IMES DISCUSSION PAPER SERIES

多様化するリテール取引システムのセキュリティ:
ビジネスリスク管理に焦点を当てて

宇根正志(うねまさし)・沖野健一(おきのけんいち)

Discussion Paper No. 2020-J-5

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒103-8660 東京都中央区日本橋本石町 2-1-1

IMES Discussion Paper Series 2020-J-5
2020 年 3 月

多様化するリテール取引システムのセキュリティ:
ビジネスリスク管理に焦点を当てて

宇根正志(うねまさし)*・沖野健一(おきのけんいち)**

要　　旨

近年、実店舗で現金を使わずに商品やサービスを購入できるリテール取引システムが多様化している。支払いに当たり、専用端末ではなくスマートフォン等の汎用モバイル端末を用いる取引が広がっているほか、顧客自身がモバイル端末の通信網を介して決済事業者と直接通信することも行われている。また、QR コードの利用や暗号資産による取引もみられている。本稿では、こうした最近のリテール取引システムの特徴を決済事業者により取引が承認されるタイミングや取引承認を要請する主体等の見地から類型化し、各類型についてビジネスリスク管理の観点から、想定される攻撃やセキュリティ対策の方針を検討する。

キーワード：暗号資産、クレジットカード取引、セキュリティ、電子マネー取引、ビジネスリスク管理、リテール取引システム、QR コード

JEL classification: L86、L96、Z00

*　日本銀行金融研究所企画役（E-mail: masashi.une@boj.or.jp）
**　日本銀行金融研究所企画役補佐（E-mail: kenichi.okino@boj.or.jp）

本稿の作成に当たっては、九州大学教授の櫻井幸一氏、元金融研究所テクニカルアドバイザーの廣川勝久氏から有益なコメントを頂戴した。ここに記して感謝したい。ただし、本稿に示されている意見は、筆者たち個人に属し、日本銀行の公式見解を示すものではない。また、ありうべき誤りはすべて筆者たち個人に属する。

目　次

１．はじめに

近年、実店舗で商品やサービスを購入する際に、紙幣や硬貨のやり取りの代わりに、取引金額や取引当事者のアカウント等にかかるデータのやり取りにより支払いを行うシステムが一般的になってきている（日本銀行決済機構局［2018］、山本［2017］）。本稿では、そのようなシステムを「リテール取引システム」と呼ぶ。

かつてのリテール取引システムでは、店舗の専用端末と顧客の IC カードが用いられることが多かったが、最近は店舗と顧客の双方において、スマートフォンやタブレット PC 等の汎用モバイル端末が広く使われている。また、QR コードを用いて取引当事者間でデータをやり取りする方式が注目を集めているほか、一部ではビットコイン等の暗号資産による支払いも行われている[1,2]。さらには、SNS（social networking service）と連動した送金も実用化されている[3]。こうしたリテール取引システムの変化により新たなセキュリティリスクが発生しており、ビジネスリスク管理の観点から対応を講じておくことが求められる。

リテール取引システムにおけるビジネスリスク管理については、これまでに多くの文献で分析・議論されている。例えば、中山・太田・松本［1999］や鈴木・廣川・宇根［2008］では、電子マネー取引のシステムを対象に電子マネーの偽造や二重使用等への対策等を示している。もっとも、いずれも IC カードを利用するシステムのモデルを主に想定しており、最近のリテール取引システムの特徴を十分には反映していない。他方、廣川［2010］では、取引当事者間の通信に非接触インタフェースを用いるシステムを対象としており、携帯電話を端末として利用するケースも想定するなど、より一般的なモデルとなっている。

そこで本稿では、廣川［2010］が対象としたリテール取引システムを参照しつつ、最近のリテール取引システムの特徴を考慮したモデルを設定し、想定される主な攻撃と対策方針を検討する。2 節で検討対象とするモデルを説明し、3 節で想定される主な攻撃とその対策の方針を示す。4 節では、QR コードを用いる方式と暗号資産による支払いのそれぞれについて、3 節での分析を踏まえてビジネスリスク管理上の留意点を考察する。

---

1 これらが注目を集める背景としては、①電子レシートや購買履歴データの活用ニーズの高まり、②インバウンド旅行者の取り込み、③スマートフォンアプリとインターネットを活用した支払いサービスの普及、等が挙げられる（経済産業省［2018］）。中でも QR コード方式は国によっては広く使われていることから、上記②への対応として普及を推進する動きがみられている。

2 ビットコイン等は、以前は「仮想通貨（virtual currency）」や「暗号通貨（crypto-currency）」と呼ばれていたが、近年では「暗号資産（crypto-asset）」と呼ぶことが一般的（Financial Stability Board [2018]および 2019 年 6 月 7 日に公布された改正資金決済法）。

3 QR コードを用いる方式や SNS と連動する方式を含むキャッシュレス決済の普及を展望したキャッシュレス・ビジョンが公表されている（経済産業省［2018］）。

２．リテール取引システムの構成

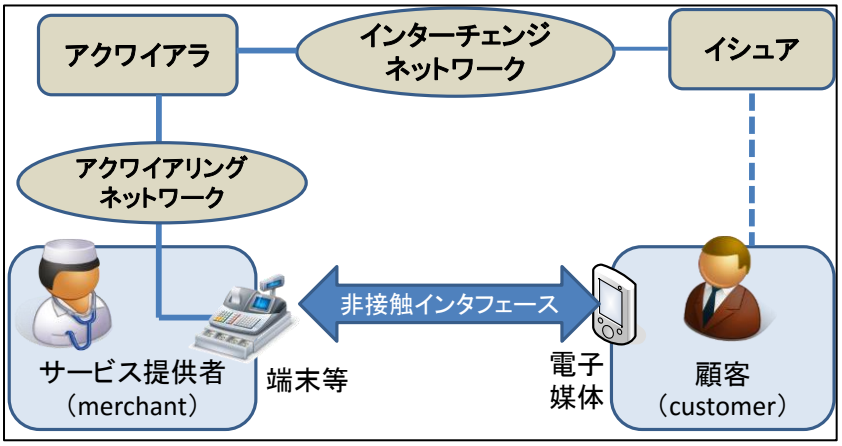
（１）廣川のモデル

イ．エンティティ

廣川［2010］によるリテール取引システムのモデルは、①イシュア（カード等の発行会社／発行銀行）、②アクワイアラ（加盟店契約会社／提携銀行）、③サービス提供者（加盟店／発行銀行または提携銀行の顧客窓口等）、④顧客（カード所持者／口座保有者）の４種類のエンティティからなる（図表１を参照）[4,5]。

顧客が用いる「電子媒体」としては、従来から使用されている磁気カードやICカードに加えて非接触型のICカードや非接触インタフェース機能付きの携帯電話が想定されている[6]。一方、サービス提供者が用いる「端末等」としては、各リテール取引用の専用端末（店舗の専用端末のうち非接触型のICカード対応端末）が利用される。いずれも、リテール取引システムの運営主体であるイシュアまたはアクワイアラが指定する機種であるほか、一定の管理条件の下で運用される。また、顧客とイシュアの間の通信はサービス提供者を経由して行われる。

図表１　廣川のリテール取引システムのモデル



資料：廣川［2010］

[4] この４種類のエンティティからなるモデルは、欧州決済協議会（European Payments Council）によるモバイル決済のホワイト・ペーパーでも議論の前提とされている（European Payments Council [2012]）。

[5] アクワイアラはサービス提供者（加盟店等）を募集し取り纏める役割を担う。イシュア自身で手掛けるよりも多くのサービス提供者をリテール取引システムに取り込むことが可能となる。

[6] 非接触型のICカードあるいはNFC（Near Field Communications）やブルートゥース（bluetooth）等の非接触インタフェースを有した（スマートフォン登場前の）携帯電話を想定しており、後出する汎用モバイル端末とは異なる。

