

**PCI**

データセキュリティ基準(PCIDSS)

自己査定アンケート**D**

および遵守証明書

---

その他すべての加盟店と

**SAQ**認定サービスプロバイダー

---

バージョン1.1

2008年2月

## 目次

<b>PCIデータセキュリティ基準(PCIDSS) : 関連文書</b> .....	<b>iii</b>
開始前に .....	<b>iv</b>
自己査定アンケートの完了 .....	<b>iv</b>
<b>PCI DSS遵守 – 完了ステップ</b> .....	<b>iv</b>
特定要件除外のガイダンス .....	<b>v</b>
<b>遵守証明書、SAQ D—加盟店バージョン</b> .....	<b>1</b>
<b>遵守証明書、SAQ D—サービスプロバイダーバージョン</b> .....	<b>6</b>
<b>自己査定アンケートD</b> .....	<b>11</b>
<b>安全なネットワークの構築と管理</b> .....	<b>11</b>
要件 1 : カード会員データを保護するために、ファイアウォール設定をインストールし、管理する。 .....	<b>11</b>
要件 2 : システムパスワードおよびその他セキュリティパラメータは、ベンダーの初期設定をそのまま使用しない。 .....	<b>13</b>
<b>カード会員データの保護</b> .....	<b>16</b>
要件 3 : 保管されたカード会員データを保護する。 .....	<b>16</b>
要件 4 : オープンまたはパブリックネットワークのカード会員データの送信を暗号化する。 .....	<b>18</b>
<b>脆弱性管理プログラムの管理</b> .....	<b>19</b>
要件 5 : ウィルス対策ソフトウェアまたはプログラムを定期的に使用し、更新する。 .....	<b>19</b>
要件 6 : 安全なシステムおよびアプリケーションを開発、管理する。 .....	<b>20</b>
<b>厳しいアクセス規制措置の実装</b> .....	<b>23</b>
要件 7 : 既知の業務のニーズによりカード会員データへのアクセスを制限する。 .....	<b>23</b>
コンピュータへのアクセスには、個人それぞれ独自のIDを割り当てる。 .....	<b>23</b>
要件 9 : カード会員データへの物理的アクセスを制限する。 .....	<b>25</b>
<b>定期的なネットワークの監視およびテスト</b> .....	<b>28</b>
要件 10 : ネットワーク資源およびカード会員データへのすべてのアクセスをトラックし監視する。 .....	<b>28</b>
要件 11 : セキュリティシステムおよび手順を定期的にテストする。 .....	<b>30</b>
<b>情報セキュリティ方針の管理</b> .....	<b>32</b>
要件 12 : 従業員と契約者に向けた、情報セキュリティ取り扱いの方針を管理する。 .....	<b>32</b>
<b>PCI DSS ホスティングプロバイダ適用性 (PCI DSS Applicability for Hosting Providers)</b> .....	<b>35</b>
要件 A.1 : 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します。 .....	<b>35</b>
<b>代替管理手段付属書</b> .....	<b>36</b>
要件 3.4 の代替管理手段 .....	<b>36</b>
代替管理手段ワークシート .....	<b>37</b>

代替管理ワークシート一記入例 .....38

---

## PCI データセキュリティ基準(PCIDSS) : 関連文書

---

以下の文書は、加盟店とサービスプロバイダーのPCIデータセキュリティ基準(PCIDSS)およびPCI DSS SAQの理解の促進のために作成されたものです。

文書	対象
PCIデータセキュリティ基準(PCIDSS)	すべての加盟店とサービスプロバイダー
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ー
PCIデータセキュリティ基準(PCIDSS): 自己査定ガイドラインとインストラクション	すべての加盟店とサービスプロバイダー
PCIデータセキュリティ基準(PCIDSS): 自己査定アンケートA(PCI DSS SAQ A)と証明書	加盟店 <sup>1</sup>
PCIデータセキュリティ基準(PCIDSS): 自己査定アンケートBと証明書	加盟店 <sup>1</sup>
PCIデータセキュリティ基準(PCIDSS): 自己査定アンケートCと証明書	加盟店 <sup>1</sup>
PCIデータセキュリティ基準(PCIDSS): 自己査定アンケートDと証明書	サービスプロバイダーとすべてのその他加盟店 <sup>1</sup>
PCI DSS用語集、略語、および頭文字語	すべての加盟店とサービスプロバイダー

---

<sup>1</sup> 適切な自己査定アンケートを決定するには、*PCI データセキュリティ基準: 自己査定ガイドラインとインストラクション*、「あなたのベンダーに最もよく合う SAQ および証明書の選び方」を参照してください。

## 開始前に

---

### 自己査定アンケートの完了

SAQ D は、以下の表に簡潔に説明されている、また *PCI DSS 自己査定アンケートインストラクション* および *ガイドライン* に完全に説明されている SAQ 適格サービスプロバイダー、および SAQ A-C の詳細を満たさないすべての加盟店のために作成されたものです。

SAQ 認証タイプ	説明	SAQ
1	非対面式(電子商取引かメール/電話による注文の)加盟店で、すべてのカード会員データ機能が外部に委託されている。これは対面式の加盟店に適用されることはありません。	A
2	カード会員データの電子的保管のない、インプリントのみの加盟店。	B
3	カード会員データの電子的保管のない、スタンドアロン型端末の加盟店。	B
4	カード会員データの電子的保管のない、POS システムがインターネットに接続されていない加盟店。	C
5	(以上の SAQs A-C への説明に含まれていない)すべての他の加盟店、およびカードブランドに SAQ を完了する必要がある定義されるすべてのサービスプロバイダー。	D

上記の SAQ A-C への基準を満たさないこれらの加盟店、およびカードブランドに SAQ を完了する必要があると定義されるすべてのサービスプロバイダーは、本書および *PCI DSS 自己査定アンケートインストラクション* および *ガイドライン* で、SAQ 認証タイプ 5 と定義されています。

SAQ D を完了する会社の多くは各 PCI DSS 要件の遵守を立証する必要がありますが、特定のビジネスモデルの会社には適用されない要件もあります。例えば、潜在的にワイヤレステクノロジーを使用しないベンダーは、ワイヤレステクノロジーに特有の PCI DSS のセクションの遵守を立証することを求められません。ワイヤレステクノロジーおよび他の特定の要件の除外についての情報は、以下のガイダンスをご覧ください。

アンケートの各セクションでは、PCI データセキュリティ基準(PCI DSS)の要件に基づいて、特定のセキュリティ分野に焦点をあてています。

### PCI DSS 遵守 – 完了ステップ

1. 自己査定アンケートインストラクションおよびガイドラインに従って、自己査定アンケート (SAQ D) を完了してください。
2. PCI SSC 認定スキャンングベンダー(ASV)により完全な脆弱性スキャンを行い、ASV より安全であるという診断の証拠を取得してください。
3. 遵守証明書をすべて完了させてください。
4. SAQ、脆弱性スキャン合格証、遵守証明書を、その他求められる文書すべてと一緒に (加盟店は) アクワイアラに、または (サービスプロバイダーは) カードブランドまたはリクエストに提出してください。

## 特定要件除外のガイダンス

PCI DSSへの遵守を証明するためにSAQ Dに回答することを求められている場合、以下の例外が考慮されることがあります。

- ワイヤレスに特有の質問は、あなたのネットワークのどこかにワイヤレスが存在する場合にのみ回答される必要があるものです(要件 1.3.8、2.1.1、4.1.1)。あなたのネットワークにワイヤレスが存在しない場合でも、アナライザが加盟店の知らないところで追加された不正または非認定デバイスを検出するため、要件11.1(ワイヤレスアナライザの使用)は回答する必要があることにご注意ください。
- カスタムアプリケーションおよびコード (要件6.3-6.5)は、あなたの会社が独自のカスタムウェブアプリケーションを作成している場合のみ回答する必要があります。
- データセンターに特有の質問(要件9.1-9.4)は、専用データセンターまたはサーバールームが存在する場合のみ回答する必要があります。専用のデータセンターとは、PCI SSCによると、IT基盤(アプリケーションサーバー、データベースサーバー、ウェブサーバー、および/またはネットワークデバイス)を中心に収容し、その主な目的がカード会員データの保管、プロセス、送信である、物理的に安全な部屋または構造であると定義されています。「データセンター」は、サーバールーム、ネットワークオペレーションセンター(NOC)、ISPまたはホスティングプロバイダーのコロケーション施設と同義語であることがあります。

## 遵守証明書、SAQ D—加盟店バージョン

### 提出方法

加盟店は PCI データセキュリティ基準(PCIDSS)の加盟店の遵守状態の宣言として遵守証明書に記入する必要があります。すべての適用セクションに記入し、本書内の「PCI DSS 遵守 – 完了ステップ」の提出方法を参照してください。

