PCI（Payment Card Industry）

データセキュリティ基準

PCI DSS バージョン 1.2.1 からバージョン 2.0 への変更点のまとめ

2010 年 10 月

セクションまたは要件		変更点	種類[i]
変更前	変更後		
全般	全般	**全体** 他の用語集の用語に関する参照は通常提供されないため、参照物としての用語集の具体的な言及を削除した。	明確化
全般	全般	**準拠証明書** ▪ 準拠証明書を付録から削除し、別の文書にした。 ▪ 参照と付録のタイトルをドキュメント全体で不一致がないように更新した。	明確化
全般	全般	**概論および PCI データセキュリティ基準の概要** ▪ カード会員データの保護における PCI DSS の役割に関する情報を追加した。 ▪ 要件のタイトルを反映するように、「概要」の図を更新した。 ▪ PCI DSS が準拠評価中に使用するための評価ツールであることを明確化した。 ▪ PCI SSC Web サイトで利用できるリソースに関する情報を追加した。	追加のガイダンス
全般	全般	**PCI DSS 適用性情報** ▪ PTS Secure Reading and Exchange of Data（SRED）モジュールと整合するように、「*アカウントデータ*」という用語を追加した。 ▪ 「*カード会員データ*」と「*センシティブ認証データ*」に関する詳細を追加した。 ▪ プライマリアカウントデータ（PAN）が PCI DSS の適用性を決定する要素であることを明確化した。 ▪ 他の法律について説明した注釈を削除し、更新されたテキストに置き換えた。 ▪ PCI DSS 要件 3.4 に従って、どのデータ要素を読み取り不能にする必要があるかを明確化した段落と適用性の表を更新した。	明確化
N/A	全般	**PCI DSS と PA-DSS との関係** ▪ PA-DSS の内容を反映する新しいセクションを追加した。 ▪ PA-DSS 準拠アプリケーションのみの使用では、事業体の PCI DSS 準拠は実現されないことを明確化した。	追加のガイダンス

セクションまたは要件		変更点	種類[i]
変更前	変更後		
全般	全般	**PCI DSS 要件への準拠の評価範囲** ▪ 「*仮想コンポーネント*」を「*システムコンポーネント*」の定義に追加した。 ▪ カード会員データ環境は、"*カード会員データまたはセンシティブ認証データを保存、処理、または送信する人、処理、およびテクノロジ*" で構成されることを明確化した。	追加のガイダンス
全般	全般	**PCI DSS 要件への準拠の評価範囲** PCI DSS レビューの最初の手順は、カード会員データの場所とフローをすべて識別し、そのような場所のすべてが評価に含まれていることを確認することによって、評価の範囲を正確に決定することであることを明確化した詳細な段落を追加した。	追加のガイダンス
全般	全般	**ネットワークセグメンテーション** ▪ セグメンテーションが、物理的または論理的な手段を通じて説明できることを含めた説明を追加した。 ▪ 意味を明確化するために、いくつかの表現をマイナー変更した。	明確化
全般	全般	**ワイヤレス** LAN だけでなく WLAN の存在を明確化した。	明確化
全般	全般	**第三者/アウトソーシング** 整合性のため用語をマイナー変更した。	明確化
全般	全般	**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** ▪ 評価担当者が個別にサンプリングすること、また最初にビジネスをサンプリングしてから、選択された各設備内のシステムコンポーネントをサンプリングする必要があることを明確化した。 ▪ サンプリングが、カード会員データ環境または PCI DSS の適用性の範囲を狭めないこと、また、個別の PCI DSS 要件のサンプリングは許可されていないことを明確化した。 ▪ サンプリングを使用するときは、評価担当者が文書化する必要があるという特定の基準を明確化した。評価担当者はサンプリングの根拠を各評価ごとに再検証する必要があるという基準を追加した。	追加のガイダンス

セクションまたは要件		変更点	種類[i]
変更前	変更後		
全般	全般	**準拠に関するレポートについての指示と内容** ▪ 評価担当者が PCI DSS 評価範囲の正確性を検証した方法をレポートするための基準をパート 2 に追加した。 ▪ パート 2 のサンプリングの根拠とサンプルサイズの検証に関するレポート方法の詳細を、「サンプリング」セクションの明確化された内容と整合するように更新した。 ▪ インタビューした個人のリストに、その人の組織および対象トピックが含まれている必要があることをパート 3 で明確化した。 ▪ 「*評価期間*」をパート 2 からパート 4 へ移動し、評価期間が期間を示すものであり、評価を行った期間を特定するものである必要があることを追加した。 ▪ パート 5 の「*PCI DSS セキュリティスキャン手順*」を「*認定スキャニングベンダプログラムガイド*」に変更した。 ▪ パート 6 に N/A 回答に関する説明を追加した。 ▪ 整合性のため表現をマイナー変更した。	追加のガイダンス
全般	全般	**PA-DSS 準拠 - 完了手順** PCI SSC Web サイトの準拠証明書の参照を更新した。	明確化
全般	全般	**PCI DSS 要件およびセキュリティ評価手順の詳細** N/A 回答は「*対応*」列で報告する必要があるという説明を追加した。	明確化
1	1	**導入段落** ▪ 整合性のため表現をマイナー変更した。 ▪ ファイアウォール機能を提供するその他のシステムコンポーネントは、要件 1 に従って扱われる必要があるという説明を追加した。	追加のガイダンス
1.1.3	1.1.3.a、1.1.3.b	**テスト手順** テスト手順 1.1.3 をテスト手順 1.1.3.a ～ 1.1.3.b に分割した。	明確化
1.1.5	1.1.5	**要件** 安全でないサービス、プロトコル、またはポートの例を追加した。	追加のガイダンス
1.2	1.2	**要件** テスト手順に整合するように要件を更新した。	明確化

