2021-10-20

学認次世代認証連携検討作業部会

IAL2 の新学認での運用に当たって（案）

次世代認証連携検討作業部会では、学内外で配慮を要する情報を扱うサービス、強いセキュリティが担保されていることが大前提となるサービスへのアクセス、特に国内外にあるさまざまな研究コミュニティが持つ情報・計算リソースへのアクセスを認証面からサポートするために、認証強度についての基準作成とともに、大学等研究機関や研究コミュニティへの参加を呼びかけて、大きな信頼の枠組（トラストフレームワーク）を運用することを目指している。その際に、身元確認の保証度（Identity Assurance Level）と本人確認の保証度（Authentication Assurance Level）の基準策定と運用が必須になる。本作業部会では、参加機関が運用可能でありかつ国際的に合意の取れる基準を策定する。

認証に携わる業界では、この種の話のベースラインとして必ず出てくるのが米 NIST の基準であり、その運用団体の一つである Kantara である。学認は、従来実施要領と技術基準の策定と運用によって基本的な保証度を担保した運用を行ってきた。実際、学認は Kantara に参加の上、基本的な保証レベルである LoA1 の認定を学認内で運用可能にしてきた。

今回、一段強い基準である IAL2, AAL2 を運用することが必要になったことをうけ、具体的に NIST SP800-63 と Kantara KIAF1430 に従って、新学認において IAL2 を運用するときの基準を定めるについて、以下の見解と規程作成に当たっての方針案を述べる。内容は以下からなる

1. CSP の大学内での定義と、それに従う NIST/KIAF の読み替えの方針
2. CSP の運用範囲内で定めることと、より上の大学運営にかかわることの分離
3. CSP 運用の一般的な条項
4. 一般的なセキュリティ
5. CrP/CrPS のテンプレート
6. IAL2 を実現するための身元確認の基準
7. 学認トラスト WG による認定と運用、監査体制
8. 本文書に関する意見、問い合わせ先

なお、AAL2 については、策定作業を開始するにあたり、現状調査の準備をしている。これについても協力をぜひお願いしたい。

1. CSP の大学内での定義と、それに従う NIST/KIAF の読み替えの方針

NIST や KIAF の文書のモデルでは従来 IdP と呼ばれていたものを CSP（Credential Service Provider）といい、パスワードや証明書などのクレデンシャルを利用者に発行するサービスを行うところを規制の対象としている。そのモデルでは Verifier が、そのクレデンシャルを検証して RP(SP)にアサーションを発行する役割を持っている。我々が一般的に考える IdP は、Verifier と（クレデンシャルの発行という意味での）一部の CSP の機能を合わせた機能を持っている。CSP の持つ利用者登録は、大学や研究所でいえば、学務や人事を担当する部局の責任の下行われるだろう。CSP と IdP が NIST のモデル的には不完全に分離して運用されていることから、例えば本文書内での IAL2 の実現主体が（我々の言う）IdP なのか CSP なのか、振れることになる。

ここでは、最初にこの誤解を生じかねない事態を整理することから始めたい。

1.1 大学や研究所で学務や人事が CSP として利用者登録をおこなっている場合

現在、統一アカウントの運用が大学で普通に観察されるようになっている。アカウントの発行は、例えば情報基盤センターで行うのではなく、学務や人事の組織にとって信頼できるデータベース（以下 Trusted DB と言う）から直接プロビジョニングされる。また、IdP の運用を外部委託（IDaaS）していても、Trusted DB に接続されていればここに当てはまる。

このような場合、NIST で規定されている CSP の身元確認は、入学、採用時のプロセスとそれを反映した Trusted DB の維持管理の一部として行われる。このような場合、IdP を運用する部署は NIST に定められた IAL 維持のためのアクションの多くについて責任を持つ必要はない。**組織の成熟度（入学や採用が事故なく円滑に行われていること）を評価すれば足りる。**IdP は、アカウントの生成プロセスとそのポリシーについて、上位の規程を参照しながら定めることで足りる。

1.2 IdP が、組織内で運用する共同利用のサービスの IdP として、アカウントを運用している場合

例えば、共同利用システムを運用していて、組織外部の利用者にアカウントを発行して運用する大学の部局や研究所がこれに当てはまる。この場合は、以降規定することがフルセットで当てはまる。ただし、大学や研究所のアカウントが十分信用できるのならば、それを利用してアカウントを作成する場合、IAL 審査のコストを大きく下げることができる。この意味でもホームとなる機関での IAL（と AAL）は重要である。

