



OpenID ファウンデーション・ジャパン
決済ワーキング・グループ

資金移動業に関するあり方 ガイドライン

2010年3月10日

I	はじめに	2
I-1	ガイドライン策定の背景	2
I-2	ガイドライン策定の目的	2
I-3	ガイドラインの位置付け	2
II	想定する基本モデル	3
II-1	基本モデルの位置付け	3
II-2	基本モデルの流れ	3
II-3	基本モデルにおける各行為の内容、及び関連事項	3
III	当人・身元確認	6
III-1	当人確認および身元確認の関連するシーン	6
III-2	当人確認および身元確認の定義	6
III-3	利用シーンおよび送金金額別に見た当人確認・身元確認の必要性	6
III-4	当人確認および身元確認における保証レベルの考え方	8
III-5	推奨する保証レベル	11
IV	送受信情報	12
IV-1	送受信情報	12
IV-2	推奨する送受信情報	13
V	情報安全管理	14
V-1	管理体制の整備	14
V-2	安全対策	15
V-3	データ保護・保全	15
V-4	システム監査	16
V-5	コンティンジェンシープランの策定	16
V-6	障害・災害対策	16
VI	業務委託	17
VI-1	資金移動業務の委託の適正性の担保	17
VI-2	各管理責任者による外部委託の管理体制の整備・確立	17
VI-3	外部委託業務のリスク管理	18
VII	おわりに	19
<付録 1>	用語の定義	20
<付録 2>	参考文献	22
<付録 3>	参加企業一覧	22

I はじめに

インターネットにおけるユーザー認証技術のひとつである「OpenID」の国内普及・国際化を支援している、一般社団法人 OpenID ファウンデーション・ジャパン (所在地: 東京都港区、代表理事: 八木晃二、以降「OIDF-J」) は、OIDF-J 会員企業とともに「決済ワーキング・グループ (以降「決済 WG」)」を立ち上げ、資金移動業に関するガイドライン (以降「本ガイドライン」) の策定を行った。そこで、本ガイドラインについて、背景と目的、および位置付けを明示する。

I-1 ガイドライン策定の背景

2009年6月24日に「資金決済に関する法律」が公布、同年12月7日に政令・内閣府令案、同年12月14日に金融庁の事務ガイドライン案が公表され、法律の施行以降、様々な業種・企業の参入による資金送金・決済に関する新サービスの誕生が予想される。新規参入企業は、既存の仕組みを活用することで参入コストを抑えることができるが、消費者に対し安全で利便性の高い決済サービスを提供することが求められる。

I-2 ガイドライン策定の目的

上記の背景から、決済 WG では、企業が資金決済 (資金移動) の事業を運営する上で、準拠するのが望ましい内容を明記する目的で、本ガイドラインを策定した。

具体的には、新たな決済サービスに関する要点を抽出・整理し、資金決済に対応する基本モデル (資金移動モデル) を想定した上で、重視すべき「当人・身元確認」「情報安全管理」「送受信情報」およびそれに伴う「委託業務」部分を中心としたものである。従って、本ガイドラインで取扱わない内容は、その他のガイドライン等に委ねるものとする。

なお、今後は、本ガイドラインに加えて、これらを OpenID に適用し、OpenID を活用した簡単かつ安心・安全な決済サービスのユースケースを示す「OpenID 適用ガイドライン」を別途策定する。

I-3 ガイドラインの位置付け

本ガイドラインは、上記の「資金決済に関する法律」(資金移動)、政令・内閣府令 (資金移動)、および金融庁の事務ガイドライン (資金移動業者関係) を受けて、新たに資金移動業を行うことを検討する各種事業者が構成する民間団体 (OIDF-J) が策定した。

また、本ガイドラインは、各種基準やガイドラインを参照した上で、以降で想定する基本モデルおよびそれから類推できるモデルを対象として策定されたものである。従って、資金決済 (資金移動) に該当しない行為、例えば企業ポイントの交換等については、本ガイドラインの対象外とする。なお、本ガイドラインの行為の対象は、OIDF-J 会員企業のみならず、民間事業者が資金移動業を行うことを想定している。

II 想定する基本モデル

II-1 基本モデルの位置付け

「資金決済に関する法律」の施行後は、資金移動業の新たなモデルが創出されていくものと想定されるが、現時点においてこれら全てのモデルを網羅することは現実的ではない。従って、現時点では比較的基本的なモデルと想定されるものを本ガイドラインの基本モデルとして定め、その実施に関するあり方を以下に記述する。なお、新たなモデルが創出された場合には、必要に応じて追加の検討を行う。

