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

PCI DSS ナビゲート

基準要件の目的の理解

バージョン 2.0

2010 年 10 月

文書の変更

日付	バージョン	説明
2008 年 10 月 1 日	1.2	新しい PCI DSS v1.2 の内容に合わせて改訂、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。
2010 年 10 月 28 日	2.0	新しい PCI DSS v2.0 に合わせて改訂。

目次

序文

この文書では、PCI データセキュリティ基準（PCI DSS）の 12
の要件を、各要件の目的を説明するガイダンスと合わせて記述します。この文書は、カード会員データ環境をサポートするシステムコンポーネント（サーバ、ネットワーク、アプリケーションなど）をセキュリティ保護するために PCI Payment Card Industry
データセキュリティ基準と、その詳細な要件の背後にある意味と目的をより明確に理解することを望む加盟店、サービスプロバイダ、金融機関を支援することを目的としています。

注: ***『PCI DSS ナビゲート: 基準要件の目的理解』は、ガイダンスの提供のみを目的としています。***PCI DSS
オンサイト評価または自己問診（SAQ: Self Assessment Questionnaire）を完了するときは、『PCI DSS
要件およびセキュリティ評価手順』と『PCI DSS 自己問診（Self-Assessment Questionnaires）2.0』が記録文書となります。

PCI DSS 要件は、すべてのシステムコンポーネントに適用されます。PCI DSS では、"システムコンポーネント"
とは、カード会員データ環境に含まれる、またはこれに接続するすべてのネットワークコンポーネント、サーバ、またはアプリケーションとして定義されます。"システムコンポーネント"
には仮想マシン、仮想スイッチ/ルーター、仮想機器、仮想アプリケーション/デスクトップ、ハイパーバイザなどのあらゆる仮想コンポーネントも含まれます。カード会員データ環境は、カード会員データまたはセンシティブ認証データを処理する人、処理、およびテクノロジで構成されます。

- ネットワークコンポーネントにはファイアウォール、スイッチ、ルーター、ワイヤレスアクセスポイント、ネットワーク機器、その他のセキュリティ機器などが含まれる可能性がありますが、これらに限定されるわけではありません。
- サーバタイプには、Web、アプリケーション、データベース、認証、メール、プロキシ、ネットワークタイムプロトコル（NTP）、ドメインネームサーバ（DNS）などが含まれますが、これらに限定されるわけではありません。
- アプリケーションには、内部および外部（インターネットなど）アプリケーションなど、すべての市販およびカスタムアプリケーションが含まれる場合がありますが、これらに限定されるわけではありません。

PCI DSS
評価の最初の手順は、レビューの範囲を正確に決定することです。少なくとも年に一度、毎年の評価前に、評価対象の事業体はカード会員データの場所とフローをすべて識別し、それらが PCI DSS の範囲に含まれていることを確認することによって、PCI DSS
の範囲の正確性を確認する必要があります。PCI DSS の範囲の正確性と適用性を確認するには、以下を実行します。

- 評価対象の事業体は環境内に存在するすべてのカード会員データを識別および文書化して、現在定義されているカード会員データ環境（CDE）の外部にカード会員データが存在していないことを確認します。
- カード会員データのすべての場所を識別および文書化したら、事業体はその結果を使用して PCI DSS
の範囲が適切であることを確認します（たとえば、結果はカード会員データの場所を表す図やインベントリである場合があります）。

- 事業体は、データが削除されていたり、現在定義されている CDE に移行/統合されている場合を除いて、見つかったすべてのカード会員データを PCI DSS 評価範囲内にあるものと見なします。
- 事業体は評価担当者のレビューのため、または翌年の PCI SCC の範囲確認作業で参照するため、PCI DSS の範囲の確認方法と結果を示す文書を保持します。

カード会員データ環境のネットワークセグメンテーション、またはカード会員データ環境の残りの企業ネットワークからの隔離（セグメント化）は、PCI DSS 要件ではありません。ただし、ネットワークセグメンテーションはカード会員データ環境の範囲を縮小する方法として強く推奨されます。認定セキュリティ評価機関（QSA）は、事業体のカード会員データ環境内の範囲決定を支援すると共に、適切なネットワークセグメンテーションを実装して PCI DSS 評価の範囲を狭める方法についてガイダンスを提供します。

特定の実装が基準と整合性を保っているか、または特定の要件に「準拠」しているかどうかに関して疑問がある場合、PCI SSC は、QSA にテクノロジとプロセスの実装、および PCI データセキュリティ基準への準拠の検証を依頼することをお勧めします。複雑なネットワーク環境の扱いに関する QSA の専門知識は、準拠を実現しようとする加盟店またはサービスプロバイダへのベストプラクティスおよびガイダンスの提供に非常に役立ちます。PCI SSC の認定セキュリティ評価機関の一覧については、https://www.pcisecuritystandards.org を参照してください。

仮想化

仮想化を実装している場合、仮想環境内のすべてのコンポーネント（個々の仮想ホストまたは仮想デバイス、ゲストマシン、アプリケーション、管理インターフェイス、一元管理コンソール、ハイパーバイザなど）が識別され、レビューの範囲に含まれる必要があります。ホスト内の、および仮想コンポーネントとその他のシステムコンポーネント間のすべての通信およびデータフローを識別し、文書化する必要があります。

仮想化環境の実装は、仮想化システムを単独のハードウェアとしてみなすことができるようにするなど、すべての要件の目的を満たす必要があります。たとえば、さまざまなセキュリティレベルでの機能の明確なセグメンテーションとネットワークの分離が必要です。セグメンテーションでは、本番環境とテスト/開発環境の共有を防ぐ必要があります。仮想構成では、1 つの機能の脆弱性が他の機能のセキュリティに影響しないようにセキュリティ保護する必要があります。USB やシリアルデバイスなどの接続機器には、一切の仮想インスタンスからアクセスできないようにする必要があります。

また、すべての仮想管理インターフェイスプロトコルをシステム文書に記載し、仮想ネットワークおよび仮想システムコンポーネントの管理に関する役割と権限を定義する必要があります。仮想化プラットフォームには、仮想ネットワークの管理と仮想サーバの管理を分離するために、責務を分離し、最小限の特権を付与する機能が必要です。

認証管理を実装する場合、細心の注意を払って、ユーザが適切な仮想システムコンポーネントに対して認証され、ゲスト VM（仮想マシン）とハイパーバイザが区別されるようにする必要があります。

カード会員データとセンシティブ認証データの要素

PCI DSS はアカウントデータが保存、処理、または送信されるすべての場所に適用されます。
アカウントデータは以下のように、カード会員データとセンシティブ認証データで構成されます。

カード会員データには、以下の情報が含まれます。	*センシティブ認証データには、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	• 完全な磁気ストライプデータや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は、PCI DSS 要件の適用性を決定する要素です。
プライマリアカウント番号（PAN）が保存、処理、または送信される場合、PCI DSS 要件が適用されます。PAN
が保存、処理、または送信されない場合、PCI DSS 要件は適用されません。

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 PAN にのみ適用される要件 3.3 および 3.4
以外のすべての PCI DSS 要件に従って保護される必要があります。

PCI DSS
はローカル、地域およびセクターの法律や規定によって拡張される可能性があるコントロールの目的の最小限のセットを表します。さらに、法律または規制上の要件により、個人を特定できる情報またはその他のデータ要素（カード会員名など）の特定の保護が必要になるか、または消費者情報に関連した事業体の開示方法を定義する場合があります。たとえば、消費者のデータ保護、プライバシ、ID
盗難、またはデータセキュリティに関連する法律が挙げられます。PCI DSS
はローカルまたは地域の法律、政府規制などの法的要件にとって代わるものではありません。

次の表は、カード会員データとセンシティブ認証データの一般的な構成要素、そのデータの**保存**が許可されるか禁止されるか、各データ要素を**保護する**必要があるかどうかを示したものです。この表は完全なものではありません。その目的は、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に限定されます。

		データ要素	保存の許可	要件 3.4 に従って、保存されたアカウント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
	センシティブ認証データ[1]	完全な磁気ストライプデータ[2]	いいえ	要件 3.2 に従って保存できない
		CAV2/CVC2/CVV2/CID	いいえ	要件 3.2 に従って保存できない
		PIN/PIN ブロック	いいえ	要件 3.2 に従って保存できない

PCI DSS 要件 3.3 と 3.4 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。

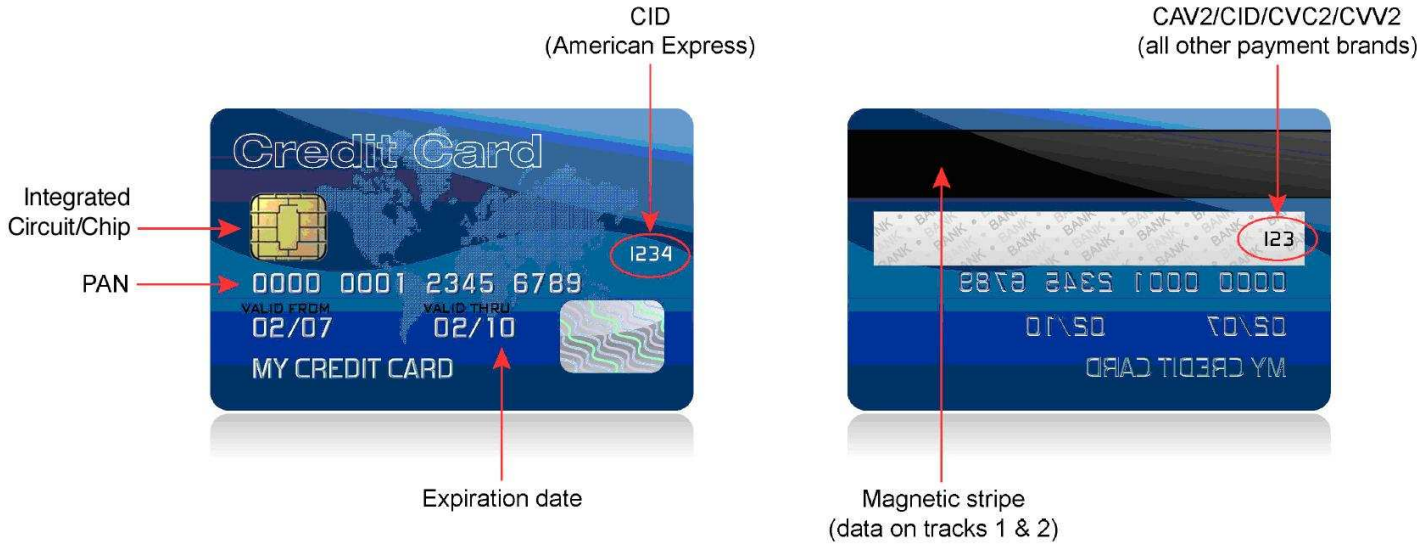
PCI DSS は PAN が保存、処理、または送信される場合にのみ適用されます。

1 センシティブ認証データは承認後、（たとえ暗号化していても）保存してはなりません。

2 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

カード会員データとセンシティブ認証データの位置

センシティブ認証データは、磁気ストライプ（またはトラック）データ[3]、カード検証コードまたは値[4]、および PIN データで構成されます。[5]。**センシティブ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人々にとって非常に貴重です。「センシティブ認証データ」の完全な定義については、『PCI DSS と PA-DSS の用語集（用語、略語、および頭字語）』を参照してください。以下のクレジットカードの前面と背面の写真に、カード会員データとセンシティブ認証データの位置を示します。



注:
チップにはトラックに相当するデータとその他のセンシティブデータが記録されています。これらのデータには、集積回路（IC）チップカード検証値（チップ CVC、iCVV、CAV3、または iCSC とも呼ばれる）などが含まれます。

---

3 カードを提示する取引中に、承認のために使用される磁気ストライプにエンコードされたデータ。このデータは、チップ上、またはカード上のその他の場所にある場合もあります。取引承認の後、事業体は磁気ストライプデータ全体を保持してはいけません。保持できるトラックデータの要素は、プライマリアカウント番号、カード会員名、有効期限、サービスコードのみです。

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

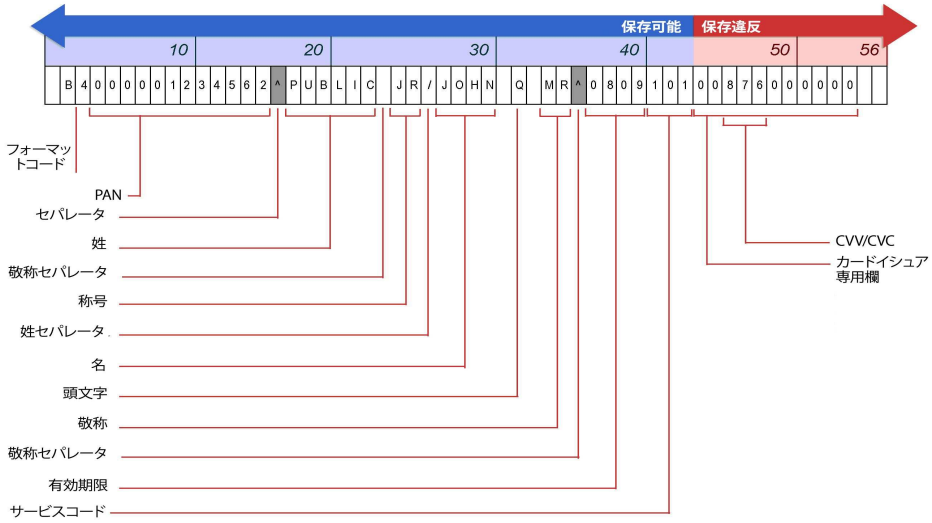
5 カードを提示する取引中に、カード会員によって入力される個人識別番号、または取引メッセージ内に存在する暗号化された PIN ブロック、あるいはその両方。

トラック 1 およびトラック 2 のデータ

トラック（磁気ストライプ、チップ内の磁気ストライプイメージ、またはその他の場所からのトラック 1 またはトラック 2 のいずれか）の全データが保存される場合、そのデータを入手した悪意のある人々はペイメントカードを複製して世界中で販売することができます。全トラックデータの保存は、ペイメントブランドの運用規定にも違反し、罰金または罰則が科せられる可能性があります。以下の図に、トラック 1 とトラック 2 のデータの違いと、磁気ストライプに保存されるときのデータのレイアウトを示します。

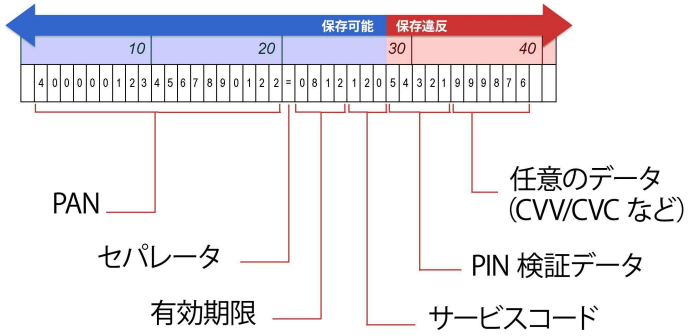
トラック 1

- トラック 1 とトラック 2 両方のすべてのフィールドを含む
- 長さは最大 79 文字



トラック 2

- 旧式のダイヤルアップ送信用に処理時間を短縮
- 長さは最大 40 文字



注:

任意のデータのフィールドはカードイシュアまたはペイメントカードブランド（あるいはその両方）によって定義されます。イシュア/ペイメントブランドによってセンシティブ認証データとみなされないデータが記入されたイシュア定義フィールドは、トラックの任意のデータの部分に含めることができます。この特殊なデータはイシュアまたはペイメントカードブランド（あるいはその両方）による定義に従って一定の状況および条件下で保存できます。

センシティブ認証データとみなされるデータは、任意のデータのフィールドに記入されている場合も、その他の場所に記入されている場合も、承認後に保存できません。

PCI データセキュリティ基準の関連ガイダンス

安全なネットワークの構築と維持

要件 1: カード会員データを保護するために、ファイアウォールをインストールして構成を維持する

要件 2: システムパスワードおよび他のセキュリティパラメータにベンダ提供のデフォルト値を使用しない

カード会員データの保護

要件 3: 保存されたカード会員データを保護する

要件 4: オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化する

脆弱性管理プログラムの整備

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

要件 6: 安全性の高いシステムとアプリケーションを開発し、保守する

強固なアクセス制御手法の導入

要件 7: カード会員データへのアクセスを、業務上必要な範囲内に制限する

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

要件 9: カード会員データへの物理アクセスを制限する

ネットワークの定期的な監視およびテスト

要件 10: ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する

要件 11: セキュリティシステムおよびプロセスを定期的にテストする

情報セキュリティポリシーの整備

要件 12: すべての担当者の情報セキュリティポリシーを整備する

要件 1 と 2 のガイダンス: 安全なネットワークの構築と維持

要件 1: カード会員データを保護するために、ファイアウォールをインストールして構成を維持する

ファイアウォールは事業体のネットワーク（社内）と信頼できないネットワーク（外部）とのコンピュータトラフィック、および事業体の信頼できる内部ネットワーク内の機密性の高い領域へのトラフィックを制御する装置です。事業体の信頼できるネットワーク内の非常に機密性の高い領域の例として、カード会員データ環境が挙げられます。

