



VeriTrans4G 開発ガイド別冊

本人認証(3D セキュア 2.0) ご利用ガイド

Ver. 1.0.17 版 (2024 年 12 月～)

目次

第 1 章	本ガイドの内容	2
1-1	本ガイドの内容	2
1-2	著作権、および問い合わせ先	2
1-3	改訂履歴	2
第 2 章	本人認証サービス概要	7
2-1	本人認証サービス(3D セキュア 2.0)について	7
2-2	3D セキュアバージョンアップによる VeriTrans4G 本人認証サービスへの影響	7
第 3 章	MDK の処理概要	8
3-1	機能一覧(決済要求コマンド)	8
3-2	決済処理シーケンス	9
第 4 章	インターフェース詳細	11
4-1	基本項目について	11
4-2	特記事項	11
4.2.1	カード決済関連	11
4.2.2	3D セキュア 2.0 関連	12
4-3	本人認証要求	13
4.3.1	認可	13
4.3.2	再取引	21
4-4	本人認証およびカード決済の結果取得	22
4.4.1	消費者のブラウザを経由した結果の取得	22
4.4.2	本人認証結果確認	26
4-5	結果通知	28
4-6	検索	29
第 5 章	その他 補足事項	35
5-1	決済サービスオプションタイプについて	35
5-2	決済結果の判定について	36
5-3	決済サーバーと加盟店サイト間の取引不整合の問題	36
5-4	決済結果の詳細パラメータ連携と GET によるリダイレクション URI へのアクセス	36
5-5	結果通知の送信(Push)	37
5-6	本人認証処理の有効期限	38
5-7	検索(Search)に関する補足	38
5-8	3D セキュア認証が成功しない場合の対処方法	39
第 6 章	導入・テストに関する補足	41

第1章 本ガイドの内容

1-1 本ガイドの内容

本ガイドは、(株)DG フィナンシャルテクノロジーが提供する VeriTrans4G の本人認証サービス(3D セキュア 2.0)を EC サイトに導入するための、アプリケーション開発者向けのガイドです。

本ドキュメントと併せて「本人認証サービス補足資料(3D セキュア 2.0 対応版)」もご確認ください。

1-2 著作権、および問い合わせ先

[著作権]

本ドキュメントの著作権は株式会社 DG フィナンシャルテクノロジーが保有しています。

Copyright © 2024 DG Financial Technology, Inc., a Digital Garage company. All rights reserved.

[お問い合わせ先]

株式会社 DG フィナンシャルテクノロジー ベリトランス テクニカルサポート

電子メール: tech-support@veritrans.jp

1-3 改訂履歴

2021/07 : Ver. 1.0.0 版リリース

2021/07 : Ver. 1.0.1 版リリース

「第 4 章 インターフェース詳細」に再与信で引き継がれるデータについて記載。

「4.1.3 本人認証結果確認」のレスポンス項目の記載ミスを修正(要求通貨単位、本人認証結果コード)。

「4-4 結果通知」のトランザクションタイプの値に 2.0 で追加された値を記載。

2021/09 : Ver. 1.0.2 版リリース

「第 4 章 インターフェース詳細」にカード保有者名省略フラグの説明を追記。

「4.1.1 認可」の要求電文項目に「カード保有者名省略フラグ」を追加。

「4.1.1 認可」の HTTP ユーザーエージェント、HTTP アクセプトの設定を任意項目に変更。

「4.1.2 再取引」で元取引からの引継ぎ項目に関する補足を追記。

「4.1.3 本人認証結果確認」の mpi-none の場合に返戻する項目の条件から、詳細パラメータ連携ありを削除。

「4.1.3 本人認証結果確認」のレスポンス項目の追加(3D トランザクションステータス理由)。

「4.1.3 本人認証結果確認」のレスポンス項目と「4.2.1 リダイレクト受信内容: 決済サーバーから消費者ブラウザ経由で店舗へリダイレクトされる内容」の 3D トランザクションステータスの値に「R: 本人認証拒否」を追記。

「4.1.3 本人認証結果確認」のレスポンス項目と「4.2.1 リダイレクト受信内容: 決済サーバーから消費者ブラウザ経由で店舗へリダイレクトされる内容」の 3D トランザクション ID の説明から、3D メッセージバージョンの記載を削除して、AMEX の場合の記載を追加。3DECI の説明を変更。

2022/01 : Ver. 1.0.3 版リリース

「第 4 章 インターフェース詳細」の以下の点を修正。

リダイレクション URI (redirectionUri) の「設定」を「○: 必須」に変更。

請求先住所_国 (billingAddressCountry)、配送先住所_国 (shippingAddressCountry) の各国コードのフォーマットを「3 桁以内」から「3 桁」に変更。

2022/02 : Ver. 1.0.4 版リリース

「3-1 機能一覧(決済要求コマンド)」の内容を見直し、3D セキュアのフローに関する説明を補足

第 4 章の構成を変更し、以下の節を追加

「4-1 基本項目について」

「4-2 特記事項」

「4.2.1 カード決済関連」

「4.2.2 3D セキュア 2.0 関連」

第 4 章の構成を変更し、以下の節を変更

変更前:

VeriTrans4G 本人認証(3D セキュア 2.0) ご利用ガイド

「4.1 本人認証」

「4.1.3 本人認証結果確認」

「4-2 本人認証およびカード決済の結果」

「4.2.1 リダイレクト受信内容: 決済サーバーから消費者ブラウザ経由で店舗へリダイレクトされる内容」

「4-3 共通」 「4.3.1 検索」

「4-4 結果通知」

変更後:

「4.3 本人認証要求」

「4-4 本人認証およびカード決済の結果取得」

「4.4.1 消費者のブラウザを経由した結果の取得」

「4.4.2 本人認証結果確認」

「4-5 結果通知」

「4-6 検索」

「■vAuthInfo および authParams を利用した改ざんチェックについて」を削除

「■カード保有者名の設定について」を追加

「4.3.1 認可」の「cardNumber」「cardExpire」「securityCode」の説明を修正

「4.3.1 認可」の「cardholderName」の説明に追記

「4-6 検索」の応答電文の階層を修正

「5-3 決済結果の詳細パラメータ連携と GET によるリダイレクション URI へのアクセス」の記載内容を見直し

2022/05 : Ver. 1.0.5 版リリース

「4.3.1 認可」に処理の概要の説明を追加

「4.3.1 認可」の「cardholderHomePhoneNumber」「cardholderMobilePhoneCountry」

「cardholderMobilePhoneNumber」の項目名を修正

「4.3.2 再取引」に処理の概要の説明を追加

「4.3.2 再取引」に元取引 ID が 3D セキュア 1.0 の取引だった場合の注意点についての説明を追加

「4.4.1 消費者のブラウザを経由した結果の取得」の表「消費者ブラウザ経由で店舗へ送信される詳細パラメータ (POST)」に、mpi-none の場合に必要項目「dddCavvAlgorithm」の説明が不足していたため修正

2022/06 : Ver. 1.0.6 版リリース

「4.3.2 再取引」に元取引 ID に 3D セキュアを実施していないカード決済も指定できることを追加

「4.4.1 消費者のブラウザを経由した結果の取得」の、

表「消費者ブラウザ経由で店舗へ送信される詳細パラメータ (POST)」の以下のパラメータを修正

「dddMessageVersion」の書式を修正

前: 半角英数字、" " 10 桁以内

後: 半角英数字記号 10 桁以内

「dddTransactionId」の説明を修正

「dddTransactionId」「dddCavv」の書式・制限の誤りを修正

誤: 半角英数字、"+", "-", "=" 28 桁

正: 半角英数字、"+", "/", "=", 28 桁

「dddDsTransactionId」の書式・制限を修正 (AMEX 仕様変更による)

前: 半角英数字、" " 36 桁以内

後: 半角英数字、"-", "+", "/", "=", 36 桁以内

「dddTransactionStatusReason」を予約項目から修正

「4.4.2 本人認証結果確認」

「dddTransactionStatusReason」を予約項目から修正

「4-6 検索」の「res3dTransactionId」の書式・制限の誤りを修正

誤: 半角英数字、"+", "-", "=" 28 桁

正: 半角英数字、"+", "/", "=", 28 桁

「4-6 検索」の「txnKind」の説明を追加

「5-5 本人認証処理の有効期限」の説明文の順序を一部変更

「5-6 検索 (Search)」に関する補足 (詳細コマンドタイプ)」の記載内容を見直し、章のタイトルを「5-6 検索

(Search)」に関する補足 (トランザクションタイプ)」に変更

「4.7.1 MPI トランザクションタイプ」を削除 (5-6 に説明を集約)

2022/07 : Ver. 1.0.7 版リリース

「4.3.1 認可」以下の項目を修正

要求電文「請求住所_国」と「配送先住所_国」に必須となる条件を記載。

応答電文「mpiTransactionType」を削除 (値が設定されないため)

2022/10 : Ver. 1.0.8 版リリース

「4.3.1 認可」以下の項目を修正

要求電文「deviceChannel」の設定列を△から○ (必須項目) に変更

「4-5 結果通知」の補足説明に、以下の下線の内容を追記

VeriTrans4G 本人認証(3D セキュア 2.0) ご利用ガイド

・本人認証サービスの結果通知機能をご利用の場合は、認可の要求電文に pushUrl を指定するか、MAP の各種設定変更より、本人認証の結果通知 URL を設定してください。

2023/02 :Ver. 1.0.9 版リリース

「3-2 決済処理シーケンス」の内容を見直し

図と説明を別冊の『概略処理フロー図』から抜粋して本書にも掲載し、補足資料への参照を促す文章を削除

2023/09 :Ver. 1.0.10 版リリース

「4.3.1 認可」以下の項目を修正

冒頭の説明文に authStartUrl(認証開始 URL)を使用するパターンを追記

要求電文「カード保有者名」の説明に補足を追記

要求電文「請求先郵便番号」の書式制限を半角数字→半角英数字記号に修正

要求電文「配送先郵便番号」の書式制限を半角数字→半角英数字記号に修正

要求電文「リクエストチャレンジインジケータ」を追加

応答電文「authRequestDatetime」の項目名と説明 本人認証→認可に変更

応答電文「authResponseDatetime」の項目名と説明 本人認証→認可に変更

応答電文「応答コンテンツ」の説明に authStartUrl を利用する場合は不要な旨を追記

応答電文「認証開始 URL」を追加

「4.4.1 消費者のブラウザを経由した結果の取得」

消費者ブラウザ経由で店舗へ送信される詳細パラメータ(POST)の「要求通貨単位」を△に修正

「4.4.2 本人認証結果確認」

応答電文「トランザクションタイプ」を追加

「4-6 検索」以下の項目を修正

応答電文「serviceType」を追加

応答電文「authRequestDatetime」の項目名と説明 本人認証→認可に変更

応答電文「authResponseDatetime」の項目名と説明 本人認証→認可に変更

「5-5 本人認証処理の有効期限」1)のタイミングでタイムアウトした場合の説明を修正

2024/04 :Ver. 1.0.11 版リリース

「4.2.2 3D セキュア 2.0 関連」

「■ブランドルールによる必須項目について」を追加

「■カード保有者情報、請求先情報、配送先情報について」の説明を修正

「■端末種別(browserDeviceCategory)について」の説明を削除

「再与信」を「再取引」に変更(用語統一のため)

「4.3.1 認可」の注 1～注 3 の必須項目(以下に列挙)に関する説明を追加

cardholderName

cardholderNameOmitFlag

cardholderEmail

cardholderHomePhoneCountry

cardholderHomePhoneNumber

cardholderMobilePhoneCountry

cardholderMobilePhoneNumber

cardholderWorkPhoneCountry

cardholderWorkPhoneNumber

customerIp

「4.3.2 再取引」の cardholderNameOmitFlag に関する説明を追加(ブランドルールにより推奨しない旨を追記)

