NISTスペシャル・パブリケーション800
NIST SP 800-63Bsup1

Syncable 認証機能の組み込み

NIST SP 800-63Bへ

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

マネジメント

ライアン・
ガルッツォ アンド
リュー・レーゲン
スシャイト デイビ
ッド・テモショク
コニー・ラサール

本書は https://doi.org/10.6028/NIST.SP.800-63Bsup1 より無料で入手可能。

NISTスペシャル・パブリケーション800

NIST SP 800-63Bsup1

NISTスペシャル・パブリケーション800

NIST SP 800-63Bsup1

Syncable 認証機能の組み込み

NIST SP 800-63Bへ

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

マネジメント

ライアン・

ガルッツォ デ

イビッド・テ

モショク コニ

ー・ラサール

応用サイバーセキュリティ

部 情報技術研究所

アンドリュー・レ

ーゲンスシャイト *コンピュ*

ータ・セキュリティ部 情報技術

研究所

本書は https://doi.org/10.6028/NIST.SP.800-63Bsup1 より無料で入手可能。

2024年4月

NISTスペシャル・パブリケーション800

NIST SP 800-63Bsup1

米国商務省
ジーナ・M・ライモンド 秘書

国立標準技術研究所
ローリー・E・ロカシオ、NIST理事兼標準技術担当商務次官

本論文では、実験手順を適切に特定するために、商用、非商用を問わず、特定の機器、装置、ソフトウェア、または材料を特定している。このような特定は、NISTによるいかなる製品またはサービスの推奨または保証を意味するものではなく、また特定された材料または装置が必ずしもその目的に対して利用可能な最良のものであることを意味するものでもありません。

本書には、NIST がその法定責任に従って現在開発中の他の出版物を参照している場合がある。概念や方法論を含む本書の情報は、そのような関連出版物の完成前であっても、連邦機関によって使用される可能性があります。
従って、各出版物が完成するまでは、現行の要求事項、ガイドライン、手順が存在する場合は、それらが引き続き有効である。計画と移行を目的として、連邦政府機関はNISTによるこれらの新しい出版物の開発を注意深く見守ることをお勧めします。

各組織は、パブリックコメント期間中にすべての出版物の草案を検討し、NIST にフィードバックを提供することが推奨される。上記以外の多くの NIST サイバーセキュリティ出版物は、
https://csrc.nist.gov/publications で入手できます。

権威

本書は、2014年連邦情報セキュリティ近代化法（FISMA）（44 U.S.C. § 3551 et seq.、公法（P.L.）113-283）に基づく法的責任に基づき、NISTが作成したものである。NISTは、連邦情報システムの最低要件を含む情報セキュリティ基準およびガイドラインを策定する責任を負うが、そのような基準およびガイドラインは、そのようなシステムに対する政策権限を行使する適切な連邦政府当局者の明示的な承認がない限り、国家安全保障システムに適用されないものとする。本ガイドラインは、行政管理予算局（OMB）サーキュラーA-130の要件と一致している。

本書のいかなる内容も、法的権限に基づき商務長官が連邦政府機関に義務付け、拘束力を持たせた基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、これに取って代わるものと解釈されるべきでもない。本書は、非政府組織が任意で使用することができ、米国における著作権の対象ではない。ただし、NISTは帰属を認める。

NISTテクニカルシリーズ方針

著作権、使用およびライセンスに関する声明
NIST技術シリーズ出版識別子の構文

出版履歴

2024-04-11、NIST編集審査委員会承認

このNISTテクニカルシリーズ出版物の引用方法

Galluzzo R, Temoshok D, LaSalle C, Regenscheid A (2024) Incorporating Syncable Authenticators Into NIST SP 800-

63B: 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

ライアン・ガルッツォ：0000-0003-0304-

4239 アンドリュー・レーゲンスシャイ

ト：0000-0002-3930-527X デイビッド・

テモショク：0000-0001-6195-0331
コニー・ラサール：0000-0001-6031-7550

連絡先

dig-comments@nist.gov

国立標準技術研究所

担当：情報技術研究所 応用サイバーセキュリティ部 100 Bureau Drive
(Mail Stop 2000) Gaithersburg, MD 20899-2000

