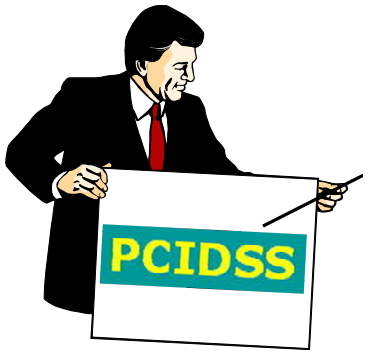
PCI DSS準拠の方法と
JCDSC によるサポート体制

(Japan Card Data Security Consortium)



2016年7月25日版

日本カード情報セキュリティ協議会

（JCDSC）

日本カード情報セキュリティ協議会（JCDSC）について

安全なカード社会の実現を図ることをテーマに、PCIDSS の普及・推進活動や、カード情報に関係する企業・団体の情報交流を行うため、2009年4月に設立されました。

会員企業は大手コンピューターメーカー、セキュリティ専門会社、国内QSA・ASV会社、コンサル会社、ITベンダー会社など160社以上が参加（2016年7月現在）

PCISSC（国際評議会）のGM, CTOも来日して、
JCDSC主催のセキュリティ・フォーラム。
（2014.7.29 東京国際フォーラム）

PCI DSS新バージョンの早期日本語化について、
PCISSCのマーケティング担当役員、J.King氏と運営委員・QSA部会の会合。
（2016.4.20JCDSC定時総会後、日本橋公会堂）

おもな内容

1. クレジットカード情報保護の世界基準=PCI DSS
2. 適用レベルの分類と準拠確認の手続き
3. 準拠に向けた取組み
4. JCDSCの役割とカード会社との連携
5. 参考資料

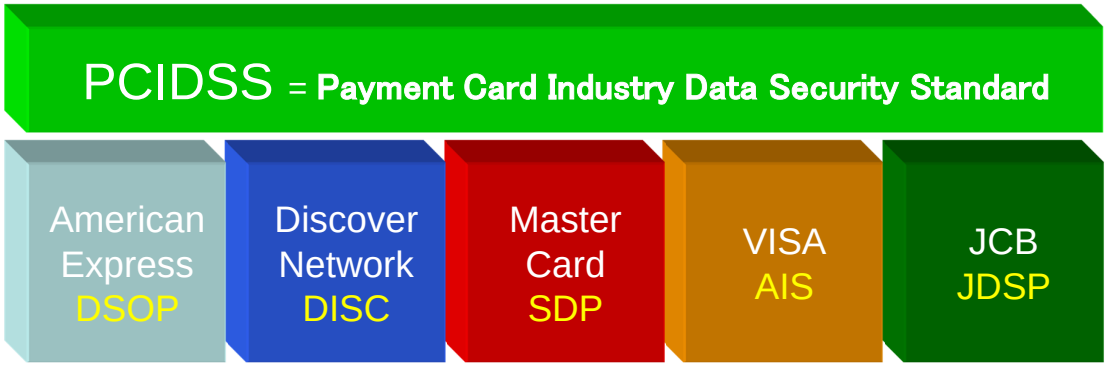
【本資料について】
・「クレジット取引セキュリティ対策協議会　実行計画-2016-」に基づき、(一社)日本クレジット協会が同協会会員を対象に、6月～7月に札幌から沖縄まで全国9都市で説明会を行い、その中で、PCI DSSについてJCDSC運営委員が説明を担当いたしました。
・この資料は、会場で配付したものを一部更新して、公開するものです。
・今後も新しい情報により、適宜改訂していきます。

1.クレジットカード情報保護の世界基準=PCI DSS

PCI DSSとは

1. カード会員情報や取引情報の保護を目的に、2004年に国際クレジットカードブランドが共同で策定した、ネットワークなどの処理システムや情報管理に関するセキュリティ要件（基準）
2. ISMSより範囲は狭いが、具体的で深さが要求される。
3. 「クレジット取引セキュリティ対策協議会」の実行計画は、カード情報を保持する事業者については、PCI DSS準拠を求めることとした。

