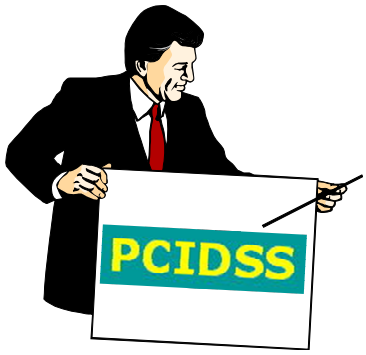
PCI DSS準拠の方法と
JCDSC によるサポート体制

(Japan Card Data Security Consortium)



2019年2月15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、PCI DSS 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ベンダー会社など約240社が参加（2019年2月現在）

JCDSC主催のPCI DSSセキュリティ・フォーラム
（2018.6.22 東京国際フォーラム）

PCI DSS 準拠の推進について、経産省取引監督課と日本クレジット協会、JCDSC運営委員・QSA部会による情報交換会。（2017.5.24）

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と参考資料
4. 実行計画におけるJCDSCの役割

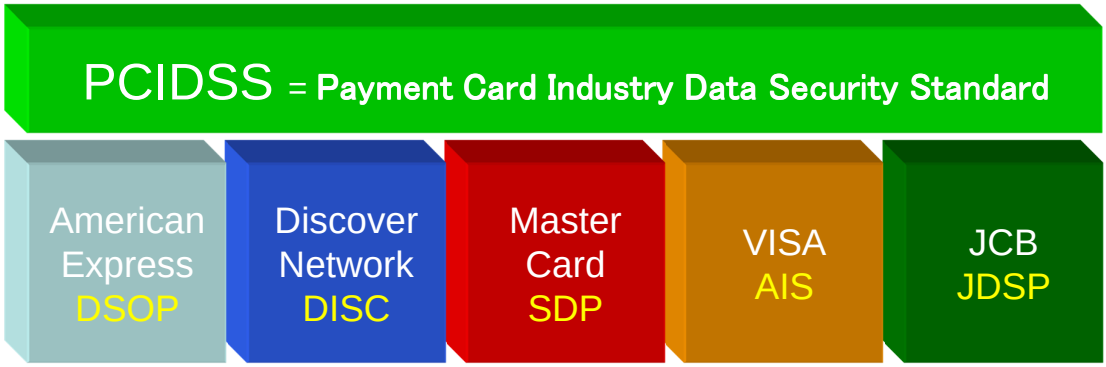
【本資料について】
・「クレジット取引セキュリティ対策協議会　実行計画2016」に基づき、(一社)日本クレジット協会が同協会会員を対象に、2016年6月～7月に札幌から沖縄まで全国9都市で説明会を行い、その中で、PCI DSSについてJCDSC運営委員が説明を担当いたしました。
・この資料は会場で配付したものを基本に、「実行計画2018」の内容やPCI DSSに関する2019年2月現在の情報を加えて更新しています。

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）。ISMSより範囲は狭いが、具体的で深さが要求される。
2. 「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、対面加盟店は改正割賦販売法の施行2018年6月を期限とし、最終的には2020年3月末にすべての事業者が対応完了をめざす。



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 Ver3.2.1

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、これを自己問診（SAQ）、もしくは第三者（QSA）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

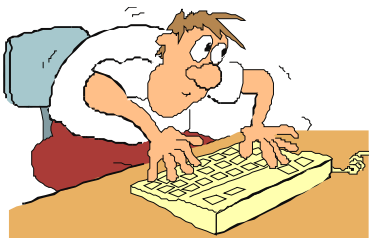
JCDSC Japan Card Data Security Consortium

例：パスワードに関する要求事項の比較

【ISMS】 ISO/IEC 27001:2014 付属書A
A.9.4.3 パスワード管理システム

- P/W管理システムは、**対話式**でなければならず、また**良質なP/Wを確実に**するものでなければならない。

「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】 v3.2.1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

JCDSC Japan Card Data Security Consortium

- PCI SSCの日本語サイトからv3.2.1日本語版が取り出せます。
  https://ja-pci.onelink-translations.com/minisite/env2/

PCI Security Standards Council

ドキュメントライブラリ

英語で表示されているドキュメントの一覧は、まだ翻訳されていません。翻訳版が利用可能になると、それに応じて一覧も更新されます。

PCI DSS	
基準	
PCI DSS	v3.2.1 - 2018 年 5 月
サポート文書	
用語集（用語、略語、および頭字語）	v3.2 - 2016 年 4 月

