NIST Special Publication 800-63
Version 1.0.2

電子認証に関するガイドライン

米国国立標準技術研究所
による推奨

William E. Burr
Donna F. Dodson
W. Timothy Polk

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

情 報 セ キ ュ リ テ ィ

米国国立標準技術研究所
情報技術ラボラトリ
コンピュータセキュリティ部門
Gaithersburg, MD 20899-8930

2006 年 4 月

米国商務省　長官
Donald L. Evans

技術管理局　技術担当商務次官
Robert Cresanti

米国国立標準技術研究所　所長
William Jeffrey

この文書は下記団体によって翻訳監修されています
IPA 独立行政法人 情報処理推進機構 INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
NRI SECURE TECHNOLOGIES

コンピュータシステムの技術に関する報告書

米国国立標準技術研究所（NIST: National Institute of Standards and Technology, 以下 NIST と称す）の情報技術ラボラトリ（ITL: Information Technology Laboratory）は、国家の測定および標準に関する基盤において技術的リーダーシップを提供することにより、米国の経済と公共福祉に貢献している。情報技術ラボラトリは、テストの実施、テスト技法の開発、参照データの作成、実装によるコンセプト実証、技術的分析を通じて、情報技術の開発と生産的利用の発展に努めている。情報技術ラボラトリの責務は、連邦政府の情報システムにおいて、費用対効果の高いセキュリティと国家安全保障関連を除く情報のプライバシを確保するための技術的、物理的、管理的および運用のための標準とガイドラインを策定することにある。NIST Special Publication 800 シリーズでは、コンピュータセキュリティにおける情報技術ラボラトリの調査、ガイドライン、普及活動と、産業界、政府機関および教育機関との共同活動について報告する。

作成機関

本文書は、NIST が、Federal Information Security Management Act of 2002 (2002 年施行の連邦情報セキュリティマネジメント法、以下、FISMA と称す)に基づく法的責務を果たす一環として作成したものである。

NIST は、政府機関のすべての業務と資産に十分な情報セキュリティを提供するための標準とガイドライン(最小限の要求事項を含む)を作成する責任を負うが、このような標準およびガイドラインは国家安全保障にかかわるシステムには適用されない。このガイドラインは、行政管理予算局(Office of Management and Budget、以下、OMB と称す)の通達(Circular)A-130 の第 8b(3)項「政府機関の情報システムの保護(Securing Agency Information Systems)」の要求事項と一致しており、これは A-130 の付録 IV「重要部門の分析(Analysis of Key Sections)」で分析されているとおりである。補足情報は、A-130 の付録 III に記載されている。

このガイドラインは連邦政府機関が使用する目的で作成されている。非政府組織が自由意志で使用することもでき、著作権の制約はない(出自を明らかにする場合は NIST とする)。(翻訳者注:著作権に関するこの記述は、SP800-63 の英語の原文のことを言っており、日本語へ翻訳した本書の著作権は、独立行政法人情報処理推進機構および NRI セキュアテクノロジーズ株式会社に帰属する)。

本文書におけるいっさいは、商務長官が法的権威に基づき連邦政府機関に対して義務付けた拘束力を有する標準およびガイドラインを否定するものではない。また、これらのガイドラインは、商務長官、行政管理予算局長、または他のすべての連邦政府当局者の既存の権威を変更したり、これらに取って代わったりするものと解釈してはならない。

米国国立標準技術研究所、Special Publication 800-63、64ページ
(2006年4月)

この文書中で特定される商業的組織、装置、資料は、実験手順または概念を適切に説明するためのものである。したがって、NIST による推薦または保証を意味するものではなく、これらの組織、資料、または装置が、その目的に関して得られる最善のものであると意味しているわけでもない。

概要

本文書は、連邦政府機関において電子認証を実装する際の技術的な指針を提供するものである。本文書では、公開ネットワークを経由したユーザのリモート認証について説明する。身元識別情報の検証、登録、トークン、認証プロトコル、および関連するアサーションの分野における 4 つの保証レベルについて、それぞれの技術的な要求事項を規定している。

キーワード：認証、認証保証、CSP（クレデンシャルサービスプロバイダ）、暗号化、電子認証、電子クレデンシャル、電子トランザクション、電子政府、身元識別情報の検証、パスワード、PKI、公開鍵基盤、トークン。

謝辞

本書執筆者である Bill Burr、Tim Polk、および Donna Dodson（ともに NIST）は、本文書の草稿をレビューし、文書の向上に貢献をしてくれた同僚に対し感謝の意を表したい。また、公共部門および民間部門の方々から建設的で思慮に富むご意見を多数いただき、本書の品質と有益性の向上を果たせたことに深く感謝する。

本書の日本語版作成にあたっては、 セコム株式会社 IS 研究所 松本 泰様に、ご指導を賜りました。ここに、心より感謝の意を表します。

本文書の概要

電子認証は、電子的な手段によって情報システムに提示されるユーザ身元識別情報の信用を確立するプロセスである。このプロセスにおいて、電子政府や電子商取引を目的として、ネットワーク経由で個人をリモートより認証する必要がある場合、電子認証には技術的に困難な課題が伴う。本文書は、連邦政府機関の職員が連邦の IT システムに対して各自の身元をリモートで証明できるようにするための、技術的な指針を提供するものである。本指針では、秘密情報に基づいたリモート認証を行うために従来から広く実装されている手段のみを対象とする。認証対象となる個人はこれらの手段を通じて、自分がなんらかの秘密情報を知っていることまたは所持していることを証明する。NIST では、ほかのリモート認証手段（生体認証を使用するものや、個人的ではあるが真の意味で秘密ではない個人情報の詳細な知識を使用するものなど）についても調査し、それらのリモート認証手段の使用に関する追加の指針を作成することも検討している。

本技術指針はOMBのガイダンスである『*E-Authentication Guidance for Federal Agencies*』[OMB 04-04]を補足するものである。このOMBガイダンスでは、認証エラーとクレデンシャルの誤用によって生じる結果に応じた、レベル 1～4 の 4 つの認証レベルを定義している。レベル 1 は最低の保証レベルであり、レベル 4 は最高の保証レベルである。このOMBガイダンスでは、認証エラーによって生じる可能性が高い結果に応じて、必要となる認証保証レベルを定めている。認証エラーによって生じる結果が深刻であるほど、必要となる保証レベルが高くなる。また、このOMBガイダンスでは、具体的な応用事例やトランザクションに必要な電子認証の保証レベルを決定するための基準を提供している。この基準は、応用事例やトランザクションのリスクとそれらが発生する可能性に基づく。

政府機関は、リスクアセスメントを完了し、明らかになったリスクを要求される保証レベルに対応付けたあと、その要求保証レベルの技術的要求事項を最低限満たす適切な技術を選択できる。特に本書では、次の分野における 4 つの保証レベルのそれぞれについて具体的な技術的要求事項を提示する。

- トークン。身元を証明するもの（通常は暗号鍵またはパスワード）。
- 身元識別情報の検証。身元識別情報をトークンに結び付けるクレデンシャルの登録と提供。
- リモート認証メカニズム。すなわち、認証要求者が実際に加入者本人であることを証明するために用いられる、クレデンシャル、トークン、および認証プロトコルの組み合わせ。
- アサーションメカニズム。リモート認証の結果を第三者に伝えるために用いられる。

以下に、4 つの保証レベルのそれぞれについて技術的要求事項の概要を示す。

レベル 1：このレベルでは身元識別情報の検証は要求事項になっていないが、保護されたトランザクションやデータにアクセスするのが同一の認証要求者であることに対するなんらかの保証が、認証メカニズムによって提供される。このレベルでは広

範な認証技術を利用することが可能であり、レベル 2、3、または 4 のどのトークン手法も利用できる。認証要求者が認証に成功するには、セキュアな認証プロトコルを通じて、認証要求者本人がトークンを管理していることを証明する必要がある。

レベル 1 では、平文のパスワードや秘密情報はネットワーク経由で送信されない。ただし、このレベルでは盗聴者によるオフライン攻撃を阻止する暗号手段は要求されていない。たとえば、単純な、パスワードに基づく challenge-response プロトコルが許される。多くの場合、そのようなプロトコルによるやり取りを傍受した盗聴者は、単純な辞書攻撃によりパスワードを知ることが可能である。

レベル 1 では、認証用の長期共有秘密情報が検証者に開示されることがある。認証の成功の結果として発行される認証要求者に関するアサーションは、それに依拠する当事者が（承認された手段を用いて）暗号学的な処理を行うことで認証するか、またはセキュアな認証プロトコルを通じて信頼のおける第三者から直接取得する。

レベル 2：レベル 2 では、単一要素によるリモートネットワーク認証を提供する。レベル 2 では、身元識別情報の検証に関する要求事項が導入され、識別のための有形物または情報の提示が求められる。レベル 2 では広範な認証技術を利用することが可能であり、レベル 3 または 4 のどのトークン手法も利用できるほか、パスワードや PIN も利用できる。認証要求者が認証に成功するには、セキュアな認証プロトコルを通じて、認証要求者本人がトークンを管理していることを証明する必要がある。盗聴、リプレイ攻撃、およびオンライン推測攻撃が阻止される。

認証用の長期共有秘密情報を使用する場合、認証要求者およびクレデンシャルサービスプロバイダ（CSP）が運営する検証者以外にその情報が開示されることは決してない。ただし、セッションの（一時的な）共有秘密情報は、CSP によって独立した検証者に対して提供される場合がある。承認された暗号化技法が要求される。認証の成功の結果として発行される認証要求者に関するアサーションは、それに依拠する当事者が（承認された手段を用いて）暗号学的な処理を行うことで認証するか、またはセキュアな認証プロトコルを通じて信頼のおける第三者から直接取得する。

レベル 3：レベル 3 では、複数要素によるリモートネットワーク認証を提供する。このレベルでは、身元識別情報の検証手順において、識別のための物または情報を検証することが求められる。レベル 3 の認証では、暗号化プロトコルを通じて、鍵またはワンタイムパスワードの所持を証明することが基本となる。レベル 3 の認証では、プロトコルに対する各種の脅威（盗聴、リプレイ攻撃、オンライン推測攻撃、検証者になりすます攻撃（Verifier impersonation attack）、中間者攻撃など）を通じて、一次認証トークン（秘密鍵、プライベート鍵、またはワンタイムパスワード）が危殆化されることを防ぐために、高い強度を持った暗号メカニズムが要求される。2 つ以上の認証要素も求められる。使用することができるトークンは、「ソフト」暗号化トークン、「ハード」暗号化トークン、および「ワンタイムパスワード」デバイストークンの 3 種類である。

認証では、認証要求者がセキュアな認証プロトコルを通じて、認証要求者本人がトークンを管理していることを証明する必要がある。また、最初にパスワードや生体

認証情報を使用してトークンのロックを解除する必要がある。あるいは、セキュアな認証プロトコルのなかでパスワードを使用し、2 要素による認証を確立しなければならない場合もある。認証用の長期共有秘密情報を使用する場合、認証要求者、およびクレデンシャルサービスプロバイダ（CSP）が直接運営する検証者以外にその情報が開示されることは決してない。ただし、セッションの（一時的な）共有秘密情報は、CSP によって独立した検証者に対して提供される場合がある。承認された暗号化技法がすべての操作で使用される。認証の成功の結果として発行される認証要求者に関するアサーションは、それに依拠する当事者が（承認された手段を用いて）暗号学的な処理を行うことで認証するか、またはセキュアな認証プロトコルを通じて信頼のおける第三者から直接取得する。

レベル 4 – レベル 4 は、リモートネットワーク認証について実用上最大限の保証を提供することを目的とする。レベル 4 の認証では、暗号化プロトコルを通じて鍵の所持を証明することが基本となる。レベル 4 はレベル 3 に似ているが、「ハード」暗号化トークンのみが許可され、暗号モジュールの有効性確認に関する FIPS 140-2 の要求事項が厳しくなっているほか、認証後の重要なデータ転送をその認証プロセスに結び付けられた鍵を通じて認証しなければならない点がレベル 3 と異なる。トークンは、全体として FIPS 140-2 のレベル 2 以上で有効性が確認されているハードウェア暗号モジュールとし、少なくとも FIPS 140-2 のレベル 3 の物理セキュリティを備えたものとする。容易に複製できない物理トークンを要求することにより、また、FIPS 140-2 ではレベル 2 以上のオペレータ認証が要求されるため、このレベルでは適切な 2 要素によるリモート認証が保証される。

レベル 4 では、すべての当事者、および当事者間でのすべての機密データの転送について、強力な暗号認証が求められる。公開鍵または対称鍵のどちらの技術も利用できる。認証では、認証要求者がセキュアな認証プロトコルを通じて、認証要求者本人がトークンを管理していることを証明する必要がある。プロトコルに対する、盗聴、リプレイ攻撃、オンライン推測攻撃、検証者になりすます攻撃（Verifier impersonation attack）、中間者攻撃などの脅威が阻止される。認証用の長期共有秘密情報を使用する場合、認証要求者、およびクレデンシャルサービスプロバイダ（CSP）が直接運用する検証者以外にその情報が開示されることは決してない。ただし、セッションの（一時的な）共有秘密情報は、CSP から独立した検証者に提供される場合がある。承認された強力な暗号化技法がすべての操作で使用される。機密データの転送はすべて、認証プロセスに結び付けられた鍵を通じて、暗号による手段で認証される。

目次

1. 目的

本文書は、政府機関において電子認証を実装する際の技術的な指針を提供するものである。

2. 作成機関

本文書は、NIST が、Federal Information Security Management Act of 2002 (2002 年施行の連邦情報セキュリティマネジメント法、以下、FISMA と称す)に基づく法的責務を果たす一環として作成したものである。

NIST は、政府機関のすべての業務と資産に十分な情報セキュリティを提供するための標準とガイドライン(最小限の要求事項を含む)を作成する責任を負うが、このような標準およびガイドラインは国家安全保障にかかわるシステムには適用されない。このガイドラインは、行政管理予算局(Office of Management and Budget、以下、OMB と称す)の通達(Circular)A-130 の第 8b(3)項「政府機関の情報システムの保護(Securing Agency Information Systems)」の要求事項と一致しており、これは A-130 の付録 IV「重要部門の分析(Analysis of Key Sections)」で分析されているとおりである。補足情報は、A-130 の付録 III に記載されている。

このガイドラインは連邦政府機関が使用する目的で作成されている。非政府組織が自由意志で使用することもでき、著作権の制約はない(出自を明らかにする場合は NIST とする)。(翻訳者注:著作権に関するこの記述は、SP800-63 の英語の原文のことを言っており、日本語へ翻訳した本書の著作権は、独立行政法人情報処理推進機構および NRI セキュアテクノロジーズ株式会社に帰属する)。

本文書におけるいっさいは、商務長官が法的権威に基づき連邦政府機関に対して義務付けた拘束力を有する標準およびガイドラインを否定するものではない。また、これらのガイドラインは、商務長官、行政管理予算局長、または他のすべての連邦政府当局者の既存の権威を変更したり、これらに取って代わったりするものと解釈してはならない。

3. はじめに

電子認証は、電子的な手段によって情報システムに提示されるユーザ身元識別情報の信用を確立するプロセスである。このプロセスにおいて、ネットワーク経由で個人をリモートより認証する必要がある場合、電子認証には技術的に困難な課題が伴う。本文書は、連邦政府機関の職員が連邦の IT システムに対して各自の身元をリモートで証明できるようにするための、技術的な指針を提供するものである。

本技術指針はOMBのガイダンスである『*E-Authentication Guidance for Federal Agencies*』[OMB 04-04]を補足するものである。このOMBガイダンスでは、認証エラーとクレデンシャルの誤用によって生じる結果に応じた、レベル 1～4 の 4 つの保証レベルを定義している。レベル 1 は最低の保証レベルであり、レベル 4 は最高の保証レベルである。このガイダンスでは、認証エラーによって生じる可能性が高い結果に応じて、必要となる認証保証レベルを定めている。認証エラーによって生じる結果が深刻であるほど、必要となる保証レベルが高くなる。また、このOMBガイダンスでは、具体的な電子的トランザクション

やシステムに必要な電子認証の保証レベルを決定するための基準を提供している。この基準は、リスクとそれらが発生する可能性に基づく。

本文書では、次の分野における 4 つの保証レベルのそれぞれについて具体的な技術的要求事項を提示する。

- トークン。身元を証明するもの（通常は暗号鍵またはパスワード）。
- 身元識別情報の検証。身元識別情報をトークンに結び付けるクレデンシャルの登録と提供。
- リモート認証メカニズム。すなわち、認証要求者が実際に加入者本人であることを証明するために用いられる、クレデンシャル、トークン、および認証プロトコルの組み合わせ。
- アサーションメカニズム。リモート認証の結果を第三者に伝えるために用いられる。

全体の認証保証レベルは、上記の 4 つの分野のなかで達成される保証レベルのうち、最も低いレベルによって決まる。

本技術指針は、人間のユーザが、連邦政府機関の IT システムに対してネットワーク経由でリモートから行う電子認証を対象とする。建物への立ち入りなど、物理的にその場にいる人物の認証は対象外である。ただし、リモートで使用するクレデンシャルやトークンによっては、ローカルでの認証にも使用される場合もある。本技術指針では、多くの場合、認証プロトコルに関与する連邦政府の IT システムやサービスプロバイダを、加入者に対して認証するという要求事項を設けている。しかし、ルータ間など、マシン間での認証については具体的には取り上げていない。また、マシンやサーバが人を対象とした電子認証プロトコルとの関連で使われる場合に、認証のクレデンシャルやトークンをそれらのマシンやサーバに発行するための具体的な要求事項も設けていない。

本文書の論理的な枠組みは、個人が登録され、身元識別情報の検証プロセスを経ることで、個人の身元識別情報がトークンと呼ばれる認証用の秘密情報に結び付けられる、というものである。以後、その個人は、認証プロトコルのなかでトークンを使用して公開のネットワーク経由でシステムやアプリケーションに対してリモートで認証される。認証プロトコルでは、秘密情報が各種の攻撃による危殆化から保護される方法によって、個人が検証者に対して秘密のトークンを所持していること、またはそれを知っていることを示すことができる。認証の保証レベルが高いほど、より強力な（秘密情報を推測しにくい）トークンの使用と、トークンへの攻撃に対するより優れた保護が求められる。本文書では、個人が特定の秘密情報を所持し管理していることを示すことによって機能する認証メカニズムのみを扱っている。

個人の私的な知識をテストすることによる認証（知識ベースの認証とも呼ばれる）が現実的な場合もある。知識ベースの認証では、情報はプライベートなものではあるが実際には秘密でないので、個人の身元識別情報の信用性を確立することが困難になるおそれがある。また、知識ベースの認証システムの複雑さや相互依存性は数値化が難しい。しかし、本文書では知識ベースの認証技法を登録の一部として含めている。

生体認証による方法は、建物に立ち入る際など、本人が物理的に認証が行われる場所にいる場合にその個人を認証する方法として広く使用されている。生体認証情報は、本文書で説明している従来型のリモート認証プロトコルにおける使用に適した秘密情報ではない。ローカル認証では、認証要求者が観察され、検証者によって管理されている取り込み装置を認証要求者が使用するため、生体認証情報の秘密は維持される必要がない。本文書では、従来型の認証トークンの「ロックの解除」と登録の否認防止に生体認証情報を使用することについて明示する。

NIST では知識ベースの認証と生体認証の両方について引き続き調査を行っており、ネットワーク経由での個人のリモート認証にそれらの認証方式を使用することに関して追加の指針を発行する可能性もある。

本文書では、身元をリモートで認証するための最低限の技術的要求事項を明らかにしている。政府機関は、各自のリスク分析に応じ、特定の状況において追加措置が適切であると判断することもできる。特に、プライバシに関わる義務および法的なリスクのために、追加の認証手段やそのほかのプロセス保護手段が適切であると判断することができる。政府機関において電子認証のプロセスやシステムを開発する際には、『*OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*』[OMB 03-22]を参照すること。法的リスクの詳細については、『*Guide to Federal Agencies on Implementing Electronic Processes*』を参照のこと。特に、証明と否認防止の法的標準を満たす必要性に関連する法的リスクについては、[DOJ 2000]を参照のこと。

