AAL2 運用規程 解説書

Rev.1b 2026 年 5 月 28 日

本解説書は、AAL2 運用規程および「AAL2 の新学認での運用に当たって 第 2 版（案）」を基に、各条項の趣旨、実装上の考え方および審査観点を整理したものである。
本書では、単に条文を言い換えるのではなく、「なぜその要件が必要なのか」「どのようなリスクを防止するのか」「大学・研究機関においてどのように実装するのか」を中心に解説する。

第 3 条（認証器の要件）

本条は、AAL2 における認証器の基本要件を定めるものである。AAL2 では、単純な ID・パスワードのみの認証ではなく、多要素認証または同等の強度を持つ認証方式を採用することが求められる。ここで重要なのは、「認証器そのものの性能」だけではなく、「その認証器が実際にどのように運用されるか」である。例えば、FIDO 認証器のように技術的に強固な認証器であっても、登録手続きや失効処理が不適切であれば、全体としては AAL2 の保証を満たさない可能性がある。

また、認証器の強度評価では、以下の観点が重要となる。

- フィッシング耐性
- 鍵保護機能
- 複製耐性
- 利用者認証方法
- 外部認定状況

大学・研究機関では、Microsoft Authenticator、Google Authenticator、FIDO2 セキュリティキー、UPKI クライアント証明書等の利用が想定される。

第 4 条（認証器の評価）

本条は、認証器を採用する際の評価基準を定めるものである。AAL2 では、「どの認証器を利用するか」を明確に説明できる必要がある。そのため、認証器の技術仕様だけではなく、発行主体、サポート状況、既知脆弱性、外部認定等を総合的に評価する必要がある。特に学認では、各参加機関が個別に認証器評価を行う負担を軽減するため、学認認証器レジストリの活用を前提としている。FIDO Alliance 認定を受けた認証器については、その認定結果を参考にすることで、一定の信頼性を確保できる。NII が運用している学認認証器レジストリ

では認証器を評価しており AAL2 の対応条件を満たしている。

学認認証器レジストリ（https://level2.gakunin.jp/）: 学認は認証器の性能を調査し、AAL2 の認証に使用できるかどうかのレジストリを用意している。また、参加機関の求めに応じて、認証器の審査・認定を行った場合、その結果を登録し、定期的に更新することで、他機関の認定に使用することができる。

認証器の採用にあたっては次の点がポイントとなる。

・採用理由
・認証器の認定状況
・脆弱性対応
・更新履歴
・運用制限事項

第 5 条（パスワード要件）

本条は、多要素認証におけるパスワード運用の基準を定めるものである。NIST SP800-63 では、PII（個人識別情報）を扱う場合、パスワード単独認証を推奨していない。そのため AAL2 では、パスワードは多要素認証の一部としてのみ利用される。しかし、パスワードが攻撃対象となりやすいことは変わらないため、一定以上の強度を確保する必要がある。特に「推測されやすいパスワードの禁止」は重要である。これは単なる文字数制限ではなく、辞書攻撃や漏洩済みパスワードへの対策を意味する。

例えば具体的には以下のようなパスワードは禁止対象となる。

- password
- 12345678
- 大学名＋年度
- 利用者名を含む文字列
- その他、辞書攻撃耐性一般

また、長すぎるパスワード入力を不当に制限しないことも重要である。これは、利用者がパスフレーズを利用できるようにするためである。

第 6 条（パスワード検証）

本条は、パスワードをシステム側でどのように扱うべきかを定める。最も重要なのは、「平文保存を行わないこと」である。保存時にはハッシュ化およびソルト化を行い、万が一デー

タベースが漏洩しても、元のパスワードが容易に復元されないようにする必要がある。また、「スロットリング」はオンライン推測攻撃対策として重要である。短時間に大量のログイン試行が行われた場合、遅延や一時停止を行うことで総当たり攻撃を防止する。さらに、パスワード入力時に「どこが間違っているか」を過度に表示してはならない。これは攻撃者へヒントを与えないためである。

運用においては例えば以下のような項目に対応して運用を実施することが重要となる。

- ハッシュアルゴリズム
- ソルト利用
- 試行回数制限
- パスワード変更手順
- 侵害検知時の対応

第 7 条（認証器登録）

本条は、利用者へ認証器を登録する際の要件を定める。認証器登録は、認証システム全体の安全性を左右する重要な工程である。特に、攻撃者が自身の認証器を他人のアカウントへ登録できてしまうと、その後の認証をすべて突破できる危険がある。そのため、登録時には利用者本人確認を行い、安全な通信経路を用いて登録処理を実施する必要がある。リモート登録では、一時コードや確認リンクを利用することが一般的である。この際、確認コードは短時間のみ有効とし、十分なランダム性を持たせる必要がある。大学では、学認 IdP と Authenticator アプリを組み合わせた登録運用が典型例となる。

第 8 条（認証器結合）

本条は、認証器と利用者アカウントを安全に結合するための要件を定める。ここでいう「結合（Binding）」とは、「この認証器はこの利用者のものである」とシステムが認識する処理を意味する。Binding 時に本人確認が不十分である場合、第三者が自身の認証器を登録してしまうリスクがある。そのため、Binding では以下が重要となる。

・本人確認
・保護された通信
・認証済みセッション
・登録ログ

また、Binding 完了前に利用者情報を表示してはならない。これは情報漏洩防止のためである。

第 9 条（認証器失効）

本条は、認証器が危殆化した場合の失効処理を定める。「危殆化」とは、盗難、紛失、複製、漏洩等により、認証器の安全性が失われた状態を指す。例えばスマートフォン紛失時には、Authenticator アプリが不正利用される危険があるため、速やかな失効が必要となる。失効処理では、以下が重要となる。

- 利用者への通知
- 即時無効化
- ログ保存
- 代替認証手段

「利用者がどのように失効申請を行うか」等も重要なポイントである。

第 10 条（認証器回復）

本条は、認証器紛失時等における回復手続きを定める。認証器回復は、攻撃者に狙われやすい工程である。もし回復手続きが弱い場合、正規利用者の認証器を失効させた上で、攻撃者自身の認証器を登録できてしまう。そのため、回復時には元の保証レベルと同等以上の確認を行う必要がある。例えば以下のような方法が利用される。

- 対面確認
- 既存認証器確認
- 別チャネル確認
- ヘルプデスク本人確認

また、回復処理の記録は長期間保存し、後から追跡可能である必要がある。

第 11 条（セッション管理）

本条は、認証後のセッションをどのように管理するかを定める。セッション管理は、認証後の安全性を維持するために重要である。認証が安全でも、セッション管理が不十分であれば、セッション乗っ取り等の攻撃が成立してしまう。特に重要なのは以下である。

- セッションタイムアウト
- セッションキー保護
- Cookie 属性
- セッション固定化対策

また、長時間放置された端末からの不正利用を防止するため、一定時間経過後には再認証を要求する必要がある。

第 12 条（再認証）

本条は、一定時間経過後に利用者へ再認証を要求する要件を定める。AAL2 では、30 分非アクティブ、または 12 時間経過時に再認証を要求することが推奨されている。これは、共有端末や放置端末からの不正利用を防止するためである。また、RP（サービス提供側）から再認証要求が来た場合、新しい認証セッションを開始する必要がある。再認証では、単なる Cookie 確認ではなく、実際の認証要素入力を伴うことが重要となる。

第 13 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。AAL2 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。