AMERICAN EXPRESS

# データセキュリティ運営方針 (DSOP)

## 変更バー

重要な更新は変更の概要一覧に掲示され、DSOP の中でも変更バー。変更バーは左マージンにある縦線で、修正、追加、削除された文言があることを示しています。DSOP の中のすべての変更は、ここに示す変更バーで表示します。

## 変更の概要一覧

重要な更新は以下の表に示されており、*DSOP* の中でも変更バーにより表示されています。

| 項／節 | 変更の要旨 |
|---|---|
| 今回のリリースに変更点はありません。 | |

# データ事故が起きた場合に何をするか。

加盟店の事業でデータ事故が判明した場合、以下のステップを取ってください。

### ステップ 1:

データ事故を発見してから 72 時間以内に加盟店データ事故初期通知書に記入し EIRP@aexp.com に電子メールで送信します。

### ステップ 2:

徹底的な調査を行います。これにはペイメントカード業界（PCI）フォレンジック調査機関を雇うことを求められる場合があります。

### ステップ 3:

漏洩したすべてのアメリカン・エキスプレス ® カード番号を当社に提出します。

### ステップ 4:

データ事故に起因するすべての問題の解決に向けて当社と取り組みます。

データ事故の管理義務の詳細については 3 項「データ事故の管理義務」をご覧ください。

*さらに確認したいことがありますか。*

米国 : (888) 732-3750（通話料無料）

国際通話 : +1 (602) 537-3021

EIRP@aexp.com

**アメリカン・エキスプレスは、消費者保護の先駆者として、カード会員データ及び機密認証データが安全に保たれるよう保護することに長期にわたり取り組んでいます。**

漏洩したデータは消費者、加盟店、サービスプロバイダー及びカード発行者にネガティブな影響を及ぼします。たった一度の事故でも企業の評判に深刻な被害をもたらし、効果的な業務遂行能力を損なう可能性があります。セキュリティ運営方針の導入によりこの脅威に対処することは顧客の信頼を改善し、収益力を増強し、企業の評判を高めます。

アメリカン・エキスプレスは加盟店及びサービスプロバイダが（総称して貴店という）当社の関心事を共有していることを信頼しており、貴店の責任の一部として、**貴店**がアメリカン・エキスプレス ® カードを取り扱い（加盟店の場合）または処理する（サービスプロバイダの場合）ための**契約**（それぞれの各契約）にあるデータセキュリティ規定及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ことを求めます。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（またはその組み合わせ）を保管、処理または伝送する貴店のすべての機器、システム及びネットワーク（及びその部品）に適用されます。

*ここで使用されているものの定義されていない用語（英文では大文字で表記されている）は、本方針の末尾にある用語集で説明されている意味です。*

## 1 項　対象分析プログラム（TAP）

カード会員データの漏洩はカード会員データ環境（CDE）のデータセキュリティギャップにより発生することがあります。

カード会員データの漏洩の例には、以下を含みますが、これらに限定されません。

- **共通購買時点（CPP）**：アメリカン・エキスプレスカード会員は、自分のカードアカウントで不正な取引が行われたことを報告し、貴店の指定店舗での購入に起因するものであると特定及び判断されました。
- **カードデータ検出**：貴店の指定店舗での取引に関連付けられたアメリカン・エキスプレスカードまたはカード会員データがウェブ上で見つかりました。
- **マルウェアの疑い**：アメリカン・エキスプレスは、貴店の使用しているソフトウェアが悪意のあるコードに感染しているか、悪意のあるコードに対して脆弱であると疑っています。

TAP はカード会員データの漏洩の可能性を特定するために設計されています。

アメリカン・エキスプレスからカード会員データの漏洩の可能性について通知を受けた場合、貴店は下記の要件を遵守しなければならず、加盟店関係者にもそれを行わせなければなりません。

