認証処理

3DSリクエスターは、認証中に次の3つの処理を実行します。

1. **認証の初期化**ー3DSリクエスターは**ActiveServer**にリクエストを送信して認証を初期化し、認証を行えるよう**ActiveServer**を準備します。
2. **認証の実行**ー**ActiveServer**は認証を実行します。3DS2には2つの主要な認証フロー**フリクションレス・フロー**と**チャレンジ・フロー**があります。これらについては処理フローの項で説明します。
3. **認証結果の取得**ー3DSリクエスターに認証結果が返されます。

処理 1: 認証の初期化

このステップで、フロントエンドの**3DS web adapter**はカード会員が入力した情報を取り込み、バックエンドの**3DSリクエスター**に渡します。次に**3DSリクエスター**は、3DS2から要求されたすべての情報を**ActiveServer**に渡し、認証処理が開始されます。

実装方法まとめのサンプルで、利用者が***Checkout***を選択すると、**3DS web adapter**が3DSリクエスターに `認証の初期化` メッセージを送信します。

3DSリクエスターは `認証の初期化` メッセージを受信し、ActiveServer認証APIに適合する形式にし、一意の**3DS Requestor transaction ID**(`threeDSRequestorTransID`)を生成して、メッセージへ追加します。メッセージのデータ項目が揃いましたら、メッセージは**ActiveServer**へ送信されます(**`/api/v2/auth/brw/init`**)。

ActiveServerが `認証の初期化` メッセージを受信するとチェックアウトページで**3DSリクエスター**がページフォワーディングをセットアップするためのコールバックURL(`threeDSServerCallbackUrl`)を返却します(`3DS Web Adapter` のコールバックは隠されたiframeを使用します）。このiframeが設置されることで、**ActiveServer**は、ブラウザー情報を収集し、認証処理を行える状態になります。

> **備考**
>
> 3DSサーバーとACSは自動的にブラウザー情報を収集します。この処理の概要は**3DSリクエスター**には含まれ**ません**。

Requestor Browser Collection (RBC)

ActiveServeによる自動での処理の代わりに3DSリクエスターでブラウザ情報を収集したい場合もあると思います。ActiveServerは、異なる環境に適応し、ブラウザ情報の受信をサポートすることで、リクエスターがページフローをよりコントロールできるようにすることができます。

デフォルトのブラウザ情報収集処理をスキップするには、`/auth/brw/init` リクエストの任意パラメータ `skipAutoBrowserInfoCollect` をご利用ください。このパラメータに `true` が設定されている場合、ActiveServerはブラウザ情報収集処理を実施**しません**。

その際、3DSリクエスターはJavascriptを使ってユーザーのブラウザからブラウザ情報を収集し、`browserUserAgent` や `browserIP` などのサーバー側のブラウザ情報フィールドを収集する実装をする必要があります。詳細については、 サンプルコード をご参照ください。

`skipAutoBrowserInfoCollect` に `true` が設定されていた場合、 `/auth/brw/init` リクエストでの `acctNumber` は**任意パラメータ**になります。 `acctNumber` が設定されていない場合、3DSメソッドはスキップされます。

