NIST SP800シリーズ
NIST SP 800-63Bsup1

同期可能な認証器の NIST SP 800-63Bへの対応について

デジタルアイデンティティガイドライン: 認証とライフサイクル管理

Ryan Galluzzo
Andrew Regenscheid
David Temoshok
Connie LaSalle

本文書は以下のサイトから無料でダウンロードできます:
https://doi.org/10.6028/NIST.SP.800-63Bsup1

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST SP800シリーズ

NIST SP 800-63Bsup1

同期可能な認証器の NIST SP 800-63Bへの対応について

デジタルアイデンティティガイドライン: 認証とライフサイクル管理

Ryan Galluzzo
David Temoshok
Connie LaSalle
Applied Cybersecurity Division
Information Technology Laboratory

Andrew Regenscheid
Computer Security Division
Information Technology Laboratory

本文書は以下のサイトから無料でダウンロードできます:
https://doi.org/10.6028/NIST.SP.800-63Bsup1

2024年4月

米国国務省長官
Gina M. Raimondo

米国国立標準技術研究所(NIST)所長兼、標準技術商務次官
Laurie E. Locascio

本文書では、実験手順を適切に示す目的で、商用または非商用に関わらず、特定の機器、装置、ソフトウェア、または素材を例示しているが、そのような特定の記載は、NISTがいかなる製品やサービスをも推奨または承認していることを意味するものではなく、また、例示された素材や機器が必ずしもその目的に対して最適なものであることを意味するものでもない。

本文書では、NISTが法定責任に基づいて現在策定中の他の発行物に言及している場合がある。概念や方法論を含む本文書の内容は、そのような関連発行物の完成前であっても、連邦政府機関によって使用される可能性がある。従って、各発行物の完成までは、現行の要求事項、ガイドライン、手順が存在する場合には、それらを有効なものとする。計画や移行の観点から、連邦政府機関では、NISTによるこれらの新しい発行物の動向を詳細に確認することが望まれる。

各組織には、パブリックコメント期間中にすべての発行物のドラフトを検討し、NISTにフィードバックを行うことが望まれる。上記以外のNISTによるサイバーセキュリティに関する発行物の多くは、以下のウェブサイトで公開している。
https://csrc.nist.gov/publications

権限

本文書は、2014年施行の米国連邦政府情報セキュリティ近代化法（FISMA: Federal Information Security Modernization Act of 2014、44 U.S.C. § 3551 et seq.）、公法（P.L.）113-283に基づき、NISTがその法定責任において作成したものである。NISTは、連邦情報システムに対する最低限の要求事項を含む情報セキュリティ標準およびガイドラインを策定する責任を負うが、このような標準およびガイドラインは、そのようなシステムに関する政策権限を持つ適切な連邦政府当局者の明示的な承認がない限り、国家安全保障にかかわるシステムには適用されない。本ガイドラインは、行政管理予算局の通達A-130（OMB: Office of Management and Budget, Circular A-130）の要求事項と一致するものである。

本文書のいかなる内容も、法定権限に基づき商務長官が連邦政府機関に義務付け、拘束力を持たせた標準やガイドラインと矛盾するものであってはならない。また、本ガイドラインは、商務長官、OMB長官、その他の連邦政府当局者の既存の権限を変更したり、取って代わったりするものと解釈されるべきではない。本文書は、非政府組織が任意で使用することができ、また、米国において著作権の対象とはならない。ただし、NISTへの帰属表示を推奨する。

NISTテクニカルシリーズポリシー
Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

発行履歴
2024-04-11、NIST編集審査委員会により承認。

NISTテクニカルシリーズ刊行物の引用方法
Galluzzo R, Temoshok D, LaSalle C, Regenscheid A (2024) Incorporating Syncable Authenticators Into NIST SP 80063B: Digital Identity Guidelines — Authentication and Lifecycle Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-63Bsup1. https://doi.org/10.6028/NIST.SP.800-63Bsup1

