PCI Security Standards Council

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

要件とセキュリティ評価手順

バージョン 3.0

2013 年 11 月

文書の変更

日付	バージョン	説明	ページ
2008 年 10 月 1 日	1.2	内容を新しい PCI DSS v1.2 に合わせて改訂、およびオリジナルの v1.1 以降に加えられた若干の変更を追加。	
2009 年 7 月	1.2.1	「PA-DSS の範囲」の内容を『PA-DSS プログラム ガイド v1.2.1』に合わせ、PA-DSS が適用されるアプリケーションを明確にした。	v、vi
		ラボラトリ要件 6 の「OWASP」のスペルを修正。	30
		「検証証明書パート 2a」で、『PA-DSS プログラムガイド』に一覧表示されているアプリケーションの種類と一致するようにペイメントアプリケーション機能を更新して、パート 3b の年 1 回の再検証手続きを明確にした。	32, 33
2010 年 10 月	2.0	v1.2.1 からのマイナー変更を更新して実装し、新しい PCI DSS v2.0 と整合。詳細については、「PA-DSS—PA-DSS バージョン 1.2.1 から 2.0 への変更点のまとめ」を参照してください。	
2013 年 11 月	3.0	PA-DSS v2 からアップデート。詳細については、「PA-DSS - PA-DSS バージョン 2.0 から 3.0 への変更点のまとめ」を参照してください。	

目次

概要

この文書の目的

PCI 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）の要件およびセキュリティ監査手続きは、ペイメントアプリケーションを提供するソフトウェアベンダのセキュリティ要件と監査手続きを定義するものです。この文書は、ペイメントアプリケーションが PA-DSS に準拠することを検証するため、ペイメントアプリケーションのレビューを実施する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）によって使用されます。PA-DSS 監査の文書化および検証報告書（ROV）の作成方法については、PA-QSA は、PCI セキュリティスタンダードカウンシル（PCI SSC）のウェブサイト、www.pcisecuritystandards.org *から利用できる PA-DSS ROV 報告書テンプレートを参照してください。*

検証証明書、よくある質問（FAQ）、および『PCI DSS と PA-DSS の用語集（用語、略語、および頭字語）』などのその他のリソースは、PCI Security Standards Council（PCI SSC）の Web サイト（www.pcisecuritystandards.org）に掲載されています。

PCI DSS と PA-DSS との関係

PA-DSS 準拠アプリケーションを単独で使用しても、事業体の PCI DSS 準拠は確立されません。これは、そのアプリケーションが PCI DSS 準拠環境で実装され、ペイメントアプリケーションベンダが提供する『PA-DSS 実装ガイド』に従っている必要があるためです（PA-DSS 要件 13 に従う）。PA-DSS の要件は、*Payment Card Industry データセキュリティ基準（PCI DSS）の要件およびセキュリティ監査手続き*から派生しており、PCI DSS に準拠するために何が必要かを詳細に記しています（つまり、ペイメントアプリケーションが顧客の PCI DSS に準拠するには、何をサポートする必要があるか）。PCI SSC については、www.pcisecuritystandards.org を参照してください。

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

ペイメントアプリケーションベンダが顧客のカード会員データを保存、処理、または送信しない限り、PCI DSS は、ペイメントアプリケーションベンダに直接適用されない場合があります。ただし、これらのペイメントアプリケーションは顧客によってデータの保存、処理、送信に使用され、顧客は PCI DSS に準拠することが要求されるため、ペイメントアプリケーションは顧客の PCI DSS 準拠を促進すべきで、妨げてはいけません。次のようないくつかの場合に、安全でないペイメントアプリケーションは準拠を妨げる可能性があります。

1. 承認後の顧客のネットワークへの磁気ストライプデータやチップ内の相当するデータの保存
2. ペイメントアプリケーションが適切に動作するために、ウィルス対策ソフトウェアやファイアウォールなど、PCI DSS が必要とする他の機能を無効にすることを顧客に要求するアプリケーション
3. アプリケーションに接続して顧客へのサポートを提供するための、ベンダによる安全でない方法の使用

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

インテグレータとリセラー

アプリケーションベンダは、ベンダに代わってペイメントアプリケーションの販売、インストール、メンテナンスを行うインテグレータとリセラーと契約する場合があります。インテグレータ/リセラーは、ベンダの顧客に対するオンサイトサービスを提供し、検証済みの PA-DSS
ペイメントアプリケーションのインストールを支援するため、ペイメントアプリケーションの安全なインストールと操作性を確保する役割を担います。アプリケーションの構成、メンテナンス、サポートが正しくないと、攻撃者によって悪用される可能性があり、顧客のカード会員データ環境でセキュリティの脆弱性発生につながる可能性があります。アプリケーションベンダは、PCI DSS に準拠する形でペイメントアプリケーションをインストールして構成する方法を顧客、リセラー、インテグレータに教育する必要があります。

PCI 公認のインテグレータおよびリセラー（QIR）は、ペイメントアプリケーションを安全に実装するために、PCI DSS と PA-DSS
のカウンシルによるトレーニングを受けています。PCI QIR プログラムの詳細については、www.pcisecuritystandards.org を参照してください。

PCI DSS 適用性情報

PCI DSS
は加盟店、プロセサー、金融機関、サービスプロバイダのほか、カード会員データや機密認証データを保存、処理、または送信するその他の事業体などの、ペイメントカードの処理を行うすべての事業体に適用されます。

カード会員データと機密認証データの定義は次の通りです。

アカウントデータ	
カード会員データには、以下の情報が含まれます。	***機密認証データには、以下の情報が含まれます。***
▪ プライマリアカウント番号（PAN） ▪ カード会員名 ▪ 有効期限 ▪ サービスコード	▪ 全トラックデータ（磁気ストライプデータまたはチップ上の同等のデータ） ▪ CAV2/CVC2/CVV2/CID ▪ PIN または PIN ブロック

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

次のページにある表は、カード会員データと機密認証データの一般的に使用される要素について、そのデータの保存が許可されるか禁止されるか、このデータを保護する必要がある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。目的は、各データ要素に適用されるさまざまな種類の要件を示すことだけです。

		データ要素	***保存の許可***	***PA-DSS 要件 2.3 に従って、保存されたデータを読み取り不能にする***
アカウントデータ	***カード会員データ***	*プライマリアカウント番号（PAN）*	*はい*	*はい*
		カード会員名	*はい*	*いいえ*
		サービスコード	*はい*	*いいえ*
		有効期限	*はい*	*いいえ*
	機密認証データ	*全トラックデータ*[1]	*いいえ*	*PA-DSS 要件 1.1 に従って保存できない*
		CAV2/CVC2/CVV2/CID[2]	*いいえ*	*PA-DSS 要件 1.1 に従って保存できない*
		PIN/PIN ブロック[3]	*いいえ*	*PA-DSS 要件 1.1 に従って保存できない*

PCI DSS 要件 2.2 と 2.3 は PAN にのみ適用されます。PAN がカード会員データの他の要素と共に保存された場合、PCI DSS 要件 3.4 に従って PAN のみを読み取り不能にする必要があります。

機密認証データは承認後、たとえ暗号化していても保存してはなりません。これは環境内に PAN がない場合にも当てはまります。

1 *磁気ストライプのすべてのトラックのデータ、チップ上の同等のデータなど*
2 *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*
3 *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。*

PA-DSS の範囲

PA-DSS
は、カード会員データおよび/または重要な認証データを保存、処理、または送信する、ペイメントアプリケーションを開発するソフトウェアベンダなどに適用されます。異なるアプリケーションのタイプの適用性に関する詳細については、『*PA-DSS プログラムガイド*』を参照してください。

PA-DSS 評価の範囲には以下を含めてください。

- すべてのペイメントアプリケーションの機能として以下が挙げられますが、これらに限定されません。

  1) エンドツーエンドのペイメント機能（承認と決済）、

  2) 入力と出力、

  3) エラー状況、

  4）他のファイル、システム、またはペイメントアプリケーションやアプリケーションコンポーネント（あるいはこれらすべて）へのインターフェイスと接続、

  5）すべてのカード会員データフロー、

  6）暗号化メカニズム、

  7）認証メカニズム。

- ペイメントアプリケーションベンダが顧客とリセラー/インテグレータに提供することが期待されるガイダンス（この文書の「アプリケーションPA-DSS 実装ガイド」を参照してください）は、以下のことを保証します。

  1）顧客に PCI DSS に準拠する方法でペイメントアプリケーションを実装する方法を認識させ、

  2）特定のペイメントアプリケーションと環境の設定が PCI DSS 準拠を妨げる可能性があることを顧客に明確に伝える。

  ペイメントアプリケーションベンダは、特定の設定が以下の場合でもこのようなガイダンスを提供することを期待される可能性があります。

  1）アプリケーションを顧客がインストールした後はペイメントアプリケーションベンダが制御できない場合、または

  2）ペイメントアプリケーションベンダではなく顧客の責任である場合。

- レビューされるペイメントアプリケーションバージョンに対して選択されたすべてのプラットフォーム（関係するプラットフォームを指定してください）。
- カード会員データへのアクセスや表示のためにペイメントアプリケーションによって、またはペイメントアプリケーション内で使用されるツール（レポートツール、ログツールなど）。
- サードパーティソフトウェアの要件と依存関係を含め、すべてのペイメントアプリケーション関連のソフトウェアコンポーネントの範囲
- 完全な実装に必要なその他のペイメントアプリケーションのタイプの範囲。
- ベンダーのバージョン管理方法の範囲。

ハードウェア端末のペイメントアプリケーションに対する **PA-DSS 適用性**

このセクションではハードウェア端末（スタンドアロンまたは専用ペイメント端末とも呼ばれる）に常駐するペイメントアプリケーションの PA-DSS 検証を実行するベンダ向けのガイダンスを提供します。

ハードウェア端末に常駐するペイメントアプリケーションの PA-DSS 検証を実現するには次の 2 つの方法があります。

1. 常駐ペイメントアプリケーションがすべての PA-DSS 要件を直接満たしていて、標準の PA-DSS 手続きに従って検証される。
2. 常駐ペイメントアプリケーションは PA-DSS 要件のすべてを満たしているわけではないが、アプリケーションが常駐するハードウェアが PCI SSC の認定された PIN トランザクションセキュリティ（PTS）装置のリストに現在の PCI PTS 承認済み加盟店端末装置（POI）として一覧表示される。このシナリオでは、アプリケーションは PA-DSS と PTS の検証済みコントロールを組み合わせて、PA-DSS 要件を満たすことができる場合があります。

このセクションの残りは、検証済み PCI PTS の承認済み POI に常駐するペイメントアプリケーションにのみ適用されます。

ペイメントアプリケーションが 1 つ以上の PA-DSS 要件を直接満たすことができない場合は、PCI PTS 検証の一部としてテストされたコントロールによって間接的に満たすことができます。ハードウェアデバイスが PA-DSS レビューの対象となるようにするには、ハードウェアデバイスが PCI PTS 認定された POI として検証され、PCI SSC の承認済み PTS 装置のリストに含まれている必要があります。信頼できるコンピューティング環境を提供する PTS の検証済み POI はペイメントアプリケーションに "***必要な依存***" となり、アプリケーションとハードウェアの組み合わせが検証ペイメントアプリケーションの PA-DSS リストに一緒に表示されます。

PA-DSS 評価を実行するときに、PA-QSA はすべての PA-DSS 要件について、その依存するハードウェアと共にペイメントアプリケーションを完全にテストする必要があります。PA-QSA は、1 つ以上の PA-DSS 要件を常駐するペイメントアプリケーションでは満たすことができなくても、PCI PTS で検証されたコントロールで満たすことができると判断した場合、PA-QSA は以下を実行する必要があります。

1. どの要件が PA-DSS で規定されているように（通常どおり）満たされているかを明確に文書化する
2. どの要件が PCI PTS により満たされたかを"対応" ボックスに明確に文書化する
3. ペイメントアプリケーションが PA-DSS 要件を満たすことができなかった理由について詳細な説明を記載する
4. その要件が PCI PTS 検証済みコントロールによってどのように完全に満たされたかを判断するために実行された手続きを文書化する
5. 検証に関する報告書の概要で必要な依存として PCI PTS で検証されたハードウェア端末をリストに含める。

ペイメントアプリケーションの PA-QSA の検証が完了し、その後 PCI SSC によって承認されると、PTS 検証済みハードウェアデバイスは検証されたアプリケーションの PA-DSS リストにペイメントアプリケーションの依存として一覧表示されます。

PA-DSS と PCI PTS のコントロールの組み合わせによって検証されるハードウェア端末に常駐するペイメントアプリケーションは次の基準を満たす必要があります。

1. ハードウェア端末とアプリケーションの両方がまとめて顧客に提供される。または、個別に提供される場合、アプリケーションベンダまたはインテグレータ/リセラーは、検証済みのハードウェア端末でのみアプリケーションが稼働するように配布用のアプリケーションをパッケージ化する。
2. デフォルトで顧客の PCI DSS 準拠のサポートが有効化されている。
3. PCI DSS 準拠を維持するために、継続したサポートおよび更新が提供される。
4. アプリケーションが顧客に個別に販売、配布、またはライセンス供与される場合、ベンダは PA-DSS 検証の一覧に従って、アプリケーションと共に使用する必要のある依存ハードウェアの詳細を記述する。

PA-DSS 実装ガイド

検証されるペイメントアプリケーションは、PCI DSS に準拠する方法で実装できる必要があります。ソフトウェアベンダは、顧客とインテグレータ/リセラーに『*PA-DSS 実装ガイド*』を提供して、安全な製品実装を指示し、この文書で言及されている安全な構成の詳細を文書化し、PCI DSS 要件への対応に対するベンダ、インテグレータ/リセラー、顧客の責任を明確化する必要があります。顧客やインテグレータ/リセラーが顧客のネットワーク内でセキュリティ設定を有効にする方法を詳述します。たとえば、『PA-DSS 実装ガイド』では、ペイメントアプリケーションによって制御されない場合であっても PCI DSS パスワードセキュリティの責任および基本機能について説明してください。顧客またはインテグレータ/リセラーが PCI DSS 準拠のための安全なパスワードを実装する方法を理解できるようにするためです。

『PA-DSS 実装ガイド』は、PCI DSS または PA-DSS から要件を再度説明するだけでなく、要件を満たすペイメントアプリケーションを構成する方法について、詳細を提供する必要があります。評価中に、PA-QSA は、指示が正確かつ有効であることを確認する必要があります。PA-QSA は、『PA-DSS 実装ガイド』が顧客とインテグレータ/リセラーに配布されたことを確認する必要もあります。

ペイメントアプリケーションは、『PA-DSS 実装ガイド』に従って実装され、PCI DSS 準拠の環境に実装されるときに、顧客の PCI DSS 準拠を促進し、サポートします。

『PA-DSS 実装ガイド』に指定されている *コントロールの実装に関する責任の比較については、「付録 A: PA-DSS 実装ガイドの内容の要約」を参照してください。*

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

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）の会社に雇用されている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）のみが PA-DSS 評価を実施することができます。PA-DSS 評価の実施を認定されている会社の一覧については、www.pcisecuritystandards.org にあるペイメントアプリケーションQSAの一覧を参照してください。

- PA-QSA は、このペイメントアプリケーションデータセキュリティ基準文書に記述されているテスト手続きを利用する必要があります。
- 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。

テストラボラトリ

- テストラボラトリは、PA-QSA ロケーションにオンサイトで、またはソフトウェアベンダロケーションにオンサイトで設置できます。
- テストラボラトリは、ペイメントアプリケーションの本番環境をシミュレートできる必要があります。
- PA-QSA はクリーンインストールのラボラトリ環境を検証して、環境が実際に本番の状況をシミュレートしていること、ベンダが環境をいっさい変更または改ざんしていないことを確認する必要があります。
- ラボラトリと関連する ラボラトリプロセスの詳しい要件については、この文書の「付録 B: PA-DSS 評価用テストラボラトリ構成確認書」を参照してください。
- PA-QSA は、レビューでペイメントアプリケーションに対して使用された特定のラボラトリに関して付録 B を完成させ、完成した検証報告書（ROV）の PA-DSS 報告書の一部として提出する必要があります。

検証報告書についての指示と内容

PA-DSS の検証報告書（ROV）の指示と内容は、*PA-DSS ROV 報告書テンプレートにて提供されています。PA-DSS ROV報告書テンプレート*は、準拠に関する報告書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。準拠したペイメントアプリケーション ROV のみを、PCI SSC に提出する必要があります。ROV の提出プロセスの詳細については、『PA-DSS プログラムガイド』を参照してください。

PA-DSS 完了手順

この文書には、要件とセキュリティ評価手順を示す表、「付録 B: PA-DSS 評価用テストラボラトリ構成」が含まれています。要件とセキュリティ評価手順は、PA-QSA が実施する必要がある手続きを詳しく説明したものです。.

PA-QSA は以下の手順を実行する必要があります。

1. PA-DSS 評価の対象範囲を確認します。
2. PA-DSS 評価を実施します。
3. *PA-DSS ROV テンプレート*を使用して、PA-DSS 評価で使用されるテストラボラトリ構成を含む、検証報告書(ROV)を完成させます。
4. 検証証明書を完成させて署名する(PA-QSA とソフトウェアベンダの両方)。検証証明書は PCI SSC Web サイト(www.pcisecuritystandards.org)から入手できます。
5. 完了後、上記の文書すべてと PA-DSS 実装ガイドを『PA-DSS プログラムガイド』に従って PCI SSC に提出します。

注: *すべての PA-DSS 要件が所定の位置にあると検証されない限り、PA-DSS の提出は実施されるべきではありません。*

PA-DSS プログラムガイド

次のトピックを含め、PA-DSS プログラムの管理に関する情報については、『PA-DSS プログラムガイド』を参照してください。

- 異なるタイプのアプリケーションに対する PA-DSS 適用性
- PA-DSS 報告書の提出と承認プロセス
- 検証済みアプリケーションのリストに含まれるペイメントアプリケーションの年 1 回の更新プロセス
- 掲載されたペイメントアプリケーションが情報漏洩において問題があると判断された場合の通知責任

PCI SSC
には、ペイメントアプリケーションデータセキュリティ基準への大幅な変更、または掲載されたペイメントアプリケーションで具体的に特定された脆弱性(あるいはその両方)を理由として再検証を要求する権利があります。

PA-DSS 要件およびセキュリティ評価手順の詳細

以下に、PA-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。

- **PA-DSS 要件** - この列は、検証されるペイメントアプリケーションのセキュリティ要件を定義します。
- **テスト手順** - この列は、PA-DSS 要件を満たしていることを検証するために、PA-QSA が行うテストプロセスを定義します。
- **ガイダンス** – この列は、各 PA-DSS 要件の意図とセキュリティ目標を定義し、要件の理解に役立つことを意図しています。この列のガイダンスは、PA-DSS 要件およびテスト手順を置き換えたり拡張するものではありません。

注: *コントロールがまだ導入されていないか、将来の日付に完了する予定の場合には、PA-DSS 要件に未対応と見なされます。*

要件1:　　完全なトラックデータ、カード検証コードまたは値（CAV2 、CID 、CVC2 、CVV2 ）、または PIN ブロックデータを保存しない

PA-DSS 要件	テスト手順	ガイダンス
1.1 承認後に機密認証データを保存しない（暗号化されている場合でも）： 機密認証データを受け取った場合、認証プロセスが完了し次第すべてのデータを復元不可能にする。 機密認証データには、以降の要件 1.1.1 ～ 1.1.3 で言及されているデータを含む。 ***PCI DSS 要件 3.2 に対応***	**1.1.a** このペイメントアプリケーションで、機密認証データが保存される場合は、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のためだけに意図されたものであることをを確認します。 **1.1.b** その他のすべてのペイメントアプリケーションでは、機密認証データ（以下の 1.1.1 ～ 1.1.3 を参照）が承認前に保存される場合は、データを安全に削除する方法を入手してレビューし、データが回復不能であることを確認します。 .	機密認証データは、フルトラックデータ、カード検証コードまたは値、PIN データから構成されます。承認後の機密認証データの保存は禁止されています。このデータからペイメントカードを偽造し、不正トランザクションを作成することができるため、このデータは悪意のある者にとって非常に貴重です。 ペイメントカードを発行するか、発行サービスを実施するかサポートする事業体は、発行機能の一部として機密認証データを作成・制御することがよくあります。業務上の理由があり、データが安全に保存される場合は、発行者と企業が、機密認証データを保存するため、発行サービスをサポートすることが可能である。 発行しない事業体では、認証後機密認証データを保存することは許可されず、アプリケーションは、データを回復できないように安全に削除するメカニズムを持つ必要があります。

PA-DSS 要件	テスト手順	ガイダンス
1.1.1 承認後、(カードの裏面やチップ内に含まれる同等のデータにある)磁気ストライプのいかなるトラックのいかなるデータも保存しない。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ます。 ***注:*** *通常の取引過程では、磁気ストライプからの以下のデータ要素を保存する必要が生じる場合があります。* ▪ *アカウント会員名* ▪ *プライマリアカウント番号(PAN)* ▪ *有効期限* ▪ *サービスコード* *リスクを最小限に抑えるため、取引に必要なデータ要素のみを保存する。* ***PCI DSS 要件 3.2.1 に対応***	**1.1.1** ペイメントアプリケーションをインストールし、エラー状況とログエントリを生成することを含め、ペイメントアプリケーションの全機能をシミュレートする多数のトランザクションテストを実施します。フォレンジックツールまたはフォレンジック手法(市販ツール、スクリプトなど)[4]を使用して、ペイメントアプリケーションによって作成されるすべての出力を調べ、カード裏面またはチップ上の同等のデータにある磁気ストライプからいかなるトラックのいかなる内容も承認後に保存されないことを確認します。少なくとも以下の種類のファイル(およびペイメントアプリケーションによって生成されるその他すべての出力)が含まれます。 ▪ 受信トランザクションデータ ▪ すべてのログ(トランザクション、履歴、デバッグ、エラーなど) ▪ 履歴ファイル ▪ トレースファイル ▪ 不揮発性キャッシュを含む、不揮発性メモリ ▪ データベーススキーム ▪ データベースコンテンツ	全トラックデータが保存されると、そのデータを入手した悪意のある者はそのデータを使ってペイメントカードを複製し、不正なトランザクションを行うことができます。

[4] フォレンジックツールまたはフォレンジック手法:
フォレンジックデータを発見、分析、提示するためのツールまたは手法で、コンピュータエビデンスを迅速かつ徹底的に認証、検索、回復するための確実な方法を提供します。PA-QSA が使用するフォレンジックツールまたは手法の場合は、ペイメントアプリケーションが書き込む機密認証データを正確に見つける必要があります。これらのツールは、市販、オープンソース、PA-QSA による社内開発のいずれでもかまいません。

PA-DSS 要件	テスト手順	ガイダンス
1.1.2 承認後、カードを提示しない取引を検証するために使用された、カード検証値またはコード（ペイメントカードの前面または背面に印字されている 3 桁または 4 桁の数字）を保存しない。 ***PCI DSS 要件 3.2.2 に対応***	**1.1.2** ペイメントアプリケーションをインストールし、エラー状況とログエントリを生成することを含め、ペイメントアプリケーションの全機能をシミュレートする多数のトランザクションテストを実施します。フォレンジックツールまたはフォレンジック手法（市販ツール、スクリプトなど） を使用して、ペイメントアプリケーションによって作成されるすべての出力を調べ、カードの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（CVV2、CVC2、CID、CAV2 データ）が承認後に保存されないことを確認します。少なくとも以下の種類のファイル（およびペイメントアプリケーションによって生成されるその他すべての出力）が含まれます。 ▪ 受信トランザクションデータ ▪ すべてのログ（トランザクション、履歴、デバッグ、エラーなど） ▪ 履歴ファイル ▪ トレースファイル ▪ 不揮発性キャッシュを含む、不揮発性メモリ ▪ データベーススキーム ▪ データベースコンテンツ	カード検証コードの目的は、消費者とカードを対面で取引しない、「カードを提示しない」取引（インターネットまたは通信販売（MO/TO）取引）を保護することです。このデータが盗まれた場合、悪意のある者はインターネットおよび MO/TO 取引を偽造できます。
1.1.3 承認後、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。 ***PCI DSS 要件 3.2.3 に対応***	**1.1.3** ペイメントアプリケーションをインストールし、エラー状況とログエントリを生成することを含め、ペイメントアプリケーションの全機能をシミュレートする多数のトランザクションテストを実施します。フォレンジックツールまたはフォレンジック手法（市販ツール、スクリプトなど） を使用して、ペイメントアプリケーションによって作成されるすべての出力を調べ、PIN と暗号化された PIN ブロックが承認後に保存されないことを確認します。少なくとも以下の種類のファイル（およびペイメントアプリケーションによって生成されるその他すべての出力）が含まれます。 ▪ 受信トランザクションデータ ▪ すべてのログ（トランザクション、履歴、デバッグ、エラーなど） ▪ 履歴ファイル ▪ トレースファイル ▪ 不揮発性キャッシュを含む、不揮発性メモリ ▪ データベーススキーム ▪ データベースコンテンツ	これらの値を知っている必要があるのは、カード所有者またはカードを発行した銀行のみです。このデータが盗まれた場合、悪意のある者は PIN ベースの引き落とし取引（ATM での引き出しなど）を偽造することができます。

