

3G-Web 開発ガイド

Ver. 1.5.13（2026 年 10 月～）

Copyright © 2026 DG Financial Technology, Inc., a Digital Garage company. All rights reserved.

目次

第 1 章　サービス導入の前に 4
1-1 本ガイドの内容 4
1-2 対象者 4
1-3 制限事項 4
1-4 著作権、および問い合わせ先 5
1-5 改訂履歴 5

第 2 章　概要 10
2-1 利用できる決済サービス 10
2-2 サンプルプログラムについて 10
2-3 サンプルプログラム処理概要 11
2-4 各決済サービスの処理概要 13
2.4.1 クレジットカード決済 13
2.4.2 クレジットカード決済（本人認証有り） 14
2.4.3 クレジットカード決済（有効性確認機能） 15
2.4.4 コンビニ決済 15
2.4.5 電子マネー決済 16
2.4.6 銀行決済 19
2-5 URL リンク生成機能について 22

第 3 章　結果通知受信処理 23
3-1 結果通知受信処理の対象 23
3.1.1 Web リンクサーバーからの結果通知受信処理 23
3.1.2 決済サーバーからの結果通知受信処理 24

第 4 章　インターフェース詳細 25
4-1 アクセス URL 25
4-2 暗号鍵取得 26
4.2.1 要求電文 26
4.2.2 応答電文 34
4-3 Web リンクサーバー転送 34
4-4 消費者ブラウザからの結果連携 35
4-5 Web リンクサーバーからの結果通知電文 36
4.5.1 結果通知電文の概要 36
4.5.2 結果通知受信 36
4-6 決済サーバーからの結果通知電文 39
4-7 決済結果の改ざんチェック 40
4.7.1 Web リンクサーバーからの結果通知 40

4.7.2 決済サーバーからの入金通知 41
4-8 決済リンク無効化 42
4.8.1 要求電文 42
4.8.2 応答電文 42
4.8.3 処理結果の判定について 43

第 5 章　その他補足事項 44
5-1 決済結果の確認方法 44
5-2 テスト実施にあたっての注意事項 45
5-3 クレジットカード決済 仕向け先カード会社の一覧 46
5-4 他ソフトウェア等の影響 48

第1章 サービス導入の前に

1-1 本ガイドの内容

本ガイドは、店舗様の EC サイトより株式会社 DG フィナンシャルテクノロジー（以下、弊社）が提供する 3G-Web（以下、Web リンクサーバー）へ接続し、利用する際に参考となるサンプルプログラム、電文フォーマットなどについて記載しています。

1-2 対象者

本ガイドは、Web リンクサーバーへ接続し利用する店舗様 EC サイトの開発者を対象としております。

タイトル	概要	企画者	開発者	運用者
3G-Web 開発ガイド	店舗様の EC サイトより Web リンクサーバーへ接続し、利用する方法について記載されています。		◎	

表 1-2-1 ドキュメント一覧

1-3 制限事項

店舗様の EC サイトより Web リンクサーバーへ接続し、利用するにあたり、以下の制限があります。

【消費者様環境】

消費者様がご利用いただける環境（ブラウザ）は以下となります。

（ご利用の環境によっては、正常に動作しない場合があります。）

■ PC

- Microsoft Edge 最新安定版
- Google Chrome 最新安定版
- Mozilla Firefox 最新安定版
- Safari 最新安定版（MacOS のみ）

■ スマートフォン

- 標準ブラウザ
- docomo、au、SoftBank、Y!mobile のキャリア以外のスマートフォン端末ではスマートフォン対応画面が表示されない場合があります。

■ その他

・TLS1.2 以上の通信に未対応の端末ではご利用になれません。

【JavaScript】

JavaScript が利用できない環境ではご利用になれません。

1-4 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 © 2026 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

1-5 改訂履歴

2011/09 ：Ver1.0.0 リリース
2011/12 ：Ver1.1.0 リリース
文言追加・修正、レイアウト変更
2012/01 ：Ver.1.1.1 リリース
「1-3 制限事項」 説明文追加
「3-1 暗号鍵取得」 説明文追加
2012/04 ：Ver.1.1.2 リリース
戻るボタン実装、マルチランゲージ対応に伴い、「3-1 暗号鍵取得」の要求電文項目追加
2012/05 ：Ver.1.2.0 リリース
社名・ロゴ変更対応、「3-1 暗号鍵取得」の要求電文項目説明追加
2012/09 ：Ver.1.3.0 リリース
「3-1 暗号鍵取得」の要求電文項目追加
2013/03 ：Ver.1.3.1 リリース
「1-4 著作権、および問い合わせ先」の contact の記載を削除
ベリトランス株式会社 テクニカルサポートのメールアドレスを変更
2013/05 ：Ver.1.3.2 リリース
「3-1 暗号鍵取得」の「②要求電文 ： EC サイト → VTWeb」の「決済方法サブタイプ」を修正（ファミリーマートの econ 仕向け対応））
「3-1 暗号鍵取得」の「②要求電文 ： EC サイト → VTWeb」の「カナ１」、「カナ２」の説明欄を修正
「3-1 暗号鍵取得」の「②要求電文 ： EC サイト → VTWeb」の「カード所有者名」の書式・制限欄を修正
2013/08 ：Ver.1.4.0 リリース
「VTWeb 開発ガイド」リニューアル
2014/01 ：Ver.1.4.1 リリース
「第 4 章 インターフェース詳細」に文字コードに関する記載を追記
「4-1 暗号鍵取得」の「⑤要求電文 ： EC サイト → VTWeb」の「SETTLEMENT_SUB_TYPE」について、ミニストップを"204"（その他）から"205"（イーコン）へ変更
「4-1 暗号鍵取得」の「 ⑤要求電文 ： EC サイト → VTWeb」の「MERCHANTHASH」の説明を追記
2014/06 ：Ver.1.4.2 リリース
「2-1 VTWeb で利用できる決済サービス」のクレジットカード決済の注意事項として、店舗様の持つ 1 つのマーチャント ID に対して、クレジットカード会社が指定する加盟店番号は 1 つしか設定でない旨を追記
「表 2-4 1 VTWeb 導入時処理概要（クレジットカード決済）」、「表 2-4 3 VTWeb 導入時処理概要（コンビニ決済）」、「表 2-4 4 VTWeb 導入時処理概要（電子マネー決済（PC Edy／PC Suica／PC WAON））」、「表 2-4 5 VTWeb 導入時処理概要（電子マネー決済（モバイル Edy／モバイル Suica））」、「表 2-4 6 VTWeb 導入時処理概要（電子マネー決済（モバイル WAON））」、「表 2-4 7 VTWeb 導入時処理概要（銀行決済（ATM））」、「表 2-4 8 VTWeb 導入時処理概要（銀行決済（ネットバンク・PC））」、「表 2-4 9 VTWeb 導入時処理概要（銀行決済（ネットバンク・モバイル））」の「決済申込完了通知」の説明を修正
「3.1.1 VeriTrans3G からの結果通知受信処理」に結果通知電文の受信部分に関する記載を追記
「3.1.2 VTWeb からの結果通知受信処理」の説明を修正、また、決済結果通知受信部分に関する記載を追記
「4-1 暗号鍵取得」の「⑤要求電文 ： EC サイト → VTWeb」の表にて以下を追記
・URL を追記
・「FINISH_PAYMENT_ RETURN_URL」「UNFINISH_PAYMENT_RETURN_URL」
「ERROR_PAYMENT_RETURN_URL」の説明に URL パラメータ、およびアンカーの指定はできない旨を追記
・「FINISH_PAYMENT_ACCESS_URL」の説明に URL パラメータの指定はできない旨を追記
・「UNFINISH_PAYMENT_RETURN_URL」の説明を修正
「4-1 暗号鍵取得」の【要求電文設定項目一覧】の「TIMELIMIT_OF_PAYMENT」の「銀行」の欄を「□」から「◇」へ修正
「4-2 VTWeb 転送」の「⑨転送電文 ： EC サイト → 消費者ブラウザ」の表に URL を追記

「4-3 取引情報」の項目を削除、以下項番が繰り下がります。
「4-3 決済結果照合」に、戻り URL に関する記載を追記
「4-3 決済結果照合」の「⑭送信情報 : 消費者ブラウザ → EC サイト」の「mStatus」、「vResultCode」、「sessionId」について設定欄を修正、設定の条件を説明欄に追記
「4.5.1 結果通知電文の概要」の「結果通知受信処理結果について」の「決済報告リトライ回数上限」を「決済結果通知リトライ回数上限」に修正
「4.5.2 決済申込結果受信」に使用可能なフィールドに関する注意事項を追記
「4.5.2 決済結果通知受信」の「mErrMsg(エラーメッセージ)」の「説明」、「設定」欄を修正

2014/07 :Ver.1.4.3 リリース
「4-1 暗号鍵取得」の「⑤要求電文 : EC サイト → VTWeb 」の表から「郵便番号」「住所 1～3」「生年月日」「性別」を削除。また、【要求電文設定項目一覧】についても同項目を削除
「4.5.2 決済結果通知受信」の「⑪受信情報 : VTWeb → EC サイト」の表から「住所」「性別」「郵便番号」「誕生日」を削除

2014/09 :Ver.1.4.4 リリース
「2-1 VTWeb で利用できる決済サービス」にフィーチャー・フォンが本人認証に対応していないことを追記
「2.4.2 クレジットカード決済(本人認証有り) 」の表下にフィーチャー・フォンが本人認証に対応していないことを追記
「4-1 暗号鍵取得」の「⑥応答電文 VTWeb -> EC サイト」に注釈として「マーチャント暗号鍵」が決済処理で使用できないことを追記

2014/10 :Ver.1.4.5 リリース
サークル K サンクスの econ 仕向けに伴い、「4-1 暗号鍵取得」の「⑤要求電文 : EC サイト → VTWeb 」の「SETTLEMENT_SUB_TYPE」でコンビニ選択時の決済方法を修正
「4-1 暗号鍵取得」の「⑤要求電文 : EC サイト → VTWeb 」の「MERCHANT_ID」、「CARD_CAPTURE_FLAG」、「SHOP_NAME」、「SCREEN_TITLE」、「CONTENTS」、「CONTENTS_KANA」に説明を追加

2015/04 :Ver.1.4.6 リリース
サービス名称を VTWeb から 3G-Web へ変更
名称変更に伴い、各画像を差し替え
「2-3 サンプルプログラム処理概要」⑥内の「EC サイト用暗号鍵」に「(以下、マーチャント暗号鍵)」を追加
「4-1 暗号鍵取得」の「⑤要求電文 : EC サイト → 3G-Web 」の表を修正
「4-1 暗号鍵取得」の「購入金額」に決済金額の上限と下限の説明を追加
「4-1 暗号鍵取得」の「支払期限」と「支払取消期限」に説明を追加

2016/01 :Ver.1.4.7 リリース
「2.4.2 クレジットカード決済(本人認証有り)」の処理概要図を修正。また、処理概要に「決済申込完了通知」についてを追記
「2.4.4 電子マネー決済」の「図 2-4-4 3G-Web 利用時システム処理概要図(電子マネー決済(PC Edy／PC Suica／PC WAON))」を修正
「4-1 暗号鍵取得」の「⑤要求電文 : EC サイト → 3G-Web」の「CARD_NUMBER_OF_ INSTALLMENT(カード分割回数)」の説明を追記
「4-3 決済結果照合」の「⑭送信情報 : 消費者ブラウザ → EC サイト」の「mStatus」、「vResultCode」、について書式・制限欄の参照先を修正
「4-5 3G-Web からの結果通知電文」の 「⑪受信情報 : 3G-Web → EC サイト」の「mErrMsg」の項目名を「メッセージ」に修正、また、「漢字氏名」「カナ氏名」「メールアドレス」「電話番号」の説明欄を追記
「第 5 章 その他補足事項」を新設し、「5-1 テスト実施にあたっての注意事項」、「5-2 MAP を利用したテスト取引の結果確認」を追記

2016/04 :Ver.1.4.8 リリース
「1-3 制限事項」を修正
「4-1 アクセス URL」を追加し、SHA-2 証明書に対応した新環境の URL を記載
「3.1.1 3G-Web からの結果通知受信処理」と「3.1.2 VeriTrans3G からの結果通知受信処理」の記載順序を変更

2016/05 :Ver.1.4.9 リリース
「2.4.2 クレジットカード決済(本人認証有り)」の「表2-4 2 Simple Web 導入時処理概要(クレジットカード決済(本人認証有り))の「5 決済申込」の処理説明を修正(本人認証不可の場合は、エラー画面に遷移する旨を記載)
「2.4.4 電子マネー決済」の「図 2-4-4 3G-Web 利用時システム処理概要図(電子マネー決済(PC Edy／PC Suica／PC WAON))」を修正
「2.4.4 電子マネー決済」のモバイル WAON の※1 の説明内容を修正
「結果通知」に関連する用語の統一
「VeriTrans3G 開発ガイド」の参照する章が誤っていたため修正(章番号を削除)
「第 3 章 結果通知受信処理」の説明の分かりにくい点を補足・修正
「4-4 決済結果照合」の説明を補足・修正

2016/06 :Ver.1.4.10 リリース
「4-2 暗号鍵取得」の JPO に関するパラメータの追加・修正。

2017/06 :Ver.1.5.0 リリース

「2-3 サンプルプログラム処理概要」の説明を修正
「2-5 URL リンク生成機能について」を追加
「4.2.1 要求電文」の見出しを追加し以下パラメータを追加。それに伴う注意書き等の修正。
- RESPONSE_TYPE
- AUTO_RETURN_FLAG
- AUTO_RETURN_WAITING_TIME
- LINK_PAYMENT_FLAG
- LINK_EXP_DATETIME

「4.2.2 応答電文」の見出しを追加しリンク決済利用可否による電文仕様を記載
「4.5.2 結果通知受信」で通知メッセージタイプ別の通知仕様を記載
「5-3 クレジットカード決済仕向け先カード会社の一覧」を追加

2017/06 :Ver.1.5.1 リリース
2 章以降の用語の表記を次のように変更し、関連する表記を含む章タイトルを修正。
「3G-Web」 ⇒ 「Web リンクサーバー」
「VeriTrans3G」 ⇒ 「決済サーバー」
「1-3 制限事項」に、以下の説明を追加
「docomo、au、SoftBank、Y!mobile のキャリア以外のスマートフォン端末ではスマートフォン対応画面が表示されない場合があります。」
「2.4.4 電子マネー決済」の PC Suica の処理概要図表を修正。
「4.2.1 要求電文」に、銀行決済の項目に使用できない文字の説明を補足

2017/09 :Ver.1.5.2 リリース
「4.2.1 要求電文」の「請求内容」の注記(※3)を追加し、※3～※5 の記載順序を調整。
「4.2.2 応答電文」の「※1:【結果コード一覧】をご参照ください。」の記載を「※1 : 『3G-Web 結果コード一覧』をご参照ください。」へ修正。
「4.5.2 結果通知受信」の「別紙 【MDK 結果コード一覧】をご参照ください。」の記載を
「別紙『決済結果コード一覧』をご参照ください。」へ修正。

2017/12 :Ver.1.5.3 リリース
「2-1 利用できる決済サービス」にクレジットカード決済(2 円与信機能)を追加。その他サービスの説明を修正。
「2-3 サンプルプログラム処理概要」に Web リンクサーバーの決済完了画面、結果通知に関する注意書きを追加。
「2.4.3 クレジットカード決済(2 円与信機能)」を追加。
「2-5 URL リンク生成機能について」
・他章に記載の内容を一部削除。
・URL リンクをメール送信する場合の処理概要の表を追加。
「4.2.1 要求電文」
・MERCHANTHASH の書式・制限の説明を追加。
・SessionID の説明を修正。
・決済完了後戻り URL、未決済時戻り URL、決済エラー時戻り URL の説明を修正。
・自動遷移フラグの注記(※2)について修正し、
完了画面自動遷移機能の利用条件から、trAd(広告表示プログラム)未使用であることを削除。
・購入金額の説明および※1 にクレジットカード決済(2 円与信機能)を利用する場合の説明を追加。
・※3 として言語選択可否フラグと使用言語の設定による Web リンクサーバーの画面表示仕様を追加。
それに伴い既存の注意書き項番を修正。
・TIMELIMIT_OF_PAYMEN の注記(※5)について追記
「4-4 決済結果照合」
説明の内容を修正。
「4.5.2 決済結果通知受信」
デフォルト、拡張、縮小で別立てにしていた受信情報の説明と表を統合。
※2 を表形式に変更。
「5-1 決済結果の確認方法」を追加し、既存の「MAP を利用したテスト取引の結果確認」を削除。
その他文言等の微調整

