Sat, 09 Dec 2017 11:45:58 +0900

**NIST 特別出版物 800-63B**



**デジタル ID ガイドライン（**翻訳版）

*認証とライフサイクル管理*



Paul A. Grassi James L. Fenton Elaine M. Newton Ray A. Perlner

Andrew R. Regenscheid

William E. Burr Justin P. Richer

**Privacy Authors:** Naomi B. Lefkovitz Jamie M. Danker

**Usability Authors:** Yee-Yin Choong Kristen K. Greene Mary F. Theofanos

この出版物は以下から無料で入手できる: https://doi.org/10.6028/NIST.SP.800-63b





**NIST 特別出版物 800-63B**

**デジタル ID ガイドライン**

### *認証とライフサイクル管理*

Paul A. Grassi Elaine M. Newton

*Applied Cybersecurity Division Information Technology Laboratory*

James L. Fenton *Altmode Networks Los Altos, CA*

##### Privacy Authors:

Naomi B. Lefkovitz

*Applied Cybersecurity Division*

*Information Technology Laboratory*

Jamie M. Danker *National Protection and Programs Directorate Department of Homeland Security*

Ray A. Perlner Andrew R. Regenscheid *Cybersecurity Division*

*Information Technology Laboratory*

##### William E. Burr *Dakota Consulting, Inc. Silver Spring, MD*

Justin P. Richer

*Bespoke Engineering*

##### *Billerica, MA*

**Usability Authors:**

Yee-Yin Choong

Kristen K. Greene

*Information Access Division*

*Information Technology Laboratory*

Mary F. Theofanos

*Oﬃce of Data and Informatics*

*Material Measurement Laboratory*

### 翻訳者

Tatsuya Katsuhara (勝原 達也)

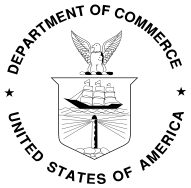
*NRI SecureTechnologies, Ltd.*

Hitomi Kimura (木村 瞳)

*Trend Micro Inc.*

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-63b

June 2017



U.S. Department of Commerce

*Wilbur L. Ross, Jr., Secretary*

National Institute of Standards and Technology

*Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology*

### **権限**

この出版物は, 2014年の連邦情報セキュリティ現代化法 (Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283) の下で NIST がその法定責任に従って発展させた. NIST は, 連邦情報システムのための最小限の要件を含め, 情報セキュリティの標準およびガイドラインの発展に責任を負うが, その標準とガイドラインは, 全国的なセキュリティシステムにポリシー権限を行使する適切な連邦政府職員の明確な承認がなければ, そうしたシステムに適用されてはならない. このガイドラインは, 行政管理予算局 (OMB) の回状 A-130 の要件と一致している.

この出版物に記述されたいかなることも, 商務長官が法的権限の下で連邦機関に義務付け拘束力を持たせた標準とガイドラインに反駁するために用いられるべきではない. また, これらのガイドラインは, 商務長官, 行政管理予算局長官, またはその他の連邦職員の既存の権限を変更したりそれに取って代わったりすると解釈されるべきではない. この出版物は, 非政府組織が自由意志に基づいて使用でき, 米国において著作権の対象にならないが. 引用で出典として示されることが望ましい.

National Institute of Standards and Technology Special Publication 800-63B

Natl. Inst. Stand. Technol. Spec. Publ. 800-63B, 78 pages (June 2017)

CODEN: NSPUE2

この出版物は以下から無料で入手できる: https://doi.org/10.6028/NIST.SP.800-63b

|  |
| --- |
| この文書では, 試験的な手順や概念を適切に記述する目的でいくつかの商業的なエンティティ, 装置, 材料を特定している場合がある. こうした特定は, NIST による推奨や支持を意味せず, そうしたエンティティ, 装置, 材料がその目的に対して最も有効であることを必ずしも意味していない.  この出版物では, 割り当てられた法的責任に応じてNIST が現在開発中の他の出版物を参照に挙げている場合がある。この出版物に含まれる情報は, 概念と方法論も含め, 付属文書が完成する前でも連邦機関て使用する場合がある. したがって, 現在の要件, ガイドライン, 手順がある場合は, それぞれの出版物が完成するまでそれが有効である. 計画目的と移行目的に対しては, 連邦機関は NIST によるこうした新しい出版物の発展に綿密に従うことを求めてもよい.  各機関は, パブリックコメントの期間中にすべての暫定版を調べ, NIST に意見を提示することが奨励される. 上記の他にもサイバーセキュリティに関する NIST の多くの出版物は, http://csrc.nist.gov/publicationsから入手できる. |

**この出版物に関する意見の提出先**

National Institute of Standards and Technology

Attn: Applied Cybersecurity Division, Information Technology Laboratory

100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Email: [dig-comments@nist.gov](mailto:dig-comments@nist.gov%20)

すべての意見は, 情報公開法 (FOIA) の下で公表される.

## **コンピュータシステム技術に関するレポート**

国立標準技術研究所 (National Institute of Standards and Technology, NIST) の情報技術研究所 (Information Technology Laboratory, ITL) は, 測定と標準に関する全国インフラのための技術的リーダーシップを提供することにより, 米国経済と福祉を促進する. ITL は, 情報技術の発展と生産的利用を押し進めるために, テスト, テスト方法, 参照データ, 概念検証の実装, テクニカル分析を開発している. ITL の責任には, 連邦システムの全国セキュリティ関連情報以外の経済的なセキュリティとプライバシーに対し, マネージメント, 行政, 技術, 物理上の標準とガイドラインの促進が含まれている. 特別出版物 800 シリーズは, 情報システムセキュリティにおける ITL の研究, ガイドライン, 社会福祉の支援努力と, 産業, 政府, 学術組織の共同作業に関するレポートである.

### **概要**

こうしたガイドラインは, デジタル身元識別情報 (ID) サービスを実施する連邦機関に技術要件を提供するもので, この目的に外れる標準の開発または使用を妨げる意図はない. ガイドラインは, 政府のシステムとオープンなネットワークを介してやりとりする主体の認証に焦点を当て, 所定の認証要求者が以前に認証された加入者であることを確定する。認証プロトコルの結果は, 認証を実施するシステムがローカルで使用されたり, 連携 ID システムのどこか別の場所で表明されたりする. この文書では, ３種類の身元情報保証レベルのそれぞれに対する技術的要件を定義する.この出版物は, NIST SP 800-63-2 の対応するセクションに代わるものである.

### **キーワード**

認証; 認証情報サービスプロバイダ; デジタル 認証;デジタル認証情報; 電子認証; 電子認証情報, 連携

### **謝辞**

Kaitlin Boeckl は SP 800-63 のすべての巻で芸術的な図表を作成してくれた. また, Digital ID & Authentication Council of Canada (DIACC) の Joni Brennan, NIST のKat Megas, Ellen Nadeau, Ben Piccarreta, そしてDeloitte & Touche LLP のRyan Galluzzo と Danna Gabel O’Rourke を含めた多くの方々にお世話になった.

原文を執筆してくれた Donna F. Dodson, W. Timothy Polk, Sarbari Gupta, Elaine M. Newton, Emad A. Nabbus のリーダーシップと革新的な考え方に敬意を表したい. こうした方々のたゆまない努力がなければ, SP 800-63 を今日ある文書に発展させたすばらしい土台は築けなかったであろう. これに加え, プライバシーに関する要件と考慮事項の発展に貢献してくれた連邦プライバシー委員会のデジタル認証タスクフォースの方々に特にお礼を申し上げる.

### **表記法**

「SHALL（しなければならない）」および「SHALL NOT（してはならない）」という用語は, この出版物に厳密に従うことを要求しており, これから逸脱することは許されない.

「SHOULD（すべきである）」および「SHOULD NOT（すべきでない）」という用語は, いくつかある選択肢の中で特に適切なものとして１つが推奨されることを示しており, 他の選択肢については言及も除外もしない. または, ある行動方針が望ましいが必ずしも要求されないことを示す. または, （否定の意味では）ある可能性や行動方針を推奨しないが禁止もしないことを示す.

「MAY（してもよい）」および「NEED NOT（しなくてよい）」という用語は, 出版物の範囲において行動方針が許容できることを示す.

「CAN（できる）」および「CANNOT（できない）」という用語は, 物質的であれ, 物理的であれ, 必然的であれ,可能性や能力があることを示し, 否定の意味では可能性や能力がないことを示す.

# 目次

1. 目的
2. はじめに
3. 定義と略語
4. **Authenticator Assurance Levels**

4.1 Authenticator Assurance Level 1

4.1.1 Permitted Authenticator Types

4.1.2 Authenticator and Verifier Requirements

4.1.3 再認証

4.1.4 Security Controls

4.1.5 Records Retention Policy

4.2 Authenticator Assurance Level 2

4.2.1 Permitted Authenticator Types

4.2.2 Authenticator and Verifier Requirements

4.2.3 再認証

4.2.4 Security Controls

4.2.5 Records Retention Policy

4.3 Authenticator Assurance Level 3

4.3.1 Permitted Authenticator Types

4.3.2 Authenticator and Verifier Requirements

4.3.3 再認証

4.3.4 Security Controls

4.3.5 Records Retention Policy

4.4 Privacy Requirements

4.5 Summary of Requirements

1. AuthenticatorおよびVerifierの要件

5.1 Requirements by Authenticator Type

5.1.1 Memorized Secrets

5.1.2 Look-Up Secrets

5.1.3 アウトオブバンドDevices

5.1.4 Single-Factor OTP Device

5.1.5 Multi-Factor OTP Devices

5.1.6 Single-Factor Cryptographic Software

5.1.7 Single-Factor Cryptographic Devices

5.1.8 Multi-Factor Cryptographic Software

5.1.9 Multi-Factor Cryptographic Devices

5.2 General Authenticator Requirements

5.2.1 Physical Authenticators

5.2.2 Rate Limiting (Throttling)

5.2.3 Use of Biometrics

5.2.4 Attestation

5.2.5 Verifier Impersonation Resistance

5.2.6 Verifier-CSP Communications

5.2.7 Verifier-Compromise Resistance

5.2.8 Replay Resistance

5.2.9 認証 Intent

5.2.10 Restricted Authenticators

1. Authenticatorライフサイクルの要件

6.1 Authenticator Binding

6.1.1 Binding at 登録

6.1.2 Post-登録 Binding

6.1.3 Binding to a Subscriber-provided Authenticator

6.1.4 Renewal

6.2 Loss, Theft, Damage, and Unauthorized Duplication

6.3 Expiration

6.4 Revocation and Termination

1. セッション管理

7.1 セッション Bindings

7.1.1 Browser Cookies

7.1.2 Access Tokens

7.1.3 Device Identification

7.2 再認証

7.2.1 再認証 from a Federation or アサートion

1. 脅威とセキュリティに関する考慮事項

8.1 Authenticator Threats

8.2 Threat Mitigation Strategies

8.3 Authenticator Recovery

8.4 セッション Attacks

1. プライバシに関する考慮事項

9.1 Privacy Risk Assessment

9.2 Privacy Controls

9.3 Processing Limitation

9.4 Agency-Specific Privacy Compliance

1. ユーザービリティに関する考慮事項

10.1 Usability Considerations Common to Authenticators

10.2 Usability Considerations by Authenticator Type

10.2.1 Memorized Secrets

10.2.2 Look-Up Secrets

10.2.3 Out-of-Band

10.2.4 Single-Factor OTP Device

10.2.5 Multi-Factor OTP Device

10.2.6 Single-Factor Cryptographic Software

10.2.7 Single-Factor Cryptographic Device

10.2.8 Multi-Factor Cryptographic Software

10.2.9 Multi-Factor Cryptographic Device

10.3 Summary of Usability Considerations

10.4 Biometrics Usability Considerations

1. 参照

11,1 General References

11,2 Standards

11.3 NIST Special Publications

11. 4 Federal Information Processing Standards

List of Appendices

付録A — 記憶シークレットの強度

A.1 Introduction

A.2 Length

A.3 Complexity

A.4 Randomly-Chosen Secrets

A.5 Summary

List of Tables

Table 2-1 Normative and Informative Sections of SP 800-63B

Table 4-1 AAL Summary of Requirements

Table 8-1 Authenticator Threats

Table 8-2 Mitigating Authenticator Threats**正誤表**

この表は, 特別出版物 800-63B で加えられた変更の一覧である. 正誤表の更新には, 編集上または実質上の修正, 明確化, その他のマイナーな変更を含めることができる.

|  |  |  |  |
| --- | --- | --- | --- |
| **日付** | **種類** | **変更** | **場所** |
| **2017-12-01** | 編集上 | 文書の他のテキストと一貫性を持たせるために AAL の説明を更新 | はじめに |
|  | 編集上 | AAL3 の認証コードの選択肢を反映させるために “cryptographic” を削除 | セクション 4.3 |
|  | 実質上 | 属性の所有要件を明確化 | セクション 4.4 |
|  | 編集上 | マルチファクタ認証コードのアクティベーションファクタに関する記述の矛盾を訂正 | セクション 5.1.5.1, 5.1.8.1, 5.1.9.1 |
|  | 実質上 | ハードウェア TPM をハードウェア暗号認証コードとして使用を受け入れ | セクション 5.1.7.1, 5.1.9.1 |
|  | 編集上 | 生体認証に認められた保護チャネルの規範の説明を改善 | セクション 5.2.3 |
|  | 編集上 | 要件が認証トランザクションに適用されないことを強調するために, “トランザクション” を “結び付けトランザクション” に変更 | セクション 6.1.1 |
|  | 編集上 | セクション 7.2 の “注意” を入れ替え | セクション 7.2 |
|  | 編集上 | この文書の他の箇所で使われている用語と一致させるために, IdP を CSP に変更 | 表 8-1 |
|  | 編集上 | サイドチャネル攻撃の文字頭を大文字に変更 | 表 8-2 |
|  | 実質上 | タイトルを “処理制限” に変更. 説明を明確化. プライバシー目的の説明を追加. 同意が明示的であることを指定 | セクション 9.3 |
|  | 編集上 | 参照として NISTIR 8062 を追加 | セクション 11.1 |
|  | 編集上 | SP 800-63C のタイトルを訂正 | セクション 11.3 |

# 目的

*このセクションは参考情報である.*

この文書と付随する特別出版物 (SP) 800-63 (sp800-63-3.html), SP 800-63A (sp800-63a.html), SP 800-63C (sp800-63c.html)は, デジタル認証の実装のための技術的なガイドラインを政府機関に提供する．

# はじめに

*このセクションは参考情報である.*

デジタル身元情報 (ID) はオンライントランザクションに関わる主体の一意な表現である．デジタル ID はデジタルサービスの文脈では常に一意だが，必ずしも実在する主体まで遡って追跡できる必要はない．言い換えれ ば，デジタルサービスへのアクセスは，その基礎となる主体の実際の名称が知られていることを意味しなくてもよい．身元情報の検証は, 主体が実際に主張している本人であることを確認する．デジタル認証は，デジタル ID を主張するために用いる１つ以上の認証コードの妥当性を確定するプロセスである．認証は, デジタルサービスにアクセスしようとしてい る主体が，認証に用いる技術の管理下にあることを確認する．何度も利用するサービスでは，正常な認証によって現在サービスにアクセスしている主体が以前にアクセスした人と同一であるという適切なリスクベースの確証が得られる．デジタル ID は多くの場合オープンなネットワークを介した個人の検証を伴い，やはりオープンなネットワークを介した個人の認証が必ず必要となるため, 技術的な課題が存在する．この課題には，主体のデジタル ID の不正使用につながるなりすましや他の攻撃の可能性が数多くある．

加入者の継続的な認証は，加入者をそのオンライン活動と関連付けるプロセスの要である．加入者の認証は，認証要求者が所定の加入者と関連付けられている１つ以上の*認証コード*(旧バージョンのSP 800-63では*トークン*と呼ばれていた)を管理していることを検証して実施される．成功した認証は，証明書利用者 (RP) に対して, 仮名か実名の識別子と他の随意の属性情報のアサーションになる．

この文書では，さまざまな*認証コード保証レベル* (AAL) で利用できる認証プロセス (認証コードの選択を含む) の種類に関する推奨事項を提供する．さらに，紛失や盗難の際の取り消しを含めた認証コードのライフサイクルに関する推奨事項も提供する．

この技術的ガイドラインは，ネットワーク経由のシステムに対する主体のデジタル認証に適用される．物理的アクセス (建物など) の際の認証については扱わないが，デジタルアクセスに利用される一部の認証情報は, 物理的アクセスの認証にも利用できる．さらにこの技術的ガイドラインは，認証プロトコルに参加する連邦政府機関のシステムとサービスプロバイダが加入者に対して認証されることを規定する．

認証トランザクションの強度はAALとして知られている序数的指標に特徴がある．より強力な認証(より高いAAL)では，悪意のある攻撃者が認証プロセスを欺くにはさらに高度な能力とさらに多くのリソースが必要になる．より高いAALでの認証は, 攻撃のリスクを効果的に減少させることができる．それぞれのAAL に要求される技術要件の概要を以下に示す. 特定の規範の要件については，この文書のセクション 4 と 5 を参照．

**認証コード保証レベル 1** - AAL 1では, 加入者のアカウントに結び付けられた認証コードを認証要求者が管理していることがある程度の確実性で保証される．AAL 1では利用可能な幅広い認証技術を使用する単一ファクタかマルチファクタの認証を必要とする．認証を成功させるには，セキュアな認証プロトコルによって認証要求者が認証コードを所有し管理していることを証明する必要がある．

**認証コード保証レベル 2** - AAL 2では，加入者のアカウントに結び付けられた認証コードを認証要求者が管理していることが高い確実性で保証される．異なる2つの認証ファクタを所有し管理しているいることをセキュアな認証プ ロトコルを通して証明する必要がある．AAL2 以上では，認可された暗号化技術が要求される．

**認証コード保証レベル 3** - AAL 3では，加入者のアカウントに結び付けられた認証コードを認証要求者が管理していることが非常に高い確実性で保証される．AAL 3における認証は，暗号プロトコルによる鍵の所有の証明に基づく．AAL 3の認証では，ハードウェアベースの認証コードと, 検証者に偽装耐性を提供 する認証コードが要求される．同じデバイスが両方の要件を満たしていてもよい．AAL 3で認証するには，認証要求者はセキュアな認証プロトコルを通して2つの異なる認証ファクタを所有し管理していることを証明する必要がある．認可された暗号化技術が要求される．

次の表はこの文書の各セクションが規範であるか参考情報であるかを示している:

**表 2-1 SP 800-63B の規範と参考情報セクション**

|  |  |
| --- | --- |
| セクション名 | 標準**/**参考情報 |
| 1. 目的 | 参考情報 |
| 2. はじめに | 参考情報 |
| 3. 定義と略語 | 参考情報 |
| 4. 認証コードの保証レベル | 規範 |
| 5. 認証コードと検証者の要件 | 規範 |
| 6. 認証コードのライフサイクル要件 | 規範 |
| 7. セッション管理 | 規範 |
| 8. 脅威とセキュリティの考慮事項 | 参考情報 |
| 9. プライバシーの考慮事項 | 参考情報 |
| 10. ユーザビリティの考慮事項 | 参考情報 |
| 11. 参考文献 | 参考情報 |
| 付録A — 記憶シークレットの強度 | 参考情報 |

## **定義と略語**

定義と略語についてはSP 800-63 (sp800-63-3.html) 付録 Aを参照．

# 認証コードの保証レベル

*このセクションは規範と参考情報の両方を含む.*

指定されたAALの要件を満たすには，認証要求者は加入者として認識される少なくとも所定の強度で認証されなければならない(SHALL)．認証プロセスの結果は識別子になり，加入者がそのRPに対して認証するたびに使われなければならない(SHALL)．それは匿名でもよい(MAY)，加入者の識別子は別の主体のために再利用すべきではない(SHOULD NOT)が，CSPによって過去に登録済みの主体を再登録する場合には再利用すべきである(SHOULD)．加入者を一意な主体であると識別する他の属性も提供されてもよい(MAY)．

各AALにおける認証コードと検証者に対する規範要件は, セクション5に詳しく説明してある．

最も適切なAALの選択方法は SP 800-63 (sp800-63-3.html) セクション6.2に詳しく説明してある．

FIPS 140 要件は，FIPS 140-2またはより新しい改訂版により満たされる．

IAL1では，デジタル ID サービスで属性を収集して利用可能にすることができる．どのようなPIIまたは他の個人情報も, 自己表明であっても確認済みであっても, マルチファクタ認証を必要とする．したがって，連邦政府機関は自己表明のPIIや他の個人情報をオンラインで利用可能にするとき，最低でもAAL2を選択しなければならない(SHALL)．

### **認証コード保証レベル 1**

*このセクションは規範である．*

AAL 1は, 加入者のアカウントに結び付けられた認証コードを認証要求者が管理していることをある程度の確実性で保証する．AAL 1では, 利用可能な幅広い認証技術による単一ファクタかマルチファクタの認証を必要とする．認証を成功させるには，セキュアな認証プロトコルを通して認証要求者が認証コードを所有し管理していることを証明する必要がある．

#### **許可されている認証コードのタイプ**

AAL1の認証では，セクション 5 で定義されている次のタイプの認証コードを利用しなければならない(SHALL):

* 記憶シークレット (セクション 5.1.1)
* ルックアップシークレット (セクション 5.1.2)
* アウトオブバンドデバイス (セクション 5.1.3)
* 単一ファクタワンタイムパスワード (OTP) デバイス (セクション 5.1.4)
* マルチファクタ OTP デバイス (セクション 5.1.5)
* 単一ファクタ暗号化ソフトウェア (セクション 5.1.6)
* 単一ファクタ暗号化デバイス (セクション 5.1.7)
* マルチファクタ暗号化ソフトウェア (セクション 5.1.8)
* マルチファクタ暗号化デバイス (セクション 5.1.9)

#### **認証コードと検証者の要件**

AAL 1で使用する暗号認証コードは，認可された暗号化技術を用いなければならない (SHALL)．オペレーティングシステムに関連して機能するソフトウェアベースの認証コードを使用して，それが当てはまる場合は動作している利用者のエンドポイントの危殆化 (マルウェアなど) の検出を試みてもよく(MAY)，そうしたセキュリティ侵害が検出された場合は運用を完成させるべきでない(SHOULD NOT)．

認証要求者と検証者との間の通信(アウトオブバンド認証コードの場合はプライマリチャネルを利用)は，認証コード出力値の秘匿性と中間者攻撃に対する耐性を提供する認証済み保護チャネルを介して行わなければならない(SHALL)．

政府機関がAAL 1で運用する検証者は，FIPS 140 レベル 1 の要件に適合していることが確認されなければならない(SHALL)．

#### **再認証**

セクション 7.2に説明してあるように，加入者のセッションは定期的に再認証されなければならない(SHALL)．AAL 1では，ユーザーの活動とは無関係に加入者の再認証を少なくとも30日に1回実施すべきである(SHOULD)．セッションはこの時間制限に到達したら終了(つまりログアウト) されるべきである(SHOULD).

