EMV 3-D セキュア導入ガイド

１．２版

2023年1月31日

クレジット取引セキュリティ対策協議会

内容

0. はじめに

（背景と目的）

非対面取引でのクレジットカード利用は拡大する一方で、不正利用も増加しており、同分野における不正利用対策の強化は喫緊の課題である。

当協議会のクレジットカード・セキュリティガイドライン（以下「セキュリティガイドライン」）では、非対面取引加盟店における不正利用対策の具体的方策の 1 つに、EMV 3-D セキュアの導入を掲げており、カード会社（アクワイアラーおよびイシュアー）、PSP には、EMV 3-D セキュアの導入態勢整備を求めている。

この状況を受け、EMV 3-D セキュアを導入する全ての事業者に向けて「EMV 3-D セキュア導入ガイド」を作成し、これが関係事業者間での共通のガイドとして円滑な推進の一助となるべく策定に至ったものである。

（対象読者）

- 非対面取引のクレジットカード加盟店　企画担当者、システム担当者
- 加盟店 EC サイト構築ベンダー　企画担当者、システム担当者
- カード会社（アクワイアラー）・PSP　企画担当者、システム担当者
- カード会社（イシュアー）　企画担当者、システム担当者

（本書の利用について）

「EMV 3-D セキュア導入ガイド」は、記載内容のアップデートが予定されるため最新版を利用すること。また、各章ごとに個別に利用できるように工夫しているため、関係事業者ごとに必要な章をご使用いただき、EMV 3-D セキュアの導入に役立てていただきたい。

1. EMV 3-D セキュアの概要

1. EMV 3-D セキュアの概要

（1） 3-D セキュアとは

3-D セキュアとは、オンラインショッピング時にクレジットカード番号等の情報の盗用による不正利用を防ぎ、安全にクレジットカード決済を行うために国際ブランドが推奨する本人認証サービスとなる。

3-D セキュアの国際ブランド毎の正式名称が異なる為、P9（図 6）を参照いただきたい。

（2） EMV 3-D セキュアとは（3-D セキュア 1.0 との比較）

EMV 3-D セキュアは、従来の 3-D セキュア（1.0）のバージョンアップされたスキームとして EMVCo[1]が新たに標準化した仕様であり、国際ブランドが導入を推進している。

また、EMV 3-D セキュアは、3-D セキュア（1.0）の課題であった、「パスワード等の入力負荷を軽減」「スマートフォンアプリへの対応」「非決済分野への対応」を実現する。

以下が、EMV 3-D セキュアの主な特徴である。

- ①リスクベース認証（詳細は次項参照）により、会員は ID・パスワード等の入力をすることなく認証が完了。
- ②スマートフォンやタブレットによるアプリ内での利用が可能。
- ③デジタルウォレットへのカード登録等、非決済分野での利用が可能。
- なお EMV 3-D セキュアと 3-D セキュア（1.0）は異なる技術仕様であり、互換性はない。

[1] EMVCo とは、カード決済の安全と普及促進のために、American Express、Discover、JCB、MasterCard、銀聯（UnionPay）、Visa という国際ブランド 6 社で構成された団体で様々なセキュリティに関するグローバルな標準仕様を策定している。

図 1【EMV 3-D セキュア特徴】

EMV 3-D セキュア				3-D セキュア1．0
特徴	内容	メリット		
		会員	加盟店	
パスワード等の入力負荷を軽減[2]	・原則リスクベース認証のみとなり、顧客へのパスワード要求が不要(フリクションレス) ・中リスク判定時のみワンタイムパスワード(イシューアーによって異なる)による認証を行う(「チャレンジ認証」を実施する)	入力負荷軽減	取引離脱(カゴ落ち)の減少	全取引にID・パスワード等を入力し認証を実施
スマホアプリへの対応	・ブラウザに加え、スマートフォンやタブレットのアプリ内決済に対応	利便性向上	認証強化	ブラウザ取引のみ推奨
非決済分野への対応	・モバイルウォレット等へのカード登録等、決済以外の利用が可能	入力負荷軽減	認証強化	決済分野のみ対応

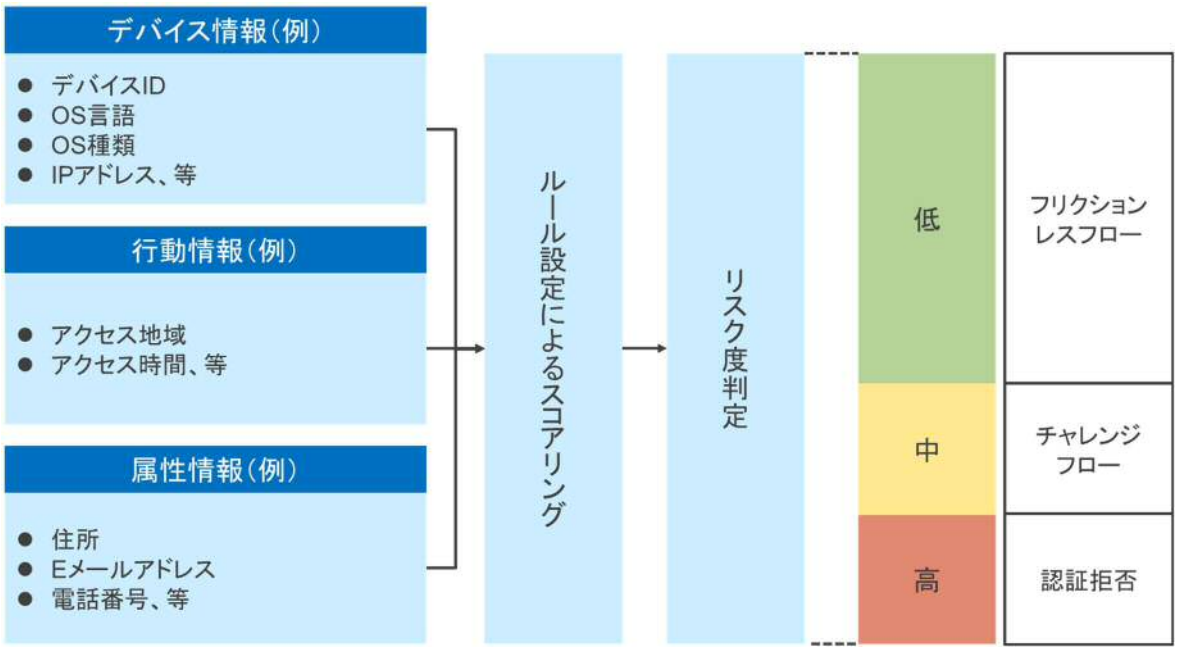
(3) リスクベース認証とは

リスクベース認証とは、不正購入防止の観点から本人認証強化のために、カード会社によって行われる当該取引における不正度合いの評価をさす。EC サイトで買い物を行う際、利用者から提供される個人情報や、利用者が決済に用いるパソコンやスマートフォンなどのデバイスから得られる情報などのデータを活用して、その購入が利用者本人のものであるかどうかを数値化して評価する。

EMV 3-D セキュアでは、リスクベース認証が必須化されている。リスクベース認証の活用により、リスクが低いと判定された取引は利用者の ID・パスワードの入力が省略可能となりユーザビリティが大きく改善し(「フリクションレス取引」が実現され)、クレジットカード決済時の離脱(カゴ落ち)の改善が見込まれる。

[2] リスクベース認証の判定結果により ID・パスワード等の入力が必要となる場合もある。

図 2【リスクベース認証のイメージ】



① フリクションレスフローとチャレンジフロー

リスクベース認証で判定されたリスク度合いに応じて、認証処理は下記の通りフローが異なる。

- 低：フリクションレスフローとしてパスワード等の入力なしに認証が完結する。
- 中：チャレンジフローとして会員に対して追加の認証（パスワードなど）を要求する。
- 高：認証拒否

図 3【EMV 3-D セキュアの認証フロー】

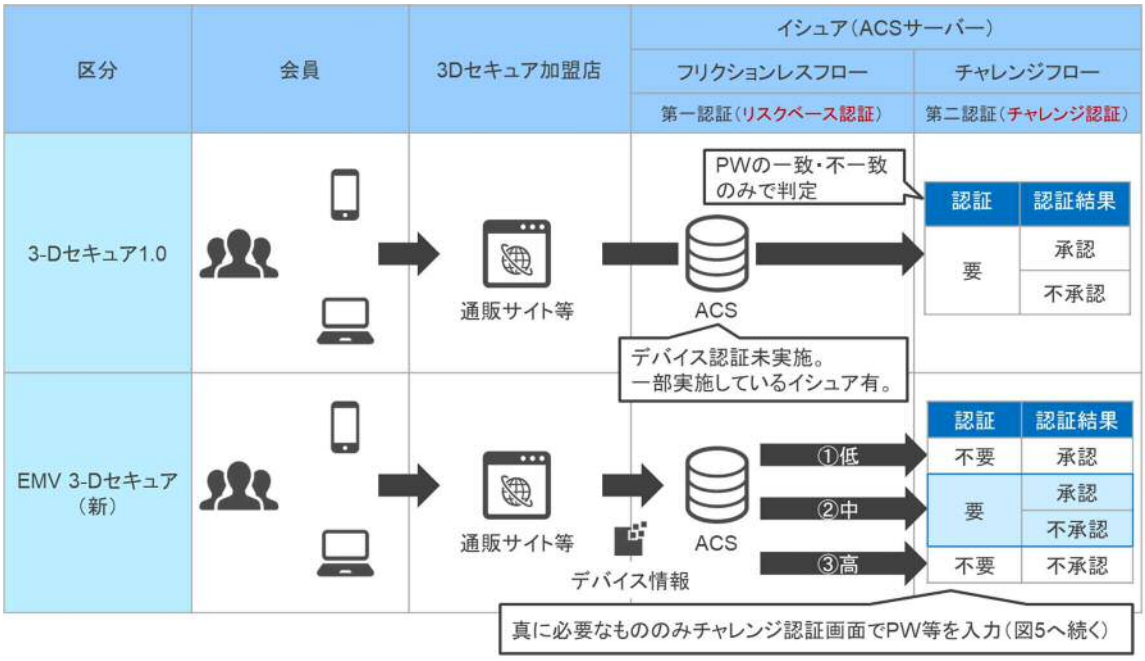


図 4【チャレンジ認証画面】[3]