#### パート1 認定審査機関(QSA)会社情報 (該当する場合)

ベンダー名：			
QSA 問い合わせ担当者名：		タイトル：	
電話：		電子メール：	
事業所住所：			
州／県：		国：	郵便番号：
URL：			

#### パート2 加盟店会社情報

ベンダー名：		データベース管理者 (DBA(S))：	
問い合わせ担当者名：		タイトル：	
電話：		電子メール：	
事業所住所：			
州／県：		国：	郵便番号：
URL：			

#### パート 2a 加盟店業種 (適用するものすべてチェックしてください)：

- 小売ベンダー       電気通信       食料品店とスーパーマーケット  
 石油       電子商取引       メール／電話による注文  
 その他 (記入してください)：

PCI DSS 審査に含まれる施設および所在地をリストしてください。

#### パート2b 関係

あなたのベンダーは、1つ以上の第三者サービスプロバイダー(例えば、ゲートウェイ、ウェブホスティングベンダー、航空券予約代理店、ロイヤルティプログラムベンダーなど)と関係を結んでいますか？       はい       いいえ

あなたのベンダーには、1つ以上のアクワイアラとの関係がありますか？

はい  いいえ

## パート2c 取引処理

使用しているペイメントアプリケーション(PA) :

ペイメントアプリケーション(PA)バージョン :

## パート 3 PCI DSS 認証

(completion date)のSAQ Dに述べられた結果に基づいて、(Merchant Company Name)は以下の遵守状態を表明します。(1つをチェックする)

- 遵守** : PCI SAQのすべてのセクションを完了し、そのすべての質問に対し「はい」と答えた結果、評価は全面的**遵守**となり、PCI SSC認定スキャンベンダーによる脆弱性スキャンで合格であるという診断を受け、(Merchant Company Name)のPCI DSSへの完全な遵守が示されました。
- 未遵守** : PCI SAQのすべてのセクションが完了しておらず、質問のいくつかに対し「いいえ」と答えた結果評価が全面的**未遵守**となった、またはPCI SSC認定スキャンベンダーによる脆弱性スキャンで合格であるという診断を受けていないために、(Merchant Company Name)のPCI DSSへの完全な遵守が示されていません。
- 遵守の 目標日程 :
    - 未遵守の状態でのこのフォームを提出する事業者は、本ドキュメントのパート4にある行動計画を完了することを求められることがあります。カードブランドによってはこのセクションを必要としないものもありますので、パート4を完了する前にアクワイアラもしくはカードブランドを確認してください。

## パート3a 遵守状況の確認

加盟店は以下を確認します。

- PCI DSS自己査定アンケートD、バージョン(version of SAQ)は同書にあるインタラクションに従って完了されました。
- 上述のSAQおよび本証明書にあるすべての情報は、自社の査定の結果を公正に示すものです。
- 自社は、使用している決済システムが認証後に機密認証データを保管しないものであることを、ペイメントアプリケーション(PA)ベンダーに確認しました。
- 自社はPCI DSSを読み、いかなるときもPCI DSSへの完全な遵守を行う必要があることを認めます。
- 決済認証後、磁気ストライプ（例えば、追跡）データ<sup>2</sup>、CAV2、CVC2、CID、またはCVV2データ<sup>3</sup>、もしくは暗証番号データ<sup>4</sup>がこの認証中に審査されるいかなるシステムにも保管された形跡はありません。

## パート3b 加盟店承認

<sup>2</sup> 対面式決済の認証に使用される磁気ストライプ内にエンコードされたデータ。決済認証の後、事業者は磁気ストライプデータ全体を保持することはありません。追跡データの中で、保持してもよいものは、カード番号、有効期限、氏名のみです。

<sup>3</sup> 署名欄かその右、もしくはクレジットカード表面に印刷されている3桁または4桁の数字は顔面識決済に使用されるもの。

<sup>4</sup> 対面式決済中に、カード所有者により入力された暗証番号(PIN)、および/または決済メッセージ中に暗号化されたPINブロック。

加盟店役員の署名 ↑	日付 ↑
加盟店役員名 ↑	役職 : ↑
加盟店ベンダー代表 ↑	

#### パート4 未遵守の行動計画

各要件の適切な「遵守状態」を選択してください。要件のいずれかに「いいえ」と回答する場合、要件を遵守する日程および要件を満たす行動の詳細を簡単に説明し、提出する必要があります。カードブランドによってはこのセクションを必要としないものもありますので、パート4を完了する前にアクワイアラもしくはカードブランドを確認してください。

PCI DSS 要件	要件の詳細	遵守状態(1つを選択してください)		改善日程および行動 (遵守状態が「いいえ」である場合)
		はい	いいえ	
1	カード会員データを保護するために、ファイアウォール設定をインストールし、管理する。	<input type="checkbox"/>	<input type="checkbox"/>	
2	システムパスワードおよびその他セキュリティパラメータは、ベンダーの初期設定をそのまま使用しない。	<input type="checkbox"/>	<input type="checkbox"/>	
3	保管されたカード会員データを保護する。	<input type="checkbox"/>	<input type="checkbox"/>	
4	オープンまたはパブリックネットワークのカード会員データの送信を暗号化する。	<input type="checkbox"/>	<input type="checkbox"/>	
5	ウィルス対策ソフトウェアを使用し、定期的に更新する。	<input type="checkbox"/>	<input type="checkbox"/>	
6	安全なシステムおよびアプリケーションを開発、管理する。	<input type="checkbox"/>	<input type="checkbox"/>	
7	既知の業務のニーズによりカード会員データへのアクセスを制限する。	<input type="checkbox"/>	<input type="checkbox"/>	
8	コンピュータへのアクセスには、個人それぞれ独自のIDを割り当てる。	<input type="checkbox"/>	<input type="checkbox"/>	
9	カード会員データへの物理的アクセスを制限する。	<input type="checkbox"/>	<input type="checkbox"/>	
10	要件 10：ネットワーク資源およびカード会員データへのすべてのアクセスをトラックし監視する。	<input type="checkbox"/>	<input type="checkbox"/>	
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。	<input type="checkbox"/>	<input type="checkbox"/>	

		遵守状態(1つを選択してください)	
12	情報セキュリティを扱う方針を管理する。	<input type="checkbox"/>	<input type="checkbox"/>

## 遵守証明書、SAQ D—サービスプロバイダーバージョン

### 提出方法

加盟店は PCI データセキュリティ基準(PCIDSS)の加盟店の遵守状態の宣言として遵守証明書に記入する必要があります。すべての適用セクションに記入し、本書内の「PCI DSS 遵守 – 完了ステップ」の提出方法を参照してください。

#### パート1 認定審査機関(QSA)ベンダー情報 (該当する場合)

ベンダー名：				
QSA 問い合わせ担当者名：		タイトル：		
電話：		電子メール：		
事業所住所：				
州／県：		国：		郵便番号：
URL：				

#### パート2 サービスプロバイダー会社情報

ベンダー名：				
問い合わせ担当者名：		タイトル：		
電話：		電子メール：		
事業所住所：				
州／県：		国：		郵便番号：
URL：				

#### パート2a サービス

提供サービス (適用するものすべてをチェックしてください):

- |                                      |                                       |  |
|--------------------------------------|---------------------------------------|--|
| <input type="checkbox"/> 認証サーバー      | <input type="checkbox"/> ロイヤルティプログラム  | <input type="checkbox"/> 3-D セキュア・アクセス・コントロール・ |
| <input type="checkbox"/> スイッチング      | <input type="checkbox"/> IPSP (電子商取引) | <input type="checkbox"/> 磁気ストライプ決済処理           |
| <input type="checkbox"/> ペイメントゲートウェイ | <input type="checkbox"/> 清算 & 決済      | <input type="checkbox"/> MO/TO 決済処理            |
| <input type="checkbox"/> ホスティング      | <input type="checkbox"/> 発行処理         | <input type="checkbox"/> その他 (具体的に記入してください):   |

PCI DSS 審査に含まれる施設および所在地をリストしてください。

## パート2b 関係

あなたのベンダーは、1つ以上の第三者サービスプロバイダー(例えば、ゲートウェイ、ウェブホスティングベンダー、航空券予約代理店、ロイヤルティプログラムベンダーなど)と関係を結んでいますか？  はい  いいえ

## パート2c : 決済処理

あなたの業務ではどのように、またどのような性質でカード会員データを保管、処理および/または送受信しますか？

使用している、またはあなたのサービスの一部として提供されたペイメントアプリケーション(PA) :

ペイメントアプリケーション(PA)バージョン :

## パート 3 PCI DSS 認証

(completion date of SAQ)のSAQ Dに述べられた結果に基づいて、(Service Provider Company Name)は以下の遵守状態を表明します。(1つをチェックする)