PA-DSS 要件	テスト手順	ガイダンス
1.1.4 以前のバージョンのペイメントアプリケーションによって保存されるトラックデータ、カード検証値またはコード、PIN または PIN ブロックデータを、たとえば国家安全保障局またはその他の州や国家の標準または規制によって維持管理される承認済み製品のリストで定義されている、安全な削除に関する業界承認の標準に従って安全に削除する。 ***注:*** *この要件は、以前のバージョンのペイメントアプリケーションで機密認証データを保存していた場合にのみ適用されます。* ***PCI DSS 要件 3.2 に対応***	**1.1.4.a** ベンダが準備する『PA-DSS 実装ガイド』に目を通し、文書に顧客とインテグレータ/リセラー向けの以下の指示が含まれていることを確認します。 ▪ 履歴データを削除する必要がある（以前のバージョンのペイメントアプリケーションによって保存されるトラックデータ、カード検証コード、PIN、または PIN ブロック） ▪ 履歴データの削除方法 ▪ このような削除が PCI DSS 準拠のために絶対に必要であること	重要な認証データの全要素は、承認語に保存することを許可されていません。ペイメントアプリケーションの古いバージョンで、この情報を保存した場合、ペイメントアプリケーションベンダは、『PA-DSS実装ガイド』に指示を記載するとともに、安全なワイプツールまたは手順を提供する必要があります。このデータが安全に削除されず、加盟店システムで隠された状態を維持すると、この情報へのアクセスを取得する悪意のある個人が、偽造支払カードを製造したり、不正トランザクションを実行したりするために使用できます。
	1.1.4.b ペイメントアプリケーションソフトウェアのファイルと構成文書を検査し、ベンダがデータを削除するための安全なワイプツールまたは手続きを提供していることを確認します。	
	1.1.4.c フォレンジックツールまたはフォレンジック手法（あるいはその両方）を使用して、ベンダが提供する安全なワイプツールまたはワイプ手続きによって、データの安全な削除に関する業界承認標準に従ってデータが安全に削除されることを確認します。	
1.1.5 ベンダのシステムに機密認証データを保存しない。機密認証データ（承認前のデータ）がデバッグまたはトラブルシューティング目的に使用される場合は、以下のことを確認します。 ▪ 機密認証データは、特定の問題を解決するために必要な場合のみ収集する ▪ このようなデータは、アクセスが限定された特定の既知の場所にのみ保存する ▪ 特定の問題を解決するために必要に応じて限られた量だけ収集する ▪ 機密認証データは保存時に暗号化される ▪ データは、以下の含める保存先から使用後すぐに安全に削除する。 • ログファイル • デバッグファイル	**1.1.5.a** 顧客の問題をトラブルシューティングするための *ソフトウェアベンダ* の手続きを調べ、手続きに以下が含まれていることを確認します。 ▪ 特定の問題を解決するために必要な場合のみ、機密認証データを収集する ▪ このようなデータは、アクセスが限定された特定の既知の場所にのみ保存する ▪ 特定の問題を解決するために必要な限られた量のデータのみを収集する ▪ 保存の際に機密認証データを暗号化する ▪ このようなデータは使用後すぐに安全に削除する	ベンダが（トラブルシューティングやデバッグの目的で）機密認証データの収集につながる可能性のあるサービスを顧客に提供する場合、ベンダは、データの収集を最小限に抑え、安全に取扱、不要になった時点で直ちにかつ安全に削除されたことを確認する必要があります。 問題のトラブルシューティングでアプリケーションを一時的に構成して機密認証データ（SAD）をキャプチャする必要がある場合は、アプリケーションは、必要なデータ取得が完了した時点で、直ちに通常の安全な構成（つまり、SAD の収集を無効にする）に戻される必要があります。 不要になった時点で、SAD は、業界が承認した標準（データを回復できないようにする安全なワイププログラムなど）によって、削除する
	1.1.5.b 顧客から得た最近のトラブルシューティング要求のサンプルを選択し、各イベントが 1.1.5.a で調べた手続きに従っていることを確認します。	

PA-DSS 要件	テスト手順	ガイダンス
• 顧客から受け取ったその他のデータソース。 . ***PCI DSS 要件 3.2 に対応***	**1.1.5.c** ベンダが準備する『PA-DSS 実装ガイド』に目を通し、文書に顧客とインテグレータ/リセラー向けの以下の指示が含まれていることを確認します。 ▪ 特定の問題を解決するために必要な場合のみ、機密認証データを収集する。 ▪ このようなデータは、アクセスが限定された特定の既知の場所にのみ保存する。 ▪ 特定の問題を解決するために必要な限られた量のデータのみを収集する。 ▪ 保存の際に機密認証データを暗号化する。 ▪ このようなデータは使用後すぐに安全に削除する。	必要があります。

要件2:　　保存されるカード会員データを保護する

PA-DSS 要件	テスト手順	ガイダンス
2.1 ソフトウェアベンダは、顧客が定義した保存期間が過ぎた後のカード会員データの安全な削除に関するガイダンスを顧客に提供する必要がある。 ***PCI DSS 要件 3.1 に対応***	**2.1** ベンダが準備する『PA-DSS 実装ガイド』に目を通し、文書に顧客とインテグレータ/リセラー向けの以下のガイダンスが含まれていることを確認する。 ▪ 顧客が定義した保存期間を過ぎたカード会員データは安全に削除する必要がある ▪ ペイメントアプリケーションがカード会員データを保存するすべての場所の一覧（削除する必要があるデータの場所を顧客が認識できるようにするため） ▪ 顧客が、法律上、規制上、または業務上の理由で不要になったカード会員データの安全な削除を行う必要があるという指示 ▪ 基盤ソフトウェアまたはシステム（OS やデータベースなど）でのデータ保存を含め、ペイメントアプリケーションで保存されるカード会員データを安全に削除する方法に関する指示 ▪ 基盤ソフトウェアまたはシステム（OS やデータベースなど）を構成し、システムのバックアップや回復ポイントなど、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ことに関する指示。	PCI DSS 要件 3.1 をサポートするために、ベンダがペイメントアプリケーションが基盤ソフトウェアまたはシステム（OSやデータベースなど）などに、カード会員データを保存するすべての場所の詳細を提供しなければならないだけでなく、データが顧客の定義された保存期間を超えた時点で、データを安全に削除するための指示の詳細を提供する必要があります。 顧客およびインテグレータ/リセラーは、これらの基盤システムが、顧客の知識なしに、カード会員データをキャプチャしないように、アプリケーションが実行される基盤システムおよびソフトウェアの構成詳細を提供される必要があります。顧客は、データがキャプチャされることを防ぎ、正しく保護されるよう、基盤システムがアプリケーションからデータをキャプチャする方法について知る必要があります。
2.2 表示時に PAN をマスクして（最初の 6 桁と最後の 4 桁が最大表示桁数）、業務上の正当な必要性がある関係者だけが PAN 全体を見ることができるようにする。 ***注:*** ▪ *カード会員データの表示（法律上、またはペイメントカードブランドによる POS レシート要件など）に関するこれより厳しい要件がある場合は、その要件より優先されることはありません。* ***PCI DSS 要件 3.3 に対応***	**2.2a** ベンダが準備する『PA-DSS 実装ガイド』に目を通し、文書に顧客とインテグレータ/リセラー向けの以下のガイダンスが含まれていることを確認する。 ▪ POS デバイス、画面、ログ、および領収書を含むがこれらに限定されない、PAN が表示されるすべてのインスタンスの詳細。 ▪ ペイメントアプリケーションがすべてのディスプレイにおいて、デフォルトで PAN をマスクすることを確認する。 ▪ 業務上の合法的な必要性により PAN 全体を見る必要がある担当者のみが PAN 全体を表示することができるようにペイメントアプリケーションを構成する方法に関する指示。	コンピュータ画面、ペイメントカードの領収書、FAX、または紙の計算書などのアイテムに PAN 全体が表示されると、このデータが権限のない人々によって取得され、不正に使用される可能性があります。 この要件は画面や紙の領収書などに表示された PAN の保護に関連します。ファイルやデータベースなどに保存された PAN の保護に関する要件 2.3 と混同しないよう注意してください。

PA-DSS 要件	テスト手順	ガイダンス
	2.2.b ペイメントアプリケーションをインストールし、POS デバイス、画面、ログ、および領収書を含むがこれらに限定されない、PAN のすべての表示を検査する。PAN が表示されるインスタンスごとに、表示されたときに PAN がマスクされていることを確認します。	
	2.2.c 業務上の合法的な必要性を持つ担当者のみに完全な PAN が表示されるよう、『PA-DSS実装ガイド』に従ってペイメントアプリケーションを構成する。PAN が表示される各インスタンスでは、アプリケーションの構成と PAN の表示を検査し、PAN が正確で業務上の合法的な必要性を持つ担当者のみに完全な PAN が表示されるよう、その指示を確認する。	
2.3 以下の手法を使用して、すべての保存場所で PAN を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、ログのデータを含む）。 ▪ 強力な暗号化をベースにしたワンウェイハッシュ（PAN全体をハッシュする必要がある） ▪ トランケーション（PAN の切り捨てられたセグメントの置き換えにはハッシュを使用できない） ▪ インデックストークンとパッド（パッドは安全に保存する必要がある） ▪ 関連するキー管理プロセスおよび手順を伴う、強力な暗号化 ***注:*** ▪ *悪意のある個人がトランケーションされた PAN とハッシュ化された PAN の両方を取得した場合、元の PAN を比較的容易に再現することができる。ペイメントアプリケーションで生成したものと同じ PAN をハッシュ化したものとトランケーションしたものがある場合、追加のコントロールを実施し、ハッシュ化した PAN とトランケーションした PAN を相関付けて元の PAN を再現することができないようになっていることを確認する必要がある。* ▪ *ペイメントアプリケーションの外部であろうと、すべての*	**2.3a** ベンダが準備する『PA-DSS実装ガイド』に目を通し、文書に顧客とインテグレータ/リセラー向けの以下のガイダンスが含まれていることを確認する。 ▪ カード会員データを読み取り不能にするためにアプリケーションによって使用される各方法の設定可能なオプションの詳細、およびカード会員データが、（PA-DSS 要件 2.1 により）ペイメントアプリケーションで保存されるすべての場所で、各方法を設定する方法に関する指示。 ▪ カード会員データが、ペイメントアプリケーション外で保管する加盟店用に出力されるすべてのインスタンスのリスト、および加盟店がそのようなインスタンスで PAN を読み取り不能にする責任があることを説明する指示。	PAN の保護が不十分だと、悪意のある人々がこのデータを表示またはダウンロードできる可能性があります。 強力な暗号化技術をベースにしたワンウェイハッシュ関数を使用して、カード会員データを読み取り不能にすることができます。ハッシュ関数は元の数値を取得する必要がない場合に適しています（ワンウェイハッシュは復元できません）。 トランケーションの目的は、PAN の一部のみ（最初の 6 桁と最後の 4 桁を超えないようにする）を保存することです。 インデックストークンは、指定のインデックスをベースに PAN を予測不能な値に置き換える暗号トークンです。ワンタイムパッドは、ランダム生成の秘密キーを 1 回だけ使用してメッセージを暗号化するシステムです。暗号化されたメッセージは、一致するワンタイムパッドとキーを使用して復号化されます。 強力な暗号化技術（*『PCI DSS とPA-DSS の用語集（用語、略語、および頭字語）』*で定義）の目的は、暗号化のベースを強力な暗号化キーを持つ、（専用または「自家製」のアルゴリズムではなく）業界がテスト済みの認められたアルゴリズムにすることです。 悪意のある個人は、特定の PAN
	2.3.b 暗号化アルゴリズム（該当する場合）など、PAN の保護に使用されている方法を調査する。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。 ▪ 強力な暗号化技術をベースにしたワンウェイハッシュ ▪ トランケーション ▪ インデックストークンとパッド（パッドは安全に保存する必要がある） ▪ 関連するキー管理プロセスおよび手順を伴う、強力な暗号化	
	2.3.c アプリケーションで作成または生成されたデータリポジトリ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。	

PA-DSS 要件	テスト手順	ガイダンス
保存場所で PAN を読み取り不能にする必要がある（加盟店環境で保管するために、アプリケーションによって出力されたログファイルなど）。 ***PCI DSS 要件 3.4 に対応***	**2.3.d** アプリケーションの外部で使用するファイル（エクスポートまたはバックアップ用のファイルなど）を作成または生成し、リムーバブルメディアに保存するなどした場合、リムーバブルメディア（バックアップテープなど）に生成したファイルを含めた生成ファイル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。	をハッシュ化したものとトランケーションしたものを相関付けて元の PAN を容易に再現することができます。このデータの相関付けを防ぐコントロールを実施することで、元の PAN を読み取り不能の状態に保つことが可能になります。
	2.3.e アプリケーションで作成または生成した監査ログのサンプルを調査し、PAN が読み取り不能になっているか、ログから削除されていることを確認する。	
	2.3.f ソフトウェアベンダが何からの理由（ログファイル、デバッグファイル、その他のデータソースがデバッグまたはトラブルシューティング目的で顧客から受信されるため、など）で PAN を保存する場合は、PAN が前述の要件 2.3.a ～ 2.3.d に従い、読み取り不能になっていることを確認する。	
2.4 ペイメントアプリケーションは、カード会員データのセキュリティ保護に使用されるキーを開示や誤使用から保護する必要がある。 ***注:*** *この要件は、保存されているカード会員データを暗号化するキーに適用され、またデータ暗号化キーの保護に使用するキー暗号化キーにも適用されます。つまり、キー暗号化キーは、少なくともデータ暗号化キーと同じ強度を持つ必要があります。* ***PCI DSS 要件 3.5 に対応***		暗号化キーへのアクセスを取得するとデータを複合化できるため、暗号化キーは厳重に保護する必要があります。 キーを開示と誤使用から保護するためのペイメントアプリケーションの要件は、データ暗号化キーとキー暗号化キーの両方に適用されます。 暗号化キーにアクセスできる人物はごく少数にする必要があります（通常、キー管理者のみ）。
	2.4.a 製品のドキュメントに目を通し、責任者にインタビューすることにより、アプリケーションによって使用される暗号化キーへのアクセスが制限される制御が導入されていることを確認する。	
	2.4.b システム構成ファイルを調べて、以下のことを確認する。 ▪ キーが暗号化された形式で保存されている ▪ キー暗号化キーがデータ暗号化キーとは別に保存されている ▪ キー暗号化キーが少なくとも保護対象データの暗号化キーと同じ強度を持つ	

PA-DSS 要件	テスト手順	ガイダンス
	2.4.c ベンダが準備する『PA-DSS 実装ガイド』に目を通し、顧客とリセラー/インテグレータ向けに以下の指示が含まれていることを確認する。 ▪ キーへのアクセスを、必要最小限の管理者に制限する。 ▪ キーの保存場所と形式を最小限にし、安全に保存する。	
2.5 ペイメントアプリケーションは、カード会員データの暗号化に使用される暗号化キーに対して、少なくとも次の要件に従ってキー管理プロセスと手続きを実装する必要がある。 ***PCI DSS 要件 3.6 に対応***	**2.5.a** ベンダが準備する『PA-DSS 実装ガイド』に目を通し、文書に顧客とインテグレータ/リセラー向けの以下の指示が含まれていることを確認する。 ▪ 顧客またはインテグレータ/リセラーがキー管理作業に関わっている場合に暗号化キーの生成、配布、保護、変更、保存、破棄/取替を安全に行う方法。 ▪ キー管理者が自身のキー管理の責務を理解して受諾したことを確認するためのサンプルのキー管理フォーム。 ▪	暗号化キーの管理方法は、ペイメントアプリケーションのセキュリティを継続させるための重要な要素です。適切なキー管理プロセスは、手動、または暗号化製品の一部として自動化されている場合のいずれも、業界標準に基づき、すべてのキー要素を 2.5.1 ～ 2.5.7 に対応させます。 顧客に暗号化キーを安全に送信、保存、更新するためのガイダンスを提供することは、キーの管理上のミスや無許可の事業体への開示の防止に役立ちます。 この要件は、保存されたカード会員データの暗号化に使用するキーおよび個々のキー暗号化キーを適用対象とします。
2.5.1 強力な暗号化キーの生成	**2.5.1.a** 『PA-DSS 実装ガイド』に目を通し、文書に顧客とインテグレータ/リセラー向けに、暗号化キーを安全に生成する方法に関する指示が含まれていることを確認する。	ペイメントアプリケーションは、『PCI DSS と PA-DSS の用語集（用語、略語、および頭字語）』の「強力な暗号化技術」に定義されている強力なキーを生成する必要があります。
	2.5.1.b 暗号化キーを生成するために使用される方法を含め、アプリケーションをテストし、『PA-DSS 実装ガイド』の指示が強力な暗号化キーを生成する結果に至ることを確認する。	
2.5.2 安全な暗号化キーの配布	**2.5.2.a** 『PA-DSS 実装ガイド』に目を通し、文書に顧客とインテグレータ/リセラー向けに、暗号化キーを安全に配布する方法に関する指示が含まれていることを確認する。	ペイメントアプリケーションは、キーを安全に配布する必要があります。つまり、キーを平文で配布せず、承認されたプロセスによってのみ配布することを意味します。
	2.5.2.b 暗号化キーを配布するために使用される方法を含め、アプリケーションをテストし、『PA-DSS 実装ガイド』の指示が暗号化キーを安全に配布する結果に至ることを確認する。	

PA-DSS 要件	テスト手順	ガイダンス
2.5.3 安全な暗号化キーの保存	**2.5.3.a** 『PA-DSS 実装ガイド』に目を通し、文書に顧客とインテグレータ/リセラー向けに、暗号化キーを安全に保管する方法に関する指示が含まれていることを確認する。	ペイメントアプリケーションは、キーを安全に保存する必要があります（キー暗号化キーで暗号化するなど）。
	2.5.3.b 暗号化キーを保管するために使用される方法を含め、アプリケーションをテストし、『PA-DSS 実装ガイド』の指示が暗号化キーを安全に保管する結果に至ることを確認する。	
2.5.4 関連アプリケーションベンダまたはキーオーナーが定義し、業界のベストプラクティスおよびガイドライン（たとえば、NIST Special Publication 800-57）に基づいた、暗号化期間の終了時点に到達したキーの暗号化キーの変更。暗号化期間の終了時点とは、たとえば、定義された期間が経過した後、または付与されたキーで一定量の暗号化テキストを作成した後（またはその両方）である。	**2.5.4.a** 『PA-DSS 実装ガイド』に目を通し、文書に顧客とインテグレータ/リセラー向けの以下の指示が含まれていることを確認する。 • アプリケーションによって使用される各キーの種類に対して定義される暗号化期間 • 定義された暗号化期間の最後で、キーの変更を強制する手順	暗号化期間とは、定義された目的で特定の暗号化キーを使用できる期間のことです。暗号化期間を定義する場合には、基盤アルゴリズムの強度、キーのサイズまたは長さ、キーが危険にさらされるリスク、暗号化するデータの機密性などを考慮する必要があります。 キーの暗号化期間の終わりに暗号化キーの定期的な変更を行うことは、暗号化キーが取得され、データが復号化されるリスクを最小限に抑えるために必須です。
	2.5.4.b 暗号化キーを変更するための方法を含め、アプリケーションをテストし、『PA-DSS 実装ガイド』の指示が定義された暗号期間の終わりにキーが変更される結果に至ることを確認する。 .	
2.5.5 キーの完全性が弱くなったとき（たとえば、平文のキーの情報を持つ従業員が業務から離れる場合）またはキーが危険にさらされている疑いがあるときに必要とみなされる、キーの破棄または取替（アーカイブ、廃棄、廃止など）。 ***注:*** *破棄された、または取り替えられた暗号化キーを保持する必要がある場合、そのキーを（たとえば、キー暗号化キーを使用することにより）安全にアーカイブする必要がある。アーカイブされた暗号化キーは、復号化または検証にのみ使用される。*	**2.5.5.a** 『PA-DSS 実装ガイド』に目を通し、文書に顧客とインテグレータ/リセラー向けの以下の内容が含まれていることを確認する。 • キーの整合性が脆弱になった場合、またはキーの悪用が存在するまたは疑われる場合に、キーが破棄または取り替えられるための指示。 • キーの破棄や取り替えの手順（アーカイブ、廃棄、廃止など）。 • 破棄または取り替えられた暗号化キーが、暗号化操作に使用されていないことを確認する手順。	使われなくなった、または不要になったキー、および脆弱であることがわかっているまたは疑われるキーは、破棄するか破壊して使用できないようにする必要があります。（アーカイブされた暗号化データをサポートするなどのために）そのようなキーを保管しておく必要がある場合は、厳重に保護する必要があります。 ペイメントアプリケーションでは、侵害されたことがわかっている、またはその疑いがあるキーを取り替えるプロセスを提供し、使いやすくする必要があります。
	2.5.5.b 暗号化キーを破棄する、または取り替える方法を含め、アプリケーションをテストし、『PA-DSS 実装ガイド』の指示が暗号化キーの破棄または取り替えに至る（アーカイブ、廃棄、廃止など）ことを確認する。 .	

PA-DSS 要件	テスト手順	ガイダンス
	2.5.5.c 破棄された/取り替えられた暗号化キーをテストし、『PA-DSS 実装ガイド』の指示により、アプリケーションが、暗号化操作に破棄または取り替えられたキーを使用しないことを確認する。	
2.5.6 ペイメントアプリケーションが手動での平文暗号化キー管理の操作をサポートする場合、キーの知識分割と二重管理を使用する必要がある。 **注:** 手動のキー管理操作の例には、キーの生成、伝送、読み込み、保存、破棄などが含まれますが、これらに限定されません。	**2.5.6.a** 『PA-DSS 実装ガイド』に目を通し、文書に顧客とインテグレータ/リセラー向けの以下の内容が含まれていることを確認する。 • アプリケーションによってサポートされている手動クリアテキスト暗号化キー管理操作の詳細 • そのような操作に関する知識分割と二重管理の指示 **2.5.6.b** すべての手動の平文暗号化キー管理操作を含め、アプリケーションをテストし、『PA-DSS 実装ガイド』の指示が、すべての手動の平文暗号化キー管理手順に必要なキーの知識分割と二重管理に至ることを確認する。	キー知識の分割と二重管理は、1 人の人物がキー全体にアクセスできる可能性を排除するために使用されます。この管理は、手動キー管理操作に適用されます。 キー知識分割方法では、2 人以上が別々にキーコンポーネントを持っており、個々の知識では暗号化キーを生成できないようにした状態を指します。各人は、自分のキーコンポーネントしか知っておらず、各キーコンポーネントは元の暗号化キーの知識を伝えません。 二重管理では、2 人以上が 1 つの機能を実行し、どの 1 人も他方の認証情報にアクセスも使用もできなくなっています。
2.5.7 暗号化キーの不正置換の防止	**2.5.7.a** 『PA-DSS 実装ガイド』に目を通し、文書に顧客とインテグレータ/リセラー向けに、暗号化キーの不正な置換を防ぐ方法に関する指示が含まれていることを確認する。 **2.5.7.b** 暗号化キーを置換するすべての方法を含め、アプリケーションをテストし、『PA-DSS 実装ガイド』の指示が暗号化キーの不正な置換を防ぐ結果に至ることを確認する。.	ペイメントアプリケーションは、許可されたキーの置換のみを行うことができるように、アプリケーションのユーザー用の方法を定義する必要があります。アプリケーション構成には、不正なソースまたは予期しないプロセスからのキーの置換を許可するものを含めてはいけません。
2.6 ペイメントアプリケーションによって保存された暗号化キー要素または暗号文を業界が承認した標準に従って取得不能にするメカニズムを提供する。 これらは、カード会員データを暗号化または確認するために使用される暗号化キーである。 ***注:*** *この要件は、ペイメントアプリケーションまたは以前のバージョンのペイメントアプリケーションで、カード会員データの暗号化に暗号化キー要素または暗号文が使用されていた*	**2.6.a** ベンダが準備する『PA-DSS 実装ガイド』に目を通し、文書に顧客とインテグレータ/リセラー向けの以下の指示が含まれていることを確認する。 ▪ 暗号化要素を取得不能にするためにアプリケーションに提供されているツールまたは手続きを使用する詳細な手順 ▪ キーが使用されなくなった時に、PCI DSS のキー管理要件に従って、暗号化キーの要素を取得不能にすること ▪ 復号/再暗号化プロセスの間に、クリアテキストデータのセキュリティを維持するための手順を含め、新しいキーで履歴データの再暗号化を行う手順	ベンダは、顧客が必要としなくなった場合に、顧客が古い暗号化要素を削除することができるよう、メカニズムを提供する必要があります。古い暗号化要素の削除は、顧客の裁量であることに注意してください。 暗号化キー要素および暗号文、またはそのいずれかを取得不能にするために使用できるツールまたはプロセスの例として以下があります。 - 国家安全保障局またはその他の州や国家の標準または規制によって維持管理される承認済み製品のリストなどで定義されている安全な削除。 - 残りのデータ暗号化キーがすべて削除した KEK

PA-DSS 要件	テスト手順	ガイダンス
場合にのみ適用されます。 ***PCI DSS 要件 3.6 に対応***	**2.6.b** 最終的なアプリケーション製品を検査し、ベンダが暗号化要素を取得不能にするためのツールまたは手続きを提供していることを確認する。	の形式で暗号化されている場合のキー暗号化キー（KEK）の削除。
	2.6.c 暗号化キーの要素が取得不能になるように提供されている方法を含め、アプリケーションをテストする。フォレンジックツールまたはフォレンジック手法（あるいはその両方）を使用して、ベンダによって提供されている安全なワイプツールまたはワイプ手続きによって、業界承認標準に従って暗号化要素が取得不能になることを確認します。	
	2.6.d 新しいキーで履歴データを再暗号化する方法をテストし、『PA-DSS 実装ガイド』の指示が新しいキーで履歴データが再暗号化される結果に至ることを確認する。	

要件 3:　　安全な認証機能の提供

PA-DSS 要件	テスト手順	ガイダンス
3.1 ペイメントアプリケーションでは、すべての管理アクセスおよびカード会員データへのアクセスに一意のユーザ ID と安全な認証の使用をサポートおよび適用する必要がある。安全な認証は、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。 アプリケーションは、以下の 3.1.1 から 3.1.11 を強制する必要があります。 ***注:*** *要件 3* *全体で使用される「インストール後の変更」とは、ユーザアカウントをデフォルト設定に戻したことによるアプリケーションのあらゆる変更、既存のアカウント設定のあらゆる変更、新規アカウントの生成または既存アカウントの再作成をもたらす変更などがあります。* ***注:*** *これらのパスワード管理は、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担当者に適用することを意図したものではありません。これらの管理は、管理機能を持つ担当者によるアクセス、カード会員データを含むシステムへのアクセス、ペイメントアプリケーションによって制御されるアクセスに適用されます。* *この要件は、カード会員データを表示またはアクセスするために使用されるペイメントアプリケーションとすべての関連ツールに適用されます。* ***PCI DSS 要件 8.1 および 8.2 に対応***	**3.1.a** ベンダが準備する『PA-DSS 実装ガイド』に目を通し、顧客とリセラー/インテグレータが以下に当てはまることを確認する。 ▪ ペイメントアプリケーションが、次の手順によって生成される強力な認証をすべての認証資格情報に適用する方法について、明確かつ正確な指示を提供する。 - 要件 3.1.1 ～ 3.1.11 に従って、インストールの完了時に、認証資格情報に安全な変更を適用する。 - 要件 3.1.1 ～ 3.1.11 に従って、インストール後に変更があるたびに、認証資格情報に安全な変更を適用する。 ▪ PCI DSS の準拠を維持するため、認証設定に加えた変更は、少なくとも PCI DSS の要件と同程度に厳格である認証方法を提供するものとして検証する必要がある。 ▪ すべてのデフォルトアカウントに安全な認証を割り当ててから（使用しない場合でも）、アカウントを無効にするか使用しないことを推奨する。 ▪ ペイメントアプリケーションによって使用されるすべての認証資格情報（ただし、アプリケーションによる生成や管理は行わない）について、明確かつ正確な指示を提供する場合、後述の要件 3.1.1 ～ 3.1.11 に従ってインストールの完了時およびインストール後の変更時に管理アクセス権限を持つすべてのアプリケーションレベルのアカウントとカード会員データへのすべてのアクセスに関して認証資格情報を変更し、強力な認証を作成する方法について明確な指針を示している。	複数の従業員が 1 つの ID を使用するのではなく、各ユーザが一意に識別されるようにすることで、アプリケーションは PCI DSS の要件をサポートし、アクションに対する個人の責任と従業員ごとの有効な監査証跡を保持することができます。これは、誤使用や悪意のある意図が発生した場合に、問題を迅速に解決および抑制するのに役立ちます。 安全な認証を一意の ID に加えて使用すると、侵害を試みようとする人物は一意の ID に加えてパスワード（またはその他の認証アイテム）を知る必要があるため、ユーザの ID が侵害されるのを防ぐことができます。