●**準拠期限**：カード会社・PSP・EC加盟店は2018年3月、対面加盟店は2020年3月



国際カードブランド各社と実施プログラム（下段の文字）

PCI DSS要求基準の構成 = 6つの項目・12の要件

PCIDSS Ver3.2

I. 安全なネットワークの構築と維持
- 要件1:カード会員データを保護するために、ファイアウォールをインストールして構成を維持する
- 要件2:システムパスワードおよび他のセキュリティパラメーターにベンダー提供のデフォルト値を使用しない

II. カード会員データの保護
- 要件3:保存されるカード会員データを保護する
- 要件4:オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化する

III. 脆弱性管理プログラムの維持
- 要件5:すべてのシステムをマルウェアから保護し、ウィルス対策ソフトウェアまたはプログラムを定期的に更新する
- 要件6:安全性の高いシステムとアプリケーションを開発し、保守する

IV. 強力なアクセス制御手法の導入
- 要件7:カード会員データへのアクセスを、業務上必要な範囲内に制限する
- 要件8:システムコンポーネントへのアクセスを確認・許可する
- 要件9:カード会員データへの物理アクセスを制限する

V. ネットワークの定期的な監視およびテスト
- 要件10:ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する
- 要件11:セキュリティシステムおよびプロセスを定期的にテストする

VI. 情報セキュリティ・ポリシーの維持
- 要件12:すべての担当者の情報セキュリティに対応するポリシーを維持する

対象となる範囲において上記の要件をすべて遵守し、これを自己、もしくは第三者の確認によって証明する ＝ PCI DSS準拠

参考：ISMS (ISO27001) と PCI DSSの比較

例：パスワードに関する要求事項の比較

【ISMS】 ISO/IEC 27001:2013 付属書A
A.9.4.3 パスワード管理システム

- パスワード管理システムは、**対話式**とすることが望ましく、また、**良質なパスワード**を確実としなければならない。

「良質なパスワード」のレベルは、守るべき情報資産の機密度合や、リスクの大きさを考慮して、企業が自主的に決定する。

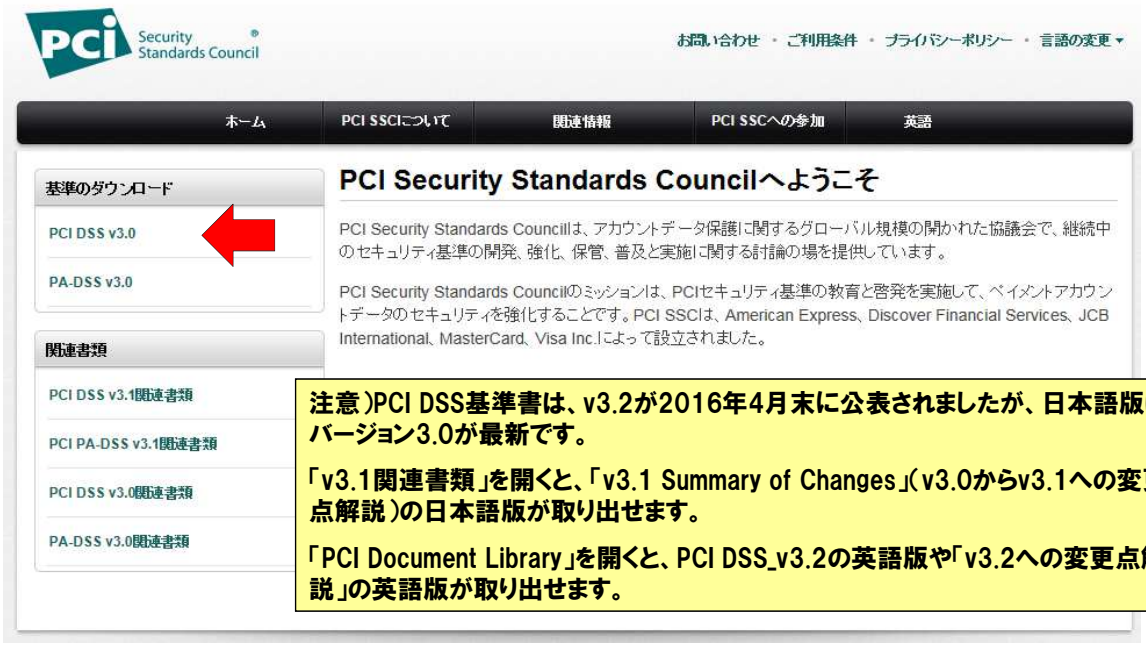
【PCI DSS】 v3.2要求事項

- パスワードは**数字と英字の両方を含めて**、少なくとも**7文字**にする。(8.2.3)
- パスワード/パスフレーズは少なくとも**90日ごと**に変更する。(8.2.4.a)
- **直近4回**使用されたパスワードは、新しいパスワードとして使用できないようにする。(8.2.5.a)
- ユーザーIDのロックアウトにより、連続したアクセス試行を**6回以内**に制限する。(8.1.6)
- ロックアウト時間は**最低30分間**、または管理者が許可するまでとする。(8.1.7)
- セッションのアイドル時間が**15分**を超えた場合、パスワードの入力を再び要求する。(8.1.8)
- ユーザーが、デフォルト(配布時の)パスワードから変更していることを確認する。(8.2.6)

クレジットカード情報の安全に特化しているので、
・内容を具体的に指示
・対応レベルが示されている

参考：PCI DSS基準書・日本語版のダウンロード

- PCI SSCの日本語サイトからアプローチします。
  https://ja.pcisecuritystandards.org/minisite/en/index.php



