

ペイメントカード業界データセキュリティ基準 (PCI DSS)

ペイメントカード業界データセキュリティ基準(PCI DSS)は、業界全体にわたり適用される国際統一基準 およびプロセスであり、ペイメントカード業界セキュリティスタンダードカウンシル (PCI SSC)により統制され、主要な国際ペイメントカードシステムすべてによりサポートされています。この基準は、外部、及び内部のデータ漏洩のリスクを管理するために開発されています。

PCI DSSには、安全性の高いシステムの利用を重視する12項目の基本的な要件が定められています。この要件には、ファイアウォールのインストール、デフォルトパスワードの変更、保存したデータの保護、パブリックネットワーク全体でのウィルス対策ソフトウェアと暗号化伝送の使用などが含まれます。

貴社がVisaカードをお取り扱いの場合は、PCI DSS要件を順守しなければなりません。

お客様のビジネスにおけるメリット

PCI DSSの業界全体での要件を順守することで、参加組織は以下のような利点を得ることができます。

- 顧客の個人情報の保護
- 高度なデータセキュリティの提供により顧客からの信頼を向上
- 経済的損失と改善経費の削減
- 顧客の信頼を維持し、自社ブランドを保護
- 顧客の個人情報を保存、伝送しているビジネスに完全な「検診」を提供
- 貴社のお客様とビジネスの保護



詳細のお問い合わせとご相談について

弊社のメンバーカード会社（加盟店契約会社）とともに、貴社がペイメントカードをできる限り簡単で便利に、また安全にお取り扱いいただけるよう努めています。ご質問がある場合は、まず貴社のビザカード加盟店契約会社にご連絡くださるようお願い申し上げます。

PCI DSSの詳細に関しては、以下のウェブサイトもご覧ください。

貴社のお客様とビジネスの保護

ペイメントカード業界データセキュリティ基準 (PCI DSS)の導入に関するご案内



Visaアカウント情報セキュリティプログラム

<http://www.visa-asia.com/ap/jp/merchants/riskmgmt/ais.shtm>
Eメール: vpss@visa.com または apjprisk@visa.com



貴社のお客様やビジネスを危険からお守りください

増加の一途にあるハイテク犯罪から顧客のアカウント情報を保護することは、今日のビジネスが直面する最大の課題の一つとなっています。加盟店やその提携先がご利用のテクノロジーが発達するにつれ、カード犯罪もますます複雑なものとなっています。

カード会員のアカウントデータを処理、保存、伝送するビジネスであれば、このような犯罪に狙われる可能性があります。

ハッカーがコンピュータシステムにアクセスし、カード会員のデータを盗んだうえで、このデータを利用して犯罪を行うといった事件は、世界各国で多数発生しています。

加盟店や関連事業者には、機密とすべき個人金融情報を保護するために日常とらなければならない措置を理解していただくことが大切です。

問題が発生した場合

2005年、米国の大手プロセッサが深刻なセキュリティ侵害にあったことに続き、オーストラリア人12万人のクレジットカード情報が犯罪に使われる可能性にさらされました。この侵害は、カード不正検知システムによって検知されました。

昨年、強盗がデータベースにアクセスし、140万人のクレジットカード情報及びカード会員の名前を盗んだため、某有名靴店は、やむを得ず顧客にその旨を傳達することになりました。

別の事件では、店舗のソフトウェアに問題があったため、米国デザイナーブランドのブティックは、最高18万人の顧客のクレジットカード情報を漏洩するという事態に直面しました。

米国の某データブローカーは、14万5000人の顧客のアカウント情報が漏洩したために、1500万ドルの損害を被ったと報告しています。調査企業Gartner社の推定では、システムやプロセスの修正にかかった費用を考慮すると、漏洩したアカウント1件につき約118ドルの支出がかかったこととなります。

PCI DSSを導入することにより、データ漏洩のリスクを最小限に抑え、ビジネスにふりかかる金融債務、調査費用、さらに執拗なメディアの関心的になるリスクを防止することができます。

主要な要件12項目

PCI DSS要件に従い、以下を査定することができます。

- 貴社がカード会員データを保護しているかどうか
- 貴社のネットワークが安全なものであるかどうか
- 貴社が強力なアクセス管理措置を維持しているかどうか
- 貴社がネットワークを定期的に監視しテストしているかどうか
- 貴社がセキュリティ方針を維持しているかどうか
- 貴社がサードパーティーを活用しているかどうか。活用している場合は、その会社がPCI DSS要件を順守しているかどうか