2018/06 :Ver.1.5.4 リリース
「1-3 制限事項」を最新の情報に更新（SSL3.0/TLS1.0 の廃止に伴う更新）。
「4-1 アクセス URL」から暫定環境（SSL3.0/TLS1.0 有効環境）の記載を削除。
「2-1 利用できる決済サービス」から電子マネー決済（WAON）の記述を削除。
「2.4.5 電子マネー決済」から PC WAON、モバイル WAON の記述を削除。
「4.2.1 要求電文」
・SETTLEMENT_SUB_TYPE から"331":PC WAON、"332":モバイル WAON を削除。
・TIMELIMIT_OF_CANCEL を削除。
・注釈から WAON の記述を削除。
・【要求電文設定項目一覧】の表と注釈から TIMELIMIT_OF_CANCEL と WAON の記述を削除。
「4-4 決済結果照合」で文言の微調整。
「4.5.2 結果通知受信」
・settlementSubType から"331":PC WAON、"332":モバイル WAON を削除。

2020/07 :Ver.1.5.5 リリース
「1-3 制限事項」を最新の情報に更新（TLS1.1 の廃止に伴う更新）。
「4-1 アクセス URL」から暫定環境（TLS1.1 有効環境）の記載を削除。
「4.2.1 要求電文」の※3 の誤植を修正
誤: 言語選択可否フラグが"1":選択不可
正: 言語選択可否フラグが"1":選択可
第 4 章の要求電文の表に、HTTP のメソッド（POST または GET）を明示

2021/09 :Ver.1.5.6 リリース
「4.2.1 要求電文」
DDD_VERSION を追加。
※3D セキュア 2.0 を有効にするために必要。

2023/06 :Ver.1.5.7 リリース
サークル K サンクスを削除
「4.2.1 要求電文」
・MERCHANTHASH の説明欄の"決済タイプ"を"決済方法"へ変更。
・COMMODITY_ID・JAN_CODE を削除。
・SETTLEMENT_TYPE の説明欄に補足を追加。
・SETTLEMENT_SUB_T YPE の説明欄に補足を追加。
「5-3 クレジットカード決済 仕向け先カード会社の一覧」 表を更新

2024/01 :Ver.1.5.8 リリース
「3.1.1 Web リンクサーバーからの結果通知受信処理」に SNI 非対応の旨を追記

2024/03 :Ver.1.5.9 リリース
「第 4 章 インターフェース詳細」 アクセス URL のドメインを「pay.veritrans.co.jp」から「pay3.veritrans.co.jp」に変更

2024/05 :Ver.1.5.10 リリース
「4.2.1 要求電文」に以下のパラメータを追加
CARDHOLDER_EMAIL、
CARDHOLDER_HOME_PHONE_NUMBER、CARDHOLDER_HOME_PHONE_COUNTRY、
CARDHOLDER_MOBILE_PHONE_NUMBER、CARDHOLDER_MOBILE_PHONE_COUNTRY、
CARDHOLDER_WORK_PHONE_NUMBER、CARDHOLDER_WORK_PHONE_COUNTRY

2024/07 :Ver.1.5.11 リリース
「5-3 クレジットカード決済 仕向け先カード会社の一覧」
「ご利用のカード会社」を「ご契約されているカード会社（アクワイアラ）」に修正
「5-4 他ソフトウェア等の影響」を追加

3G-Web 開発ガイド

2026/05 :Ver1.5.12 リリース

フィーチャー・フォンの記載を削除

「1-3 制限事項」

Internet Explorer の記載を削除

「2-1 利用できる決済サービス」

「クレジットカード決済（2 円与信機能）」を「クレジットカード決済（有効性確認機能）」に変更し、説明を修正

「2.4.3 クレジットカード決済（有効性確認機能）」

「クレジットカード決済（2 円与信機能）」を「クレジットカード決済（有効性確認機能）」に変更し、説明を修正

「2.4.4 コンビニ決済」「2.4.5 電子マネー決済」「2.4.6 銀行決済」

「基本機能」について、「決済完了」から「決済申込完了」へ表記を修正

「3.1.1 Web リンクサーバーからの結果通知受信処理」

改ざんチェックについての注意書きを追加

SNI に対応したため、SNI 非対応の記載を削除

「3.1.2 決済サーバーからの結果通知受信処理」

入金通知先の設定方法を追記

「4.2.1 要求電文」

FINISH_PAYMENT_ACCESS_URL の説明に未設定時に設定される URL を追記

FINISH_PAYMENT_RETURN_URL の説明に未設定時に設定される URL を追記

※1 の「クレジットカード決済（2 円与信機能）」を「クレジットカード決済（有効性確認機能）」に変更

※5 に支払期限の計算例を追記

「4-4 消費者ブラウザからの結果通知」、「4-5 Web リンクサーバーからの結果通知電文」

改ざんチェックの説明と関連する以下のパラメータを追加

- resultHash
- sessionId

「4-7 決済結果の改ざんチェック」を追加

「5-1 その他補足事項」

注意点から、「本人認証可否確認」エラー時の通知についての記載を削除

2026/10 :Ver1.5.13 リリース

「4.7.2 決済サーバーからの入金通知」 ソースコードが【開発ガイド本体】にも記載されている旨を追記

「4-8 決済リンク無効化」を追加

「5-3 クレジットカード決済 仕向け先カード会社の一覧」を更新

第2章 概要

2-1 利用できる決済サービス

店舗様は、弊社の提供するサンプルプログラムをカスタマイズして EC サイトへ導入する事により、弊社 Web リンクサーバーへ接続し、下記の各種オンライン決済サービスを利用することができます。

決済サービス名	説明
クレジットカード決済	VISA、MasterCard、JCB 等、各種ブランドのクレジットカードに対応しています。
クレジットカード決済 （本人認証有り）	本人認証（3-D Secure）機能付きのクレジットカード決済が利用できます。 VISA、MasterCard、JCB 等、各種ブランドの本人認証（3-D Secure）に対応しています。
クレジットカード決済 （有効性確認機能）	クレジットカードの有効性を確認するために 0 円与信を実行し、クレジットカード情報を弊社システムに登録します。 クレジットカード情報は、本機能の実行時に利用した「取引 ID」に関連付けられますので、この取引 ID を使って後から再取引（再与信）を実行することができます。 ※再取引のための決済画面は提供しておりません。再取引の実行には、MDK や MAP をご利用いただく必要があります。 ※ 本機能のご利用には、別途お申込みが必要です。
コンビニ決済	セブンーイレブン、ローソン、ファミリーマート等のコンビニエンスストア店舗でのお支払いを選択可能です。
電子マネー決済	電子マネー（楽天 Edy、Suica）でのお支払いを選択可能です。
銀行決済	ご利用の金融機関（銀行、信用金庫等）の ATM やインターネットバンキング、Pay-easy（ペイジー）でのお支払いが可能です。

表 2-1-1 決済サービス一覧

2-2 サンプルプログラムについて

店舗様システムから Web リンクサーバーへ接続し、利用する EC サイトの機能一式をサンプルプログラムとして提供しています。

サンプルプログラムは、画面などを店舗様の EC サイトにあわせてカスタマイズいただき、ご利用いただくことが可能です。（カスタマイズは店舗様にて実施していただきます）

サンプルプログラムは Java、PHP 等複数言語別にご用意しています。

サンプルプログラムのインストールについては各言語別のインストールガイドをご参照ください。

2-3 サンプルプログラム処理概要

以下にサンプルプログラムの動作を図示します。

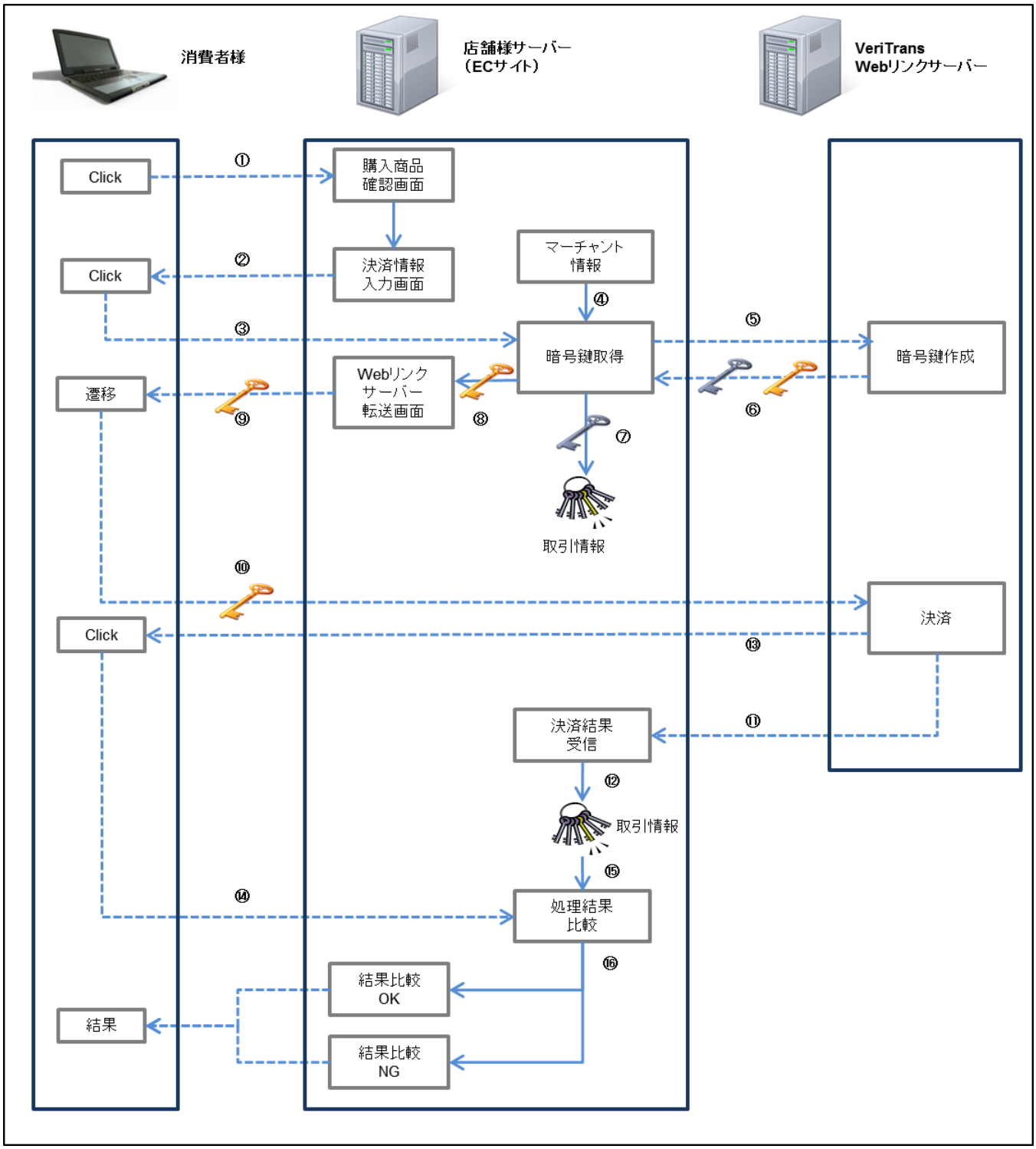


図 2-3-1 サンプルプログラム動作全体図

以下に「図 2-3-1 サンプルプログラム動作全体図」の説明を記載します。図中の番号と照らし合わせてご確認ください。

① 本画面（購入商品確認画面）は消費者様が購入する商品の選択を終了し、決済前の最終確認を行う画面を想定しています。

② 手順①の画面で決済方法を選択すると決済情報入力画面に遷移します。

③ 決済情報入力画面で必要な情報を入力し「購入」ボタンを押下すると「暗号鍵取得」の処理に移ります。

④ マーチャント ID、決済後 EC サイトに戻る際の URL などのマーチャント情報を取得し暗号鍵取得時のパラメータに設定します。
サンプルプログラムではこれらのマーチャント情報は設定ファイルに記載されています。
※設定ファイルにて定義する項目につきましてはサンプルプログラムのインストールガイドをご参照ください。

⑤ ②、③の入力情報および④の設定情報で EC サイトから Web リンクサーバーに暗号鍵取得を要求します。
送信パラメータにつきましては「4.2.1 要求電文」をご参照ください。

⑥ EC サイトは Web リンクサーバーからの返戻として、消費者様用の暗号鍵（以下、ブラウザ暗号鍵）と EC サイト用暗号鍵(以下、マーチャント暗号鍵)を受信します。
受信パラメータにつきましては「4.2.2 応答電文」をご参照ください。

⑦ EC サイトは⑤の暗号鍵取得で送信した取引 ID を取得キーとして取引情報を保存します。
※サンプルプログラムでは簡易性を重視して HashMap(Java)やテキストファイル(PHP)として保存していますが、実際の運用では Database 等に保存される事を推奨します。

⑧ Web リンクサーバーに連携する暗号鍵等の情報を、転送画面に設定します。

⑨ 消費者ブラウザに、Web リンクサーバーへの転送画面を表示します。

⑩ 「入力画面へ」ボタンを押下すると消費者ブラウザは転送画面から Web リンクサーバーの提供する決済画面に遷移します。
遷移後、消費者様は決済画面にて必要な情報を入力し決済を行います。
転送パラメータにつきましては「4-3Web リンクサーバー転送」をご参照ください。

⑪ Web リンクサーバーは決済終了後、EC サイトへ決済結果を通知します。
通知パラメータにつきましては「4-5Web リンクサーバーからの結果通知電文」をご参照ください。

⑫ EC サイトは受信した決済結果の取引 ID を取得キーとして該当の取引情報を取得し、受信した決済結果情報を保存します。

⑬ Web リンクサーバーは消費者ブラウザへ決済結果を返戻します。

⑭ 「注文サイトへ戻る」ボタンを押下すると、消費者ブラウザは EC サイトの決済完了後戻り URL へ遷移します。
消費者ブラウザから EC サイトへの送信パラメータにつきましては「4-4 消費者ブラウザからの結果連携」をご参照ください。 **※1**

⑮ EC サイトは処理結果比較を行います。処理結果比較では取引 ID を取得キーとして該当の取引情報を取得し、渡されたパラメータの照合を行います。

⑯ 処理結果比較を行い「決済処理成功」「決済処理エラー」を消費者ブラウザへ返戻します。
※処理結果比較の成功・失敗は決済の成功・失敗ではありません。
※サンプルプログラムでは処理結果の比較のみを行っています。実際の運用では、必要に応じて処理結果やエラーコードの値に拠る分岐を発生させる等の処理を店舗様に実装していただくことが可能です。

※1 ： ⑤の暗号鍵取得時に決済完了後戻り URL を設定しなかった場合やリンク生成型決済の場合には「注文サイトへ戻る」ボタンは表示されません。また消費者様がボタンを押下しなかった場合等、消費者ブラウザが EC サイトに遷移せず⑮以降の処理が行えない場合を考慮し、その場合にも決済ステータスを取りこぼさないように⑪の Web リンクサーバーから EC サイトへの結果通知の受信を実装いただくことを推奨いたします。⑪の結果通知送信処理につきましては「4-5 Web リンクサーバーからの結果通知電文」をご参照ください。