PA-DSS 要件	テスト手順	ガイダンス
3.1.1 ペイメントアプリケーションは、他の必要なソフトウェアに対してデフォルトの管理アカウントを使用しない（または使用を要求しない）ことを確認する（たとえば、ペイメントアプリケーションはデータベースのデフォルト管理アカウントを使用してはいけません）。 ***PCI DSS 要件 2.1 に対応***	**3.1.1** すべての必要なソフトウェアのための管理アカウントを設定を含め、『PA-DSS 実装ガイド』に従い、ペイメントアプリケーションをインストールおよび構成する。ペイメントアプリケーションをテストして、ペイメントアプリケーションが他の必要なソフトウェアに対してデフォルトの管理アカウントを使用しない（または使用を要求しない）ことを確認します。	デフォルトの管理アカウント（とパスワード）は公共知識であり、ペイメントアプリケーションまたは基盤のシステムコンポーネントに精通している全員に知られています。デフォルトの管理アカウントとパスワードを使用すると、許可されていない個人が、公的に知られている認証情報でログインし、アプリケーションとデータへのアクセスを得ることができる場合があります。
3.1.2 アプリケーションは、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で、デフォルトの全アプリケーションパスワードの変更を強制する必要がある。 これは、ユーザアカウント、アプリケーション、サービスアカウント、サポート目的のためにベンダによって使用されるアカウントを含むすべてのアカウントに適用されます。 ***注:*** *この要件は、ユーザプロセスの指定、または『PA-DSS 実装ガイド』の指示によって満たすことはできません。インストールの完了およびその後の変更時に、アプリケーションは、デフォルトのパスワードが変更されるまで、デフォルトまたは内蔵のアカウントが技術的に使用されてないようにする必要があります。* ***PCI DSS 要件 2.1 に対応***	**3.1.2** アプリケーションで生成または管理されるすべてのアカウントについては、以下のようにアプリケーションをテストする。	アプリケーションがデフォルトパスワードの変更を強制しない場合は、アプリケーションがデフォルトの設定に精通する人物により、不正アクセスされる可能性があります。
	3.1.2.a 『PA-DSS 実装ガイド』に従ってアプリケーションをインストールし、アカウントとパスワード設定を検査する。さらに、すべてのデフォルトパスワードを使用して、インストールプロセスの完了時までに、デフォルトのペイメントアプリケーションのパスワードが変更されることを確認する。	
	3.1.2.b ユーザアカウントがデフォルト設定に戻る、既存アカウント設定が変更される、新しいアカウントが生成される、既存アカウントが再作成されるすべてのアプリケーション機能をテストする。 実行される、あらゆる種類の変更について、アカウントおよびパスワードの設定を検査し、すべてのデフォルトのパスワードを使用して、アプリケーションが変更の完了時に、デフォルトのパスワードをすべて変更するよう強制することを確認する。	
3.1.3 ペイメントアプリケーションは、ユーザアカウントに一意のID を割り当てる。 ***PCI DSS 要件 8.1.1 に対応***	**3.1.3** アプリケーションで生成または管理されるすべてのアカウントについては、以下のようにアプリケーションをテストする。	各ユーザに一意のユーザ ID が割り当てられている場合、ペイメントアプリケーションへのアクセスと活動は、それらを実行する個人にまで遡ることができる。
	3.1.3.a 『PA-DSS 実装ガイド』に従ってペイメントアプリケーションをインストールし、同じユーザ ID を使用して異なるアプリケーションアカウントの作成を試み、ペイメントアプリケーションがインストールプロセスの完了時に、一意のユーザ ID のみを割り当てることを確認する。	

PA-DSS 要件	テスト手順	ガイダンス
	3.1.3.b ユーザアカウントがデフォルト設定に戻る、既存アカウント設定が変更される、新しいアカウントが生成される、既存アカウントが再作成されるすべてのアプリケーション機能をテストする。 実行される、あらゆる種類の変更について、アカウントの設定を検査してアプリケーションの機能をテストし、変更の完了時に、すべてのアカウントに一意のユーザ ID が割り当てられていることを確認します。	
3.1.4 ペイメントアプリケーションは、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。 ▪ ユーザが知っていること（パスワードやパスフレーズなど） ▪ トークンデバイスやスマートカードなど、ユーザが所有しているもの ▪ ユーザ自身を示すもの（生体認証など） ***PCI DSS 要件 8.2 に対応***	**3.1.4** アプリケーションで生成または管理されるすべてのアカウントについては、以下のようにアプリケーションをテストする。	これらの認証方法を一意の ID に加えて使用すると、侵害を試みようとする人物は一意の ID に加えてパスワード（またはその他の認証アイテム）を知る必要があるため、ユーザの ID が侵害されるのを防ぐことができます。
	3.1.4.a『PA-DSS 実装ガイド』に従ってペイメントアプリケーションをインストールし、認証方法をテストして、アプリケーションが、インストールプロセスの完了時に、すべてのアカウントに対して、少なくとも 1 つの定義済み認証方法を必要とすることを確認する。	
	3.1.4.b ユーザアカウントがデフォルト設定に戻る、既存アカウント設定が変更される、新しいアカウントが生成される、既存アカウントが再作成されるすべてのアプリケーション機能をテストする。 実行される、あらゆる種類の変更について、認証方法をテストして、アプリケーションが、変更の完了時に、すべてのアカウントに対して、少なくとも 1 つの定義済み認証方法を必要とすることを確認する。	
3.1.5 ペイメントアプリケーションは、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要求または使用しない。 ***PCI DSS 要件 8.5 に対応***	**3.1.5** アプリケーションで生成または管理されるアカウントについては、以下に従ってアプリケーションをテストする。	複数のユーザが同じ認証資格情報（アカウントとパスワードなど）を共有すると、個人のアクションに責任を割り当てたり、アクションの有効なログを記録したりすることができなくなります。アクションを実行したユーザが、認証資格情報を知っているのが誰であるかを特定できないためです。
	3.1.5.a『PA-DSS 実装ガイド』に従ってペイメントアプリケーションをインストールしてアプリケーションの機能をテストし、インストールプロセスの完了時に、アプリケーションがグループ、共有、または汎用のアカウントおよびパスワードを要求または使用しないことを確認する。	
	3.1.5.b ユーザアカウントがデフォルト設定に戻る、既存アカウント設定が変更される、新しいアカウントが生成される、既存アカウントが再作成されるすべてのアプリケーション機能をテストする。 実行される、あらゆる種類の変更について、アカウントの設定を検査してアプリケーションの機能をテストし、変更の完了時に、アプリケーションがグループ、共有、または汎用のアカウントおよびパスワードに依存または使用しないことを確認します。	

PA-DSS 要件	テスト手順	ガイダンス
3.1.6 ペイメントアプリケーションは、以下を満たすパスワードを要求する。 • パスワードに 7 文字以上が含まれることが必要 • 数字と英文字の両方を含む あるいは、上記のパラメータに等しい複雑さと強度を持つパスワード/パスフレーズ	**3.1.6** アプリケーションで生成または管理されるすべてのアカウントについては、以下のようにアプリケーションをテストする。	悪意のある人々は、アプリケーションやシステムにアクセスするため、最初に弱いパスワードを持つ、またはパスワードが存在しないアカウントを見つけようとします。パスワードが短くて推測しやすい場合、悪意のある者がこれらの脆弱なアカウントを見つけ、有効なユーザ ID を装ってアプリケーションやシステムを侵害することは比較的簡単です。 この要件は、パスワードに 7 文字以上の数字と英字を両方含むことを指定しています。技術的な制限上、この最小限を満たせない場合、事業体は「等価強度」を使用してその代替値を評価します。NIST SP 800-63-1 では、エントロピーは「パスワードまたはキーを推定または決定する難易度」として定義されています。パスワードの異なる最小形式について、パスワードエントロピーの値や等価強度の詳細情報は、この文書またはその他の文書で参照できます
	3.1.6.a 『PA-DSS 実装ガイド』に従ってペイメントアプリケーションをインストールしてアプリケーションの機能をテストし、インストールプロセスの完了時に、アプリケーションが以下の複雑性と強度を最小限要求するパスワードを必要とすることを確認する。 • パスワードに 7 文字以上が含まれる • 数字と英文字の両方を含む	
	3.1.6.b ユーザアカウントがデフォルト設定に戻る、既存アカウント設定が変更される、新しいアカウントが生成される、既存アカウントが再作成されるすべてのアプリケーション機能をテストする。 実行される、あらゆる種類の変更について、アカウントの設定を検査してアプリケーションの機能をテストし、変更の完了時に、アプリケーションが以下の複雑性と強度を最小限要求するパスワードを必要とすることを確認します。 • パスワードに 7 文字以上が含まれる • 数字と英文字の両方を含む	

PA-DSS 要件	テスト手順	ガイダンス
	3.1.6.c アプリケーションがパスワードで異なる最小の文字セットと長さを使用する場合は、アプリケーションに必要なパスワードのエントロピーを計算し、上記で指定したパラメータと少なくとも同等であること（つまり、数字およびアルファベット文字の 7 文字と同じ程度に強力である）を確認する。	。
3.1.7 ペイメントアプリケーションは、少なくとも 90 日ごとにユーザパスワードの変更を要求する。 ***PCI DSS 要件 8.2.4 に対応***	**3.1.7** アプリケーションで生成または管理されるすべてのアカウントについては、以下のようにアプリケーションをテストする。	長期間変更されずに有効なままになっているパスワード/パスフレーズは、悪意のある者がパスワード/パスフレーズを解読する行為により長い時間を与えることになります。
	3.1.7.a『PA-DSS 実装ガイド』に従ってペイメントアプリケーションをインストールしてアプリケーションの機能をテストし、インストールプロセスの完了時に、アプリケーションが、少なくとも 90 日ごとにユーザパスワードの変更を要求することを確認する。	
	3.1.7.b ユーザアカウントがデフォルト設定に戻る、既存アカウント設定が変更される、新しいアカウントが生成される、既存アカウントが再作成されるすべてのアプリケーション機能をテストする。 実行される、あらゆる種類の変更について、アカウントの設定を検査してアプリケーションの機能をテストし、変更の完了時に、アプリケーションが、少なくとも 90 日ごとにユーザパスワードの変更を必要とすることを確認します。	
3.1.8 ペイメントアプリケーションは、パスワードの履歴を保持し、新しいパスワードには最後に使用した 4 つのパスワードと異なるものを使用することを要求する。 ***PCI DSS 要件 8.2.5 に対応***	**3.1.8** アプリケーションで生成または管理されるすべてのアカウントについては、以下のようにアプリケーションをテストする。	パスワード履歴が保持されていない場合、以前のパスワードが何度も再使用されることがあるため、パスワードを変更することの効果が低減します。一定期間ほどパスワードを再使用できないことを要求することで、推定されたか総当たり攻撃で見つけられたパスワードが今後使用される可能性が低減されます。
	3.1.8.a『PA-DSS 実装ガイド』に従ってペイメントアプリケーションをインストールしてアカウント設定を検査し、インストールプロセスの完了時に、アプリケーションがパスワードの履歴を保持し、新しいパスワードには最後に使用した 4 つのパスワードと異なるものを使用するよう要求することを確認する。	
	3.1.8.b ユーザアカウントがデフォルト設定に戻る、既存アカウント設定が変更される、新しいアカウントが生成される、既存アカウントが再作成されるすべてのアプリケーション機能をテストする。 実行される、あらゆる種類の変更について、アカウントの設定を検査してアプリケーションの機能をテストし、変更の完了時に、アプリケーションがパスワードの履歴を保持し、新しいパスワードには最後に使用した 4 つのパスワードと異なるものを使用するよう要求することを確認します。	
3.1.9 ペイメントアプリケーションは、最大 6	**3.1.9** アプリケーションで生成または管理されるすべてのアカウントについては、以下の	アカウントロックアウトメカニズムがないと、攻撃者

PA-DSS 要件	テスト手順	ガイダンス
回のログインの試行後にユーザアカウント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。 ***PCI DSS 要件 8.1.6 に対応***	ようにアプリケーションをテストする。	は、手動または自動ツール（パスワード解読ツールなど）を使用し、推測に成功してユーザアカウントへのアクセスを得るまで、継続してパスワードの推測を試みることができます。
	3.1.9.a『PA-DSS 実装ガイド』に従ってペイメントアプリケーションをインストールしてアカウント設定を検査し、インストールプロセスの完了時に、アプリケーションが、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。	
	3.1.9.b ユーザアカウントがデフォルト設定に戻る、既存アカウント設定が変更される、新しいアカウントが生成される、既存アカウントが再作成されるすべてのアプリケーション機能をテストする。 実行される、あらゆる種類の変更について、アカウントの設定を検査してアプリケーションの機能をテストし、変更の完了時に、アプリケーションが、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します。	
3.1.10 ペイメントアプリケーションは、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。 ***PCI DSS 要件 8.1.7 に対応***	**3.1.10** アプリケーションで生成または管理されるすべてのアカウントについては、以下のようにアプリケーションをテストする。	パスワードの推測が絶えず試みられたためにアカウントがロックアウトされる場合、アカウント再有効化の遅延管理により、悪意のある者がこれらのロックされたアカウントのパスワードを継続して推測することを防ぐことができます（アカウントが再有効化されるまで少なくとも 30 分待つ必要があります）。さらに、再有効化を要求する必要がある場合、管理者は、実際にアカウント所有者が再有効化をリクエストしていることを検証できます。
	3.1.10.a『PA-DSS 実装ガイド』に従ってペイメントアプリケーションをインストールしてアカウント設定を検査し、インストールプロセスの完了時に、アプリケーションが、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 を有効にするまでと設定することを確認する。	
	3.1.10.b ユーザアカウントがデフォルト設定に戻る、既存アカウント設定が変更される、新しいアカウントが生成される、既存アカウントが再作成されるすべてのアプリケーション機能をテストする。 実行される、あらゆる種類の変更について、アカウントの設定を検査してアプリケーションの機能をテストし、変更の完了時に、アプリケーションが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 を有効にするまでと設定することを確認します。	
3.1.11 ペイメントアプリケーションは、セッションが 15 分を超えてアイドル状態の場合、セッションを再有効化するためにユーザに再認証を要求する。 ***PCI DSS 要件 8.1.8 に対応***	**3.1.11** アプリケーションで生成または管理されるすべてのアカウントについては、以下のようにアプリケーションをテストする。	ペイメントアプリケーションへのアクセスでオープンなセッションからユーザが離れるとき、その接続がユーザの不在時にその他の者によって使用され、権限のないアカウントアクセスやアカウントの誤使用が発生する可能性があります。
	3.1.11.a『PA-DSS 実装ガイド』に従ってペイメントアプリケーションをインストールしてアカウント設定を検査し、インストールプロセスの完了時に、アプリケーションが、セッションのアイ	

PA-DSS 要件	テスト手順	ガイダンス
	ドルタイムアウトを 15 分以下に設定することを確認する。	
	3.1.11.b ユーザアカウントがデフォルト設定に戻る、既存アカウント設定が変更される、新しいアカウントが生成される、既存アカウントが再作成されるすべてのアプリケーション機能をテストする。 実行される、あらゆる種類の変更について、アカウントの設定を検査してアプリケーションの機能をテストし、変更の完了時に、アプリケーションがセッションのアイドルタイムアウトを 15 分以下に設定することを確認します。	
3.2 ソフトウェアベンダは、ペイメントアプリケーションからPC、サーバ、データベースにアクセスする場合に一意のユーザ ID と安全な認証を必要とすることに関して、顧客にガイダンスを提供する必要がある。 ***PCI DSS 要件 8.1 および 8.2 に対応***	**3.2** ベンダが作成する『PA-DSS 実装ガイド』を調べて、顧客とインテグレータ/リセラーに、一意のユーザ ID とPCI DSS 準拠の安全な認証を使用して、PC、サーバ、データベースへのペイメントアプリケーションアクセスとカード会員データによるアクセスを制御するように指示していることを確認します。	アプリケーションがインストールまたは強力な個人識別と認証コントロールを強制しないシステムによってアクセスされる場合、アプリケーションによって提供される強力な認証をが無視され、安全でないアクセスを招く場合があります。
3.3 送信および保管中に、すべてのペイメントアプリケーションのパスワードを安全にする（ユーザとアプリケーションアカウントのパスワードを含め）。 ***PCI DSS 要件 8.2.1 に対応***	**3.3** 以下の項目を実行する。	ペイメントアプリケーションのパスワードが暗号化なしでネットワークにわたって保存または伝送されると、悪意のある者は、「スニッファー（Sniffer）」を使用してパスワードを伝送中に容易に傍受したり、保存されているファイル内の暗号化されていないパスワードに直接アクセスしたりして、この盗難データを使用して不正にアクセスすることができます。ハッシュアルゴリズムが適用される前に、各パスワードに一意の入力変数を連結させることで、ブルートフォース攻撃の効果を減少させることができます。パスワードをハッシュ化するのに適した強力な一方向暗号アルゴリズムの例には、PBKDF2やbcryptがあります。
3.3.1 伝送中に、すべてのペイメントアプリケーションのパスワードを読み取り不能にする強力な暗号化を使用する。	**3.3.1.a** ベンダの文書とアプリケーション構成を検査し、伝送中にすべてのパスワードが読み取り不能となるよう、強力な暗号化が使用されていることを確認する。	
	3.3.1.b すべてのタイプのアプリケーションパスワードでは、パスワードの伝送（別のシステムからアプリケーションにログインする、アプリケーションを他のシステムに対して認証するなど）を検査し、強力な暗号化によりパスワードが常に読み取り不能にされていることを確認する。	
3.3.2 保管中にすべてのペイメントアプリケーションのパスワードが読み取り不能になるよう、承認された標準に基づき、強力な一方向暗号化アルゴリズムを使用していることを確認する。 各パスワードは、暗号化アルゴリズムが適用される前に	**3.3.2.a** ベンダの文書とアプリケーション構成を検査し、以下のことを確認する。 • 保存されるパスワードは、承認済みの標準に基づく強力で一方向の暗号化アルゴリズムを使用して、読み取り不能にする。 • 暗号化アルゴリズムが適用される前に、一意の入力変数が、各パスワードと連結される。	

PA-DSS 要件	テスト手順	ガイダンス
、パスワードを使用して連結される一意の入力変数を持つ必要があります。 ***注:*** *入力変数は予測不能や秘密にする必要はありません。*	**3.3.2.b** アプリケーションパスワードのすべての種類について、アプリケーション自体、基盤システム、ログファイル、レジストリ設定などで、アプリケーションがパスワードを保存できるすべての場所を特定する。すべての場所とパスワードの種類について、保存されるパスワードファイルを調べ、パスワードが、強力で一方向の暗号化アルゴリズムを使用して、読み取り不能になっていて、保存されるときは常に一意の入力変数を持っていることを確認する。	
3.4 ペイメントアプリケーションは、必要な機能/リソースへのアクセスを制限し、内蔵アカウントで以下のように最低限の権限を強制する必要がある。 • デフォルトで、すべてのアプリケーション/サービスアカウントは、特にアプリケーション/サービスアカウントの目的に必要な機能/リソースのみへのアクセスを持つ • デフォルトで、すべてのアプリケーション/サービスアカウントは、アプリケーション/サービスアカウントで必要な各機能/リソースに割り当てられる最小レベルの権限を持つ ***PCI DSS 要件 7 に対応***	**3.4.a** 『PA-DSS 実装ガイド』に従ってペイメントアプリケーションをインストールし、インストールプロセスの完了時に、以下について内蔵アカウントの設定を調べる。 • すべてのアプリケーション/サービスアカウントは、特にアプリケーション/サービスアカウントの目的に必要な機能/リソースのみへのアクセスを持つ • すべてのアプリケーション/サービスアカウントは、アプリケーション/サービスアカウントで必要な各機能/リソースに割り当てられる最小レベルの権限を持つ **3.4.b** ユーザアカウントがデフォルト設定に戻る、既存アカウント設定が変更される、新しいアカウントが生成される、既存アカウントが再作成されるに至るものを含め、内蔵アカウントへの変更を招くすべてのアプリケーション機能をテストする。 実行される、あらゆる種類の変更について、内蔵アカウントの設定を調べて、アプリケーションの機能をテストし、変更の完了時に以下のことを確認します。 • すべてのアプリケーション/サービスアカウントは、特にアプリケーション/サービスアカウントの目的に必要な機能/リソースのみへのアクセスを持つ • すべてのアプリケーション/サービスアカウントは、アプリケーション/サービスアカウントで必要な各機能/リソースに割り当てられる最小レベルの権限を持つ	このようなアクセスを必要とするアカウントのみに、カード会員データと機密機能へのアクセスを制限するため、アクセスの必要性と必要な権限のレベルは、各内蔵アカウントで定義される必要があります。つまり、割り当てられる機能は実行できるが、不要なその他のアクセスや権限は授与されません。 必要最小限の特権を割り当てることで、アプリケーションについて十分な知識のないユーザが間違って、または知らないでアプリケーションの構成を変更したり、セキュリティ設定を変更することを防止できます。必要最小限の特権を割り当てることはまた、無許可の人物があるユーザ ID にアクセスできた場合の損害範囲を最小限にとどめるためにも役立ちます。

要件 4: ペイメントアプリケーションの動作のログ

PA-DSS 要件	テスト手順	ガイダンス
4.1 インストールプロセスが完了したペイメントアプリケーションのデフォルトの "アウトオブボックス" インストールでは、すべてのユーザアクセスのログが記録され、すべての動作を個々のユーザに関連付けられるようにする必要がある。 ***PCI DSS 要件 10.1 に対応***	**4.1.a** ペイメントアプリケーションをインストールする。アプリケーションをテストし、インストール時に、ペイメントアプリケーションの監査証跡が自動的に有効になっていることを確認する。 **4.1.a** ベンダが作成する『PA-DSS 実装ガイド』を調べて、以下の指示が含まれていることを確認する。 ▪ インストールプロセスの完了時に、ログが設定され、デフォルトで有効にされるようにアプリケーションをインストールする方法 ▪ インストール後、顧客によって構成可能なログオプションについて、後述の PA-DSS 要件 4.2、4.3 および 4.4 に従い、PCI DSS 準拠のログ設定を設定する方法。 ▪ ログの無効化は PCI DSS に準拠しなくなるため行うべきではないこと。 ▪ インストール後、顧客によって構成可能なログオプションについて、ペイメントアプリケーションに付属している、または必要とされるサードパーティのソフトウェアコンポーネントで、PCI DSS 準拠のログ設定を設定する方法。	ペイメントアプリケーションは、ユーザをアクセスしたアプリケーションリソースにリンクし、監査ログを生成するプロセスまたはメカニズムを持ち、疑わしい活動を行ったユーザを特定できる機能を適用することが重要です。インシデント後のフォレンジックチームは、これらのログを頼りに調査を開始します。
4.2 ペイメントアプリケーションでは、次のイベントを再構築するための自動監査証跡を記録する必要がある。 ***PCI DSS 要件 10.2 に対応***	**4.2** ペイメントアプリケーションの監査ログ設定と監査ログ出力を調査してペイメントアプリケーションをテストし、次の事項を実行する。	4.2.1 から 4.2.7 のイベントをログに記録することにより、組織は悪意のある行為の可能性を識別および追跡できます。
4.2.1 ペイメントアプリケーションからカード会員データへのすべての個人アクセス	**4.2.1** ペイメントアプリケーションからの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します。	悪意のある個人が、アプリケーションを通してカード会員データにアクセスできるユーザアカウント情報を取得したり、カード会員データにアクセスするために新しい不正なアカウントを作成する可能性があります。カード会員データへのすべての個人アクセスの記録から、侵害または誤使用されている可能性があるアカウントを識別できます。

PA-DSS 要件	テスト手順	ガイダンス
4.2.2 ペイメントアプリケーションで管理権限が割り当てられた個人によって行われたすべてのアクション	**4.2.2** ペイメントアプリケーションに対する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します。	高い権限を持つ「管理者」などのアカウントは、アプリケーションのセキュリティや本番環境機能に多大な影響を及ぼす可能性があります。実行されたアクティビティのログがなければ、組織は管理者権限の誤使用によって生じた問題を追跡し、原因となる行為や個人を特定することができません。
4.2.3 アプリケーションによって、またはアプリケーション内で管理される監査証跡へのアクセス	**4.2.3** アプリケーションによって、またはアプリケーション内で管理される監査証跡へのアクセスがログ記録されることを確認します。	悪意のある者は、多くの場合、自身の行為を隠すために監査ログの変更を試みます。アクセスの記録があれば、組織はログの矛盾や改ざんの可能性を追跡して個人のアカウントを特定できます。
4.2.4 無効な論理アクセス試行	**4.2.4** 無効な論理アクセス試行が記録されていることを確認する。	悪意のある者は、多くの場合、ターゲットとなるシステムに対する複数のアクセスを試みます。無効なログインが何度も試行された場合、不正ユーザが「総当たり」によるパスワードの推測を試行している可能性があります。
4.2.5 アプリケーションの識別と認証メカニズムの使用および変更（新しいアカウントの作成、特権の上昇などを含むがこれらに限定されない）、およびルートまたは管理者権限を持つアプリケーションアカウントの変更、追加、削除のすべて	**4.2.5** アプリケーションの識別と認証メカニズムの使用（新しいアカウントの作成、特権の上昇などを含むがこれらに限定されない）、およびルートまたは管理者権限を持つアプリケーションアカウントの変更、追加、削除のすべてが記録されることを確認する。	インシデントの発生時点で誰がログオンしていたかがわからなければ、使用された可能性があるアカウントを特定できません。また、悪意のある者が認証をバイパスしたり、有効なアカウントになりすましたりする目的で認証管理の操作を試みる可能性もあります。新規アカウントの作成、権限の昇格、アクセス権限の変更などのアクティビティは、システムの認証メカニズムの不正使用を示す場合があります。
4.2.6 アプリケーション監査ログの初期化、停止、一時停止	**4.2.6** アプリケーション監査ログの初期化がログ記録されることを確認する。	不正なアクティビティを実行する前に監査ログを停止する（または一時停止する）ことは、悪意のある者が検出から逃れるための一般的な手法です。監査ログの初期化は、ユーザが自身の行為を隠蔽するためにログ機能を無効にした可能性を示します。

