導入補足資料

– EMV 3Dセキュア（ブラウザベース）

第1.3.1版 2024年11月20日
株式会社ペイジェント

改訂履歴

版数	日付	変更箇所	変更内容
1.0.0	2021年2月15日		新規作成
1.0.1	2021年4月5日	5	限定公開機能についての記載を別紙へ移動 リスクベース認証 - 異常ケース No1 加盟店へ応答しないケースに変更 No2,3 レスポンスコードを削除（正常終了時はレスポンスコードを応答しない） チャレンジ認証 - 異常ケース No1 加盟店へ応答しないケースに変更, パスワードを29999に変更 No2,3 レスポンスコードを削除（正常終了時はレスポンスコードを応答しない）
1.0.2	2021年4月8日	2,3,6	3Dセキュア2.0認証電文の電文種別IDを450に修正
1.0.3	2021年6月23日	3.1	チャレンジフローでの取引の流れの項番と説明がずれていた箇所を修正
1.0.4	2021年8月26日	目次、 2、 3、 6	目次に後述の追加分の内容を追記 2.1をモジュール向けの説明と明記し、2.2をリンクタイプ向けで追加 3.1をモジュール向けの説明と明記し、3.2をリンクタイプ向けで追加 6.2をモジュール向けの説明と明記し、6.3をリンクタイプ向けで追加
1.0.5	2021年9月21日	5.1 5.2	以下の処理結果、attempt区分、レスポンスコードを修正と※2の記述を削除 5.1.リスクベース認証の返却値を確認する スクベース認証 - 正常ケース No22,27 リスクベース認証 - 異常ケース No1（設定する決済金額も修正） 5.2.チャレンジ認証の返却値を確認する チャレンジ認証 - 異常ケース No1（設定するパスワードも修正） ※2 カード会社からの返却値が予期しない内容の場合 の記述を削除
1.0.6	2021年11月24日	5	未定義の金額、未定義のパスワードを入力した場合の応答内容を追記 リスクベース認証 - 正常ケース MasterCardのレスポンスコード：E001 を返却する 2ケースを削除
1.0.7	2021年12月27日	7	.認証タイムアウトに関する説明を追加
1.0.8	2022年6月22日	5	・1.0.6 版の改定により不要となった記載内容「※1 ブランド判定について」を削除 ・本章に記載されていない ブランド 、決済金額、パスワード の組み合わせに対する ペイジェント返却値 についてはサポート対象外となる旨を記載
1.0.9	2022年8月24日	2、 3、 6	以下のシーケンス図において、3Dセキュア2.0認証結果応答がリダイレクトであることを表現できていなかった問題を修正 2.1.フリクションレスフローでの取引の流れ（モジュールタイプ） 3.1.チャレンジフローでの取引の流れ（モジュールタイプ） 6.2.3Dセキュア1.0実施時のイメージ（モジュールタイプ）
1.1.0	2023年2月21日	4.3	文字コード：UTF-8に対応した最新の通信モジュールを使用する必要性について追加
1.1.1	2023年5月24日	4.2	サンプル：同意取得文言を最新化

版数	日付	変更箇所	変更内容
1.1.2	2023年8月9日	全般	「3Dセキュア2.0」から「EMV 3Dセキュア」に表記を修正
		5.1 5.2	・試験環境で利用可能となった決済金額の追記とNoの誤字修正 5.1.リスクベース認証の返却値を確認する リスクベース認証 – 正常ケース リスクベース認証 – 異常ケース ・試験環境で利用可能となったパスワードの追記とNoの誤字修正 5.2.チャレンジ認証の返却値を確認する チャレンジ認証 – 正常ケース チャレンジ認証 – 異常ケース
		6	「6.3Dセキュア2.0未対応カード」を削除 また、7.認証タイムアウト通知から6.認証タイムアウト通知に修正
1.1.3	2024年4月5日	全般 2、3、6 目次、7	誤字脱字を修正 図の中の名称をEMV 3Dセキュア(3DS 2.0)に修正 7.カード情報お預かりを追加
1.1.4	2024年8月27日	2、 3	各「取引完了」工程説明に「＜ご注意＞」文を追記
1.2.0	2024年10月16日	5.1	5.1.リスクベース認証の返却値を確認する 試験環境のEMV 3Dセキュア（3DS 2.0）認証電文では、要求情報の決済金額または、カード名義人を元にリスクベース認証の返却値を制御します。に修正 決済金額、カード名義人両方を設定した場合、返却値は決済金額の値となります。 を追記 リスクベース認証 – 正常ケース 新たな表に差し替え リスクベース認証 – 異常ケース新たな表に差し替え
		5.2	5.2.チャレンジ認証の返却値を確認する 試験環境のEMV 3Dセキュア（3DS 2.0）認証電文では、要求情報の決済金額に「200,000」またはカード名義人にブランド毎の値を設定することで認証画面へ遷移し、認証画面のパスワードを元にチャレンジ認証の返却値を制御します。に修正 チャレンジ認証 – 正常ケース 新たな表に差し替え チャレンジ認証 – 異常ケース 新たな表に差し替え
1.3.0	2024年11月14日	5.1	下線部分の文章、・・・決済金額またはカード名義人・・・に修正
		5.2	要求情報の決済金額に「200,000」または「400,000」またはカード名義人に・・・ に修正 下線部分の文章、・・・決済金額またはカード名義人・・・に修正 チャレンジ認証 – 正常ケースの表と、チャレンジ認証 – 異常ケースの表の決済金額orカード名義人に、400,000 を追加
		7.2	EMV 3Dセキュア(3DS 2.0)を利用したカード情報お預かりの流れ（リンクタイプ）を追加
1.3.1	2024年11月20日	5.	設定値に応じてペイジェント返却値を定めています。本章に記載の決済金額、カード名義人両方を設定した場合、返却値はカード名義人の値となります。 の文章と、設定の例の記載を追加
		5.1	決済金額、カード名義人両方を設定した場合、返却値はカード名義人の値となります。 を削除
		5.2	要求情報の決済金額に「0」または「1」または「200,000」または「400,000」、またはカード名義人に・・・ に修正 チャレンジ認証 – 正常ケースの表と、チャレンジ認証 – 異常ケースの表の決済金額orカード名義人に、0、1　を追加

はじめに

本書について

本書は、株式会社ペイジェント(以下、「ペイジェント」といいます。)のEMV 3Dセキュア(ブラウザベース)の仕様について説明いたします。
今後ペイジェントでは、「3Dセキュア 2.0」は「EMV 3Dセキュア（3DS 2.0）」と表記いたします。

目次

1.EMV 3Dセキュア(3DS 2.0)の概要

1.1.EMV 3Dセキュア(3DS 2.0)とは

EMV 3Dセキュア(3DS 2.0)とは、クレジットカード決済をインターネット上で、より安全に行うための仕組みです。

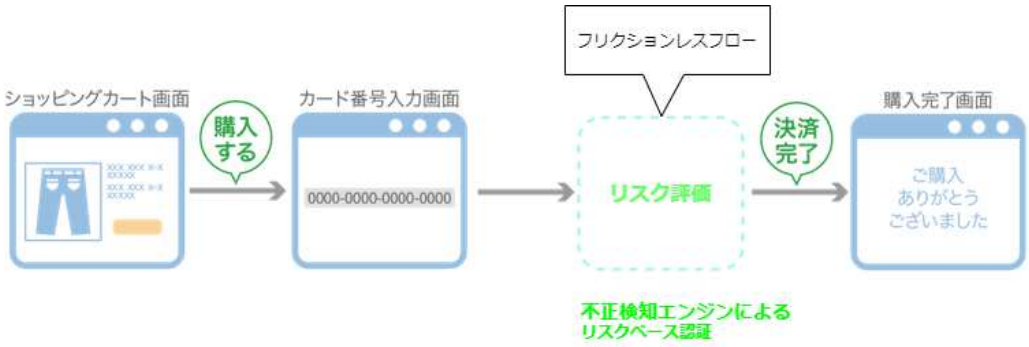
1.2.3Dセキュア1.0との違い

旧来の3Dセキュア（以下、「3Dセキュア1.0」と呼びます）では、ユーザーが3Dセキュアの認証画面に遷移し、認証情報を入力することで本人確認しましたが、3Dセキュア1.0の認証方法には以下の問題点がありました。
・ユーザーがパスワード認証を煩わしく感じてしまったり、認証画面に移動することを不審に思い、購入を諦めてしまう「カゴ落ち」が発生していた。
・第三者による「なりすまし」を検知できない。（カード番号・パスワードが漏洩してしまうと、不正利用が防げない）

