



## PCI DSS準拠体制構築支援 クレジットカード情報管理へのアプローチ

クレジットカードが広く利用されている現在の社会において、情報漏えい等を防ぐため、クレジットカード情報を取り扱う事業者における情報セキュリティの確保は重要な事項です。

そのためには、クレジットカード情報を保存、処理、伝送するすべての事業者がクレジットカード業界の情報セキュリティ基準であるPCI DSSに準拠することが求められています。対象となる事業者には、例えば、クレジットカードの加盟店やデータ処理事業者等が挙げられます。

トーマツの専門家が独自のアプローチで管理体制の構築を支援します。

### PCI DSSとは

PCI DSS (Payment Card Industry Data Security Standards) は、国際カードブランド5社 (American Express, Discover Financial Services, JCB International, MasterCard Worldwide, VISA Inc.) が共同で設立したPCI SSC (Payment Card Industry Security Standard Council) が、クレジットカード情報の保護のために制度運営しているクレジットカード業界の情報セキュリティに関する基準です。

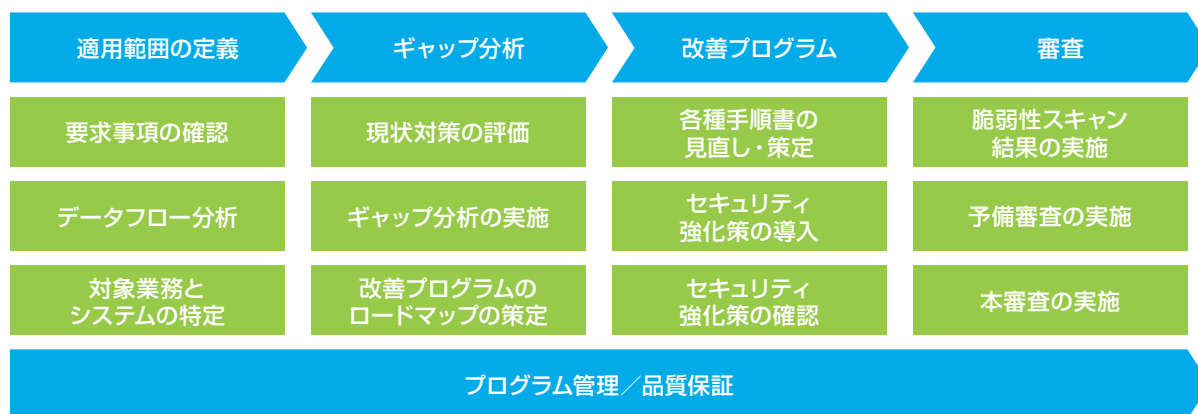
### クレジットカード情報管理に対するアプローチ

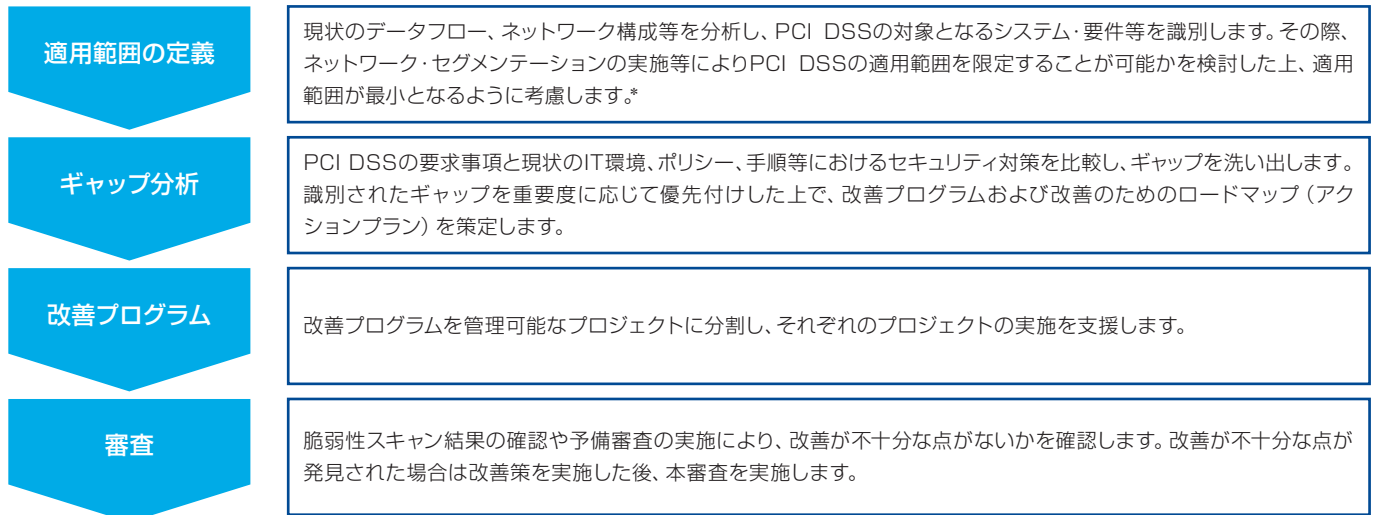
PCI DSSでは、クレジットカード情報と取引情報を保護するために、12のセキュリティ要件が定められています。これらは次に示す6カテゴリに分類することができます。