2-4 各決済サービスの処理概要

ここでは、各決済サービスの処理概要（処理フロー）を説明します。

図中の水色の枠は、弊社のサーバーを示しています。

- ✧ Web（Web リンクサーバー）
- ✧ 決済サーバー

2.4.1 クレジットカード決済

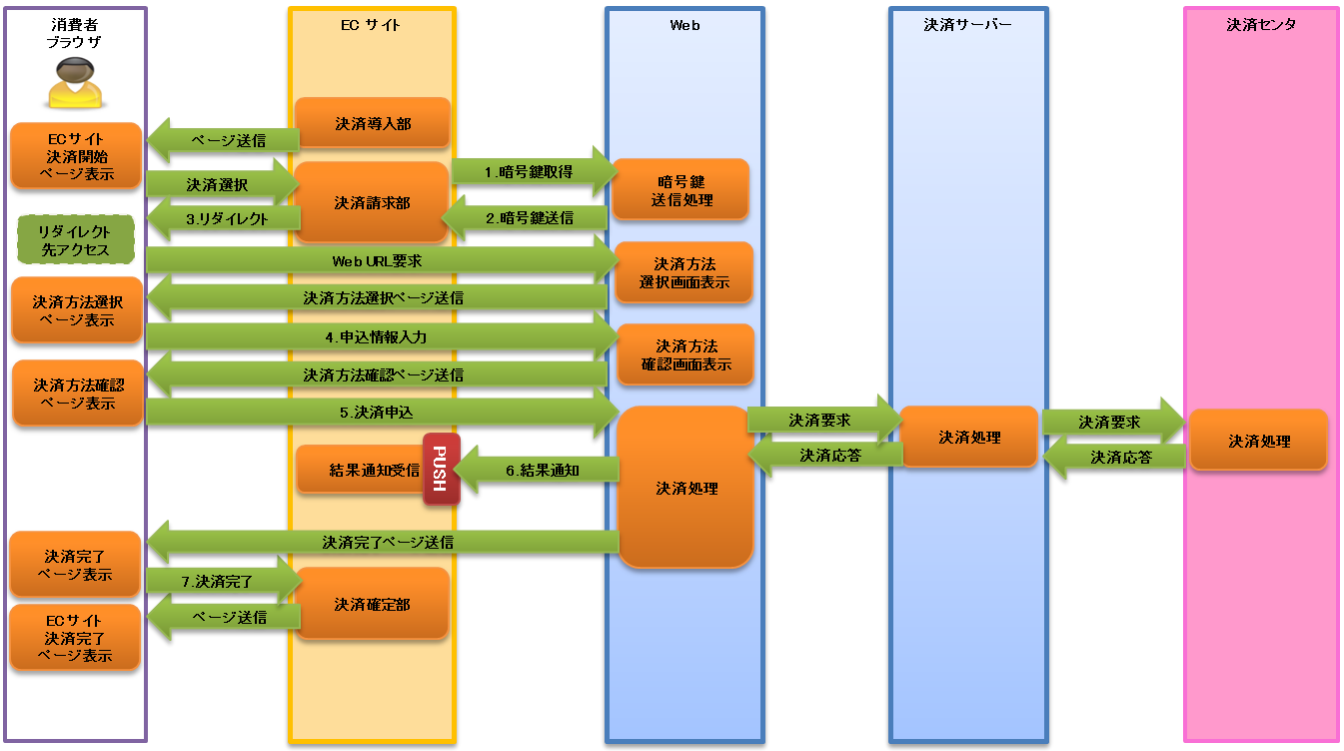


図 2-4-1 Web リンクサーバー利用時システム処理概要図（クレジットカード決済）

No.	基本機能	処理説明
1	暗号鍵取得	EC サイト上の決済申込部に渡された決済申込情報を電文化し、Web リンクサーバーに送信します。
2	暗号鍵送信	Web リンクサーバーは EC サイトからのリクエストを受け、消費者様の暗号鍵(以下ブラウザ暗号鍵)と EC サイト用の暗号鍵をそれぞれ作成し、EC サイトに返却します。
3	リダイレクト	EC サイトは取引 ID、ブラウザ暗号鍵及びマーチャント ID をパラメータに設定した Web リンクサーバーの決済画面の URL を消費者様に送信し、決済画面に遷移するように促します。 ※決済画面を表示させる際は、ポップアップなど別画面上で表示させるのではなく、同一画面上に表示させるようにしてください。
4	申込情報入力	消費者様は決済方法を選択し、申込情報を入力します。 決済方法の選択を行うと、消費者ブラウザは決済方法確認画面に遷移します。
5	決済申込	消費者様は決済申込を実行します。
6	結果通知	Web リンクサーバーは EC サイトへ結果通知を POST 形式で送信します。
7	決済完了	消費者様が「注文サイトへ戻る」ボタンを押下すると、Web リンクサーバーの決済画面は EC サイトが用意する完了画面へ遷移します。

表 2-4-1 Web リンクサーバー利用時システム処理概要（クレジットカード決済）

2.4.2 クレジットカード決済（本人認証有り）

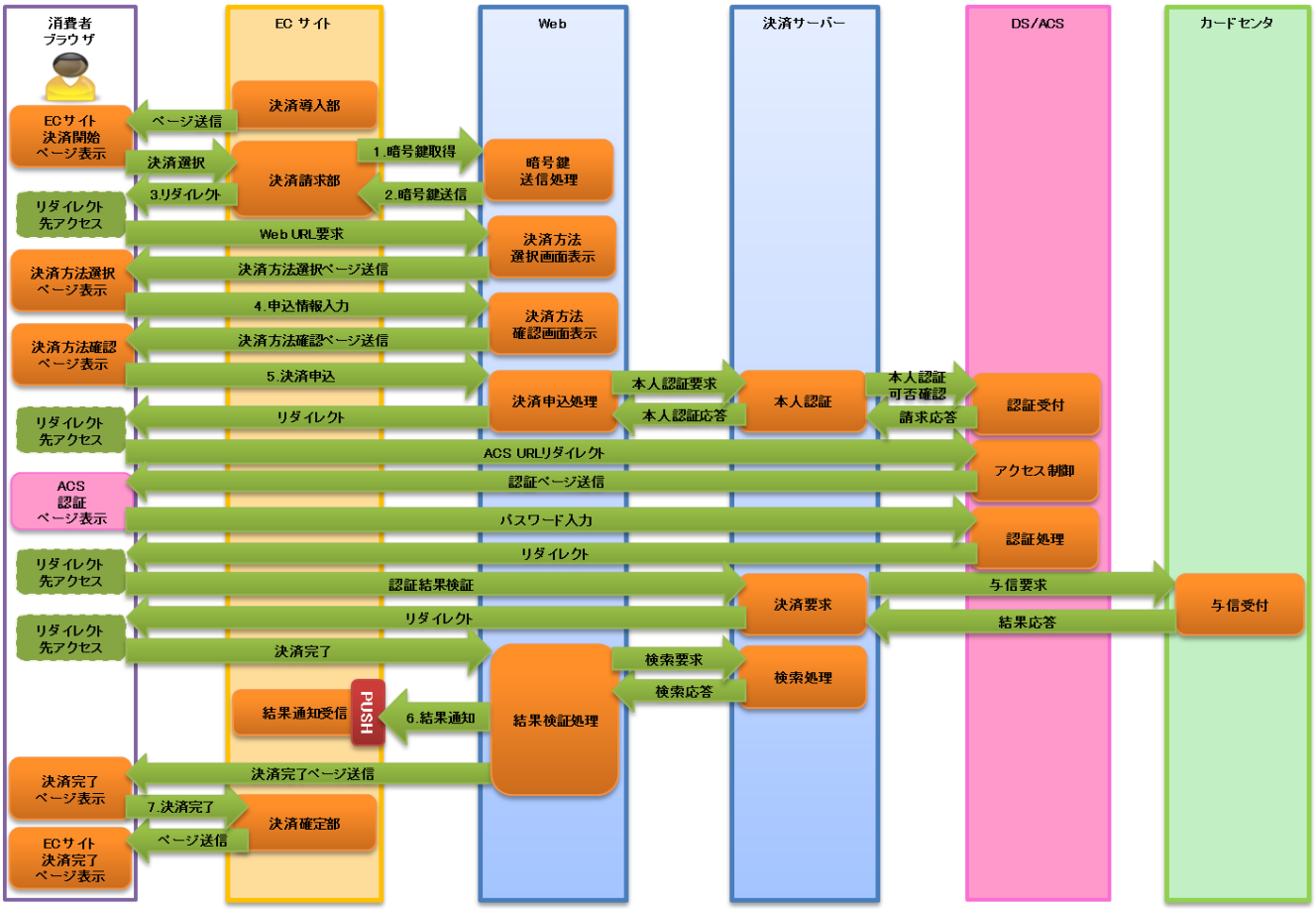


図 2-4-2 Web リンクサーバー利用時システム処理概要図（クレジットカード決済（本人認証有り））

No.	基本機能	処理説明
1	暗号鍵取得	EC サイト上の決済申込部に渡された決済申込情報を電文化し、Web リンクサーバーに送信します。
2	暗号鍵送信	Web リンクサーバーは EC サイトからのリクエストを受け、消費者様の暗号鍵(以下ブラウザ暗号鍵)と EC サイト用の暗号鍵をそれぞれ作成し、EC サイトに返却します。
3	リダイレクト	EC サイトは取引 ID、ブラウザ暗号鍵及びマーチャント ID をパラメータに設定した Web リンクサーバーの決済画面の URL を消費者様に送信し、決済画面に遷移するように促します。 ※決済画面を表示させる際は、ポップアップなど別画面上で表示させるのではなく、同一画面上に表示させるようにしてください。
4	申込情報入力	消費者様は決済方法を選択し、申込情報を入力します。 決済方法の選択を行うと、消費者ブラウザは決済方法確認画面に遷移します。
5	決済申込	消費者様は決済申込を実行します。 本人認証可能の場合、消費者ブラウザは ACS 認証画面に遷移(リダイレクト)します。 本人認証不可の場合は、エラー画面に遷移します。
6	結果通知	Web リンクサーバーは EC サイトへ結果通知を POST 形式で送信します。
7	決済完了	消費者様が「注文サイトへ戻る」ボタンを押下すると、Web リンクサーバーの決済画面は EC サイトが用意する完了画面へ遷移します。

表 2-4-2 Web リンクサーバー利用時システム処理概要（クレジットカード決済（本人認証有り））

2.4.3 クレジットカード決済（有効性確認機能）

Web リンクサーバーへのリクエスト時、購入金額に 0 円を指定すると、クレジットカード登録画面となります。

（この機能を利用する場合は、他の決済手段は選択できません。）

画面遷移は通常のクレジットカード決済と同様ですが、文言や表示項目はクレジットカード登録専用の表示となります。

✧　この機能を利用する場合は、暗号鍵取得の「4.2.1 要求電文」で「AMOUNT（購入金額）」に 0 円を指定してください。

2.4.4 コンビニ決済

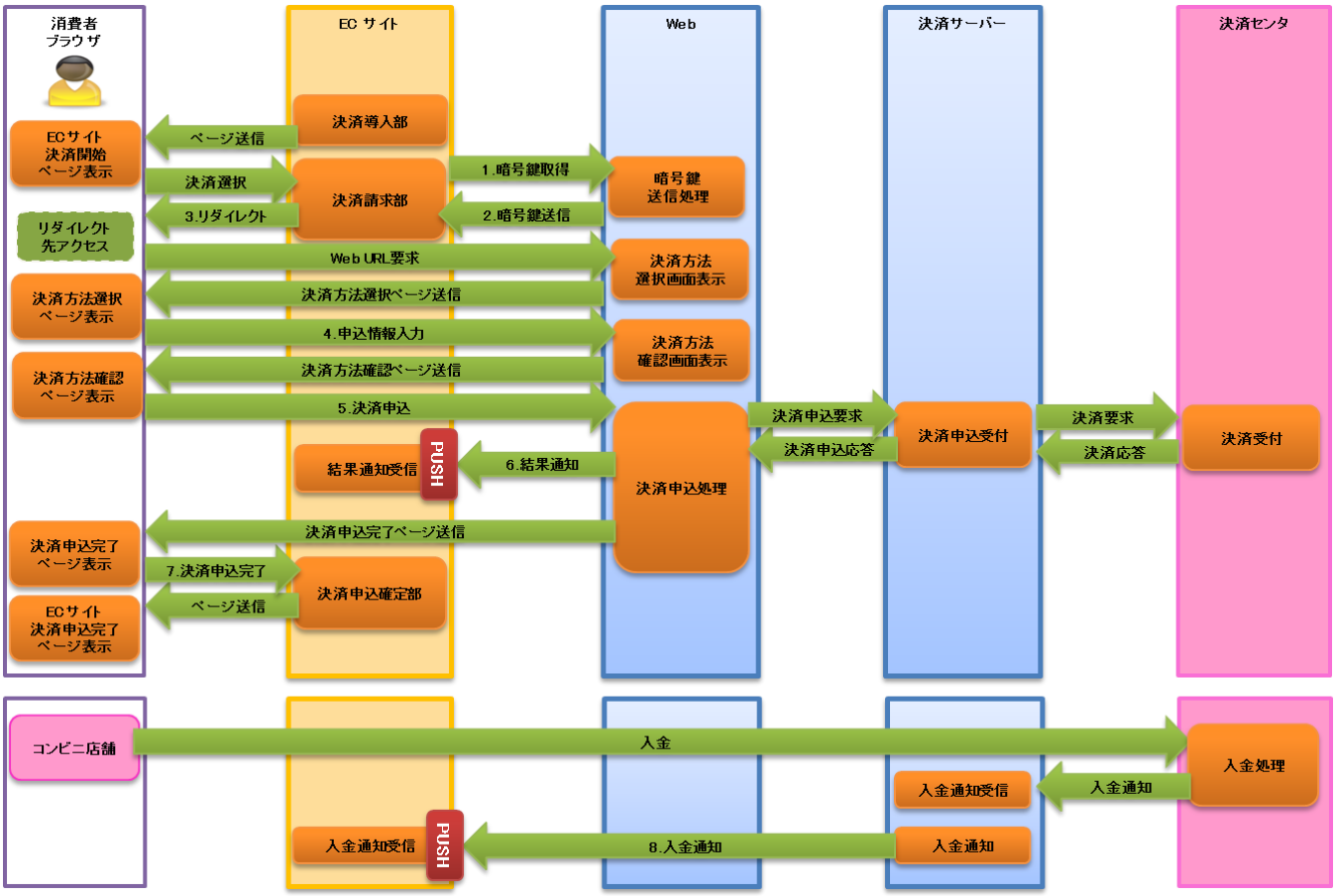


図 2-4-3 Web リンクサーバー利用時システム処理概要図（コンビニ決済）

No.	基本機能	処理説明
1	暗号鍵取得	EC サイト上の決済申込部に渡された決済申込情報を電文化し、Web リンクサーバーに送信します。
2	暗号鍵送信	Web リンクサーバーは EC サイトからのリクエストを受け、消費者様の暗号鍵(以下ブラウザ暗号鍵)と EC サイト用の暗号鍵をそれぞれ作成し、EC サイトに返却します。
3	リダイレクト	EC サイトは取引 ID、ブラウザ暗号鍵及びマーチャント ID をパラメータに設定した Web リンクサーバーの決済画面の URL を消費者様に送信し、決済画面に遷移するように促します。 ※決済画面を表示させる際は、ポップアップなど別画面上で表示させるのではなく、同一画面上に表示させるようにしてください。
4	申込情報入力	消費者様は決済方法を選択し、申込情報を入力します。 決済方法の選択を行うと、消費者ブラウザは決済方法確認画面に遷移します。
5	決済申込	消費者様は決済申込を実行します。
6	結果通知	Web リンクサーバーは EC サイトへ結果通知を POST 形式で送信します。

7	決済申込完了	消費者様が「注文サイトへ戻る」ボタンを押下すると、Web リンクサーバーの決済画面は EC サイトが用意する完了画面へ遷移します。
8	入金通知	決済サーバーにて消費者様による入金が完了したと確認された取引については、EC サイトへ入金通知を POST 形式で送信します。

表 2-4-3 Web リンクサーバー利用時システム処理概要(コンビニ決済)

2.4.5 電子マネー決済

【電子マネー決済(PC Edy)】

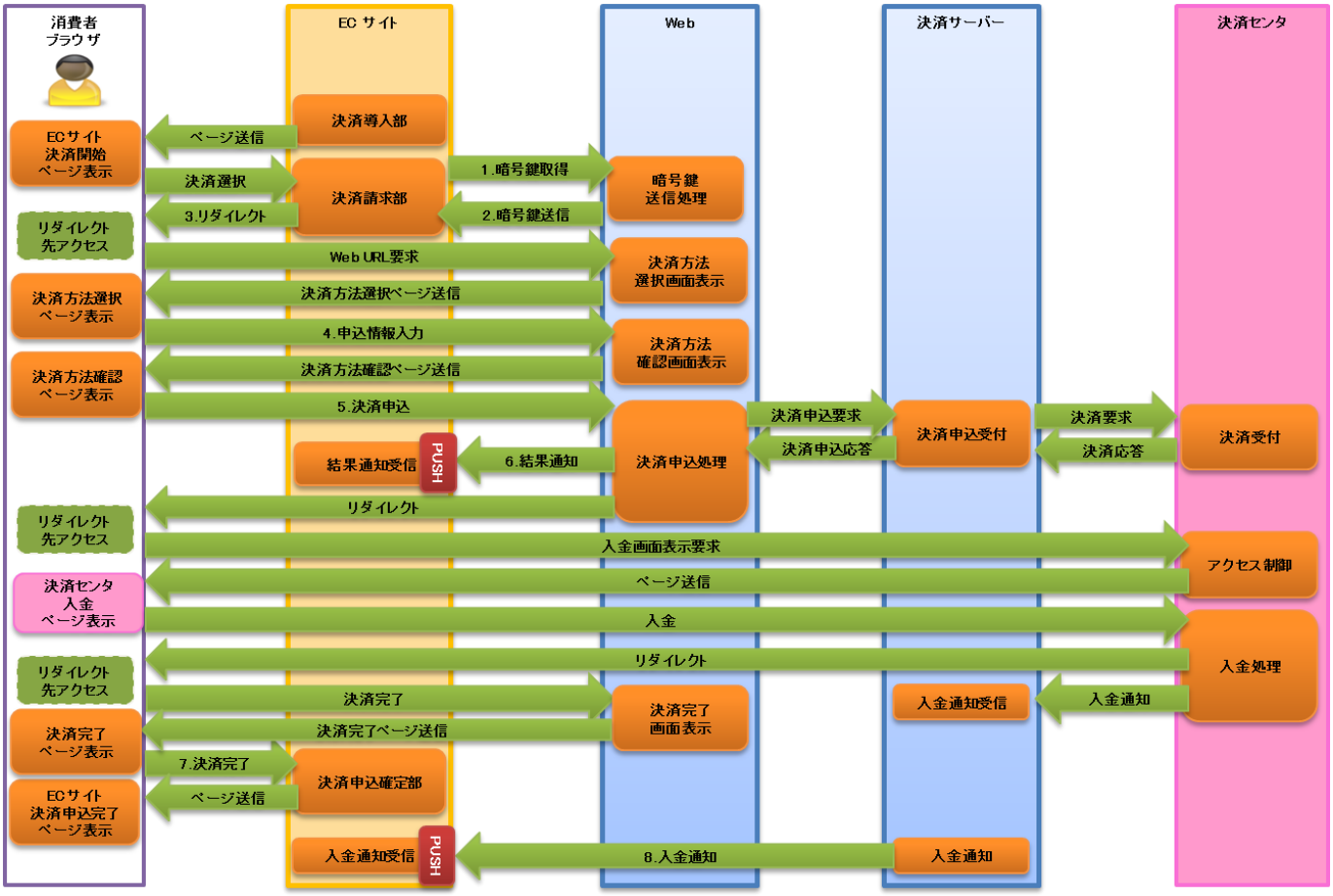


図 2-4-4 Web リンクサーバー利用時システム処理概要図(電子マネー決済(PC Edy))