EMV 3Dセキュアでは、「フリクションレスフロー」と「チャレンジフロー」の2段階のフローで認証するように変更され、これらの問題点の改善を図っています。

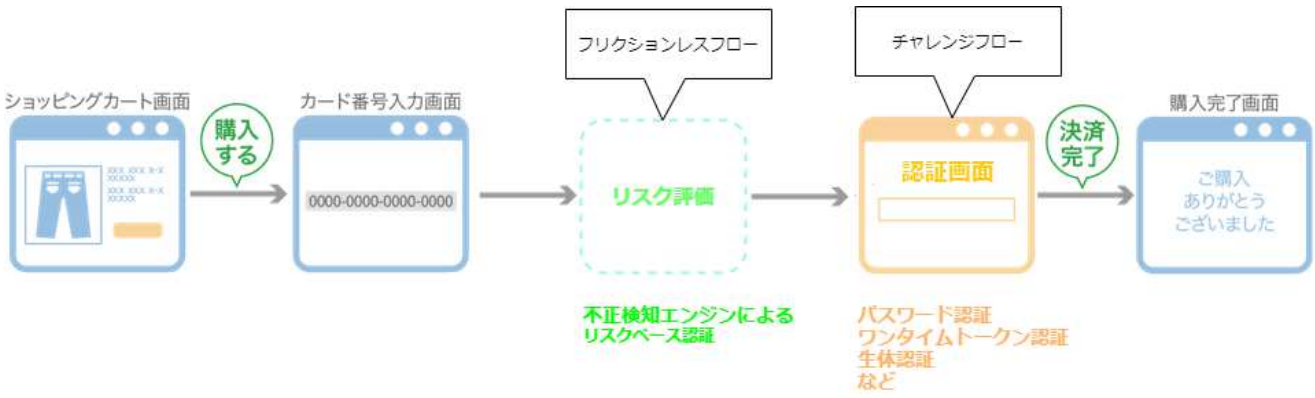
1.3.フリクションレスフローとは

「フリクションレスフロー」とは、ユーザーの行動情報・属性情報・取引情報等をもとに、不正検知エンジンによるリスクベース認証を行うフローです。
フリクションレスフローでリスクが判定できる場合、ユーザーに認証情報の入力を求めずに、認証を終了します。
フリクションレスフローではユーザーが3Dセキュア認証を意識する必要がないため、カゴ落ちを抑制できます。
フリクションレスフローの詳細については「2. フリクションレスフロー」をご参照ください。



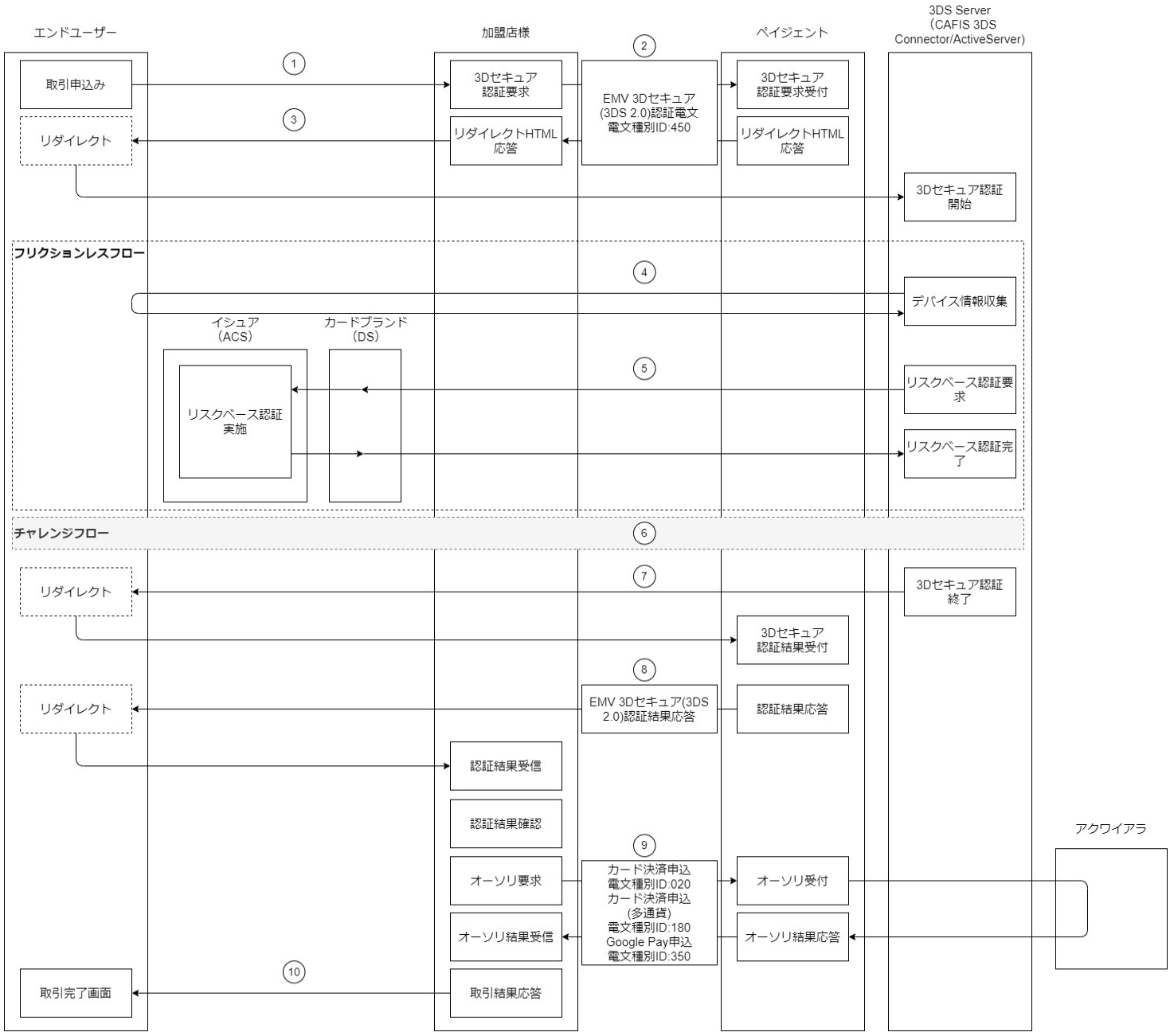
1.4.チャレンジフローとは

「チャレンジフロー」とは、3Dセキュア1.0のパスワード認証に相当する、ユーザーによる追加認証を行うフローです。
チャレンジフローは、フリクションレスフローで追加の認証が必要と判定された場合のみ実施します。
EMV 3Dセキュアでは従来のパスワード認証に加えて、動的パスワード認証（SMSやメールを使ったワンタイムパスワード等）、生体認証（指紋や顔等）に対応します。（※）
動的パスワード認証や生体認証では、第三者によるなりすましが困難になるため、不正利用の低減が期待できます。
※実際にどの方法で認証を行うかは、各カード会社が提供する本人認証サービスによって異なります。
　カード会社によっては引き続きパスワード認証を使用する可能性があります。



