PCI DSS 準拠を達成するための優先的なアプローチ

ペイメントカード業界データセキュリティ基準（PCI DSS）には、加盟店およびその他の組織がカード会員のデータを保管、処理、および伝送する際に、そのデータの安全を守るための 12 要件から成る詳細な枠組みが用意されています。この規準は該当する範囲が広いため、セキュリティに関しても非常に数多くの規定があります。カード会員データの管理責任者の中には、準拠させようにもどこから手をつけたらよいかわからない人も出てくるかもしれません。このような場合に備え、準拠プロセスの早い段階でリスクを減らすためには、利害関係者はどの時点で行動したら良いかがわかるように、PCI Security Standards Council は次のような優先的なアプローチを用意しています。優先的なアプローチに示されたマイルストーンは、それぞれが単独では包括的なセキュリティや PCI DSS 準拠を達成することはできませんが、利害関係者はこのガイドラインに沿っていれば、カード会員データの安全確保に向けたプロセスが前進します。

特長

加盟店が最もリスクの高い対象を識別する際に支援する

PCI DSS の実装および評価作業のための共通言語を作成する

マイルストーンにより、加盟店は準拠プロセスの進行状況を提示することが可能

優先的なアプローチとはどのようなものですか？

優先的なアプローチには、6 つのセキュリティマイルストーンが用意されています。加盟店やその他の組織は、これらのマイルストーンに沿って、最高のリスク要因や拡大しつつある脅威に対する防御を段階的に達成することにより、PCI DSS 準拠に到達することができます。優先的なアプローチとそのマイルストーン（2 頁で説明）は、次の効果を目指しています。

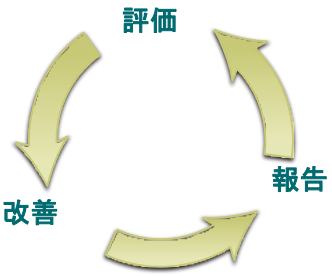
- リスクに優先順位を付けて対処するためのロードマップ
- 「迅速な効果」を得るための実際的な手法
- 財務計画および運用計画を作成支援する
- 客観的で測定可能な進捗指標の使用を促進する
- 評価機関の一貫性を促進する

優先的なアプローチの目標

優先的なアプローチには、カード会員データの保存、処理、および伝送に関連するリスクに基づいて、準拠作業を行うためのロードマップが用意されています。ロードマップを使用することにより、準拠を達成するための各作業に優先順位を付けられ、マイルストーンが確立され、準拠プロセスの早い段階でカード会員データ侵害のリスクが低減されます。また、ロードマップを使用することにより、アクワイアラーは、加盟店やサービスプロバイダなどの準拠作業とリスク低減について、客観的に測定することができます。優先的なアプローチは、実際の侵害のデータならびに認定セキュリティ評価機関、フォレンジック調査機関、および PCI SSC の諮問委員会からのフィードバックを分析して考案されました。これは、PCI DSS 準拠に替わるものでも、近道でも、またはギャップを埋めるためのものではなく、また、すべての組織に採用が義務付けられた一律のフレームワークでもありません。優先的なアプローチは、オンサイト評価を選択する加盟店または SAQ D を使用する加盟店に適しています。

2016 年 5 月

PCI DSS への準拠は継続的なプロセス



PCI SSC の設立メンバ

参加団体

加盟店、銀行、プロセサー、開発者、POS ベンダ

免責事項

PCI DSS 準拠を達成するには、PCI DSS の要件をすべて満たす必要があります。この場合、各要件の達成の順序や、その組織が PCI DSS の優先的なアプローチに従ったかどうかは問題になりません。この文書は、PCI DSS またはその要件のいずれをも変更または簡略化するものではなく、また、予告なしに変更される可能性があります。

PCI SSC は、ここに記載された情報を使用して生じた誤りや損害に対して一切責任を負いません。PCI SSC は、ここで提供される情報について、いかなる保証も表明もいたしません。また、こうした情報の使用または誤使用についても、PCI SSC は一切責任を負いません。

PCI DSS 準拠作業に優先順位を付けるマイルストーン

優先的なアプローチには 6 つのマイルストーンがあります。以下のマトリックスは、各マイルストーンの目標と意図の概略を示しています。この文書の残りの部分では、各マイルストーンと、PCI DSS の全 12 項目およびその下位要件との対応関係を示しています。

マイルストー	目的
1	**センシティブ認証データを削除し、データの保存を制限する。**このマイルストーンでは、侵害の被害があった事業体における重要なリスク領域を対象とします。センシティブ認証データと他のカード会員データが保存されていなければ、侵害の影響は大幅に軽減されます。必要ない場合は、保存してはいけません。
2	**システムとネットワークを保護し、システム違反に対応できるよう準備する。**このマイルストーンでは、侵害の大多数が発生するポイントの制御方法と対応のプロセスを取り上げます。
3	**ペイメントカードアプリケーションの安全を確保する。**このマイルストーンでは、アプリケーション、アプリケーションプロセス、アプリケーションサーバの制御を対象とします。これらの領域に脆弱性が存在すると、システムが侵害され、カード会員データが簡単にアクセスされる危険にさらされます。
4	**システムへのアクセスを監視および管理する。**このマイルストーンの制御により、ネットワークおよびカード会員データ環境へ、誰が、どのデータに、いつ、どのようにしてアクセスしたかを検出できます。
5	**保存されたカード会員データを保護する。**ビジネスプロセスを分析し、PAN の保存が必要であると決定した組織の場合、マイルストーン 5 ではそれらの保存されたデータの主な保護メカニズムを対象とする。
6	**残りの準拠作業を終了し、すべてのコントロールが実施されていることを確認する。**マイルストーン 6 の目的は、PCI DSS 要件を完了し、カード会員データ環境の保護に必要な残りすべての関連するポリシー、手順、プロセスを終了することにある。

PCI DSS 要件 v3.2	マイルストーン					
	1	2	3	4	5	6
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						
1.1 以下を含むファイアウォールとルーターの構成基準を確立し、実施する:						
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						6
1.1.2 ワイヤレスネットワークを含め、カード会員データ環境と他のネットワークとの間のすべての接続を識別化した最新のネットワーク図	1					
1.1.3 システムとネットワーク内でのカード会員データのフローを示す最新図	1					
1.1.4 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		2				
1.1.5 ネットワークコンポーネントを管理するためのグループ、役割、責任に関する記述						6
1.1.6 使用が許可されているすべてのサービス、プロトコル、ポートの業務上の理由と承認の文書化（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）。		2				
1.1.7 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						6
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の接続を制限する、ファイアウォールとルーターの構成を構築する。 *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。*						
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し、それ以外のすべてのトラフィックを特定的に拒否する。		2				
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。		2				
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、ワイヤレス環境とカード会員データ環境間のトラフィックを拒否または、業務上必要な場合、承認されたトラフィックのみを許可するようにファイアウォールを構成する。		2				
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。						
1.3.1 DMZ を実装し、承認された公開サービス、プロトコル、ポートを提供するシステムコンポーネントのみへの着信トラフィックに制限する。		2				
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。		2				
1.3.3 アンチスプーフィング対策を実施し、偽の送信元 IP アドレスを検出して、ネットワークに侵入されないようにブロックする。 （たとえば、内部送信元アドレスを持つインターネットからのトラフィックをブロックするなど。）		2				
1.3.4 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禁止する。		2				
1.3.5 ネットワーク内へは、「確立された」接続のみ許可する。		2				