（スマートフォン：サンプル）

（PC：サンプル）

（4）EMV 3-D セキュアの不正リスク負担について

EMV 3-D セキュアを実装した取引のうち、認証成功/カード会社もしくは会員未参加の取引において不正利用が発生した場合、原則リスク負担はカード会社（イシュアー）となる。

図 5【EMV 3-D セキュアの不正リスク負担】

	ステータス	リスク負担
1	EMV 3-D セキュア認証成功	加盟店は免責対象[4]
2	会員のカード発行会社または会員が EMV 3-D セキュア未参加	
3	EMV 3-D セキュア認証取引外	加盟店[5]は免責対象外

※2021 年 11 月現在

※詳細は契約カード会社（アクワイアラー）等への確認が必要。

（5）各国際ブランドの3-D セキュアのサービス名称

クレジット取引セキュリティ対策協議会としては、「3-D セキュア/EMV 3-D セキュア」を正式名称として各種案内をしているが、国際ブランドでは以下の通り、個々のサービス名称で呼ばれている。

---

[3] 「ブランドロゴ/サービスロゴ」は、国際ブランドによって「（国際）ブランドロゴ」と「3-D セキュアのサービスロゴ」どちらを掲載しているのかが異なるため、このような記載とした。

[4] カード登録時に EMV 3-D セキュア認証していても、以降の取引時にも EMV 3-D セキュア認証しない限りは免責対象外となる。

[5] 契約のカード会社（アクワイアラー）との契約内容による。

図 6【各国際ブランドの3-D セキュアのサービス名称】

	サービス名称	サービスロゴ
Visa	Visa Secure	
Mastercard	Mastercard ID Check	
JCB	J/Secure	
AMEX	American Express SafeKey	
Diners （Discover）[6]	ProtectBuy	
UnionPay International （銀聯国際）	UnionPay 3-D Secure	

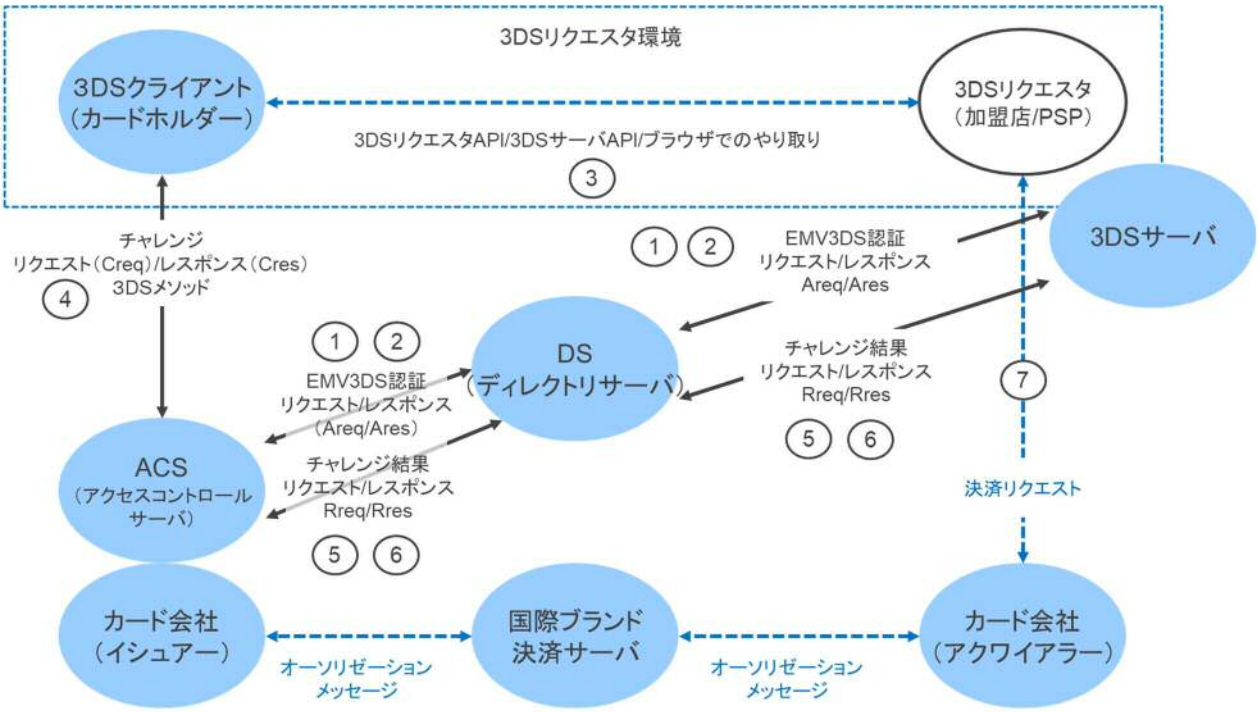
（6）EMV 3-D セキュア処理フロー概要

EMV 3-D セキュアは、加盟店や決済代行会社から本人認証に必要な情報をカード会社（イシュアー）へ送信することで、カード会社が当該取引の不正利用のリスク判断を行う。

主に ACS（Access Control Server）、DS（Directory Server）、3-D セキュア Server（以下 3DS サーバー）の 3 つの仕組みから構成され、ACS はイシュアーの提供機能として本人認証やリスクベース認証を行い、DS は 3DS サーバーと ACS との中継、3DS サーバーは EC サイトと DS 間の中継を担い、不正利用の低減を行う。

[6] Discover は Diners の 3-D セキュアサービスを利用している。（※2022 年 2 月現在）

図 7【EMV 3-D セキュア全体】[7]



① 処理フロー概要 （ブラウザベース・チャレンジフローの一例）

I. 加盟店/PSP と 3DS サーバーは、利用者の個人情報や利用デバイスから得た情報をもとに AReq 電文を生成し、DS へ送信。DS は該当するイシュアーの ACS へ中継する。

II. ACS は、AReq 電文の内容をもとにリスクベース認証を行い、認証結果の応答電文（ARes）を応答する。
（この場合は ACS が「チャレンジ要求」の判定をしている。）

III. 3DS サーバーは、チャレンジの実施を受け容れた場合、利用者のブラウザにチャレンジに必要な情報を送信する。

IV. 利用者のブラウザから ACS へ直接 CReq 電文を送信し、ブラウザにはチャレンジ認証画面が表示され、利用者は必要な情報を入力する（CRes）。

V. ACS は、チャレンジ認証を実行し、認証結果を RReq 電文に設定して DS へ送信。DS は 3DS サーバーへ中継する。

VI. 3DS サーバーは、認証結果を受け取った応答として RRes 電文を DS へ送信。DS は ACS へ中継する。

VII. 加盟店/PSP は、利用者のブラウザを通して最終的な認証結果を確認し、認証結果および認証情報（AAV、CAVV）を設定したオーソリゼーションをアクワイアラーへ送信する。

[7] 点線および 3DS リクエスタは 3DS 仕様の一部ではないが、説明目的でのみ記載している。出典：EMVCo より。

図 8【(トランザクションステータス表)3DS 認証結果表】

ステータス	最終的な Transaction Status の値	ECI の値	オーソリゼーション
認証成功: Authentication Verification Successful	Y	05 Mastercard は 02	送信可能
アテンプト(ISS 未対応 or 会員未登録): Attempts Processing Performed; Not Authenticated/Verified, but a proof of attempted authentication/verification is provided	A	06 Mastercard は 01	送信可能
3DS 認証が出来なかった: Authentication/Account Verification Could Not Be Performed; Technical or other problem, as indicated in the ARes or RReq	U	07 Mastercard は 00	送信する場合は 3DS 取引ではなく通常 EC 扱い
認証しなかった: Not Authenticated/Account Not Verified[8]; Transaction denied	N	ー	送信する場合は 3DS 取引ではなく通常 EC 扱い
チャレンジ認証要(CReq/CRes): Challenge Required; Additional authentication is required using the CReq/Cres	C		
チャレンジ認証要(Decoupled Authentication): Challenge Required; Decoupled Authentication confirmed	D		
認証拒否: Authentication/ Account Verification Rejected; Issuer is rejecting authentication/verification and request that authorization not be attempted.	R	ー Mastercard は 00	送信不可
情報提供のみ: Informational Only; 3DS Requestor challenge preference acknowledged	I	07 Mastercard は 06	送信可能

※本表は EMVCo の定義に沿って記載しているが、実際の取引で使用される返却値については各国際ブランドによって異なる場合がある。(例:「A」を使用しない場合があるなど)

[8] Account Not Verified は、イシュアーがリスクベース認証を実施する対象で無いカード番号を意味する(チャレンジ認証のためのパスワード等の登録が無いという事でない)。

② 各プレイヤーの説明

主に ACS（Access Control Server）、DS（Directory Server）、3-D セキュア Server（以下 3DS サーバー）の 3 つの仕組みから構成される。

ACS はイシュアーの提供機能として本人認証やリスクベース認証を行い、DS は 3DS サーバーと ACS との中継を担うブランドシステム、3DS サーバーは EC サイトと DS 間の中継を担う加盟店のシステムとして、認証のうえ不正利用の低減を行う。

✓ ACS（Access Control Server）：イシュアーが運営する認証サーバー

【概要】

ACS はイシュアーにより提供される機能で、認証要求に対するリスク判定や個別のトランザクションの認証を実行する。

【主な機能】

カード番号が 3DS 認証の対象であるかを検証する。利用者のデバイスから得られる情報や属性情報を利用し、認証要求があったトランザクションについてリスク判定[9]を行う。判定されたリスク度合いに応じてチャレンジ認証によりカード会員を認証する。

後続のオーソリゼーションの要求が正しく 3DS 認証されたかを検証するために、オーソリゼーションに設定するための認証情報（AAV、CAVV）を生成し、3DS サーバーへ提供する。

