2020年 ペイメントセキュリティのニーズに応えて

ペイメントカード・セキュリティフォーラム2020

2020年11月13日

井原　亮二
アソシエイト・ディレクター　- 日本
PCI セキュリティ スタンダード カウンシル

PCI Security Standards Council

PCI DSS v4.0の状況

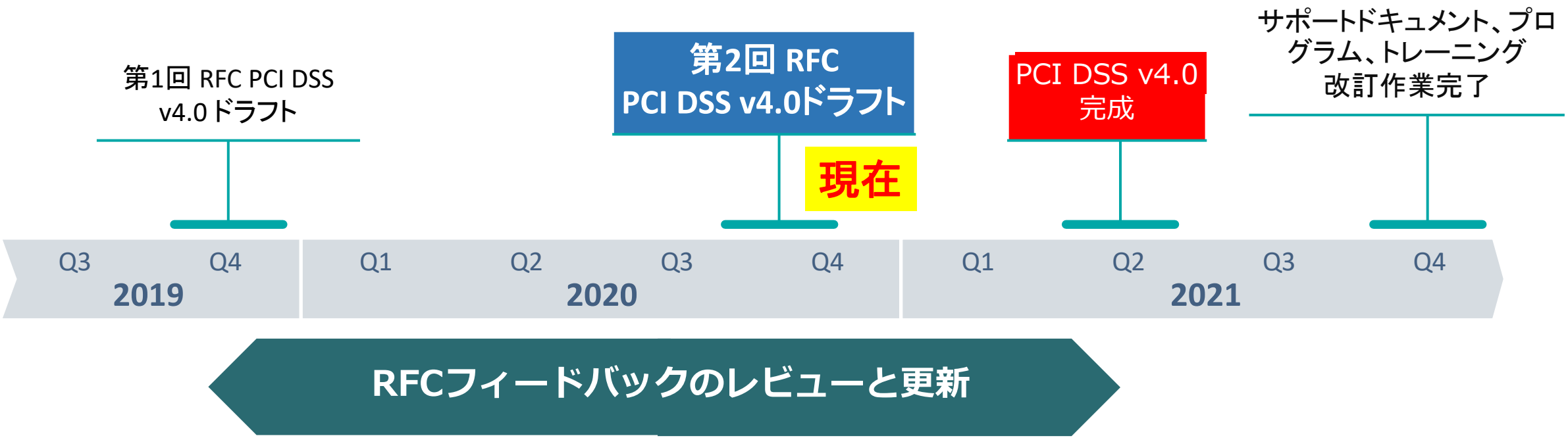
作業は進行中: PCI DSS v4.0

主な作業ステップ

- 前回RFC フィードバックの分析
- 第2回目RFC
- 評価者トレーニングとプログラム要件
- PCI DSS v4.0の完成
- サポートドキュメントの更新

