クレジット取引セキュリティ対策協議会
EMV 3-Dセキュア導入ガイド1.4版
加盟店様向けサマリー版
2024年3月14日

目次

※本導入ガイドサマリー版は、EMV3-Dセキュア導入ガイドから抜粋して作成したものであるため、詳細はEMV3-Dセキュア導入ガイドを参照いただきたい。

1. はじめに
（導入ガイド P4）

■ 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。
- EC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いる。
- セキュリティガイドライン5.0版では、「2025年3月末までに、原則、全てのEC加盟店にEMV 3-Dセキュアの導入を求める」こととしており、全てのEC加盟店は、カード会社（アクワイアラー）・PSPと連携の上、EMV 3-Dセキュアの導入計画を策定し早期にEMV 3-Dセキュアの導入に着手することが求められる。
- また、カード会社（イシュアー）は、EMV 3-Dセキュアを導入し、継続的に安定稼働のための対応をするとともに、2025年3月末時点で、EMV 3-Dセキュア登録率80%(EC利用会員ベース)・「静的（固定）パスワード」以外の認証方法への移行率100%(EMV 3-Dセキュア登録会員ベース)を目指し、取組むこととしている。また、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。
- これらの状況を受けて、クレジット取引セキュリティ対策協議会では、円滑なEMV 3-Dセキュア導入推進の一助となるべく、全ての事業者間での共通のガイドとして「EMV 3-Dセキュア導入ガイド」を作成した。

2. EMV 3-Dセキュアについて

（導入ガイド　1章　P6,7　4章　P34）

EMV 3-Dセキュアは、3-Dセキュア（1.0）の課題であった、パスワード入力負荷の軽減やユーザビリティの改善により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。

- 3-Dセキュア1.0（2022年10月サービス終了）
  - 全取引にパスワードを毎回入力
  - 固定パスワードで一律認証
  - ブラウザ取引のみ

EMV 3-Dセキュア			
特長	内容	メリット	
		会員	加盟店
パスワード入力負荷を低減	・原則リスクベース認証のみとなり、会員へのパスワード要求が不要（フリクションレス）※	入力負荷軽減	取引離脱（カゴ落ちの減少）
ワンタイムパスワードによる本人認証	・中リスク判定時のみワンタイムパスワードなどによる追加認証を実施	パスワード漏洩による不正リスクの軽減	会員のパスワード忘れによる機会損失の軽減
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	
3DS Requestor Initiated（3RI）※	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	—	商品の配送分割や配送遅延の場面で利用可能