2 CSP の運用範囲内で定めることと、より上の大学運営にかかわることの分離

以上の観察に基づき、以降では NIST/KIAF の文書のうち、規定をタイプ 1, 2 に分類

して議論し、新学認参加の IdP が措置することを定める。

タイプ１) CSP 運用の一般的条項（NIST/KIAF では General Requirements, CrP/CrPS, Security Control, Trusted Referee Proofing で規定されているもの）
タイプ２) Identity Proofing の各条項（同じく resolution, evidence collection, validation, verification, presence, address confirmation で規定されているもの）

規程 0 は、IdP を運用する機関が、タイプ１と２のどちらに分類されるかを定める。

規程 0.1　IdP がサービスを提供するアカウントのうち、機関の Trusted DB から直接プロビジョニングされているものについての IAL は、タイプ１に関係する規程を適用する。それ以外のアカウントの IAL は、タイプ１とタイプ２に関係する規程を適用する。

規程 0.2　**0.1** において認定機関（学認）は、被審査機関が、その Trusted DB から直接プロビジョニングされているかどうかを認定し、それぞれ適用する項目を決定する。
注)「直接プロビジョニングされているか」は、以下に関する認定で判断する
１．プロビジョニングのシステムアーキテクチャが、十分自動化されていて、組織による恣意的な運用（当該プロビジョニング以外のプロセスによるアカウントの作成等）を十分抑止できているか
２．プロビジョニングの運用実態が、システムセキュリティと権限管理において十分統制されているか

規程 0.3　**0.2** で Trusted DB から直接プロビジョニングされていると認定された場合においては、当該 Trusted DB が IAL2 に相当する強度の身元確認を実施しているかを認定する
注）日本における大学、研究機関では、学生の入学試験の実施、入学、また教職員の採用に関しては、文部科学省等による規制がある。その規制に従っていると判断される場合は、それらの規制項目を準用して認定することができる。一般的に言って、日本の機関での運用を前提にすれば、IAL2 の強度を満たすことが期待される。ただし、オンラインで完結する大学等では、身元確認の運用について従来より緩和された基準で運用されている可能性がある。この場合、「組織の成熟度」と「過去の事故履歴」を総合的に勘案して認定することができる
注）大学、研究機関によっては研究倫理に関する問題、学生や教職員の不良行為の問題を抱えているところがある。これらは、サービスを提供する RP にとって重大な関心を持たざるを得ない。新学認の認定はこれについて個々の RP の事情を勘案するものではないが、ただし「組織の成熟度」の判断に組織の抱えている問題の要素を勘案することもできる。

3　CSP 運用の一般的な条項

ここでは、CSP 運用の一般的な条項を定める。運用上の規程文書の整備とリスク評価、監査、苦情処理等のいわゆる「静脈系」サービスの整備が求められる。

プライバシーに関係する条項

規程 1.1 CSP が保持する個人情報は最小限の原則に基づくこと。収集保持に当たって、プライバシー上の配慮をすること
注）Trusted DB 等外部からプロビジョニングされる場合、運用される項目を運用に求められる最小限にすること。
規程 1.2 CSP が属性を収集・保持する場合は、利用目的の明確化、利用シナリオの制限を行い、CrP 内で公開し、最小限の原則に基づいて運用すること
2. 属性を収集する場合に、プライバシーに関する規程を定め、利用者に示した上で同意を得ること。
注）プライバシーに関する規程には、収集する属性が必須か任意か、属性収集に同意しない場合の不利益についての記述を含む。
規程 1.3 アイデンティティに関係するサービス以外の目的のために追加で属性を収集運用する場合、収集に不同意の利用者に不利益を与えてはならない。
2.　収集する場合、効果に対する評価を、関連するプライバシーリスク評価とともに行い、文書として記録すること。
注）「アイデンティティに関係するサービス以外」には、攻撃機会の軽減や法律の要請を含む

3.1　苦情処理に関係すること

規程 1.4 利用者の登録に関する苦情処理の手続きを定め、運用すること。
２．苦情処理の手続きは１年に最低１回、効果についての評価を行うこと

3.2　CrP/CrPS の制定と運用

クレデンシャルについてのポリシーと運用規定（CrP/CrPS）を定めることが求められる。テンプレートを別文書で与える。

規程 1.5 身元確認と登録のポリシーはクレデンシャルポリシー（CrP: Credential Policy）として事前に公開すること。

2. CrP では、以下を規定しなければならない。

A. 採用する身元確認の方法の種類と、それぞれについて用いる証拠の発行元

B. 利用者の種類に応じて適用する/適用しない身元確認の方法

規程 1.6 CrP を実現するための実施要領（CrPS: Credential Practice Statement）は、以下を規定しなければならない。

A. CrP に定めた身元確認の方法の具体的な実施方法と手続き

B. それぞれの実施方法について、身元確認が成功しない場合の対処方法

規程 1.7 CrP/CrPS の運用に関し、プライバシーとセキュリティに関するリスク管理を最低 6 か月に一度定期的に又は CrP に大きな変更が生じた場合はその都度実施し、その結果を文書として残すこと。リスク管理の具体的な内容には以下を含むこと