ロ．一連の処理

リテール取引システムにおける処理は、支払処理と決済処理からなる。支払処理は、サービス提供者と顧客間での取引情報の送受信からサービス提供者が取引金額相当の金銭的価値の請求権を取得するまでのプロセスを指す。また、決済処理は、サービス提供者がイシュアに対する金銭的価値の請求権に基づいて金銭的価値を取得するまでのプロセスを指す[7]。

廣川のモデルでは、支払処理および決済処理として以下の仕組みを想定している。

― 支払処理 ―

（A）サービス提供者は端末等（リテール取引用の専用端末）を使って顧客と通信する。

（B）サービス提供者はアクワイアラ経由でイシュアに取引の承認を要請する。

（C）イシュアは、承認の可否を決定し、その結果をアクワライア経由でサービス提供者に伝達する[8]。イシュアは、承認に際し顧客に直接問い合せる場合もある。イシュアが取引を承認すれば、顧客からサービス提供者への支払いが完了し、サービス提供者はイシュアに対する金銭的価値の請求権を取得する。

― 決済処理 ―

支払処理が完了した後、サービス提供者はイシュアに対する金銭的価値の請求権に基づいて金銭的価値を取得する。

ハ．イシュアによる取引の承認

イシュアによる取引の承認の形態は、リテール取引システムのセキュリティにおいて重要なポイントとなる。上記ロ．で示した支払処理の流れには、次の 2 つのケースがある。

まず、顧客とサービス提供者が支払処理を実行する過程で、その取引データをイシュアが即時に承認してはじめて金銭的価値の請求権をサービス提供者に認めるというケース（「即時承認型」と呼ぶ）がある。

---

[7] 詳しくみると、まずサービス提供者がアクワイアラから、次いでアクワイアラがイシュアから、さらにイシュアが顧客から金銭的価値を取得するという流れで処理が構成される。

[8] イシュアが実装する承認処理手順は個々のシステムにおけるビジネスリスク管理等に依存する。例えば、対面取引の承認の可否については、取引場所にかかる情報（店舗の地理的情報等）を受信し、直近の取引場所と時刻を参照しつつ、現在の取引場所への物理的な移動可能性を判断材料の一つとすることが考えられる。

また、イシュアが事前に指定した一定の条件内で支払いにかかる処理を実行する場合には、イシュアからその都度承認を受けなくても、顧客とサービス提供者との間で処理を実行した時点でイシュアに対する金銭的価値の請求権をサービス提供者に認めるケース（「条件指定型」と呼ぶ）がある[9]。

なお、条件指定型において支払処理の内容は次のようになる。

― 支払処理（条件指定型の場合） ―

（A）サービス提供者は端末等（リテール取引用の専用端末）を使って顧客と通信する（即時承認型と同じ）。

（B’）サービス提供者は、当該取引をイシュアが事前に指定した条件内のものと判定した場合、イシュアに対する金銭的価値の請求権を取得する（即時承認型との違い）。

― 支払処理は上記（A）および（B’）で完結し、下記（C’）は後刻実施される―

（C’）イシュアは、事後的に当該取引データに問題がないことを確認し、その結果をアクワイアラ経由でサービス提供者に伝達する。イシュアは確認に際し顧客に直接問い合せる場合もある。なお、即時承認型と異なり、（C’）は決済処理の一部となる。

即時承認型では、仮に不正な処理が顧客やサービス提供者において発生したとしても、金銭的価値の請求権をサービス提供者が取得する前にイシュアが承認の可否を決定する段階で不正な処理を検知できる可能性がある。

一方、条件指定型では、こうした不正な取引をイシュアが支払いの時点では検知する機会がなく、取引結果に基づく請求に対する決済の時点での検知になるため、不正な取引のリスクは即時承認型に比べて高まる可能性がある。

（２）最近のリテール取引システムに加わった特徴

最近のリテール取引システムでは、顧客やサービス提供者がスマートフォンやタブレット PC 等の汎用モバイル端末に専用の「アプリ」（アプリケーション・

9 例えば、少額でのクレジットカード取引において、サービス提供者がイシュアの承認を取引時点で求めることなく支払いを完了させるケースが相当する。このほか、顧客が事前にイシュアから金銭的な価値を示すデータを入手し、取引時に支払金額に相当するデータをサービス提供者に送信するというケースもありうる。こうしたケースの 1 つである電子現金方式では、イシュアが金銭的な価値を示すデータにデジタル署名を付与し、それによってデータに一定の金銭的な価値を付与する（森畠ほか［1997］）。電子現金方式のシステムでは、その運営主体を介さず、複数の利用者間で価値データを転々流通させることが想定されている（中山・太田・松本［1999］）。もっとも、筆者たちが知る限り、最近、このようなシステムが実運用されている例はないため、本稿では検討対象外とする。

ソフトウェア）をインストールして使用するケースが多い。このケースでは、リテール取引システムの運営主体であるイシュアまたはアクワイアラ（以下、特に断らない限り、運営主体を構成する両者を総称してイシュアという）は、アプリを開発しモバイル端末にインストールさせることにより、IC カード等のハードウェアの配付や店舗の専用端末の設置及びそのメンテナンスを行わずに新たな支払手段を提供できる。

もっとも、モバイル端末にはさまざまな機種が存在し、それらが標準的に装備する機能は異なる。また、出荷後にインストールされるアプリも顧客やサービス提供者によって異なる。こうしたことから、顧客やサービス提供者のモバイル端末に関して、イシュアがセキュリティ・パッチの適用や OS のアップデート等の状況を管理することは困難である。その結果、顧客やサービス提供者が当該アプリをインストールしたモバイル端末を自ら悪用するリスクや、不正にインストールされたマルウェア等によって第三者に操作されるリスクがある。

一方、顧客がモバイル端末を介してイシュアと直接通信できることは、セキュリティ上重要なポイントである。例えば、顧客がイシュアに取引の承認を直接要請し、承認が得られてはじめて、サービス提供者がその取引にかかる支払いをイシュアから受けられるというシステムが想定される[10]。こうしたシステムでは、仮にサービス提供者が不正な取引を実行しようとしても、顧客からの承認要請の時点でイシュアが不正を検知できる余地が生まれ、サービス提供者による不正のリスクが軽減されうる。

（３）検討対象とするシステムのモデル

イ．廣川のモデルの拡張

本稿では、本節（２）で述べたリテール取引システムの変化点を考慮し、汎用的なモバイル端末の利用、および、顧客によるイシュアへの直接的な承認要請を加えるかたちで廣川のモデルを拡張する。

廣川のモデルにおける「電子媒体」と「端末等」の対象を汎用的なモバイル端末の利用にも拡大するにあたっては、イシュアやアクワイアラの管理下にない状況を想定したモデルとする。

そこで、「電子媒体」、「端末等」に汎用モバイル端末も含め、以下ではそれぞれ「C 端末（顧客＜customer＞の端末）」、「M 端末（サービス提供者＜merchant＞の端末）」と呼ぶ。後述するセキュリティの検討では、C 端末や M 端末が不正に

10 サービス提供者（店舗等）が取引データを埋め込んだ QR コードを生成し、顧客が自分のモバイル端末でそれを読み取ってイシュアに承認を要請するケースが考えられる。もっとも、顧客が直接イシュアと通信することが技術的に可能であったとしても、取引発生の都度、イシュアに対して必ず承認を要請するとは限らない。少額取引であれば、取引に伴うリスクと取引の承認を要請するコストを勘案し、リアルタイムで承認を要請しないケースもありうる。

操作されるケースを考える。

まず、即時承認型の場合、サービス提供者がイシュアに支払いの承認を要請するケースだけでなく、顧客がサービス提供者を介さずにイシュアと直接通信し承認を要請するケースも対象とする。本稿では、サービス提供者が承認を要請する形態を「M＜merchant＞要請型」と呼び、顧客が承認を要請する形態を「C＜customer＞要請型」と呼ぶ[11]。