2.フリクションレスフロー

2.1.フリクションレスフローでの取引の流れ（モジュールタイプ）



1．注文

ユーザーがECサイトで取引を申込みます。

2．3Dセキュア認証申込み

加盟店様からペイジェントへ、「EMV 3Dセキュア（3DS 2.0）認証電文（電文種別ID:450）」でEMV 3Dセキュア(3DS 2.0)の認証を申込んでいただきます。
ペイジェントは加盟店様へ認証を開始するためのリダイレクトHTMLを応答します。

3．3Dセキュア認証開始

加盟店様は、[2]で取得したリダイレクトHTMLをユーザーへ応答してください。
ユーザーがリダイレクトHTMLを表示すると、CAFIS 3DS Connectorへアクセスし、EMV 3Dセキュア認証を開始します。

4．デバイス情報収集

CAFIS 3DS Connectorはユーザーからデバイス情報を収集します。

5．リスクベース認証実施

CAFIS 3DS Connectorは、イシュアへユーザーの行動情報・属性情報・取引情報等を送信します。
イシュアは、それらの情報をもとにリスクベース認証を行い、認証結果をCAFIS 3DS Connectorへ応答します。

6．チャレンジフロー

フリクションレスフローでリスク判定できない場合のみ、チャンレンジフローを実施します。
チャレンジフローについては「3．チャレンジフロー」をご参照ください。

7．ユーザーからペイジェントへ認証結果を通知

ユーザーからペイジェントへ認証結果が送信されます。

8．ペイジェントから加盟店様へ認証結果を通知

ペイジェントから加盟店様へ認証結果を送信します。
加盟店様は、「EMV 3Dセキュア（3DS 2.0）認証結果応答電文」の処理結果・Attempt区分をもとに、取引継続の可否をご判断ください。
Attempt区分につきましては、「02_PG外部インターフェース仕様説明書（別紙：EMV 3Dセキュア）」記載の「1.2.EMV 3Dセキュア（3DS 2.0）認証結果応答電文」及び「Attemptについて」をご確認ください。

9．決済を申込む

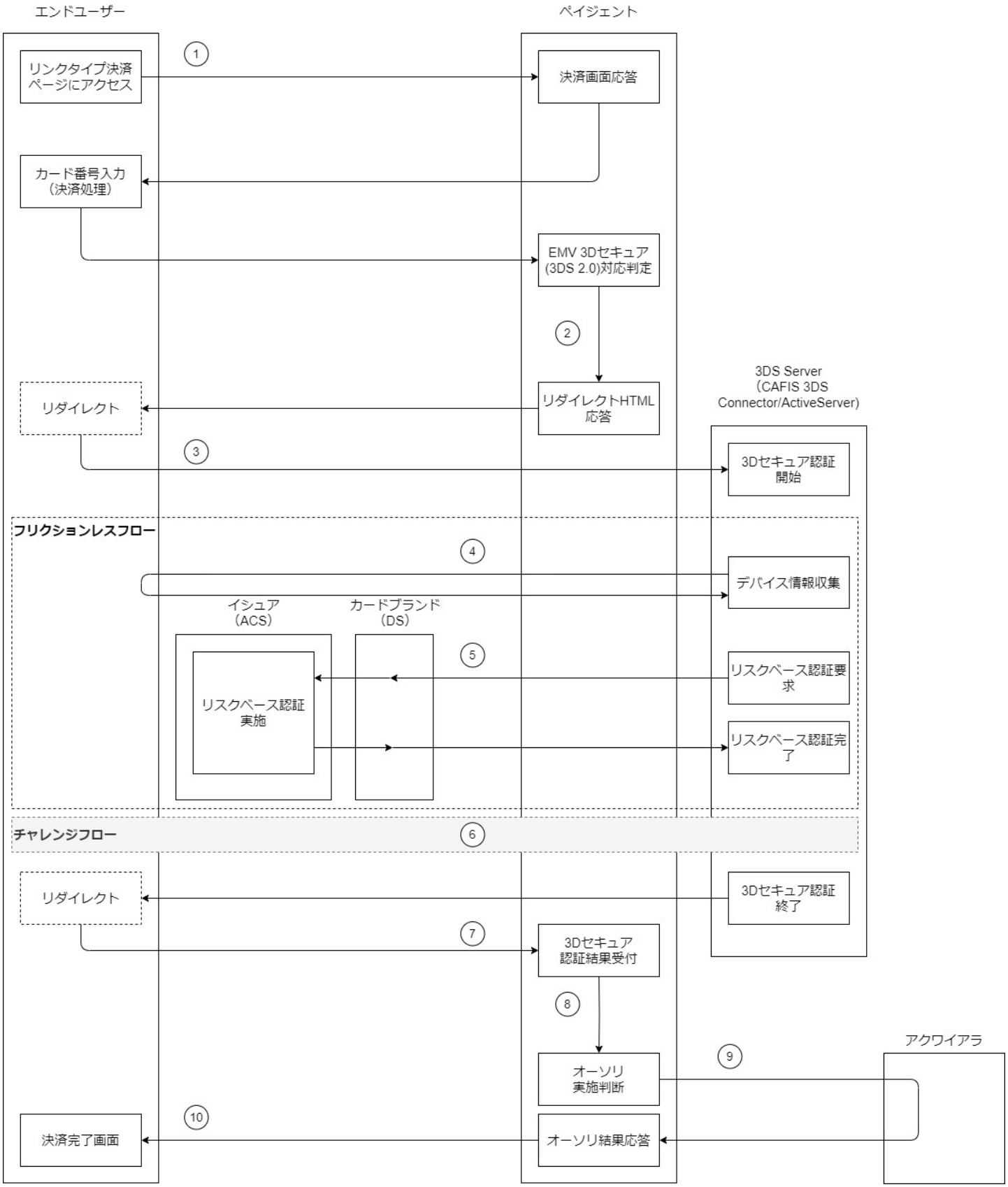
取引を継続可能な場合、ペイジェントへ各種決済を申込んでください。
決済申込みの際、インタフェース仕様書を参考に、3Dセキュア認証IDを指定してください。
EMV 3Dセキュア（3DS 2.0）認証に対応する決済申込み電文は以下のとおりです。
・カード決済申込（電文種別ID:020）
・カード決済申込(多通貨)（電文種別ID:180）
・Google Pay申込（電文種別ID:350）

10．取引完了

以上でEMV 3Dセキュア(3DS 2.0)を利用した取引は終了です。
ユーザーへ取引完了を通知してください。

＜ご注意＞
EMV 3Dセキュア認証済の決済でもオーソリ変更は可能です。
ただし、EMV 3Dセキュアを省略してオーソリを取り直す為、チャージバックリスクが発生しますので、ご留意下さい。

2.2.フリクションレスフローでの取引の流れ（リンクタイプ）



1．注文

ユーザーがリンクタイプ決済ページにアクセスし取引開始します。

※フォーム連携方式、URL連携方式共に同じ動作となります。
連携方式についてはリンクタイプインターフェース仕様説明書をご参照ください。

2．EMV 3Dセキュア(3DS 2.0)対応判定

ユーザーから入力されたカード情報と加盟店様の契約状況を元に、3Dセキュアの利用可否や利用バージョンを判定します。
EMV 3Dセキュア(3DS 2.0)が実施可能と判定された場合、ユーザーへEMV 3Dセキュア(3DS 2.0)の認証を開始するためのリダイレクトHTMLを応答します。

3．3Dセキュア認証開始

ユーザーがリダイレクトHTMLを表示すると、CAFIS 3DS Connectorへアクセスし、EMV 3Dセキュア（3DS 2.0）認証を開始します。

4．デバイス情報収集

CAFIS 3DS Connectorはユーザーからデバイス情報を収集します。

5．リスクベース認証実施

CAFIS 3DS Connectorは、イシュアへユーザーの行動情報・属性情報・取引情報等を送信します。
イシュアは、それらの情報をもとにリスクベース認証を行い、認証結果をCAFIS 3DS Connectorへ応答します。

