VOL. 4

PCI DSS 徹底解説 第 4 回
Prioritized Approach の活用

川島 祐樹

NTT データ・セキュリティ株式会社

PCI セキュリティスタンダードカウンシル (以下、SSC) では、2009 年 3 月 31 に "Prioritized Approach for PCI DSS 1.2" と称した文書とツールを公開しました。(URL: https://www.pcisecuritystandards.org/education/prioritized.shtml)
上記リンク先では、2 つのファイルがダウンロード可能となっています。

① Prioritized Approach for PCI DSS 1.2 (PDF ファイル、英語)

② Prioritized Approach for PCI DSS 1.2 (XLS ファイル、英語)

この文書では、PCI DSS の 12 要件を 6 つの "Milestone" に分類し、リスクを早期に排除するためのアプローチ方法が示されています。今回はこの文書における考え方、と注意点、また、活用方法を説明します。

Prioritized Approach とは？

Prioritized Approach とは、PCI DSS12 要件の優先順位付けを行うための参考資料です。注意しなければならないのは、これはあくまで優先順位を示すだけのものであり、対応すべき要件を取捨選択するものではありません。つまり、この文書で示された優先順位の高い要件に対応すれば、優先順位の低い要件は実施しなくても良いというわけではありません。

優先順位は、6 つの "Milestone" に分類されます。それぞれの Milestone は以下の通りです。

Milestone(1) センシティブ認証データを削除し、データの保持を制限すること
Milestone(2) 境界、内部、無線ネットワークを保護すること
Milestone(3) ペイメントカードアプリケーションを安全にすること
Milestone(4) システムへのアクセスを監視し、制御すること
Milestone(5) 保存されたカード会員データを保護すること
Milestone(6) 残りの準拠努力を完了し、すべての制御が実施されていることを確認すること

. なぜ、12 の観点で分けられた PCI DSS の要件を、このような形で再分類する必要が出てきたのでしょうか。それは、PCI DSS はあくまで対策を実施すべき対象をベースに分類されているためと考えられます。PCI DSS の要件 1 の観点は、「安全なネットワークの構築・維持」ですが、実際に要件を見てみると、主にファイアウォールとルータ、無線ネットワークに対する要件と、関連するプロセスに対する要件になっています。要件 1 すべてに対応すれば「安全なネットワークの構築・維持ができる」というわけではありませんし、これがもっとも重要かつリスクの高い箇所に対する要件というわけでもありません。

一方、Milestone1 では、以下の要件が分類されています。

- 1.1.2 ワイヤレスネットワークを含む、カード会員データへのすべての接続を示す最新ネットワーク図
- 3.1 保存するカード会員データは最小限に抑える。データの保存と廃棄に関するポリシーを作成する。データ保存ポリシーに従って、保存するデータ量と保存期間を、業務上、法律上、規則上必要な範囲に限定する。
- 3.2 承認後にセンシティブ認証データを保存しない（暗号化されている場合でも）。
- センシティブ認証データには、以降の要件 3.2.1 ～ 3.2.3 で言及されているデータを含む。
- 3.2.1 磁気ストライプのいかなるトラックのいかなる内容も保存しない（カードの裏面、チップ内、その他に存在する）。このデータは、全トラック、トラック、トラック 1、トラック 2、磁気ストライプデータとも呼ばれる。
- 3.2.2 カードを提示しない取引の確認に使用されるカード検証コードまたは値（ペイメントカードの前面または裏面に印字された 3 桁または 4 桁の数字）を保存しない。
- 3.2.3 個人識別番号（PIN）または暗号化された PIN ブロックを保存しない。
- 9.10 次のように、ビジネスまたは法律上の理由で不要になったカード会員データを含む媒体を破棄する。
- 9.10.1 カード会員データを再現できないよう、ハードコピー資料を裁断、焼却、またはパルプ化する。
- 9.10.2 カード会員データを再現できないように、電子媒体上のカード会員データを回復不能にする。
- 12.1.1 すべての PCI DSS 要件に対応する。

Milestone1 の目的として「センシティブ認証データを削除し、データの保持を制限すること」とある通り、CVV2/CVC2/CID、完全な磁気ストライプデータ、PIN または PIN ブロックなどのセンシティブ認証データの非保持を達成するための要件が分類されています。つまり、カード会員データを扱う企業のもつリスクを排除するために最も優先すべきことはセンシティブ認証データを持たないようにすることである、という考え方が読み取れます。

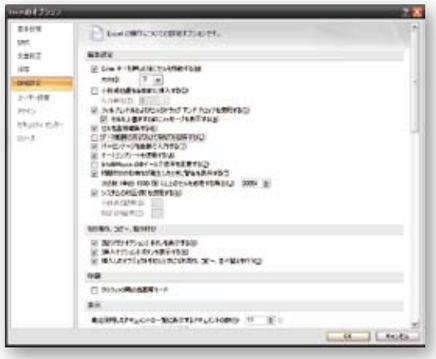
このように、Milestone(1)～ (6) では、リスクの高い順に要件が再整理されているため、同じ「完全準拠」を目指すとしても、より早い段階でリスクを排除するアプローチをとることができます。

