Deloitte.
デロイト トーマツ

PCI DSS準拠体制構築支援サービス

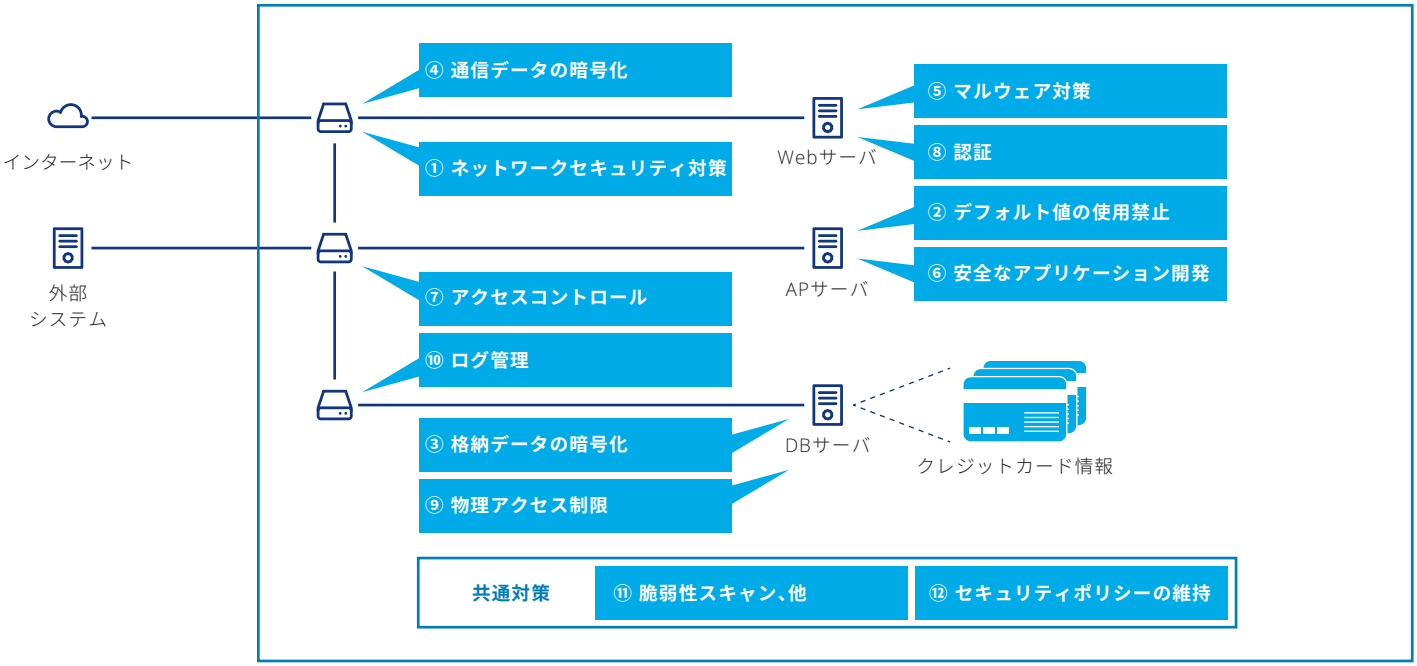
クレジットカード情報の安全管理に向けたアプローチ

PCI DSSとは

PCI DSS（Payment Card Industry Data Security Standard）は、クレジットカード情報を安全に取り扱うことを目的として策定された、クレジットカード業界のセキュリティ基準です。PCI DSSは、クレジットカードブランド5社（American Express、Discover、JCB、MasterCard、VISA）が共同で設立したPCI SSC（Payment Card Industry Security Standards Council）によって策定され、最新のセキュリティ動向を踏まえ定期的に改訂されています。
PCI DSSは、クレジットカード情報を取り扱うすべての事業者を対象としており、クレジットカード会社や決済代行事業者（PSP: Payment Service Provider）だけではなく、カード決済を行っている加盟店も対象となる可能性があります。

PCI DSSの対象となるシステム範囲

情報システムにおいて、クレジットカード情報の取り扱い（保存、処理または送信のいずれか1つでも）が行われる範囲全体がPCI DSSの対象となります。対象範囲内のシステムコンポーネント（サーバ、ネットワーク機器等）には、PCI DSSで定められた12要件（約400項目）のセキュリティ対策を施す必要があります。



