No.	PCI DSS 要件		テスト手順		文書化要件	共有ホスティングプロバイダに対する追加要件	サービスプロバイダに対する追加要件	提供文書名 （テンプレートとして提供）	基準・ポリシー	手順書	図	リスト	記録	参考文書	参考URL
1	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。													
2	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	ファイアウォール/ルーター構成基準および以下で指定されたその他の文書を検査し、標準が完全であり、以下のように実施されていることを確認する：	○								○		
3	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。	1.1.1.a	文書化された手順を調べて、すべてをテストし承認するための正式なプロセスがあることを確認する。 • ネットワーク接続および • ファイアウォール/ルーター構成の変更	○			PCIDSS運用ポリシー 2 ファイアウォール/ルーター管理ポリシー		○					
4			1.1.1.b	ネットワーク接続のサンプルでは、責任者をインタビューし、記録を検査してネットワーク接続が承認されてテストされていることを確認する。	○					○			○		
5			1.1.1.c	ファイアウォールおよびルーター構成に実際に加えられた変更のサンプルを特定し、変更記録と比較して、責任者をインタビューして変更が承認されテストされたことを確認する。	○					○			○		
6	1.1.2	ワイヤレスネットワークなど、カード会員データ環境とその他のネットワーク間のすべての接続ををを示す最新ネットワーク図。	1.1.2.a	ネットワーク図を検査してネットワーク構成を観察し、現在のネットワーク図が存在すること、また、その文書がワイヤレスネットワークを含む、カード会員データへの全接続を含んでいることを確認する。	○						○				
7			1.1.2.b	責任者をインタビューして、図が最新のものであることを確認する。	○						○				
8	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。	1.1.3.a	データフロー図を調べ、担当者をインタビューして図を確認する。 • システムとネットワーク内でのすべてのカード会員データのフローを示す • 最新状態に保たれており、環境に変化があれば必要に応じて更新されている	○						○				
9	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。	1.1.4.a	ファイアウォール構成基準を調べて、各インターネット接続、およびDMZ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が含まれていることを確認する。	○			PCIDSS運用ポリシー ファイアウォール/ルーター管理ポリシー							
10			1.1.4.b	現在のネットワーク図が、ファイアウォール構成基準と一致していることを確認する。	○						○				
11			1.1.4.c	文書化されている構成基準とネットワーク図に基づき、ネットワーク構成を見て、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との間にファイアウォールがあることを確認する。	○						○				
12	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。	1.1.5.a	ファイアウォールおよびルーター構成基準に、ネットワークコンポーネントの管理のためのグループ、役割、責任に関する記述が含まれていることを確認する。	○										
13			1.1.5.b	ネットワークコンポーネントの管理責任者をインタビューし、文書通りに役割と責任が割り当てられていることを確認する。	○								○		
14	1.1.6	安全でないと見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を含む、使用が許可されているすべてのサービス、プロトコル、ポートの使用に対する業務上の正当な理由および承認の文書化。	1.1.6.a	ファイアウォール/ルーター構成基準に、業務上の正当な理由と承認を含む、すべてのサービス、プロトコル、ポートを文書化したリストが含まれていることを確認する。	○			PCIDSS運用ポリシー 2 ファイアウォール/ルーター管理ポリシー		○		○	○		
15			1.1.6.b	使用が許可されているが安全でないサービス、プロトコル、ポートを特定する。かつ、各サービスについてセキュリティ機能が文書化されていることを検証する。	○										
16			1.1.6.c	ファイアウォールとルーターの構成を検査し、文書化されているセキュリティ機能が安全でない各サービス、プロトコル、ポートに実装されていることを確認する。	○										
17	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。	1.1.7.a	ファイアウォール/ルーター構成基準で、ファイアウォールおよびルーターのルールセットを少なくとも 6 カ月ごとにレビューするように要求していることを確認する。	○			PCIDSS運用ポリシー 2 ファイアウォール/ルーター管理ポリシー							
18			1.1.7.b	ルールセットのレビューに関連した文書を検査し、担当者をインタビューすることで、ルールセットが少なくとも 6 カ月ごとにレビューされていることを確認する。	○								○		
19	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	ファイアウォール/ルーター構成を調べて、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システムコンポーネント間で接続が制限されていることを確認する。				PCIDSS運用ポリシー 2 ファイアウォール/ルーター管理ポリシー							
20	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。	1.2.1.a	ファイアウォール/ルーター構成基準を調べて、カード会員データ環境に必要な着信および発信トラフィックが特定されていることを確認する。	○			PCIDSS運用ポリシー 2 ファイアウォール/ルーター管理ポリシー							
21			1.2.1.b	ルーター構成を調べて、同期化されていることを確認する。例えば、実行（アクティブ）構成ファイルが起動構成（マシンの再起動時に使用）に一致することを確認する。											
22			1.2.1.c	ファイアウォール/ルーター構成を検査して、例えば明示の「すべてを拒否」、または許可文の後の暗黙の拒否を使用することで、他のすべての着信および発信トラフィックが明確に拒否されていることを確認する。											
23	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。	1.2.2.a	ルーター構成ファイルを調べて、不正アクセスからセキュリティ保護されていることを確認する。											
24			1.2.2.b	ルーター構成を調べて、同期化されていることを確認する。たとえば、実行（アクティブ）構成ファイルが起動構成（マシンの再起動時に使用）に一致することを確認する。											
25	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業務上必要な場合に拒否または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。	1.2.3.a	ファイアウォール/ルーター構成を調べて、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間に境界ファイアウォールがインストールされていることを確認する。				PCIDSS運用ポリシー 2 ファイアウォール/ルーター管理ポリシー							