American Express SafeKey®に関するよくある質問（FAQ）

セクション1: 一般的なFAQ

Q1.1 AMERICAN EXPRESS SAFEKEY®とは?

American Express SafeKeyは、グローバルな業界標準を活用し、カード会員がオンラインあるいはモバイルデバイスでショッピングをする際のセキュリティを強化することで、オンライン上の不正を検知して、発生件数を抑えます。SafeKey 2.0はEMV® 3-D Secureプロトコルをベースにしています。

購入時に提供される氏名やEメールアドレス、電話番号や送付先住所といったカード会員のデータを利用して、正当な取引や不正な取引をより正確に判断できます。

SafeKeyでは、リスクに基づく認証方法をイシュアが使用することにより、煩雑さを軽減し、チェックアウト時の操作をより簡素化することができます。またカード会員はSafeKeyを利用し、スマート デバイスによるアプリ内ショッピングなど、最も使いやすいデバイス上でショッピングを楽しめます。

Q1.2 SAFEKEYの主なメリットは?

SafeKeyにより、eコマースの取引における不正を抑制することができます。これにより、カード会員のカードが許可なく使用されることを防ぎ、認証評価にイシュアを関与させ、Fraud Liability Shiftを加盟店に移行することができます（詳細はFLSセクションを参照してください）。

Q1.3 SAFEKEYの仕組みは?

SafeKeyでは、取引が承認される前にカード会員の本人認証をイシュアに依頼することで、オンライン上の不正使用を抑制できます。

1. 認証フローは、カード会員によるオンライン上の加盟店での商品購入時から始まります。
2. 加盟店は、SafeKeyを介した取引を3DSサーバー（加盟店向けプラグイン）プロバイダー経由でアメリカン・エキスプレスのディレクトリ サーバー（DS）へ送信します。
3. 次に、DSはこのリクエストを関連するイシュアのAccess Control Server（ACS）に転送します。
4. ACSは高度なリスク モデリング技術を適用してカード会員の本人認証を行います。
5. ある特定の状況では、カード会員がワンタイムパスワードをACSに送信するよう求められることがあります。

Q1.4 SAFEKEYはどこで入手できますか?

SafeKeyの導入を希望するアクワイアラとイシュアは、あらゆるマーケットでSafeKeyを入手できます。加盟店がこのサービスを利用するには、アクワイアラがSafeKeyの認定を取得する必要があります。

Q1.5 3-D SECURE（3DS）2.0とは? また業界で新しいバージョンが必要な理由とは?

当初、業界の3DS 1.0.2プロトコルをベースとするSafeKeyは、PCのブラウザーベースのeコマース取引におけるカード会員の認証をサポートするために開発されました。アメリカン・エキスプレスが所属するグローバルな 技術機関であるEMVCoは、その範囲を拡大し、3DS 2.0の仕様、および関連するテスト・承認プログラムの開発を促進し、ペイメント業界をリードしています。

3DS 2.0は、アプリ内、モバイルおよびデジタル ウォレットといった、ブラウザーを使用しない遠隔決済に対応しています。またこのアプローチにより、テクノロジー、セキュリティ、パフォーマンス、ユーザー エクスペリエンス、および長期利用を可能にする柔軟性の観点から、新しい機能を提供しています。

Q1.6 SAFEKEYは、EMV 3DS仕様の進化（V2.1.0、V2.2.0など）にどのように対応しますか?

SafeKey 2.0の機能は、EMV 3DSの最新バージョンを反映して更新されます。すべての機能を使用するためには、SafeKey参加事業者（3DS Server, ACS, 決済代行業者、加盟店）は最新バージョンの認証を再度受ける必要があります。

Q1.7 3DS 2.0にはどのような機能がありますか?

EMV 3DS 2.0は、遠隔決済環境の進化する要件を満たすことを目指しており、次のような機能が含まれています。

- ブラウザーおよびアプリ内のショッピング ニーズへの対応と直接的な統合
- 拡張データを使用したイシュアによるリスク評価の向上
- ワンタイム パスコード、生体認証、リスクベース認証（追加認証）機能など、さまざまな認証方式をサポート
- セキュリティを強化し、トークン利用の拡大に対応するため、トークンベースの取引をサポート
- デジタル ウォレットに対するカードのプロビジョニングなど、決済を伴わない本人認証に対応
- 加盟店が認証を起動する機能（継続課金、通信販売、電話注文など）
- カード会員の決済フローの改善と利用体験の向上
- PSD2(EUにおける改正決済サービス指令）に対応

注記: 各SafeKeyバージョンの詳細な機能比較については、付録を参照してください

Q1.8 SAFEKEY 2.0の仕様はどこで確認できますか?

