4. 電子認証の運用に関するドキュメントの現状

本章では、電子認証に関わるオープンなガイドラインを日本において運用するための要件を明らかにするため、IETF、IP レジストリ及び国内外の政府によるガイドライン・ドキュメントの現状について述べる。はじめに電子認証の分野でガイドラインが求められる背景と必要性について整理するとともに、IETF より提供されるドキュメントのうち、Best Current Practice として扱われるものに着目し、その策定プロセスの分析を行う。次に海外の政府もしくは民間団体によってまとめられた電子認証に関わるガイドラインについて、目的、利用者・利用方法の想定、運用の特徴などについて述べる。

4.1. 情報ネットワークやシステムを対象とするドキュメント

本章では、電子認証に関するフレームワークに関する検討を行うに先立ち、電子認証のような情報ネットワークや情報システムを利用したサービスの構築や運用、利用に関するドキュメントの種類と特徴について概観する。

電子認証に関する構築や運用、利用のために提供されるドキュメントについて、その種類に応じて例を挙げるとともに、どのような経緯で作成されてきたかについて整理する。なお法令、条例等の法的拘束力を有するドキュメントについては、調査対象から除外した。

4.1.1. 各種ガイドライン

文書名に「ガイドライン」を含むドキュメントはこれまでに数多く発行されている。ここではその発行主体によって分類した上でその傾向を示す。

4.1.1.1. 国際機関によるガイドライン

代表例として、OECD（経済協力開発機構）が情報セキュリティと個人情報保護を対象に策定したガイドラインの例を示す。

（1） 情報システム及びネットワークのセキュリティのためのガイドライン（OECD）

1992 年に策定され、2002 年に大規模な改訂が行われた。情報システムとネットワークに関するすべての関係者（参加者）を対象として「セキュリティ文化の醸成」を

目指し、9 つの原則が示されている。[1]

（2） 個人情報保護ガイドライン（OECD）

1980 年に策定された 8 原則からなる。本ドキュメントはガイドラインの位置づけであるが、各国における個人情報保護に関する法制度が本ガイドラインに準拠している場合も多く、影響力が大きいことが特徴である。

（3） Interchange of Data between Administrations (IDA) Authentication Policy（EU）

EU の政府間データ交換委員会（IDA）において、分野別ネットワークとプロジェクトにおける適切な認証メカニズムの構築を目的とした基本ポリシーを定めるものである。保証レベル等の考え方は、1.1.1.2(1)の E-Authentication Guidance と共通する部分が多いが、EU における条件を踏まえて追加されているものもある。

4.1.1.2. 各国政府によるガイドライン

各国政府が策定しているガイドラインの例を示す。ただし、日本以外については電子認証に関するものを中心として扱う。このうち、海外の電子認証に関するガイドラインの事例については次節において詳細な分析を行う。

（1） E-Authentication Guidance for Federal Agencies（米国）

政府内において電子認証に関する一貫したアプローチの保証を実現することを目的として、2003 年 12 月に策定された。電子認証サービスを提供する政府機関におけるリスクアセスメントの実施を定めることにより、サービス利用者としての国民の判断基準を提供している。

（2） Registration and Authentication －e-Government Strategy Framework Policy and Guidelines －（英国）

英国の電子政府が提供する電子認証サービスにおける保証レベルを定めることを目的として 2002 年 9 月に策定された。匿名でのアクセスに関する取扱いが区分されて扱われている点などに特色がある。

[1] OECD情報システム及びネットワークのセキュリティのためのガイドライン
http://www.meti.go.jp/policy/netsecurity/oecd2002.htm

（3） Australian Government Electronic Authentication Framework（オーストラリア）

オーストラリア政府機関を対象とした電子認証フレームワーク（AGAF）において、リスクレベルに対応した認証手段を実施することを目的として 2005 年に策定された。副題として認証とアクセス管理のための「Better practice guide」との標題がつけられている。

（4） Authentication for e-government Best Practice Framework for Authentication（ニュージーランド）

ニュージーランド政府の電子認証サービスにおけるリスク評価の方針と保証レベルの定義を定めたガイドラインとして、2004 年 4 月に策定された。オンライン認証の実装方法についても解説がある。

（5） Evidence of Identity Framework（ニュージーランド）

ニュージーランドの政府機関において高いリスクを伴う情報処理を行う際の高レベルの機密性確保と個人認証の実現を目的として、2004 年 10 月に策定された。リスクの分析に重点が置かれているほか、政府内の事例毎の詳細な説明が添付されている。

（6） 経済産業省による各種基準・ガイドライン（日本）

電子認証フレームワークに関連して政府が定めた法規としては、「電子署名及び認証業務に関する法律（平成 12 年法律第 102 号）」が存在するが、これ以外に直接的に電子認証サービスを対象とする政府によるガイドライン等のドキュメントは存在しない。情報セキュリティに関連する各種基準、ガイドラインの例としては以下の例が挙げられる。

- 情報セキュリティ管理基準（2004 年 10 月策定）
- 電子政府情報セキュリティ管理基準モデル（2004 年 10 月策定）
- 情報セキュリティ監査基準（2004 年 10 月策定）

4.1.1.3. 民間団体によるガイドライン

民間主導で作成されたガイドラインの例を示す。

（1） Trust Framework（米国Electronic Authentication Partnership）[2]

5.1.1.2(1)の E-Authentication Guidance で定められた内容をもとに、政府と民間の連携、ないし民間同士での連携のスキームの確立を目指すもものである。

（2） 認証局運用ガイドライン（電子商取引実証推進協議会（ECOM））[3]

ECOM により、国際標準化機構（ISO）、IETF 等で検討されている認証もしくは認証局に係わる各種のガイドラインの内容や、ECOM 内で認証局の実験を行ったプロジェクト等からの意見をもとに、1998 年 10 月に策定されたガイドラインである。

本ガイドラインは認証局の運用を対象として、以下の特徴を有する。

- 認証局の機能として、登録局機能、リポジトリ機能等も包含した認証管理サービス全体を対象とする要件を規定するなど、汎用性を意識したものとなっている。
- ガイドラインの内容は ISO の TTP（Trusted Third Party）ガイドライン、金融向けの認証管理、IETF/PKIX の認証ポリシーと認証実施フレームワーク等のドラフトにおいて検討されている要件をもとに、セキュアな認証局の運用のために備えるべきものをを洗い出した上で規定されており、国際整合性に配慮している。
- 認証局の用途等をもとに３段階のレベル付けを行っている。具体的は、以下の 3 種類が想定した上で、それぞれのレベルの認証局の要件をマネジメント、業務運用、設備・システムなどの単位で規定している。
  i) 電子メールに対する認証書のような信頼度の保証が比較的低いレベルの認証書を発行する認証局
  ii) 電子商取引において高額ではないが決済の保証をする信頼度中レベルの認証書を発行する認証局
  iii) 下位の認証局に高い信頼度を持った認証書を発行する認証局

[2] Electronic Authentication Partnership Trust Framework
http://eapartnership.org/docs/Trust_Framework_010605_final.pdf
[3] 電子商取引実証推進協議会, 認証局運用ガイドライン(1.0 版), 1998 年 10 月.

4.1.2. BCP（Best Current Practice）

インターネットで利用される技術の標準化を行う組織である IETF（Internet Engineering Task Force）において策定されるドキュメントの中には、“ Best Current Practice ”と名付けられたカテゴリーに所属する一連の文書がある。これは、インターネット運用における組織や管理に関して現在行われている各種の手続きを文書化したものが中心となっている。「現時点における最良の方法、実践、規範」など直訳的に解釈されるほか、「現状通知」などと訳される場合もある。ドキュメントは主に開発者を対象に書かれているが、ネットワークサービスの提供者を対象としたものもある。

BCP も IETF で扱われる正式文書の総称である RFC（Request For Comments）に属するドキュメントであるが、後の策定プロセスの項で説明するように、RFC のうち“ Standard ”に属するドキュメントがその策定に際して広範なテストと意見の募集を経るのに対し、BCP に属するドキュメントについては、IETF の下部組織である技術専門家グループの IESG（Internet Engineering Steering Group）によるレビューと承認を経るのみで決定される点が異なる。

BCP の定義については、過去には単独の RFC として RFC1818（Best Current Practice）が提供されていたが、現在、RFC1818 は Historic（歴史的）の位置づけとなり、RFC2026（The Internet Standards Process - インターネット標準化手続 - Revision 3）のセクション 5 に規定された内容に基づいて策定されている。RFC2026 も Best Current Practice のカテゴリーに所属する RFC である。

現在 BCP として提供されているドキュメントをカテゴリー別に整理すると、以下のようになる。

（1） ガイドライン、規範的な位置づけのもの

あるプロセスや活動における望ましい規範として IETF が定めるものであり、本調査におけるガイドラインの位置づけの規範となるものである。ここに該当する BCP の例としては以下のようなものがある。

- Recommended Internet Service Provider Security Services and Procedures（RFC 3013, BCP 46）
- IANA Guidelines for IPv4 Multicast Address Assignments（RFC 3171, RFC 51)
- Management Guidelines & Operational Requirements for the Address and Routing Parameter Area Domain ("arpa")（RFC 3172, RFC 52)
- Guidelines for Evidence Collection and Archiving（RFC 3227, BCP 55）
- Guidelines for the Use of Extensible Markup Language (XML) within IETF Protocols（RFC 3470, BCP 70）
- Guidelines for Writing RFC Text on Security Considerations（RFC 3552, BCP 72）

- DNS IPv6 Transport Operational Guidelines（RFC 3901, BCP 91）
- Guidelines for Cryptographic Key Management（RFC 4107, BCP 107）
- Guidelines and Registration Procedures for New URI Schemes（RFC 4395, BCP 115）

（2） 個別事項についてのベストプラクティス

ガイドラインのように一般化するのではなく、個別事項についての対応方法をベストプラクティスとしてまとめたものである。ここに該当する例としては以下のようなものがある。

- Address Allocation for Private Internets（RFC 1918, BCP 5）
- Use of DNS Aliases for Network Services（RFC 2219, BCP 17）
- Classless IN-ADDR.ARPA delegation（RFC 2317, BCP 20）
- Change Process for the Session Initiation Protocol (SIP)（RFC 3427, BCP 67）

（3） 特定のリスクに対する対応のあり方を示すもの

(2)の特殊な例として、特定のリスクへの対処のあり方を示すものがある。ここに該当する BCP の例としては以下のようなものがある。

- Hanging the Default for Directed Broadcasts in Routers（RFC 2644, BCP 34）
- Inappropriate TCP Resets Considered Harmful（RFC 3360, BCP 60）
- Embedding Globally-Routable Internet Addresses Considered Harmful（RFC 4085, BCP 105）

（4） 自らの組織とプロセスに関するもの

BCP の中には、IETF 自らの組織とその活動についての規定を行っているものが存在する。これが BCP に位置づけられるのは、通常の標準文書のようにテストを実施することが適切でなく、かつ内部での承認の必要性を伴うものであることにより、必然的に BCP の扱いで策定せざるを得ないことによる。ここに該当する BCP の例としては以下のようなものがある。

- Guide for Internet Standards Writers（RFC 2360, BCP 22）
- IETF Working Group Guidelines and Procedures（RFC 2418, BCP 25）
- IETF Guidelines for Conduct（RFC 3184, BCP 54）
- Defining the IETF（RFC 3233, BCP 58）
- The IESG and RFC Editor Documents: Procedures（RFC 3932, BCP 92）
- A Model for IETF Process Experiments（RFC 3933, BCP 93）
- Updates to RFC 2418 Regarding the Management of IETF Mailing Lists（RFC

3934, BCP 94）
- A Mission Statement for the IETF（RFC 3935, BCP 95）
- Structure of the IETF Administrative Support Activity (IASA)（RFC 4071, 4371, BCP 101）
- IAB Processes for Management of IETF Liaison Relationships（RFC 4052, BCP 102）
- Procedures for Handling Liaison Statements to and from the IETF（RFC 4053, BCP 103）
- The IETF Administrative Oversight Committee (IAOC) Member Selection Guidelines and Process（RFC 4333, BCP 113）

（5） 知的財産権に関するもの

(4)の特殊な例として、知的財産権に関する扱いを BCP として定めた RFC の例として以下のものがある。

- IETF Rights in Contributions（RFC 3978, BCP 78）
- Intellectual Property Rights in IETF Technology（RFC 3979, BCP 79）

これらを含め、現在 IETF から BCP として公開されているドキュメントの一覧を章末の Appendix 2 に示す。

4.2. ドキュメントの策定プロセス

前項で示した各種のドキュメントについて、その策定プロセスを整理する。

4.2.1. IETF におけるドキュメント策定プロセス

IETFにおける標準的なRFCの策定手順の流れをJPNICが一般向けに公開している資料「What is IETF」[4]ならびに「Introduction to RFC(s)」[5]をもとに図に示す。

プロセス内に位置するドキュメントのステータスとして、以下の種類が定められている。

（1） Internet-draft

Internet-draft は誰でも自由に投稿することができる Working-in-Progress の扱いのドキュメントである。IETF に Internet-draft が投稿されると、FTP サーバおよび Web サーバを通じて 6 か月間公開される。この間に広くインターネット業界に有用な情報を含んでいると判断されると、これを RFC あるいは BCP にするよう IESG に申請が行われる。申請が承認されると、ドキュメントには RFC 番号（あるいは BCP 番号）が割り当てられ、公式に IETF の FTP および Web サーバを通じて恒常的に参照可能なドキュメントとして扱われるようになる。

（2） Standard Track RFC（Proposed Standard、Draft Standard、Standard）

これらはドキュメントが Internet-draft の段階を経て、業界での国際標準とすべく Working Group においてコンセンサスが得られた仕様としてとりまとめられたものである。Proposed、Draft などの種類は、実装や運用のテストの経過段階に応じて定められており、Proposed Standard は複数の組織での独立な実装テストと相互接続性の確認、Draft Standard は実質的かつ広範囲での運用テストがそれぞれ条件となっている。これらの段階を経て Standard の状態になると、RFC の番号とは別に STD 番号が割り振られる。RFC として管理されているドキュメントの中で、STD 番号を有するものは非常に少数であり、Draft Standard の段階の RFC であっても、実質的に国際標準として利用されているものも少なくない。

---

[4] 江崎 浩: What is IETFより第４章「IETFにおける標準化プロセス」
http://rfc-jp.nic.ad.jp/what_is_ietf/ietf_section4.html
[5] 宇夫 陽次朗: Introduction to RFC(s)
http://rfc-jp.nic.ad.jp/introduction/

（3） BCP（Best Current Practice）

前述の通り、BCP は IESG による承認を得たドキュメントであるが、標準として扱うに際して実装や運用のテストを経ない点で(2)と異なる。しかしながら標準として利用することを意図していることでは(2)と共通であり、BCP に位置づけられるドキュメントはすでに広く利用されている手続きや規範を扱ったものが多い。STD 番号と同様、BCP 番号が RFC の番号と別に割り振られる。

（4） Experimental RFC

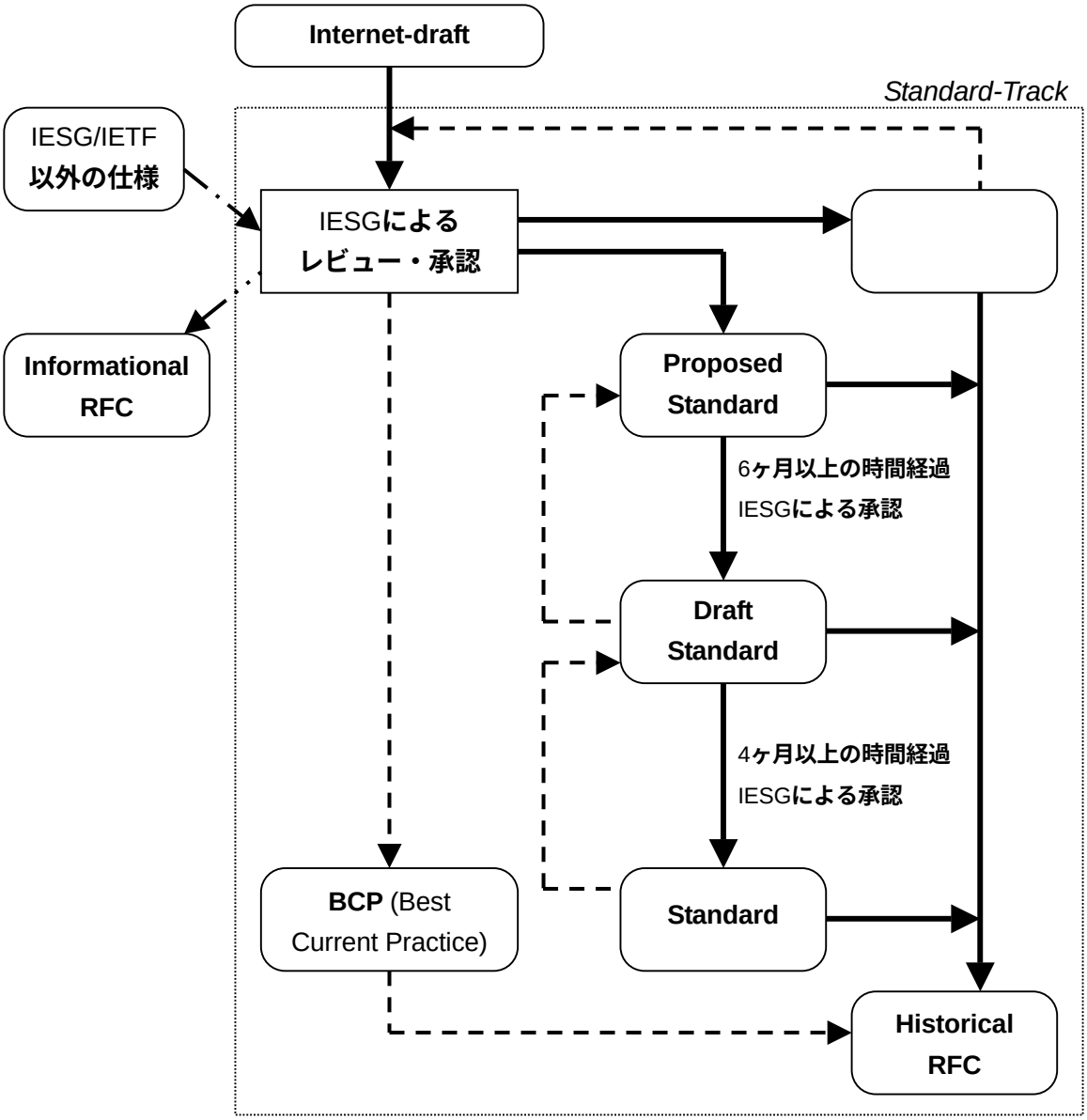
Experimental に分類されるドキュメントには、標準化を目的とせず、研究等における技術仕様を規定したものも含まれる。これは、純粋な研究目的のほか、本来企業独自の仕様であるものをデファクト化することを目的として提供される場合もある。