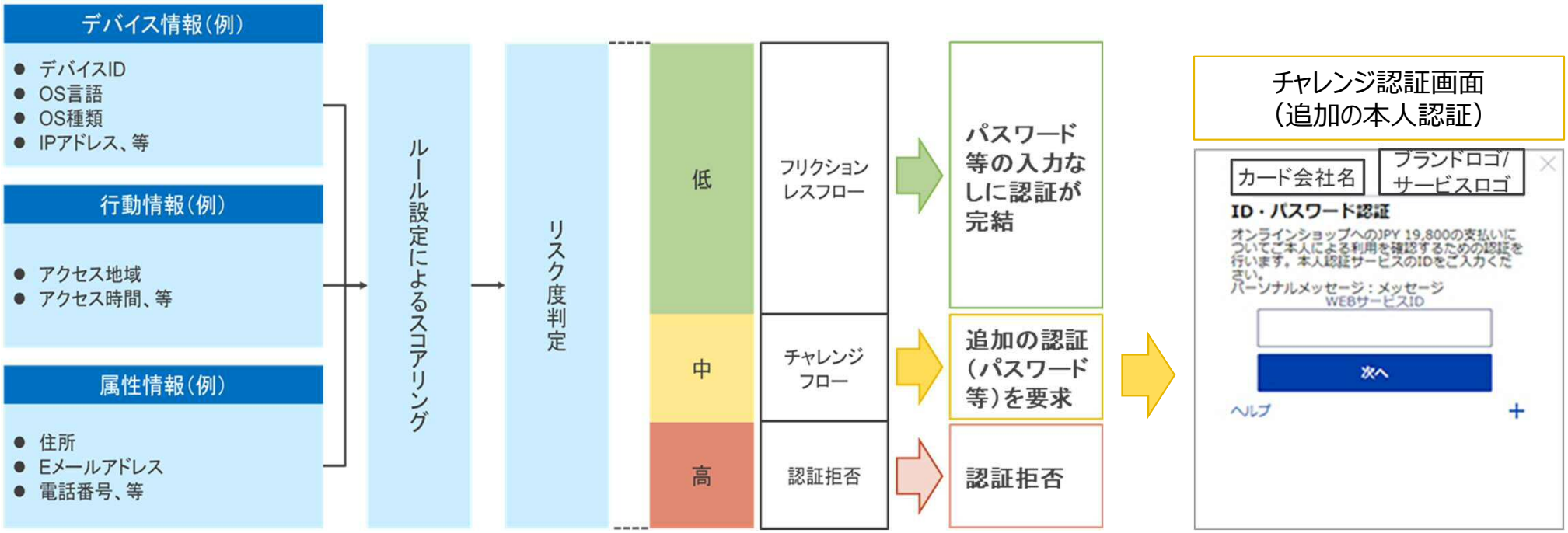
※リスクベース認証、3RIについては次ページ以降で説明

3. EMV 3-Dセキュアのリスクベース認証について

（導入ガイド　1章　P8）

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。

リスクベース認証のイメージ



4. EMV 3-Dセキュアの不正リスク負担

（導入ガイド　1章　P10）

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。
（詳細は契約するカード会社（アクワイアラー）、PSP等への確認が必要）

EMV 3-Dセキュアの不正リスク負担（表）

	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※1
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※2は免責対象外

※1　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。
※2　契約のカード会社（アクワイアラー）との契約内容による。

5. カード会社（イシュアー）おけるEMV 3-Dセキュア導入推進ロードマップについて（１）

（導入ガイド 2章　P18,19）

2025年3月末までのEC加盟店におけるEMV 3-Dセキュア導入に向けて、カード会社（イシュアー）はEMV 3-Dセキュアを有効なものとすべく環境を整えていくことが強く求められる。特に、チャレンジ認証を行うための「EMV 3-Dセキュアの登録」の促進と、フィッシング等により漏えいした静的パスワードでの第三者によるなりすましを防止するための「動的（ワンタイム）パスワード等による認証」が求められる。

カード会社（イシュアー）の取り組み事項

取組事項	求められる対応
（1）EMV 3-Dセキュアの導入	➢ **未導入イシュアーによる即時導入** ※95%(*1)は導入完了（2023年10月末現在）
（2）カード会員へのEMV 3-Dセキュアの利用登録の推進	**【目標】2025年3月末時点で、EC利用会員ベース(*2)80%** ➢ カード会員へのEMV 3-Dセキュアの利用登録の要請 ➢ EMV 3-Dセキュアの利用登録に関する周知・啓発（業界横断的に実施）(*3)
（3）動的（ワンタイム）パスワード等による認証の実施	**【目標】2025年3月末時点で、EMV 3-Dセキュア登録会員ベースで100%(*4)** ➢ 動的（ワンタイム）パスワード等による認証を実施するためのシステム構築 ➢ カード会員への動的（ワンタイム）パスワード等の利用手続（携帯電話番号やメールアドレスの登録、アプリのダウンロード等）の要請 ➢ 動的（ワンタイム）パスワードの利用に関する周知・ 啓発（業界横断的に実施）

*1 ・協議会 EMV 3-Dセキュア等推進WGによるアンケート調査回答会社のうち、国際ブランド付きクレジットカードを発行するイシュアーの調査結果。

*2 ・EC利用会員は、過去1年間でEC（インターネット通信での販売） で利用実績のある会員とするが、計数抽出が難しい場合は、各社独自の判断によるEC利用会員の概数の推測も可能とする。
・法人契約カード等、個社の事情によりEMV 3-D セキュアの設定ができないカードを母数に含めないことを許容する。

