令和 4 年 7 月 15 日

国立情報学研究所 学術認証運営員会 次世代認証連携検討作業部会
主査 佐藤 周行

IDaaS や共同利用機関の管理するアカウントが IAL2 を満たすためのガイドライン（案）

この文書は、一部の SP において海外の研究者、企業等の研究者がアカウントを与えられ、実際にサービスを提供されていることに鑑み、そのような運用形態を IAL2 の観点から収容するための方法についてガイドラインの形でまとめたものである。現在策定が進められている IAL2 の規準文書では、タイプ 1. 2 に相当する CSP が対象になる。

タイプ 1.2 に相当する CSP として想定されるのは、具体的には、IDaaS と共同研究利用機関が独自に運用する CSP である。Orthros は、運用の形態、収容する CSP の種類によって一部が対象になることがある。これらをまとめて、今後タイプ 1.2 と記すことにする。

I. 方針

1. 解決すべき問題

IAL2 規準文書に照らし、対象となる CSP のアカウント管理で問題となるのは、本人確認手段が、学認加入研究機関の運用する CSP に比較して、制限されていることである。大学等研究機関は、文部科学省の指導等によって強い規制がかかっていることを前提に組織のアイデンティティ管理の信頼性を学認が認めている一方、タイプ 1.2 の CSP については、その信頼性を所属企業 又は 社会が提供する手段によって確保するしかない。

一方、タイプ 1.2 の評価についても、従業員管理の統制が正しくとれている企業（特に研究に一定のリソースを割いている企業）が多くあること、金融機関や携帯キャリア等では、犯罪収益移転防止法等を根拠として、本人確認を行うスキームが一定程度確立されていることを考えれば、合理的なコストをかければ、IAL2 規準をみたすことは十分可能である。

そこで、以下、タイプ 1.2 の CSP が IAL2 を満たすために適用すべき身元確認手段のガイドラインを定める。このガイドラインは、社会情勢を反映したリスク評価を不断に行うことで常に最新のものに保守されなければならない。

2. 資格確認（Due Diligence）の利用

CSP が、企業等、組織の研究者等のアカウントを作成する場合は、一般にその組織に属していることを確認する。その組織が十分信頼のおけるものである場合は、社会

的に利用可能な身元確認手段（運転免許証、健康保険証等、公的に発行された証明書の利用）の利用の一部を、組織のメールドメイン利用等で代替することが可能である。この場合、身元確認は、個人に対するものと、組織に対するものからなる。メールドメインについては、組織の代表 Web ページや四季報等、権威があると認められているデータベースをたどることで確認することが可能である。その上で、例えばメールアドレスの到達性等については、IAL2 規準文書に従うことができる。この組織の身元確認の結果は、ホワイトリストとして以後他からも利用可能にするのがよい。

なお、Due Diligence は、一般に SP が確認するものとされ、CSP でなされることは禁忌とされる（NIST SP800-63A）。ここでいう Due Diligence は、利用資格というよりは、利用者が「正当な」組織に所属していることを確認するプロセスと理解すべきである。また、各サービス提供者の定める利用資格確認に関する判断を拘束するものではない。

3. ホワイトリストの管理保守

何が「正当な組織」であるかの判断は、一般に研究コミュニティに依存した運用が行われてきた。研究者が他の研究者を紹介するという紹介システムが機能してきたことも大きい。これを学認全体で共有するためには、学認が、組織の正当性を評価する基準を定め、ホワイトリストの形で保守することがコスト合理性の上からも、強く求められる。

4. eKYC の利用

ホワイトリストに属さない利用者（フリーランス、海外在住の研究者等）に対する身元確認としては、Due Diligence の利用が制限される。この場合、eKYC の積極的な利用を推進すべきである。現状では、eKYC をビジネスとして展開しているところもあるので、その利用が考えられる。また、IDaaS 等で KYC を実施する場合は、以下に定める基準以上の確認を行っていると認められる場合は、積極的に認定すべきである。

また、eKYC の結果として IAL2 以上の身元確認がなされ、その上でアカウントを与えているようなシステムでは、そのアカウントによるアクセス（IAL2 規準文書では AAL2 以上が必要）が IAL2 を保証すると考えることができる。この意味で、公的個人認証や gbizID を含む他のアカウント体系との連携ができている IDaaS の評価を上げるべきである。

II. Due Diligence, eKYC の具体的なガイドライン

以下、NIST SP800-63A と具体的には NIMS で運用されるに従い、使用する確認書類の解決/収集/正当性証明/検証の結果、NIST SP800-63 で言う「STRONG」と認定するためのガイドラインを具体的に定める。さらに、eKYC の利用に際して、タイプ 1.2 の CSP が満たすべき点を述べる。eKYC に関しては、CSP 自らが行っても良いし、