No.	基本機能	処理説明
1	暗号鍵取得	EC サイト上の決済申込部に渡された決済申込情報を電文化し、Web リンクサーバーに送信します。
2	暗号鍵送信	Web リンクサーバーは EC サイトからのリクエストを受け、消費者様の暗号鍵(以下ブラウザ暗号鍵)と EC サイト用の暗号鍵をそれぞれ作成し、EC サイトに返却します。
3	リダイレクト	EC サイトは取引 ID、ブラウザ暗号鍵及びマーチャント ID をパラメータに設定した Web リンクサーバーの決済画面の URL を消費者様に送信し、決済画面に遷移するように促します。 ※決済画面を表示させる際は、ポップアップなど別画面上で表示させるのではなく、同一画面上に表示させるようにしてください。
4	申込情報入力	消費者様は決済方法を選択し、申込情報を入力します。 決済方法の選択を行うと、消費者ブラウザは決済方法確認画面に遷移します。
5	決済申込	消費者様は決済申込を実行します。 決済申込の実行を行うと、消費者ブラウザは決済センタの入金画面に遷移(リダイレクト)します。
6	結果通知	Web リンクサーバーは EC サイトへ結果通知を POST 形式で送信します。

7	決済完了	消費者様が「注文サイトへ戻る」ボタンを押下すると、Web リンクサーバーの決済画面は EC サイトが用意する完了画面へ遷移します。
8	入金通知	決済サーバーにて消費者様による入金が完了したと確認された取引については、EC サイトへ入金通知を POST 形式で送信します。

表 2-4-4 Web リンクサーバー利用時システム処理概要(電子マネー決済(PC Edy))

【電子マネー決済(PC Suica)】

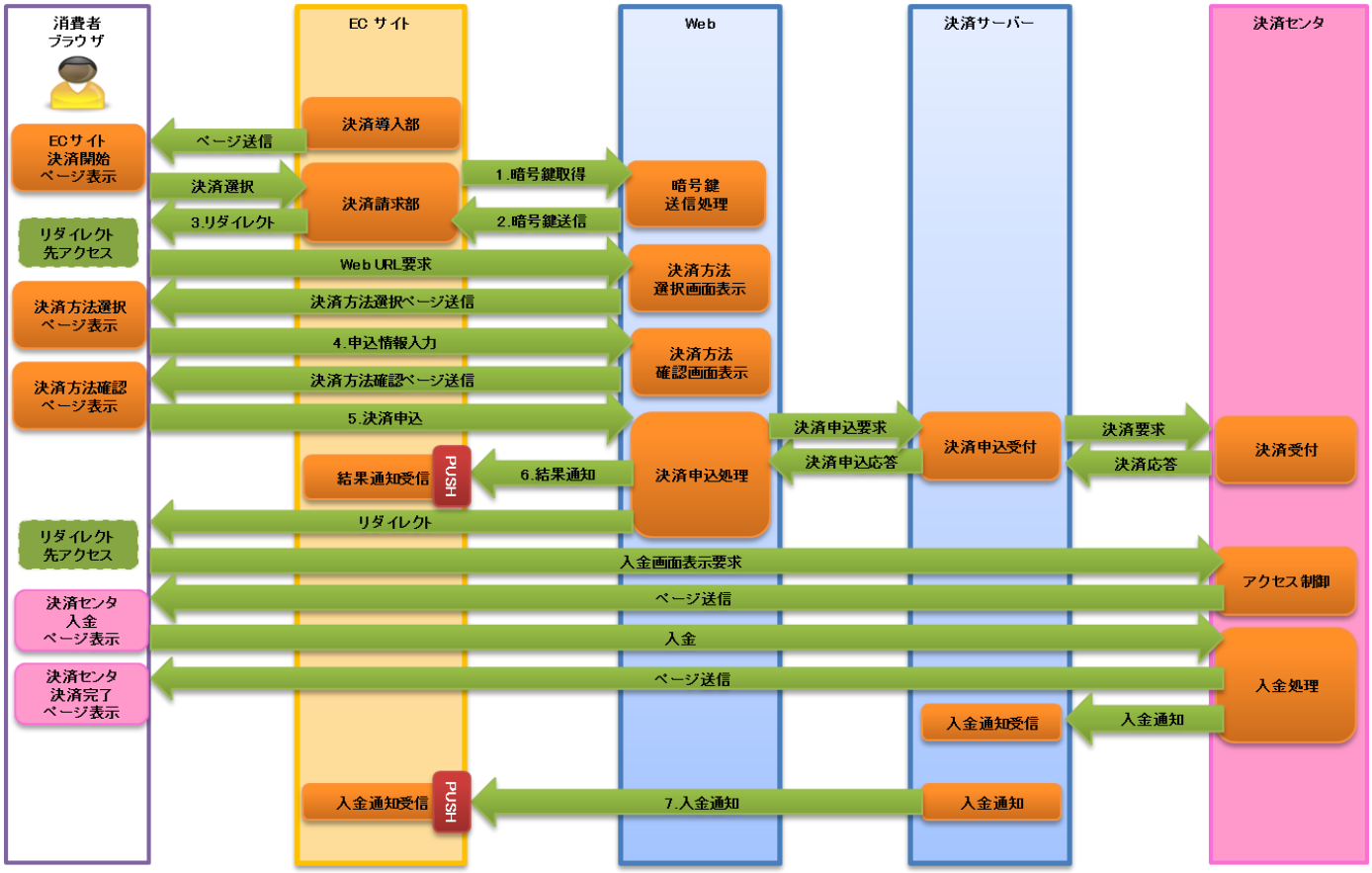


図 2-4-5 Web リンクサーバー利用時システム処理概要図(電子マネー決済(PC Suica))

No.	基本機能	処理説明
1	暗号鍵取得	EC サイト上の決済申込部に渡された決済申込情報を電文化し、Web リンクサーバーに送信します。
2	暗号鍵送信	Web リンクサーバーは EC サイトからのリクエストを受け、消費者様の暗号鍵(以下ブラウザ暗号鍵)と EC サイト用の暗号鍵をそれぞれ作成し、EC サイトに返却します。
3	リダイレクト	EC サイトは取引 ID、ブラウザ暗号鍵及びマーチャント ID をパラメータに設定した Web リンクサーバーの決済画面の URL を消費者様に送信し、決済画面に遷移するように促します。 ※決済画面を表示させる際は、ポップアップなど別画面上で表示させるのではなく、同一画面上に表示させるようにしてください。
4	申込情報入力	消費者様は決済方法を選択し、申込情報を入力します。 決済方法の選択を行うと、消費者ブラウザは決済方法確認画面に遷移します。
5	決済申込	消費者様は決済申込を実行します。 決済申込の実行を行うと、消費者ブラウザは決済センタの入金画面に遷移(リダイレクト)します。
6	結果通知	Web リンクサーバーは EC サイトへ結果通知を POST 形式で送信します。
7	入金通知	決済サーバーにて消費者様による入金が完了したと確認された取引については、EC サイトへ入金通知を POST 形式で送信します。

表 2-4-5 Web リンクサーバー利用時システム処理概要(電子マネー決済(PC Suica))

【電子マネー決済(モバイル Edy／モバイル Suica)】

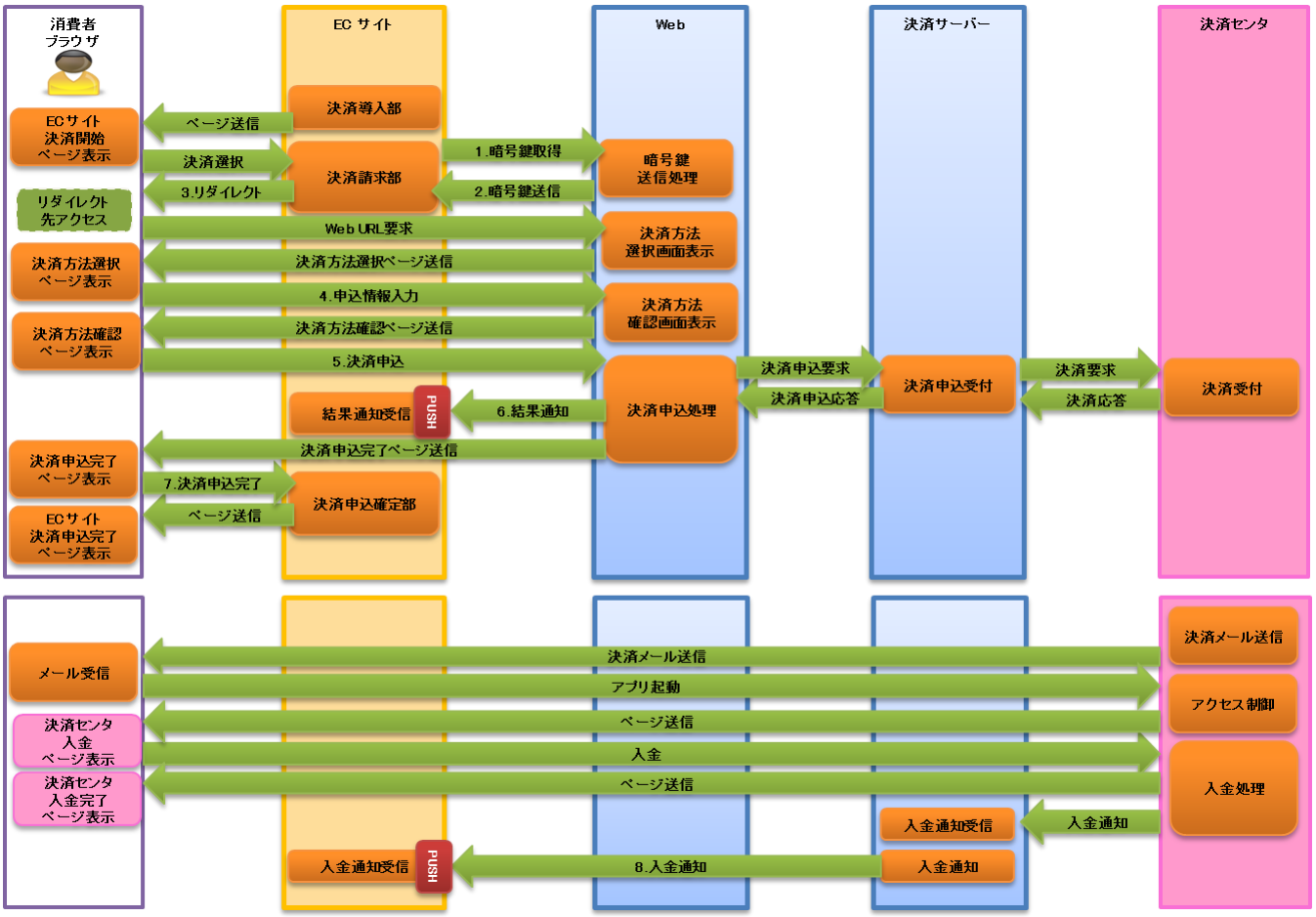


図 2-4-6 Web リンクサーバー利用時システム処理概要図(電子マネー決済(モバイル Edy／モバイル Suica))

No.	基本機能	処理説明
1	暗号鍵取得	EC サイト上の決済申込部に渡された決済申込情報を電文化し、Web リンクサーバーに送信します。
2	暗号鍵送信	Web リンクサーバーは EC サイトからのリクエストを受け、消費者様の暗号鍵(以下ブラウザ暗号鍵)と EC サイト用の暗号鍵をそれぞれ作成し、EC サイトに返却します。
3	リダイレクト	EC サイトは取引 ID、ブラウザ暗号鍵及びマーチャント ID をパラメータに設定した Web リンクサーバーの決済画面の URL を消費者様に送信し、決済画面に遷移するように促します。 ※決済画面を表示させる際は、ポップアップなど別画面上で表示させるのではなく、同一画面上に表示させるようにしてください。
4	申込情報入力	消費者様は決済方法を選択し、申込情報を入力します。 決済方法の選択を行うと、消費者ブラウザは決済方法確認画面に遷移します。
5	決済申込	消費者様は決済申込を実行します。
6	結果通知	Web リンクサーバーは EC サイトへ結果通知を POST 形式で送信します。
7	決済申込完了	消費者様が「注文サイトへ戻る」ボタンを押下すると、Web リンクサーバーの決済画面は EC サイトが用意する完了画面へ遷移します。
8	入金通知	決済サーバーにて消費者様による入金が完了したと確認された取引については、EC サイトへ入金通知を POST 形式で送信します。

表 2-4-6 Web リンクサーバー利用時システム処理概要(電子マネー決済(モバイル Edy／モバイル Suica))

2.4.6 銀行決済

【銀行決済(ATM)】

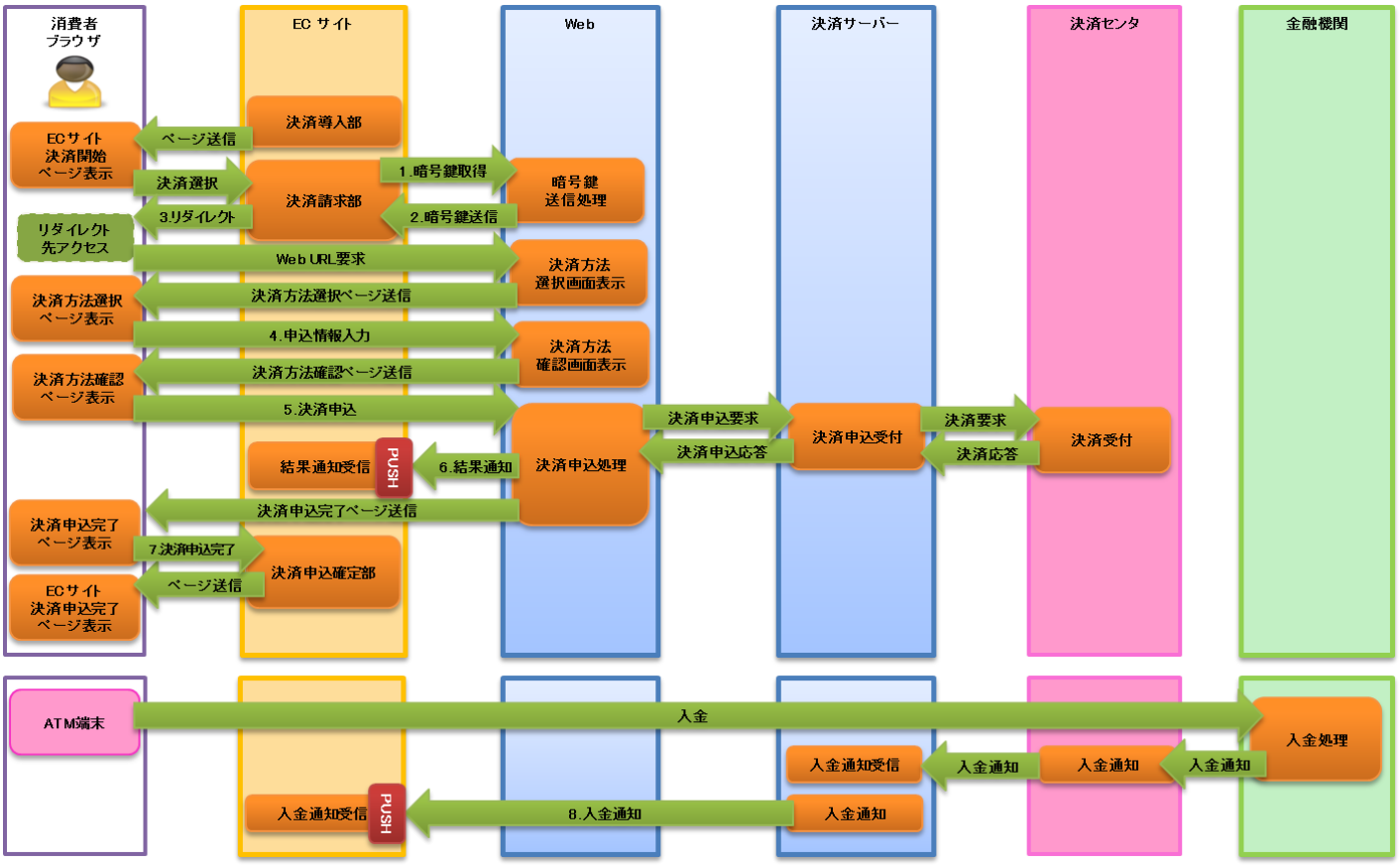


図 2-4-7 Web リンクサーバー利用時システム処理概要図(銀行決済(ATM))