一方、条件指定型の場合、本稿では、金銭的価値を取得するための取引データの提示（請求）をサービス提供者から行う形態（「M＜merchant＞請求型」と呼ぶ）を対象とする。顧客から請求を行う形態（顧客請求型と呼ぶ）もありうるが、顧客には（サービス提供者に比較すれば）決済を進める強いインセンティブはなく、顧客の請求に依存する形態では、その分未払いリスクは比較的高いと思われる[12]。こうしたリスクをあえて冒してまで、顧客請求型のモデルでリテール取引システムを構築するメリットはなく一般的なリテール取引システムとして想定しにくいことから、本稿では対象外とする。

本節（１）ハ．で示したように、イシュアによる支払いの承認の形態として、即時承認型と条件指定型がある。これらを、本節（３）イ．で説明した内容でそれぞれ拡張し、即時承認型である M 要請型と C 要請型、および、条件指定型である M 請求型の計 3 つのタイプを検討する。廣川のモデルと本稿のモデルの比較を図表 2 に、本稿のモデルにおける 3 つのタイプを図表 3 に、それぞれ示す。なお、図表 3 における各タイプは、「イシュアによる取引の承認」と「イシュアへの要請・請求の主体」を基にした概念上の分類であり、実際に市中で提供されている特定のサービスに直接対応するものではないことに留意されたい。

ロ．3 つのタイプにおける処理の流れ

支払処理は、サービス提供者と顧客間での取引情報の送受信から開始される。ここでは、取引情報として、①サービス提供者のアカウント、②顧客のアカウント、③取引実行時刻のタイムスタンプ、④取引金額、を想定し、これらをまとめて「取引データ」と呼ぶ[13]。取引を開始するタイミングでは、サービス提供者は、自分のアカウント、タイムスタンプ、金額を知っているものの、顧客のアカウン

---

11 M 要請型では、承認要請はサービス提供者からアクワイアラを介してイシュアに送信され、承認結果は逆の流れで送信されるとする。イシュアとアクワイアラが同一のエンティティの場合、サービス提供者がイシュアに承認を直接要請する場合と同等になる。

12 顧客には決済の遅延や未払いによる信用低下を避けたいという動機が働くため、顧客請求型では未払いが頻発するとまでは言えないかもしれない。

13 タイムスタンプによって、取引データが実際に取引実施のタイミングで生成されたものであることを確認するものとする。

図表 2 廣川のモデルと本稿のモデルの比較

	廣川のモデルでの想定	本稿のモデルでの想定
主に想定している取引	非接触型のICカード（および携帯電話）を使ったクレジットの取引	汎用的なモバイル端末を使ったクレジット・電子マネーの取引、QRコードを使った取引や暗号資産の取引
サービス提供者の端末	運営主体が指定するリテール取引用の専用端末であり、一定の管理条件で運用	汎用的なモバイル端末（左記の端末と比較して、不正に操作されるリスクが高い）
顧客の端末	ICカード、または、ICカード相当の機能を持つ携帯電話	
イシュアに対する取引承認の要請	サービス提供者のみ	サービス提供者、または、顧客

トを知らない。顧客は、自分のアカウント、金額を知っているものの、サービス提供者のアカウント、タイムスタンプを知らない。そこで、顧客とサービス提供者は、自分が知らないデータを相手から受信し、取引データにかかる自分の認識と相手の認識が一致していることを確認する。

こうした点を踏まえ、3つのタイプにおける支払処理の流れをそれぞれ以下のとおり想定する。ここでは、いずれも支払処理をサービス提供者が起動するケースに焦点を当てる。

図表 3　本稿のモデルにおける 3 つのタイプ

タイプ名	イシュアによる取引の承認	イシュアへの要請・請求の主体
即時承認・M要請型	イシュアが即時に実施	サービス提供者が承認を要請
即時承認・C要請型		顧客が承認を要請
条件指定・M請求型	イシュアが事前に指定した一定の条件内であれば、イシュアからその都度承認を受けなくても、金銭的な価値の請求権がサービス提供者に認められる。	サービス提供者が金銭的な価値を取得するための取引データを提示（請求）

【即時承認・M要請型】（図表4左を参照）

（A） サービス提供者は、サービス提供者のアカウント、金額、タイムスタンプを顧客に送信する。

（B） 顧客は、上記（A）のデータを受信後、それらに顧客のアカウントを追加したものを取引データとしたうえで、取引データと「顧客確認済」を示すデータをサービス提供者に送信する。

（C） サービス提供者は、取引データ等をイシュアに送信し承認を要請する。

（D） イシュアは、取引データ等を確認し、承認の可否を決定してサービス提供者に送信する。

（E） 上記（D）の承認可否の結果は、顧客にも送信される。

（F） 後刻、イシュアは取引データ等に基づいて、金銭的価値の移転等の決済にかかる処理を実行する。

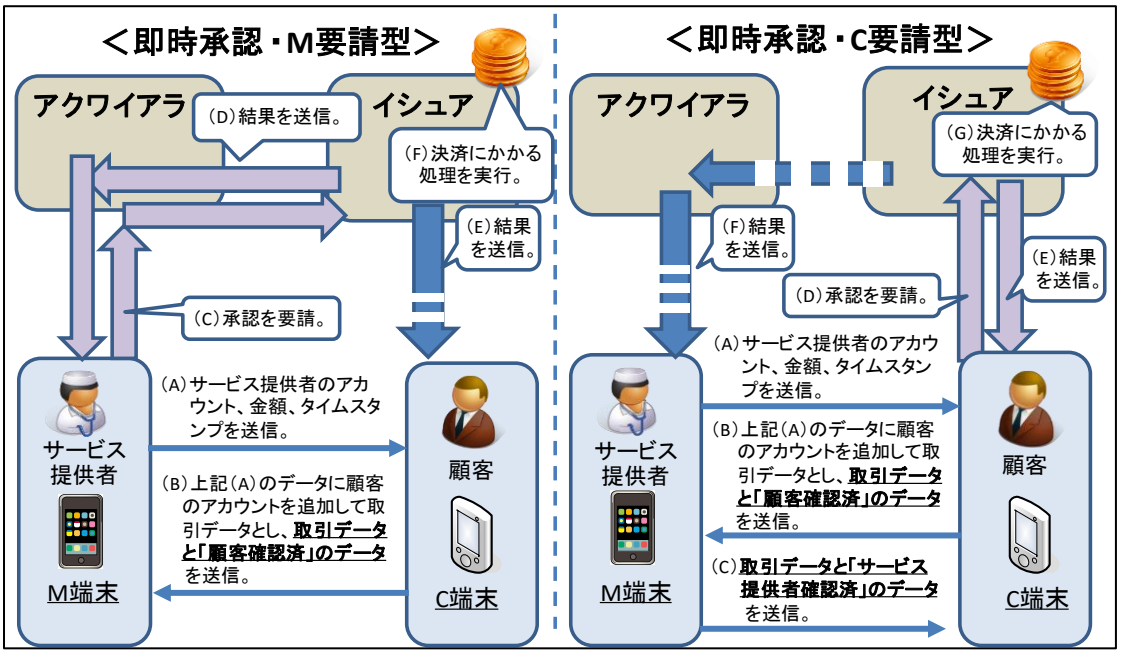
【即時承認・C 要請型】（図表 4 右を参照）

（A） サービス提供者は、サービス提供者のアカウント、金額、タイムスタンプを顧客に送信する。

（B） 顧客は、上記（A）のデータを受信後、それらに顧客のアカウントを追加したものを取引データとしたうえで、取引データと「顧客確認済」を示すデータをサービス提供者に送信する。

