PA-DSS から PCI セキュアソフトウェア基準への移行を確実に行う方法

2022 年 10 月 28 日、「ペイメントアプリケーション データセキュリティ基準（PA-DSS）」プログラムは正式に終了します。このブログでは PCI SSC エマージング スタンダード、シニアマネージャー、Jake Marcinko より PA-DSS がその後継であ「PCI ソフトウェアセキュリティフレームワーク（SSF）」に属する「PCI セキュアソフトウェア基準」との比較を示し、PCI SSC サーティフィケーションプログラムのマネージャー、Tracey Harrington が主なタイムラインと移行に向けた準備の方法についてサジェスチョンを提示します。

PCI ソフトウェアセキュリティフレームワーク(SSF)と PCI セキュアソフトウェア基準とは何でしょうか？

Jake Marcinko: PCI ソフトウェアセキュリティフレームワーク(SSF)はひとつの要件アーキテクチャーの下でペイメントソフトウェアとソフトウェア開発事業者のためにソフトウェアセキュリティの原則と運用を統合し標準化したものです。SSF には 2 つの基準、PCI セキュアソフトウェアライフサイクル基準（セキュア SLC）と PCI セキュアソフトウェア基準があり、それぞれバリデーションと認定リストを管理するためのプログラムがあります。このブログではペイメントソフトウェアの安全のための主な基準として PA-DSS に置き換わる PCI セキュアソフトウェア基準に焦点を当てます。PCI セキュアソフトウェア基準は PA-DSS で最初に導入されたペイメントアプリケーションとデータを保護する鍵となる原則を拡張します。そしてより大きなソフトウェアアーキテクチャー、機能、ソフトウェア開発手法をサポートするように設計されています。