4. 用語の定義と略語

能動型攻撃 （Active Attack）	認証プロトコルに対する攻撃で、攻撃者が認証要求者または検証者にデータを送信する。能動型攻撃の例として、中間者攻撃、なりすまし、セッションハイジャックなどがある。
記録上の住所 （Address of Record）	特定の個人が見つかる公の場所。記録上の住所には、必ず個人の居住場所が含まれ、個人の郵送先住所が含まれていることもある。ひじょうに限られた状況で、個人の居住する住所が利用できない場合に、軍事郵便局私書箱番号、海軍郵便局私書箱番号（いずれも米国）、あるいは、近親者または別の連絡先を使用することができる場合がある。
攻撃（Attack）	加入者のトークンを取得する試み。または、検証者をだまし、権限のない個人が認証要求者のトークンを所持していると信じ込ませる試み。
攻撃者（Attacker）	認証要求者や検証者ではないのに、認証要求者として認証プロトコルの実行を成功させようとする人物。
承認済み（Approved）	FIPS による認可、または NIST による推奨を受けたこと。1) FIPS または NIST の推奨文書で規定されたか、2) FIPS または NIST の推奨文書で採用された、アルゴリズムまたは技法。承認された暗号化アルゴリズムは、FIPS 140-2 のもとで有効性が確認された暗号モジュール内に実装されなければならない。有効性確認の詳細と、FIPS 140-2 のもとで有効性が確認された暗号モジュールの一覧については、http://csrc.nist.gov/cryptval/を参照のこと。
アサーション （Assertion）	検証者から、その検証者に依拠する当事者に対して送られる、加入者に関する身元識別情報を収めた表明。アサーションには検証済みの属性が含まれることがある。アサーションは、ディジタル署名されたオブジェクトであったり、セキュアなプロトコルを通じて信頼できる情報源から取得できたりする。
非対称鍵 （Asymmetric keys）	公開鍵とプライベート鍵という、対で使用される鍵。これらは、暗号化、復号、署名の生成、署名の検証などの補完的な処理の実行に使用される。
認証（Authentication）	ユーザの身元識別情報に関する信用を確立するプロセス。
認証プロトコル （Authentication protocol）	認証要求者をリモートで認証するためにトークンの所持を確認する、厳密に規定されたメッセージ交換プロセス。認証プロトコルによっては暗号鍵を生成するものもある。暗号鍵はセッション全体を保護するのに使用され、セッション中に転送されるデータが暗号による手段で保護される。
信ぴょう性 （Authenticity）	データがしかるべき発生源から発生したものであることを示す性質。
ビット（Bit）	2 進数の 1 桁。0 または 1。
生体認証情報 （Biometric）	個人の識別に使用することができる可能性のある、生理学的な属性（指紋など）の画像またはテンプレート。本文書では、認証トークンのロックの解除および登録の否認防止に、生体認証を使用することがある。

認証局（Certification Authority、CA）	公開鍵証明書の発行および失効を行う、信頼のおける機関。
証明書失効リスト（Certificate Revocation List、CRL）	認証局によって作成されディジタル署名されたあとで失効した公開鍵証明書のリスト。[RFC 3280]を参照のこと。
challenge-response プロトコル (Challenge-response protocol)	認証プロトコルの一種。検証者は認証要求者に challenge（通常は乱数値または一時的な使い捨ての値）を送信し、認証要求者は共有の秘密をその challenge と組み合わせることで（challenge と秘密を組み合わせてハッシュ処理することが多い）response を生成して、その response を検証者に送信する。検証者は共有の秘密を知っており、独自に response を算出して、認証要求者が生成した response と比較することができる。両者が同じであれば、認証要求者の認証は成功したとみなされる。共有の秘密が暗号鍵の場合、この種のプロトコルは一般に盗聴者に対して安全である。共有の秘密がパスワードの場合、盗聴者はパスワードそのものを直接傍受することはないが、オフラインでのパスワード推測攻撃によってパスワードを知ることができる場合がある。
認証要求者（Claimant）	認証プロトコルを使用して身元を証明する当事者。
クレデンシャル（Credential）	身元識別情報（および場合によってはそのほかの属性）と、特定の人物が所持し管理しているトークンとを公的に結び付けるオブジェクト。
クレデンシャルサービスプロバイダ（Credentials Service Provider、CSP）	加入者トークンの発行または登録を行い、電子的クレデンシャルを加入者に発行する、信頼のおける機関。CSP が、登録機関と、登録機関が運営する検証者を兼務することがある。CSP は、独立の第三者機関である場合がある。また、独自に使用するクレデンシャルを発行する場合がある。
暗号鍵（Cryptographic key）	暗号処理（復号、暗号化、署名の生成、署名の検証など）の制御に使用される値。本文書で扱う暗号鍵は、少なくとも 80 ビットの保護を提供する必要がある。つまり、たとえ情報が認証を通じて盗聴者に漏えいしたとしても、未知の鍵の発見やメッセージの復号が、80 ビットの乱数を推測する難しさと同等である必要がある。 「非対称鍵（Asymmetric keys)」、「対称鍵(Symmetric key)」も参照のこと。
暗号化強度（Cryptographic strength）	暗号メカニズムの無効化に必要となると想定される演算回数を尺度とするものさし。本文書では、処理の無効化や復号の試みが、少なくとも 80 ビットブロック暗号の鍵を総当り検索によって見つけ出すのと同等の困難が伴う、つまり、少なくとも 2^{79}回の演算を必要とするような困難が伴うことを意味するものとしてこの用語を定義している。
暗号トークン（Cryptographic token）	暗号鍵を秘密情報とするトークン。
データの完全性（Data integrity）	データが権限のない第三者によって改ざんされていないことを示す性質。

ディジタル署名（Digital Signature）	プライベート鍵を使用して電子文書に電子的に署名する非対称鍵の操作。その署名の検証には、公開鍵を使用する。ディジタル署名により、認証と完全性の保護が実現する。
電子クレデンシャル（Electronic Credential）	認証において、身元識別情報や属性を加入者のトークンに結び付けるのに使用されるディジタル文書。本文書では、クレデンシャルとトークン（「トークン（Token）」を参照）を区別しているが、これらの用語を区別なく使用する文書もある。
エントロピー（Entropy）	攻撃者が秘密の値を特定するために直面する不確実性の量を測るものさし。通常、エントロピーはビットで表現される。詳細は「付録A」を参照のこと。
FIPS	Federal Information Processing Standard（連邦情報処理規格）
推測エントロピー（Guessing entropy）	システムで使用されている平均的なパスワードを攻撃者が推測する難しさを測るものさし。本文書では、エントロピーをビットで表現する。パスワードの推測エントロピーがnビットならば、攻撃者が平均的なパスワードを推測する難しさは、nビットのランダムな数値を推測する難しさと同等である。攻撃者がパスワードの実際の度数分布を知っているものと仮定する。詳細は「付録A」を参照のこと。
ハッシュ関数（Hash function）	任意の長さのビット文字列を固定長のビット文字列に対応付ける関数。承認されたハッシュ関数は次の性質を満足する。 1.（一方向）あらかじめ指定された出力に対応する入力を計算によって求めるのが不可能であり、かつ、 2.（衝突への耐性）同じ出力に対応する 2 つの異なる入力を計算によって求めるのが極めて困難である。
HMAC	ハッシュベースのメッセージ認証コード（Hash-based Message Authentication Code）。ハッシュ関数を使用した対称鍵による認証方式。
身元識別情報（Identity）	個人のユニークな名前。個人の法的な名前は必ずしも一意とは限らないため、個人の身元識別情報には名前全体が一意となるように十分な補足情報（たとえば、住所、あるいは従業員番号や口座番号といったユニークな識別子など）を含める必要がある。
身元識別情報の検証（Identity proofing）	CSP および RA が個人を一意に識別できる十分な情報の有効性を検証するプロセス。
Kerberos	MIT において開発され、広く普及している認証プロトコル。「旧式」の Kerberos では、ユーザは鍵配布センタ（Key Distribution Center、KDC）と秘密パスワードを共有する。たとえば、ユーザ Alice が別のユーザ Bob と通信したい場合、Alice は KDC に対して本人認証を行って KDC から「チケット」を受け取り、そのチケットを使用して Bob との本人認証を行う。パスワードに基づく Kerberos 認証の場合、そのプロトコルは、ユーザから KDC への最初の交換を傍受した盗聴者によるオフライン辞書攻撃に対し脆弱であることが知られている。
中間者攻撃（Man-in-the-middle attack、MitM）	認証プロトコル実行に対する攻撃で、攻撃者が認証要求者と検証者のあいだに介入し、両者を往来するデータを横取りして改ざんする。
メッセージ認証コード	偶発的および意図的なデータ改ざんの両方を検出するために対称鍵

（Message Authentication Code、MAC）	を使用する、データの暗号チェックサム。
最小エントロピー（Min-entropy）	システムで最も一般的に使用されているパスワードを攻撃者が推測する難しさを測るものさし。本文書では、エントロピーをビットで表現する。パスワードの最小エントロピーがnビットならば、攻撃者が該当パスワードを持つユーザを見つけ出す難しさは、nビットのランダムな数値を推測する難しさと同等である。攻撃者が最も一般的に使用されている 1 つ以上のパスワードを知っているものと仮定する。詳細は「付録A」を参照のこと。
ネットワーク（Network）	公開の通信媒体。通常はインターネットを指し、認証要求者と他者とのあいだでメッセージを転送するのに使用される。特に明記しない限り、ネットワークのセキュリティについていかなる仮定もしないものとする。つまり、ネットワークは公開であり、当事者（認証要求者、検証者、CSP、または検証結果の利用者）間の任意の地点において能動型攻撃（なりすまし、中間者攻撃、セッションハイジャックなど）および受動型攻撃（盗聴など）を受ける可能性があるものとする。
ノンス（一時的な使い捨ての値）（Nonce）	セキュリティプロトコルで使用され、同じ鍵で繰り返されることが決してない値。たとえば、challenge-response 認証プロトコルで使用される challenge は通常、認証鍵が変更されるか、リプレイ攻撃のおそれがある限り、繰り返されてはならない。ノンスを challenge として使用するという要求事項は、ランダムな challenge を使用することとは異なる。これは、ノンスは必ずしも予測不可能とは限らないからである。
オフライン攻撃（Off-line attack）	攻撃者がなんらかのデータを入手し、それを自身が任意に選んだシステムのなかで分析する攻撃。通常、攻撃者は実行されている認証プロトコルを盗聴するか、システムに侵入してセキュリティファイルを盗み出すことによってデータを入手する。
オンライン攻撃（On-line attack）	認証プロトコルに対する攻撃で、攻撃者は正式な検証者に対して認証要求者になりすますか、認証チャネルを能動的に改ざんする。認証アクセスを実現すること、または認証の秘密情報を入手することが、この攻撃の目的として考えられる。
オンライン証明書状態プロトコル（On-Line Certificate Status Protocol、OCSP）	公開鍵証明書の状態を知るのに使用されるオンラインプロトコル。[RFC 2560]を参照のこと。
受動型攻撃（Passive attack）	認証プロトコルに対する攻撃で、攻撃者は、認証要求者と検証者のあいだをネットワーク経由で往来するデータを傍受する（つまり、盗聴する）が、データの改ざんは行わない。
パスワード（Password）	認証要求者が自身の身元を証明するために記憶し使用する秘密情報。通常、パスワードは文字列である。
トークンの所持と管理（Possession and control of a token）	認証プロトコルにおいてトークンを活性化し使用することができること。
PIN（Personal	10 進数のみで構成されるパスワード。

Identification Number）	
実施規程（Practice Statement）	認証局（RA、CSP、検証者など）が従っている公式の実施規程。一般的には、身元識別情報の登録と検証、クレデンシャルの発行、および認証要求者の認証に必要な具体的な手順を規定している。
プライベート鍵（Private key）	非対称鍵ペアのうちの秘密の部分で、通常はデータのディジタル署名または復号に使用される。
所持証明プロトコル（Proof of Possession（PoP）protocol）	認証要求者が検証者に対し、自身がトークン（鍵やパスワードなど）を所持し管理していることを証明するためのプロトコル。
プロトコル実行（Protocol run）	定義済みの認証プロトコルにおける、認証要求者と検証者のあいだのある特定のメッセージ交換。プロトコル実行の結果、認証要求者が認証される（または認証が失敗する）。
公開鍵（Public key）	非対称鍵ペアのうちの公開の部分で、通常は署名の検証やデータの暗号化に使用される。
公開鍵証明書（Public key certificate）	認証局によって発行され、認証局のプライベート鍵を使用してディジタル署名されたディジタル文書。公開鍵証明書によって、加入者の名前が公開鍵に結び付けられる。公開鍵証明書は、当該証明書に示されている加入者が、プライベート鍵を独占的に管理しアクセスできることを示す。[RFC 3280]も参照のこと。
仮名（Pseudonym）	加入者によって選択され、身元識別情報の検証によって意味のあるものとして確認されない加入者名。
登録（Registration）	当事者が CSP の加入者となるために申請を行い、RA が CSP に代わってその当事者の身元を確認するまでのプロセス。
登録機関（Registration Authority、RA）	CSP に対し加入者の身元を証明し、その保証を行う、信頼のおける機関。RA は CSP の一部である場合がある。または、CSP から独立しているものの、1 つ以上の CSP と連携することもある。
検証結果の利用者（Relying party）	通常、トランザクションの処理や、情報またはシステムへのアクセス許可の付与を目的として、加入者のクレデンシャルを利用するエンティティ。
salt	暗号化処理のなかで使用される、秘密でない値。通常、特定の計算結果が攻撃者によって再利用されないようにするために使う。
SAML（Security Assertion Markup Language、セキュリティアサーションマークアップ言語）	XML マークアップ言語を使用してセキュリティアサーションをエンコードするための仕様。http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security を参照のこと。
共有の秘密（Shared secret）	認証の中で使用され、認証要求者と検証者が知っている秘密情報。
主体（Subject）	身元識別情報が特定のクレデンシャルに結び付けられている人物。
加入者（Subscriber）	CSP からクレデンシャルまたはトークンを受け取り、認証プロトコルにおいて認証要求者となる人物。
対称鍵（Symmetric key）	暗号処理とその逆の処理（暗号化と復号、メッセージ認証コードの作成とコードの検証など）の両方に使用される暗号鍵。

トークン（Token）	認証要求者が所持し管理しているなんらかの情報（通常は鍵またはパスワード）。認証要求者の身元識別情報の認証に使用される。
TLS（Transport Layer Security、トランスポートレイヤセキュリティ）	ブラウザやWebサーバで広く実装されている認証およびセキュリティプロトコル。TLSは[RFC 2246]および[RFC 3546]により規定されている。TLSは従来のSSL（Secure Socket Layer、セキュアソケットレイヤ）プロトコルに似ており、実質的にはSSLバージョン 3.1 と同じである。
トンネル通過パスワードプロトコル（Tunneled password protocol）	保護されたチャネルを通じてパスワードが送信されるプロトコル。たとえば、TLS プロトコルでは多くの場合、検証者の公開鍵証明書を使用して次のことを行う。(1)認証要求者に対して検証者を認証する、(2)検証者と認証要求者とのあいだに暗号化されたセッションを確立する、および(3)認証要求者のパスワードを検証者に送信する。暗号化された TLS セッションにより、認証要求者のパスワードが盗聴から保護される。
検証済みの名前（Verified Name）	身元識別情報の検証による確認が済んだ加入者名。
検証者（Verifier）	認証要求者がトークンを所持していることを認証プロトコルを使用して確認することにより、認証要求者の身元識別情報を検証するエンティティ。この目的のために、検証者はトークンと身元識別情報を結び付けるクレデンシャルの有効性を検証し、それらの状態を確認しなければならないこともある。
検証者になりすます攻撃（Verifier impersonation attack）	認証プロトコルのなかで攻撃者が検証者になりすます攻撃。通常はパスワードの入手が目的である。

5. 電子認証のモデル

[OMB 04-04]によれば、電子認証とは、電子的な手段によって情報システムに提示されるユーザ身元識別情報の信用を確立するプロセスである。システムは認証済みの身元識別情報を使用して、その個人が電子的トランザクションを実行することを認可されているかどうかを判断することができる。ほとんどの場合、認証とトランザクションはインターネットなどの公開のネットワークを経由して行われる。しかし、場合によっては、ネットワークへのアクセスが制限され、アクセス制御の決定においてそのことが考慮されることがある。

電子認証では、まず「*登録*」が行われる。「*申請者*」は「*登録機関(RA)*」に申請を行って「*クレデンシャルサービスプロバイダ(CSP)*」の「*加入者*」となる。加入者には、「*トークン*」と呼ばれる秘密情報と、RA による検証が済んだ名前(および、場合によってはそのほかの属性)にトークンを結び付ける「*クレデンシャル*」が発行される。あるいは、加入者がトークンおよびクレデンシャルを登録する。発行又は登録されたトークンとクレデンシャルは、以降の認証手続きで使用することができる。

加入者の名前は「*検証済みの名前*」または「*仮名*」のいずれかである。検証済みの名前は実在する人物の身元識別情報に関連付けられる。申請者がクレデンシャルを受け取るためには、あるいは検証済みの名前に関連付けられたトークンを登録するためには、身元識別情報が実在の身元識別情報であり、かつその身元識別情報を使用する資格を持つ人物であることを証明する必要がある。このプロセスのことを「*身元識別情報の検証*」と呼ぶ。身元識別情報の検証は、加入者を CSP に登録する RA が実施する。レベル 1 では、名前は検証されないため、名前は常に仮名であるとみなされる。レベル 2 では、クレデンシャルおよびアサーションにおいて、名前が検証済みの名前か仮名かを示す必要がある。この情報は、「*検証結果の利用者*」(名前やそのほかの認証済みの属性に依拠する当事者)によるアクセス制御または認可に関わる決定に役立てられる。レベル 3 および 4 では検証済みの名前のみ使用することができる。

本指針では、認証の対象となる当事者を「*認証要求者*」と呼び、その身元識別情報を検証する当事者を「*検証者*」と呼ぶ。「*認証要求者*」が「*検証者*」に対し、トークンを所持し管理していることをオンライン認証のなかで「*認証プロトコル*」を通じて証明できると、検証者は認証要求者が加入者であることを確認できる。検証者は、加入者の身元識別情報に関するアサーションを検証結果の利用者に渡す。このアサーションには、加入者に関する身元識別情報が含まれている。たとえば、加入者名や、登録時に割り当てられた識別子など、登録プロセスにおいて検証された加入者属性が含まれている(これらは CSP のポリシーやアプリケーションのニーズよって異なる)。検証者が検証結果の利用者を兼ねている場合には、アサーションが暗黙に行われることがある。また、認証要求者が提示するクレデンシャル(公開鍵証明書など)に加入者の身元識別情報を組み込むことができる。検証結果の利用者は、検証者または CSP によって提供される認証済みの情報を使用して、アクセス制御または認可に関する判断を行うことができる。

認証では、単に身元識別情報または場合によっては検証済みの個人的な属性(たとえば、加入者がアメリカ合衆国の市民である、特定の大学の学生である、あるいは政府機関や他の組織から特定の番号やコードを割り当てられているなど)を証明するだけである。そ

の身元識別情報によって認可される行為やアクセス権限は、認証では証明されず、別途決定される。検証結果の利用者（通常は政府機関）は、加入者の認証済みの身元識別情報やそのほかの要素を使用して、アクセス制御または認可の決定を下す。多くの場合、認証のプロセスおよびサービスは多数のアプリケーションや政府機関によって共有されるが、アクセス許可を付与したり、アプリケーションの個々の要求事項に基づいてトランザクションを処理したりするのは、検証結果の利用者である個々の政府機関やアプリケーションである。本指針では、認可ではなく認証のプロセスに関する技術的な推奨事項について説明する。

