

小規模加盟店向けペイメント保護リソース

安全なペイメントのガイド

バージョン 1.0 | 2016 年 7 月



リスクを理解する	4
基本的なセキュリティ措置による事業の保護	7
ヘルプの入手先	20



リスクを理解する

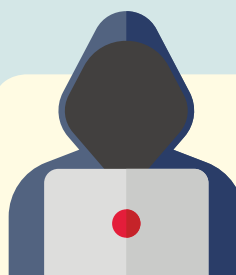
リスクを理解する

中小企業は、データ泥棒の格好の標的です。

ペイメントカードの情報が漏えいすると、その影響はすぐに現れます。顧客は、個人情報保護を貴社の能力への信頼を失います。そして、取引先を他の会社に変更してしまいます。また、訴訟による罰金刑や損害賠償の可能性があり、あなたの会社は、ペイメントカードを受け付ける能力を失うことになるかもしれません。中小企業 1,015 社を調査した結果、データ漏えいが発生した会社の 60% が 6 ヶ月以内に廃業してしまいました。(NCSA)

60%

サイバー攻撃によるデータ漏えいを経験した中小企業の割合
(HM Government)



71%

従業員が 100 人未満の会社を攻撃するハッカーの割合
(Verizon 2012)

\$20,752



中小企業が支払ったハッキング対策の平均費用。2013 年の \$8,600 から増加
(NSBA)

69%



ペイメントカードデータの盗難を心配しているアメリカの消費者の割合
(Gallup)

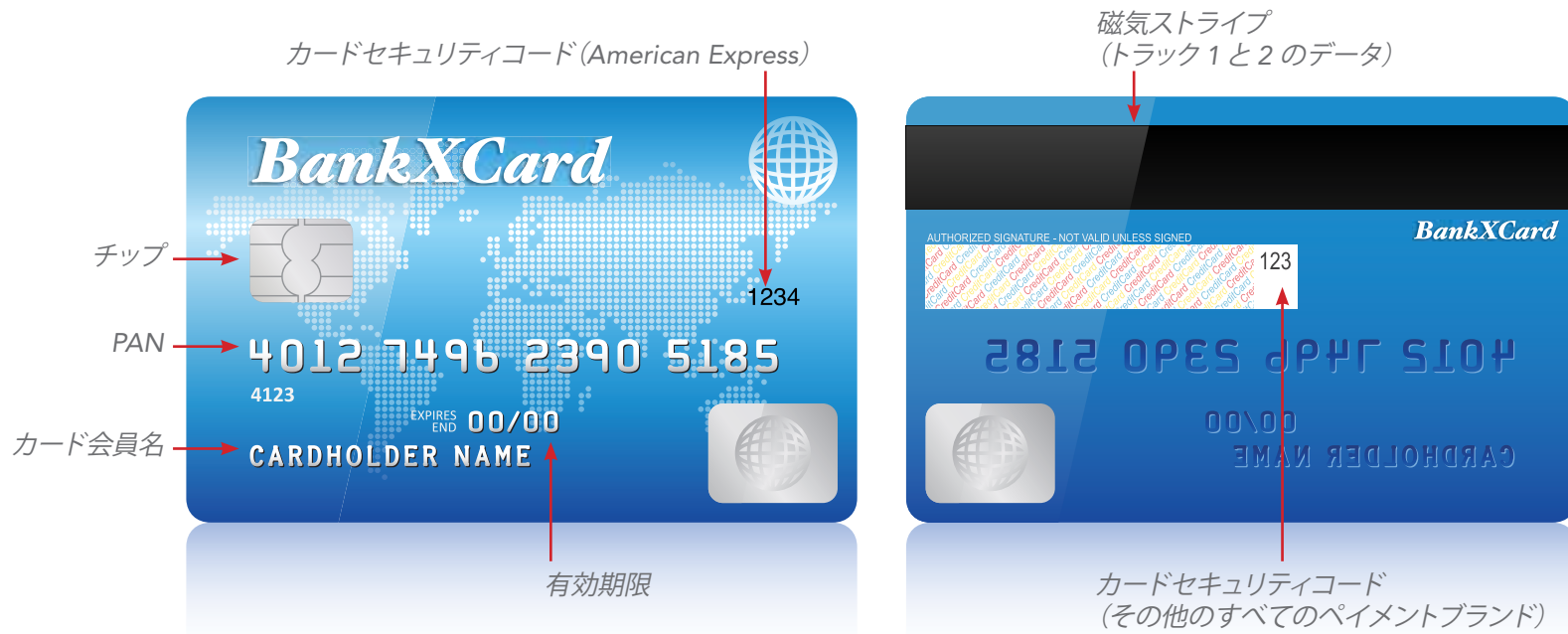
危険にさらされているもの

顧客のカードデータは、犯罪者にとって、宝の山です。このことから貴社を守らなければなりません！

このガイドの手順に従って、データ泥棒から情報を保護してください。

ペイメントカードデータの例には、プライマリアカウント番号 (PAN) と 3 桁または 4 桁のカードセキュリティコードがあります。赤い矢印は、保護が必要なデータの種類を示しています。

ペイメントカードのデータの種類



PCI DSS とは

Payment Card Industry データセキュリティ基準 (PCI DSS) は、小規模加盟店がペイメントカードの顧客カードデータを保護するための一連のセキュリティ要件です。

小規模加盟店の中には、自己評価アンケート (SAQ) を使用して PCI DSS 準拠を検証することに精通している方もいます。

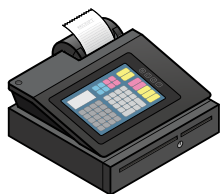
PCI DSS の詳細については、このガイドの最後に記載されているリソースを参照してください。

