コード決済に関する統一技術仕様ガイドライン

【店舗提示型】

MPM(Merchant-Presented Mode)

一般社団法人キャッシュレス推進協議会

Ver.1.1

2019 年 10 月 31 日

【履歴】

2019 年 3 月 29 日　新規制定（Ver. 1.0）

2019 年 10 月 31 日　第 1 部 6.5 を追加、従前の 6.5 を 6.6 に繰り下げ、第 2 部 6.4 を追加、従前の 6.4 を 6.5 に繰り下げ、別紙 1（第 1 部及び第 2 部共通）を追加等（Ver. 1.1）

目次

【用語集】

本ガイドラインにおける用語は以下の通りの意味を有する。

用語	定義
アクワイアラ	契約店と契約を締結の上、契約店がコード決済を取り扱えるようにする事業者
協議会	一般社団法人キャッシュレス推進協議会
協議会事務局	一般社団法人キャッシュレス推進協議会の事務局
契約店	コード決済事業者やアクワイアラ等との契約に基づき、自己の商品・サービス等の対価を利用者からコード決済にて支払いをうける者
ゲートウェイ事業者	契約店とコード決済事業者の間で、契約店からのコード決済情報をコード決済事業者へと仕向けを行う事業者
コード決済	バーコード又は QR コード®[1]を用いたキャッシュレス決済。ただし、店舗提示型においてはバーコードの利用は想定されていない。
コード決済アプリ	コード決済を行うことを目的とした、利用者又は契約店用アプリケーション
コード決済関連事業者	コード決済事業者、コード決済アプリ開発者、アクワイアラ、契約店への処理端末提供者、ゲートウェイ事業者等コード決済に関係する幅広い事業者
コード決済事業者	コード決済を利用者及び契約店に提供する事業者
事業者識別コード	統一 QRコードを用いたコード決済において使用される、8 桁の数字で構成される各コード決済サービス固有の番号
静的 QR コード	あらかじめ印刷等の上契約店に設置され、繰り返し決済に利用される固定のコード決済用の QR コード
接続 API	システム間のデータ送受信に関してあらかじめ定められたルールであり、当該ルールに沿って外部機能を呼び出し、データ連携する。なお、API とは、Application Programming Interface の略称である。
店舗提示型 [MPM]	決済に際し、契約店にあらかじめ設置されている QR コード又は契約店側の動的 QR コード表示端末に表示さ

[1] QR コード®は、株式会社デンソーウェーブの登録商標である。

	れた QR コードを利用者が自己のスマートフォン等のモバイルデバイスで読み取る方式。MPM(Merchant-Presented Mode)とも言う。
統一静的 QR コード	本ガイドラインに定められた仕様に準拠した静的 QR コード
統一店舗識別コード	統一 QR コードを使用する際に用いられる 29 桁の数字で構成される各契約店固有の識別番号
統一動的 QR コード	本ガイドラインに定められた仕様に準拠した動的 QR コード
統一 QR コード	統一静的 QR コード及び統一動的 QR コードの総称
動的 QR コード	決済の都度、契約店側の動的 QR コード表示端末で生成されるコード決済用の QR コード
利用者	コード決済事業者の提供する利用規約等にあらかじめ同意した上で、自己が契約店から受けた商品・サービス等の対価をコード決済によって支払おうとする者
利用者提示型 [CPM]	決済に際し、利用者が自己のスマートフォン等のモバイルデバイスにバーコード又は QR コードを表示して契約店側の処理端末に読み取らせる方式。CPM(Consumer-Presented Mode)とも言う。
EMV 仕様(MPM)	EMVCo, LLC.が公表している「EMV® QR Code Specification for Payment Systems (EMV QRCPS) Merchant-Presented Mode」(Version 1.0, July 2017)及びこれに対するその後の修正版・改訂版において定められている QR コードの仕様(静的 QR コードと動的 QR コードの双方を含む。)
QR コード	コード決済用の二次元コード(二次元シンボル)。静的 QR コードと動的 QR コードの双方を含む。

はじめに

1　本ガイドラインの目的

キャッシュレス化は少子高齢化や人口減少に伴う労働者人口の減少の時代を迎えた現在、実店舗等の無人化・省力化や支払データの利活用による顧客のニーズに対応した経営を可能にするといった店舗側のメリットのみならず、現金準備の手間からの解放や家計の見える化による自己の消費動向の把握等利用者側のメリットも大きく、政府も「未来投資戦略 2018」においてキャッシュレス決済比率を 4 割程度とすることを目指すとしている。

スマートフォンの普及に伴い、コード決済は、従来のクレジットカード、デビットカード、プリペイドカード等に加えて、新しいキャッシュレス決済手段としてその活用及び発展が期待されるところである。一方で、各コード決済事業者が独自の仕様による QR コードを用いることとなる場合、契約店において、各コード決済事業者の QR コードにそれぞれ対応する必要に迫られるため、導入コストや従業員教育コストが増加するだけでなく、利用者においても乱立したQRコードによる混乱が生じることが懸念される。あるいは、契約店が加盟店契約を締結するコード決済事業者を限定する結果、利用者側の利便性が損なわれることも考えられる。こういった事態を回避し、コード決済の導入・普及を促進するためには、QRコードの乱立状態を解消・防止し、契約店及び利用者にとってわかりやすいコード決済手段の提供が不可欠であると考える。本ガイドラインは、コード決済のうち、店舗提示型にかかる QR コードの仕様を定め、コード決済に用いられる QR コードの統一化を図るものである。これにより、契約店及び利用者における混乱を抑止し、コード決済の迅速かつ円滑な普及を促すとともに、コード決済の社会的コストの低減に寄与することを目的とする。同時に、本ガイドラインはコード決済市場における自由な競争を阻害することがないよう、QRコードの統一化において一定の拡張性・柔軟性を確保することに留意している。

また、コード決済の普及及び活用には、契約店及び利用者にとって安心かつ安全な決済手段であることが必須の条件となる。コード決済関連事業者は安心かつ安全な決済手段を提供するよう常にセキュリティ対策の検討及び実施を行う必要がある。本ガイドラインにおいては、QR コードの仕様の統一化のみならず、コード決済におけるセキュリティ対策について、必須の対策から参考となる対策までレベルを分けて記載している。ただし、決済関連分野におけるテクノロジーの発展は著しいものがあり、各コード決済関連事業者は本ガイドライン記載のセキュリティ対策にのみとらわれることなく、常に自己のセキュリティ対策を向上させてもらいたい。なお、本ガイドラインに記載されるセキュリティ対策以外にも協議会、関係省庁、関係団体等がセキュリテ

ィ対策に関する指針やガイドラインを策定している場合があり、各コード決済関連事業者はこれらも参照されたい。

なお、本ガイドラインは、コード決済事業者、ゲートウェイ事業者、アクワイアラ、流通事業者、関係団体、専門家等の幅広い会員を有する協議会における検討及び2019 年 3 月 21 日から 26 日まで実施されたパブリックコメントの結果を踏まえて作成されたものであり、本ガイドラインに基づいた統一 QR コードの活用により、さらなるコード決済の普及及び活用を期待するものである。

2 本ガイドラインの適用範囲・注意事項

- 本ガイドラインは、コード決済のうち、店舗提示型にかかる QR コードの統一仕様を定めるものであるが、統一 QR コードを利用しない場合においても、参考となるべき記載事項（セキュリティ等）が含まれる。なお、第 1 部において静的 QR コードについて、第 2 部において動的 QR コードについての仕様等を定めている。それぞれに共通する項目については各部において重複して記載しているが、表題部に「【共通】」と記載することによって容易に識別が可能なようにしてある。利用者提示型にかかるバーコード及び QR コードの統一仕様等については、協議会が別途定める「コード決済に関する統一技術仕様ガイドライン【利用者提示型】 CPM(Consumer-Presented Mode)」を参照されたい。
- 本ガイドラインは、幅広くコード決済関連事業者を対象とするものである。
- 本ガイドラインは強制力を持つものではないが、「1.1　本ガイドラインの目的」に記載のとおり、本ガイドラインはコード決済の発展のために、コード決済に関係する幅広い関係者による検討及びパブリックコメントを踏まえて作成されたものであり、本ガイドラインの目的達成のためにもコード決済関連事業者は本ガイドラインを遵守されたい。既に各コード決済関連事業者によって展開されている各事業者独自の QR コードから統一 QR コードへの移行には、現在のシステムの変更、統一店舗識別コードの発番作業、店頭に設置されている QR コードの貼り換え作業等、様々な移行手続きを要するものであり、本ガイドラインはコード決済関連事業者に対して統一 QR コードへの移行をただちに求めるものではないが、本ガイドライン目的の達成のためにも、各 QR コード関連決済事業者には統一 QR コードへの移行に関してご協力を願いたい。なお、インバウンドにおけるキャッシュレス需要に対応することは重要であり、本ガイドラインにおける統一 QR コードは海外のコード決済事業者等の統一店舗識別コードを利用しないコード決済事業者にも利用可能な仕様としているため、海外のコード決済事業者等にも統一 QR コードの積極的な利用を期待する。
- 本ガイドラインは、各コード決済関連事業者が協調できる領域について共通事

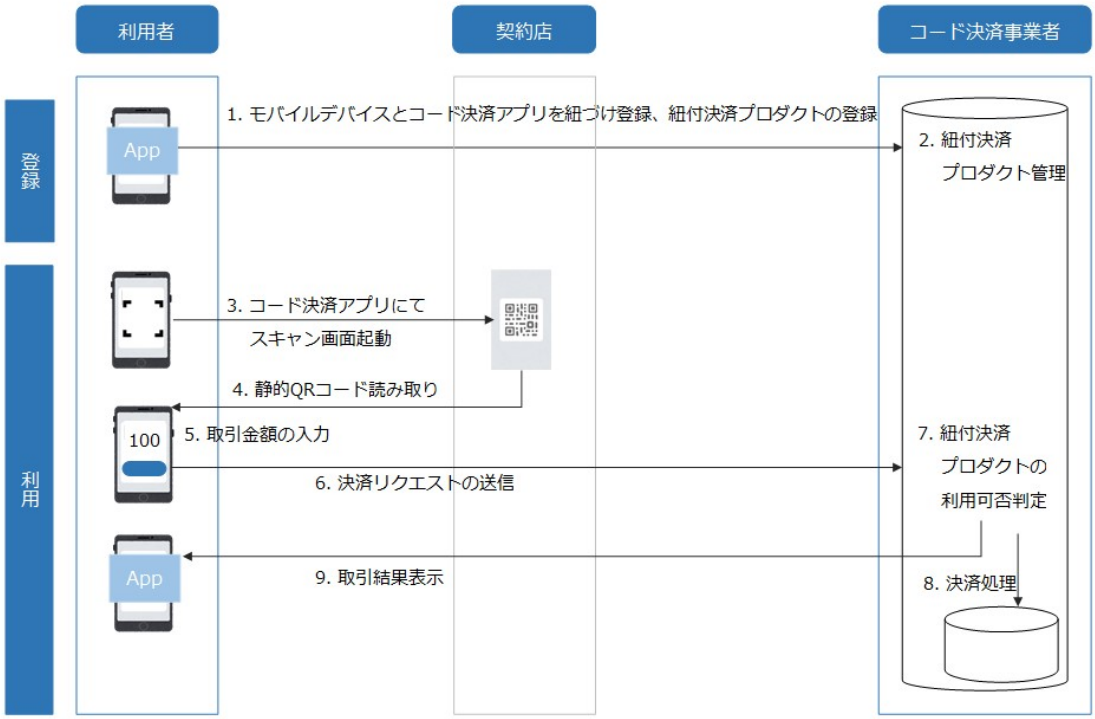
項を定めるものであり、協調領域以外の領域における自由な競争を否定するものではない。

- **本ガイドラインは、QR コードの統一化に関連する事項を記載するものであり、本ガイドラインの遵守により、決済事業に適用のある関連法令の適合性を保証するものではない。各コード決済関連事業者は、自己の責任と負担において関連法令を調査し、これらを遵守しなければならない。また、本ガイドラインの遵守により安全かつ欠陥のない決済システムを構築できることを保証するものでもない。**
- **協議会は、本ガイドラインに含まれるすべての事項につき、明示的であれ非明示的であれ、商品適格性、特定の目的への適合性、第三者の権利（特許権を含むがこれに限らない。）の非侵害性、その他一切の事項について、いかなる表明も保証も行わない。本ガイドラインを利用する者は、自己の責任と負担において本ガイドラインを利用するものとし、協議会は本ガイドラインの利用によりコード決済関連事業者、契約店、利用者、その他第三者に生じた損害・損失・負担等の一切の結果についていかなる責任も負わず、本ガイドラインを利用する者は協議会に対していかなる責任の追及も行わないものとする。**

