附属文書 14

EMV 3-D セキュア導入ガイド

2.0 版

クレジット取引セキュリティ対策協議会

2025 年 3 月

内容

0.はじめに 3
1.EMV 3-D セキュアの概要 5
（1）　3-D セキュアとは 5
（2）　EMV 3-D セキュアとは（3-D セキュア 1.0 との比較） 5
（3）　EMV 3-D セキュアのバージョンについて 5
（4）　リスクベース認証とは 6
①フリクションレスフローとチャレンジフロー 7
（5）　EMV 3-D セキュアの不正リスク負担について 8
（6）　各国際ブランドの EMV 3-D セキュアのサービス名称 8
（7）　EMV 3-D セキュア処理フロー概要 9
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） 10
②各プレイヤーの説明 12
③3RI（3DS Requester Initiated）について 13
2.EMV 3-D セキュア導入について各事業者に求められる対応 19
（1）　カード会社（イシュアー） 19
（2）　カード会社（アクワイアラー）・PSP 19
（3）　加盟店 19
①EMV 3-D セキュアの導入 19
②EMV 3-D セキュアの運用 21
3.導入手続きについて 26
（1）　加盟店の導入形態について 26
①自社構築（カード会社直接契約加盟店、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 27
②PSP の業務代行（カード会社直接契約加盟店）の場合 29
③PSP のサービス利用（包括代理契約加盟店）の場合 30
（2）　本番確認 31
（3）　その他 31
①EC サイト構築における留意事項 31
②EMV 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 31
4.システム開発要件（開発者向け） 33
（1）　AReq 設定項目 33
（2）　PA(Payment Authentication）と NPA(Non–Payment Authentication）の実装方法 33
（3）　3DS Requestor Authentication Indicator の実装方法 33
（4）　全件チャレンジ認証を行う場合の実装方法 34
①PA（Payment Authentication） 34

②NPA（Non-Payment Authentication） 34
③当該カードが EMV 3-D セキュア未登録の場合 34
（5） オーソリゼーションへの項目設定 35
（6） 個人情報の同意画面の作成内容について 36
（7） 3DS Method について 36
（8） 3RI について 37
5.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 40
（1） 個人情報保護法とは 40
（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 40
（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 42
①個人情報保護法上の義務（概要） 42
②対応例 43
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 47
（1） EMV 3-D セキュアの安定稼働と障害発生時等の対応について 47
①障害等発生防止に向けたシステムのキャパシティ確保と安定稼働に向けた対応強化 47
②障害等発生時の対応と情報連携 47
③障害等発生時の取引と不正利用対策 47
（2） 認証精度の向上に関する推奨事項 48
①加盟店/PSP 48
②カード会社（アクワイアラー） 49
③カード会社（イシュアー） 49
7.改訂履歴 52

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。

クレジット取引セキュリティ対策協議会（以下「協議会」という）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」という）6.0 版では、EC 加盟店における不正利用対策の指針対策の 1 つとして、「EMV 3-D セキュアの導入」を掲げている。

EMV 3-D セキュアは、カード会員のデバイス情報等を用いて「なりすまし」による不正利用のリスク判断を行うとともに、本人確認が必要な取引と判断した場合は、動的（ワンタイム）パスワードの入力等を要求することにより、当該取引がカード発行会員本人によるものかを確認する仕組みである。

また、カード会社（イシュアー）は、EC 加盟店における円滑な取引や不正利用の抑止等のために、自社カード会員の EMV 3-D セキュアの登録を行うとともに動的（ワンタイム）パスワードの入力又は生体認証等を求めるチャレンジフローが行われるようカード会員への周知・啓発、携帯電話番号等の登録情報の最新化、さらにリスクベース認証（RBA）による「なりすまし」のリスク判定の精度向上を常に行うことが求められる。

このことから、「EMV 3-D セキュア導入ガイド」を作成し、EC 加盟店やカード会社（イシュアー）等のすべての関係事業者の共通ガイドとして EMV 3-D セキュアの円滑な導入・運用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、不正対応・処理の実務担当者
（以降本書で「加盟店」という。非対面取引の定義は「セキュリティガイドライン 6.0 版」20 ページを参照）
・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、 加盟店における非対面不正利用防止のための本人認証手法の一つ。

利用者がカード会員本人であることを確認する仕組みであり、カード会員に本人のみが知る情報を入力させることなどにより、本人認証を行う。

3-D セキュアの国際ブランド毎の正式名称が異なるため、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、過去の 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る。

各カード会社（イシュアー）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ともに、必要に応じて動的（ワンタイム）パスワード入力等を要求することで当該取引における安全性を確保する。

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。

・リスクベース認証（詳細は後述）により、低リスクと判断された場合、会員は動的（ワンタイム）パスワードの入力等をすることなく認証が完了。
・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。
・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。

(3) EMV 3-D セキュアのバージョンについて

EMV 3-D セキュアは、EMVCo からバージョン 2.1、バージョン 2.2、バージョン 2.3 の仕様がこれまでに公開されている。

バージョン 2.1 では、上記のような機能がサポートされ、バージョン 2.2 では本章（7）及び第 4 章に記述している 3RI などの新機能が追加された。また、バージョン 2.3 においては、IoT 機器やスマートスピーカーにも対応ができるなどの特徴がある。

なお、バージョン 2.1 は既にサポートが終了となった。

---

[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 セキュアの特徴】

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） ・中リスク判定時に動的（ワンタイム）パスワード等による認証を行う（「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	UI/UX の改善		ブラウザ取引のみ推奨
非決済分野への対応	・デジタ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	認証機能の活用範囲拡大		決済分野のみ対応

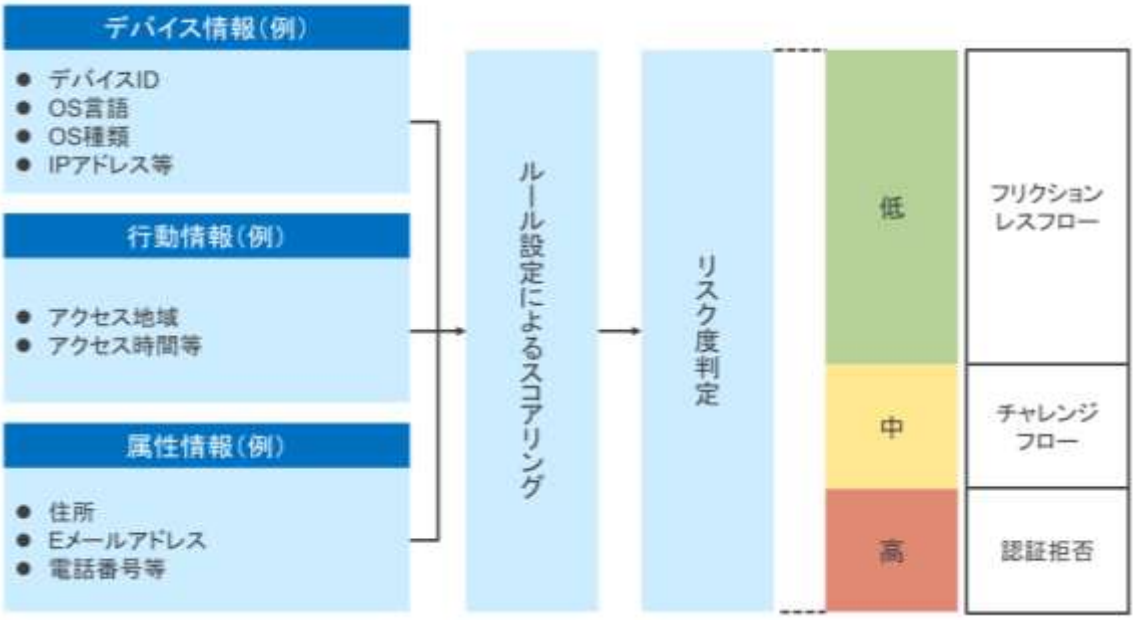
（4） リスクベース認証とは

リスクベース認証とは、EMV 3-D セキュアにおいて、利用者が決済に使用するデバイスの設定情報や利用者から提供される個人情報等の様々なデータを活用して本人の利用であるかを確認し認証する仕組みであり、カード会社（イシュアー）が当該取引におけるリスク度合いを評価する。