ペイメントシステムを理解する 一般的な支払い条件

使用する国によって、ペイメントの実行に使用される機器は異なる名称で呼ばれます。以下に、この資料で使用するタイプと一般的な名称をご紹介します。



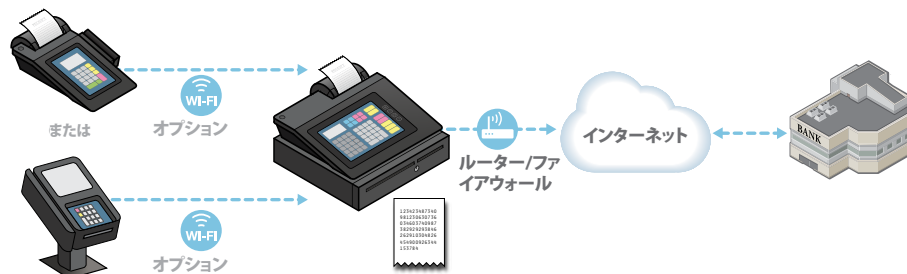
決済端末とは、スワイプ、ディップ、挿入、タップ、またはカード番号の手動入力によって顧客のカード決済に使用される装置です。POS (Point-of-Sale) 端末、クレジットカードマシン、PDQ端末、またはEMV/チップ対応端末もこのような装置を示す名称です。



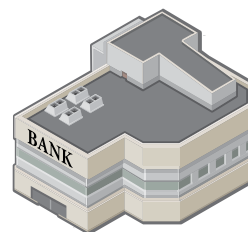
レジ(またはキャッシュドローアー)は、取引を登録および計算するものです。領収書を出力する場合もありますが、顧客のカード決済には対応していません。



統合決済端末は、決済端末とレジを1つに統合したもので、カード決済を実行し、取引を登録および計算して、受領書を出力します。



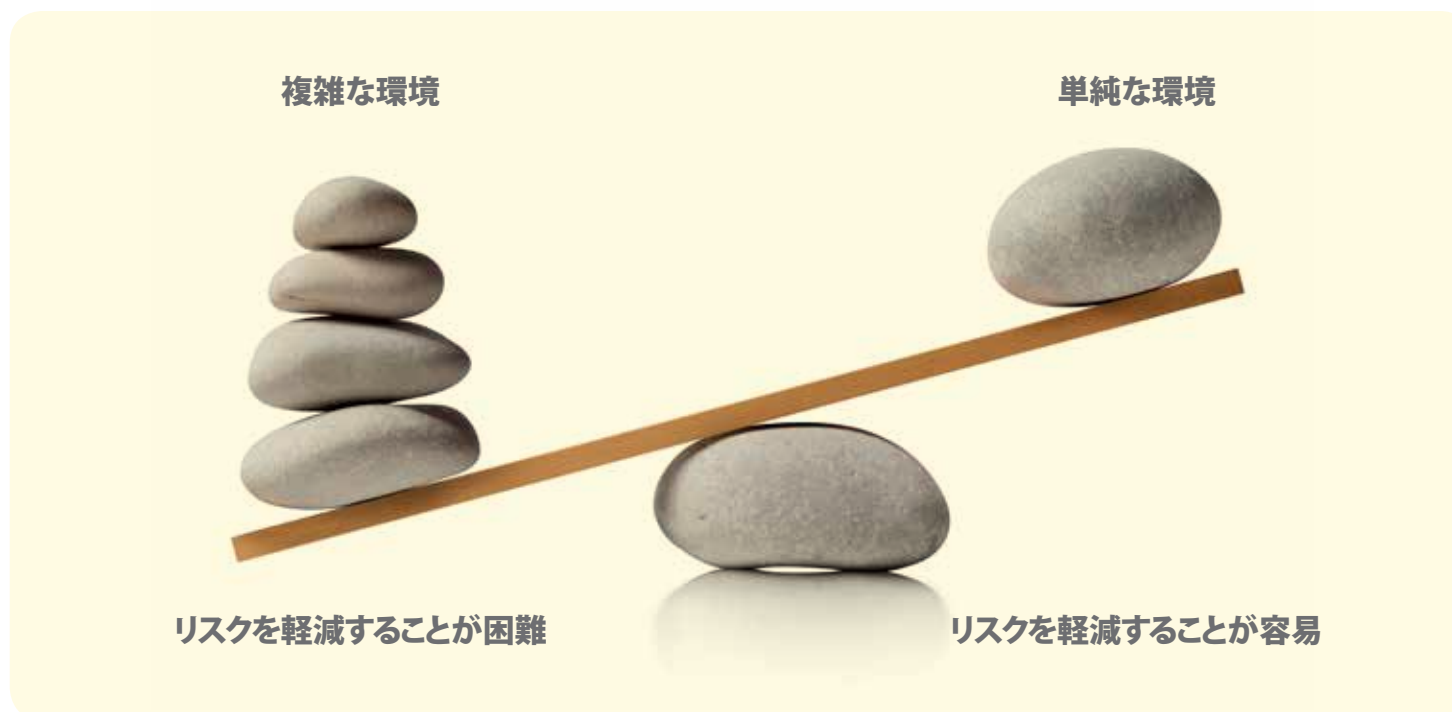
ペイメントシステムには、小売店舗(小売店/ショップや電子商取引を行う店舗を含む)でのカード決済に対応するプロセス全体が含まれ、決済端末、レジ、決済端末に接続されたその他の装置またはシステム(接続を確立するためのWi-Fiや在庫管理のためのPCなど)、決済ページなどの電子商取引コンポーネントを備えたサーバー、および加盟店銀行への接続を含む場合があります。



加盟店銀行とは、加盟店に代わってクレジットカードやデビットカードの決済を処理する銀行または金融機関です。アクワイアラー、提携銀行、カードまたはペイメントのプロセサーもこの事業体の用語です。

