PCI DSS準拠支援サービスのご紹介

クレジットカード取扱企業としての義務

カード会員情報の漏えい事故は後を絶ちません。一度漏えい事故が発生すると、金銭的補償による直接的な影響だけでなく、社会的な信用失墜による有形無形の影響があります。 このような社会的背景を受け、カード会員情報を保護するために必要な措置を講じることが法的に義務付けられ、違反事業者に対する行政処分が法制化されています(改正割賦販売法の可決など)。

また、国際的なクレジット産業向けのデータセキュリティ基準が、VISA, MasterCard, AMEX, JCB, Discoverの5大ブランドにより、2006年9月に設立されたPCIセキュリティ基準審議会(米国)によって、制定されました。
この基準がPCI DSS(Payment Card Industry Data Security Standard)で、カード会員データの伝送/処理/格納を行うシステム、ネットワーク及びアプリケーションを対象としており、VISAは、カード発行会社(イシュア)、加盟店、加盟店契約会社(アクワイアラ:加盟店開拓および加盟店管理を行う事業者)、カード関連データ取扱事業者(サービスプロバイダ)、の全てに、そのレベルに応じた準拠条件及び、対応期限を規定しています。

つまり、上記のカード取扱企業にとって、PCI DSS準拠は、避けて通れない必須事業プロセスです。当サービスは、その準拠対応を、効率的に実現するためのPCI DSS準拠支援サービスです。

- **PCI DSS準拠状況を診断します**
  - PCI DSSに対応するシステム範囲を決定する
  - PCI DSS要件に対する実装評価を行う
- **PCI DSS準拠に向けての対策方針を立案し、ロードマップを策定します**
  - PCI DSS要件に対して未実装あるいは実装不足なセキュリティリスクの強化方針を策定する
- **各領域別の個別施策の計画策定と実行を支援します**
  - 要件対応すべき各システム領域における個別計画の策定
  - 個々のセキュリティリスク要件に対する対応策実施
- **信頼できる「認定セキュリティ評価機関(QSA)」との連携により確実な認定を支援します**
  - 日本におけるPCI DSS審査機関6社のうち、もっとも実績のある国際マネジメント認証機構(ICMS)と連携し、評価認定をスムーズに受けられるよう支援します。

お客様のニーズ

- クレジットカードを発行(イシュア)しているが、PCI DSS準拠範囲が広範であり、客観的な準拠診断が困難
- 通販事業を運営しているカード加盟店だが、カード不正利用等の事故が多く困っている
- 親会社のカード事業のトランザクションを扱っているシステム会社(サービスプロバイダ)だが問診票を使った自己診断だけでは、準拠対応のための施策立案ができず困っている

お問い合せ先:
株式会社デナリコンサルティング
TEL:03-6890-1121 / E-mail: info@denaliconsulting.jp

サービス概要

アウトプットイメージ

PCI DSS要件チェックシート

要件① データを保護するためにファイアウォールの導入をし、最適な設定を維持すること

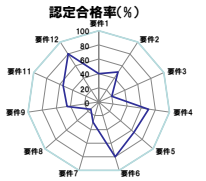
PCI DSS要件	テスト手順	確認区分	対応	未対応	対応目標期日/コメント
1.1 以下を含むファイアウォール及びルーター構成基準を確立する	1.1 ファイアウォール/ルーター構成基準及び以下で指定されたその他文書を入手及び検査し、標準が完全であることを確認する。	E, I, S		09/08/10	09/9/末までに対応
1.1.1 全てのネットワーク接続及びファイアウォール/ルーター構成への変更を承認及びテストする正式なプロセス	1.1.1 全ての接続及びファイヤウォール/ルーター構成への変更を承認及びテストする、正式なプロセスがある事を確認する。	E, S	09/8/10		変更プロセス仕様書確認
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全ての接続を示す最新ネットワーク図	1.1.2a 最新のネットワーク図(ネットワーク上のカード会員データフローを示す図など)が存在し、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ての接続が記載されていることを確認する。	S	09/8/10		ネットワーク図Ver2.1確認
	1.1.2b 図が最新のものであることを確認する。	E	09/8/10		上記
1.1.3 各インターネット接続及び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	1.1.3 ファイアウォール構成基準に、各インターネット接続及び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事を確認する。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。	I, S		09/8/10	09/9/末までに対応
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	1.14 ファイアウォール/ルーター構成基準に、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、責任に関する記述が含まれていることを確認する。	I, S		09/8/10	09/9/末までに対応
1.1.5 使用が許可されている全てのサービス、プロトコル、ポートの文書化、及び、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言など)	1.1.5a ファイアウォール/ルーター構成基準に、業務に必要なサービス、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(HTTP、SSL、SSH、VPNなど)	I, S	09/8/10		構成基準確認

インタビュー結果報告書

<ヘッダー>
- 件名: PCI DSS実装評価結果
- 評価実施期間: 2009/09/01～2009/09/10
- 評価担当者: ○○○○　評価者 : △△△△　評価責任者:□□□□

<実績>
- PCI DSS実装評価全体件数: 200件
- PCI DSS実装評価実施件数: 200件
- 評価内容対応件数 : 100件
- 評価内容未対応件数: 100件
- PCI DSS認定合格率: 50%

認定合格率(%)



リスク一覧表

<要件別>

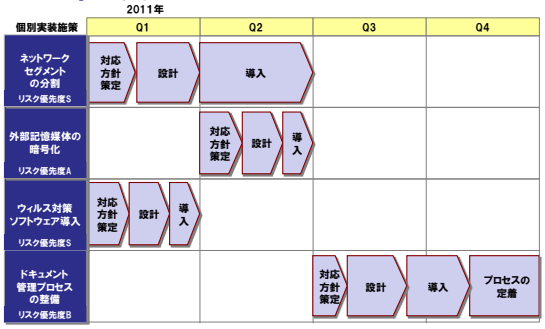
要件1	カード会員データを保護するために、ファイアウォールをインストールして構成を維持すること	評価件数	23
件数詳細	対応 23 / 未対応 5		

未対応詳細

優先度	件数	コメント
S	1	項番:1-2
A	2	パラメータ設定変更ミスによる
B	2	
C	0	

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こと	評価件数	13
件数詳細	対応 8 / 未対応 5		

ロードマップ



支援作業プロセス

	フェーズ1 準拠状況診断	フェーズ2 対策方針＆ロードマップ策定	フェーズ3 個別施策の計画策定と実行
目的	・PCI DSSに対応するシステム範囲を決定する ・PCI DSS要件に対する実装評価を行う	・PCI DSS要件に対して未実装あるいは実装不足なセキュリティリスクの強化方針を策定する	・計画の策定 ・個々のセキュリティリスク要件に対する対応策実施
作業内容	・インタビュー(1～2名) ・実装状況評価 ・結果報告	・現状分析 ・リスク評価 ・各リスク要素に対する到達基準策定 ・ロードマップ策定	・個別施策の詳細計画策定および実行 ・個別施策の効果測定 ・改善策検討