PCI DSS 要件 v3.2	マイルストーン					
	1	2	3	4	5	6
1.3.6 DMZ やその他の信頼できないネットワークから隔離されている内部ネットワークゾーンで、カード会員データを保存するコンポーネント（データベース）が実装されている。		2				
1.3.7 プライベート IP アドレスとルーティング情報を許可されていない第三者に開示しない。 *注: IP アドレスを開示しない方法には、以下のものが含まれるが、これらに限定されるわけではない:* ● *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 アドレス空間を内部で使用する。*		2				
1.4 インターネットに直接接続するポータブルコンピュータデバイス（会社あるいは従業員が所有するものも含む）で、ネットワークの外側ではインターネットに接続され、また CDE へのアクセスにも使用されるものに（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か同等機能のソフトウェアをインストールする。ファイアウォール（またはそれに相当する）構成には以下が含まれます。 ● 特定の構成設定が定義されている。 ● パーソナルファイアウォール（またはそれに相当する機能）がアクティブに実行中である。 ● パーソナルファイアウォール（またはそれに相当する機能）がモバイルデバイスのユーザによって変更できないようになっている。		2				
1.5 ファイアウォールの管理に関するセキュリティポリシーと操作手順が文書化および使用されており、影響を受ける関係者全員に知らされていることを確認する。		2				
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						
2.1 システムをネットワークに導入する前に、必ずベンダ提供のデフォルト値を変更し、不要なデフォルトアカウントを無効にする。 これは、オペレーティングシステム、セキュリティサービスを提供するソフトウェア、アプリケーション、システムアカウント、POS 端末、ペイメントアプリケーション、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で使用されるがこれらに限定されない、すべてのデフォルトパスワードに適用されます。		2				
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、インストール時にすべての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が、これらに限定されない。		2				
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）。 ● インターネットセキュリティセンター（CIS） ● 国際標準化機構（ISO） ● SANS Institute ● 米国国立標準技術研究所（NIST）			3			

PCI DSS 要件 v3.2	マイルストーン					
	1	2	3	4	5	6
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、ウェブサーバ、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: 仮想化テクノロジを使用している場合は、1 つの仮想システムコンポーネントに主要機能を 1 つだけ実装する。*			3			
2.2.2 システムの機能に必要なサービス、プロトコル、デーモンなどのみを有効にする。			3			
2.2.3 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、またはデーモンに追加のセキュリティ機能を実装する。 *注: SSL/early TLS が使用されている場合、付録 A2 の要件が満たされている必要がある。*		2				
2.2.4 システムセキュリティのパラメータが、誤用を防ぐために設定されている。			3			
2.2.5 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、および不要なウェブサーバなど、すべての不要な機能を削除する。			3			
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。 *注: SSL/early TLS が使用されている場合、付録 A2 の要件が満たされている必要がある。*		2				
2.4 PCI DSS の適用範囲であるシステムコンポーネントのインベントリを維持する。		2				
2.5 ベンダデフォルト値およびその他のセキュリティパラメータの管理に関するセキュリティポリシーと操作手順が文書化されて使用されており、影響を受ける関係者全員に知られていることを確認する。		2				
2.6 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 A1:「共有ホスティングプロバイダでの追加 PCI DSS 要件」に示されているように、特定の要件を満たす必要がある。			3			
要件 3: 保存されるカード会員データを保護する						
3.1 データ保存および廃棄ポリシー、手順、プロセスを実装し、すべてのカード会員データ(CHD)ストレージに少なくとも以下のものを含めようにすることで保存するカード会員データを最小限に抑える。 ● 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 ● カード会員データの特定のデータ保存要件 ● 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 ● 定義された保存要件を超えるカード会員データを安全に廃棄する四半期ごとのプロセス。	1					
3.2 承認後に機密認証データを保存しない(暗号化されている場合でも)。機密認証データを受け取った場合、認証プロセスが完了し次第すべてのデータを復元不可能にする。 以下の場合に、データが安全に保存される場合は、発行者と企業が、機密認証データを保存するため、発行サービスをサポートすることが可能である。 ● 業務上の理由がある ● データが安全に保存されている 機密認証データには、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。	1					

PCI DSS 要件 v3.2	マイルストーン					
	1	2	3	4	5	6
3.2.1 (カードの背面やチップ上の同等のデータなどにある磁気ストライプの)追跡データの完全な内容を承認後に保存しない。このデータは、全トラック、トラック、トラック 1、トラック 2、磁気ストライプデータとも呼ばれます。 注: 通常の取引過程では、磁気ストライプからの以下のデータ要素を保存する必要が生じる場合があります。 ● 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、取引に必要なデータ要素のみを保存します。	1					
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)を承認後に保存しない。	1					
3.2.3 個人識別番号(PIN)または暗号化された PIN ブロックを承認後に保存しない。	1					
3.3 表示時に PAN をマスクして(最初の 6 桁と最後の 4 桁が最大表示桁数)、業務上の正当な必要性がある関係者だけが PAN の最初の 6 桁と最後の 4 桁以外の桁を見ることができるようにする。 *注: カード会員データの表示(法律上、またはペイメントカードブランドによる POS レシート要件など)に関するこれより厳しい要件がある場合は、その要件より優先されることはありません。*					5	
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) ● 強力な暗号化をベースにしたワンウェイハッシュ(PAN 全体をハッシュする必要がある) ● トランケーション(PAN の切り捨てられたセグメントの置き換えにはハッシュを使用できない) ● インデックストークンとパッド(パッドは安全に保存する必要がある) ● 関連するキー管理プロセスおよび手順を伴う、強力な暗号化 *注: 悪意のある個人がトランケーションされた PAN とハッシュ化された PAN の両方を取得した場合、元の PAN を比較的容易に再現することができます。ハッシュ化および切り捨てられた PAN の同じバージョンが事業体の環境に存在する場合、元の PAN を再構築するために、ハッシュ化および切り捨てられたバージョンを関連付けることはできないことを確認する追加コントロールを導入する必要があります。*					5	
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認証および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や一般的なネットワークログイン資格情報を使用しないなどの方法で)。復号キーがユーザアカウントと関連付けられていない。 *注: この要件は他のすべての PCI DSS 暗号化およびキー管理要件に加えて適用されます。*					5	
3.5 カード会員データを漏洩と誤用から保護するために使用されるキーを保護するための手順を文書化し、実施する。 *注: この要件は、保存されているカード会員データを暗号化するキーに適用され、またデータ暗号化キーの保護に使用するキー暗号化キーにも適用される。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。*						

