外部サプライヤー管理義務

PCI データセキュリティスタンダード(PCI DSS)

2022 年 10 月付け第 12.0 版

1.カードデータコンプライアンスの取得	サプライヤーは、PCI DSS、PA-DSS、PCI-P2PE、PCI-PTS、PCI カードプロダクションなど、ペイメントセキュリティスタンダード協議会が定めるペイメントカード業界データセキュリティ基準の最新版を遵守するものとします。	カード所有者データの保護保護を可能にするための標準として認められているのが PCI DSS であり、業界の世界的な規制要件です。PCI セキュリティ基準は、カード所有者データの保護のために、ペイメントカード業界セキュリティスタンダード協議会が定めた技術的および運用上の要件です。
2.サプライヤーおよび加盟店認証	サプライヤーは、契約前、およびその後は年に 1 度、Barclays に提供されるサービスの範囲に該当するオンサイト・アセスメント(AoC)を遵守していることを示す証明書、または必要に応じ自己評価質問票(SAQ)を提出するものとします。これは、PCI DSS の要件 www.pcisecuritystandards.org/ に従って行う必要があります。 サービス範囲、環境の説明、サプライヤーの PCI コンプライアンスなどについて、AoC の審査に際して疑問が生じた場合は根拠となる「準拠レポート」に書かれた詳細な情報を要請し、確認することができます。RoC の改訂は、PCI 認証の範囲が提供されるサービス範囲に適用されることを確認した場合、または AoC の審査後に Barclays が提起したその他の疑問が確認された場合に許容されることがあります。 サプライヤーは、準拠していないとされた場合は可能な限り早く、かつ検証書類の有効期限満了から 30 日以内に Barclays に通知しなければなりません。	サプライヤーまたは加盟店は、Barclaysに提供するサービス範囲に関連するカードデータのコンプライアンスを遵守し、要件を満たしていることを証明するものとします。サプライヤーの認証AoC/RoCまたはSAQが提供するサービスに関連していることを証明するものとします。 Barclays が PCI DSS に準拠していないサプライヤーまたは加盟店を採用する場合は、サプライヤーまたは加盟店が PCI DSS に準拠していることを確認し、Visa Europe の審査および認証のために PCI DSS ステータス計画（Visa Europe テンプレートを使用）を Visa Europe に提供していることを確認するため、Visa Europe Third Party Risk チーム(agentcompliance@visa.com)までメールで連絡する必要があります。.
3.サプライヤーの認識	サプライヤーは、サプライヤーが保有・保存・処理・送信する以下のサービス、または Barclays の顧客のカード所有者データ環境のセキュリティに影響を与える可能性のあるサービス（セキュリティサービス（認証サーバーなど））、ウェブホスティングなど）のカード保有者データのセキュリ	**PCI DSS v3.2.1より** **12.8.2のテスト手順**書面による契約書の内容を確認し、サービスプロバイダーが所有する、もしくは顧客に代わって保管、処理、送信するカード所有者データのセキュリティ、または顧客のカード所有者データ環境のセキュリティに影響を与える可能性のある範囲について、サービスプロバイダーが責任を負うことに、サービスプロバイダーが了承していることを確認する必要があり

	ティについて責任を負っていることを、契約前に Barclays に書面で確認する必要があります。 提供されているサービスに変更があった場合は、変更する前に書面で Barclays に通知する必要があります。	ます。注: 要件 12.9 と合わせて、組織とサービスプロバイダーの間の書面による合意に関する本要件は、適用される PCI DSSの責任について当事者間で一貫したレベルの理解を深めることを目的としています。例えば、提供するサービスの一部として維持するために、契約には適用されるPCI DSSの要件が含まれる場合があります。 **12.8.2の要領**サービスプロバイダーの承認は、顧客から取得したカード所有者データをセキュリティを適切に維持するという意思を表明しています。 サービスプロバイダーのお客様との契約プロセスに関連する内部方針および手順、ならびに書面による契約に使われる様式には、顧客に対する該当の PCI DSS の承認が含まれていなければなりません。サービスプロバイダーが書面で承認を提示する方法は、サービスプロバイダーとその顧客との間で合意する必要があります。

サードパーティサービスプロバイダーの利用・アウトソーシング

サービスプロバイダーまたは加盟店は、サードパーティのサービスプロバイダーを使用して、カード会員データを保存、処理、または送信する、またはルータ、ファイアウォール、データベース、物理的なセキュリティ、サーバなどのコンポーネントを管理することができます。その際、カード所有者のデータ環境のセキュリティに影響を及ぼす可能性があります。

関係者は、サービスプロバイダーの PCI DSS の評価の範囲に含まれるサービスおよびシステムコンポーネント、およびサービスプロバイダーが対象とする特定の PCI DSS の要件、ならびにサービスプロバイダーの顧客が独自の PCI DSS の審査に織り込む責任のある要件を明確に指定する必要があります。例えば、マネージドホスティングプロバイダは、四半期ごとの脆弱性スキャンサービスの一環として、どの IP アドレスをスキャンするのか、どの IP アドレスを顧客の責任で四半期ごとのスキャンに含めるのかを明確に定義する必要があります。

サービスプロバイダーは、PCI DSS への準拠を証明する責任があり、各決済ブランドごとに説明を要求されることがあります。サービスプロバイダーは、データ取得先や決済ブランドに対し、この基準を満たしている旨を明確に示す必要があります。

サードパーティサービスプロバイダーが基準への準拠を検証するには、2 つの方法があります。

1) **年ごとの評価:** サービスプロバイダは、自社で PCI DSS 評価を年に 1 度受けることで、顧客に準拠を示す証明書を提供することができます。
2) **複数回の、要請ごとの評価。**PCI DSS の評価を毎年実施していない場合、サービスプロバイダーは、顧客の要求に応じて評価を受けるか、または顧客の PCI DSS の審査に参加しなければならず、その結果はそれぞれの顧客に提供されます。

サードパーティが独自の PCI DSS の評価を実施する場合、サービスプロバイダーの PCI DSS の評価の範囲が顧客に適用されるサービスをカバーしており、関連する PCI DSS の要件が検討され、その要件が満たされていると判断されたことを確認するための十分な証拠を顧客に提供するものとします。サービスプロバイダーが顧客に提供する具体的な証拠の内容は、各当事者間で締結されている合意/契約によって異なります。例えば、サービスプロバイダーの AOC および/または ROC（機密情報を保護するために編集されているもの）の関連セクションを提供することで、情報のすべてまたは一部の提供に役立つ可能性もあります。

さらに、加盟店およびサービスプロバイダーは、カード所有者データにアクセスする、すべての関連サードパーティサービスプロバイダーの PCI DSS への準拠を管理および監視する必要があります。*詳細は本文書に記載の要件 12.8 を参照してください。*