



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 1.2

2008 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。

目次

文書の変更	i
序文	iii
カード会員データとセンシティブ認証データの要素	1
カード会員データとセンシティブ認証データの位置	2
トラック1 およびトラック2 のデータ	3
PCI データセキュリティ基準の関連ガイダンス	4
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	5
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こと	5
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こと	10
要件 3 と 4 のガイダンス: カード会員データの保護	13
要件 3: 保存されるカード会員データの保護	13
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、暗号化すること	19
要件 5 と 6 のガイダンス: 脆弱性管理プログラムの整備	21
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、定期的に更新すること	21
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、保守すること	23
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	30
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	30
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	31
要件 9: カード会員データへの物理アクセスを制限する	35
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	39
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	39
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	42
要件 12 のガイダンス: 情報セキュリティポリシーの整備	44
要件 12: 従業員および請負業者向けの情報セキュリティポリシーを整備する	44
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	49
付録 A: PCI データセキュリティ基準: 関連文書	51

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)v1.2』が記録文書となります。

PCI DSS 要件は、カード会員データ環境に含まれる、または接続されるすべてのシステムコンポーネントに適用されます。カード会員データ環境とは、カード会員データまたはセンシティブ認証データを保有するネットワークの部分で、ネットワークコンポーネント、サーバ、アプリケーションが含まれます。

- 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、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、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)などが含まれる場合があります、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)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、これらに限定されるわけではありません。

ネットワークを適切にセグメント化し、カード会員データを保管、処理、伝送するシステムをそれ以外のシステムから隔離することで、カード会員データ環境の範囲を狭めることができます。認定セキュリティ評価機関(QSA)は、事業者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、認定セキュリティ評価機関(QSA)にテクノロジーとプロセスの実装、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/pdfs/pci_qsa_list.pdf を参照してください。

カード会員データとセンシティブ認証データの要素

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。

カード会員データは、プライマリアカウント番号（「PAN」、またはクレジットカード番号）およびペイメントトランザクションの一部として取得されるその他のデータとして定義され、次のデータ要素が含まれます（詳細については以下の表を参照）。

- PAN
- カード会員名
- 有効期限
- サービスコード
- 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)CAV2/CVC2/CVV2/CID、(3)PIN/PIN ブロック

プライマリアカウント番号(PAN)は、PCI DSS 要件と PA-DSS の適用性を決定する要素です。PAN が保存、処理、または送信されない場合、PCI DSS と PA-DSS は適用されません。

	データ要素	保存の許可	保護の必要性	PCI DSS 要件 3, 4
カード会員データ	プライマリアカウント番号	はい	はい	はい
	カード会員名 ¹	はい	はい ¹	いいえ
	サービスコード ¹	はい	はい ¹	いいえ
	有効期限 ¹	はい	はい ¹	いいえ
センシティブ認証データ ²	完全な磁気ストライプデータ ³	いいえ	N/A	N/A
	CAV2/CVC2/CVV2/CID	いいえ	N/A	N/A
	PIN/PIN ブロック	いいえ	N/A	N/A

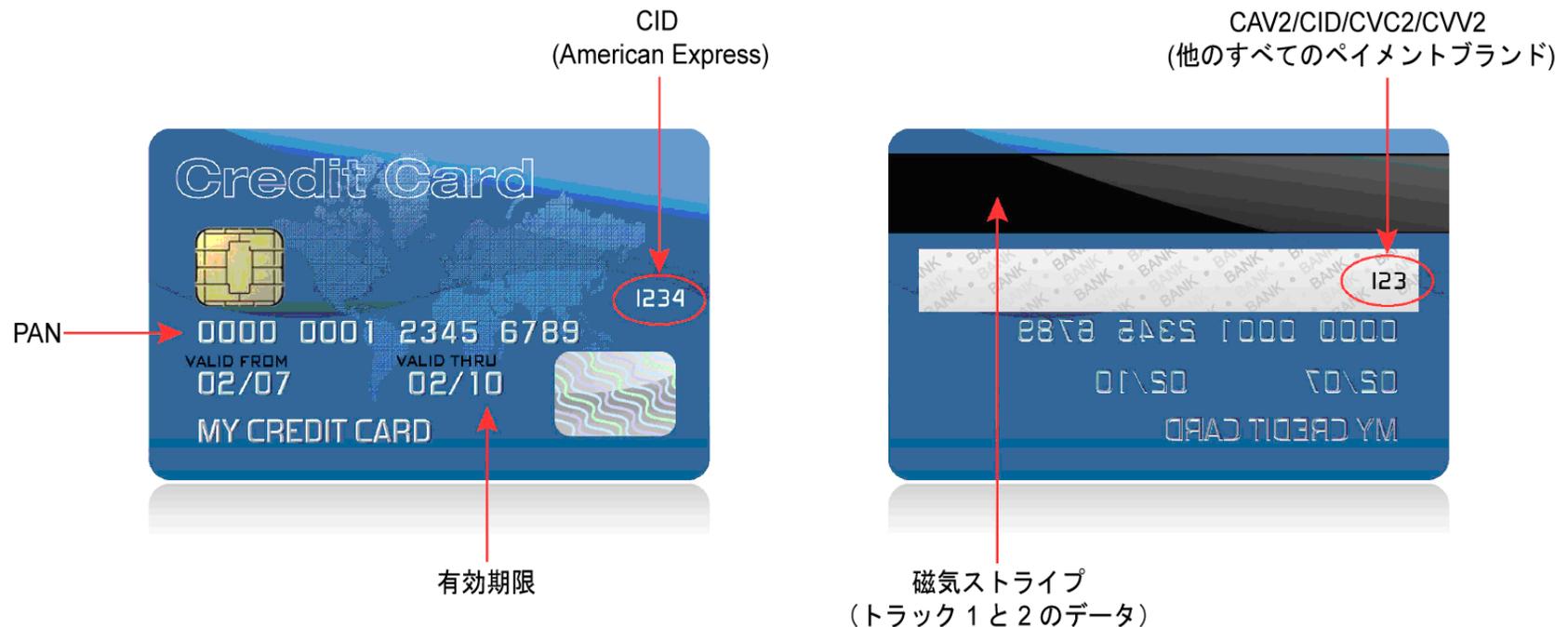
¹ これらのデータ要素は、PANと共に保存される場合は保護が必要です。この保護は、カード会員環境の全般的な保護に関する PCI DSS 要件に従います。さらに、他の法律（消費者の個人データ保護、プライバシー、ID 盗難、またはデータセキュリティに関連するものなど）により、このデータの特定の保護、または取引過程で消費者関連の個人データが収集される場合は会社の実施方法の適切な開示が必要になる可能性があります。ただし、PCI DSS は、PAN が保存、処理、または送信されない場合は適用されません。