ビジネスの危険度

使用するペイメントシステムの機能が多いほど、セキュリティがより複雑になります。これらの追加機能は、往々にして犯罪者が顧客のカードデータを簡単に盗むための手段として悪用されます。これらの追加機能 (Wi-Fi やカメラなど) が、実際に業務に必要なかどうかを慎重に検討してください。

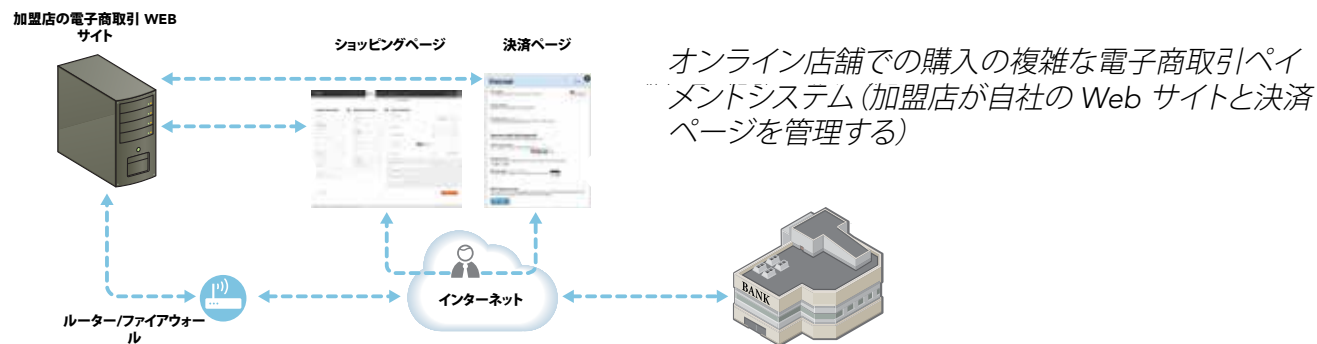
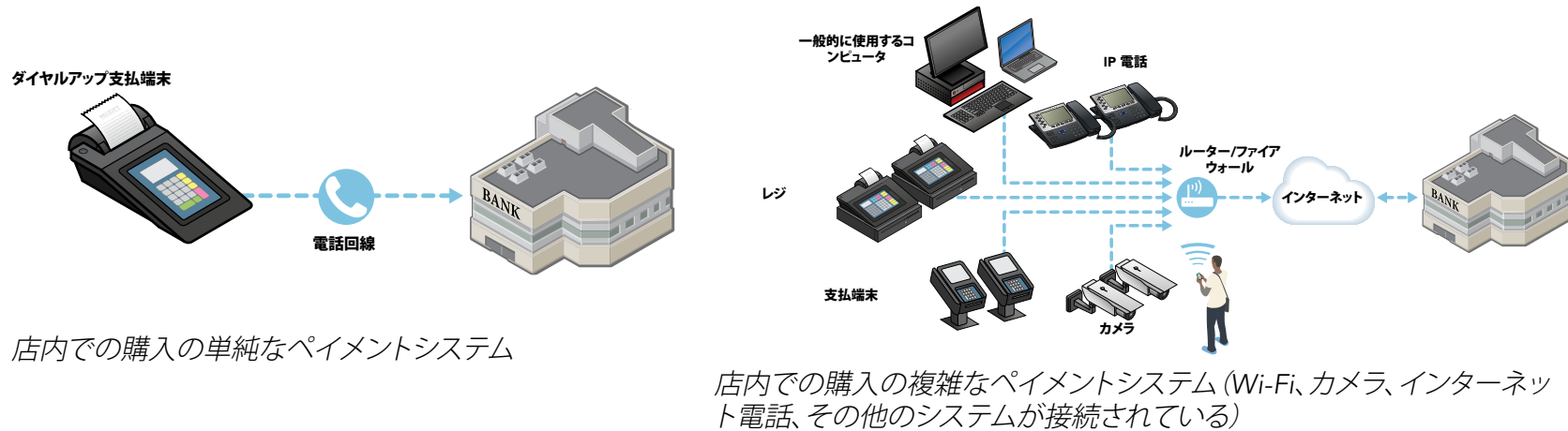


商品やサービスをどのように販売しますか? 主に3つの方法があります。

1. お客様が店舗を訪れ、カードで購入する。
2. お客様が Web サイトを訪問して、オンラインで支払う。
3. お客様が店舗に電話をして、カード情報を電話、郵送、または Fax で伝える。

リスクを理解する: ペイメントシステムタイプ

セキュリティリスクは、ペイメントシステムの複雑さ(取引が対面かオンラインか)によって大きく異なります。



加盟店銀行およびベンダのパートナーとの協議の開始点として、使用しているペイメントシステムのタイプ、リスク、および推奨されるセキュリティのヒントを、『一般的なペイメントシステム』を使用して確認してください。

基本的なセキュリティ措置 による事業の保護



事業を保護する方法

幸い、以下の基本的なセキュリティ措置を実践するにより、今すぐに事業の保護を開始できます。

データ漏えいから事業を保護する方法	コスト	難易度	リスク軽減
 強力なパスワードを使用し、デフォルトのパスワードを変更する			
 カードデータを保護し、必要なデータのみを保持する			
 決済端末が改ざんされていないかを点検する			
 ベンダからのパッチをインストールする			
 信頼できるビジネスパートナーを選び、連絡方法を確認する			
 カードデータへの社内アクセスを保護する			
 ハッカーがシステムに簡単にアクセスできないようにする			
 ウイルス対策ソフトウェアを使用する			
 脆弱性をスキャンし、問題を修正する			
 セキュリティで保護された決済端末とソリューションを使用する			
 事業をインターネットから保護する			
 最善の保護として、データを犯罪者の役に立たないようにする			