（5） Informational RFC

Informational に分類されるドキュメントには、標準化は想定していないが、業界にとって有用と判断されるものが含まれる。すなわち、仮に特定の企業などに固有の仕様であっても、それが、標準仕様の議論や策定に有効であると認められる場合には RFC とすることができる。(4)と同様、企業が標準化を待たずに製品展開を行うような場合に、Informational RFC としてその仕様を広く公開することにより、デファクト・スタンダードを確立するための手段として利用されることもある。

（6） Histrorical RFC

かつては標準として利用されていたが、技術の進展や環境の変化などの影響により同一の分野での別の RFC が承認されたことを通じて、現役のドキュメントとして利用されなくなったものは Historical（歴史的）として位置づけられる。



（江崎 浩「What is IETF」[6]挿入図より作成）

図 4−1 IETF における RFC の策定プロセス

[6] 江崎 浩「What is IETF」第４章「IETFにおける標準化プロセス」
http://rfc-jp.nic.ad.jp/what_is_ietf/ietf_section4.html

4.2.2. その他の策定プロセス

IETF における策定プロセスの説明を補足する視点から、IP レジストリなど他機関における類似ドキュメントの策定プロセスについて示す。

4.2.2.1. JPNIC における策定プロセス

参考情報として、JPNIC で用いている策定プロセスの例として、IP アドレスポリシーに関する策定プロセスを示す。

ポリシー提案は、以下のステップに基づく議論をもとに、その採用ないし実装が検討される[7]。

（1） ポリシー提案の提出

ポリシー提案が、提案者から JPNIC ポリシーワーキンググループ（以下ではポリシーWG という）に提出される。

（2） APNIC に対する提案の必要性の確認

提出された提案について、APNIC に対しても提案が必要かどうかの確認をポリシーWG が JPNIC と共同で行い、その結果を提案者に連絡する。

（3） ポリシー提案の公開

ポリシーWG は提出されたポリシー提案を、オンサイトフォーラム（会議場に参加者が集合して行う形式のもので、この場合は JPNIC オープンポリシーミーティングが該当する）の開催にあたり、事前に Web もしくはオンラインフォーラム上、あるいはその双方で公開する。

（4） ポリシー提案の議論

オンサイトフォーラムの場で提出したポリシー提案に関する説明を提案者が行い、参加者からの質問に対応する。

[7] JPNICにおけるIPアドレスポリシー策定プロセス
http://www.nic.ad.jp/doc/jpnic-00962.html

（5） コンセンサスの醸成

提出されたポリシー提案に対し、オンサイトフォーラムの参加者の過半数の賛同が得られた場合に、そのポリシー提案はコンセンサスを得たものとされる。このコンセンサスの確認はポリシーWG のチェアによって行われる。このコンセンサスは「1 次コンセンサス」と呼ばれる。

（6） 最終コメント期間

1 次コンセンサスを得たポリシー提案は、オンラインフォーラム上で公開され、最低 2 週間の最終コメント期間を経るものとする。この最終コメント期間は、ポリシーWG のチェアの裁量で延長することができる。

（7） 最終的なコンセンサスの確認

前項の最終コメント期間において本質的な反対がなければ、当該ポリシー提案は最終的なコンセンサスを得たものとされる。この判断は、ポリシーWG のチェアによって行われる。

（8） コンセンサス内容の確認と実装勧告

最終的なコンセンサスを得たポリシー提案について、ポリシーWG によってその内容の妥当性の再評価が行われ、コンセンサスの内容が整理される。その結果をもって、ポリシーWG は JPNIC に対し、当該ポリシー提案の実装勧告を行う。

（9） JPNIC による実装検討

JPNIC では、ポリシーWG からの実装勧告を受け、実務的な面で実装が可能か、採算上問題ないか、APNIC のポリシーに反しないかなどの確認と検討を行う。

（10） JPNIC による承認プロセス

実装勧告に対して JPNIC が実装可否の判断を行い、この結果は JPNIC の理事会の審議を経て最終的に決定される。

（11） JPNIC による結果報告

JPNIC による実装検討の結果が、オープンポリシーフォーラムへ報告される。実装が決定したポリシー提案は、実施日などの調整を行ったうえで施行の運びとなる。

一方、提案者から提出されたポリシー提案が棄却となる条件としては、以下の場合が挙げられている。

- オンサイトフォーラムの場で、参加者の過半数の賛同を得られなかった場合
- オンサイトフォーラムでは参加者の過半数の賛同を得たが、オンラインフォーラムでの最終コメント期間中、最終的なコンセンサスの確認が取れないとポリシーWG のチェアが判断した場合
- 最終的なコンセンサスが確認されたが、その内容が妥当でないとポリシーWG によって判断された場合
- ポリシーWG からの実装勧告に対し、JPNIC が実務的な面、採算上の問題、APNIC とのポリシーとの整合性等の観点から実装することができないと判断した場合
- ポリシー提案の実装が JPNIC だけで決定できず、APNIC に提案する必要があり、その提案が APNIC オープンポリシーミーティングにおいて賛同を得られなかった場合

提出されたポリシー提案が棄却された場合は、ポリシーWG もしくは JPNIC が、オンサイトフォーラムまたはオンラインフォーラム、もしくはその両方で、棄却となった理由について報告を行う。

4.3. 電子認証に関わる既存ガイドライン等の分析

IETF、IP レジストリ、日本政府、諸外国政府及び外郭団体のガイドラインを挙げ、その状況と特徴をまとめる。

4.4. 調査対象の概要

本調査では、以下の観点から各ガイドラインの分析を行う。

本調査の結果は、章末に記載した表 4-1「海外における電子認証に関わる既存ガイドラインの例」に掲載する。

（1） 目的

ガイドライン作成の目的を識別する。

（2） 利用者

ガイドラインを利用するターゲットについて、文書中に記述されている場合はそれを抽出し、そうでない場合は内容から想定を行う。

（3） 利用方法の想定

ガイドラインをどのような場合に利用することを想定しているかについて、検討を行う。

（4） 運用方法

ガイドラインの運用（改定等のメンテナンス、普及・広報活動等）について、関係する情報を整理する。

（5） 特徴

他のガイドラインと比較した特徴的な事項の抽出を行う。

4.5. E-Authentication Guidance for Federal Agencies（米国）

本文書の要約として、以下の事項が示されている。

> This guidance requires agencies to review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance. It establishes and describes four levels of identity assurance for electronic transactions requiring authentication. Assurance levels also provide a basis for assessing Credential Service Providers (CSPs) on behalf of Federal agencies. This document will assist agencies in determining their e-government authentication needs. Agency business-process owners bear the primary responsibility to identify assurance levels and strategies for providing them. This responsibility extends to electronic authentication systems.

＜引用部の訳文＞

本ガイダンスは、政府機関に対して認証プロセスが適切な保証レベルを提供することを確実にするために、新規および既存の電子的なトランザクションの見直しを要求するものである。

本ガイダンスでは、認証が要求される電子的なトランザクションの為の、本人性保証の 4 つのレベルが規定され、説明されている。また、保証レベルは連邦政府関係機関を代表してクレデンシャル・サービス・プロバイダー（Credential Service Providers: CSPs）を評価するための原則を提供している。本ドキュメントは、政府機関が電子政府認証ニーズを決定することの手助けともなる。政府機関の業務プロセス所有者は、本人保証レベル及びそれらを提供する戦略に対して主要な責務を担う。この責務は、電子認証システムにまで及ぶこととなる。

> Agencies should determine assurance levels using the following steps, described in Section 2.3:
>
> 1. Conduct a risk assessment of the e-government system.
> 2. Map identified risks to the applicable assurance level.
> 3. Select technology based on e-authentication technical guidance.
> 4. Validate that the implemented system has achieved the required assurance level.

5. Periodically reassess the system to determine technology refresh requirements.

＜引用部の訳文＞

政府機関は、本ガイダンスの 2.3 節で説明される、次の手順に従って保証レベルを決定すべきである。

1. 電子政府システムのリスクアセスメントを実施する。
2. 判明しているリスクを該当する保証レベルに位置づける。
3. 電子認証の技術ガイダンスに基づいて技術を選択する。
4. 実装されたシステムが、要求された保証レベルに達しているかを検証する。
5. 定期的にシステムを見直して 技術更新要件を決定する。

4.5.1. 保証レベルの説明

本文書において、保証レベルの説明として以下の事項が示されている。

This guidance describes four identity authentication assurance levels for e-government transactions. Each assurance level describes the agency's degree of certainty that the user has presented an identifier (a credential in this context) that refers to his or her identity. In this context, assurance is defined as

1) the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and
2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.

The four assurance levels are:

Level 1: Little or no confidence in the asserted identity's validity.

Level 2: Some confidence in the asserted identity's validity.

Level 3: High confidence in the asserted identity's validity.

Level 4: Very high confidence in the asserted identity's validity.

＜引用部の訳文＞

本ガイダンスでは、電子政府のトランザクションのための 4 つの identity 認証保証レベルについて説明をする。利用者が提示した自らを参照する識別子（本文書ではクレデンシャル）についての政府機関の確度で各レベルは述べられている。本文書において、保証は次のように定義される。

1) クレデンシャルが発行された個人の身元をするために立証するために使用される審査プロセスにおける信頼度
2) クレデンシャルを使用する個人が、クレデンシャルを発行された個人であることの信頼度

4 つの保証レベルとは、

レベル１：asserted identity's validity の信頼はほとんどない

レベル２：asserted identity's validity の信頼は若干ある

レベル３：asserted identity's validity の信頼は高い

レベル４：asserted identity's validity の信頼は非常に高い

である。

4.5.2. リスク、潜在的影響、および保証レベル

本文書において、リスク・潜在的影響・保証レベルの説明として以下の事項が示されている

> While, this guidance addresses only those risks associated with authentication errors, NIST Special Publication 800-30, “Risk Management Guide for Information Technology Systems,” recommends a general methodology for managing risk in Federal information systems. In addition, other means of risk management, (e.g., network access restrictions, intrusion detection, and event monitoring) may help reduce the need for higher levels of authentication assurance.

＜引用部の訳文＞

本ガイダンスでは、認証エラーに関連するそれらのリスクのみを扱っているが、NIST Special Publication 800-30 の「情報技術システムのためのリスク管理ガイド（Risk Management Guide for Information Technology Systems）」では、連邦情報システムのリスク管理のための一般方法論が推奨されている。そして、リスク管理の他の手段（例えば、ネットワークアクセス制限、侵入検知、モニタリングなど）を用いることにより、さらに高い認証保証レベルの必要性を軽減させることが可能である。

4.5.2.1. 潜在的影響カテゴリー

本文書において、潜在的リスクの説明として以下の事項が示されている。

> To determine the appropriate level of assurance in the user's asserted identity, agencies must assess the potential risks, and identify measures to minimize their impact. Authentication errors with potentially worse consequences require higher levels of assurance. Business process, policy, and technology may help reduce risk. The risk from an authentication error is a function of two factors:
>
> 1) potential harm or impact, and
>
> 2) the likelihood of such harm or impact.

＜引用部の訳文＞

利用者の asserted identity における適切な保証レベルを決定するために、政府機関は潜在的リスクを評価し、その影響が最小に抑えられるための対策を特定しなければならない。潜在的により悪い結果を招く認証エラーは、より高い保証レベルを必要とします。業務プロセス、政策、および技術は、リスク軽減に役立つ可能性がある。認証エラーに起因するリスクは、次の 2 つの要因による作用である。

a) 潜在的な損害または影響

b) 潜在的な損害または影響の見込み

（1） 損害と影響のカテゴリー

損害と影響のカテゴリーには次が含まれる。

- 不便、苦痛、または地位や評判に対する損害
- 経済的損失または政府機関の負担
- 政府機関の計画や公益への損害
- 機密情報の不正発表
- 個人の安全
- 民事または刑事上の違反行為

連邦情報処理規格(FIPS) 199、「連邦政府の情報と情報システムのセキュリティ分類の規格（Standards for Security Categorization of Federal Information and Information Systems)」に記述されている潜在的影響値を使用して、電子的なトランザクションのために要求される保証レベルは、上記のそれぞれのカテゴリーの潜在的影響の評価によって決定される。3 つの潜在的影響の評価とは次の通りである。

・ 低影響

・ 中影響

・ 高影響

（2） 認証エラーの潜在的影響の決定

上記で述べた各カテゴリーにおける潜在的影響の定義付けを行う。

表 4-1　各カテゴリーにおける潜在的影響の定義付け

カテゴリー	低影響	中影響	高影響
不便、苦痛、または地位や評判に対する損害の潜在的影響	最悪の場合、苦痛や当事者の当惑が限定的、短期間の不便さである。	最悪の場合、苦痛や当事者の地位や評判に対する損害が、深刻で短期間または（範囲が）限定的で長期間の不便さである。	苦痛や当事者の地位や評判に対する損害が、重度のまたは深刻な長期間の不便さである（通常は、著しく深刻な影響を伴った状況または多くの人に影響を及ぼす)。
経済的損失の潜在的影響	最悪の場合、当事者に対する重要ではない場合や取るに足りない回復不能な経済的損失であるか、または、重要ではない場合や取るに足りない政府機関の負担である。	最悪の場合、当事者に対する深刻な回復不能な経済的損失であるか、深刻な政府機関の負担である。	当事者に対する重度のまたは壊滅的な回復不能な経済的損失であるか、重度のあるいは壊滅的な政府機関の負担である。

カテゴリー	低影響	中影響	高影響
政府機関の計画や公益への損害の潜在的影響	最悪の場合、組織の運営や資産、あるいは公益への限定的悪影響。限定的悪影響の例： 1) 組織において、かなり（noticeably）限定された効力で主要な機能を遂行できる程度と期間に対する、任務実行能力の低下。 2) 組織の資産や公益への軽度の損害	最悪の場合、組織の運営や資産、あるいは公益への深刻な悪影響。深刻な悪影響の例： 1) 組織において、かなり（sig-nificantly）限定された効力で主要な機能を遂行できる程度と期間に対する、任務実行能力の著しい低下。 2) 組織の資産や公益への多大な損害	組織の運営や資産、あるいは公益への深刻な又は破滅的な悪影響。深刻な又は破滅的な悪影響の例： 1) 組織において、かなり（severe）限定された効力で 1 つ又は複数の主要な機能を遂行できる程度と期間に対する、任務実行能力の重度の低下。 2) 組織の資産や公益への大規模な損害
機密情報の不正発表の潜在的影響	最悪の場合、FIPS PUB 199 に定義されているような機密を、低影響によって、認可されていない当事者へ、個人または米国政府の機微、商業的に機密な情報を限定的に公表	最悪の場合、FIPS PUB 199 に定義されているような機密を、中影響によって、認可されていない当事者へ、個人または米国政府の機微、商業的に機密な情報を限定的に公表	FIPS PUB 199 に定義されているような機密を、高影響によって、認可されていない当事者へ、個人または米国政府の機微、商業的に機密な情報を限定的に公表
個人の安全の潜在的影響	最悪の場合、医療手当を必要としない軽傷	最悪の場合、医療手当を必要とする、軽傷の中程度のリスクまたは負傷の限定的リスク	重傷または死のリスク

カテゴリー	低影響	中影響	高影響
民事または刑事上の違反行為の潜在的影響	最悪の場合、通常は執行対象とならないような種類の民事または刑事上の違反行為	最悪の場合、執行対象となり得るような種類の民事または刑事上の違反行為	執行プログラムにとって特に重要な民事または刑事上の違反行為

4.5.2.2. 保証レベルの決定

本文書において、保証レベルの決定についての説明として以下の事項が示されている

Compare the impact profile from the risk assessment to the impact profiles associated with each assurance level, as shown in Table 1 below. To determine the required assurance level, find the lowest level whose impact profile meets or exceeds the potential impact for every category analyzed in the risk assessment.