（C） サービス提供者は、上記（B）のデータを確認したうえで、取引データと

図表 4　即時承認・M 要請型と即時承認・C 要請型の処理の流れ（概念図）



「サービス提供者確認済」を示すデータを顧客に送信する。

(D) 顧客は、取引データ等をイシュアに送信し承認を要請する。

(E) イシュアは、取引データ等を確認し、承認の可否を決定して顧客に送信する。

(F) 上記（E）の承認可否の結果は、サービス提供者にも送信される。

(G) 後刻、イシュアは取引データ等に基づいて、金銭的価値の移転等の決済にかかる処理を実行する。

【条件指定・M 請求型】（図表 5 を参照）

(A) サービス提供者は、サービス提供者のアカウント、金額、タイムスタンプを顧客に送信する。

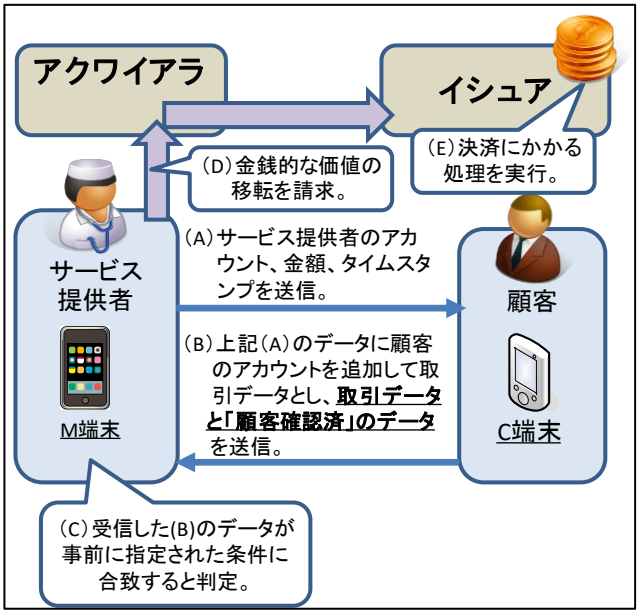
(B) 顧客は、上記（A）のデータを受信後、それらに顧客のアカウントを追加したものを取引データとしたうえで、取引データと「顧客確認済」を示すデータをサービス提供者に送信する。

(C) サービス提供者は、上記（B）のデータを受信し、イシュアが事前に指定した条件に合致するか否かを判定する（合致する場合、顧客からサービス提供者への支払いにかかる処理はこの時点で完了する）。

(D) 後刻、サービス提供者は、アクワイアラ経由でイシュアにそれらを送信して、金銭的な価値の移転をイシュアに請求する。

(E) イシュアは、上記（D）で受信したデータに基づいて金銭的な価値の移転等の決済処理を実行する。

図表 5　条件指定・M 請求型における処理の流れ（概念図）



条件指定型では、顧客からサービス提供者への支払処理が完了する前に取引の内容をイシュアが確認する機会がないことから、イシュアが事前にどのような条件を指定するかが重要となる。条件は取引の形態に依存すると考えられるが、その条件によって、イシュアが不正な支払いにかかる処理のリスクを制御し、そのビジネス上・技術上のリスク（の期待値）を許容できるレベルとする必要がある[14]。

なお、上記の 3 つのタイプでは、いずれも、支払処理が完了後、事前にイシュアが決定したタイミングで決済処理が実行されるものとする。

３．想定される攻撃と対策の方針にかかる検討

（１）攻撃の目的と攻撃者の能力

本稿では、モデルを構成するエンティティのうち、顧客が攻撃者となる場合とサービス提供者が攻撃者となる場合を想定する[15]。そのうえで、攻撃者は、支払いの金額を自身の都合の良いように改変することを試みるものとする。すなわち、顧客が攻撃者の場合、取引データにおける金額を実際のものよりも減額することを試み、サービス提供者が攻撃者の場合には、それを増額することを試みるものとする[16]。イシュアとアクワイアラに関しては、信頼できるエンティティと仮定し、攻撃に関与しないものとする。

攻撃者の能力に関しては、マルウェア等の不正なプログラムを自らの端末に仕込んだり、取引相手方の端末に送り込んだりすることにより、端末を不正に操作できる場合も想定する[17]。なお、イシュアが管理する実行環境が端末に設定さ

---

14 リスク管理上は、C 端末や M 端末についてイシュアが管理可能な環境下でのみ取引データを生成できるようにすること、例えば、端末にセキュア・エレメント（secure element）やトラスティッド・エグゼキューション・エンバイロメント（trusted execution environment）を実装させることが考えられる。セキュア・エレメントは、暗号処理等のセキュリティ機能を有し、外部からの物理的攻撃（例えば、IC チップのカバーを除去し内部構造を観察することにより暗号鍵を推定する攻撃）に対しても高い安全性を有するモジュールの総称である。ハードウェアとソフトウェアを組み合わせて実現され、スマートフォン上の通常の実行環境から物理的かつ論理的に分離された状態で使用できる。トラスティッド・エグゼキューション・エンバイロメントは、主にソフトウェアを用いて通常の実行環境から論理的に分離された実行環境を実現する技術であり、物理的な攻撃は想定されていない。これらに関しては、宇根・廣川［2017］を参照されたい。

15 顧客やサービス提供者が組織の場合、一部の内部者が攻撃者となるケースが想定される。

16 なお、攻撃としては架空の取引を捏造することも考えうるが、それには実存しない取引を相手方に誤認させる（または存在を隠ぺいする）必要がある点で、改変（実際に存在する取引に対する取引金額の改ざん）よりも難易度が高いため、本稿では議論の対象としない。

17 中山・太田・松本［1999］や鈴木・廣川・宇根［2008］では、電子マネー取引のシステムにおいて、攻撃者が IC カードを不正に用いる状況や端末を不正に操作する状況を想定しているが、これらは C 端末と M 端末の不正操作の想定にそれぞれ対応する。

れている場合、そうした実行環境での処理を攻撃者が不正に操作することは困難であるものとする[18]。

通信路上のデータに関しては、攻撃者は、それを盗取したり改変したりすることができるとする。ただし、アクワイアラとイシュアの間の通信路については、暗号化等の手段が講じられており、それへの攻撃は成功しないものとする。

（２）検討対象とする攻撃

２節（３）ロ．で示した 3 つのタイプに対して上記の攻撃の成否を検討する。最近のリテール取引システムにおいて新たに発生しうるリスクを明らかにするために、最近のシステムの新たな特徴に焦点を当てて、従来のシステムにおいて主に想定されていた攻撃との差分を分析対象とする。

3 つのモデルに共通する差分は、M 端末が専用端末から汎用モバイル端末となり、攻撃者によって不正に操作されうることである。そこで、サービス提供者が自らの端末（M 端末）のみを不正操作する場合と、サービス提供者あるいは顧客が自分と相手方の双方の端末を不正操作する場合を検討する。

ただし、即時承認・C 要請型については、顧客が自らの端末（C 端末）を用いてイシュアに承認を直接要請するという新しい形態であることから、上記の 2 つの場合に加えて、顧客が自らの端末のみを不正に操作する場合も想定する。

（３）即時承認・M 要請型の分析

イ．サービス提供者が攻撃者の場合

（イ）M 端末のみを不正に操作するケース

サービス提供者が取引金額を増額してイシュアに送信し、承認を要請することが想定される。

対策の方針としては、取引データが顧客の意思に基づいていることをイシュアが確認することが考えられる。例えば、顧客が C 端末で取引データを確認した後、自らのデジタル署名を取引データに付与し、イシュアがそれを検証することや、イシュアが C 端末に取引データを送信して顧客に確認を求めることが挙げられる。

（ロ）M端末とC端末の両方を不正に操作するケース

サービス提供者が M 端末を不正に操作し C 端末に送信する取引金額を増額する一方、C 端末に不正なプログラムを仕込むことなどにより C 端末の画面上には増額前の金額が表示されるようにし、顧客に金額を誤認させることが考えら

