チャージ型決済の実現方法とそのセキュリティについて

田村裕子（たむらゆうこ）

要　旨

近年、デジタル決済サービスの利用が拡大している。なかでも、電子マネーやコード決済のように、決済事業者が金銭的価値を発行し、それを利用して決済を行うサービス（チャージ型決済）が普及してきている。また、暗号資産もユーザ間で金銭的価値の授受を可能とするスキームの1つである。チャージ型決済には、金銭的価値の保管形態や保管場所の違いによって、いくつかの実現方法が存在する。決済サービスの提供に当たっては、その実現方法に由来する情報セキュリティ面のリスクに応じて対策を講じる必要があることから、本稿では、チャージ型決済における金銭的価値の保管形態や保管場所によって、セキュリティ対策がどのように異なるのか整理を試みる。具体的には、チャージ型決済の各実現方法について、金銭目的の攻撃として想定される不正行為の種類を列挙し、それに対抗するためのセキュリティ対策の差異について考察を行う。

キーワード：　暗号資産、コード決済、セキュリティ対策、チャージ型決済、デジタル決済、電子マネー

本稿を作成するに当たっては、佐古和恵教授（早稲田大学）、大塚玲教授（情報セキュリティ大学院大学）から有益なコメントをいただいた。ここに記して感謝したい。本稿に示されている意見は、筆者個人に属し、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個人に属する。

田村裕子　日本銀行金融研究所企画役補佐（E-mail: yuuko.tamura@boj.or.jp）

1. はじめに

わが国では、政府によるキャッシュレス推進の取組みもあり、デジタル化された手段で決済を行うサービスの利用が拡大している。特に、電子マネー[1]やコード決済[2]のように、現金等の見合いとして金銭的価値の発行を受け、それを利用して決済を行うサービス（以降、「チャージ型決済」と呼ぶ）については、現金に近い感覚で利用できることから、小売店の店頭等における少額の現金決済を代替しうる手段として普及してきている。チャージ型決済のうち、電子マネーでは、IC カードやスマートフォンといった個別ユーザのデバイス上に金銭的価値を保管し、小売店の店頭に設置された決済用端末や他のユーザのデバイスとの間での通信を介して決済を行うことが多い。これに対し、コード決済では、決済事業者のサーバ上に金銭的価値を保管し、決済の都度サーバにアクセスすることによって、ユーザ間、あるいは、ユーザと店舗（インターネット上の販売サイト等を含む）との間の決済を行うことが多くなっている。

ビットコインをはじめとする暗号資産についても、決済処理に対する報酬として金銭的価値（暗号資産）が発行され、そのユーザ間で金銭的価値の授受が可能であることから、広い意味でチャージ型決済の 1 類型として挙げられよう。暗号資産は、ブロックチェーン[3]の生成や記録に参加するコンピュータで構成される P2P ネットワーク上にすべての金銭的価値を保管しており、同ネットワーク上で金銭的価値の授受を行うことが可能な仕組みとなっている。

また、価格変動が大きいという暗号資産の問題点を解決するスキームとしてステーブルコインを発行する動きも活発化している。特に、テック企業が巨大な顧客基盤をベースに独自コインを発行しようとする計画は大きな注目を集めた。こうした民間主体の決済手段に対して、中央銀行が発行するデジタル通貨（Central Bank Digital Currency: CBDC）への関心も高まってきている。多くの海外中銀が CBDC

1 非接触 IC カード機能を利用した前払式の決済方式。電子マネーが実装されるデバイスには、非接触 IC カードのほか、非接触 IC カード機能を搭載したスマートフォン等がある。

2 コード決済は、店舗が提示するコード（バーコードや QR コード®）をユーザがデバイスで読み取り、決済を行う方式をいう。こうしたコードには店舗に関する情報が埋め込まれており、カメラで QR コードを撮影するだけで、送金先を容易に指定できるという特徴がある。また、ユーザが提示したコードを店舗側が読み取って決済を行う方式もある（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）。

3 ブロックチェーンとは、データ共有のための基盤技術であり、ブロックと呼ばれる単位にまとめたデータをチェーン状に連結して共有することから、ブロックチェーンと呼ばれる。ブロックチェーンで構成されたデータは、不特定多数の参加者が管理するノードと呼ばれるコンピュータで構成されるピア・ツー・ピア（Peer-to-Peer: P2P）ネットワーク（ブロックチェーン・ネットワーク）で共有される。

に関する実証実験やパイロット・プロジェクトの実施を行っているほか（Boar and Wehrli [2021]）、わが国においても、CBDC に対する社会のニーズが高まった場合に備えて、個人や企業を含む幅広い主体の利用を想定した CBDC に関する検討が開始されている（日本銀行［2020］）。

決済サービスの提供に当たっては、想定される情報セキュリティ面のリスクに応じて必要な対策を講じることが必要となる。その実現方法については、金銭的価値の保管形態やその保管場所の違いについて議論されているが（日本銀行決済機構局［2020］）、こうした実現方法の違いがセキュリティに与える影響について考察を行った先行研究がある（中山・太田・松本［1999］、鈴木［2010］）。これらの先行研究では、ユーザが決済で利用する暗号処理用の秘密情報を悪用する不正行為の種類について比較・評価が行われている。もっとも、チャージ型決済において想定されるリスクとしては、他のユーザの秘密情報を用いる攻撃や、金銭的価値を改ざんするといった攻撃も考えられることから、こうしたリスクへの対応についても整理しておくことが必要であろう。そのほか、先行研究では、金銭的価値をデバイスに保管する場合の検討が主となっているが、暗号資産の登場や通信コストの大幅な低下といった環境変化や技術革新を踏まえ、金銭的価値の保管場所をサーバやネットワーク上に広げて整理することも必要と考えられる。

そこで、本稿では、改めてチャージ型決済の実現方法の種類について整理し、各タイプのセキュリティ要件と必要なセキュリティ対策を導出することで、実現方法の選択による差異を明らかにすることを目的とする。まず、2 節において、チャージ型決済の概要と事例を説明する。3 節では、決済の実現方法を具体化し、各タイプで想定されるリスクをもとに必要なセキュリティ対策技術を導出する。そのうえで、4 節において、金銭的価値の保管場所ごとに、保管形態の違いによってセキュリティ対策に差異が生じるかを考察するとともに、デバイスに付与したセキュリティ対策の有効性が低下した場合の影響について比較・評価を行う。

2. チャージ型決済の実現方法

(1) チャージ型決済の概要

本稿が対象とするチャージ型決済とは、決済事業者が現金等の見合いで発行した金銭的価値を用いて行う対面または非対面の決済方式であり、主に以下の関係者等（エンティティ）で構成される。

（エンティティ）

- 決済事業者：金銭的価値の発行者であり、決済サービスを提供する。ユーザがデバイスを用いて決済サービスを利用できるよう、決済サービス・アプリを提供する。
- サーバ等：決済事業者が運営するサーバ、または、ブロックチェーン・ネットワーク。ユーザの金銭的価値の保管等に利用される。
- ユーザ：決済サービスの利用者。金銭的価値の保有者であり、金銭的価値を利用して決済（他ユーザへの送金、他ユーザからの受領）を行う。
- デバイス：ユーザが決済サービスを利用する際に用いる端末であり、金銭的価値の保管を行うこともある。決済サービス・アプリを搭載しているほか、ネットワーク通信機能やデバイス間通信のための近距離無線通信機能を有している。以降、ユーザ A が使用するデバイスを、デバイス A と呼ぶ。

決済サービスの多くは、特定の事業者によって運営が行われているが、暗号資産には特定の運営者が存在せず、不特定多数のコンピュータによって形成されたブロックチェーン・ネットワークによって自律システムが構築されている。ブロックチェーンの生成は、コンピュータ間で合意をとりながら行われることから[4]、ブロックチェーン・ネットワークを決済事業者とみれば、チャージ型決済に分類することができる。

上記エンティティで構成される決済サービスの主な処理手順は以下のとおりである。

（手順）

- ユーザ登録：決済サービスの利用に当たり、ユーザは決済事業者にサービス利用の申請を行う。決済事業者は、ユーザに決済サービス内で利用する ID を割り振る。
- チャージ：ユーザからの依頼を受け、決済事業者は、現金等の見合いとして金銭的価値を発行する。発行された金銭的価値は、ユーザのものとして保管される。
- 送金：ユーザは、金銭的価値を他ユーザに送付する指示をデバイスに入力する。これを受け、決済事業者は決済サービス・アプリを通して送金処理を行う。金銭的価値は、送金先ユーザのものとして保管される。

4 コンピュータ間で合意をとる方法には、PoW（Proof of Work）や PoS（Proof of Stake）等がある。PoW は計算量に応じてブロックを生成する権利を付与する方法であり、PoS は暗号資産の保有量と保有期間に応じて権利を付与する方法である。

受領した金銭的価値の保管形態と保管場所にはいくつのバリエーションがある。金銭的価値を受領した際の保管形態については、決済事業者や他ユーザから受領した金銭的価値を合算して保管する方法と、一度の取引で得た金銭的価値を合算せずにそのまま区別して保管する方法の 2 種類が存在する。こうした 2 種類の保管形態に基づく実現方法は、それぞれ「残高管理型」と「電子証書型」と呼ばれている（中山・太田・松本［1999］）[5]。すなわち、残高管理型では、それまでに実行された個々の取引における金銭的価値を合算して保管し、電子証書型では、個々の取引で受領した金銭的価値が区別して保管される。

保管される金銭的価値を金銭データと呼ぶとき、残高管理型は、保管先で金銭データを生成（金銭的価値を合算）して保管する方式であり、受領したタイミングで金銭データを更新することになる。これに対し、電子証書型は、決済事業者によって発行された金銭的価値を送付する方式であり、送金者から受領したデータを加工することなく、そのまま個々の金銭データとして保管する方式となる（図表 1 参照）[6]。

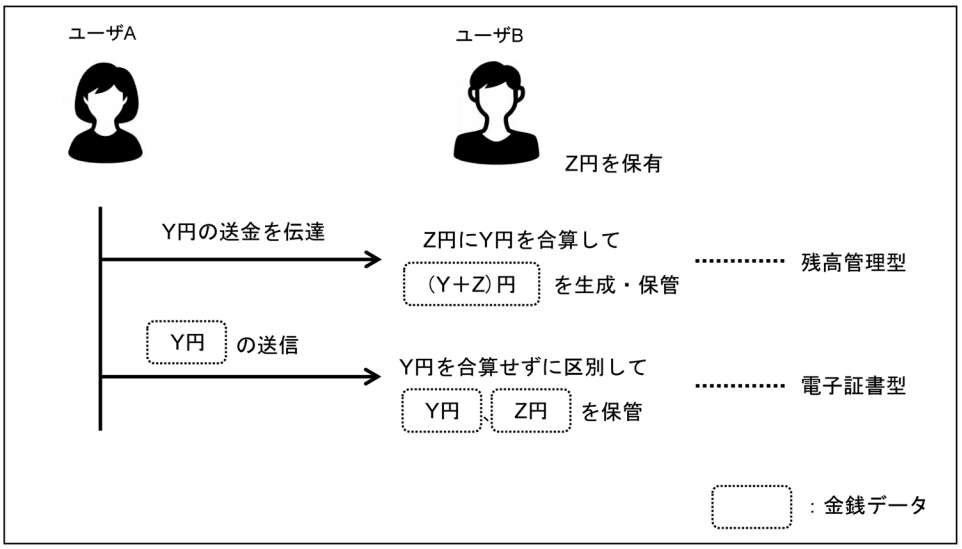
また、その保管場所については、決済事業者が全ユーザ分をまとめて保管する方法と、各ユーザがそれぞれローカルに保管する方法がある。前者はユーザからみてリモートでの保管であり、決済事業者のサーバやブロックチェーン・ネットワークが保管場所となりうるほか、後者にはスマートフォンが保管媒体として挙げられる。金銭データをリモートで保管する方法では、ユーザと決済事業者のやりとりによって決済が行われるのに対し、ローカルで保管する方法では、ユーザ間のやりとりによって決済を実行することが可能となる。