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パスワードの入力等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動的（ワンタイム）パスワードの入力等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動的（ワンタイム）パスワードの入力等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（動的（ワンタイム）パスワードの入力等）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】

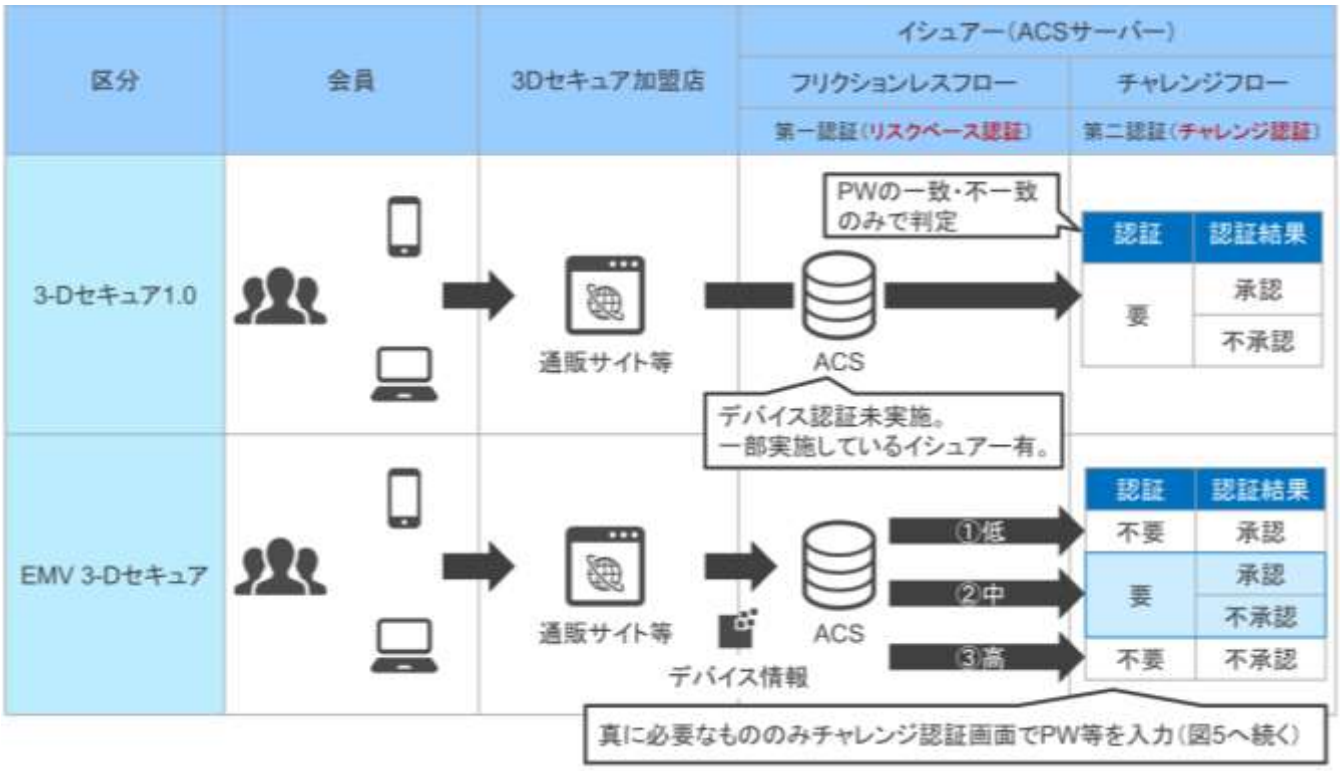


図 4 【チャレンジ認証画面】[3]

（サンプル）

（5） EMV 3-D セキュアの不正リスク負担について

EMV 3-D セキュアによる認証を行った取引のうち、認証成功/カード会社（イシュアー）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	加盟店は免責対象外

※2025 年 3 月現在

※図 5 のリスク負担の詳細は契約のカード会社（アクワイアラー）等への確認が必要。

（6） 各国際ブランドの EMV 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。

---

[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。

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	
American Express	American Express SafeKey	
Diners	ProtectBuy[5]	
Discover		
UnionPay International（銀聯国際）	UnionPay 3-D Secure	

(7) EMV 3-D セキュア処理フロー概要

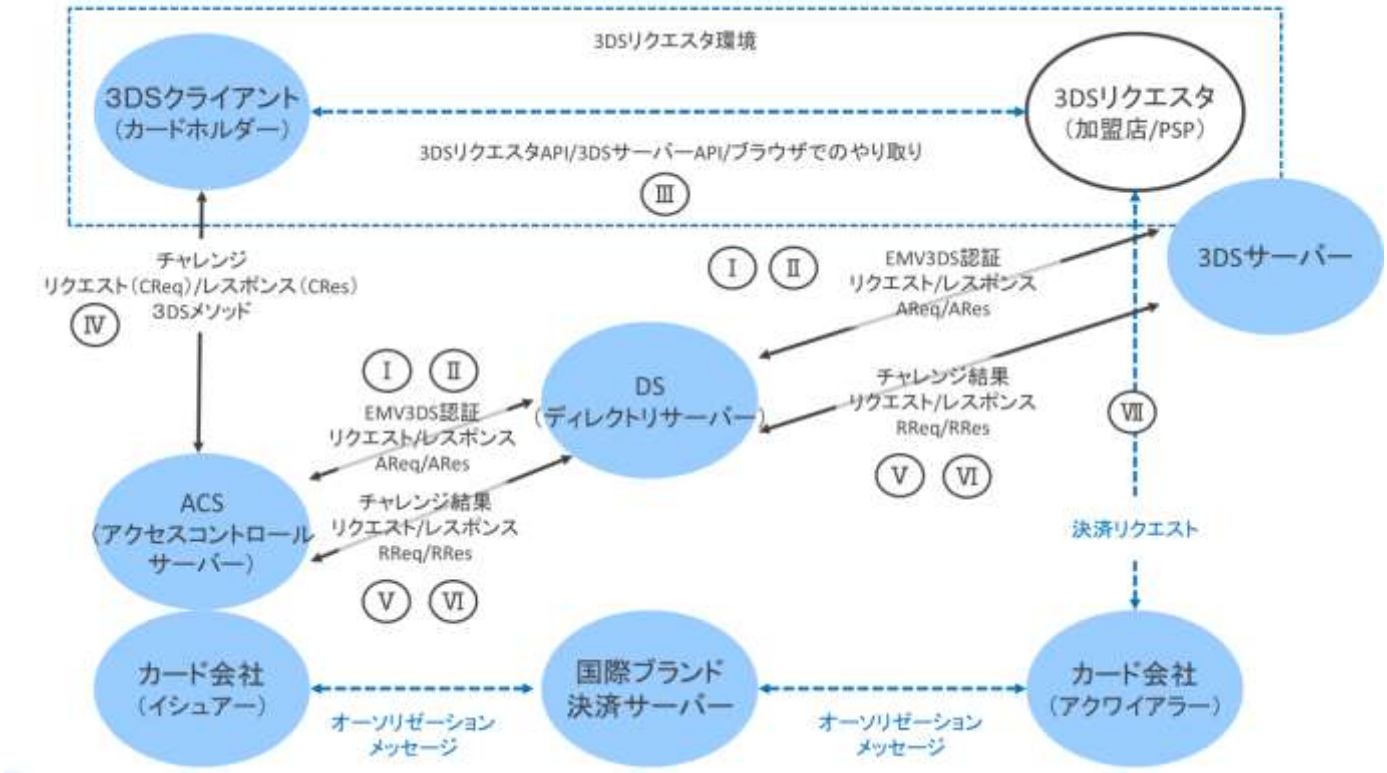
EMV 3-D セキュアは、加盟店や PSP から本人認証に必要な情報をカード会社（イシュアー）へ送信することで、カード会社（イシュアー）が当該取引の不正利用のリスク判断を行う。