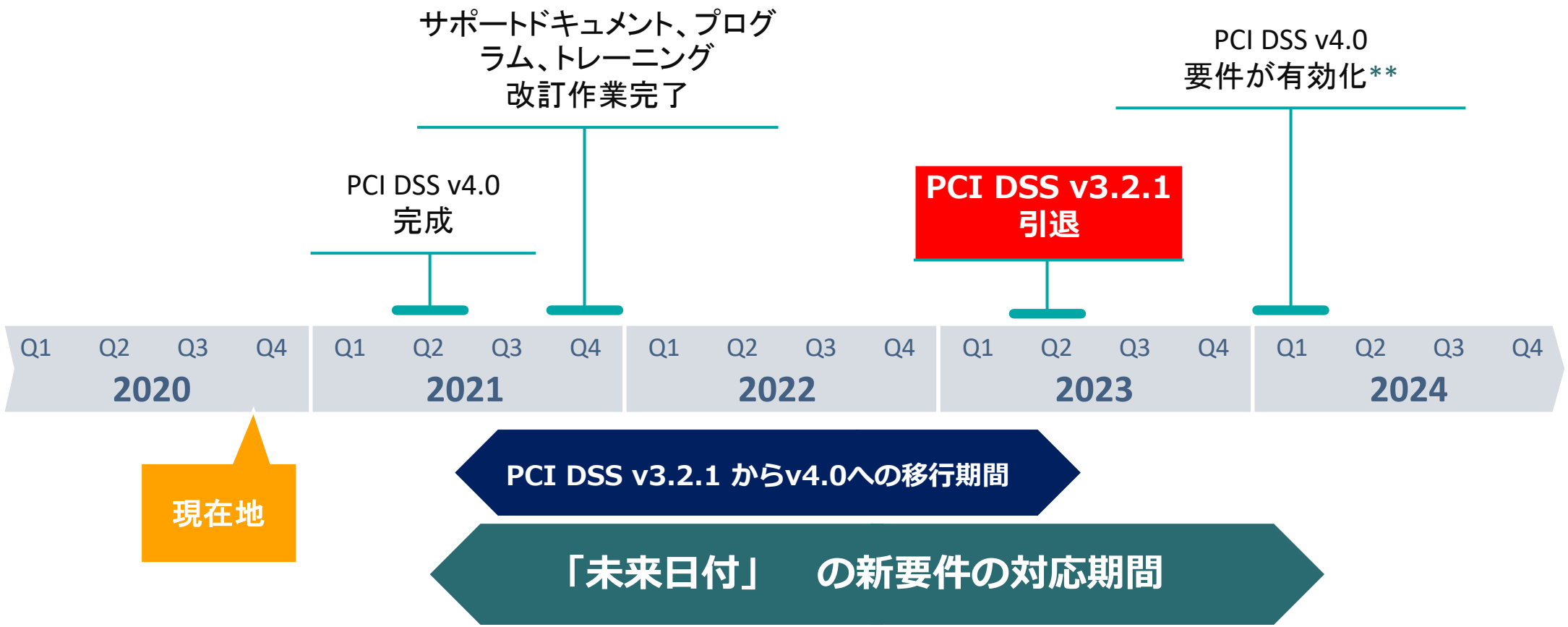
PCI Security Standards Council

PCI DSS v4.0 策定タイムフレーム*



* 全ての日付は現時点での予定であり今後変更される可能性があります

PCI DSS v4.0 移行タイムライン*



*全ての日付は現時点での予定であり今後変更される可能性があります

** 「未来日付」の新要件を参照
有効化の日付は全ての新要件の確認のうえ決定されます.

業界からのフィードバックが PCI DSS v4.0を形づくる

フィードバックの機会
Request for Comments (RFCs)

- PCI SSCはPCI基準およびプログラムの策定に際し、世界中のペイメント業界関係者から質の高いフィードバックを受けます
- 策定プロセスのなかでステークホルダーがインプットを提示します
- あくまでドラフトであり最終版ではありません

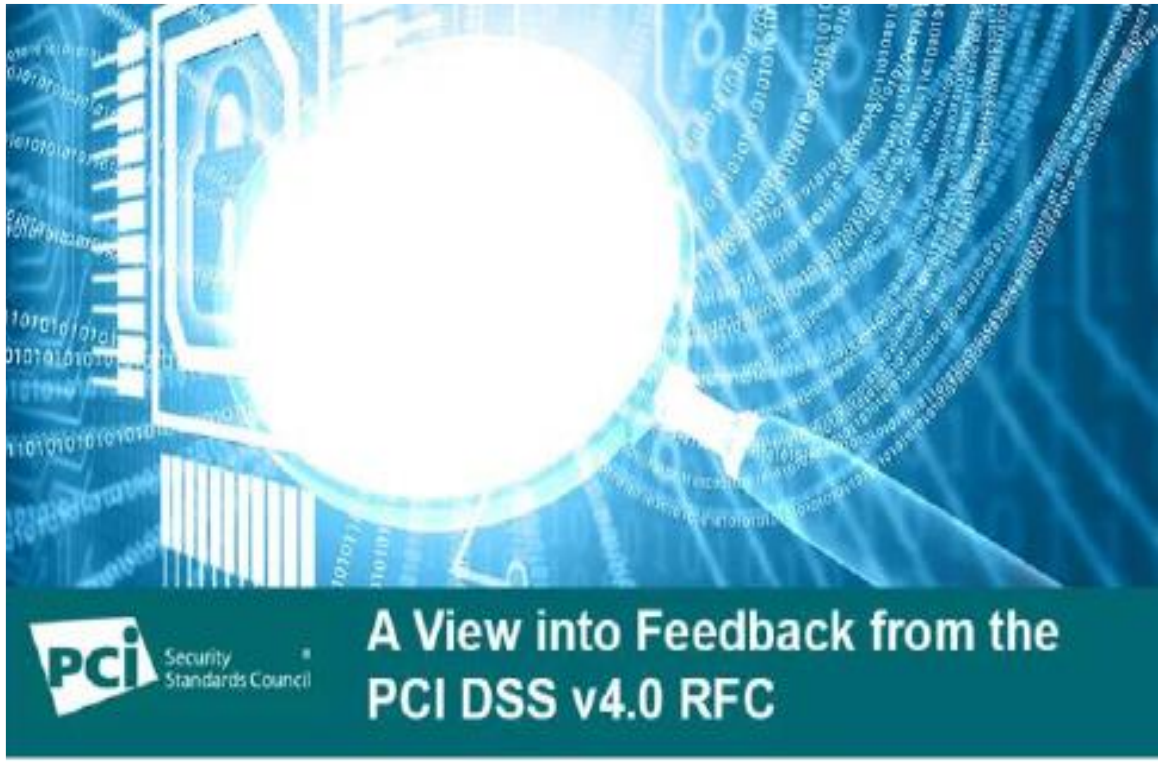
PCI Security Standards Council

提示されたインプットはどうなる？

- PCI SSC はRFCを通じ提示されたすべてのコメントについて基準の策定作業のなかでレビューします
- フィードバック・サマリは参加者と共有されます

2019 RFCからの主なフィードバック

- カード会員データの全ての伝送の保護
- パスワード長、変更履歴、 変更頻度など業界ガイダンスとの調和
- 新規パスワードを既知、不良パスワードリストと比較
- 認証ファクターの成功・失敗を示す前段階で全ての多要素認証ファクターの確認
- アプリケーション/システムアカウント用にセキュアな認証
- 年次のリスクアセスメント
- データ検知と流出防止のための手法