「PCI DSS」をクリックし、PCI SSCの使用許諾契約書に「同意する」をクリックしたあと、再び「PCI DSS」をクリックすれば、PDF版が開きます。

2.適用レベルの分類と準拠確認の手続き

PCI DSSの適用レベル

「PCI DSS準拠にかかる基準及び検証方法等に関する実施要領」2017.6 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	クレジットカード会社
	対面	非対面	（非対面/ネット）	
レベルA	①～④を基に、4ブランドにより選別する ①VISA　600万件以上 ②Master 600万件以上 ③JCB　100万件以上 ④Amex　250万件以上 QSA審査または※SAQ		すべて ※SAQの場合はROCの作成が必要	レベルA 国際ブランドから指定のアクワイアラー または プロセッシング全社
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 イシュアー または レベルA以外のアクワイアラー
レベルC	4ブランドいずれも100万件未満	対面加盟店の対応期限は改正割賦販売法の施行2018年6月を意識。		
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
	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。	

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9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

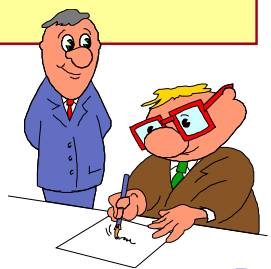
1. **内部・外部N/Wスキャン検査を四半期ごとに実施し、対応の必要がある脆弱性がない・または解決済である結果レポート1年分をそろえます。**※システム環境により、内部・外部ペネトレーションテストや、アプリケーションぜい弱性検査も求められます。

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。**※業務内容により適合するSAQタイプは異なります。次のページの資料を参照ください。

3. **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提出します。**※決済件数の取扱いレベルにより、必ず提出する場合と、要求されたら提出する場合があります。ブランドやカード会社によりガイドラインが異なりますので、契約先へお問合せください。

※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の適用区分と適用項目数一覧

V3.2.1版	加盟店の業態	カード情報の取扱い形態	タイプ	項目数
非対面 EC/通信販売加盟店	・PSPのﾘﾝｸ(ﾘﾀﾞｲﾚｸﾄ)型の決済ｻｰﾋﾞｽを使用するEC加盟店 ・ｶｰﾄﾞ情報の全ての処理を外部委託するEC/通信販売加盟店	ECまたは通信販売の加盟店でｶｰﾄﾞ情報をｼｽﾃﾑまたは加盟店内で電子形式で通過、処理、保存しない。	A	24
	・PSPのJavaScript型の決済サービスを使用するEC加盟店	ECの決済をPCI DSS準拠済みのｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞｰに部分的に委託しているECの加盟店で、カード情報をｼｽﾃﾑまたは加盟店内で電子形式で通過、処理、保存しない。	A-EP	192
対面/通信販売加盟店 ※EC加盟店には適用されない	CCTなどの決済端末をﾀﾞｲｱﾙｱｯﾌﾟ接続する、主に対面加盟店	ｲﾝﾌﾟﾘﾝﾀｰ、ｽﾀﾝﾄﾞｱﾛﾝ型のﾀﾞｲｱﾙｱｯﾌﾟの決済端末のみによってカード情報を処理する加盟店であり、ｶｰﾄﾞ情報を保存していない。	B	41
	CCTなどの決済端末をIP接続する、主に対面加盟店	決済ﾈｯﾄﾜｰｸまたはASP/ｸﾗｳﾄﾞ事業者にIP接続されるｽﾀﾝﾄﾞｱﾛﾝ型のPCI PTS認定の決済端末のみによってｶｰﾄﾞ情報を処理する加盟店であり、ｶｰﾄﾞ情報を保存していない。	B-IP	87
	POSをｲﾝﾀｰﾈｯﾄに接続してｶｰﾄﾞ処理する、主にPOS加盟店	POSｼｽﾃﾑまたはその他のｲﾝﾀｰﾈｯﾄに接続されているﾍﾟｲﾒﾝﾄｱﾌﾟﾘｹｰｼｮﾝ経由で、ｶｰﾄﾞ情報を処理するが、カード情報をｺﾝﾋﾟｭｰﾀｰｼｽﾃﾑに保存しない加盟店。	C	161
	電話やﾊｶﾞｷ/FAXでｶｰﾄﾞ処理する、主に通信販売加盟店	Webﾌﾞﾗｳｻﾞなどの仮装端末のみでｲﾝﾀｰﾈｯﾄを経由して、1件ずつｶｰﾄﾞ情報を処理し、ｶｰﾄﾞ情報をｺﾝﾋﾟｭｰﾀｰｼｽﾃﾑに保存しない。決済に利用するWebｱﾌﾟﾘｹｰｼｮﾝはPSP、ｱｸﾜｲｱﾗｰなどｻｰﾄﾞﾊﾟｰﾃｨｰから提供される必要がある。	C-VT	84
	PCI P2PEｿﾘｭｰｼｮﾝを導入した主にPOS加盟店	PCI P2PEに認定されたｿﾘｭｰｼｮﾝを導入し、それらに含まれる決済端末のみでｶｰﾄﾞ情報を処理する加盟店であり、ｶｰﾄﾞ情報を保存していない。	P2PE	33
対面/非対面加盟店	・PSPのﾓｼﾞｭｰﾙ(ﾌﾟﾛﾄｺﾙ)型を使用するEC加盟店 ・ｶｰﾄﾞ情報をｻｰﾊﾞｰやPCで保存するPOSや通信販売加盟店 ・ｶｰﾄﾞ情報をPOSｼｽﾃﾑで通過、処理、保存する加盟店	・ｶｰﾄﾞ情報を自社のｻｰﾊﾞで処理する加盟店 ・ｶｰﾄﾞ情報を電子形式で保存する加盟店 ・ｶｰﾄﾞ情報を電子形式で保存しないが他のSAQﾀｲﾌﾟの基準を満たさない加盟店 ・他のSAQﾀｲﾌﾟを満たす環境にあるが、自社の環境に他のPCI DSS要件が適用されるような加盟店	D-M	330
サービスプロバイダー	・カード発行のみ行うカード会社（イシュア） ・決済サービスプロバイダー（PSP） ・カード会社・PSP以外で、カード情報を取り扱っている事業者	ペイメントブランドによりSAQ対象として定義された、すべてのサービスプロバイダー。	D-S	369