主に ACS（Access Control Server）、DS（Directory Server）、3-D セキュア Server（以下「3DS サーバー」という）の 3 つの仕組みから構成され、ACS はカード会社(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、不正の低減を行う。

[5] Discover Global Network ProtectBuy は Discover と Diners Club、およびその他のネットワークアライアンスをサポートしている。

[6] Discover もしくは Diners いずれかのみ取扱いの場合に使用される。

図 7 【EMV 3-D セキュア全体図】[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 は該当するカード会社(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カード会社(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。 処理フローに進む前に、3DS サーバーと ACS 間で P 電文（PRes 電文、PReq 電文）を通して、ACS にサポートされている EMV 3-D セキュアのバージョン情報をキャッシュする必要がある。

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 もしくは 07[8]	送信可能
アテンプト（カード会社(イシュアー)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[9]; Transaction denied	N	－	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	－ 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] Mastercard では加盟店側の操作（3RI）による取引の場合、ECI の返却値は「07」となる。

[9] Account Not Verified は、カード会社（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

・ACS：カード会社（イシュアー）が運営する認証サーバー

【概要】

ACS はカード会社（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。利用者が決済に使用するデバイスの設定情報や利用者から提供される個人情報等の様々なデータを利用し、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[10]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：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[11]（3DS の認証要求を行う加盟店や PSP）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。

---

[10] ACS が取得した、利用者が決済に使用するデバイスの設定情報や利用者から提供される個人情報等の様々なデータ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動的（ワンタイム）パスワードの入力等なしに認証が完結）

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（動的（ワンタイム）パスワードの入力等）を要求する）

[11] 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。

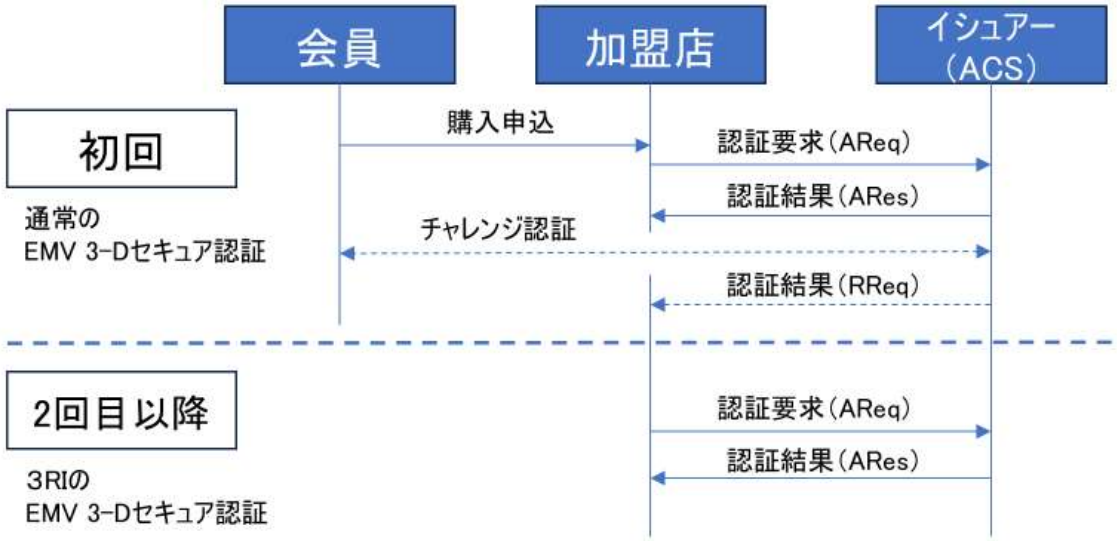
③ 3RI（3DS Requester Initiated）について

3RI はカード会員が取引に介在しない MIT（Merchant Initiated Transaction）でも EMV 3-D セキュアが利用できる手法であり、分割配送、配送遅延など 1 度の取引に対して複数回オーソリゼーションが必要となるケースにおいても EMV 3-D セキュアが利用可能となる。

3RI を利用するユースケースにおいては初回の取引時に通常の EMV 3-D セキュア認証を行なうが、2 回目以降のオーソリゼーション時にはカード会員が不在であるため、3DS リクエスタ（加盟店）が起点となり 3RI による認証要求が行われることで初回の取引時に獲得した不正リスクの免責を維持することができる。

3RI のオプションである Decoupled Authentication という認証手法は加盟店とカード会社（イシュアー）が対応している場合に限り 3RI の認証フローが一旦終わってから、カード会社（イシュアー）がカード会員と連絡して追加認証（チャレンジ）を行う認証方法であるが、現時点では対応しているカード会社（イシュアー）は少なく、カード会社（アクワイアラー）においてもオーソリ電文への影響が発生するため実施にあたっては留意が必要である。

図 9 【3RI 処理フローのイメージ】



・カード会社（イシュアー）における留意事項

3RI は通常の EMV 3-D セキュア認証とは異なり、3DS リクエスタ（加盟店環境）が認証処理の起点となるためカード会員のデバイス関連情報は送信できない等の制約がある。

ACS として機能はサポートされているものの、RBA 判定等のルール設定はカード会社（イシュアー）の判断により行われる必要があるため、カード会社（イシュアー）は加盟店から 3RI による認証要求が求められることを想定し、以下の事項について留意しつつ対応する必要がある。

I. 3RI の認証で考慮すべき AReq データ項目

- Device Channel：**当該取引がブラウザベース、APP ベース、3RI、であるかを識別する情報**（「03」が 3RI の認証要求であることを示す）
- 3RI Indicator：**当該取引の 3RI ユースケース（後述）の種類を示す情報**

- 3DS Requestor Prior Transaction Authentication Information： **前回の認証に関する情報（チャレンジ有無、タイムスタンプ、**ACS Transaction ID **など）**

