小規模加盟店向けペイメント保護リソース

ペイメントおよび情報セキュリティに関する用語集

バージョン 1.0 | 2016 年 7 月

PCI Security Standards Council®

はじめに

この『*ペイメントおよび情報セキュリティに関する用語集*』は、『*安全なペイメントのガイド*』（小規模加盟店のためのペイメント保護リソースの一部）の補足情報です。この用語集の目的は、該当するペイメントカード業界（PCI）および情報セキュリティ用語をわかりやすい言葉で説明することです。

アスタリスク（*）の付いている用語の定義は、『*ペイメントカード業界（PCI）データセキュリティ基準（DSS）*』および『*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）の用語集（用語、略語、および頭字語）*』バージョン 3.2、2016 年 4 月の定義に基づいているか、定義から派生したものです。

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
ベンダにすべき質問	https://ja.pcisecuritystandards.org/pdfs/Small_Merchant_Questions_To_Ask_Your_Vendors.pdf

注:
『*ペイメントカード業界（PCI）データセキュリティ基準（DSS）*』および『*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）の用語集（用語、略語、および頭字語）*』の最新バージョンは権威あるソースとして定評があり、最新の完全な PCI DSS および PA-DSS 定義については、これを参照する必要があります。

用語集

用語	定義
アクワイアラー *	「*加盟店銀行*」および「*ペイメントプロセサー*」を参照してください。
ウイルス対策ソフトウェア *	ウイルス、ワーム、トロイ（またはトロイの木馬）、スパイウェア、アドウェア、ルートキットなど、悪意のあるソフトウェア（「マルウェア」とも呼ばれます）を検出、除去し、これらのソフトウェアからコンピュータを保護するソフトウェアプログラムです。「マルウェア対策ソフトウェア」とも呼ばれます。
アプリケーション *	PC、スマートフォン、タブレット、内部サーバ、Web サーバで実行されるソフトウェアプログラムまたはプログラムグループです。
認定スキャニングベンダ（ASV） *	PCI セキュリティスタンダードカウンシルによって承認され、システム構成における一般的な弱点を識別するためにスキャンサービスを実施する企業です。「*ASV*」も参照してください。
ASV *	「Approved Scanning Vendor」の頭字語です。
認証 *	個人、デバイス、またはプロセスが本人（またはその物）であることを検証するプロセスです。通常、認証には次のような 1 つまたは複数の認証要素を使用します。 • パスワードやパスフレーズなど、ユーザが知っていること • トークンデバイスやスマートカードなど、ユーザが所有しているもの • 生体認証などユーザ自身を示すもの
承認 *	ペイメントカードトランザクションでは、承認は、アクワイアラーがイシュア/プロセサーとの取引を検証した後、加盟店が取引承認を受け取った時点で発生します。
銀行識別番号（BIN）	ペイメントカードをカード会員に発行した金融機関を識別するペイメントカード番号の最初の 6 桁（またはそれ以上）です。
業務上必要な範囲	システムまたはデータへのアクセスは、ユーザの業務上の必要性に従って、ユーザの職務に必要なものだけが付与されるという原則です。
カードデータ/顧客カードデータ *	カードデータには、プライマリアカウント番号（PAN）が含まれ、カード会員名および有効期限が含まれることもあります。PAN はカードの前面に記載され、カードの磁気ストライプや埋め込みチップにエンコードされています。カード会員データとも呼ばれます。ペイメントトランザクションの一部で、トランザクションの承認後に保存されないその他のデータ要素については、「*機密認証データ*」を参照してください。
チップ	「EMV チップ」とも呼ばれます。EMV トランザクションの国際仕様に従ってトランザクションを処理する際に使用される、ペイメントカード上のマイクロプロセッサ（または「チップ」）のことです。

