情 報 種 別: 秘密（関係者限り）
会 社 名 ： NTTデータ先端技術株式会社
情報所有者: セキュリティ事業本部 セキュリティコンサルティング事業部

あなたとともに、変わる世界をかえていく

NTTデータ 先端技術株式会社

ペイメントカードセキュリティフォーラム

講演資料

PCI SSC の最新ソフトウェアセキュリティ基準のご紹介（アップデート版）

2020年11月13日

2 NTTデータ先端技術株式会社のご紹介

社　名　エヌ・ティ・ティ・データ先端技術株式会社
（NTT DATA INTELLILINK CORPORATION）
代表者　　代表取締役社長　木谷　強
設　立　　平成11年8月3日
株　主　　株式会社エヌ・ティ・ティ・データ（100%）
連結社員数 1361名（2020年4月1日現在）

事業内容【セキュリティ事業本部】
1）情報セキュリティに関するトータルソリューションの提供
2）企業情報システムのセキュリティコンサルティング
　サービスの提供
3）セキュリティ診断・不正アクセス監視・セキュアSI等の
　サービス提供
4）セキュリティ教育に関する各種サービスの提供

保有資格
1）QSA（PCI DSS認定セキュリティ評価機関）
2）PA-QSA（PA-DSS認定セキュリティ評価機関）
3）QSA（P2PE）（P2PE認定セキュリティ評価機関）
4）PA-QSA（P2PE）（P2PEアプリケーション認定セ
　キュリティ評価機関）
5）3DS Assessor（3DS評価機関）
6）QPA（認定PIN評価機関）
7）ASV（脆弱性スキャニングベンダー）

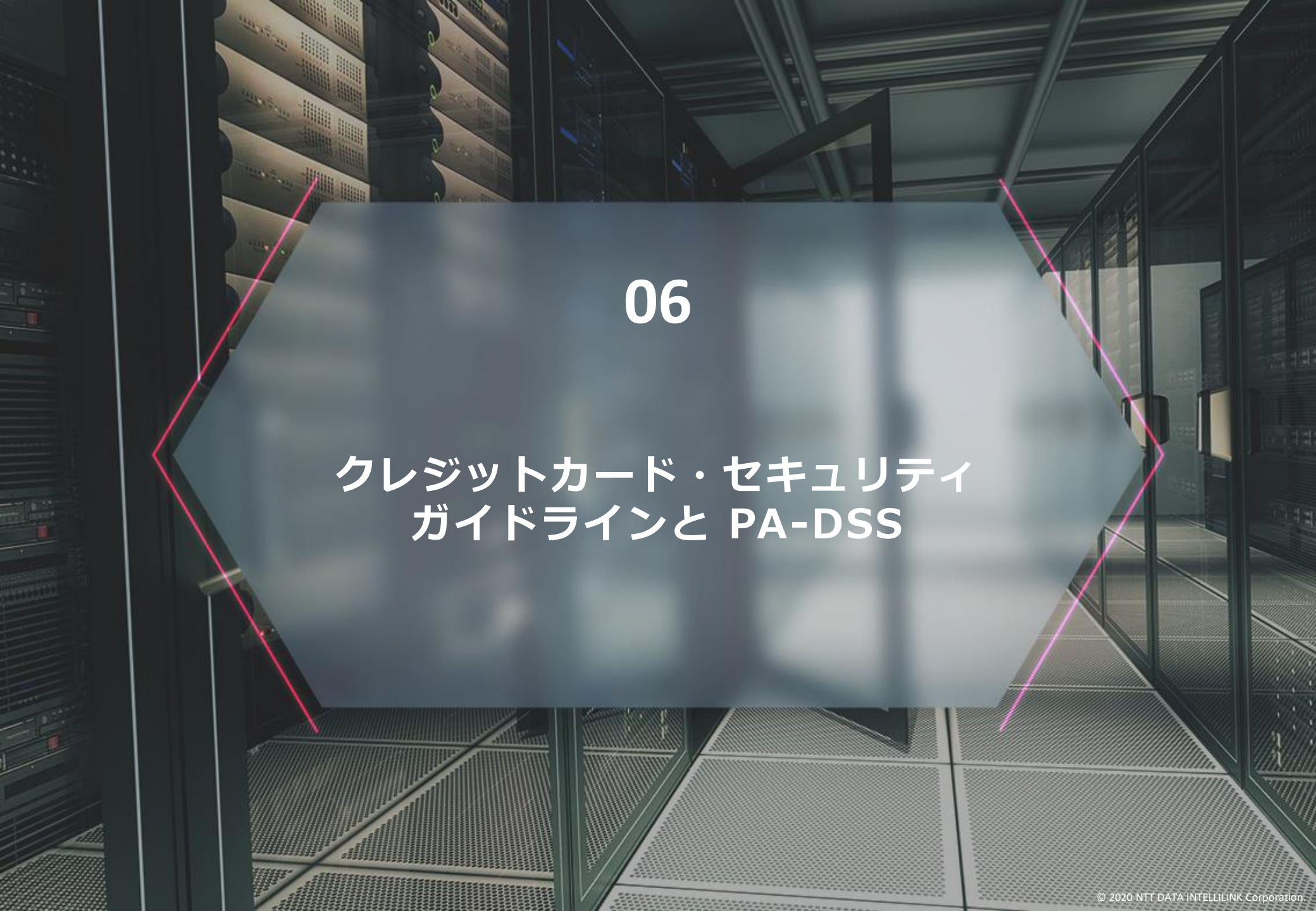
アジェンダ

2019年1月にPCI SSCより、PA-DSSの後継となる新たなソフトウェアセキュリティ基準として、Software Security Framework（SSF）がリリースされました。SSFについては2019年3月の本フォーラムでも紹介させていただきましたが、その後、プログラムガイドのリリースや PA-DSS からの移行についてのアナウンスなどがありました。また日本国内では、PA-DSSはクレジットカード・セキュリティガイドラインにおける「非保持と同等相当」でも参照されており、その後継となる SSF が注目されます。
本講演では2019年の講演のアップデート版として、プログラムガイドなどの前回の講演の後に公開された内容を中心に、PA-DSS審査員（PA-QSA）が SSF の概要をご紹介します。