このように、金銭データの保管形態や保管場所によって、決済処理を実施するエンティティ、エンティティ間で通信されるデータの種類、各エンティティに保管が求められるデータ等が異なる。

5 こうした分類は、1990 年代に世界各国で行われたデジタル決済に関する実証実験の事例がベースとなっており（Committee on Payment and Settlement Systems and the Group of Computer Experts of the Central Banks of the Group of Ten Countries [1996]、中山［1998a］）、昨今の CBDC に関する議論においても、同様の定義に基づいた整理がみられている（Bank of England [2020]、European Central Bank [2020]）。残高管理型については、口座型や残高型等と呼ばれることがあるほか、電子証書型についても、トークン型、電子貨幣型、紙幣型、持参人払型等と呼ばれることがある。こうした 2 つのスキームが誕生した背景は、発想の起源や研究・開発のアプローチにある（中山［1998b］）。

6 電子証書型は、暗号学者らが現金の電子化を目指して研究開発を進めてきたものである。当初は、銀行券や貨幣のように固定された金額の金銭データの送受信が想定されていたが、その後、分割支払いが可能な方式も提案された（岡本・太田［1993］）。

図表 1　金銭データの保管形態（残高管理型、電子証書型）



(2)　チャージ型決済の事例

残高管理型の事例には、コード決済、電子マネー、暗号資産がある。電子証書型については、暗号資産が事例として挙げられるほか、過去には各国で複数の実証実験が行われていた（中山［1998a］）。暗号資産をみると、イーサリアムでは、個々のユーザにアカウントが付与されており、決済の都度、各ユーザが受領した金銭的価値が合算されるようになっている。これに対し、ビットコインでは、送金内容を示すデータ（トランザクション）そのものがブロックチェーンで保管されており、ユーザのもつ金銭的価値を合算することなく、すべての金銭データを区別して保管するという方式が採られている。このようにみると、イーサリアムは残高管理型、ビットコインは電子証書型に分類できる[7]。

金銭データの保管場所にも場合分けがある。電子マネーでは、ユーザが所有するICカードやスマートフォン内で管理することが多い。一方、コード決済では、決済事業者がサーバで全ユーザ分を管理することが多く、ユーザは決済事業者のサーバにアクセスして送金処理を行うことになる。暗号資産においても、全ユーザ分をまとめてブロックチェーン・ネットワークが管理しており、ユーザはブロックチェー

7 ビットコインでは、UTXO（Unspent Transaction Output）と呼ばれる方法で金銭データの管理が行われている。送金元ユーザが生成するトランザクションは、インプット（送金元ユーザID、数量）とアウトプット（送金先ユーザID、数量）によって構成され、そのアウトプットは以降に生成されるトランザクションのインプットとなる。このように、トランザクションとは、ユーザが保有するビットコインの保有者を変更する旨を示したものであり、それがそのままブロックチェーンに記載される。

図表 2　残高管理型と電子証書型の事例

金銭データの保管形態	金銭データの保管場所	チャージ型決済の事例（*は過去の実証実験）
残高管理型	リモート	コード決済、暗号資産イーサリアム
	ローカル	電子マネー、MONDEX*
電子証書型	リモート	暗号資産ビットコイン
	ローカル	eCash*、スーパーキャッシュ*

ン・ネットワークにアクセスして送金を行う。

以上の整理に基づき、国内で利用可能なチャージ型決済、および、過去に実施された代表的な実証実験の事例[8]を、保管形態と保管場所別に整理すると、図表 2 のとおりである。

(3)　対象とするチャージ型決済

チャージ型決済サービスの提供に当たっては、決済処理が正しく実行されること、および、第三者による不正行為を防止できることといった機能の具備が必須となる。特に、後者は悪意をもったユーザ（以降、「攻撃者」と呼ぶ）への耐性を求めるものであり、攻撃の手口が日々進化していくことから継続的な対応が必要となる。そこで、本稿では攻撃者による金銭目的の不正行為を想定してセキュリティ対策を整理することとしたい。具体的には、保管形態（残高管理型、電子証書型）、保管場所（リモート、ローカル）を組み合わせた 4 つの方法について、セキュリティの観点から比較を行う。なお、中山・太田・松本［1999］においても、同様の整理が行われているが、電子証書型については、現金の電子化を目指して研究開発された経緯から、保管場所をローカルとする実現方法のみが想定されていた。そこで、本稿では、暗号資産の登場や通信コストの大幅な低下といった環境変化や技術革新を踏まえ、金銭データの保管場所をサーバやネットワーク上に広げて整理を行う。

整理の対象は、①ユーザによるチャージ・フェーズ、および、②ユーザによる送金フェーズとし、対象フェーズ以外で想定される不正行為[9]については取り扱わな

8 MONDEX は、英国ナットウエスト銀行が中心となって開発・実用化が進められた決済方式であり、1995 年以降、世界各国で実証実験が行われた。eCash は、オランダの Digicash 社が開発した決済方式である。1995 年に米国マークトウェイン銀行が eCash を発行したが、1998 年にサービスは打ち切られた（相澤［2000］）。スーパーキャッシュは、日本電信電話株式会社が開発した決済方式であり、1999 年に NTT コミュニケーションズと国内金融機関 22 行からなる協議会によって実証実験が行われた（エヌ・ティ・ティ・コミュニケーションズ株式会社［2000］）。なお、本方式は、日本電信電話株式会社と日本銀行金融研究所との共同研究の成果がベースとなっている（日本電信電話株式会社［1996］）。

9 チャージより前に行われる不正としては、盗取した現金によるチャージや他ユーザの銀行口座から

い。また、デバイスにインストールされた決済サービス・アプリは正しく機能することを前提とするほか[10]、決済事業者による不正は対象外とする[11]。

3. リスク分析とその対策事例

本節では、残高管理型と電子証書型の各チャージ型決済について、主な処理を整理するとともに、想定されるリスクに対して必要となるセキュリティ対策の例を挙げる。

(1) 残高管理型決済

イ. 主な処理

サービス利用を開始するに当たり、ユーザは決済事業者にユーザ登録を行う。その際、決済事業者は、ユーザに ID を割り当て、金銭データの保有者識別に利用する。以下、ユーザ A の ID を ID_A と表す[12]。

残高管理型決済の主な処理について、ユーザ A が X 円のチャージを行った後、ユーザ B に Y 円を送金する場合を例に説明する（図表 3 参照）。なお、デバイス上で行われる処理は、決済サービス・アプリによって実行される。

- 金銭データをリモートで保管する場合

  チャージ処理：ユーザ A は、入金処理端末等を利用して[13]、決済事業者に ID_A へのチャージを依頼する。決済事業者はサーバ等内で管理する ID_A の金銭データを△X 円に上書きする[14]。

のチャージ等がある。

10 例えば、マルウェアへの感染等により、デバイスやアプリが正しく機能しないことも考えられる。その場合には、3 節以降で考察を行うセキュリティ対策も有効に機能しない可能性があることから、マルウェア等への対策は重要である。こうしたデバイスのセキュリティ対応のあり方については、磯部・宇根［2021］、山内［2021］を参考にされたい。

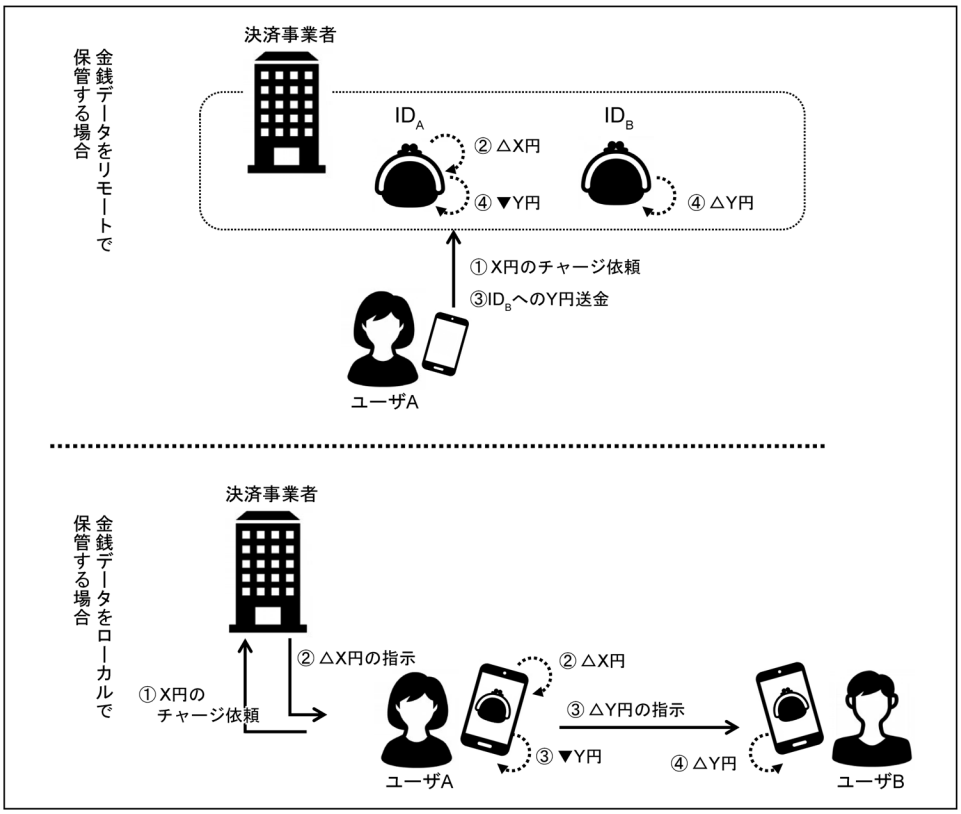
11 決済事業者の内部犯行については、運用面の対応のほか、システムへのアクセス権限の設定等の対応が必要となる。また、不特定多数のノードで構成されるパブリック型ブロックチェーンでは、ネットワークを構成するノードのうち、悪意のあるノードの数が半数以下であれば、不正な取引を防止することが可能となっている。

12 金銭データをローカルで保管するタイプについては、金銭データに保有者の ID を紐づける方法のほか、ID に対応するユーザのデバイス内で保管されていることをもって ID と紐づいているとみなすこともできる。

13 金銭的価値を発行する入金処理端末を利用する方法のほか、オンラインで発行する方法も考えられる。

14 「△」は、基準となる値に対しプラスを表す。

図表３　残高管理型における主な処理



送金処理[15]：ユーザ A は、決済事業者あるいはユーザ B からユーザ B の ID を入手する[16]。ユーザ A はデバイス A を介して、決済事業者に ID_B への Y 円送金を示す電文を送信する。決済事業者は、サーバ等で管理する ID_A と ID_B の金銭データを、それぞれ▼Y 円と△Y 円に上書きする[17]。

- 金銭データをローカルで保管する場合

  チャージ処理：ユーザ A は、入金処理端末等を利用して、決済事業者に ID_A

15 ここでは、送金者であるユーザ A が決済事業者に送金電文を送信する場合を想定したが、受領者であるユーザ B が決済を主導する場合もある。その場合には、ユーザ B がユーザ A からの送金を請求する電文を決済事業者に送信することになる。決済事業者が送金処理を行う際には、送金者の同意を確認するステップが別途必要となる。