ファイアウォールはすべてのネットワークトラフィックを調査して、指定されたセキュリティ基準を満たさない伝送をブロックします。

すべてのシステムは、電子商取引、従業員のデスクトップブラウザからのインターネットアクセス、従業員の電子メールによるアクセス、B2B 接続などの専用接続、ワイヤレスネットワーク、その他のソースを介したシステムへのアクセスなど、信頼できないネットワークからの不正なアクセスから保護されなければなりません。しばしば、信頼できないネットワークへの（からの）問題ないように思われるアクセス経路が、重要なシステムへの侵入経路になっていることがあります。ファイアウォールは、すべてのコンピュータネットワークのための、重要な保護メカニズムです。

要件 1
に記載されているファイアウォールの最小要件を他のシステムコンポーネントが満たしている場合は、それらのファイアウォール機能を利用できます。カード会員データ環境内の他のシステムコンポーネントのファイアウォール機能を使用している場合は、要件 1
の評価範囲にそれらの装置が含まれている必要があります。

要件	ガイダンス
1.1 以下の項目を含むファイアウォールおよびルーター構成基準を確立する。	ファイアウォールとルーターは、ネットワークへの出入りを管理するアーキテクチャの重要コンポーネントです。これらのデバイスは、不要なアクセスをブロックし、ネットワークに出入りする承認済みアクセスを管理するソフトウェアまたはハードウェアデバイスです。ファイアウォールとルーターの構成方法をスタッフに指示する文書化されたポリシーと手順が存在しないと、企業はデータ保護のための防御の第一線を容易に失うことになります。ポリシーと手順は、データを保護するための組織における防御の第一線の強度を維持するのに役立ちます。 データフローが物理ネットワークを通過しない仮想環境には、適切なネットワークセグメンテーションを行って対処する必要があります。
1.1.1 すべてのネットワーク接続およびファイアウォール/ルーター構成への変更を承認およびテストする正式なプロセス	ファイアウォールとルーターへのすべての接続と変更を承認およびテストするポリシーとプロセスは、ネットワーク、ルーター、またはファイアウォールの誤った構成により発生するセキュリティ上の問題を防ぐのに役立ちます。 仮想マシン間のデータフローをポリシーとプロセスに含める必要があります。

要件	ガイダンス
1.1.2 ワイヤレスネットワークを含む、カード会員データへのすべての接続を示す最新ネットワーク図	ネットワーク図により、組織はすべてのネットワークデバイスの位置を把握できます。さらに、ネットワーク図を使用してネットワーク内および個々のデバイス間のカード会員データのデータフローをマッピングすることで、カード会員データ環境の範囲を完全に理解することができます。最新のネットワーク図およびデータフロー図がないと、カード会員データを含むデバイスが見過ごされ、PCI DSS 用に実装されるレイヤ化されたセキュリティコントロールから意図せずに外れ、侵害を受けやすくなる可能性があります。 ネットワーク図およびデータフロー図に仮想システムコンポーネントを含め、ホスト内データフローを文書化する必要があります。
1.1.3 各インターネット接続、および DMZ（demilitarized zone）と内部ネットワークゾーンとの間のファイアウォール要件	対してファイアウォールを使用することで、組織は着信アクセスと発信アクセスを監視および管を最小限に抑えることができます。
1.1.4 ネットワークコンポーネントを論理的に管理するためのグループ、役割、責任に関する記述	この役割と責任の割り当ての記述により、すべてのコンポーネントに対して、特定の人物がそのセキュリティに明確に責任を負い、責任を認識するとともに、管理されない状態のままになるデバイスを確実になくします。
1.1.5 使用が許可されているすべてのサービス、プロトコル、ポートの文書化、および使用が許可されている業務上の理由（安全でないとみなされているプロトコルに実装されているセキュリティ機能の文書化など）。 安全でないサービス、プロトコル、ポートの例として、FTP、Telnet、POP3、IMAP、SNMP などがある。	未使用または安全でないサービスとポートには、多くの既知の脆弱性があるため、多くの場合、侵害はこれらが原因で発生します。多くの組織は、（その脆弱性がいまだに存在するにもかかわらず）使用しないサービス、プロトコル、ポートのセキュリティ脆弱性のパッチ処理を行わないため、これらの種類の侵害に対して脆弱になっています。各組織は、どのサービス、プロトコル、ポートがビジネスにとって必要かを明確に決定し、記録のために文書化し、その他のサービス、プロトコル、ポートはすべて無効にするか削除する必要があります。また、組織は、これらのポートのトラフィックをすべてブロックし、必要性が決定されて文書化された場合にのみ、ポートを再度開くことを検討する必要があります。 さらに、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サービス、プロトコル、またはポート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）場合があります。これらの安全でないサービス、プロトコル、またはポートが業務上必要な場合、これらのプロトコルの使用によってもたらされるリスクが組織によって明確に理解および承認され、プロトコルの使用が正当化され、さらにこれらのプロトコルを安全に使用できるようにするセキュリティ機能が文書化されて実装されている必要があります。これらの安全でないサービス、プロトコル、またはポートがビジネスにとって不要な場合は、無効にするか削除する必要があります。

要件	ガイダンス
1.1.6 ファイアウォールおよびルーターのルールセットは少なくとも 6 カ月ごとにレビューされる必要がある	このレビューにより、組織は少なくとも 6 カ月ごとに不要、期限切れ、または不正なルールを取り除くことができ、すべてのルールセットで業務上の正当な理由に一致する承認済みのサービスとポートのみが許可されていることを確認できます。 これらのレビューを月に 1 回など、もっと頻繁に実施し、ルールセットが最新で、セキュリティホールが開かれたり不要なリスクを引き起こしたりすることなくビジネスのニーズを満たしていることを確認することをお勧めします。
1.2 信頼できないネットワークとカード会員データ環境内のすべてのシステムコンポーネントとの接続を制限するファイアウォール/ルーター構成を構築する。 ***注:*** *「信頼できないネットワーク」とは、レビュー対象の事業体に属するネットワーク外のネットワーク、または事業体の制御または管理が及ばないネットワーク（あるいはその両方）のことである。*	内部の信頼できるネットワークと、外部にある、または事業体の制御または管理が及ばないその他の信頼できないネットワークとの間にネットワーク保護、つまり少なくともステートフルインスペクションファイアウォール機能を備えたシステムコンポーネントをインストールすることは不可欠です。この手段を正しく実装しないと、事業体は悪意のある人々やソフトウェアによる不正アクセスに対して脆弱になります。 ファイアウォール機能がインストールされていても、特定のトラフィックを制御または制限するルールがなければ、脆弱なプロトコルとポートを利用して、悪意のある人々によりネットワークが攻撃される可能性があります。
1.2.1 着信および発信トラフィックを、カード会員データ環境に必要なトラフィックに制限する。	この要件は、悪意のある人々が不正な IP アドレス経由で組織のネットワークにアクセスしたり、不正な方法でサービス、プロトコル、またはポートを使用（組織のネットワーク内から取得したデータを信頼できないサーバに送出するなど）したりするのを防止することを目的としています。 すべてのファイアウォールに、具体的に必要とされていない着信および発信トラフィックをすべて拒否するルールを含める必要があります。これにより、意図しない、有害の可能性があるその他のトラフィックの着信または発信を可能にするセキュリティホールが不用意に開かれるのを防ぐことができます。

要件	ガイダンス
1.2.2 ルーター構成ファイルをセキュリティ保護および同期化する。	実行中の構成ファイルは通常、安全な設定で実装されますが、スタートアップファイル（ルーターは再起動時にのみこれらのファイルを実行します）は実行頻度が低いため同じ安全な設定で実装されない場合があります。ルーターが実行中の構成ファイルと同じ安全な設定で再起動されない場合、スタートアップファイルが実行中の構成ファイルと同じ安全な設定で実装されず、弱いルールが適用され、悪意のある人々によりネットワークに侵入される可能性があります。

要件	ガイダンス
1.2.3 すべてのワイヤレスネットワークとカード会員データ環境の間に境界ファイアウォールをインストールし、ワイヤレス環境からカード会員データ環境へのすべてのトラフィックを拒否または制御するように（そのようなトラフィックが業務上必要な場合）ファイアウォールを構成する。	ネットワーク内のワイヤレステクノロジの既知の（または不明な）実装および利用は、悪意のある人々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。ワイヤレスデバイスまたはネットワークが企業の知らない間にインストールされた場合、悪意のある人々はネットワークに容易に、かつ「認識されずに」侵入できます。ファイアウォールがワイヤレスネットワークからペイメントカード環境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人々は、容易にペイメントカード環境に接続し、アカウント情報を侵害することができます。 ワイヤレスネットワークが接続されている環境の目的に関係なく、すべてのワイヤレスネットワークと CDE の間にファイアウォールをインストールする必要があります。これには企業ネットワーク、小売店、倉庫などの環境も含まれます。
1.3 カード会員データ環境内にあるすべてのシステムコンポーネントとインターネット間における直接のパブリックアクセスを禁止する。	ファイアウォールの目的は、公共システムと内部システム（特にカード会員データを保存、処理、または伝送するシステム）との間のすべての接続を管理および制御することです。公共システムと CDE との間で直接のアクセスが許可されている場合、ファイアウォールが提供する保護が迂回され、カード会員データを保存するシステムコンポーネントが侵害にさらされる可能性があります。
1.3.1 DMZ を実装し、誰でもアクセス可能な承認済みのサービス、プロトコル、ポートを提供するシステムコンポーネントにのみ着信トラフィックを制限する。	DMZ は、インターネット（またはその他の信頼できないネットワーク）と組織が公開する必要がある内部サービス（Web サーバなど）との間の接続を管理するネットワークの一部です。内部ネットワークと通信する必要があるトラフィックをそうでないトラフィックから分離して隔離する、防御の第一線です。 この機能は、悪意のある人々が不正な IP アドレス経由で組織のネットワークにアクセスしたり、不正な方法でサービス、プロトコル、またはポートを使用したりするのを防止することを目的としています。
1.3.2 着信インターネットトラフィックを DMZ 内の IP アドレスに制限する。	IP 接続を DMZ で停止することにより、送信元/宛先の検査および制限や、コンテンツの検査/ブロックを行い、信頼できない環境と信頼できる環境との間のフィルタ処理されていないアクセスを阻止することができます。

要件	ガイダンス
1.3.3 インターネットとカード会員データ環境間トラフィックの、すべての直接接続（着信/発信）を使用不可にする。	着信と発信の両方の IP 接続を停止することにより、送信元/宛先の検査および制限や、コンテンツの検査/ブロックを行い、信頼できない環境と信頼できる環境との間のフィルタ処理されていないアクセスを阻止することができます。この要件は、悪意のある人々が組織のネットワーク内から取得したデータを信頼できないネットワーク内にある外部の信頼できないサーバに送出したりするのを防止することを目的としています。
1.3.4 インターネットから DMZ 内へ通過できる内部アドレスを使用不可にする。	通常、パケットには、最初にそのパケットを送信したコンピュータの IP アドレスが含まれます。これにより、ネットワーク内の他のコンピュータはパケットの送信元を知ることができます。場合によっては、この送信元 IP アドレスが悪意のある人々によってスプーフィング（盗用、およびなりすまし）されることがあります。 たとえば、悪意のある人々は、内部の正当なトラフィックであるように見せかけて、パケットを（ファイアウォールで禁止されていない場合に）インターネットからネットワークに送り込めるよう、スプーフィングしたアドレスを使用して送信します。いったんネットワーク内部に入ると、悪意のある人々はシステムの侵害を開始します。 Ingress フィルタリングは、ネットワークに入ってくるパケットをフィルタリングして、パケットが内部ネットワークから送信されたものであるかのように「スプーフィング」されていないことを特に確認するためにファイアウォール上で使用できるテクニックです。 パケットフィルタリングの詳細については、「Egress フィルタリング」と呼ばれる結果テクニックに関する情報の入手を検討してください。
1.3.5 カード会員データ環境からインターネットへの不正な発信トラフィックを使用不可にする。	カード会員データ環境から発信されるすべてのトラフィックも評価して、発信トラフィックが確立され、承認されたルールに確実に従うようにする必要があります。接続を検査して、許可された通信のみにトラフィックを制限する必要があります（送信元/宛先のアドレス/ポートの制限やコンテンツのブロックなど）。 一切の着信接続を許可しない環境では、発信接続は割り込みによって IP 接続を検査するアーキテクチャまたはシステムコンポーネントによって実現できます。
1.3.6 動的パケットフィルタリングとも呼ばれる、ステートフルインスペクションを実装する。（ネットワーク内へは、「確立された」接続のみ許可される。）	ステートフルパケットインスペクションを実行するファイアウォールは、ファイアウォールへの各接続の「ステート」（状態）を保持します。「ステート」を保持することで、ファイアウォールは以前の接続への応答であるように見えるものが本当に応答なのか、それとも悪意のある人々やソフトウェアが、スプーフィングしたりファイアウォールをだましたりして接続の許可を得ようとしているのかを判断できます（以前の接続を「覚えている」ため）。

要件	ガイダンス
1.3.7 DMZ や信頼できないネットワークから分離された内部ネットワークゾーンに、カード会員データ（データベースなど）を保存するシステムコンポーネントを配置する。	カード会員データは、最高レベルの情報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。 ***注:*** *揮発性メモリへの保存はこの要件の趣旨に含まれません。*
1.3.8 プライベート IP アドレスとルート情報を信頼できない関係者に開示しない。 ***注****: IP* *アドレス指定を隠す方法には、たとえば以下のような方法がある。* ▪ *ネットワークアドレス変換（NAT）* ▪ *カード会員データを保持するサーバをプロキシサーバ/ファイアウォールの背後またはコンテンツキャッシュに配置する。* ▪ *登録されたアドレス指定を使用するプライベートネットワークのルートアドバタイズを削除するか、フィルタリングする。* ▪ *登録されたアドレスの代わりに RFC1918 アドレス領域を内部で使用する。*	IP アドレスのブロードキャストを制限することは、ハッカーに内部ネットワークの IP アドレスを「知られ」て、この情報をネットワークへのアクセスに使用されることを防ぐために不可欠です。 この要件の目的を満たすための有効な手段は、環境内で使用しているネットワークテクノロジによって異なる場合があります。たとえば、この要件を満たすために使用するコントロールは、IPv4 ネットワークの場合と IPv6 ネットワークの場合とで異なる可能性があります。 IPv4 ネットワークで IP アドレス情報が検出されることを防ぐ方法の 1 つに、ネットワークアドレス変換（NAT）の実装があります。通常ファイアウォールによって管理される NAT により、組織はネットワーク内部でのみ表示可能な内部アドレスと、外部に表示される外部アドレスを持つことができます。ファイアウォールが内部ネットワークの IP アドレスを「非表示」にしたりマスクしたりしない場合、悪意のある人々が内部 IP アドレスを検出し、スプーフィングした IP アドレスを使用してネットワークへのアクセスを試みる可能性があります。 IPv4 ネットワークでは、内部アドレス指定用に予約されている RFC1918 アドレス空間をインターネット上でルーティング可能にすることは禁じられています。したがって、RFC1918 アドレス空間は内部ネットワークの IP アドレス指定に適しています。ただし、組織の事情によっては、内部ネットワークに非 RFC1918 アドレス空間を使用する場合があります。このような場合、ルートアドバタイズなどの技法を防止することによって、内部アドレス空間がインターネット上でブロードキャストされること、または不正な関係者に公開されることを防ぐ必要があります。

要件	ガイダンス
1.4 インターネットに直接接続するすべてのモバイルコンピュータまたは従業員所有のコンピュータ（あるいはその両方）で、企業ネットワークへのアクセスに使用されるものに（従業員が使用するラップトップなど）、パーソナルファイアウォールソフトウェアをインストールする。	コンピュータにファイアウォールまたはアンチウィルスプログラムがインストールされていない場合、スパイウェア、トロイの木馬、ウィルス、ワーム、ルートキット（マルウェア）が知らないうちにダウンロードされたりインストールされたりする可能性があります。インターネットに直接接続され、企業ファイアウォールの背後にない場合、コンピュータはさらに脆弱性が高くなります。企業ファイアウォールの背後にない場合にコンピュータに読み込まれたマルウェアは、コンピュータが企業ネットワークに再接続されたときに、ネットワーク内の情報を悪意をもってターゲットにすることができます。 ***注:*** *この要件は、所有者が従業員であるか、会社であるかに関係なく、リモートアクセスコンピュータを適用対象とします。会社のポリシーで管理できないシステムは境界に弱点をもたらし、悪意のある人々により攻撃される可能性があります。*

要件 2: システムパスワードおよびその他のセキュリティパラメータにベンダ提供のデフォルト値を使用しない

（社内外の）悪意のある人々は多くの場合、ベンダのデフォルトパスワードおよびベンダのその他のデフォルト設定を使用して、システムを脅かします。これらのパスワードと設定はハッカーの間でよく知られており、公開情報を通じて容易に特定できます。