6．チャレンジフロー

フリクションレスフローでリスク判定できない場合のみ、チャンレンジフローを実施します。
チャレンジフローについては「3．チャレンジフロー」をご参照ください。

7．ユーザーからペイジェントへ認証結果を通知

ユーザーからペイジェントへ認証結果が送信されます。

８．認証結果からオーソリ実施判定

認証結果・Attempt区分・Attemptオーソリ制御区分をもとに、ペイジェントにて取引継続の可否を判定します。
Attempt区分につきましては、「02_PG外部インターフェース仕様説明書（別紙：EMV 3Dセキュア）」記載の「1.2.EMV 3Dセキュア（3DS 2.0）認証結果応答電文」及び「Attemptについて」をご確認ください。
Attemptオーソリ制御区分につきましては「02_PG外部インターフェース仕様説明書」記載の「8. 3Dセキュア補足説明」をご確認ください

９．決済処理

取引を継続可能な場合、オーソリ処理を実施します。

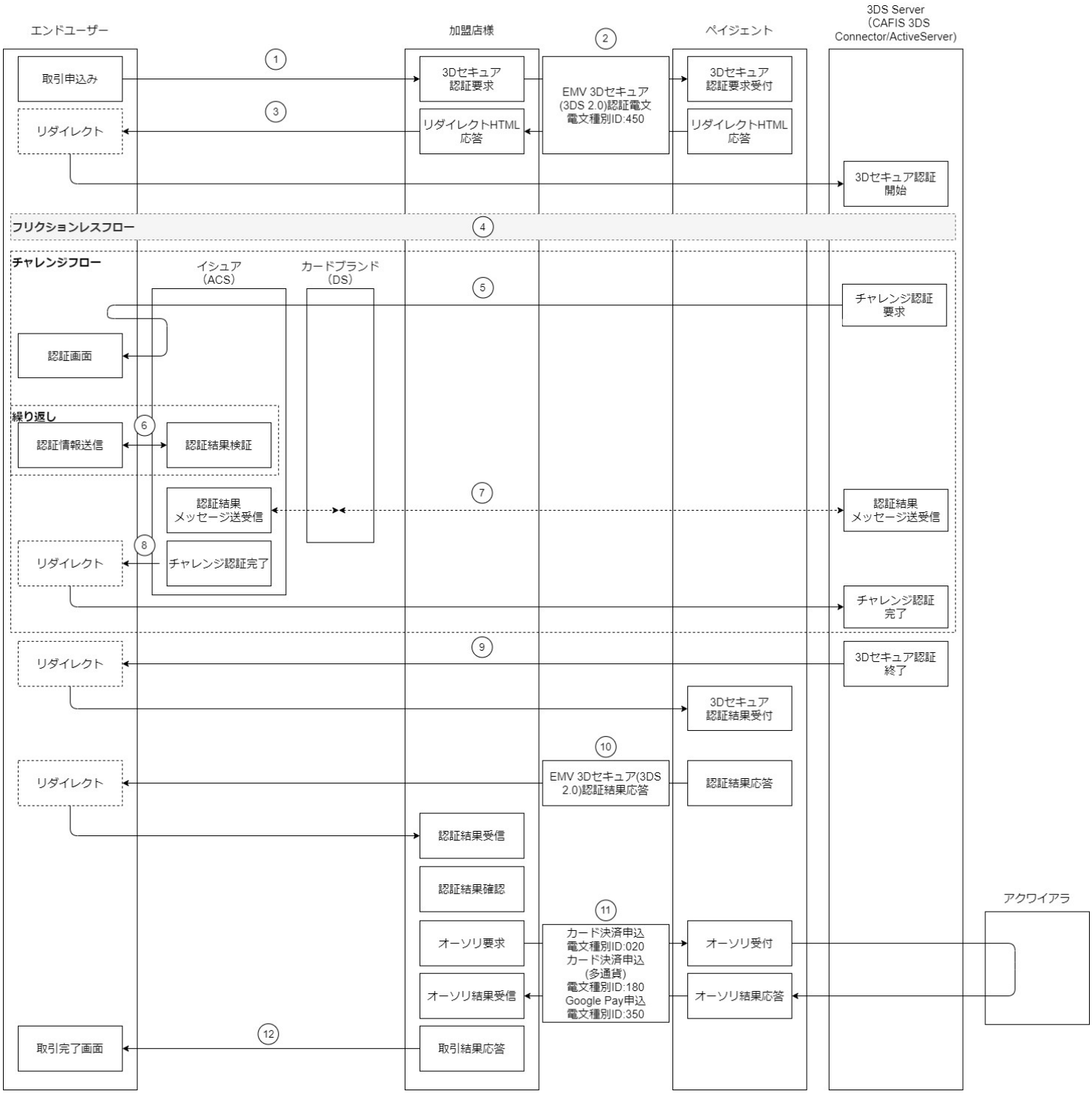
１０．取引完了

以上でEMV 3Dセキュア(3DS 2.0)を利用した取引は終了です。
以降はリンクタイプ決済の取引完了後のフローとなります。

＜ご注意＞
EMV 3Dセキュア認証済の決済でもオーソリ変更は可能です。
ただし、EMV 3Dセキュアを省略してオーソリを取り直す為、チャージバックリスクが発生しますので、ご留意下さい。

3.チャレンジフロー

3.1.チャレンジフローでの取引の流れ（モジュールタイプ）



1．注文

ユーザーがECサイトで取引を申込みます。

2．3Dセキュア認証申込み

加盟店様からペイジェントへ、「EMV 3Dセキュア（3DS 2.0）認証電文（電文種別ID:450）」でEMV 3Dセキュア(3DS 2.0)の認証を申込んでいただきます。
ペイジェントは加盟店様へ認証を開始するためのリダイレクトHTMLを応答します。

3．3Dセキュア認証開始

加盟店様は、[2]で取得したリダイレクトHTMLをユーザーへ応答してください。
ユーザーがリダイレクトHTMLを表示すると、CAFIS 3DS Connectorへアクセスし、EMV 3Dセキュア(3DS 2.0)認証を開始します。

4．フリクションレスフロー

フリクションレスフローについては「2．フリクションレスフロー」をご参照ください。

5．認証画面表示

3DS Serverは、ユーザーにイシュアが提供する認証画面を表示させます。

6．認証情報入力

ユーザーは認証画面で、認証情報を入力・送信します。
認証情報はイシュアのACSで検証され、認証情報に誤りがある場合、認証情報の再入力を求める場合があります。

7．認証結果メッセージ送受信

イシュアと3DS Serverの間でチャレンジ認証の結果が送受信されます。

８．チャレンジ認証終了

チャレンジ認証が終了すると、ユーザーは3DS Serverへ通信します。

９．ユーザーからペイジェントへ認証結果を通知

ユーザーからペイジェントへ認証結果が送信されます。

１０．ペイジェントから加盟店様へ認証結果を通知

ペイジェントから加盟店様へ認証結果を送信します。
加盟店様は、「EMV 3Dセキュア（3DS 2.0）認証結果応答電文」の処理結果・Attempt区分をもとに、取引継続の可否をご判断ください。
Attempt区分につきましては、「02_PG外部インターフェース仕様説明書（別紙：EMV 3Dセキュア）」記載の「1.2.EMV 3Dセキュア（3DS 2.0）認証結果応答電文」及び「Attemptについて」をご確認ください。