² 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。

³ 磁気ストライプ、チップ上の磁気ストライプイメージなどに存在する全トラックデータ。

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⁴、カード検証コードまたは値⁵、PIN データ⁶ から構成されます。**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。



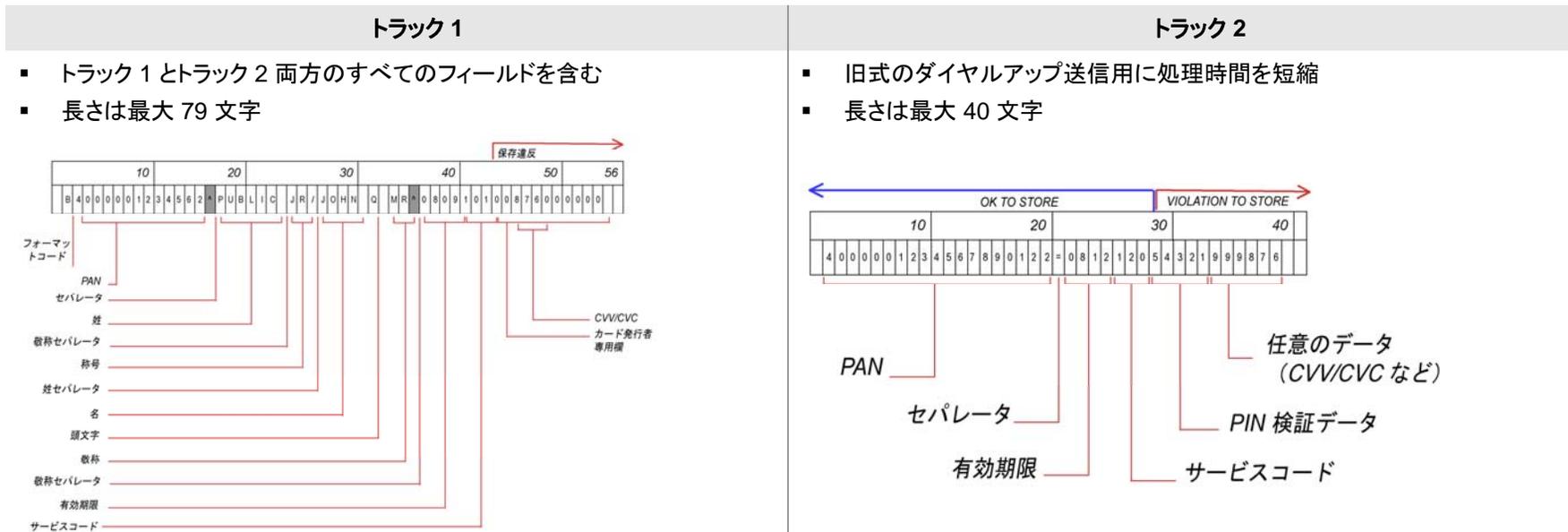
⁴ カードを提示する取引中に、承認のために使用される磁気ストライプにエンコードされたデータ。このデータは、チップ上の磁気ストライプイメージ内、またはカード上のその他の場所にある場合もあります。取引承認の後、事業者は磁気ストライプデータ全体を保持してはいけません。保持できる追跡データの要素は、プライマリアカウント番号、カード会員名、有効期限、サービスコードのみです。

⁵ 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。

⁶ 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クレジッ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データのレイアウトを示します。



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こと

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こと

カード会員データの保護

要件 3: 保存されるカード会員データの保護

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、暗号化すること

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を使用し、定期的に更新すること

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、保守すること

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こと

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: 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こと

ファイアウォールは企業のネットワーク(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、および企業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コンピュータ装置です。企業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ベースのアクセス、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	ガイダンス
<p>1.1 以下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</p>	<p>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となります。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。</p>
<p>1.1.1 すべての外部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</p>	<p>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。</p>
<p>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</p>	<p>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逃され、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。</p>

要件	ガイダンス
<p>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</p>	<p>ネットワークへの(およびネットワークからの)すべての接続に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理し、悪意のある人々が内部ネットワークにアクセスする可能性を最小限に抑えることができます。</p>
<p>1.1.4 ネットワークコンポーネントの論理的管理のためのグループ、役割、責任に関する記述</p>	<p>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。</p>
<p>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)</p>	<p>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。</p> <p>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、またはポートがビジネスにとって必要な場合、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。</p>
<p>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</p>	<p>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。</p> <p>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。</p>