II. 3RI の認証では使用されない AReq データ項目

利用者の環境から得られる情報は使用できないため、以下のデータは設定されない。

Browser Accept Headers, Browser JavaScript Enabled, Browser Language, Browser User-Agent, Browser IP Address, Browser Java Enabled, Browser Screen Color Depth, Browser Screen Height, Browser Screen Width, Browser Time Zone など

III. RBA 等のリスク判定において 2 回目以降の取引についてはチャレンジ要求（Transaction Status="C"）ができない。

IV. 初回の取引時に認証成功していることを考慮する。

データ項目が少ない、チャレンジ認証できないという制約があるものの、カード会社（イシュアー）は既に認証成功した取引に後続した取引であることを考慮したリスク判定を行う必要がある。

・ユースケースと加盟店における留意事項

3RI がサポートされるユースケースは国際ブランドによって異なるため、最新の情報については各国際ブランドへの確認が必要となるが、現時点において全ての国際ブランド共通で使用できるユースケースは「分割配送」と「配送遅延」である。

「リカーリング」については国際ブランドによって使用できる取引が具体的に制限されているため留意が必要である。

現時点における具体的なユースケースの詳細については本書別紙「【EMV 3-D セキュア】統合版_AReq 設定項目及び 3RI の仕様・ユースケース」（以下「別紙_統合版_AReq 設定項目」という）及び、各国際ブランドの仕様を参照すること。

また、3RI は運用が開始されてから日が浅いこともあり、加盟店における実装にあたっては仕様やユースケース、および国際ブランドのルールなどについて変更が生じる可能性があることと、カード会社（イシュアー・アクワイアラー）・PSP のサポートが過渡期であることを認識し、予め十分に調整を行う必要がある。

3RI は加盟店起点の取引であるため、ユースケースによってはバッチ処理による大量の認証要求を連続して送信する運用も想定されるが、DS・ACS の処理性能には限界があるため、そのようなケースにおいては処理を行う時間帯や処理量について考慮するべきである。

図 10 【用語集】

用語	用語説明
AReq（Authentication Request Message） 認証リクエスト電文	EMV 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。電文には利用者が決済に使用するデバイスの設定情報や利用者から提供される個人情報等の様々なデータを含める事が出来る。
ARes （Authentication Response Message） 認証レスポンス電文	ARes 電文はカード会社（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 3DS 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）	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機能。 例えば、商品の配送分割や配送遅延の場面で利用することができる。

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。動的パスワードの入力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。
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（7）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（7）EMV 3-D セキュア処理フロー概要を参照

用語	用語説明
PReq（Preparation Request Message） EMV 3-D セキュア対応有無確認電文	PReq 電文は、3DS サーバーから DS サーバーを通して ACS に対して、EMV 3-D セキュアによる処理フローに入る前にやり取りが行われる。 3DS サーバーが、EMV 3-D セキュアへの対応の有無や EMV 3-D セキュアのバージョン情報を ACS から取得するための電文。
PRes（Preparation Response Message） EMV 3-D セキュア対応有無結果電文	PRes 電文は、ACS から DS サーバーを通して 3DS サーバーに対して、PReq 電文の結果を伝達する。
動的（ワンタイム）パスワード	利用する都度変更される使い捨てパスワード。

2.　EMV 3-D セキュア導入について

各事業者に求められる対応

2. EMV 3-D セキュア導入について各事業者に求められる対応

クレジットカード・セキュリティガイドラインでは関係事業者に対し EMV 3-D セキュアの導入を求めている。各事業者に対して求められる対応は以下のとおり。

(1) カード会社（イシュアー）

カード会社（イシュアー）は以下の対応が求められる。

①発行カードの EMV 3-D セキュアの導入

自社カード会員の EMV 3-D セキュアの登録を行う。また、登録にあたりチャレンジフローにおける追加認証方法は動的（ワンタイム）パスワード等の「静的（固定）パスワード」以外の認証方法とする。

②リスクベース認証（RBA）の精度向上

自社カード会員取引のリスク度合いを適切に判定するために、データ処理能力の向上や認証精度の分析及びルール設定等の最適化を常に行い、リスクベース認証の精度向上に継続的に取組むことが求められる。

③動的（ワンタイム）パスワード等の送付先の登録情報の最新化

自社カード会員に対して、EMV 3-D セキュアを導入した加盟店から決済時に「動的（ワンタイム）パスワード」の入力等を要求されることがあることの周知・啓発を行う。

また、カード会員に「動的（ワンタイム）パスワード等」が確実に届くために、携帯電話番号やメールアドレス等のカード会員情報が常に最新化されていることが求められる。

(2) カード会社（アクワイアラー）・PSP

カード会社（アクワイアラー）と PSP は連携し、加盟店が適切に EMV 3-D セキュアの導入及び運用を行えるようサポートする。

(3) 加盟店

以下については、関係事業者向けに 2024 年 5 月に公開した「加盟店における導入・運用ガイダンス関係者版 1.1 版」の内容を再掲するものである。

本書別紙の FAQ（EMV 3-D セキュア導入ガイド【附属文書 14】に関する FAQ ）も併せて参照されたい。

① EMV 3-D セキュアの導入

カード会社（イシュアー）による本人確認が適切に行われるための措置として、加盟店は EMV 3-D セキュアを導入することが求められる。

なお、EMV 3-D セキュアの未導入が認められる取引は以下のとおり。

（1） EMV 3-D セキュアの導入が技術的にできないもの
（2） システムにより特定の者とのみ取引可能な措置が講じられており、なりすましによる不正が発生する蓋然性が極めて低いもの
（3） 取引対象となる本人が特定されており、なりすましによる不正が発生する蓋然性が極めて低いもの

・取引具体例は図 11 に示す。

【留意事項】　（但し、上記（１）のケースを除く）

EMV 3-D セキュアの未導入が認められる取引であっても、不正顕在化加盟店（3 ヵ月連続 50 万円超）となった場合には、EMV 3-D セキュアの導入が必要。

また、不正利用の発生状況からカード会社（アクワイアラー）・PSP が対策の緊急性が高いと判断した場合には、加盟店に対して EMV 3-D セキュアの導入を要請し、加盟店は EMV 3-D セキュアの導入を行う。

図 11 【EMV 3-D セキュアの未導入が認められる取引（導入の対象外）】

要件	取引具体例
（１）EMV 3-D セキュアの導入が技術的にできないもの(赤枠の【留意事項】については対応不要)	電話・FAX・郵便によりクレジットカード番号の通知を受ける取引（いわゆるメールオーダー、テレフォンオーダー取引）
	ゲーム機・スマートスピーカー等の EMV 3-D セキュアが利用できない機器での EC 取引
（２）システムにより特定の者とのみ取引可能な措置が講じられており、なりすましによる不正が発生する蓋然性が極めて低いもの	個人事業主または法人が契約主体のクレジットカードに限定したサイトでの BtoB 取引 （事業者購買専用サイト、法人間取引専用サイト、宿泊代金精算用の法人契約カード取引等）
	イントラネット環境、IP アドレス等による外部からの通信制限によって利用者を特定することにより、不特定多数の者が利用できない取引（従業員専用サイトでの取引、販売代理店専用サイトでの取引等）
（３）取引対象となる本人が特定されており、なりすましによる不正が発生する蓋然性が極めて低いもの	・公共料金（電気、ガス、水道、固定電話） ・国や自治体の請求に基づいて納付する税金・料金・手数料 ・保険料、共済掛金 ・学校教育費（学校教育法で定める「学校」「専修学校」「各種学校」が対象）