セクションまたは要件		変更点	種類[i]
変更前	変更後		
1.3	1.3	**テスト手順** 手順の目的を明確化するために再構成した。	明確化
1.3.1	1.3.1	**要件とテスト手順** DMZ の要件は、承認済みのサービス、プロトコル、ポートを提供するシステムコンポーネントに対する着信トラフィックの制限を目的としていることを明確化した。	明確化
1.3.3	1.3.3	**要件とテスト手順** インターネットと内部ネットワークの直接接続は許可されていないことを明確化した。	明確化
1.3.5	1.3.5	**要件とテスト手順** 承認された発信トラフィックのみが許可される目的を明確化した。	明確化
1.3.6	1.3.6	**テスト手順** ポートスキャナの使用の説明を削除することによって、テスト手順の柔軟性を向上した。	明確化
1.3.7	1.3.7	**要件とテスト手順** 要件が、データベースだけでなくあらゆる種類のカード会員データの保存に適用されることを明確化した。	明確化
1.3.8	1.3.8.a – 1.3.8.b	**要件とテスト手順** ▪ プライベート IP アドレスをインターネットに開示できないようにする目的、また、外部の事業体へのそのような開示を確実に承認されないようにする目的を明確化した。 ▪ IP マスカレードおよびネットワークアドレス変換（NAT）テクノロジの使用に関する言及を削除し、プライベート IP アドレスが開示されないようにする方法の例を追加した。 ▪ テスト手順を 2 つの手順に分割した。	追加のガイダンス
1.4.b	1.4.b	**テスト手順** テスト手順を要件と整合するように、パーソナルファイアウォールソフトウェアが、従業員が所有するコンピュータのユーザによって変更できないようにする必要があることを明確化した。	明確化
2.1	2.1	**要件** 明確化のため表現をマイナー変更した。	明確化

セクションまたは要件		変更点	種類[i]
変更前	変更後		
2.1.1	2.1.1.a – 2.1.1.e	**要件とテスト手順** ▪ 要件 4.1.1 と重複する内容を削除し、この要件の目的がベンダのデフォルト値が変更されていることを確認することであることを明確化した。 ▪ テスト手順 2.1.1 をテスト手順 2.1.1a ～ 2.1.1.e に分割した。 ▪ それだけでは強力な暗号化とは見なされなくなったため、WPA への言及を削除した。	明確化
2.2	2.2	**要件とテスト手順** システム強化基準の例をテスト手順から要件に移動し、ISO を強化基準のソースとして追加した。	明確化
6.2.b	2.2.b	**テスト手順** システム構成基準が要件 6.2 で特定された脆弱性で確実に更新されるようにするために、以前のテスト手順 6.2.b の内容を 2.2.b に移動した。	明確化
2.2.b	2.2.d	**テスト手順** テスト手順 2.2.b を 2.2.d に振り直した。	明確化
2.2.1	2.2.1	**要件** "*1 つのサーバに 1 つの主要機能*" にする目的と仮想化の使用を明確化するために要件を更新した。	追加のガイダンス
N/A	2.2.1.b	**テスト手順** ▪ 仮想化技術に関する新しいオプションのテスト手順を追加した。 ▪ テスト手順 2.2.1 を 2.2.1.a に振り直した。	追加のガイダンス
2.2.2	2.2.2、2.2.2.a – 2.2.2.b	**要件とテスト手順** ▪ 必要かつ安全なサービス、プロトコル、デーモンなどのみを有効にする必要があること、および安全でないサービスなどに実装されているセキュリティ機能について例を挙げて明確化した。 ▪ テスト手順 2.2.2 を手順 2.2.2.a と 2.2.2.b に分割した。	明確化
2.2.4	2.2.4.a ～ 2.2.4.c	**テスト手順** テスト手順 2.2.4 を手順 2.2.4.a ～ 2.2.4.c に分割した。	明確化