著者**ORCID iDs**
Ryan Galluzzo: 0000-0003-0304-4239
Andrew Regenscheid: 0000-0002-3930-527X
David Temoshok: 0000-0001-6195-0331
Connie LaSalle: 0000-0001-6031-7550

問い合わせ先
dig-comments@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

追加情報
関連コンテンツ、今後の更新、発行履歴など、本書に関する追加情報は <CSRC link>で公開する。

すべてのコメントは情報公開法（**Freedom of Information Act: FOIA**）に基づき公開される。

概要

本文書は、NIST Special Publication 800-63B『デジタルアイデンティティガイドライン：認証とライフスタイル管理』の補足資料であり、デバイス間で同期できる認証器の使用に関するガイダンスを各機関に対して補足的に提供するものである。

キーワード

認証（authentication）; 認証保証（authentication assurance）; デジタル認証（digital authentication）; デジタル資格情報（digital credentials）; デジタルアイデンティティ（digital identity）; 電子認証（electronic authentication）; 電子資格情報（electronic credentials）; パスキー（passkey）; 同期可能な認証器（syncable authenticator）.

コンピュータシステムの技術に関する報告書

米国国立標準技術研究所（NIST: National Institute of Standards and Technology）の情報技術ラボラトリ（ITL: Information Technology Laboratory）は、米国における測定および標準に関する基盤について技術的リーダーシップを担うことで、米国の経済と公共福祉に貢献している。ITLでは、テストの開発、テスト技法の開発、参照データの作成、概念実証の実施および技術的分析を通じて、情報技術の開発と生産的利用を促進している。ITLの責務には、連邦政府の情報システムにおける国家安全保障に関わるもの以外の情報に対して、費用対効果の高いセキュリティとプライバシーを確保するための、管理面、運用面、技術面および物理面での標準およびガイドラインを策定することが含まれる。本 SP (Special Publication)800 シリーズでは、情報システムセキュリティに関する ITLの調査、ガイドラインおよびアウトリーチ活動、ならびに業界団体、政府機関および学術機関との連携について報告する。

読者への注記

本文書は、NIST Special Publication (SP) 800-63B『デジタルアイデンティティガイドライン：認証とライフスタイル管理』の補足資料である。同ガイドラインに記載された認証技法に、複製された認証器（同期可能な認証器またはパスキーとして知られる）の使用を組み込んだものである。本文書の公開時点で、NISTではSP800-63の改訂版を作成中である。この改訂版SPは、最終報告書として公開された時点で本補足資料を置き換えるものとなる。本文書に対するコメントは、2024年中期に実施されるSP 800-63-4の第2回パブリックコメント期間中に提出のこと。

目次

表リスト

1. はじめに

『NIST デジタルアイデンティティガイドライン』[1]は、身元確認、認証およびフェデレーションを含むデジタルアイデンティティに関する手順と技術的な要求事項を規定したものである。NIST Special Publication (SP) 800-63B（SP800-63-3付属の分冊B）は、認証とライフサイクル管理に関わる要求事項について特に対応したものであり、使用可能な認証器の種類ごとに具体的な要求事項を含めたものである [2] 。第3改訂版は、同ガイドラインの最新の大幅な改訂版であり、2017年6月に発行された。現在シリーズ全体の更新が進められており、第4改訂版をもって完結する予定であるが、技術の進歩は NISTの典型的な文書作成や改定の手順よりも早いため、このような更新によって補足するものである。

SP 800-63Bで扱われる認証器の種類の1つに、多要素暗号認証器がある。通常、この認証タイプでは、ハードウェアまたはソフトウェアで暗号鍵を保護し、第2の認証要素（（パスワードなど）記憶する秘密情報または生体情報上の特徴）による有効化を必要とする。秘密鍵を不正な開示から保護することは、多要素暗号認証のセキュリティモデルの基本である。これには従来、秘密鍵がエクスポートや複製されないようにすることが含まれた。しかし、このパラダイムが変わり始めている。特に、一連の新しい認証プロトコルと仕様により、同期可能な認証器（一般に「パスキー（passkeys）」と呼ばれる）が急速に採用されるようになり、ユーザが異なるデバイス間で秘密鍵を同期（すなわち、複製）できるようになった。