【留意事項】
EMV 3-D セキュアの未導入が認められる取引であっても、不正顕在化加盟店（3 ヵ月連続 50 万円超）となった場合には、EMV 3-D セキュアの導入が必要。
また、不正利用の発生状況からカード会社（アクワイアラー）・PSP が対策の緊急性が高いと判断した場合には、加盟店に対して EMV 3-D セキュアの導入を要請し、加盟店は EMV 3-D セキュアの導入を行う。

② EMV 3-D セキュアの運用

加盟店は、EMV 3-D セキュアを導入した上で、原則としては決済の都度、EMV 3-D セキュアによる認証を行うことが求められるが、加盟店が EMV 3-D セキュア以外に講じる不正利用対策の内容や抑止効果に応じて、カード番号の登録時に EMV 3-D セキュアによる認証を行う運用や加盟店のリスク判断により EMV 3-D セキュアによる認証を行う運用も認められる。

EMV 3-D セキュアを導入する加盟店における具体的な運用については以下のとおり。

図 12 【EMV 3-D セキュアの具体的な運用】

<table>
<tr><th colspan="2" rowspan="2">パターン</th><th colspan="2">EMV 3-D セキュアの具体的な運用</th></tr>
<tr><th>カード番号
登録時</th><th>決済の都度</th></tr>
<tr><td>①</td><td>加盟店のリスク判断により EMV 3-D セキュアによる
認証を行う場合</td><td colspan="2">加盟店が網羅的に行う不正利用対策が、EMV 3-D セキュアと同等以上の不正抑止効果があることを前提として、加盟店の不正リスク判断によって必要な場合に EMV 3-D セキュアによる認証を行う。</td></tr>
<tr><td rowspan="2">②</td><td rowspan="2">カード番号登録時に EMV 3-D セキュアによる認証を行う場合</td><td colspan="2">アカウント等の厳格な管理及び不正ログイン対策を講じた上で、
ログインが行われる際にアカウント等の利用者であることの確認を行う。</td></tr>
<tr><td>EMV 3-D セキュアによる認証を行う。</td><td>加盟店の不正リスク判断によって必要な場合に EMV 3-D セキュアによる認証を行う。</td></tr>
<tr><td>③</td><td>決済の都度、
EMV 3-D セキュアによる認証を行う場合</td><td>EMV 3-D セキュアによる認証を行うことを推奨する。</td><td>EMV 3-D セキュアによる認証を行う。</td></tr>
<tr><td>-</td><td>加盟店起点の取引における例外</td><td colspan="2">初回決済時やカード番号登録時等に EMV 3-D セキュアによる認証を行う。ただし、顧客からの契約内容の変更の申出、購入商品・サービスの追加等の顧客接点が生じた場合には認証を行う。</td></tr>
</table>

・前提として、当該運用を行う加盟店は、EMV 3-D セキュアを導入することが必要。

・本書に示す各運用は標準的なモデルであり、加盟店は不正利用の発生状況に応じて、附属文書 20_別紙 a「EC 加盟店におけるセキュリティ対策一覧」に記載の対策を講じることが求められる。

パターン①　加盟店のリスク判断により EMV 3-D セキュアによる認証を行う場合

加盟店が網羅的に行う不正利用対策が EMV 3-D セキュアと同等以上の不正抑止効果があることを前提として、加盟店の不正リスク判断によって必要な場合に EMV 3-D セキュアによる認証を行う。

■要件

・加盟店は、「決済前」「決済時」「決済後」全ての場面で網羅的（※1）に不正対策を講じる。
・自社のアクセス履歴・購買履歴等を軸にした属性・行動分析（※2）による不正リスク判断を行う。
・加盟店の不正リスク判断の結果、必要な場合には EMV 3-D セキュアによる認証を行う。
・本運用を行うためには、 加盟店において 24 時間 365 日継続的なセキュリティ対策の実施を可能とするため、専門部署設置や専任担当者の配置等の組織体制整備（※3）を行う。
・本運用は、カード会社（アクワイアラー）・PSP の了解の上で行う。
・加盟店は、不正利用の発生状況に応じて更なる不正利用対策の強化を行う。

※1 「決済前」「決済時」「決済後」に以下の対策を講じた上で、附属文書 20_別紙 a「EC 加盟店におけるセキュリティ対策一覧」の「３．不正ログイン対策（決済前の対策）」及び「４．決済時・決済後の対策」に記載されている対策を網羅的に行う。

図 13 【「決済前」「決済時」「決済後」の対策】

決済前	「EC 加盟店におけるセキュリティ対策一覧」に記載の「不正ログイン対策」の３つの場面（会員登録、会員ログイン、属性情報変更）に記載の対策を網羅的に行い、さらに属性・行動分析を行う。
決済時	属性・行動分析による不正検知を行う。
決済後	配送停止・配送保留について、配送先情報の目視等での確認、カード会社からの要請への協力、および属性・行動分析による確認等を行う。

※2 自社での属性・行動分析の導入、運用にあたっては附属文書 19「属性・行動分析ガイダンス」に準じた運用を前提とする。
※3 PCI DSS 準拠で求められる体制整備と同等以上のものとする。

パターン② カード番号登録時に EMV 3-D セキュア認証を行う場合

カード番号登録時には必ず EMV 3-D セキュアによる認証を行い、
以降の決済時にはアカウント等の利用者であることの確認および加盟店の不正リスク判断によって必要な場合に EMV 3-D セキュアによる認証を行う。

■要件

・加盟店がカード番号の登録時（※1）に EMV 3-D セキュアによる認証を行う。
・加盟店はアカウント等の厳格な管理及び不正ログイン対策（※2）を講じた上で、ログインが行われる際にアカウント等の利用者であることの確認を行う。
・加盟店は決済の都度、取引金額や取引商材、属性・行動分析（※3）等により不正リスク判断を行い、その結果、必要な場合には EMV 3-D セキュアによる認証を行う。
・加盟店は不正利用の発生状況に応じて、その他の対策（※4）も行う。

※1 加盟店等のアカウント等へクレジットカード番号を紐づけすること。クレジットカード番号の変更、再登録、追加等を含む（有効期限の更新は除く）。
※2 附属文書 20_別紙 a「EC 加盟店におけるセキュリティ対策一覧」に記載の「３．不正ログイン対策（決済前の対策）」の内「会員ログイン時」の対策を複数行う。
※3 属性・行動分析を運用する場合には附属文書 19「属性・行動分析ガイダンス」に準じた運用を行う。
※4 附属文書 20「EC 加盟店におけるセキュリティ対策　導入ガイド」に記載の「不正利用対策」から適宜必要な対策を講じる。

パターン③　決済の都度、EMV 3-D セキュアによる認証を行う場合

パターン①②に該当しない加盟店は、決済の都度、EMV 3-D セキュアによる認証を行う（※1）。

■要件

・加盟店は不正利用の発生状況に応じて、その他の対策（※2）も行う。

※1 カード番号登録時においても、EMV 3-D セキュアによる認証を行うことを推奨する。
※2 附属文書 20「EC 加盟店におけるセキュリティ対策　導入ガイド」に記載の対策から適宜必要な対策を講じる。