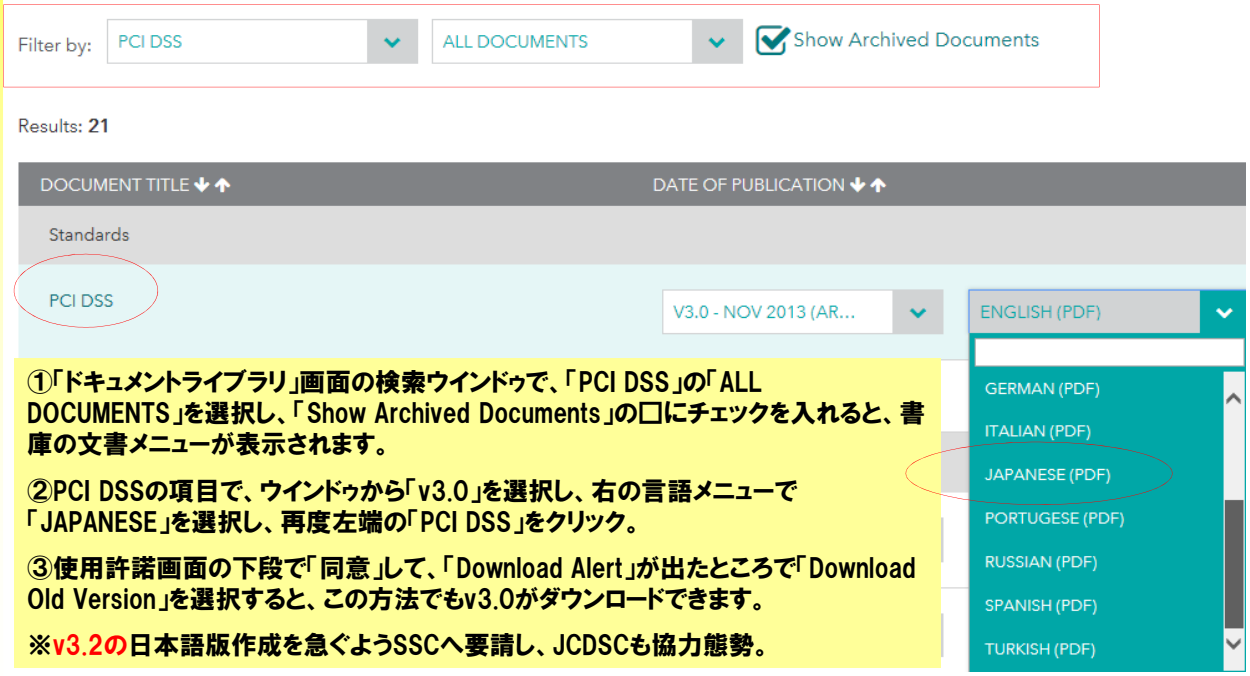
注意)PCI DSS基準書は、v3.2が2016年4月末に公表されましたが、日本語版は、バージョン3.0が最新です。

「v3.1関連書類」を開くと、「v3.1 Summary of Changes」(v3.0からv3.1への変更点解説)の日本語版が取り出せます。

「PCI Document Library」を開くと、PCI DSS_v3.2の英語版や「v3.2への変更点解説」の英語版が取り出せます。

参考:PCI DSS基準書や関連文書はライブラリーに

https://www.pcisecuritystandards.org/document_library



①「ドキュメントライブラリ」画面の検索ウインドゥで、「PCI DSS」の「ALL DOCUMENTS」を選択し、「Show Archived Documents」の□にチェックを入れると、書庫の文書メニューが表示されます。

②PCI DSSの項目で、ウインドゥから「v3.0」を選択し、右の言語メニューで「JAPANESE」を選択し、再度左端の「PCI DSS」をクリック。

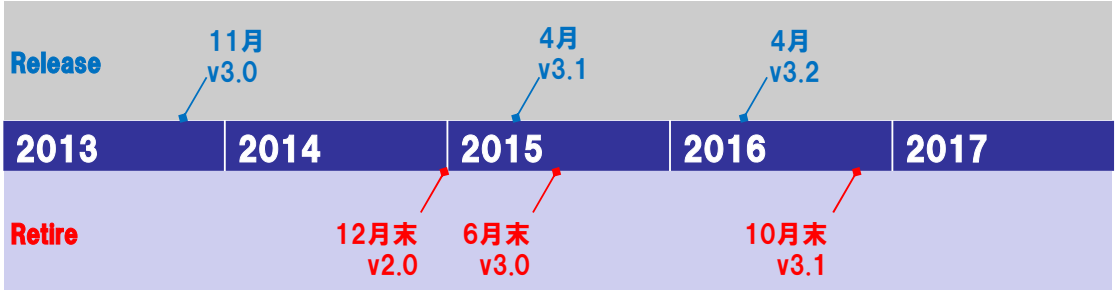
③使用許諾画面の下段で「同意」して、「Download Alert」が出たところで「Download Old Version」を選択すると、この方法でもv3.0がダウンロードできます。

※v3.2の日本語版作成を急ぐようSSCへ要請し、JCDSCも協力態勢。

参考: PCI DSS v3.2－主要な変更点

- v3.2への移行スケジュール
  - 2016年4月末公開と同時に発効
  - v3.1は、v3.2公開後6カ月で終息(2016年10月末日まで)
  - v3.2で追加される新たな要件は2018年2月1日から有効化

リリースと終息のタイムライン



2.適用レベルの分類と準拠確認の手続き

PCI DSS準拠の適用レベル分類

日本におけるクレジットカード情報管理スキーム　改訂版 より

QSA による訪問審査

（Qualified Security Assessors:認定審査会社）

自己問診（SAQ）

（Self Assessment Questionnaire）

加盟店		PSP（非対面/ネット）	クレジットカード会社
対面	非対面		
レベルA ①～④の2つ以上に該当する場合 ①VISA　600万件以上 ②Master 600万件以上 ③JCB　100万件以上 ④Amex　250万件以上		**すべて**	**レベルA** アクワイアラーまたはプロセッシング
レベルB 4ブランドいずれかが100万件以上	**レベルB** （レベルA以外）		**レベルB** イシュイングのみ （カード発行枚数の多少にかかわらず）
レベルC 4ブランドいずれも100万件未満			

対応期限（年度）

2019年度	2017年度

ASVスキャン

（Approved Scanning Vendors：認定スキャニングベンダー）

・内部・外部ネットワークのぜい弱性スキャン
（四半期毎）
※外部N/Wスキャンは ASVが実施する

内部・外部ネットワーク、アプリケーションへの ペネトレーションテスト
（年1回）はシステム環境により別途必要

QSAの訪問審査によるPCI DSS準拠

QSA（認定審査会社）の審査員が、実際にクレジットカード情報が取り扱われているシステムや業務を調査し、報告を行う。

- ✓ **訪問審査は年1回行われる。**
- ✓ **審査後、結果を記したレポートが引き渡される。**
  - ➢ 「ROC（Report on Compliance：報告書）」
  - ➢ 「AOC（Attestation of Compliance：準拠証明書）」
- ✓ **契約先のアクワイアラーまたはカードブランドによるAOCの提出を求められた場合、すみやかに提出する。**

