.1** | その他の該当するすべての脆弱性（高リスクまたは重要であるとランク付けされていないもの）を管理する。 | ✓ | | | ✓ |
| **11.3.1.2** | 内部脆弱性スキャンが認証されたスキャンによって実行される。 | ✓ | | | ✓ |
| **11.4.7** | マルチテナント型サービスプロバイダーは、外部からの侵入テストのためにお客様をサポートします。。 | | ✓ | | ✓ |
| **11.5.1.1** | 秘密のマルウェア通信チャネルは、侵入検知および/または侵入防止技術によって、検知、警告および/または防止、および対処を行います。 | | ✓ | | ✓ |
| **11.6.1** | 決済ページに対する変更および改ざん検知メカニズムが導入されている。 | ✓ | | | ✓ |

| 新要件 | | 適用範囲 | | 発効日 | |
|---|---|---|---|---|---|
| | | 全ての事業体 | サービスプロバイダのみ | すべての v4.0 アセスメントで即時実施 | 2025 年 3 月 31 日 |
| **12.3.1** | 各 PCI DSS 要件に対して、実行頻度に柔軟性を持たせたターゲットリスク分析が行われる。 | ✓ | | | ✓ |
| **12.3.2** | カスタマイズアプローチで満たされる各 PCI DSS 要件に対して、ターゲットとなるリスク分析が実行される。 | ✓ | | ✓ | |
| **12.3.3** | 使用されている暗号スイートおよびプロトコルが文書化され、レビューされる。 | ✓ | | | ✓ |
| **12.3.4** | ハードウェアおよびソフトウェア技術のレビューが行われる。 | ✓ | | | ✓ |
| **12.5.2** | PCI DSS の範囲を文書化し、少なくとも 12 カ月に 1 回確認する。 | ✓ | | ✓ | |
| **12.5.2.1** | PCI DSS の範囲は、少なくとも 6 カ月に 1 回、および大幅な変更時に文書化され、確認される。 | | ✓ | | ✓ |
| **12.5.3** | 重要な事業体の変更が PCI DSS の範囲に及ぼす影響を文書化し、確認し、その結果を経営陣に伝達する。 | | ✓ | | ✓ |
| **12.6.2** | セキュリティ意識向上プログラムは、少なくとも 12 カ月に 1 回レビューされ、必要に応じて更新される。 | ✓ | | | ✓ |
| **12.6.3.1** | セキュリティ意識向上トレーニングには、フィッシングおよび関連攻撃、ソーシャルエンジニアリングなど、カード会員データ環境（CDE）のセキュリティに影響を与える可能性のある脅威に関する意識が含まれている。 | ✓ | | | ✓ |
| **12.6.3.2** | セキュリティ啓発トレーニングには、エンドユーザ・テクノロジの許容される使用に関する啓発が含まれる。 | ✓ | | | ✓ |
| **12.9.2** | TPSP は、PCI DSS 準拠状況および TPSP の責任である PCI DSS 要件に関する情報を提供するよう顧客の要求をサポートする。 | | ✓ | ✓ | |
| **12.10.4.1** | インシデント対応担当者の定期的なトレーニングの頻度を決定するために、ターゲットリスク分析が実行される。 | ✓ | | | ✓ |

| 新要件 | | 適用範囲 | | 発効日 | |
|---|---|---|---|---|---|
| | | 全ての事業体 | サービスプロバイダのみ | すべての v4.0 アセスメントで即時実施 | 2025 年 3 月 31 日 |
| **12.10.5** | セキュリティインシデント対応計画には、決済ページの変更および改ざん検出メカニズムからのアラートが含まれる。 | ✓ | | | ✓ |
| **12.10.7** | インシデント対応手順が整備され、PAN が検出されると開始される。 | ✓ | | | ✓ |
| **A1.1.1** | マルチテナント型サービス事業者は、顧客環境とのアクセスが論理的に分離され、不正なアクセスを防止していることを確認する。 | | ✓ | | ✓ |
| **A1.1.4** | マルチテナント型サービス事業者は、顧客環境を分離するための論理的分離制御の有効性を、半年に一度以上、侵入テストにより確認しています。 | | ✓ | | ✓ |
| **A1.2.3** | マルチテナント型サービスプロバイダは、疑わしい又は確認されたセキュリティインシデント及び脆弱性を報告し、対処するためのプロセス又はメカニズムを実装している。 | | ✓ | | ✓ |
| **A3.3.1** | 以下のような障害が適時に検知され、警告され、報告されている。<br>ログレビューの自動化機構<br>コードレビューの自動化ツール | ✓ | | | ✓ |
| **合計:** | | 53 | 11 | 13 | 51 |
| **総計:** 64 | | | | | |