IAL2 運用規程 解説書

Rev.1 2026 年 6 月 1 日

本解説書は、IAL2 運用規程を基に、学認における IAL2 運用の背景、設計思想、実装方法および審査観点を整理したものである。本書では、単なる条文説明に留まらず、大学・研究機関における実際の運用を想定しながら、各要件が何を意味し、どのようなリスクに対応するためのものなのかを解説する。

IAL（Identity Assurance Level）は、利用者の身元確認がどの程度信頼できるかを示す保証レベルである。近年、研究データ基盤、GPU/HPC 資源、国際共同研究基盤等において、単なる認証ではなく「誰が利用しているか」を保証する要求が強まっている。特に eduGAIN、MyAcademicID、EBSI 等の国際連携では、組織がどの程度信頼できる本人確認を行っているかが重要となる。学認では、大学が既に保有している学務・人事システムを活用しながら、国際標準へ適合する形で IAL2 運用を実現するため、NIST SP800-63 および Kantara KIAF を参考にした運用モデルを採用している。

IAL2 運用は、単なる本人確認手順ではなく、「大学・研究機関がどの程度信頼できる組織運用を行っているか」を示すトラストフレームワークである。そのため、審査では「完全性」だけではなく、「説明可能性」「再現性」「統制可能性」が重視される。学認における IAL2 は、大学が本来持つ Authority としての役割を、国際的なデジタルトラスト基盤へ接続するための重要な仕組みである。

第 5 条（Trusted DB 判定）

本条は、IAL2 運用における中核概念である Trusted DB の妥当性を確認するための条項である。

Trusted DB ベースの運用では、個別に証拠収集を行わずとも、既存の大学業務プロセスに基づいて本人確認済みとみなすことができる。しかし、その前提として、組織運用が適切に統制されている必要がある。特に「正式業務プロセスとの連携」とは、入学、採用、受入れ等の大学公式手続きとアカウント生成が密接に連動していることを意味する。例えば、学生が入学手続きを完了した後、自動的に学務システムへ登録され、その情報が統合 ID 管理基盤を経由して IdP へ反映されるような構成が該当する。

「継続的な更新」とは、一度登録した情報を放置するのではなく、退学、退職、所属変更等を適切に反映することを意味する。これが行われない場合、実在しない利用者や権限を失った利用者が引き続き認証可能となる危険がある。

「追跡可能性」とは、誰が、いつ、どのような変更を行ったかを後から確認可能な状態を指す。これは監査やインシデント対応時に重要となる。

「権限統制」とは、誰でも自由にアカウントを追加・変更できないよう、適切な権限分離

と承認フローが存在することを意味する。

- 入学時に対面確認済みの学生情報を学務システムへ登録
- 人事システムから自動的に IDaaS へ同期
- LDAP 更新ログを SIEM へ転送

単に「学務システムを利用している」だけでは不十分であり、例外運用、手動登録、特権アカウント運用等を含めて、組織として説明可能な統制が存在するかが重要である。

第 16 条（証拠収集）

本条は、利用者の身元確認に用いる証拠を収集する際の基準を定める。

証拠（Evidence）は、利用者の氏名、生年月日、所属等を第三者が保証する情報である。IAL2 では、本人確認を第三者へ説明可能とするため、十分な信頼性を有する証拠が必要となる。

「発行主体の信頼性」とは、その証拠を発行している組織が社会的・制度的に信頼できることを意味する。政府機関、大学、研究機関等は典型例である。

「顔写真または生体情報」とは、証拠に本人確認可能な情報が含まれていることを意味する。これにより、証拠と実際の利用者を照合できる。

「暗号的保護」とは、電子署名、IC チップ、QR 署名等によって改ざん耐性を持つことを意味する。近年はデジタル証明書において重要性が増している。

「偽造耐性」とは、券面コピーや単純な画像編集で容易に偽造できない構造を持つことである。

「一意性」とは、その証拠が単一人物へ一意に紐づくことを意味する。

- マイナンバーカード
- IC カード学生証

「STRONG と判断した理由」を説明できることが重要となる。単に「学生証だから安全」ではなく、発行・失効・回収・更新等を含めた運用全体が重要となる。

第 17 条（妥当性確認）

本条は、収集した証拠が真正かつ有効であることを確認するための条項である。妥当性確認（Validation）は、「証拠そのものが本物であるか」を確認する工程であり、本人との一致確認（Verification）とは区別される。例えば学生証であれば、「現在も有効な学生証か」「失

