2021-12-07

学認次世代認証連携検討作業部会
佐藤周行

AAL2 の新学認での運用に当たっての見解（案）

この文書は、別文書「IAL2 の新学認での運用に当たって（案)」に引き続き、AAL2 の新学認での運用にあたっての方針を定めるものである。**統制対象は IdP である。**

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受け、具体的に NIST SP800-63 と Kantara KIAF1440 に従って、新学認において AAL2 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. AAL2 運用の基本方針
2. 個々の認証器評価に際しての認証器レジストリの構築
3. パスワード運用の統制
4. 認証器の運用の統制（スマートフォンのロック解除の解釈と生体情報の利用についての方針を含む）
5. 認証器のライフサイクルの統制
6. CSP 運用の統制と利用者の統制の関係
7. AAL2 運用の一般的な条項

1. AAL2 運用の基本方針

AAL2 運用/認定に当たっては、KIAF1440 では、認証器に次の要求要件を定めている。「多要素認証器一個またはパスワード認証に所持要素に基づく認証器を組み合わせたもの」

現在、様々なベンダーから多様な認証器が発表されている。認証器のセキュリティの観点からの評価には、FIPS140-1 のように、各種認定を取得するもの、たとえば FIDO のようにコンソーシアムで保証するもの、デファクト標準を取って、採用側が考慮せざるを得ない状況にする戦略を取るものなどが存在する。運用パラメタを含めてこれらの運用をいちいち評価するのは難しいし、業界標準を満たしているものを再度評価することは屋上屋を架すことになる。

そこで、技術的には業界標準を含む外部認定を積極的に参照することにし、運用上の問題に注力するのが効率的である。運用上の問題は、認証器と利用者の初期結合、失効を含むラ

イフサイクル管理、CSP 運用に属するセッション管理を含む。また、AAL2 でも重要な意味を持つパスワード認証の統制についても定めることが重要である。

2. 個々の認証器評価に際しての認証器レジストリの構築

AAL2 に使えるものは「多要素認証器 1 個またはパスワード認証に所持要素に基づく認証器を組み合わせたもの」である。世間的には多くの認証器が発表・運用されている。これらの認証器採用の認定を参加機関ごとに行うことは合理的ではない。そこで、代表的な認証器に対してあらかじめ調査・認定を行っておくことが望ましい。もしくは参加機関の要求によって認証器の認定を行うとき、その結果を他機関にも適用する枠組を構築しておくべきである。

学認認証器レジストリ：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する。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、他機関の認定に使用することができる。

認定は KIAF1440 の該当する技術基準に従って行うことが適当である。

認証器レジストリへの登録の際、当該認証器がすでに外部機関、信頼できるコンソーシアムなどから認定を受けている場合、その外部の認定を流用することによって認定のスピードを上げることができる（ので、積極的に利用すべきである）。

認証器の強度は、ハードウェア・ソフトウェアの性能の他に運用パラメタ、初期結合、失効を含めたライフサイクル管理に依存する。レジストリに登録するのはハードウェア・ソフトウェアの性能を評価した結果のみにとどめ、残りは認定を要求する機関ごとに評価することが求められる。以下の規程は学認に対する要件であり、認定を要求する参加機関の要件ではないので、他の規程とは別に扱う。

規程 0.1 AAL2 相当の認証に用いることができると学認が認定した単要素認証器又は単要素認証器は、学認認証器レジストリに登録した上で、参加機関の AAL2 認定に利用する。
注）情報提供、認定協力を要請する候補をあげる。MS, Google, FIDO Consortium。 IDaaS が提供している多要素認証については、規程 3.x 群の認定込みで協力を要請する必要がある。

KIAF で現在認定対象になっているパスワード以外の認証器を列挙する。
Look-Up secret/帯域外認証器/公衆回線を用いた認証/単要素 OneTimePassword/多要素 OneTimePassword/単要素暗号ソフトウェア（Authenticator、鍵ペア等）/単要素暗号装置/多要素暗号ソフトウェア/多要素暗号装置（IC カードに格納した鍵ペア等）/