SafeKey 2.0の仕様および導入ガイドは次の場所で入手できます。

- イシュア / アクワイアラ: https://network.americanexpress.com/globalnetwork/sign-in/
- ACS および 3DS サーバー（MPI） プロバイダー: https://network.americanexpress.com/globalnetwork/amex-enabled/

- 加盟店: http://www.americanexpress.com/merchantspecs
- EMVの基本仕様: www.emvco.com

Q1.9 SAFEKEY 1.0に対するアメリカン・エキスプレスの対応は?

アメリカン・エキスプレスは業界のSafeKey 1.0の利用状況をモニターしており、SafeKey 2.0の導入件数が増加している間は、引き続き1.0のサービスをサポートします。また、今後SafeKey 1.0のサービスがSafeKey 2.0に完全に引き継がれる時期を発表し、適切なリード タイムを設ける予定です。

Q1.10 SAFEKEY 1.0とSAFEKEY 2.0を共存させることはできますか?

SafeKey 1.0と2.0はそれぞれ独立して動作するため、共存させることが可能です。SafeKey 1.0は徐々に2.0に置き換わることが予想されますが、この移行期間中、加盟店には両方の製品をサポートする3DSサーバー（MPI）プロバイダーのサービスをご利用になることをお勧めします。加盟店が取引の認証を求めた場合に、適切なSafeKeyバーションを使用する責任は3DSサーバー（MPI）プロバイダーにあります。

Q1.11 使用するSAFEKEYのバーションを3DSサーバー（MPI）が知る方法とは?

SafeKeyサービスではカード記録（BIN）が管理されていますが、これはSafeKey 2.0でサポートされ、これらの詳細情報はすべての3DSサーバー（MPI）で使用できます。加盟店がカード会員の認証を求めた場合、3DSサーバー（MPI）はその特定のカードがSafeKey 2.0対応かどうかを確認します。もし対応していればSafeKey 2.0のサービスを、そうでない場合はSafeKey 1.0を使用します。

Q1.12 SAFEKEY 1.0がなくてもSAFEKEY 2.0を導入できますか?

はい。新規導入を検討中のお客様にとっては、SafeKey 2.0が徐々に標準の製品となっていくはずです。ただ、SafeKey 2.0が完全に標準となるまでには、一定期間要するということを理解しておく必要があります。

Q1.13 カード会員は、すでにSAFEKEY 1.0に登録済みであっても、SAFEKEY 2.0に登録しなければならないのでしょうか?

カード会員はSafeKey 2.0に登録する必要はありません。すべての対象カード会員について、EMVCo仕様の要件に従ってイシュアが事前登録を行います。

Q1.14 SAFEKEYはあらゆるカード商品のオンライン取引に使用できますか?

SafeKeyは取引を実行しようとしている人物がカード会員であることを認証するサービスを提供しているため、プリペイド カードなど、ユーザーの身元情報が登録されていない無記名の商品には使用できません。

セクション2: Fraud Liability Shift（FLS）に関するFAQ

Q2.1 SAFEKEY FRAUD LIABILITY SHIFT（FLS）とは?

正規の取引で不正使用が行われた場合、SafeKey FLSはその責任を加盟店からイシュアに移行します。

Q2.2 加盟店がFLSの適用を受けるにはどうすればよいでしょうか?

加盟店は、FLSポリシーの基準を満たしている場合、SafeKeyによって認証された取引についてFLSの適用を受けます。加盟店は低い不正発生率を維持し、またSafeKeyメッセージに正確なデータを提供するなど、SafeKey 仕様の要件を満たすことを求められます。FLSポリシーの詳細については、アクワイアラにお問い合わせください。

Q2.3 認証済みのSAFEKEY取引とは?

認証済みの取引とは、イシュアが、応答メッセージに含まれる認証値に基づいてカード会員の本人認証を行った取引を指します。詳しくは、SafeKeyの仕様を参照してください。

Q2.4 SAFEKEYの認証試行取引とは?