セクションまたは要件		変更点	種類[i]
変更前	変更後		
2.3	2.3、 2.3.a ～ 2.3.c	**要件とテスト手順** ▪ 強力な暗号化が必要であることを明確化した。 ▪ テスト手順 2.3 を手順 2.3.a ～ 2.3.c に分割した。	明確化
3	3	**導入段落** "*電子メールやインスタントメッセージングなどのエンドユーザメッセージングテクノロジを使用して保護されていない PAN を送信してはならない*" ことを明確化した。	明確化
3.1	3.1	**要件とテスト手順** 要件をより一般化して、以前 3.1 で定義されていたテスト手順を新しい要件およびテスト手順 3.1.1 に移動した（以下を参照）。	明確化
N/A	3.1.1、 3.1.1.a ～ 3.1.1.e	**要件およびテスト手順** ▪ 以前のテスト手順 3.1 をテスト手順 3.1.1.a ～ 3.1.1.d に振り直した。 ▪ テスト手順と整合するように要件に詳細を追加した。 ▪ 新しいテスト手順 3.1.1.e を追加して、保存されたデータがポリシーで定義されたデータ保存要件を超えていないことを評価担当者が確認する必要があることを明確化した。	明確化
3.2	3.2	**要件およびテスト手順** ▪ サービスの発行をサポートする発行者および会社は、業務上の理由がある場合やデータが安全に保存されている場合は、センシティブ認証データを保存できることを明確化した注を要件に追加した。 ▪ サービスの発行をサポートする発行者および会社が、センシティブ認証データを保存する場合は、業務上の理由があることを確認するための新しいテスト手順 3.2.a が追加された。 ▪ 以前のテスト手順 3.2 を "*その他のすべての事業体では*" で始まる 3.2.b に振り直した。	明確化
3.2.1	3.2.1	**要件およびテスト手順** 整合性のため "*チップ内の*" を "*チップ上の同等のデータ*" に置き換えた。	明確化
3.2.1 ～ 3.2.3	3.2.1 ～ 3.2.3	**テスト手順** "*以下を含むがこれらに限定されないデータソースを調べる*" ためにテスト手順を明確化した。	明確化

セクションまたは要件		変更点	種類[i]
変更前	変更後		
3.4	3.4	**要件** ▪ 要件が PAN にのみ適用されることを明確化した。 ▪ 最小限のアカウント情報に関しては要件および PCI DSS 適用性の表で明確化されているため、注を削除した。 ▪ ハッシングまたはトランケーションを使用して、PAN を読み取り不能にしている場合の要件を明確化した。 ▪ 同じ環境内のハッシュされた PAN およびトランケーション PAN のリスクを識別するために注を追加した。また、この注で、元の PAN データを再現できないことを確認するために追加のセキュリティコントロールが必要であることを説明した。 ▪ （代替コントロールはほとんどの PCI DSS 要件に適用できるため）代替コントロールの使用に関する注を削除した。	明確化
3.4.d	3.4.d	**テスト手順** PAN の "不適切な部分を削除" が "削除" と重なるため、PAN を "*読み取り不能にするかまたは削除する*" 必要があることを明確化した（以前の "*不適切な部分を削除または削除*" から変更）	明確化
3.4.1.c	3.4.1.c	**テスト手順** ディスク暗号化でリムーバブルメディアを暗号化できない場合、他の方法を使用する必要があることを注で明確化した。	明確化
3.5	3.5	**要件** ▪ カード会員データのセキュリティ保護に使用されているキーを開示や誤使用から保護する必要があることを明確化した。 ▪ この要件をキー暗号化キー（使用している場合）に適用する方法を明確化した注を追加した。	明確化
3.5.1	3.5.1	**テスト手順** 要件と整合するようにテスト手順を更新した。	明確化
3.5.2	3.5.2、 3.5.2.a ～ 3.5.2.b	**要件およびテスト手順** 要件と整合するテスト手順を追加した。	明確化

セクションまたは要件		変更点	種類[i]
変更前	変更後		
3.6	3.6	**要件およびテスト手順** ▪ 注をテスト手順から要件に移動した。 ▪ テスト手順 3.6.b で、サービスプロバイダは、サブ要件 3.6.1 から 3.6.8 に従って、顧客のキーの（単なる保存だけでなく）送信、保存、更新について説明したキー管理のガイダンスを顧客に提供する必要があることを明確化した。 ▪ サブ要件で説明されていたそのようなキーの安全な送信に関する注を削除した。	明確化
3.6.4	3.6.4	**要件およびテスト手順** ▪ "*少なくとも年に一度*" ではなく、定義された暗号化期間が終了した時点でキーを変更する必要があることを明確化した。 ▪ 業界のベストプラクティスに関するガイダンスを追加した。	明確化
3.6.5	3.6.5	**要件およびテスト手順** ▪ 表現を変更して、キーの完全性が弱くなった場合にキーを破棄または取り替える必要があることを例を挙げて明確化した。 ▪ 破棄された、または取り替えられたキーを保持する場合、そのキーは復号化または検証の目的でのみ安全にアーカイブおよび保持される必要があることを述べた注を追加した。 ▪ 破棄された、または取り替えられたキーを保持する場合、そのキーが暗号化操作に使用されていないことを検証するためのテスト手順を追加した。	明確化
3.6.6	3.6.6	**要件およびテスト手順** ▪ "*知識分割と二重管理*" は手動での平文暗号化キー管理の操作のみに適用されることを明確化した。 ▪ キー管理の操作の例を示す注を追加した。	明確化
3.6.8	3.6.8	**要件およびテスト手順** キー管理者が "*書面への署名*" だけでなく、自身のキー管理者としての責務を "*正式に確認する*" 必要があることを明確化した。	明確化