PCI DSS 要件 v3.2	マイルストーン					
	1	2	3	4	5	6
3.5.1 サービスプロバイダ用の追加要件: 以下を含む暗号化アーキテクチャの説明文書を整備する: ● キー強度および有効期限を含む、カード会員データの保護に使用されるすべてのアルゴリズム、プロトコル、キーの詳細 ● 各キーの使用法の説明 ● キー管理に使用される HSM およびその他の SCD のインベントリ *注: この要件は、2018 年 1 月 31 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。*					5	
3.5.2 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。					5	
3.5.3 カード会員データの暗号化/復号に使用される秘密キーは、以下のいずれかの形式(複数可)で常時保存する。 ● 少なくともデータ暗号化キーと同じ強度のキー暗号化キーで暗号化されており、データ暗号化キーとは別の場所に保存されている ● 安全な暗号化デバイス(ホストセキュリティモジュール(HSM)または PTS 承認の加盟店端末装置など)内 ● 業界承認の方式に従う、少なくとも 2 つの全長キーコンポーネントまたはキー共有として *注: 公開キーがこれらの形式で保存されていることは要求されていません。*					5	
3.5.4 暗号化キーを最小限の場所に保存する。					5	
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。 *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す。						
3.6.1 強力な暗号化キーの生成					5	
3.6.2 安全な暗号化キーの配布					5	
3.6.3 安全な暗号化キーの保存					5	
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 SP 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。					5	
3.6.5 クリアテキストキーの知識を持つ従業員が離職したなど、キーの整合性が脆弱になっている場合、またはキーの脆弱性が悪用された可能性がある場合に必要な、キーの破棄または取り替え(アーカイブ、破壊、無効化など)。 注: 破棄された、または取り替えられた暗号化キーを保持する必要がある場合、そのキーを(たとえば、キー暗号化キーを使用することにより)安全にアーカイブする必要がある。アーカイブされた暗号化キーは、復号/検証の目的のためにのみ使用できます。					5	

PCI DSS 要件 v3.2	マイルストーン					
	1	2	3	4	5	6
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。 注: 手動のキー管理操作の例には、キーの生成、伝送、読み込み、保存、破棄などが含まれますが、これらに限定されません。					5	
3.6.7 暗号化キーの不正置換の防止。					5	
3.6.8 暗号化キー管理者が自身の責務を理解し、キー管理者としての責務を受諾する。					5	
3.7 保存されているカード会員データを保護するためのセキュリティポリシーと操作手順が文書化および使用されており、影響を受ける関係者全員に知られていることを確認する。					5	
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						
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、以下を含む強力な暗号化とセキュリティプロトコルを使用する。 • 信頼できるキーと証明書のみを受け入れる。 • 使用されているプロトコルが、安全なバージョンまたは構成のみをサポートしている。 • 暗号化の強度が使用中の暗号化方式に適している。 *注: SSL/early TLS が使用されている場合、付録 A2 の要件が満たされている必要がある。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が、これらに限定されない。* • *インターネット* • *802.11 とブルートゥースを含むワイヤレステクノロジ* • *グローバル移動通信システム（GSM）や符号分割多元接続（CDMA）などの携帯端末テクノロジ* • *汎用パケット無線サービス（GPRS）* • *衛星通信。*		2				
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されているワイヤレスネットワークが、認証および伝送用に強力な暗号化を実装するため、業界のベストプラクティスを使用していることを確認する。		2				
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、SMS、チャットなど）で送信しない。		2				
4.3 カード会員データの伝送を暗号化するためのセキュリティポリシーと操作手順が文書化されて使用されており、影響を受ける関係者全員に知られていることを確認する。		2				
要件 5: ウィルス対策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						
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、ウィルス対策ソフトウェアを導入する。		2				
5.1.1 ウィルス対策プログラムが、既知の悪意のあるソフトウェアの全タイプに対して、検出、削除、保護が可能であることを確認する。		2				
5.1.2 一般的に悪意のあるソフトウェアに影響されないとみなされているシステムでは、定期的に評価を行って、進化を続けるマルウェアの脅威を特定して評価することで、システムにウィルス対策ソフトウェアが依然として必要ないかどうかを判断する。		2				

PCI DSS 要件 v3.2	マイルストーン					
	1	2	3	4	5	6
5.2 すべてのウィルス対策メカニズムが以下のように維持されていることを確認する。 ● 最新の状態である ● 定期的にスキャンを行う ● PCI DSS 要件 10.7 に従って監査ログを生成・保持する。		2				
5.3 ウィルス対策メカニズムがアクティブに実行されており、経営管理者からケースバイケースで期間を限って特別に許可されない限り、ユーザが無効にしたり変更できないことを確認する。 *注: ウィルス対策ソリューションは、ケースバイケースで経営管理者により許可されたことを前提に、正当な技術上のニーズがある場合に限り、一時的に無効にすることができます。特定の目的でアンチウィルス保護を無効にする必要がある場合、正式な許可を得る必要があります。アンチウィルス保護が無効になっている間、追加のセキュリティ手段が必要になる場合があります。*		2				
5.4 マルウェアからシステムを保護するためのセキュリティポリシーと操作手順が文書化されて使用されており、影響を受ける関係者全員に知られていることを確認する。		2				
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						
6.1 セキュリティ脆弱性情報の信頼できる社外提供元を使ってセキュリティの脆弱性を特定し、新たに発見されたセキュリティの脆弱性にリスクのランク(「高」、「中」、「低」など)を割り当てる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と考えられる影響の程度に基づいている必要があります。たとえば、脆弱性をランク分けする基準は、CVSS ベーススコア、ベンダによる分類、影響を受けるシステムの種類などを含む場合があります。* *脆弱性を評価し、リスクのランクを割り当てる方法は、組織の環境とリスク評価戦略によって異なります。リスクのランクは、最小限、環境に対する「高リスク」とみなされるすべての脆弱性を特定するものである必要があります。リスクのランク分けに加えて、環境に対する差し迫った脅威をもたらす、重要システムに影響を及ぼす、対処しないと侵害される危険がある場合、脆弱性は「重大」とみなされます。重要システムの例としては、セキュリティシステム、一般公開のデバイスやシステム、データベース、およびカード会員データを保存、処理、送信するシステムなどがあります。*			3			
6.2 すべてのシステムコンポーネントとソフトウェアに、ベンダ提供のセキュリティパッチがインストールされ、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: 要件 6.1 で定義されているリスクのランク分けプロセスに従って、重要なセキュリティパッチを識別する必要があります。*			3			
6.3 内部および外部ソフトウェアアプリケーション(アプリケーションへのウェブベースの管理アクセスを含む)を次のように開発する。 ● PCI DSS (安全な認証やロギングなど)に従って。 ● 業界基準やベストプラクティスに基づいて。 ● ソフトウェア開発ライフサイクル全体に情報セキュリティが組み込まれている *注: これは、社内開発ソフトウェアすべて、および第三者によって開発されたカスタムソフトウェアにも当てはまります。*			3			
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、テスト/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。			3			