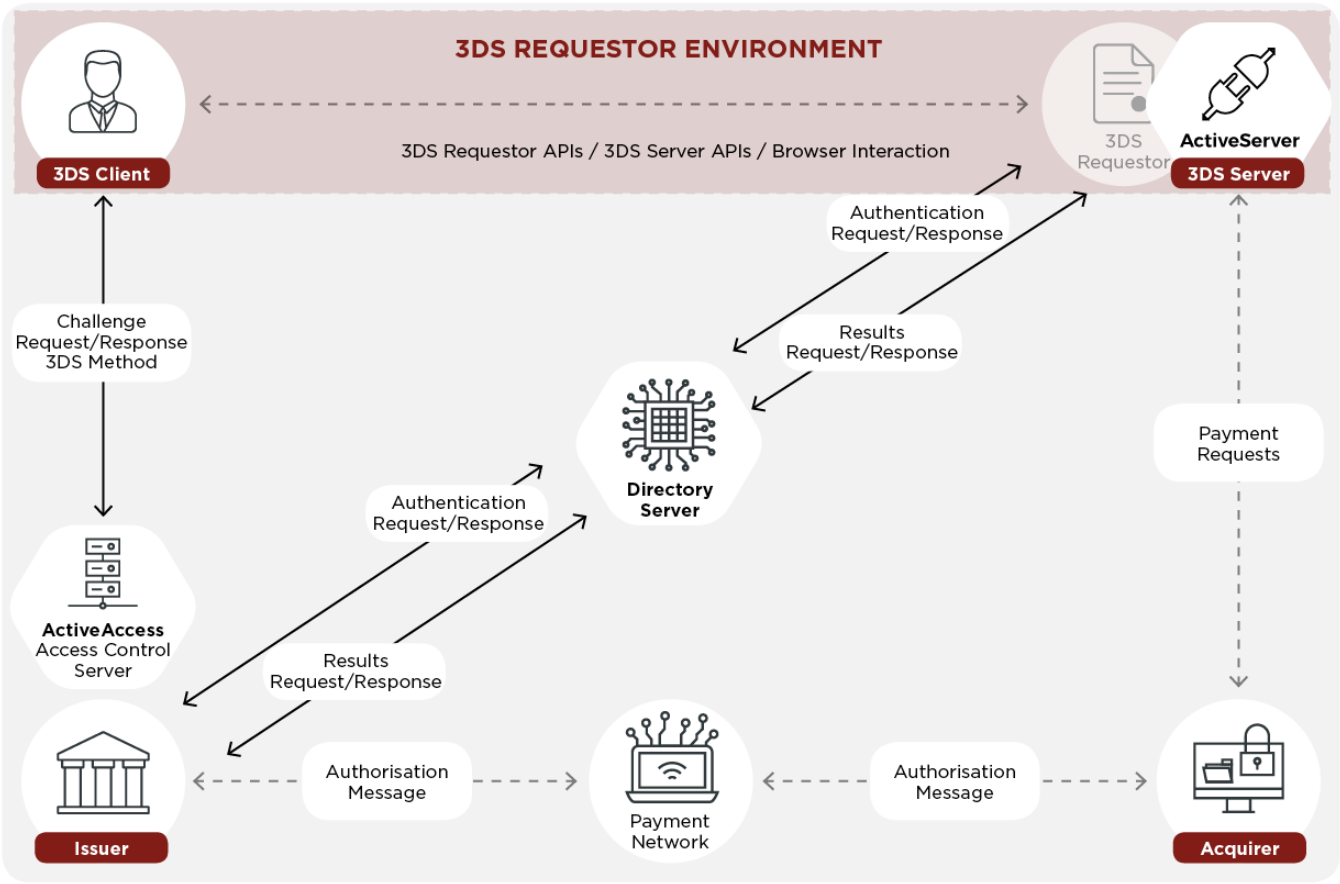
`/auth/brw/init` のレスポンスに含まれている `threeDSMethodAvailable` は、提供された `acctNumber` で3DSメソッド処理が利用できるかを意味し、 `threeDSServerCallbackUrl` の実行を希望するかどうか選択可能にします。 `/auth/brw/init` で `acctNumber` が提供されなかった場合、 `/auth/brw` リクエストで提供されるカードレンジに関わらず、 `threeDSMethodAvailable` には `false` が設定されます。

処理 2: 認証の実行

ブラウザー情報の収集が完了すると、加盟店は **`/api/v2/auth/brw`** を呼び出して認証を実行できます。この処理が実行されると、**ActiveServer**が3DS2メッセージング処理を開始します。3DS2には2つの主要な認証フロー**フリクションレス・フロー**と**チャレンジ・フロー**があります。

- **フリクションレス・フロー**ー**AReq/ARes**認証メッセージからなる3Dセキュア認証フローを開始します。 与えられた情報から取引が低リスクであるとACSが判断した場合は、直ちに認証が承認されます。
- **チャレンジ・フロー**ー取引が特定の許容限界値より高リスクであるとACSが判断した場合、または法律によってチャレンジが必須である場合は、カード会員がさらに操作を行うことが必要な、**フリクションレス・フロー**が**チャレンジ・フロー**に切り替わります。**チャレンジ・フロー**は**フリクションレス・フロー**でもあった**AReq/ARes**メッセージ、**CReq/CRes**チャレンジメッセージと**RReq/RRes**結果メッセージから構成されます。

チャレンジ・フローを次の図に示します。



> ***点線は、クライアント/3DSリクエスターと信用承認機能の間の通信など、3DS2プロトコルの範囲外のメッセージングを示します。***

処理 3: 認証結果の取得

3DS2処理が完了すると、加盟店は認証結果を取得します。認証結果（チャレンジのステータスによりAResまたはRRes）には、ECI、認証値（CAVVなど）、および3DSリクエスターへの最終取引ステータスなどの情報が含まれています。

次のチャプター

次を選択し、**認証シーケンス**の詳細をご覧ください。