用語集

用語	定義
チップおよび PIN	商品またはサービスの購入時に、顧客が EMV チップ対応支払端末に PIN を入力する検証プロセスです。
チップおよび署名	商品またはサービスの購入時に、顧客が EMV チップ対応支払端末で署名をする検証プロセスです。
資格情報	システムにアクセスするためにユーザを識別および認証する際に使用される情報です。たとえば、資格情報はユーザ名とパスワードである場合がほとんどです。資格情報には、指紋、網膜スキャン、または携帯可能な「トークン生成器」によって生成された 1 回限りの番号などが含まれることがあります。複数の資格情報が必要となるアクセスの方が、セキュリティはより強固になります。
サイバー攻撃	コンピュータまたはシステムへの侵入を目的としたあらゆる種類の攻撃的な操作のことです。サイバー攻撃は、PC 上へのスパイウェアのインストール、カードデータの盗難を目的としたペイメントシステムへの侵入、電力網などの重要なインフラストラクチャの破壊工作など、多岐にわたります。
データ違反	データ違反は、センシティブデータの表示、盗難、または権限のない第三者による使用が疑われるインシデントです。データ違反には、カードデータ、個人健康情報 (PHI) 、個人情報 (PII) 、企業秘密、または知的財産などが含まれることがあります。
デフォルトパスワード	新しいソフトウェアまたはハードウェアに付属している単純なパスワードです。デフォルトパスワード (「admin」、「password」、「123456」など) は簡単に推測でき、通常はオンライン検索で入手可能です。これらのパスワードは代用品であり、確かなセキュリティは提供されません。新しいソフトウェアまたはハードウェアのインストール後に、より強力なパスワードに変更する必要があります。
レジ (ECR)	トランザクションの登録および計算を行うデバイスで、領収書を出力できますが、顧客のカード決済には対応していません。「キャッシュドロアー」とも呼ばれます。
暗号化	特定のデジタルキーの保持者以外には使用不可能な形式に情報を数学的に変換するために、暗号化技術を使用するプロセスです。暗号化して、情報を犯罪者にとって価値のないものにすることにより、情報を保護します。「*暗号化技術*」も参照してください。
ファイアウォール *	ネットワークリソースを不正アクセスから保護するハードウェアまたはソフトウェア (あるいはその両方) です。ファイアウォールは、セキュリティレベルの異なるコンピュータまたはネットワーク間の通信を、一連のルールやその他の基準に基づいて許可または拒否します。
フォレンジック調査機関	PCI フォレンジック調査機関 (PFI) は、PCI カウンシルによって承認された企業で、カードデータ違反が発生した時期および方法の特定をサポートします。同調査機関では、実績のある調査方法およびツールを使用して金融業界内の調査を実施します。また、犯罪捜査となった際に、法執行機関と共に利害関係者をサポートします。

用語集

用語	定義
ハッカー	コンピュータシステムのセキュリティ対策を巧みに回避して、コントロール権およびアクセス権を入手しようとする人物または組織のことです。通常、カードデータの盗難が目的です。
ホスティングプロバイダ *	顧客のデータがプロバイダのサーバ上で「ホストされている」かサーバ上に常駐する場合、加盟店および他のサービスプロバイダにさまざまなサービスを提供します。通常のサービスには、サーバ上に複数の加盟店用の共有スペースが含まれ、1 つの加盟店に 1 台の専用サーバまたは「ショッピングカート」オプション付き Web サイトなどの Web アプリを提供します。
統合支払端末	支払端末とレジを 1 つに統合したもので、ペイメントを実行し、取引の登録および計算を行って、領収書を出力します。
インテグレータ/リセラー	インテグレータ/リセラーとは、加盟店の支払端末、ペイメントシステム、ペイメントアプリケーションの実装、構成、サポートを行う会社のことです。このような会社では、サービスの一環としてペイメント装置またはアプリケーションも販売していることがあります。「*認定インテグレータまたはリセラー (QIR)*」も参照してください。
ログ *	特定の事前定義された (たいていの場合はセキュリティ関連の) イベントがコンピュータシステムまたはネットワーク内で発生する際に自動的に作成されるファイルです。ログデータには、日時スタンプ、イベントの説明、およびそのイベント固有の情報が含まれます。これらのファイルは、技術的な問題のトラブルシューティングまたはデータ違反調査に役立ちます。「監査ログ」または「監査証跡」とも呼ばれます。
マルウェア *	データの盗難や、アプリケーションまたはオペレーティングシステムの破損を目的としてコンピュータシステムに侵入するために設計された悪意あるソフトウェアのことです。通常、このようなソフトウェアは電子メールや Web サイトの閲覧などの多くの業務上承認された活動中にネットワークに侵入します。マルウェアの例として、ウイルス、ワーム、トロイ (またはトロイの木馬) 、スパイウェア、アドウェア、ルートキットなどがあります。
加盟店銀行 *	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」、「カードプロセサー」、または「ペイメントプロセサー」とも呼ばれます。「*ペイメントプロセサー*」も参照してください。
モバイルデバイス	スマートフォンやタブレットといった、小型で携帯可能な、無線でコンピュータネットワークに接続できる家庭用電子機器に対する一般用語です。
モバイル支払承認	ペイメントトランザクションを承認および処理するためにモバイルデバイスを使用することを指します。通常、モバイルデバイスは既製のカードリーダーアクセサリと組み合わせて使用されます。
多要素認証 *	2 つ以上の要素を検証してユーザを認証する方法です。検証する要素は、ユーザが持っているもの (スマートカードやドングルなど) 、ユーザが知っていること (パスワード、パスフレーズ、PIN など) 、またはユーザ自身 (指紋や他の形式の生体認証など) などです。
ネットワーク *	物理的手段または無線により接続された 2 台以上のコンピュータを指します。