16 送金先の ID を決済事業者から入手する方法としては、オンラインで検索できるようにする方法がある。ただし、ID を利用した不正行為（例えば、本人の同意なく送金し、利息を請求する「押貸し」等）を防止する観点からは、検索できる範囲を限定したり、送金時に受領者による受領の意思を確認したりするといった対策が必要となる。

17 「▼」は、基準となる値に対しマイナスを表す。ID_A がもつ金銭データが Y 円より小さい場合、送金処理は中断される。

へのチャージを依頼する。決済事業者は、入金処理端末等からデバイス A に対して、金銭データを△X 円に上書きする電文を送信する。電文を受け取ったデバイス A は、金銭データを△X 円に上書きする。

送金処理：ユーザ A は、ユーザ B の ID を入手し、デバイス A に ID_B への Y 円送金を指示する。デバイス A は、内部に有する金銭データを▼Y 円とし、デバイス B に Y 円送金を示す電文を送信する[18]。電文を受け取ったデバイス B は、内部に格納する金銭データを△Y 円に上書きする。

ロ. 想定されるリスクとセキュリティ対策例

金銭データは ID とセットで保管されることから、このいずれかを偽造・改ざん、複製することで、攻撃者がもつ金銭的価値を増やしたり、送金を行ったりしようとする攻撃が考えられる[19]。また、決済事業者からのチャージや他ユーザからの送金にかかる電文を偽造・改ざん、複製することで不正にチャージ・送金を行う攻撃も想定されるほか、他ユーザになりすまして当該ユーザの金銭データを送付する攻撃も考えられる。こうしたリスクを踏まえたセキュリティ要件は、①金銭データと ID（以降、「金銭データ・ID」と表す）の偽造・改ざん、および、複製対策を講じること、②第三者によるなりすまし対策を講じること、③電文の偽造・改ざん、および、複製対策を講じることである。

以下では、セキュリティ要件を充足するための対応案について整理する。なお、想定される攻撃の詳細とその要件を充足するための対策例については、補論 1 に整理している。

（イ） 金銭データをリモートで保管する方法

（金銭データ等の偽造・改ざん、複製への対策）

保管先にある金銭データの偽造・改ざん、および、複製への対策には、これらの攻撃を防ぐ事前の対策と、攻撃を検知可能とする事後的な対策の 2 種類がある。サーバで保管する金銭データ・ID の偽造・改ざんに対しては、不正アクセス対策等によってデータを保護する、あるいは、決済事業者によるデジタル署名[20] の付与に

18 金銭データを▼X 円とするタイミングについては、デバイス B における増額処理が完了した後とすることも可能である。

19 偽造とは、偽のデータを作り出すことを指し、改ざんとは、既存のデータの一部を不正に書き換えることを指す。そのため、改ざんは偽造のための 1 つの手段であるといえる。また、既存データの複製についても、用途によっては偽造に含まれるが、本稿では、偽造・改ざんと複製をわけて整理する。

20 デジタル署名とは、公開鍵暗号方式を利用した文書の改ざん検知機能である。署名者 S は、署名鍵 sk_S と検証鍵 pk_S のペアを有する。署名者 S が秘密裏に管理する sk_S を用いて生成されたデジタル署名は、公開可能な検証鍵 pk_S を用いて検証される。検証の結果は「真」または「偽」で表され、真であれば、デジタル署名は S によって生成されたものであり、対象となる文書が改ざんされていないことが示される。

よって偽造・改ざんを検知できるようにしておく方法がある。金銭データ・ID の複製に関しても、不正アクセス対策によって複製を困難にする方法のほか、仮に複製が行われたとしてもそれを検知できるよう、ID の重複を常時チェックするという方法が挙げられる。

また、ブロックチェーンを利用することで、金銭データを偽造・改ざんから保護することも考えられる。ブロックチェーンでは、ブロックチェーン・ネットワークによる合意を得たものだけが保管される仕組みが採用されていることから、特定のユーザによるデータの偽造・改ざん、および、複製が困難となっている。

（なりすましへの対策）

ユーザはデバイスを介して送金を行うため、デバイスが盗取された場合にはなりすましによる送金がリスクとなる。なりすましへの対策としては、デバイスを操作して送金を依頼しているユーザが、金銭データの ID に対応するユーザであることを確認する必要がある。ユーザ認証は、事前にユーザによって登録されたデータ（登録データ）と認証時にユーザから提示されるデータ（提示データ）との照合によって行われる。そのためには、登録データや提示データが偽造・改ざんされたり、複製されたりすることがないよう対策を講じておくことが求められる。

ユーザ認証には、登録データと提示データの照合処理をサーバ等で行う方法のほか、デバイス上で照合処理を行い、その結果を決済事業者に送信するという方法がある。後者の場合には、デバイスから送信される認証結果についても、偽造・改ざん、および、複製への対策が必要となる。

（電文の偽造・改ざん、複製への対策）

デバイスから決済事業者に送信される電文を偽造・改ざんする攻撃に対しては、電文へのデジタル署名が対策として考えられる。このとき、デジタル署名を生成するための署名鍵はデバイス内で安全に管理する必要があるほか、デジタル署名者と金銭データに付与された ID との対応関係を決済事業者が確認できるようにしておくことも必要となる。例えば、検証鍵と ID の対応関係をリスト化して安全に管理する方法や検証鍵を ID として用いる方法等はその一例となろう。

電文の複製については、電文に改ざん耐性のある識別番号を付与しておくことで重複を検知できるようにしておく方法のほか、電文がリアルタイムで生成されたことを確認するために、チャレンジ・レスポンス方式の認証[21] を採用することも対策の一例となる。

21 ある命題を証明する者と検証する者との間で実行されるプロトコルであり、検証者は、毎回異なるデータをチャレンジとして証明者に送信し、証明者はチャレンジに応じたレスポンスを返す。このため、過去のプロトコルで送受信されたデータを複製してレスポンスに利用するリプレイ攻撃への耐性を有する。

ブロックチェーンを利用した暗号資産においても、電文の偽造・改ざん対策としてデジタル署名が利用されている。また、電文には識別番号が付与されており、ブロックチェーン・ネットワークにおいて重複の確認が行われている[22、23]。

（ロ） 金銭データをローカルで保管する場合

（金銭データ等の偽造・改ざん、複製への対策）

金銭データをローカルに保管する場合では、金銭データの正規保有者やそれ以外の第三者によって、デバイス内にある金銭データ・ID の偽造・改ざんが行われるリスクがある。こうした攻撃を困難にするには、デバイス自体が備えている耐タンパー性[24] によってデータを保護する方法のほか、デバイスによるデジタル署名の付与によって、アプリが攻撃を検知できるようにしておくことが必要となる。

また、攻撃者が金銭データを偽造、複製したうえで、攻撃用に用意したデバイスから送金するという不正も考えられることから[25]、受領した金銭的価値が偽造されたものでないことを受領側で確認できるような対策も必要である。

（なりすましへの対策）

なりすましのリスクは、金銭データをリモートで保管する場合と同様である。ただし、金銭データの保管場所がデバイスであることから、ユーザ認証はデバイス上で実施することになる。

（電文の偽造・改ざん、複製への対策）

電文の偽造・改ざんによる不正に対しては、デジタル署名による対策を施しておく方法が考えられる。あわせて、決済事業者から公開鍵証明書[26] の発行を受けるなどの方法によって、ID と検証鍵との関係性を確認可能としておく必要がある。ま

22 イーサリアムでは、ユーザから送信されるトランザクションがここでの電文に該当する。トランザクションには、その内容によって一意に定まる ID（トランザクション・ハッシュ）が割り当てられており、ID の確認によってトランザクションの複製による不正行為を防止している。

23 ブロックチェーンがソフト・フォークしている状態であれば、電文の複製による不正も可能となるが、最長のブロックチェーンを正規チェーンとみなすルールにより、一方のチェーンに記載された送金はいずれ無効となる。

24 耐タンパー性とは、秘密情報や秘密情報の処理メカニズムを外部から不当に観測・改変することや、秘密情報を処理するメカニズムを不当に改変することが極めて困難である性質をいう（日本規格協会情報技術標準化研究センター［2003］）。

25 偽造、複製した金銭データを攻撃用デバイスから別のユーザに送金するという不正のほか、自身の正規デバイスに送信させることで不正に金銭データを増やすという不正が考えられる。

26 ここでの公開鍵証明書とは、決済事業者が ID_A と公開鍵（検証鍵）との対応関係を保証するものである。ユーザ A から、①電文、②電文のデジタル署名、③公開鍵証明書を受信したユーザは、まず、公開鍵証明書の検証によって公開鍵と ID_A の対応関係を確認した後、当該公開鍵を用いて電文のデジタル署名の検証を行う。こうした手順を踏むことで、電文が ID_A に該当するユーザによって生成されたものであることを確認することができる。なお、誰もが自由に参加可能な暗号資産では、利用者登録といった手順はなく、自身で生成した公開鍵を ID に利用することとなっている。

た、電文の複製によって、二重に送金を受ける不正を防止するには、電文がリアルタイムで生成されたことを確認することが必要であり、チャレンジ・レスポンス方式の認証を採用することが対策の一例となる。

(2) 電子証書型決済

イ. 主な処理

サービス利用を開始するに当たり、ユーザは決済事業者にユーザ登録を行う。その際、決済事業者は、ユーザに ID を割り当て、金銭データの保有者識別に利用する。以下、ユーザ A に割り当てた ID を ID_A と表す。

電子証書型決済の主な処理について、ユーザ A が X 円のチャージを行った後、ユーザ B に Y 円を送金する場合を例に説明する（図表 4 参照）[27]。また、Y 円（≤ X 円）の送金に当たっては、X 円を送付しておつりを受領する方式、額面金額が Y 円となるように 1 つ以上の金銭データを使用する方式、X 円の金銭データを分割して Y 円とする方式がある（岡本・太田［1993］）。

- 金銭データをリモートで保管する場合

  チャージ処理：ユーザ A は、入金処理端末等を利用して、決済事業者に ID_A へのチャージを依頼する。決済事業者は保有者を ID_A とする X 円の金銭データを生成し、サーバ等に保管する。

  送金処理：ユーザ A は、決済事業者あるいはユーザ B からユーザ B の ID を入手する。ユーザ A は、デバイス A に ID_B への Y 円送金を指示する。デバイス A は、サーバ上にある Y 円分の金銭データを参照し、当該金銭データの保有者を ID_A から ID_B に変更する処理を行う。デバイスが保有者を変更した金銭データをデバイスから決済事業者に送信すると、決済事業者は、デバイスから送信された金銭データをサーバ等に保管する。