訪問審査の方法

QSAは、PCI DSSで求められる要件の準拠状況を“テスト手順”に定められた方法（規定や証跡の確認、インタビュー、システム設定の確認）で審査。

約250項目 **約400項目**

PCI DSS 要件	テスト手順	ガイダンス
1.1 以下を含むファイアウォールとルーターの構成基準を確立し、実施する:	**1.1** ファイアウォール/ルーター構成基準および以下で指定されたその他の文書を検査し、標準が完全であり、以下のように実施されていることを確認する：	ファイアウォールとルーターは、ネットワークへの出入りを管理するアーキテクチャの重要コンポーネントです。これらのデバイスは、不要なアクセスをブロックし、ネットワークに出入りする承認済みアクセスを管理するソフトウェアまたはハードウェアデバイスです。 構成基準と手順は、データを保護するための組織における防御の第一線の強度を維持するのに役立ちます。
1.1.1 すべてのネットワーク接続およびファイアウォール/ルーター構成への変更を承認およびテストする正式なプロセス	**1.1.1.a** 文書化された手順を調べて、すべてをテストし承認するための正式なプロセスがあることを確認する。 • ネットワーク接続および • ファイアウォール/ルーター構成の変更	ファイアウォールとルーターへのすべての接続と変更を承認およびテストするために文書化されて実施されているプロセスは、ネットワーク、ルーター、またはファイアウォールの誤った構成により発生するセキュリティ上の問題を防ぐのに役立ちます。 変更の正式な承認とテストなしでは、変更の記録が更新されず、ネットワーク文書と実際の構成間に不整合が生じる原因となります。
	1.1.1.b ネットワーク接続のサンプルでは、責任者をインタビューし、記録を検査してネットワーク接続が承認されてテストされていることを確認する。	
	1.1.1.c ファイアウォールおよびルーター構成に実際に加えられ	

要件によっては、１つの要件に対して、複数のテスト手順（＝審査項目）が存在

QSAの連絡先

日本国内のおもなQSAは、JCDSCサイトに一覧表を掲載し、各QSAの連絡先や担当者（部署）、特色なども申告原稿ベースで載せています。（現在8社を掲載中）

※現在時点で免許が有効なQSAの登録状況は、PCISSCのサイトで、英文名称で検索して確認してください。

https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors

SAQによるPCI DSS準拠

SAQ（自己問診 = Self Assessment Questionnaire）は、
自己調査によって準拠を証明する方法

1. 内部・外部N/Wスキャン検査を四半期ごとに実施し、対応の必要がある脆弱性がない・または解決済である結果レポート1年分をそろえます。

※システム環境により、内部・外部ペネトレーションテストや、アプリケーションぜい弱性検査も求められます。

2. 所定のSAQに指定されている、PCI DSS要件のすべての項目に対応済であることを確認して記入し、内容責任について事業者の役員が署名します。

3. AOC（Attestation of Compliance：準拠証明書）をPCI SSCサイトからダウンロードして記入します。

4. 契約先のアクワイアラーまたはカードブランドによる、所定の手続きに添って上記1,2,3を提出します。

※SAQには、支援したQSAや ISA（Internal Security Assessor＝PCI DSSの社内審査資格者）**がある場合、署名する欄があります。**

QSAの支援・署名は必須ではありません。受理はアクワイアラー判断です。

業種によるSAQの適用区分

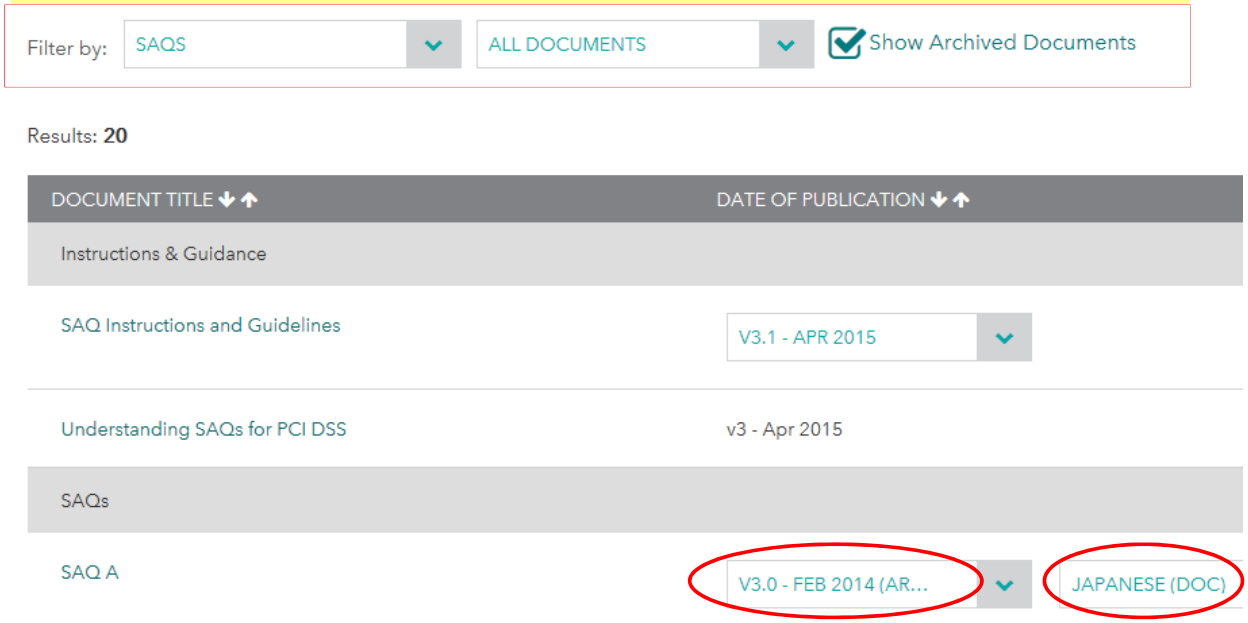
Type	対象
A	カードを提示しない加盟店（すべてのカード会員データ機能を外部委託）
A-EP	支払処理に第三者 Web サイトを使用することで部分的に外部委託している電子商取引加盟店
B	インプリンターまたはスタンドアロン型ダイアルアップ端末のみを使用する加盟店（カード会員データを電子形式で保存しない）
B-IP	スタンドアロン型 IP 接続 PTS加盟店端末装置（POI）端末を持つ加盟店（カード会員データを電子形式で保存しない）
C	ペイメントアプリケーションシステムがインターネットに接続されている加盟店（カード会員データを電子形式で保存しない）
C-VT	Web ベースの仮想端末を使用する加盟店（カード会員データを電子形式で保存しない）
D-M	その他すべての SAQ 適用加盟店（MはMerchants の略）
D-S	サービスプロバイダー用（SはService Providers の略）