要件	ガイダンス
<p>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、ファイアウォール構成を構築する。</p> <p>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。</p>	<p>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、つまりファイアウォール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。</p>
<p>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。</p>	<p>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。</p> <p>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。</p>
<p>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。</p>	<p>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。</p>
<p>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のすべてのトラフィックを拒否または制御(そのようなトラフィックが業務上必要な場合)するようにファイアウォールを構成する。</p>	<p>ネットワーク内のワイヤレステクノロジーの既知の(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。</p>

要件	ガイダンス
<p>1.3 インターネット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間の、直接的なパブリックアクセスを禁止する。</p>	<p>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。公共システムとカード会員データを保存するシステム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。</p>
<p>1.3.1 DMZ を実装し、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。</p>	<p>これらの要件は、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。</p>
<p>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。</p>	
<p>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、すべての直接経路（着信/発信）を使用不可にする。</p>	<p>DMZ は、公共のインターネットに面するファイアウォールの一部で、インターネット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します。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。</p>
<p>1.3.4 インターネットから DMZ 内へ通過できる内部インターネットアドレスを禁止する。</p>	<p>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。</p> <p>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。</p> <p>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。</p>
<p>1.3.5 カード会員データ環境からインターネットへの発信トラフィックが、DMZ 内の IP アドレスにのみアクセス可能なように制限する。</p>	<p>DMZ は、ネットワーク内部から発信されるすべてのトラフィックも評価して、すべての発信トラフィックが確立されたルールに確実に従うようにする必要があります。DMZ がこの機能を効果的に実行するためには、ネットワーク内部からネットワーク外のアドレスへのすべての接続を、最初に DMZ を通過して、DMZ により正当性を評価されない限り許可しないようにする必要があります。</p>

要件	ガイダンス
<p>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。)</p>	<p>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)。</p>
<p>1.3.7 DMZ から分離された内部ネットワークゾーンに、データベースを配置する。</p>	<p>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。</p>
<p>1.3.8 RFC 1918 アドレス領域を使用して、IP マスカレードを実装し、内部アドレスが変換されインターネット上で露出することを防ぐ。ポートアドレス変換(PAT)などのネットワークアドレス変換(NAT)テクノロジーを使用する。</p>	<p>ファイアウォールによって管理される IP マスカレードにより、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。</p>
<p>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。</p>	<p>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。</p>

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こと

(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
<p>2.1 システムをネットワーク上に導入する前に、ベンダ提供のデフォルト値を必ず変更する(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など)。</p>	<p>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攻撃に対するシステムの脆弱性が非常に高くなります。</p>
<p>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)。認証および伝送のために、強力な暗号化技術のワイヤレスデバイスセキュリティ設定が有効になっていることを確認する。</p>	<p>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および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 WPA/WPA2 のような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。</p>
<p>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。</p>	<p>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、Web サイト www.nist.gov、www.sans.org、www.cisecurity.org に記載されている例を参照してください。</p>

要件	ガイダンス
<p>2.2.1 1つのサーバには、主要機能を1つだけ実装する。</p>	<p>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：</p> <ol style="list-style-type: none"> 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。 <p>この要件は、サーバ(通常は Unix、Linux、または Windows ベース)を対象としており、メインフレームシステムは対象ではありません。</p>
<p>2.2.2 安全性の低い不必要なサービスおよびプロトコルはすべて無効にする(デバイスの特定機能を実行するのに直接必要でないサービスおよびプロトコル)。</p>	<p>1.1.7 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。新しいサーバの導入時に、常にこれらのサービスとプロトコルを確実に無効化とするためには、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。</p>
<p>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。</p>	<p>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。</p>
<p>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。</p>	<p>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。</p>
<p>2.3 すべてのコンソール以外の管理アクセスの暗号化。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 などのテクノロジーを使用する。</p>	<p>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ければならない場合、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。</p>

要件	ガイダンス
<p>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。</p>	<p>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。</p>

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: 保存されるカード会員データの保護

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手段は、カード会員データ保護のための重要な要素です。侵入者が他のネットワーク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、暗号化されていない電子メールで PAN を送信しない、などがあります。

強力な暗号化技術⁷およびその他の PCI DSS 用語の定義については、『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。

要件	ガイダンス
3.1 保存するカード会員データは最小限に抑える。データの保存と廃棄に関するポリシーを作成する。データ保存ポリシーに従って、保存するデータ量と保存期間を、業務上、法律上、規則上必要な範囲に限定する。	カード会員データを業務上必要な範囲より以上に保存すると、不要なリスクが発生します。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または PAN(読み取り不能に処理したもの)、有効期限、名前、サービスコードのみです。 必要ない場合は、保存してはいけません。
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。	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 ⁷ 、カード検証コードまたは値 ⁸ 、PIN データ ⁹ から構成されます。 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。

⁷ 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、チップ上の磁気ストライプイメージ内、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、事業者は磁気ストライプデータ全体を保持してはいけません。保持できる追跡データの要素は、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。