追加情報

関連コンテンツ、更新の可能性、文書の履歴など、この出版物に関する追加情報は<CSRCリンク>で入手できる。

すべてのコメントは情報公開法（FOIA）に基づき公開される。

要旨

この付録は、NIST Special Publication 800-63B「*デジタル ID ガイドライン」である：認証およびライフサイクル管理」は*、デバイス間で同期される認証子の使用に関する追加ガイダ ンスを機関に提供する。

キーワード

認証、認証保証、デジタル認証、デジタル・クレデンシャル、デジタル ID、電子認証、電子クレデンシャル、パスキー、同期可能な認証子。

コンピュータ・システム技術レポート

国立標準技術研究所（NIST）の情報技術研究所（ITL）は、国家の測定および標準インフラストラクチャのための技術的リーダーシップを提供することにより、米国経済と公共の福祉を促進します。ITLは、試験、試験方法、参照データ、概念実証実装、技術分析を開発し、情報技術の開発と生産的利用を促進しています。ITLの責任には、連邦情報システムにおける国家安全保障関連情報以外のコスト効率の良いセキュリティとプライバシーのための管理、管理、技術、物理的な標準とガイドラインの開発が含まれる。Special Publication 800シリーズは、情報システム・セキュリティに関するITLの研究、ガイドライン、アウトリーチ活動、および産業界、政府機関、学術機関との協力活動について報告している。

読者の皆様へ

本文書は、NIST 特別刊行物（SP）800-63B「*デジタル ID ガイドライン」の*補足である：*認証およびライフサイクル管理」を補足するものである*。同ガイドラインに記載されている認証技法に、複製された認証子（*同期可能認証子*ま たはパスキーとして知られている）の使用を組み込んでいる。発行時点で、NIST は、SP 800-63 の改訂版を作成中である。最終報告書として発行された場合、SP はこの補足文書に優先する。本文書に対するコメントは、2024 年半ばに行われる SP 800-63-4 の第 2 回パブリック・コメン

ト期間に提出すること。

目次

テーブル一覧

1. はじめに

NIST デジタル ID ガイドライン［1］は、ID 証明、認証、およびフェデレーションを含む、デジタル ID のプロセスと技術要件を規定している。NIST 特別刊行物（SP）800-63B（SP 800-63-3 に関連する第 B 巻）は、認証およびライフサイクル管理 の要件に特に対応しており、許容可能な認証子の種類ごとに具体的な要件が含まれている[2]。シリーズ全体の更新が進行中であり、改訂 4 で完結する予定であるが、技術のペースは NIST の典型的な文書開発およびレビューのプロセスよりも速いため、この補足的な更新が正当化される。

SP 800-63B で扱われるこのような認証タイプは、多要素暗号認証である。通常、この認証タイプは、ハードウェアまたはソフトウェア内の暗号鍵を保護し、第 2 の認証要素（記憶された秘密またはバイオメトリック特性のいずれか）による起動を必要とする。秘密鍵を不正な暴露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 エクスポートやクローンができないようにすることが含まれていた。しかし、このパラダイムは変わり始めている。特に、新しい一連の認証プロトコルと仕様により、同期可能な認証子（一般に「パス キー」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（つまり、 複製）できるようになった。

SP 800-63-3 が 2017 年に発行されたとき、2 つの重要なサポート仕様（FIDO（Fast Identity Online）Client to Authenticator Protocol（CTAP）[3]および W3C の Web Authentication[4]（一緒に使用される場合は FIDO2 として知られる））は存在せず、実装の強固でよく理解されたエコシステムもなかった。当時利用可能であった暗号認証のタイプに基づき、2017 年のガイドラインは、多要素暗号認証が他のデバイスに鍵を「クローン」する能力を制限した。しかし、この2年間でエコシステムは急速に加速し、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している。これらの認証機能には、フィッシング対策など多くの利点がある、[1]特定の依拠当事者にバインドする能力、パスワードの送信の必要性の排除、 認証者のリカバリーの簡素化、保存された秘密鍵に付随する第 2 要素としての多様なデ バイス・ネイティブ・バイオメトリクスおよび PIN の使用などである。また

