小規模加盟店向けペイメント保護リソース

ベンダにすべき質問

バージョン 1.0 | 2016 年 6 月

PCI Security Standards Council®

はじめに

この文書は、小規模加盟店の所有者および経営者向けに準備されたものです。ここで準備したベンダやサービスプロバイダに質問すべき事項は、ベンダやサービスプロバイダが顧客のカードデータをどのように保護しているかを理解していただくことを目的としています。

*ベンダにすべき質問*は、『*安全なペイメントのガイド*』（小規模加盟店向けペイメント保護リソースの一部）の補足情報として作成されています。次の場所にある『*安全なペイメントのガイド*』およびその他の小規模加盟店向けペイメント保護リソースを参照してください。

リソース	URL
安全なペイメントのガイド	https://ja.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf
一般的なペイメントシステム	https://ja.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf
ペイメントおよび情報セキュリティに関する用語集	https://ja.pcisecuritystandards.org/pdfs/Small_Merchant_Questions_To_Ask_Your_Vendors.pdf

ベンダとサービスプロバイダ、およびそれらの機能

小規模事業者/加盟店は、多くのペイメントベンダまたはサービスプロバイダと取引することがあるため、加盟店は、取引するベンダのタイプについて理解し、ベンダがカードデータの保護に関して適切な措置を講じていることを確認することが重要です。

2ページ目の表では、ごく一般的なペイメントベンダとサービスプロバイダのタイプを挙げ、ベンダを探すときに加盟店が確認すべき事項を示します。

3ページ以降の表では、ベンダやサービスプロバイダにカードデータを保護する際の役割を理解してもらうために、加盟店がベンダやサービスプロバイダにすべき質問の例を示しています。

ベンダとサービスプロバイダ

次の表に、最も一般的なペイメントのベンダおよびサービスプロバイダを挙げ、ベンダを探すときに加盟店が確認すべき事項を示します。

ベンダ/サービスプロバイダのタイプ	機能	PCI基準またはプログラム	確認する事項
ペイメントアプリケーションベンダ	カード会員データを保管、処理、および/または送信するアプリケーションを販売およびサポートします。	ペイメントアプリケーションデータセキュリティ基準（PA-DSS）	アプリケーションが、List of PCI PA-DSS of Validated Payment Applications (検証済みペイメントアプリケーションの PCI PA-DSS の一覧) に掲載されている。
決済端末ベンダ	カード支払いを受け入れるために使用するデバイス（決済端末など）を販売およびサポートします。	PINトランザクションセキュリティ	決済端末が、List of PCI Approved PTS Devices (PCI 承認済み PTS 装置の一覧) に掲載されている。
ペイメントプロセサー、電子商取引ホスティングプロバイダ/プロセサー	加盟店に代わってカード会員データを保存、処理、または送信します。 加盟店の電子商取引サーバ/Web サイトをホスティングおよび管理したり、加盟店の Web サイトを開発およびサポートしたりする場合もあります。	PCI データセキュリティ基準（PCI DSS）	PCI DSS 準拠証明書を取得しているか、および使用するサービスが評価に含まれているかを問い合わせる。 サービスプロバイダが、以下のいずれかのリストに掲載されている。 MasterCard's List of Compliant Service Providers (MasterCard の準拠サービスプロバイダの一覧) Visa's Global Registry of Service Providers (Visa のサービスプロバイダのグローバルレジストリ) Visa Europe's Registered Member Agents (Visa Europe の登録済みメンバエージェント)
サービスとしてのソフトウェアのプロバイダ	クラウドベースの Web アプリケーションまたはペイメントアプリケーション（オンラインチケット販売や予約アプリケーションなど）を開発、ホスティング、および/または管理します。	PCI DSS	PCI DSS 準拠証明書を取得しているか、および使用するサービスが評価に含まれているかを問い合わせる。 サービスプロバイダが、以下のいずれかのリストに掲載されている。 MasterCard's List of Compliant Service Providers (MasterCard の準拠サービスプロバイダの一覧) Visa's Global Registry of Service Providers (Visa のサービスプロバイダのグローバルレジストリ) Visa Europe's Registered Member Agents (Visa Europe の登録済みメンバエージェント)
インテグレータ/リセラー	加盟店に代わってPA DSS検証済みペイメントアプリケーションをインストールします。	認定インテグレータおよびリセラー（QIR）	ベンダが PCI 認定インテグレータまたはリセラー（QIR）であるかどうかを問い合わせる。ベンダがベンダが List of PCI QIRs (PCI QIR の一覧) に掲載されている。に掲載されている。
PCI DSS 要件を満たすサービスのプロバイダ	加盟店に代わって、システムまたはサービスを管理/運営します（ファイアウォール管理、パッチ適用/AV サービスなど）。	PCI DSS	PCI DSS 準拠証明書を取得しているか、および使用するサービスが評価に含まれているかを問い合わせる。 サービスプロバイダが、以下のいずれかのリストに掲載されている。 MasterCard's List of Compliant Service Providers (MasterCard の準拠サービスプロバイダの一覧) Visa's Global Registry of Service Providers (Visa のサービスプロバイダのグローバルレジストリ) Visa Europe's Registered Member Agents (Visa Europe の登録済みメンバエージェント)