2024/04 :Ver. 1.0.12 版リリース

「4.3.1 認可」の「cardholderEmail」の説明に RFC 非準拠の場合エラーになる旨追記

2024/04 :Ver. 1.0.13 版リリース

「4.3.1 認可」の「cardholderHomePhoneCountry」「cardholderMobilePhoneCountry」

「cardholderWorkPhoneCountry」の説明に ITU-T E.164 の値である旨追記

2024/05 :Ver. 1.0.14 版リリース

「2-2 3D セキュアバージョンアップによる VeriTrans4G 本人認証サービスへの影響」

3D セキュア 1.0 から 2.0 の移行についての記述を削除

「3-1 機能一覧(決済要求コマンド)」

イシューをカード発行会社(イシュー)に修正

「3-2 決済処理シーケンス」

authStartUrl の追加に伴い、リダイレクト指示の説明を修正

「4.2.1 カード決済関連」

VeriTrans4G 本人認証(3D セキュア 2.0) ご利用ガイド

■ワンクリック継続課金サービスについて

カード登録について「◆3D セキュア利用時の注意事項(重要)」参照の旨追記

「4.2.2 3D セキュア 2.0 関連」

■ブランドルールによる必須項目について

ブラウザの高さと幅を追記

■再取引とカード保有者名について

(3D セキュア 1.0 の取引 ID)を削除

■再取引で引き継がれるデータ

引き継がれない値としてカード保有者名以外の個人情報(メールアドレス、電話番号、IP アドレスなど)を追加

「4.3.1 認可」

MpiAuthorizeRequestDto

verifyResultLink 未指定の説明を修正

deviceChannel 説明の文言を修正

accountType 用途に関する説明を追記

cardholderNameOmitFlag 説明の書き方を変更

cardholderEmail RFC を RFC5322 に修正

cardholderHomePhoneNumber 設定例を追加

cardholderMobilePhoneNumber 設定例を追加

cardholderWorkPhoneNumber 設定例を追加

withChallenge 用途がないため削除

注意1 カード保有者名省略フラグの説明の文言を修正

MpiAuthorizeResponseDto

Mstatus を mstatus に修正

「4.3.2 再取引」

消費者ブラウザを遷移させる必要がある旨を追記

ワンクリック継続課金の会員 ID 併用の文言を修正

セキュリティコードの利用について追記

カードの有効期限を設定した場合について追記

元取引から引き継がれない項目について追記

「4.4.1 消費者のブラウザを経由した結果の取得」

改ざんチェックの実装についての文言を修正

「4.4.2 本人認証結果確認」

MpiGetResultResponseDto

vResultCode 成功した場合は G021 が返戻される旨を追記

「4-5 結果通知」

結果通知 URL が MAP と要求電文の両方に設定された場合は要求電文の値が優先される旨追記

「5-2 決済サーバーと加盟店サイト間の取引不整合の問題」

説明文の文言を修正

「5-3 決済結果の詳細パラメータ連携と GET によるリダイレクション URI へのアクセス」

verifyResultLink のデフォルトの記載を削除

2024/07 :Ver. 1.0.15 版リリース

「3-1 機能一覧(決済要求コマンド)」

使用可能な決済要求コマンドの表に売上と取消を追加

「4.3.1 認可」

MpiAuthorizeRequestDto

httpAccept を削除(設定不要なため)

billingAddressState 説明に先頭の 0 を省略不可の旨を追記

shippingAddressState 説明に先頭の 0 を省略不可の旨を追記

customerIp の書式・制限 半角英数字を半角英数字記号に修正

注 2 に以下を追記

電話番号は自宅/携帯/勤務先のうち1つを設定していただければ問題ありません。

メールアドレス・電話番号はワンタイムパスワード等の送信先として使用されることはありません。

「4-5 結果通知」

4 ケタの連番(0000~0999)を(0000~0049)に修正

「5-1 決済サービスオプションタイプについて」を追加し、以降の項番を繰り下げ

VeriTrans4G 本人認証(3D セキュア 2.0) ご利用ガイド

2024/09 : Ver. 1.0.16 版リリース

「4.3.1 認可」

MpiAuthorizeRequestDto

cardholderEmail 書式・制限に RFC5322 準拠を追記

「4.3.2 再取引」

元取引に使用できる取引について説明を追記

2024/12 : Ver. 1.0.17 版リリース

「4.3.1 認可」

MpiAuthorizeRequestDto

cardholderEmail 弊社ではフォーマットチェックを行っていない旨を追記

customerIp IPv4、IPv6 のどちらの形式でも問題ない旨を追記

MpiAuthorizeResponseDto

reqHttpUserAgent 要求電文の設定値から弊社で取得した値に変更

reqHttpAccept 要求電文の設定値から弊社で取得した値に変更

「4-5 結果通知」 txnType の“Verify”は 3DS1.0 のみであることを追記

「5-8 3D セキュア認証が成功しない場合の対処方法」を追加

第2章 本人認証サービス概要

2-1 本人認証サービス(3D セキュア 2.0)について

本人認証サービスはクレジットカード決済と連動する 3D セキュアによる認証サービスです。

3D セキュア 2.0 は、EMVCo が中心となって策定された本人認証サービスの総称で、クレジットカードブランドごとにサービスの名称が異なります。

Visa Secure (旧 VISA 認証サービス)

Mastercard ID Check(TM)

JCB J/Secure(TM)

American Express SafeKey(R)

Diners Club ProtectBuy(R)

ブランドのサービス名称は変更となる場合があります(上記は 2022 年 2 月現在)。

2-2 3D セキュアバージョンアップによる VeriTrans4G 本人認証サービスへの影響

本資料は 3D セキュア 2.0 に対応した資料となります。以前のバージョン(3D セキュア 1.0)と用語が異なる箇所があります。

3D セキュア 1.0 では、加盟店(EC サイト)側で 3D セキュア認証を処理する部分(機能)を「MPI(Merchant Plug-In)」と呼びますが、3D セキュア 2.0 では MPI という表現は用いられません。3D セキュア 1.0 における「MPI」は、3D セキュア 2.0 では「3DS サーバー」となります。

そのため、厳密には「MPI ホスティング」という表現は、3D セキュア 2.0 では適切でない表現となりますが、「3D セキュア認証サービス(1.0 か 2.0 に限らず)」と「MPI ホスティングサービス」は同等の機能(サービス)として扱っても大きな問題はありません。

なお、2022 年 2 月時点で VeriTrans4G 本人認証サービスは、3D セキュア 2.0 の「ブラウザベース認証」に対応しています。「アプリベース認証」には対応していません。

第3章 MDK の処理概要

3-1 機能一覧(決済要求コマンド)

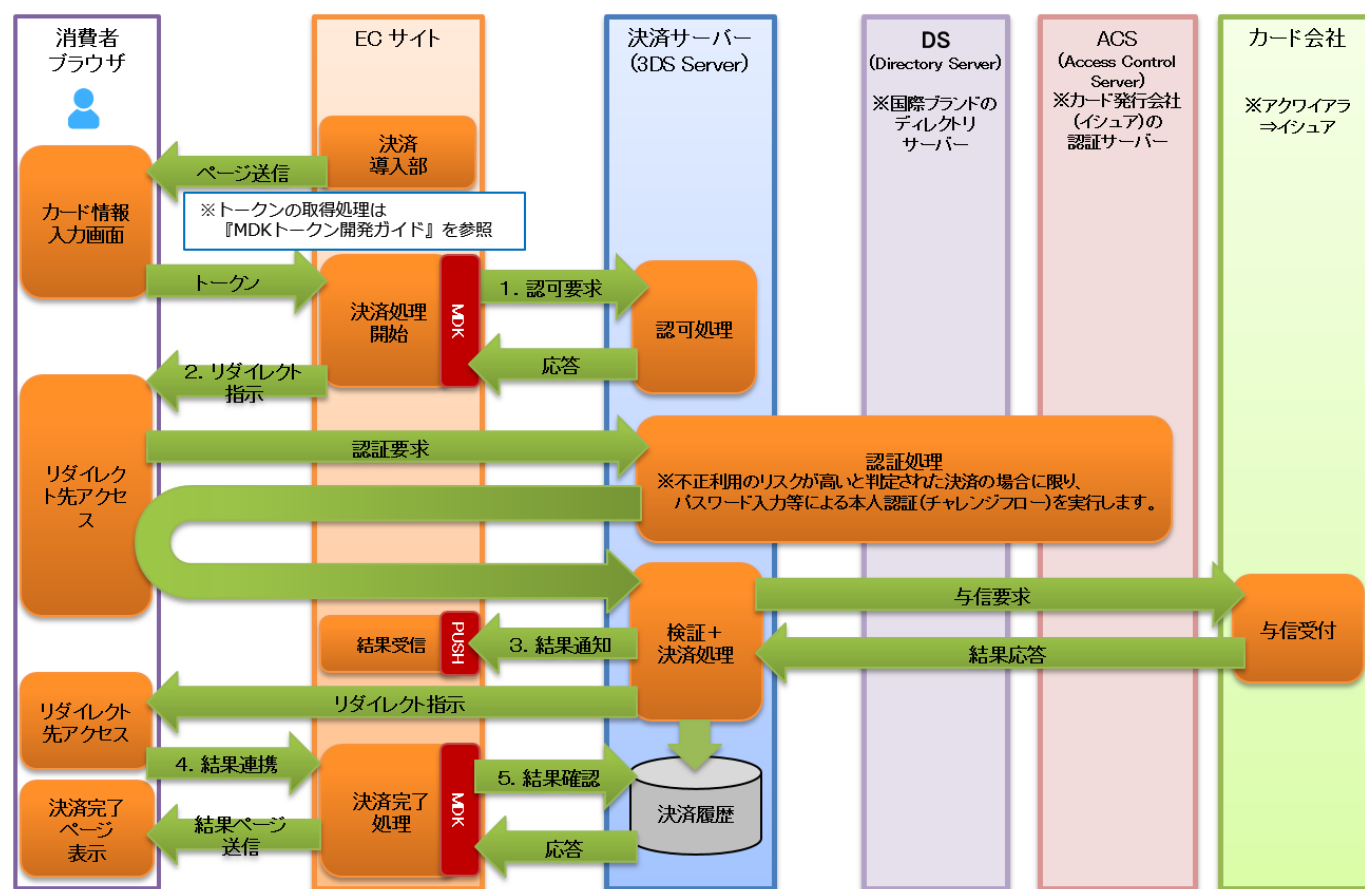
使用可能な決済要求コマンドを下表に示します。

決済要求種類 /コマンド	概要
認可 /Authorize	カード番号を元にカード発行会社(イシュア)判定を実施し、3D セキュアの利用可否を判定します。
再取引(認可) /ReAuthorize	過去の取引で利用されたカード番号で、再度認可を要求します。
本人認証結果確認 /GetResult	本人認証結果を取得できます。
売上 /Capture	与信取得済みの取引に対して売上処理を要求します。 クレジットカード決済と同じコマンドを使用します。詳細はクレジットカード決済のインターフェース詳細をご参照ください。
取消 /Cancel	売上済みまたは与信済みの取引に対して取消を要求します。 クレジットカード決済と同じコマンドを使用します。クレジットカード決済のインターフェース詳細をご参照ください。

表 3.1 使用可能なコマンド一覧

- ✓ 3D セキュアの処理フローでは、認可の成功後、消費者のブラウザをカード会社のサイトに遷移させることで認証が行われます。その後、決済サーバーが認証結果の判定(検証)を実施し、判定結果と認証タイプ(本書では「決済サービスオプションタイプ」)を元にカード決済(与信)の実行に進みます。

3-2 決済処理シーケンス



注) 「3. 結果通知 (PUSH 通知)」と「4. 結果連携」は非同期で実行されますので、どちらの結果を先に受信しても処理できるように実装してください。

図 3-2-1 MDK 利用時システム処理概要図 (3D セキュア)

No.	処理	説明
1	認可要求	3D セキュア認証および決済に必要な情報を電文化し、決済サーバーに送信します。 ※ トークン取得時の処理フローは、『MDKトークン開発ガイド』をご参照ください。
2	リダイレクト指示	認可要求の応答に含まれる2つのパラメータのどちらかを利用して、消費者ブラウザを画面遷移させます。 ・authStartUrl (認証開始 URL) ・resResponseContents (自動遷移用の JavaScript を含む HTML コンテンツ)
3	結果通知 (PUSH 通知)	決済サーバーは、認証結果およびカード決済の結果を EC サイトに通知します。 【4. 結果連携】が正しく行われなかった場合にも、この結果通知を受信することで認証および決済の結果を取得できます。
4	結果連携 (ブラウザ経由での結果連携)	決済サーバーは、認証結果およびカード決済の結果を EC サイトにブラウザ経由で連携します。 ブラウザ経由での結果連携は、消費者の端末(PC やスマートフォン)のネットワーク環境の問題や、誤操作(ブラウザやタブを閉じてしまう等)により、正しく行われない可能性がありますので、必ず【3. 結果通知】を受信してください。 また、ブラウザの操作によっては、EC サイトの URL に複数回のアクセスが発生する可能性があります。複数回のアクセスが発生しても、連携された結果が正しい(改ざんされていない)場合には、エラーにならないように適切に処理してください。
5	結果確認	必要に応じて EC サイトから決済サーバーに結果を問い合わせることもできます。 ※【3. 結果通知】【4. 結果連携】によって結果を正常に取得できた場合は、この処理は不要です。

