PCI DSS準拠と運用
簡単ガイド
～ICMSのQSAが支援します～

国際マネジメントシステム認証機構
International Certificate Authority of Management System

PCI DSS準拠・運用の流れ

Phase1: PCI DSSに関する教育

▼

Phase2: 対象範囲の策定（人とシステム）

▼

Phase3: GAP分析

▼

Phase4: 改善

▼

Phase5: 予備調査

▼

Phase6: PCI DSSオンサイト監査

▼

Phase7: 運用

PCI DSS業務
運用サイクル

ICMSは安全なクレジット
カード社会を目指しています。

国際マネジメントシステム認証機構
International Certificate Authority of Management System

Phase1
PCI DSSに関する教育

対象担当者全員の教育は必須。

重要

関連する全ての人がPCI DSSの概念とカードデータの重要性を理解すること。

※教育は要件12.6を満たす事にもなります。

問題　PCI DSSの仕組み、要件が分かりづらい。
そもそも何故必要なの？

解決　QSAによるオンサイト実務研修。または
QSA監修によるWeb学習。組織全体でPCI DSSの主旨を理解する。

ポイント
PCI DSSは"人"が大事

国際マネジメントシステム認証機構
International Certificate Authority of Management System

Phase2

対象範囲の策定（人とシステム）

次にPCI DSSの対象範囲を決めます、最も重要！！

重要

適切な対象範囲の策定。

問題　対象範囲が広くなり設備投資と維持に多大な費用が発生、準拠までの準備に長期間必要となり運営は複雑化した。

解決　**ビジネス主体**で**QSA**が対象範囲を確認。コスト及び期間を最小限で策定。オンサイト監査での対象範囲の**出戻りなし。**

ポイント

人的投資、設備投資を適切に
必要最小限に

国際マネジメントシステム認証機構
International Certificate Authority of Management System

Phase3　GAP分析

いざ現状をPCI DSS要件でチェック!

重要

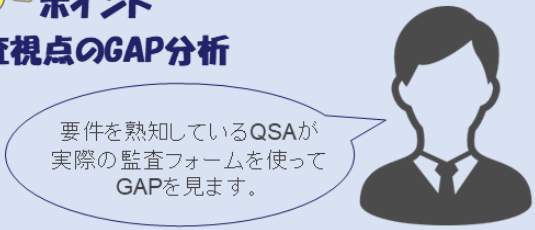
現状とのギャップを適切に行う。

問題　分析に要件の正確な理解、多大な時間とコストが求められる。

解決　QSAによる実際の監査報告書を用いた適切なGAP分析。

ポイント

監査視点のGAP分析



国際マネジメントシステム認証機構
International Certificate Authority of Management System

Phase4 改善

GAP分析をもとに組織に適した構築、再構築を行う。

重要

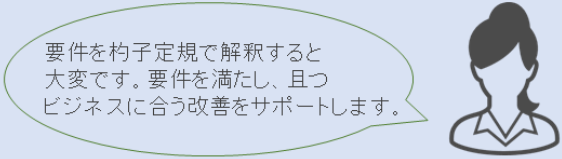
「ビジネスに適した」セキュアなカード会員データ環境の構築と運用。

問題 改善に要件の専門的な知識、多大な時間とコストが求められる。最適な実装及び代替コントロールが分からない。

解決 直接QSAに確認

ポイント

設備投資に無駄なく、運用に無理なく



国際マネジメントシステム認証機構
International Certificate Authority of Management System

Phase5　予備調査

監査直前のシミュレーション。最終調整に向けて。

重要

構築した内容が実運用できているかを実際の監査視点で最終確認

問題　Phase4 改善の段階では未明だった、想定範囲外なところからカード会員番号が発見された。

解決　QSAによる模擬監査を実施。カード会員データ検出ツールで徹底チェックを行う。

ポイント

ビジネス主体の範囲とカード会員データ環境は適切だったか最終確認

PAN: カード会員番号
CDE: カード会員データ環境

国際マネジメントシステム認証機構
International Certificate Authority of Management System

Phase6
PCI DSSオンサイト監査

対象範囲：全てのカード会員データ環境とそれらに接続されるネットワークコンポーネント、サーバー、アプリケーション、ならびにカード会員データが取り扱われる全ての拠点。