- 遵守** : PCI SAQのすべてのセクションを完了し、そのすべての質問に対し「はい」と答えた結果、評価は全面的**遵守**となり、またPCI SSC認定スキャンベンダーによる脆弱性スキャンで合格であるという診断を受けたので、(Service Provider Company Name)のPCI DSSへの完全な遵守が示されました。
- 未遵守** : PCI SAQのすべてのセクションが完了しておらず、質問のいくつかに対し「いいえ」と答えた結果評価が全面的**未遵守**となった、またはPCI SSC認定スキャンベンダーによる脆弱性スキャンで合格であるという診断を受けていないため、(Service Provider Company Name)のPCI DSSへの完全な遵守が示されていません。
- 遵守の **目標日程** :
  - 未遵守の状態でのこのフォームを提出する事業者は、本ドキュメントのパート4にある行動計画を完了することを求められることがあります。カードブランドによってはこのセクションを必要としないものもありますので、パート4を完了する前にアクワイアラもしくはカードブランドを確認してください。

## パート3a 遵守状況の確認

サービスプロバイダーは以下を確認します。

- PCI DSS自己査定アンケートD、バージョン(insert version number)は、そこに示された指示に従って完了されました。
- 上記に参照したSAQ内および本証明のすべての情報は、自社の査定の結果を公正に表すものです。
- 自社はPCI DSSを読み、いかなるときもPCI DSSへの完全な遵守を行う必要があることを認めます。
- 決済認証後、磁気ストライプ (例えば、追跡)データ<sup>5</sup>、CAV2、CVC2、CID、またはCVV2データ<sup>6</sup>、もしくは暗証番号データ<sup>7</sup>がこの認証中に審査されるいかなるシステムにも保管された形跡はありません。

## パート3b サービスプロバイダー承認

<sup>5</sup> 対面式決済の認証に使用される磁気ストライプ内にエンコードされたデータ。決済認証の後、事業者は磁気ストライプデータ全体を保持することはありません。追跡データの中で、保持してもよいものは、カード番号、有効期限、氏名のみです。

<sup>6</sup> 署名欄かその右、もしくはクレジットカード表面に印刷されている3桁または4桁の数字は非対面式決済に使用されるもの。

<sup>7</sup> 対面式決済中に、カード所有者により入力された暗証番号(PIN)、および/または決済メッセージ中に暗号化されたPINブロック。

サービスプロバイダー役員の署名 ↑	日付 ↑
サービスプロバイダー役員名 ↑	役職 : ↑
サービスプロバイダーベンダー代表 ↑	

#### パート4 未遵守の行動計画

各要件の適切な「遵守状態」を選択してください。要件のいずれかに「いいえ」と回答する場合、要件を遵守する日程および要件を満たす行動の詳細を簡単に説明し、提出する必要があります。カードブランドによってはこのセクションを必要としないものもありますので、パート4を完了する前にアクワイアラもしくはカードブランドを確認してください。

PCI DSS 要件	要件の詳細	遵守状態(1つを選択してください)		改善日程および行動 (遵守状態が「いいえ」である場合)
		はい	いいえ	
1	カード会員データを保護するために、ファイアウォール設定をインストールし、管理する。	<input type="checkbox"/>	<input type="checkbox"/>	
2	システムパスワードおよびその他セキュリティパラメータは、ベンダーの初期設定をそのまま使用しない。	<input type="checkbox"/>	<input type="checkbox"/>	
3	保管されたカード会員データを保護する。	<input type="checkbox"/>	<input type="checkbox"/>	
4	オープンまたはパブリックネットワークのカード会員データの送信を暗号化する。	<input type="checkbox"/>	<input type="checkbox"/>	
5	ウィルス対策ソフトウェアを使用し、定期的に更新する。	<input type="checkbox"/>	<input type="checkbox"/>	
6	安全なシステムおよびアプリケーションを開発、管理する。	<input type="checkbox"/>	<input type="checkbox"/>	
7	既知の業務のニーズによりカード会員データへのアクセスを制限する。	<input type="checkbox"/>	<input type="checkbox"/>	
8	コンピュータへのアクセスには、個人それぞれ独自のIDを割り当てる。	<input type="checkbox"/>	<input type="checkbox"/>	
9	カード会員データへの物理的アクセスを制限する。	<input type="checkbox"/>	<input type="checkbox"/>	
10	ネットワーク資源およびカード会員データへのすべてのアクセスをトラックし監視する。	<input type="checkbox"/>	<input type="checkbox"/>	
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。	<input type="checkbox"/>	<input type="checkbox"/>	

12	情報セキュリティを扱う方針を管理する。	<input type="checkbox"/>	<input type="checkbox"/>	
----	---------------------	--------------------------	--------------------------	--

## 自己査定アンケート D

完了日：

### 安全なネットワークの構築と管理

要件1：カード会員データを保護するために、ファイアーウォール設定をインストールし、管理する。

質問	回答：	はい	いいえ	特別な*
1.1 構築されたファイアーウォール設定の基準には以下が含まれていますか？				
1.1.1 すべての外部接続およびファイアーウォール設定への変更を承認およびテストする正式な手順？		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.2 すべてのカード会員データへの接続、ワイアレスネットワークを含む最新ネットワーク図？		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.3 各インターネット接続および非武装地帯(DMZ)と内部ネットワークゾーン間のファイアーウォールに関する要件？		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.4 ネットワークコンポーネントのグループ、役割、論理的管理の責任の説明？		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.5 業務に必要なサービスおよびポートのリスト？		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.6 ハイパーテキスト・トランスファー・プロトコル(HTTP)、セキュア・ソケット・レイヤー(SSL)、セキュア・シェル(SSH)、仮想プライベートネットワーク(VPN)以外の利用可能なプロトコルに関して、正当化の証明および書類がありますか？		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.7 危険性の高いプロトコル(例えば、ファイル・トランスファー・プロトコル[FTP])に関して、プロトコルの使用理由と実行するセキュリティ対策を含む正当化および書類？		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.8 ファイアーウォールおよびルーター規則設定の年4回の点検？		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.9 ルーターの設定基準？		<input type="checkbox"/>	<input type="checkbox"/>	

\* 「不適用」(表示がある場合のみ選択可能)または「代替管理手段を使用」。代替管理手段を使用する組織は、付属書にある代替管理ワークシートに記入する必要があります。

質問		回答：	はい	いいえ	特別な*
1.2	ファイアウォール設定は、カード会員の環境に必要となるプロトコルを除き、「信用しない」ネットワーク、ホストからのトラフィックを拒否するようになっていますか？		<input type="checkbox"/>	<input type="checkbox"/>	
1.3	(a) 公的にアクセス可能なサーバーと、カード会員データを保管するシステムコンポーネントの接続が、ワイヤレスネットワークからの接続も含め、ファイアウォール設定により制限されていますか？ (b) ファイアウォール設定は以下のようになっていますか？		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.1	DMZ内のインターネットプロトコル(IP)アドレスへのインターネットからの進入を制限する (進入フィルタ)。		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.2	インターネットから DMZ への内部アドレスの通過を禁止する。		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.3	(「構築された」接続のみがネットワークに許可される)ダイナミックパケットフィルタリングとして知られるステートフルインスペクションを実行する。		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.4	データベースを DMZ から分離し、内部ネットワークゾーンに配置する。		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.5	カード会員データ環境に必要となる進入および発信トラフィックを制限する。		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.6	ルーター設定ファイルを保管、同期する。(例えば、(ルーターの通常機能の)実行設定ファイル、(機器が再起動された場合の)起動設定ファイルが同じ安全設定となっている必要があります。)		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.7	特別に許可しているものを除き、すべての発信トラフィックを拒否する。		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.8	ワイヤレスネットワークおよびカード会員データ環境の間の境界のファイアウォールのインストールを含み、これらのファイアウォールが、ワイヤレス環境からの、またはトラフィックの制御からのトラフィックを拒否するよう(このようなトラフィックが業務の目的に必要な場合)設定されている。		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
1.3.9	インターネットへ直接接続でき、会社のネットワークへのアクセスに使用されるモバイルおよび従業員が所有するコンピューター(例えば、従業員に使用されるラップトップ)へのパーソナルファイアウォールソフトウェアのインストールを含む。		<input type="checkbox"/>	<input type="checkbox"/>	

質問	回答：	はい	いいえ	特別な*
1.4 (a) 外部ネットワークと（例えばデータベース、ログ、トレースファイルなどの）カード会員データを保管するシステムコンポーネントの直接パブリック・アクセスがファイアーウォール設定により禁止されていますか？		<input type="checkbox"/>	<input type="checkbox"/>	
(b) このコントロールにより、最低でも以下が行われていますか？				
1.4.1 すべてのトラフィックをフィルターおよびスクリーンし、インターネット進入および発信トラフィックの直接ルートを禁止するために DMZ が実行されていますか？		<input type="checkbox"/>	<input type="checkbox"/>	
1.4.2 クレジットカードアプリケーションから DMZ 内の IP アドレスへの発信トラフィックが制限されていますか？		<input type="checkbox"/>	<input type="checkbox"/>	
1.5 内部アドレスが変換され、インターネットに漏洩するのを防ぐために、IP マスカレードが実行されていますか？ ポートアドレス変換(PAT)またはネットワークアドレス変換(NAT)などの RFC1918 アドレススペースを実行する技術を採用してください。		<input type="checkbox"/>	<input type="checkbox"/>	

