

管理者が 知っておきたい

現場に役立つ新しい
セキュリティスタンダード



文●ネットワンシステムズ株式会社
営業推進グループ
セキュリティ事業推進本部
コンサルティング部
部長 豊田祥一

2005年にネットワンシステムズ入社。前職において、PKIを導入したインターネットサービスの運用業務設計と運用管理に携わるとともに、個人情報保護法対応、電子認証局構築、等のコンサルティング業務を担当。現職においては、ネットワークベンダーの視点に基づくコンサルティングビジネスを推進。各種PCI DSSに関するセミナー講師も担当。前宮内庁CIO補佐官。

編集●大谷イビサ

PCI DSSは なぜ注目される?

最近、セキュリティ業界ではPCI DSSというキーワードをよく耳にする。PCI DSSとは、クレジットカードやキャッシュカードなども含めた支払いカード業界(Payment Card Industry)におけるデータセキュリティ基準(Data Security Standard)のことであり、この頭文字を取ってPCI DSSと呼ばれている。

カード情報の漏えい事件が多発している今日では、PCI DSSを遵守させることに対する国際カードブランドの動きが活発化することは疑う余地がない。また、米国におけるPCI DSSを取り入れた州法の制定、あるいは日本における改正割賦販売法の動向等、今後PCI DSSは活発に議論されている。今後はクレジットカード情報の保護に止まらず、広く重要情報を保護するためのベンチマークとしての役割を担うことになると思われる。

このような状況下、ITネットワークセキュリティの実装基準として、PCI DSSの有用性は確実に定着していくものと筆者は考えている。すなわち、ネットワーク管理者においては、単にネットワーク構成のみに注視した運用管理を行なう時代は過ぎ去り、潜在するさまざまな脅威から重要情報を保護するためにネットワーク構成はいかにあるべきか、ということに視点を置いた業務活動が必要となる。また、Webシステムの管理者においては、ネットワーク管理にも

注視する必要が出てきている。Webシステムの脆弱性とネットワーク構成とは密接な関わりを持ったものであり、一方のみに重点を置くというわけにはいかないのである。

クレジットカード業界のプレイヤー

PCI DSSを理解するためには、まずクレジットカード業界の構造を理解する必要がある。基本的な構図としては、PCI DSSの遵守を要求する側と要求される側とに分けられる(図1)。

PCI DSSの遵守を要求する側として、まず「国際カードブランド」が挙げられる。これはAmerican Express、Diners Club、JCB、Master Card、VISAの5ブランドが有名だ。こうした国際カードブランドとしては、ブランドイメージの維持・向上と情報漏えいに伴う損害回避や事故防止の

仕組み作りに迫られている。そのため、こうした国際カードブランドの各社は、PCI DSSを始めとするセキュリティ基準を策定し、これを遵守させるための組織として、PCISSC (PCI Security Standard Council)や審査機関(QSA)、認定スキャンニングベンダー(ASV)を構築している。

PCI SSCのおもな任務は、PCI DSSの普及と啓蒙、改訂管理、QSAおよびASVの認定の大きく3つである。そして、QSAはPCI DSSに基づくオンサイト評価を行ない、ASVは文字通りスキャンニングテストを行なう。

一方で、PCI DSSの遵守を要求される側としては、カード会社、加盟店およびプロセッサ(カードの代金請求を日常的に行なう業者)が挙げられる。

カード会社は、国際カードブランドより、傘下の加盟店やプロセッサがPCI DSSに準拠していることを求められる。

加盟店およびプロセッサは、クレジット決済の取引処理件数に応じてQSAが実施する年次訪問審査、およびASVが実施する脆弱性スキャンテストを受けて、これに合格する必要がある。