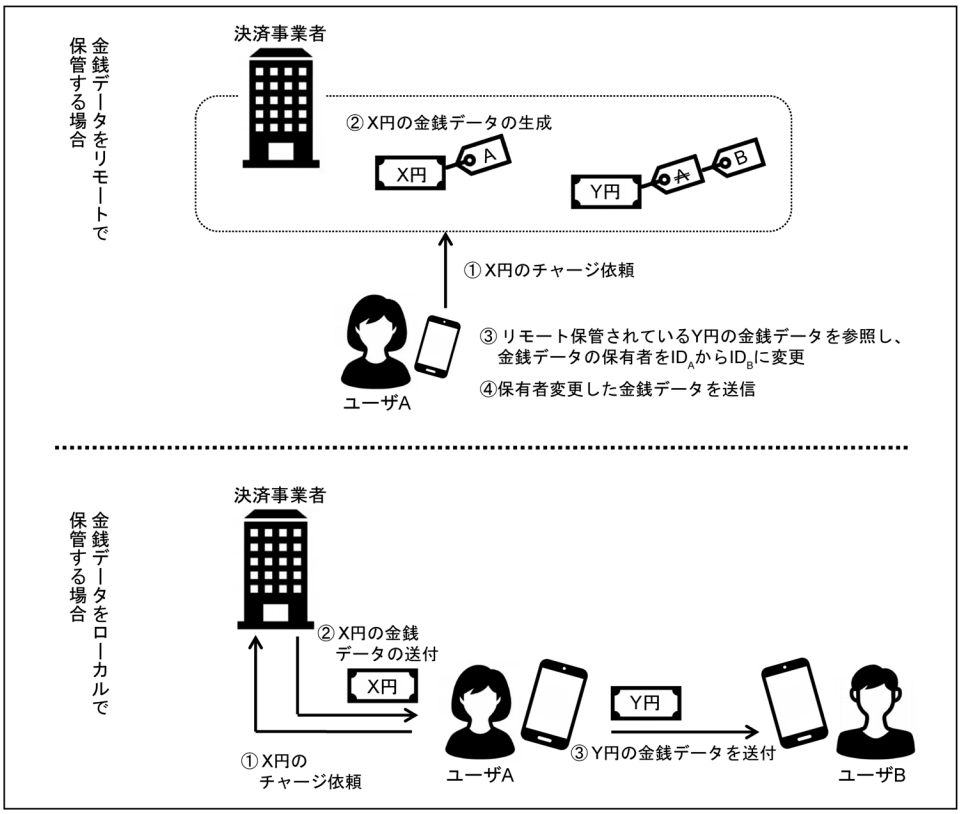
- 金銭データをローカルで保管する場合

  チャージ処理：ユーザ A は、入金処理端末等を利用して、決済事業者に ID_A へのチャージを依頼する。決済事業者は、入金処理端末等内で X 円分の金銭データを生成し、デバイス A に送信する。デバイス A は、受信した金銭データを保管する。

  送金処理：ユーザ A は、ユーザ B の ID を入手し、デバイス A に ID_B への Y 円送金を指示する。デバイス A は、内部に有する Y 円分の金銭データをデ

27 金銭データをリモートで保管する電子証書型については、中山・太田・松本［1999］における金銭データの保管先を、ローカルからリモートに変更したスキームとした。もっとも、ユーザから送金を示す電文を受け、決済事業者が金銭データの保有者情報を変更するというスキームも考えられるが、本稿における電子証書型には当てはまらないため検討の対象としない。

図表 4　電子証書型における主な処理



バイス B に送信するとともに、当該金銭データを消去する。デバイス B は、受信した金銭データを保管する。

ロ.　想定されるリスクとセキュリティ対策例

電子証書型では、保管されている金銭データを偽造・改ざん、複製することで、不正に攻撃者がもつ金銭的価値を増やす攻撃が考えられる。また、送金時には、金銭データそのものが送付されるスキームとなっていることから、偽造・改ざん、複製した金銭データを送信することで不正なチャージ・送金を行う攻撃が考えられるほか、他ユーザになりすまして不正送金を行う方法も考えられる。こうしたリスクを踏まえたセキュリティ要件は、①保管先にある金銭データ、および、送受信される金銭データの偽造・改ざん、複製対策を講じること、②第三者によるなりすまし対策を講じることである。なお、想定される攻撃とその具体例については、補論 2 に整理した。

（イ） 金銭データをリモートで保管する場合

電子証書型では、送金元デバイスから送信されてきた金銭データをそのままサーバ等で保管することから、送信される金銭データと保管されている金銭データの両方を偽造・改ざん、複製から保護する必要がある。

（金銭データ等の偽造・改ざん、複製への対策）

チャージ処理では、決済事業者によって新規発行される金銭データの偽造・改ざん、複製を困難にする必要がある。金銭データの複製については、複製されたとしても、正規保有者以外による金銭データの使用を困難にするとともに、正規保有者であっても同じ金銭データを二度使用することができないようにする仕組みが必要となる。

サーバで金銭データを管理する場合では、決済事業者によるデジタル署名によって、チャージ処理で新規発行された金銭データの偽造・改ざんを困難にしたり検知したりすることができる。また、ブロックチェーンでは、マイニング[28]に成功した者に対し、報酬として暗号資産が自動的に新規発行される。新規発行された暗号資産はブロックチェーンに書き込まれることによって改ざんが困難となっている。

正規保有者以外による金銭データの複製対策としては、正規保有者だけが金銭データを利用できるような仕組みが必要である。そのためには、金銭データに付与されたIDと、当該金銭データを決済に使用しようとするユーザとの対応関係を確認できるようにすればよい。その実現方法としては、金銭データにIDの履歴を付属させることとし、金銭データの移転時には、IDに送金先ユーザのIDを追加したうえで、送金元ユーザのデジタル署名を付与することが考えられる。金銭データを受け取った決済事業者は、金銭データの前保有者IDとデジタル署名との対応関係を確認することによって、正規保有者から送信された金銭データであることを確認することができる（中山ほか［1997］、Nakamoto [2009]）[29]。金銭データに付与され

28 合意形成アルゴリズムにPoWを採用しているブロックチェーンにおいて、ブロックの生成者を決定するための行為。例えば与えられたハッシュ関数の出力が一定の条件を満たす入力値を総当たりで計算すること。

29 メッセージmに対するユーザIによるデジタル署名付きメッセージを$Sig_I(m)$と表すとき、決済事業者Sがユーザ A に発行したX円の金銭データ（ID付き）は、$Sig_S(X, ID_A)$と表すことができる。次に、この金銭データの保有者をユーザBに変更する際には、「Aが保有していた金銭データをBに移転させる」という情報に対してAのデジタル署名を付与することになる：$Sig_A(Sig_S(X, ID_A), ID_B)$。これを受領したユーザは、デジタル署名の検証鍵$pk_A$と$ID_A$との対応関係が確認できれば、デジタル署名の検証によって、ユーザAが金銭データについて保有者をユーザBに変更したということが確認できる。

金銭データを受け取ったユーザは、当該金銭データが決済事業者によって発行されたものであり、その移転が正しく行われてきたことを確認する必要があるため、金銭データに付与されているすべてのデジタル署名を検証する必要がある。このように、電子証書型では、金銭データに次の保有者のIDを加えてデジタル署名を付与するという送金者による処理が繰り返されるため、金銭データは移転回数に伴い肥大化し、検証作業に伴う負荷も大きくなる。ただし、金銭データをリモートで保管す

たデジタル署名と ID との関係については、別途、それらをリストにして確認できるようにしておく方法のほか、ID にデジタル署名用の検証鍵を用いることで、ID とデジタル署名者との関係確認を容易にするものもある。

また、電子証書型では、通信路の盗聴によって金銭データの複製が可能となることから、複製された金銭データを送金に再利用する攻撃に対しては、改ざん耐性をもつ識別番号のチェックによって検知することが求められる[30]。また、ブロックチェーンを利用する場合においても、ブロックチェーン・ネットワークによる識別番号のチェックにより複製への対策が講じられている。

（なりすましへの対策）

デバイスを盗取することで、デバイスの持ち主になりすまして決済を行う攻撃の手順は、残高管理型と同様であり、同様のセキュリティ対策が求められる。

（ロ） 金銭データをローカルで保管する場合

（金銭データ等の偽造・改ざん、複製への対策）

金銭データをローカルで保管する場合では、金銭データの偽造・改ざん対策として決済事業者によるデジタル署名の付与が必要となる。また、第三者による金銭データの複製への対策としては、正規保有者だけが金銭データを利用できるようにする仕組みが必要であり、（A）金銭データが外部に漏洩することがないよう、デバイスの耐タンパー性と暗号化通信による対策方法のほか（Brands [1993]）、（B）金銭データの受領者が不正を検知できるよう、金銭データと ID を紐づけする対策方法が考えられる（中山ほか［1997］）。

（B）の対策方法は、金銭データをリモートで管理する場合と同様の対策方法であり、金銭データに ID の履歴を付属させ、送金元ユーザのデジタル署名によって金銭データの偽造・改ざんを困難にするというものである。金銭データに付与されるデジタル署名が、当該金銭データの保有者によって生成されたものであることについては、別途、金銭データの ID と検証鍵との対応関係によって確認する必要がある。不特定多数のユーザとエンド・ツー・エンドで決済を行う方法では、決済事業者の公開鍵証明書を利用することによって検証鍵と ID の対応関係を確認することができる。

また、ユーザが金銭データを複数回使用する攻撃への対策として、まず、複製した金銭データを正規デバイスに書き込むことができないような対策が必要であり、

るタイプでは、決済事業者による移転履歴の削除（金銭データの再発行）によって、金銭データのサイズを小さくすることも可能である。なお、暗号資産では、金銭データのすべての移転履歴をブロックチェーンに保管することで、いつでも金銭データの正当性を確認することが可能となっている。

30 ビットコインでは、トランザクションの内容によって一意に定まる ID（トランザクション ID）がトランザクションに振られている。

耐タンパー性による保護が求められよう。また、攻撃用デバイスを保管媒体として使用する攻撃も想定されることから、本人であっても送金時に使用する署名鍵にアクセスすることができないようにする必要がある。そのほか、ユーザ自身が過去の決済で使用した金銭データを複製して使用する不正に対しては、金銭データの受領者側がリアルタイムで生成されたデータであることを確認できるような、チャレンジ・レスポンス方式の認証等を採用する方法が考えられる[31]。

（なりすましへの対策）

デバイスを盗取することで、デバイスの持ち主になりすまして決済を行う攻撃の手順は、残高管理型と同様であり、同様のセキュリティ要件が求められる。

4. 保管場所の違いによるセキュリティ評価

(1) 金銭データをリモートで保管する場合

3 節で考察した内容について、残高管理型と電子証書型で必要となるセキュリティ対策を比較すると図表 5 のとおりとなる。両者を比較すると、金銭データをリモートで保管する場合には同じ対策技術を用いてシステムを構成することが可能であり、想定される同じリスクに対して、同じ対策技術を選択した場合には、セキュリティ対策技術が期待通りに機能している限りにおいて、両システムは同水準のセキュリティを実現することが可能といえる。

また、残高管理型と電子証書型のどちらについても、保管されている金銭データの偽造・改ざん、複製対策としてブロックチェーンを利用することが考えられる。ブロックチェーンは、ブロックチェーン・ネットワークによる合意形成によって金銭データの保管が行われるものであり、膨大な計算コスト等をかけてブロックをハッシュ・チェーンでつなぐことによって、ブロックに格納されている金銭データの偽造・改ざんを困難としている。複製対策についても、ブロックチェーンでは、ブロックチェーン・ネットワークによる ID の重複チェックや識別番号の重複チェックが行われており、サーバを利用した決済事業者が単独で行う対策と類似の

31 そのほか、サーバに還流してきた金銭データの識別番号を保管することで、複製された金銭データを特定するという方法もある（中山ほか［1997］）。同じ識別番号をもつ金銭データが決済事業者に複数還流すれば、金銭データに付随する保有者の履歴から複製者を特定可能であるため、攻撃者に複製をとどまらせる抑制効果を期待することができる。なお、ここでの還流とは、①サービス等への対価として決済事業者に金銭データを送信する、②現金に引き換えるために金銭データを送信する、③金銭データを再発行してもらうために金銭データを送信するなどを指す。