効していないか」「改ざんされていないか」を確認する必要がある。

真正性を確認するための実装としては下記の例が挙げられる。

- 学務 DB 照合

審査では、Validation が人手依存なのか、自動化されているのか、失効確認をどこまで実施しているか等が確認される。将来的にはデジタル証明書を用いた確認への拡張を予定している。

第 18 条（検証）

本条は、証拠に記載された人物と実際の利用者が同一であることを確認するための条項である。Verification では、証拠そのものではなく、「その証拠が本当に本人のものか」を確認する。

「映像品質」とは、顔写真や本人の特徴を十分確認できる解像度・明るさが確保されていることを意味する。

「リアルタイム性」とは、録画映像ではなく、その場で本人が応答していることを確認することである。

「なりすまし対策」とは、他人が本人を装って確認を受けることを防止する仕組みであり、生体動作確認や追加質問等が用いられる。

「AI ディープフェイク対策」とは、生成 AI による偽映像や音声合成への対策を意味する。近年は、瞬き、顔向き、ランダム動作要求等が利用される。

- 対面確認
- eKYC（electronic Know Your Customer）
- ビデオ通話確認

本人確認担当者の教育、録画保存、AI 対策、通信品質等が重要である。

第 23 条（一般セキュリティ要件）対応解説

本条は、認証システム全体のセキュリティ要求を定める包括条項である。IAL2 では、認証機能だけではなく、システム全体として十分なセキュリティ対策を講じる必要がある。例えば下記の項目について考慮されているかが重要となる。

- 脆弱性管理

- アクセス制御
- 監査ログ
- バックアップ
- インシデント対応

また、大学・研究機関では、共同利用基盤や国際研究基盤との接続を前提とするため、第三者監査に耐えうる説明可能性が重要となる。

その他用語

CrP と CrPS の考え方

CrP（Credential Practice Statement）は、どのようなポリシーに基づき本人確認を行うかを示す上位文書である。一方、CrPS（Credential Practice Statement Supplement）は、実際の運用手順や実装内容を記載する詳細文書である。

CrP では、以下を定義する。
- 適用範囲
- 保証レベル
- 証拠分類
- リスク方針

CrPS では、以下を定義する。
- 運用手順
- 担当者
- ログ管理
- 回復処理
- 例外運用

重要な点は、「規程に書いてある」だけではなく、「実際に運用されている」ことである。

STRONG / FAIR / SUPERIOR の考え方

学認 IAL2 では、証拠の強度を評価する際に、STRONG、FAIR、SUPERIOR 等の概念を用いる。STRONG とは、高い信頼性を有する証拠であり、一般的には以下を満たす。

- 信頼できる発行主体
- 顔写真または生体情報
- 偽造耐性
- 一意性
- 失効管理

SUPERIOR は、政府発行 ID 等、さらに高い保証を持つ証拠を指す場合に利用される。一方、FAIR は、一定の信頼性を有するものの、単独では十分な保証を持たない証拠である。大学においては、IC カード学生証や職員証を STRONG として扱える場合があるが、その前提として発行・回収・失効管理等の運用統制が必要となる。

【実装例】
- IC カード学生証・職員証
- マイナンバーカード

参考文献

NIST SP800-63A : https://pages.nist.gov/800-63-3/sp800-63a.html?utm_source=chatgpt.com
NIST SP800-63A 日本語訳 : https://www.nri-secure.co.jp/blog/nist-sp-800-63-4-draft02?utm_source=chatgpt.com