PCI DSS 要件 v3.2	マイルストーン					
	1	2	3	4	5	6
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の、本番または顧客のリリース前のカスタムコードを、少なくとも以下の各項を含めてレビューする（手動または自動プロセスによる）。 ● コード変更は、コード作成者以外の、コードレビュー手法と安全なコーディング手法の知識のある人がレビューする。 ● コードレビューにより、コードが安全なコーディングガイドラインに従って開発されたことが保証される ● リリース前に、適切な修正を実装している。 ● コードレビュー結果は、リリース前に管理職によってレビューおよび承認される。*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ウェブ 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。*			3			
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、以下を含める必要がある。			3			
6.4.1 開発/テスト環境を本番環境から分離し、分離を実施するためのアクセス制御を行う。			3			
6.4.2 開発/テスト環境と本番環境での責務の分離			3			
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			3			
6.4.4 システムがアクティブ/実稼働になる前に、システムコンポーネントからテストデータとテストアカウントを削除する。			3			
6.4.5 変更管理手順には、以下を含める必要がある。						6
6.4.5.1 影響の文書化。						6
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。						6
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ないことを確認するための機能テスト。						6
6.4.5.4 回復手順。						6
6.4.6 大幅な変更の完了時に、ただちにすべての関連 PCI DSS 要件を新規または変更されたシステムとネットワークに適用し、ドキュメントを適宜更新する必要がある。 *注: この要件は、2018 年 1 月 31 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。*						6
6.5 次のようにしてソフトウェア開発プロセスで一般的なコーディングの脆弱性に対応する。 ● 開発者に少なくとも年に一度、一般的なコーディングの脆弱性を回避する方法を含む最新の安全なコーディング技法をトレーニングをする。 ● 安全なコーディングガイドラインに基づいてアプリケーションを開発する。 *注: 要件 6.5.1 ～ 6.5.10 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、脆弱性管理のための業界のベストプラクティスは更新されているため（OWASP ガイド、SANS CWE Top 25、CERT Secure Coding など）、現在のベストプラクティスは、これらの要件を使用する必要がある。*			3			
注: 以下の要件 6.5.1 から 6.5.6 は、すべてのアプリケーション（内部または外部）に適用されます。						

PCI DSS 要件 v3.2	マイルストーン					
	1	2	3	4	5	6
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。			3			
6.5.2 バッファオーバーフロー			3			
6.5.3 安全でない暗号化保存			3			
6.5.4 安全でない通信			3			
6.5.5 不適切なエラー処理			3			
6.5.6 脆弱性特定プロセス（PCI DSS 要件 6.1 で定義）で特定された、すべての「高リスク」脆弱性。			3			
注: 以下の要件 6.5.7 ～ 6.5.10 は、ウェブアプリケーションとアプリケーションインタフェース（内部または外部）に適用される。						
6.5.7 クロスサイトスクリプティング（XSS）			3			
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、機能へのユーザアクセス制限の失敗など）			3			
6.5.9 クロスサイトリクエスト偽造（CSRF）			3			
6.5.10 不完全な認証管理とセッション管理			3			
6.6 一般公開されているウェブアプリケーションで、継続的に新たな脅威や脆弱性に対処し、これらのアプリケーションが、次のいずれかの方法によって、既知の攻撃から保護されていることを確認する。 ● 一般公開されているウェブ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。 *注: この評価は、要件 11.2 で実施する脆弱性スキャンとは異なる。* ● ウェブベースの攻撃を検知および回避するために、一般公開されているウェブアプリケーションの手前に、ウェブ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。			3			
6.7 セキュアシステムとアプリケーションを開発・保守するためのセキュリティポリシーと操作手順が文書化されて使用されており、影響を受ける関係者全員に知られていることを確認する。			3			
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						
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。						
7.1.1 以下を含む、各役割のアクセスニーズを定義する ● 各役割が職務上アクセスする必要のあるシステムコンポーネントとデータリソース ● リソースへのアクセスに必要な特権レベル（ユーザ、管理者など）				4		
7.1.2 特権ユーザ ID に与えるアクセス権を職務の実行に必要な最小限の特権に制限する。				4		
7.1.3 個人の職種と職務に基づくアクセス権の割り当て。				4		

PCI DSS 要件 v3.2	マイルストーン					
	1	2	3	4	5	6
7.1.4 適切な権限を持つ関係者による文書化された変更承認の必要性。				4		
7.2 システムコンポーネントで、ユーザの必要性に基づいてアクセスが制限され、特に許可のない場合は「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				4		
7.2.2 職種と職務に基づく、個人への特権の付与。				4		
7.2.3 デフォルトでは「すべてを拒否」の設定。				4		
7.3 カード会員データへのアクセスを制限するためのセキュリティポリシーと操作手順が文書化されて使用されており、影響を受ける関係者全員に知られていることを確認する。				4		

