| | 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<br>✓ 審査機関の選定<br>✓ 準拠スコープの策定 | ✓ ギャップ分析<br>✓ 改善策の検討<br>✓ 改善計画の策定<br>✓ 製品・ソリューションの選定 | ✓ システム基盤改修<br>✓ システム運用変更<br>✓ 文書化 | ✓ 本審査対応<br>✓ 証跡等の準備<br>✓ 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<br>✓ 準拠スコープの策定<br>✓ 審査機関の選定<br>✓ 準拠プロジェクト管理<br>✓ 社内体制の構築 | ✓ ギャップ分析の実施<br>✓ 改善策の策定<br>✓ 準拠スケジュールの策定<br>✓ 製品・ソリューションの選定 | ✓ 規程文書の作成・修正<br>✓ システム改修に関する助言<br>✓ 改善状況の評価・レビュー<br>✓ 代替コントロールの検討<br>✓ 改善プロジェクトの進捗管理 | ✓ 審査立会い<br>✓ 審査フォローアップ<br>✓ 審査結果のマネジメント報告<br>✓ 継続準拠に向けた方針検討<br>✓ 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。