PA-DSS 要件	テスト手順	ガイダンス
4.2.7 アプリケーションによるシステムレベルオブジェクトの作成および削除	**4.2.7** アプリケーションによる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。	悪意のあるユーザは、多くの場合、システムの特定の機能や操作を制御するためにターゲットシステム上のシステムレベルオブジェクトを作成または置換します。データベーステーブルやストアドプロシージャなど、システムレベルのオブジェクトが作成または削除されるたびにログに記録することで、そのような変更が承認されたものであったかを判断しやすくなります。
4.3 ペイメントアプリケーションは、イベントごとに、少なくとも以下の監査証跡エントリを記録する必要がある。 ***PCI DSS 要件 10.3 に対応***	**4.3** ペイメントアプリケーションをテストして監査ログ設定と監査ログ出力を調査し、監査可能なイベント（4.2 に記載）ごとに、以下を実行します。	4.2 に記載されている監査可能なイベントに対して 4.3.1 から 4.3.6 の詳細を記録することにより、侵害の可能性を迅速に識別し、人物、内容、場所、方法に関する十分な詳細を把握することができます。
4.3.1 ユーザ識別	**4.3.1** ユーザ識別がログエントリに含まれることを確認する。	
4.3.2 イベントの種類	**4.3.2** ログエントリにイベントの種類が含まれていることを確認する。	
4.3.3 日付と時刻	**4.3.3** ログエントリに日付と時刻が含まれていることを確認する。	
4.3.4 成功または失敗を示す情報	**4.3.4** ログエントリに成功または失敗を示す情報が含まれることを確認する。	
4.3.5 イベントの発生元	**4.3.5** ログエントリにイベントの発生元が含まれていることを確認する。	
4.3.6 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	**4.3.6** 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。	

PA-DSS 要件	テスト手順	ガイダンス
4.4 ペイメントアプリケーションではログの一元管理を強化する必要がある。 ***注:*** *この機能の実装例として以下が挙げられますが、これらに限定されません。* ▪ ログの記録に Common Log File System（CLFS）、Syslog、区切り文字テキストなどの業界標準のログファイルメカニズムを使用する。 ▪ アプリケーション固有のログ形式を一元管理された迅速なログ記録に適した業界標準のログ形式に変換する機能とそのマニュアルを用意する。 ***PCI DSS 要件 10.5.3 に対応***	**4.4.a** ベンダが準備する『PA-DSS 実装ガイド』に目を通し、顧客とインテグレータ/リセラーに以下が提供されていることを確認する。 ▪ サポートされているログの一元管理メカニズムに関する説明 ▪ 一元管理されるログサーバにペイメントアプリケーションのログを統合するための指示と手順	監査ログが適切に保護されていないと、完全性、正確性、整合性が保証されず、侵害後の調査ツールとして役に立たないことがあります。一元管理されるログシステムでのペイメントアプリケーションのログは、顧客がログを統合し、それらを相関させることができ、環境で一貫したログを確保できる必要があります。
	4.4.b 『PA-DSS 実装ガイド』に従ってペイメントアプリケーションをインストールして構成し、指示が正確で、加盟店がログを一元管理ログサーバに統一するための機能があることを確認する。	

要件 5:　　安全なペイメントアプリケーションの開発

PA-DSS 要件	テスト手順	
5.1 ソフトウェアベンダは、以下の事項を含め、ペイメントアプリケーションのセキュアな開発について、正式なプロセスを定義し、実装しています。 • ペイメントアプリケーションは PCI DSS および PA-DSS（安全な認証やロギングなど）に従って開発されている • 開発プロセスは業界標準またはベストプラクティス（あるいはその両方）に基づいている • ソフトウェア開発ライフサイクル全体に情報セキュリティが組み込まれている • セキュリティのレビューは、アプリケーションまたはアプリケーションのアップデートをリリースする前に実行されている。 : ***PCI DSS 要件 6.3 に対応***	**5.1.a** 文書化されたソフトウェア開発プロセスを調査し、プロセスが業界標準またはベストプラクティス（あるいはその両方）に基づいていることを確認する。	ソフトウェア開発の要件定義、設計、分析、およびテスト段階にセキュリティを含めないと、セキュリティの脆弱性が過失または故意によってアプリケーションコードにもたらされる可能性があります。
	5.1.b 文書化されたソフトウェア開発プロセスを確認し、プロセスに以下が含まれることを確認する。 • ソフトウェア開発ライフサイクル全体に情報セキュリティが組み込まれている • ペイメントアプリケーションが PCI DSS および PA-DSS の要件に従って開発されている	
	5.1.c 文書化されたソフトウェア開発プロセスに、以下が含まれてことを確認する。 • セキュリティのレビューが、アプリケーションまたはアプリケーションのアップデートをリリースする前に定義されている • PCI DSS と PA-DSS のセキュリティ対策方針が満たされていることを確認するための、セキュリティレビューの手順。	
	5.1.d ソフトウェア開発者にインタビューを行い、以下のように、文書化されたプロセスに従ったことを確認する。 • ソフトウェア開発ライフサイクル全体に情報セキュリティが組み込まれている • ペイメントアプリケーションが PCI DSS および PA-DSS の要件に従って開発されている • 開発プロセス全体を通して、定義された間隔でセキュリティレビューがリリース前に実施され、PCI DSS および PA-DSS 要件を含むセキュリティ対策方針が満たされていることを保証する	

PA-DSS 要件	テスト手順	
5.1.1 テストまたは開発に実際の PAN が使用されない。 ***PCI DSS 要件 6.4.3 に対応***	**5.1.1.a** ソフトウェア開発プロセスをレビューし、実際の PAN がテストまたは開発に使用されていないことを確認する手順が含まれていることを確認する。	リリース前にアプリケーションの機能をテストするために現実的な PAN が必要な場合、ペイメントカードブランドおよび多くのアクワイアラーは、テストに適したアカウント番号を提供できます。
	5.1.1.b テストプロセスを観察し、担当者をインタビューすることで、実際の PAN がテストまたは開発に使用されていないことを確認する。	
	5.1.1.c テストデータのサンプルを観察して、実際の PAN がテストまたは開発に使用されていないことを確認する。	
5.1.2 顧客にリリースする前にテストデータとテストアカウントを削除する。 ***PCI DSS 要件 6.4.4 に対応***	**5.1.2.a** ソフトウェア開発プロセスをレビューし、ペイメントアプリケーションが顧客にリリースされる前に、テストデータとアカウントが削除されていることを確認する手順が含まれていることを確認する。	テストデータとテストアカウントは、アプリケーションが顧客にリリースされる前にアプリケーションから削除する必要があります。これらのアイテムは、アプリケーションに関する情報を漏洩する場合があるためです。
	5.1.2.b テストプロセスを観察し、担当者をインタビューすることで、顧客にリリースされる前にテストデータとアカウントが削除されることを確認する。	
	5.1.2.c 最終のペイメントアプリケーション製品を調査し、顧客にリリースされる前に、テストデータとアカウントが削除されていることを確認する。	
5.1.3 ペイメントアプリケーションが顧客にリリースされる前に、カスタムペイメントアプリケーションアカウント、ユーザ ID、パスワードが削除される ***PCI DSS 要件 6.3.1 に対応***	**5.1.3.a** ソフトウェア開発プロセスをレビューし、ペイメントアプリケーションが顧客にリリースされる前に、カスタムペイメントアプリケーションのアカウント、ユーザ ID、パスワードが削除されていることを確認する手順が含まれていることを確認する。	リリース前のカスタムアカウント、ユーザ ID、パスワードは、アプリケーションへのアクセスを得るために、開発者またはそれらのアカウントの知識を持つ他の個人により、バックドアとして使用される可能性があり、アプリケーションと関連するカード会員データの侵害を招くことにつながります。
	5.1.3.b テストプロセスを観察し、担当者にインタビューを行うことで、ペイメントアプリケーションが顧客にリリースされる前に、カスタムペイメントアプリケーションアカウント、ユーザ ID、パスワードが削除されることを確認する。	
	5.1.3.c 最終のペイメントアプリケーション製品を調査し、ペイメントアプリケーションが顧客にリリースされる前に、カスタムペイメントアプリケーションアカウント、ユーザ ID、パスワードが削除されることを確認する。	
5.1.4 コーディングの脆弱性の可能性を識別し（手動または自動プロセスによる）、少なくとも以下が含まれていることを確認するため、ペイメントアプリケーションのコードは、著しい変更の後で、顧客のリリース前にレビューされる。 • コード変更は、コード作成者以外の、コードレビュー手法と安全なコーディング手法の知識のある人がレ	**5.1.4.a** 文書化されたソフトウェア開発手順を調べ、責任者をインタビューすることで、すべての著しいアプリケーションコードの変更は、次のように（手動または自動化されたプロセスのいずれかを使用して）ベンダがレビューしたことを確認する。 • コード変更は、コード作成者以外の、コードレビュー手法と安全なコーディング手法の知識のある人がレビューする。 • コードレビューにより、コードが安全なコーディングガイドラインに従って開	アプリケーションコードのセキュリティの脆弱性は、悪意のある者によってネットワークにアクセスし、カード会員データを侵害するために一般的に悪用されます。このような種類の攻撃に対する保護を実装するため、適切なコードレビューテクニックを用いる必要があります。 コードレビューテクニックは、安全なコーディングのベストプ

PA-DSS 要件	テスト手順	
ビューする。 • コードレビューにより、コードが安全なコーディングガイドラインに従って開発されたことが保証される（PCI DSS 要件 5.2 を参照）。 • リリース前に、適切な修正を実装している。 • コードレビュー結果は、リリース前に管理職によってレビューおよび承認される。 • 文書化されたコードレビュー結果には、管理職、コード作成者、コードレビュー担当者による承認とリリース前に実装された修正が含まれます。 **注:** このコードレビュー要件は、システム開発ライフサイクルの一環として、すべてのペイメントアプリケーションコンポーネント（内部および公開用 Web アプリケーション）に適用されます。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ます。 ***PCI DSS 要件 6.3.2 に対応***	発されたことが保証される（PCI DSS 要件 5.2 を参照）。 • リリース前に、適切な修正を実装している。 • コードレビュー結果は、リリース前に管理職によってレビューおよび承認される。 • コードレビュー結果には、管理職、コード作成者、コードレビュー担当者による承認とリリース前に実装された修正が含まれます。 **5.1.4.b** コード変更のサンプルでコードレビュー結果を調査し、以下の事項を確認する。 • コードレビューは、コード作成者以外の知識のある個人によって実施される • コードレビューは、コードが安全なコーディングガイドラインに従って開発される • リリース前に、適切な修正を実装している • コードレビュー結果は、リリース前に管理職によってレビューおよび承認される	ラクティスが、開発プロセス全体を通じて採用されたことを確認する必要があります。アプリケーションベンダは、使用された特定のテクノロジに適用可能な安全なコーディング手法を採用する必要があります。 レビューは、コーティング問題の可能性を特定できるよう、コードレビューテクニックの技術知識と経験のある人によって実施される必要があります。コードレビューをコードの開発者以外の担当者に割り当てることにより、独立した客観的なレビューを実施できます。 コードがリリースされる前にコードエラーを訂正することで、コードが環境を潜在的な侵害にさらすことを防止できます。コードエラーは、導入後に対処する場合、その前に比べてずっと難しく、高価な代償を支払う結果になります。リリース前に経営管理者の正式なレビューと承認を含めることにより、コードが承認され、ポリシーと手順に従って開発されていることが確認できます。
5.1.5 開発プロセス中のソースコードの完全性を検証するため、安全なソース管理実践が実施される。	**5.1.5.a** ソフトウェア開発手続きを調査し、責任者にインタビューを行うことで、ベンダが、開発プロセス中のソースコードの完全性を検証するため、安全なソース管理実践を維持したことを確認する。 **5.1.5.b** メカニズムを調査し、ソースコードを安全にする手続きを観察し、ソースコードの完全性が、開発プロセス中に維持されたことを確認する。	良いソースコード管理の実践は、コードに対するすべての変更が意図され、承認を受けており、コードを変更する正当な理由を持つもののみによって実行されていることを確認するのに役立ちます。これらの実践例には、厳格なアクセス制御によるコードのチェックインとチェックアウト、最後の承認バージョンが変更されていないことを確認するため、コードを更新する前に直ちに比較する（チェックサムを使用するなど）などが含まれます。

PA-DSS 要件	テスト手順	
5.1.6 ペイメントアプリケーションは、以下を含め、業界のベストプラクティスに基づいて開発されている。 • アプリケーション環境で最低限の権限を使用した開発。 • フェイルセーフデフォルト（初期設計の範囲内で指定されていない限り、すべての実行がデフォルトで拒否される）を使用した開発 • アプリケーションへのマルチチャンネル入力などの入力差異を含め、すべてのアクセスポイントを考慮した開発。	**5.1.6.a**ソフトウェア開発プロセスを調査し、安全なコーディング技法が定義され、以下が含まれていることを確認する。 • アプリケーション環境で最低限の権限を使用した開発。 • フェイルセーフデフォルト（初期設計の範囲内で指定されていない限り、すべての実行がデフォルトで拒否される）を使用した開発 • アプリケーションへのマルチチャンネル入力などの入力差異を含め、すべてのアクセスポイントを考慮した開発 **5.1.6.b** 開発者にインタビューを行い、アプリケーションが、以下を含め、業界のベストプラクティスに基づいて開発されていることを確認する。 • アプリケーション環境で最低限の権限を使用した開発。 • フェイルセーフデフォルト（初期設計の範囲内で指定されていない限り、すべての実行がデフォルトで拒否される）を使用した開発 • アプリケーションへのマルチチャンネル入力などの入力差異を含め、すべてのアクセスポイントを考慮した開発。	最小限の権限を使用したアプリケーション開発は、アプリケーションに安全でない想定が導入されないようにするための最も効果的な方法です。フェイルセーフデフォルトを含めることは、攻撃者が、アプリケーションの障害についての機密情報を得て、その後の攻撃を作成するのに使用することを防御できます。アプリケーションへのすべてのアクセスや入力にセキュリティが適用されていることを保証することは、入力チャネルが脆弱な状態で開いたままにされる可能性を回避できます。コードの開発中に、これらの概念を考慮しないと、安全でないアプリケーションをリリースし、後の過剰な修復につながる可能性があります。
5.1.6.1 コーディング技法に、メモリ内での PAN/SAD の処理方法を記す文書が含まれている。	**5.1.6.1.a** コーディング技法を調査し、メモリ内での PAN/SAD の処理方法を記す文書が含まれていることを確認する。 **5.1.6.1.b** 開発者にインタビューを行い、PAN/SAD がメモリ内で処理される方法について、アプリケーション開発プロセス中に考慮したことを確認する。	攻撃者はマルウェアツールを使って、メモリから機密データを取り込みます。メモリ内で PAN/SAD の開示を最小限にとどめることで、悪意のある者によって取り込まれたり、知らないうちにメモリファイル内のディスクに保存されて保護のない状態が維持される可能性を低減できます。 この要件は、PAN と SAD がメモリ内でどのように処理されるかが考慮されていることを確認するためのものです。機密データがメモリ内にいつ、どの程度の期間存在しているかだけでなく、どのような形式で存在するかを理解すると、アプリケーションベンダが、アプリケーションにおける潜在的なセキュリティ上の不安を特定し、追加の保護が必要とされるかどうかを決定するのに役立ちます。 この操作によってコーディング技法が必要となるかどうかは、開発される特定のソフトウェアと使用するテクノロジによって異なります。

PA-DSS 要件	テスト手順	
5.1.7 例えば、開発者の業務や使用されるテクノロジに適用可能なセキュリティ開発実践のトレーニングを、アプリケーション開発者に提供する。 • 安全なアプリケーション設計 • 一般的なコーディングの脆弱性（OWASP Top 10、SANS CWE Top 25、CERT Secure Coding など）を避けるための安全なコーディング技法 • メモリ内での機密データの管理 • コードレビュー • セキュリティテスト（侵入テスト技法など） • 脅威のモデリング技法 *注:* *アプリケーション開発者のトレーニングは、社内で行うことも第三者によって行うこともできます。トレーニングの配布方法の例としては、オンザジョブ、インストラクタ主導、コンピュータベースの形式があります。*	**5.1.7.a** 文書化されたソフトウェア開発プロセスが、アプリケーション開発者に開発者の業務や使用されるテクノロジに適用可能なセキュリティ開発実践のトレーニングを必要としている。	開発者が安全な開発実践の知識を持っていることを確認することにより、稚拙なコーディング方法によりもたらさせるセキュリティの脆弱性を最小限に抑えることができます。トレーニングを受けた者は、アプリケーションの設計やコードで潜在的なセキュリティ問題を識別する可能性が高くなります。ソフトウェアアプリケーションへの脅威とリスクがそうであるように、ソフトウェア開発プラットフォームと方法論は、頻繁に変わります。安全な開発実践に関するトレーニングもそれに合わせて更新する必要があります。
	5.1.7.b 数人の開発者をインタビューし、使用されるテクノロジについて、安全な開発実践とコーディング技法に精通していることを確認する。	
	5.1.7.c トレーニング記録を調べて、すべてのアプリケーション開発者が、業務と使用されるテクノロジに適用されるトレーニングを受けたことを確認する。	
5.1.7.1 使用される新しい開発テクノロジや方法に対処するため、必要に応じてトレーニングを更新する	**5.1.7.1** トレーニング資料を調査し、開発者の何人かにインタビューを行って、新たな開発テクノロジと使用されている方法に対処するため、必要に応じてトレーニングが更新されたかどうかを確認する。	
5.2 すべてのペイメントアプリケーションは、ソフトウェア開発プロセスで、一般的なコーディングの脆弱性を防ぐため、以下のように開発する。 ***注:*** *PCI DSS 要件 5.2.1 ～ 5.2.9 および PCI DSS 6.5.1 ～ 6.5.9 に挙げられている脆弱性は、このバージョンの PA DSS が発行された時点の最新の業界ベストプラクティスを踏襲しているが、脆弱性管理に関する業界のベストプラク*		アプリケーション層はリスクが高く、内部と外部の両方の脅威の標的となる可能性があります。適切なセキュリティがないと、カード会員データおよび企業のその他の機密情報が公開される可能性があります。 要件 5.2.1 から 5.2.9 は備える必要がある最小限のコントロールです。この一覧は、このバージョンの PA-DSS が発行された時点の最も一般的なコーディングの脆

PA-DSS 要件	テスト手順	
ティス(OWASP Top 10、SANS CWE Top 25、CERT Secure Coding など)が更新された場合は、これらの要件に最新のベストプラクティスを適用する必要があります。 ***PCI DSS 要件 6.5 に対応***	**5.2.** ペイメントアプリケーションに対し、以下の脆弱性を悪用するペネトレーションテストを手動または自動で実行することで、ペイメントアプリケーションが一般的なコーディング脆弱性に対して脆弱でないことを確認します。	弱性で構成されています。業界で認知された、一般的なコーディングの脆弱性が変化した場合は、ベンダのコーディング手法もそれに合わせて更新する必要があります。
***注:** 以下の要件 5.2.1 から 5.2.6 は、すべてのペイメントアプリケーション(内部または外部)に適用されます。*		
5.2.1 インジェクションの不具合(特に SQL インジェクション)。OS コマンドインジェクション、LDAP および Xpath のインジェクションの不具合、その他のインジェクションの不具合も考慮する。	**5.2.1** インジェクションの不具合、特定の SQL インジェクションが以下を含むコーディング技法によって対処される • 入力を調べて、ユーザデータがコマンドとクエリの意味を変更できないことを確認する • パラメーター化クエリを使用する	インジェクションの不具合(特に SQL インジェクション)は、アプリケーションの侵害に使用される一般的な方法です。インジェクションは、ユーザ入力データがコマンドまたはクエリの一部としてインタプリタに送信されるときに発生します。攻撃者の悪意を持ったデータは、インタプリタに意図しないコマンドを実行したりデータを変更したりするよう仕向け、アプリケーション内部のコンポーネントを露呈させ、バッファオーバーフローなどの攻撃を開始しようとします。 すべての入力データは、処理される前に、アプリケーションによって、すべての英字、英字と数字の混合をチェックするなどして検証される必要があります。
5.2.2 バッファオーバーフロー	**5.2.2** バッファオーバーフローが以下を含むコーディング技法によって対処される • バッファ境界を検証する • 入力文字列をトランケーションする	バッファオーバーフローは、アプリケーションにバッファ領域での適切なバインドチェック機能がない場合に発生します。これにより、バッファ内の情報がバッファのメモリ領域から押し出され、実行可能メモリ領域に移動する可能性があります。その場合、攻撃者は悪意のあるコードをバッファの最後に挿入し、バッファをオーバーフローさせることによって、そのコードを実行可能メモリ領域に押し出すことができます。この方法で悪意のあるコードが実行され、多くの場合、攻撃者はアプリケーションや感染したシステムにリモートアクセスできます。
5.2.3 安全でない暗号化保存	**5.2.3** 安全でない暗号化保存が次のようなコーディング技法で対処される • 暗号化の不具合を防止する • 強力な暗号化アルゴリズムとキーを使用する	データの保存に強力な暗号化機能を適切に利用していないアプリケーションは、侵害されて認証情報やカード会員データが漏洩するリスクが高くなります。
5.2.4 安全でない通信	**5.2.4** 安全でない通信がすべての機密情報の通信を適切に認証して暗号化するコーディング技法によって対処されている	機密のネットワークトラフィックを強力な暗号化によって適切に暗号化していないアプリケーションは、侵害されてカード会員データが漏洩するリスクが高くなります。

PA-DSS 要件	テスト手順	
5.2.5 不適切なエラー処理	**5.2.5** 不適切なエラー処理が、エラーメッセージを通して情報を漏洩しないコーディング技法によって対処されている （たとえば、具体的なエラー情報ではなく汎用エラーメッセージを返すなど）	不適切なエラー処理方法によって構成、内部動作、特権情報に関する情報が漏洩するアプリケーションは、脆弱性のリスクを抱えます。攻撃者は、このような弱点を利用して、機密データを盗んだり、システムを侵害したりします。悪意のある者は、アプリケーションが正しく処理しないエラーを作成して、詳細なシステム情報を取得したり、サービス拒否割り込みを作成したり、セキュリティを失敗させたり、氏アプリケーションやシステムをクラッシュさせたりすることができます。たとえば、「提供されたパスワードが正しくありません」というメッセージは、提供されたユーザ ID は正確であり、パスワードにのみ焦点を合わせればよいことを攻撃者に伝えてしまいます。「データを確認できませんでした」など、より汎用的なエラーメッセージを使用します。
5.2.6 脆弱性特定プロセス（PA-DSS 要件 7.1 で定義）で特定された、すべての「高」脆弱性	**5.2.6** コーディング技法により、アプリケーションを侵害する可能性のある、PA-DSS 要件 7.1 で特定されたすべての「高リスク」脆弱性に対処する。	ベンダの脆弱性リスクのランク分けプロセス（PA-DSS 要件 7.1 で定義）で「高リスク」に特定され、アプリケーションを侵害する可能性があるすべての脆弱性は、アプリケーション開発中に特定・対処する必要がある。
注: *以下の要件 5.2.7 から 5.2.10 は、Web ベースのアプリケーションとアプリケーションインターフェース（内部または外部）に適用されます。*		Web アプリケーションにはアーキテクチャに応じて特有のセキュリティリスクがあり、侵害が比較的容易で発生しやすいという特徴があります。
5.2.7 クロスサイトスクリプティング（XSS）	**5.2.7** クロスサイトスクリプティング（XSS）が以下を含むコーディング技法によって対処される • 取り込む前にすべてのパラメータを検証 • コンテキスト依存エスケープの使用	XSS の不具合は、アプリケーションがユーザ入力データを取り入れ、検証したりコンテンツをエンコードしたりする前に Web ブラウザに送信するたびに発生します。XSS により、攻撃者は、被害者のブラウザでスクリプトを実行して、ユーザセッションを乗っ取ったり、ワームを取り込んだりすることができます。

PA-DSS 要件	テスト手順	
5.2.8 不適切なアクセス制御（安全でないオブジェクトの直接参照、URL アクセス制限の失敗、ディレクトリトラバーサルなど）	**5.2.8** 不適切なアクセス制御（安全でないオブジェクトの直接参照、URL アクセス制限の失敗、ディレクトリトラバーサルなど）が以下を含むコーディング技法によって対処されている。 • ユーザの適切な認証 • 入力値の削除 • 内部オブジェクト参照をユーザに公開しない • ユーザインタフェースで無許可の機能へのアクセスを許可しない	オブジェクトの直接参照は、開発者が内部実装オブジェクト（ファイル、ディレクトリ、データベースレコード、キーなど）を URL または form（形式）パラメータとして公開するときに発生します。攻撃者は、これらの参照を操作して、承認を受けずにその他のオブジェクトにアクセスできます。 Web サイトのディレクトリ構造（ディレクトリトラバーサル）を列挙してナビゲートできる攻撃者は、情報に不正アクセスし、後から攻撃するためにサイトの動作を詳細に調べることができます。 無許可の機能へのアクセスが許可されるユーザインタフェースにより、無許可のユーザが特権情報やカード会員データにアクセスできるようになります。データリソースへのアクセスを制限することは、カード会員データが無許可のリソースに提示されることを防止する役に立ちます。
5.2.9 クロスサイトリクエスト偽造（CSRF）	**5.2.9** クロスサイトリクエスト偽造（CSRF）は、アプリケーションがブラウザから自動的に送信された認証情報とトークンに依存しないコーディング技法によって対処される。	CSRF 攻撃は、ログオン済みの被害者のブラウザを使用して未認証の要求を脆弱な Web アプリケーションへ送信させ、攻撃者が被害者に実行が許可されているステート変更操作（アカウント情報の更新、購入、さらにはアプリケーションの認証などさえも）を行えるようにします。
5.2.10 不完全な認証管理とセッション管理	**5.2.10** 不完全な認証管理とセッション管理は、以下を含むコーディング技法によって対処される。 • セッショントークン（クッキーなど）を「安全」としてフラグ付けする • URL にセッションを含めない • ログイン後の適切なタイムアウトとセッション ID の巡回を組み込む	安全な認証とセッション管理は、無許可ユーザによる合法的なアカウントの資格情報、キー、またはセッショントークンの侵害を防止し、侵入者が許可されているユーザの ID を盗用できなくする。