(重要)

- ◇ 【2. リダイレクト指示】で resResponseContents を利用する場合は、決済サーバーから受信した resResponseContents を加工・編集せずに、そのままブラウザに送信してください。加工・編集を加えた場合、認証処理が正しく動作しない可能性があります。
- ◇ 【3. 結果通知(PUSH 通知)】と【4. 結果連携】は非同期で実行されます。どちらを先に受信しても処理できるように実装してください。
結果の取得方法の詳細は「4-4 本人認証およびカード決済の結果取得」を参照して下さい。

第4章 インターフェース詳細

ここでは本人認証サービスで利用する MDK インターフェース項目を説明します。

4-1 基本項目について

■「設定」欄の内容は以下の通りです。

要求電文 … 必須項目:○ 任意項目:△ 設定不可:× その他条件付:※、※n(条件は説明欄、または欄外に記入)
応答電文 … 必ず返戻:○ 処理成功時のみ返戻:△ 返戻なし:× その他条件付:※

■orderId(取引 ID)について

店舗で任意に採番してください。申込処理毎に付ける必要があります。他の取引 ID と重複しないよう採番してください。他決済サービスとも重複できません。

また、テスト取引で使用した取引 ID を、本番取引で再度使用することはできません。

取引 ID には、半角英数字以外に“-”(ハイフン)、“_”(アンダースコア)も使用可能です。

■応答電文について

応答電文には、本書に記載されていないフィールド(パラメータ)も存在しますが、通常は、記載されているフィールド以外は加盟店様の方で意識する必要はございません。

4-2 特記事項

4.2.1 カード決済関連

■売上、キャンセル処理について

本人認証によるクレジットカード決済取引は、クレジットカード決済の Capture 処理により売上を行います。また、Cancel 処理により取消・返金を行います。

Capture 処理、Cancel 処理については、『インターフェース詳細 ～クレジットカード決済～』を参照してください。

■カード情報の非保持化について

クレジットカード取引におけるセキュリティ対策として、加盟店様にはカード情報の非保持化(自社で保有する機器・ネットワークにおいて、カード情報を保存、処理、通過しないこと)が求められています。

非保持化に対応するためには、MDK の要求電文に、カード番号を設定して送信することはできません。そのため、VeriTrans4G の MDK 型(モジュール方式)では、トークン方式による非保持化・非通過化に対応しています。

トークン方式では、カード情報は消費者の端末から直接弊社のサーバーに送信します。

加盟店様のシステムでは、カード情報の代わりに弊社が発行したトークンを用いて、その後の決済要求を行っていただきますので、加盟店様のシステムをカード情報が通過することはありません。

◇ トークン方式については『MDKトークン 開発ガイド』を参照してください。

◇ 加盟店様のシステムでカード情報を保持する(非保持化に対応しない)場合は、PCI-DSS への準拠が必要になります。
なお、カード有効期限、セキュリティコードは、カード番号と同時に設定しなければカード情報の通過には該当しません。

例えば、再取引(以前の決済で使用了カード情報で決済する機能)をご利用の際に、更新された有効期限を設定して送信することや、不正防止のために購入の都度、セキュリティコードを消費者に入力させて送信することは、カード情報の通過にはあたりません。

◇ セキュリティコードは加盟店および決済代行会社で保存はできません。

■ワンクリック継続課金サービスについて

ワンクリック継続課金サービスを利用するためのインターフェースは、以下のドキュメントに記載されています。

『インターフェース詳細～ワンクリック継続課金サービス～』

◇ 3D セキュア認証(および与信)が成功したカードの登録を行いたい場合は、「2.2.2 クレジットカード決済実行時の会員 ID 管理と決済機能」の「◆3D セキュア利用時の注意事項(重要)」を必ず確認してください

ワンクリック継続課金サービスをご利用の際は、本書に記載の要求電文のフィールドと、ワンクリック継続課金サービス用のフィールドを設定して決済を行ってください。

また、応答電文のフィールドにも、ワンクリック継続課金サービス用のフィールドが追加されますのでご注意ください。

4.2.2 3D セキュア 2.0 関連

■ブランドルールによる必須項目について

2024 年 8 月より、ブランドルールにより以下の項目が必須となりますので、「4.3.1 認可」の説明を参考に必ず設定してください。

- カード保有者名
- 消費者のメールアドレス または 電話番号
- 消費者の IP アドレス
- ブラウザの高さと幅 ※ この項目は決済サーバー側で自動収集するため加盟店側で設定は不要です

■カード保有者情報、請求先情報、配送先情報について

カード保有者情報、請求先情報、配送先情報は、認可要求時の先頭と末尾の半角スペースを除いた値で本人認証処理に使用します。特に、3D セキュア 2.0 の要求では必須項目となるカード保有者名について、スペースのみで書式を満たす桁数を設定した場合も未指定の場合と同様に書式エラーとなります。

(重要) カード保有者名は、ブランドルールにより必須項目となりましたので、以下の記載は削除します。

3D セキュア 2.0 においてカード保有者名の値は限りなく必須の表現となっております。加盟店サイトの仕様としてカード保有者を指定しないと判断した場合は、カード保有者名省略フラグを `true` で指定することで、カード保有者名が未指定でも書式エラーとせずに本人認証をリクエストすることができます。

カード保有者名を指定しないことによる影響度(認証エラー、チャレンジ認証と判断される確率が上がる等)はカード会社が開示していない為、不明となります(弊社にも情報がありません)。カード保有者名省略フラグは加盟店様の判断でご利用ください。

■カード保有者名の設定について

トークン発行時にカード保有者名を設定する場合は、他のカード情報と同様にトークンに紐づいたカード保有者名を使用するため、3D セキュア要求電文に設定する必要がありません。

■再取引とカード保有者名について

再取引では、カード保有者名の値も元取引 ID に指定した取引に紐づく値を利用しますが、指定した元取引 ID にカード保有者名が紐づいていない場合は、パラメータ不足でエラーとなります。

■再取引で引き継がれるデータ

再取引では、カード保有者名は元取引の値を引き継ぎます。

以下の値は引き継がれませんのでご注意ください。「4.3.2 再取引」の説明を参照してください。

- デバイスチャネル
- HTTP ユーザーエージェント
- HTTP アクセプト
- カード保有者名以外の個人情報(メールアドレス、電話番号、IP アドレスなど)

4-3 本人認証要求

4.3.1 認可

3D セキュアの実行に必要なパラメータ、およびカード決済に必要なパラメータを送信します。

3DS サーバーは、クレジットカード番号からカード発行会社(イシュア)を判定し、3D セキュアを開始するために必要な情報を返します。

加盟店サーバーは認可の成功後、消費者ブラウザを「認証サーバーにアクセスさせるためのページ」に誘導する必要があります。認可のレスポンスに含まれる2つのパラメータのどちらかを利用して、消費者ブラウザを画面遷移させてください。

- authStartUrl (認証開始 URL)
- resResponseContents (自動遷移用の JavaScript を含む HTML コンテンツ)

パラメータの利用方法を以下に示しますので、加盟店様の EC サイトの実装上、利用しやすい方を選択してください。

- authStartUrl を利用する場合には、HTTP レスポンスヘッダ(Location ヘッダ)にリダイレクト先 URL を設定し、HTTP ステータスコード=302 でリダイレクトするか、JavaScript を利用してリダイレクト先 URL に自動遷移させてください。
- resResponseContents を使う場合は、そのままブラウザに送信してください。JavaScript により自動的にカード会社の認証サーバーに遷移します。(コンテンツの中身の編集は絶対に行わないでください。画面遷移ができなくなる可能性があります。)

要求電文 : MpiAuthorizeRequestDto				
フィールド名	項目名	書式・制限	説明	設定
serviceOptionType	決済サービスオプションタイプ (認証タイプ)	右記参照	"mpi-complete" : 完全認証 "mpi-company" : 通常認証(カード会社リスク負担) "mpi-merchant" : 通常認証(カード会社、加盟店リスク負担) "mpi-none" : 本人認証単体サービス	○
orderId	取引 ID	半角英数字 100 桁以内	取引を識別する一意の ID 「4-1 基本項目について」を参照してください。	○
amount	決済金額	半角数字 8 桁以内	1 以上 99,999,999 以下	○
token	トークン	半角英数記号 36 桁	トークンサーバーが発行した、クレジットカード情報の識別に用いるトークンの値 詳細は『MDK トークン開発ガイド』を参照してください。 ※トークンまたはカード情報が必須	※

要求電文 : MpiAuthorizeRequestDto				
フィールド名	項目名	書式・制限	説明	設定
cardNumber	カード番号	半角数字 16 桁以内	(重要) カード情報の非保持(非通過、非保持)への対応のため、通常は設定しないでください。 詳しくは「4.2.1 カード決済関連」の「■カード情報の非保持化について」を参照してください。 数字のみ、またはハイフン含みで指定(ハイフン含みの場合は 19 桁以内で指定) ※トークンまたはカード情報が必須	※
cardExpire	カード有効期限	半角英数字 5 桁	(重要) カード情報の非保持(非通過、非保持)への対応のため、通常は設定しないでください。 詳しくは「4.2.1 カード決済関連」の「■カード情報の非保持化について」を参照してください。 MM/YY (月 + "/" + 年)の形式 (例 "08/18")	※
jpo	支払種別	半角英数字 83 桁以内 右記参照	"10" (一括払い) "21" (ボーナス一括) "61Cxx" (分割払い、xx に分割回数指定) "80" (リボルビング払い) ※ 指定が無い場合は、"10" (一括払い) が適用されます。 ※直接契約 / 包括契約でそれぞれ使用できる支払種別が異なります。 詳細は『インターフェース詳細 ~クレジットカード決済~』の「クレジットカード決済 支払種別情報の指定」を参照してください。	△
withCapture	売上フラグ	右記参照	"true": 与信・売上 "false": 与信のみ ※指定が無い場合は、デフォルト値の"false"が設定されます。	△
securityCode	セキュリティコード	半角数字 3 桁 or 4 桁	(重要) カード情報の非保持(非通過、非保持)への対応のため、通常は設定しないでください。 詳しくは「4.2.1 カード決済関連」の「■カード情報の非保持化について」を参照してください。 セキュリティコード(CVV2/CVC2)とは、カード券面に記載された 3 桁ないし 4 桁の数字です。	△
redirectionUri	リダイレクション URI	半角英数字 1024 バイト以内	検証結果を返す URI を指定 (重要) 決済サービスオプションタイプ (serviceOptionType) で MPI 単体サービス ("mpi-none") を選択する場合は、SSL を必須とします。必ず "https://" から始まる URI をご指定下さい。	○
verifyResultLink	詳細パラメータ連携フラグ	半角数字	0:パラメータ連携しない 1:パラメータ連携する 2:パラメータ連携しない(GET) ※ 未指定の場合は、加盟店毎の設定で異なる挙動になるため、このフラグを設定することをお勧めします。	△

要求電文 : MpiAuthorizeRequestDto				
フィールド名	項目名	書式・制限	説明	設定
httpUserAgent	HTTP ユーザーエージェント	制限なし	消費者のブラウザ情報 ※ 3D セキュア 2.0 で未指定の場合は、決済サーバー側で表示する画面から取得した値を使用します。	△
pushUrl	プッシュ URL	URLに使用可能な半角文字 256 桁以内	結果通知先 URL を指定 指定がない場合には予め登録された URL を用います。	△
verifyTimeout	本人認証有効期限	半角数字 3 桁以内	本人認証処理の有効期限(分単位のタイムアウト値)を指定 1 以上 999 以下 消費者が本人認証の画面で長時間滞留する等、認証完了までに時間がかかった取引を無効(エラー)にする場合は、この値を設定してください。 タイムアウト判定の起点は、認可要求の処理時刻です。 EC サイトのセッションタイムアウト値よりも数分程度短く設定することを推奨します。 ※未指定の場合、弊社サービス上のタイムアウトは発生しないため、長時間経過後に決済が成立する場合があります。	△
deviceChannel	デバイスチャネル	半角数字 2 桁	デバイスチャネルを指定します。 "02": ブラウザベース 重要:本パラメータは必ず設定してください。	○
accountType	アカウントタイプ	半角数字 2 桁	アカウントの種類を指定します。 "01": 該当なし "02": クレジット "03": デビット ※通常は指定する必要はありません。また、デビットカードを拒否する等の用途で利用できるものではありません。	△
cardholderName	カード保有者名	半角英数記号 2 桁以上 45 桁以内	カード保有者名を指定します。 トークンにカード保有者名設定している場合は、ここでの設定は不要です。 姓名の書き方には明確なルールはありません。カード券面に記載されている通りの表記で設定することを推奨しますが、以下のような場合にも弊社システム上はエラーにはせず、カード会社の判断に委ねます。 ・名と姓の順番が逆 ・名と姓の間にスペースがない ・名と姓の間に半角スペースが複数ある	○ 注1