2017年のSP800-63-3の発行時には、『Fast Identity Online [FIDO] Client to Authenticator Protocol [CTAP]』 [3] および、W3Cによる『Web Authentication』 [4] （併用される場合には FIDO2として知られる）の2つの重要なサポート仕様は存在せず、また、実装に関して頑健かつよく知られたエコシステムも存在しなかった。

当時利用可能だった暗号認証器のタイプに基づき、2017年のガイドラインでは、多要素暗号認証器が鍵を他のデバイスに「クローン（複製）」する能力を制限していた。しかし、過去2年間でエコシステムは急速に発展し、現在ではほとんどの主要なプラットフォームプロバイダが、スケーラブルで同期可能な認証機能を実装するようになった。これらの認証器は、耐フィッシング性へのサポート[1]、特定のリライングパーティに限定する機能、パスワード送信の必要性の排除、認証器のリカバリの簡素化、保存された秘密鍵に付随する第2要素としての様々なデバイス固有の生体情報およびPINの使用など、多くの利点を提供している。また、ますます拡大するマルチデバイス・マルチプラットフォームの世界に対応した利便性も提供している。

あらゆる新技術にいえることであるが、技術革新は、新たな脅威と課題を伴うものであり、それらを調査し理解する必要がある。そのため、本補足資料では、連邦政府機関が同期可能な認証器を導入するかどうか、またどのように導入するかを決定する際に考慮すべき事項について、最新の脅威も含めて概説する。

[1] 認証器は、その出力情報を通信経路（例. クライアント認証TLS）または検証者名（例. FIDO2/WebAuthN）にバインドする暗号認証器であれば、フィッシングへの耐性がある。どちらの技術も、認証器の出力情報が意図したコンテキスト以外で使用されることを防ぐ。フィッシング耐性については、SP 800-63B-4およびOMB Memorandum 22-09『Zero Trust Implementation Strategy』 を参照のこと。

2. 目的

本文書の目的は、変化し続ける認証・クレデンシャル市場を反映するために、現行のNISTガイドラインを更新することである。本補足資料では、同期可能な認証器がSP800-63-3で定められた認証保証レベル（Authentication Assurance Levels）と整合する方法で脅威を軽減する方法について示し、SP800-63-3認証保証レベル2（Authentication Assurance Level 2: AAL2）を実現するために利用できる同期可能な認証器の機能についての理解を連邦政府機関に提供する。また、SP800-63B[2]の.5.1.8で検討されたソフトウェア暗号認証器の使用に関する最新情報、特に、鍵が別のデバイスに複製（「クローン」または「同期」など）された場合でも、このような認証器がAAL2の認証要件をサポートできることについても示す。最後に、本文書では、2つのユースケース、すなわち、一般向けアプリケーション（OMB Memorandum M-19-17記載の、公衆向けアイデンティティと連携する連邦情報システム）、および連邦政府業務用アプリケーション（OMB Memorandum M19-17記載の、主に連邦政府業務用アイデンティティと連携する連邦情報システム）に基づいた実装に関する考慮事項について示す。本文書は、SP800-63-3記載の既存のガイダンスを補足するものであり、最終版SP800-63B-4によって置き換えられる予定である。

3. 同期可能な認証器の**AAL2**の要件達成

NISTの認証器保証レベルは、認証器が認証プロセスにおける特定の脅威から保護する機能を中心に設定されたものである。AAL2では、ユーザが単一要素認証器を2つ、またはユーザのアカウントに紐付けられた多要素認証器を1つ有しているという高い信頼性を提供することが意図されている。表1に、SP800-63-3[1]で要求される脅威に対する軽減策と、適切に実装された同期可能な認証器がどのようにこれらの脅威から保護することができるかを示す。

