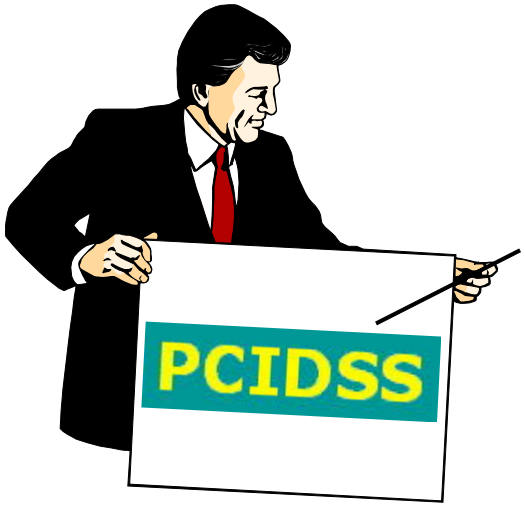
PCI DSSの基本説明と
JCDSC によるサポート体制

(Japan Card Data Security Consortium)



2025年3月12日版

日本カード情報セキュリティ協議会

（JCDSC）

Copyright 2025 © 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、カード会社、決済代行企業、加盟店企業、ソリューションベンダー会社など約370社が参加（2025年3月現在）

JCDSC主催のカードセキュリティ・フォーラム
（2024.6.19 東京国際フォーラム）

https://www.jcdsc.org/

PCI DSSの国際評議会（PCI SSC）米国本部から、Executive DirectorのLance Johnson氏が来日。
JCDSC運営委員らと行われた会議
（2023.7.11、中央区の日本橋人形町）

Copyright 2025 © JCDSC

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. クレジットカード・セキュリティガイドラインにおける
   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、PCI DSSについては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、その後改訂を続けた「実行計画」や2020年から毎年改訂されている「クレジットカード・セキュリティガイドライン」の内容、PCI DSSに関する2025年3月現在の情報を加えて更新しています。

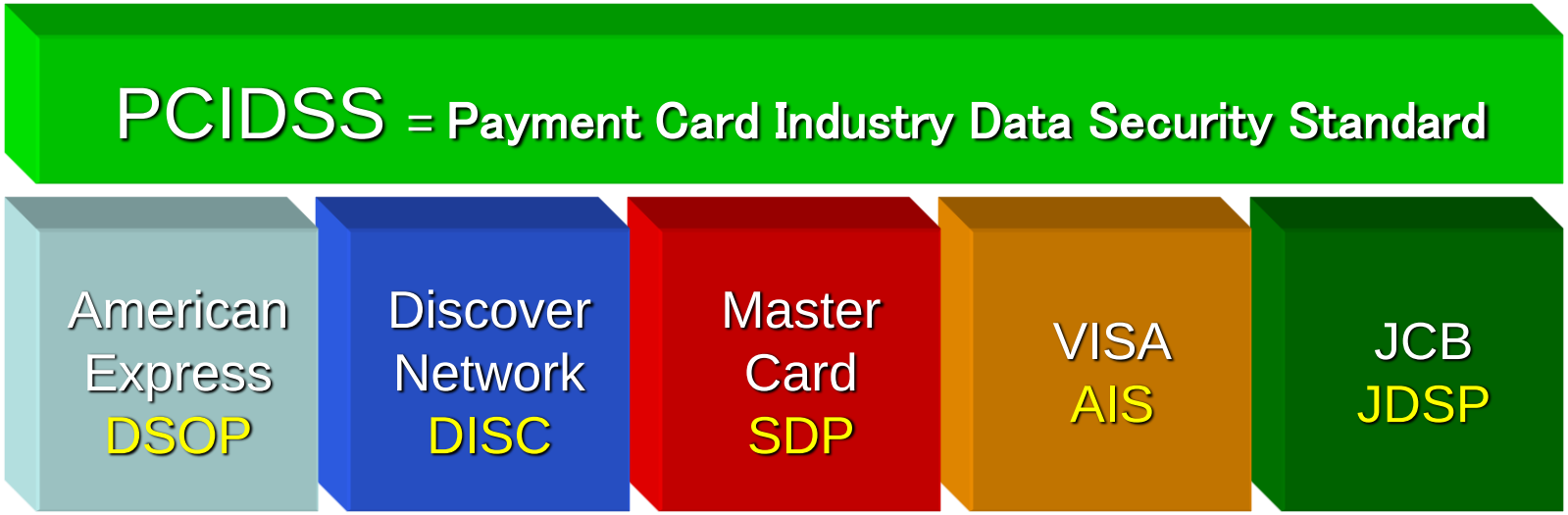
Copyright 2025 © JCDSC

1.クレジットカード情報保護の世界基準=PCI DSS

Copyright 2025 © JCDSC

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。



国際カードブランド各社と実施プログラム（下段の文字）

Copyright 2025 © JCDSC

PCI DSS要求基準の構成 = 6つの項目・12の要件

PCIDSS Ver4.0.1

I. 安全なネットワークのシステムの構築と維持

要件1: ネットワークセキュリティコントロールの導入と維持

要件2: すべてのシステムコンポーネントにセキュアな設定を適用する

II. アカウントデータの保護

要件3: 保存されたアカウントデータの保護

要件4: オープンな公共ネットワークでの送信時に、強力な暗号化技術でカード会員データを保護する

III. 脆弱性管理プログラムの維持

要件5: 悪意のあるソフトウェアからすべてのシステムおよびネットワークを保護する

要件6: 安全なシステムおよびソフトウェアの開発と維持

IV. 強力なアクセス制御の実施

要件7: システムコンポーネントおよびカード会員データへのアクセスを、
業務上必要な適用範囲 (Need to Know) によって制限する

要件8: ユーザーの識別とシステムコンポーネントへのアクセスの認証

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とテスト

要件10: システムコンポーネントおよびカード会員データへのすべてのアクセスをログに記録し、監視すること

要件11: システムおよびネットワークのセキュリティ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: 組織の方針とプログラムによって情報セキュリティをサポートする