要求電文 : MpiAuthorizeRequestDto				
フィールド名	項目名	書式・制限	説明	設定
cardholderNameOmitFlag	カード保有者名省略フラグ	右記参照	※このパラメータの使用は非推奨です。 (注 1 を参照) "true": カード保有者名を省略可能 "false": カード保有者名は必須 ※指定が無い場合は、デフォルト値の"false"が設定されます。	△ 注1
cardholderEmail	カード保有者メールアドレス	半角英数記号 254 桁以内 RFC5322 準拠 (右記参照)	カード保有者メールアドレスを指定します。 RFC5322 に準拠していないメールアドレスを設定すると、エラーが発生する可能性があります。弊社ではフォーマットチェックを行っていないので、加盟店様にてチェックをかけ、RFC に準拠していないメールアドレスの場合は当項目は設定せず、代わりに電話番号を設定するなどしてください。 参考: https://www.docomo.ne.jp/service/docomo_mail/rfc_add/	○ 注2
cardholderHomePhoneCountry	カード保有者自宅電話番号国コード	半角数字 3 桁以内	カード保有者自宅電話番号の国コード ITU-T E.164 で規定された地域別国コードを指定 (日本の場合は「81」)	○ 注2
cardholderHomePhoneNumber	カード保有者自宅電話番号	半角数字 15 桁以内	カード保有者自宅電話番号を指定します。 (例: 0312345678)	○ 注2
cardholderMobilePhoneCountry	カード保有者携帯電話番号国コード	半角数字 3 桁以内	カード保有者携帯電話番号の国コード ITU-T E.164 で規定された地域別国コードを指定 (日本の場合は「81」)	○ 注2
cardholderMobilePhoneNumber	カード保有者携帯電話番号	半角数字 15 桁以内	カード保有者携帯電話番号を指定します。 (例: 09012345678)	○ 注2
cardholderWorkPhoneCountry	カード保有者勤務先電話番号国コード	半角数字 3 桁以内	カード保有者勤務先電話番号の国コード ITU-T E.164 で規定された地域別国コードを指定 (日本の場合は「81」)	○ 注2
cardholderWorkPhoneNumber	カード保有者勤務先電話番号	半角数字 15 桁以内	カード保有者勤務先電話番号を指定します。 (例: 0312345678)	○ 注2
billingAddressCity	請求先住所_市区町村	文字列 50 文字以内	請求先住所の市区町村を指定します。	△
billingAddressCountry	請求先住所_国	半角数字 3 桁	請求先住所_都道府県を指定した場合は必須 請求先住所の国を指定します。ISO 3166-1 numeric で定義されているコードを設定します。先頭が 0 の場合も省略せずに 3 桁で設定してください(例:「040」)。	※
billingAddressLine1	請求先住所 1	文字列 50 文字以内	請求先住所 1 を指定します。	△
billingAddressLine2	請求先住所 2	文字列 50 文字以内	請求先住所 2 を指定します。	△
billingAddressLine3	請求先住所 3	文字列 50 文字以内	請求先住所 3 を指定します。	△

要求電文 : MpiAuthorizeRequestDto				
フィールド名	項目名	書式・制限	説明	設定
billingPostalCode	請求先郵便番号	半角英数字記号 16 桁以内	請求先郵便番号を指定します。	△
billingAddressState	請求先住所_都道府県	半角英数字 3 桁以内	請求先住所の都道府県を指定します。 ISO 3166-2 で定義されているコードを設定します。先頭が 0 の場合も省略せずに設定してください(例 JP-01 の場合は「01」)。	△
shippingAddressCity	配送先住所_市区町村	文字列 50 文字以内	配送先住所の市区町村を指定します。	△
shippingAddressCountry	配送先住所_国	半角数字 3 桁	配送先住所_都道府県を指定する場合は必須 配送先住所の国を指定します。 ISO 3166-1 numeric で定義されているコードを設定します。先頭が 0 の場合も省略せずに 3 桁で設定してください(例:「040」)。	※
shippingAddressLine1	配送先住所 1	文字列 50 文字以内	配送先住所 1 を指定します。	△
shippingAddressLine2	配送先住所 2	文字列 50 文字以内	配送先住所 2 を指定します。	△
shippingAddressLine3	配送先住所 3	文字列 50 文字以内	配送先住所 3 を指定します。	△
shippingPostalCode	配送先郵便番号	半角英数字記号 16 桁以内	配送先郵便番号を指定します。	△
shippingAddressState	配送先住所_都道府県	半角英数字 3 桁以内	配送先住所の都道府県を指定します。 ISO 3166-2 で定義されているコードを設定します。先頭が 0 の場合も省略せずに設定してください(例 JP-01 の場合は「01」)。	△
customerIp	消費者 IP アドレス	半角英数字記号 45 桁以内 IPv4 または IPv6 形式	消費者のブラウザ情報をアプリケーションサーバから取得して設定します。 MAP の「各種設定変更」のページで以下のチェックボックスをチェックしている場合はここでは設定不要です。 IP アドレスを自動収集する ☒	○ 注 3
requestorChallengeIndicator	リクエスターチャレンジインジケータ	半角数字 2 桁	このリクエストに対してチャレンジ認証を要求するかを指定します。 "01": No preference (任意) "02": No challenge requested (チャレンジ認証を要求しない) "03": Challenge requested (3DS Requestor preference) (チャレンジ認証を要求する) "04": Challenge requested (Mandate) (チャレンジ認証を要求する) ※"04"を指定しても必ずチャレンジ認証が行われるとは限りません。 ※このパラメータは、通常は指定する必要はありません。カード会社から設定を指示された場合にご利用ください。(カード会社からの指示に従ってください) ※未指定の場合は'01'と同様の挙動になります。	△

注1 カード保有者名省略フラグ(cardholderNameOmitFlag)は、カード保有者名を消費者から取得することができないケースを除き、設定しないでください。カード保有者名(cardholderName)は、ブランドルールにより必須項目となりましたので、cardholderNameOmitFlag の利用は推奨されません。

カード保有者名は、以下のケースを除き設定が必要です。

- ◇ MDK トークンの取得時に設定している場合
- ◇ 過去の認証時にカード保有者名を指定していた取引 ID を「元取引 ID」にして再取引を実行する場合
- ◇ ワンクリック継続課金サービスの会員 ID を利用して認証を行う場合で、会員 ID に紐づくカード情報にカード保有者名が保存されている場合

(補足)

cardholderNameOmitFlag に true を設定した場合にも、指定された cardholderName は認証に利用されます。

- ◇ 以下のケースでは、エラーにならず、設定された cardholderName が認証に利用されます。

cardholderNameOmitFlag : true cardholderName : 設定あり

- ◇ 以下のケースでは、パラメータエラーになります。

cardholderNameOmitFlag : false cardholderName : 設定なし

注2 ブランドルールにより、カード保有者の「メールアドレス」または「電話番号」が必須項目となりました。どちらかの項目は必ず設定してください。

電話番号を設定する際には「国コード」と「電話番号」をセットで設定してください。

電話番号は自宅/携帯/勤務先のうち1つを設定していただければ問題ありません

加盟店様のシステムで電話番号の属性(自宅/携帯/勤務先)を管理していない場合は、「自宅」の情報として設定してください。

メールアドレス・電話番号はワンタイムパスワード等の送信先として使用されることはありません。

注3 ブランドルールにより、消費者の IP アドレスが必須項目になりました。

MAP の「各種設定変更」のページで以下のチェックボックスをチェックしている場合はここでは設定不要です。

IP アドレスを自動収集する ☒

* 注2～注3 は必須項目ですが、未設定の場合にも弊社システムではエラー応答はしませんのでご注意ください。

カード会社側の認証判定に利用される重要な項目のため、必ず設定するようにしてください。

応答電文 : MpiAuthorizeResponseDto				
フィールド名	項目名	書式・制限	説明	設定
serviceType	決済サービスタイプ	半角英数字 10 桁以内	要求電文を送信した決済サービスタイプ。	○
mstatus	処理結果コード	半角英数字 32 文字以内	“success”: 正常終了 “failure”: 異常終了	○
vResultCode	詳細結果コード	文字列 16 桁	処理の結果を詳細に表すコード 4 桁ずつ 4 つのブロックで構成され、各ブロックでサービス毎の処理結果を表します。 詳細は『結果コード一覧』を参照下さい。	○
merrMsg	エラーメッセージ	文字列	処理結果を日本語で表示します。	○
marchTxn	電文 ID	文字列 100 桁以内	決済サーバーにて決済処理電文(内部処理も含む)毎に付与する ID 1つの取引 ID に対して、複数の ID が付与されます。	○
orderId	取引 ID	半角英数字 100 文字以内	決済要求時に加盟店にて任意に採番し送信された取引 ID	○
custTxn	取引毎に付く ID	文字列 100 桁以内	決済サーバーがオーダー(取引 ID)と紐付ける為に採番する ID	○
txnVersion	MDK バージョン	半角英数字 5 桁	電文のバージョン 問題発生時などに用いますが、通常ご利用になることはありません。	○
reqCardNumber	要求カード番号	文字列 16 桁以内	要求電文に設定した値 上 6 桁下 2 桁のみ数字表示され、その他は“*” (アスタリスク) に変換されます。 (例 “411111*****11”)	△
reqCardExpire	要求カード有効期限	文字列 5 桁以内	要求電文に設定した値 全桁“*” (アスタリスク) に変換されます。(例 “*****”)	△
reqAmount	要求取引金額	文字列 12 桁以内	要求電文に設定した値	△
reqJpoInformation	要求支払種別情報	文字列 83 桁以内	要求電文に設定した値	△
reqWithCapture	要求同時売上	文字列 5 桁以内	要求電文に設定した値	△
reqSecurityCode	要求セキュリティコード	文字列 4 桁以内	要求電文に設定した値 全桁“0” (ゼロ) に変換されます。	△
reqRedirectionUri	要求リダイレクション URI	文字列 1024 桁以内	要求電文に設定した値	△
reqHttpUserAgent	要求 HTTP ユーザーエージェント	無制限	弊社にて消費者ブラウザから取得した UserAgent	△
reqHttpAccept	要求 HTTP アクセプト	無制限	弊社にて消費者ブラウザから取得した HTTP の Accept リクエストヘッダー	△
resResponseContents	応答コンテンツ	無制限	消費者ブラウザを「認証サーバー」に自動遷移させる javascript を含む HTML コンテンツ。 このコンテンツをブラウザにそのまま送信することで、3D セキュア認証を開始できます。 ※コンテンツの中身は絶対に編集しないでください。画面遷移できなくなる可能性があります。 ※authStartUrl を利用する場合は、このパラメータを利用する必要はありません。	△