要件	ガイダンス
2.1 ネットワークにシステムをインストールする**前に**ベンダ提供のデフォルト値を必ず変更する。これには、パスワード、簡易ネットワーク管理プロトコル（SNMP）コミュニティ文字列の変更、不必要なアカウントの削除が含まれる（ただし、これらに限定されない）。	悪意のある人々（社内外にかかわらず）は多くの場合、ベンダのデフォルト設定、アカウント名、およびパスワードを使用して、システムを侵害します。これらの設定はハッカーの間でよく知られており、そのままにしておくと攻撃に対するシステムの脆弱性が非常に高くなります。
2.1.1 カード会員データ環境に接続されている、またはカード会員データを伝送するワイヤレス環境の場合、ワイヤレスベンダのデフォルト値を変更する。これには、デフォルトのワイヤレス暗号化キー、パスワード、SNMP コミュニティ文字列が含まれる（ただし、これらに限定されない）。	多くのユーザは、管理者による承認を得ずにこれらのデバイスをインストールして、デフォルト設定の変更やセキュリティ設定の構成を行いません。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。さらに、古いバージョンの 802.11x 暗号化（WEP）用のキー交換プロトコルは破られており、暗号化が役に立たなくなっている可能性があります。デバイスのファームウェアが WPA2 などの安全性の高いプロトコルをサポートするように更新されていることを確認します。
2.2 すべてのシステムコンポーネントについて、構成基準を作成する。この基準は、すべての既知のセキュリティ脆弱性をカバーし、また業界で認知されたシステム強化基準と一致している必要がある。 業界で認知されたシステム強化基準のソースには以下が含まれる（これらに限定されない）。 ▪ Center for Internet Security（CIS） ▪ 国際標準化機構（ISO） ▪ SysAdmin Audit Network Security（SANS） ▪ 米国国立標準技術研究所（NIST）	多くのオペレーティングシステム、データベース、エンタープライズアプリケーションには既知の弱点があります。また、セキュリティの脆弱性を修正するようにこれらのシステムを構成する既知の方法もあります。セキュリティの専門家でない人々のために、セキュリティ組織ではシステム強化に関する推奨事項を確立し、これらの弱点を修正する方法についてアドバイスしています。弱いファイル設定または（しばしば必要としないサービスまたはプロトコルの）デフォルトのサービスとプロトコルなど、これらの弱点がシステムに残されている場合、攻撃者は、既知である複数のセキュリティ上の弱点を利用して、脆弱なサービスとプロトコルを攻撃し、組織のネットワークにアクセスすることができます。構成基準の実装に役立つ業界のベストプラクティスの詳細については、www.nist.gov、www.sans.org、www.cisecurity.org、www.iso.org などのソース Web サイトを参照してください。 システムをネットワーク上にインストールする前に、新たに発見された弱点を確実に修正するためには、システム構成基準を最新状態に保つ必要もあります。

要件	ガイダンス
2.2.1 同じサーバに異なったセキュリティレベルを必要とする機能が共存しないように、1つのサーバには、主要機能を 1 つだけ実装する。（たとえば、Web サーバ、データベースサーバ、DNS は別々のサーバに実装する必要がある。） ***注:*** *仮想化技術が使用されている場合は、1 つの仮想システムコンポーネントには、主要機能を 1 つだけ実装する。*	この目的は、組織のシステム構成基準と関連プロセスによって、さまざまなセキュリティレベルを備える必要がある、または同じサーバ上の他の機能にセキュリティ上の弱点をもたらす可能性があるサーバ機能に確実に対処することです。例: 1. 強力なセキュリティ手段を講じる必要があるデータベースは、オープンでインターネットに直接接続する必要がある Web アプリケーションとサーバを共有するとリスクにさらされます。 2. 一見マイナーな機能にパッチを適用せずにいると、同じサーバ上の他のより重要な機能（データベースなど）に影響を及ぼす侵害が発生する可能性があります。 この要件は、カード会員データ環境内のすべてのサーバ（通常は Unix、Linux、または Windows ベース）を対象としています。この要件は、単一サーバ上でセキュリティレベルをネイティブに実装する機能を持つシステム（メインフレームなど）には適用されない場合があります。 仮想化技術が使用されている場合は、各仮想コンポーネント（仮想マシン、仮想スイッチ、仮想セキュリティ機器など）を「サーバ」境界とみなす必要があります。ハイパーバイザによってサポートする機能が異なる場合がありますが、単一の仮想マシンには「主要機能を 1 つだけ」実装するというルールは厳守する必要があります。この場合、ハイパーバイザの侵害によってすべてのシステム機能が侵害される可能性があります。そのため、単一の物理システムに複数の機能またはコンポーネントを配置する場合のリスクレベルについても考慮する必要があります。
2.2.2 システムの機能に必要な安全性の高いサービス、プロトコル、デーモンなどのみを有効にする。 安全でないとみなされている必要なサービス、プロトコル、またはデーモンにセキュリティ機能を実装する。たとえば、SSH、S-FTP、SSL、または IPSec VPN などの安全なテクノロジを使用して、NetBIOS、ファイル共有、Telnet、FTP などの安全性の低いサービスを保護する。	要件 1.1.5 に記述されているとおり、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業務上必要となる（またはデフォルトで有効になっている）場合があります。新しいサーバを導入する前に、必要なサービスとプロトコルのみを有効にし、すべての安全でないサービスとプロトコルに十分なセキュリティを施すことを確実にするためには、この要件を組織の構成基準と関連プロセスの一部にする必要があります。
2.2.3 システムの誤用を防止するためにシステムセキュリティパラメータを構成する。	この目的は、組織のシステム構成基準と関連プロセスによって、セキュリティへの影響があることが明らかであるセキュリティ設定およびパラメータを確実に設定することです。

要件	ガイダンス
2.2.4 スクリプト、ドライバ、機能、サブシステム、ファイルシステム、不要な Web サーバなど、不要な機能をすべて削除する。	サーバ強化基準には、セキュリティに特定の影響を与える不要な機能に対応するプロセス（サーバが FTP または Web サーバ機能を実行しない場合、これらの機能を削除/無効化するなど）が含まれている必要があります。
2.3 強力な暗号化を使用して、すべてのコンソール以外の管理アクセスを暗号化する。Web ベースの管理やその他のコンソール以外の管理アクセスについては、SSH、VPN、または SSL/TLS などのテクノロジを使用する。	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。悪意のある人々は、この情報を使用してネットワークにアクセスし、管理者となってデータを盗むことができます。
2.4 共有ホスティングプロバイダは、各事業体のホスト環境およびカード会員データを保護する必要がある。これらのプロバイダは、「付録 A: 共有ホスティングプロバイダ向けの PCI DSS 追加要件」に詳しく説明されている要件を満たす必要がある。	これは、同じサーバ上で複数のクライアント向けの共有ホスティング環境を提供するホスティングプロバイダを対象としています。すべてのデータが同じサーバ上にあり、単一の環境の管理下にあると、多くの場合、これらの共有サーバの設定が個々のクライアントから管理できず、クライアントはその他のすべてのクライアント環境のセキュリティに影響を及ぼす安全でない機能やスクリプトを追加できるため、悪意のある人々はあるクライアントのデータを容易に侵害でき、さらにその他のすべてのクライアントのデータにアクセスすることができます。付録 A を参照してください。

要件 3 と 4 のガイダンス: カード会員データの保護

要件 3: 保存されたカード会員データを保護する

暗号化、トランケーション、マスキング、ハッシュなどの保護方式は、カード会員データ保護のための重要な要素です。侵入者が他のセキュリティコントロールを回避し、暗号化されたデータにアクセスできても、正しい暗号化キーがなければ、そのデータを読み取り、使用することはできません。保存したデータを保護するための効果的な別の方法として考えられるのは、リスクを軽減する方法です。たとえば、リスクを最小限にする方法として、カード会員データが絶対的に必要でない限り保存しない、完全な PAN が不要ならカード会員データを切り捨てる、電子メールやインスタントメッセージングなどのエンドユーザメッセージング技術を使用して保護されていない PAN を送信しない、などがあります。

「強力な暗号化技術」および他の PCI DSS 用語については、『PCI DSS Glossary of Terms, Abbreviations, and Acronyms』を参照してください。

要件	ガイダンス
3.1 次のようにデータの保存と破棄に関するポリシー、手順、プロセスを実装して、保存するカード会員データを最小限に抑える。 **3.1.1** 以下を含むデータの保存と破棄に関するポリシーを実施する。 ▪ 保存するデータ量と保存期間を、法律上、規則上、業務上必要な範囲に限定する。 ▪ 必要性がなくなった場合のデータを安全に削除するためのプロセス ▪ カード会員データの特定のデータ保存要件 ▪ 定義した保存要件を超えて保存されているカード会員データを識別および安全に削除するための四半期ごとの自動または手動のプロセス	正式なデータ保存ポリシーで、保存する必要があるデータとそのデータの保存場所を識別し、不要になった場合は即座に安全な方法で破棄または削除できるようにしておきます。適切な保存要件を定義するには、まず、事業体は固有のビジネスニーズと、業界または保存するデータの種類（あるいはその両方）に適用される法律上または規則上の義務を理解する必要があります。 カード会員データを業務上必要な範囲を越えて保存すると、不要なリスクが発生します。承認後に保存できるカード会員データは、プライマリアカウント番号（PAN）（読み取り不能に処理したもの）、有効期限、カード会員名、サービスコードのみです。 安全な削除方法を実装することにより、不要になったデータを確実に取得できなくします。 **必要ない場合は、保存してはいけません。**

要件	ガイダンス
3.2 承認後にセンシティブ認証データを保存しない（暗号化されている場合でも）。 センシティブ認証データには、以降の要件 3.2.1 ～ 3.2.3 で言及されているデータを含む。 ***注:*** *サービスの発行をサポートする発行者および会社は、業務上の理由がある場合やデータが安全に保存されている場合は、センシティブ認証データを保存できる。*	センシティブ認証データは、磁気ストライプ（またはトラック）データ[6]、カード検証コードまたは値[7]、および PIN データで構成されます。[8]。**承認後のセンシティブ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人々にとって非常に貴重です。「センシティブ認証データ」の完全な定義については、『PCI DSS と PA-DSS の用語集（用語、略語、および頭字語）』を参照してください。 ***注:*** *サービスの発行を実施、推進、またはサポートする会社は、業務上の正当な理由がある場合に限り、センシティブ認証データを保存できます。イシュアにはすべての PCI DSS 要件が適用されますが、イシュアとイシュアプロセサーにとって唯一の例外は、業務上の正当な理由がある場合はセンシティブ認証データを保存できるということです。正当な理由とは、イシュアが提供する機能の遂行に必要で、単なる利便性を目的としない理由のことです。* *これらのデータは PCI DSS および個別のペイメントブランド要件に従って安全に保存する必要があります。*

6 カードを提示する取引中に、承認のために使用される磁気ストライプにエンコードされたデータ。このデータは、チップ上、またはカード上のその他の場所にある場合もあります。取引承認の後、事業体は磁気ストライプデータ全体を保持してはいけません。保持できるトラックデータの要素は、プライマリアカウント番号、カード会員名、有効期限、サービスコードのみです。

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

8 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。

要件	ガイダンス
3.2.1 （カードの背面やチップ上の同等のデータ上などにある磁気ストライプの）いかなるトラックデータのいかなる内容も保存しない。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呼ばれることもある。 ***注:*** *通常の業務範囲では、磁気ストライプの以下のデータ要素を保存する必要が生じる場合がある。* ▪ *カード会員名* ▪ *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、業務上必要なデータ要素のみを保存する。*	もし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人々はペイメントカードを複製し、販売することができます。
3.2.2 カードを提示しない取引を検証するために使用された、カード検証コードまたは値（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。	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。これらの種類の取引は、カード所有者から取引が開始されたときにこのカード検証コードを要求するだけで認証することができます。カード所有者はカードを手元に持っていて、値を読み取ることができるためです。この禁止されたデータが保存されていて盗まれた場合、悪意のある人々はインターネットおよび MO/TO 取引を偽造することができます。
3.2.3 個人識別番号（PIN）または暗号化された PIN ブロックを保存しない。	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。この禁止されたデータが保存されていて盗まれた場合、悪意のある人々は 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。

要件	ガイダンス
3.3 表示時に PAN をマスクする（最初の 6 桁と最後の 4 桁が最大表示桁数）。 ***注:*** ▪ *従業員およびその他の関係者が、業務上の合法的なニーズにより PAN 全体を見る必要がある場合、この要件は適用されない。* ▪ *カード会員データの表示に関するこれより厳しい要件（POS レシートなど）がある場合は、そちらに置き換えられる。*	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。「加盟店保管用」の領収書には PAN 全体を表示できます。ただし、紙の領収書は、電子コピーと同じセキュリティ要件に従い、PCI データセキュリティ基準のガイドライン、特に物理セキュリティに関する要件 9 に従う必要があります。業務上の合法的なニーズにより PAN 全体を見る必要がある場合も、PAN 全体を表示することができます。 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 3.4 と混同しないよう注意してください。

要件	ガイダンス
3.4 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）。 ▪ 強力な暗号化技術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。事業体の環境内に、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。*	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。主な保管場所（データベース、またはテキストファイルスプレッドシートなどのフラットファイル）およびそれ以外の保管場所（バックアップ、監査ログ、例外またはトラブルシューティングログ）に保存される PAN はすべて保護する必要があります。輸送中のバックアップテープの盗難または紛失による損害は、暗号化、トランケーション、またはハッシュによって PAN を読み取り不能にすることによって少なくすることができます。監査、トラブルシューティング、および例外ログは保持する必要があるため、ログ内の PAN を読み取り不能にする（または削除する）ことでログ内のデータの開示を防止することができます。 悪意のある個人は、特定の PAN 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。 「強力な暗号化技術」の定義については、『PCI DSS と PA-DSS の用語集（用語、略語、および頭字語）』を参照してください。
▪ 強力な暗号化技術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）	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（Secure Hash Algorithm（SHA）など）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）。 レインボーテーブルの作成を複雑にするために、ハッシュ関数に PAN と共に salt 値を入力することが推奨されますが、これは要件ではありません。

要件	ガイダンス
▪ 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）	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。これはマスキングとは異なります。マスキングでは、PAN 全体が保存されますが、表示時に PAN がマスキングされます（つまり、PAN の一部のみが画面、レポート、領収書などに表示されます）。 この要件はファイルやデータベースなどに*保存された* PAN の保護に関連します。画面や紙の領収書などに表示された PAN の保護に関する要件 3.3 と混同しないよう注意してください。
▪ 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）	インデックストークンとパッドを使用して、カード会員データを読み取り不能にすることもできます。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、ランダムに生成される秘密キーを 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。
▪ 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	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）』で定義およびキーの長さを参照してください）の目的は、暗号化のベースを（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。
3.4.1 （ファイルまたは列レベルのデータベース暗号化ではなく）ディスク暗号化が使用される場合、論理アクセスはネイティブなオペレーティングシステムのアクセス制御メカニズムとは別に管理する必要がある（ローカルユーザアカウントデータベースを使用しないなどの方法で）。暗号解除キーをユーザアカウントに結合させてはいけない。	この要件の目的は、カード会員データを読み取り不能にするためのディスク暗号化の許容基準を設定することです。ディスク暗号化は、コンピュータの大容量記憶装置に保存されたデータを暗号化し、権限のあるユーザが要求したときに情報を自動的に復号化します。ディスク暗号化システムは、オペレーティングシステムの読み取りおよび書き込み操作を遮断し、セッション開始時のパスワードまたはパスフレーズの入力以外、ユーザによる特別な操作を一切必要とせずに適切な暗号化変換を実行します。ディスク暗号化のこれらの特性に基づいてこの要件に準拠するには、ディスク暗号化方式で次のものを使用しないようにする必要があります。 1）オペレーティングシステムとの直接的な関連付け、または 2）ユーザアカウントと関連付けられている暗号解除キー。

要件	ガイダンス
3.5 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。 ***注:*** *この要件は、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る。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る。*	暗号化キーへのアクセスを取得するとデータを復号化できるため、暗号化キーは厳重に保護する必要があります。キー暗号化キーを使用する場合、データを暗号化するキーとそのキーで暗号化されたデータを適切に保護するには、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。 キーを開示と誤使用から保護するための要件は、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。1 つのキー暗号化キーで複数のデータ暗号化キーへのアクセスが付与される場合があるため、キー暗号化キーには強力な保護手段が必要です。キー暗号化キーの安全な保護手法には、ハードウェアセキュリティモジュール（HSM）、二重管理と知識分割による改ざん防止ストレージなどがあります。
3.5.1 暗号化キーへのアクセスを、必要最小限の管理者に制限する。	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）。
3.5.2 暗号化キーの保存場所と形式を最小限にし、安全に保存する。	暗号化キーは、通常はキー暗号化キーで暗号化して、安全に最小限の場所に保存する必要があります。この要件の目的は、キー暗号化キーを暗号化することではなく、要件 3.5 の定義に従って開示と誤使用から保護することです。キー暗号化キーを物理的または論理的（あるいはその両方）にデータ暗号化キーとは別の場所に保存することで、2 つのキーに不正アクセスされるリスクが軽減されます。
3.6 カード会員データの暗号化に使用される以下の暗号化キーのキー管理プロセスおよび手順をすべて文書化し、実装する。 ***注:*** *キー管理には多数の業界標準があり、NIST（http://csrc.nist.gov を参照）などさまざまなリソースから入手可能である。*	暗号化キーの管理方法は、暗号化ソリュ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 3.6.1 ～ 3.6.8 に対応させます。
3.6.1 強力な暗号化キーの生成	暗号化ソリューションは、『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。
3.6.2 安全な暗号化キーの配布	暗号化ソリュ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、3.5.1 で識別される管理者にのみ配布します。
3.6.3 安全な暗号化キーの保存	暗号化ソリューションはキーを安全に保存する必要があります。つまり、キーを平文で保存しません（キー暗号化キーで暗号化します）。