✓ DS（Directory Server）：国際ブランドが提供する機能で、ACS と 3DS サーバー間のデータ通信を取り持つ認証サーバー

【概要】

DS はカード番号に紐付く ACS を判別し、3DS サーバーと ACS 間の電文の仕向け中継を行う。

【主な機能】

3DS サーバー・ACS のサーバーを認証する。3DS サーバーと ACS の間で電文をルーティングする。

✓ 3DS サーバー：DS と加盟店とのデータ通信を取り持つ認証サーバー

【概要】

3DS サーバーは、3DS リクエスタ[10]（3DS の認証要求を行う加盟店や PSP（決済代行会社））と DS 間の機能的インタフェースを提供する。

【主な機能】

3DS 認証要求の電文に必要なデータ要素を収集する。DS、3DS SDK、及び 3DS リクエスタを検証する。電文内容が保護されている事を確実にする。

---

[9] ACS が取得したデバイス情報や属性情報等を用いて当該認証要求のリスク度を3段階に判定する。リスク判定後の認証処理は次のフローとなる。
①低リスク：①低（フリクションレスフローとしてパスワード等の入力なしに認証が完結）
②高リスク：②高（認証失敗（拒否））
③上記以外：③中（チャレンジフローとして会員に対して追加の認証（パスワードなど）を要求する）

[10] 3DS リクエスタ環境：利用者デバイス、EC サイト、PSP、3DS サーバーによって提供される環境であって、3DS の認証要求の起点となる。クレジットカード決済時に 3DS リクエスタ環境から 3DS サーバーで収集された認証用データが、3DS サーバーから DS を経由して ACS に送信される。

図 9【用語集】

用語	用語説明
AReq（Authentication Request Message） 認証リクエスト電文	3-D セキュア認証フローにおいて、最初の電文である。3DS サーバーが AReq 電文を生成し、カード会員の認証を要求する。電文には当該トランザクションのカード会員属性情報、決済、及び、デバイス情報を含める事が出来る。
ARes（Authentication Response Message） 認証レスポンス電文	ARes 電文はイシュアーの ACS が AReq 電文に応答するものである。カード会員が認証された事または、認証を完了する為にさらにカード会員とのやり取り（チャレンジフロー）が要求される事、または認証拒否を示す事が出来る。
CReq（Challenge Request Message） チャレンジリクエスト電文	CReq 電文は、チャレンジフローにおいてカード会員とのやり取りを開始する。カード会員からの認証データを伝送する事に使用出来る。
CRes（Challenge Response Message） チャレンジレスポンス電文	CRes 電文は、CReq に対する ACS の応答である。カード会員の認証結果または、App-ベースモデルの場合は、追加のカード会員とのやり取りが認証完了の為に要求される事を示す事が出来る。
App-based App-ベース	EMV 3-D セキュアがサポートする3つのデバイスチャネルの1つで、利用者の環境が iOS や Android OS などのコンシューマデバイス上のアプリで認証を実施するために用意された認証プロトコル。 3DS サーバー事業者が提供する 3DDS SDK をアプリに実装することで実現する。
Browser-based ブラウザベース	EMV 3-D セキュアがサポートする3つのデバイスチャネルの1つで、利用者の環境が PC やスマートフォンのブラウザで認証を実施するために用意された認証プロトコル。
3DS Requestor Initiated（3RI） 3RI	EMV 3-D セキュアがサポートする3つのデバイスチャネルの1つ。利用者が介在しない環境で加盟店のシステムを起点として認証処理を実施するために用意された認証プロトコル。 例えば、カード情報の登録型加盟店において、登録されているカードの有効性確認などを行うことに用いることが想定される。

用語	用語説明
RReq (Results Request Message) 結果リクエスト電文	RReq 電文は、認証または検証の結果をやり取りする。当該電文は、ACS から、DS を介して 3DS サーバーに要求される。1回の AReq 電文につき、1つの RReq 電文のみである。RReq 電文は、フリクションレスフローでは使用されない。
RRes (Results Response Message) 結果レスポンス電文	RRes 電文は、RReq 電文を受領したことを知らせる電文である。当該電文は、3DS サーバーから DS を経由して ACS に送信される。1 回の RReq 電文につき、1 つの RRes 電文のみである。
3DS Method	ACS のリスクベース認証をより効果的に行うために、加盟店の決済用ページなどを通じて利用者の環境から直接ブラウザ情報を得る方法
3DS Method URL	3DS Method を実行するために使用する URL
3DS SDK	App-ベースのデバイスチャネルにおいて、アプリに実装することで 3DS サーバーと必要なデータ通信を行うことが可能となるもの。 3DS サーバー事業者が提供する。
Challenge Flow チャレンジフロー	ACS のリスク判定結果により利用者に対してチャレンジ認証を要求する認証フロー。ID/パスワード等による認証が求められる。
Frictionless Flow フリクションレスフロー	ACS のリスク判定結果により、チャレンジが不要であり、リスクベース認証のみで完了するフロー※。 利用者は決済時に追加のアクションなしで認証が完了するため、カゴ落ちの防止に貢献することが期待できる。※チャレンジフローと平仄を取るべきである。
Electronic Commerce Indicator (ECI)	各国際ブランドが規定する 3-D セキュアの認証結果を表す値で、加盟店は認証結果に含まれる最終的なトランザクションステータス等から判断してオーソリゼーションに値を設定する。 国際ブランドによって値が異なるため注意が必要。 詳細は(6)EMV 3-D セキュア処理フロー概要を参照
Transaction Status トランザクションステータス	ACS が最終判定した認証結果の値。 詳細は(6)EMV 3-D セキュア処理フロー概要を参照

２．導入手続きについて

2. 導入手続きについて

（1）加盟店の導入形態について

3-D セキュアの認証やオーソリゼーションなどの決済システムを自社で構築しているケースや PSP・決済代行事業者等（以下、PSP）のサービスを利用しているケースなど、導入形態により手続きやシステム対応の方法は異なる。

図 10【導入形態について】

図 11【導入形態に応じた、加盟店の対応事項】

手続き対象	①自社構築[11] （カード会社直接加盟店、3DS サーバー事業者ホスティングサービス利用の場合）	②PSP の業務代行 （カード会社直接契約加盟店）	③PSP のサービス利用 （包括代理契約加盟店）
カード会社 （アクワイアラー）	・（必要な場合）EMV 3-D セキュア覚書締結 ・Acquirer Merchant ID, Acquirer BIN, MCC など設定情報の取得・調整 ・（必要な場合）国際ブランドテスト実施申請	・（必要な場合）EMV 3-D セキュア覚書締結 ・（必要な場合）Acquirer Merchant ID, Acquirer BIN, MCC など設定情報の取得・調整 ・（必要な場合）国際ブランドテスト実施申請	基本的なカード会社(アクワイアラー)との契約については、PSP にて実施。
3DS サーバー事業者	・利用申込と契約 ・接続仕様と必要な設定情報の受領 ・3DS SDK の受領	対応不要（接続条件、SDK も PSP より受領）	
情報処理センター	・オーソリゼーションの EMV 3-D セキュア対応申込 ・接続確認試験等の申込	対応不要（PSP にて代行）	
PSP	―	・EMV 3-D セキュア利用申込	
システム対応	・3DS サーバーの接続 ・3DS SDK の実装（App ベースの場合） ・Acquirer Merchant ID, Acquirer BIN, MCC などの設定 ・3DS サーバーとの接続テスト ・AReq 認証要求データ項目の設定 ・（必要な場合）国際ブランドテストの実施 ・情報処理センターとのオーソリゼーション接続確認試験の実施	・（必要な場合） Acquirer Merchant ID, Acquirer BIN, MCC などの設定 ・AReq 認証要求データ項目の設定 ・PSP との接続テスト ・（必要な場合）国際ブランドテストの実施および証明書の取得	

[11] ①自社構築においては、3DS サーバー事業者ホスティングサービス利用以外に、3DS サーバー製品を購入して自社サーバーで運用する方法や、3DS サーバーを自社開発する方法など、複数の選択肢があるが、代表例として 3DS サーバー事業者が運営するサーバーによるホスティングサービス利用について記載する。

①自社構築（カード会社直接加盟店、3DS サーバー事業者ホスティングサービス利用の場合）の場合

■ **カード会社（アクワイアラー）との手続き**

✓ **EMV 3-D セキュア覚書締結（必要な場合）**

- カード会社（アクワイアラー）との加盟店契約等に含まれているケースや、加盟店契約に付随して 3-D セキュア利用に関する覚書などが必要になるケースなどがあるため、契約カード会社（アクワイアラー）に確認が必要。

✓ **Acquirer Merchant ID, Acquirer BIN など設定情報の取得・調整**

- 契約カード会社（アクワイアラー）へ申請して 3-D セキュア認証要求時の電文に設定が必要となる設定情報（Acquirer Merchant ID、Merchant Name、MCC、Acquirer BIN）を受領する。また、Merchant Name、Merchant Category Code（MCC）については実態に即した値を設定する必要がある為、Merchant ID の 1 本化等、例外的な運用の場合は契約カード会社への確認が必要。（MCC の設定は「別紙_統合版_AReq 設定項目」を参照）
- 申請の際には、加盟店 Web サイトの URL、契約カード会社（アクワイアラー）の加盟店番号などが必要となる場合があるため、詳しくは契約カード会社（アクワイアラー）への確認が必要となる。

✓ **国際ブランドテスト実施申請（必要な場合）**

- 3DS サーバー事業者ホスティングサービス利用の場合、通常は不要だが、必要となる場合があるため、契約カード会社へ確認すること。

■ **3DS サーバー事業者との手続き**

✓ **利用申込と契約**

- 契約する 3DS サーバー事業者に対して利用の申込み、契約等の手続きを行う。
- 利用する 3DS サーバー製品の要件を以下に示す。
  I. 3DS サーバー製品が EMVCo および国際ブランド所定のテストに合格し、認定を受けていること。
  II. 3DS ホスティングサービス事業者が国際ブランドから 3DS サービスプロバイダーとしての登録を受けていること。
  III. 3DS ホスティングサービスが国際ブランド所定のテストに合格し、認定を受けていること。
  IV. 3DS ホスティングサービスが PCI DSS または PCI 3DS に準拠していること。

