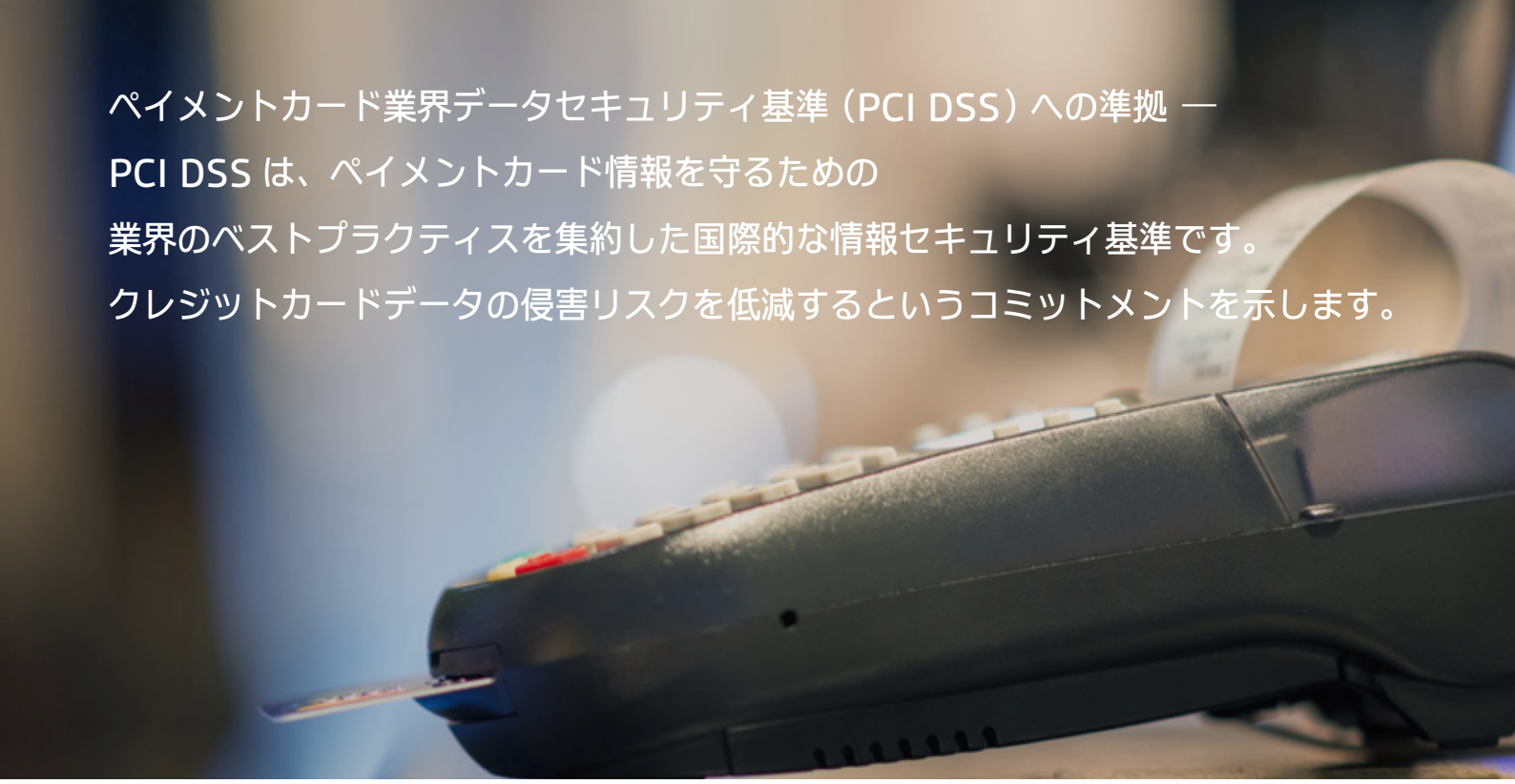
...making excellence a habit.™

ペイメントカード業界 データセキュリティ基準 (PCI DSS) のご紹介

カードデータの保護のために



ペイメントカード業界データセキュリティ基準（PCI DSS）への準拠 —

PCI DSS は、ペイメントカード情報を守るための
業界のベストプラクティスを集約した国際的な情報セキュリティ基準です。
クレジットカードデータの侵害リスクを低減するというコミットメントを示します。

PCI DSS の利点

- 信頼おける組織の証明
- クレジットカードデータの侵害リスクの低減
- 財務リスク及びレピュテーションリスクの低減
- サービス復元における関連コストを最小限に抑える

技術が進歩し続け、新たな支払い方法が定期的に開発される今日の相互接続された世界では、特に財務データなど情報に対するリスクが増加します。

VISA、MasterCard、JCB、AMEX、Discover の専門家が PCI Security Standards Council（PCI SSC）と協力してペイメントカード業界の規格である PCI DSS を開発しました。この規格は、クレジットカードのデータ侵害を低減するための一連のセキュリティ管理策です。

PCI DSS は、サービスプロバイダ、イシュア、アクワイアラ、加盟店など、支払いカードのデータを保存、処理、または伝送する組織にとって、支払いカードのデータが安全であることをステークホルダーに確信させます。これにより、決済カード処理システムに関わる人材、プロセス、技術を組織が考慮するようになります。セキュリティマネジメント、方針、手順、ネットワーク構成、ソフトウェアデザインなどの 12 の主要な要件を多面的に規定しているため、組織は支払いカードデータ周辺にレジリエンス（回復力）を構築できます。

BSI では、PCI SSC 認定監査員が専門知識を活かし、お客様が構築したシステムが PCI DSS の要求事項に準拠しているかを「リスクベース」で評価いたします。

bsi.