図表５　金銭データをリモートで保管する場合のセキュリティ対策例

	残高管理型	電子証書型
保管先にある金銭データ等の偽造・改ざん対策	• ①または②または③の対策 ①サーバの不正アクセス対策 ②決済事業者によるデジタル署名の付与（データ更新の都度）、決済事業者の署名鍵の保護 ③ブロックチェーンの利用	• ①または②の対策 ①決済事業者によるデジタル署名等の付与（発行時）、決済事業者の署名鍵の保護 ②ブロックチェーンの利用
保管先にある金銭データ等の複製対策	• ①または②の対策 ①サーバの不正アクセス対策 ②ID の重複チェック	• ①または②の対策 ①サーバの不正アクセス対策 ②識別番号の重複チェック
通信されるデータ（電文／金銭データ等）の偽造・改ざん対策	• デバイスによる電文／金銭データへのデジタル署名の付与 • 決済事業者の署名鍵の保護 • デバイスの耐タンパー性（署名鍵の保護） • 検証鍵と ID のリスト化等	
通信されるデータ（電文／金銭データ等）の複製対策	• ①または② ①チャレンジ・レスポンス方式の採用 ②サーバ等での識別番号チェック	
なりすまし対策	• サーバの不正アクセス対策（登録データの保護）[1] • デバイスにおける登録データの暗号化[1] • デバイスが送信するユーザ認証結果へのデジタル署名の付与[2] • デバイスの耐タンパー性（提示データの保護、登録データの保護[2]）	

備考：1：ユーザ認証をサーバ等で行う場合
　　2：ユーザ認証をデバイスで行い、その結果をサーバ等に送信する場合

手法が利用されている。

決済サービスを提供するに当たっては、セキュリティ対策技術の有効性低下により、リスクが顕現化してしまった場合の影響についても考察しておくことが必要であろう。特に、決済に利用されるデバイスは、ユーザの管理下にあることから、攻撃に晒されるリスクが高いほか、仮に攻撃が行われた場合、決済事業者がそれを検知することは難しい。そのため、デバイスが攻撃を受けた場合にどのような影響が及ぶかを事前に把握しておくことは重要である。

例えば、残高管理型と電子証書型のどちらについても、デバイス A への攻撃によってユーザ A の署名鍵を盗取できれば、デバイス A が手元になくとも、攻撃者は自身のデバイスを使って不正送金できる可能性があることには留意が必要である。もっとも、署名鍵が盗取されてしまった場合であっても、こうした不正送金を防止可能とするユーザ認証やデバイス認証等の実行について考慮しておくことは必要であろう。

(2) 金銭データをローカルで保管する場合

3節で考察した内容について、残高管理型と電子証書型に必要なセキュリティ対策を比較すると、図表6のとおりとなる。両者を比較すると、金銭データをローカルで保管する場合においても、同じ対策技術でシステムを構成することが可能であり、想定される同じリスクに対して、同じ対策技術を選択した場合には、当該セキュリティ対策技術が期待通りに機能している限りにおいて、両システムは同水準のセキュリティを実現することが可能といえる。

デバイスに対するセキュリティ対策については、どちらの実現方法も耐タンパー性で保護すべきデータが多い。金銭データの偽造・改ざん対策としては、耐タンパー性によってデータを保護するか、あるいは、デバイス内でデジタル署名を付与するという方法が考えられる。ただし、後者を選択した場合であっても、署名鍵や決済事業者の検証鍵が偽造・改ざんされることのないよう、耐タンパー性による保

図表6 金銭データをローカルで保管するケースのセキュリティ対策例

<table>
<tr><th></th><th>残高管理型</th><th colspan="2">電子証書型</th></tr>
<tr><th></th><th></th><th>(A) 金銭データを外部に漏洩させない対策</th><th>(B) 金銭データと ID を紐づけする対策</th></tr>
<tr><td>保管先にある金銭データ等の偽造・改ざん、複製対策</td><td>• 決済事業者による ID へのデジタル署名の付与、決済事業者の署名鍵の保護、デバイスの耐タンパー性（決済事業者の検証鍵の保護）
• ①または②の対策
①デバイスの耐タンパー性（金銭データの保護）
②デバイスによる金銭データへのデジタル署名の付与、デバイスの耐タンパー性（署名鍵の保護）
• デバイスの耐タンパー性（署名鍵の保護）</td><td>• 決済事業者によるデジタル署名の付与、決済事業者の署名鍵の保護
• デバイスの耐タンパー性（金銭データの保護）</td><td>• 決済事業者によるデジタル署名の付与、決済事業者の署名鍵の保護
• デバイスの耐タンパー性（金銭データの保護）</td></tr>
<tr><td rowspan="3">通信されるデータ（電文／金銭データ等）の偽造・改ざん、複製対策</td><td rowspan="2">• デジタル署名の付与、デバイスの耐タンパー性（署名鍵の保護）
• チャレンジ・レスポンス方式等の採用等</td><td>• 暗号通信、耐タンパー性（復号鍵の保護）</td><td>• デジタル署名の付与、デバイスの耐タンパー性（署名鍵の保護）</td></tr>
<tr><td colspan="2">• ①または②の対策
①チャレンジ・レスポンス方式の採用等
②サーバに還流した識別番号の重複チェック</td></tr>
<tr><td colspan="3">• 公開鍵証明書の利用、決済事業者の署名鍵の保護、デバイスの耐タンパー性（決済事業者の検証鍵の保護）</td></tr>
<tr><td>なりすまし対策</td><td colspan="3">• デバイスの耐タンパー性（登録データの保護、提示データの保護）</td></tr>
</table>

護が必要となる。また、デバイス間で送受信されるデータの複製への対策としては、残高管理型と電子証書型のどちらについても、過去の決済で利用されたデータの複製でないことを確認する手段が必要となる。

金銭データをローカルで保管する場合についても、本節（1）と同様、セキュリティ対策技術の有効性が低下した場合の影響について、特に、ユーザの管理下にあるデバイスが攻撃された状況を想定しておくことは重要である。

残高管理型では、デバイスの耐タンパー性によって金銭データが保護される。そのため、仮に攻撃者 C が自身のデバイスへの攻撃に成功し、内部にあるデータの書換えを行うことができた場合、攻撃者 C は金銭データを繰り返し偽造することが可能となる。

一方、電子証書型では、金銭データに決済事業者によるデジタル署名が付与されるため、攻撃者がデバイス内のデータを自由に書換えできるようになったとしても金銭データの偽造・改ざんは引き続き困難であるといえる。また、デバイス内にある金銭データの複製対策には、3 節（2）ロ．で説明したとおり、（A）金銭データが外部に漏洩することがないよう、デバイスの耐タンパー性と暗号化通信による方法と、（B）金銭データの受領者が不正を検知できるよう、金銭データと ID を紐づけする方法が考えられる。（A）は、耐タンパー性で金銭データを保護する対策であるため、自身のデバイスへの攻撃に成功した場合には、繰り返し金銭データの複製が可能であり、複製した金銭データを不正に使用することができてしまう。金銭データには識別番号が振られているものの、複数のユーザに複製した金銭データを送信する場合には、受領者単独で複製であることを検知することは困難である[32]。また、（B）は、金銭データにデジタル署名を付与するという対策を講じるものであり、デバイスへの攻撃によって、金銭データと同様に署名鍵も読み出すことができれば、複製した金銭データを繰り返し送金に使用することが可能となる。

このように、残高管理型では、デバイス内部にあるデータの改ざんによって金銭データを限りなく増やすことが可能であり、電子証書型では、デバイス内データの複製によって金銭データを限りなく増やすことができる。ただし、電子証書型では、金銭データの識別番号を利用することで、複製による不正を働いたユーザを事後的に特定するという方法も提案されていることから、攻撃を抑止できる可能性がある。攻撃者の手元にあるデバイスへの攻撃リスクは、相対的に高く、決済事業者がデバイスへの攻撃を直ちに検知することは難しいことから、仮に攻撃が成功した場合においても、そのリスクを低く抑える仕組みが必要であろう。

32 ID に対応するユーザだけが金銭データを使用できるよう対策を講じた方法（B）では、金銭データに移転履歴が付与される。これにより、決済事業者に金銭データが還流してきたタイミングで同じ識別番号をもつ金銭データがあれば、どのユーザが複製したのかを特定することができる。しかし、耐タンパー性で金銭データの漏洩を防止する方法では、金銭データに保有者の ID がつかないため、同様の方法で決済事業者が不正者を特定することは困難である。

また、攻撃者Cが他ユーザAのもつデバイスAへの攻撃に成功した場合を想定すると、残高管理型では、ユーザAの金銭データを繰り返し偽造できるほか、電子証書型においても、ユーザAの金銭データを複製できることになる。電子証書型のうち、金銭データとIDを紐づけする対策を講じた方法（B）については、さらに、デバイスAに保管されている決済事業者の検証鍵を改ざんすることで、偽造した金銭データを受け入れさせるようにする攻撃も考えられる[33]。他ユーザのデバイスへの攻撃は、自身のデバイスへの攻撃より相対的に難しいとは考えられるが、電子証書型においても、金銭データの偽造リスクがある点には留意が必要である。

5. おわりに

本稿では、チャージ型決済について、その実現方法を金銭データの保管形態と保管場所の違いで4つの方法に分類し、金銭目的とした不正行為で想定される攻撃手順を分析したうえで、必要となるセキュリティ対策について考察を行った。その結果を金銭データの保管場所で整理すると、金銭データをリモートで保管する方法については、残高管理型と電子証書型のどちらについても、同じセキュリティ対策によって、金銭目的の攻撃を防止することが可能であるといえる。また、金銭データをローカルで保管する方法についても、残高管理型と電子証書型では、同じセキュリティ対策技術によって不正を防止することが可能である。そのため、残高管理型と電子証書型については、セキュリティ対策が期待通りに機能している限りにおいて、同水準のセキュリティを実現可能であるといえる。

セキュリティ対策技術の有効性低下によって、リスクが顕現化してしまった場合の影響度合いについては、金銭データの保管形態や保管場所によって違いがあることがわかった。ユーザが所有するデバイスは攻撃に晒されるリスクが高いほか、決済事業者が攻撃を検知することは難しいため、デバイスの耐タンパー性低下による影響度合いについて整理しておくことは重要である。金銭データをローカルで保管する方法では、デバイスの耐タンパー性に安全性を依拠する範囲が相対的に大きいため、デバイスの所有者自身がデバイス内のデータを不正に操作することで、金銭データを無制限に偽造したり、金銭データを繰り返し複製して決済に使用したりできてしまう。一方、金銭データをリモートで保管する場合には、攻撃者が自分のデバイス内のデータを不正に操作できたとしても、不正に金銭的価値を増やすことはできないが、他ユーザのデバイスへの攻撃に成功すれば、当該ユーザの金銭データ

33 偽造された金銭データを受け取ったユーザAは、（決済事業者の検証鍵が改ざんされていないデバイスをもつ）他ユーザに同金銭データを送金すると、その時点で、偽造であることが判明するため、偽造された金銭データの送金元を特定することが可能ではある。

で不正決済を行うことができる。もっとも、こうした攻撃はサーバ等でのユーザ認証によって防ぐことも可能であることから、デバイスの耐タンパー性低下をリスクとして考えた場合には、金銭データをサーバ等で保管する方法の安全性が相対的に高いといえよう。

このように、チャージ型決済については、さまざまな状況を考慮して方式の選択を行うことが望ましい。また、セキュリティ対策を講じるに当たっては、金銭データの保管形態や保管場所によって、対策にかかる計算量や通信量に差異が生じる。こうした違いはユーザの利便性に大きく影響するため、セキュリティと利便性のトレードオフにも留意が必要であろう。