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)、もしくは認定審査機関 (QSA) の確認によって証明する = PCI DSS準拠

Copyright 2025 © JCDSC

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 27001:2014 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】 v4.0.1の要求事項

- パスワードは**数字と英字の両方を含めて12文字**以上にする。(8.3.6) ※システムの都合で12文字にできない場合は8文字で可
- **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。(8.3.7)
- 無効な認証試行が行われた場合、**10回以下の試行回数**でユーザーIDをロックアウトする。(8.3.4)
- ロックアウト時間は**最低30分間**、または本人確認ができるまでとする。(8.3.4)
- ユーザーが、デフォルト(配布時の)パスワードを最初に使用した後、強制的に変更する(8.3.5)

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

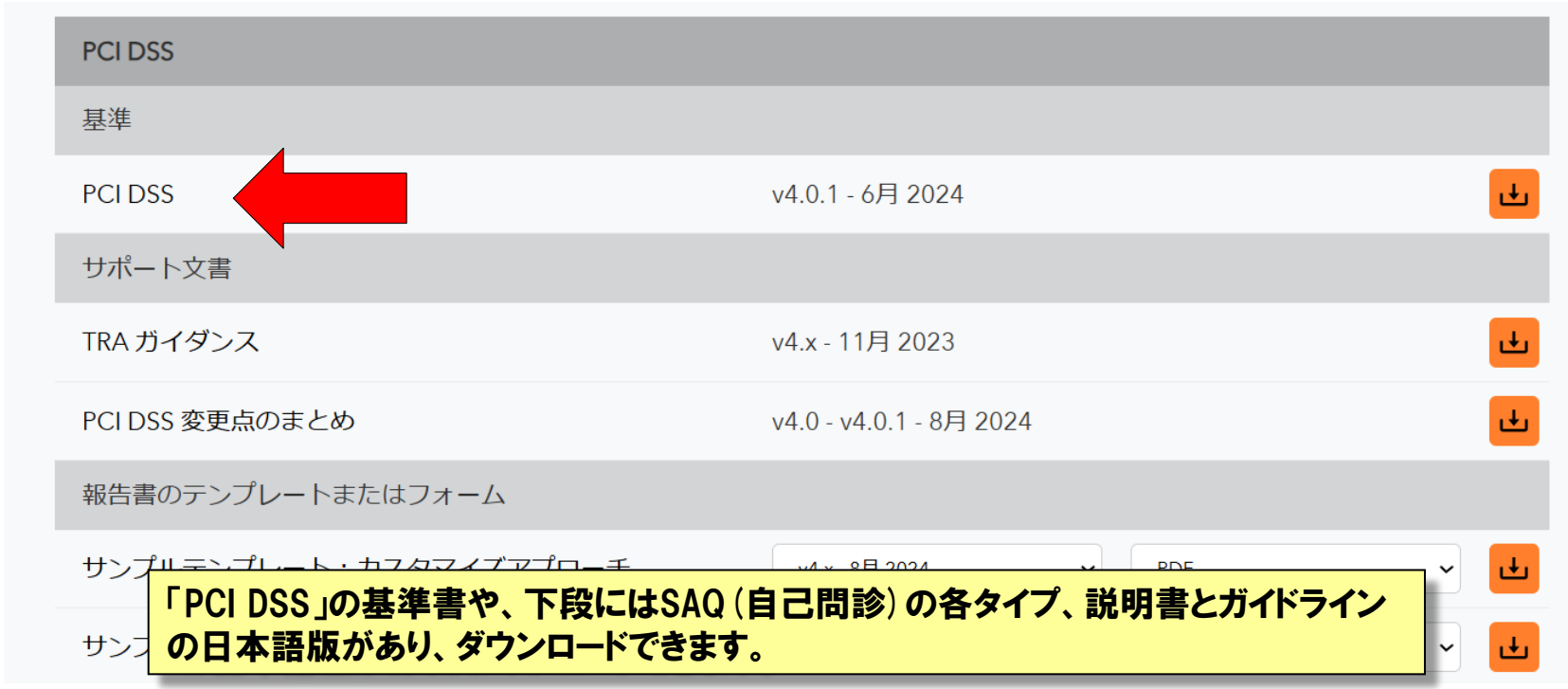
Copyright 2025 © JCDSC

PCI DSS基準書・日本語版の入手

- PCI SSCの日本語サイトから基準書日本語版が取り出せます。
  https://www.pcisecuritystandards.org/lang/ja-ja/