- 貴店は CDE のデータセキュリティギャップを迅速に確認し、何か気づいた点があれば改善しなければなりません。
  - 外部委託している場合は、第三者ベンダに CDE の徹底的な調査を行わせなければなりません。
- アメリカン・エキスプレスからの通知に応じて、レビュー、評価、または改善作業後に実行または計画された処置の概要を提供しなければなりません。
- 貴店は、5 項「システムの重要な定期検証」に従って、更新された PCI DSS 調査報告書を提供する必要があります。
- 該当する場合、貴店または加盟店関係者が以下に該当する場合、貴店は、貴店の CDE を調査するために認定 PCI フォレンジック調査機関（PFI）を関与させなければなりません。
  - カード会員データの漏洩をアメリカン・エキスプレスが決定する合理的な期間内に解決できない場合、または
  - データ事故が起きたことを確認し、3 項「データ事故の管理義務」に定められている要件を遵守する場合。

表 A-1: TAP 非遵守費用

| 説明 | レベル 1 の加盟店またはレベル 1 のサービスプロバイダー | レベル 2 の加盟店またはレベル 2 のサービスプロバイダー | レベル 3 またはレベル 4 の加盟店 |
|---|---|---|---|
| TAP 義務が最初の期限までに果たされない場合、非遵守費用が課せられる場合があります。 | $25,000 米ドル | $5,000 米ドル | $1,000 米ドル |
| TAP 義務が 2 回目の期限までに果たされない場合、非遵守費用が課せられる場合があります。 | $35,000 米ドル | $10,000 米ドル | $2,500 米ドル |
| TAP 義務が 3 回目の期限までに果たされない場合、非遵守費用が課せられる場合があります。<br>**注：***義務を果たすか TAP が解決されるまで非遵守費用が継続的に課せられ続けることがあります。* | $45,000 米ドル | $15,000 米ドル | $5,000 米ドル |

加盟店の TAP についての義務が果たされない場合、アメリカン・エキスプレスは非遵守費用を累積して課し、支払いを保留し、または契約を解除する権利を有します。

## 2 項　暗号化キー、カード会員データ及び機密認証データの保護基準

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：

- カード会員データを、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。
- カード会員データまたは機密認証データの処理、保存または送信に適用される現行の PCI DSS 及び他の PCI SSC 要件に、適用されるバージョンの要件が施行される有効日までに適合する。
- 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アメリカン・エキスプレスの請求記録及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、（5 項に他の規定がある場合を除いて、5 項「システムの重要な定期検証」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、アメリカン・エキスプレスに財務上及びその他の義務を負うものとします。

## 3 項　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 72 時間以内にアメリカン・エキスプレスに通知するものとします。

アメリカン・エキスプレスに通知するには、+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*）に連絡するか、または EIRP@aexp.com に電子メールを送信することができます。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名しなければなりません。それに加え、

- 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 件以上のカード番号が関与するデータ事故の場合、データ事故の発覚から 5 日以内に、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集のまま、アメリカン・エキスプレスに提出しなければなりません。
- すべての漏洩したカード番号を速やかにアメリカン・エキスプレスに提出しなければなりません。アメリカン・エキスプレスは、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。

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。当該レポートは、フォレンジックレビュー、準拠状況報告書、及びデータ事故に関するその他の関連する情報を含んでいなければならず、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) 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（以下に記載）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、非準拠が改善されたことを示す認定審査機関（QSA）による検証を提供するものとします。

本 3 項「データ事故の管理義務」の前項までの規定に関わらず、以下が適用します。

- 異なる 10,000 件未満のカード番号が関与するデータ事故の場合、アメリカン・エキスプレスは、その独自の裁量により、PFI がデータ事故の調査を実施するよう貴店に求めることができます。その調査は 3 項「データ事故の管理義務」に規定された要件に適合しなければならず、アメリカン・エキスプレスに求められた期間内に完了しなければなりません。
- アメリカン・エキスプレスは、いかなるデータ事故についても、その独自の裁量により、別途 PFI が調査を実施するようにすることができ、調査の費用を貴店に請求することができます。