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

8.1 ポリシーと手順を定義して実装することで、次のように、すべてのシステムコンポーネントで、非消費者ユーザと管理者のための適切なユーザ識別および認証の管理が行われるようにする。						
8.1.1 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。		2				
8.1.2 追加、削除、ユーザ ID の変更、資格情報、およびその他の識別オブジェクトを管理する。		2				
8.1.3 契約終了したユーザのアクセスを直ちに取り消す。		2				
8.1.4 90 日以内に非アクティブなユーザアカウントを削除/無効にする。		2				
8.1.5 第三者がリモートアクセス経由でシステムコンポーネントのアクセス、サポート、メンテナンスに使用する ID を以下のように管理する。 ● 必要な期間内だけ有効になり、使用されていないときは無効になっている。 ● 使用時に監視されている。		2				
8.1.6 6 回以下の試行で、ユーザ ID をロックアウトすることによって、アクセスの試行回数を制限する。		2				
8.1.7 最低 30 分間、または管理者がユーザ ID を有効にするまでのロックアウト期間を設定する。		2				
8.1.8 セッションのアイドル状態が 15 分を超えた場合、ターミナルまたはセッションを再度アクティブにするため、ユーザの再認証が必要となる。		2				
8.2 一意の ID を割り当てることに加え、すべてのユーザを認証するため、次の方法の少なくとも 1 つを使用することで、すべてのシステムコンポーネント上での顧客以外のユーザと管理者の適切なユーザ認証管理を確認する。 ● 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）		2				
8.2.1 すべてのシステムコンポーネントで強力な暗号化を使用して、送信と保存中に認証情報（パスワード/パスフレーズなど）をすべて読み取り不能としている。		2				
8.2.2 パスワードのリセット、新しいトークンの準備、新しいキーの生成など、認証情報を変更する前に、ユーザの身元を確認する。		2				

PCI DSS 要件 v3.2	マイルストーン					
	1	2	3	4	5	6
8.2.3 パスワード/パスフレーズは以下を満たす必要がある。 ● パスワードに 7 文字以上が含まれる ● 数字と英文字の両方を含む あるいは、上記のパラメータに等しい複雑さと強度を持つパスワード/パスフレーズ		2				
8.2.4 ユーザパスワード/パスフレーズは、少なくとも 90 日ごと変更する。		2				
8.2.5 これまでに使用した最後の 4 つのパスワード/パスフレーズのいずれかと同じである新しいパスワード/パスフレーズを許可しない。		2				
8.2.6 初期パスワード/パスフレーズとリセットパスワード/パスフレーズをユーザごとに一意の値にリセットし、初回の使用後直ちに変更する。		2				
8.3 すべてのコンソール以外の管理アクセスと CDE に対するすべてのリモートアクセスを多要素認証を使用してセキュリティで保護する。 *注: 多要素認証では、3 つの認証方法のうち最低 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、多要素認証とは見なされない。*						
8.3.1 管理アクセス権限を持つ担当者のすべてのコンソール以外の CDE への管理アクセスに多要素認証を組み込む。 *注: この要件は、2018 年 1 月 31 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。*		2				
8.3.2 ネットワーク外部からのネットワークへのリモートアクセスすべてに(ユーザと管理者、サポートやメンテナンス用の第三者のアクセスを含む)多要素認証を組み込む。		2				
8.4 以下を含む認証手順およびポリシーを文書化し、すべてのユーザに通達する。 ● 強力な認証情報を選択するためのガイダンス ● ユーザが自分の認証情報を保護する法方についてのガイダンス ● 前に使用していたパスワードを再使用しないという指示 ● パスワードが侵害された疑いがある場合にはパスワードを変更するという指示				4		
8.5 次のように、グループ、共有、または汎用の ID やパスワード、または他の認証方法が使用されていない。 ● 汎用ユーザ ID が無効化または削除されている。 ● システム管理作業およびその他の重要な機能に対する共有ユーザ ID が存在しない。 ● システムコンポーネントの管理に共有および汎用ユーザ ID が使用されていない。				4		
8.5.1 サービスプロバイダ用の追加要件: (POS システムやサーバーのサポートのために)顧客環境へのリモートアクセス権を持つサービスプロバイダは、各顧客環境に一意な認証情報(パスワード/パスフレーズなど)を使用する必要がある。 *注: この要件は、複数顧客環境がホストされている共有ホスティングプロバイダ自身のホスティング環境に適用されることは意図されていません。*		2				

PCI DSS 要件 v3.2	マイルストーン					
	1	2	3	4	5	6
8.6 他の認証メカニズムが使用されている場合（物理または論理セキュリティトークン、スマートカード、証明書など）、そのメカニズムの使用は次のように割り当てられている。 ● 認証メカニズムは、個々のアカウントに割り当てなければならず、複数アカウントで共有することはできない。 ● 物理/論理制御により、意図されたアカウントのみがアクセスできるようにする必要がある。				4		
8.7 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（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を含む）が以下のように制限されている。 ● データベースへのユーザアクセス、データベースのユーザクエリ、データベースに対するユーザアクションはすべて、プログラムによる方法によってのみ行われる。 ● 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のみに制限される。 ● データベースアプリケーション用のアプリケーション ID を使用できるのはそのアプリケーションのみである（個々のユーザやその他の非アプリケーションプロセスは使用できない）。				4		
8.8 識別と認証に関するセキュリティポリシーと操作手順が文書化されて使用されており、影響を受ける関係者全員に知られていることを確認する。				4		
要件 9: カード会員データへの物理アクセスを制限する						
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。		2				
9.1.1 ビデオカメラまたはその他のアクセス制御メカニズム（あるいはその両方）を使用して、秘密性の高い領域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、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である。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。*		2				
9.1.2 物理/論理制御を実施することで、誰でもアクセス可能なネットワークジャックへのアクセスを制限する。 たとえば、公共の場や訪問者がアクセス可能なエリアにあるネットワークジャックは、無効にしておき、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にのみ有効にすることができる。または、アクティブなネットワークジャックがあるエリアでは訪問者に常に同行者をつけるプロセスを実施できる。		2				
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、および電気通信回線への物理アクセスを制限する。		2				
9.2 次のよう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開発する。 ● オンサイト要因や訪問者を識別する（バッジの使用など） ● アクセス要件を変更する ● 契約が終了したオンサイト要員や期限切れの訪問者の ID（バッジなど）を無効にする					5	
9.3 オンサイト要員の機密エリアへの物理アクセスを次のように制御する。 ● アクセスが個々の職務に基づいて許可される。 ● 職務の終了後直ちにアクセスを無効とし、鍵、アクセスカードなどすべての物理アクセスメカニズムを返還するか無効にする。		2				

