

クレジットカード トークン方式
3Dセキュア2.0
(概要・処理フロー・画面フロー)

■概要

- :対応ブラウザ.....P.3
- :トークン決済方式について.....P.4
- :3Dセキュア2.0についてP.5
- :3Dセキュア2.0 画面フローP.6
- :3Dセキュア2.0 処理フロー(ポップアップ方式) ..P.7
- :3Dセキュア2.0 処理フロー(カスタマイズ方式) ..P.8

対応ブラウザ

対応ブラウザは以下です。

- Internet Explorer (Microsoftがサポート対象としているバージョンに限る)
- Microsoft Edge 最新版
- Google Chrome 最新版
- Firefox 最新版
- Safari 最新版

※JavaScriptの利用できない端末(一部フィーチャーフォン等)では、トークン決済を行う事が出来ません。

トークン決済方式について

トークン決済ではユーザーが入力するクレジットカード情報を、別の文字列(トークン)に置き換えて決済を行います。クレジットカード番号を保持することなく決済が完了でき、情報漏洩リスクを軽減できる方法です。

トークン決済にはポップアップ方式・カスタマイズ方式の2種類があります。

【ポップアップ方式】

加盟店様のカード情報入力フォームの実装が不要な方式です。

JavaScriptでユーザーのブラウザ内に弊社が用意した決済画面をポップアップで表示します。入力されたカード情報をトークンに置き換えて加盟店様へ返却し、最終的にそのトークンを用いて決済リクエストを行います。

<ポップアップ方式決済画面イメージ>



The image shows a popup window titled "クレジットカード情報を入力してください" (Please enter your credit card information). At the top, there are logos for VISA, Mastercard, JCB, American Express, Diners Club International, and DISCOVER. Below the logos, there are input fields for: "カード番号" (Card number) with the example "4444 3333 2222 1111" and a note "(半角数字)"; "有効期限" (Expiration date) with two dropdown menus and a note "(月/年)"; "カード名義" (Card name) with two fields: "TAROU" (name) and "YAMAMOTO" (surname), with a note "(姓) (半角文字のみ)". At the bottom, there are two red buttons: "閉じる" (Close) and "確定" (Confirm).

【カスタマイズ方式】

加盟店様のカード情報入力フォームの実装が必要な方式です。

加盟店様サイト内にカード情報入力画面を実装します。入力されたカード情報を、JavaScriptで弊社サーバーへ送信し、弊社はカード情報をトークンに置き換えて返却します。最終的にそのトークンを用いて決済リクエストを行います。

※以下の決済方式は3DS認証が行われません。

- ・再オーソリ
- ・実売上(SALES)

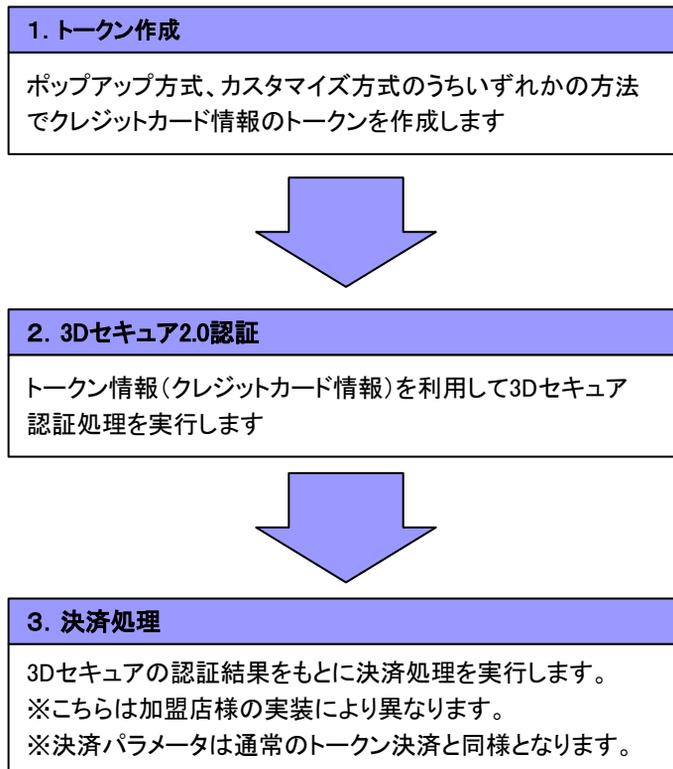
3Dセキュア2.0について

3Dセキュア2.0はEMVCo(国際カードブランド6社によるカード決済の安全、促進のための団体)によって作成された3Dセキュアの改良版となります。従来どおり本人認証を行いながら、不正利用のリスクが低ければ本人認証画面をスキップするフリクションレスフローが導入されました。3Dセキュアの最大のメリットとして、ネット決済でも実店舗での決済と同様に本人確認をすることができるために、加盟店様で「なりすまし被害」等によるチャージバックを防ぐことができる点があげられます。

■3Dセキュアご利用のご注意点

3Dセキュアの認証には通常のトークン決済方式に追加で3Dセキュア認証用ソースコードを準備する必要があります。3Dセキュアの認証方法、サンプルソースにつきましては次ページ以降をご確認ください。