PCI Security Standards Council

ドキュメントライブラリー



Copyright 2025 © JCDSC

2.適用レベルの分類と準拠確認の手続き

Copyright 2025 © JCDSC

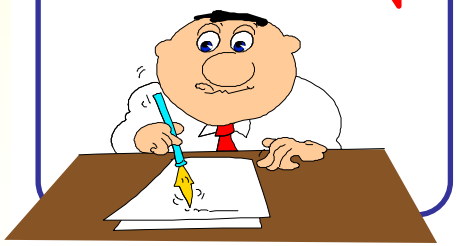
PCI DSSの適用レベル

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			

サービスプロバイダーのレベル・件数は別途定められています。

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
（3か月ごと）
※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

Copyright 2025 © JCDSC

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審査して、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り、AOCの提出を求められた場合、すみやかに提出する必要がある。

Copyright 2025 © JCDSC

QSA（認定審査期間）による訪問審査

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。

PCI Security Standards Council

要件とテスト手順		ガイダンス
3.1 保存されているアカウントデータを保護するためのプロセスとメカニズムが定義され、理解されている。		
定義されたアプローチの要件	定義されたアプローチのテスト手順	目的
3.1.1 要件３で特定されたすべてのセキュリティポリシーと運用手順が • 文書化されている。 • 最新の状態に保たれている。 • 使用されている。 • すべての関係者に周知されている。	**3.1.1** 要件３で特定されたセキュリティポリシーと運用手順が、この要件で指定されたすべての要素に従って管理されていることを確認するために、文書を調査し、担当者にインタビューする。	要件 3.1.1 は、要件３を通して指定された様々なポリシーと手順を効果的に管理し、維持することです。要件３で指定された特定のポリシーや手順を定義することは重要ですが、それらが適切に文書化され、維持され、周知されていることを確認
カスタマイズアプローチの目的		
要件３内の活動を充足するための期待、コントロール、および監視活動が定義され、影響を受ける担当者によって順守されている。すべての支援活動が再現可能であり、一貫して適用され、経営者の意図に適合している。		

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

V4.0以降では、セキュリティ目的を達成するための異なる手法を採用している事業体のために、「カスタマイズアプローチ」という柔軟性を高める仕組みを導入した。

Copyright 2025 © JCDSC

日本国内QSAの一覧と連絡先

JCDSC
Japan Card Data Security Consortium

ＱＳＡ（Qualified Security Assessors:認定審査機関）

日本国内QSAの特色・連絡先一覧表(Excel) 2025.3.1版 ダウンロード>>

PCI DSS準拠の訪問審査を行う、PCI SSCが認定した審査機関(QSA)の一覧表です。
PA-DSSのQSAおよびP2PEのQSAも掲載しています。

- ICMSソリューションズ株式会社 [ICMS Solutions Co., Ltd.]
- NECセキュリティ株式会社 (旧インフォセック) [NEC Security, Ltd.]
- 株式会社 SP・コンプライアンス [SP Compliance Co., LTD]
- NRIセキュアテクノロジーズ株式会社 [NRI Secure Technologies LTD]
- NTTデータ先端技術株式会社 [NTT Data Intellilink Corporation]
- 国際マネジメントシステム認証機構株式会社 [International Certificate Authority of Management System]
- 株式会社GRCS [GRCS Inc.]

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。

※現在時点で免許が有効なQSAであるかは、PCI SSC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/

Copyright 2025 © JCDSC

SAQによるPCI DSS準拠

SAQ（自己問診 = Self Assessment Questionnaire）は、
自社の内部監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。

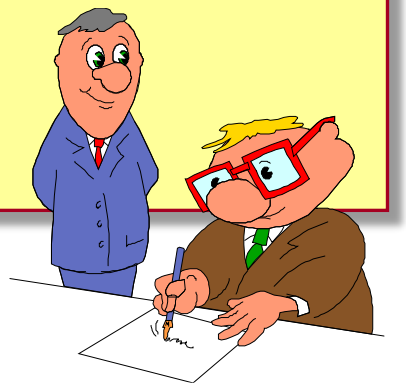
※システム環境により、内部・外部ペネトレーションテストや、アプリケーションぜい弱性検査も求められます。

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等により、必ず提出が必要な場合と、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。

Copyright 2025 © JCDSC

どのタイプのSAQを使えばよいか（1）

加盟店の業態により、使用するSAQにはいろいろなタイプがあります。

P8に案内したPCI SSCのサイトから「SAQの説明書とガイドライン」の日本語版をダウンロードして、どのタイプのSAQを使用すべきか、検討しましょう。サービスプロバイダー用は1種類のみです。

タイプ A すべてのアカウントデータ機能をPCI DSSに準拠した検証済みサードパーティに完全に委託する、カード非提示型加盟店（Eコマースまたは通信販売／電話注文）。加盟店のシステムまたは施設でアカウントデータを電子的に保存、処理、または伝送しない。対面チャネルには適用されない。サービスプロバイダーには適用されない。

タイプ A-EP 決済処理をPCI DSSに準拠した検証済みサードパーティに部分的に委託し、それ自体はアカウントデータを受領しないが、決済取引のセキュリティおよび／または消費者アカウントデータを受領するページの整合性に影響を与えるウェブサイトを持つEコマース加盟店。加盟店のシステムまたは施設でアカウントデータを電子的に保存、処理、または伝送しない。Eコマースチャネルにのみ適用される。サービスプロバイダーには適用されない。

