PCI DSS

SAQ（自己問診）

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: SAQタイプと対象範囲の決定

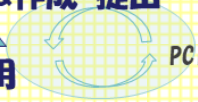
Phase3: GAP分析

Phase4: 改善

Phase5: 予備調査

Phase6: SAQ作成・提出

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重要。

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。

PCI SSC公式ホームページ（日本語版）
https://ja-pci.onelink-translations.com/minisite/env2/

ポイント

PCI DSSは"人"が大事

ICMSの*QSA監修による教材でカード会員データの重要性、要件について学びます。

*QSA：PCI SSC認定監査員

ICMS PCI DSS 教育eラーニング

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

Phase2
SAQタイプと対象範囲の決定

カード会員データを保存、処理または送信に関わる人とシステムを確認。

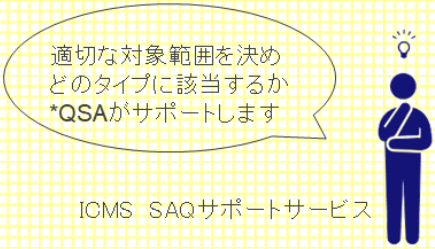
重要

該当する適切なSAQタイプを判断

タイプ（項目数）	説明
A (22)	カードを提示しない（電子商取引または通信販売）加盟店で、カード会員データのすべての処理はPCI DSS認定の外部に委託されている。対面式の加盟店に適用されることはない
A-EP (193)	カードを提示しない（電子商取引または通信販売）加盟店で、支払ページを除くカード会員データのすべての処理はPCI DSS認定の外部に委託されている。対面式の加盟店に適用されることはない
B (41)	カード会員データを電子形式で保存しない、インプリントまたはスタンドアロン型のダイアルアップ端末のみの加盟店。インターネット加盟店に適用されることはない
B-IP (88)	カード会員データを電子形式で保存しない、IP経由で接続されているスタンドアロン型PTS承認の加盟店端末装置(POI)（SCRを除く）のみを使用

SAQタイプ（つづき）

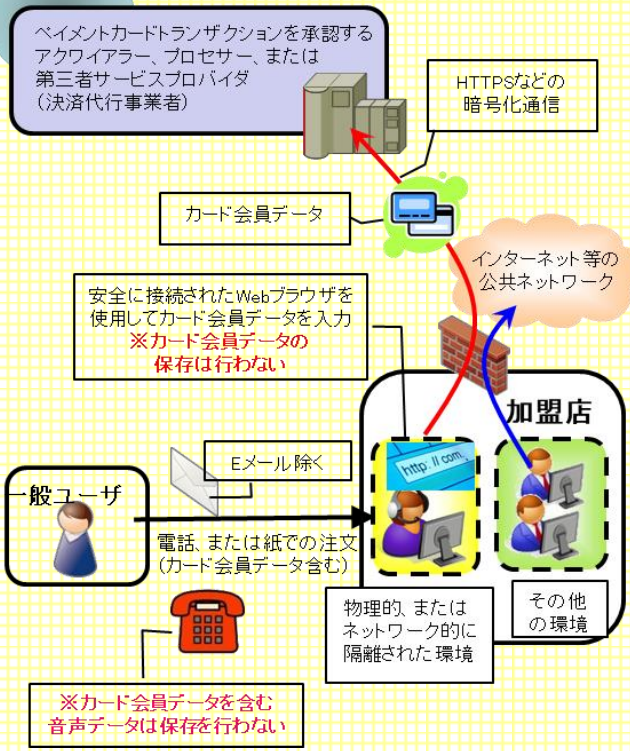
タイプ (項目数)	説明
C (162)	カード会員データを電子形式で保存しない、インターネットに決済アプリケーションシステムを接続する加盟店
C-VT (85)	カード会員データを電子形式で保存しない、Webベースの仮想端末のみを使用する加盟店
D(加盟店)(331)	（上記のSAQ A-Cの説明に含まれない）他のすべての加盟店
D (サービスプロバイダ)(369)	自己問診を行なうサービスプロバイダ



ICMS　SAQサポートサービス

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

SAQ 一例：C-VT 図解


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
（決済代行事業者）
HTTPSなどの
暗号化通信
カード会員データ
インターネット等の
公共ネットワーク
安全に接続されたWebブラウザを
使用してカード会員データを入力
※カード会員データの
保存は行わない
加盟店
Eメール除く
一般ユーザ
電話、または紙での注文
（カード会員データ含む）
物理的、または
ネットワーク的に
隔離された環境
その他
の環境
※カード会員データを含む
音声データは保存を行わない

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。

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。

監査視点のGAP分析で
改善は設備投資に無駄なく、
運用に無理なく。

ICMS SAQサポートサービス

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

準拠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の最終確認

PANがCDE外で残ってないか?

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

想定外なところでPANが発見されるケースが多々あります。カード会員データ検出ツールで徹底調査を行います。

ICMS　カード会員データ検出サービス

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

Phase6 SAQ作成・提出

いざPCI DSS準拠へ！

SAQ、準拠証明書を完成し、提出。

Phase7 運用 日々PCI DSS要件を満たす運用を。

1. 定期に運用チェックし、不備をただちにカバーする。
2. ベストプラクティスやバージョンアップで変更した要件に対処する。

重要

日々の運用でお客様の大切な資産を守る！

ICMSのQSAがオンサイト監査を実施し、準拠証明書（AOC）を発行します。ICMS発行の認証マークでカード情報の安全性のPRができます。

ICMS SAQ AOCサービス

国際マネジメントシステム認証機構

International Certificate Authority of Management System

ICMS SAQ関連サービス

SAQ策定支援サポートメニュー
～ICMSのQSAが支援します～

策定はほぼ自社で可能、少しのサポートが必要！

1.SAQ QAサービス
QSAによるメールでのQA対応

要所要所QSAの確認がほしい

2. SAQ アドバイザリサービス
QSAによる電話、メールでのQA対応＋訪問１回/月

組織に無理なく最適な準拠と運用を目指したい

3. SAQサポートサービス
QSAによる電話・メールでのQA対応 ＋ 訪問、範囲策定支援、GAP分析、改善支援

SAQ AOCサービスICMSのQSAがオンサイト監査を実施し、準拠証明書(AOC)とICMSの認証マークを発行します。

カード会員データ検出サービスPCIに特化してQSAが開発した業界トップレベルのカード会員データ検出ツールにより、スキャンを行います。

eラーニングPCI DSSの抄訳に沿った前文・全12要件をカバーし、各要件のポイントに加えシステム図解やテストが含まれるICMSのQSA監修の実用的な教材です。

PCI DSS教育研修PCI DSSとは、カード会員データの重要性、SAQの概説をQSAが分かり易く説明します。

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

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)の送付を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

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

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