✓ **接続仕様と必要な設定情報の受領**

- 契約する 3DS サーバー事業者から接続に必要となる仕様書や 3DS Requestor ID、3DS Requestor Name など、システム対応に必要な設定情報を受領する。

✓ **3DS SDK の受領**

- App ベースの場合は 3DS SDK を受領し、自社アプリへの実装に必要となる仕様書や設定情報を受領する。

■ **情報処理センターとの手続き**

✓ **オーソリゼーションの EMV 3-D セキュア対応申込**

- EMV 3-D セキュアの認証結果情報をオーソリゼーション電文に設定するためには、オーソリゼーションネットワークを運営する情報処理センターとの手続きが必要となる。

✓ **接続確認試験等の申込**

- EMV 3-D セキュアに対応したオーソリゼーション電文の確認試験が必要となる。詳細は契約する情報処理センターへ確認すること。

■ **システム対応**

✓ **3DS サーバーの接続、3DS SDK の実装**

- 3DS サーバー事業者所定の手順に従い、システムに 3DS ホスティングサービスを組み込む。
- App ベースの場合は 3DS サーバー事業者から提供された 3DS SDK をアプリへ組み込む。

✓ **Acquirer Merchant ID, Acquirer BIN などの設定**

- カード会社との手続きにて受領した Acquirer Merchant ID, Acquirer BIN をシステムに設定する。
- MCC、Merchant Name は実態に即した情報を設定する。（MCC の設定は「別紙_統合版_AReq 設定項目」を参照）
- 3DS サーバー事業者から受領した 3DS Requestor ID、3DS Requestor Name も設定する。

✓ **AReq 認証要求データ項目について**

- AReq 認証要求電文には EMVCo および国際ブランドが定めるデータ項目を設定する必要がある。
- 取引内容（一般的な通信販売、配送を伴わないサービス提供やデジタルコンテンツの販売、会員制サービスへのクレジットカード登録など）により設定する内容が異なる場合がある。
- 詳細は第 3 章で説明する。

✓ **3DS サーバーとの接続テスト**

- 3DS サーバー事業者所定の手順に従い、接続テストを実施する。

✓ **国際ブランドテストの実施（必要な場合）**

- 必要な場合はカード会社との手続きにて申し込んだ国際ブランドの DS との接続テストを実施する。詳しくは契約カード会社への確認が必要となる。

✓ **情報処理センターとのオーソリゼーション接続確認試験の実施**

- オーソリゼーションネットワークの仕様に従い、EMV 3-D セキュアの認証結果情報をオーソリ電文に設定できるようシステム構築を行う。
- システム構築完了後に情報処理センターとのオーソリゼーション接続確認試験が必要となる。詳細は契約する情報処理センターへの確認が必要となる。

② PSP の業務代行（カード会社直接契約加盟店）の場合

■ カード会社との手続き

✓ EMV 3-D セキュア覚書締結

- 3-D セキュアのシステムは PSP 提供となるが、前述の「EMV 3-D セキュア覚書締結」「Acquirer Merchant ID, Acquirer BIN など設定情報の取得・調整」「テスト」が必要となる場合がある。詳しくは契約する PSP および契約カードへの確認が必要となる。

✓ Acquirer Merchant ID, Acquirer BIN など設定情報の取得・調整

- 契約カード会社へ申請して 3-D セキュア認証要求時の電文に設定が必要となる Acquirer Merchant ID、Acquirer BIN など設定情報を受領する。また、Merchant Category Code（MCC）について実態に即した値を設定する。（MCC の設定は「別紙_統合版_AReq 設定項目」を参照）
- 申請の際には英字の Merchant Name、加盟店 Web サイトの URL、契約カード会社の加盟店番号などが必要となる場合がある。詳しくは契約カード会社への確認が必要。

✓ 国際ブランドテスト実施申請（必要な場合）

- 3DS サーバー事業者ホスティングサービス利用の場合、通常は不要だが、必要となる場合があるので、契約カード会社へ確認すること。

■ PSP との手続き

✓ EMV 3-D セキュア利用申込

- 契約する PSP に対して EMV 3-D セキュアの利用申込を行う。詳細は契約する PSP への確認が必要となる。

■ システム対応

✓ Acquirer Merchant ID, Acquirer BIN, MCC などの設定（必要な場合）

- カード会社から受領した Acquirer Merchant ID, Acquirer BIN 設定が必要となる場合があるので、契約する PSP への確認が必要となる。
- PSP の仕様に基づき、MCC、Merchant Name は実態に即した情報を設定する。（MCC の設定は「別紙_統合版_AReq 設定項目」を参照）

✓ AReq 認証要求データ項目の設定

- PSP の仕様に基づき、AReq 認証要求電文には EMVCo および国際ブランドが定めるデータ項目を設定する必要がある。詳細は第 3 章で説明する。

✓ PSP との接続テスト

- PSP の仕様に基づき、正しく設定がされているか接続テストにより確認を行う。詳細は契約する PSP への確認が必要となる。

✓ 国際ブランドテストの実施（必要な場合）

- 必要な場合はカード会社との手続きにて申し込んだ国際ブランドの DS との接続テストを実施する。詳しくは契約カード会社への確認が必要となる。

③ PSP のサービス利用（包括代理契約加盟店）の場合

■ **PSP との手続き**

✓ **EMV 3-D セキュア利用申込**

- 契約する PSP に対して EMV 3-D セキュアの利用申込を行う。詳細は契約する PSP への確認が必要となる。

■ **システム対応**

✓ **Acquirer Merchant ID, Acquirer BIN, MCC などの設定（必要な場合）**

- カード会社から受領した Acquirer Merchant ID, Acquirer BIN 設定が必要となる場合があるので、契約する PSP への確認が必要となる。
- PSP の仕様に基づき、MCC、Merchant Name は実態に即した情報を設定する。（MCC の設定は「別紙_統合版_AReq 設定項目」を参照）

✓ **AReq 認証要求データ項目の設定**

- PSP の仕様に基づき、AReq 認証要求電文には EMVCo および国際ブランドが定めるデータ項目を設定する必要がある。詳細は第 3 章で説明する。

✓ **PSP との接続テスト**

- PSP の仕様に基づき、正しく設定がされているか接続テストにより確認を行う。詳細は契約する PSP への確認が必要となる。

（2） 本番確認

一般のお客様へのサービス開始前に関係者にて本番確認を行うことを推奨する。実装した国際ブランドのカードを用意し、動作確認を行うことで導入時における品質の確保が図れる。

（3） その他

① EC サイト構築における留意事項

✓ **個人情報提供に関する同意取得について**

- EMV 3-D セキュアの認証要求時に利用者の個人情報を設定する場合は、利用者からの同意を得る必要がある。詳しくは第 4 章で説明する。

✓ **各国際ブランドのサービスロゴの入手と表示**

- EMV 3-D セキュアは夫々の国際ブランドがサービス名・サービスロゴを設けているため、利用者への解り易さを向上するためにもサービスロゴを EC サイトで表示することを推奨する。詳しくは第 5 章で説明する。

② 3-D セキュア認証要求時の電文設定に関する PSP の仕様に関する留意事項

✓ Merchant Name は加盟店店子単位での設定を必須とする。

✓ Merchant ID、MCC は原則として加盟店店子単位が望ましい。

３. システム開発要件（開発者向け）

3. システム開発要件（開発者向け）

（AReq 認証要求データ項目について）

本章では、加盟店/PSP が EMV 3-D セキュアを導入する際、システム実装時において課題となることが多いポイントにフォーカスしている。なお、本書は EMV®3-D Secure Protocol and Core Functions Specification（以降「EMV 仕様」という）ならびに、各ブランドの仕様書改訂に伴い、必要に応じて改訂される可能性がある。そのため、システム実装における詳細については、EMV 仕様ならびに、各ブランドの仕様書を参照することに留意する必要がある。

（1） AReq 設定項目

EMV 3-D セキュアにおいては、加盟店/PSP から AReq 電文を送信することで認証処理が開始される。

AReq 電文項目には、イシュアーにおける不正検知精度向上のため、利用者の端末情報を含む各種個人情報を送信するための項目が設計されている。

将来的には、各種個人情報を利用し、さらに不正検知精度向上を図ることを検討するものの、まずは EMV 3-D セキュアへの移行を円滑に推進することを目的として、AReq 電文の各項目について必須送信項目と不正検知精度向上に向けた推奨項目を「別紙_統合版_AReq 設定項目」に示す。

なお、「別紙_統合版_AReq 設定項目」では、最終的にイシュアーに届ける電文項目の一覧を示しており、AReq 電文の必須項目及び、不正顕在化加盟店や高リスク商材加盟店等で使用するオプション項目をどのように設定するかについては、当事者間（アクワイアラー、PSP、加盟店）で確認が必要である。

なお、AReq 項目の設定にあたり EMVCo 必須項目が未設定の場合に DS や ACS でエラーとなる可能性があることに留意する必要がある。

（2） PA（Payment Authentication）と NPA（Non － Payment Authentication）の実装方法

EMV 3-D セキュアにおいては、決済利用（PA）と決済外（非決済）（NPA）での利用を Data Element の「Message Category」で識別する。また、PA と NPA それぞれで AReq 設定項目の必須、任意が異なる点に留意する必要がある。

NPA での AReq 要求に対するイシュアーからの応答には認証結果および認証情報（AAV、CAVV）が設定されない場合があり、後続のオーソリゼーションは 3-D セキュアとして適正に処理できないと考えられる。よって NPA の使用にあたっては予め契約カード会社（アクワイアラー）との調整が必要な点に留意する必要がある。

（3） 3DS Requestor Authentication Indicator の実装方法

EMV 3-D セキュアにおいては、Data Element の「3DS Requestor Authentication Indicator」で認証の対象となる取引を識別する。「3DS Requestor Authentication Indicator」に値を設定する際に、PA と NPA で一般的に設定されると考えられる値は以下の通りとなる。ただし、詳細な使い方については、各ブランドの仕様書を参照することに留意する必要がある。