タイプ B 以下のみを使用する加盟店：電子アカウントデータ保存しないインプリンタ、および／または
電子アカウントデータを保存しないスタンドアロン型ダイヤルアップ端末。 Eコマースチャネルには適用されない。
サービスプロバイダーには適用されない。

タイプ B-IP ペイメントプロセッサーにIP接続された、スタンドアロン型のPCIリストに掲載された認可済みPTS（PINトランザクションセキュリティ）POI（加盟店端末装置）デバイスのみを使用する加盟店。電子アカウントデータは保存しない。
Eコマースチャネルには適用されない。サービスプロバイダーには適用されない。

タイプ C インターネット接続された決済アプリケーションシステムを持つ加盟店。電子アカウントデータは保存しない。
Eコマースチャネルには適用されない。サービスプロバイダーには適用されない。

Copyright 2025 © JCDSC

どのタイプのSAQを使えばよいか（2）

タイプ C-VT 孤立したコンピューティングデバイスと安全に接続されたウェブブラウザを使用して、PCI DSSに準拠した検証済みサードパーティの仮想決済端末ソリューションに、キーボードで一度に1件の取引について決済アカウントデータを手入力する加盟店。電子アカウントデータは保存しない。 Eコマースチャネルには適用されない。サービスプロバイダーには適用されない。。

タイプ P2PE 検証済みでPCIリストに掲載されたポイントツーポイント暗号化（P2PE）ソリューションのみを利用する加盟店。平分アカウントデータにアクセスできず、電子アカウントデータを保存しない。 Eコマースチャネルには適用されない。サービスプロバイダーには適用されない。

タイプ SPoC PCI SCC検証済みSPoCソリューションリストに掲載された、セキュアカードリーダーを備える商用オフザシェルフのモバイルデバイス（例：スマートフォン、タブレット等）を使用する加盟店。平分アカウントデータにアクセスできず、電子アカウントデータを保存しない。無人カード提示型、通信販売／電話注文（MOTO）、Eコマースチャネルには適用されない。
サービスプロバイダーには適用されない。

タイプ D（加盟店用） D：上記のタイプの説明に含まれていないすべての加盟店。 サービスプロバイダーには適用されない。

タイプ D（サービスプロバイダー用） ペイメントブランドによってSAQ実施対象と定義されるすべてのサービスプロバイダー。
※ブランドごとのルールにより、SAQでの準拠を認めず、QSA審査が求められる場合があります。

【注】加盟店から委託を受けてカード情報の取扱いやシステム運用を行っている会社は、加盟店自身ではありませんから、SAQはサービスプロバイダー用のタイプDを用いる必要があります。

SAQはタイプD（サービスプロバイダー用）以外は、すべて加盟店のためのものです。

Copyright 2025 © JCDSC

SAQへの記入

業態などの設問に回答を記入し、セCI DSSの要件に対応しているかどうかを回答していきます。そして回答内容に間違いがないことを、経営役員が署名して完成させます。

下は「タイプD 加盟店用」の一例です。

PCI DSS 要件		期待されるテスト	回答 (各要件に対して1つ回答を選んでください) 対応	CCW で対応	該当なし	未テスト	未対応
▪1.2 ネットワークセキュリティコントロール（NSC）が設定され、維持されている。							
1.2.1	NSC ルールセットの構成基準が • 定義されている。 • 実装されている。 • 維持されている。	• 構成基準の調査 • 構成設定の調査	☐	☐	☐	☐	☐
1.2.2	ネットワーク接続及び NSC の構成に関するすべての変更は、要件 6.5.1 に定義された変更管理プロセスに従って承認および管理する。	• 文書化された手順の調査 • ネットワーク構成の調査 • 変更管理記録の調査 • 責任者のインタビュー	☐	☐	☐	☐	☐
	適用に関する注意事項						
	ネットワーク接続の変更には、接続の追加、削除、または修正が含まれる。 NSC の設定の変更には、コンポーネント自体に関連するものと、そのセキュリティ機能の実行方法に影響を与えるものが含まれる。						
1.2.3	カード会員データ環境（CDE）と他のネットワーク（無線ネットワークを含む）間のすべての接続を示	• ネットワーク図の調査 • ネットワーク構成の調査	☐	☐	☐	☐	☐

事業体役員の署名 ↑	*日付：* 2024-05-20
事業体役員名 ： 東京 一郎 / Ichiro Tokyo	*役職：* 代表取締役社長

Copyright 2025 © JCDSC

ASVスキャン および ペネトレーションテスト

No.	PCI要件	頻度	検査名称	内容
①	11.2	3か月ごと	ワイヤレスアクセスポイントの特定・監視	・不正なワイヤレスアクセスに対処する
②	11.3	3か月ごと	外部脆弱性スキャン	・ASVが実施する
③	11.3	3か月ごと	内部脆弱性スキャン	・有資格の内部スタッフが実施する
④	11.4	年1回	外部・内部へのペネトレーション（侵入）テスト	・カード会員データ環境（CDE）の境界全体および重要なシステムを対象とする ・要件 6.2.4に記載された脆弱性を最低限特定するためのアプリケーション層ペネトレーションテスト ・侵入テストの結果および是正活動の結果を少なくとも12か月間保存