*3 ・「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」を関係者（イシュアー、加盟店等）がEC利用者へ周知・啓発する。

*4 ・既存会員によっては連絡不能等で動的（ワンタイム）パスワード等の利用手続の案内が出来ないケースも想定されるため、母数を稼働会員とする等、個社判断とする。

5. カード会社（イシュアー）おけるEMV 3-Dセキュア導入推進ロードマップについて（２）
（導入ガイド　2章　P19）

不正利用被害額の早期削減の実現のために、イシュアーの対応の促進と業界横断的な周知・啓発活動を行うためのロードマップを作成した。

カード会社（イシュアー）として取り組むべき事項とスケジュール

	2023年	2024年	2025年
イベント	◆2023/11 ロードマップ公表	◆2024/3 セキュリティGL改定	◆2025/3 全てのEC加盟店で EMV 3-Dセキュア導入
EMV 3-Dセキュアの導入	95%導入完了 未導入イシュアの即時導入 ・・・		
カード会員へのEMV 3-Dセキュアの利用登録の推進	カード会員へのEMV 3-Dセキュア利用登録の要請		2025年3月末までに80% （EC利用会員ベース）
動的（ワンタイム）パスワード等による認証の実施	動的（ワンタイム）パスワード等による 認証に係るシステム構築 ・・・ カード会員への動的（ワンタイム）パスワード等の利用手続の要請		2025年3月末までに100% （EMV 3-Dセキュア登録会員ベース）
業界横断的な周知・啓発	カード会員への周知・啓発（業界横断の取組） （未登録ではEC利用できない場合がある旨） EMV 3-Dセキュアの利用登録／ 動的（ワンタイム）パスワード等の利用		

6. 加盟店におけるEMV 3-Dセキュア導入推進ロードマップについて

（導入ガイド 2章 P19,20）

不正利用被害額の早期削減を実現するためには、不正利用リスクが大きいEC加盟店からEMV 3-Dセキュアの導入を進めることが有効であることから、加盟店の不正利用リスクに応じた2025年3月末までのEMV 3-Dセキュア導入推進ロードマップを作成した。

EMV 3-Dセキュアの導入推進ロードマップ

（1）既存加盟店

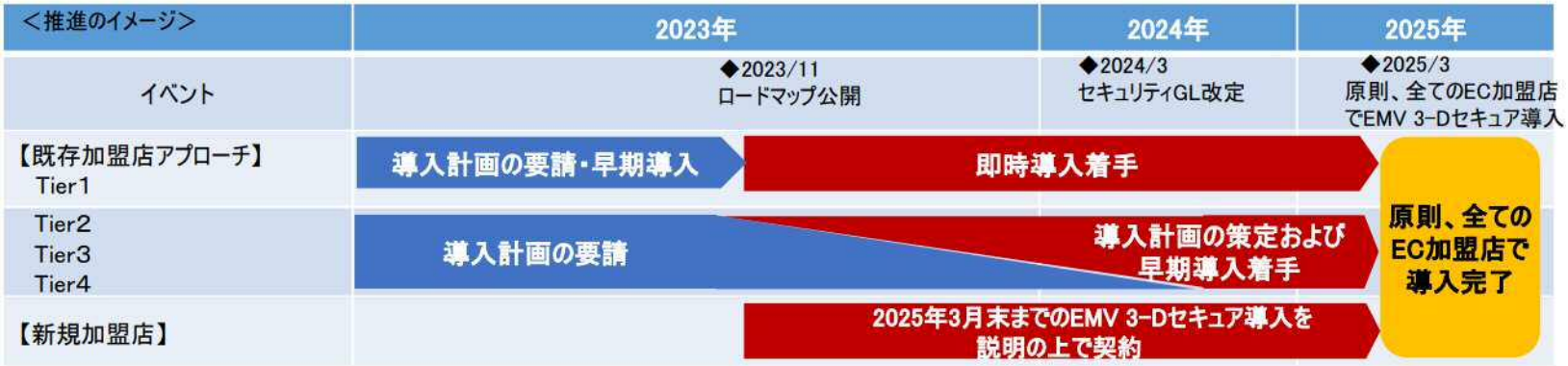
アクワイアラー・PSPは以下の優先順位でEC加盟店に対するEMV 3-Dセキュアの導入を求めることとする。

