全国銀行協会
資金移動業者等との口座連携に
関するガイドライン

（令和２年 11 月 30 日制定）

一般社団法人
全国銀行協会

１．はじめに

✧ 本ガイドラインは、預金者の口座情報等を不正に入手した悪意のある第三者が、銀行口座と連携して利用する決済サービスを提供している事業者（資金移動業者等[1]）を通じて、銀行口座から不正な出金を行う事案が複数発生したことを契機として、各銀行が資金移動業者等と連携して決済サービスを提供するに際しての考え方・例示等を取りまとめたものである。

✧ 当協会会員銀行においては、本ガイドラインも踏まえ、資金移動業者等と連携し、安心・安全を旨とする銀行口座の位置づけおよびその期待を踏まえたうえで、利便性を意識しつつも、お客さまの資産保全を最優先に、真摯かつ適切に対応いただきたい。

1.1 ガイドライン策定の経緯

✧ 近時、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資金移動業者等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が複数発生している。

✧ こうした不正出金は、資金移動業者等において犯罪収益移転防止法施行規則第 13 条第１項第１号にもとづく確認を実施し、それにもとづく銀行での取引確認済みの確認および口座振替契約（チャージ契約）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、その発生が確認されている。

✧ 当協会は、これまでもインターネット・バンキングでの預金不正引出しに関する注意喚起、セキュリティ対策強化や補償に関する申し合わせなどにより、お客さまが安心・安全にサービスをご利用いただくための取組みを実施してきているが、今回こうした不正出金の発生を受け、その再発防止に向けて、業界としてさらなる取組みが必要であるとの認識にたち、今回、各銀行が資金移動業者等と連携して決済サービスを提供するに際しての考え方・例示等をガイドラインとして取りまとめた。

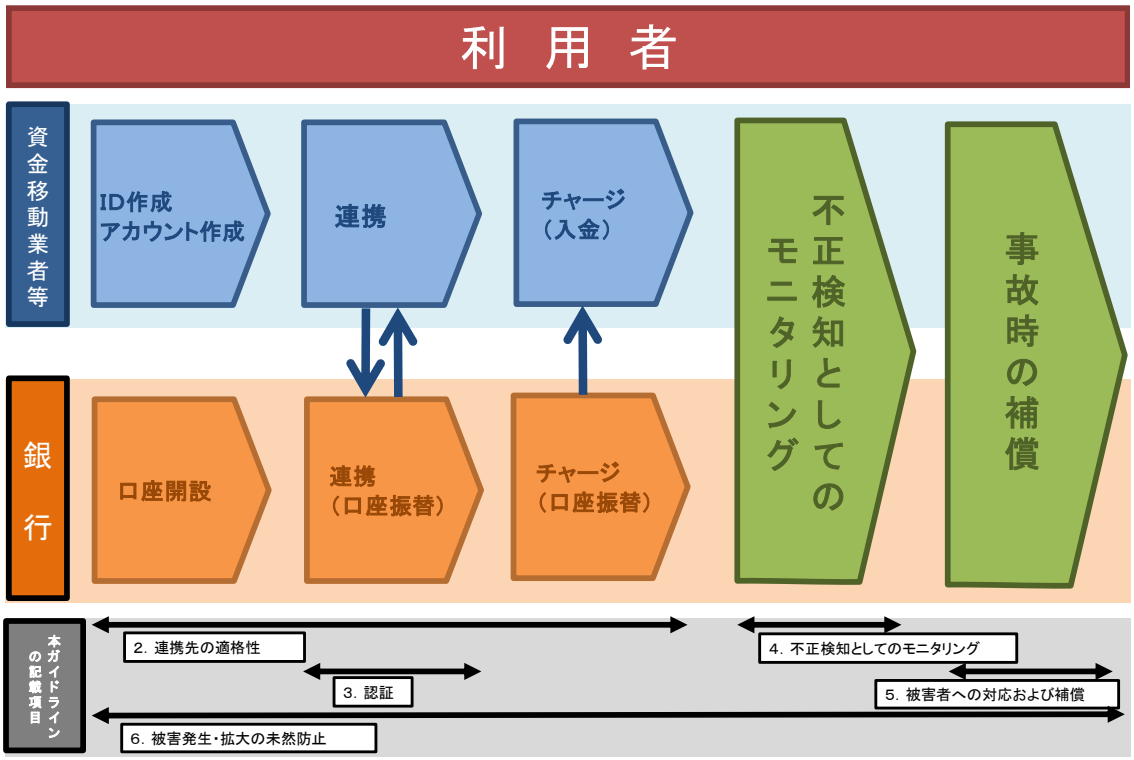
1.2 本ガイドラインの適用範囲

✧ 本ガイドラインでは、今回の不正事案への対策の他、各銀行が資金移動業者等と連携して決済サービスを提供するに際して、銀行側が行う対策を中心に記載している（下表フロー図の銀行側連携、チャージ、モニタリング、補償が本ガイドラインの対象範囲）。なお、資金移動業者等が行う対策については、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

