

## アカウント情報セキュリティ (AIS) プログラム

### Q&A 集

#### Q AIS とは？

A アカウント情報セキュリティ、もしくは AIS は、アカウントと取引情報を処理し、保存及び/または、送信するすべての事業者がクレジットカード業界 (PCI) のセキュリティ基準 (DSS) に従って業務を行うに際して、アカウント及び/または、取引情報を保護することを目的とした Visa によって提供されるセキュリティ管理プログラムです。

自ら基準を管理・監督するため、2006 年に 5 つの主要なカードブランド会社による業界団体 PCI Security Standards Council (PCI SSC) が設立されました。運営については各々のカード会社が認証要件、締切り及び、罰則料料についての要点をまとめた独自のプログラムを実行しています。

PCI DSS 及び PCI SSC の詳細についてのお問い合わせは、PCI SSC ウェブサイト [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org) にアクセスしてください。

#### Q どのような事業者が PCI DSS を遵守しなければならないのか？

A 加盟店、サービスプロバイダー (例えば、決済ゲートウェイ・IPSP・決済代行会社)、カード発行会社 (イシュア) 及び加盟店契約会社 (アクワイアラ) など、カードホルダーデータを保存、処理または/及び送信する全ての事業者が PCI DSS を遵守しなければなりません。当該要件は、対面販売の小売店、非対面販売の通販/テレフォンオーダー (MOTO) 及び、e コマースを含む全てのカード受入れチャネルに適用されます。

#### Q 第三者事業者がカードホルダーデータの取扱い、送信もしくは保存を外部委託した場合は？

A カード発行銀行 (イシュア) 及び、加盟店銀行 (アクワイアラ) の双方は共に、各々の加盟店が PCI DSS を遵守するサービスプロバイダーを使用し、且つその徹底に対して責任を負います。加盟店サービスプロバイダーと加盟店契約会社 (アクワイアラ) メンバー間に直接契約上の関係は無いとしても、Visa 加盟店契約会社 (アクワイアラ) は PCI DSS に対する不遵守に起因する全ての責任を負うものとします。

#### Q PCI DSS への遵守をどのように規定するか？

A 加盟店とサービスプロバイダーの遵守要件は、当該事業者により取り扱われるカードホルダーデータの年間取り扱い件数に基づきます。加盟店及びサービスプロバイダーのレベルと要件の詳細については [www.visa-asia.com/secured](http://www.visa-asia.com/secured) にアクセスしてください。

検証ツール：

- 毎年の PCI SSC の QSA によるオンサイト PCI データセキュリティアセスメント。
- 四半期ごとの PCI SSC の認定スキャニングベンダー (ASV) による外部と内部の脆弱性スキャン。
- 毎年の PCI DSS の自己問診 (SAQ) を使用した自己問診。

QSA、ASV、及び SAQ の詳細リストについては、[www.pcisecuritystandards.org](http://www.pcisecuritystandards.org) にアクセスしてください

**Q PCI の自己問診(SAQ)とは何か？**

A PCI 自己問診(SAQ)は、PCI DSS への遵守を自己評価するにあたって、加盟店及びサービスプロバイダーへの遵守支援を目的とした検証ツールです。SAQ は、ウェブサイト [www.pcisecuritystandards.org/saq/instructions.shtml](http://www.pcisecuritystandards.org/saq/instructions.shtml) からダウンロードすることができます。

**Q 脆弱性スキャンとは何か？**

A 潜在的なカードホルダーデータを脅かす恐れのある未承認または悪意に満ちたユーザーによるネットワークに対するアクセスは、情報漏えいなどの原因となります。脆弱性スキャンは、ネットワークにおける脆弱性または、ギャップが無いかをインターネットを経由して、自動的にネットワークを遠隔スキャンし評価判定するシステムです。

**Q PCI DSS の遵守は一回限りの要件か？**

A いいえ。PCI DSS の遵守は継続的なプロセスです。検証活動は事業者が年間に処理する取引件数に応じて、継続して全ての加盟店及びサービスプロバイダーは常時 PCI DSS を遵守することが求められます。

**Q 遵守についての期限はあるか？**

A はい。期限は以下の通りです：

レベル1 加盟店

- 禁止データ保存を保存していないこと、不所持を証明期限は、**2009年9月30日**。
- PCI DSS 遵守期限は、**2010年9月30日**。

レベル2 加盟店

- 禁止データ保存を保存していないこと、不所持を証明期限は、**2009年9月30日**。

サービスプロバイダー

- PCI DSS 遵守期限は、**2008年12月31日**。

**Q 加盟店のレベル決定の方法及び、その検証要件は？**

A PCI DSS 遵守の必須要件を鑑みながら、Visa は、Visa カードに関わる取引高・潜在的なりスク及び起こり得る脅威に基づいて検証レベルの決定を行っております。Visa は、毎年の PCI DSS 遵守の検証ルールをグローバル化して同じ条件で行うべく加盟店レベルと検証要件を同調させるシステムを確立しております：