1. クレジットカード・セキュリティガイドラインと PA-DSS
2. PCI Software Security Framework の概要
3. Software Security Framework の認定プログラム
4. Secure Software Standard プログラム
5. Secure SLC Standard プログラム
6. Secure Software Standard の概要
7. Secure SLC Standard の概要
8. まとめ

前回の講演後に公開された内容のご紹介

前回、詳しくご紹介したので今回はあっさりめに

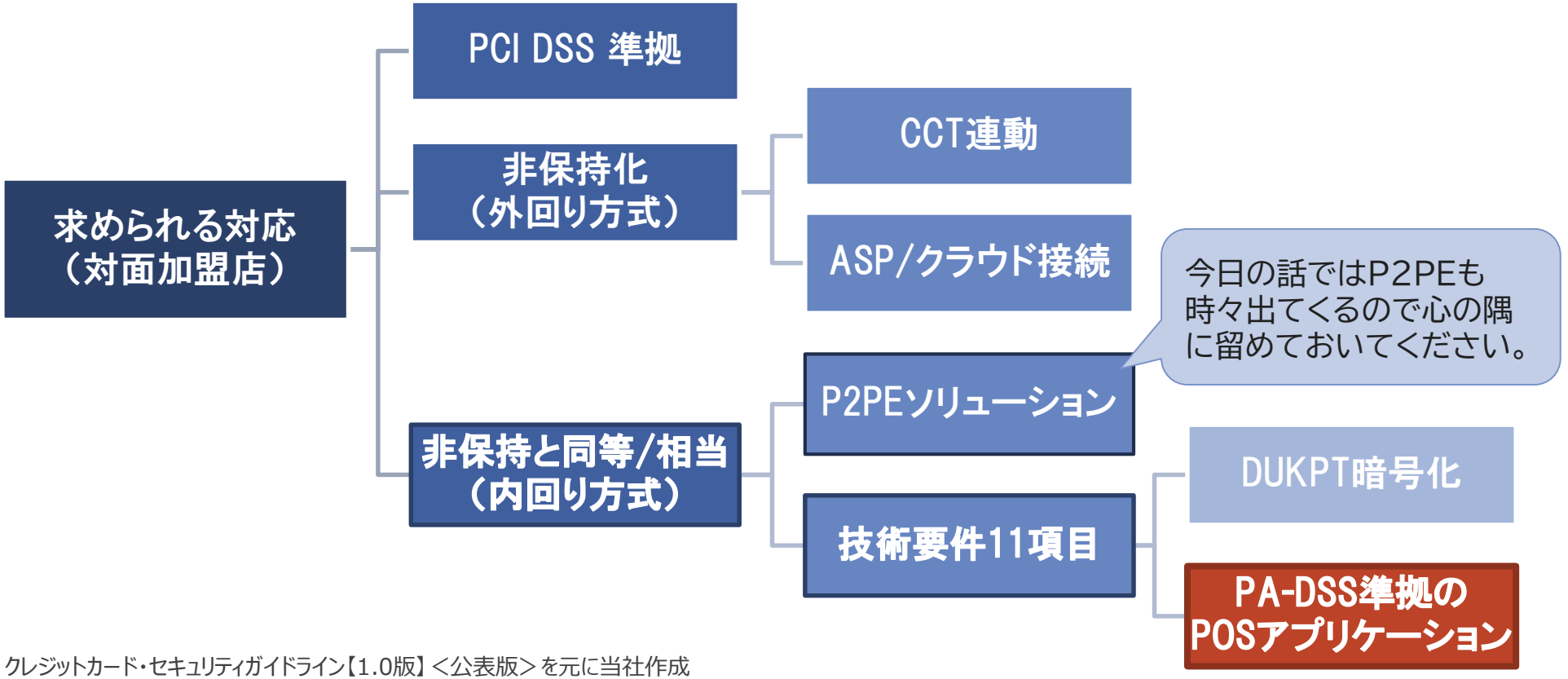


06

クレジットカード・セキュリティ ガイドラインと PA-DSS

7 クレジットカード・セキュリティガイドラインと PA-DSS

改正割賦販売法（2018年6月施行）において、クレジットカード情報を取り扱う事業体に対して求められる情報管理・保護の義務を履行する際の実務上の指針であった「クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画」の実施期限2020年3月以降も、クレジットカード取引の関係事業者が実施するべきセキュリティ対策を取りまとめたものが、クレジットカード・セキュリティガイドラインです。ガイドラインにおいて対面加盟店に求められている対応の中で、非保持と同等/相当を実現するための対策の一つとして、**PA-DSS 準拠の POS アプリケーション実装**があります。



出所：クレジットカード・セキュリティガイドライン【1.0版】＜公表版＞を元に当社作成

PA-DSSプログラムの終了と後継基準 Software Security Framework

- PA-DSS は最新の v3.2 が終息する 2022/10/28 をもってプログラム自体が終了
  - 新規の PA-DSS 認定申請の受付は 2021/6/30 まで
  - 既存の PA-DSS 認定アプリケーションは 2022/10/28 までは現在と同じ扱いで、プログラム終了までは変更申請が可能
  - 2022/10/28 以降は、全ての PA-DSS 認定アプリケーションが「既存の導入済みのみ認められる」のステータスとなる（新規の導入が認められなくなる）

- PA-DSS の後継基準として策定されたのが PCI Software Security Framework（SSF）
  - SSF の認定プログラムは、ソフトウェア・ベンダの認定、および審査員の認定のいずれも開始されている
  - PA-DSSの終了までは、SSFとPA-DSSの平行期間となる
  - PA-QSA（PA-DSSの審査員資格）は、P2PEアプリケーションの審査員資格であるPA-QSA（P2PE）取得の前提資格となっているが、現時点でこの点に関する移行/変更のアナウンスはない
    ※将来的には P2PEアプリケーションと SSF が関連するかも？