＜引用部の訳文＞

下記の表 4-2 においてリスクアセスメントからの影響プロファイルとそれぞれの保証レベルに関連する影響プロフィールを比較する。要求される保証レベルを決定するために、リスクアセスメントで分析された各カテゴリーに対して、影響プロファイルが潜在的影響と一致または超える最低限のレベルを見つける。

表 4-2　各保証レベルの最大潜在的影響

	保証レベル影響プロファイル			
認証エラーの潜在的影響カテゴリー	1	2	3	4
不便、苦痛、または地位や評判に対する損害	低	中	中	高
経済的損失または政府機関の負担	低	中	中	高
政府機関の計画や公益への損害	N/A	低	中	高
機密情報の不正発表	N/A	低	中	高
個人の安全	N/A	N/A	低	中／高
民事または刑事上の違反行為	N/A	低	中	高

4.5.3. 保証レベルの決定とリスクアセスメントを用いた認証ソリューションの選択

本文書において、リスクアセスメントを利用した保証レベルの決定法と認証ソリューションの選択について説明が述べられている。政府機関は下記で説明する手順に従って、保証レベルを決定する。

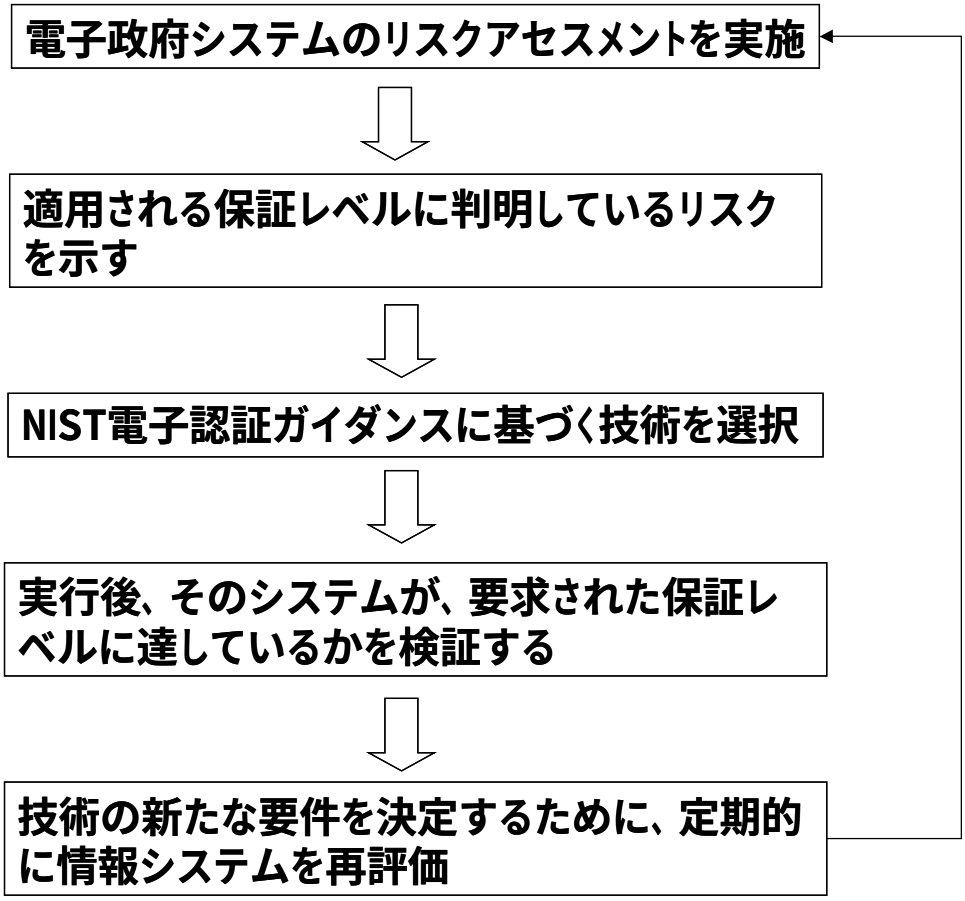


図 4−2　保証レベル決定の手順

手順１：電子政府システムのリスクアセスメントを実施する

Conduct a risk assessment of the e-government system.

Guidance for agencies in conducting risk assessments is available in A-130, Section 5 of OMB's GPEA guidance and existing NIST guidance. The risk assessment will measure the relative severity of the potential harm and likelihood of occurrence of a wide range of impacts (to any party) associated with the e-government system in the event of an identity authentication error.

Risk analysis is to some extent a subjective process, in which agencies must consider harms that might result from, among other causes, technical failures, malevolent third parties, public misunderstandings, and human error. Agencies should consider a wide range of possible scenarios in seeking to determine what potential harms are associated with their business process. It is better to be over-inclusive than under-inclusive in conducting this analysis. Once risks have been identified, there may also be ways to adjust the business process to mitigate particular risks by reducing the likelihood that they will occur (see Step 4).

＜引用部の訳文＞

政府機関がリスクアセスメントを実施するためのガイダンスは、OMB の GPEA ガイダンスのセクション５の A-130 および既存の NIST ガイダンスから入手可能である。リスクアセスメントは、電子政府システムでの identity 認証エラー発生時における、潜在的損害の相対的重大性と（当事者に対する）広範囲の影響の発生見込みを測るものである。

リスク分析はある程度主観的であるので、（この他の原因もあるが）技術的な失敗、維持の悪い第三者、人的ミスなどから生じる損害について政府機関は考慮しなければならない。どんな潜在的損害がビジネスプロセスに関連するかを決定しようとする際に、政府機関は広範囲に可能なシナリオを考慮すべきである。この分析を実施する際には、包括的でないよりも過剰に包括的である方が好ましい。一度リスクが確認されると、そのリスクが発生する可能性を低減させることにより、特定の危険を緩和するようにビジネスプロセスを調整する方法（手順４参照）があるかもしれない。

手順２：判明しているリスクを要求されている保証レベルに対応付ける

Map identified risks to the required assurance level.

The risk assessment should be summarized in terms of the potential impact categories in Section 2.2.

To determine the required assurance level, agencies should initially identify risks inherent in the transaction process, regardless of its authentication technology. Agencies should then tie the potential impact category outcomes to the authentication level, choosing the lowest level of authentication that will cover all of potential impacts identified. Thus, if five categories of potential impact are appropriate for Level 1, and one category of potential impact is appropriate for Level 2, the transaction would require a Level 2 authentication. For example, if the misuse of a user's electronic identity/credentials during a medical procedure presents a risk of serious injury or death, map to the risk profile identified under Level 4, even if other consequences are minimal.

＜引用部の訳文＞

リスクアセスメントは、セクション 2.2 での潜在的影響カテゴリーの観点から要約されるべきである。

所要の保証レベルを決定するためには、認証技術に関係なく、政府機関は最初にトランザクションプロセスにおける固有のリスクについて確認すべきである。そして、政府機関は潜在的影響カテゴリーの結果を認証レベルに結び付け、確認される全ての潜在的影響をカバーする最低の認証レベルを選択すべきである。従って、潜在的影響カテゴリーにおいて、５つがレベル１相当で、１つがレベル２相当である場合には、トランザクションはレベル２の認証を要求する。例えば、医療処理においてユーザの電子 identity/credentials の誤用が大怪我か死の危険を招く場合には、たとえ他の項目の結果が最小限であるとしても、レベル４より下で識別されるリスクプロファイルについても対応付ける必要がある。

手順３：NIST 電子認証ガイダンスに基づく技術を選択する

Select technology based on the NIST e-authentication technical guidance.

After determining the assurance level, the agency should refer to the NIST e-authentication technical guidance to identify and implement the appropriate technical requirements.

＜引用部の訳文＞

保証レベルを決定した後、政府機関は適切な技術的要件を識別し実装するために NIST 電子認証技術ガイダンスを参照すべきである。

手順４：実行後、そのシステムが、要求された保証レベルに達しているかを検証する

After implementation, validate that the information system has operationally achieved the required assurance level.

Because some implementations may create or compound particular risks, conduct a final validation to confirm that the system achieves the required assurance level for the user-to-agency process. The agency should validate that the authentication process satisfies the systems's authentication requirements as part of required security procedures (e.g., certification and accreditation).

＜引用部の訳文＞

実行によっては特定のリスクを生み出したり悪化させたりするので、ユーザから政府機関へのプロセスにおいて要求された保証レベルをシステムが満たしていることを確認する最終確認を行うこと。認証プロセスが（例えば、証明と認可など）要求されたセキュリティ・プロシジャーの一部分としてシステムの認証要件を満たしていることを、政府機関は確認すべきである。

手順５：技術の新たな要件を決定するために、定期的に情報システムを再評価

Periodically reassess the information system to determine technology refresh requirements.

The agency must periodically reassess the information system to ensure that the identity authentication requirements continue to be valid as a result of technology changes or changes to the agency's business processes. Annual information security assessment requirements provide an excellent opportunity for this. Agencies may adjust the identity credential's level of assurance using additional risk mitigation measures. Easing identity credential assurance level requirements may increase the size of the enabled customer pool, but agencies must ensure that this does not corrupt the system's choice of the appropriate assurance level.

＜引用部の訳文＞

技術の変化または政府機関におけるビジネスプロセスの変化の結果、identity 認証要件が、有効であり続けるのを保証するために、政府機関は定期的に情報システムを再評価しなければならない。年に一度の情報セキュリティ評価要件を設けることは、再評価のための格好の機会である。追加的なリスク緩和処置を用いて、政府機関は identity 信用証明書の保証レベルを調整することができる。identity 信用証明書の要件保証レベルを緩和することは、有効な顧客プールの規模を増大させる可能性がある。しかし政府機関は、（レベルの緩和が）システムによる保証レベルの選択に悪影響を及ぼさないようにする必要がある。

4.5.4. 保証レベルとリスクプロファイル

表 4-3　保証レベルに応じたリスクプロファイル

保証レベル	説明	例
レベル 1	asserted identity において信頼はほとんど又は全くない。例えば、レベル 1 信用証明書は、人々が今後の参考のためにウェブページにブックマークを付けることを許可する。	1. 電子トランザクションにおける個人によるフォームの提出：駐車場の年間利用許可証を申請するときなど。 2. ユーザがカスタマイズすることができる教育省のウェブページ“My.ED.gov”に、ユーザが独自で登録した ID やパスワードを提示して利用するとき。 3. 名前と場所以外の身元情報を要求されないホワイトハウスのオンラインディスカッションに参加するとき。
レベル 2	総じて asserted identity が正確であるという信頼はある。政府機関が初めに identity 特定を必要とする国民に対する広範囲の業務に、レベル 2 信用証明書が使われる。	1. 政府オンライン学習センター（Gov Online Learning Center）へ会員登録するとき。このトランザクションに関する唯一のリスクは、第三者が成績情報にアクセスするときである。この損害が小さいと判断したとき、政府機関はこの保証レベルの認証と決定する。 2. 社会保障ウェブサイトを通じて、受給者は住所変更を行う。支払額や口座の状態、変更履歴公式通知を受益者の記録されている住所に送るので、機密情報の不正発表の中程度リスクを伴う。 3. 銀行口座やプログラム資格、支払情報を政府機関のプログラムクライアントが更新する。紛失や遅延は重大な影響を与えるが、長期

保証レベル	説明	例
		間ではない。個人の経済的損失の潜在的影響は低いが、総計では中程度の影響である。 4. 潜在的に機密な個人クライアント情報へ政府機関職員がアクセスする。制限の少ない状況では、政府機関職員が行う個人的な機密情報へのアクセスは、機密情報の不正発表の中程度の潜在的影響であるが、システムのセキュリティ対策により低影響になる。
レベル 3	レベル 3 は、asserted identity の正確性において高い信頼度を必要とするトランザクションに適している。追加的な identity assertion の規則を適用せず、ウェブサービスへアクセスするために、人々はレベル 3 信用証明書を使用できる。	1. 特許弁理士が、米国特許商標局へ電子的に機密特許情報を提出する。 2. 大きな政府調達のために、供給者が共通役務庁（General Services Administration）の契約担当官と取引を維持する。経済的損失の潜在的影響はかなり（significant）あるが、重度（severe）や破壊的ではないので、レベル 4 は適切でない。 3. インシデントの報告や運用情報の共有、応答活動の調整のために、最初に応答する人は災害管理報告ウェブサイトへアクセスする。 4. 政府機関の職員または契約者が、潜在的に機密な個人クライアント情報へリモートアクセスで接続する場合（連邦政府のアクセス制御されたビルで働いているものとする）。このとき、入手可能な機密個人情報の不正発表は中程度である。

保証レベル	説明	例
レベル 4	レベル 4 は、asserted identity の正確性において非常に高い信頼度を必要とするトランザクションに適している。identity assertion 以上の規則を要求せずに assert identity によって厳しく制限されたウェブの情報資源へアクセスするために、利用者はレベル 4 認証証明書を提示してもよい。	1. 法執行機関の当局者が、捜査当局にある犯罪歴を含むデータベースへアクセスする。不正アクセスは、プライバシー問題を引き起こし、また捜査を危うくする。 2. 復員軍人省の薬剤師が、規制医薬品を調剤する。その薬剤師は、有資格医師が処方する全ての保証を必要とする。薬剤師は、処方を確認して、定められた量で正しい薬を調剤することに関するあらゆる失敗に対して、刑法上責任がある。 3. 政府機関の調査官が、潜在的に機密な個人クライアント情報へリモートアクセスで接続する場合（ノート PC を用いて外部から接続する）。このとき、不正認証による機密個人情報の不正な流出は中程度であるが、ノート PC の脆弱性と安全でないインターネットアクセスにより、総合的なリスクを引き起こす。

4.5.5. リスクの範囲と要素

リスクの範囲と要素に関して、本ガイダンスに以下の事項が示されている。

When determining assurance levels, one element of the necessary risk assessment is the risk of denial (or repudiation) of electronically transmitted information. Section 9c of OMB's GPEA guidance states agencies should plan how to minimize this risk by ensuring user approval of such information. Section 8c of the OMB Procedures and Guidance on Implementing GPEA includes guidance on minimizing the likelihood of repudiation.

OMB's GPEA guidance states that properly implemented technologies can offer degrees of confidence in authenticating identity that are greater than a handwritten signature can offer. Conversely, electronic transactions may increase the risk and harm (and complicate redress) associated with criminal and civil violations. The Department of Justice's "Guide for Federal Agencies on Implementing Electronic Processes" discusses the legal issues surrounding electronic government. Legal and enforcement needs may affect the design of an e-authentication system and may also entail generation and maintenance of certain system management documentation.

＜引用部の訳文＞

保証レベルを決定する際、必要なリスクアセスメントの 1 つに電子的に送信された情報の拒否（または否認）のリスクがある。OMB の GPEA ガイダンスのセクション 9c では、そのような情報のユーザ承認を確実にすることにより、このリスクを最小にする方法を、政府機関は計画すべきであると記載されている。OMB の GPEA 実行に関する手順とガイダンスのセクション 8 には、否認の可能性を最小限にすることのガイダンスを含まれている。

OMB の GPEA ガイダンスでは、identity 認証において、適切に実行された技術は手書きの署名よりも高い信頼度を提供すると記載されている。逆に、電子的なトランザクションは、民事または刑事上の違反行為に関するリスクと損害（そして補償を困難にすること）を増加させる可能性がある。司法省の「電子プロセスの実行にあたっての連邦政府機関のためのガイド」では、電子政府にまつわる法的な問題について論じられている。法律および施行のニーズは、電子認証システムの設計に影響を及ぼす可能性がある。また、あるシステム管理ドキュメントの作成とメンテナンスを必要とする可能性がある。

4.5.6. クレデンシャル・サービス・プロバイダーの信頼評価

クレデンシャル・サービス・プロバイダーの信頼評価に関して、本ガイダンスに以下の事項が示されている。

> Since identity credentials are used to represent one's identity in electronic transactions, it is important to assess the level of confidence in the credential. Credential Service Providers (CSPs) are governmental and non-governmental organizations that issue and sometimes maintain electronic credentials. These organizations must have completed a formal assessment against the assurance levels described in this guidance.
>
> The CSP's issuance and maintenance policy influences its e-authentication process trustworthiness. The E-Authentication Initiative will therefore develop an assessment process for the government to determine the maximum assurance level merited by the CSP. For example, if a CSP follows all process/technology requirements for assurance Level 3, a user may use a credential provided by the CSP to authenticate himself for a transaction requiring assurance Levels 1, 2, or 3.