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）により実施される必要があります。

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。

Copyright 2025 © JCDSC

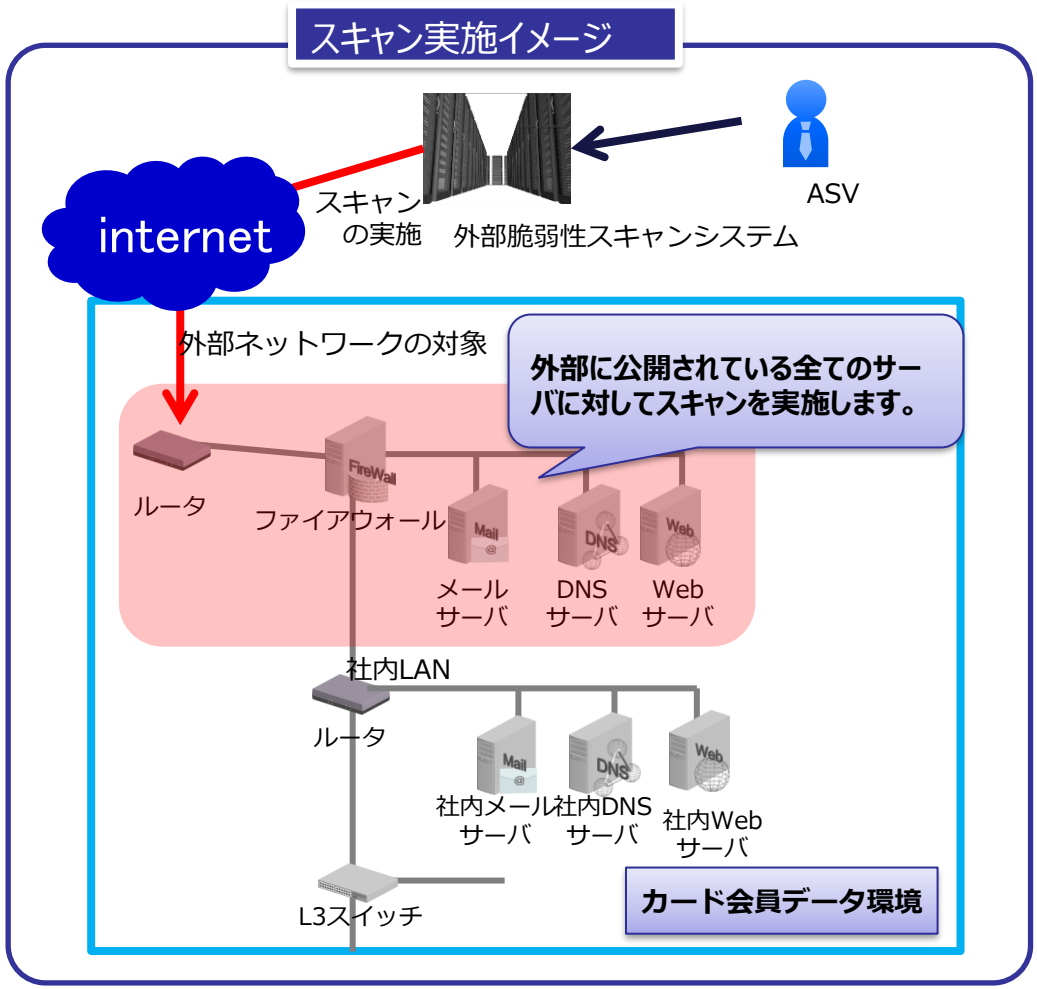
ASVスキャンとは

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11.3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

