VOL. 1

PCI DSS 徹底解説 第 1 回
PCI DSS の概要 - 起源とその必要性 -

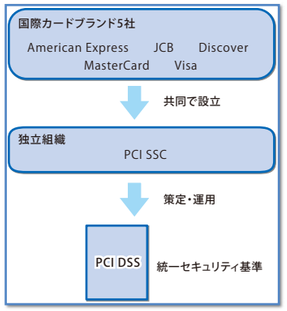
川島 祐樹

NTT データ・セキュリティ株式会社

PCI DSS とはなにか？
良い点と悪い点、必要性について解説します。

PCI DSS とは

PCI DSS とは、加盟店やサービスプロバイダにおいて、クレジットカード会員データを安全に取り扱う事を目的として策定された、クレジットカード業界のセキュリティ基準です。Payment Card Industry Data Security Standards の頭文字をとったもので、国際カードブランド 5 社 (American Express、Discover、JCB、MasterCard、VISA) が共同で設立した PCI SSC(Payment Card Industry Security Standards Council) によって運用、管理されています。



PCI DSS の生い立ち

本来競合であるはずの国際カードブランド間で最初から PCI SSC の設立、PCI DSS の策定に至った訳ではありません。元々は各国際カードブランドが独自に運用していたリスク管理プログラムがあり、加盟店は各ブランドの求める要求に応える必要がありました。

つまり、マルチアクワイヤリング (ひとつの加盟店で複数のカードが使える仕組み) が一般的な現在、各ブランドの要求に対応しなくてはならない加盟店にとっては、非常に大きな負荷とならざるを得ない状況だったわけです。その状況とは裏腹に、インターネットの普及に合わせ、国境を隔てたネット決済の普及とともに、極めて大規模なクレジットカード被害も世界規模で発生するようになり、IC カードによるカード偽造防止や対面取引における暗証番号での本人確認ではますます不十分となってきました。ここで、加盟店のリスクとコストに対応できる仕組みを作るべく、国際カードブランド 5 社が手を合わせ、世界的に統一されたクレジットカード情報保護のためのセキュリティ対策フレームワークができる流れとなりました。

現在の動向

個人情報の他にも多くの機密情報の漏洩や紛失事故が起きている現在、「セキュリティ」という単語はもはや日常的に聞かれるようになりました。しかし、セキュリティとは言っても何からすれば良いのか、どこまでやれば良いのかというのは大変難しく、ISMS(情報セキュリティマネジメントシステム) やプライバシーマークなどを用い、セキュリティレベルを向上、維持する動きが一般的になっています。これら、多くの基準や制度では包括的なセキュリティ対策を実施する手段、その枠組みを作る手段が示されており、有効活用することができます。

いま、企業に新しいセキュリティ基準が必要な理由

では、なぜ今になって新しいセキュリティ基準が必要なのでしょうか？セキュリティという言葉を聞いて、何が思い浮かぶでしょうか。「パソコンが使いづらくなる」、「せっかく便利なものがあるのに禁止される」、「いちいち承認が必要になって面倒だ」色々な声が上がるでしょう。

一方、経営者の方々が最も懸念している点は、恐らくコスト面で、「セキュリティはいくらお金をかけて良いのかわからない」、「高いお金をかけて導入したセキュリティ対策製品やソリューションでも、効果がよくわからない」ということでしょう。しかし、何もしなくても良いわけではなさそうなのが、難しいところです。ここで役に立つのが、ISMS です。自社の持つ資産と、それを損失した際のリスクを適切に把握して対策を実施するといった PDCA サイクルを回し、その有効性の評価と費用対効果の分析を行うことで、実施したセキュリティ対策がコストに見合っているかどうかがわかるはずです。

つまり、ISMS によるボトムアップ式のリスクマネジメントから、確実にセキュリティレベルを上げ、これを維持することは、企業にとって極めて基本的で包括的なセキュリティ対策であるといえます。リスク管理とそれに付随する費用対効果分析こそが、企業にとってのセキュリティであるといえるわけです。

しかし、一般的にこのプロセスを実現するには年単位での予算と実施計画が必要です。つまり、一言で言うと、時間がかかります。利便性、可用性が向上するとともに、それ以上の速さで脅威がシフトしている現在、自社のシステムや運用の弱点はどこなのか、そしてその弱点に対してどのような施策を打つべきなのかを迅速に判断し、適用していくことも非常に重要であるわけです。

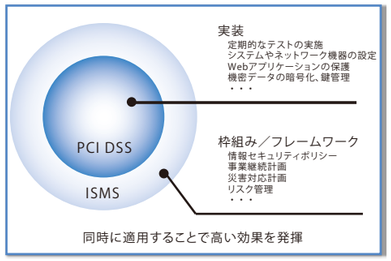
現実問題、セキュリティ対策を実施するまでの間に、SQL インジェクションなどの脆弱性を利用した攻撃により被害を受ける企業が相次いでいます。ここで、具体的で、すぐにでも実施できる対策が盛り込まれている新しい基準、つまり PCI DSS の必要性が重要視されてきたわけです。特に、クレジットカード情報の危殆は、不正利用などによる被害に加えて、カードの再発行、EC サイトの一時的閉鎖や原因調査、復旧、企業イメージの失墜など多大な被害を直接的に引き起こしうるものであることから、より確実にセキュリティ対策を施さなくてはなりません。もちろん、クレジットカード情報だけではなく、各業界、分野によって様々なものに置き換えて考える事もできます。

PCI DSS には、具体的で、すぐにでも実施できる対策が盛り込まれています。機密性の高い情報、つまりクレジットカード会員データについて、さらにはそのカード会員データの中でもどの情報が特に重要であり、どのように対策するべきかが記載されています。具体的には、6 つのカテゴリー、12 の要件から成り、それぞれの観点でどのような文書を作成し、どのような設定を施し、どのように運用するべきかが明確に記載されています。

では、ISMS よりも、PCI DSS を採用したほうが良いのでしょうか？

ISMS と PCI DSS は、互いに補完し合うものです。PCI DSS には、様々な対策が具体的に、明確に記載されていますが、その反面、例えばリスク管理については「リスク評価を行い、これに基づく情報セキュリティポリシーが策定され、運用されていること」というような書き方しかされていません。

つまり、ISMS で求められる情報セキュリティマネジメントのフレームワークが構築、運用されていることは、ある意味「前提」であると捉えることができます。実際に訪問調査を行ってきた経験を振り返ってみると、ISMS の認定を維持している企業の場合、PCI DSS における不適合項目が発見されても、これに対応するための体制や変更管理プロセスが整っているため、比較的短時間で是正が行われており、このことの裏付けであるといえます。



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。

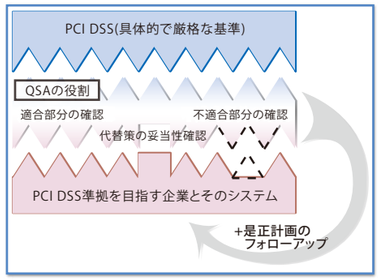
このような場合のために「代替策」という考え方が存在しますが、これは次回以降、説明いたします。

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。