⁸ 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。

⁹ 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
<p>3.2.1 磁気ストライプのいかなるトラックのいかなる内容も保存しない(カードの裏面、チップ内、その他に存在する)。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る。</p> <p><i>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。</i></p> <ul style="list-style-type: none"> ▪ 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 <p><i>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。</i></p> <p><i>注: 詳細については、『PCI DSS と PA-DSS の用語集(用語、略語、および頭字語)』を参照。</i></p>	<p>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、世界中で販売することができます。</p>
<p>3.2.2 カードを提示しない取引の確認に使用される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裏面に印字された 3 桁または 4 桁の数字)を保存しない。</p> <p><i>注: 詳細については、『PCI DSS と PA-DSS の用語集(用語、略語、および頭字語)』を参照。</i></p>	<p>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。</p>
<p>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。</p>	<p>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。</p>

要件	ガイダンス
<p>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)。</p> <p>注:</p> <ul style="list-style-type: none"> ▪ 従業員およびその他の関係者が、特定のニーズにより 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。 	<p>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。</p>
<p>3.4 以下の手法を使用して、すべての保存場所で PAN を少なくとも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)。</p>	<p>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で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(または削除したりマスキングしたりする)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。「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。</p>
<ul style="list-style-type: none"> ▪ 強力な暗号化技術をベースにしたワンウェイハッシュ 	<p>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(SHA-1 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)。</p>
<ul style="list-style-type: none"> ▪ トランケーション 	<p>トランケーションの目的は、PAN の一部のみに(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、受領書などに表示されます)。</p>
<ul style="list-style-type: none"> ▪ 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) 	<p>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。</p>

要件	ガイダンス
<ul style="list-style-type: none"> ▪ 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 <p>アカウント情報のうち、少なくとも PAN は読み取り不能にする必要がある。</p> <p>注:</p> <ul style="list-style-type: none"> ▪ 何らかの理由で PAN を読み取り不能にできない場合は、「付録 B: 代替コントロール」を参照してください。 ▪ 「強力な暗号化技術」は、『PCI DSS と PA-DSS の用語集(用語、略語、および頭字語)』で定義されています。 	<p>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。</p>
<p>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は、オペレーティングシステムのネイティブのアクセス制御メカニズムとは別に論理アクセスを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。</p>	<p>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。</p> <ol style="list-style-type: none"> 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。
<p>3.5 カード会員データの暗号化に使用される暗号化キーを、漏洩と誤使用から保護する。</p>	<p>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。</p>
<p>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。</p>	<p>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)。</p>
<p>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。</p>	<p>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。</p>

要件	ガイダンス
3.6 カード会員データの暗号化に使用されるキーの管理プロセスおよび手順をすべて文書化し、実装する。これには、以下が含まれる。	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、すべてのキー要素を 3.6.1 から 3.6.8 1 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、キーをクリアテキストで配布せず、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、キーをクリアテキストで保存しません(キー暗号化キーで暗号化します)。
3.6.4 定期的な暗号化キーの変更 <ul style="list-style-type: none"> ● 関連するアプリケーションで必要とされる場合、自動的に行われることが望ましい(再キー入力など)。 ● 少なくとも年 1 回 	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。 暗号化キーの年 1 回の変更は、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。
3.6.5 古いキーまたは危険にさらされた疑いのあるキーの破棄または取替	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。
3.6.6 暗号化キーの知識分割と二重管理	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、手動のキー暗号化システムに、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。この種類の管理は通常、ハードウェアセキュリティモジュール内に実装されます。
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。

要件	ガイダンス
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示す書面への署名	このプロセスにより、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、暗号化すること

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
<p>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 SSL/TLS または IPSEC などのセキュリティプロトコルを使用する。</p> <p>PCI DSS では、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。</p> <ul style="list-style-type: none"> ▪ インターネット ▪ ワイヤレステクノロジー ▪ Global System for Mobile Communications (GSM) ▪ General Packet Radio Service (GPRS) 	<p>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 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。</p> <p>v3.0 より前のバージョンの SSL 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。</p>
<p>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。</p> <ul style="list-style-type: none"> ▪ 新しいワイヤレス実装において、2009 年 3 月 31 日以降は WEP を実装できない。 ▪ 現在のワイヤレス実装において、2010 年 6 月 30 日以降は WEP を使用できない。 	<p>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。適切な暗号化を使用すると、ネットワーク上での機密情報の傍受と開示を防ぐことができます。ワイヤード(有線)ネットワーク内にも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。</p> <p>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 は強力な暗号化を利用しません。WEP 暗号化は、WEP キー交換プロセス内の初期化ベクトル (IV) が弱く、必要な交換キーが不足しており脆弱であるため、単独で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 暗号化を突破できます。</p> <p>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 WPA 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必要があります。</p> <p>ワイヤレスネットワークが WEP を利用している場合は、ネットワークからカード会員データ環境にアクセスできないようにする必要があります。</p>

要件	ガイダンス
4.2 暗号化されていない PAN をエンドユーザメッセージングテクノロジー(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ффイングによって容易に傍受することができます。暗号化機能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: アンチウイルスソフトウェアまたはプログラムを使用し、定期的に更新すること

一般に「マルウェア」と呼ばれる悪意のあるソフトウェア(ウイルス、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、アンチウイ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
<p>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、アンチウイルスソフトウェアを導入する。</p>	<p>広く公開されるエクスプロイト(多くの場合「0 day Exploit」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。</p> <p>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。アンチウイ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。</p> <p>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。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。</p> <p>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 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。</p>

要件	ガイダンス
<p>5.1.1 すべてのアンチウイルスプログラムは、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。</p>	<p>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。</p>
<p>5.2 すべてのアンチウイルスメカニズムが最新で、有効に実行されており、監査ログが生成できる。</p>	<p>最高のアンチウイルスソフトウェアでも、アンチウイ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、ウイルスの活動とアンチウイルスの対応を監視することができます。</p>