＜引用部の訳文＞

identity 信用証明書は、電子的なトランザクションにおいて人の識別を行うために使用されるので、信用証明書の信頼レベルの評価することは重要である。クレデンシャル・サービス・プロバイダー（CSP）とは、電子信用証明書を発行し、場合によっては維持を行う政府や非政府機関である。これらの組織は、本ドキュメントに記述してある保証レベルに対して公式な評価を終えていなければならない。

CSP の（電子信用証明書を）発行および維持管理方針は、電子認証プロセスの信頼性に影響を与える。それゆえ、政府機関が CSP によって得られた最大の保証レベルを決定するための評価プロセスを、E-authentication initiative は明らかにする。例えば、もし CSP が保証レベル 3 に要求される全てのプロセスと技術要件に従っているならば、利用者が、保証レベルが 1, 2, 3 を要求するトランザクションにおいて自分自身を認証するために CSP によって付与された信用証明書を利用しても良い。

4.5.7. 電子認証プロセス

電子認証プロセスに関して、本ガイダンスに以下の事項が示されている。

> Each step of the authentication process influences the assurance level chosen. From identity proofing, to issuing credentials, to using the credential in a well-managed secure application, to record keeping and auditing—the step providing the lowest assurance level may compromise the others. Each step in the process should be as strong and robust as the others. Agencies will achieve the highest level of identity assurance through strong identity proofing, a strong credential, and robust management (including a strong archive and audit process). However, the best authentication systems result from well-engineered and tested user and agency software applications. A process currently being developed for enabling authentication across Federal agencies will be published for implementation when complete.

＜引用部の訳文＞

認証プロセスの各ステップは、選択された保証レベルに影響を与える。identity proofing からクレデンシャル発行、適切に管理されたセキュリティ・アプリケーションにおけるクレデンシャルの使用、記録保存および会計監査まで、最も保証レベルの低い手順は、他の手順も危うくする可能性がある。プロセスの各手順は、他の手順と同様に強く頑丈であるべきである。強固な identity proofing、強固なクレデンシャル、（強固なファイル保管庫や監査プロセスを含む）堅固な管理を通じて、政府機関は最高レベルの identity 保証を成し遂げるだろう。しかしながら、最良の認証システムは、優れた技術と、ユーザと政府機関のソフトウェア・アプリケーションのテストによって支えられる。連邦政府機関で横断的に認証を可能とするための現在の開発されているプロセスは、完成次第、実施のために発表される。

4.5.8. 匿名信用証明書の使用

匿名信用証明書の使用に関して、本ガイダンスに以下の事項が示されている。

> Unlike identity authentication, anonymous credentials may be appropriate to use to evaluate an attribute when authentication need not be associated with a known personal identity. To protect privacy, it is important to balance the need to know who is communicating with the Government against the user's right to privacy. This includes using information only in the manner in which individuals have been assured it will be used. It may be desirable to preserve anonymity in some cases, and it may be sufficient to authenticate that:
>
> - The user is a member of a group; and/or
> - The user is the same person who supplied or created information in the first place; and/or
> - A user is entitled to use a particular pseudonym.
>
> These anonymous credentials have limited application and are to be implemented on a case-by-case basis. Some people may have anonymous and identity credentials. As general matter, anonymous credentials are appropriate for Levels 1 and 2 only.

＜引用部の訳文＞

identity 認証とは異なり、認証が既知の個人識別と関係している必要はないとき、匿名信用証明書は属性を評価するために使用するのが適切だろう。プライバシーを守るために、利用者のプライバシーの権利と誰が政府と通信しているかについて知ることの、必要性のバランスを取るのは重要である。これには、個人がそれが使われると確信した方法だけで情報を使うことを含む。場合によっては匿名性を保つことは、望ましいことがある。その場合、以下のことを認証すれば十分である。

- 利用者はグループのメンバーである。
- 利用者は初めに情報を提供したか作成した人と同一である。
- 利用者は特定の匿名を使用する資格がある。

これらの匿名信用証明書は、アプリケーションを制限し、ケースバイケースで使用される。人によっては、匿名および identity 信用証明書を持っているだろう。一般的

な問題として、匿名信用証明書はレベル 1 か 2 においてのみ相応しい。

4.5.9. 情報共有とプライバシー法

情報共有とプライバシー法に関して、本ガイダンスに以下の事項が示されている。

> When developing authentication processes, agencies must satisfy the requirements for managing security in the collection and storage of information associated with validating user identities. The E-Government Act of 2002, section 208 requires agencies to conduct privacy impact assessments for electronic information systems and collections. This includes performing an assessment when authentication technology is added to an electronic information system accessed by members of the public. For additional information on privacy impact assessments, consult OMB guidance.

＜引用部の訳文＞

認証プロセスを構築するとき、政府機関はユーザアイデンティティの検証に関する情報の収集と保管において、セキュリティを管理するための要件を満たさなければならない。2002 年の電子政府法令においてセクション 208 では、政府機関に電子情報システムと収集のためのプライバシー影響評価を実施することを要求している。これには認証技術が国民によってアクセスされる電子情報システムに追加されるとき、プライバシー影響評価を行うことが含まれている。プライバシー影響評価に関する追加情報については、OMB ガイダンスを参照のこと。

4.5.10. コスト／便益における考慮

コスト／便益における考慮に関して、本ガイダンスに以下の事項が示されている。

> Like any capital purchase, implementing e-authentication requires consideration of the benefit and costs, and thus a cost-benefit analysis is required by the Capital Programming Guide. It is also important to match the required level of assurance against the cost and burden of the business, policy, and technical requirements of the chosen solution.

＜引用部の訳文＞

投資購入と同じように、電子認証を実施するには利益とコストの考慮が必要である。そのため費用便益分析は Capital Programming Guide において必要とされている。更に、選択されたソリューションにおいて、コストやビジネスの負荷、政策および技術的要件に対して必要な保証レベルに合わせることも重要である。

4.6. Registration and Authentication －e-Government Strategy Framework Policy and Guidelines －（英国）

本文書は、電子政府のサービスへのアクセスを求める市民や組織の登録と認証に関するフレームワークのポリシーとガイドラインを示すものである。

4.6.1. 目的

本文書の目的として、以下の事項が示されている。

> This document is intended to set out a number of trust levels for registration and authentication in e-Government transactions.
>
> Current guidance on the use of registration and authentication services in the context of e-Government services is set out in the companion security architecture document.

＜引用部の訳文＞

本書は、電子政府の transaction における登録と認証についての保証レベルを定めることを目的としたである。電子政府サービスに関する登録と認証サービスの利用に関する現行のガイダンスについては、セキュリティアーキテクチャの手引きにおいて示すものとされ、本文書の対象外となっている。

4.6.2. 利用者

本文書の利用者として、以下の事項が示されている。

> This document is aimed at those procuring and providing e-Government services. This includes Central Government Departments, non-departmental public sector bodies, Local Authorities and other local government bodies charged with the provision of e-Government services. It also encompasses regulatory bodies responsible for the proper audit and control of public assets and information.
>
> In addition it includes the suppliers and service providers who wish to offer services themselves, provide and operate such systems on behalf of government or provide equipment in support of e-Government services.
>
> It is also relevant to security authorities that may use this document to assess the suitability of offered solutions and accredit them for operational use.

＜引用部の訳文＞

本ドキュメントは電子政府サービスの入手や提供をするものを対象としている。それには、中央政府省庁、外郭公共団体、地方自治体や、電子政府サービスの提供を担当するその他の地方政府機関等、電子政府サービスの入手や提供をするものも含まれている。また、公的な資産と情報を適切に審査・管理するための責任ある取締機関も含まれる。

そのうえ、政府に代わってサービスを提供・運用を望むサービスプロバイダーや、電子政府を維持させるための機器を提供することを望むものも含まれる。

更に、本ドキュメントは、ソリューションの適合性を評価し、そうしたソリューションの実用を認可するためのセキュリティ機関にも関係がある。

4.6.3. 利用方法の想定

本文書の利用方法の想定として、以下の事項が示されている。

It applies in circumstances where government needs to have trust in the identity (real-world or otherwise) and authority of those it is dealing with to ensure that there is no breach of privacy or confidentiality, theft/misuse of data, or other harm. The framework includes those cases where anonymous or pseudonymous access is acceptable.

Business sponsors must also consider the role of registration, authentication, access control and user access management in the context of government users. The exact requirements may differ from those that relate to clients, since other aspects of security (*eg* physical and procedural) may be applicable.

The applicability of the framework to transactions where government is simply receiving payments *via* electronic media in exchange for the provision of goods, services or information to consumers, for example where a government department wishes to sell goods over the Internet and sets up a website accepting credit card payments, needs to be examined on a case by case basis. It is likely that in these circumstances, good commercial practice should be appropriate.

＜引用部の訳文＞

本ドキュメントが適用する状況は、政府が取引相手の本人性（現実世界またはそれ以外）と権限を信頼し、プライバシーや機密性の侵害、データの盗難／不正使用、その他の危害が存在しないことを確保することが必要な場合である。このフレームワークには、匿名または偽名でのアクセスが認められる場合も含まれる。

ビジネススポンサーは、政府ユーザに関する登録、認証、アクセス制御、ユーザーアクセス管理の役割も考慮しなければならない。セキュリティの他の側面（物理的な面、手順面など）が適用することも考えられるため、ビジネススポンサーに対する厳密な要件はクライアントに関係する要件とは異なりうる。

政府が消費者への財、サービス、または情報の提供の見返りとしての支払いを電子的媒体で受領するだけの取引の場合（たとえば政府省庁がインターネットでの財の販売を希望してクレジットカード決済を引き受けるウェブサイトを設ける場合）は、取引に対するこうしたフレームワークの適用性をケースバイケースで検討する必要がある。そのような状況では、良い商慣行が使用されるべきであると思われる。

4.6.4. 運用方法

特に記述されていない。

4.6.5. 特徴

本フレームワークは、登録や認証が必要である全ての電子政府または電子政府代理との電子取引に適用される。また、中央政府省庁および政府機関は、電子取引に関して本フレームワークを満たさなければならない。その他公共団体については、企業や他の公共団体、公共団体の代理との間で行なわれる取引において、本フレームワークの助言を受け入れることが強く推奨される。

4.7. Australian Government E-Authentication Framework（オーストラリア）

4.7.1. 目的

本文書の目的として、以下の事項が示されている。

> Being able to conduct transactions online provides advantages to businesses and government by enabling around-the-clock services, shorter waiting times, paperless transactions and streamlined processes. However, as online transactions increase in frequency and signifi cance, the risks associated with such transactions can also increase.
>
> To provide a consistent, whole-of-government approach to managing these risks, the Australian Government Information Management Office (AGIMO) of the Department of Finance and Administration has developed the Australian Government e-Authentication Framework (AGAF).

＜引用部の訳文＞

オンラインによる取引を行えるようにすることは、24 時間サービスの実現、待ち時間の短縮、ペーパーレス取引と能率化されたプロセスにより企業と政府に便宜をもたらす。しかしながら、オンライン取引の頻度と重要性が増大すると、そうした取引に関連したリスクもまた増大する。

こうしたリスクを管理するための一貫した政府全体へのアプローチを提供するため、オーストラリア政府の財務管理省情報管理局（AGIMO）はオーストラリア政府認証フレームワークを作成した。

4.7.2. 利用者

本フレームワークの利用者としては、まず政府と企業が対象とされ、個人への拡張が進められている。

（1） 政府と企業

フレームワークの利用により、政府とのオンライン取引における信頼性の強化と取引におけるリスクレベルに応じた電子認証メカニズムとの適合を目指している。本フレームワークで規定するリスクレベルは、記述の米国 OMB によるものと同趣旨の 4 段階となっている。

（2） 政府と個人

個人を対象とするものについては、政府と企業を対象にするフレームワークを拡張

する形で、オーストラリア政府により議論が進められている。

4.7.3. 利用方法の想定

本フレームワークが企業にもたらす利点として、以下の事項が示されている。

Benefits to businesses

The AGAF provides a guide for Australian businesses on how to conduct transactions securely with Australian Government agencies on a wide range of matters and through a wide range of deliverychannels.

This will benefit businesses by enabling:

+ electronic transfer of funds or private information by government

+ around-the-clock services

+ shorter waiting times for services

+ paperless transactions with government, and

+ streamlined processes.

＜引用部の訳文＞

AGAF は、広範囲の流通チャネルを通じた広範囲の状況において、オーストラリアの企業がオーストラリア政府機関と安全な取引を確立する方法のガイドを提供する。

これは以下の事項を可能とすることでビジネスに利点をもたらす。

- 政府による資金やプライベート情報の電子的移送
- 24 時間サービス
- サービスの待ち時間減少
- 政府とのペーパーレス取引
- 能率化されたプロセス

4.7.4. 運用方法

AGAF は以下の原則のもとに運用されることが示されている。

Principles guiding the AGAF

The following principles will guide the selection and implementation of e-authentication approaches:

+ Transparency – e-authentication decisions will be made in an open and understandable manner.

+ Cost-effectiveness – businesses will not have to undergo cumbersome and expensive e-authentication processes for simple or low-risk transactions.

+ Risk management – the selection of e-authentication mechanisms will be guided by the likelihood and impact of identified risks.

+ Consistency – government agencies will apply a consistent approach to selecting e-authentication mechanisms.

+ Trust – the mechanisms used will support online services and be useful and safe.

+ Improved privacy – personal information will be collected only where necessary for the business processes being undertaken.

＜引用部の訳文＞

電子認証のアプローチに関する選択と実装は、以下の原則のもとで定められる：

- 透過性：電子認証における決定は、オープンかつ理解できるような方法でなされる。
- 費用対効果：企業は単純であるかリスクの低い取引のために、扱いにくく高価な電子認証プロセスに耐える必要はない。
- リスクマネジメント：電子認証メカニズムの選択は、起こり得る可能性と識別されたリスクの影響によって定められる。
- 一貫性：政府機関は、電子認証メカニズムの選択に対して一貫した方法を適用する。
- 信頼：使用されるメカニズムは、オンラインサービスをサポートし、便利かつ安全である。
- プライバシー強化：個人情報は、保証されたビジネスプロセスにおいて必要な場合にのみ収集される。

4.7.5. 特徴

本フレームワークの特徴として、政府と企業それぞれに向けて、オンライン取引を行う際に考慮すべき項目のチェックリストを提供していることが挙げられる。

4.8. Authentication for e-government Best Practice Framework for Authentication（ニュージーランド）

リスク評価の方針と信用レベルの定義についてのガイドラインである。また、オンライン認証ソリューションの実装方法について解説している。

4.8.1. 目的

本文書の目的として、以下の事項が示されている。

> The Framework is one of a series of documents related to an all-of-government approach to online authentication and is aimed at providing a guideline for agencies in the area of authentication.

> The Framework provides:
>
> - information on concepts and terminology related to authentication;
> - references to an all-of-government approach and the long-term strategic vision for all-of-government authentication;
> - guidance and advice regarding the issues that need to be addressed through planning and policy work; and
> - information on implementing an online authentication initiative and issues to consider.

＜引用部の訳文＞

本フレームワークは、オンライン認証に関係する全ての政府機関のアプローチに関する一連の資料の 1 つであり、政府機関での認証分野におけるガイドラインを提供することを目的としている。

具体的には、本フレームワークは以下の情報を提供している。

- 認証に関する概念と用語についての情報
- 全ての政府組織へのアプローチ、及び全ての政府組織における電子認証の長期的戦略ビジョンについてのリファレンス
- 計画と方針決定においての取り組むべき問題に関する指針と助言
- オンライン認証 initiative の実行と考慮すべき問題に関する情報

4.8.2. 利用者

オンライン認証プロジェクトの計画に関わる人、または要件決定を行う人を対象としている。特に以下の人を対象としている。

- 政府の認証構想とオンライン認証向け長期戦略目標を高いレベルから俯瞰することを希望する人
- 認証ソリューション案が省庁とクライアントに与える可能性のある効果と方針に関心のある人
- 認証の技術的実現について興味のある読者、計画と構築に関する認証オプションの検討を考える人
- 大規模な IT プロジェクト導入関連の基準と、政府の指示遵守に関心のある人

4.8.3. 利用方法の想定

電子政府サービスの中でも特に認証が必要なサービスを構築する際に利用される。

4.8.4. 運用方法

認証技術と実践の変化、オンライン認証の戦略的方向性に関する政府の意思決定を反映されるため、本フレームワークは定期的に改訂されることに注意すること。

4.8.5. 特徴

電子認証の実装方法について詳細に述べており、また製品やサービス選択に関する助言も含まれている。

本フレームワークでは、省庁が必ず採択すべき基準は指示していない。

4.9. Interchange of Data between Administrations (IDA) Authentication Policy（EU）

4.9.1. 目的

本文書の目的として、以下の事項が示されている。

This document aims at defining the IDA authentication policy, which can serve as a basic policy for establishing the appropriate authentication mechanisms in sectoral networks and in horizontal security-related projects.