※ PCI DSSに基づくセキュリティ対策の例（数字は要件番号）

日本におけるPCI DSSを取り巻く状況

2016年2月、クレジット取引セキュリティ対策協議会より『クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画 -2016-』が公表されました。この実行計画において、各事業者には事業形態に応じて「クレジットカード情報の非保持化」または「PCI DSS準拠」を実施することが求められています。

対象	求められる対応（概要）	対応期限
加盟店（EC）	カード情報の非保持化またはPCI DSS準拠	2018年3月
加盟店（対面）		2020年3月
カード会社（イシュアー／アクワイアラー）、PSP	PCI DSS準拠	2018年3月

※PCI DSS準拠の検証方法としては、クレジットカード情報の取扱形態や規模によって、QSAによる訪問審査、または、自己問診による方法があります。

PCI-DSS準拠体制構築に向けたデロイト トーマツ グループのアプローチ

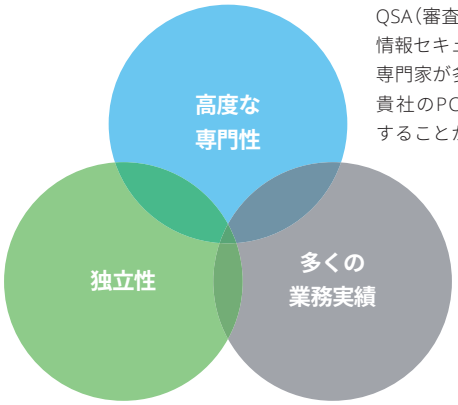
デロイトの方法論に基づいたPCI DSS準拠体制構築フレームワークを活用し、貴社のPCI DSS準拠活動を支援します。
貴社のご要望に応じて、フルオーダーメイドによる最適なサービス提供が可能です。

	①準拠対象範囲の策定	②ギャップ分析と改善策の策定	③改善策の 実行	④本審査
目的	✓ PCI DSS準拠対象とする業務およびシステムを特定する	✓ 現行システムのPCI DSS要件とのギャップを分析し、改善策を策定する	✓ 改善策に基づき、システム改修および文書化（規程、マニュアル等）を行う	✓ QSAによる訪問審査、ASVによるスキャンを受ける
主な作業	✓ 業務・システム情報の整理 ✓ 審査機関の選定 ✓ 準拠スコープの策定	✓ ギャップ分析 ✓ 改善策の検討 ✓ 改善計画の策定 ✓ 製品・ソリューションの選定	✓ システム基盤改修 ✓ システム運用変更 ✓ 文書化	✓ 本審査対応 ✓ 証跡等の準備 ✓ 予備審査対応（必要な場合）
デロイトトーマツグループによる支援例	✓ 担当者向け教育 ✓ 準拠スコープの策定 ✓ 審査機関の選定 ✓ 準拠プロジェクト管理 ✓ 社内体制の構築	✓ ギャップ分析の実施 ✓ 改善策の策定 ✓ 準拠スケジュールの策定 ✓ 製品・ソリューションの選定	✓ 規程文書の作成・修正 ✓ システム改修に関する助言 ✓ 改善状況の評価・レビュー ✓ 代替コントロールの検討 ✓ 改善プロジェクトの進捗管理	✓ 審査立会い ✓ 審査フォローアップ ✓ 審査結果のマネジメント報告 ✓ 継続準拠に向けた方針検討 ✓ 予備審査の実施

※ 当社は、PCI DSS審査（QSA審査）は実施しておりません。

デロイト トーマツ グループの強み

情報セキュリティの専門性に特化したコンサルティングファームとして、単なるPCI DSS認証取得にとどまらない、貴社の情報セキュリティガバナンスの継続的改善に向けた取り組みを支援します。



QSA（審査員）資格を保有するコンサルタントをはじめ、情報セキュリティおよび情報システムの各分野における専門家が多数在籍しています。
貴社のPCI DSS準拠活動に応じて、幅広い知見を提供することが可能です。

有限責任監査法人トーマツを母体とするコンサルティングファームとして、独立性、客観性を重視します。特定の製品およびソリューションに偏ることなく、常に貴社にとっての利益を最優先すべく対応します。

クレジットカード会社、加盟店に対する多数の業務提供実績を有しており、過去の事例において検証済みの様々なナレッジを提供することが可能です。

デロイト トーマツ リスクサービス株式会社

本　社　〒100-0005　東京都千代田区丸の内3-3-1 新東京ビル　Tel:03-6213-1300
名古屋　〒450-6337　愛知県名古屋市中村区名駅1-1-1 JPタワー名古屋　Tel:052-565-5950

2016.10_0049