**要件 2 :** システムパスワードおよびその他セキュリティパラメータは、ベンダーの初期設定をそのまま使用しない。

質問	回答：	はい	いいえ	特別な*
2.1 ベンダーの初期設定は常に、ネットワーク上にシステムをインストールする前に変更されていますか？ 例えば、パスワード、簡易ネットワーク管理プロトコル(SNMP)コミュニティストリング、不必要なアカウントの削除などが挙げられます。		<input type="checkbox"/>	<input type="checkbox"/>	
2.1.1 ワイヤレス環境初期設定は、ワイヤレスシステム導入前に変更されていますか？ ワイヤレス環境初期設定には、WEP キー、デフォルト SSID、パスワード、SNMP コミュニティストリングを含みますが、これに限定されるものではありません。		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
(a) SSID のブロードキャストが無効とされていますか？		<input type="checkbox"/>	<input type="checkbox"/>	
(b) 暗号化および認証に、WPA が可能な場合、WiFi 保護アクセス(WPA と WPA2)技術が有効となっていますか？		<input type="checkbox"/>	<input type="checkbox"/>	

\* 「不適用」（表示がある場合のみ選択可能）または「代替管理手段を使用」。代替管理手段を使用する組織は、付属書にある代替管理ワークシートに記入する必要があります。

2.2	(a) すべてのシステムコンポーネントに対し、設定基準が作成されていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) これらの基準は、既知のセキュリティ上の脆弱性すべてを含んでいますか？また、例えば <b>SysAdmin Audit Network Security Network (SANS)</b> 、 <b>米国標準技術局(NIST)</b> 、 <b>インターネットセキュリティセンター(CIS)</b> などに定義される産業で受け入れられているシステムハードニング基準と一致していますか？	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) このコントロールは、以下を行うものですか？			
2.2.1	サーバーにつき1つのプライマリ機能が実行されていますか？(例えば、ウェブサーバー、データベース、DNSは異なるのサーバーで実行される必要があります。)	<input type="checkbox"/>	<input type="checkbox"/>	
2.2.2	不必要および安全でないサービスおよびプロトコルがすべて無効とされていますか？(デバイス特定の機能に直接必要でないサービスおよびプロトコル)	<input type="checkbox"/>	<input type="checkbox"/>	
2.2.3	システムセキュリティパラメータは悪用を防ぐよう設定されていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
2.2.4	スクリプト、機能、サブシステム、ファイルシステム、不必要なウェブサーバーなどのすべての不必要な機能は削除されていますか？	<input type="checkbox"/>	<input type="checkbox"/>	

質問	回答：	はい	いいえ	特別な*
2.3	<p>ノンコンソール管理的アクセスはすべて暗号化されていますか？ ウェブベースの管理およびその他ノンコンソール管理的アクセスには、SSH、VPN、SSL/TLS (トランスポート・レイヤ・セキュリティ)などの技術を使用してください。</p>	<input type="checkbox"/>	<input type="checkbox"/>	
2.4	<p>ホスティングプロバイダーである場合、あなたのシステムは事業者のホスト環境とデータを保護するよう設定されていますか？ 満たす必要のある特定の要件は、付属書A：「PCI DSS ホスティングプロバイダー適用性」を参照ください。</p>	<input type="checkbox"/>	<input type="checkbox"/>	

\* 「不適用」 (表示がある場合のみ選択可能) または「代替管理手段を使用」。代替管理手段を使用する組織は、付属書にある代替管理ワークシートに記入する必要があります。

## カード会員データの保護

要件 3 : 保管されたカード会員データを保護する。

質問	回答：	はい	いいえ	特別な*
3.1	(a) カード会員データの保管は最小限に抑えられていますか？また、保管量と保管期間は業務、法的、および／または規制を目的とし、制限されていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) データ保管および処分方針がありますか？また、これには上述の制限が含まれていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
3.2	すべてのシステムは、機密認証データの保管に関する以下の要件に従っていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
3.2.1	(カードの裏面、チップ内などにある)磁気ストライプからのトラックのいかなる内容も保管しない。このデータはまた、フルトラック、トラック、トラック 1、トラック 2、磁気ストライプデータと呼ばれます。 <i>通常業務の決済処理では、磁気ストライプからのデータの中で、カード会員の氏名、カード番号(PAN)、有効期限、およびサービスコードが、保有される必要があります。危険性を最小限に抑えるために、業務に必要なデータ要素のみを保管してください。決して、カード認証コードまたは値、または暗証番号認証値のデータ要素を保存しないでください。</i>	<input type="checkbox"/>	<input type="checkbox"/>	
3.2.2	非対面式決済を認証するために使用されるカード認証コードまたは値（決済カードの表面または裏面に印刷されている 3 桁もしくは 4 桁の数字）を保管しない。	<input type="checkbox"/>	<input type="checkbox"/>	
3.2.3	暗証番号(PIN)または暗号化された PIN ブロックを保管しない。	<input type="checkbox"/>	<input type="checkbox"/>	
3.3	カード番号が表示される際、隠されていますか？(最初の 6 桁および最後の 4 桁が表示されてよい最大桁数です。) <i>注記：この要件は、カード番号全てを見る必要のある特定のニーズを持つ従業員およびその他の当事者には適用されません。また、カード会員データの表示に関して実施されているより厳格な要件（例えば店頭(POS)受領書など）に優先するものではありません。</i>	<input type="checkbox"/>	<input type="checkbox"/>	

\* 「不適用」（表示がある場合のみ選択可能）または「代替管理手段を使用」。代替管理手段を使用する組織は、付属書にある代替管理ワークシートに記入する必要があります。

質問	回答：	はい	いいえ	特別な*
<p>3.4 少なくともカード番号は、以下のいずれかの方法で、保管場所(携帯デジタルメディア、バックアップメディア上やログ内のデータ、ワイヤレスネットワークから受信し、保管されたデータなどを含む)で、読み取り不可能とされていますか？</p> <ul style="list-style-type: none"> <li>- 強力な一方向ハッシュ関数(ハッシュ・インデックス)</li> <li>- トランケーション</li> <li>- インデックストークンおよびパッド (パッドは安全に保存されている必要があります)</li> <li>- 関連キー・マネージメント・プロセスおよび手順を伴った強力な暗号</li> </ul> <p><b>アカウント情報の中で、最低でもカード番号は読み取り不可能とされる必要があります。</b></p> <p>何かの理由により、ベンダーがカード会員データを暗号化することができない場合は、付属書B：「保管データ暗号化の補償コントロール」を参照してください。</p>		<input type="checkbox"/>	<input type="checkbox"/>	
<p>3.4.1 (ファイルまたはカラムレベルのデータベース暗号化より、) ディスク暗号化 が使用されている場合、</p>				
<p>(a) 基底オペレーティング・システム・アクセス制御機構とは独立に(例えば、ローカルシステムまたはアクティブ・ディレクトリ・アカウントを使用せずに)、論理的アクセスが管理されていますか？</p>		<input type="checkbox"/>	<input type="checkbox"/>	
<p>(b) 暗号化キーはユーザー・アカウントとは独立していますか？</p>		<input type="checkbox"/>	<input type="checkbox"/>	
<p>3.5 カード会員データを開示や悪用から保護する暗号化キーが使用されていますか？</p>		<input type="checkbox"/>	<input type="checkbox"/>	
<p>3.5.1 キーへのアクセスは必要最低限の人数の管理人に制限されていますか？</p>		<input type="checkbox"/>	<input type="checkbox"/>	
<p>3.5.2 キーは可能な限り最低限の場所と形式で、安全に保管されていますか？</p>		<input type="checkbox"/>	<input type="checkbox"/>	
<p>3.6 (a) カード会員データの暗号化に使用されるキーのためのすべてのキー管理プロセスと手順は、完全に文書化され、実行されていますか？</p> <p>(b) この管理には、以下が含まれていますか？</p>		<input type="checkbox"/>	<input type="checkbox"/>	
<p>3.6.1 多くの強いキーの生成。</p>		<input type="checkbox"/>	<input type="checkbox"/>	
<p>3.6.2 安全なキー配布。</p>		<input type="checkbox"/>	<input type="checkbox"/>	
<p>3.6.3 安全なキー保管。</p>		<input type="checkbox"/>	<input type="checkbox"/>	

質問	回答：	はい	いいえ	特別な*
3.6.4 定期的なキー変更。 <ul style="list-style-type: none"> <li>- 関連アプリケーション(例えば、キー交換)に必要なであると考えられる、または推奨されるとおりに、望ましくは自動的に</li> <li>- 少なくとも年1回は</li> </ul>		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.5 古いキーの破棄		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.6 (キーの異なる部分を知る2人または3人で、キー全体が再現されるように)その知識を分散し、キーの二重統制を構築する。		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.7 認証していないキー変換の防止。		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.8 既知の、または疑わしい改ざんキーの交換。		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.9 古いまたは無効キーの取り消し。		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.10 キー管理者が、キー管理者の責任を理解し、承認するというフォームに署名するという要件。		<input type="checkbox"/>	<input type="checkbox"/>	