認証試行取引とは、加盟店がSafeKeyの認証を試みたものの、イシュアがSafeKeyに対応していないか、イシュアのACSを利用できない取引を指します。SafeKeyでは、応答メッセージに含まれる認証値に基づいて認証試行を許可する場合があります。詳しくは、SafeKeyの仕様を参照してください。

セクション3: 加盟店に関するFAQ

Q3.1 SAFEKEYの導入に必要な作業を見極める方法は?

SafeKeyの導入を希望する加盟店は、検討中の3DSサーバー（MPI）プロバイダーまたは決済代行業者にご相談ください。

Q3.2 加盟店としてSAFEKEYに登録する方法は?

3DSサーバー（MPI）プロバイダーまたは決済代行業者に連絡してSafeKeyへの登録を依頼します。

Q3.3 加盟店として使用するSAFEKEYのバージョンを知る方法は?

全SafeKeyバージョンに対応する3DSサーバー（MPI）プロバイダーを利用することをお勧めします。プロバイダーは、イシュアが対応するSafeKeyバージョンを把握しているため、適切なバージョンを選択し、適切な拡張機能を使用します。

Q3.4 加盟店として利用している3DSサーバー（MPI）プロバイダーがSAFEKEY 2.0に対応しているかどうかを知る方法は?

3DSサーバー（MPI）プロバイダーはSafeKey 2.0の認定を取得するために、EMVCoおよびアメリカン・エキスプレスの協力を得ています。加盟店は、決済代行業者に連絡して今後の予定を話し合う必要があります。アメリカン・エキスプレスの認定を受け、AMEX Enabledに登録済みの3DSサーバー（MPI）プロバイダーの一覧は、AMEX Enabledウェブサイト（www.amexenabled.com）でご確認いただけます。

Q3.5 加盟店は、すでにSAFEKEY 1.0に登録済みであっても、SAFEKEY 2.0に登録しなければならないのでしょうか?

SafeKey 2.0の利用にあたって必要な手続きについて、加盟店は3DSサーバー（MPI）プロバイダー又は決済代行業者に問い合わせる必要があります。

Q3.6 私は加盟店ですが、現在SAFEKEYを使用していません。SAFEKEY 2.0の登録方法を教えてください。

SafeKeyの登録方法については、まず3DSサーバー（MPI）プロバイダー又は決済代行業者にご相談ください。アメリカン・ エキスプレスに登録済みの認定3DSサーバー（MPI）プロバイダーの一覧は、AMEX Enabledウェブサイト（www.amexenabled.com）でご確認いただけます。

Q3.7 イシュアが対応するSAFEKEYのバージョンを加盟店または3DSサーバー（MPI）が知る方法は?

3DSサーバー（MPI）では、SafeKey 2.0に対応するイシュアと、対応する2.0バージョンに関する情報を取得しています。3DSサーバー（MPI）ではこのデータを使用して、適切な認証機能を判断します。

Q3.8 加盟店として、SAFEKEY用のアプリを有効にする方法は?

加盟店がSafeKey用のアプリをSafeKey 2.0で利用できるようにするには、3DSソフトウェア開発キット（SDK）を加盟店アプリに統合する必要があります。ご利用の3DSサーバー（MPI）プロバイダーまたは3DS SDKプロバイダーに協力を依頼してください。3DS SDKはEMVCoによるテストと承認を受ける必要があります。承認済みのSDKプロバイダーについては、www.emvco.comを参照してください。

Q3.9 3DSソフトウェア開発キット（SDK）とは?

3DS SDKとは、加盟店アプリに組み込まれるコンポーネントです。3DS SDKは加盟店アプリの代わりにSafeKeyの処理を行い、3DSサーバーとのやり取りを行います。

Q3.10 SAFEKEYの利用にあたって、アメリカン・エキスプレスは手数料を適用しますか?

いいえ。サービスの利用に伴うコストについては、3DSサーバー（MPI）プロバイダー又は決済代行業者にお問い合わせください。

Q3.11 イシュアがSAFEKEYに対応していない場合はどうなりますか?

現在、イシュアに対してSafeKeyはオプションのサービスになっていますが、イシュアはSafeKeyに参加していなくても、加盟店がSafeKey認証を試行した不正取引の債務責任を負う場合があります。SafeKey FLSポリシーの詳細については、ご利用のアクワイアラにご確認ください。

Q3.12 加盟店のアクワイアラがSAFEKEYに対応していない場合はどうなりますか?