応答電文 : MpiAuthorizeResponseDto				
フィールド名	項目名	書式・制限	説明	設定
resCorporationId	応答会社 ID	文字列 2 桁以内	店舗が加盟店契約をしているカード会社のコード 最終的に決済を行うカード発行会社ではなく、決済要求電文が最初に仕向けられる加盟店管理会社です。 『インターフェース詳細 〜クレジットカード決済 〜』の「クレジットカード決済 仕向け先カード会社の一覧」を参照	△
resBrandId	応答ブランド ID	文字列 2 桁以内	以下の値が設定されます。 3D メッセージバージョンが“2.1.0”以上の場合 “35”: JCB “4”: VISA “5”: MASTER “37”: AMEX “36”: DINERS 3D メッセージバージョンが“1.0.2”の場合 “35”: JCB “4”: VISA “5”: MASTER “34”: AMEX “37”: AMEX	△
res3dMessageVersion	応答 3D セキュア メッセージバージョン	文字列 10 桁以内	3D セキュアプロトコルのメッセージバージョン	△
authRequestDatetime	認可要求日時	文字列 28 桁以内	認可要求の受付時間 EEE MMM dd HH:mm:ss JST yyyy 形式 (例 “Tue Mar 07 13:17:40 JST 2017”)	△
authResponseDatetime	認可応答日時	文字列 28 桁以内	認可の応答時間 EEE MMM dd HH:mm:ss JST yyyy 形式 (例 “Tue Mar 07 13:17:40 JST 2017”)	△
authStartUrl	認証開始 URL	文字列 1024 桁以内	ブラウザをこの URL に遷移させると 3D セキュアの認証を開始できます。 HTTP レスポンスヘッダ (Location ヘッダ) にこの URL を設定し、HTTP ステータスコード=302 を使ってリダイレクトさせるか、JavaScript で遷移させてください。 ※有効期限: 認可応答日時から 3 分 ※既に処理済みの場合はエラーとなります。 ※エラー時は加盟店サイトの結果画面に遷移 (リダイレクト) します。 ※resResponseContents を利用する場合は、このパラメータを利用する必要はありません。	

4.3.2 再取引

過去の決済時に利用したクレジットカード情報を用いて認可要求を実行します。

MpiReAuthorizeRequestDto の実行だけでは 3D セキュア認証および決済は成立しません。「4.3.1 認可」と同様に消費者ブラウザを遷移させて、認証処理を行う必要がありますのでご注意ください。

注) 再取引を利用する場合は、ワンクリック継続課金サービスの会員 ID を指定しないでください。

要求電文 : MpiReAuthorizeRequestDto				
フィールド名	項目名	書式・制限	説明	設定
originalOrderId	元取引 ID	半角英数字 100 桁以内	再取引を行う過去取引の取引 ID	○
※元取引 ID 以外については認可要求電文を参照				

- ✓ カード保有者名 (cardholderName) は元取引から値を引き継ぐため指定不要です。ただし、セキュリティコードは保存できないため、セキュリティコードを指定する場合は消費者に都度入力を求める必要があります。
- ✓ カード有効期限を指定した場合は、元取引のカード番号と指定したカード有効期限で決済が行われます。
- ✓ 以下の値は元取引から引き継がれませんのでご注意ください。
 - デバイスチャネル
 - HTTP ユーザエージェント
 - HTTP アクセプト
 - カード保有者名以外の個人情報(メールアドレス、電話番号、IP アドレスなど)
- ✓ 元取引 ID にカード保有者名 (cardholderName) が保存されていない場合は、以下のどちらかの対応が必要です。
 - cardholderName を指定する
 - cardholderNameOmitFlag を指定する **注) ブランドルールによりカード保有者名は必須項目のため推奨されません。**
- ✓ 元取引 ID には 3D セキュアを実施しなかったカード決済の取引 ID も指定可能です。3D セキュアを実施しないカード決済でトークン取得時にカード保有者名を設定した場合は、取引 ID にカード保有者名 (cardholderName) が登録されます。この取引を元取引 ID とする場合はカード保有者名 (cardholderName) は元取引から値が引き継がれます。
- ✓ CardReAuthorizeRequestDto では決済サービスオプションタイプを“mpi-none”に設定した取引は元取引には使用できませんが、MpiReAuthorizeRequestDto では使用可能です。ただし、認可失敗 (MpiAuthorizeResponseDto の mstatus が failure) の取引は使用できません。

応答電文 : MpiReAuthorizeResponseDto				
フィールド名	項目名	書式・制限	説明	設定
※応答電文は認可の応答電文 (MpiAuthorizeResponseDto) と同じ				

4-4 本人認証およびカード決済の結果取得

本人認証およびカード決済の結果は、以下の 4 通りの方法で取得することができます。

項番	結果の取得方法	本ガイドの参照先
①	消費者のブラウザを経由して結果を取得する	4.4.1 消費者のブラウザを経由した結果の取得
②	決済サーバーからの結果通知を受信する	4-5 結果通知
③	本人認証結果確認コマンドを利用する	4.4.2 本人認証結果確認
④	検索(Search)コマンドを利用する	4-6 検索

- ①はブラウザを経由した結果連携のため、画面遷移が正常に行われないケースでは結果を取得することができません。そのため、②の結果通知の受信と組み合わせて確実に結果を取得するようにしてください。
- ③と④は、取引 ID 等のキーとなるパラメータを条件に指定した問合せ型のコマンドになります。
 - ✧ その他の方法と組み合わせて利用されることを想定しています。

4.4.1 消費者のブラウザを経由した結果の取得

本人認証およびカード決済の完了後、消費者のブラウザは加盟店の URL へ画面遷移します。加盟店側のシステムでは、該当取引のキー情報(取引 ID)と認証および決済結果をブラウザを経由して受信することができます。

送信される取引のキー情報を次の表に示します。

消費者ブラウザ経由で店舗へ送信されるキー情報(POST または GET)				
フィールド名	項目名	書式・制限	説明	設定
RequestId	リクエスト ID	半角英数字記号 128 文字以内	本人認証の結果を検索する際のキー項目	○
OrderId	取引 ID	半角英数字 100 文字以内	決済要求時に加盟店サイトにて任意に採番し送信された取引 ID	○

- ✧ ここで送信されるフィールド名「RequestId」と「OrderId」は、旧仕様との互換性を保つため、その他の項目と異なり、先頭文字が大文字となりますのでご注意ください。
- ✧ 旧仕様(veritrans3G の初期仕様)では、「RequestId」をキーとして検索(Search)コマンドによって結果を取得する方法しか提供していませんでしたが、現在の仕様では、その他の方法でも結果をシンプルに取得することが可能になりましたので、これから実装を検討される場合には、RequestId の利用はお勧めしません。

このタイミングで取引の結果は取得せずに、上記のキー情報のみを受信することも可能です。この場合は、別途、結果を決済サーバーに問い合わせる必要があります。キー情報のみを受信する場合は、「4.3.1 認可」の「詳細パラメータ連携フラグ(verifyResultLink)」で、以下のどちらかのパラメータを指定します。

- ✓ 前者を指定すると POST、後者を指定すると GET パラメータとして受信できます。
 - 0:詳細パラメータ連携しない
 - 2:詳細パラメータ連携しない(GET)

次に、このタイミングで取引の結果を取得する場合は、「詳細パラメータ連携フラグ(verifyResultLink)」に以下のパラメータを指定します。

- 1:詳細パラメータ連携する

送信される結果の詳細パラメータを次の表に示します。送信されるパラメータは、今後の機能拡張により追加される可能性がありますので、本書に記載されていないパラメータが連携された場合でもエラーとならないように実装してください。

消費者ブラウザ経由で店舗へ送信される詳細パラメータ(POST)				
フィールド名	項目名	書式・制限	説明	設定
reqAmount	要求取引金額	半角数字 12 桁以内	要求電文に設定した値	○
reqCardNumber	要求カード番号	文字列 16 桁以内	要求電文に設定した値 上 6 桁下 2 桁のみ数字表示され、その他は"*" (アスタリスク)に変換されます。(例 "411111*****11")	○
reqCurrencyUnit	要求通貨単位	半角英字 3 桁以内	要求電文に設定した値	△
mpiMstatus	MPI 結果コード	半角英数字 32 文字以内	本人認証の処理結果ステータス "success": 正常終了 "failure": 異常終了	○
vResultCode	詳細結果コード	文字列 16 桁	処理の結果を詳細に表すコード 4 桁ずつ 4 つのブロックで構成され、各ブロックで サービス毎の処理結果を表します。 詳細は『結果コード一覧』を参照下さい。	○
vAuthInfo	改ざんチェック用 ハッシュ値	文字列 右記参照	下記文字列を連結し、SHA-256 によって算出した ハッシュ値 ・マーチャント CCID ・パラメータ値の連結文字列(authParams が 示す順序で連結) ・パスワード 尚、パラメータ値を連結する際は、パラメータ名 や区切り文字は含めず、パラメータ値のみを連結 しています。連結した文字列をバイナリに変換す る際の文字エンコーディングは、UTF-8 を使用し ています。	○
authParams	ハッシュ値算出パ ラメータ順序	文字列 右記参照	vAuthInfo のハッシュ値を算出する元とした文字 列の、パラメータの連結順序を示す値 パラメータ名のカンマ区切り文字列を Base64 エ ンコードしています。デコードを行うと文字列が復 元されます。 例) "mpiMstatus,vResultCode,OrderId" "OrderId,mpiMstatus,vResultCode" (パラメータの個数と順序は固定ではないため、 リクエスト受信のたびに動的に処理する必要が あります。)	○
以下は、serviceOptionType が(mpi-complete / mpi-company / mpi-merchant)の場合に連携される項目です。				
cardMstatus	カード結果コード	半角英数字 32 文字以内	カード決済の処理結果ステータス "success": 正常終了 "failure": 異常終了 "pending": ペンディング ※MPI 結果コードが failure の場合は空	△

消費者ブラウザ経由で店舗へ送信される詳細パラメータ(POST)				
フィールド名	項目名	書式・制限	説明	設定
cardTransactionType	カードトランザクションタイプ	文字列 6 桁以内	カード決済取引の詳細な状態 "a": 与信 "ax": 与信(期限切れ) "ap": 与信(保留) "ac": 与信売上 "acp": 与信売上(保留)	△
centerRequestDate	センター要求日時	文字列 14 桁以内	カード決済センターへ決済要求を行った日時 YYYYMMDDhhmmss 形式	△
centerResponseDate	センター応答日時	文字列 14 桁以内	カード決済センターの決済応答を受けた日時 YYYYMMDDhhmmss 形式	△
connectedCenterId	接続先カード接続センター	文字列 5 桁以内	決済サーバー⇒カード会社間の接続センター名 例: 'jcn'	△
acquirerCode	要求仕向け先コード	文字列 2 桁以内	決済要求電文が最初に仕向けられたカード会社のコード 仕向け先カード会社の一覧は『インターフェース詳細 〜クレジットカード決済〜』の「クレジットカード決済 仕向け先カード会社の一覧」を参照	△
authCode	応答承認番号	半角英数字スペース 7 桁以内	カード会社が発行する承認番号	△
fdResult	不正検知結果コード	半角数字 3 桁以内	不正検知結果 "100": accept "200": deny "300": challenge "400": error "500": timeout "600": internal error "": 値なし(空白) 不正検知を実施する場合のみ返戻します。	※
tradUrl	trAd URL	半角文字列 512 文字以内	現在使用していません。	×
以下は、serviceOptionType が(mpi-none)の場合に連携される項目です。				
dddMessageVersion	3D メッセージバージョン	半角英数字記号 10 桁以内	Message Version Number (例 "2.1.0")	△
dddTransactionId	3D トランザクション ID	半角英数字、 "+", "/", "=", 28 桁	Transaction Identifier(XID)の値を Base64 で変換した値 ※3D セキュア 2.0 でも、AMEX の場合にカード与信に本項目を設定する必要があります。 ※値が返戻された場合はカード与信電文に本項目を設定してください。	△
dddDsTransactionId	3DDS トランザクション ID	半角英数字、 "-", "+", "/", "=", 36 桁以内	DS Transaction ID ※3D メッセージバージョンが"2.1.0"以上の場合のみ返戻します。 ※UUID のフォーマットまたは BASE64 エンコードされた値が返戻されます。	△
dddServerTransactionId	3D サーバートランザクション ID	半角英数字、 "-" 36 桁以内	Server Transaction ID ※3D メッセージバージョンが"2.1.0"以上の場合のみ返戻します。 ※UUID のフォーマットで返戻されます。	△

消費者ブラウザ経由で店舗へ送信される詳細パラメータ(POST)				
フィールド名	項目名	書式・制限	説明	設定
dddTransactionStatus	3D トランザクションステータス	半角英数字 1 桁 右記参照	3D セキュアトランザクションステータス "Y": 本人認証成功 "N": 本人認証失敗(イシューまたは会員が原因) "U": 本人認証失敗(上記以外が原因) "A": Attempt(暫定的に本人認証成功) "R": 本人認証拒否 "": 値なし(空白) ※値のバリエーションは増える可能性があります	△
dddTransactionStatusReason	3D トランザクションステータス理由	半角数字 2 桁	3D トランザクションステータスの値の設定理由 ※3D メッセージバージョンが"2.1.0"以上の場合のみ返戻します。	△
dddCavvAlgorithm	3DCAVV アルゴリズム	半角英数字 1 桁 右記参照	3D セキュア CAVV アルゴリズム "0": HMAC "1": CVV "2": CVV with ATN "3": SPA Algorithm "4": AEVV Algorithm "9": 取引毎の指定なし(2.1.0 以上の場合) "": 値なし(空白) ※値のバリエーションは増える可能性があります	△
dddCavv	3DCAVV	半角英数字、 "+", "/", "=" 28 桁	3D セキュア CAVV (Base64 で変換した値)	△
dddEci	3DECI	半角数字 2 桁 右記参照	3D セキュア ECI "02", "05": 認証成功 "01", "06": Attempt "04", "07": 認証実行失敗または不能 "": 値なし(空白) ※値のバリエーションは増える可能性があります	△