#### **セキュリティ管理策**

CSPは，SP 800-53 やそれに相当する連邦基準（例えば FEDRAMP）または業界標準に定められた低レベルのセキュリティ管理策の中から,適切に調整したセキュリティ管理策を採用しなければならない (SHALL)．CSPは影響が低レベルのシステムやそれに相当する最低限の保証関連管理が十分であることを保証しなければならない (SHALL)．

#### **記録保管ポリシー**

CSPは，準拠法と規則そして国立公文書館（NARA）の任意の記録保管スケジュールを含む政策に合致するそれぞれの記録保管ポリシーに従わなければならない．CSPはいずれの必須要件もない場合に記録を保管するときは，記録を保管すべき期間を決定するためにプライバシーとセキュリティリスク評価を含むリスク管理プロセスを実施しなければならず (SHALL)，加入者にその保管ポリシーについて通知しなければならない (SHALL)．

### **認証コード保証レベル 2**

*このセクションは規範である．*

AAL 2は，加入者のアカウントに結び付けられている認証コードを認証要求者が管理していることを高い確実性で証明する．セキュアな認証プロトコルによって2つの異なる認証ファクタを所有し管理していることが求められる．AAL2以上では, 認可された 暗号化技術が必要である．

#### **許可されている認証コードのタイプ**

AAL2の認証では，１つのマルチファクタ認証コードか2つの単一ファクタ認証コードの組み合わせのどちらかを利用しなければならない (SHALL)．１つのマルチファクタ認証コードは，1回の認証イベントを実行するために２つのファクタを必要とする．例えば, デバイスを起動するために必要な統合型生体認証センサーを備えた暗号的にセキュアであるようなデバイスである. 認証コードの要件はセクション 5で指定されている．

マルチファクタ認証コードを利用するとき，以下を使用してよい(MAY):

* マルチファクタ OTP デバイス（セクション5.1.5）
* マルチファクタ暗号化ソフトウェア（セクション 5.1.8）
* マルチファクタ暗号化デバイス（セクション 5.1.9）

2つの単一ファクタ認証コードを組み合わせる場合は，記憶シークレット認証コード（セクション 5.1.1）と, 以下のリストから1つの所有ベース（つまり “本人が持っているもの”）認証コードを含めなければならない (SHALL):

* ルックアップシークレット（セクション 5.1.2）
* アウトオブバンドデバイス（セクション 5.1.3）
* 単一ファクタ OTP デバイス（セクション 5.1.4）
* 単一ファクタ暗号化ソフトウェア（セクション 5.1.6）
* 単一ファクタ暗号化デバイス（セクション 5.1.7）

注意: 生体認証がセクション 5.2.3 の要件を満たす場合は, 生体認証に加えてデバイスが認証されなければならない. 生体認証はファクタとして認識されるが, それ自身で認証コードとして認識されないからである. したがって, 生体認証で認証を行う場合, 関連するデバイスは "本人が持っているもの" になり, 生体認証も "本人が持っているもの" となるため, ２種類の認証コードを使用する必要はない.

#### **認証コードと検証者の要件**

AAL 2で用いられる暗号認証コードは，認可された暗号化技術を使用しなければならない(SHALL)．政府機関が入手する認証コードは，FIPS 140 レベル 1の要件に適合していることが確認されなければならない(SHALL)．オペレーティングシステムに関連して機能するソフトウェアベースの認証コードは，それが当てはまる場合は動作している利用者のエンドポイントの危殆化（マルウェアなど）の検出に用いてもよく(MAY)，そうしたセキュリティ侵害が検出された場合は運用を完成させるべきでない(SHOULD NOT)． AAL2で使用する少なくとも1つの認証コードは, セクション 5.2.8に記述してあるようにリプレイ耐性がなければならない (SHALL)．AAL2の認証は, セクション 5.2.9に記述してあるように少なくとも1つの認証コードから認証意図を明示するべきである(SHOULD)．

認証要求者と検証者との間の通信(アウトオブバンド認証コードの場合はプライマリチャネルを利用)は，認証コード出力値の秘匿性と中間者攻撃に対する耐性を提供する認証済み保護チャネ ルを介して行わなければならない(SHALL)．

政府機関がAAL 2で運用する検証者は， FIPS 140 レベル 1 の要件に適合していることが確認されなければならない(SHALL)．

認証プロセスでスマートフォンなどのデバイスが利用される場合，そのデバイスのアンロック（一般的にPIN か生体認証を使用）を認証ファクタの１つと見なしてはならない(SHALL NOT)．一般的に，検証者はそのデバイスがロックされていたことや，アンロックプロセスが適切な認証コードタイプの要件に合致しているのかどうかを知ることは不可能だからである．

生体認証ファクタがAAL 2で利用される場合，セクション 5.2.3に規定されたパフォーマンス要件を満たさなくてはならず(SHALL)，検証者は生体認証センサーと後続処理がそうした要件に合致していることを明確にすべきである(SHOULD)．

#### **再認証**

セクション 7.2に記述してあるように，加入者のセッションを定期的に再認証しなければならない(SHALL)．AAL 2では，ユーザーの活動とは無関係に，加入者の再認証はセッションの利用が延長されている間は少なくとも12時間に1回繰り返されなければならない(SHALL)．30分以上活動がない場合も加入者の再認証が繰り返されなければならない(SHALL)．セッションはこれらの時間制限に到達したら終了（すなわちログアウト）されなければならない(SHALL)．

まだ時間制限に到達していないセッションの再認証は，記憶シークレットだけを要求するか，または まだ有効なセッションシークレットと連動している生体認証を要求してもよい(MAY)．検証者は非活動によるタイムアウトの直前に，ユーザーに活動を促してもよい(MAY)．

#### **セキュリティ管理策**

CSPは，SP 800-53 やそれに相当する連邦基準（例えば FEDRAMP）または業界標準に定められた中レベルのセキュリティ管理策の中から適切に調整したセキュリティ管理策を採用しなければならない (SHALL)．CSPは影響が中レベルのシステムやそれに相当する最低限の保証関連管理が十分であることを保証しなければならない (SHALL)．

**4.2.5 記録保管ポリシー**

CSPは，準拠法と規則そして国立公文書館 (NARA) の任意の記録保管スケジュールを含む政策に合致するそれぞれの記録保管ポリシーに従わなければならない．いずれの必須要件もないときに記録を保管する場合は，CSPは記録を保管すべき期間を決定するためにプライバシーとセキュリティリスク評価を含むリスク管理プロセスを実施しなければならず (SHALL)，加入者にその保管ポリシーについて通知しなければならない (SHALL)．

### **認証コード保証レベル 3**

*このセクションは規範である．*

AAL3は，加入者のアカウントに結び付けられている認証コードを認証要求者が管理していることを非常に高い確実性で証明する． AAL3における認証は，暗号プロトコルを介した鍵の所有の証明に基づいている．AAL3 認証は，1つのハードウェアベースの認証コードと，検証者なりすまし耐性を備えた１つの認証コードを利用しなければならない (SHALL)．同じデバイスが両方の要件を満たしてもよい(MAY)．AAL3で認証するためには，認証要求者はセキュアな認証プロトコルを介して2つの異なる認証ファクタの所有と管理を証明しなければならない (SHALL)．承認された 暗号化技術が必要である．

#### **許可されている認証コードのタイプ**

AAL3の認証では，セクション4.3の要件を満たす認証コードの組み合わせの1つを利用しなければならない (SHALL)．有効な組み合わせは次のとおり:．

* マルチファクタ暗号化デバイス（セクション 5.1.9）
* 単一ファクタ暗号化デバイス（セクション 5.1.7）を記憶シークレット（セクション 5.1.1）と併用
* マルチファクタ OTP デバイス(ソフトウェアまたはハードウェア) (セクション 5.1.5)を単一ファクタ暗号化デバイス(セクション 5.1.7)と併用
* マルチファクタ OTP デバイス(ハードウェアのみ) (セクション 5.1.5)を単一ファクタ暗号化ソフトウェア (セクション 5.1.6)と併用
* 単一ファクタ OTP デバイス(ハードウェアのみ) (セクション 5.1.4) をマルチファクタ暗号化ソフトウェア認証コード (セクション 5.1.8)と併用
* 単一ファクタ OTP デバイス(ハードウェアのみ) (セクション 5.1.4) を単一ファクタ暗号化ソフトウェア認証コード(セクション 5.1.6)と記憶シークレット(セクション 5.1.1)と併用

#### **認証コードと検証者の要件**

認証要求者と検証者との間の通信は，認証コード出力値の秘匿性と中間者攻撃に対する耐性を提供する認証済み保護チャネルを介して行わなければならない(SHALL)．AAL3 認証で利用されるすべての暗号化デバイス認証コードは，セクション 5.2.5に記述してあるように検証者なりすまし耐性を備えていなければならず(SHALL)，セクション 5.2.8に記述してあるようにリプレイ耐性がなければならない(SHALL)．AAL3のすべての認証プロセスと再認証プロセスは, セクション 5.2.9に記述してあるように少なくとも1つの認証コードから認証意図を明示しなければならない(SHALL)．

AAL 3で利用されるマルチファクタ認証コードは，少なくともFIPS 140 レベル 3の物理的セキュリティを備え，総合的にFIPS 140 レベル 2以上で確認されたハードウェア暗号モジュールでなければならない (SHALL)．AAL3で利用される単一ファクタ暗号化デバイスは，少なくともFIPS 140 レベル 3の物理的セキュリティを備え，総合的にFIPS 140 レベル 1以上で確認されされなければならない (SHALL)．

AAL3における検証者は，FIPS 140 レベル 1以上で確認されなければならない(SHALL)．

AAL3における検証者には，少なくとも１つの認証ファクタに関してセクション 5.2.7に記述のあるように検証者危殆化耐性がなければならない(SHALL)．

AAL3におけるハードウェアベースの認証コードと検証者は，関連するサイドチャネル攻撃（タイミングや消費電力の分析）への耐性を備えているべきである(SHOULD)．関連するサイドチャネル攻撃 は，CSPが実施するリスク評価で確定されなければならない(SHALL)．

認証プロセスでスマートフォンなどのデバイスが上記の要件を満たすことを想定して使用する場合, 認証ファクタの１つを満たすためにデバイスをアンロックすることを検討してはならない (SHALL NOT)．一般的に，検証者はそのデバイスがロックされていたことを知ることはできず，アンロックプロセスが適切な認証コードタイプの要件に合致しているのかどうかもわからないためである．

生体認証ファクタがAAL3で利用される場合，検証者は生体認証センサーと後続処理がセクション 5.2.3 に規定されたパフォーマンス要件に合致していることを確実にしなければならない(SHALL)．

#### **再認証**

セクション 7.2に記述してあるように，加入者のセッションを定期的に再認証しなければならない(SHALL)．AAL3では，セクション 7.2に記述してあるように，ユーザーの活動とは無関係に加入者の再認証をセッション利用が延長されている間は少なくとも12時間に1回繰り返されなければならない (SHALL)．15分以上活動がない場合も加入者の再認証が繰り返されなければならない (SHALL)．再認証には両方の認証ファクタを用いなければならない(SHALL)．セッションはこれらの時間制限に到達したら終了（すなわちログアウト）されなければならない (SHALL)．検証者はタイムアウトの直前にユーザーに活動を促してもよい(MAY)．

#### **セキュリティ管理策**

CSPは，SP 800-53 やそれに相当する連邦基準（例えば FEDRAMP）または業界標準に定められた高レベルのセキュリティ管理策の中から適切に調整したセキュリティ管理策を採用しなければならない (SHALL)．CSPは影響が高レベルのシステムやそれに相当する最低限の保証関連管理が十分であることを保証しなければならない (SHALL)．

* + 1. **記録保管ポリシー**

CSPは，準拠法と規則そして国立公文書館（NARA）の任意の記録保管スケジュールを含む政策に合致するそれぞれの記録保管ポリシーに従わなければならない．いずれの必須要件もないときに記録を保管する場合は，CSPは記録を保管すべき期間を決定するためにプライバシーとセキュリティリスク評価を含むリスク管理プロセスを実施しなければならず (SHALL)，加入者にその保管ポリシーについて通知しなければならない (SHALL)．

### **プライバシー要件**

このセクションは規範である。

CSPはSP 800-53かそれに相当する業界基準で定義されている適切に調整されたプライバシー管理策を採用しなければならない (SHALL)．

CSP は, 身元情報の検証, 認証, 属性アサーション（これらをまとめて “身元情報サービス”と言う）, 関連する不正行為の防止, 法律や法的手続きの準拠以外の⽬的で属性を処理する場合は, 追加処理によるプライバシーのリスクに釣り合った予測可能性と管理可能性を維持する措置を講じなければならない (SHALL). こうした措置には, 明確な通知の提供, 加入者の同意の取得, 属性の選択的使用または開示の有効化を含めてもよい (MAY). CSP は同意措置を利用する場合, 追加処理のための同意を身元情報サービスの条件にしてはならない (SHALL NOT).

CSPが政府機関か民間プロバイダかに関係なく，次の要件が認証サービスを提供または利用する機関に適用される:

* 自らのプライバシー上級担当者 (SAOP) と協議し, 身元情報の検証を実施するための PII 収集に*1974年プライバシー法* [Privacy Act]（セクション 9.4を参照）の要件が適⽤されるかどうか判断するための分析を実施しなければならない(SHALL)．
* 該当する場合はそうした収集をカバーするために, 記録通知システム (SORN) を公開しなければならない(SHALL)．
* SAOP と協議し, 身元情報の検証を実施するための PII 収集に*2002年電子政府法* [E-Gov]の要件が適⽤されるかどうか判断するための分析を実施しなければならない(SHALL)．
* 該当する場合はそうした収集をカバーするために, プライバシー影響評価 (PIA) を公開しなければならない(SHALL)．

### **要件のまとめ**

*このセクションは参考情報である*

表 4-1 に各AALの要件をまとめる:

**表 4-1 各AALの要件のまとめ**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 要件 | | **AAL1** | **AAL2** | **AAL3** | |
| **許可されている**  **認証コードタイプ** | | 記憶シークレット;  ルックアップシークレット; アウトオブバンド;  単一ファクタOTP デバイス;  マルチファクタOTPデバイス;  単一ファクタ暗号化ソフトウェア; 単一ファクタ暗号化デバイス;  マルチファクタ暗号化ソフトウェア; マルチファクタ暗号化デバイス | マルチファクタOTPデバイス;  マルチファクタ暗号化ソフトウェア; マルチファクタ暗号化デバイス; または 記憶シークレット  および:   * ルックアップシークレット * アウトオブバンド * 単一ファクタOTPデバイス * 単一ファクタ暗号化ソフトウェア * 単一ファクタ暗号化デバイス | マルチファクタ暗号化デバイス;  単一ファクタ暗号化デバイスおよび記憶シークレット;  単一ファクタOTPデバイスおよびマルチファクタ暗号化デバイスまたはソフトウェア;  単一ファクタOTPデバイスおよび単一ファクタ暗号化ソフトウェアおよび記憶シークレット | |
| **FIPS 140 確認** | | レベルl 1（政府機関の検証者） | レベル1（政府機関の  認証コードと検証者） | レベル2 全体（マルチファクタ認証コード）  レベル1 全体（検証者と単一ファクタ暗号化デバイス）  レベル3 物理セキュリティ  (すべての認証コード) | |
| **再認証** | | 30 日 | 12 時間 または 30 分 間活動なし; 1つの認証ファクタ使用してもよい(MAY) | 12 時間 または 15 分 間活動なし; 両方の認証ファクタを使用しなければならない(SHALL) | |
| **セキュリティ管理策** | | SP 800-53 低レベルのベースライン（または同等） | SP 800-53 中レベルのベースライン（または同等） | SP 800-53 高レベルのベースライン（または同等） | |
| **中間者攻撃耐性** | | 必須 | 必須 | 必須 | |
| **検証者なりすまし耐性** | | 不要 | 不要 | 必須 | |
| **検証者危殆化耐性** | | 不要 | 不要 | 必須 | |
| **リプレイ耐性** | | 不要 | 必須 | 必須 | |
| **認証意図** | | 不要 | 推奨 | 必須 | |
| **記録保管ポリシー** | | 必須 | | 必須 | 必須 |
| **プライバシー管理策** | | 必須 | | 必須 | 必須 |

# 認証コードと検証者の要件

*このセクションは規範である．*

このセクションでは，認証コードタイプごとの要件について詳しく説明する．セクション 4で指定された再認証要件と, [セクション 5.2.5]に記述されているAAL3における検証者なりすまし耐性の例外を除いて，各認証コードタイプの技術要件は認証コードが利用されるAALに関係なく同じであ る．

### **認証コードタイプごとの要件**

#### **記憶シークレット**

記憶されたシークレット認証コードは, 一般的にパスワードや数字の場合は *PIN* と呼ばれるが, ユーザーが選択して記憶する意図のあるシークレット値である。記憶されたシークレットは, 攻撃者が推測できない十分な複雑性と機密性を備えている必要がある。そうしないと, 正しいシークレット値が漏洩してしまう。記憶されたシークレットは, *本人が知っているもの*である.

記憶シークレット認証コードは, 一般的にパスワードや数字の場合は PIN と呼ばれるが, ユーザーが選択して記憶することを意図したシークレット値である。記憶シークレットは, 攻撃者が推測できない十分な複雑性と機密性を備えている必要がある。そうしないと, 正しいシークレット値が漏洩してしまう。記憶シークレットは, 本人が知っているものである.

* + - 1. **記憶シークレット認証コード**

記憶シークレットを加入者が選択する場合は, その長さは少なくとも8文字でなければならない(SHALL)．CSP か検証者がランダムに選択する場合は，その長さは 少なくとも6文字でなければならず (SHALL)，すべて数字でもよい(MAY)．CSPや検証者が選択された記憶シークレットを危殆化した値のブラックリストに基づいて拒否する場合，加入者は別の記憶シークレットを選ぶよう要求されなければならない(SHALL)．記憶シークレットの複雑性に関する他の要件を強要すべきではない(SHOULD NOT)．その理由は付録Aの *記憶シークレットの強度*に説明してある．

#### **記憶シークレットの検証者**

検証者は，加入者が選択した記憶シークレットの長さが最低8文字であることを要求しなければならない (SHALL)．検証者は，加入者が選択した記憶シークレットに最低64文字を許可すべきである(SHOULD)．すべての印字可能なASCII [RFC 20] 文字(スペースも同様)は記憶シークレットに使用できるべきである(SHOULD)．Unicode[ISO/ISC 10646]文字も同様に使用できるべきである(SHOULD)．検証者は，検証結果が8文字以上であれば, タイプミスを考慮して, 検証の前に連続した空白文字を１つの空白文字に置き換えてもよい (MAY)．シークレットの切り詰めを実施してはならない(SHALL NOT)．前述の長さ要件を満たすために，それぞれのUnicodeのコードポイントは１文字としてカウントされなければならない(SHALL)．

Unicode文字が記憶シークレットで使用できる場合，検証者は Unicode Standard Annex 15 [UAX 15] の セクション 12.1で定義されている”Stablized Strings”のためのNFKCまたはNFKD正規化のいずれかを用いた正規化処理を適用すべきである(SHOULD)．この処理は記憶シークレットを表すバイト文字列のハッシュ化の前に適用される．Unicode文字を含む記憶シークレットを選択した加入者は，一部のエンドポイントでは異なって表示されるかも知れない文字があることと，それが認証に影響する可能性があることを警告されるべきである(SHOULD)．

CSP(登録時など)や検証者(ユーザーが新しいPINを要求する時など) によりランダムに選択される記憶シークレットは，長さが最低6文字でなければならず(SHALL)，承認された乱数生成器[SP 800-90Ar1] を利用して生成されなければならない(SHALL)．

記憶シークレットの検証者は，未認証の認証要求者がアクセスできる “ヒント” を加入者が保管することを許可してはならない (SHALL NOT)．検証者は加入者が記憶シークレットを選択する際，特定のタイプの情報（”最初のペットの名前はなんですか？” など）の使用を促してはならない (SHALL NOT)．

検証者は記憶シークレットの設定と変更の要求を処理するとき，候補となっているシークレットの値を，一般的に利用されている値，予想されうる値，危殆化した値として知られている値を含むリストと比較しなければならない (SHALL)．例えば，リストには以下を含めてもよいが(MAY)，それに限 定するものではない:

* 過去に漏洩した語彙集から得られるパスワード
* 辞書に含まれる言葉
* 繰り返しや連続文字 (例：‘aaaaaa’，’1234abcd’)
* サービス名，ユーザー名，そこから派生するような，文脈で特定可能な単語

選択したシークレットがリストにある場合，CSPまたは検証者は加入者に別のシークレットを選ぶ必要があることを知らせ，その拒否理由を説明し，加入者が別の値を選択するようにしなければならない (SHALL)．

検証者はユーザーが強力な記憶シークレットを選択するのを支援するために，パスワード強度メーター [メーター] といったガイダンスを加入者に提供すべきである(SHOULD)．これは上記リストに載っている記憶シークレット[ブラックリスト]を拒否した後に特に重要で，拒否された記憶シークレットをわずかに手直しするだけでは十分でないと加入者に知らせることになる．

検証者は, セクション 5.2.2に説明してあるように加入者のアカウントにおける認証失敗回数を効果的に制限する仕組みを実装しなければならない (SHALL)．

検証者は記憶シークレットに対して他の構成ルール(異なる文字種の組み合わせの要求や，文字の繰り返しの禁止など)を強要すべきではない(SHOULD NOT)．検証者は，記憶シークレットを任意で(例えば定期的に)変更するよう要求すべきではない(SHOULD NOT)．しかし, 認証コードが危殆化した証拠がある場合は，変更を強制しなければならない (SHALL)．

検証者は, 認証要求者が記憶シークレットを入力するときに”貼り付け”機能を利用できるようにすべきである(SHOULD)．これは, 広く普及しているパスワードマネージャの使用を促進し, 多くの場合ユーザーがさらに強力な記憶シークレットを選択する可能性を高める．

認証要求者が記憶シークレットを正しく入力できるように，検証者は入力をドットやアスタリスクで表示するのではなく，入力が終わるまでシークレットを表示するオプションを提供すべきである(SHOULD)．これにより，認証要求者は画面が盗み見られる可能性が低い場所にいる場合に，入力内容を確認することができる．また検証者は，正しく入力していることをユーザーが確認できるように, デバイスが入力後の文字を短時間表示することを許可してもよい(MAY)．これは特に モバイルデバイスに当てはまる．