まとめると、まず、個人の申請者が RA に対して申請を行う。RA ではその申請者について身元識別情報の検証を行う。身元識別情報の検証結果に問題がなければ、申請者は RA と連携している CSP の加入者となり、クレデンシャルと秘密のトークンが加入者について登録される。加入者は、トランザクションを実行するための認証を必要とするときに、検証者に対する認証要求者となる。認証要求者は検証者に対し、認証プロトコルを通じて、自身がトークンを管理していることを証明する。検証者が検証結果の利用者（依拠アプリケーション）とは別に存在する場合、検証者は認証要求者に関するアサーションを検証結果の利用者に提供する。検証結果の利用者はアサーション内の情報を使用して、アクセス制御または認可の決定を下す。重要なトランザクションの場合、検証結果の利用者は、認証に使用された加入者の身元識別情報と 1 つ以上のクレデンシャルを、関連するトランザクションデータと一緒にログに記録することもできる。

5.1. 加入者、RA、およびCSP

電子認証の概念モデルでは、認証プロトコルにおける認証要求者はいずれかの CSP の加入者である。申請者は、ある時点で RA に登録を行い、RA は、通常は書面のクレデンシャルの提示とデータベースの記録を通じて、申請者の身元識別情報を検証する。このプロセスのことを身元識別情報の検証と呼ぶ。RA はさらに、CSP に対して申請者の身元識別情報（およびそのほかの検証済みの属性）の保証を行う。以降、申請者は CSP の加入者となる。

CSP は、各加入者と、その加入者に対して発行され関連付けられたトークンおよびクレデンシャルについて、それらを一意に識別するためのメカニズムを確立する。CSP は加入者に対して、認証プロトコルで使用されるトークンを登録するか、または付与する。そして、必要に応じてクレデンシャルを発行し、そのトークンを身元識別情報に結び付けるか、または身元識別情報をほかのなんらかの有用な検証済み属性に結び付ける。登録時に、トークンと一緒に電子的なクレデンシャルを加入者に付与することもできる。あるいは、必要に応じてあとでクレデンシャルを生成することもできる。加入者は自分のトークンを維持管理する義務と、CSP に対する責任を負う。登録されている記録の復元が可能なように、CSP では加入者ごとに登録されている記録を維持する。

RA と CSP は常に連携している。最も簡単で、おそらく最も一般的なのは、RA と CSP が同一のエンティティの異なる機能となっている場合である。しかし、RA が、加入者を独立の CSP または複数の異なる CSP に登録させる企業や組織の一部である場合もある。したがって、CSP が RA を統合している場合や、CSP が複数の独立した RA と連携している場合がある。同様に、RA が複数の異なる CSP と連携している場合もある。

セクション 7 で、身元識別情報の検証と登録のプロセスに関する推奨事項について説明する。

5.2. トークン

一般に、トークンとは、認証要求者が所持し管理する何かであり、認証要求者の身元識別情報の認証に使用することができる。電子認証では、認証要求者はネットワーク経由でシステムやアプリケーションに対し認証を行う。したがって、電子認証に使用されるトークンは秘密情報であり、トークンを保護する必要がある。たとえば、暗号鍵として使用するトークンを、パスワードを使用して暗号化することによって保護できる。不正な第三者が暗号化された鍵を盗み出しても、パスワードを知らなければトークンを利用することはできない。

認証システムは、組み入れている要素の数に応じて分類されることが多い。一般に次の 3 つが認証の基本要素とみなされている。

- 知っていること（パスワードなど）
- 持っているもの（身分証明書や暗号鍵など）
- 持っている特徴（声紋やそのほかの生体認証情報など）

これら 3 つの要素がすべて組み込まれた認証システムは、1 つまたは 2 つの要素しか組み込まれていないシステムよりも強固である。複数の要素が検証者に提示されるようにシステムを実装したり、検証者に提示される秘密情報をなんらかの要素を使用して保護したりできる。たとえば、暗号鍵を保持するハードウェアデバイスを考える。この場合、パスワードによって鍵を活性化することが考えられる。または、ハードウェアデバイスに生体情報取り込み装置が組み込まれていて、生体認証情報を使用して鍵を活性化することも考えられる。このようなデバイスは実質的に 2 つの要素による認証を提供するものとみなされるが、検証者と認証要求者間での実際の認証プロトコルでは鍵の所持が証明されるだけである。

秘密情報は「*公開鍵ペア*（非対称鍵）」か「*共有秘密情報*」をベースとするものが多い。公開鍵ペアは、「*公開鍵*」と、それに対応するプライベート鍵で構成される。「*プライベート鍵*」は認証要求者がトークンとして使用する。検証者はなんらかのクレデンシャル（通常は「*公開鍵証明書*」）を通じて認証要求者の公開鍵を入手し、認証プロトコルを使用してその公開鍵に対応するプライベート鍵トークンを認証要求者が管理していることを証明することで（「*所持の証明*」）、認証要求者の身元識別情報を検証する。

共有秘密情報は「*対称鍵*」かパスワードのどちらかである。プロトコルという面から見れば、共有秘密情報はどれも公開鍵ペアと似たようなものであり、同様の認証プロトコルで使用することができる。ただし、パスワードは脳に記憶しておくことが多いため、認証要求者が持っているものというよりは、認証要求者が知っていることに該当する。パスワードは脳に記憶されるため、その値の範囲は通常は暗号鍵よりも狭い。そして、多くのプロトコルにおいては暗号鍵に対しては効果のないネットワーク攻撃に対して脆弱である。そのうえ、パスワードを（通常はキーボードを通じて）システムに入力することは、ひじょうに単純なキーロガーまたは「ショルダーサーフィン（人の肩越しにのぞき見すること）」による攻撃の可能

性を与えることになる。したがって、鍵とパスワードは認証に関していくぶん異なる性質を示す（持っているものというよりは、知っていることに該当する）。パスワードのほうがネットワーク攻撃に対する耐性が弱いことが多い。しかし、公開鍵ペアまたは共有秘密情報のどちらを使用する場合でも、加入者は自分のトークンを他人に使用されないように維持管理する義務を負う。これは、トークンを所持し管理しているということによって、加入者の身元識別情報の認証が行われるからである。

生体認証情報はユニークで個人的な属性であり、個人の識別に使用することができる。これには、顔写真、指紋、DNA、虹彩や網膜のスキャン、声紋など多数ある。本文書では、生体認証情報を登録プロセスで使用し、実際に登録を済ませた加入者があとで登録を否認するのを防止したり、虚偽登録を試みる人物の特定に役立てたり、トークンのロックを解除することに使われる。本文書では生体認証情報をトークンとして直接使用することはない。

セクション 6 で規定しているように、本指針では 4 種類の認証要求者トークンを扱う。これらは、ハードトークン、ソフトトークン、ワンタイムパスワードデバイストークン、およびパスワードトークンである。

5.3. 電子的クレデンシャル

書面によるクレデンシャルは、個人やそのほかのエンティティ（クレデンシャルの主体と呼ばれる）の身元識別情報やそのほかの属性を立証する文書である。書面による一般的なクレデンシャルには、旅券、出生証明書、運転免許証、社員証などがある。クレデンシャルそのものはさまざまな方法で認証される。従来は、署名や捺印、特殊な用紙とインク、高品質の刻印などが用いられていたが、現在では、ホログラムをはじめ、より複雑なメカニズムが用いられており、クレデンシャルを認識しやすくするとともに、複製や偽造をしにくくしている。場合によっては、クレデンシャルを所持しているだけで、その物理的な所持者が確かにクレデンシャルの主体であることが十分に立証されることもある。より一般的には、主体に関する記述や写真、手書きの署名といった、生体認証情報がクレデンシャルに含まれている。これらを使用することで、クレデンシャルの所持者が確かにクレデンシャルの主体であることを認証できる。このような書面によるクレデンシャルが対面によって直接提示される場合は、それらのクレデンシャルに含まれている生体認証情報を検査することで、クレデンシャルの物理的な所持者がクレデンシャルの主体であることを確定できる。

電子的な身元識別情報のクレデンシャルは、名前と、場合によってはそれ以外の属性を、トークンに結び付ける。本文書では特定の種類の電子的クレデンシャルについては規定していない。こんにち使用されている電子的クレデンシャルにはさまざまな種類があり、新しい種類のクレデンシャルが次々と作成されている。最低限、クレデンシャルには、そのクレデンシャルに対応する登録の記録を復元できるようにするための身元識別情報と、加入者に対応する名前が含まれる。いずれの場合も、クレデンシャル内の発行者と身元識別情報を使用し、そのクレデンシャルに基づく登録の記録を復元できなければならない。電子的クレデンシャルには、汎用のものと、特定の検証者を対象としたものがある。一般的な種類のクレデンシャルの例として次のものがある。

- X.509 公開鍵身元識別情報証明書。身元識別情報を公開鍵に結び付ける。
- X.509 属性証明書。身元識別情報または公開鍵をなんらかの属性に結び付ける。

- Kerberos チケット。所持者をなんらかの属性や特権に結び付ける、暗号化されたメッセージである。

電子的クレデンシャルはデータとしてディレクトリやデータベースに格納することもできる。これらのクレデンシャルがディジタル署名されたオブジェクト（X.509 証明書など）であれば、完全性を検証することもできる。この場合、ディレクトリやデータベースが提供するデータは自己認証されたものであるので、ディレクトリやデータベースは信頼できないエンティティであるかもしれない。あるいは、ディレクトリサーバやデータベースサーバが自身を検証結果の利用者や検証者に対して認証する、信頼のおけるエンティティであるかもしれない。ディレクトリサーバやデータベースサーバが信頼できる場合、署名のないクレデンシャルは単に署名のないデータとして格納することもできる。

5.4. 検証者

認証が行われるすべてのオンライントランザクションにおいて、検証者は、認証要求者が自身の身元を証明するトークンを所持し管理していることを検証する必要がある。認証要求者は、トークンと認証プロトコルを使用することによって、自身の身元を検証者に証明する。このことを「*所持の証明（Proof of Possession、PoP）*」と呼ぶ。PoP プロトコルの多くは、認証プロトコル実行の前に対象トークンについて何も知らない検証者が、実行後もトークンについて何も学習することがないように設計されている。検証者と CSP が同一エンティティである場合もあれば、検証者と検証結果の利用者が同一エンティティである場合もある。あるいは、3 者とも別々のエンティティである場合もある。検証者がトークンの登録を行った CSP と同一のエンティティを構成するのでない限り、検証者が共有秘密情報を知ることは好ましくない。検証者と検証結果の利用者が別々のエンティティである場合には、検証者は認証プロトコルの結果を検証結果の利用者に伝達する必要がある。この結果を伝達するために検証者が作成するオブジェクトのことを、アサーションと呼ぶ。

5.5. アサーション

アサーションは、認証要求者に関する情報や、電子認証プロセスに関する情報を、検証者から検証結果の利用者に渡すために使用することができる。アサーションには少なくとも認証要求者の名前のほか、登録記録の復元を可能にする識別情報が含まれる。検証結果の利用者は、アサーションの提供元、作成時間、および認証要求者に関連付けられている属性に基づいて、アサーションを信頼する。

アサーションの例として次のものがある。

- SAML アサーション。セキュリティアサーションの記述を目的としたマークアップ言語を使用して指定される。検証者は SAML アサーションを使用して、検証結果の利用者に対して認証要求者の識別情報に関する表明ができる。SAML アサーションはディジタル署名される場合もある。
- クッキー。Webブラウザの記憶域に格納される文字列。Webブラウザにクッキーを置いたサーバと同じインターネットドメイン内にあるWebサイトは、そのクッキーを利

用できる。クッキーはさまざまな目的に利用される。アサーションそのものである場合もあれば、アサーションへの参照を含んでいる場合もある[1]。

アサーションはディレクトリオブジェクトまたはデータベースオブジェクトとして格納することもできる。アサーションがディジタル署名されたオブジェクト（署名付きの SAML アサーションなど）である場合は、その完全性が検証されているかもしれない。あるいは、ディレクトリサーバまたはデータベースサーバが、信頼のおける、認証されたエンティティである場合もある。サーバが信頼されている場合、署名のないアサーションをサーバの信頼性に基づいて受容することもできる。

5.6. 検証結果の利用者

検証結果の利用者は、なんらかのトランザクションを目的として、加入者の身元識別情報または属性の保証を得るために、オンライン認証の結果を利用する。検証者と検証結果の利用者は、同一エンティティの場合もあれば、別々のエンティティである場合もある。
別々のエンティティである場合、検証結果の利用者は通常、検証者からアサーションを受け取る。検証結果の利用者は、アサーションが検証結果の利用者が信頼している検証者から送られたものであることを確認する。また、検証結果の利用者は個人の属性や有効期限など、アサーション内のそのほかの情報も処理する。

[1] 政府機関はクッキーを実装する場合には、特定の要求事項に従う必要がある。詳細については、OMB Memorandum M-03-22、『OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002』（http://www.whitehouse.gov/omb/memoranda/m03-22.html）を参照のこと。

6. トークン

本指針では、電子認証に利用できる 4 種類の認証要求者のトークンを扱う。どの種類のトークンも 1 つ以上の認証要素（知っていること、持っているもの、持っている特徴）が組み込まれている。高いレベルの保証を提供するトークンには複数の要素が組み込まれている。この 4 種類のトークンは次の通りである。

- *ハードトークン*: 保護された暗号鍵を備えているハードウェアデバイス。デバイスを所持し鍵を管理していることを証明することで、認証が達成される。ハードトークンは次の条件を満たすものとする。
    - 認証鍵を活性化するために、パスワードまたは生体認証情報の入力を要求する。
    - 認証鍵を外部に出力する機能を持たない。
    - FIPS 140-2 への適合性が確認されている。
        - 全体としての適合性がレベル 2 以上であることが確認されている。
        - 物理セキュリティがレベル 3 以上である。

- *ソフトトークン*: 通常はディスクあるいはほかのなんらかの媒体に格納される暗号鍵。鍵を所持し管理していることを証明することで、認証が達成される。ソフトトークンの鍵は、活性化のためのなんらかのデータから派生した鍵を利用して暗号化されているものとする。通常、この活性化のためのデータは、対象ユーザだけが知っているパスワードである。したがって、トークンを活性化するにはパスワードが必要になる。ソフトトークンの場合、暗号モジュールは FIPS 140-2 のレベル 1 以上に適合していなければならない。また、ハードウェアデバイスかソフトウェアモジュールのどちらでもよい。認証のたびに、パスワードまたはそのほかの活性化データの入力を要求するものとし、暗号化されていない認証鍵のコピーは、認証が終わるたびに消去するものとする。

  一部の「可搬型ソリューション」によっては、サーバに鍵を格納し、必要に応じて加入者のシステムにダウンロードできるものがある。また、パスワードに基づいて生成される鍵要素を利用する可搬型ソリューションもある。これらの鍵要素は、分割署名の仕組みでの利用のためにサーバに格納される。このようなソリューションは、ソフトトークンとして条件を満足する場合がある。ただし、鍵のダウンロードと活性化のために加入者のパスワードまたはそのほかの活性化データを要求すること、鍵をダウンロードするためのプロトコルが盗聴や中間者攻撃を阻止すること、および、認証プロセスによって承認されたディジタル署名またはメッセージ認証コードが生成されることが条件となる。これらの可搬型ソリューションは通常、検証結果の利用者が通常の PKI ディジタル署名と認識するものを提示し、PKI の横断認証（cross-certification）の要求事項を満たすことを条件に、本文書においては認められる場合がある。この横断認証については、該当する可搬方式の実装を詳細に分析する必要がある。

- *ワンタイムパスワードデバイストークン*: 認証に使用する「ワンタイム（1 回限りの）」パスワードを生成する個人用のハードウェアデバイス。デバイスは、なんらかの組

み込みの入力パッド、組み込みの生体認証リーダ（指紋などを読み取るもの）、コンピュータとの直接のインタフェース（USB ポートなど）を備えている場合もあれば備えていない場合もある。パスワードは承認されたブロック暗号またはハッシュアルゴリズムを使用して生成されるものとし、個人用のハードウェアデバイスに格納されている対称鍵を、一時的な値と組み合わせることにより、ワンタイムパスワードを生成するものとする。一時的な値としては、日付と時刻、デバイス上で生成されるカウンタ、または検証者から送られた challenge（デバイスが入力機能を備えている場合）などが考えられる。通常、ワンタイムパスワードはデバイス上に表示され、パスワードとして手動で検証者に対して入力される（デバイスからコンピュータへの直接の電子的入力も許される）。ワンタイムパスワードは数分程度の有効期限を設けるものとする。ただし、有効期限は短いほどよい。

- *パスワードトークン*: 認証要求者が自分の身元を証明するために記憶し使用する秘密情報。通常、パスワードは文字列だが、システムによっては、加入者が記憶している複数の画像を使用し、ほかの同様の画像を一緒に提示して加入者に識別を求めるものがある。

6.1. トークンの脅威

攻撃者がトークンをコントロール下におくことができた場合、攻撃者はトークンの所有者になりすますことができる。トークンに対する脅威は、認証の 3 要素に対する攻撃に分類できる。

- 「*持っているもの*」が攻撃者の手によって所有者から盗み取られたり複製されたりする場合。たとえば、所有者のコンピュータへのアクセス権を獲得した攻撃者が、ソフトウェアトークンをコピーするかもしれない。ハードウェアトークンが盗まれたり複製されたりすることもある。
- 「*知っていること*」が攻撃者に知られる場合。攻撃者はパスワードや暗証番号を推測するかもしれない。トークンが共有の秘密情報である場合、攻撃者が CSP や検証者へのアクセス権を獲得して秘密の値を入手する可能性がある。これらの情報を入手するために、攻撃者が悪意のソフトウェア（キーロガーなど）をインストールすることもある。最後に、攻撃者は認証の試みによるネットワークトラフィックを対象にオフライン攻撃を仕掛けることで、秘密情報を突き止める可能性がある。
- 「*持っている特徴*」が複製される場合。攻撃者はトークン所有者の指紋のコピーを入手して、複製を作成するおそれがある。

このような脅威を軽減するための補助的な方策がいくつか存在する。

- 「*複数要素*」にすることで、攻撃を成功させるために越える必要のある敷居を高くすることができる。攻撃者が暗号トークンを盗み出し、かつ、パスワードも推測しなければならないとすれば、作業負担を過大なものにできる可能性がある。
- 「*物理的なセキュリティメカニズム*」を採用すれば、トークンが盗まれてもその複製を防止できる可能性がある。物理的なセキュリティメカニズムでは、改ざんの証拠、検出、および対応措置を提供することができる。
- 「*複雑なパスワード*」により、推測攻撃の成功率が下がる可能性がある。一般の辞書に載っている単語を使わない長いパスワードの使用を義務付けることで、攻撃者は考え得るあらゆるパスワードを試さざるを得なくなる可能性がある。

- 「*システムおよびネットワークのセキュリティ管理策*」を導入することで、攻撃者によるシステムへのアクセス権の獲得や悪意のソフトウェアのインストールを防止することができる可能性がある。

6.2. トークンのレベル

パスワード認証は実装が容易でユーザにも受け入れられやすい。そのため、パスワードによる認証のみに頼っているシステムが多い。この場合、偽装者はパスワードを入手するだけで身元を偽ることができる。そのうえ、人が無作為の長いパスワードを記憶する能力は限られているため、パスワードトークンは、推測や、よく使われるパスワードを集めた辞書、パスワードとして考えられるすべての可能性を試す単純な行為といった、さまざまな攻撃に対して脆弱であることが多い。パスワード認証プロトコルの種類は広範囲にわたるが、その脆弱性は大幅に異なり、パスワードメカニズムの多くは能動型および受動型のネットワーク攻撃に対して脆弱である。暗号パスワードプロトコルの中には、ほぼあらゆる直接的なネットワーク攻撃に耐えるものもあるが、現時点ではそのような技法は広く用いられておらず、すべてのパスワード認証メカニズムはキーロガーやパスワード入力時ののぞき見に対して脆弱である。また、経験上、ユーザは未知の第三者（要するに「詐欺師」）にパスワードを開示するように説得される「ソーシャルエンジニアリング」攻撃に対して脆弱である。