優先順位	対象	求められる対応
Tier 1	不正顕在化加盟店*1	即時EMV 3-Dセキュア導入着手
Tier 2	不正顕在化加盟店ではないが不正が発生している加盟店 直近2年で、不正が5件以上または累計で10万円以上発生した加盟店	EMV 3-Dセキュア導入計画の策定および早期の導入着手
Tier 3	高リスク商材取扱加盟店 ①デジタルコンテンツ、②家電、③電子マネー、④チケット、⑤宿泊予約サービス	EMV 3-Dセキュア導入計画の策定および早期の導入着手
Tier 4	上記以外の加盟店	EMV 3-Dセキュア導入計画の策定および早期の導入着手

*1：カード会社（アクワイアラー）各社が把握する不正利用金額が「3ヵ月連続50万円超」に該当するEC加盟店

（2）新規加盟店

アクワイアラー・PSPがEC加盟店と新規に加盟店契約する際、2025年3月末までにEMV 3-Dセキュアを導入することを説明した上で契約することとする。

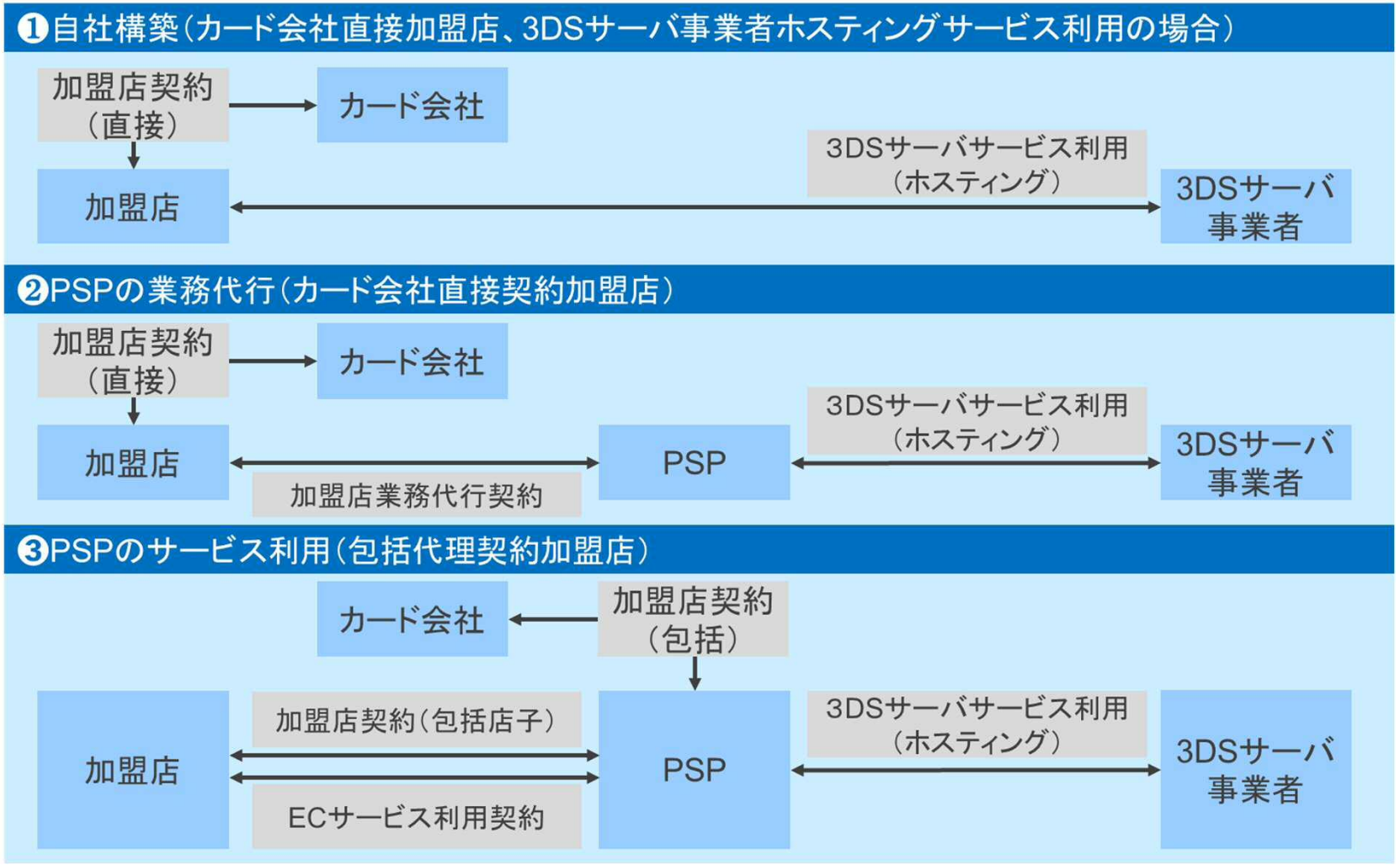


７．導入手続きについて

（導入ガイド　3章　P23～28）

加盟店によって契約形態は異なるが、いずれの契約形態においてもEMV 3-Dセキュア未導入の場合は、契約するカード会社（アクワイアラー）及びPSPに詳細をご確認いただきたい。

導入形態について



８．個人情報の取扱いに関する同意取得について

（導入ガイド　4章　P32,33　5章　P37～42）

EMV 3-Dセキュアで利用できるデータ項目には個人情報又はそれになり得る情報が含まれることがあるため、加盟店がカード会員から情報提供にかかる同意を取得する必要がある。

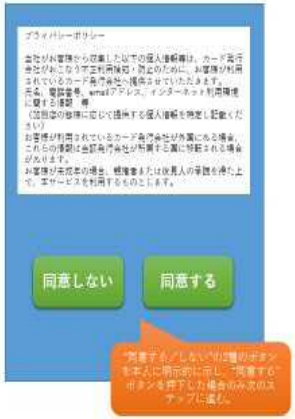
個人情報保護法の遵守

- 利用できるデータ項目の中には個人情報又はそれに準ずる情報が含まれる。