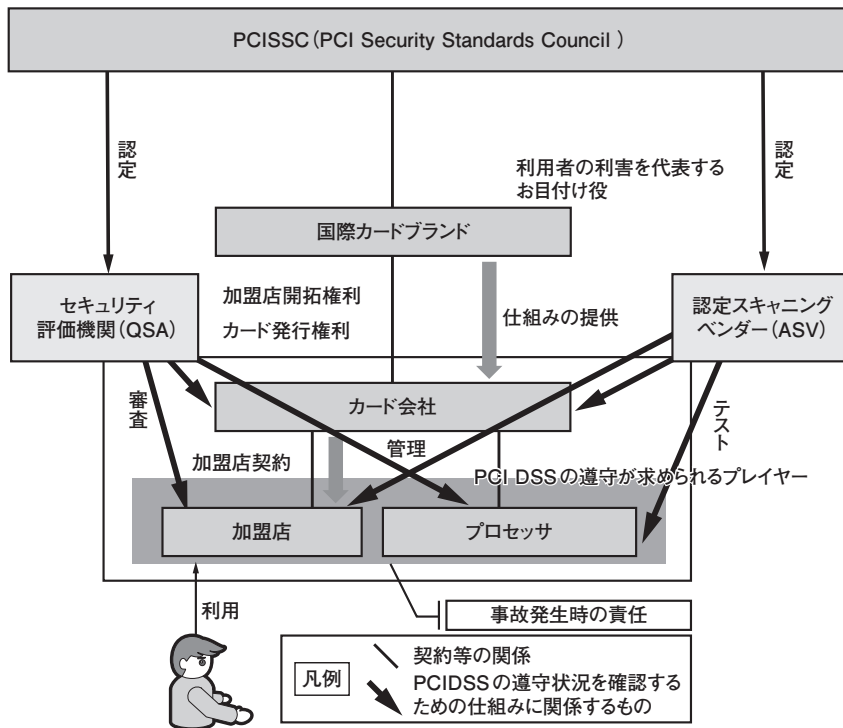
なお、取引処理件数が少ない場合には、年次訪問審査の代わりに年次自己診断を実施する。また、自己診断に用いる問診票は、PCI SSCより提供されている。

PCI DSSの目的と要件

さて、PCI DSSはカード会員データのセキュリティを強化し、向上するため、そして全世界を対象とした広い範囲に対して、整合性のあるデータセキュリティの測定手法を適用。促進することを目的として2004年に開発されたものである。このことは、PCI DSSを理解する上で重要である。

たとえば、海外旅行でクレジットカードを利用することを考えれば、カード会員データが全世界を流通する情報であることは自明である。そのため、全世界の利用者が安全にクレジットカードで買い物をするためには、世界中のさまざまな関連組織が最低限遵守しなければならない手法が必要であり、各国の安全性の水準について利用者が納得できるようにする必要がある。PCI DSSの要件が具体的に規定されている理由はこの点にある。

PCI DSSは、カード会員データとセンシティブ認証データの保護を目的として作成されたものであり、PCI DSSは保護対象となる情報を明確に定義している(図2)。これにより、PCI DSSの要件を具体的に規定することが可能となっている。PCI DSSは、6つの目的



(「PCIデータセキュリティ基準完全対策」より引用)

図1 PCI DSSを巡る各プレイヤーの関係



とこれらに対応する12の要件から構成されている(図3)。

PCI DSSの12の要件は、すべての「システム構成要素」に適用される。システム構成要素とは、カード会員データ環境に含まれるネットワーク、サーバ、あるいはアプリケーションである。

このうち「カード会員データ環境」とは、カード会員データやセンシティブ認証データを保有するネットワークの該当部分にあたる。

ネットワーク管理の観点から見ると、PCI DSSは他の認証基準に比べて非常にわかりやすい。PCI DSSが目的とすることは、データセントリックとエンドツーエンドの2点に集約できる。すなわち、図2において示したデータに重点を置き、これらのデータが保管および処理されるポイント、そしてこれらのデータが伝送される経路のセキュリティをいかに保護すべきかが、規定されているということだ。これはWebのセキュリティ確保の考え方を包含しており、到達点とポイントが明確だ。