Considering the nature of the IDA mission as defined by the European Commission, we believe that the scope of the IDA Authentication Policy shall be limited to the remote authentication of participants in IDA Sectoral Networks (i.e. primarily public servants of the Member State Administrations and the European Institutions) using electronic credentials.

Moreover the above analysis shows that:

- 2 main phases shall be considered in the whole authentication process: the registration phase (i.e. identity proofing + token delivery) and the remote electronic authentication (i.e. proof of possession of the token);
- The registration phase requires a Registration Authority and a Credential Service Provider to be present in one way or another (preferably locally so as to cope with the subsidiarity principle) in the authentication process;
- Several Authentication Assurance Levels shall to be defined;
- Common rules have to be defined and agreed (in particular to achieve the identity proofing of public servants) to encourage mutual recognition within sectoral applications;
- Authentication and authorisation are separate decisions
- Not only individual authentication but also group authentication shall be considered.

＜引用部の訳文＞

本ドキュメントは、IDA（Interchange of Data between Administrations）認証ポリシーの定義を行うことを目的としている。そのポリシーは、部門毎のネットワークや横断的なセキュリティに関するプロジェクトにおいて、適切な認証メカニズムを規定するための基本ポリシーとして役立つものである。

欧州委員会によって定義ていることから、IDA ミッションは IDA 認証ポリシーの対象は電子証明書を用いた IDA Sectoral Network （つまり、主として加盟国の政府やヨーロッパの公共機関の公務員）において、参加者の遠隔認証に限られていると考えられる。

更に、上記の分析は次のものを示す。

- 全体の認証プロセスにおいて、次の 2 つの主なフェーズがある：登録フェーズ（つまり、identity proofing とトークン配送）と遠隔電子認証（つまり、トークン所有の証明）。
- 登録フェーズでは、認証プロセスにおいて何らかの方法（望ましくは、欧州連合における補完性原理を対処する局所的なもの）で、登録局（Registration Authority）とクレデンシャル・サービス・プロバイダーが存在することを必要とする。
- 幾つかの認証保証レベルが定義されるようにすべきである。
- 部門別のアプリケーションにおける、相互の認識（特に、公務員による identity proofing の実現）の為、共通のルールが定義され、合意を得ている必要がある。
- 認証（authentication）と認可（authorisation）は別々に決定する。
- 個人の認証だけでなく、グループ認証も考慮されるべきである。

4.9.1.1. 用語の説明

（1） identity proofing

identity proofing は、正しく関連している(恐らく名前だけの)属性を用いて、identity が実際に実在の人物であることを保証するプロセスである。保証のレベルを上げることは、参加者の identity を保証するための取り組みを増やすことを必要とする。identity proofing を行うエンティティは、Registration Authority (RA)である。

（2） Registration Authority (RA)

Registration Authority (RA)は、通常は紙の証明書の提示やデータベースの記録によって加入者の identity 確認する役割を果たす。RA は順々に CSP へ参加者の identity を保証する。

（3） クレデンシャル・サービス・プロバイダー (CSP)

CSP は、参加者へ認証プロセスにおいて使用されるトークンを登録または与え、トークンと identity を結びつけたり、identity と何かしら使いやすい属性と結びつけたりする必要に応じて証明書を発行する。参加者は、登録の時点でトークンと組になる電子証明書を受け取るか、後ほど必要に応じて証明書を発行してもらう。

常に RA と CSP は結びついている。最も単純で、おそらく最も一般的な場合は、RA と CSP は同一のエンティティで別々の機能を有しているものである。しかしながら、RA は、独立している CSP や複数の異なる CSP の参加者を登録する会社や組織の一部であるかもしれない。従って、ある CSP には不可欠な RA が存在するかもしれないし、複数の独立した RA と結びついているかもしれない。そして、RA もまた複数の CSP と結びついている可能性がある。

（4） sectoral application（SA）

部門別のアプリケーションは、運用や共同利用できる telematic networks を設立することにより、加盟国の政府へ汎ヨーロッパサービスを提供することを目的としたアプリケーションである。

4.9.2. Sectoral Project 認証ポリシーの作成

Sectoral Application[8] Ownersは、次のように認証ポリシーを作成すべきである。基本的な流れは、米国の“ E-Authentication Guidance for Federal Agencies ”と同様である。

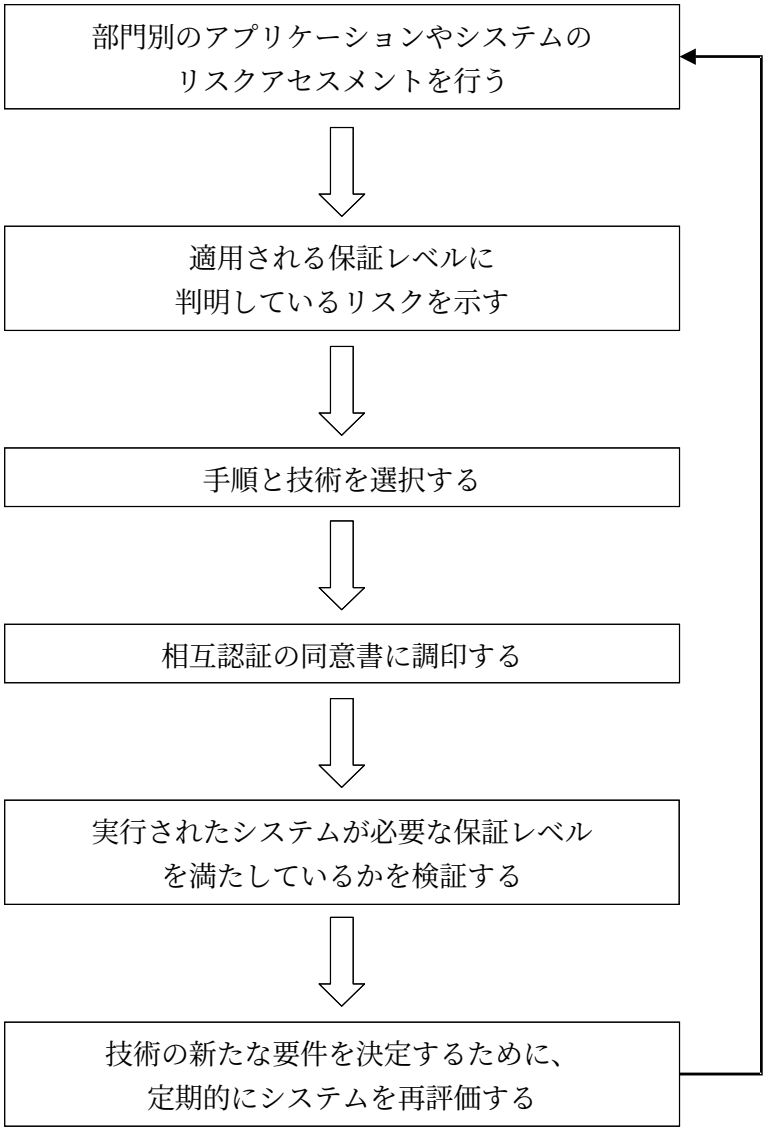


図 4−3 認証ポリシー作成の手順

[8] ここではsectoral applicationを部門別または部門内のアプリケーションと記述する。

ステップ 1：Sectoral Application やシステムのリスクアセスメントを早急に行う

公務員の主張した identity における適切な保証レベルの決定のために、sectoral application Owners は潜在的リスクの評価とそれらの影響を最小にする処置を特定しなければならない。潜在的により悪い結果を及ぼす認証エラーは、より高い保証レベルを必要とする。ビジネスプロセスとポリシー、技術はリスクを低減させることに役立つだろう。

ステップ 2：適用される保証レベルに判明しているリスクを示す

このステップは、全ての確認されたリスクの基準に従って要求される認証保証レベルを定めることにある。表 4.9.3 にあるマトリックスを参照のこと。

ステップ 3：手順と技術を選択する

リスクアセスメントと適用される保証レベルに判明しているリスクを示した後、sectoral application Owners は、適切な技術（つまり、要求する保証レベルの要件で最低限の技術）を選択する。特に、この提案されている IDA 認証ポリシーは、以下の分野における 4 つの各々の保証レベルに対する特定の技術要件について述べられている。

- identity proofing とクレデンシャルの交付を含む登録
- identity を証明するためのトークン
- 遠隔認証メカニズム
- メカニズムの判定

ステップ 4：相互認証の同意書（MRA）に調印する

いったん認証ポリシーが選ばれると、当事者間で MRA に調印しなければならない。1 つの部門内プロジェクトに対して双方での MRA の調印を行うことが膨大な数になることを避けるために、部門内プロジェクトのマネージャーと担当している専門家の委員会／グループの間で、一回の MRA に調印を行うことが望ましい。もし、部門内プロジェクトにそのような専門家の委員会／グループがないならば、欧州委員会と各々関わった加盟国の間で一回の MRA に調印しなければならない。

ステップ 5：実行されたシステムが必要な保証レベルを満たしているかを検証する

複数の実行が特定のリスクを生じさせるか悪化させるので、そのシステムが部門別のアプリケーションを利用するために要求された保証レベルを満たしていることを確認し、最終的な検証を行う。認証プロセスが必要な（例えば certification と authentication の）セキュリティ手順の一部としてシステムの認証要件を満たしていることを、部門別プロジェクトでは確認されなければならない。

ステップ 6：技術の新たな要件を決定するために、定期的にシステムを再評価する

技術の変化や部門内アプリケーションにおけるビジネスプロセスの変化の結果 identity 認証要件が有効であり続けていることを保証するために、sectoral project は定期的に情報システムを再評価しなければならない。年に一度、情報セキュリティの評価要件を設けることは、上記のための格好の機会を与える。部門内プロジェクトでは、追加的なリスク緩和処置を用いて identity 証明書の保証レベルを調整してもよい。identity 証明書の要件保証レベルを緩和することは、使用可能となる顧客対象を増加させるかもしれないが、部門内プロジェクトは、（レベルの緩和が）システムの保証レベルの選択に悪影響を及ぼさないように実施される必要がある。

4.9.3.（Annex）認証保証レベルの定義テンプレート

ここに、本文書の付録にある認証保証レベルの定義テンプレートの 1 つを載せる。表 2 5 ではリスクとして Fictitious real-world identity を記しているが、実際の付録には各リスクに対して同様の定義テンプレートが載せてある。

表 4-4　認証保証レベルの定義テンプレート

リスク	可能性	損害のインパクト				
		非常に高い	高い	中間	低い	極わずか
Fictitious real-world identity	ほとんど確か	（＊）	（＊）	レベル 4	レベル 3	レベル 3
	起こりえる	（＊）	レベル 4	レベル 3	レベル 3	レベル 2
	中程度	レベル 4	レベル 3	レベル 3	レベル 2	レベル 2
	起きそうもない	レベル 3	レベル 3	レベル 2	レベル 2	レベル 1
	滅多にない	レベル 3	レベル 2	レベル 2	レベル 1	レベル 1

（＊）：オープンネットワーク上では遠隔認証は適用できない

4.9.4. 認証ポリシーフレームワーク

ここでは、まず始めに保証レベルを定義し、次に迅速なリスクアセスメントに基づく保証レベルの選択方法を説明する。最後に、各レベルでの登録と電子認証を成し遂げるための手順と技術を示す。

4.9.4.1. 認証保証レベルの定義

（1） 認証保証

本文書では認証保証に関して、以下の事項が示されている。

Note: The authentication assurance describes the Sectoral Application's degree of certainty that the public servant has presented a credential that refers to his identity.

In this context, authentication assurance is defined as

- the degree of confidence in an asserted real-world identity (i.e. identity proofing)
- the degree of confidence in an electronic identity presented to a service provider by means of a credential (i.e. proof of possession)

＜引用文の訳文＞

注意：この認証保証は、公務員による本人性を示すクレデンシャルの提示に対する、部門別のアプリケーションにとっての確実さの度合いを記述している。

ここでは、認証保証は次のように定義される。

- 現実社会で主張されている本人性の信頼の程度（すなわち本人性の証拠）
- クレデンシャルを使ってサービスプロバイダーへ提示された電子的な本人性の信頼の程度（すなわち所有の証明）

（2） レベル

本文書ではレベルに関して、以下の事項が示されている。

Note: Our approach is to consider that authentication assurance levels should be layered according to the severity of the impact of damages that might arise from misappropriation of a person identity.

The more severe the likely consequences are, the more confidence in an asserted identity will be required to engage in a transaction.

We suggest 4 assurance levels to be defined:

- Level 1: .....Minimal Assurance
- Level 2: .....Low Assurance
- Level 3: .....Substantial Assurance
- Level 4: .....High Assurance

＜引用部の訳文＞

注意： person identity の不正流出から生じ得る損害の影響の重大性によって認証保証レベルが階層化されるべきだ、という考えからのアプローチである。

起こりうる結果がより深刻なほど、トランザクションに携わっている主張された本人性についてより多くの信頼が要求される。

4 つの保証レベルを次のように定義する。

- レベル 1：最小の保証
- レベル 2：低い保証
- レベル 3：かなりの保証
- レベル 4：高い保証

（3） 登録と認証の方法へのアプローチ

本文書では登録と認証の方法へのアプローチに関して、以下の事項が示されている。

It should be noted that, for a given transaction, registration and authentication might not possess equal emphasis and thus would attract different levels (i.e. Level 2 registration does not necessarily imply a requirement for Level 2 authentication and so on).

As an example, a transaction such as pseudonymous access to medical testing would need unequal levels of registration and authentication since a real-world identity is not required but strong authentication is needed to ensure that the results are disclosed only to the client possessing the correct electronic identity.

Note: Member State Administrations should allocate each sectoral application to both a registration and authentication level in accordance with the guidance contained in the proposed IDA Authentication Policy.

＜引用部の訳文＞

あるトランザクションにおいて、登録と認証は同等の重要性を持っていないかもしれなく、その結果、異なるレベルを招く（つまり、レベル 2 の登録は必ずしもレベル 2 の認証を必要とするわけではない）ことを注意しなければならない。

例えば偽名などを用いて医療検査へアクセスするトランザクションは、登録及び認証と同等のレベルは必要とされない。なぜなら、現実世界の本人性は要求せず、電子的に正しい本人性を持つ患者にだけ結果を開示することを保証するために強い認証を必要とするからである。

注意：加盟国の政府は提案された IDA 認証ポリシーに含まれるガイダンスに従ってそれぞれの sectoral application を登録と認証レベルへ割り当てるべきである。

4.9.5. リスクマネジメント

sectoral application Owners が受け入れるリスクのレベルは、資産評価やリスクの正しい識別、それらリスクを管理するために利用できる資産提供のレベル、生命・資産・サービスに及ぼす潜在的影響を含む幾つかの要因に依存している。

4.9.5.1. 評価

IDA 認証ポリシーの定義を目的としているため、データの評価のみを対象とする。

本文書では評価に関して、以下の事項が示されている。

> Whatever the nature of the DATA being exchanged over sectoral networks, i.e. CLASSIFIED or UNCLASSIFIED, there is so far no possibility to establish a one-to-one mapping between EC classification levels for information security (as defined by Council Decision [RD8]) and authentication assurance levels. The explanation for this is twofold:
>
> - On one hand, the processing of "unclassified" data over sectoral networks does not necessarily indicate a "low assurance" as far as authentication is concerned;
> - On the other hand, the use of "remote electronic authentication" may reveal not secure enough to process EU-Confidential data (or even more sensitive data), as regard to the impact of damage in case of disclosure, loss, or unauthorised modification of such data (as described in Annex A).

