PCI（Payment Card Industry）

ペイメントアプリケーションデータセキュリティ基準

PA-DSS バージョン 1.2.1 から 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	**検証証明書** 検証証明書を付録から削除し、別の文書として作成した。これに従い文書への参照が削除された。	明確化
全般	全般	**この文書の目的** PCI SSC Web サイトで利用できるその他のリソースへの参照を追加した。	追加のガイダンス
全般	全般	**PCI DSS と PA-DSS との関係** ▪ 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する文章を追加した。 ▪ 磁気ストライプデータ "*またはチップ上の同等のデータ（あるいはその両方）*" の明確化	明確化
全般	全般	**PA-DSS の範囲** PA-DSS は、1 つの顧客用に開発され、その顧客のみに販売されるペイメントアプリケーションには適用されないことを明確化した。	明確化
全般	全般	**ハードウェア端末でのペイメントアプリケーションに対する PA-DSS 適用性** ハードウェア端末でのペイメントアプリケーションを取り扱うセクションを、（ペイメントアプリケーション以外で PA-DSS 要件を満たすことができる可能性があるため）更新、拡張、明確化し、セクション名を変更した。	追加のガイダンス
全般	全般	**ペイメントアプリケーション認定セキュリティ評価機関（PA-QSA）要件** 「*PA-QSA は、検証プロセスが実施されるラボラトリに自由に出入りできる必要があります*」をテストラボラトリから PA-QSA 要件のセクションへ移動した。	明確化
全般	全般	**テストラボラトリ** ラボラトリ環境のクリーンインストールを検証するために、PA-QSA のテストラボラトリのロケーションと要件を明確化した。	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		
全般	全般	**PCI DSS 適用性情報** ▪ PCI DSS と整合するように更新した。 ▪ 「*アカウントデータ*」という用語を追加し、「*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。 ▪ 段落を追加して（以前の注釈を置き換え）、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するために表を更新した。	明確化
全般	全般	**検証レポートについての指示と内容** 要件が指定されたペイメントアプリケーションに適用されない場合のレポート方法に関する基準をパート 3 に追加した。	明確化
全般	全般	**PA-DSS 完了手順** 検証証明書に関する言及を更新した。	明確化
すべての要件	すべての要件	**基準全体の要件列** 以前は「*PCI データセキュリティ基準の要件 X.X*」と記載されていた各注を、PCI DSS と PA-DSS 間の整合性を明確化するために、「*PCI DSS 要件 X.X に対応*」に書き換えた。	明確化
すべての要件	すべての要件	**基準全体の要件およびテスト手順** PA-DSS 要件を検証するために、"*PCI DSS 要件 X.X に従って*" PA-DSS 要件を検証するように以前記載されていた箇所はすべて、適切な要件とテスト手順を PCI DSS から取り込んで、ペイメントアプリケーションに適用できるように書き換えた。	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		
1.1	1.1	**要件およびテスト手順** ▪ 発行処理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、ペイメントアプリケーションがサービスの発行をサポートする発行者または会社（あるいはその両方）のみを対象としていることを確認するためのテスト手順 1.1.a を追加した。 ▪ 以前のテスト手順 1.1 を 1.1.b に振り直し、文頭に「*その他のすべてのペイメントアプリケーションでは*」を追加した。	明確化
1.1.1	1.1.1	**要件およびテスト手順** 「*チップ上の*」を「 *チップ上の同等のデータ* 」に変更した。	明確化
1.1.1 ～ 1.1.3	1.1.1 ～ 1.1.3	**要件およびテスト手順** 他の用語集の用語が、基準を通して用語集への参照が記載されていないため、用語集への具体的な参照を削除した。	明確化
1.1.1 ～ 1.1.3	1.1.1 ～ 1.1.3	**テスト手順** テストに "*少なくとも次の種類のデータファイル*" のレビューを含める必要があることを明確化した。	明確化
2.1	2.1	**テスト手順** カード会員データのすべての場所の識別に、過失によるカード会員データのキャプチャまたは保存を防ぐための基盤ソフトウェアを構成するための指示が含ま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		
2.3	2.3、 2.3.a ～ 2.3.e	**要件およびテスト手順** ▪ 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 を読み取り不能にす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。 ▪ テスト手順を PCI DSS から取り込んで、新しい手順 2.3.a ～ 2.3.e を作成した。	明確化
2.4	2.4、 2.4.a ～ 2.4.c	**テスト手順** PCI DSS への言及を削除し、PCI DSS のテスト手順を書き換えて、ペイメントアプリケーションに対応した新しい手順 2.4.a ～ 2.4.c を作成した。	明確化
2.5	2.5、 2.5.a ～ 2.5.c	**要件およびテスト手順** ▪ 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。 ▪ PCI DSS への言及を削除し、PCI DSS のテスト手順を書き換えて、ペイメントアプリケーションに対応した新しい手順 2.5.a ～ 2.5.c を作成した。	明確化
