Payment Card Industry（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）

用語集（用語、略語、および頭字語）

バージョン 3.2

2016 年 4 月

用語	定義
AAA	「認証（authentication）、承認（authorization）、およびアカウンティング（accounting）」の頭字語です。検証可能な個人情報に基づいてユーザを認証し、ユーザ権限に基づいてユーザを承認し、ユーザのネットワークリソースの消費状況を管理するためのプロトコル（規約）です。
アクセス制御	情報または情報処理を行うリソースの利用を、承認されたユーザまたはアプリケーションのみに制限するメカニズムです。
アカウントデータ	アカウントデータは、カード会員データおよび/またはセンシティブ認証データから構成されます。「*カード会員データ*」と「*センシティブ認証データ*」を参照してください。
アカウント番号	「*プライマリアカウント番号（PAN）*」を参照してください。
アクワイアラー	「マーチャントバンク」、「加盟店銀行」または「加盟店金融機関」とも呼ばれます。加盟店に代わってペイメントカードトランザクションを処理し、ペイメントブランドによってアクワイアラーとして定義された事業体、通常は金融機関のことです。アクワイアラーは、加盟店の準拠についてペイメントブランドのルールおよび手順に従います。「ペイメントプロセサー」も参照してください。
管理アクセス	システム、ネットワーク、アプリケーションを管理するためアカウントにより高い特権を与えることです。 管理アクセスは、個別のアカウントまたは組み込みシステムアカウントに割り当てることができます。管理アクセス権が設定されているアカウントは、オペレーティングシステムや組織構造に応じて、多くの場合に「スーパーユーザ」、「ルート」、「管理者」、「アドミン」、「シスアドミン」、または「スーパバイザ状態」と呼ばれます。
アドウェア	悪意のあるソフトウェアの一種で、アドウェアがインストールされると、コンピュータは強制的に広告を自動で表示またはダウンロードします。
AES	「Advanced Encryption Standard（次世代標準暗号化方式）」の略語です。NIST（アメリカ国立標準技術研究所）が 2001 年 11 月に FIPS PUB 197（または FIPS 197）として採用した共通鍵暗号方式で使用されているブロック暗号です。「強力な暗号化技術」を参照してください。
ANSI	「American National Standards Institute（米国規格協会）」の頭字語です。米国の自主的な標準化機構および適合性認定機構を管理および調整する、私的な非営利団体です。
アンチウィルス	ウィルス、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、さまざまな形式の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プログラム（ソフトウェア）です。
AOC	「準拠証明書」の頭字語です。AOCは、コンプライアンスに関する自己問診または報告書に記録されている通り、加盟店およびサービスプロバイダがPCI DSS評価結果を証明するための文書です。
AOV	「検証証明書」の頭字語です。AOV は PA-QSA のフォームで、PA-DSS 検証レポートに文書化される通りに PA-DSS 評価の結果を証明するものです。
アプリケーション	内部および外部（例：Web）アプリケーションを含む、すべての市販およびカスタムソフトウェアプログラムまたはソフトウェアプログラムグループを指します。

用語	定義
ASV	「Approved Scanning Vendor」の頭字語です。PCI SSC によって承認された、外部の脆弱性スキャンサービスを実施する会社です。
監査ログ	「監査証跡」とも呼ばれます。システムアクティビティの時系列の記録です。取引の開始から最終結果までのオペレーション、手順、またはイベントを取り巻く、または牽引する一連の環境およびアクティビティの再構築、レビュー、調査に十分な、単独で検証可能な証跡を提供します。
監査証跡	*「監査ログ」を参照してください。*
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。 ▪ ユーザが知っていること（パスワードやパスフレーズなど） ▪ 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 ▪ ユーザ自身を示すもの（生体認証など）
認証資格情報	ユーザ ID またはアカウント ID と個人、デバイス、またはプロセスの認証に使用する認証要素の組み合わせです。
承認	アクセス制御の状況下で、ユーザ、プログラム、またはプロセスにアクセス権または他の権利を許可します。ネットワークでは、承認により、認証後にユーザまたはプログラムが行うことのできる動作が定義されます。 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。
バックアップ	アーカイブ目的で、またはデータを損傷または損失から保護する目的のために作成される、データの複製コピーです。
BAU	「通常通りのビジネス」の頭字語 BAU は会社の通常通りの日常ビジネス業務です。
Bluetooth（ブルートゥース）	短距離通信技術を使用して、近距離にあるデータのやり取りを平易に行う無線通信規格です。
バッファオーバーフロー	安全でないコーディング方法によって作り出された脆弱性で、プログラムがバッファ境界をオーバーランしてデータを近隣のメモリースペースに書き込むことです。バッファオーバーフローは、攻撃者がシステムやデータへの不正なアクセスを得るために使用されます。
カードスキマー	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kら情報を取り込んで保存するために使用されます。

用語	定義
カード検証コードまたは値	カード検証コードまたは値、またはカードセキュリティコードとも呼ばれます。次のいずれかを指します。(1)磁気ストライプデータ、または(2)印刷されたセキュリティ機能。 (1) カードの磁気ストライプ上のデータ要素で、安全な暗号化処理を使用してストライプ上のデータ整合性を保護し、変更や偽造があった場合、それを明らかにします。ペイメントカードブランドによって、CAV、CVC、CVV、または CSC と呼ばれます。各カードブランドで使用されている用語を次に示します。 ▪ **CAV** – Card Authentication Value(JCB ペイメントカード) ▪ **PAN CVC** – Card Validation Code(MasterCard ペイメントカード) ▪ **CVV** – Card Verification Value(Visa および Discover ペイメントカード) ▪ **CSC** – Card Security Code(American Express) (2) Discover、JCB、MasterCard、および Visa ペイメントカードの場合、カード裏面の署名欄領域の右端に印刷されている 3 桁の数値が、2つ目の種類のカード検証コードまたは値になります。American Express ペイメントカードの場合、ペイメントカードの表面の PAN の上に印刷されている 4桁のエンボス加工された数値が、このコードになります。このコードは、各プラスティックカードと一意に関連付けられており、PAN とプラスティックカードを結び付けています。各カードブランドで使用されている用語を次に示します。 ▪ **CID** – Card Identification Number(American Express および Discover ペイメントカード) ▪ **CAV2** – Card Authentication Value 2(JCB ペイメントカード) ▪ **PAN CVC2** – Card Validation Code 2(MasterCard ペイメントカード) ▪ **CVV2** – Card Verification Value 2(Visa ペイメントカード)
カード会員	ペイメントカードが発行される対象となる消費者または消費者以外の顧客、またはペイメントカードの使用を承認された個人を指します。
カード会員データ	カード会員データの最小限のデータ要素は、プライマリアカウント番号(以降、PAN)の全桁数です。カード会員データは、PAN の全桁数に次のいずれかのデータ要素を加えた形式で構成することもできます: カード会員名、有効期限、サービスコード。 ペイメントトランザクションの一部として伝送または処理される可能性のある、その他のデータ要素については、「センシティブ認証データ」を参照してください。
CDE	「カード会員データ環境」の頭字語 カード会員データまたは機密認証データを保存、処理、または送信する人、処理、およびテクノロジで構成されます。
携帯端末テクノロジ	ワイヤレス電話網経由のモバイル通信で、モバイル通信用のグローバルシステム (GSM)、コードデビジョンマルチプルアクセス (CDMA)、汎用パケット無線通信システム (GPRS)を含むがこれらに限定されません。
CERT	カーネギーメロン大学の「コンピューター緊急事態対策チーム」の頭字語 カーネギーメロン大学の「Computer Emergency Response Team」の頭字語です。CERT プログラムは、ネットワークシステムに対する攻撃に対抗して損害を最小限に食い止め、重要なサービスの継続性を確保するために使用する適切なテクノロジとシステム管理手法を開発および推進するプログラムです。

