銀行口座との連携における不正防止に関するガイドライン

（令和2年12月3日制定）

一般社団法人日本資金決済業協会

第１　はじめに

今般、悪意のある第三者が不正に入手した預金者の口座情報等をもとに当該預金者の名義で資金移動業者のアカウントを開設し、銀行口座と連携した上で、銀行口座から資金移動業者のアカウントへ資金をチャージすることで不正な出金を行う事象（以下「本事象」という。）が複数発生した。本事象では、資金移動業者において犯罪による収益の移転防止に関する法律（以下「犯罪収益移転防止法」という。）施行規則第13条第1項第1号に基づく確認を実施し、それに基づく銀行での取引時確認済みの確認及び口座振替契約の締結に際してキャッシュカードの暗証番号のみで認証するケースにおいて、被害の発生が確認されている。

銀行、資金移動業者は、それぞれ、犯罪収益移転防止法に基づく取引時確認義務を負い、また、各法令、監督指針、事務ガイドライン等においても、それぞれ、セキュリティ対策が求められている。

しかしながら、キャッシュレス化において決済手段の連携が進む中、犯罪収益移転防止法施行規則第13条第1項第1号に基づく銀行での取引時確認済みの確認により資金移動業アカウント（以下「アカウント」という。）が開設され、キャッシュカードの暗証番号のみで銀行口座との連携による入金（チャージ）や送金が可能なサービスについては、ひとたび銀行口座情報が不正に入手されてしまった場合には、本事象のように、当該連携の仕組みを悪用した犯罪の被害が生じうる。

当協会は、本事象を受けて、会員の資金移動業者のセキュリティ対策や銀行との連携サービスに関して緊急調査を実施した。同調査等を踏まえ、本ガイドラインは、銀行口座との連携における不正防止のために資金移動業者が講じるべき措置等の考え方及び具体例等を示したものである。

当協会の会員である資金移動業者においては、本ガイドラインの趣旨を踏まえ、自らの提供するサービスを改めて検証し、本ガイドラインに沿った対応を実施することが求められる。

第２　本ガイドラインの適用範囲

本ガイドラインは、当協会の会員である資金移動業者が提供する資金移動サービスを銀行口座と連携する場合において、資金移動業者側が不正防止のために講じるべき措置の考え方及び具体例等を示したものである。

会員の資金移動業者は、本ガイドラインに基づき、銀行口座とアカウントの連携に先立って確認すべき事項、連携後の態勢や被害発生時の対応等、自らの提供するサービスのリスクに応じて講じるべき措置等を検討し、実施されたい。

なお、本ガイドラインでは、資金移動業者側の対応措置等を示すにとどまるが、銀行をはじめとした金融機関、コード決済事業者やシステムベンダー、これらの業界団体等による指針やガイドライン等も参照のうえ、関係各社の連携した対応が不可欠である。

第３　銀行口座との連携に係る不正防止の対応に関する考え方

１．不正防止策の実施

(1) リスク評価等

○　資金移動業者は、アカウントと銀行口座を連携した口座振替によるチャージ機能を提供しようとする場合やその内容・方法を変更しようとする場合には、予め、連携先の銀行（以下、「提携銀行」という。）の口座振替サービスを含むサービス全体のリスクを評価する必要がある。その上で、協力して適切な不正防止策を講じる必要がある。

すなわち、資金移動業者や銀行による確認・認証、口座連携、チャージなど、口座振替に係る一連のプロセスに脆弱性がないか確認し、問題があると認められた場合には、不正防止策を講じた上で、銀行口座との連携の開始やその内容・方法の変更を行う必要がある。

○　また、銀行口座・資金移動サービスの不正利用やシステムへのサイバー攻撃などの手口は、日々、高度化・巧妙化することを踏まえ、資金移動業者は、定期的かつ適時にリスクを再評価し、不正防止策の継続的な改善・向上を図る必要がある。

○　リスクの評価は、提携銀行と協力して実施することが重要であり、双方が相手方の作業に協力する必要がある。

○　口座振替に係る一連のプロセスに脆弱性が認められた場合には、それが解消されるまでの間、アカウントと銀行口座の連携は行わないこと、また、既に銀行口座と連携している場合には、当該銀行の口座からアカウントへの入金を一時停止し、改善を行う必要がある。

(2) 提携銀行による不正防止策の確認

○ 提携銀行の不正防止策について、資金移動業者が確認すべき事項の例は、以下のとおりである。

① (1)のリスク評価を踏まえ、アカウントと銀行口座の連携時における認証手段及び方式がリスクに見合った、実効的な要素を組み合わせた多要素認証(＊)となっているか。