2.6	2.6、 2.6.1 ～ 2.6.7	**要件およびテスト手順** ▪ PCI DSS への言及を削除し、PCI DSS のテスト手順を書き換えて、ペイメントアプリケーションに対応した新しいサブ要件および手順 2.6.1 ～ 2.6.7 を作成した。 ▪ 『*PA-DSS 実装ガイド*』の確認をテスト手順 2.6.a に追加し、前の手順 2.6.a を 2.6.b に振り直した。	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		
2.7	2.7	**要件およびテスト手順** ▪ 安全な削除という以前の表現は、以前のバージョンのペイメントアプリケーションで保存された暗号化キーまたは要素を取得不能にするツールまたはプロセスを意味することを明確化した。 ▪ 暗号化キー要素または暗号文を取得不能にする例として「*キー暗号化キーの削除*」を追加した。	明確化
3.1	3.1、 3.1.1 ～ 3.1.10	**要件およびテスト手順** ▪ PCI DSS への言及を削除し、PCI DSS のテスト手順を書き換えて、ペイメントアプリケーションに対応した新しいサブ要件および手順 3.1.1 ～ 3.1.10 を作成した。 ▪ 安全な認証がアプリケーションのインストール完了およびインストール後の変更によって生成または管理されるすべてのアカウントに適用する必要があることを明確化した。	明確化
3.1.a ～ 3.1.c	3.1.a ～ 3.1.d	**テスト手順** ▪ 『*PA-DSS 実装ガイド*』の確認を取り扱うために、テスト手順 3.1.c を 3.1.a に移動し、取り込まれたサブ要件と整合するように内容を明確化した。 ▪ 取り込まれたサブ要件と整合するようにテスト手順 3.1.a を 3.1.d に移動し、安全な認証がアプリケーションのインストール完了およびインストール後の変更によって適用されることをテストすることについて明確化した。 ▪ ペイメントアプリケーションでデフォルトアカウントが変更されることをテストする新しいテスト手順を 3.1.c に追加した。	明確化
3.2	3.2	**要件** この要件が顧客へのベンダのガイダンスを取り扱っていることを明確化した。	明確化
4.1	4.1、 4.1.a ～ 4.1.b	**テスト手順** 再構成された要件と整合するように、テスト手順 4.2.b を 4.1.b に移動した。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		
4.2	4.2、 4.2.1 ～ 4.2.7	**要件およびテスト手順** ▪ 明確化のため、ログファイルに含める必要のある具体的な情報を追加した。 ▪ PCI DSS への言及を削除し、PCI DSS のテスト手順を書き換えて、ペイメントアプリケーションに対応した新しいサブ要件およびテスト手順 4.2.1 ～ 4.2.7 を作成した。	明確化
4.2	4.3、 4.3.1 ～ 4.3.6	**要件およびテスト手順** ▪ 明確化のため、ログファイルに含める必要のある具体的な情報を追加した。 ▪ PCI DSS（以前の 4.2）への言及を削除し、PCI DSS のテスト手順を書き換えて、ペイメントアプリケーションと対応する新しい要件、サブ要件、およびテスト手順 4.3.1 ～ 4.3.6 を作成した。	明確化
N/A	4.4	**新しい要件およびテスト手順** PCI DSS 要件 10.5.3 に整合するように、ペイメントアプリケーションでログの一元管理を強化する必要があることを追加した。	発展型要件
5.1	5.1	**要件およびテスト手順** PCI DSS 要件 6.3 と整合するように更新した。	明確化
5.1.1	N/A	**要件およびテスト手順** 5.1.1 を削除して、脆弱性テストが 5.2.1 ～ 5.2.9 で取り扱われるようにした。	明確化
5.1.2 ～ 5.1.3	N/A	**要件およびテスト手順** PA-DSS では本番環境はアプリケーション開発者に適用できないため説明を削除した。	明確化
5.1.1 ～ 5.1.7	5.1.1 ～ 5.1.4	**要件およびテスト手順** 前の要件 5.1.1 ～ 5.1.3 を削除したため、番号を振り直した。	明確化
5.1.4	5.1.1	**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
5.1.5	5.1.2	**要件およびテスト手順** テストデータとテストアカウントを "*顧客にリリースする*" 前に削除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		
5.1.7	5.1.4	**要件およびテスト手順** ▪ テスト手順（以前の 5.1.7.a と 5.1.7.b）を 1 つの手順 5.1.4.a に統合して、"内部" および "Web" アプリケーションを 1 つの手順にまとめ、以前の重複したテスト手順 5.1.7.b を削除した。 ▪ Web アプリケーションと OWASP ガイドへの具体的な言及を削除して、Web 以外のアプリケーションを含め、範囲内のすべてのアプリケーションの安全なコーディング要件を 1 つにまとめた。	明確化
5.2	5.2	**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の要件を Web アプリケーションだけでなく、範囲内の顧客が開発したすべての種類のアプリケーションに適用す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
5.2.1 ～ 5.2.10	5.2.1 ～ 5.2.9	**要件およびテスト手順** ▪ 以前の 5.2.1 ～ 5.2.10 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ように前の要件 5.1.1 とまとめた。 ▪ 要件 5.2.7 ～ 5.2.9 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	5.2.6	**要件およびテスト手順** 7.1 に記載されたリスクの高い脆弱性に対処するための新しい要件 5.2.6 を追加した。	発展型要件