用語	定義
変更制御	実装前に影響のあるシステムまたはソフト輪への変更のレビュー、テスト、承認プロセスおよび手順
CIS	「Center for Internet Security」の頭字語です。不適切な技術セキュリティ制御による、企業の事業および電子商取引の中断によるリスクを削減することを目的とした、非営利企業です。
列レベルのデータベース暗号化	データベース全体の内容をすべて暗号化する技術に対して、データベースの特定列の内容を暗号化する技術またはテクノロジ（ソフトウェアまたはハードウェア）です。「ディスク暗号化」または「ファイルレベル暗号化」も参照してください。
代替コントロール	事業体が正当な技術上の制約または文書化されたビジネス上の制約のために記載されているとおりに明示的に要件を満たすことができないが、その他のコントロールを通じて要件に関連するリスクを十分に軽減している場合、代替コントロールを検討することができます。代替コントロールは、次の要件を満たす必要があります。 (1) 元の PCI DSS 要件の目的および厳密さを満たす。 (2) 元の PCI DSS 要件と同等レベルの防御を提供する。 (3) （単にその他の PCI DSS 要件に準拠するだけでなく）その他の PCI DSS 要件 "以上" のことを実現する。 (4) PCI DSS 要件に従わないことによって課せられるその他のリスクを考慮する。 代替コントロールの使用法については、『*PCI DSS の要件およびセキュリティ評価手順*』の付録 B および C「代替コントロール」を参照してください。
侵害	「データ侵害」または「データ違反」とも呼ばれます。コンピュータシステムへの侵入があり、カード会員データの不正な開示/盗難、変更、または破壊が疑われることです。
コンソール	ネットワーク環境で、サーバ、メインフレームコンピュータ、またはその他の種類のシステムへのアクセスまたは制御を行うための画面およびキーボードです。
消費者	商品、サービスまたはその両方を購入する個人です。
重要なシステム / 重要なテクノロジ	事業体が特に重要とみなしたシステムまたはテクノロジです。たとえば、重要なシステムは業務のパフォーマンスやセキュリティ機能を維持するために不可欠な場合があります。重要システムの一般的な例としては、セキュリティシステム、一般公開のデバイスやシステム、データベース、およびカード会員データを保存、処理、送信するシステムなどがあります。特定のシステムやテクノロジが重要かどうかは、組織の環境とリスク評価戦略に応じて判断します。
クロスサイトリクエスト偽造（CSRF）	認証セッションを通して不要なアクションの実行を許可する安全で荷個ーデング方法により作り出される脆弱性 XSS や SQL インジェクションで使用されることがよくあります。
クロスサイトスクリプティング（XSS）	安全でないコーディング方法から作り出される脆弱性で、不適正な入力検証になります。CSRF や SQL インジェクションで使用されることがよくあります。
暗証化キー	暗号化技術では、キーは、平文（暗号化されていないテキスト）を暗号化テキストに変換する際に暗号化アルゴリズムの出力を決定する値です。一般に、キーの長さによって、任意のメッセージで暗号化テキストを復号化する難しさが決まります。「強力な暗号化技術」を参照してください。

用語	定義
暗号化キーの生成	キーの生成はキー管理の機能の 1 つです。適切なキーの生成に関して広く認められたガイダンスが以下の文書に記載されています。 • NIST Special Publication 800-133: 暗号化キーの生成に関する推奨事項 • ISO 11568-2 金融サービス – キー管理(小売) – パート 2: 対称暗号、そのキー管理、およびライフサイクル o 4.3 キーの生成 • ISO 11568-4 金融サービス – キー管理(小売) – パート 4: 対称暗号 – キー管理およびライフサイクル o 6.2 キーのライフサイクルステージ – 生成 • European Payments Council(欧州決済協議会) EPC 342-08 アルゴリズムの使用とキー管理に関するガイドライン o 6.1.1 キーの生成 [対称アルゴリズム] o 6.2.1 キーの生成 [非対称アルゴリズム]
暗証化キーの管理	暗号化技術で、必要に応じて古いキーを新しいキーに交換するなど、キーの確立と維持をサポートする一連のプロセスおよびメカニズムです。
暗号化技術	情報セキュリティ、特に暗号化と認証に関する数学的処理およびコンピュータサイエンス技術です。アプリケーションおよびネットワークセキュリティにおいて、アクセス制御、情報の機密保護および整合性を実現するためのツールです。
暗号化期間	定義された期間または作成された暗号化テキストの量(あるいはその両方)などに基づき、業界のベストプラクティスおよびガイドライン(たとえば、*NIST Special Publication 800-57*)に従って、定義された目的で特定の暗号化キーを使用できる期間です。
CVSS	Common Vulnerability Scoring System(通脆弱性評価システム)の頭字語 ベンダ不可知、業界オープン標準で、コンピュータシステムセキュリティの脆弱性を伝え、対応の緊急性と優先度の決定を支援します。詳細については、*ASV プログラムガイド*を参照してください。
データフロー図	データがアプリケーション、システム、またはネットワークを通して流れる様子を示す図
データベース	容易に抽出できるように、情報を整理および管理するための構造化された形式です。簡易なデータベースの例として、テーブルやスプレッドシートが挙げられます。
データベース管理者	「DBA」とも呼ばれます。データベースの管理責任者です。
デフォルトアカウント	システムを最初に使用する際、初期アクセスを可能にするために、システム、アプリケーション、またはデバイスで事前定義されているログインアカウントです。インストールプロセスの一部として、システムで追加デフォルトアカウントを生成することもできます。
デフォルトパスワード	システム、アプリケーション、またはデバイスで事前定義されているシステム管理アカウント、ユーザアカウント、またはサービスアカウントのパスワードです。一般に、デフォルトアカウントと関連付けられています。デフォルトアカウントおよびデフォルトパスワードは、公開され広く知られているため、容易に推測できます。

用語	定義
消磁	「ディスク消磁」とも呼ばれます。ディスクの磁気を除去して、ディスクに格納されているすべてのデータを永久に破棄するプロセスまたは技術です。
依存関係	PA-DSS の状況下では、依存関係とは支払アプリケーションが PA-DSS 要件を満たすために必要な特定のソフトウェアまたはハードウェアコンポーネント（ハードウェア端末、データベース、オペレーティングシステム、API、コードライブラリなど）です。
ディスク暗号化	デバイス（ハードディスク、フラッシュドライブなど）に格納されているすべてのデータを暗号化する技術またはテクノロジ（ソフトウェアまたはハードウェア）です。特定のファイルまたは列の暗号化には、*ファイルレベル暗号化*または*列レベルのデータベース暗号化*が使用されます。
DMZ	「Demilitarized Zone（非武装地帯）」の略語です。組織の内部プライベートネットワークへの追加のセキュリティ層となる、物理または論理サブネットワークまたはコンピュータホストです。DMZ はインターネットと組織の内部ネットワークの間に新たなネットワークセキュリティ層を追加し、外部の者が内部ネットワーク全体ではなく、DMZ 内のデバイスにのみ直接接続できるようにします。
DNS	「ドメインネームシステム（Domain Name System）」または「ドメインネームサーバ（Domain Name Server）」の頭字語です。インターネットなどネットワーク上のユーザに名前解決サービスを提供するために、分散データベースにドメイン名に関連する情報を格納するシステムです。
DSS	「データセキュリティ基準 (Data Secrity Standard)」の頭字語　*PA-DSS* と *PCI DSSを参照。*
二重管理	2 つ以上の別個の事業体（一般にユーザ）が協力して、機密性の高い機能またはセンシティブ情報を保護するプロセスです。攻撃を受けやすい取引に関わるマテリアルの物理的な保護に、両方の事業体が均等に責任を持ちます。1 人のユーザにマテリアル（暗号キーなど）へのアクセスまたはマテリアルの使用が許可されることはありません。二重管理では、手動によるキーの生成、移送、読み込み、保管、取得の際、事業体間でキーに関する知識を分割することが求められます。（「*知識分割*」も参照してください。）
動的パケットフィルタリング	「*ステートフルインスペクション」を参照してください。*
ECC	「Elliptic Curve Cryptography（楕円曲線暗号）」の頭字語です。有限領域での楕円曲線に基づく公開鍵暗号化方式です。「強力な暗号化技術」を参照してください。
Egress フィルタリング	明示的に許可されたトラフィックのみがネットワークから出て行くように、発信ネットワークトラフィックをフィルタリングする手法です。
暗号化	情報を、特定の暗号化キーの所有者以外は理解できない形式に変換するプロセスです。暗号化を使用すると、暗号化プロセスと復号化プロセス（暗号化の逆）の間で情報を不正な開示から保護できます。「強力な暗号化技術」を参照してください。