レベル/ 段階	加盟店基準	検証要件
1	年間（全てのチャネル）の Visa 取引量 600 万件以上を処理する加盟店または、何れかの Visa リージョンでレベル1として認定されるグローバル加盟店	<ul style="list-style-type: none"> <li>■ 公認の監査会社（「QSA」）による遵守についての報告（「ROC」）</li> <li>■ 四半期毎の認定セキュリティ評価ベンダー（Approved Scan Vendor – 「ASV」）によるネットワークスキャン</li> <li>■ コンプライアンス遵守証明(Attestation of</li> </ul>

レベル/ 段階	加盟店基準	検証要件
		Compliance Form)
2	年間（全てのチャネル）の Visa 取引量 100 万から 600 万件未満を処理する加盟店	<ul style="list-style-type: none"> <li>年間自己問診（「SAQ」）</li> <li>ASV による四半期毎のネットワークスキャン</li> <li>コンプライアンス遵守証明(Attestation of Compliance Form)</li> </ul>
3	年間 20,000 件から 100 万件未満の e コマース取引量を処理する加盟店	<ul style="list-style-type: none"> <li>年間 SAQ</li> <li>ASV による四半期毎のネットワークスキャン</li> <li>コンプライアンス遵守証明(Attestation of Compliance Form)</li> </ul>
4	20,000 件以上の Visa e コマース取引量を処理する加盟店及び年間 Visa 取引量 100 件未満までを処理する全てのその他の加盟店	<ul style="list-style-type: none"> <li>年間 SAQ 推奨</li> <li>該当する場合 ASV による四半期毎のネットワークスキャン</li> <li>加盟店契約会社によるコンプライアンス検証要件</li> </ul>

\*全ての加盟店は、12ヶ月の期間にVisa取引量に基づいて4つのレベルに分類されることとなります。取引量は、特定の名称で事業営業中（「DBA」）の加盟店からのVisa取引（クレジット、デビット、プリペイドを含む）の総数に基づきます。加盟店会社が1DBA以上を擁する場合は、クライアントは会社事業体によって保存、処理または、送信される取引量の総数を以って検証要件を決定しなければなりません。データの総計が不明な場合、即ちかかる会社事業体が複合DBAを代表してカード保有者のデータを保存、処理または、送信していない場合は、メンバーは検証レベルを決定するに当たって以下の通りDBA個別の取引量を考慮するものとします。

**Q サービスプロバイダーのレベル決定の方法及び検証要件は？**

A Visa は、毎年の PCI DSS 遵守の検証を同じ条件で行うべく以下の通りに、サービスプロバイダーのレベルと検証要件をグローバルに同調させるシステムを確立しております：

レベル	全てのリージョン	検証要件
1	年間 300,000 件以上の取引を保存、処理及びまたは、送信する VisaNet プロセッサまたは、何れかのサービスプロバイダー	<ul style="list-style-type: none"> <li>公認の監査会社（「QSA」）による準拠性についての年間報告（「ROC」）</li> <li>ASV による四半期毎のネットワークスキャン</li> <li>コンプライアンス遵守証明(Attestation of Compliance Form)</li> </ul>
2	年間 300,000 件未満の取引を保存、処理及びまたは、送信する何れかのサービスプロバイダー	<ul style="list-style-type: none"> <li>年間自己問診（SAQ）</li> <li>ASV による四半期毎のネットワークスキャン</li> <li>コンプライアンス遵守証明(Attestation of Compliance Form)</li> </ul>

**Q アカウント情報セキュリティ（AIS）プログラムに参加しない選択をした場合は？**

- A AIS プログラムへの参加は、グローバルに全ての Visa カード発行（イシュア）及び加盟店カード会社（アクワイアラ）及びそのエージェント（例えば、加盟店、サービスプロバイダーなど）に必須の要件です。イシュアまたは、アクワイアラのエージェントが AIS 要件を遵守していないことが判明した場合は、当該イシュアまたは、アクワイアラは Visa により罰金を科せられることとなります。最終的には、加盟店及びサービスプロバイダーは Visa ペイメントプロダクトを継続して受け入れて行くためには AIS 要件を満たさなければなりません。

**Q. AIS プログラム要件に関して質問のある場合は、誰に連絡すれば良いか？**

- A 加盟店カード会社（アクワイアラ）に連絡するかまたは、以下の AIS ウェブサイト [www.visa-asia.com/secured](http://www.visa-asia.com/secured) にアクセスしてください。

PCI DSS 及びそれに関連する情報についてのお問い合わせは、ウェブサイト [www.pcisecuritystandards.org/about/contact.shtml](http://www.pcisecuritystandards.org/about/contact.shtml) にアクセスして PCI SSC 宛ご連絡ください。