- 従って、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為には、情報主体であるカード会員から、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。

「同意取得」に係るサンプル画像（例）

【具体例１】

【具体例２】



システム開発要件

- EMV 3-Dセキュアの導入の際には、開発が必要になります。詳細は、「導入ガイド」4章を確認のうえ、委託先などにご依頼いただきたい。

９．EMV 3-Dセキュアのバージョンについて

（導入ガイド　1章　P6,7）

EMV 3-DセキュアはEMVCoの仕様でバージョン2.1、2.2、2.3まで公表されており、
バージョンアップに伴い、新たな機能が追加されている。
バージョン2.1については、2024年9月にサービス終了を迎えるため移行が必要となる。

	EMV 3-Dセキュア v2.1	EMV 3-Dセキュア v2.2	EMV 3-Dセキュア v2.3
バージョン公開日	**2017**	**2018**	**2021**
特徴	• リスクベース認証 • スマートフォンやタブレットによるアプリ内での利用 • デジタルウォレットへのカード登録 など	• 3RIの拡張 など	• 新しい技術環境(IOT、スマートスピーカーなど) への対応 など
関連情報	• **2024年9月に各国際ブランドでサービス終了**（詳細は導入ガイド1章（3）を参照）	• 主流となっているバージョン	• デバイスの追加とセキュリティの向上が期待される
メリット	• 「拒否」が減る(より多くのデータ共有) • かご落ちの減少(UXの向上による)	• 加盟店における認証機能（3RI）の拡充	• 新しいデバイスによるセキュリティとカスタマーエクスペリエンスの向上が期待される

