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)

一般社団法人キャッシュレス推進協議会

Ver. 1.2

2019 年 10 月 31 日

【履歴】

2019 年 1 月 31 日　新規制定（Ver. 1.0）

2019 年 3 月 29 日　統一 QR コード仕様等追加（Ver. 1.1）

2019 年 10 月 31 日　6.5 を追加、従前の 6.5 を 6.6 に繰り下げ、別紙 1 を追加等（Ver. 1.2）

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
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 コード等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
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。
電文	一定の形式に従って記述された、システム間で送受信されるひとまとまりのデータ
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-

[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。

	Presented Mode)とも言う。
統一バーコード	本ガイドラインで定められた仕様に準拠したコード決済用のバーコード
統一 QR コード	本ガイドラインに定められた仕様に準拠したコード決済用の QR コード
統一 QR コード等	統一バーコード及び統一 QR コードの総称
バーコード	コード決済用の一次元コード（一次元シンボル）
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(CPM)	EMVCo, LLC. が公表している「EMV® QR Code Specification for Payment Systems (EMV QRCPS) Consumer-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
QR コード	コード決済用の二次元コード（二次元シンボル）
QR コード等	バーコード及び QR コードの総称

1　はじめに

1.1　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 コード等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 コード等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 コード等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 コード等の乱立状態を解消・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、利用者提示型にかかる QR コード等の仕様を定め、コード決済に用いられる QR コード等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 コード等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 コード等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 コード等の活用により、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。

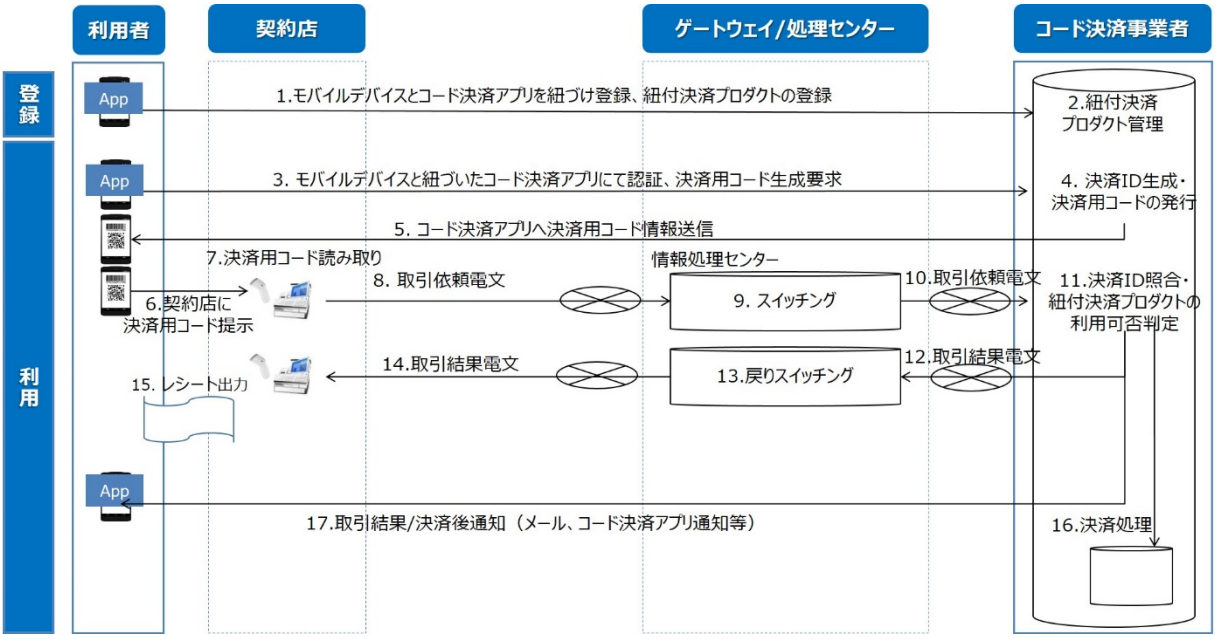
1.2 本ガイドラインの適用範囲・注意事項

- 本ガイドラインは、コード決済のうち、利用者提示型にかかる QR コード等の統一仕様を定めるものであるが、統一 QR コード等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。店舗提示型にかかる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【店舗提示型】MPM(Merchant-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。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、本ガイドラインは、本ガイドラインに記載される仕様と異なる仕様等にて運用を行っている海外のコード決済事業者による、又はかかる海外のコード決済事業者との提携によるインバウンド向けコード決済の提供を排除するものではない。
- 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 コード等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。