No.	基本機能	処理説明
1	暗号鍵取得	EC サイト上の決済申込部に渡された決済申込情報を電文化し、Web リンクサーバーに送信します。
2	暗号鍵送信	Web リンクサーバーは EC サイトからのリクエストを受け、消費者様の暗号鍵(以下ブラウザ暗号鍵)と EC サイト用の暗号鍵をそれぞれ作成し、EC サイトに返却します。
3	リダイレクト	EC サイトは取引 ID、ブラウザ暗号鍵及びマーチャント ID をパラメータに設定した Web リンクサーバーの決済画面の URL を消費者様に送信し、決済画面に遷移するように促します。 ※決済画面を表示させる際は、ポップアップなど別画面上で表示させるのではなく、同一画面上に表示させるようにしてください。
4	申込情報入力	消費者様は決済方法を選択し、申込情報を入力します。 決済方法の選択を行うと、消費者ブラウザは決済方法確認画面に遷移します。
5	決済申込	消費者様は決済申込を実行します。
6	結果通知	Web リンクサーバーは EC サイトへ結果通知を POST 形式で送信します。
7	決済申込完了	消費者様が「注文サイトへ戻る」ボタンを押下すると、Web リンクサーバーの決済画面は EC サイトが用意する完了画面へ遷移します。
8	入金通知	決済サーバーにて消費者様による入金が完了したと確認された取引については、EC サイトへ入金通知を POST 形式で送信します。

表 2-4-7 Web リンクサーバー利用時システム処理概要(銀行決済(ATM))

【銀行決済（ネットバンク・PC）】

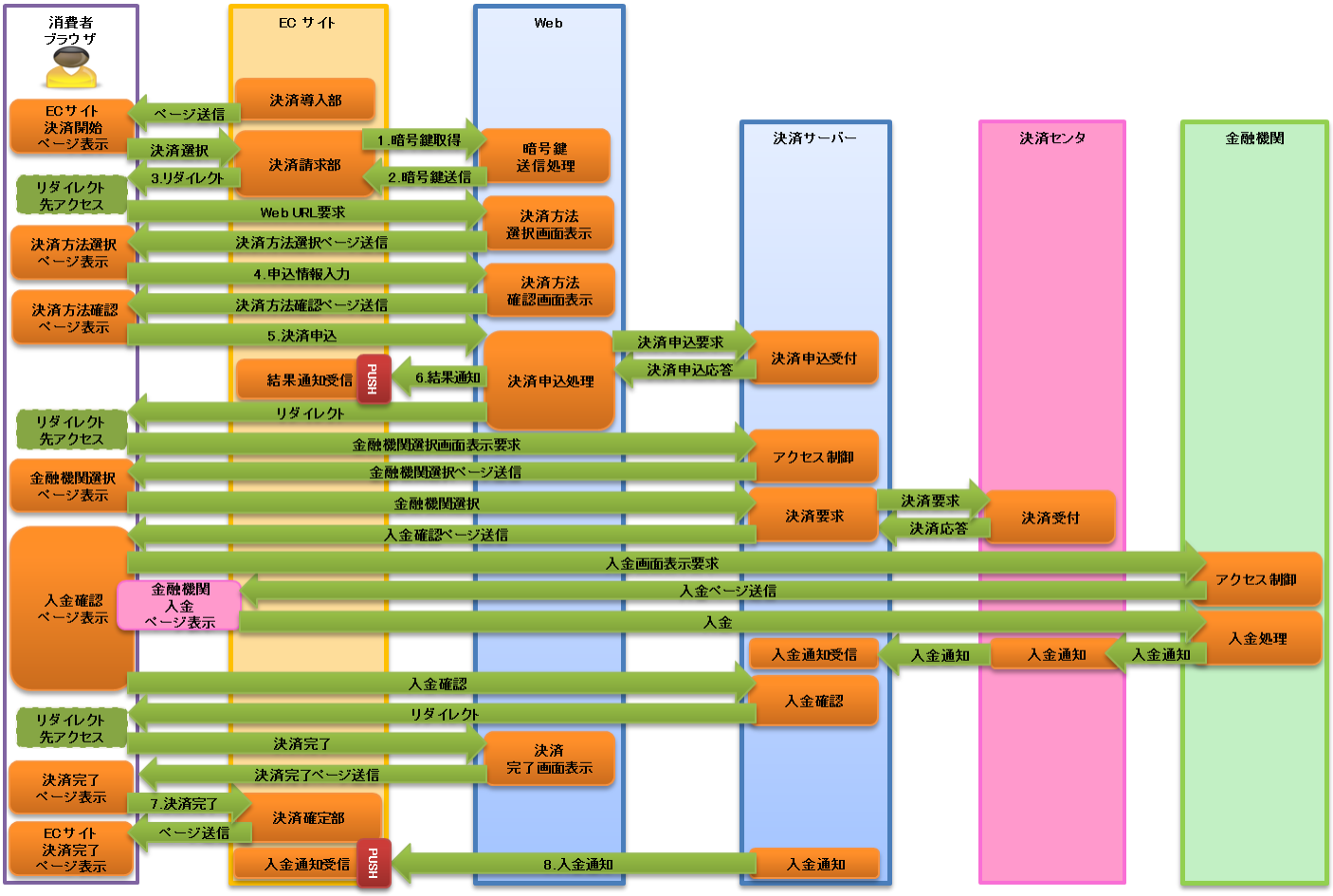


図 2-4-8 Web リンクサーバー利用時システム処理概要図（銀行決済（ネットバンク・PC））

No.	基本機能	処理説明
1	暗号鍵取得	EC サイト上の決済申込部に渡された決済申込情報を電文化し、Web リンクサーバーに送信します。
2	暗号鍵送信	Web リンクサーバーは EC サイトからのリクエストを受け、消費者様の暗号鍵(以下ブラウザ暗号鍵)と EC サイト用の暗号鍵をそれぞれ作成し、EC サイトに返却します。
3	リダイレクト	EC サイトは取引 ID、ブラウザ暗号鍵及びマーチャント ID をパラメータに設定した Web リンクサーバーの決済画面の URL を消費者様に送信し、決済画面に遷移するように促します。 ※決済画面を表示させる際は、ポップアップなど別画面上で表示させるのではなく、同一画面上に表示させるようにしてください。
4	申込情報入力	消費者様は決済方法を選択し、申込情報を入力します。 決済方法の選択を行うと、消費者ブラウザは決済方法確認画面に遷移します。
5	決済申込	消費者様は決済申込を実行します。
6	結果通知	Web リンクサーバーは EC サイトへ結果通知を POST 形式で送信します。
7	決済完了	消費者様が「注文サイトへ戻る」ボタンを押下すると、Web リンクサーバーの決済画面は EC サイトが用意する完了画面へ遷移します。
8	入金通知	決済サーバーにて消費者様による入金が完了したと確認された取引については、EC サイトへ入金通知を POST 形式で送信します。

表 2-4-8 Web リンクサーバー利用時システム処理概要（銀行決済（ネットバンク・PC））

【銀行決済（ネットバンク・モバイル）】

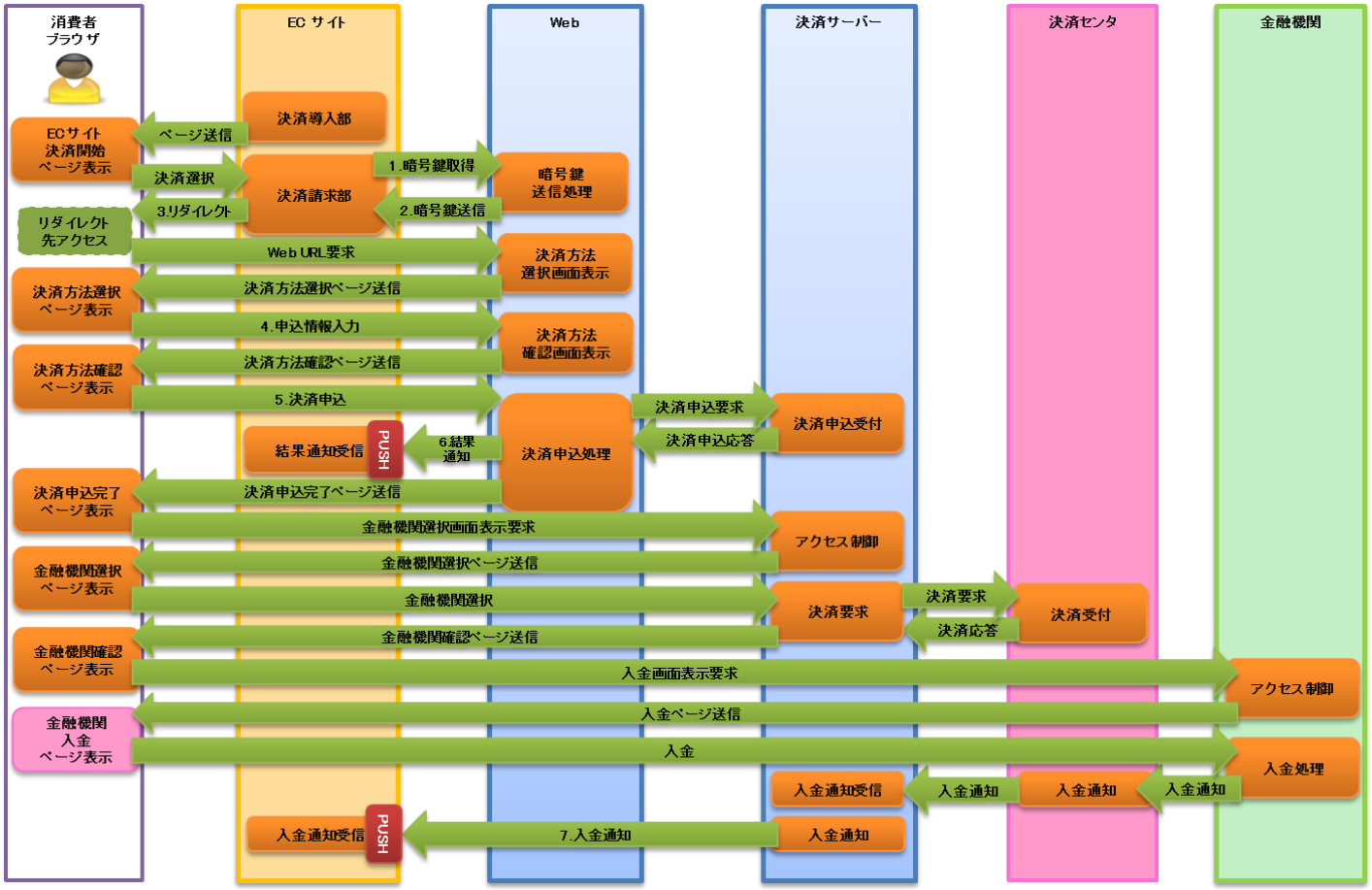


図 2-4-9 Web リンクサーバー利用時システム処理概要図（銀行決済（ネットバンク・モバイル））

No.	基本機能	処理説明
1	暗号鍵取得	EC サイト上の決済申込部に渡された決済申込情報を電文化し、Web リンクサーバーに送信します。
2	暗号鍵送信	Web リンクサーバーは EC サイトからのリクエストを受け、消費者様の暗号鍵(以下ブラウザ暗号鍵)と EC サイト用の暗号鍵をそれぞれ作成し、EC サイトに返却します。
3	リダイレクト	EC サイトは取引 ID、ブラウザ暗号鍵及びマーチャント ID をパラメータに設定した Web リンクサーバーの決済画面の URL を消費者様に送信し、決済画面に遷移するように促します。 ※決済画面を表示させる際は、ポップアップなど別画面上で表示させるのではなく、同一画面上に表示させるようにしてください。
4	申込情報入力	消費者様は決済方法を選択し、申込情報を入力します。 決済方法の選択を行うと、消費者ブラウザは決済方法確認画面に遷移します。
5	決済申込	消費者様は決済申込を実行します。 決済申込の実行を行うと、消費者ブラウザは決済サーバーの金融機関選択画面に遷移（リダイレクト）します。
6	結果通知	Web リンクサーバーは EC サイトへ結果通知を POST 形式で送信します。
7	入金通知	決済サーバーにて消費者様による入金が完了したと確認された取引については、EC サイトへ入金通知を POST 形式で送信します。

表 2-4-9 Web リンクサーバー利用時システム処理概要（銀行決済（ネットバンク・モバイル））

2-5 URL リンク生成機能について

店舗様システムのアプリケーションから暗号鍵取得の要求電文でリンク生成フラグを設定することで、Web リンクサーバーが生成した決済画面の URL を取得できます。
店舗様は、取得した URL を電子メールや SNS のメッセージ機能等を使って消費者様に送信し、Web リンクサーバーの決済画面に誘導することが可能です。

以下に、URL リンク生成機能を使って取得した決済 URL を、メールで消費者様に送信する場合の決済フローを示します。

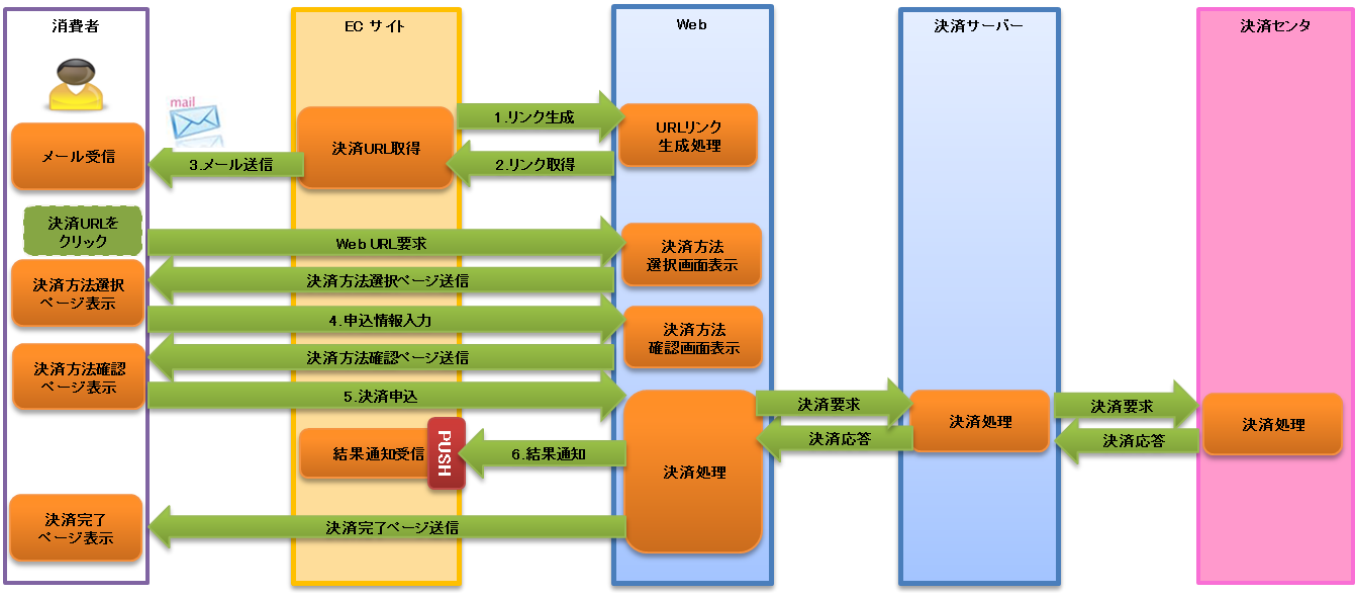


図 2-5-1 URL リンクをメール送信する場合の処理概要（URL リンク生成）

No.	基本機能	処理説明
1	リンク生成	EC サイト上の決済申込部に渡された決済申込情報を電文化し、Web リンクサーバーに送信します。
2	リンク取得	Web リンクサーバーは EC サイトからのリクエストを受け、Web リンクサーバーの決済画面の URL を返却します。
3	メール送信	EC サイトはメール本文等に上記で取得した Web リンクサーバーの決済画面の URL を記載し消費者様にメールを送信します。
4	申込情報入力	消費者様がメールにて受信した URL を開くと Web リンクサーバーの決済画面に遷移します。 決済方法を選択し、申込情報を入力後、決済方法確認画面に遷移します。
5	決済申込	消費者様は決済申込を実行します。
6	結果通知	Web リンクサーバーは EC サイトへ結果通知を POST 形式で送信します。