A. CrPS 中の必須要件を超えて身元確認を行う場合、その手続き

B. CrP で定めた身元確認の手続きの一環として収集保存する個人情報の一覧

C. 法令、内規等の要求するところによる記録の保存、廃棄のスケジュール

D. 不正防止策を講じる場合、その防止策

規程 1.8 身元確認の実施、監査のためのログを保存すること。特に身元確認の方法、収集する証拠、証拠の発行元への問い合わせ記録、証拠の妥当性確認のすべての手続き、証拠の検証のすべての手続きの実施それぞれの実施結果と身元判断の最終判断を含むこと。

3.3　セキュリティ対策

規程 1.9 身元確認の際に収集した個人情報の情報セキュリティ保護を行うこと。

規程 1.10 身元確認の手順全体は、セキュリティで保護された通信を使って行わなければならない。

3.4　サービスの終了

規程 1.11 CSP が、サービスを終了する場合、それまでに収集した個人情報の廃棄、破壊の仕方、不正なアクセスからの保護について定めること。

4　一般的なセキュリティ

規程 1.12 CSP を運用するシステムは、一般的なセキュリティ基準に従い、十分なセキュリティ対策を実施すること。

注）セキュリティポリシーの政府統一基準でもよいし、それを大学のセキュリティポリシーが参照しているならば、大学のセキュリティポリシーでもかまわない。とりあえずだが、皆が納得できるポリシーや基準を定め、それに従って運用されていることを示すことが大切である。

5　CrP/CrPS のテンプレート

⇒別文書

6　IAL2 を実現するための身元確認の基準

以下は、1.2（全国共同利用の IdP を運用する）で定めたタイプに当てはまる条項である。この場合はアカウントを審査、発行する手続きについて定めなければならない。

ほとんどの、Trusted DB に直接接続してプロビジョニングしている大学の IdP では、これまでの議論に従い、ここでの議論は適用されない。

２つのタイプは、たとえば、大学のアカウントで、全国共同利用の IdP に登録する場合に出会う。大学のアカウントが IAL(≧2)、AAL(≧2)の保証レベルを満たすなら、そこでのログインのアサーションを STRONG な証拠（後述）として主張できる。

6.1　文書解決（Resolution）

規程 2.1 収集したデータを特定人の身元確認の証拠として採用するときの個人情報の収集は、社会的に合意のとれた最低限のものにすること。

6.2　証拠の収集（Evidence Collection）

規程 2.2 CSP は、利用者から（後述の）STRONG 以上の証拠を 1 個集めること。ただし、発行元が 2 個以上の証拠を収集した上で証拠を発行し、CSP がそれを直接確認できること。

2. CSP が上記の確認をできない場合、STRONG 以上の証拠を 2 個集めること。

3. それができない場合、STRONG の証拠を 1 個、FAIR の証拠を 2 個で代替しても良い。

規程 2.3 証拠のレベルの判断理由を文書に記録しておくこと

例）A. 日本の大学の発行する写真入り学生証又は職員証は STRONG として扱ってよい。

B. 一般の会社の発行する職員証は FAIR と扱わざるを得ない

C. パスポートや運転免許証は STRONG である。ただし、内部に格納されている生体情報にアクセスできるのならば SUPERIOR として扱ってよい

D. リモートでの大学 IdP が発行した認証アサーションは（何らかのトラスト内で）IAL2、AAL 2 であることを前提として、名前（CommonName）の保証度が 2 になっていれば、CSP が直接確認可能な STRONG な証拠として扱ってよい。

6.3　証拠の妥当性確認

規程 2.4 収集した証拠は、その強度に依存し、後述の妥当性確認レベルをそれと同等以上にして妥当性確認を行うこと。

規程 2.5 妥当性確認のレベルの判断理由を記録しておくこと。

2. 妥当性判断のための人員の研修のためのポリシー、ガイドライン、要件を文書化すること。

6.4　証拠の検証

規程 2.6 証拠の検証は STRONG 以上の強度で行うこと。特に知識ベースの検証は行わないこと。

規程 2.7 STRONG 以上での検証を行ったことの判断理由を記録しておくこと。

6.5　実在性確認

規程 2.8 実在性確認は、対面、又はリモートで監視下にある場合、もしくはリモートで監視下にない場合の最低 1 種類を用いて行う。実施要領は CrP に記載すること。