検証者は記憶シークレットを要求するときに盗聴と中間者攻撃を防ぐために, 承認された暗号化技術と認証済み保護チャネルを使用しなければならない(SHALL)．

検証者は，オフライン攻撃に耐性がある形で記憶シークレットを保存しなければならない (SHALL)．記憶シークレットは，ソルトを追加したうえで適切な一方向の鍵導出関数を利用してハッシュされなければならない(SHALL)，鍵導出関数は，パスワード，ソルト，コスト要因を入力値としてパスワードハッシュを生成する．その目的は, パスワードハッシュファイルを入手した攻撃者によるパスワードの推測を高くつくものにし, 類推攻撃がコストに見合わないようにすることにある. 適切な鍵導出関数の例としてPassword-based Key Derivation Function 2 (PBKDF2) [SP800-132]とBalloon [BALLOON]がある．攻撃コストを高くするには多量のメモリを必要とする関数を利用すべきである(SHOULD)．鍵導出関数は承認済みの一方向関数を使用しなければならない(SHALL). 例えば，Keyed Hash Message Authentication Code (HMAC) [FIPS 198-1]，SP 800-107 の承認済みハ ッ シ ュ関 数，Secure Hash Algorithm 3 (SHA-3) [FIPS 202]，CMAC [SP 800-38B]，Keccak Message Authentication Code (KMAC)，Customizable SHAKE (cSHAKE)，ParallelHash [SP 800-185]などがある．鍵導出関数から選択する出力の長さは，元となる一方向関数の出力と長さが同じであるべきである(SHOULD)．

ソルトは少なくとも32ビットの長さで，保存されたハッシュ間でソルト値の衝突が最小化されるように恣意的に選択されなければならない(SHALL)．ソルト値と結果のハッシュはいずれも記憶シークレット認証コードを利用して加入者ごとに保存されなければならない(SHALL)．

PBKDF2ではコスト要因は繰り返し回数である. PBKDF2関数の繰り返し回数が増えれば増えるほど，パスワードハッシュの計算時間が長くなる．したがって，繰り返し回数は検証サーバの性能が許す限り大きくするべきであり(SHOULD)，最低でも10,000回が目安になる．

これに加え，検証者は自分だけが知っている秘密のソルト値を使用して鍵導出関数の適用を追加で繰り返すべきである(SHOULD)．このソルト値を使用する場合, 承認済み乱数生成器 [SP800-90Ar1]を利用して生成し，少なくともSP 800-131Aの最新版で指定されている最低限のセキュリティ強度(本書の公開時点では112ビット)を備えなければならない(SHALL)． この秘密のソルト値は，ハッシュ化された記憶シークレットとは別に(例えば，ハードウェアセキュリティモジュールなどの特別なデバイスに)保存されなければならない(SHALL)．この追加の繰り返しにより，シークレットソルト値が秘密である限り，ハッシュされた記憶シークレットに対するブルートフォース攻撃は不可能になる．

#### **ルックアップシークレット**

#### ルックアップシークレット認証コードは, 認証要求者と CSP の間で共有するシークレットのセットを保管する物理的または電子的記録である. 認証要求者は, 検証者からの要求に応えるのに必要な適切なシークレットを調べるために認証コードを使用する. 例えば, 検証者は認証要求者に対し, カードに表形式で印刷された数字か文字列の特定のサブセットを求める場合がある. ルックアップシークレットの一般的な応用は, 別の認証コードを紛失したり不具合があったりする場合に備えて加入者が保管する "回復キー" である。ルックアップシークレットは, *本人が持っているもの*である.

* + - 1. **ルックアップシークレット認証コード**

ルックアップシークレット認証コードを生成する CSP は，承認済みの乱数生成器 [SP 800-90Ar1] を用いてシークレットのリストを生成し，加入者に認証コードを安全に届けなければならない(SHALL)．ルックアップシークレットは最低20ビットのエントロピーを持たなければならない(SHALL)．

ルックアップシークレットは，CSPによる対面，加入者の記録上の住所への郵送またはオンラインで配布してもよい(MAY)，オンラインの場合は，セクション 6.1.2の登録後の結び付け要件を満たすセキュアなチャネルで配布しなければならない(SHALL)．

認証コードがリストから連続してルックアップシークレットを使用する場合，加入者は使用したシークレットを破棄してもよい(MAY)．ただし, 認証に成功した後に限られる.

#### **ルックアップシークレットの検証者**

ルックアップシークレットの検証者は, 認証要求者が使用する認証コードから得られる次のシーク レットか，特定の(例えば番号の付けられた)シークレットの入力を促さなければならない(SHALL)．認証コードから得られるシークレットが正常に使用できるのは, １回だけでなければならない(SHALL)．ルックアップシークレットが表形式のカードから得られる場合は，それぞれのセルの使用は１回だけでなければならない (SHALL)．

検証者は，オフライン攻撃に対抗できる形でルックアップシークレットを保存しなければならない (SHALL)．112ビット以上のエントロピーを持ったルックアップシークレットは，セクション 5.1.1.2に説明してあるように承認済みの一方向関数でハッシュ化されなければならない(SHALL)．エントロピーが112ビット未満の場合はソルトを追加したうえで適切な一方向の鍵導出関数を用いてハッシュしなければならない(SHALL)．ソルト値は32ビット以上の長さで，保存されたハッシュ間でソルト値の衝突が最小化されるように恣意的に選択されなければならない(SHALL)．ソルト値とその結果のハッシュはいずれもルックアップシークレットに対して保存 されなければならない(SHALL)．

64ビット未満のエントロピーを持つルックアップシークレットでは，検証者はセクション 5.2.2に説明してあるように加入者のアカウントにおける認証失敗回数を効果的に制限する仕組みを実装しなければならない (SHALL)．

検証者はルックアップシークレットを要求するとき, 盗聴と中間者攻撃を防ぐために, 承認された暗号化技術と認証済み保護チャネルを使用しなければならない(SHALL)．

#### **アウトオブバンドデバイス**

アウトオブバンド認証コードは，アドレスで一意に呼び出すことができるセカンダリチャネルと呼ばれる別の通信チャネルを介して検証者と安全に通信できる物理デバイスである．デバイスは認証要求者が所有し管理しており，電子認証のためのプライマリチャネルと分離されたセカンダリチャネルを介したプライベートな通信をサポートしている．アウトオブバンド認証コードは, *本人が持っているもの*である．



アウトオブバンド認証コードは以下の方法の1つで動作する:

* 認証要求者はアウトオブバンドデバイスによってセカンダリチャネルを介して受け取ったシークレットを，プライマリチャネルを使って検証者に送信する．例えば，認証要求者は自身のモバイルデバイスでシークレットを受信し，それ（一般的には数字6桁のコード）を認証セッションで入力できる．
* 認証要求者はプライマリチャネルを介して受け取ったシークレットをアウトオブバンドデバイスに送信し，セカンダリチャネルを介して検証者に送信する．例えば，認証要求者は自身の認証セッション上で確認したシークレットを，モバイルデバイスのアプリケーションに入力したり，バーコードやQRコードといった技術を利用したりして送信できる．
* 認証要求者はプライマリチャネルとセカンダリチャネルから得たシークレットを比較し，セカンダリチャネルを介して認証を確認する．

このシークレットの目的は, プライマリチャネルの認証操作をセカンダリチャネルに安全に結び付けることである．レスポンスがプライマリチャネルを介すると，シークレットはアウトオブバンドデバイスを認証要求者が管理していることの証明にもなる．

#### **アウトオブバンド認証コード**

アウトオブバンド認証コードは, アウトオブバンドシークレットや認証リクエストを取得するために検証者と個別の通信チャネルを確立しなければならない (SHALL)．このチャネルは, 認証要求者の認可なしに１つのチャネルから別のチャネルに情報が漏洩しないデバイスであれば,　プライマリ通信チャネルに対して(同じデバイスに接続されている場合でさえも)アウトオブバンドと見なされる.

アウトオブバンドデバイスは一意にアドレスで呼び出すことができるべきで(SHOULD)，セカンダリチャネルを介した通信は，公衆交換電話網(PSTN)を使用するのでなければ暗号化されなければならない(SHALL)．PSTNに固有な追加の認証コード要件に対しては，セクション 5.1.3.3を参照．IP電話 (VoIP)やEメールなどのように特定のデバイスの所有が証明されない方式は，アウトオブバンド認証で使用してはならない (SHALL NOT)．

アウトオブバンド認証コードは，検証者との通信において以下の方法の1つを用いて，自身を一意に認証しなければならない (SHALL):

* 承認済みの暗号化技術を利用し,認証済み保護チャネルを検証者に対して確立する．使用する鍵は. 認証コードアプリケーションが利用できる適切でセキュアなストレージ(例:キーチェーンストレージ，TPM，TEE，セキュアエレメント)に保管されなければならない(SHALL)．
* 一意にデバイスを識別するSIMカードやそれに相当する方法を用いて公衆携帯電話網に対して認証する．この方法が使用できるのは, PSTN(SMSまたは音声)を介してシークレットが検証者からアウトオブバンドデバイスに送信される場合に限らなければならない(SHALL)．

検証者からアウトオブバンドデバイスにシークレットが送信される場合，デバイスは所 有者によってロックされている(例えば, PINやパスコードの入力や生体認証が必要)間は認証シークレットを表示すべきではない(SHOULD NOT)．とはいえ, 認証コードはロックされたデバイス上で認証シークレットの受信を表示すべきである(SHOULD)．

受け取ったシークレットをプライマリ通信チャネルに送信する認証要求者によってではなく,アウトオブバンド認証コードがセカンダリ通信チャネルを介して承認メッセージを送信する場合は,次のうち1つを実施しなければならない (SHALL):

* 認証コードはプライマリチャネルから得たシークレットを転送することを許可し，認証トランザクションと承認を関連付けるためにセカンダリチャネルを介して検証者に送信しなければならない (SHALL)．認証要求者は手動で送信するか，バーコードやQRコードといった技術を利用して送信してもよい(MAY)．
* 認証コードはセカンダリチャネルを介して検証者から受け取ったシークレットを提示し，認証要求者にプライマリチャネルとシークレットとの整合性を検証するよう促し，認証要求者から受けた「はい/いいえ」の応答を検証者に送信しなければならない (SHALL)．

#### **アウトオブバンドの検証者**

PSTNに特有の追加の検証要件は，セクション 5.1.3.3を参照．

アウトオブバンド検証がセキュアなアプリケーション（例えばスマートフォンのアプリ）を利用して行われる場合，検証者はデバイスにプッシュ通知を行ってもよい(MAY)．検証者は認証済み保護チャネルの確立を待ち，認証コードの識別キーを検証する．認証コードは識別キー自体を保管してはならないが (SHALL NOT)，認証コードを一意に識別するための検証方法(例えば, 承認済みのハッシュ関数や，識別キーの所持証明)を用いなければならない(SHALL)．検証が終わったら検証者は認証シークレットを認証コードに送信 する．

アウトオブバンド認証コードのタイプに応じて，以下のうち1つを実施しなければならない (SHALL):

* シークレットをプライマリチャネルに送信: 検証者は加入者の認証コードを持つデバイスに対して認証の準備ができたことを示すシグナルを送信してもよい(MAY)．次に，アウトオブバンド認証コードにランダムなシークレットを送信しなければならない (SHALL)．検証者 はプライマリ通信チャネルでシークレットが送り返されるのを待たなければならない(SHALL)．
* シークレットをセカンダリチャネルに送出: 検証者はランダムな認証シークレットをプライマリチャネル経由で認証要求者に表示しなければならない (SHALL)．次に，認証要求者のアウトオブバンド認証コードからセカンダリチャネルでシークレットが送り返されるのを待たなければならない (SHALL)．
* 認証要求者によるシークレットの検証: 検証者はランダムな認証シークレットをプライマリチャネル経由で認証要求者に表示しなければならず(SHALL)，セカンダリチャネルを介してアウトオブバンド認証コードに同じシークレットを送信して認証要求者に提示しなければならない (SHALL)．次に，セカンダリチャネルを介して送られてくる承認(または非承認)メッセージを待たなければならない(SHALL)．

すべてのケースにおいて，10分以内に完了しない認証は無効と見なさなければならない (SHALL)．セクション 5.2.8に説明してあるようにリプレイ攻撃に対抗するために，検証者が確認期間中に受け取る所定の認証シークレットは１回だけでなければならない (SHALL)．

検証者は，承認済みの乱数生成器 [SP 800-90Ar1] を用いて少なくとも20ビットのエントロピーでランダムな認証シークレットを生成しなければならない (SHALL)．認証シークレットが64 ビット未満のエントロピーの場合は，検証者はセクション 5.2.2に説明してあるように加入者のアカウントにおける認証失敗回数を効果的に制限する仕組みを実装しなければならない (SHALL)．

#### **公衆交換電話網を利用する認証**

アウトオブバンドでの検証を目的としたPSTNの利用は，このセクションとセクション 5.2.10 にあるように制限される．アウトオブバンドでの検証にPSTNを利用する場合は，検証者は使用する事前登録済みの電話番号が特定の物理デバイスに結び付けられていることを検証しなければならない (SHALL)．事前登録済みの電話番号の変更は新しい認証コードの結び付けとみなされ，セクション 6.1.2 に説明されている場合に限られなければならない (SHALL)．

検証者は，アウトオブバンド認証シークレットの配送にPSTNを使用する前に, デバイスの交換，SIMの変更，電話番号の移行，その他の異常な作動といったリスク指標を考慮すべきである(SHOULD)．

注意: NIST はセクション 5.2.10 の認証コードの制約と整合性を保つために, 脅威の拡大と PSTN の技術的操作に基づいて PSTN の制限ステータスを調整できる.

#### **単一ファクタOTPデバイス**

#### 単一ファクタ OTP デバイスは OTP を生成する. このカテゴリーにはハードウェアデバイスと, 携帯電話などのデバイスにインストールされたソフトウェアベースの OTP 生成装置が含まれる. こうしたデバイスは, OTP の生成元として使用される埋込型シークレットを備えているが, ２番目のファクタを使用したアクティベーションを必要としない. OTP はデバイスに表示され, 手動で入力されてから検証者に送信される. これにより, デバイスの所有と管理が証明される. 例えば, OTP デバイスは一度に６文字を表示できる. 単一ファクタ OTP デバイスは自分か持っているものである.

単一ファクタOTPデバイスはルックアップシークレット認証コードと同じであるが，シークレットは暗号理論に基づいて独立して認証コードと検証者によって生成され，検証者によって比較されるという点が異なる．シークレットは，時間ベースのノンスまたは認証コードと検証者のカウンタに基づいて計算される

* + - 1. **単一ファクタOTP 認証コード**

単一ファクタOTP認証コードは2つの永続的な値を含む.1つ目はデバイスが有効な限り存続し続ける対象鍵であり, 2つ目は認証コードが使用されるたびに変化するか実時間時計に基づいて変化するノンスである.

秘密鍵とそのアルゴリズムは少なくともSP800-131Aの最新版で定義された最低限のセキュリティ強度（本書の公開時点では112ビット）でなければならない(SHALL)．ノンスは，デバイスの有効期間にわたり操作されるたびに確実に一意な値になるように十分長くなければならない (SHALL). OTP 認証コードは, 特にソフトウェアベースのOTP生成装置の場合は, 複数のデバイスに対して秘密鍵を複製できないようにすべきであり(SHOULD)，容易に複製させてはならない(SHALL NOT)．

認証コード出力値を得るには，セキュアな方法で鍵とノンスとを安全な方法で組み合わせるために，承認されたブロック暗号かハッシュ関数を使用する．認証コード出力値は６桁の数字 (およそ20ビットのエントロピー)になるよう切り詰めてもよい(MAY).

認証コード出力値の生成に利用するノンスが実時間時計をベースとしている場合，ノンスは少なくとも2分ごとに変化しなければならない (SHALL). 所定のノンスと関連するOTP値の受け入れは一度だけでなければならない(SHALL).

#### **単一ファクタOTP の検証者**

単一ファクタOTP の検証者は，認証コードが使用するOTPの生成プロセスを実質的に再現する．したがって，認証コードが使用する対称鍵も検証者が所持しており，改竄に対して強力に保護されていなければならない (SHALL)．

単一ファクタOTP 認証コードが加入者アカウントに関連付けられているとき，検証者または関連するCSPは，認証コードの出力値を再現するために必要なシークレットを生成，交換または取得するために, 承認された暗号化技術を使用しなければならない (SHALL)．

検証者は，OTPを収集する際に盗聴や中間者攻撃に対抗するため，承認された暗号化技術と認証済み保護チャネルを利用しなければならない (SHALL)．時間ベースのOTP[RFC 6238] には，決められた有効期間がなければならず (SHALL)，認証コードの有効期間で予測される時間のズレ（何れかの方向）と, ネットワーク遅延とユーザーによるOTP入力の許容時間を加えて決定される．セクション 5.2.8に記述されているリプレイ耐性を備えるため，検証者が所定の時間ベースのOTPを有効期間内に受け取れるのは一度だけにしなければならない(SHALL)．

認証コード出力値が64ビット未満のエントロピーの場合は，検証者はセクション 5.2.2に説明してあるように，加入者のアカウントにおける認証失敗回数を効果的に制限する仕組みを実装しなければならない(SHALL)．

#### **マルチファクタ OTP デバイス**

#### マルチファクタ OTP デバイスは, アクティベーション後に追加の認証ファクタを使用した認証で使用するための OTP を生成する. これにはハードウェアデバイスと, 携帯電話などのデバイスにインストールされたソフトウェアベースの OTP 生成装置が含まれる.認証の２つ目のファクタは, 同じ種類の統合型入力パット, 統合型生体情報 (指紋など) リーダー, コンピュータの直接的なインタフェース (USBポートなど) を通して認証を行う.OTP はデバイスに表示され, 手動で入力されてから検証者に送信される. 例えば, OTP デバイスは一度に６文字を表示でき, これにより デバイスの所有と管理が証明される.マルチファクタ OTP デバイスは*本人が持っているもの*であり, 本人が知っていることか本人の特徴であるもののどちらかで有効にしなければならない (SHALL).

* + - 1. **マルチファクタOTP 認証コード**

マルチファクタOTP 認証コードは，認証コードから OTP を得るために記憶シークレットの入力または生体認証の利用を要求する点を除くと，単一ファクタOTP 認証コード(セクション 5.1.4.1参照)と同じ方法で機能する．認証コードを使用するたびに追加ファクタの入力を要求しなければならない (SHALL)．

アクティベーション情報に加えて，マルチファクタOTP 認証コードは2つの永続的な値を含んでいる．1つ目はデバイスが有効な限り永続する対称鍵である．2つ目は認証コードが使用されるたびに変化するか実時間時計に基づいて変化するノンスである.

秘密鍵とそのアルゴリズムは少なくともSP800-131Aの最新版で定義された最低限のセキュリティ強度（本書の公開時点では112ビット）でなければならない(SHALL)．ノンスは，デバイスの有効期間にわたりデバイスが操作されるたびに確実に一意の値になるために十分長くなければならない (SHALL). OTP 認証コードは, 特にソフトウェアベースのOTP生成装置の場合は, 複数のデバイスに対して秘密鍵を複製できないようにすべきであり(SHOULD)，容易に複製させてはならない(SHALL NOT)．

認証コード出力値を得るには，セキュアな方法で鍵とノンスとを安全な方法で組み合わせるために，承認されたブロック暗号かハッシュ関数を使用する．認証コード出力値は６桁の数字 (およそ20ビットのエントロピー)になるよう切り詰めてもよい(MAY).

認証コード出力値の生成に利用するノンスが実時間時計をベースとしている場合，ノンスは少なくとも2分ごとに変化しなければならない (SHALL). 所定のノンスと関連するOTP値の受け入れは一度だけにしなければならない(SHALL)

認証コードがアクティベーションに使用するどのような記憶シークレットも，ランダムに選ばれた最 低6文字の数字シークレットか, セクション 5.1.1.2 の要件を満たすその他の記憶シークレットでなければならない(SHALL). そして，セクション 5.2.2に指定してあるように認証失敗回数が制限されなければならない (SHALL)．生体認証を有効にするファクタは，連続して認証に失敗する回数制限を含めセクション 5.2.3の要件を満たさなければならない (SHALL).

暗号化されていない鍵とアクティベーションシークレット，または生体認証サンプル（そして, 信号処理により生成されたプローブのような生体認証サンプルに由来する任意の生体認証データ）は，OTP の生成が終わると直ちにゼロ埋めされなければならない(SHALL)．

#### **マルチファクタOTP の検証者**

マルチファクタOTP の検証者は，認証コードが使用するOTPの生成プロセスを実質的に再現するが，２つ目のファクタを要求しない．したがって，認証コードが使用する対称鍵は改竄に対して強力に保護されていなければならない (SHALL)．

マルチファクタOTP 認証コードが加入者アカウントに関連付けられていると，検証者または関連するCSPは，認証コードの出力値を再現するために必要なシークレットを生成，交換または取得するために承認された暗号化技術を使用しなければならない (SHALL)．検証者またはCSPは，認証コードのソースを経由して，認証コードがマルチファクタデバイスであることも確認しなければならない (SHALL)．それがマルチファクタデバイスであるという信頼できる主張がない場合、検証者はセクション 5.1.4に従い認証コードを単一ファクタとして扱わなければならない(SHALL)．

検証者は，OTPを収集する際の盗聴や中間者攻撃に対抗するために，承認された暗号化技術と認証済み保護チャネルを利用しなければならない (SHALL)．時間ベースのOTP[RFC 6238] には，決められた有効期間がなければならず (SHALL)，認証コードの有効期間にわたり予想される時間のズレ（何れかの方向）と, ネットワーク遅延とユーザーによるOTP入力の許容時間を加えて決定される．セクション 5.2.8に記述されているリプレイ耐性を備えるため，検証者が所定の時間ベースのOTPを有効期間内に受け取れるのは一度だけにしなければならない(SHALL)．OTPの使い回しにより認証要求者の認証が拒否される場合には，検証者は攻撃者が先に認証できる可能性を認証要求者に警告してもよい(MAY)．検証者は，OTPの使い回しが試みられた既存のセッションの加入者にも警告してもよい(MAY)．

認証コード出力値が64ビット未満のエントロピーの場合は，検証者はセクション 5.2.2に記述してあるように，加入者のアカウントにおける認証失敗回数を効果的に制限する仕組みを実装しなければならない(SHALL)．生体認証のアクティベーションファクタは，連続して認証に失敗する回数制限を含めセクション 5.2.3の要件を満たさなければならない (SHALL).