質問

次の表には、カードデータを保護するために適切なコントロールが実施されているかどうかを判断するために加盟店がベンダ/サービスプロバイダに質問する事項が含まれています。

質問 *加盟店からベンダへの質問*	**ベンダからの望ましい回答**	**推奨される措置** *ベンダの回答に基づく*
貴社のソリューションまたは製品の安全性について		
1. 貴社のソリューション/製品は、カード会員データの取得および送信の安全性を確保していますか?	**対面でのカード提示による支払取引の場合:** **はい** • 決済端末が PCI PTS 認定であるかどうかは、ここで確認できます。 List of PCI Approved PTS Devices (PCI 承認済み PTS 装置の一覧) および/または • ペイメントアプリケーションが PCI PA-DSS 検証済みであるかどうかは、ここで確認できます。List of PCI PA-DSS of Validated Payment Applications (検証済みペイメントアプリケーションの PCI PA-DSS の一覧) または • 暗号化ソリューションが PCI P2PE 検証済みであるかどうかは、ここで確認できます。List of PCI P2PE Validated Solutions (PCI P2PE 検証済みソリューションの一覧) **カード提示がない取引 (電子商取引、通販/電話注文など) の場合:** **はい** • ペイメントアプリケーションが PCI PA-DSS 検証済みであるかどうかは、ここで確認できます。 List of PCI PA-DSS of Validated Payment Applications (検証済みペイメントアプリケーションの PCI PA-DSS の一覧) または • サービスプロバイダが PCI DSS 準拠であるかどうかは、ここで確認できます。 MasterCard's List of Compliant Service Providers (MasterCard の準拠サービスプロバイダの一覧) Visa's Global Registry of Service Providers (Visa のサービスプロバイダのグローバルレジストリ) Visa Europe's Registered Member Agents (Visa Europe の登録済みメンバエージェント)	**いいえ**の場合、質問 2 に進みます。

質問

質問 *加盟店からベンダへの質問*	**ベンダからの望ましい回答**	**推奨される措置** *ベンダの回答に基づく*
貴社のソリューションまたは製品の安全性について *(続き)*		
2. 当社と貴社 (ベンダ) との契約に、貴社の製品/サービスが PCI DSS 準拠を維持する (つまり PCI DSS 準拠の検証を受ける) ことを明記する条項が含まれていますか?	**はい** 既に PCI DSS 準拠であるか、または今後準拠となる製品/ソリューションのベンダは、それを書面契約に明記することに同意する必要があります。 PCI DSS 準拠の製品/ソリューションに関して確認すべき証拠の詳細については、上記の質問 1 を参照してください。	**いいえ**の場合、別のベンダまたはソリューションを検討してください。
3. 貴社の製品/ソリューションは、ペイメントカード情報をローカル (当社の店内) に保管しますか?	**いいえ** 保管する場合、加盟店はカードデータの保護を強化するためにトークン化または暗号化ソリューションを検討できます。トークン化または暗号化については、『*安全なペイメントのガイド*』を参照してください。	**はい**の場合、加盟店は、データが PCI DSS 要件に従って保管されることをベンダと確認してください。そうでない場合は、別のベンダを検討してください。
4. 貴社の製品/ソリューションは、ペイメントカード情報を強力な暗号化で保護しますか?	**はい** 暗号化は情報を保護する方法であり、これにより情報が盗まれる可能性が低くなります。可能な場合は、List of PCI P2PE Validated Solutions (PCI P2PE 検証済みソリューションの一覧) から選択してください。これらのソリューションでは、カードデータを受信後すぐに暗号化し、ネットワークを通過する間も保護します。	**いいえ**の場合、別のベンダまたはソリューションを検討してください。