要件	ガイダンス
3.6.4 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。	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。 キーが暗号化期間の終了時点に到達した場合の暗号化キーの定期的な変更は、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。 暗号化アプリケーションベンダによってキーの定期的な変更に関するベンダの文書化されたプロセスまたは推奨事項が提供されている場合は、それらに従います。指定されたキーオーナーまたはキー管理者は、さまざまなアルゴリズムやキーの長さに関する適切な暗号化期間のガイダンスとして、暗号化アルゴリズムとキー管理に関する業界のベストプラクティス（たとえば、*NIST Special Publication 800-57*）を参照することもできます。 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。
3.6.5 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。キーの破棄または取替とは、たとえば、アーカイブ、破棄、または廃止（あるいはこれらのすべて）である。 ***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。*	使われなくなった、または不要になった古いキーは、破棄および破壊してキーを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ためなど）古い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。（3.6.6 を参照してください。）また、暗号化ソリューションでは、侵害が判明している、またはその疑いがあるキーを取り替えるプロセスを許可し、促進する必要があります。

要件	ガイダンス
3.6.6 平文暗号化キー管理を手動で操作する場合、キーの知識分割と二重管理を使用する必要がある（例: キー全体を再構築するには、2 ～ 3 人を必要とし、各自がキーの一部のみを知っている）。 ***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、破棄などが含まれる（これらに限定されない）。*	キーの知識分割と二重管理は、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。この管理は通常、手動のキー管理操作に、またはキー管理が暗号化製品によって実装されていない場合に適用されます。
3.6.7 暗号化キーの不正置換の防止。	暗号化ソリューションでは、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してはいけません。
3.6.8 暗号化キー管理者が自身の責務を理解し、それを受諾したことを正式に確認するための要件。	このプロセスにより、キー管理者がキー管理役割を誓約し、自身の責務を理解することを確実にします。

要件 4: オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化する

ネットワークには悪意のある人々が容易にアクセスできるため、機密情報をネットワーク経由で伝送する場合は暗号化する必要があります。誤って構成されたワイヤレスネットワーク、および従来の暗号化や認証プロトコルの脆弱性は、こうした脆弱性につけこんでカード会員データ環境への特権アクセスを取得する、悪意のある人々の標的となります。

要件	ガイダンス
4.1 オープンな公共ネットワーク経由で機密性の高いカード会員データを伝送する場合、強力な暗号化と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。 *PCI DSS の範囲内であ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。* ▪ *インターネット* ▪ *ワイヤレステクノロジ* ▪ *Global System for Mobile Communications（GSM）* ▪ *General Packet Radio Service（GPRS）*	悪意のある人々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。 Secure Sockets Layer（SSL）は、Web ページとそれらに入力されるデータを暗号化します。SSL でセキュリティ保護された Web サイトを使用するときは、URL の一部が「https」であることを確認します。 一部のプロトコルの実装（SSL バージョン 2.0 や SSH バージョン 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。どのセキュリティプロトコルを使用する場合も、安全な構成およびバージョンのみが使用され、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。

要件	ガイダンス
4.1.1 カード会員データを伝送する、またはカード会員データ環境に接続しているワイヤレスネットワークには、業界のベストプラクティス（IEEE 802.11i など）を使用して、認証および伝送用に強力な暗号化を実装する。 *注: セキュリティ制御としての WEP の使用は、2010 年 6 月 30 日をもって禁止された。*	悪意のあるユーザは、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、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。ワイヤード（有線）ネットワーク内にのみ保存されるカード会員データの既知の侵害の多くは、悪意のあるユーザが安全でないワイヤレスネットワークからアクセスを広げたときに発生しました。強力な暗号化が必要なワイヤレス実装の例として、GPRS、GSM、WIFI、衛星、Bluetooth などが挙げられます。 悪意のあるユーザがワイヤレスネットワークとそのネットワーク上のデータにアクセスしたり、ワイヤレスネットワークを利用してその他の内部ネットワーク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。WEP 暗号化は、WEP キー交換プロセス内の初期化ベクトルが弱く、必要な交換キーが不足しており脆弱であるため、ワイヤレスチャネル上のデータを暗号化する単独の手段として使用してはいけません。攻撃者は、無料で入手できる強力な解読ツールを使用して WEP 暗号化を容易に突破できます。 現在のワイヤレスデバイスを強力な暗号化をサポートするようにアップグレードする必要があります（例: アクセスポイントファームウェアを WPA2 にアップグレードする）。現在のデバイスをアップグレードできない場合は、新しい機器を購入するか、その他の代替コントロールを実装して、強力な暗号化を実装する必要があります。
4.2 保護されていない PAN をエンドユーザメッセージングテクノロジ（電子メール、インスタントメッセージング、チャットなど）で送信しない。	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。強力な暗号化を提供できる場合を除き、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。

要件 5 と 6 のガイダンス: 脆弱性管理プログラムの整備

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

一般に「マルウェア」と呼ばれる悪意のあるソフトウェア（ウィルス、ワーム、トロイの木馬など）は、従業員の電子メール、インターネット、モバイルコンピュータ、ストレージデバイスの使用など、業務上承認された活動を通じて、システムの脆弱性を利用してネットワークに侵入します。マルウェアの影響を受けやすいすべてのシステムで、アンチウィルスソフトウェアを使用して、最新の進化するマルウェアソフトウェアの脅威からシステムを保護する必要があります。

要件	ガイダンス
5.1 悪意のあるソフトウェアの影響を受けやすいすべてのシステム（特にパーソナルコンピュータとサーバ）に、アンチウィルスソフトウェアを導入する。	広く公開されるエクスプロイト（多くの場合「0 day Expolit」で、発見から 1 時間以内にネットワーク全体で公開されて広まります）を使用して、保護されているはずのシステムが絶えず攻撃されます。定期的にアンチウィルスソフトウェアを更新せずにいる場合、これらの新しい形式の悪意のあるソフトウェアにより、ネットワークが攻撃され、使用できなくなる恐れがあります。 悪意のあるソフトウェアは知らないうちにインターネットからダウンロードされたり、インストールされたりする場合がありますが、CD、DVD、USB メモリスティックおよびハードドライブ、デジタルカメラ、PDA（携帯情報端末）、その他の周辺機器などのリムーバブルストレージデバイスを使用しているときもコンピュータは脆弱になります。アンチウィルスソフトウェアがインストールされていないと、これらのコンピュータはネットワークへのアクセスポイントになり、ネットワーク内の情報が悪意をもって標的にされます。 悪意のあるソフトウェアによって一般的に影響を受けるシステムには、通常メインフレームやほとんどの Unix システムは含まれませんが（以下の詳細を参照してください）、各事業体には、PCI DSS 要件 6.2 に従って新しいセキュリティの脆弱性を識別して対応し、構成基準およびプロセスを適宜更新するためのプロセスが必要です。この要件を満たすため、別のソリューションで同じ脅威にシグネチャベースの手法以外の方法で対処することも許容されます。 事業体が使用するオペレーティングシステムに関連した悪意のあるソフトウェアの傾向を、新しいセキュリティの脆弱性の識別に含め、必要に応じて、新しい傾向への対応方法を企業の構成基準および保護メカニズムに組み込む必要があります。 通常、次のオペレーティングシステムは悪意のあるソフトウェアによって一般的に影響を受けません: メインフレーム、特定の Unix サーバ（AIX、Solaris、HP-Unix など）。ただし、悪意のあるソフトウェアの業界での傾向は急速に変化する可能性があり、各組織は要件 6.2

要件	ガイダンス
	に従って新しいセキュリティの脆弱性を識別して対応し、構成基準およびプロセスを適宜更新する必要があります。
5.1.1 すべてのアンチウィルスプログラムは、すべての既知のタイプの悪意のあるソフトウェアに対して検知、駆除、保護が可能でなければならない。	**すべての**種類および形式の、悪意のあるソフトウェアから保護することが重要です。
5.2 すべてのアンチウィルスメカニズムが最新で、有効に実行されており、監査ログが生成されることを確認する。	最高のアンチウィルスソフトウェアでも、アンチウィルス署名が最新でなかったり、ネットワークまたは個人のコンピュータで有効になっていなかったりする場合、その効果が制限されます。 監査ログで、ウィルスの活動とアンチウィルスの対応を監視することができます。監査ログを生成するようにアンチウィルスソフトウェアを構成し、ログを要件 10 に従って管理することが不可欠です。

要件 6: 安全性の高いシステムとアプリケーションを開発し、保守する

悪意のある人々は、セキュリティの脆弱性を利用して、システムへの特権アクセスを取得します。このような脆弱性の多くは、ベンダが提供するセキュリティパッチによって修正されます。システムを管理する事業体はこうしたパッチをインストールする必要があります。すべての重要なシステムは、最新リリースの適切なソフトウェアパッチを適用することにより、悪意のある人々および不正なソフトウェアによるカード会員データの不正使用および侵害から保護される必要があります。

注:
適切なソフトウェアパッチとは、既存のセキュリティ構成と競合しないことが十分に評価およびテストされたパッチを指します。自社開発アプリケーションの場合、標準のシステム開発プロセスと安全なコーディング技術を使用することで、多くの脆弱性を回避できます。

要件	ガイダンス
6.1 すべてのシステムコンポーネントとソフトウェアに、ベンダ提供の最新セキュリティパッチが適用され、既知の脆弱性から保護されている。重要なセキュリティパッチは、リリース後 1 カ月以内にインストールする。 ***注:*** *組織は、パッチインストールの優先順位を付けるために、リスクに基づくアプローチの適用を検討できる。たとえば、重要なインフラストラクチャ（一般に公開されているデバイス、システム、データベースなど）に重要性の低い内部デバイスよりも高い優先順位を付けることで、優先順位の高いシステムおよびデバイスは 1 カ月以内に対処され、重要性の低いシステムおよびデバイスは 3 カ月以内に対処されるようにする。*	広く公開されるエクスプロイト（多くの場合「0 day」で、1 時間以内に公開）を使用して、保護されているはずのシステムを狙う攻撃が大量に存在します。可能な限り迅速に重要なシステムに最新のパッチを実装しないと、悪意のある人々によりこれらのエクスプロイトが使用され、ネットワークが攻撃されて使用不可になる可能性があります。重要なシステムまたは危険な状態にあるシステムへの重要なセキュリティパッチを 30 日以内にインストールできる、その他の危険度の低い変更は 2 ～ 3 カ月内にインストールするよう、変更に優先順位を付けることを検討してください。

要件	ガイダンス
6.2 新たに発見されたセキュリティの脆弱性を特定し、リスクのランク分けを割り当てるためのプロセスを確立する。 ***注**:* *リスクのランク分けは、業界のベストプラクティスに基づいている必要がある。たとえば、「高」リスクの脆弱性とランク分けする基準には、CVSS のベーススコアが 4.0 以上であること、ベンダが提供するパッチがベンダによって「重要」と分類されていること、脆弱性が重要なシステムコンポーネントに影響することの 1 つ以上が含まれる。* *要件 6.2.a に定義された脆弱性のランク分けは、2012 年 6 月 30 日まではベストプラクティスとみなされ、それ以降は要件になる。*	この要件の目的は、組織の環境に影響を及ぼす可能性がある新しい脆弱性に関する情報を最新状態に保つことです。 ベンダによる製品関連の脆弱性やパッチに関するニュース告知を監視することと同様に、一般的な業界の脆弱性に関するニュースグループや、ベンダによってまだ知られていない、または解決されていない可能性がある脆弱性や可能な回避策に関するメーリングリストを監視することも重要です。 組織の環境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。それには、組織が脆弱性を評価し、リスクをランク分けするための一貫性のある方法を設ける必要があります。脆弱性を評価し、リスクをランク分けする方法は組織によって異なり、独自の CDE に基づいている可能性がありますが、一般に業界で認められたリスクのランク分けシステム（CVSS 2.0、NIST SP 800-30 など）に基づくことも可能です。 リスクの分類（「高」、「中」、「低」など）により、組織は優先順位の高いリスク項目をより迅速に特定して対処し、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。
6.3 PCI DSS（安全な認証やロギングなど）に従い、業界のベストプラクティスに基づいてソフトウェアアプリケーション（内部、外部、アプリケーションへの Web ベースの管理アクセス）を開発し、ソフトウェア開発ライフサイクル全体を通じて情報セキュリティを徹底させる。これらのプロセスには、以下の項目を含める必要がある。	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本番環境にもたらされる可能性があります。
6.3.1 アプリケーションがアクティブになる前、または顧客にリリースされる前に、カスタムアプリケーションアカウント、ユーザ ID、パスワードを削除する	カスタムアプリケーションアカウント、ユーザ ID、パスワードは、アプリケーションがアクティブになる前、または顧客にリリースされる前に本番環境コードから削除する必要があります。これらのアイテムは、アプリケーションの機能に関する情報を漏洩する場合があるためです。このような情報を保持していると、アプリケーションおよび関連するカード会員データの侵害を容易にする可能性があります。

要件	ガイダンス
6.3.2 コーディングの脆弱性がないことを確認するために、本番または顧客へのリリースの前に、カスタムコードをレビューする。 ***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、すべてのカスタムコード（内部および公開）に適用される。コードレビューは、知識を持つ社内担当者または第三者が実施できます。一般に公開されている Web アプリケーションも、実装後の脅威および脆弱性に対処するために、PCI DSS 要件 6.6 に定義されている追加コントロールの対象となる。*	カスタムコードのセキュリティの脆弱性は、悪意のある人々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。 コードレビューは、手動で実施することも、自動レビューツールを使用して行うこともできます。自動レビューツールにはコードをレビューして一般的なコーディングの誤りや脆弱性を検出する機能があります。自動レビューは便利なツールですが、一般にコードレビューの単独の手段として完全に信頼することはできません。自動ツールで特定が困難な、または特定が不可能なコードの問題を特定するには、コードレビューの知識と経験のある人がレビューのプロセスに関与する必要があります。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。
6.4 システムコンポーネントへのすべての変更において、変更管理のプロセスおよび手順に従う。これらのプロセスには、以下の項目を含める必要がある。	適切な変更管理がないと、セキュリティ機能が過失または故意によって省略あるいは動作不能にされたり、処理の不規則性が発生したり、悪意のあるコードが取り込まれる可能性があります。
6.4.1 開発/テスト環境と本番環境の分離	開発およびテスト環境は絶えず状態が変化するため、本番環境より安全性が低くなります。環境を適切に分離しないと、テストまたは開発環境の脆弱性のために本番環境およびカード会員データがリスクにさらされる可能性があります。
6.4.2 開発/テスト環境と本番環境での責務の分離	本番環境およびカード会員データにアクセスできる担当者の数を少なくすることにより、リスクは最小限に抑えられ、アクセスは業務上必要とするユーザのみに制限できます。 この要件の目的は、開発/テスト機能を本番機能から確実に分離することです。たとえば、開発者は、開発環境では権限を昇格して管理者レベルのアカウントを使用し、本番環境では別のユーザレベルアカウントでアクセスするという方法があります。 1 人が複数の役割（たとえば、アプリケーション開発と本番システムへの更新の実装）を果たす環境では、独立したチェックポイントのない、プロセスのエンドツーエンドのコントロールを 1 人の担当者が持たないように責務を割り当てる必要があります。たとえば、開発、承認、監視の責務はそれぞれ別の担当者に割り当てます。

要件	ガイダンス
6.4.3 テストまたは開発に本番環境データ（実際のPAN）を使用しない	セキュリティコントロールは、通常、開発環境ではそれほど厳しくありません。本番環境データを使用すると、悪意のある人々に本番環境データ（カード会員データ）に不正にアクセスする機会を与えることになります。 リリース前にシステム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。
6.4.4 本番環境システムがアクティブになる前にテストデータとテストアカウントを削除する	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アクティブになる前に本番環境コードから削除する必要があります。これらのアイテムは、アプリケーションの機能に関する情報を漏洩する場合があるためです。このような情報を保持していると、アプリケーションおよび関連するカード会員データの侵害を容易にする可能性があります。
6.4.5 セキュリティパッチの実装とソフトウェアの変更に関する管理手順を変更する。手順には以下の項目を含める必要がある。	適切な変更管理がないと、セキュリティ機能が過失または故意によって省略あるいは動作不能にされたり、処理の不規則性が発生したり、悪意のあるコードが取り込まれる可能性があります。また、変更がシステムのセキュリティ機能に悪影響を及ぼし、変更の取り消しが必要になる可能性もあります。
6.4.5.1 影響の文書化。	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。
6.4.5.2 適切な権限を持つ関係者による文書化された変更承認。	適切な権限を持つ関係者による承認は、変更が組織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。
6.4.5.3 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。	徹底的なテストを実施して、変更の実装によって環境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、環境の変更後に、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。 カスタムコードの変更の場合、変更によってコーディングの脆弱性がもたらされないことの確認がテストに含まれます。
6.4.5.4 回復手順。	変更ごとに、変更が失敗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。