- クレジットカード・セキュリティガイドラインにおける対応
  - 2020/3に公開された1.0版では PA-DSS の終息について特に触れられていないが、PA-DSSが終息する2022/10までには何らかの更改がされることが期待される

010

PCI Software Security Framework の概要

11 PCI Software Security Framework の概要

策定の背景

- PA-DSSは2008年の策定。POSのような昔ながらの決済アプリのみを対象にデザイン
- 近年の業界動向を反映し、新しい開発手法(Agile/DevOps)や技術を利用した決済アプリも含めて対象とする基準およびプログラムとして新たに策定(クラウドのようなサービスとして提供されるソフトウェアを含む)

二つの基準で構成

- PCI Secure Software Standard：認定対象はソフトウェア。PA-DSSの直接の後継。
  ※公式な略称がないのですが、長いので本資料内では SSS と略記する場合があります。
- PCI Secure Software Lifecycle (Secure SLC) Standard:認定対象は開発ベンダ。取得は任意。
- いずれも認定を受けると、PCI SSC の Web サイトに掲載される
  ※2020/11/10時点で Secure SLC 認定を受けたベンダが一つ、SSS認定を受けたソフトウェアはないようです。

Objective-based Approach

- 要件(Requirements)からコントロール目標(Control Objectives)へ
- There is no “one size fits all” method to software security.
  (全てに対応できる万能のソフトウェアセキュリティ手法はない)
- SSF のコントロール目標では、特定のレベル、厳密さ、頻度などは、ほぼ定められていない
  (暗号鍵強度や、「少なくとも年次」での実施を求める要件がいくつかあるのみ)
- ベンダは強固なリスクアセスメントプロセスをBAUの一部として保持しなくてはならない
  - 厳密さや頻度は、リスクアセスメントの結果に基づいてベンダが決定
  - ベンダは、その有効性と要件を満たすことを示せなくてはならない

出所:PCI SSC 公式ブログ (https://blog.pcisecuritystandards.org/topic/software-security-framework)
PCI Secure Software Standard v1.0, PCI Secure SLC Standard v1.0
(https://www.pcisecuritystandards.org/document_libraryからダウンロード可能)

12 他の PCI 基準との関係

PA-DSS との関係

- SSF は PA-DSS とは分離、独立した基準
- PCI DSS 環境で利用される決済アプリケーションに特化して設計された PA-DSS に対して、より広い範囲の決済ソフトウェアの種類、技術、開発手法、および将来の技術・ユースケースをサポートするよう設計
- 最終的には PA-DSS およびその認定プログラムは Software Security Framework に統合される（現在は移行期間）

PCI DSS との関係

- PA-DSS 認定アプリケーションと同様に、Software Security Framework で認定されたソフトウェアは PCI DSS 準拠の助けになるが、利用するだけで PCI DSS 準拠となる訳ではない
- 事業体は PCI DSS の評価の中で、ソフトウェアが適切に設定され、適用対象となる PCI DSS 要件を満たしていることを示さなければならない

その他の PCI 基準との関係

- Software Security Framework の下での認定（ソフトウェアに対する validation、ベンダに対する qualification）は、他のいずれの PCI 基準に対する認定も意味しない（現時点では分離、独立した基準）
- ただし将来的に、他の PCI 基準とプログラムの一部が Software Security Framework に統合されるかもしれないことがアナウンスされている

※国内では、P2PEのアプリケーションを対象とするドメイン2が統合された場合、インパクトが大きいかもしれません。

出所：FAQs for PCI Software Security Framework v2.0

Terminal Software Module と Secure Software Standard v1.1

- Secure Software Standard の新たなモジュールとなる Terminal Software Module の RFC が 2020/5/1-6/22 に実施された
- 決済端末上で動作する決済ソフトウェアを対象とするモジュール
- このモジュールを含む Secure Software Standard v1.1 が2020年下期にリリース予定

※NDAがあるので、中身についてはお話しできません

※(私見ですが) P2PE のドメイン 2 (P2PE アプリケーションを対象とするドメイン)を SSF に統合する準備かも？

出所:PCI SSC 公式ブログ Request for Comments: Secure Software Standard Update: Draft Terminal Software Module
(https://blog.pcisecuritystandards.org/request-for-comments-secure-software-standard-update-draft-terminal-software-module)

