

PCI DSS 運用規程

2018年 mm月 dd日 (X.X版)

目次

1	はじめに
1.1	目的
1.2	適用範囲
1.3	準拠規格
2	PCI DSS セキュリティ要件
2.1	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 1) 7
2.1.1	ファイアウォールおよびルーターの構成基準の確立(要件 1.1)
2.1.2	信頼できないネットワークとの接続制限(要件 1.2)
2.1.3	インターネットとカード会員データ環境の直接的なパブリックアクセスの禁止(要件 1.3) ...
2.1.4	パーソナルファイアウォールの導入(要件 1.4)
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等の周知(要件 1.5)
2.2	システムパスワード及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こ と(要件 2)
2.2.1	デフォルト値の変更(要件 2.1)
2.2.2	セキュリティ構成基準の作成(要件 2.2)
2.2.3	すべてのコンソール以外の管理アクセスの暗号化(要件 2.3)
2.2.4	システムコンポーネントのインベントリの維持(要件 2.4)
2.2.5	セキュリティパラメータ管理のセキュリティポリシーと管理手順の周知(要件 2.5)
2.2.6	共有ホスティングプロバイダとしてのカード会員データの保護(要件 2.6)
2.3	保存されるカード会員データを保護する(要件 3)
2.3.1	データ保存および廃棄のポリシー・手順の確立(要件 3.1)
2.3.2	センシティブ認証データの保存禁止(要件 3.2)
2.3.3	表示する際の PAN のマスク(要件 3.3)
2.3.4	PAN の読み取り不能化(要件 3.4)
2.3.5	暗号化キーの保護手順の作成(要件 3.5)
2.3.6	暗号化キーの管理手順の作成(要件 3.6)
2.3.7	カード会員データ保存時のセキュリティポリシー及び管理手順の周知(要件 3.7)
2.4	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(要件 4) ...
2.4.1	カード会員データの伝送時の暗号化(要件 4.1)
2.4.2	エンドユーザメッセージングツールの利用制限(要件 4.2)
2.4.3	カード会員データ伝送時の暗号化ポリシー及び管理手順の周知(要件 4.3)
2.5	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(要件 5)
2.5.1	アンチウイルスソフトウェアの導入(要件 5.1)

1 はじめに

1.1 目的

本規程は、「個人情報保護方針」に基づき、PCI DSS の各要件に適合するための、実装方式と運用方針について記述する。本規程では、XX システム(以降本システムと表記する)におけるセキュリティ方式およびセキュリティ実装方式の前提事項について記述する。

1.2 適用範囲

カード会員データ（PAN）が保存、処理、送信されるすべてのシステムコンポーネントを対象とする。今回の対象範囲を別紙 1. 「PCIDSS 適用範囲」に示す。

注) 別紙 1.「PCIDSS 適用範囲」は別途作成する必要があります。

1.3 準拠規格

本システムが準拠する PCI DSS の版は「PCI DSS v3.2」とする。

2 PCI DSS セキュリティ要件

2.1 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 1)

カード会員データを保護するために、カード会員データ環境の境界にファイアウォールを設置し、構成を維持する。

2.1.1 ファイアウォールおよびルーターの構成基準の確立(要件 1.1)

ファイアウォールおよびルーターは、構成基準を定め、基準に従って管理する。構成基準に含む内容を、以下に示す。

- (1) すべてのネットワーク接続、ファイアウォール/ルーター構成の変更を承認し、テストする手順(要件 1.1.1)
- (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示す最新ネットワーク図(要件 1.1.2)
- (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(要件 1.1.3)
- (4) DMZ と内部ネットワークの間にファイアウォールを導入(要件 1.1.4)
- (5) 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(要件 1.1.4)
- (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、及び特に安全でないもの (FTP,Telnet,POP3,IMAP,SNMP v1,v2 など) が使われる業務上の理由等(要件 1.1.6)
- (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する(要件 1.1.7)

【関連文書】

PCI DSS 運用ポリシー

2.1.2 信頼できないネットワークとの接続制限(要件 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し、ファイアウォール構成を構築する。

- (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の拒否する。(要件 1.2.1)
- (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。(要件 1.2.2)
- (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する。(要件 1.2.3)

【関連文書】

TBD

変更履歴

版番号	制定/改訂日	改訂内容	作成者	承認者
1.0	2018/mm/dd			