※ なお、アカウントの連携後に口座振替によるチャージをする際の手続においても、一定の牽制の仕組みが設けられていることが望ましい。

② 提携銀行のインターネットバンキングやコールセンター等における認証に用いる情報の登録・変更手続に堅牢な認証を求めているか。

(＊)「多要素認証」
多要素認証とは、本人だけが知りうる情報による認証(パスワード・秘密の質問等)、本人だけが所持しうる物による認証(キャッシュカード、登録済みの端末への SMS 等)、生体認証(顔、指紋、静脈等による認証)のうち、複数の要素を組み合わせた認証をいう。

(3) 資金移動業者による不正防止策(認証等)

○ 銀行における不正防止策のほか、資金移動業者は、(1)のリスク評価及び(2)の提携銀行による不正防止策の確認を踏まえ、下記①の対策を基本とし、それが困難な場合には②～⑤のいずれか若しくは複数の対策又はこれらと同等以上のリスクに見合った不正防止策を追加的に講じる必要がある。

① 資金移動業の利用者に対し、公的個人認証や eKYC 等の方法により自ら取引時確認を行い、本人確認書類等により確認した当該利用者の情報と提携銀行が保有する情報を照合することにより、預金者と当該利用者の同一性を確認すること

※ 提携銀行と照合可能な情報は、各銀行によって異なるものの、提携銀行と協力の上、両者の連携サービス全体において、預金者と当該利用者の同一性を確認する実効的な照合の方法を採用することが必要である。

② 提携銀行に登録された預金者の携帯電話番号に資金移動業者における認証に必要な情報を SMS で送付するなど、電話の所持確認を行うこと

③ 提携銀行に登録された預金者の住所宛てに資金移動業者における認証に必要な情報を転送不要郵便で送付するなど、住所の確認を行うこと

④ 提携銀行のキャッシュカードの所持確認を行うこと

⑤ 銀行口座との連携後、初回のチャージから一定期間、チャージ上限額を犯罪に利用されるおそれが極めて低いと考えられる水準に設定すること

※ 提携銀行における認証の内容と重複しない不正防止策を実施する必要がある。

※ 資金移動業アカウント作成時における犯罪収益移転防止法上の取引時確認を同法施行規則 13 条第 1 項第 1 号に規定する方法により実施する場合には、実効的な取引時確認済みの確認、資金移動業者における継続的顧客管理の充実等の観点から、提携銀行の情報と照合することなどの方法により、資金移動業の利用者から申告を受けた本人特定事項(氏名・住所・生年月日)が正確か確認する必要がある。

○ また、資金移動サービスのリスク・特性に応じて、例えば、チャージ金額が多額である場合には、認証の要素を追加するなどの措置が考えられる。加えて、認証による不正防止策のレベルや、資金移動サービスのリスク・特性に応じて、チャージ金額や回数の上限設定、モニタリング体制のレベルも個別に判断し、実効性のある措置を講じることが重要である。

○ 加えて、提携銀行又は資金移動業者において、口座連携時、チャージ、決済等の利用があった旨を、預金者が銀行に登録したメールアドレス等に通知することにより、被害の早期発見を促す仕組みを講じることも有益である。

※ 提携銀行におけるメールアドレス等の登録・変更時の認証が堅牢であることに留意する必要がある。

○ さらに、犯罪収益移転防止法第 3 条第 3 項に基づき国家公安委員会が作成・公表する犯罪収益移転危険度調査書の内容を勘案し、取引・商品特性や取引形態、取引に関係する国・地域、顧客属性等の観点から、自らが行う取引がテロ資金供与やマネー・ローンダリング等に利用されるリスクについて適切に調査・分析した上で、リスクに応じた適切な取引時確認の方法を採用する必要がある。また、テロ資金供与やマネー・ローンダリング、資金移動サービスの不正利用といった組織犯罪等の手法や態様の高度化・巧妙化を含めた環境変化や自社又は他の事業者における事件の発生状況を踏まえ、定期的かつ適時にリスクを認識・評価し、公的個人認証の導入を含め、取引時確認の向上を図って

いく必要がある。

○　なお、口座振替に係る一連のプロセスに脆弱性が認められ、チャージを停止した資金移動業者がこれを再開する場合には、既存の口座振替契約の中に不正に締結された契約が存在するリスクを踏まえ、再開に先立ち、例えば、資金移動業者側で公的個人認証や eKYC 等の方法により既存利用者の取引時確認をやり直すことや相応の期間において既存利用者のチャージ上限額を犯罪に利用されるおそれが極めて低いと考えられる水準に設定すること等の対策を実施し、また、提携銀行側で不正な契約がないか確認作業を行うことや強化した認証方式により認証をやり直す等の対策を実施し、双方でリスクの低減に関する認識を共有する必要がある。