#### **5.1.6 単一ファクタ暗号化ソフトウェア**

#### 単一ファクタソフトウェア暗号認証コードは, ディスクやその他の "ソフトな" メディアに保管される暗号鍵である. この鍵の所有と管理を証明することにより認証が完了する. 認証コード出力値は特定の暗号プロトコルに大きく左右されるが, 一般的にはある種の署名付きメッセージである. 単一ファクタソフトウェア暗号認証コードは, *本人が持っているもの*である.

* + - 1. **単一ファクタ暗号化ソフトウェアの認証コード**

単一ファクタ暗号化ソフトウェアの認証コードは、認証コードに対して一意の１つまたは複数の秘密鍵を格納している．鍵は認証コードアプリケーションが利用できる適切でセキュアなストレージ（例:キーチェーンストレージ，TPM，または利用可能であれば TEE）に保管されなければならない (SHALL)．アクセスを要求するデバイス上のこうしたソフトウェアコンポーネントにのみ鍵へのアクセスを許可するアクセス制御を使用し、不正な開示から鍵を強力に保護しなければならない(SHALL)．単一ファクタ暗号化ソフトウェア認証コードは，複数のデバイスに対して秘密鍵を複製できないようにすべきであり(SHOULD)，容易に複製させてはならない(SHALL NOT)．

#### **単一ファクタ暗号化ソフトウェアの検証者**

単一ファクタ暗号化ソフトウェアの検証者に対する要件は，セクション 5.1.7.2 に記述されている単一ファクタ暗号化デバイスの検証者に対する要件と同じである．

#### **単一ファクタ暗号化デバイス**

#### 単一ファクタ暗号化デバイスは. 保護された暗号鍵を使用して暗号化を行うハードウェアデバイスで, 直接的な接続を通して認証コード出力値をユーザーのエンドポイントに提供する. デバイスは埋込型の対称または非対称暗号鍵を使用し, ２番目の認証ファクタを用いたアクティベーションは要求されない. 認証プロトコルを通してデバイスの所有を証明すると認証が完了する. 認証コード出力値は, ユーザーのエンドポイントに直接接続して提供され, 特定の暗号プロトコルに大きく左右されるが, 一般的にはある種の署名付きメッセージである. 単一ファクタ暗号化デバイスは, *本人が持っているもの*である.

#### **単一ファクタ暗号化デバイスの認証コード**

単一ファクタ暗号化デバイスの認証コードは１つまたは複数の秘密鍵を格納しており，その鍵はデバイスに対して一意であり, エクスポート（つまり, デバイスから削除）できてはならない (SHALL NOT)．認証コードは，通常はUSBポートなどのコンピュータの直接的なインタフェー スを介して提供されるチャレンジノンスに署名することによって機能する．または, 認証コードは, ユーザーのエンドポイントと統合された適切でセキュアな処理装置になることもできよう（例えばハードウェア TPM）. 暗号化デバイスはソフトウェアを含んでいるが，すべての組込みソフトウェアがCSPまたは発行者の管理下にあるという点と，認証コード全体が認証時のAALにおける適用可能なすべてのFIPS 140要件の対象になる点において，暗号化ソフトウェアの認証コードとは異なる．

秘密鍵とそのアルゴリズムは, SP 800-131Aの最新版で定義された最低限のセキュリティ強度（本書の刊行時点では112ビット）を少なくとも提供しなければならない(SHALL)．チャレンジノンスは少なくとも64ビット長でなければならない(SHALL)．承認された暗号化技術が利用されなければならない(SHALL)．

単一ファクタ暗号化デバイス認証コードが機能するには, ボタンを押すなどの物理的な入力が必要となるべきである(SHOULD)．これにより，デバイスが接続しているエンドポイントがセキュリティ侵害を受けている場合に起こりうる意図しない動作が防止される.

#### **単一ファクタ暗号化デバイスの検証者**

単一ファクタ暗号化デバイスの検証者は, チャレンジノンスを生成して対応する認証コードに送信し, 認証コード出力値を利用してデバイスの所有を検証する．認証コード出力値は特定の暗号化デバイスとプロトコルに大きく依存するが，一般的にはある種の署名付きメッセージである．

検証者は，各認証コードに対応する対称か非対称のどちらかの暗号鍵を保管している．どちらのタイプの鍵も改竄に対して保護されていなければならない(SHALL) が，対象鍵は不正な開示に対して追加保護が取られなければならない (SHALL)．

チャレンジノンスは少なくとも64ビット長でなければならず(SHALL)，認証コードの有効期間を通じて一 意であるか，統計的に一意(つまり，承認された乱数生成器[SP 800-90Ar1]を用いて生成)でなければならない(SHALL)．承認された暗号化技術が利用されなければならない(SHALL)．

#### **マルチファクタ暗号化ソフトウェア**

#### 

#### マルチファクタソフトウェア暗号認証コードは, ２番目の認証ファクタを用いてアクティベーションが必要なディスクやその他の "ソフトな" メディアに保管される暗号鍵である. この鍵の所有と管理を証明することにより認証が完了する.認証コード出力値は特定の暗号プロトコルに大きく左右されるが, 一般的にはある種の署名付きメッセージである. マルチファクタソフトウェア暗号認証コードは*本人が持っているもの*であり, *本人が知っていること*か*本人の特徴であるもの*のどちらかを用いてアクティベートされなければならない (SHALL).

#### **マルチファクタ暗号化ソフトウェアの認証コード**

マルチファクタ暗号化ソフトウェアの認証コードは秘密鍵を１つまたは複数格納しており，その鍵はデバイスに対して一意で記憶シークレットか生体認証のどちらかの追加ファクタの入力があるときだけアクセスできる．鍵は認証コードアプリケーションが利用できる適切でセキュアなストレージ(例:キーチェーンストレージ，TPM，TEE)に保管されるべきである(SHOULD)．アクセスを要求するデバイス上のこうしたソフトウェアコンポーネントにのみ鍵へのアクセスを許可するアクセス制御を使用し、不正な開示から鍵を強力に保護しなければならない(SHALL)．マルチファクタ暗号化ソフトウェア認証コードは，複数のデバイスに対して秘密鍵を複製できないようにすべきであり(SHOULD)，容易に複製させてはならない(SHALL NOT)．

認証コードを用いた各認証操作には, 両方のファクタの入力を必要としなければならない (SHALL)．

認証コードがアクティベーションに使用するどのような記憶シークレットも，ランダムに選ばれた最 低6文字の数字シークレットか, セクション 5.1.1.2 の要件を満たすその他の記憶シークレットでなければならない(SHALL). そして，セクション 5.2.2に指定してあるように認証失敗回数が制限されなければならない (SHALL)．生体認証のアクティベーションファクタは，連続して認証に失敗する回数制限を含めセクション 5.2.3の要件を満たさなければならない (SHALL).

暗号化されていない鍵とアクティベーションシークレット，または生体認証サンプル（そして, 信号処理により生成されたプローブのような生体認証サンプルに由来する任意の生体認証データ）は，認証トランザクションが終わると直ちにゼロ埋めされなければならない(SHALL)．

#### **マルチファクタ暗号化ソフトウェアの検証者**

マルチファクタ暗号化ソフトウェアの検証者に対する要件は，セクション 5.1.7.2 に記述されている単一ファクタ暗号化デバイスの検証者に対する要件と同じである．マルチファクタ暗号化ソフトウェア認証コード出力を検証することで，アクティベーションファクタの使用が証明される．

#### **マルチファクタ暗号化デバイス**

#### マルチファクタ暗号化デバイスは. 保護された暗号鍵の１つまたは複数を使用して暗号化を行うハードウェアデバイスで, ２番目の認証ファクタを用いたアクティベーションを必要とする. デバイスの所有と鍵の管理を証明すると認証が完了する. 認証コード出力値は, ユーザーのエンドポイントに直接接続して提供され, 特定の暗号プロトコルに大きく左右されるが, 一般的にはある種の署名メッセージである. マルチファクタ暗号化デバイスは*本人が持っているもの*であり, *本人が知っていること*か*本人の特徴であるもの*のどちらかを用いて有効にされなければならない (SHALL).

#### **マルチファクタ暗号化デバイスの認証コード**

マルチファクタ暗号化デバイスの認証コードは, 改竄耐性を備えたハードウェアを用いて１つまたは複数の秘密鍵を格納しており，その鍵はデバイスに対して一意で記憶シークレットか生体認証のどちらかの追加ファクタの入力があるときに限りアクセスできる．認証コードは，通常はUSBポートなどのコンピュータの直接的なインタフェー スを介して提供されるチャレンジノンスに署名することによって機能する．または, 認証コードは, ユーザーのエンドポイントと統合された適切でセキュアな処理装置になることもできよう (例えばハードウェア TPM). 暗号化デバイスはソフトウェアを含んでいるが，すべての組込みソフトウェアがCSPまたは発行者の管理下にあるという点と，認証コード全体が認証時のAALにおける適用可能なすべてのFIPS 140要件の対象になる点において，暗号化ソフトウェアの認証コードとは異なる．

秘密鍵とそのアルゴリズムは, SP 800-131Aの最新版で定義された最低限のセキュリティ強度(本書の刊行時点では112ビット)を少なくとも提供しなければならない(SHALL)．チャレンジノンスは少なくとも64ビット長でなければならない(SHALL)．承認された暗号化技術が使用されなければならない(SHALL)．

認証コードを用いたそれぞれの認証操作には追加ファクタの入力を必要とすべきである(SOULD)． 追加ファクタの入力は，デバイスに直接入力するかハードウェア接続(USBやスマートカードなど)を用いてもよい(MAY)．

認証コードがアクティベーションに使用するどのような記憶シークレットも，ランダムに選ばれた最 低6文字の数字シークレットか, セクション 5.1.1.2 の要件を満たすその他の記憶シークレットでなければならない(SHALL). そして，セクション 5.2.2に指定してあるように認証失敗回数が制限されなければならない (SHALL)．生体認証のアクティベーションファクタは，連続して認証に失敗する回数制限を含めセクション 5.2.3の要件を満たさなければならない (SHALL).

暗号化されていない鍵とアクティベーションシークレット，または生体認証サンプル（そして, 信号処理により生成されたプローブのような生体認証サンプルに由来する任意の生体認証データ）は，認証トランザクションが終わると直ちにゼロ埋めされなければならない(SHALL)．

#### **マルチファクタ暗号化デバイスの検証者**

マルチファクタ暗号化デバイス検証者に対する要件は，セクション 5.1.7.2 に記述されている単一ファクタ暗号化デバイスの検証者に対する要件と同じである．マルチファクタ暗号化デバイスの認証コード出力を検証することにより，アクティベーションファクタの使用が証明される．

#### **認証コードの一般要件**

#### 以下のサブセクションで, 認証コードの一般要件について説明する.

* + 1. **物理的認証コード**

CSPは加入者に対し，認証コードの盗難や紛失を適切に防止する方法について指示しなければならない (SHALL)．CSPは加入者から認証コードの盗難や紛失の疑いがあると通知を受けると直ちに認証コードを無効化または停止する措置を講じなければならない (SHALL)．

#### **回数制限（スロットリング）**

セクション 5.1の認証コードタイプの説明に当てはまる場合，検証者はオンライン推測攻撃に対抗するための管理策を実装しなければならない (SHALL)．所定の認証コードの説明に別のように記されていない場合に限り，検証者は同じアカウントで認証に連続して失敗できる回数を100回に制限をしなければならない (SHALL)．

回数制限の結果として攻撃者が正しい認証要求者を締め出す確立を低下させるために, 以下のような追加のテクニックを用いてもよい(MAY)．

* 認証要求者が認証を行う前にCAPTCHAの入力を要求する．
* 認証要求者が認証に失敗したら一定時間待つことを要求する. 連続して失敗する許容回数に近づくにつれて時間を長くする（例えば30秒から1時間まで）．
* 加入者が以前に正常に認証したIPアドレスのホワイトリストに由来する認証要求だけを受け入れる．
* ユーザーの行為が通常の範疇にあるかないかを特定するリスクベースまたは適応型認証テクニックを活用する．

加入者が認証に成功したら，検証者は同じIPアドレスのユーザーが以前に失敗した試みを無視すべきである(SHOULD)．

* + 1. **生体認証の利用**

認証における生体情報（*本人の特徴であるもの*)の利用には，物理的な特性(指紋，虹彩，顔の特徴など)と動作特性（入力のリズムなど）の測定がある．両方とも生体認証の方法と見なされるが, 他の方法はセクション 5.2.9に説明されているように認証意図を確認する範囲の点で異なる場合がある.

この文書では, 以下のようなさまざまな理由から, 認証に生体認証を限定的に利用することを支持する．

* 生体認証の誤合致率 (FMR)は，それ自身では加入者の認証に確実性を与えない．さらに，FMRはなりすまし攻撃を考慮していない．
* 生体認証の比較は確率論的だが，他の認証ファクタは決定論的である．
* 生体認証のテンプレート保護スキームには，他の認証ファクタ（PKI証明書とパスワードなど）と同じように生体認証情報を無効にする手段がある．しかし，そのようなソリューションの有効性は限られており，そうした手段を試験するための標準も策定中の段階である．
* 生体認証の特性はシークレットにはならない．それらはオンラインで取得したり，了解の上か無断で携帯電話のカメラで誰かの写真（例えば顔）を撮ったり，誰かが 触った物から採取したり（例えば指紋），高精細な画像から入手したりできる（例えば虹彩パターン）．生体検知のようなプレゼンテーション検出 (PAD) 技術は，これらのタイプの攻撃リスクを緩和できるが，PAD がCSPと加入者のニーズに合うように機能していることを保証するために,　センサーや生体認証処理に信頼性を持たせることが追加で必要になる．

したがって，認証における制限された生体認証の使用は，以下の要件とガイドラインの下で支持される:

生体認証は物理的な認証コード(*本人が持っているもの*)を用いたマルチファクタ認証の一部としてのみ使用されなければならない(SHALL)．

センサー（または取り替えできないセンサーがあるエンドポイント）と検証者の間の認証済み保護チャネルが確立されなければならず(SHALL)，センサーまたはエンドポイントが設置されなければならず(SHALL)，認証要求者から生体認証サンプルを採取する前に, センサーまたはエンドポイントが認証されなければならない(SHALL)．

生体認証システムは，誤合致率が1000分の1かさらに優れた FMR [ISO/IEC 2382-37]で運用されなければならない(SHALL)．このFMRは, [ISO/IEC 30107-1]で定義されているように合致攻撃Conformant attack(つまり, ゼロエフォートのなりすまし)の条件下で達成されなければならない(SHALL)．

生体認証システムは PADを実装すべきである(SHOULD)．導入する生体認証システムのテストでは，それぞれ関連する攻撃タイプ（つまり人間）のためのプレゼンテーション攻撃に対して少なくとも90%の耐性があることを示すべきである(SHOULD)．ここでの耐性はプレゼンテーション攻撃の回数で割った失敗回数として定義される．プレゼンテーション攻撃耐性のテストは，[ISO/IEC 30107-3]の12条に従い行わなければならない(SHALL)．PADは認証要求者のデバイス上でローカルに実施されても，または中央の検証者によって実施されてもよい(MAY)．

注意: PAD はこのガイドラインの今後の版で必須要件として検討されている.

生体認証システムは, 5回の連続した認証試行の失敗を許容しなければならないが (SHALL), PADが上記の要件を満たして実装されている場合は，その回数は10回でなければならない (SHALL)．一度上限に達すると，生体認証コードは以下のどちらかを実行しなければならない(SHALL):

* 次回の試行までに少なくとも30秒時間を空け，試行回数が増えるたびに指数関数的に増加させる（例えば，その次の試行前に1分，さらに次の試行前に2分）
* すでに利用可能な代替手段があればその生体認証を無効にし，もう１つのファクタ（例えば，異なる生体計測手段や，まだ要求されていないファクタであればPIN/パスコード）を提供する．

検証者はセンサーとエンドポイントのパフォーマンス，一貫性，信憑性を確定しなければならない (SHALL)．確定するために容認できる方法には以下があるが，これに限定されない:

* センサーまたはエンドポイントの認証
* 承認済みの認定機関による保証
* セクション 5.2.4に記述されている署名済みメタデータの実効時の調査(例: アテステーション)

生体情報の比較は, 認証要求者のデバイス上でローカルに実施されるか，中央の検証者で実施される．中央の検証者に対する大規模な攻撃の可能性が増加しつつあるため，ローカルでの比較が好ましい．

比較が中央で実施される場合:

* 認証ファクタとしての生体情報の使用は, 承認された暗号化技術を用いて識別される１つ以上の特定デバイスに限定されなければならない(SHALL)．生体認証がまだメインの認証鍵を解読していないのであれば，別の鍵をデバイスの識別に使用しなければならない (SHALL)．
* ISO/IEC 24745で生体認証テンプレート保護と呼ばれている生体認証情報の破棄を実装しなければならない (SHALL)．
* すべての生体認証情報の送信は, 認証済み保護チャネルを利用しなければならない(SHALL)．

認証プロセスで収集された生体認証サンプルは，比較アルゴリズムの試験目的か, ユーザーの同意を得て別の研究目的に利用してもよい(MAY)．生体認証サンプルとそこから派生する生体データ（信号処理により生成されるプローブなど）は，試験が終わったり研究データが得られたりした後は直ちにゼロ埋めされなければならない(SHALL)．

生体認証は，SP 800-63A（sp800-63a.html）に記述されているように, 登録の否認を防ぐ目的で利用され, そして検証プロセスのすべての段階で同じ個人が参加していることを検証するために利用されるケースもある．

#### **アテステーション**

アテステーションとは，直接接続されている認証コードや認証操作に参加するエンドポイントに関して検証者に伝達される情報のことである．アテステーションにより伝達される情報は次を含んでもよい(MAY)が，これに限定されない:

* 認証コードとエンドポイントの出所（製造元やサプライヤ証明書など），健全性および一貫性
* 認証コードのセキュリティ機能
* 生体認証センサーのセキュリティと性能特性
* センサーの計測手段

このアテステーションに署名する場合は，少なくともSP 800-131Aの最新版で定義された最低限のセキュリティ強度(本書の刊行時点では112ビット)を備えるデジタル署名を用いなければならない(SHALL)．

アテステーション情報は，検証者のリスクベースの認証判断の一部として利用してもよい(MAY)．

* + 1. **検証者なりすまし耐性**

検証者なりすまし攻撃とは，しばしばフィッシング攻撃と呼ばれ，検証者やRPになりすまして不注意な認証要求者を不正なサイトで認証させる試みである．SP800-63の旧版では，検証者なりすまし攻撃に対するプロトコル耐性は，”強力な中間者攻撃耐性”とも呼ばれていた．

検証者なりすまし耐性のある認証プロトコルは，認証済み保護チャネルを検証者との間に確立しなければならない (SHALL)．したがって, 保護チャネルを確立するためにネゴシエートしたチャネル識別子を認証コード出力値に変更できない強力な形で結び付けなければならない(SHALL) (例えば，検証者が知っている公開鍵に対して認証要求者が管理しているプライベート鍵を用いて2つの値をいっしょに署名する)．検証者は, 検証者なりすまし耐性を証明するために使用する署名やその他の情報を確認しなければならない (SHALL)．これにより，不正な検証者が実際の検証者を表す証明書を持っている場合でさえも，その認証を異なる保護チャネルで再生することが防止される．

検証者なりすまし耐性が要求された場合に，それを確立するために承認された暗号アルゴリズムを使用しなければならない(SHALL)．この目的で使用する鍵は，少なくともSP 800-131Aの最新版で定義された最低限のセキュリティ強度（本書の刊行時点では112ビット）を備えていなければならない (SHALL)．

検証者なりすまし耐性を備えた認証プロトコルの例としては，TLSクライアント認証がある．クライアントは，ネゴシエートされる特定のTLS接続に一意なプロトコルから予め受け取ったメッセージと共に認証コード出力値に署名する．

アウトオブバンド認証コードや OTP 認証コードといった認証コード出力値を手動で入力する認証コードでは，認証コード出力値を認証される特定のセッションに結び付けないため，検証者なりすまし耐性があると見なしてはならない (SHALL NOT)．中間者攻撃では，不正な検証者はOTP 認証コード出力値を検証者に対してリプレイし，認証に成功してしまう可能性がある．

#### **検証者とCSPの通信**

検証者とCSPが個別のエンティティである場合（SP 800-63-3 図 4-1 (sp800-63-3.html#63Sec4- Figure1)の点線で示されているように），検証者とCSPの間の通信は，承認された暗号化技術を利用する相互認証されたセキュアなチャネル（TLSクライアント認証接続など）を介して行わなければならない(SHALL)．

#### **検証者危殆化耐性**

認証コードの一部のタイプでは，検証者が認証コードシークレットのコピーを保管する必要がある．例えば，OTP 認証コード（セクション 5.1.4）では，検証者が認証要求者から送信された値と比較するために，個別に認証コード出力値を生成する必要がある．検証者が危殆化されて保管されているシークレットが盗まれる危険があるため，検証者が認証に永続的に利用するシークレットを保管する必要のない認証プロトコルはより強力であると見なすことができる. この場合に*検証者危殆化耐性*があるとする．しかし,そのような検証者がすべての攻撃に耐性があるのではない．検証者は，特定の認証コード出力値を常に受け付けるように操作されるなど，別の手段で危殆化される可能性がある．

検証者危殆化耐性は以下のように異なる方法で実現することができる．

* 認証コードが保管するプライベート鍵に対応する公開鍵の保持を検証者に要求する暗号認証コードを使用する．
* 予測される認証コード出力値をハッシュ形式で保管する．この方法は，例えば一部のルックアップシークレット認証コード(セクション 5.1.2)と共に使用することができる．

検証者危殆化耐性を考慮し，検証者が保管する公開鍵は，承認された暗号アルゴリズムの利用と関連付けられなければならず(SHALL)，少なくともSP 800-131Aの最新版で定義された最低限のセキュリティ強度（本書の刊行時点では112ビット）を備えていなければならない(SHALL)．

他の検証者危殆化耐性のあるシークレットは，承認された暗号アルゴリズムを利用しなければならなず (SHALL)，基礎となるシークレットは少なくともSP 800-131Aの最新版で定義された最低限のセキュリティ強度（本書の刊行時点では112ビット）を備えていなければならない(SHALL)．より複雑性の低いシークレット（記憶シークレットなど）は，辞書検索や全検索を通してハッシュ処理を攻略できる可能性があるため，ハッシュされていても検証者危殆化耐性を持つと見なしてはならない(SHALL NOT)．