[1] 銀行口座と連携して利用する決済サービスを提供している資金移動業者、前払式支払手段発行者、電子決済等代行業者等のうち、特にスマートフォン等を用いた利便性の高いサービスの提供を行っている事業者。電気料金、ガス料金、電話料金、水道料金、保険料金、NHK（受信料）、国民年金保険料、各種税金など公金の料金収納に係るサービスを提供する者は除く。

[2]を策定している場合があるので、これらも参照されたい。

【図表 1】資金移動業者等の決済サービスにおける全体のフローの例



2．連携先の適格性

2.1 各フェーズにおける確認手法

2.1.1 資金移動業者等との連携前

✧ 銀行・資金移動業者等は、他の事業者と連携することによって生じるリスクを含め、サービス全体のリスクを確認することが必要である。

✧ そのうえで、銀行は、資金移動業者等のアカウント[3]と銀行口座を連携させるための資金移動業者等との口座振替サービスの収納契約等を行うのに先立ち、利用者保護およびセキュリティ等の観点から資金移動業者等の適格性に問題ないかを審査することが必要である。

✧ また、当該収納契約にもとづき、資金移動業者等のユーザーとの口座振替契約（チャージ[4]契約）の締結に際しては（特にオンラインでこれを行う場合）、今回の不正事案等も踏まえ資金移動業者等のアカウントと銀行口座の連携

[2] 例えば、一般社団法人キャッシュレス推進協議会が令和２年９月 18 日に策定・公表した「コード決済における不正な銀行口座紐づけの防止対策に関するガイドライン」が該当。

[3] 利用者が決済サービスを利用することのできる権利であり、決済サービスを利用するにあたり、利用者ごとに作成されるもの。

[4] 口座振替契約にもとづき銀行口座から資金移動業者等のアカウントへ資金を入金することをいう。

時における銀行側の認証手続きに問題がないか、資金移動業者等が行う顧客管理態勢（アカウント開設時の本人確認プロセス、KYC[5]等）に脆弱性がないかを確認することが必要である。

✧ 加えて、連携先との役割分担・責任関係について、相手方と連携して、予め明確化しておくことが重要である。

2.1.2 資金移動業者等との連携後

✧ 連携先の適格性や資金移動業者等の本人確認プロセスについては、連携後も継続的に確認することが必要である。加えて、銀行側または資金移動業者等の資金決済サービスに関する事項について、例えば、認証方法を含むセキュリティや、サービス、ビジネスモデルを変更する場合には原則として予め相手方に連絡を行う体制を整備しておくことが必要である。

✧ 上記確認（事後的に連絡を受けた場合を含む）や自社または他社で発生した不正送金事案を踏まえ、何らかの問題や脆弱性が見出だされた場合には、利用者の資産保全を最優先に、新規連携や資金移動業者等のアカウントへの資金のチャージを一時停止する等の対応を行い、脆弱性を解消してからサービスを再開することが必要である。

2.2 確認すべき項目

2.2.1 利用者保護の観点からの適格性の審査

✧ 利用者保護の観点から連携先の適格性を確認することが必要である。適格性の審査は、画一的・機械的に行うものではなく、各銀行の顧客保護等管理規程や、個別のビジネス、各サービスのリスク、連携先の態様等に応じて、各銀行が独自に必要と判断した事項についても追加的に実施することが望ましい。

2.2.2 セキュリティに関連した適格性の審査

✧ セキュリティの観点から連携先の適格性を確認することが必要である。適格性の審査は、画一的・機械的に行うものではなく、各銀行のセキュリティポリシーや、個別のビジネス、各サービスのリスク、連携先の態様等に応じて、各銀行が独自に必要と判断した事項についても追加的に実施することが望ましい。

2.2.3 資金移動業者等の顧客管理態勢（本人確認プロセス、KYC 等）に脆弱性がないかの確認

✧ 不正利用防止の観点で、資金移動業者等が行っている本人確認プロセスを確

[5] 「Know Your Customer」の略で、顧客の情報や当該顧客が行う取引の内容等を調査し、講ずべき低減措置を判断・実施する一連の流れのことをいう。

認することが必要である。特に、資金移動業者等の利用者がアカウント開設する際の実在性・同一性の確認や、銀行口座と連携する際の犯収法上の取引時確認のプロセス（犯収法施行規則第 13 条の銀行依拠（取引時確認方法の特例）を行っている場合のプロセスや追加確認事項、銀行依拠以外の確認プロセス）の確認を行うことが重要である。