6.6　アドレス確認

規程 2.9 利用者のアドレスは、証拠の発行元のみから識別しなければならず、自己申告を認めてはならない。

規程 2.10 監視下での実在性確認を行った場合、登録コードは利用者のアドレスに送付するか、又は直接手渡ししても良い。登録コードの有効期間は 7 日を超えてはならない。

2. 監視下にない環境で実在性確認を行った場合、登録コードは利用者のアドレスに送付しなければならない。この場合、送付された登録コードを提示させることで身元確認を終了させること。登録コードの有効期間は 7 日を超えてはならない。

規程 2.11 登録コードを認証要素として利用する場合は、最初の認証要素として利用するときにその要素は無効化しなければならない。この時の有効期間は郵送の場合は 10 日、電話を利用する場合は 10 分、メールを利用する場合は 24 時間を超えてはならない。

規程 2.12 登録コードと身元確認の結果通知を同一のアドレスに送付してはならない。

注）ここでのアドレスとは郵送可能な物理住所、携帯電話, 固定電話、電子メールのいずれかとする。

6.7　証拠、妥当性確認、検証の Fair/Strong/Superior の基準と例示

6.7.1 STRONG の強度を持つ証拠の要件

A. 発行ポリシーが、生存している人間に対して合理的に定められていて、当人に対して発行されている。さらにそのポリシーが文書化され、規制当局により適切に監督されている。

B. 参照番号が一意に振られている

C. 記載されている名前は、公式に認識されたものである。フルネームのみを許容し、省略形を許容しない

D. 写真がついているか、生体情報を含む。又は、IAL2, AAL2 の保証レベルを持つアサーションである

E. 以上の情報のうち、ディジタルなものは暗号的に保護されている
F. 物理特徴(券面情報等)を含む場合、それをコピーして複製するのが困難である
G. 有効期限以内であることが確認される。
例）1. 公的機関が発行した写真付き証明書。パスポート、運転免許証、無線従事者証等。文科省の監督下にある大学の発行したものも、適切に運用されていれば、この扱いをしてよい。
2. 大学の IdP によって発行されたアサーションを STRONG とみなすには、uid（一意に定まるもの）と CommonName に IAL2 の保証を与えることが必要である。

なお、証拠で FAIR の強度を持つ規程は省略する。

6.7.2 STRONG の強度を持つ妥当性確認の要件

A. 適切な手段（人による確認を含む）で、証拠が、券面または含まれるディジタル情報において改ざんされていないことを確認できる
B. 発行元の出す情報と照合して、証拠中の個人情報が正当であると確認できる
注）パスポートや免許証に不審な点がないと注意深く確認できる。これらについては、偽造は法律（公文書偽造）で罰則が定められているのでそれが社会的な抑止力になっていると考えてよい
注）アサーションについては、保護された通信で送られてきたのならば、STRONG とみて差し支えない

6.7.3 STRONG の強度を持つ検証の要件

A. 対面での写真と本人の比較、または生体情報の比較による本人一致の検証。対面の場合、通信の品質、画面の品質などを十分高く保ち、十分な検証品質を保たなければならない。厳密には、NIST/KIAF で提示されている品質を保証するための技術的検証を必要とする。
注）証拠中の写真と本人の照合。登録された生体情報を利用する（出入国審査で利用されているもの等）時と同様の精度が要求されている。人間が対面で審査する場合は信用されているが、リモートの場合は、対面と同様の審査を可能にする通信と画質の品質の保証が求められる。
注）アサーションの場合は、内容の審査をすることで差し支えない。

7　学認トラスト WG による認定と運用、監査体制

現在、学認では、参加組織に対して LoA1（NIST SP800-63-1 相当）の認定の枠組を提供している。実作業はトラスト WG が担当している。IAL2 とそれに続く AAL2 につ

いて、本文書が Kantara の基準に従うかどうかを判断するのは Kantara であるが、それが認められた場合、学認のトラスト WG が（少なくとも）日本での Kantara 認定作業を担当することができるかもしれない。IAL2 と言っても、Kantara のものか、学認独自のものかによって違いができる。国内では違いは問題にならない。eduGain 等、国際研究協力に資するサービス提供者への対応は交渉を必要とするだろう。

いずれの場合でも、学認トラスト WG は、学認内での IAL2 認定を担当する。認定された IdP が assurance に関する属性値を送出することを許可する。例えば、gakunin-IAL2 のような属性値が少なくとも国内で流通することになるだろう。これらの運用に対する監査もトラスト WG が担当することになる。

さらに、学認に属する機関が IAL2 認定を受けるための助言をトラスト WG が積極的に担当する。この場合、認定をする者と別の者が助言に当たることになるだろう。

8　本文書に関する意見、問い合わせ先

本文書に関する意見、問い合わせは、以下からお願いします。

https://www.gakunin.jp/contact