2　全体フロー

利用者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 2　基本的な全体フロー】

3　統一 QR コード等仕様

3.1　統一バーコード

(1)　データフォーマット

統一バーコードのデータレイアウトは以下の通りとし、コード決済事業者はかかるデータレイアウトに従わなければならない。また、統一バーコードの表示データは Code128 形式でエンコードしなければならない。なお、事業者識別コードの詳細については、「4　事業者識別コード」を参照されたい。

【図 3.1(1)　データフォーマット】

(2)　表示要件

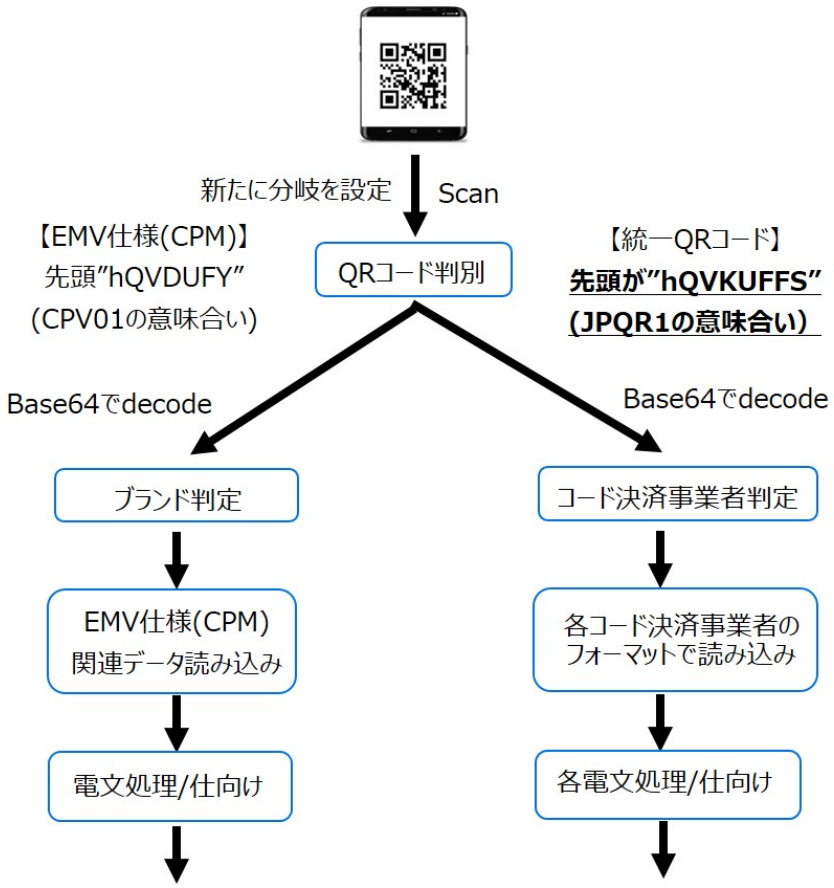
統一バーコードは、市場に一般的に流通・導入されているバーコードリーダーで読み取り可能なサイズで表示しなければならない。ただし、利用者のモバイルデバイス（スマートフォン等）の画面サイズにより、読み取りに際して統一バーコードを十分な大きさで表示することができない場合は、拡大機能を提供することをもって代替することができる。

なお、現行のバーコードリーダーの読み取り要件により、統一バーコードの最大サイズは 6cm を目安とする。

3.2　統一 QR コード

(1)　総論

統一 QR コードにおいては、コード決済事業者の独自のサービスを阻害することがないように配慮する必要があり、かつ、契約店側の対応負担が少ないことが望ましい。また、インバウンド対応のために海外のコード決済事業者の QR コードとの識別が可能であることが必要である。そこで、統一 QR コードにおいては、国際的な決済プロトコル(ルール)を定める EMVCo, LLC.が定める EMV 仕様(CPM)を参考とし、EMV 仕様(CPM)に準拠している QR コードと共存可能で、かつ、よりデータ容量の少ない独自の仕様を策定した。「図 3.2(1) EMV 仕様(CPM)との関係」記載のとおり、EMV 仕様(CPM)と統一 QR コードはペイメント・フォーマット識別子に記載される内容によって QR コードを区別するため、EMV 仕様(CPM)に対応している契約店においては少ない開発負担で統一 QR コードに対応することが可能であり、逆についても同様である。統一 QR コードの仕様と EMV 仕様(CPM)を並存させるために、コード決済関連事業者は、両者の振り分けが可能な分岐処理を実装しなければならない。



