cpl.thalesgroup.com

THALES
Building a future we can all trust

タレス SafeNet Trusted Accessによる PCI DSS 4.0への対応

PCI DSSとは？

PCI DSS（Payment Card Industry Data Security Standard）とは、決済データを保護してクレジットカード詐欺を減らすために規定された、技術要件および運用要件のベースラインを提供する情報セキュリティ基準です。

どんなデータを保護するのか？

PCI DSSは、カード会員データ（CHD）や機密認証データ（SAD）を保存、処理、送信するすべての事業体に適用されます。カード会員データと機密認証データはアカウントデータと見なされ、次のように定義されます。

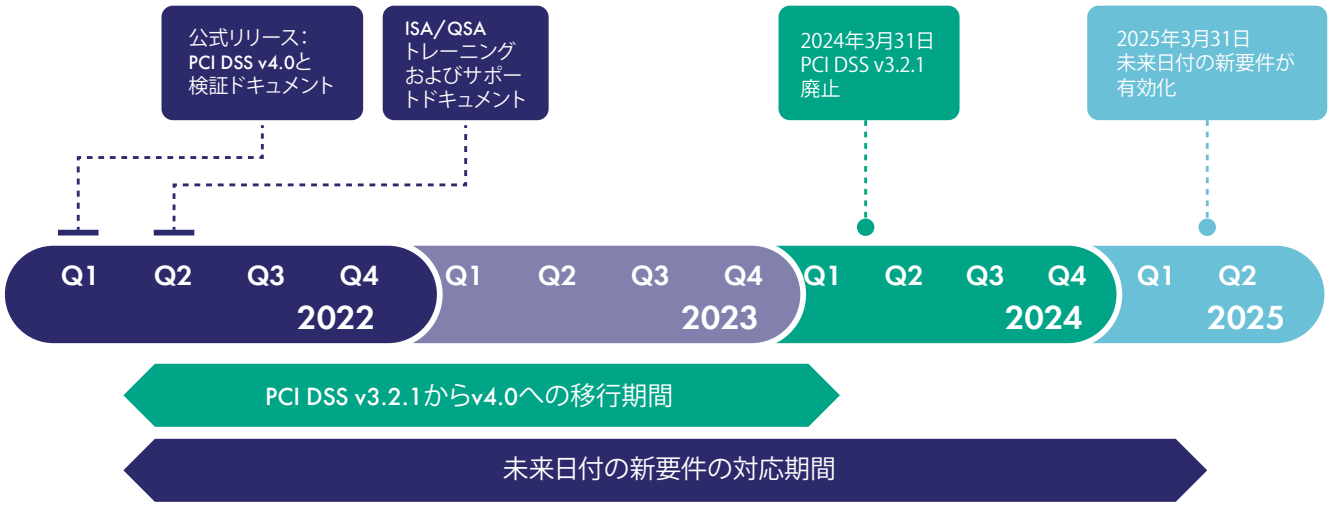
アカウントデータ	
カード会員データに含まれる情報	**機密認証データに含まれる情報**
• プライマリアカウント番号（PAN） • カード会員名 • 有効期限 • サービスコード	• 全トラックデータ（磁気ストライプデータまたはチップ上の同等データ） • カード確認コード • PIN/PINブロック

PCI DSS 4.0での変更点は？

PCI DSSの新しいバージョンが2022年3月31日に公開されました。以前のバージョン3.2.1からの変更点は次のとおりです。

- カード会員データ環境へのすべてのアクセスに多要素認証（MFA）を実装するように要件8を拡張。
- ファイアウォールの用語をネットワークセキュリティコントロールに更新して、ファイアウォールによって従来対応されてきたセキュリティ目標を達成するために使われる、より幅広いテクノロジーをサポート。
- セキュリティ目標を達成するために組織がさまざまな方法をどのように使用しているかを示すための柔軟性を向上。
- 各事業体がそのビジネスニーズとリスク影響度に最適な形で、特定のアクティビティの実行頻度を柔軟に定義できるようにするため、ターゲットリスク分析を追加。

更新内容の詳細については、PCI SSC Webサイトの PCI DSS v4.0 Summary of Changes（変更点の概要）ドキュメント を参照してください。



PCI DSS 4.0はいつ有効になるのか？

PCI DSS v3.2.1は、v4.0が公開された後も2年間有効です。この間に、組織は新バージョンについてよく理解し、必要な変更を計画し実施します。実施スケジュールは図をご覧ください。

準拠しないとどうなるのか？

- 高額な罰金
- 収益と顧客の損失
- 評判と信頼へのダメージ

準拠すべき対象者は?