表**1**. **SP800-63-3**（表 **4-1**）**[1]**記載の脅威に対する軽減策の要件

要件	AAL2	同期可能な認証器（パスキーなど）
中間者攻撃への耐性	必須	要件達成。適切に実装された同期可能な認証器では、認証に使うすべてのデータが認証済みかつ保護された経路でやり取りされる。
検証者なりすましへの耐性	非必須	要件達成。適切に実装された同期可能な認証器は、一意の公開・秘密鍵のペアを生成し、生成されたドメインのみで使えるように制限する（すなわち、鍵は特定のウェブサイトまたはリライングパーティのみで使用可）。これにより、偽のウェブサイトなどが認証器からの出力情報を窃取して再利用することを防ぐ。
検証者侵害への耐性	非必須	要件達成。適切に実装された同期可能な認証器では、検証者側には公開鍵のみが保管される。これらの公開鍵はユーザとしての認証には使えない。同期ファブリックに保管される秘密鍵は認定された暗号方法で暗号化された上でのみ保管される。認証されたユーザのみが保管された鍵にアクセスできるようにアクセス管理がなされている。
リプレイ攻撃への耐性	必須	要件達成。同期可能な認証器は、認証処理の都度、ランダムなナンスを使用することで、リプレイ攻撃を防ぐ（すなわち、将来の認証処理で再利用されることを防ぐ）。
認証の意思確認	推奨	要件達成。同期可能な認証器は、ユーザが暗号化された認証プロトコルを開始するにあたり、有効化シークレットの入力を要求する。これにより認証の意思が確認され、ユーザが主体的に参加しない限り認証が進められないようになっている。

第5節（Section 5）では、同期可能な認証器の実装に関する追加的な考慮事項について検討している。

AAL2の要求事項を満たすには、同期可能な認証器は、ローカル認証を利用してローカルに保管された鍵のロック解除をするか、ローカル認証の仕組みが利用できない場合には、別の認証器（ユーザが選択したパスワードなど）を利用しなければならない（SHALL）。FIDO2 Web Authentication (WebAuthn)のコンテキストでは、W3C Web Authentication仕様の認証器データで利用可能なユーザ検証フラグの値によって示される。FIDO2 WebAuthn 認証器データフラグの詳細については第5節を参照のこと。

4. 認証鍵の複製の許可に関する更新

SP 800-63Bの 5.1.8.1「多要素暗号ソフトウェア認証器」では、認証器があるデバイスから別のデバイスに暗号化された認証鍵を「クローン（複製）」することを制限している。具体的には、以下の記載の通り。

> 多要素暗号ソフトウェア認証器は、複数のデバイスへの秘密鍵のクローン作成を抑制すべき（SHOULD）であり、また容易化する機能を提供してはならない（SHALL NOT）。

同期可能な認証器では、明示的に鍵の複製を促進し、デバイスや異なるプラットフォームプロバイダ間で、過去に登録された認証器へのアクセスをユーザに提供する。これは、適切に行われれば、安全かつ便利な体験となるものであり、NISTは、SP 800-63B-4の当初のパブリックドラフト（ipd）からこの制約を削除することで、この事実を認めている。

本文書の発行時点で、5.1.8.1の上記の記述は本補足資料により置き換えられ、本補足資料に規定される要求事項に基づいて導入される同期可能な認証器は、AAL2で想定される脅威から保護するのに十分であるとみなされなければならない（SHALL）。