参考文献

相澤英孝、『電子マネーと特許法』、弘文堂、2000 年
磯部光平・宇根正志、「スマートフォン等のスマート・デバイスにおけるセキュリティ：プラットフォーム化によるリスクの現状と展望」、『金融研究』第 40 巻第 3 号、日本銀行金融研究所、2021 年、77～102 頁
エヌ・ティ・ティ・コミュニケーションズ株式会社、「電子マネー『スーパーキャッシュ』に関する今後の NTT コミュニケーションズの取組みについて」、エヌ・ティ・ティ・コミュニケーションズ株式会社、2000 年（https://www.ntt.com/release/2000NEWS/0004/0428.html、2021 年 10 月 28 日）
岡本龍明・太田和夫、「理想的電子現金方式の一方法」、『電子情報通信学会論文誌』、J76-D-I No. 6、電子情報通信学会、1993 年、315～323 頁
鈴木雅貴、「電子マネー・システムにおけるセキュリティ対策」、『知識ベース　知識の森』、電子情報通信学会、11 群―7 編―7 章、2010 年
中山靖司、「実現せまる電子マネーの現状　電子マネーの仕組みとその技術的背景」、『Dr. Dobb's JOURNAL JAPAN』1998 年 2 月号、翔泳社、1998 年 a、70～81 頁
――――、「電子マネー技術と特許」、金融研究所ディスカッション・ペーパー No. 1998-J-33、日本銀行金融研究所、1998 年 b
――――・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
――――・森畠秀実・阿部正幸・藤崎英一郎、「電子マネーの一実現方式について―安全性、利便性に配慮した新しい電子マネー実現方法の提案―」、『金融研究』第 16 巻第 2 号、日本銀行金融研究所、1997 年、75～86 頁
日本規格協会情報技術標準化研究センター、「平成 14 年度耐タンパー性調査研究委員会報告書」、情報処理推進機構、2003 年
日本銀行、「中央銀行デジタル通貨に関する日本銀行の取り組み方針」、日本銀行、2020 年
日本銀行決済機構局、「中銀デジタル通貨が現金同等の機能を持つための技術的課題」、決済システムレポート別冊、日本銀行、2020 年
日本電信電話株式会社、「新しい電子マネー実験システムを試作―安全性、信頼性、効率性を一段と高めた新方式を採用―」、日本電信電話株式会社、1996 年
山内利宏、「スマートフォン端末におけるセキュリティ上の脅威と対策：権限昇格攻撃と悪性ウェブサイトへの誘導に焦点を当てて」、『金融研究』第 40 巻第 4 号、日本銀行金融研究所、2021 年、25～54 頁
Bank of England, "Central Bank Digital Currency, Opportunities, Challenges and Design," Bank of England, 2020.

Basin, David, Ralf Sasse, and Jorge Toro-Pozo, “The EMV Standard: Break, Fix, Verify,” arXiv:2006.08249, 2020.

Boar, Codruta, and Andreas Wehrli, “Ready, Steady, Go? - Results of the Third BIS Survey on Central Bank Digital Currency,” BIS Papers, 114, Bank for International Settlements, 2021.

Brands, Stefan, “Untraceable Off-Line Cash in Wallet with Observers,” Proceedings of CRYPTO ’93, Lecture Notes in Computer Science, 773, Springer, 1993, pp. 302–318.

Committee on Payment and Settlement Systems and the Group of Computer Experts of the Central Banks of the Group of Ten Countries, “*Security of Electronic Money*,” Bank for International Settlements, 1996.

European Central Bank, “Report on a Digital Euro,” European Central Bank, 2020.

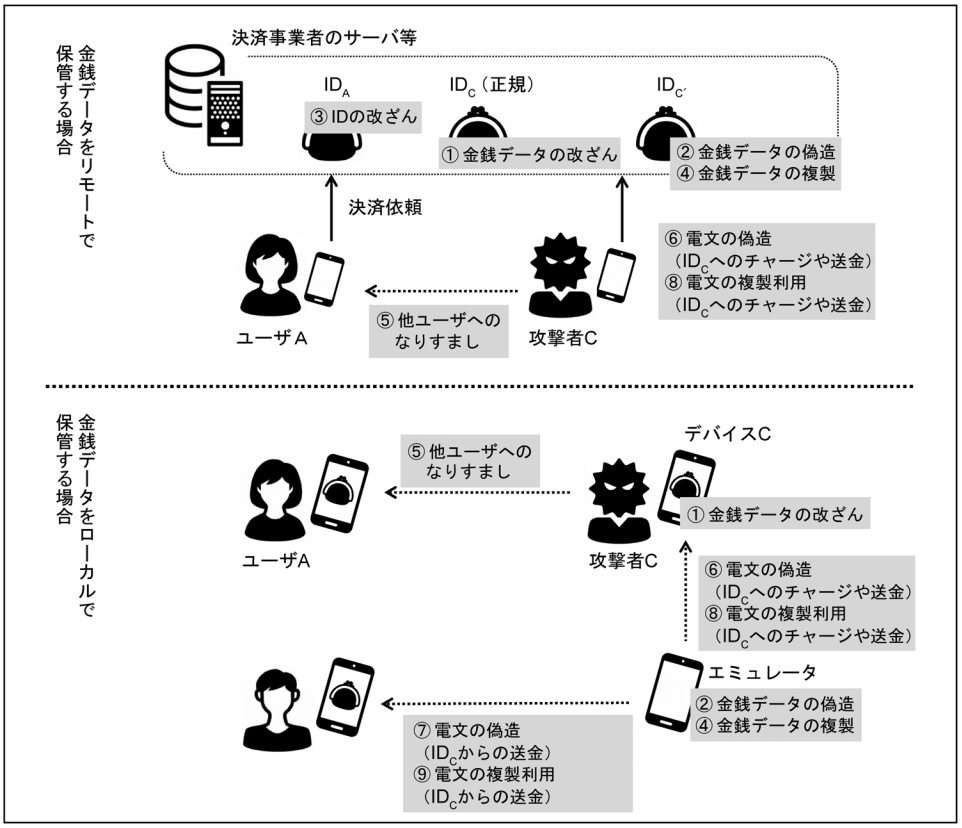
Nakamoto, Satoshi, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2009 (available at https://bitcoin.org/bitcoin.pdf、2021 年 10 月 28 日).

補論 1.　残高管理型決済におけるリスクとその対策

(1)　想定されるリスク

残高管理型決済スキームに対して考えうる金銭目的の攻撃には、攻撃者が有する金銭的価値を増やすために、サーバ等／デバイスにある金銭データを偽造・改ざん、複製（リスク①～④）する攻撃と、他ユーザから攻撃者への送金を偽装（リスク⑥、⑧）する攻撃がある。また、他ユーザの金銭データを奪取する攻撃（リスク③、⑤）のほか、不正送金用に電文を偽造・改ざん、複製する攻撃（リスク⑦、⑨）がある。これら攻撃の詳細は以下のとおりである（図表 A-1 参照）。なお、以下はすべて攻撃者 C によって実施される行為を示すものであり、攻撃者 C が決済サービスを利用する際に使用する ID を ID_C とする。

図表 A-1　残高管理型で想定されるリスク



① 保管先にある金銭データを改ざんすることで、不正に資産を増やす。
— ID_C の金銭データを改ざんする。
② 金銭データを偽造することで、不正に資産を増やす。
— ID を $ID_{C'}$ とする金銭データを偽造し、サーバ等あるいは攻撃用のデバイス（以降、「エミュレータ」と呼ぶ）に書き込む[34]。
③ 保管先にある他ユーザの ID を改ざんすることで、不正に資産を増やす[35]。
— サーバ等にある他ユーザの ID を $ID_{C'}$ に改ざんする。
④ 金銭データを複製することで、不正に資産を増やす。
— 金銭データ・ID_C を複製し、サーバ等あるいはエミュレータに書き込む。
⑤ 他ユーザになりすますことで、不正に送金を行う。
— 他ユーザのデバイスを盗取し、当該ユーザの金銭データを使用して不正に送金を行う。
— 他ユーザの送金電文を通信路から入手し、当該ユーザになりすまして不正に送金を行う[36]。
⑥ 送金先を ID_C とする電文を偽造し、不正に資産を増やす。
— 入金処理端末等や他ユーザから ID_C へのチャージ・送金を示す電文を偽造する。
— リモートで金銭データを保管する場合には、送金元ユーザになりすまして偽造した電文を決済事業者に送信する。ローカルで保管する場合では、偽造した電文をエミュレータからデバイス C に送信する。
⑦ 送金元を ID_C とする電文を偽造し、不正に送金を行う[37]。
— ID_C からの送金を示す電文を偽造し、エミュレータから決済事業者や他ユーザのデバイスに送信する（エミュレータから送信するため、ID_C の金銭データは減額されない）。
⑧ 送金先を ID_C とする電文を複製し、不正に資産を増やす。
— 入金処理端末等や他ユーザから ID_C へのチャージ・送金処理に使用された電文を複製する。
— リモートで金銭データを保管する場合には、送金元ユーザになりすまして複製した電文を決済事業者に送信する。ローカルで保管する場合では、複

34 攻撃者が有する正規金銭データとの違いを表すため、偽造された金銭データの ID を $ID_{C'}$ とした。
35 ローカル保管タイプでは、デバイスを盗取できれば、ID を改ざんせずとも、同デバイス内の金銭データを送金できる可能性があることから、金銭データをローカルで保管する場合に同攻撃は想定されない。
36 例えば、デバイス A とデバイス B の通信路上に侵入することで、デバイス A による決済を不正に実行する攻撃は、中間者侵入攻撃と呼ばれる。スマートフォンによる非接触型のクレジットカード決済に対して、中間者侵入攻撃を実施した例もある（Basin, Sasse, and Toro-Pozo [2020]）。
37 リモート保管タイプでは、ID_C からの送金を示す電文を偽造すると、サーバ等にある ID_C の金銭データが減額されてしまうことから、金銭データをリモートで保管する場合に同攻撃は想定されない。

製した電文をエミュレータからデバイス C に送信する。

⑨ 送金元を ID_C とする電文を複製し、不正に送金を行う[38]。

— 一度送金に使用した電文を複製し、エミュレータから決済事業者や他ユーザのデバイスに送信する（エミュレータから送信するため、ID_C の金銭データは減額されない）。

(2) セキュリティ対策

イ. 金銭データの偽造・改ざん耐性

（金銭データをリモートで保管する場合）

リスク①～③への対応として、金銭データ・ID の偽造（リスク②）・改ざん（リスク①、③）への対策を講じることが求められる。金銭データをサーバで保管する場合では、サーバへの不正アクセス対策によって金銭データ・ID の偽造を防止し、改ざんから保護する方法のほか、金銭データ・ID に決済事業者のデジタル署名を付与することで偽造・改ざんを検知可能にする方法もある。後者の場合には、決済事業者による署名鍵の安全な保管も必要となる。

金銭データの保管をブロックチェーンで行う場合では、ブロックチェーン・ネットワークによる合意形成により、金銭データの偽造・改ざんの防止を図ることになる。イーサリアムでは、全ユーザの金銭データのハッシュ値をブロックに含めることで偽造・改ざんを困難にする手法が採られている。ブロックの生成には膨大な計算を必要とする仕組みが採られているほか[39]、過去に生成されたブロックと新規ブロックをハッシュ・チェーンで連結させることで、ブロックの前後関係の担保とブロック内データの偽造・改ざんを困難にしている。

（金銭データをローカルで保管する場合）

金銭データをデバイスに保管する場合においては、金銭データの偽造・改ざん（リスク①、②）を防止するうえで、デバイスの保有者本人であってもアクセスできないよう、耐タンパー性によって金銭データを保護する方法のほか、金銭データ更新の都度、デバイスによるデジタル署名を付与することで、偽造・改ざんを検知できるようにしておくことが考えられる。後者の場合には、別途、署名鍵の保護が必須であり、デバイスの耐タンパー性が求められるという点は前者と共通である。

