PCI DSS v4.0 : 「カスタマイズアプローチ」は貴社に適しているか？

本ブログは「カスタマイズアプローチ」に関する記事シリーズの 2 回目です。初回の記事は「カスタマイズアプローチ」の概要と「代替コントロール」との相違点について掘り下げました。本ブログでは「カスタマイズアプローチ」の実行について事業体が考慮すべき点と PCI DSS の中で事業体に提供されるリソースと評価者向けに提供される PCI DSS Report On Compliance (ROC) テンプレートの詳細に焦点を当てます。

「カスタマイズアプローチ」はセキュリティの目的を達成するために異なる手法を採用している事業体を、より柔軟性もって支援するために導入されました。「カスタマイズアプローチ」はセキュリティの目的を達成するため革新的なテクノロジーを使うために、柔軟性を求めたステークホルダーからのフィードバックに基づき策定されました。新しいテクノロジーが PCI DSS の実行とバリデーションのための従来のアプローチの枠内では適合しないことがあります。

「カスタマイズアプローチ」についていくつかの共通の質問に答えるためデータセキュリティ基準担当ダイレクターである Lauren Holloway, Director of Data Security Standards と話をします。

事業体が「カスタマイズアプローチ」を実行すべきかどうか誰が判断するのでしょうか？

各事業体は「定義されたアプローチ」または「カスタマイズアプローチ」のどちらに則り対応するかを含め、PCI SSC 要件にどのように準拠するか判断します。

「定義されたアプローチ」は事業体と評価者が長年にわたり PCI DSS 要件の実行とバリデーションのために取組んできたアプローチです。そして PCI DSS v4.0 でも選択肢として継続されます。このアプローチはすでに要件対応のためのコントロールが設定されており、それらのコントロールのバリデーションに現在の手法を志向す

る事業体に適しています。また、新規に PCI DSS に取り組み、セキュリティの目的への対応方法につき具体的な方向を模索している事業体にも適しています。

「カスタマイズアプローチ」は「定義されたアプローチ」とは異なる新たな選択肢であり、PCI DSS 要件に示された「カスタマイズアプローチの目的」に集中します。このアプローチはより柔軟性を提示し、「カスタマイズアプローチの目的」に対応する他のセキュリティコントロールもしくは新しいテクノロジーの使用を希望する事業体に適しています。

事業体と評価者が協力し、評価者は事業体によって設計されたカスタマイズされたコントロールを完全に理解し、そして事業体は評価者がコントロールの評価結果に基づき実施するテストについて理解することが重要です。

「カスタマイズアプローチ」の採用を志向する事業体は、関連する要件や影響を理解するためにコンプライアンス-受付団体（アクワイアラもしくはペイメントブランド）と協議するべきです。

事業体はいつ「カスタマイズアプローチ」を使うための判断をすべきですか？

「カスタマイズアプローチ」の使用には、そのコントロールが全ての必要なドキュメントにより適格に実行され、サポートされていることを確実にするため、事業体に初期段階での努力が求められており、それが有効に評価されます。事業体より適格に検討、文書化、テスト、そして維持されるカスタマイズされた実行策は、評価者にコントロールがどのように機能しているかについて正確な詳細情報を提供することになり、評価プロセスを効果的に促進させることになります。これは評価者が評価時に実行策をバリデートするために必要とする適切なテストの決定を助けることになります。

事業体は PCIDSS 準拠評価が開始されるよりも以前に「カスタマイズアプローチ」のためのコントロールを設計、実行、文書化していることが推奨されます。

この他に事業体が「カスタマイズアプローチ」を実施するかどうか判断する時に何を考慮すべきでしょうか？

「カスタマイズアプローチ」は規定されている PCIDSS 要件に準拠対応しなければならない一時的な措置として、また評価時に確認された未準拠項目について対応するために使われることを意図していません。

もし事業体が評価期間中に「カスタマイズアプローチ」の実施を判断する場合、事業体がカスタマイズされたコントロールを設計、実行、文書化するまでの間、その評価手続きは相当遅延することになります。