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することに同意します。これには、データの事故の影響を受けたカード会員への連絡についてアメリカン・エキスプレスと協議すること、及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、すべての関連情報をアメリカン・エキスプレスに提供すること（及び提供に必要な放棄の取得）が含まれます。

契約の秘密保持の条項にも関わらず、アメリカン・エキスプレスは、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、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、及び一般に開示する権利を保持します。

## 4 項　データ事故の損害賠償義務

データ事故に関する契約に基づき、貴店のアメリカン・エキスプレスへの損害賠償の義務は、アメリカン・エキスプレスのその他の権利及び救済手段を放棄することなく、本 4 項「データ事故の損害賠償義務」に基づき決定されるものとします。損害賠償義務（ある場合）に加え、貴店は、以下の本 4 項「データ事故の損害賠償義務」に示されているデータ事故非遵守費用を支払わなければならない場合があります。

データ事故について、

- 以下のいずれかを含む 10,000 件以上のアメリカン・エキスプレスカード番号、
  - 機密認証データ、または
  - 使用期限

  に関連する場合、貴店は各口座番号につき $5 米ドルの割合でアメリカン・エキスプレスに賠償しなければなりません。

ただし、アメリカン・エキスプレスは、以下の該当するデータ事故については貴店に賠償を求めることはありません。

- 10,000 件未満のアメリカン・エキスプレスカード番号、または
- 以下に該当する場合、10,000 件以上のアメリカン・エキスプレスカード番号。
  - 貴店が、3 項「データ事故の管理義務」に基づきデータ事故をアメリカン・エキスプレスに通知した場合、
  - データ事故が発生した時点でPCI DSSを遵守していた場合（PFIのデータ事故調査により決定される）、及び
  - データ事故は貴店、もしくは貴店関係者の不法行為に起因しない場合。

4 項「データ事故の損害賠償義務」の前項までの規定に関わらず、アメリカン・エキスプレスカード番号の件数に関わりなく、いかなるデータ事故についても、貴店が 3 項「データ事故の管理義務」に規定された義務を遵守しなかった場合には、アメリカン・エキスプレスに、各データ事故につき $100,000 米ドルを超えない（アメリカン・

エキスプレスが、その独自の裁量により定めた）データ事故非遵守費用を支払わなければなりません。誤解を避けるために記すと、1 つのデータ事故について課されるデータ事故非遵守費用は $100,000 米ドルを超えることはありません。

アメリカン・エキスプレスは、通知日に先立つ 12 カ月以内になされた以前のデータ事故の損害賠償請求に関与していたアメリカン・エキスプレスカード番号をその計算から除外します。本方法に基づくアメリカン・エキスプレスのすべての算出額は最終的なものとします。

アメリカン・エキスプレスは、本契約に基づき、データ事故の賠償義務について全額貴店に請求するか、アメリカン・エキスプレスの貴店に対する支払いからその額を控除する（または貴店の銀行口座から適宜引き落とす）ことができます。

貴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。

その独自の裁量により、アメリカン・エキスプレスは、以下の基準を満たすデータ事故についてのみ加盟店の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。
- 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。
- 貴店が難読化されていない機密認証データまたはカード会員データを保存していないこと（及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。

### 表 A-2: TAP 賠償義務の減免に要求される基準

| 賠償義務の減免 | 要求される基準 |
|---|---|
| 標準減免：<br>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：<br>75% から 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及び、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の使用にあたり適格となるためには、その設計及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。

表 A-3: 賠償義務の拡張減免

| 例 | リスク緩和テクノロジーの使用 | 対象 | 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<br>店舗の 0% で他の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<br>店舗の 77% で他の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<br>店舗の 100% で他の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<br>店舗の 90% で他の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] アカウント番号 1 件当たり $5 米ドルの、10,000 件のアメリカン・エキスプレス・カード番号が関わるデータ事故では（10,000 x $5 = $50,000 米ドル）、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 $50,000 米ドルから $25,000 米ドルに減額される場合があります。