要件	ガイダンス
6.5 アプリケーションを安全なコーディングガイドラインに基づいて開発する。ソフトウェア開発プロセスにおける一般的なコーディングの脆弱性対策に、以下の項目を含める。 ***注**: 要件 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 PCI 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ティス（OWASP ガイド、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る。*	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、企業とその顧客が損害を被り、評判に傷がつく可能性があります。 すべての PCI DSS 要件と同様に、要件 6.5.1 ～ 6.5.5 および 6.5.7 ～ 6.5.9 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 PCI DSS が発行された時点の最も一般的で認知された安全なコーディング手法で構成されています。業界で認知された安全なコーディング手法が変化した場合は、組織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。 提供されている安全なコーディングリソースの例（SANS、CERT、および OWASP）は推奨される参考資料であり、ガイダンスの提供のみを目的としています。組織は、環境内の個々のテクノロジに適用可能な適切で安全なコーディング手法を採用する必要があります。
6.5.1 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。	入力を検証して、ユーザデータがコマンドとクエリの意味を変更できないことを確認します。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て、攻撃者が、アプリケーションを通じてネットワーク内部のコンポーネントを攻撃したり、バッファオーバーフローなどの攻撃を開始したり、機密情報とサーバアプリケーション機能の両方を露出させたりすることを可能にします。これは、商取引対応の Web サイトで不正トランザクションを実行する方法としても一般的です。要求からの情報は、アプリケーションに送信する前に、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する必要があります。
6.5.2 バッファオーバーフロー	アプリケーションがバッファオーバーフロー攻撃に対して脆弱でないことを確認します。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。攻撃者は、バッファオーバーフローの脆弱性を利用するために、特定のバッファで処理できる容量を超える大量の情報をアプリケーションに送ります。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。

要件	ガイダンス
6.5.3 安全でない暗号化保存	暗号化の不具合を防止します。 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、侵害されてカード会員データが漏洩するリスクが高くなります。攻撃者が脆弱な暗号化プロセスを利用して、暗号化されたデータに平文アクセスすることも可能になります。
6.5.4 安全でない通信	認証されたすべての機密通信を適切に暗号化します。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。攻撃者が弱い暗号化プロセスを利用して、アプリケーションを制御したり、暗号化されたデータに平文アクセスすることも可能になります。
6.5.5 不適切なエラー処理	エラーメッセージまたはその他の手段で情報を漏洩してはいけません。アプリケーションは、さまざまなアプリケーションの問題を介して構成、内部動作に関する情報を意図せずに漏洩したり、プライバシーを侵害したりする可能性があります。攻撃者は、この弱点を利用して、機密データを盗んだり、より深刻な攻撃を実行したりします。また、不適切なエラー処理により、悪意のある人々がシステムを侵害するのに利用できる情報が提供されます。悪意のある人々が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、サーバ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、より汎用なエラーメッセージを使用します。
6.5.6 脆弱性特定プロセス（PCI DSS 要件 6.2 で定義）で特定された、すべての「高」脆弱性。 ***注**: この要件は、2012 年 6 月 30 日まではベストプラクティスとみなされ、それ以降は要件になる。*	要件 6.2 に従って規定された、アプリケーションに影響する可能性がある高脆弱性は、開発段階で対処する必要があります。たとえば、共有ライブラリや基盤オペレーティングシステムで特定された脆弱性は、アプリケーションが本番環境にリリースされる前に評価して対応する必要があります。
Web アプリケーションおよびアプリケーションインターフェイス（内部または外部）の場合、次の追加要件が適用されます。	内部および外部（公開）の 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。
6.5.7 クロスサイトスクリプティング（XSS）	すべてのパラメータは、含める前に検証を行う必要があります。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、Web サイトを書き換えたり、ワームを取り込んだりすることができます。

要件	ガイダンス
6.5.8 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）	内部オブジェクト参照をユーザに公開してはいけません。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。 すべての URL に対してプレゼンテーション層とビジネスロジックでアクセス制御を一貫して実施します。多くの場合、アプリケーションが機密機能を保護する唯一の方法は、権限のないユーザにリンクまたは URL を表示しないことです。攻撃者は、この弱点を使用してアクセスし、これらの URL に直接アクセスすることで不正な操作を実行できます。 ディレクトリトラバーサルから保護します。攻撃者は Web サイトのディレクトリ構造を列挙してナビゲートすることで、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。
6.5.9 クロスサイトリクエスト偽造（CSRF）	ブラウザによって自動的に送信される資格情報およびトークンの承認に応答してはいけません。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と送信させ、被害者のブラウザに攻撃者の利益となる悪意を持ったアクションを実行させます。CSRF は、攻撃対象の Web アプリケーションと同じぐらい強力である場合があります。
6.6 一般公開されている Web アプリケーションは、常時、新しい脅威と脆弱性に対処し、以下のいずれかの手法によって既知の攻撃から保護する必要がある。 ▪ 一般公開されている Web アプリケーションは、アプリケーションのセキュリティ脆弱性を手動/自動で評価するツールまたは手法によって、少なくとも年 1 回および何らかの変更を加えた後にレビューする ▪ 一般公開されている Web アプリケーションの手前に、Web アプリケーションファイアウォールをインストールする	Web に公開されているアプリケーションへの攻撃は一般的で、多くの場合、これらの攻撃は不適切なコーディングの実行によって可能となり、成功します。アプリケーションのレビューまたは Web アプリケーションファイアウォールのインストールに関するこの要件の目的は、カード会員データの侵害につながる、一般公開されている Web アプリケーションへの侵害の数を大幅に削減することです。 ▪ アプリケーションの脆弱性をレビューまたはスキャンする手動/自動の脆弱性セキュリティ評価ツールまたは手法を使用して、この要件を満たすことができます。 ▪ Web アプリケーションファイアウォールは、アプリケーション層で不要なトラフィックをフィルタリングおよびブロックします。適切に構成された Web アプリケーションファイアウォールをネットワークベースのファイアウォールと組み合わせて使用することで、アプリケーションが正しくコーディングまたは構成されていない場合にアプリケーション層への攻撃が防止されます。

要件 7、8、9 のガイダンス: 強固なアクセス制御手法の導入

要件 7: カード会員データへのアクセスを、業務上必要な範囲内に制限する

権限を与えられた担当者のみが重要なデータにアクセスできるように、システムおよびプロセスでは、職責に応じて必要な範囲にアクセスを制限する必要があります。「必要な範囲」とは、アクセス権が職務の実行に必要な最小限のデータ量および特権にのみ付与されることを示します。

要件	ガイダンス
7.1 システムコンポーネントとカード会員データへのアクセスを、業務上必要な人に限定する。アクセス制限には以下の項目を含める必要がある。 **7.1.1** 特権ユーザ ID に関するアクセス権が、職務の実行に必要な最小限の特権に制限されている **7.1.2** 特権の付与は、個人の職種と職能に基づく **7.1.3** 権限を持つ関係者による、必須権限を指定する文書化された承認が要求される。 **7.1.4** 自動アクセス制御システムを実装する	カード会員データにアクセスする人が増えるほど、ユーザのアカウントが不正に使用されるリスクが高まります。アクセスを、業務上必要とする強い理由がある人に限定すると、組織での経験不足や悪意によるカード会員データの不適切な処理を防ぐことができます。アクセス権が職務の実行に必要な最小限のデータ量および特権にのみ付与される場合、これは「最小限の特権」および「必要な範囲」と呼ばれます。特権が職種と職能に基づいて個人に付与される場合、これは「役割ベースのアクセス制御」（RBAC）と呼ばれます。役割ベースのアクセス制御の実施は、アプリケーション層または特定の承認ソリューションに限定されません。たとえば、Active Directory または LDAP、アクセス制御リスト（ACL）、TACACS などのディレクトリサービスを含むテクノロジは、適切に構成され、「最小限の特権」と「必要な範囲」の原則に従っている限り、有望なソリューションです。 組織では、必要な範囲に基づいたデータアクセス制御のための明確なポリシーとプロセスを作成し、役割ベースのアクセス制御を使用して、適切な管理者承認プロセスを含めたアクセスの付与方法および付与対象を定義する必要があります。
7.2 複数のユーザが使用するシステムコンポーネントで、ユーザが必要とする範囲に基づいてアクセスが制限され、明示的に許可のない限り「すべてを拒否」に設定された、アクセス制御システムを確立する。 アクセス制御システムには以下の項目を含める必要がある。 **7.2.1** すべてのシステムコンポーネントを対象に含む **7.2.2** 職種と職能に基づく、個人への特権の付与 **7.2.3** デフォルトでは「すべてを拒否」の設定	ユーザが必要とする範囲に基づいてアクセスを制限するメカニズムがないと、ユーザは知らないうちにカード会員データへのアクセスを付与される場合があります。複数のユーザを管理するには、自動化されたアクセス制御システムまたはメカニズムの使用が不可欠です。このシステムは、組織のアクセス制御ポリシーおよびプロセス（「必要な範囲」と「役割ベースのアクセス制御」を含む）に従って確立され、すべてのシステムコンポーネントへのアクセスを管理し、このようなアクセスを明確に付与するルールが確立されない限り誰にもアクセスが付与されないよう、デフォルトの設定が「すべて拒否」になっている必要があります。

要件	ガイダンス
注: *一部のアクセス制御システムはデフォルトで「すべてを許可」が設定されており、個別に拒否するためのルールを記述しない限り、または記述するまでは、アクセスが許可される。*	

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

アクセスが可能な各ユーザに一意の ID を割り当てて、各ユーザが自身の行動に独自に説明責任を負うようにします。このような説明責任に対応している場合、重要なデータおよびシステムに対するアクションは既知の承認されたユーザによって実行され、そのユーザを追跡することが可能です。

***注:** これらの要件は、管理機能を持つすべてのアカウント（POS アカウントを含む）、およびカード会員データの閲覧またはアクセス、あるいはカード会員データを保存するシステムへのアクセスに使用されるすべてのアカウントに適用可能です。ただし、要件 8.1、8.2、および 8.5.8 ～ 8.5.15 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、POS ペイメントアプリケーション内のユーザアカウント（レジ係のアカウントなど）に適用することを意図していません。*

要件	ガイダンス
8.1 システムコンポーネントまたはカード会員データへのアクセスを許可する前に、すべてのユーザに一意の ID を割り当てる。	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、組織は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。
8.2 一意の ID の割り当てに加え、以下の方法の少なくとも 1 つを使用してすべてのユーザを認証する。 ▪ 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）	これらの認証アイテムを一意の ID に加えて使用すると、ユーザの一意の ID が侵害されるのを防ぐことができます（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）。 デジタル証明書は、一意である限り、「ユーザが所有しているもの」での認証形式として有効なオプションです。

要件	ガイダンス
8.3 従業員、管理者、および第三者によるネットワークへのリモートアクセス（ネットワーク外部からのネットワークレベルアクセス）には 2 因子認証（たとえば、RADIUS（Remote Authentication and Dial-In Service）とトークン、TACACS（Terminal Access Controller Acceess Control System）とトークン、などの 2 因子認証を行うテクノロジ）を組み込む。 ***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る（認証方法については、要件 8.2 を参照）。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ません。*	2 因子認証は、ネットワーク外からのアクセスなど、リスクの高いアクセスに対して 2 つの形式の認証を要求します。セキュリティをさらに高めるために、組織では、セキュリティの低いネットワークからセキュリティの高いネットワーク（企業のデスクトップ（低いセキュリティ）からカード会員データを含む本番環境のサーバ/データベース（高いセキュリティ）など）にアクセスするときにも 2 因子認証を使用することを検討できます。 この要件は、リモートアクセスによってカード会員データ環境にアクセスされる可能性があるネットワークにリモートアクセスするユーザが適用対象です。 この場合のリモートアクセスとは、事業体が所有するネットワークの外部からのネットワークレベルアクセスのことです。これにはインターネットからのアクセス、または「信頼できない」ネットワークやシステムからのアクセス（第三者または従業員がモバイルコンピュータを使用して事業体のネットワークにアクセスする場合など）が含まれます。内部 LAN 間アクセス（安全な VPN 経由での 2 つのオフィス間のアクセスなど）はこの要件の趣旨ではリモートアクセスとはみなされません。 リモートアクセスの接続先が、適切なセグメンテーションを使用し、リモートユーザがカード会員データ環境にアクセスしたり、影響を及ぼしたりすることができないようになっている事業体のネットワークである場合、そのネットワークへのリモートアクセスに 2 因子認証を組み込むことは PCI DSS の要件ではありませんが、カード会員データ環境にアクセスできるネットワークへのリモートアクセスには 2 因子認証が必要であり、事業体のネットワークへのすべてのリモートアクセスに 2 因子認証を使用することが推奨されます。
8.4 強力な暗号化を使用して、すべてのシステムコンポーネントにおいて伝送および保存中にすべてのパスワードを読み取り不能にする。	多くのネットワークデバイスおよびアプリケーションは、ネットワーク内でユーザ ID と暗号化されていないパスワードを伝送し、パスワードを暗号化せずに保存します。悪意のある人々は、暗号化されていない、または読み取り可能なユーザ ID とパスワードを「スニッファー（Sniffer）」を使用して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ユーザ ID と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。伝送時に、ユーザ資格情報またはそのトンネルを暗号化できます。
8.5 すべてのシステムコンポーネントで、以下のように、消費者以外のユーザおよび管理者に対して適切なユーザ識別と認証管理を確実に行う。	悪意のある人々がシステムを侵害するために最初に行うステップの 1 つが弱いまたは存在しないパスワードを利用することであるため、ユーザ識別と認証管理のための適切なプロセスを実装することが重要です。

要件	ガイダンス
8.5.1 ユーザ ID、資格情報、およびその他の識別子オブジェクトの追加、削除、変更を管理する。	システムに追加されるユーザがすべて有効な認識済みのユーザであることを確実にするためには、ユーザ ID の追加、削除、変更を、特定の権限を持つ少人数グループで管理および制御する必要があります。これらのユーザ ID の管理を、この少人数のグループのみに限定する必要があります。
8.5.2 パスワードのリセットを実行する前にユーザ ID を確認する。	多くの悪意のある人々は「ソーシャルエンジニアリング」（ヘルプデスクに電話して正当なユーザを装うなど）を使用してパスワードを変更し、自身でユーザ ID を利用できるようにします。管理者がパスワードのリセット前にユーザを識別できるよう、正しいユーザのみが答えることができる「秘密の質問」を使用することを検討してください。このような質問が、共有されることなく、適切にセキュリティで保護されるようにします。
8.5.3 初期パスワードをユーザごとに一意の値に設定し、初回使用後に直ちに変更する。	新規ユーザの設定ごとに同じパスワードを使用すると、内部ユーザ、元従業員、または悪意のある人々により、このパスワードが知られ、または容易に発見されて、それを使用してアカウントへのアクセスが可能になります。
8.5.4 契約終了したユーザのアクセスは直ちに取り消す。	従業員の退職後も彼らのユーザアカウント経由でネットワークへのアクセスが可能な場合、カード会員データへの不要な、または悪意のあるアクセスが発生する可能性があります。このアクセスは、元従業員または、古いアカウントや未使用のアカウントを利用する悪意のあるユーザによって行われる可能性があります。ユーザアカウントを速やかに無効にできるよう、従業員が退職したときに直ちに通知するプロセスを人事部門との間で実装することを検討します。
8.5.5 少なくとも 90 日ごとに非アクティブのユーザアカウントを削除/無効化する。	非アクティブのアカウントが存在すると、権限のないユーザが未使用のアカウントを使用してカード会員データにアクセスする可能性があります。
8.5.6 リモートアクセスのためにベンダが使用するアカウントは、必要な期間のみ有効にする。ベンダのリモートアクセスアカウントが使用されている間、そのアカウントを監視する。	システムをサポートする必要がある場合に備えてベンダ（POS ベンダなど）がネットワークに週 7 日 24 時間アクセスできるようにすると、ネットワークへのこの常時使用可能な外部エントリポイントを見つけて使用する、ベンダ環境内のユーザ、または悪意のある人々からの不正なアクセスが行われる可能性が増加します。 カード会員データ環境へのベンダのアクセスの監視も他のユーザ（組織の担当者など）の場合と同様に適用されます。これには、PCI DSS 要件 10.1 と 10.2 に従ってアクティビティを監視し、ログに記録すること、および要件 12.3.8 と 12.3.9 に定義されたポリシーに従ってベンダのリモートアカウントの使用を確認することが含まれます。
8.5.7 認証手順およびポリシーを、カード会員データにアクセスできるすべてのユーザに伝達する。	パスワード/認証手順をすべてのユーザに伝達すると、ユーザのポリシーの理解および準拠に役立ちます。また、パスワードを不正使用してカード会員データにアクセスしようとする可能性がある悪意のある人々（従業員に電話して「問題のトラブルシューティング」に必要であるからとパスワードを聞き出すなどする）に注意するよう促します。

要件	ガイダンス
8.5.8 グループ、共有、または汎用のアカウントとパスワードなどの認証方法を使用しない。	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グループ内の誰であるかを特定できないためです。 一意の ID と複雑なパスワードに関するこの要件は、多くの場合、たとえば SUDO や SSH などを使用して管理機能内で満たされます。この場合、管理者が最初に自身の一意の ID とパスワードでログオンした後、SUDO や SSH を使用して管理者アカウントに接続します。多くの場合、この共有管理アカウントの使用を防ぐため、直接のルートログインは無効にします。この方法で、個人の責任と監査証跡を維持します。ただし、SUDO や SSH などのツールを使用した場合も、実際の管理者 ID とパスワードは誤使用を防ぐために PCI DSS 要件を満たす必要があります（これらのアカウントが無効になっていない場合）。
8.5.9 少なくとも 90 日ごとにユーザパスワードを変更する。	悪意のある人々は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することが多いため、強力なパスワードはネットワーク防御の第一線です。パスワードが短くて推測しやすく、また変更されずに長期間有効になっている場合、悪意のある人々がこれらの弱いアカウントを見つけ、有効なユーザ ID を装ってネットワークを侵害する機会が増加します。オペレーティングシステム（Windows など）、ネットワーク、データベース、およびその他のプラットフォームに付属しているパスワードおよびアカウントセキュリティ機能を有効にすることにより、これらの各要件に従う強力なパスワードを適用して維持することができます。
8.5.10 パスワードに 7 文字以上が含まれることを要求する。	
8.5.11 数字と英文字の両方を含むパスワードを使用する。	
8.5.12 ユーザが新しいパスワードを送信する際、最後に使用した 4 つのパスワードと同じものを使用できないようにする。	
8.5.13 最大 6 回の試行後にユーザ ID をロックアウトして、アクセス試行の繰り返しを制限する。	アカウントロックアウトメカニズムがないと、攻撃者は、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。
8.5.14 ロックアウトの期間を、最小 30 分または管理者がユーザ ID を有効にするまで、に設定する。	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、悪意のある人々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、管理者またはヘルプデスクは、アカウント所有者がロックアウトの原因（入力エラー）であるか検証できます。