第 1 部　静的 QR コード

1　全体フロー

静的 QR コードを利用した店舗提示型のコード決済における基本的なデータ処理のフローは以下のとおりである。



※上記フローはあくまで基本的なフローであり、上記フロー以外のバリエーションも考えられる。

【図 1　静的 QR コードを利用した店舗提示型の基本的な全体フロー】

2　統一静的 QR コード仕様

2.1　データフォーマット

統一静的 QR コードのデータレイアウトは、EMV 仕様(MPM)に従い、かつ、EMV 仕様(MPM)に定められる以下の特定の項目については、以下のとおりのデータ編集を行うものとする。なお、本ガイドラインにおいては、EMV 仕様(MPM)に記載される仕様のうち、統一静的 QR コードの仕様として全コード決済事業者が共通して従うべきデータ編集項目だけを抽出して以下に記載しており、その他の QR コードへのデータの格納方法等の仕様については、各決済事業者が自己の責任において EMV 仕様(MPM)を確認し、これに準拠しなければならない。なお、統一静的 QR コードにおける EMV 仕様(MPM)への準拠は、EMV 仕様(MPM)に記載される QR コードの仕様以外の事項

について、クレジットカード決済等の決済方法の特定の仕様、システムをコード決済において採用することを意味するものではない。

下記表における「存在(Presence)」は統一静的 QR コードにおいて必須かどうかを意味し、EMV 仕様(MPM)における必須性を意味するものではない。なお、EMV 仕様(MPM)において「Mandatory(必須)」とされている事項については、統一静的 QR コードにおいても必須となる。なお、下記表にて「任意」とされているものについては、コード決済関連事業者は、協議会事務局に対し、入力したい内容を通知することによって統一静的 QR コードへの入力希望の申請をすることができる。この場合、協議会事務局は当該希望する内容、必要性等を踏まえ、当該任意項目への入力の可否及びその内容を決定するものとする。既に入力されている任意項目についての変更、追加等を希望する場合も同様とする。また、業種(ID52)、英数字の契約店名(ID59)、英数字の契約店所在地(ID60)、日本語の契約店情報(ID64)等の統一静的 QR コードに共通して入力する内容として特定の内容を決定する必要がある項目についても、協議会事務局がコード決済事業者及び契約店の希望を踏まえながら最終的な決定を行うものとする。既に決定した入力内容の変更・廃止・追加も同様とする。

【表 2.1-1 統一静的 QR コードの格納データ】

項目名 (Name)	ID	存在 (Presence)	内容
仕様バージョン (Payload Format Indicator)	“00”	**必須**	“000201”
静的/動的フラグ (Point of Initiation Method)	“01”	**必須**	“11”(静的 QR コードの場合)
契約店情報 (Merchant Account Information)	“26” – “51”	**必須**	“xx680019jp.or.paymentsjapan0113aaaaaaaaaaaa0204bbbb0306cccccc0406dddddd”(2 桁の x には ID 番号が(ID26 の場合は 26)、13 桁の a には統一店舗識別コードの管理レベル 1 が、4 桁の b には統一店舗識別コードの管理レベル 2 が、6 桁の c には統一店舗識別コードの管理レベル 3 が、6 桁の d には統一店舗識別コードの管理レベル 4 がそれぞれ入る。)

			空いている領域のうち、もっとも若い ID 番号の領域にデータを格納する（具体的な領域は協議会事務局が指定）。 その他の領域は、海外のコード決済事業者等統一店舗識別コードを利用しないコード決済事業者等のための領域となる。
業種 (Merchant Category Code)	“52”	**必須**	契約店の業種（ISO 18245 に従った分類）
取引通貨 (Transaction Currency)	“53”	**必須**	通貨コード（円 “392”）
取引金額 (Transaction Amount)	“54”	任意	取引金額（チップ除く）
国コード (Country Code)	“58”	**必須**	国コード（日本 “JP”）
契約店名 (Merchant Name)	“59”	**必須**	英字表記による契約店名
契約店所在地 (Merchant City)	“60”	**必須**	英字表記による契約店所在地
契約店郵便番号 (Postal Code)	“61”	**必須**	契約店所在地の郵便番号
契約店情報（日本語） (Merchant Information–Language Template)	“64”	**必須**	日本語による契約店に関する情報
チェックディジット (Cyclic Redundancy Check (CRC))	“63”	**必須**	チェックディジット

※括弧内の英字表記は EMV 仕様(MPM)【EMV®QR Code Specification for Payment Systems (EMV QRCPS) Merchant-Presented Mode, Version 1.0】における表記

【表 2.1-2　ID64 の格納データ】

項目名 (Name)	ID	存在 (Presence)	内容
使用言語 (Language Preference)	“00”	**必須**	“0002JA” Tag：　00（項目 ID）

			Length： 02 Value： JA (ISO639 上の日本語の言語コード)
契約店名(日本語) (Merchant Name-Alternate Language)	“01”	**必須**	契約店ごとに協議会事務局が決定 文字コードは UTF-8 <例> 契約店名が「キャッシュレス推進協議会」の場合： “0112 キャッシュレス推進協議会” Tag： 01 (項目 ID) Length： 12 (契約店名の長さ) Value： キャッシュレス推進協議会

※括弧内の英字表記は EMV 仕様(MPM)【EMV®QR Code Specification for Payment Systems (EMV QRCPS) Merchant-Presented Mode, Version 1.0】における表記

契約店情報(Merchant Account Information)として統一店舗識別コード等が入力される領域は ID26 から ID51 の領域のうち、最初に契約店に対して統一店舗識別コードが発行された時点で使用可能な領域のうちもっとも若い ID 番号の領域とする。したがって、例えば、ある契約店に対し統一店舗識別コードが発行された時点で、当該契約店が統一静的 QR コード以外の EMV 仕様(MPM)に従った QR コードを使用していない場合には ID26 に統一店舗識別コード等が記載されることになるが、既に当該契約店が統一静的 QR コード以外の EMV 仕様(MPM)に従った QR コードを使用し、ID26 に特定のコード決済事業者の契約店を識別するための符号が記載されている場合には、統一店舗識別コード等は ID27 に記載されることになる。

また、海外のコード決済事業者等統一店舗識別コードを利用しないコード決済事業者は、ID26 から ID51 の間のうち、統一店舗識別コード等の入力及びそれ以外のコード決済事業者に利用されていない領域のいずれかを自己の領域として使用することになる。かかる割振りは、海外のコード決済事業者等用の領域の有限性に鑑みて、海外のコード決済事業者等の申請に基づき、当該コード決済の利用者数、主に利用されている国等様々な要素を総合考慮して協議会事務局が決定するものとする。また、割振りを受けた当該海外のコード決済事業者等統一店舗識別コードを利用しないコード決済事業者は、協議会事務局に対して、当該割振りを受けた領域に記載したい事項を申請しなければならない。ただし、当該記載内容の最終的な決定権限は、統一静的 QR コードに記載できるデータ容量の有限性から、協議会事務局に留保される。

ID02 から ID25 の領域については、EMV 仕様(MPM)において特定の決済事業者に

留保されている。この領域を使用する権限を EMV 仕様(MPM)において与えられている決済事業者が統一静的 QR コードを利用したいと思う場合、自己が使用する領域と当該領域に記載したい内容について協議会事務局に申請するものとする。ただし、統一静的 QR コードに記載できるデータ容量の有限性から、かかる記載を統一静的 QR コードに認めるかどうかの権限は協議会事務局に留保される。

なお、海外のコード決済事業者等又は EMV 仕様(MPM)において自己の領域を割振られている決済事業者は、統一店舗識別コードを利用することも可能である。この場合、これらのコード決済事業者又は決済事業者は、統一店舗識別コードの発番申請、事業者識別コードの取得等本ガイドラインに記載される統一店舗識別コードを利用した統一静的 QR コードを使用するために必要なすべての手続きを行わなければならない。

本「2.1 データフォーマット」において協議会事務局に決定権限が留保されている場合、協議会事務局は当該権限が留保されている趣旨を踏まえて公平かつ公正に当該権限を行使せねばならず、特定のコード決済事業者に恣意的に損害を与える目的等不当な目的で権限を行使してはならない。なお、統一静的 QR コードのデータ容量は EMV 仕様(MPM)に従い 512byte を上限とするが、協議会事務局は統一静的 QR コードに格納されるデータの容量が読み取り速度に影響することを考慮して、格納するデータを決定するものとする。

2.2 表示要件

統一静的 QR コード（その周辺部及びアクセプタンスマークを含む。以下本「2.2 表示要件」において同じ。）は別途協議会が定めるデザインとする。統一静的 QR コードの最小セルサイズは 1 セルあたり 0.33 ㎜以上で印刷されなければならない。ただし、読み取り精度の向上の観点から、1 セルあたり 0.5 ㎜以上での印刷を推奨する。また、印刷するにあたっては、1 セルあたり 4dot 以上で印刷されなければならない。統一静的 QR コードに表示されるアクセプタンスマークはコード決済サービスの名称の五十音順に並べられるものとする。

各コード決済関連事業者は独自のデザインの追加・一部のデザインの変更等の加工・修正・変更等を一切行ってはならず、契約店に対しこれらを行ってはいけない旨を明確に通知しなければならない。さらに、契約店がかかる加工・修正・変更等を行っていることを認識した場合は、直ちに当該行為を中止させ、本来の統一静的 QR コードを利用するよう指導しなければならない。本「2.2 表示要件」における規定は、統一静的 QR コードへの加工・修正・変更等を行う以外の方法で、契約店において特定のコード決済事業者を利用することができる旨の表示、宣伝等を禁止するものではない。ただし、コード決済事業者は当該表示・宣伝等において、統一静的 QR コードが

自己や特定のコード決済事業者のためのものだけの QR コードであるかのような表示を行ったり、自己が統一静的 QR コードを管理運営する主体であるかのような表示を行ったりする等、統一静的 QR コードの公平性や信頼を損なうような表示を行ってはならない。

2.3 検証 【共通】

コード決済事業者は統一 QR コードを読み取ることが想定される利用者のモバイルデバイス及び契約店側で利用することが想定される統一 QR コードを用いて、統一 QR コードの読み取りが可能であることを検証する等、コード決済サービス開始時及びコード決済アプリのアップデート時には、円滑なコード決済を提供するための品質保証対策を講じなければならない。

3 統一店舗識別コード 【共通】

3.1 総則

統一店舗識別コードは、統一 QR コードを用いた決済を行う際に、各契約店を識別するために使用する。統一 QR コードを使用してコード決済サービスを提供する場合、コード決済事業者は統一店舗識別コードを契約店のために取得しなければならない。

3.2 統一店舗識別コードの取得

統一店舗識別コードは 29 桁の数字で構成される各契約店固有の番号とする。統一店舗識別コードは協議会事務局から発番されるものとする。各コード決済関連事業者は、新たに契約店と契約を締結した場合には、当該契約店の商号（屋号）、住所等協議会事務局が指定する情報を協議会事務局に提供して発番申請を行い、統一店舗識別コードの発番を受けるものとする。既に当該契約店が他のコード決済関連事業者と契約を締結している場合等、既に当該契約店が統一店舗識別コードを保有している場合であっても、新たに契約店と契約を締結したコード決済関連事業者は、協議会事務局に対して発番申請を行わなければならない。この場合、当該コード決済関連事業者は当該契約店から既に当該契約店に対して発番されている統一店舗識別コードを確認した上で、当該発番済み統一店舗識別コードの情報と共に協議会事務局に対して発番申請を行うものとする。ただし、この場合、新しい管理レベルの追加、従前の管理レベルの詳細化（例えば、従前はテーブル番号 3 までの登録がされ

ており、これをテーブル番号 10 までに拡張する場合）等が行われた場合を除き、新しい統一店舗識別コードは発番されない。なお、統一店舗識別コードの発番申請にあたっては、コード決済事業者は事業者識別コードを取得している必要がある。事業者識別コードについては、「4.　事業者識別コード」を参照されたい。