【図 3.2(1) EMV 仕様(CPM)との関係】

(2)　データフォーマット

「3.2(1) 総論」記載のとおり、統一 QR コードは協議会が定める独自の仕様となるが、EMV 仕様(CPM)をベースとしている。したがって、下記「表 3.2(2) 統一 QR コードの格納データ」に記載されているデータ格納場所及び格納データに関する定め以外のデータの QR コードへの記載方法等の詳細については、EMV 仕様(CPM)に従うものとする。各コード決済事業者は自己の責任において EMV 仕様(CPM)を確認する必要がある。

統一 QR コードには、下記の表に従ってデータが格納されていなければならない。下記表において「必須」とされている項目については、統一 QR コードに必ず含まれていなければならない。「任意」とされている領域については、各決済事業者が自由に使用することができる。かかる格納されるべきデータはすべて Base64 でエンコードされなければならない。また、統一 QR コードとしては特定のデータ量の上限を義務付けるものではないが、読み取り速度等を考慮すると 128 byte を上限とすることを推奨する。なお、事業者識別コードの詳細については、「4 事業者識別コード」を参照されたい。

【表 3.2(2) 統一 QR コードの格納データ】

タグ (Tag)	Tag 説明 ※EMV 仕様(CPM)準拠		長さ (Length)	フォーマット (Formant)	値 (Value)	存在 (Presence)
'85'	–	ペイメント・フォーマット識別子 (Payload Format Indicator)	5	英数/ 大小文字	**JPQR1** 4A 50 51 52 31 (バイナリ)	**必須**
'61'	–	アプリケーション・テンプレート (Application Template)	可変長	EMV 仕様 (CPM) 規定 bit	Tag61 の長さ	**必須**
	'4F'	ADF Name (ブランド識別子≒仕向け先に使うもの) (Application Definition File (ADF) Name)	可変長	EMV 仕様 (CPM) 規定 bit	事業者識別コード 8 桁	**必須**
	'57'	ID 等を格納する場所 (Track 2 Equivalent Data)	可変長	EMV 仕様 (CPM) 規定 bit	決済 ID(事業者識別コード 8 桁 +トークン部(桁	**必須**

					規定なし))	
	'99'	任意領域 (Other template)	可変長	EMV 仕様 (CPM) 規定 bit	自由領域	任意

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

(3) 表示要件

統一 QR コードは、原則として ISO/IEC18004 及び JIS X 0510 の規格に準拠しなければならない。ISO/IEC18004 及び JIS X 0510 の規格に準拠した QR コードと互換性がある QR コードを含む二次元コード(二次元シンボル)の利用は否定されないが、ISO/IEC18004 及び JIS X 0510 の規格に準拠した QR コードと同等(以上)の品質が保証されていなければならない。また、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 QR コードの周囲には 4 セル分の余白を設ける必要がある[2]。

統一 QR コードは読み取りやすいことから正方形の QR コードを黒と白で表示することを推奨する。統一 QR コードをカラーで表示することは、十分なコントラストがないと契約店側が導入する読み取り機器によっては読み取れない又は読み取りにくい場合があることには留意が必要である(例えば、限定的な例ではあるが、赤い光源を用いた読み取り機器では、赤と白で表示された QR コードは十分なコントラストが出ず、読み取れない可能性がある。)。またコントラストについては ISO/IEC18004 及び JIS X 0510 の規格に規定があることに注意が必要である。

統一 QR コード内にロゴ等を埋め込んでデコレーションすることは、当該ロゴの存在により、QR コードの特徴である汚損・欠損を想定した誤り訂正機能が機能せず、読み取り率に影響を及ぼすことに留意する必要がある。