Copyright 2025 © JCDSC

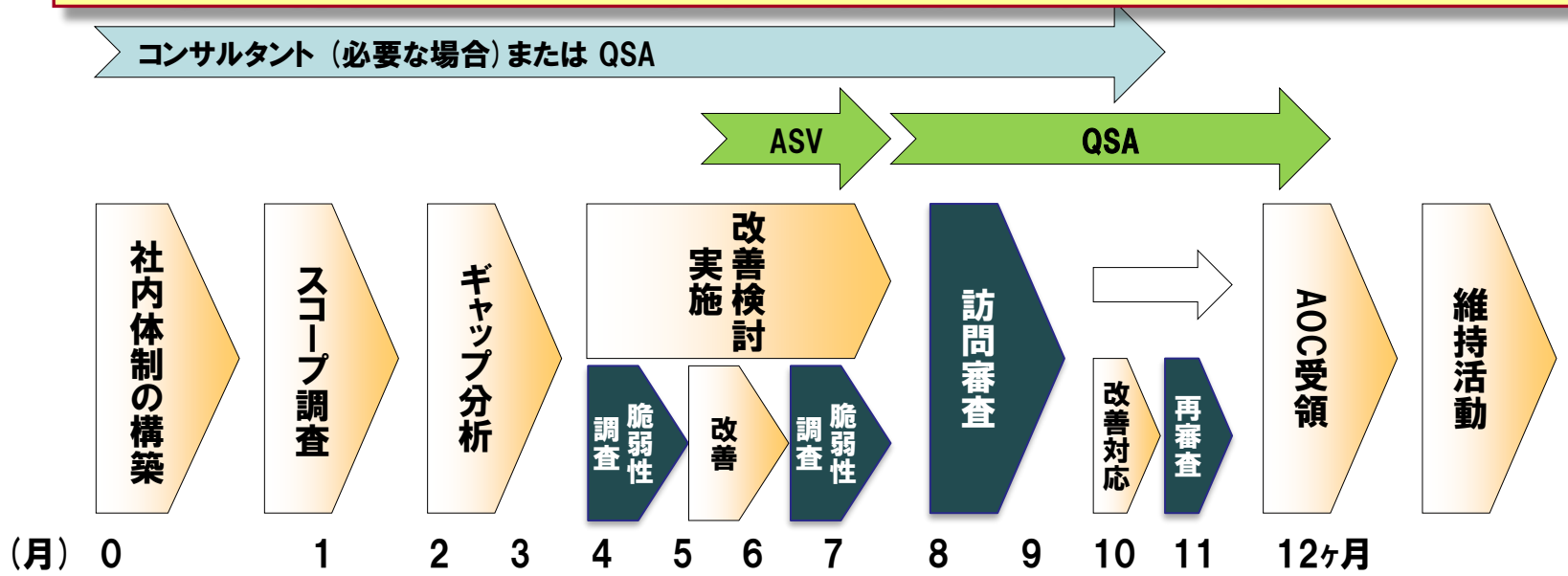
3.準拠に向けた取組みと参考資料

Copyright 2025 © JCDSC

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

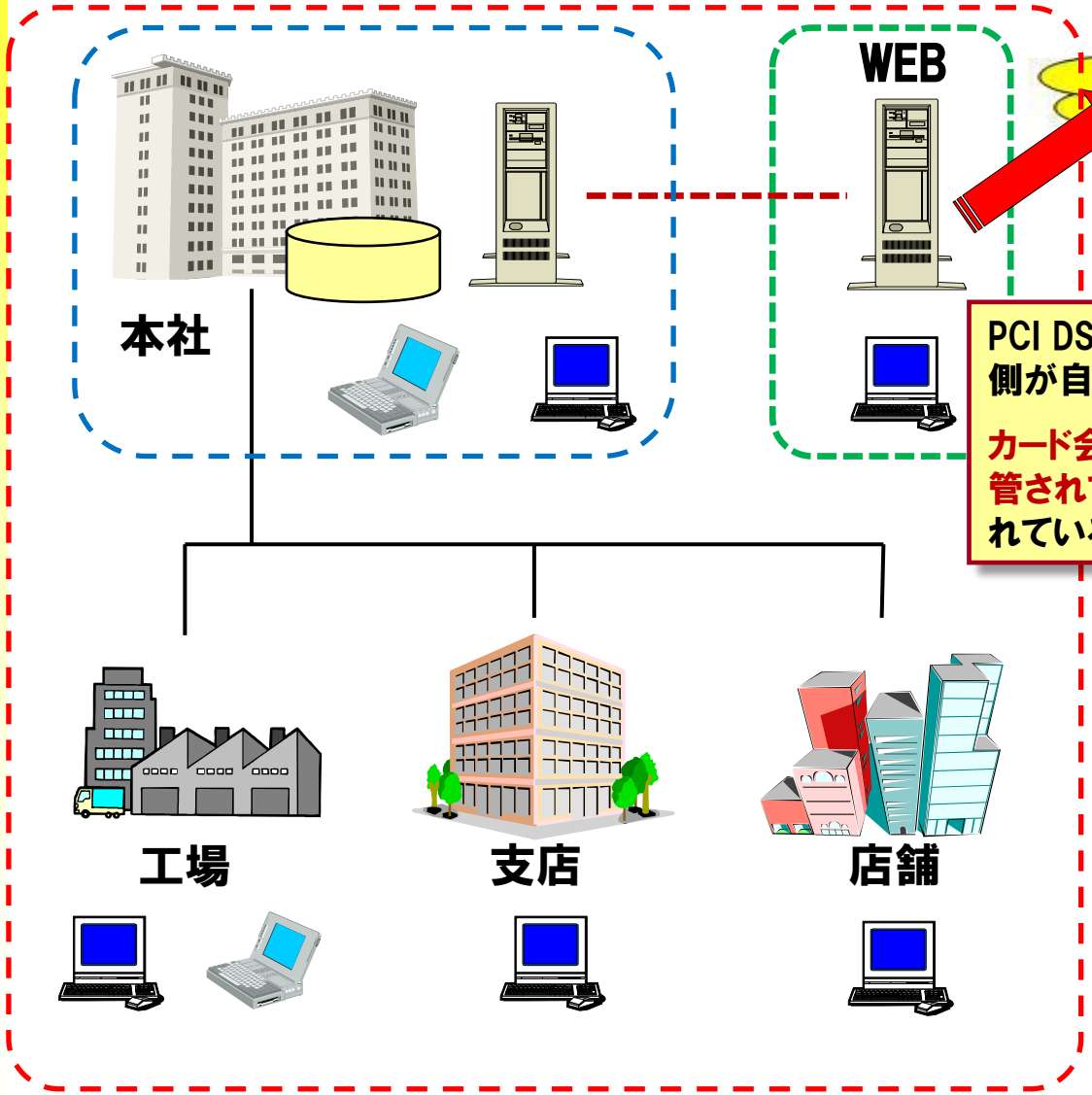


※SAQを用いる場合は、QSAに依頼する必要はありません。

規模やセキュリティ達成状況によって、準拠までの期間や費用に差

Copyright 2025 © JCDSC

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ている環境はすべて対象になります。

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

Copyright 2025 © JCDSC