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、保守すること

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者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
<p>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を適用する。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。</p> <p>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 カ月以内に対処し、重要性の低いシステムおよびデバイスは 3 カ月以内に対処するようにする。</p>	<p>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、変更優先順位を付けることを検討してください。</p>
<p>6.2 新たに発見された脆弱性を特定するためのプロセスを確立する(インターネット上で無料で入手可能な警告サービスに加入するなど)。新たな脆弱性の問題に対処するために、PCI DSS 要件 2.2 で要求されているとおりに構成基準を更新する。</p>	<p>この要件の目的は、組織が新しい脆弱性を常に把握して、ネットワークを適切に保護し、新しく発見された関連する脆弱性を構成基準に組み込むことができるようにすることです。</p>
<p>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を開発し、ソフトウェア開発ライフサイクル全体を通して情報セキュリティを実現する。これらのプロセスには、以下を含める必要がある。</p>	<p>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。</p>

要件	ガイダンス
<p>6.3.1 導入前にすべてのセキュリティパッチ、システムとソフトウェア構成の変更をテストする</p> <p>6.3.1.1 すべての入力の検証(クロスサイトスクリプティング、インジェクションの不具合、悪意のあるファイル実行などを防止するため)</p> <p>6.3.1.2 適切なエラー処理の検証</p> <p>6.3.1.3 暗号化による安全な保存の検証</p> <p>6.3.1.4 安全な通信の検証</p> <p>6.3.1.5 適切な役割ベースのアクセス制御(RBAC)の検証</p>	<p>すべてのインストールと変更が予期されるとおりに実行していること、および予期されない、不要な、または有害な機能が一切含まれていないことを確実にします。</p>
<p>6.3.2 開発/テスト環境と本番環境の分離</p>	<p>多くの場合、開発およびテスト環境は本番環境より安全性が低くなります。適切な分離がないと、脆弱性または弱い内部プロセス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場合があります。</p>
<p>6.3.3 開発/テスト環境と本番環境での責務の分離</p>	<p>これにより、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が最小限に抑えられ、アクセスはそのアクセスを本当に必要とするユーザに制限されることを確実にします。</p>
<p>6.3.4 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</p>	<p>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。</p>
<p>6.3.5 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</p>	<p>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ります。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。</p>
<p>6.3.6 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</p>	<p>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ります。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。</p>

要件	ガイダンス
<p>6.3.7 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</p> <p>注: このコードレビュー要件は、PCI DSS 要件 6.3 で要求される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が実施できる。一般に公開されている Web アプリケーションは、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。</p>	<p>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。安全なコーディング技術の知識を持つ人がコードをレビューして脆弱性を識別する必要があります。</p>
<p>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、変更管理手順に従う。手続きには以下を含める必要がある。</p>	<p>適切なソフトウェア変更管理がないと、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。バックグラウンドチェックおよびシステムアクセス制御に関連する担当者ポリシーが適切でない場合、信頼できない未トレーニングの人々がソフトウェアコードへの無制限のアクセスを持ったり、契約終了した従業員がシステムを侵害する機会を持っていたり、不正なアクションが検出されなかったりする可能性があります。</p>
<p>6.4.1 影響の文書化</p>	<p>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。</p>
<p>6.4.2 適切な関係者による管理承認</p>	<p>管理承認は、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。</p>
<p>6.4.3 本番環境機能のテスト</p>	<p>徹底的なテストを実施して、すべてのアクションが予期されていること、レポートが正確であること、考えられるすべてのエラー状況に適切に対応していることなどを確認する必要があります。</p>
<p>6.4.4 回復手順</p>	<p>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。</p>

要件	ガイダンス
<p>6.5 すべての Web アプリケーション(内部、外部、アプリケーションへの Web 管理アクセス)を、『オープン Web アプリケーションセキュリティプロジェクトガイド』などの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共通するコーディングの脆弱性の防止に対応して、以下を含める。</p> <p><i>注: PCI DSS v1.2 が発行されたときに 6.5.1 ~ 6.5.10 に挙げられている脆弱性は、現在 OWASP ガイドに掲載されている。ただし、OWASP ガイドが更新されている場合、これらの要件には現在のバージョンを使用する必要がある。</i></p>	<p>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。</p>
<p>6.5.1 クロスサイトスクリプティング (XSS)</p>	<p>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。</p>
<p>6.5.2 インジェクションの不具合(特に SQL インジェクション)。また、LDAP と 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。</p>	<p>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、Web アプリケーションで一般的です。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。Web 要求からの情報は、Web 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。</p>

要件	ガイダンス
<p>6.5.3 悪意のあるファイル実行</p>	<p>入力を検証して、アプリケーションが予期しないファイル名またはファイルをユーザから受け付けないことを確認します。リモートファイルインクルージョン (RFI) に対して脆弱なコードがあると、攻撃者は、サーバ全体の侵害などの壊滅的な攻撃につながる、悪意を持ったコードとデータを含めることができます。悪意のあるファイル実行を使用する攻撃は、PHP、XML、およびファイル名またはファイルをユーザから受け付けるすべてのフレームワークに影響を与えます。</p>
<p>6.5.4 安全でないオブジェクトの直接参照</p>	<p>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。</p>
<p>6.5.5 クロスサイトリクエスト偽造 (CSRF)</p>	<p>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回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くらい強力である場合があります。</p>
<p>6.5.6 情報漏洩と不適切なエラー処理</p>	<p>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 Web 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。</p>

