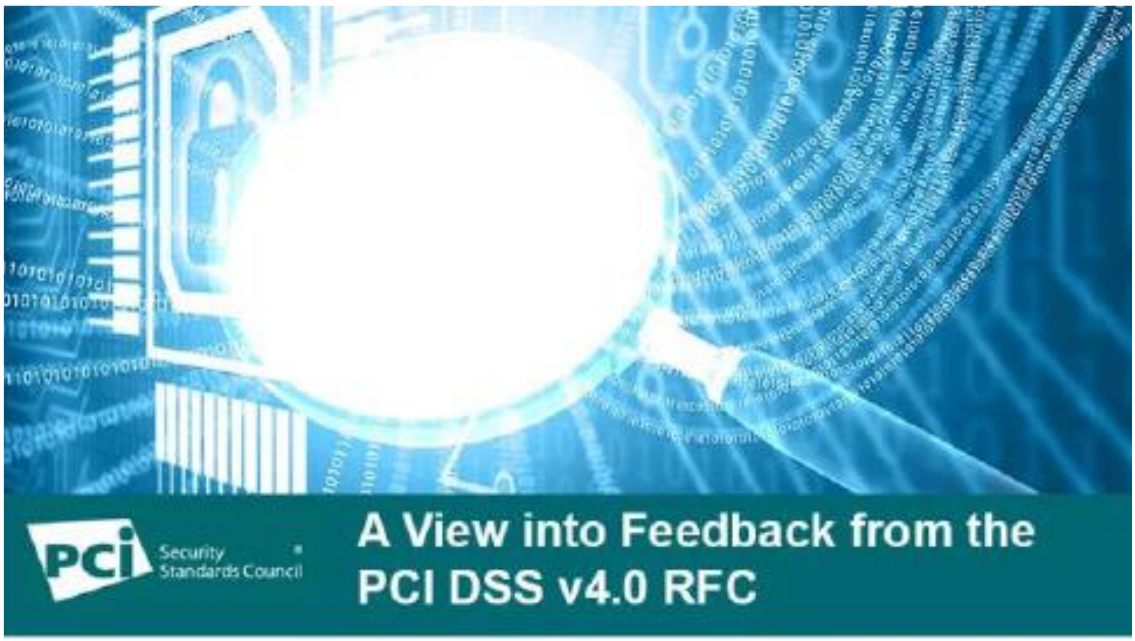

PCI DSS v4.0 RFC で提示されたフィードバックの概要

PCISSC は昨年実施された第 1 回目の PCI DSS v4.0 RFC(Request For Comments) にて提示された 3,000 件以上のコメントについて、先ごろレビューを完了しました。この RFC では単体の PCI 基準として最も多くのコメントが提示され、また業界レベルで PCI DSS の策定段階のドラフトレビューに参加した初めてのケースでした。次回の RFC は本年後半に予定されています。 RFC ではこのようなステークホルダーとの協働作業を通じ基準の新バージョンが形づくられていきます。
PCI DSS v4.0 策定タイムラインについての詳細は this blog post をご覧ください。

提案された要件の更新に関するフィードバック

2019 年の RFC で提示された PCI DSS v4.0 ドラフトには新規要件の追加と既存要件の変更の提案が含まれていました。これらの提案の意図はペイメントデータに対する新たなリスクや脅威への対応、ステークホルダーの対応への柔軟性の強化、そして継続的なプロセスとしてのセキュリティ強化を目指すものです。
下記は多くのフィードバックを通じ提示されたトピックの内、いくつか代表的な項目を記しています。

- 要件 4: 伝送時における強固な暗号化によるカード会員データ(CHD)の保護
  - CHD の全ての伝送の保護
  - 自己署名/内部証明書の使用
- 要件 8: ユーザーの特定とアクセスの認証
  - パスワード長、履歴、変更頻度など業界ガイダンスとの調和

    - 新規パスワードを既知、不良パスワードのリストと比較
    - 認証ファクターの成功•失敗結果を示す前段階ですべての多要素認証ファクターの確認
    - アプリケーション/システムのアカウント用にセキュアな認証
- 要件 9: カード会員データへの物理的アクセスを制限
    - カード会員データ環境内での機微なエリアの所在場所
- 要件 11: セキュリティシステムと処理の定期的なテスト
    - 脆弱性スキャン用に認証されたスキャニング
- 要件 12: ポリシーとプログラムで情報セキュリティを支援
    - 重要なテクノロジーを保護するためのポリシーの使用
    - 年次のリスクアセスメント
    - データ検知と流出防止のための手法

RFC が同一テーマで異なる組織から相反するフィードバックをもたらすことは稀なことではありません、そして PCI DSS v4.0 RFC もその例外ではありません。肯定的と否定的双方のフィードバックが提示されたトピックがあります。このようなフィードバックを評価する際に、PCI SSC は最善の判断をするために多様なファクターを考慮します。これらのファクターにはトピックで提示されたコメントに対応するための知見、フィードバックの提出者からのアドバイスやソリューション、そしてフィードバックの全体像を視野に判断します。

これらのフィードバックにおける議論では要件のセキュリティ価値の重要度、要件の意図と意味の明確性を確実にする方法、あらゆるタイプの環境とステークホルダーにおいて実施可能であることを確実にする方法、そして要件に準拠するための手法により柔軟性を提供する方法が考慮されます。次回の RFC に向けた PCI DSS v4.0 ドラフトの準備として、これらのフィードバックと結論を導き出す議論について現在検討を進めています。

新しいカスタマイズド•アプローチに関するフィードバック

PCI DSS v4.0 ドラフトにはカスタマイズド•アプローチ（これは PCI DSS 要件への対応と準拠確認の新しいアプローチ）を含みます。 このアプローチでは組織が PCI DSS 要件の目的に合致するための異なるセキュリティ•テクノロジーや手法を活用できるように、より柔軟性を付与します。これは新しいアプローチになりますので PCI SSC は大変多くのフィードバックを受理しています。PCI SSC はこの新しいアプローチ用に追加的なガイダンスを策定するためにこれらのフィードバックを活用しています。 これは次回の RFC におけるレビューの中に含まれます。

フィードバックのサマリー

2019 年の RFC 全体のフィードバックサマリーレポートは 2020 年 9～10 月に実施される次回の RFC と同時に PCI ポータルを通じて配信されます。サマリーレポートは PCI SSC が受理した各フィードバックとそれに対しどのように対応したかを示すものになります。

次回の RFC への準備

次回の RFC は 2020 年 9～10 月に予定されています。これはすべての PO(Participating Organization – 参加団体）と審査機関のコミュニティを対象に実施されます。

PCI SSC の RFC は PO メンバーを通じ関連業界に開かれています。もし次回の RFC へのご参加を希望される場合は PO にご参加いただくことにより可能になります。PO プログラムおよびメリットなどの詳細については here をご確認ください。

また、RFC プログラムについての詳細はリンク Request for Comments page. をご確認ください。

2020 年 7 月 31 日