セクションまたは要件		変更点	種類[i]
変更前	変更後		
4.1	4.1、 4.1.a ～ 4.1.e	**要件およびテスト手順** ▪ セキュリティプロトコルの例として SSH を含め、テスト手順から例を削除した。 ▪ テスト手順 4.1 をテスト手順 4.1.a ～ 4.1.e に分割した。 ▪ 信頼できるキーまたは証明書（あるいはその両方）が、SSL/TLS だけでなくすべての種類の送信で必要なことを、テスト手順 4.1.b で明確化した。 ▪ 安全な構成を使用するために、プロトコルを実装する必要があることを、手順 4.1.c で明確化した。	明確化
4.1.1	4.1.1	**要件** 2010 年 6 月 30 日時点の WEP の使用に関する注を更新した。	明確化
4.2	4.2	**要件およびテスト手順** 保護されていない PAN は、エンドユーザメッセージングテクノロジで決して送信してはならないことを 「暗号化されていない」という表現を変更して明確化した。	明確化
5.2	5.2	**要件およびテスト手順** アンチウィルスメカニズムが単に監査ログを "*生成できる*" だけでなく、そのようなログを生成している必要があることを明確化した。	明確化
6.1	6.1	**要件** システムコンポーネントとソフトウェアを既知の脆弱性から保護する目的を明確化した。	明確化
6.2	6.2	**要件およびテスト手順** プロセスに、脆弱性の特定だけでなく、リスクに応じた脆弱性のランク分けが含まれている必要があることを追加した。リスクをランク分けする方法についてガイダンスを提供した。 ***注:*** *要件 6.2.a に定義された脆弱性のランク分けは、2012 年 6 月 30 日まではベストプラクティスとみなされ、それ以降は要件になる。*	発展型要件
6.3	6.3、 6.3.a ～ 6.3.d	**要件およびテスト手順** ▪ 安全な開発手法が適用されるソフトウェアアプリケーションの種類が追加された。 ▪ テスト手順 6.3.a をテスト手順 6.3.a ～ 6.3.d に分割した。	明確化

セクションまたは要件		変更点	種類[i]
変更前	変更後		
6.3.1	N/A	**要件およびテスト手順** 以前の 6.3.1 の脆弱性テストは 6.5.1 ～ 6.5.9 で扱われているため、要件およびテスト手順を削除した。	明確化
6.3.2 ～ 6.3.5	6.4.1 ～ 6.4.4	**要件およびテスト手順** 要件とテスト手順を 6.4 に移動し、要件が開発環境だけでなく、テストと開発環境に適用される目的を明確化した。	明確化
6.3.6 ～ 6.3.7	6.3.1 ～ 6.3.2	**要件およびテスト手順** 以前の要件がマージまたは移動（あるいはその両方）されたため、要件とテスト手順の番号を振り直した。	明確化
6.3.7	6.3.2	**要件およびテスト手順** ▪ 注から循環参照を削除した。 ▪ テスト手順（以前の 6.3.7.a と 6.3.7.b）を手順 6.3.2.a に統合して、"内部" アプリケーションと "Web" アプリケーションを 1 つの手順にまとめた。 ▪ Web 以外のアプリケーションなど範囲内のアプリケーションの安全なコーディング要件を統合するために、Web アプリケーションと OWASP ガイドへの言及を削除した。 ▪ 以前のテスト手順 6.3.7.c を 6.3.2.b に振り直した。	明確化
6.4	6.4	**要件およびテスト手順** ▪ コントロールプロセスと手順の変更に適用される要件とテスト手順を明確化した。 ▪ 以前のテスト手順 6.3.2 ～ 6.3.5 に整合するように、以前のテスト手順 6.3 から内容を取り込んだ。	明確化
6.3.4	6.4.3	**テスト手順** 目的を明確化するために、「*または使用する前に不適切な部分を削除する*」という表現を削除した。	明確化
6.4、 6.4.a ～ 6.4.b	6.4.5、 6.4.5.a ～ 6.4.5.b	**要件およびテスト手順** セキュリティパッチとソフトウェア変更に対処するために、以前の要件 6.4 を以前のテスト手順 6.4.a ～ 6.4.b と整合するように更新した。	明確化