以上の基本的なセキュリティ措置は、簡単で最も実施コストが低い方法から、より複雑で実施コストの高い方法の順に並べてあります。それぞれの措置により小規模加盟店のリスクが低くなる度合いは「リスク軽減」欄に示しています。



強力なパスワードを使用し、デフォルトのパスワードを変更する

コスト	
難易度	
リスク軽減	

パスワードは、コンピュータとカードデータのセキュリティを確保するのに不可欠です。パスワードは、物理的な資産を保護するためにドアの鍵を掛けるのと同様に、業務データの保護に役立ちます。細かい設定なしですぐに使えるコンピュータ機器およびソフトウェア（決済端末を含む）には、たいてい、ハッカーが容易に推測できる「password」や「admin」などのデフォルト（設定済み）のパスワードが設定されており、それが小規模加盟店への侵入経路として頻繁に使用されます。

およそ

80%

のデータ漏えいに、推測されたか、盗まれたパスワードが使用されています

Verizon PCI 2015

パスワードを定期的に変更する。パスワードを歯ブラシのように考えてください。他の人には使用させず、3 か月ごとに新しいものに取り替えます。

助けを求める。ベンダやサービスプロバイダにデフォルトのパスワードとその変更方法について問い合わせます。そして実行します！

推測しにくいものにします。最も一般的なパスワードは「password」と「123456」です。過半数の人々が簡単に推測できるパスワードを使用しているため、ハッカーはこれらを試します。パスワードを強化するには、7 文字以上で、大文字と小文字の英字、数字、記号 (!@#\$%* など) を組み合わせます。たとえば、「B1gMac&frieS」のような表現で、パスワードを強化できます（同時に覚えやすくなります）。

人に知らせない。従業員がそれぞれ、独自のログイン ID とパスワードを持ち、決して人に知らせないことを徹底してください。

変更しなければならない一般的なデフォルトのパスワード:

[なし]

[製品/ベンダの名前]

1234 または 4321

access

admin

anonymous

database

guest

manager

pass

password

root

sa

secret

sysadmin

user

パスワードのセキュリティの詳細については、PCI カウンシルの Web サイトの以下のリソースを参照してください。



インフォグラフィック

パスワードを変更する時期です



動画

2 分で学ぶパスワードセキュリティ



カードデータを保護し、必要なデータのみを保持する

コスト



難易度



リスク軽減



カードデータがどこにあるかわからないと、保護できません。

どうすれば、よいのでしょうか。

トークン化は暗号化と同様の目的で使われますが、動作が異なります。カードデータをハッカーにとって無意味なデータ(トークン)に置き換えます。


専門家に問い合わせる。 決済端末ベンダまたは加盟店銀行に、データがシステムのどこに保存されるのか、また、支払処理をどのように簡素化できるのかを問い合わせます。また、カードのセキュリティコードを保存せずに、特定の取引(定期的なペイメントなど)を行う方法を問い合わせます。

外部委託。 データ漏えいから保護するための最善の方法は、カードデータを一切保存しないことです。PCI DSS 準拠のサービスプロバイダにカード処理を外部委託することを検討してください。準拠サービスプロバイダの一覧は、22 ページのリソースを参照してください。

カードデータが必要ない場合は、保存しない。

カードデータが必要ない場合は、安全な方法で破壊/細断します。機密性の高いカードデータが記載された書類を保管しなければならない場合は、それが読めなくなるまで、太く黒いマーカーでデータを塗りつぶし、限られた人物だけが閲覧可能な鍵のかかる引き出しや金庫に保管します。

リスクを制限する。 ペイメントの詳細は電子メールでは受け付けず、電話、Fax、または郵便で送るようお客様に依頼します。

トークン化または暗号化する。 本当にカードデータを保存する必要があるのかを加盟店銀行に問い合わせます。保存する必要がある場合は、たとえカードデータが盗まれた場合であってもそのデータを役に立たなくする暗号化またはトークン化の技術について、加盟店銀行またはサービスプロバイダに問い合わせます。(詳細については、19 ページの  を参照してください)

暗号化の基本

暗号化では、数式を使用して、「キー」と呼ばれる特殊な情報がなければプレーンテキストとして読み取ることができないようにします。暗号化技術はローカルに保存されたデータにも、ネットワークを経由して伝送されたデータにも適用されます。

暗号化プレーンテキストを暗号化テキストに変換します。

暗号解除 暗号化テキストをプレーンテキストに戻します。

例:

これは秘密情報なので注意

暗号化キー

5a0 (k\$hQ%...

暗号解除キー

これは秘密情報なので注意



決済端末が改ざんされていないかを点検する

コスト



難易度



リスク軽減



「スキミング装置」とは、決済端末で顧客のカードデータを読み込むときにその情報を読み取る装置です。従業員全員が、スキミング装置の発見方法を知っていることが重要です。決済端末が改ざんされていないことを定期的に検査する必要があります。どの決済端末を、いつ、誰が検査し、何か異常が発見されたかどうかを記録しておきます。

『PCI Council's guide: Skimming Prevention: Overview of Best Practices for Merchants (PCIカウンスルのガイド: スキミング防止 - 加盟店のためのベストプラクティスの概要)』を参照してください。

慎重に、次の手順に従ってください。

リストを管理する すべての決済端末の一覧を作成し、写真(前、後ろ、コード、接続部分)を撮影して、本来の姿を把握しておきます。

明らかな兆候を探す アクセスカバープレートやネジの封印が破られている、普通と違う/いつもとは異なるケーブル接続、または心当たりのない新しい装置や機能といった改ざんの兆候を探します。PCI カウンシルのガイド(下記を参照)が役立ちます。