同期可能な認証器のすべての使用に関する一般要件：

- すべての鍵が認定された暗号技術を使用して生成されなければならない（**SHALL**）。
- デバイスからクローン（複製）またはエクスポートされた秘密鍵は暗号化された状態で保管しなければならない（**SHALL**）。
- すべての認証処理が、デバイス上で生成された、または同期ファブリック（クラウドストレージなど）から復元された暗号鍵を使用して、ローカルのデバイス上で秘密鍵の操作を実行しなければならない（**SHALL**）。
- クラウドベースのアカウントに保管されている秘密鍵は、認証されたユーザのみが同期ファブリック上で秘密鍵にアクセスできるようなアクセス管理のメカニズムで保護されなければならない（**SHALL**）。
- 同期ファブリック上の秘密鍵へのユーザによるアクセスは、同期された鍵を用いた認証プロトコルの完全性を確保するために、AAL2相当の多要素認証（MFA）によって保護されなければならない（**SHALL**）。
- これらの一般要件、および同期可能な認証器の使用に関するその他の機関ごとの要件は、それが該当する場合には、一般向けウェブサイト上およびデジタルサービスポリシーを含め、文書化かつ通知されなければならない（**SHALL**）。

同期可能な認証器の連邦政府業務[2]での使用に関する追加要件：

- 連邦政府業務用秘密鍵（federal key）は、FISMA（米国連邦政府情報セキュリティ管理法）の中程度または同等の保護を満たす同期ファブリックに保管しなければならない（**SHALL**）。

[2]これらの要求事項の目的上、連邦政府業務用システムおよび鍵には、政府請負業者、政府職員、およびミッションパートナーなど、PIVガイダンスの対象範囲とみなされるものが含まれる。政府対消費者または一般向けのユースケースは含まれない。

- 連邦政府業務用秘密鍵を生成、保管、同期する認証器を含むデバイス（携帯電話、ノートパソコン、タブレットなど）は、モバイル端末管理ソフトウェアまたはその他のデバイス設定管理を用いて、許可されていないデバイスや同期ファブリックへの鍵の同期や共有から保護しなければならない（**SHALL**）。
- 連邦政府業務用秘密鍵のライフサイクルを管理できるようにするために、同期ファブリックへのアクセスは、政府機関が管理するアカウント（一元的なアイデンティティアクセス管理ソリューションまたはプラットフォームベースの管理アカウントなど）によって管理しなければならない（**SHALL**）。
- 秘密鍵を生成する認証器は、認証器自体の機能や出自を検証するために使用できるアテステーション機能（enterprise attestationなど）を用意すべきである（**SHOULD**）。

これらの管理措置は、特に同期をサポートするものであり、FIPS 140の検証を含む、既存の多要素ソフトウェア暗号化認証要件やAAL2要件に付加的なものとみなされるべきである。

5. 実装上の考慮事項と要件

同期可能な認証器は、W3CのWebAuthn仕様に基づいて構築されており、共通のデータ構造、チャレンジレスポンス暗号プロトコル、および公開鍵認証情報を活用するためのAPIを提供している。この仕様は柔軟で適応性があるため、WebAuthn認証情報のすべての実装が連邦政府機関の実装要件を満たすとは限らない。

この仕様には一連の「フラグ」があり、リライングパーティ（RP）アプリケーションは、認証イベントがRPのアクセスポリシーに合致しているかどうかを判断するために、認証器に対して追加のコンテキストの提供を要求することができる。本節では、RPとして機能する連邦政府機関が、NISTのAAL2脅威軽減策に適合するように同期可能な認証器の実装を構築する際に理解し照会すべき、WebAuthn仕様の特定のフラグについて説明する。