（4） モニタリング態勢

○　資金移動業者は、銀行口座との連携を行った場合において、資金移動アカウントへの不正なチャージ等が行われていないか、不正検知のモニタリングを行う必要がある。

○　モニタリング態勢の整備にあたっては、銀行口座と連携した資金移動サービスのリスク・特性に応じて、チャージの手続も考慮し、通常の取引とは異なる頻度や金額での取引などについて、適切なシナリオ・閾値を設けるほか、過去の不正利用、詐欺被害、捜査機関等からの照会事例を分析するなど、早期に不正の疑いのある取引を検知できる仕組みを構築し、継続的に見直しを行うことで実効性を高める必要がある。

○　また、不正が疑われる取引を検知した場合には、速やかに提携銀行と情報を共有し、必要に応じてサービスの一時的な利用停止等を実施すること、十分な調査を実施すること、預金者やアカウント保有者に通知することを適切に実行するための態勢を整備する必要がある。

（5） 銀行との契約において考えられる対応

○　以上を講じるため、資金移動業者は、提携銀行との間の契約において、あらかじめ、認証方法、モニタリング態勢や不正が検知された場合の対応等について具体的に合意しておくことが必要である。また、その際、提携銀行との役割分担や責任を明確化しておく必要がある。

２．補償方針について

○　不正が判明した事案において、被害者から資金移動業者に対して補償の求めがあった場合、資金移動業者は、当該被害者が預金口座を有する提携銀行と連携し、速やかに被害金額の補償を実施する必要がある。ただし、被害者に過失がある場合等には個別対応を妨げるものではない。

○　この場合、提携銀行と連携することによって、銀行の預金者に不利益が生じることのないよう、あらかじめ、提携銀行等との間で、預金者保護を最優先とした補償の方針を合意しておく必要がある。また、補償の方針（下記の⑤求償関係は除く。）については、提携銀行等と協力し、周知する必要がある。

○　なお、補償の手続や提携銀行との責任の分担の内容は、個別具体的な契約によるものの、例えば、以下のような項目を契約に盛り込む必要がある。

（補償に関して提携銀行と合意する項目の例）

①　被害者からの被害申告を受け付ける窓口
②　補償する場合の基準や手続（被害者に求める情報や、過失の有無の判断等）
③　補償する場合の方法（補償の実施者を含む）
④　補償する場合の補償範囲
⑤　いずれか一方が補償した場合の求償関係（損害の分担）

○　本事象では、被害者が銀行との間で預金契約を有するものの、資金移動業者との間では直接契約関係にない例であったが、他の不正取引の事案では、被害者が銀行、資金移動業者双方と契約関係にある例も想定される。いずれの場合であっても、銀行、資金移動業者のどちらに先に被害を申告したかによって補償の有無や範囲に差異が生ずるのは避けるべきであり、関係当事者の法的関係を踏まえつつも、提携銀行の定める基準や全国銀行協会による「預金等の不正な払戻しへの対応について」の申し合わせ等も参照し、迅速かつ丁寧に対応する必要がある。

３．相談態勢について

○　資金移動業者は、銀行口座とアカウントの連携を行った場合において、提携銀行の預金者から資金移動サービスに関する問い合わせがあった場合にも、これを受け付け、責任を持って提携銀行と協力して真摯に対応する必要がある。

○　この場合、あらかじめ、提携銀行との間で互いの問い合わせ対応窓口を取決めたうえで、担当部署と密に連携する必要がある。
○　銀行との連携に限らず、今後、決済手段を含むあらゆる金融サービスの連携の促進が見込まれるところ、問い合わせ窓口の一元化などにより、複数の決済手段の連携によって消費者に混乱が生じないよう十分留意する必要がある。
○　なお、相談窓口の設置にあたっては、消費者が安心してアクセスできるように、メールや電話等、一般にアクセス可能な方法を確保するとともに、広く周知する必要がある。
○　また、不正事案の被害者や資金移動サービスのアカウント保有者からの相談事案の集積・分析を行い、リスクの早期検知、対応等の改善を行う必要がある。
○　加えて、提携銀行と相互に相手方への相談を促すこと（たらい回し）などの不適切な対応を行っていないか検証し、不適切な対応が認められる場合には、提携銀行とともに、発生原因の究明、改善措置、再発防止策を的確に講じる必要がある。

４．不正利用が発生した場合の対応態勢について

○　資金移動業者は、銀行口座とアカウントを連携したサービスを提供する場合には、提携銀行と協力の上、不正利用が発生した場合に備えた態勢の整備をすることが不可欠である。
○　資金移動業者側で不正利用の発生を認めた場合には、直ちに、対象となる提携銀行に通知の上、協力して被害の拡大防止に向けた対応を最優先すべきである。
○　例えば、一部の預金者情報が流出し、銀行口座とアカウントの連携における双方の本人認証プロセスに脆弱性があると考えられる場合には、一連のサービス全体としての認証の強化が行われ、安全性が確認されるまでの間は、対象となる提携銀行の口座からアカウントへのチャージを一時停止するなど、資金移動サービスを必要な範囲で制限する措置を講じる必要がある。
○　同時に、提携銀行等の関係者と連携の上、事実関係を調査し、被害の対象となったアカウントの保有者又は連携する銀行口座の預金者への通知や相談対応、当局や当協会への報告のほか、補償に関する対応を行う必要がある。
○　また、資金移動業者が複数の銀行と連携している場合において、他の銀行に