１１．決済を申込む

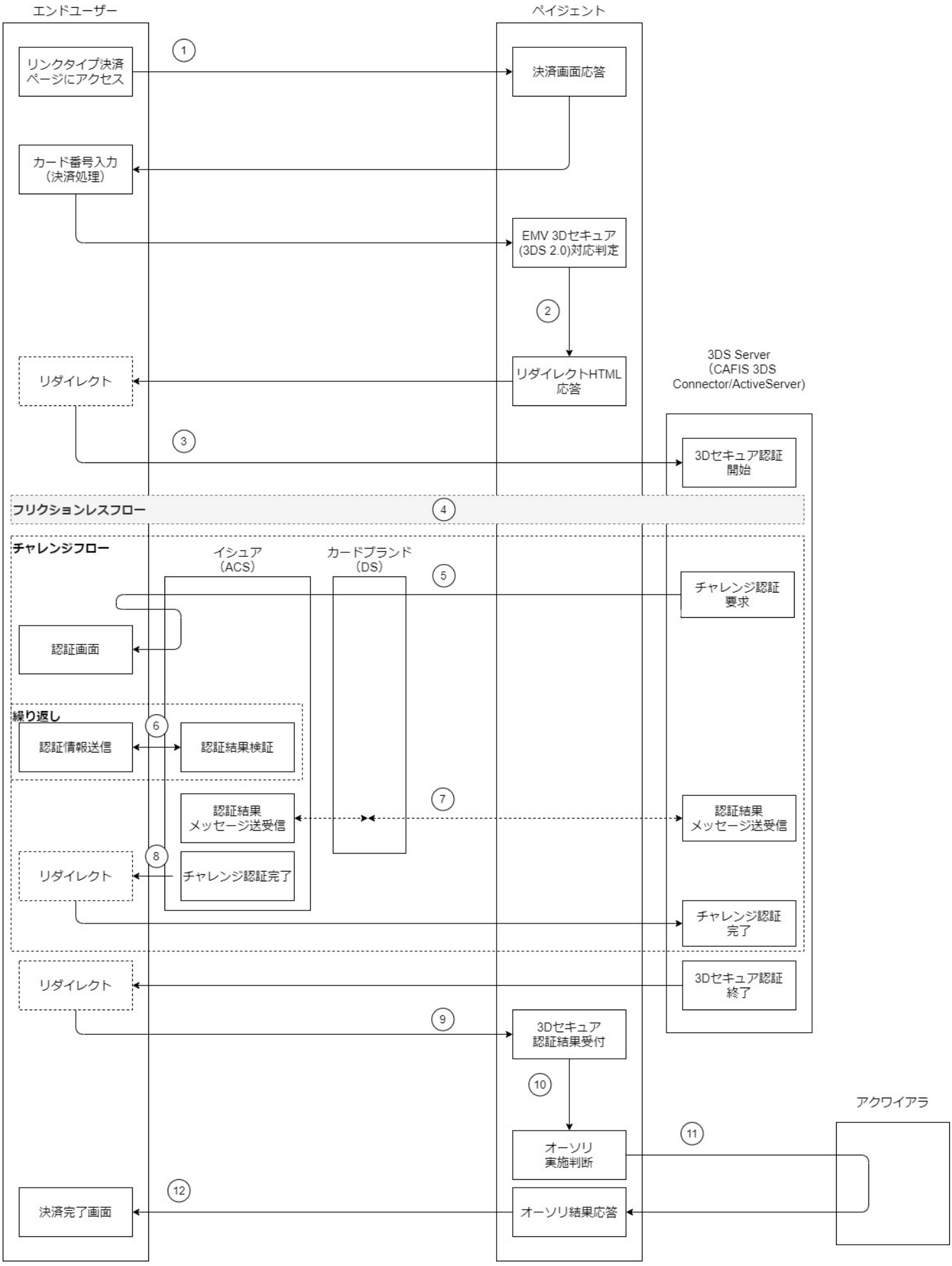
取引を継続可能な場合、ペイジェントへ各種決済を申込んでください。
決済申込みの際、インタフェース仕様書を参考に、3Dセキュア認証IDを指定してください。
EMV 3Dセキュア（3DS 2.0）認証に対応する決済申込み電文は以下のとおりです。
・カード決済申込（電文種別ID:020）
・カード決済申込(多通貨)（電文種別ID:180）
・Google Pay申込（電文種別ID:350）

１２．取引完了

以上でEMV 3Dセキュア(3DS 2.0)を利用した取引は終了です。
ユーザーへ取引完了を通知してください。

＜ご注意＞
EMV 3Dセキュア認証済の決済でもオーソリ変更は可能です。
ただし、EMV 3Dセキュアを省略してオーソリを取り直す為、チャージバックリスクが発生しますので、ご留意下さい。

3.2.チャレンジフローでの取引の流れ（リンクタイプ）



1．注文

ユーザーがリンクタイプ決済ページにアクセスし取引開始します。

※フォーム連携方式、URL連携方式共に同じ動作となります。
連携方式についてはリンクタイプインターフェース仕様説明書をご参照ください。

2．EMV 3Dセキュア(3DS 2.0)対応判定

ユーザーから入力されたカード情報と加盟店様の契約状況を元に、3Dセキュアの利用可否や利用バージョンを判定します。
EMV 3Dセキュア(3DS 2.0)が実施可能と判定された場合、ユーザーへEMV 3Dセキュア(3DS 2.0)の認証を開始するためのリダイレクトHTMLを応答します。

3．3Dセキュア認証開始

ユーザーがリダイレクトHTMLを表示すると、CAFIS 3DS Connectorへアクセスし、EMV 3Dセキュア（3DS 2.0）認証を開始します。

4．フリクションレスフロー

フリクションレスフローについては「2．フリクションレスフロー」をご参照ください。

5．認証画面表示

3DS Serverは、ユーザーにイシュアが提供する認証画面を表示させます。

6．認証情報入力

ユーザーは認証画面で、認証情報を入力・送信します。
認証情報はイシュアのACSで検証され、認証情報に誤りがある場合、認証情報の再入力を求める場合があります。

7．認証結果メッセージ送受信

イシュアと3DS Serverの間でチャレンジ認証の結果が送受信されます。

８．チャレンジ認証終了

チャレンジ認証が終了すると、ユーザーは3DS Serverへ通信します。

９．ユーザーからペイジェントへ認証結果を通知

ユーザーからペイジェントへ認証結果が送信されます。

１０．認証結果からオーソリ実施判定

認証結果・Attempt区分・Attemptオーソリ制御区分をもとに、ペイジェントにて取引継続の可否を判定します。
Attempt区分につきましては、「02_PG外部インターフェース仕様説明書（別紙：EMV 3Dセキュア）」記載の「1.2.EMV 3Dセキュア（3DS 2.0）認証結果応答電文」及び「Attemptについて」をご確認ください。
Attemptオーソリ制御区分につきましては「02_PG外部インターフェース仕様説明書」記載の「8. 3Dセキュア補足説明」をご確認ください

１１．決済処理

取引を継続可能な場合、オーソリ処理を実施します。

１２．取引完了

以上でEMV 3Dセキュア(3DS 2.0)を利用した取引は終了です。
以降はリンクタイプ決済の取引完了後のフローとなります。

＜ご注意＞
EMV 3Dセキュア認証済の決済でもオーソリ変更は可能です。
ただし、EMV 3Dセキュアを省略してオーソリを取り直す為、チャージバックリスクが発生しますので、ご留意下さい。

4.ECサイト組み込みにあたって

4.1.本人認証サービスロゴの表示について

国際ブランドが定める本人認証サービスのロゴをECサイトに掲載してください。

ブランドロゴファイル及びガイドラインは加盟店サポートサイト
（https://support.paygent.co.jp）でダウンロードできます。
カテゴリー検索から、[ロゴデータ > カードに関するロゴ]と進んでダウンロードしてください。