下の基準を満たす外部機関の結果を利用しても良い。

1. 身元確認のためのアーキテクチャ
   A. CSP 自らがすべての手続きを行う場合

      規程 1.A.1 CSP の属する組織は、組織外の人間を、タイプ 1.1 と相互運用性を持つ適切な身元確認を通して CSP に登録することができる。

      規程 1.A.2 所属が「組織外」であるかどうかの判定は、別に定める

      注）従来から、学術振興会特別研究員や一般の客員研究員等の扱いが問題になっている。これらの扱いは、今まで醸成されてきた信頼関係によって定まることになる。ただし、文書を通して明示的に定め、検証可能になっていることが求められる。

      規程 1.A.3 CSP は、規程 1.A.1 と規程 1.A.2 に関する事項を CrP/CrPS に明示的に記さなければならない。

   B. 一部について、他の検証結果を利用する場合

      規程 1.B.1 CSP は、身元確認に、別途認定した eKYC 業者の結果を利用することができる。

      規程 1.B.2 CSP は、規程 1.B.1 に関する事項を CrP/CrPS に明示的に記さなければならない。

      規程 1.B.3 eKYC 業者の認定要件は、NII が別に定める。NII は、認定に当たってタイプ 1.1 と相互運用性をもつことを評価しなければならない。

   C. 確認書類自体が検証可能な形式をもっている場合

      規程 1.C.1 CSP は、eKYC に当たり、身元確認の確認書類を、CrP/CrPS に明示的に記したうえで利用することができる。

      規程 1.C.2 利用できる確認書類について、確認書類自体の検証と発行者の検証の仕方を定めなければならない。

2. 身元確認のための確認書類の特定と収集
   A. 組織へ所属していることを証明する文書

      規程 2.A.1 組織に所属していることを証明する、当該組織が発行した文書は、身元確認の確認書類として利用することができる。

      規程 2.A.2 身元確認に利用できる意味での組織の正当性は、NII が認定し、管理する。その上で、当該組織の発行した以下の文書を確認書類として認める。

      1. 写真入り身分証

      規程 2.A.3 組織へ所属していることの証明には、公式メールアドレス、公式窓口への電話を含む、7 日間以内の確認を含まなければならない。確認したことは記録に残さなければならない。

   B. 公的性格をもつ文書

規程 2.B.1 国、地方自治体が発行した文書及びその中に記された情報は、公的性格を持つ文書として身元確認の確認書類として利用することができる。

規程 2.B.2 公的性格を持つ文書を用いて発行される文書は、公的性格を持つ文書に準じる。

注）銀行口座の情報等を想定する

規程 2.B.3 身元確認に利用できる意味での文書の正当性は、NII が認定し、管理する。当面、以下の文書を確認書類として認める。

1. 運転免許証
2. 運転経歴証明書
3. マイナンバーカード（表面のみ）
4. 住民基本台帳カード
5. パスポート
6. 在留カード
7. 特別永住者証
8. 本人写真

注）たとえばパスポートは、すべての国のものを認定することが適切であるが、それ以外であれば、国によって認定する文書の種類が異なることが想定される。

規程 2.B.4 確認書類は原本、本人写真の場合は撮影データでなければならない。

3. 確認書類の正当性証明

規程 3 提出された確認書類は、CSP がそれを真正であると判断した根拠を記録しなければならない。

注）提出された確認書類が正当であることを証明するために、電子的な方法が提供されているものがあるが、運転免許証に代表的なように、その一般的な利用が制限されていることも多い。その場合は、原本 又は その撮影データを目視で確認することを許容する。

4. 確認書類からの情報検証

A. 利用する情報の特定

規程 4.A.1 確認書類中、本人確認に用いる情報は以下に限定する。

1. 氏名
2. 生年月日
3. 本人写真

注）特に due diligence の一環として収集した確認書類に記された情報の利用を制限する。マイナンバーカードを確認書類として用いる場合も表面に記された情報しか利用してはならない。