ハードトークンまたはソフトトークンを使用して身元を詐称するには、偽装者は 2 つの別々の情報が必要になる。すなわち、鍵（トークン）とパスワード、あるいは、トークンと生体認証情報をトークンに入力できることである。したがって、ハードトークンとソフトトークンはどちらも、パスワード単独で通常提供するものよりも高い保証が得られる。さらに、ハードトークンは物理的な実体であり、その盗難が所有者に気づかれる可能性は高いが、ソフトトークンはしばしば所有者が気づかないうちにコピーされるおそれがある。したがって、ハードトークンのほうがソフトトークンよりも高い保証が得られる。

ワンタイムパスワードデバイストークンはハードトークンに似ている。これらのトークンをパスワードと組み合わせて使用したり、パスワードや生体情報によってトークンを活性化したりすることで、複数要素による認証を提供できる。ただし、ワンタイムパスワードデバイスでは、認証に基づく共有セッション認証鍵が生成されることはない。

本文書では、認証保証レベル 3 および 4 を実現するには複数要素による認証を要求し、OMB ガイダンスに対応した 4 つのレベルにトークンを次のように割り当てている。

- パスワードトークンは、レベル 1 および 2 の保証に関する要求事項を満たす。
- ソフト暗号トークンは認証保証レベル 1～3 で使用することもできるが、レベル 3 を達成するにはパスワードや生体認証と組み合わせる必要がある。
- ワンタイムパスワードデバイスは、レベル 1～3 の保証に関する要求事項を満たすものとみなされ、レベル 3 を達成するにはパスワードや生体認証と組み合わせて使用する必要がある。
- パスワードや生体認証によって活性化するハードトークンは、レベル 1～4 の保証に関する要求事項を満たす。

以上はトークンの保証レベルの全般的な概要である。しかし、具体的な要求事項については認証プロトコルの詳細に応じて異なる。レベル 3 および 4 では 2 要素の認証が求められる。つまり、通常はレベル 3 および 4 を達成するためには、パスワードまたは生体認証を使用して鍵を活性化する必要がある。あるいは、パスワードプロトコルをソフトトークン、ハードトークン、またはワンタイムパスワードトークンと組み合わせて使用することで、2 要素の認証を達成することもできる。レベルごとの詳細なトークンの要求事項については、プロトコルの要求事項と合わせてセクション 8 で説明する。

7. 登録と身元識別情報の検証

登録プロセスでは、申請者が、信頼のおける登録機関（RA）による身元識別情報の検証を受ける。RA が申請者の身元識別情報を検証することができた場合、CSP によって申請者のトークンが登録または付与され、そのトークンを身元識別情報またはなんらかの関連する属性に結び付けるクレデンシャルが必要に応じて発行される。その時点で、申請者は CSP の加入者となり、認証プロトコルのなかで認証要求者としてトークンを使用することができるようになる。

RA は、CSP の一部の場合もあれば、別の独立したエンティティの場合もある。しかし、RA と CSP のあいだには信頼関係が常に存在する。RA または CSP は、そのどちらかで登録の記録を維持管理する必要がある。RA および CSP は、組織に代わってサービスを提供したり、公にサービスを提供したりする場合がある。その結果、RA が身元識別情報の検証に利用することができるプロセスやメカニズムはさまざまである。RA が組織に代わって運営される場合は、身元識別情報の検証プロセスで既存の関係を活用できることがある（たとえば、申請者が従業員や学生であるなど）。RA が公にサービスを提供する場合には、身元識別情報の検証プロセスは通常、公に利用できる情報と以前に発行されたクレデンシャルの確認に限定される。

登録と身元識別情報の検証のプロセスは、多かれ少なかれ保証レベルに応じて、RA および CSP の一方または両方が申請者の真の身元を知ることができるように設計されている。具体的には、次のことを保証する措置が要求事項に含まれる。

1. 申請者に要求されている属性を持つ人物が存在し、それらの属性が単一の人物を一意に識別するのに十分であること。
2. トークンが登録されている申請者が、実際にその身元識別情報に該当する人物であること。
3. 申請者があとで登録を否認できないこと。したがって、あとで加入者のトークンを使用して行う認証に関して異議申し立てが生じても、加入者は自分がそのトークンを登録したことを否定することはできない。

申請者は本人が出向いて登録することも、リモートより登録することもできる。それぞれの場合において、身元識別情報の検証に多少異なるプロセスやメカニズムが適用される。リモート登録はレベル 1～3 に限定される。

7.1. 登録の脅威

登録プロセスに対する脅威には 2 つの一般的な分類がある。1 つはなりすましであり、もう 1 つはインフラストラクチャ（RA や CSP）の危殆化または不正行為である。本文書では、主になりすましの脅威への対応について説明する。インフラストラクチャの脅威に対してはコンピュータのセキュリティに関する一般的な管理策（職務の分離、記録の保持、独立した監査など）で対応する。これらの管理策については本書の範囲外である。

7.1.1. 脅威のモデル

詐称者によっては任意の加入者としてシステムへの登録を試みたり、特定の加入者としての登録を望んだりする可能性があるが、登録の脅威は次のように分類できる。

- 主張する身元へのなりすまし:申請者が不正な身元を主張し、時間をかけて作り上げた特定の属性セットによって、あるいは偽のクレデンシャルの提示によって、その主張を裏付ける。
- 登録の否認:加入者が登録を否認し、そのトークンを登録しなかったと主張する。

7.1.2. 登録の脅威に対する耐性

登録詐欺は、その達成をさらに難しくしたり、検出率を高めたりすることによって阻止できる。本文書ではなりすましをより難しくするための手段について主に取り上げるが、なりすましを実行した人物の立証に役立つ可能性のある特定の手段や手続きについても規定している。各レベルにおいて、求められた身元識別情報を持つ人物が存在すること、申請者がその身元識別情報に該当する人物であること、および、申請者があとで登録を否認できないことを、それぞれ判断するための手段が利用される。保証のレベルが高くなるにつれて、偶発的ななりすまし、組織的ななりすまし、および内部の者によるなりすましに対して、より強度の強い手段が利用される。

7.2. 登録のレベル

以降の各項では、OMB ガイダンスに対応した 4 つのレベルについて、登録と身元識別情報の検証を行うための NIST による推奨事項を説明する。OMB ガイダンスで示されているように、レベル 1 および 2 では匿名のクレデンシャルの使用を認めている。匿名のクレデンシャルを使用してグループへの所属を暗黙に示す場合、検証のレベルは、そのレベルの身元識別情報のクレデンシャルに求められる要求事項と一致するものとする。匿名クレデンシャルの登録プロセスの要求事項は、個々のグループの所属基準に固有のものとなるため、明示的には規定しない。

レベル 2 以上では、登録の記録を、状況に照らして RA か CSP のどちらかで維持管理するものとする。RA または CSP のどちらかが、身元識別情報の検証が済んだ各個人の記録と、その個人の身元識別情報を検証するために実施した手順を維持管理するものとする。その際、以降の各項で要求されている証拠も含めて維持管理する。CSP は、身元識別情報の検証記録を必要に応じて検証結果の利用者に提供できるよう準備しておく。身元識別情報の検証と登録のプロセスは、身元を確認するために実施すべき具体的な手順を規定した、書面によるポリシーまたは「実施規程」に従って実施するものとする。

RA と CSP が離れた場所に存在し、ネットワーク経由で通信する場合は、認証プロトコルを使用して RA と CSP のあいだの登録トランザクション全体を暗号による手段で認証するものとする。この場合、認証プロトコルは、登録の保証レベルの要求事項を満たすものとし、送信される秘密情報はすべて承認された暗号化方式を使用して暗号化するものとする。

CSP は、各加入者と、その加入者に対して発行され関連付けられたトークンおよびクレデンシャルについて、それらを一意に識別できるものとする。CSP はこの情報を検証者と検証結果の利用者に伝達する能力を有するものとする。レベル 1 では、加入者に対応する名

前が申請者によって提示され、検証されることなく受理される。レベル 2 では、加入者に対応する名前が仮名であってもよいが、RA または CSP が加入者の実際の身元を知っている必要がある。また、仮名によるレベル 2 のクレデンシャルは、有意の名前を含んだレベル 2 のクレデンシャルとは区別できる必要がある。レベル 3 以上では、加入者に対応する名前は有意である必要がある。すべてのレベルにおいて、登録プロセスの一環として収集された個人識別情報は、不正な漏えいや改ざんが行われないように保護する必要がある。

次の 7.2.1 項では、それぞれのレベルに固有の登録と身元識別情報の検証の要求事項を定める。各レベルの記録保持の要求事項については 7.2.2 項で規定する。

7.2.1. 登録と身元識別情報の検証の要求事項

次の文は、各レベル固有の登録に関する要求事項を規定する。レベル 1 ではレベル固有の要求事項は存在しない。レベル 2 および 3 では、対面による登録とリモートによる登録の両方が許される。レベル 2 および 3 のそれぞれのシナリオについて、明示的な要求事項が規定されている。レベル 4 では、対面による登録のみが許される。

レベル 2 以上では、申請者は自分の法的な氏名、記録上の住所、および誕生日を提示する。また、RA または CSP のポリシーによっては、それ以外の個人識別情報を提示することもある。レベルごとの身元識別情報の検証の要求事項については、以下の表 1 に詳しく示す。

表 1:保証レベル別の身元識別情報検証の要求事項

	対面	リモート
レベル 2		
クレデンシャルを発行する根拠	申請者の写真と、記録上の住所または国籍のいずれかを含んだ、政府発行の現在有効な一次的な写真つき身分証明書を所持していること(運転免許証やパスポートなど)。	政府発行の有効な身分証明書(運転免許証やパスポートなど)の番号と金融口座番号(当座預金口座、普通預金口座、融資カード、クレジットカードなど)を所持しており、いずれかの番号の記録を通じて確認できること。
RA の実施内容	写真つき身分証明書を検査し、写真と、申請者、記録 ID 番号、住所、および生年月日とを比較する。身分証明書が有効と思われ、写真が申請者と一致する場合は、次のことを行う。 a) 記録上の住所が身分証明書によって確認された場合は、クレデンシャルの承認または発行を行い、記録上の住所宛てに通知書を送付する。または、 b) 記録上の住所が身分証明書によって確認できない場合は、記録上の住所を確認できる方法で、クレデンシャルを発行する。	• 申請者から提示された ID 番号と口座番号の両方を検査する。申請者から提示された ID 番号または口座番号を含む情報について、該当する政府機関または公共機関あるいは信用調査所や同様のデータベースを通じて記録を確認することで検証を行う。このとき、記録されている名前、生年月日、住所そのほかの個人情報が申請内容と最終的に一致し、特定の個人を一意に識別するのに十分であることを確認する。 • 住所の確認と通知を行う。 a) 記録検査で確認された記録上の住所宛てに、通知書を送付する。または、 b) 申請者から提示された記録上の住所を確認できる方法で、クレデンシャルを発行する。または、 c) 記録されている申請者に関連付けられている電話番号または電子メールアドレスを通じて申請者と電話または電子メールによる連絡ができることを確認できる方法で、クレデンシャルを発行する。
レベル 3		
クレデンシャルを発行する根拠	申請者の写真と、記録上の住所または国籍のいずれかを含んだ、政府発行の現在有効な検証済みの一次的な写真つき身分証明書を所持していること(運	政府発行の有効な身分証明書(運転免許証やパスポートなど)の番号と金融口座番号(当座預金口座、普通預金口座、融資カード、クレジットカード

	対面	リモート
	転免許証やパスポートなど)。	など)を所持しており、両方の番号の記録を通じて確認できること。
RA の実施内容	写真つきの身分証明書を検査し、発行元の政府機関あるいは信用調査所や同様のデータベースを通じて検証する。そして、記録されている名前、生年月日、住所そのほかの個人情報が申請内容と一致することを確認する。写真と、申請者、記録 ID 番号、住所、および生年月日とを比較する。身分証明書が有効で、写真が申請者と一致する場合は、次のことを行う。 a) 記録上の住所が身分証明書によって確認された場合は、クレデンシャルの承認または発行を行い、記録上の住所宛てに通知書を送付する。または、 b) 記録上の住所が身分証明書によって確認できない場合は、記録上の住所を確認できる方法で、クレデンシャルを発行する。	• 申請者から提示された ID 番号および口座番号を含む情報について、該当する政府機関または公共機関あるいは信用調査所や同様のデータベースを通じて記録を確認することで検証を行う。このとき、記録されている名前、生年月日、住所そのほかの個人情報が申請内容と一致し、特定の個人を一意に識別するのに十分であることを確認する。 • 住所の確認 a) 申請者から提示された記録上の住所を確認できる方法で、クレデンシャルを発行する。または、 b) 記録されている申請者に関連付けられている電話番号によって申請者と電話連絡ができることを確認した上でクレデンシャルを発行するとともに、申請者の音声を記録する。
レベル 4		
クレデンシャルを発行する根拠	本人が出頭し、2 つの別々の身分証明文書または口座を検証して、レベル 3 の要求事項を満たすこと(出頭およびリモート)。そのうちの 1 つは、申請者の写真と、記録上の住所または国籍のいずれかを含んだ、政府発行の現在有効な一次的な写真つき身分証明書(運転免許証やパスポートなど)である必要がある。そして、申請時に申請者の生体情報の新しい記録をとる。	適用不可
RA の実施内容	• *一次的な写真つきの身分証明書:* 写真つきの身分証を検査し、発行元の政府機関を通じて検証を行い、写真と、申請者、記録 ID 番号、住所、および生年月日とを比較する。 • *政府発行の二次的な身分証明書ま*	適用不可

	対面	リモート
	または金融口座 a) 写真つきの身分証明書を検査し、有効と思われる場合、写真と、申請者、記録 ID 番号、住所、および生年月日とを比較する。または、 b) 申請者から提示された金融口座番号について、記録検査を通じて、あるいは信用調査所や同様のデータベースを通じて、検証を行う。このとき、記録されている名前、生年月日、住所そのほかの個人情報が申請内容と最終的に一致し、特定の個人を一意に識別するのに十分であることを確認する。 • *最新の生体情報の記録* 最新の生体情報（写真や指紋など）を記録し、申請者が申請を否認できないようにする。 • *住所の確認* 記録上の住所を確認できる方法で、クレデンシャルを発行する。	

レベル 2 において、上記のレベル 2 について示した内容と同等の手段で職員または学生の身元識別情報を検証する雇用者および教員は、RA または CSP になることを選択し、クレデンシャルを職員または学生に発行することができる。対面による発行の場合は、企業または学校から発行された写真つきの身分証明書を検査する。オンラインプロセスを通じて発行する場合は、個人の機密通信に通常使用される配布経路を通じて通知を行う。

レベル 2 において、米国財務省の通貨監督庁の監督下にある金融機関は、オンラインバンキングのクレデンシャル用に通常使用されているメカニズムを通じて、各自の顧客にクレデンシャルを発行することができる。そして、セクション 8 の規程を満たす限り、オンラインバンキングのクレデンシャルとトークンをレベル 2 のクレデンシャルとして使用することができる。

状況によっては、政府機関は、知っていることに基づく追加の認証手段を使用することで、登録プロセスの信頼性を高めることもできる。たとえば、申請者に対し、政府機関自身との過去の関わりに関する非公開の情報を提示するように求め、申請者の身元の確認に役立てることができる。

7.2.2. 記録保持の要求事項

登録に関する事実の記録（失効を含む）は、CSP またはその代理者によって維持管理されるものとする。レベル 2 のクレデンシャルの登録データに対する最短の記録保持期間は、クレデンシャルの有効期限満了または失効のいずれか遅いほうを起点として 7 年 6 か月と

する。また、政府行政機関あるいはその代理者が運営する CSP では、米国国立公文書館（National Archives and Records Administration）が規定する一般文書保管計画（General Records Schedule）または機関固有の計画の規程に従う必要がある。それ以外のすべてのエンティティは、各エンティティに適用される法律に基づいたそれぞれの記録保持ポリシーを順守するものとする。登録データの最短の記録保持期間は次のとおりとする。

- レベル 2 および 3 では、有効期限満了から 7 年 6 か月
- レベル 4 では、有効期限満了から 10 年 6 か月

7.3. 登録レベルに対する FPKI 証明書ポリシーの対応付け

連邦 PKI 証明書ポリシー[FCBA1、FBCA2、FBCA3]に規定されている身元識別情報検証と証明書発行のプロセスは、前のセクションに規定した登録レベルに対応付けることができる。これらの対応付けは次のようになる。

- Citizen and Commerce Class policies（市民および商業クラスポリシー） [FBCA2]に対応付けられたポリシーのもとでの、連邦ブリッジ CA と横断認証（cross-certification）を行う認証局における身元識別情報検証と証明書発行のプロセスは、レベル 2 の身元識別情報の検証の規程を満たすものとみなされる。
- Basic Certificate Policy（基本認証ポリシー）[FBCA1]に対応付けられたポリシーのもとでの、連邦ブリッジ CA と横断認証を行う認証局における身元識別情報検証と証明書発行のプロセスは、レベル 2 および 3 の身元識別情報の検証の規程を満たすものとみなされる。
- [FBCA1]の Medium（中位）、Medium-HW（中位-ハードウェア）または High Assurance Certificate（高保証証明書）ポリシー、または[FBCA3]の Common-Auth（共通-認証）、Common-SW（共通-ソフトウェア）、Common-HW（共通-ハードウェア）、および Common-High Certificate（共通-高保証証明書）ポリシーに対応付けられたポリシーのもとでの、連邦ブリッジ CA と横断認証を行うう認証局における身元識別情報検証と証明書発行のプロセスは、レベル 2、3、および 4 の身元識別情報の検証の規程を満たすものとみなされる。

ただし、レベル 1 および 2 においては、政府機関は、連邦ブリッジCAと横断認証するCAによる証明書のみに依拠する必要はない。これらのレベルでは、政府機関は、7.2.1 項の全体要求事項に示した身元識別情報の検証と登録の要求事項を満たすことが確認されている任意のCAに依拠することもできる。レベル 3 および 4 では、上記のいずれかの証明書ポリシーのもとで、あるいはそれらのいずれかのポリシーに対応付けられたポリシーのもとで、連邦ブリッジCAと横断認証を行う[2]CAが、PKIのクレデンシャルを発行する必要がある。

[2] 双方向の横断認証は必須ではない。ブリッジCAから発行元CAへの有効な証明書パスが存在すれば十分である。逆方向の証明書パスは存在する必要はない。

8. 認証プロトコル

認証プロトコルは、認証要求者と検証者のあいだで取り交わされるメッセージの、定義済みのシーケンスである。認証プロトコルによって、検証者は、認証要求者が自身の身元を証明するための有効なトークンを管理していることを検証できる。認証要求者と検証者のあいだのメッセージの交換のことを、プロトコル実行という。プロトコル実行の結果、認証要求者が認証される(または認証が失敗する)。

8.1. 認証の脅威

脅威は、実行中の認証プロトコルそのものに対する攻撃を伴うものや、トークン値を暴いたり機密情報を危殆化する攻撃を伴うものに分けることができる。一般に、トークン値を暴く攻撃は、攻撃者がそのあとトークンを使用して加入者を装うことができるので、なんらかの情報を危殆化するだけの攻撃よりも悪質である。

8.1.1. 認証プロトコルの脅威

登録機関、CSP、検証者、および検証結果の利用者は、通常は(正しく機能し故意に悪質でないという意味で)信頼し得る。しかし、認証要求者やそのシステムは信頼し得るとはいえない場合がある(そうでなければ彼らの身元識別情報の主張を単純に信頼できることになる)。そのうえ、RA、CSP、および検証者は、通常は信頼し得るが、脆弱性がないわけではなく、機能不全となる可能性がある。したがって、認証用の長期共有秘密情報を絶対に必要とされる期間を超えて長期にわたって開示するプロトコルは、たとえ信頼のおけるエンティティに開示する場合でも避けるべきである。