図 12【PA と NPA での一般的な設定値】

取引名称	一般的な設定値 （3DS Requestor Authentication Indicator）
PA（Payment Authentication） NPA（Non – Payment Authentication）	01（決済取引：Payment transaction）
	02（定期的取引：Recurring transaction）
	03（割賦取引：Instalment transaction）
	04（カード登録・追加：Add card）
	05（カード情報変更・更新：Maintain card）

（4）全件パスワード認証を行う場合の実装方法

デジタルウォレットへのクレジットカードの登録等、一部の認証取引においては、チャレンジ認証による本人確認を必須としたいという加盟店/PSP のニーズがある。

そういったニーズに対応する場合の加盟店/PSP の実装ガイドを下記に示す。なお、会員利便性の観点から国際ブランドの規定により一定水準のフリクションレス率を求められていること、及びフリクションレスフローは EMV 3-D セキュアのメリットであることから、一部イシュアーにおいては下記ガイドに従って実装した場合でも、イシュアー判断でフリクションレスフローに遷移する可能性があるが、その場合であっても Transction Status が“Y”であった場合は認証成功として処理を継続することが可能である点に留意する必要がある。

① PA(Payment Authentication)

PA 取引にて、全件パスワード認証を行う場合、Data Element のオプション項目である「3DS Requestor Challenge Indicator」を設定する必要がある。「3DS Requestor Challenge Indicator」には 03、または 04 のいずれかを設定するが、それぞれの使い分けの例は以下の通り。

✓ **03：イシュアーにチャレンジを求める**

✓ **04：イシュアーに必ずチャレンジを求める**

② NPA(Non-Payment Authentication)

NPA 取引にて、全件パスワード認証を行う場合、PA 取引と同様に Data Element のオプション項目である「3DS Requestor Challenge Indicator」を設定する必要がある。

「3DS Requestor Challenge Indicator」は PA 取引と同様 03、または 04 のいずれかを設定する。使い分けについても PA 取引と同様となる。

＜当該カードが EMV 3-D セキュア未登録の場合＞

加盟店から認証要求時（AReq）に「3DS Requestor Challenge Indicator」に 03、または 04 が設定されていても、当該カードが EMV 3-D セキュア未登録もしくはイシュアーが未対応の場合はチャレンジ認証に遷移することができない。

この場合の認証結果（ARes）は、イシュアーもしくは DS のリスク判定に応じた Transaction Status の設定が国際ブランドの規定に沿った対応となる事に留意する必要がある。

なお、04 が設定されている場合は加盟店による強い要望であることを考慮し、当該カードが EMV 3-D セキュア未登録の場合において、イシュアーとしては国際ブランドの規定も確認しつつ、当該取引の不正リスクを十分に検証のうえ判定することが望ましい。国内クレジットカード会社には本内容を周知するが、実際の判定はイシュアーに委ねられる。

図 13【会員未登録もしくは ISS 未対応の場合において想定される認証結果の例】

	Transaction Status	Transaction Status Reason	
会員未登録もしくは ISS 未対応（アテンプト）	A※		
認証しなかった（会員未登録）	N	13=Cardholder not enrolled in service	
認証成功	Y		低リスクと判定された場合
認証拒否	R	01=Card authentication failed など	高リスクと判定された場合

※一部の国際ブランドでは、イシュアーが認証結果（ARes）の Transaction Status に”A”を設定することが許容されていない。また、イシュアーが設定した Transaction Status を DS が”A” もしくは“Y”に変更して応答する場合がある。

※ISS 未対応の場合は DS が Transaction Status を応答するが、一部の国際ブランドでは DS のリスク判定に基づいた Transaction Status を各取引に対し応答する場合がある。

（5）オーソリゼーションへの項目設定

EMV 3-D セキュア実施後、加盟店/PSP よりオーソリゼーションを実施する場合は、EMV3-D セキュアの認証結果の情報を電文にセットする必要がある。

EMV 3-D セキュアにおいてオーソリゼーション時に設定が必要な項目を以下に示す。設定の詳細については、ネットワーク事業者の仕様書及び、各ブランドや PSP の仕様書を確認すること。

図 14【オーソリゼーション時に設定が必要な項目（例）】

EMV 3-D セキュアの項目	
Data Element	Field Name
Cardholder Account Number	acctNumber
Card/Token Expiry Date	cardExpiryDate
Purchase Amount	purchaseAmount
Message Version Number	messageVersion
Transaction Status	transStatus
Authentication Value	authenticationValue
Electronic Commerce Indicator	eci
DS Transaction ID	dsTransID
3DS Server Transaction ID	threeDSServerTransID

（6）個人情報の同意画面の作成内容について

カードホルダーから提供をうける個人属性情報は本人に利用について明示的に同意を取るような画面構成とする。

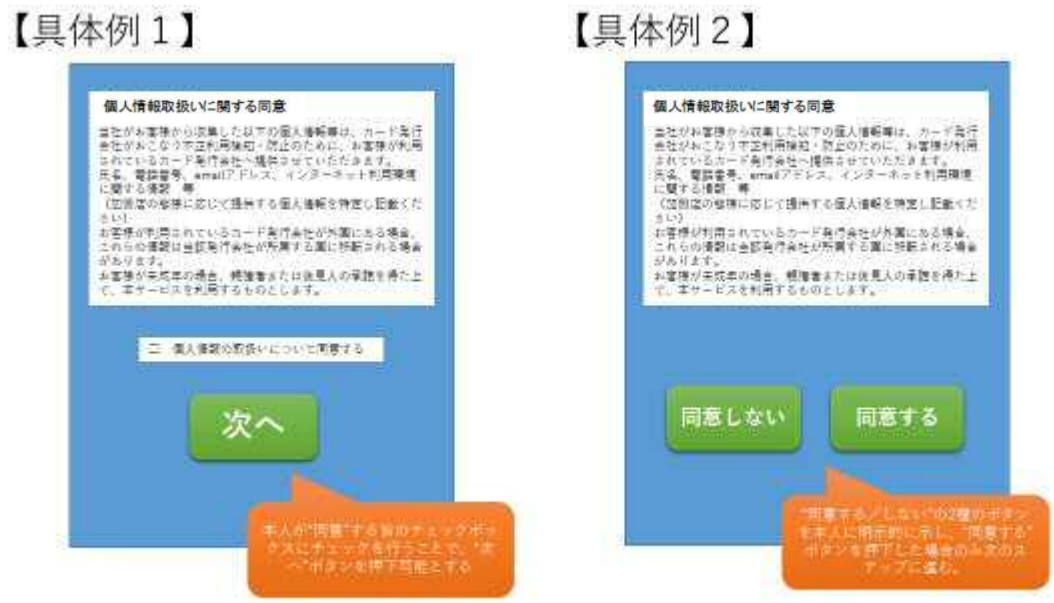
画面構成の具体例

例1：画面の下段に同意する旨のチェックを行うチェックボックスを設け、本人がチェックを行うことで次のステップに進むボタンを押下できる仕様とする。

例2：画面の下段に”同意する／しない”のボタンを明示的に設け、本人が”同意する”ボタンを押下することで次のステップに進む仕様とする。

なお、同意文案は第 4 章を参照のこと。

図 15【同意取得画面の構成サンプル画像例】



（7）3DS Method について

3DS Method は、ACS（イシュアー）が 3DS クライアント（カードホルダー）の利用デバイス情報を取得し、リスクベース認証をより効果的に実行することができる方法である。3DS Method は認証処理の範囲外で、3DS サーバーが DS に対し 3DS Method URL（3DS Method を実行するための URL）を取得しており、加盟店/PSP が 3DS クライアント環境で 3DS Method URL を実行することで、ACS が 3DS クライアントの利用デバイス情報を収集する。加盟店/PSP は 3DS Method URL を 3DS サーバーが取得している場合、3DS Method を実行する点があることに留意する必要がある。

４. EMV 3-D セキュア導入加盟店における
個人情報保護法の遵守に関する留意点

4. EMV 3-D セキュア導入加盟店における個人情報保護法の遵守に関する留意点

EMV 3-D セキュアの仕組みにおいて、各カード会社が、カード会員のデバイス情報等を用いて不正利用のリスク判断を行うと共に、必要に応じてパスワード入力を要求することで当該取引における安全性を確保する。関係事業者はこの仕組みを有効に活用する一方で、利用できる情報が個人情報になり得る場合には、個人情報保護法に従った適切な取扱いを行う必要がある。なお、本章は、クレジット取引セキュリティ対策協議会が令和 4 年 12 月 27 日に発信した「2022 業企 252 号」の文書に基づいて作成しており、最終的な実務運用は関係当事者間（アクワイアラー、PSP、加盟店）での判断をお願いしたい。

