クレジットカードセキュリティ基準「PCI DSS」の有用性

クレジットカードの国際的なセキュリティ基準「PCI DSS」が注目されるようになっている。2010年９月の順守期限が近づき、審査機関もそろってきたことで、PCI DSSの導入は現実的な段階に入ってきた。本稿では、PCI DSSの概要と、2008年10月にリリースされたバージョン1.2の概要を紹介し、今後の日本での取り組みについて考察する。

汎用性の高いセキュリティ基準

PCI DSS（Payment Card Industry Data Security Standard）は、VISA、MasterCard、JCB、American Express、Discoverのクレジットカード大手５社により2004年12月に策定されたカード情報のセキュリティ基準である。

PCI DSSでは、下記の６つのカテゴリーに分けて、カード情報と決済情報を保護するためのデータの取り扱い方を規定している。

①安全なネットワークの構築と維持
②カード会員データの保護
③ぜい弱性管理プログラムの整備
④強固なアクセス制御手法の導入
⑤ネットワークの定期的な監視およびテスト
⑥情報セキュリティポリシーの整備

たとえば、「完全な磁気ストライプデータ、カード検証コード、暗証番号は保存してはいけない」「クレジットカード番号は保存する際に読み取り不能にしなくてはいけない」などクレジットカード情報の取り扱いに関する細かい決まりがある。また、クレジットカードに特有の規定以外に、一般にもあてはまるセキュリティ要件が定められている。そのカバー範囲が十分であることに加え、記述が具体的であるため、クレジットカード情報を扱わない一般企業にとってもセキュリティ対策基準としての有用性が認知されているのである。

PCI DSSで特徴的なのは、それぞれの基準に対して記述のとおりに対応できなかったとしても、その基準の目的に合致した代替手段を講じてもよいとされている点である。詳細な規定によってセキュリティ対策を求めると同時に、それを補完する代替手段を組み合わせることで、厳密さと実効性とのバランスを考慮したものと言える。

バージョン1.2の変更点

PCI DSSの最新版が、2008年10月にリリースされたバージョン1.2である。基本的には２年ごとの定期見直しにあたるが、記述のあいまい性の修正、冗長性の排除が見てとれる。

大きな変更としては、以前のバージョンで関係者の議論の的となっていた「Webアプリケーションの防御」の解釈があげられる。

バージョン1.2では、「Webアプリケーションの防御」について下記の２点のいずれかの対応を求めている。

①一般公開されているWebアプリケーションは、セキュリティのぜい弱性を手動または

NRIパシフィック
セキュリティアナリスト
曽谷祐一（そたにゆういち）
専門はWebサイトネットワークセキュリティ

自動で評価するツールまたは手法によって、少なくとも年1回、および何らかの変更を加えた後にレビューすること。

②一般公開されているWebアプリケーションの手前に、Webアプリケーションファイアウォールをインストールすること。

これ以外にも細かい修正が多数ある。たとえば、以前のバージョンでは、無線LANにおける暗号方式に、セキュリティの甘いWEP（Wired Equivalent Privacy）の利用を認めるなど、ところどころ要件が甘い点が見受けられたのに対し、新バージョンでは厳しいレベルでその基準が統一されたと感じられる。

より現実的な内容に改められた点もいくつかある。たとえば、従来は「セキュリティパッチはリリース後1カ月以内」とされていたのが、「リスクベースアプローチを適用し優先度を考慮することが可能」で、「重要度の低いシステムは3カ月以内」と変更された。これにより、公開サーバーなど優先度が高い部分での対応が早まることが期待できる。

一方、仕様書の形式も大きく変更された。前バージョンまでは、PCI DSSの基準のみ記載した資料と、その基準に合致することを評価するためのテスト手順に分かれていたが、バージョン1.2から、評価用のテスト手順に統一され、冗長性が解消されることになった。

加速する日本での取り組み

米国ではPCI DSSの導入はかなり進んでいるが、日本ではあまり普及してこなかった。それは、PCI DSSという基準があるのみで準拠の義務化までは明確にうたわれていなかったことと、日本では審査機関が少なかったことが理由と思われる。しかし、状況は大きく変わりつつある。

たとえば2008年11月には、VISAが「レベル1加盟店（取り扱い数が年間600万件以上）は2010年9月末まで」と順守期限を発表した。このため、PCI DSS対応機運が急速に高まることが予想される。

また、割賦販売法の改正（2008年6月18日公布、1年6カ月以内に施行）により、クレジットカード情報保護のために必要な措置が義務づけられたことも、普及を加速する要因としてあげられる。クレジットカード利用者のカード情報を保護するという目的はPCI DSSと同じなので、その内容はPCI DSSと矛盾するものにはならないはずであり、セキュリティ対策がPCI DSSに沿った形で進むことは間違いない。

なお、企業がPCI DSSへ準拠しているかどうか訪問調査する審査機関はQSA（Qualified Security Assessor）と呼ばれ、NRI（野村総合研究所）グループのNRIセキュアテクノロジーズ社も2009年1月にQSAに認定されている。また、同社やNTTデータ・セキュリティ社など合計31社による「日本カード情報セキュリティ協議会」が4月21日に発足し、PCI DSSの普及に向けた活動が進む見通しである。■