表2. **WebAuthnレベル3フラグ**

フラグ	説明	要求事項および推奨
User Present (UP)	ユーザが認証器の操作をしたことを確認するための「存在」テストを示す（USBポートに挿入されたハードウェアトークンのタッピングなど）。	連邦政府機関は、「User Present」フラグが設定されていることを確認しなければならない（**SHALL**）。認証の意思確認をサポート。
User Verified (UV)	使用可能な「ユーザ検証」方法のいずれかを使用して、ユーザが認証器によってローカル認証されたことを示す。	連邦政府機関は、「UV」が優先されることを示さなければならず（**SHALL**）、かつ、「UV」フラグの値を確認するために、すべてのアサーションを検査しなければならない（**SHALL**）。これにより、認証器が多要素暗号認証器として扱えるかどうかが示される。ユーザが検証されない場合でも、機関は、認証イベントにRP固有の保存された秘密情報を追加することで、認証器を単要素暗号認証器として扱うことができる。WebAuthnレベル3仕様のさらなる拡張により、機関がローカル認証イベントのコンテキストを要求する場合、検証方法に関する追加データが提供される [4] 。
Backup Eligibility	認証器を別のデバイスに同期できるかどうか（すなわち、鍵を別の場所に保管できるかどうか）を示す。認証器が同期可能であっても、同期されたことを意味するわけではない点に留意のこと。	連邦政府機関が同期可能な認証器の使用を制限するポリシーを策定する場合には、このフラグを使用してもよい（**MAY**）。このフラグは、デバイスにバインドされる認証器と、複数のデバイスにクローン（複製）される可能性のある認証器とを区別するために必要。
Backup State	認証器が別のデバイスに同期されているかどうかを示す。	連邦政府機関が他のデバイスに同期された認証器について制限を設ける場合には、このフラグを使用してもよい（**MAY**）。一般向けアプリケーションの場合には、ユーザ体験上の懸念から、機関は、このフラグに基づいて承認を変更すべきではない（**SHOULD NOT**）。連邦政府業務に関する判断の場合には、特定のアプリケーションでの同期可能な認証器の制限をサポートするために、このフラグを使用してもよい（**MAY**）。

表2に示されるフラグに加えて、各機関は、実装や採用を決定した同期可能な認証器の出自と機能について、より詳細な情報を希望することができる。FIDO2のWebAuthnのコンテキストに

おいて、一部の認証器では、特定の認証器の機能や製造者を判断するために使用できるアテステーション機能をサポートしている。連邦政府業務におけるユースケースの場合には、機関は、プラットフォームプロバイダが提供する機能に基づいて、アテステーション機能を実装すべきである（**SHOULD**）。できれば、これは、RPが認証器に関する一意の識別情報を要求するエンタープライズ・アテステーション（enterprise attestation）の形式をとることが望ましい。

アテステーションは、広く一般向けのアプリケーションに対して使用すべきではない（**SHOULD NOT**）。このような要件（すなわち、アテステーションをサポートしていない場合に、一部の一般ユーザの同期可能な認証器をブロックするような要件）は、ショートメッセージサービス（SMS）のワンタイムパスワード（OTP）のような、フィッシングに対して脆弱な、より安全性の低い認証オプションにユーザを向かわせる可能性がある。

RPがフラグやアテステーション情報を要求する場合でも、認証器は要求された情報のすべてを返信しなかったり、あるいはリソースへのアクセスに必須の期待されるレスポンスと矛盾する情報を返信することがある。したがって、機関では、同期可能な認証器を使用するユースケースを評価し、かつ返信された情報に基づいて適切なアクセスポリシー上の判断を下すことが極めて重要である。