[18] こうした対策は以下で検討するケースに共通するため、各ケースで個別には言及しない。

れる[19]。この場合、イシュアが顧客に取引データの内容を確認させたとしても、C 端末上に増額前の金額が表示されていれば、実質的には顧客による確認は意味を持たなくなる[20]。

対策の方針としては、まず、①不正なプログラムが C 端末に送り込まれるのを防ぐことである。顧客が C 端末に不審なアプリケーション・プログラムのインストールを行わないようにする、C 端末の脆弱性を極力排除するように OS 等のアップデートを実行するなどの運用面での対応が挙げられる。また、②承認要請として送信された取引データが顧客の意思に基づいていることを、イシュアが安全に確認できるようにすることも考えられる。例えば、イシュアから顧客に対し、M 端末への通信に用いた経路（例えば NFC）とは別の経路（例えばメールや SNS 等）を使って取引内容を安全に確認できるようにすることが考えられる[21]。

ロ．顧客が攻撃者の場合

顧客が C 端末を不正に操作し M 端末に送信する取引金額を減額する一方、M 端末に不正なプログラムを仕込むことなどにより M 端末の画面上には減額前の金額が表示されるようにし、サービス提供者に金額を誤認させることが考えられる。その場合、サービス提供者は、不正な取引データを（それと気づかず）イシュアに送信して承認を要請するほか、イシュアが承認した旨を M 端末で受信しても攻撃されていると気づかない可能性がある。また、顧客は、暗号通信プロトコル等の処理を M 端末において無効化することも考えられる[22]。

対策の方針としては、まず、①不正なプログラムが M 端末に送り込まれるのを防ぐことである。また、②M 端末が不正に操作されたとしても、承認を要請された取引データがサービス提供者の意思に基づいていることをイシュアが安全に確認できるようにすることも考えられる。

---

19 スマートフォンの場合、マルウェアが OS の脆弱性を悪用して管理者権限を奪取し、画面に表示する情報を操作するという攻撃が知られている。例えば、不正な画面を真の画面の上に表示させるスクリーン・オーバーレイ等が挙げられる（井澤・五味［2016］、Mathews [2018]）。

20 イシュアが承認後に結果を顧客に直接送信する場合でも、あたかも正規の取引データによって承認されたように C 端末上に表示させることが考えられる。

21 ここでの趣旨は、別の経路を使って顧客に確認を求める方が、同一の経路を用いるよりも、攻撃者による改変等を受ける確率が低くなることが期待できるということである。

22 例えば、M 端末に送り込まれた不正なプログラムが（M 端末の）OS の管理者権限を奪取し、暗号通信プロトコルにかかる処理を中断したり、スキップしたりすることがありうる。

（４）即時承認・C 要請型の分析

イ．サービス提供者が攻撃者の場合

サービス提供者が M 端末と C 端末の両方を不正に操作するケースを考える。サービス提供者が M 端末を不正に操作し C 端末に送信する取引金額を増額する一方、C 端末に不正なプログラムを仕込むことなどにより C 端末の画面上には増額前の金額が表示されるようにし、顧客に金額を誤認させることが考えられる。

対策の方針は、即時承認・M 要請型において顧客が攻撃者となる場合（本節（３）ロ.）とパラレルに考えることができる。すなわち、①不正なプログラムが C 端末に送り込まれるのを防ぐことや、②C 端末が不正に操作されたとしても、承認を要請した取引データが顧客の意思に基づいていることをイシュアが安全に確認できるようにすることが考えられる。

ロ．顧客が攻撃者の場合

（イ）C 端末のみを不正に操作するケース

顧客が取引金額を減額してイシュアに送信し、承認を要請するという攻撃が想定される。対策の方針は、即時承認・M 要請型においてサービス提供者が攻撃者となる場合（本節（３）イ.（イ））とパラレルに考えることができる。すなわち、取引データがサービス提供者の意思に基づいていることを、イシュアが安全に確認できるようにすることが考えられる。

（ロ）C 端末と M 端末の両方を不正に操作するケース

顧客が C 端末を不正に操作し M 端末に送信する取引金額を減額する一方、M 端末に不正なプログラムを仕込むことなどにより C 端末の画面上には減額前の金額が表示されるようにし、サービス提供者に金額を誤認させることが考えられる。

対策の方針は、即時承認・M 要請型においてサービス提供者が攻撃者となる場合（本節（３）イ.（ロ））とパラレルに考えることができる。すなわち、①不正なプログラムが M 端末に送り込まれるのを防ぐことや、②M 端末が不正に操作されたとしても、承認を要請された取引データがサービス提供者の意思に基づいていることを、イシュアが安全に確認できるようにすることが考えられる。

（５）条件指定・M 請求型の分析

イ．サービス提供者が攻撃者の場合

（イ）M 端末のみを不正に操作するケース

サービス提供者が取引金額を増額してイシュアに送信し、承認を要請するこ

とが想定される（本節（３）イ.（イ）と同様)。

ただし、即時承認・M 要請型とは異なり、イシュアが C 端末に取引データを送信して顧客に確認を求める手段が存在しない。そのため、対策の方針としては、M 端末においてサービス提供者による取引データの改変を防ぐことよりない。例えば、イシュアによって管理された実行環境を M 端末内に準備し、その実行環境内でのみ取引データにかかる処理を実行するという方法が考えられる。

（ロ）M 端末と C 端末を不正に操作するケース

サービス提供者が M 端末を不正に操作し C 端末に送信する取引金額を増額する一方、C 端末に不正なプログラムを仕込むことなどにより C 端末の画面上には増額前の金額が表示されるようにし、顧客に金額を誤認させることが考えられる（(本節（３）イ.（ロ）と同様)。

対策の方針は、①イシュアによって管理された実行環境を M 端末内に準備することなどにより M 端末においてサービス提供者による取引データの改変を防ぐほか、②不正なプログラムが C 端末に送り込まれるのを防ぐことが考えられる。

ロ．顧客が攻撃者の場合

顧客が C 端末と M 端末を不正に操作できるケースを考える。顧客が C 端末を不正に操作し M 端末に送信する取引金額を減額する一方、M 端末に不正なプログラムを仕込むことなどにより M 端末の画面上には減額前の金額が表示されるようにし、サービス提供者に金額を誤認させることが考えられる（(本節（３）ロ．と同様)。さらに条件指定・M 請求型に特有の攻撃として、顧客が少額の取引を繰り返し実施し、一定期間内における取引可能な金額の上限（事前に決定）を超える取引の実行を試みることも想定される。仮に、M 端末がこうした上限を超えているか否かを確認する機能を搭載していたとしても、顧客は、M 端末を不正に操作して上記の機能を無効化することが考えられる。

対策の方針は、①イシュアによって管理された実行環境を C 端末内に準備することなどにより C 端末において顧客による取引データの改変を防ぐほか、②不正なプログラムが M 端末に送り込まれるのを防ぐことが考えられる。

（６）新たなリスクへの対策の方針にかかる考察

これまで分析してきた、各タイプにおける攻撃への対策や留意点をまとめると、図表 6 のようになる。

まず、即時承認型で取引当事者が自らの端末のみを不正に操作するケースでは、イシュアは、承認を要請された取引データが不正なものである可能性に留意し、それが取引相手方の意思に合致していることを確認する必要がある。例えば、