II-2 基本モデルの流れ

基本モデルでは、送金人（「甲」とする）が送金原資を資金移動業者 A が管理する口座（一般的な銀行口座と区別するために、以降「チャンネル」とする。また、送金人のチャンネルを便宜上「α」とする）に一時的に預け入れた後、資金移動業者 B が管理する、受取人用のチャンネル（「β」とする）から受取人（「乙」とする）が原資を受け取るまでを主な行為に分けて記述する。

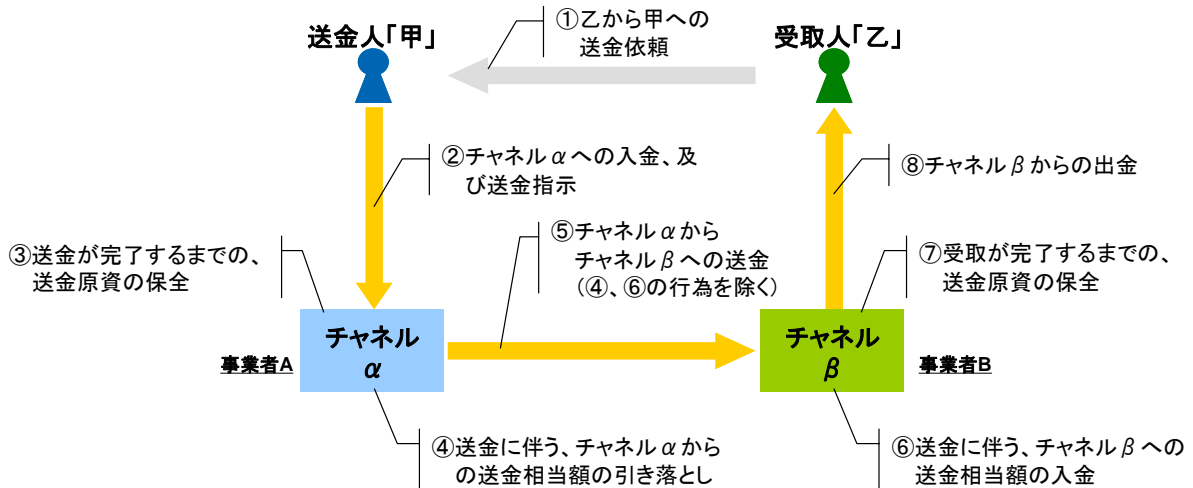
II-3 基本モデルにおける各行為の内容、及び関連事項

本ガイドラインでは、基本モデルを構成する主な行為として、以下①～⑧を定義する。

- ①乙から甲への送金依頼
- ②甲によるチャンネル α への入金、及び送金指示
- ③送金が完了するまでの、資金移動業者 A による送金原資の保全
- ④送金に伴う、資金移動業者 A によるチャンネル α からの送金相当額の引き落とし
- ⑤資金移動業者 A によるチャンネル α からチャンネル β への送金
- ⑥送金に伴う、資金移動業者 B によるチャンネル β への送金相当額の入金
- ⑦受取が完了するまでの、資金移動業者 B による送金原資の保全
- ⑧乙によるチャンネル β からの出金

これらを簡単なモデル図に示したものが、図表 II-1 の資金移動業者の基本モデルである。なお、①は資金移動には直接あたらない行為であるが、行為としては存在するため、明記しておく。

図表 II-1：資金移動業の基本モデル



なお、この基本モデルでは、資金移動業者 A と資金移動業者 B が同一の事業者である場合でも、同様の行為が発生すると想定される。また、資金移動業者の業務委託は、銀行代理業者のような許可制になっておらず、行為が発生する以上、全てにおいて業務委託が発生する可能性があり、主体者が変わることも想定されるため、各行為の主体者は明記していない。

送金人「甲」や受取人「乙」に該当する者としては、それぞれ個人、法人が共に挙げられる。また、①～⑧の各行為を資金移動業者に代わって実施する事業者（外部委託先）としては、現時点では以下が想定される。但し、資金移動業者 A と資金移動業者 B との間には、業務委託関係が存在していないものとしている。

図表 II-2：各行為に関して想定される主な代行事業者

行為番号	想定される主な代行事業者（例）
①	通信事業者
②	収納代行事業者、代金引換事業者
③	金融機関（銀行、信託銀行）
④	システムアウトソーサー
⑤	ネットワーク事業者
⑥	システムアウトソーサー
⑦	金融機関（銀行、信託銀行）
⑧	金融機関、現金の授受が可能な店舗を有する事業者

