VOL. 2

# PCI DSS 徹底解説 第２回
# PCI DSS の概要 -PCI DSS の 12 要件を読み解く -


## 川島 祐樹

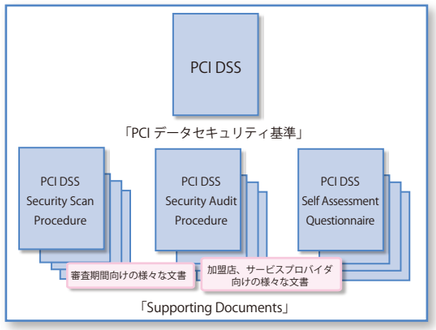
NTT データ・セキュリティ株式会社


**PCI DSS の構成とその内容について具体例を交え解説します。**

### PCI DSS の構成

PCI DSS は、”Payment Card Industry Data Security Standard”の頭文字語となっており、単一のセキュリティ基準だけではなく、用語集や手順書、ASV や QSA などの認定審査機関の認定の仕組みなど、様々な文書や制度を含めて、基準を取り巻く体系全体を指しています。
全ての文書は、PCI SSC のサイトからダウンロードすることができます。

- ●PCI SSC のサイト ( 英文 )
  https://www.pcisecuritystandards.org/
- ●PCI DSS のダウンロード (「License Agreement」に同意後ダウンロード可 )
  https://www.pcisecuritystandards.org/security_standards/pci_dss_download_agreement.shtml
- ●Supporting Documents のダウンロード
  https://www.pcisecuritystandards.org/security_standards/supporting_documents.shtml




関連文書や仕組みを含めて「PCI DSS」

**PCI DSS の核であるセキュリティ基準の内容について解説します。**

### 1. 序文

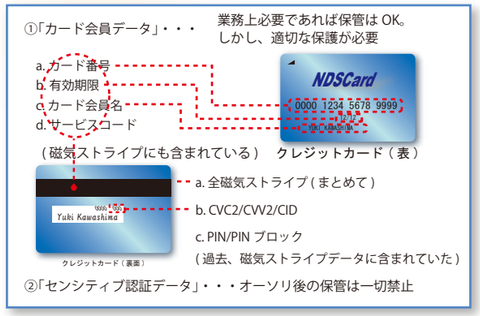
序文には、PCI DSS を適用する対象範囲の決定方法と、保護対象となるカード会員データの各要素に対する扱い方の基本的な方針が記載されています。ここでは、重要な点が３点挙げられますので、引用、解説します。

**1. 適用範囲 ( スコープ )**
PCI DSS は、PAN( カード会員番号 ) を扱っている部分に適用されます。「扱う」というのは、伝送、処理、保管のどれかを行っていることを指し、その業務で PAN を扱っていない場合は、PCI DSS の適用義務はありません。

**2. カード会員データとセンシティブ認証データの定義**
データ要素として、カード会員データとセンシティブ認証データの 2 種類に大別され、カード会員データを適切に保護すること、およびセンシティブ認証データはさらに厳密な対策を施す必要があること、が記載されています。
カード会員データは、伝送、処理、保管する場合は暗号化など適切な対策を施す必要があり、センシティブ認証データは、オーソリゼーション（※）後に適切に破棄する必要があります。つまり、センシティブ認証データは、オーソリゼーション後に保持することが認められません。

※ オーソリゼーションとは、そのカード情報で決済しても良いかを、発行元カード会社が判断する処理のことで、カード決済しようとしている加盟店から、様々なネットワークを経由して発行元カード会社まで届き、決済の可否結果が加盟店に返るまでのプロセスを指します

PCI DSS で保護が求められるデータ




**3. スコープの縮小**
これは、1. の補足事項といえます。カード会員データ環境、つまりカード会員データを扱う環境と、それに接続された環境が PCI DSS の対象であり、サーバやネットワーク機器、無線機器などを含むことになりますが、適切にセグメンテーション、アクセス制御を行うことにより、対象範囲を縮小することもできます。
これらの基本的な考え方を元に、それぞれの要素に対してどのような対策を行わなければならないのかが、要件 1 ～ 12 で示されています。