5.3.2	5.3.2	**要件およびテスト手順** 要件とテスト手順を変更して、"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であることを明確化した。	明確化
5.3.3	5.3.3、5.3.3.a ～ 5.3.3.b	**要件およびテスト手順** ▪ 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に関する要件とテスト手順 5.3.3.a の目的を明確化した。 ▪ 5.2 に準拠した変更のテストに対応するために、前の要件 5.1.1 を新しいテスト手順 5.3.3.b にマージした。	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		
5.4	5.4	**要件およびテスト手順** ▪ 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明確化した。 ▪ テスト手順 5.4 を手順 5.4.a と 5.4.b に分割して、必要なサービスが "アウトオブボックス" で安全に構成されていることを確認するテスト手順 5.4.b に説明を追加した。 ▪ 『*PA-DSS 実装ガイド*』に必要なすべてのプロトコル、サービス、コンポーネント、依存するソフトウェアおよびハードウェアが記載されていることを確認するためのテスト手順 5.4 を追加した。	明確化
6.1	6.1、 6.1.a ～ 6.1.f	**テスト手順** ▪ PCI DSS への言及を削除して、PCI DSS テスト手順を取り込んで、ペイメントアプリケーションに対応した新しいテスト手順 6.1.a ～ 6.1.f を作成した。 ▪ テスト手順 6.1.f を更新して、『*PA-DSS 実装ガイド*』に含める必要のある指示を明確化した。	明確化
6.2	6.2	**要件およびテスト手順** ▪ 2010 年 6 月 30 日時点の WEP の使用に関する注を更新した。 ▪ テスト手順 6.2.b の PCI DSS への言及を削除して、『*PA-DSS 実装ガイド*』に含める項目を明確化した。	明確化
7.1	7.1、 7.1.a ～ 7.1.d	**要件およびテスト手順** 特定される脆弱性がリスクによってランク分けされていることを確認する 要件を更新した。要件と整合するように、テスト手順 7.1.a を追加した。 前のテスト手順 7.1 を 7.1.a ～ 7.1.d に分割した。	発展型要件
7.2.a ～ 7.2.b	7.2.a ～ 7.2.e	**テスト手順** 前のテスト手順 7.2.a を 7.2.a ～ 7.2.d に分割した。 前のテスト手順 7.2.b を 7.2.e に振り直した。	明確化
10、11	10	**要件およびテスト手順** 要件 10 と 11 をまとめて、冗長さを削除した。元の要件 10.1 を要件 10.3.1 に変更した。	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		
10、11	10	**要件およびテスト手順** ▪ 前の 11.1 を 10.1 に振り直した。ペイメントアプリケーションは安全なリモートアクセスのための 2 因子認証テクノロジの使用に干渉してはならないことを明確化した。"*トークンを使用する Radius*" の例を更新した。 ▪ 前の 11.2 を 10.2 に振り直した。内容には変更なし。 ▪ ペイメントアプリケーションへのリモートアクセスに関する親要件 10.3 を追加した。前の要件 10.1 と 11.3 をそれぞれ 10.3.1 と 10.3.2 に振り直した。内容には変更なし。 ▪ 例をテスト手順から要件の列に移動した。	明確化
12、13、14	12、13、14	**要件およびテスト手順** 要件 10 と 11 を 1 つにまとめたため、前の要件 12、13、および 14 をそれぞれ要件 11、12、および 13 に振り直した。	明確化
12.1	11.1	**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。 ▪ 整合性のため、用語 "*強力な暗号化とセキュリティプロトコル*" を明確化した。	明確化
12.2	11.2	**要件** ペイメントアプリケーションでエンドユーザメッセージングテクノロジによる PAN の送信が促進されている場合は、PAN を読み取り不能にするか、強力な暗号化を実装する必要があることを明確化した。	明確化
13.1	12.1	**要件およびテスト手順** 整合性のため、用語 "*強力な暗号化とセキュリティプロトコル*" を明確化した。	明確化
付録 A	付録 A	**すべての要件** ▪ PA-DSS 要件のマイナー変更に合わせて、『*PA-DSS 実装ガイド*』の内容を更新した。 ▪ PA-DSS 要件を反映するように PCI DSS への言及を更新した。	明確化
付録 B	付録 B	**項目 5.b** 前のバージョンから間違って削除したラボラトリ手順を再度追加した。	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 B	付録 B	**項目 6.b** PA-DSS 要件 5.1 および 5.2 への変更に対応して、脆弱性に関する言及を更新して、OWASP のみの言及を削除した。	明確化
付録 B	付録 B	**項目 7.c** PA-QSA がリモートラボラトリ環境のクリーンインストールを検証して、環境が実際に本番の状況をシミュレートしていることを確認する必要があるという説明を追加した。	明確化
付録 C	検証証明書	**付録から削除した** PA-QSA 情報の前にアプリケーションベンダ情報を提供するようにフォーマットを再編成した。	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