プロトコルの脅威には次のようなものがある。

- 盗聴者が実行中の認証プロトコルを観察し、後で分析する。場合によっては、CSPと検証者、または認証要求者と検証者以外の第三者とのあいだで取り交わされるメッセージを、盗聴者が傍受することがある。通常、盗聴者はトークンを取得して認証要求者になりすますことを試みる。
- 詐称者。
  - 検証者に対して加入者になりすました偽の認証要求者が、推測したトークンを試したり、特定の加入者に関するほかの情報を入手したりする。
  - 正規の加入認証要求者に対して検証者になりすました偽の検証者が、正規の検証者に対して加入者を装うために使用することができるトークンの入手を行う。
  - 検証者に対して連邦 IT システムになりすました偽の検証結果の利用者が、ユーザの機密情報を入手する。
- すでに認証済みのセッションを乗っ取ったハイジャック者が、そのあと次のような行為を行う。
  - 検証結果の利用者に対して加入者になりすまし、機密情報を探ったり無効な情報を入力したりする。
  - 検証者に対して検証結果の利用者になりすまし、機密情報を探ったり無効な情報を出力したりする。

盗聴者は実行中の認証プロトコルを物理的に傍受できるものと想定されている。しかし、傍受されたメッセージを理解不能にするように、あるいは認証要求者を装うのに役立つ情

報を得ることを可能にする分析に耐え得るように、プロトコルを設計することもできる。加入者になりすました者は、検証者または検証結果の利用者に対する通常の通信アクセス経路を必要とする。検証者になりすました者は、パケットの宛先変更、挿入、または削除を行う特殊なネットワーク機能を持っている場合があるが、多くの場合、そのような攻撃は、不正なリンクを電子メールや Web ページに組み込んで加入者をだましたり、検証結果の利用者や検証者のものに似せたドメイン名を使用したりするという、単純な手口で仕掛けられる。したがって、詐称者は必ずしも特別なネットワーク機能を持っている必要がない。パスワードプロトコルにおいては、Web ブラウザクライアントが広く使用されるようになったことと、その実装方法に起因して、Web ブラウザのユーザは、特に検証者になりすました者に対して脆弱となる。ハイジャックをするには通信セッションの宛先を変更できなければならないが、多くの加入者が無線によるネットワークアクセスを利用するこんにちでは、比較的容易に達成できる場合がある。

認証プロトコルに対する攻撃の具体的なメカニズムとしては次のものがある。

- 盗聴者が、認証プロトコルのやりとりを受動的に傍受し、パスワードや鍵などの秘密情報を探ろうとする。
- 認証メカニズムに対する次のような能動的なオンライン攻撃:
    - 認証経路内攻撃。攻撃者が認証要求者になりすまし、本物の検証者とやり取りする。これには次のものがある。
        - パスワード推測攻撃。詐称者がログオンを何度も試みることでパスワードを推測し、システムにログインできると成功となる。
        - 標的を定めた推測攻撃。名前が分かっているユーザを選択し、そのユーザのパスワードに対して攻撃を行う。
        - リプレイ攻撃。攻撃者は、検証者に対する以前の正常なプロトコル実行の一部分を記録して再生する。
    - 認証経路外攻撃。攻撃者が認証経路を次のような方法で変更する。
        - 認証の完了後にセッションをハイジャックする。
        - 検証者なりすまし攻撃。攻撃者が検証者になりすまし、認証要求者をだまして認証要求者の秘密トークンを開示させる。たとえ、検証者を認証するセキュアなプロトコル（TLS など）を使用している場合、あるいは「使用していると思われる」場合でも、機能的な複雑さ、ユーザインタフェースの複雑さ、および、ユーザへの表示に関してサーバに与える制御範囲のために、Web ブラウザのユーザはパスワード検証者を詐称する攻撃に対して脆弱である可能性が高い。
        - 中間者攻撃。攻撃者が認証交換の経路に自身を介入させ秘密トークンを入手する。たとえ、そのような攻撃を防ぐセキュアなプロトコル（TLS など）を使用している場合、あるいは「使用していると思われる」場合でも、機能的な複雑さ、ユーザインタフェースの複雑さ、および、ユーザへの表示に関してサーバに与える制御範囲のために、Web ブラウザのユーザは中間者攻撃に対して脆弱である可能性が高い。

8.1.2. プロトコルの脅威に対する耐性

この項では、個々のプロトコルの脅威に対する耐性の意味について定義する。

- *盗聴に対する*耐性：認証要求者と検証者または検証結果の利用者とのあいだでやり取りされるすべてのメッセージを記録する盗聴者が、プライベート鍵、秘密鍵、またはパスワードを探ること、あるいは盗聴者が認証要求者になりすますことを可能にする情報を入手することが現実的でないと判断する場合、認証プロトコルは、盗聴攻撃に対して耐性がある。盗聴に対する耐性のあるプロトコルでは、攻撃者がオフライン攻撃を実行すること、つまり、攻撃者が認証プロトコルの実行を記録し、大きな辞書にあるすべてのパスワードを体系的に試したり、あらゆる可能性を総当たりで試したりするなど、その記録を自分のシステムで長期間分析することが現実的ではなくなる[3]。
- *パスワード推測に対する*耐性：パスワードを「*事前に*」知らない攻撃者が、パスワードを推測して認証を繰り返し試すことによってパスワードを見つけ出すのが現実的でない場合、認証プロトコルは、パスワード推測に対して耐性がある。パスワードのエントロピーとプロトコルそのもののエントロピーの両方が、この性質に貢献する。パスワード認証システムでは、エントロピーの高いパスワード（付録Aを参照）の使用を求め、認証の失敗回数に上限を設けるか、認証の試行頻度を制御することによって、標的を定めたパスワード推測攻撃を現実的でないものにすることが可能である。標的を定めないパスワード攻撃に対しては、検証者がネットワークセキュリティ管理策によってこれらの管理策を補うことで耐性を持たせることもできる。
- *リプレイ攻撃に対する*耐性：以前の認証メッセージを記録してそれを再現することによって認証を成功させることが現実的でない場合、認証プロトコルは、リプレイ攻撃に対する耐性がある。
- *ハイジャックに対する*耐性：認証プロトコルと、それに引き続くデータ転送に用いられるセッションプロトコルの両方に関わる性質である。メッセージの挿入、削除、または宛先変更を行う能力を有する攻撃者が、認証要求者と検証結果の利用者とのあいだでやり取りされる情報の内容を検知されることなく改ざんするのを防ぐような方法で、認証とデータ転送が結び付けられている場合、認証プロトコルと転送プロトコルの組み合わせは、ハイジャックに対して耐性がある。通常、この耐性は、認証プロセス中にセッション固有の共有秘密情報を生成し、以降その情報を認証要求者と検証結果の利用者が使用してすべての機密情報の転送を認証することによって達成される。
- *検証者へのなりすましに対する*耐性：検証者になりすます攻撃では、攻撃者が正規の検証者になりすます。検証者へのなりすましは「名前のなりすまし」によって比較的容易に行える場合もあれば、より高度ななんらかのネットワーク攻撃を必要とするものもある（こんにちの無線 LAN アクセスは、多くの状況において攻撃者がそのような「高度な」ネットワーク攻撃を行うことを比較的容易にしている）。詐称者が検証者として振舞ったときにトークンの値を知ることができなければ、認証プロトコルは検証者へのなりすましに対して耐性がある。ただし、セキュアなプロトコルであっても、認証要求者をだまして別のプロトコルを使用させたり、または（検証されてい

[3] ここでは「現実的でない」という言葉を、暗号学的にほぼ不可能であるという意味で使用している。つまり、わずかながら成功の確率が常に存在するが、膨大なリソースを有する攻撃者であってもほぼ必ず失敗するという意味である。オフライン攻撃の場合の「現実的でない」とは、プロトコルを「解読」するのに必要な作業の量が少なくとも 2^{80} 程度の回数の暗号演算であることを意味する。オンライン攻撃の場合の「現実的でない」とは、オンラインで試行できる回数が、可能性のある鍵やパスワードの値の数と比べてひじょうに少ないことを意味する。

ないサーバ証明書を受け入れさせるなどして）セキュリティ管理策をオーバーライドすることによって、その使用が回避される場合がある。

- *中間者攻撃に対する耐性*: 認証プロトコルに対する中間者攻撃では、攻撃者が認証要求者と検証者のあいだに割り込み、認証要求者に対しては検証者を装い、検証者に対して認証要求者を装うことにより、認証トークンの値を知る。第三者が検出されずに参加することを防ぐような方法で、両方の当事者（認証要求者と検証者）が他方に対して認証される場合、認証プロトコルは中間者攻撃に対して耐性がある。ただし、セキュアなプロトコルであっても、認証要求者をだまして別のプロトコルを使用させたり、または（検証されていないサーバ証明書を受け入れさせるなどして）セキュリティ管理策をオーバーライドすることによって、その使用が回避される場合がある。

8.1.3. そのほかの脅威

攻撃の対象は、認証プロトコルに限定されない。ほかにも次のような攻撃がある。

- 悪意のコードによる攻撃。認証トークンを危殆化するおそれがある。
- 侵入攻撃。加入者／認証要求者、CSP、または検証者のシステムに侵入することによってクレデンシャルやトークンを入手する。
- 内部の者による攻撃。認証トークンを危殆化するおそれがある。
- 帯域外攻撃。加入者がパスワードを攻撃者に開示すよう仕向けるソーシャルエンジニアリングや、「ショルダーサーフィン」などの手口でトークンを入手する。
- 認証要求者をだまして、安全なプロトコルを使用しているかのように見せかけて、安全でないプロトコルを使用するように仕向けたり、（正当性を確認できないサーバ証明書を受け入れさせるなどして）セキュリティ管理策を無効にさせる攻撃。
- 意図的な否認。これは加入者が自分のトークンを故意に危殆化することによる。

認証要求者の認証トークンを危殆化する目的で、悪意のコードが認証要求者のコンピュータシステムに仕組まれるおそれがある。悪意のコードは数多くの手段によって送り込まれるおそれがある。ここではそのいくつかを詳しく説明する。認証要求者のシステムにおいて悪意のコードのリスクを軽減することのできる対抗手段は、ウイルスチェッカやファイアウォールなど数多くある。悪意のコードによる脅威を緩和するための一般的で適切な実践事項は、本書の範囲外である。ハードウェアトークンにより、悪意のソフトウェアがそのトークンから認証用秘密トークンを抽出・コピーするのを防ぐことができる。しかし、悪意のコードによってトークンが濫用される可能性は残っている。特にトークンを活性化するデータがコンピュータを通じてトークンに提示される場合はそのおそれがある。同様に、暗号トークンは、少なくとも、ユーザをだまして認証用の秘密情報を口頭で伝えさせることを困難にすることでソーシャルエンジニアリングをより難しくするが、一方で数多くの種類のパスワードが電話を通じて手軽に伝えられている。

内部の者による脅威は数多くの IT システムにおいて重要な懸念事項である。しかし、適切なセキュリティ、人員、および監査の実践によって、これらのリスクが軽減される可能性がある。内部の者による脅威を緩和するための一般的で適切な実践事項は、本書の範囲外である。

プロトコルの観点から見た場合、共有秘密情報はCSPがしっかり所持し、注意深く保護する必要がある。一般に、保証レベル 2、3、および 4 では、CSPは独立の検証者に対し、長期共有秘密情報を与えてはならない。これは、内部の者による攻撃の危険性が高まるためである。共有秘密情報が暗号鍵である場合、独立の検証者に対して、1 回限りのchallenge-response情報を与えることができる[4]。共有秘密情報がパスワードの場合、challenge-responseのメカニズムは内部の者による攻撃または侵入攻撃に対して脆弱になる。

ネットワーク侵入攻撃は多くの点で内部の者による脅威に似ており、あらゆるオンラインITシステムのリスクとなっている。ファイアウォール、システム構成、侵入検知など、ネットワーク侵入攻撃のリスクを軽減するための防止手段の使用については、参考となる情報が多数ある（いくつかの有益な参考情報については10.2項および10.3項を参照のこと）。加入者／認証要求者のシステムはネットワーク侵入攻撃も受けるおそれがあるが、適切な認証メカニズムがそうした攻撃に対する防衛の 1 つとなる。

ネットワーク侵入攻撃の最も深刻な結果は、認証プロトコルで使用されるトークンの入手またはコントロールを攻撃者に許してしまうおそれがあることである。侵入攻撃を軽減するための一般的な対処方法は、本書の範囲外である。しかし、内部の者による脅威と同様に、認証サービスの設計要素の一部には、認証サービスそのものに対する侵入リスクを増加させるあるいは軽減するものがある。ハードウェアトークンや暗号モジュールは、鍵を所持する環境を制限することによって、鍵やパスワードを侵入攻撃から保護する。他の認証メカニズム には、認証要求者のシステムにアクセスまたは侵入できる攻撃者に対して脆弱である可能性があるものもある。しかし、共有秘密情報のメカニズムは、検証者および CSP に対する侵入攻撃の対象となりやすく、攻撃者が多数の共有秘密情報のファイルを見つけ出すおそれもある。公開鍵のメカニズムのほうが、通常は検証者および CSP への攻撃に対する脆弱性が低い。長期共有秘密情報を収めたファイルを暗号化すれば、侵入攻撃が成功した場合のリスクが低下する。

加入者が認証を否認する目的で故意にトークンを危殆化することがある。認証否認の詳細については本書の範囲を越える。しかし、通常は、認証プロトコルをほかの脅威から保護することが否認の限定に寄与する。否認のリスクは、ユーザがセキュリティ上の要求事項を順守していることを定期的に確認する、トランザクションを別の経路（電子メールなど）を通じて確認する、トークンの移譲が禁じられていることをユーザに思い出させるといった、さまざまな措置によって低減することができる。詳細な議論については DOJ 2000 を参照のこと。

[4] 携帯電話システムではこのような共有秘密情報によるchallenge-response認証メカニズムが一般的に採用されている。共有秘密鍵は、携帯電話機と、ホームサービスプロバイダの「ホームロケーションレジスタ」で維持管理されている。ユーザーがローミングによって移動し、別のホストプロバイダの基地局に登録されると、ホームサービスプロバイダはchallengeと応答を生成し、ローミングユーザーの認証に使用するためにホストサービスプロバイダに送信する。共有秘密鍵のエントロピが十分であれば、内部の者によるホストサービスプロバイダでのオフライン攻撃は非現実的となる。

8.2. 認証メカニズムの要求事項

本項では、トークンの登録をすでに済ませた認証要求者を機械的に認証するプロセスについて説明する。身元識別情報の検証と登録については、セクション7で別途取り上げている。認証プロセスは、検証結果の利用者に対して、加入者によって提供され、クレデンシャル発行時にRAによって検証される登録情報を一意に識別するのに十分な情報を提示するものとする。

1～4 の番号が付けられた 4 つの保証レベルが定義されている。レベル 4 が最も高いレベルの認証保証を提供し、レベル 1 は最も低いレベルの認証保証を提供する。認証メカニズムの技術的な要求事項（トークン、プロトコル、およびセキュリティ保護）を本項で規定する。

8.2.1. レベル 1

このレベルでは身元識別情報の検証は要求事項になっていないが、保護されたトランザクションやデータにアクセスするのが同じ認証要求者であるというなんらかの保証が、認証メカニズムによって提供される。このレベルでは広範な認証技術を利用することが可能であり、レベル 2、3、または 4 のトークン手法を利用することが許される。認証が成功するためには、セキュアな認証プロトコルを通じて、認証要求者本人がトークンを管理していることを証明することが必要である。

レベル 1 では、平文のパスワードや秘密情報はネットワーク経由で送信されないものとする。ただし、このレベルでは盗聴者によるオフライン分析を阻止する暗号手段は要求されない。たとえば、パスワードと challenge を組み合わせて認証応答を生成するパスワード challenge-response プロトコルは、この要求事項を満たす。ただし、challenge と response を傍受する盗聴者が、オフラインでの辞書攻撃またはパスワードの総当り攻撃を行って、パスワードを復元する可能性がある。レベル 1 の要求事項を満たす一般的なプロトコルとしては、APOP [RFC 1939]、S/KEY [SKEY]、および Kerberos [KERB]がある。こうしたプロトコルのやりとりを傍受する攻撃者は多くの場合、単純な辞書攻撃によってパスワードを知ることができ、このような脆弱性は演算強度とは独立のものであるため、このレベルでは承認された暗号化技法を使用するという要求事項はない。

レベル 1 では、認証用の長期共有秘密情報が検証者に開示されることがある。

8.2.1.1.クレデンシャルの有効期限、状態、または失効

レベル 1 では、クレデンシャルの失効および有効期限についての規程はない。

8.2.1.2.アサーション

検証結果の利用者は次のアサーションを受理できる。

- 信頼のおけるエンティティ（検証者）によってディジタル署名されたもの。または、
- 信頼のおけるエンティティ（リポジトリや検証者など）から直接取得したもの。その際使用されるプロトコルでは、暗号による手段で検証者を認証しアサーションを保護するセキュアなプロトコル（TLS など）を使用して、信頼のおけるエンティティが検証結果の利用者に対して認証を行う。

8.2.1.3.長期共有秘密情報の保護

レベル 1 認証で検証者が使用する共有秘密情報のファイルは、アクセスを管理者およびアクセスを必要とするアプリケーションのみに制限する任意のアクセス制御によって保護される。そのような共有秘密情報ファイルには平文のパスワードを含めないものとする。通常、これらのファイルにはパスワードの一方向のハッシュまたは「反転」が含まれている。また、レベル 2、3、4 において長期共有秘密情報の保護手段として許可されている任意の手段を、レベル 1 で使用することができる。

8.2.1.4.パスワードの強度

パスワード（または暗証番号）ベースのレベル 1 認証システムでは、パスワードを「*事前に*」知らないが、攻撃対象のユーザ名を知っている攻撃者が、標的を定めたオンラインパスワード推測攻撃を成功させる確率が、パスワードの有効期限において 2^{-10}（1,024 分の 1）を超えないものとする。レベル 1 では最小エントロピーに関する要求事項はない。付録A には、パスワードのエントロピーを推定することに関する情報が記載されている。

8.2.1.5.実装例

多種多様な技術がレベル 1 の要求事項を満たせるはずである。たとえば、検証者は加入者のパスワードを CSP から入手し、challenge-response プロトコルを使用して認証要求者を認証することができる。

8.2.2. レベル 2

レベル 2 では広範な認証技術を利用することが可能であり、レベル 2、3、または 4 のどのトークン手法の利用も許される。パスワードの利用についても同様である。認証要求者が認証に成功するには、セキュアな認証プロトコルを通じて、認証要求者本人がトークンを管理していることを証明することが必要である。盗聴、リプレイ攻撃、およびオンライン推測攻撃が阻止されるものとする。盗聴を阻止するためには承認された暗号技術が必要である。

8.2.2.1.クレデンシャルおよびトークンの有効期限、状態、または失効

CSP は、クレデンシャルがまだ有効であることを検証者や検証結果の利用者が確認できるようにセキュアなメカニズム（ディジタル署名された失効リストやステータスレスポンダなど）を提供するものとする。検証者や検証結果の利用者は、使用するクレデンシャルが有効であることを確認するものとする。共有秘密情報に基づく認証システムでは、失効した加入者が単に検証データベースから削除される場合もある。

CSP は、クレデンシャルが有効ではなくなったこと、またはトークンが危殆化されたことを通知されてから 72 時間以内に、クレデンシャルまたはトークンを失効させ、そのトークンを使用する認証要求者の認証が成功しないことを保証するものとする。CSP が 72 時間以内に自動的に有効期限切れとなるクレデンシャルを発行する場合（たとえば、1 日ごとに 24 時間の有効期限を持つ新規の証明書を発行する場合など）には、クレデンシャルを失効させるための明示的なメカニズムを CSP が提供する必要はない。パスワードを登録する CSP は、72 時間以内にパスワードの失効または登録解除が達成できること、および、そのパスワードを使用した認証が失敗することを、保証するものとする。

基本（Basic）、中位（Medium）、高位（High）、市民および商業クラス（Citizen and Commerce Class）、または共通証明書ポリシー（Common Certificate Policy）のレベルにお