要件	ガイダンス
<p>6.5.7 不完全な認証管理とセッション管理</p>	<p>ユーザを適切に認証し、アカウント資格情報とセッショントークンを保護します。アカウント資格情報とセッショントークンは、多くの場合、適切に保護されていません。攻撃者は、パスワード、キー、または認証トークンを侵害して、他のユーザの ID を装います。</p>
<p>6.5.8 安全でない暗号化保存</p>	<p>暗号化の不具合を防止します。多くの Web アプリケーションは、暗号化機能を適切に使用したデータと資格情報の保護を行っていません。攻撃者は、保護の弱いデータを使用して、ID 盗難やクレジットカード偽造などのその他の犯罪を実行します。</p>
<p>6.5.9 安全でない通信</p>	<p>認証されたすべての機密通信を適切に暗号化します。アプリケーションは、機密通信を保護する必要があるときにネットワークトラフィックを暗号化していないことが多くあります。</p>
<p>6.5.10 URL アクセスの制限失敗</p>	<p>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 を表示しないことによって機密機能のみを保護します。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。</p>

要件	ガイダンス
<p>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。</p> <ul style="list-style-type: none">▪ 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	<p>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。</p> <ul style="list-style-type: none">▪ 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。 <p>詳細については、「補足情報: 要件 6.6 アプリケーションの見直しと Web アプリケーションファイアウォールの明確化」(www.pcisecuritystandards.org)を参照してください。</p>

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
<p>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を含める必要がある。</p> <p>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こと</p> <p>7.1.2 特権の付与は、個人の職種と職能に基づくこと</p> <p>7.1.3 管理職により署名され、必要な特権を特定する承認フォームが要求される</p> <p>7.1.4 自動アクセス制御システムを実装する</p>	<p>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「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。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、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。</p>
<p>7.2 複数のユーザを持つシステムコンポーネントに対して、ユーザの必要な範囲に基づいてアクセスを制限し、明確に許可されていない場合は「すべてを拒否」するように設定されるメカニズムを確立する。アクセス制御システムには以下を含める必要がある。</p> <p>注: 「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。</p> <p>7.2.1 すべてのシステムコンポーネントを対象に含む</p> <p>7.2.2 職種と職能に基づく、個人への特権の付与</p> <p>7.2.3 デフォルトでは「すべてを拒否」の設定</p>	<p>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。</p>

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。

要件	ガイダンス
<p>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。</p>	<p>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拠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。</p>
<p>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。</p> <ul style="list-style-type: none"> ▪ パスワードまたはパスフレーズ ▪ 2 因子認証(トークンデバイス、スマートカード、生体認証、公開鍵など) 	<p>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)。</p>
<p>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 因子認証を組み込む。RADIUS(Remote Authentication and Dial-In Service)、TACACS(Terminal Access Controller Access Control System)とトークン、または VPN(SSL/TLS または IPSEC ベース)と個々の証明書などのテクノロジーを使用する。</p>	<p>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。</p>
<p>8.4 (『PCI DSS と PA-DSS の用語集(用語、略語、および頭字語)』で定義されている)強力な暗号化技術を使用して、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。</p>	<p>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。</p>
<p>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認証とパスワード管理を確実に行う。</p>	<p>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、ユーザ認証とパスワード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。</p>

要件	ガイダンス
<p>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。</p>	<p>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、この少数のグループのみに限定する必要があります。</p>
<p>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。</p>	<p>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。</p>
<p>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。</p>	<p>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。</p>
<p>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。</p>	<p>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 HR との間で実装することを検討します。</p>
<p>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。</p>	<p>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。</p>
<p>8.5.6 リモート保守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。</p>	<p>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。このトピックの詳細については、12.3.8 と 12.3.9 も参照してください。</p>
<p>8.5.7 パスワード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。</p>	<p>パスワード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。</p>

要件	ガイダンス
<p>8.5.8 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使用しない。</p>	<p>複数のユーザが同じアカウントとパスワードを共有すると、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、アカウントとパスワードを共有するグループ内の誰であるかを特定できないためです。</p>
<p>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。</p>	<p>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のが多いため、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。</p>
<p>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。</p>	
<p>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。</p>	
<p>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。</p>	
<p>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。</p>	<p>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。</p>
<p>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。</p>	<p>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。</p>
<p>8.5.15 セッションが 15 分を超えてアイドル状態の場合、端末を再有効化するためにユーザにパスワードの再入力を要求する。</p>	<p>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。</p>

要件	ガイダンス
<p>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。</p>	<p>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)。</p>

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	ガイダンス
<p>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。</p>	<p>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。</p>
<p>9.1.1 ビデオカメラやその他のアクセス管理メカニズムを使用して、機密エリアへの個々の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関連付ける。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、サーバールーム、またはカード会員データを保存するシステムが設置されているエリアのことです。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ません。</p>	<p>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。</p>
<p>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。</p>	<p>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。</p>
<p>9.1.3 無線アクセスポイント、ゲートウェイ、およびハンドヘルドデバイスへの物理アクセスを制限する。</p>	<p>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、企業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。施錠されたクローゼットやサーバールーム内など、ワイヤレスアクセスポイントおよびゲートウェイを安全な保管エリアに配置することを検討します。強力な暗号化が有効になっていることを確認します。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します。</p>