#### **リプレイ耐性**

認証プロセスは，以前の認証メッセージを記録し再生して認証を成功させることが困難であれば，リプレイ攻撃に耐性がある．リプレイ耐性は，認証コード出力値が保護チャネルに入力される前に盗まれる可能性があるため，認証済み保護チャネルプロトコルのリプレイ耐性に加えて施される．ノンスやチャレ ンジをトランザクションの”新鮮さ”を示すために用いるプロトコルは，再生されるメッセージが適切なノンスや時系列データを含まないことから, 検証者は容易に過去のプロトコルメッセージが再生されたことを検知できるため，リプレイ耐性がある．

リプレイ耐性のある認証コードの例として，OTPデバイス，暗号化認証コード, ルックアップ シークレットがある．

反対に記憶シークレットは認証コード出力値がシークレットそのものであり，それぞれの認証で入 力されるため，リプレイ耐性があると見なされない．

* + 1. **認証意図**

認証プロセスは，主体がそれぞれの認証や再認証の要求に明示的に応じる必要がある場合の意図を明らかにする．認証意図の目的は，直接接続された物理的な認証コード（例えば，マルチファクタ暗号デイバス）が，エンドポイント上でマルウェアなどにより主体が知らないうちに利用されることを困難にすることにある．認証意図はその認証コードそのものにより明らかにならねばならないが (SHALL)，マルチファクタ暗号化デバイスがその認証コードが利用されるエンドポイント上で他の認証ファクタを再入力することにより認証意図を明らかにしてもよい(MAY)．

認証意図はいくつかの方法で明らかにしてもよい(MAY)．例えば, 主体の介入（例えば, OTPデバイスから得た認証コード出力値を認証要求者が入力）を必要とする認証プロセスは認証意図を明らかにする．それぞれの認証や再認証操作に対してユーザーアクション（例えば, ボタンの押し下げや再挿入）を必要とする暗号化デバイスも認証意図を明らかにする．

生体情報の提示は，計測手段に応じて認証意図を明らかにしたりしなかったりする．指紋の提示は通常は意図を明らかにするだろうが，カメラを用いた認証要求者の顔の観測は一般的にはそうならない．行動に基づく生体認証も，認証要求者側で特定の行為を常に要求するわけではないため，認証意図を明らかにする可能性は低いと思われる．

#### **制限付き認証コード**

一般的に, 認証コードが攻撃に対抗する能力は脅威の進化につれて低下する．逆に言うと，いくつかの認証コードは性能が改善する可能性がある. 例えば，根拠となる標準が改定されると, 特定の攻撃に対抗する能力が増す．

認証コードの性能におけるこうした変化を考慮するため，NISTは認証コードのタイプや特定のクラスまたはインスタンスに対して追加的な制限を設けた．

制限付き認証コードを利用するには，認証する組織が制限付き認証コードに関連するリスクを評価，理解，許容し，時間の経過とともにリスクが高まる恐れがあることを認識する必要がある．組織の責任は，システムと関連データに対してリスク許容レベルを決定し，リスクの脅威を緩和する方法を定義することである．組織は任意の主体に対するリスクが許容できないと判断するいかなる時点においても，その認証コードを使用してはならない (SHALL NOT)．

さらに，一般的に認証エラーのリスクは，認証する組織，認証結果に依存する組織，加入者を含む複数の当事者に関係する．組織が制限付き認証コードを受け入れると, 加入者が追加のリスクにさらされる可能性があり, 加入者はそのリスクに対して十分な理解と対処能力を備えていない場合がある．そのため，CSPは次のことを実施しなければならない (SHALL)．

* + - 1. 加入者に対して, 制限付きではない代替認証コードを少なくとも1つ提示し，要求されるAALで認証に使用できるようにする．
      2. 制限付き認証コードのセキュリティリスクと，制限付きではない代替認証コードが利用可能であることを, 加入者が理解しやすいように通知する．
      3. リスク評価において加入者に対する追加のリスクに対処する．
      4. 将来のある時点で制限付き認証コードが許容できなくなる可能性を踏まえて移行計画を立て，デジタル ID 許容表明にこの移行計画を含める．

# 認証コードのライフサイクル管理

*このセクションは規範である．*

加入者の認証コードのライフサイクルにわたって数多くのイベントが発生し,　その認証コードの使用に影響する．そうしたイベントは，結び付け，紛失，盗難，不正な複製，有効期限切れ，破棄を含む．このセクションでは, こうしたイベントで取るべき行動について説明する．

### **認証コードの結び付け**

*認証コードの結び付け* は, 特定の加入者アカウントと認証コードの関連を確立し，認証コードを - 他の認証コードと組み合わせることもできる - そのアカウントを認証するために利用できる状態にする．

認証コードは以下のどちらかの方法で加入者アカウントに結び付けなければならない(SHALL):

* 登録の一部としてCSPが発行する.
* 加入者が提示した許容できる認証コードを CSP に関連付ける

これらのガイドラインでは，両方の方法について認証コードの発行ではなく*結び付け*について説明する．

CSPは, それぞれの身元情報と関連付けられるか既に関連付けられたすべての認証コードの記録を, デジタル ID のライフサイクルを通して保管しなければならない(SHALL)．CSPまたは検証者は，セクション 5.2.2に説明してあるように，認証試行の回数制限に必要な情報を保管しなければならない(SHALL)．また，CSPは, 検証者が各AALの要件に合致していることが確定できるように, ユーザーが提示した認証コードのタイプ(例えば，単一ファクタ暗号化デバイスとマルチファクタ暗号化デバイス)を検証しなければならない(SHALL)．

CSPによって生成される記録は，認証コードがアカウントに結び付けられた日時を含まなければならない (SHALL)．記録には登録に関連するあらゆるデバイスの結び付けの発 生源（IPアドレス，デバイス識別子など）に関する情報が含まれるべきである(SHOULD)．可能であれば，認証コードで認証に失敗した際の発生源についての情報も含まれるべきである(SHALL)．

新しい認証コードを加入者アカウントに結び付けるとき，CSPは，結び付けプロトコルと関連鍵を提供するプロトコルが，その認証コードが使われるAALに見合ったセキュリティレベルで結び付けられることを保証しなければならない(SHALL)．例えば，鍵を提供するプロトコルは, 認証済み保護チャネルを使用するか, 中間者攻撃を防止するために直ちに実施されなければならない(SHALL)．マルチファクタ認証コードの結び付けには，認証コードを結び付けるためにマルチファクタ認証かそれに相当するもの(例えば，身元情報の検証が完了した直後のセッションとの関連)を使用しなければならない (SHALL). 認証コードが鍵ペアを生成して公開鍵がCSPに送信されるときも，同じ条件が適用される．

#### **登録時の結び付け**

SP 800-63A (sp800-63a.html)に記述されているように, 身元情報の検証トランザクションが成功した結果として認証コードが身元情報に結び付けられるときに以下の要件が適用される．行政命令 13681 [EO 13681]は, 個人データの開示にマルチファクタ認証の使用を義務付けているため，認証コードが加入者アカウントに登録時に結び付けられ，身元情報の検証で確立された情報を含む個人データへアクセスできるようにすることが重要である．

CSPは，記憶シークレットまたは1つ以上の生体認証に加えて，加入者のオンライン身元情報に対して物理的な (*本人が持っているもの*) 認証コードを少なくとも1つ結び付けなければならず (SHALL)，少なくとも2つ結び付けるべきである(SHOULD)．

すべての識別情報はIAL1で自己表明されているが，認証コードの紛失が原因でアカウントが管理できなくなると, オンライン上の情報や評判が危険にさらされる．２つ 目の認証コードを使用すると, 認証コードの紛失から安全に回復させることができる．この理由により，CSPはIAL1でも同様に加入者認証情報に少なくとも2つの物理的認証コードを結び付けるべきである(SHOULD)．

IAL2以上では，識別情報はデジタル ID に関連付けられ，加入者はSP 800-63A (sp800-63a.html)に記述されているように身元情報検証プロセスを受けている．結果として，望ましいIALと同じAALの認証コードがアカウントに結び付けられなければならない(SHALL)．例えば，加入者がIAL2で検証に成功したら，AAL2またはAAL3の認証コードはIAL2の身元情報に結び付けるために適切である．CSPはAAL1の認証コードをIAL2の身元情報に結び付けてもよいが(MAY)，加入者がAAL1で認証される場合には，それが自己表明であっても個人情報を加入者に開示してはならない(SHALL NOT)．前の段落で述べたように，追加の認証コードを使用すれば，認証コードの破損，紛失，盗難に備えることができる．

単一の物理的対面や電子的トランザクション（つまり，保護された単一セッション）で登録と結び付けが完了できない場合は，同じ主体がプロセスを通して認証申請者として行動することを保証するために, 以下の方法を使用しなければならない(SHALL):

リモートトランザクションの場合:

1. 認証申請者は，新しい結び付けトランザクションのたびに，以前のトランザクションで確立されたか，自分の電話番号，Eメールアドレス，記録された住所に送付された一時的なシークレットを提示して本人であることを証明しなければならない(SHALL)．
2. 長期間の認証コードシークレットは，保護セッションで認証申請者だけに発行されなければならない (SHALL)．

対面トランザクションの場合:

1. 認証申請者は上記リモートトランザクション(1)のシークレットを利用するか，以前の対面時に記録された生体認証を利用し，対面で本人であることを証明しなければならない(SHALL)．
2. 一時的なシークレットを再利用してはならない(SHALL NOT)．
3. CSPが物理的なトランザクションの間に長期間の認証コードシークレットを発行する場合は，シークレットは対面で認証申請者に発行される物理デバイスにローカルでロードされるか，記録上の住所を確認する方法で配送されなければならない(SHALL)．

#### **登録後の結び付け**

#### 以下のサブセクションで認証コードを加入者のアカウントに結び付けることに関して説明する.

* + - 1. **既存のAALにおける追加認証コードの結び付け**

記憶シークレットとは別に，CSPと検証者は，使用するそれぞれのファクタの少なくとも2つの有効な認証コードの保管を加入者に促すべきである(SHOULD)．例えば，普段は物理的認証コードとしてOTPデバ イスを利用している加入者は，物理的認証コードの紛失，盗難，破損に備えて，複数のルックアップシークレット認証コードの発行を受けたり，アウトオブバンド認証用のデバイスを登録したりしてもよい(MAY)．記憶シークレット認証コードの取り替えに関する詳細はセクション 6.1.2.3 を参照．

したがって，CSPは加入者のアカウントに追加の認証コードを結び付けることを許可すべきである(SHOULD)．新しい認証コードを追加する前に，CSPは加入者に対して，新しい認証コードを使用するAAL（またはそれ以上のAAL）で認証することを要求しなければならない(SHALL)．認証コードを追加するとき，CSPは新しい認証コードを結び付けるトランザクションと独立した方法（例えば，加入者に以前に関連付けられたアドレスへのEメール）で加入者に通知すべきである(SHOULD)．CSPは，この方法でバインドできる認証コードの数を制限してもよい(MAY)．

#### **単一ファクタアカウントに追加ファクタを追加**

加入者のアカウントに認証ファクタが１つだけ結び付けられていて(すなわちIAL1/AAL1)，別の認証ファクタの認証コードを追加する場合，加入者はアカウントを AAL2 に更新するよう要求してもよい(MAY)．IALはIAL1のままになる．

新しい認証コードを結び付ける前に，CSPは加入者にAAL1で認証するよう要求しなければならない(SHALL)．CSPは新しい認証コードを結び付けるトランザクションと独立した方法（例えば，加入者に以前に関連付けられたアドレスへのEメール）で加入者に通知すべきである(SHOULD)．

#### **紛失した認証ファクタの取り替え**

加入者がマルチファクタ認証に必要なファクタのすべての認証コードを失い，身元情報がIAL2かIAL3で証明されている場合，加入者はSP 800-63A (sp800-63a.html)に説明されている身元情報検証プロセスを繰り返さなければならない (SHALL)．CSPはSP 800-63A (sp800-63a.html) セクション 4.2に記述されているようにプライバシーリスク評価に従って元の検証プロセスから証拠を得ている場合は，以前提供された証拠と認証要求者とが結び付けられていることを確認した上で簡略型の検証プロセスを利用してもよい(MAY)．CSPは．既存の身元情報への結び付けを確認するために，残りのファクタがあればその認証コードを用いて認証するよう認証要求者に要求しなければならない(SHALL)．IAL3における認証ファクタの再確立は，対面またはSP 800-63A (sp800-63a.html) セクション 5.3.3.2にあるように監視リモートプロセスを通して実施されなければならず(SHALL)，元の検証プロセスで収集した生体認証情報を検証しなければならない(SHALL)．

CSPは加入者にこのイベントを通知すべきである(SHOULD)．検証プロセスの一部として要求されている通知と同じでもよい(MAY)．

記憶シークレットの紛失(つまり忘れること)は頻繁に起きるため,　取り替えには多くの問題がある．追加の “バックアップ” 記憶シークレットは，結局忘れる可能性があるために緩和策にはならない．生体認証がアカウントに結び付けられている場合は，生体認証と関連する物理認証コードを使って新しい記憶シークレットを設定すべきである(SHOULD)．

上記の再検証プロセスの代わりとして生体認証がアカウントに結び付けられていない場合は，CSPは加入者の記録上の住所の１つに送付した確認コードとともに, 2つの物理的認証コードを用いる認証で新しい記憶シークレットを結び付けてもよい(MAY)．確認コードは，少なくともランダムな6文字の半角英数字で構成され，乱数生成器 [SP 800-90Ar1] を利用して生成されなければならない(SHALL)．記録上の住所に郵送される確認コードは，最大7日間有効でなければならな(SHALL)．しかし，合衆国郵便公社が直接配送できない住所に対応するための例外措置として最大21日まで有効としてもよい(MAY)．物理的な方法以外で送付された確認コードの有効期限は最大10分でなければならない(SHALL)．

#### **加入者が提示する認証コードとの結び付け**

加入者は特定のAALの認証に適した認証コードをすでに所持している場合もある．例えば，ソーシャルネットワークプロバイダからAAL2とIAL1とみなされる 2ファクタ認証コードを入手しており，そうした認証情報をIAL2が必要なRPで使用したいとする．

大量の認証コードを管理する加入者の負荷を軽くするために，CSPは不都合がなければ加入者が提供する認証コードの利用に対応するべきである(SHOULD)．これらの認証コードの結び付けは，セクション 6.1.2.1に記述してあるように実施しなければならない(SHALL)．認証コードの強度が自明でない場合(例えば，所定のタイプの単一ファクタ認証コードとマルチファクタ認証コードの間)は，CSPは強度の高い認証コードが実際に使用されていることが（例えば，認証コードの発行者や製造元の検証などにより）確認できない限り，強度の低い認証の利用を前提とすべきである(SHOULD)．

#### **更新**

CSPは，既存の認証コードの有効期限に到達する前に適切な時間を確保して，更新される認証コードを結び付けるべきである(SHOULD)．このプロセスは，認証コードを結び付ける最初のプロセス（例えば，記録上の住所を確認）に正確に従うべきである(SHOULD)．新しい認証コードが正しく使用できるようになれば，CSPは取り替えられる認証コードを無効にしてもよい(MAY)．

### 紛失，盗難，破損，不正な複製

危殆化した認証コードには，盗難，紛失，不正な複製の対象になったものがある．一般的に，紛失した認証コードに対して, 盗難または不正な加入者による危殆化を想定しなければならない．破損しているか不具合のある認証コードも，認証コードシークレットが抽出された可能性に対処するために改竄されたと見なされる．その明らかな例外は, 攻撃者が入手したなどの形跡がない，忘れられた記憶シークレットである．

危殆化した認証コードの停止，取り消し，破棄は，その検出後に速やかに行われるべきである(SHOULD)．政府機関はこのプロセスに時間制限を設けるべきである(SHOULD)．

認証コードの紛失，盗難，破損を確実に報告することを促すために，CSPは加入者がバックアップまたは代替の認証コードを利用してCSPに対して認証できる方法を提供すべきである(SHOULD)．このバックアップ認証コードは, 記憶シークレットか物理的認証コードのどちらかでなければならない (SHALL)．どちらを使用してもよい(MAY)が，報告を行うためには認証ファクタが１つだけ必要になる．または，加入者はCSPに対して認証済み保護チャネルを確立し，検証プロセスで収集された情報を検証してもよい(MAY)．CSPは記録上の住所(つまりEメール，電話，郵送先)を検証し，危殆化されたと報告のあった認証コードを停止してもよい(MAY)．加入者が正当な（つまり停止されていない）認証コードを用いて正しくCSPに対して認証し，この方法で停止された認証コードを再び有効にすることを要求する場合，停止を取り消さなければならない(SHALL)．CSPは停止されている認証コードが再有効化できなくなるまでの時間を制限してもよい(MAY)．

### **有効期限切れ**

CSPは有効期限がある認証コードを発行してもよい(MAY)．有効期限が切れた認証コードは, 認証に使用できてはならない(SHALL NOT)．有効期限切れの認証コードを用いて認証が試行された場合は，CSPは加入者に対してこの認証失敗は有効期限切れによるものであり他の理由ではないことを知らせるべきである(SHOULD)．

CSPは, 認証コードの有効期限が切れたり更新された認証コードを受け取ったりした後に，CSPによって署名された属性証明書を含む物理的認証コードの放棄または破棄した証明を加入者にできる限り速やかに要求しなければならない(SHALL)．

### **失効と取り消し**

認証コードの失効は，特にPIV 認証コードでは取り消しと呼ばれることがあるが，認証コードとCSPが保管する認証情報との結び付けを解除することを指す．

CSPは，オンライン ID が存在しなくなった（例えば，加入者が死亡，不正な加入者であることが判明した）とき，加入者が要求したとき，または加入者がもはや適性要件を満たしていないと判断されるとき，速やかに認証コードの結び付けを解除しなければならない(SHALL)．

CSPは，失効または取り消しの後, CSPによって署名された属性証明書を含む物理的認証コードの放棄または破棄したことの証明を加入者にできる限り速やかに要求しなければならない(SHALL)．

PIV 認証コードの取り消しに関する要件の詳細はFIPS 201 に説明されている．

# セッション管理

*このセクションは規範である.*

一度認証イベントが行われると，加入者はその後のやりとりで認証イベントを繰り返さずにアプリケーションを継続して使用できることが望ましい．この要件が特に当てはまるのは，認証イベントがネットワーク経由で複数のコンポーネントとエンティティの調整を必要とする連携シナリオ ( SP 800-63C (sp800-63c.html)) である．

これを容易にするため，*セッション*は認証イベントに対応して開始され, それが終わるまで継続されてもよい (MAY) ．セッション は， 活動がないときのタイムアウト, 明示的なログアウトイベント，その他の方法などさまざまな理由により終了されてもよい (MAY) ．セッションは， 再認証 イベント ( セクション 7.2) を通して維持されてもよい (MAY) ．このときユーザーは，初回の認証イベントの一部または全部を繰り返すことによってセッションを再確立する．

セッション管理は認証情報の継続的な提示よりも望ましい．認証情報を頻繁に提示することはユーザビリティを低下させ，認証情報のロックを解除するキャッシュなどの回避策が助長され，認証イベントの有効性が損なわれる．

### **セッションの結び付け**

セッションは，ブラウザ，アプリケーション，オペレーティング システム（つまりセッション主体）などの加入者が実行しているソフトウェアと，加入者がアクセスしている RP や CSP（つまりセッション ホスト）の間に発生する．セッションシークレットは，加入者のソフトウェアとアクセスしているサービスの間で共有されなければならない (SHALL) ． このシークレットは，セッションの両端を結び付け，加入者が継続的にサービスを使用することを許可する． シークレットは，加入者のソフトウェアによって直接提示されなければならない (SHALL) ．または，暗号化メカニズムによってシークレットの所有が証明されなければならない (SHALL) ．

セッションの結び付けに使用するシークレットは，セッション ホストが認証イベントに直接対応して生成されなければならない(SHALL) ．セッションは生成のきっかけとなった認証イベントの AAL プロパティを継承するべきである (SHOULD) ．セッションは認証イベントよりもAALが低いと見なしてもよいが (MAY)，認証イベントよりもAALが高いと見なしてはならない(SHALL NOT) ．

セッションの結び付けに使用するシークレットの要件は以下のとおりである.

1. 情報のやりとりの中で通常は認証の直後にセッションホストによって生成されなければならない(SHALL) ．
2. 承認された乱数生成器[SP 800-90Ar1] によって生成され，少なくとも64 ビットのエントロピーを含まなければならない(SHALL) ．
3. 加入者 のログアウト時に，セッション主体によって消去または無効にされなければならない (SHALL) ．
4. ユーザーがログアウトするとき，またはシークレットの有効期限が切れたと見なされるとき，加入者エンドポイントから消去されるべきである (SHOULD) ．
5. クロスサイトスクリプティング(XSS) 攻撃でローカルストレージが開示される可能性があるため，HTML5 ローカル ストレージなどの安全でない場所に配置されるべきでない (SHOULD NOT) ．
6. 認証済み保護チャネルを使用するデバイスから送信または受信されなければならない(SHALL) ．
7. セクション 4.1.4，4.2.4，4.3.4 に指定されている時間の後は, AAL の必要に応じてタイムアウトしなければならず(SHALL)，受け付けられてはならない．
8. ホストと 加入者エンドポイントの間の安全でない通信に利用できてはならない(SHALL NOT) ．認証済みセッション は，認証 の後にHTTPSからHTTP へというような安全でないトランスポートにフォールバックしてはならない (SHALL NOT) ．

URL か POST コンテンツはセッション識別子を含まなければならず (SHALL),そのセッション識別子は， セッションの外で行われたアクションが保護セッションに影響しないことを保証するために RP が検証しなければならない (SHALL) ．

経時的にセッションを管理する仕組みはいくつかある．次のセクションでは，それぞれの技術に特有の追加要件と考慮事項に沿って例を示す．補足的な参考ガイダンスは，OWASP *セッション管理チートシート* [OWASP-session] から入手できる．

#### **ブラウザクッキー**

ブラウザクッキーは広く普及している方法で，サービスにアクセスする加入者に対してセッションが生成されて追跡される．

クッキーの要件は以下のとおりである.