※カード発行会社（イシュア）で、QSA受審レベルでない場合は、SAQのD-Sを使用します。

SAQの入手

Page-8の要領で「PCI DSS v3.1関連書類」から「PCI Document Library」を開きます。

「SAQs」の「ALL DOCUMENTS」を選択し、「Show Archived Documents」の□にチェック。各種のSAQsで希望の種類の「v3.0」を指定すると日本語版をダウンロードできます。※基準書と同じくv3.1・v3.2の日本語版がまだありません。



ASVスキャン および ペネトレーションテスト

No.	PCI基準	頻度	検査名称	内容
①	11.1	四半期	ワイヤレスアクセスポイント検査	
②	11.2	四半期	外部ネットワーク脆弱性スキャン	・ASVが実施する
③	11.2	四半期	内部ネットワーク脆弱性スキャン	
④	11.3	年1回	ペネトレーションテスト	・ネットワークの内部と外部からの侵入テスト ・アプリケーション層のペネトレーションテストには、要件 6.5に記載の脆弱性を含める ・セグメンテーションと範囲減少制御の有効性テスト

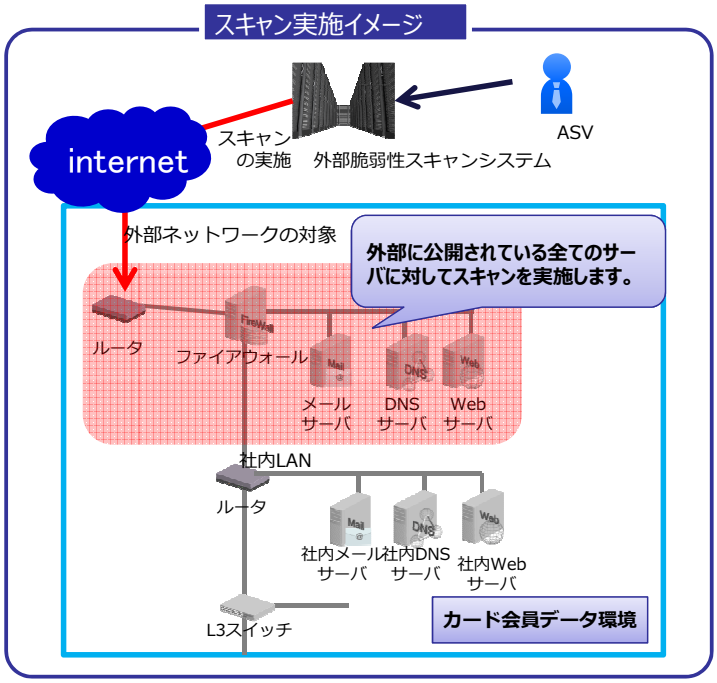
内部・外部のN/Wスキャンは全事業者に必須の検査で、そのうち外部N/WスキャンはPCI SSC認定の検査機関(ASV)が実施します。

国内ASVはQSAと同じく、JCDSCサイトに一覧表が掲載されています。

ASVスキャンとは

PCI SSCによって認定されたベンダー(ASV: Approved Scanning Vendor)によって実行される外部からの脆弱性スキャン

- PCI DSS 要件11.2で要求される項目
- 「ASV Program Guide」で定められているセキュリティレベルを満たしているか確認する
  → アカウント推測攻撃やサービス不能攻撃などは実施対象外ではあるが、業界標準のセキュリティレベルを確認可能
- PCI DSS対象システムが所持している全てのグローバルIPアドレスが対象
  → カード情報を取り扱っていないシステムでも、扱っているシステムと同一のセグメントに設置されている場合はスキャン対象となる
- 4半期に一度、ASVによって実施される必要がある
- ASVによって合格(PASS)レポートが発行されるまで繰り返す必要がある