PCI DSS への一般的な流れ

ペイメントカードセキュリティについて新たな担当になった、もしくは現在のシステムを強化することになった場合でも、BSI は PCI DSS の理解と実装に役立つ適切なリソースとトレーニングコースをご用意しています。しかし、我々の支援はそこで終わりではありません。お客様のシステムがビジネスに最適な状態を維持しているかどうか確認を行ってまいります。

	お客様が行うべき内容	当社の支援内容
理解と準備	• PCI DSS の規格書をダウンロードし、内容及び事業をどのように改善するか理解を深める • 貴組織のニーズに即した提案を BSI へ依頼する ◎ P2PE 審査サービスもご提供しております。お気軽にお問い合わせください。	• BSI Web サイトにて、FAQ やホワイトペーパー等の情報を提供 **bsigroup.com/ja-JP/** をご覧ください。
準備状況の確認	• PCI DSS 準拠評価の適用範囲を決定する • 組織が、 PCI DSS の原則、及び事業における個人の役割が、規格に対して活動を実施し見直す必要があることを理解しているかを確認する	• PCI DSS に準拠したシステムの構築・導入・運用スキルを身につけられる PCI DSS 研修コース（インハウス研修も実施可）※ ※ PCI DSS 準拠の検討組織を対象に、概要理解のための無料セミナーも随時開催しております。 • BSI ギャップ分析 • PCI DSS の実装をサポートする BSI Entropy™ ソフトウェア
レビューと準拠証明書取得	• BSI に連絡し、自己問診（SAQ）を提出するか、認定セキュリティ評価機関（QSA）の準拠評価を予約する	• SAQ（自己問診）レビュー • BSI 準拠評価 ※ PCI DSS と ISMS（ISO/IEC 27001）の合同審査をご検討のお客様はお問い合わせください。

継続的改善を実施し、エクセレンスを習慣にします。

お客様の行程は、準拠証明書の取得で終了ではありません。
組織のパフォーマンスを最善に保ち、組織を適切に運営できるように支援します。

- 準拠証明書の取得を公表します。
- QSA である BSI は、コンプライアンス維持が確実であるか定期的に準拠評価を行い、継続的改善をサポートします。
- 情報セキュリティのパフォーマンスを継続的に向上させるための知識とスキルを身に付けるよう従業員のトレーニングに投資します。
- BSI のペネトレーションテストと脆弱性スキャンサービスを使用し、システム全体の耐性を確認します。
- BSI Entropy™ Software を使用して、システムの管理とパフォーマンスの向上に役立てます。
- 他のマネジメントシステム規格を統合してビジネス上の利点を最大化することを検討します

PCI DSS と ISMS の合同審査

日本では企業の情報セキュリティの認証制度として ISMS が広く知られ、今日、国内約 5500 社が ISMS の認証を取得しています。ISMS は情報セキュリティの質を維持・管理していく仕組みに主眼が置かれています。これに対して PCI DSS はカード情報保護のために実装レベルの要件が定義されており、互いに相互補完の関係にあると言えます。PCI DSS と ISMS 双方の規格・基準を活用することによって、情報セキュリティレベルをより強化向上することができます。

PCI DSS への準拠及び ISMS の認証を維持するためには、毎年継続的に評価及び審査を受ける必要があります。合同審査を実施することにより、重複項目を避けて審査工数と負荷を低減することができます。例えば PCI DSS に準拠していれば、右表の ISMS の管理策の要件は満たされていると考えられます。(ISMS と PCI DSS の適用範囲によって異なります。)

また、ISMS の認証を取得していれば、PCI DSS の下記の要件の多くの部分は満たされていると考えられます。

要件 12：情報セキュリティに対応するポリシーを維持すること

BSI ジャパンは ISMS において、日本国内 No.1 の認証実績を保持しています。PCI DSS においても 2004 年から VISA 公認の審査機関として認定され、2008 年からは PCI SSC 公認の QSA として、多くの大手決済代行業者、加盟店などで審査実績があります。BSI ジャパンでは情報セキュリティにおけるマネジメントシステム審査の豊富な経験を生かし、ISMS と PCI DSS の同時審査が可能な審査機関として、お客様に付加価値を提供する審査サービスを展開してまいります。

表：ISMS の管理策

A.9.1 **A.9.2** **A.9.4**	アクセス制御に対する業務上の要求事項 利用者アクセスの管理 システム及びアプリケーションのアクセス制御
A.12.1.4	開発環境、試験環境及び運用環境の分離
A.12.2	マルウェアからの保護
A.12.4	ログ取得及び監視
A.12.6.1	技術的ぜい弱性の管理
A.13.1	ネットワークセキュリティ管理
A.14.2.2	システムの変更管理手順
A.14.2.9	システムの受入れ試験

About BSI?

BSI は、組織がベストプラクティスである規格を「卓越した習慣」に変えることを可能にする事業サポート企業です。
一世紀以上にわたり、BSI は、世界中の組織において何が良い行いかというベストプラクティスに挑戦してきました。
193 カ国、86,000 以上のお客様と協力し、自動車、航空宇宙、環境、食品、ヘルスケアなどの分野で
数多くのスキルと経験を持つ真の国際事業を行っています。
規格開発およびナレッジ・ソリューション、保証およびプロフェッショナル・サービスの専門知識によって、
BSI は事業パフォーマンスを向上させ、顧客の持続可能な成長、リスクマネジメント、
そして最終的にはよりレジリエントな企業を支援します。

BSI グループジャパン株式会社
TEL 03-6890-1172　　www.bsigroup.com/ja-JP/

PCI DSS
Payment Card
Industry Data
Security Standard

By Royal Charter