加盟店起点の取引における例外

・「クレジットカード番号が通知される取引の次の取引以降に顧客からのクレジットカード番号の通知が行われない取引（加盟店起点の取引）」については、初回決済時やカード番号登録時等に EMV 3-D セキュアによる認証を行う。
・ただし、顧客からの契約内容の変更の申出、購入商品・サービスの追加等の顧客接点が生じた場合には認証を行う。

図 14 【加盟店起点の取引具体例】

加盟店起点の取引具体例
定期的な商品・サービスの購入における同一のクレジットカード番号による継続的な支払 （いわゆる継続課金（リカーリング）取引）
チャージ型決済手段におけるオートチャージ
既存取引における加盟店側の事情による再オーソリ （事前予約後の金額確定時決済、商品の一部返品による金額変更、商品の分割出荷時等）

3. 導入手続きについて

3. 導入手続きについて

（1） 加盟店の導入形態について

EMV 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 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 15 【導入形態について】

図 16 【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[12]（カード会社直接契約加盟店、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）EMV 3-D セキュア覚書締結 ・（必要な場合）Acquirer Merchant ID, Acquirer BIN, MCC な	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。

[12] 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。

	・（必要な場合）国際ブランドテスト実施申請	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	
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	

① 自社構築（カード会社直接契約加盟店、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

a. 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 EMV 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 EMV 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。

b. 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。

c. 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。

d. 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（アクワイアラー）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 4 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

a. カード会社との手続き

- ✓ **EMV 3-D セキュア覚書締結**
- ✓ EMV 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 および契約カード会社（アクワイアラー）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（アクワイアラー）へ申請して EMV 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（アクワイアラー）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（アクワイアラー）へ確認すること。

b．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。

c．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（アクワイアラー）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 4 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（アクワイアラー）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（アクワイアラー）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

a．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。

b．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 4 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 5 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 セキュアはそれぞれ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 1 章（6）を参照。

② EMV 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。

4. 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、カード会社（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、最終的にカード会社（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相対的にリスクが高い商材を取扱う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（カード会社（アクワイアラー）、PSP、加盟店）で確認[13]が必要である。

また、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 要求に対するカード会社（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[14]、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。

---

[13] 国際ブランドによって独自の推奨項目が存在する場合があるため確認することを推奨する。

[14] 国際ブランドによっては、NPA においても CAVV（AAV）を必須化しているため留意が必要。

図 17 【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） 全件チャレンジ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、一部カード会社(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、カード会社（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 Transaction 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、全件チャレンジ認証を行う場合、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：カード会社（イシュアー）にチャレンジを求める

・04：カード会社（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、全件チャレンジ認証を行う場合、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。

③ 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カード会社（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、カード会社（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、カード会社（イシュアー）は、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、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、実際の判定はカード会社（イシュアー）に委ねられる。

図 18 【会員未登録もしくはカード会社(イシュアー)未対応の場合に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カード会社（イシュアー）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、カード会社（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、カード会社（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。
※カード会社（イシュアー）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、EMV 3-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 19 【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。

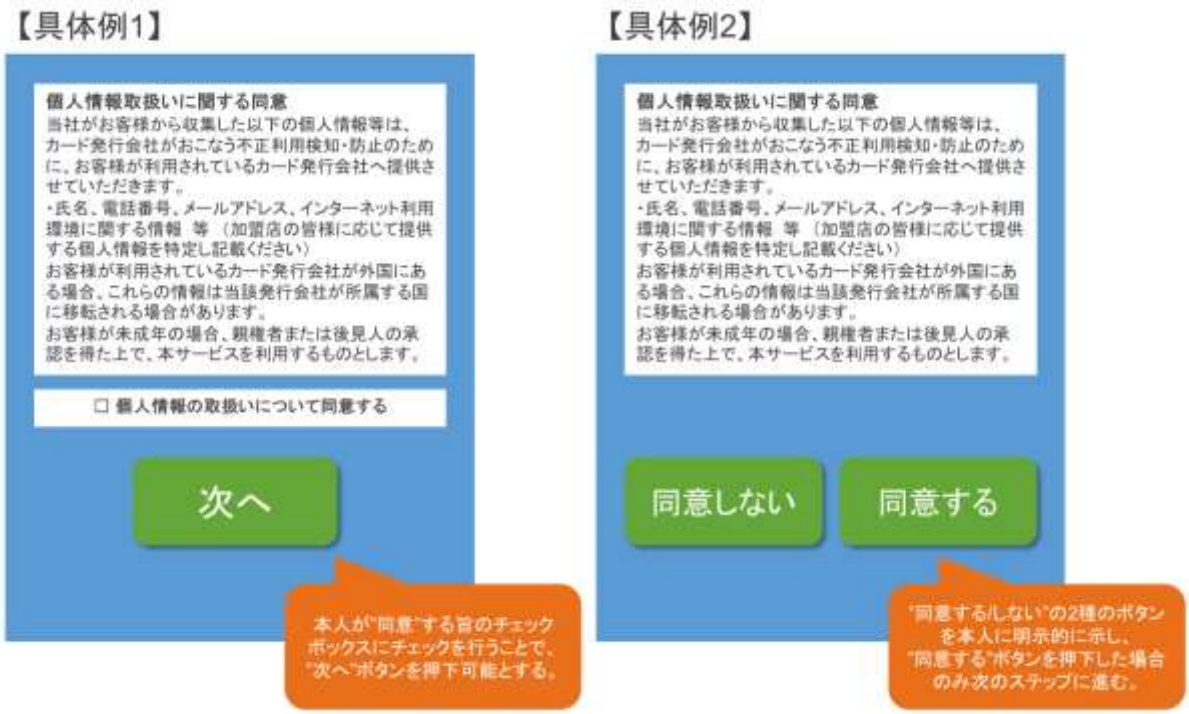
・画面構成の具体例

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 5 章を参照のこと。

図 20 【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。

（8） 3RI について

3RI の概要については P13「1. EMV 3-D セキュアの概要（７）EMV 3-D セキュア処理フロー概要③3RI（3DS Requester Initiated）について」を参照のこと。

3RI をリクエストする加盟店/PSP は、AReq 電文にデバイスチャネル「03」を設定し、利用する 3RI のユースケースに沿った 3RI Indicator 及び各国際ブランドが定める項目を設定した上で送信することで、ACS（イシュアー）から新たな CAVV（AAV）の取得が可能となる。