PCI DSS 要件 v3.2	マイルストーン					
	1	2	3	4	5	6
9.4 訪問者を識別し、承認する手順を実施する。 手順には、以下を含める必要がある。						
9.4.1 訪問者は、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、そのエリアにいる間ずっと同行者に付き添われている。					5	
9.4.2 訪問者は識別され、有効期限があり、目視でオンサイト関係者と区別できるバッジその他の ID が与えられる。					5	
9.4.3 施設を出る前、または期限が切れる日にバッジその他の ID の返還を求められる。					5	
9.4.4 訪問者ログを使用して、カード会員データの保存または送信が行われているコンピュータルームやデータセンターなどの施設への訪問者の行動の物理的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。					5	
9.5 すべての媒体を物理的にセキュリティ保護する。					5	
9.5.1 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。					5	
9.6 次の項目を含め、あらゆるタイプの媒体を内部または外部に配布する際の厳格な管理を維持する。						
9.6.1 データの機密性を識別できるように、媒体を分類する。					5	
9.6.2 安全な配達業者または正確に追跡することができるその他の方法によって媒体を送付する。					5	
9.6.3 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していることを確認する（媒体が個人に配布される場合を含む）。					5	
9.7 媒体の保管およびアクセスについて、厳密な管理を維持する。						
9.7.1 すべての媒体の在庫ログを保持し、少なくとも年に一度、媒体の在庫調査を実施する。					5	
9.8 次のように、ビジネスまたは法律上不要になった媒体を破棄する。						
9.8.1 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。破棄する資料を保管する容器を安全に保護する。	1					
9.8.2 カード会員データを再現できないよう、電子媒体上のカード会員データを回復不能にする。	1					
9.9 カードの物理的な読み取りによってペイメントカードデータを取り込むデバイスを改ざんや不正置換から保護する。 *注: この要件には、カード（カードのスワイプやディップ）によるトランザクションに使用されるカード読み取り装置も含まれる。この要件は、コンピュータのキーボードや POS のキーパッドのような手動キー入力コンポーネントには適用されない。*						
9.9.1 装置の最新リストを保持する。リストには以下を含める必要がある。 • 装置のメーカーと型式 • 装置の場所（装置が設置されている店舗の住所など） • 装置の連番や他の一意識別方法		2				

PCI DSS 要件 v3.2	マイルストーン					
	1	2	3	4	5	6
9.9.2 定期的に装置の表面を検査して改ざん（カードスキマーの取り付けなど）や不正置換（連番など装置の特性を調べて偽の装置に差し替えられていないことを確認する）を検出する。 *注: 装置が改ざんされたり不正置換された兆候の例としては、予期していない付着物やケーブルが装置に差し込まれている、セキュリティラベルが無くなっていたり、変更されている、ケースが壊れていたり、色が変わっている、あるいは連番その他の外部マーキングが変更されているなどがある。*		2				
9.9.3 関係者が装置の改ざんや不正置換の試みを認識できるようにトレーニングを実施する。トレーニングには以下を含める必要がある。 • 第三者の修理・保守関係者を名乗っている者に POS 装置へのアクセスを許可する前に、身元を確認する。 • 検証なしで装置を設置、交換、返品しない。 • 装置の周辺での怪しい行動（知らない人が装置のプラグを抜いたり装置を開けたりする）に注意する • 怪しい行動や POS 装置が改ざんや不正置換された形跡がある場合には適切な関係者（マネージャやセキュリティ関係者など）に報告する		2				
9.10 カード会員データへのアクセスを制限するためのセキュリティポリシーと操作手順が文書化されて使用されており、影響を受ける関係者全員に知られていることを確認する。					5	
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						
10.1 システムコンポーネントへのすべてのアクセスを各ユーザにリンクする監査証跡を確立する				4		
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。						
10.2.1 カード会員データへのすべての個人アクセス				4		
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				4		
10.2.3 すべての監査証跡へのアクセス				4		
10.2.4 無効な論理アクセス試行				4		
10.2.5 識別と認証メカニズムの使用および変更（新しいアカウントの作成、特権の上昇を含むがこれらに限定されない）、およびアカウントの変更、追加、削除のすべてはルートまたは管理者権限が必要である。				4		
10.2.6 監査ログの初期化、停止、一時停止				4		
10.2.7 システムレベルオブジェクトの作成および削除				4		
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				4		
10.3.2 イベントの種類				4		
10.3.3 日付と時刻				4		
10.3.4 成功または失敗を示す情報				4		
10.3.5 イベントの発生元				4		
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。				4		

PCI DSS 要件 v3.2	マイルストーン					
	1	2	3	4	5	6
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: ネットワークタイムプロトコル(NTP)は、時刻同期技術の一例である。*				4		
10.4.1 重要なシステムが正確で一貫性のある時刻を持っている。				4		
10.4.2 時刻データが保護されている。				4		
10.4.3 時刻設定は、業界で認知されている時刻ソースから受信されている。				4		
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。						
10.5.1 仕事関連のニーズを持つ個人に監査証跡の表示を制限する。				4		
10.5.2 監査証跡ファイルを不正な変更から保護する。				4		
10.5.3 監査証跡ファイルは、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。				4		
10.5.4 外部に公開されているテクノロジのログを、安全な一元管理の内部ログサーバまたは媒体デバイス上に書き込む。				4		
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、新しいデータの追加は警告を発生させない)。				4		
10.6 すべてのシステムコンポーネントのログとセキュリティイベントを調べ、異常や怪しい活動を特定する。 *注: この要件に準拠するために、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。*						
10.6.1 毎日一度以上以下をレビューする ● すべてのセキュリティイベント ● CHD や SAD を保存、処理、または送信するすべてのシステムコンポーネントのログ ● すべての重要なシステムコンポーネントのログ ● すべてのサーバとセキュリティ機能を実行するシステムコンポーネント(ファイアウォール、侵入検出システム/侵入防止システム(IDS/IPS)、認証サーバ、電子商取引リダイレクションサーバなど)のログ				4		
10.6.2 組織のポリシー、および年間リスク評価によって決定されたリスク管理戦略に基づいて他のシステムコンポーネントすべてのログを定期的にレビューする。				4		
10.6.3 レビュープロセスで特定された例外と異常をフォローアップする。				4		
10.7 監査証跡の履歴を少なくとも 1 年間保持し、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)。				4		

PCI DSS 要件 v3.2	マイルストーン					
	1	2	3	4	5	6
10.8 サービスプロバイダ用の追加要件: 以下の重要なセキュリティ管理システム（ただし、これらに限定されない）の障害をタイムリーに検出し報告するプロセスを実装する。 ● ファイアウォール ● IDS/IPS ● FIM ● アンチウィルス ● 物理アクセス制御 ● 論理アクセス制御 ● 監査ログ記録メカニズム ● セグメンテーションコントロール（使用している場合） *注: この要件は、2018 年 1 月 31 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。*				4		
10.8.1 サービスプロバイダ用の追加要件: 重要なセキュリティコントロールの失敗にタイムリーに対応する。セキュリティコントロールの失敗に対処するためのプロセスには以下のようなものがあります。 ● セキュリティ機能を復元する ● セキュリティ障害の期間（開始と終了の日時）を特定および文書化する ● 根本原因を含む失敗の原因を特定および文書化し、根本原因に対処するために必要な修正を文書化する ● 失敗した際に発生したセキュリティ問題を特定し、対処する ● セキュリティの失敗の結果、さらにアクションが必要かどうかを判定するためにリスク評価を実施する ● 失敗の原因再発を防止するコントロールを実装する ● セキュリティコントロールの監視を再開する *注: この要件は、2018 年 1 月 31 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。*				4		
10.9 ネットワークリソースとカード会員データへのすべてのアクセスを監視するためのセキュリティポリシーと操作手順が文書化され、使用されており、影響を受ける関係者全員に知られていることを確認する。				4		
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						
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（802.11）、すべての承認されているワイヤレスアクセスポイントと承認されていないワイヤレスアクセスポイントを検出し識別するプロセスを実施する。 *注: プロセスで使用される方法には、ワイヤレスネットワークのスキャン、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論理的/物理的な検査、ネットワークアクセス制御（NAC）、無線 IDS/IPS が含まれるがこれらに限定されるわけではない。いずれの方法を使用する場合も、承認されているデバイスと承認されていないデバイスを両方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。*				4		
11.1.1 文書化されている業務上の理由を含め、承認されているワイヤレスアクセスポイントのインベントリを維持する。				4		
11.1.2 不正なワイヤレスデバイスが検出された場合のインシデント対応計画を実装する。		2				