**要件4：オープンまたはパブリックネットワークのカード会員データの送信を暗号化する。**

4.1	オープン、パブリック・ネットワーク上での通信の際、カード会員機密データを保護するために、セキュアソケットレイヤー(SSL) / トランスポート・レイヤ・セキュリティ(TLS)およびインターネット・プロトコル・セキュリティ(IPSEC)などの強力な暗号法およびセキュリティプロトコルが使用されていますか？  <i>PCI DSS の範囲にあるオープン、パブリック・ネットワークの例には、インターネット、WiFi (IEEE 802.11x)、グローバル・システム・フォー・モバイルコミュニケーション(GSM)、ジェネラルパケットラジオサービス(GPRS)が挙げられます。</i>	<input type="checkbox"/>	<input type="checkbox"/>	
4.1.1	(a) カード会員データを送受信するワイヤレスネットワークでは、送受信はWi-Fi 保護アクセス(WPA または WPA2) 技術、IPSEC VPN、または SSL/TLS を使用して暗号化されていますか？  <i>機密情報の保護とワイヤレス LAN へのアクセスの保護に関しては、WEP(有線同等プライバシー)を信用しないこと。</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
	(b) WEP が使用されている場合、以下の制御がなされていますか？			

質問	回答：	はい	いいえ	特別な*
- WEPは最小の104ビット暗号キー、および24ビット初期化値で使用する		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
- WEPはWiFi保護アクセス(WPAまたはWPA2)技術、VPN、またはSSL/TLSのみと同時に使用されること。		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
- 共有WEPキーは年4回(もしくは技術的に可能である場合、自動的に)交換されること。		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
- キーへのアクセスを行う従業員が変更されるたびに、共有WEPキーは交換されること。		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
- アクセスは、媒体アクセス制御(MAC)アドレスに基づいて、制限されること。		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
4.2 実施されている方針、手順、業務は、非暗号化カード番号の電子メールでの送信を防ぐものとなっていますか？		<input type="checkbox"/>	<input type="checkbox"/>	

## 脆弱性管理プログラムの管理

要件5：ウイルス対策ソフトウェアまたはプログラムを定期的に使用し、更新する。

質問	回答：	はい	いいえ	特別な*
5.1 ウィルス対策ソフトウェアは、ウイルスの影響を共通に受けるシステムすべて(特にパーソナルコンピューターおよびサーバー)で稼動していますか？  注記：ウイルスの影響を共通に受けるシステムには、UNIXベースのオペレーティングシステムまたはメインフレームは含まれません。		<input type="checkbox"/>	<input type="checkbox"/>	
5.1.1 ウィルス対策プログラムは、スパイウェアやアドウェアを含む他の形式の不当ソフトウェアを検知、削除し、システムを保護することが可能ですか？		<input type="checkbox"/>	<input type="checkbox"/>	
5.2 すべてのウイルス対策装置は最新のもので、積極的に動作しており、スキャンログを作成することができますか？		<input type="checkbox"/>	<input type="checkbox"/>	

\* 「不適用」(表示がある場合のみ選択可能)または「代替管理手段を使用」。代替管理手段を使用する組織は、付属書にある代替管理ワークシートに記入する必要があります。

質問	回答：	はい	いいえ	特別な*
----	-----	----	-----	------

**要件 6 : 安全なシステムおよびアプリケーションを開発、管理する。**

6.1	(a) すべてのシステムコンポーネントおよびソフトウェアには、ベンダーが提供する最新のセキュリティパッチがありますか？	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) 関連セキュリティパッチがリリース 1 ヶ月以内にインストールされていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
6.2	(a) 新たに発見されるセキュリティ上の脆弱性を識別するプロセス (例えば、インターネット上で無料で利用できるアラートサービスを購読する) がありますか？	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) 基準は適切に更新され、新たな脆弱性問題に対処していますか？	<input type="checkbox"/>	<input type="checkbox"/>	
6.3	(a) ソフトウェアアプリケーションは 産業のベストプラクティスに基づき、開発されていますか？また、ソフトウェア開発ライフサイクルを通して、情報セキュリティが組み込まれていますか？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
	(b) このコントロールは、以下を行うものですか？			
6.3.1	すべてのセキュリティパッチ、システム、ソフトウェア設定変更の配備前のテスト。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.3.2	開発、テスト、製作環境を分けること。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.3.3	開発、テスト、製作環境の職務を分けること。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.3.4	テストまたは開発に、製作データ(稼動 PAN)を使用しないこと。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.3.5	製作システムが有効となる前に、テストデータおよびアカウントの削除すること。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A

質問		回答：		特別な*
		はい	いいえ	
6.3.6	有効となる前、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、ユーザ名、パスワードを削除していますか？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.3.7	製品化、または発売される前にカスタムコードを検査し、コーディングの潜在的な脆弱性を識別していますか？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.4	(a) すべてのシステムおよびソフトウェア設定変更は、変更管理手順に従っていますか？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
	(b) この管理は、以下を行うものですか？			
6.4.1	影響の文書化。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.4.2	適切な当事者によるサインオフの管理。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.4.3	業務の機能性のテスト。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.4.4	バックアウト手順。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.5	(a) 安全な Web アプリケーション構築の手引き (Open Web Application Security Project guidelines) などの安全なコーディングガイドラインに基づいて、すべてのウェブアプリケーションが開発されていますか？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
	(b) コーディングの脆弱性を識別するために、カスタムアプリケーションコードが検査されていますか？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
	(c) ソフトウェア開発過程で、以下を含む共通のコーディング脆弱性の防止対策が行われていますか？			
6.5.1	入力が無効とされていますか？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.5.2	アクセスコントロール故障(例えば、ユーザ ID の悪意ある利用)？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.5.3	認証およびセッション管理故障(アカウント機密およびセッションクッキーの使用)？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.5.4	クロスサイトスクリプティング (XSS) アタック？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A

\* 「不適用」(表示がある場合のみ選択可能)または「代替管理手段を使用」。代替管理手段を使用する組織は、付属書にある代替管理ワークシートに記入する必要があります。

質問		回答：		特別な*
		はい	いいえ	
6.5.5	バッファオーバーフロー？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.5.6	インジェクションフロー(例えば、SQL インジェクション)？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.5.7	不適切なエラー処理？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.5.8	安全でない保管？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.5.9	サービスの拒絶？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.5.10	安全でない設定管理？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.6	<p>すべてのウェブ接続アプリケーションは、以下のいずれかの方法を使用し、既知の攻撃から保護されていますか？</p> <ul style="list-style-type: none"> <li>－ 一般的な脆弱性について、アプリケーションセキュリティを専門とするベンダーにすべてのカスタムアプリケーションコードを点検してもらう。</li> <li>－ ウェブ接続アプリケーションの前に、アプリケーションレイヤー・ファイアーウォールをインストールする。</li> </ul> <p>注記：2008年6月30日まで、6.6はベストプラクティスと考えられていましたが、それ以降、要件となりました。</p>	<input type="checkbox"/>	<input type="checkbox"/>	

## 厳しいアクセス規制措置の実装

要件7：既知の業務のニーズによりカード会員データへのアクセスを制限する。

質問	回答：	はい	いいえ	特別な*
7.1	コンピューティング資源およびカード会員情報へのアクセスは、このアクセスを必要とする職を持つ個人に制限されていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
7.2	複数ユーザが存在するシステムについて、実施しているメカニズムはユーザの知りたいことのニーズに基づいて、アクセスを制限していますか？また、特別に許可されない限り「すべてを拒絶」に設定されていますか？	<input type="checkbox"/>	<input type="checkbox"/>	

コンピュータへのアクセスには、個人それぞれ独自のIDを割り当てる。

8.1	システムコンポーネントもしくはカード会員データへのアクセスを許可する前に、すべてのユーザが独自のユーザ名で識別されるようになっていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
8.2	独自のIDの割り当てに加え、すべてのユーザの認証に以下の方法が使用されていますか？ <ul style="list-style-type: none"> <li>- パスワード</li> <li>- トークンデバイス(例えば、セキュアID、証明書、パブリックキー)</li> <li>- バイオメトリクス</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	
8.3	従業員、管理者、サードパーティによるネットワークへのリモートアクセスには、二要素認証が実行されていますか？ <i>リモート認証ダイヤルインサービス(RADIUS)、トークンを伴うターミナルアクセスコントロールシステム(TACACS)、または各々の証明書を伴う(SSL/TLS または IPSEC に基づく)VPN などの技術を使用してください。</i>	<input type="checkbox"/>	<input type="checkbox"/>	
8.4	すべてのパスワードはシステムコンポーネント上での送受信および保管中、暗号化されていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
8.5	すべてのシステムコンポーネント上で、消費者でないユーザおよび管理者に対し、正しいユーザ認証およびパスワード管理コントロールが以下のように実施されていますか？			