### 2. 安全なネットワークの構築と維持

本カテゴリーの 2 つの要件では、ファイアウォールとルータの安全な設定方法と運用方法、サーバやネットワーク機器においてデフォルト設定値を使用しないことを含む、セキュリティ強化基準の策定が求められています。

ファイアウォールとルータでは、外部ネットワークと DMZ、内部ネットワークの適切なセグメンテーション、業務上必要な通信に限定するためのアクセスリストの定義、安全なプロトコルの使用、設定内容の定期的なレビュー、また、これらを含む設定基準の文書化と運用が求められています。

要件 2 では主に、サーバやネットワーク機器において各種サーバやネットワーク機器の種別毎にセキュリティを強化するため、NIST や SANS、CIS などで定義されているものと同等の基準を策定、運用することが求められています。具体的には、

- ・無線ベンダのデフォルト SSID を使用しないこと
- ・Web サーバなどを構築する際、デフォルトでインストールされてしまう不必要な設定やコンテンツを削除すること
- ・サーバにデフォルトでインストールされるサービス、プロトコルを削除もしくは無効化すること

などが定められています。

### 3. カード会員データの保護

要件 3 では、「序文」で示された通り、センシティブ認証データをオーソリゼーション後に保持しないこと、カード会員データは必要最低限の量、必要最低限の期間のみ保管し、かつ安全に保管することが求められています。
安全に保管する方法として、一方向ハッシュ、トランケーション、インデックストークン、暗号化の４つの手法が挙げられています。つまり、必ずしも暗号化ではなく、一方向ハッシュなどの方法で判読不可能な状態にすることも含め、最善策の実施が求められています。業務上、カード会員番号の全桁を完全に復元する必要がないのであれば、トランケーションで必要な部分のみ保管することも選択肢として考えられます。もしくは、顧客サポートなどで一時的に手元のカード番号と電話口のカード番号を照合させるような場合は、一方向ハッシュを利用することも選択肢として考えられる場合もあるかもしれません。

また、ここで注意すべきことは、対策に暗号化を選択する場合のみ、追加の対策として鍵管理プロセスが求められることです。鍵が安全に管理されない暗号化は、全く意味を為さないものであり、極論をいえば暗号化していないのと同じ状態であると考えられるためです。例えば、暗号化していても、その暗号鍵が暗号化されたデータと同じ場所に保管されていては意味がありませんし、暗号鍵が容易に予測可能なものであっても効果は低いでしょう。また、1 人の管理者が鍵全体を知っているような場合、その管理者 1 名のモラルに依存することになり、その鍵と暗号化されたデータの安全性は著しく低下することを理解する必要があります。

そこで、要件 3.6 では、暗号鍵の生成方法、配布、保管方法が安全であること、鍵を定期的に変更すること、分割管理、鍵の漏洩、盗難、紛失の際の交換方法を定めること、などが求められています。

要件 4 では、カード会員データの伝送路上の安全の確保が求められています。要件の項目としては少なく、小項目で数えても３項目しかありません。

カード会員データを公衆ネットワーク上で送受信しなければいけない場合、暗号化することが求められています。公衆ネットワークとしては、インターネットや無線ネットワーク、GSM、GPRS が挙げられていますが、日本においては GSM よりも一般的な 3G や HSDPA ネットワークも当てはまると考えられます。逆に、専用線や相手先を限定、もしくはコールバック機能を適用したダイヤルアップ通信などは、公衆ネットワークとは考えません。暗号化の手法としては、HTTP の場合は SSL/TLS、IP レイヤーで行う必要があれば IPSEC などが必要です。無線ネットワークの場合は、WEP のみに頼ることなく、WPA、WPA2、および VPN や SSL/TLS との併用、WEP の共有鍵の定期的な変更や、MAC アドレスによる制御なども求められます。