用語	定義
暗号化アルゴリズム	「暗号アルゴリズム」とも呼ばれます。暗号化されていないテキストまたはデータを暗号化されたテキストまたはデータに変換する（および元に戻す）一連の数学的な手順です。「強力な暗号化技術」を参照してください。
事業体	PCI DSS レビューを受ける企業、組織、またはビジネスを表す用語です。
ファイル整合性監視	特定のファイルまたはログを監視して、変更された場合にそれを検出する技術またはテクノロジです。重要なファイルまたはログが変更された場合、該当するセキュリティ担当者に警告を送信します。
ファイルレベル暗号化	特定ファイルの内容をすべて暗号化する技術またはテクノロジ（ソフトウェアまたはハードウェア）です。あるいは、*「ディスク暗号化」*または*「列レベルのデータベース暗号化」を参照してください。*
FIPS	「Federal Information Processing Standards（連邦情報処理標準）」の頭字語です。米国連邦政府により公的に認められた標準で、民間の機関および請負業者でも使用されます。
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テクノロジ（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ネットワーク間のコンピュータトラフィックを、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	「コンピュータフォレンジック」とも呼ばれます。情報セキュリティに関連しており、調査ツールや分析技術を応用して、コンピュータリソースから証拠を収集し、データ侵害の原因を特定します。
FTP	「ファイル転送プロトコル(Fail Transfer Protocol)」の頭字語です。インターネットなどの公共ネットワークを介して、コンピュータ間でデータを転送するネットワークプロトコルです。パスワードやファイル内容が平文で保護されずに送信されるため、FTP は一般に安全でないプロトコルと考えられています。FTP は、SSH などの技術を使用することで安全に実装できます。*「S-FTP」*を参照してください。
GPRS	「General Packet Radio Service（汎用パケット無線通信システム）」の頭字語です。GSM 携帯電話ユーザが利用できるモバイルデータサービスです。制限された帯域幅を効率的に使用します。特に、電子メールや Web の閲覧など、少量のデータを送受信する際に適しています。
GSM	「Global System for Mobile Communications」の頭字語です。携帯電話およびモバイルネットワークの一般的な標準です。GSM 標準のユビキティにより、携帯電話の利用者の間での国際ローミングが一般的になり、利用者は世界の多くの場所で携帯電話を使用できるようになります。

用語	定義
ハッシュ（ハッシング）	データを固定長のメッセージダイジェストに変換し、カード会員データを読み取り不能にするプロセスです。ハッシュは、非秘密アルゴリズムを任意のサイズのメッセージに入力として適用することにより、固定サイズの結果（通常「ハッシュコード」または「メッセージダイジェスト」と呼ばれる）を出力する数学的関数です。ハッシュ関数には次の特性があります。 (1)　ハッシュコードだけでは元の入力を計算によって特定することはできない。 (2)　同じハッシュコードを付与された 2 つの入力を計算によって検出することはできない。 PCI DSS では、ハッシュコードが読み取り不能になっているとみなされるためには、ハッシュを PAN 全体に適用する必要があります。ハッシュされたカード会員データがハッシュ機能への入力変数（「salt」など）を含めて、事前計算されたレインボーテーブルアタックの効果を軽減または無効にすることが推奨されます（*「入力変数」*を参照）。 その他のガイダンスについては、現行バージョンの NIST Special Publications 800-107 および 800-106、Federal Information Processing Standard（FIPS: 連邦情報処理標準）180-4 Secure Hash Standard（SHS: セキュアハッシュ標準）、FIPS 202 SHA-3 標準: 順列ベースハッシュ関数と可変長出力関数 などの業界標準を参照してください。
ホスト	コンピュータのソフトウェアが配置されている、メインコンピュータのハードウェアです。
ホスティングプロバイダ	加盟店およびその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。サービスの範囲は、サーバ上の共有領域から「ショッピングカード」オプションの全範囲まで、ペイメントアプリケーションからペイメントゲートウェイおよびプロセッサへの接続まで、および 1 台のサーバにつき 1 人の顧客の専用ホスティングなど、簡易なものから複雑なものまで多岐にわたります。ホスティングプロバイダは、単一サーバ上で複数の事業体をホストする共有ホスティングプロバイダである場合があります。
HSM	「hardware security module」または「host security module」の頭字語です。アカウントデータの暗号キー管理機能または復号に使用する、暗号化サービスを提供する物理的および論理的に保護されているハードウェア装置です。
HTTP	「ハイパーテキスト転送プロトコル(Hypertet Transfer Protocol)」の頭字語 World Wide Web 上で情報を転送または伝達する、オープンなインターネットプロトコルです。
HTTPS	「セキュアソケット層経由ハイパーテキスト転送プロトコル(Hypertet Transfer Protocol Over Secure Socket Layer)」の頭字語 World Wide Web 上で認証および暗号化された通信を提供する、セキュリティ保護された HTTP。Web ベースのログインなど、セキュリティが問題となる通信のために設計されています。
ハイパーバイザ	仮想マシンをホストおよび管理するソフトウェアまたはファームウェアです。PCI DSS では、ハイパーバイザシステムコンポーネントには仮想マシンモニタ（VMM）も含まれます。
ID	特定のユーザまたはアプリケーションの識別子です。
IDS	「侵入検知システム（Intrusion Detection System）」の頭字語です。ネットワークまたはシステムへの侵入の試みを識別し、警告するソフトウェアまたはハードウェアです。イベントを監視してセンサーに対する警告および制御を行うコンソール、センサーによってログ記録されたイベントをデータベースに記録する中央エンジンなど、セキュリティイベントを生成するセンサーで構成されています。検知されたセキュリティイベントに対して、システムのルールを使用して警告を生成します。*「IPS」*を参照してください。