\* 「不適用」(表示がある場合のみ選択可能)または「代替管理手段を使用」。代替管理手段を使用する組織は、付属書にある代替管理ワークシートに記入する必要があります。

8.5.1	ユーザ ID およびその他の識別オブジェクトの追加、削除、変更は管理されていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.2	パスワードの再設定の前に、ユーザの身元が確認されていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.3	初期パスワードは各ユーザに独自の値となっていますか？また、各ユーザは初回利用の後、ただちにそのパスワードを変更する必要がありますか？	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.4	終了したユーザのアクセスはただちに無効とされていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.5	使用されていないユーザアカウントは、少なくとも 90 日ごと無効とされていますか？	<input type="checkbox"/>	<input type="checkbox"/>	

質問	回答：	はい	いいえ	特別な*
8.5.6	リモート管理でベンダーに使用されるアカウントは、必要な時間だけ有効にされていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.7	パスワード手順および方針は、カード会員データにアクセスを持つすべてのユーザに知らされていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.8	グループ、共有、または一般アカウントおよびパスワードが無許可とされていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.9	ユーザパスワードは少なくとも 90 日ごとに変更される必要がありますか？	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.10	パスワードの長さは、最低でも 7 文字以上が求められていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.11	パスワードは数字とアルファベット両方を含む必要がありますか？	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.12	個人の新しいパスワードは、過去に使用した 4 つのパスワードと異なるものである必要がありますか？	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.13	6 回以上のアクセスの試みの後、ユーザをロックアウトすることで、繰り返しのアクセスの試みが制限されていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.14	ロックアウトの期間は 30 分、もしくは管理者がユーザ ID を有効とするまでに設定されていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.15	セッションが 15 分以上アイドル状態となる場合、ユーザはパスワードを再入力し、端末を再度有効化する必要がありますか？	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.16	カード会員データを含むいかなるデータベースへのアクセスも認証されていますか？ (これにはアプリケーション、管理者、その他すべてのユーザによるアクセスが含まれます。)	<input type="checkbox"/>	<input type="checkbox"/>	

**要件 9 : カード会員データへの物理的アクセスを制限する。**

9.1	カード会員データを保管、処理、送受信するシステムへの物理的アクセスを制限および監視するために、設備への適切な進入管理が実施されていますか？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
9.1.1	(a) カメラは情報焦点地域を監視していますか？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A

\* 「不適用」 (表示がある場合のみ選択可能) または「代替管理手段を使用」。代替管理手段を使用する組織は、付属書にある代替管理ワークシートに記入する必要があります。

質問	回答：	はい	いいえ	特別な*
(b) ビデオカメラからのデータは監査され、その他の進入と相互関連付けられていますか？		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
(c) ビデオカメラからのデータは法律により制限されない限り、少なくとも3ヶ月保存されていますか？		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
9.1.2 公的にアクセス可能なネットワークジャックへの物理的アクセスは制限されていますか？		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
9.1.3 ワイヤレスアクセスポイント、ゲートウェイ、携帯端末への物理的アクセスは制限されていますか？		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
9.2 カード会員データにアクセス可能な区域内では特に、従業員と訪問者を簡単に区別する手順が実施されていますか？ 「従業員」とは、常勤および非常勤の従業員、派遣社員および人材、企業の敷地に「常駐」のコンサルタントをさします。「訪問者」とは加盟店、従業員の客、サービス員、短期間、通常1日以内、設備に入る必要のある人と定義されます。		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
9.3 すべての訪問者は以下のように扱われます。				
9.3.1 カード会員データが処理および管理される区域に入る前に認可を受けていますか？		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
9.3.2 訪問者を無効とし、非従業員として識別する物理的トークン(例えば、バッジまたはアクセスデバイス)がありますか？		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
9.3.3 設備を出る前に、または有効期限の前に、物理的トークンを返却するよう求められていますか？		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
9.4 (a) 訪問者の活動の物理的監査トレイルを管理するために、訪問者ログが使用されていますか？		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
(b) 訪問者ログは、法律で制限されない限り、最低3ヶ月間保持されていますか？		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
9.5 メディアバックアップは安全な場所、できれば、代替サイトまたはバックアップサイト、または商用ストレージ設備などのオフサイト設備に保管されていますか？		<input type="checkbox"/>	<input type="checkbox"/>	
9.6 カード会員データを含むすべての紙と電子メディアは、物理的に安全ですか？ (このメディアには、コンピュータ、電子メディア、ネットワーク、通信ハードウェア、通信回線、紙の受領書、カード利用控、およびファックスなどが含まれます。)		<input type="checkbox"/>	<input type="checkbox"/>	
9.7 (a) カード会員データを含む、あらゆる種類のメディアの社内、または社外分配に関し、厳重な管理が行われていますか？		<input type="checkbox"/>	<input type="checkbox"/>	
(b) この管理には、以下が含まれていますか？				

質問		回答：	はい	いいえ	特別な*
9.7.1	メディアは、部外秘と識別できるように分類されていますか？		<input type="checkbox"/>	<input type="checkbox"/>	
9.7.2	メディアは安全な宅配便または正確に追跡できる他の発送方法で送られていますか？		<input type="checkbox"/>	<input type="checkbox"/>	
9.8	安全な場所からメディアを動かす前に管理者の承認を得ることを(特にメディアが個人に配布される場合)確実にするプロセスや手順が適所ありますか？		<input type="checkbox"/>	<input type="checkbox"/>	
9.9	カード会員データを含むメディアの保管とアクセシビリティに関し、厳重な管理が行われていますか？		<input type="checkbox"/>	<input type="checkbox"/>	
9.9.1	すべてのメディアは正しく一覧され、安全に保管されていますか？		<input type="checkbox"/>	<input type="checkbox"/>	
9.10	業務上または法律上に必要でなくなった場合、カード会員データを含むメディアは無効にされていますか？ 無効の方法は以下のものである必要があります。		<input type="checkbox"/>	<input type="checkbox"/>	
9.10.1	ハードコピーの文書は、クロスカットシュレッダーにかけるか、焼却するか、またはパルプにされていますか？		<input type="checkbox"/>	<input type="checkbox"/>	
9.10.2	カード会員データが再現できないように、電子メディアは消去、消磁、粉碎、ないしは破壊されていますか？		<input type="checkbox"/>	<input type="checkbox"/>	

## 定期的なネットワークの監視およびテスト

要件 10：ネットワーク資源およびカード会員データへのすべてのアクセスをトラックし監視する。

質問	回答：	はい		特別な*
		はい	いいえ	
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者権限で行われたアクセス)を各個人のユーザに関連付けるプロセスが実施されていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
10.2	すべてのシステムコンポーネントが以下のアクションを再現できるように、自動監査トレイルが実施されていますか？			
10.2.1	すべての個人ユーザのカード会員データへのアクセス	<input type="checkbox"/>	<input type="checkbox"/>	
10.2.2	個人によりルートまたは管理者権限で行われたアクション	<input type="checkbox"/>	<input type="checkbox"/>	
10.2.3	すべての監査トレイルへのアクセス	<input type="checkbox"/>	<input type="checkbox"/>	
10.2.4	無効な論理的アクセスの試み	<input type="checkbox"/>	<input type="checkbox"/>	
10.2.5	身元確認および認証メカニズムの使用	<input type="checkbox"/>	<input type="checkbox"/>	
10.2.6	監査ログの初期化	<input type="checkbox"/>	<input type="checkbox"/>	
10.2.7	システムレベルのオブジェクト作成および削除	<input type="checkbox"/>	<input type="checkbox"/>	
10.3	各アクションにつき、すべてのシステムコンポーネントに以下の監査トレイル入力記録されていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
10.3.1	ユーザ確認	<input type="checkbox"/>	<input type="checkbox"/>	
10.3.2	アクションの種類	<input type="checkbox"/>	<input type="checkbox"/>	
10.3.3	日時	<input type="checkbox"/>	<input type="checkbox"/>	
10.3.4	成功または失敗の表示	<input type="checkbox"/>	<input type="checkbox"/>	
10.3.5	アクションの起因	<input type="checkbox"/>	<input type="checkbox"/>	
10.3.6	影響データ、システムコンポーネント、リソースの識別または名前	<input type="checkbox"/>	<input type="checkbox"/>	
10.4	すべての重要なシステム時計と時間が同期されていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
10.5	(a) 監査トレイルは改ざんできないよう、安全に保管されていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) この管理は、以下を行うものですか？			

\* 「不適用」(表示がある場合のみ選択可能)または「代替管理手段を使用」。代替管理手段を使用する組織は、付属書にある代替管理ワークシートに記入する必要があります。

質問		回答：	<u>はい</u>	<u>いいえ</u>	<u>特別な*</u>
10.5.1	監査トレイルの閲覧は、職務において必要とする人に制限されていますか？		<input type="checkbox"/>	<input type="checkbox"/>	
10.5.2	監査トレイルファイルは、認証を受けていない修正から保護されていますか？		<input type="checkbox"/>	<input type="checkbox"/>	
10.5.3	監査トレイルファイルは、集中ログサーバーまたは改ざんが困難であるメディアに正しくバックアップされていますか？		<input type="checkbox"/>	<input type="checkbox"/>	