統一店舗識別コードは、下記表のとおり、4 つの階層（管理レベル 1 乃至 4）で管理される。管理レベル 1 は 13 桁、管理レベル 2 は 4 桁、管理レベル 3 は 6 桁、管理レベル 4 は 6 桁で構成される（全 29 桁）。統一店舗識別コードの発番にあたっては、最低限管理レベル 1 の登録を行う必要があるが、その他の下位階層については必ずしも登録を要するものではない。この場合、登録されていない各階層にはすべて 0 が割り振られる。コード決済関連事業者は、統一店舗識別コードの取得にあたっては契約店の要望を把握し、必要な階層数を、各階層にどのような内容を登録したいかの希望を添えて協議会事務局に発番申請しなければならない。なお、下記表における各管理レベルの名称は一例であり、必ずしも名称に従った情報の登録が義務付けられる訳ではない（例えば、ショッピングモールを複数運営する事業者の場合、管理レベル 2 に各ショッピングモールを、管理レベル 3 にショッピングモール内の契約店を登録することも可能である。）。ただし、各階層に何を登録するかについては、契約店及びコード決済関連事業者の希望、従前の登録状況等を総合考慮した上で、協議会事務局が決定権を有する。新しい管理レベルの追加、従前の管理レベルの詳細化、従前使用していた管理レベルの廃止等統一店舗識別コードの追加発行、変更等を希望する場合についても、コード決済事業者が協議会事務局に対して申請を行うものとする。本ガイドラインに記載される事項のほか、統一店舗識別コードの発番、変更等に関する具体的な基準・諸手続き等は、協議会事務局の指示に従うものとする。

【表 3.2　統一店舗識別コードの管理レベル】

管理レベル	桁数	名称	想定される管理単位	例
1	13 桁	法人	利用契約を締結する主体	○○株式会社
2	4 桁	ブランド	ブランド/法人内区分	○○屋
3	6 桁	契約店	契約店名	新橋 1 号店
4	6 桁	端末/ステッカー	動的：動的 QR コード表示端末等 静的：ステッカー等	3 番テーブル

4　事業者識別コード【共通】

4.1　総則

事業者識別コードは、統一 QR コードを用いた決済を行う際に、各コード決済サービスを識別するために使用され、特に店舗提示型においては、正確なアクセプタンスマークを統一 QR コード及び/又は契約店に表示するために、統一店舗識別コードと共に、どの契約店がどのコード決済サービスと契約しているかを協議会事務局で管理するために用いられる。統一 QR コードを使用してコード決済サービスを提供する場合、コード決済事業者は事業者識別コードを取得しなければならない。

4.2　事業者識別コードの取得

事業者識別コードは 8 桁の数字で構成される各コード決済サービス固有の番号とする。なお、利用者提示型と店舗提示型における事業者識別コードは共通である。ただし、協議会事務局が必要と認めた場合、利用者提示型と店舗提示型とで異なる事業者識別コードが発番されることがある。

事業者識別コードは協議会事務局に発番申請をすることによって協議会事務局から発番されるものとする。ただし、コード決済事業者は、協議会事務局が発番した事業者識別コード以外の 8 桁の数字を、協議会事務局の承諾を得た上で自己のコード決済サービスの事業者識別コードとして使用することができる。この場合、コード決済事業者は当該番号の登録が協議会事務局において完了するまでは、当該番号を自己のコード決済サービスの事業者識別コードとして使用することはできない。

コード決済事業者は、協議会事務局から発番された又は協議会事務局にて承認・登録された事業者識別コード以外のいかなる識別記号も、形式の如何を問わず、統一 QR コードにおける事業者識別コードとして使用することはできない。事業者識別コードの発番、登録、変更等に関する具体的な基準・諸手続き等は、協議会事務局の指示に従うものとする。

5　契約店との接続等

5.1　契約店への統一静的 QR コードの設置

統一静的 QR コードを利用したコード決済を行うためには、契約店に印刷された統一静的 QR コードが設置されていなければならない。契約店に設置される統一静的

QR コードは「2.2　表示要件」記載の要件を満たすものである必要がある。統一静的 QR コードのステッカー印刷、契約店への配布等の統一静的 QR コードを設置するために必要となる事項の詳細については、協議会にて別途定めるものとする。

5.2　QR コードの特性の説明

静的 QR コードを用いた店舗提示型によるコード決済は、あらかじめ印刷されたステッカー等で QR コードが提示され、それを利用者のモバイルデバイス等で読み取って決済を行うものであり、従来の現金決済、クレジットカード等のカード決済、非接触決済等にはない特性が存在する。コード決済事業者は、円滑なコード決済の促進のため、コード決済の特性に留意した上で、契約店に対しその対応を説明（各種マニュアル・注意文書の配布等を含む。）する必要があることに注意を要する。なお、下記は、静的 QR コードの読み取りの可否に影響する事象の一例である。

【表 5.2　静的 QR コード読み取りの可否に影響する事象の例】

◆　ステッカー等にフィルムが貼られている。
◆　ステッカー等に貼られているフィルムに気泡がある。
◆　ステッカー等に汚損がある。
◆　ステッカー等の印刷にヨレや不鮮明な部分がある。
◆　ステッカー等が設置されている場所が暗い（光量が不足している。）。
◆　ステッカー等が照明を反射している。

静的 QR コードのヨレ、汚損、不鮮明な印刷等は、当該静的 QR コードの読み取り不可や誤った決済情報の読み取りを生じ、決済不能や意図しない決済を引き起こす可能性がある。したがって、静的 QR コードは常に良好な状態を保たなければならない。コード決済事業者は、契約店に対し、静的 QR コードを常に良好な状態に保つ必要性を説明しなければならない。

6　セキュリティ

6.1　総論

コード決済の普及及び活用には、契約店及び利用者にとって安心かつ安全な決済手段であることは必須の条件であり、安心かつ安全な決済手段の提供は、すべてのコード決済関連事業者が検討及び実施しなければならない事項である。本項目で

はコード決済において必須と思われるセキュリティ対策のほか、参考となるセキュリティ対策を例示的に記載しているが、本項目に記載されているセキュリティ対策を行うことで安全で欠陥のない決済システムを構築できることを保証するものではない。各コード決済関連事業者は決済関連分野におけるテクノロジーの発展が著しいことを踏まえ、自己の責任と負担において常に最新のセキュリティ情報を収集し、自己の決済システムに必要かつ十分なセキュリティを施す責務があることを常に意識しなければならない。なお、本ガイドラインに記載されるセキュリティ対策以外にも協議会、関係省庁、関係団体等がセキュリティ対策に関する指針やガイドラインを策定している場合があり、各コード決済関連事業者はこれらも参照されたい。なお、ギフトコード等譲渡を前提とするビジネスモデル、オフラインによるコード決済の提供等本項目記載のセキュリティ対策を講じることが事業上又は事実上困難な場合、当該コード決済事業者は、本項目で要求される各セキュリティ対策の趣旨を十分に理解した上で、利用者及び契約店を保護するために、本項目の各セキュリティ対策と同等相当の安全性を確保できる代替的なセキュリティ対策を講じなければならない。

コード決済における不正利用は様々な場面が考えられるが、以下は静的 QR コードを用いた店舗提示型によるコード決済において想定される不正利用の代表例である。

【表 6.1　想定される静的QRコードの不正利用例】

No.	起因箇所1	起因箇所2	想定事象	不正者	具体的な不正の例	対策方針
1	モバイルデバイス	-	紛失・盗難	第三者	第三者が利用者のモバイルデバイスを利用して決済する	本人認証の実施
2		-	意図的流出	利用者	利用者が第三者と結託して利用の覚えなしとして申告する	
3	オペレーション	-	詐欺	利用者	利用者が決済完了画面を偽造し加盟店に提示し代金支払を免れる	決済完了画面の表示仕様の策定、契約店への取引完了確認手段の提供、契約店への啓発
4		-	詐欺	第三者	ステッカー等を貼り換え・偽造により、代金を不正取得する	決済画面の表示仕様、契約店への取引完了確認手段の提供、契約店への啓発
5	システム	コード決済アプリ	ハッキング等	第三者	利用者のID等の抜き取り及び不正利用/利用者が意図しない決済の実行	システム設計時の脆弱性排除と監視体制強化
6		通信経路	ハッキング等	第三者	利用者のID等の抜き取り及び不正利用	
7		各サーバー	ハッキング等	第三者	同上/利用者のID等の不正生成/決済履歴の追加・改ざん	

6.2　本人認証 【共通】

(1)　総論

コード決済事業者においては、不正利用等を防止するためにコード決済を利用できる者を本人に限定するとともに、決済を行おうとする者が当該決済を行う権限がある者であること（多くの場合では、当該決済によって支払い義務を負う者と決済を行おうとしている者が同一であること。）を担保するために、本人認証を行うことが重要と考えられる。なお、関連法令において、利用者の氏名等特定の項目の確認がコード決済関連事業者に義務付けられている場合がある。かかる法令が自己に適用があるか否かについては各コード決済関連事業者が自己の責任において確認する必要がある。また、かかる法令においては、本人確認義務以外の義務がコード決済関連事業者に課されている場合があることにも注意が必要である。

本人認証には大きく分けて(1)利用者が初めて当該決済手段を利用する際に当該利用者を限定する目的で行われる本人認証（基礎認証）と(2)決済を行おうとする際に決済を行おうとしている者が事前に登録されている利用者と一致するかを確認する目的で行われる本人認証（利用時認証）がある。本人認証のあり方においては、これらの組み合わせにより様々なパターンが考えられるが、事業者は想定される不正利用を防止するために、適切な本人認証プロセスを設けなければならない。

(2) 基礎認証

コード決済事業者は、第三者によるコード決済アプリ ID やパスワードの不正取得による不正利用を防止するために、利用者のモバイルデバイスとコード決済アプリを紐づけ管理しなければならない。また、基礎認証にあたっては、利用者を特定するために必要な情報の受領・確認を行うことも考えられる。同時に、コード決済アプリにクレジットカード、デビットカード、銀行口座等の支払手段を登録しようとしている利用者が、当該支払手段の利用に関し正当な権限を有する者であることを確認する等、不正利用を未然に防止するための対策を行うことも重要である。

(3) 利用時認証

利用時認証のタイミングについては、(1)利用者のモバイルデバイスの立上げ時、(2)コード決済アプリの立上げ時、(3)決済時（QR コード読み取り時）等が考えられる。利用時認証の方法については、PIN の入力、指紋認証、顔認証等がある。利用者及び契約店に安心・安全なコード決済を提供するため、決済時（QR コード読み取り時）に本人認証を行うことが推奨される。利用時認証については、利用者のモバイルデバイスの機能及び設定に依存する場合があり、コード決済事業者がすべてをコントロ

ールできる訳ではない。また、各利用者、各契約店によって、希望するセキュリティレベルは大きく異なる場合もあり、本人認証スキームの構築にあたっては、不正防止の観点はもちろんのこと、利用者のモバイルデバイスの種類、利用状況、契約店における決済オペレーションの負荷、利用者及び契約店のニーズ等様々な事項を考慮し、慎重に判断していく必要がある。各利用者、各契約店のニーズに対応できるように、セキュリティレベルを各利用者、各契約店が選択できるようにするのも一つの方策である。

【表 6.2(3) 利用時認証組合せパターン】

組み合わせパターン	モバイルデバイス 立上げ時	コード決済アプリ 立上げ時	決済時
	○	○	○
	○	-	○
	○	○	-
	-	○	○
	○	-	-
	-	○	-
	-	-	○

※セキュリティ対策は、他のセキュリティ対策（本ガイドラインで言及されているか否かを問わない。）との組み合わせにより行うものであり、本人認証の頻度のみで当該決済システムの安全性を決められるものではない。

6.3 静的 QR コードの管理

静的 QR コードを用いたコード決済は、あらかじめ契約店が印刷の上設置した QR コードを用いて決済を行うため、当該設置されている静的 QR コードが不正に貼り換え、偽造等されれば、正常な決済が行われなくなる。また、同一の静的 QR コードを複数回利用することが想定されているため、ワンタイムトークン等による偽造防止策を行うことができない。そのため、契約店における印刷済みの静的 QR コードの適切な管理が不正利用防止のためには重要になってくる。コード決済事業者は、かかる静的 QR コードの不正な貼り換え、偽造等に対する必要な対策を行わなければならない。具体的には例えば、静的 QR コードを容易に複製することが難しいパネル・特殊な用紙等に印刷する、設置してある静的 QR コードの上に別の静的 QR コードが貼られていないか契約店に定期的に確認するよう指導する、定期的に契約店が自分で決済をしてみてその正当性を確認するよう指導する、といった手段が考えられる。