そのほか、資金移動業者が行う資金移動の一部として、行為全体で、以下の行為のみを、資金移動者自らを行うことなく、第三者に委託することも考えられる。

- ⑨ 契約の勧誘を目的とした商品説明
- ⑩ 契約の締結に向けた条件交渉
- ⑪ 契約締結申込の受領
- ⑫ 契約の締結の承諾

なお、上記にはあたらない行為として、⑬広告掲載等による勧誘、⑭商品案内チラシやパンフレットの配布および説明、⑮契約申込書の配布・回収等、これらのみを第三者に委託する場合がある。この場合、資金移動業者が資金移動を行うまでの間に自らの責任のもと、契約締結のための説明等を行う必要がある。

III 当人・身元確認

III-1 当人確認および身元確認の関連するシーン

前述の資金移動業の基本モデルにおいて、そのサービスを実施する上では、「当人確認」や「身元確認」（両者の定義は次節参照）を実施しなければならないシーン、および実施することが望ましいシーンが存在する。

基本モデルを構成する①～⑧の行為において、特に②③④、⑥⑦⑧の行為を行うためには、以下のような初期の登録が発生する。

<②③④の行為を行い、甲がチャンネルαに入金して乙に送金するため>

②'甲が資金移動業者Aに何かしらの登録をする。(チャンネルαでない場合も含む)

③'甲がチャンネルαの登録をする。

<⑥⑦⑧の行為を行い、乙が甲から受金してチャンネルβから出金するため>

⑦'乙が資金移動業者Bに何かしらの登録をする。(チャンネルβでない場合も含む)

⑧'乙がチャンネルβの登録をする。

III-2 当人確認および身元確認の定義

当人確認とは、当事者が身元識別情報の指し示す主体であるかどうか（当人性）を確認するプロセスである。より高い保証レベルを得るためには、より多くの攻撃に対応する必要がある。

身元確認とは、その身元識別情報が実在する主体であること、および身元識別情報に結びつけられた属性（例：氏名）が正しいことを確認するプロセスである。より高い保証レベルを得るためには、より多くの検証を要する。この身元確認の際の確認項目には、以下のようなものがある。

- 存在性：その身元識別情報が存在すること
- 生存性：その身元識別情報が生存していること
- 当人性：当事者がその身元識別情報の指し示す主体であること
- 唯一性：当事者がその身元識別情報を主張する唯一の主体であること
- 利用性：当事者がその身元識別情報を利用していること

III-3 利用シーンおよび送金金額別に見た当人確認・身元確認の必要性

②～⑤（②'③'含む）では、甲に関する当人確認や身元確認が必要であり、⑥～⑧（⑦'⑧'含む）では、乙に関する当人確認や身元確認が必要である。

但し、全ての資金移動において当人確認および身元確認を行う必要があるわけではない。「犯罪による収益の移転防止に関する法律の施行令」によると、「現金の受払いをする取

引で為替取引」で10万円を超える場合には「本人確認」（身元確認）を行わなければならない、とある。すなわち、送金金額が10万円を超える場合には、資金移動を行う事業者は利用者の身元確認を行う必要がある。一方、送金金額が10万円以下の場合には、資金移動を行う事業者は身元確認を求められているわけではない。なお、本ガイドラインでは、「資金決済に関する法律」の政令・内閣府令（資金移動）で規定されている送金金額100万円以下に限定した場合の、資金移動業における当人確認や身元確認を対象とする。そのため、送金金額100万円超の場合については、本ガイドラインの対象外とする。

以上を踏まえて、送金金額別に資金移動業者による当人確認および身元確認の必要性を整理すると、以下のようになる。

【②～⑤（②'③'含む）のプロセス：甲に対する当人確認・身元確認】

＜⑤における送金金額が10万円以下の場合＞

- 当人確認：
 - ◇ 資金移動業者Aは、⑤の送金において、甲に対する当人確認を行う必要がある。（②の入金において、甲に対する当人確認を行うかどうかは、資金移動業者Aが判断すればよい。）
- 身元確認：
 - ◇ 資金移動業者Aは、本プロセスのいずれでも甲に対する身元確認を行うかどうかを判断すればよい。

＜⑤における送金金額が10万円超～100万円以下の場合＞

- 当人確認：
 - ◇ 資金移動業者Aは、⑤の送金において、甲に対する当人確認を行う必要がある。（②の入金において、甲に対する当人確認を行うかどうかは、資金移動業者Aが判断すればよい。）
- 身元確認：
 - ◇ 資金移動業者Aは、10万円超の送金サービスを初めて甲に提供するまで（本プロセス）の間に、甲に対する身元確認を少なくとも1度以上行う必要がある。