、ますます多様化するマルチデバイス、マルチプラットフォームの世界に適合する利便性も提供する。

どのような新しい技術でもそうであるように、技術革新の約束には、調査し理解しなければならない新 たな脅威と課題が伴う。そのため、この補足では、連邦機関が同期可能な認証機能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、現代の脅威を含めて考慮すべき事項の概要を示す。

[1]認証者が、その出力を通信チャネル(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化認証者である場合、フィッシング耐性がある。どちらの技術も、認証者の出力が意図したコンテキスト以外で使用されることを防ぐ。フィッシングへの耐性については、SP 800-63B-4 および OMB Memorandum 22-09, *Zero Trust Implementation Strategy* を参照のこと。

2. 目的

この文書の目的は、変化する認証およびクレデンシャル市場を反映するために、現行の NIST ガイドラインを適合させることである。この補足では、SP 800-63-3 で確立された認証保証レベル（Authentication Assurance Levels）と一致する方法で、同期可能な認証子がどのように脅威を軽減するかについて説明し、SP 800-63-3 認証保証レベル 2（AAL2）を達成するために活用できる同期可能な認証子の機能についての理解を連邦機関に提供する。また、SP 800-63B [2]の第 5.1.8 節で説明されているソフトウェア暗号化認証子の使用に関する最新情報、 特に、鍵が別のデバイスに複製（例えば、「クローン」または「同期」）された場合でも、当該認証子が AAL2 認証要件をサポートする能力についても提供する。最後に、本文書は、公衆向けアプリケーション（すなわち、OMB Memorandum M-19-17 に記述されているような、公衆 ID と相互作用する連邦情報システム）と連邦エンタープライズ・アプリケーション（すなわち、OMB Memorandum M- 19-17 に記述されているような、主に連邦エンタープライズ ID と相互作用する連邦情報システム）という 2 つのユースケースに基づく実装に関する考察を示す。この文書は、SP 800-63-3 にある既存のガイダンスを補足するものであり、SP 800-63B-4 の最終版に取って代わられる。

3. 同期可能な認証機能でAAL2を実現

NIST の認証子保証レベルは、主に、認証プロセスに対する特定の脅威から保護する認証子の能力 を中心に構成される。AAL2 では、ユーザが 2 つの 1 要素認証子、またはユーザ・アカウントにバインドされた多要素認証子 を所持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 は、SP 800-63-3 [1]から要求される脅威軽減策と、適切に構成された同期可能な認証機 能がこれらの脅威からどのように保護されるかを示している。

表 1.SP 800-63-3 における必要な脅威の緩和（表 4-1）[1]。

必要条件	AAL2	同期可能なオーセンティケータ（パスキーなど）
マン・イン・ザ・ミドル	必須	**達成された。**適切に構成された同期可能な認証機関は、以下の方法ですべての認証データを交換する。 認証され、保護されたチャンネル。
検証者-なりすまし抵抗	不要	**達成された。**適切に設定された同期可能な認証子は、一意の公開鍵または秘密鍵のペアを作成し、そのペアの 使用は、作成されたドメインに限定される（すなわち、鍵は特定のウェブサイトまたは 依拠当事者とのみ使用できる）。これにより、改ざんされたウェブ・ページが認証子をキャプチャして再利用することを防ぐことができる。 を出力した。
ベリファイアの耐妥協性	不要	**達成された。**適切に構成された同期可能な認証機関は、検証機関側にのみ公開鍵を保存する。これらの鍵は、ユーザーとしての認証には使用できない。同期ファブリックによって保存される秘密鍵は、承認された暗号技術を使用して暗号化された形でのみ保存される。アクセス・コントロールにより、認証されたユーザー以外の ユーザが保存された鍵にアクセスできないようにする。
リプレー耐性	必須	**達成された。**同期可能な認証子は、ランダムなノンスを使用することで、リプレイ耐性（