表 2-5-1 URL リンクをメール送信する場合の処理概要（URL リンク生成）

第3章 結果通知受信処理

3-1 結果通知受信処理の対象

3.1.1 Web リンクサーバーからの結果通知受信処理

Web リンクサーバーは、決済結果（または決済申込結果）のステータス判明後、店舗様（EC サイト）へ結果通知を PUSH 送信します。
この結果通知では、決済結果にかかわらず全ての取引が通知の対象となります。

結果通知の送信は HTTP の POST メソッドを使用しています。
Webリンクサーバーからの結果通知は、店舗様からWebリンクサーバーへの要求電文で指定した「決済結果通知先URL」に送信されます。要求電文で URL を指定しなかった場合には、ご利用申請時に登録した「決済結果通知先 URL」に送信されます。
Web リンクサーバーからの結果通知を受信するために必要な処理（ソースコード）は、サンプルプログラム内に用意しています。サンプルプログラムを店舗様の EC サイトにあわせてカスタマイズいただき、ご利用いただくことが可能です。（カスタマイズは店舗様にて実施していただきます）

※プロトコルは HTTP（Port:80）、HTTPS（Port:443）に対応しております。
これ以外のプロトコル・ポートの組み合わせには対応しておりません。

※改ざんチェック機能はサンプルプログラムに実装されていません。処理の詳細については「4-7 決済結果の改ざんチェック」を参照してください。

HTTPS での結果通知受信を希望される場合は、店舗側設置サーバーにて SSL 通信環境をご用意ください。SSL 証明書は認証局発行のものをご使用ください。
※自己署名（Self-Sign）の SSL 証明書はご利用できませんので、ご注意ください。
Web リンクサーバーからの接続時、証明書チェックでエラー扱いとなり結果通知データの送信が中止されます。

結果通知受信後の応答は、HTTP プロトコルのレスポンスメッセージの書式に準じ、HTTP ステータスコード"200"を返戻してください。
※HTTP ステータスコード"200"以外のステータス、またはサーバーから応答がない場合は、通知エラーとして処理され、マーチャント登録時に登録したリトライ回数上限（決済結果通知リトライ回数上限）までリトライを行います。

3.1.2 決済サーバーからの結果通知受信処理

特定のサービスにおいて、Web リンクサーバーからの結果通知とは別に、決済サーバーから店舗様（EC サイト）へ消費者アクションの結果、または決済サーバーにおける取引のステータスの変化を PUSH 送信することが可能です。

決済サーバーは、各決済センタから結果通知電文を受信後、店舗様へ PUSH 送信します。

決済サービス名	結果通知	説明
クレジットカード決済	ー	ー
コンビニ決済	入金通知	決済サーバーはコンビニ決済センタより消費者様の入金完了情報を受信した後に、店舗側へ入金完了を通知します。 この入金通知を売上の確定情報とし、発送処理等は、入金通知を受取ったタイミングで行ってください。
電子マネー決済	入金通知	決済サーバーは電子マネー決済センタより消費者様の入金完了情報を受信した後に、店舗側へ入金完了を通知します。 この入金通知を売上の確定情報とし、発送処理等は、入金通知を受取ったタイミングで行ってください。
銀行決済	入金通知	決済サーバーは銀行決済センタより消費者様の入金完了情報を受信した後に、店舗側へ入金完了を通知します。 この入金通知を売上の確定情報とし、発送処理等は、入金通知を受取ったタイミングで行ってください。

表 3-1-2 結果通知対象サービス一覧（決済サーバーから PUSH 送信）

決済サーバーからの結果通知受信処理の詳細につきましては、別紙 MDK【開発ガイド本体】をご参照ください。

なお、受信処理は店舗様（EC サイト）に実装していただきますが、サンプルソースコードは、別資料の MDK サンプルプログラム内にあります。サポートサイトよりダウンロードして頂きますようお願いします。

入金通知先は MAP の各種設定変更で設定します。コンビニ決済、電子マネー決済、銀行決済で別の URL を設定することが可能です。

未設定の場合は、入金通知は送信されません。リクエストパラメータによる設定はできません。

第4章 インターフェース詳細

本章では、Web リンクサーバーで使用する電文について説明します。

各項目は文字コード UTF-8 で URL エンコードされているものとします。

4-1 アクセス URL

アクセス URL	
暗号鍵取得用	https://pay3.veritrans.co.jp/web1/commodityRegist.action
Web リンクサーバー転送用	https://pay3.veritrans.co.jp/web1/deviceCheck.action
決済リンク無効化用	https://pay3.veritrans.co.jp/web1/linkRevoke.action
※ この URL にアクセスするためには、TLS1.2 をサポートするクライアントが必要です。 ※ TLS1.2 をサポートしていないクライアントではご利用できません。	

4-2 暗号鍵取得

「図 2-3-1 サンプルプログラム動作全体図」の手順⑤⑥で送受信する内容は以下の通りです。

Web リンクサーバーでは全決済方法の情報を統合しているため、決済方法／決済方法サブタイプによって必須／任意項目が異なります（後述）。

4.2.1 要求電文

■ 「設定」欄の内容は以下の通りとなります。

リンク生成以外 ： 要求電文「LINK_PAYMENT_FLAG」を**利用しない**決済

リンク生成 ： 要求電文「LINK_PAYMENT_FLAG」を利用する決済

要求電文 … 必須項目：○　任意項目：△

後述：※（決済方法／決済方法サブタイプにより異なる。【要求電文設定項目一覧】を参照してください。）

設定不可：×（設定した際にエラーとはならず、決済に利用されない項目となります）

⑤要求電文 ： EC サイト → Web リンクサーバー（HTTP POST）					
URL ： https://pay3.veritrans.co.jp/web1/commodityRegist.action					
フィールド名	項目名	書式・制限	説明	設定	
				リンク生成以外	リンク生成
MERCHANT_ID	マーチャント ID	半角英数字 22 桁以内	弊社より通知のマーチャント ID を指定します。	○	○
ORDER_ID	取引 ID	半角英数字記号 100 桁以内	店舗様にて任意に採番してください。申込処理毎につ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。決済手段が異なっても重複できません。 ※記号は"-"（ハイフン）、"_"（アンダースコア）のみ使用可能です。	○	○
MERCHANTHASH	マーチャント生成ハッシュ値	小文字のみ（大文字不可）	ハッシュシード・マーチャント ID・決済方法・取引 ID・金額をカンマ区切りで連結し SHA512 でハッシュした値を指定します。	○	○
SESSION_ID	SessionID	半角英数字 50 桁以内	店舗様にて任意に発番する乱数を指定してください。SessionID は決済完了後、Web リンクサーバーの決済完了画面から店舗様 EC サイトへ戻る際の消費者ブラウザからの通知に含まれます。店舗様で決済結果照合処理を行い暗号鍵取得リクエスト時の値と通知の値を突合し、変更がないことをご確認いただくことを推奨致します。 詳細は「4-4 消費者ブラウザからの結果連携」をご参照ください。	○	○

AMOUNT	購入金額	半角数字 9 桁以内	決済金額を指定します。**※1** クレジットカード決済（有効性確認機能）をご利用の場合は、**"0"**を指定してください。	○	○
RESPONSE_TYPE	通知メッセージタイプフラグ	右の説明を参照	Web リンクサーバーからの結果通知メッセージタイプを設定できます。 "0"：デフォルトの通知メッセージ （未指定の場合） "1"：拡張通知メッセージ（今後フィールドが追加される可能性があります。） "2"：縮小通知メッセージ	△	△
AUTO_RETURN_FLAG	自動遷移フラグ	右の説明を参照	Web リンクサーバーの決済画面での決済完了後に消費者様が「注文サイトへ戻る」ボタンを押下しなくても自動的に EC サイトの完了画面に遷移するよう設定できます。当該機能の利用条件につきましては下記 **※2** をご参照ください。 "0"：自動遷移しない（未指定の場合。Web リンクサーバーの完了画面を表示する） "1"：即時自動遷移する "2"：AUTO_RETURN_WAITING_TIME に設定された時間を待って自動遷移する。	※	×
AUTO_RETURN_WAITING_TIME	自動遷移待ち時間	1～999 で設定可能	秒単位。 AUTO_RETURN_FLAG="2"の場合、設定必須。	※	×
LINK_PAYMENT_FLAG	リンク生成フラグ	右の説明を参照	暗号鍵取得の応答電文で Web リンクサーバーが生成した決済画面の URL を取得する場合に指定します。詳細は「2-5 URLリンク生成機能について」をご参照ください。 "1"のみ指定可	×	○
LINK_EXP_DATETIME	リンク有効期限	半角数字 14 桁	YYYYMMDDhhmmss 形式 発行したリンクの有効期限を指定します。未指定の場合は無期限となります。	×	△
FINISH_PAYMENT_ACCESS_URL	決済結果通知先 URL	半角英数字記号 256 桁以内	「図 2-3-1 サンプルプログラム動作全体図」の手順⑪における、EC サイトへの決済通知先 URL を電文毎に変更する為の URL 設定項目。 URL パラメータの指定はできません。 未設定の場合は、申請時に登録した URL に送信されます。MAP での設定はできません。	△	△
FINISH_PAYMENT_RETURN_URL	決済完了後戻り URL	半角英数字記号 256 桁以内	決済が成功した後、消費者様が Web リンクサーバーの決済完了画面で「注文サイトへ戻る」ボタンを押下した際に遷移する URL。URL パラメータ、およびアンカーの指定はできません。 未設定の場合は、申請時に登録した URL に送信されます。MAP での設定はできません。	△	×
UNFINISH_PAYMENT_RETURN_URL	未決済時戻り URL	半角英数字記号 256 桁以内	消費者様が決済を行わずに Web リンクサーバーの画面で「注文サイトへ戻る」ボタンを押下した際に遷移する URL。URL パラメータ、およびアンカーの指定はできません。	△	×
ERROR_PAYMENT_RETURN_URL	決済エラー時戻り URL	半角英数字記号 256 桁以内	決済が失敗した後、消費者様が Web リンクサーバーの画面で「注文サイトへ戻る」ボタンを押下した際に遷移する URL。 URL パラメータ、およびアンカーの指定はできません。	△	×

DUMMY_PAYMENT_FLAG	ダミー取引フラグ	半角数字 1 桁	ダミー取引の実施可否を設定します。 "0":本番取引（未指定の場合） "1":ダミー取引	△	△
SETTLEMENT_TYPE	決済方法	半角数字 2 桁	"00":決済方法指定なし "01":カード決済 "02":コンビニ決済 "03":電子マネー決済 "04":銀行決済 "01"～"04"を設定した場合は、決済方法は固定になります。 消費者に決済方法を選択させる場合は、「"00":決済方法指定なし」 を設定してください。 “カード決済と銀行決済から選択させる”のような設定はできません。	○	○
SETTLEMENT_SUB_TYPE	決済方法サブタイプ	半角数字 3 桁	SETTLEMENT_TYPE（決済方法）で"02"～"04"を設定した場合にサブタイプを設定できます。 （例えばコンビニ決済で、コンビニを自由に選択させるのではなくセブンーイレブンに限定したい場合等に設定します。） 決済方法で「"02":コンビニ決済」を選択した場合 "201":セブンーイレブン "205":イーコン（ローソン、ファミリーマート、ミニストップ、セイコーマート） "204":その他（デイリーヤマザキ） 「"03":電子マネー決済」を選択した場合 "311":PC Edy "312":モバイル Edy "321":PC Suica "322":モバイル Suica 「"04":銀行決済」を選択した場合 "411":ATM 決済 "420":ネットバンク決済 決済方法で「"00":決済方法指定なし」「"01":カード決済」を設定した場合は本項目は設定できません。	※	※
LANG_ENABLE_FLAG	言語選択可否フラグ	半角数字 1 桁	"0":選択不可 "1":選択可	△	△
LANG	使用言語	右の説明を参照	下記の使用可能言語をカンマ区切りで入力 "ja":日本語 "en":英語 "zh":中国語 言語選択可否フラグと使用言語の設定に関する詳細につきましては下記 **※3** をご参照ください。	△	△
CARD_INSTALLMENT_JPO	カード支払区分	半角数字 2 桁以内	店舗様のご利用できる支払区分 例: "10":一括 "21":ボーナス一括 "61":分割 "80":リボルビング	※	※

CARD_INSTALLMENT_JPO_CNT	カード分割回数	半角数字 2 桁以内	店舗様のご利用できる分割回数 例: "03":3 回 "06":6 回 "10":10 回 "12":12 回 "15":15 回 "16":16 回 "18":18 回 "20":20 回 "24":24 回 ※CARD_INSTALLMENT_JPO は"61"の場合のみ指定可能。	※	※
CARD_CAPTURE_FLAG	カード売上フラグ	半角数字 1 桁	"0":与信のみ "1":与信・売上	※	※
DDD_ENABLE_FLAG	本人認証有効フラグ	半角数字 1 桁	クレジットカード決済にて本人認証が利用可能な場合に、電文毎に利用可否を設定する項目。未設定の場合は"1"となります。 "0":本人認証利用しない "1":本人認証利用する(登録済みの場合のみ)	※	※
DDD_VERSION	3D セキュアバージョン	半角数字 1 桁	本人認証有効時の 3D セキュアのバージョン "1":3D セキュア "2":3D セキュア 2.0 ※本パラメータが未指定の場合、MAP の「各種設定変更」の「3G-Web 設定情報変更」で設定可能な「3D セキュアバージョン」の設定値を参照します。どちらも未設定の場合は"1"となります。	※	※
CARDHOLDER_EMAIL	カード保有者メールアドレス	半角英数字記号 254 桁以内	カード保有者メールアドレス 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。 RFC5322 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/	※	※
CARDHOLDER_HOME_PHONE_NUMBER	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	※	※
CARDHOLDER_HOME_PHONE_COUNTRY	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してください。 本パラメータが未指定の場合、日本の国コード(81)となります。	※	※
CARDHOLDER_MOBILE_PHONE_NUMBER	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	※	※

CARDHOLDER_MOBILE_PHONE_COUNTRY	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してください。 本パラメータが未指定の場合、日本の国コード(81)となります。	※	※
CARDHOLDER_WORK_PHONE_NUMBER	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	※	※
CARDHOLDER_WORK_PHONE_COUNTRY	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してください。 本パラメータが未指定の場合、日本の国コード(81)となります。	※	※
SHOP_NAME	モバイル Edy 用ショップ名	文字列 48 バイト以内	決済依頼メール、決済完了メールで使用する店舗名	※	※
SCREEN_TITLE	Suica 用商品名	文字列 40 バイト以内	決済完了画面・決済確認画面等で「商品・サービス名」に表示される文字列	※	※
CONTENTS	請求内容	全角 12 文字以内	インフォメーションとして ATM 等に表示される文字列 **※4**	※	※
CONTENTS_KANA	請求内容カナ	全角カナ 24 文字以内	インフォメーションとして ATM 等に表示される文字列	※	※
TIMELIMIT_OF_PAYMENT	支払期限	半角数字 8 桁	YYYYMMDD 形式 **※5**	※	※
以下、商品の数だけ繰り返し設定					
COMMODITY_UNIT	単価	半角数字 9 桁以内	未設定の場合、Web リンクサーバー決済確認画面に表示されないため、設定が望ましい	△	△
COMMODITY_NUM	個数	半角数字 4 桁以内		△	△
COMMODITY_NAME	商品名	文字列 50 バイト以内		△	△

※1: 決済金額の上限と下限の詳細を以下に示します。決済方法と種別を指定している場合は、下記の制限となります。

ただし、決済方法の指定がない場合や電子マネー決済指定で serviceOptionType(決済サービスオプション)の指定がない場合は、利用可能決済の中で一番小さい上限が使用されます。

決済方法		決済金額の上限
クレジットカード決済		1 以上 99,999,999 以下
コンビニ決済		1 以上 299,999 以下
電子マネー決済	Edy	1 以上 50,000 以下
	Suica	1 以上 20,000 以下
銀行決済		1 以上 999,999,999 以下