（1）個人情報保護法とは

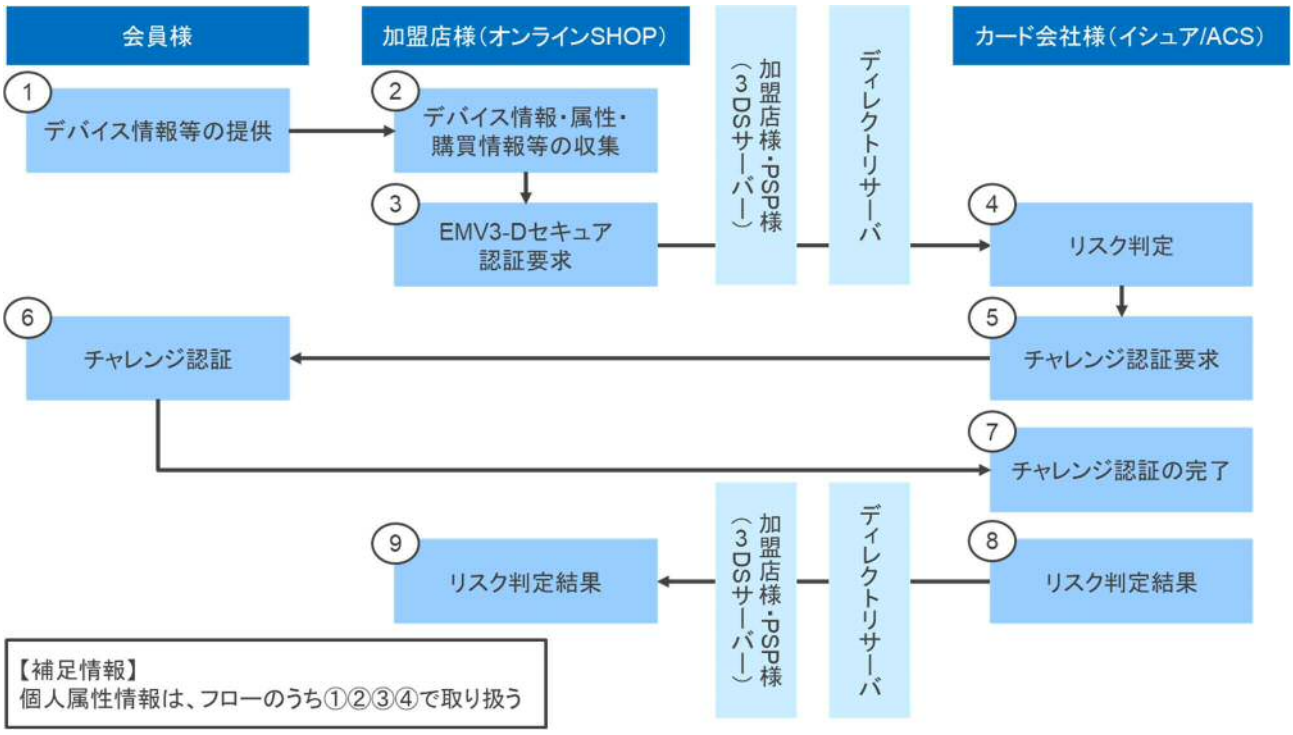
個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とした個人情報の取扱いに関連する法律。この法律では個人情報の定義を「生存する個人に関する情報であって、この情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの」と定められている。

（2）EMV 3-D セキュアにおける個人情報の取扱いにおける留意点

「EMV 3-D セキュア」の仕様において、利用できるデータ項目の中に個人情報またはそれになり得る情報が含まれる。加盟店が、個人情報取扱事業者としてそれらの項目を取り扱うためには、情報主体（カード会員）から情報取得・利用・提供にかかる同意を取得するなど、個人情報保護法などの関連する法令等を遵守することが求められている。

＜参考：EMV 3-D セキュアで利用できるデータ項目の例＞
「会員氏名」、「e メールアドレス」、「会員電話番号（自宅・携帯・勤務先）」、
「配送先住所」、「カードの請求書送付先住所」、「IP アドレス」、「デバイス情報」、「加盟店が保有している会員に関する情報」等

図 16【「EMV 3-D セキュア」の仕組みにおける情報連携フロー】



関係事業者はこの仕組みを有効に活用する一方で、利用できる情報が個人情報になり得る場合には、個人情報保護法に従った適切な取扱いを行う必要がある。

【①②③】

加盟店（オンライン SHOP）は、クレジットカード取引時に、クレジットカード会員のインターネット利用環境に関する情報等を収集し、属性情報、購買情報と共に 3DS サーバー及び DS を経由して、カード会社（イシュアー）へリスク判定要求を行う。

【④】

カード会社（イシュアー）は、加盟店（オンライン SHOP）より受け取った情報を利用して、クレジットカード取引のリスク判定を行う。

【⑤⑥⑦】

カード会社（イシュアー）は、リスク判定結果に応じ、クレジットカード会員へチャレンジ認証を行う。その要求に対して、会員が応答することで、チャレンジ認証が完了する。

【⑧⑨】

カード会社（イシュアー）は、リスク判定結果（チャレンジ認証を行った場合は、チャレンジ認証結果を含む）を加盟店に通知する。

具体的には、「EMV 3-D セキュア」の運用にかかる個人情報の取り扱いとして、EC 加盟店による利用目的の特定や制限、EC 加盟店の本人からの第三者提供の同意取得、EC 加盟店・イシュアーの確認・記録義務が論点となるが、個人情報保護法ガイドライン（第三者提供時の確認・記録義務編）の本人の委託等に基づき個人データを第三者提供する解釈を採ることにより、個人データの第三者提供の同意取得は必要であるものの、確認・記録義務は適用されないこととなる。なお、EC 加盟店の記録保存履行及びイシュアーの確認記録の履行を妨げるものではない。

図 17【個人情報保護法の内容と加盟店の対応】

該当条項	概要（要約）	協議会の見解	EC 加盟店の対応
第 27 条 第三者提供の制限	個人データを第三者に提供する場合は、原則として本人の同意を得なければならない	個人情報保護法ガイドライン（第三者提供時の確認・記録義務編）の本人の委託等に基づき個人データを第三者提供する解釈を採ることにより、個人データの同意取得は必要であるものの、確認・記録義務は適用されない	利用者の同意取得が必要
第 28 条 外国にある第三者への提供の制限	外国にある第三者に個人データを提供する場合には、原則として本人の同意を得なければならない		
第 29 条 第三者提供に係る記録の作成等	個人データを第三者へ提供したときは、提供した年月日、氏名等を記録作成しなければならない		確認・記録義務は適用されない

【解説】

- 個人情報取扱事業者が本人からの委託等に基づき当該本人の個人データを第三者に提供する場合は、当該個人情報取扱事業者は「本人に代わって」個人データの提供をしているものである。

  したがって、この場合の第三者提供については、提供者・受領者のいずれに対しても確認・記録義務は適用されない。

  個人情報取扱事業者が本人の委託等に基づいて個人データを提供しているものと評価し得るか否かは、主に、委託等の内容、提供の客体である個人データの内容、提供するとき及び提供先の個人情報取扱事業者等の要素を総合的に考慮して、本人が当該提供を具体的に特定できているか否かの観点から判断することになる。

＜参照＞個人情報の保護に関する法律についてのガイドライン（第三者提供時の確認・記録義務編）
2-2-1-1（2）「本人に代わって提供」

（3）個人データの第三者（イシュアー）提供により提供者（加盟店）へ求められる個人情報保護法上の義務と対応例

（利用者からの委託等に基づき個人データを第三者提供するという解釈を採る場合）

① 個人情報保護法上の義務（概要）

i. 「個人データを第三者に提供する」といったあらかじめの本人の同意取得（第 27 条第 1 項）

ii. 外国にある第三者（海外イシュアー）に個人データを提供する際の同意取得と情報提供（第 28 条）

② 対応例

（以下に提示する方法は例であり、各事業者にて法令の趣旨に則り対応すること）

図 18【同意取得方法例と同意文言例】 ※いずれか1つの方法にて同意取得

会員との接点	同意取得方法（例）	
加盟店サービス登録入会時、初回利用など	(1)	**【明示的同意（加盟店登録時 WEB・次工程ボタン押下）】** ・WEB 画面上に利用目的や第三者提供を表示。 ・会員は同意する場合のみ次工程に進むボタンを押下。
	(2)	**【明示的同意（加盟店登録時 WEB・チェックボックス）】** ・WEB 画面上に利用目的や第三者提供を表示。 ・会員は、同意のチェックボックスにチェックをつける。
	(3)	**【明示的同意（加盟店登録用紙・サイン）】** ・紙申込書上に利用目的や第三者提供する旨を記載。 ・会員は、当該申込用紙に同意する旨のサインをする。
利用時	(4)	**【明示的同意（加盟店利用時 WEB・次工程ボタン押下）】** ・WEB 画面上に利用目的や第三者提供を表示。 ・会員は同意する場合のみ次工程に進むボタンを押下。
	(5)	**【明示的同意（加盟店利用時 WEB・チェックボックス）】** 利用目的や第三者提供する旨の文言を都度 WEB 上に表示し、同意のチェックボックスにチェックをつける。

※なお、Web 画面のサンプルについては第 3 章（6）を参照。

なお、EC 加盟店は上記に示すほか、利用目的の特定(法第 17 条第 1 項)、利用目的の制限(法第 18 条第 1 項)に対応する必要がある。

【解説】

- 法文上、「あらかじめ」と規定されているが、その具体的な時期については限定されていない。加盟店はカード会員との接点を考慮し、当該個人データが第三者へ提供される時点より前までに同意を得ればよいとされている。また、必ずしも第三者提供のたびに同意を得なければならないわけでもない。例えば、個人情報の取得時に、その時点で予測される個人データの第三者提供について、包括的に同意を得ておくことも可能。

  <参照>個人情報の保護に関する法律についてのガイドライン 3-7-2-1「本人の同意」
  「個人情報の保護に関する法律についてのガイドライン」に関する Q＆A Q7-6 Q7-7 Q7-8

- 「本人の同意を得（る）」とは、本人の承諾する旨の意思表示を当該個人情報取扱事業者が認識することをいい、事業の性質及び個人情報の取扱状況に応じ、本人が同意にかかる判断を行うために必要と考えられる合理的かつ適切な方法によらなければならない。

<本人の同意を得ている事例（EC 加盟店に関連する事例のみ抜粋）>
・事例1）本人による同意する旨のホームページ上のボタンのクリック
・事例2）本人による同意する旨の確認欄へのチェック
・事例3）本人からの同意する旨の書面（電磁的記録含む。）の受領

<参照>個人情報の保護に関する法律についてのガイドライン（通則編）2-16「本人の同意」

図 19【同意取得文言例※】

当社がお客様から収集した以下の個人情報等は、カード発行会社が行う不正利用検知・防止のために、お客様が利用されているカード発行会社へ提供させていただきます。
氏名、電話番号、email アドレス、インターネット利用環境に関する情報　等
（加盟店の態様に応じて提供する個人情報を特定し記載ください）
お客様が利用されているカード発行会社が外国にある場合、これらの情報は当該発行会社が所属する国に移転される場合があります。当社では、お客様から収集した情報からは、ご利用のカード発行会社及び当該会社が所在する国を特定することができないため、以下の個人情報保護措置に関する情報を把握して、ご提供することはできません。
・提供先が所在する外国の名称
・当該国の個人情報保護制度に関する情報
・発行会社の個人情報保護の措置
なお、個人情報保護委員会のホームページ（https://www.ppc.go.jp/）では、各国における個人情報保護制度に関する情報について掲載されています。
お客様が未成年の場合、親権者または後見人の承諾を得た上で、本サービスを利用するものとします。