■実装イメージ



3Dセキュア2.0 画面フロー

① 購入確認

確認画面

加盟店様側で実装した購入画面より決済処理を開始します。



トークンポップアップ：弊社が用意した入力フォーム
 トークンカスタマイズ：加盟店様が実装した入力フォーム

② カード情報入力

カード番号のトークン化

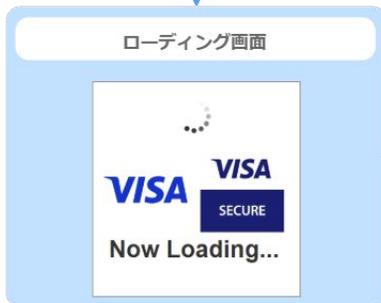
クレジットカード番号のトークン化はポップアップ方式、カスタマイズ方式のどちらかを選択します。ポップアップ方式は弊社で用意したカード情報入力フォームを使用します。カスタマイズ方式は加盟店様側でカード情報入力フォームを実装します。



③ 本人認証

リスクベース認証

カード会員様のリスク度合いに応じてフリクションレス認証、チャレンジ認証へ分岐します。低リスクと判定された場合はカード会員様側で操作不要で取引完了となります。それ以外の場合は本人を確認する認証を実施するフロー（チャレンジ認証）となります。



※チャレンジ認証画面・認証方法はカード会社ごとに異なります。



④ 完了画面

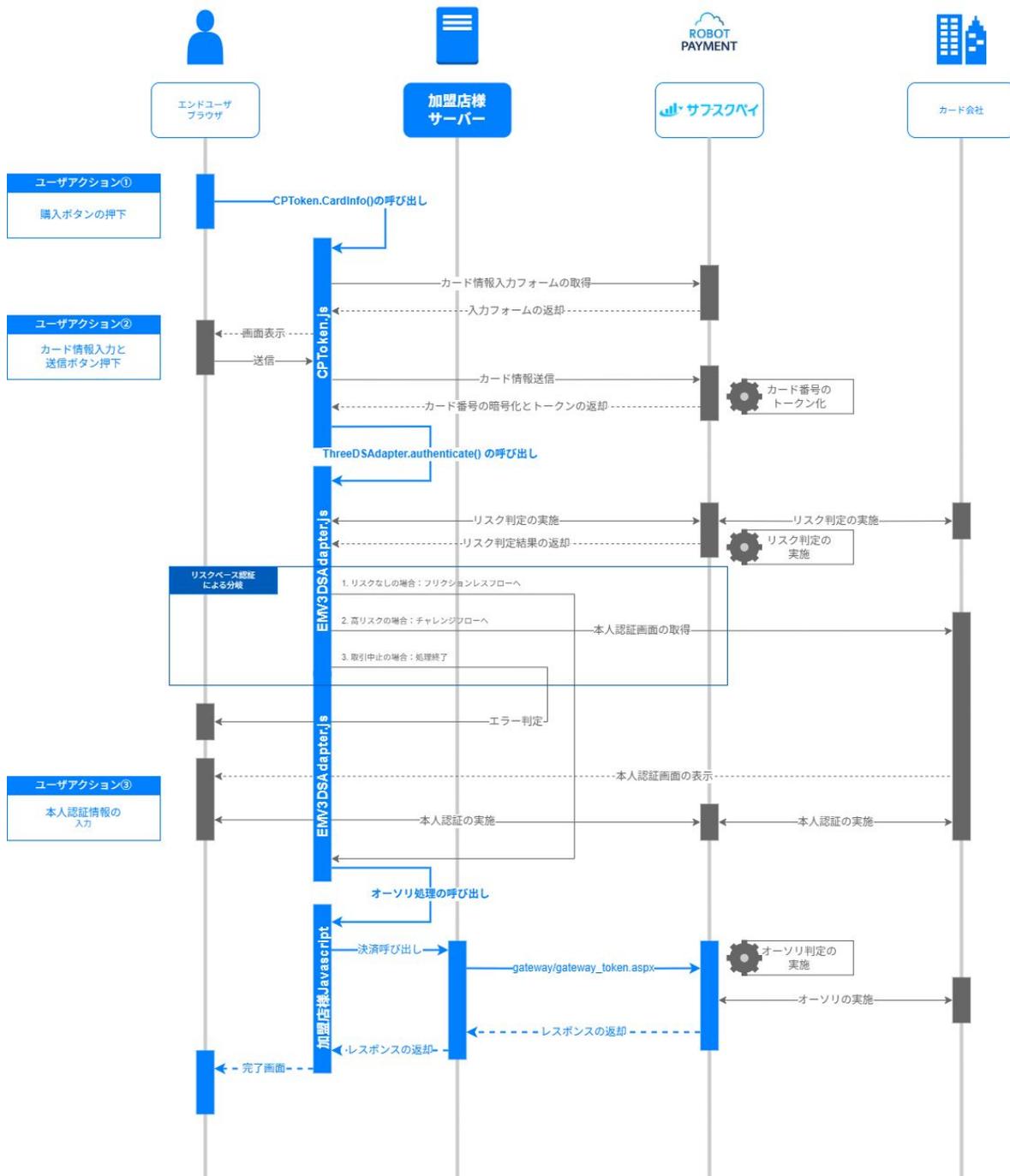
認証完了後に決済実施

認証を完了したあと決済を実施します。

フリクションレス認証



3Dセキュア2.0 処理フロー(ポップアップ方式)