１０. EMV 3-Dセキュアの認証精度向上に向けた推奨事項について

（導入ガイド　7章　P50）

EMV 3-Dセキュアの認証精度向上のためには、加盟店からカード会社に伝送するデータ項目（AReq設定項目やAReqオプション項目）の種類を豊富さと、データ項目の一貫性や正確性が必要である。それにより、認証精度の向上とフリクションレス率の向上がもたらされる。特に以下が重要なデータ項目である。

データ項目	内容説明
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。
Merchant Name	Merchant IDとともにカード会社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。
Merchant Category Code	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求められる。
Browser IP Address、 Cardholder Phone Number または Cardholder Email Address、 Cardholder Name	一部国際ブランドでは必須項目とされており、カードホルダーが購入した場所を把握するためのデータとしてカード会社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。

*設定について不明点がある場合は、契約カード会社もしくはPSPに問い合わせいただきたい。

１１．3RIについて

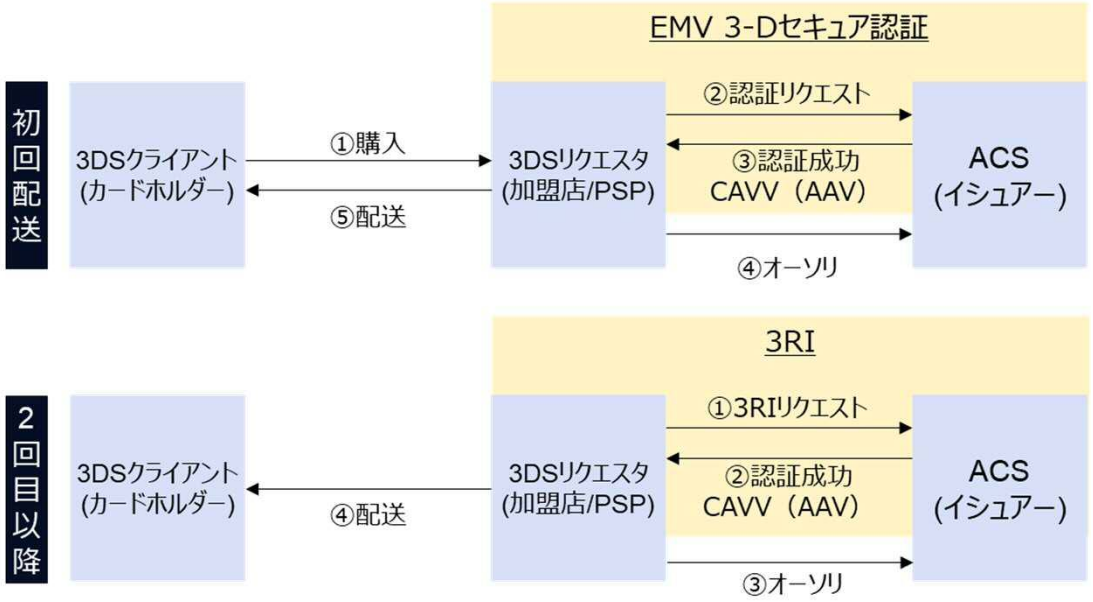
（導入ガイド　4章　P34）

3RIとは、分割配送や配送遅延などの1度の認証に対して複数回オーソリゼーションが行われる取引において、加盟店が2回目以降のオーソリゼーション時に再度オーソリゼーションに設定するための認証情報（AAV、CAVV）の再取得ができる機能である*。

*国際ブランドによって対応の有無があるため、契約カード会社への確認が必要である

3RIのユースケースの代表例	内容説明
分割配送	2つ以上の商品・サービスを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
遅延配送	商品・サービスをカードホルダーが購入したが、配送までに一定期間経過してしまう場合のユースケース

例：「分割配送」時の3RIのフローと概要



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メッセージに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メッセージ上のCAVV（AAV）を用いて行い、初回配送をする。
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。

3RIのその他のユースケースや国際ブランドの仕様については、**【公表版】統合版_AReq設定項目及び3RIの仕様・ユースケース**を参照