用語集

用語	定義
オペレーティングシステム *	すべての動作の管理と調整、およびコンピュータリソースの共有を行う、コンピュータシステムのソフトウェアです。例としては、Microsoft Windows、Apple OSX、iOS、Android、Linux、および UNIX が挙げられます。
P2PE	PCI カウンシルの「Point-to-Point 暗号化（Point-to-Point-Encryption）」基準の頭字語です。詳細は、*www.pcisecuritystandards.org* を参照してください。
PA-DSS *	PCI カウンシルの「ペイメントアプリケーションデータセキュリティ基準（Payment Application Data Security Standard）」の頭字語です。 詳細は、*www.pcisecuritystandards.org* を参照してください。
パスワード *	ユーザを認証するために使用される単語、フレーズ、または文字列のことです。ユーザ名と組み合わせて使用するとき、パスワードは、コンピュータリソースにアクセスするユーザの ID を証明することを目的としています。
パッチ *	機能を追加したり、不具合（または「バグ」）を修正したりする、既存のソフトウェアのアップデートです。
ペイメントアプリケーション *	PA-DSS に関連し、承認または決済の一環としてカード会員データを保存、処理、または送信するソフトウェアアプリケーションです。
ペイメントアプリケーションベンダ	POS インテグレータ/リセラーが加盟店のペイメントシステムに統合できるように、または加盟店が直接インストールして使用できるようにするために、ペイメントアプリケーションを販売、配信、またはライセンス付与する事業体です。
ペイメントミドルウェア	2 つ以上の無関係なペイメントアプリケーションを接続するソフトウェアの一般用語です。たとえば、ペイメントミドルウェアを使用すると、カードデータをプロセサーに送信する支払端末のアプリケーションと他の加盟店システムの間でカードデータを引き渡すことができます。
ペイメントプロセサー *	加盟店に代わってペイメントカードのトランザクションを処理するために加盟店と契約を結んだ事業体です。通常、ペイメントプロセサーは加盟店サービスを提供しますが、ペイメントカードのブランドから定義されない限り、ペイメントプロセサーはアクワイアラー（加盟店銀行）とは見なされません。「ペイメントゲートウェイ」または「ペイメントサービスプロバイダ（PSP）」とも呼ばれます。「*加盟店銀行*」*も参照してください。*
ペイメントシステム	加盟店の小売場所（小売店/ショップおよび電子商取引店頭を含む）でのカード決済に対応するプロセス全体が含まれ、支払端末、レジ、支払端末に接続されたその他の装置やシステム（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含むサーバ、および加盟店銀行への接続を含む場合もあります。
ペイメントシステムベンダ	加盟店に完全なペイメントソリューションを販売、ライセンス付与、または配布するベンダです。ソリューションには、店舗内で支払を処理するために必要なハードウェアおよびソフトウェアが含まれ、ペイメントプロセサーに接続する方法も提供されます。
支払端末	スワイプ、ディップ、挿入、タップなどによって顧客のカード決済の承認に使用されるハードウェア装置です。「店頭（POS）端末」、「クレジットカードマシン」、または「PDQ 端末」とも呼ばれます。