用語	定義
IETF	「インターネットエンジニアリングタスクフォース（Internet Engineering Task Force）」の頭字語です。インターネットアーキテクチャの発展およびスムースなインターネット運用を図るネットワーク設計者、作業者、ベンダ、研究者の、オープンかつ大規模な国際コミュニティです。IETF には正式なメンバーシップはなく、関心のあるすべての個人ユーザに開かれています。
IMAP	「Internet Message Access Protocol」の頭字語です。電子メールクライアントがリモートメールサーバ上で電子メールにアクセスすることを許可するアプリケーション層インターネットプロトコルです。
インデックストークン	指定されたインデックスに基いて、PAN を予測不可能な値に置き換える暗号トークンです。
情報セキュリティ	情報を保護し、情報の機密性、整合性、可用性を保証します。
情報システム	情報の収集、処理、保全、使用、共有、配布、処分のために組織化された、個別の構造化データリソースの集合です。
Ingress フィルタリング	明示的に許可されたトラフィックのみがネットワークに入るように、着信ネットワークトラフィックをフィルタリングする手法です。
インジェクションの不具合	安全でないコーディング方法から作り出される脆弱性で、不適正な入力検証になり、これにより攻撃者が悪意のあるコードを Web アプリケーションを介して基礎システムにリレーします。このクラスの脆弱性には、SQL インジェクション、LDAP インジェクション、XPath インジェクションがあります。
入力変数	一方向性ハッシュ機能が適用される前にソースデータに連結されるランダムデータ列 入力変数はレインボーテーブル攻撃の効果を軽減するのに役立ちます。*「ハッシュ」*と *「レインボーテーブル」も参照してください。*
安全でないプロトコル/サービス/ポート	機密性または整合性（あるいはその両方）が完全に制御されていないために、セキュリティ上の問題が発生しているプロトコル、サービス、またはポートです。こうしたセキュリティ上の問題として、データおよび認証の資格情報（例: インターネット上で転送する平文のパスワード/パスフレーズ）を伝送するサービス、プロトコル、およびポート、またデフォルトで、または誤った構成により、不正使用を容易に許可してしまうこれらのものを含みます。安全でないサービス、プロトコル、ポートの例として、FTP、Telnet、POP3、IMAP、SNMP v1 および v2 などがあるがこれらに限定されない。
IP	「Internet Protocol」の頭字語です。パケットをルーティングするためのアドレス情報および一部の制御情報を含む、ネットワーク層のプロトコルでソースホストから宛先ホストに配信されます。IP は、インターネットプロトコルスイートの主要なネットワーク層プロトコルです。*「TCP」*を参照してください。
IP アドレス	「インターネットプロトコルアドレス（Internet Protocol Address）」とも呼ばれます。インターネット上で特定のコンピュータ（ホスト）を一意に識別する、数値コードです。

用語	定義
IP アドレススプーフィング	ネットワークやコンピュータにフセインアクセスを得るために使用される攻撃手法 悪意のあるユーザは、信頼できるホストから来たことを示す IP アドレスで、虚偽のメッセージをコンピュータに送信します。
IPS	「侵入防止システム（Intrusion Prevention System）」の頭字語です。IDS は侵入の試みを検知しますが、IPS はさらに侵入の試みをブロックします。
IPSEC	「Internet Protocol Security（インターネットプロトコルセキュリティ）」の頭字語です。すべての IP パケットを暗号化または認証（あるいはその両方）を行い、IP 通信をセキュリティ保護するための規格です。
ISO	業界標準とベストプラクティスの観点から「国際標準化機構（International Organization for Standardization）」の呼び名でより広く知られる ISO は、国の標準化機関ネットワークからなる非政府機関です。
イシュア	発行銀行や発行プロセサーなど、ペイメントカードを発行し、発行サービスを実施、促進、または支援する事業体です。「発行銀行」または「発行金融機関」とも呼ばれます。
発行サービス	発行サービスの例として、承認やカードパーソナライゼーションなどが挙げられます。
LAN	「ローカルエリアネットワーク（Local Area Network）」の頭字語です。一般に 1 つまたは複数の建物内で通信回線を共有するコンピュータやその他のデバイスの集まりです。
LDAP	「Lightweight Directory Access Protocol」の頭字語です。ユーザのアクセス許可のクエリおよび修正、および保護されたリソースへのアクセス権の付与に利用される認証および承認データリポジトリです。
最小特権	職務関係の業務または責任を果たすために最小限必要なアクセス権や特権を持つことです。
ログ	*「監査ログ」を参照してください。*
LPAR	「Logical Partition（論理パーティション）」の略語です。コンピュータの全リソース – プロセッサ、メモリおよび記憶装置 – をより小さい単位に分割またはパーティショニング（区画化）し、別個のオペレーティングシステムおよびアプリケーションを実行できるようにするシステムです。一般に、異なるオペレーティングシステムやアプリケーションを単一のデバイスで使用できるようにするために、論理パーティションを使用します。各パーティション（区画）は互いに通信をするように設定したり、ネットワークインタフェースなどサーバの一部のリソースを共有するように設定したり、またはしないように設定する場合があります。
MAC	「Message Authentication Code」の頭字語です。暗号化技術で、メッセージの認証のために使用する情報の一部分です。「強力な暗号化技術」を参照してください。
MAC アドレス	「Media Access Control Address（媒体アクセス制御アドレス）」の略語です。製造業者がネットワークアダプタやネットワークインタフェースカードに割り当てる、一意の ID 番号です。
磁気ストライプデータ	*「トラックデータ」を参照してください。*

用語	定義
メインフレーム	大容量のデータ入力/出力を処理するために設計され、スループットコンピューティングに重点をおいたコンピュータです。メインフレームでは、複数のコンピュータを操作しているかのように、複数のオペレーティングシステムを実行できます。多くの従来型システムではメインフレームシステムが使用されています。
悪意のあるソフトウェア/マルウェア	機密性、完全性、または所有者のデータ、アプリケーション、またはオペレーティングシステムの機能を侵害するために、所有者に意識されることも同意もなくコンピュータシステムに侵入または損害を加えることを意図したソフトウェアまたはファームウェア。こうしたソフトウェアは、一般に、業務上承認された活動を通じて、システムの脆弱性を利用してネットワークに侵入します。例として、ウィルス、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。
マスキング	PCI DSS では、表示または印刷する際に、データの一部（セグメント）を隠す方法のことを指します。マスキングは、PAN 全体を表示する業務上の要件がない場合に使用されます。マスキングは表示または印刷時の PAN の保護に関連します。ファイルやデータベースなどへの保存時の PAN の保護については、「*トランケーション*」を参照してください。
メモリスクレイピング攻撃	まだ適切にフラッシュも上書きもされていない、メモリ内にあるデータを処理中に検査して抽出するマルウェアアクティビティ
加盟店	PCI DSS では、加盟店は、PCI SSC のメンバー 5 社（American Express、Discover、JCB、MasterCard、Visa）のいずれかのロゴが記載されたペイメントカードを、商品またはサービス（あるいはその両方）の支払に受け入れる事業体として定義されます。ペイメントカードを商品またはサービス（あるいはその両方）の支払に受け入れる加盟店は、販売したサービスにより、他の加盟店またはサービスプロバイダの代わりにカード会員データを保管、処理、伝送する処理が発生する場合、サービスプロバイダともなる場合があります。たとえば、ISP は月次請求にペイメントカードを受け入れる加盟店ですが、加盟店を顧客としてホストする場合は、サービスプロバイダでもあります。
MO/TO	「通信販売」の頭字語です。
監視	停電、警報、または他の事前定義イベントが発生した場合に、担当者に警告するために、継続的にコンピュータまたはネットワークリソースを監督するシステムまたはプロセスの使用。
MPLS	「マルチプロトコルラベルスイッチング（Multi Protocol Label Switching）」の頭字語です。パケット通信ネットワーク群に接続するための、ネットワークまたは通信メカニズムです。
多要素認証	2 つ以上の因子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。
NAC	「ネットワークアクセス制御（Network Access Control）」または「Network Admission Control」の頭字語です。定義されたセキュリティポリシーに従ってエンドポイントデバイスへのネットワークリソースの利用可能性を制限することでネットワーク層にセキュリティを実装する方法