どのタイプのSAQを使えばよいか

各タイプ別SAQの冒頭に「開始する前に」をよく読んで検討しましょう。

適合する業務内容が詳しく書かれています。下は一例として「C-VT」タイプの一部分です。

開始する前に

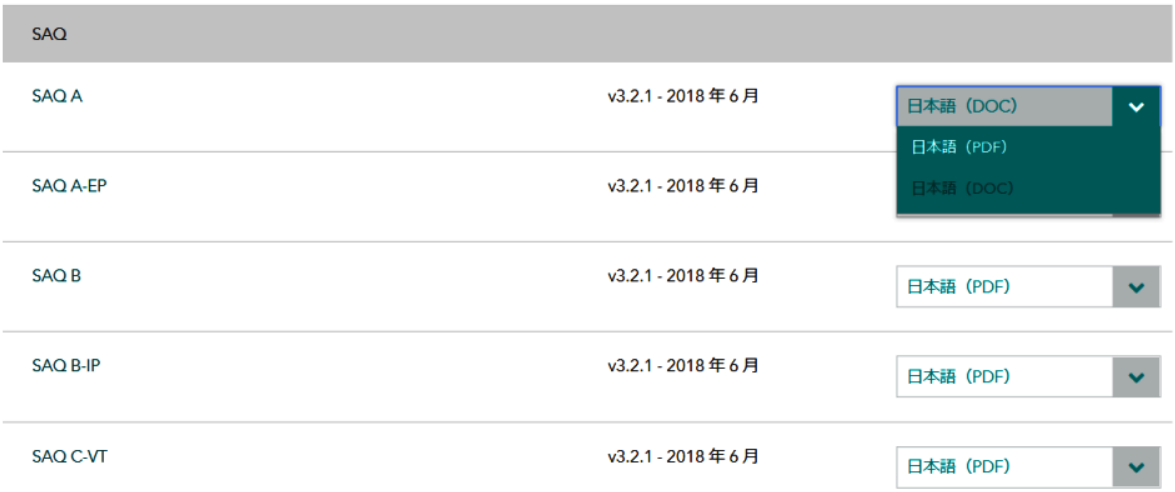
SAQ C-VT は、インターネットに接続されたパーソナルコンピュータ上にある隔離された仮想端末のみによってカード会員データを処理する加盟店に適用される要件を示すために作成されました。