端末を保護する 使用しないときは、お客様の手の届かないところに置き、画面が他者から見えないように設置します。毎日の閉店前に、顧客のペイメントカードの読み取りや個人識別番号(PIN)の入力を行う装置を含む、すべての決済端末を安全な場所に保管します。

修理を管理する 決済端末の修理は、正規の修理業者によって、修理を予定している場合にのみ許可します。従業員にも知らせてください。

電話で連絡する 異変を察知した場合は、決済端末ベンダまたは加盟店銀行にすぐに電話で連絡してください。



ベンダからのパッチをインストールする

コスト



難易度



リスク軽減



多くの場合、ソフトウェアには、プログラマがコードを書いたときに発生した欠陥や間違い（セキュリティホール、バグ、脆弱性などとも呼ばれる）が含まれていることがよくあります。ハッカーは、これらの間違いを悪用して、コンピュータに侵入し、アカウントのデータを盗みます。コードのエラーを修正するためにベンダが提供する「パッチ」を適用して、システムを保護します。セキュリティ修正プログラムを直ちにインストールすることが非常に重要です！

質問する ベンダまたはサービスプロバイダに新しいセキュリティパッチの通知方法を問い合わせ、その通知を確実に受信して、読みます。

どのベンダがパッチを送るのか？ パッチは、決済端末、ペイメントアプリケーション、その他のペイメントシステム（レジ、キャッシュレジスタ、PCなど）、オペレーティングシステム（Android、Windows、iOSなど）、アプリケーションソフトウェア（Web ブラウザを含む）、ビジネスソフトウェアなどのベンダから配布されます。

確認する 最新のセキュリティパッチをサポートできるように、決済端末、オペレーティングシステムなどをベンダに更新してもらいます。要請してください。

電子商取引加盟店。 パッチをできるだけ早くインストールすることは、電子商取引加盟店にとっても非常に重要です。支払サービスプロバイダが配布するパッチもチェックしてください。電子商取引ホスティングプロバイダがお使いシステムにパッチを適用するかどうか（および、その頻度）を問い合わせます。最新のパッチをサポートできるように、オペレーティングシステム、電子商取引プラットフォーム、または Web アプリケーション、またはそのすべてを更新することを確認します。

指示に従う ベンダ/サービスプロバイダの指示に従い、パッチを早急にインストールします。



信頼できるビジネスパートナーを選び、連絡方法を確認する

コスト



難易度



リスク軽減



ペイメントに関連するサービス、装置、アプリケーションに外部プロバイダを使用します。カードデータを共有したり、ペイメントシステムの管理やサポートをしてもらったり、カードデータへのアクセス権を与えるサービスプロバイダを使用する場合もあります。プロセサー、ベンダ、サードパーティ、またはサービスプロバイダと呼ばれることがあります。これらは、すべて貴社のカードデータを保護する能力に影響するため、その会社についてよく理解し、質問すべき事項を明確にしておくことが非常に重要です。

誰に電話すべきかを知る。加盟店銀行はどの銀行ですか？ 決済処理には他に誰が関与していますか？ 決済装置/ソフトウェアはどこから購入しましたか？ また、誰がインストールしましたか？ サービスプロバイダはどの会社ですか？

リストを管理する。誰に電話すべきかがわかったら、会社と連絡先名、電話番号、Web サイトのアドレス、その他の連絡先詳細を緊急時に簡単に見つけられる場所に保管しておきます。

サービスプロバイダのセキュリティを確認する。サービスプロバイダは、PCI DSS 要件を遵守していますか？ 電子商取引を行う加盟店の場合、ペイメントサービスプロバイダが PCI DSS 準拠であることも重要です！ 準拠サービスプロバイダの一覧は、22 ページのリソースを参照してください。

質問する。外部プロバイダが誰であるか、何をすることがわかったら、そのプロバイダに電話して、どのようにカードデータを保護しているかを問い合わせます。『[ベンダにすべき質問](#)』を使用して、何について質問するかを決めます。

一般的なベンダを理解する。一般的なタイプのベンダやサービスプロバイダについて、右側のサイドバーを参照してください。

一般的なベンダ

これらの一般的なベンダの詳細については、『[ベンダにすべき質問](#)』の表を参照してください。

決済端末のベンダ

ペイメントアプリケーションのベンダ

ペイメントシステムインストロー(インテグレータ/リセラーと呼ぶ)

決済処理や電子商取引のホスティングまたは処理を行うサービスプロバイダ

PCI DSS 要件を満たすよう支援するサービスプロバイダ(たとえば、ファイアウォールやウイルス対策サービスの提供)

サービスとしてのソフトウェアのプロバイダ

データへの社内アクセスを保護する



コスト



難易度



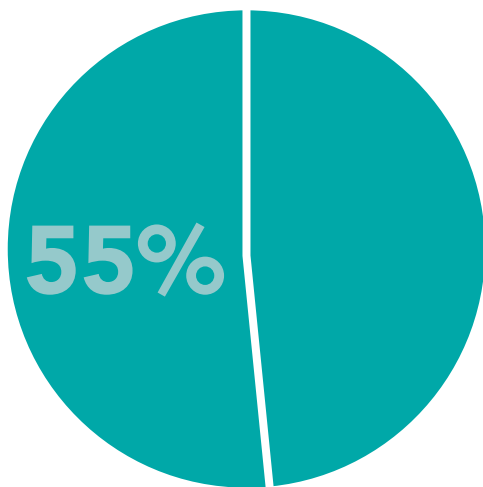
リスク軽減



特権濫用とは、以下のことを行っている人を指します。

アクセス権を付与されていないシステムやデータにアクセスするために、他人のアクセス権や権限を使用している者。

特権濫用は、最もデータ漏えいを引き起こす行為であり、報告された全インシデントの約 55% を占めています。



Verizon 2015

アクセス制御が非常に重要。業務上知る必要がある場合にのみシステムへのアクセスを許可するように設定します。事業主であるあなたには、すべてのアクセス権限があります。しかし、ほとんどの従業員は、一部のデータ、アプリケーション、および機能にアクセスするだけで業務を遂行できます。