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？

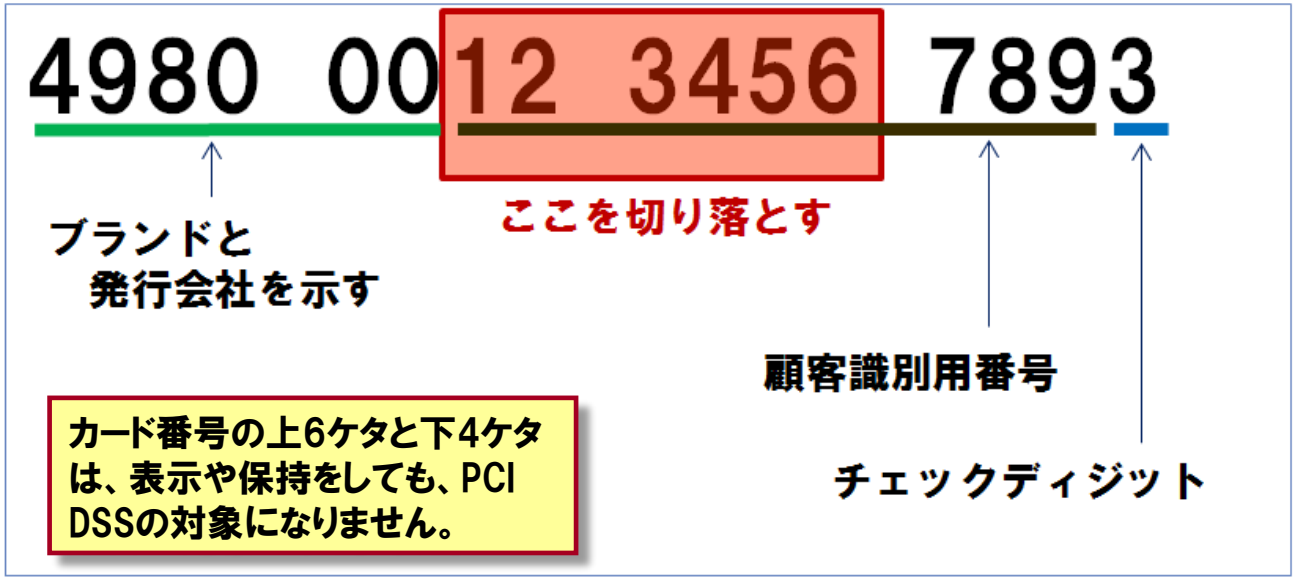
→ そのシステムコンポーネントも、すべて対象です

接続するシステムを限定、分離（セグメンテーション）

Copyright 2025 © JCDSC

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**-****

Copyright 2025 © JCDSC

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。

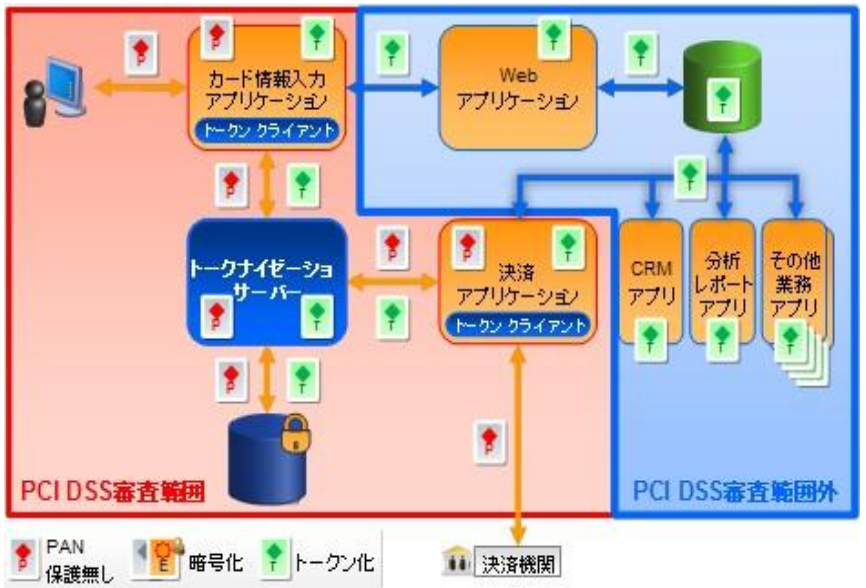
- トークンはカード会員データとしては扱わない
  ※PCI DSSでは暗号化された場合でもカード会員データとして扱う
- 手続きを踏むことで元のデータの参照が可能
- トークナイゼーションの仕組みそのものは検証される必要がある。