暗号化されていないカード会員データの電子メールによる送受信の禁止も、この要件の中で求められています。

### PCI DSS の具体性の裏にあるもの

PCI DSS は、これまで述べた通り、具体的、明確にセキュリティ対策が記載されているため、より即効性が高く、かつ効果の高いセキュリティ基準であるといえますが、良い事ばかりではありません。その明確さゆえに、多種多様な業務形態、システムの構成やビジネスの内容に必ずしもうまく適合するとはいえません。つまり、具体的であるほど何をすべきかが分かりやすい反面、柔軟性に欠ける部分があります。また、U.S. 発祥の基準であることから、その内容に文化の違いがあることも否定できません。

例えば、PCI DSS では、カード会員データを保持しているシステムの場合、Linux サーバであろうと、メインフレームであろうと、同じセキュリティ対策、つまり暗号化やハッシュ化、トランケーションなどによる会員番号の保護が必要、と記載されています。しかし本当に、DMZ に存在する Linux サーバと、システムの最深部に存在するメインフレームに、同じセキュリティ対策が必要なのでしょうか。同じリスクが存在するのであれば、同じセキュリティ対策が必要になるかもしれませんが、必ずしもそうとは言えないはずです。

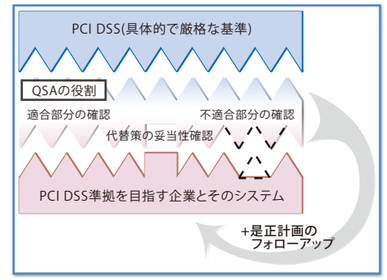
このような場合のために「代替策」という考え方が存在しますが、これは次回以降、説明いたします。

このように、具体的である反面、必ずしも現場に即さない要件が存在するのは否定できませんが、多くの要件では適切なセキュリティ対策を行うための指標となるはずです。また、全てを自分達で行うわけではなく、正しく PCI DSS の意図する対策が適切に施されており運用されているかを判断するために認定された企業「QSA」が存在します。

### QSA とは

QSA(Qualified Security Assessor) は、企業とその企業に所属する従業員の双方が要件を満たして初めて認定されるもので、企業を指して QSA と呼ぶことと、個人を指して QSA と呼ぶことがあり、どちらも間違いではありません。以前は、より明確に QSAC(QSA Company) と、QSAP(QSA Personnel) と呼ぶこともありましたが、最近は QSA と呼ぶことが多いようです。

企業としての QSA に求められるのは、企業としての安定性や訪問調査を行う上での独立性、企業保険、品質管理などがあります。個人としての QSA に求められるのは、主にセキュリティ関連業務の経験と知識、およびカードシステムについての知識です。




### PCI DSS はクレジットカード業界のもの？

PCI DSS はここまで述べたとおり、クレジットカード業界における、カード会員データを保護するために策定、運用、管理されている基準です。よって、カード会員データの内容について、詳細に保護、対策方法が示されています。しかし、カード会員データにあたる部分を、企業が持つ特に重要な情報、と読み替えることで、「カード業界で利用されている、強固なセキュリティ基準」と捉えることもできます。

PCI DSS は業界で認知されたシステム強化基準 SANS（SysAdmin, Audit, Network, Security）や NIST（National Institute of Standards Technology）、CIS（Center for Internet Security）などの考え方を多々取り入れており、かつ世界中の情報セキュリティの専門家が議論を重ね、策定され、運用され、かつ可能な限り実装に落とされている、非常に良くまとまった基準です。

PCIDSS は、あらゆる環境に対応できる基準となっていますが、特に不正アクセスの標的となり易いインターネット環境、Web 環境、に重点の置かれた要件が多く、より細かく、効果が期待できるものとなっています。よって、特にインターネット系、オープン系システムを採用している企業にとって、セキュリティ強化のためのガイドラインとして有効活用できます。