014

Software Security Framework の認定プログラム

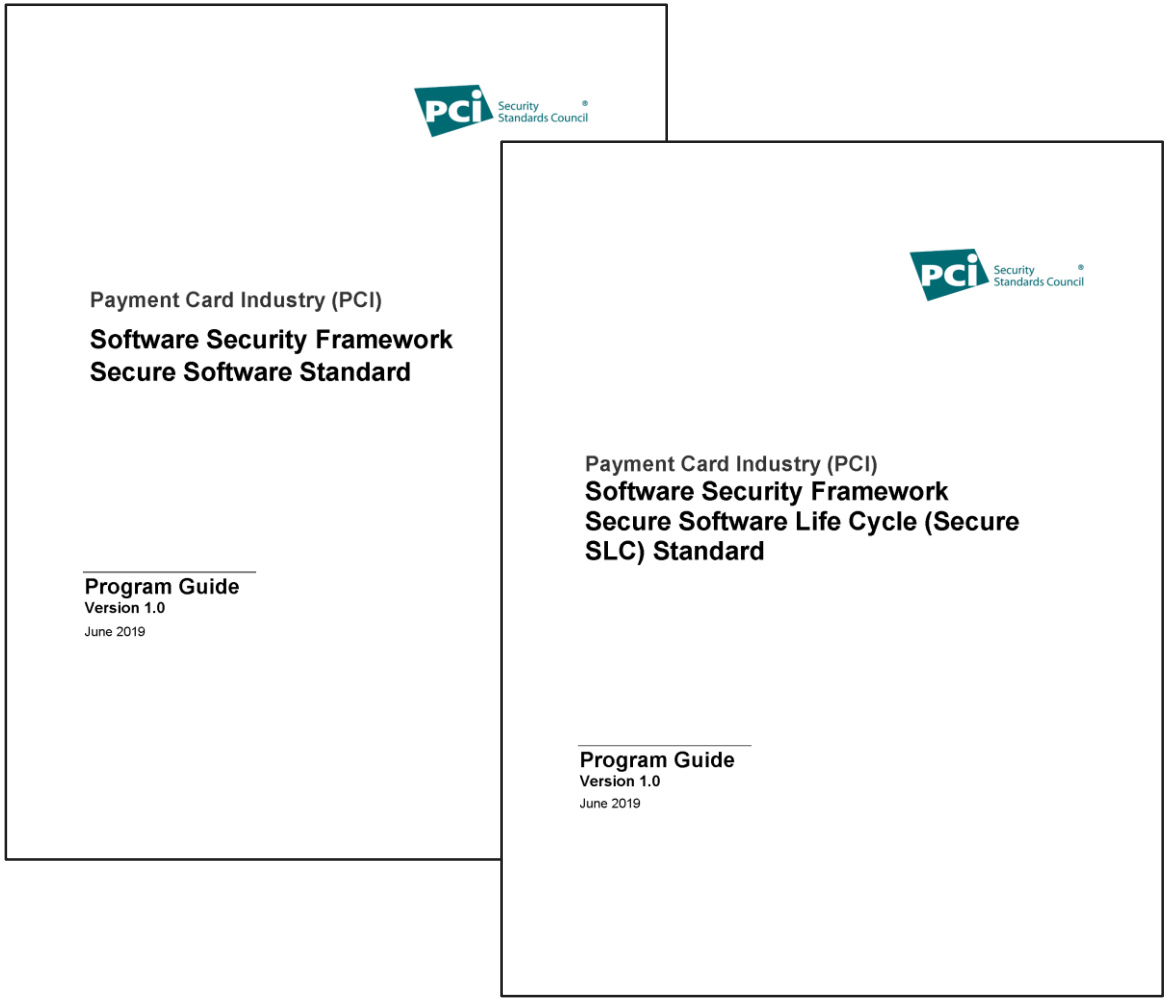
プログラムガイド

Secure Software Standard, Secure SLC Standard の認定プログラムを定めた文書

- プレイヤーとその役割
- 審査･認定プロセスの概要
- 認定の維持、登録変更管理
- レポート受付プロセス

更にSSSの場合：

- 認定対象となるソフトウェア
- バージョニング

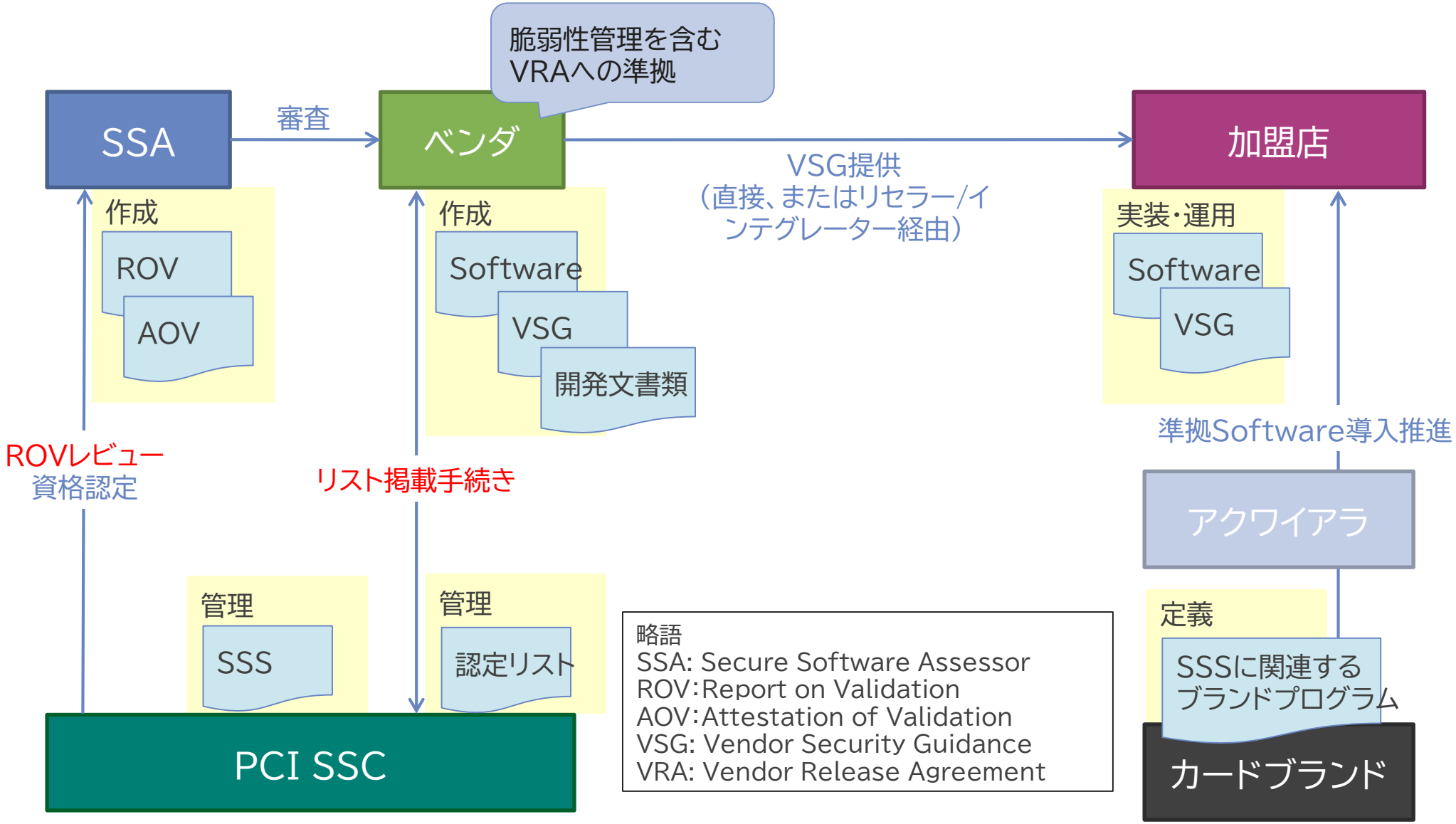


出所：https://www.pcisecuritystandards.org/document_library（Filter by: で SOFTWARE SECURITY を選択）