PCI Security Standards Council

フィードバックに対応する場合の考慮

- この要件のセキュリティ価値とは何か？
- 要件の意味合いや意図は明確か？
- この要件は全てのタイプの環境とステークホルダーに適合するか？
- 要件に適合するためにより柔軟な手法を提供できるか？

PCI Security Standards Council

新しい カスタマイズド アプローチ

PCI DSS 要件を準拠確認するための新しいオプション

- **異なるセキュリティ手法やテクノロジーを使う組織により柔軟性を提供**
- **このテーマに多くのフィードバックが寄せられた**
- **追加的なガイダンスが策定され第2回目のRFCで提示**

PCI Security Standards Council

フィードバックがPCIDSSv4.0を形づくる

PCIDSSで適用される情報について明確化

- **「アカウントデータ」の定義**
- **PANの「存在」/「不存在」と適用性**

PCI DSS と PCI ソフトウェアスタンダードに関する新たなセクション

- **PCI評価済みソフトウェアおよびソフトウェアベンダーがどのようにPCIDSS基準（要件６）の準拠に役立つかについての記述**

フィードバックがPCIDSSv4.0を形づくる

PCIDSS要件のスコープ

第2回目RFCドラフトに含まれるもの:

- クラウドとソフトウェア設定管理ツールの適合性
- スコープとネットワークセグメンテーションへの考慮
- 暗号化されたアカウントデータのスコープと適合性
- サードパーティーサービスプロバイダーを活用する場合の更なる考慮

サンプリング

- 評価者用の追加ガイダンス

フィードバックがPCIDSSv4.0を形づくる

タイムフレームに対する新たな表記

- PCIDSS要件における「毎日」「毎月」「四半期毎」の意味
- 「定期的」「速やか」「重大な変更」など用語の定義
- カスタマイズドアプローチにける“意図”を“目的”に変更
- 新しい Appendix B

PCI SSC
新型コロナウィルス
(COVID-19)対応

PCI SSC COVID-19 特設サイト

https://ja.pcisecuritystandards.org/index.php

COVID-19コロナウィルス関連の情報は専用の特設サイトに掲載

PTS POI 期限延長

・　COVID-19に関係するサプライチェーンの行き詰まりに対応するため、PCI SSCは　PCI PIN Transaction Security Point-of-Interaction (PTS POI) v3.0 デバイスの導入期限を　2020年4月30日から2021年4月30日に変更しました

PCI PINセキュリティ要件（18-3）の実施期日延長

・　PCI SSCは PINセキュリティ要件（18-3）のKey Block の実施期日を見直し延期しました

・　この変更は即時有効となっています、この変更は年内に発行されPCIPINセキュリティ要件およびテスト手順v3.1で反映されます

・　改訂後の期日の詳細等は下記サイトからブリテンをご覧ください

https://www.pcisecuritystandards.org/pdfs/Key%20Block%20Implementation%20Revision%20Bulletin%20FINAL.pdf

PCI Security Standards Council

COVID-19 の P2PE 評価への影響

・PCI SSCはCOVID-19問題がP2PEソリューション、コンポーネント、アプリケーション年次リバリデーションの実施を困難にしている状況を認識しています

・　P2PEプロダクトについて年次のリバリデーションの期限延長について2020年10月31日まで延期しておりましたが、今回これをさらに2021年6月末ま再延期いたします

詳細は P2PE@pcisecuritystandards.org
へメールにてご相談 ください

リモートによる評価（アセスメント）

・　COVID-19問題の結果、対面会議や移動の制限などが続いたため、PCI SSCはリモートによる評価について評価者向けに追加的なガイダンスを発行しました

・　もし、貴社がこれらに起因するコンプライアンス義務に関する課題に遭遇している場合は、契約先アクワイアラまたは国際ブランドと対応を協議してください

講師派遣によるオンサイト・トレーニングの中止とオンライン対応

・　PCI SSCは2020年末まで全世界レベルで講師派遣型オンサイト・トレーニングの中止を決定しました

・　PCI SSCは10月15日（木）にリモートオンライン方式によるISA/　QSAトレーニングコースを実施しました（日本語同時通訳付き）

https://training.pcisecuritystandards.org/qsa-training-schedule


Helping Secure
Payment
Data Globally