セクションまたは要件		変更点	種類[i]
変更前	変更後		
6.4.1 ～ 6.4.4	6.4.5.1 ～ 6.4.5.4	**要件およびテスト手順** 取り込まれた要求およびテスト手順（以前の 6.3.2 ～ 6.3.5）と整合するように、番号を振り直した。	明確化
6.4.1	6.4.5.1	**テスト手順** 既存の要件と整合するように、影響に関して文書化が必要であることをテスト手順で明確化した。	明確化
6.4.2	6.4.5.2	**要件およびテスト手順** "*管理者*" ではなく "*適切な権限を持つ関係者*" による承認が必要なことを要件およびテスト手順で明確化した。	明確化
6.4.3	6.4.5.3、6.4.5.3.a ～ 6.4.5.3.b	**要件およびテスト手順** ▪ 以前の 6.4.3 の要件およびテスト手順は、"*変更がシステムのセキュリティに悪影響を与えていないことを確認するための機能テスト*" を意図していることを明確化した。 ▪ 6.5 に準拠して、カスタムコード変更のテストに対応するために、前の要件 6.3.1 を新しいテスト手順 6.4.5.3.b にマージした。	明確化
6.5	6.5	**要件およびテスト手順** ▪ 安全なコーディングと脆弱性の防止が、Web アプリケーションだけでなく、顧客が開発したすべての種類の評価範囲内のアプリケーションに適用されることを明確化した。 ▪ OWASP のみではなく、他の業界の例（SANS、CWE、CERT）を追加した。	明確化
6.5.1 ～ 6.5.10	6.5.1 ～ 6.5.9	**要件およびテスト手順** ▪ 以前の 6.5.1 ～ 6.5.10 の脆弱性を更新し、CWE、CERT、および OWASP の現在のガイダンスを反映するため、前の要件 6.3.1 と結合した。 ▪ 6.5.7 ～ 6.5.9 で Web アプリケーションに固有の脆弱性について特定した。	明確化
N/A	6.5.6	**要件およびテスト手順** 要件 6.2 に記載されたリスクの高い脆弱性に対処するために、新しい要件およびテスト手順を追加した。 ***注:*** *要件 6.2.a に定義された脆弱性のランク分けは、2012 年 6 月 30 日まではベストプラクティスとみなされ、それ以降は要件になる。*	発展型要件

セクションまたは要件		変更点	種類[i]
変更前	変更後		
7.1.3	7.1.3	**要件およびテスト手順** "*管理職により署名されたフォーム*" だけでなく、権限を持つ関係者による文書化された承認に関する要件を明確化した。	明確化
7.2.3	7.2.3	**要件およびテスト手順** 注をテスト手順から要件に移動した。	明確化
8	8	**導入段落** PA-DSS 要件 3.2 と整合するために注を追加した。注で "*1 つの取引を行うために一度に 1 つのカード番号にしかアクセスできない、POS ペイメントアプリケーション内のユーザアカウント（レジ係のアカウントなど）*" に対する一意のユーザ ID の適用性と安全な認証コントロールについて説明した。	明確化
8.2	8.2	**要件** 認証方法の明確化と例を追加した。	明確化
8.3	8.3	**要件およびテスト手順** "*トークンを使用する*" Radius および "*強力な認証をサポートするその他のテクノロジ*" を含めるために、2 因子認証の例を明確化した。 2 因子認証の意図を明確化する注を追加した。	明確化
8.5	8.5	**要件およびテスト手順** 「*識別*」という用語を追加した。	明確化
8.5.2、8.5.7、8.5.8、8.5.13	8.5.2、8.5.7、8.5.8、8.5.13	**要件およびテスト手順** パスワード以外の認証メカニズムを使用する会社に柔軟性を提供するために "*認証*" を追加した。	明確化
8.5.3	8.5.3	**要件およびテスト手順** 一意の値を設定し、初回使用後に直ちに変更する必要がある "*パスワードのリセット*" に関する記載を追加した。	明確化
8.5.6	8.5.6、8.5.6.a ～ 8.5.6.b	**要件およびテスト手順** ▪ ベンダによる "*アクセス*" を明確化した。テスト手順と整合するように要件を更新した。 ▪ テスト手順 8.5.6 を手順 8.5.6.a ～ 8.5.6.b に分割した。	明確化