016

Secure Software Standard プログラム

17 Secure Software Standard のプレイヤーとその役割



Secure Software Standard 認定の維持：年次検証（ソフトウェアの変更がない場合）

年次再検証の依頼

- 次の年次検証日はPCI SSC リストに記載
- 90日前にアプリケーションベンダーコンタクトへ PCI SSC から年次再検証実施の依頼

自己検証（AOV署名）

- ソフトウェアが引き続きSSS要件を満たしていること
- 変更が認定ソフトウェアのバージョニング方法論と矛盾なく実施されていること
- ウェブサイト登録情報に対して反映が必要となる変更が PCI SSC に通知されること

AOVレビュー

- 提出物の網羅性確認
- リストの更新
- AOVの署名およびベンダーへの返送

- 変更が発生しない場合、年次検証を継続することで、最初の認定から三年間は継続して維持される。
- 自己評価されたAOVが期日までに提出されない場合、期日に達した時点で、決済アプリケーションの認定は終了（expired）となる。

Secure Software Standard 認定の維持：ソフトウェアの変更がある場合

変更種別	内容	補足
High Impact（影響大）	機密データ、機能、リソースを扱う、または影響を及ぼす（interact with）全ての変更	PA-DSS では Low Impact と見なせた変更の多くが High Impact 扱いになると思われる
Low Impact（影響小）	任意のソフトウェアアーキテクチャ、ソースコード、コンポーネントに対する変更で、High impact に該当しないもの	No Impact が無くなったため、ソースコードに修正が入ると必ず Low Impact 以上
Administrative（管理）	アプリケーションの名称や、ベンダ会社自体の情報などの、Listing 情報に関する変更	

PA-DSS と比較して

- 変更種別 “No Impact” が無くなった
- High Impact/Low Impact の区別は簡潔になった
- Expiry Date は登録してから3年後
- 各変更種別に対する認定手続きはベンダがSecure SLC 認定ベンダかどうかで異なる

Secure Software Standard
変更種別と検証方法（Secure SLC認定ベンダでない場合）

申請種別	検証方法			頻度
	SSA 会社による評価	ベンダ自己評価・自己検証	ベンダの差分レビューによる自己評価、およびSSAによるテスト	
最初の検証/フル検証	✔			3年ごと（最初の検証の後）
High Impact（フル検証）	✔			変更の実装ごと
年次検証		✔		年次
Administrative		✔		変更の実装ごと
Low Impact（差分検証）			✔	変更の実装ごと

Secure SLC 認定ベンダでない場合は、ソースコードに修正が入ると Low Impact または High Impact になるので、SSAによる評価が必ず必要になる

※PA-DSSではワイルドカードバージョニングを使うことで No Impact の場合は評価もSSCへの申請も不要

Secure Software Standard
変更種別と検証方法（Secure SLC認定ベンダの場合）

申請種別	検証方法		頻度
	SSA 会社による評価	ベンダ自己評価･自己検証	
最初の検証/フル検証	✔		3年ごと （最初の検証の後）
High Impact （フル検証）	✔		変更の実装ごと
年次検証		✔	年次
Administrative		✔	変更の実装ごと
Low Impact （差分検証）		✔	変更の実装ごと

Secure SLC 認定ベンダであれば、Low Impact の場合は自己検証が出来る

Secure Software Standard の適用対象（イメージ）

決済アプリケーション/ソフトウェア

- 内製・社内向け
- 特定の一顧客向け
- 決済専用でない消費者向けモバイルデバイス上で動作するソフトウェア（mPOSなど）
- PTS POI デバイスなどのハードウェア端末上で動作するもの