6.4　取引の管理

(1) 取引検証 【共通】

コード決済事業者は、不正利用を防止するとともに正常な取引を実行するために、以下の各場面において以下の表記載の各事項を検証しなければならない。

【表 6.4(1) 必要とされる取引検証】

取引依頼電文送信時	
1	スマートフォン用のコード決済アプリからの取引においては、あらかじめ紐づけられた利用者のモバイルデバイスから行われたものであること。
取引依頼電文検証時	
2	当該決済を行おうとしている利用者の会員ステータスが有効であること。
3	有効な QR コードの利用であること。

(2) 決済完了画面の表示

静的 QR コードを用いたコード決済では、原則的にはユーザーのモバイルデバイスに表示された決済完了画面を契約店が視認することによって決済の完了を確認する。当該決済完了画面が、以前に行われた決済画面のスクリーンショットや偽造・変造された画面等の不正な画面であった場合、契約店は決済が行われていないにもかかわらず、決済が行われたと誤認してしまう可能性がある。そのため、決済完了画面は容易に偽造等できるものであってはならない。コード決済事業者は、利用者がかかる決済完了を偽装する行為を防止でき、かつ、契約店が容易に決済の正当性を確認できるような決済完了画面を構築しなければならない。具体的には、決済画面にアニメーションやタイムスタンプを表示することや決済完了時に決済完了を知らせる音を出す等が考えられる。また、契約店に対し、決済完了画面の確認方法を周知することも大切である。

(3) 契約店への取引確認手段の提供

上記「6.4(2) 決済完了画面の表示」記載のとおり、決済完了画面の視認による決済完了の確認には、利用者による決済完了偽装の可能性が存在する。そのため、決済完了画面に偽装防止策を行うことに加えて、決済が行われた場合に契約店が決済完了したことを契約店側の端末やモバイルデバイスで確認できるようにすることが重要である。コード決済事業者は、契約店に対し、契約店が任意に決済完了情報を確認できる手段を提供しなければならない。なお、ここで要求されているのは、契約店側がオンライン環境下で決済完了の確認を希望したときに確認ができる状態の構築であり、契約店側がオフライン環境にある場合や決済時に契約店側の端末やモバイ

ルデバイスが手元にない場合が考えられることから、決済完了と同時に契約店側が決済完了した旨を実際に確認できることまでを要求するものではない。通知手段等については以下を推奨する。

【表 6.4(3) 推奨される取引情報提供手段等】

情報提供手段	Push 通知、email、SMS、契約店側コード決済アプリ上での表示等
情報提供時期	取引の成立後すみやかに
情報提供内容	日時、金額等

(4) 利用者への取引通知 【共通】

利用者のモバイルデバイスの盗難、契約店による不正操作又は偽造・変造されたQR コードを使った決済等による不正利用に対応するためには、速やかに利用者に対し、当該利用者の決済アカウントを用いて決済が行われたことを通知することが重要である。コード決済事業者は、決済の都度、利用者に決済が行われた旨を通知しなければならない。通知手段等については以下を推奨する。

【表 6.4(4) 推奨される取引完了通知の手段等】

通知手段	Push 通知、email、SMS、コード決済アプリ画面での表示等
通知時期	取引成立後すみやかに
通知内容	日時、金額、契約店名称等

(5) 事後的な不正利用検証 【共通】

将来における不正利用防止のためには、事前のセキュリティ対策のみならず、事後的な不正利用検証も重要である。かかる事後的検証を可能にするために必要となる利用者に関する情報、取引データ等を適切な期間保存することが推奨される。

6.5 システム間の情報連携におけるリスク検証の実施

決済システムは安全なシステムである必要があり、コード決済事業者は、コード決済サービスのリリース前、機能追加時等の適時のタイミングにおいて、自己のコード決済システム間の情報連携におけるリスク検証を行い、リスクの洗い出しを行うことが推奨される。ここでいう「システム」とは、連携する外部システムだけではなく、自己の内部システム同士で情報をやりとりする場合も含む。

かかるリスクをチェックする手段の一つとして、BCM 原則に基づいたチェックがあ

る。BCM 原則の内容とその検証方法の例は別紙 1 のとおりである。BCM 原則は、システム間の情報連携におけるリスクを洗い出すには非常に有用な原則である。かかるリスクチェックにおいては、第三者の目（第三者機関のみならず、当該決済システムの開発に関与していない自社内の開発者も含む。）で見ることも大切である。

コード決済事業者は、リスク検証の結果、脆弱性が発見された場合は、技術的対策、業務運用による対策等の必要な対策を検討・実施する必要がある。

6.6 その他 【共通】

上記各セキュリティ対策のほか、コード決済においてはシステム面及び体制面において以下のような各セキュリティ対策を検討することも考えられる。

【表 6.5 その他の考えられるセキュリティ対策】

＜システム面＞

No.	項目	内容（実装の手引き）
1	決済 ID 管理	利用者のモバイルデバイス上の決済 ID 保有は必要最低限の範囲内で設計する
2	アクセス権限	コード決済関連事業者における決済 ID 管理部分へのアクセス権限付与は、必要最低限の範囲とする
3	暗号鍵管理	高セキュリティ事項として厳重な管理方法を定める
4	コード決済アプリ開発	開発プロセスにおいて脆弱性がないセキュアコーディングを行う
5	通信暗号化	コード決済アプリとコード決済関連事業者サーバー間の通信プロトコルはセキュアなものを採用する
6	ネットワーク構成	ネットワーク構成の区分け及びファイヤーウォール設置等により不正アクセスのリスクを低減する
7	取引データ履歴	取消返品の店頭運用に支障を生じさせないように適切な期間、履歴を保存する（その他、決済に係る法令・会計の定めを考慮すること）

＜体制面＞

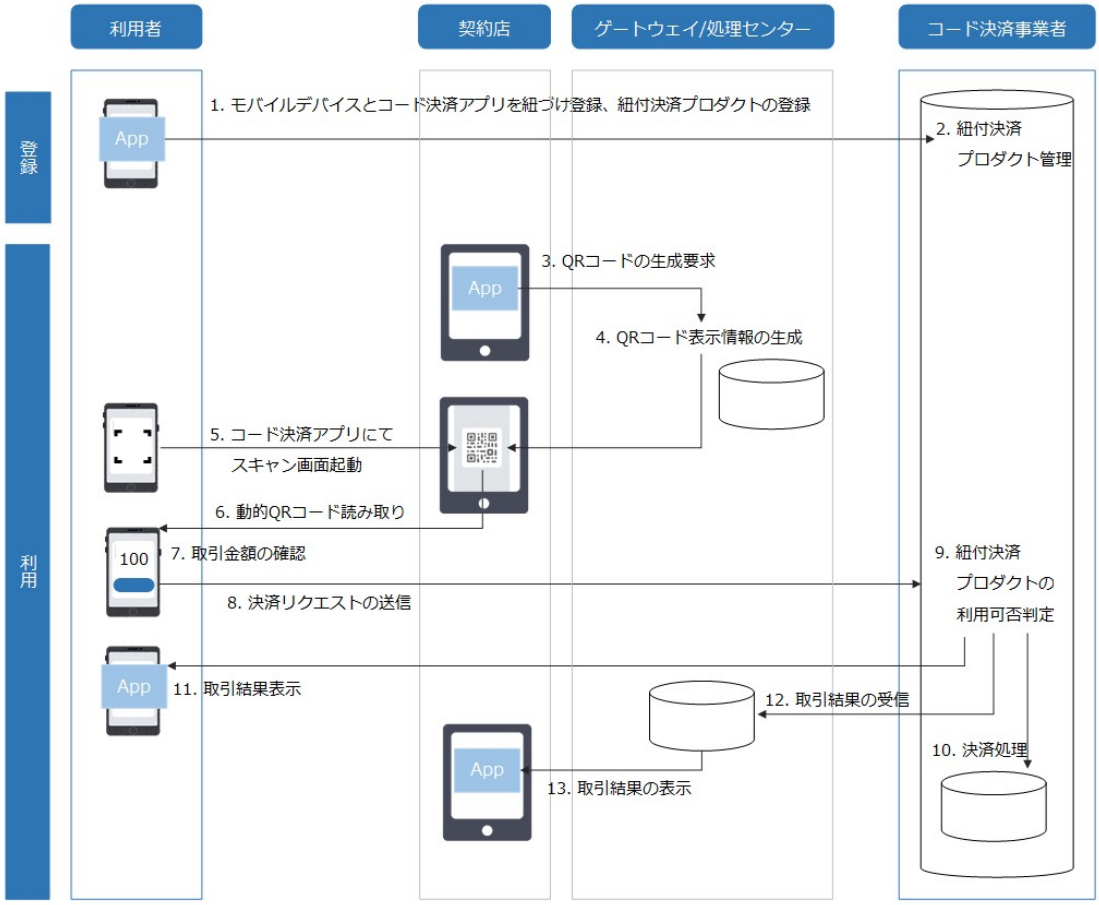
No.	項目	内容（実装の手引き）
1	不正利用の監視体制	不正利用検知を行う体制構築を行う（システム導

		入含む）
2	網羅的な検証	不正取引を検証し、新たな対策に活かす
3	取引ごとのリスクベース認証設定	対策の一つとして、利用者のステータス・利用状況等に応じたリスクベース認証を実施する

第 2 部　動的 QR コード

1　全体フロー

動的 QR コードを利用した店舗提示型のコード決済における基本的なデータ処理のフローは以下のとおりである。



※上記フローはあくまで基本的なフローであり、上記フロー以外のバリエーションも考えられる。

【図 1　動的 QR コードを利用した店舗提示型の基本的な全体フロー】

2　統一動的 QR コード仕様

2.1　データフォーマット

統一動的 QR コードのデータレイアウトは、EMV 仕様(MPM)に従い、かつ、EMV 仕様(MPM)に定められる以下の特定の項目については、以下のとおりのデータ編集を行うものとする。なお、本ガイドラインにおいては、EMV 仕様(MPM)に記載される仕様

のうち、統一動的 QR コードの仕様として全コード決済事業者が共通して従うべき特定のデータ編集項目だけを抽出して以下に記載しており、その他のデータ編集項目については、各決済事業者が自己の責任において EMV 仕様(MPM)を確認し、これに準拠しなければならない。なお、統一動的 QR コードにおける EMV 仕様(MPM)への準拠は、EMV 仕様(MPM)に記載される QR コードの仕様以外の事項について、クレジットカード決済等の決済方法の特定の仕様、システムをコード決済において採用することを意味するものではない。

下記表における「存在(Presence)」は統一動的 QR コードにおいて必須かどうかを意味し、EMV 仕様(MPM)における必須性を意味するものではない。なお、EMV 仕様(MPM)において「Mandatory(必須)」とされている事項については、統一動的 QR コードにおいても必須となる。なお、業種(ID52)、英数字の契約店名(ID59)、英数字の契約店所在地(ID60)、日本語の契約店情報(ID64)等の統一動的 QR コードに共通して入力する内容として特定の内容を決定する必要がある項目については、コード決済事業者及び契約店の希望を踏まえながら協議会事務局が最終的な決定を行うものとする。既に決定した入力内容の変更・廃止・追加も同様とする。なお、統一動的 QR コードに格納されるべきデータの具体的な内容の協議会事務局からコード決済事業者への共有方法等については、別途協議会が定めるものとする。

【表 2.1-1　統一動的 QR コードの格納データ】

項目名 (Name)	ID	存在 (Presence)	内容
仕様バージョン (Payload Format Indicator)	“00”	**必須**	“000201”
静的/動的フラグ (Point of Initiation Method)	“01”	**必須**	“12”(動的 QR コードの場合)
契約店情報 (Merchant Account Information)	“26” – “51”	**必須**	“xx680019jp.or.paymentsjapan0113aaaaaaaaaaaa0204bbbb0306cccccc0406dddddd”(2 桁の x には ID 番号が(ID26 の場合は 26)、 13 桁の a には統一店舗識別コードの管理レベル 1 が、4 桁の b には統一店舗識別コードの管理レベル 2 が、6 桁の c には統一店舗識別コードの管理レベル 3 が、6

