VOL. 7

PCI DSS 徹底解説 第 7 回
基準のライフサイクル変更でどうなるのか？

池谷 陽
NTT データ・セキュリティ株式会社

基準ライフサイクルの変更

2010 年 10 月に予定されている PCI DSS、PA-DSS の改訂に合わせて、3 つの基準（PCI DSS、PA-DSS、PTS）のライフサイクルを 3 年に変更することが、2010 年 6 月 22 日付けで PCI SSC より発表されました。
今回は、ライフサイクルが変更された 3 つの基準のうち、PCI DSS と PA-DSS について、ライフサイクルの主な変更点と今後の展開を説明したいと思います。

主な変更点

PCI SSC の公開資料 " Lifecycle for Changes to the PCI DSS and PA-DSS " に記載されている変更点のうち、審査に直接影響するものを抜粋すると、以下の 2 点が挙げられます。

・3 年のライフサイクルで基準を改訂
・旧バージョンからの移行期間を 14 ヶ月に拡大

従来は、2 年ごとに基準が改訂され、改訂後 3 ヶ月弱で旧バージョンでの審査から新バージョンでの審査に移行する必要がありました。移行への猶予期間が短いことから、多くの PCI DSS 準拠企業では、基準が改訂されると対応が間に合わず、たちまち非準拠となってしまう心配があったのではないでしょうか。

図 1：従来のライフサイクル

■引用元
https://www.pcisecuritystandards.org/security_standards/pdfs/OS_PCI_Lifecycle.pdf

今回の変更で、3 年ごとの基準改訂となり、改訂後 14 ヶ月の移行期間が設けられたため、より現実的な準備期間を経て新バージョンでの審査に臨むことができるようになりました。
これは、PCI DSS に準拠する企業にとっては、改訂内容を十分に理解した上で、計画的に予算を確保して無理のないシステム改修や実装を行うための機会と捉えることができると思います。

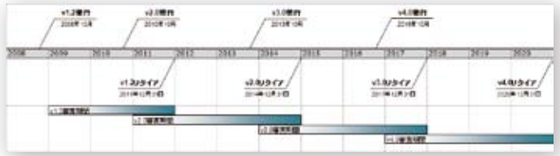
図 2：新しいライフサイクル

■引用元
https://www.pcisecuritystandards.org/security_standards/pdfs/OS_PCI_Lifecycle.pdf

PCI DSS バージョン移行のタイムライン

先述の図 2 をもとに、今後発行される PCI DSS 基準のバージョン番号を、順番に v2.0、v3.0、v4.0 と仮定して、バージョン移行のタイムラインを表すと以下のようになります。

図 3：PCI DSS バージョン移行のタイムライン



現行バージョンの 1.2 は、2011 年 12 月 31 日まで審査に使用可能なバージョンとなります。
次期バージョンの 2.0 は、2010 年 10 月に発行後、2011 年 1 月 1 日から有効となり、2014 年 12 月 31 日まで審査に使用可能です。
PCI DSS 準拠企業の対応としては、2011 年は v1.2 の審査を受けつつ v2.0 の対応を進め、2012 年に v2.0 の審査を受けるというのが典型例になるのではと予想しています。
あるいは、セキュリティ意識の高い企業では、2011 年中に v2.0 の審査を行い、いち早く新バージョンに対応したことを対外的にアピールするケースもあるかもしれません。

また、v1.2 の審査を受ける場合でも、効果的に v2.0 を活用することができると思います。
例えば、新バージョンには通常新たな脅威と技術が反映されて発行されますので、追加された要件を分析して、以下の PCI DSS 要件で要求されているリスク評価プロセスのインプットとして利用することが考えられます。

・12.1.2 脅威、脆弱性、結果を識別する年に一度のプロセスを正式なリスク評価に含める。
・12.1.3 レビューを少なくとも年に一度含め、環境の変化に合わせて更新する。

このように部分的に新バージョンを取り入れることで、次年度審査への準備に着手することもでき、バージョン移行をスムーズに推進できるのではないでしょうか。

PA-DSS バージョン移行のタイムライン

今後発行される PA-DSS 基準のバージョン番号を、順番に v2.0、v3.0、v4.0 と仮定して、バージョン移行のタイムラインを表すと以下のようになります。先述の図 2 にあるとおり、PA-DSS と PCI DSS のライフサイクルは共通なのですが、PA-DSS には有効期限（※）がありますので、以下の図にはバージョンの失効タイミングを追加しています。

図 4：PA-DSS バージョン移行のタイムライン

2011 年中に PA-DSS の審査を計画しているソフトウェアベンダーとしては、審査を受ける PA-DSS 基準は v1.2 と v2.0 の選択肢があります。v1.2 で審査を受ける場合、2013 年 10 月には有効期限を迎えて v2.0 での再検証が必要になりますので、製品寿命によっては審査回数が増え、トータルコストの増加につながってしまうことが考えられます。
審査を受けるバージョンを検討する際には、基準移行のタイムラインと製品ライフサイクルを考慮することをお勧めします。

※有効期限とは
ソフトウェアベンダーがペイメントアプリケーションの承認を維持するために、現在の PA-DSS 要件に対する再検証を受けなければならない期限のことです。
ベンダーが当該アプリケーションの販売を継続しない、つまり承認を維持しないことを選択した場合は、再検証が実施されずに有効期限を迎え、PCI SSC のリストに記載されているステータスが、"Acceptable only for Pre-Existing Deployments（既存の実装に対してのみ許容）" に変更されます。

参考リソース

■PCI Security Standards Council Announces New Three Year Lifecycle For Standards Development
https://www.pcisecuritystandards.org/pdfs/pr_100622_lifecycle.pdf

■Lifecycle for Changes to the PCI DSS and PA-DSS
https://www.pcisecuritystandards.org/pdfs/pci_lifecycle_for_changes_to_dss_and_padss.pdf

■Lifecycle for Changes to PTS
https://www.pcisecuritystandards.org/pdfs/pci_lifecycle_for_changes_to_pts.pdf