NIST Special Publication 800-63B

Digital Identity Guidelines (翻訳版)

Authentication and Lifecycle Management

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

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

COMPUTER SECURITY

NIST Special Publication 800-63B

Digital Identity Guidelines

Authentication and Lifecycle Management

Paul A. Grassi
Elaine M. Newton
Applied Cybersecurity Division
Information Technology Laboratory

Ray A. Perlner
Andrew R. Regenscheid
Cybersecurity Division
Information Technology Laboratory

James L. Fenton
Altmode Networks
Los Altos, CA

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

Privacy Authors:
Naomi B. Lefkovitz
Applied Cybersecurity Division
Information Technology Laboratory

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

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

Justin P. Richer
Bespoke Engineering
Billerica, MA

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

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-63B
Natl. Inst. Stand. Technol. Spec. Publ. 800-63B, 78 pages (June 2017)
CODEN: NSPUE2

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

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at http://csrc.nist.gov/publications/ (http://csrc.nist.gov/publications/).

Comments on this publication may be submitted to:

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)

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

概要

これらのガイドラインは, Digital Identityサービスを実装する連邦政府機関に対する技術的要件を提供し, この目的以外の標準の開発や利用を制限してはいない. これらのガイドラインは, オープンなネットワークを介して政府のシステムと相互作用するSubjectのAuthenticationに焦点を当て, 与えられたClaimantが以前にAuthenticateされたSubscriberであることを確認する. Authenticationプロセスの結果は, Authenticationを行うシステムによってローカルで使用されたり, Federated Identity システムの他の場所でassertされたりすることがある. このドキュメントでは, 3つのAuthenticator Assuarance Levelのそれぞれに対して技術要件を定義する. この刊行物は, NIST Special Publication（SP）800-63-2の対応するセクションに優先するものである.

キーワード

authentication; credential service provider; digital authentication; digital credentials; electronic authentication; electronic credentials, federation.

謝辞

The authors gratefully acknowledge Kaitlin Boeckl for her artistic graphics contributions to all volumes in the SP 800-63 suite and the contributions of our many reviewers, including Joni Brennan from the Digital ID & Authentication Council of Canada (DIACC), Kat Megas, Ellen Nadeau, and Ben Piccarreta from NIST, and Ryan Galluzzo and Danna Gabel O'Rourke from Deloitte & Touche LLP.

The authors would also like to acknowledge the thought leadership and innovation of the original authors: Donna F. Dodson, W. Timothy Polk, Sarbari Gupta, and Emad A. Nabbus. Without their tireless efforts, we would not have had the incredible baseline from which to evolve 800-63 to the document it is today. In addition, special thanks to the Federal Privacy Council's Digital Authentication Task Force for the contributions to the development of privacy requirements and considerations.

要求記法および規則

「SHALL(するものとする)」及び「SHALL NOT(しないものとする)」という用語は, 刊行物に厳密に従うことを要求しており, 内容と異なってはならない.

「SHOULD(すべきである)」及び「SHOULD NOT(すべきではない)」という用語は, いくつかある選択肢の中で特定の推奨があ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. ある行動指針を推奨するが, 必須であることまでは要求しない. (否定の意味では)ある選択肢または行動指針を非推奨するが, 禁止はしない.

「MAY(してもよい)」及び「NEED NOT(しなくてよい)」という用語は, 刊行物の範囲において, 行動指針が許容できることを示す.

「CAN(できる)」及び「CANNOT(できない)」という用語は, 物質的, 物理的, 偶発的であろうとなかろうと, 可能性や能力があること, または否定の意味ではその可能性や能力が欠如していることを意味する.

Table of Contents

1 Purpose

本セクションは参考情報である.

本書及び付随文書であるSpecial Publication (SP) 800-63 (sp800-63-3.html), SP 800-63A (sp800-63a.html)およびSP 800-63C (sp800-63c.html)は, 政府機関に対してDigital Authenticationの実装のための技術的なガイドラインを提供する.

2 Introduction

本セクションは参考情報である.

Digital Identityはオンライン取引に関わるSubjectの一意な表現である. Digital Identity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Sujectまで追跡できる必要はない. 言い換えれば, デジタルサービスにアクセスするということが, 根本的なSubjectの実在の表現が知られていることを意味していなくてもよい. Identity ProofingはSubjectが実際には彼らが何者であるかを確認する. Digital Authenticationは, Digital Identityを主張するために利用いる一つ以上のAuthenticatorの妥当性を決定するプロセスである. Authentcationはデジタルサービスに対してアクセスしようとしているSubjectが, Authenticateするための技術を制御しているということを確認する行為である. 再訪問するようなサービスでは, 正常にAuthenticateすることが今日サービスにアクセスしているSubjectが以前サービスにアクセスした人と同一であるということを示す合理的なリスクベースの保証をもたらす. Digital Identityは多くの場合オープンなネットワークを介した個人のProofingを伴い, 常にオープンなネットワークを介した個人のAuthenticationが必要となるため技術的な技術的な課題がある. この課題には, SubjectのDigital Identityを不正にかたることにつながるなりすましや他の攻撃の可能性

が複数存在している.

Subscriberの継続的なAuthenticationは，Subscriberを彼らのオンラインでの活動と結びつけるプロセスの中心である．Subscriber Authenticationは，Claimantが指定されたSubscriberと関連付けられている一つ以上の*Authenticator*(以前のバージョンのSP 800-63では*token*と呼ばれていたもの)を制御していることを検証することで実施される．Authenticationが成功した結果は，Relying Party(RP)に対する仮名または仮名でない識別子のAssertionであり，オプションで他のIdentity情報も対象となる.

本書は，様々な*Authenticator Assurance Level*(AAL)で利用されるAuthenticatorの選択を含むAuthenticationプロセスの分類における推奨を提供する．さらに本書は，紛失や盗難に際しての取り消しを含む，Authenticatorのライフサイクルにおける推奨を提供する.

この技術的ガイドラインは，ネットワーク越しのシステムに対するSubjectのDigital Authenticationに適用される．ガイドラインは(ビルなどへの)物理アクセスのための人物のAuthenticationについては考慮していないが，デジタルアクセスのために利用されるものと同じクレデンシャルが，物理アクセスのAuthenticationの目的でも利用されてよい．さらにこの技術的ガイドラインは，Authenticationプロトコルに参加する連邦政府機関のシステム及びサービスの提供者が，Subscriberに対してAuthenticateされることを要求する.

Authenticationトランザクションの強度はAALとして知られている分類によって特徴付けられる．より強力な認証(より高いAAL)では，悪意のある当事者がAuthenticationプロセスを成功裏に覆すために一層の機能及びリソースが必要となる．より高いAALでのAuthenticationは攻撃リスクを効果的に減少させることができる．個々のAALに求められる技術要件の概要を以下に記載する; 特別な標準要求については，本書の Section 4 及び 5 を参照.

Authenticator Assurance Level 1 - AAL 1はSubscriberのアカウントに対して結び付けられているAuthenticatorをClaimantが制御しているというある程度の保証をもたらす．AAL 1では幅広く利用可能なAuthentication技術を利用した，単一要素または多要素のAuthenticationを必要とする．Authenticationが成功するには，そのClaimantが，セキュアなAuthenticationプロトコルを介して，自身がそのAuthenticatorを所有・制御していることを証明する必要がある.

Authenticator Assurance Level 2 - AAL 2は，Subscriberのアカウントに対して結び付けられているAuthenticatorをClaimantが制御しているという高い確実性をもたらす．セキュアなAuthenticationプロトコルを介して，異なる2つのAuthentication要素を所有・制御していることを証明する必要がある．AAL 2及びそれ以上では，Approved Cryptography技術が必要とされる.

Authenticator Assurance Level 3 - AAL 3は，Subscriberのアカウントに対して結び付けられているAuthenticatorをClaimantが制御しているという非常に高い確実性をもたらす．AAL 3におけるAuthenticationは，暗号プロトコルを介した鍵を所有していることの証明に基づいている．AAL 3のAuthenticationは，ハードウェアベースのAuthenticatorまたはVerifierに対してなりすまし耐性を提供するAuthenticatorを要求す．この際，同じデバイスが両方の要件を満たしていても良い．AAL 3でAuthenticateするために，ClaimantはセキュアなAuthenticationプロトコルを介して2つの異なるAuthentication要素を所有・制御していることを証明する必要がある．Approved Cryptography技術

が必要とされる.

次の表は本文書の各セクションが標準であるか参考情報であるかを示している:

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. 定義及び略語	参考情報
4. Authenticator Assurance Levels	標準
5. Authenticator及びVerifierの要件	標準
6. Authenticatorライフサイクルの要件	標準
7. セッション管理	標準
8. 脅威とセキュリティに関する考慮事項	参考情報
9. プライバシに関する考慮事項	参考情報
10. ユーザビリティに関する考慮事項	参考情報
11. 参照	参考情報
付録A — 記憶シークレットの強度	参考情報

3 定義及び略語

定義及び略語の全体一式についてはSP 800-63 (sp800-63-3.html) 付録 Aを参照.

4 Authenticator Assurance Levels

本セクションは標準及び参考情報の題材両方を含む.

指定されたAALの要件を満たすために，Claimantは少なくとも自身がSubscriberとして認識される強度のレベルでAuthenticateされるものとする(SHALL). Authenticationプロセスの結果は識別子であり，SubscriberがRPに対してAuthenticateするたびに使われるものとする(SHALL). それは仮名でもよい(MAY)，Subscriberの識別子は異なる目的で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Subjectが再登録される場合には再利用すべきである(SHOULD). Subscriberをを一意なSubjectであると識別する他の属性もまた提供されてもよい(MAY).

各AALにおけるAuthenticator及びVerifierに対する標準要件の詳細についてはセクション5に示されている.

最も適切なAALの選択方法の詳細については SP 800-63 (sp800-63-3.html) セクション6.2参照.

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

IAL1では，属性はDigital Identityサービスによって収集され，利用可能となる. 任意のPIIまたは他の個人情報は - self-assertedまたは確認されたもののどちらでも - 多要素Authenticationを必要とする. 従って，連邦政府機関はself-assertedであるPIIや他の個人情報がオンラインで利用可能である場合，最低でもAAL2を選択するものとする(SHALL).

4.1 Authenticator Assurance Level 1

本セクションは標準である.

AAL 1はSubscriberのアカウントに対して結び付けられているAuthenticatorをClaimantが制御しているという，ある程度の保証を提供する. AAL 1では幅広く利用可能なAuthentication技術を利用した，単一要素または多要素のAuthenticationを必要とする. Authenticationが成功するには，そのClaimantが，セキュアなAuthenticationプロトコルを介して，自身がそのAuthenticatorを所有・制御していることを証明する必要がある.

4.1.1 許可されているAuthenticatorタイプ

AAL1のAuthenticationでは，Section 5 で定義されている次のAuthenticatorタイプの何れかを利用するものとする(SHALL):

- 記憶シークレット (Section 5.1.1)
- ルックアップシークレット (Section 5.1.2)
- アウトオブバンドデバイス (Section 5.1.3)
- 単一要素ワンタイムパスワード (OTP) デバイス (Section 5.1.4)
- 多要素 OTP デバイス (Section 5.1.5)

- 単一要素暗号ソフトウェア (Section 5.1.6)
- 単一要素暗号デバイス (Section 5.1.7)
- 多要素暗号ソフトウェア (Section 5.1.8)
- 多要素暗号デバイス (Section 5.1.9)

4.1.2 Authenticator及びVerifierの要件

AAL 1で用いられる暗号Authenticatorは，Approved Cryptographyを利用するものとする(SHALL). オペレーティング・システム環境で動作するソフトウェアベースのAuthenticatorは，該当する場合(例，マルウェアによって)それ自身が動作している利用者のエンドポイントのセキュリティ侵害検出を試みてもよく(MAY)，そのようなセキュリティ侵害が検出された場合には操作を完了すべきででではない(SHOULD NOT).

ClaimantとVerifierとの間の通信(アウトオブバンドAuthenticatorの場合はプライマリチャネル)は，Authenticator出力の秘匿性と中間者攻撃に対する耐性を提供するAuthenticateされた保護チャネルを介して行われるものとする(SHALL).

政府機関が運用するVerifierは，AAL 1において，FIPS 140 Level 1 の要件に適合していることが確認されるものとする(SHALL).

4.1.3 Reauthentication

Section 7.2に記載があるように，Subscriberのセッションの定期的なReauthenticationが行われるものとする(SHALL)．AAL 1では，ユーザの活動に関わらず，SubscriberのReauthenticationは少なくとも30日に1回は繰り返し実施すべきである(SHOULD)．セッションはこの時間制限に到達したら終了される(すなわちログアウトされる)べき(SHOULD)である

4.1.4 セキュリティ統制

CSPは，SP 800-53 または等価な連邦政府機関(例えば FEDRAMP) あるいは業界標準で定義されているセキュリティ統制の低度な基準から適切に調整されているセキュリティ統制を採用することとする(SHALL)．CSPは影響が低度なシステム，またはそれに相当するものに対する最低限の保証関連の統制を果たしていることを保証することとする(SHALL).

4.1.5 レコード保持ポリシ

CSPは，準拠法，規則，及び任意のNational Archives and Records Administration (NARA)のレコード保持スケジュールを含むポリシに合致するそれぞれのレコード保持ポリシに従う．もしCSPがいずれの必須要件なくレコードを保持することを選択する場合，CSPはレコードの保持期間を決定するためのプライバシ及びセキュリティリスクのアセスメントを含むリスク管理プロセスを実施するものとし(SHALL)，Subscriberに対して当該保持ポリシについて通知するものとする(SHALL).

4.2 Authenticator Assurance Level 2

本セクションは標準である.

AAL 2は，Subscriberのアカウントに対して結び付けられているAuthenticatorをClaimantが制御しているという，高い確実性を提供する．セキュアなAuthenticationプロトコルを介して，2つの異なるAuthentication要素の所有と制御の証明を必要とする．Approved Cryptographic技術がAAL2及びそれ以上では必要である.

4.2.1 許可されているAuthenticatorタイプ

AAL2のAuthenticationでは， 一つの多要素Authenticatorまたは2つの単一要素Authenticatorの組み合わせのどちらかを利用するものとする(SHALL)．一つの多要素Authenticatorは，デバイスをアクティベートするために統合されたバイオメトリックセンサを備え，暗号的にセキュアであるようなデバイスのように，1回のAuthenticationイベントで二つの要素を必要とする．Authenticatorの要件はSection 5で指定されている.

多要素Authenticatorを利用する際，以下の任意のものを利用してよい(MAY):

- 多要素 OTP デバイス (Section 5.1.5)
- 多要素暗号ソフトウェア (Section 5.1.8)
- 多要素暗号デバイス (Section 5.1.9)

2つの単一要素Authenticatorを組み合わせる際には，記憶シークレットAuthentiactor (Section 5.1.1)と以下のリストから1つの所有ベース(“something you have”)のAuthenticatorを含むこととする(SHALL):

- ルックアップシークレット (Section 5.1.2)
- アウトオブバンドデバイス (Section 5.1.3)
- 単一要素 OTP デバイス (Section 5.1.4)
- 単一要素暗号ソフトウェア (Section 5.1.6)
- 単一要素暗号デバイス (Section 5.1.7)

> 注記: Section 5.2.3でのバイオメトリックAuthenticationの要件を満たすために，デバイスはバイオメトリックに加えて，デバイスをAuthenticateされる必要がある &mdash バイオメトリックは1つの要素としてみなせるが，それ自体をAuthenticatorとしてみなしてはいない．従って，バイオメトリックを用いたAuthenticationを実施する時，2つのAuthenticatorを使う必要はない．なぜならば，関連付けられたデバイスは”something you have”として機能し，バイオメトリックは”something you are”として機能するからである.

4.2.2 Authenticator及びVerifierの要件

AAL 2で用いられる暗号Authenticatorは，Approved Cryptographyを使うものとする(SHALL)．政府機関によって調達されたAuthenticatorは，FIPS 140 Level 1の要件に適合していることを確認される

ものとする(SHALL). オペレーティング・システム環境で動作するソフトウェアベースのAuthenticatorは，該当する場合(例，マルウェアによって)それ自身が動作しているプラットフォームのセキュリティ侵害検知を試みてもよく(MAY)，そのようなセキュリティ侵害が検出されると操作を拒否すべき(SHOULD)である. AAL2では少なくとも1つのAuthenticatorはSection 5.2.8に記載されているように，リプレイ耐性があるものとする(SHALL). AAL2のAuthenticatorはSection 5.2.9に記載されているように，少なくとも1つのAuthenticatorからAuthenticationの意図を明示するべきである(SHOULD).

ClaimantとVerifierとの間の通信(アウトオブバンドAuthenticatorの場合はプライマリチャネル)は，Authenticator出力の秘匿性と中間者攻撃に対する耐性を提供するAuthenticateされた保護チャネルを介して行われるものとする(SHALL).

政府機関が運用するVerifierは，AAL 2において，FIPS 140 Level 1 の要件に適合していることが確認されるものとする(SHALL).

Authentication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際に，（典型的にはPINやバイオメトリックを利用して）デバイスをアンロックする行為はAuthentication要素の一つとしてみなされないものとする(SHALL NOT). 一般的には，Verifierがそのデバイスがロックされていたのか，あるいはアンロックプロセスが関連するAuthenticatorタイプの要件に合致していたのかを把握することができない.

バイオメトリック要素がAAL 2で利用される場合，Section 5.2.3に規定されたパフォーマンス要件を満たすものとし(SHALL)，Verifierはバイオメトリックセンサー及び後続処理がこれらの要件に合致していることを明確にしなければならない(SHOULD).

4.2.3 Reauthentication

Section 7.2に記載があるように，Subscriberのセッションの定期的なReauthenticationが行われるものとする(SHALL). AAL 2では，ユーザの活動に関わらず，SubscriberのReauthentication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回は繰り返されるものとする(SHALL). 30分以上継続している非活動期間の後は，SubscriberのReauthenticationは繰り返されるものとする(SHALL). セッションはこの時間制限に到達したら終了される(すなわちログアウトされる)ものとする(SHALL).

まだ時間制限に到達していないセッションのReauthenticationは，記憶シークレットだけ，あるいはまだ有効なセッションシークレットと連動しているバイオメトリックを要求してもよい(MAY). Verifierは非活動によるタイムアウトの直前に，ユーザに対して活動を促してもよい(MAY).

4.2.4 セキュリティ統制

CSPは，SP 800-53 または等価な連邦政府機関(例えば FEDRAMP) あるいは業界標準で定義されているセキュリティ統制の中度な基準から適切に調整されているセキュリティ統制を採用することとする(SHALL). CSPは影響が中度なシステム，またはそれに相当するものに対する最低限の保証関連の統制を果たしていることを保証することとする(SHALL).

4.2.5 レコード保持ポリシ

CSPは，準拠法，規則，及び任意のNational Archives and Records Administration (NARA)のレコード保持スケジュールを含むポリシに合致するそれぞれのレコード保持ポリシに従う．もしCSPがいずれの必須要件なくレコードを保持することを選択する場合，CSPはレコードの保持期間を決定するためのプライバシ及びセキュリティリスクのアセスメントを含むリスク管理プロセスを実施するものとし(SHALL)，Subscriberに対して当該保持ポリシについて通知するものとする(SHALL).

4.3 Authenticator Assurance Level 3

本セクションは標準である.