✧ 加えて、資金移動業者等の管理態勢に、マネー・ローンダリングおよびテロ資金供与のリスクがないかの確認を行うことが重要である。

2.3 適格性の審査・顧客管理態勢の確認を踏まえた対応

✧ 上記の適格性の審査・顧客管理態勢の確認の結果、問題や脆弱性が確認された場合には、連携の可否を含め、慎重に検討する必要がある。

３．認証

3.1 認証におけるセキュリティ対策

✧ 犯罪手口は技術の進展と相まって複雑高度化することが想定されるため、各銀行は、採用している認証方法に脆弱性がないかを定期的に見直し、セキュリティ対策の強化・高度化に向けた取組みを継続して行うことが必要である。例えば、平成 28 年に全銀協が公表した「インターネット・バンキングにおける預金等の不正な払戻しについて」の中の「インターネット・バンキングにおけるセキュリティ対策事例」も参考にしながら、実効的な多要素認証の導入が必要である。その他お客さまの動作環境整備等のセキュリティ対策を講じることが望ましい。

3.2 認証手段・方式の考え方

✧ 資金移動業者等のアカウントに銀行口座を連携させる際の手順は、インターネット・バンキングのログインパスワード等に加え、ワンタイムパスワード等の複数の要素による認証手段を組み合わせることによる堅牢な認証手続きとすることが必要である。

✧ これら認証方式の選択に当たっては、銀行において採用されているインターネット・バンキングの振込等の為替取引時に用いられる認証方式の水準が一つの目安となり得る。

✧ また、資金をチャージする際の手順においても、リスクに応じて、認証手続き等の牽制の仕組みを設けることが、セキュリティ対策の強化・高度化の観点からは望ましい。

✧ 銀行において採用されている非対面取引チャネルの認証方式と比較して、強度の劣後する認証方式を採用する場合には（例：インターネット・バンキング契約がなく、ワンタイムパスワードを発行する仕組みを有さない利用者を

対象としてキャッシュカードの暗証番号での確認を許容する場合等)、不正アクセスのリスクが高まることを踏まえた利用者保護上の別途の対策が必要となる。

3.3 その他留意点

✧ 「主要行等／中小・地域金融機関向けの総合的な監督指針」や金融情報システムセンター(FISC)の「金融機関等コンピュータシステムの安全対策基準」、当協会の「インターネット・バンキングにおいて留意すべき事項について」等を参考にすることが考えられる。

４．不正検知としてのモニタリング

✧ 銀行は、資金移動業者等と連携し、一連の資金の流れの中で、定期的な不正検知のためのモニタリング態勢を構築することが必要である。加えて、銀行または資金移動業者等が、不正が疑われる取引を検知した際には相手方に連絡を行う体制を関係法令等を踏まえたうえで整備しておくことが望ましい。

✧ 銀行においてはまずは、資金移動業者等が行っているモニタリング態勢を定期的に確認する必要がある（特にサービスの変更・拡大があった際には慎重な確認が必要)。

✧ 加えて、銀行でも定期的に不正検知のモニタリングを実施し、こうしたモニタリングの見直し・高度化を図ることが望ましい。

✧ 併せて、未然防止においては、預金者が口座振替の契約事実や契約内容を確認できるようにすることが重要である。

✧ なお、モニタリング態勢の確認方法、深度、頻度等については、銀行のセキュリティポリシーや、個別のビジネス、各サービスのリスク、連携先の態様・モニタリング態勢、利用者の属性や取引のリスク等に応じて、個別に判断されるものと考えられる。

✧ 資金移動業者等への態勢確認の結果、不備や不足が確認された場合には、サービスの一時停止等の対策を検討する必要がある。

５．被害者への対応および補償

✧ 利用者保護の観点から、補償を含めた被害者への対応を迅速かつ適切に実施することが必要である。

5.1 連携先との事前の取決め

✧ 銀行は、利用者に対して迅速かつ丁寧な対応を行うとともに、速やかな被害回復、補償等を図る観点から、不正利用等が発生した場合の問い合わせ等を受け付ける窓口や、利用者に損害が生じた場合の補償・返金方法、補償範囲