図表 6 各タイプにおける攻撃への対策や留意点

タイプ名	想定される攻撃	対応方針や留意点
即時承認・M要請型	サービス提供者がM端末のみを不正に操作 ＜(3)イ．（イ）＞	取引データが顧客の意思に基づいていることをイシュアが確認（署名による検証や顧客への取引データの送信等）
	サービス提供者がM端末とC端末の両方を不正に操作＜(3) イ．（ロ）＞	不正なプログラムがC端末に送り込まれるのを防ぐ（OS等のアップデートの励行等）、および、取引データが顧客の意思に基づいていることをイシュアが確認（メールやSNS等の別経路を用いての顧客への取引データの送信等）
	顧客がM端末とC端末の両方を不正に操作 ＜(3) ロ．＞	不正なプログラムがM端末に送り込まれるのを防ぐ、および、取引データがサービス提供者の意思に基づいていることをイシュアが確認（別経路を用いてのサービス提供者への取引データの送信等）
即時承認・C要請型	サービス提供者がM端末とC端末の両方を不正に操作＜(4) イ．＞	不正なプログラムがC端末に送り込まれるのを防ぐ、および、取引データが顧客の意思に基づいていることをイシュアが確認（即時承認・M要請型＜(3) ロ．＞と同様）
	顧客がC端末のみを不正に操作＜(4)ロ．（イ）＞	取引データがサービス提供者の意思に基づいていることを、イシュアが確認（即時承認・M要請型＜(3)イ．（イ）＞と同様）
	顧客がM端末とC端末の両方を不正に操作 ＜(4)ロ．（ロ）＞	不正なプログラムがM端末に送り込まれるのを防ぐ、および、取引データがサービス提供者の意思に基づいていることをイシュアが確認（即時承認・M要請型＜(3)イ．（ロ）＞と同様）
条件指定・M請求型	サービス提供者がM端末のみを不正に操作 ＜(5)イ．（イ）＞	M端末においてサービス提供者による取引データの改変を防ぐ（イシュアによって管理された実行環境をM端末内に準備する等）
	サービス提供者がM端末とC端末の両方を不正に操作＜(5) イ．（ロ）＞	M端末においてサービス提供者による取引データの改変を防ぐ（上述の対策）、および、不正なプログラムがC端末に送り込まれるのを防ぐ
	顧客がM端末とC端末の両方を不正に操作 ＜(5) ロ．＞	C端末において顧客による取引データの改変を防ぐ（上述の対策）、および、不正なプログラムがM端末に送り込まれるのを防ぐ

デジタル署名の活用や、取引相手方への取引内容の確認が挙げられる[23]。

また、即時承認型で取引当事者双方の端末が不正に操作されるケースでは、端末において不正なプログラムのインストールを防止することが重要である。もっとも、昨今ではマルウェアの侵入を完全に防ぐことは容易でなく、むしろ不正なプログラムの侵入を前提とした対応を考えておくことも必要である。この点では、イシュアが安全なチャネルで取引相手方の意思を確認することが基本になる。

この間、条件指定型では、イシュアが取引時点で取引相手方の意思を確認する術がないため、技術的な対策としては、各端末に不正なプログラムが送り込まれ

[23] デジタル署名の活用には、すべてのサービス提供者と顧客が署名用の鍵ペアを生成し、署名生成用の鍵を端末内で安全に管理できるようにするとともに、取引実行時には電子証明書の有効性を確認できるようにすることが必要となる。

るのを防ぐとともに、イシュアによって管理された実行環境を両方の端末に準備し、その実行環境において取引にかかる処理をそれぞれ実行するなどの対応が必要となる。運用で対応するのであれば、1 回当たりの取引可能金額を低く抑え、不正な取引によるリスクを低下させることが挙げられる。

４．リテール取引システムの新しいサービスに関する考察

本節では、最近のリテール取引システムの例として、①情報のやり取りに QR コードを用いる方式と、②暗号資産を通じた支払いに焦点を当てて、想定される実現形態の 1 つをモデル化する。そのうえで、2 節と 3 節の検討結果を適用する。

（１）QR コードを用いる方式

イ．顧客提示型とサービス提供者提示型

取引データが埋め込まれる QR コードを用いる方式は、顧客が QR コードをサービス提供者に提示する CPM（Consumer Presented Mode）と、サービス提供者が顧客に提示する MPM（Merchant Presented Mode）に分けられる[24]。

CPM のうち、例えば、以下の方式は即時承認・M 要請型に相当する。（図表 7 左を参照）。①顧客は顧客のアカウント情報等を埋め込んだ QR コードを C 端末に表示する。②サービス提供者は、上記①の QR コードを読み取るとともに、サービス提供者のアカウント、タイムスタンプ、金額等の情報を加えることにより取引データを生成し、取引データと「サービス提供者確認済」を示すデータを顧客に送信する。③顧客は、上記②の取引データを確認し、それと「顧客確認済」を示すデータをサービス提供者に送信する。④サービス提供者は、上記③で受信した取引データを確認し、取引データ等をイシュアに送信して承認を要請する。⑤イシュアは取引の承認の可否を決定し、その結果をサービス提供者と顧客に送信する[25]。

MPM のうち、例えば、以下の方式は即時承認・C 要請型に相当する（図表 7 右を参照）[26]。①サービス提供者は自らのアカウント、タイムスタンプ、金額等

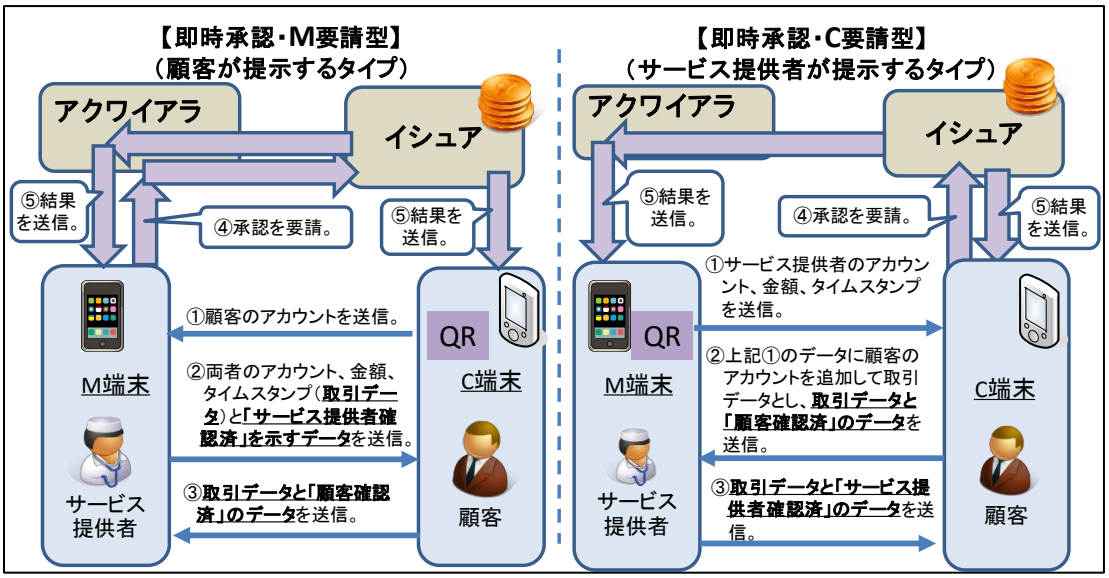
---

[24] CPM および MPM については、キャッシュレス推進協議会が統一技術仕様のガイドラインを公表している（キャッシュレス推進協議会［2019a, b］）。

[25] QR コード自体に埋め込まれているのは図表 7 の①の処理にかかるデータのみであり、図表 7 の②～⑤の処理にかかる通信は、他の電子的な通信手段を用いて行われるか、実装によっては一部省略される可能性もある。

[26] 本稿ではいわゆる動的 QR コードを想定して説明をしているが、静的 QR コード型の MPM の場合も即時承認・C 要請型に含まれる。

図表 7　QR コードを用いる方式のモデルの例（概念図）



を埋め込んだ QR コードを M 端末に表示する。②顧客は、上記①の QR コードを読み取るとともに、顧客のアカウント情報等を加えることにより取引データを生成し、取引データと「顧客確認済」を示すデータをサービス提供者に送信する。③サービス提供者は、上記②で受信した取引データを確認し、それと「サービス提供者確認済」を示すデータを顧客に送信する。④顧客は、取引データ等をイシュアに送信し承認を要請する。⑤イシュアは取引の承認の可否を決定し、その結果をサービス提供者と顧客に送信する。