Terminal Software Module の対象が含まれる？

Secure Software Standard の対象

左記に該当しない、複数の顧客に販売・配布される、決済トランザクションを直接サポートするか容易にするソフトウェア。ソフトウェアの配布形態には寄らない。

PAの対象でないがSSSの対象となるソフトウェアの例：

- SaaS
- 決済ソフトウェアと統合されているOS、DBなど

PA-DSS の対象

- 商用 off the shelf（COTS）
- 決済モジュール

として販売されるもの

OS/DB/Others（決済アプリケーション/ソフトウェアスイートの一部）

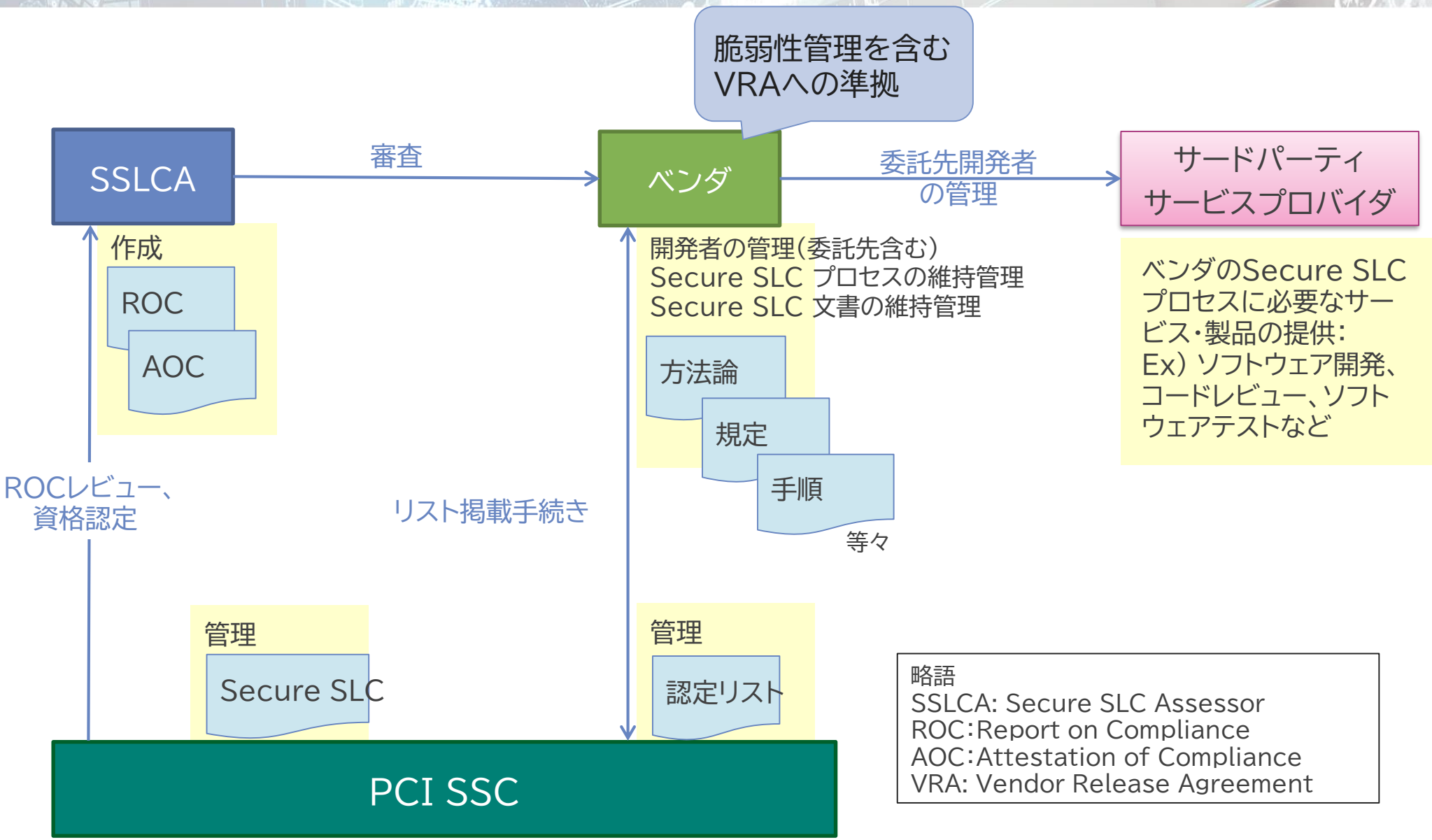
ただし将来的に適用対象が増える可能性があることが FAQ でアナウンスされています。

出所：Secure Software Standard Program Guide を元に当社作成

023

Secure SLC プログラム

Secure SLC のプレイヤーとその役割



Secure SLC 認定の維持：年次検証（変更がない場合）

年次再評価依頼

- 90日前にアプリケーションベンダーコンタクトへ PCI SSC から年次再検証の実施の依頼

中間自己評価（AOC署名）

- Secure SLC プロセスが継続して Secure SLC 要件を満たしていること
- Secure SLC プロセスへの変更がSecure SLC プログラムおよび要件への準拠に影響を与えないこと
- ウェブサイト登録情報に対して反映が必要となる変更が PCI SSC に通知されること

AOCレビュー

- 提出物の網羅性確認
- リストの更新
- AOCの署名およびベンダーへの返送

自己評価されたAOCが期日までに提出されない場合：

- 期日の14日～90日後まではオレンジ表示。この間に提示すれば、オレンジ表示は黒表示に戻る。
- 90日を過ぎてしまうと、**赤表示**。いったん赤表示になると、元に戻すにはフル審査が必要。

Secure SLC 認定の維持：変更がある場合

変更種別	内容
Designated （指定）	Secure SLC 開発における製品カテゴリ※の変更または削除
Administrative （管理）	ベンダの Secure SLC 準拠状況に影響しない変更。 例）社名などの変更、リストの「記述」欄の内容変更

- Secure SLC の変更種別は Designated, Administrative の二つだけ

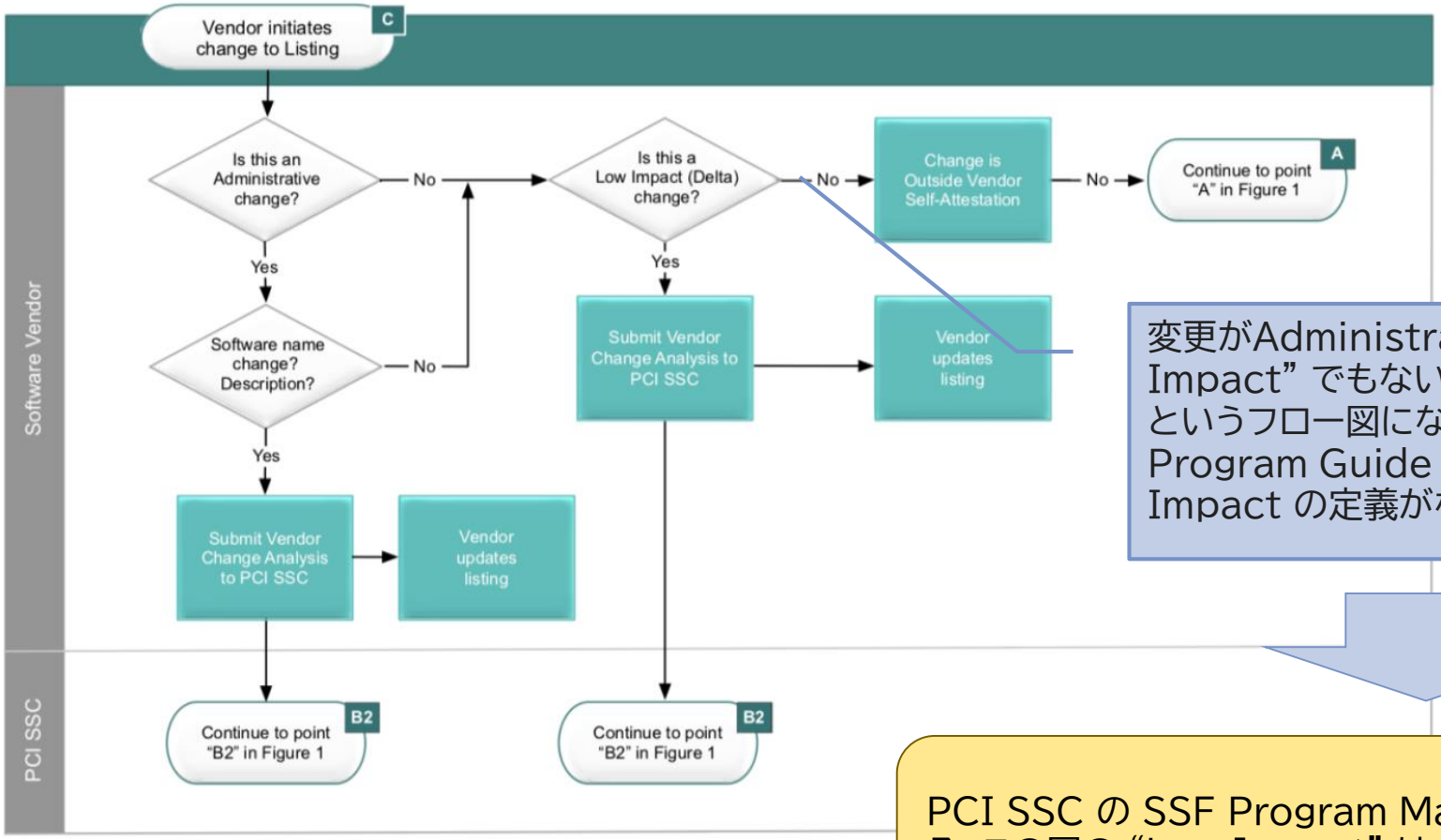
※製品カテゴリ：ベンダが開発しているアプリケーションが、どのような業態向けであるかの種別。 PA-DSSの決済アプリケーション種別（SSSでは決済ソフトウェア種別）と同じような内容の分類。詳細は Secure SLC Program Guide A.3 を参照。