◇ 改ざんチェックの実装について

決済サーバーから消費者ブラウザを経由して加盟店サイトの結果画面に遷移(リダイレクト)しますが、ここで加盟店サイトが受け取った POST パラメータが改ざんされていないか検証することを推奨しています。この改ざんチェックでは、リダイレクト時に返戻される「vAuthInfo」、および「authParams」パラメータを使用します。店舗側システムで算出したハッシュ値が、リダイレクト時のパラメータより取得した「vAuthInfo」と一致している場合は、パラメータは改ざんされていない、とみなすことができます。

※悪意を持った第三者によって、不正なリダイレクト電文を受信する可能性がありますので、改ざんチェックの**実装を強く推奨します**。

※実装方法の詳細につきましては、弊社より提供しているサンプルプログラムをご参照ください。

4.4.2 本人認証結果確認

指定した取引IDの認証結果およびカード決済の結果を取得します。

要求電文 : MpiGetResultRequestDto				
フィールド名	項目名	書式・制限	説明	設定
orderId	取引 ID	半角英数字 100 桁以内	取引を識別する一意の ID	○

応答電文 : MpiGetResultResponseDto				
フィールド名	項目名	書式・制限	説明	設定
serviceType	決済サービスタイプ	半角英数字 10 桁以内	要求電文を送信した決済サービスタイプ。	○
mstatus	処理結果コード	半角英数字 32 文字以内	“success” : 正常終了 “failure” : 異常終了 注意: 本要求(コマンド)に対する処理結果を示します。 決済の成功・失敗を示すものではありません。	○
vresultCode	詳細結果コード	文字列 16 桁	処理結果の詳細を示すコードです。 詳細は『結果コード一覧』をご参照下さい。 注意: 本要求(コマンド)に対する処理結果を示します。 決済の成功・失敗を示すものではありません。 本要求が成功した場合は「G021000000000000」が返戻されます。	○
merrMsg	エラーメッセージ	文字列	処理結果を日本語で表示します。	○
orderId	取引 ID	文字列 100 桁以内	決済要求時に加盟店にて任意に採番し送信された取引 ID	○
txnVersion	MDK バージョン	半角英数字 5 文字以内	電文のバージョン 問題発生時などに用いますが、通常ご利用になることはありません。	○
requestId	リクエスト ID	半角英数字記号 128 桁以内	本人認証の結果を検索する際のキー項目	○
reqAmount	要求取引金額	半角数字 12 桁以内	要求電文に設定した値	○
reqCardNumber	要求カード番号	文字列 16 桁以内	要求電文に設定した値 上 6 桁下 2 桁のみ数字表示され、その他は“*” (アスタリスク)に変換されます。(例 “411111*****11”)	△
reqCurrencyUnit	要求通貨単位	半角英字 3 桁以内	要求電文に設定した値	△
mpiMstatus	本人認証処理結果コード	半角英数字 32 桁以内	本人認証の処理結果ステータス “success” : 正常終了 “failure” : 異常終了	△
mpiVresultCode	本人認証詳細結果コード	文字列 16 桁以内	本人認証の処理結果の詳細を示すコードです。 4 桁ずつ 4 つのブロックで構成され、各ブロックで サービス毎の処理結果を表します。 詳細は『結果コード一覧』を参照下さい。	△
txnType	トランザクションタイプ	半角英数字 32 桁以内	本人認証の実施方法を表す値 “AuthorizeConfirm” : フリクションレスフロー “VerifyNotify” : チャレンジフロー	△

以下のフィールドは、消費者ブラウザ経由で店舗へ送信されるパラメータと同じです。各フィールドの詳細は「4.4.1 消費者のブラウザを経由した結果の取得」をご参照ください。

フィールド名	項目名	書式・制限	説明	設定
以下は、serviceOptionType が(mpi-complete / mpi-company / mpi-merchant)の場合に連携される項目です。				
cardMstatus	カード結果コード	詳細は「4.4.1 消費者のブラウザを経由した結果の取得」をご参照ください。		△
cardTransactionType	カードトランザクションタイプ			△
centerRequestDate	センター要求日時			△
centerResponseDate	センター応答日時			△
connectedCenterId	接続先カード接続センター			△
acquirerCode	要求仕向け先コード			△
authCode	応答承認番号			△
fdResult	不正検知結果コード			※
tradUrl	trAd URL			×
以下は、serviceOptionType が(mpi-none)の場合に連携される項目です。				
dddMessageVersion	3D メッセージバージョン	詳細は「4.4.1 消費者のブラウザを経由した結果の取得」をご参照ください。		△
dddTransactionId	3D トランザクション ID			△
dddDsTransactionId	3DDS トランザクション ID			△
dddServerTransactionId	3D サーバトランザクション ID			△
dddTransactionStatus	3D トランザクションステータス			△
dddTransactionStatusReason	3D トランザクションステータス理由			△
dddCavvAlgorithm	3DCAVV アルゴリズム			△
dddCavv	3DCAVV			△
dddEci	3DECI			△

4-5 結果通知

決済サーバーは、本人認証、およびクレジットカード決済の結果を加盟店サイトへ通知します。

尚、本人認証結果の検証後(連動してクレジットカード決済が実行される場合は決済実行後)に、決済成否に関わらず通知します。

結果通知に関するサービス共通の仕様については、『開発ガイド』を併せてご参照ください。

項番	フィールド名	項目名	書式・制限	説明
1	numberOfNotify	通知件数	半角数字 4桁以内	1度に通知可能な件数は50件 51件以上は次回通知
2	pushTime	送信時刻	半角数字 14桁	決済サーバーから通知した時刻 YYYYMMDDhhmmss 形式
3	pushId	識別 ID	半角数字 8桁	プッシュ処理を行うたびに採番される ID 注) 他の決済サービスで使用された ID と重複する場合があります。
通知件数分下記の項番(4~9)を繰り返す。尚、フィールド名の後ろに4ケタの連番(0000~0049)を付与する。				
4	orderId	取引 ID	半角英数字 100桁以内	取引を識別する一意の ID
5	vResultCode	詳細結果コード	半角英数字 16桁	処理結果を詳細に表すコード 処理結果コードの詳細は、『結果コード一覧』をご参照ください。
6	txnType	トランザクションタイプ	半角英数字 32桁以内	"Verify": 本人認証結果(3D セキュア 1.0 のみ) "AuthorizeConfirm": 本人認証結果(2.0 で追加) "VerifyNotify": 本人認証結果(2.0 で追加)
7	mpiMstatus	MPI 結果コード	半角英数字 8桁以内	本人認証の処理結果ステータス "success": 正常終了 "failure": 異常終了
8	cardMstatus	カード結果コード	半角英数字 8桁以内	"success": 正常終了 "failure": 異常終了 "pending": ペンディング ※mpi-none(MPI 単体サービス)の場合と MPI 結果コードが failure の場合は空
9	dummy	ダミー決済フラグ	半角数字 1桁	ダミー取引の場合"1"、本番取引の場合"0"

(注意事項)

- ◇ 本人認証サービスの結果通知機能をご利用の場合は、認可の要求電文に pushUrl を指定するか、MAP の各種設定変更より、本人認証の結果通知 URL を設定してください。どちらも設定した場合には、要求電文の pushUrl が優先されます
- ◇ pushId(識別 ID)は、他の決済サービスで使用された Id と重複する場合がありますので、ユニークキーとして処理しないようにしてください。
- ◇ 項目の並び順は、必ずしも表の順序とは一致しません。

4-6 検索

■「設定」欄の内容は以下の通りとなります。

要求電文 … 必須項目:○ 任意項目:△ 設定不可:× その他条件付:※(条件は説明欄に記入)

応答電文 … 必ず返戻:○ 該当取引存在時に返戻:△ 返戻なし:× その他条件付:※

■複数指定は 0～の添字を指定します。

例) exparam.serviceTypeCd[0]=card&exparam.serviceTypeCd[1]=mpi

■ワイルドカードは値の一部と“*”を組み合わせで検索します。“*”のみの指定はできません。

例) exparam.searchParameters.common.orderId=123*

要求電文 : SearchRequestDto						
※ 以下は、共通の検索要求フィールドです。						
検索フィールド名	検索項目名	書式・制限	複数指定	ワイルドカード	説明	設定
requestId	リクエスト ID	半角英数字記号 128 文字以内			リクエスト ID を指定します。指定した場合は、それ以外のパラメータは指定できなくなります。	△
serviceTypeCd	決済サービスタイプ	右記参照	○		検索対象の決済を指定します。未指定の場合は、全決済が検索対象となります。 “mpi”: 本人認証	△
newerFlag	最新トランザクションフラグ	右記参照			成功、失敗に関係なく、最新トランザクションのみを検索する場合に使用します。 “true”: 1 取引内の最新トランザクションのみ検索 “false”: 全てのトランザクションを検索 ※指定しない場合は“false”になります。	△
containDummyFlag	ダミー決済対象フラグ	右記参照			ダミー取引も検索する場合に使用します。 “true”: ダミー取引も検索する “false”: ダミー取引は検索しない ※指定しない場合は“false”になります。	△
maxCount	検索最大件数	1～1000			取得したい検索結果の最大件数です。未指定の場合、最大値となります。 ※短時間で大量の検索を繰り返すような処理はサーバーに負荷が掛かりますのでご遠慮頂けますようお願いいたします。	△
common 共通						
orderId	取引 ID	半角英数字 100 桁以内		○	検索したい取引 ID を指定します。	△

orderStatus	取引決済状態	右記参照	○		以下のいずれかを指定します。 " initial ": 初期状態 " end ": 終了 " end_presentation ": 画面遷移正常終了 " pending ": 保留 " validation_error ": 検証エラー " expired ": 期限切れ " error ": エラー	△
command	コマンド	右記参照	○		決済で使用するコマンドを指定します。 " Authorize ": 認可申込 " Verify ": 検証(3D セキュア 1.0) " AuthorizeNotify ": 認可通知(3D セキュア 2.0) " AuthorizeConfirm ": 認可確認(同) " VerifyNotify ": 検証通知(同) " ResultRedirect ": 結果リダイレクト(同)	△
mstatus	ステータスコード	右記参照	○		決済結果として返戻されるステータスコードを指定します。 " success ": 成功 " failure ": 失敗	△
txnDatetime.from	取引日(From)	文字列 12 桁			取引日時の範囲(From)を指定します。 YYYYMMDDhhmm 形式	△
txnDatetime.to	取引日(To)	文字列 12 桁			取引日時の範囲(To)を指定します。 YYYYMMDDhhmm 形式	△
amount.from	金額(From)	数字 12 桁以内			決済金額の範囲(From)を指定します。	△
amount.to	金額(To)	数字 12 桁以内			決済金額の範囲(To)を指定します。	△

※ 以下は、本人認証 固有の検索要求フィールドです。

mpi 本人認証 固有						
detailOrderType	詳細オーダー決済状態	右記参照	○		※「detailOrderType」の詳細は 5-7 検索(Search)に関する補足を参照	△
res3dTransactionId	応答 3D トランザクション ID	半角英数字、“+”、“/”、“=” 28 桁 or 0 桁			応答 3D トランザクション ID を指定	△
resTransactionStatus	応答 3D トランザクションステータス				応答 3D トランザクションステータスを指定	△
res3dId	応答 3D ECI				応答 3D ECI を指定	△
deviceChannel	デバイスチャネル	半角数字 2 桁			デバイスチャネルを指定 3D セキュア 2.0 で追加された項目	△
accountType	アカウントタイプ	半角数字 2 桁			アカウントタイプを指定 3D セキュア 2.0 で追加された項目	△
authenticationIndicator	認証要求タイプ	半角数字 2 桁			認証要求タイプを指定 3D セキュア 2.0 で追加された項目(予約項目)	△
messageCategory	メッセージカテゴリ	半角数字 2 桁			メッセージカテゴリを指定 3D セキュア 2.0 で追加された項目(予約項目)	△