PCI DSS 要件 v3.2	マイルストーン					
	1	2	3	4	5	6
11.2 内部と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）後実行する。 *注: 四半期ごとのスキャンプロセスの複数のスキャンレポートをまとめて、すべてのシステムがスキャンされ、該当するすべての脆弱性に対処されたことを示すことができる。未修正の脆弱性が対処中であることを確認するために、追加の文書が要求される場合がある。* *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、四半期に一度のスキャンに 4 回合格することは要求されない。初回 PCI DSS レビュー以降は毎年、四半期ごとのスキャンに 4 回合格しなければならない。*		2				
11.2.1 四半期ごとの内部脆弱性スキャンを実施する。脆弱性に対応し、事業体の脆弱性ランキング（要件 6.1 参照）に従ってすべての「高リスク」脆弱性が解決されたことを検証するために再スキャンを実施する。スキャンは有資格者が実施する必要がある。		2				
11.2.2 四半期に一度の外部の脆弱性スキャンは、ペイメントカード業界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。スキャンに合格するまで、必要に応じて再スキャンする。 *注: 四半期に一度の外部の脆弱性スキャンは、ペイメントカード業界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。スキャンにおける顧客の責任、スキャンの準備などについては、PCI SSC ウェブサイトで公開されている『ASV プログラムガイド』を参照してください。*		2				
11.2.3 大幅な変更後、必要に応じて内部と外部のスキャン、再スキャンを実施する。スキャンは有資格者が実施する必要がある。		2				
11.3 以下を含むペネトレーションテスト方法を実装する。 • 業界承認のペネトレーションテスト方法（NIST SP800-115 など）に基づいている • CDE 境界と重要システム全体を対象とした対応 • ネットワークの内部と外部からのテスト • セグメンテーションと範囲減少制御の有効性テスト • アプリケーション層のペネトレーションテストは、少なくとも要件 6.5 に記載されている脆弱性を含める必要がある • ネットワーク層のペネトレーションテストには、ネットワーク機能とオペレーティングシステムをサポートするコンポーネントを含める必要がある • 過去 12 カ月にあった脅威と脆弱性のレビューと考慮 • ペネトレーションテスト結果と修正実施結果の保持。		2				
11.3.1 外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、環境へのウェブサーバの追加など）後に実行する。		2				

PCI DSS 要件 v3.2	マイルストーン					
	1	2	3	4	5	6
11.3.2 内部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、環境へのウェブサーバの追加など）後に実行する。		2				
11.3.3 ペネトレーションテストで検出された悪用可能な脆弱性が修正され、テストが繰り返されて修正が確認される。		2				
11.3.4 セグメンテーションを用いて CDE を他のネットワークから分離した場合、少なくとも年に一度とセグメンテーションの制御/方法が変更された後にペネトレーションテストを行って、セグメンテーション方法が運用可能で効果的であり、CDE 内のシステムから適用範囲外のシステムをすべて分離することを確認する。		2				
11.3.4.1 サービスプロバイダ用の追加要件: セグメンテーションが使用されている場合は、少なくとも 6 か月に一度とセグメンテーションの制御/方法が変更された後にセグメンテーション制御のペネトレーションテストを行って PCI DSS スコアを確認する。 *注: この要件は、2018 年 1 月 31 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。*		2				
11.4 侵入を検出/防止するための侵入検出/侵入防止技法をネットワークに組み込む。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。		2				
11.5 変更検出メカニズム（ファイル整合性監視ツールなど）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（変更、追加、削除を含む）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: 変更検出目的で、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を示す。ファイル整合性監視製品などの変更検出メカニズムでは通常、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。*				4		
11.5.1 変更検出ソリューションによって生成された警告に対応するプロセスを実装する。				4		
11.6 セキュリティ監視とテストに関するセキュリティポリシーと操作手順が文書化されて使用されており、影響を受ける関係者全員に知られていることを確認する。				4		
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						
12.1 セキュリティポリシーを確立、公開、維持、普及させる。						6
12.1.1 少なくとも年に一度レビューし、環境が変更された場合にポリシーを更新する。						6

PCI DSS 要件 v3.2	マイルストーン					
	1	2	3	4	5	6
12.2 次のリスク評価プロセスを実装する。 ● 少なくとも年に一度と環境に大きな変更があった場合（買収、合併、移転など）に実施されている ● 重要な資産、脅威、脆弱性を特定する ● 正式な「文書化されたリスク分析」を生成する リスク評価方法の例としては、OCTAVE、ISO 27005、および NIST SP 800-30 が挙げられますが、これらに限定されません。	1					
12.3 重要なテクノロジ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 *注: 重要なテクノロジの例には、リモートアクセスおよびワイヤレステクノロジ、ノートパソコン、タブレット、リムーバブル電子媒体、電子メールの使用、インターネットの使用がありますが、これらに限定されません* これらの使用ポリシーで以下を要求することを確認する。						6
12.3.1 権限を持つ関係者による明示的な承認						6
12.3.2 テクノロジの使用に対する認証						6
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						6
12.3.4 デバイスの所有者、連絡先情報、目的を正確にその場で識別できる方法（ラベル付け、コーディング、デバイスのインベントリ）						6
12.3.5 テクノロジの許容される利用法						6
12.3.6 テクノロジの許容されるネットワーク上の場所						6
12.3.7 会社が承認した製品のリスト						6
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						6
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						6
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媒体へのカード会員データのコピー、移動、保存を禁止する。 承認されたビジネスニーズがある場合、使用ポリシーはデータが適用される PCI DSS 要件すべてに従って保護されることを要求する必要がある。						6
12.4 セキュリティポリシーと手順が、すべての担当者に関する情報セキュリティ責任を明確に定義していることを確認する。						6
12.4.1 サービスプロバイダ用の追加要件: エグゼクティブマネジメンによってカード会員データの保護および PCI DSS 準拠プログムの責任を明確化する。次の項目を含む。 ● PCI DSS 準拠を維持するための全体的な責任 ● PCI DSS 準拠プログラムとエグゼクティブマネジメントへの報告に関する権限の定義 *注: この要件は、2018 年 1 月 31 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。*						6