			桁の d には統一店舗識別コードの管理レベル 4 がそれぞれ入る。） 空いている領域のうち、もっとも若い ID 番号の領域にデータを格納する（具体的な領域は協議会事務局が指定）。 その他の領域は、海外のコード決済事業者等統一店舗識別コードを利用しないコード決済事業者等のための領域となる。
業種 (Merchant Category Code)	“52”	**必須**	契約店の業種（ISO 18245 に従った分類）
取引通貨 (Transaction Currency)	“53”	**必須**	通貨コード（円 “392”）
取引金額 (Transaction Amount)	“54”	**必須**	取引金額（チップ除く）
国コード (Country Code)	“58”	**必須**	国コード（日本 “JP”）
契約店名 (Merchant Name)	“59”	**必須**	英字表記による契約店名
契約店所在地 (Merchant City)	“60”	**必須**	英字表記による契約店所在地
契約店郵便番号 (Postal Code)	“61”	**必須**	契約店所在地の郵便番号
契約店情報（日本語） (Merchant Information–Language Template)	“64”	**必須**	日本語による契約店に関する情報
チェックディジット (Cyclic Redundancy Check (CRC))	“63”	**必須**	チェックディジット

※括弧内の英字表記は EMV 仕様(MPM)【EMV®QR Code Specification for Payment Systems (EMV QRCPS) Merchant-Presented Mode, Version 1.0】における表記

【表 2.1-2　ID64 の格納データ】

項目名	ID	存在	内容

(Name)		(Presence)	
使用言語 (Language Preference)	“00”	**必須**	“0002JA” Tag： 00 (項目 ID) Length： 02 Value： JA (ISO639 上の日本語の言語コード)
契約店名(日本語) (Merchant Name-Alternate Language)	“01”	**必須**	契約店ごとに協議会事務局が決定 文字コードは UTF-8 <例> 契約店名が「キャッシュレス推進協議会」の場合： “0112 キャッシュレス推進協議会” Tag： 01 (項目 ID) Length： 12 (契約店名の長さ) Value： キャッシュレス推進協議会

※括弧内の英字表記は EMV 仕様(MPM)【EMV®QR Code Specification for Payment Systems (EMV QRCPS) Merchant-Presented Mode, Version 1.0】における表記

契約店情報(Merchant Account Information)として統一店舗識別コード等が入力される領域は ID26 から ID51 の領域のうち、最初に契約店に対して統一店舗識別コードが発行された時点で使用可能な領域のうちもっとも若い ID 番号の領域とする。したがって、例えば、ある契約店に対し統一店舗識別コードが発行された時点で、当該契約店が統一動的 QR コード以外の EMV 仕様(MPM)に従った QR コードを使用していない場合には ID26 に統一店舗識別コード等が記載されることになるが、既に当該契約店が統一動的 QR コード以外の EMV 仕様(MPM)に従った QR コードを使用し、ID26 に特定のコード決済事業者の契約店を識別するための符号が記載されている場合には、統一店舗識別コード等は ID27 に記載されることになる。

また、海外のコード決済事業者等統一店舗識別コードを利用しないコード決済事業者は、ID26 から ID51 の間のうち、統一店舗識別コード等の入力及びそれ以外のコード決済事業者に利用されていない領域のいずれかを自己の領域として使用することになる。かかる割振りは、海外のコード決済事業者等用の領域の有限性に鑑みて、海外のコード決済事業者等の申請に基づき、当該コード決済の利用者数、主に利用されている国等様々な要素を総合考慮して協議会事務局が決定するものとする。また、割振りを受けた当該海外のコード決済事業者等統一店舗識別コードを利用しないコード決済事業者は、協議会事務局に対して、当該割振りを受けた領域に記載したい事項を申請しなければならない。ただし、当該記載内容の最終的な決定権限は、

統一動的 QR コードに記載できるデータ容量の有限性から、協議会事務局に留保される。

ID02 から ID25 の領域については、EMV 仕様(MPM)において特定の決済事業者に留保されている。この領域を使用する権限を EMV 仕様(MPM)において与えられている決済事業者が統一動的 QR コードを利用したいと思う場合、自己が使用する領域と当該領域に記載したい内容について協議会事務局に申請するものとする。ただし、統一動的 QR コードに記載できるデータ容量の有限性から、かかる記載を統一動的 QR コードに認めるかどうかの権限は協議会事務局に留保される。

なお、海外のコード決済事業者等又は EMV 仕様(MPM)において自己の領域を割振られている決済事業者は、統一店舗識別コードを利用することも可能である。この場合、これらのコード決済事業者又は決済事業者は、統一店舗識別コードの発番申請、事業者識別コードの取得等本ガイドラインに記載される統一店舗識別コードを利用した統一動的 QR コードを使用するために必要なすべての手続きを行わなければならない。

本「2.1 データフォーマット」において協議会事務局に決定権限が留保されている場合、協議会事務局は当該権限が留保されている趣旨を踏まえて公平かつ公正に当該権限を行使せねばならず、特定のコード決済事業者に恣意的に損害を与える目的等不当な目的で権限を行使してはならない。なお、統一動的 QR コードのデータ容量は EMV 仕様(MPM)に従い 512byte を上限とするが、協議会事務局及び各コード決済事業者は統一動的 QR コードに格納されるデータの容量が読み取り速度に影響することを考慮して、格納するデータ量を決定しなければならない。

2.2 表示要件

統一動的 QR コード（その周辺部及びアクセプタンスマークを含む。以下本「2.2 表示要件」において同じ。）は別途協議会が定めるデザインとする。統一動的 QR コードの最小セルサイズは 1 セルあたり 0.33 ㎜相当以上で表示されなければならない。ただし、読み取り精度の向上の観点から、1 セルあたり 0.5 ㎜相当以上での表示を推奨する。統一動的 QR コードに表示されるアクセプタンスマークはコード決済サービスの名称の五十音順に並べられるものとする。

各コード決済関連事業者は独自のデザインの追加・一部のデザインの変更等の加工・修正・変更等を一切行ってはならない。ただし、コード決済事業者は、統一 QR コード表示端末（「5.1 動的 QR コード表示端末の設置」参照）の表示領域の限界等を理由に、別途協議会事務局が承認した場合は統一動的 QR コードのデザインの一部を表示しないことができる。なお、この場合であっても、統一動的 QR コードの QR コード部分に対し、自己のロゴ等を追加したり、アクセプタンスマークとして自己や特定の

コード決済事業者のマークのみを表示したりすることはできない。本「2.2　表示要件」における規定は、統一動的 QR コードへの加工・修正・変更等を行う以外の方法で、契約店において特定のコード決済事業者を利用することができる旨の表示、宣伝等を禁止するものではない。ただし、コード決済事業者は統一動的 QR コードが自己や特定のコード決済事業者のためのものだけの QR コードであるかのような表示を行ったり、自己が統一動的 QR コードを管理運営する主体であるかのような表示を行ったりする等、統一動的 QR コードの公平性や信頼を損なうような表示を行ってはならない。

2.3　画面輝度

統一動的 QR コードは、利用者のモバイルデバイスにて読み取るに際して十分な輝度で表示されなければならない。

2.4　検証 【共通】

コード決済事業者は統一 QR コードを読み取ることが想定される利用者のモバイルデバイス及び契約店側で利用することが想定される統一 QR コードを用いて、統一 QR コードの読み取りが可能であることを検証する等、コード決済サービス開始時及びコード決済アプリのアップデート時には、円滑なコード決済を提供するための品質保証対策を講じなければならない。

3　統一店舗識別コード 【共通】

3.1　総則

統一店舗識別コードは、統一 QR コードを用いた決済を行う際に、各契約店を識別するために使用する。統一 QR コードを使用してコード決済サービスを提供する場合、コード決済事業者は統一店舗識別コードを契約店のために取得しなければならない。

3.2　統一店舗識別コードの取得

統一店舗識別コードは 29 桁の数字で構成される各契約店固有の番号とする。統一店舗識別コードは協議会事務局から発番されるものとする。各コード決済関連事業者は、新たに契約店と契約を締結した場合には、当該契約店の商号（屋号）、住所等

協議会事務局が指定する情報を協議会事務局に提供して発番申請を行い、統一店舗識別コードの発番を受けるものとする。既に当該契約店が他のコード決済関連事業者と契約を締結している場合等、既に当該契約店が統一店舗識別コードを保有している場合であっても、新たに契約店と契約を締結したコード決済関連事業者は、協議会事務局に対して発番申請を行わなければならない。この場合、当該コード決済関連事業者は当該契約店から既に当該契約店に対して発番されている統一店舗識別コードを確認した上で、当該発番済み統一店舗識別コードの情報と共に協議会事務局に対して発番申請を行うものとする。ただし、この場合、新しい管理レベルの追加、従前の管理レベルの詳細化（例えば、従前はテーブル番号 3 までの登録がされており、これをテーブル番号 10 までに拡張する場合）等が行われた場合を除き、新しい統一店舗識別コードは発番されない。なお、統一店舗識別コードの発番申請にあたっては、コード決済事業者は事業者識別コードを取得している必要がある。事業者識別コードについては、「4.　事業者識別コード」を参照されたい。

統一店舗識別コードは、下記表のとおり、4 つの階層（管理レベル 1 乃至 4）で管理される。管理レベル 1 は 13 桁、管理レベル 2 は 4 桁、管理レベル 3 は 6 桁、管理レベル 4 は 6 桁で構成される（全 29 桁）。統一店舗識別コードの発番にあたっては、最低限管理レベル 1 の登録を行う必要があるが、その他の下位階層については必ずしも登録を要するものではない。この場合、登録されていない各階層にはすべて 0 が割り振られる。コード決済関連事業者は、統一店舗識別コードの取得にあたっては契約店の要望を把握し、必要な階層数を、各階層にどのような内容を登録したいかの希望を添えて協議会事務局に発番申請しなければならない。なお、下記表における各管理レベルの名称は一例であり、必ずしも名称に従った情報の登録が義務付けられる訳ではない（例えば、ショッピングモールを複数運営する事業者の場合、管理レベル 2 に各ショッピングモールを、管理レベル 3 にショッピングモール内の契約店を登録することも可能である。）。ただし、各階層に何を登録するかについては、契約店及びコード決済関連事業者の希望、従前の登録状況等を総合考慮した上で、協議会事務局が決定権を有する。新しい管理レベルの追加、従前の管理レベルの詳細化、従前使用していた管理レベルの廃止等統一店舗識別コードの追加発行、変更等を希望する場合についても、コード決済事業者が協議会事務局に対して申請を行うものとする。本ガイドラインに記載される事項のほか、統一店舗識別コードの発番、変更等に関する具体的な基準・諸手続き等は、協議会事務局の指示に従うものとする。

【表 3.2　統一店舗識別コードの管理レベル】

管理レベル	桁数	名称	想定される管理単位	例
1	13 桁	法人	利用契約を締結する主体	○○株式会社
2	4 桁	ブランド	ブランド/法人内区分	○○屋

3	6 桁	契約店	契約店名	新橋 1 号店
4	6 桁	端末/ステッカー	動的:動的 QR コード表示端末等 静的:ステッカー等	3 番テーブル

4 事業者識別コード【共通】

4.1 総則

事業者識別コードは、統一 QR コードを用いた決済を行う際に、各コード決済サービスを識別するために使用され、特に店舗提示型においては、正確なアクセプタンスマークを統一 QR コード及び/又は契約店に表示するために、統一店舗識別コードと共に、どの契約店がどのコード決済サービスと契約しているかを協議会事務局で管理するために用いられる。統一 QR コードを使用してコード決済サービスを提供する場合、コード決済事業者は事業者識別コードを取得しなければならない。

4.2 事業者識別コードの取得

事業者識別コードは 8 桁の数字で構成される各コード決済サービス固有の番号とする。なお、利用者提示型と店舗提示型における事業者識別コードは共通である。ただし、協議会事務局が必要と認めた場合、利用者提示型と店舗提示型とで異なる事業者識別コードが発番されることがある。

事業者識別コードは協議会事務局に発番申請をすることによって協議会事務局から発番されるものとする。ただし、コード決済事業者は、協議会事務局が発番した事業者識別コード以外の 8 桁の数字を、協議会事務局の承諾を得た上で自己のコード決済サービスの事業者識別コードとして使用することができる。この場合、コード決済事業者は当該番号の登録が協議会事務局において完了するまでは、当該番号を自己のコード決済サービスの事業者識別コードとして使用することはできない。

