PCI DSS v4.0：今後のスケジュールと最新情報

ペイメント、テクノロジーそしてセキュリティの変化と共に業界からのフィードバック（ご意見）が PCI DSS v4.0 改訂へのアプローチをリードしています。PCI SSC は業界関係者との協議を通じ、PCI DSS v4.0 について多くのご質問を受けました。そこで PCI DSS v4.0 の現在の状況について鍵となるご質問に対し、DSS 担当ディレクターである Lauren Holloway がインタビューを通じ回答をいたします。

注意： *本記事の中で述べられている日付はすべて現時点での見通しに基づくもので今後変更される可能性があります*

PCI DSS 文書化処理は現在どのような状況でしょうか？

Lauren Holloway： 2019 年 10 月～12 月に実施された The request for comment（RFC）ではドラフト版に対し 3,000 件以上のご意見が寄せられました。現在、PCI SSC は受理したこれらのフィードバックをすべてレビューし検討しています。追加の RFC が 2020 年 9 月～10 月に計画されています。追加の RFC では前回受理したフィードバックをベースとして新しく更新された PCI DSS v4.0 ドラフトバージョンが使われます。

次回の RFC および RFC のプロセスについての詳細情報は RFC Page をご確認ください。

PCI DSS v4.0 はいつリリースされますか？

Lauren Holloway： PCI DSS v4.0 の最終版の発表は現時点では 2021 年中頃に予定されています。このタイムフレームは従来の PCI DSS の改訂よりも際立って長めの時間が設定されていることになります。

今回の改訂プロセスの中ではステークホルダーがフィードバックを提示する機会が追加され、それについて対応するためにこの延長されたタイムフレームが設定されました。

詳細（英語のみ）：3 Things to Know about PCI DSS v4.0 Development

2019 年の RFC にて受理されたフィードバックの詳細の分析結果は提示されるのでしょうか？

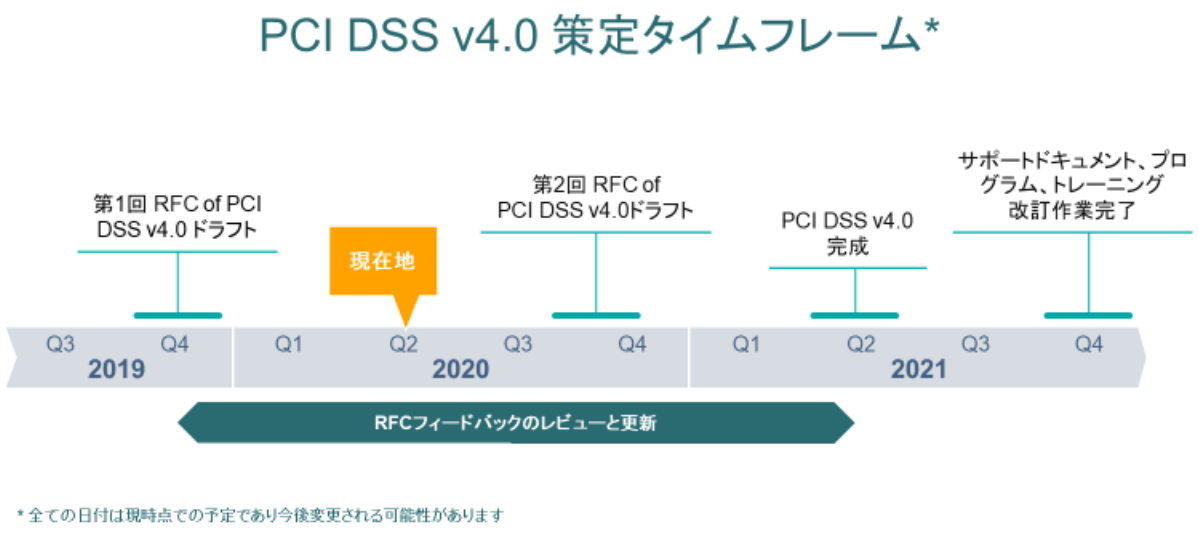
Lauren Holloway： 3,000 件以上のフィードバックのレビューが完了し PCI DSS v4.0 ドラフトが更新された時点で、「RFC フィードバックサマリーレポート」が 2019 年の RFC ご参加者に PCI Portal を通じ供給されます。このサマリーでは各フィードバックがどのように対応されたかを示しますが、追加 RFC の時にこれらの参加者宛てにアクセスが可能となります。