「カスタマイズアプローチ」はどのようなタイプの事業体を想定していますか？

「カスタマイズアプローチ」を実行する事業体は「カスタマイズアプローチの目的」を達成するためのコントロールを設計、実行、維持すること、そしてそのコントロールが有効に機能していることを確実にすることが期待されます。それ故に「カスタマイズアプローチ」はセキュリティに対する強固なリスク管理アプローチを表明するリスクに関し成熟した事業体を想定しています。

リスクに成熟していることが強く推奨されているのは、これが事業体の「カスタマイズアプローチ」の成功に寄与することになるからです。事業体が「カスタマイズアプローチの目的」をより良く理解、達成し、そして PCI DSS の中で明示されている必要な文書化要件を有効に履行するための助けになります。

カスタマイズされたコントロールの設計や実行にあたり QSA の支援を必要とする事業体は、コントロールを維持し効果的な運用を確実に継続するのが困難と想定されるため、「カスタマイズアプローチ」は良い選択肢ではないかも知れません。

リスクに成熟した事業体の典型的な特徴として以下のようなものが含まれます:

- リスクを管理するために組織全体に亘るアプローチを定義している確立されたリスク管理プログラムがある
- ビジネスの全てのラインに跨りリスクが考慮されていることをシニア経営層が確実にしている
- リスクと事業の目的において、両者の関係がクリアに理解され意思決定時に考慮されている
- リスク管理のプラクティスが正式に承認され、組織の方針の中で明記されている
- 技術的に複雑なリスク分析を実行するために人材が特別に訓練され認定されている
- 組織の資産に対するリスクの継続的なモニタリングが行われている
- 脅威やテクノロジーの環境変化に対しプロアクテイブに適合している
- リスク分野において変化に対し継続的な改善と効果的に対応する手法が適切に装備されている

公的に認められた成熟したリスク管理アプローチの事例の中には、ISO、NIST、MITRE、そして COSO によって開発されたものが含まれます。

「カスタマイズアプローチ」のリソース

下記の「カスタマイズアプローチ」のリソースは PCI DSS 基準書内に含まれます :

- *セクション 8: PCI DSS の導入と検証のためのアプローチ*– 「定義されたアプローチ」、「代替コントロール」「カスタマイズアプローチ」の概要を提示
- *要件 12.3.2* –「カスタマイズアプローチ」を実行する事業体は、各影響を受ける要件について「ターゲットリスク分析」を実行しなければならないという要件を設定
- *付録 D:「カスタマイズアプローチ」* – 「カスタマイズアプローチ」を実行する事業体によって、そしてカスタマイズされたコントロールの評価を実行する評価者によって満たさなければならない基準の明示
- *付録 E:「カスタマイズアプローチ」を支援するテンプレートの例*
  - *付録 E1:「コントロール マトリックス」の例* – 事業体が「コントロールマトリックス」の中に含めなければならない最小限の情報を指定しているテンプレートを提示
  - *付録 E2:「ターゲットリスク分析」テンプレートの例* – 事業体が「ターゲットリスク分析」の中に含めなければならない最小限の情報を指定しているテンプレートを提示

下記の「カスタマイズアプローチ」のリソースは PCI DSS ROC テンプレート内に含まれます:

- *パート II: 発見結果と観察* – 各影響を受ける要件において、評価者は事業体が要件対応のためにどこで、そして要件のどの点においてカスタマイズされたコントロールを採用したかを指定する
- *付録 E:「カスタマイズアプローチ」テンプレート* – 評価者は PCI DSS 要件に対応するためにカスタマイズされたコントロールが使われた実例を文書化するためにこのテンプレートを使用する

本シリーズ 3 回目が発行された時にお知らせするためにブログの購読は Subscribe to the blog になります。 第 3 回目の記事は、「カスタマイズアプローチ」においてカスタマイズされたコントロールを開発し実行する事業体と PCI DSS 評価の一部としてカスタマイズされたコントロールを評価する評価者の役割と責任に焦点を当てます。

PCIDSS に関する詳細情報については「PCI DSS v4.0 Resource Hub」（下記リンク）をご確認ください。

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