ロ．セキュリティ対策の方針

即時承認・C 要請型（MPM のモデルの例）についてサービス提供者が攻撃者となる場合のセキュリティ対策を考える。サービス提供者が C 端末と M 端末の両方を不正に操作する状況への対策としては、C 端末への不正なプログラムの送り込みを防ぐことや、C 端末が不正に操作される場合でも、取引データが顧客の意思に基づいていることをイシュアが安全に確認できるようにすることが挙げられる。

もっとも、実際の対策では、QR コードに埋め込まれたデータを人間が読み取ることができない点に留意が必要である。近年、QR コードが偽造され不正なサイトに誘導されるなどの攻撃が知られており（大熊・瀧田・森井［2018］）、サービス提供者が支払金額を正規の金額よりも増額して QR コードを生成・提示したり、承認要請時にイシュアとは別のサイトに顧客を誘導したりする（例えば、サービス提供者の従業員が不正に準備した偽のサーバに対して支払わせること

で当該金額を横取りしてしまう）可能性もある。QR コードに埋め込まれたデータの内容を端末の画面に表示させ、それを取引相手方が確認すれば不正な QR コードを検知できる。しかし、確認が不十分である場合、ビジネスリスク管理上、何らかの対応が必要なケースがありうる[27]。

例えば、C 端末のアクセスをイシュアのサイトに擬した不正なサイトに誘導する攻撃に対しては、接続先のサイトを暗号通信プロトコル等によって認証した際に、その結果（接続先のサイトの正当性）を顧客が正しく認識できるようにすることが求められる。顧客に正しいイシュアのサイトを予め登録させておき、認証時にそのサイトの確認の成否によって C 端末の画面の色を変化させるといった方法も考えられる[28]。

（２）暗号資産による支払い

イ．暗号資産の位置づけ

ビットコイン等の暗号資産の移転による支払いをサービス提供者が認めているケースがある。暗号資産では、取引にかかるデータ（移転先と移転元のアドレス、移転額等）が分散台帳に記録されることによって移転が完了する。その際、台帳を共有するノード（マイナー）群において、移転の正当性（二重使用されていないことなど）が検証されるとともに、移転にかかるデータが別の（複数の）移転にかかるデータと関連付けられる[29]。

暗号資産は、中央集権的な組織が運営するのではなく、分散されたノード群が連携して運営するという考え方に基づいている。そうであれば、ノード群の集合体を上述の各モデルにおける運営主体に相当するものとみなすこともできる。暗号資産では、通常、移転を行うエンティティ、例えば顧客が、移転にかかるデータをノードの 1 つに送信し、一定の時間が経過してそのデータが台帳に記録されたところで移転が完了する[30]。移転にかかるデータが顧客からノードに送信され、他のノードと共有されると、サービス提供者はその移転にかかるデータを確

---

27 このほか、QR コードに関するリスクとして、C 端末に表示された QR コードを第三者が盗撮して自らの支払いに利用するという不正行為（ショルダーハック）の危険性も指摘されている（笹崎ほか［2018］）。

28 一部のブラウザでは、特定の種類のサーバ証明書によってサーバ認証を行う際、ブラウザの画面のアドレスバーの色が変化し、ユーザーが認証結果を容易に認識できるようにしている（三井住友銀行［2017］）。こうしたインタフェースの機能を利用することも考えられる。

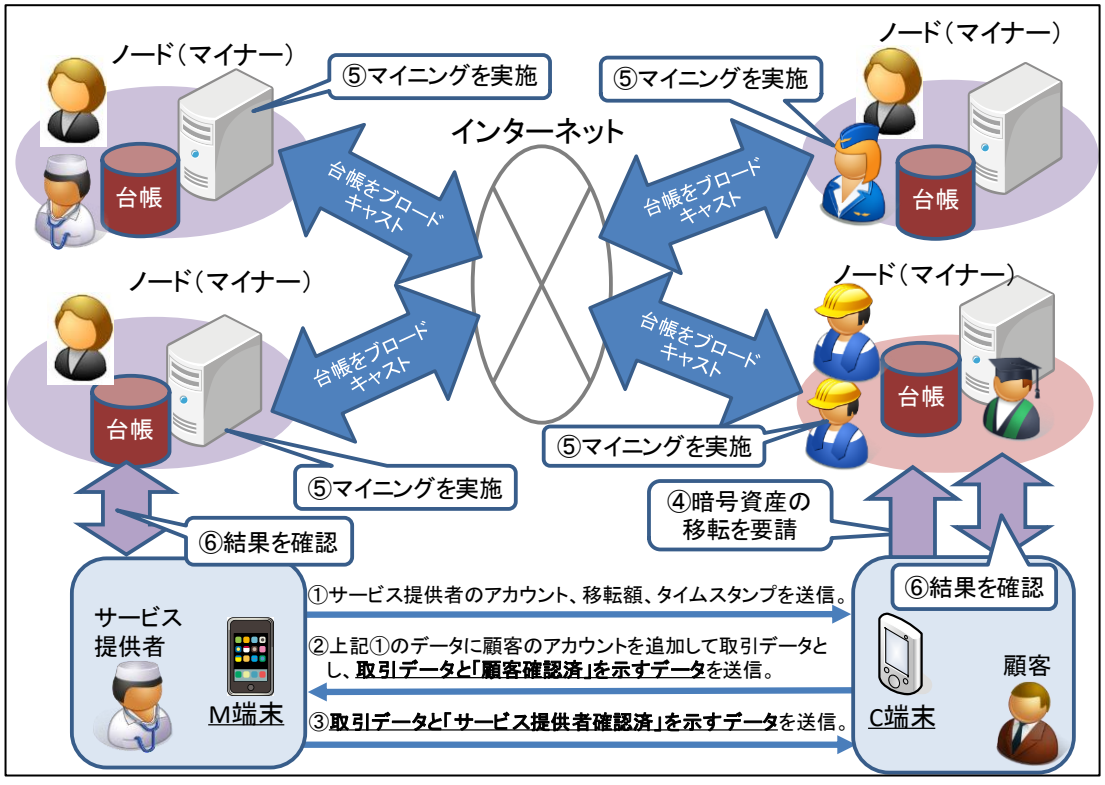
29 ビットコインでは、複数の取引が一定時間毎にブロックと呼ばれるデータとして形成され、過去のブロックとの間でハッシュ値によって関連づけられる。この関連付けにいち早く成功したノードだけが報酬を得られることから、この関連付けを鉱物資源の採掘になぞらえてマイニングという。マイニング競争に敗れたノードは、次のブロックにおけるマイニング競争に備えて関連付けの結果を台帳に反映させるので、すべてのノードで同じ台帳が共有されることになる。

30 ビットコインの場合、移転にかかるデータが台帳に記録されるまでに一定の時間を要するが、これが暗号資産に特有の脆弱性となる可能性がある（詳細は後述）。

認することができる。

このように整理すると、暗号資産を用いる方式は即時承認・C 要請型に近い（図表 8 を参照）[31]。まず、①サービス提供者は、サービス提供者のアカウント、金額、タイムスタンプを顧客に送信する。②顧客は、上記①のデータに自分（顧客）のアカウント情報等を追加して取引データとしたうえで、取引データと「顧客確認済」を示すデータをサービス提供者に送信する。③サービス提供者は、上記②の取引データを確認し、取引データと「サービス提供者確認済」を示すデータを顧客に送信する。④顧客は、ノードに取引データを送信し、暗号資産の移転を要請する。⑤ノードは、要請を受けてブロックを生成し、他のノードにそれを同報通信するとともに（このタイミングでサービス提供者は取引データにかかる移転が進行していることを確認することもできる）、他のノードとともにマイニングを実行する。マイニングが成功すれば、当該取引データにかかる暗号資産の移転が台帳に記録され、移転が完了する。⑥サービス提供者と顧客は、台帳を参照することで、取引データと移転結果の整合性を確認することができる。