要件	ガイダンス
8.5.15 セッションが 15 分を超えてアイドル状態の場合、端末または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。	重要なネットワークまたはカード会員データにアクセス可能なオープンマシンからユーザが離れるとき、そのマシン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。
8.5.16 カード会員データを含むデータベースへのすべてのアクセスを認証する。これには、アプリケーション、管理者、およびその他のすべてのユーザによるアクセスが含まれる。 データベースへの直接アクセスまたはクエリはデータベース管理者に制限される。	データベースおよびアプリケーションへのアクセス時にユーザ認証を行わないと、権限のないアクセスまたは悪意のあるアクセスが発生する可能性が増え、さらにユーザが認証されていないためシステムに認識されず、このようなアクセスをログに記録できません。また、データベースアクセスは、エンドユーザによるデータベースへの直接アクセスではなく、プログラムによる方法（ストアドプロシージャなど）を通じてのみ許可される必要があります（管理職務のためにデータベースに直接アクセスできる DBA を除きます）。

要件 9: カード会員データへの物理アクセスを制限する

データまたはカード会員データを格納するシステムへの物理アクセスは、デバイスまたはデータにアクセスし、システムまたはハードコピーを削除する機会をユーザに提供するため、適切に制限する必要があります。要件 9 において、"オンサイト要員"
とは、フルタイムおよびパートタイムの従業員、一時的な従業員、事業体の施設内に物理的に存在する請負業者やコンサルタントのことです。"訪問者"
は、ベンダ、オンサイト要員の客、サービス要員、または短期間（通常は 1 日以内）施設に入る必要がある人のことです。"メディア"
は、カード会員データを含むすべての紙および電子媒体のことです。

要件	ガイダンス
9.1 適切な施設入館管理を使用して、カード会員データ環境内のシステムへの物理アクセスを制限および監視する。	物理アクセス管理がないと、権限のない人々が建物に入り機密情報にアクセスしたり、システム構成を変更したり、ネットワークに脆弱性を導入したり、機器を破壊または盗難したりすることができます。
9.1.1 ビデオカメラやアクセス制御メカニズムを使用して、機密エリアへの個々の物理アクセスを監視する。収集されたデータを確認し、その他のエントリと相関付ける。法律によって別途定められていない限り、少なくとも 3 カ月間保管する。 ***注:*** *"機密エリア"とは、データセンター、サーバルーム、またはカード会員データを保存、処理、または伝送するシステムが設置されているエリアのこと。これには、小売店のレジなど、POS 端末のみが存在するエリアは含まれない。*	物理的な侵入の調査時、これらの管理は、カード会員データを保存する機密エリアに物理的にアクセスする個人を特定するのに役立ちます。機密エリアの例として、社内データベースサーバルーム、カード会員データが保存されている小売店舗のバックエンドサーバルーム、大量のカード会員データの保管エリアなどがあります。
9.1.2 誰でもアクセス可能なネットワークジャックへの物理アクセスを制限する。 たとえば、訪問者がアクセス可能なエリアでは、ネットワークへのアクセスが明示的に承認されている場合を除いて、ネットワークポートを有効にしないようにする必要がある。	ネットワークジャックへのアクセスを制限すると、悪意のある人々が差し込み可能なネットワークジャックを利用して内部ネットワークリソースにアクセスするのを防ぐことができます。使用していないネットワークジャックはオフにし、必要なときのみ再有効化することを検討します。会議室などの公共エリアでは、ベンダや訪問者がインターネットにのみアクセスできるプライベートネットワークを確立して、内部ネットワークにアクセスできないようにします。

要件	ガイダンス
9.1.3 ワイヤレスアクセスポイント、ゲートウェイ、ハンドヘルドデバイス、ネットワーク/通信ハードウェア、および通信回線への物理アクセスを制限する。	ワイヤレスコンポーネントおよびデバイスへのアクセスに対するセキュリティがないと、悪意のあるユーザは、組織の無人ワイヤレスデバイスを使用してネットワークリソースにアクセスしたり、さらには自身のデバイスをワイヤレスネットワークに接続して不正アクセスしたりすることができます。また、ネットワークと通信ハードウェアをセキュリティ保護することにより、悪意のあるユーザがネットワークトラフィックを傍受したり、自身のデバイスをワイヤード（有線）ネットワークリソースに物理的に接続したりすることを防ぎます。 施錠されたクローゼットやサーバルーム内など、ワイヤレスアクセスポイント、ゲートウェイ、およびネットワーク/通信ハードウェアを安全な保管エリアに配置することを検討します。ワイヤレスネットワークの強力な暗号化を必ず有効にします。長時間アイドル状態が続いたときのワイヤレスハンドヘルドデバイスの自動デバイスロックアウトを有効にし、電源をオンにするときにパスワードを要求するようにデバイスを設定することも検討します。
9.2 カード会員データにアクセス可能なエリアでは特に、オンサイト要員と訪問者を容易に区別できるような手順を作成する。	バッジシステムや入室の管理がないと、権限のないまたは悪意のあるユーザは、施設に容易に入り、重要なシステムやカード会員データを盗難、無効化、中断、または破壊することができます。管理を最適なものにするには、カード会員データを含む作業エリアへの出入りに対してバッジまたはカードアクセスシステムを実装することを検討します。 承認された訪問者を識別し、オンサイト要員と容易に区別できるようにすることで、カード会員データが存在するエリアに不正な訪問者が出入りを許可されることを防止します。
9.3 すべての訪問者が次のように取り扱われることを確認する。	訪問者管理は、権限のない人々や悪意のある人々が施設（さらにカード会員データ）にアクセスするリスクを削減するために重要です。
9.3.1 カード会員データが処理または保守されているエリアに入る前に承認が行われる	訪問者管理は、訪問者が入室を認められているエリアにのみ入室できること、担当者が行動を監視できるように訪問者として識別可能であること、およびアクセスが正当な訪問時間内のみに制限されることを確実にするために重要です。
9.3.2 有効期限があり、訪問者を非オンサイト要員として識別する物理トークン（バッジ、アクセスデバイスなど）が与えられる。	
9.3.3 施設を出る前、または期限切れの日に物理トークンの返却を求められる	

要件	ガイダンス
9.4 訪問者ログを使用して、訪問者の行動の物理的な監査証跡を保持する。訪問者の名前、所属会社、物理アクセスを承認したオンサイト要員をログに記録する。法律によって別途定められていない限り、このログを少なくとも 3 カ月間保管する。	訪問者に関する最小限の情報を文書化する訪問者ログは、容易に低コストで維持できます。また、データ侵害の可能性を調査するときに建物または部屋への物理アクセス、およびカード会員データへのアクセスの可能性の識別に役立ちます。施設の入口、特にカード会員データが保存されている領域の入口にログを実装することを検討します。
9.5 メディアバックアップを安全な場所に保管する（代替またはバックアップサイト、商用ストレージ施設などのオフサイト施設が望ましい）。保管場所のセキュリティを少なくとも年に一度確認する。	セキュリティで保護されていない施設に保存されている場合、カード会員データを含むバックアップは、紛失、盗難、または悪意のある目的でコピーされる可能性があります。安全に保管するには、商用データストレージ企業と契約するか、小規模の事業体の場合は、銀行の貸金庫を利用することを検討します。
9.6 すべてのメディアを物理的に保護する。	カード会員データは、リムーバブルメディアまたはポータブルメディア上、印刷時、または誰かの机の上などに置かれ保護されていない場合、不正に表示、コピー、またはスキャンされやすくなります。
9.7 あらゆる種類の媒体の内部または外部での配布に関して、以下の項目を含め、厳格な管理を維持する。	手順とプロセスによって内部および外部ユーザに配布されるメディア上のカード会員データを保護します。このような手順がないと、データが紛失または盗難に遭い、偽造目的で使用される可能性があります。
9.7.1 データの機密性を識別できるように、媒体を分類する。	分類ステータスを容易に識別できるように媒体を分類することが重要です。媒体を機密であることが分かるように分類しないと、適切に保護されなかったり、盗難または紛失が発生する可能性があります。
9.7.2 安全な配達業者または正確に追跡できるその他の配送方法によって媒体を送付する。	通常郵便などの追跡不可能な方法で送付された場合、媒体が紛失または盗難に遭う可能性があります。カード会員データを含む媒体の配送には安全な配達業者のサービスを使用して、追跡システムを使用して配送品の在庫と場所を維持管理できるようにします。
9.8 安全なエリアから移動されるすべての媒体を管理者が承認するようにする（特に媒体が個人に配布される場合）。	カード会員データが管理者によって承認されたプロセスを経ずに安全なエリアから移動されると、データの紛失や盗難につながる可能性があります。決定されたプロセスがないと、媒体の場所が追跡されず、データの移動先やその保護方法に関するプロセスも存在しません。
9.9 媒体の保管およびアクセスに関して厳格な管理を維持する。	慎重な在庫管理方法と保管管理がないと、媒体の盗難または紛失に無限に気付かない可能性があります。

要件	ガイダンス
9.9.1 すべての媒体の在庫ログを適切に保持し、少なくとも年に一度メディアの在庫調査を実施する。	媒体の在庫が管理されていない場合、媒体の盗難または紛失に長い間、または全く気付かない可能性があります。
9.10 ビジネスまたは法律上の理由で不要になった媒体を次のように破棄する。	ハードディスク、ポータブルドライブ、CD/DVD、または紙に含まれている情報を破棄するための手順が事前に講じられていない場合、破棄された媒体から悪意のある人々が情報を取得し、データを侵害する可能性があります。たとえば、悪意のある人々は、「ダンプスターダイビング」と呼ばれる技法を使用して、ゴミ箱をあさり、見つけた情報を使用して攻撃を開始することができます。 電子媒体を安全に破棄する方法の例として、安全な消去、消磁、物理的な破壊（ハードディスクの粉砕や裁断など）などがあります。
9.10.1 カード会員データを再現できないよう、ハードコピー資料を裁断、焼却、またはパルプ化する。	
9.10.2 カード会員データを再現できないように、電子媒体上のカード会員データを回復不能にする。	

要件 10 と 11 のガイダンス: ネットワークの定期的な監視およびテスト

要件 10: ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する

ログ記録メカニズムおよびユーザの行動を追跡する機能は、データへの侵害を防ぐ、検出する、またはその影響を最小限に抑えるうえで不可欠です。すべての環境でログが存在することにより、何か不具合が発生した場合に徹底的な追跡、警告、および分析が可能になります。侵害の原因の特定は、システムアクティビティログなしでは非常に困難です。

要件	ガイダンス
10.1 システムコンポーネントへのすべてのアクセス（特に、ルートなどの管理権限を使用して行われたアクセス）を各ユーザにリンクするプロセスを確立する。	ユーザアクセスをアクセス先のシステムコンポーネントにリンクするプロセスまたはシステムを確立することが（特に管理権限を持つユーザの場合）重要です。このシステムは、監査ログを生成し、疑わしいアクティビティを特定のユーザまで追跡する機能を提供します。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。
10.2 以下のイベントを再現するためにすべてのシステムコンポーネントの自動監査証跡を実装する。	疑わしいアクティビティの監査証跡の生成は、システム管理者に警告を送信し、データを他の監視メカニズム（侵入検知システムなど）に送信し、インシデント後の追跡用の履歴証跡を提供します。次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。
10.2.1 カード会員データへのすべての個人アクセス	悪意のある人々が CDE でシステム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。
10.2.2 ルート権限または管理権限を持つ個人によって行われたすべてのアクション	高い権限を持つ「管理者」や「ルート」などのアカウントは、システム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。
10.2.3 すべての監査証跡へのアクセス	悪意のあるユーザは、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。
10.2.4 無効な論理アクセス試行	悪意のある人々は、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。

要件	ガイダンス
10.2 5 識別および認証メカニズムの使用	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、悪意のあるユーザ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。権限の昇格や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。
10.2.6 監査ログの初期化	不正なアクティビティを実行する前に監査ログを無効にすることは、悪意のあるユーザが検出から逃れるための一般的な目標です。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。
10.2.7 システムレベルオブジェクトの作成および削除	マルウェアなどの悪意のあるソフトウェアは、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。 「システムレベルオブジェクト」の定義については、『PCI DSS と PA-DSS の用語集（用語、略語、および頭字語）』を参照してください。
10.3 イベントごとに、すべてのシステムコンポーネントについて少なくとも以下の監査証跡エントリを記録する。 **10.3.1** ユーザ識別 **10.3.2** イベントの種類 **10.3.3** 日付と時刻 **10.3.4** 成功または失敗を示す情報 **10.3.5** イベントの発生元 **10.3.6** 影響を受けるデータ、システムコンポーネント、またはリソースの ID または名前	10.2 に記載されている監査可能なイベントに対してこれら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。

要件	ガイダンス
10.4 時刻同期技術を使用してすべての重要なシステムクロックおよび時間を同期し、時間を取得、配布、保存するために以下の要件が実施されていることを確認する。 ***注:*** *時刻同期技術の一例として、ネットワークタイムプロトコル（NTP）が挙げられる。* **10.4.1** 重要なシステムが正確で一致した時間を保持する **10.4.2** 時刻データが保護されている **10.4.3** 時刻設定は業界で認知された時刻ソースから受信されている	時刻同期技術は複数のシステムのクロックを同期するために使用されます。適切に導入すれば、この技術によって多数のシステムのクロックを 1 秒未満の誤差で同期できます。クロックが正しく同期されていない場合に発生する可能性がある問題として、他のシステムとのログファイルの比較および正確なイベント順序の設定が困難になる（これらは侵害が発生した場合のフォレンジック分析に不可欠です）、絶対時刻に依存する SSH などの暗号化プロトコルが正しく機能しない、などが挙げられます。インシデント後のフォレンジックチームにとって、すべてのシステムの時刻の正確性と一貫性、および各アクティビティの時刻は、システムがどのように侵害されたかを判断するうえで重要です。 時刻を確実に統一するには、事業体内でごく少数の内部（一元管理された）タイムサーバを使用することが望まれます。これらのサーバは特殊電波、GPS 衛星、またはその他の外部ネットワークソースを利用して信頼できる既知の外部タイムサーバから UTC（協定世界時）データを直接受信し、互いに連携して正確な時刻を維持します。他のシステムはこれらのサーバから時刻を受信します。 悪意のある人々がネットワークに侵入した場合、多くの場合、彼らは監査ログ内で自身のアクションのタイムスタンプを変更してアクティビティが検出されないようにしようとします。悪意のある人々は、自身の存在を隠すためにシステムコンポーネントの時刻を直接変更しようとする場合もあります（システム時刻を実際より早めるなど）。そのため、すべてのシステムの時刻を正確に保ち、時刻データを不正なアクセスや変更から保護することが重要です。時刻データには各システムのクロックの設定に使用するパラメータや方式が含まれます。 時刻、時刻標準、サーバに関する情報を含む NTP の詳細については、*www.ntp.org* を参照してください。
10.5 変更できないよう、監査証跡をセキュリティで保護する。	多くの場合、ネットワークに侵入した悪意のある人々は、監査ログを編集して自身の行動を隠そうとします。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。

要件	ガイダンス
10.5.1 監査証跡の表示を、業務上の必要がある人物のみに制限する。 **10.5.2** 監査証跡ファイルを不正な変更から保護する。 **10.5.3** 監査証跡ファイルを、変更が困難な一元管理ログサーバまたは媒体に即座にバックアップする。 **10.5.4** 外部に公開されているテクノロジのログを内部 LAN 上のログサーバに書き込む。	監査ログの適切な保護には、強力なアクセス制御（ログへのアクセスを「必要な範囲」に基づいて制限する）と、内部分離の使用（ログを検索および変更しにくくするため）が含まれます。ワイヤレス、ファイアウォール、DNS、メールサーバなどの外部に公開されているテクノロジからのログを安全性がより高い内部ネットワーク内に書き込むことにより、これらのログは失われたり変更されたりするリスクが軽減されます。
10.5.5 ログに対してファイル整合性監視または変更検出ソフトウェアを使用して、既存のログデータを変更すると警告が生成されるようにする（ただし、新しいデータを追加する場合は警告を発生させない）。	ファイル整合性監視システムは、重要なファイルへの変更を確認し、このような変更が検出されたときに通知します。ファイル整合性監視では、事業体は通常、定期的に変更されないが、変更される場合は侵害の可能性を示すファイルを監視します。ログファイル（頻繁に変更される）の場合、監視する必要がある対象は、ログファイルが削除、突然に大幅な拡大または縮小されたとき、また悪意のある人々がログファイルを改ざんしたことを示すその他の要素などです。市販のツールとオープンソースツールの両方をファイル整合性監視に使用できます。
10.6 少なくとも日に一度、すべてのシステムコンポーネントのログを確認する。ログの確認には、侵入検知システム（IDS）や認証、認可、アカウンティングプロトコル（AAA）サーバ（RADIUS など）のようなセキュリティ機能を実行するサーバを含める必要がある。 ***注:*** *要件 10.6 に準拠するために、ログの収集、解析、および警告ツールを使用することができます。*	多くの侵害は、検出されるまでに数日または数カ月かけて行われています。ログを毎日確認することで、侵害の可能性が明らかになるまでの時間と露出を最小限に抑えることができます。ログ確認プロセスは手動にする必要はありません。多数のサーバを所有する事業体では特に、ログの収集、解析、および警告ツールの使用を検討します。