おいても同様の事案が発生するおそれがある場合には、当該他の銀行に対してもただちに連絡し、被害拡大を未然に防止することに努めることが期待される。加えて、利用者の不安や混乱を回避するため、資金移動業者及び提携銀行は適時・適切な情報発信・対外公表を行うよう努める。

○　これらの対応を迅速に行うためには、あらかじめ、不正による被害が発生した場合の緊急連絡ルートや指揮命令系統の構築、提携銀行との連絡態勢、サービスの停止の手続や、補償に関する基準や手続等について、定めておくことが必要である。

５．当協会の取組み

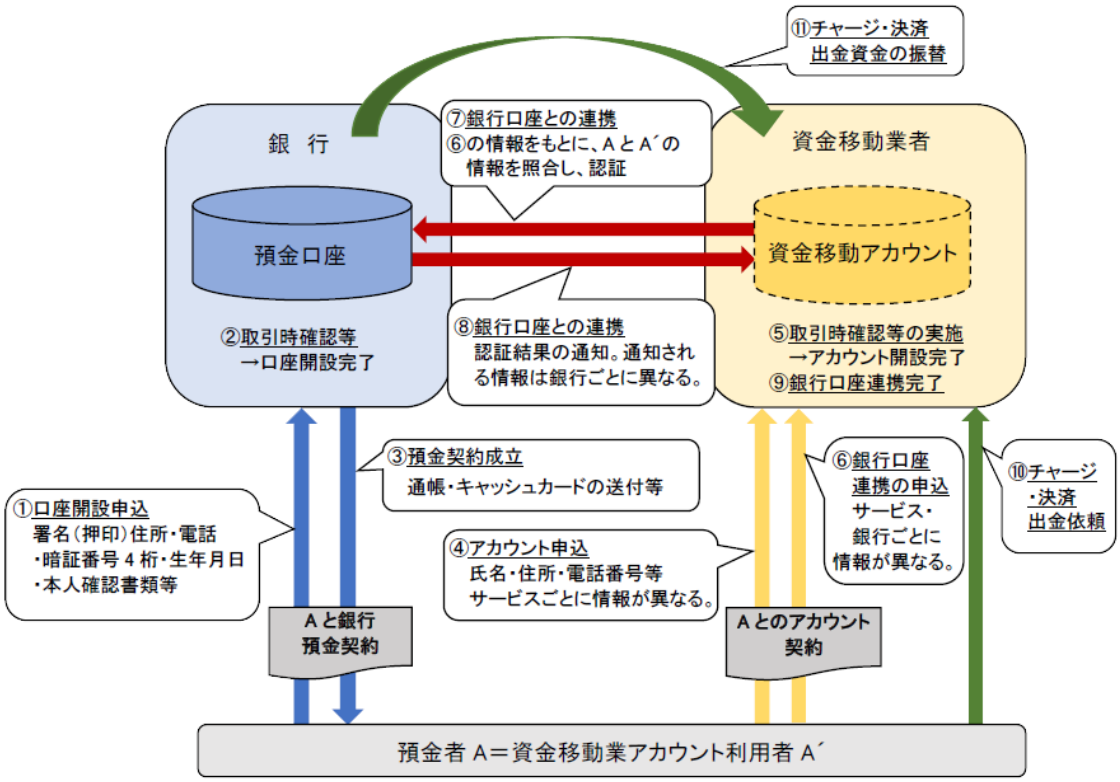
○　当協会においても、資金移動サービスに関する苦情、問い合わせ窓口を設置しており、当協会に寄せられる相談や問い合わせに対し、本事象のような複数のサービスが連携した場合も踏まえた適切な対応をする。

○　そして、当協会に寄せられる相談や問い合わせの内容に加え、会員から報告された不正事案を分析し、会員に共有すること、また、当協会の会員以外の連携先に関する事項についても、他の関係団体と協力し、速やかに会員を通じた連携が可能となるよう努める所存である。加えて、適時に本ガイドラインの適切性を評価し、必要に応じ、改訂を行っていく所存である。

以　上

（参考）

（図１）　資金移動サービスと銀行口座の連携における一般的な各当事者の関係及び手続フロー



（参考）

（図２）　今般の不正利用の事象における当事者の関係と事務フロー