クレジットカード決済(有効性確認機能)を利用する場合は"0"を指定してください。

※2: 完了画面自動遷移機能をご利用いただく場合、以下の条件を満たす必要があります。

・クレジットカード決済であること。

・決済自体は成功すること。

※3: 言語選択可否フラグと使用言語の設定による Web リンクサーバーの画面表示仕様は以下の通りです。

言語選択可否フラグが"0":選択不可
消費者様ブラウザの設定言語で表示。言語選択コンボボックスは表示されません。 ブラウザの設定言語が Web リンクサーバーが対応する言語でない場合は日本語で表示されます。

言語選択可否フラグが"1":選択可	
使用言語を 1 つだけ指定	指定の使用言語で表示。言語選択コンボボックスは表示されません。 "en" (英語)を指定した場合、Web リンクサーバーの決済画面は英語表示となります。
使用言語を複数指定	初期表示は消費者様ブラウザの設定言語で表示します。 ブラウザの設定言語が Web リンクサーバーが対応する言語でない場合は日本語で表示されます。 言語選択コンボボックスが表示され、指定した使用言語での表示を選択できます。

※4: 銀行決済の場合、請求内容(CONTENTS)は以下のような常用漢字以外の文字はご使用いただけない場合があります。使用不可な文字の場合、支払い申込後、エラーコード PG06 が発生し、決済失敗となりエラー画面に遷移します。

使用可能な文字の詳細は、別紙【インターフェース詳細 銀行】の利用可能文字一覧をご参照ください。

注) 発生するエラーコードは、予告なしに別コードになる場合があります。

<使用できない文字の例>

髙、﨑、琦、栁、德、悟、棄、郎、朗、彌、匡、㈱、㈲、㈹、ｉ、Ⅰ

※5: 支払期限の詳細を以下に示します。

決済方法と種別を指定している場合は、下記の制限となります。

ただし、決済方法の指定がない場合やコンビニ決済指定で種別の指定がない場合は、一番短い当日～60 日の制限になります。

決済方法		支払期限
コンビニ決済	セブン－イレブン	当日～150 日後
	ローソン・ファミマ・セイコーマート	当日～60 日後
	その他	当日～365 日後
電子マネー決済		当日～90 日後
銀行決済		当日～60 日後

当該項目が要求電文で指定されない場合には、加盟店マスタに登録されている支払期限日数が適用されます。

申込当日を起算日として指定の日数で期限日付を算出します。

例）TIMELIMIT_OF_PAYMENT を 10 日とする場合、2026/4/1 15:00 に決済申込を行うと、支払期限は 2026/4/11 23:59 になります。

【要求電文設定項目一覧】

必須項目：○

任意項目（決済時必須）：□（要求電文では任意項目ですが、設定しない場合は画面入力時に必須となります）

任意項目（決済時補完）：◇（要求電文では任意項目ですが、設定しない場合は Web リンクサーバーにて補完されます）

任意項目（決済時任意）：△（要求電文時、画面入力時共に任意項目となります）

設定不可：×（設定した際にエラーとはならず、決済に利用されない項目となります）

⑤要求電文 ： EC サイト → Web リンクサーバー											
フィールド名	決済方法／決済方法サブタイプ										
				電子マネー					銀行		
	指定なし	カード	コンビニ	指定なし	PC Edy	モバイル Edy	PC Suica	モバイル Suica	指定なし	ATM	ネットバンク
AUTO_RETURN_FLAG	△	△	×	×	×	×	×	×	×	×	×
AUTO_RETURN_WAITING_TIME	※1	※1	×	×	×	×	×	×	×	×	×
SETTLEMENT_SUB_TYPE	×	×	△	×	○	○	○	○	×	○	○
CARD_INSTALLMENT_JPO	×	□	×	×	×	×	×	×	×	×	×
CARD_INSTALLMENT_JPO_CNT	×	□	×	×	×	×	×	×	×	×	×
CARD_CAPTURE_FLAG	◇	◇	×	×	×	×	×	×	×	×	×
DDD_ENABLE_FLAG	◇	◇	×	×	×	×	×	×	×	×	×
DDD_VERSION	◇	◇	×	×	×	×	×	×	×	×	×
CARDHOLDER_EMAIL	※4	※4	×	×	×	×	×	×	×	×	×
CARDHOLDER_HOME_PHONE_NUMBER	※4	※4	×	×	×	×	×	×	×	×	×
CARDHOLDER_HOME_PHONE_COUNTRY	※4	※4	×	×	×	×	×	×	×	×	×
CARDHOLDER_MOBILE_PHONE_NUMBER	※4	※4	×	×	×	×	×	×	×	×	×
CARDHOLDER_MOBILE_PHONE_COUNTRY	※4	※4	×	×	×	×	×	×	×	×	×
CARDHOLDER_WORK_PHONE_NUMBER	※4	※4	×	×	×	×	×	×	×	×	×
CARDHOLDER_WORK_PHONE_COUNTRY	※4	※4	×	×	×	×	×	×	×	×	×
SHOP_NAME	△	×	×	△	×	△	×	×	×	×	×
SCREEN_TITLE	※2	×	×	※2	×	×	○	○	×	×	×
CONTENTS	※3	×	×	×	×	×	×	×	○	○	○
CONTENTS_KANA	※3	×	×	×	×	×	×	×	○	○	○
TIMELIMIT_OF_PAYMENT	△	×	◇	◇	×	◇	◇	◇	◇	◇	◇

※1 ： AUTO_RETURN_FLAG="2"の時は、必須項目となります。

※2 ： Suica 決済（PC Suica／モバイル Suica）ご利用時は、必須項目となります。

※3 ： 銀行決済（ATM／ネットバンク）ご利用時は、必須項目となります。

※4 ： 本人認証が有効な場合、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。

日本以外の電話番号を設定する場合、「電話番号」と「国コード」をセットで設定してください。

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。

4.2.2 応答電文

■ 「設定」欄の内容は以下の通りとなります。

応答電文 … 条件付返戻:※

【リンク生成以外の場合】

⑥応答電文 ： Web リンクサーバー → EC サイト				
フィールド名	項目名	書式・制限	説明	設定
MERCHANT_ENCRYPTION_KEY	マーチャント暗号鍵	半角英数字 120 桁以内	EC サイトが保管する暗号鍵 （成功時のみ返戻）	※
BROWSER_ENCRYPTION_KEY	ブラウザ暗号鍵	半角英数字 120 桁以内	ブラウザに戻される暗号鍵 （成功時のみ返戻）	※
ERROR_MESSAGE	エラーメッセージ	別紙 ※1	Web リンクサーバーが戻すエラーメッセージ （エラー時のみ返戻）	※

※「マーチャント暗号鍵」は決済処理では使用しません。決済情報照会の際に必要になる場合がございますので大切に保管してください。

【リンク生成の場合】

⑥応答電文 ： Web リンクサーバー → EC サイト				
フィールド名	項目名	書式・制限	説明	設定
VTW_START_URL	リンク URL	URL 形式	Web リンクサーバーの決済画面へ遷移するためのリンク URL （成功時のみ返戻）	※
ERROR_MESSAGE	エラーメッセージ	別紙 ※1	Web リンクサーバーが戻すエラーメッセージ （エラー時のみ返戻）	※

※1 ： 『3G-Web 結果コード一覧』をご参照ください。

4-3 Web リンクサーバー転送

※ リンク生成の場合は利用しません。

「図 2-3-1 サンプルプログラム動作全体図」 手順⑨の暗号鍵取得で返戻されたブラウザ暗号鍵とマーチャント ID および取引 ID を電文に設定し、POST で消費者ブラウザを Web リンクサーバーの決済画面へ転送します。

■ 「設定」欄の内容は以下の通りとなります。

転送電文 … 必ず転送:○

⑨転送電文 ： EC サイト → 消費者ブラウザ（HTTP POST） URL ： https://pay3.veritrans.co.jp/web1/deviceCheck.action				
フィールド名	項目名	書式・制限	説明	設定
MERCHANT_ID	マーチャント ID	半角英数字 22 桁以内	マーチャントを識別する ID	○
ORDER_ID	取引 ID	半角英数字記号 100 桁以内	マーチャントの注文を識別する ID	○
BROWSER_ENCRYPTION_KEY	ブラウザ暗号鍵	半角英数字 120 桁以内	ブラウザに戻される暗号鍵	○

4-4 消費者ブラウザからの結果連携

※ リンク生成の場合は利用しません。

「図 2-3-1 サンプルプログラム動作全体図」の手順⑭で Web リンクサーバーの決済完了画面で消費様が「注文サイトへ戻る」ボタンを押下すると、消費者ブラウザが指定の URL に遷移し決済結果が GET メソッドで送信されます。店舗様では決済が完了した場合に遷移する画面にて、決済情報が改ざんされていないことをご確認いただく為、以下の実装をしていただくことを推奨致します。

- 消費者ブラウザから送信された各パラメータから算出したハッシュ値と、resultHash が一致すること。
  ハッシュ値の算出方法など、詳細は「4-7 決済結果の改ざんチェック」をご覧ください。

消費者ブラウザから店舗様 EC サイトへの戻り URL は、「4-2 暗号鍵取得」の要求電文で取引毎に設定することができます。要求電文で URL を設定せずマーチャント登録申請時にマスタ登録した URL がある場合はその URL が使われます。両方ある場合には要求電文の URL を使用します。

決済が完了したか否か、エラーが発生したかにより、店舗様 EC サイトへ戻る際の遷移先を指定することができ、それぞれ以下の戻り URL へ遷移します。

決済が完了した場合 ： 決済完了後戻り URL
決済がエラーで終了した場合 ： 決済エラー時戻り URL
消費者様が決済を行わなかった場合 ： 未決済時戻り URL

消費者ブラウザから送信される内容は以下の通りです。

■ 「設定」欄の内容は以下の通りとなります。
送信情報 …必ず送信：〇 その他条件付き：※（条件は説明欄に記載）

⑭送信情報 ： 消費者ブラウザ → EC サイト（HTTP GET）						
フィールド名	項目名	書式・制限	説明	設定		
				決済完了	決済エラー	未決済
orderId	取引 ID	半角英数字記号 100 桁以内	EC サイトから送信された取引 ID	〇	〇	〇
mStatus	ステータス	4.5.2 参照	4.5.2 参照	〇	〇	×
vResultCode	結果コード	4.5.2 参照	4.5.2 参照	〇	〇	×
sessionId	セッション ID	4-2 参照	4-2 で送信した SESSION_ID	〇	〇	×
resultHash	改ざんチェック用ハッシュ値	右記で算出した値	改ざんチェック用の値 詳細は「4-7 決済結果の改ざんチェック」をご確認ください。 （マスタ設定で改ざんチェックが有効になっている場合のみ返戻されます。）	※	※	×

4-5 Web リンクサーバーからの結果通知電文

4.5.1 結果通知電文の概要

■ **機能概要**

Web リンクサーバーは決済結果（または決済申込結果）のステータス判明後、EC サイトへ結果通知を PUSH 送信します。

結果通知は、HTTP の POST で通知します。

※ プロトコルは HTTP（Port：80）、HTTPS（Port：443）に対応しています。

処理の概要については本ガイド「第 3 章 結果通知受信処理」を参照してください。

■ **結果通知受信処理結果について**

Web リンクサーバーからの通知に対して EC サイトが HTTP ステータスコード"200"を返戻した場合、受信処理が正常に終了したものと判断します。

"200"以外のコードを返した場合は、受信失敗と判断し、マーチャント登録時に登録したリトライ回数上限（結果通知リトライ回数上限）までリトライを行います。

※ 規定の回数失敗した場合は、通知処理が停止しますのでご注意ください。

※ Web リンクサーバーからの結果通知電文には、HMAC 値（content-hmac）は含まれません。

■ **改ざんチェックについて**

結果通知を受信した際、決済情報が改ざんされていないことをご確認いただく為、以下の実装をしていただくことを推奨致します。

- Web リンクサーバーから送信された各パラメータから算出したハッシュ値と、resultHash が一致すること。
  ハッシュ値の算出方法など、詳細は「4-7 決済結果の改ざんチェック」をご覧ください。

4.5.2 結果通知受信

「図 2-3-1 サンプルプログラム動作全体図」の手順⑪で Web リンクサーバーから EC サイトへ決済結果を通知します。

結果通知の形式には「デフォルト」「拡張」「縮小」の 3 つのタイプがあり、いずれのタイプで通知するかは暗号鍵取得要求電文の「通知メッセージタイプ」で指定可能です。詳細は「4.2.1 要求電文」をご参照ください。

通知メッセージは将来的にフィールドが追加される可能性がございます。以下に定義されたフィールド名以外のフィールドが連携された場合でもエラーとならないようご注意ください。

※ 結果通知は HTTP で受信することが可能ですが、決済方法によって個人情報（氏名、電話番号等）が設定されるケースがある為、HTTP での受信は非推奨となります。HTTP で受信する場合には「縮小通知メッセージ」をご利用ください。

尚、今後「縮小通知メッセージ」にフィールドを追加する場合でも HTTP で送信しても問題ない項目のみを追加します。

■ 「設定」欄の内容は以下の通りとなります。

受信情報 … 必ず受信:○　場合により受信:△

⑪受信情報 ： Web リンクサーバー → EC サイト（HTTP POST メソッド）						
フィールド名	項目名	書式・制限	説明	設定		
				デフォルト	拡張	縮小
orderId	取引 ID	半角英数字記号 100 桁以内	EC サイトから送信された取引 ID	○	○	○
mStatus	ステータス	右の説明を参照	処理結果に対するステータス "success":正常終了 "failure":異常終了 "pending":保留	○	○	○
mErrMsg	メッセージ	別紙 **※1**	処理結果に対するメッセージ ※クレジットカード決済（本人認証有り）の場合、この値は連携されません。 ※クレジットカード決済（本人認証有り）以外の決済では必ず連携されます。	△	△	△
vResultCode	結果コード	別紙 **※1**	処理結果を詳細に表すコード	○	○	○
userName	漢字氏名	全角 20 文字以内	Web リンクサーバーの決済画面で入力した個人情報 ※個人情報の受信には**別途ご登録が必要**のため、営業担当までご相談ください。 ※個人情報を受信する場合は、**http（ポート 80）のご利用はできません。** ※決済方法／決済方法サブタイプ毎に返戻される項目詳細については、下記**※2** をご参照ください。	△ ※2	△ ※2	－
userNameKana	カナ氏名	全角カナ 20 文字以内		△ ※2	△ ※2	－
mailAddress	メールアドレス	半角英数字記号 50 桁以内		△ ※2	△ ※2	－
telephoneno	電話番号	半角数字 11 桁以内		△ ※2	△ ※2	－
settlementType	決済方法	半角数字 2 桁	最終的に支払った決済方法。 "01":カード決済 "02":コンビニ決済 "03":電子マネー決済 "04":銀行決済	－	○	－
settlementSubType	決済方法サブタイプ	半角数字 3 桁	最終的に支払った決済方法サブタイプ。 決済方法にてコンビニ決済選択時 "201":セブンーイレブン "205":イーコン（ローソン、ファミリーマート、ミニストップ、セイコーマート） "204":その他（デイリーヤマザキ） 決済方法にて電子マネー決済選択時 "311":PC Edy "312":モバイル Edy "321":PC Suica "322":モバイル Suica	－	△	－

⑪受信情報 ： Web リンクサーバー → EC サイト（HTTP POST メソッド）						
フィールド名	項目名	書式・制限	説明	設定		
				デフォルト	拡張	縮小
			決済方法にて銀行決済選択時 "411"：ATM 決済 "420"：ネットバンク決済			
acquirerCode	仕向け先コード	半角数字 2 桁以内	決済要求電文が仕向けられるカード会社です。 消費者様が保持しているクレジットカードのカード発行会社ではなく、店舗様が加盟店契約をしている加盟店管理会社です。 「5-3 クレジットカード決済 仕向け先カード会社の一覧」をご参照ください。	－	△ ※ 3	－
resAuthCode	応答承認番号	文字列 12 桁以内	カード会社が発行する承認番号	－	△ ※ 3	－
resCardNumber	カード番号	文字列 16 桁以内	消費者様が入力したカード番号。 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"）	－	△ ※ 3	－
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が応答電文を返した日時 （YYYYMMDDhhmmss 形式）	－	△ ※ 3	－
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。 "35"：JCB "4"：VISA "5"：MASTER "34", "37"：AMEX	－	△ ※ 4	－
receiptNo	受付番号	文字列 32 文字以内	正常に決済請求が完了した際に返戻されるコンビニの受付番号 ・セブンーイレブン ： 払込票番号（13 桁） ・イーコン ： 受付番号（6 桁） ・その他 ： オンライン決済番号（11 桁）	－	△ ※ 5	－
haraikomiUrl	払込票 URL	半角英数字 256 文字以内	コンビニから返される払込票 URL。 ※セブンーイレブン ： PC 用画面・スマートフォン用画面・携帯用画面を消費者様の利用端末を判別して表示します。 ※イーコン ： 返戻されません。 ※デイリーヤマザキ、ヤマザキデイリーストアー：携帯での表示・支払に対応しています。戻り値の「 https:// ～ .info/JLP/JLPcon 」の部分を「https://w2.kessai.info/JLM/JLMcon」に置換えてご利用ください。 例）https://w2.kessai.info/JLM/JLMcon?code=xxx～&rkbn=1	－	△ ※ 5	－
shunoKikanNo	収納機関番号	半角英数字 8 桁以内	銀行決済（ATM 決済）にて返戻される収納機関番号	－	△ ※ 6	－