5 項

## システムの重要な定期検証

貴店は、PCI DSS に基づき、以下に説明するアクションにより、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、貴店または貴店のフランチャイズ店の設備、システム、及び／またはネットワーク（及びそのコンポーネント）の状態を年次及び 90 日毎に検証するものとします。

検証を完了するための 4 つのアクションは以下のとおりです。

アクション 1：本方針に基づきアメリカン・エキスプレスの PCI コンプライアンスプログラム（「プログラム」）に参加する。

アクション 2：貴店の加盟店レベルと検証要件について理解する。

アクション 3：アメリカン・エキスプレスに送付すべき調査報告書を完成させる。

アクション 4：指定の期間内に調査報告書を当社に提出する。

### アクション 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、及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、本方針に基づきプログラムに参加する必要があります。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 及びレベル 4 の加盟店に、本方針に基づき、プログラムに参加するよう指名する場合があります。

プログラムに参加することが求められているすべての加盟店及びサービスプロバイダーは、定められた期限までに、アメリカン・エキスプレスにより選ばれたプログラム管理者が提供するポータルから登録しなければなりません。

- 加盟店はポータルの使用に関連する合理的な利用条件をすべて承諾しなければなりません。
- 加盟店はポータル内で最低一つのデータセキュリティの窓口を割り当て、その正確な情報を提供しなければなりません。必要なデータ要素には以下が含まれます。
  - フルネーム
  - 電子メールアドレス
  - 電話番号
  - 郵送先住所
- 加盟店は情報に変更が生じた場合、ポータル内でデータセキュリティの窓口の更新されたまたは新規の連絡先情報を提供しなければなりません。
- 加盟店はポータルの指定されたドメインからサービスに関する通信が可能となるようシステムが最新のものであるようにしなければなりません。

加盟店が最新のデータセキュリティ窓口情報を提供しないことまたは電子メールの通信を利用可能にしないことは当社が料金を徴収する権利に影響を与えないものとします。

## アクション 2：貴店の加盟店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 つの加盟店レベルの加盟店と 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指定店舗により提出された取引件数です。*
- サービスプロバイダーの場合、これは、サービスを提供する先のサービスプロバイダー及び事業体サービスプロバイダーが提出する取引件数の合計です。

購入者支払い (BIP) 取引は、加盟店のレベル及び検証要件を特定するためのアメリカン・エキスプレスのカードの取引件数には含まれません。貴店は、加盟店及びサービスプロバイダーの以下の表に指定された加盟店レベルの 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指定店舗からの取引件数が含まれます。フランチャイズ加盟店に、特定のポイント・オブ・セール（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。

### 加盟店調査報告書要件

加盟店（サービスプロバイダーを除く）は、4 つの加盟店レベルの分類があります。以下のリストから加盟店のレベルを特定し、表 A-4: 加盟店調査報告書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 と見なす加盟店。
- **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。

表 A-4: 加盟店調査報告書

| 加盟店レベル／アメリカン・エキスプレスの年間取引件数 | コンプライアンスレポート準拠証明書（ROC AOC） | 問診準拠証明書（SAQ AOC）及び四半期外部ネットワーク脆弱性スキャン（スキャン） | 有資格加盟店の STEP 証明 |
|---|---|---|---|
| レベル 1/<br>250 万件以上 | 必須 | 該当なし | オプション（アメリカン・エキスプレスの承認が必要）（ROC に代わる） |
| レベル 2/<br>5 万件以上 250 万件未満 | オプション | SAQ AOC 必須（ROC AOC 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 及びネットワークスキャン、または ROC に代わる） |
| レベル 3/<br>1 万件以上 5 万件未満 | オプション | SAQ AOC 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 及びネットワークスキャン、または ROC に代わる） |
| レベル 4/<br>1 万件以下 | オプション | SAQ AOC 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 及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 及びレベル 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。