		将来のトランザクショ ンにおける再利用の 防止）を防止する。 各認証トランザクションに組み込まれる。
認証の意図	おすすめ	**達成された。**同期可能なオーセンティケータは 、暗号化認証プロトコルを開始するために、ユ ーザがアクティ ベーション・シークレットを入 力することを要求する。これは、ユーザの 積極的な参加。

セクション5では、同期可能な認証子の設定に関する追加的な考慮事項について論じる。

AAL2 の要件を満たすために、同期可能な認証子は、ローカルに保存された鍵のロックを解除するた めにローカル認証イベントを利用**しなければならない[SHALL]**。または、ローカル認証メカニズムが 利用できない場合は、別の認証子(たとえば、ユーザーが選択したパスワード)を使用**しなけれ ばならない[SHALL]。**FIDO2 Web認証(WebAuthn)コンテキストでは、W3C Web認証仕様の認証子データで利用可能な User Verificationフラグの値によって示される。FIDO2 WebAuthn 認証データフラグの詳細については、セクション5を参照のこと。

4. 認証キーのクローンの許可に関する最新情報

SP 800-63B のセクション 5.1.8.1「多要素暗号化ソフトウェア認証機能」は、認証機能 があるデバイスから別のデバイスへ暗号化認証鍵を「クローン」する能力を制限している。具体的には、以下のとおりである：

> 多要素暗号ソフトウェア認証機能は、複数のデバイスへの秘密鍵のクローニングを抑制すべきであり、 また促進すべきではない（SHALL NOT）。

同期可能な認証子は、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、以前に登録された認証子へのアクセスをユーザに提供する。NISTがSP800-63B-4の初期公開草案（ipd）からこの制限を削除したことで、この現実が認識された。

本文書の発行時点で、5.1.8.1 節の上記記述は本補足文書によって置き換えられ、本補足文書に規定 される要件に基づいて導入される同期可能な認証機能は、AAL2 で想定される脅威から保護するために十 分であるとみなされる**ものとする**。

同期可能な認証子のすべての使用に関する一般要件：

- すべての鍵は、承認された暗号技術を用いて生成さ**れなければならない**。
- クローンされた秘密鍵またはデバイスからエクスポートされた秘密鍵は、暗号化された形でのみ保存 さ**れなければならない**。
- すべての認証トランザクションは、デバイス上で生成された、またはシンクファブリック（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、ローカルデバイス上で秘密鍵操作を実行**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存される秘密鍵は、認証されたユーザのみがシンクファブリック内の 秘密鍵にアクセスできるよう、アクセス制御メカニズムによって保護さ**れなければならない**。
- 同期ファブリック内の秘密鍵へのユーザ・アクセスは、同期された鍵を使用する認証プロトコルの完全 性を保持するために、AAL2相当のMFAによって保

護さ**れなければならない（SHALL）**。

- これらの一般要件及び同期可能な認証子の使用に関するその他の機関固有の要件は、該当する場 合、一般向けウェブサイト及びデジタル・サービス・ポリシーに記載するなどして、文書化し、 伝えなければ**ならない（SHALL）**。

連邦企業に対する追加要件[2]同期可能な認証子の使用

- 連邦企業の秘密鍵（すなわち、連邦鍵）は、FISMA Moderate の保護または同等の保護を達成したシンク ファブリックに保管**しなければならない。**

[2]これらの要件の目的上、連邦企業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公衆向けの使用例は含まれない。

- 連邦政府の企業秘密鍵を含む認証子を生成、保管、同期するデバイス（携帯電話、ノートパソコン、タ ブレットなど）は、モバイル・デバイス管理ソフトウェアまたはその他のデバイス・コンフィギュレーショ ン・コントロールによって保護され、権限のないデバイスまたは同期ファブリックへの鍵の同期または共 有を防止**しなければならない。**
- 同期ファブリックへのアクセスは、秘密鍵のライフサイクルに対するエンタープライズ・コントロールを維持するた め、省庁が管理するアカウント（例えば、中央アイデンティティ・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）によって制御さ**れなければならない（SHALL）**。
- 秘密鍵を生成する認証機関は、認証機関の能力およびソースを検証するために使用できる認証 機能をサポート**すべきである（**例えば、エンタープライズ認証）。