⑪受信情報 ： Web リンクサーバー → EC サイト（HTTP POST メソッド）						
フィールド名	項目名	書式・制限	説明	設定		
				デフォルト	拡張	縮小
customerNo	お客様番号	半角英数字 20 桁以内	銀行決済(ATM 決済)にて返戻されるお客様番号	−	△ ※6	−
confirmNo	確認番号	半角英数字 6 桁以内	銀行決済(ATM 決済)にて返戻される確認番号	−	△ ※6	−
resultHash	改ざんチェック用ハッシュ値	右記で算出した値	改ざんチェック用の値 詳細は「4-7 決済結果の改ざんチェック」をご確認ください。	△ ※7	△ ※7	△ ※7
sessionId	セッション ID	4-2 参照	4-2 で送信した SESSION_ID	△ ※7	△ ※7	△ ※7

※1 ： 別紙 『決済結果コード一覧』をご参照ください。

※2 ： 入力値の返戻について

各情報が返戻される決済は、以下の通りです。

	カード	コンビニ	電子マネー	銀行
漢字氏名	−	○	−	○
カナ氏名	−	○	−	○
メールアドレス	−	−	○	−
電話番号	−	○	−	−

※3 ： カード決済の場合のみ返戻されます。(settlementType="01")

※4 ： カード決済にて本人認証利用する場合のみ返戻されます。

※5 ： コンビニ決済の場合のみ返戻されます。(settlementType="02")。

※6 ： 銀行決済(ATM 決済)の場合のみ返戻されます。(settlementType=04,settlementSubType="411")

※7 ：改ざんチェック機能の設定が有効になっている場合のみ返戻されます。設定は MAP より確認・変更いただけます。

上記※3～※6 については、必ず値が返戻されるわけではありません。クレジットカードの与信取得エラー時など、値が設定されない場合があります。

4-6 決済サーバーからの結果通知電文

決済サーバーからの結果通知電文送信の機能がある決済サービスは、「表 3-1-2 結果通知対象サービス一覧（決済サーバーから PUSH 送信）」をご参照ください。

結果通知電文の概要、および各決済サービスの結果通知電文のインターフェース詳細については、決済サーバーの【開発ガイド】をご参照ください。

4-7 決済結果の改ざんチェック

4.7.1 Web リンクサーバーからの結果通知

「4-4 消費者ブラウザからの結果連携 消費者ブラウザからの結果連携」、および「4-5 Web リンクサーバーからの結果通知電文」で決済結果を受信した際、改ざんチェックの実施を推奨いたします。

■ 改ざんチェックの利用方法

- 改ざんチェック機能を利用するには、改ざんチェック機能の設定が有効である必要があります。設定は MAP より確認・変更いただけます。
- 改ざんチェック機能が有効な場合、「4-4 消費者ブラウザからの結果連携」と「4-5 Web リンクサーバーからの結果通知」で改ざんチェック用のハッシュ値(resultHash)を連携いたします。結果通知を受信した際に、下記ハッシュ値算出方法に従って算出したハッシュ値と照合を行い、受信した決済結果が改ざんされていないことを確認してください。

■ ハッシュ値算出方法

- 算出に必要な情報

対象パラメータ	説明
orderId	結果通知で受信した取引 ID
mStatus	結果通知で受信した決済結果
vResultCode	結果通知で受信した結果コード
sessionId	結果通知で受信したセッション ID
ハッシュシード	3G-Web のマーチャント認証用のハッシュシード （MAP からご確認いただけます）

- 算出方法

  上記パラメータを、上から順にカンマ区切りで結合した文字列を、SHA512 でハッシュ化する。

■ 算出例

- 通知内容例

```
settlementType=01&kindCode=null&orderId=test_0001&cardHolderName=****&mStatus=success&mErrMsg=null&cardExpDate=01/27&centerResponseDate=20260403175037&resBrandId=4&sessionId=Abcd12345&resultHash=9fdd51fb435dbc7e9dfcf393cff996e0393cf9d591af53480f5ed049db439538fcfb449b41ea77b27fa98663b99931388b35aa8c9da2d66556c5f69136ad028c&resAuthCode=000000&resCardNumber=411111******1111&acquirerCode=01&vResultCode=G011A00100000000
```

- 使用するパラメータ

対象パラメータ	サンプル値
orderId	test_0001
mStatus	success
vResultCode	G011A00100000000
sessionId	Abcd12345
ハッシュシード	abcdefghijklmnopqrstuvwxyz0123456789abcdefghijklmnopqrstuvwxyz01

- サンプル値を用いて算出されるハッシュ値

```
9fdd51fb435dbc7e9dfcf393cff996e0393cf9d591af53480f5ed049db439538fcfb449b41ea77b27fa98663b99931388b35aa8c9da2d66556c5f69136ad028c
```

■ 実装例

➢ ハッシュ値を取得するための Java コードサンプルです。

```
package jp.co.veritrans.vtweb.hashsample;

import java.nio.charset.StandardCharsets;
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;
import java.util.HexFormat;

public class HashSample {

    public static void main(final String[] args) throws NoSuchAlgorithmException {
        // 結果通知で取得した”resultHash”の値
        String resultHash =
        "9fdd51fb435dbc7e9dfcf393cff996e0393cf9d591af53480f5ed049db439538fcfb449b41ea77b27fa98663b99931388b3
        5aa8c9da2d66556c5f69136ad028c";

        // ハッシュ値算出対象のパラメータを結合した文字列
        String hashKey =
        "test_0001,success,G011A00100000000,Abcd12345,abcdefghijklmnopqrstuvwxyz0123456789abcdefghijklmnopqrstu
        vwxyz01";

        byte[] hash = MessageDigest.getInstance("SHA-512").digest(hashKey.getBytes(StandardCharsets.UTF_8));
        String calcHash = HexFormat.of().formatHex(hash);

        System.out.println(resultHash.equals(calcHash));
    }

}
```

4.7.2 決済サーバーからの入金通知

「3.1.2 決済サーバーからの結果通知受信処理」で入金通知（結果通知）を受信した際、改ざんチェックの実施を推奨いたします。

決済サーバーからの入金通知の詳細につきましては、別紙 MDK【開発ガイド本体】（4.2 決済結果通知）をご参照ください。

なお、受信処理および改ざんチェックの実装につきましては、加盟店様（EC サイト）にてご対応をお願いします。実装の参考となるサンプルソースコードは、【開発ガイド本体】（4.2.4 HMAC による結果通知の改ざんチェック）に記載されているほか、サポートサイトからダウンロード可能な MDK【サンプルプログラム】内にも同梱されております。

サポートサイト（MDK）：

https://www.veritrans.co.jp/trial/4g/download/mdk.html

4-8 決済リンク無効化

4-2 暗号鍵取得で生成した取引(決済リンク含む)を無効化します。

無効化に成功した取引では、以降決済を実施することができなくなります。

以下の条件に該当する取引に対してご利用いただけます。

- 決済方法
  - 全ての決済方法
- Web リンクサーバーへの接続方式
  - 全ての接続方式(リンク生成・リンク生成以外のいずれも対象)
- 取引の状態
  - 無効化を実施する時点で未決済であること
    - 既に消費者の操作で決済リクエストが実施されている場合は無効化の対象外となります。決済の成功・失敗は問いません。

4.8.1 要求電文

- 「設定」欄の内容は以下の通りとなります。

転送電文 … 必ず転送:○

転送電文 : EC サイト → Web リンクサーバー (HTTP POST)				
URL : https://pay3.veritrans.co.jp/web1/linkRevoke.action				
フィールド名	項目名	書式・制限	説明	設定
MERCHANT_ID	マーチャント ID	半角英数字 22 桁以内	マーチャントを識別する ID	○
ORDER_ID	取引 ID	半角英数字記号 100 桁以内	無効化を実施する対象の取引 ID	○
MERCHANTHASH	マーチャント生成ハッシュ	小文字のみ(大文字不可)	以下の値を上から順にカンマ区切りで連結し、SHA512 でハッシュ化した値。 ・MID ・取引 ID ・ハッシュシード	○

4.8.2 応答電文

- 「設定」欄の内容は以下の通りとなります。

応答電文 … 必ず返戻:○ 場合により返戻:△

応答電文 : Web リンクサーバー → EC サイト				
フィールド名	項目名	書式・制限	説明	設定
ORDRE_ID	取引 ID	半角英数字記号 100 桁以内	EC サイトから送信された取引 ID	○
STATUS	ステータス	右記参照	処理結果に対するステータス “success”:処理成功 ”failure”:異常終了	○
V_RESULT_CODE	結果コード	別紙 ※1	処理結果を詳細に表すコード	○
ERROR_MESSAGE	エラーメッセージ	別紙 ※1	処理結果に対するメッセージ ※STATUS が failure の場合のみ返戻されます	△

※1 : 別紙 『3G-Web 結果コード一覧』をご参照ください。

4.8.3 処理結果の判定について

本インターフェースの成功・失敗判定の例は以下の通りです。

- **成功**
  - 指定された取引の無効化処理が正常に終了した場合。
  - リンク有効期限がすでに切れていた場合。
  - 指定された取引がすでに無効化されていた場合。
- **失敗**
  - 決済が実行されていた場合。
  - 指定された取引が存在しない場合。

※各エラーの詳細は「ERROR_MESSAGE」、または別紙『3G-Web 結果コード一覧』をご確認ください。

第5章 その他補足事項

5-1 決済結果の確認方法

各方法の導入につきましては店舗様にてご検討いただき、取引管理/運用にご活用ください。
これらの方法は併用してご活用いただくことが可能です。

✧ Web リンクサーバーからの結果通知電文を受信する(**推奨**)
詳しくは「4-5 Web リンクサーバーからの結果通知電文」をご参照ください。

✧ MAP で確認する
MAP(Merchant Administration Portal)は決済サーバーにおける管理・運用上の各種情報・機能を提供する Web 型の管理ツールです。
本番運用時の取引だけでなく、テスト取引などの処理結果も MAP を利用して検索・参照することが可能です。
Web リンクサーバーからの結果通知受信に失敗した場合や、受信設定ができない場合などはこちらをご利用いただくことで取引の処理結果を確認することができます。
MAP のご利用方法の詳細につきましては、MAP のヘルプメニューから各種ドキュメントをご参照ください。

✧ MDK を利用して取引の検索処理を実装する
弊社が提供する MDK(Merchant Development Kit)を店舗様のシステムに導入し、検索機能をご利用いただくことで、取引の結果を取得することができます。
MDK のご利用方法の詳細につきましては、別冊のガイドをご参照ください。

※ 注意点

・ 暗号鍵取得処理が失敗した場合は応答電文にて結果が返却される為、上記の方法では結果が確認できません。

5-2 テスト実施にあたっての注意事項

Web リンクサーバーのテストを実施する際のテスト仕様につきましては、別紙「テスト導入テストガイド」をご参照ください。
以下にテスト実施の際の主な注意事項を記載します。

✧ テスト取引を行う場合は「ダミー取引フラグ」を必ず ″1″ に設定してください。
「4-2 暗号鍵取得」の「⑤要求電文 ： EC サイト → Web リンクサーバー」にて「DUMMY_PAYMENT_FLAG（ダミー取引フラグ）」を「″1″:ダミー取引」に設定してください。

✧ テスト取引を行うには決まった設定条件（所定のカード番号、所定の決済金額など）が必要です。
テスト時の設定条件につきましては、別紙「導入テストガイド」をご参照ください。

✧ 取引テスト時には、下記の事項に注意してください。
- 取引 ID（orderId）：任意に設定してください。重複しないように設定する必要があります。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。
- 金額：有効な金額データをセットしてください。（小数点の入った数値は使用できません）
- ダミー取引に対する本番リクエスト、本番取引に対するダミーリクエストはエラーとなります。

✧ 「お支払い方法選択（クレジットカード決済）」画面の「カード有効期限」の「年(西暦下 2 桁)」選択肢について
「お支払い方法選択（クレジットカード決済）」画面の「カード有効期限」の選択肢について、ダミーモードの場合は、異常系のテスト用に「年(西暦下 2 桁)」の値で「90」～「99」が表示されます。



図 5-2-1 「お支払い方法選択」画面の「カード有効期限」の選択肢について

※ダミーモードでは、異常系のテストのために「カード有効期限」の値により特定のエラーコードを返戻します。詳細は、別紙「導入テストガイド」をご参照ください。

※本番取引では、「年(西暦下 2 桁)」の値は、「現在の年-1 年」から「現在の年を含む未来 15 年」までが選択肢として表示されます。

例）現在：2016 年

→選択肢は(20)15 年から(20)30 年が表示されます。

5-3 クレジットカード決済 仕向け先カード会社の一覧

カード会社コード	社名
01	三井住友トラストクラブ(株)
02	(株)ジェーシービー
03	三菱 UFJ ニコス(株) (DC カード)
04	三井住友カード(株)
05	三菱 UFJ ニコス(株) (UFJ カード)
06	ユーシーカード(株)
07	アメリカンエキスプレスインターナショナル
08	(株)ジャックス
09	三菱 UFJ ニコス(株)(日本信販)
10	(株)オリエントコーポレーション
12	(株)アプラス
13	ライフカード (株)
14	楽天カード(株)
21	(株)クレディセゾン
22	ポケットカード(株)
23	三井住友カード(株) (OMC)
24	イオンフィナンシャルサービス(株)
31	トヨタファイナンス(株)
33	全日信販(株)
34	山陰信販(株)
38	東急カード(株)
40	(株)UCS
41	(株)エスコートカード
42	(協) エヌシー日商連
43	九州日本信販(株)
44	ライフカード(株) (すみしんライフ)
45	(株)ニッセンレンライフ
50	(株)ゆめカード
51	(株)オークス
52	(株)ビューカード
53	イズミヤカード(株)
56	(株)エポスカード
57	天満屋カードサービス(株)
58	(株)京王パスポートクラブ

59	(株)オーシー
60	(株)エヌシーガイドショップ
61	(株)エヌケーシー
62	JFR カード(株)
64	三井住友カード(株) (MCP)
65	三菱 UFJ ニコス(株) (MCP)
67	三井住友カード(株) (銀聯)
68	トヨタファイナンス(株) (銀聯)
69	(株)ジェーシービー(銀聯)
70	Pay Pay カード(株)
71	(株)USEN FinTech (ACQ)
72	(株)ジャックス (ACQ)
73	(株)日専連
74	(株)りそな銀行
75	(株)エムアイカード
76	SB ペイメントサービス(株)
77	(株)東武カードビジネス
78	(株)ニッセンレンエスコート
79	(協組)日専連札幌
83	(株)ジェーシービー(プレモ)
84	三菱 UFJ ニコス(株)(銀聯)
85	三菱 UFJ ニコス(株) (DCC)
90	(株)日専連釧路
91	(株)日専連旭川
92	(株)日専連ベネフル
93	(株)NTT ドコモ
99	ダミーテストカード会社
1A	(株)日専連ライフサービス
1B	(株)琉球銀行
2A	(株)日専連静岡
2B	(株)埼玉りそな銀行
3A	(株)日専連ファイナンス
3B	(株)北國銀行
4A	(株)モデル百貨
4B	au フィナンシャルサービス(株)
5A	シティックスカード(株)
5B	au フィナンシャルサービス(株) (ONUS)
6A	モデルクレジット(株)
6B	(株)静岡銀行
7A	(株)宮崎信販

7B	(株)セブンカードサービス
8A	(株)千葉銀行
8B	三井住友カード(株)(提携)
9A	(株)いよてつカードサービス

※上記一覧は **2026 年 10 月現在**のものです。

5-4 他ソフトウェア等の影響

iOS をご利用かつ Microsoft Edge ブラウザをご利用で、Microsoft Defender を有効にしていますと、RA22 のエラーが発生することが分かっております(2024 年 7 月時点)。RA22 のエラーが発生する場合は、Microsoft Defender を無効にしていただくか、Microsoft Edge 以外のブラウザを使用していただくようお客様にお伝えください。