アメリカン・エキスプレスは、PCI 調査報告書の完全性、正確性、妥当性を検証する権利を留保します。アメリカン・エキスプレスはこの目的の裏付けとして評価のために追加の裏付けの書類を求める場合があります。加えて、アメリカン・エキスプレスは加盟店に対して、PCI Security Standards Council によって認定された QSA または PFI を関与させるよう求める権利を有します。

## 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は、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% が以下の高度セキュリティオプションの組み合わせを使用している場合のみです。

- **EMV、EMV コンタクトレスまたはデジタルウォレット** – 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。( 米国の加盟店は非接触型を含めなければなりません )
- **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。
- **トークン化** – 導入されているトークン化ソリューションは以下を満たしていなければなりません。
  - EMVCo 仕様を満たしていること。
  - PCI に準拠した第三者のサービスプロバイダーにより保護、処理、保存、送信、そして全体を管理されていること。
  - トークンは、マスキングされていない主要口座番号（PAN）を加盟店に明らかにすることがないようにリバース・エンジニアリングがかけられないものであること。

STEP の資格を有する加盟店については PCI 調査報告の要件が緩和されています。詳しくは下記のアクション 3：「アメリカン・エキスプレスに送付すべき調査報告書を完成させる」に説明されています。

### 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つのレベル分類があります。以下のリストからサービスプロバイダーレベルを特定し、表 A-5: サービスプロバイダー文書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 STEP の対象ではありません。

#### 表 A-5: サービスプロバイダー文書

| レベル | 調査報告書 | 必須性 |
|---|---|---|
| 1 | 年次コンプライアンスレポート準拠証明書（ROC AOC） | 必須 |
| 2 | 年次 SAQ D（サービスプロバイダー）及び四半期ネットワークスキャンまたは望ましい場合、年次コンプライアンスレポート準拠証明書（ROC AOC） | 必須 |

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

## アクション３：アメリカン・エキスプレスに送付すべき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。

貴店は該当する評価タイプに応じた準拠証明書（AOC）を提供しなければなりません。AOC は貴店の準拠状況についての宣誓であるため、貴店の組織内の適切なレベルの幹部により署名され日付が付されているものでなければなりません。

AOC に加えて、アメリカン・エキスプレスは全体の評価の写しを、また裁量により、PCI DSS 要件の遵守を証明する追加の裏付けの書類の提供を求める場合があります。この調査報告者は貴店の費用において作成するものとします。

**コンプライアンスレポート準拠証明書（ROC AOC）-（年次要件）** – コンプライアンスレポート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、または伝送される加盟店のすべての設備、システム、及びネットワーク（及びそのコンポーネント）の詳細なオンサイト監査の結果を示す文書です。二つのバージョンがあります。一つは加盟店用でもう一つはサービスプロバイダー用です。コンプライアンスレポートは、

- 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なければなりません。

AOC は QSA または内部セキュリティ評価者（ISA）及び貴店の組織内の権限のあるレベルの幹部により署名され日付が付され少なくとも１年に１回はアメリカン・エキスプレスに提供されなければなりません。

**自己問診準拠証明書（SAQ AOC）-（年次要件）** – 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、及びネットワーク（及びそのコンポーネント）を自己検証できるようにします。SAQ には複数のバージョンがあります。貴店はカード保有者データ環境に基づいて１つ以上を選択します。

SAQ は質問に対し正確かつ完全に答えることができる社内の資格のある従業員が作成するか、サポートのために QSA を関与させることができます。AOC は貴店の組織内の権限のあるレベルの幹部により署名され日付が付され、少なくとも１年に１回はアメリカン・エキスプレスに提供されなければなりません。

**認定スキャンニングベンダ外部ネットワーク脆弱性スキャンサマリー（ASV スキャン）-（90 日要件）**– 外部脆弱性スキャンは貴店のカード保有者データ環境のインターネット接続コンポーネント（例、ウェブサイト、アプリケーション、ウェブサーバー、メールサーバー、公開ドメインまたはホスト）の潜在的な弱点、脆弱性及び不適当な設定を特定する遠隔テストです。