セクションまたは要件		変更点	種類[i]
変更前	変更後		
8.5.9 ～ 8.5.13	8.5.9 ～ 8.5.13	**テスト手順** ▪ "*消費者以外のユーザ*" のパスワード管理要件をサービスプロバイダの観点から明確化した。 ▪ 各要件ごとにサービスプロバイダの手順を識別できるようにテスト手順を分割した。	明確化
8.5.16、8.5.16.a	8.5.16、8.5.16.a ～ 8.5.16.d	**要件およびテスト手順** ▪ データベースへの直接アクセスまたはクエリの制限がユーザアクセスに適用されることを明確化した。 ▪ テスト手順 8.5.16.a をテスト手順 8.5.16.a ～ 8.5.16.d に分割した。	明確化
9	9	**導入段落** ▪ 要件全体で使用される「*オンサイト要員*」、「*訪問者*」、および「*媒体*」の定義を追加した。 ▪ 以前使用されていた「*従業員*」を、新しい定義とともに新しい用語「*オンサイト要員*」に置き換え、範囲の意図を明確化した。	明確化
9.1.1	9.1.1.a ～ 9.1.1.c	**テスト手順** ▪ 以前のテスト手順 9.1.1 をテスト手順 9.1.1.a ～ 9.1.1.c に分割した。 ▪ ビデオカメラはアクセス制御メカニズムとともに使用される可能性があるアクセス監視メカニズムであるため、テスト手順の表現を "*ビデオカメラまたはアクセス制御メカニズム（あるいはその両方）*" に変更した。	明確化
9.1.2	9.1.2	**要件およびテスト手順** 「*従業員*」を「*オンサイト要員*」に置き換えた。物理的にアクセス可能なエリアの例を追加した。	明確化
9.1.3	9.1.3	**要件およびテスト手順** 「*ネットワーク/通信ハードウェアと通信回線*」を物理アクセスを制限する項目のリストに追加した。これらは以前は要件 9.6 に含まれていた。	明確化
9.2、9.2.a	9.2、9.2.a ～ 9.2.b	**要件およびテスト手順** ▪ 「*従業員*」を「*オンサイト要員*」に置き換えた。 ▪ テスト手順 9.2.a を手順 9.2.a ～ 9.2.b に分割した。	明確化

セクションまたは要件		変更点	種類[i]
変更前	変更後		
9.2.b	9.2.c	**テスト手順** 訪問者バッジにより訪問者とオンサイト要員が簡単に識別されることを確認することを明確化した。	明確化
9.3	9.3	**テスト手順** 要件と整合するために、テスト手順を訪問者管理に適用することを明確化した。	明確化
9.3.1	9.3.1	**テスト手順** アクセスの試行から訪問者は物理エリアに同行者なしでアクセスできないことの確認までの手順を明確化した。	明確化
9.3.2	9.3.2、 9.3.2.a ～ 9.3.2.b	**要件およびテスト手順** ▪ 「*従業員*」を「*オンサイト要員*」に置き換えた。 ▪ テスト手順 9.3.2 を手順 9.3.2.a ～ 9.3.2.b に分割した。 ▪ テスト手順 9.3.2.a は、訪問者の ID バッジが使用され、訪問者がオンサイト要員から識別できることを確認することを目的としていることを明確化した。	明確化
9.4	9.4	**要件およびテスト手順** 「*従業員*」を「*オンサイト要員*」に置き換えた。	明確化
9.5	9.5.a ～ 9.5.b	**テスト手順** ▪ テスト手順 9.5 を手順 9.5.a ～ 9.5.b に分割した。 ▪ テスト手順 9.5.a が保管場所の物理セキュリティの観察を目的としていることを明確化した。	明確化
9.6	9.6	**要件およびテスト手順** ▪ 導入段落で定義されている 「*紙および電子媒体*」を「*すべての媒体*」に置き換えた。 ▪ 「*ネットワーク、通信ハードウェア、通信回線*」をテスト手順 9.1.3 に移動した。	明確化
9.7 ～ 9.9	9.7 ～ 9.9	**要件およびテスト手順** 導入段落で既に定義されているため、「*カード会員データを含む媒体*」への言及を「*媒体*」への言及に置き換えた。	明確化
9.7.1	9.7.1	**要件およびテスト手順** 媒体上のデータの機密性を識別できるようにすることが目的であることを明確化した。	明確化

セクションまたは要件		変更点	種類[i]
変更前	変更後		
10.4	10.4、 10.4.1 ～ 10.4.3	**要件およびテスト手順** ▪ 時刻同期技術を使用して、システムクロックおよび時間を同期し、時間が適切に取得、配布、保存されていることを確認することが目的であることを明確化した。 ▪ 10.4 の「*時刻同期*」と「*NTP*」を「*時刻同期技術*」に変更し、「*NTP*」が時刻同期技術の一例であることを明確化した。 ▪ 前のテスト手順 10.4.a ～ 10.4.c を新しいサブ要件とテスト手順 10.4.1 ～ 10.4.3 に分割した（以下を参照）。	明確化
10.4	10.4.1	**要件およびテスト手順** ▪ 重要なシステムが確実に正確で一致した時間を保持するために、前のテスト手順 10.4.b から新しいサブ要件を作成した。 ▪ 時間を取得および配布する方法を説明するために、前のテスト手順 10.4.b を新しいテスト手順 10.4.1.a と 10.4.1.b に再構成した。	明確化
10.4	10.4.2	**要件およびテスト手順** 時刻データが保護されていて、時刻設定の変更が承認されていることを明確化する、新しいサブ要件とテスト手順 10.4.2.a と 10.4.2.b を追加した。	明確化
10.4.c	10.4.3	**要件およびテスト手順** 業界が承認したソースから時刻が確実に取得されるように、前の 10.4.c を新しいサブ要件に再構成した。	明確化
10.7.b	10.7.b	**テスト手順** ログデータを "*すぐ分析できる*" ようにする必要があるのではなく、監査ログプロセスがログデータを "*すぐ復元*' するために設けられていることを、テストで確認する必要があることを明確化した。	明確化