3.3 QR コード等共通項目

(1) 画面輝度

統一 QR コード等を表示する際の画面輝度は、最大輝度とすることを推奨する。

2 かかる余白に関する規定は ISO/IEC18004 及び JIS X 0510 の規格にも規定されている事項ではあるが、本ガイドラインにおいては表示にかかる重要な要件は記載するという観点から敢えて余白に関する規定を別途記載した。

(2)　QR コード等の配置

コード決済事業者は、統一バーコードと統一 QR コードの双方を利用者提示型用の QR コード等として生成する場合には、コード決済を行う際に消費者が契約店においてどちらを表示しなければならないか考える必要がないように、例えば利用者のモバイルデバイスにおいて、両方の統一 QR コード等を同一画面で表示するなど、その配置を考慮しなければならない。

(3)　検証

コード決済事業者は統一 QR コード等を表示す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処理端末(「図 5.1(1) コード決済に用いられる処理端末の例」参照。)を用いて、表示される統一 QR コード等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。

4　事業者識別コード

4.1　総則

事業者識別コードは、統一 QR コード等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する。統一 QR コード等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 コード等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　受入準備

(1) 処理端末の設置

統一バーコードを利用してコード決済を行おうとする契約店には、レーザー又は CCD 方式のいずれかの方式で 6cm 幅のバーコードを読み取り可能なインフラが整備されなければならない。

統一 QR コードを利用してコード決済を行おうとする契約店には、最低限 128 byte（バージョン 8）の QR コードを読み取り可能なインフラが整備されなければならない。なお、128 byte より大きなデータ容量を採用するコード決済事業者の統一 QR コードをも読み取る場合やインバウンド需要に対応するため等 EMV 仕様(CPM)の QR コードをも読み取る場合には、当該コード決済事業者のデータ容量に対応したデータ容量まで読み取り可能なインフラや EMV 仕様(CPM)のデータ容量上限である 512 byte まで読み取り可能なインフラが整備される必要がある。

【図 5.1(1) コード決済に用いられる処理端末の例】

(2) QR コード等の特性の説明

利用者提示型のコード決済は、利用者のモバイルデバイスに QR コード等が表示され、それを契約店の処理端末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、

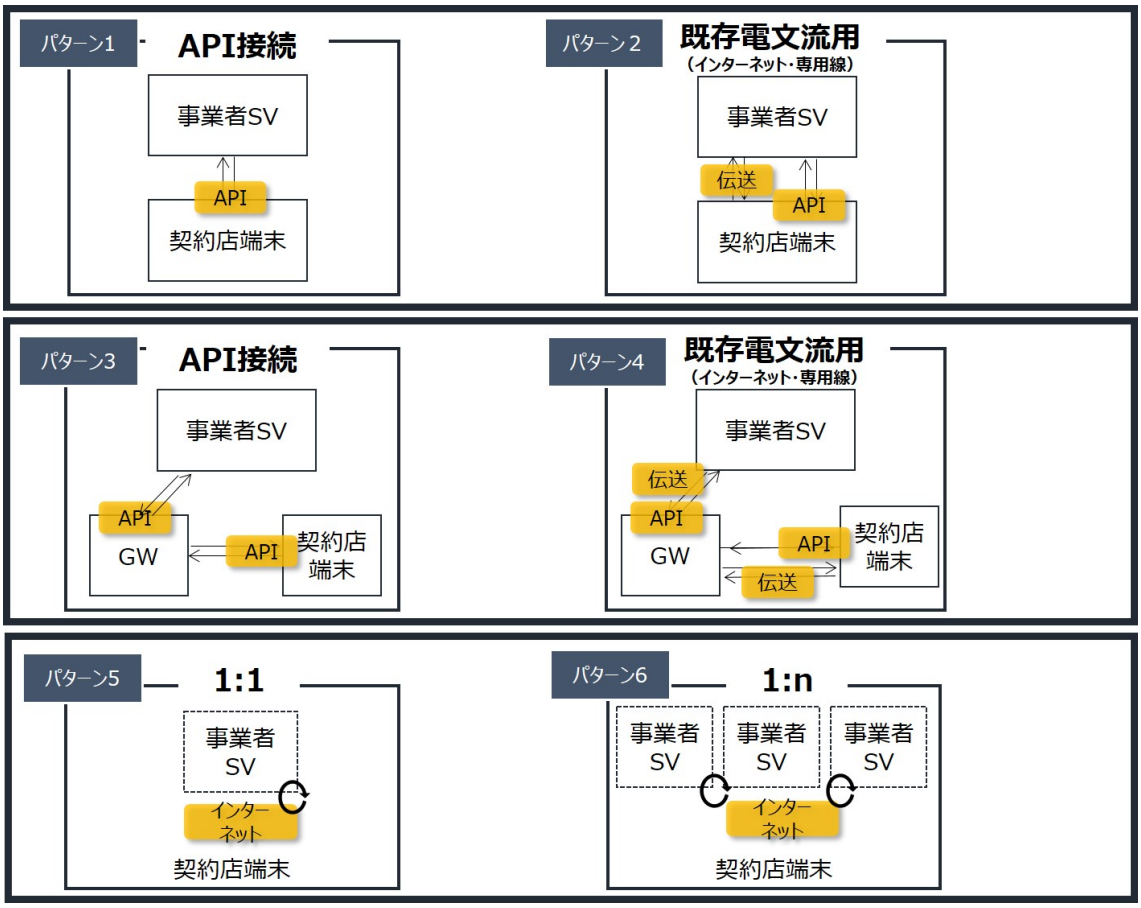
契約店に対しその対応を説明（各種マニュアル・注意文書の配布等を含む。）する必要があることに注意を要する。なお、下記は、QRコード等の読み取りの可否に影響する事象の一例である。