4.2.個人情報保護法上の義務と対応について

EMV 3Dセキュア(3DS 2.0)では、加盟店様が取得した会員に関する情報はペイジェント及び3DSサーバーを通じイシュアに送信されます。
この情報は加盟店様にとって会員の個人データに当たる為、関係法令および個人情報保護委員会のガイドラインならびに日本クレジット協会（JCA）の法令解釈等に従い、予め会員からの同意取得が必要となります。
3Dセキュア認証を実施する際、会員に同意取得文言を明示していただくようお願いします。

同意取得文言の記載例を以下に示します。

サンプル：同意取得文言

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。

4.3.通信モジュールについて

通信モジュールをご利用の加盟店様は、文字コード：UTF-8に対応した最新の通信モジュールをご利用いただくようお願いします。文字コード：UTF-8に対応していない旧通信モジュールを使用し、「EMV 3Dセキュア（3DS 2.0）認証電文（電文種別ID:450）」の全角文字を使用する項目（例：請求先情報（住所1））を使用した場合、文字化けが発生し正常な認証結果を得ることが出来ません。

5.試験環境を利用する

ペイジェントの提供する試験環境でEMV 3Dセキュア(3DS 2.0)認証電文の動作確認をする方法を以下に示します。
設定値に応じてペイジェント返却値を定めています。本章に記載の決済金額、カード名義人両方を設定した場合、返却値はカード名義人の値となります。
（例.設定値に決済金額：0（チャレンジ認証返却値の条件）かつ、カード名義人：BAJYA（リスクベース認証 - 正常ケースNo1の返却値のの条件）を設定した場合、リスクベース認証 - 正常ケースNo1の返却値となります。）

5.1.リスクベース認証の返却値を確認する

試験環境のEMV 3Dセキュア（3DS 2.0）認証電文では、要求情報の決済金額または、カード名義人を元にリスクベース認証の返却値を制御します。
本章に記載されていない ブランド 、決済金額またはカード名義人 の組み合わせに対する ペイジェント返却値 についてはサポート対象外になります。

リスクベース認証 - 正常ケース

No	ブランド	設定値	ペイジェント返却値		
		決済金額　or　カード名義人	処理結果	attempt区分	レスポンスコード
1	JCB	313,510　or　BAJYA	0	-	-
2		313,520　or　BAJAA	0	0	-
3		313,550　or　BAJUA	0	1	-
4		313,560　or　BAJRA	1	-	31007
5	Diners	313,610　or　BADYA	0	-	-
6		313,620　or　BADAA	0	0	-
7		313,640　or　BADNA	1	-	31007
8		313,650　or　BADUA	0	1	-
9		313,660　or　BADRA	1	-	31007
10	AMEX	313,710　or　BAAYA	0	-	-
11		313,740　or　BAANA	1	-	31007
12		313,750　or　BAAAA	0	0	-
13		313,751　or　BAAUA	0	1	-
14		313,760　or　BAARA	1	-	31007

リスクベース認証 - 正常ケース

No	ブランド	設定値	ペイジェント返却値		
		決済金額　or　カード名義人	処理結果	attempt区分	レスポンスコード
15	VISA	314,010 or BAVYA	0	-	-
16		314,020 or BAVAA	0	0	-
17		314,040 or BAVNA	1	-	31007
18		314,050 or BAVUA	0	1	-
19		314,060 or BAVRA	1	-	31007
20	MasterCard	315,010 or BAMYA	0	-	-
21		315,020 or BAMAA	0	0	-
22		315,040 or BAMNA	1	-	31007
23		315,050 or BAMUA	0	1	-
24		315,060 or BAMRA	1	-	31007

リスクベース認証 - 異常ケース

No	シナリオ	設定値	ペイジェント返却値		
		決済金額　or　カード名義人	処理結果	attempt区分	レスポンスコード
1	ActiveServerよりエラー応答	221,001 or BBErrABAB	0	1	-
2	CAFIS 3DS Connectorにて取引タイムアウト発生	130,000 or BCErrTimeOut	0	1	-
3	CAFIS 3DS Connectorより報告電文チェックエラー応答	140,000 or BDErrInvalidInput	0	1	-

5.2.チャレンジ認証の返却値を確認する

試験環境のEMV 3Dセキュア（3DS 2.0）認証電文では、要求情報の決済金額に「0」または「1」または「200,000」または「400,000」、またはカード名義人にブランド毎の値を設定することで認証画面へ遷移し、認証画面のパスワードを元にチャレンジ認証の返却値を制御します。
本章に記載されていない ブランド 、決済金額またはカード名義人、パスワード の組み合わせに対する ペイジェント返却値 についてはサポート対象外になります。

チャレンジ認証 - 正常ケース

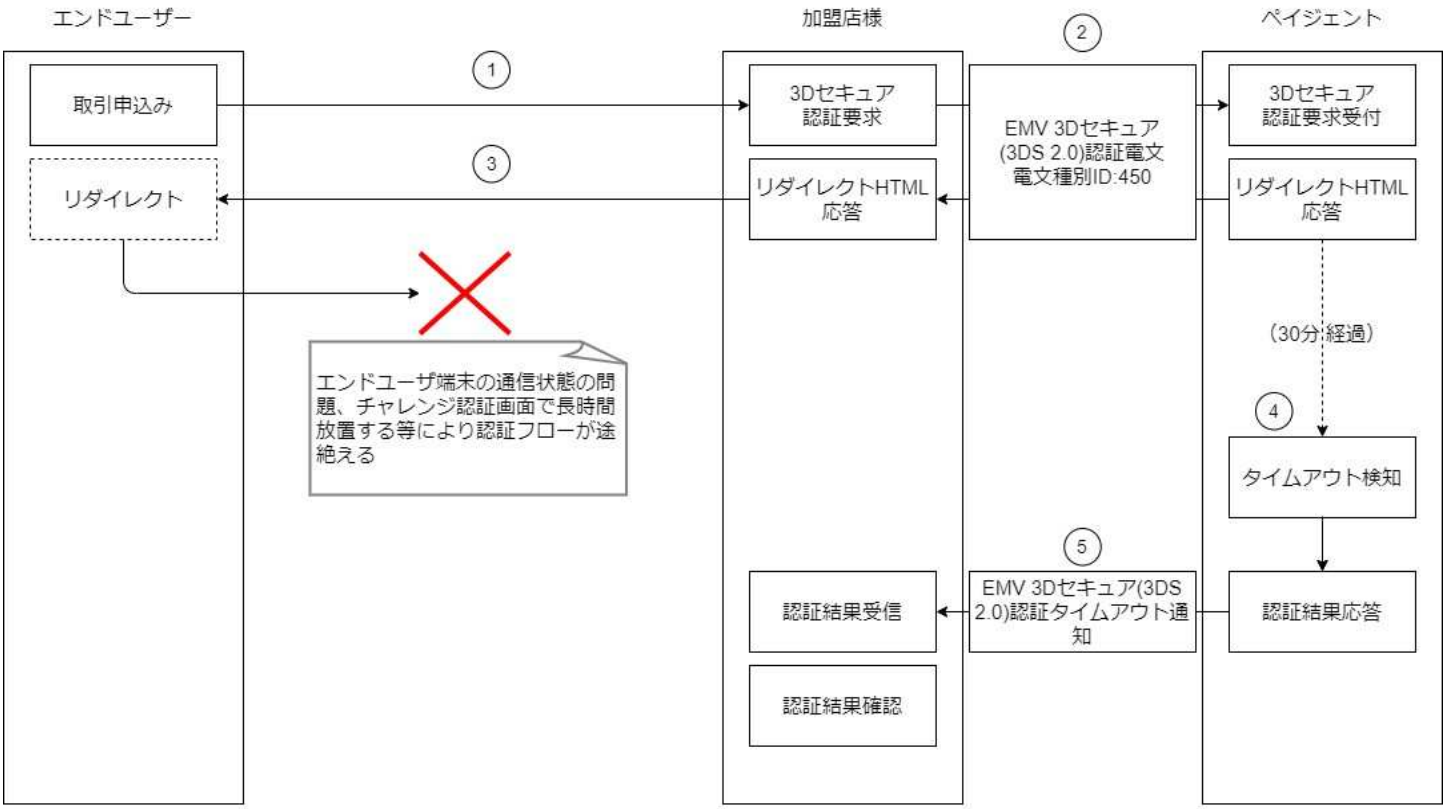
No	ブランド	設定値		ペイジェント返却値		
		決済金額 or カード名義人	パスワード	処理結果	attempt区分	レスポンスコード
1	JCB	0 or 1 or 200,000 or 400,000 or BAJCA	13512	0	-	-
2			13542	1	-	31007
3			13552	0	1	-
4	Diners	0 or 1 or 200,000 or 400,000 or BADCA	13612	0	-	-
5			13642	1	-	31007
6			13652	0	1	-
7	AMEX	0 or 1 or 200,000 or 400,000 or BAACA	13712	0	-	-
8			13742	1	-	31007
9			13752	0	1	-
10	VISA	0 or 1 or 200,000 or 400,000 or BAVCA	14012	0	-	-
11			14042	1	-	31007
12			14052	0	1	-
13	MasterCard	0 or 1 or 200,000 or 400,000 or BAMCA	15012	0	-	-
14			15042	1	-	31007
15			15052	0	1	-