要件	ガイダンス
10.7 監査証跡の履歴を少なくとも 1 年間保持する。少なくとも 3 カ月はすぐに分析できる状態にしておく（オンライン、アーカイブ、バックアップから復元可能など）。	少なくとも 1 年間ログを保持することで、侵害が発生した、または発生していることに気付くまでにしばらくの間かかることが多いという事実に基づき、発生した可能性のある侵害と、システムが影響を受けた期間をより適切に判断するための十分なログ履歴を調査官に提供することができます。過去 3 カ月間のログをすぐに利用できるようにしておくことで、事業体はデータ侵害をすばやく識別し、影響を最小限に抑えることができます。バックアップテープをオフサイトに保管すると、データの復元、分析の実行、および影響を受けたシステムまたはデータの識別に、より長い時間がかかる可能性があります。

要件 11: セキュリティシステムおよびプロセスを定期的にテストする

脆弱性は、悪意のある個人や研究者によって絶えず検出されており、新しいソフトウェアによって広められています。システムコンポーネント、プロセス、およびカスタムソフトウェアを頻繁にテストして、セキュリティ管理が変化する環境に継続的に対応できるようにする必要があります。

要件	ガイダンス
11.1 四半期ごとにワイヤレスアクセスポイントの存在をテストし、承認されていないワイヤレスアクセスポイントを検出する。 ***注:*** *このプロセスで使用できる方法には、ワイヤレスネットワークスキャン、システムコンポーネントおよびインフラストラクチャの物理/論理検査、ネットワークアクセス制御（NAC）、ワイヤレス IDS/IPS などがある。* *いずれの方法を使用する場合も、不正なデバイスを検出および識別できる機能を十分に備えている必要がある。*	ネットワーク内でのワイヤレステクノロジの実装や利用は、悪意のあるユーザ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に使用する最も一般的な経路の 1 つです。ワイヤレスデバイスまたはネットワークが企業の知らない間にインストールされた場合、攻撃者はネットワークに容易に、かつ「認識されずに」侵入できます。 不正なワイヤレスデバイスはコンピュータまたは他のシステムコンポーネント内に隠れているか、接続している可能性があります。または、ネットワークポートや、スイッチやルーターなどのネットワークデバイスに直接接続している可能性もあります。このような不正デバイスは環境内への不正なアクセスポイントになる可能性があります。 ワイヤレスアクセスポイントをネットワークに簡単に接続できること、その存在を検出するのが困難なこと、および権限のないワイヤレスデバイスがもたらすリスクの増加により、ワイヤレステクノロジの使用を禁止するポリシーが存在する場合でも、これらのプロセスを実行する必要があります。 環境内に不正なワイヤレスアクセスポイントがインストールされていないことを確実にするための適切なツールとプロセスは、環境の規模と複雑度によって決まります。 たとえば、ショッピングモール内の単独の小売キオスクの場合、すべての通信コンポーネントを改ざん防止機能の付いたケースに収容し、キオスクの詳細な物理検査を行うことで、不正なワイヤレスアクセスポイントが接続またはインストールされていないことを十分に確認できますが、複数のノードを持つ環境（大規模な小売店、コールセンター、サーバルーム、データセンターなど）の場合、不正なワイヤレスアクセスポイントがインストールされている、または隠れている可能性があるシステムコンポーネントおよびネットワークポイントの数が多いため、詳細な物理検査を行うことは困難です。この場合、物理的なシステム検査とワイヤレスアナライザの結果を組み合わせるなど、複数の方法を組み合わせることで要件を満たすことが可能になります。 ネットワークアクセス制御（NAC）ソリューションには、デバイス認証と構成管理を行って、不正なシステムのネットワークへの接続や、ネットワーク上の不正なシステムへの不正なデバイスの接続を防止する機能があります。 組織は、インシデント対応計画の一部として、不正なワイヤレスアクセスポイントが検出された場合に従う手順を文書化しておく必要があります。ワイヤレス IDS/IPS

要件	ガイダンス
	は警告を自動的に生成するように構成されますが、計画では、不正なデバイスが手動ワイヤレススキャン中に検出された場合の対応手順も文書化しておく必要があります。
11.2 内部および外部ネットワークの脆弱性スキャンを少なくとも四半期に一度およびネットワークでの大幅な変更（新しいシステムコンポーネントのインストール、ネットワークトポロジの変更、ファイアウォール規則の変更、製品アップグレードなど）後に実行する。 ***注:*** *評価者が* *1）最新のスキャン結果が合格スキャンであったこと、2）事業体で四半期に一度のスキャンを要求するポリシーと手順が文書化されていること、および* *3）スキャン結果で判明した脆弱性が再スキャンにおいて示されているとおりに修正されたことを確認した場合、初回の PCI DSS 準拠のために、4 つの四半期に一度のスキャンに合格する必要はない。初回の PCI DSS レビュー以降の年は、4 つの四半期に一度のスキャンに合格している必要がある。*	脆弱性スキャンは、外部および内部のネットワークデバイスとサーバに対して実行される自動化ツールで、悪意のある人々により発見されて利用される可能性があるネットワーク内の脆弱性の可能性を明らかにするよう設計されています。これらの弱点が識別されたら、事業体はこれを修正し、スキャンを繰り返して脆弱性が修正されたことを確認します。 事業体の最初の PCI DSS 評価の時点では、4 回の四半期ごとのスキャンがまだ実行されていない場合があります。最新のスキャン結果が合格スキャンの基準を満たしていて、将来の四半期に一度のスキャンのためのポリシーと手順が確立されている場合は、この要件の目的は満たされています。これらの条件が満たされている場合は、4 回のスキャンが不足しているという理由で、この要件の「対応」評価を遅延させる必要はありません。

要件	ガイダンス
11.2.1 内部の脆弱性スキャンを四半期ごとに実行する。	CDE 内の内部システムの脆弱性を特定するために確立されたプロセスでは、四半期ごとの脆弱性スキャンを実施する必要があります。脆弱性を遅滞なく特定して対処することで、脆弱性が利用されてシステムコンポーネントやカード会員データが侵害される可能性は低下します。 環境に最大のリスクをもたらす脆弱性（要件 6.2 に従って「高」にランク分けされた脆弱性など）は、最優先で解決する必要があります。 内部ネットワークは 1 年中で絶えず変化する場合があるため、事業体は完全な内部脆弱性スキャンを一貫して行うことができない可能性があります。目的は、検出された脆弱性を事業体が適切な期間内に解決するための確実な脆弱性管理プログラムを設置することです。最低でも「高」脆弱性は適切な時期に対処する必要があります。 内部の脆弱性スキャンは、スキャン対象となるシステムコンポーネントから適切に独立し、資格を与えられた内部スタッフによって実行できます（たとえば、ファイアウォールの管理者がファイアウォールのスキャンを担当することは不適切です）。または、事業体は内部の脆弱性スキャンを認定スキャニングベンダ（ASV）、QSA、または脆弱性スキャンを専門とするその他の企業に委託することもできます。
11.2.2 四半期に一度の外部の脆弱性スキャンは、PCI（Payment Card Industry）セキュリティ基準審議会（PCI SSC）によって資格を与えられた認定スキャニングベンダ（ASV）によって実行される必要がある。 ***注:*** *四半期に一度の外部の脆弱性スキャンは、PCI（Payment Card Industry）セキュリティ基準審議会（PCI SSC）によって資格を与えられた認定スキャニングベンダ（ASV）によって実行される必要がある。ネットワーク変更後に実施されるスキャンは、内部スタッフによって実行することができる。*	外部ネットワークは侵害されるリスクがより高いため、四半期に一度の外部の脆弱性スキャンは PCI SSC 認定スキャニングベンダ（ASV）が実施する必要があります。 ASV は、PCI SSC によって『Approved Scanning Vendor Program Guide（認定スキャニングベンダプログラムガイド）』に規定された一連のスキャンおよびレポート基準に従う必要があります。

要件	ガイダンス
11.2.3 大幅な変更後は、内部および外部スキャンを実行する。 ***注:*** *変更後に実施されるスキャンは、内部スタッフによって実行することができる。*	大幅な変更を行った後に環境をスキャンすることにより、変更は適切に完了し、変更によって環境のセキュリティが損なわれていないことを確認できます。変更後には必ずしも環境全体をスキャンする必要はありませんが、変更の影響を受けたすべてのシステムコンポーネントをスキャンする必要があります。
11.3 外部および内部のペネトレーションテストを少なくとも年に一度および大幅なインフラストラクチャまたはアプリケーションのアップグレードや変更（オペレーティングシステムのアップグレード、環境へのサブネットワークの追加、環境へのWebサーバの追加など）後に実行する。これらのペネトレーションテストには以下の項目を含める必要がある。 **11.3.1** ネットワーク層のペネトレーションテスト **11.3.2** アプリケーション層のペネトレーションテスト	ペネトレーションテストの目的は、攻撃者が環境にどの程度まで侵入できるかを特定することを目標に、実際の攻撃の状況をシミュレーションすることです。これにより、事業体は露出の可能性をより的確に把握し、攻撃から防御するための戦略を策定できます。 脆弱性スキャンとは異なり、ペネトレーションテストは、特定された脆弱性を利用するなどのアクティブなプロセスです。多くの場合、脆弱性スキャンの実行はペネトレーションテスターが攻撃の戦略を立てるために最初に行う手順の 1つです。脆弱性スキャンによって既知の脆弱性が検出されなかった場合でも、多くの場合、ペネトレーションテスターはセキュリティギャップの可能性を特定するための、システムに関する十分な情報が得られます。 ペネトレーションテストは一般に手動操作主体のプロセスです。場合によっては自動化ツールも使用可能ですが、テスターはシステムに関する自らの知識を利用して環境に侵入する必要があります。多くの場合、テスターは防御の層を突破することを目標にして数種類の利用手段を連結します。たとえば、テスターは、アプリケーションサーバにアクセスする手段を見つけると、侵害されたサーバを、そのサーバがアクセスできるリソースに基づいて新しい攻撃を行うためのポイントとして使用します。このようにして、テスターは環境内で対処の必要がある弱点となる可能性がある領域を特定するために、攻撃者が行う方法をシミュレーションできます。

要件	ガイダンス
11.4 侵入検知システムや侵入防止システムを使用して、カード会員データ環境との境界およびカード会員データ環境内の重要なポイントを通過するすべてのトラフィックを監視し、侵害の疑いがある場合は担当者に警告する。 すべての侵入検知および防止エンジン、ベースライン、シグネチャを最新状態に保つ。	侵入検出/侵入防止システム（IDS/IPS）は、ネットワークに入って来るトラフィックを既知の「署名」や数千種類の侵害（ハッカーツール、トロイの木馬、およびその他のマルウェア）と比較し、警告を送信し、侵害の試みが発生した場合は阻止します。これらのツールを使用する権限のないアクティビティを検出するためのプロアクティブな手法がないと、コンピュータリソースへの攻撃（または誤使用）についてリアルタイムで気付かない可能性があります。侵入の試みを阻止できるよう、これらのツールによって生成されるセキュリティに関する警告を監視する必要があります。 IDS/IPS デバイスは、着信および発信トラフィックを CDE の境界および CDE 内の重要なポイントで監視するように実装する必要があります。CDE 内の重要なポイントには、事業体の環境およびリスク評価で文書化された規定に応じて、カード会員データを保存するデータベースサーバ、暗号化キーの保管場所、処理ネットワーク、その他のセンシティブシステムコンポーネントなどが含まれる場合があります。 最近の多くの IDS/IPS デバイスには 1 つのデバイスで CDE 内部の複数のポイントを監視する機能がありますが、その場合、1 つのデバイスの障害によって露出が発生する可能性が高まることを念頭に置く必要があります。したがって、IDS/IPS インフラストラクチャに適切な冗長性を組み込むことが重要です。 侵害の種類は数千に及び、毎日のように新しい種類が発見されています。IDS/IPS デバイスの古い署名とスキャンエンジンに新しい脆弱性を識別する機能がなく、侵害が検出されない可能性があります。これらの製品のベンダは、頻繁に（多くの場合、毎日）更新を提供しています。これらの更新を定期的に評価し、適用する必要があります。

要件	ガイダンス
11.5 ファイル整合性監視ツールを導入して重要なシステムファイル、構成ファイル、またはコンテンツファイルの不正な変更を担当者に警告し、重要なファイルの比較を少なくとも週に一度実行するようにソフトウェアを構成する。 ***注:*** *ファイル整合性監視において、重要なファイルとは通常、定期的に変更されないが、その変更がシステムの侵害や侵害のリスクを示す可能性があるファイルのことである。ファイル整合性監視製品では通常、関連オペレーティングシステム用の重要なファイルがあらかじめ構成されている。カスタムアプリケーション用のファイルなど、その他の重要なファイルは、事業体（つまり、加盟店またはサービスプロバイダ）による評価および定義が必要である。*	ファイル整合性監視（FIM）ツールは、重要なファイルへの変更を調べ、このような変更が検出されたときに通知します。市販のツールとオープンソースツールの両方をファイル整合性監視に使用できます。適切に実装されておらず、FIM の出力が監視されていない場合、悪意のある人々により、構成ファイルの内容、オペレーティングシステムのプログラム、またはアプリケーション実行可能ファイルが変更される可能性があります。このような権限のない変更が検出されない場合、既存のセキュリティ管理が無効となり、通常の処理へ影響が認識されることなくカード会員データが盗まれる可能性があります。

要件 12 のガイダンス: 情報セキュリティポリシーの整備

要件 12: すべての担当者の情報セキュリティポリシーを整備する

強力なセキュリティポリシーは、事業体全体でのセキュリティの方向性を設定し、担当者に対して期待される内容を示します。すべての担当者は、データの極秘性とその保護に関する自身の責任を認識する必要があります。要件 12 において、"担当者" とは、フルタイムおよびパートタイムの従業員、一時的な従業員、事業体の敷地内に "常駐" しているか、またはカード会員データ環境にアクセスできる請負業者やコンサルタントのことです。

要件	ガイダンス
12.1 以下を実現するセキュリティポリシーを確立、公開、維持、および周知する。 **12.1.1** すべての PCI DSS 要件に対応する。	企業の情報セキュリティポリシーは、最も貴重な資産を保護するセキュリティ手段を実装するためのロードマップを作成します。強力なセキュリティポリシーは、会社全体でのセキュリティの方向性を設定し、要員に対して期待される内容を示します。すべての担当者は、データの極秘性とその保護に関する自身の責任を認識する必要があります。
12.1.2 脅威、脆弱性、結果を識別する年に一度のプロセスを正式なリスク評価に含める。（リスク評価方法の例としては、OCTAVE、ISO 27005、および NIST SP 800-30 が挙げられるが、これらに限定されない。）	リスク評価によって、組織は業務に悪影響を及ぼす可能性がある脅威および関連する脆弱性を識別できます。さらに、リソースを効果的に割り当てて、認識された脅威の影響を受ける可能性を低下させるコントロールを実装できます。 リスク評価を少なくとも年に一度実施することで、組織の変更、進化する脅威、傾向、テクノロジに関する情報を最新状態に保つことができます。
12.1.3 レビューを少なくとも年に一度含め、環境の変化に合わせて更新する。	セキュリティの脅威と保護方式は、1 年を通じて急速に進化します。関連する変更を反映するようにセキュリティポリシーが更新されない場合、これらの脅威に対抗するための新しい保護方式が確立されません。
12.2 この仕様の要件と整合する日常的な運用上のセキュリティ手順を作成する（たとえば、ユーザアカウント保守手順、ログレビュー手順）。	日常的な運用上のセキュリティ手順は、担当者が毎日のシステム管理および保守業務で使用するための「マニュアル」として機能します。運用上のセキュリティ手順が文書化されていないと、担当者は自身の仕事の完全な範囲を把握できず、新しい担当者はプロセスを容易に繰り返すことができず、悪意のある人々が重要なシステムとリソースにアクセスすることを可能にするギャップがこれらのプロセスで生じる可能性があります。