* + - 1. セキュアな (HTTPS) セッションだけでアクセスできるようにタグ付けされなければならない(SHALL)．
      2. ホスト名とパスの最小で実際的なセットにアクセスできなければならない(SHALL)．
      3. JavaScript (HttpOnly) 経由でアクセスできないようにタグ付けされるべきである (SHOULD)．
      4. セッションの有効期間，またその直後に有効期限切れとなるようタグ付けされるべきである(SHOULD) ．この要件はクッキーの蓄積を制限することを目的としているが，強制的にセッションをタイムアウトさせるために決められてはならない (SHALL NOT)．

#### **アクセストークン**

OAuth に見られるようなアクセストークンは, 認証イベントの後にアプリケーションが加入者に代わって一連のサービスにアクセスできるようにする．OAuthアクセストークンは，他のシグナルがない場合，RP はこれを加入者の存在として解釈してはならない (SHALL NOT) ．OAuthアクセストークンと, 関連するリフレッシュトークンは，認証セッションが終わり加入者がアプリケーションを終了した後も長い間有効であってもよい (MAY) ．

#### **デバイスの識別**

加入者とサービスの間のセッションの確立には，セキュアなデバイス識別の他の方法（相互 TLS やトークン結び付け，その他のメカニズムを含むがこれに限定されない）が使用されてもよい (MAY) ．

### **再認証**

認証されたセッションの継続性は，認証の際に検証者が発行してセッション中に随意に更新されたセッションシークレットの所有に基づかなければならない(SHALL) ．セッションの性質はアプリケーションに依存し, 以下のいずれかになる :

1. “セッション” クッキーのあるWeb ブラウザセッション
2. セッションシークレットを保管するモバイルアプリケーションのインスタンス

セッションシークレットは非永続的でなければならない (SHALL) ．つまり，関連するアプリケーションやホストデバイスの再起動後に残ってはならない (SHALL NOT) ．

セッションの定期的な再認証は，認証されたセッションで加入者 が継続して存在していること (つまり加入者がログアウトしていないこと) を確認するために実行されなければならない (SHALL) ．

セッション は，セッション シークレット単独の提示に基づくセクション 4.1.3, 4.2.3, 4.3.3 (AAL による) のガイドラインを超えて延長されてはならない (SHALL NOT) ．再認証のタイムリミットは，セッションが無効になる前に表 7-1で指定された認証ファクタの提示を加入者に促して延長されなければならない(SHALL) ．

タイムアウトやその他のアクションによってセッションが終了されたとき，ユーザーに再認証による新しい セッション の確立を要求しなければならない(SHALL) ．

**表 7-1 AALの再認証要件**

|  |  |  |
| --- | --- | --- |
| **AAL** | 要件 | |
| 1 | 任意の 1 つのファクタの提示 | |
| 2 | 記憶シークレットまたは生体認証の提示 |
| 3 | すべてのファクタの提示 |

注意：AAL2 では, セッションシークレットは本人が持っているものであり, セッションを継続するには追加の認証コードファクタが必要になるため, 物理的な認証コードではなく, 記憶されたシークレットか生体認証が要求される.

#### **7.2.1 連携またはアサーションからの再認証**

CSP と RP を接続するために SP 800-63C (sp800-63c.html) のセクション5で説明されているように連携プロトコルを使用するとき，セッション管理と再認証に特別な考慮事項が適用される．連携プロトコルは CSP と RP の間で認証 イベントを伝えるが，両者の間にセッション を確立しない．CSP と RP はセッション管理に別々の技術を採用している場合が多いため，こうしたセッションの間に相互関係があると推定してはならない(SHALL NOT) ．したがって，RP 側のセッションが完了し RP が再認証を要求するとき，CSP 側のセッション が終了しておらず， ユーザーの再認証なしにこのセッション から新しいアサーションが生成される可能性は十分にある．

連携プロトコルによる再認証を必要とする RP は，可能な場合はプロトコル内で, 許容可能な最大経過時間をCSPに指定しなければならならず (SHALL)，その時間内に認証が行われていない場合は CSP は 加入者を再認証しなければならない (SHALL) ．CSP は，アサーション が 再認証 に十分かどうかについて, そして次の再認証イベントの時間について RP が決定できるように，認証イベントの時間を RP に伝えなければならない (SHALL) ．

1. **脅威とセキュリティに関する考慮事項**

*このセクションは参考情報である.*

### **認証コードへの脅威**

認証コードをコントロールできる攻撃者は, 認証コードの所有者を装うことができる．

認証コードへの脅威は，認証コードを構成する認証ファクタの種類ごとの攻撃に基づいて分類することができる :

* *本人が知っていること*は攻撃者に暴露される恐れがある．攻撃者は記憶シークレットを推測できるかもしれない．認証コードが共有シークレットの場合，攻撃者は CSP または検証者にアクセスしてシークレットの値を入手したり，その値のハッシュに辞書攻撃を行ったりできる．攻撃者は，PIN やパスコードの入力を観察した り，それが書かれた記録や入力記録を見つけたり，シークレットを盗むために不正なソフトウェア（キーボードロガーなど）をインストールしたりするかもしれない．さらに，攻撃者は検証者が管理しているパスワードデータベースにオンライン攻撃を仕掛けてシークレットを特定するかもしれない．
* *本人が持っているもの* は所有者が紛失したり，破損させたり，盗難にあったりするか, 攻撃者が複製する恐れがある．例えば，所有者のコンピュータへアクセスできた攻撃者は，ソフトウェアの認証コードをコピーするかもしれない． ハードウェアの認証コードは，盗難，改竄，複製の対象になるかもしれない．アウトオブバンドのシークレットは攻撃者によって傍受され，不正なセッションを認証するために利用されるかもしれない．
* *本人の特徴であるもの*は複製される恐れがある．例えば，攻撃者は加入者の指紋をコピーしたり，レプリカを作ったりするかもしれない．

この文書では, 検証者に対して不正な認証を試みる攻撃者と加入者が共謀してないことを前提としている．この前提に立って，デジタル認証に使用される認証コードへの脅威をいくつかの例とともに表 8-1 にまとめた．

##### 表 8-1 - 認証コードへの脅威

|  |  |  |  |
| --- | --- | --- | --- |
| **認証コードへの**  **脅威/攻撃** | **説明** | **例** | |
| **アサーション の作成または変更** | 攻撃者が偽のアサーションを生成する | 危殆化した CSP が 正しく認証されていない認証要求者の身元情報を表明する | |
| 攻撃者が既存のアサーションを変更する | 危殆化したプロキシが認証アサーション の AAL を変更する | |
| **盗難** | 物理的な認証コードを攻撃者が盗む | ハードウェア暗号化デバイスが盗まれる | |
| OTP デバイスが盗まれる | |
| ルックアップシークレットの認証コード が盗まれる | |
| 携帯電話が盗まれる | |
| **複製** | 加入者の認証コードが知らない間に複製される | 紙に書かれたパスワードが開示される | |
| 電子ファイルに格納されたパスワード  がコピーされる | |
| ソフトウェア PKI 認証コード (プライベート鍵) がコピーされる | |
| ルックアップシークレットの認証コード がコピーされる |
| 生体情報の認証コードが偽造される |
| **盗聴** | 加入者が認証を行っているときに認証コードシークレットや認証コード出力値が攻撃者に暴露される | キーボードの入力を監視して記憶シークレットを取得する |
| キーストロークを記録するソフトウェアによって，記憶シークレットや認証コード出力値を取得する |
| PIN の入力デバイスから PIN がキャプチャされる |
| ハッシュされたパスワードを攻撃者が手に入れて別の認証で使用する (*pass-the-hash攻撃*) |
| アウトオブバンドシークレットが通信チャネルの危殆化によって傍受される | アウトオブバンドシークレットが暗号化されていないWi-Fiで送信され，攻撃者に受信される |
| **オフライン クラッキング** | 認証コードが認証メカニズムの外で解析手法によって明らかにされる | ソフトウェア PKI 認証コードが辞書攻撃を受け, プライベート鍵の復号に使用する正しいパスワードが突き止められる |
| **サイドチャネル攻撃** | 認証コードの物理的特性を利用して認証コードシークレットが暴露される | ハードウェア暗号化認証コードの電力解析によって鍵が抽出される |
| 大量の認証試行で認証コードの応答時間が解析され, 暗号化認証コードのシークレットが抽出される |
| **フィッシングまたはファーミング** | 検証者 や RP になりすました攻撃者によって認証コード出力値が漏洩する | 検証者に偽装した Web サイトに加入者が入力することでパスワードが漏洩する |
| 銀行の担当者に偽装した攻撃者からのメールに返信することで，記憶シークレットが漏洩する |
| DNS スプーフィングによって偽の検証者の Webサイトに加入者がアクセスし，記憶シークレットが漏洩する |
| **ソーシャルエンジニアリング** | 攻撃者は加入者と信頼関係を築き,　認証コードシークレットや認証コード出力値を明らかにするよう説得する | 加入者の上司の代理としてパスワードを聞いてきた同僚に対して加入者が記憶シークレットを明らかにする |
| システム管理者を装った攻撃者からの電話問い合わせによって加入者が記憶シークレットを明らかにする |
| 加盟者の携帯電話を攻撃者にリダイレクトするようにモバイル担当者を説得し，SMS経由でアウトオブバンドシークレットが攻撃者に受信される |
| **オンラインでの推測** | 攻撃者が検証者にオンラインで接続し，有効な認証コード出力値の推測を試みる | 記憶シークレットを推測するためにオンライン辞書攻撃が使われる |
| 正当な認証要求者に登録された OTP デバイスの認証コード出力値を割り出すために，オンラインで推測が試みられる |
| **エンドポイントの危殆化** | エンドポイント上の不正なコードがプロキシを利用し，加入者の同意なしに接続された認証コードにリモートアクセスを | エンドポイントに接続された暗号化認証コードが，リモート攻撃の認証に利用される |
| エンドポイント上の不正なコードにより，意図した検証者以外に対して検証が行われる | 加入者ではなく攻撃者のために認証が行われる |
|  | エンドポイント上の不正なアプリがSMS 経由で送信されたアウトオブバンドシークレットを解読し，攻撃者がそれを認証に利用する |
| エンドポイント上の不正なコードが，マルチファクタのソフトウェア暗号化認証コード を危殆化させる | 不正なコードがプロキシを利用して認証するか，エンドポイントから認証コードの鍵をエクスポートする |
| **認証されていない結び付け** | 攻撃者が管理下の認証コードを加入者 のアカウントに結び付ける | 加入者に認証コードや提供される鍵が送られる経路に攻撃者が割り込む |

* 1. **脅威の軽減策**

表 8-2 は，上記の脅威の軽減を支援する仕組みをまとめたものである．

**表 8-2 - 認証コード の脅威を軽減する**

|  |  |  |  |
| --- | --- | --- | --- |
| **認証コードへの脅威/攻撃** | **脅威を軽減する仕組み** | **規約の参照** | |
| **盗難** | 記憶シークレットまたは生体認証によって有効にする必要があるマルチファクタ認証コードを使用する | 4.2.1, 4.3.1 | |
| 記憶シークレットまたは生体認証を含む認証コードを組み合わせて使用する | 4.2.1, 4.3.1 | |
| **複製** | 認証シークレットの抽出や複製が長期的に困難な認証コードを使用する | 4.2.2, 4.3.2,  5.1.7.1 | |
| **盗聴** | 特にキーロガーなどのマルウェアに感染していないか，エンドポイントがセキュリティを確保できているか，使用する前に確かめる | 4.2.2 | |
| 信頼されていないワイヤレスネットワークを，暗号化されていない２番目のアウトオブバンド認証チャネルとして使用することを避ける | 5.1.3.1 | |
|  | 認証されて保護されたチャネル経由で認証を行う (例 : ブラウザウィンドウのロックアイコンを確認する) | 4.1.2, 4.2.2, 4.3.2 | |
| *pass-the-hash* のようなリプレイ攻撃に耐性のある認証プロトコルを使用する | 5.2.8 | |
|  | | 信頼された入力と信頼された表示機能がある 認証エンドポイントを使用する | 5.1.6.1, 5.1.8.1 |
| **オフライン クラッキング** | | エントロピーの高い認証コードシークレットで 認証コード を使用する | 5.1.2.1, 5.1.4.1,  5.1.5.1, 5.1.7.1,  5.1.9.1 |
| 鍵付きハッシュを含む，ソルト付きでハッシュ化された状態で記憶シークレットを保存する | 5.1.1.2, 5.2.7 |
| **サイドチャネル攻撃** | | シークレットの値に関係なく消費電力とタイミングが一定に保たれるように設計された認証コードアルゴリズムを使用する | 4.3.2 |
| **フィッシングまたはファーミング** | | 検証者なりすましへの防御が提供される認証コードを使用する． | 5.2.5 |
| **ソーシャルエンジニアリング** | | カスタマーサービス代行者などの第三者によるソーシャルエンジニアリングのリスクを引き起こす認証コードの使用を避ける | 6.1.2.1, 6.1.2.3 |
| **オンラインでの推測** | | エントロピーの高い出力を生成する認証コードを使用する | 5.1.2.1, 5.1.7.1,  5.1.9.1 |
| アクティベーションの試行に繰り返し失敗するとロックされる認証コードを使用する | 5.2.2 |
| **エンドポイントの危殆化** | | 加入者の物理的なアクションを必要とするハードウェア認証コードを用する | 5.2.9 |
| ソフトウェアベースの鍵をアクセスが制限されたストレージで保管する | 5.1.3.1, 5.1.6.1,  5.1.8.1 |
| **認証されていない結び付け** | | 認証コードと関連する鍵の提供には中間者攻撃に耐性のあるプロトコルを使用する | 6.1 |

表 8-1 で説明した脅威を軽減するためにその他の対策を適用してもよい:

* マルチファクタは攻撃を難しくする．攻撃に暗号認証コードと記憶シークレットが必要になると，両方のファクタを入手したり類推したりする作業は膨大になる．
* 物理的なセキュリティメカニズムは, 盗まれた認証コードの複製に対抗するために採用できる．こうしたメカニズムは，改竄の明示，検出，対応を可能にする．
* 一般的な辞書に載っていない長い*記憶シークレット*を使用すると，攻撃者はあらゆる値を試すことになる．
* システムとネットワークのセキュリティ管理は，攻撃者がシステムへアクセスしたり不正なソフトウェアをインストールしたりすることを防ぐ．
* 定期的なトレーニングは，危殆化またはその疑いをいつどのように報告するのか, または認証プロセスへの攻撃を示すパターンをどのように識別するのかを加入者に理解させる．
* *アウトオブバンド*テクニックは，登録されたデバイス (例えば携帯電話) を所有していることの検証に使用される．

### **認証コード の回復**

多くの認証メカニズムの弱点は，加入者 が管理できなくなった1 つまたは複数の認証コードを取り替えるためのプロセスにある．多くの場合，加入者の認証に残された選択肢は限られており, 経済上の理由から（コールセンター運営コストなど），安全性が低いが安価なバックアップ認証方式が採用される傾向がある．認証コードの回復は，人の手が必要になる限り，ソーシャルエンジニアリング攻撃のリスクもある．

認証ファクタの完全性を維持するためには，1 つのファクタを使用した認証を別のファクタの認証コードを取得するために使用できないことが必要不可欠である．たとえば，記憶シークレットを使用してルックアップシークレットの新しいリストが入手できてはならない．

### **セッション攻撃**

上記の論議では認証イベント自体に対する脅威に焦点を当てているが，認証イベントに続くセッションのハイジャック攻撃はセキュリティ上同様のインパクトを持つ．セクション 7 の セッション 管理ガイドラインは XSSのような攻撃に対してセッションの完全性を維持するために必要不可欠である．さらに，実行可能なコンテンツが含まれていないことを確実にするために，表示されるすべての情報をサニタイズすることが重要である[OWASP-XSS-prevention]．これらのガイドラインでは，セッションシークレットの漏洩に対してさらなる保護を提供するため，セッションシークレットがモバイルコードにアクセスできないようにすることも推奨している．

もう１つの認証後の脅威であるクロスサイトリクエストフォージェリ(CSRF) は，複数のセッションを同時に有効にするユーザー傾向を利用する．有効なURLやリクエストが意図せずまたは悪意を持ってアクティブ化される可能性を防ぐために, Web リクエストの中にセッション識別子を埋め込み検証することが重要である．

## **プライバシーの考慮事項**

*これらのプライバシーに関する考慮事項はセクション 4 のガイダンスを補足する．このセクションは参考情報である.*

### **プライバシーリスク評価**

セクション 4.1.5, 4.2.5, 4.3.5 は, 記録保持に対してプライバシーリスク評価を実施することをCSP に求めている．こうしたプライバシーリスク評価には以下が含まれる :

1. 記録保持が加入者の情報に対して侵害や不正アクセスなどの問題を引き起こす可能性
2. そのような問題が発生した場合の影響

CSP はリスクの許容，軽減，共有など，特定したプライバシーリスクに対処する方法が理に適っていることを説明できるべきである．加入者の同意を得ることはリスク共有の形であるため，共有されたリスクを評価して許容できることが加入者に期待できる場合にのみ適している．

### **プライバシー管理**

セクション 4.4 は, CSP が適切に調整したプライバシー管理を採用することを求めている．SP 800-53 は，CSP が認証メカニズムを展開するときに検討すべき一連のプライバシー管理を提供する．これらの管理は，信頼できるメカニズムの展開を成功させるための通知や救済，その他の重要な考慮事項をカバーしている．

### **処理制限**

セクション 4.4 は, 身元情報の検証, 認証, 認可, 属性アサーション, これらに関連する不正の軽減以外の目的で属性を処理することから生じるプライバシーリスクと同一基準の予測可能性 （PII と情報システムによるその処理について, 個人と所有者と処理担当者が確実に予測できること）と管理可能性（変更, 削除, 選択的公開を含め, PII をきめ細かく管理できること）の目標を維持するための措置を講じること, または, 法律や法的手続きを遵守するための措置を講じることを CSP に求めている[NISTIR8062].

CSP には, 身元情報に関係しないサービスを加入者に提供することを含め, 属性処理に対してさまざまな業務上の目的がある. しかし, 身元情報サービス以外の目的で属性を処理することは, 個人がその追加処理を予測していないか無関心なときにプライバシーリスクを生じさせる. CSP は, 追加処理から生じるプライバシーリスクと同一基準の適切な措置を決めることができる. 例えば, 適用可能な法律, 規制またはポリシーがない場合, 加入者が依頼した身元情報に関係しないサービスを提供するために属性を処理するとき, 通知によって加入者がその処理について確実な予測（予測可能性）を維持する助けとなるかもしれないが, 明確な同意を得る必要はない場合もある. 属性のその他の処理は, 明示的な同意の取得や, 特定の属性の使用や公開を加入者がさらに細かく管理できること（管理可能性）を求める別のプライバシーリスクをもたらす場合もある. 加入者の同意には意味があることが必要である. したがって, CSP が同意を利用するとき, 追加利用を加入者が受け入れることを身元情報サービスの提供条件にすることはできない.

提案する処理が, 許可された処理や適切なプライバシーリスク軽減措置の範囲外かどうかについて疑問がある場合は, SAOP に意見を求めなければならない.

### **機関特有のプライバシー準拠**

セクション 4.4 は，連邦機関の CSP に対する特定の準拠義務について述べている. 機関の SAOP をデジタル認証システムの開発初期段階から参加させることは, プライバシーリスクの評価および軽減と準拠義務の助言 （認証コードの発行や維持のための PII 収集が, PIA を実施するための1974 年プライバシー法 [Privacy Act] や 2002年電子政府法 [E-Gov] の要件の対象になるかどうかなど）の上で非常に重要である. 例えば, 生体認証の集中管理に関してはプライバシー法の要件が適⽤され, 認証に必要な PII やその他の属性の収集と保持の理由から, プライバシー法の下で新規または既存の記録システムによる対応が求められる可能性がある. 同様に SAOP も PIA が必要かどうかを決める際に機関を⽀援できる.

これらの考慮事項は,身元情報の検証だけのためにプライバシー法の下で SORN や PIA の開発が要件になると読むべきではない. 多くの場合,デジタル認証プロセス全体を網羅する PIA と SORN を設計したり, 機関がオンラインで確⽴しているサービスやメリットについて議論するさらに広範で計画的な PIA の⼀部としてデジタル認証プロセスを含めたりすることが, もっとも理に適っていよう.

デジタル認証には多くの構成要素があることから, SAOP に各要素を認識させ理解させることが重要である. 例えば, 連携 CSP または RP サービス (Data Use Agreements（データ使用合意書）や Computer Matching Agreements（コンピュータ一致合意書）など を提供したり利⽤したりする機関にその他のプライバシー要件が適用できる場合がある. SAOP は機関にどの追加要件を適⽤するのか決定する際に⽀援を⾏なうことができる. さらにデジタル認証の個々の要素を完全に理解することで, SAOP は準拠プロセスかその他の⼿段を通してプライバシーリスクを細かく評価し,リスクを緩和することができる

1. **ユーザビリティの考慮事項**

*このセクションは参考情報である.*

ISO/IEC 9241-11 は，ユーザビリティを「特定のユーザーが特定の使用状況において，有効性，効率性，満足感をもって特定の目標を達成するために製品を使用できる程度」として定義している．この定義は有効性，効率性，満足感を達成するのに必要な主要素として，ユーザー，その目標，使用状況に焦点を当てて いる． ユーザビリティを達成するためには，カギとなるこうした要素を考慮した全体的なアプローチが必要である．

情報システムにアクセスするユーザーの目標は，意図したタスクを実行することである．認証 はこの目標を実現する機能である．しかしユーザーの視点からは，認証はユーザーと意図したタスクの間にある．認証の効果的な設計と実装は，正当なことを実行することを簡単にし，不正なことを実行することを難しくし，不正なことが起きたときにそこから回復することを簡単にする．

組織は関係者の全体的なデジタル認証エコシステムの包括的な関係性を認識する必要がある．ユーザーは多くの場合，１つ以上の認証コードをそれぞれ異なる RP に利用する．その結果, ユーザーはパスワードを覚えたり，どの認証コードがどの RP 用なのかを思い出したり，複数の物理的認証デバイスを持ち歩いたりすることを煩わしく感じる．ユーザビリティが低いと, さまざまな不具合や意図しない回避策を生じさせ，最終的にセキュリティ管理の有効性を低下させるため，認証のユーザビリティを評価することは極めて重要である．

ユーザビリティを開発プロセスに取り入れることにより，ユーザーの認証ニーズと組織の業務上の目標に取り組みながらセキュアで使いやすい認証ソリューションを導くことができる．

デジタルシステムにおけるユーザビリティの影響は，適切な AAL を決定する際のリスク評価の一環として考慮する必要がある．より高い AAL の認証コードはより優れたユーザビリティを提供することがあるため，より低い AAL アプリケーションに対して使用を許可すべきである．

認証のために連携を活用することで，ユーザビリティの多くの問題が軽減できるが，そのようなアプローチは SP 800-63C (sp800-63c.html) で説明されているように独自の代償を伴う．

このセクションでは, 一般的なユーザビリティの考慮事項と実装方法について説明するが，特定のソリューションは推奨しない．説明されている実装は特定のユーザビリティのニーズに取り組む革新的な技術的アプローチを促進するための例である．さらに，ユーザビリティの考慮事項とその実装は, 画一的なソリューションを防止する多くの要因に大きな影響を受ける．例えば，デスクトップ環境で使っているフォントサイズは，小さな OTP デバイスの画面ではテキストがはみ出してしまうかもしれない．選択した認証コードでユーザビリティ評価を実施することは，実装の極めて重要な構成要素である．代表的なユーザー，現実的な目標とタスク，適切な使用状況とともに評価を行う ことが重要である．

**前提**

このセクションでは，「ユーザー」は「認証要求者」または「加入者」を意味する．

ガイドラインと考慮事項はユーザー視点から記述される．

アクセシビリティはユーザビリティとは異なり, この文書の扱う範囲ではない. セクション 508 は情報技術の障壁を排除するために策定され, オンライン公開コンテンツに障害者がアクセスできるようにすることを連邦機関に求めている. アクセシビリティのガイドラインについてはセクション 508 の法律と標準を参照.