セクションまたは要件		変更点	種類[i]
変更前	変更後		
11.1	11.1	**要件およびテスト手順** ▪ "*四半期ごとに承認されていないワイヤレスアクセスポイントが検出される*" ようにプロセスが設けられている必要があることを明確化した。 ▪ 使用する方法にワイヤレスネットワークスキャン、システムコンポーネントおよびインフラストラクチャの物理/論理検査、ネットワークアクセス制御（NAC）、またはワイヤレス IDS/IPS を含めることができ、いずれの方法を使用する場合も、不正なデバイスを検出および識別できる機能を十分に備えている必要があることを追加した。	追加のガイダンス
11.1.a ～ 11.1.c	11.1.a ～ 11.1.e	**テスト手順** ▪ 前のテスト手順 11.1.a を手順 11.1.a ～ 11.1.c に分割した。 ▪ 承認されていないワイヤレスアクセスポイントを検出できる方法であることをテストするための新しいテスト手順 11.1.b を追加した。 ▪ 前のテスト手順 11.1.b を 11.1.d に振り直し、自動監視が使用されている場合、担当者に警告を生成する構成が適用されることを明確化した。 ▪ 前のテスト手順 11.1.c を 11.1.e に振り直した。	明確化
11.2	11.2、11.2.1 ～ 11.2.3	**要件およびテスト手順** ▪ 内部および外部スキャン要件を以前の 11.2 からサブ要件とテスト手順 11.2.1 ～ 11.2.3 に分割した。 ▪ 前のテスト手順 11.2.b の注を要件 11.2 に移動して、4 つの内部および外部スキャンが検証される必要があることを明確化した。	明確化
11.2.a	11.2.1.a ～ 11.2.1.c	**テスト手順** ▪ 内部スキャンプロセスに、合格結果が取得されるまでまたは PCI DSS 要件 6.2 で定義されているすべての「*高*」脆弱性が解消されるまで、再スキャンを実行することが含まれていることを明確化した。 ▪ 内部スキャンが認定された第三者によって実施される必要があることを明確化した。	明確化

セクションまたは要件		変更点	種類[i]
変更前	変更後		
11.2.b	11.2.2.a ～ 11.2.2.b	**テスト手順** ▪ 「*PCI セキュリティスキャン手順*」を「*ASV プログラムガイドの要件*」に置き換えた。 ▪ ASV が PCI セキュリティ基準審議会（ PCI SSC）によって承認されていることを明確化した。	明確化
11.2.c	11.2.3.a ～ 11.2.3.c	**テスト手順** 内部および外部スキャンに、高リスク脆弱性が対処されるまで、再スキャンを実行することを含める必要があり、認定された第三者によって実行される必要があることを記載した、の要件を明確化した。	明確化
11.3	11.3	**要件およびテスト手順** ▪ 判明した脆弱性が対処される必要があることを明確化した。 ▪ テスト手順 11.3.a をテスト手順 11.3.a ～ 11.3.b に分割した。	明確化
11.3.2	11.3.2	**要件およびテスト手順** アプリケーションのペネトレーションテストが関連する脆弱性に対してテストされる必要があること、およびアプリケーションのすべての種類を範囲に含める必要があることを明確化した。	明確化
11.4	11.4	**要件およびテスト手順** IDS/IPS が CDE 内のすべてのトラフィックだけでなく、境界および CDE 内の重要なポイントでトラフィックを監視することを明確化した。	明確化
11.5	11.5、 11.5.a ～ 11.5.b	**要件およびテスト手順** ▪ 「*ソフトウェア*」を「 *ツール*」に置き換えて、市販のソフトウェアが要件を満たす唯一の手段ではないことを意図していることを明確化した。 ▪ 既存の要件と整合するように、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テスト手順 11.5.b を追加した。	明確化
12	12	**要件のタイトル** 「*従業員および派遣社員*」を 「*すべての担当者*」に置き換えた。	明確化
12	12	**導入段落** 「*従業員*」を「*担当者*」に置き換えて、定義を少し変更した。	明確化