図表 8　暗号資産を用いる方式のモデルの例（概念図）



31 上記のケースは、サービス提供者と顧客がノードでない場合を想定したものである。ノードは、通常、取引データを他のノードに送信・共有しつつ、マイニングを実行する。したがって、顧客がノードの場合でも、顧客は他のノードに取引データを送信することとなり、上記と同様に、即時承認・C 要請型に近いと位置づけることができる。

ロ．セキュリティ対策の方針

即時承認・C 要請型でサービス提供者が M 端末と C 端末の両方を不正に操作する状況を想定するならば、対策の方針としては、３節（４）イ．（ロ）で示したように、不正なプログラムが C 端末に送り込まれるのを防ぐことや、C 端末が不正に操作されたとしても、承認を要請した取引データが顧客の意思に基づいていることをイシュアが安全に確認できるようにすることである。

なお、暗号資産による取引では、顧客から取引データがノードに送信され、それがノード群に展開・共有されることから、サービス提供者あるいは顧客が不正な取引データを検知してノード群に報告することができれば、その取引データを含むブロックのマイニングを成立させないことができる場合がありうる。したがって、「イシュアが安全に確認できるようにする」という方針は、そのままでは適用できず、「顧客やサービス提供者が（取引データにかかる暗号資産移転のトランザクションが含まれる）ブロックにアクセスして確認する」と解釈して対応を検討することが求められる。

こうした対策の方針を検討する際には、マイニングの手法によっては、顧客が取引データをノードに送信してから台帳に記録されるまでに相応の時間がかかることに伴う脆弱性に留意する必要がある[32]。例えば、暗号資産がプルーフ・オブ・ワークに基づくブロックチェーンを利用している場合に特有の攻撃として「51%攻撃」が知られている[33]。これは、ノードの集合全体の計算能力の半分を超える計算能力を有するサービス提供者（を含むノードの集合）が存在する場合、そのサービス提供者は（移転額を増額させた）不正な取引データを含むブロックについて秘密裡にマイニングできるという攻撃方法である。顧客が不正な取引データが含まれていることをブロック確定前に検知できない場合、不正な取引データに基づく暗号資産の移転が成立してしまう。マイニング後に顧客が台帳上の不正な取引データを知ることができても、台帳に記録された取引自体は取り消すことができない。このように、個々の暗号資産に特有の脆弱性を悪用されることも想定しつつ、ビジネスリスク管理上望ましい方針を決定することが求められる。

---

32 ビットコインでは、1 つのブロックが台帳に記録されるまでに 10 分程度の時間が必要になるとともに、そのブロックが確定するまでに約 60 分（6 つのブロックが確定する時間）かかる。

33 ノード全体の計算能力の半分以上を特定のノード（の集合）が有していた場合、秘密裡にフォークを形成し、ブロックが確定する直前にそのフォークを他のノードに同報通信することによって、チェーンが形成されつつあった他のブロック（に含まれる取引）を無効化しつつ自分のフォーク（に含まれる取引）を有効化するという攻撃である。最近では、2019 年 1 月にイーサリアム・クラシック（Ethereum Classic）においてこの攻撃が行われたとみられている（Han *et al.* [2019]）。

５．おわりに

本稿では、まず、既存の廣川のモデルを参考にしつつ、近年の新しいリテール取引システムの形態（汎用モバイル端末の利用、顧客によるイシュアへの承認要請等）を考慮して、リテール取引システムのモデルを拡張した。そのうえで、顧客あるいはサービス提供者が取引金額の改変（減額あるいは増額）を試みるケースに焦点を当てて、新たなリスクとなりうる攻撃やそれらへの対策の方針を示した。さらに、QR コードを用いる方式や暗号資産による支払いをモデル化し、想定される攻撃やそれらへの対策の方針を検討した。暗号資産ではプルーフ・オブ・ワークに基づき取引が台帳に記録されるまでのタイムラグを悪用した攻撃についても考慮する必要があるなど、個々のリテール取引システムに特有の脆弱性に留意することも重要である旨を説明した。今後も、本稿のモデルによる検討の枠組みを各種のリテール取引システムに適用し、想定される攻撃や対策の方針について検討を進めていきたい。

以　上

【参考文献】

井澤秀益・五味秀仁、「次世代認証技術を金融機関が導入する際の留意点 : FIDOを中心に」、『金融研究』第35巻第4号、日本銀行金融研究所、2016年、21～54頁

宇根正志・廣川勝久、「モバイル端末による金融サービスの安全性を高めるために：セキュア・エレメント等の活用」、金融研究所ディスカッション・ペーパーNo. 2017-J-15、日本銀行金融研究所、2017年

大熊浩也・瀧田　愼・森井昌克、「偽装QRコードの構成とその効果、およびその対策について」、コンピュータセキュリティシンポジウム2018論文集、情報処理学会、2018年

キャッシュレス推進協議会、「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】」、キャッシュレス推進協議会、2019年a（https://www.paymentsjapan.or.jp/wordpress/wp-content/uploads/2019/03/MPM_Guideline_1.0.pdf、2019年10月7日）

————、「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】」、キャッシュレス推進協議会、2019年b（https://www.paymentsjapan.or.jp/wordpress/wp-content/uploads/2019/03/CPM_Guideline_1.1.pdf、2019年10月7日）

経済産業省、「キャッシュレス・ビジョン」、経済産業省、2018年

笹崎寿貴・シュウインゴウ・丸山誠太・森　達哉、「SeQR：ショルダーハック耐性を持つQRコード生成方法」、コンピュータセキュリティシンポジウム2018論文集、情報処理学会、2018年

鈴木雅貴・廣川勝久・宇根正志、「電子マネー・システムにおけるセキュリティ対策：リスク管理に焦点を当てて」、『金融研究』第27巻別冊第1号、日本銀行金融研究所、2008年、39～78頁

中山靖司・太田和夫・松本　勉、「電子マネーを構成する情報セキュリティ技術と安全性評価」、『金融研究』第18巻第2号、日本銀行金融研究所、1999年、57～114頁

日本銀行決済機構局、「キャッシュレス決済の現状」、決済システムレポート別冊シリーズ、日本銀行決済機構局、2018年

廣川勝久、「非接触インタフェース経由取引の技術とビジネスリスク管理の課題」、『金融研究』第29巻第4号、日本銀行金融研究所、2010年、79～106頁

三井住友銀行、「アドレスバーが緑色になるのですが？」、よくあるご質問、三井住友銀行、2017年（https://qa.smbc.co.jp/faq/show/297、2019年10月7日）

森畠秀実・阿部正幸・藤崎英一郎・中山靖司、「電子現金方式」、1997年暗号と情報セキュリティシンポジウム発表論文、SCIS97-3C、電子情報通信学会、1997年

山本正行、「キャッシュレス化で拡大する送金市場 : 主要サービスに見るビジネスモデル」、『CardWave』11・12月号、カード・ウェーブ、2017年、18～25頁

European Payments Council, “White Paper Mobile Payments,” Document EPC 492-09, Version 4.0, European Payments Council, 2012.

Financial Stability Board, “Crypto-Assets: Report to the G20 on Work by the FSB and Standard-Setting Bodies,” Financial Stability Board, 2018.

Han, Runchao, Zhimei Sui, Jiangshan Yu, Joseph Liu, and Shiping Chen, “Sucker Punch Makes You Richer: Rethinking Incentives in Proof-of-Work-Based Blockchains,” Cryptology ePrint Archive, Report 2019/752, International Association for Cryptologic Research, 2019.

Mathews, Lee, “Sneaky New Android Malware Robs Users Through Fake PayPal Alerts,” Forbes, 2018 (available at: https://www.forbes.com/sites/leemathews/2018/12/13/sneaky-new-android-malware-robs-users-through-fake-paypal-alerts/、2019年10月7日).