アメリカン・エキスプレス

データセキュリティ運営方針（DSOP）– 日本

消費者保護のリーダーとして、アメリカン・エキスプレスは、カード保有者のデータおよび機密認証データを保護し常に安全な状態に保つことをお約束しています。

情報漏洩は、カード会員、加盟店、サービスプロバイダー、およびカード発行者にネガティブな影響を及ぼします。たった一度のデータ事故が、会社の信頼を深く傷つけ、効果的な業務遂行能力を損なう可能性があります。セキュリティに関する運営方針を遂行しこの脅威に取り組むことは、顧客の信頼を向上させ、収益を伸ばし、会社の評判を高めるのに役立ちます。

アメリカン・エキスプレス（以下「**アメリカン・エキスプレス**」または「**当社**」という）は、当社の加盟店およびサービスプロバイダー（以下総称して「**貴店**」という）が当社の懸念を共有していることを理解しており、貴店は、アメリカン・エキスプレスのカードの取扱い（加盟店の場合）または処理（サービスプロバイダーの場合）を行う契約（以下、「**契約**」という）で定められたデータセキュリティ条項、および当社が随時改定するデータセキュリティ運営方針を遵守するものとします。これらの要件は、暗号化キー、カード会員データ、または機密認証データ（またはそれらの組み合わせ）が保存、処理、または伝送される貴店のすべての設備、システム、ネットワーク（およびそのコンポーネント）に適用されます。

上記で定義されていない本文中の用語の定義は、本方針の別表 B に定められています。

第1条 - 暗号化キー、カード会員データおよび機密認証データの保護

貴店は、以下を必ず行い、また貴店関係者に行わせるものとします。

- カード保有者のデータを、契約に従い、またそれにより義務付けられる通り、アメリカン・エキスプレス・カードの取引を容易にするためのみに保存する。
- 最新バージョンのペイメントカード業界データセキュリティ基準（**PCI DSS**）とPCI PINセキュリティ要件が実施される発効日までに、それらを遵守する。
- 店舗にPIN入力装置またはペイメントアプリケーション（または両方）を設置または置換する際、PCI認定済みのもののみを使用すること。

貴店は、データセキュリティ条項に従い、契約において保有しているすべての当社の請求記録および取消記録を保護するものとし、契約で定められた目的のみにこれらの記録を使用し適宜それらを保護するものとします。貴店は、（第4条に他の規定がある場合を除いて、第4条に基づく本方針の貴店関係者の遵守証明とは別に）貴店関係者にデータセキュリティ条項を遵守させることについて、当社に財務上およびその他の義務を負うものとします。

第2条 - データ事故の管理義務

貴店は、速やかに、データ事故の発覚から原則24時間以内に、当社に通知するものとします。

当社に通知するには、当社営業担当者、またはアメリカン・エキスプレス加盟店サービスホットライン 0120-333983（9:00-17:00／土日祝休）に連絡するものとします。貴店はまた、+1 (602) 537-3021（+は国際直通ダイヤルの「IDD」を表し、国際通話料金が適用）からアメリカン・エキスプレスのエンタープライズインシデントレスポンスプログラム（**EIRP**）に連絡する（英語のみ）か、またはEIRP@aexp.comに電子メールを送信する（英語のみ）ことができます。貴店は、かかるデータ事故に関する窓口として担当者を指定しなければなりません。

- 貴店は、各データ事故の徹底的なフォレンジック調査を実行しなければなりません。異なる10,000件以上のアメリカン・エキスプレスのカード番号が関与するデータ事故の場合（または当社の要請に基づき）、データ事故の発覚から5日以内に、あるいはアメリカン・エキスプレスの独自の裁量に基づく要請により、PCIフォレンジック調査機関（PFI）にこの調査を依頼しなければなりません。調査完了後10営業日以内に、フォレンジック調査のレポートを未編纂のまま、当社に提出しなければなりません。必要な

場合、アメリカン・エキスプレスは別途PFIに調査を依頼し、この調査費用を貴店に課す場合があります。貴店は、データ事故について徹底的なフォレンジック調査を実施しなければなりません。貴店は、すべての漏洩したカード番号とデータ事故のフォレンジック調査レポートを当社に速やかに提出しなければなりません。当社は、データ事故に関連するカード番号を特定するため、独自に内部分析を行う権利を有します。

- 貴店は、すべての漏洩したカード番号とデータの事故のフォレンジック調査レポートをアメリカン・エキスプレスに速やかに提供する必要があります。アメリカン・エキスプレスは、データ事故に関係するカード番号を特定するため、独自に内部解析を行う権利を留保します。
- 貴店は、アメリカン・エキスプレスと協力して、データの事故から生じた問題を修正しなければなりません。これには、データの事故の影響を受けたアメリカン・エキスプレスのカード会員への通信に関するアメリカン・エキスプレスとの協議、および契約と整合する方法で、今後のデータの事故を防止する能力を確認するための、すべての関連情報のアメリカン・エキスプレスへの提供（および提供に必要な放棄の取得）が含まれます。