AAL 3は，Subscriberのアカウントに対して結び付けられているAuthenticatorをClaimantが制御しているという，極めて高い確実性を提供する．AAL3におけるAuthentication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 Authenticationは，1つのハードウェアベースのAuthenticatorと，1つのVerifierなりすまし耐性を備えるAuthenticatorを利用するものとする(SHALL)．同じデバイスが両方の要件を満たしても良い(MAY)．AAL3でAuthenticateするために，claimantはセキュアなAuthenticationプロトコルを介して，2つの異なるAuthentication要素の所有と制御を証明するものとする(SHALL)．Approved Cryptographic技術が必要である.

4.3.1 許可されているAuthenticatorタイプ

AAL3のAuthenticationでは， セクション4.3の要件を満たすAuthenticatorの組み合わせの1つを利用するものとする(SHALL)．有効な組み合わせは次の通り:.

- 多要素暗号デバイス (Section 5.1.9)
- 単一要素暗号デバイス (Section 5.1.7)を記憶シークレット (Section 5.1.1)と併用
- 多要素 OTP デバイス(ソフトウェアまたはハードウェア) (Section 5.1.5)を単一要素暗号デバイス (Section 5.1.7)と併用
- 多要素 OTP デバイス(ハードウェアのみ) (Section 5.1.5)を単一要素暗号ソフトウェア (Section 5.1.6)と併用
- 単一要素 OTP デバイス(ハードウェアのみ) (Section 5.1.4) を多要素暗号ソフトウェア (Section 5.1.8)と併用
- 単一要素 OTP デバイス(ハードウェアのみ) (Section 5.1.4) を単一要素暗号ソフトウェア (Section 5.1.6)及び記憶シークレット(Section 5.1.1)と併用

4.3.2 Authenticator及びVerifierの要件

ClaimantとVerifierとの間の通信は，Authenticator出力の秘匿性と中間者攻撃に対する耐性を提供するAuthenticateされた保護チャネルを介して行われるものとする(SHALL)．AAL3 Authenticationで利用される全ての暗号デバイスAuthenticatorは，Section 5.2.5に記載されているVerifierなりすまし耐性を備えているものとし(SHALL)，Section 5.2.8に記載されているように，リプレイ耐性があるものとする(SHALL)．AAL3のAuthenticatorはSection 5.2.9に記載されているように，少なくとも1つの

AuthenticatorからAuthentication及びReauthenticationの意図を明示するべきである(SHOULD).

AAL 3で利用される多要素Authenticatorは，少なくともFIPS 140 Level 3物理セキュリティを伴っており，総合的にFIPS 140 Level 2またはそれ以上で確認されたハードウェア暗号モジュールであるものとする(SHALL). AAL3で利用される単一要素暗号デバイスは，少なくともFIPS 140 Level 3物理セキュリティを伴っており，総合的にFIPS 140 Level 1またはそれ以上で確認されたハードウェア暗号モジュールであるものとする(SHALL).

AAL3におけるVerifierは，FIPS 140 Level 1またはそれ以上の基準で確認されるものとする(SHALL).

AAL3におけるVerifierは，Section 5.2.7に記載のあるように，少なくとも 1 つのAuthenticator要素においてVerifier危殆化耐性があるものとする(SHALL).

AAL3におけるハードウェアベースのAuthenticatorとVerifierは，関連するサイドチャネル(例，タイミング及び消費電力分析)攻撃への耐性があるべきである(SHOULD). 関連するサイドチャネル攻撃は，CSPによって実施されるリスクアセスメントにより，明確にされるものとする(SHALL).

Authentication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際に，デバイスが上記の要件に合致している可能性が推測される場合でも，デバイスをアンロックする行為はAuthentication要素の一つとしてみなされないものとする(SHALL NOT). これは，一般的には，Verifierがそのデバイスがロックされていたのか，あるいはアンロックプロセスが関連するAuthenticatorタイプの要件に合致していたのかを把握することができないからである.

バイオメトリック要素がAAL3で利用される場合，Verifierはバイオメトリックセンサー及び後続処理が，Section 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明確にしなければならない(SHALL).

4.3.3 Reauthentication

Section 7.2に記載があるように，Subscriberのセッションの定期的なReauthenticationが行われるものとする(SHALL). AAL3では，Section 7.2に記載があるように，ユーザの活動に関わらず，SubscriberのReauthentication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回は繰り返されるものとする(SHALL). 15分以上継続している非活動期間の後は，SubscriberのReauthenticationは繰り返されるものとする(SHALL). Reauthenticationには両方のAuthenticator要素を用いるものとする(SHALL). セッションはこれらの時間制限に到達したら終了される(すなわちログアウトされる)ものとする(SHALL). Verifierは非活動によるタイムアウトの直前に，ユーザに対して活動を促してもよい(MAY).

4.3.4 セキュリティ統制

CSPは，SP 800-53 または等価な連邦政府機関(例えば FEDRAMP) あるいは業界標準で定義されているセキュリティ統制の高度な基準から適切に調整されているセキュリティ統制を採用することとする(SHALL). CSPは影響が高度なシステム，またはそれに相当するものに対する最低限の保証関連の統制を果たしていることを保証することとする(SHALL).

4.3.5 レコード保持ポリシ

CSPは，準拠法，規則，及び任意のNational Archives and Records Administration (NARA)のレコード保持スケジュールを含むポリシに合致するそれぞれのレコード保持ポリシに従う．もしCSPがいずれの必須要件なくレコードを保持することを選択する場合，CSPはレコードの保持期間を決定するためのプライバシ及びセキュリティリスクのアセスメントを含むリスク管理プロセスを実施するものとし(SHALL)，Subscriberに対して当該保持ポリシについて通知するものとする(SHALL).

4.4 プライバシ要件

CSPはSP 800-53で定義された適切に調整されたプライバシコントロール，または他の等価な業界標準を採用するものとする(SHALL).

CSPは，追加の用途のために明確な通知を行い加入者から承諾を得なければ，Authentication実施，詐欺緩和，または法令遵守や法的手続き以外のいかなる目的でもSubscriberの情報を利用・開示しないものとする(SHALL NOT)．CSPは，同意をサービスの条件としてはならない(SHALL NOT)．情報を収集した際の元々の目的に利用が限定されていることを保証するための対策が講じられるものとする(SHALL)．このような情報の利用が，Authenticationや法令遵守，法的手続きに関連する用途に該当しないのであれば，CSPは通知を行い，Subscriberから同意を得るものとする(SHALL)．この通知は，SP 800-63A (sp800-63a.html) Section 8.2の*Notice and Consent*に記載されているのと同じ原則に従うべき(SHOULD)であり，法律に固執し過ぎたプライバシポリシや一般的な利用規約に丸め込むべきではない(SHOULD NOT)．明示的な目的外の用途がある場合は，むしろSubscriberが追加の利用目的を理解するための意味のある方法，及び承諾または辞退する機会が提供されるべきである(SHOULD).

CSPが政府機関または民間のプロバイダであるかどうかにかかわらず，次の要件がAuthenticationサービスを提供・利用する政府機関に対して適用される:

- 政府機関は，Authenticatorの発行・維持を目的としたPIIの収集が*Privacy Act of 1974* [Privacy Act] (Section 9.4参照)の要件をもたらすかどうか明確にするため，各機関のSenior Agency Official for Privacy (SAOP)と協議するものとする(SHALL).
- 政府機関は，必要に応じてそのような収集活動を対象とするSystem of Records Notice (SORN)を公開するものとする(SHALL).
- 政府機関は，Authenticatorの発行・維持を目的としたPIIの収集が*E-Government Act of 2002* [E-Gov]の要件をもたらすかどうか明確にするため，各機関のSAOPと協議するものとする(SHALL).
- 政府機関は，必要に応じてそのような収集活動を対象とするPrivacy Impact Assement(PIA)を公開するものとする(SHALL).

4.5 要件サマリ

本セクションは参考情報である

Table 4-1 にて各AAL毎の要件のサマリを述べる:

Table 4-1 各AAL毎の要件サマリ

要件	AAL1	AAL2	AAL3
許可されている Authenticator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; 単一要素OTPデバイス; 多要素OTPデバイス; 単一要素暗号ソフトウェア; 単一要素暗号デバイス; 多要素暗号ソフトウェア; 多要素暗号デバイス	多要素OTPデバイス; 多要素暗号ソフトウェア; 単一要素暗号デバイス; または 記憶シークレット及び: ・ルックアップシークレット ・アウトオブバンド ・単一要素OTPデバイス ・単一要素暗号ソフトウェア ・単一要素暗号デバイス	多要素暗号デバイス; 単一要素暗号デバイス及び 記憶シークレット; 単一要素OTPデバイス及び多要素暗号デバイスまたはソフトウェア; 単一要素OTPデバイス及び単一要素暗号ソフトウェア及び記憶シークレット
FIPS 140 確認	Level 1 (政府機関のVerifier)	Level 1 (政府機関のAuthenticator及びVerifier)	Level 2 総合 (多要素Authenticator) Level 1 総合 (Verifier及び単一要素暗号デバイス) Level 3 物理セキュリティ (全てのAuthenticator)
Reauthentication	30 日	12 時間 または 30 分 の非活動; 1つのAuthentication要素でもよい(MAY)	12 時間 または 15 分 の非活動; 両方のAuthentication要素をつかうものとする (SHALL)
セキュリティ統制	SP 800-53 低度のベースライン(または等価)	SP 800-53 中度のベースライン(または等価)	SP 800-53 高度のベースライン(または等価)
中間者攻撃耐性	必須	必須	必須
Verifierなりすまし耐性	不要	不要	必須
Verifier危殆化耐性	不要	不要	必須
リプレイ耐性	不要	必須	必須
Authentication意図	不要	推奨	必須

要件	AAL1	AAL2	AAL3
レコード保持ポリシ	必須	必須	必須
プライバシ統制	必須	必須	必須

5 Authenticator及びVerifier要件

本セクションは標準である.

本セクションでは，各Authenticatorタイプごとの要件詳細について記載する．Section 4で指定されたReauthentication要件及び[Section 5.2.5]に記載があるAAL3におけるVerifierなりすまし耐性の例外を除いて，各Authenticatorタイプ毎の技術要件はAuthenticatorが利用されるAALに関わらず同様である.

5.1 Authenticatorタイプ毎の要件

5.1.1 記憶シークレット

記憶シークレットAuthenticator — 一般的にはパスワードや，数字ならば*PIN*として表現されているもの — は，ユーザによって選択され，記憶されるシークレットである．記憶シークレットは攻撃者が正しい値を推測したり秘密の値を特定できないように，十分に複雑かつ秘密にしておく必要がある． 記憶シークレットは *something you know* である.

5.1.1.1 記憶シークレット**Authenticator**

記憶シークレットは，Subscriberにより選択されば場合少なくとも8文字とするものとする(SHALL)．記憶シークレットがCSPまたはVerifierによってランダムに選択されたものである場合は，少なくとも6文字であるものとし(SHALL)，全て数字でもよい(MAY)． CSPやVerifierが，危殆化した値のブラックリストに出現状況に基づいて指定された記憶シークレットを拒否した場合，Subscriberは別の記憶シークレット値を選ぶよう要求されるものとする(SHALL)．記憶シークレットの複雑さに関する他の要件を課すべきではない(SHOULD)．本件についての論拠はAppendix Aの *Strength of Memorized Secrets* に記載されている.

5.1.1.2 記憶シークレット**Verifier**

Verifierは，Subscriberが選択した記憶シークレットに対して最低8文字であることを要求するものとする(SHALL)．Verifierは，Subscriberが選択した記憶シークレットに対して最低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として許容されるべきである(SHOULD)．Unicode[ISO/ISC 10646]文字も同様に許容されるべきである(SHOULD)．Verifierは，8文字以上であることの検証を行う前に，タイピングミスの類を考慮して連続した複数のスペースまたは全てのスペースを除去してもよい(MAY)．シークレットの切り詰めについては実施しないものとする(SHALL NOT)．前述の記憶シークレットの長さ要件を満たすために，そ

れぞれのUnicodeの符号位置は一文字としてカウントされるものとする(SHALL).

もしUnicode文字が記憶シークレットとして許容されるならば，Verifierは，Unicode Standard Annex 15 [UAX 15] の Section 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のバイト文字表現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Subscriberは，いくつかのエンドポイントでは異なる表現になるかもしれない文字があり，それが彼らが正しくAuthenticationを行う能力に影響する可能性があるということをことを通知されるべきである(SHOULD).

記憶シークレットは，CSP(例えばEnrollment時など)やVerifier(ユーザが新しいPINを要求した時など)によりランダムに選択されるもので，最低6文字であるものとし(SHALL)，Approve済み乱数生成器 [SP 800-90Ar1] を利用して生成されるものとする(SHALL).

記憶シークレットVerifierは，Subscriberに対して，UnauthenticatedでないClaimantでも到達可能な「ヒント」を記録することを許可しないものとする(SHALL NOT). 記憶シークレットを選択する際，VerifierはSubscriberに対して特定のタイプの情報（例えば，「あなたが飼った最初のペットの名前はなんですか？」といったもの）の入力を求めないものとする(SHALL NOT).

記憶シークレットの設定，変更の要求を処理する際，Verifierは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に対し，比較するものとする(SHALL). 例えば，以下のリストが含んでいるものでよい(MAY)が，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
- 繰り返しまたはシーケンシャルな文字 (例： ‘aaaaaa’，’1234abcd’)
- サービス名や，ユーザ名，そこから派生するようなものなど，文脈で特定可能な単語

もし選択したシークレットがリスト中に存在したら，CSPまたはVerifierはSubscriberに対して異なるシークレット値を選ぶ必要があるということを知らせるものとし(SHALL)，その理由を提供するものとし(SHALL)，そしてSubscriberに異なる値を選択するよう求められるものとする(SHALL).

VerifierはSubscriberに対して，ユーザ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 [Meters] のようなガイダンスを行うべきである(SHOULD). 上記におリストに載っている記憶シークレットを拒否したのち，[Blacklists]化されている(そしておそらく非常に弱い)記憶シークレットからのささいな変更を思いとどまらせることは特に重要である.

Verifierは，Section 5.2.2に記載されているように，SubscriberのアカウントにおけるAuthentication失敗回数を効果的に制限するレート制限の仕組みを実装するものとする(SHALL).

Verifierは他の構成ルール(例えば，異なる文字種の組み合わせ，一定の文字の繰り返し)を記憶シークレットに課すべきではない(SHOULD NOT). Verifier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). しかしながらAuthenticatorが危殆化した証拠がある場合は，変更を強制するものとする(SHALL).

VerifierはClaimantによる記憶シークレットを入力時に”ペースト”機能を利用することを許可すべきである(SHOULD). これはパスワードマネージャの利用を促進し，広く利用されるようになることで多くの場合ユーザがより強力な記憶シークレットを選択する可能性を増加させる.

Claimantが記憶シークレットを正しく入力することを支援するために，Verifierは，ドットやアスタリスク表示ではなく，入力され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(SHOULD)である．こうすることで，Claimantは彼らのスクリーンが盗み見られる可能性が低い場所にいる場合に，入力内容を検証することができる．Verifierは更に，ユーザのデバイスに対して，入力が正しいことを確認する目的で個々の文字を入力後に短期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.

VerifierはApprove済み暗号化を利用するものとし(SHALL)，記憶シークレットを要求する際には，盗聴や中間者攻撃を防止するためにAuthenticateされた保護チャネルを用いるものとする(SHALL).

Verifierは，オフライン攻撃に対して耐性をもった形式で記憶シークレットを保存するものとする(SHALL). 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るものとする(SHALL)，鍵導出関数は，パスワード，ソルト，コストファクタを入力して，パスワードハッシュを生成する．例えば[SP800-132]で記載されているPBKDF2のようなApprove済みハッシュを用いてハッシュ化されるものとする(SHALL). ソルト値は32ビット以上のランダム値で，承認済み(approved)の乱数生成器を用いて生成され，ハッシュ結果とともに記録される．少なくとも繰り返し10000回のハッシュ関数を適用すべきである(SHOULD). ハッシュAuthenticatorから分離されて記録される鍵(例:ハードウェアセキュリティモジュール中)を用いる鍵付ハッシュ関数(例:HMAC)は，記録済みハッシュ化Authenticatorに対する辞書攻撃に対する更なる対抗方法として利用されるべきである(SHOULD). パスワードハッシュのファイルを入手した攻撃者によってパスワード推測の試行に費用がかかるようにする．そのためパスワード推測攻撃のコストは高い，もしくは非常に法外なものになる．適切な鍵導出関数の例としてPassword-based Key Derivation Function 2 (PBKDF2) [SP 800-132]及びBalloon [BALLOON]がある．攻撃コストを増加させることができるため，memory-hardな関数が利用されるべきである(SHOULD). 鍵導出関数はApprove済み一方向関数が用いられるべき(SHOULD)であり，例えば，Keyed Hash Message Authentication Code (HMAC) [FIPS 198-1]，SP 800-107のApprove済みハッシュ関数の何れか，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．鍵導出関数からの出力を選択する際，根拠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任意に選択されたものとする(SHALL). ソルト値及び結果のハッシュはいずれも記憶シークレットAuthenticatorを利用してSubscriber毎に保存されるものとする(SHALL).

PBKDF2において，コストファクタは繰り返し回数である: PBKDF2関数が繰り返し適用される回数が増加すれば，パスワードハッシュの計算時間が必要となる．すなわち，繰り返し回数は検証サーバのパフォーマンスが許す限り大きくするべきであり(SHOULD)，概ね10,000以上とすべきである.

加えて，Verifierは，自身だけが知っているシークレットをソルト値として用いた鍵導出関数の適用を

追加で実施すべきである(SHOULD). もし可能ならばソルト値はApprove済み乱数生成器 [SP 800-90Ar1]を利用して生成されるべき(SHOULD)であり，SP 800-131Aの最新版で指定されている最小のセキュリティ強度(本書の公開日時点では112ビット)を少なくとも備えるべき(SHOULD)である. このシークレットソルト値は，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の中に)保存されるものとする(SHALL). この追加の適用により，シークレットソルト値が秘密である限り，記憶シークレットのハッシュに対するブルートフォース攻撃は非現実的である.

5.1.2 ルックアップシークレット

ルックアップシークレットAuthenticatorは物理的または電子的なレコードであり，ClaimantとCSPとの間で共有されているシークレット一式を記録するものである. Claimantは，Verifierからの入力要求に答えるために必要とされる適切なシークレットを検索するためにAuthenticatorを利用する. 例えば，Verifierは Claimantに対して，カード上に印字された表形式の数字または文字列のうち特定の一部を提示するよう求められるかもしれない. ルックアップシークレットの一般的な適用としては，Subscriberによって保存され，別のAuthenticatorが紛失したり機能しなくなった際に用いる"リカバリキー"の利用がある. ルックアップシークレットは*something you have*である.

5.1.2.1 ルックアップシークレットAuthenticator

CSPがルックアップシークレットAuthenticatorを生成する際，Approve済み乱数生成器 [SP 800-90Ar1] を用いてシークレットのリストを生成するものとし(SHALL)，Subscriberに対して Authenticatorを安全に届けるものとする(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つものとする(SHALL).

ルックアップシークレットは，CSPの人間の手での配布，Subscriberの住所宛への配送，またはオンラインでの配布が行われてもよい(MAY)，もし配布がオンラインで行われるならば，ルックアップシークレットはpost-enrollment binding要件Section 6.1.2を満たすセキュアチャネル上で配布されるものとする(SHALL).

