

PCI DSS オンサイト評価のご紹介

PCI DSS とは？

PCI DSS とは、Payment Card Industry Data Security Standard の略称で、ペイメントカードブランド 5 社が展開しているセキュリティプログラムの拠り所となる、**国際的なカード会員データセキュリティ基準**です。

PCI DSS の対象となる企業は、**カード会員データやカード取引情報の保存、処理、伝送を行う全ての加盟店および関連事業者**です。

国内外で PCI DSS の取得を義務付ける動きが進んでおり、カード情報を扱う上で避けて通れない基準の一つとなっています。

PCI DSS 認定の仕組み

QSAC は、カード加盟店及び関連事業者に対して PCI DSS に準拠していることを評価する認定セキュリティ評価機関であり、PCI DSS 評価手順に則ってセキュリティ評価を実施します。

PCI DSS の完全準拠が認められた場合、QSAC は評価対象企業へ **ROC（準拠レポート）** 及び **AOC（準拠認定証明書）** を提出し、そのレポートをもって**評価対象企業は完全準拠を外部へ公表することが可能**となります。

BBSec に在籍している多数の経験と知識を持った QSA により、PCI DSS のオンサイト評価を実施致します。

PCI DSS オンサイト評価の概要

- 準拠基準
Payment Card Industry Data Security Standard Ver3.2.1
- 評価対象
カード会員データ環境におけるネットワーク、サーバ、アプリケーション、物理セキュリティ、カード会員データ取扱業務全般
- 評価項目
全 12 要件（+付属 3 要件）
- 評価手法
①インタビュー ②現地視察 ③システム・設備などの実機確認
④文書・記録類の確認 ⑤準拠レポート（ROC）作成
※適宜サンプリングを実施する。
- 準拠認定証明
準拠認定証明書（AOC）の発行、準拠認定証明ロゴマークの使用許諾

オンサイト評価プランについて

BPO として、一部の要件のみに準拠できれば良いのだが...12要件すべての確認が必要？



準拠はしたいが、価格が高くコスト面で難しい。なんとか安く実施する方法はないか？

多様なニーズに合わせた様々な評価プランをご用意しております。

通常のオンサイト評価では、原則として QSA が現地訪問し12 要件すべての確認を行います。以下のような方法でコンパクトに準拠を目指すことも可能です。

・ Value オンサイト評価

キックオフから報告会まで、すべての作業をリモートで完結させる評価です。QSA による現地訪問を行わない代わりに、低価格でのご提供が可能です。

・ データセンター向けオンサイト評価

カード会員データを扱う顧客を持つデータセンター向けの評価です。要件 9（物理セキュリティ）及び要件12（ポリシー、教育、インシデント対応）に関する要件を中心に、対象を絞って確認します。

■ まずは御相談ください。お問合せはこちら。



03-6433-3116 (受付時間 平日9:30~17:00)

mailto:Consulting-Sales@bbsec.co.jp

※本カタログは2020年9月現在のものです。これらは予告なしに変更する場合がございますので予めご了承ください。

※記載の会社名、商品およびサービスの名称は、当社ならびに各社の商標または登録商標です。



株式会社ブロードバンドセキュリティ



■ 本 社
〒160-0023 東京都新宿区西新宿8-5-1 野村不動産西新宿共同ビル4F TEL: 03-5338-7425 FAX: 03-5338-7427
URL : <https://www.bbsec.co.jp/>