ASV スキャンは、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。

SAQ で求められた場合、スキャン対象の数、結果が PCI DSS スキャニング手順を満たすことの証明及び ASV により作成された準拠状況を含むスキャン準拠証明書の ASV スキャンレポート(AOSC)またはエグゼクティブサマリーを少なくとも 90 日に 1 回アメリカン・エキスプレスに提出しなければなりません。

ROC AOC または STEP では特に求められていない限り AOSC または ASV スキャンのエグゼクティブサマリーを提供する必要はありません。疑義を避けるために付言すると、該当する SAQ で求められる場合、スキャンは必須です。

疑義を避けるために付言すると、該当する SAQ で求められる場合、ASV は必須です。

**STEP 認証調査報告（STEP）-（年次要件）**– STEP は上記アクション 2：「貴店の加盟店レベルと検証要件について理解する」「加盟店レベルと検証要件について理解する」の基準を満たす加盟店だけが利用することができます。会社に資格がある場合、貴店は STEP 認証書を作成し、毎年アメリカン・エキスプレスに提出しなければなりません。年次 STEP 認証フォームは、ポータルからダウンロードできます。

**PCI DSS 非準拠 -（年次、90 日またはアドホック要件）**– 貴店が 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」（PCI Security Standards Council のウェブサイトからダウンロード可能）
- PCI 優先アプローチツールのサマリー（PCI Security Standards Council のウェブサイトからダウンロード可能）
- プロジェクトプランテンプレート（ポータルからダウンロード可能）年次証明（SAQ/ROC）の代わりに、あるいはスキャン要件の代わりにプロジェクトプランを提出することができます。

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、非準拠状態に対する改善（レベル 1、レベル 2、レベル 3、及びレベル 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。PCI DSS の準拠のために必要な改善措置は貴店の費用においてなされるものとします。

PCI DSS の準拠のために必要な改善措置は貴店の費用においてなされるものとします。

当社は、改善日以前の非準拠に対して、貴店に後述する未検査費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。

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。

## アクション 4：調査報告書を当社に提出する

プログラムに参加することが求められているすべての加盟店及びサービスプロバイダーはアクション 2：「貴店の加盟店レベルと検証要件について理解する」で「必須」と記されている調査報告書を該当する期限までにアメリカン・エキスプレスに提出しなければなりません。

貴店は、アメリカン・エキスプレスが選んだプログラム管理者が提供するポータルを使用して調査報告書をアメリカン・エキスプレスに提出しなければなりません。調査報告書を提出することにより、貴店はアメリカン・エキスプレスに対し、以下の事項を表明し、可能な限り最善の範囲で保証するものとします

- 貴店の評価が完全で網羅的であること。
- 完了時の PCI DSS の状況が、準拠であれ非準拠であれ、正確に反映されていること。
- 貴店はそこに含まれている情報を公開する権限があり、他の第三者の権利を侵害することなくアメリカン・エキスプレスに調査報告書を提出していること。

### 未検査費及び契約の終了

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、未検査費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。

**表 A-6: 未検査費**

| 説明 * | レベル 1 の加盟店またはレベル 1 のサービスプロバイダー | レベル 2 の加盟店またはレベル 2 のサービスプロバイダー | 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、未検査費が課せられます。 | $25,000 米ドル | $5,000 米ドル | $50 米ドル |
| 調査報告書が 2 回目の期限までに未受領の場合、追加の未検査費が課せられます。 | $35,000 米ドル | $10,000 米ドル | $100 米ドル |
| 調査報告書が 3 回目の期限までに未受領の場合、追加の未検査費が課せられます。<br>**注**：調査報告書が提出されるまで未検査費が継続的に課せられます。 | $45,000 米ドル | $15,000 米ドル | $250 米ドル |