質問

質問 *加盟店からベンダへの質問*	**ベンダからの望ましい回答**	**推奨される措置** *ベンダの回答に基づく*
私の製品のインストールの安全性について		
5. ベンダが PCI カウンシルの List of Validated Payment Applications (検証済みペイメントアプリケーションの一覧) にあるペイメントアプリケーションをインストールする場合は、次の質問をします。 貴社は PCI 認定インテグレータまたはリセラ (QIR) ですか?	**はい** QIR は、PA DSS ペイメントアプリケーションのインストールと統合に関して審議会によるトレーニングと認定を受けているため、QIR によるインストールは、PA DSS のペイメントアプリケーションが PCI DSS に準拠した形で実装されていることが期待できます。 ベンダが記載されているかどうかは、ここで確認できます。List of PCI QIRs (PCI QIR の一覧)	**いいえ**の場合、左のフォローアップ質問をします。
上の回答が いいえの場合のフォローアップ質問: ベンダがインストールするアプリケーションが PCI SSC 検証済みでない場合、またはベンダが QIR でない場合は、次の質問をします。 • 実装が PCI DSS 要件を確実に満たすように、インストール中、サポートを提供しますか? • 実装ガイドを提供しますか? • カードデータを保存、処理、または送信するすべての場所でカードデータを確実に保護する方法についてのインストールガイダンスを提供しますか?	**はい** ベンダは、PCI DSS 要件に準拠したソリューションのインストールを支援するプロセス定義している必要があります。不適切なインストールは、ソリューションをデータ侵害に対して脆弱にしてしまう可能性があります。 製品/ソリューションが PCI DSS 要件を満たす、または満たせるようにサポートするというベンダからの約束を要求します。	**いいえ**の場合は、別のベンダを検討してください。

質問

質問 *加盟店からベンダへの質問*	**ベンダからの望ましい回答**	**推奨される措置** *ベンダの回答に基づく*
製品/ソリューションに関して継続的なサポートとメンテナンスを提供しますか? 提供する場合、どのように提供しますか?		
6. 貴社の製品/ソリューションは、ネットワークまたはシステムにインストールするものですか?	**はい** ベンダは、ソフトウェア更新およびセキュリティパッチに関してメンテナンスとサポートを提供する必要があります。さらに、将来のバージョンのリリースのサポートを提供し、申し出る必要があります。 自社製品を完全にサポートし、システムへの変更が PCI 要件を満たすようにインストール /パッチに関して支援するベンダ/サプライヤを選択することは、あなたの最善の利益になります。	応答が**はい**の場合、左にフォローアップ質問を参照してください。 **いいえ**の場合、質問 7 に進みます。
上の回答がはい**の場合のフォローアップ質問:** • システム/ソリューションにパッチや更新をインストールしますか? • PCI DSS 要件に合った方法でそれを行いますか? • どのように私に通知しますか? どのようにパッチを提供しますか? どのようなサポートを提供しますか?	**はい** ソリューションを更新しない場合、将来の侵害により脆弱性が発生する可能性あります。	**いいえ**の場合は、別のベンダを検討してください。
7. ソリューションは、サービスプロバイダが所有および管理 (ホスティング) するシステムにインストールされますか?	**はい** これは、管理サービスと見なされます。サービスプロバイダがソリューションをホスティングする場合、PCI DSS 準拠証明書を取得しているか、および使用するサービスが評価に含まれているかを問い合わせます。	**はい**の場合、左のフォローアップ質問をします。 **いいえ**の場合 (管理サービスが PCI DSS 準拠でない場合)、別のソリューションを検討してください。
上の回答が**はい**の場合のフォローアップ質問: サービスプロバイダの環境は PCI DSS 準拠ですか?	サービスプロバイダが、以下のいずれかのリストに掲載されていることを確認します。 MasterCard's List of Compliant Service Providers (MasterCard の準拠サービスプロバイダの一覧) Visa's Global Registry of Service Providers (Visa のサービスプロバイダのグローバルレジストリ) Visa Europe's Registered Member Agents (Visa Europe の登録済みメンバエージェント)	