【⑥～⑧（⑦'⑧'含む）のプロセス：乙に対する当人確認・身元確認】

＜送金金額に関わらず＞

- 当人確認：
 - ◇ 資金移動業者Bは、⑧の出金において、乙に対する当人確認を行う必要がある。

- 身元確認：

- ◇ 資金移動業者Bは、本プロセスのいずれかにおいて乙に対する身元確認を行うかどうかを判断すればよい。

資金移動業者は、「犯罪による収益の移転防止に関する法律」、「犯罪による収益の移転防止に関する法律施行令」、「犯罪による収益の移転防止に関する法律施行規則」および「犯罪による収益の移転防止に関する法律施行規則の一部を改正する命令案」（以降「マネロン防止法・令・規則」）で規定されている「特定事業者」に該当する。そのため、資金移動業者の提供するサービスが、「マネロン防止法・令・規則」で記載されている「継続的に又は反復して行う」契約に基づく場合、資金移動業者は「マネロン防止法・令・規則」における「本人確認」に準拠するように、身元確認を行うかどうかを判断すればよい。

なお、資金移動業者は、毎回の資金移動に関する情報・データ（送金先、送金金額、送金頻度、本人確認・身元確認の有無など）をモニタリングできるようにしておくことが望ましい。

III-4 本人確認および身元確認における保証レベルの考え方

資金移動業者は、自らの提供するサービスの社会的な影響や脅威の程度に応じて、適切な「保証レベル」を確保するよう、サービスの本人確認および身元確認のレベルを決定する必要がある。本ガイドラインにおける「保証レベル」とは、本人確認や身元確認において、消費者や事業者に与える影響の度合いを表す抽象的な指標である。本人確認や身元確認には脅威が存在しており、どの程度の脅威に対応できているか、によってレベルを定義している。保証レベル毎に、本人確認および身元確認を行う際に要求されている事項について、図表III-1に整理する。但し、本人確認と身元確認の保証レベルは互いに独立に勘案されるべきであり、利用に当たっては同一レベルになるように揃える必要は無い。

なお、本ガイドラインにおける保証レベルの区分けの考え方は、NIST SP800-63 rev1を参照している。

図表Ⅲ-1：保証レベル毎の要求事項（当人確認、身元確認）

保証レベル	レベルの定義	要求事項	
		当人確認	身元確認
レベル1 （基本的な保証）	消費者や事業者にあまり影響を与えない脅威にだけ対応している。 （例：感覚的に「かゆい」レベルの脅威へ対応）	確認対象の秘密情報（パスワード等）を有効期間内で推測できる確率が $1/2^{10}$ 以下であること。（※1） （例：6文字以上の無作為パスワード、1分間に3回まで入力可能、有効期限10年以内） かつ、注釈のa～eができないようになっていること。	身元確認の要求事項は特にない。 （自己申告レベルで登録された電子メールアドレスの確認程度）
レベル2 （中程度の保証）	消費者や事業者にある程度影響を与える脅威に対応している。 （例：感覚的に「痛い」レベルの脅威へ対応）	有効期間内で推測できる確率が $1/2^{14}$ 以下であること。 （※1） （例：一部のPINなしOTPトークン、およびPINなし秘密鍵） かつ、注釈のa～kができないようになっていること。	金融機関等第三者のデータベースを照会して取得したデータをもとにした確認（例：口座番号、またはクレジットカード番号を元に金融機関等に照会を行い、氏名、生年月日、住所を確認（住所は特に郵送等で確認）する。）
レベル3 （高いレベルの保証）	消費者や事業者にかなり影響を与える脅威に対応している。 （例：感覚的に「大怪我な」レベルの脅威へ対応）	複数種類の認証要素を用いること。 （例：PINありOTPトークン、PINあり秘密鍵、住基カード（ICチップ）+専用リーダー） かつ、注釈のa～oができないようになっていること。	公的な身分証明書（写真付、もしくは2種類）を元に、氏名、生年月日、住所を確認（住所は特に郵送等で確認）する。

レベル4 (最高レベルの保証)	消費者や事業者に回復不能な程の大きい影響を与える脅威に対応している。 (例: 感覚的に「回復不能な」レベルの脅威へ対応)	複数の認証要素を用いること。またその1つとして、秘密情報を取り出すことが不可能なハードウェア本人証明機を用いること。 (例: レベル3の2種類の組み合わせ、生体認証) かつ、注釈のa～pができないようになっていること。	対面で、公的身分証明書(写真付)を元に、訓練された検査人によって、本人を確認する。
--------------------	---	---	---

(※1) 推定確率の算出方法は NIST SP800-63 rev1 の Appendix A: Estimating Entropy and Strength を参照。OTP トークンの場合、パスワードの有効期限が短いため、推定確率は非常に低くなる。