フォレンジック調査のレポートは、PCIから入手できる最新のフォレンジック事故最終レポートテンプレートを使って作成しなければなりません。PFIは、フォレンジックレビュー、準拠状況報告書、およびデータ事故に関するその他の関連する情報を含み、データ事故の原因を特定し、貴店がデータ事故の際にPCI DSSに準拠していたか否かを確認し、さらに、(i) すべてのPCI DSSの非準拠要件に対するアクションプランを提出し、(ii) 後述するアメリカン・エキスプレスのコンプライアンスプログラムに参加することにより、将来のデータ事故防止能力について検証します。アメリカン・エキスプレスの要請により、貴店は、認定審査機関（**QSA**）による不足が改善されたことを示す検証を提供するものとします。

契約の秘密保持の条項にも関わらず、当社は、適用ある法律、裁判所、行政、または規制機関の命令、法令、召喚状、要請、またはその他のプロセスにより義務付けられている通り、不正利用もしくはその他の損害のリスクを軽減するために、またはその他アメリカン・エキスプレスのネットワークの運営に適切な限りで、データ事故に関する情報を、アメリカン・エキスプレスのカード会員、カード発行者、アメリカン・エキスプレスネットワークの提携会社、および一般に開示する権利を保持します。

第3条 - データ事故の損害賠償義務

貴店の当社への損害賠償の義務は、当社のその他の権利および救済手段を放棄することなく、本第 3 条に基づき決定されるものとします。貴店は、以下の場合、当社にデータ事故賠償金を支払うものとします。

- データ事故について、事故の発覚から24時間以内に当社に通知することを怠った場合。
- データ事故の発覚から5日以内に、あるいはアメリカン・エキスプレスの要請に基づいて、PFIに調査を依頼することを怠った場合。
- 調査完了後10営業日以内に、未編纂のフォレンジック調査レポートを提出することを怠った場合。
- すべての漏洩したカード番号を速やかに当社に提出することを怠った場合。
- 将来のデータ事故防止能力についての検証も含み、データ事故に起因する問題を解決することを怠った場合。

以下の場合、当社は、前項に規定する要因に基づいて課されるデータ事故賠償金以外に、データ事故に関して貴店に損害賠償を求めることはありません。アメリカン・エキスプレス・カード口座番号のみに関するデータ事故については、1 事故につき 10 万米ドルを超えない範囲でデータ事故賠償金を当社に対して速やかに支払うものとします。機密認証データを含むアメリカン・エキスプレスのカード番号のデータ事故については、当社に対して以下を速やかに支払うものとします。

- データ事故1件につき、10万米ドルを超えない範囲のデータ事故賠償金（本条第2項の規定以外の要因も考慮し、アメリカン・エキスプレスによって決定される）
- カード番号1件につき5米ドル（この算出方法は、2016年4月14日を過ぎてアメリカン・エキスプレスに報告されたデータ事故すべてに適用される）

アメリカン・エキスプレスは、その費用算出から、機密認証データを伴うアメリカン・エキスプレス・カード番号の他のデータ事故に関連するアメリカン・エキスプレス・カード番号は除外します。ただし、当社が通知日の12カ月前以内に該当する他のデータ事故の通知を受領している場合に限ります。本方法に基づく当社の算出額は最終的なものとします。

加盟店のデータ事故に対する賠償義務は、契約における偶発的、間接的、投機的、結果的、特殊な、処罰的、または懲罰的損害賠償とはみなさないものとします。ただし、このような義務には、逸失利益や収入減、営業権の侵害、営業機会の逸失に関するものや類するものは含みません。

アメリカン・エキスプレスは、独自の裁量に基づき、2017年10月13日以降に発覚したデータ事故に限り、以下の各基準を満たす加盟店について賠償義務を減免する場合があります。

- 適用されるリスク緩和テクノロジーがデータ事故の前に使用されており、データ事故イベントウインドウ中に使用されていたこと。
- Payment Card Industry Forensic Investigator（PFI）プログラムに従って徹底的な調査が完了していること（事前に書面によりその他合意した場合を除く）。
- フォレンジックレポートにおいて、データ事故発生時のデータ処理、保存および/または伝送に使用されていたリスク緩和テクノロジーが明記されていること。
- 加盟店が難読化されていない機密認証データまたはカード保有者のデータを保存していないこと（およびデータ事故イベントウィンドウ中に保存していなかったこと）。

賠償義務が減免される場合、賠償義務（支払われるべき非遵守費用を除く）の減免は以下のように決定されます。

賠償義務の減免	要求される基準
標準減免:50%	合計取引金額の 75%超がチップ対応機器で処理されていること [1] または
	加盟店舗の 75%超でリスク緩和テクノロジーが使用されていること [2]
拡張減免: 75%～100%	合計取引金額の 75%超がチップ対応機器で処理されていること [1] かつ、加盟店舗の 75%超で別のリスク緩和テクノロジーが使用されていること [2]