用語	定義
NAT	「ネットワークアドレス変換（Network Address Translation）」の頭字語です。ネットワークマスカレードまたは IP マスカレードと呼ばれています。1 つのネットワーク内で使用されている IP アドレスを別のネットワーク内で知られている異なる IP アドレスに変更し、会社が内部的に見える内部アドレスと外部でのみ見える外部アドレスを持つことを可能にします。
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。
ネットワーク管理者	事業体内にあるネットワークを管理する責任者です。ネットワーク管理者の一般的な責務として、ネットワークセキュリティ、インストール、アップグレード、保守、アクティビティの監視などが挙げられます。
ネットワークコンポーネント	ファイアウォール、スイッチ、ルーター、ワイヤレスアクセスポイント、ネットワーク機器、その他のセキュリティ機器などが含まれますが、これらに限定されるわけではありません。
ネットワーク図	ネットワーク環境内のシステムコンポーネントと接続を示す図
ネットワークセキュリティスキャン	事業体のシステムの脆弱性を、手動/自動ツールを使用してリモートでチェックするプロセスです。内部および外部システムの調査や、ネットワークに公開されているサービスのレポートなどを行うセキュリティスキャンです。このスキャンでは、悪意のあるユーザに利用される可能性のある、オペレーティングシステム、サービス、デバイスの脆弱性を特定できます。
ネットワークセグメンテーション	「セグメンテーション」または「分離」とも呼ばれます。ネットワークをセグメント化することによって、カード会員データを保存、処理、伝送するシステムはそれ以外のシステムから隔離されます。ネットワークを適切にセグメント化することで、カード会員データ環境の範囲を狭め、結果として PCI DSS 評価の範囲を縮小することができます。ネットワークセグメンテーションの使用については、『*PCI DSS 要件およびセキュリティ評価手順*』のネットワークセグメンテーションに関するセクションを参照してください。ネットワークセグメンテーションは PCI DSS 要件ではありません。
ネットワークスニフィング	「パケットスニフィング」または「スニフィング」とも呼ばれます。受動的にネットワーク通信を監視するか収集して、プロトコルを復号し、内容に関心対象情報があるかを検査する技法。
NIST	「National Institute of Standards and Technology（米国国立標準技術研究所）」の頭字語です。米国商務省の技術局内にある、規制管理を行わない連邦政府機関です。
NMAP	ネットワークをマップし、ネットワークリソース内で開放されている（オープンな）ポートを識別する、セキュリティスキャンソフトウェアです。
コンソール以外のアクセス	直接の物理接続ではなくネットワークインターフェース経由でのシステムコンポーネントへの論理アクセスを指します。コンソール以外のアクセスには、ローカル/内部ネットワーク内からのアクセスと外部またはリモートネットワークからのアクセスが含まれます。
消費者以外のユーザ	カード会員を除く、システムコンポーネントにアクセスするユーザです。従業員、管理者、サードパーティなどですが、これらに限定されるわけではありません。

用語	定義
NTP	「ネットワークタイムプロトコル（Network Time Protocol）」の頭字語です。コンピュータシステム、ネットワークデバイス、およびその他のシステムコンポーネントの時計を同期するためのプロトコルです。
NVD	[National Vulnerability Database（米国脆弱性データベース）」の頭字語です。米国政府の規格ベース脆弱性管理データのリポジトリです。NVDにはセキュリティチェックリスト、セキュリティ関連ソフトウェア不具合、構成エラー、製品名、影響指標のデータベースが含まれます。
OCTAVE®	「Operationally Critical Threat, Asset, and Vulnerability Evaluation（捜査上重大な脅威、資産、および脆弱性の評価）」の頭字語です。リスクベースの情報セキュリティ戦略的評価と計画用のツール、技法、および方法のスイートです。
オフザシェルフ（そのまま）	特定の顧客またはユーザ向けにカスタマイズまたは設計されたのではなく、在庫品をすぐに使用できる製品を指します。
オペレーティングシステム/OS	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。オペレーティングシステムの例として、Microsoft Windows、Mac OS、Linux および Unix などがあります。
組織不依存	アクティビティを行っている人または部門とそのアクティビティを評価している人または部門との間に利害の衝突がないようにする組織構造。たとえば、評価を行っている個人は評価対象環境の管理職から組織的に分離されます。
OWASP	「Open Web Application Security Project」の頭字語です。アプリケーションソフトウェアのセキュリティを向上させるために、2004年に設立された非営利団体です。OWASP は、Web アプリケーションの重要な脆弱性の一覧を管理しています（http://www.owasp.org を参照してください）。
PA-DSS	「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。
PA-QSA	「ペイメントアプリケーション認定セキュリティ評価機関(Payment Application Qualified Security Assessor)」の頭字語です。PA-QSA は PCI SSC によって PA-DSS に対して支払アプリケーションを評価する基準とされます。PA-QSA 会社と従業員用の要件の詳細については、*「PA-DSS プログラムガイド」*と*「PA-QSA 対象要件」*を参照してください。
パッド	暗号化技術において、ワンタイムパッドとは、平文と同じ長さの乱数キー、すなわち「パッド」を 1 回だけ使用する暗号化アルゴリズムです。さらに、キーが本当に乱数で、決して再使用されず、秘密が保持される場合、ワンタイムパッドは解読できません。
PAN	「プライマリアカウント番号（Primary Account Number）」の頭字語で、「アカウント番号」とも呼ばれます。イシュアおよび特定のカード会員アカウントを識別する、一意なカード番号（一般に、クレジットカードまたはデビットカード）です。
パラメーター化クエリ	エスケープ処理を制限してインジェクションの攻撃を防ぐための SQL クエリの作成方法です。

用語	定義
パスワード/パスフレーズ	ユーザを認証する文字列です。
PAT	「ポートアドレス変換（Port Address Translation）」の頭字語で、「ネットワークアドレスポート変換」とも呼ばれます。ポート番号も変換する *NAT* の種類です。
パッチ	機能を追加したり、不具合を修正したりする、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 において、ペイメントアプリケーションは、承認または決済の一部としてカード会員データを保存、処理、または送信し、第三者に販売、配布、またはライセンス供与されるアプリケーションと定義されます。詳細については、*『PA-DSS プログラムガイド』*を参照してください。
ペイメントカード	PCI DSS では、PCI SSC の設立メンバーである American Express、Discover Financial Services、JCB International、MasterCard Worldwide、Visa Inc. のロゴが記載されたすべてのペイメントカード/デバイスを指します。
ペイメントプロセサー	「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）と呼ばれることもあります。 加盟店またはその他の事業体がペイメントカードトランザクションを処理するために契約している事業体。ペイメントプロセサーは一般にアクワイアリングサービスを提供しますが、ペイメントカードブランドによってアクワイアラーとして定義されていない限り、アクワイアラーとはみなされません。「アクワイアラー」も参照してください。
PCI	「Payment Card Industry」の頭字語です。
PCI DSS	「Payment Card Industry（データセキュリティ基準）」の頭字語です。
PDA	「Personal Data Assistant」または「Personal Digital Assistant」の頭字語です。携帯電話、電子メール、Web 閲覧などの機能を持つ小型の携帯情報端末です。
PED	PIN 入力装置
ペネトレーションテスト	ペネトレーションテストは、システムコンポーネントのセキュリティ機能を回避または打破するために脆弱性を悪用することを試みます。ペネトレーションテストでは、ネットワークとアプリケーションに関連する管理と処理の他に、ネットワークとアプリケーションのテストが行われます。また、ネットワーク外部からの侵入（外部テスト）とネットワーク内部からの漏えいの両方に対して実施します。
パーソナルファイアウォールソフトウェア	1 台のコンピュータにインストールされるソフトウェアファイアウォール製品
個人情報	名前、住所、社会保障番号、生体認証データ、生年月日など、個人を識別または追跡できる情報です。
担当者	フルタイムおよびパートタイムの従業員、一時的な従業員、事業体の敷地内に "常駐" しているか、またはカード会員データ環境にアクセスできる請負業者やコンサルタントのことです。