コード決済事業者は、協議会事務局から発番された又は協議会事務局にて承認・登録された事業者識別コード以外のいかなる識別記号も、形式の如何を問わず、統一 QR コードにおける事業者識別コードとして使用することはできない。事業者識別コードの発番、登録、変更等に関する具体的な基準・諸手続き等は、協議会事務局の指示に従うものとする。

5　契約店との接続等

5.1　動的 QR コード表示端末の設置

動的QRコードを用いた店舗提示型によるコード決済を可能にするためには、契約店に動的 QRコードを表示可能な動的 QRコード表示端末が設置されていなければならない。動的 QRコード表示端末には、動的 QRコード表示専用端末、タブレット端末、モバイルデバイス等が存在する。

5.2　動的 QR コードの特性の説明

動的 QR コードを用いた店舗提示型によるコード決済は、契約店の動的 QR コード表示端末に動的 QR コードが表示され、それを利用者が自己のモバイルデバイスで読み取って決済を行うものであり、従来の現金決済、クレジットカード等のカード決済、非接触決済等にはない特性が存在する。コード決済事業者は、円滑なコード決済の促進のため、コード決済の特性に留意した上で、契約店に対しその対応を説明（各種マニュアル・注意文書の配布等を含む。）する必要があることに注意を要する。なお、下記は、動的 QR コードの読み取りの可否に影響する事象の一例である。

【表 5.2　動的 QR コード読み取りの可否に影響する事象の例】

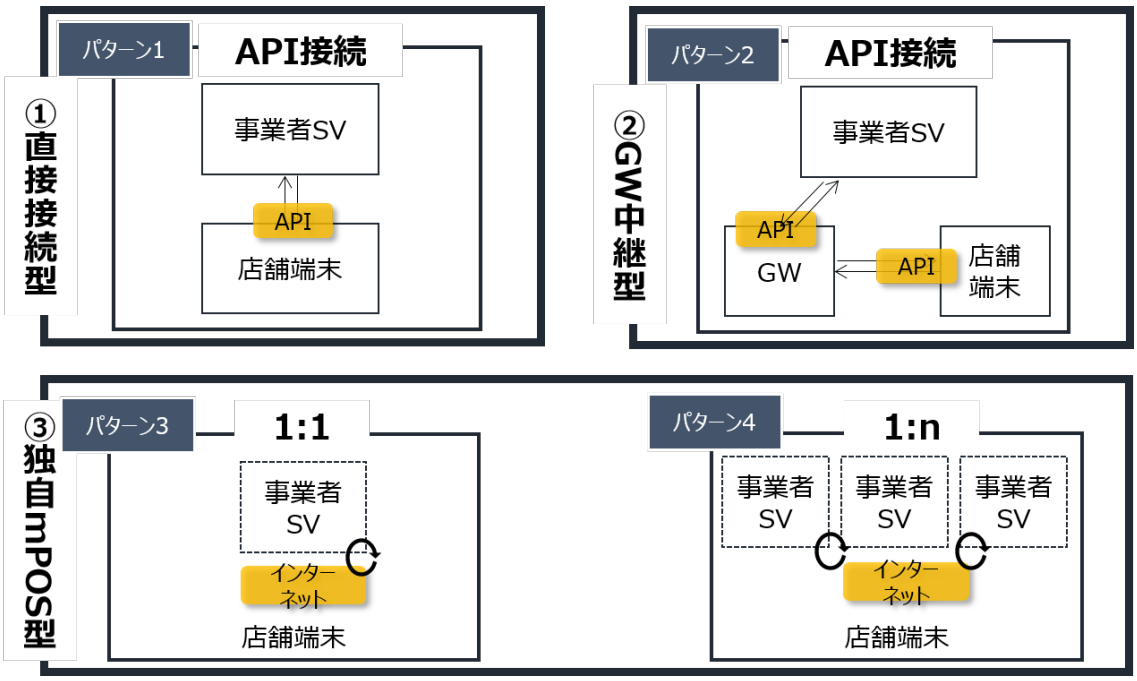
- ◆ 画面にのぞき見防止フィルムが貼られている。なお、現時点では、高光沢フィルム及び指紋・反射防止フィルムによる影響は確認されていない。
- ◆ ベールビューモード（のぞき見防止）が設定されている。
- ◆ 画面に貼られているフィルムに気泡がある。
- ◆ 画面輝度が不足している（バックライトの設定において画面を暗くしている。）。
- ◆ 画面にキズ・割れがある。
- ◆ 画面が自動で回転する（QR コードの読み取り最中に回転するために読み取りがやり直しになる。）。
- ◆ 読み取り時に画面がスクロールする。

5.3　接続パターン

店舗提示型の動的 QR コードを用いたコード決済においては、契約店が保有しているインフラ、コード決済関連事業者が提供するサービスの種類等により様々な接続パターンがあり得る。コード決済関連事業者は、自己が提供するコード決済サービス

に応じて契約店との接続を行わなければならない。

【図 5.3　想定される接続パターン】



6　セキュリティ

6.1　総論

コード決済の普及及び活用には、契約店及び利用者にとって安心かつ安全な決済手段であることは必須の条件であり、安心かつ安全な決済手段の提供は、すべてのコード決済関連事業者が検討及び実施しなければならない事項である。本項目ではコード決済において必須と思われるセキュリティ対策のほか、参考となるセキュリティ対策を例示的に記載しているが、本項目に記載されているセキュリティ対策を行うことで安全で欠陥のない決済システムを構築できることを保証するものではない。各コード決済関連事業者は決済関連分野におけるテクノロジーの発展が著しいことを踏まえ、自己の責任と負担において常に最新のセキュリティ情報を収集し、自己の決済システムに必要かつ十分なセキュリティを施す責務があることを常に意識しなければならない。なお、本ガイドラインに記載されるセキュリティ対策以外にも協議会、関係省庁、関係団体等がセキュリティ対策に関する指針やガイドラインを策定している場合があり、各コード決済関連事業者はこれらも参照されたい。なお、ギフトコード等譲渡を前提とするビジネスモデル、ブラウザベースによるコード決済の提供、オフライン

によるコード決済の提供等本項目記載のセキュリティ対策を講じることが事業上又は事実上困難な場合、当該コード決済事業者は、本項目で要求される各セキュリティ対策の趣旨を十分に理解した上で、利用者及び契約店を保護するために、本項目の各セキュリティ対策と同等相当の安全性を確保できる代替的なセキュリティ対策を講じなければならない。

コード決済における不正利用は様々な場面が考えられるが、以下は動的 QR コードを用いた店舗提示型によるコード決済において想定される不正利用の代表例である。

【表 6.1　想定される動的 QR コードの不正利用例】

No.	起因箇所1	起因箇所2	想定事象	不正者	具体的な不正の例	対策方針
1	モバイルデバイス	-	紛失・盗難	第三者	第三者が利用者のモバイルデバイスを利用して決済する	本人認証の実施
2		-	意図的流出	利用者	利用者が第三者と結託して利用の覚えなしとして申告する	
3	オペレーション	-	詐欺	利用者	利用者が決済完了画面を偽造し加盟店に提示し代金支払を免れる	決済完了画面の表示仕様の策定、契約店への取引完了確認手段の提供、契約店への啓発
4	システム	コード決済アプリ	ハッキング等	第三者	利用者のID等の抜き取り及び不正利用/利用者が意図しない決済の実行	システム設計時の脆弱性排除と監視体制強化
5		通信経路	ハッキング等	第三者	利用者のID等の抜き取り及び不正利用	
6		各サーバー	ハッキング等	第三者	同上/利用者のID等の不正生成/決済履歴の追加・改ざん	

6.2　本人認証 【共通】

(1) 総論

コード決済事業者においては、不正利用等を防止するためにコード決済を利用できる者を本人に限定するとともに、決済を行おうとする者が当該決済を行う権限がある者であること（多くの場合では、当該決済によって支払い義務を負う者と決済を行おうとしている者が同一であること。）を担保するために、本人認証を行うことが重要と考えられる。なお、関連法令において、利用者の氏名等特定の項目の確認がコード決済関連事業者に義務付けられている場合がある。かかる法令が自己に適用があるか否かについては各コード決済関連事業者が自己の責任において確認する必要がある。なお、かかる法令においては、本人確認義務以外の義務がコード決済関連事業者に課されている場合があることにも注意が必要である。

本人認証には大きく分けて⑴利用者が初めて当該決済手段を利用する際に当該利用者を限定する目的で行われる本人認証（基礎認証）と⑵決済を行おうとする際に決済を行おうとしている者が事前に登録されている利用者と一致するかを確認する目的で行われる本人認証（利用時認証）がある。本人認証のあり方においては、これらの組み合わせにより様々なパターンが考えられるが、事業者は想定される不正利用を防止するために、適切な本人認証プロセスを設けなければならない。

⑵ 基礎認証

コード決済事業者は、第三者によるコード決済アプリ ID やパスワードの不正取得による不正利用を防止するために、利用者のモバイルデバイスとコード決済アプリを紐づけ管理しなければならない。また、基礎認証にあたっては、利用者を特定するために必要な情報の受領・確認を行うことも考えられる。同時に、コード決済アプリにクレジットカード、デビットカード、銀行口座等の支払手段を登録しようとしている利用者が、当該支払手段の利用に関し正当な権限を有する者であることを確認する等、不正利用を未然に防止するための対策を行うことも重要である。

⑶ 利用時認証

利用時認証のタイミングについては、⑴利用者のモバイルデバイスの立上げ時、⑵コード決済アプリの立上げ時、⑶決済時（QR コード読み取り時）等が考えられる。利用時認証の方法については、PIN の入力、指紋認証、顔認証等がある。利用者及び契約店に安心・安全なコード決済を提供するため、決済時（QR コード読み取り時）に本人認証を行うことが推奨される。利用時認証については、利用者のモバイルデバイスの機能及び設定に依存する場合があり、コード決済事業者がすべてをコントロールできる訳ではない。また、各利用者、各契約店によって、希望するセキュリティレベルは大きく異なる場合もあり、本人認証スキームの構築にあたっては、不正防止の観点はもちろんのこと、利用者のモバイルデバイスの種類、利用状況、契約店における決済オペレーションの負荷、利用者及び契約店のニーズ等様々な事項を考慮し、慎重に判断していく必要がある。各利用者、各契約店のニーズに対応できるように、セキュリティレベルを各利用者、各契約店が選択できるようにするのも一つの方策である。

【表 6.2⑶ 利用時認証組合せパターン】

	モバイルデバイス 立上げ時	コード決済アプリ 立上げ時	決済時
組み合わせパターン	○	○	○
	○	-	○
	○	○	-
	-	○	○
	○	-	-
	-	○	-
	-	-	○

※セキュリティ対策は、他のセキュリティ対策（本ガイドラインで言及されているか否かを問わない。）との組み合わせにより行うものであり、本人認証の頻度のみで当該決済システムの安全性を決められるものではない。

6.3 取引の管理

(1) 取引検証 【共通】

コード決済事業者は、不正利用を防止するとともに正常な取引を実行するために、以下の各場面において以下の表記載の各事項を検証しなければならない。

【表 6.3(1) 必要とされる取引検証】

取引依頼電文送信時	
1	スマートフォン用のコード決済アプリからの取引においては、あらかじめ紐づけられた利用者のモバイルデバイスから行われたものであること。
取引依頼電文検証時	
2	当該決済を行おうとしている利用者の会員ステータスが有効であること。
3	有効な QR コードの利用であること。

(2) 決済完了画面の表示

動的 QR コードを用いたコード決済では、契約店側がオフライン環境下で決済を行う場合等にはユーザーのモバイルデバイスに表示された決済完了画面を視認することによって決済完了を確認する必要がある場合がある。当該決済完了画面が、以前に行われた決済画面のスクリーンショットや偽造・変造された画面等の不正な画面であった場合、契約店は決済が行われていないにもかかわらず、決済が行われたと誤認してしまう可能性がある。そのため、決済完了画面は容易に偽造等できるものであってはならない。コード決済事業者は、利用者がかかる決済完了を偽装する行為を防止でき、かつ、契約店が容易に決済の正当性を確認できるような決済完了画面を

構築しなければならない。具体的には、決済画面にアニメーションやタイムスタンプを表示することや決済完了時に決済完了を知らせる音を出す等が考えられる。また、契約店に対し、決済完了画面の確認方法を周知することも大切である。