質問

質問 *加盟店からベンダへの質問*	**ベンダからの望ましい回答**	**推奨される措置** *ベンダの回答に基づく*
製品/ソリューションに関して継続的なサポートとメンテナンスを提供しますか? *(続き)*		
8. 当社のペイメントシステム/ソリューションをサポートするためにリモートアクセスが必要ですか?	**いいえ** リモートアクセスは、支払いデータ侵害に頻繁に悪用されています。リモートアクセス機能は、短時間の定期的な使用に限定し、それ以外のときは無効にする必要があります。	**いいえ**の場合、質問 9 に進みます。 **はい**の場合、左のフォローアップ質問をします。
上の回答が*はい*の場合のフォローアップ質問: • リモートアクセスを常にアクティブにしておくことが必要ですか?	**いいえ** リモートアクセス機能は、短時間の定期的な使用に限定し、それ以外のときは無効にする必要があります。	**はい**—リモートアクセスを常にアクティブにしておく必要がある場合、別のベンダまたはソリューションを検討してください。
• リモートアクセス接続を保護するためにどのような措置を取りますか?	**ベンダは、多要素認証を使用し、リモートアクセスする顧客ごとに別のユーザ名とパスワードを使用する必要があります。** システムを使用する個人ごとに一意のユーザ ID とパスワードを使用することにより、リモートアクセス接続をセキュリティ保護できます。さらに、システムにアクセスするユーザを識別するために複数の方法 (多要素認証) を使用する必要があります。 顧客ごとに一意のユーザ名/パスワードを使用するベンダでは、その顧客の 1 人が侵害された場合に、その顧客と同じユーザ名とパスワードを使用して、ベンダの多くの、またはすべての顧客が侵害されるのを防止できます。	製品/ソリューションがリモートアクセス用の多要素認証を提供しない場合は、別のソリューションを検討してください。
9. ソリューション/製品は、決済端末、売掛金管理、またはカード会員データを含むその他のシステムなど、他のシステムとの統合が必要ですか?	**いいえ** スタンドアロンの決済端末は、他の多数のシステムと接続されている可能性のある複雑なペイメントシステムよりもセキュリティを確保するのが簡単です。 ソリューションに他のシステムとの統合が必要な場合、それによって処理環境が簡素化しますか?また、業務にどのような付加価値が増しますか? 統合ソリューションによりカード会員データ環境は拡大し、より複雑になり、PCI DSS のスコープが拡大するため、統合には、より強力な業務ニーズが必要です。 MasterCard's List of Compliant Service Providers (MasterCard の準拠サービスプロバイダの一覧)	**はい**の場合、他のシステムと接続する、より高度なソリューションを必要とする強力な業務要件がない限り、別のベンダまたは製品を検討してください。

質問

質問 *加盟店からベンダへの質問*	**ベンダからの望ましい回答**	**推奨される措置** *ベンダの回答に基づく*
データ漏えいが発生した場合の対応		
10. 発生したデータ漏えいに貴社の製品/ソリューションが関係している場合: • 当社が罰則を受けた場合、貴社はサポートおよび保護を提供しますか? • データ漏えいが発生した場合、いつ、どのようにして当社に通知しますか? • データ漏えいや不審な活動をどのように監視しますか?	**はい** ベンダ/サービスプロバイダは、カード会員データの漏えいが発生した場合にサポートを提供する必要があります。 ベンダ/サービスプロバイダは、提供する管理サービスまたはソリューションについて質問を受けた場合は、フォレンジック捜査官に協力する必要があります。 ベンダ/サービスプロバイダは、データ漏えいが発生し、その根本的な原因がベンダのソリューションにあると判断された場合、加盟店の罰金を補償する必要があります。	**いいえ**の場合、別のベンダまたはソリューションを検討してください。
11. ベンダ/サービスプロバイダは自社の製品/ソリューションに関連するデータ漏えいを補償する保険に加入していますか?	**はい** 保険に加入しているベンダ/サービスプロバイダは、カード情報の漏えいに関して自社の責任と賠償責任を検討していると考えられます。 **はい**の場合、その補償範囲と貴社の実装が補償対象であるかを問い合わせます。	**いいえ**の場合 (ベンダが保険に加入していないか、自家保険を掛ける意思がない場合)、自社で自家保険を掛けるか、他のベンダを利用することを検討してください。
12. データ漏えいが発生し、貴社の製品/ソリューションがその根本的な原因の場合、ベンダ/サービスプロバイダは、当社の顧客への通知を支援しますか?	**はい** ベンダ/サービスプロバイダのペイメントシステムがデータ漏えいの根本的な原因である場合、ベンダ/サービスプロバイダは、漏えいの通知に関して加盟店を積極的に支援する必要があります。	**はい**の場合、左のフォローアップ質問をします。 **いいえ**の場合 (ベンダが通知を支援しない場合)、通知の計画を立てるか、別のベンダを検討するか、その両方を行う必要があります。
はいの場合、どの程度、通知を支援しますか? • 費用を負担しますか? • 通知を送信しますか? • 影響を受けた顧客のクレジットモニタリングを行いますか?		