# セキュリティ基準「PCI DSS」の有用性
## ―他業種へ適用する際のポイント―

クレジットカードのセキュリティを定めた国際基準「PCI DSS（Payment Card Industry Data Security Standard）」は、個人情報と金銭情報を扱うがゆえに厳格なルールとなっている。そのため、クレジットカードを扱わない業種のセキュリティ基準としても有効である。本稿では、PCI DSSの概要と普及状況、これを他業種へ適用する際のポイントを解説する。

### 国際セキュリティ基準「PCI DSS」

PCI DSSは、国際カードブランド５社で構成されるPCI SSC（Payment Card Industry Security Standard Council）が、クレジットカード情報を取り扱う事業者に求められる要件についてまとめた国際セキュリティ基準である。2004年12月に策定され、改訂を経て現在はバージョン3.0（2013年11月）に至っている。

表１に示すように、PCI DSSでは12の要件が規定されている。表には示していないが、いずれの要件も具体的に定められている点が特徴であり、ISMS（情報セキュリティマネジメントシステム）など他の広く知られた基準との大きな違いである。例えばパスワードについては「英文字と数字の組み合わせで７文字以上」「90日ごとに変更」「直近の４回と同じパスワードを利用禁止」などとしている。

なおPCI SSCの構成メンバーはAmerican Express、Discover、JCB、MasterCard、Visaである。

### PCI DSSの普及状況

PCI SSCは、クレジットカードを取り扱う事業者をカード取引件数によってレベル分けし、レベルごとにPCI DSSへの準拠期限やその確認方法を定め、全ての加盟店とサービスプロバイダー（決済代行会社、会員を募集するカード会社、データ処理会社など）に対して準拠を求めている。最もPCI DSSへの準拠が進んでいる米国においては、PCI DSSに準拠すれば事故発生時に金融機関への損害賠償を免れることができるという州法や、PCI DSSに準拠しない場合は刑事罰もあるという州法があるなど、準拠が進む環境がある。

一方、日本ではまだまだ準拠が進んでいないというのが実情である。日本では改正割賦販売法（2010年12月施行）がクレジットカード情報の安全管理について定めているものの、PCI DSSに準拠しない法人に対する罰則規定は存在しない。このため、多くの企業では、多額の投資を行ってまでPCI DSSに準拠する明確な理由がなく、米国と比べると準拠への取り組みがあまり行われてこなかった。

このような状況下で、一般社団法人日本クレジット協会は経済産業省と連携し、2011年３月に「日本におけるクレジットカード情報管理強化に向けた実行計画」（www.j-credit.or.jp/info_management.html）を策定した。

NRIセキュアテクノロジーズ
マネジメントコンサルティング部
主任セキュリティコンサルタント
**板田俊一**（いただしゅんいち）

専門は情報セキュリティ全般に関するコンサルティング

**表1　PCI DSSセキュリティ基準**

| 項目 | 内容 |
|---|---|
| 安全なネットワークとシステムの構築と維持 | 1. カード会員データを保護するために、ファイアウオールをインストールして維持する<br>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ーにベンダー提供のデフォルト値を使用しない |
| カード会員データの保護 | 3. 保存されたカード会員データを保護する<br>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 |
| ぜい弱性管理プログラムの維持 | 5. 全てのシステムをマルウェアから保護し、ウイルス対策ソフトウェアを定期的に更新する<br>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 |
| 強力なアクセス制御手法の導入 | 7. カード会員データへのアクセスを、業務上必要な範囲内に制限する<br>8. システムコンポーネントへのアクセスを識別・認証する<br>9. カード会員データへの物理アクセスを制限する |
| ネットワークの定期的な監視およびテスト | 10. ネットワークリソースおよびカード会員データへの全てのアクセスを追跡および監視する<br>11. セキュリティシステムおよびプロセスを定期的にテストする |
| 情報セキュリティポリシーの維持 | 12. 全ての担当者の情報セキュリティに対応するポリシーを維持する |

この計画でも罰則規定はないが、準拠に向けた対応期限が定められていることから、現状を調査して部分的に対応を始める企業が徐々に増えている。

## 幅広い業種のセキュリティ基準として

PCI DSSは、クレジットカードの情報を扱わない企業にとっても、セキュリティ基準として非常に参考になる。これは、PCI DSSがクレジットカード情報という機微な情報の保護に関するグローバル基準であり、その内容が具体的という特徴があるからである。実際に、アカウント管理のルールについてPCI DSSの要件8を参考にしたり、システムのリスク評価に際して、PCI DSSに規定された評価項目を参考にしたりする企業がある。

ただし、PCI DSSをそのまま適用すればいいわけではない。例えば、PCI DSSは非常に高い水準のセキュリティ対策を求めているため、機微な情報を扱わない企業やシステムでは、費用対効果が釣り合わない過剰投資を招く恐れがある。PCI DSSではネットワークとサーバーに対して定期的なぜい弱性スキャン（検査）を外部（インターネット）と内部（社内ネットワーク）の両方のネットワークから実施することを求めているが、クレジットカード情報を扱わないのであれば、インターネットからの不特定多数の不正アクセスのリスクを考慮して、外部ネットワークからのスキャンを優先するという考え方もある。

このようにPCI DSSは、その要件を十分に理解した上で自社の事情に合わせて適切に取捨選択すれば、幅広い業種の企業で有効なセキュリティ基準として適用可能であろう。■