別文書で KIAF に準拠した認証器の登録項目の例をあげる。

3. パスワード運用の統制

AAL2 を単要素認証器 2 個の組み合わせによって実現するときに、パスワードは採用を義務付けられている認証器である。パスワードの統制は必須である。よって、特に規程を設ける。以下の規程は KIAF1440 に準拠する。

規程 1.1 パスワードを認証器として用いる時は以下を満たさなければならない。

a. パスワードの要件：

利用者が設定する場合は 8 文字以上、システムがランダムに設定する場合は 6 文字以上でなければならない。システムがブラックリスト等への登録等、設定を禁止しているパスワードが設定されるようになっていてはならない。

b. パスワード検証側の要件：

以下を認定基準とする。

1. 設定されたパスワードを truncate なしに検証すること
2. システムがランダムに設定する場合はランダム性の要件を充たしていること
3. パスワード入力に際してヒントを与えないこと
4. 不適切と定めたパスワードを登録させないこと。拒否の場合は理由を提示すること
5. スロットリングを実装すること
6. パスワードが突破されたと判断した場合はパスワード変更を強制できること
7. パスワードを格納する場合は、ハッシュ化、ソルトについて「適切に」暗号学的な処理がなされていること。

本文書の基本になる KIAF1440（及び NIST SP800-63）では、個人識別情報（PII）を扱う際にはパスワードのみの認証を禁止している。つまり、重要な情報は多要素認証で守るという姿勢を明確にしている。したがって、パスワード認証単独に要求する強度は必ずしも高いとは言えない。この姿勢を正しく理解し、日本でパスワード認証のみを使っている機関が多くあること、そこで PII を含む情報を処理していることが行われていることを考えれば、ここで定める基準が参加機関でより強力なパスワードポリシーを定めることの妨げになってはならない。

注）例えば、総務省では以下でパスワードの一般的なポリシーを提示している。
https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/staff/01.html

この基準は上記(b).4 を評価するときに具体的な基準として使うことができる。

4. 認証器の運用の統制（スマートフォンのロック解除の解釈と生体情報の利用についての方針を含む）

現在、多要素認証を行う場合に有力な装置の一つになっているスマートフォンの利用者側での運用の統制を含む規程を定める。

規程 2.1 CSP は、認証器を格納した装置が盗難、紛失にあった場合の対処方法についてあらかじめ指示を出し、さらに実際に起こった場合、認証器の取消、停止についての手続きを文書化しなければならない。
規程 2.2 CSP は、オンライン推測攻撃からの防御方法を定めなければならない。認証器に特に機構がない場合、連続した認証失敗回数を 100 回以下に制限しなければならない。

以下、認証プロセス中、検証者との通信についての規程。
規程 2.3 CSP が認証検証結果に署名する場合は、NIST SP800-131A に定めるもの以上の強度を持つ電子署名を使わなければならない。
規程 2.4 CSP と検証者が独立している場合、その間の通信は承認された暗号を用いた相互に認証した通信経路を通じて行わなければならない。
規程 2.5 検証者の鍵を CSP が使用する場合、その鍵は承認された暗号またはハッシュ関数を用い、NIST SP800-131A に定めるもの以上の強度を持たなければならない。

加えて、スマートフォンなどで典型的なロック解除のための PIN や生体認証を認証要素として考慮してはならないことを定める。検証側でロック解除がなされたかどうかの確認ができないからである。

規程 2.6 認証の一部に物理装置を利用する場合、その装置のロック解除の要素、特にそのための PIN や生体情報は認証要素としてはならない。

NIST や KIAF の定める生体情報の認証についての利用については一定の制限を設けている。具体的には、生体情報の利用は多要素認証の一部として利用することのみを認め、単要素認証の組み合わせの要素の一つとしては認めていない。それでも生体情報を利用する多要素認証が一般的となっている（例えば FIDO の生体情報登録・利用）ことを考え、これを採用する場合は、適当な技術水準に従うことの証明を求めるべきである。「適当な技術水準」は NIST や KIAF でも米水準が参照されているが、日本でそれと同等以上の水準が定められればそれに従うべきである。現状では、生体情報を認証に利用するときは多要素認証器の一