加盟店のアクワイアラはSafeKeyの認定を受ける必要があります。必要な認証およびメッセージ送信が処理され、Fraud Liability Shiftの移行が適切に実行されるようにするためです。注: 加盟店の処理業者はSafeKeyに対応し、必要なデータをアクワイアラに転送できなければなりません。

Q3.13 SAFEKEYには、加盟店が強力な顧客認証に対応するための機能はありますか?

はい。SafeKeyの全バージョンは、PSD2要件など、強力な顧客認証に対応しています。

Q3.14 加盟店はSAFEKEYの承認および売上取引に関する仕様書をどこで入手できますか?

最新の技術仕様書については、ご利用のアクワイアラにお問い合わせください。アメリカン・エキスプレスが直接取得した加盟店は、www.americanexpress.com/merchantspecsにアクセスしてください。

セクション4: ACSおよび3DSサーバー（MPI）プロバイダーに関するFAQ

Q4.1 ACSおよび3DSサーバー（MPI）プロバイダーがSAFEKEYの認定を取得する方法は?

SafeKeyの認定を取得する最初のステップとして、AMEX Enabledに登録します。プロバイダーがSafeKeyの文書にアクセスするには、www.amexenabled.comの会社登録フォームに入力する必要があります。

Q4.2 認定ACSおよび認定3DSサーバー（MPI）プロバイダーのリストはどこで見られますか?

AMEX Enabledに登録済みの認定ACSおよび認定3DSサーバー（MPI）プロバイダーの一覧は、AMEX Enabledウェブサイト（www.amexenabled.com）でご確認いただけます。

Q4.3 SAFEKEY1.0の認定を取得している場合でも、SAFEKEY2.0の認定を受けなければならないのでしょうか?

はい。ACSおよび3DSサーバー（MPI）プロバイダーは、SafeKeyのバージョン別に個別に認定を取得する必要があります。詳しくは、www.amexsafekey.comをご覧ください。EMVCoについては、ACSおよび3DSサーバー（MPI）プロバイダー向けに必須のEMV 3DS認定サービスを提供していますが、この認定はアメリカン・エキスプレスによるSafeKey 2.0認定を受ける前に取得する必要があります。

Q4.4 認定とテストにはどのように登録しますか?

SafeKey認定プロセスを開始するには、www.amexenabled.comに登録してください。アメリカン・エキスプレスの認定アナリストがSafeKeyテスト ラボへのアクセス法を説明します。

セクション5: イシュアおよびアクワイアラに関するFAQ

Q5.1 イシュアおよびアクワイアラがSAFEKEYの認定を取得する方法は?

SafeKeyの認定取得方法については、アメリカン・エキスプレスの担当者にご相談いただくか、www.amexsafekey.comで詳細をご確認ください。

Q5.2 イシュアまたはアクワイアラがSAFEKEY1.0の認定を取得している場合でも、SAFEKEY2.0の認定を受けなければならないのでしょうか?

SafeKey 1.0および2.0のネットワーク メッセージに変更がないため、再認定は不要です。ただし、ACSの認証プロセスについては、認定を受ける必要があり総合確認テストを完了する必要があります。

付録: 機能比較図表

American Express SafeKey®の比較図

機能	SafeKey 1.0	SafeKey 2.0	
		SafeKey 2.1（EMV 2.1.0）	SafeKey 2.2（EMV 2.2.0）
業界標準の3-D Secureベース	▮	▮	▮
決済時のセキュリティを強化	▮	▮	▮
支払い認証	▮	▮	▮
ブラウザーベースの認証	▮	▮	▮
さまざまな認証方式を使用可能（ワンタイム パスコード、リスクベースの意思決定など）	▮	▮	▮
PSD2コンプライアンス対応	▮	▮	▮
円滑な認証を可能にする幅広いデータ要素をサポート	米国および米国の海外領土で使用可能	▮	▮
アプリベース（アプリ内）ショッピング対応	–	▮	▮
決済を伴わない本人認証	–	▮	▮
トークンベース取引	–	▮	▮
リスクベース認証（追加認証）機能	–	▮	▮
加盟店が起動する本人認証	–	–	▮
分離型認証	–	–	▮
PSD2追加インジケーター	–	–	▮

注記: 一部の機能については、追加認証が必要になる場合があります。