## ペイメント・アプリケーション

### Q PA DSS とは何?

ペイメント・アプリケーション・データ・セキュリティ・スタンダード (PA-DSS)は、Visa によって導入されたペイメント・アプリケーション・ベストプラクティス (PABP)を基盤としたもので、当初は PCI DSS をサポートし、ソフトウェアベンダーのアプリケーションに於いて、セキュリティ面で強固である、磁気ストライプや PIN データ/セキュリティコードの全ての情報を保存しない安全性の高い決済システムの開発を支援する目的として、導入されました。PA-DSS は、Payment Card Industry Security Standards Council (PCI SSC)により PCI DSS 及び PCI PED などその他の業界基準と共に管理運営され、全ての主要な大手カードブランドにより承認されております。

PCI DSS 準拠についての要件詳細については、ウェブサイト [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org) にアクセスしてください。

### Q どのペイメント・アプリケーションの種類が PA-DSS 要件の対象となるか?

A PA-DSS は、ソフトウェアベンダー及び認証または、決済の一部としてカードホルダーのデータを保存、処理または、送信するペイメント・アプリケーション開発に適用されます。これらのペイメント・アプリケーションは、加盟店、サービスプロバイダーなどの第三者に販売、配布または、ライセンスされます。

PA-DSS に従って認証されたペイメント・アプリケーションは、PCI DSS 準拠環境に於いて一旦実行されれば、磁気ストライプ/トラック/セキュリティコード (CAV2, CID, CVC2 及び CVV2) /PIN データ及び PIN ブロックに対する脅威となる潜在的セキュリティ侵害及びそれらの侵害に起因する重大な損害をもたらす不正行為を最小限に止めることができます。

### Q どの種類のペイメント・アプリケーションが PA-DSS 要件の対象とならないか?

- A
1. 特定単一の顧客のために開発され販売されたペイメント・アプリケーションは PA-DSS 要件の対象とはなりません；しかしそれらのペイメント・アプリケーションは顧客自身の PCI DSS アセスメントにより填補されなければなりません。
  2. 加盟店または、サービスプロバイダーにより内部で開発され使用されるペイメント・アプリケーションで第三者に販売されないものについては PA-DSS の対象とはなりません；それらは加盟店またはサービスプロバイダー自身の PCI DSS アセスメントにより填補されなければなりません。
  3. スタンドアロン POS ターミナルにインストールされるペイメント・アプリケーションは PA-DSS 要件の対象とはなりません。
  4. 以下のリストは、全てを含むものではありませんが、PA-DSS を目的とするペイメント・アプリケーションに該当しないアプリケーションを例示しています：ペイメント・アプリケーションがインストールされた OS (例えば、Windows, Unix)、カードホルダーデータが保存されたデータベース・システム (例えば、Oracle)、及びカードホルダーデータを保存したバックオフィス・システム (例えば、レポート用または、顧客サービス目的)。

**Q PCI SSC は、既存のビザ PABP プログラムに基づき以前に認証済みであったアプリケーションを受け入れるか？**

**A** PCI SSC は PABP 認証済みのペイメント・アプリケーションを承認し、それらを認証対象となるように PABP バージョンにリストアップします。詳細については、以下の表をご参照ください。

		期間満了以前に PCI SSC リストに記載		期間満了後に PCI SSC リストに記載	
バージョン	有効期限	認証注記	配置注記	認証注記	配置注記
PABP 1.4	24 ヶ月	PABP に従って認証済	新配置で受入可	PABP に従って認証済	新配置での受入不可
PABP 1.3	18 ヶ月	PABP に従って認証済	新配置で受入可	PABP に従って認証済	新配置での受入不可
PABP 1.3 以前	12 ヶ月	PCI 前アプリケーション	新配置推奨不可	PCI 前アプリケーション	新配置での受入不可
PA-DSS 1.1	基準移行後 3 年	PA-DSS に従って認証済	新配置で受入可	PA-DSS に従って認証済	新配置での受入不可

**Q PA-DSS は、顧客に対してどのような影響を与えるか？**

**A** 安全なペイメント・アプリケーションは、顧客の PCI DSS コンプライアンスの促進に役に立ちます。PCI DSS 準拠環境に於いて一旦実行されれば、磁気ストライプデータ／セキュリティコード (CAV2, CID, CVC2 及び CVV2) /PIN データ及び PIN ブロックに対する脅威となる潜在的セキュリティ侵害を最小限に止めることができます。

**Q PA-DSS アセスメントはだれが実施するのか？**

**A** PCI SSC によって認定されたペイメント・アプリケーション・クオリファイド・セキュリティ・アセッサ (PA-QSA 認定評価機関) のみがペイメント・アプリケーションの精査を実施することができます...ここで留意していただきたいのは、QSA が全て PA-QSA ではないことです—即ち、QSA が PA-QSA の資格を得るためには、追加で取得しなければならない資格要件があるからです。PA-QSA の詳細は、PCI SSC のウェブサイトでご覧することができます。

**Q PA DSS 認証コストはどれぐらいか？**

**A** コンプライアンス認証は、ソフトウェアベンダーの経費で行われます。PA-DSS 認証のコストは、ペイメント・アプリケーションの複雑さとサイズに従って決定されるだけでなく、精査に要する時間及び PA-QSA の値段もコスト決定の要因となります。