Prioritized Approach ツール (上記②の Excel シート) の内容

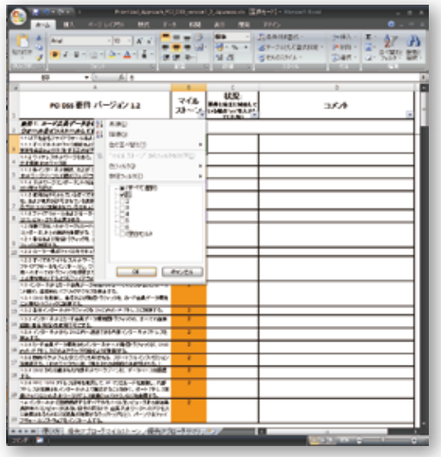
Prioritized Approach ツールは Excel シートとなっており、3 つのシートからなっています。それぞれのシートの説明をしたいと思います。ここでは便宜上、日本語版を使用しますが、PCI SSC から公開されているものではありませんので、PCI SSC からダウンロードできる英語版の内容と読み替えていただくか、個別にお問い合わせください。

シート (1) 使い方
使い方のシートには、この Excel シートの使用方法が記載してあります。このツールの使い方の流れの概要が記載されていますので、このシートでおおよその使い方がわかります。ここで示されたステップに従って作業を進めます。

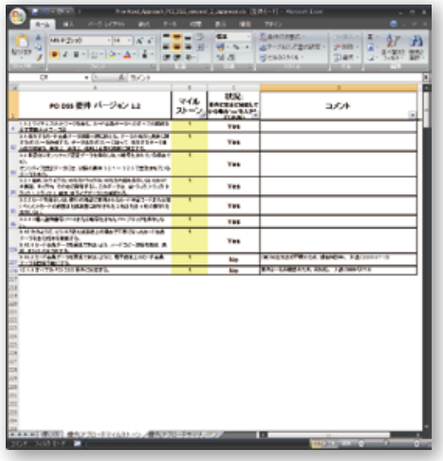
まず、ステップ 1 に示された通り、Excel の設定を変更する必要があります。



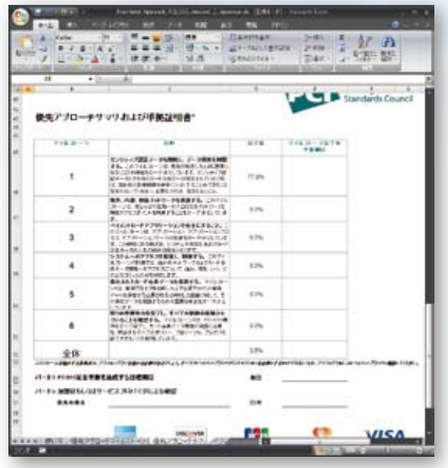
次に、ステップ 2 およびステップ 3 を実施しますが、ここではこれから実施するマイルストーンをフィルタ機能で選択します。優先アプローチマイルストーンのシートを開き、マイルストーンのセルの「▼」をクリックし、実施するマイルストーンを選択してください。



マイルストーンを選択したら、それぞれの要件の「状況」セルに「Yes」もしくは「No」を入力します。対策済項目には Yes、見対策項目には No を入力します。特に No の項目については現在どのような状況か、また、対応はいつ頃までに行うのか、対応者なども記入しておくと、後程役に立つはずです。また、Yesの場合も、参照するドキュメントや担当者を記入しておくことで、再確認する際にも非常に役に立ちます。



上記手順を実施した後、「優先アプローチサマリ」シートを確認することで、各マイルストーンおよび全体における「完了率」を確認することができます。



どのような場面で活用できるか

優先アプローチサマリは、あくまで PCI DSS に準拠しようとする組織が高いリスクを優先的に排除するためのツールです。加盟店やサービスプロバイダにおけるサービスレベルの定義や、バリデーション手続き（準拠証明に何が必要かがブランド毎に定められた手続き）に従って対応、報告をしなければなりませんが、自主的な診断であるとはいえ、どのように対応が進んでいるのか内部で情報を共有するためにも、経営層に報告するためにも、後々審査を行う QSA に確認してもらうためにも使えるでしょう。

また、今のところこの証明書を使用した正式なバリデーション手続きについてはまだ聞いたことがありませんが、今後、このようなツールが使用されるケースもあるかもしれません。テスト手順までは細かく記載されていない、全体の概要を把握するためのツールですので、うまく活用し、リスクの早期排除と PCI DSS 対応状況の把握と情報共有のために活用していただくことをお勧めします。

※日本語版 Prioritized Approach につきましては、E-mail にてお問い合わせください。
E-mail：pci@nttdata-sec.co.jp

※本ツールを使用することによっていかなる損害が生じようとも、当社は一切責任を負いません。