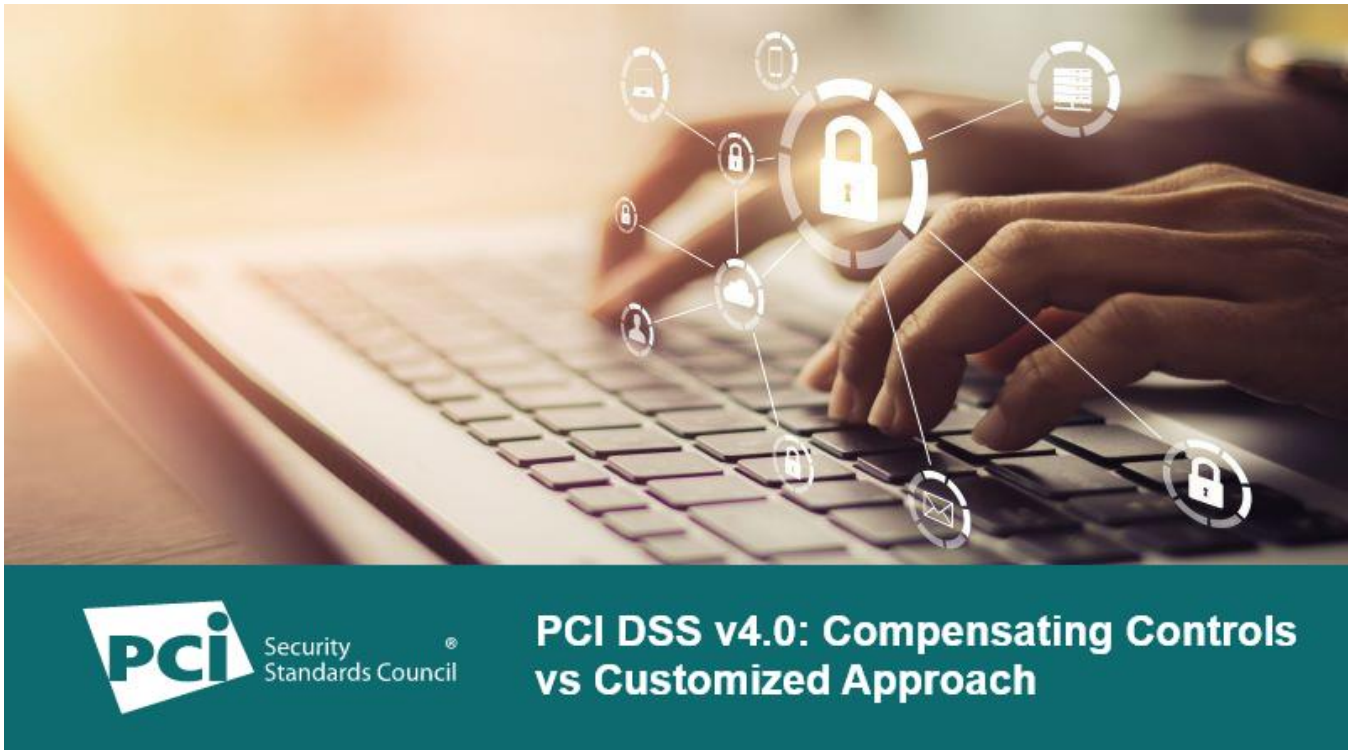


# PCI DSS v4.0: 代替コントロール 対 カスタマイズアプローチ

PCI DSS v4.0 の主要なゴールはセキュリティ目的を達成するための異なる手法を採用している事業体のために柔軟性を高めることです。新基準ではこれを実現させる方策の一つとしてカスタマイズアプローチを導入しています。私たちはこのカスタマイズアプローチについてのいくつかの共通する質問についてデータセキュリティ基準担当ダイレクター Lauren Holloway に話を伺います。

**代替コントロールとカスタマイズアプローチの違いとは何ですか？**

**Lauren Holloway:** PCI DSS v4.0 では事業体が PCI DSS 要件を実行し準拠確認するための 2 つの方法、すなわち－定義されたアプローチとカスタマイズアプローチ－を提示しています。定義されたアプローチは PCI DSS コントロールを実行し準拠確認する旧来の手法で、事業体が現在 PCI DSS v3.2.1 の要件に対応するために実施している手法です。代替コントロー

ルは正当で文書化された技術的またはビジネス上の事情により定義されたアプローチ要件への対応を阻害されている事業体に対し、定義されたアプローチの範囲での選択肢になります。代替コントロールはしばしば要件対応のために改変できないレガシーシステムやプロセスが存在する状況で使われます。

PCI DSS v4.0 では Appendix B の中で代替コントロールが過去に逸した要件対応について遡って対応するために使用することができない旨を明らかにしてます。代替コントロールは例えば、実施されるべきであったタスクが実施されなかった場合、そしてそれを対応するための行動がとられなかった場合に使うことを意図した選択肢ではありません。

代替コントロールはカスタマイズアプローチとは異なる目的で使われることに留意することが重要です。事業体が事情を抱え記載通りの要件対応ができない時の代替コントロールのような手法ではなく、異なる手法での要件対応をめざす事業体にカスタマイズアプローチは適しています。この場合、事業体は記載された要件でなく、規定されたカスタマイズアプローチの目的に対応しなければなりません。カスタマイズアプローチは頑強なセキュリティプロセスと強力なリスクマネジメントプラクティスを有し、目的を達成するためにセキュリティコントロールの効果的な設計、文書化、テストそして維持ができる事業体が最も成功させることができます。

PCI DSS v4.0 要件 12.3.2 と Appendices D および E ではカスタマイズアプローチの全ての要素、ここには必要なターゲットリスク分析、事業体と評価者双方の責任、カスタマイズアプローチを文書化する事業体によって含まれなけれななならない情報を網羅したサンプルテンプレートが含まれています。

各要件において、定義されたアプローチの要件とカスタマイズアプローチの目的の所在を特定するために、図５：「要件 部分の理解」をご参照ください。

**代替コントロールはカスタマイズアプローチの目的に対応するために使うことができますか？**

**Lauren Holloway:** いいえ、代替コントロールはカスタマイズアプローチに伴う選択肢ではありません。カスタマイズアプローチは当該要件のカスタマイズアプローチの目的に対応するため事業体自身がコントロールを開発する事業体のためにあります。事業体が新たな代替コントロールを開発することもまた意味を成しません、なぜなら事業体がそのために開発した実行策はカスタマイズアプローチの目的に対応することができません。

**代替コントロールとカスタマイズアプローチは同一要件のために使うことができますか？**

**Lauren Holloway:** はい、事業体は特定のシステムコンポーネントのために代替コントロール、他のシステムコンポーネントにおいて同一要件に対応するためにカスタマイズアプローチを使うことができます。例えば要件 5.3.1 において、事業体は正当で文書化されたビジネス上の事情がある特定のタイプのサーバーについて、規定された要件対応から外し、要件に対応するために代替コントロールを使うことができます。 事業体ははまた、最新のマルウエアの脅威を検知・対応するためにユニークなアプローチを実行しているその他のシステムコンポーネントが同一要件に対応するためカスタマイズアプローチの活用を選択することができます。事業体はさらに他のシステムコンポーネントグループのために同一要件に対応するため定義されたアプローチを活用することもできます。

Subscribe to the blog ブログを購読するとカスタマイズアプローチのについての詳細情報、事業体と評価者のタスクと責任、カスタマイズアプローチを選択する前に検討すべき重要項目などを含むトピックの次のブログの投稿についてもお知らせします。

**PCI DSS v4.0 に関する詳細情報は下記サイトをご確認ください:**

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