<注釈> 上記図表の本人確認の要求事項内に記載している a～p は、それぞれ以下を指す。

- | | |
|---------------------|---------------------|
| a : オンライン上の推測 | b : リプレイ |
| c : 偽アサーション生成 | d : 偽アサーション・ポインタ生成 |
| e : アサーション再利用 | f : 盗聴 |
| g : セッション・ハイジャック | h : アサーション内容の開示 |
| i : アサーション・リダイレクト | j : アサーション/同ポインタの奪取 |
| k : アサーション・ポインタの入替え | l : フィッシング |
| m : ファーミング | n : アサーションの無効主張 |
| o : 一部の中間者攻撃 | p : 全ての中間者攻撃 |

(上記の「用語の定義」については、後述の<付録1>を参照のこと。)

本人確認では、「本人証明証(トークン)の保証レベル」、「本人確認のプロセス全体の保証レベル」、「本人証明証の管理における保証レベル」という3つの保証レベルが存在し、その中で最も低いレベルが本人確認の保証レベルとして採用される。3つの保証レベルは、それぞれのプロセスに対する脅威への対応度合いによって定義されており、それぞれの保証レベルの要求事項は、NIST SP800-63 rev1に準拠している。そのうち、前者2つは上記図表に簡潔に包含し、それぞれの保証レベルに明記している。(上記図表では、「本人証明証の管理における保証レベル」については割愛している。)

なお、JSA(日本規格協会)のアイデンティティ管理技術の標準化調査研究委員会において、Kantara Initiativeが作成しているIAF(Identity Assurance Framework)と、ISO(国際標準化機構)/ITU-T(国際電気通信連合 電気通信標準化部門)共同委員会が作成しているEAA(Entity Authentication Assurance)を参照し、JIS(日本工業規格)の電子認証ガイドラインを策定しようと検討が進められている。従って、上記の保証レベルは、

適宜これらの策定結果を踏まえ、更新していく必要がある。

また、身元確認は、「マネロン防止法・令・規則」で規定されている、「現金の受払いをする取引で為替取引」で10万円を超える場合に実施しなければならない「本人確認」に準拠するように実施すればよい。

III-5 推奨する保証レベル

以上より、資金移動業の基本モデルにおいて、実施するサービスに関連する当人確認および身元確認について整理すると、以下のようになる。

10万円以下の送金を行う際には、資金移動業者Aは送金人（甲）に関する適切なレベル（例：レベル2）の当人確認を行うことが望ましい。（前述のように、身元確認を行うかどうかは、資金移動業者Aが判断すればよい。）

10万円超～100万円以下の送金を行う際には、資金移動業者Aは送金人（甲）に関する適切なレベル（例：レベル2）の当人確認と、マネロン防止法・令・規則に準拠した身元確認を行うことが望ましい。

金額によらず、送金を受ける際には、資金移動業者Bは受取人（乙）に関する適切なレベル（例：レベル2）の当人確認を行うことが望ましい。（前述のように、身元確認を行うかどうかは、資金移動業者Bが判断すればよい。）

IV 送受信情報

IV-1 送受信情報

資金移動業において、実施するサービスに関連する情報・データが、送金人、資金移動業者、受取人の間で流通する。その情報・データが流通するシーンを、前述の基本モデルの中で整理すると以下のように考えられる。

- 1) 甲から資金移動業者A、および資金移動業者Aから甲
- 2) 資金移動業者Aから資金移動業者B、および資金移動業者Bから資金移動業者A
- 3) 資金移動業者Bから乙、および乙から資金移動業者B
- 4) 資金移動業者Bから資金移動業者A、および資金移動業者Aから甲

それぞれのシーンの流通する情報について、以下に例を示す。

(1)甲から資金移動業者Aへ流通する主な情報

- 送金元情報
- 送金先情報
- 送金金額情報（円）
- 送金日時情報（指定日時）
- 甲の当人確認情報
- 甲の身元確認情報（必要時）

(2)資金移動業者Aから甲へ流通する主な情報

- 送金依頼の確認情報

(3)資金移動業者Aから資金移動業者Bへ流通する主な情報

- 送金元情報
- 送金先情報
- 送金金額情報（円）
- 送金日時情報（指定日時）
- 甲の当人確認レベル
- 甲の身元確認レベル（必要時）
- 乙に要求する当人確認レベル
- 乙に要求する身元確認レベル（必要時）