応答電文 : SearchResponseDto

※ 以下は、共通の検索結果フィールドです。

検索フィールド名	検索項目名	書式・制限	説明	設定
result	処理結果	—		○
serviceType	サービスタイプ	右記参照	"search"	○
mstatus	処理結果コード	半角英数字 32 文字以内	処理の結果ステータスが格納されます。 "success": 正常終了 "failure": 異常終了	○
vResultCode	詳細結果コード	半角英数字 16 文字	処理の結果を詳細に表すコードとなります。 詳細は別途『結果コード一覧』を参照下さい。	○
merrMsg	エラーメッセージ	文字列 300 文字以内	処理結果を日本語又は英語で表示します。	○
overMaxCountFlag	最大件数超えフラグ	右記参照	検索対象データが要求電文で指定した検索最大件数より多いかどうかを表します。 "true": 最大件数以上 "false": 最大件数未満	△
searchCount	検索結果件数	0～1000	検索結果件数(オーダー件数)が格納されます。	△
orderInfos	オーダー情報リスト		複数のオーダー情報(orderInfo)が格納されます。	△
orderInfo	オーダー情報	—	検索条件に該当した取引の情報が該当件数分繰り返されます。0～1000 件(要求電文で指定した検索最大件数まで)となります。	△
index	インデックス	0～999	検索された情報のインデックスが格納されます。	△
serviceTypeCd	決済サービスタイプ	右記参照	決済の種類が格納されます。 "mpi": 本人認証サービス	△
orderId	取引 ID	文字列	取引の取引 ID が格納されます。	△
orderStatus	取引決済状態	右記参照	決済の状態が格納されます。 "initial": 初期状態 "end": 終了 "end_presentation": 画面遷移正常終了 "pending": 保留 "validation_error": 検証エラー "expired": 期限切れ "error": エラー ※このフィールドは、取引 ID に関連する注文データの 状態を完全に表現するものではありません。サ ービスタイプによっては詳細な状態遷移を別のフ ィールドに保持している場合がありますので、店 舗側システムの用途に合わせて successDetailTxnType や、決済固有の状態フィー ルドをご参照ください。	△
lastSuccessTxnType	最終成功トランザクションタイプ	文字列	直近の成功したコマンド名が格納されます。	△
successDetailTxnType	詳細トランザクションタイプ	文字列	取引の詳細な状態が格納されます。 検索要求電文の各決済の detailOrderType 参照。	△
properOrderInfo	固有オーダー情報	—	各決済サービスの固有オーダー情報が格納されま す。後述の一覧参照。	△

				transactionInfos	決済トランザクションリスト	—	複数の決済トランザクション情報 (transactionInfo) が格納されます。	△	
				transactionInfo	transactionInfo	決済トランザクション情報	—	検索条件に該当した取引の情報が該当件数分繰り返されます。	△
					txnId	トランザクション管理 ID	文字列	決済サーバーが採番する管理 ID となります。	△
					command	コマンド	文字列	実行されたコマンド名が格納されます。 ※MDK で要求したコマンドだけでなく、決済サーバーの内部処理コマンドも含まれます。	△
					mstatus	処理結果コード	半角英数字 32 文字以内	処理の結果ステータスが格納されます。 "success": 正常終了 "failure": 異常終了 "pending": 保留	△
					vResultCode	詳細結果コード	文字列 16 桁	処理の結果を詳細に表すコードとなります。 詳細は別途『結果コード一覧』を参照下さい。	△
					txnDatetime	取引日時	文字列 23 桁	取引日時が格納されます。 YYYY-MM-DD hh:mm:ss.mmm 形式	△
					amount	金額	半角数字 12 桁以内	決済した金額が格納されます。	△
					properTransactionInfo	固有トランザクション情報	—	各決済サービスの固有トランザクション情報が格納されます。後述の一覧参照。	△
★ 以下の情報は、上記「固有オーダー情報」「固有トランザクション情報」内の階層にセットされます。									
※ 以下は、本人認証 固有の検索結果フィールドです。									
properOrderInfo		本人認証 固有オーダー情報							
	startTxn	電文 ID	文字列					△	
	dddMessageVersion	メッセージバージョン						△	
	requestCurrencyUnit	要求通貨単位	半角英数字 4 桁以内					△	
	cardExpire	カード有効期限	文字列 5 桁以内			有効期限 (全桁平文)		△	
	deviceChannel	デバイスチャネル	半角数字 2 桁			3D セキュア 2.0 で追加された項目		△	
	accountType	アカウントタイプ	半角数字 2 桁			3D セキュア 2.0 で追加された項目		△	
	authenticationIndicator	認証要求タイプ	半角数字 2 桁			3D セキュア 2.0 で追加された項目 (予約項目)		△	
	messageCategory	メッセージカテゴリ	半角数字 2 桁			3D セキュア 2.0 で追加された項目 (予約項目)		△	
properTransactionInfo		本人認証 固有トランザクション情報							
	txnKind	トランザクション種類	文字列			"mpi": 3D セキュア "card": カード決済		△	
	mpiTransactionType	MPIトランザクションタイプ	文字列 6 桁以内			取引の詳細な状態 検索要求電文の各決済の detailOrderType 参照。		△	
	reqCardNumber	要求カード番号	文字列 16 桁以内			上 6 桁下 2 桁のみ数字表示され、その他は "*" (アスタリスク) 1 つに変換されます。 (例 "411111*11")		△	
	reqCardExpire	要求カード有効期限	文字列 5 桁以内			全桁 "*" (アスタリスク) に変換されます。 (例 "*****")		△	
	reqAmount	要求取引金額	文字列 12 桁以内					△	

reqRedirectionUri	要求リダイレクション URI	文字列 1024 桁以内		△
corporationId	会社ID	文字列 2 桁以内		△
brandId	ブランドID	文字列 2 桁以内		△
acquirerBinary	仕向け先 Binary	文字列		△
dsLoginId	dsLoginId	文字列		△
crresStatus	crresStatus	文字列		△
veresStatus	veresStatus	文字列		△
paresSign	paresSign	文字列		△
paresStatus	paresStatus	文字列		△
paresEci	paresEci	文字列		△
authResponseCode	本人認証応答コード	文字列		△
verifyResponseCode	認証結果検証応答コード	文字列		△
res3dMessageVersion	応答 3D メッセージバージョン	文字列 10 桁以内		△
res3dTransactionId	応答 3D トランザクション ID	文字列 28 桁以内		△
res3dDsTransactionId	応答 3D DS トランザクション ID	文字列 36 桁以内	3D セキュア 2.0 で追加された項目	△
res3dServerTransactionId	応答 3D サーバトランザクション ID	文字列 36 桁以内	3D セキュア 2.0 で追加された項目	△
res3dTransactionStatus	応答 3D トランザクションステータス	文字列 1 桁以内		△
res3dCavvAlgorithm	応答 3D CAVV アルゴリズム	文字列 1 桁以内		△
res3dCavv	応答 3D CAVV	文字列 28 桁以内		△
res3dEci	応答 3D ECI	文字列 2 桁以内		△
authRequestDatetime	認可要求日時	文字列 23 桁以内	認可要求の受付時間 (YYYY-MM-DD hh:mm:ss.mmm)	△
authResponseDatetime	認可応答日時	文字列 23 桁以内	認可の応答時間 (YYYY-MM-DD hh:mm:ss.mmm)	△
verifyRequestDatetime	認証結果検証要求日時	文字列 23 桁以内	認証結果検証要求の受付時間(YYYY-MM-DD hh:mm:ss.mmm)	△
verifyResponseDatetime	認証結果検証応答日時	文字列 23 桁以内	認証結果検証の応答時間 (YYYY-MM-DD hh:mm:ss.mmm)	△
reqCurrencyUnit	要求通貨単位	文字列 4 桁以内	※現在はこちらはご利用いただくことはできません。	△
reqAcquirerCode	要求仕向け先コード	文字列 2 桁以内	※現在はこちらはご利用いただくことはできません。	△

reqItemCode	要求商品コード	文字列 7 桁以内	※現在のご利用いただくことはできません。	△
reqCardCenter	要求カードセンター	文字列 7 桁以内	※現在のご利用いただくことはできません。	△
reqJpoInformation	要求支払種別情報	文字列 83 桁以内		△
reqSalesDay	要求売上日	文字列 8 桁以内	※現在のご利用いただくことはできません。	△
reqWithCapture	要求同時直接	文字列 8 桁以内		△
reqSecurityCode	要求セキュリティコード	文字列 4 桁以内	全桁“0”(ゼロ)に変換されます。 (例 “0000”)	△
reqBirthday	要求誕生日	文字列 4 桁以内	※現在のご利用いただくことはできません。	△
reqTel	要求電話番号	文字列 4 桁以内	※現在のご利用いただくことはできません。	△
reqFirstKanaName	要求カナ名前(名)	文字列 15 桁以内	※現在のご利用いただくことはできません。	△
reqLastKanaName	要求カナ名前(姓)	文字列 15 桁以内	※現在のご利用いただくことはできません。	△

第5章 その他 補足事項

5-1 決済サービスオプションタイプについて

VeriTrans4G 本人認証サービスでは、3D セキュア認証の結果をもとにクレジットカード与信(カード与信)処理まで実施可能です。カード与信を実施するかしないかの判定ルールは、「決済サービスオプションタイプ(serviceOptionType)」に指定する値によって異なります。

① mpi-complete(完全認証)

カード会社が認証成功と判定した場合のみ、カード与信を実施します。

② mpi-company(通常認証)

カード会社が認証成功 または みなし認証成功(Attempt)と判定した場合、カード与信を実施します。

③ mpi-merchant(通常認証:加盟店リスクあり)

できる限りカード与信を実施するモードになります。加盟店様が 3D セキュアのご利用契約をされていないブランドのカード、処理中にエラーが発生した場合でも加盟店リスク負担でカード与信を実施します。ただし、3D セキュア認証処理が正常に行われ、明確に NG(ステータス N 受信ケースなど)の場合、カード与信は行いません。

④ mpi-none(単体認証)

本人認証(3D セキュア認証)のみを実施し、カード与信は実施しません。カード与信を実施するかの判断とカード与信の処理(リクエスト)は加盟店様で行う必要があります。カード与信を実施するかの判断方法は mpi-none 以外のモードの判定を参考に実装してください。カード与信は CardAuthorizeRequestDto を使用します。「MPI(3D セキュア)の結果を連携する場合に使用するフィールド」に本人認証の結果を設定してください。詳しくは、クレジットカード決済のインターフェース詳細をご参照ください。

mpi-none は、3D セキュア認証とカード決済の処理を分けて実行できるため、カード決済の与信を加盟店様のタイミングで実行したい場合に利用されるケースが多いです。また、何等かの理由で弊社からの結果通知を受信できない場合にも利用されることがあります。

しかし、mpi-none の場合は、与信を実行するか否かの判定を加盟店様のシステムで実装する必要があり、また、与信の要求時には 3D セキュアの認証結果を正確に設定しなければチャージバックリスクとなるため、少し難易度が高いです。

mpi-none 以外を利用する場合は、弊社側でこれらの処理を行いますのでその点では難易度は低いです。しかし、結果通知を必ず受信していただく必要があります。

※結果通知を受信しないと、決済の成立を加盟店側で検知できないことがあり、お客様が支払ったのに注文が成立しなかったり、注文が不成立のため、再度お客様が決済を実行して 2 重決済となるなど、クレームに発展するリスクがあります。

決済サービスオプションタイプ別の結果の判定方法の詳細については、「本人認証サービス補足資料(3D セキュア 2.0 版)」の「1.決済サービスオプションタイプについて」「4-3.結果判定マトリックス」を参照してください。

5-2 決済結果の判定について

本人認証サービスでは、決済サービスオプションタイプ(serviceOptionType)が”mpi-none”である場合を除き、本人認証の成功時(みなし成功を含む)には、カード決済が実行されます。

加盟店サイトでは、必ずカード決済が成功したことをご確認のうえ、商品の発送やサービスのご提供を行うようにしてください。

カード決済が成功した場合の結果コードの例を以下に示します。

```
vResultCode      : G012A001
mpiMstatus       : success
cardMstatus      : success
```