PA-DSS 要件	テスト手順	
5.3 ソフトウェアベンダは、すべてのアプリケーション変更について変更管理手続きに従う必要がある。変更管理手続きは、新しいリリース（PA-DSS 要件 5.1 で定義されている）と同じソフトウェア開発プロセスに従っており、以下が含まれている必要がある。 ***PCI DSS 要件 6.4.5 に対応***	**5.3.a** ベンダのソフトウェア変更に関する変更管理手続きを入手して調べ、以下のことを実施する。 ▪ 文書化されたソフトウェア開発プロセスが、要件 5.1 で定義されている内容に従っていることを確認する ▪ 手続きが以下の 5.3.1 ～ 5.3.4 の項目を要求していることを確認する。	適切に管理しないと、ソフトウェア更新とセキュリティパッチの効果が完全に実現されず、意図しない結果を招く可能性があります。
	5.3.b 開発者にインタビューを行い、最近行ったペイメントアプリケーションの変更を特定する。 最近のペイメントアプリケーション変更を調べ、これらの変更について、変更管理文書でトレースする。調べる変更ごとに、変更管理手続きに従って以下が文書化されていることを確認する。	
5.3.1 影響の文書化	**5.3.1** 各変更がどのように顧客に影響するかに関する文書化が変更管理文書に含まれていることを確認します。	変更の影響を文書化して、影響を受けるすべての関係者が処理の変更に対して適切に計画できるようにする必要があります。
5.3.2 適切な権限を持つ関係者による文書化された変更承認	**5.3.2** 各変更について、適切な権限を持つ関係者により文書化された承認が行われていることを確認します。	適切な権限を持つ関係者による承認は、変更が管理層によって許可された正当な承認済みの変更であることを示します。
5.3.3 変更がシステムのセキュリティに悪影響を与えないことを確認するための機能テスト。	**5.3.3.a** サンプルの各変更について、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が実施されたことを確認します。	徹底的なテストを実施して、変更の実装によってペイメントアプリケーションのセキュリティが低下しないことを確認する必要があります。テストでは、アプリケーションの変更後に、すべての既存のセキュリティコントロールが元どおりに保たれ、同等の強力なコントロールに置き換えられているか、強化されていることを検証する必要があります。
	5.3.3.b リリースする前に、要件 5.2 への準拠について、すべての変更（パッチを含む）がテストされていることを確認します。	
5.3.4 取り消しまたは製品のインストール解除手続き	**5.3.4** 各変更に対して取り消しまたは製品のインストール解除手続きが準備されていることを確認します。	変更ごとに、変更が失敗したか、アプリケーションに悪影響を及ぼした場合に以前の状態に復元するための回復手順が存在する必要があります。

PA-DSS 要件	テスト手順	
5.4 ペイメントアプリケーションベンダは、システム開発ライフサイクルの一部として、ソフトウェアのバージョン管理方法論を文書化し、それに従っている必要がある。方法論は、ペイメントアプリケーションへの変更に関して、『PA-DSS プログラムガイド』の手続きに従い、少なくとも以下を含む必要がある。	**5.4.a** 文書化されたソフトウェア開発プロセスを調査し、ソフトウェアベンダのバージョン管理方法論が含まれており、バージョン管理の方法論は、『PA-DSS プログラムガイド』に従わなければならないことを確認する。 ペイメントアプリケーションに対するすべての変更を含め、ペイメントアプリケーションで文書化されたバージョン管理の方法論に従っていることを確認する。	徹底的に定義されているバージョン管理の方法論がないと、アプリケーションへの変更が正しく識別されないことがあり、顧客やインテグレータ/リセラーが、アプリケーションへのバージョン変更の影響を理解できない可能性があります。 ペイメントアプリケーションベンダのバージョン管理方法論には、特定のペイメントアプリケーションについて、使用されている要素、バージョンの形式、異なるバージョン要素の階層などを特に識別する、定義されたバージョンスキームを含める必要があります。 バージョンスキームは、明らかに様々な要素のそれぞれがバージョン番号でどのように使用されるかを指定する必要があります。 バージョンスキームは、「N」は数値要素、「A」はアルファベット要素を示す N.NN.NNA など、多くの方法で示すことができます。バージョン管理スキームには、バージョンの各要素に対して使用できる、0～9、A～Z といった文字セットの識別を含める必要があります。 適切に定義されたバージョンスキームがないと、アプリケーションへの変更をバージョン番号の形式で正確に表すことができない場合があります。
5.4.1 バージョン管理の方法論は、以下のように、使用される特定のバージョン要素を定義する必要がある。 ▪ バージョンスキームの要素が、『PA-DSS プログラムガイド』で指定されている要件にどのように従っているかに関する詳細。 ▪ 要素の数、セパレータ、文字セットなどを含むバージョンスキームの形式（英文字、数字、その両方から構成される） ▪ 各要素が、バージョンスキームで何を表しているかの定義（変更のタイプ、メジャー、マイナー、メンテナンスリリース、ワイルドカードなど） ▪ ワイルドカードの使用を示す要素の定義 *注:* *ワイルドカードは、セキュリティ以外に影響を与える変更を表すバージョン番号の要素で代替が可能です。ワイルドカードの使用に関する追加の要件については、5.5.3 を参照してください。*	**5.4.1.a** 文書化されたバージョニング方法を調査し、以下が含まれていることを確認する。 ▪ バージョンの番号スキームの要素が、『PA-DSS プログラムガイド』で指定されている要件にどのように従っているかに関する詳細。 ▪ バージョン番号のスキーム形式が指定され、要素の数、セパレータ、文字セットなどを含む（英文字、数字、その両方から構成される 1.1.1.N など） ▪ 各要素が、バージョン番号スキームで何を表しているかの定義（変更のタイプ、メジャー、マイナー、メンテナンスリリース、ワイルドカードなど） ▪ ワイルドカードの使用を示す要素の定義	
	5.4.1.b バージョンスキームの要素が、『PA-DSS プログラムガイド』で指定されている変更の種類にどのように従っているかに関する詳細。	
	5.4.1.c 最近のペイメントアプリケーションの変更、割り当てられたバージョン番号、およびアプリケーションの変更の種類を指定する変更管理文書を調べ、バージョン番号の要素が、適用可能な変更および文書化されたバージョン管理の方法で定義されたパラメータと一致していることを確認する。	
	5.4.1.d 数人の開発者をインタビューし、バージョン番号のワイルドカード使用など、バージョンスキームに精通していることを確認する。	
5.4.2 バージョン管理の方法は、『PA-DSS プログラムガイド』に従って、以下を含む、すべてのアプ	**5.4.2.a** ソフトウェアベンダの文書化されたバージョン管理方法を調べ、以下を含む、バージョン方法を確認する。	

PA-DSS 要件	テスト手順	
リケーションの変更の種類と影響を示す必要がある。 • アプリケーションの変更のすべての種類と影響に関する説明 • 変更の具体的な識別と定義: o アプリケーションの機能またはその依存要素に影響を与えない o アプリケーションの機能に影響はあるが、セキュリティや PA-DSS 要件への影響はない o どのようなセキュリティ機能や PA-DSS 要件にも影響を与える。 • 変更の各種類が特定のバージョン番号にどのように結びつけられているか	• アプリケーションの変更のすべての種類と影響に関する説明(アプリケーションい影響を与えない、多少の影響を与える、大きな影響を与える変更など)、 • 変更の具体的な識別と定義: o アプリケーションの機能またはその依存要素に影響を与えない o アプリケーションの機能に影響はあるが、セキュリティや PA-DSS 要件への影響はない o どのようなセキュリティ機能や PA-DSS 要件にも影響を与える • 変更の各種類が特定のバージョン番号にどのように結びつけられているか	
	5.4.2.b バージョン管理の方法が、『PA-DSS プログラムガイド』の要件に従っていることを確認する。	
	5.4.2.c 担当者にインタビューを行い、変更の各種類に関するプロセスを観察し、文書化された方法が、すべての種類の変更で従われていることを確認する。	
	5.4.2.d 最近のペイメントアプリケーションの変更からサンプルを選び、アプリケーションの変更の種類を指定する変更管理文書に目を通し、割り当てられたバージョン番号が、文書化された方法に従った変更の種類に一致することを確認する。	
5.4.3 バージョン管理の方法は、具体的にワイルドカードが使用されているかどうかを識別する必要がある。使用されている場合は、どのように使用されているかも識別する。以下の内容を含める。 • ワイルドカードが、バージョン管理の方法でどのように使用されるかの詳細 • ワイルドカードが、セキュリティまたは任意の PA-DSS 要件に影響を与える変更に使用されることはない • セキュリティ以外に影響を与える変更(ワイルドカード要素を含む)を表すために使用されるバージョン番号の要素が、セキュリティに影響を与える変更を表すために決して使用されない	**5.4.3.a** ソフトウェアベンダの文書化されたバージョン管理方法を調べ、以下を含め、ワイルドカードがどのように使用されているかが含まれていることを確認する。 • ワイルドカードが、バージョン管理の方法でどのように使用されるかの詳細 • ワイルドカードが、セキュリティまたは任意の PA-DSS 要件に影響を与える変更に使用されることはない • セキュリティ以外に影響を与える変更(ワイルドカード要素を含む)を表すために使用されるバージョン番号の要素が、セキュリティに影響を与える変更を表すために決して使用されない • ワイルドカードの右側の要素は、セキュリティに影響を与える変更に使用することはできない • セキュリティに影響を与える変更には、最初のワイルドカード要素の「左側に」表示される、その他のバージョン番号要素の変更が必要となる	PA-DSS の「ワイルドカード」の要素は、必要に応じて、複数のセキュリティ以外の影響を与える変更を表すために、バージョンスキームで使用できます。 ワイルドカードは、ベンダのバージョンスキームの唯一の可変要素であり、ワイルドカード要素によって表される各バージョン間には、マイナーで、セキュリティ以外に影響を与える変更のみが存在することを示すために使用されます。 たとえば、バージョン番号 1.1.x は、1.1.2 や 1.1.3 などをカバーしており、これらの間のコードベースには、外観上またはその他のマイナーな種類を除き、基本的に代わっていないことを顧客に示しています。 ワイルドカードの使用はベンダのバージョン管理方法で事前に定義され、『PA-DSS プログラムガイド』の要件に従っている場合のみ使用

PA-DSS 要件	テスト手順	
• ワイルドカード要素は、セキュリティに影響を与える変更を表すバージョン要素の前に使用することはできません。ワイルドカード要素の後に続くバージョン要素は、セキュリティに影響を与える変更を表すために使用することはできません。 ***注:*** *ワイルドカードは、『PA-DSS プログラムガイド』に従ってのみ使用できます。*	**5.4.3.b** ワイルドカードの使用が、『PA-DSS プログラムガイド』の要件に従っていることを確認する（たとえば、ワイルドカード要素の後に現れる要素は、セキュリティに影響を与える変更のために使用することはできない）。	できます。 *注:* *ワイルドカードの使用はオプションで必須ではありません。*
	5.4.3.c 担当者にインタビューを行い、変更の各種類に関するプロセスを観察し、以下のことを確認する。 • ワイルドカードが、セキュリティまたは任意の PA-DSS 要件に影響を与える変更に使用されることはない • セキュリティ以外に影響を与える変更（ワイルドカード要素を含む）を表すために使用されるバージョン番号の要素が、セキュリティに影響を与える変更を表すために使用されない	
	5.4.3.d 最近のペイメントアプリケーションの変更からサンプルを選び、アプリケーションの変更の種類を指定する変更管理文書に目を通す。以下の点を確認する: • ワイルドカードが、セキュリティまたは任意の PA-DSS 要件に影響を与える変更に使用されない • セキュリティ以外に影響を与える変更（ワイルドカード要素を含む）を表すために使用されるバージョン番号の要素が、セキュリティに影響を与える変更を表すために使用されない	
5.4.4 ベンダの公開されたバージョン管理方法は、顧客やインテグレータ/リセラーに伝達しなければならない	**5.4.4** 『PA-DSS 実装ガイド』に目を通し、顧客およびインテグレータ/リセラー用に、ベンダの公開されたバージョン方法の説明が含まれており、以下を含んでいることを確認する。 • 要素の数、セパレータ、文字セットなど、バージョンスキームの形式を含むバージョンスキームの詳細 • セキュリティに影響を与える変更が、バージョンスキームよってどのように示されているかの詳細 • 変更のその他の種類がバージョンにどのような影響を与えるかの詳細 • セキュリティに影響を与える変更を表すために使用されないことの確認を含め、使用されるワイルドカード要素の詳細	ベンダのバージョン管理方法が、『PA-DSS 実装ガイド』に含まれていることを確認すると、使用されているペイメントアプリケーションのバージョンとペイメントアプリケーションの各バージョンに加えられた変更の種類を理解するため、顧客やインテグレータ/リセラーに必要な情報を提供できます。
5.4.5 内部バージョンを公開されているバージョン管理方法にマッピングする場合は、バージョン管理方法に、外	**5.4.5.a** 文書化されたバージョン管理方法を調査し、内部バージョンの公開されている外部バージョンへのマッピングが含まれていることを確認する。	ペイメントアプリケーションのベンダよっては、外部（またはパブリック）リリースに使用されるバージョン管理方法とは異なるバージョン管理方法を使用して、内部

PA-DSS 要件	テスト手順	
部バージョンへの内部バージョンのマッピングを含める必要がある。	**5.4.5.b** 最近の変更を調べ、変更の種類に応じて、公開されているバージョン管理スキームが内部バージョンのマッピングに一致していることを確認する。	使用または参照を行うことがあります。このような状況では、両方のバージョン管理方法が、よく定義・文書化され、それらの間の関係が十分に文書化されていることが重要です。
5.4.6 ソフトウェアベンダは、リリース前のバージョン管理方法に準拠するため、アプリケーションのアップデートを確認するプロセスを導入している必要がある。	**5.4.6.a** 文書化されたソフトウェア開発プロセスとバージョン管理方法を調べ、リリース前のバージョン管理方法に準拠するため、アプリケーションのアップデートを確認するプロセスが導入されていることを確認する。	製品のアップデートが計画されたリリースの意図と範囲に一致していること、およびこれらの変更が顧客に正確に伝えられたことを確認するプロセスをペイメントアプリケーションベンダが導入していることが重要です。このようなプロセスがないと、顧客が知らないうちに、顧客のアプリケーションにマイナスの影響を与えるような変更がアプリケーションに加えられる可能性があります。
	5.4.6.b ソフトウェア開発者にインタビューを行い、プロセスを観察して、リリース前のバージョン管理方法に準拠するため、アプリケーションのアップデートが調査されていることを確認する。	

PA-DSS 要件	テスト手順	
5.5 リスク評価手法（たとえば、アプリケーションの脅威モデリング）が、ソフトウェア開発プロセスの間に、アプリケーションの潜在的なセキュリティ設計上の欠陥や脆弱性を識別するために使用される。リスク評価プロセスには、以下が含まれる。 ▪ セキュリティに影響を与える機能と相互信頼境界の機能を含むがこれらに限定されない、ペイメントアプリケーションのすべての機能 ▪ アプリケーション決定ポイント、プロセスフロー、データフロー、データストレージ、および信頼境界の評価 ▪ PAN および/または SAD やカード会員データ環境（CDE）と相互動作するペイメントアプリケーション内のすべてのエリア、およびカード会員データの露呈を招くプロセスでもたらされる結果の識別 ▪ カード会員データフロー分析に起因する潜在的な脅威と脆弱性の一覧、およびそれぞれに割り当てられるリスク格付け（たとえば、高、中、または低優先順位） ▪ 開発プロセス中の適切な修正と対策の実施 ▪ 管理層のレビューと承認に関するリスク評価結果の文書化	**5.5** 文書化されたソフトウェア開発手続きを調査し、責任者にインタビューを行うことで、ベンダが、ソフトウェア開発プロセスの一部としてリスク評価手法を使用していることを確認する。また、プロセスに以下が含まれていることを確認する。 ▪ セキュリティに影響を与える機能と相互信頼境界の機能を含むがこれらに限定されない、ペイメントアプリケーションのすべての機能 ▪ アプリケーション決定ポイント、プロセスフロー、データフロー、データストレージ、および信頼境界の評価 ▪ PAN/SAD や CDE と相互動作するペイメントアプリケーション内のすべてのエリア、およびカード会員データの露呈を招くプロセスでもたらされる結果の識別 ▪ カード会員データフロー分析に起因する潜在的な脅威と脆弱性の一覧、およびそれぞれに割り当てられるリスク格付け（たとえば、高、中、または低優先順位） ▪ 開発プロセス中の適切な修正と対策の実施 ▪ 管理層のレビューと承認に関するリスク評価結果の文書化	ペイメントアプリケーションの品質とセキュリティを維持するため、リスク評価手法は、ソフトウェア開発プロセス中にアプリケーションベンダによって導入されるべきである。 脅威モデリングは、機密情報が承認されていないアプリケーションユーザに公開される機会について、アプリケーションのコンストラクトおよびデータフローを分析するために使用できるリスク評価の一形態です。これらのプロセスにより、ソフトウェア開発者やアーキテクトが、開発プロセスの初期段階で潜在的なセキュリティ上の問題を特定し、解決することが可能になり、アプリケーションのセキュリティ向上や開発コストの最小化につながります。
5.6 ソフトウェアベンダは、アプリケーションと任意のアプリケーションアップデートの最終リリースを文書化および承認するプロセスを実装する必要がある。以下の文書を含む。 ▪ アプリケーションまたはアプリケーションアップデートのリリースを正式に承認する権限当事者による署名 ▪ セキュアな開発プロセスがベンダによって使用されたことの確認	**5.6.a** 文書化されたプロセスを調査し、アプリケーションの最終的なリリースと任意のアプリケーションアップデートが、すべての SDLC プロセスに従ったリリースと確認を正式に承認する権限当事者による署名を含め、正式に承認および文書化される必要があることを確認する。 **5.6.b** アプリケーションと任意のアプリケーションアップデートの最終リリースのサンプルについて、承認文書に目を通し、以下のことを確認する。 ▪ 正式な承認と権限当事者による署名。 ▪ セキュアな開発プロセスが使用されたことの確認。	ペイメントアプリケーションベンダの組織内の誰かが、セキュアな開発プロセスのすべての側面（5.1 ～ 5.5 に定義されているように）が実施されていることをレビューおよび確認する責任を有します。責任当事者からの正式なレビューと承認がないと、重要なセキュリティプロセスがなかったり、除外されたりするため、障害のある、または安全性の低いアプリケーションが製造されることにつながります。

要件 6:　　ワイヤレス送信の保護

PA-DSS 要件	テスト手順	ガイダンス
6.1 ワイヤレステクノロジを使用するペイメントアプリケーションについては、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）。ワイヤレステクノロジを安全に実装する必要がある。 ***PCI DSS 要件 1.2.3 および 2.1.1 に対応***	**6.1** ワイヤレステクノロジを使用して開発するペイメントアプリケーション、およびペイメントアプリケーションにバンドルされるワイヤレスアプリケーションについて、ワイヤレスアプリケーションでベンダのデフォルト設定が使用されないことを次のようにして確認する。 **6.1.a** ベンダが準備する『PA-DSS 実装ガイド』に目を通し、顧客とインテグレータ/リセラーのために、以下が含まれていることを確認する。 ▪ ▪ アプリケーションによって制御されるすべてのワイヤレスコンポーネントについて、ペイメントアプリケーションは、インストール時に、デフォルトの暗号化キー、パスワード、SNMP コミュニティ文字列の変更を強制する。 ▪ キー/パスワードの知識を持つ人物が退社または異動するたびに、ワイヤレス暗号化キーおよび SNMP 文字列を含むパスワードを変更する手続き ▪ ペイメントアプリケーションによって制御されていない付属のワイヤレスコンポーネントで、デフォルトの暗号化キー、パスワード、SNMP コミュニティ文字列を変更する指示 ▪ 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、ファイアウォールをインストールする指示 ▪ ペイメントアプリケーションのワイヤレス機能が使用するであろうすべての無線トラフィック（特定のポート情報を含む）の詳細 ▪ ワイヤレス環境とカード会員データ環境間のすべてのトラフィックを拒否または、業務上必要な場合、承認されたトラフィックのみ許可するようファイアウォールを構成する指示	ワイヤレステクノロジの利用は、悪意のある者がネットワークとカード会員データにアクセスするための一般的な経路となります。ワイヤレスネットワークが十分なセキュリティ構成（デフォルト設定の変更を含む）で実装されていない場合、盗聴者はワイヤレストラフィックを傍受し、データとパスワードを容易にキャプチャしてネットワークに容易に侵入して攻撃することができます。これらの理由から、ペイメントアプリケーションは、デフォルトまたは安全でないワイヤレス設定の使用を必要とすることはできません。 ファイアウォールがワイヤレスネットワークから CDE へのアクセスを制限していない場合、ワイヤレスネットワークへの不正アクセスを得た悪意のある者は、容易に CDE に接続し、アカウント情報を侵害することができます。

PA-DSS 要件	テスト手順	ガイダンス
	6.1.b『PA-DSS 実装ガイド』に従ってアプリケーションをインストールし、アプリケーションとワイヤレス設定をテストして、ペイメントアプリケーションによって管理されるすべてのワイヤレス機能について、以下のことを確認する。 • 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 • 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インストール時に変更されてること • アクセスポイントのデフォルトのパスワード/パスフレーズがインストール時に変更されてること • 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 • 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が変更されていること（該当する場合）	
	6.1.c ペイメントアプリケーションによって管理されるすべてのワイヤレス機能について、『PA-DSS実装ガイド』のワイヤレス暗号化キーパスワード/パスフレーズ、SNMP 文字列を変更する指示に従う。『PA-DSS 実装ガイド』の指示が正確で、ワイヤレス暗号化キー、パスワード、および SNMP 文字列が変更されるようになることを確認する。	
	6.1.d ペイメントアプリケーションによって制御されないすべてのワイヤレス機能について、『PA-DSS実装ガイド』のデフォルト暗号化キーパスワード/パスフレーズ、SNMP 文字列を変更する指示に従う。『PA-DSS 実装ガイド』の指示が正確で、ワイヤレス暗号化キー、パスワード、および SNMP 文字列が変更されるようになることを確認する。	
	6.1.e アプリケーションをインストールし、アプリケーションによって使用されるワイヤレストラフィックとポートが、『PA-DSS 実装ガイド』で文書化されているものに準拠していることを確認する。	

PA-DSS 要件	テスト手順	ガイダンス
6.2 ワイヤレステクノロジを使用するペイメントアプリケーションの場合、ペイメントアプリケーションは、業界のベストプラクティス（IEEE 802.11i など）を使用して、認証および伝送に強力な暗号化を促進する必要がある。 ***注:*** *セキュリティ制御としての WEP の使用は、禁止されています。* ***PCI DSS 要件 4.1.1 に対応***	**6.2.a** ワイヤレステクノロジを使用するペイメントアプリケーションでは、アプリケーションが（IEEE 802,11.i などの）業界のベストプラクティスを使用しており、認証と送信において強力な暗号化を提供していることを確認する。 **6.2.b** アプリケーションにバンドルされるすべてのワイヤレスアプリケーションでは、（IEEE 802,11.i などの）業界のベストプラクティスが使用され、認証と送信において強力な暗号化が提供されていることを確認する。 **6.2.c** ベンダが準備する『PA-DSS 実装ガイド』に目を通し、顧客とインテグレータ/リセラーのために、以下の指示が含まれていることを確認する。 • 認証および伝送用の強力な暗号化について、業界のベストプラクティス（IEEE 802.11i など）を使用するため、アプリケーションがどのように構成されているか • 認証と送信において強力な暗号化を提供するため、業界のベストプラクティスを使用するため、アプリケーションにバンドルされるすべてのワイヤレスアプリケーションがどのように構成されているか	悪意のある者は、入手が容易な無料のツールを使用して、ワイヤレス通信を傍受します。強力な暗号化を使用すると、ワイヤレスネットワーク上での機密情報の開示を制限することができます。 悪意のある者がワイヤレスネットワークにアクセスしたり、ワイヤレスネットワークを利用してその他のシステムまたはデータにアクセスするのを防ぐには、カード会員データの認証と伝送に対する強力な暗号化が必要です。
6.3 ワイヤレステクノロジの安全な利用についての顧客向けの指示を提供する。 *注:* *この要件は、アプリケーションがワイヤレステクノロジを使用するよう開発されているかどうかにかかわらず、すべてのペイメントアプリケーションコンポーネントに適用されます。* ***PCI DSS 要件 1.2.3、2.1.1、4.1.1 に対応***	**6.3** ベンダが準備する『PA-DSS 実装ガイド』を調べて、PCI DSS 準拠のワイヤレス設定に関する指示が顧客とインテグレータ/リセラーに与えられていることを確認する。これには、ワイヤレスベンダのデフォルト値を変更すること、業界のベストプラクティスを使用して、カード会員データの認証と送信に強力な暗号化を実装することが含まれる。 ▪ インストール時に、すべての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を変更する指示 ▪ キー/パスワードの知識を持つ人物が退社または異動するたびに、ワイヤレス暗号化キー、パスワード、SNMP 文字列を変更する指示 ▪ すべてのワイヤレス環境とカード会員データ環境の間にファイアウォールをインストールし、ワイヤレス環境とカード会員データ間のトラフィックを拒否または（業務上必要な場合）承認されたトラフィックのみを許可するようにファイアウォールを構成する指示 ▪ 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の強力な暗号化を提供する指示	ペイメントアプリケーションベンダは、アプリケーションがワイヤレス環境での使用について明示的に設計されていない場合でも、ワイヤレステクノロジの使用をサポートするアため、アプリケーションの構成について顧客に指示を提供する必要があります。ワイヤレスネットワークは一般的であり、顧客は、一般的なワイヤレスセキュリティ設定を認識し、ペイメントアプリケーションのセキュリティを確保するためにそれを実施する必要があります。

要件 7:

脆弱性に対応し、ペイメントアプリケーションのアップデートを維持するために、ペイメントアプリケーションをテストする

PA-DSS 要件	テスト手順	ガイダンス
7.1 ソフトウェアベンダは、以下のように、ペイメントアプリケーションをテストするためのプロセスを確立し、脆弱性を識別および管理する必要がある。 ***注:*** *ペイメントアプリケーションと共に提供される、またはペイメントアプリケーションが必要とする基盤ソフトウェアまたはシステム（Web サーバ、サードパーティのライブラリやプログラムなど）は、このプロセスに含める必要がある。* ***PCI DSS 要件 6.1 に対応***	**7.1.a** 脆弱性管理プロセスの文書を調べて、プロセスに 7.1.1 ～ 7.1.3 の手続きが以下のように含まれていることを確認する。 • セキュリティ脆弱性情報を得るための信頼できる情報源を使用し、新しいセキュリティの脆弱性を特定する • 特定されたすべての脆弱性にリスクのランク分けを割り当てる • リリース前に、脆弱性が存在しているかどうかについて、ペイメントアプリケーションとアップデートをテストする	ベンダは、アプリケーションに同梱の、またはアプリケーションで必要とされる基盤のコンポーネントやソフトウェアに存在する脆弱性を含め、アプリケーションに影響を与える可能性がある新たな脆弱性について、最新情報を維持する必要があります。 ペイメントアプリケーションのベンダは、独自のアプリケーションまたは基盤のコンポーネント内に存在する脆弱性に関して熟知し、リリース前にこれらの脆弱性を解決できる必要があります。または、その他のメカニズムを実装し、サードパーティのセキュリティパッチが直ちに利用可能にならない場合に、脆弱性が悪用される可能性を低減する必要があります。
	7.1.b 新しい脆弱性を特定し、ペイメントアプリケーションに修正を実装するためのプロセスが、ペイメントアプリケーションと共に提供される、またはペイメントアプリケーションが必要とするすべてのソフトウェア（Web サーバ、サードパーティのライブラリやプログラムなど）に適用されていることを確認します。	
7.1.1 セキュリティ脆弱性情報を得るための信頼できる情報源を使用し、新しいセキュリティの脆弱性を特定する。	**7.1.1** 責任者にインタビューして、プロセスを観察し、新たなセキュリティ脆弱性が以下のように特定されていることを確認する。 ▪ ペイメントアプリケーションおよびペイメントアプリケーションと共に提供される、またはペイメントアプリケーションが必要とする基盤ソフトウェアまたはシステムの両方で ▪ 信頼できる情報源（ソフトウェア/システムベンダの Web サイト、NIST の NVD、MITRE の CVE、DHS の US-CERT の Web サイトなど）を使用して	信頼できる情報源は、サードパーティのソフトウェアコンポーネントにおける脆弱性の情報および/またはパッチに使用される必要があります。脆弱性情報の情報源は信頼できるものでなければならず、ベンダの Web サイト、業界ニュースグループ、メーリングリスト、RSS フィードなどがあります。業界の情報源の例には、NIST の国立脆弱性データベース、MITRE の Common Vulnerabilities and Exposures のリスト、および国土安全保障省の US-CERT の Webサイトがあります。

PA-DSS 要件	テスト手順	ガイダンス
7.1.2 ペイメントアプリケーションと共に提供される、またはペイメントアプリケーションが必要とする基盤ソフトウェアまたはシステムが関与する脆弱性を含め、識別されたすべての脆弱性にリスクのランク分けを割り当てる。 ***注:*** *.* *リスクのランク分けは、業界のベストプラクティスと考えられる影響の程度に基づいている必要があります。たとえば、脆弱性をランク分けする基準は、CVSS ベーススコア、ベンダによる分類、アプリケーション機能への影響などを含む場合があります。* *リスクのランクは、最小限、アプリケーションに対する「高リスク」とみなされるすべての脆弱性を特定するものである必要があります。リスクのランク分けに加えて、差し迫った脅威をもたらす、重要なアプリケーションコンポーネントに影響を及ぼす、対処しないと侵害される危険がある場合、脆弱性は「重大」とみなされます。*	**7.1.2** 責任者のインタビューを行い、プロセスを観察し、ペイメントアプリケーションと共に提供される、またはペイメントアプリケーションが必要とする基盤ソフトウェアまたはシステムが関与する脆弱性を含め、識別されたすべての脆弱性にリスクのランク分けが割り当てられていることを確認する。	ベンダがアプリケーションに影響を及ぼす可能性がある脆弱性を特定したら、その脆弱性のリスクを評価およびランク分けする必要があります。これは、脆弱性情報の業界情報源をアクティブに監視するプロセスを必要とします。 リスクの分類（「高」、「中」、「低」など）により、ベンダは優先順位のもっとも高いリスク項目をより迅速に特定して対処し（たとえば、優先順位の高いパッチをより迅速にリリースするなど）、最もリスクが高い脆弱性を利用される可能性を低下させることができます。
7.1.3 リリース前に、脆弱性が存在しているかどうかについて、ペイメントアプリケーションとアップデートをテストする	**7.1.3** 責任者のインタビューを行い、プロセスを観察し、ペイメントアプリケーションがリリース前に脆弱性の存在についてテストされていることを確認する。	ペイメントアプリケーションベンダの脆弱性管理プロセスには、十分なテストが含まれ、リリース前に特定された脆弱性が正しく対処されていることを確認する必要があります。 *テスト方法の例には、不正な、または予期しないデータを注入する、またはデータのビットサイズを変更することにより、脆弱性の可能性を識別するための侵入テストおよびまたはファズテストテクニックが含まれます。*
7.2 ソフトウェアベンダは、セキュリティパッチとアップグレードを適切なタイミングで開発および導入するためのプロセスを確立する必要がある。.	**7.2** セキュリティパッチとアップグレードの開発および配布のプロセスの文書を調べて、プロセスに 7.2.1 ～ 7.2.2 の手続きが以下のように含まれていることを確認する。	重大な脆弱性が特定されたら可能な限り迅速に、セキュリティの脆弱性に対処するためのソフトウェアアップデートを開発して顧客にリリースし、脆弱性が悪用される期間と可能性を最小限に抑える必要がある。
7.2.1 パッチとアップデートは、既知の信頼チェーンを使用して安全な方法で配信される。	**7.2.1** 責任者にインタビューを行い、プロセスを観察して、パッチとアップデートが既知の信頼チェーンを使用して安全な方法で配信されることを確認する。	セキュリティパッチは、悪意のある個人がトランジットでアップデートを傍受すること、アップデートを変更すること、疑うことを知らない顧客にそれらを再配布しないことを防ぐ方法を配布する必要があります。

PA-DSS 要件	テスト手順	ガイダンス
7.2.2 パッチとアップデートが、パッチとアップグレードコードの整合性を維持する方法で、顧客に配布される。	**7.2.2.a** 責任者のインタビューを行い、プロセスを観察して、パッチとアップデートが、パッチとアップグレードコードの整合性を維持する方法で、顧客に配布されていることを確認する。	セキュリティのアップデートはアップデートプロセス内のメカニズムに含め、アップデートコードが置き換えられたり、改ざんされていないかどうかを確認する。整合性チェックの例には、チェックサム、デジタル署名証明書などが含まれますが、これらに限定されるわけではない。
	7.2.2.b 責任者のインタビューを行い、アプリケーションのアップデートプロセスを観察して、インストール前にターゲットシステムでパッチとアップデートの整合性がテストされることを確認する。	
	7.2.2.c パッチとアップデートコードの整合性が維持されていることを確認するため、任意のコードでアップデートプロセスを実行し、システムでアップデートの実行が許可されないことを確認する。	
7.3 アップデートの詳細と影響、バージョン番号がアプリケーションのアップデートを反映するようどのように変更されたか含むリリースノートを、すべてのアプリケーションアップデートに含める。	**7.3.a** アップデートをリリースするプロセスを調査し、担当者のインタビューを行い、アップデートの詳細と影響、バージョン番号がアプリケーションのアップデートを反映するようどのように変更されたか含むリリースノートが、すべてのアプリケーションアップデートに含まれていることを確認する。	リリースノートは、どのファイルが変更されたか、どのアプリケーション機能が変更されたかに加え、影響を受ける可能性があるセキュリティ関連の機能を含む、ソフトウェアのアップデートの詳細を顧客に提供します。リリースノートには、特定のパッチまたはアップデートが、パッチリリースに関連付けられている全体のバージョン番号にどのように影響するかを示す必要があります。
	7.3.b アプリケーションのアップデートサンプルに関するリリースノートを調査し、それらがアップデートで提供されたことを確認する。	

要件 8:　　安全なネットワーク実装の促進

PA-DSS 要件	テスト手順	ガイダンス
8.1 ペイメントアプリケーションは、安全なネットワーク環境への実装が可能でなければならない。アプリケーションは、PCI DSS 準拠のために必要なデバイス、アプリケーション、または構成に干渉してはならない。 *たとえば、ペイメントアプリケーションは PCI DSS 準拠に必要なマルウェア対策保護、ファイアウォール構成、またはその他のデバイス、アプリケーション、構成に干渉してはならない。* ***PCI DSS 要件 1、3、4、5、6 に対応***	**8.1.a**『PA-DSS 実装ガイド』に従って、アプリケーションを PCI DSS 準拠のラボラトリ環境にインストールする。ペイメントアプリケーションをテストして、PCI DSS に完全に準拠するネットワーク内で実行可能である証拠を入手する。	ペイメントアプリケーションは、アプリケーションのインストールと動作が、PCI DSS準拠に必要なその他のコントロールを実装するうえで、組織を妨げない方法を用いて設計され、開発されるべきである。たとえば、ペイメントアプリケーションは、ウイルス対策ソリューションを実行している環境で動作できる必要がある（これらのソリューションはオフにするかアンインストールする必要はない）。
	8.1.b ペイメントアプリケーションと基盤システムをテストし、ペイメントアプリケーションが、PCI DSS の機能の使用を妨げるまたは干渉しないことを確認する（たとえば、アプリケーションがパッチやマルウェア対策アップデートのインストールを妨げる、またはその他の PCI DSS 機能の操作に干渉しないなど）。	
8.2 ペイメントアプリケーションで使用するサービス、プロトコル、デーモン、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は、第三者によって提供されるものも含め、すべてペイメントアプリケーションの機能に必要で安全性の高いものでなければならない。 *たとえば、アプリケーションに NetBIOS、ファイル共有、Telnet、FTP などが必要な場合、SSH、S-FTP、SSL、IPSec などの技術でセキュリティ保護する。* ***PCI DSS 要件 2.2.2 に対応***	**8.2.a** ペイメントアプリケーションによって有効にされる、または要求されるシステムサービス、プロトコル、デーモン、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を調べる。デフォルトの "アウトオブボックス" のサービス、プロトコル、デーモン、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は、必要で安全性の高いもののみが有効になっていることを確認する。	悪意のある人々によりネットワークを侵害するために一般的に使用される多くのプロトコルがビジネスで必要となる（またはデフォルトで有効になっている）場合がある。ペイメントアプリケーションは、安全でないプロトコル、サービス、デーモンなどを使用することを要求してはならない。アプリケーションが安全性の低いサービス、デーモン、プロトコル、またはコンポーネントをサポートする場合、デフォルトでこれらが安全となっている必要があります。
	8.2.b アプリケーションをインストールし、アプリケーションの機能をテストして、アプリケーションが安全性の低いサービス、デーモン、プロトコル、またはコンポーネントをサポートする場合、デフォルトの "アウトオブボックス" でこれが安全に構成されていることを確認する。	
	8.2.c『PA-DSS 実装ガイド』に、第三者によって提供されるものも含め、ペイメントアプリケーションの機能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します。	

PA-DSS 要件	テスト手順	ガイダンス
8.3 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通常の使用または通常の操作に干渉するサービスやプロトコルの使用を必要としてはならない（外部ネットワークに起因する、CDE 内に常駐するネットワークリソースへのネットワークレベルのアクセス）。 ***注:*** *2 因子認証では、3 つの認証方法（下記参照）のうち 2 つを認証に使用する必要があります。1 つの因子を 2 回使用すること（たとえば、2 つの個別パスワードを使用する）は、2 因子認証とは見なされない。因子とも呼ばれる認証方法は次のとおりです。* ▪ *ユーザが知っていること（パスワードやパスフレーズなど）* ▪ *トークンデバイスやスマートカードなど、ユーザが所有しているもの* ▪ *ユーザ自身を示すもの（生体認証など）* トークンを使用する RADIUS、トークンを使用する TACACS、または 2 因子認証を促進するその他のテクノロジの例。***PCI DSS 要件 8.3 に対応***	**8.3** ペイメントアプリケーションの機能を調査し、アプリケーションがリモートアクセスのための 2 因子認証テクノロジの通常の使用または通常の操作に干渉するサービスやプロトコルの使用を必要としないことを確認する。 アプリケーションによってサポートされているリモートアクセスのメカニズムを識別し、そのメカニズムが 2 因子認証を妨げないことを確認する。	アプリケーションのインストールと動作が、安全なリモートアクセスを実現するための 2 因子認証ソリューションの組織における実装や動作を妨げるようなサービスやプロトコルの使用を要求しない方法で、ペイメントアプリケーションが設計および開発される必要があります。RADIUS がサポートされる認証と承認テクノロジとなることを意図している場合は、たとえば、アプリケーションは、デフォルトで、ポート 1812（通常、RFC 2865 によって RADIUS に割り当てられることが知られている）を使用するべきではありません。

要件 9:　　カード会員データをインターネット接続のサーバに保存してはならない

PA-DSS 要件	テスト手順	ガイダンス
9.1 ペイメントアプリケーションは、Web サーバとカード会員データのストレージコンポーネント（データベースサーバなど）が同じサーバ上であることを要求しない方法、およびデータストレージコンポーネントが Web サーバ共に同じネットワークゾーン（DMZ など）内にあることを要求しない方法で開発する必要がある。 ***PCI DSS 要件 1.3.7 に対応***	**9.1.a** すべてのペイメントアプリケーションのデータストレージコンポーネント（データベースなど）とすべての Web サーバを識別する。 データストレージコンポーネントと Web サーバを異なるサーバにインストールし、異なるサーバ全体でアプリケーションの機能をテストして、ペイメントアプリケーションが、データストレージコンポーネント（データベースなど）が、機能上 Web サーバと同じサーバにインストールされることを要求しないことを確認する。	ペイメントアプリケーションの Web サーバコンポーネントは、パブリックネットワークのオープンな性質（インターネット、公衆ワイヤレスなど）、これらのネットワークからの攻撃の性質や攻撃の量から、悪用されるリスクが実質的に高くなります。 カード会員データのストレージコンポーネントは、公衆向けのアプリケーションコンポーネントより、高いレベルの保護を必要とします。カード会員データが DMZ 内に配置されている場合、侵入する層の数がより少ないため、この情報へのアクセスは外部の攻撃者にとって容易になります。 同じ理由で、Web サーバは、データストレージコンポーネントと同じサーバ上に配置してはなりません。悪意のある個人が Web サーバでアカウントを悪用できるようになると、その他の努力をせずに、カード会員データのデータベースも悪用できるようになります。
	9.1.b データストレージコンポーネントと Web サーバーを、異なるネットワークゾーンにインストールする。ネットワークゾーン全体ですべてのアプリケーション機能をテストし、ペイメントアプリケーションが、データストレージコンポーネント（データベースなど）が、機能上 Web サーバと同じサーバにインストールされることを要求しないことを確認する。	

PA-DSS 要件	テスト手順	ガイダンス
	9.1.c ベンダが準備する『PA-DSS 実装ガイド』に目を通し、顧客とインテグレータ/リセラーのために、以下が含まれていることを確認する。 • インターネットにアクセス可能なシステムにはカード会員データを保存しない（Web サーバとデータベースサーバが同じサーバ上にあってはならない、など）ことを促す指示。 • カード会員データを保管するシステムからインターネットを分離するために DMZ を使用するペイメントアプリケーションを構成する方法に関する指示（たとえば、DMZ に Web サーバコンポーネントをインストールし、内部の異なるネットワークゾーンにデータストレージ･コンポーネントをインストールするなど） • アプリケーションが、2 つのネットワークゾーンを介して通信するために使用する必要のあるサービス/ポートのリスト（加盟店だけがファイアウォールを設定し、必要なポートを開くことができる）	
要件 10. ペイメントアプリケーションへの安全なリモートアクセスの促進		
10.1 顧客環境の外部からペイメントアプリケーションに対するすべてのリモートアクセスで、2 因子認証が使用される必要がある。 ***注:*** *2 因子認証では、3 つの認証方法のうち 2 つを認証に使用する必要があります（認証方法については、PA-DSS 要件 3.1.4（または 8.3 を参照）。* ***PCI DSS 要件 8.3 に対応***	**10.1.a** ベンダが準備する『PA-DSS 実装ガイド』に目を通し、顧客とインテグレータ/リセラーのために、以下が含まれていることを確認する。 ▪ 顧客のネットワークの外部からペイメントアプリケーションへのすべてのリモートアクセスは、PCI DSS の要件を満たすために、2 因子認証を使用する必要があることの指示。 ▪ アプリケーションによってサポートされている 2 因子認証メカニズムの説明 ▪ 2 因子認証（PA-DSS 要件 3.1.4 で説明されている 3 つの認証方法のうち 2 つを認証）をサポートするようアプリケーションを構成する指示。	2 因子認証は、ネットワーク外からのアクセスに関して、2 つの形式の認証を要求します。 ペイメントアプリケーションベンダは、メカニズムが正しく実装され、適用可能な PCI DSS 要件を満たすことを確認するため、指定されている 2 因子認証メカニズムをサポートするようアプリケーションの構成について顧客に指示を提供する必要があります。 2

PA-DSS 要件	テスト手順	ガイダンス
	10.1.b アプリケーションベンダが顧客のペイメントアプリケーションに顧客環境の外部からアクセスする場合は、顧客環境の外部から行うすべてのリモートアクセスについて、ベンダが 2 因子認証に関する顧客の要件をサポートしていることを確認する。	因子認証の要件は、顧客環境外部からのリモートアクセスがある場合にのみ適用されます。
10.2 ペイメントアプリケーションへのリモートアクセスは、以下のように安全に行われる必要がある。	**10.2** リモートアクセスが以下のように行われることを確認する。	リモートアクセスメカニズムが、プロバイダによって提供される継続的なサービスをサポートするためにペイメントアプリケーションベンダ、および/またはインテグレータ/リセラーによって採用される場合は、リモートアクセスメカニズムは、適用可能な PCI DSS 要件をサポートする必要がある。
10.2.1 ペイメントアプリケーションの更新がリモートアクセス経由で顧客のシステムに配信される場合、ソフトウェアベンダは顧客に対し、ベンダからのダウンロードのために必要な場合にのみリモートアクセステクノロジをオンにし、ダウンロード完了後すぐにオフにするように指示する必要がある。 または、VPN またはその他の高速接続経由で配信される場合、ソフトウェアベンダは顧客に対し、ファイアウォールまたはパーソナルファイアウォール製品を適切に構成して "常時" 接続をセキュリティで保護するように助言する必要がある。 ***PCI DSS 要件 1 および 12.3.9 に対応***	**10.2.1.a** ペイメントアプリケーションのアップデートがリモートアクセス経由で顧客ネットワークに配信される場合は、ベンダが準備する『PA-DSS 実装ガイド』を調べ、以下が含まれていることを確認する。 ▪ ベンダおよびビジネスパートナーによって使用されているリモートアクセステクノロジを必要な場合にのみアクティブ化し、使用後直ちに非アクティブ化する必要があることを指定する、リモートアクセステクノロジの安全な使用に関する顧客とインテグレータ/リセラーへの指示。 ▪ PCI DSS 要件 1 に従い、コンピュータが VPN またはその他の高速接続経由で接続されている場合は、これらの "常時" 接続をセキュリティで保護するためにファイアウォールまたはパーソナルファイアウォール製品を使用することを顧客とインテグレータ/リセラーに推奨する。	
	10.2.1.b ベンダがペイメントアプリケーションまたはアップデート（あるいはその両方）をリモートアクセス経由で顧客ネットワークに配信する場合は、ペイメントアプリケーションおよび/またはアップデートをリモートアクセス経由で子役ネットワークに配信するベンダの方法を観察し、ベンダの方法に以下が含まれていることを確認する。 ▪ 必要とする場合にのみ顧客ネットワークへの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 ▪ リモートアクセスが VPN またはその他の高速接続を介して行われる場合は、その接続が PCI DSS 要件 1 に従って安全であること	

PA-DSS 要件	テスト手順	ガイダンス
10.2.2 ベンダまたはインテグレータ/リセラーが、顧客のペイメントアプリケーションにリモートアクセスできる場合、各顧客に対して一意の認証情報（パスワード/フレーズなど）が使用される必要がある。 ***PCI DSS 要件 8.5.1 に対応***	**10.2.2** ベンダまたはインテグレータ/リセラーが、顧客のペイメントアプリケーションにリモートアクセスできる場合、ベンダのプロセスを調査し、担当者のインタビューを行って、アクセスを持つ各顧客に対して一意のパスワードが使用されていることを確認する。	1 つの認証情報セットを使用して、複数の顧客がアクセスすることを防止するため、顧客の環境へのリモートアクセスアカウントを持つベンダは、顧客ごとに異なる認証情報を使用する必要があります。 推測が容易なパスワードを生成する、反復可能な数式の使用を避ける。このような認証情報は、時間の経過とともに一般的に知られるようになり、ベンダの顧客情報を悪用するため、承認されていない個人いよって使用される可能性がある。
10.2.3 ベンダ、リセラー/インテグレータ、または顧客による顧客のペイメントアプリケーションへのリモートアクセスは、たとえば以下のように安全に実装される必要がある。 ▪ リモートアクセスソフトウェアのデフォルト設定を変更する（たとえば、デフォルトパスワードを変更し、顧客ごとに一意のパスワードを使用する）。 ▪ 特定の（既知の）IP/MACアドレスからの接続のみを許可する。 ▪ ログインに強力な認証と複雑なパスワードを使用する（PA-DSS 要件 3.1.1 ～ 3.1.10 を参照）。 ▪ PA-DSS 要件 12.1 に従い、暗号化されたデータ送信を有効にする。 ▪ ログイン試行が一定回数失敗した後のアカウントのロックアウトを有効にする（PA-DSS 要件 3.1.8 を参照）。 ▪ アクセスが許可される前に、ファイアウォール経由での仮想プライベートネットワーク（以下、VPN）接続	**10.2.3.a** ソフトウェアベンダが準備する『PA-DSS 実装ガイド』を調べて、ペイメントアプリケーションへのすべてのリモートアクセスは、安全に実装される必要があることを顧客とインテグレータ/リセラーに指示していることを確認する。 ▪ リモートアクセスソフトウェアのデフォルト設定を変更する（たとえば、デフォルトパスワードを変更し、顧客ごとに一意のパスワードを使用する）。 ▪ 特定の（既知の）IP/MACアドレスからの接続のみを許可する。 ▪ ログインに強力な認証と複雑なパスワードを使用する（PA-DSS 要件 3.1.1 ～ 3.1.10 を参照）。 ▪ PA-DSS 要件 12.1 に従い、暗号化されたデータ送信を有効にする。 ▪ ログイン試行が一定回数失敗した後のアカウントのロックアウトを有効にする（PA-DSS 要件 3.1.8 を参照）。 ▪ アクセスが許可される前に、ファイアウォール経由での仮想プライベートネットワーク（以下、VPN）接続を確立する。 ▪ ログ機能を有効にする。 ▪ 顧客環境へのアクセスを、承認されたインテグレータ/リセラー担当者に制限する。	ペイメントアプリケーションベンダは、メカニズムが正しく実装され、PCI DSS の要件を満たしていることを確認するため、安全なリモートアクセスをサポートするようアプリケーションを構成する方法について、顧客およびインテグレータ/リセラーに指示を提供する必要があります。 この要件は、顧客環境へのアクセスに使用されるすべてのリモートアクセスの種類に適用されます。

PA-DSS 要件	テスト手順	ガイダンス
を確立する。 ▪ ログ機能を有効にする。 ▪ 顧客環境へのアクセスを、承認されたインテグレータ/リセラー担当者に制限する。 ▪ . ***PCI DSS 要件 2、8、10 に対応***	**10.2.3.b**ソフトウェアベンダが顧客のペイメントアプリケーションにリモートでアクセスできる場合は、ベンダのリモートアクセス方法を観察し、担当者のインタビューを行って、リモートアクセスが安全に実装されていることを確認する。	

PA-DSS 要件	テスト手順	ガイダンス
要件 11. 公共ネットワークでのセンシティブトラフィックの暗号化		
11.1 ペイメントアプリケーションが公共ネットワーク経由でカード会員データを送信する、または送信を促進する場合、ペイメントアプリケーションは強力な暗号化とセキュリティプロトコル（たとえば、SSL/TLS、IPSEC、SSH など）の使用をサポートして、以下のような、強力な暗号化とセキュリティプロトコル（SSL/TLS、IPSEC、SSH など）を使用して保護する。 ▪ 信頼できるキーと証明書のみを受け入れる ▪ 使用されているプロトコルが、安全なバージョンまたは構成のみをサポートしている ▪ 暗号化の強度が使用中の暗号化方式に適している *オープンな公共ネットワークの例として以下が挙げられるが、これらに限定されない。* ▪ *インターネット* ▪ *802.11 と Bluetooth（ブルートゥース）を含むがこれらに限定されないワイヤレステクノロジ* ▪ *Global System for Mobile Communications（GSM）や*Code division multiple access（CDMA）などの携帯端末テクノロジ ▪ *General Packet Radio Service（GPRS）* ▪ *衛星通信* ***PCI DSS 要件 4.1 に対応***	**11.1.a** ペイメントアプリケーションがカード会員データを公共ネットワークを介して送信するか、または送信することが促進されている場合は、強力な暗号化とセキュリティプロトコルがアプリケーションと共に提供されていること、またはそれらの使用が指定されていることを確認します。 **11.1.b** ベンダが準備する『PA-DSS 実装ガイド』を調べ、ベンダがアプリケーションで強力な暗号化とセキュリティプロトコルを使用するように顧客とインテグレータ/リセラーに指示していることを確認する。 ▪ 公共ネットワーク経由でカード会員データを安全に送信する場合は、強力な暗号化とセキュリティプロトコルを実装して使用する必要がある ▪ 信頼できるキーおよび/または証明書のみが受け付けられていることを確認する指示 ▪ 安全な構成およびセキュリティプロトコルの安全な実装のみを使用するよう、ペイメントアプリケーションを構成する方法 ▪ 使用中の暗号化方式に適した暗号化の強度が使用されるよう、ペイメントアプリケーションを構成する方法 **11.1.c** 強力な暗号化とセキュリティプロトコルがペイメントアプリケーションと共に提供される場合は、『PA-DSS 実装ガイド』の指示に従ってアプリケーションをテストし、以下のことを確認する。 ▪ 信頼できるキーおよび/または証明書のみが使用されるよう、デフォルトでプロトコルが実装されている ▪ プロトコルが、安全な構成のみを使用するよう実装され、安全でないバージョンまたは構成がサポートされない。 ▪ 使用中の暗号化手法について、適切な強度の暗号化が実装されている	悪意のある者が伝送中にデータを傍受したり宛先を変更させたりすることは容易で一般的であるため、機密情報を公共ネットワーク経由で伝送する場合は暗号化する必要があります。 カード会員データの安全な送信には、信頼されているキー/証明書、トランスポート用の安全なプロトコル、適切な強度の暗号化の使用が必要です。 一部のプロトコルの実装（SSL バージョン 2.0、SSH バージョン 1.0、TLS 1.0 など）では、影響を受けるシステムで攻撃者が制御を得るために使用できる、バッファオーバーフローなどの文書化された脆弱性が存在することに注意してください。ペイメントアプリケーションによってどのセキュリティプロトコルが使用されている場合も、デフォルトで、安全な構成のみが使用され、安全でない接続の使用が防止されることを確認してください。