いて、連邦ブリッジ CA と横断認証を行う CA は、このレベルにおけるクレデンシャルの状態と失効に関わる規程を満たすものとみなされる。

8.2.2.2.アサーション

検証結果の利用者は次のアサーションを受理できる。

- 信頼のおけるエンティティ（検証者）によってディジタル署名されたもの。または、
- 信頼のおけるエンティティ（リポジトリや検証者など）から直接取得したもの。その際使用されるプロトコルでは、暗号による手段で検証者を認証しアサーションを保護するセキュアなプロトコル（TLS など）を使用して、信頼のおけるエンティティが検証結果の利用者に対して認証を行う。

検証者によって生成されたアサーションは 12 時間後に有効期限切れになり、それ以後は検証結果の利用者によって受理されないものとする。

8.2.2.3.長期共有秘密情報の保護

認証用の長期共有秘密情報を使用する場合、加入者と CSP（CSP の一部として運営されている検証者を含む）以外にその情報は決して開示されない。ただし、セッションの（一時的な）共有秘密情報は、CSP が独立した検証者に対して提供される場合がある。

レベル 2 で CSP が使用する共有秘密情報のファイルは、アクセスを管理者およびアクセスを必要とするアプリケーションのみに制限する任意のアクセス制御によって保護される。そのような共有秘密情報ファイルには平文のパスワードまたは秘密を含めないものとする。共有秘密情報を保護する手段の候補は 2 つある。

1. パスワードを salt やユーザ名あるいはその両方に連結したあと、承認されたアルゴリズムを使用してハッシュ処理することにより、盗んだパスワードファイルに対する辞書攻撃や総当り攻撃の計算結果が、ほかの同様のパスワードファイルへの攻撃に役立たなくなる。ハッシュ処理したパスワードはパスワードファイルに格納される。

2. 共有秘密情報を、承認された暗号化アルゴリズムおよびモードを使用して、暗号化された形式で格納し、認証のためにすぐに必要とする場合にのみ、必要な秘密情報を復号する。さらに、レベル 3 または 4 で共有秘密情報を保護するために許可されているすべての手段を、レベル 2 で使用することができる。

8.2.2.4.パスワードの強度

パスワード（または暗証番号）ベースのレベル 2 認証システムでは、パスワードを「*事前に*」知らないが攻撃対象のユーザ名を知っている攻撃者が、オンラインパスワード推測攻撃を成功させる確率が、パスワードの有効期限において 2^{-14}（16,384 分の 1）を超えないものとする。レベル 2 のパスワードの最小エントロピーは少なくとも 10 ビットでなければならない。付録Aに、パスワードのエントロピーを推定することに関する情報が記載されている。

8.2.2.5.実装例

多種多様な技術がレベル 2 の要求事項を満たせるはずである。たとえば、検証者はセキュアな（暗号化された）TLS プロトコルセッション（トンネリング）を通じてパスワードを提示する認証要求者を認証することが考えられる。これにより盗聴攻撃は防止できるが、一般に中間者攻撃や検証者になりすます攻撃を阻止するには不十分である。これは、一般的

な Web ブラウザクライアントには、ユーザをだましたりわなを仕掛けたりするための抜け道が数多く存在するためである。認証に成功したあと、検証者は認証要求者のセキュリティアサーションをセキュアなサーバに格納し、そのアサーションの「ハンドル」を HTTP 参照として検証結果の利用者に送信する。

8.2.3. レベル 3

レベル 3 の認証では、暗号化プロトコルを使用して暗号鍵を所持していることを証明することが基本となる。レベル 3 の認証保証では、一次認証トークン（秘密鍵またはプライベート鍵）を、8.1.1 項に定義されている各種のプロトコル脅威（盗聴、リプレイ攻撃、オンライン推測攻撃、検証者になりすます攻撃、中間者攻撃など）による危殆化から保護する、高い強度を持つ暗号メカニズムが必要となる。また、レベル 3 では 2 要素の認証も必要になる。鍵に加えて、ユーザは鍵を活性化するためにパスワードまたは生体情報を利用しなければならない。

レベル 3 の要求事項を満たすには、次の 3 種類のトークンが使用することができる。

- *ソフト暗号トークン*: 汎用のコンピュータに格納される暗号鍵。FIPS 140-2 のレベル 1 以上で有効性が確認されたハードウェアトークンに鍵を格納し、暗号処理を実行することもできる。認証要求者には、鍵を使用する前に、パスワードまたは生体情報を使用して鍵を活性化することが求められるものとする。あるいは、検証者との認証プロトコルにおいて鍵とパスワードを併せて使用するものとする。パスワードを利用してソフトトークン鍵のロックを解除する場合、その鍵は、レベル 2 認証の要求事項を満たすパスワードから派生した鍵を利用して暗号化された状態で保管するものとし、実際に認証で使用する場合にのみ復号するものとする。あるいは、パスワードプロトコルを検証者に対して使用する場合には、パスワードの使用がレベル 2 の認証保証の要求事項を満たすものとする。

- *ハードトークン*: 特殊なハードウェアデバイスに格納される暗号鍵。トークンは、全体として FIPS 140-2 のレベル 1 以上で有効性が確認されなければならない。認証要求者には、鍵を使用する前に、パスワードまたは生体認証情報を使用して鍵を活性化することが求められるものとする。あるいは、検証者との認証プロトコルにおいて鍵とパスワードを併せて使用するものとする。認証要求者を認証してトークンのロックを解除するのに使用される認証メカニズムは、FIPS 140-2 のレベル 2 のオペレータ認証に関する要求事項を満たしていることが確認されるものとする。あるいは、パスワードプロトコルを検証者に対して使用する場合には、パスワードの使用がレベル 1 の認証保証の要求事項を満たすものとする。

- *ワンタイムパスワードデバイストークン*: 認証は、FIPS 140-2 のレベル 1 以上で有効性が確認された暗号モジュールである個人用のハードウェアデバイスに格納された対称鍵に依存する。このデバイスは、一時的な使い捨ての値と暗号鍵を組み合わせて出力を生成し、その出力は、検証者にパスワードとして送信される。パスワードは 1 回だけ使用され、暗号の手法を用いて生成されるものとする。したがって、盗聴に対する追加保護策は必要ない。デバイスが出力するワンタイムパスワードは、少なくとも 10^6個の値を取る事が可能である。検証者は認証要求者に対して、たとえ

ばTLSサーバを使用して、暗号の手法を用いて認証される必要がある。盗まれたトークンの使用から保護するために、次のいずれかの措置を講じるものとする。

- トークンに対して認証要求者の認証を行うのに使用される認証メカニズムが、FIPS 140-2 のレベル 2 のオペレータ認証の要求事項を確実に満たしている。
- 認証要求者は、ワンタイムパスワードに関する（電子認証）レベル 1 の要求事項を満たしている個人のパスワードを、検証者に送信する。

認証では、認証要求者がセキュアな認証プロトコルを通じて、認証要求者本人がトークンを管理していることを証明する必要がある。認証用の長期共有秘密情報を使用する場合、認証要求者と CSP 以外にその情報が開示されることは決してない。ただし、セッションの（一時的な）共有秘密情報は、CSP が検証者に対して提供する場合がある。承認された暗号化技法がすべての演算において使用されるものとする。

3 種類のトークンが持つ有用性とセキュリティの性質はそれぞれ若干異なる。ソフトトークンによるソリューションは、「シンクライアント」において、TLS とクライアント証明書を使用して容易に実現できる。さらに、このソリューションでは認証要求者の最初の認証だけでなく、セッション全体を、またはセッションにおいてセキュリティが重要となる期間だけ、認証プロセスの実行中に作成された鍵によって、暗号による手法を用いて認証することが可能である。ハードトークンによるソリューションでは、物理トークンという追加保証が提供され、ユーザはトークンが盗まれたかどうかを知ることができる。ソフトトークンと同様に、ハードトークンでは認証要求者の最初の認証だけでなく、セッション全体を、またはセッションにおいてセキュリティが重要となる期間だけ、認証プロセスの実行中に作成された鍵によって、暗号による手法を用いて認証することが可能である。ワンタイムパスワードデバイストークンのシステムは市販されており、携帯性があり、任意のブラウザクライアントで容易に動作する。ハードトークンと同様に、ワンタイムパスワードデバイストークンには、トークンが有形の物理的な実体であるというセキュリティ上の利点がある。加入者は自分のトークンが盗まれたことがわかるはずである。そして、鍵はネットワーク攻撃、ショルダーサーフィン攻撃、またはキーボードスニファ攻撃に対して脆弱ではない。ソフトトークンやハードトークンとは異なり、引き続いて行われるデータ転送を認証するためのセッション鍵は認証プロセスから作成されることはない。

3 種類のトークンはすべて、盗聴に対して同等の強力な暗号による保護をもたらす。それぞれ、各種の攻撃に対して長所と短所がある。3 つのトークンはすべて、レベル 2 のソリューションよりもかなり高い強度を提供する。特定の技術を選択する必要があるレベル 3 の具体的な認証に関する要求事項を実装するアプリケーション実装者は、機能上のニーズと各自のアプリケーションのリスクに最も適したものを選択するべきである。

8.2.3.1. クレデンシャルおよびトークンの有効期限、状態、または失効

CSP は、クレデンシャルが有効であることを検証者や検証結果の利用者が確認できるように、セキュアなメカニズムを提供するものとする。このようなメカニズムとしては、失効リスト、オンライン検証サーバ、有効期間の短いクレデンシャルの使用、あるいは、認証トランザクションにおける状態記録へのアクセスが可能な CSP サーバの関与などがある。共有秘密情報に基づく認証システムでは、失効した加入者を単に検証データベースから削除する場合がある。検証者は、使用するクレデンシャルが有効であることを確認するものとする。

CSP は、クレデンシャルとトークンを 24 時間以内に失効させるための手順を備えるものとする。基本（Basic）、中位（Medium）、高位（High）、または共通証明書ポリシー（Common Certificate Policy）のレベルにおいて、連邦ブリッジ CA と横断認証を行う CA の証明書状態に関する規程は、このレベルにおけるクレデンシャルの状態と失効に関する規程を満たすものと考えられる。

検証者は、信頼するトークンが（24 時間以内に）新規に発行されたものであるか、あるいはまだ有効であるかを確認するものとする。

8.2.3.2.アサーション

検証結果の利用者は次のアサーションを受理することができる。

- 信頼のおけるエンティティ（検証者）によってディジタル署名されたもの。または、
- 信頼のおけるエンティティ（リポジトリや検証者など）から直接取得したもの。その際使用されるプロトコルでは、暗号を用いた手法により検証者を認証し、アサーションを保護するセキュアなプロトコル（TLS など）を使用して、信頼のおけるエンティティが検証結果の利用者に対して認証を行う。

検証者によって生成されたアサーションは 2 時間後に有効期限が切れ、それ以後は検証結果の利用者によって受理されないものとする。

8.2.3.3.長期共有秘密情報の保護

レベル 3 で CSP または検証者が使用する長期共有秘密情報のファイルは、アクセスを管理者およびアクセスを必要とするアプリケーションに限定する、任意のアクセス制御によって保護される。そのような共有秘密ファイルは、下記の項目を満たすように暗号化されるものとする。

1. 共有秘密情報ファイルの暗号鍵は、FIPS 140-2 のレベル 2 以上を満たすことが確認されたハードウェア暗号モジュールか、FIPS 140-2 のレベル 3 または 4 を満たす任意の暗号モジュールに記録された鍵を使用して暗号化され、認証の演算にすぐに必要となる場合にのみ復号される。

2. 共有秘密情報は、FIPS 140-2 のレベル 2 以上を満たすことが確認されたハードウェア暗号モジュールか、FIPS 140-2 のレベル 3 または 4 を満たす任意の暗号モジュールの境界の内側で鍵として保護され、鍵はモジュールから平文で外部にエクスポートされることはない。

3. 共有秘密情報は、暗号秘密情報共有手段によって分割され、*m* 個の別々の検証システムにより保持される。その結果、認証を実行するためには、セキュアなプロトコルを用いて *n* 個（ただし $2 \le n \le m$）のシステムが協調動作する必要があり、攻撃者が *n*-1 個の分割された秘密情報を入手しても、秘密情報に関しては何も得ることができない（恐らく、秘密情報のサイズ以外には）。

CSP では、長期共有秘密鍵から一時的なセッション認証鍵を生成し、それを適切なプロトコルを使用して第三者の検証者に配布することができるが、長期共有秘密情報は、第三者の検証者も含むいかなる第三者とも共有されないものとする。セッション認証鍵は通常、長期共有秘密情報と一時的な値である challenge とを、暗号を用いた手法により組み合わ

せることで生成されるセッション鍵から作成される。challenge とセッション鍵はセキュアな方法により検証者に送信される。検証者は challenge のみを認証要求者に送り、認証要求者はその challenge を長期共有秘密情報に適用してセッション鍵を生成する。これで、認証要求者と検証者の双方がセッション鍵を共有し、認証に使用することができるようになる。このようなプロトコルはこのレベルにおいては、すべての鍵が少なくとも 80 ビットのエントロピーを保っていて、すべての演算に承認された暗号化アルゴリズム（AES、SHA-1、SHA256、HMAC など）が使用される場合にのみ許可される。

8.2.3.4.実装例

レベル 3 の保証は、公開鍵証明書を持つ認証要求者とのあいだでのクライアントが認証された TLS（最近のすべてのブラウザに実装されている）によって満たすことができる。同様の性質を持つほかのプロトコルも使用することができる。レベル 3 の認証保証は、ワンタイムパスワードデバイスの出力とレベル 1 の個人パスワードを、TLS セッションを通じてトンネリングすることによって満たすこともできる。

8.2.4. レベル 4

レベル 4 は、リモートネットワーク認証に対する実用上最大限の保証を提供することを目的とする。レベル 4 の認証では、暗号プロトコルを通じて鍵の所持を証明することが基本となる。レベル 4 はレベル 3 に似ているが、「ハード」暗号化トークンのみが許可され、暗号モジュールの有効性確認に関する FIPS 140-2 の要求事項が厳しくなっているほか、認証後の重要なデータ転送を認証プロセスに結び付けられた鍵を通じて認証しなければならない点がレベル 3 と異なる。トークンは、全体として FIPS 140-2 のレベル 2 以上で有効性が確認されているハードウェア暗号モジュールとし、少なくとも FIPS 140-2 のレベル 3 の物理セキュリティを備えたものとする。容易に複製できない物理トークンを要求することにより、また、FIPS 140-2 ではレベル 2 以上のオペレータ認証が要求されるため、このレベルでは適切な 2 要素によるリモート認証が保証される。

レベル 4 では、すべての当事者、および当事者間でのすべての機密データの転送について、強力な暗号認証が求められる。公開鍵または対称鍵のどちらの技術も利用できる。認証では、認証要求者がトークンを管理していることをセキュアな認証プロトコルを通じて認証要求者が証明することが要求される。前述の 8.1.1 項で定義されているプロトコル脅威（盗聴、リプレイ攻撃、オンライン推測攻撃、検証者になりすます攻撃、中間者攻撃）が阻止されるものとする。また、トークンは、前述の 8.1.3 項に記述した悪意のあるコードの脅威による危殆化から秘密情報を保護するものとする。認証用の長期共有秘密情報を使用する場合、認証要求者と CSP 以外にその情報が開示されることは決してない。ただし、CSP がセッションの（一時的な）共有秘密情報を、検証者または検証結果の利用者に提供する場合がある。承認された強力な暗号化技法がすべての演算において使用されるものとする。機密データの転送はすべて、認証プロセスにおいて得られた鍵を使用して、暗号を用いた手法により認証されるものとする。

8.2.4.1.クレデンシャルおよびトークンの有効期限、状態、または失効

CSP は、クレデンシャルが有効であることを検証者や検証結果の利用者が確認できるように、セキュアなメカニズムを提供するものとする。このようなメカニズムとしては、失効リスト、オンライン検証サーバ、有効期間の短いクレデンシャルの使用、あるいは、認証トランザクションにおいて状態記録へのアクセスが可能な CSP サーバの関与などがある。共有

秘密情報に基づく認証システムでは、単に失効した加入者が検証データベースから削除される。検証者は、使用するクレデンシャルが新規に発行されたものであること、あるいは有効であることを確認するものとする。

CSPは、クレデンシャルを 24 時間以内に失効させるための手順を備えるものとする。検証者または検証結果の利用者は、信頼するクレデンシャルが（24 時間以内に）新規に発行されたものであるか、あるいはまだ有効であるかを確認するものとする。高位（High）および共通証明書ポリシー（Common Certificate Policy）のレベルにおいて、連邦ブリッジCAと横断認証を行うCAの証明書状態の規程は、レベル 4 におけるクレデンシャルの状態の規程を満たすものとみなされる[FBCA1]。

このレベルでは、機密データの転送は、認証プロセスに結び付けられた鍵を通じて、暗号を用いた手法により認証されるものとする。元の認証処理中に得られた一時的な鍵または有効期限の短い鍵はすべて、最初の認証から 24 時間以内に期限切れとなり、再認証が必要になるものとする。

8.2.4.2.長期共有秘密情報の保護

レベル 4 でCSPまたは検証者が使用する長期共有秘密情報のファイルは、レベル 3 の長期共有秘密情報と同じ方法（前述の8.2.3.3項で規定した方法）で保護するものとする。

8.2.4.3.実装例

レベル 4 の保証は、公開鍵ハードトークンを持つ認証要求者とのあいだでの、クライアントが認証された TLS（最近のすべてのブラウザに実装されている）によって満たすことができる。同様の性質を持つほかのプロトコルも使用することができる。

9. レベル別の技術的要求事項のまとめ

本セクションでは、レベルごとの技術的要求事項を表形式でまとめて説明する。表 2 に、各認証保証レベルにおいて使用することのできるトークンの種類を示す。表 3 に、各レベルで必要となる保護を示す。保護は前述の8.1.2項で定義している。表 4 に、オンラインでのパスワード推測攻撃に対するパスワードの耐性に関する要求事項をまとめて示す。表 5 に、各保証レベルに適用可能な認証プロトコルの種類を示す。表 6 に、各レベルでそのほかに必要なプロトコルとシステムプロパティを示す。

表 2:各保証レベルで使用することができるトークンの種類

トークンの種類	レベル 1	レベル 2	レベル 3	レベル 4
ハード暗号トークン	√	√	√	√
ワンタイムパスワードデバイス	√	√	√	
ソフト暗号トークン	√	√	√	
パスワードおよび暗証番号	√	√		

表 3:必要な保護

保護の対象となる攻撃	レベル 1	レベル 2	レベル 3	レベル 4
オンライン推測	√	√	√	√
再現	√	√	√	√
盗聴		√	√	√
検証者なりすまし			√	√
中間者			√	√
セッションハイジャック				√

表 4:オンラインパスワード推測に対する最小限の耐性

攻撃の種類	レベル 1	レベル 2
標的を定めた攻撃:ユーザ名以外に「*事前に*」何も知らない攻撃者が、パスワードの有効期限にわたって、選択したユーザのパスワードを推測する最大の確率	2^{10}分の 1（1/1024）	2^{14}分の 1（1/16384）
標的を定めない攻撃:最小エントロピー	-	10 ビット

表 5:認証プロトコルの種類

プロトコルの種類	レベル 1	レベル 2	レベル 3	レベル 4
プライベート鍵 PoP	√	√	√	√
対称鍵 PoP	√	√	√	√
トンネルされたパスワードまたはゼロ知識パスワード	√	√		
challenge-response パスワード	√			

表 6:そのほかの必要なプロパティ

必要なプロパティ	**レベル 1**	**レベル 2**	**レベル 3**	**レベル 4**
検証者または CSP によって第三者に開示されない共有秘密情報		√	√	√
複数要素の認証			√	√
認証される機密データ転送				√

9.1.1. 電子認証の保証レベルに対する PKI ポリシーの関係

一般に、政府機関は、共通ポリシーフレームワーク（Common Policy Framework）[FBCA3]に規定されているポリシーに基づいて証明書を発行することにより FIPS 201 を満たしている。表 7 に、これらのポリシーのもとで発行される証明書が電子認証の保証レベルにどのように対応するのかを示す。ここでは「*カード認証*」と「*共通デバイス*」のポリシーは挙げていない。これらのポリシーは人ではなくシステムまたは暗号モジュールの認証をサポートする。