これらの管理は、特に同期をサポートし、FIPS 140 検証など、既存の多要素ソフトウェア暗号 認証要件および AAL2 要件に付加的に考慮されるべきである。

5. 実装に関する考慮事項と要件

Syncable 認証機能は、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、公開鍵認証情報を活用するための API を提供する。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導入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、依拠当事者（RP）アプリケーションは、認証イベ ントの追加コンテキストを提供し、RP のアクセス・ポリシーに適合するかどうかを判断する ために、認証者に要求することができる。本節では、RP として活動する連邦機関が、NIST AAL2 脅威緩和策に適合する同期可能な認証機 能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

フラッグ	説明	要件と推奨事項
ユーザープレゼント（UP）	ユーザが認証子と相互作用したことを確認するための「プレゼンス」テストを示す（例： ハードウェアのタップ USBポートに挿入されたトークン)	連邦機関は、ユーザ提示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）**。**認証意図を**サポートする。
ユーザー認証済み (紫外線)	利用可能な「ユーザー検証」メソッドのいずれかを使用して、ユーザーが認証者によってローカル認証されたことを示す。	連邦機関は、UV が望ましいことを示す**ものとし**、すべてのアサーションを検査して UV フラグの値を確認**しなけれ ばならない（SHALL）**。これは、認証子が**多要素暗号認証子として**扱えるかどうかを示す。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 固有の暗記秘密を追加することで、認証器を **1 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、機関が以下のような検証方法を求める場合、 検証方法に関する追加データが提供される。 ローカル認証イベントのコンテキスト [4]

バックアップ参加資格	認証子を別のデバイスと同期できるかどうか（鍵を別の場所に保存できるかどうか）を示す。重要なのは、認証子が同期可能であるというだけでは、以下のことを意味しないことである。 それは同期されたことを意味する。	連邦機関は、**同期可能な認証子の**使用を制限するポリシーを確立する場合、このフラグを使用しても**よい**。このフラグは、デバイスにバインドされる認証子と、デバイスにクローンされる 認証子を区別するために必要である。 複数のデバイス。
バックアップ状態	認証*者が* 別のデバイスに同期された	連邦機関は、他のデバイスに**同期された**認証子に対する制限を確立する場合、このフラグを使用しても**よい。**公衆向けアプリケーションの場合、ユーザエクスペリエンスを考慮し、連邦政府 機関はこのフラグに基づいて受諾を変更すべきでは**ない[SHOULD NOT]。**企業の意思決定のために、このフラグを使用して、特定のデバイスに同期可能な 認証子の制限をサポートしても**よい[MAY]**。 アプリケーションを使用する。

表 2 に示されるフラグに加えて、機関は、実装および受け入れを選択する同期可能な認証機 関の出所および能力について、より詳細な情報を得ることを望むかもしれない。FIDO2 WebAuthn のコンテキストにおいて、一部の認証機関は、特定の認証機関の能力と製造者を判断 するために使用できる認証機能をサポートしている。企業ユースケースの場合、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、認証機能を実装**するべきである(SHOULD)**。好ましくは、RP が認証機に関する一意の識別情報を要求するエンタープライズ認証の形をとる。

認証は、広範な公衆向けアプリケーションに使用すべきでは**ない（SHOULD NOT）**。このような要件（すなわち、認証に対応していない場合、一部の一般ユーザの同期可能な認証機 能をブロックする要件）は、ユーザを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、フィッシングに脆弱な安全性の低い認証オプションに誘導する可能性がある。