(3) 契約店への確認手段の提供

上記「6.3(2) 決済完了画面の表示」記載のとおり、決済完了画面の視認による決済完了画面の確認には、利用者による決済完了偽装の可能性が存在する。そのため、決済完了画面に偽装防止策を行うことに加えて、決済が行われた場合に契約店が決済完了したことを契約店側の端末やモバイルデバイスで確認できるようにすることが重要である。コード決済事業者は、契約店に対し、契約店が任意に決済完了情報を確認できる手段を提供しなければならない。なお、ここで要求されているのは、契約店側がオンライン環境下で決済完了の確認を希望したときに確認ができる状態の構築であり、契約店側がオフライン環境にある場合が考えられることから、決済完了と同時に契約店側が決済完了した旨を実際に確認できることまでを要求するものではない。通知手段等については以下を推奨する。

【表 6.3(3)-1 推奨される取引情報提供手段等】

情報提供手段	Push 通知、email、SMS、契約店側コード決済アプリ上での表示等
情報提供時期	取引の成立後すみやかに
情報提供内容	日時、金額等

なお、動的 QR コードにおいては、静的 QR コードと異なり、契約店は決済完了通知を受けるための端末等を保有していることが多い。そして、上記記載の決済完了確認手段の提供においては、契約店側の端末やモバイルデバイスとコード決済事業者のサーバー等とのやり取りが発生する。本ガイドラインでは、かかる通信について、特定の接続 API を定めるものではないが、開発に際しての参考とすべく下記に決済完了確認手段の提供において必要となる接続 API リクエスト項目の代表例を一覧にしてある。ただし、かかるリクエスト項目はあくまで代表例であり、必要となるリクエスト項目を網羅したものではない。各決済事業者は下記表を参考にしつつ、各自必要な開発を行ってもらいたい。

【表 6.3(3)-2 決済完了確認手段の提供における接続 API リクエスト項目の代表例】

No.	項目名	属性	必須	説明
1	notification_type	英数字	Y	“Transaction”固定
2	BizCode	英数字	Y	契約店 ID

3	storeCode	英数字	N	契約店コード
4	termCode	英数字	N	端末コード
5	transId	英数字	Y	取引番号
6	receiptNo	英数字	N	契約店レシート番号
7	transTime	英数字	N	処理日時（取引成功時のみ）
8	Amount	数字	Y	取引金額
9	Result	英数字	Y	“COMPLETED”, “FAILED”

(4) 利用者への取引通知 【共通】

利用者のモバイルデバイスの盗難、契約店による不正操作又は偽造・変造されたQR コードの表示等による不正利用に対応するためには、速やかに利用者に対し、当該利用者の決済アカウントを用いて決済が行われたことを通知することが重要である。コード決済事業者は、決済の都度、利用者に決済が行われた旨を通知しなければならない。通知手段等については以下を推奨する。

【表 6.4(4) 推奨される取引完了通知の手段等】

通知手段	Push 通知、email、SMS、コード決済アプリ画面での表示等
通知時期	取引成立後すみやかに
通知内容	日時、金額、契約店名称等

(5) 事後的な不正利用検証 【共通】

将来における不正利用防止のためには、事前のセキュリティ対策のみならず、事後的な不正利用検証も重要である。かかる事後的検証を可能にするために必要となる利用者に関する情報、取引データ等を適切な期間保存することが推奨される。

6.4 システム間の情報連携におけるリスク検証の実施

決済システムは安全なシステムである必要があり、コード決済事業者は、コード決済サービスのリリース前、機能追加時等の適時のタイミングにおいて、自己のコード決済システム間の情報連携におけるリスク検証を行い、リスクの洗い出しを行うことが推奨される。ここでいう「システム」とは、連携する外部システムだけではなく、自己の内部システム同士で情報をやりとりする場合も含む。

かかるリスクをチェックする手段の一つとして、BCM 原則に基づいたチェックがある。BCM 原則の内容とその検証方法の例は別紙 1 のとおりである。BCM 原則は、システム間の情報連携におけるリスクを洗い出すには非常に有用な原則である。かか

るリスクチェックにおいては、第三者の目（第三者機関のみならず、当該決済システムの開発に関与していない自社内の開発者も含む。）で見ることも大切である。

コード決済事業者は、リスク検証の結果、脆弱性が発見された場合は、技術的対策、業務運用による対策等の必要な対策を検討・実施する必要がある。

6.5 その他 【共通】

上記各セキュリティ対策のほか、コード決済においてはシステム面及び体制面において以下のような各セキュリティ対策を検討することも考えられる。

【表 6.4 その他の考えられるセキュリティ対策】

＜システム面＞

No.	項目	内容（実装の手引き）
1	決済 ID 管理	利用者のモバイルデバイス上の決済 ID 保有は必要最低限の範囲内で設計する
2	アクセス権限	コード決済関連事業者における決済 ID 管理部分へのアクセス権限付与は、必要最低限の範囲とする
3	暗号鍵管理	高セキュリティ事項として厳重な管理方法を定める
4	コード決済アプリ開発	開発プロセスにおいて脆弱性がないセキュアコーディングを行う
5	通信暗号化	コード決済アプリとコード決済関連事業者サーバー間の通信プロトコルはセキュアなものを採用する
6	ネットワーク構成	ネットワーク構成の区分け及びファイヤーウォール設置等により不正アクセスのリスクを低減する
7	取引データ履歴	取消返品の店頭運用に支障を生じさせないように適切な期間、履歴を保存する（その他、決済に係る法令・会計の定めを考慮すること）

＜体制面＞

No.	項目	内容（実装の手引き）
1	不正利用の監視体制	不正利用検知を行う体制構築を行う（システム導入含む）
2	網羅的な検証	不正取引を検証し、新たな対策に活かす

3	取引ごとのリスクベース認証設定	対策の一つとして、利用者のステータス・利用状況等に応じたリスクベース認証を実施する

今後について

1　本ガイドラインの改訂方針

本ガイドラインは、EMV 仕様(MPM)の変更、コード決済を巡る環境の変化やテクノロジーの発展等に応じ改訂が必要である。協議会は適時、本ガイドラインの改訂についての検討を行うものとする。

2　コード決済の発展に向けて

コード決済は、キャッシュレスの推進において今後重要な意味を持つと思われる。コード決済関連事業者間のみならず、契約店や他の分野の事業者との連携も大切にしながら、コード決済関連事業者、契約店、利用者の三方がそれぞれ利益を享受できるようなキャッシュレスの在り方を今後も引き続き模索していきたい。本ガイドラインがコード決済、ひいては日本のキャッシュレス社会の発展の一助になれば幸いである。

以 上

【参考：店舗提示型における必要要件チェックリスト】

※このチェックリストは、コード決済関連事業者が統一 QR コードを用いた店舗提示型によるコード決済を行う場合に満たすべき要件を便宜的に一覧にしたものであり、コード決済関連事業者においては本チェックリストのみに依拠するのではなく、ガイドライン本体を必ず参照されたい。

＜凡例＞
◎：具体的な対応内容を義務化
〇：具体的な対応内容は義務化しないが、目的に応じた各社の対応を義務化
△：義務化はしないが、各社に対応を推奨
！：参考

＜第 1 部　静的 QR コード＞

No.	項目	義務化レベル	内容	ガイドライン該当箇所
1	表示	◎	データフォーマット（EMV 仕様(MPM)準拠及び協議会事務局が定めた入力内容の入力）	2.1
2		◎（該当者のみ）	データフォーマット上、任意とされている項目について入力を希望する場合への協議会事務局への入力希望申請	2.1
3		◎（該当者のみ）	海外のコード決済事業者等の統一店舗識別コードを利用しないコード決済事業者が統一静的 QR コードの利用を希望する際の協議会事務局への申請	2.1
4		◎（該当者のみ）	EMV 仕様(MPM)において自己の領域を確保されている決済事業者が統一静的 QR コードの利用を希望する際の協議会事務局への申請	2.1
5		◎	協議会が定めるデザインでの掲示	2.2
6		◎	読み取り可能なサイズによる印刷（1 セルあたり 0.33 ㎜以上必須(1 セルあたり 0.5 ㎜以上が推奨)、1 セルあたり 4dot 以上）	2.2

7	表示	◎	協議会が定める統一静的 QR コードのデザインの変更等の禁止	2.2
8		○	統一静的 QR コードのデザインの変更等の禁止について契約店への明確な通知	2.2
9		○	契約店が統一静的 QR コードのデザインの変更等を行っていることを認識した場合における契約店への指導	2.2
10		○	読み取りが適正に行われる品質保証対策	2.3
11	統一店舗識別コード	◎	統一店舗識別コードの発番申請	3.2
12	事業者識別コード	◎	事業者識別コードの取得又は登録	4.2
13	契約店との接続等	◎	契約店への統一静的 QR コードの設置	5.1
14		!	静的 QR コードを用いたコード決済の特性についての契約店への注意喚起	5.2
15	セキュリティ	○	本人認証プロセスの導入	6.2
16		◎	利用者のモバイルデバイスとコード決済アプリの紐づけ	6.2(2)
17		!	利用者を特定するために必要な情報の受領・確認	6.2(2)
18		△	決済時における本人認証	6.2(3)
19		○	静的 QR コードの不正な貼り換え、偽造等への対策	6.3
20		◎	決済時における取引検証	6.4(1)
21		○	決済完了画面の偽造防止等	6.4(2)
22		◎	契約店への取引確認手段の提供（ただし、具体的内容等については推奨レベル）	6.4(3)
23		◎	利用者への取引完了通知（ただし、具体的内容等については推奨レベル）	6.4(4)

24	セキュリティ	△	事後的な不正検証に必要な情報・データの保存	6.4(5)
25		△	システム間の情報連携におけるリスク検証	6.5 別紙 1
26		（〇）	（25 の検証を行った場合）発見された脆弱性への対応	6.5
27		!	システム面・体制面でのセキュリティ対策	6.6

＜第 2 部　動的 QR コード＞

No.	項目	義務化レベル	内容	ガイドライン該当箇所
1	表示	◎	データフォーマット（EMV　仕様(MPM)及び協議会事務局が定めた入力内容の入力）	2.1
2		◎ （該当者のみ）	海外のコード決済事業者等の統一店舗識別コードを利用しないコード決済事業者が統一動的 QR コードの利用を希望する際の協議会事務局への申請	2.1
3		◎ （該当者のみ）	EMV 仕様(MPM)において自己の領域を確保されている決済事業者が統一動的　QR　コードの利用を希望する際の協議会事務局への申請	2.1
4		◎	協議会が定めるデザインでの表示	2.2
5		◎	読み取り可能なサイズによる表示（1 セルあたり 0.33 ㎜相当以上必須(1 セルあたり 0.5 ㎜相当以上が推奨）	2.2
6		◎	協議会が定める統一動的　QR　コードのデザインの変更等の禁止（協議会事務局が承認した場合を除く）	2.2
7		〇	十分な画面輝度による表示	2.3
8		〇	読み取りが適正に行われるための品	2.4

			質保証対策	
9	統一店舗識別コード	◎	統一店舗識別コードの発番申請	3.2
10	事業者識別コード	◎	事業者識別コードの取得又は登録	4.2
11	契約店との接続等	◎	動的 QR コード表示端末の設置	5.1
12		!	動的 QR コードを用いたコード決済の特性についての契約店への注意喚起	5.2
13		◎	コード決済サービスに応じた契約店との接続	5.3
14	セキュリティ	○	本人認証プロセスの導入	6.2
15		◎	利用者のモバイルデバイスとコード決済アプリの紐づけ	6.2(2)
16		!	利用者を特定するために必要な情報の受領・確認	6.2(2)
17		△	決済時における本人認証	6.2(3)
18		◎	決済時における取引検証	6.3(1)
19		○	決済完了画面の偽造防止等	6.3(2)
20		◎	契約店への取引確認手段の提供（ただし、具体的内容等については推奨レベル）	6.3(3)
21		!	契約店への取引確認手段の提供に必要な接続 API の開発	6.3(3)
22		◎	利用者への取引完了通知（ただし、具体的内容等については推奨レベル）	6.3(4)
23		△	事後的な不正検証に必要な情報・データの保存	6.3(5)
24		△	システム間の情報連携におけるリスク検証	6.4 別紙 1
25		（○）	（25 の検証を行った場合）発見された脆弱性への対応	6.4
26		!	システム面・体制面でのセキュリティ対策	6.5