【表 5.1(2) QR コード等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（バーコードが回転して読み取りエリア外になることがある。）。
◆ 読み取り時に画面がスクロールする。

5.2 接続パターン

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契約店のインフラとコード決済事業者との接続パターン・接続先に応じたデータ編集を行わなければならない。



※SV=Server、GW＝Gateway、mPOS＝mobile POS

【図 5.2　想定される接続パターン】

5.3　　接続 API/電文

コード決済における接続 API/電文は各コード決済関連事業者によって異なっている。そして、支払電文、返金電文及び確認・照会電文の 3 つに集約される。下記はコード決済関連事業者に共通すると考えられる接続 API/電文の項目及び項目の説明等を一覧にしたものである。ただし、下記表は接続 API/電文の代表例であり、必要となるすべての接続 API/電文を網羅的に記載したものではない。各コード決済関連事業者のうち接続 API/電文の編集を行う必要がある者は、自己のサービスの種類、想定される決済フロー（返金フローを含む。）等を検討し、下記表を参考にしつつ、自己に必要な接続 API/電文の編集を行わなければならない。なお、下記表において「必須」部分に「Y」と記載されているものは、必ず編集を行わなければならない項目となる（なお、「N」は必ずしも編集を行う必要のない項目であることを意味する。）。また、下記表において桁数が明記されているもの（決済 ID 等及び取引金額）については、コード決済関連事業者はこれに従わなければならない。なお、接続 API/電文には、サービスによって下記表に記載されているもの以外にも固有のデータ項目がある場合

があり、コード決済サービスの導入にあたっては他のコード決済関連事業者の仕様にも留意する必要がある。

【表 5.3　コード決済関連事業者に共通の接続 API/電文項目等の代表例】

1. 支払電文

1.1 リクエスト項目（共通部）

No.	項目名	属性(桁)	必須	説明
1	requestId	数字	Y	要求ID

1.2 リクエスト項目

No.	項目名	属性(桁)	必須	説明
1	oneTimeCode	数字(32桁以下)	Y	決済ID（事業者仕分8桁+トークン部）
2	BizCode	英数字	Y	契約店ID
3	storeCode	英数字	Y	契約店コード
4	termCode	英数字	Y	端末コード
5	receiptNo	数字	N	契約店レシート番号
6	reqTime	数字	Y	契約店端末 送信日時
7	amount	数字(8桁)	Y	取引金額

1.3 レスポンス項目

No.	項目名	属性(桁)	必須	説明
1	result	数字	Y	結果コード
2	message	英数字	Y	結果メッセージ
3	transId	英数字	Y	取引番号
4	transTime	英数字	Y	処理日時
5	amount	数字(8桁)	Y	取引金額