表 7：電子認証の保証レベルと共通ポリシーフレームワーク

電子認証のレベル	選択されたポリシーコンポーネント			全体的な等価性
	身元識別情報の検証	トークン	状態の報告	
レベル 2	Common-Auth、Common-SW、Common-HW、Common-High Certificate Policies（共通-認証、共通-ソフトウェア、共通-ハードウェア、共通-高位証明書ポリシー）	Common-Auth、Common-SW、Common-HW、Common-High Certificate Policies（共通-認証、共通-ソフトウェア、共通-ハードウェア、共通-高位証明書ポリシー）	Common-Auth、Common-SW、Common-HW、Common-High Certificate Policies（共通-認証、共通-ソフトウェア、共通-ハードウェア、共通-高位証明書ポリシー）	Common-Auth、Common-SW、Common-HW、Common-High Certificate Policies（共通-認証、共通-ソフトウェア、共通-ハードウェア、共通-高位証明書ポリシー）
レベル 3	Common-Auth、Common-SW、Common-HW、Common-High Certificate Policies（共通-認証、共通-ソフトウェア、共通-ハードウェア、共通-高位証明書ポリシー）	Common-Auth、Common-SW、Common-HW、Common-High Certificate Policies（共通-認証、共通-ソフトウェア、共通-ハードウェア、共通-高位証明書ポリシー）	Common-Auth、Common-SW、Common-HW、Common-High Certificate Policies（共通-認証、共通-ソフトウェア、共通-ハードウェア、共通-高位証明書ポリシー）	Common-Auth、Common-SW、Common-HW、Common-High Certificate Policies（共通-認証、共通-ソフトウェア、共通-ハードウェア、共通-高位証明書ポリシー）
レベル 4	Common-Auth、Common-SW、Common-HW、Common-High Certificate Policies（共通-認証、共通-ソフトウェア、共通-ハードウェア、共通-高位証明書ポリシー）	Common-Auth、Common-HW、Common-High Certificate Policies（共通-認証、共通-ハードウェア、共通-高位証明書ポリシー）	Common-Auth、Common-SW、Common-HW、Common-High Certificate Policies（共通-認証、共通-ソフトウェア、共通-ハードウェア、共通-高位証明書ポリシー）	Common-Auth、Common-HW、Common-High Certificate Policies（共通-認証、共通-ハードウェア、共通-高位証明書ポリシー）

PKI 技術を早くから採用している政府機関、および連邦政府以外の組織では、共通ポリシーフレームワークではなく組織固有のポリシーのもとで、PKI 証明書を発行する。組織固有のポリシーのもとで発行される公開鍵証明書によって提供される保証を評価するための主な手段は、連邦ポリシー機関のポリシーを連邦ブリッジ CA のポリシーに対応付けることである。これらのポリシーには、[FBCA1]に規定されている Rudimentary（初歩）、Basic（基本）、Medium（中位）、Medium-HW（中位-ハードウェア）、High（高位）の各保証ポリシーと、[FBCA2]に規定されている Citizen and Commerce Class（市民および商業クラス）ポリシーがある。表 8 に、これらの証明書ポリシーが電子認証の保証レベルにどのように対応しているのかを示す。レベル 2 では、連邦ポリシー機関によってまだ対応付けられていないものの、レベル 2 における身元識別情報の検証、トークン、状態の報告の各要求事項を満たすこと確認されたポリシーのもとで発行された証明書を政府機関が使用することもできる。

表 8：電子認証の保証レベルと PKI 証明書ポリシーの対応関係

電子認証のレベル	選択されたポリシーコンポーネント			全体的な等価性
	身元識別情報の検証	トークン	状態の報告	
レベル 2	Basic（基本）、Citizen and Commerce Class（市民および商業クラス）、Medium（中位）、Medium-HW（中位-ハードウェア）、または High（高位）の証明書ポリシー、あるいは、レベル 2 における身元識別情報の検証に関する要求事項を満たすそのほかのポリシー	Rudimentary（初歩）、Basic（基本）、Citizen and Commerce Class（市民および商業クラス）、Medium（中位）、Medium-HW（中位-ハードウェア）、または High（高位）の証明書ポリシー、少なくとも 1,024 ビットの RSA 鍵と SHA1 あるいはそれと同等なものを持つ任意の証明書	Basic（基本）、Citizen and Commerce Class（市民および商業クラス）、Medium（中位）、Medium-HW（中位-ハードウェア）、または High（高位）の証明書ポリシーまたは証明書で、ほかの CA により発行され、72 時間以内の CRL あるいは失効サイクルを持つもの	Basic（基本）、Citizen and Commerce Class（市民および商業クラス）、Medium（中位）、Medium-HW（中位-ハードウェア）、または High（高位）の証明書ポリシー、あるいは、レベル 2 のすべての要求事項を満たすそのほかのポリシー
レベル 3	Basic（基本）、Medium（中位）、Medium-HW（中位-ハードウェア）、または High（高位）の証明書ポリシー	Rudimentary（初歩）、Basic（基本）、Citizen and Commerce Class（市民および商業クラス）、Medium（中位）、Medium-HW（中位-ハード	Basic（基本）、Medium（中位）、Medium-HW（中位-ハードウェア）、または High（高位）の証明書ポリシー	Basic（基本）、Medium（中位）、Medium-HW（中位-ハードウェア）、または High（高位）の証明書ポリシー

		ウェア）、または High（高位）の証明書ポリシー		
レベル 4	Medium（中位）、Medium-HW（中位-ハードウェア）、または High（高位）の証明書ポリシー	Medium-HW（中位-ハードウェア）、または High（高位）の証明書ポリシー	Medium（中位）、Medium-HW（中位-ハードウェア）、または High（高位）の証明書ポリシー	Medium-HW（中位-ハードウェア）、または High（高位）の証明書ポリシー

連邦政府 PKI にはまた、連邦政府以外の PKI を認識できるように、Medium Commercial Best Practices（Medium-CBP：中位 CBP）および Medium Hardware Commercial Best Practices（MediumHW-CBP：中位-ハードウェア CBP）の 2 つのポリシーも追加されている。電子認証のレベルから見た場合、Medium CBP および MediumHW-CBP はそれぞれ Medium および Medium-HW に相当する。

10.参考文献

10.1. 全般に関する参考文献

[DOJ 2000] Guide to Federal Agencies on Implementing Electronic Processes (November 2000), available at:http://www.usdoj.gov/criminal/cybercrime/ecommerce.html

[OCC] Customer Identification Programs for Banks, Savings Associations, Credit Unions and Certain Non-Federally Regulated Banks. Office of the Comptroller of the Currency, 12 CFR Part 21. May 2003. Available at: http://www.fdic.gov/regulations/laws/federal/03joint326.pdf

http://www.treas.gov/press/releases/reports/326finalrulebanks.pdf

[OMB 04-04] OMB Memorandum M-04-04, E-Authentication Guidance for Federal agencies, December 16, 2003, available at: http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

[OMB 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: http://www.whitehouse.gov/omb/memoranda/m03-22.html.

[KERB] Neuman, C., and T. Ts'o, Kerberos:An Authentication Service for Computer Networks, IEEE Communications, vol. 32, no.9, 1994.

[RFC 1939] IETF, RFC 1939, Post Office Protocol - Version 3, May 1996, available at:http://www.ietf.org/rfc/rfc1939.txt

[RFC 2246] IETF, RFC 2246, *The TLS Protocol, Version 1.0*.January 1999, available at:http://www.ietf.org/rfc/rfc2246.txt

[RFC2560] IETF, RFC 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, available at:http://www.ietf.org/rfc/rfc2560.txt

[RFC 3280] IETF, RFC 3280, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, available at:http://www.ietf.org/rfc/rfc3280.txt

[RFC 3546] IETF, RFC 3546, Transport Layer Security (TLS) Extensions, June 2003, available at:http://www.ietf.org/rfc/rfc3546.txt

[SKEY] IETF, RFC 1760, The S/KEY One Time Password System, February 1995, available at:http://www.ietf.org/rfc/rfc1760.txt

10.2. NIST ITL Bulletin

NIST ITL Bulletin は http://csrc.nist.gov/publications/nistbul/index.html から入手できる。電子認証を必要とする応用事例のシステムを実装する場合は、次の公報が特に参考になると考えられる。

[ITL Dec02] ITL Bulletin, *Security of Public Webservers*, Dec. 2002

[ITL July02] ITL Bulletin, *Overview:The Government Smartcard Interoperability Specification*, July 2002

[ITL Jan02] ITL Bulletin, *Guideline on Firewalls and Firewall Policy*, January 2002

[ITL Feb00] ITL Bulletin, *Guideline for Implementing Cryptography in the Federal Government*, February 2000

[ITL Dec99] ITL Bulletin, *Operating System Security:Adding to the Arsenal of Security Techniques*, December 1999

[ITL Nov99] ITL Bulleting, *Acquiring and Deploying Intrusion Detection Systems*, November 1999

[ITL Sep99] ITL Bulletin, *Securing Web Servers*, September 1999

[ITL May99] ITL Bulletin, *Computer Attacks:What They Are and How to Defend Against Them*, May 1999

10.3. NIST Special Publication（NIST SP シリーズ文書）

NIST 800 シリーズの Special Publication は http://csrc.nist.gov/publications/nistpubs/index.html から入手できる。電子認証を必要とするアプリケーションを提供するシステムを導入する人にとって、次の刊行物が特に参考になるだろう。

[SP 800-31] NIST Special Publication, 800-31, *Intrusion Detection Systems (IDS)*, November 2001

[SP 800-32] NIST Special Publication, 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, February 2001

[SP 8000-33] NIST Special Publication 800-33, *Underlying Technical Models for Information Technology Security*, December 2001

[SP 800-40] NIST Special Publication 800-40, *Procedures for Handling Security Patches*, September 2002

[SP 800-41] NIST Special Publication 800-41, *Guidelines on Firewalls and Firewall Policy*, January 2002

[SP 800- 42] NIST Special Publication 800-42, *Guideline on Network Security Testing*, draft

[SP 800-43] NIST Special Publication 800-43, *Guide to Securing Windows 2000 Professional*, November 2002

[SP 800-44] NIST Special Publication 800-44, *Guidelines on Securing Public Web Servers*, September 2002

[SP 800- 47] NIST Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, September 2002

[SP 800- 52] NIST Special Publication 800-52, Guidelines for the Selection and Use of Transport Layer Security Implementations, draft.

10.4. FIPS (連邦情報処理規格)

FIPSはhttp://csrc.nist.gov/publications/fips/ から入手できる。

[FIPS 46-3] Federal Information Processing Standard Publication 46-3, *Data Encryption Standard (DES)*, NIST, October 25, 1999

[FIPS 140-2] Federal Information Processing Standard Publication 140-2, *Security Requirements for Cryptographic Modules*, NIST, May 25, 2001

[FIPS 180-2] Federal Information Processing Standard Publication 180-2, *Secure Hash Standard (SHS)*, NIST, August 2002.

[FIPS186-2] Federal Information Processing Standard Publication 186-2, *Digital Signature Standard (DSS)*, NIST, June 2000.

[FIPS 197] Federal Information Processing Standard Publication197, *Advanced Encryption Standard (AES)*, NIST, November 2001.

[FIPS 198] Federal Information Processing Standard Publication 198, *Keyed-Hash Message Authentication Code (HMAC)*, NIST, March 2002.

10.5. 証明書ポリシー

次の証明書ポリシーはhttp://www.cio.gov/fpkipa/policies.htm から入手できる。

[FBCA1] *X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA)*, Version 2.1 January 12, 2006. Available at http://www.cio.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf

[FBCA2] *Citizen & Commerce Certificate Policy*, Version 1.0 December 3, 2002. Available at http://www.cio.gov/fpkipa/documents/citizen_commerce_cpv1.pdf

[FBCA3] *X.509 Certificate Policy for the Common Policy Framework*, Version 2.4 February 15, 2006. Available at http://www.cio.gov/fpkipa/documents/CommonPolicy.pdf

付録 A:パスワードのエントロピーと強度の推定

情報理論において「エントロピー[5]」という用語の使用を考案したのはClaude Shannonである。この概念は情報理論や通信に数多く応用されており、Shannonは英語の文字列における実際の情報量を表すためにもこの概念を応用した。以下はShannonの文献からの引用である。「エントロピーは、ある意味では、言語の文章の各文字についてどの程度の情報量が平均として生成されるのかを測る統計パラメータである。言語を最も効率的な方法で 2 進数(0 または 1)に変換した場合、エントロピーHは、元の言語の 1 文字あたりに必要な 2 進数の平均数である」[6]。

この意味でのエントロピーは、熱力学でのこの用語の使い方に漠然と関連している程度にすぎない。確率分布関数の観点から見たエントロピーの数学的な定義は次のとおりである。

$$H(X) := -\sum_{x} P(X = x) \log_2 P(X = x)$$

ここで、$P(X=x)$は変数 X が値 x を取りうる確率である。

Shannon は通常の英語の文字列に着目し、それらを可能な限り効率的な方法で符号化するのに何ビット必要であるかに関心を寄せた。Shannon がこの用語を考案して以来、暗号の分野では、パスワードまたは鍵を推測または特定する難しさを示す尺度として「エントロピー」という用語が使用されている。特定のサイズにおける最も強力な鍵またはパスワードは、真にランダムな選択であることは明らかであり、平均として、そのような選択は圧縮できないこともまた明らかである。しかし、圧縮が鍵やパスワードの強度を示す最善の測定値であることが明らかであるとは言えないため、暗号の専門家たちは、「推測エントロピー」や「最小エントロピー」といったエントロピーの代替となる尺度をいくつも考案している。パスワードの分布に応用される推測エントロピーとは、大まかにいえば、特定のユーザのパスワードを推測するのに必要となる作業の平均量の推定値のことである。また、最小エントロピーとは、母集団の中から最も容易に推測できる単一のパスワードを推測する難しさを示す尺度のことである。

一連の特定の規則のもとで選択されるパスワードの度数分布が十分に分かっていれば、いかなるパスワードについても推測エントロピーあるいは最小エントロピーを知ることは容易である。パスワードの分布を知っている攻撃者ならば、選択したユーザについて、最初に最も可能性の高いパスワードを試し、次に 2 番目に可能性の高いパスワードを試す、というように、成功するパスワードが見つかるまで可能性の高い順からパスワードを試すことによって、選択したユーザのパスワードを見つけることができる。すべてのパスワードを対象にしたときの平均が、推測エントロピーということになる。任意のユーザのパスワードを見つけることができればよいという攻撃者であれば、いくぶん異なる戦法をとると予想される。つまり、すべてのユーザ名を対象に最も可能性の高いパスワードを試し、次に、すべてのユ

[5] C. E. Shannon, “A mathematical Theory of Communication,” *Bell System Technical Journal*, v. 27, pp. 379-423, 623-656, July, October 1948、http://cm.bell-labs.com/cm/ms/what/shannonday/paper.htmlを参照のこと
[6] C. E. Shannon, “Prediction and Entropy of Printed English”, *Bell System Technical Journal*, v.30, n. 1, 1951, pp. 50-64.

ーザ名を対象に 2 番目に可能性の高いパスワードを試す。以下同様に試行を続け、最初に「当たり」となるものを見つけるのである。これに対応するのが最小エントロピーである。

残念ながら、特定の規則のもとでユーザが選択するパスワードに関する十分なデータはなく、われわれが実際に知っていることのほとんどは、システム管理者が自分のシステムにあるハッシュ処理されたパスワード（ほとんどのシステムでは、パスワードは平文では保管されない）のファイルを対象に、大量の辞書攻撃を仕掛けてパスワードを「クラッキング」することにより経験的に発見されたものである。NIST では、ユーザが実際に選択するパスワードに関して、より詳しいデータを入手したいと考えている。しかし、データを保持しているシステム管理者は、当然ながら他人にパスワードデータを開示することには前向きではない。経験およびたまたま得られたデータが示すところでは、ユーザの多くが、システムで許される場合には、ひじょうに推測しやすいパスワードを選択している。

A.1 ランダムに選択するパスワード

ここで用語として使用している「エントロピー」は、パスワードの値の不確実性を示している。パスワードのエントロピーは、慣習的にビットで表現される。kビットのパスワードを無作為に選択すると、取り得る値は 2^k通りある。この場合、パスワードはkビットのエントロピーを持つ、という。長さがl文字のパスワードをb個の文字で構成されるアルファベット（たとえば、通常のキーボードには 94 個の印字可能なISO文字が刻印されている）から無作為に選択した場合、パスワードのエントロピーはb^lである。たとえば、94 個の印字可能なISO文字から選択した 8 文字で構成されるパスワードの場合、エントロピーは $94^8 \approx 6.09 \times 10^{15}$となる。これはおよそ 2^{52}であり、このパスワードは約 52 ビットのエントロピーを持つ、という。ランダムに選択したパスワードの場合、推測エントロピー、最小エントロピー、およびShannonのエントロピーは、いずれも同じ値になる。エントロピーHは次の一般公式で与えられる。

$$H = \log_2 (b^l)$$

表 A.1 に、標準的な 94 個のキーボード文字（スペース文字は除く）から無作為に選択して生成されるパスワードの文字数と、それに対応するエントロピーを示す。ほかのアルファベットから無作為に選択するパスワードの計算は単純である。

A.2 ユーザが選択するパスワード

ユーザが自分で選択するパスワードのエントロピーを推定することはずっと難しい。これは、無作為に選択されるものではなく、一様にランダムな分布にならないためである。おそらく、ユーザが選択するパスワードは、通常の英語の文字列の傾向や文字の度数分布をおおむね反映し、ユーザ自身が覚えておけるものが選択されると考えられる。経験的に、多くのユーザは自由にパスワードが選べる場合には、容易に推測できるパスワードを選ぶ。そして、ユーザがよく選択する数千のパスワードを収めたかなり小さな辞書であっても、ユーザが実際に選択したパスワードと突き合わせると、それらのパスワードの多くを「クラックする（破る）」ことができる。

A.2.1 推測エントロピーの推定

推測エントロピーは、標的を定めた帯域内パスワード推測攻撃に対する耐性を大きく左右するので、パスワードシステムの強度を測る最も重要な尺度であるといえる。

本指針では、ユーザが選択するパスワードのエントロピーを推定するための出発点として、通常の英語の文字列のエントロピーを推定する Shannon の方法を使用することにした。ここでパスワードがほかの英語の文字列ときわめて似ているとするのは大きな仮定である。本来は、さまざまな組み合わせ規則に従ってユーザが選択した実際のパスワードの大きな標本を基礎にするのがよいのだが、そのような情報源は存在しないので、Shannon の手法を利用しておおよその推定をするのが少なくとも妥当である。以降で説明する規則は、電子認証の目的に用いるきわめて大まかな経験則として解釈されるべきものに過ぎないことに注意されたい。

Shannon は、被験者に英語の文字列を提示し、文字列の次の文字を推測してもらうという実験を行った。この結果に基づき、文字列に続く各文字のエントロピーを推定した。彼は、通常の英語の小文字にスペース文字を加えた、27 文字で構成されるアルファベットを使用した。

以降の議論で想定するパスワードは、通常のキーボードに刻印されている 94 個の印字可能なアルファベット文字からユーザが選択した文字で構成され、長さが少なくとも 6 文字であるものとする。Shannon は 27 文字で構成されるアルファベットを使用したので、ユーザが選択するパスワードのエントロピーはずっと大きくなると思われるかもしれない。しかし、ここではユーザは小文字以外を選択するよう強制されない限り、ほとんど小文字だけのパスワードを選択するものと仮定する。また、大文字やアルファベット以外の文字を含めるよう強制するという規則は、通常はごく単純かつ予測可能な方法によって満たされるものしている。たとえば、通常の英語のように先頭を大文字にして末尾に句読点や特殊な文字を添えたり、あるいはなんらかの簡単な置き換え（文字「s」を$に置き換えるなど）を行ったりすることで満たされることが多い。さらに、パスワードを高度にランダムなものになるよう強制するという規則は逆効果を生む。これは、そうした規則によってパスワードが覚えにくくなるためである。そうするとユーザはパスワードを書き留め、すぐに参照できる（つまり安全でない）場所に置く。たとえば、コンピュータディスプレイに貼り付けるなどする。したがって、27 文字だけで構成されるアルファベットを想定し、単純な英語の文字列のエントロピーを推定することから始めるのは妥当である。