要件	ガイダンス
12.3 重要なテクノロジ（リモートアクセステクノロジ、ワイヤレステクノロジ、リムーバブル電子メディア、ラップトップ、タブレット、携帯情報端末（PDA）、電子メールの使用、インターネットの使用など）に関する使用ポリシーを作成して、これらのテクノロジの適切な使用を定義する。これらの使用ポリシーでは以下を要求します。	担当者の使用ポリシーでは、会社のポリシーである場合に特定のデバイスとその他のテクノロジの使用を禁止したり、正しい使用法と実装に関するガイダンスを担当者に提供したりすることができます。使用ポリシーがない場合、担当者は会社のポリシーに違反するテクノロジを使用する可能性があり、その結果、悪意のある人々により重要なシステムとカード会員データへのアクセスが可能となります。例として、ワイヤレスネットワークを知らずにセキュリティなしでセットアップしてしまう、などがあります。会社の基準に従い、承認済みのテクノロジのみが実装されるようにするために、実装を運用チームにのみ制限し、専門でない一般の要員がこれらのテクノロジをインストールできないようにすることを検討します。
12.3.1 権限を持つ関係者による明示的な承認	これらのテクノロジの実装に対して適切な承認を要求しないと、担当者は、認識されたビジネスニーズに対するソリューションを実装し、知らずに重要なシステムとデータを悪意のある人々にさらす大きなセキュリティホールを開いてしまう可能性があります。
12.3.2 テクノロジの使用に対する認証	テクノロジが適切な認証（ユーザ ID、パスワード、トークン、VPN など）なしで実装される場合、悪意のある人々は、この保護されていないテクノロジを使用して、容易に重要なシステムとカード会員データにアクセスできます。
12.3.3 このようなすべてのデバイスおよびアクセスできる担当者のリスト	悪意のある人々は、物理セキュリティを侵害し、自身のデバイスをネットワーク上に「裏口」として配置する場合があります。担当者も、手順を無視してデバイスをインストールする場合があります。デバイスへの適切なラベル添付を使用する正確な在庫管理により、未承認のインストールをすばやく識別できます。デバイスの正式な名前付け規則を確立することを検討し、確立された在庫管理に従ってすべてのデバイスにラベルを添付し、記録します。デバイスを所有者、連絡先情報、目的に関連付けられるコードなどの情報を記載した論理ラベルを使用する場合もあります。
12.3.4 デバイスへの所有者、連絡先情報、目的を記載したラベルの添付	
12.3.5 テクノロジの許容される利用法	会社が承認したデバイスとテクノロジの許容されるビジネス利用と場所を定義することにより、会社は、悪意のある人々が重要なシステムとカード会員データにアクセスするために利用する「裏口」が開かれないよう、構成と運用管理におけるギャップをより適切に管理および制御できます。
12.3.6 テクノロジの許容されるネットワーク上の場所	
12.3.7 会社が承認した製品のリスト	
12.3.8 非アクティブ状態が特定の期間続いた後のリモートアクセステクノロジのセッションの自動切断	リモートアクセステクノロジは、重要なリソースとカード会員データへの「裏口」となることが多くあります。未使用時のリモートアクセステクノロジ（POS またはその他のベンダ、あるいはビジネスパートナーがシステムをサポートするために使用するテクノロジなど）を切断することで、ネットワークへのアクセスとリスクは最小限に抑えられます。管理を使用して非アクティブ状態が 15 分続いた後でデバイスを切断することを検討します。このトピックの詳細については、要件 8.5.6 も参照してください。
12.3.9 ベンダおよびビジネスパートナーには必要とする場合にのみリモートアクセステクノロジをアクティブ化し、使用後直ちに非アクティブ化する	

要件	ガイダンス
12.3.10 リモートアクセステクノロジ経由でカード会員データにアクセスする担当者については、定義されたビジネスニーズのために明示的に承認されていない限り、ローカルハードドライブおよびリムーバブル電子メディアへのカード会員データのコピー、移動、保存を禁止する。	カード会員データをローカルのパーソナルコンピュータやその他のメディアに保存したりコピーしたりしてはいけないという責任をすべての担当者に認識させるには、明示的に承認された担当者以外にこのような行動を明確に禁止するポリシーが必要です。承認されたリモート担当者の環境は組織のカード会員データ環境の一部とみなされるため、その担当者は保持しているカード会員データをすべての PCI DSS 要件に従って取り扱う責任があります。
12.4 セキュリティポリシーおよび手順に、すべての担当者の情報セキュリティに対する責任を明確に定義する。	明確に定義されたセキュリティの役割と責任が割り当てられていないと、セキュリティグループとのやりとりが統一されず、テクノロジがセキュリティで保護されずに実装されたり、古くなったテクノロジや安全でないテクノロジが使用されたりします。
12.5 個人またはチームに以下の情報セキュリティ管理責任を割り当てる。 **12.5.1** セキュリティポリシーおよび手順を確立、文書化、および周知する。 **12.5.2** セキュリティに関する警告および情報を監視して分析し、該当する担当者に通知する。 **12.5.3** セキュリティインシデントの対応およびエスカレーション手順を確立、文書化、および周知して、あらゆる状況をタイムリーかつ効果的に処理する。 **12.5.4** 追加、削除、変更を含め、ユーザアカウントを管理する **12.5.5** データへのすべてのアクセスを監視および管理する。	情報セキュリティ管理について責任がある各個人またはチームは、特定のポリシーを通じて、その責任と関連タスクを明確に理解している必要があります。この説明責任がないと、プロセスにおけるギャップが重要なリソースまたはカード会員データへのアクセスを開放してしまう場合があります。
12.6 正式なセキュリティに関する認識を高めるプログラムを実施して、すべての担当者がカード会員データセキュリティの重要性を認識するようにする。	担当者がセキュリティ責任について教育されていない場合、実装されたセキュリティ対策およびプロセスが、ミスや意図的なアクションによって無効になる可能性があります。

要件	ガイダンス
12.6.1 雇用時および少なくとも年に一度担当者を教育する。 ***注:*** *方法は、担当者の役割およびカード会員データへのアクセスレベルによって異なる場合がある。*	セキュリティに関する認識を高めるプログラムに定期的な再訓練セッションが含まれていないと、主要なセキュリティプロセスおよび手順が忘れられたり無視されたりして、重要なリソースおよびカード会員データの公開につながる可能性があります。初期訓練および再訓練の重点と深度は担当者の役割によって異なる場合があり、対象者に適した内容にする必要があります。たとえば、データベース管理者を対象とするセッションでは技術的な管理とプロセスに重点を置き、小売店のレジ係の訓練では安全な取引手順に重点を置くことが考えられます。 従業員を常に最新のポリシーと手順に従わせるための継続的な認識の更新を含めることを検討します。実施方法も対象者または訓練内容に応じて異なる場合があります。たとえば、初期訓練および年に一度の訓練を実習形式またはコンピュータベースのトレーニングセッションで実施し、継続的で定期的な更新を電子メール、ポスター、ニュースレターなどで実施することが考えられます。
12.6.2 セキュリティポリシーおよび手順に目を通して理解したことについての同意を、少なくとも年に一度担当者に求める。	担当者の同意を書面または電子的に要求することは、担当者がセキュリティポリシー/手順に目を通して理解したこと、およびこれらのポリシーへの準拠を約束したこと、また今後も約束することを確認するのに役立ちます。
12.7 雇用する前に、可能性のある担当者を選別して、内部ソースからの攻撃リスクを最小限に抑える。（バックグラウンドチェックの例には、職歴、犯罪歴、信用履歴、経歴照会があります。） ***注:*** *トランザクションを進めるときに一度に1つのカード番号にしかアクセスできない、店のレジ係など特定のポジションに雇用される可能性のある担当者については、この要件は推奨のみです。*	カード会員データへのアクセスを許可される予定の担当者を雇用する前に徹底的なバックグラウンドチェックを実行すると、不審な経歴または犯罪歴を持つ人々による PAN およびその他のカード会員データの不正使用のリスクが軽減されます。会社には、どのバックグラウンドチェック結果が雇用の決定に影響を及ぼすか（およびその影響はどのようなものか）を明確にする独自の決定プロセスを含め、背景チェックに関するポリシーとプロセスを用意することが期待されます。 効果的に実施するためには、バックグラウンドチェックのレベルは個々の職務に適している必要があります。たとえば、責任の大きい職務または重要なデータやシステムに対する管理アクセス権限が付与される職務の場合は、責任やアクセス権限が小さい職務より詳細なバックグラウンドチェックを行うことが妥当です。これは、リスクの低い職務に就き、詳細なバックグラウンドチェックを受けていない担当者が昇進または異動によって責任またはアクセス権限が大きい職務に就く、内部異動を対象とするプロセスにも適している場合があります。
12.8 カード会員データをサービスプロバイダと共有する場合は、サービスプロバイダを管理するためのポリシーと手順を維持および実施して、以下を含める。	加盟店またはサービスプロバイダがサービスプロバイダとカード会員データを共有する場合、特定の要件を適用して、このデータの保護がサービスプロバイダによって継続的に実施されることを確実にします。

要件	ガイダンス
12.8.1 サービスプロバイダのリストを維持する。	すべてのサービスプロバイダを追跡することで、リスクの可能性が組織の外部でどこまで広がるかを識別できます。
12.8.2 サービスプロバイダが自社の所有するカード会員データのセキュリティに対して責任を負うことに同意した、書面での契約を維持する。	サービスプロバイダの同意は、クライアントから取得するカード会員データの適切なセキュリティを維持することに対するコミットメントの証拠となり、責任を負わせます。
12.8.3 契約前の適切なデューディリジェンスを含め、サービスプロバイダとの契約に関するプロセスが確立されている。	プロセスにより、サービスプロバイダの契約は組織によって内部で徹底的に精査されます。サービスプロバイダとの正式な契約関係を築く前のリスク分析を含める必要があります。
12.8.4 少なくとも年 1 回サービスプロバイダの PCI DSS 準拠ステータスを監視するプログラムを維持する。	サービスプロバイダの PCI DSS 準拠ステータスを知ることで、組織が従う要件と同じ要件にサービスプロバイダが準拠していることが確実となります。 サービスプロバイダがさまざまなサービスを提供している場合、この要件はクライアントに実際に提供する、クライアントの PCI DSS 評価の範囲内にあるサービスにのみ適用されます。たとえば、プロバイダがファイアウォール/IDS サービスと ISP サービスを提供している場合、ファイアウォール/IDS サービスのみを利用するクライアントはその PCI DSS 評価の範囲内のサービスのみを含めます。
12.9 インシデント対応計画を実施する。システム違反に直ちに対応できるよう準備する。	責任を持つ関係者によって適切に周知され、読まれて、理解されている綿密なセキュリティインシデント対応計画がない場合、混乱や統一された対応の不足により、ビジネスのダウンタイム、公共メディアへの不要な公開、および新しい法的責任が増える可能性があります。

要件	ガイダンス
12.9.1 システム違反が発生した場合に実施されるインシデント対応計画を作成する。計画では、最低限、以下に対応する。 ▪ ペイメントブランドへの通知を最低限含む、侵害が発生した場合の役割、責任、および伝達と連絡に関する戦略 ▪ 具体的なインシデント対応手順 ▪ ビジネスの復旧および継続手順 ▪ データバックアッププロセス ▪ 侵害の報告に関する法的要件の分析 ▪ すべての重要なシステムコンポーネントを対象とした対応 ▪ ペイメントブランドによるインシデント対応手順の参照または包含	インシデント対応計画は綿密で、カード会員データに影響を及ぼす可能性がある違反が発生した場合に会社が効果的に対応できるようにするためのすべての主要要素が含まれている必要があります。
12.9.2 計画を少なくとも年に一度テストする。	適切なテストが行われないと、インシデント発生時の漏洩が増大する可能性がある主要な手順が見過ごされる場合があります。 計画のすべてのコンポーネント、および実際のインシデントの詳細なレビューとその対応を含むインシデント対応計画全体が過去 1 年以内にアクティブ化された場合、適切なテストとしてはそれで十分であると考えられます。計画の一部のコンポーネントのみを最近アクティブ化した場合、残りのコンポーネントもテストする必要があります。過去 12 カ月以内に計画のコンポーネントを一切アクティブ化していない場合、計画のすべてのコンポーネントを年に一度のテストの対象にする必要があります。
12.9.3 警告に 24 時間体制で対応できる担当者を指定する。 **12.9.4** セキュリティ違反への対応を担当するスタッフに適切なトレーニングを提供する。	訓練済みのすぐに対応できるインシデント対応チームがないと、ネットワークへの損害が拡大し、重要なデータとシステムが対象システムの不適切な処理によって「汚染」される可能性があります。これにより、インシデント後の調査が妨げられる可能性があります。内部リソースで対応できない場合は、これらのサービスを提供するベンダとの契約を検討します。
12.9.5 侵入検知、侵入防止、およびファイル整合性監視システムからの警告を含める。	これらの監視システムは、データへの可能性のあるリスクに焦点を合わせるように設計されており、違反を防ぐための迅速な措置を講じるうえで重要で、インシデント対応プロセスに含める必要があります。
12.9.6	インシデント後に「得られた教訓」をインシデント対応計画に組み込むことで、計画を最新状

要件	ガイダンス
得られた教訓を踏まえてインシデント対応計画を変更および改善し、産業の発展を組み込むプロセスを作成する。	態に保ち、新たな脅威やセキュリティの傾向に対応することができます。

要件 A.1 のガイダンス: 共有ホスティングプロバイダ向けの PCI DSS 追加要件

要件 A.1: 共有ホスティングプロバイダはカード会員データ環境を保護する

要件 12.8 に言及されているとおり、カード会員データにアクセスするすべてのサービスプロバイダ（共有ホスティングプロバイダを含む）は PCI DSS に従う必要があります。さらに、要件 2.4
には、共有ホスティングプロバイダは各事業体のホストされている環境およびデータを保護する必要があると記載されています。したがって、共有ホスティングプロバイダは、加えてこの付録に記載されている要件に従う必要があります。

要件	ガイダンス
A.1 A.1.1 ～ A.1.4 に従い、各事業体（つまり、加盟店、サービスプロバイダ、またはその他の事業体）のホストされている環境およびデータを保護する。 ホスティングプロバイダは、これらの要件および PCI DSS のその他すべての関連セクションを満たす必要がある。 ***注:*** *ホスティングプロバイダがこれらの要件を満たすことができたとしても、そのホスティングプロバイダを使用する事業体の準拠が保証されるわけではない。各事業体は、PCI DSS に従い、準拠を適宜検証する必要がある。*	PCI DSS の付録 A は、顧客である加盟店やサービスプロバイダに PCI DSS 準拠のホスティング環境を提供することを希望する共有ホスティングプロバイダを対象としています。その他のすべての関連 PCI DSS 要件に加えて、これらの手順に対応する必要があります。
A.1.1 各事業体が、その事業体のカード会員データ環境にアクセスするプロセスのみを実行するようにする。	加盟店またはサービスプロバイダが共有サーバ上で独自のアプリケーションを実行することを許可されている場合、これらのアプリケーションは特権ユーザではなく加盟店またはサービスプロバイダのユーザ ID を使用して実行する必要があります。特権ユーザは、自身の環境だけでなく、その他のすべての加盟店およびサービスプロバイダのカード会員データ環境にアクセスできます。
A.1.2 各事業体のアクセスおよび権限をその事業体のカード会員データ環境のみに制限する。	各加盟店またはサービスプロバイダが自身のカード会員データ環境のみにアクセスできるようにアクセスおよび権限を制限するには、以下を考慮します。（1）加盟店またはサービスプロバイダの Web サーバユーザ ID の権限、（2）ファイルを読み取り、書き込み、および実行するために付与される許可、（3）システムバイナリに書き込むために付与される許可、（4）加盟店およびサービスプロバイダのログファイルへのアクセス権の付与、（5）1 つの加盟店またはサービスプロバイダがシステムリソースを独占できないようにするための管

要件	ガイダンス
	理。
A.1.3 ログ記録および監査証跡が有効になっていて、各事業体のカード会員データ環境に固有であり、PCI DSS 要件 10 と整合性を保つようにする。	加盟店およびサービスプロバイダがカード会員データ環境に固有のログにアクセスして確認することができるよう、共有ホスティング環境でログを使用可能にする必要があります。
A.1.4 ホストされた加盟店またはサービスプロバイダへの侵害が発生した場合にタイムリーなフォレンジック調査を提供するプロセスを可能にする。	共有ホスティングプロバイダは、侵害に対するフォレンジック調査が必要になった場合に、個別の加盟店またはサービスプロバイダの詳細を把握できるように、適切な詳細レベルまで、迅速かつ簡単に応答するためのプロセスを確立する必要があります。

付録 A:　PCI データセキュリティ基準: 関連文書

以下のドキュメントは、加盟店とサービスプロバイダが PCI
データセキュリティ基準、準拠要件、および責任についての理解を深めるのに役立ちます。

文書	対象読者
PCI データセキュリティ基準の要件とセキュリティ評価手順	すべての加盟店とサービスプロバイダ
PCI DSS ナビゲート: 基準要件の目的理解	すべての加盟店とサービスプロバイダ
PCI データセキュリティ基準: 自己問診のガイドラインと手引き	すべての加盟店とサービスプロバイダ
PCI データセキュリティ基準: 自己問診 A と証明書	該当する加盟店[9]
PCI データセキュリティ基準: 自己問診 B と証明書	該当する加盟店[9]
PCI データセキュリティ基準: 自己問診 C-VT と証明書	該当する加盟店[9]
PCI データセキュリティ基準: 自己問診 C と証明書	該当する加盟店[9]
PCI データセキュリティ基準: 自己問診 D と証明書	該当する加盟店とサービスプロバイダ[9]
PCI DSS と PA-DSS の用語集（用語、略語、および頭字語）	すべての加盟店とサービスプロバイダ

[9] 該当する自己問診を判断するには、『PCI データセキュリティ基準 : 自己問診のガイドラインと手引き』の「組織に最適な SAQ および証明書の選択」を参照してください。