規程 4.A.2 規程 4.A.1 に関わらず、due diligence の一環として収集した確認書類

中、本人の所属に関する情報を本人確認に用いてよい。

規程 4.A.3 規程 4.A.1 に関わらず、規程 2.A.3 の実施のために、住所 又は メールアドレスが確認書類に記されている場合、それを利用しても良い。

B. 検証に用いる手続き

規程 4.B.1 本人確認の手続きを前もって申請人に提示しなければならない。

規程 4.B.2 本人確認は、以下の手順を含まなければならない。

1. 申請者から得た氏名・生年月日と、同申請者から提供された確認書類記載の情報を比較し、両者が合致することを確認する。

2. 申請者から得た自己の写真と、同申請者から提供された確認書類の顔写真を比較し、両者が合致することを確認する。

規程 4.B.3 本人確認の結果として、以下の場合は否認の判断をしなければならない。また、否認の理由を申請人に開示しなければならない。

1. 指定する確認書類ではない。
2. 指定する確認書類の原本ではなく、コピーやスキャンデータなどの撮影データである。
3. 確認書類中、本人確認に用いる情報が視認できない。
4. 確認書類の有効期限が切れている。
5. 確認書類の発行元の記載がない。
6. 確認書類が運転免許証であり、裏面が隠されている。
7. 確認書類がパスポートであり、所持人記載面に氏名が書かれていない。
8. 確認書類がマイナンバーカードであり、下記のいずれかに該当する
   a. マイナンバーが 1 桁でも視認できる
   b. マイナンバーカード裏面の QR コードが視認できる
9. 確認書類が在留カードであり、下記のいずれかに該当する
   a. 顔写真の掲載がない
   b. 交付期間と発行者の組み合わせが下記と相違する
      - 交付日が 2019 年 3 月 31 日まで：法務大臣
      - 交付日が 2019 年 4 月 1 日以降：出入国在留管理庁長官

注）具体的な否認の基準を申請人に前もって開示する必要はない。

C. 検証の内容

規程 4.C.1CSP は検証に用いる各情報につき、申請者と確認書類の情報が合致する・しないと判断する基準を定めなければならない。各判断は記録しなければならない。

注 1）具体的な基準を申請人に前もって開示する必要はない。

規程 4.C.2 検証を遠隔で行う場合、本人が確認書類を所持していることとその確認書類が真正であることの証明ができる程度の映像の品質、本人の遠隔監視の品

質の下で行わなければならない。検証時の映像は録画し、アカウント発行のリスクが十分下がったと判断するまで記録しておかなければならない。
注)「アカウント発行のリスク」は、発行したアカウントが何らかの規定に違反する行動をとる恐れを含まなければならない。記録の期間は、CSP ごとに定めてよいが、一般のネットワークログの保存期間に準じるのが妥当である。

規程 4.C.3 氏名情報の確認は以下に従う。

1. 日本名
   a. 合致すると判断する場合
      i. 氏名の表記が一致する
         異体字は一致すると判断する。
         新旧の姓が記載されている場合、新姓を確認に用いる。
         氏名の間が全角または半角スペースで区切られている。
   b. 合致しないと判断する場合
      i. 氏名の表記が一致しない
         氏名の間が全角または半角スペースで区切られていない。
         ひらがな、カタカナ、アルファベットの表記が異なる。
         姓名が逆に書かれている。
   c. 判断を保留する場合
      i. 氏名の一部の漢字がひらがな・カタカナで記載されている。
2. 日本名以外
   a. 合致すると判断する場合
      i. 氏名のひらがな、カタカナ、アルファベットの表記が一致する。
         申請者から得た氏名でミドルネームが省略されていても一致すると判断する。
         南アジアに関係すると判断される書類においては、氏の記述がなくても名前の一致だけで判断してよい。
         確認書類に通称名が記載されている場合、そのいずれかと一致する。
         確認書類にアルファベットと漢字が併記されている場合、そのいずれかと一致する。
         氏名の間が全角または半角スペース、ハイフンで区切られている。
   b. 合致しないと判断する場合
      i. 氏名のひらがな、カタカナ、アルファベットの表記が一致しない
         中国語の繁体字と簡体字の違いは一致しないと判断する。
         氏名の間が全角または半角スペース、ハイフンで区切られていない。
         申請者から得た氏名に、確認書類にないミドルネームが追加されている。
   c. 判断を保留する場合

i. 申請者から得た氏名と確認書類にある氏名の差異判断に迷う。

規程 4.C.4 氏名情報の確認は以下に従う。

1. 合致すると判断する場合

   申請者から得た生年月日と確認書類記載の生年月日が一致する。

2. 合致しないと判断する場合

   申請者から得た生年月日と確認書類記載の生年月日が一致しない。

規程 4.C.5 本人写真の確認は以下に従う。

1. 合致すると判断する場合

   本人写真と確認書類の顔写真が同一人物だと判断できる。

2. 合致しないと判断する場合

   「目、鼻、口」の 3 つが写っていない。

   サングラス、帽子などで顔が隠れている。

   本人写真と、確認書類の顔写真が同一人物だと判断できない。

5. 確認した情報の開示

規程 5 CSP は、本人確認に利用した情報を、作成したアカウントの属性情報としてサービス提供者に開示する場合、その範囲を CrP/CrPS にあらかじめ規定しなければならない。