



Changes to PCI DSS v4.0 Reporting: In Place with Remediation

PCI DSS v4.0 のレポーティングの変更: 「是正を伴う対応」

2022年3月に PCI DSS v4.0 がリリースされた際、「是正を伴う対応」という新しいレポーティングの選択肢が文書の要件に組み込まれました。この選択肢のゴールは事業者が年次ごとに改善の必要な領域を特定するための手法として提示することにより、継続的プロセスとしてセキュリティを推進するためのものでした。この手法がセキュリティを向上させるために有効であるという点についてステークホルダーより合意を得ておりましたが、最近のフィードバックではこのゴールを達成するためにより良いと思われる方法があるとの指摘を受けています。

このフィードバックへの対応として、PCI SSC は「是正を伴う対応」という選択肢を取り除くために PCI DSS v4.0 のバリデーション文書を更新します。私たちは今回の PCI DSS v4.0 バリデーション文書の更新に関して、いくつかの共通の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 に話を聞きます。

どの文書が更新されますか？

Lauren Holloway: PCI DSS v4.0 の Report on Compliance (ROC) テンプレート, 準拠証明書 (AOCs), そして自己問診票 (SAQs)でレポーティングの選択肢として「是正を伴う対応」を取り除くために更新されます。

この更新は基準に影響がありますか?

Lauren Holloway: いいえ、この更新は PCI DSS v4.0 バリデーション文書に限定されています。この更新を反映する形で、「*The Report on Compliance Template - Frequently Asked Questions*」という文書も更新されます。

バリデーション文書ではその他の変更も発生しますか?

Lauren Holloway: 「是正を伴う対応」の削除に加えて、文書フォーマットの修正といくつかの明確化のための修正を含みます。

更新された文書はいつから利用可能となりますか?

Lauren Holloway: 更新されたバリデーション文書は 2022 年末までに発表されるように計画しています。文書が PCI SSC ドキュメントライブラリに追加されたら RSS フィードで通知されるように設定をご確認ください。設定が有効になり次第、以前のバージョンが保持されます。

これは PCI DSS v4.0 評価の途上、もしくはすでに完了した場合にどのような影響がありますか?

Lauren Holloway: 今回の更新が PCI DSS v4.0 評価の途上、もしくはすでに完了している場合の影響に関するご質問は、各事業体のコンプライアンス管理-受付団体にご連絡ください。なお、ペイメントブランドへの連絡先情報の詳細については FAQ 1142 “How do I contact the Payment Card Brands” をご覧ください。

改善が必要な領域についての情報を文書化するために他の手法は提示されますか？

Lauren Holloway: はい、継続的プロセスとしてセキュリティへ取り組む事業体をご支援するため、PCI SSC は改善が必要な領域について評価者が文書化するための別立てのワークシートを作成中です。事業体が分かりやすくワークシートを活用できるようにするため、例えば FAQ やその他の資料など追加的なガイダンスが提示されます。

QSA プログラムガイドについても評価者がワークシートの完成のための要件と期待すべき点を明らかにするために更新されます。

新しいワークシートはいつ利用可能になりますか？

Lauren Holloway: 新しいワークシートと FAQ やその他の資料など追加ガイダンスは 2023 年の早い時期に利用可能となります。

すべての文書は PCI SSC ウェブサイト上のドキュメントライブラリのなかで公開されます。