PCI DSS v4.0：カスタマイズドアプローチのための役割と責任

本ブログは一連のカスタマイズドアプローチに関する記事の第 3 回目になります。第 1 回目ではカスタマイズドアプローチのハイレベルの概要と代替コントロールとの違いについて探求しました。第 2 回目では事業体がカスタマイズドアプローチの実行を考える場合に考慮すべきポイントに焦点を当て、そして PCI DSS と ROC テンプレートに含まれるカスタマイズドアプローチのリソースについて詳細を提示しました。今回は実際にカスタマイズドアプローチの開発と実行に取り組む事業体と PCI DSS 評価の一環としてカスタマイズドアプローチをレビューする評価者双方の役割と責任に焦点を当てます。

PCI DSS v4.0 ではカスタマイズドアプローチは事業体がセキュリティ目的を達成するため異なる手法を使う柔軟性を支援するために導入されました。カスタマイズドアプローチはセキュリティ目的を達成するために、革新的なテクノロジーを活用できるように、より柔軟性を希望していたステークホルダーからのフィードバックに対応するために開発されました。これらの新しいテクノロジーは従来型の PCI DSS の実行や準拠確認手法の範囲では適合しない場合があります。

このポストでは、データセキュリティ基準担当ダイレクター Lauren Holloway がカスタマイズドアプローチについてのいくつかの共通質問に対応します。

カスタマイズドアプローチで評価される事業体の役割とは何ですか?

Lauren Holloway: 評価される事業体はカスタマイズされたコントロールを設計、開発、分析、実行そして維持します。これには以下のステップが含まれます:

- 要件 8 、要件 12.3.2、そして付録 D と E を含む PCI DSS に含まれるカスタマイズドアプローチ情報をレビューする。
- 当該コントロールがどのように要件の目的に適合するのかの記述を含んだ各カスタマイズされたコントロールの定義と文書化する。サンプルのコントロールマトリックスは PCI DSS 付録 E1 に含まれている。
- カスタマイズされたコントロールが定義された要件と少なくとも同等の保護を提供するために十分に強固であることを示すターゲットリスク分析を実行し文書化する。サンプルのターゲットリスク分析は PCI DSS 付録 E 2 に含まれている。
- 各カスタマイズされたコントロールが要件の目的に効果的に適合していることを確認するテストの実行と文書化する。
- 各コントロールの有効性がどのようにメンテナンスされ随時モニターされているかについて記述する。
- カスタマイズアプローチを実行するための計画について評価者と早期に情報連携する。
- 各カスタマイズアプローチについて評価者への全ての文書を提示する。

どのカスタマイズされたコントロールについても評価される事業体が責任を内製化し、その実行当事者として積極的に管理してゆくことが重要です。

カスタマイズドアプローチで評価者の役割とは何ですか?

Lauren Holloway: 評価者は事業体からすべてのカスタマイズアプローチ文書を受け取り以下のステップを実行します:

- カスタマイズされたコントロールを完全に理解するために事業体の文書をレビューする。
- 各カスタマイズされたアプローチが文書化され、必要な情報が網羅され、そしてカスタマイズされたコントロールがどのように定義された要件と少なくとも同等の保護を提示しているかを確認する。各カスタマイズされたコントロールの徹底的なテストの結果を得られるテスト手順を考案する。
- 以下について判断するため、各カスタマイズされたコントロールの実行をテストする
    - カスタマイズアプローチの目的に適合しているか
    - 継続的に有効でるあることを確保するためにメンテナンスされているか、そして
    - 評価結果として適合と結論できるか
- 各コントロール、考案されたテスト手順、テスト結果、そしてその他の関連する詳細を ROC（要件と ROC 付録 E 双方）に文書化する。

QSA 会社は事業体の代わりにカスタマイズされたコントロールを設計または実行できるか？

Lauren Holloway: QSA スタッフはカスタマイズされたコントロールを設計または実行のアシストをすることができますが、QSA 会社は QSA 資格要件および QSA プログラムガイド（QSA Qualification Requirements and QSA Program Guide）で定義された独立要件を固守しなければなりません。これには PCI DSS 評価を実施またはアシストする QSA スタッフが独立しており利害の衝突がないことを確実にするため義務の分離が適正に管理されていることを含みます。

カスタマイズされたコントロールの設計や実行に関与した QSA スタッフが、そのカスタマイズされたコントロールのテスト手順の考案、評価または評価のアシストするのは利害の衝突になります。FAQ 1562 に“顧客のために特定のコントロールを設計、開発、実行する QSA スタッフはそれらの同一コントロールを評価することが許可されるか？”という PCI SSC の FAQ とその詳細な情報があります。

QSA スタッフはカスタマイズアプローチに関係するコンサルテイングサービスを提供することができますが、カスタマイズされたコントロールを設計または実行するために QSA を必要としている事業体は、そのコントロールを維持し効果的な運用を継続することを確実にすることが難しいのでカスタマイズアプローチに取り組む良い候補ではないでしょう。リスクに対する成熟、コミットメントおよび自身のカスタマイズされたコントロールを開発、実行、維持するために必要なリソースを伴う事業体がカスタマイズされたコントロールで長期的に有効なセキュリティをより達成できます。

より詳細は情報は　PCI DSS v4.0 リソースハブをご覧ください

(**Visit the Resource Hub for More Information on PCI DSS v4.0**