チャレンジ認証 - 異常ケース

No	シナリオ	設定値		ペイジェント返却値		
		決済金額 or カード名義人	パスワード	処理結果	attempt区分	レスポンスコード
1	ActiveServerよりエラー応答	0 or 1 or 200,000 or 400,000 or BAJCA or BADCA or BAACA or BAVCA or BAMCA	51001	0	1	-
2	CAFIS 3DS Connectorにて取引タイムアウト発生		30000	0	1	-
3	CAFIS 3DS Connectorより報告電文チェックエラー応答		40000	0	1	-

6.認証タイムアウト通知

6.1.認証タイムアウト通知の流れ



1．注文

ユーザーがECサイトで取引を申込みます。

2．3Dセキュア認証申込み

加盟店様からペイジェントへ、「EMV 3Dセキュア（3DS 2.0）認証電文（電文種別ID:450）」でEMV 3Dセキュア(3DS 2.0)の認証を申込んでいただきます。
ペイジェントは加盟店様へ認証を開始するためのリダイレクトHTMLを応答します。

3．3Dセキュア認証開始

加盟店様は、[2]で取得したリダイレクトHTMLをユーザーへ応答してください。
ユーザーがリダイレクトHTMLを表示すると、CAFIS 3DS Connectorへアクセスし、EMV 3Dセキュア（3DS 2.0）認証を開始します。

4．タイムアウト検知

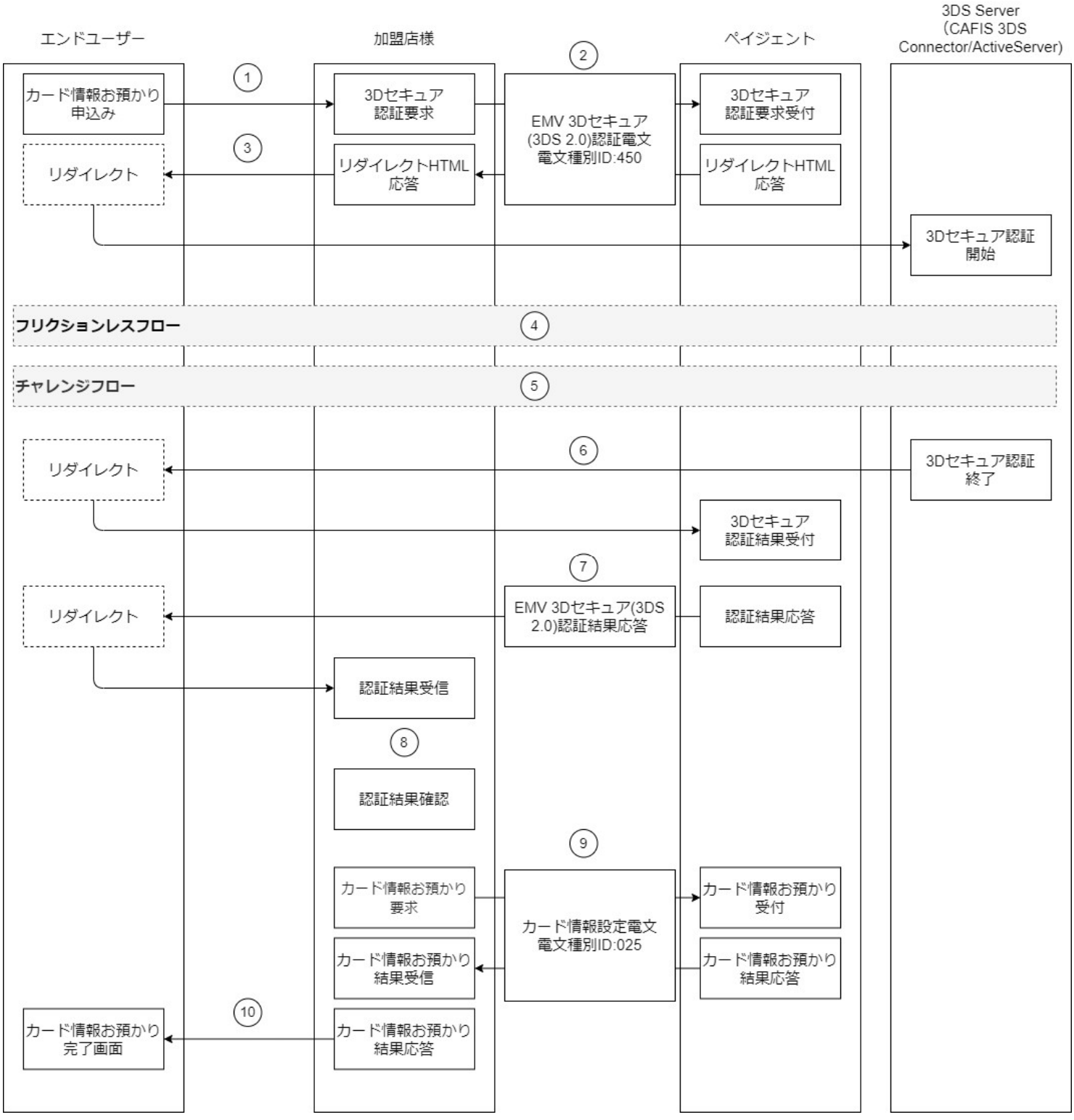
ペイジェントから加盟店様へリダイレクトHTMLを応答後、30分以内にユーザーからペイジェントへ認証結果が送信されなかった場合は、当該取引のステータスをタイムアウトに更新します。

5．ペイジェントから加盟店様へ認証結果を通知

ペイジェントから加盟店様へ認証結果（31013：認証タイムアウト）を送信します。
加盟店様は、「EMV 3Dセキュア（3DS 2.0）認証タイムアウト通知電文」を受信後、「3Dセキュア認証ID」を元に該当取引を特定することができます。
※「3Dセキュア認証ID」は「EMV 3Dセキュア（3DS 2.0）認証電文（電文種別ID:450）」の応答項目になります。

7.カード情報お預かり

7.1.EMV 3Dセキュア(3DS 2.0)を利用したカード情報お預かりの流れ（モジュールタイプ）



1．カード情報お預かり申込

ユーザーがECサイトでカード情報お預かりを申込みます。

2．3Dセキュア認証申込み

加盟店様からペイジェントへ、「EMV 3Dセキュア（3DS 2.0）認証電文（電文種別ID:450）」でEMV 3Dセキュア(3DS 2.0)の認証を申込んでいただきます。
※決済金額には0円か1円をご設定ください。
ペイジェントは加盟店様へ認証を開始するためのリダイレクトHTMLを応答します。