PCI DSS 要件 v3.2	マイルストーン					
	1	2	3	4	5	6
12.5 個人またはチームに以下の情報セキュリティの責任を割り当てる。						6
12.5.1 セキュリティポリシーおよび手続きを確立、文書化、配布する。						6
12.5.2 セキュリティの警告や情報を監視および分析し、適切な担当者に配布する。						6
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、配布し、すべての状況にタイムリーかつ効率的に対処することを確認する。		2				
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。						6
12.5.5 すべてのデータへのアクセスを監視および管理する。						6
12.6 カード会員データセキュリティポリシーおよび手順を全担当者が認識できるように正式なセキュリティ意識向上プログラムを実装する。						6
12.6.1 担当者の教育を採用時および少なくとも年に一度行う。 注: 方法は、担当者の役割とカード会員データへのアクセスレベルに応じて異なる。						6
12.6.2 担当者は、少なくとも年に一度セキュリティポリシーおよび手順を読み、理解したことを認める必要がある。						6
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、経歴照会がある。) *注: このような可能性のある担当者を、トランザクションの実施で一度に 1 つのカード番号にしかアクセスできないようなレジ係など、特定の役職に採用する場合は、この要件は推奨のみです。*						6
12.8 カード会員データがサービスプロバイダと共有される場合は、次の項目を含め、サービスプロバイダを管理するポリシーと手順を維持および実装する。		2				
12.8.1 提供するサービスの記載を含むサービスプロバイダのリストを維持する。		2				
12.8.2 サービスプロバイダが自社の所有する、または顧客に委託されて保管、処理、伝送する、あるいは顧客のカード会員データ環境の安全に影響を及ぼすような、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、書面での契約が維持されている。 *注: 同意の正確な言葉づかいは、両当事者間の同意事項、提供サービスの詳細、各当事者に割り当てられた責任によって異なります。同意には、この要件に記載されているのとまったく同じ言葉づかいを含める必要はありません。*		2				
12.8.3 契約前の適切なデューデリジェンスを含め、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。		2				
12.8.4 少なくとも年に一度、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。		2				
12.8.5 どの PCI DSS 要件がそれぞれのサービスプロバイダにより管理され、どの要件が対象の事業体により管理されるかについての情報を維持する。		2				

PCI DSS 要件 v3.2	マイルストーン					
	1	2	3	4	5	6
12.9 サービスプロバイダ用の追加要件: サービスプロバイダが自社の所有する、または顧客に委託されて保管、処理、伝送する、あるいは顧客のカード会員データ環境の安全に影響を及ぼすような、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ている。 *注: 同意の正確な言葉づかいは、両当事者間の同意事項、提供サービスの詳細、各当事者に割り当てられた責任によって異なります。同意には、この要件に記載されているのとまったく同じ言葉づかいを含める必要はありません。*		2				
12.10 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。						
12.10.1 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		2				
12.10.2 要件 12.10.1 に列挙されたすべての要素を含むテストプランの見直しを、少なくとも年に一度行う。		2				
12.10.3 警告に 24 時間 365 日体制で対応できる担当者を指定する。		2				
12.10.4 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。		2				
12.10.5 侵入検知、侵入防止、ファイアウォール、ファイル整合性監視システムを含むがこれらに限定されない、セキュリティ監視システムからの警告を含める。		2				
12.10.6 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、業界の発展を組み込むプロセスを作成する。		2				
12.11 サービスプロバイダ用の追加要件: 少なくとも四半期に一度、担当者がセキュリティポリシーと操作手順を遵守しているかの見直しを行う。見直しには以下のプロセスを含める必要がある。 ● 日常のログのレビュー ● ファイアウォールルールセットのレビュー ● 新しいシステムに構成基準を適用しているか ● セキュリティに関する警告への対応 ● 変更管理プロセス *注: この要件は、2018 年 1 月 31 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。*						6

PCI DSS 要件 v3.2	マイルストーン					
	1	2	3	4	5	6
12.11.1 サービスプロバイダ用の追加要件: 以下の項目を含む四半期見直しプロセスの文書を整備する。 • 見直しの結果の文書化 • PCI DSS 準拠プログラムの責任者による結果の見直しと承認 *注: この要件は、2018 年 1 月 31 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。*						6
付録 A1: 共有ホスティングプロバイダ向けの PCI DSS 追加要件						
A1 各事業体(加盟店、サービスプロバイダ、またはその他の事業体)のホスト環境とデータを、A1.1 ～ A1.4 に従って保護する。 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ります。 *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。*			3			
A1.1 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。			3			
A1.2 各事業体のアクセスおよび特権が、その事業体のカード会員データ環境のみに制限されている。			3			
A1.3 ログ記録と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一意であり、PCI DSS 要件 10 と一致していることを確認する。			3			
A1.4 ホストされている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。			3			
付録 A2: SSL/early TLS を使用している事業体向けの PCI DSS 追加要件 *注: この付録は CDE または CHD を保護するために SSL/early TLS をセキュリティ制御として使用している事業体に適用されます。*						
A2.1 POS POI 端末(および接続先の SSL/TLS ターミネーションポイント)が SSL/early TLS を使用している場合、事業体は以下の両方の条件を満たす必要があります。 • デバイスがこれらのプロトコルに対する既知の攻撃を受けやすいものでないことを確認する または: • 正式なリスク緩和および緩和計画が整備されている		2				
A2.2 既存の実装(A2.1 で許可された以外)のある事業体が SSL/early TLS を使用している場合は、正式なリスク緩和および緩和計画が整備されている必要がある。		2				
A2.3 サービスプロバイダ用の追加要件: すべてのサービスプロバイダは、2016 年 6 月 30 日までに、安全なサービス提供を行うようにする必要があります。 *注: 2016 年 6 月 30 日までは、サービスプロバイダは自ら提供するサービスに安全なプロトコルのオプションを含めるか、または文書化したリスク緩和および緩和計画(A2.2 参照)に 2016 年 6 月 30 日以前に設定した安全なプロトコルオプション提供の目標期日を含める必要があります。この期日以降は、すべてのサービスプロバイダは自らのサービスに安全なプロトコルのオプションを提供する必要があります。*		2				