仮想端末は、ペイメントカードトランザクションを承認するアクワイアラー、プロセサー、または第三者サービスプロバイダの Web サイトへの Web ブラウザベースのアクセスです。加盟店は安全に接続された Web ブラウザを使用してペイメントカードデータを手動で入力します。物理端末の場合と異なり、仮想端末はデータをペイメントカードから直接には読み取りません。ペイメントカードトランザクションを手動で入力するため、一般に仮想端末は取引量の少ない加盟店環境で物理端末の代わりに使用されます。

SAQ C-VT 加盟店は仮想端末のみによってカード会員データを処理し、カード会員データをコンピュータシステムに保存しません。これらの仮想端末は、仮想端末の支払い処理機能をホストする第三者にアクセスするインターネットに接続されています。この第三者は、加盟店の仮想端末ペイメント取引を承認および/または決済するため、カード会員データを保存、処理、および/または伝送するプロセサー、アクワイアラー、またはその他の第三者サービスプロバイダがありえます。

SAQの入手

Page-8の要領で、PCI SSCの日本語サイトから、各種SAQのv3.2.1日本語版が取り出せます。
PDF版とWord版が発行されています。



※P15掲載のタイプ別SAQの一覧表や、詳しい説明書は、JCDSCホームページの「PCI DSS準拠に向けて」参考資料集をごらんください。(https://www.jcdsc.org/topics/special2015.php)