3．3Dセキュア認証開始

加盟店様は、[2]で取得したリダイレクトHTMLをユーザーへ応答してください。
ユーザーがリダイレクトHTMLを表示すると、CAFIS 3DS Connectorへアクセスし、EMV 3Dセキュア認証を開始します。

4．フリクションレスフロー

フリクションレスフローについては「2．フリクションレスフロー」をご参照ください。

5．チャレンジフロー

チャレンジフローについては「3．チャレンジフロー」をご参照ください。

6．ユーザーからペイジェントへ認証結果を通知

ユーザーからペイジェントへ認証結果が送信されます。

7. ペイジェントから加盟店様へ認証結果を通知

ペイジェントから加盟店様へ認証結果を送信します。

8. 認証結果の確認

加盟店様は、「EMV 3Dセキュア（3DS 2.0）認証結果応答電文」の処理結果・Attempt区分をもとに、カード情報お預かり処理の継続の可否をご判断ください。
Attempt区分につきましては、「02_PG外部インターフェース仕様説明書（別紙：EMV 3Dセキュア）」記載の「1.2.EMV 3Dセキュア（3DS 2.0）認証結果応答電文」及び「Attemptについて」をご確認ください。

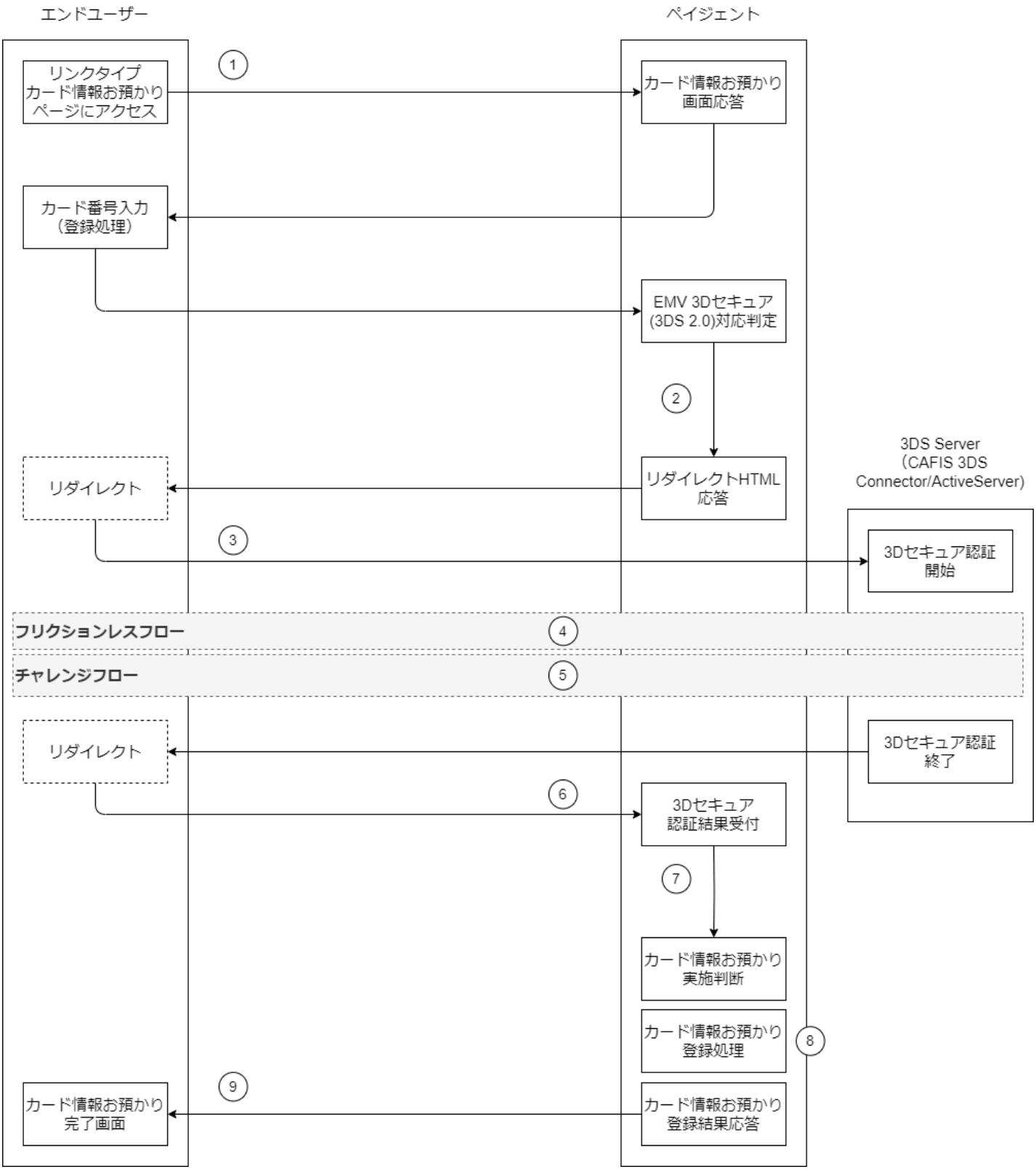
9. カード情報を預ける

カード情報お預かり処理を継続する場合、ペイジェントへ「カード情報設定電文（電文種別：025）」を申込ください。
その際、有効性チェックのご利用は加盟店様の任意となります。

10. 取引完了

以上でEMV 3Dセキュア(3DS 2.0)を利用したカード情報お預かりは終了です。
ユーザーへカード情報お預かり完了を通知してください。

7.2.EMV 3Dセキュア(3DS 2.0)を利用したカード情報お預かりの流れ（リンクタイプ）



1．カード情報お預かり申込

ユーザーがリンクタイプカード情報お預かりページにアクセスします。

※フォーム連携方式、URL連携方式共に同じ動作となります。
連携方式についてはリンクタイプインターフェース仕様説明書をご参照ください。

2．EMV 3Dセキュア(3DS 2.0)対応判定

ユーザーから入力されたカード情報と加盟店様の契約状況を元に、3Dセキュアの利用可否や利用バージョンを判定します。
EMV 3Dセキュア(3DS 2.0)が実施可能と判定された場合、ユーザーへEMV 3Dセキュア(3DS 2.0)の認証を開始するためのリダイレクトHTMLを応答します。

3．3Dセキュア認証開始

ユーザーがリダイレクトHTMLを表示すると、CAFIS 3DS Connectorへアクセスし、EMV 3Dセキュア（3DS 2.0）認証を開始します。

4．フリクションレスフロー

フリクションレスフローについては「2．フリクションレスフロー」をご参照ください。

5．チャレンジフロー

チャレンジフローについては「3．チャレンジフロー」をご参照ください。

6．ユーザーからペイジェントへ認証結果を通知

ユーザーからペイジェントへ認証結果が送信されます。

7. 認証結果からカード情報お預かり実施判定

認証結果・Attempt区分・Attemptオーソリ制御区分をもとに、ペイジェントにて処理継続の可否を判定します。
Attempt区分につきましては、「02_PG外部インターフェース仕様説明書（別紙：EMV 3Dセキュア）」記載の「1.2.EMV 3Dセキュア（3DS 2.0）認証結果応答電文」及び「Attemptについて」をご確認ください。
Attemptオーソリ制御区分につきましては「02_PG外部インターフェース仕様説明書」記載の「8. 3Dセキュア補足説明」をご確認ください

8. カード情報お預かり登録処理

処理を継続可能な場合、カード情報お預かり登録処理を実施します。

9. 取引完了

以上でEMV 3Dセキュア(3DS 2.0)を利用した取引は終了です。
以降はリンクタイプカード情報お預かりの取引完了後のフローとなります。