IAL2 運用規程（案）

Rev 1 2026 年 6 月 1 日

本規程は、学術認証連携において利用者の身元確認保証レベル Identity Assurance Level 2（IAL2）を実現するために必要な運用要件を定めるものである。近年、研究データ基盤、スーパーコンピュータ、国際共同研究環境及びデジタル証明書基盤との連携において、認証された利用者が「誰であるか」を第三者に対して説明可能な状態で保証することが求められている。そのため、大学及び研究機関において実施される身元確認の信頼性を、組織的かつ継続的に担保することが重要となる。本規程は、NIST SP800-63 および Kantara Identity Assurance Framework を参考としつつ、大学及び研究機関における実運用を踏まえた学術認証連携向け IAL2 運用モデルを定義するものである。

第 1 章 総則

第 1 条（目的）
本規程は、学術認証連携における身元確認保証レベル IAL2 の達成および維持に必要な要件を定め、当該要件に基づく運用が第三者による審査および監査において説明可能である状態を確保することを目的とする。

第 2 条（適用範囲）
本規程は、IdP および CSP に適用される。
2. 本規程は、すべてのアカウントに対する身元確認手続きに適用される。

第 3 条（用語の定義）
本規程において使用する用語は、NIST SP800-63 に準拠し、CSP、IdP、証拠、妥当性確認、検証及び実在性確認はそれぞれ当該基準において定義される意味を有するものとする。

第 2 章 IdP・CSP 運用基盤

第 4 条（Trusted DB の定義）
Trusted DB とは、公式な業務プロセスに基づき登録された情報を管理するデータベースをいう。当該データベースは継続的に正確性が維持されなければならない。

第 5 条（Trusted DB 判定）
IdP および CSP は、アカウントが Trusted DB に基づき生成されているかを判定しなければならない。

2. Trusted DB とは、組織の正式な業務プロセス（入学、採用等）に基づき登録された情報を管理するデータベースをいう。
3. IdP および CSP は、当該データベースが以下を満たすことを確認しなければならない。
（1）登録プロセスが制度的に管理されていること
（2）登録内容の正確性が継続的に維持されていること
（3）登録および更新の履歴が記録されていること
4. 前項の確認結果は文書化し、監査可能な状態で保持しなければならない。

第 6 条（証跡管理）
IdP および CSP は、アカウントの生成、変更及び削除に関する操作について、実施主体、日時及び内容を含むログを記録し、後から追跡可能な状態で保持しなければならない。

第 3 章 プライバシーおよび運用管理

第 7 条（個人情報の最小化）
IdP および CSP は、身元確認および認証に必要な範囲を超えて個人情報を収集してはならず、収集対象となる情報の範囲を事前に定義し、その必要性を説明可能な状態で文書化しなければならない。

第 8 条（利用目的の明確化）
IdP および CSP は、収集した個人情報の利用目的を具体的に定義し、当該目的の範囲内でのみ利用するものとし、目的外利用を行ってはならない。

第 9 条（同意の取得および管理）
IdP および CSP は、個人情報の収集に際して利用者の同意を取得し、その同意の取得方法、取得日時及び同意内容を記録し、利用者が同意の撤回を行うことができる手段を提供しなければならない。

第 10 条（苦情処理）
IdP および CSP は、利用者からの苦情を受け付ける体制を整備し、苦情の内容、対応状況及び対応結果を記録し、継続的な改善に資するものとしなければならない。

第 11 条（CrP）
IdP および CSP は、身元確認の方針を示す CrP(Credential Practice Statement)を策定し、証拠の種類、適用範囲及び確認方法を明確に記載した上で公開しなければならない。

第 12 条（CrPS）
IdP および CSP は、CrP を具体的に実施するための手順を定めた CrPS(Credential Practice Statement Supplement)を策定し、担当者の役割及び例外時の対応手順を含めて運用しなければならない。

第 13 条（リスク管理）
IdP および CSP は、身元確認および認証に係るリスクを定期的に評価し、その評価結果に基づき必要な対策を講じるとともに、当該評価結果を記録しなければならない。

第 4 章 身元確認

第 14 条（証拠収集の基本）
IdP および CSP は、利用者の識別情報を第三者が保証する証拠を収集し、当該証拠に基づいて利用者の身元を確認しなければならない。