もしAuthenticatorがルックアップシークレットを連続してリストから利用する場合，Subscriberは一度Authenticationに成功した場合に限ってシークレットを破棄してもよい(MAY).

5.1.2.2 Look-Up Secret Verifiers

ルックアップシークレットのVerifierはClaimantに対して，彼らのAuthenticatorから得られる次のシークレット，または特定の(例:付番された)シークレットの入力を促すものとする (SHALL). Authenticatorから得られたシークレットは1度しか正常に利用できないものとする (SHALL). もしルックアップシークレットが格子状のカードから得られる場合，格子の各セルは1度だけ利用するものとする(SHALL).

Verifierは，オフライン攻撃へ対策する形式でルックアップシークレットを保存するものとする

(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，Section 5.1.1.2に記載されているようにApprove済み一方向関数でハッシュ化されるものとする(SHALL). 112ビット未満のエントロピーを持ったルックアップシークレットはSection 5.1.1.2に記載されているように，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されるものとする．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任意に選択されるものとする(SHALL). ソルト値及び結果のハッシュはいずれもルックアップシークレット毎に保存されるものとする(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に対して，Verifierは，Section 5.2.2に記載されているように，Subscriberのアカウントにおける Authentication失敗回数を効果的に制限するレート制限の仕組みを実装するものとする(SHALL).

VerifierはApprove済み暗号化を利用するものとし(SHALL)，ルックアップシークレットを要求する際には，盗聴や中間者攻撃を防止する目的で，Authenticateされた保護チャネルを利用するものとする(SHALL).

5.1.3 アウトオブバンドデバイス

アウトオブバンドAuthenticatorは，一意にアドレス可能，かつセカンダリチャネルと呼ばれる異なる通信チャネルを介してVerifierと安全に通信することができる物理デバイスである．デバイスはClaimantによって所有及び制御されており，E-Authentication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Authenticatorは*something you have*である．

アウトオブバンドAuthenticatorは以下の方法の1つで動作する:

- Claimant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Verifierに送信する．例えば，Claimantは自身のモバイルデバイス上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)を自身のAuthenticationセッションに対して入力してもよい．

- Claimant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対して送信し，セカンダリチャネルを介してVerifierに対して送信する．例えば，Claimantは自身のAuthenticationセッション上で確認したシークレットを，モバイルデバイス上のアプリケーション対して入力したり，バーコード・QRコードといった技術を利用して送信を行ってもよい．

- Claimant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たAuthenticationを確認する．

シークレットの目的は安全にAuthentication操作をプライマリとセカンダリのチャネルに結びつけることである．プライマリ通信チャネルを介してレスポンスをする場合，シークレットはアウトオブバンドデバイスをClaimantが制御していることもまた証明していることになる．

5.1.3.1 アウトオブバンドAuthenticator

アウトオブバンドAuthenticatorはアウトオブバンドシークレットやAuthenticationリクエストを取得するためにVerifierとの分離された通信チャネルを確立するものとする(SHALL). このチャネルはプライマリ通信チャネルとの関係においてアウトオブバンドであるとし，(同じデバイス上で終端されている場合でさえも)，Claimantの認可なしに一方から他方に対して情報が漏洩することがないようなデイバイスであることを前提とする.

アウトオブバンドデバイスは一意にアドレス可能であるべきであり(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)を介して送信されない場合は暗号化されているものとする(SHALL). PSTNに固有な追加のAuthenticator要件に対しては，Section 5.1.3.3を参照すること．Voice-over-IP(VoIP)やEmailなど，特定デバイスの所有を証明を行わない方式は，アウトオブバンドAuthenticationを行う目的では利用しないものとする(SHALL).

アウトオブバンドAuthenticatorは，Verifierとの通信において以下に記載する方法の1つを用いて，一意に自身の真正性を証明するものとする(SHALL):

- Approve済み暗号理論を利用してVerifierに対するAuthenticateされた保護チャネルを確立すること．鍵はAuthenticatorアプリケーションが利用可能なデバイス上で適切にセキュアであるストレージ(例:キーチェーンストレージ，TPM，TEE，セキュアエレメント)に記録されるものとする(SHALL).
- SIMカードまたはデバイスを一意に識別する等価な方法を用いて公衆携帯電話網に対してAuthenticateする．この方法はPSTN(SMSまたは音声)を介してアウトオブバンドデバイスに対してVerifierからシークレットが送信される場合に限り用いるものとする(SHALL).

もしVerifierからアウトオブバンドデバイスに対してシークレットが送信されるならば，デバイスは所有者によってデバイスがロックされている(例:表示するために，PINやパスコード入力，またはバイオメトリックの入力が必要とされる)間はAuthenticationシークレットを表示すべきではない(SHOULD NOT). しかしながらAuthenticatorはロックされたデバイス上でAuthenticationシークレットを受信したことを表示すべきである(SHOULD).

もしアウトオブバンドAuthenticator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ならば(Claimantがプライマリ通信チャネルに対して受け取ったシークレットを送信するよりもむしろ)，次のうち1つを実施するものとする(SHALL):

- Authenticator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容するものとし(SHALL)，Authenticationトランザクションに対する承認と関連付けるために，セカンダリチャネルを介してVerifierに対して送信するものとする(SHALL). Claimantは送信を手動で実施，またはバーコード・QRコードといった技術を利用して送信を行ってもよい(MAY).
- Authenticatorはセカンダリチャネルを介してVerifierから受け取ったシークレットを提示し，Claimantに対してプライマリチャネルのシークレットとの一貫性を検証するよう促した上で，Claimantから「はい/いいえ」の応答を受け入れるものとする(SHALL).

5.1.3.2 アウトオブバンドVerifier

PSTNに特有の追加の検証要件は，Section 5.1.3.3を参照すること.

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:スマートフォン上)を利用して行われる場合，Verifierはデバイスに対してPush通知を行ってもよい(MAY). VerifierはAuthenticateされた保護チャネルの確立を待ち，Authenticatorの識別キーを検証する. Authenticatorは識別キー自身を記録しないものとする(SHALL NOT)が，Authenticatorを一意に識別するためにハッシュのような検証方法(例えばApprove済みのハッシュ関数や，識別キーの所持証明)を用いるものとする(SHALL). Authenticateされると，VerifierはAuthenticationシークレットをAuthenticatorに対して送信する.

アウトオブバンドAuthenticatorの種別に応じて，以下のうち1つを行うものとする(SHALL):

- シークレットをプライマリチャネルに送出: VerifierはSubscriberのAuthenticatorを持つデバイスに対してAuthenticationの準備を示すシグナルを送信してもよい(MAY). そのうえで，アウトオブバンドAuthenticatorに対してランダムなシークレットを送信するものとする(SHALL). Verifierはプライマリ通信チャネル上でシークレットが返却されるのを待つものとする(SHALL).
- シークレットをセカンダリチャネルに送出: VerifierはランダムなAuthenticationシークレットをプライマリチャネル経由でClaimantに対して表示するものとする(SHALL). そのうえで，セカンダリチャネル上でClaimantのアウトオブバンドAuthenticatorからシークレットが返却されるのを待つものとする(SHALL).
- ClaimantによるシークレットのVerifier: VerifierはランダムなAuthenticationシークレットをプライマリチャネル経由でClaimantに対して表示するものとし(SHALL)，セカンダリチャネルを介してアウトオブバンドAuthenticatorに対して同じシークレットを送信しClaimantに提示するものとする(SHALL). そのうえで，セカンダリチャネルを介した承認(非承認)メッセージを待つものとする(SHALL).

全てのケースにおいて，10分以内に完了しないAuthenticationは不正とみなすものとする(SHALL). Section 5.2.8に記載されているリプレイ耐性を備えるために，Verifierは特定のAuthenticationシークレットを確認期間の間で一度だけ受け付けるものとする(SHALL).

Verifierは，Approve済み乱数生成器 [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Authenticationシークレットを生成するものとする(SHALL). もし認証シークレットが64ビット未満のエントロピーを持つ場合は，ルックアップシークレットに対して，Verifierは，Section 5.2.2に記載されているように，Subscriberのアカウントにおける Authentication失敗回数を効果的に制限するレート制限の仕組みを実装するものとする(SHALL).

5.1.3.3 公衆交換電話網を利用するAuthenticator

アウトオブバンドでの検証を目的としたPSTNの利用は，本セクション及び Section 5.2.10 に記載されているように制限されている(RESTRICTED). もしアウトオブバンドでの検証がPSTNを用いて実施される場合は，Verifierは利用されてい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つけ

られていることを検証するものとする(SHALL). 事前登録済みの電話番号の変更は，新しいAuthenticatorのバインディングとみなされ，Section 6.1.2 に記載されている場合のみ発生するものとする(SHALL).

Verifierは，デバイス入れ替え，SIM変更，番号ポーティング，あるいはその他にアウトオブバンドAuthenticationシークレットの配送にPSTNを利用する以前の異常な振る舞いのようなリスク指標を考慮すべきである(SHOULD).

> 注記: Section 5.2.10におけるAuthenticatorの制限に従い，NISTは脅威状況及びPSTNの技術的な運用の発展に基づき，PSTNの制限(RESTRICTED)状態を時間の経過とともに調整するかもしれない.

5.1.4 単一要素OTPVerifier

単一要素OTPデバイスはOTPの生成をサポートするデバイスである. 単一要素OTPデバイスは，携帯電話のようなデバイスにインストールされたソフトウェアのOTP生成器及びハードウェアデバイスが含まれる. これらのデバイスは，OTPの生成のシードとして利用される組み込みのシークレットを保持しており，二要素目によるアクティベーションを必要としない. OTPはデバイス上で表示，手動でVerifierに対して入力され，そのことによりデバイスの所持と制御を証明する. OTPデバイスは例えば一度に6文字の表示を行うことがある. 単一要素OTPデバイスは*something you have*である.

単一要素OTPデバイスはルックアップシークレットAuthenticatorと同様，暗号理論に基づいてAuthenticatorとVerifierがシークレットを生成し，Verifierによって比較されるという例外を除いて同様である. シークレットは，時間ベースのノンスまたはAuthenticatorとVerifierのカウンタに基づいて計算される.

5.1.4.1 Single-Factor OTP Authenticators

単一要素OTPAuthenticatorは2つの永続的な値を保持する.1つ目はデバイスの存続期間にわたり保持し続ける対象鍵である.2つ目は認証機が使われる都度変化する，またはリアルタイムクロックに基づいているノンスである.

秘密鍵とそのアルゴリズムは少なくともSP 800-131Aの最新版で定義された最低のセキュリティ強度(本書の刊行現在では112ビット)であるものとする(SHALL). ノンスは，デバイスの存続期間にわたりデバイスが操作される都度一意な値であることを確実にするために十分長いこととする(SHALL). OTP Authenticatorは - 特にソフトウェアベースのOTP生成器の場合 - 複数デバイスに対して秘密鍵を複製する行為を思いとどまらせるべきであり(SHOULD)，助長しないものとする(SHALL NOT).

Authenticator出力は，鍵とノンスとを安全な方法で組み合わせ，Approveされたブロック暗号またはハッシュ関数を用いることで得られる. Authenticator出力は少なくとも(約20ビットのエントロピーの)6桁の数字になるよう切り詰めてもよい(MAY).

もしAuthenticator出力を生成するために利用されるノンスがリアルタイムクロックをベースとしている場合，ノンスは少なくとも2分毎に変化するものとする(SHALL).与えられたノンスと関連するOTP値は一度だけ受け入れられるものとする(SHALL).

5.1.4.2 単一要素OTP Verifier

単一要素OTP Verifierは，AuthenticatorによるOTPの生成プロセスを実質的に再現する．Verifierは，Authenticatorが使う対称鍵を所持しており，セキュリティ侵害に対する強力な防御が行われているものとする(SHALL).

単一要素OTP AuthenticatorがSubscriberアカウントに紐付けられている時，Verifierまたは関連するCSPは，Authenticatorの出力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Approveされた暗号理論を利用するものとする(SHALL).

Verifier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，Approveされた暗号化を利用し，Authenticateされた保護チャネルを利用するものとする(SHALL)．時間ベースのOTP[RFC 6238]は，有効期間を定義するものとし(SHALL)，Authenticatorの存続期間にわたり予想される（何れの方向に対する）時刻ずれにネットワーク遅延とユーザによるOTP入力の許容時間を加えて決定される．Section 5.2.8に記載されているリプレイ耐性を備えるために，Verifierは指定された時間ベースのOTPを有効期間で一度だけ受け付けるものとする(SHALL).

もしAuthenticator出力が64ビット未満のエントロピーを持つ場合は，Verifierは，Section 5.2.2に記載されているように，Subscriberのアカウントにおける Authentication失敗回数を効果的に制限するレート制限の仕組みを実装するものとする(SHALL).

5.1.5 Multi-Factor OTP Devices

多要素OTPデバイスは，追加の認証要素によりアクティベートされた後にAuthenticationで使われるワンタイムパスワードを生成する．多要素OTPデバイスは，ハードウェアデバイス及び携帯電話のようなデバイスにインストールされたソフトウェアのOTP生成器が含まれる．Authenticationの2要素目は組み込みの入力パッド，組み込みのバイオメトリック(例：指紋)リーダ，USBポートなどのコンピュータに対するダイレクトなインタフェースを介して実現される．ワンタイムパスワードはデバイス上で表示，手動でVerifierに対して入力され，そのことによりデバイスの所持と制御を証明する．ワンタイムパスワードデバイスは例えば一度に6文字の表示を行うことがある．多要素OTPデバイスは*something you have*である．また，*something you know*または*something you are*のどちらかによってアクティベートされるものとする(SHALL).

5.1.5.1 多要素OTP Authenticator

多要素OTP Authenticatorは，Authenticatorからパスワードを得るために記憶シークレットの入力またはバイオメトリクスの利用を要求する点を除いて，単一要素OTP Authenticator(Section 5.1.4.1参照)と同じ方法で動作する．いずれの場合でも追加要素の入力が必要であるものとする(SHALL).

アクティベーション情報に加えて，多要素OTP Authenticatorは2つの永続的な値を含んでいる．1つ目はデバイスの存続期間にわたり永続する対称鍵である．2つ目は，Authenticator利用の都度変化する，またはリアルタイムクロックに基づいているノンスである．

秘密鍵とそのアルゴリズムは少なくとも[SP 800-131A]の最新版で定義された最低のセキュリティ強度(本書の刊行現在では112ビット)であるものとする(SHALL)．ノンスは，デバイスの生存期間に渡りデバイスが操作される都度一意な値であることを確実にするために十分長いこととする(SHALL)．OTP Authenticatorは - 特にソフトウェアベースのOTP生成器の場合 - 複数デバイスに対して秘密鍵を複製する行為を思いとどまらせるべきであり(SHOULD)，助長しないものとする(SHALL NOT)．

Authenticator出力は，鍵とノンスとを安全な方法で組み合わせ，Approveされたブロック暗号またはハッシュ関数を用いることで得られる．Authenticator出力は少なくとも(約20ビットのエントロピーの)6桁の数字になるよう切り詰めてもよい(MAY)．

もしAuthenticator出力を生成するために利用されるノンスがリアルタイムクロックをベースとしている場合，ノンスは少なくとも2分毎に変化するものとする(SHALL)．与えられたノンスと関連するOTP値は一度だけ受け入れられるものとする(SHALL)．

Authenticatorのアクティベーションのために利用される記憶シークレットは，ランダムに選ばれた最低6文字の数字またはSection 5.1.1.2に記載されているものと同等な複雑さを備えた他の記憶シークレットであるものとし(SHALL)，Section 5.2.2に記載されているようにレート制限が行われるものとする(SHALL)．バイオメトリックのアクティベーション要素は，Section 5.2.3の要件を満たすものとし(SHALL)，連続するAuthentication失敗回数に制限がある．

暗号化されていない秘密鍵とアクティベーションシークレット，またはバイオメトリック標本（及び信号処理により生成されたプローブのようなバイオメトリック標本に由来する任意のバイオメトリックデータ）は，パスワード生成が終わると直ちにゼロ埋めされるものとする(SHALL)．

5.1.5.2 多要素OTP Verifier

多要素OTP Verifierは，AuthenticatorによるOTPの生成プロセスを実質的に再現するが，2要素目の要求は行わない．例えば，Authenticatorが用いる対象鍵は，セキュリティ侵害に対して強力な防御が行われているものとする(SHALL)．

多要素OTP AuthenticatorがSubscriberアカウントに紐付けられている時，Verifierまたは関連するCSPは，Authenticatorの出力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Approveされた暗号理論を利用するものとする(SHALL)．VerifierまたはCSPは，Authenticatorの出所によって，Authenticatorが多要素デバイスであることを証明するものとする(SHALL)．それが多要素Authenticatorであるという信頼できる報告がない場合、VerifierはSection 5.1.4に従いAuthenticatorを単一要素として扱うものとする(SHALL)．

Verifier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，Approveされた暗号化を利用し，Authenticateされた保護チャネルを利用するものとする(SHALL)．時間ベースのOTP[RFC 6238]は，有効期間を定義するものとし(SHALL)，Authenticator自体の寿命までに予想される（何れの方向に対する）時刻ずれにネットワーク遅延とユーザによるOTP入力の許容時間を加えて決定され

る．Section 5.2.8に記載されているリプレイ耐性を備えるために，Verifierは指定された時間ベースのOTPを有効期間で一度だけ受け付けるものとする(SHALL)．あるOTPの使い回しによりClaimantのAuthenticationが拒否されるような場合には，VerifierはClaimantに対して，攻撃者が先回りしてAuthenticationを行うことができる可能性があることを警告してもよい(MAY)．Verifierは，あるOTPの使い回しが試みられた既存セッションのSubscriberに対して同様に警告してもよい(MAY)．

もしAuthenticator出力またはアクティベーションシークレットが64ビット未満のエントロピーを持つ場合は，Verifierは，Section 5.2.2に記載されているように，Subscriberのアカウントにおける Authentication失敗回数を効果的に制限するレート制限の仕組みを実装するものとする(SHALL)．バイオメトリックのアクティベーション要素は，Section 5.2.3の要件を満たすものとし(SHALL)，連続するAuthentication失敗回数に制限がある．

5.1.6 単一要素暗号ソフトウェア

単一要素ソフトウェア暗号Authenticatorは、ディスクあるいは"ソフト"媒体に記録された暗号鍵である．Authenticationは鍵の所有と制御を証明することで行われる．Authenticator出力は特定の暗号プロトコルに強く依存し、一般的にはある種の署名付メッセージになっている．単一要素ソフトウェア暗号Authenticatorは *something you have* である．

5.1.6.1 単一要素暗号ソフトウェアAuthenticator

5.1.6.1 Single-Factor Cryptographic Software Authenticators

単一要素暗号ソフトウェアAuthenticatorは、Authenticatorで一意な秘密鍵を保持している．鍵はAuthenticatorアプリケーションが利用可能なデバイス上で適切にセキュアであるストレージ(例:キーチェーンストレージ，TPMまたは可能であればTEE)に記録されるものとする(SHALL)．デバイス上のソフトウェアコンポーネントがアクセス要求を行ったときのみ鍵にアクセスできるよう制限するアクセス制御を用いて、鍵は許可のない暴露から強力に保護されているものとする(SHALL)．単一要素暗号ソフトウェアAuthenticatorは，複数デバイスに対して秘密鍵を複製する行為を思いとどまらせるべきであり(SHOULD)，助長しないものとする(SHALL NOT)．