【別紙１】

BCM 原則を満たすとは？

BCM 原則を満たすとは以下のすべてを満たすことをいう。

原則1.　送信元・送信先を認証することができ、
原則2.　どのプロトコルのどのバージョンどのメッセージかを識別することができ、
原則3.　当該トランザクションに関与する全アクター・ロールを知ることができ、
原則4.　かつ、それぞれのメッセージの改ざん検知が可能である。

ここで、

- 送信元認証とは、受信者が送信元の提示する識別情報・認証情報を、事前に記録してあるデータと突き合わせて、確率的一致性を確認すること。
- 送信先認証とは、送信者が送信先の識別情報（アドレス、URL）およびその認証情報を、事前に記録してあるデータと突き合わせて、確率的一致性を確認すること。

実際の点検では、これを以下の処理に関して行うものとする。

1. クライアントアプリの登録（インストール・再インストール時）
2. ユーザの登録
3. ユーザの認証
4. クレデンシャルのリセット（例：パスワードのリセット）
5. アカウントの一時停止
6. アカウントの再開
7. 支払い処理
8. アカウントの停止
9. アカウントの廃止

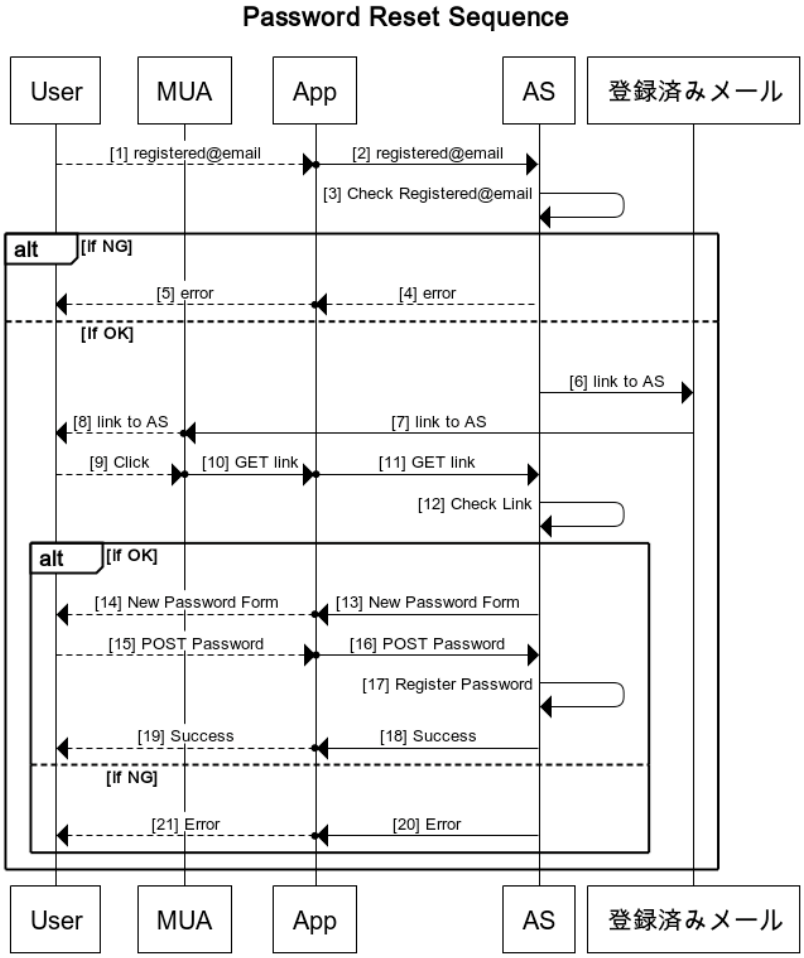
点検にあたっては、シーケンス図とその解説を作成、それぞれを BCM 原則に照らして評価し、プロトコルとしての安全性を見て、リスク評価をする。

例として、ありがちな「パスワードリセット」手続きについて、以下に記載する。

例：パスワード・リセットのケース

[注] この例は、とくにセキュアな例ではない。むしろ、例として、意図的に技術的にはセキュアでない部分を作ってある。

シーケンス図



プロトコル説明

[1]. ユーザがスマホ上の App のパスワード忘れ画面を開いて、自らのユーザ名（メアド）を入力。

[2]. App は自ら保存していた最後のログイン用 ID トークン{id_token}と、ユーザが入力したメアド{email}および乱数{nonce}を以下の様式で HTTPS 上で

AS のパスワードリセット URLhttps://example.com/app1/passr/1.0/へ送信。なお、この時の{email}と{nonce}を App は保存しておくとともに、自分がパスワードリセット中であることも保存しておく。

```
POST /app1/passr/1.0/ HTTP/1.0
Host: example.com
Authorize: Bearer {access_token}
Content-Type: application/x-www-form-urlencoded
Content-Length: {length}
email={email}&id_token_hint={id_token}&nonce={nonce}
```

[3]. AS は、{email}、{id_token}、および{email}に付随して AS 内の Identity Register に保存されていた値から整合性をチェック。このとき、{email}は、{id_token}から取得された{email}に等しくなければならず、またこの値は Identity Register で有効でなければならない。
[4]. NG であれば、400 Error を返す。
[5]. 同上。
[6]. OK であれば、パスワードリセット用ワンタイムリンク{link}を記載したメールを送る。
[7]. [6]で送ったメールを MUA が取得、
[8]. ユーザに提示。
[9]. ユーザはリンクをクリック。
[10]. {link}は https claimed URI になっているため、App に値が引き渡される。{link}の中には{nonce}も入っているため、App は[2]で保存した値と突合。あっていれば、[11]に進む。そうでなければエラー表示。
[11]. App は{link}にアクセス。

```
GET /app1/passr/1.0/s2/?nonce={nonce} HTTP/1.0
Host: example.com
Authorize: Bearer {access_token}
Content-Type: application/x-www-form-urlencoded
Content-Length: {length2}
```

[12]. AS は{nonce}と{access_token}を[2]の値と突合。
[13]. OK であればパスワードリセットフォームを返却、
[14]. App はそれをユーザに提示。
[15]. ユーザは新パスワードを2回入力、App 上で突合。
[16]. App は新パスワードおよび{nonce}を AS の /app1/passr/1.0/s3/に送信

```
POST /app1/passr/1.0/s3/ HTTP/1.0
Host: example.com
```

```
Authorize: Bearer {access_token}
Content-Type: application/x-www-form-urlencoded
Content-Length: {length}
nonce={nonce}&p1={pass1}&p2={pass2}
```

[17]. AS は{access_token}と{nonce}の整合性を確認の後、これらから該当アカウントを特定、{pass1}=={pass2}ならば、これを新パスワードとして登録。
[18]. 200 OK を返すとともに、{email}に変更したことを通知、
[19]. 成功画面をユーザに提示。
[20]. NG だった場合には 400 Error を返し、
[21]. ユーザに表示する。

BCM 原則評価

全体

本パスワードリセットプロトコルでは、全アクター（User, MUA, App, AS, 登録済みメール）がプロトコル開始時に確定しているため、プロトコル・トランザクション中のメッセージであることが分かれば、各シーケンスにおいて、当該トランザクションに関与する全アクター・ロールを知ることができる。

[1] システム外なので対象外
[2] 原則 1: App は AS の TLS 証明書を確認。AS は App を、個別のクライアント別シークレットで確認。
原則 2: 本プロトコルでコールされる AS のアドレスは本プロトコル・バージョンに専用のものであるため満たされる。
原則 3: 原則2が満たされているため、「全体」に記述したとおり満たされる。
原則 4: TLS で保護されているため満たされる。
[3] サーバー内通信であるため対象外
[4] 原則 1: TLS セッションで守られており、[2]での確認が有効なため満たされている。
原則 2: 同上。
原則 3: 同上。
原則 4: 同上。
[5] システム外なので対象外
[6] 原則 1: リレーされる可能性があるため満たされていない。
原則 2: メールヘッダ及び本文に記載しているが、MUA ではチェックされないた

め満たされない。
原則 3: 同上
原則 4: S/MIME 署名はつけておらず、検知できないため未達。

[7] 原則 1: MUA はクライアント認証を行わないため未達。
原則 2: [6]の原則2に同じ。
原則 3: 同上
原則 4: S/MIME 署名はつけておらず、検知できないため未達。

[8] システム外なので対象外

[9] システム外なので対象外

[10] 原則 1: Claimed HTTPS URL を用いて App を起動するので送信先は認証されているが、送信元は認証されない。なお、リセットフローをはじめた端末以外でこのリンクを開いた場合はエラーになる。
原則2: リンクの中にプロトコル名とバージョンの識別子が入っている。
原則3:[6]の原則3に同じ
原則4:URL 自体は署名されていないので満たされていない。

[11] 原則 1: App は AS の TLS 証明書を確認。AS は App を、個別のクライアント別シークレットで確認、さらにリンクのパラメータが当該 App 向けであることを確認。
原則 2:コールされる AS のアドレスは本プロトコル・バージョンに専用のものであり、また、[2][16]のものとも異なるため満たされる。
原則 3: 原則2が満たされているため、「全体」に記述したとおり満たされる。
原則 4: TLS で保護されているため満たされる。

[12] サーバー内通信であるため対象外

[13] 原則 1: TLS セッションで守られており、[11]での確認が有効なため満たされている。
原則 2: 同上。
原則 3: 同上。
原則 4: 同上。

[14] システム外なので対象外

[15] システム外なので対象外

[16] 原則 1: App は AS の TLS 証明書を確認。AS は App を、個別のクライアント別シークレットで確認。
原則 2:コールされる AS のアドレスは本プロトコル・バージョンに専用のものであり、また、[2][11]のものとも異なるため満たされる。
原則 3: 原則2が満たされているため、「全体」に記述したとおり満たされる。
原則 4: TLS で保護されているため満たされる。

[17] サーバー内通信であるため対象外

[18] 原則 1: TLS セッションで守られており、[16]での確認が有効なため満たされている。
原則 2: 同上。
原則 3: 同上。
原則 4: 同上。

[19]　システム外なので対象外
[20]　原則 1: TLS セッションで守られており、[16]での確認が有効なため満たされている。
原則 2: 同上。
原則 3: 同上。
原則 4: 同上。

（評価）

BCM 原則は[6][7][10]が満たしていないため満たされていない。そのため、このプロトコルは、技術的には安全ではないと考えられる。技術以外の対策が必要である。

リスクの評価

（シーケンス・ステップ毎の評価）

[1] n/a
[2] 影響度:高　頻度:低　評価:低　理由:破られた場合の個別の影響度は高いものの、頻度は低いと考えられ、総合評価は「低」とする。
[3] n/a
[4] 上記[2]に同じ
[5] n/a
[6] 影響度:高　頻度:中　評価:中　理由:攻撃内容はフィッシングであるが、[10]での対策により、その成功する確率は低い。
[7] 同上
[8] n/a
[9] n/a
[10]　影響度:高　頻度:低　評価:低　理由:URL のパラメータの書換は可能ではあるものの、[11]でのチェックにひっかかるはず。
[11]　影響度:高　頻度:低　評価:低　理由:破られた場合の個別の影響度は高いものの、頻度は低いと考えられ、総合評価は「低」とする。
[12]　n/a
[13]　上記[2]に同じ
[14]　n/a
[15]　n/a
[16]　影響度:高　頻度:低　評価:低　理由:破られた場合の個別の影響度は高いものの、頻度は低いと考えられ、総合評価は「低」とする。
[17]　n/a
[18]　影響度:高　頻度:低　評価:低　理由:破られた場合の個別の影響度は高いものの、頻度は低いと考えられ、総合評価は「低」とする。
[19]　n/a

[20]　影響度:高　頻度:低　評価:低　理由:破られた場合の個別の影響度は高いものの、頻度は低いと考えられ、総合評価は「低」とする。
[21]　n/a

（全体評価）
プロトコルとしてはステップ[6][7][10]のために脆弱性があると考えられるが、たとえば[11]などである程度対処されているため、リスク評価は「中」とする。

技術的対策以外の対策

技術的対策だけだと残存リスクが「中」となるため、運用的対策を行う。

具体的には、本プロトコルフローでパスワードのリセットを行った場合には、当該アカウントを一定期間、要注意リストに入れ、支払限度額を下げ、必要に応じて別途本人に電話で確認をとるものとする。

以上


PAYMENTS
JAPAN