加えて、PCI SSC は四半期ごとのステークホルダーウェブキャストと本年後半に計画されているコミュニティ・ミーティングを通じ PCI SSC のコミュニティにアップデートを提示します。

自己問診票（SAQ）はいつ更新されますか？また どのような変更が含まれますか？

Lauren Holloway： SAQ、ROC、PCI DSS Glossary そして Prioritized Approach を含むサポートドキュメントの改訂は PCI DSS が改訂される時に、その改訂作業プロセスの一環として行われます。PCI SSC は本年後半に PCI DSS v4.0 と連動してすべてのサポートドキュメントについて改訂作業を開始し、進捗の状況を提示いたします。PCI SSC は PCI DSS v4.0 最終版発表後、数か月以内にこれらのドキュメントを完成させリリースできるように計画しています。

下記のチャートは RFC, 予定されている PCI DSS v4.0 関連マテリアルを含む、PCI DSS v4.0 の策定に向けた現在のタイムラインの概要を示します。



PCI DSS v4.0 のリリース後どれくらいの期間で実行しなければなりませんか？

Lauren Holloway： PCI DSS v4.0 発表後、PCI DSS v3.2.1 から v4.0 に更新する組織に対して拡張的な移行期間が提示されるでしょう。移行期間は更新作業を支援するために、PCI DSS v4.0 発表後さらに関連するすべてのマテリアル、すなわち　基準、サポートドキュメント（SQ,ROC,と AOC を含む）トレーニングそしてプログラムがリリースされた後に 18 か月間設定されます。

> ***注意：****PCI DSS v4.0 基準はその運用を支援するために必要とされるサポートドキュメント、トレーニングとプログラムの改訂に先立ち 6 か月前に発表されるようにスケジュールされます。そのため結果的に、PCI DSS v4.0 基準の発表から PCIDSS v3.2.1 の引退まで 2 年間の移行期間があります。*

この拡張的な移行期間の設定により組織が PCI DSS v4.0 の変更点に慣れ親しみ、報告用のテンプレートや書式を更新し、そして更新された要件に対応するための計画立案と実行を支援します。移行期間の終了後は PCI DSS v3.2.1 は引退し v4.0 のみが有効となります。

PCI DSS V3.2.1 と v4.0 の双方が有効である 18 か月間に加えて、v4.0 の新要件の中には計画導入のために `future-dated（未来日付）`として臨時の追加対応期間が設定される要件があるでしょう。

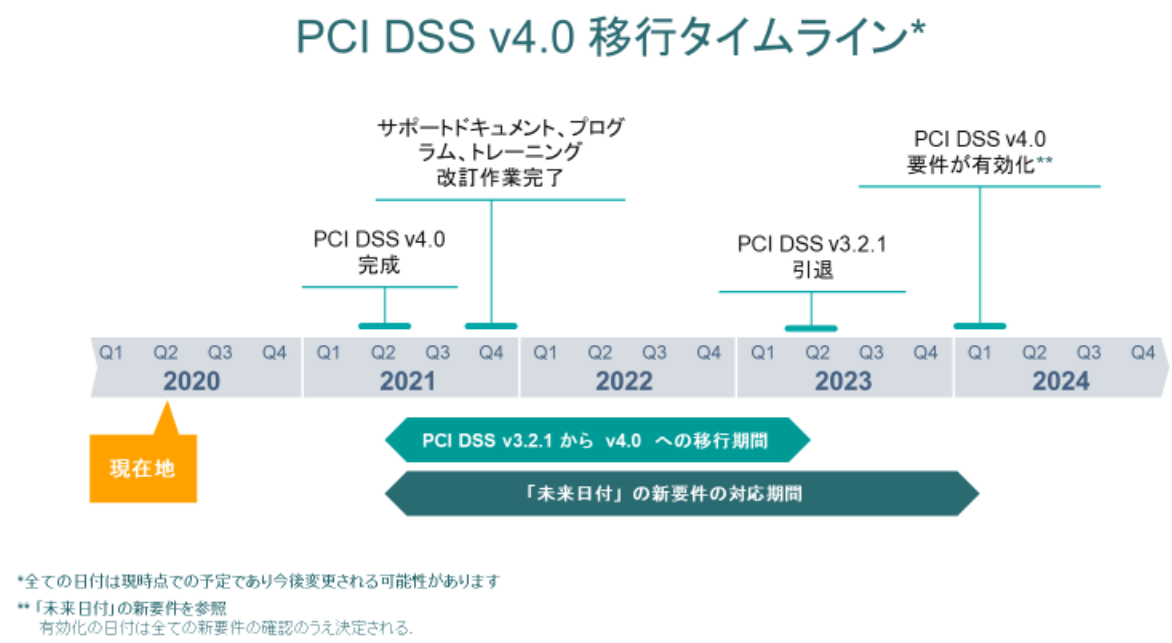
`future-dated（未来日付）`の要件とは何ですか？　そしていつ有効になりますか？