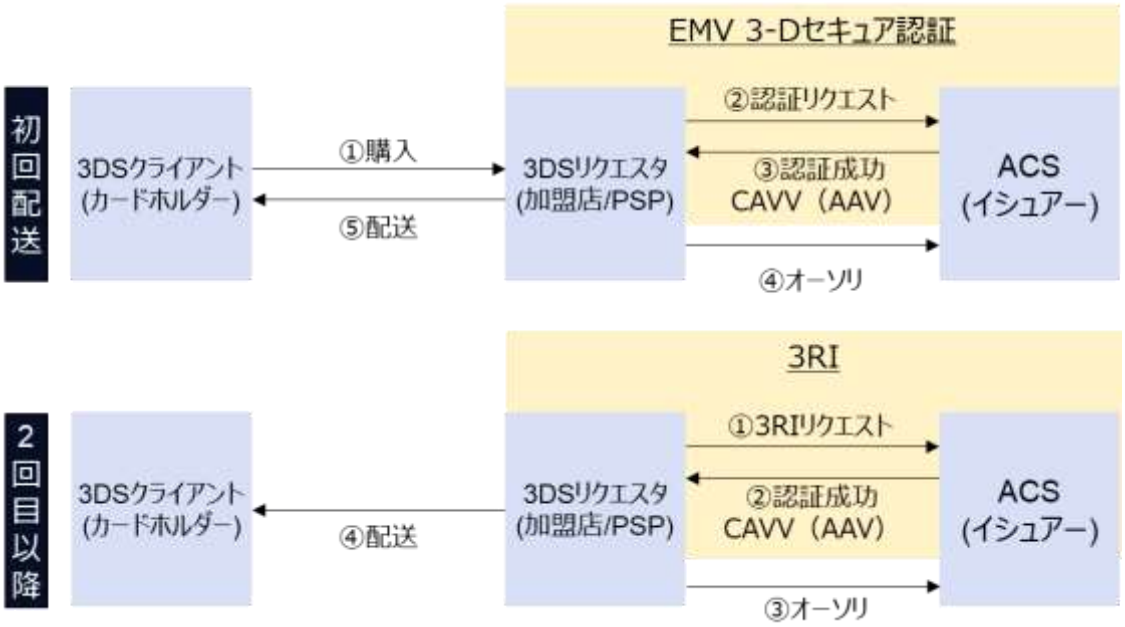
一方で、国際ブランドによって仕様や利用できるユースケース、加盟店における CAVV（AAV）の再利用や期限が異なるため留意が必要。[15]以下に 3RI が利用できるユースケースの一部事例を示す。

また、ユースケースの詳細や運用については「別紙_統合版_AReq 設定項目」及び、各国際ブランドの仕様を参照すること。

・ 3RI のユースケース「分割配送」

2 つ以上の商品・サービスを 3DS クライアント（カードホルダー）が同時購入したが、配送のタイミングはそれぞれ別の場合のユースケース。

図 21 【分割配送における 3RI の利用フロー】



3DS クライアント（カードホルダー）が 3DS リクエスタ（加盟店）で商品・サービスを購入する際に EMV 3-D セキュアによる認証を行う。認証成功となった場合、ACS（イシュアー）は ARes 電文に CAVV（AAV）を含めて応答を行う。3DS リクエスタ（加盟店/PSP）は、初回配送の商品のオーソリゼーションを ARes 電文上の CAVV（AAV）を用いて行い、初回配送をする。

---

[15] 導入にあたっては、カード会社の対応状況も影響するため、3RI での運用を検討する際には、カード会社(アクワイアラー)との協議が望ましい

2 回目以降の配送時には、3DS リクエスタ（加盟店/PSP）は 3RI を用いて CAVV（AAV）の再取得を行い、取得した CAVV（AAV）でオーソリゼーションを行い配送することが可能となる。

5. 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

5. 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（イシュアー）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、必要に応じて動的（ワンタイム）パスワード入力等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、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。

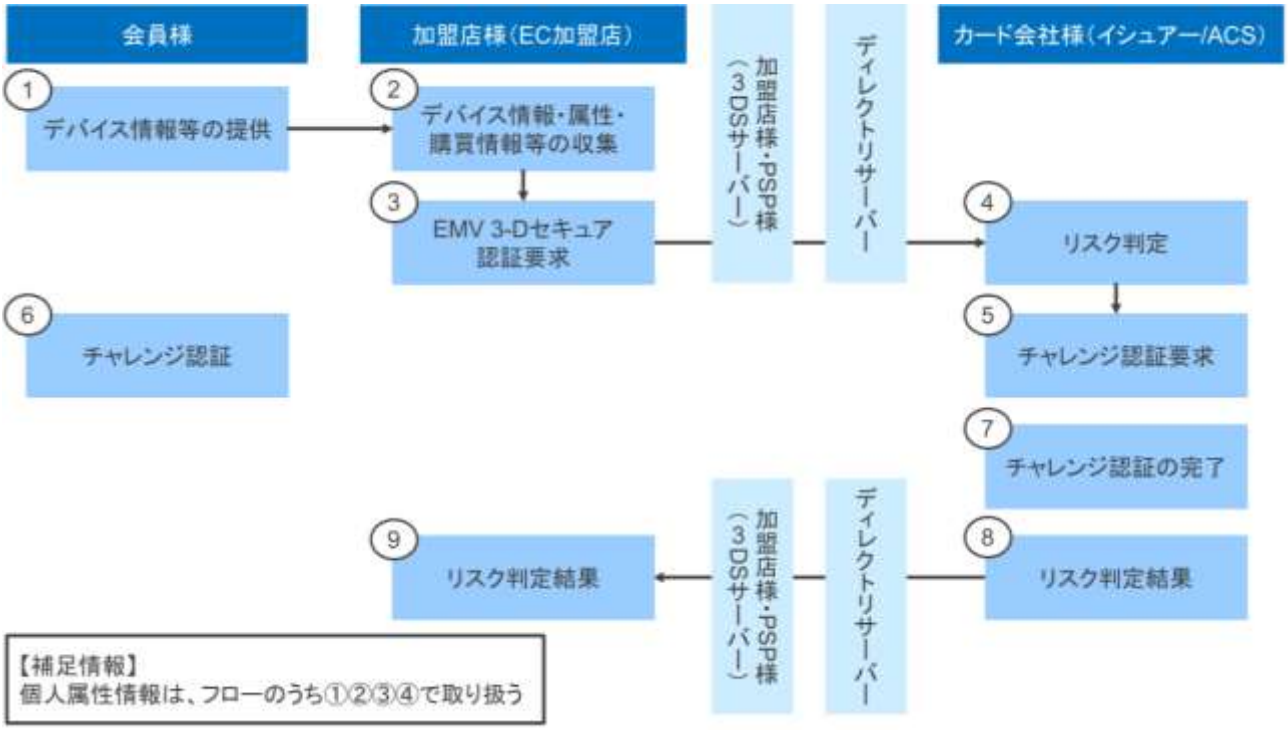
(2) EMV 3-D セキュアにおける個人情報の取扱いにおける留意点

「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 22 【「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】

加盟店は、クレジットカード取引時に、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、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、加盟店による利用目的の特定や制限、加盟店の本人からの第三者提供の同意取得、加盟店・カード会社(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、加盟店の記録保存履行及びカード会社(イシュアー)の確認記録の履行を妨げるものではない。

図 23 【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	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 24 【同意取得方法（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 4 章（6）を参照。

なお、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（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 25 【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）「○○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」

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

クレジットカード取引の安定性・信頼性を確保しつつ、不正利用被害の極小化に資する対策の継続的な運用のために、EMV 3-D セキュアに関するシステムの安定稼働が重要であることは言うまでもなく、セキュリティガイドラインにおいても各 EMV 3-D セキュア関係事業者に対して継続的な安定稼働に向けた取組が求められている。