6. 同期可能な認証器への脅威と課題

同期可能な認証器には、実装や開発の前に各機関で評価すべき明確な脅威や課題がある。表3に、これらの脅威と推奨される対処方法の概要を示す。

表3. 同期可能な認証器への脅威、課題および対処方法

脅威や課題	説明	同期可能な認証器での対処方法
許可されていない鍵の利用または鍵の制御不能	同期可能な認証器の中には、鍵を悪用することができる他のユーザ所有のデバイスに秘密鍵を共有できる実装がある。	● 連邦政府業務のデバイス管理機能や管理プロファイルを強化することにより同期された鍵の共有を防止 ● 鍵の共有が発生した際には、すべての利用可能な通知経路を用いてユーザに通知 ● 鍵自体、鍵の状態、鍵が共有されたかどうか／どこで共有されたかなどを確認できる仕組みをユーザに提供 ● 既存の啓発・研修制度を利用し、許可されていない鍵の利用のリスクについてユーザに注意喚起
同期ファブリックの侵害	鍵を同期するために、ほとんどの実装が、アカウントと紐づく複数のデバイスに接続されたクラウドベースのサービスである「同期ファブリック」に鍵をクローン（複製）するようになっている。	● 暗号化されたキーマテリアルのみを保管 ● 認証されたユーザ以外が秘密鍵にアクセスできないように、同期ファブリックのアクセス管理を実装 ● クラウドサービスの基本的なセキュリティ機能を評価（FISMAの中程度または同等の保護） ● ハードウェアセキュリティモジュールを活用して暗号化された鍵を保護
同期ファブリックへの許可されていないアクセスとリカバリ	同期された鍵がクラウドベースのアカウントリカバリ手順でアクセス可能になっている。これらの手順は潜在的な弱点になりえる。	● NIST SP800-63Bに沿った認証リカバリ手順を実装 ● デバイス管理やアカウント管理機能を通して、連邦政府業務用鍵（federal enterprise keys）のリカバリ機能を制限 ● りカバリ用に、複数の認証器をAAL2以上でバインドする ● ユーザが同期ファブリックにアクセスする新しい認証器を追加する際には、AAL2認証を要件とする ● 連邦政府業務内での利用では、導出認証器としてのみ利用[6] ● いかなるリカバリの処理がなされた際にはユーザに通知 ● ユーザが管理する秘密情報（すなわち、同期ファブリックプロバイダの知らない情報）を利用して、鍵の暗号化と復号を実施
失効	同期可能な認証子はRPごとに固有の鍵を使用するため、それらの鍵に基づいてアクセスを一括して失効させることが困難。たとえば、従来のPKIでは、CRLを使用してアクセスを一括して失効させることができるが、同様の手順は、同期可能な認証器（ま	● ユーザが認証器を管理するための中央ID管理（IDM: Identity Management）アカウントを実装し、危殆化または失効した場合に、当該の認証器を「所属機関」アカウントから削除する

	たは FIDO WebAuthnベースの認証器）では利用できない。	● SSOとフェデレーションを活用し、インシデント発生時に失効するRP固有の鍵の数を制限する ● 鍵の有効性と最新性をユーザに定期的に確認するよう求めるポリシーとツールを定める

7. 共有について

これまでセキュリティガイドラインでは、異なるユーザがそれぞれ独自の認証器を持つことを想定し、ユーザ間で認証器を共有しないよう注意喚起してきた。このガイダンスにも関わらず、一部のユーザグループやアプリケーションで認証器やパスワードの共有が行われ、個人間でデジタルアカウントへのアクセスが共有されている。

表 3 に示したように、一部の同期可能な認証器の実装では、このようなユーザの行動を 受け入れ、異なるユーザ間で認証鍵を共有する方法を確立している。さらに、一部の実装では、一般的なサービスにおいて、パスワード共有に代わる便利でより安全な方法として、同期可能な認証器の共有を積極的に奨励している。

連邦政府業務でのユースケースの場合には、許可されたデバ イスや同期ファブリックからの鍵の移動を制限するデバイス管理技術を使用することで、鍵の共有に関する懸念を効果的に緩和することができる。しかし、一般向けのユースケースでは、同様の緩和策は今のところ存在しないため、リライングパーティは同期可能な認証器プロバイダが採用する共有モデルに依存することになる。一般向けアプリケーションの所有者は、共有される認証器に関わるリスクを認識すべきである。一般利用者との通信では、ユーザがどの認証器を使用しているかについて機関が把握できる範囲は限られており、同期可能なすべての認証器が共有の対象となる可能性があることを想定すべきである。多くの共有モデルでリスクを最小化するための実質的な管理（共有を許可するためにデバイス間の近接を要求するなど）が行われている一方で、それほど厳密でない実装も存在する。

この新種の認証器がもたらす共有に関するリスクは特別なものではない。実際には、すべてのAAL2認証器のタイプに該当し、それらの中には同期可能な認証器より脆弱なものもある。いかなるAAL2認証であっても、それを共有しようとするユーザによって共有される可能性がある。ユーザは、パスワード、OTP、帯域外認証器、さらにはプッシュ認証イベントを積極的に共有したり、指定された者（正式か否かを問わず）がエンドユーザに代わって認証することを許可したりすることができる。