部としてのみ認められていることから、**規程 0.1** で定める認証器レジストリ中の認証器の認定の中で、各認証器のレジストリ項目の一部として扱うのが適当である。

5. 認証器のライフサイクルの統制

認証器は、利用者への配布から更新、失効まで管理（ライフサイクル管理）を必要とする。この部分についての規程を定める。IdP の運用を評価、認定する。

規程 3.1（認証器の利用者への結合）CSP は、利用者登録時に利用者に認証器を配布するか、又は利用者が提示した認証器のうち、CSP が認めたものを登録しなければならない。
2 利用者登録時に行う場合、身元確認を正常に実行した後、利用者の所持する認証器とパスワード又は最低 1 個の生体情報をオンラインで結合できる。その際に、CSP は、認証器が AAL2 以上であることを確認しなければならない。また、AAL2 の認証が完了しないうちに個人情報を利用者に開示してはならない。
3　利用者登録と結合が 1 回の物理的または保護された電子的なセッションで完了しない場合、CSP は、その後のプロセスで、申請者の同一性を確認するために以下を行わなければならない。
a. リモートで行う場合、事前に確立された電話番号、電子メール 又は 郵送先に対して秘密情報を発行して確認する。この時、保護されたセッション内でのみ認証器に秘密情報を発行できる。
b. 対面の場合、上記 a. と同じ秘密情報 又は 前回以前で記録された生体情報を用いて確認する。この利用は 1 回だけとする。この時、認証器に秘密情報を発行するのは、その認証器が対面で発行されるか、又は申請者の住所を確認できる方法で配布されたときだけとする。
4 利用者に対して新たな認証器を結合する場合、又は利用者が提示した認証器に新たに認証器を登録する場合、CSP は、まず利用者を AAL2 で認証しなければならない。
5 多要素認証器の場合、登録者が、多要素認証を完了する前にひとつの認証要素のすべての認証器を失ったとき、その代替手段として次を提供しなければならない
a. 登録者に自身で身元確認を、本文書の IAL 対応文書の基準に従って実施することを要求する
b. CSP が、登録者の登録に当たっての証拠を保持している場合、残りの認証要素が利用可能であれば、それを用いて既存のアカウントに認証することを要求しなければならない
c. CSP が、2 個の物理的な認証器を用いてパスワードを本人に結合して身元確認を再度行う場合、秘密情報として確認コードを発行する。発行されるコードは、承認された乱数発生器を用いて最低 6 文字以上の文字数字列でなければならない。コードの有効期限は、本人の登録住所に郵送する場合は 7 日、それ以外は 10 分とする。

注）スマートフォンや PC 上の各種 Authenticator では、自己申告でスマートフォンとの紐づけが一般的になっている。この運用の統制のために、一度紐づけた状態にして、後で IdP 側が検証するプロセスを定め、そのリスク評価をする必要がある。さらに、一部の Authenticator ではキーの利用者による複製を許容するものがあるので、その統制（禁止）の担保の仕方が問題になる。

規程 3.2（認証器の利用者への結合）CSP は、定められた記録保持期間の間、認証器のライフサイクルの期間中、アカウントに結合された認証器の記録、及びその保守に関して重要な事項のすべてを保存しなければならない。

規程 3.3（認証器の利用者への結合）CSP は、必要に応じて、利用承認証のスロットリングの情報を保守しなければならない。

規程 3.4（認証器の利用者への結合）CSP は、利用可能な利用者提供認証器の種類を決定し、検証者の AAL2 の判断のためにその情報を提供しなければならない。

規程 3.5（認証器の利用者への結合）CSP は、定められた記録保持期間の間、認証器のライフサイクルの期間中、アカウントに結合された認証器の記録、及びその保守記録を保存しなければならない。