5.1.6.2 単一要素暗号ソフトウェアVerifier

単一要素暗号ソフトウェアVerifierに対する要件は，Section 5.1.7.2 に記載されている単一要素暗号デバイスVerifierに対する要件と同一である．

5.1.7 単一要素暗号デバイス

単一要素暗号デバイスは，保護された暗号鍵を用いた暗号操作，及びユーザエンドポイントに対する直接コネクションを介してAuthenticator出力を提供するハードウェアデバイスである．デバイスは組み込みの対象暗号鍵，非対称暗号鍵を利用し，Authenticationの2要素目を用いたアクティベーションを要求しない．AuthenticationはAuthenticationプロトコルを介してデバイスの所持証明を行うことにより達成される．Authenticator出力はユーザエンドポイントに対する直接接続により提供され，特定の暗号デバイスとプロトコルに強く依存し，典型的にはある種の署名付メッセージになっている．単一要素暗号デバイスは*something you have*である．

5.1.7.1 単一要素暗号デバイスAuthenticator

単一要素暗号デバイスAuthenticatorは秘密鍵を格納しており，その鍵はデバイスで一意かつエクスポートされない(つまりデバイスから除去することができない)ものとする(SHALL NOT)．Authenticatorは，通常はUSBポートなどのコンピュータに対するダイレクト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で動作する．暗号デバイスはソフトウェアを含んでいるが，全ての組み込みソフトウェアがCSP(または発行者)の制御下にあるという点，及びAuthenticator全体でAuthentication時のAALにおけるFIPS 140要件に適合する必要がある点において，暗号ソフトウェアAuthenticatorとは異なる．

秘密鍵とそのアルゴリズムは少なくともSP 800-131Aの最新版で定義された最低のセキュリティ強度(本書の刊行現在では112ビット)であるものとする(SHALL)．チャレンジノンスは少なくとも64ビット長であるものとする(SHALL)．Approveされた暗号理論が利用されるものとする(SHALL)．

単一要素暗号デバイスAuthenticatorは動作するために(ボタンを押すなどの)物理的な入力を必要とすべきである(SHOULD)．これにより，デバイスが接続している先がセキュリティ侵害をうけているような場合に起こりうる，デバイスの意図しない動作を防止することができる．

5.1.7.2 単一要素暗号デバイスVerifier

単一要素暗号デバイスVerifierはチャレンジノンスを生成して，対応するAuthenticatorに送信する．また，Authenticator出力をデバイスの所有を検証するために用いる．Authenticator出力は特定の暗号デバイスとプロトコルに強く依存し，典型的にはある種の署名付メッセージになっている．

Verifierは，各Authenticatorに対応する対象鍵または非対称暗号鍵を保持している．どちらのタイプの鍵も改変に対して保護されているものとし(SHALL)，対象鍵については追加で許可のない暴露に対して保護されているものとする(SHALL)．

チャレンジノンスは少なくとも64ビット長であるとし(SHALL)，Authenticatorの有効期間を通じて一意，または統計上一意(したがって，Approveされた乱数生成器[SP 800-90Ar1]を用いて生成されたもの)であるとする(SHALL)．

5.1.8 多要素暗号ソフトウェア

多要素ソフトウェア暗号Authenticatorは，ディスクあるいは"ソフト"媒体に記録された暗号鍵であり，Authenticationの2要素目を用いたアクティベーションを必要とする．Authenticationは鍵の所有と制御を証明することで行われる．Authenticator出力は特定の暗号プロトコルに強く依存し，一般的にはある種の署名付メッセージになっている．多要素ソフトウェア暗号Authenticatorは*something you have*であり，*something you know*または*something you are*のどちらかによってアクティベートされるものとする(SHALL).

5.1.8.1 多要素暗号ソフトウェアAuthenticators

多要素暗号ソフトウェアAuthenticatorは秘密鍵を格納しており，その鍵はデバイスで一意であり記憶シークレットやバイオメトリックなどの追加の要素の入力を経たときだけアクセスできる．鍵はAuthenticatorアプリケーションが利用可能なデバイス上で適切にセキュアであるストレージ(例:キーチェーンストレージ，TPM，TEE)に記録されるべきである(SHOULD)．デバイス上のソフトウェアコンポーネントがアクセス要求を行ったときのみ鍵にアクセスできるよう制限するアクセス制御を用いて、鍵は許可のない暴露から強力に保護されているものとする(SHALL)．多要素暗号ソフトウェアAuthenticatorは，複数デバイスに対して秘密鍵を複製する行為を思いとどまらせるべきであり(SHOULD)，助長しないものとする(SHALL NOT).

Authenticatorを用いた各Authentication操作には両方の要素の入力を必要とするものとする(SHALL).

Authenticatorのアクティベーションのために利用される記憶シークレットは，最低6文字の数字または同等な複雑さを備えたものとし(SHALL)，Section 5.2.2に記載されているようにレート制限が行われるものとする(SHALL)．バイオメトリックのアクティベーション要素は，Section 5.2.3の要件を満たすものとし(SHALL)，連続するAuthentication失敗回数に対する制限を含むものとする.

暗号化されていない秘密鍵とアクティベーションシークレット，またはバイオメトリック標本（及び信号処理により生成されたプローブのようなバイオメトリック標本に由来する任意のバイオメトリックデータ）は，Authenticationトランザクションが行われたら直ちにゼロ埋めされるものとする(SHALL).

5.1.8.2 多要素暗号ソフトウェアVerifier

多要素暗号ソフトウェアVerifierに対する要件は，Section 5.1.7.2 に記載されている単一要素暗号デバイスVerifierに対する要件と同一である．多要素暗号ソフトウェアAuthenticator出力を検証することで，アクティベーション要素の使用の証明となる.

5.1.9 多要素暗号デバイス

多要素暗号デバイスは，1つ以上の保護された暗号鍵を用いた暗号操作を行うハードウェアデバイスであり，2要素目を用いたアクティベーションを要求する．Authenticationはデバイスの所持と鍵の制御を証明することで実現される．Authenticator出力はユーザエンドポイントに対する直接接続を介して提供され，特定の暗号デバイスとプロトコルに強く依存し，典型的にはある種の署名付メッセージになっている．多要素暗号デバイスは*something you have*であり，*something you know*または*something you are*のどちらかによってアクティベートされるものとする(SHALL).

5.1.9.1 多要素暗号デバイスAuthenticator

多要素暗号デバイスAuthenticatorは耐タンパ性を有するハードウェアを用いて秘密鍵を格納しており，その鍵はデバイスで一意であり記憶シークレットやバイオメトリックなどの追加の要素の入力を経たときだけアクセスできる．鍵はAuthenticatorアプリケーションが利用可能なデバイス上で適切にセキュアであるストレージ(例:キーチェーンストレージ，TPM，TEE)に記録されるべきである(SHOULD)．デバイス上のソフトウェアコンポーネントがアクセス要求を行ったときのみ鍵にアクセスできるよう制限するアクセス制御を用いて、鍵は許可のない暴露から強力に保護されているものとする(SHALL)．多要素暗号ソフトウェアAuthenticatorは，複数デバイスに対して秘密鍵を複製する行為を思いとどまらせるべきであり(SHOULD)，助長しないものとする(SHALL NOT).

秘密鍵とそのアルゴリズムは少なくともSP 800-131Aの最新版で定義された最低のセキュリティ強度(本書の刊行現在では112ビット)であるものとする(SHALL)．チャレンジノンスは少なくとも64ビット長であるものとする(SHALL)．Approveされた暗号理論が利用されるものとする(SHALL).

Authenticatorを用いた各Authentication操作には追加の要素の入力を必要とすべきである(SOULD)．追加要素の入力は，デバイスへの直接入力かハードウェア接続(例：USB，スマートカード)を介して実施されてもよい(MAY).

Authenticatorのアクティベーションのために利用される記憶シークレットは，最低6文字の数字または同等な複雑さを備えたものとし(SHALL)，Section 5.2.2に記載されているようにレート制限が行われるものとする(SHALL)．バイオメトリックのアクティベーション要素は，Section 5.2.3の要件を満たすものとし(SHALL)，連続するAuthentication失敗回数に対する制限を含むものとする.

暗号化されていない秘密鍵とアクティベーションシークレット，またはバイオメトリック標本（及び信号処理により生成されたプローブのようなバイオメトリック標本に由来する任意のバイオメトリックデータ）は，Authenticationトランザクションが行われたら直ちにメモリが上書きされるものとする(SHALL).

5.1.9.2多要素暗号デバイスVerifier

多要素暗号デバイスVerifierに対する要件は，Section 5.1.7.2 に記載されている単一要素暗号デバイスVerifierに対する要件と同一である．多要素暗号デバイスAuthenticator出力を検証することで，アクティベーション要素の使用の証明となる.

5.2. 一般Authenticator要件

5.2.1 Physical Authenticators

CSPはSubscriberに対して，Authenticatorの盗難や紛失を正しく防止する方法について指示するものとする(SHALL)．CSPはSubscriberから認証機の盗難や紛失の疑いがある旨の通知に対し，直ちにAuthenticatorを無効化，停止するメカニズムを備えるものとする(SHALL).

5.2.2 レート制限 (スロットリング)

Section 5.1のAuthenticatorタイプの説明で要求される場合，Verifierはオンライン推測攻撃に対抗するための制御を実装するものとする(SHALL)．指定されたAuthenticatorの説明に記載がなければ，Verifierはオンライン攻撃者に対し，同一アカウントで100回以上の連続した認証失敗試行を制限をするものとする(SHALL).

レート制限の結果として攻撃者が正しいclaimantをロックアウトさせる頻度を減少させるために用いられる追加のテクニックを用いてもよい(MAY)．追加テクニックは以下を含む:

- Claimantに対して，Authentication試行前にCAPTCHAの入力を要求する.
- Claimantに対して認証失敗後に一定期間待つように要求し，連続する認証失敗の最大回数に近づくにつれてその時間を(例えば30秒から1時間まで)増加させる.
- Subscriberが以前Authenticationに成功したことがあるIPアドレスのホワイトリストからのみ行われるAuthentication要求だけを受理する.
- ユーザの振る舞い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Authenticationの手法を活用する.

SubscriberがAuthenticationに成功した場合，Verifierは同一IPアドレスからの以前の失敗したAuthenticationの試行を無視すべきである(SHOULD).

5.2.3 バイオメトリクスの利用

Authenticationにおけるバイオメトリクス(*something you are*)の利用は，物理的な特性(例：指紋，虹彩，顔の特徴)及び振る舞い特性(例：タイピングのリズム)の両方を測定法を含んでいる．Section 5.2.9に記載されているAuthentication意図を確認する範囲とは差があるかもしれないが，両方の分類ともに，異なるバイオメトリック計測手段とみなされる.

様々な理由で，本書はAuthenticationにおけるバイオメトリクスの利用を限定的にサポートする．それらは以下のとおりである:

- バイオメトリックのFalse Match Rate(FMR)は，それ自身ではSubscriberのAuthenticationにおける確実性を与えるものではない．更に，FMRはスプーフィング攻撃を考慮したものではない.
- バイオメトリックの比較は確率的なものであるが，他のAuthentication要素は決定的なものであ

る.

- バイオメトリックのテンプレート保護スキームは，他のAuthentication要素(例: PKI証明書やパスワード)に相当するバイオメトリッククレデンシャルを無効化するための手段を提供する．しかしながら，そのようなソリューションの可用性は制限されており，これらの手段を試験するための標準も策定中の段階である.
- バイオメトリック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，知識のあるなしに関わらず誰かが携帯電話のカメラで(例えば顔の)写真を取ることができ，誰かが触った物から(例えば潜在的に指紋を)採取することができ，高精細な画像から(例えば虹彩パターンを)キャプチャすることができる．生体検知のようなPresentation attack detaction(PAD)技術は，これらの種別の攻撃リスクを緩和することができるが，センサーやバイオメトリック処理はCSPとSubscriberのニーズに合うようにPADを適切に実施していることを保証する必要がある.

したがって，Authenticationにおける制限されたバイオメトリクスの利用は，以下の要件とガイドラインの下でサポートされる:

バイオメトリクスは物理的なAuthenticatorを用いた多要素Authentication(*something you have*)の一部としてのみ利用されるものとする(SHALL).

センサ(またはセンサ置き換え耐性のあるセンサーを持ったエンドポイント)とVerifier間のAuthenticateされた保護チャネルが確立され(SHALL)，センサーまたはエンドポイントが設置され(SHALL)，Claimantからバイオメトリック標本を取得するのに先立ってセンサーまたはエンドポイントがAuthenticateされているものとする(SHALL).

バイオメトリックシステムは，FMR [ISO/IEC 2382-37]は1000分の1より優れたレートで運用されるものとする．このFMRは[ISO/IEC 30107-1]で定義されているConformant attack(すなわちZero-effort imporster attempt)の条件下で達成されるものとする(SHALL).

バイオメトリックシステムは，PADを実装すべきである(SHOULD)．バイオメトリックシステムを配備を目的として実施するテストでは，各関連攻撃タイプ(すなわち種類)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失敗回数をプレゼンテーション攻撃の試行回数で割ったものとして定義される．プレゼンテーション攻撃耐性のテストは，[ISO/IEC 30107-3]の12条に従い行われるものとする(SHALL)．PADはClaimantのデバイス上でローカルに実施されても，または中央のVerifierによって実施されてもよい(MAY).

> 注釈: PADはガイドラインの将来の版では必須要件としてみなされる.

バイオメトリックシステム5回の連続したAuthentication試行の失敗を許容するものとする(SHALL).
もしPADが上記の要件を満たして実装されている場合は，10回の連続したAuthentication試行の失敗を許容するものとする(SHALL)．一度上限に達すると，バイオメトリックAuthenticatorは以下の何れかであるものとする(SHALL):

- 次回の試行までに少なくとも30秒の遅延を課し，試行回数が増える毎に指数関数的に遅延を増

加させる(例えば，後続の失敗する試行の前に1分，その次の試行では2分)か，

- もし既に利用可能な代替手段があるのであれば，バイオメトリックユーザAuthenticationを無効化し，もう一つの要素(例えば，異なるバイオメトリック計測手段や，まだ要求されていない要素であればPIN/パスコード)の利用を試みる.

Verifierはセンサー及びポイントのパフォーマンス，一貫性，真正性について決定するものとする(SHALL). この決定を行うために容認できる方法として以下があるが，限定はされていない:

- センサー及びエンドポイントのAuthentication.
- 承認済みの適格性認定機関による認定.
- Section 5.2.4に記載されている署名済みメタデータの実効時照会(例: アテステーション)

バイオメトリックの比較はClaimantのデバイス上でローカルに実施されるか，中央のVerifierで実施される. 中央のVerifierでの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.

もし比較が中央で実施される場合:

- Authenticationとしてのバイオメトリック利用はApproveされた暗号理論を用いて特定される一つ以上の特定デバイスに限定されるものとする(SHALL). バイオメトリックがまだメインのAuthentication鍵をアンロックしていないのであれば，分離している鍵がデバイスの特定のために利用されるものとする(SHALL).
- バイオメトリックの破棄は，ISO/IEC 24745中のバイオメトリックテンプレート保護と呼ばれており，実装するものとする(SHALL).
- 全てのバイオメトリクスの送信はAuthenticateされた保護チャネルを介して行われる.

Authenticationプロセス中で収集されたバイオメトリック標本は，ユーザの同意の下で，研究目的で比較アルゴリズムの学習に利用してもよい(MAY). バイオメトリック標本及び信号処理により生成されたプローブのようなバイオメトリック標本に由来する任意のバイオメトリックデータは，学習や派生した研究データが得られた後は直ちにゼロ埋めされるものとする(SHALL).

バイオメトリクスは，SP 800-63A (sp800-63a.html)で記載されている全てのEnrollmentプロセスフェーズにおいて，Enrollmentの否認を防ぐため，また関与する同一個人であることを検証するために利用される.

5.2.4 アテステーション

アテステーションは，直接接続されているAuthenticatorやAuthentication操作に参加するエンドポイントに関してVerifierに対して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，限定はされていない:

- Authenticatorやエンドポイントの出所(例えば，製造元やサプライヤ認定など)，健康および一貫性.
- Authenticatorのセキュリティ機能
- バイオメトリックセンサーのセキュリティや性能特性

- センサー計測手段

このアテステーションが署名される場合，少なくともSP 800-131Aの最新版で定義された最低のセキュリティ強度(本書の刊行現在では112ビット)を備えるデジタル署名を用いて署名されるものとする(SHALL).

アテステーション情報は，VerifierのリスクベースAuthenticationの判断の一部に利用してもよい(MAY).

5.2.5 Verifierなりすまし耐性

Verifierなりすまし攻撃は，しばしばフィッシング攻撃と呼ばれ，VerifierやRPになりすまして不用心なClaimantを騙して詐欺サイトに対してAuthenticateさせる試みである．SP 800-63の以前の版では，Verifierなりすまし攻撃に対するプロトコル耐性は，中間者攻撃への強い耐性と呼ばれていた.

Verifierなりすまし耐性のあるAuthenticationプロトコルは，Authenticateされた保護チャネルをVerifierとの間に確立するものとする(SHALL)．Authenticateされた保護チャネルを確立する際にネゴシエートされたチャネル識別子は強く，変更できない形で(例えば，Verifierが知っている公開鍵に対する，Claimantが制御している秘密鍵を用いて2つの値を署名することにより)Authenticator出力に結び付けられるものとする(SHALL)．Verifierは署名またはVerifierなりすまし耐性を確認するための情報を確認するものとする(SHALL)．このようにすることで，不正なVerifierが，実際のVerifierを表す証明書を得た場合でさえも，異なるAuthenticateされた保護チャネルでAuthenticationを再生することを防止できる.

Verifier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Approveされた暗号アルゴリズムが利用されるものとする(SHALL)．この目的で利用される鍵は，少なくともSP 800-131Aの最新版で定義された最低のセキュリティ強度(本書の刊行現在では112ビット)を備えるものとする(SHALL).

Verifierなりすまし耐性のあるAuthenticationプロトコルの例としては，Client-authenticated TLSがある．クライアントは，ネゴシエーション済みの特定TLSコネクション対して一意なプロトコルから予めメッセージを受取り，そのメッセージと共にAuthenticator出力に対して署名を行う.

アウトオブバンドAuthenticatorやOTP Authenticatorのような，Authenticator出力を手動入力するようなAuthenticatorでは，手動入力ではAuthenticator出力を特定のAuthenticateされたセッションに結びつけていないため，Verifierなりすまし耐性があるとは考えないものとする(SHALL NOT)．中間者攻撃の場合には，不正なVerifierはOTP Authenticator出力をVerifierに対して再生し，Authenticationが成功してしまう.

5.2.6 Verifier-CSP通信

VerifierとCSPが個別のエンティティである場合(SP 800-63-3 Figure 4-1 (sp800-63-3.html#63Sec4-Figure1)の点線で示されているように)，VerifierとCSPの間の通信は，(Client-authenticated TLS接続のような)Approveされた暗号理論を利用する相互にAuthenticateされたセキュアチャネルを介して行われるものとする(SHALL).

