AAL2 運用規程（案）

Rev.1 2026 年 6 月 1 日

本規程は、認証保証レベル AAL2 の達成および維持に必要な認証運用要件を定めるものである。認証器の登録、利用、失効および回復を含む認証ライフサイクル全体について運用可能な状態を維持しなければならない。

第 1 章 総則

第 1 条（目的）
本規程は、多要素認証を前提とした認証運用に必要な要件を定め、認証器、認証処理およびセッション管理を適切に保護することを目的とする。認証運用では、単に認証を成功させるだけではなく、認証器の安全性、利用者本人性および認証後セッションの継続的な保護を確保する必要がある。

第 2 条（適用範囲）
本規程は、利用者認証、認証器管理、認証器登録、認証器回復およびセッション管理を含むすべての認証関連処理に適用する。クラウドサービス、学内システム、共同利用基盤等、認証結果を利用するすべてのシステムは、本規程に基づく運用を前提とする。

第 2 章 認証器要件

第 3 条（認証器の要件）
認証は、多要素認証または同等以上の強度を有する方式によって実施しなければならない。
2. 認証器には、フィッシング耐性、秘密情報保護機能および不正利用対策が求められる。

第 4 条（認証器の評価）
利用する認証器について、その真正性、安全性および運用継続性を確認しなければならない。

第 3 章 パスワードおよび認証

第 5 条（パスワード要件）
パスワードを利用する場合には、多要素認証の一部として利用しなければならない。
2. 推測されやすいパスワード、漏洩済みパスワードおよび利用者属性に依存したパスワードの利用を禁止する必要がある。

第 6 条（パスワード検証）
パスワードは安全な方法で保存し、平文保存を行ってはならない。
2. 保存時にはハッシュ化およびソルト化を適用し、漏洩時に容易に復元できない状態を維持する必要がある。

第 4 章 認証器ライフサイクル管理

第 7 条（認証器登録）
認証器の登録時には、利用者本人による登録であることを確認しなければならない。
2. 登録処理には、本人確認済みセッション、確認コードまたは安全な通信経路を利用する必要がある。

第 8 条（認証器結合）
認証器と利用者アカウントの結合は、安全に保護された認証済み状態で実施しなければならない。
2. 結合処理では、第三者による不正登録を防止するため、追加確認、確認済み連絡先利用または多要素確認を行う必要がある。

第 9 条（認証器失効）
認証器の盗難、紛失、漏洩または不正利用が疑われる場合には、速やかに失効処理を行わなければならない。

第 10 条（認証器回復）
認証器回復時には、元の保証レベルと同等以上の本人確認を行わなければならない。
2. 回復処理では、対面確認、既存認証器確認、別チャネル確認等を組み合わせ、不正回復を防止する必要がある。

第 5 章 セッション管理

第 11 条（セッション管理）
認証後のセッションは、安全な状態で維持しなければならない。セッション管理では、セッション固定化、セッション乗っ取りおよび Cookie 窃取等への対策が必要となる。

第 12 条（再認証）
一定時間非アクティブ状態となった場合、または長時間経過した場合には、再認証を要求しなければならない。

第 6 章　一般セキュリティ要件

第 13 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。