(4)資金移動業者Bから資金移動業者Aへ流通する主な情報

- 資金移動業者Bの送金受領の確認情報

(5)資金移動業者Bから乙へ流通する主な情報

- 送金元情報
- 送金金額（円）
- 送金日時（完了日時）
- 乙に要求する当人確認レベル
- 乙に要求する身元確認レベル（必要時）

(6)乙から資金移動業者Bへ流通する主な情報（出金時）

- 乙の当人確認情報
- 乙の身元確認情報（必要時）

(7)資金移動業者Bから資金移動業者Aへ流通する主な情報（出金後）

- 乙の送金受領の確認情報

(8)資金移動業者Aから甲へ流通する主な情報（出金後）

- 乙の送金受領の確認情報

IV-2 推奨する送受信情報

資金移動業者Aが送金を行う際には、送金に伴う適切な情報（少なくとも送金元と送金先、送金金額（円）、送金日時）を紐付けて送金することが望ましい。

また、資金移動業者Aと資金移動業者Bが相互運用性を確保したい場合は、送金に伴う適切な情報として、当人確認レベルと身元確認レベルも紐付けて送金することが望ましい。

V 情報安全管理

V-1 管理体制の整備

資金移動業者（A および B）は、資金移動業の各業務における情報安全管理を適切に行うため、情報安全管理体制を整備することが望まれる。具体的には、以下の取組みが挙げられる。

(1)情報安全管理における責任の明確化

- 情報安全管理の責任者等を定め、その職務範囲と権限および責任について定めること。

(2)セキュリティポリシー等の策定

- セキュリティポリシーや情報安全管理の具体的手順、責任等を明確にした文書を策定すること。

(3)遵守状況の確認

- セキュリティポリシー等に定められた事項の遵守状況を確認し、全役職員のセキュリティポリシー等に対する意識やセキュリティレベルの向上を図ること。

(4)セキュリティポリシー等の改定

- 情報安全管理の方法を最適なものとするため、作成されたセキュリティポリシー等については、業務の実態にあっているかを定期的に評価し、必要に応じて改訂すること。

(5)移動資金移動管理に関わる管理体制の整備

<移動資金管理の管理部門による管理体制>

- 移動資金管理の管理部門の管理者は、移動資金管理の状況を的確に把握し、適正な移動資金管理を行うための方策を講じる社内体制を整備していることが望ましい。

<移動資金管理の管理部門の役割>

- 移動資金管理の管理部門は、経営が定めた移動資金管理に関わる管理方針に則り、移動資金の管理に関わる内部規程を制定していることが望ましい。また、必要に応じて内部規程・業務細則を改廃する等の措置を社内で講じていることが望ましい。

(6)顧客情報の管理体制の整備

- 個人顧客の顧客情報に関しては、個人情報保護法に基づく措置（顧客情報管理のための組織の整備等）が社内で講じられている必要がある。
- また、第三者との間で顧客情報を共有する場合、共有に関わる同意を、原則として書面による等の方法により、事前かつ適切に当該個人より取得する体制となっていることが望ましい。

V-2 安全対策

資金移動業者（A および B）は、資金移動業の各業務に対して、安全対策を行うことが望まれる。具体的には、以下の取組みが挙げられる。

(1)安全対策の基本方針等の策定

- 安全対策の基本方針、基準及び手順を策定すること。

(2)安全対策の管理体制の確立

- システム、データ、コンピュータネットワークの安全かつ円滑な運用と不正防止のため、管理体制を整備すること。

(3)資金移動取引の安全対策

- 不正、不当な資金移動取引を防止するため、資金移動取引業務に従事する担当者の権限の範囲を明確にすること。
- 複数の事業者が関わる資金移動取引においては、各業務における責任範囲を明確にすること。

V-3 データ保護・保全

資金移動業者（A および B）は、顧客データ等の重要なデータを保護するために、以下の取組みを行うことが望ましい。

(1)データ漏洩防止

- 蓄積データや転送データに対して、漏洩防止策を設けること。

(2)不正プログラム防止

- コンピュータウイルスやフィッシング等の不正プログラムによる被害を防ぐため、防御対策を講ずること。

(3)データ不正使用防止

- 不正アクセス等からデータを保護するため、プログラムとファイル間のアクセス権限チェック機能等を設けること。

(4)検知策

- 重要なデータに対しては、改ざん検知のための対策を講じておくこと。

(5)トレーサビリティの確保

- 取引データについては、処理の顛末を記録すること。
- 適切な保存期間を設けること。

V-4 システム監査

資金移動業者（A および B）は、資金移動業におけるコンピュータシステムおよびその管理について、有効性、効率性、信頼性、遵守性、および安全性の面から把握、評価するため、システム監査体制を整備することが望ましい。

V-5 コンティンジェンシープランの策定

資金移動業者（A および B）は、不慮の災害や事故、あるいは障害等により重大な損害を被り、業務の遂行が困難になった場合の損害の範囲と業務への影響を極小化し、早期復旧をはかるために、あらかじめコンティンジェンシープランを策定することが望ましい。