Secure SLC 変更種別と検証方法

申請種別	評価方法		頻度
	SSLCA 会社による評価	ベンダ自己評価・自己検証	
最初の検証/フル検証	✔		3年ごと （最初の検証の後）
年次検証		✔	年次
Administrative		✔	変更発生時
Designated		✔	変更発生時

補足：Low Impact Change?

Figure 3: Updates to Secure SLC Qualified Vendor Listings



変更がAdministrativeでも “Low Impact” でもない時はフル審査が必要というフロー図になっているが、Program Guide のどこにも Low Impact の定義がない

PCI SSC の SSF Program Manager に尋ねたところ、この図の “Low Impact” は “Designated” の誤りとのこと

出所：Secure SLC Program Guide v1.0, p.12, Figure 3.

029

Secure Software Standard の概要

PA-DSS との比較

項目	PA-DSS v3.2	Secure Software Standard v1.0
保護対象とするデータ	アカウントデータ （カード会員データ＋機密認証データ）	機密データ（Sensitive Data） SSF の文脈では以下の通り定義される： 「承認されていない開示（機密性）および変更（完全性）からの保護が要求される任意のデータ」 例） • カード会員データ • 機密認証データ • トークン • 暗号鍵マテリアル • 認証情報 • 内部システム情報 • その他ベンダの定義する保護の必要なデータ
基とする基準	PCI DSS を基に構成 PCI DSS 要件のサブセット＋α（実装ガイド等）	PCI DSS/PA-DSS とは異なる観点（Objective-Based Approach）から新たに策定
要件モジュール	N/A	全ての対象に適用されるコア要件（Core Requirements）と 特定の対象に適用される要件モジュール（Requirement Modules）で構成 ※v1.0 ではアカウントデータを伝送、処理、保存するアプリケーションを対象とするモジュール Aのみ ※v1.1 として Terminal Software を対象とする Module の追加の計画がアナウンスされている

PA-DSS の要件と Secure Software Standard のコントロール目標

PA-DSS v3.2 要件
1 完全なトラックデータ、カード検証コードまたは値、またはPINブロックデータを保存しない
2 保存されるカード会員データを保護する
3 安全な認証機能の提供
4 ペイメントアプリケーションの動作のログ
5 安全なペイメントアプリケーションの開発
6 ワイヤレス送信の保護
7 脆弱性に対応し、ペイメントアプリケーションのアップデートを維持するために、ペイメントアプリケーションをテストする
8 安全なネットワーク実装の促進
9 カード会員データをインターネット接続のサーバに保存してはならない
10 ペイメントアプリケーションへの安全なリモートアクセスの促進
11 公共ネットワークでのセンシティブトラフィックの暗号化
12 すべてのコンソール以外の管理アクセスを安全にする
13 顧客、リセラー、インテグレータ向けの『PA-DSS実装ガイド』の維持
14 PA-DSSの責任を担当者に割り当てること、および担当者、顧客、リセラー、インテグレータ向けのトレーニングプログラムの保守

Secure Software Standard v1.0 コントロール目標	
Core Requirements	1 重要な資産の識別
	2 安全なデフォルト
	3 機密情報の保持
	4 重要な資産の保護
	5 認証とアクセス制御
	6 機密情報の保護
	7 暗号の利用
	8 活動の追跡
	9 攻撃の検知
	10 脅威と脆弱性の管理
	11 安全なソフトウェアの更新
	12 ベンダセキュリティガイダンス
Module A	A.1 機密認証データ
	A.2 カード会員データの保護

Secure Software Standard の階層構造

コア要件（またはモジュール）
└ セキュリティ目標
└ コントロール目標
└ コントロール目標/テスト要件/ガイダンス

Secure Software Core Requirements

Security Objective: Minimizing the Attack Surface

The attack surface of the software is minimized. Confidentiality and integrity of all software critical assets are protected, and all unnecessary features and functionality are removed or disabled.