PA-DSS 要件	テスト手順	ガイダンス
11.2 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（たとえば、電子メール、インスタントメッセージング、チャットなど）による PAN の送信が促進されている場合、ペイメントアプリケーションは、PAN を読み取り不能にする、または強力な暗号化を実装するソリューションを提供するか、PAN を暗号化するための強力な暗号化の使用を指定する必要がある。 ***PCI DSS 要件 4.2 に対応***	**11.2.a** 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 の送信が許可されている、または送信が促進されている（あるいはその両方）場合は、PAN を読み取り不能にする、または強力な暗号化を実装するソリューションが提供されていること、またはこれを使用することが指定されていることを確認します。	電子メール、インスタントメッセージング、チャットは、内部および公共ネットワーク上での配信トラバーサル中にパケットスニッフィングによって容易に傍受することができます。ペイメントアプリケーションが強力な暗号化を使用できるよう、これらのテクノロジを提供し、PAN を読み取り不能にしていない限り、これらのメッセージングツールを利用して PAN を送信してはいけません。
	11.2.b ベンダが準備する『PA-DSS 実装ガイド』を調べ、ベンダが、アプリケーションで提供しているソリューションまたはアプリケーションと共に使用するよう指示されているソリューションの使用について、顧客とインテグレータ/リセラーへの以下の指示が含まれていることを確認する。 • PAN を読み取り不能にする、または強力な暗号化を使って PAN のセキュリティを確保する、定義済みソリューションを使用する手順。 • エンドユーザメッセージングテクノロジで送信される場合は、PANを読み取り不能にするか、強力な暗号化で保護する必要があるという指示。	
	11.2.c ソリューションがペイメントアプリケーションと共に提供されている場合は、アプリケーションをインストールしてテストし、ソリューションが PAN を読み取り不能にするか、強力な暗号化を実装していることを確認する。	

要件 12:　　すべてのコンソール以外の管理アクセスの暗号化

PA-DSS 要件	テスト手順	ガイダンス
12.1 ペイメントアプリケーションがコンソール以外の管理アクセスを採用している場合は、SSH、VPN、または SSL/TLS などのテクノロジを使用して、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、強力な暗号技術で暗号化する。 ***注:*** *管理アクセスには、Telnet または rlogin などの平文プロトコルを使用してはなりません。* ***PCI DSS 要件 2.3 に対応***	**12.1.a** ラボおよびコンソール以外の管理接続にペイメントアプリケーションをインストールし、管理者のパスワードが要求される前に、強力な暗号化方法が実行されていることを確認する。	リモート管理が安全な認証と暗号化された通信を使用して行われない場合、管理または運用レベルの機密情報（管理者のパスワードなど）が盗聴者に知られてしまう可能性があります。悪意のある者は、この情報を使用してアプリケーションおよび/またはネットワークにアクセスし、権限を変更してデータを盗むことができます。
	12.1.b ペイメントアプリケーションの構成設定を調べ、Telnet や rlogin などの平文プロトコルが、コンソール以外の管理アクセスでペイメントアプリケーションによって使用されていないことを確認する。	
	12.1.c ベンダが準備する『PA-DSS 実装ガイド』を調べ、ベンダがコンソール以外の管理アクセスの暗号化について、SSH、VPN、SSL/TLS などのテクノロジを使用した強力な暗号化を使用するために、アプリケーションを構成する方法について、顧客およびインテグレータ/リセラーへの指示が含まれていることを確認する。	
12.2 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して、コンソール以外の管理アクセスをすべて強力な暗号技術で暗号化するように顧客に指示する。 ***注:*** *管理アクセスには、Telnet または rlogin などの平文プロトコルを使用してはなりません。* ***PCI DSS 要件 2.3 に対応***	**12.2** ベンダが準備する『PA-DSS 実装ガイド』を調べ、ベンダがすべてのコンソール以外の管理アクセスの暗号化について、SSH、VPN、SSL/TLS などのテクノロジを使用した強力な暗号化を実装するための、顧客およびインテグレータ/リセラーへの指示が含まれていることを確認する。	ペイメントアプリケーションベンダは、すべてのコンソール以外の管理アクセスの暗号化について、強力な暗号化を使用するために、アプリケーションを構成する方法について、顧客およびインテグレータ/リセラーへの指示を提供する必要があります。そうすることで、セキュリティコントロールが適切に実装されていることを確認し、PCI DSS や PA-DSS のガイドラインを満たすのに役立ちます。

要件 13: 顧客、リセラー、インテグレータ向けの『PA-DSS 実装ガイド』の維持

PA-DSS 要件	テスト手順	ガイダンス
13.1 顧客、リセラー、インテグレータ向けに、以下を実現する『PA-DSS 実装ガイド』を作成、保守、配布する。	**13.1** 『PA-DSS 実装ガイド』および関連するベンダのプロセスを調べて、担当者のインタビューを行い、以下を確認する。 • 『PA-DSS 実装ガイド』が、すべてのアプリケーションの顧客、リセラー、インテグレータによって知られている • ベンダが、要求に応じて、『PA-DSS 実装ガイド』を顧客、リセラー、インテグレータに提供するメカニズムが導入されている	よく設計されており、詳細な『PA-DSS 実装ガイド』は、顧客やインテグレータ/リセラーが、カード会員データを保護するための関連 PCI DSS と PA-DSS のガイドラインを満たすため、ペイメントアプリケーションとその基盤となるコンポーネント内の適切なセキュリティ対策と構成を実装するのに役立ちます。
13.1.1 顧客、リセラー、およびインテグレータ向けに、使用するアプリケーションに固有の関連情報を提供する。	**13.1.1** 『PA-DSS 実装ガイド』を調べて、以下を確認する。 • 該当するペイメントアプリケーションの名前とバージョン番号を明確に識別する • アプリケーションが PCI DSS に準拠する方法で構成されるのに必要なすべてのアプリケーションの依存関係に関する詳細を提供する	
13.1.2 この文書内で『PA-DSS 実装ガイド』が言及されているすべての要件を記載する。	**13.1.2** 『PA-DSS 実装ガイド』を調べ、参考として付録 A を使用し、『PA-DSS 実装ガイド』にこの文書の関連要件がすべて記載されていることを確認する。	
13.1.3 少なくとも年に 1 回およびアプリケーションや PA-DSS 要件に変更があった場合にレビューを行う。また、アプリケーションに影響を与えるすべての変更とこの文書内の要件の変更を反映することによって、文書を最新状態に保つ。	**13.1.3.a** 『PA-DSS 実装ガイド』に目を通し、担当者のインタビューを行って、以下のように『PA-DSS 実装ガイド』がレビューされていることを確認する。 • 少なくとも年に一度実施する • アプリケーションに変更があった場合 • PA-DSS 要件に変更があった場合	各アプリケーションのアップデートでは、システムの機能、時には重要なアプリケーションのセキュリティメカニズムが変更または導入されます。『PA-DSS 実装ガイド』がペイメントアプリケーションの最新バージョンに関して最新の状態に保たれていないと、顧客やインテグレータ/リセラーは、最終的にはそのようなセキュリティ機構をバイパスし、機密データを危険にさらすような攻撃を可能にする、重要なアプリケーションセキュリティコントロールを見落としたり、誤って設定することにつながります。
	13.1.3.b 『PA-DSS 実装ガイド』が、必要に応じて以下の最新情報を反映するよう更新されていることを確認する。 • PA-DSS 要件への変更 • アプリケーションの機能またはその依存要素への変更	

PA-DSS 要件	テスト手順	ガイダンス
	13.1.3.c『PA-DSS 実装ガイド』と関連のベンダプロセスを調べ、担当者のインタビューを行って、必要な場合にベンダが、顧客、リセラー、インテグレータとコミュニケーションをとるためのメカニズムを導入していて、更新されたバージョンを提供していることを確認する。	

要件 14: PA-DSS の責任を担当者に割り当てること、および担当者、顧客、リセラー、インテグレータ向けのトレーニングプログラムの保守

PA-DSS 要件	テスト手順	ガイダンス
14.1 少なくとも年に 1 回、PA-DSS の責任について、ベンダ担当者向けの情報セキュリティや PA-DSS に関するトレーニングを提供する。	**14.1** トレーニング資料を調べ、責任を持つ担当者のインタビューを行って、PA-DSS の責任を持つすべてのベンダ担当者は、少なくとも年 1 回、PA-DSS および情報セキュリティのトレーニングを受けていることを確認する。	PA-DSS のガイドラインを満たす、効果的に設計されたペイメントアプリケーションを利用するには、ペイメントアプリケーションベンダの担当者が、継続される PA-DSS 評価に関して、PA-DSS とその責任の知識を持つことが必要です。担当者が適切にこれらの分野で教育を受けていることを確認するのは、ペイメントアプリケーションベンダの責任です。
14.2 以下を含む役割や責任をベンダの担当者に割り当てる。 ▪ PA-DSS の全要件を満たすための全体的な責任 ▪ PCI SSC PA-DSS プログラムガイドで、変更を最新状態に保つ ▪ 安全なコーディング慣行に従っていることを確認する ▪ インテグレータ/リセラーがトレーニングを受け、サポート資料を受け取っていることを確認する ▪ 開発者を含め、PA-DSS の責任を持つすべてのベンダ担当者がトレーニングを受けていることを確認する	**14.2.a** 文書化された責任を調べて、以下の役割の責任が正式に割り当てられていることを確認する。 ▪ PA-DSS の全要件を満たすための全体的な責任 ▪ PCI SSC PA-DSS プログラムガイドで、変更を最新状態に保つ ▪ 安全なコーディング慣行に従っていることを確認する ▪ インテグレータ/リセラーがトレーニングを受け、サポート資料を受け取っていることを確認する ▪ 開発者を含め、PA-DSS の責任を持つすべてのベンダ担当者がトレーニングを受けていることを確認する	各ペイメントアプリケーションベンダの組織内で、責任当事者（個人またはチーム）は、PA-DSS の正式な責任を割り当て、すべての PA-DSS 要件が満たされていることを確認する必要があります。
	14.2.b 以下の役割を担う担当者のインタビューを行い、責任が定義され、理解されていることを確認する。 ▪ PA-DSS の全要件を満たすための全体的な責任 ▪ PCI SSC PA-DSS プログラムガイドで、変更を最新状態に保つ ▪ 安全なコーディング慣行に従っていることを確認する ▪ インテグレータ/リセラーがトレーニングを受け、サポート資料を受け取っていることを確認する ▪ 開発者を含め、PA-DSS の責任を持つすべてのベンダ担当者がトレーニングを受けていることを確認する	

PA-DSS 要件	テスト手順	ガイダンス
14.3 ペイメントアプリケーションのインテグレータとリセラー向けに、トレーニングプログラムとコミュニケーションプログラムを開発および実装する。トレーニングには、少なくとも以下を含める必要がある。 • ペイメントアプリケーションおよび関連するシステムとネットワークを、PCI DSS に準拠する方法でどのように実装するか • この文書内（および付録 A）で『PA-DSS 実装ガイド』について言及されているすべての項目がそれらの資料に記載されていること。	**14.3.a** リセラーとインテグレータ向けのトレーニング資料とコミュニケーションプログラムを調べ、資料に以下の内容が記載されていることを確認する。 • ペイメントアプリケーションおよび関連するシステムとネットワークを、PCI DSS に準拠する方法でどのように実装するかのトレーニング。 • この文書内（および付録 A）で『PA-DSS 実装ガイド』について言及されているすべての項目がそれらの資料に記載されていること。	アプリケーションの構成、メンテナンス、サポートが正しくないと、攻撃者によって悪用される可能性があり、顧客のカード会員データ環境でセキュリティの脆弱性につながる可能性があります。アプリケーションベンダは、アプリケーションのインストールと構成が安全に行われるよう、インテグレータ/リセラーにトレーニングを提供し、加盟店の環境にインストールされる場合に、アプリケーションが PCI DSS に容易に準拠していることを確認する インテグレータやリセラーにこのようなエリアのトレーニングを提供するのは、ペイメントアプリケーションベンダの責任です。
	14.3.b ベンダのコミュニケーションプログラムおよび関連するベンダのプロセスを調べて、担当者のインタビューを行い、以下を確認する。 • トレーニング資料がインテグレータとリセラーに提供されている • 要求に応じて、ベンダが資料をインテグレータとリセラーに提供するメカニズムが導入されている	
	14.3.c 一部のリセラーとインテグレータを選んでインタビューして、アプリケーションベンダからトレーニングを受け、その資料を受領したことを確認する。	
	14.3.d インテグレータやリセラーがソフトウェアベンダからトレーニングを受け、サポート資料を受け取ったという証拠に目を通す。	
14.3.1 少なくとも年 1 回、およびアプリケーションや PA-DSS 要件が変更された場合に、トレーニング資料をレビューする。 新しいペイメントアプリケーションのバージョンや PA-DSS 要件への変更について、必要に応じて文書を最新の状態に保つよう、トレーニング資料を更新する。	**14.3.1.a** リセラーとインテグレータ向けのトレーニング資料を調べ、資料について以下のことを確認する。 • 少なくとも年 1 回、およびアプリケーションまたは PA-DSS 要件が変更された時点でレビューする • 新しいペイメントアプリケーションのバージョンや PA-DSS 要件への変更について、必要に応じて文書を最新の状態に保つよう更新する	ペイメントアプリケーションベンダの担当者、インテグレータ、リセラーのためのトレーニング資料は、少なくとも年 1 回更新し、アプリケーションと PA-DSS 要件の最新バージョンを反映するよう更新されていることを確認する必要があります。内容が最新でない状態でトレーニング資料を使用すると、アプリケーション内のセキュリティ機能設計が不十分になったり、またはインテグレータやリセラーによって不適切なアプリケーション構成がもたらされることにつながります。
	14.3.1.b 新しいバージョンのペイメントアプリケーションの配布プロセスを調べ、更新されたドキュメントがアップデートされたペイメントアプリケーションと共にインテグレータやリセラーに配布されることを確認する。	
	14.3.1.c 一部のインテグレータとリセラーを選んでインタビューして、アプリケーションベンダから更新されたトレーニング資料を受領したことを確認する。	

付録 A: PA-DSS 実装ガイドの内容の要約

この付録の目的は、『PA-DSS 実装ガイド』のトピックが関連する PA-DSS 要件を要約し、『PA-DSS 実装ガイド』で提供されている内容について顧客やインテグレータ/リセラーに説明し（『PA-DSS 実装ガイド』の 11 ページを参照）、関連するコントロールの実装責任を明確にすることです。

PA-DSS 要件	PA-DSS トピック	必須 実装ガイドの内容	コントロールの実装責任
1.1.4	以前のペイメントアプリケーションバージョンによって保存される機密認証データを削除する。	顧客やインテグレータ/リセラー向けに、以下の指示が提供される必要があります。 ▪ 履歴データを削除する必要がある（以前のバージョンのペイメントアプリケーションによって保存されるトラックデータ、カード検証コード、PIN、または PIN ブロック） ▪ 履歴データの削除方法 ▪ このような削除が PCI DSS 準拠のために絶対に必要である	**ソフトウェアベンダ**: PA-DSS 要件 1.1.4 に従い、顧客が以前のバージョンによって保存された認証データを安全に削除するためのツールまたは手続きを提供する。 **顧客とインテグレータ/リセラー**:『PA-DSS 実装ガイド』と PA-DSS 要件 1.1.4 に従い、履歴データを削除する。
1.1.5	ペイメントアプリケーションのトラブルシューティングの結果として収集される機密認証データ（認証前）を削除する。	顧客やインテグレータ/リセラー向けに、以下の指示が提供される必要があります。 ▪ 機密認証データ（認証前）は、特定の問題を解決する必要がある場合にのみ収集する必要がある ▪ このようなデータは、アクセスが限定された特定の既知の場所にのみ保存する必要がある ▪ このようなデータは特定の問題を解決するために必要に応じて限られた量だけ収集する ▪ 機密認証データは保存時に暗号化する必要がある ▪ このようなデータは使用後すぐに安全に削除する必要がある	**ソフトウェアベンダ**: 機密認証データを保存したり、PA-DSS 要件 1.1.5.a に従い、顧客の問題のトラブルシューティングを実行しない。 **顧客とインテグレータ/リセラー:**『PA-DSS 実装ガイド』と PA-DSS 要件 1.1.5.a に従い、機密認証データを保存したり、問題のトラブルシューティングを実行しない。

PA-DSS 要件	PA-DSS トピック	必須 実装ガイドの内容	コントロールの実装責任
2.1	顧客が定義した保存期間後、カード会員データを安全に削除する。	顧客やインテグレータ/リセラー向けに、以下が提供される必要があります。 ▪ 顧客が定義した保存期間を過ぎたカード会員データを安全に削除する指示 ▪ 削除する必要があるデータの場所を顧客が認識できるようにするため、ペイメントアプリケーションがカード会員データを保存するすべての場所の一覧 ▪ 顧客が、法律上、規制上、または業務上の理由で不要になったカード会員データの安全な削除を行う必要があるという指示 ▪ 基盤ソフトウェアまたはシステム（OSやデータベースなど）でのデータ保存を含め、ペイメントアプリケーションで保存されるカード会員データを安全に削除する指示 ▪ 基盤ソフトウェアまたはシステム（OSやデータベースなど）を構成する方法（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）。	**ソフトウェアベンダ**: 顧客が定義した保存期間を過ぎたカード会員データを安全に削除する必要があること、このようなデータがペイメントアプリケーションや基盤となるソフトウェアやシステムによってどこに保存されるか、ペイメントアプリケーションによって保存されるカード会員データを安全に削除される方法について、顧客にガイダンスを提供する。 **顧客とインテグレータ/リセラー**:『PA-DSS 実装ガイド』と PA-DSS 要件 2.1 に従い、顧客が定義した保存期間を過ぎたカード会員データを安全に削除する。

PA-DSS 要件	PA-DSS トピック	必須 実装ガイドの内容	コントロールの実装責任
2.2	表示される場合、PAN は、業務上の必要性により PAN 全体を見る必要がある担当者のみが全体を表示できるようにマスクする	顧客やインテグレータ/リセラー向けに、以下が提供される必要があります。 ▪ POS デバイス、画面、ログ、および領収書を含むがこれらに限定されない、PAN が表示されるすべてのインスタンスの詳細。 ▪ ペイメントアプリケーションがすべてのディスプレイにおいて、デフォルトで PAN をマスクすることを確認する。 ▪ 業務上の合法的な必要性により PAN 全体を見る必要がある担当者のみが PAN 全体を表示することができるようにペイメントアプリケーションを構成する方法に関する指示。	**ソフトウェアベンダ**: 業務上の必要性により PAN 全体を見る必要がある担当者のみが全体を表示できるようにマスクする指示を顧客に提供する。 **顧客とインテグレータ/リセラー**:『PA-DSS 実装ガイド』と PA-DSS 要件 2.2 に従って、業務上の必要性により PAN 全体を見る必要がある担当者のみが全体を表示できるようにマスクする。
2.3	すべての保存場所で PAN を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、ログのデータを含む）	顧客やインテグレータ/リセラー向けに、以下が提供される必要があります。 ▪ カード会員データを読み取り不能にするためにアプリケーションによって使用される各方法の設定可能なオプションの詳細、およびカード会員データが、（PA-DSS 要件 2.1 により）ペイメントアプリケーションで保存されるすべての場所で、各方法を設定する方法に関する指示。 ▪ カード会員データが、ペイメントアプリケーション外で保管する加盟店用に出力されるすべてのインスタンスのリスト、および加盟店がそのようなインスタンスで PAN を読み取り不能にする責任があることを説明する指示。	**ソフトウェアベンダ**: アプリケーションの内外に関わらず、すべての保存場所で PAN を読み取り不能にする指示を顧客に提供する。 **顧客とインテグレータ/リセラー**:『PA-DSS 実装ガイド』と PA-DSS 要件 2.3 に従い、保存される場所すべてで PAN を読み取り不能にする。

PA-DSS 要件	PA-DSS トピック	必須 実装ガイドの内容	コントロールの実装責任
2.4	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。	顧客やインテグレータ/リセラー向けに、以下の指示が提供される必要があります。 ▪ キーへのアクセスを、必要最小限の管理者に制限する。 ▪ キーの保存場所と形式を最小限にし、安全に保存する	**ソフトウェアベンダ**: 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できるだけ少数の場所に安全に保存し、キーへのアクセスをできるだけ少数の管理者に制限するように顧客にガイダンスを提供する。 **顧客とインテグレータ/リセラー**:『PA-DSS 実装ガイド』と PA-DSS 要件 2.4 に従い、できるだけ少数の場所にキーを安全に保存し、キーへのアクセスをできるだけ少数の管理者に制限する。
2.5	カード会員データの暗号化に使用される暗号化キーについてキー管理プロセスと手続きを実装する。	顧客やインテグレータ/リセラー向けに、以下が提供される必要があります。 ▪ 顧客またはインテグレータ/リセラーがキー管理作業に関わっている場合に暗号化キーの生成、配布、保護、変更、保存、破棄/取替を安全に行う方法に関する指示。 ▪ キー管理者が自身のキー管理の責務を理解して受諾したことを確認するためのサンプルのキー管理フォーム。 ▪	**ソフトウェアベンダ**: カード会員データの暗号化に使用される暗号化キーにアクセスする顧客に、キー管理プロセスと手続きを実装するための指示を与える。 **顧客とインテグレータ/リセラー**:『PA-DSS 実装ガイド』と PA-DSS 要件 2.5 に従い、カード会員データの暗号化に使用される暗号化キーについてキー管理プロセスと手続きを実装する。

PA-DSS 要件	PA-DSS トピック	必須 実装ガイドの内容	コントロールの実装責任
2.5.1 ～ 2.5.7	安全なキー管理機能の実装	顧客やインテグレータ/リセラー向けに、キー管理機能を実行する方法について、以下の指示を提供する。 • 強力な暗号化キーの生成 • 安全な暗号化キーの配布 • 安全な暗号化キーの保存 • 暗号化期間の終わりに達した場合の暗号化キーの変更 • キーの整合性が脆弱になったとき、またはキーが悪用された疑いがある場合のキーの破棄または取り替え • ペイメントアプリケーションでサポートされている手動での平文暗号化キー管理の操作について、知識を分割し、二重管理を使用する • 暗号化キーの不正置換の防止	**ソフトウェアベンダ**: 安全なキー管理機能を実装するよう、顧客に指示を提供する。 **顧客とインテグレータ/リセラー**:『PA-DSS 実装ガイド』と PA-DSS 要件 2.5.1 ～ 2.5.7 に従い、暗号化キーに関するキー管理プロセスと手続きを実装する。
2.6	ペイメントアプリケーションバージョンによって保存される暗号化キーまたは暗号文を取得不能にするメカニズムを提供する。	顧客やインテグレータ/リセラー向けに、以下が提供される必要があります。 ▪ 暗号化要素を取得不能にするためにアプリケーションに提供されているツールまたは手続きを使用する詳細な手順 ▪ キーが使用されなくなった時に、PCI DSS のキー管理要件に従って、暗号化キーの要素を取得不能にする指示 ▪ 復号/再暗号化プロセスの間に、クリアテキストデータのセキュリティを維持するための手順を含め、新しいキーで履歴データの再暗号化を行う方法に関する指示	**ソフトウェアベンダ**: アプリケーションによって保存される暗号化キー要素または暗号文を安全に削除するツールまたは手続き、または履歴データを新しいキーで再暗号化するツールまたは手続きを提供する。 **顧客とインテグレータ/リセラー**:『PA-DSS 実装ガイド』と PA-DSS 要件 2.6 によるキー管理要件に従って、履歴の暗号化資料を削除する。

PA-DSS 要件	PA-DSS トピック	必須 実装ガイドの内容	コントロールの実装責任
3.1	管理アクセスとカード会員データへのアクセスのために一意のユーザ ID と安全な認証を使用する。	顧客やインテグレータ/リセラー向けに、以下が提供される必要があります。 ▪ ペイメントアプリケーションが生成または管理する認証の資格情報（ユーザ名やパスワードなど）に対して、次の方法による安全な認証をアプリケーションでどのように実施するかに関する指示。 - 要件 3.1.1 ～ 3.1.11 に従い、インストールの完了時に、認証資格情報に安全な変更を適用する - PA-DSS 要件 3.1.1 ～ 3.1.11 に従い、インストールの完了以降のすべての変更（インストール後）に対して、認証資格情報に安全な変更を適用する。 ▪ PCI DSS の準拠から外れることを避けるため、認証設定に加えた変更は、少なくとも PCI DSS の要件と同程度に厳格である認証方法を提供するものとして検証する必要がある ▪ デフォルトアカウントに安全な認証を割り当て（使用しない場合でも）、これらのアカウントを無効にする、または使用しない。 ▪ 認証の資格情報がペイメントアプリケーションによって生成または管理されない場合に、PA-DSS 要件 3.1.1 ～ 3.1.11 に従い、インストールの完了時までと以降の変更（インストール後）について、管理アクセス権を持つ、またはカード会員データにアクセスするすべてのアプリケーションレベルアカウントを対象に、このような資格情報を変更および作成する方法。	**ソフトウェアベンダ**: アプリケーションが生成または管理するすべての認証資格情報について、PA-DSS 要件 3.1.1 ～ 3.1.11 に従い、アカウント/パスワードに対してペイメントアプリケーションが顧客による一意のユーザ ID と安全な認証の使用を実施することを確認する。 ペイメントアプリケーションによって生成または管理されない認証資格情報については、顧客とインテグレータ/リセラー向けに、PA-DSS 要件 3.1.1 ～ 3.1.11 に従い安全な認証の資格情報を変更および作成する方法について明確であいまいさのないガイダンスを『PA-DSS 実装ガイド』で提供していることを確認する。 **顧客とインテグレータ/リセラー**:『PA-DSS 実装ガイド』と PA-DSS 要件 3.1.1 ～ 3.1.11 に従い、一意のユーザ ID と安全な認証を確立し、維持する。