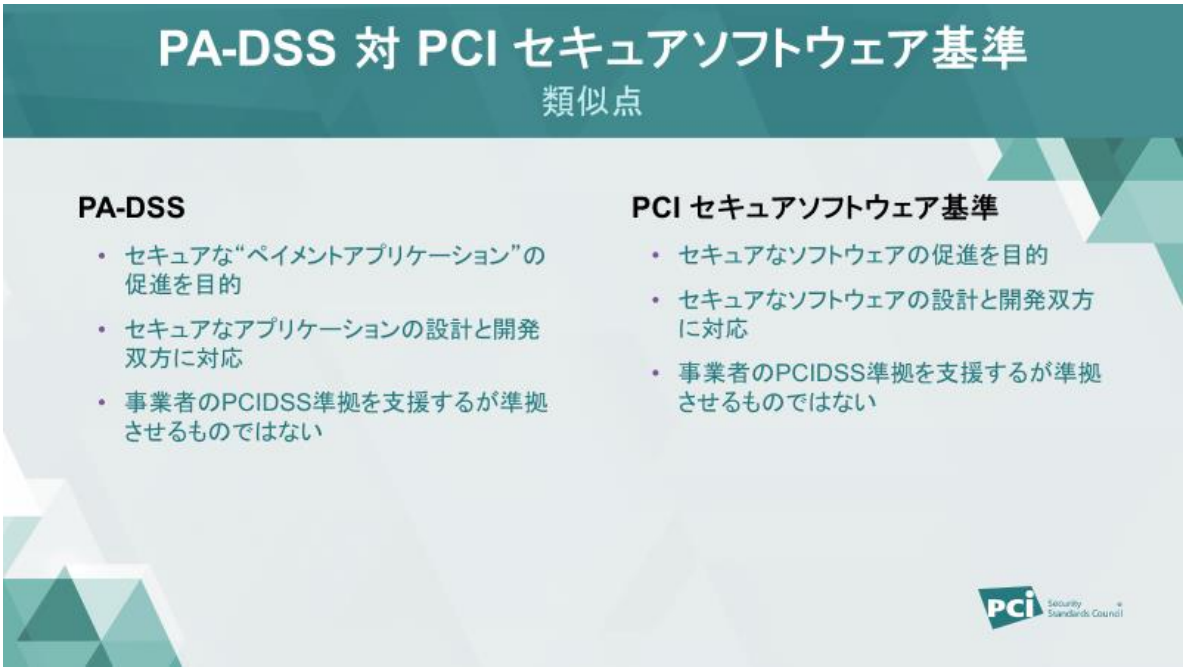
なぜ PCI セキュアソフトウェア基準は PA-DSS に置き変わるのですか？

Jake Marcinko: PCI セキュアソフトウェア基準は PA-DSS を超えるいくつかの利点を提示しています。

- 従来よりも多様なソフトウェアについて評価が可能
- 最新の開発技術やリリースサイクルに応じた敏捷性
- 全ての PCI 基準を見据えたソフトウェアセキュリティ使用における一貫性
- 暫定的なソフトウェア更新の透明性の向上
- PCI ソフトウェアセキュリティの目標達成に向けたソフトウェアベンダーの柔軟性と説明責任の向上
- ペイメントセキュリティの重要性に対するソフトウェアベンダーコミュニティへの教育の強化

PCI セキュアソフトウェア基準と関連するバリデーションプログラムでは、柔軟性が強化されたことにより、多様なソフトウェア管理、簡素化された評価プロセス、そして単純化されたリスト管理が可能になっています。PA-DSS の下ではバリデーションできなかったペイメントソフトウェアについても可能となるような拡張性を認めています。

PCI セキュアソフトウェア基準と PA-DSS の類似点とは？また相違点とは何ですか？



Jake Marcinko: PCI セキュアソフトウェア基準と PA-DSS の関係性をより良く理解するためには並べて比較するのが分かりやすくなります。この表はこの 2 つの類似点と相違点を説明するのに役立ちます。要件について 1 対 1 の関係でクリアに対応されていないことに注意が必要です。双方のプログラムはセキュアなペイメントアプリケーションとソフトウェアの開発を促進し、そしてセキュアなアプリケーションの設計と開発に取り組むことを目的としています。

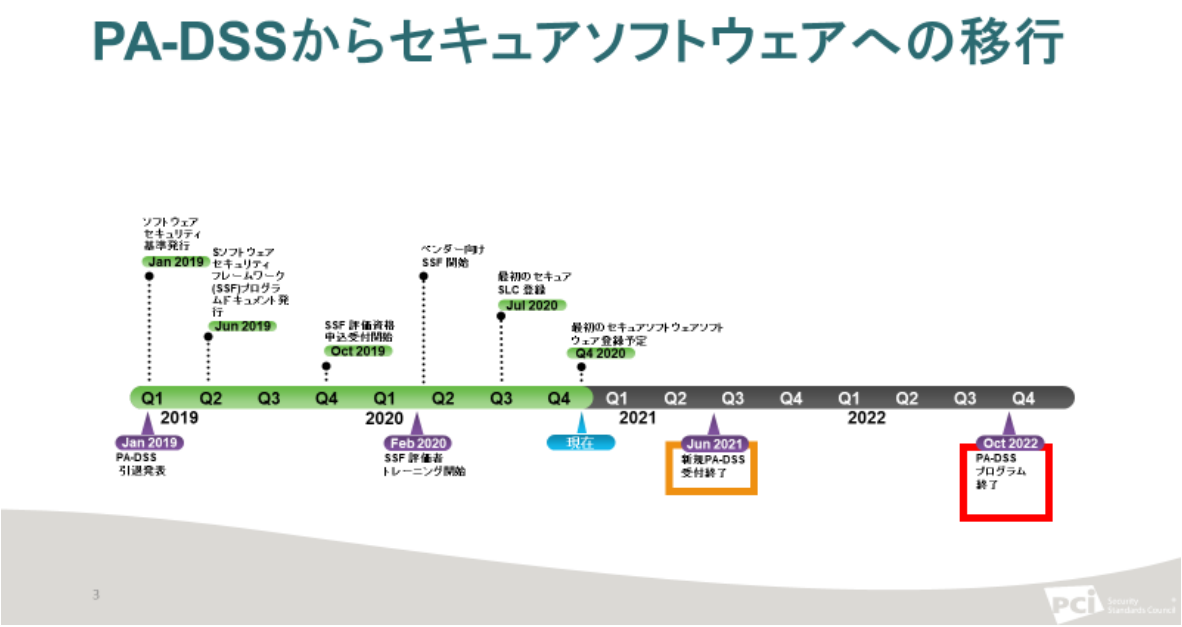
PCI セキュアソフトウェア基準と PA-DSS が相違する項目の中に“モジュール”要件の採用があります。“モジュール”は特殊なケースに対処する要件のグループです。PCI セキュアソフトウェア基準には現在２つの“モジュール”が存在します。それは”全てのペイメントソフトウェアに適用される一般要件を含む“Core モジュール”そして平文のアカウントデータの保管、処理または伝送するペイメントソフトウェアに追加的なセキュリティ要件を含む“Account Data Protection モジュール“があります。 2020 年 12 月に 3 つ目のモジュール“Terminal Software モジュール”の導入が計画されています。そして将来的には追加的なモジュールが予定されています。PCI セキュアソフトウェア基準のモジュールの本来的な特性により全ての要件が全てのソフトウェアに適用されるものではなありません。