[1] アメリカン・エキスプレスの内部解析により判定

[2] PFI 調査により判定

- 拡張減免（75%～100%）は、合計取引金額のうちチップ対応機器で処理されているものの比率および、加盟店舗のうち別のリスク緩和テクノロジーが使用されている店舗の比率のいずれか低い方に基づいて判定されます。下の例では、賠償義務の減免の計算について説明しています。
- リスク緩和テクノロジーとして適格となるためには、その設計および使用目的にしたがって、当該テクノロジーを有効に活用していることを実証する必要があります。たとえば、チップ対応機器を導入しているものの、チップ カードを磁気ストライプまたはキー入力取引として処理している場合は、このテクノロジーを有効に活用しているとはみなされません。
- リスク緩和テクノロジーが使用されている店舗の比率は、PFI調査により判定されます。
- 賠償義務の減免は、データ事故に関連して支払われるべき非遵守費用には適用されません。

例	リスク緩和 テクノロジーの使用	賠償義務の拡張減免の対象となるか?	減免
1	取引金額の 80%がチップ対応機器で処理されている 店舗の 0%でリスク緩和テクノロジーを使用している	いいえ	50%:標準減免（リスク緩和テクノロジーの使用率が 75%以下のため、拡張減免の対象とはなりません）[1]
2	取引金額の 80%がチップ対応機器で処理されている 店舗の 77%でリスク緩和テクノロジーを使用している	はい	77%:拡張減免（リスク緩和テクノロジーの使用率 77%に基づく）
3	取引金額の 93%がチップ対応機器で処理されている 店舗の 100%でリスク緩和テクノロジーを使用している	はい	93%:拡張減免（チップ対応機器での取引金額の比率 93%に基づく）
4	取引金額の 40%がチップ対応機器で処理されている 店舗の 90%でリスク緩和テクノロジーを使用している	いいえ	50%:標準減免（チップ対応機器での取引金額の比率が 75%以下のため、拡張減免の対象とはなりません）

[1] 口座番号 1 件当たり US $5 の、10,000 件のアメリカン・エキスプレス・カード口座番号が関わるデータ事故では（10,000 x $5 = $50,000）、非遵守費用を除き、賠償義務の 50%減免の対象となり、賠償義務が US $50,000 から US $25,000 に減額される場合があります。

第4条 - 【重要】システムの定期的検証

貴店は、PCI DSSに基づき、以下に説明する手順により、カード会員データまたは機密認証データが保存、処理、または伝送される、貴店および貴店のフランチャイズ店の設備、システム、および／またはネットワーク（およびそのコンポーネント）の状態を年次および毎四半期に検証するものとします。

検証を完了するための手順は以下のとおりです。

手順 1 –本方針に基づきアメリカン・エキスプレスのコンプライアンスプログラムに参加する

手順 2 –貴店のレベルと検証要件について理解する

手順 3 –調査報告書を完成させる

手順 4 –指定の期間内に調査報告書を当社に提出する

手順 1 –本方針に基づきアメリカン・エキスプレスのコンプライアンスプログラムに参加する

レベル1の加盟店、レベル2の加盟店、およびすべてのサービスプロバイダーは、以下に説明するとおり、一般的なデータセキュリティの窓口になる個人のフルネーム、電子メールアドレス、電話番号、および住所を提供することにより、本方針に基づきアメリカン・エキスプレスのコンプライアンスプログラムに参加する必要があります。貴店は、以下の手順4に記載する方法のいずれかにより、この情報を当社の代理でプログラムを管理するTrustwave社に提出するものとします。貴店は、この情報が変更された場合、Trustwave社に通知し、適宜、更新された情報を提供しなければなりません。

アメリカン・エキスプレスは、独自の裁量に基づき、特定のレベル3およびレベル4の加盟店に、本方針に基づき、書面の通知を送付することにより、アメリカン・エキスプレスのコンプライアンスプログラムに登録するよう要請する場合があります。指定された加盟店は、通知の受領から90日以内に登録しなければなりません。

当社は、当社の費用で、当社が選択した認定審査機関（QSA）を利用し、貴店のPCI検証プロセスの結果を確認する場合があります。

手順 2 –貴店のレベルと検証要件について理解する

アメリカン・エキスプレスのカード取引件数に基づいて、4つのレベルの加盟店と2つのレベルのサービスプロバイダーがあります。加盟店の場合、これは、最高のアメリカン・エキスプレス加盟店アカウントレベルを頂点とする加盟店の施設により提出された取引件数です。

*貴店は、加盟店およびサービスプロバイダーの以下の表に指定されたレベルの1つに該当します。*フランチャイザーの場合、カード取扱件数にフランチャイズ加盟店からの取引件数が含まれます。フランチャイズ加盟店に、特定のPOSシステムまたはサービスプロバイダーを使用するよう義務付けているフランチャイザーは、その影響下にあるフランチャイズ加盟店の調査報告書も提出する必要があります。