また、偽造した金銭データをエミュレータ内に書き込み（リスク②）、偽造した金銭データを用いて送金する攻撃に対しては、決済時に決済相手の ID が決済事業

38 リスク⑦と同様の理由により、金銭データをサーバ等で保管する場合に対する攻撃は想定されない。
39 イーサリアムでは、合意形成アルゴリズムを PoW から PoS に移行する予定としている。

者によって付与されたものであり、偽造されたものでないことの確認によって対応することが考えられる。こうした確認には、ID に決済事業者によるデジタル署名を付与しておき、それを受領者に送信する方法が考えられる。受領者側では、デジタル署名の検証に用いる決済事業者の検証鍵が正しいものであることを確認したうえで、デジタル署名を検証することになる。インターネット接続している場合には、公開鍵認証局のサイト等にアクセスすることで、決済事業者の検証鍵が正当であることを確認可能であるが、インターネット接続が困難な環境では、同様の確認ができない。そのため、インターネット接続が困難な環境での決済を想定する場合には、すべてのデバイスに、決済事業者の検証鍵を事前に保管しておくことが必要であり、改ざんされることのないよう耐タンパー性による保護が求められる[40]。

ロ. 金銭データの複製耐性

（金銭データをリモートで保管する場合）

金銭データ・ID の複製（リスク④）への対応について、金銭データをサーバで保管する場合には、サーバへの不正アクセス対策によって、データを複製させない事前の対策のほか、ID の重複チェックによって複製を検知するという方法もある。ブロックチェーンでは、ブロックチェーン・ネットワークによって、ID の重複チェックが行われており、複製されたデータの書込みが困難となっている。

（金銭データをローカルで保管する場合）

金銭データをデバイスで保管する場合には、正規デバイス内の金銭データ・ID をエミュレータに複製し（リスク④）、複製したデータを用いて送金を行う攻撃が考えられる。ただし、決済相手となるデバイスとの間ではデジタル署名を付与した電文の送受信が必要となることから（本節（2）ニ.）、本攻撃を行うには、署名生成のための署名鍵も複製する必要がある。そのため、正規デバイス内の署名鍵を保護することで、間接的に複製した金銭データによる決済を防止することが考えられる。

ハ. なりすまし耐性

第三者によるなりすまし（リスク⑤）へは、デバイスを操作して送金しようとするユーザが、送金元の ID に対応するユーザであることの確認によって防止することが考えられる。ID に対応するユーザであることの確認は、ユーザ認証と呼ばれ、ID に紐づけする形で事前登録した情報（登録データ）とユーザがデバイスに入力するデータ（提示データ）との照合によって行われる。ユーザ認証を実施する主体は、決済事業者となるが、ユーザ認証を実施する場所については、サーバ等やデバイスが考えられる。

40 決済事業者の検証鍵が有効期限を迎えた場合等には、再インストールの作業が必要となる。

サーバ等で行うユーザ認証のうち、登録データと提示データに同じものを利用する場合には、登録データを管理するサーバへの不正アクセス対策が必要であるほか、提示データが漏洩しないよう暗号化等によって対策を講じることが必要となる。ユーザ認証に非対称なデータを用いる場合では、登録データが公開可能となるが、当該データが偽造・改ざんされることのないよう、対策が必要である。

デバイスで実施するユーザ認証では、デバイス内の登録データや認証時に使用した提示データが漏洩しないよう、耐タンパー性による保護が必要になる。また、デバイス内で実施した認証結果を決済事業者に送信する際には、認証結果の偽造・改ざん対策として、デジタル署名の付与が必要となることから、署名鍵の安全な保管も要件となる。

金銭データをサーバ等で保管している場合には、ユーザ認証をサーバ等とデバイスのいずれでも実行できるが、金銭データをデバイスで保管する場合では、ユーザ認証もデバイスで実行することになる。

ニ．電文の偽造・改ざん耐性

送金を示す電文の偽造（リスク⑥）に対しては、電文の送信者が金銭的価値の正規保有者であることを確認できる仕組みが必要である。つまり、決済事業者や金銭データの受領者には、受信した電文が当該金銭的価値の保有者によって生成されたものであり、かつ、電文が改ざんされていないことの確認が求められる。電文の改ざん対策にはデジタル署名が利用可能であり、別途、デジタル署名の生成者と ID との対応関係を確認することで、金銭的価値の保有者によって生成された電文であることが確認可能となる。

チャージを示す電文については、決済事業者によって生成され、改ざんされていないことの確認が必要であり、これもデジタル署名によって実現可能である。ブロックチェーンの場合には、金銭データの発行がブロックチェーン上で行われるため、入金処理端末等からブロックチェーン・ネットワークに対してチャージを指示する電文が送信されることはない。

（金銭データをリモートで保管する場合）

金銭データをサーバ等で保管する場合、デジタル署名の生成者と ID との対応関係については、決済事業者がデジタル署名の検証鍵と ID をリストにしておくことで確認することができる。こうしたデジタル署名用の検証鍵は、サービス利用開始時に登録することになる。署名鍵と検証鍵のペアについては、決済事業者が生成する場合とデバイス内で生成する場合が考えられるが、スマートフォンの多くは、デバイス内の安全な領域で鍵を生成・保管する機能を有しており、こうした機能が利用できるのであれば、デバイス内で生成する方が望ましい。また、署名鍵については、外部からアクセスできないように保護することが必要となる。なお、暗号資産

では、検証鍵を ID として利用することで対応関係を確認できるようにしている。

（金銭データをローカルで保管する場合）

金銭データをデバイスで保管する場合では、電文の送受信がデバイス間で行われるため、送金先となるデバイスがデジタル署名の検証を行う。不特定多数との決済が想定される場合には、全員分の検証鍵を事前に入手し、検証鍵と ID をリストにしてデバイス内に保管しておくことは難しい。そのため、リスト方式ではない方法で ID と検証鍵との関係を確認する手段が必要であり、その実現には決済事業者による公開鍵証明書が利用できる。署名鍵が漏洩してしまった場合への対応として、公開鍵証明書は、署名鍵に対応する検証鍵の有効性を保証する役割も担っており、デバイスがインターネットに接続できる環境であれば、デジタル署名の検証時にリアルタイムで検証鍵の有効性を確認することができる。

また、攻撃者が自身の金銭データを送金する電文を偽造して（リスク⑦）、エミュレータから送信する攻撃に対しては、ユーザ本人であってもデバイス内の署名鍵にアクセスできないよう保護することで対策を講じることが必要である。

ホ．電文の複製耐性

送金を示す電文を複製して利用する攻撃（リスク⑧、⑨）に対しては、当該取引にしか使用することができないよう、リアルタイムで生成されたものであることを確認できる仕組みが有効である。そのためには、デジタル署名の生成方法を対話型に変更したチャレンジ・レスポンス方式の採用が考えられるほか、リモート保管の場合であれば、改ざん困難な識別番号を電文に付与して決済事業者が重複をチェックするという方法等が考えられる。

ヘ．まとめ

本節での考察をまとめると、残高管理型に想定されるリスクとその対策技術は、図表 A-2 のようにまとめられる。

図表 A-2　残高管理型のセキュリティ要件を充足する具体的対策案

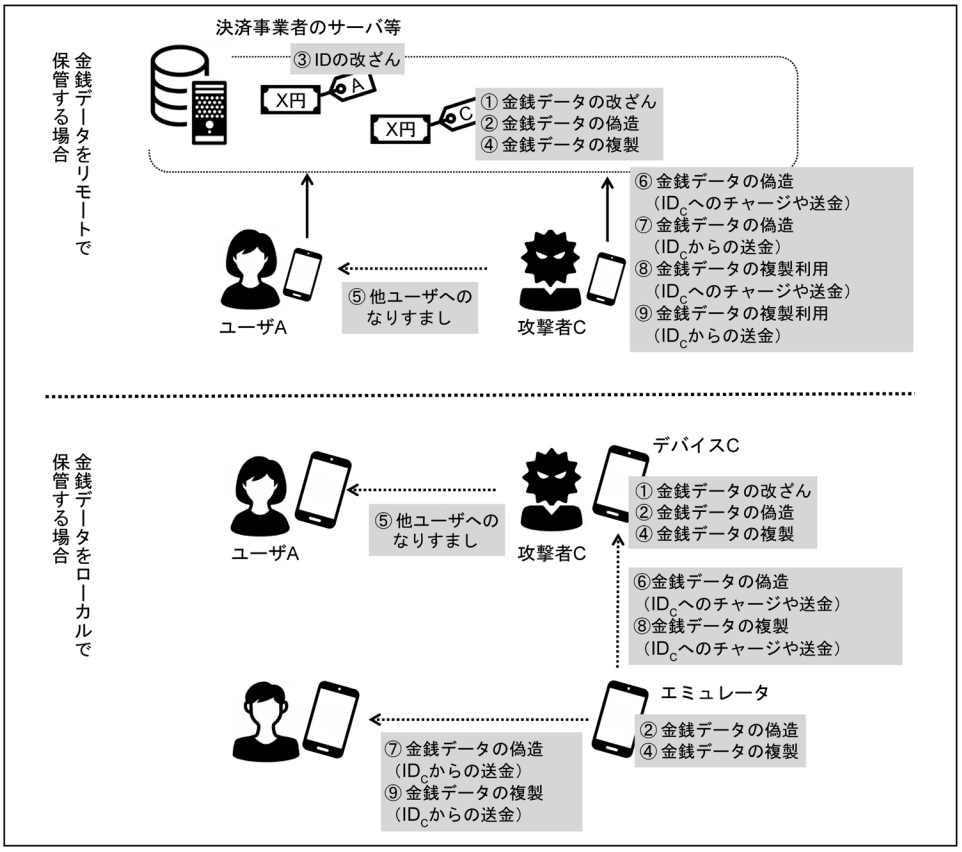
	金銭データをリモートで保管する場合	金銭データをローカルで保管する場合
イ．金銭データ・ID の偽造・改ざん対策	• ①または②または③の対策 ①サーバの不正アクセス対策（金銭データの保護） ②決済事業者による金銭データ・ID へのデジタル署名付与、決済事業者の署名鍵の保護 ③ブロックチェーンの利用	• ①または②の対策 ①デバイスの耐タンパー性（金銭データの保護） ②デバイスによる金銭データへのデジタル署名の付与、デバイスの耐タンパー性（署名鍵の保護） • 決済事業者による ID に対するデジタル署名の付与、決済事業者の署名鍵の保護、デバイスの耐タンパー性（決済事業者の検証鍵の保護）
ロ．金銭データの複製対策	• ①または②の対策 ①サーバの不正アクセス対策（金銭データの保護） ②ID の重複チェック	• デバイスの耐タンパー性（署名鍵の保護）
ハ．なりすまし対策（登録データと提示データに同じものを利用するケース）	サーバでの認証の場合 • サーバへの不正アクセス対策（登録データの保護） • デバイスの耐タンパー性（提示データの保護） • 通信データの暗号化 デバイスでの認証の場合 • デバイスの耐タンパー性（登録データの保護、提示データの保護）	• デバイスの耐タンパー性（登録データの保護、提示データの保護）
ニ．電文の偽造・改ざん対策	• 電文へのデジタル署名の付与、決済事業者の署名鍵の保護、デバイスの耐タンパー性（署名鍵の保護）	
	• 検証鍵と ID のリスト化等	• 公開鍵証明書の利用、決済事業者の署名鍵の保護、デバイスの耐タンパー性（決済事業者の検証鍵の保護）
ホ．電文の複製対策	• チャレンジ・レスポンス方式の採用等	