＜引用部の訳文＞

sectoral network 上でやり取りされているデータの性質が何であれ（すなわち CLASSIFIED または UNCLASSIFIED であれ）、（Council Decision [RD8]として定義されている）情報セキュリティのための EC（Electronic Certificate）分類と認証保証レベルの間には 1 対 1 の対応を付ける実現性は今のところない。これについての説明は次の 2 つである。

- 一方では、認証に関する限り、sectoral network 上で『分類されていない』データの処理は必ずしも『低い保証』を示すというわけではない。
- 他方では、（Annex A に記述されている）データの公開または損失、未許可の変更などの場合には損害の影響を考慮して、『遠隔電子認証』の使用は EU 秘密データ（又は更に機密なデータ）の処理においては充分には安全でないと示されるかもしれない。

表 4-5　レベルによるデータ評価の分類

<table>
<tr><td>情報セキュリティに対して EU 分類と認められたもの</td><td colspan="4">認証保証レベル</td></tr>
<tr><td></td><td>1</td><td>2</td><td>3</td><td>4</td></tr>
<tr><td colspan="5">分類された情報</td></tr>
<tr><td>EU 最高機密
（Top-Secret）</td><td colspan="4" rowspan="3">（1）</td></tr>
<tr><td>EU 機密
(Secret)</td></tr>
<tr><td>EU 秘密
(Confidential)</td></tr>
<tr><td>EC 部外秘
（Restricted）</td><td></td><td></td><td>×（2）</td><td>×（2）</td></tr>
<tr><td colspan="5">分類されていない情報</td></tr>
<tr><td>制限されている
（Limited）</td><td>×</td><td>×</td><td>×</td><td>×</td></tr>
<tr><td>内部の
（Internal）</td><td>×</td><td>×</td><td>×</td><td></td></tr>
<tr><td>公開
（Public）</td><td colspan="4">N/A</td></tr>
</table>

（1） 分類された情報に対する認証保証レベルは、Council と Commission Security の規定によって特定されている要件を遵守しなければならない。具体的には、最低でも次を満たすこと。

- そのような機密扱いの情報へのアクセスを必要としている人は、適切な認可を必要とする（EU-Confidential またはそれより上位）
- そのような情報の電子取り扱いを必要とするシステム（特に電子資

格証明書を使用する遠隔認証）は、対応するレベルで『公認されること』を要求する。従って、その公認のための SSRS は、そのようなシステムの認証の観点で規則と状況を正確に定義する。

そういうわけで、現在では IDA 認証ポリシーの範囲外にある。

（2） 適切なリスクアセスメントを受ける

4.9.5.2. リスクによる識別

本文書ではリスクによる識別に関して、以下の事項が示されている。

Risk is normally defined as the chance or likelihood of damage or loss. This definition can be extended to include the impact of damage or loss. That is, it is a function of two separate components, the likelihood that an unwanted incident will occur and the impact that could result from the incident. **Note: Only general risks pertaining to registration and authentication processes and those pertaining to misappropriation of credentials/electronic identity and/or real-world identity are considered here.**

＜引用部の訳文＞

リスクは通常、損害や損失の機会もしくは見込みとして定義される。損害や損失の影響を含むように、この定義を拡張することができる。つまり、望まれていないインシデントが起こりそうな見込みとそのインシデントによる影響という 2 つの別々のコンポーネントの機能である。

注意：登録と認証プロセスに関係する一般的なリスクと、電子および現実の identity 証明書の悪用に関係する一般的なリスクのみここでは考慮されている。

表 4-6　認証エラーに関係するセキュリティリスクの一覧

リスク ID	タイプ	説明
リスク 1	Fictitious real-world identity	クライアントが Fictitious real-world identity に関係する証明書を得る。
リスク 2	False details	偽の情報が実世界の identity に扮いて記録され、それが信頼を得てしまう。
リスク 3	アクセストークンの盗難	証明書を含むアクセストークンがユーザから盗まれるかユーザへ配送中に盗まれるかして、成りすましによってそれを使用される又はユーザの情報を得るためにその後不正使用されること。
リスク 4	実世界での identity（real-world identity）の盗難	本物の実世界での identity は、登録の時点で悪用される。
リスク 5	秘密の認証情報の妨害または暴露	（PIN や個人の署名鍵のような）秘密情報は、証明書を使用したとき送信中に傍受されるか、ユーザまたは第三者の故意・不注意によって露呈してしまう。
リスク 6	信頼されていない端末での秘密の認証情報の記憶	（家庭用またはオフィスの PC、インターネットカフェや公共のキオスクの PC など）信頼されていない端末に秘密情報が記憶される。そのような秘密情報（例えば、端末での暗号機能を実行するために使われる個人の署名鍵や暗証番号）は、ウェブベースのフォームに入れられ、後にキャッシュに保存されるかもしれない。
リスク 7	アクセストークンの権限のない使用	トークンとして発行されたユーザ以外の者によってアクセストークンが使用される。

リスク ID	タイプ	説明
リスク 8	危殆化された証明書の使用	証明書が危殆化した後に使用される。
リスク 9	状況の実質的な変化の後の証明書の使用	本来なら証明書が発行されていないことを意味するくらい状況が変化したところで証明書が使用される。
リスク 10	意図されていない目的での証明書の利用	想定した取引の種類や価値のために発行者が発行した証明書を、準備されていない取引に関して使用される。
リスク 11	正統な理由のない証明書の取り消し	状況の変化や証明書の危殆化などにおいて、誤りか悪意ある報告により証明書が取り消される。
リスク 12	証明書の詐欺的な使用	個人的にか第三者を通じて、所有する証明書が権限の与えられていない取引への使用が試みられる。
リスク 13	ハッカー攻撃	何らかの私利を獲得する目的や EU への迷惑行為、システムへのアクセス拒否、システムへの損傷をもたらすために、敵意ある部外者が Sectoral Application サービスに直接のアクセス権を得るかもしれない。
リスク 14	情報の分散格納	様々な電子政府サービスに集められた情報の断片化のために、クライアントの情報がより危ういリスクとなる。

4.9.5.3. 損害

本文書では損害に関して、以下の事項が示されている。

Every sectoral application owner will be in charge of analysing damages resulting from a breach in the authentication process and assess their impact. To help him in this process, we suggest the possible impact of damages to be chosen among those listed below (Table 3).

＜引用文の訳文＞

全ての部門別アプリケーション所有者は、認証プロセスでの違反から生じる損害を分析し、損害の影響を評価することの責務を負う。このプロセスの手助けのために、以下に記載したリスト表 5‐7 から損害の起こりうる影響を選択することを推奨する。

表 4-7　損害

損害	コメント
完全性の喪失	システムとデータの完全性は、情報が不適当な変更から保護されるという要件について言及している。意図的であるか偶然の行為によってデータや IT システムに許可されていない変更が行なわれると、完全性は喪失する。もしシステムやデータにおける完全性の喪失が修正されないのならば、汚染されたシステムや改竄されたデータの継続的使用は、不正確や詐欺、誤った決定をもたらすかもしれない。また、完全性の侵害は、システムの可用性や機密性に対する攻撃に先立って実行されたものかもしれない。これら全ての理由のために、完全性の喪失は IT システムの保証を低減させることとなる。
可用性の喪失	エンドユーザが基幹 IT システム（mission-critical IT system）を利用できないならば、組織のミッションに影響を及ぼすかもしれない。例えば、システム機能と操作の有効性の損失は、生産的な時間の損失をもたらすかもしれない。その結果、組織のミッションをサポートするシステム機能は、エンドユーザのパフォーマンスを阻害する。
機密性の喪失	システムとデータの機密性は、不正開示からの保護の観点から言及される。機密情報の不正開示における影響は、国家の安全を危険にさらすことからプライバシー保護法データ（個人データ等のプライバシー保護の対象となるデータ）の流出にまで及ぶ。未許可または予期しない、意図的でない流出によって組織存続の上での評価を失う。これは評判の悪化、信憑性の損失や不利な結果、信用の失墜、困惑、または訴訟を伴う。

損害	コメント
個人の安全に対するリスク	情報の不正開示や変更、非可用性は、個人の安全を生死にかかわる危険にさらしめる可能性がある。例えば次の通りである。 ・ 特定個人の住所の不正開示は、政治的・不平・その他の動機であれ、その人に害を加えたいと望んでいる人々に狙われるかもしれない。 ・ （例えば、製造プロセスや交通移動、医療行為などに関わる）情報の不正変更は、設備の誤作動、安全や人々の幸福での悪影響によって誤った決定などを起こしかねない。 ・ （例えば、交通移動や医療行為などに関わる）システムの情報の非可用性は、安全や人々の幸福での悪影響によって決定が遅れたり誤ったりすることをもたらしかねない。
経済的損失	金銭的な取引に直接関わる情報や関係組織の経済的な状態に関する情報が IT システムに格納され処理される。非可用性や破壊と同様に、そのような情報の不正開示と改竄によって経済的損失を被るだろう。例えば、遅延かアクションが無いことによる、株価の低下や詐欺、契約違反による損害である。同時に、非可用性の結果や情報の破壊などは、ユーザへの混乱を招く。そのようなインシデントからの修正または復旧は時間と労力を要する。このようなことは場合によっては重要であり、考慮されなければならない。共通名目を利用するために、復旧のための時間を人月によって計算し、財務費用に換算すべきである。この費用は、組織内で適当な等級/レベルでの人月の正常原価を参照することによって計算されるべきである。

4.9.5.4. Likelihood Determination

本文書では Likelihood Determination に関して、以下の事項が示されている。

To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment, the following governing factors must be considered:

- Threat-source motivation and capability
- Nature of the vulnerability
- Existence and effectiveness of current controls.

＜引用文の訳文＞

潜在的脆弱性が関連する脅威環境の構図の範囲内で実行されるかもしれないという可能性を指し示す総合的な見込み評価を導くために、以下の支配的な要因は考慮しなければならない。

- 脅威の原因のモチベーションと脅威ができること
- 脆弱性の本質
- 現在のコントロールの存在と有効性

表 4-8　Likelihood Level

Likelihood Level	Likelihood Definition
ほとんど確か	脅威の原因は、大いに動機付けられていて充分な能力を有している。そして、その脆弱性が実行されることを阻止するコントロールは効果がない。
起こりえる	脅威の原因は、大いに動機付けられていて充分な能力を有している。しかし、その脆弱性が実行されているところはコントロールが効く。
中程度	脅威の原因は、動機付けられていて能力を有している。しかし、その脆弱性が実行されているところはコントロールが効く。
起きそうもない	脅威の原因は、動機付けか能力に欠けている。又は、コントロールによって脆弱性の実行を阻止できるか、少なくともかなり阻止できる。
滅多にない	脅威の原因は、動機付けと能力に欠けている。又は、コントロールによって脆弱性の実行を阻止できる

4.9.5.5. Impact Severity Scaling

表 4-9　Scale ranging of impact severity.

記号	範囲	説明
N	無視できる	損害は通常の操作で対処される
L	低い	損害は、いくらかのサービスの効率または効果を脅すが、内部的に対処することができる
M	中間	損害は、サービスの提供は脅かさないが、加盟国の政府は重大な検査を受けるか機能の方法を換えることを意味する。
H	高い	損害は、サービスの継続的な供給を脅かし、トップレベルのマネジメントか政府の干渉を要する
V	非常に高い	損害は、クライアントと政府に対して重大な問題を引き起こして、主要なサービスの供給を脅かす

4.9.5.6. レベルによるリスクの測定

既存のリスク低減尺度のあるバックグラウンドとは対照的に、リスクの測定は事件の起こりやすさと損害の影響の両方の関係で決定される。

損害の影響、及び起こりやすさは、リスクレベルの決定に対して決定的になってはならない。部門内アプリケーションでの最も大きなリスクは、強烈な影響を持っており、ほぼ間違いなく起きてしまうというものである。逆に、影響を無視でき、また滅多に起きない事件は取るに足らないものと考えられる。滅多に起こらないが強烈な影響を与えるイベントは、重大なリスクであると考えられる。

特定されたリスクを考慮に入れて、Application に必要な認証保証レベルを推測するために部門別アプリケーションの責任者は、効果的なリスクマトリックスの開発が望ましいかも知れない。このプロセスを手助けするために、リスクの測定（MoR: Measure of Risk）から、考慮されたそれぞれのリスクを低減させることを要求するし最小の認証保証レベルへ落とし込むことができる参照マトリックス（表 4-10）を作成した。

表 4-10　リスクの測定／認証保証レベルマトリックス

		損害の影響				
	Likelihood	非常に高い	高い	中間	低い	無視できる
リスク i	ほとんど確か	（＊）	（＊）	レベル 4	レベル 3	レベル 3
	起こりえる	（＊）	レベル 4	レベル 3	レベル 3	レベル 2
	中程度	レベル 4	レベル 3	レベル 3	レベル 2	レベル 2
	起きそうもない	レベル 3	レベル 3	レベル 2	レベル 2	レベル 1
	滅多にない	レベル 3	レベル 3	レベル 2	レベル 2	レベル 1
	ほとんど確か	レベル 3	レベル 2	レベル 2	レベル 1	レベル 1
（＊）オープンネットワーク上では遠隔認証は適用できない						

4.9.6. 登録

本文書では登録に関して、以下の事項が示されている。

> In our approach, levels 1 and 2 recognise the use of anonymous credentials. When anonymous credentials are used to imply membership in a group, the level of proofing should be consistent with the requirements for the identity credential of that level. Explicit requirements for registration processes for anonymous credentials are not specified, as they are unique to the membership criteria for each specific group.
>
> At Level 2 and higher, records of registration shall be maintained either by the RA or by the CSP, depending on their relationship.

＜引用部の訳文＞

本ポリシーのアプローチでは、レベル 1 と 2 は匿名の証明書の使用を認める。匿名の証明書がグループの会員資格を意味するのに用いられるとき、証明のレベルは identity 証明のために要求されるレベルと一致しているべきである。匿名の証明書のための登録プロセスは明確な用件は特定されておらず、それぞれ特定のグループおいて特有の会員基準に則る。

レベル 2 やそれ以上において、登録に関する記録は、それらの関係によって RA か CSP により保守されるべきである。

4.9.7. 電子認証方法

本文書での POLSECD[RD7]からの引用部分を以下に示す。

Extract from POLSEC [RD7]:

Authentication is generally achieved through one or more of the following methods:

- **Authentication by Knowledge (a.k.a. "Something you know").** This method is based on something the user knows. This could be a password or a Personal Identification Number (PIN). This method is based on the assumption that the value used for authenticating a certain person is only known to that person.
- **Authentication by Ownership (a.k.a. "Something you have").** This method is based on something that the user possesses. This could be, for example, a smart card, hardware token, an identity card or a door key. The method is based on the assumption that it is difficult for an attacker to replicate the object used for authentication, and that users do not allow other persons to use their authentication objects.
- **Authentication by Characteristic (a.k.a. "Something you are").** This method is based on the utilisation of biometrics to recognise one or more unique characteristics of the user, such as the retina pattern and fingerprints. This method is based on the assumption that certain human characteristics can uniquely identify human beings.

＜引用部の訳文＞

POLSEC [RD7]からの引用：

一般に、認証は以下の方法の 1 つ以上を用いて達成される。

知識（"Something you know" の別名でも知られる）による認証。この方法は、ユーザの何かしらの知識に基づいている。これは、パスワードや暗証番号（Personal Identification Number：PIN)）によってなされる。この方法は、" 特定の人を認証するために使用される値は、その人しか知らない値である "という仮定に基づいている。

所有（"Something you have"の別名でも知られる）による認証。この方法は、ユーザの何かしらの所有に基づいている。例えば、スマートカードやハードウェアトークン、ID カード、ドアの鍵などがこれに当たる。この方法は、" 認証のために使用されるものを攻撃者が複製することが困難であり、ユーザはそれら認証のためのものを他人が使用することを許さない " という仮定に基づいている。

特徴（“Something you are” の別名でも知られる）による認証。この方法は、網膜パターンや指紋などのユーザ特有の 1 つ以上の特徴を、バイオメトリックスによる認識を利用することに基づいている。この方法は、“ 特定の人の特徴は、その人を唯一特定することができる ” という仮定に基づいている。

本文書では電子認証方式に関して、以下の事項が示されている。

> In electronic authentication, the claimant authenticates to a system or application over a network. Therefore, a token used for electronic authentication shall include some secret information and it is important to provide security for the token. In fact, the three methods (or “factors”) mentioned above often influence the security provided by tokens. Tokens that incorporate all three factors are stronger than tokens that only incorporate one or two of the factors.

