EMV V2.2.0へ移行

このガイドでは、EMV 3DS2.1.0仕様からv2.2.0仕様への技術的な移行ガイドの概要を説明します。 **ActiveServer**バージョン2.0.0以降、EMV v2.2.0認証リクエストは、認証APIリクエストで `messageVersion` フィールドを指定することでサポートされます。

変更の概要

- ActiveServer V2.0.0にアップグレードすることによる既存の3DSリクエスターの実装を壊す変更はありません。既存の3DSリクエスターの実装は、アップグレードの完了後もEMVv2.1.0メッセージを使用して認証要求を送信し続けることができます。
- EMV v2.2.0仕様をサポートするために、認証APIに新しいフィールドが追加され、既存のフィールドに新しい値が追加されました。追加された新しいフィールドと値は、認証APIドキュメントで `[V2.2.0以降]` タグでマークされています。新しく追加されたv2.2.0フィールドはすべてオプションであり、SCAなどの既存のプロセスを強化するために導入されました。
- 新しいオプションで提供できる `messageVersion` フィールドが次のエンドポイントに追加されました： `/api/v2/auth/brw` 、 `/api/v2/auth/3ri` 、 `/api/v2/auth/app` 。このフィールドは任意で提供でき、メッセージバージョンを上書きするために使用されます。詳細については、下記のアップグレードガイドを参照してください。
- v2.1.0のリクエストでv2.2.0フィールドが指定されている場合、**ActiveServer**はAReqを形成するときにフィールドを無視します。例: フィールド `threeDSDecReqInd` が認証APIリクエストで送信されたが、ACSのカードレンジがEMV v2.1.0メッセージのみをサポートしている場合、**ActiveServer**はリクエストをv2.1.0にダウングレードしようとし、v2.2.0のフィールドを無視します。ただし、v2.1.0フィールド、例えば `challengeInd` に `challengeInd = 07` などのv2.2.0でのみ指定可能な値が指定されている場合、EMV仕様要件に従ってエラーコード `203` を返却します。
- 3DSサーバー参照番号とPReqプロセスがEMV2.2.0プロセス用に更新されました。詳細については、以下のActiveServerの変更点セクションを参照してください。
- `/api/v2/auth/enrol` APIが更新され、ACSにてサポートされているメッセージバージョン（ `supportedMessageVersions` ）とACS情報インジケーター（ `acsInfoInd` ）が含まれるようになりました。詳細については、下記のEnrol APIセクションを参照してください。

- 新しいデカップルド認証フローがEMVv2.2.0で導入されました。詳細については、下記のデカップルド認証セクションを参照してください。
- 新しいマーチャントホワイトリスト機能がEMVv2.2.0で導入されました。詳細については、下記のマーチャントホワイトリスティングセクションを参照してください。
- `/api/v2/auth/3ri/result` APIエンドポイントが追加され、3DSリクエスターがデカップルド認証の結果を取得できるようになりました。
- GPayments TestLabs は `messageVersion` 2.2.0 に対応しております。

3DSリクエスターの v2.2.0 への更新手引き

v2.2.0 のフィールドと値を送信するよう、3DSリクエスターのコードを更新する必要があります。メッセージバージョン v2.2.0 フィールドをご利用になりたい場合は `messageVersion` フィールドを `2.2.0` に設定していただく必要があります。これは、メッセージバージョンフィールドが提供されない場合、**ActiveServer** は最も高い共通の `messageVersion` をデフォルトで利用するためです。

また、3DSリクエスターはEnrol APIの新しい応答フィールド `supportedMessageVersions` を処理する必要があります。応答フィールド `supportedMessageVersions` に `2.2.0` が含まれている場合、カードレンジはv2.2.0プロトコルをサポートされているので、APIリクエストの `messageVersion` フィールドを使用して2.2.0の認証リクエストを送信できます。

> **V2.2.0がサポートされていない場合、メッセージバージョンはダウングレードされます**
>
> 認証APIにてメッセージバージョンがv2.2.0に指定されているが、Enrol APIにて指定したカード番号の `supportedMessageVersions` に `2.2.0` が含まれていない場合、**ActiveServer**は `messageVersion` をv2.1.0にダウングレードします。これは、互換性を最大化するためであり、3DSリクエスターがACSがサポートしていないメッセージバージョンを送信したときに認証が失敗しないようにします。
>
> メッセージバージョンがv2.2.0に指定されていて、カードレンジが見つからない場合、**ActiveServer**はv2.2.0メッセージをディレクトリサーバーに送信しようとします。

ActiveServerの変更点

3DSサーバー参照番号

3DSサーバーがEMVコンプライアンステストを完了すると、3DSサーバー参照番号が発行されます。この番号は、ディレクトリサーバーに送信されるすべてのAReqに含まれています。下位互

換性のために、デフォルトで**ActiveServer V2.0.0**のリリース時点ではv2.1.0のみ認定中にEMVcoによって発行された3DSサーバー参照番号を使用します。デフォルトの参照番号はv2.1.0要求の送信にのみ有効であり、国際ブランドDSはこの参照番号を使用した場合、v2.2.0要求を拒否する可能性があります。