* 未検査費は現地通貨相当額で課せられます。

* アルゼンチンには適用されません。

貴店の PCI DSS 調査報告書についての義務が果たされない場合、アメリカン・エキスプレスは未検査費を累積して課し、支払いを保留し、または契約を解除する権利を有します。

## 6 項　秘密保持

アメリカン・エキスプレスは、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（ポータルのプロバイダーを含む代理店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店、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。

a. 開示する以前にアメリカン・エキスプレスに既知のもの
b. アメリカン・エキスプレス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
c. 秘密保持義務なしに合法的に第三者からアメリカン・エキスプレスが入手したもの
d. アメリカン・エキスプレスが個別に作成したもの
e. 裁判所、行政機関または政府当局の命令、法律、法規または規則、召喚、開示要求、喚問、他の行政手続または訴訟手続、政府機関または当局（取締官、検査官、審査官、司法当局など）の公式または非公式の調査または捜査により開示を要求されたもの

## 7 項　免責事項

アメリカン・エキスプレスは、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 の仕様及び設定、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：www.americanexpress.com/datasecurity

PCI Security Standards Council, LLC: www.pcisecuritystandards.org

## 用語集

本データセキュリティ運営方針（DSOP）に限って、以下の定義を適用し、*加盟店規程*の用語と矛盾する場合に優先されます。

**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関連会社の名前、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、カード発行者により発行されたカード、アカウントアクセス機器、支払機器またはサービス、あるいはカード番号のことです。

**準拠証明書 (AOC)** とは、Payment Card Industry Security Standards Council（有限責任会社）により提供されたフォームで、貴店の PCI DSS への準拠状況の申告書をいいます。

**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。

**認定スキャニングベンダ (ASV)** とは、Payment Card Industry Security Standards Council, LLC 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事業体をいいます。

**スキャン準拠証明書 (AOSC)** とは、Payment Card Industry Security Standards Council, LLC 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。

**購入者支払い（BIP）**取引とは BIP を通して処理された支払い指示ファイルを介して利用できる支払い取引をいいます。

**カード会員データ** は、PCI DSS の当時の最新版用語集に掲載されている意味です。

**カード会員データ環境（CDE）**は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、プロセス及び技術を意味します。

**カード会員**とは、以下の個人または事業体をいいます。(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及びカード取引に関する情報をいい、氏名、住所、カード番号、及びカード識別番号（CID）を含みます。

**カード番号**とは、カードを発行するときに発行者が割り当てる固有の識別番号です。

**立替払金**とは、カードでなされる支払いまたは購入をいいます。

**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、カード会員及び口座情報を含みます。

**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（当社の資料の中で「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 POS 機器をいいます。

**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。

**貴店関係者**とは、貴店の従業員、代理店、代表者、下請契約者、プロセッサー、サービスプロバイダー、ポイントオブセールス設備（POS）またはシステムの業者、決済処理ソリューション事業者、貴店のアメリカン・エキスプレス加盟店アカウントの関連事業体、及び契約に基づいて貴店がカード会員データ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。

**取消**とは、カードで行われた購入または支払について、貴店がカード会員に払い戻す立替払金の金額のことをいいます。

**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・カード番号のいずれかのことです。

- 貴店の設備、システム、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）または貴店の委託先にその使用を義務付け、もしくは提供もしくは利用可能にしているものについての許可されていないアクセスまたは使用。
- 本契約で認められている以外の目的での、当該暗号化キー、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。
- 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、最終フォレンジックレポート（PFI レポートなど）に記載されている侵入のウィンドウ（または同様に決定された期間）、または不明の場合は、当社に報告されたデータ漏洩に関与する漏洩した可能性のあるカード番号の最終通知日の 365 日前から始まる期間を意味します。