※本「同意取得文言例」は、あくまで「例」であり、最終的には個人情報取扱事業者が個人情報保護法などの関連する法令等を遵守することが求められる。

【解説】

- あらかじめ、個人情報を第三者に提供することを想定している場合には、利用目的において、その旨を特定しなければならず、利用目的の特定に当たっては、利用目的を単に抽象的、一般的に特定するのではなく、個人情報が最終的にどのような目的で利用されるのかが、本人にとって一般的かつ合理的に想定できる程度に具体的に特定することが望ましいとされている。

<具体的に利用目的を特定している事例>
事例）「〇〇事業における商品の発送、関連するアフターサービス、新商品・サービスに関する情報のお知らせのために利用いたします。」

＜参照＞個人情報の保護に関する法律についてのガイドライン（通則編）3-1-1「利用目的の特定」、3-6-1「第三者提供の制限の原則」

- 第三者提供の同意を得るに当たり、提供先を個別に明示することまでが求められるわけではない。もっとも、想定される提供先の範囲や属性を示すことは望ましいと考えられる。

  ＜参照＞「個人情報の保護に関する法律についてのガイドライン」に関する Q＆A　Q7-9

- 個人情報取扱事業者は、個人データを外国にある第三者に提供するに当たっては、法第 28 条第 1 項に従い、次の（1）から（3）までのいずれかに該当する場合を除き、あらかじめ「外国にある第三者への個人データの提供を認める旨の本人の同意」を得る必要がある。
  （1）当該第三者が、我が国と同等の水準にあると認められる個人情報保護制度を有している国として法令で定める国にあるとき。
  （2）当該第三者が、個人情報取扱事業者が講ずべき措置に相当する措置を継続的に講ずるために必要な体制として以下のいずれかの基準に適合する体制を整備しているとき。
  イ　与信事業者と個人データの提供を受ける者との間で、当該提供を受ける者における当該個人データの取扱いについて、適切かつ合理的な方法により、法第 4 章 2 節の規定の趣旨に沿った措置の実施が確保されていること。
  ロ　個人データの提供を受ける者が、個人情報の取扱いに係る国際的な枠組みに基づく認定を受けていること。
  （3）法第27条に該当するとき。

  ＜参照＞個人情報保護法ガイドライン（外国第三者提供編）2．総論

- 法第 28 条において求められる本人の同意を取得しようとする場合には、本人に対して（1）当該外国の名称（2）当該外国における個人情報に関する制度に関する情報（3）当該第三者が講ずる個人情報保護のための措置に関する情報を提供しなければならない。また、同意取得時に、提供先の第三者が所在する外国を特定できない場合には、（1）（2）に代えて①特定できない旨及びその理由②提供先の第三者が所在する外国の名称に代わる本人に参考となるべき情報を、（3）に代えて③提供できない旨及びその理由について情報提供しなければならない。

  ＜参照＞個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）5-2「提供すべき情報」5-3「同意取得時に移転先が特定できない場合等の取扱い」

- 未成年者等、個人情報の取扱いに関して同意したことによって生ずる結果について判断できる能力を有していないなどの場合は、親権者や法定代理人等から同意を得る必要がある。

  ＜参照＞個人情報の保護に関する法律についてのガイドライン（通則編）2-16「本人の同意」

５．カード発行会社（イシュアー）に対する推奨事項

5. カード発行会社（イシュアー）に対する推奨事項

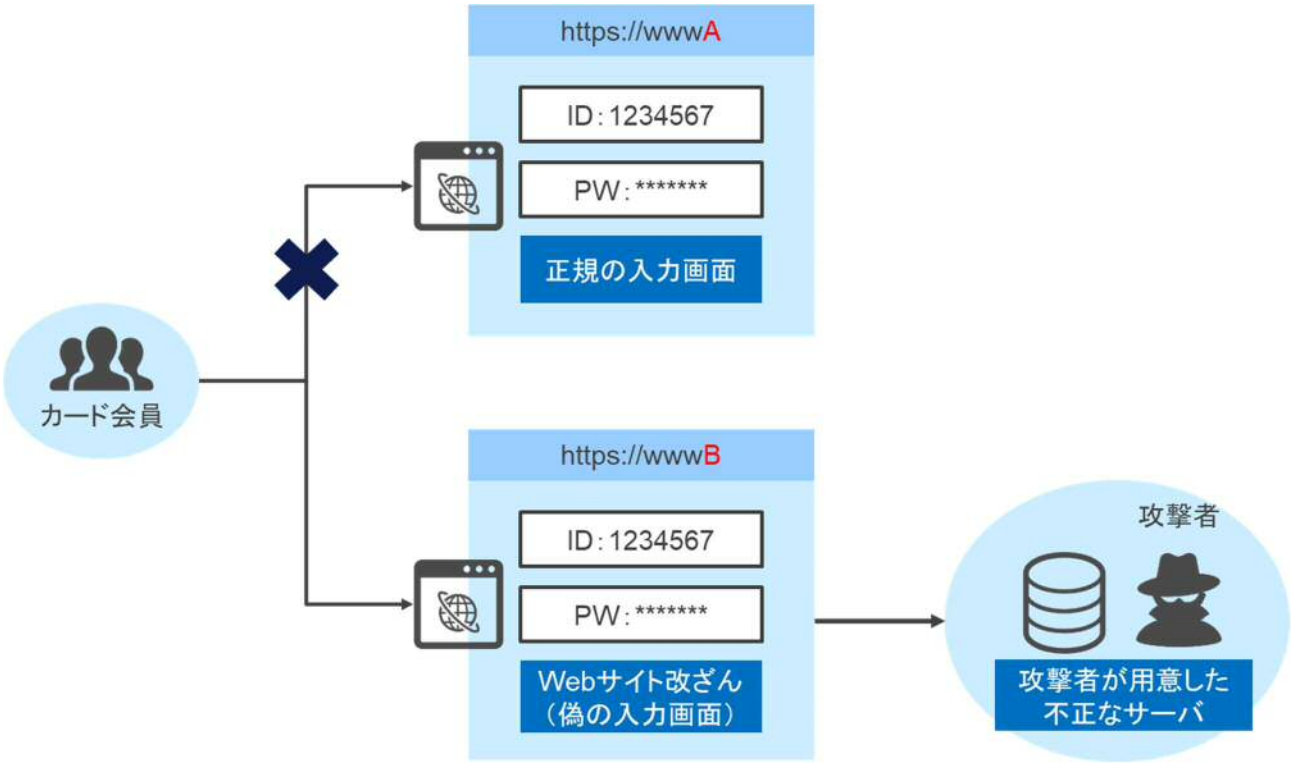
EMV 3-D セキュアを導入する加盟店のセキュリティ対策もさることながら、近年では、カード会員様が自らフィッシングサイトに誘導されてカード会員データが漏洩する事案も多発している為、イシュアーにおいても注意喚起を促し自社のホームページを活用、カード会員に対して周知・啓発の徹底を取り組んでいくことが求められる。

（1）利用者向け説明事項

EMV 3-D セキュアでは、リスクが高いと思われる場合以外では、リスクベース認証で本人認証を行うため、EC 加盟店に個人情報を利用される事の同意をすれば、ID とパスワードによる本人認証は実施されない。

リスクが高いと思われる場合には、チャレンジ認証（パスワード認証など）を実施する必要があり、ID とパスワードを入力する為のフォーム画面が転送される。この入力フォームは特定の URL 以外からは転送されない。URL を確認して特定の URL ではないフォーム画面での ID とパスワードの入力は漏洩リスクが伴うため、利用者に注意を促す必要がある。

図 20【チャレンジ認証に伴う偽の入力画面】



（2）利用者への周知（チャレンジ画面の URL）

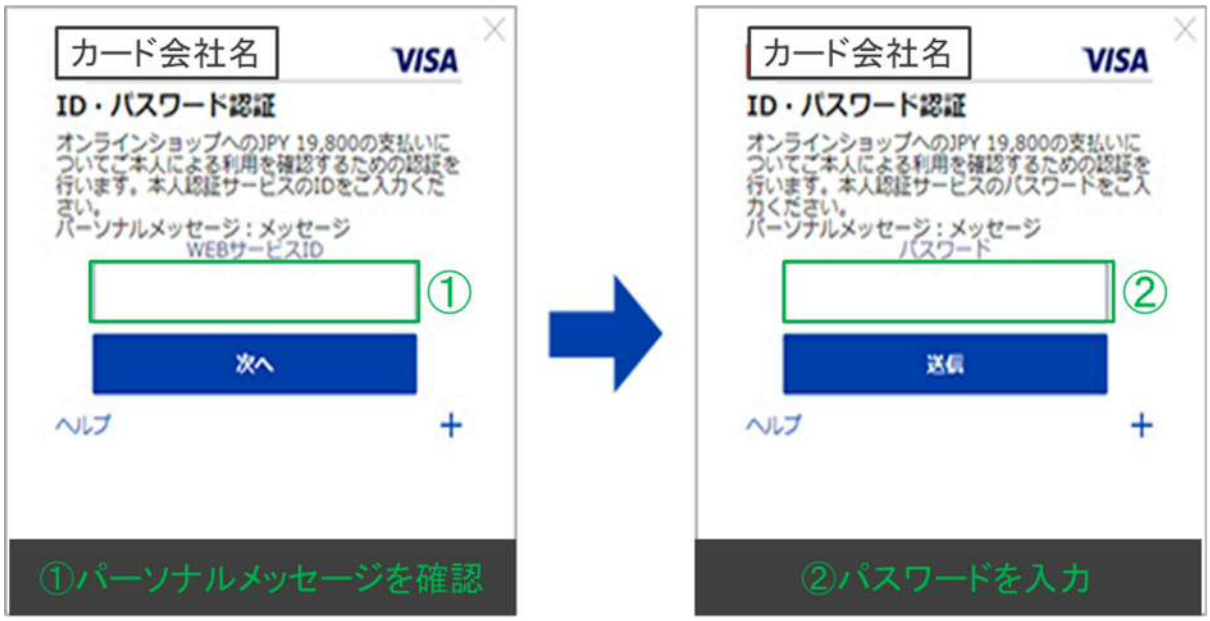
カード会員には、クレジットカード決済時にリスク判定を行う ACS（本人認証システム）から発行される図 21 のチャレンジ認証の画面以外では、ID とパスワードの入力は控える周知が必要となる。但し、チャレンジ認証の画面を公開する事で模倣されるなどのリスクも残存する為、各イシュアーのポリシーのもとカードホルダーに対してフィッシング対策の注意啓発が必要。