5.2.7 Verifier危殆化耐性

いくつかのAuthenticatorタイプを利用に際しては，VerifierがAuthenticatorシークレットのコピーを記録する必要がある．例えば，OTP Authenticator(Section 5.1.4で記載)では，VerifierがClaimantから送信された値と比較するために，個別にAuthenticator出力を生成する必要がある．Verifierが危殆化され，記録されているシークレットが窃取される可能性があるため，Verifierが永続的にAuthenticationに利用するシークレットを記録する必要のないAuthenticationプロトコルは，より強力であるとみなされ，ここでは*Verifier*危殆化耐性があるものとして記載されている．そのようなVerifierが，全ての攻撃に耐性があるのではないことに注意すること．Verifierは，特定のAuthenticator出力を常に受け付けるように操作されるなど，異なる方法で危殆化される可能性がある．

Verifier危殆化耐性は異なる方法で実現することができる．例えば:

- 暗号Authenticatorを利用して，Authenticatorが保持する秘密鍵に対応する公開鍵をVerifierに記録する．
- 期待するAuthenticator出力をハッシュ形式で記録する．この方式は，例えばルックアップシークレット(Section 5.1.2に記載)で用いることができる．

Verifier危殆化耐性を考慮し，Verifierによって記録される公開鍵は，Approveされた暗号アルゴリズムの利用と関連付けられているものとし(SHALL)，少なくともSP 800-131Aの最新版で定義された最低のセキュリティ強度(本書の刊行現在では112ビット)を備えるものとする(SHALL)．

他のVerifier危殆化耐性のあるシークレットは，Approveされた暗号アルゴリズムを利用するものとし(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のセキュリティ強度(本書の刊行現在では112ビット)を備えるものとする(SHALL)．より複雑性の低いシークレット(例えば記憶シークレット)は，辞書の探索や全探索など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Verifier危殆化耐性を持つものと満たさないものとする(SHALL NOT)．

5.2.8 リプレイ耐性

Authenticationプロセスは，以前のAuthenticationメッセージを記録し再生することでAuthenticationを成功させることが困難であるならば，リプレイアタックに耐性を持つ．リプレイ耐性は，Authenticator出力が保護チャネルに入力されるまえに窃取される可能性があるため，Authenticateされた保護チャネルのリプレイ耐性に加えて施されるものである．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んでおらず，Verifierが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しうるため，リプレイ耐性があるといえる．

リプレイ耐性のあるAuthenticatorの例として，OTPデバイス，暗号Authenticatorおよび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Authenticator出力がシークレットそのものであり，各Authenticationで入力されるため，リプレイ耐性があるものとはみなさない．

5.2.9 Authentication意図

Authenticationプロセスは，Subjectが明示的に各AuthenticationやReauthenticationの要求に応じる必要がある場合，意図を明らかにする．Authentication意図の目的は，直接接続された物理的なAuthenticator(例えば，多要素暗号デイバス)が，エンドポイント上でマルウェアなどによりSubjectが知らないうちに利用されることをより困難にすることである．Authentication意図はそのAuthenticatorそのものにより立証するものとする(SHALL)が，多要素暗号デバイスがそのAuthenticatorが利用されるエンドポイント上で，他のAuthentication要素を再入力することにより立証してもよい(MAY).

Authentication意図は，いくつかの方法で立証してもよい(MAY)．Subjectの介入(例えばOTPデバイスから得たAuthenticator出力をClaimantが入力すること)を必要とするAuthenticationプロセスは意図を立証している．各AuthenticationやReauthentication操作に対して(例えばボタン押下や再挿入のような)ユーザアクションを必要とする暗号デバイスもまた意図を立証している.

バイオメトリクスのプレゼンテーションは，計測手段に応じてAuthentication意図を立証したりしなかったりする．指紋のプレゼンテーションは通常は意図を立証するが，一方カメラを用いたClaimantの顔の観測は，一般的にはそうならない．行動バイオメトリクスは，Claimant側で特定のアクションを常に要求されるわけではないので，同様にAuthentication意図を立証する可能性は低い.

5.2.10 制限された(RESTRICTED) Authenticator

脅威の進化につれて，Authenticatorが攻撃に対抗する能力は一般的には減少する．一方で，いくつかのAuthenticatorの性能は改善するかもしれない — 例えば，根拠となる標準が改定されることで特定の攻撃に対抗する能力が増加する.

Authenticatorの性能におけるこれらの変更を考慮するために，NISTは追加の制限を，Authenticatorタイプや特定のクラスまたはAuthenticatorタイプのインスタンスに対して設けた.

制限された(RESTRICTED) Authenticatorを利用するには，実装した組織が，制限された(RESTRICTED) Authenticator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増加しうるということを認識する必要がある．組織の責任は，彼らのシステムおよび関連データにおけるリスクを許容できるレベルを決定し，過度なリスクを緩和する方法を定義することである．何れかの当事者に対するリスクが許容できないと組織が判断した時点で，Authenticatorは利用されないものとする(SHALL NOT).

更に，Authenticationエラーのリスクは一般的には，実装した組織，Authentication結果に依存する組織，Subscriberを含む複数の当事者が負うものである．組織が制限された(RESTRICTED) Authenticatorを採用すると，Subscriberがそのリスクを十分に理解していない，またリスクを統制する能力が制限されている可能性があり，Subscriberは追加のリスクにさらされることになる．その為，CSPは次のことを実施することとする(SHALL).

1. Subscriberに対して少なくとも1つの制限されていない代替Authenticatorを提示し，要求されるAALでAuthenticateできるようにする.

2. Subscriberが理解しやすいように，制限されているAuthenticatorのセキュリティリスクと，制限されていない代替Authenticatorが利用可能であることを通知する.
3. リスクアセスメントにおけるSubscriberに対する追加のリスクに対処する.
4. 将来的にある地点で制限された(RESTRICTED) Authenticatorが許容可能でなくなる可能性を踏まえて移行プランを立て，digital identity acceptance statement (sp800-63-3.html#daps)の内容ににこの移行プランを含めておく.

6 Authenticator Lifecycle Management

本セクションは標準である.

SubscriberのAuthenticatorのライフサイクルにわたってAuthenticatorの利用に影響する様々なイベントが発生する．これらのイベントは，バインディング，紛失，盗難，不正な複製，有効期限切れ，破棄を含む．本性ではそれぞれのイベントで取るべきアクションについて述べる.

6.1 Authenticatorバインディング

*Authenticator*バインディング は特定のSubscriberアカウントとAuthenticator間の関連を確立するものであり，Authenticatorを - 他のAuthenticatorと組み合わせる場合もあるが - そのアカウントをAuthenticateするために利用できる状態にする.

AuthenticatorはSubscriberアカウントに以下のいずれかによって結び付けられるものとする(SHALL):

- Enrollmentの一部としてCSPにより発行される，または
- Subscriberが提示したCSPで利用するのに適切なAuthenticatorを関連付ける

これらのガイドラインでは， 双方の選択肢に対応するために，Authenticatorの発行よりもむしろ バインディング について述べる.

デジタルアイデンティティのライフサイクルを通じて，CSPは各アイデンティティと関連付けられる，または既に関連付けられている全てのAuthenticatorのレコードを保持する(SHALL)．CSPやVerifierは，Section 5.2.2に記載されているように，Authentication試行のスロットリングに必要な情報を保持する(SHALL)．また，CSPはユーザが提示したAuthenticatorのタイプ(例えば，単一要素暗号デバイスであるのか，多要素暗号デバイスであるのか)を検証し(SHALL)，Verifierは各AALの要件に合致しているかどうかを明らかにすることができる.

CSPによって生成されるレコードは，Authenticatorがアカウントに結び付けられた日時を含むものとする(SHALL)．レコードは，Enrollmentに関連づけられている全てのデバイスのバインディングの発生源(例えばIPアドレス，デバイス識別子)に関する情報を含むべきである(SHOULD)．可能であれば，レコードは，AuthenticatorでのAuthentication試行が失敗した際の発生源についての情報についてもまた含むべきである(SHALL).

何らかの新しいAuthenticatorがSubscriberアカウントに結び付けられる際，CSPは，バインディングプロトコルおよび関連する鍵のプロビジョニングを目的としたプロトコルが，そのAuthenticatorが使われるAALに見合ったセキュリティのレベルで，実施されたということを保証する(SHALL)．例え

ば，鍵のプロビジョニングを目的としたプロトコルがAuthenticateされた保護チャネルを利用して行われるものとする(SHALL)，または中間者攻撃を防御するため人間によって実施されるものとする(SHALL)．多要素Authenticatorのバインディングには，多要素Authenticationまたは等価(例えば，Identity proofingが実施された直後のセッションとの関連付け)なものがAuthenticatorをバインドするために必要である．Authenticatorが鍵ペアを生成して公開鍵をCSPに送信する際には，同じ条件が適用される．

6.1.1 Enrollment時のバインディング

AuthenticatorがSP 800-63A (sp800-63a.html)に記載されているIdentity proofingのトランザクションが成功した結果として，アイデンティティにバインドされる時，次の要件が適用される．Executive Order 13681 [EO 13681]によりあらゆる個人データの開示には，多要素Authenticationを利用する必要があるため，AuthenticatorはSubscriberアカウントにEnrollment時にバインドされ，Identity proofingに確立されているものを含む個人データへのアクセスが許可されることが重要である．

CSPは，記憶シークレットまたは1つ以上のバイオメトリクスに加えて，Subscriberのオンラインアイデンティティに対する物理的な (*something you have*) Authenticatorを少なくとも1つはバインドし(SHALL)，2つ以上バインドすべきである(SHOULD)．

全ての識別情報はIAL1でself-assertedされているが，オンライン素材の保存やオンラインでの評判は，Authenticatorの紛失が原因でアカウントの制御を消失することを望ましくないようにする．二つ目のAuthenticatorはあるAuthenticatorの紛失から安全に復活させることを可能にする．この理由により，CSPは少なくともIAL1でも同様にSubscriberクレデンシャルに少なくとも2つの物理Authenticatorをバインドすべき(SHOULD)である．

IAL2以上では，識別情報は，デジタルアイデンティティに関連付けられ，SubscriberはSP 800-63A (sp800-63a.html)に記載されているIdentity proofingプロセスを受ける．結果として，要求するIALと同じAALのAuthenticatorがアカウントにバインドされるものとする(SHALL)．例えば，もしSubscriberがIAL2でproofingに成功したならば，AAL2またはAAL3のAuthenticatorがIAL2のアイデンティティにバインドするために適切である．CSPはAAL1のAuthenticatorをIAL2のアイデンティティにバインドしてもよい(MAY)が，もしSubscriberがAAL1でAuthenticateされた場合には，CSPは，それが仮にself-assertedであっても，個人情報をSubscriberに対して開示しない(SHALL NOT)．以前の文章で述べているように，追加のAuthenticatorが利用可能であれば，あるAuthenticatorが破損，紛失，盗難してしまった場合に備える手段を提供することになる．

もし，一度の物理的接触や，電子的トランザクション(すなわち，単一保護セッション)でEnrollmentおよびバインディングを完了することができない場合には，プロセスを通じてApplicantとして振る舞う当事者であることを保証するために以下の方法が利用されるものとする(SHALL):

リモートトランザクションの場合:

1. Applicantは，新しいバインディングのトランザクションにおいて，以前のトランザクションの間に確立した，またはApplicantの電話番号，Emailアドレス，住所に送付された一時的なシークレットを提示することで，自分自身であることを識別する(SHALL)．

2. 長期間のAuthenticatorシークレットは，保護セッション中でApplicantに対して発行されたものに限るものとする(SHALL).

対面トランザクションの場合:

1. Applicantは上記リモートトランザクション(1)で記載したシークレットを利用するか，以前の接触時に記録したバイオメトリックの利用を通じて，対面で自分自身であることを識別する(SHALL).
2. 一時シークレットは再利用されないものとする(SHALL NOT).
3. もしCSPが物理的なトランザクションの間に長期間のAuthenticatorシークレットを発行するならば，それは対面でApplicantに対して発行された物理デバイスに対して局所的にロードされる，またはアドレスレコードを確認する方法で配送されるものとする(SHALL).

6.1.2 Post-Enrollment Binding

6.1.2.1 既存AALにおける追加Authenticatorのバインディング

記憶シークレットを除いて，CSPとVerifierは，使用する各要素の少なくとも2つ有効なAuthenticatorの保持をSubscriberに促すべきである(SHOULD). 例えば，普段は物理AuthenticatorとしてOTPデバイスを利用しているSubscriberは，物理Authenticatorの紛失，盗難，破損に備えて，ルックアップAuthenticatorの番号を発行したり，アウトオブバンドAuthenticatorとしてデバイスを登録してもよい(MAY). 記憶シークレットAuthenticatorの置き換えに関するより多くの情報は Section 6.1.2.3 を参照すること.

したがって，CSPはSubscriberアカウントに対して追加のAuthenticatorをバインドすることを許可すべきである(SHOULD). 新しいAuthenticatorを追加する前に，まずCSPはSubscriberに対して，新しいAuthenticatorが使用されるAAL(またはそれ以上のAAL)でAuthenticateするよう要求する(SHALL). Authenticatorの追加後は，CSPはSubscriberに対して，新しいAuthenticatorをバインドしたトランザクションと独立した方法(例えば，Subscriberに以前関連付けられているアドレスへのEmail)で，通知を行うべきである(SHOULD). CSPは，この方法でバインドできるAuthenticatorの数を制限してもよい(MAY).

6.1.2.2 単一要素アカウントに対する追加要素の追加

Subscriberアカウントに1つのAuthentication要素がバインドされていて(すなわちIAL1/AAL1)，異なるAuthentication要素の追加Authenticatorを追加する場合，Subscriberはアカウントを AAL2 にアップグレードするよう要求してもよい(MAY). IALはIAL1のままである.

新しいAuthenticatorのバンディング前に，CSPはSubscriberに対してAAL1でAuthenticateするよう要求する(SHALL). 新しいAuthenticatorをバインドしたトランザクションと独立した方法(例えば，Subscriberに以前関連付けられているアドレスへのEmail)で，通知を行うべきである(SHOULD).

6.1.2.3 紛失したAuthentication要素の置き換え

Subscriberが多要素Authenticationに必要な全ての要素のAuthenticatorを失い，かつIdentity proofがIAL2またはIAL3で実施されていた場合，SubscriberはSP 800-63A (sp800-63a.html)で記載されているIdentity proofingプロセスを再び実施する(SHALL)．もしCSPがオリジナルのproofingプロセスから証拠を得ることができるならば，SP 800-63A (sp800-63a.html) Section 4.2に記載されているプライバシリスクアセスメントに従って，以前提供された証拠とClaimantとがバインドされていることを確認する簡易Proofingプロセスを利用してもよい(MAY)．CSPは．既存のアイデンティティへのバインディングを確認するために，Claimantに対して可能であれば残りの要素のAuthenticatorを用いてAuthenticateするよう要求する(SHALL)．IAL3におけるAuthentication要素の再確立は，対面またはSP 800-63A (sp800-63a.html) Section 5.3.3.2に記載された監督済みリモートプロセスを通じて実施し(SHALL)，オリジナルのProofingプロセスで収取したバイオメトリックを検証する(SHALL)．

CSPはSubscriberに対して，そのイベントを通知すべきである(SHOULD)．Proofingプロセスの一部として要求されているものと同じ通知でもよい(MAY)．

記憶シークレットの紛失(すなわち忘れてしまうこと)の置き換えは，非常に一般的であるがゆえに解決が難しい問題である．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．もしバイオメトリックがアカウントにバインドされていれば，バイオメトリックと関連する物理Authenticatorが新しい記憶シークレットを設定するために利用されるべきである(SHOULD)．

アカウントにバイオメトリックがバインドされていない場合には，上記のre-proofingプロセスの代わりとして，CSPは，Subscriberの住所の一つに送信された確認コードとともに2つの物理Authenticatorを用いたAuthenticationを行い新しい記憶シークレットをバインドしてもよい(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るものとする(SHALL)．それらは，住所に送付され，最大7日間有効であるものとする(SHALL)．しかし，U.S. Postal Serviceが直接配送できない範囲の住所に適用する場合，例外プロセスとして最大21日まで有効としてもよい(MAY)．物理的なメール以外の方法で送信された確認コードの有効期限は最大10分とする(SHALL)．

6.1.3 Subscriberが提示するAuthenticatorとのバインディング

Subscriberは特定のAALのAuthenticationにふさわしいAuthenticatorを既に所持しているかもしれない．例えば，彼らはAAL2及びIAL1とみなせるソーシャル・ネットワーク・プロバイダから2要素Authenticatorを受領しており，そのクレデンシャルをIAL2を必要とするRPで利用したいとする．

現実的には大量のAuthenticatorを管理するSubscriberの負荷を軽減するために，CSPはSubscriberが提供するAuthenticatorの利用に対応するべきである(SHOULD)．これらのAuthenticatorのバインディングは，Section 6.1.2.1に記載されているように実施する(SHALL)．Authenticator強度がself-evidentでない(例えば，与えられたAuthenticatorタイプが単一要素か多要素か)場合は，CSPは実際により強いAuthenticatorが使用されていることが(例えば，Authenticatorの発行者や製造者の検証などにより)分かるようにならない限り，より弱いAuthenticationの利用を前提とすべきである(SHOULD)．

6.1.4 更新

CSPは，既存のAuthenticatorの有効期限に到達する前に適切な時間を確保して，更新後のAuthenticatorをバインドすべきである(SHOULD)．このプロセスは，初期のAuthenticatorバインディングプロセス(例えば，アドレスレコードを確認するなど)に正確に従うべきである(SHOULD)．新しいAuthenticatorが正しく使用できるようになると，CSPはそれが置き換えているAuthenticatorを無効化してもよい(MAY)．

6.2 紛失，盗難，破損，不正な複製

危殆化したAuthenticatorには，盗難，紛失，不正な複製の対象となったものが含まれる．一般的に，紛失したAuthenticatorは盗難されたりAuthenticatorの正当なSubscriberではない誰かによって危殆化されたものであると仮定しなければならない．破損または故障したAuthenticatorもまた，Authenticatorシークレットが抽出されたいかなる可能性に対しても防御するために，侵害されたとみなされる．攻撃者に入手されるといった危殆化した形跡がなく，忘れてしまった記憶シークレットは顕著な例外である．

危殆化したAuthenticatorの中断，無効化，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)．

Authenticatorの紛失，盗難，破損の安全に報告することを促すために，CSPは，Subscriberに対してバックアップまたは代替Authenticatorを利用してCSPに対してAuthenticateする方法を提供すべきである(SHOULD)．このバックアップAuthenticatorは記憶シークレットか物理Authenticatorのいずれかとする(SHALL)．どちらが利用されてもよい(MAY)が，この報告を行うためには1つだけのAuthentication要素だけが必要である．あるいは，Subscriberは，Authenticate済み保護チャネルを確立し，Proofingプロセスにおいて収集された情報を検証してもよい(MAY)．CSPはアドレスレコード(すなわちEmail，電話，住所)を検証し，危殆化したと報告のあったAuthenticatorを中断してもよい(MAY)．中断は，Subscriberが正当な(すなわち，中断されていない) Authenticatorを用いて正しくCSPに対してAuthenticateすることができ，Authenticatorを再アクティベーションを要求する場合，再開できるものとする(SHALL)．CSPは中断されているAuthenticatorがもはや再アクティベートができなくなるまでの時間制限を設けてもよい(MAY)．

6.3 有効期限切れ

CSPは有効期限があるAuthenticatorを発行してもよい(MAY)．Authenticatorの有効期限が切れた際には，Authenticationに利用することはできない(SHALL NOT)．有効期限切れのAuthenticatorを用いてAuthenticationが試行された時には，CSPはSubscriberに対してこのAuthentication失敗は他の理由ではく有効期限によるものであることを指摘すべきである(SHOULD)．

CSPはAuthenticatorの有効期限切れまたは更新されたAuthenticatorを受領した後，できるだけ早くCSPによって署名された属性証明書を含む物理Authenticatorの引き渡しまたは破棄したことの証明をSubscriberに対して求める(SHALL)．

6.4 失効と解約

Authenticatorの失効は，特にPIV Authenticatorの文脈では解約と呼ばれることがあるが，AuthenticatorとCSPが保持するクレデンシャルとのバインディングを除去することを指す.