金融機関

銀行、保険会社、融資機関、証券会社。

マーチャント（加盟店）

レストラン、小売店、交通機関、娯楽業。クレジットカードを処理するPOS端末を使用するすべての企業。

サービスプロバイダー

トランザクションプロセッサ、決済ゲートウェイ、セルセンターなど。

Thales SafeNet Trusted Accessで対処されるPCI DSS 4.0要件

条項	7	8.2	8.3	8.4	8.5	8.6	9	10
アクセス管理	√						√	√
OTP		√	√	√	√	√		
FIDO		√	√	√	√	√		
PKIベース		√	√	√	√	√		
証明書ベース		√	√	√	√	√		
コンテキストに応じたアクセス		√	√	√	√	√		

Thales SafeNet Trusted Access が PCI DSS 4.0 要件への準拠にどのように役立つか

要件7.2

7.2.1 アクセス要件は、最小特権およびNeed-to-knowの原則に従って、職務機能に基づき確立されている。

7.2.2 システムおよびデータへのアクセスは、関連するアクセスロールで定義された職務機能を実行するために必要なアクセスのみに制限されている。

ソリューション:

SafeNet Trusted Accessを使用することで、一意のユーザーIDとリスクベースの認証ポリシーを一元管理し、カード会員データ環境（CDE）システムへのアクセスを追加/取り消すことができます。SafeNet Trusted Accessは、多様なユーザーおよびユーザータイプのニーズを満たす強力かつ広範な最新の認証機能を提供します。

要件8.2

8.2.1 すべてのユーザーによるすべてのアクションは、個人の責に帰される。

8.2.2 汎用ID、システムID、または共有IDを持つユーザーによって実行されたすべてのアクションは、個人の責に帰される。

8.2.4 ユーザーIDと認証要素のライフサイクルイベントは、適切な許可なくして発生しない。

8.2.5 契約終了したユーザーのアクセスは、直ちに取り消される。

8.2.6 非アクティブなユーザーアカウントは、非アクティブ化された日から90日以内に削除または無効化される。

ソリューション:

Thales SafeNet Trusted Accessは、個々のユーザーに一意の資格情報が割り当てられるようにします。このソリューションは、上記の要件に記載されているすべての機能性を網羅したプロビジョニングルールとポリシーエンジンの完全なセットを提供します。SafeNet Trusted Access認証ソリューションは、すべての認証および管理イベントの最新状況を示す、広範なログおよびレポート機能を提供します。

要件8.3、8.4、8.5

8.3.1 ユーザーIDと認証要素の組み合わせがない限り、アカウントにアクセスすることはできない。

8.3.3 許可されていない個人が、許可されたユーザーのIDを偽装してシステムにアクセスすることはできない。

8.3.4 オンラインのブルートフォース攻撃で認証要素を推測することはできない。

8.3.11 認証要素は、それが割り当てられているユーザー以外は使用できない。

8.4.1 CDEへの管理アクセス権を持つ担当者によるすべての非コンソールアクセスにMFAが実装されている。

8.4.2 CDEへのすべてのアクセスにMFAが実装されている。

8.4.3 CDEにアクセスしたり影響を与えたりする可能性のある、事業体のネットワーク外から発信されるすべてのリモートネットワークアクセスにMFAが実装されている。

8.5 誤用が防止されるように多要素認証（MFA）システムが構成されている。

ソリューション:

幅広い認証方法とフォームファクタを提供するタレスの製品を使用することにより、ユーザーはクラウドまたはオンプレミスで提供される1つの認証バックエンドから管理される、一元管理された統合ポリシーによって、多数のユースケース、保証レベル、脅威ベクトルに対応できます。サポートされている認証方法には、ステップアップ機能と組み合わせたコンテキストベースの認証、ワンタイムパスワード（OTP）、X.509証明書ベースのソリューション、およびFIDOセキュリティキーが含まれます。

要件9

カード会員データへの物理的アクセスを制限する。

ソリューション:

タレスは、これらのアクセス要件に対処するための効果的な機能を提供します。スマートカードは、さまざまな入退室管理技術と統合でき、従業員の物理IDとデジタルIDの両方として機能します。

要件10

システムコンポーネントとカード会員データへのすべてのアクセスをログに記録して監視するためのプロセスとメカニズムを導入して実施する。

ソリューション:

Thales SafeNet Trusted Accessは、アクセスイベントの完全な監査証跡、自動ログエクスポート、SIEMシステムとのシームレスな統合を提供して、継続的な監視とコンプライアンスを確保します。

タレスについて

皆様がプライバシー保護を信頼して任せている相手は、そのデータを保護するためにタレスに頼っています。データセキュリティに関しては、組織が直面する決定的な局面は次々と増え続けています。その局面が暗号化戦略の策定、クラウドへの移行、コンプライアンス要件の順守のいずれであっても、デジタルトランスフォーメーションを保護するためにタレスに頼ることができます。

決断の瞬間のための、確実なテクノロジー。

詳細については、Thales PCI DSSの監査とコンプライアンス ページをご覧ください。

THALES

Building a future we can all trust

お問い合わせ先

cpl.jpsales@thalesgroup.com
すべてのオフィスの所在地と連絡先情報につきましては、cpl.thalesgroup.com/ja/contact-us
をご覧ください。

> cpl.thalesgroup.com <