注）3.2—3.5 は関連するログの保存に関係する規程である。

規程 3.6（認証器の利用者への結合）CSP は、利用者に新しい認証器を結合する際に、結合するプロトコルと鍵を提供するプロトコルのセキュリティレベルを確認しなければならない。

規程 3.7（認証器の利用者への結合）多要素認証器を結合する場合は、身元確認終了後、または多要素認証がすでに完了した後でなければならない。

規程 3.8（紛失、盗難、損壊、無許可複製）CSP がバックアップ又は代替認証器を用いて対象を認証する方法を用意している場合、その方法はパスワード又は所持認証器に限る。

2　CSP が、認証器の危殆化が報告された時に一時停止を用意している場合、利用者が他のより強力な方法で認証でき、さらに一時停止した認証器の再アクティベーションを要求した場合、一時停止からの復帰を実施しなければならない。

注）「無許可複製」の禁止はこの部分ではなく、各認証器の認定（規程 0.1）で規定すべきであるというのが NIST や KIAF の立場である。実際の運用を考えると、特にソフトトークンでは何らかの運用的な統制を定める必要があるかもしれない。

規程 3.9（失効）認証器の期限が切れた場合、CSP はその期限切れの認証器を用いた認証要求を受理してはならない。

2 認証器の期限が切れた場合、利用者が新しい認証器を受領後 又は 失効、終了の通知受領後、実務上速やかに、CSP は、利用者に物理認証器（CSP が署名した属性証明書を含む）を引き渡すか破壊を証明するように要求しなければならない。

規程 3.10 CSP は、以下のいずれかの場合が生じた時、速やかにアカウントと認証器の結合を失効し、利用者に通知しなければならない。

a. アカウントが存在しなくなった
b. 利用者が失効を要求した
c. CSP が利用者が資格要件を満たさなくなったと決定した
d. CSP が法的手段としてそれを実行する義務を負った

2 認証器が失効した場合、失効、終了の発生後実務上速やかに、CSP は、利用者に物理認証器（CSP が署名した属性証明書を含む）を引き渡すか破壊を証明するように要求しなければならない。

6. CSP 運用の統制と利用者の統制の関係

再認証に関する規程を定める。

規程 4.1 CSP は、利用者の非アクティブな状態が 30 分に達したとき、又は状態に関係なく最後に成功した認証から 12 時間に達したときに再認証を要求し、それが成功しない場合、セッションを終了させなければならない。

規程 4.2 CSP は、RP から再認証の要求が来たときはそれに応じ、新しいセッションを開始しなければならない。

注) AAL2 を要求する RP は、セッションの非アクティブ期間が 30 分に達したとき、また、アクティビティに関係なく最後に成功した認証から 12 時間後には再認証を要求するであろう。

規程 4.3 CSP は、セッションの終了を超えてセッションのキーを延長してはならない。

規程 4.4 非アクティブという理由でセッションが終了する場合、CSP は利用者に対してパスワード又は生体情報の入力を要求しなければならない。

7. AAL2 運用の一般的な条項

一般的なセキュリティとプライバシー保護に関する規程について定める。

規程 5.1 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。セキュリティ対策は、たとえば ISMAP やそのもととなった FedRAMP の中程度のレベルであること。

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。なお、これは IAL2 の規程 1.12 と同じ趣旨である。

規程 5.2 CSP は、各種法令の要求を満たすように各種データの保存について定め、あらかじめ利用者に公表すること。
規程 5.3 CSP は、個人情報保護に関する法令や規則、さらに各種技術基準に従った運用を行うこと。
規程 5.4 CSP は、利用者の個人情報を認証、認証に関する不正軽減、関連法令遵守の目的以外で用いる時は、明確な利用者同意を得ること。
2. 上記に不同意の利用者に不利益を与えてはならない。