RP がフラグおよび認証データを要求しても、認証局は要求された情報をすべて返さないかもしれず、ま たはリソースへのアクセスに義務付けられる期待応答と矛盾する情報を返すかもしれない。したがって、各機関は、同期可能な認証機を使用するユースケースを評価し、返された情報に基 づいて適切なアクセスポリシー決定を行うことが決定的に重要である。

6. 同期可能な認証機能の脅威と課題

同期可能な認証機能には、導入または展開の前に機関が評価すべきいくつかの明確な脅威および課 題がある。表 3 に、これらのリスクと推奨される軽減策の概要を示す。

表 3.同期可能な認証機能の脅威、課題、および緩和策

脅威と課題	説明	同期可能な認証機能の緩和
鍵の不正使用または管理の喪失	シンク可能な認証システムの中には、鍵を悪用する可能性のある他のユーザが所有するデバ イスへの秘密鍵の共有をサポートするものもある。	- 同期されたキーの共有を防止するために、エンタープライズ・デバイス管理機能または管理されたプロファイルを強制する。 - 利用可能なすべての通知チャネルを通じて、鍵共有イベントをユーザーに通知する。 - 利用者が鍵、鍵の状態、鍵の共有の有無を確認できる仕組みを提供する。 - 鍵の不正使用のリスクについて、既存の鍵管理システムを通じてユーザーを教育する。 意識向上とトレーニングの仕組み
シンク生地の妥協	鍵の同期をサポートするために、ほとんどの実装は、アカウントに関連付けられた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」に鍵をクローンする。	- 暗号化された鍵素材のみを保存する。 - 認証されたユーザー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制御を実装する。 - クラウドサービスの基本的なセキュリティ機能（例えば、FISMAの中程度の保護または同等の保護）を評価する。 - ハードウェア・セキュリティ・モジュールの活用 暗号化された鍵を保護する。

無許可 同期ファブリックへの アクセスとリカバリー	同期された鍵は、クラウドベースのアカウント回復プロセスを通じてアクセスできる。これらのプロセスは、認証者にとって潜在的な弱点となる。	- SP 800-63B に準拠した認証回復プロセスを実装する。 - デバイス管理またはマネージド・アカウント機能により、連邦政府エンタープライズ・キーの回復機能を制限する。 - AAL2およびAAL3で複数の認証機関をバインドする。 上記のように、回復をサポートする。 - シンクファブリックへのユーザーアクセスに新しい認証者を追加する場合は、AAL2認証を要求する。 - の派生認証子としてのみ使用する。 フェデラル・エンタープライズ・シナリオ [6] - 回復活動をユーザーに通知する。 - ユーザーが管理する秘密（つまり、シンクファブリックが知らないもの）を利用する。 プロバイダー）を使って暗号化し、鍵を復元する。

脅威と課題	説明	同期可能な認証機能の緩和
取り消し	同期可能な認証子はRP固有の鍵を使用するため、その鍵に基づいてアクセスを一元 的に取り消すことは困難である。たとえば、従来の PKI では、CRL を一元的に使用してアクセスを取り消すことができる。同様のプロセスは、同期可能な認証子（または FIDO WebAuthn ベースの認証子）では利用できない。	- ユーザが認証子を管理するための中央 ID 管理（IDM）アカウントを導入し、危殆化または期限切れの場合、「本国機関」アカウントから当該認証子を削除する。 - 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させる必要のあるRP固有鍵の数を制限する。 - ユーザーに対して定期的にレビューを要求するためのポリシーとツールを確立する。 キーの有効性と通貨性。

7. シェアリング

サイバーセキュリティ・ガイドラインは、歴史的に、ユーザ間で認証子を共有しないよう警告してきた。このガイダンスにもかかわらず、一部のユーザ・グループやアプリケーションでは、個人がデジタル・アカウントへのアクセスを共有できるようにするために、認証子とパスワードの共有が行われている。

表 3 に示すように、一部の同期可能認証機能実装は、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キーを共有する方法を確立している。さらに、一部の実装は、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、同期可能な認証子の共有を積極的に推奨している。