Control Objectives	Test Requirements	Guidance
Control Objective 1: Critical Asset Identification All software critical assets are identified and classified.		
1.1 All sensitive data stored, processed, or transmitted by the software is identified.	**1.1.a** The assessor shall examine vendor evidence to confirm that it details all sensitive data that is stored, processed, and/or transmitted by the software. At a minimum, this shall include all payment data, authentication credentials, cryptographic keys and related data (such as IVs and seed data for random number generators), as well as system configuration data (such as registry entries, platform environment variables, prompts for plaintext data in software allowing for the entry of PIN data, or configuration scripts).	Software security controls are designed and implemented to protect the confidentiality or integrity of critical assets. To make sure these controls are effective and appropriate, the software vendor should identify all sensitive data the software collects, stores, processes, or transmits, as well as all sensitive functions and resources it either provides or uses.

※Secure SLC は要件モジュールがないのでセキュリティ目標が階層の最上位になるが、それ以降は Secure Software Standard と同様

Secure Software Standard
モジュールとセキュリティ目標

1つのコア要件と1つのモジュールで構成(v1.0)

- コア要件は共通適用
- モジュールは該当する場合に追加で適用

コア要件: 4つのセキュリティ目標 で構成

- 攻撃可能面の最小化
- ソフトウェア保護機構
- 安全なソフトウェアのオペレーション
- 安全なソフトウェアライフサイクル管理

モジュール A – アカウントデータの保護: 1つのセキュリティ目標で構成

- アカウントデータの保護

✓ Module A は、通常のカード情報を扱う決済ソフトウェアであれば適用対象となると思われる
✓ Module A の対象とならない例としては、トークンのみを扱うソフトウェアなどが考えられる
✓ 将来的に他の PCI のソフトウェア系基準がマージされる際には、Module として追加される？
その場合、マージされた基準の適用対象になるソフトウェアにはコア要件の準拠も求められると思われる

Secure Software Standard で注目されるコントロール目標

- リスク評価に関するコントロール目標
  - 1.1 ソフトウェアが保存、処理、伝送する全ての機密情報の識別
  - 1.2 ソフトウェアが提供または利用する全ての機密機能およびリソースの識別
  - 1.3 重要な資産のクラス分け
  - 4.1 攻撃可能シナリオを識別する
  - 10.1ソフトウェアの脅威と脆弱性が識別、評価、対処されること
- 機密情報の保護に関するコントロール目標
  - 6.2 機密情報は、伝送される間、安全であること
- 暗号の利用に関するコントロール目標
  - 7.2 認定された鍵管理プロセスと手順をサポートする
    ※同等ビット強度として128bit以上が要求されているためTDESは不可
  - 7.3 認定された乱数生成アルゴリズムまたはライブラリを用いて生成された乱数のみを利用する
  - 7.4 乱数値は、それが依存する暗号プリミティブと暗号化鍵の最低有効強度要件を満たすエントロピーを持つこと
- 攻撃の検知に関するコントロール目標
  - 9.1 ソフトウェアは、配布後の設定変更や明白な攻撃などの異常な振る舞いを検知して警告すること
- アカウントデータの保護に関するコントロール目標
  - A2.3 PAN を保存する場合は、トランケーション、インデックストークンとパッド、強力な暗号化のいずれかの方法で読み取り不能にすること

035

Secure Software Lifecycle (Secure SLC) Standard の概要

Secure SLC Standard のセキュリティ目標とコントロール目標

4つのセキュリティ目標/10個のコントロール目標で構成

- ソフトウェアセキュリティのガバナンス
  - コントロール目標1: セキュリティの責任とリソース
  - コントロール目標2: ソフトウェアセキュリティのポリシーと戦略
- 安全なソフトウェアエンジニアリング
  - コントロール目標3: 脆弱性の識別と緩和
  - コントロール目標4: 脆弱性の検知と緩和

PA-DSS には含まれない、または詳細化された項目で、対応の難易度が高いと思われる

- 安全なソフトウェアとデータの管理
  - コントロール目標5: 変更管理
  - コントロール目標6: ソフトウェアの完全性の保護
  - コントロール目標7: 機密データの保護
- セキュリティに関する情報伝達
  - コントロール目標8: ベンダセキュリティガイダンス
  - コントロール目標9: ステークホルダーとの情報伝達
  - コントロール目標10: ソフトウェア更新情報

PA-DSS にも同様な要件があり、対応の難易度は相対的に高くないと思われる

Secure Software Standard と同名のコントロール目標
- Secure SLC: プロセスの確認に重点
- Secure Software Standard: 対象のソフトウェアに対するプロセスの実施結果の確認に重点

037

まとめ

まとめ

Software Security Framework の構成

- Secure Software Standard/Secure SLC Standard の二つの基準と関連プログラムで構成される
- Secure Software Standard: ソフトウェアを認定対象とする PA-DSS の直接の後継基準
- Secure SLC Standard: 開発ベンダが認定対象。取得は任意だが、認定ベンダではない場合、コード修正を伴う変更の際は必ず審査会社による評価が必要になる

PA-DSS との相違点

- Objective-based Approachに基づいて新たに策定。「要件」は「コントロール目標」に。
- 認定対象ソフトウェアの広がり：配布形態によらなくなったため、特にSaaSのようなクラウドで提供されるソフトウェアも対象に含まれる。さらに将来的に対象が広がる可能性があることもアナウンスされている。
- 保護対象の広がり：アカウントデータ以外でも、機密性・完全性が求められるデータは保護対象であることが明確化。
- ソフトウェアのリスク評価や、ベンダのソフトウェアセキュリティ対策に関する戦略策定からそのパフォーマンスのモニタリングなど、対応の難易度が高いと思われる項目の追加

Objective-Based Approach の考え方

- PCI DSS/PA-DSS のような具体的な頻度や厳密さはほとんど定められていない
  (There is no “one size fits all” method to software security)
- 頻度や厳密さを決める根拠となるベンダのリスク評価が非常に重要

他の PCI 基準との関係

- 現時点では、他の PCI 基準とは独立した基準となっている。ただし将来的に、他の PCI 基準とプログラムの一部が Software Security Framework に統合されるかもしれないことがアナウンスされている。
- もし P2PE ドメイン2（P2PE アプリケーションに関する要件）が統合された場合、国内でのインパクトが大きいかも？

あなたとともに、変わる世界をかえていく ――

NTT DATA

NTTデータ 先端技術株式会社