2. 返金電文

2.1 リクエスト項目（共通部）

No.	項目名	属性(桁)	必須	説明
1	requestId	数字	Y	要求ID

2.2 リクエスト項目

No.	項目名	属性(桁)	必須	説明
1	originRequestId	数字(32桁以下)	Y	返金対象の要求ID
2	BizCode	英数字	Y	契約店ID
3	storeCode	英数字	Y	契約店コード
4	termCode	英数字	Y	端末コード
5	receiptNo	数字	N	契約店レシート番号
6	reqTime	数字	Y	契約店端末 送信日時
7	amount	数字(8桁)	Y	取引金額

2.3 レスポンス項目

No.	項目名	属性(桁)	必須	説明
1	result	数字	Y	結果コード
2	message	英数字	Y	結果メッセージ
3	transId	英数字	Y	取引番号
4	transTime	英数字	Y	処理日時
5	amount	数字(8桁)	Y	取引金額

3. 確認・照会電文

3.1 リクエスト項目（共通部）

No.	項目名	属性(桁)	必須	説明
1	requestId	数字	Y	要求ID

3.2 リクエスト項目

No.	項目名	属性(桁)	必須	説明
1	originRequestId	数字(32桁以下)	Y	照会対象の要求ID
2	BizCode	英数字	Y	契約店ID
3	storeCode	英数字	Y	契約店コード
4	termCode	英数字	Y	端末コード
5	receiptNo	数字	N	契約店レシート番号
6	reqTime	数字	Y	契約店端末 送信日時

3.3 レスポンス項目

No.	項目名	属性(桁)	必須	説明
1	result	数字	Y	結果コード
2	message	英数字	Y	結果メッセージ
3	transId	英数字	Y	取引番号
4	transTime	英数字	Y	処理日時
5	amount	数字(8桁)	Y	取引金額

※現状のゲートウェイ事業者等の仕様を考慮して表 5.3 では決済 ID が含まれる電文項目については 32 桁としている。そのため、決済 ID が含まれる電文項目では、トークン部が 24 桁（32 桁－事業者仕分けコード 8 桁＝24 桁）までしか入力できない。しかしながら、「3.1（1）データフォーマット」及び「3.2（2）データフォーマット」記載のとおり、本ガイドライン上はトークン部の桁数の上限を設けていない。トークン部を 25 桁以上にするコード決済事業者は、独自の電文項目としてトークン部を記載する電文項目を設けることによって、25 桁以上のトークンを電文内に含めることができる。

各コード決済関連事業者は、統一 QR コード等内の決済 ID 情報部にセットされる事業者識別コードに基づき、電文仕向け又は接続 API 呼び出しを行わなければならない。なお、ゲートウェイ中継型（「図 5.2　想定される接続パターン、パターン 3 及び 4」参照。）及び独自 mPOS 型（同「パターン 6」参照。）では複数の事業者識別コードに対応した仕向け先・接続 API が存在することとなる。

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、以下は利用者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	利用時のID表示仕様及び本人認証の実施
2		-	盗み見/複製	第三者	第三者がQRコード等を盗用・複製して決済する	
3		-	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	
4	システム	コード決済アプリ	ハッキング等	第三者	決済ID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	決済ID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/決済ID不正生成/決済履歴の追加・改ざん	

6.2 本人認証

(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 コード等の表示時)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 コード等の表示時)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 (QRコード等表示時)
	○	○	○
	○	-	○
	○	○	-
	-	○	○
	○	-	-
	-	○	-
	-	-	○

※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 QR コード等の管理

(1) ワンタイムトークンの有効時間の設定

利用者提示型においては、利用者のモバイルデバイスに表示された QR コード等

によって利用者を特定して決済を行うため、当該 QR コード等の画像等を入手した第三者が不正に決済を行うおそれがある。コード決済事業者は、QRコードの盗用・不正複製等による不正利用を防止するために、生成する QR コード等内のワンタイムトークンに有効時間を設定しなければならない。有効時間については、短時間であれば決済時に有効時間切れが多発しかねず、利用者の利便性が低下し、契約店にも過度なオペレーション負荷をかけることになりかねない。一方で、長時間の有効時間を設定すれば、QR コード等の盗用・不正複製等のリスクが増加することとなる。有効時間の設定にあたっては、コード決済事業者は、この両者のバランスを考慮する必要がある。有効時間の長さは各コード決済事業者の判断によるが、不正防止と利便性とを考慮すると 5 分（300 秒）程度の有効時間が目安となると思われる。