について、資金移動業者等との間で予め取り決めておくことが必要である。

- ✧ また、銀行は、資金移動業者等が当該取り決め内容を利用者に周知していることを確認することが望ましい。
- ✧ なお、利用者に対して銀行・資金移動業者等の双方とも責任を負わない等の利用者保護に著しく欠ける取決めは、行わないようにする必要がある。
- ✧ また、利用者への補償・返金後の、銀行と資金移動業者等の間の内部分担（求償）についても、別途予め取り決めておくことが必要である。
- ✧ 加えて、利用者からみて対応窓口・主体等がわかりにくくなるおそれがあることから、銀行と資金移動業者等との間で、任意の一時的な補償・返金方法（含む、その主体）等について、予め取り決めておくことが望ましい。
- ✧ 今回の不正事案においては、資金移動業者等が提供する決済サービスを利用していない方の被害も確認されている。こうした決済サービスを利用していない方が被害に遭われたケースにおいては、銀行は主体的に問い合わせや相談に応じることが必要である。

5.2 利用者への対応

- ✧ 銀行・資金移動業者等の双方は、利用者からの問い合わせやご相談を受けた際には、被害の有無によらず、利用者の不安を解消するべく、真摯な姿勢で迅速かつ丁寧に対応し、利用者をたらい回しにするようなことがないようにする必要がある。
- ✧ そのうえで、不適切な顧客対応とならないよう、利用者からの問い合わせやご相談を受け付ける窓口を取り決めておくなど、銀行と資金移動業者等の間で協力することが重要である。加えて、連携先との協力方法・責任関係について、相手方と連携して、予め明確化しておくことが重要である。
- ✧ また、銀行・資金移動業者等は、各々が利用者からの問い合わせやご相談を受けた情報について収集・分析するための体制を構築したうえで、それらについて相手方とも共有するための体制を関係法令等を踏まえたうえで整備しておくことが重要である。

5.3 補償内容・範囲に関する考え方

- ✧ 利用者が個人であって利用者自身の責任によらずに被害に遭われた場合については、上記取決めにもとづいて銀行・資金移動業者等の双方が連携のうえ、補償を迅速かつ適切に行うことが必要である。
- ✧ なお、利用者に過失がある場合については、被害に遭った利用者の態様やその状況等を加味して、全額あるいは一部を利用者負担とすることも含め、預金者保護法および盗難通帳等による預金等の不正な払戻しへの対応に関する全銀協申し合わせ（平成 20 年２月 19 日付「預金等の不正な払戻しへの対応について」）等を参考にしつつ、個別に判断されることが必要である。
- ✧ 法人の利用者については、個人の利用者と比較して、セキュリティ対策等へ

の対応力が相対的に高いと考えられる。利用者の利用環境やセキュリティレベルを原因として不正利用される可能性がある中では、サービス提供者側のセキュリティ対策に加え、利用者においてもセキュリティ対策を講じ、不正利用被害の防止に努めていくことが重要であると考えられる。こうした点を踏まえ、法人の利用者に対する補償については、利用者が行っていたセキュリティ対策や不正利用被害の防止に関する状況、法人の属性やセキュリティ対策への対応力の点を考慮して、個別に判断されることが必要である。

６．被害発生・拡大の未然防止

✧ 不正利用による被害を防止するため、次のような措置により対策を講じる。

6.1 利用者への注意喚起

✧ 不正事案の未然防止のため、銀行・資金移動業者等は連携して、利用者に対してキャッシュカードおよび暗証番号、あるいはログイン ID およびパスワードを適切に管理し、取り扱うよう、継続的に注意喚起を行うことが重要である。

✧ また、利用者が実際に被害に遭った場合は、銀行または資金移動業者等への速やかな連絡や、捜査機関への被害事実等の事情説明を求めるとともに、調査への協力を求めることが望ましい。

✧ 不正事案が発生した場合には、悪意のある第三者が、利用者の口座情報や本人確認情報を不正に入手している可能性も想定されることから、銀行のウェブサイト等を通じて注意喚起を行うことが望ましい。

6.2 初動対応

✧ 銀行または連携先において不正アクセス等が判明した場合、被害発生・拡大を未然に防止する観点から、速やかに、銀行においては新規連携や資金移動業者等のアカウントへの資金のチャージを一時停止する等の対応を、連携先においてはサービス利用の制限、停止を行うこと等、お客さまの資産の保全を最優先に対応を検討する必要がある。

✧ 銀行と連携先双方において速やかに機能制限、停止、その他必要な措置を行う観点から、銀行口座と連携して利用する決済サービスに関連した不正アクセス、情報流出・漏洩が判明した場合にはただちに他方に連絡することとし、その場合の連絡先や連絡方法等を銀行と連携先間において取り決めておく等、被害拡大防止に向けた必要な態勢を整備しておくことが必要である。

✧ 資金移動業者等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、資金移動業者等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。

✧ 利用者の不安や混乱を回避するため、銀行・資金移動業者等は適時、適切な情報発信、対外公表を行うよう努める。

6.3 被害を最小限にとどめる措置

✧ 万一不正利用が発生した際の被害を最小限にとどめる措置を講じることが必要である。

以　上