補論 2.　電子証書型決済におけるリスクとその対策

(1)　想定されるリスク

電子証書型決済スキームに対して考えうる金銭目的の攻撃には、攻撃者が有する金銭データを増やすために、サーバ等／デバイスにある金銭データを偽造・改ざん、複製（リスク①～④）する攻撃と、他ユーザから攻撃者への金銭データの送信を偽装（リスク⑥、⑧）する攻撃がある。また、他ユーザの金銭データを奪取する攻撃（リスク⑤）のほか、不正送金用に金銭データを偽造・複製する攻撃（リスク⑦、⑨）がある。これら攻撃の詳細は以下のとおりである（図表 A-3 参照）。

図表 A-3　電子証書型で想定されるリスク



① 保管先にある金銭データを改ざんすることで、不正に資産を増やす。
— 保有者を ID_C とする金銭データを改ざんする。
② 金銭データを偽造することで、不正に資産を増やす。
— 保有者を ID_C とする金銭データを偽造し、サーバ等あるいは正規デバイスやエミュレータに書き込む。
③ 保管先にある他ユーザの金銭データに対応する ID を改ざんすることで、不正に資産を増やす[41]。
— サーバ等にある他ユーザの金銭データの保有者を ID_C に改ざんする。
④ 金銭データを複製することで、不正に資産を増やす。
— 保有者を ID_C とする金銭データを複製して、サーバ等あるいは正規デバイスやエミュレータに書き込む。
⑤ 他ユーザになりすますことで、不正に送金を行う。
— 他ユーザのデバイスを盗取し、当該ユーザの金銭データを使用して不正に送金を行う。
— 他ユーザの金銭データを通信路から入手し、当該ユーザになりすまして不正に送金を行う。
⑥ 送金先を ID_C とする金銭データを偽造し、不正に資産を増やす[42]。
— 入金処理端末等や他ユーザから ID_C に発行・送金される金銭データを偽造する。
— リモートで金銭データを保管する場合は、送金元ユーザになりすまして偽造した金銭データを決済事業者に送信する。ローカルで保管する場合には、偽造した金銭データをエミュレータからデバイス C に送信する。
⑦ 送金元を ID_C とする金銭データを偽造し、不正に送金を行う。
— 送金元を ID_C とする金銭データを偽造し、エミュレータから決済事業者あるいは他ユーザのデバイスに送信する。
⑧ 送金先を ID_C とする金銭データを複製し、不正に資産を増やす。
— 入金処理端末等や他ユーザから ID_C に発行・送金された金銭データを複製する。
— リモートで金銭データを保管する場合は、送金元ユーザになりすまして複製した金銭データを決済事業者に送信する。ローカルで保管する場合には、複製した金銭データをエミュレータからデバイス C に送信する。
⑨ 送金元を ID_C とする金銭データを複製し、不正に送金を行う。

41 ローカル保管タイプでは、他ユーザのデバイスを盗取できれば、ID を改ざんせずとも当該ユーザとしてデバイス内の金銭データを使用できる可能性があるため、金銭データをローカルで保管する場合に同攻撃は想定されない。

42 金銭データに送金元や送金先の情報が含まれない場合、リスク⑥と⑦は、データの複製によって成立する攻撃と位置付けられる。

― 一度送金に使用した金銭データを複製し、エミュレータから決済事業者あるいは他ユーザのデバイスに送信する。

(2) セキュリティ対策

イ. 金銭データの偽造・改ざん耐性

電子証書型では、送金元デバイスから送信された金銭データがそのままサーバ等やデバイスで保管されるため、送信データと保管データのいずれかを偽造・改ざんしようとする攻撃が想定される。こうしたリスク①～③、⑥、⑦への対応としては、決済事業者によって発行される金銭データの偽造・改ざんを困難にすること、および、正規保有者以外は金銭データを決済に利用できないことの 2 つの性質が必要となる。

(金銭データをリモートで保管する場合)

まず、決済事業者によって発行される金銭データについては、決済事業者によるデジタル署名等を付与することで偽造・改ざんの検知を可能にする方法が考えられる。ブロックチェーンを利用する場合には、それとは異なる方法で対策が採られている。例えば、ビットコインでは、マイニングに成功したマイナーにその報酬として暗号資産が自動的に新規発行される。新規発行にかかるトランザクションには、「マイナーのアドレス（公開鍵）、金額」が示されており、これらの内容を改ざんするといった不正も想定されるが、マイナーには不正を行わないインセンティブ設計がなされているほか、マイナーのアドレスはマイニングの入力となっており、マイニング結果との照合により偽造・改ざんが検知可能となっている。

すべての金銭データがサーバ等で保管される場合については、正規保有者のみが金銭データを使用できるようにする必要がある。そのためには、金銭データに ID を付与し、金銭データの保有者を確認できるようにすればよい。その一例として、送金時、送金先ユーザの ID を金銭データに加え、当該データに対して送金元ユーザのデジタル署名を付与して金銭データを作成するという方法がある（中山ほか[1997]、Nakamoto [2009]）。金銭データには ID の移転履歴が付与されることになるため、決済事業者は金銭データの前所有者によって ID が変更されたことを確認できる。なお、デジタル署名の生成者と ID との対応関係については、それらをリストにしておく方法等によって別途確認する必要がある。

ブロックチェーンでは、膨大な計算コスト等をかけて、ブロックをハッシュ・チェーンでつなぐことで、ブロックの前後関係を担保するとともに、事後的にブロックの中身を改ざんすることを困難としている。このように、ブロックチェーンは、ブロックチェーン・ネットワークによる合意を得たものだけを保管するという

仕組みとすることで、特定のユーザによる偽造・改ざん、および、複製を困難にしている。

（金銭データをローカルで保管する場合）

金銭データをローカルで保管する場合についても、決済事業者によって発行される金銭データは、デジタル署名によって偽造・改ざんの検知を可能にすることができる。決済事業者によって生成された金銭データを正規保有者以外が使用できないようにする方法には、（A）金銭データが外部に漏洩することがないよう、耐タンパー性によって保護するとともに、金銭データの送信時には送金先ユーザの公開鍵で暗号化を行うという方法が挙げられる（Brands [1993]）。また、もう 1 つのアプローチには、リモート保管の場合と同様、（B）金銭データと ID を紐づけし、決済時に ID とユーザとの対応関係を確認できるようにする方法がある。前者は金銭データそのものを耐タンパー性で保護するものであるのに対し、後者はデジタル署名によって偽造・改ざん耐性をもたせることから耐タンパー性で保護すべき対象はデジタル署名用の署名鍵のみという違いがある。また、前者では送金時に使用する暗号鍵が送金先ユーザの鍵であるか検証が必要であり、後者では受領時に金銭データの ID とデジタル署名との対応関係を確認する必要がある。いずれにおいても、決済事業者による公開鍵証明書の利用が必要であり、決済事業者の検証鍵が改ざんされることのないよう、耐タンパー性による保護が必要である。

ロ．金銭データの複製耐性

（金銭データをリモートで保管する場合）

保管先に金銭データを複製する攻撃（リスク④）については、サーバ等への不正アクセス対策によってデータの複製を防止する方法のほか、金銭データに付与された識別番号のチェックによって複製を検知する方法がある。また、複製した金銭データを利用する攻撃（リスク⑧、⑨）に対しても、受信した金銭データの識別番号をチェックすることで複製を検知可能であるほか、チャレンジ・レスポンス方式を採用することも考えられる。ブロックチェーンにおいても、ブロックチェーン・ネットワークによって、識別暗号のチェックが行われている。

（金銭データをローカルで保管する場合）

複製した金銭データを送金に使用する攻撃に対しては、まず、複製した金銭データをデバイスに書き込む（リスク④）ことができないよう、デバイスの耐タンパー性が必要となるほか、複製した金銭データをエミュレータから正規デバイスに送信する攻撃（リスク④、⑧、⑨）への対策が必要となる。他ユーザから受領した金銭データを複製して使用する場合（リスク⑧）には、本節（2）イ．で整理したとおり、正規デバイス内にある復号鍵や署名鍵が必要となるため、デバイスの所有者で

あっても復号鍵や署名鍵にアクセスできないよう耐タンパー性で保護することによって攻撃を防ぐことが可能である。さらに、他ユーザに送信した金銭データを複製して使用する攻撃（リスク⑨）については、受信したデータがリアルタイムで生成されたものであることを確認できるチャレンジ・レスポンス方式等を利用することで対策が可能である。そのほか、決済事業者に還流してきた金銭データの識別番号を保管し、重複チェックすることで、複製された金銭データを事後的に特定するという方法もある（中山ほか［1997］）。

ハ．なりすまし耐性

リスク⑤のうち、デバイスを盗取して不正決済を行う攻撃については、補論 1（2）ハ．で整理したユーザ認証によって対策を講じることができる。また、通信路から他ユーザの金銭データを入手して行う不正決済については、本節（2）イ．で整理したとおり、正規保有者以外が使用できないように対策を講じておくことで防止することができる。耐タンパー性と暗号化によって金銭データを保護する対策を採用している場合においては、暗号文の複製を送信して不正決済を行う攻撃も考えられるため、本節（2）ロ．で整理したように複製されたデータでないことを確認可能とする仕組みとして、チャレンジ・レスポンス認証のようにリアルタイム性を確認できる方法を採用する必要がある。

ニ．まとめ

本節での考察をまとめると、電子証書型に想定されるリスクとその対策技術は、図表 A-4 のようにまとめられる。

図表 A-4　電子証書型のセキュリティ要件を充足する具体的対策

<table>
<tr><th></th><th>金銭データをリモートで保管する場合</th><th colspan="2">金銭データをローカルで保管する場合</th></tr>
<tr><th></th><th></th><th>（A）金銭データを外部に漏洩させない対策</th><th>（B）金銭データと ID を紐づけする方法</th></tr>
<tr><td>イ. 金銭データ・ID の偽造・改ざん対策</td><td>• ①または②の対策
①決済事業者によるデジタル署名の付与、決済事業者の署名鍵の保護
②ブロックチェーンの利用
• ユーザによるデジタル署名の付与（送金時）、デバイスの耐タンパー性（署名鍵の保護）
• 署名検証鍵と ID のリスト化</td><td>• 決済事業者によるデジタル署名の付与、決済事業者の署名鍵の保護
• デバイスの耐タンパー性（金銭データの保護）
• 金銭データの暗号通信（送金時）</td><td>• 決済事業者によるデジタル署名の付与、決済事業者の署名鍵の保護
• ユーザによるデジタル署名の付与（送金時）、デバイスの耐タンパー性（署名鍵の保護）</td></tr>
<tr><td></td><td></td><td colspan="2">• 公開鍵証明書の利用、決済事業者の署名鍵の保護、デバイスの耐タンパー性（決済事業者の検証鍵の保護）</td></tr>
<tr><td>ロ. 金銭データの複製対策</td><td>• ①または②の対策
①サーバ等の不正アクセス対策（金銭データの保護）
②識別番号の重複チェック
• ③または④の対策
③チャレンジ・レスポンス方式の採用等
④識別番号の重複チェック</td><td>• 耐タンパー性（復号鍵の保護）</td><td>• 耐タンパー性（署名鍵の保護）</td></tr>
<tr><td></td><td></td><td colspan="2">• ①または②の対策
①チャレンジ・レスポンス方式の採用等
②サーバに還流した識別番号の重複チェック</td></tr>
<tr><td>ハ. なりすまし対策</td><td>サーバでの認証のケース
• サーバへの不正アクセス対策（登録データの保護）
• デバイスの耐タンパー性（提示データの保護）
• 通信データの暗号化

デバイスでの認証のケース
• デバイスの耐タンパー性（登録データの保護、提示データの保護）</td><td colspan="2">• デバイスの耐タンパー性（登録データの保護、提示データの保護）</td></tr>
</table>