7番に「日本語版PCI DSS基準書と各種タイプ別SAQ」が掲載されています。

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。

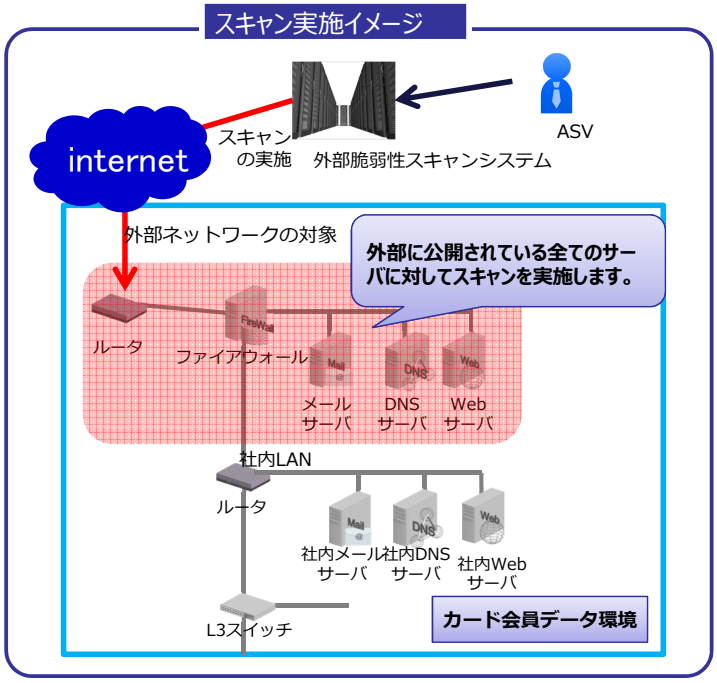
国内ASVはQSAと同じく、JCDSCサイトに一覧表が掲載されています。

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

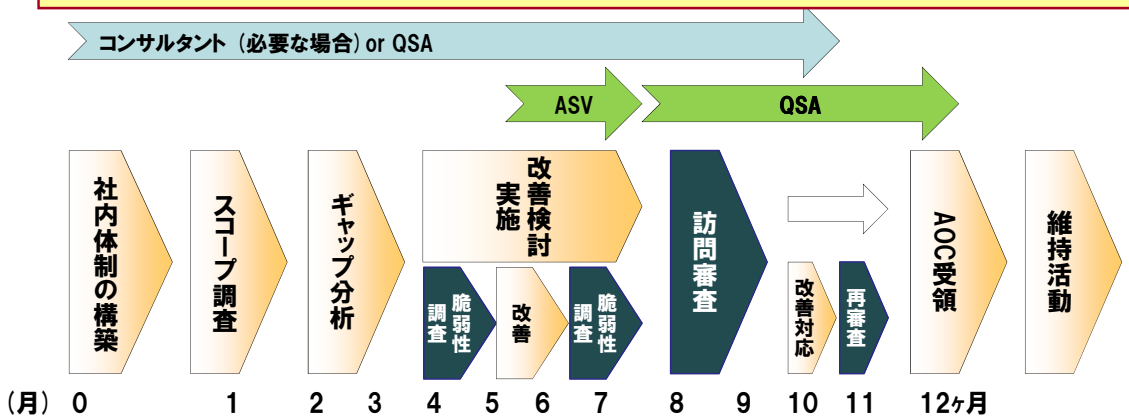


3.準拠に向けた取組みと参考資料

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

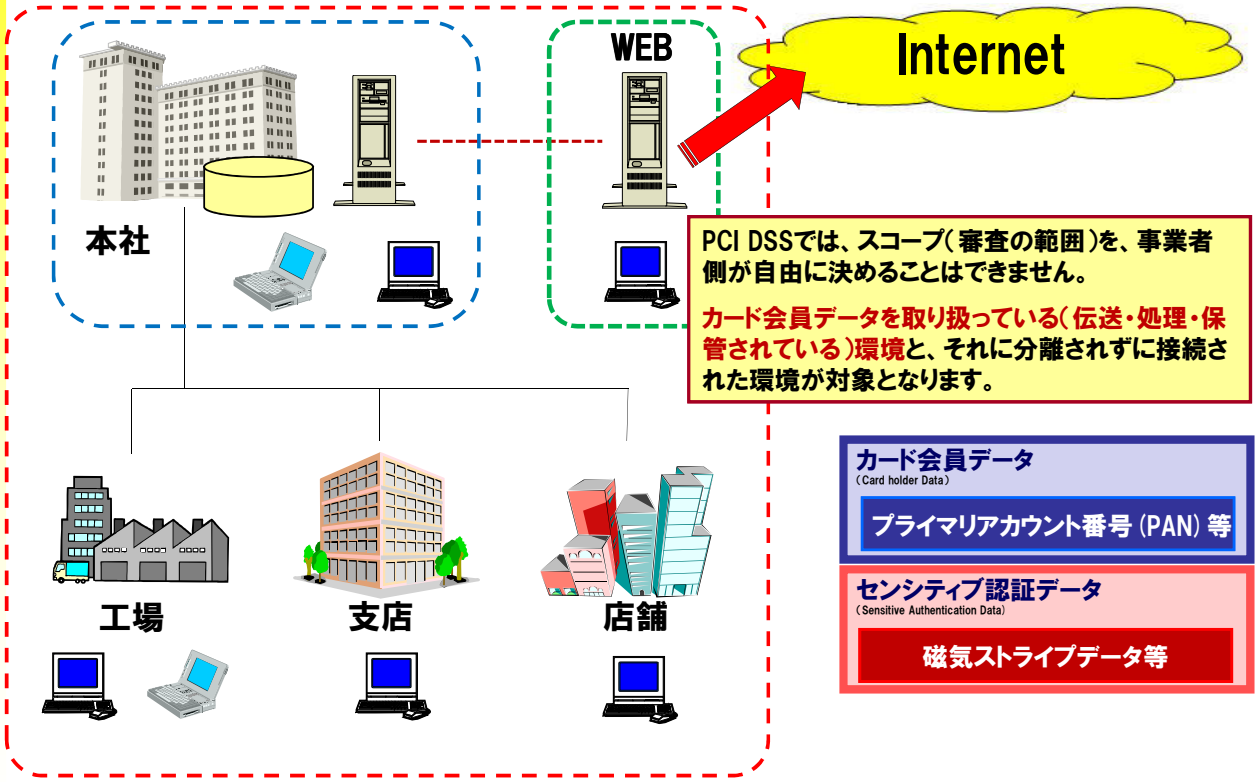
① QSAに審査を依頼する前に「ギャップ分析」を行った上で、プロジェクト全体のスケジュールを立てる
② PCI DSSすべての要件が満たされるよう対策を行う
③ 審査の前には、「ASVスキャン」や「ペネトレーションテスト」によって脆弱性の対処が完了していることを確認し、規程類や証跡なども準備しておく



※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

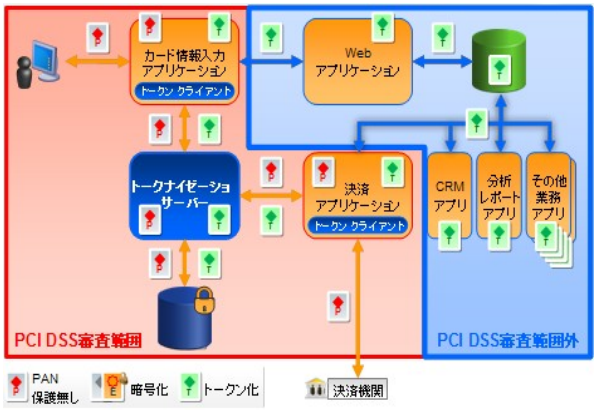
トークナイゼーションとは、データの一部、または全部を別の一意の乱数に取り替えて単独では元に戻せないトークンとすること。

- 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.