CSPは，オンラインアイデンティティが存在しなくなった(例えば，Subscriberが死亡，詐称Subscriberであることが判明した)とき，Subscriberに要求されたとき，またはCSPがSubscriberがもはや加入要件を満たさなくなったと判断したとき，速やかにAuthenticatorのバインディングを削除する(SHALL).

CSPは，失効または解約の実施後できるだけ早くCSPによって署名された属性証明書を含む物理Authenticatorの引き渡しまたは破棄したことの証明をSubscriberに対して求める(SHALL).

PIV Authenticatorの解約に関するさらなる要件は FIPS 201 にある.

7 Session 管理

This section is normative.

一度 Authentication イベントが行われると，Subscriber が複数のインタラクションをまたぐアプリケーションを Authentication イベントを繰り返す必要なく継続して使用し続けられることはしばしば望まれる． この要件は， Authentication イベントがネットワーク経由で調整したいくつかのコンポーネントやパーティを巻き込む Federation シナリオ (SP 800-63C (sp800-63c.html) で説明される) に特に当てはまる.

この振る舞いを容易にするため，* Session * は，ある Authentication イベントへの応答によって開始されてもよい (MAY) ．そしてその Session はそれが終了されるときまで維持される． Session 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，その他の理由など，様々な理由により終了されることがある (MAY) ． Session は， Reauthentication イベント (Section 7.2 で説明される) を通して維持されてもよい (MAY) ．ユーザーは，初回の Authentication 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.

Session 管理は 頻繁な Credential の提示よりも望ましい． Credential を頻繁に提示することのユーザビリティの低さは，しばしばロック解除用 Credential のキャッシュなどの回避策に対するインセンティブを生み出し， Authentication イベントの新鮮さを無効にする.

7.1 Session Bindings

Session は， Subscriber が動作しているソフトウェア — ブラウザー，アプリケーション，オペレーティング システム (つまり Session Subject) — と， Subscriber がアクセスする RP や CSP (つまり Session ホスト) の間に発生する． Session シークレットは， Subscriber のソフトウェアとアクセスされているサービスの間で共有されることとする (SHALL) ． このシークレットは，Session の 2 つのエンドをバインドし， Subscriber が経時的にサービスを使用し続けることを許可する． シークレットは，Subscriber のソフトウェアによって直接提示されることとする (SHALL) ．または，シークレットの所有は暗号化メカニズムによって証明されることとする (SHALL) .

Session のバインドに使用されるシークレットは， Session ホストによって Authentication イベントへの直接の応答の中で生成されることとする (SHALL) ． Session はその生成がトリガーされた

Authentication イベントの AAL プロパティ 継承するべきである (SHOULD) . Session は Authentication イベントよりも低い AAL で考えられてもよい (MAY) が, Authentication イベントよりも高い AAL では考えないこととする (SHALL NOT) .

Session Binding に使用されるシークレットは :

1. インタラクションの間に，通常は Authentication の直後に Session ホストによって生成されることとする (SHALL) .
2. 承認されたランダムビットジェネレーター [SP 800-90Ar1] によって生成され，少なくとも64ビットの Entropy を含むこととする (SHALL) .
3. Subscriber のログアウト時に, Session Subject によって消去または無効にされることとする (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期限が切れたとみなされるとき，Subscriber エンドポイントから消去されるべきである (SHOULD) .
5. Cross-site Scripting (XSS) 攻撃によるローカルストレージ暴露の可能性があるため，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. Authenticated Protected Channel を使用してデバイスから送信，または受信されることとする (SHALL) .
7. Section 4.1.4，4.2.4，4.3.4 の AAL にふさわしい時間の後は，タイムアウトすることとし，受け付けられてはならないこととする (SHALL) .
8. ホストと Subscriber のエンドポイント間の安全でないコミュニケーションでは有効にしないこととする (SHALL NOT) . Authenticated Session は，Authentication の後，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ないこととする (SHALL NOT) .

URL か POST 内容は Session identifier を含むこととする (SHALL) . Session identifier は, Session の外側で行われたアクションが Protected Session に影響しないことを保証することを RP によって検証されることとする (SHALL) .

経時的に Session を管理するためにはいくつかのメカニズムがある. 次のセクションでは，各例のテクノロジー特有の追加要件と考慮事項に沿って，それぞれの例を示す. 追加の有用なガイダンスとして, OWASP *Session Management Cheat Sheet* [OWASP-session] がある.

7.1.1. ブラウザー クッキー

ブラウザー クッキーは，サービスにアクセスする Subscriber のための Session の作成と追跡において，有力なメカニズムである.

クッキーは :

1. セキュアな (HTTPS) Session のみでアクセス可能なようにタグ付けされることとする (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可能であることとする (SHALL) .
3. JavaScript (HttpOnly) からアクセス不可となるようにタグ付けされるべきである (SHOULD) .
4. Sessionの有効な期間，またそのすぐ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，強制的な Session タイムアウトへの依存はしないこととする (SHALL NOT)．

7.1.2 Access Tokens

Access Token — OAuth に見られるような — はアプリケーションが Authentication イベントの後，Subscriber のために一連のサービスに Access することを許可するために使用される． OAuth Access Token の存在は，他のシグナルがない場合，RP によって Subscriber の存在として解釈されないこととする (SHALL NOT)． OAuth Access Token，および関連付けられた Refresh Token は，Authentication Session が終了され，Subscriber そのアプリケーションから去ったあとでも，有効であってもよい (MAY)．

7.1.3 デバイスの識別

Subscriber とサービス間の Session の制定には，安全なデバイス識別の他の方法 — 相互 TLS や Token Binding，その他のメカニズムを含み，これに限らない — が使用されてもよい (MAY)．

7.2 Reauthentication

認証された Session の継続性は，Authentication の際に Verifier によって発行され，セッション中に任意に更新される Session シークレット の所有に基づくこととする (SHALL)． Session の性質は以下を含むアプリケーションに依存する：

1. Web ブラウザー Session と “Session” クッキー
2. Session シークレットを保持するモバイルアプリケーションのインスタンス

Session シークレットは非永続的であることとする (SHALL)．つまり，関連するアプリケーションのリスタートやホストデバイスのリブートを超えて残置されないこととする (SHALL NOT)．

Session の 定期的な Reauthentication は，認証された Session において，Subscriber が継続して存在していること (すなわち Subscriber がログアウトせずに立ち去っていないこと) を確認するために実行されることとする (SHALL)．

Session は，Session シークレット単独の提示に基づいて，セクション 4.1.3, 4.2.3 そして 4.3.3 (AAL に応じる) のガイドラインを超えて拡張されないこととする (SHALL NOT)． Reauthentication のタイムリミットは，Session が 満了する前に，表 7-1で指定された Authentication Factor を Subscriber に促すことで延長されることとする (SHALL)．

タイムアウトやその他のアクションによって Session が終了されたとき，ユーザーは再度の Authenticate によって新しい Session の確立を要求されることとする (SHALL)．

表 7-1 AAL Reauthentication 要件

AAL	要件
1	任意の 1 つのファクターの提示

AAL	要件
2	Memorized Secret または Biometrics の提示
3	全てのファクターの提示

> ノート: AAL2では，Session シークレットは *something you have* であり，また追加の Authentication Factor が Session を継続するために要求されるため， 物理的な Authenticator でない，Memorized Secret または Biometrics が必須とされる.

7.2.1 Federation または Assertion からの Reauthentication

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 Federation プロトコルを使用するとき，Session 管理と Reauthentication は特別な考慮事項が適用される． Federation プロトコルは CSP と RP の間の Authentication イベントを執り行うが，それらの間に Session を確立しない． CSP と RP は，しばしば別々の Session 管理技術を採用しているので，これらのセッション間にはどんな相関も仮定しないこととする (SHALL NOT) . したがって，RP の Session が満了し RP が再認証を必要とするとき，CSP の Session が満了しておらず，ユーザーの Reauthentication なしに CSP でこの Session から新しい Assertion が生成される可能性は十分にある.

Federation プロトコルによる Reauthentication を必要とする RP は，— 可能な場合はプロトコル内で — CSPへの許容可能な最大の Authentication 経過時間を指定することとし (SHALL)，その期間内に Authentication が行われていない場合，CSP は Subscriber を Reauthentication することとする (SHALL) . CSP は，RP が，Assertion が Reauthentication に十分かを決定でき且つ次の Reauthentication イベントの時間を決定するために， Authentication イベントの時間を RP へ伝えることとする (SHALL) .

8 脅威とセキュリティに関する考慮事項

This section is informative.

8.1 Authenticator の脅威

Authenticator を制御できる Attacker は Authenticator の所有者のように偽装することができる. Authenticator への脅威は，Authenticator を構成する Authentication 要素の種類ごとの Attack に基づいて分類されることができる :

- *Something you know* は攻撃者に開示されることがある． Attacker は Memorized Secret を推測するかもしれない． Authenticator が Shared Secret である場合，Attacker は CSP または Verifier への Access を得てシークレットの値を入手する，または，その値のハッシュに対して辞書 Attack を行うことができるだろう． Attacker は，PIN やパスコードの入力を観察したり，PIN やパスコードが書かれた記録やジャーナルエントリを見つけたり，またはシークレッ

トをキャプチャーするために不正なソフトウェア (例：キーボードロガー) をインストールしたりするかもしれない． さらに，Attacker は Verifier によってメンテナンスされている Password データベースに対する Offline Attack によってシークレットを特定するかもしれない．

- *Something you have* は紛失，破損，所有者から盗難される，または Attacker によって複製されることがある． たとえば，所有者のコンピューターへの Access を得た Attacker は，ソフトウェアの Authenticator をコピーするかもしれない． ハードウェアの Authenticator は，盗難されたり，いじられたり，複製されるかもしれない． Out-of-band のシークレットは，Attacker によって傍受され，彼らの Session を Authenticate するために利用されるかもしれない．
- *Something you are* は複製されることがある．たとえば，Attacker は Subscriber の指紋のコピーを得たり，レプリカを製作するかもしれない．

このドキュメントは Subscriber が Verifier に対して虚偽の Authenticate を試みようとしている Attacker と共謀してないことを前提としている． この前提に立って，Digital Authentication に使用される Authenticator への脅威はいくつかの例とともに 表 8-1 にリストされる．

表 8-1 - Authenticator の脅威

Authenticator の脅威/攻撃	**説明**	**例**
Assertion の製造または変更	Attacker が偽の Assertion を生成する	危殆化した CSP が 正しく Authenticate されていない Claimant の Identity を主張する
	Attacker が既存の Assertion を変更する	Authentication Assertion の AAL を変更する危殆化したプロキシ
盗難	物理的な Authenticator が Attacker によって盗難される	ハードウェア暗号化デバイスが盗難される
		OTP デバイスが盗難される
		ルックアップシークレット Authenticator が盗難される
		携帯電話が盗難される
複製	Subscriber の Authenticator が，本人の知識ごと，または知識なしに複製される	Password が書かれた紙が開示される
		電子ファイルに格納されている Password がコピーされる
		ソフトウェア PKI Authenticator (Private Key) がコピーされる

Authenticatorの脅威/攻撃	説明	例
		ルックアップシークレットAuthenticator がコピーされる
		偽造された Biometric Authenticator が製造される
盗聴	Subscriber が認証を行っているときに， Authenticator Secret または Authenticator Output が攻撃者に暴露される	キーボードエントリーを監視して Memorized secret を取得する
		キーストロークをロギングするソフトウェアによって，Memorized secret または Authenticator の出力を横取りする
		PIN パッドデバイスから PIN がキャプチャされる
		ハッシュされた Password が取得され，Attacker に別の Authentication で使用される (*pass-the-hash Attack*)
	Out of band シークレットが，通信チャネルの危殆化によって Attacker に傍受される	Out of band シークレットが暗号化されていないWi-Fiで送信され，Attacker に受信される
オフライン クラッキング	Authenticator が，Authentication メカニズムの外側で解析メソッドによって明らかにされる	Software PKI authenticator が，Private Key の復号に使用する正しい Password を識別するための辞書 Attack を受ける
サイドチャネル Attack	Authenticator Secret が，Authenticator の物理的特性を利用して明らかにされる.	鍵がハードウェア Cryptographic Authenticator の差分電力解析によって明らかにされる
		Authenticator への無数の試行の応答時間の解析によって， Cryptographic Authenticator シークレットが抽出される
Phishing または Pharming	Attacker が Verifier や RP であると考えるように Subscriber をだますことで，Authenticator Output がキャプチャされる	Subscriber が Verifier に偽装した Web サイトに入力することで，Password が明らかにされる

Authenticatorの脅威/攻撃	説明	例
		銀行 Subscriber が，銀行担当者に見せかけたフィッシャーからのメールに返信することで，Memorized Secret が明らかにされる
		Subscriber が DNS スプーフィングを介して偽の Verifier Webサイトにアクセスしてしまうことで，Memorized Secret が明らかにされる
Social Engineering	Attacker が，Subscriber 自身が Authenticator Secret または Authenticator Output を明らかにするように説き伏せるために Subscriber と信頼関係を構築する	Subscriber の上司の代理として Password を聞いてきた同僚に対して Subscriber が Memorized Secret を明らかにする
		システム管理者を装った Attacker からの電話問い合わせによって，Subscriber が Memorized Secret を明らかにする
		Attacker が，犠牲者の携帯電話を Attacker にリダイレクトするようにモバイルオペレーターをやりこめることで，SMS経由の Out-of-band シークレットが Attacker に受信される
オンラインでの推測	Attacker が Verifier にオンラインで接続し，その Verifier のコンテキストで有効な Authenticator Output を推測しようと試行する	Memorized Secret を推測するためにオンライン辞書 Attack が利用される
		正当な Claimant に登録された OTP デバイスの Authenticator Output を推測するために，オンラインでの推測が使用される
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，接続された Authenticator への Remote Access を Subscriber 同意なしにプロキシする.	エンドポイントに接続された Cryptographic Authenticator が，Remote から Attacker の Authenticate に使用される
	エンドポイント上の不正なコードが，Verifier が意図していない Authentication を引き起こす	Authentication が，Subscriber ではなく Attacker のために行われる

Authenticator の脅威/攻撃	説明	例
		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 Out-of-band シークレットを読みだし，Attacker がシークレットを Authenticate に使用する
	エンドポイント上の不正なコードが，Multi-Factor ソフトウェア Cryptographic Authenticator を危殆化させる	不正なコードが Authentication をプロキシする，またはエンドポイントから Authenticator の鍵をエクスポートする
認証されていない Binding	Attacker が彼らの管理下の Authenticator を Subscriber のアカウントにバインドさせる	Attacker が Subscriber への経路の途中で Authenticator やプロビジョニングキーを傍受する

8.2 脅威を軽減するストラテジー

表 8-2 は，上記で説明された脅威の軽減を支援するメカニズムをまとめたものである.

表 8-2 - Authenticator の脅威を軽減する

Authenticator の脅威/攻撃	脅威を軽減するメカニズム	規約の参照
盗難	Memorized Secret または Biometrics によってアクティブにされる必要がある Multi-Factor Authenticator を使用する	4.2.1, 4.3.1
	Memorized Secret または Biometrics を含む Authenticator を組み合わせて使用する	4.2.1, 4.3.1
複製	Authentication シークレットの抽出や複製が長期的に困難な Authenticator 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セカンダリの out-of-band の Authentication 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，保護されたチャネル経由で Authenticate を行う (例 : ブラウザー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 Attack に耐性のある Authentication プロトコルを使用する	5.2.8

Authenticator の脅威/攻撃	脅威を軽減するメカニズム	規約の参照
	信頼された入力と信頼された表示機能の Authentication 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	高い Entropy の Authenticator Secret で Authenticator 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，ハッシュ化された状態で Memorized Secret を保存する	5.1.1.2, 5.2.7
サイドチャネル Attack	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 Authenticator アルゴリズムを使用する	4.3.2
Phishing または Pharming	Verifier Impersonation への防御が提供される Authenticator を使用する.	5.2.5
Social Engineering	カスタマーサービスエージェントなどの第三者による Social Engineering のリスクを引き起こす Authenticator の使用を避ける	6.1.2.1, 6.1.2.3
オンラインでの推測	高い Entropy の出力を生成する Authenticator 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した後にはロックアップする Authenticator を使用する	5.2.2
エンドポイントの危殆化	Subscriber の物理的なアクションを必要とするハードウェア Authenticator を使用する	5.2.9
	ソフトウェアベースの鍵は Restricted-Access ストレージで保持する	5.1.3.1, 5.1.6.1, 5.1.8.1
認証されていない Binding	Authenticator と 関連する鍵のプロビジョニングには MitM に体制のあるプロトコルを使用する	6.1

表 8-1 で説明された脅威を軽減するために，いくつかのストラテジーを適用できる：

- 複数の要素 があると，Attack がより成功しにくくなる． もし Attacker が Cryptographic Authenticator を盗むことと Memorized Secret の推定の両方を必要とするなら，その両方を達成することはとても困難になり得る.
- 物理的なセキュリティメカニズム は盗難された Authenticator を複製から保護するために採用されることがある．物理的なセキュリティメカニズムは，耐タンパー性の確保，検出，および対応を可能にする.
- 共有されている辞書に現れない 長い *Memorized Secret* の使用を要求する ことは，Attacker に

すべての入力可能な値を試させる.

- システムと *Network* のセキュリティコントロール は，Attacker がシステムへの Access を得ることや，不正なソフトウェアをインストールすることを防ぐために使用される.
- 定期的なトレーニング は，いつどのように危殆化 ーまたは危殆化の疑いー を報告するか Subscriber の理解を促したり，また，Attacker の Authentication プロセスを破るための試行を示す振る舞いのパターンを認識したりするために実施される.
- *Out of band* テクニック は，登録されたデバイス (例: 携帯電話) を所有していることの検証に使用される.

8.3 Authenticator の復旧

多くの Authentication メカニズムの弱点は，Subscriber が 1 つまたは複数の Authenticator のコントロールを失い，それらを交換する必要がある場合の手続きである． 多くの場合，Subscriber を Authenticate できる残りの選択肢は限られている．経済的な心配 (例 : コールセンター運営のコスト) から，安価であまりセキュアでないバックアップの Authentication メソッドを使用したいと考えさせる． Authenticator の復旧は，人がアシストをするという点で，Social Engineering Attack のリスクもある.

Authentication 要素の完全性を維持するためには，1 つの要素を使用した Authentication を異なる要素の Authenticator を取得するために活用できないことが必要不可欠である． たとえば，Memorized Secret は新しいルックアップシークレットのリストを得るために使用できてはならない.