企業ユースケースの場合、鍵の共有に関する懸念は、鍵が承認されたデバイスや同期ファブリックから移動されることを制限するデバイス管理技術を使用することで、効果的に緩和することができる。しかし、公衆向けのユースケースでは、同様の緩和策は現在のところ利用できないため、 依拠当事者は、同期可能な認証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。公衆向けアプリケーションの所有者は、共有認証子に関連するリスクを認識する必要がある。公衆と対話する場合、機関は、ユーザがどの特定の認証子を使用しているのかについて限られ た可視性しか持たないため、すべての同期可能な認証子が共有の対象となる可能性があることを想定す る必要がある。多くの共有モデルには、リスクを最小化する実質的な制御（例えば、共有を許可するためにデバイス間の近接を要求する）があるが、他の実装はそれほど制限的ではない。

この新しいクラスの認証子がもたらす共有リスクは、特別なものではない。実際には、すべての AAL2 認証タイプに適用され、中には同期可能な認証タイプより弱いものもある。AAL2 のどの認証子も、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、帯域外認証子、さらにはプッシュ認証イベントを積極的に共有したり、被指名人（正式か否かを問わない）がエンドユーザに代わって認証を行うことを許可したりすることができる。

各省庁は、直面する特定のリスク、脅威、およびユーザビリティの考慮事項に基づいて、アプリ ケーションにどの認証手段を受け入れるかを決定する。同期可能な認証方式は、AAL2 までの実装を求めるアプリケーションの新しいオプションとして提供され

るかもしれず、他の認証方式と同様に、この技術のトレードオフは、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する期待される結果に基づいて、うまくバランスをとるべきである。

8. 結論

同期可能な認証子は、認証の状況、特に多要素暗号認証子の使用における実質的な技術的変化を示 すものである。暗号鍵の複製とクラウド・インフラへの保存を許可することに関連するトレードオフの 評価は、必然的に行われることになる。このことは、明確なリスク（認証鍵に対する企業の管理能力の喪失など）をもたらすが、同時に、一般市民や企業にとっての主要な脅威ベクトルを排除する、便利でフィッシングに強い認証機能への道筋を提供する。同期可能な認証機能は、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、本補足文書に含まれるガイドラインに沿った方法で導入される場合、AAL2 リスク軽減策との整合性を達成し、フィッシング耐性認証の採用をより広範に促進することができる。

この文書は、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、各省庁が十分な情報に基づ いてリスクベースの意思決定を行い、適切な場合には最新の業界イノベーションを統合できるような情 報を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-authenticator-protocol-v2.2-rd-20230321.html

[4] World Wide Web Consortium (2021) Web Authentication：公開鍵クレデンシャルにアクセスするための API レベル 3。https://www.w3.org/TR/webauthn-3/。

[5] ワード・ワイド・ウェブ・コンソーシアム（2021）ウェブ認証：公開鍵クレデンシャルにアクセスするための API レベル 3。セクション 10.2 認証機能拡張。https://www.w3.org/TR/webauthn-3/#sctn-defined-authenticator-extensions

[6] Ferraiolo H, Regenscheid AR, Fenton J (2023) 派生個人 ID 検証（PIV）クレデンシャルのガイドライン。(National Institute of Standards and Technology, Gaithersburg, MD）, NIST Special Publication (SP) NIST SP 800-157r1 ipd（初期公開草案）。https://doi.org/10.6028/NIST.SP.800-157r1.ipd。

付録 A.用語集

本補足版で導入された新しい用語を以下に示す。使用されている他のすべての用語は、https://doi.org/10.6028/NIST.SP.800-63-3 で入手可能な SP 800-63-3 の用語集と一致している。

同期可能な認証機能

ソフトウェアまたはハードウェアの暗号化オーセンティケータで、他のオーセンティケー タ（すなわち、デバイス）と同期させるために、認証鍵をクローンし、他のストレージに エクスポートすることを可能にするもの。

シンクファブリック

ユーザのデバイスにローカルではない、同期可能な認証子によって生成された認証鍵を保存、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サービス。