監査サイクル：年次

監査手法：オンサイト監査

監査項目数：12要件/約400項目

項目毎に準拠/不準拠を判断

不適合への対処は、是正の目標期日を明確にし、必要に応じフォローアップ監査を実施

代替策による対応：

オリジナルの要件に準拠できない場合、理由と代替策により目的が達成される手段を文書化し「準拠に関するレポート（ROC）」と共に提出

ポイント

事前の業務支援で出戻りなし最少コストで円滑な監査

Phase7　運用

90日毎パスワードの変更、脆弱性スキャン、ペネトレーション等々、
日々PCI DSS要件を満たす運用

重要

準拠したPCI DSSの「要件を満たす運用」が実施出来ているか定期的に確認

問題

①準拠後の運用が出来ない。
②バージョンアップで変更した要件にどう対処すればいいか分からない。

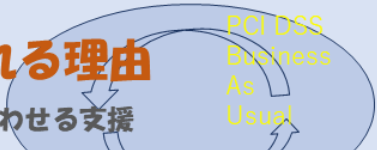
解決

①定期的に運用チェック。不備をただちにカバー。
②QSAに直接確認

ポイント
日々の運用でお客様の資産を守る！

国際マネジメントシステム認証機構
International Certificate Authority of Management System

ICMS 当社が選ばれる理由



ビジネスに規格を合わせる支援

日々組織とデータを守るPCI DSS。ビジネスの負担にならない準拠と運用をICMSはサポートします。
教育から予備調査、監査、監査後の運用まで、現役QSAが信頼性の高い、価値ある価格でカード会員データ環境の実現を支援します。
ICMSは2008年より日本国内では先駆的にPCI DSS監査を開始しました。大手の決済代行会社を中心に約220社以上（2020年11月現在）と卓抜した、国内No.1クラスの監査実績を持ちます。
その豊富な経験で培われた監査ノウハウを発揮し、それぞれのお客様立場（加盟店、決済代行事業者等のサービスプロバイダ、アクワイアラ等）のビジネスに適合するように、支援します。規格に合わせるのではなく、**ビジネスに規格を合わせる支援**を行います。監査実績を長年積むICMSの最大の特徴といえます。
ICMSの準拠支援サービスは、お客様のご要望に応じて一部、或いは一括と提供が可能です。弊社のQSA監修によるPCI DSS教育eラーニングを合わせてご利用いただく事で、運用をより早く定着させる効果を期待できます。

お問合せ・ご相談には、 QSA の資格を持つ営業が対応致します。右記までお気軽にお問合せ下さい。

国際マネジメントシステム認証機構
International Certificate Authority of Management System

ICMS
3大セキュリティ監査サービス

1. PCI DSSオンサイト監査
2. ISMS/JIS Q27001認証審査
3. PCI DSS監査とISMS審査のブリッジ審査

重複する部分の監査を一本化し、工数の低減と受審組織の負担を軽減します。

ICMSについて　～セキュアな未来を創造する～
国際マネジメントシステム 認証機構株式会社
略称：ICMS（International Certificate authority of Management System Co.,Ltd.）
1999年設立。2003年JIPDECから認定を受けたISO27001/JISQ27001審査認証機関としてISMS審査事業、2008年PCI SSCの認定セキュリティ評価機関（QSAs）としてPCI DSS監査事業を始めました。規格の制定早期より携わる審査スキルを強みとし、ITエンジニアスキルをベースとした審査・監査事業を中心に、情報セキュリティ関連の教育、サービスを提供しています。

お問合せ
国際マネジメントシステム認証機構株式会社（ICMS）
TEL: 0120-796-115　Mail: suishin@icms.co.jp
URL: https://www.icms.co.jp/　Twitter: @iCMS_JP
〒141-0021　東京都品川区上大崎 2-24-11　目黒西口 M2 号館　5F

本資料の冊子版(A6 サイズ)を無料配布しております。ご希望の方はお問い合わせ下さい。

国際マネジメントシステム認証機構
International Certificate Authority of Management System

ICMSのセキュリティサービス

審査/監査

■ISMS、ISMSクラウドセキュリティ
■PCI DSS、PCI P2PE、PCI 3DS、PCI PIN（QPA）

国内の主要インターネット決済代行事業者や金融系をはじめ幅広い業界でのオンサイト監査実績を持つ。国内最多クラスの実績・220社以上(2020年11月現在)。

実績の一部はWebに公開されています。

ソリューション

■PCI DSS/P2PE 準拠支援、SAQ策定支援
■SAQ AOC署名サービス
■PCI DSS セキュリティサービス（診断）
■Wi-Fiセキュリティ診断サービス
■端末セキュリティHysolate Workspace
■カード情報セキュリティ支援サービス

教育

■PCI DSS eラーニング(v3.2.1)
■ISMS/PCI DSS トレーニング
■書籍 PCI DSS Version3.2徹底解説

お問合せ
国際マネジメントシステム認証機構株式会社（ICMS）

国際マネジメントシステム認証機構
International Certificate Authority of Management System

PCI DSS準拠のコツ

国際マネジメントシステム認証機構
代表取締役社長
PCI DSS 上級QSA 監査員
ISO27001 上級主任審査員
上野 洋一（Twitter: @iCMS_JP）

PCI DSS準拠をするには、コストがどの位掛かるのと良く聞かれます。この明確な回答は正直難しいです。なぜ？
基本、監査にはオンサイト監査に掛かる費用にプラスしてシステムの追加や改修などに対するコストが掛かることになりますが、このシステム投資費用の見積もりが難しいのです。
自社の投資対効果を計るには、PCI DSS全体と各要件の目的と意味を理解し、ベンダーやコンサルタントの提案の妥当性を判断することが最重要課題です。
PCI DSSを準拠する皆様にお願いしたいことは、規格解釈を外部に頼るのではなく、組織で正しく理解し対応を検討することです。
ICMSは、その組織のお悩みを解決する各種メニューを用意しました。また、今無いメニューでも豊富な監査実績から組織様毎に合ったサービスを提供することが可能ですので、何でも相談してください。
ICMSは、2008年からPCI DSS監査を開始し9年の月日が経過しました。その間、2012年ならびに2015年にPCI SSCによるQSAとしての品質保証プログラムを経て、その監査内容および各種レポートの記載についてチェックを受け、日々改善を図っています。
今後もPCI SSCとの連携を深め、全てのクレジットカードセキュリティを守るためにPCI P2PEも既にサービスを開始しており、今後PA-DSSなど新しい規格にも対応していく予定です。ぜひこれからも、ICMSにご期待ください。

PCI SSC：米国PCIデータセキュリティ基準審議会