なお、コード決済事業者は、残有効時間の表示、QR コード等の自動更新又は更新ボタンの配置による手動での更新の許容等を行い、有効時間が契約店におけるスムーズな決済を阻害しないよう留意するものとする。

(2) QRコード等再生成の際の従前の QRコード等の無効化

利用者の利便性を考慮すると、決済直前での QR コード等の有効時間切れを防ぐために、生成された QR コード等の有効時間内であっても新たな QR コード等の生成を許容することが考えられる。しかし一方で、従前の QR コード等の有効時間内に新たな QRコード等の生成を許すと、従前の QRコード等と新たな QRコード等の双方で決済が可能となり、多重決済や不正利用の可能性を生じる。コード決済事業者はかかる事態を防ぐために、新たな QR コード等が生成された場合には速やかに従前の QR コード等を無効化しなければならない。ただし、かかる規定は一定期間経過後の同一トークンの再利用を妨げるものではない。

なお、コード決済事業者は有効時間内の新たな QR コード等の生成を許容する場合には、システム上における第三者による不正に留意し、不正利用を抑止する手段を考慮する必要がある。

6.4 取引の管理

(1) オンライン処理

決済 ID の生成及び QRコード等の表示処理はすべてオンラインで実施しなければならない。かかる規定は通信環境が悪い場合等を考慮し、一時的にオフラインで当該生成又は表示処理を行える仕組みを否定するものではない。ただし、かかる仕組みを導入するにあたっては、「6.1　総論」において記載のとおり、利用者及び契約店を保護するために、オフライン処理では導入することができない本「6. セキュリティ」の項目記載の各セキュリティ対策について、当該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。

(2) 取引検証

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(2) 必要とされる取引検証】

QR コード等表示時（決済 ID 発行時）	
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、当該利用リクエストが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	自らが発行した QR コード等であること。
4	有効な QR コード等の利用であること。

(3) 取引通知

利用者のモバイルデバイスの盗難や QR コード等の画像の流出・盗用又は契約店による不正操作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取引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、利用者に取引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(3) 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

(4) 事後的な不正利用検証

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

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

7　今後について

7.1　本ガイドラインの改訂方針

本ガイドラインは、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。

7.2　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：利用者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 コード等を用いた利用者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
○：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
【BC】：統一バーコードにのみかかる事項
【QR】：統一 QR コードにのみかかる事項

No.	項目	義務化レベル	内容	ガイドライン該当箇所
1	表示	◎	【BC】データレイアウト	3.1(1)
2		◎	【BC】Code128 形式でエンコード	3.1(1)
3		◎	【BC】読み取り可能なサイズによる表示（最大サイズ 6cm が目安）	3.1(2)
4		◎	【QR】統一 QR コードと EMV 仕様（CPM）との振り分けが可能な分岐処理の実装	3.2（1）
5		◎	【QR】データレイアウト（データレイアウト以外のデータ記載方法等は EMV 仕様(CPM)に従う）	3.2(2)
6		◎	【QR】Base64 でエンコード	3.2(2)
7		△	【QR】データ容量上限 128 byte	3.2(2)
8		◎	【QR】原則として ISO/IEC18004 及び JIS X 0510 に準拠	3.2(3)
9		◎	【QR】最小セルサイズ（1 セルあたり 0.33 ㎜相当以上。ただし、1 セルあたり 0.5 ㎜相当以上を推奨）	3.2(3)
10		◎	【QR】QR コードの周囲に 4 セル分の余白を配置	3.2(3)