**EMV 仕様**とは、EMVCo, LLC 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。www.emvco.com

**EMV 取引**とは、有効で最新の EMV 型式認定を取得した IC カードの処理が可能な POS 端末で行った、集積回路カード（「IC カード」、「チップカード」、「スマートカード」、「EMV カード」、「ICC」ということもあります）による取引をいいます。EMV 型式認可は次の URL で閲覧できます。www.emvco.com

**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）及びゾーンピンキー（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）、及び ZPK

**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をいいます。これは次の URL で閲覧できます。www.pcisecuritystandards.org

**フランチャイズ加盟店**とは、独立して所有及び運営される第三者（フランチャイズ加盟店、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。

**フランチャイザー**とは、事業者の商標の下で物品及び / 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、個人または事業体（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。

**発行者**とは、アメリカン・エキスプレスまたはアメリカン・エキスプレス関連会社によりカードの発行及びカード発行事業を行うことのライセンスを受けた事業体（アメリカン・エキスプレスとその関連会社を含む）をいいます。

**レベル 1 の加盟店**とは、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 と見なす加盟店のことです。

**レベル 2 の加盟店**とは、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 万件未満の加盟店のことです。

**レベル 3 の加盟店**とは、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 万件未満の加盟店のことです。

**レベル 4 の加盟店**とは、アメリカン・エキスプレスのカードの年間取引高が 1 万件未満の加盟店のことです。

**レベル 1 のサービスプロバイダー**とは、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のことです。

**レベル 2 のサービスプロバイダー**とは、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のことです。

**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及びそのすべての関連会社のことです。

**加盟店レベル**と 5 項「システムの重要な定期検証」で述べられているとおり、加盟店の PCI DSS 準拠の検証に関する義務について当社が加盟店に割り当てる指定番号です。

**通知日**とは、カード発行者がデータ事故の最終通知をアメリカン・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。

**ペイメントアプリケーションの意味**は、安全ソフトウェア規準及び安全ソフトウェアライフサイクル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。www.pcisecuritystandards.org

**Payment Card Industry Data Security Standard（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、www.pcisecuritystandards.org で確認することができます。

**Payment Card Industry Security Standards Council（PCI SSC）要件**とは、PCI DSS 及び PA DSS を含む支払いカードデータの確保及び保護に関連した基準及び要件をいい、www.pcisecuritystandards.org で確認することができます。

**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及びプロバイダのリスト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。www.pcisecuritystandards.org

**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。www.pcisecuritystandards.org

**PCI フォレンジック調査機関 (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。

**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。www.pcisecuritystandards.org

**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。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。

**認定済みポイントツーポイント暗号化 (P2PE)** とは、加盟店がペイメントカードを受け付ける場所から、暗号解読のセキュアな場所までカードデータを暗号により保護するソリューションをいいます。

**ポータル**とは、アメリカン・エキスプレスに選ばれたアメリカン・エキスプレス PCI プログラム管理者により提供される報告システムです。加盟店とサービスプロバイダーはアメリカン・エキスプレスに PCI 検証文書を提出するときポータルを使用する必要があります。

**主要口座番号（PAN）**は、PCI DSS の当時の最新版用語集に掲載されている意味です。

**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。

**プログラム**とは、アメリカン・エキスプレス PCI コンプライアンスプログラムです。

**認定審査機関 (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。

**リスク緩和テクノロジー**とは、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・カード会員データ及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をいいます。リスク緩和テクノロジーとして適格となるためには、その設計及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が、これに限定されません。

**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。

**自己問診 (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。

**機密認証データ は**、PCI DSS の当時の最新版用語集に掲載されている意味です。

**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、及び加盟店に対して 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。

**対象分析プログラム**はカード会員データ環境（CDE）でカード会員データの漏洩の可能性を早期に特定するプログラムです。1 項「対象分析プログラム（TAP）」を参照してください。

**トークン**とは、指定されたインデックスに基づいて、PAN を予測不可能な値に置き換える暗号トークンです。

**取引**とは、カードで行われた立替払金や取消をいいます。

**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 及び所見のエグゼクティブサマリーをいいます。