加盟店の要件

加盟店（サービスプロバイダーを除く）は、4つのレベルと検証要件に分類されます。以下のリストから加盟店のレベルを特定し、加盟店の表で該当レベルの調査報告書の要件を確認してください。

レベル1の加盟店 -アメリカン・エキスプレスのカードの年間取引高が250万件以上、またはその他アメリカン・エキスプレスがレベル1と見なすサービスプロバイダー。

レベル2の加盟店 - アメリカン・エキスプレスのカードの年間取引高が5万件以上250万件未満の加盟店。

レベル 3 の加盟店 - アメリカン・エキスプレスのカードの年間取引高が 1 万件以上 5 万件未満の加盟店

レベル 4 の加盟店 - アメリカン・エキスプレスのカードの年間取引高が 1 万件未満の加盟店

加盟店の表

	調査報告書		
加盟店レベル／アメリカン・エキスプレスの年間取引件数	**コンプライアンスのオンサイト評価レポート（ROC）**	**自己問診（SAQ）および四半期毎のネットワークスキャン**	**有資格加盟店の STEP 証明**
レベル 1/ 250 万件以上	必須	該当なし	オプション（ROC に代わる）
レベル 2/ 5 万件以上 250 万件未満	オプション	SAQ 必須（オンサイト評価レポートを提出する場合を除く）特定の種類の SAQ はスキャンが必須	オプション（SAQ およびネットワークスキャン、または ROC に代わる）
レベル 3/ 1 万件以上 5 万件未満	オプション	オプション（SAQ およびネットワークスキャン、または ROC に代わる）特定の種類の SAQ はスキャンが必須	オプション（SAQ およびネットワークスキャン、または ROC に代わる）
レベル 4/ 10,000 件 以下	オプション	SAQ はオプション（アメリカン・エキスプレスが要請する場合は必須）特定の種類の SAQ はスキャンが必須	オプション（SAQ およびネットワークスキャン、または ROC に代わる）

*誤解を避けるために付言すると、レベル3およびレベル4の加盟店は、アメリカン・エキスプレスの裁量に基づき要求される場合を除き調査報告書を提出する必要はありませんが、必ず本データセキュリティ運営方針のその他すべての条項を遵守しなければならず、それらに基づく責任を負います、

セキュリティテクノロジー強化プログラム（STEP）

PCI DSS に準拠している加盟店も、カード処理環境全体において追加のセキュリティテクノロジーを使用している場合、アメリカン・エキスプレスの裁量に基づき、当社のセキュリティテクノロジー強化プログラム（STEP）の対象とみなされることがあります。STEP が適用されるのは、加盟店で過去 12 カ月にデータ事故が発生しておらず、全カード取引件数の最低 75%が次のテクノロジーを使用している場合のみです。

- EMV - 有効で最新のEMVCo (www.emvco.com)の承認/認定を取得しAEIPS準拠チップカード取引の処理が可能な、チップ対応機器での取引。
- ポイントツーポイント暗号化 (P2PE) - PCI-SSC承認またはQSA承認のポイントツーポイント暗号化システムを使って、加盟店のプロセッサーと通信された取引。

セキュリティテクノロジー強化プログラムの有資格加盟店では、下の手順3でさらに述べるように、PCI調査報告書の要件が引き下げられています。

サービスプロバイダーの要件

サービスプロバイダー（加盟店を除く）は、2つのレベルと検証要件に分類されます。以下のリストからサービスプロバイダーのレベルを特定し、サービスプロバイダーの表で該当レベルの調査報告書の要件を確認してください。

レベル1のサービスプロバイダー - アメリカン・エキスプレスのカードの年間取引件数が250万件以上、またはその他当社がレベル1とみなすサービスプロバイダー。

レベル2のサービスプロバイダー - アメリカン・エキスプレスのカードの年間取引件数が250万件未満、または当社がレベル1でないとみなすサービスプロバイダー。

サービスプロバイダーは、セキュリティテクノロジー強化プログラムの対象ではありません。

サービスプロバイダーの表

レベル	調査報告書	必須性
1	年次オンサイトセキュリティ評価レポート	必須
2	年次の自己問診 D（サービスプロバイダー）および四半期毎のネットワークスキャン。 または、希望する場合、コンプライアンスの年次のオンサイトセキュリティ評価レポート	必須

サービスプロバイダーも、PCI 認定認定機関補助検証に準拠することが推奨されます。

手順 3 –調査報告書を完成させる

前述の加盟店の表とサービスプロバイダーの表に記載のある通り、以下の報告書が各レベルの加盟店とサービスプロバイダーに対して要求されます。

年次オンサイトセキュリティ評価 - 年次オンサイトセキュリティ評価は、カード会員データまたは機密認証データ（またはその両方）が保存、処理、または伝送される貴店のすべての設備、システム、およびネットワーク（およびそのコンポーネント）の詳細なオンサイト監査です。オンサイト監査は、