### **認証コード に共通するユーザビリティの考慮事項**

認証システムの選択や実装を行う際は，ユーザー，その目標，使用状況の組み合わせに注意しながら，選択した認証コードのライフサイクル全体にわたるユーザビリティ（代表的な使用法や断続的なイベントなど）を検討する．

単一の認証コードタイプは，ユーザー全員にとって十分なわけではない．したがって， AAL の要件に基づいて CSPは可能な限り代わりの認証コードをサポートし，ユーザーが必要に応じて選択できるようにすべきである．多くの場合，タスクの即時性，費用と利便性の明らかな相殺，馴染みのない特定の認証コードが選択に影響を与える．ユーザーはその時点で最小の負担または費用となる選択肢を選ぶ傾向がある．例えば，タスクが情報システムへの即時アクセスを必要とするとき，ユーザーはより多くのステップを必要とする認証コードを選択するのではなく，新しいアカウントとパスワードを作成することを好むかもしれない．または，ユーザーがすでに身元情報プロバイダのアカウントを持っている場合，（適切なAALで承認された）身元情報の連携という選択肢を選ぶかもしれない． ユーザーはいくつかの認証コードを他の認証コードよりもよく理解しているかもしれず，その理解と経験に応じて信頼レベルは異なる．

肯定的なな認証の経験は，望ましいビジネス成果を達成する組織の成功に不可欠である．したがって，ユーザー視点から認証コードを検討すべきである．包括的な認証ユーザビリティ の目標は，ユーザーの負担と認証 のわずらわしさ (例えば, 認証が必要な回数，それに関連するステップ，ユーザーが追跡しなければならない情報の量) を最小限に抑えることである． シングルサインオンは, そのような最小化策の一例である．

ほとんどの認証コードに適用できるユーザビリティの考慮事項を以下に説明する．後のセクションでは，特定の認証コードに固有の考慮事項について説明する．

すべての認証コードの代表的な使用法に関するユーザビリティの考慮事項 :

* 認証コードの使用と保守に関連する情報を提供する．例えば認証コードの紛失や盗難があった場合の対応方法や使用方法（特に初回の使用や初期化の際に異なる要件がある場合）．
* ユーザーが自分の認証コードをすぐに利用できるようにするため，認証コードの可用性も考慮されるべきである．紛失，破損，その他の元の認証コードへの悪影響に対応するため，代替認証の選択肢の必要性を検討する．
* AAL の要件に基づいて，可能な限りユーザーには代替の認証の選択肢が提供されるべきである． これによりユーザーは，使用状況，目標，タスク (タスクの頻度や即時性など) に基づいて認証コードを選択することができる．代替認証の選択肢は特定の認証コードで生じる可用性の問題にも役立つ．
* ユーザー向けテキストの特徴 :
* 対象となるユーザーに対して平易な言葉でテキスト（説明，指示，通知，エラーメッセージなど）を作成する．専門的な技術用語を避け，第6学年から第8学年の子供でも理解できるような文章にする.
* ユーザー向けおよびユーザーが入力したテキストについて，フォントのスタイル，サイズ， 色，背景とのコントラストなどを含めた可読性を考慮する． 読みにくいテキストはユーザーの入力ミスを引き起こす．可読性を高めるため，以下の使用を検討する :
  + ハイコントラスト．最も高いコントラストは白地に黒である．
  + 電子ディスプレイにはサンセリフを．印刷にはセリフを使う．
  + 間違いやすい文字を明確に区別するフォント（大文字の「O」と数字「0」など）を使う．
  + デバイスの画面に収まる限り最小フォントサイズを 12 ポイントとする．
* 認証コード入力中のユーザーエクスペリエンス :
* マスクされたテキスト入力はエラーを起こしやすいため，入力中にテキストを表示するオプションを提供する．ユーザーが確認するのに十分長く表示された文字は非表示にできる．従来のデスクトップに比べてモバイルデバイス（タブレットやスマートフォンなど ）では記憶シークレットの入力に時間がかかるため，マスキング遅延時間を決定する際にはデバイスを考慮する．マスキング遅延時間がユーザーのニーズと一致していることを確認する．
* テキスト入力に十分な時間が与えられていることを確認する（つまり, 入力画面がすぐに消えない）．与えられた入力時間がユーザーのニーズと一致していることを確認する．
* ユーザーの混乱や不満を軽減するため，入力エラーに対する明確で意味のあるアクション可能なフィードバックを提供する． ユーザーが誤ってテキストを入力したことを知らないと, ユーザビリティに大きな影響が生じる．
* ユーザーが認証コード出力値を入力する必要がある認証コードに対して，少なくとも10回の入力を許可する. 入力テキストが長く複雑になればなるほど，入力エラーの可能性が高くなる．
* 残された試行回数について，明確で意味のあるフィードバックを提供する．混乱と不満を軽減するため，回数制限（つまりスロットリング）に対して次の試行まで待機しなければならない時間を知らせる．
* モバイルデバイスでのタッチ領域や表示領域の制限など，形状による制約の影響を最小限に抑える :
* 小さなデバイスでの入力はフルサイズキーボードでの入力よりもはるかにエラーが発生しやすく時間がかかるため，大きなタッチ領域はユーザビリティを向上させる．画面上のキーボードが小さければ小さいほど，入力箇所の大きさに対する入力手段（指など）の大きさが原因で入力が困難になる．
* 小さなディスプレイのための適切なユーザーインタフェースと情報デザインを追求する．

断続的なイベントには，再認証，アカウントのロックアウト，有効期限切れ，失効，破損， 紛失，盗難，ソフトウェアの不具合などが含まれる．

認証コードタイプの断続的なイベントに関するユーザビリティの考慮事項 :

* ユーザーの非アクティブ状態によって再認証が必要になることを防ぐために，非アクティブのタイムアウトが起きる直前（2分前など）に活動を促す．
* ユーザーの活動に関係なく必要になる定期的な再認証イベントの前に，十分な時間（例えば 1時間前）を設けてユーザーに作業を保存することを促す．
* 技術的な支援が得られる方法と場所をはっきりと伝える．例えば，オンラインセルフサービス機能へのリンク，チャットセッション，ヘルプデスクの電話番号などの情報をユーザーに提供する．理想としては，外部からの介入なしにユーザーが断続的なイベントから自ら回復できるよう十分な情報が提供できるようにする．

### **認証コードタイプごとのユーザビリティ考慮事項**

ほとんどの認証コードに適用可能な前述の一般的なユーザビリティ の考慮事項（ セクション 10.1）に加え，以下のセクションでは，特定の認証コードタイプに固有のユーザビリティの考慮事項について説明する．

#### **記憶シークレット**

***代表的な使用法***

ユーザーは記憶シークレット（一般的に, パスワードや PIN と呼ばれている）を手動で入力する．

典型的な使用法のためのユーザビリティ考慮事項 :

* 記憶しやすさ
* ユーザーが覚えなければならないことが多いほど，思い出すことができなくなる可能性が高くなる．記憶シークレットの数が少なくなるほど，特定の RP に必要な特定の記憶シークレットを簡単に思い出すことができる．
* パスワードの使用頻度が低くなるほど記憶負担が大きくなる．
* 入力中のユーザーエクスペリエンス
* パスフレーズを含む記憶シークレットを入力するためのフィールドにコピー＆ペースト機能をサポートする．

***断続的なイベント***

断続的なイベントのユーザビリティ考慮事項:

* ユーザーが記憶シークレットを作成または変更するとき :
* 記憶シークレットの作成や変更の方法を明確に伝える．
* セクション5.1.1 で指定してあるように，記憶シークレットの要件を明確に伝える．
* パスフレーズの使用をサポートするに少なくとも64文字の長さを許容する．ユーザーが記憶しやすいように好きな文字（空白を含む）を使用して好きな長さの記憶シークレットを作成させる.
* 記憶シークレットに他の構成ルール（別の文字タイプの混合など）を強制しない．
* ユーザーからの要求や認証コードが危殆化した証拠がない限り，記憶シークレット の恣意的な（例 : 定期的な）変更を要求しない（詳細はセクション 5.1.1 を参照）.
* 選択されたパスワードを拒否する場合（例えば, ブラックリストに含まれている，過去に使用されたなど），明確で意味のあるアクション可能なフィードバックを提供する．

#### **ルックアップシークレット**

***代表的な使用法***

ユーザーは認証コードが記録されている印刷物か電子的ファイルを使って，検証者の要求に応えるために必要で適切なシークレットを探す．例えば，ユーザーはカードに表形式で印刷された数字や文字から特定のサブセットを提供するように求められる．

代表的な使用法のためのユーザビリティ考慮事項 :

* 入力中のユーザーエクスペリエンス
* シークレットの複雑さとサイズを考慮する．ユーザーが探すように促されるシークレットのサブセットが大きいほど，ユーザビリティへの影響は大きくなる．認証のためのルックアップシークレットの量と複雑さを決める際には，探す手間と入力の煩わしさの両方を考慮に入れるべきである．

#### **アウトオブバンド**

***代表的な使用法***

アウトオブバンド認証では，ユーザーはプライマリとセカンダリの通信チャネルへアクセスする必要がある．

代表的な使用法のためのユーザビリティ考慮事項 :

* ロックされたデバイスでシークレットを受け取るようユーザーに通知する．ただしアウトオブバンドデバイスがロックされている場合，シークレットにアクセスするにはデバイスへの認証を必要にすべきである．
* 実装に応じて，ユーザーがモバイルデバイスにテキストを入力するときに特に問題となる入力フォームの制約を考慮する．より大きなタッチ領域を提供すれば, モバイルデバイスでシークレットを入力する際のユーザビリティが向上する．
* より適切なユーザビリティの選択肢は，モバイルデバイス上にテキスト入力を必要としない機能を提供することである（例 : ユーザーがシークレットをコピーして貼り付けられるような画面でのシングルタップやコピー機能など）．このような機能をユーザーに提供することは，プライマリチャネルとセカンダリチャネルが同じデバイス上にある場合に特に役立つ． 例えば，ユーザーがスマートフォンで認証シークレットを送信することは，アウトオブバンドアプリケーションとプライマリチャネルを切り替える必要があるため （複数回の場合もある）困難である．

#### **単一ファクタ OTP デバイス**

***代表的な使用法***

ユーザーは単一ファクタ OTP デバイスによって生成された OTP にアクセスする．一般的に認証コード出力値はデバイスに表示され，ユーザーは検証者に対してその値を入力する．代表的な使用法のためのユーザビリティ考慮事項は以下のとおりである.

* 認証コード出力値は変更まで時間を少なくとも1分にできるが, 理想的にはセクション5.1.4.1 に指定してあるように2分にできる．ユーザーは認証コード出力値を入力するのに十分な時間を必要とする（単一ファクタ OTP デバイスと入力画面の間を往復する時間を含む）．
* 実装者に対する実装に応じた追加のユーザビリティ考慮事項を以下に示す.
* 単一ファクタ OTP デバイスがその出力値を電子的インタフェース（ USB ポートなど）を介して提供する場合，ユーザーは認証コード出力値を手動で入力する必要はない．しかし，物理的な入力操作（ボタンを押すなど）が必要な場合，USBポートの位置はユーザビリティの問題となる可能性がある． 例えば，USB ポートが背面にあるコンピュータもあり，ユーザーの手が届きにくい．
* USB ポートのような直接的なコンピュータインターフェースの利用が限られる場合はユーザビリティの問題を引き起こすことがある．例えば，ラップトップコンピュータの USB ポートの数は限られている．ユーザーは単一ファクタ OTP デバイスのために他の USB 周辺機器を取り外すことを強いられる場合がある．

#### **マルチファクタ OTP デバイス**

***代表的な使用法***

ユーザーは第２の認証ファクタを通してマルチファクタ OTP デバイスによって生成される OTP にアクセスする． 一般的に, ユーザーはデバイスに表示された OTP を検証者に対して手動で入力する．第２の認証ファクタは, 記憶シークレットを入力するある種の一体型入力パッド，一体型生体情報（指紋認証など）リーダー，直接的なコンピュータインターフェース（例えば USB ポート）などで達成される場合がある．この追加ファクタに対してもユーザビリティ考慮事項が適用される．マルチファクタ認証コードに使用される記憶シークレットについてはセクション10.2.1 を，生体認証についてはセクション 10.4 を参照．

代表的な使用法のためのユーザビリティ考慮事項は以下を含む.

* 認証コード出力値の手動入力中のユーザーエクスペリエンス
* 時間ベースの OTP の場合は，OTP が表示されている時間に加えて猶予時間を設ける． ユーザーはマルチファクタ OTP デバイスと入力画面の間を往復することを含め，認証コード出力値を入力するのに十分な時間を必要とする．
* ユーザーが一体型入力パッドを使用してマルチファクタ OTP デバイスのロックを解除するか，モバイルデバイスで認証コード出力値を入力する必要がある場合は，入力フォームの制約について考慮する．小さなデバイスでの入力は従来のキーボードよりはるかにエラーが発生しやすい上に時間がかかる．一体型入力パッドと画面上のキーボードが小さくなればなるほど，入力がより難しくなる．大きなタッチ領域を提供することは, マルチファクタ OTP デバイスのロックを解除したりモバイルデバイスで 認証コード出力値を入力したりする際のユーザビリティを向上させる．
* USB ポートのような直接的なコンピュータインターフェースの利用が限られる場合は, ユーザビリティの問題を引き起こすことがある． 例えば，ラップトップコンピュータの USB ポートの数は限られている．ユーザーはマルチファクタ OTP デバイスのために他の USB 周辺機器を取り外すことを強いられる場合がある．

#### **単一ファクタ暗号化ソフトウェア**

***代表的な使用法***

ユーザーは暗号化ソフトウェア鍵の所持と管理を証明することによって認証を受ける．代表的な使用法のためのユーザビリティ考慮事項は以下を含む.

* ユーザーは暗号鍵をどの認証タスクに使用するのか覚える必要があるため，ユーザーにとって意味のある適切で説明的な名前を暗号鍵に付ける．これにより, ユーザーはよく似た紛らわしい名前の複数の暗号鍵を扱わなくても済む．小さなモバイルデバイスで複数の暗号鍵から選択する場合，画面が小さいために暗号鍵の名前が短縮されると特に問題が多くなる．

#### **単一ファクタ 暗号化デバイス**

***代表的な使用法***

ユーザーは単一ファクタ暗号化デバイスの所持を証明することで認証を受ける．代表的な使用法のためのユーザビリティ考慮事項は以下を含む.

* 単一ファクタ暗号化デバイスを操作するために物理的な入力（ボタンを押すなど）を必要とする場合， ユーザビリティが問題になる可能性がある．例えば，いくつかの USB ポートはコンピュータの背面にあり，ユーザーの手が届きにくい．
* USB ポートのような直接的なコンピュータインターフェースの利用が限られる場合もユーザビリティがの問題になることがある． 例えば，ラップトップコンピュータの USB ポートの数は限られている．ユーザーは単一ファクタ OTP デバイスのために他の USB 周辺機器を取り外すことを強いられる場合がある．

#### **マルチファクタ暗号化デバイス**

***代表的な使用法***

ユーザーは認証のためにディスクかアクティベーションを必要とする”ソフト”メディアに保存された暗号鍵の所有とコントロールを証明する．アクティベーションには，記憶シークレットか 生体認証である第２の 認証ファクタを入力する．この追加ファクタに対してもユーザビリティ考慮事項が適用される．マルチファクタ認証コードに使用される記憶シークレットについてはセクション10.2.1 を，生体認証についてはセクション 10.4 を参照．

代表的な使用法のためのユーザビリティ考慮事項は以下を含む.

* ユーザーは暗号鍵をどの認証タスクに使用するのか覚える必要があるため，ユーザーにとって意味のある適切で説明的な名前を暗号鍵に付ける．これにより, ユーザーはよく似た紛らわしい名前の複数の暗号鍵を扱わなくても済む．小さなモバイルデバイスで複数の暗号鍵から選択する場合，画面が小さいために暗号鍵の名前が短縮されると特に問題が多くなる．

#### **マルチファクタ 暗号化デバイス**

***代表的な使用法***

ユーザーは認証のためにマルチファクタ暗号化デバイスの所持と保護された暗号鍵の管理を証明する．そのデバイスは，記憶シークレットか 生体認証の第２の認証ファクタによって有効化される． この追加ファクタに対してもユーザビリティ考慮事項が適用される．マルチファクタ認証コードに使用される記憶シークレットについてはセクション10.2.1 を，生体認証についてはセクション 10.4 を参照．

代表的な使用法のためのユーザビリティ考慮事項は以下を含む.

* 認証後もマルチファクタ暗号化デバイスを接続したままにすることをユーザーに要求してはならない．ユーザーは認証が終わった後にマルチファクタ暗号化デバイスを取り外すことを忘れる場合もある（例えば, スマートカードリーダー内にスマートカードを入れたままコンピュータから離れる）．
* ユーザーはマルチファクタ暗号化デバイスを接続されたままにする必要があるのかどうかについて通知を受ける必要がある．
* ユーザーは暗号鍵をどの認証タスクに使用するのか覚える必要があるため，ユーザーにとって意味のある適切で説明的な名前を暗号鍵に付ける．これにより, ユーザーはよく似た紛らわしい名前の複数の暗号鍵を扱わなくても済む．スマートフォンのような小さなモバイルデバイスで複数の暗号鍵から選択する場合，画面が小さいために暗号鍵の名前が短縮されると特に問題が多くなる．
* USB ポートのような直接的なコンピュータインターフェースの利用が限られる場合もユーザビリティがの問題になることがある． 例えば，ラップトップコンピュータの USB ポートの数は限られている．ユーザーはマルチファクタ OTP デバイスのために他の USB 周辺機器を取り外すことを強いられる場合がある．

### **ユーザビリティに関する考慮事項のまとめ**

それぞれの認証コードタイプの代表的な使用法と断続的なイベントに関するユーザビリティ考慮事項を表10-1 にまとめる．代表的な使用法についてのユーザビリティ考慮事項の多くは，行で示してあるようにほとんどの認証コードタイプに適用される．この表では，ユーザビリティについて認証コードタイプ全体に共通する特性と異なる特性を強調している．各列は，それぞれの認証コードに対処するユーザビリティの属性を簡単に識別できるようにしてある． ユーザーの目標や使用状況により，特定の属性が他の属性よりも重視されることがある．可能な限り代替の認証コードタイプを提供し，ユーザーがその中から選択できるようにする．

マルチファクタ認証コード（マルチファクタ OTP デバイス，マルチファクタ暗号化ソフトウェア，マルチファクタ 暗号化デバイスなど）もそれらの第２のファクタのユーザビリティ考慮事項を引き継ぐ． 生体認証はマルチファクタ認証ソリューションのアクティベーションファクタとしてのみ許可されているため，生体認証のユーザビリティ考慮事項は表 10-1 には含まれず，セクション 10.4 に説明してある．

**表 10-1 認証コードタイプ別のユーザビリティ考慮事項のまとめ**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ユーザビリティ考慮事項 | 記憶シークレット | ルックアップシークレット | アウトオブバンド | 単一ファクタ OTP デバイス | マルチファクタ OTP デバイス | 単一ファクタ暗号化ソフトウェア | 単一ファクタ暗号化デバイス | マルチファクタ暗号化ソフトウェア | マルチファクタ暗号化デバイス |
| **一般的な使用** | | | | | | | | | |
| 認証コードの利用可能性 –  ユーザーによる認証コードの保持のし易さ | w | w | w | w | w | w | w | w | w |
| ユーザー向けの平易な言葉づかい（指示, 説明, 通知, エラーメッセージなど） | w | w | w | w | w | w | w | w | w |
| ユーザー向けテキストや入力テキストの読みやすさ | w | w | w | w | w | w | w | w | w |
| 入力テキストの表示 |  | w | w | w | w |  |  |  |  |
| 入力サポート–64 文字の長さ, コピー＆ペースト | w |  |  |  |  |  |  |  |  |
| 入力テキストの非表示の遅延 | w |  |  |  |  |  |  |  |  |
| 適切な入力制限時間 | w | w | w | w | w |  |  |  |  |
| 入力ミス – 明確で意味あるフィードバックの必要性 | w | w | w | w | w |  |  |  |  |
| 最低10 回の入力再試行 | w | w | w | w | w |  |  |  |  |
| 残りの再試行回数の通知–明確で意味あるフィードバックの必要性 | w | w | w | w | w |  |  |  |  |
| 入力フォームの制限 | w | w | w | w | w | w | w | w | w |
| USB ポートなどの直接的インタフェースの場所と利用可能性 |  |  |  | w | w |  | w |  | w |
| 必要な物理的入力 (ボタンを押すなど) |  |  |  | w |  |  | w |  |  |
| 復号に必要な暗号鍵と意味をなす名前 |  |  |  |  |  | w |  | w | w |
| 入力要求の複雑さとサイズ |  | w |  |  |  |  |  |  |  |
| 認証シークレットにアクセスするためのセカンダリデバイスへの認証 |  |  | w |  |  |  |  |  |  |
| ハードウェアの継続接続の必要性なし |  |  |  |  |  |  |  |  | w |
| **断続的なイベント** | | | | | | | | | |
| ユーザーの非活動による再認証 | w | w | w | w | w | w | w | w | w |
| 定期的な再認証 | w | w | w | w | w | w | w | w | w |
| 技術サポートの提供 | w | w | w | w | w | w | w | w | w |
| 記憶シークレットの生成と変更のための提供 | w |  |  |  |  |  |  |  |  |

### **生体認証のユーザビリティの考慮事項**

このセクションは生体認証の一般的なユーザビリティの考慮事項について高度な視点から説明する． 生体認証のユーザビリティの更に詳しい説明は, *Usability & Biometrics, Ensuring Successful Biometric Systems* NIST Usability を参照．

生体認証方法にはいくつかあるが，認証には指紋, 顔, 虹彩の3つがよく利用されている.