コンティンジェンシープランには、資金移動取引における送金データ等のトレーサビリティの確保やバックアップ等の対策を含むことが望ましい。

V-6 障害・災害対策

資金移動業者（A および B）は、障害時・災害時の対応策として、以下の取組みを行うことが望ましい。

- 障害または災害等によりコンピュータシステムが正常に稼働しなくなった場合の連絡手順や復旧手順を明確にすること。なお、当該手順については、コンティンジェンシープランと整合性のとれた内容にすること。
- すばやく復旧するため、障害の原因を調査する手法を講じておくこと。また、障害の発生原因を記録し、傾向分析等を通じて再発防止に役立てること。

VI 業務委託

本ガイドラインでは、チャンネルの開設や残高管理は、資金移動業者が自ら行う行為であるとみなし、それ以外の行為（Ⅱ章にて定めた行為では④と⑥、および⑬～⑮以外が該当）を委託するケースを想定する。

VI-1 資金移動業務の委託の適正性の担保

(1) 資金移動業務の委託

資金移動に関わる業務の一部の委託に関しては、その委託及び委託先について資金委託契約において定めていることが望ましい。なお、その選定においては、業務委託先が、委託元に対し管理状況に関する十分な情報を提供する体制となっていることを確認しておくことが望ましい。また、業務委託契約の内容は、善管注意義務を適切に履行する観点から十分なものとなっているべきである。例えば、業務委託先を不当に免責する等、利用者を害するおそれのある規定が定められていてはならない。

(2) 業務委託先の管理体制

業務委託先に対する指図書類と委託内容に齟齬はないかを、定期的に確認する体制を取っていることが望ましい。また、業務委託先で発生した業務執行上の問題点について、業務委託先に対して速やかに是正を求めるとともに、是正状況の報告を求める体制となっていることが望ましい。

VI-2 各管理責任者による外部委託の管理体制の整備・確立

(1) 内部規定等の策定

外部委託管理責任者は、外部委託に関し、その管理の方法等を定めた内部規程（以降「外部委託規程」）を策定していることが望ましい。なお、外部委託規程は、リーガル・チェック等を受け、経営の承認を受けた上で、組織内に周知されていることが望ましい。

外部委託規程の内容は、業務の規模・特性に応じ、外部委託管理の適切性の確保についての管理に必要な取決めを網羅し、管理を行うための組織体制、権限及び役割、方法等を明確に定める等、適切に規定されていることが望ましい。

(2) 外部委託管理の実施

外部委託管理責任者は、業務を第三者に委託する場合、当該業務の規模・特性に応じ、その的確な遂行を確保するための措置（委託契約等において外部委託先に対して体制整備を求めることを含む）を講じていることが望ましい。

具体的には、例えば以下が挙げられる。

- 外部委託業務を的確、公正かつ効率的に遂行することができる能力を有する者に委託するように外部委託先を選定すること。

- 委託契約の内容について、適切な措置を講じることができる内容となっているか確認する体制を整備すること。
- 外部委託先に対する必要かつ適切なモニタリング等を行うための措置を講じていること。
- 外部委託先が行う外部委託業務に関わる顧客からの相談・苦情等を適切かつ迅速に処理するために必要な措置を講じていること。
- 顧客の保護を図る観点から当該外部委託業務に支障が生じることを防止するための措置を講じていること。
- 外部委託業務に関わる顧客の保護を図るため必要がある場合には、速やかに当該外部委託業務の委託契約の変更、または解除等の必要な措置を講ずるための事前の方策を講じていること。
- 外部委託先における顧客情報管理のための措置を講じていること。

(3)評価・改善活動

外部委託管理責任者は、定期的にもたは必要に応じて随時、外部委託規程の遵守状況等外部委託管理の状況に関する報告・調査結果、モニタリングの結果等を踏まえ、外部委託管理体制の実効性を検証し、適時に外部委託管理規程の内容等の見直しを行う事が望ましい。

VI-3 外部委託業務のリスク管理

当該事業の実施に必要となるシステムに関し、外部委託している場合、そのシステムリスクを認識・評価し、必要なセキュリティ対策が講じられるよう適切に外部委託先の管理状況をモニタリングし、監督していることが望ましい。

また、オペレーショナル・リスクの総合的な管理部門は、当該外部委託業務に内在するオペレーショナル・リスクを特定し、委託契約において、提供されるサービス水準、外部委託先との責任分担（例えば、委託契約に沿ってサービスが提供されない場合における外部委託先の責務、または委託に関連して発生するおそれのある損害の負担の関係）について定めていることを確認するための措置を講じるほか、定期的にモニタリングを行い、問題点等を発見した場合には、速やかに是正する措置を講じていることが望ましい。