電子認証では、要求者はネットワーク上でシステムやアプリケーションを認証する。従って、電子認証のために使用されるトークンは、何かしらの秘密情報を含んでいるべきであり、トークンによってセキュリティを供給することは重要である。実際、上記で言及されている 3 つの方法（もしくは要素は）は、しばしばトークンによって提供されたセキュリティに影響を及ぼす。3 つの要素全てを取り入れたトークンは、1 つか 2 つの要素しか取り入れていないトークンより強固である。

4.9.7.1. トークンタイプ

本文書ではトークンタイプに関して、以下の事項が示されている。

> In this sense, four types of tokens for authentication are presented below (Table 7). Each type of token incorporates one or more of the methods (something you know, something you have, and something you are.)
>
> **Note: Only electronic tokens are considered here.**

＜引用部の訳文＞

この意味で、認証のための 4 つのタイプのトークンは、下記の表 4-11 で示される。それぞれのタイプのトークンは、（知っていること、持っていること、本人の性質）方法の 1 つかそれ以上を取り入れている。

注意：ここでは電子的なトークンのみを扱っている。

表 4-11　トークンタイプ

トークンタイプ	説明
パスワードまたは PIN トークン	クライアントが自分自身のアイデンティティを認証するために暗記して、使用する秘密の文字列
ワンタイムパスワードデバイストークン	認証のために“ one time ”パスワードを生成するパーソナルハードウェアデバイスである。デバイスは、ある種の不可欠な entry pad や不可欠な（指紋などの）バイオメトリック読み取り機、（USB ポートのような）直接的なインターフェースを持ち合わせているかどうか分からない。 ハードウェアデバイスに保管された対称鍵とワンタイムパスワードを生成するために使われたノンスを組み合わせる為、パスワードは、ブロック暗号かハッシュアルゴリズムを用いて生成されるべきである。ノンスは、日時やデバイスで生成されたカウンター、（デバイスに入力機能があれば）検証者から送られてきたチャレンジでもよい。 ワンタイムパスワードは、通常はデバイスに表示されパスワードとして検証者に手動入力する（デバイスからコンピュータへ直接の電子入力も許可されている）。
ソフト暗号トークン	暗号鍵は、通常はディスクか何か他のメディアに保存されている。認証は、鍵の所有証明と管理によって成される。ソフトトークンは、ユーザしか知らないパスワードから得られた鍵を用いて暗号化されるので、パスワードに関する知識はトークンを使える状態にするために必要である。それぞれの認証はパスワード入力を必要とするべきであり、認証鍵の暗号化されていない複製は認証後に消去されるべきである。
ハード暗号トークン	保護された暗号鍵を含んでいるスマートカード。認証は、そのデバイスの所有を鍵管理の証明によって成される。ハードトークンは、 ・ パスワード入力か認証鍵を有効にするためのバイオメトリックを要求し、 ・ 認証鍵をエクスポートすることができない でなければならない。

（1） レベルによるトークンタイプ

表 4-12　レベルによるトークンタイプ

トークンタイプ	保証レベル			
	1	2	3	4
ハード暗号トークン	×	×	×	×
ソフト暗号トークン	×	×	×	
ワンタイムパスワード デバイストークン	×	×		
パスワードまたは PIN トークン	×			

4.9.7.2. 遠隔認証メカニズム

本文書では遠隔認証メカニズムに関して、以下の事項が示されている。

> **Remote authentication mechanisms are basically the credentials, tokens and authentication protocols used to establish that a claimant is in fact the subscriber he or she claims to be.**

＜引用部の訳文＞

遠隔認証メカニズムは、基本的には、証明書やトークン、要求者が実際に自分自身だと主張する加入者であることを確認する認証プロトコルである。

（1） Authentication Protocols Threat Model

本文書では、Authentication Protocols Threat Model に関して、以下の事項が示されている。

> RAs, CSPs, verifiers and relying parties are ordinarily trustworthy (in the sense of correctly implemented and not deliberately malicious). However, claimants or their systems may not be trustworthy (or else we could simply trust their identity assertions).

＜引用部の訳文＞

通常、RAs、CSPｓ、検証、および relaying parties は信頼できる（正しく実行されていて故意に悪意がないことの意味において)。しかしながら、主張者やそのシステムは信頼できないかもしれない（我々は、identity の主張についてのみ信頼できる)。

（2） レベルによる認証プロトコル

表 4-13 レベルによる認証プロトコルタイプ

許可されたプロトコルタイプ	保証レベル			
	1	2	3	4
秘密鍵 PoP	×	×	×	×
共通鍵 PoP	×	×	×	×
ワンタイム（又は強力な）パスワード PoP	×	×	×	
Tunnelled password PoP	×	×		
Challenge-reply password PoP	×			

PoP: Proof of Possession

（3） レベルによる保護要件

表 4-14　レベルによる保護要件

保護	認証保証レベル			
	1	2	3	4
盗聴者		×	×	×
リプレイ	×	×	×	×
オンライン推測	×	×	×	×
検証者に成りすまし			×	×
中間者攻撃			×	×
セッションハイジャック			×	×

4.9.7.3. Assertion Mechanisms

本文書では、Assertion Mechanisms に関して、以下の事項が示されている。

Assertion mechanisms are used to communicate the results of a remote authentication to other parties.

Relying parties may accept assertions that are:

- Digitally signed by a trusted identity (e.g. the verifier); or
- Obtained directly from a trusted entity using an authentication protocol of the corresponding level or above.

Assertions shall expire after a certain period, defined by level (see …). They should not be accepted afterwards.

＜引用部の訳文＞

Assertion mechanisms は、遠隔認証の結果を他の関係者へ伝えるために使用される。

当てにされた関係者は、次の場合には主張を受け入れるだろう。

- （例えば検証者など）信頼された identity によって電子的に署名された

・ 対応するレベルかそれ以上のレベルの認証プロトコルを通じて信頼されたエンティティから直接受け取る。

レベルによって定められたある期間の後に、Assertions は期限が切れるものとするべきである。その後は、その Assertions を受け入れるべきではない。

表 4-15　レベルによる有効期限

有効期限	保証レベル			
	1	2	3	4
24 時間	×			
12 時間	×	×		
2 時間	×	×	×	
直ちに	×	×	×	×

4.9.8. Common Practice Statement

表 4-16　レベル 1　ポリシー

情報分類	sectoral network 上だけでは分類されていない情報の交換は適用できる
登録フェーズ	
・ identity proofing の手続き ・ ユーザ登録の詳細 ・ トークンと信用証明書の交付	**レベル 1 の登録** 1．定義 実世界での identity の流出によって起こり得る損害が「無視できる」または「低い」影響の sectoral application transaction に対しては、レベル 1 の登録は適当である。 この登録レベルは（ウェブメール、オンライン、オークションなど）多くのインターネットアプリケーションで使用頻度が高い。 2．要件 identity 証明や登録事実の記録を保持するといった要件はない。主張者の identity 断言は受け入れられる。e-メールアドレスだけは一義的で検証されなければならない。
登録データの保存期間	**なし**
トークンタイプ	多くの場合、パスワードや PIN トークン しかしリスクアセスメントによれば、以下のものも可能である。 ・ ワンタイムパスワード・デバイス・トークン ・ ソフト暗号トークン ・ ハード暗号トークン

電子認証フェーズ	
PoP (Proof of Possession)のための認証プロトコル	大抵の場合、Challenge-reply password PoP しかしリスクアセスメントによれば、以下のものも可能である。 ・ Tunelled password PoP ・ ワンタイム（又は強力な）パスワード PoP ・ 共通鍵 PoP ・ 秘密鍵 PoP
保護実行のために Sectoral Application owner に対する要件	・ リプレイ ・ オンライン推測

表 4-17　レベル 2　ポリシー

情報分類	sectoral network 上だけでは分類されていない情報の交換は適用できる
登録フェーズ	
・ identity proofing の手続き ・ ユーザ登録の詳細 ・ トークンと信用証明書の交付	**レベル 2 の登録** 1．定義 実世界での identity の流出によって起こり得る損害が「中間」影響の sectoral application transaction に対しては、レベル 2 の登録は適当である。 レベル 2 登録のほとんどの場合、オンラインですぐに成し遂げることができる。 ２．要件 述べられている登録ポリシーによると、加入者の identity 情報が検証、確認されることを RA が確実にするべきである。identity 情報は、加入者を一意的に特定することができる最低限で完全な正式氏名、他をサポートしている情報を含むべきである。 登録事実の記録は、CSP かその代表によって保存されるべきである。Level 2 証明書のための登録データのために提案された最小限の保持期間は、証明書の満期または取り消し（より遅いものはどれでも）を越えた 5 年である。 もし、RA と CSP が分離していてネットワーク上で交信するのであれば、RA と CSP 間の登録取引全体を含む交信は、承認された方法での暗号的保護と少なくともレベル 2 保証での要件を満たしている認証プロトコルであるべきである。 3．手順 少なくとも、登録手続は次を行う。 (1)　加入者の主張された identity が、機構との認証された進行中のビジネス関係の人であることを確認する。そのために、RA は実世界 identity 証明（例えば、

	国家の ID カード、運転免許証、パスポートなど）の署名済みコピーを要求しなければならない。 (2) 検証された identity と下記の何れかで確認されたものを紐ける形で、証明書やトークンを発行や更新する。 (a)加入者の記録のポータルアドレス（例えば、認証者が記録されているアドレスへ手紙を送る） (b)加入者の電話番号（例えば、記録されている加入者電話番号へ掛ける又は掛けさせるを要求する） (c)記録されたアドレスへ電子メールか他の電子的ビジネスコミュニケーション（例えば、認証者から加入者の電子メールアドレスへ送る）
登録データの保存期間	証明書の満期または取り消し（より遅いものはどれでも）を越えた 5 年。
トークンタイプ	望ましくは、ワンタイムパスワード・デバイス・トークン しかしリスクアセスメントによれば、以下のものも可能である。 ・ ソフト暗号トークン ・ ハード暗号トークン
電子認証フェーズ	
PoP (Proof of Possession)のための認証プロトコル	たいてい、Tunnelled 又はワンタイムパスワード PoP しかしリスクアセスメントによれば、以下のものも可能である。 ・ 共通鍵 PoP ・ 秘密鍵 PoP
保護実行のために Sectoral Application owner に対する要件	・ 盗聴者 ・ リプレイ ・ オンライン推測

表 4-18　レベル 3　ポリシー

情報分類	sectoral network 上での分類されていない情報と EU-RESTRICTED レベルの分類された情報の交換へ適用できる
登録フェーズ	
・ identity proofing の手続き ・ ユーザ登録の詳細 ・ トークンと信用証明書の交付	**レベル 3 の登録** 1. 定義 実世界での identity の流出によって起こり得る損害が「高い」影響の sectoral application transaction に対しては、レベル 3 の登録は適当である。 レベル 3 での identity proofing は、RA が加入者の identity の実質証拠を検証することを必要とする。しかし、加入者が登録するために自分で現れることを必ずしも義務づけるというわけではない。一般的に、identity を検証するために用いられた証明書や記録の少なくとも幾つかの実態が、現在でも有効だと確認するということを、レベル 3 での identity proofing は必要とする。それには物理的アドレスや記録にある電話番号の確認も必要とする。 2. 要件 加入者の identity 情報が述べられている登録ポリシーに従って検証・チェックされていることを RA は確認すべきである。identity 情報は少なくとも次のものを含む。 ・ 完全な正式氏名 ・ 誕生の日付と場所（検証されないかもしれないが、集められるべきである） ・ 記録の現在の場所 ・ パスポート番号や社会保険番号、運転免許証番号など、登録プロセスでチェックされた全ての文書の identity 番号 実世界 identity の証拠（例えば、国民 ID カード、運転免許証、パスポートなど）の提示によって identity は検査され

	なければならない。加入者は、組織における自分の活動に関する証拠（例えば、加盟国政府の手紙など）のうち 1 つは提示もしなければならない。 登録の事実に関する記録は、CSP かその代表によって保存されるべきである。Level 3 証明書のための登録データのために提案された最小限の保持期間は、証明書の満期または取り消し（より遅いものはどれでも）を越えた 7 年である。 もし RA と CSP が分離していてネットワーク上で交信するのであれば、レベル 3 以上で要求されるものに合致する認証プロトコルを用いて暗号的に認証し、暗号化では承認された暗号方法を用いて、登録取引全体を行うべきである。 3. 手順 少なくとも、登録手続は次を行う。 (1) 加入者の主張された identity が、現在の個人で、証明書（例えば、加盟国政府の手紙など）の提示によって組織との関係が優良な状態であることを確認する。 (2) 検証された identity と下記のどちらかで確認されたものを紐ける形で、証明書やトークンを発行や更新する。 (a)加入者の記録のポータルアドレス（例えば、認証者が記録されているアドレスへ手紙を送る） (b)加入者の電話番号（例えば、記録されている加入者電話番号へ掛ける又は掛けさせるを要求する）
登録データの保存期間	証明書の満期または取り消し（より遅いものはどれでも）を越えた 7 年。
トークンタイプ	ソフト暗号トークン しかしリスクアセスメントによれば、次のものも可能である。 ・ ハード暗号トークン

電子認証フェーズ	
PoP (Proof of Possession)のための認証プロトコル	望ましくは、ワンタイムパスワード PoP しかしリスクアセスメントによれば、以下のものも可能である。 ・ 共通鍵 PoP ・ 秘密鍵 PoP
保護実行のために Sectoral Application owner に対する要件	・ 盗聴者 ・ リプレイ ・ オンライン推測 ・ 検証者に成りすまし ・ 中間者攻撃 ・ セッションハイジャック

表 4-19　レベル 4　ポリシー

情報分類	sectoral network 上での分類されていない情報と EU-RESTRICTED レベルの分類された情報の交換へ適用できる
登録フェーズ	
・ identity proofing の手続き ・ ユーザ登録の詳細 ・ トークンと信用証明書の交付	**レベル 4 の登録** 1. 定義 実世界での identity の流出によって起こり得る損害が「非常に高い」影響の sectoral application transaction に対しては、レベル 4 の登録は適当である。 加入者の写真を含む identity 文書と、加入者から撮影された写真や指紋などのバイオメトリックと記録に保存されたもので、対面の identity proofing を必要とするという点で、レベル 4 での identity proofing は異なっている。 トークンの配送も、RA において実際に現れて関連付けられるべきである。このレベルでは、加入者がアプリケーションへ手書きでサインをし、これは違反すれば偽証罪が適用される。 2. 要件 加入者の identity 情報が述べられている登録ポリシーに従って検証・チェックされていることを RA は確認すべきである。 最初のステップとして、加盟国政府の公務員へ信用証明書を発行するために、組織管理から認証された要請が、RA／CSP によって必要とされる。さらに、RA／CSP は加入者によって提供されたバイオメトリックを用いて検証することを必要とする。 取られた方法と加入者の identity を検証するために試験されたあらゆるドキュメントのコピーを含む登録事実の記録は、CSP かその代表によって保守されるべきである。 Level 4 証明書のための登録データのための最小限の保持期間は、証明書の満期または取り消し（より遅いものはどれ

	でも）を越えた 10 年である。 もし RA と CSP が分離していてネットワーク上で交信するのであれば、レベル 4 で要求されるものに合致する認証プロトコルを用いて暗号的に認証し、暗号化では承認された暗号方法を用いて、登録取引全体を行うべきである。 3. 手順 少なくとも、登録手続は次を行う。 （1)　加入者に対するクレデンシャルの発行要求が、組織管理の上で提出されたことを検証する。 （2)　公式の組織人事記録を利用することにより加入者の職業を検証する。 （3)　登録同局の前に、次のプロセスに基づいて対面の検査により加入者の identity を証明する。 （a)identity 証明として､加入者は政府によって発行された識別（例えば、現在のパスポートや運転免許証）または組織の発行した写真つき ID （b)RA は､提示された信用証明書に加入者に結びつくバイオメトリックデータがないか検査する。 （c) 上記(3)(a)で提示された信用証明書が、現在でも通用し合法的だということを RA によって検証されるべきである（例えば、組織発行 ID は有効かどうかが検証される)。通常これは、信用証明書を発行した組織に保存してある人事記録に問い合わせを行うことにより成し遂げられる。 （4)　加入者のバイオメトリック（例えば､写真や指紋）を記録し保存する。 その上、RA は各々の信用証明書を発行するために辿ったプロセスを記録すべきである。プロセス文書と認証要求は次のものを含むべきである。 ・　識別をしている人の identity

	・ CSP によって要求され identity 検証された加入者が署名した宣言書 ・ 加入者の ID や ID の複製による一意的な identity ナンバー ・ 加入者のバイオメトリック ・ 検証の日付と時間 ・ 加入者の手書き署名によって署名され、identity 認証を実行する人の面前で行なわれる identity 宣言書 ・ 受領者と、加入者が手書きで署名をし、identity 認証を実行する人の面前で行なわれたトークン利用者との間での義務に関する協定書
登録データの保存期間	証明書の満期または取り消し（より遅いものはどれでも）を越えた 10 年。
トークンタイプ	ハード暗号トークン
電子認証フェーズ	
PoP (Proof of Possession)のための認証プロトコル	次の何れか ・ 共通鍵 PoP ・ 秘密鍵 PoP
保護実行のために Sectoral Application owner に対する要件	・ 盗聴者 ・ リプレイ ・ オンライン推測 ・ 検証者に成りすまし ・ 中間者攻撃 ・ セッションハイジャック

4.9.9. 利用者

IDA 認証ポリシーの範囲は、電子証明書を用いることにより、IDA Sectoral Networks における関係者間の遠隔認証に限定されるものとする。

4.9.10. 利用方法の想定

Sectoral Project Authentication Policy を作成する、またはこれを利用する際に本ドキュメントの参考を利用する。

4.9.11. 運用方法

特に記されていない。

4.9.12. 特徴

本ドキュメントは、フレームワーク規約 ENTR/01/67-CONSEC の下で準備されたものである。また、本ドキュメントは 2003 年に発表された米国の“ E-Authentication Guidance for Federal Agencies ”を参考に作成されたもので、一部文言などが同一である。

フレームワークの登録段階において、バイオメトリックを使用する記述があるので人の認証のみを扱っている。

4.10. TRUST FRAMEWORK（米国）

4.10.1. 目的

本文書の目的として、以下の事項が示されている。

> Signatories to these business rules agree that these rules govern the use and validation of Electronic Authentication Partnership (EAP) certified credentials, the certification of such credentials and the accreditation of those who assess issuers of such credentials. These business rules are intended to cover use of credentials for purposes of authentication and not specifically for the application of a legal signature, which may be subject to other rules depending upon the parties and transactions involved.