- QSAまたは
- 貴店により実施され、貴店の最高経営責任者、最高財務責任者、最高情報責任者、または担当部門長により保証され、該当する準拠証明書（**AOC**）を当社に毎年提出しなければなりません。

AOCは、PCI DSSのすべての要件の準拠を証明するものでなければならず、要請により、準拠に関する完全なレポートのコピーを含める必要があります（レベル1の加盟店とレベル1のサービスプロバイダー）。

年次自己問診 - 年次自己問診は、カード会員データもしくは機密認証データ（またはその両方）が保存、処理、または伝送される貴店のすべての設備、システム、およびネットワーク（およびそのコンポーネント）の自己検証ができるPCI DSSの自己問診（**SAQ**）を利用するプロセスで、貴店が実施し、貴店の最高経営責任者、最高財務責任者、最高情報責任者、または担当部門長が保証しなければなりません。貴店は、SAQのAOC部分を当社に毎年提出しなければなりません。SAQのAOC部分は、PCI DSSのすべての要件の準拠を証明するものでなければならず、要請により、SAQの完全なコピーを含める必要があります（レベル2、通知されたレベル3およびレベル4の加盟店、レベル2のサービスプロバイダー）。

四半期毎のネットワークスキャン - 四半期毎のネットワークスキャンは、潜在的な弱点および脆弱性について、貴店のインターネットに接続されたコンピューターネットワークとウェブサーバーを遠隔でテストするプロセスです。これは、認定スキャニングベンダ（**ASV**）により実施されなければなりません。貴店は、ASV スキャンレポート、スキャン準拠証明書（**AOSC**）またはスキャン結果に関するエグゼクティブサマリー（要請により、完全なスキャンのコピー）を毎四半期作成し、当社に提出しなければなりません。AOSC またはエグゼクティブサマリーでは、結果がPCI DSS のスキャニング手順を満たし、高リスクの問題が特定されておらず、スキャンが合格または適合していることを証明する必要があります（オンサイトセキュリティ評価レポートも提出した加盟店以外、STEP 有資格加盟店、およびすべてのサービスプロバイダー）。疑義を避けるために付言すると、該当する自己問診で求められる場合、四半期毎のネットワークスキャンは必須です。

年次セキュリティテクノロジー強化プログラム（STEP）認証検証文書 - アメリカン・エキスプレス年次 STEP 資格認証（「STEP 認証」）は、上記の手順 2 に列挙された基準を満たす加盟店のみが利用できます。STEP 認証には、PCI DSS 要件を使用する処理が含まれ、カード保有者のデータまたは機密認証データ（またはその両方）が保管、処理、または伝送される貴店の設備、システム、およびネットワーク（およびそのコンポーネント）の自己検査を可能にします。それは、貴店により実施され、貴店の最高経営責任者、最高財務責任者、最高情報責任者、または主任により認定されなければなりません。貴店は、アメリカン・エキスプレスに STEP 認証フォームを年 1 回提出することによって、当プロセスを完了しなければなりません。（STEP 有資格加盟店のみ）。年次セキュリティテクノロジー強化プログラム認証フォームは、Trustwave のセキュアポータルからダウンロードできます。

コンプライアンスの要約（「SOC」）とは、フランチャイザーまたはサービスプロバイダーがフランチャイズ加盟店の PCI コンプライアンス状況を報告できる文書のことです。SOC テンプレートは、Trustwave 社のセキュアポータルからダウンロードできます。

PCI DSS 非準拠 – 疑義を避けるために付言すると、貴社が PCI DSS に準拠していない場合、以下の文書の 1 つを提出しなければなりません。

- 準拠証明書（AOC）、「パート4、非準拠状態のためのアクションプラン」を含む
- PCI優先アプローチツールのサマリーおよび準拠証明（PASAOC）
- プロジェクトプランテンプレート（Trustwave社のセキュアポータルからダウンロード可能）

上記の各文書は、コンプライアンスの達成のために、ドキュメント完成日から12カ月以内に改善日を指定しなければなりません。貴店は、以下の手順4に記載した方法のいずれかにより、該当する文書を当社に提出しなければなりません。貴店は、非準拠状態に対する改善（レベル1、レベル2、レベル3、およびレベル4の加盟店、すべてのサービスプロバイダー）に基づき、アメリカン・エキスプレスに改善に向けた進捗の定期的な更新情報を提供するものとします。疑義を避けるために付言すると、PCI DSSに準拠していない加盟店は、セキュリティテクノロジー強化プログラム（STEP）の対象ではありません。

当社は、改善日以前の非準拠に対して、貴店に後述する非準拠による違反金を課さないものとしますが、貴店は、データ事故によるすべての損害賠償の義務に関して当社に責任を負っており、また本方針のその他すべての条項の対象となります。