VII おわりに

本ガイドラインは、今後の資金移動業を取り巻く環境の変化や関連ビジネスの発展、新たに発生する課題を踏まえ、必要に応じて適時適切に見直しを行うものとする。

また、今後は、民間事業者による資金移動業への新たな参入や、資金移動業者同士の提携が広がっていくものと想定される。そこで、OIDF-Jは、OIDF-J会員企業のみならず、その参入や提携を行おうとする企業の支援を行えるよう、継続的にビジネスを観察し、適宜提言を行っていく。

<付録 1> 用語の定義

用語	内容
オンライン上の推測 (a)	正当なサービス利用者以外の第三者が、サービスを利用するため、認証に必要な情報（パスワード等）の値を推測して、サービス利用のためにログオンを繰り返し試行すること。
検証者	サービス提供者の提供サービスを利用するために必要となる、検証結果表明書（アサーション）を発行する主体のこと。アサーションを発行するために、サービス利用者の身元識別情報を検証する等とする。（例：OpenIDプロバイダー）
アサーション	検証結果表明書のこと。検証者が作成するもので、「サービス利用者はいくらの人だと思います」等の検証結果を表明するもの。表明する対象の属性には、氏名、住所、星座、支払い能力等、自由な項目を持たせることができる。
リプレイ (b)	正当なサービス利用者以外の第三者が盗聴等で入手した、正当なサービス利用者と検証者の間のメッセージ（ID、パスワード等）を、検証者に対して送付することで、正当なサービス利用者になりすまそうとすること。
偽アサーション生成 (c)	正当なサービス利用者以外の第三者が、サービス提供者（例：OpenIDを利用する事業者）が信用してしまうようなアサーションを独自に生成すること。
アサーション・ポインタ	アサーションを一意に特定する情報のこと。検証者からアサーションがサービス提供者に送られる際、アサーション・ポインタは、サイズが大きくなる可能性のあるアサーションの代わりに、ブラウザ経由で送られるもので、サービス提供者は送られた情報を元に検証者からアサーションを取得する仕組みをとる。
偽アサーション・ポインタ生成 (d)	正当なサービス利用者以外の第三者が、アサーション・ポインタを生成して、同じアサーション・ポインタを持っている正当なサービス利用者として、サービスを利用すること。
アサーション再利用 (e)	正当なサービス利用者以外の第三者が、盗聴等で取得したアサーションをもう一度サービス提供者に提示してサービスを利用すること。
盗聴 (f)	正当なサービス利用者以外の第三者が、認証プロトコルを盗み取り、ユーザーになりすまして、サービスを利用することができる情報を取得すること。

セッション・ハイジャック (g)	サービス提供者に対して検証者になりすます、もしくは検証者に対してサービス提供者になりすますこと。また、サービス利用者と提供者のセッションを示す「認証クッキー」を偽装するような、なりすまし攻撃を示す場合もある。
アサーション内容の開示 (h)	アサーションの内容が、正当なサービス利用者やサービス提供者以外に対して開示されること。アサーションには、加入者についての情報を含んでおり、開示されることによって多種多様な脅威に晒される可能性がある。
アサーション・リダイレクト (i)	正当なサービス利用者以外の第三者が、あるサービス提供者に対して発行された正当なサービス利用者に関するアサーションを、別のサービス提供者に転送して、そのサービスを利用すること。但し、あるサービス提供者の正当なサービス利用者は、別のサービス提供者の正当なサービス利用者であることが前提となる。
アサーション/アサーション・ポイントの奪取 (j)	正当なサービス利用者以外の第三者が、アサーションもしくはアサーション・ポイントを中間者攻撃等により奪取し、それを自分のものとして活用することでサービスを利用すること。
アサーション・ポイントの入替 (k)	当該サービスの利用者が、アサーション・ポイントを書き換えること等によって自分より高い権限を持つ人間のアサーションを取得し、より高いアクセス権限を取得すること。
フィッシング (l)	正当なサービス利用者が、偽の検証者と相互通信するように誘い出され、サービスを利用するために必要な秘密情報（秘密鍵等）、機密の個人情報、または検証者に対してサービス利用者と認識させることができる認証情報の値等を騙し取られること。
ファーミング (m)	正当なサービス利用者が、正当な検証者へ接続しようとした際に、ドメインネームサービスまたはルーティングテーブルの操作によって、悪意のある第三者のWebサイトに導かれること。
資格証明局 (CSP : Credential Service Provider)	金融機関等によって身元確認をされたサービス利用者に対して、トークン等を発行することで、利用者がその金融機関等により身元確認された当人であることを証明する機関のこと。
アサーションの無効主張 (n)	資格証明局が、正当なサービス利用者に対して発行したアサーションを無効と主張すること。