Shannonは、文字の確率分布が一様でないものの、英語の文字列の最初の文字を予測することは比較的困難であるが、最初の文字がわかれば 2 番目の文字はずっと容易に推測でき、最初の 2 文字がわかれば 3 番目の文字はさらに容易に推測でき、以下同様であることを発見した。彼は、最初の文字記号のエントロピーが 4.6～4.7 ビットであり、8 文字目以降は 1.5 ビット程度まで低下すると概算した。ひじょうに長い英語の文字列（たとえばShakespeareの作品集など）の場合、1 文字あたりのエントロピーは 0.4 ビットしかないと推定されている[7]。同様に、単語の文字列の場合、最初の文字を予測することは以降の文字を予測するよりも難しく、最初の文字は 5 文字目以降の文字のおよそ 6 倍の情報量を持つ[8]。

[7] Thomas Schurmann and Peter Grassberger, “Entropy estimation of symbol sequences,” http://arxiv.org/ftp/cond-mat/papers/0203/0203436.pdf
[8] *ibid.*

パスワードを見つけ出そうとする攻撃者は、まず、選択される可能性が最も高いパスワードから試す。この目的のために、ひじょうに大規模なパスワード辞書が作られている。ユーザは一般的な単語やひじょうに単純なパスワードを選択することが多いため、システムではパスワードの選択に対していくつかの規則を課すのがふつうである。そうすることで、「不適切」なパスワードの選択を防ぎ、こうした辞書攻撃や規則に基づいたパスワード推測攻撃に対して、ユーザが選択するパスワードの耐性を高める。本指針ではこれらの規則を次の 2 つに分類する。

1. 辞書テスト。パスワード候補を対象に、一般的な単語や一般に使用されているパスワードからなる「大規模な辞書テスト」を実施して、辞書のなかで見つかったパスワードを許可しない。ここでは辞書テストについて厳密な定義はしない。パスワードの長さと規則に応じてカスタマイズする必要があるからである。ただし、辞書テストは、英語の大辞典に記載されている任意の単語を単純に変形したようなパスワードの選択を防止するものとする。また、少なくとも 50,000 語の単語が含まれているべきである。長いパスワード（フレーズに基づく 16 文字以上のパスワード）の選択を禁止する理由はなく、そのような 16 文字以上の長いパスワードに対して辞書テストを課す必要もない。
2. 組み合わせ規則。通常は、小文字、大文字、およびアルファベット以外の記号（たとえば、;: “~!@#$%^&*()_-+={}[]|\:;’<,>.?/1234567890”）を含むパスワードを選択するよう、ユーザに求める。

辞書テストと組み合わせ規則のいずれによっても、パスワードのいくつかの候補が排除され、攻撃者が推測攻撃や総当り攻撃でパスワードを見つけ出すために試さなければならない文字列の範囲が狭くなる。しかし、数多くの明白な選択肢を削減することができるので、パスワードの「実用上のエントロピー」が全般的に高くなるものと考えられる。もっとも、徹底した総当り攻撃に必要な作業も減ることになる。辞書検査では、よく選択されるパスワードを排除するために選択された、少なくとも 50,000 語の正当なパスワードで構成される辞書が必要である。パスワード候補の大文字は、比較の前に小文字に変換する。

表 A.1 に、ユーザが選択するパスワードについて推定されるエントロピーのおおよその平均を、パスワード長の関数として示す。通常のキーボードのアルファベットから選択すること以外に規則を設けなかった場合にユーザが選択するパスワード、一般的な単語や一般に選択されるパスワードの使用を防止する辞書検査を受けたパスワード、および、組み合わせ規則と辞書テストの両方の対象となったパスワードのそれぞれについて推定を行った。また、10 桁のアルファベットで構成されるパスワードや暗証番号についても推定を行った。表ではまた、無作為に選択したパスワードと暗証番号のエントロピーも算出している。表 A.1 の値を絶対的なエントロピーの正確な推定値として解釈するべきではない。しかし、ユーザが選択するパスワードのエントロピーの相対的な推定の概算値を示し、パスワード強度の基準を設ける際の一定の基礎にはなる。

キーボードのすべてのアルファベットからユーザが選択するパスワードについて、表 A.1 の計算の過程を以下に示す。

- 1 文字目のエントロピーは 4 ビットとする。

- 次の 7 文字のエントロピーは 1 文字あたり 2 ビットである。これは、「最大 8 文字までの文字列に及ぼす統計的な効果を考慮した場合、エントロピーは 1 文字あたりおよそ 2.3 ビットである」という Shannon の推定とおおむね一致している。
- 9 文字目から 20 文字目までについては、エントロピーは 1 文字あたり 1.5 ビットとする。
- 21 文字目以降の文字については、エントロピーは 1 文字あたり 1 ビットとする。
- 大文字とアルファベット以外の文字の両方を要求する組み合わせ規則には、6 ビットのエントロピーが「ボーナス」として割り当てられる。この規則ではこれらの文字の使用が強制されるが、多くの場合、これらの文字が出現するのはパスワードの先頭または末尾だけである。探索の範囲が全体としていくぶん減少するので、この規則のメリットはおそらく控えめなものであり、パスワードの長さとはほとんど関係がない。
- 大規模な辞書検査を受ける場合は、さらに最大 6 ビットのボーナスエントロピーが加算される。攻撃者が辞書を知っていれば、そこに含まれているパスワードのテストを避けられるが、いずれにしても攻撃者は辞書の大部分を推測することができるだろう。しかし、それらは辞書規則がない場合に選択される可能性が最も高いパスワードである。ここでの仮定は、辞書テストを受けた場合の推測エントロピーの利点のほとんどは、比較的短いパスワードに集約されるというものである。なぜなら、覚えておくことのできる長いパスワードは必然的に辞書の単語で構成される「パスフレーズ」だからである。そのため、20 文字の時点でボーナスは 0 ビットまで減る。

ユーザが選択する暗証番号の場合、表 A.1 の前提は、少なくともすべて同じ数字からなる番号や、連続する数字の並び（「1234」や「76543」など）で構成される暗証番号の選択を防ぐ規則が適用されるというものである。表 A.1 のこの欄は、よくてもひじょうにおおまかな推定であり、パスワードクラッカの経験が示すところでは、ユーザは単純な数字パターンや最近の日付（たとえば、誕生年など）を優先的に選択することが多い。

A.2.2 最小エントロピーの推定

経験が示すところでは、かなり多くのユーザがひじょうに推測されやすいパスワードを選択する。システムで許されていれば、「password」がパスワードとして最もよく選択される可能性がある。たとえば、1,000 人のうち 1 人のユーザが、最も一般的な 2 つのパスワードのうちの 1 つを選択するとする。また、パスワードを試せるのは 3 回までで、以降はシステムがパスワードをロックするものとする。ユーザ名の一覧を入手し、最もよく選択される 2 つのパスワードを知っている攻撃者は、ユーザ名ごとにその 2 つのパスワードを試す自動攻撃を行うことができる。700 人分のユーザ名に対し 2 つのパスワードを試せば 2 回のうち 1 回はどちらかが当たることを期待できる。選択した特定のユーザになりすますのではなく、システムへのアクセスだけが目的であれば、明らかにこうした攻撃は実際的である。こうした可能性を無視することは、通常はあまりにも危険である。

パスワードシステムの規則に従ってユーザが実際に選択するパスワードを詳しく調査せずに、ユーザが選択するパスワードの実際の最小エントロピーを正確に推定する汎用的な手段はわれわれの知る範囲では存在しない。しかし、規則がない場合に一般的に選択される正当なパスワードで構成される大規模な辞書を使用して、ユーザが選択したパスワードをテストし、一致するものの使用を禁止すれば、パスワードの最小エントロピーが上昇すると考えるのは妥当である。ここでは、少なくとも 10 ビットの最小エントロピーを保証することを目的として、辞書テストを規定する。テストは次のようなものである。

- パスワード内の大文字をすべて小文字に変換し、規則がない場合に一般に選択される正当なパスワードを少なくとも 50,000 個含む辞書と比較して、辞書項目と一致する場合は却下する。そして、
- ユーザ名の並べ替えとして認識できるパスワードの使用を禁止する。

このテストは少なくとも 10 ビットの最小エントロピーを保証するものと推定される。ほかの手段によって、少なくとも 10 ビットの最小エントロピーが保証することもできる。ユーザが選択した少なくとも 15 文字からなるパスワードは、少なくとも 10 ビットの最小エントロピーを持つとみなせる。たとえば、無作為に選択された 2 文字からなる短い文字列をユーザが提示されることが考えられる（94 文字のアルファベットから無作為に選択された 2 文字は、およそ 13 ビットのエントロピーを持つ）。パスワードとして、たとえばシステムによって選択された短い無作為の要素を、10 ビットの最小エントロピーを保証するために、それよりも長い、ユーザが選択したパスワードに組み合わせることができる。

A.2 そのほかの種類のパスワード

顔写真などのいくつかの画像を記憶するようにユーザに求めるパスワードシステムもある。以降、一般的にはユーザに対していくつかの画像（一般的には一度に 9 枚）で構成される連続するフィールドが提示される。フィールドにはそれぞれ記憶した画像の 1 つが含まれている。選択するそれぞれの画像のエントロピーは約 3.17 ビットである。このようなシステムで、5 回分の画像を記憶して用いるとすれば、システムのエントロピーはおよそ 16 ビットになる。これは無作為に選択されるパスワードであるため、推測エントロピーと最小エントロピーはどちらも同じ値である。

無作為に選択される要素とユーザが選択する要素を組み合わせて、1 つの複合パスワードにすることが可能である。たとえば、最小エントロピーを保証するために、無作為に選択される短い値をユーザに提示し、それをユーザが選択するパスワード文字列と組み合わせて使用することが考えられる。この無作為の構成要素としては画像や文字列が考えられる。

A.3 例

本指針では、パスワード認証システムを設計する設計者や実装者に対して自由度を与えることを意図している。システム設計者は、攻撃者がパスワードを試せる回数を制限するために設けられている、パスワードの長さ、規則、および手段の兼ね合いを考慮することができる。

本文書におけるパスワード強度へのアプローチは、ユーザの名前以外に何も知らない攻撃者が「帯域内の」パスワード推測攻撃によってユーザのパスワードを見つけ出すことができる確率を測ることである。つまり、攻撃者は認証が成功するまで、異なるパスワードを試し続けようとする。次に示した各レベルについて、パスワードの「*事前の*」知識を持たない攻撃者が、パスワードの有効期限のあいだに、帯域内パスワード推測攻撃を成功させる最大の確率は次のとおりである。

1. レベル 1 - 2^{-10}（1,024 分の 1）
2. レベル 2 - 2^{-14}（16,384 分の 1）

たとえば、キーボードに刻印されている 94 個の印字可能なアルファベット文字の中から無作為に選択した 6 文字のパスワードを加入者に割り当てるシステムを考える。表A.1 から、そのようなパスワードは 39.5 ビットのエントロピーを持つとみなせる。認証システムにおいて、認証失敗の許容回数を $2^{39.5}/2^{14} = 2^{25.5}$回に制限すれば、レベル 2 におけるパスワード強度の要求事項が満たされる。たとえば認証システムで、認証失敗の合計回数が $2^{25.5}$ 回（およそ 4,500 万回）に達した時点でパスワードをロックするカウンタを設けるだけでもよい。別の方式としては、認証失敗が 3 回連続したあと、認証要求者を 1 分間ロックアウトすることも考えられる。このようなロックアウトであれば、自動化された攻撃の試みを 1 分間で 3 回に限定するには十分であり、そうすれば $2^{25.5}$回の試み実行するのに約 90 年かかることになる。システムにおいて、3 回の試行が失敗したらパスワード認証を 1 分間ロックし、10 年ごとにパスワードを変更することを求めるとすれば、標的を定めたパスワード推測攻撃に対するレベル 2 の要求事項を十分に満たすことになる。無作為に選択されるパスワードの最小エントロピーは推測エントロピーと同じであるため、レベル 2 における最小エントロピーの要求事項が満たされる。

次のようなシステムを考える。

- 最低 8 文字のパスワードを使用する。加入者が 94 個の印字可能なアルファベット文字から選択する。
- パスワードに、少なくとも大文字を 1 個、小文字を 1 個、数字を 1 個、特殊文字を 1 個、それぞれ含めることを加入者に求める。そして、
- 一般的な単語が含まれるのを防ぐために辞書を使用し、ユーザ名の並べ替えをパスワードとして使用することを防止する。

このようなパスワードであれば、ユーザが選択するパスワードについて付録Aで示した組み合わせ規則と辞書規則を満たし、表A.1 から推測エントロピーは 30 ビットと推定される。パスワードの有効期限のあいだに、加入者による認証失敗を 2^{16}（約 65,000）回未満に制限するシステムであれば、標的を定めた推測攻撃に対するレベル 2 の要求事項を十分に満たすことになる。たとえば、パスワードを 2 年ごとに変更することを求め、認証の試みが 6 回連続して失敗したらアカウントを 24 時間ロックすることによって再試行を制限するシステムを考える。攻撃者はパスワードが有効なあいだに、2×365×6 ＝ 4,380 回の試みが可能となるが、これは標的を定めた攻撃に対するレベル 2 の要求事項を十分に満たす。また、辞書テストを行っているため、レベル 2 における最小エントロピーの規則も満たすことになる。

より長いパスワードに対して辞書規則を課すことはたいへん難しく、多くの人は、より無作為な短めのパスワードよりも、複数の単語で構成される比較的長い「パスフレーズ」を記憶するほうを好む場合がある。そうした例として、たとえば「IamtheCapitanofthePina4」などが考えられる。

認証システムでは、任意の特定のルールセットを課す代わりに、前述の規則を使用してユーザのパスワードを格付けし、最小エントロピーの基準を満たす全てのパスワードを受け入れることが考えられる。たとえば、少なくとも 24 ビットのエントロピーを持つパスワード

を必要とする場合を考える。「IamtheCapitanofthePina4」は、23 文字で構成されており、大文字とアルファベット以外の文字を要求する組み合わせ規則を満たしていることから、そのエントロピーの推定値を計算することができる。表 A.1 から、このパスワードの推測エントロピーは 45 ビットと推定される。

表 A.1 – パスワードの推測エントロピの推定値(ビット数)とパスワード長

	ユーザによる選択				無作為の選択	
	94 文字のアルファベット			10 文字のアルファベット		94 文字のアルファベット
長さ(文字数)	検査なし	辞書規則	辞書規則と組み合わせ規則			
1	4	-	-	3	3.3	6.6
2	6	-	-	5	6.7	13.2
3	8	-	-	7	10.0	19.8
4	10	14	16	9	13.3	26.3
5	12	17	20	10	16.7	32.9
6	14	20	23	11	20.0	39.5
7	16	22	27	12	23.3	46.1
8	18	24	30	13	26.6	52.7
10	21	26	32	15	33.3	65.9
12	24	28	34	17	40.0	79.0
14	27	30	36	19	46.6	92.2
16	30	32	38	21	53.3	105.4
18	33	34	40	23	59.9	118.5
20	36	36	42	25	66.6	131.7
22	38	38	44	27	73.3	144.7
24	40	40	46	29	79.9	158.0
30	46	46	52	35	99.9	197.2
40	56	56	62	45	133.2	263.4

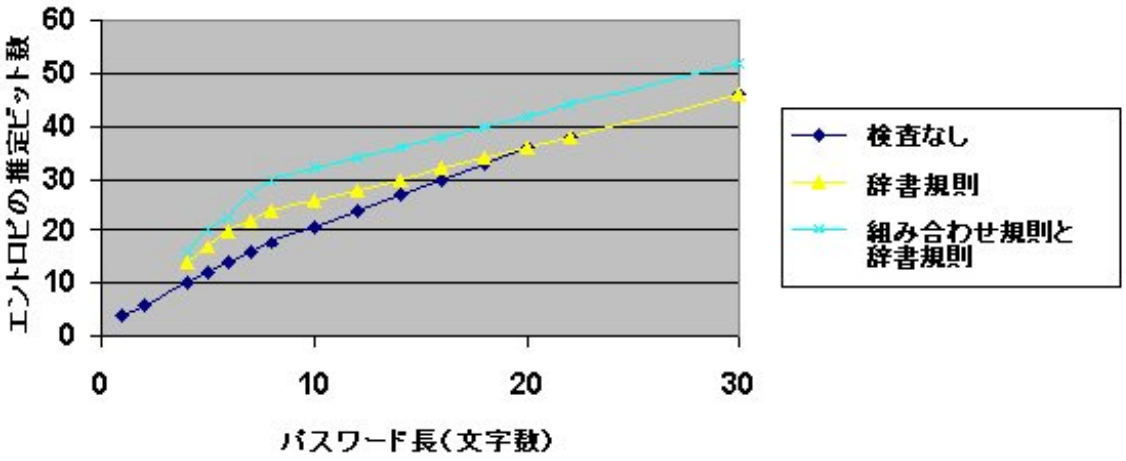

図 A.1:ユーザが選択するパスワードのエントロピの推定値とパスワード長

付録 B: 変更履歴

付録 B.1 : バージョン 1.0.1 における変更履歴

1. 表紙: バージョン番号を 1.0 から 1.0.1 に変更した。
2. 表紙: 日付を 2004 年 6 月から 2004 年 9 月に変更した。
3. vii ページ: ワンタイムパスワードを使用してレベル 3 の認証をサポートすることはできるが、再利用可能なパスワードではサポートできないことを示すように、文章を明確にした。
4. 「認可済み」の定義について、FIPS 140-2 における暗号モジュールの有効性確認の記述を含め、有効性が確認されたモジュールの一覧を参照する URL を含めるように改訂した。
5. 27 ページ: 連邦ブリッジ CA との「横断認証」の意味を明確にするため、連邦ブリッジ CA との横断認証は本ガイドラインにおいては双方向である必要がないことを明記した脚注を追加した。
6. 41 ページの表 2: パスワードの形態の 1 つである暗証番号がレベル 1 および 2 で許されることを明記した。

そのほか、編集上の小さな変更(小文字の大文字化、綴り、句読点など)を全般的に加え、リンクの一部を修正した。

付録 B.2 : バージョン 1.0.2 における変更履歴

1. 表紙: バージョン番号を 1.0.1 から 1.0.2 に変更した。
2. 表紙: 日付を 2004 年 9 月から 2006 年 4 月に変更した。
3. 表紙: William Jeffrey の役職を NIST 所長とし、Robert Cresanti の役職を米国商務省技術担当商務次官とした。
4. 26 ページ: FPKI 証明書ポリシーの 800-63 登録レベルへの対応付けについて、FBCA における Basic Assurance Level(基本保証レベル)の変更が反映され、新しい 3 つの FPKI 証明書ポリシー(FBCA の Medium Hardware(中位-ハードウェア)ポリシー、Common Authentication(共通認証)、および Common-High(共通-高位))が盛り込まれるように、更新を行った。FBCA の Basic(基本)は連邦 PKI ポリシー機関により、レベル 3 の登録に関する要求事項を満たすように格上げされた。新しいポリシーはレベル 4 の登録に関する要求事項を満たす。
5. 43 ページ: 新しい表 7 を挿入し、共通ポリシーフレームワークにおける証明書ポリシーと、電子認証の保証レベルとの関係を明確にした。この表に対応する新しい導入文章では、カード認証と共通デバイスのポリシーについて、それらがデバイスの認証をサポートするものであるため、検討から除外していることを説明している。
6. 44 ページ: 表 8(バージョン 1.0.1 では表 7)について、Basic(基本)証明書ポリシーがレベル 3 を満たすようになったため、それに伴う変更が反映されるように更新した。また、レベル 4 を満たす新しい Medium-HW(中位-ハードウェア)証明書ポリシーもこの表に追加した。共通ポリシーフレームワークの証明書ポリシーについては、新しい表 7 で規定しているためこの表から削除した。
7. 48 ページ: FPKI 証明書ポリシーを参照する URL を更新した。