以下は、本人認証は成功、カード決済は失敗の例です。

```
vResultCode      : G012AG33
mpiMstatus       : success
cardMstatus      : failure
```

注意:

本人認証結果確認コマンドで確認する場合、決済結果の判別は mpiVresultCode で行ってください。vResultCode に設定される値は本人認証結果確認コマンド自体の処理結果コードとなります。

5-3 決済サーバーと加盟店サイト間の取引不整合の問題

本人認証およびカード決済の成功後、消費者のブラウザから加盟店サイトの完了画面に遷移しなかった場合、あるいは遷移に失敗して処理の途中で離脱した場合には、加盟店サイトではカード決済の成立を認識できないという問題が発生する場合があります(取引不整合)。この問題は、以下のような状況で発生する可能性があります。

- カード会社の本人認証画面(パスワード入力画面)で長時間滞留したため、加盟店サイトでセッションタイムアウト(注文の期限切れ等)が発生したことによって、決済結果の反映処理が行えなかった場合
- 本人認証の成功後にブラウザを閉じる等の操作を行った

この問題に対処するために、加盟店サイトでは以下の何れかの実装を行って頂きますようお願いいたします。

- ① 決済サーバーからの決済結果通知(PUSH)を受信する(「5-5 結果通知の送信(Push)」をご参照ください)
- ② 本人認証結果確認コマンドで、決済が成立していないかどうかを確認する
- ③ 未成立の取引を Search コマンドで検索し、決済が成立していないかどうかを確認する(新規に実装される場合、非推奨。② 本人認証結果確認コマンドをご利用ください)

なお、Search コマンドをご利用の場合は、必ず「5-2 決済結果の判定について」を参考に、「カード決済が成功しているかどうか」をご確認ください。

5-4 決済結果の詳細パラメータ連携と GET によるリダイレクション URI へのアクセス

消費者のブラウザを経由して送信する認証結果およびカード決済の結果は、HTTP の POST メソッドで送信しています。そのため、各種ブラウザの仕様変更に伴う、Cookie の SameSite 属性の挙動変更の影響には注意が必要です。

VeriTrans4G では、3D セキュア 2.0 への対応に合わせて、リダイレクション URI に遷移する際に HTTP GET で遷移できるようにするフラ

グを用意しましたので、POST メソッドでの遷移に問題がある場合にはこのフラグの利用をご検討ください。

- ✓ 「4.3.1 認可」の「詳細パラメータ連携フラグ (verifyResultLink)」で、2 を指定すると HTTP GET で遷移します。

0:詳細パラメータ連携しない	(キー情報のみ POST で送信)
1:詳細パラメータ連携する (POST)	(キー情報と結果すべてを POST で送信)
<u>2:詳細パラメータ連携しない (GET)</u>	(キー情報のみ GET で送信)

ただし、HTTP GET による遷移の場合、クエリパラメータにはキー情報のフィールド(「取引 ID」と「リクエスト ID」)のみが設定されますので、別途、キー情報を利用して認証および決済の結果を問い合わせる必要があります。詳しくは、「4-4 本人認証およびカード決済の結果取得」をご参照ください。

- ◇ HTTP GET による遷移は、ブラウザの再読み込み(リロード)操作により、**同じリクエストが複数回届くケースが発生**いたしますので、同じリクエストが届いても問題ないように実装してください。(HTTP POST による実装の場合、再読み込みを行った場合はリクエストからパラメータが取得できないため、動作として問題となっていない可能性もあります。)
- ◇ 従来の仕様では、詳細パラメータ連携の有効・無効の切り替えは、決済サーバーのマスタ設定を弊社で変更するしかありませんでしたが、verifyResultLink フラグによる制御を優先するようになり、加盟店様の実装にて切り替えが可能となりましたので、フラグによる切替を実装される加盟店様は、特にマスタ設定を意識する必要はありません。
- ◇ 詳細パラメータ連携を有効にする場合、決済サービスオプションタイプ (serviceOptionType) で MPI 単体サービス ("mpi-none") を選択する場合は、リダイレクト先となる加盟店サイトの結果画面の URI は SSL(https://)を必須とします。ダミーモードでのテストも考慮し、HTTP の URI を指定した場合でもエラーにはなりませんのでご注意ください。

5-5 結果通知の送信 (Push)

決済サーバーから加盟店サイトへ、本人認証結果、およびクレジットカード決済結果を送信 (Push) する機能です。

本人認証サービスの決済フローは、加盟店サイトから一度外部サイトにブラウザ(クライアント)を遷移する形となっており、外部サイトにて決済処理を行い、またブラウザを経由して加盟店サイトに戻ります。

ブラウザを経由した遷移は、正しく行われない(リダイレクトが届かない)ケースは発生するものとしてご認識ください。

つまり、外部サイト (VeriTrans4G 側) で本人認証の結果、クレジットカード与信処理が行われたが、その後、加盟店サイトに戻ってこない事象が発生し、加盟店サイトでは決済が完了していないという不整合が発生する可能性があります。

結果通知を受信することで、消費者が離脱してしまった場合でも、決済が行われたかどうかを加盟店サイトにて把握することが可能となります。

なお、結果通知は、クレジットカード決済の結果が失敗の場合も送信 (PUSH) されます。

結果通知は、認可要求時のパラメータ、または MAP (マーチャント管理ポータル) の「各種設定変更」より設定した URL に届きます。

なお、古いバージョンの MDK では、認可要求時に通知先 URL を指定できないものもございますが、3D セキュア 2.0 対応の MDK では指定可能となっております。

結果通知の受信処理については、『4G 開発ガイド』を参照してください。

5-6 本人認証処理の有効期限

本人認証有効期限 (verifyTimeout) の設定により、本人認証の画面で長時間滞留する等、認証完了までに時間がかかった取引を無効 (タイムアウトエラー) にすることができます。

例えば、加盟店サイトのセッションタイムアウトが 30 分の場合は、verifyTimeout 値を 30 分よりも短く設定することで、決済サーバー側で決済が成立しているにもかかわらず、加盟店サイトに戻ったときにセッションタイムアウトエラーになる、という問題を回避することができます。

3D セキュア 2.0 のフローでタイムアウトがチェックされるのは次の 2 つのタイミングとなります。

- 1) 検証処理開始時 (AReq 送信前)
- 2) RReq 受信時

- ◇ 処理フローについては、「本人認証サービス補足資料(3D セキュア 2.0 版)」を参照してください。
- ◇ タイムアウト判定の起点は、厳密には決済サーバーの認可処理の完了時間に近いタイミングとなり、加盟店サイトからリクエストを送信したタイミングが起点ではないためご注意ください。

1)のタイミングでタイムアウトした場合は、決済サーバーは AReq 送信を行わず、MPI 処理結果失敗 (mpiMstatus=failure) でリダイレクション URI に遷移が戻るフローとなります。

- ◇ verifyTimeout 値は分単位の設定のため、1)のタイミングでタイムアウトする可能性は高くはありません。

2)のタイミングでタイムアウトした場合は、RReq の内容が認証可 (オーソリ可) の場合でも決済サーバーはオーソリを行わず、MPI 処理結果失敗 (mpiMstatus=failure) でリダイレクション URI に遷移が戻るフローとなります。

タイムアウト発生時の結果コードは 3D セキュア 1.0 と変わりません。

GA11000000000000: 認証処理の制限時間を過ぎているため、注文処理に失敗しました。

消費者様より当エラーに関する問合せがあった場合は、「タイムアウトエラーのため注文をやり直していただく必要がある」ことをご案内ください。

本人認証有効期限を設定しなければ、有効期限の判定は行われません。この場合、弊社サービス上のタイムアウトは発生しないため、消費者のブラウザ操作のタイミング次第で、長時間経過後に決済が成立することがあります。

5-7 検索(Search)に関する補足

決済サーバーは、取引 ID 毎の内部処理(トランザクション)の履歴と現在の決済状態を保持しています。

Search コマンドでは決済サーバーが保持しているトランザクション情報を取得することが可能ですが、各トランザクションの種類は「トランザクションタイプ」で表されます。

下表に 3D セキュアおよびカード決済の主なトランザクションタイプを示します。

タイプ名	設定値	処理成功時の状態
3D セキュアのトランザクションタイプ		
認可	auth	本人認証の認可が成功したことを示す。
認可(条件付)	authc	本人認証の認可が条件付き成功となったことを示す。
検証	vd	本人認証の検証が成功したことを示す。
検証(条件付)	vdc	本人認証の検証が条件付き成功となったことを示す。
検証(スキップ)	vds	本人認証をスキップしたことを示す。
チャレンジ認証	chg	本人認証のチャレンジ認証を実施したことを示す。
カード決済のトランザクションタイプ		
与信	a	与信が成功したことを示す。
与信売上	ac	与信同時売上が成功したことを示す。
売上	pa	売上が成功したことを示す。(与信後の売上要求による)
与信→取消	va/rad/rae	与信の取消が成功したことを示す。 与信に対する一部金額の取消は通常は実行されませんが、実行された場合に金額の残りがあ る場合は rae、ない場合は rad となります。
与信売上→取消	vac/racd/race	与信売上の取消が成功したことを示す。 部分返品を実行後の時点で、残高がある場合は race、残高がない場合は racd となる。
売上→取消	vpa/rpad/rpae	売上の取消が成功したことを示す。 部分返品を実行後の時点で、残高がある場合は rpae、残高がない場合は rpad となる。
与信有効期限切れ	ax	与信有効期限(通常 60 日)を超えた取引を示す。

注) 一覧に記載していないタイプも存在します。

表 5.1 トランザクションタイプ

- ✓ 取引の状態確認が必要な場合には、Search の結果から orderInfo.successDetailTxnType(詳細トランザクションタイプ)を参照することで、現在の決済状態を確認できます。ただし、orderInfo.successDetailTxnType には「直前に成功したトランザクションのタイプ」が設定される仕様のため、その後の処理が失敗したことを明確に示すことはできません。

例)

"successDetailTxnType": "a" ⇐ 与信が成功した状態であることを示します。

"successDetailTxnType": "vpa" ⇐ 売上の取消が成功した状態であることを示します。

- ✓ 取引 ID 毎の Search の結果には、3D セキュアの認証結果とカード決済の結果が含まれます。カード決済の結果詳細を確認するには、カード決済のトランザクション情報(transactionInfo)を参照してください。トランザクション情報の種類は、properTransactionInfo.txnKind(トランザクション種類)で識別できます。

✧ "txnKind": "mpi" ⇐ 3D セキュアのトランザクション情報であることを示します。

✧ "txnKind": "card" ⇐ カード決済のトランザクション情報であることを示します。

5-8 3D セキュア認証が成功しない場合の対処方法

3D セキュアのエラーのうち、消費者起因の認証エラーの原因は、消費者(カードの所有者)からカード発行元にお問い合わせいただかなければ開示されません。

消費者から発行元カード会社へお問い合わせする際には、次の内容を伝えるようにご案内ください。

- ・サイト名
- ・決済日時
- ・決済金額
- ・エラー内容(必ず、3D セキュアで認証エラーになったことを伝えてください)

何らかの事情で 3D キュア認証がエラーになるものの、決済ができないと困るというケースでは、3Dセキュアなしの決済 (CardAuthorizeRequestDto または CardReAuthorizeRequestDto)を行ってください。3Dセキュアなしの決済ですのでチャージバックリスクは加盟店様の負担になります。利用者の身元確認など不正利用が発生しないよう対処を行った上で決済するようにしてください。

現時点で、3D セキュア未対応のカードを使用した場合の認証結果はカード会社の判定次第となります。必ずエラーとなるとは限りません。なお、3D セキュア未対応のカードの確実な判別方法はありません。(ブランドキャッシュに存在しないカードは 3D セキュア未対応の可能性が高いです。)

第6章 導入・テストに関する補足

決済サーバーに接続し、テストを実施するための各種手続き・手順の詳細につきましては、『導入テストガイド』を参照してください。

本人認証サービスにおける 3D-Secure のテストは、発行カード会社対応状況、カード保有者パスワード登録状況、マーチャント設定(認証実行不可のカードの決済を許可する、しないなど)により複雑なパターンが存在します。それぞれのテストパターンについてテストカード番号を準備しております。カード番号により、本人認証成功、失敗、認証不可、異常終了等のシナリオテストが実施可能です。テストカード以外で取引を実施された場合、vResultCode は「NH02」となります。詳細は、別資料『本人認証サービス補足資料(3D セキュア 2.0 版)』をご参照ください。