質問	回答：	はい	いいえ	特別な*
10.5.4	ワイヤレスネットワークのログは内部 LAN 上のログサーバーにコピーされていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
10.5.5	ファイル完全性監視および変更検知ソフトウェアがログ上で使用されており、(新データの追加ではアラートが発せられるべきではありませんが、)既存ログデータの変更で、アラートが発せられますか？	<input type="checkbox"/>	<input type="checkbox"/>	
10.6	すべてのシステムコンポーネントのログは少なくとも毎日検査されていますか？ <i>ログの点検では、侵入検知システム(IDS)および認証・認可・課金プロトコル(AAA)サーバー(例えば、RADIUS)のようなセキュリティ機能を実行するサーバーが含まれる必要があります。 注記：要件 10.6 の遵守に、ログ収集、構文解析、警報ツールが使用されることがあります。</i>	<input type="checkbox"/>	<input type="checkbox"/>	
10.7	監査トレイル履歴は 3 ヶ月以上オンラインで利用可能とし、少なくとも 1 年間、保存されていますか？	<input type="checkbox"/>	<input type="checkbox"/>	

**要件 11：セキュリティシステムおよび手順を定期的にテストする。**

11.1	(a) セキュリティコントロール、制限、ネットワーク接続、制約は、認証していないアクセスの試みを十分に識別し、防ぐよう、毎年テストされていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) 使用中のワイヤレスデバイスをすべて識別するために、少なくとも年 4 回ワイヤレスアナライザが使用されていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
11.2	内部および外部ネットワークの脆弱性スキャンが少なくとも年 4 回、および(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・トポロジーの変更、ファイアウォール規則の変更、製品アップデートなどの) ネットワークへの重要な変更が行われた後、実行されていますか？ <i>注記：PCI 認定のスキャンベンダーによる外部脆弱性スキャンを、年 4 回実行する必要があります。ネットワーク変更後に行われるスキャンは、ベンダー内部のスタッフにより実行されることがあります。</i>	<input type="checkbox"/>	<input type="checkbox"/>	

\* 「不適用」(表示がある場合のみ選択可能)または「代替管理手段を使用」。代替管理手段を使用する組織は、付属書にある代替管理ワークシートに記入する必要があります。

質問		回答：	はい	いいえ	特別な*
11.3	(a) 少なくとも1年に一度、および(オペレーティングシステムアップグレードされた、環境にサブネットワークやウェブサーバーが追加されたなど)重要な基礎構造やアプリケーションのアップグレードもしくは修正が行われた後、貫入試験が実行されていますか？		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) これらの貫入試験には以下が含まれますか？				
11.3.1	ネットワークレイヤー貫入試験		<input type="checkbox"/>	<input type="checkbox"/>	
11.3.2	アプリケーションレイヤー貫入試験		<input type="checkbox"/>	<input type="checkbox"/>	
11.4	(a) ネットワーク侵入検出システム、ホストベース侵入検出システム、侵入防止システムがすべてのネットワークトラフィックの監視に使用され、疑わしいセキュリティ侵害に対し警告を発していますか？		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) すべての侵入検出および防止エンジンは最新のものとなっていますか？		<input type="checkbox"/>	<input type="checkbox"/>	
11.5	(a) ファイル保全監視ソフトウェアは、重要システムもしくはコンテンツファイルの未承認の改ざんに対し、警告を発すよう展開されていますか？また、		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) 少なくとも週に1度、重要なファイルの比較を実行するようソフトウェアが設定されていますか？ <i>重要なファイルとは、カード会員データを含むものとは限りません。ファイル完全性監視の目的において、重要なファイルとは通常定期的に変更されず、変更された場合、システムのセキュリティ侵害またはセキュリティ侵害の危険性が示される可能性があるものです。ファイル完全性監視製品は通常、関連オペレーティングシステムの重要ファイルに初期設定されています。カスタムアプリケーションのファイルなど、その他の重要ファイルは企業(加盟店またはサービスプロバイダー)により査定、定義される必要があります。</i>		<input type="checkbox"/>	<input type="checkbox"/>	

## 情報セキュリティ方針の管理

要件 12：従業員と契約者に向けた、情報セキュリティ取り扱いの方針を管理する。

質問	回答：	はい	いいえ	特別な*
12.1	セキュリティ方針が作成、発行、管理、普及され、以下が実行されていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
12.1.1	本仕様書内のすべての要件を取り扱う	<input type="checkbox"/>	<input type="checkbox"/>	
12.1.2	脅威や脆弱性を識別するための、年 1 度の正式なリスク評価となるプロセスを含む	<input type="checkbox"/>	<input type="checkbox"/>	
12.1.3	少なくとも 1 年に 1 回は審査され、環境の変化に伴い、更新されること。	<input type="checkbox"/>	<input type="checkbox"/>	
12.2	本仕様書の要件と一致する操作セキュリティ手順(例えば、ユーザアカウント管理手順、ログ点検手順)が作成されていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
12.3	(a) 重要な従業員が向き合う技術（モデムやワイヤレス）に関する使用方針は、すべての従業員および契約者に対して、これらの技術の正しい用を定義するために作成されていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) これらの使用方針は以下を必要としますか？			
12.3.1	管理者承認を明示する	<input type="checkbox"/>	<input type="checkbox"/>	
12.3.2	技術使用の認証	<input type="checkbox"/>	<input type="checkbox"/>	
12.3.3	アクセスを行うデバイスと人物をすべてリストする	<input type="checkbox"/>	<input type="checkbox"/>	
12.3.4	デバイスに所有者、連絡先情報、目的のラベルを貼る	<input type="checkbox"/>	<input type="checkbox"/>	
12.3.5	技術の承認された使用法	<input type="checkbox"/>	<input type="checkbox"/>	
12.3.6	技術に承認されるネットワークの場所	<input type="checkbox"/>	<input type="checkbox"/>	
12.3.7	ベンダー承認の製品リスト	<input type="checkbox"/>	<input type="checkbox"/>	
12.3.8	特定期間不動作であった後、モデムセッションが自動的に切断される	<input type="checkbox"/>	<input type="checkbox"/>	
12.3.9	加盟店が必要とする場合のみ、モデムを有効とし、使用後はただちに無効とする	<input type="checkbox"/>	<input type="checkbox"/>	
12.3.10	カード会員データにモデムを通じて遠隔アクセスする場合、その方針は以下を規定していますか？			
	(a) ローカルハードドライブ、フロッピーディスク、その他外部メディア上のカード会員データの保管禁止	<input type="checkbox"/>	<input type="checkbox"/>	

\* 「不適用」（表示がある場合のみ選択可能）または「代替管理手段を使用」。代替管理手段を使用する組織は、付属書にある代替管理ワークシートに記入する必要があります。

質問	回答：	はい	いいえ	特別な*
		<input type="checkbox"/>	<input type="checkbox"/>	
(b) 遠隔アクセス中のカットアンドペーストおよび印刷機能の禁止		<input type="checkbox"/>	<input type="checkbox"/>	
12.4 セキュリティ方針および手順は、すべての従業員および契約者に対し明確に情報セキュリティの責任お定義していますか？		<input type="checkbox"/>	<input type="checkbox"/>	
12.5 以下の情報セキュリティ管理責任は、個人または団体に課せられるものですか？				
12.5.1 セキュリティ方針と手順の構築、文書化、配布		<input type="checkbox"/>	<input type="checkbox"/>	
12.5.2 セキュリティアラートと情報を監視、分析し、適切な人に配布する		<input type="checkbox"/>	<input type="checkbox"/>	
12.5.3 セキュリティに関する事故への対応および上申の手順は、すべての状況をタイムリーかつ効率的に取り扱うように作成、記録、分配されていますか？		<input type="checkbox"/>	<input type="checkbox"/>	
12.5.4 ユーザアカウントの追加、削除、変更を含む管理		<input type="checkbox"/>	<input type="checkbox"/>	
12.5.5 データへのアクセスすべてを監視、管理する		<input type="checkbox"/>	<input type="checkbox"/>	
12.6 実施されている正式なセキュリティ意識向上プログラムは、すべての従業員にカード会員データのセキュリティの重要性を意識させるものとなっていますか？		<input type="checkbox"/>	<input type="checkbox"/>	
12.6.1 従業員は雇用時、および少なくとも年に1度(例えば、手紙、ポスター、メモ、会議、宣伝など)、教育を受けていますか？		<input type="checkbox"/>	<input type="checkbox"/>	
12.6.2 従業員はベンダーのセキュリティ方針と手順を読み、理解したことを書面で認めることを求められていますか？		<input type="checkbox"/>	<input type="checkbox"/>	
12.7 潜在的従業員は、内部ソースからの攻撃の危険性を最小限に抑えるために審査されていますか？ <i>取引を促進する際、同時にひとつのカード番号のみにアクセスを行う店舗のレジ係などの従業員に対する本要件は推奨のみです。</i>		<input type="checkbox"/>	<input type="checkbox"/>	
12.8 カード会員データがサービスプロバイダーと共有される場合、契約上、以下のものは必要となりますか？		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.1 サービスプロバイダーは PCI DSS 要件を厳守する必要がありますか？		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.2 契約には、サービスプロバイダーはプロバイダーが所有するカード会員データのセキュリティに責任を負うという認識が含まれていますか？		<input type="checkbox"/>	<input type="checkbox"/>	