8.4 Session Attack

上記のディスカッションでは Authentication イベント自体に対する脅威に焦点を当てているが，Authentication イベントに続く Session 上のハイジャック Attack は同様のセキュリティインパクトを持つ可能性がある． セクション 7 の Session 管理ガイドラインは XSSのような Attack に対して Session の完全性を維持するために必要不可欠である． さらに，実行可能な内容が含まれていないことを確実にするために，[OWASP-XSS-prevention]に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． これらのガイドラインでは，Session 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，Session シークレットが Mobile Code にアクセスできないようにすることも推奨している.

もう一つの Authentication 後の脅威である Cross-site Request Forgery (CSRF) は，複数の Session を同時に有効にするユーザ傾向の利点を利用する． 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 Session 識別子を埋め込んで検証することが重要である.

9 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． *This section is informative.*

9.1 プライバシー Risk Assessment

セクション 4.1.5, 4.2.5, 4.3.5 は CSP にレコード保有のためのプライバシー Risk Assessment を行わせることを必要とする．このようなプライバシー Risk Assessment が含まれる：

1. レコード保有が Subscriber に侵害や権限のない情報への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インパクト

CSP はリスク受容，リスク軽減，リスク共有など，特定されたプライバシーリスクをとった場合に起こることを合理的に正当化できるべきである． Subscriber の同意を得ることはリスク共有の形と見なされ，Subscriber が共有されたリスクを適切に評価し，受け入れる能力があることが合理的に期待される場合にのみ適している．

9.2 プライバシー コントロール

セクション 4.4 は CSP が適切に調整されたプライバシーコントロールを採用することを必要とする． SP 800-53 は，CSP が Authentication メカニズムをデプロイするときに検討するべき一連のプライバシーコントロールを提供する． これらのコントロールは，成功し，信頼できるデプロイメントのための通知や救済策，その他の重要な考慮事項をカバーする．

9.3 使用制限

セクション 4.4 は，Authentication 以外のいかなる目的，詐欺の緩和，または法律や法的手続きにおいて，CSP が明確な通知を提供し Subscriber からの追加の用途についての同意を取得しない限り，Authentication プロセス中に収集され保持される Authenticator についての情報の使用を禁止する． そのような情報の使用は，収集の本来の目的に限定されていることが保証されるよう注意が払われるべきである． 提案されたエージェンシーの使用がこのスコープに該当するが疑問がある場合は，あなたの SAOP に相談してほしい． セクション 4.4 で述べられているように，Subscriber による追加の要件の受諾は，Authentication サービスを提供する条件としないこととする．

9.4 Agency-Specific Privacy Compliance

セクション 4.4 は，連邦政府の CSP に関する特定の遵守義務をカバーする． プライバシーリスクを評価，軽減し，Authenticator を発行または維持する PII のコレクションが PIA を実施するための *Privacy Act of 1974* Privacy Act や *E-Government Act of 2002* E-Gov 要件をトリガーするかどうかなど，コンプライアンス要件について助言するように，Digital Authentication システム開発の最初期段階にあなたのエージェンシーの SAOP を参画させることが重要である． たとえば，Biometrics の集中保有に関して， Privacy Act requirements がトリガーされ，Authentication に必要なその他の属性や PII の収集，維持のために，新規または既存の Privacy Act 記録のシステムによってカバーされる必要があるかもしれない． SAOP は PIA が必要かどうかを判断する際， 同様にエージェンシーを支援することができる．

これらの考慮事項は Authentication だけのために Privacy Act SORN や PIA を開発するための要件として読まれるべきでない． 多くの場合，全体を網羅する Digital Authentication プロセスの PIA と

SORN を下書きすることや，エージェンシーがオンラインで確立しているサービスやベネフィットを議論する，より大きなプログラマティック PIA の一部として Digital Authentication を含めることが最も理にかなっている.

多くの Digital Authentication コンポーネントのために，SAOP がそれぞれ個別のコンポーネントの認識と理解を持つことが重要である． たとえば，他のプライバシー成果物は連携された CSP や RP のサービスを提供または使用するエージェンシーに適用可能であってもよい (例 : データ使用規約，コンピュータマッチング規約) . SAOP は追加要件の適用を判断する際にエージェンシーを支援できる． また，Digital Authentication の個別のコンポーネントを完全に理解することは，コンプライアンスプロセスまたはほかの手段によって，SAOP が徹底的にプライバシーリスクを評価，軽減することを可能にする.

10. Usability の考慮事項

This section is informative.

ISO/IEC 9241-11 は，Usability を「特定のユーザが特定の使用状況において，有効性，効率，満足をもって特定のゴールを達成するためにある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，満足を達成する鍵となる要素として，ユーザ，そのゴール，使用状況に焦点を当てている． Usability を達成するためには，これらの鍵となる要素を占める全体論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のゴールは，意図したタスクを実行することである．
Authentication はこのゴールを実現する機能である． しかしユーザの視点からは，Authentication はそれらと意図したタスクの間にある． Authentication の効果的な設計と実装は，正しいことを行うことを簡単にし，謝ったことを行うことを難しくし，誤ったことが起きたとき，回復することを簡単にする．

組織はステークホルダーの Digital Authentication エコシステム全体における全体的な影響を認識する必要がある． ユーザは多くの場合，一つか複数の Authenticator をそれぞれ異なる RP に対して採用する． 続いて，彼らはパスワードを覚えたり，どの Authenticator がどの RP のものかを思い出したり，複数の物理的な Authentication デバイスを持ち歩いたりすることに奮闘する． プアーな Usability はしばしば対抗メカニズムや意図しない回避策を生じさせ，結果としてセキュリティ管理の有効性を低下させるため，Authentication の Usability を評価することは極めて重要である．

Usability を開発プロセスに取り入れることで，ユーザの Authentication ニーズ と組織のビジネス上のゴールに取り組みながら，セキュアで使いやすいAuthentication ソリューションをリードすることができる．

デジタルシステムにおける Usability のインパクトは，適切な AAL を決定する際の Risk Assessment の一環として考慮される必要がある． より高い AAL の Authenticator はより良い Usability を提供することがあり，より低い AAL アプリケーションとしての使用を許すべきである．

Authentication のための Federation を活用することで，多くの Usability の問題を楽にすることができるが，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な独自のトレードオフを持つ．

このセクションは一般的な Usability の考慮事項と実装方法を提供するが，特定のソリューションを推奨しない． 言及された実装は特定の Usability 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示である． さらに，Usability の考慮事項とその実装は one-size-fits-all のソリューションを予防する多くの要素に対して敏感である． たとえば，デスクトップコンピューティング環境で使っているフォントサイズは，小さな OTP デバイスのスクリーンではテキストを画面の外に出してしまうかもしれない． 選択した Authenticator の Usability 評価を実施することは，実装の極めて重要な要素である． ユーザの代表者，実際的なゴールとタスク，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」という単語は「Claimant」または「Subscriber」を意味する.

ガイドラインと考慮事項はユーザ視点から記述される.

アクセシビリティは Usability とは異なり，このドキュメントの対象外である． セクション 508 は情報技術のバリアを排除し，連邦政府機関に対して障害を持つ人々がオンラインの公開コンテンツにアクセスできるようにすることを求めるために制定された． アクセシビリティのガイダンスについてはセクション 508 の法律と標準を参照すること.

10.1 Authenticator に共通する Usability の考慮事項

Authentication システムの選択や実装を行う際は，ユーザ，そのゴール，使用状況の組み合わせに注意しながら，選択した Authenticator のライフサイクル全体にわたる Usability (例 : 代表的な使用法や断続的なイベント) を検討する.

単一の Authenticator Type では通常，利用人口のすべてを満足させることはできない． したがって，可能な限り — AAL の要件に基づいて — CSPは代わりの Authenticator をサポートし，ユーザが必要に応じて選択できるようにするべきである． 多くの場合，タスクの即時性，知覚されるコストベネフィットのトレードオフ，特定の Authenticator に対する不慣れさが選択に影響を与える． ユーザはその時点での最小の負担またはコストとなる選択肢を選ぶ傾向がある． たとえば，タスクが情報システムへの即時の Access を必要とするとき，ユーザはより多くのステップを必要とする Authenticator を選択するのではなく，新しいアカウントと Password を作成することを好むかもしれない． あるいは，ユーザがすでに Identity 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) Identity 連携という選択肢を選ぶかもしれない． ユーザはいくつかの Authenticator を他のものよりもよく理解し，また彼らの理解と経験に基づいた異なる信頼レベルを持っている.

ポジティブな Authentication 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，ユーザ視点から Authenticator を検討するべきである． 包括的な Authentication Usability のゴールは，ユーザの負担と Authentication の摩擦 (例 : ユーザが Authenticate する回数，関連するステップ，ユーザ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ストラテジーの一つを例示する.

ほとんどの Authenticator に適用可能な Usability の考慮事項を以下に説明する．後続のセクションでは，特定の Authenticator に固有の Usability の考慮事項について説明する.

すべての Authenticator の代表的な使用法に関する Usability の考慮事項 :

- Authenticator の使用と保守に関連する情報を提供する．たとえば Authenticator 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) .
- ユーザが自分の Authenticator をすぐに利用できるようにするため，Authenticator 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 Authenticator へのネガティブなインパクトに対応するため，代替の Authentication の選択肢が必要であると考える.
- 可能な限り，AAL の要件に基づいて，ユーザは代替の Authentication の選択肢を提供されるべ

きである． これによりユーザは，コンテキスト，ゴール，およびタスク (例 : タスクの頻度や即時性) に基づいて Authenticator を選択することができる． 代替の Authentication の選択肢は特定の Authenticator で発生する可用性の問題にも役立つ.

- ユーザ向けテキストの特徴 :
  - 意図されたオーディエンスに対して，平易な言語でユーザ向けテキストを書く (例 : 説明，指示，通知，エラーメッセージなど) ． 専門的な技術用語を避け，通常，第6学年から第8学年の識字レベルで書く.
  - ユーザ向けおよびユーザ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，周囲の背景とのコントラストなどを含む可読性を考慮する． 読みづらいテキストはユーザ入力のミスを引き起こす． 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黒上の白である.
    - 電子ディスプレイ用には Sans serif フォント． 印刷用には Serif フォント.
    - 混乱しやすい文字を明確に区別するフォント (例 : 大文字の「O」と数字「0」など) .
    - デバイスの画面に収まる限りは，最小フォントサイズを 12 ポイントとする.
- Authenticator 入力中のユーザ体験 :
  - マスクされたテキスト入力はエラーを起こしやすいので，入力中にテキストを表示するオプションを提供する． ユーザに対して一度十分に表示された文字はまた非表示にされる． 従来のデスクトップコンピュータよりもモバイルデバイス (例 : タブレットやスマートフォン) では Memorized Secret を入力するの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.
  - テキスト入力に不足しない時間が与えられていることを確認する (すなわち，入力画面が尚早にタイムアウトしない) ．与えられたテキスト入力時間がユーザのニーズと一致していることを確認する.
  - ユーザの混乱や不満を軽減するため，入力エラーに対する明確，有意義かつアクション可能なフィードバックを提供する． ユーザが誤ってテキストを入力したことを知らない場合，重大な Usability への影響が生じる.
  - ユーザが Authenticator Output を入力する必要がある Authenticator に対して，少なくとも10回の入力を許す． 入力テキストがより長く複雑になるほど，ユーザ入力エラーの可能性は大きくなる.
  - 残された試行回数について，明確で有意義なフィードバックを提供する． 混乱と不満を軽減するため，レート制限 (すなわち，スロットリング) によって次の試行までどらくらい待たなければならないかを知らせる.
- 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，フォーム要因の制約の影響を最小限に抑える :
  - 小さなデバイスでのタイピングはフルサイズキーボードでのタイピング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 Usability を向上させる． 画

面上のキーボードサイズが小さいほど，画面上のターゲットのサイズに対する入力メカニズム (例 : 指など) のサイズにより，タイプすることがより困難になる.
    - 小さなディスプレイのための優良なユーザインターフェースと情報デザインを追及する.

断続的なイベントには，Reauthentication，アカウントロックアウト，有効期限切れ，失効，破損，紛失，盗難，機能しないソフトウェアなどのイベントが含まれる.

Authenticator タイプ間の断続的なイベントに関する Usability の考慮事項 :

- ユーザの非アクティブ状態によって Reauthenticate が必要となることを予防するために，非アクティブタイムアウトが起こらないようその直前(例 : 2分など) に活動をトリガーするためのプロンプトを出す.
- ユーザの操作に関係のない定期的な Reauthentication イベントが必要となる前には，ユーザが作業を保存することを十分な時間 (例 : 1時間など) を以って促す.
- どのようにして，どこで技術的な支援を得られるか明確にする． たとえば，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，ヘルプデスクサポートのための電話番号などの情報をユーザに提供する． 理想的には，十分な情報が提供された場合は，外部からの介入なしにユーザが断続的なイベントから自分たちで回復できるようになる.

10.2 Authenticator Type による Usability の考慮事項

ほとんどの Authenticator (セクション 10.1) に適用可能な前述の一般的な Usability の考慮事項に加えて，以下のセクションでは，特定の Authenticator Type に固有のその他の Usability の考慮事項について説明する.

10.2.1 Memorized Secret

代表的な使用法

ユーザは，Memorized Secret (一般的に Password や PIN といわれる) を手動で入力する.

典型的な使用法のための Usability の考慮事項 :

- Memorized Secret の記憶しやすさ
    - ユーザが覚えておくべき項目が多いほど，思い出すことに失敗する可能性は大きくなる. Memorized Secret が少なくなるほど，特定の RP に必要な特定の Memorized Secret をより簡単に思い出すことができる.
    - 使用頻度の低い Password は記憶負担が大きくなる.
- Memorized Secret 入力中のユーザ体験
    - Passphrase を含む Memorized Secret を入力するためのフィールドにコピーアンド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 Usability の考慮事項は以下を含む :

- ユーザが Memorized Secret を作成または変更するとき :
  - Memorized Secret の作成や変更の方法を情報を明確に伝える.
  - セクション5.1.1 で指定されているように，Memorized Secret の要件を明確に伝える.
  - Passphrase の使用をサポートするには，少なくとも64文字の長さを許容する． ユーザが空白を含む任意の文字を使用して，望み通りの長さで Memorized Secret を作成し記憶を手助けすることを奨励する.
  - Memorized Secret に他の構成ルール (例 : 異なる文字タイプの混合) を課さない.
  - ユーザの要求や Authenticator の危殆化の証拠がない限り，Memorized Secret は恣意的な (例 : 定期的な) 変更を必要としない． (詳細については セクション 5.1.1 を参照)
- 選択された Password を拒否された場合，(例 : 受け入れられない Password の”ブラックリスト”に含まれる，過去に使用されたなど) 明確，有意義でアクション可能なフィードバックを提供する.

10.2.2 ルックアップ シークレット

代表的な使用法

ユーザは印刷物または電子的な Authenticator を使用して，Verifier の問いかけに応答するために必要な適切なシークレットを探す． たとえば，ユーザはカードにテーブル形式で印刷された数字または文字列のうち，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 Usability の考慮事項 :

- ルックアップシークレット入力中のユーザ体験
  - プロンプトの複雑さとサイズを考慮する． ユーザ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，Usability への影響は大きくなる． Authentication のためのルックアップシークレットの量と複雑さを選択する際には，認知的作業負荷と入力の物理的な難しさの両方を考慮に入れるべきである.

10.2.3 Out-of-Band

代表的な使用法

Out-of-band authentication では，ユーザはプライマリとセカンダリの通信チャネルへの Access を持つ必要がある.

代表的な使用法のための Usability の考慮事項 :

- ロックされたデバイス上でシークレットの受信を通知する．ただし Out-of-Band デバイスがロックされている場合，シークレットに Access するにはデバイスへの Authentication が必要とされるべきである.
- 実装に応じて，ユーザがモバイルデバイスにテキストを入力しなければならない場合に特に問題となるフォーム要因の制約を考慮する． より大きなタッチ領域を提供することはモバイルデバイスでシークレットを入力する際の Usability を向上させる.

- より良い Usability 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だ (例 : ユーザが Out-of-Band シークレットをコピーアンドペースト出来るような画面上でのシングルタップ，コピー機能など) ． このような機能をユーザに提供することは，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． たとえば，ユーザがスマートフォンで Authentication Secret を転送することは，Out-of-Band アプリケーションとプライマリチャネルを (もしかすると複数回にわたり) 前後に切り替える必要があるため，困難である．

10.2.4 Single-Factor OTP デバイス

代表的な使用法

ユーザは Single-Factor OTP デバイスによって生成された OTP に Access する．Authenticator Output は通常デバイスに表示され，ユーザは Verifier のためにそれを入力する．

代表的な使用法のための Usability の考慮事項は以下を含む :

- Authenticator Output は少なくとも変更までに1分を許容する．しかし理想的には セクション 5.1.4.1 で指定されているように満2分間を許容する． ユーザは Authenticator Output を入力するのに十分な時間を必要とする (Single-Factor OTP デバイスとその入力画面の間を前後に行き来することを含む) ．
- 実装に応じた，実装者にとっての追加の Usability の考慮事項は以下のとおり :
    - もし Single-Factor OTP デバイスがそのアウトプットを電子インターフェース (例 : USB など) を介して提供する場合，ユーザが Authenticator Output を手動で入力する必要がないことが望ましい． しかし，物理的インプットの操作 (例 : ボタンを押すなど) が必要とされる場合，USBポートの位置は Usability の問題となる可能性がある． たとえば，一部のコンピュータの USB ポートはコンピュータの背面にあり，ユーザの手が届きにくくなる．
    - USB ポートのような直接的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 Usability の問題を引き起こすことがある． たとえば，ラップトップコンピュータの USB ポートの数はしばしばとても限られる． これはユーザに対して Single-Factor OTP デバイスのために他の USB 周辺機器の接続解除を強制するかもしれない．

10.2.5 Multi-Factor OTP デバイス

代表的な使用法

ユーザは第二の Authentication Factor を通じて Multi-Factor OTP デバイスによって生成された OTP に Access する． 通常 OTP はデバイスに表示され，Verifier のためにそれを手動で入力する． 第二の Authentication Factor は Memorized Secret ，一体型 Biometrics (例 : 指紋など) リーダー，または直接的なコンピュータインターフェース (例 : USB ポート) などの統合的なエントリーパッドに入力することで達成されてもよい． 追加の要素に対する Usability の考慮事項も同様に適用される． ー Multi-Factor Authenticator に使用される Memorized Secret については セクション

10.2.1，Biometrics については Section 10.4 を参照.

代表的な使用法のための Usability の考慮事項は以下を含む：

- Authenticator Output の手動入力中のユーザ体験
  - タイムベース OTP の場合は，OTP が表示されている時間に加えて猶予期間を設ける. ユーザは Multi-Factor OTP デバイスとその入力画面の間を前後に行き来することを含む，Authenticator Output を入力するのに十分な時間を必要とする.
  - ユーザが統合的なエントリーパッドを使用するか，モバイルデバイス上に Authenticator Output を入力して Multi-Factor OTP デバイスのロックを解除する必要がある場合は，フォーム要因の制約について考慮する． 小さなデバイスでのタイピングは従来のキーボードよりはるかにエラーが発生しやすく，時間がかかる． 統合的なエントリーパッドとオンスクリーンキーボードが小さくなるほど，タイプすることがより難しくなる． より大きなタッチ領域を提供することは Multi-Factor OTP デバイスのロックを解除する，またはモバイルデバイスで Authenticator Output を入力する際の Usability を向上させる.
  - USB ポートのような直接的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 Usability の問題を引き起こすことがある． たとえば，ラップトップコンピュータの USB ポートの数はしばしばとても限られるため，ユーザに対して Multi-Factor OTP デバイスのために他の USB 周辺機器の接続解除を強制するかもしれない.