手順4 -調査報告書を当社に提出する

すべての加盟店とサービスプロバイダーは、手順2の表で「必須」と記された調査報告書を提出しなければなりません。

貴店は、以下の方法のいずれかでTrustwave社に調査報告書を提出するものとします。

セキュアポータル：調査報告書をTrustwave社のセキュアポータルを介してアップロードすることができます。

このポータルの使用に関する説明は、Trustwave社に電話（+1 (312) 267-3208）もしくは電子メール（AmericanExpressCompliance@trustwave.com）にてご連絡ください（英語のみ）。

セキュアファックス：調査報告書をファックスで送信することができます。ファックス番号 +1 (312) 276-4019（+は国際直通ダイヤル「IDD」コードです。国際通話料金がかかります）。氏名、貴店名、データセキュリティ担当者名、住所、電話番号、加盟店の場合は10桁のアメリカン・エキスプレス加盟店番号もご記入ください。

プログラムや上記プロセスについて一般的なご質問がある場合は、Trustwave社に電話（+1 (312) 267-3208）もしくは電子メール（AmericanExpressCompliance@trustwave.com）にてご連絡ください（英語のみ）。

基準の準拠や検証は貴店の費用で実施するものとします。調査報告書を提出することにより、貴店は当社に対して、その中に記された情報の公開を許可されていること、および他の第三者の権利を侵害することなく当社に調査報告書を提出していることを表明し、保証します。

未検査費および契約の終了

アメリカン・エキスプレスは、これらの要件を満たさない場合、あるいは必要な調査報告書をアメリカン・エキスプレスに期日までに提出しない場合、非遵守課徴金を課す権利及び契約を終了する権利を有しています。アメリカン・エキスプレスは別途、各年次、四半期毎の報告期日をお知らせします。

説明	レベル1の加盟店またはサービスプロバイダー	レベル2の加盟店、レベル2サービスプロバイダー、またはSTEP加盟店	レベル3またはレベル4の加盟店
調査報告書が最初の期日までに未受領の場合、非遵守課徴金が課せられます。	¥3,000,000	¥60,000	¥2,000/月
調査報告書が最初の期日から30日以内に未受領の場合、追加の非遵守課徴金が課せられます。	¥4,000,000	¥120,000	
調査報告書を最初の期日から60日以内に未受領の場合、追加の非遵守課徴金が課せられます。	¥5,200,000	¥180,000	

アメリカン・エキスプレスが必要な調査報告書を最初の期日から60日以内に未受領の場合は、 アメリカン・エキスプレスは契約条件に基づいて契約を終了する権利に加えて非遵守課徴金の累積合計を課す権利を有しています。

第5条 - 秘密保持

当社は、貴店の準拠レポートを保管するために適切な措置を講じ（Trustwave社を含む代理人や下請け業者に講じさ

せ）ます。これには、データ受領日から3年間、調査報告書の秘密を保持することや調査報告書を第三者（当社の関連会社や代理人、代表者、サービス提供者、下請け業者を除く）に開示しないことを含みます。ただし、この秘密保持に関する義務は以下の調査報告書には適用されません。

i. 当社に開示する以前に既知のもの
ii. 当社による本項の不履行ではなく、公開されているものあるいは公開されたもの
iii. 秘密保持義務なしに合法的に第三者から当社が入手したもの
iv. 当社が個別に作成したもの
v. 裁判所の命令、法律、法規、召喚、開示要求、喚問、他の行政手続または訴訟手続、政府機関（取締官、検査官、審査官、司法当局など）により開示を要求されたもの

第6条 - 免責事項

当社は、商品性あるいは特定の目的への適合性に関するいかなる保証も含め、このデータセキュリティ運営方針(DSOP)、PCI DSS、EMVの仕様および設定、QSA、ASV、PFI（あるいはこれらのうちいずれか）の任務遂行に関して、明示黙示、法的を問わずいかなる表明も保証もするものではなく、責任を負うものではありません。アメリカン・エキスプレスのカード発行者は、本方針下では第三者受益者ではありません。

ウェブサイトのご案内

アメリカン・エキスプレス データセキュリティ：

http://www.americanexpress.com/datasecurity

PCI Security Standards Council, LLC：

https://ja.pcisecuritystandards.org/minisite/en/

定義

本方針に限って、以下の定義を適用します。

EMV仕様とは、EMVCoより発行された仕様をいいます。これは次のURLで閲覧できます。http://www.emvco.com

PCI DSSとは、ペイメントカード業界データセキュリティ基準をいいます。これは以下のURLで閲覧できます。
https://www.pcisecuritystandards.org/

PCI PINセキュリティ要件とは、ペイメントカード業界PINセキュリティ要件をいいます。これは次のURLで閲覧できます。
https://www.pcisecuritystandards.org/

PCI認定済みとは、PIN入力装置またはペイメントアプリケーション（あるいは両方）が設置時点で、PCI SSCが管理する承認された会社およびプロバイダに掲載されていることをいいます。これは以下のURLで閲覧できます。

https://www.pcisecuritystandards.org/

PCIフォレンジック調査機関または**PFI**とは、PCI SSCに認定された、ペイメントカードデータの流出や漏洩についてフォレンジック調査を行う機関をいいます。