・ ※自社の保有するシステム内部でトークン化を
・ 行った場合は、非保持化とは認められない。

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

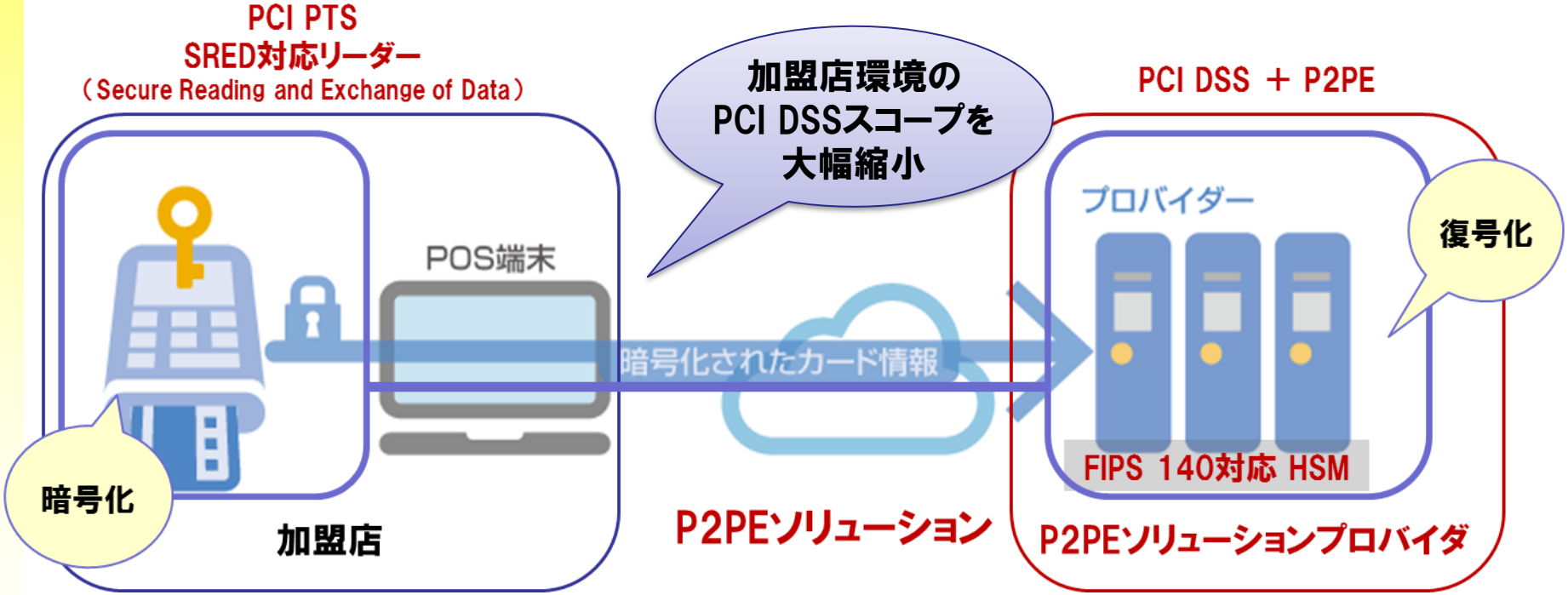


https://www.jcdsc.org/topics/vol02.php

Copyright 2025 © JCDSC

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れば、PCI DSSスコープを縮小できる



出典：PCI DSS徹底解説 / NTTデータ先端技術株式会社

https://www.intellilink.co.jp/article/pcidss/15.html

Copyright 2025 © JCDSC

各種検査会社・コンサル会社の一覧「参考資料集」

JCDSC
Japan Card Data Security Consortium

協議会について
- 日本カード情報セキュリティ協議会とは
  - 概要・ごあいさつ
  - 会員企業一覧
  - 会則
  - 入会案内
- カード業界を取り巻く環境とセキュリティーの重要性

PCI DSS
- グローバルセキュリティ基準 PCI DSSとは
  - 概要
  - 認定取得のメリット
  - 認定取得について
  - 認定審査機関について
  - 導入が必要な企業
  - QSA/ASV 企業一覧
  - PCI DSS準拠への参考資料集
  - 会員専用コンテンツ
- サイトスポンサー

PCI DSS準拠に向けて

PCI DSS準拠をご検討の方へ
参考資料のダウンロード配布を開始いたしました

「PCI DSS準拠に向けて」参考資料集

PCI DSS準拠やカード情報非保持化の検討を開始されたご担当者さまに向けて、当協議会の会員各社から、参考となる情報を集めました。

1. PCI DSS対応ソリューション表 ※

PCI DSSの各要件別に、対応するセキュリティ・ソリューションと特色説明を一覧表に作成しています。

2. PCI DSSコンサル、各種検査実施会社の特色・連絡先一覧表 ※

PCI DSS準拠を支援するコンサル企業、および準拠に要求されている、各種の検査の実施企業について特色や連絡先をとりまとめました。
また、PCI DSS準拠でなく、カード情報非保持を選択する事業者が、「非保持」を

・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準拠を支援するセキュリティ・ソリューションを、要求事項別に一覧表にして掲載しています。

・日本語版PCI DSS基準書と各種タイプ別SAQの入手方法も紹介。

Copyright 2025 © JCDSC

4.クレジットカード・セキュリティガイドラインにおける、JCDSCの役割

Copyright 2025 © JCDSC

JCDSCの役割

割賦販売法の実施基準に位置づけられている、クレジットカード・セキュリティガイドライン【6.0版】（2025年3月改訂・公表）

国内のPCI DSS 認定セキュリティ評価機関（QSA）のほとんどが参加している団体である、日本カード情報セキュリティ協議会（以下「JCDSC」という。）が、PCI DSS準拠の取組をサポートするため、各種資料の提供や相談窓口を設置しており活用されたい。

・2016年の「実行計画」の段階から、現在の「クレジットカード・セキュリティガイドライン」に至るまで、PCI DSSに関する専門団体としてJCDSCが記述されてきました。

PCI DSS準拠を支援するセミナーの開催や、多くの問合せに対応しています。

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

JCDSC
Japan Card Data Security Consortium

Copyright 2025 © JCDSC