アクセスを制限する ペイメントシステムおよび暗号化されていないカードデータへのアクセスは、アクセスが必要な従業員だけに限定し、さらに、業務遂行に必要なデータ、アプリケーション、機能に限定して付与します。

ログを記録する。店舗のカウンタの奥への訪問者は、全員記録します。訪問者の氏名、訪問を許可した従業員の名前、訪問理由を記録します。ログは最低 1 年間、保管します。

装置を安全に廃棄する。ペイメントデータ装置を売却または廃棄する前に、(データを復元できないように)カードデータを安全に削除する方法をペイメントシステムのベンダまたはサービスプロバイダに問い合わせます。

この情報を共有する。従業員やビジネスパートナーに注意事項を理解してもらうために、このガイドを渡します。

従業員に付与する権限を、支払いを受け取る権限に限定し、払い戻しを処理する権限は付与しない、または、新規の予約/注文を受け付ける権限に限定し、既存の予約/注文に関するペイメントカードのデータにアクセスする権限は付与しないことを検討してください。アクセス権限を一切もつべきでない従業員も存在します。



ハッカーがシステムに簡単にアクセスできないようにする

コスト



難易度



リスク軽減



ハッカー = 犯罪者

ハッカーがシステムに侵入するための最も簡単な方法の1つは、あなたが信頼している人物を通じての侵入です。ベンダがハッカーにシステムの入口を開けてしまっていないかを確認するには、ベンダがシステムにアクセスする方法を知っておく必要があります。

多要素認証は、ユーザー名とパスワードに加え、少なくとも1つのその他の要因（スマートカード、dongle* またはワンタイムパスワードなど）を使用します。

* コンピュータに接続して、ワイヤレスでソフトウェア機能などにアクセスできるようにする便利な装置。

確認する。ペイメントシステムのベンダまたはサービスプロバイダが貴社にアクセスするためにリモートアクセスを使用するかどうかについて問い合わせます。

リモートアクセスの使用を制限する方法を問い合わせる。多くのリモートアクセスプログラムは、デフォルトでは常に有効になっています。リスクを減らすために、必要のないときにリモートアクセスを無効にする方法、およびベンダやサービスプロバイダから要求があったとき有効にする方法をベンダに問い合わせます。

終わったら、無効にする。

強力な認証方法を使用する。リモートアクセスを許可する必要がある場合は、多要素認証と強力な暗号化を要求します。

サービスプロバイダに一意の資格情報を使用することを要求する。サービスプロバイダに、事業所固有のリモートアクセス資格情報を使用し、他の顧客と同じ資格情報を使用しないことを要求します。

支援を求める。ベンダまたはサービスプロバイダに、リモートアクセスを無効にする方法、または（ベンダまたはサービスプロバイダがリモートアクセスを必要とする場合）多要素認証を設定する方法を問い合わせます。具体的な質問の例は、『[ベンダにすべき質問](#)』を参照してください。

ベンダが決済端末を（店舗ではなく）自社のオフィスからサポートしたり、トラブルシューティングを行ったりする場合は、インターネットとリモートアクセスソフトウェアを使用します。

ベンダがリモートでサポートを行う場合は、端末に VNC や LogMeIn などの製品をインストールして使用します。



ウイルス対策ソフトウェアを使用する

コスト	
難易度	
リスク軽減	

システムおよびソフトウェアは非常に柔軟であるため、さまざまな機能が提供されます。ハッカーは、これらの機能やコーディングのミスを悪用するウイルスや他の悪意のあるコードを作成して、他人のシステムに侵入し、カードデータを盗みます。最新のウイルス対策ソフトウェア(マルウェア対策ソフトウェアとも呼ばれる)は、システムを保護するのに役立ちます。

ペイメントシステムを保護するウイルス対策ソフトウェアをインストールする。 インストールは簡単で、最寄りのオフィス用品店または IT 小売業者から購入できます。

ソフトウェアの「自動更新」を有効にする 常に最新の保護を入手できます。

アドバイスを得る。 お勧めのウイルス対策/マルウェア対策ソフトウェア製品について IT 小売業者に問い合わせます。

定期的にスキャンを実行する。 現在、使用中のウイルス対策ソフトウェアによる検出が可能になる前に発見された新しいマルウェアにシステムが感染している可能性があるため、定期的にシステムの完全スキャンを実行します。



脆弱性をスキャンし、問題を修正する

コスト



難易度



リスク軽減



新たな脆弱性、セキュリティホール、バグは毎日発見されています。これらの新たなリスクを識別するために、インターネットに露出しているシステムは定期的にテストし、これらのリスクに早急に対処することが重要です。インターネットに露出しているシステム(多くのペイメントシステムなど)は非常に脆弱であるため、犯罪者によって簡単に悪用され、システムへの侵入を許すこととなります。

PCI カウンシルの認定スキャンングベンダ(ASV)は、外部の脆弱性のスキャンとレポートを実行します。『List of PCI-Approved Scanning Vendors (PCI 認定スキャンングベンダの一覧)』を参照してください。

アドバイスを得る。加盟店銀行に、PCI 認定スキャンングベンダ(ASV)と提携しているかどうかについて問い合わせます。ベンダとサービスプロバイダにも問い合わせます。