セクションまたは要件		変更点	種類[i]
変更前	変更後		
12.1	12.1	**テスト手順** 「*従業員*」を「*担当者*」に置き換えた。	明確化
12.1.2	12.1.2	**要件およびテスト手順** ▪ リスク評価方法の例を追加した。 ▪ テストでリスク評価文書が検証される必要があることを明確化した。	追加のガイダンス
12.1.3	12.1.3	**要件** 「*年に一度*」を「*年に一度*」に置き換えた。	明確化
12.3	12.3	**要件およびテスト手順** ▪ 明確化のため "*従業員に公開されている*" を削除した。 ▪ テクノロジの例に「*タブレット*」を追加した。	明確化
12.3.1	12.3.1	**要件およびテスト手順** 「*管理者*」を「*権限がある関係者*」に置き換えた。	明確化
12.3.4	12.3.4	**要件およびテスト手順** 論理ラベルを使用することを明確化した。	明確化
12.3.9	12.3.9	**要件およびテスト手順** 「*ビジネスパートナー*」を「*ベンダ*」とともに要件に追加した。	明確化
12.3.10	12.3.10、12.3.10.a ～ 12.3.10.b	**要件およびテスト手順** ▪ 禁止を許可のない担当者に制限して柔軟性を提供した。 ▪ テスト手順を 12.3.10 から 12.3.10.a に振り直した。適切な承認のある担当者が PCI DSS 要件に従ってカード会員データを保護していることを確認するための新しいテスト手順 12.3.10.b を追加した。	明確化
12.4	12.4	**要件およびテスト手順** 「*従業員と請負業者*」を「*担当者*」に置き換えた。	明確化
12.6	12.6	**要件およびテスト手順** 「*従業員*」を「*担当者*」に置き換えた。	明確化
12.6.1	12.6.1	**要件およびテスト手順** ▪ 「*従業員*」を「*担当者*」に置き換えた。 ▪ 担当者の役割に応じた方法の変更に関するガイダンスを提供する注を追加した。	追加のガイダンス

セクションまたは要件		変更点	種類[i]
変更前	変更後		
12.6.2	12.6.2	**要件およびテスト手順** ▪ 「*従業員*」を「*担当者*」に置き換えた。 ▪ 「*会社*」を「*事業体*」に置き換えた。	明確化
12.7	12.7	**要件およびテスト手順** ▪ 「*従業員*」を「*担当者*」に置き換えた。 ▪ 例をテスト手順から要件に移動した。 ▪ "*特定のポジションに雇用される可能性のある担当者*" に適用する要件 12.7 の注を明確化した。	明確化
12.8	12.8	**テスト手順** 整合性のため「*評価される事業体*」を「*事業体*」に置き換えた。	明確化
12.8.4	12.8.4	**要件およびテスト手順** 少なくとも年 1 回サービスプロバイダの PCI DSS 準拠ステータスを監視するための要件を明確化した。「*評価される事業体*」を「 *事業体*に置き換えた。	追加のガイダンス
12.9.1	12.9.1、12.9.1.a – 12.9.1.b	**テスト手順** ▪ テスト手順 12.9.1.b を追加して、文書化された手順が実際に運用されていることを確認することがテストに含まれている必要があることを明確化した。 ▪ テスト手順 12.9.1 を 12.9.1.a に振り直した。	明確化
12.9.3	12.9.3	**テスト手順** 要件と整合するために、指定された担当者が 24 時間体制でインシデントに対応できる必要があることを明確化した。	明確化
付録 D	準拠証明書– 加盟店	**準拠証明書** ▪ 付録から削除し、別の文書にした。 ▪ 評価担当者と加盟店の連絡先情報を再編成した。	明確化
付録 E	準拠証明書– サービスプロバイダ	**準拠証明書** ▪ 付録から削除し、別の文書にした。 ▪ 評価担当者とサービスプロバイダの連絡先情報を再編成した。 ▪ "*PCI DSS 評価範囲に含まれていたサービス*" のリストに追加のオプションを提示し、PCI DSS 評価で扱われていないサービスのリストを追加した。	明確化

セクションまたは要件		変更点	種類[i]
変更前	変更後		
付録 F	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** ▪ セグメンテーションとサンプリングのプロセスフローを明確化するためにタイトルを変更した。 ▪ ネットワークセグメンテーションとサンプリングに関する個別のセクションタイトルを作成した。 ▪ 導入部のサンプリングセクションと整合するように更新した。	明確化

[i] **「種類」の説明:**

変更後の種類	変更前の種類	定義
明確化	明確化	要件の趣旨を明確化する。基準の用語が、要件の目的を適切かつ簡潔に表現していること。
追加のガイダンス	説明	特定のトピックについて理解を深めるための、または特定のトピックの詳細情報を提供する説明または定義（あるいはその両方）
発展型要件	拡張	基準を新種の脅威や市場の変化に応じた最新の状態にするための変更