PCI セキュアソフトウェア基準と PA-DSS の２つのプログラム上の主な相違点は何ですか？

Jake Marcinko: 全体的に PCI セキュアソフトウェアプログラムは PA-DSS よりダイナミックであり、基準および補助的なドキュメントの頻繁な更新・変更に備えられます。モジュ

ールの追加に応じ「プログラムガイド」「評価者資格要件」そして補助的なドキュメントはこれらの追加を取り込むために必要に応じレビュー更新されることになります。

PCI セキュアソフトウェア基準と PA-DSS のもう 1 点の主要な相違は、ベンダーが PCI セキュア SLC 基準 に参加し、彼らの認定されたペイメントソフトウェアの維持のために追加的な柔軟性の機会が得られることです。より詳細な情報は最新のブログ「PCI セキュア SLC 基準 の価値」に掲載されています。(blog).



PA-DSS から PCI セキュアソフトウェア基準への移行タイムラインはどのようになっていますか？

Tracey Harrington: 移行タイムラインの中で、注意すべき次の重要な日付は 2021 年 6 月と 2022 年 10 月になります。PA-DSS 認定評価のための新規のペイメントアプリケーションの提出は 2021 年 6 月 30 日までとなります。すでに PA-DSS 認定されている既存のアプリケーションはプログラムが終了する 2022 年 10 月 28 日まで認定済みペイメントアプリケーションリストに残されベンダーは通常通り継続して変更を提出できます。この日付以降は全ての PA-DSS 認定アプリケーションは“既存導入済みのみ適用可能”リストに移動することにります。

PCI SSC ステークホルダーはどにようにこの移行に備えたらよいでしょうか？

Tracey Harrington: まずは全てのステークホルダーが PCI セキュアソフトウェア基準と PCI ソフトウェアセキュリティフレームワーク(SSF)全体について理解・学習することが重要な第一歩になります。PCI SSC は 現在、情報提供トレーニングへの参加を提案して

います。(informational training) このトレーニングはこのプログラムの評価者として資格取得ではなく、PCI セキュアソフトウェア基準からもたらされるものを理解したい方、評価から期待できることなどを理解したい方に適合しています。

ベンダーとしてこの移行に向けどのように準備したらよいでしょうか？

Tracey Harrington: ベンダーにとっての第一歩は PA-DSS 用にリストされているアプリケーションについて PA-DSS と PCI セキュアソフトウェア基準のギャップ分析を実施することになります。

評価者はこの移行にどのように備えたらよいでしょうか？

Tracey Harrington: 2022 年 10 月に終了する際に、それを支援する PA-QSA 資格プログラムも引退します。PCI セキュアソフトウェア基準のバリデーションに興味がある既存の PA-QSA はセキュアソフトウェア評価者(Secure Software Assessors) オンライントレーニングへの参加が可能となります。QSA および新規評価者向けリモートによる講師トレーニングと資格テストが予定されます。セキュアソフトウェア評価者に興味がある個人はまずは「資格要件」を確認し、要件への不足がある場合それを補うための時間を確保することを推奨します。

この移行を支援するためのリソースはありますか？

Tracey Harrington: PCI SSC ウエブサイト(Document Library) には SSF 用の全ての基準書とプログラムドキュメント用リソースへのアクセスがあります。PCI SSC ブログ（PCI SSC blogs) は SSF やその他のトピックだけでなく PCI セキュアソフトウェア基準に関する最新情報を得るための手段になります。興味がある個人は最新の更新情報をメールを通じ受け取るよう購読することができます。さらに移行準備が完了したベンダーは PCI ソフトウェアセキュリティフレームワーク評価者（PCI Software Security Framework Assessors）のオンラインリストを参照することができます。