用語集

用語	定義
PCI *	「ペイメントカード業界（Payment Card Industry）」の頭字語です。
PCI DSS *	PCI カウンシルの「ペイメントカード業界データセキュリティ基準（Payment Card Industry Data Security Standard）」の頭字語です。詳細は、*www.pcisecuritystandards.org を参照してください。*
PCI DSS 準拠	通常業務手法によって継続的に現行の PCI DSS に適用されるすべての要件を満たすことです。準拠はある時点で評価および検証されますが、強固なセキュリティを確保するために引き続き要件に従うかどうかは、加盟店次第です。加盟店銀行やペイメントブランドは、PCI DSS 準拠について年 1 回の正式な検証を行う必要がある場合もあります。
PCI DSS 検証済み	適用される PCI DSS 要件すべてがある時点で満たされているという証拠を示すことです。特定の加盟店銀行やペイメントブランドの要件に応じて、適用される PCI DSS 自己問診、またはオンサイト評価から得た「準拠に関するレポート」をて検証できます。
PCI 検証済みペイメントアプリケーション	PCI 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）によって検証され、PCI カウンシルの Web サイトに掲載されているソフトウェアアプリケーションです。
PCI 承認済み支払端末	PCI PINトランザクションセキュリティ（PTS）基準によって承認され、PCI カウンシルの Web サイトに掲載されている支払端末です。
PCI にリストされている Point-to-Point 暗号化ソリューション	PCI Point-to-Point 暗号化（P2PE）基準によって検証され、PCI カウンシルの Web サイトに掲載されている暗号化ソリューションです。
PED *	「PIN Entry Device」の頭字語です。顧客が PIN を入力するキーパッドを指します。「PIN パッド」とも呼ばれます。
PIN *	「個人識別番号（Personal Identification Number）」の頭字語です。ユーザおよびユーザ認証を行うシステムのみが知っている、一意の数です。一般に、PIN は ATM でのキャッシング取引や、カード会員の署名の代わりに EMV チップカードに使用されます。PIN は、カード会員がカードの使用を承認されているかを判断し、カードが盗まれた場合の不正使用を防止するのに役立ちます。
プライマリアカウント番号（PAN） *	カード会員の口座を識別するクレジットカードやデビットカードの一意の番号です。
特権濫用	コンピュータシステムのアクセス権限を悪意のある方法で使用すること。例としては、システム管理者が悪用目的でカードデータにアクセスする、または誰かが管理者の昇格アクセス特権を悪用目的で盗んで使用することなどが挙げられます。
PTS *	PCI カウンシルの「PIN トランザクションセキュリティ（PIN Transaction Security）」基準の頭字語です。PTS は、PIN を承認する加盟店端末装置（POI）に関する一連のモジュール化された評価要件です。詳細は、www.pcisecuritystandards.org を参照してください。
QIR *	「認定インテグレータまたはリセラー（Qualified Integrator or Reseller）」の頭字語です。詳細は、*www.pcisecuritystandards.org* を参照してください。

用語集

用語	定義
認定セキュリティ評価機関 (QSA) *	事業体が PCI DSS 要件に準拠していることを検証する、PCI セキュリティスタンダードカウンシルによって承認された会社です。
定期的なペイメント	毎月のメンバーシップまたは購読など、加盟店が顧客に対し長期にわたって定期的に請求する請求方法です。安全な請求方法は、アクワイアラーやプロセサーがカードデータをトークン化し、確実に保護して、加盟店をこの責任から解放することです。
リモートアクセス *	ネットワーク外の場所からコンピュータネットワークにアクセスすることを指します。リモートアクセス接続は、会社独自のネットワーク内部または離れた場所からできます。リモートアクセステクノロジの例として、仮想プライベートネットワーク (VPN) があります。リモートアクセスは、内部 (IT サポートなど) または外部 (サービスプロバイダ、第三者の代理店、インテグレータ/リセラーなど) のいずれかになります。
リセラー/インテグレータ *	ペイメントアプリケーションの販売または統合 (あるいはその両方) を行うが、開発は行わない事業体です。
ルーター *	2 つ以上の内部または外部コンピュータネットワークを接続し、データを「決まったルートで送信」するかネットワークを通じてデータをガイドし、適切なネットワーク間のデータの流れを確保するハードウェアまたはソフトウェアです。ルーターを使用すると、承認済みトラフィックのみを許可し、未承認のトラフィックを拒否するため、安全性をより高めることができます。
安全なカードリーダー (SCR)	ペイメントカードを安全に承認するために携帯電話またはタブレットに接続されている PTS 承認デバイスです。PCI PTS 承認済み SCR は、SRED 経由でカードデータを保護して暗号化します。「*SRED*」も参照してください。
セキュリティコード *	ペイメントカードの前面または背面の署名欄に印字された 3 桁または 4 桁の数値です。このコードは個人のカードに一意に関連付けられており、一般的には、カードを提示しない取引の際に、カードが合法的なカード所有者によって所有されていることを確認する追加の確認機能として使用されます。カードのセキュリティコードとも呼ばれます。
自己問診 (SAQ) *	事業体の PCI DSS 評価からの自己問診結果を文書化するために使用する PCI DSS 検証ツールです。
機密認証データ *	カード会員を認証してペイメントカードトランザクションを承認するために使用されるセキュリティ関連情報で、カードの磁気ストライプまたはチップに保存されています。
サービスプロバイダ *	加盟店にさまざまなサービスを提供する事業体です。一般に、これらの事業体は、他の事業体 (加盟店など) の代わりにカードデータを保存、処理、または送信します。または管理されたファイアウォール、侵入検知、ホスティング、および他の IT 関連サービスを提供する管理されたサービスプロバイダです。「ベンダ」とも呼ばれます。
スキミング	詐欺師が使う携帯カードリーダーを使用したり、加盟店の支払端末に改造を施して、顧客のペイメントカードまたは加盟店の店舗でペイメントインフラストラクチャからカードデータを直接盗むことを言います。スキミングの目的は不正行為を働くことで、重大な脅威です。あらゆる加盟店の環境を破壊する可能性があります。