***代表的な使用法***

* すべての方法に対して，ユーザーが感じる親しみやすさと慣れがデバイスのパフォーマンスを向上させる．
* デバイスアフォーダンス（つまり，ユーザーがアクションを実行することを可能にするデバイス特性），フィードバック，明確な指示は, 生体認証デバイスによるユーザー認証に極めて重要である． 例えば，生体検知のために必要なアクションについての明確な指示を提供する．
* 理想としては，ユーザーは第２の認証ファクタのために最も快適な方法を選択できるようにする．ユーザーはいくつかの生体認証方法を他の方法よりも快適に感じて受け入れる場合がある．
* 生体認証をアクティベーションファクタとするユーザーエクスペリエンス
* 残された試行回数について，明確で意味のあるフィードバックを提供する．混乱と不満を軽減するため，回数制限（つまりスロットリング）に対して次の試行まで待機しなければならない時間を知らせる．
* 指紋のユーザビリティ考慮事項:
* ユーザーは最初の登録に使用した指を覚えておく必要がある．
* 指の湿気の量はセンサーの読み取り能力に影響する．
* 指紋採取の品質に影響を及ぼす別の要因には，年齢，性別，職業がある（例 : 化学薬品を取り扱ったり手仕事が多かったりするユーザーは指紋が薄くなっている可能性がある）．
* 顔のユーザビリティ考慮事項 :
* 顔の認識精度に影響するため，ユーザーは登録の際に眼鏡などの人工物を装着していたかどうかを覚えている必要がある．
* 環境の照明条件の違いは認識精度に影響する．
* 顔の表情は認識精度に影響する（例 : 笑顔と普通の状態）．
* 顔の位置は認識精度に影響する（例 : カメラを見下ろす，カメラから遠い）．
* 虹彩のユーザビリティ考慮事項 :
* カラーコンタクトの装着は認識精度に影響することがある．
* 目の手術を受けたユーザーは手術後の再登録が必要になることがある．
* 環境の照明条件の違いは認識精度に，特に特定の虹彩色に影響することがある．

*断続的なイベント*

生体認証はマルチファクタ認証の第２のファクタとしてのみ許可されているため，第１のファクタの断続的なイベントのユーザビリティ考慮事項が引き続き適用される．認識精度に影響することがある生体認証を使用する断続的なイベントには以下があるが，これに限られない.

* 登録した指を怪我すると，指紋認識が機能しないことがある．指紋が薄くなったユ ー ザには指紋認証は困難である．
* 最初の顔認証登録から時間が経過すると，顔の自然の変化により認識精度に影響することがある． 体重の変化も影響の要因となる．
* 眼科手術を受けたユーザーは，再登録を行わないと虹彩認識が機能しないことがある．

すべての生体認証方法に対する断続的なイベントのユーザビリティ考慮事項は以下を含む.

* 代替の認証方法が利用可能で機能する必要がある．生体認証が機能しない場合，代替の第２ファクタとして記憶シークレットを使用できるようにする．
* 技術的な支援の提供 :
* 技術的な支援が得られる方法と場所をはっきりと伝える．例えば，オンラインセルフサービス機能へのリンクやヘルプデスクの電話番号などの情報をユーザーに提供する．理想としては，外部からの介入なしにユーザーが断続的なイベントから自ら回復できるよう十分な情報を提供する．
* 生体認証センサーの感度に影響する要因をユーザーに通知する (例 : センサーの清潔度 ) ．

# 参考資料

*This このセクションは参考情報である.*

### **一般**

[BALLOON] Boneh, Dan, Corrigan-Gibbs, Henry, and Stuart Schechter. “Balloon Hashing: A Memory-Hard Function Providing Provable Protection Against Sequential Attacks,” *Asiacrypt 2016*, October, 2016. Available at: https://eprint.iacr.org/2016/027.

[Blacklists] Habib, Hana, Jessica Colnago, William Melicher, Blase Ur, Sean Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Cranor. “Password Creation in the Presence of Blacklists,” 2017.

Available at: https://[www.internetsociety.org/sites/default/files/usec2017\_01\_3\_Habib\_paper.pdf](http://www.internetsociety.org/sites/default/files/usec2017_01_3_Habib_paper.pdf)

[Composition] Komanduri, Saranga, Richard Shay, Patrick Gage Kelley, Michelle L Mazurek, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Serge Egelman. “Of Passwords and People: Measuring the Eﬀect of Password-Composition Policies.” In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2595–2604. ACM, 2011. Available at: https://[www.ece.cmu.edu/~lbauer/papers/2011/chi2011-passwords.pdf](http://www.ece.cmu.edu/%7Elbauer/papers/2011/chi2011-passwords.pdf).

[E-Gov] *E-Government Act* [includes FISMA] (P.L. 107-347), December 2002, available at: <http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf>.

[EO 13681] Executive Order 13681, *Improving the Security of Consumer Financial Transactions*, October 17, 2014, available at: https://[www.federalregister.gov/d/2014-25439](http://www.federalregister.gov/d/2014-25439)

[FEDRAMP] General Services Administration, *Federal Risk and Authorization Management Program*, available at: https://www.fedramp.gov/[.](http://www.fedramp.gov/))

[ICAM] National Security Systems and 身元情報, Credential andアクセスManagement Sub-Committee Focus Group, Federal CIO Council, *ICAM Lexicon*, Version 0.5, March 2011.

[M-03-22] OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 26, 2003, available at: https://georgewbush- whitehouse.archives.gov/omb/memoranda/m03-22.html.

[M-04-04] OMB Memorandum M-04-04, *E-認証 Guidance for Federal Agencies*, December 16, 2003, available at: https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy04/m04-04.pdf.

[Meters] de Carné de Carnavalet, Xavier and Mohammad Mannan. “From Very Weak to Very Strong: Analyzing Password-Strength Meters.” In Proceedings of the Network and Distributed System Security Symposium (NDSS), 2014. Available at: <http://www.internetsociety.org/sites/default/files>/06\_3\_1.pdf

[NIST ユーザビリティ] National Institute and Standards and Technology, *ユーザビリティ & 生体認証, Ensuring Successful 生体認証ystems*, June 11, 2008, available at: <http://www.nist.gov/customcf>/get\_pdf.cfm?pub\_id=152184[.](http://www.nist.gov/customcf/get_pdf.cfm?pub_id=152184))

[OWASP-セッション] Open Web Application Security Project, *セッション Management Cheat Sheet*, available at: https://[www.owasp.org/index.php/セッション\_Management\_Cheat\_Sheet](http://www.owasp.org/index.php/Session_Management_Cheat_Sheet)

[OWASP-XSS-prevention] Open Web Application Security Project, *XSS (Cross Site Scripting) Prevention Cheat Sheet*, available at: https://www.owasp.org/index.php/XSS\_(Cross\_Site\_Scripting)\_Prevention\_Cheat\_Sheet.

[Persistence] herley, cormac, and Paul van Oorschot. “A Research Agenda Acknowledging the Persistence of Passwords,” IEEE Security&Privacy Magazine, 2012. Available at: <http://research.microsoft.com/apps/pubs/default.aspx?id=154077>.

[Privacy Act] *Privacy Act of 1974* (P.L. 93-579), December 1974, available at: https://[www.justice.gov](http://www.justice.gov/)/opcl/privacy-act-1974.

[Policies] Weir, Matt, Sudhir Aggarwal, Michael Collins, and Henry Stern. “Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords.” In Proceedings of the 17th ACM Conference on Computer and Communications Security, 162–175. CCS ’10. New York, NY, USA: ACM, 2010. doi:10.1145/1866307.1866327.

[セクション 508] セクション 508 Law and Related Laws and Policies (January 30, 2017), available at: https://[www.セクション 508.gov/content/learn/laws-and-policies](http://www.section508.gov/content/learn/laws-and-policies) .

[Shannon] Shannon, Claude E. “A Mathematical Theory of Communication,” *Bell System Technical Journal*, v. 27, pp. 379-423, 623-656, July, October, 1948.

[Strength] Kelley, Patrick Gage, Saranga Komanduri, Michelle L Mazurek, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Julio Lopez. “Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms.” In Security and Privacy (SP), 2012 IEEE Symposium On, 523–537. IEEE, 2012. Available at: <http://ieeexplore.ieee.org/iel5/6233637/6234400/06234434.pdf>.

### **標準**

[BCP 195] Sheﬀer, Y., Holz, R., and P. Saint-Andre, *Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*, BCP 195, RFC 7525,DOI 10.17487/RFC7525, May 2015, https://doi.org/10.17487/RFC7525.

[ISO 9241-11] International Standards Organization, ISO/IEC 9241-11 *Ergonomic requirements for oﬃce work with visual display terminals (VDTs) — Part 11: Guidance on ユーザビリティ*, March 1998, available at: https://[www.iso.org/standard/16883.html](http://www.iso.org/standard/16883.html)

[ISO/IEC 2382-37] International Standards Organization, *Information technology — Vocabulary — Part 37: 生体認証*, 2017, available at: http://standards.iso.org/ittf/PubliclyAvailableStandards/c066693\_ISO\_IEC\_2382-37\_2017.zip.

[ISO/IEC 10646] International Standards Organization, *Universal Coded Character Set*, 2014, available at: <http://standards.iso.org/ittf/PubliclyAvailableStandards>/c063182\_ISO\_IEC\_10646\_2014.zip.

[ISO/IEC 24745] International Standards Organization, *Information technology — Security techniques— Biometric information protection*, 2011, available at: <http://www.iso.org/iso/iso_catalogue>/catalogue\_tc/catalogue\_detail.htm?csnumber=52946.

[ISO/IEC 30107-1] International Standards Organization, *Information technology — Biometric presentation攻撃detection — Part 1: Framework*, 2016, available at: [http://standards.iso.org](http://standards.iso.org/)/ittf/PubliclyAvailableStandards/c053227\_ISO\_IEC\_30107-1\_2016.zip.

[ISO/IEC 30107-3] International Standards Organization, *Information technology — Biometric presentation攻撃detection — Part 3: Testing and reporting*, 2017.

[RFC 20] Cerf, V., *ASCII format for network interchange*, STD 80, RFC 20, DOI 10.17487/RFC0020, October 1969, https://doi.org/10.17487/RFC0020.

[RFC 5246] IETF, *The Transport Layer Security (TLS) Protocol Version 1.2*, RFC 5246, DOI 10.17487/RFC5246, August 2008, https://doi.org/10.17487/RFC5246.

[RFC 5280] IETF, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, RFC 5280, DOI 10.17487/RFC5280, May 2008, https://doi.org/10.17487/RFC5280.

[RFC 6238] IETF, *TOTP: Time-Based One-Time Password Algorithm*,RFC 6238, DOI 10.17487/RFC6238, https://doi.org/10.17487/RFC6238.

[RFC 6960] IETF, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*, RFC 6960, DOI 10.17487/RFC6960, https://doi.org/10.17487/RFC6960.

[UAX 15] Unicode Consortium, *Unicode Normalization Forms*, Unicode Standard Annex 15, Version 9.0.0, February, 2016, available at: [http://www.unicode.org/reports/tr15/.](http://www.unicode.org/reports/tr15/)

### **NIST 特別出版物**

NIST 800 Series Special Publications are available at: <http://csrc.nist.gov/publications/nistpubs>/index.html[.](http://csrc.nist.gov/publications/nistpubs/index.html)) The following publications may be of particular interest to those implementing systems of applications requiring デジタル認証.

[SP 800-38B] NIST Special Publication 800-38B, *Recommendation for Block Cipher Modes of Operation: the CMAC Mode for 認証*, October, 2016, <http://dx.doi.org/10.6028>/NIST.SP.800-38B[.](http://dx.doi.org/10.6028/NIST.SP.800-38B))

[SP 800-52] NIST Special Publication 800-52 Revision 1, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*, April, 2014, <http://dx.doi.org/10.6028>/NIST.SP.800-52r1

[SP 800-53] NIST Special Publication 800-53 Revision 4, *Recommended Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (updated January 22, 2015), <http://dx.doi.org/10.6028/NIST.SP.800-53r4>[.](http://dx.doi.org/10.6028/NIST.SP.800-53r4))

[SP 800-57 Part 1] NIST Special Publication 800-57 Part 1, Revision 4, *Recommendation for Key Management, Part 1: General*, January 2016, <http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4>[.](http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4))

[SP 800-63-3] NIST Special Publication 800-63-3, *デジタル ID Guidelines*, June 2017, https://doi.org/10.6028/NIST.SP.800-63-3.

[SP 800-63A] NIST Special Publication 800-63A, *デジタル ID Guidelines: 登録 and 身元情報 検証 Requirements*, June 2017, https://doi.org/10.6028/NIST.SP.800-63a.

[SP 800-63C] NIST Special Publication 800-63C, *デジタル ID Guidelines: 認証 and Lifecycle Management*, June 2017, https://doi.org/10.6028/NIST.SP.800-63c.

[SP 800-90Ar1] NIST Special Publication 800-90A Revision 1, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, June 2015, <http://dx.doi.org/10.6028>/NIST.SP.800-90Ar1[.](http://dx.doi.org/10.6028/NIST.SP.800-90Ar1))

[SP 800-107] NIST Special Publication 800-107 Revision 1, *Recommendation for Applications Using 承認された Hash Algorithms*, August 2012, <http://dx.doi.org/10.6028/NIST.SP.800-107r1>[.](http://dx.doi.org/10.6028/NIST.SP.800-107r1))

[SP 800-131A] NIST Special Publication 800-131A Revision 1, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, November 2015, <http://dx.doi.org/10.6028/NIST.SP.800-131Ar1>

[SP 800-132] NIST Special Publication 800-132, *Recommendation for Password-Based Key Derivation*, December 2010, <http://dx.doi.org/10.6028/NIST.SP.800-132>.

[SP 800-185] NIST Special Publication 800-185, *SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash*, December, 2016, https://doi.org/10.6028/NIST.SP.800-185.

### **Federal Information Processing Standards**

[FIPS 140-2] Federal Information Processing Standard Publication 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001 (with Change Notices through December 3, 2002), https://doi.org/10.6028/NIST.FIPS.140-2.

[FIPS 198-1] Federal Information Processing Standard Publication 198-1, *The Keyed-Hash Message 認証 Code (HMAC)*, July 2008, https://doi.org/10.6028/NIST.FIPS.198-1.

[FIPS 201] Federal Information Processing Standard Publication 201-2, *Personal 身元情報 Verification (PIV) of Federal Employees and Contractors*, August 2013, <http://dx.doi.org/10.6028>

/NIST.FIPS.201-2[.](http://dx.doi.org/10.6028/NIST.FIPS.201-2))

[FIPS 202] Federal Information Processing Standard Publication 202, *SHA-3 Standard: Permutation- Based Hash and Extendable-Output Functions*, August 2015, <http://dx.doi.org/10.6028>/NIST.FIPS.202[.](http://dx.doi.org/10.6028/NIST.FIPS.202))

**付録 A—記憶シークレットの強度**

*この付録は参考情報である.*

この付録では，説明を容易にするため”パスワード”という単語を用いる．パスワードが使用されている箇所では，パスフレーズとPINもそこに含まれると解釈すべきである．

### **はじめに**

ユーザビリティとセキュリティの観点からは, パスワードの使用には大きな不満が伴うにもかかわらず，認証の[持続性]ある形式として極めて広く利用され続けている．しかしなが ら，複雑で恣意的なシークレットを記憶する能力は限られているため，容易に推測できるパスワードを選ぶことが多い．その結果として発生するセキュリティ上の問題に対処するため，オンラインサービスではこうした記憶シークレットを複雑にするために，いくつかのルールが導入されてきた．最も注目すべき形式としては，ユーザーがパスワードを選択する際に少なくとも1文字以上の数字，大文字，記号といった文字種を組み合わせるよう求める構成ルールがある．しかし，漏洩したパスワードデータベースの分析により，そのようなルールでは，ユーザビリティと記憶能力へ与 える影響が大きいにもかかわらず, 当初策定された [ポリシー] ほど利点は大きくないことが明らかになった．

ユーザーが選択したパスワードの複雑さは， [シャノン] エントロピーという情報理論の概念を用いて特徴付けられることが多い．確定的分布関数に従うデータに対してエントロピーを計算することは容易だが，ユーザーが選択したパスワードのエントロピーを推測することは難しく，それを行うための過去の努力は特に正確というわけではなかった．このため，主にパスワードの長さの観点から, 幾分シンプルな別のアプローチをここに紹介する．

パスワードの利用に関連する多くの攻撃は, パスワードの複雑さと長さに影響されない．キー入力ロギング，フィッシング，ソーシャルエンジニアリング攻撃は，複雑で長いパスワードに対しても，それがシンプルなものであるのと同様に機能する．これらの攻撃はこの付録の対象外である．

### **長さ**

パスワードの長さは，パスワードの強度 [強度] [構成] を特徴付ける主要因であることがわかっている．短すぎるパスワードは単語や一般的に選択されたパスワードを利用する辞書攻撃と同様に総当たり攻撃を受ける．

最低でもどの程度の長さのパスワードが必要となるかは，想定する脅威モデルによって大きく左右される．攻撃者がパスワードを推測してログインを試みるオンライン攻撃では，許容するログイン試行 回数を制限して脅威を緩和することができる．攻撃者（または何度もタイプミスを繰り返す認証要求者）が大量のパスワード推測を行い加入者に対するDoS攻撃を容易に行えないようにするためには，誤った試行回数がさほど多くないのに回数制限が発生するのではなく, 推測が成功する確率が大きくなる前に発生するようにパスワードを十分複雑にする必要がある．

オフライン攻撃は，攻撃者がデータベースに侵入して1つ以上のハッシュされたパスワードを入手する場合に発生する可能性がある．攻撃者が1人または複数のユーザーのパスワードを突き止める能力は，パスワードの保管方法に左右される．一般的には，パスワードはランダム値を用いてソルトを追加したうえでハッシュ化され，計算コストが高いアルゴリズムを用いることが望ましい．そのような方法でさえも，回数制限なしでは毎秒何十億もの計算を行うことができる現在の攻撃者の能力に対抗するためには，パスワードはオンライン攻撃だけに対抗することを想定したよりもはるかに複雑な桁数にする必要がある．

ユーザーには，理に適った範囲内で望みどおりの長さのパスワードを使うことを奨励べきである． ハッシュされたパスワードの長さはパスワードそのものの長さと無関係であるため，ユーザーが希望すれば長いパスワード（またはパスフレーズ）の利用を許可しない理由はない．極端に長いパスワード（おそらくはメガバイト）はハッシュ処理に極端に時間を要すると考えられるため，何らかの制限を行うのは理に適っている．

### **複雑さ**

上記のように，構成ルールはユーザーが選択したパスワードの推測難易度を上げる目的で一般的に利用されている．しかし，研究ではユーザーが構成ルール [ポリシー] で課せられた要件に対して非常に安易な方法で対応することが明らかになった．例えば，パスワードとして”password”を選択したユーザーは，大文字と数字を含む要件を与えると，比較的高い確率で”Password1”を選択し，記号を要件に追加すると”Password1!”を選択している．

複雑なパスワードを作成しようとしてもオンラインサービスで拒否されることにもユーザーは不満を抱いている．多くのサービスではスペースや特殊文字を含むパスワードが拒否される．特殊文字が受け入れられないケースには，特殊文字を用いるSQLインジェクションのような攻撃を回避する目的がある．しかし，適切にハッシュ化されたパスワードはいかなる場合でもそのままデータベースに送信されることはないため，そのような予防策は不要である．また, フレーズが使用できるようにスペース文字を使えるようにすべきである．しかし，スペース文字はそれ自体ではパスワードの複雑さを僅かに増加させるにすぎず，ユーザビリティの問題(例えば，スペース文字を2つ使うと検出されないなど)を招く可能性があるため，入力されたパスワードから連続するスペース文字を検証の前に削除すると効果的である．

ユーザーのパスワードの選択は非常に簡単に予想でき，攻撃者は過去に成功した正しいパスワードを推測する可能性がある．こうしたパスワードには，辞書にある単語や上記の例の” Password1!” のように過去に漏洩したパスワードがある. この理由から，ユーザーが選択したパスワードを許容できないパスワードのブラックリストと比較することを推奨する．このブラックリストは，ユーザーが選択する可能性が高い過去に漏洩したパスワード，語彙集，辞書の単語, 特定の用語（サービス自体の名前など）を含むべきである．ユーザーのパスワードの選択は最低文字数の要件が適用されるため，ブラックリストには要件に合致したものだけを含める必要がある．

極端に複雑な記憶シークレットは新たな脆弱性を生み出す. シークレットを記憶できる可能性が減り，書き留めたり安全でない方法で電子的に記録したりする可能性が高まる．これらの慣例は必ずしも脆弱であるわけではないが，統計的に見るとそのような記録方法の中には脆弱なものがある．これは極端に長いか極端に複雑な記憶シークレットを要求しないということの補足的な理由である．

### ランダムに選択されたシークレット

記憶シークレットの強度を決定するもう１つの要因が，シークレットが生成されるプロセスである．（ほとんどの場合は検証者やCSPによって）ランダムに選択され一様に配布されるシークレットは、同じ長さと複雑さの要件に対してユーザーが選択するシークレットに比べ, パスワード推測や総当たり攻撃の難易度が高くなろう．そのため，LOA2ではSP 800-63-2はランダムに生成したPINを6桁以上としているのに対し，ユーザーが選択するシークレットを8文字以上としている．

上で論じたように，記憶シークレットの長さ要件を考慮した脅威モデルには，オンライン攻撃に対する回数制限が含まれているが，オフライン攻撃は含まれていない．このような限界があるため，6桁のランダムに生成されたPINは記憶シークレットに対して依然として適切であると見なされる．

### **まとめ**

ここで推奨されている内容を超える長さと複雑さの要件は，記憶シークレットの難易度を大幅に増加させ，ユーザーの不満を増加させる．結果としてユーザーはこうした制限を回避することが多いため逆効果になる．さらに，ブラックリスト，安全なハッシュストレージ，回数制限などの他の緩和策は，今日の総当たり攻撃を防ぐにはより効果的である．したがって，複雑さについて追加の要件 が課されることはない．

Privacy Policy ([http://www.nist.gov/public\_aﬀairs/privacy.cfm#privpolicy)](http://www.nist.gov/public_a%EF%AC%80airs/privacy.cfm#privpolicy)) | Security Notice ([http://www.nist.gov/public\_aﬀairs/privacy.cfm#secnot)](http://www.nist.gov/public_a%EF%AC%80airs/privacy.cfm#secnot)) | Accessibility Statement ([http://www.nist.gov](http://www.nist.gov/)

/public\_aﬀairs/privacy.cfm#accesstate) | Send feedback (https://github.com/openid-foundation- japan/800-63-3-final/issues/) ? (/800-63-3-final/comment\_help.html)