10.2.6 Single-Factor 暗号ソフトウェア

代表的な使用法

ユーザは暗号ソフトウェアキーの所持とコントロールを証明することによって Authenticate する.

代表的な使用法のための Usability の考慮事項は以下を含む：

- ユーザがどの Authentication タスクに使用する Cryptographic Key であるかを認識して呼び出す必要があるため，Cryptographic Key にはユーザにとって意味のある適切で説明的な名前がつけられる． これはユーザが，似ている，またはあいまいな名前の複数の Cryptographic Key を扱うことを予防する． より小さなモバイルデバイス上の複数の Cryptographic Key から選択することは，画面サイズが小さくなるために Cryptographic Key の名前が短縮されると特に問題になる.

10.2.7 Single-Factor 暗号デバイス

代表的な使用法

ユーザは Single-Factor 暗号デバイスの所持を証明することで Authenticate する.

代表的な使用法のための Usability の考慮事項は以下を含む：

- Single-Factor 暗号デバイスの操作として物理的インプット (例 : ボタンを押すなど) を必要とする場合， Usability の問題となる可能性がある． たとえば，いくつかの USB ポートはコン

ピュータの背面にあり，ユーザの手が届きにくい.

- USB ポートのような直接的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 Usability の問題を引き起こすことがある． たとえば，ラップトップコンピュータの USB ポートの数はしばしばとても限られるため，ユーザに対して Single-Factor 暗号デバイスのために他の USB 周辺機器の接続解除を強制するかもしれない.

10.2.8 Multi-Factor 暗号デバイス

代表的な使用法

Authenticate するために，ユーザはディスク上に格納された Cryptographic Key，またはアクティベーションを必要とするなんらかの”ソフト”メディアの所有とコントロールを証明する． アクティベーションは，Memorized Secret または Biometrics いずれかの第二の Authentication Factor のインプットによるものである． 追加の要素に対する Usability の考慮事項も同様に適用される． — Multi-Factor Authenticator に使用される Memorized Secret については セクション 10.2.1，Biometrics については Section 10.4 を参照.

代表的な使用法のための Usability の考慮事項は以下を含む：

- ユーザがどの Authentication タスクに使用する Cryptographic Key であるかを認識して呼び出す必要があるため，Cryptographic Key にはユーザにとって意味のある適切で説明的な名前がつけられる． これはユーザが，似ている，またはあいまいな名前の複数の Cryptographic Key を扱うことを予防する． より小さなモバイルデバイス上の複数の Cryptographic Key から選択することは，画面サイズが小さくなるために Cryptographic Key の名前が短縮されると特に問題になる.

10.2.9 Multi-Factor 暗号デバイス

代表的な使用法

ユーザは Multi-Factor 暗号デバイスの所持と保護された Cryptographic Key のコントロールを証明することで Authenticate する． デバイスは，Memorized Secret または Biometrics いずれかの第二の Authentication Factor によってアクティベートされる． 追加の要素に対する Usability の考慮事項も同様に適用される． — Multi-Factor Authenticator に使用される Memorized Secret については セクション 10.2.1，Biometrics については Section 10.4 を参照.

代表的な使用法のための Usability の考慮事項は以下を含む：

- ユーザは，認証のあと，Multi-Factor 暗号デバイスを接続したままにすることを必要としない． ユーザはそれが終わったあと，Multi-Factor 暗号デバイスを取り外すことを忘れるかもしれない (例 : スマートカードリーダー内にスマートカードを忘れてコンピュータから遠ざかるなど) .
    - ユーザは Multi-Factor 暗号デバイスが接続されたままである必要があるのかどうか，知らされることが求められる.

- ユーザがどの Authentication タスクに使用する Cryptographic Key であるかを認識して呼び出す必要があるため，Cryptographic Key にはユーザにとって意味のある適切で説明的な名前がつけられる． これはユーザが，似ている，またはあいまいな名前の複数の Cryptographic Key に面することを予防する． スマートフォンのような，より小さなモバイルデバイス上の複数の Cryptographic Key から選択することは，画面サイズが小さくなるために Cryptographic Key の名前が短縮されると特に問題になる．
- USB ポートのような直接的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 Usability の問題を引き起こすことがある． たとえば，ラップトップコンピュータの USB ポートの数はしばしばとても限られるため，ユーザに対して Multi-Factor 暗号デバイスのために他の USB 周辺機器の接続解除を強制するかもしれない．

10.3 ユーザビリティに関する考慮事項のまとめ

表10-1 に各 Authenticator Type の 代表的な使用法と断続的なイベントについての Usability の考慮事項 をまとめる． 代表的な使用法についての Usability の考慮事項の多くは，行で示されているように，ほとんどの Authenticator Type に適用される． この表では，Authenticator Type 全体にわたる Usability の共通で多様な特性をハイライトしている． 各列は，各 Authenticator に対処する Usability の属性を簡単に識別できるようにする． ユーザのゴールや使用状況により，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 Authenticator Type を提供し，ユーザがそれらを選択できるようにする．

Multi-Factor Authenticator (例 : Multi-Factor OTP デバイス，Multi-Factor 暗号ソフトウェア，Multi-Factor 暗号デバイスなど) はまたそれらの第二要素の Usability の考慮事項 を継承する． Biometrics は Multi-Factor Authentication ソリューションのアクティベーション要素としてのみ許されているため，Biometrics の Usability の考慮事項は 表 10-1 には含まれず，セクション 10.4 で説明される．

表 10-1 Authenticator Type による Usability の考慮事項のまとめ

Usability Considerations	Memorized secrets	Look-up Secrets	Out of Band	Single Factor OTP Device	Multi-Factor OTP Device	Single Factor Cryptographic Software	Single Factor Cryptographic Device	Multi-Factor Cryptographic Software	Multi-Factor Cryptographic Device
Typical usage									
Authenticator availability – authenticators readily in user's possession	◆	◆	◆	◆	◆	◆	◆	◆	◆
Plain language for user facing text (e.g., instructions, prompts, notifications, error messages)	◆	◆	◆	◆	◆	◆	◆	◆	◆
Legibility of user facing text or text entered by users	◆	◆	◆	◆	◆	◆	◆	◆	◆
Unmasked text entry		◆	◆	◆	◆				
Support text entry – length of 64 characters, copy and paste	◆								
Delayed masking during text entry	◆								
Adequate time allowed for text entry	◆	◆	◆	◆	◆				
Entry errors – need clear and meaningful feedback	◆	◆	◆	◆	◆				
Minimum of 10 attempts allowed	◆	◆	◆	◆	◆				
Remaining allowed attempts – need clear and meaningful feedback	◆	◆	◆	◆	◆				
Form-factor constraints	◆	◆	◆	◆	◆	◆	◆	◆	◆
Location and availability of a direct computer interface such as a USB port				◆	◆		◆		◆
Physical input required (such as pressing a button)				◆			◆		
Cryptographic keys need for descriptive and meaningful names						◆		◆	◆
Complexity and size of the prompts		◆							
Authentication to secondary device to access the authentication secret			◆						
Continuous hardware connection not required									◆
Intermittent Events									
Reauthentication due to user inactivity	◆	◆	◆	◆	◆	◆	◆	◆	◆
Fixed periodic reauthentication	◆	◆	◆	◆	◆	◆	◆	◆	◆
Provisions for technical assistance	◆	◆	◆	◆	◆	◆	◆	◆	◆
Provisions to create and change memorized secrets	◆								

10.4 Biometrics の Usability の考慮事項

このセクションは Biometrics の 一般的な Usability の考慮事項についてのハイレベルオーバービューを提供する． Biometrics Usability のより詳細な説明は *Usability & Biometrics, Ensuring Successful Biometric Systems* NIST Usability に見つけることができる．

ほかの Biometrics 様式も存在するが，以下の3つの Biometrics 様式が Authentication のためによく

利用される : 指紋，顔，虹彩

代表的な使用法

- すべての様式で，ユーザのなじみ深さと熟練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 (すなわち，ユーザがアクションを実行することを可能にするデバイスの特性)，フィードバック，および明確な指示は Biometrics デバイスによるユーザの成功にとって極めて重要である． たとえば，生存検出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.
- 理想的には，ユーザは第二の Authentication Factor のために，最も快適な様式を選択することができる． ユーザ人口は，他よりもいくつかの Biometrics 様式をより快適かつなじみ深く感じ，また受け入れるだろう.
- Biometrics をアクティベーション要素とするユーザ体験
    - 残された試行回数について，明確で有意義なフィードバックを提供する． たとえば，混乱と不満を軽減するため，レート制限 (すなわち，スロットリング) によって次の試行までに待たなければならない時間を知らせる.
- 指紋の Usability の考慮事項:
    - ユーザは最初の Enrollment 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キャプチャー成功能力に影響する.
    - 指紋採取の品質に影響を及ぼす追加の要素には，年齢，性別，職業がある (例 : 化学薬品を取り扱う，または手で広範囲に働くユーザは摩擦隆線が低下している可能性がある) .
- 顔の Usability の考慮事項 :
    - 顔認識の精度に影響するため，ユーザは Enrollment の際にアーティファクト (例 : 眼鏡など) を装着したかどうかを覚えておく必要がある.
    - 環境の証明条件の違いは顔認識の精度に影響することがある.
    - 顔の表情は顔認識の精度に影響する (例 : 笑顔に対するナチュラルな状態) .
    - 顔のポーズは顔認識の精度に影響する (例 : カメラを見下ろす，またはカメラから遠ざかる) .
- 虹彩の Usability の考慮事項 :
    - カラーコンタクトの装着は虹彩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は手術後の再登録が必要になることがある.
    - 環境の証明条件の違いは虹彩認識精度，特に特定の虹彩の色に影響することがある.

断続的なイベント

Biometrics は Multi-Factor Authentication の第二の要素としてのみ許可されているため，第一の要素の断続的なイベントの Usability の考慮事項は引き続き適用される． 認識精度に影響することがある Biometrics 使用の断続的なイベントは以下のものを含んでいるが，これに限らない :

- ユーザが登録した指にけがをすると，指紋認識が機能しないことがある．指紋が薄くなった

ユーザにとっては指紋 Authentication は困難である.

- Authentication のための顔認識の時点と最初の Enrollment の時点の間に経過した時間は，ユーザの顔の経年による自然の変化として認識精度に影響することがある． ユーザの体重の変化もまた要因となる.
- 眼科手術を受けた人は，再登録を行わない限り虹彩認識が機能しないことがある.

すべての Biometrics 様式において，断続的なイベントの Usability の考慮事項は以下を含む：

- 代替の Authentication 方法が利用可能で機能している必要がある．Biometrics が機能しない場合，代替の第二要素としてユーザが Memorized Secret を使用できるようにする.
- 技術的な支援のための規定：
    - どのようにして，どこで技術的な支援を得られるかの情報を明確に伝える． たとえば，オンラインセルフサービス機能へのリンク，ヘルプデスクサポートのための電話番号などの情報をユーザに提供する． 理想的には，外部からの介入なしにユーザが断続的なイベントから自分たちで回復できるだけの十分な情報を提供する.
    - Biometrics センサの感度に影響することがある要因をユーザに通知する (例：センサーの清浄度) .

11 References

This section is informative.

11.1 General References

[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 (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 (https://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 (https://www.ece.cmu.edu/~lbauer/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 (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 (https://www.federalregister.gov/d/2014-25439).

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

[ICAM] National Security Systems and Identity, Credential and Access 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 (https://georgewbush-whitehouse.archives.gov/omb/memoranda/m03-22.html).

[M-04-04] OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, December 16, 2003, available at: https://georgewbush-whitehouse.archives.gov/omb/memoranda /fy04/m04-04.pdf (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 (http://www.internetsociety.org/sites/default/files/06_3_1.pdf)

[NIST Usability] National Institute and Standards and Technology, *Usability & Biometrics, Ensuring Successful Biometric Systems*, 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-session] Open Web Application Security Project, *Session Management Cheat Sheet*, available at: https://www.owasp.org/index.php/Session_Management_Cheat_Sheet (https://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 (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 (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 /opcl/privacy-act-1974 (https://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.

[Section 508] Section 508 Law and Related Laws and Policies (January 30, 2017), available at: https://www.section508.gov/content/learn/laws-and-policies (https://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 (http://ieeexplore.ieee.org/iel5/6233637/6234400/06234434.pdf).

11.2 Standards

[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 (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 usability*, March 1998, available at: https://www.iso.org/standard/16883.html (https://www.iso.org/standard/16883.html).

[ISO/IEC 2382-37] International Standards Organization, *Information technology — Vocabulary — Part 37: Biometrics*, 2017, available at: http://standards.iso.org/ittf/PubliclyAvailableStandards/c066693_ISO_IEC_2382-37_2017.zip (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 (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 (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 attack detection — Part 1: Framework*, 2016, available at: http://standards.iso.org

/ittf/PubliclyAvailableStandards/c053227_ISO_IEC_30107-1_2016.zip (http://standards.iso.org/ittf/PubliclyAvailableStandards/c053227_ISO_IEC_30107-1_2016.zip).

[ISO/IEC 30107-3] International Standards Organization, *Information technology — Biometric presentation attack 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 (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 (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 (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 (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 (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/).

11.3 NIST Special Publications

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 digital authentication.

[SP 800-38B] NIST Special Publication 800-38B, *Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication*, 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 (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, *Digital Identity Guidelines*, June 2017, https://doi.org/10.6028/NIST.SP.800-63-3 (https://doi.org/10.6028/NIST.SP.800-63-3).

[SP 800-63A] NIST Special Publication 800-63A, *Digital Identity Guidelines: Enrollment and Identity Proofing Requirements*, June 2017, https://doi.org/10.6028/NIST.SP.800-63a (https://doi.org/10.6028/NIST.SP.800-63a).

[SP 800-63C] NIST Special Publication 800-63C, *Digital Identity Guidelines: Authentication and Lifecycle Management*, June 2017, https://doi.org/10.6028/NIST.SP.800-63c (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 Approved 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 (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 (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 (https://doi.org/10.6028/NIST.SP.800-185).

11.4 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 (https://doi.org/10.6028/NIST.FIPS.140-2).

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

[FIPS 201] Federal Information Processing Standard Publication 201-2, *Personal Identity 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

本付録は参考情報である.

本付録を通じて，ディスカッションを容易にするため”パスワード”という単語を用いる．使用箇所では，パスワード同様にパスフレーズおよびPINを含むものとして解釈すべきである.

A.1 Introduction

ユーザビリティとセキュリティの立場の両面からパスワードの利用は大きな不満を伴うにも関わらず，Authenticationの形式 [Persistance] として極めて広く利用され続けている．人間は，しかしながら，複雑で任意のシークレットを記憶する能力が限られているため，しばしば容易に推測できるパスワードを選ぶことがある．その結果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，これらの記憶シークレットの複雑さを増加させる努力として，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，記号のような文字種を組み合わせて作成す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難易度へ与える影響はあれど，当初 [ポリシー] で考えられていたほど得られる利益が大きくないことが明らかになった.

ユーザが選択したパスワードの複雑さは，エントロピー [Shannon] という情報理論の概念を用いて特徴づけられることが多い．確定的分布関数に従うデータに対するエントロピーを計算することは容易だが，ユーザ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ではない．このため，主にパスワードの長さの観点で差があり少しシンプルになっているアプローチがここに示されている.

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をうけない．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作用する．これらの攻撃は本付録の対象外である.

A.2 長さ

パスワードの長さは，パスワードの強度 [Strength] [Composition] 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ブルートフォース攻撃をももたらす.

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に対してレート制限をかけることで緩和することができる．攻撃者(またはしつこくタイプミスを繰り返すClaimant)が大量の誤ったパスワード推測を行いSubscriberに対するDoS攻撃を容易に行えないようにするためには，そこまで誤った試行回数が多くはないのであればレート制限を発生させな

くても済むほど十分複雑である必要がある．とはいえ，推測が成功する確率が大きくなる前にレート制限は発生する．

オフライン攻撃は，攻撃者がデータベース侵害を通じて1つ以上のハッシュされたパスワードを得た場合に発生する可能性がある．攻撃者が1人以上のユーザのパスワードを決定する能力は，パスワードの記録方法によって異なる．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，そのために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．そのような基準でさえも，レート制限なしで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するよりも複雑で大きなオーダーである必要がある．

ユーザは，こういった理由もあり，望みどおり長いパスワードが使えるよう促進されるべきである．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，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適切なことである．

A.3 複雑さ

上記のように，構成ルールはユーザ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る．しかしながら，研究者はユーザが構成ルール [Policies] で課せられた要件に対してかなり予測可能な方法で応答することを示した．例えば，パスワードとして”password”を選択したユーザは，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!”を選択する．

複雑なパスワードを作成しようとしてオンラインサービスにそれを拒否されるとユーザも不満を抱く．多くのサービスではスペースや様々な特殊文字を含むパスワードを拒否する．場合により，特殊文字が受け入れられないことがあるが，それ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ためである．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ので，そのような予防策は不要である．ユーザはフレーズの利用を許容するためにスペースを使ってもよい．しかし，スペース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，1つの場合に比べて2つのスペースを利用したことが検出されないなど)を招く可能性があるため，検証時は事前に入力されたパスワードから連続するスペースを削除すると効果的である．

ユーザのパスワードの選択は非常に予想可能であり，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．これらのパスワードには，辞書の単語や上記例の”Password1!”のような過去に漏洩したパスワード，このような状況から，ユーザが選択したパスワードは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が望ましい．このブラックリストは，ユーザ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，辞書の単語および特定の用語(サービス自体の名前など)を含むべきである．ユーザのパスワードの選択は最低文字の要件が適用されるため，この辞書は要件に合致したものだけを含んでいる必要がある．

極端に複雑な記憶シークレットは新たな潜在的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，統計的にそのようなシークレットの記録方法のなかには脆弱なものがある．これは，極端に長い、または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追加の動機付けになる．

A.4 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一つの要素が，それが生成されるプロセスである．(VerifierやCSPでは殆どの場合)分布が一様でランダムなシークレットでは、同じ長さと複雑さ要件に対してユーザが選択するシークレットに比べてパスワード推測やブルートフォース攻撃の難易度が高くなるだろう．従って，SP 800-63-2のLOA2ではランダムに選択された6桁の数字のPINが許容されるのに対し，ユーザが選択したシークレットの場合は最低8文字という要件になっている．

上で論じたように，記憶シークレットの長さ要件に考慮された脅威モデルには，オンライン攻撃に対するレート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．この制約があるものの，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は引き続き適切であるとみなされる．

A.5 サマリ

ここで推奨されている内容を超えた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，ユーザの不満を増加させる．結果としてユーザはしばしばこれらの制限を回避してしまうため，逆効果である． 更に，ブラックリスト，安全なハッシュストレージ，レート制限などの他の緩和策は，のブルートフォース攻撃をためにより効果的です．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．