PCI ASV と話す。これらのベンダは、ツールを提供することで、ネットワークを自動的に検索して脆弱性を検出し、修正プログラムを適用するなどの対策が必要な場合はレポートを提供することができます。スキャンングベンダは、PCI カウンシルの一覧(下記参照)に記載されています。

スキャナーを選択する。事業に適したプログラムを見つけるには、複数の PCI ASV に問い合わせてください。

脆弱性を解決する。スキャンングによって検出された問題の解決を ASV に依頼します。



セキュリティで保護された決済端末とソリューションを使用する

コスト




難易度



リスク軽減



事業を保護する確実な方法は、セキュリティで保護されたペイメントソリューションを使用し、訓練を受けた専門家から支援を受けることです。安全な製品を選択し、安全にセットアップされていることを確認する方法を示します。

カードデータを暗号化する PCI 決済端末およびセキュリティで保護されたカードリーダーについては、19 ページの  を参照してください。

セキュリティで保護された決済端末と PIN 入力装置を使用する。 PCI カウンシルは、PIN データを保護する決済端末を認定しています。お使いの決済端末または装置が最高のセキュリティ対策を提供し、EMV チップをサポートする機器であるかどうかは、『[List of PCI Approved PTS Devices \(PCI 認定 PTS 装置の一覧\)](#)』でご確認ください。

セキュリティで保護されたソフトウェアを使用する。 ペイメントソフトウェアが、『[List of PCI Validated Payment Applications \(PCI 検証済みペイメントアプリケーションの一覧\)](#)』に記載されていることを確認します。』。

資格のある専門家を使用する。 PA DSS 検証済みアプリケーションをインストールする担当者が、正しくかつ安全に実行することを確認します。PCI カウンシルの認定を受けている企業は、『[List of PCI QIRs \(PCI QIR の一覧\)](#)』から選択します。選択に関しては、加盟店銀行に相談してください。

ベンダへの質問の一覧を参照する。『[ベンダにすべき質問](#)』を使用して、ベンダおよびサービスプロバイダに何について質問するかを決めます。

顧客は、ペイメントカードの個人識別番号 (PIN) を決済端末または PIN 入力装置に入力します。顧客の PIN データを保護するためにセキュリティで保護された装置を使用することが重要です。



事業をインターネットから保護する

コスト



難易度



リスク軽減



インターネットは、データ泥棒が顧客のカードデータを攻撃して盗むために使用するハイウェイと言えます。このため、インターネットに接続して業務を行っている場合は、カード決済に使用するすべてのものに十分注意する必要があります。

使用を切り離す。決済を行う装置を、それ以外のいかなる目的にも使用しないでください。たとえば、ペイメントランザクションに使用する装置やコンピュータで、ネットサーフィンをしたり、電子メールやソーシャルメディアをチェックしたりしないでください。会社のソーシャルメディアのページを更新するなど、業務に必要な場合は、別のコンピュータを使用します。決済装置を使用してはなりません。

仮想端末を保護する。顧客の支払いを仮想端末(コンピュータやタブレットからアクセスする Web ページ)を通じて入力する場合は、そのれに外付けのカードリーダーを接続しないことで、リスクを最小限に抑えます。

Wi-Fi を保護する。お店で顧客に無料 Wi-Fi を提供する場合は、ペイメントシステムとは別のネットワークを使用します(これは「ネットワークのセグメント化」と呼ばれます)。Wi-Fi を安全に構成するためのサポートについては、ネットワークインストーラーに問い合わせます。

ファイアウォールを使用する。適切に構成されたファイアウォールは、ハッカーや悪意のあるソフトウェアがコンピュータおよび情報にアクセスするのを防ぐバッファとして機能します。ファイアウォールが設置されていることを決済端末のベンダまたはサービスプロバイダに確認し、正しく構成する方法について問い合わせます。

個人向けファイアウォールソフトウェアまたはそれに相当するものを使用する。ペイメントシステムが企業向けファイアウォールで保護されていない場合(公共のWi-Fi に接続されている場合など)。



最善の保護として、データを犯罪者の役に立たないようにする

コスト



難易度




リスク軽減



データが攻撃を受けやすいのは、加盟店銀行に送信されるとき、そしてコンピュータや装置に保存されているときです。データを安全に保つ最良の方法は、データを隠して、たとえそれが盗まれたとしても役に立たないようにし、必要がない場合にはすべてを削除することです。この作業は、複雑になることもありますが、長い目で見れば、セキュリティの管理がしやすくなります。

ペイメントシステムのベンダまたはサービスプロバイダに、貴社の決済端末に暗号化やトークン化の技術が採用されているかどうかを問い合わせます。

カードデータを暗号化する PCI 装置を使用する。PCI カウンシルは、PINデータを保護する決済端末 (17 ページの  を参照)、および、さらにカードデータを暗号化する決済端末および「セキュアカードリーダー」を認定しています。『[List of PCI Approved PTS Devices \(PCI 認定 PTS 装置の一覧\)](#)』を参照してください。

安全な PCI 暗号化ソリューションを使用する。貴社の決済端末の暗号化が、ポイントツーポイント暗号化ソリューションを使用して行われており、PCI カウンシルの『[List of PCI P2PE Validated Solutions \(検証済み PCI P2PE ソリューションの一覧\)](#)』に記載されているかどうかを問い合わせます。

ソリューションをアップグレードする。リスクを減らすために、ハッカーにとってカードデータを価値のないものにする暗号化およびトークン化の両方の技術を採用している新しい決済端末を購入することを検討します。