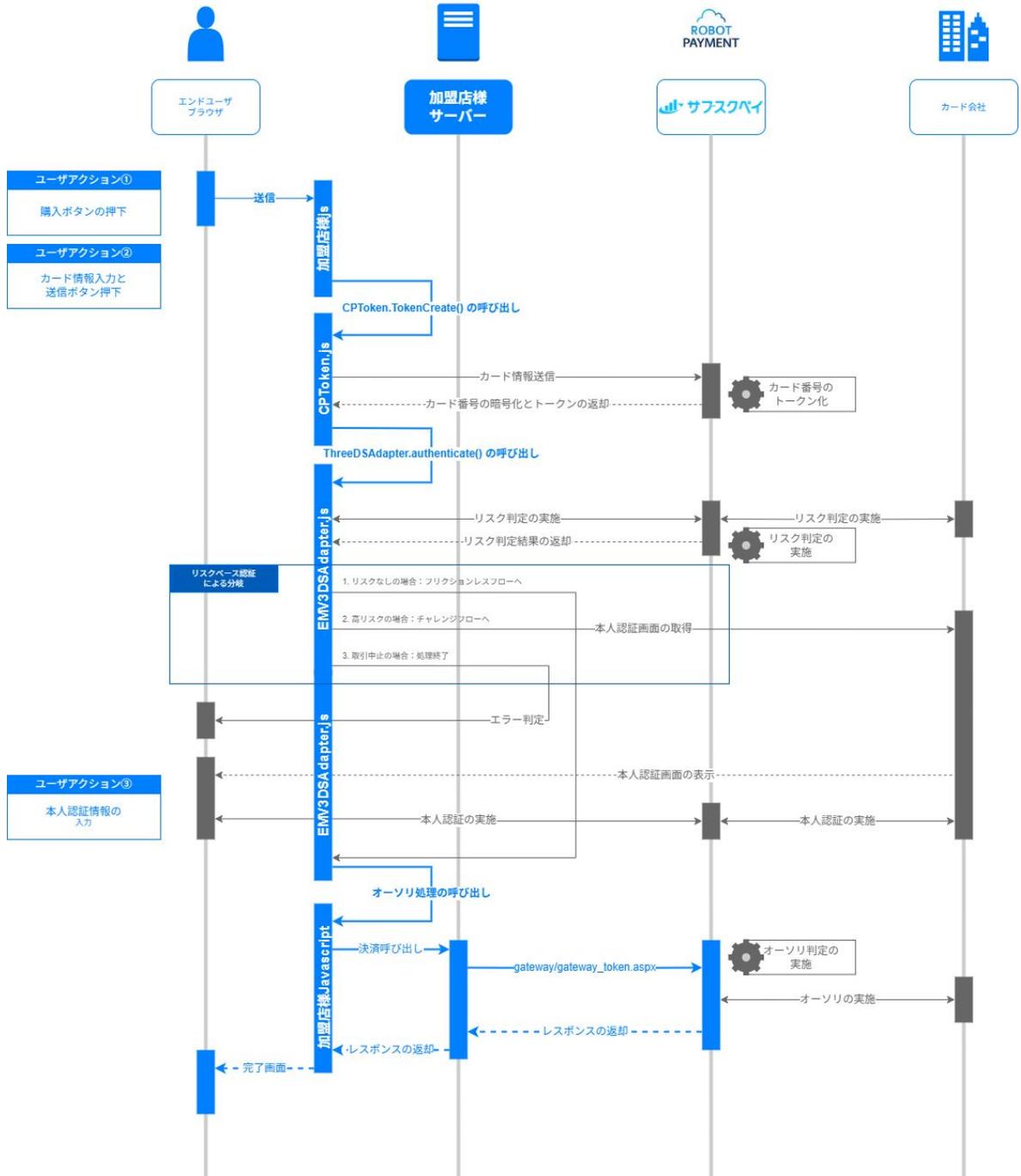
凡例

- 自動的に行われる処理 —
- 加盟店様が実装する処理 —

ご注意事項

- エラーの場合の画面表示（コールバック処理）は加盟店様側で実装してください。
- 弊社のJavaScript内で使用しているため、実装の際に「rpmvtds」クラスを使用しないでください。

3Dセキュア2.0 処理フロー(カスタマイズ方式)



凡例

- 自動的に行われる処理 — (Automatic processing)
- 加盟店様が実装する処理 — (Processing implemented by merchant)

ご注意事項

- トークン作成時のカード番号を決済リクエストに含めないでください。
- エラーの場合の画面表示（コールバック処理）は加盟店様側実装してください。
- 弊社のJavaScript内で使用しているため、実装の際に「rpmvtds」クラスを使用しないでください。