質問	回答：	はい	いいえ	特別な*
12.9	事故対応計画が実行され、以下を含んでいますか？			
12.9.1	(a) システムのセキュリティ侵害の場合に実行される事故対応計画は作成されていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) 計画には少なくとも、特定の事故への対応手順、業績回復および継続性の手順、データバックアッププロセス、役割と責任、(例えば、アクワイヤラおよびクレジットカード協会へ知らせるなど)通信および連絡戦略が含まれていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
12.9.2	計画は少なくとも年に1度テストされていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
12.9.3	24時間無休で警告に対応するための特定の人材が指名されていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
12.9.4	適切な研修により、従業員にセキュリティ違反対応責任が与えられていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
12.9.5	侵入検知、侵入防止、ファイル完全性監視システムからの警告が含まれていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
12.9.6	学んだレッスンや産業発展に従って事故対応計画を変更、発展させるためのプロセスが開発され、実行されていますか？	<input type="checkbox"/>	<input type="checkbox"/>	
12.10	(a) すべてのプロセッサおよびサービスプロバイダーは、接続企業を管理する方針および手順を管理、実行していますか？	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) この管理には、以下が含まれていますか？			
12.10.1	接続企業のリスト	<input type="checkbox"/>	<input type="checkbox"/>	
12.10.2	企業を接続する前に適切な配慮が実行されていることを確かにする	<input type="checkbox"/>	<input type="checkbox"/>	
12.10.3	企業が PCI DSS を遵守していることを確かにする	<input type="checkbox"/>	<input type="checkbox"/>	
12.10.4	構築されたプロセスに従い、企業は接続、および切断されていますか？	<input type="checkbox"/>	<input type="checkbox"/>	

\* 「不適用」(表示がある場合のみ選択可能)または「代替管理手段を使用」。代替管理手段を使用する組織は、付属書にある代替管理ワークシートに記入する必要があります。

## PCI DSS ホスティングプロバイダ適用性 (PCI DSS Applicability for Hosting Providers)

要件 A.1 : 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します。

質問		回答：	はい	いいえ	特別な*
A.1	A.1.1 から A.1.4 にあるとおりに、各企業(つまり、加盟店、サービスプロバイダー、その他企業)のホスト環境およびデータは保護されていますか？				
A.1.1	各企業は、独自のカード会員データ環境のみにアクセスを行っていますか？		<input type="checkbox"/>	<input type="checkbox"/>	
A.1.2	各企業のアクセスおよび権限はその独自のカード会員データ環境に制限されていますか？		<input type="checkbox"/>	<input type="checkbox"/>	
A.1.3	ロギングおよび監査トレイルが有効とされ、各企業のカード会員データ環境に独自のものであり、DSS の要件 10 と一致するものとなっていますか？		<input type="checkbox"/>	<input type="checkbox"/>	
A.1.4	ホストされている加盟店もしくはサービスプロバイダーへのセキュリティ侵害の際には、すべてのプロセスは、タイムリーな科学的検査を行うことができますか？		<input type="checkbox"/>	<input type="checkbox"/>	

\* 「不適用」 (表示がある場合のみ選択可能) または「代替管理手段を使用」。代替管理手段を使用する組織は、付属書にある代替管理ワークシートに記入する必要があります。

## 代替管理手段付属書

---

PCI DSS 要件の技術仕様を満たすことができないが、関連リスクを十分に軽減した場合、多くの要件には、代替管理手段を考慮することがあります。代替管理手段の完全な定義は、*PCI DSS 用語集*をご覧ください。

代替管理手段の有効性は、管理が実施される環境の特質、周囲のセキュリティ管理、管理の設定に頼るものです。ベンダーは、特定の代替管理手段は、すべての環境で有効となるわけではないことに注意する必要があります。各代替管理手段は有効性を確かめるために、実行後十分に査定される必要があります。

以下のガイダンスは、要件 3.4 につき、ベンダーがカード会員データを読み取り不可能とすることができない場合の代替管理手段を示します。

### 要件 3.4 の代替管理手段

技術上の制約または、業務上の限界により、(例えば、暗号化により)カード会員データを読み取り不可能とできないベンダーは代替管理手段を考慮することができます。危険分析を引き受け、適正な技術的または文書化された業務上の制約を持つベンダーのみが遵守を行うために代替管理手段の仕様を考慮することができます。

カード会員データを読み取り不可能とする代替管理手段を考慮するベンダーは、読み取り可能なカード会員データを維持することによる、データへの危険性を理解する必要があります。一般的に、管理では読み取り可能なカード会員データを維持することによる、データへの追加の危険性を軽減するための追加の保護対策となる必要があります。考慮する管理は、PCI DSS 内で求められる管理に追加するものであり、*PCI DSS 用語集*の「代替管理手段」定義を満たすものである必要があります。代替管理手段は、以下のすべての条件を満たすデバイスもしくはデバイス、アプリケーション、コントロールの組み合わせである可能性があります。

1. (例えば、ネットワークレイヤーに)追加の区分け/アブストラクションを提供してください。
2. カード会員データ、または以下の基準に基づくデータベースへのアクセスを制限する能力を提供してください。
  - IP アドレス/Mac アドレス
  - アプリケーション/サービス
  - ユーザアカウント/グループ
  - データ種類 (パケットフィルタリング)
3. データベースへの論理的アクセスを制限してください。
  - アクティブディレクトリ、またはライトウェイト・ディレクトリ・アクセス・プロトコル (LDAP)とは独立したデータベースへの論理的アクセスをコントロールしてください。
4. 共通アプリケーションまたはデータベース攻撃(例えば SQL インジェクション)を防止/検知してください。

## 代替管理手段ワークシート

「いいえ」がチェックされ、代替管理手段が「特別な」カラム内で言及される場合、本ワークシートを使用して、代替管理手段を定義します。

危険分析を引き受け、適正な技術的または文書化された業務上の制約を持つベンダーのみが遵守を行うために代替管理手段の仕様を考慮することができます。

### 要件番号と定義：

	必要な情報	説明
1. 制約	元の要件の遵守を除外し、制約をリストしてください。	
2. 目的	元の管理の目的を定義し、代替管理手段で満たすべき目的を識別してください。	
3. 特定リスク	元の管理を行わないことにより、追加されるリスクを識別してください。	
4. 代替管理の定義	代替管理手段を定義し、それがどのように元の管理の目的に、およびリスクが増す場合これに対処するか説明してください。	

## 代替管理ワークシート一記入例

本ワークシートを使用して、[いいえ] がチェックされ、代替管理手段が「特別」カラム内で言及される要件に対する代替管理手段を定義します。

システムコンポーネントもしくはカード会員データへのアクセスを許可する前に、すべてのユーザが独自のユーザ名で識別されるようになっていませんか？

	必要な情報	表示の意味
1. 制約	元の要件の遵守を不可能とする制約をリストしてください。	XYZ ベンダーはLDAP を伴わず、スタンドアロン型 Unix サーバーを採用しています。それ自体は、「ルート」ログインを必要とします。XYZ ベンダーが「ルート」ログインを管理することも、各ユーザによるすべての「ルート」アクティビティをログすることも不可能です。
2. 目的	元の管理の目的を定義し、代替管理手段で満たす目的を識別してください。	独自のログインを必要とする目的は、2 要素あります。1 つ目は、ログイン機密情報を共有することは、セキュリティ上承認できないと考慮するということです。2 件目は、共有ログインは、特定のアクションに対しある人が責任を負うということを定義的に明示することが不可能となることです。
3. 特定リスク	オリジナルコントロールがないことにより追加されるリスクを識別してください。	追加リスクは、すべてのユーザが独自の ID を持つことを確実にすることによってではなく、およびトラックできることによってではなく、アクセスコントロールシステムにもたらされています。
4. 代替管理手段の定義	代替管理手段を定義し、それがどのようにオリジナルコントロールの目的およびもしある場合、増加したリスクに対処するか説明してください。	XYZ ベンダーはすべてのユーザが SU コマンドを使用して、デスクトップからサーバーにログインすることを求めます。SU はユーザが「ルート」アカウントにアクセスし、「ルート」アカウントの下、アクションを実行することを許可しますが、SU ログディレクトリにログされることができます。これにより、各ユーザのアクションが SU アカウントを通じてトラックで

		きます。
--	--	------