PA-DSS 要件	PA-DSS トピック	必須 実装ガイドの内容	コントロールの実装責任
3.2	ペイメントアプリケーションから PC、サーバ、データベースにアクセスするときに、一意のユーザ ID と安全な認証を使用する。	PCI DSS 要件 3.1.1 ～ 3.1.11 に従い、ペイメントアプリケーションまたはカード会員データ（あるいはその両方）から PC、サーバ、データベースにアクセスするときに、一意のユーザ名と安全な認証を使用するよう、顧客やインテグレータ/リセラーに指示する。	**ソフトウェアベンダ**: PA-DSS 要件 3.1.2 ～ 3.1.9 に従い、PC、サーバ、データベースにアクセスするためのアカウント/パスワードが設定される場合は、顧客がそれらのために一意のユーザ ID と安全な認証をペイメントアプリケーションで使用できるようにする。 **顧客とインテグレータ/リセラー**:『PA-DSS 実装ガイド』と PA-DSS 要件 3.1.1 ～ 3.1.11 に従い、一意のユーザ ID と安全な認証を確立し、維持する。
4.1	自動化された監査証跡を実装する。	自動化された監査証跡を実装する際、以下を含める指示を提供する。 ▪ インストールプロセスの完了時に、ログが設定され、デフォルトで有効にされるようにアプリケーションをインストールする方法 ▪ インストール後、顧客によって構成可能なログオプションについて、PA-DSS 要件 4.2、4.3 および 4.4 に従い、PCI DSS 準拠のログ設定を設定する方法。 ▪ ログを有効にする必要がある。ログを無効にすると、PCI DSS に準拠しなくなる。 ▪ インストール後、顧客によって構成可能なログオプションについて、ペイメントアプリケーションに付属している、または必要とされるサードパーティのソフトウェアコンポーネントで、PCI 準拠のログ設定を設定する方法。	**ソフトウェアベンダ**: PA-DSS 要件 4.2、4.3、4.4 に従い、顧客が要件に準拠したログをペイメントアプリケーションで使用できるようにする。 **顧客とインテグレータ/リセラー:**『PA-DSS 実装ガイド』と PA-DSS 要件 4.2、4.3、4.4 に従い、PCI DSS 準拠のログを確立し、維持する。
4.4	ログの一元管理を促進する。	サポートされている一元管理のログメカニズムに関する説明と、一元管理されるログサーバにペイメントアプリケーションのログを統合するための指示と手順を提供する。	**ソフトウェアベンダ**: PA-DSS 要件 4.4 に従い、顧客環境において一元管理されるログをペイメントアプリケーション使用できるようにする。 **顧客とインテグレータ/リセラー:**『PA-DSS 実装ガイド』と PA-DSS 要件 4.4 に従い、一元管理されるログを確立し、維持する。

PA-DSS 要件	PA-DSS トピック	必須 実装ガイドの内容	コントロールの実装責任
5.4.4	アプリケーションのバージョン管理手法の実装とコミュニケーション	ベンダの公開されているバージョン管理手法の説明を提供し、以下のガイダンスを含める。 • 要素の数、セパレータ、文字セットなど、バージョンスキームの形式を含むバージョンスキームの詳細 • セキュリティに影響を与える変更が、バージョン管理スキームよってどのように示されているかの詳細 • 変更のその他の種類がバージョンにどのような影響を与えるかの詳細 • セキュリティに影響を与える変更を表すために使用されないことを含め、使用されるワイルドカード要素の詳細	**ソフトウェアベンダ**: システム開発ライフサイクルの一部として、ソフトウェアのバージョン管理手法を文書化し、実装する。手法は、PA-DSS 要件 5.5 により、ペイメントアプリケーションへの変更に関して、『PA-DSS プログラムガイド』の手続きに従う必要がある。 **顧客とインテグレータ/リセラー:** どのペイメントアプリケーションのバージョンを使用しているかを理解し、検証済みのバージョンが使用されていることを確認する。

PA-DSS 要件	PA-DSS トピック	必須 実装ガイドの内容	コントロールの実装責任
6.1	ワイヤレステクノロジを安全に実装する。	ワイヤレステクノロジを備えたペイメントアプリケーションを開発する場合は、顧客やインテグレータ/リセラーに以下が提供される必要があります。 ▪ ▪ アプリケーションによって制御されるすべてのワイヤレスコンポーネントについて、ペイメントアプリケーションが、インストール時に、デフォルトの暗号化キー、パスワード、SNMP コミュニティ文字列の変更を強制する指示 ▪ キー/パスワードの知識を持つ人物が退社または異動するたびに、ワイヤレス暗号化キーおよび SNMP 文字列を含むパスワードを変更する手続き ▪ ペイメントアプリケーションによって制御されていない付属のワイヤレスコンポーネントで、デフォルトの暗号化キー、パスワード、SNMP コミュニティ文字列を変更する指示 ▪ 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、ファイアウォールをインストールする指示 ▪ ペイメントアプリケーションのワイヤレス機能が使用するであろうすべての無線トラフィック（特定のポート情報を含む）の詳細 ▪ ワイヤレス環境とカード会員データ環境間のすべてのトラフィックを拒否または、業務上必要な場合、承認されたトラフィックのみ許可するようファイアウォールを構成する指示	**ソフトウェアベンダ**: PA-DSS 要件 6.1 に従い、ワイヤレステクノロジがペイメントアプリケーションで使用される場合は、ワイヤレスベンダのデフォルト設定を変更する必要があることを顧客とインテグレータ/リセラーに指示する。 **顧客とインテグレータ/リセラー**: 顧客またはインテグレータ/リセラーがペイメント環境にワイヤレスを実装する場合は、PA-DSS 要件 6.1 に従いベンダのデフォルト設定を変更し、『PA-DSS 実装ガイド』と PCI DSS 要件 2.1.1 に従いファイアウォールをインストールする。

PA-DSS 要件	PA-DSS トピック	必須 実装ガイドの内容	コントロールの実装責任
6.2	ワイヤレスネットワーク経由で送信されるカード会員データをセキュリティで保護する	ワイヤレステクノロジを使用するペイメントアプリケーションの場合、業界のベストプラクティス（IEEE 802.11i など）を使用して、カード会員データの認証および伝送に強力な暗号化を実装する指示を含める。これには、以下の内容が含まれる。 • 認証および伝送用の強力な暗号化について、業界のベストプラクティス（IEEE 802.11i など）を使用するため、アプリケーションがどのように構成されているか • 認証と送信において強力な暗号化を提供するため、業界のベストプラクティスを使用するため、アプリケーションにバンドルされるすべてのワイヤレスアプリケーションがどのように構成されているか	**ソフトウェアベンダ**: PA-DSS 要件 6.2 に従い、ワイヤレステクノロジがペイメントアプリケーションで使用される場合は、安全な暗号化送信を実装する必要があることを顧客とインテグレータ/リセラーに指示する。 **顧客とインテグレータ/リセラー**:『PA-DSS 実装ガイド』と PA-DSS 要件 6.2 に従い、顧客またはインテグレータ/リセラーがペイメント環境にワイヤレスを実装する場合は、安全な暗号化送信を使用する。
6.3	ワイヤレステクノロジの安全な利用についての指示を提供する。	以下を含め、PCI DSS に準拠したワイヤレス設定に関する指示を提供する。 • インストール時に、すべての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を変更する指示 • キー/パスワードの知識を持つ人物が退社または異動するたびに、ワイヤレス暗号化キー、パスワード、SNMP 文字列を変更する指示 • 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ファイアウォールをインストールし、ワイヤレス環境とカード会員データ間のトラフィックを拒否または（業務上必要な場合）トラフィックを許可するようにファイアウォールを構成する指示 • 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の強力な暗号化を提供する指示	**ソフトウェアベンダ**: PCI DSS 要件 6.3 に従い、安全なワイヤレステクノロジの使用に関して顧客とインテグレータ/リセラーに指示する。 **顧客とインテグレータ/リセラー**:『PA-DSS 実装ガイド』と PA-DSS 要件 6.2 に従い、ワイヤレステクノロジを安全に保つ。

PA-DSS 要件	PA-DSS トピック	必須 実装ガイドの内容	コントロールの実装責任
8.2	サービス、プロトコル、コンポーネント、依存するソフトウェアとハードウェアは、サードパーティから提供されるものも含め、必要かつ安全なもののみを使用する。	ペイメントアプリケーションのいずれかの機能で要求される、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とハードウェアを文書化する。	**ソフトウェアベンダ:** ペイメントアプリケーションで顧客が必要かつ安全なプロトコルやサービスなどを使用するように、1）必要なプロトコルやサービスなどだけがデフォルトによって "アウトオブボックス" で確立されるようにする、2）これらの必要なプロトコルやサービスなどがデフォルトで安全に構成されるようにする、3）顧客とインテグレータ/リセラー向けの参照基準として、必要なプロトコルやサービスなどを文書化する。 **顧客とインテグレータ/リセラー:** 『実装ガイド』で文書化されているリストを使用して、PA-DSS 要件 5.4 に従い、必要かつ安全なプロトコルやサービスなどのみがシステムで使用されるようにする。
9.1	インターネットに接続されていないサーバのみにカード会員データを保存する。	顧客やインテグレータ/リセラー向けに、以下の指示が提供される必要があります。 • 公的なシステムにはカード会員データを保存しない（Web サーバとデータベースサーバが同じサーバ上にあってはならない、など）。 • カード会員データを保存するシステムをインターネットから分離するために DMZ を使用するよう、ペイメントアプリケーションを構成する方法 • アプリケーションが、2 つのネットワークゾーンを介して通信するために使用する必要のあるサービス/ポートの一覧を提供する（加盟店だけがファイアウォールを設定し、必要なポートを開くことができる）	**ソフトウェアベンダ**: PA-DSS 要件 9 に従い、ペイメントアプリケーションが DMZ またはインターネットにアクセス可能なシステムへのカード会員データ保存を必要とせず、DMZ の使用が許可されるようにする。 **顧客とインテグレータ/リセラー**:『PA-DSS 実装ガイド』と PA-DSS 要件 9 に従い、カード会員データがインターネットにアクセス可能なシステムに保存されないように、ペイメントアプリケーションを確立して維持する。

PA-DSS 要件	PA-DSS トピック	必須 実装ガイドの内容	コントロールの実装責任
10.1	顧客環境の外部からペイメントアプリケーションに対するすべてのリモートアクセスで、2 因子認証を実装する。	顧客やインテグレータ/リセラー向けに、以下を提供する。 ▪ 顧客のネットワークの外部からペイメントアプリケーションへのすべてのリモートアクセスは、PCI DSS の要件を満たすために、2 因子認証を使用する必要があることの指示。 ▪ アプリケーションによってサポートされている 2 因子認証メカニズムの説明 ▪ 2 因子認証（PA-DSS 要件 3.1.4 で説明されている 3 つの認証方法のうち 2 つを認証）をサポートするようアプリケーションを構成する指示。	**ソフトウェアベンダ**: PA-DSS 要件 10.2 に従い、ペイメントアプリケーションが、顧客環境の外部からペイメントアプリケーションに対するすべてのリモートアクセスについて、顧客の 2 因子認証の使用をサポートしていることを確認する。 **顧客とインテグレータ/リセラー**:『PA-DSS 実装ガイド』と PA-DSS 要件 10.2 に従い、顧客環境外部からのペイメントアプリケーションへの全リモートアクセスで、2 因子認証を確立して維持する。
10.2.1	リモートペイメントアプリケーション更新を安全に配信する。	ペイメントアプリケーションのアップデートがリモートアクセス経由で顧客ネットワークに配信される場合は、以下を提供する。 ▪ PCI DSS 要件 12.3.9 に従い、ペイメントアプリケーションのアップデートを行うためのリモートアクセステクノロジの使用は、ダウンロードに必要な場合にのみアクティブ化し、ダウンロード完了後すぐにオフにする。 ▪ PCI DSS 要件 1 に従い、コンピュータが VPN またはその他の高速接続で接続されている場合は、安全に構成されたファイアウォールまたはパーソナルファイアウォール経由でリモートペイメントアプリケーションのアップデートを受信する指示。	**ソフトウェアベンダ**: PA-DSS 10.3 に従い、リモートペイメントアプリケーション更新を安全に配信する **顧客とインテグレータ/リセラー**:『PA-DSS 実装ガイド』と PA-DSS 要件 10.3、PCI DSS 要件 1 に従い、ベンダからのリモートペイメントアプリケーション更新を安全に受信する。

PA-DSS要件	PA-DSS トピック	必須 実装ガイドの内容	コントロールの実装責任
10.2.3	リモートアクセスソフトウェアを安全に実装する。	ペイメントアプリケーションへのリモートアクセスは、次のように安全に行われる必要があることの指示。 ▪ リモートアクセスソフトウェアのデフォルト設定を変更する（たとえば、デフォルトパスワードを変更し、顧客ごとに一意のパスワードを使用する）。 ▪ 特定の（既知の）IP/MACアドレスからの接続のみを許可する。 ▪ ログインに強力な認証と複雑なパスワードを使用する（PA-DSS 要件 3.1.1 ～ 3.1.10 を参照）。 ▪ PA-DSS 要件 12.1 に従い、暗号化されたデータ送信を有効にする。 ▪ ログイン試行が一定回数失敗した後のアカウントのロックアウトを有効にする（PA-DSS 要件 3.1.8 を参照）。 ▪ アクセスが許可される前に、ファイアウォール経由での仮想プライベートネットワーク（以下、VPN）接続を確立する。 ▪ ログ機能を有効にする。 ▪ 顧客環境へのアクセスを、承認されたインテグレータ/リセラー担当者に制限する。	**ソフトウェアベンダ**: （1）ベンダが顧客のペイメントアプリケーションにリモートでアクセスする場合は、PA-DSS 要件 10.3.2に指定されているような安全なリモートアクセスセキュリティ機能を実装する。（2）顧客がリモートアクセスセキュリティ機能をペイメントアプリケーションで使用できるようにする。 **顧客とインテグレータ/リセラー**:『PA-DSS 実装ガイド』と PA-DSS 要件 10.3.2 に従い、ペイメントアプリケーションへのすべてのリモートアクセスについて、リモートアクセスセキュリティ機能を使用する。

PA-DSS 要件	PA-DSS トピック	必須 実装ガイドの内容	コントロールの実装責任
11.1	公共ネットワーク経由で送信されるカード会員データをセキュリティで保護する。	ペイメントアプリケーションが公共ネットワーク経由でカード会員データを送信する、または送信を促進する場合、公共ネットワーク経由で安全にカード会員データを送信するため、強力な暗号化とセキュリティプロトコルを実装および使用する指示を含める。 ▪ 公共ネットワーク経由でカード会員データを安全に送信する場合は、強力な暗号化とセキュリティプロトコルを必要とする ▪ 信頼できるキーおよび/または証明書のみが受け付けられていることを確認する指示 ▪ 安全な構成およびセキュリティプロトコルの安全な実装のみを使用するよう、ペイメントアプリケーションを構成する方法 ▪ 使用中の暗号化方式に適した暗号化の強度が使用されるよう、ペイメントアプリケーションを構成する方法	**ソフトウェアベンダ**: PA-DSS 要件 11.1 に従い、顧客が強力な暗号化とセキュリティプロトコルを使用してペイメントアプリケーションから公共ネットワーク経由でカード会員データを送信できるようにする。 **顧客とインテグレータ/リセラー**:『PA-DSS 実装ガイド』と PA-DSS 要件 11.1 に従い、カード会員データ送信のための強力な暗号化とセキュリティプロトコルを確立して維持する。
11.2	エンドユーザメッセージングテクノロジ経由で送信されるカード会員データを暗号化する。	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ソリューションを実装および使用するか、強力な暗号化を実装する指示を含める。 ▪ PAN を読み取り不能にする、または強力な暗号化を使って PAN のセキュリティを確保する、定義済みソリューションを使用する手順。 ▪ エンドユーザメッセージングテクノロジで送信される場合は、PANを読み取り不能にするか、強力な暗号化で保護する必要があるという指示。	**ソフトウェアベンダ**: PAN がエンドユーザメッセージングテクノロジを使用して送信される場合は、PA-DSS 要件 11.2 に従い、PAN を読み取り不能にするか、強力な暗号化を実装するソリューションの使用を提供または指定し、ペイメントアプリケーションが PAN の暗号化または読み取り不能にする機能をサポートしていることを確認する。 **顧客とインテグレータ/リセラー**:『PA-DSS 実装ガイド』と PA-DSS 要件 11.2 に従い、エンドユーザメッセージングテクノロジを使用して送信されるすべての PAN を読み取る不能にするか、暗号化する。

PA-DSS 要件	PA-DSS トピック	必須 実装ガイドの内容	コントロールの実装責任
12.1	コンソール以外の管理アクセスを暗号化する。	ペイメントアプリケーションがコンソール以外の管理アクセスを促進する場合は、カード会員データ環境内のペイメントアプリケーションまたはサーバへのコンソール以外の管理アクセスを暗号化するために、強力な暗号化（SSH、VPN、SSL/TLS など）を使用するようアプリケーションを構成する方法に関する指示を含める。	**ソフトウェアベンダ**: ペイメントアプリケーションがコンソール以外の管理アクセスを促進する場合は、PA-DSS 要件 12.1 に従い、ペイメントアプリケーションがコンソール以外の管理アクセスに関して、強力な暗号化を実装していることを確認する。 **顧客とインテグレータ/リセラー**:『PA-DSS 実装ガイド』と PA-DSS 要件 12.1 に従い、コンソール以外の管理アクセスをすべて暗号化する。
12.2	コンソール以外の管理アクセスを暗号化する。	すべてのコンソール以外の管理アクセスの暗号化について、SSH、VPN、SSL/TLS などのテクノロジを使用した強力な暗号化を実装するための、顧客およびインテグレータ/リセラーへの指示を含める。	**ソフトウェアベンダ**: PA-DSS 要件 12.2 に従い、ペイメントアプリケーションが顧客のコンソール以外の管理アクセスを暗号化する機能をサポートしていることを確認する。 **顧客とインテグレータ/リセラー**:『PA-DSS 実装ガイド』と PA-DSS 要件 12.2 に従い、コンソール以外の管理アクセスをすべて暗号化する。

付録 B: PA-DSS 評価用テストラボラトリ構成

実施する PA-DSS 評価ごとに、PA-QSA は、PA-DSS
評価のテストを実施するために使用するラボラトリの状態と機能を確認する必要があります。この確認は、完成させた検証報告書（ROB）と共に提出する必要があります。

ラボラトリ検証手順ごとに、評価に使用されたラボラトリと、これらの検証手続きが行われたラボラトリが PA-QSA
のラボラトリだったのかソフトウェアベンダのラボラトリだったのかを記入します。PA-QSA
は、以下に定める要件をすべて満たしているテストラボラトリを維持し、可能な限り評価を行うために、独自のラボラトリを使用する必要があります。ソフトウェアベンダのラボラトリは、必要な場合（PA-QSA がペイメントアプリケーションが実行されるメインフレーム、AS400、または Tandem
を持っていない場合など）の場合にのみ、すべてのラボラトリ要件が満たされていることを確認した後で使用できます。

PA-QSA は、以下の表内のすべての項目も確認する必要があります。

- **PA-DSS レビューに使用されるラボの場所と所有者の特定**
- **PA-DSS レビュー用のラボラトリテストアーキテクチャと環境の説明**
- **PA-DSS レビューのために、ペイメントアプリケーションの本番環境がラボラトリ内でどのようにシミュレートされたかの説明**

PA-DSS ROV 報告書テンプレートは、各評価で提供しなければならないラボラトリの検証に関する詳細を提供します。

ラボラトリ要件	ラボラトリ検証手続き			
1. 顧客に提供されるベンダのインストール指示またはトレーニングに従ってペイメントアプリケーションをインストールする。	**1.** 顧客に提供されるベンダのインストールマニュアルまたはトレーニングを使用して、現実の顧客体験をシミュレートするため、PA-DSS 報告書に記載されたすべてのプラットフォーム上へのペイメントアプリケーション製品のデフォルトのインストールが実行されたことを確認します。			
2. PA-DSS 報告書に記載されたすべてのペイメントアプリケーションバージョンをインストールして	**2.a** テスト対象のペイメントアプリケーションのすべての一般的な実装（地域や国固有のバージョンを含む）がインストールされたことを確認します。			

ラボラトリ要件	ラボラトリ検証手続き			
テストする。	**2.b** 必要なシステムコンポーネントと依存関係すべてを含め、ペイメントアプリケーションのすべてのバージョンとプラットフォームがテストされたことを確認します。			
	2.c 各バージョンで、ペイメントアプリケーションの重要な機能がすべてテストされたことを確認します。			
3. PCI DSS が要求するすべてのセキュリティデバイスをインストールして実装する。	**3.** PCI DSS が必要とするすべてのセキュリティデバイス（ファイアウォールやウィルス対策ソフトウェアなど）がテストシステムに実装されたことを確認します。			
4. PCI-DSS が必要とするすべてのセキュリティ設定のインストールまたは構成、あるいはその両方を行う。	**4.** ペイメントアプリケーションが使用するオペレーティングシステム、システムソフトウェア、およびアプリケーション用の PCI-DSS 準拠のシステム設定、パッチなどが、すべてテストシステムに実装されたことを確認します。			
5. ペイメントアプリケーションの本番環境をシミュレートする。	**5.a** ラボラトリは、ペイメントアプリケーションが実装されるすべてのシステムとアプリケーションを含めて、ペイメントアプリケーションの '本番環境' をシミュレートします。たとえば、ペイメントアプリケーションの標準的な実装は、POS マシンを備えた小売店舗と、バックオフィスまたは企業ネットワークといったクライアント/サーバ環境で構成されます。ラボラトリは、実装全体をシミュレートします。			
	5.b ラボラトリは、シミュレーション/テスト用のテストカード番号だけを使用します。実際の PAN はテストでは使用されません。 ***注:*** *テストカードは通常、ベンダ、プロセサーまたはアクワイアラーから入手できます。）*			
	5.c ラボラトリは、ペイメントアプリケーションの承認または決済、あるいはその両方の機能を実行し、すべての出力は以下の項目 6 のとおりに調べられます。			
	5.d ラボラトリまたはプロセス、あるいはその両方は、ペイメントアプリケーションによって生成されるすべての出力（一時的、永続的、エラー処理、デバッグモード、ログファイルなど）を、考えられるあらゆるシナリオにマッピングします。			

ラボラトリ要件	ラボラトリ検証手続き			
	5.e ラボラトリまたはプロセス、あるいはその両方は、シミュレートされた '実際の' データと無効なデータの両方を使用してあらゆるエラー状況とログエントリを取り込むために、ペイメントアプリケーションのすべての機能をシミュレートおよび検証します。			
6. これらのペネトレーションテスト方式のための機能を提供し、これらを使用してテストする:	**6.a フォレンジックツール/手法を使用する:** PA-DSS 要件 1.1.1 ～ 1.1.3 に従い、機密認証データの証拠として識別されたすべての出力を検索するためにフォレンジックツール/手法（市販ツール、スクリプトなど）が使用されました。[5]			
	6.b アプリケーション脆弱性の悪用を試みる: PA-DSS 要件 5.2 に従い、ペイメントアプリケーションを悪用してみるために現在の脆弱性（たとえば、OWASP トップ 10、SANS CWE トップ 25、CERT の安全なコーディングなど）が使用されました。			
	6.c ラボラトリまたはプロセス、あるいはその両方は、ペイメントアプリケーション更新プロセス中に任意のコードを実行しようとしました。PA-DSS 要件 7.2.2 に従い、任意のコードで更新プロセスを実行します。.			
7. ベンダのラボラトリは、あらゆる要件が満たされていることを確認した後でのみ使用する。	ソフトウェアベンダのラボラトリを使用する必要がある場合（PA-QSA がペイメントアプリケーションが実行されるメインフレーム、AS400、または Tandem を持っていない場合など）、PA-QSA は、（1）ベンダから貸し出された機器を使用する、または（2）ベンダのラボラトリ施設を使用することができます。ただし、このことがテストの場所と共に報告書に詳細に記述されている場合に限ります。いずれの場合も、PA-QSA は、ベンダの機器とラボラトリが以下の要件を満たしていることを確認しました。			
	7.a PA-QSA は、ベンダのラボラトリがこの文書で指定されている上記の要件すべてを満たしていることを確認し、詳細を報告書に記述します。			

[5] フォレンジックツールまたはフォレンジック手法:
フォレンジックデータを発見、分析、提示するためのツールまたは手法で、コンピュータエビデンスを迅速かつ徹底的に認証、検索、回復するための確実な方法を提供します。PA-QSA が使用するフォレンジックツールまたは手法の場合は、ペイメントアプリケーションが書き込む機密認証データを正確に見つける必要があります。これらのツールは、市販、オープンソース、PA-QSA による社内開発のいずれでもかまいません。

ラボラトリ要件	ラボラトリ検証手続き			
	7.b PA-QSA は、クリーンインストールのリモートラボラトリ環境を検証して、環境が実際に本番の状況をシミュレートしていること、ベンダが環境をいっさい変更または改ざんしていないことを確認する必要があります。			
	7.c すべてのテストは PA-QSA によって実行されます（ベンダは自身のアプリケーションに対するテストを実行できません）。			
	7.e すべてのテストは、（1）ベンダ施設内でオンサイトで実行される、または（2）安全なリンク（VPN など）を使用してネットワーク接続経由でリモートから実行されます。			
	7.e シミュレーション/テストにはテストカード番号だけを使用します。実際の PAN はテストに使用しません。これらのテストカードは通常、ベンダ、プロセサー、またはアクワイアラーから入手できます。）			
8. 効果的な品質保証（QA）プロセスを維持する	**8.a** PA-QSA QA 担当者は、PA-DSS 報告書で識別されるすべてのバージョンとプラットフォームがテストに含まれていたことを確認します。			
	8.b PA-QSA QA 担当者は、すべての PA-DSS 要件がテストされたことを確認します。			
	8.c PA-QSA QA 担当者は、PA-QSA ラボラトリ構成とプロセスが要件を満たし、報告書に正確に文書化されていることを確認します。			
	8.d PA-QSA QA 担当者は、報告書にテストの結果が正確に報告されていることを確認します。			