また、国際ブランドのコンプライアンステスト中、またはコンプライアンステスト後、本番インスタンスで2.1.0参照番号を新しい2.2.0参照番号で上書きする必要があります。本番インスタンスの3DSサーバー参照番号は**コンプライアンステストが完了した後**にのみ上書きしてください。コンプライアンステストを完了後3DSサーバー参照番号をDSに登録していない場合、DSによって認証が拒否される可能性があります。3DSサーバー参照番号の上書きの詳細については、クイックスタートガイドのセクションを参照してください。

PReq処理のメッセージバージョン

ActiveServer v2.0.0では、Visa、Mastercard、American Expressのメッセージバージョン2.2.0でPReqを送信することにより、2.2.0のPReqプロセスを更新します。これらのディレクトリサーバーは、デフォルトでこのメッセージバージョンを処理するためです。 JCBとDiscoverでは、v2.2.0PReqを送信する前に、国際ブランドのコンプライアンステストと3DSサーバー参照番号の登録を完了する必要があるため、これらのブランドではデフォルトで2.1.0をPReqを送信します。

国際ブランドコンプライアンステスト中に、2.1.0または2.2.0PReqメッセージのいずれかを送信する必要がある場合があります。また、**コンプライアンステスト後**に本番インスタンスで2.2.0のPReqを使用するようにすべての国際ブランドを更新する必要がありますが、これを支援するために、PReqメッセージの上書き設定が `application-prod.properties` ファイルに追加されました。PReqメッセージの上書きの詳細については、クイックスタートガイドのセクションを参照してください。

Enrol API

上記のように、Enrol APIが更新され、 `supportedMessageVersions` フィールドが証明されたため、3DSリクエスターは、認証要求を行う前に、カード番号でサポートされているメッセージバージョンを知ることができます。

また、ACS側で使用可能な機能を説明するACS情報インジケーター(`acsInfoInd`)フィールドも提供します。

- 01 = ACSで認証が利用可能 - 通常の3DS認証がサポートされ、カード会員のイシュアー銀行によって利用可能です。
- 02 = ACSまたはDSでサポートされる試行 - カード会員は認証を利用できませんが、ACSまたはDSが責任シフトのために試行応答を提供できます。一部の国際ブランドでは、詐欺を最小限に抑えるために、可能であれば3DSv1.0へのフォールバックを推奨する場合があります。
- 03 = デカップルド認証がサポートされています。
- 04 = サポートされているホワイトリスト。

さらに、国際ブランド固有の値がいくつかあります。これらの値とAPIの使用法の詳細については、Enrol APIドキュメントを参照してください。

デカップルド認証

デカップルド認証は、3DSフローの外部で実行される認証です。たとえば、カード会員は、生体認証を介して銀行アプリで直接認証します。

デカップルド認証の一般的なフローは次のとおりです。

1. ACSがデカップルド認証をサポートしているか否かを確認するために、3DSリクエスターはEnrol APIを呼び出すことができます。ACSがデカップルド認証をサポートしている場合、`acsInfoInd` フィールドには `03` の値が含まれます（デカップルド認証がサポートされています）。**ActiveServer**は、 `acsInfoInd` に従って厳密な検証を行わないことに注意してください。つまり、 `acsInfoInd` の値に `03` が含まれていない場合に `threeDSDecReqInd` が指定されていても、エラーは返却されません。
2. ACSがデカップルド認証をサポートしている場合、3DSリクエスターは `threeDSDecReqInd = Y` と `threeDSDecMaxTime` を設定します。
3. ACSがデカップルド認証の実行に同意した場合、認証応答で `transStatus = D` と `acsDecConInd = Y` が返されます。3DSリクエスターは、UIに `cardholderInfo` のコンテンツを表示する必要があります。このコンテンツには、カード会員が3DSの外部で認証を実行するための指示が含まれています。たとえば、メッセージはカード会員に銀行アプリを開くように指示する場合があります。
4. カード会員がデカップルド認証を実行するか、 `threeDSDecMaxTime` を超えた後、ACSはDSを介してRReqを3DSサーバーに送信します。

5. 3DSリクエスターは、 `resultMonUrl` にポーリング要求を行うことにより、最終的な認証結果の可用性を確認できます。 RReqが3DSサーバーによって受信されると、イベントは `event = AuthResultReady` に設定されます。これにより、3DSリクエスターは `/api/v2/auth/**/result` エンドポイントを介して最終結果を取得できます。

詳細なフローについては、認証シーケンス図を参照してください。これは、デカップルド認証を含むように更新されています。デカップルド認証のリクエスター実装については、統合ガイドを参照してください。

加盟店のホワイトリスト

加盟店のホワイトリスティングはEMVv2.2.0仕様で導入されました。これは、ACSのプロセスであり、カード会員が加盟店を信頼できるホワイトリストに追加できるようにします。これにより、イシュアーは、PSD2などのSCA要件から将来的にトランザクションを免除することができます。

この機能をサポートするために、新しいフィールド `whiteListStatus` が追加されました。詳細については、認証APIドキュメントを参照してください。

ACSがホワイトリスティングをサポートしているかどうかを確認するために、3DSリクエスターはEnrol APIを呼び出すことができます。 ACSがホワイトリストをサポートしている場合、 `acsInfoInd` フィールドには値 `04` が含まれます。 **ActiveServer**は、 `acsInfoInd` に従って厳密な検証を行わないことに注意してください。つまり、 `acsInfoInd` の値に `04` が含まれていないない場合に `whiteListStatus` が3DSリクエスターによって提供されても、エラーは返却されません。