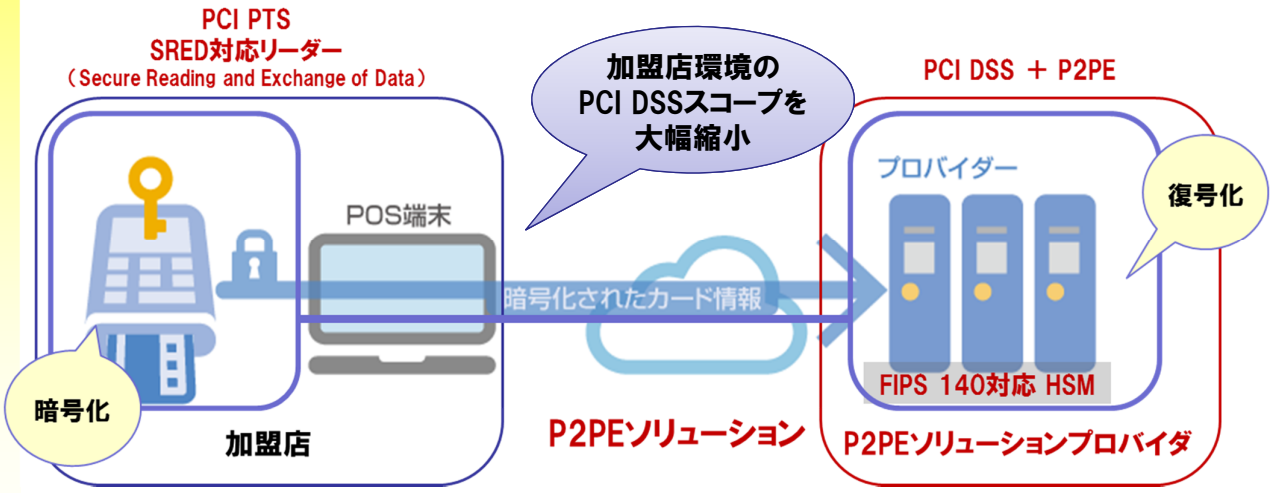
PCI SSC「PCI DSS Tokenization Guidelines」より



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.実行計画におけるJCDSCの役割

“実行計画2018“ におけるJCDSCの役割

(1) PCI DSSに関する認知度の向上及び準拠への取組促進に向けた情報提供

・基本資料や準拠のための参考情報などをJCDSCサイトへ掲載、各種セミナーの開催。PCI DSSセキュリティフォーラム、カード情報非保持セミナー、PCI DSS実務者向けセミナーなど。

(2) 準拠に向けた加盟店へのサポート体制

①理解増進のための講師派遣

・日本クレジット協会、日本通信販売協会、大手アクワイアラーなどが開催する講習会、セミナーへQSA部会等から講師派遣。

②コンテンツの提供・展開

・PCI DSS基本説明資料、FAQ、簡易自己診断表の作成・掲載。

③相談窓口の設置

・JCDSCサイトへ「事務局への問合せ」メールを設置し、随時対応中。

④分かりやすいツールの提供

・国内QSAやASV、コンサル企業等の特色・連絡先一覧をJCDSCサイトへ掲載。

⑤専門人材の育成

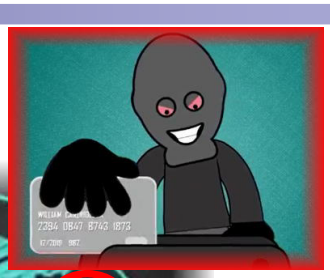
・QSA、ISA育成講習会の日本開催をPCI SSCへ協力し、日本語での案内を実施。

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。

・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 「セキュリティ啓発のビデオアニメ」が、日本語字幕入りで公開されています
https://www.jcdsc.org/memberstore_case.php

カード情報非保持・PCI DSS準拠達成を確実に

各主体の役割について （“実行計画2018“より）

●割賦販売法においては、従来カード会社に義務が課されていたが、2018年6月1日施行の改正割賦販売法では、加盟店にも義務が課されることになった。

●最終的には、全加盟店が 2020年3月末までにカード情報の適切な保護に関する対応（非保持化又はPCI DSS 準拠）が完了している状態になっていることを目指す。

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