目的① 安全なネットワークの構築・維持 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導入し、適切な設定を維持すること 要件2: システムパスワードと他のセキュリティパラメータにベンダー提供のデフォルトを使用しないこと
目的② カード会員データの保護 要件3: 保存されたカード会員データを安全に保護すること 要件4: 公衆ネットワーク上でカード会員データを送信する場合、暗号化すること
目的③ 脆弱性を管理するプログラムの整備 要件5: アンチウイルスソフトウェアまたはプログラムを利用し、定期的に更新すること 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、保守すること
目的④ 強固なアクセス制御の導入 要件7: カード会員データへのアクセスを業務上の必要範囲内に制限すること 要件8: コンピュータにアクセスする利用者毎に個別のIDを割り当てること 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こと
目的⑤ 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に対するすべてのアクセスを追跡し、監視すること 要件11: セキュリティシステムおよび管理手順を定期的にテストすること
目的⑥ 情報セキュリティポリシーの整備 要件12: 従業員と契約社員のための情報セキュリティポリシー整備すること

図3 PCI DSSの6つの目的・12の要件

2008年における PCI DSSの改訂ポイント

PCI DSSは、2006年にバージョン1.1がリリースされ、2008年10月のバージョンアップを経て、2009年1月からはバージョン1.2が正式版となる。

PCI DSSのバージョンアップは、PCI SSC主導のもと、国際カードブランド、QSA、ASV、加盟店、サービスプロバイダおよびコンサルティング提供

会社を含めた活発な議論に基づき実施されている。というのも、PCI DSSへの対応は、国際カードブランドと締結される契約内容ときわめて密接に結び付いているためだ。

PCI DSSに準拠しないことはブランド使用契約の破棄か情報漏えい事故発生時の損害賠償請求を招く恐れがあり、各利害関係者はPCI DSSの改訂動向に神経を尖らせている。このような背景があるため、基準遵守に関する現実的な改善策が議論され、改訂方針に反映されている(リスト1)。

- ・ PCI DSSの要求事項の明確化
- ・ より柔軟な対応方法の提供
- ・ 変化(進化)するリスクと脅威への対応
- ・ ベストプラクティスの取り込み
- ・ 適用範囲とレポーティングの明確化
- ・ 冗長な要求事項の排除
- ・ 書類の整理

リスト1 2008年におけるPCI DSSの改訂方針

たとえば、「より柔軟な対応方法の提供」として、パッチ適用あるいは物理的アクセス管理などの要件が緩和されている一方で、「変化(進化)するリスクと脅威への対応」についてウイルス対策あるいは無線ネットワーク等の要件が強化されている。

	データ要素	保管可能	保護必須	PCI DSS 要件 3.4の適用
カード会員データ	カード番号(PAN)	YES	YES	YES
	カード会員名	YES	YES	NO
	サービスコード	YES	YES	NO
	有効期限	YES	YES	NO
センシティブ認証データ	全磁気ストライプデータ	NO	N/A	N/A
	3CAV2 / CVC2 / CVV2 / CID	NO	N/A	N/A
	暗証番号(PIN) / PINブロック	NO	N/A	N/A

PCI DSS 要件3.4: 少なくともカード番号は、どこに保管されていても(携帯デジタル媒体やバックアップ媒体上のデータ、ログ内データを含む)、次のいずれかの手段を使用して判読不可能な状態にしておく。

- ・ 強力な暗号化に基づくワンウェイハッシュ機能(ハッシュインデックス)
- ・ トランケーション(切捨て)
- ・ インデックストークンやPAD (PADは安全に保管)
- ・ 関連する鍵管理プロセスと手順を伴う、強力な暗号化

少なくともカード番号は判読不可能な状態にしなければならない。

図2 保護対象となるデータの構成要素とその要件