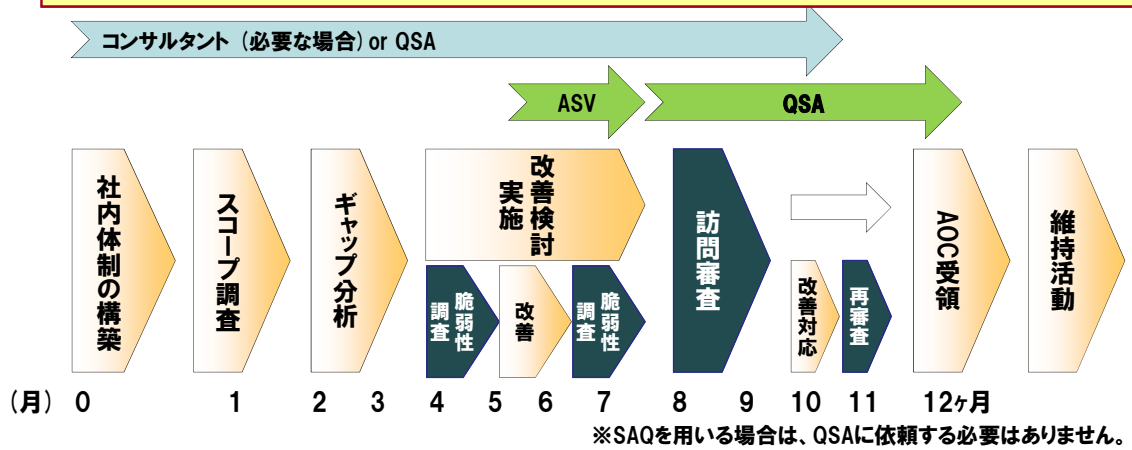
出典:NRIセキュアテクノロジー株式会社資料

3.準拠に向けた取組み

準拠までのスケジュール

準拠が確認されるまでの一般的な流れ

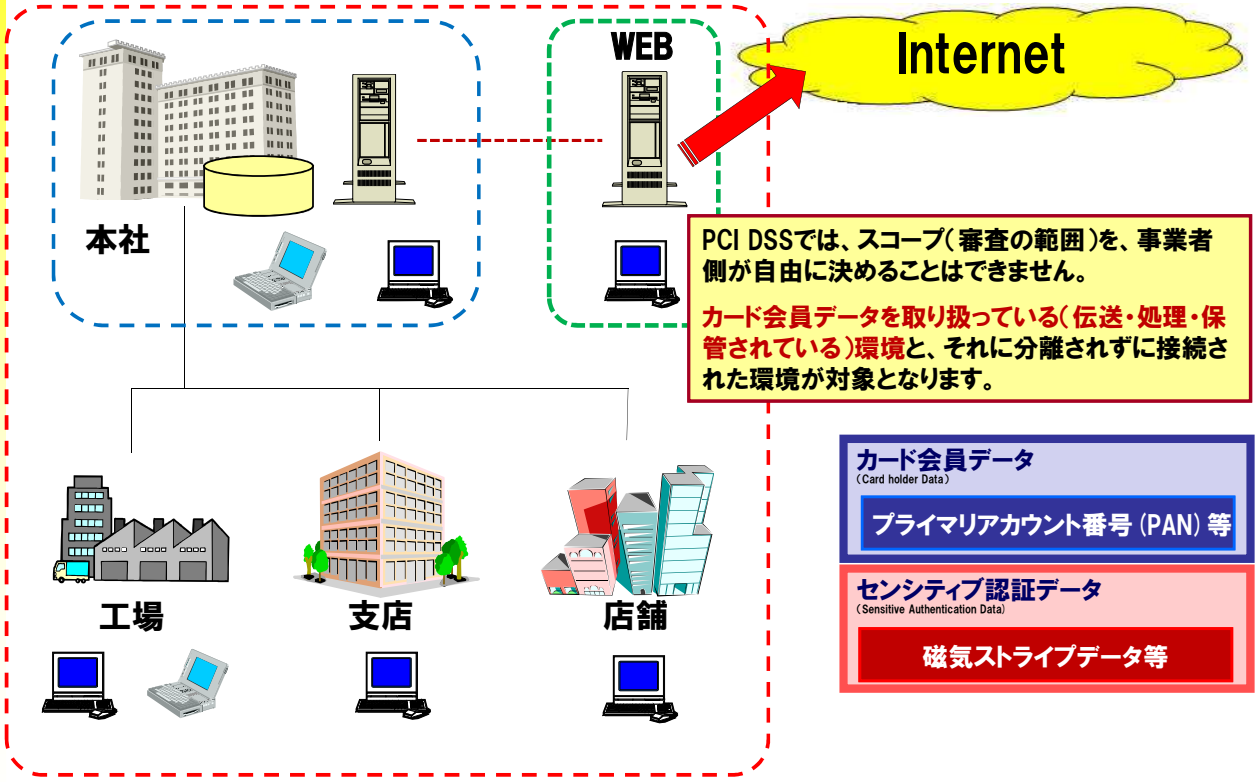
① QSAに審査を依頼する前に「ギャップ分析」を行った上で、プロジェクト全体のスケジュールを立てる
② PCI DSSすべての要件が満たされるよう対策を行う
③ 審査の前には、「ASVスキャン」や「ペネトレーションテスト」によって脆弱性の対処が完了していることを確認し、規程類や証跡なども準備しておく