例）カード会社（イシュアー）は、カード会員に対し、以下の周知が必要である。

① フィッシング対策の注意喚起

② パスワード不知会員、動的パスワード用アプリ不具合時の告知

図 21【チャレンジ認証画面サンプル】



（3） 各国際ブランドの3-D セキュアのサービス名称

協議会としては、「3-D セキュア/EMV 3-D セキュア」を正式名称として各種案内をしているが、国際ブランドでは以下の通り、個々のサービス名称で呼ばれている。また、パスワード認証時に遷移された画面において、カード会社（イシュアー）は、各国際ブランドのサービスロゴを記載する必要がある。

図 22【各国際ブランドの3-D セキュアのサービス名称】

	サービス名称	サービスロゴ
Visa	Visa Secure	
Mastercard	Mastercard ID Check	
JCB	J/Secure	
AMEX	American Express SafeKey	
Diners (Discover)[12]	ProtectBuy	
UnionPay International (銀聯国際)	UnionPay 3-D Secure	

(4) 全件パスワード認証を行う加盟店等からの認証要求について

デジタルウォレットへのクレジットカードの登録等、一部の認証取引においては、チャレンジ認証による本人確認を必須としたいという加盟店/PSP のニーズがある。

このような加盟店からの認証要求時(AReq)に「3DS Requestor Challenge Indicator」に"03"もしくは"04"の値が設定される場合があるが、特に"04"が設定されている場合は加盟店による強い要望であることを考慮し、当該カードが EMV 3-D セキュア未登録の場合において、イシュアーとしては国際ブランドの規定も確認しつつ、当該取引の不正リスクを十分に検証のうえ判定することが望ましい。

「3DS Requestor Challenge Indicator」の使い分けの例は以下の通り。

✓ 03:イシュアーにチャレンジを求める

✓ 04:イシュアーに必ずチャレンジを求める

※詳細については 24 ページ下段＜当該カードが EMV 3-D セキュア未登録の場合＞を参照

[12] Discover は Diners の 3-D セキュアサービスを利用している。(2022 年 2 月現在)

（5） App ベースの不正利用対策

EMV 3-D セキュアは、3-D セキュア 1.0 の課題であった、「スマートフォンやタブレットのアプリ内決済への対応（App ベース）」の認証プロトコルをサポートしており、App ベースに対応した取引が発生している。

これらの App ベースの取引については、加盟店/PSP が、3DS サーバー事業者が提供する 3DS SDK をアプリに実装することで実現しており、App ベースのリスクベース認証は、3DS SDK が取得を行ったデバイス情報を利用している。一方でブラウザベースの取引は、加盟店/PSP が 3DS Method を実行した際に、ACS（イシュアー）が取得を行ったデバイス情報を利用している。

従って、App ベースで 3DS SDK が取得するデバイス情報は、ブラウザベースで ACS（イシュアー）が取得するデバイス情報と異なるものになる可能性があることに留意し、リスクベース認証の設定などの不正利用対策を実施する必要がある。

6. EMV 3-D セキュアの安定した運用と認証精度の向上に関する推奨事項

6. EMV 3-D セキュアの安定した運用と認証精度の向上に関する推奨事項

（1）加盟店/PSP

① 加盟店が設定する AReq データの設定に関するベストプラクティス

設定するデータ項目の数が多いこと、一貫性があること、正確性が高いことは、ACS における認証精度向上に寄与し、不正取引の削減と不要なチャレンジ認証を削減することに繋がり、フリクションレス率の向上に貢献する。

特に重要なデータ項目について、設定に関するベストプラクティスを以下のとおり記載する。

✓ Merchant ID

ACS が認証時に加盟店を識別するために使用するデータ。

原則として極力店舗単位で設定すべきものであり、不正顕在化加盟店や高リスク商材取扱加盟店などは優先的に正しく設定することが好ましい。

2023 年 9 月 30 日までを試行期間と位置づけ、 2023 年 10 月より店舗単位で設定した運用となることを、業界共通の目標とする。

また、将来的には 3DS で加盟店が設定する Merchant ID と、売上データに設定する加盟店番号を同一にすることが好ましい。

✓ Merchant Name

Merchant ID とともに ACS が認証時に加盟店を識別するために使用するデータ。

店舗単位に設定することが求められる。

設定においては他の加盟店と識別可能となるように極力固有の店名を設定すること。

✓ Merchant Category Code (MCC)

加盟店の業種や取扱商品を判断するために使用するデータ。店舗単位で設定できることとし、不正顕在化加盟店や高リスク商材取扱加盟店などは優先的に正しく設定することが好ましい。

2023 年 9 月 30 日までを試行期間と位置づけ、 2023 年 10 月より店舗単位で設定した運用となることを、業界共通の目標とする。

（具体的な設定値は本書別紙「【EMV 3-D セキュア】統合版__Areq 設定項目（公表版） 」 参照）

✓ 条件付き必須項目・オプション項目の活用

以下のデータ項目は設定が必須ではないが、ACS でのリスク判定に有効な項目と考えられる。

設定が可能である場合、特に不正顕在化時および高リスク商材取扱加盟店においては、当事者間（アクワイアラー、PSP、加盟店）で当該項目の使用を検討することが好ましい。具体的な項目は、本書別紙「【EMV 3-D セキュア】統合版__AReq 設定項目（公表版）」を活用する。

（2）アクワイアラー

将来的には EMV 3-D セキュアで加盟店が設定する Merchant ID と、アクワイアラーがオーソリ・クリアリングを国際ブランドのネットワークへ中継する際の Merchant ID を同一にすることが好ましい。

・不正顕在化加盟店や高リスク商材取扱加盟店などにおいて更なる不正対策強化が必要な場合については、アクワイアラーが起点となり、契約先の加盟店及び包括先の場合は PSP と調整のうえ、オプション項目の活用することが望ましい。

その際には、本書別紙「【EMV 3-D セキュア】統合版__AReq 設定項目（公表版）」を活用する。

（3）イシュアー

① リスクベース認証におけるルール設定等の最適化

日々変動する悪用者の攻撃手口に対応する必要があるため、ACS ベンダーと連携して認証精度の分析および適宜リスクベース認証ルール設定等の最適化を行う必要がある。

3DS Method は、ACS（イシュアー）が 3DS クライアント（カードホルダー）の利用デバイス情報を取得し、リスクベース認証をより効果的に実行することができる方法であり、リスクベース認証の精度向上が期待される。

② フリクションレス率の向上

加盟店でのカゴ落ちリスクを低減するために、リスクベース認証ルール設定等の最適化により継続的にフリクションレス率の向上に努める。（85 %以上を目標とする）

③ EMV 3-D セキュア未登録会員の削減

リスクベース認証だけでは不正取引の検知に限界もあるため、中リスク時にチャレンジすることができないことによる不正取引の対策として早期に動的パスワードの導入やカード会員への啓発を行う。但し、静的パスワードを使用している期間は、継続的な会員への啓発等によりパスワード登録を促進する。

④ 静的パスワード以外の認証方法への移行

EMV 3-D セキュア登録済み会員のパスワードは使い回しされている事が多く、情報漏洩およびフィッシングにより ID/パスワードが漏洩した場合には、第三者によるなりすましにより、チャレンジ認証時のパスワードが認証されてしまうおそれがある。その為、完全認証時のなりすましによる不正の対策としては、静的パスワードから動的パスワード（もしくは生体認証等）等への切り替えを行うべきである。

7. EMV 3-D セキュア導入に関する FAQ

7. EMV 3-D セキュア導入に関する FAQ

	よくあるご質問	回答
1	イシュアーによって推奨ブラウザ（使用不可ブラウザ）が定義されているのか。	各 ACS が推奨環境を規定しており、一般的に利用されるブラウザはサポートされているが、詳細情報は公開されていない。
2	不正顕在化加盟店になった加盟店に対して、Merchant ID、MCC の変更及び、AReq オプション項目の設定、個人情報属性の同意画面の確認などの周知は、どこがやるのか	アクワイアラーが起点となり、直接契約先の加盟店及び、包括先の場合は PSP に要請を行う。
3	PA と NPA の違い或いは、利用する際の注意点などはあるか。	PA と NPA の違いは当導入ガイドの第 3 章（2）の記載を参照いただきたい。 留意事項として、クレジットカード登録時の認証においては、不正取引も頻繁に発生していることから NPA ではなく、PA を使用して後続のオーソリゼーションも実施する必要がある。

8. 改訂履歴

8. 改訂履歴

2022 年 9 月 16 日　1.1 版改訂箇所

3 章(4)②＜当該カードが EMV 3-D セキュア未登録の場合＞を追記

5 章(4)「全件パスワード認証を行う加盟店等からの認証要求について」を追記

5 章(5)「App ベースの不正利用対策」を追記

2023 年 1 月 31 日　1.2 版改訂箇所

3-D セキュア 1.0 の終了に伴い、3-D セキュア 1.0 に関する記述を削除

4 章「EMV 3-D セキュア導入加盟店における個人情報保護法の遵守に関する留意点」を改訂

6 章「EMV 3-D セキュアの安定した運用と認証精度の向上に関する推奨事項」を新たに作成