また、EMV 3-D セキュアの加盟店における円滑な取引及び不正利用の抑止等の向上にはカード会社（イシュアー）におけるリスクベース認証の精度向上が重要である。

本章では EMV 3-D セキュア安定稼働に向けた取組の強化と障害等発生時の対応、及び認証精度向上に向けて関係事業者に対して推奨される事項について記述する。

(1) EMV 3-D セキュアの安定稼働と障害発生時等の対応について

① 障害等発生防止に向けたシステムのキャパシティ確保と安定稼働に向けた対応強化

EMV 3-D セキュアに関するシステムの安定稼働のために、各 EMV 3-D セキュア関係事業者においてはシステムのキャパシティ確保や安定稼働に向けた対策とリソース確保が重要であり、万一の障害等の発生に備えるために緊急連絡体制の整備も重要となる。

② 障害等発生時の対応と情報連携

障害等の発生の疑いを把握した EMV 3-D セキュア関係事業者は、速やかに自社システムの状況について調査を行い、自社システムを原因として障害等が発生していることを認識した場合は、障害等発生箇所の把握、発生原因の究明、影響範囲の特定、復旧措置等を講じ、EC 利用者への顧客対応が必要となるカード会社（イシュアー）や加盟店に対し、必要に応じて障害等が発生している事実や復旧までの見込み時間等について情報連携することに努める。また、情報連携が必要と認められる場合には迅速な対応が求められる。なお、障害発生時の要因が外部からの不正アタックの場合には情報の取扱いには十分に留意し、真に必要な範囲に限定する必要がある。

また、調査の結果、他社起因による障害等であることが明確で、発生個所が特定された場合については、必要に応じて関係事業者間で連携することが望ましい。

障害等が復旧した場合にも同様に迅速な情報連携を行い、復旧後には再発防止策を講じることが求められる。

一方で、EMV 3-D セキュアはインターネット通信を利用する認証手段であることから、通信経路上の障害や一時的な通信の不安定など、EMV 3-D セキュア関係事業者にて把握や制御ができない障害が発生することも多く確認されていることについても認識する必要がある。

③ 障害等発生時の取引と不正利用対策

障害等の発生時には、各事業者の判断により EMV 3-D セキュアによる認証を行わずに取引を行うことも許容される。

一方で、障害等の発生を理由として、EMV 3-D セキュアによる認証を実施しなかった取引については、不正利用のリスクが高い取引が含まれる可能性もあるため、他の手段により不正リスクの低減を行うことが重要となる。

I. カード会社（イシュアー）

EMV 3-D セキュアによる認証をしていないオーソリゼーションを識別することが可能であるため、不正検知システム等により適切な判定を行うことが求められる。

II. 加盟店

不正利用のリスクが高い取引が含まれる可能性を考慮し、オーソリゼーションに加えて、リスクに応じて EMV 3-D セキュア以外の有効な不正利用対策により当該クレジットカード取引の真正性確認と不正利用を防止することが推奨される。

また、障害等の発生を理由として、加盟店等のアカウントへのクレジットカード紐づけ時に EMV 3-D セキュアによる認証を行えない場合においては、アカウントにカード情報を紐付けるかの判断をリスクに応じて行う必要がある。なお、EMV 3-D セキュアによる認証を行わずに紐付けをしたアカウントについては、それ以降当該アカウントへのログインにより継続的に取引が可能となることから、障害等が改善され復旧した以降の当該アカウントでの決済時等、適切なタイミングで EMV 3-D セキュアによる認証を行うことを推奨する。

(2) 認証精度の向上に関する推奨事項

① 加盟店/PSP

・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相対的にリスクが高い商材を取扱う加盟店などは優先的に正しく設定すること。

- 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。

店舗単位で設定することとし、不正顕在化加盟店や相対的にリスクが高い商材を取扱う加盟店などは優先的に正しく設定すること。

（具体的な設定値は「別紙_統合版_AReq 設定項目」 参照）

- 条件付き必須項目・オプション項目の活用

一部国際ブランドでは必須項目とされており、ACS でのリスク判定に有効な項目と考えられる。

（データ項目：Browser IP Address、Cardholder Phone Number または Cardholder Email Address、Cardholder Name）

設定が可能である場合、特に不正顕在化時および相対的にリスクが高い商材を取扱う加盟店においては、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、「別紙_統合版_AReq 設定項目」を活用する。

② カード会社（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、カード会社（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相対的にリスクが高い商材を取扱う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、カード会社（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、「別紙_統合版_AReq 設定項目」を活用する。

③ カード会社（イシュアー）

I. 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。

II. 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。

III. 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。

IV. 全件チャレンジ認証を行う加盟店等からの認証要求について

EMV 3-D セキュアにおける加盟店からのチャレンジフローでの追加認証要求（特に 3DS Requestor Challenge Indicator=04）の取引は高リスクであると見做されるため、 以下の 3 点を実施することが望ましい。

（ア）EMV 3-D セキュア登録会員においてはチャレンジフローでの確実な追加認証を実施すること。
（イ）EMV 3-D セキュア未登録会員はチャレンジフローでの追加認証が行えないため、カード会社（イシュアー）は厳正な可否判断を実施すること。
（ウ）上記（イ）の課題を踏まえ、「EMV 3-D セキュア未登録では EC 利用ができない場合があること」を EC 利用者であるカード会員に対し、周知・啓発を実施すること。
※詳細については第 4.（4）③を参照

V. チャレンジ認証手法の検討

また、チャレンジ認証においては、生体認証等の動的（ワンタイム）パスワード以外の認証技術の活用等による、カード会員の利便性や認証精度向上のための継続的な検討に努める。

なお、生体認証では必ずしもカード会社（イシュアー）がカード会員の生体情報を保有する必要はない。生体認証を導入する場合、生体情報をスマートフォン等のデバイスに登録する際に、確実な認証がカード会員により行われる必要があるが、その後の当該デバイスによるクレジットカード利用時においては、登録された生体情報による認証等も認証方法として認められるものであり、有効な対策である。

7. 改訂履歴

7. 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 版改定箇所

1 章　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

2023 年 9 月 29 日　1.3 版改定箇所

1 章（3）EMV 3-D セキュア 2.1 のサポート終了予定日の追記

1 章（7）、図 10　P 電文（PReq、PRes）について追記、「用語集」内の 3RI についての記載の修正

3 章（8）3RI の概要とユースケースを新たに記載

6 章（1）MCC と Merchant ID の施行期間の記載、フリクションレス率の目標値を削除

6 章（1）「条件付き必須項目・オプション項目の活用」に具体例を追記

7 章　FAQ の 2、3 の記載内容を変更

2024 年 3 月 14 日　1.4 版改訂箇所

0 章（背景と目的）に新たな文言を追記

2 章　章を新設

6 章　カード会社（イシュアー）に対する推奨事項（（1）、（2））を 7 章から移動

8 章　FAQ にセキュリティガイドラインに記載の FAQ を追記

全体　セキュリティガイドラインに合わせて文言修正

2025 年 3 月 4 日　2.0 版改訂箇所

0 章　加盟店の対象読者に「不正対応･処理の実務担当者」を追加

1 章　3RI に関する記載を追加

2 章　EMV 3-D セキュア導入の指針対策に伴い、導入ロードマップの削除等記載内容を更新

4 章　3RI に関する内容を更新

6 章　2 章に統合

7 章　6 章の 2 章への統合に伴い 6 章へ変更、障害発生時の対応を追加

全体　セキュリティガイドラインに合わせて文言修正

・・・・・・・