※SAQを用いる場合は、QSAに依頼する必要はありません。

規模やセキュリティ達成状況によって、準拠までの期間や予算に差

審査の範囲（スコープ）



PCI DSSでは、スコープ（審査の範囲）を、事業者側が自由に決めることはできません。

カード会員データを取り扱っている（伝送・処理・保管されている）環境と、それに分離されずに接続された環境が対象となります。

カード会員データ
（Card holder Data）
プライマリアカウント番号（PAN）等

センシティブ認証データ
（Sensitive Authentication Data）
磁気ストライプデータ等

スコープの縮小－スコーピングとセグメンテーション

・スコープ定義の手順

（１）準拠の必要性確認

当該システムでは、PANが伝送・処理・保管されていますか？

→ 伝送・処理・保管、いずれかを行っていればPCI DSS準拠の必要があります（PCI DSSの対象です）

PANを全て外部委託先に預ける

PANを取り扱わない（非保持化）

（２）-１．直接対象となる範囲の確認

PANが伝送・処理・保管されているシステムコンポーネントはどれですか？

→ あてはまるシステムコンポーネントはすべて対象です

対象システムを外部サービスに切り替える

（２）-２．間接的に対象となる範囲の確認

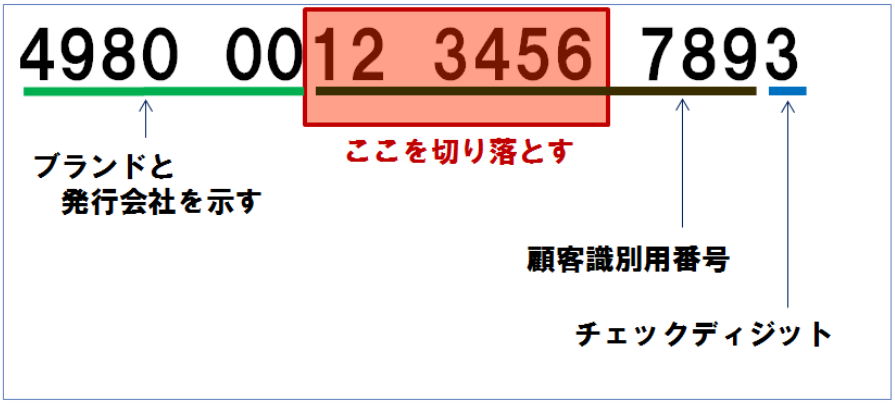
（PANを伝送・処理・保管していなくても）そこに直接接続（フラットネットワーク）しているシステムコンポーネントはどれですか？

→ そのシステムコンポーネントも、すべて対象です

接続するシステムを限定、分離（セグメンテーション）

スコープの縮小－非保持化：トランケーション

・カード番号として復元できないように切り落とす



✓ 4980-00**-****-7893
✓ 49**-****-****-**93
✗ 4980-0012-3456-****
✗ 4980-****-**56-****
✗ ****-0012-34**-****

スコープの縮小－非保持化：トークナイゼーション

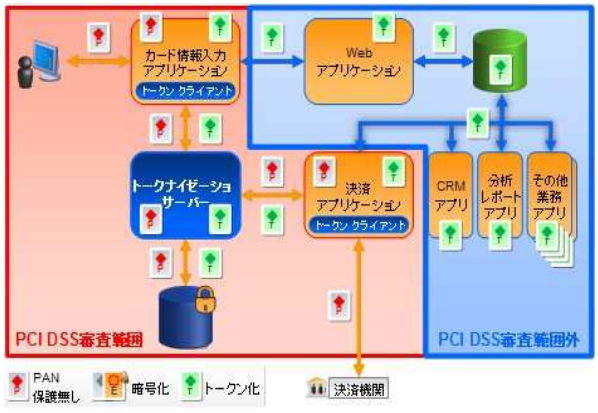
トークナイゼーションとは、データの一部、または全部を別の一意の乱数に取り替えて単独では元に戻せないトークンとすること。

- トークンはカード会員データとしては扱わない
  ※PCI DSSでは暗号化された場合でもカード会員データとして扱う
- 手続きを踏むことで元のデータの参照が可能
- トークナイゼーションの仕組みそのものは検証される必要がある。

Table 1: Selected Examples of Token Formats*

PAN	Token	Comment
3124 005917 23387	7aF1Zx118523mw4cwl5x2	Token consists of alphabetic and numeric characters
4959 0059 0172 3389	729129118523184663129	Token consists of numeric characters only
5994 0059 0172 3383	599400x18523mw4cw3383	Token consists of truncated PAN (first 6, last 4 of PAN are retained) with alphabetic and numeric characters replacing middle digits.