EMV チップ対応の端末に移行することを考えていますか？EMV チップに対応し、暗号化とトークン化によりセキュリティを強化する端末に投資する絶好のチャンスです。

質問する。ベンダまたはサービスプロバイダにすべき質問については、『[ベンダにすべき質問](#)』を参照してください。

PCI 認定の安全なカードリーダーおよび決済端末は、「Secure Reading & Exchange of Data (SRED)」と呼ばれる技術を使用してカードデータを暗号化します。貴社の決済端末が SRED を使用してカードデータを暗号化しているかどうかについて、ベンダに問い合わせてください。



ヘルプの入手先

リソース

PCI カウンシルのリソース一覧

リソース	リンク	URL
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)	PCI Council's Validated Payment Applications (PCI カウンシルの検証済みペイメントアプリケーション)	https://www.pcisecuritystandards.org/assessors_and_solutions/vpa_agreement
List of Approved PTS Devices (認定 PTS 装置の一覧)	PCI Council's Approved PTS Devices (PCI カウンシルの認定 PTS 装置)	https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices
List of Approved Scanning Vendors (認定スキャンニングベンダの一覧)	PCI Council's Approved Scanning Vendors (PCI カウンシルの認定スキャンニングベンダ)	https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors
List of Qualified Integrators / Resellers (認定インテグレータ/リセラーの一覧)	PCI Council's Qualified Integrators Resellers (PCI カウンシルの認定インテグレータおよびリセラー)	https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_integrators_and_resellers
List of P2PE Validated Solutions (P2PE 検証済みソリューションの一覧)	PCI Council's P2PE Validated Solutions (PCI カウンシルの P2PE 検証済みソリューション)	https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions

ペイメントブランドの一覧

リソース	リンク	URL
Lists of Compliant Service Providers (準拠サービスプロバイダの一覧)	MasterCard's List of Compliant Service Providers (MasterCard の準拠サービスプロバイダのリスト)	https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/merchants-need-to-know.html
	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)	http://www.visa.com/splisting/
	Visa Europe's Registered Member Agents (Visa Europe の登録済みメンバーエージェント)	https://www.visaeurope.com/receiving-payments/security/downloads-and-resources

PCI DSS および関連ガイド

リソース	リンク	URL
More about PCI DSS (PCI DSS についての詳細)	How to Secure with PCI DSS (PCI DSS でセキュリティを確保する方法)	https://www.pcisecuritystandards.org/pci_security/how
PCI DSS Self-Assessment Questionnaires (PCI DSS 自己問診)	Self-Assessment Questionnaires (自己問診)	https://www.pcisecuritystandards.org/pci_security/completing_self_assessment
Guide: Skimming Prevention: Overview of Best Practices for Merchants (ガイド: スキミング防止: 加盟店のためのベストプラクティスの概要)	Skimming Prevention: Overview of Best Practices for Merchants (スキミング防止: 加盟店のためのベストプラクティスの概要)	https://www.pcisecuritystandards.org/documents/Skimming_Prevention_At-a-Glance_Sept2014.pdf

リソース

インフォグラフィックとビデオ

リソース	リンク	URL
Infographic: It's Time to Change Your Password (インフォグラフィック: パスワードを変更する時期です)	<u>It's Time to Change Your Password (パスワードを変更する時期です)</u>	<u>https://www.pcisecuritystandards.org/pdfs/its_time_to_change_your_password_infographic.pdf</u>
Infographic: Fight Cybercrime by Making Stolen Data Worthless to Thieves (インフォグラフィック: データを盗まれても価値のないものとする事でサイバー犯罪と戦う)	<u>Fight Cybercrime by Making Stolen Data Worthless to Thieves (データを盗まれても価値のないものとする事でサイバー犯罪と戦う)</u>	<u>https://www.pcisecuritystandards.org/documents/PCI-CyberCrime-FinalR.pdf</u>
Video: Learn Password Security in 2 Minutes (ビデオ: 2分でパスワードのセキュリティを学ぶ)	<u>Learn Password Security in 2 Minutes (2分でパスワードのセキュリティを学ぶ)</u>	<u>https://www.youtube.com/watch?v=FsrOXgZKa7U</u>

小規模加盟店向け PCI ペイメント保護リソース

リソース	リンク	URL
一般的なペイメントシステム	<u>一般的なペイメントシステム</u>	<u>https://ja.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf</u>
ベンダへの小規模加盟店の質問集	<u>ベンダへの小規模加盟店の質問集</u>	<u>https://ja.pcisecuritystandards.org/pdfs/Small_Merchant_Questions_To_Ask_Your_Vendors.pdf</u>
小規模加盟店の用語集	<u>小規模加盟店の用語集</u>	<u>https://ja.pcisecuritystandards.org/pdfs/Small_Merchant_Glossary_of_Payment_and_Information_Security_Terms.pdf</u>

出典

Gallup – Gallup Poll, October 2015 (ギャラップ – ギャラップ調査、2015 年 10 月)

HM Government - *Small Businesses: What You Need to Know about Cyber Security*, UK 2014
(イギリス政府 - 中小企業向けサイバーセキュリティ対策の手引き、イギリス 2014 年)

NCSA – *National Cyber Security Alliance survey*, 2012 (NCSA – 全米サイバーセキュリティ連盟調査、2012 年)

NSBA – *National Small Business Administration, 2014 Year End Economic Report* (NSBA – 全米中小企業協会、2014 年度末経済報告書)

Verizon 2012 – *Verizon 2012 Data Breach Investigations Report* (ベライゾン 2012 – 2012 年度データ漏えい/侵害調査報告書)

Verizon 2015 – *Verizon 2015 Data Breach Investigations Report* (ベライゾン 2015 – 2015 年度データ漏えい/侵害調査報告書)

Verizon PCI 2015 – *Verizon 2015 PCI Compliance Report* (ベライゾン PCI 2015 – ベライゾン 2015 年度 PCI コンプライアンス調査報告書)