PIN入力装置とは、PCI PINトランザクションセキュリティ（PTS）、加盟店端末装置（POI）、モジュラーセキュリティ要件の最新版用語集に掲載されています。これは以下のURLで閲覧可能です。

https://www.pcisecuritystandards.org/

POSシステムとは、情報処理システムまたは設備をいい、承認取得や取引データ収集などのために加盟店で使用されている端末、パソコン、レジ、非接触リーダー、支払エンジンまたは処理を含みます。

アメリカン・エキスプレス・カードまたは**カード**とは、アメリカン・エキスプレスあるいは加盟店の名前、ロゴ、商標、サービスマーク、商品名、その他の独占所有権のあるデザインが付記され、発行者により発行されたカード、口座アクセス機器、支払機器またはサービス、あるいはカード口座番号のことです。

暗号化キー（「アメリカン・エキスプレス暗号化キー」）とは、カードデータの処理、生成、読み込みおよび/または保護におけるすべてのキーをいいます。これには以下を含みますが、限定するものではありません。主な暗号化キー：ゾーンマスターキー（ZMK）およびゾーンピンキー（ZPK）

- 安全な暗号化装置に用いられているマスターキー：ローカルマスターキー（LMKs）
- カードセキュリティコードキー（CSCK）
- PINキー：一次鍵（BDK）、PIN 暗号化キー（PEK）、およびZPK

カード会員とは、以下の個人または組織をいいます。(i) カード発行者とカード番号発行に関する約定を結んだ者、あるいは、(ii) カードに名前が表示されている者。

カード会員情報とは、アメリカン・エキスプレスのカード会員およびカード取引に関する情報をいい、氏名、住所、カード番号、およびセキュリティコード（**CID**）を含みます。

カード会員データの意味はPCI DSSの最新版用語集に掲載されています。

加盟店とは、アメリカン・エキスプレスまたはその関連会社との契約の下で、アメリカン・エキスプレス・カードを受け入れる加盟店およびそのすべての関連会社のことです。

貴店関係者とは、貴店の従業員、代理人、代表者、下請契約者、プロセッサー、サービスプロバイダー、POS設備やシステムの業者、決済処理ソリューション事業者、貴店の関連会社、および契約に基づいて貴店がカード会員データまたは機密認証データ（あるいは両方）を提供している業務提携先企業などのいずれかあるいは全部を指します。

機密認証データの意味はPCI DSSの最新版用語集に掲載されています。

サービスプロバイダーとは、認可されたプロセッサー、第三者プロセッサー、ゲートウエイプロバイダー、POSシステムのインテグレーター、および加盟店に対してPOSシステムあるいは

他の決済処理ソリューションまたはサービスを提供するプロバイダーのことです。

自己問診または**SAQ**とは、PCI SSCが、PCI DSS準拠の評価と証明を目的に作成した自己評価ツールをいいます。

コンプライアンスの要約（SOC）とは、フランチャイザーまたはサービスプロバイダーが、その影響下にあるフランチャイズ加盟店のPCIコンプライアンス状況を示すために使用するPCI検証文書のことです。

準拠証明書または**AOC**とは、PCI SSCに提供されたフォームで、貴店のPCI DSSの準拠状況の申告書をいいます。

スキャン準拠証明書または**AOSC**とは、PCI SSCにより提供されたフォームで、ネットワークスキャンに基づく貴店のPCI DSSへの準拠状況の申告書をいいます。

請求とは、カードでなされる支払いまたは購入をいいます。

セキュリティテクノロジー強化プログラム（STEP）とは、データセキュリティを改善するテクノロジーの配備を加盟店が奨励される、アメリカン・エキスプレスのプログラムのことです。STEP に適格となるためには、加盟店で年次 STEP 認証の提出に先立つ 12 か月間にデータ事故が発生しておらず、すべての取引の 75%以上をポイントツーポイント暗号化または、EMV チップ対応機器を使用した対面取引によって行っていなければなりません。

チップとは、カードに内蔵された集積化マイクロチップをいい、カード会員およびカード番号情報を含みます。

チップカードとは、チップが内蔵されたカードをいい、カード会員の認証のためのPIN及び（または）チップ内のカード番号情報が要求される場合があります（「ICカード」、「スマートカード」、「EMVカード」、「ICC」、「集積回路カード」ということもあります）。

チップ対応機器とは、有効で最新のEMVCo (www.emvco.com)の許可/認定を取得し、AEIPSに準拠したチップカード取引の処理が可能なPOS機器をいいます。

調査報告書とは、年次のオンサイトセキュリティ評価またはSAQに基づくAOC、四半期毎のネットワークスキャン、あるいは年次のセキュリティテクノロジー強化プログラム証明に関するAOSCおよび所見のエグゼクティブサマリーをいいます。

通知日とは、発行者がデータ事故の最終通知を実施アメリカン・エキスプレスから提供された日のことです。通知日は、アメリカン・エキスプレスが最終フォレンジックレポートまたは内部解析を受け取った後、アメリカン・エキスプレスの独自の裁量に基づき決定されるものとします。