用語集

用語	定義
スキミング装置	合法的なカード読み取り装置に接続されることの多い物理装置で、違法的にペイメントカードから情報を取り込んで保存するために使用されます。「カードスキマー」とも呼ばれます。
小規模加盟店	一般的に 1 店舗、場合によっては数店舗を持ち、IT 予算が限られていて、大抵の場合は IT 担当従業員がいない事業体を指します。
SRED	「データの読み取り・伝送セキュリティ（Secure Reading and Exchange of Data）」の頭字語です。支払端末のカードデータを保護して暗号化するために設計された一連の PCI PTS 要件です。PCI カウンシルにリストされた Point-to-Point 暗号化（P2PE）ソリューションは、SRED 対応で、カードデータの暗号化を実行する、PTS 承認済み・リスト済みの支払端末を使用する必要があります。
スタンドアロン型端末	加盟店環境内の他の装置への接続に依存せず、他の機能を持たない支払端末です。この端末が動作するための唯一の要件は、インターネット接続または電話回線のいずれかを通じてプロセサーに接続することです。端末をコンピュータ制御レジに接続する必要がある場合、または端末が多機能（モバイルデバイスなど）の場合、その端末はスタンドアロン型端末ではありません。
強力な認証	保護するシステムの安全性を確保するために、ユーザまたはデバイスの ID を検証する目的で使用されます。強力な認証という用語は、他要素認証（MFA）と同じ意味で使用されることがよくあります。
キャッシュドロアー	「*レジ*」を参照してください。
トークン化	プライマリアカウント番号（PAN）をトークンと呼ばれる代理値に置換するプロセスです。トークンは元の PAN の代わりに使用され、破棄、返金、または定期的な請求などのカードがない場合に機能します。トークンは使用不可で、犯罪者にとって何の価値もないため、盗難されても安全性が提供されます。
暗号化されていないデータ	最初に復号化しなくても判読できるデータです。「プレーンテキスト」や「クリアテキスト」データとも呼ばれます。
ベンダ	加盟店に対して事業に必要な製品またはサービスを提供する事業体です。サービスが提供される場所では、ベンダはサービスプロバイダと見なされ、カードデータの安全性に影響のある加盟店環境内の物理的な場所やコンピュータシステムへのアクセスが必要となる場合があります。「*サービスプロバイダ*」も参照してください。
仮想支払端末 *	ペイメントカードトランザクションを承認するアクワイアラー、プロセサー、または第三者サービスプロバイダの Web サイトへの Web ブラウザベースのアクセスです。物理端末の場合と異なり、仮想端末はデータをペイメントカードから直接には読み取りません。加盟店は、安全に接続されている Web ブラウザを使用して、手動でペイメントカードデータを入力します。ペイメントカードトランザクションを手動で入力するため、一般に仮想端末は取引量の少ない加盟店環境で物理端末の代わりに使用されます。

用語集

仮想プライベートネットワーク（VPN）*	VPN は、物理回線による直接接続ではなく、インターネットなどの大規模ネットワーク内の仮想回線で構成されています。プライベートで安全な接続を行うために作成された、大規模ネットワーク全体の VPN 「トンネル」のエンドポイントです。
ウイルス	「感染した」コンピュータ上の他のソフトウェアまたはデータファイルに、自身を複製するマルウェアです。ウイルスは、複製時にコンピュータのすべてのデータを削除するなど、悪意のあるペイロードを実行する可能性があります。潜伏してペイロードを後で実行する可能性もあれば、悪意ある操作がトリガーされない場合もあります。電子メールの添付ファイルとして、またはネットワークメッセージの一部として自身を再送信することにより複製するウイルスは「ワーム」と呼ばれます。
脆弱性 *	利用された場合にシステムに故意または意図しない侵害が発生する可能性がある不具合または弱点です。
脆弱性スキャン	コンピュータまたはネットワーク上の潜在的弱点（脆弱性）を検出して分類するソフトウェアツールです。組織の IT 部門またはセキュリティサービスプロバイダ（認定スキャニングベンダなど）によってスキャンが実行される場合があります。「*認定スキャニングベンダ（ASV）*」も参照してください。
Wi-Fi *	回線に物理的に接続することなく、コンピュータを接続する無線ネットワークです。
ワイヤレス支払端末	さまざまなワイヤレス技術を使用して、インターネットに接続される支払端末です。