主要な要件12項目は下表に記載されています。

PCI データ セキュリティ 基準	
セキュアネットワークの構築と維持	1. カード会員データを保護するため、ファイアウォールコンフィギュレーションをインストールし維持する 2. ベンダーから供給されたデフォルトのシステムパスワードやその他のセキュリティパラメータを使用しないこと
カード会員データの保護	3. 保存したカード会員データの保護 4. オープンなパブリックネットワーク全体においてカード会員データの伝送を暗号化
脆弱性管理プログラムの維持	5. ウィルス対策ソフトウェアを定期的に更新 6. 安全性の高いシステムとアプリケーションを開発、維持
強力なアクセス管理措置の導入	7. 情報を必要な人だけに開示するビジネスの仕方により、カード会員データへのアクセスを制限 8. コンピュータアクセスのための固有IDを各職員に割り当て 9. カード会員データへの物理的アクセスを制限
定期的なネットワークの監視とテスト	10. ネットワークリソースとカード会員データへのアクセスすべてを追跡記録し監視 11. セキュリティシステムとプロセスを定期的にテスト
情報セキュリティ方針の維持	12. 情報セキュリティに対処する方針を維持

ペイメントカード業界セキュリティスタンダード・カウンシル(PCISSC)のウェブサイト：
<https://www.pcisecuritystandards.org/>

PCI DSSと貴社のビジネス

貴社のビジネスにPCI DSSがどのように該当するか、またその導入方法は、以下の点により異なります。

- 貴社の事業規模や性質
- 貴社のカード取り扱いシステムとプロセスのコンフィギュレーション
- 貴社と提携しているサービスプロバイダとその会社の役割

始めるにはどうすればよいですか？

Visaでは、PCI DSSをより簡単に導入していただけるよう一連のツールとリソースをご用意いたしました。

Visaのプログラムはアカウント情報セキュリティ(AIS)と呼ばれています。このプログラムの詳細に関しては、<http://www.visa-asia.com/ap/jp/merchants/riskmgmt/ais.shtml>をご参照ください。

よくある質問

PCI DSS要件を満たしているかどうかどうやって確認できますか。

貴社がPCI DSS要件を満たしているかどうか確認するには、以下のバリデーションを行ってください。(貴社のVisa取扱件数月間平均によりどれを実施するかは異なります)。

- 問診票による自己診断
- 脆弱性スキャンテスト
- 訪問調査(オンサイトレビュー)

バリデーションすべてを行わなければならないのですか。

Visaでは、加盟店を以下の3レベルに分類し、どのバリデーションが必要かを定めています。

加盟店取扱規模		必要なバリデーション
レベル1	Visa取扱件数が年間600万件以上の加盟店	・年1回の訪問監査 ・年4回脆弱性スキャンテスト
レベル2&3	年間2万件以上のeコマースを取り扱っている加盟店	・年4回脆弱性スキャンテスト ・年1回問診票による自己診断
レベル4	その他の加盟店すべて	・年4回脆弱性スキャンテスト(推奨) ・年1回問診票による自己診断

問診票による自己診断とは何ですか

自己評価問診票は、貴社のPCI DSS順守状況の評価のために無料でお使いいただけるツールで、貴社の機密事項は保持されます。自己評価問診票は、二項選択方式の質問からなるオンラインのツールです。問診票にすべて回答いただくことで、貴社のリスクレベルを十分に把握することができます。査定により、是正措置が必要だとされた場合は、PCI DSSに順守するためにこの措置が必要となります。このプロセスは社内でも実施することもできますし、認定評価機関に代行を依頼することもできます。

脆弱性スキャンテストとは何ですか。

脆弱性スキャンは、不正アクセス、ハッキング、悪質なウィルスなどの外部からの脅威から貴社のシステムが保護されるようにするものです。スキャンツールテストは、貴社のネットワーク器具、ホスト、アプリケーションすべてを既知の脆弱性に関してテストします。スキャンは、認定ネットワークセキュリティスキャン業者が実施する非侵入型テストです。

貴社のシステムとアプリケーションがつねに適切なレベルで保護されているように保つためには、年4回の定期的なスキャンテストが必要です。Visaはの無料ネットワークスキャンを提供しています。詳細に関しては、<https://ais.hackersafe.jp> をご参照ください。

PCI DSSのバリデーションを受けると、どのような承認がなされるのですか。

貴社のメンバーカード会社がVisaに、貴社が要件を満たしたことを通達します。

このプログラムに参加しない場合はどうなりますか。

貴社が適切にカード番号等お客様の情報を保護せずデータの漏洩が発生した場合、お客様の経済的な損失を貴社及び貴社と契約のあるカード会社は負うことになり、貴社と契約のあるカード会社との加盟店契約を解除せざるを得なくなるなど不利益が発生する場合があります。