要件	ガイダンス
<p>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、すべての担当者が従業員と訪問者を容易に区別できるような手順を開発する。</p> <p>この要件において、"従業員"とは、フルタイムおよびパートタイムの従業員、一時的な従業員および要員、事業体の敷地内に"常駐"してい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、従業員の客、サービス要員、または短時間(通常は1日以内)施設に入る必要がある人として定義されます。</p>	<p>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。</p>
<p>9.3 すべての訪問者が次のように処理されることを確認する。</p> <p>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</p> <p>9.3.2 有効期限があり、訪問者を非従業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</p> <p>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</p>	<p>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。</p> <p>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、従業員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制限されることを確実にするために重要です。</p>
<p>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拠を保持する。訪問者の名前、所属会社、物理アクセスを承認した従業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。</p>	<p>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。</p>
<p>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。</p>	<p>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。</p>

要件	ガイダンス
<p>9.6 カード会員データを含むすべての紙および電子媒体を物理的にセキュリティで保護する。</p>	<p>カード会員データは、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。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するための手順とプロセスを検討します。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。</p>
<p>9.7 カード会員データを含む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、以下を含め、厳格な管理を維持する。</p>	
<p>9.7.1 秘密であると識別できるように、媒体を分類する。</p>	<p>機密であると識別されていない媒体は、必要な注意を払って扱われず、紛失または盗難に遭う可能性があります。前述の要件 9.6 で推奨されている手順に媒体分類プロセスを含めます。</p>
<p>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。</p>	<p>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。</p>
<p>9.8 安全なエリアから移動されるカード会員データを含む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)。</p>	<p>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。前述の要件 9.6 で推奨される手順に、データの移動に関する管理者承認プロセスの開発を含めます。</p>
<p>9.9 カード会員データを含む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。</p>	<p>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。前述の要件 9.6 で推奨されている手順に、カード会員データを含む媒体へのアクセスを制限するためのプロセスの開発を含めます。</p>
<p>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。</p>	<p>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気付かない可能性があります。前述の要件 9.6 で推奨される手順に、媒体の在庫管理と安全な保管のためのプロセスの開発を含めます。</p>

要件	ガイダンス
<p>9.10 次のように、ビジネスまたは法律上の理由で不要になったカード会員データを含む媒体を破棄する。</p>	<p>PC のハードディスク、CD、および紙に含まれている情報を破棄するための手順が講じられていない場合、このような情報の廃棄によって侵害が発生し、金銭的または評判の損失につなが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。前述の要件 9.6 で推奨されている手順に、カード会員データを含む媒体を適切に破棄するためのプロセス（廃棄前のこのような媒体の適切な保管を含む）の開発を含めます。</p>
<p>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。</p>	
<p>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。</p>	

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
<p>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。</p>	<p>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。</p>
<p>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。</p> <ul style="list-style-type: none"> 10.2.1 カード会員データへのすべての個人ユーザアクセス 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 10.2.3 すべての監査証跡へのアクセス 10.2.4 無効な論理アクセス試行 10.2.5 識別および認証メカニズムの使用 10.2.6 監査ログの初期化 10.2.7 システムレベルオブジェクトの作成および削除 	<p>ネットワーク上の悪意のある人々は、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。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。</p>

要件	ガイダンス
<p>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。</p> <ul style="list-style-type: none"> 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 	<p>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エントリ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。</p>
<p>10.4 すべての重要なシステムクロックおよび時間を同期する。</p>	<p>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。インシデント後のフォレンジックチームにとって、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。悪意のある人々は、タイムサーバの時刻を直接変更しようとする場合もあります。アクセス制限が適切でないと、悪意のある人々がネットワーク内に侵入した時刻よりも前の時刻に書き換えられる可能性があります。</p>
<p>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。</p> <ul style="list-style-type: none"> 10.5.1 監査証跡の表示を、仕事関連のニーズを持つ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ーのログを内部 LAN 上のログサーバに書き込む。 	<p>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。</p> <p>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ー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。</p>

要件	ガイダンス
<p>10.5.5 ログに対してファイル整合性監視および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、新しいデータの追加は警告を発生させない)。</p>	<p>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。</p>
<p>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、アカウントングプロトコル(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。</p> <p><i>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。</i></p>	<p>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。</p>
<p>10.7 監査証拠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)。</p>	<p>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。</p>

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
<p>11.1 無線アナライザを少なくとも四半期に一度使用して、または使用中のすべての無線デバイスを識別するための無線IDS/IPSを導入して、無線アクセスポイントの存在をテストする。</p>	<p>ネットワーク内での無線テクノロジーの実装や利用は、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。無線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。無線アナライザに加えて、ポートスキャナおよび無線デバイスを検出するその他のネットワークツールを使用できます。</p> <p>無線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、および権限のない無線デバイスがもたらすリスクの増加により、無線テクノロジーの使用を禁止するポリシーが存在する場合でも、これらのスキャンを実行する必要があります。</p> <p>組織は、インシデント対応計画の一部として、不正な無線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。無線IDS/IPS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無線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。</p>
<p>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。</p> <p><i>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 Approved Scanning Vendor (ASV) によって実行される必要があります。ネットワーク変更後に実施されるスキャンは、会社の内部スタッフによって実行することができます。</i></p>	<p>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、脆弱性の可能性を明らかにし、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ポートを識別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。</p> <p>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る、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。</p>