用語	定義
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、秘密の数値パスワードです。入力した PIN とシステムの PIN が一致する場合のみ、ユーザはアクセスを許可されます。一般に、PIN は ATM でのキャッシング取引に使用されます。また、カード会員の署名に替わりに PIN が使用される場合、EMV チップカードで PIN が使用されます。
PIN ブロック	処理中の PIN の暗号化に使用するデータブロックです。PIN ブロックの形式は、PIN ブロックの内容と PIN を取得するための処理方法を定義します。PIN ブロックは PIN と PIN の長さで構成され、場合によっては PAN のサブセットを含みます。
POI	「加盟店端末装置（Point of Interaction）」の頭字語です。カードからデータを読み取る最初のポイントです。POI は、ハードウェアとソフトウェアで構成される電子取引認識製品であり、カード会員がカード取引を行うことができるようにするために認識装置でホストされます。POI は有人の場合と無人の場合があります。一般に、POI トランザクションは IC（チップ）カードまたは磁気ストライプカード（あるいはその両方）を使用したペイメントトランザクションです。
ポリシー	許容できるコンピューティングリソースの使用およびセキュリティの実践を管理し、操作手順の開発を指導する、組織全体にわたるルールです。
POP3	「Post Office Protocol v3」の頭字語です。電子メールクライアントが使用してTCP/IP接続経由でリモートサーバから電子メールを取得するためのアプリケーション層のプロトコルです。
ポート	ネットワーク経由での通信をしやすくするために特定の通信プロトコルに関連付けられている論理（仮想）接続ポイント
POS	「Point of Sale（販売時点情報管理）」の頭字語です。加盟店でペイメントカードトランザクションの処理に使用される、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。
プライベートネットワーク	プライベート IP アドレス領域を使用する組織によって確立されたネットワークです。プライベートネットワークは、一般に、ローカルエリアネットワークとして設計されます。公共ネットワークからプライベートネットワークへのアクセスは、ファイアウォールやルーターを使用して適切に保護する必要があります。「公共ネットワーク」も参照してください。
特権ユーザ	基本アクセス権より上のアクセス権を持つユーザアカウント 通常、これらのアカウントは標準ユーザアカウントの権限より上の特権を持ちます。ただし、異なる特権アカウント間の特権の程度は組織、職務、使用技術により大きく異なります。
手順	ポリシーを説明したもので、ポリシーの実行方法および実装方法を示します。
プロトコル	ネットワーク内で使用される、合意された通信方式です。ネットワーク上で処理を実行する際にコンピュータ製品が従うべき、ルールや手順を説明した仕様です。
プロキシサーバ	内部ネットワークとインターネット間の中間にあるサーバです。たとえば、プロキシサーバの 1 つの機能に内部と外部接続間の接続の停止または交渉があり、それぞれプロキシサーバとのみ通信できるようになっています。

用語	定義
PTS	「PIN トランザクションセキュリティ（PIN Transaction Security）」の頭字語です。PTS は、PCI セキュリティ基準審議会によって管理される、PIN を認識する POI 端末装置に関する一連のモジュール化された評価要件です。詳細については、www.pcisecuritystandards.org を参照してください。
公共ネットワーク	公衆にデータ伝送サービスを提供する目的で、通信プロバイダによって確立および運用されるネットワークです。公共ネットワーク上でデータを伝送する場合、伝送中にデータが傍受、変更、または宛先が転換される可能性があります。公共ネットワークの例として、インターネット、ワイヤレス、およびモバイルテクノロジがあります。「プライベートネットワーク」も参照してください。
PVV	「PIN Verification Value」の頭字語です。ペイメントカードの磁気ストライプにエンコードされた任意の値です。
QIR	「Qualified Integrator or Reseller（認定インテグレータまたはリセラ）」の頭字語です。詳細については、PCI SSC Web サイトにある*『QIR プログラムガイド』*を参照してください。
QSA	「認定セキュリティ評価者(Qualified Security Assessor)」の頭字語です。QSA は PCI SSC により PCI DSS 現場評価することを認定されています。QSA 会社と従業員要件の詳細については、*QSA 認定要件*を参照してください。
RADIUS	「Remote Authentication Dial-In User Service」の略語です。認証とアカウントシステム RADIUS サーバに渡されたユーザ名やパスワードなどの情報が正しいかどうかを確認して、システムへのアクセスを許可する、認証/アカウンティングシステムです。この認証手法をトークンやスマートカードなどと組み合わせて使用することで、多要素認証を行うことができます。
レインボーテーブル攻撃	事前計算されたハッシュストリング（固定長メッセージダイジェスト）のテーブルを使用して、元のデータソースを特定するデータ攻撃方法。通常、パスワードやカード会員データハッシュの解明に使用されます。
再キー入力	暗号化キーの変更プロセスです。定期的な再キー入力により、1 つのキーで暗号化されるデータ量を制限します。
リモートアクセス	ネットワークの外部の場所からのコンピュータネットワークへのアクセス リモートアクセス接続は、会社自身のネットワーク内部から、または会社のネットワーク外のリモート場所からできます。リモートアクセステクノロジの例として、*VPN* があります。
リモートラボラトリ環境	PA-QSA によって管理されていないラボラトリです。
リムーバブル電子メディア	デジタル化されたデータを格納し、コンピュータシステム間で容易に取り外し/持ち運びできるメディアです。リムーバブル電子メディアの例として、CD-ROM、DVD-ROM、USB フラッシュドライブおよび外部/ポータブルハードドライブがあります。
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。
RFC 1918	プライベート（インターネットにルーティングできない）ネットワークの使用法と適切なアドレス範囲を定義するインターネットエンジニアリングタスクフォース（IETF）によって規定された規格です。

用語	定義
リスク分析/リスク評価	貴重なシステムリソースおよび脅威を識別するプロセスです。すなわち、予測頻度および発生コストに基づいて脆弱性による損失（潜在的な損失）を定量化し、（任意で）全体的な脆弱性を最小限に抑えるためにリソースを対応策に割り当てる方法を推奨するプロセスです。
リスク評価	ある事業体でリスク評価とリスク分析に基づく測定定義基準
ROC	「Report on Compliance（準拠レポート）」の頭字語です。事業体の PCI DSS 評価からの詳細結果を文書化したレポート
ルートキット	悪意のあるソフトウェアの一種で、許可なしにインストールされた場合、その存在を隠して、コンピュータシステムの管理者レベルの制御を取得します。
ルーター	2 つ以上のネットワークを接続するハードウェアまたはソフトウェアです。アドレスを参照して情報を正しい宛先に渡して、並べ替えおよび解釈を行います。ソフトウェアルーターは、ゲートウェイと呼ばれることもあります。
ROV	「Report on Validation（検証レポート）」の頭字語です。PA-DSS プログラムの目的で PA-DSS 評価からの詳細結果を文書化したレポート
RSA	Ron Rivest、Adi Shamir、Len Adleman によって 1977 年に MIT で開発された公開鍵暗号化アルゴリズムです。RSA はそれぞれの頭文字をとって付けられました。
S-FTP	Secure-FTP（セキュア FTP）の頭字語です。S-FTP は認証情報と転送中のデータファイルを暗号化する機能を持ちます。*「TCP」を参照してください。*
サンプリング	グループ全体を代表する特定グループの一断面を選択するプロセスです。事業体が標準的な一元化された PCI DSS セキュリティおよび運用プロセス/コントロールを確立していることを検証する際に、サンプリングを行うことで、評価者はテストの手間を省くことができます。サンプリングは PCI DSS 要件ではありません。
SANS	「SysAdmin, Audit, Networking and Security」の頭字語です。コンピュータセキュリティのトレーニングの提供および専門家を認定する機関です。（www.sans.org を参照してください）。
SAQ	「自己問診 (Self-Assessment Questionnaire)」の頭字語です。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レポートツールです。
スキーマ	データ要素の組織を含む、データベースの構成の正式な説明
範囲設定	PCI DSS 評価に含めるすべてのシステムコンポーネント、人、プロセスを規定するプロセスです。PCI DSS 評価の最初の手順は、レビューの範囲を正確に決定することです。
SDLC	「System Development Life Cycle（システム開発のライフサイクル）」の頭字語です。計画、分析、設計、テスト、および実装を含む、ソフトウェアまたはコンピュータシステムの開発段階です。
安全なコーディング	改ざんや侵害を防止できるアプリケーションを作成および実装するプロセスです。