- ・安全なネットワークの構築と維持
- ・カード会員データの保護
- ・脆弱性管理プログラムの整備
- ・強固なアクセス制御手法の導入
- ・ネットワークの定期的な監視およびテスト
- ・情報セキュリティポリシーの整備

PCI DSSの要求事項はさまざまな分野にわたっており、その対策は、人、プロセス、IT、ガバナンスに関連します。これらは組織全体に関わる問題であり、組織全体で取り組む必要のあるものです。

### トーマツのアプローチ





\*PCI DSSは、クレジットカード情報が保管、処理、あるいは伝送されている箇所のみが適用範囲となります。適切なネットワーク・セグメンテーションの実施や、業務上必要のないクレジットカード情報の保管を行わない等により、PCI DSSの適用範囲を限定し、効率的に導入、運用していくことが可能となります。これらの対応策は、改善プログラムにて実施します。

## トーマツの強み

### 広範囲にわたる深いスキル

トーマツにはPCI DSS準拠プログラムにおいて直面する問題に対処するための広範囲にわたる深いスキルを持った専門家を多数擁しています。

### 現実的なセキュリティ改善策導入支援の経験

トーマツは、人、プロセス、ITを含む複雑なセキュリティ改善プログラムに関する多くの経験と実績を有しています。

### 綿密なプログラム管理のスキル

トーマツでは数多くのプログラム管理の経験を持った専門家がプロジェクトチームを組成し、サービスを提供します。

## 改善プログラム成功のヒント

クレジットカード情報管理体制の改善プログラムを成功させるためには、例えば、次のような事項を考慮することが重要です。

- ・経営陣の積極的な関与やステークホルダーの賛同
- ・ITだけにフォーカスするのではなく、人やプロセスの要素も考慮した対策
- ・さまざまな能力を持ったメンバーによるチーム編成
- ・深い知識や経験を持ったコンサルタントの活用
- ・業務上必要のないクレジットカード情報を削除することによるPCI DSS準拠プログラムの適用範囲の縮小

## 国内ネットワーク

### 有限責任監査法人トーマツ

東京 〒100-0005 東京都千代田区丸の内3-3-1 新東京ビル Tel:03-6213-1112  
 大阪 〒541-0042 大阪府大阪市中央区今橋4-1-1 淀屋橋三井ビルディング Tel:06-4560-6021  
 名古屋 〒450-8530 愛知県名古屋市中村区名駅3-13-5 名古屋ダイヤビルディング3号館 Tel:052-565-5517  
 福岡 〒810-0001 福岡県福岡市中央区天神1-4-2 エルガーラ Tel:092-751-1517

### 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

トーマツグループは日本におけるデロイト トウシュ トーマツ リミテッド（英国の法令に基づく保証有限責任会社）のメンバーファームおよびそれらの関係会社（有限責任監査法人トーマツ、デロイト トーマツ コンサルティング株式会社、デロイト トーマツ ファイナンシャルアドバイザー株式会社および税理士法人トーマツを含む）の総称です。トーマツグループは日本で最大級のビジネスプロフェッショナルグループのひとつであり、各社がそれぞれの適用法令に従い、監査、税務、コンサルティング、ファイナンシャルアドバイザー等を提供しています。また、国内約40都市に約6,800名の専門家（公認会計士、税理士、コンサルタントなど）を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はトーマツグループWebサイト（[www.tohmatsu.com](http://www.tohmatsu.com)）をご覧ください。

Deloitte（デロイト）は、監査、税務、コンサルティングおよびファイナンシャル アドバイザーサービスを、さまざまな業種にわたる上場・非上場のクライアントに提供しています。全世界150か国を超えるメンバーファームのネットワークを通じ、デロイトは、高度に複合化されたビジネスに取り組むクライアントに向けて、深い洞察に基づき、世界最高水準の陣容をもって高品質なサービスを提供しています。デロイトの約200,000人におよぶ人材は、“standard of excellence”となることを目指しています。

Deloitte（デロイト）とは、デロイト トウシュ トーマツ リミテッド（英国の法令に基づく保証有限責任会社）およびそのネットワーク組織を構成するメンバーファームのひとつあるいは複数指します。デロイト トウシュ トーマツ リミテッドおよび各メンバーファームはそれぞれ法的に独立した別個の組織体です。その法的な構成についての詳細は [www.tohmatsu.com/deloitte/](http://www.tohmatsu.com/deloitte/) をご覧ください。