要件	ガイダンス
<p>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を含める必要がある。</p> <p>11.3.1 ネットワーク層のペネトレーションテスト</p> <p>11.3.2 アプリケーション層のペネトレーションテスト</p>	<p>ネットワークおよびアプリケーションペネトレーションテストは脆弱性スキャンとは異なります。ペネトレーションテストは手動の操作が多く、スキャンで識別された脆弱性のいくつかに対して実際に攻撃を試みます。また、悪意のある人々がセキュリティの弱いシステムまたはプロセスを利用するために使用する技術を含めます。</p> <p>アプリケーション、ネットワークデバイス、およびシステムを本番環境にリリースする前に、(要件 2.2 に従った)セキュリティに関するベストプラクティスを使用して強化し、セキュリティ保護する必要があります。脆弱性スキャンとペネトレーションテストにより、後に攻撃者により発見されて利用される可能性がある残りの脆弱性を明らかにします。</p>
<p>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内の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を最新状態に保つ。</p>	<p>これらのツールは、ネットワークに入って来るトラフィックを数千種類の侵害(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)の既知の「署名」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。</p> <p>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。これらのシステムの古いバージョンには、最新の「署名」が含まれていないため、新しい脆弱性を識別せず、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。</p>
<p>11.5 ファイル整合性監視ソフトウェア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。</p> <p><i>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す。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ます。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す。</i></p>	<p>ファイル整合性監視(FIM)システムは、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。</p>

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: 従業員および請負業者向け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、会社全体でのセキュリティの方向性を設定し、従業員に対して期待される内容を示します。すべての従業員は、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。この要件において、「従業員」とは、フルタイムおよびパートタイムの従業員、一時的な従業員および要員、会社の敷地内に「常駐」してい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
<p>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。</p> <p>12.1.1 すべての PCI DSS 要件に対応する。</p> <p>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。</p> <p>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。</p>	<p>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、従業員に対して期待される内容を示します。すべての従業員は、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。</p> <p>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。これらの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。</p>
<p>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)。</p>	<p>日常的な運用上のセキュリティ手順は、作業員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、作業員は自身の仕事の完全な範囲を把握できず、新しい作業員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。</p>
<p>12.3 従業員に公開されている重要なテクノロジー(リモートアクセステクノロジー、無線テクノロジー、リムーバブル電子メディア、ラップトップ、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、すべての従業員および請負業者向けにこれらのテクノロジー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。</p>	<p>従業員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ー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従業員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、従業員は会社のポリシーに違反するテクノロジー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、無線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ー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、専門でない一般の従業員がこれらのテクノロジーをインストールできないようにすることを検討します。</p>

要件	ガイダンス
12.3.1 管理者による明示的な承認	これらのテクノロジーの実装に対して適切な管理承認を要求しないと、従業員は、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 テクノロジーの使用に対する認証	テクノロジーが適切な認証(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ーを使用して、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。従業員も、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。
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 テクノロジー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ー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 テクノロジー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ーのセッションの自動切断	リモートアクセステクノロジーは、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ー(POS またはその他のベンダがシステムをサポートするために使用するテクノロジーなど)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ーをアクティブ化し、使用后直ちに非アクティブ化する	
12.3.10 リモートアクセステクノロジー経由でカード会員データにリモートにアクセスする場合、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従業員に認識させるには、このような行動を明確に禁止するポリシーが必要です。
12.4 セキュリティポリシーおよび手順に、すべての従業員および請負業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、テクノロジー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ーや安全でないテクノロジーが使用されたりします。

要件	ガイダンス
<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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</p> <p>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。</p>	<p>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。</p>
<p>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、すべての従業員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。</p> <p>12.6.1 雇用時および少なくとも年に一度従業員を教育する。</p>	<p>ユーザ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、従業員の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。</p> <p>セキュリティに関する認識を高めるプログラムに年に一度の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。</p>
<p>12.6.2 会社の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従業員に求める。</p>	<p>従業員の同意を要求する(書面または電子的になど)ことは、従業員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を確認するのに役立ちます。</p>
<p>12.7 雇用する前に、可能性のある従業員(上述の9.2の"従業員"の定義を参照)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。</p> <p>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、店のレジ係などの従業員については、この要件は推奨のみです。</p>	<p>カード会員データへのアクセスを許可される予定の従業員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。</p>

要件	ガイダンス
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。
12.8.1 サービスプロバイダのリストを維持する。	サービスプロバイダを認識することで、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リジエンスを含め、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 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、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さらに確実となります。
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
<p>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。</p> <ul style="list-style-type: none"> ▪ 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 	<p>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。</p>
<p>12.9.2 計画を少なくとも年に一度テストする。</p>	<p>適切なテストが行われないと、インシデント発生時に公開を制限するための主要な手順が見過ごされる場合があります。</p>
<p>12.9.3 警告に 24 時間態勢で対応できる担当者を指定する。</p>	<p>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。</p>
<p>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。</p>	
<p>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。</p>	<p>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。</p>
<p>12.9.6 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。</p>	<p>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。</p>

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こと

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
<p>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。</p> <p>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ります。</p> <p><i>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ありません。各事業体は、PCI DSS に従い、準拠を適宜検証する必要があります。</i></p>	<p>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。</p>
<p>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。</p>	<p>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。</p>
<p>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。</p>	<p>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理。</p>

要件	ガイダンス
<p>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。</p>	<p>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。</p>
<p>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。</p>	<p>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。</p>

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および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	加盟店 ¹⁰
PCI データセキュリティ基準: 自己問診 B と証明書	加盟店 ¹⁰
PCI データセキュリティ基準: 自己問診 C と証明書	加盟店 ¹⁰
PCI データセキュリティ基準: 自己問診 D と証明書	加盟店 ¹⁰ およびすべてのサービスプロバイダ
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

¹⁰適切な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。