用語	定義
セキュア暗号デバイス	暗号化プロセス（暗号化アルゴリズムとキー生成を含む）を実装するためのハードウェア、ソフトウェア、ファームウェアのセットで、定義された暗号境界内に含まれています。セキュア暗号デバイスの例には、PCI PTS で検証済みのホスト/ハードウェアセキュリティモジュール（HSM）と加盟店端末装置（POI）などがあります。
安全なワイプ	「安全な削除」とも呼ばれる、ハードディスクドライブまたは他のデジタルメディア上にあるデータを上書きする方法でデータを取得できなくします。
セキュリティイベント	システムまたはその環境にセキュリティ上の影響があると会社が見なす出来事。PCI DSS の状況化では、背九里低イベントは疑わしいかまたは異常なアクティビティです。
セキュリティ責任者	事業体のセキュリティ関連業務の最高責任者です。
セキュリティポリシー	組織が機密情報を管理、保護、配布する方法を定めた、一連の規定、ルール、および実践のセットです。
セキュリティプロトコル	データの伝送をセキュリティで保護することを目的とするネットワーク通信プロトコルです。セキュリティプロトコルの例として、TLS、IPSEC、SSH、HTTPS などがあります。
機密エリア	データセンタ、サーバルーム、またはカード会員データを保管、処理、または伝送するシステムが設置されているエリアです。これには、小売店のレジなど、POS 端末のみが存在するエリアは含まれません。
機密認証データ	カード会員の認証またはペイメントカードトランザクションの承認（あるいはその両方）に使用されるセキュリティ関連情報（カード検証コード/値、磁気ストライプ全データ、PIN、PIN ブロック）です。
責務の分離	異なる担当者間で職務の工程を分離して、1 人の担当者がプロセスを破滅させることがないようにします。
サーバ	他のコンピュータに通信処理、ファイル記憶域、印刷機器へのアクセスなどのサービスを提供するコンピュータです。サーバには、Web、データベース、アプリケーション、認証、DNS、メール、プロキシ、NTP などがありますが、これらに限定されるわけではありません。
サービスコード	磁気ストライプ内の 3 桁または 4 桁の数値で、トラックデータ上でペイメントカードの有効期限に続いて記録されています。サービス属性の定義、取引の国内外の区別、使用制限の特定など、さまざまに使用されます。
サービスプロバイダ	他の事業体の委託でカード会員データの処理、保管、伝送に直接関わる、ペイメントブランドでない事業体です。これには、カード会員データのセキュリティを制御する、またはカード会員データのセキュリティに影響を与えうるサービスを提供する会社も含まれます。例として、マネージドファイアウォール、IDS およびその他のサービスを提供するマネージドサービスプロバイダや、ホスティングプロバイダなどの事業体が挙げられます。事業体が、通信リンクのみを提供する通信事業体など、公共ネットワークアクセスのプロビジョン*のみ*のサービスを提供する場合、その事業体はそのサービスのサービスプロバイダとみなされます（他のサービスのサービスプロバイダとみなされる場合もあります。
セッショントークン	セッショントークン（「セッション識別子」または「セッション ID」とも呼ばれる）は、Web ブラウザと Web サーバ間の特定のセッションの追跡に使用される一意の識別子（Cookie など）です。
SHA-1/SHA-2	「Secure Hash Algorithm」の頭字語です。SHA-1 および SHA-2 を含む、暗号ハッシュ関数のファミリまたはセットです。「強力な暗号化技術」を参照してください。「強力な暗号化技術」を参照してください。

用語	定義
スマートカード	「チップカード」または「IC カード（Integrated Circuit Card）」とも呼ばれます。集積回路を埋め込んだペイメントカードの一種です。回路は「チップ」とも呼ばれ、磁気ストライプデータと同等のデータおよびその他のデータを含むがこれらに限定されないペイメントカードデータが収録されています。
SNMP	「Simple Network Management Protocol」の頭字語です。管理者がすべきあらゆる状況に関して、ネットワーク接続デバイスの監視をサポートします。
知識分割	2 つ以上の事業体が別々にキーコンポーネントを持っており、個々の知識では暗号化キーを生成できないようにした状態を指します。
スパイウェア	悪意のあるソフトウェアの一種で、インストールされた場合、ユーザの同意なしにユーザのコンピュータを傍受したり、部分的に制御したりします。
SQL	「Structured Query Language」の頭字語です。リレーションシップデータベースマネジメントシステムでのデータの作成、変更、抽出に使用するコンピュータ言語です。
SQL インジェクション	データベース駆動型 Web サイトでの攻撃の形式です。悪意のあるユーザが、インターネットに接続されたシステム上で安全でないコードを利用して、不正な SQL コマンドを実行することです。SQL インジェクション攻撃は、通常はデータを入手できないデータベースから情報を盗むため、またはデータベースをホストしているコンピュータを介してして組織のホストコンピュータにアクセスするために使用されます。
SSH	「Secure Shell（セキュアシェル）」の略語です。リモートログインまたはリモートファイル転送などのネットワークサービスを暗号化するプロトコルスイートです。
SSL	「Secure Sockets Layer」の頭字語です。Web ブラウザと Web サーバ間のチャネルを暗号化するための業界標準です。現在は TLS に置き換えられています。*「TLS」を参照してください。*
ステートフルインスペクション	「動的パケットフィルタリング」とも呼ばれます。ネットワーク接続状態を追跡することでセキュリティを強化するファイアウォール機能 さまざまな接続の合法的なパケットを識別するようにプログラムされており、確立された接続に一致するパケットのみがファイアウォールを通過することを許可され、その他はすべて拒否されます。

用語	定義
強力な暗号化技術	業界で認められたテスト済のアルゴリズムに、十分なキーの長さ（最低 112 ビットの有効なキー強度）と適切なキー管理の実践が伴った暗号化技術です。暗号化技術とは、データを保護する技法で、暗号化（復号可能）とハッシング（「一方向」、つまり復号不能）の両方が含まれます。「ハッシュ」を参照してください。 本書の発行時点で業界で認められているテスト済の暗号化の標準およびアルゴリズムの例として、AES（128 ビット以上）、TDES/TDEA（3倍長キー）、RSA（2048 ビット以上）、ECC（224 ビット以上）、および DSA/D-H（2048/224 ビット以上）が挙げられます。暗号キー強度とアルゴリズムの詳細なガイダンスは、現行バージョンの NIST Special Publication 800-57 Part 1（http://csrc.nist.gov/publications/）を参照してください。 *注: 前述の例は、カード会員データの固定記憶域に適しています。PCI PIN および PTS に定義されたトランザクションベースの処理に関する暗号化の最小要件は、露呈レベルを低減するための追加コントロールが設けられているため、より柔軟です。* *すべての新しい実装で、128 ビット以上の有効なキー強度を使用することが推奨されます。*
SysAdmin	「システム管理者（System Administrator）」の略語です。コンピュータシステムまたはネットワークの管理を担当する、高い権限を持つユーザです。
システムコンポーネント	カード会員データ環境に含まれる、または接続されるすべてのネットワークデバイス、サーバ、コンピュータデバイス、アプリケーション
システムレベルオブジェクト	システムコンポーネント上に存在し、システムコンポーネントの運用に必要なあらゆるものを指します。これには、アプリケーションの実行可能ファイルや構成ファイル、システム構成ファイル、静的および共有ライブラリと DLL、システム実行可能ファイル、デバイスドライバ、デバイス構成ファイル、追加したサードパーティコンポーネントが含まれますが、これらに限定されません。
TACACS	「Terminal Access Controller Access Control System」の頭字語です。リモートアクセスサーバと認証サーバ間で通信するネットワークで、ネットワークへのユーザアクセス権を決定するために使用される、一般的なリモート認証プロトコルです。この認証手法をトークンやスマートカードなどと組み合わせて使用することで、多要素認証を行うことができます。
TCP	「Transmission Control Protocol」の頭字語です。インターネットプロトコル(IP)スイートのコアトランスポート層プロトコルの一つで、インターネットの基本通信言語またはプロトコルです。*「IP」*を参照してください。
TDES	「Triple Data Encryption Standard（トリプルデータ暗号化標準）」の頭字語で、「3DES」または「Triple DES」とも呼ばれます。DES 暗号を 3 回使用するブロック暗号です。「強力な暗号化技術」を参照してください。
TELNET	「Telephone Network Protocol」の略語です。一般に、ネットワーク上のデバイスに、ユーザ主導のコマンドラインログインセッションを提供します。ユーザ資格情報は平文で伝送されます。
脅威	情報または情報処理リソースが意図的または偶発的に失われたり、変更されたり、公開されたり、アクセス不能になったり、または影響を受けたりして、組織の損失を招く原因となる可能性がある状態または行為です。