第 15 条（証拠の評価）
IdP および CSP は、証拠の発行主体の信頼性、発行プロセスの厳格性及び改ざん耐性を評価し、当該証拠が身元確認に適切であるかを判断しなければならない。

第 16 条（証拠収集）
IdP および CSP は、利用者の身元確認にあたり、信頼性のある証拠を収集しなければならない。
2. 証拠とは、利用者の氏名その他の識別情報を第三者が保証する情報をいう。
3. IdP および CSP は、証拠の発行主体、発行プロセスおよび真正性を評価し、その信頼性を判断しなければならない。
4. IdP および CSP は、証拠収集の際に、収集した証拠の種類、発行元、確認結果を記録しなければならない。
5. IdP および CSP は、証拠の組合せを用いる場合、その補完関係および妥当性を評価し記録しなければならない。
6. IdP および CSP は、証拠の強度評価基準を内部規程として明確化しなければならない。

第 17 条（妥当性確認）
IdP および CSP は、収集した証拠について、その内容が改ざんされていないことおよび有効であることを確認しなければならない。
2. 妥当性確認とは、証拠が真正であり、かつ利用者に関連付けられることを確認する行為をいう。

3. IdP および CSP は、必要に応じて証拠の発行元に対する照会または公開情報との照合を実施しなければならない。
4. 妥当性確認の手順および結果は記録しなければならない。
5. IdP および CSP は、確認手段および判断基準を明確にし、再現性を確保しなければならない。
6. IdP および CSP は、確認の実施者および確認日時を記録しなければならない。

第 18 条（検証）
IdP および CSP 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しなければならない。
2. 検証は、対面確認、映像確認、生体情報照合等の方法により実施する。
3. IdP および CSP は、検証において知識ベース認証のみを用いてはならない。
4. 検証の方法および結果は記録しなければならない。
5. IdP および CSP は、検証手段の品質要件（画質、通信品質等）を定義しなければならない。
6. IdP および CSP は、検証結果の妥当性を後から確認できるよう記録を保持しなければならない。

第 19 条（アドレス確認）
IdP および CSP は、利用者が申告したアドレスが当該利用者により管理されていることを確認しなければならない。
2. IdP および CSP は、当該アドレスについて、証拠に基づく情報との整合性を確認するか、又は当該アドレスへの到達性確認を行うものとする。
3. 到達性確認とは、当該アドレスに対して通知、コード送信その他の手段を用いて、利用者が当該情報に応答可能であることを確認する行為をいう。
4. IdP および CSP は、確認手段、確認日時および結果を記録しなければならない。
5. IdP および CSP は、自己申告のみに依拠しない確認手段を必ず適用しなければならない。
6. IdP および CSP は、確認結果を監査可能な状態で保持しなければならない。

第 20 条（実在性確認）
IdP および CSP は、利用者が実在する人物であることを確認するため、対面又は監視下における遠隔手段により本人確認を実施し、その結果を記録しなければならない。

第 21 条（初期結合）
IdP および CSP は、身元確認完了後、認証器を当該利用者のアカウントに結合しなければならない。

2. 結合は、確認済みアドレスを利用して行い、不正な登録を防止しなければならない。
3. IdP および CSP は、結合に用いた手段および結果を記録しなければならない。
4. IdP および CSP は、登録主体の正当性を確認するための追加手段を適用しなければならない。
5. IdP および CSP は、認証器登録の履歴を保持しなければならない。

第 22 条（回復）
IdP および CSP は、認証器の紛失等によりアカウント回復を行う場合、当該利用者について再度身元確認を実施しなければならない。
2. 回復手続きは、元の保証レベルと同等以上の強度を有する方法で実施するものとする。
3. IdP および CSP は、回復手続きの内容および結果を記録しなければならない。
4. IdP および CSP は、既存認証器の無効化および不正利用防止措置を講じなければならない。
5. IdP および CSP は、回復処理の監査ログを保持しなければならない。

第 5 章 一般セキュリティ要件

第 23 条（一般セキュリティ要件）
認証システム全体について、十分なセキュリティ対策を講じなければならない。