Lauren Holloway： PCI DSS において、新要件では実行するための追加的な時間を組織に提示するため「未来日付」を設定されることがあります。「未来日付」を設定された要件はその期日が来るまではベストプラクティスとして見做されます。この間、組織は「未来日付」の要件のバリデーションを求められません。その一方で、組織が当該新要件を満たすためにコントロールを実行した「未来日付」に先行して評価される準備が整っていることを推奨します。指定された「未来日付」を迎えた時点でそれらの要件は有効になり適用可能となります。

PCI DSS v4.0 ではいくつかの新要件に「未来日付」が設定されることが想定されます。しかし、幾つの新要件に「未来日付」が設定されるかは基準が完成するまでは確定しません。

これらの新要件に対し有効な「未来日付」が設定されるかは PCI DSS v4.0 の発表準備が整うまで確認できませんが、組織がすべての新要件に対応するための計画、そしてセキュリティコントロールの実行と必要な手続きのために十分な時間が提示されるでしょう。「未来日付」は基準に盛り込まれる新要件のもたらす全体的な影響の度合いに依存します。現在のドラフトのもとで計画されている移行期間を超えた「未来日付」は PCI DSS v4.0 発表後 2 年半～3 年の期間設定が想定されます。

計画された移行期間のタイムラインと「未来日付」が設定された新要件に対する可能性のあるタイムラインは下図の通りです。



詳細（英語のみ）：How Industry Feedback is Shaping the Future of PCI DSS

PCI DSS v4.0 完成前にそのドラフトは発表されますか？

Lauren Holloway： 基準のドラフトはレビューと意見提示のために PCI SSC のステークホルダーに共有されます。次回のドラフトは QSA, ASV そして Participating Organization（PO-参加団体）に対し、本年 9 月～10 月に次回の RFC の期間中にそのレビューと意見提示のために提示されます。

次回の RFC および RFC のプロセスについてのさらなる詳細は RFC Page. をご覧ください。

私は次回の PCI DSS v4.0 RFC に参加したいのですが、どのようにしたら良いですか？

Lauren Holloway： いかなる組織も Participating Organization（PO-参加団体）に参加することができます。PCI 基準ドラフトに対する意見提示に加え、PO の特典は Special Interest Groups （SIG）へ提案、投票と参加、年次の各コミュニティ・ミーティングへの無料参加、そして貴社の顧客や提携先にペイメントセキュリティに対するコミットメントを表明することができます。PO のすべての特典の詳細については how to become a PO here. をご参照ください。

PCI DSS v4.0 への準備のために組織は何ができますか？

Lauren Holloway： PCI DSS v4.0 が策定途上にある一方、PCI SSC はすべての組織に PCI DSS v3.2.1 で規定されたセキュリティコントロールを念入りに維持するように推奨します。 これは継続的なセキュリティを確保するだけでなく、PCI DSS v4.0 への移行も容易になります。

初期の PCIDSS ドラフトにアクセスされた組織はそれらの新／更新要件を実行しようとせず PCI DSS v4.0 最終版が発表されるまで待機するように強く促します。RFC はあくまでドラフトであり最終版では内容が異なります。

2020 年 5 月