11	表示	△	【QR】正方形の QR コードを黒と白で表示	3.2(3)
12		!	【QR】カラーで QR コードを表示する場合のコントラストに関する注意	3.2(3)
13		!	【QR】QR コード内にロゴ等を埋め込むと読み込み率が低下する	3.2(3)
14		△	最高画面輝度による表示	3.3(1)
15		!	バーコードと QR コードの配置	3.3(2)
16		○	読み取りが適正に行われるための品質保証対策	3.3(3)
17	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
18	契約店との接続等	◎	契約店インフラの整備 【BC】6cm 幅のバーコードを読み取り可能なレーザー方式又は CCD 方式の処理端末の設置 【QR】最低限 128 byte（バージョン 8）の QR コードを読み取り可能な処理端末の設置）	5.1(1)
19		!	コード決済の特性についての契約店への注意喚起	5.1(2)
20		◎	接続パターンに応じたデータ編集	5.2
21		◎	接続 API/電文の編集（定められた桁数への対応を含む。）	5.3
22		◎	事業者識別コードに基づいた電文仕向け/接続 API 呼び出し	5.3
23	セキュリティ	○	本人認証プロセスの導入	6.2
24		◎	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)
25		!	利用者を特定するために必要な情報の受領・確認	6.2(2)
26		△	決済時における本人認証	6.2(3)
27		◎	QR コード等の有効時間の設定（目安：5 分）	6.3(1)
28		!	QR コード等の残時間表示、自動更新	6.3(1)

			等のスムーズな決済を実現する機能の実装	
29	セキュリティ	◎	QR コード等の再発行の際の従前のQRコード等の無効化	6.3(2)
30		!	QR コード等の再発行時による不正発生抑止手段の導入	6.3(2)
31		◎	オンラインによる表示処理（ただし、一時的なオフラインによる表示処理は一定の条件で許容）	6.4(1)
32		◎	決済時における取引検証	6.4(2)
33		◎	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(3)
34		△	事後的な不正検証に必要な情報・データの保存	6.4(4)
35		△	システム間の情報連携におけるリスク検証	6.5 別紙 1
36		（〇）	（35 の検証を行った場合）発見された脆弱性への対応	6.5
37		!	システム面・体制面でのセキュリティ対策	6.6

【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

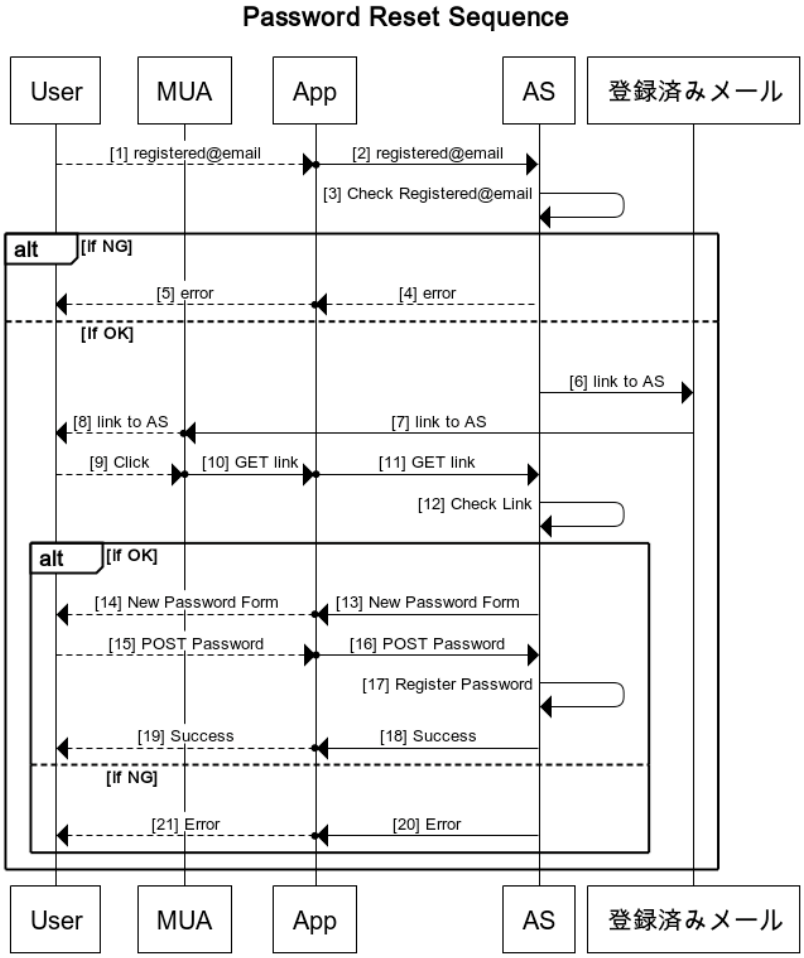
点検にあたっては、シーケンス図とその解説を作成、それぞれを BCM 原則に照らして評価し、プロトコルとしての安全性を見て、リスク評価をする。

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