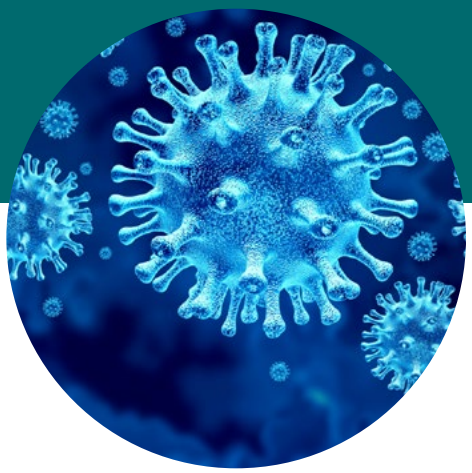
小規模加盟店のための 8 つのヒント：コロナ禍におけるペイメントカードデータの保護



新型コロナウィルス感染症の広がりで、決済を受け入れる小規模加盟店の数が劇的に変化しています。以前は実店舗しか持っていなかった加盟店が、電子商取引や 電話での取引を受け入れに動きつつあります。PCI セキュリティ・スタンダード・カウンシルは重要な留意事項を提供し、小規模加盟店がこの急速に変化する環境下で顧客のペイメントデータの安全を守るれるよう支援します。

リスクを理解する

サイバー犯罪を犯す者は、ペイメントカードデータ環境の急速な変化につけこむために、迅速に動いています。

475% コロナウィルスに関連して 3 月に見られた不正行為の増加 [1]

41% 小規模事業者のうちデータ漏洩被害からの回復に 5 万ドル以上を払った割合 [2]

29% 調査対象消費者のうち、データ漏洩被害を受けた小規模事業者は二度と利用しないと述べた割合 [3]

1: 出典：BitDefender　　2, 3: 出典：バンクオブアメリカ小規模企業決済ハイライト

小規模加盟店のためのヒント

これらの情報や詳細は PCI SSC 小規模加盟店ウェブサイトおよび PCI Perspectives ブログで確認できます。

ヒント #1: ペイメントカードのデータにアクセスできる場所を減らす

データ漏洩を防ぐ最善の方法は、カードデータをまったく保存しないことです。現在、多くの小規模加盟店が事前に注文してからお店で受け取れるサービスを提供しており、かつての対面支払いの代わりに電話決済を受け付けています。ペイメントカードの詳細を書かないようにし、代わりに安全な端末に直接入力するようにしてください。

詳細はこちら： PCI SSC Special Interest Group Paper: 安全に電話決済を受け付ける方法

ヒント #2: 強力なパスワードを使用する

弱いデフォルトパスワードを使用することが、企業にとってペイメントデータの漏洩の主な原因のひとつとなっています。効果的なパスワードにするには、強度を高め、定期的に更新する必要があります。ベンダーの弱いデフォルトのパスワードが、小規模加盟店の漏洩の原因になっていることが多いです。

詳細はこちら： 強力なパスワード Infographic

ヒント #3: ソフトウェアにパッチを適用し、最新の状態に保つ

犯罪者は、パッチが適用されていないシステムの欠陥につけこむために、古いソフトウェアを見つけようとします。セキュリティパッチを遅滞なくインストールすることが、データ漏洩のリスクを最小限に抑えるために重要です。必要な変更すべてに対応する方法の 1 つとして、セキュリティの問題を特定するために脆弱性スキャンを定期的に実行することがあります。PCI の認定スキャニングスキャンベンダ（ASV）は、インターネットに接する決済システム、電子商取引ウェブサイト、およびその他のシステムの脆弱性や設定ミスの特定に役立ち、脆弱性のレポートと対処方法（適用すべきパッチなど）を提供します。ASV 脆弱性スキャンの結果に基づいて対応を行い、ソフトウェアを最新の状態に保つようにしてください。

詳細はこちら： パッチ適用 Infographic

ヒント #4: 強力な暗号化を使用する

暗号化は、特定の鍵を持たない人がペイメントカードのデータを読み取ることができないように、また、保存されたデータやネットワーク経由で送信されるデータを保護するために使用します。決済端末の暗号化がポイント・ツー・ポイントの暗号化手法で行われ、PCI SSC の PCI P2PE　検証済みソリューションリストに記載されているかどうかベンダに問い合わせてください。新しいウェブサイトを設定する場合は、ショッピングカートのプロバイダが TLS v1.2 などの適切な暗号化を使用して顧客のデータを保護していることを確認します。

詳細はこちら： SSL/ 初期 TLS の使用に関する補足情報

ヒント #5: 安全なリモートアクセスを使用する

漏洩のリスクを最小限に抑えるには、ベンダがシステムにアクセスできる方法とタイミングの管理に関与する必要があります。犯罪者は、弱いリモートアクセス制御を介してペイメントデータを保存、処理、または送信するシステムにアクセスすることができます。リモートアクセスの使用を制限し、不要な場合は無効にする必要があります。リモートアクセスを許可する必要がある場合は、ベンダに多要素認証と強力なリモートアクセスの認証情報を使用するよう依頼してください。これらの認証情報は、自分の業務に固有であり、他の顧客に使用されたものとは異なるものでなければなりません。

詳細はこちら： PCI SSC の安全なリモートアクセス Infographic

ヒント #6: ファイアウォールが正しく設定されていることを確認する

ファイアウォールは、ネットワークとインターネットの間にあるデバイスまたはソフトウェアです。これは、ネットワークやシステムを、望ましくない・認証していないトラフィックから守るための障壁として機能します。ファイアウォールのルールは複雑に見えますが、セキュリティのためには適切に設定することが不可欠です。ファイアウォールを適切に設定するためにサポートが必要な場合は、ネットワークの担当者にお問い合わせください。

詳細はこちら： 小規模加盟店向け情報：ファイアウォールの基本

ヒント #7: クリックする前に考える

ハッカーは、フィッシングなどの人間の心理や行動の隙につけこむ手法で、本物に見えるメールやソーシャルメディアメッセージを使って企業をターゲットにし、ペイメントカード番号、加盟店アカウント番号、パスワードなどの認証資格情報をユーザに提供させようとします。小規模加盟店は十分に警戒し、よくあるフィッシングや不正行為の方法を知っておく必要があります。

詳細はこちら： コロナ関連のオンライン詐欺や脅威に気をつけましょう

ヒント #8: 信頼できるパートナーを選ぶ

サービスプロバイダが何者か、セキュリティ関連でどのような質問をすべきかを知ることが重要です。サービスプロバイダは PCI DSS 要件に準拠していますか？電子商取引の加盟店（および対面取引の代わりに最近電子商取引の決済を受け入れ始めた加盟店）にとって、決済プロセスを管理するサービスプロバイダを含む、ペイメントサービスのプロバイダ（PSP）が PCI DSS に準拠していることが重要です。

詳細はこちら： ベンダに訊くべき質問

PCI SSC の詳細な背景資料


電子商取引のセキュリティのためのベスト・プラクティス


電話による決済におけるカードデータを守るために


リモート勤務の際にペイメントを保護するには

安全な決済のためのガイド

訊くべき質問ベンダ

よくある決済システム

カウンシルではコロナ関連の最新情報を作成いたしました。状況は刻々と変化するため、
コロナ関連ウェブサイトおよびブログをぜひ定期的にぜひご覧ください。
またブログを購読していただくと通知メールを受け取ることもできます。