機関は、各自が直面している具体的なリスク、脅威、およびユーザビリティに関する考慮事項に基づいて、アプリケーションにどの認証器を採用するかを決定する。同期可能な認証器は、AAL2までの実装を求めるアプリケーションへの新たな選択肢として提供される可能性があり、他のすべての認証器と同様に、この技術におけるトレードオフは、セキュリティ、プライバシー、公平性、およびユーザビリティに対して期待される効果に基づいて、最適なバランスを取るべきである。

8. 結論

同期可能な認証器は、認証環境、特に多要素暗号認証器の使用において、大きな技術的転換をもたらした。その普及によって、暗号鍵の複製とクラウドインフラへの保管を許可することにともなうトレードオフの評価が避けられないものとなるだろう。これは明らかなリスク（認証鍵の連邦政府業務による管理が失われるなど）を伴うが、便利でフィッシング耐性のある認証への道筋を示し、一般や連邦政府業務に対する主な脅威要因を排除するものでもある。同期可能な認証器は、すべてのユースケースに適しているわけではない。しかし、本補足資料に記載されたガイドラインに従って実装された場合には、AAL2リスク対策と一致する形で、フィッシング耐性のある認証器の採用をより広く促進することができるだろう。

本文書は、既存の『デジタルアイデンティティガイドライン』[1]に付随するものであり、各機関が情報に基づいたリスクベースの判断を下し、必要に応じて、業界の最新のイノベーションを取り入れることを可能にするために情報提供するものである。

参考文献

[1] Grassi PA, Garcia ME, Fenton JL (2017) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-63-3, Includes updates as of March 02, 2020. https://doi.org/10.6028/NIST.SP.800-63-3

[2] Grassi PA, Newton EM, Perlner RA, Regenscheid AR, Fenton JL, Burr WE, Richer JP, Lefkovitz NB, Danker JM, Choong Y-Y, Greene KK, Theofanos MF (2017) Digital Identity Guidelines: Authentication and Lifecycle Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-63B, Includes updates as of March 02, 2020. https://doi.org/10.6028/NIST.SP.800-63B

[3] Fast Identity Online Alliance (2023) Client to Authenticator Protocol 2.2. https://fidoalliance.org/specs/fido-v2.2-rd-20230321/fido-client-to-authenticatorprotocol-v2.2-rd-20230321.html

[4] World Wide Web Consortium (2021) Web Authentication: An API for Accessing Public Key Credentials Level 3. https://www.w3.org/TR/webauthn-3/

[5] Word Wide Web Consortium (2021) Web Authentication: An API for Accessing Public Key Credentials Level 3. Section 10.2 Authenticator Extensions. https://www.w3.org/TR/webauthn-3/#sctn-defined-authenticator-extensions

[6] Ferraiolo H, Regenscheid AR, Fenton J (2023) Guidelines for Derived Personal Identity Verification (PIV) Credentials. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-157r1 ipd (initial public draft). https://doi.org/10.6028/NIST.SP.800-157r1.ipd

付録**A**：用語集

本補足資料で新たに追加された用語を以下に示す。使用された他のすべての用語は、SP800-63-3の用語集に準拠している。https://doi.org/10.6028/NIST.SP.800-63-3.

同期可能な認証器（**syncable authenticators**）
ソフトウェアまたはハードウェアの暗号認証器で、認証鍵をクローン（複製）し、他のストレージにエクスポートして、それらの鍵を他の認証器（すなわちデバイス）に同期させることができるようにするもの。

同期ファブリック（**sync fabric**）
ユーザのデバイスにローカルでない、同期可能な認証器によって生成された認証鍵を保管、伝送、管理するために使用されるオンプレミス、クラウドベース、またはハイブリッドのサービス。