用語	定義
TLS	「Transport Layer Security」の頭字語です。通信を行う 2 つのアプリケーション間で、データ機密性とデータ整合性を実現するために設計されています。TLS は SSL の後継です。
トークン	認証とアクセス制御の見地からは、トークンは認証サーバまたは VPN で使用され動的または多要素認証を行うハードウェアまたはソフトウェア提供の値です。「*RADIUS*」、「*TACACS*」、および「VPN」を参照してください。「セッショントークン」も参照してください。
トラックデータ	「全トラックデータ」または「磁気ストライプデータ」とも呼ばれます。ペイメントトランザクション中に、承認のために使用される磁気ストライプまたはチップにエンコードされたデータです。チップ上の磁気ストライプイメージ、または磁気ストライプのトラック 1 またはトラック 2（あるいはその両方）上のデータです。
取引データ	電子ペイメントカードトランザクションに関連するデータです。
トロイ	「トロイの木馬」とも呼ばれます。悪意のあるソフトウェアの一種で、インストールされた場合、トロイはユーザの認識なしにコンピュータシステムに対して不正な機能を実行している間に、ユーザには正常な機能を実行できるようにします。
トランケーション	PAN データのセグメントを完全に削除して、PAN 全体を読み取りできないようにする手法です。トランケーションは、ファイルやデータベースなどへの保存時の PAN の保護に関連します。画面や紙の領収書などに*表示*された PAN の保護については、「*マスキング*」を参照してください。
信頼できるネットワーク	組織の制御または管理の及ぶ範囲内のネットワークです。
信頼できないネットワーク	組織に属するネットワーク外のネットワーク、および組織の制御または管理が及ばないネットワークです。
UR:	「Uniform Resource Locator」 の頭字語です。インターネット上のネットワークリソースを特定するために Web ブラウザ、電子メールクライアント、および他のソフトウェアで使用されるフォーマットされた文字列
バージョン設定方法	アプリケーションまたはソフトウェアの特定の状態を一意に識別するためにバージョンスキームを割り当てるプロセス これらのスキームは、ソフトウェアベンダが定義したバージョン番号形式、バージョン番号用途、およびワイルドカード要素に従います。バージョン番号は通常昇順に割り当てられ、ソフトウェアの特定の変更に対応しています。
仮想アプライアンス（VA）	VA は一連の機能を実行するために事前に構成されたデバイスの概念を取得し、このデバイスをワークロードとして実行します。一般に、既存のネットワークデバイスはルーター、スイッチ、ファイアウォールなどの仮想アプライアンスとして実行するために仮想化されます。
仮想ハイパーバイザ	「*ハイパーバイザ*」**を参照してください。**
仮想マシン	独立したコンピュータのように動作する自己完結型のオペレーティング環境です。「ゲスト」とも呼ばれ、ハイパーバイザ上で動作します。

用語	定義
仮想マシンモニタ（VMM）	VMM はハイパーバイザに含まれ、仮想マシンのハードウェア抽象化を実装するソフトウェアです。VMM は、システムプロセッサやメモリなどのリソースを管理して、各ゲストオペレーティングシステムに必要なリソースを割り当てます。
仮想支払端末	仮想端末は、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。加盟店は安全に接続された Web ブラウザを使用してペイメントカードデータを手動で入力します。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。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。
仮想スイッチ/ルーター	仮想スイッチ/ルーターは、ネットワークインフラストラクチャレベルのデータのルーティングおよびスイッチング機能を提供する論理エンティティです。仮想スイッチは、ハイパーバイザのドライバ、モジュール、プラグインなどの仮想化サーバプラットフォームに内蔵されています。
仮想化	仮想化とは、コンピューティングリソースの物理的制約からの論理的抽象化のことです。一般的な抽象化の 1 つは仮想マシン（VM）と呼ばれます。仮想マシンでは、物理マシンの内容を取得して別の物理ハードウェア上や同じ物理ハードウェア上の他の仮想マシンとともに操作することができます。VM 以外に、仮想化もアプリケーション、デスクトップ、ネットワーク、記憶域など、さまざまな他のコンピューティングリソースで実行できます。
VLAN	「仮想 VLAN（Virtual LAN）」または「仮想ローカルエリアネットワーク（Virtual Local Area Network）」の頭字語です。単一の従来型物理ローカルエリアネットワークを越えて拡張可能な論理ローカルエリアネットワークです。
VPN	「仮想プライベートネットワーク（Virtual Private Network）」の頭字語です。一部の接続が、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行われるコンピュータネットワークです。この場合、仮想ネットワークのエンドポイントは、大規模ネットワークをトンネリングします。通常のアプリケーションでは公共のインターネットを介してセキュリティ保護された通信が行われますが、VPN は認証またはコンテンツの暗号化など強力なセキュリティ機能を使用する場合と使用しない場合があります。 VPN をトークンやスマートカードなどと組み合わせて使用することで、2 因子認証を行うことができます。
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。
WAN	「ワイドエリアネットワーク（Wide Area Network）」の頭字語です。一般に地域または会社全体のコンピュータシステムなど、広い範囲を対象とするコンピュータネットワークを指します。
Web アプリケーション	一般に Web ブラウザまたは Web サービスを使用してアクセスするアプリケーションです。Web アプリケーションはインターネットを使用する場合とプライベートの内部ネットワークを使用する場合があります。
Web サーバ	Web クライアントからの HTTP 要求を受け入れて、HTTP 応答（一般に Web ページ）を提供するプログラムが組み込まれたコンピュータです。

用語	定義
WEP	「Wired Equivalent Privacy」の頭字語です。ワイヤレスネットワークの暗号化に使用される弱いアルゴリズムです。WEP 接続は、容易に入手可能なソフトウェアで数分以内解読できる、などの重大な脆弱性が業界の専門家によって確認されています。*「WPA」を参照してください。*
ワイルドカード	アプリケーションバージョンスキーム内で定義されている文字のサブセットの代わりに使用する文字　PA-DSSの場合、ワイルドカードはセキュリティに影響しない変更を表すために使用できます。ワイルドカードは、ベンダのバージョンスキームの唯一の可変要素であり、ワイルドカード要素によって表される各バージョン間には、マイナーで、セキュリティ以外に影響を与える変更のみが存在することを示すために使用されます。
ワイヤレスアクセスポイント	「AP」とも呼ばれます。ワイヤレス通信デバイスをワイヤレスネットワークに接続できるようにするデバイスです。通常はワイヤード（有線）ネットワークに接続されており、ネットワーク上においてワイヤレスデバイスとワイヤード（有線）デバイス間でデータを中継できます。
ワイヤレスネットワーク	回線への物理的接続なしで、コンピュータを接続するネットワークです。
WLAN	「ワイヤレスローカルエリアネットワーク（Wireless Local Area Network）」の頭字語です。ワイヤーなしで 2 台以上のコンピュータまたはデバイスをリンクする、ローカルエリアネットワークです。
WPA/WPA2	「WiFi Protected Access」の頭字語です。ワイヤレスネットワークをセキュリティ保護するセキュリティプロトコルです。WPA は WEP の後継です。WPA の次世代プロトコルとして WPA2 も発表されました。