データ事故とは、アメリカン・エキスプレス暗号化キーの不正使用または不正使用の疑いに関する事故、あるいは、以下のアメリカン・エキスプレス・カード口座番号のいずれかのことです。

- 貴店または貴店の委託先の設備、システム、および/またはネットワーク（あるいはそのコンポーネント）で保存・処理・伝送された暗号化キー、カード会員データ、あるいは機密認証データ（あるいはそれぞれの組み合わせ）や、許可されていないアクセスまたは使用；
- 契約で認められている以外の目的で、上述の暗号化キー、カード会員データ、または機密認証データ（あるいはそれぞれの組み合わせ）の使用；および/または
- メディア、資料、記録、または暗号化キー、カード会員データ、あるいは機密認証データ（あるいはそれぞれの組み合わせ）などを含む情報の紛失、盗難、横領が疑われるまたは確認された場合。

データ事故イベントウィンドウとは、不正使用の発生日が判明している場合はその日から、不正使用の実際の発生日が不明の場合は通知日の365日前から始まる期間のことです。データ事故イベントウィンドウは、通知日の30日後に終了します。

取消とは、カードで行われた購入または支払について、請求を解消し、加盟店がカード会員に払戻す手続きのことをいいます。

取引とは、カードで行われた請求や取消をいいます。

認定審査機関または**QSA**とは、PCI SSCに認定された、PCI DSSの準拠を検証する機関をいいます。

認定スキャニングベンダまたは**ASV**とは、PCI SSCに認定された、インターネット環境の脆弱性スキャンを実行することでPCI DSSの要件への準拠を検証された機関をいいます。

認定済みポイントツーポイント暗号化（P2PE）ソリューションは、PCI SSCの認定済みソリューションのリストに含まれている、またはPCI SSC認定審査機関P2PE企業によって認定されています。

フォレンジック事故最終レポートテンプレート，とは、PCI Security Standards Council から入手できるテンプレートです。これは以下のURLからダウンロード可能です。

フランチャイザーとは、事業者の商標の下で商品および/またはサービスを提供するため、またはその商標を使用して業務を行うため、個人または組織（**フランチャイズ加盟店**）にライセンスを付与し、その業務の運用に際してフランチャイズ加盟店にサポートを提供し、またはフランチャイズ加盟店の運営方法に影響を及ぼし、フランチャイズ加盟店による手数料の支払いを求める事業者をいいます。

フランチャイズ加盟店とは、独立して所有および運営される第三者（フランチャイジー、ライセンシー、チャプターを含む）です。フランチャイザーによってフランチャイズの運営についてライセンスを付与されている関連会社、あるいはフランチャイザーの商標を使った対外的なアイデンティフィケーションを一貫して目立つ形で使用すること、あるいはフランチャイザーのグループ企業のメンバーであることを公にして運営することについてフランチャイザーと書面の契約を交わしている関連会社はこれに該当しません。

プロセッサとは、アメリカン・エキスプレスネットワークへの承認や決済処理を容易にする加盟店のサービスプロバイダーをいいます。

ペイメントアプリケーションの意味は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の最新版用語集に掲載されています。これは次のURLで閲覧できます。
https://www.pcisecuritystandards.org/

ポイントツーポイント暗号化（P2PE） とは、加盟店でのカード取扱い時点から復号化される安全なポイントまで、カード番号を暗号によって保護するソリューションをいいます。

リスク緩和テクノロジー - アメリカン・エキスプレスによって決定される、アメリカン・エキスプレス・カード保有者のデータおよび機密認証データのセキュリティを向上させるテクノロジーソリューション。リスク緩和テクノロジーとして適格となるためには、その設計および使用目的にしたがって、当該テクノロジーを有効に活用していることを実証する必要があります。例として、EMV、ポイントツーポイント暗号化、トークン化が挙げられます。

レベル1 の加盟店 - アメリカン・エキスプレスのカードの年間取引高が250万件以上、またはその他アメリカン・エキスプレスがレベル1と見なす加盟店。

レベル1 のサービスプロバイダー - アメリカン・エキスプレスのカードの年間取引高が250万件以上、またはその他当社がレベル1とみなすサービスプロバイダー。

レベル2 の加盟店 - アメリカン・エキスプレスのカードの年間取引高が5万件以上250万件未満の加盟店。

レベル2 のサービスプロバイダー - アメリカン・エキスプレスのカードの年間取引高が250万件未満、または当社がレベル1でないとみなすサービスプロバイダー。

レベル 3 の加盟店 - アメリカン・エキスプレスのカードの年間取引高が 1 万件以上 5 万件未満の加盟店

レベル 4 の加盟店 - アメリカン・エキスプレスのカードの年間取引高が 1 万件未満の加盟店

漏洩したカード番号とは、データ事故に関連するアメリカン・エキスプレスのカード番号をいいます。