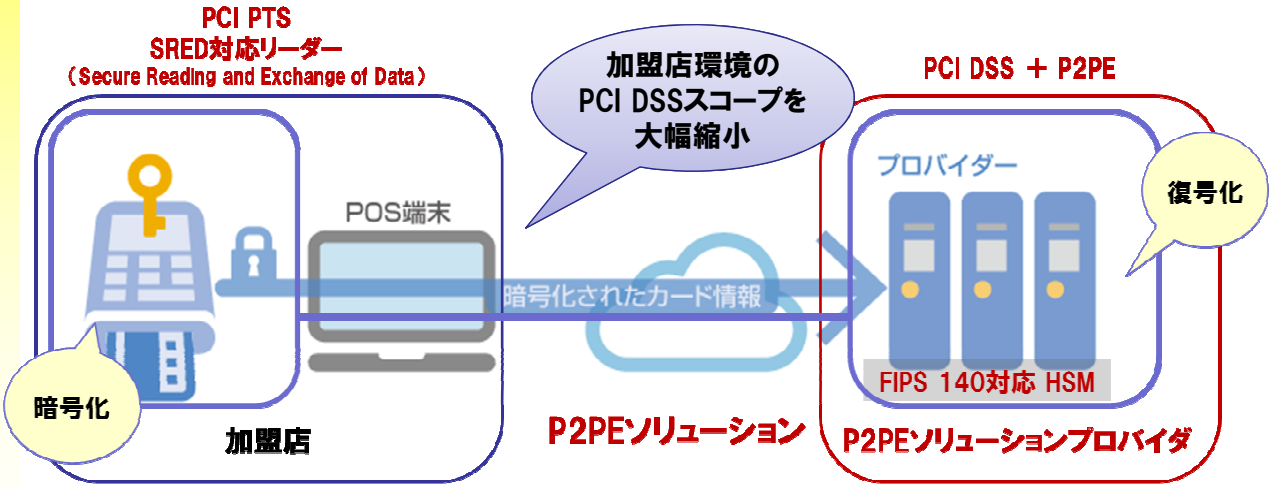
PCI SSC「PCI DSS Tokenization Guidelines」より



http://www.jcdsc.org/topics/vol02.php

外部サービスの利用－ P2PE

- Point-to-Point Encryption（P2PE）
  - ➢ P2PE準拠ソリューションを使用する加盟店のPCI DSSスコープ縮小



出典：PCI DSS徹底解説 / NTTデータ先端技術株式会社
http://www.intellilink.co.jp/article/pcidss/15.html

各種検査会社・コンサル会社の一覧「参考資料集」

・ペネトレーションテストや内部・外部ネットワーク検査など、各種ぜい弱性検査を実施できる会社、コンサル会社、およびカード情報非保持検査実施会社について、特色や連絡先情報を含めて一覧表を掲載しています。

・PCI DSSの要求事項別に、セキュリティ・ソリューションの一覧表も掲載しています。

4.JCDSCの役割とカード会社との連携

“実行計画2016“ におけるJCDSCの役割

① 加盟店のPCI DSS理解を促進するセミナーを開催し、準拠に向けた取組みをサポートする。

- ✓ 6/22（水），「PCI DSSセキュリティフォーラム2016」を東京国際フォーラム（有楽町駅前）にて開催。

② PCIDSS理解を増進するための資料を作成し、講師を派遣する。

- ✓ 基本資料をJCDSCサイトへ掲載。日本クレジット協会等が会員・加盟店向けのPCI DSSセミナーを順次計画中。講師はQSAから交代で派遣。

③ 簡易なPCIDSS自己診断票やFAQを作成し、提供する。

- ✓ 自己診断票はJCDSCサイトへ掲載済。FAQは順次整備して掲載予定。

※自己診断票ダウンロードURL→ http://www.jcdsc.org/news/160223.php

④ JCDSCサイトにPCI DSSに関する相談窓口を開設する。

- ✓ 「事務局への問合せ」フォームメールを開設済。

⑤ QSA各社の特徴等を記載したリストを作成し、JCDSCサイトで案内する。

- ✓ 掲載済。ASVや各種検査、コンサル会社の一覧、要求事項別ソリューション一覧を掲載済。適宜バージョンアップする。

実行計画の実践に、カード会社とJCDSCの連係

お願い事項

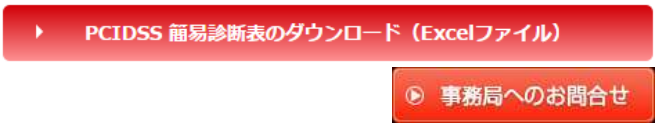
① 加盟店やPSP等に対する、JCDSC等主催PCI DSSセミナーのご案内

② 契約加盟店やPSP向けPCI DSSセミナーの開催

- JCDSCも講師派遣等協力いたします。※地方開催の場合は旅費実費

③ 加盟店に対する「JCDSC Webサイト」のご紹介

- 「PCI DSS自己診断票」
- 「事務局へのお問合せ」



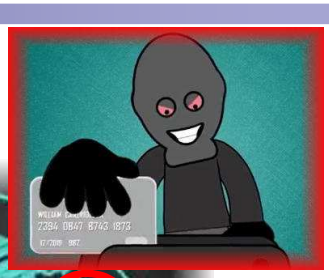
http://www.jcdsc.org/

最後に・・・

日本が世界の“セキュリティホール“になってきた

全国のコンビニATMから、偽造クレジットカードで約18億円の不正引き出し被害発生。

出し子100人以上を動員した、大規模組織犯罪。
（2016.5.24）



・米国は大統領令でICカード化を急速に進行中。2017年完了予定。

・国際犯罪組織は、犯行が困難な欧米を回避して、日本をターゲットにする傾向にある。

①南アフリカの銀行で漏えい
②中国系焼き肉店の磁気カード
③日本のATMが被害に

イラストの出典：PCISSC / Educational Resources

●PCISSC制作のビデオアニメ「モバイル決済」、「EMV」、「P2PE」公開中（日本語字幕入り）
http://www.jcdsc.org/news/151215.php

カード情報非保持またはPCI DSS準拠を急げ

各主体の役割について（“実行計画2016“より）

●カード情報保護の対策は目前リスクを排除するために早急に着手すべき課題である。

●各主体は本実行計画に示す期限を待つことなく、可能な限り前倒しで対応を進める。

ご清聴ありがとうございました

安全なカード社会の実現をめざして
JAPAN CARD DATA SECURITY CONSORTIUM
日本カード情報セキュリティ協議会