＜引用部の訳文＞

本ビジネス・ルールにおける署名者は、Electronic Authentication Partnership（EAP）証明書付きクレデンシャルの使用とバリデーション（有効性検証)、当該クレデンシャルの証明、及び当該クレデンシャルの発行者のアセスメントを担当する機関の認定に関して、当該ルールに準拠することに同意する。本ビジネス・ルールは、認証を目的とするクレデンシャルの利用を対象としており、当事者および関係取引ににより別のルールが適用され得る特定の法的署名の適用について意図しているわけではない。

4.10.2. 利用者

EAP システムに参加する全ての人々を対象とする。

4.10.3. 利用方法の想定

本文書の利用方法の想定として、以下の事項が示されている。CSP（クレデンシャル・サービス・プロバイダー）が、EAP 認定アセスメント機関によるアセスメントを無事完了することができるために利用する。アセスメントについては、下記の通りである。

The EAP Service Assessment Criteria (SAC) are prepared and maintained by the Electronic Authentication Partnership (EAP) as part of its Trust Framework. These criteria set out the requirements for services and their providers at all assurance levels within the Framework. These criteria focus on the specific requirements for EAP assessment at each assurance level (AL) for the following:

- The general business and organizational conformity of services and their providers,
- The functional conformity of identity proofing services, and
- The functional conformity of credential management services and their providers.

These criteria (at the applicable level) must be complied with by all services that are assessed for certification under the EAP Trust Framework.

＜引用部の訳文＞

EAP Service Assessment Criteria(SAC)は Trust Framework の一部として Electronic Authentication Partnership(EAP)によって作成され、維持される。この基準は、フレームワーク内のすべての保証レベルについて、サービスとプロバイダの要件を規定する。そして、各保証レベル（AL）における EAP アセスメントとして、下記の具体的要件を焦点としている。

- サービス及びサービスプロバイダーのビジネス全般と組織の適合性
- identity proofing services の機能的な適合性
- クレデンシャル管理サービスとそのプロバイダの機能的な適合性

EAP Trust Framework の下で証明用に評価されるすべてのサービスが（該当するレベルで）この基準に従っていなければならない。

4.10.4. 運用方法

本文書の運用方法として、以下の事項が示されている。

Promulgation and Amendment of Business Rules and Other Documents

The EAP shall formalize and may periodically amend these business rules. The EAP shall also formalize and may periodically amend a set of documents governing the accreditation of assessors of EAP CSPs and the certification of EAP credentials. The EAP reserves the right, at its discretion, to formalize and periodically amend such other materials, including policies or guidelines, participation agreements, handbooks or other documents relevant to the EAP. Notice of all amendments shall be given by EAP by electronic mail to the contact person(s) identified by each signatory for such purpose and by posting to the EAP web site. All amendments shall be effective as of the date specified in such notice. If a signatory objects in writing to an amendment within 30 days after notice of the amendment is given by EAP, such objection shall be deemed to be a notice of termina-tion of such signatory's participation in EAP under Section 1.2.

Relying Party, CSP and Assessor Approval

The EAP is responsible for approving participation in the EAP System by relying parties, CSPs and assessors. The EAP shall formalize and may periodically amend requirements for certification of credentials issued by a CSP and the accreditation of assessors of CSPs. The EAP shall formalize, maintain and update as needed an EAP-approved CSP list (EAP CSP list) of certified signatory CSPs. This EAP CSP list shall include, at a minimum, the names of each CSP, the level of assurance for which credentials issued by the CSP have been certified and a URL and other contact information for the CSP.

＜引用部の訳文＞

ビジネス・ルールその他の文書の正式発行と修正

EAP は、このビジネス・ルールを公式化するものとし、これを定期的に修正することができる。また、EAP は、EAP CSP のアセスメント機関の認定及び EAP クレデンシャルの証明に関する一連の文書を公式化するものとし、これを定期的に修正することができる。EAP は、EAP に関連する方針、ガイドライン、参加協定、ハンドブックまたは他の文書を、独自の判断で公式化し定期的に修正する権利を保有する。あ

らゆる修正に関する通知は EAP により、その目的で署名された連絡先への電子メール、ならびに EAP の Web サイトへの掲載により行われる。すべての修正は、当該通知に指定する日付をもって効力を発生する。EAP により修正の通知があった後 30 日以内に署名者がその修正に対して書面により異議を申し立てる場合、当該異議申し立ては本フレームワークのセクション 1.2 に基づき EAP への当該署名者の参加終了の通知であるとみなされる。

信頼当事者、CSP 及びアセスメント機関の承認

EAP は、信頼当事者、CSP 及びアセスメント機関が EPA システムへ参加を承認することに責任を負う。EAP は、CSP の発行するクレデンシャルの証明及び CSP のアセスメント機関認定の要件を公式化するものとし、これを定期的に修正することができる。EAP は、証明済みの署名者 CSP を記載する EAP 承認済み CSP リスト（EAP CSP リスト）を公式化し、維持し、必要に応じて更新する。この EAP CSP リストには、各 CSP の名称、CSP の発行するクレデンシャルが証明された際の保証レベル、及び CSP の URL その他の連絡先情報を最低限記載するものとする。

4.10.5. 特徴

各信頼当事者と CSP は、EAP システムへの参加の前提条件として、このビジネス・ルールによって制約されていることに同意しなければならない。

4.11. EVIDENCE OF IDENTITY FRAMEWORK（ニュージーランド）

本文書には、以下の事項が示されている。

This EOI Framework is a good practice tool for establishing, to a high level of confidence, the identity of individuals who wish to carry out transactions carrying a significant level of identity-related risk with government agencies – such as exchanging sensitive personal information or conducting transactions with financial implications.

It has been developed in response to a number of issues:

- Government agencies currently take different approaches to EOI, which can cause confusion for the individuals concerned, who may be asked to supply different EOI for similar uses.
- The identified need for a robust, consistent and cross-government approach to EOI that will help protect individuals against the theft or fraudulent use of their identities, and prevent the personal and public loss of money through identity fraud.
- The requirement for a robust framework has become increasingly important to the E-Government Unit's work on online identity authentication.
- Identity fraud (whether through establishing false identities or stealing legitimate ones) is increasing and has significant financial and social costs to individuals, businesses and the public.
- Identity fraud is increasingly an international problem, with links between identity fraud and other criminal activity.

＜引用部の訳文＞

本認証（EOI: Evidence Of Identity：以下 EOI と記す）フレームワークは、政府機関と identity 関連のリスク（identity-related risk）の有意水準で取引（例えば、機微な個人情報を交換や、経済的な取引。）を行いたいと思っている個人の identity を高レベルの信頼で確立するためベスト・プラクティス・ツールである。

これは、次のような多くの問題に応じて開発されたものである。

政府機関は現在、関係する個人に対して混乱を引き起こしたり、同様の用途に対して異なる EOI の提供が要求されたりする様々なアプローチの EOI を行なっている。

盗難や identity の不正使用から個人を守る手助けをし、identity 詐欺による個人や公共の金銭的損失を防ぐような、強固で一貫性のある政府横断的な EOI へのアプロー

チが認証には必要である。

強固なフレームワークの要件は、オンライン identity 認証に対する電子政府ユニットの仕事に対してますます重要になってきている。

（誤った identity の確立や合法的なものを盗むことにかかわらず）identity 詐欺は増加し、個人やビジネス、公共へ著しい財政的・社会的損失をもたらしている。

identity 詐欺は、identity 詐欺と他の犯罪行為との関連で、国際問題へと発展している。

The EOI Framework is a good practice tool for establishing, to a high level of confidence, the identity of individuals who wish to carry out transactions that have a significant level of risk with government agencies.

It is important to note that agencies should apply the Framework alongside, and not instead of, other initiatives designed to mitigate the risks associated with identity fraud.

EOI フレームワークは、政府機関と identity 関連のリスク（identity-related risk）の有意水準で取引を行いたいと思っている個人の identity を高レベルの信頼で確立するためベスト・プラクティス・ツールである。

政府機関は、identity 詐欺のリスクを低減されるために設計された他のイニシアチブの替りではなく、それらと並行して本フレームワークを適用すべきであると留意することは重要である。

次の図 4−4 は、EOI フレームワークの一部をなすものである。これは、各コンポーネントについて概説しているもので、それぞれの Objective は高レベルの認証で個人の identity を認めるために必要である。

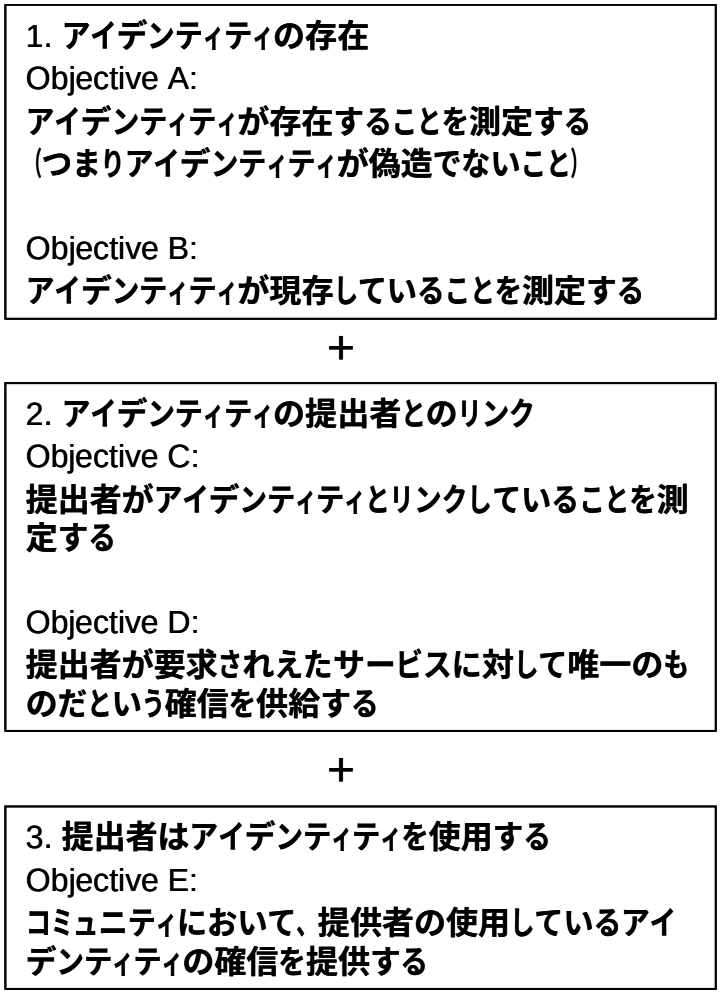


図 4−4　EOI フレームワークの認証コンポーネント

4.11.1. リスク評価と信用レベル

4.11.1.1. リスク評価

全ての取引が EOI での同一のレベルを要求するわけではなく、いくつかは全く要求しない。

取引でのリスクを次の 4 つのカテゴリーに分けることができる（本フレームワークでは最後の 2 つにだけ適用される）

- カテゴリー 0：人が特定されるのを必要としない匿名のサービス/取引
- カテゴリー 1：人が特定されるのを必要としない偽名のサービス/取引、しかし連絡先は必要とする
- カテゴリー 2：人が明確に特定されるのを必要とする認証されたサービス/取引
- カテゴリー 3:人が明確に特定されるのを必要とする検証されたサービス/取引、さらに認証データも検証される

4.11.1.2. 信用レベルの選択

一般的に、

- 信用レベルＡのプロセスは、カテゴリー 2 の取引に適用される
- 信用レベルＢのプロセスは、カテゴリー 3 の取引に適用される

取引が EOI を必要とするかどうか（つまり、その取引がカテゴリー 2 か 3 に一致しているか）を決定することは比較的簡単である。

しかしながら、それに関係する信用レベルを区別することは、より難しい。ある取引がカテゴリー 3（高リスク）取引かどうかを決定する際、政府機関は例えば次のような質問をする。

- 金融リスクの重大なレベルに関わるか？
- 個人の（例えば健康情報など）機密な情報の流出に関わるか？
- 発行している政府機関に取引リスクが含まれるか？（つまり、他の政府機関が発行したドキュメントでの結果を他の取引の identity 認証としての利用／許可する取引に対して、これは適用される）
- 取引は、個人の健康と安全に対してリスクを及ぼすか？（例えば、保護された個人情報の公開が、個人を危険にさらすことに繋がる取引か？）

4.11.2. identity プロセスの認証

本文書では identity プロセスの認証に関して、以下の事項が示されている。

The tables on the following pages provide guidance on the types of EOI that can be used to meet Confidence Levels A and B.

They cover:

- the objective: the desired results of each component of the EOI process;
- the requirement: the evidence required to achieve the objective; and
- the document or process: the physical evidence or procedures that can be used as evidence of the individual's identity according to the relevant Confidence Level. Appendix 3 provides further information on each of the EOI documents and data sources.

Note that any documents specified in the following pages are original or official documents, not photocopies (verified or otherwise).

＜引用部の訳文＞
以下のページ（表 4-20）は、信用レベル A，B に合致するために使用される EOI のタイプについて提供している。
それらは、次のことが網羅されている。

- Objective：EOI プロセスのそれぞれのコンポーネントでの望ましい結果
- 要件：Objective を成し遂げるための認証用件
- ドキュメントやプロセス：適切な信用レベルに関する個人 identity の認証として使用される物理的認証や手続き。Appendix 3 でそれぞれの EOI ドキュメントやデータソースに関する更なる情報を提供している。

以下のページで指定されているどんなドキュメントも（照合したものやその他のものの）コピーではなく、オリジナルで公式なドキュメントであることに注意をする。

表 4-20　Objective A

コンポーネント 1：identity の存在		
Objective A：アイデンティティが存在することを測定する		
要件	ドキュメントやプロセス	
	信用レベル　A	信用レベル　B
その人が生まれていることの認証 **要件：** ・ （出生から現在までの）オリジナルな名前を認証 ・ 誕生日を認証 ・ 出生地を認証 ・ 出身国の認証	**本 Objective を満たすためのオプション：** 完全な出生記録の提示 **and/or** パスポートの提示 **and/or** 銃器取扱いライセンスの提示 **and/or** ニュージーランド市民証明書の提示 **and/or** identity 証明書の提示 **and/or** 難民旅券文書の提示	**本 Objective を満たすためのオプション：** **Either** 個人から同意を得て、主要なデータの管理人へ検証を要求する **or** 完全な出生記録の提示とドキュメントが本物だと検証する **and/or** パスポートの提示とドキュメントが本物だと検証する **and/or** 銃器取扱いライセンスの提示とドキュメントが本物だと検証する **and/or** ニュージーランド市民証明書の提示とドキュメントが本物だと検証する

表 4-21　Objective B

コンポーネント 1：identity の存在		
Objective B：アイデンティティが現存していることを測定する		
要件	ドキュメントやプロセス	
	信用レベル　A	信用レベル　B
その人が死亡していないことを認証	**Objective 2C を満たしている限り、この objective においてプロセスは要求されない**	**本 Objective を満たすためのオプション：** **Either** 信頼された保証人に、主張された identity（つまりサービスに申し込んでいる人）が持ち主の identity かを検証させる **or** 以下の何れかを用いて、現れている人が申請者であることを要求 ・ 信頼された保証人によって写真の検証 ・ パスポート ・ identity の証明書 ・ 難民旅券文書 **or** ニュージーランドの死亡登録を用いて主張された identity が死亡記録に入っていないことを検証する。（海外で死亡した人については、死亡記録の登録は必要はないことを注意すること。）

表 4-22　Objective C

コンポーネント 2：identity の提出者とのリンク		
Objective C：提出者が idnetity とリンクしていることを測定する		
要件	ドキュメントやプロセス	
	信用レベル　A	信用レベル　B
物理的に提出した人が主張された identity とリンクしているかを認証	**本 Objective を満たすためのオプション：** **Either** 信頼された保証人によって検証された人の写真と、申請者 **or** 信頼された保証人によって検証された申請者の写真の提示 **or** パスポートの提示と、サービスへの申請者とパスポートの人が同じであることを保証人が検証（両方） **or** 銃器取扱いライセンスの提示と、サービスへの申請者とライセンスの人が同じであることを保証人が検証（両方） **or** 運転免許証の提示と、サービスへの申請者と運転免許証の人が同じであることを保証人が検証（両方）	**本 Objective を満たすためのオプション：** 認証レベル A の要件と次のプロセス **and** 検証のために申請者と保証人の両方によって提供された詳細を、信頼された保証人に連絡する

表 4-23　Objective D

コンポーネント 2：identity の提出者とのリンク		
Objective D：提出者が要求されたサービスに対して唯一の者だという確信を提供する		
要件	ドキュメントやプロセス	
	信用レベル　A	信用レベル　B
他の人が、サービスへのアクセスのために主張された identity を持っていないことを認証する	**サービス提供機関のデータベースをチェックする**	**サービス提供機関のデータベースをチェックする**

表 4-24　Objective E

コンポーネント 3：提出者は identity を使用する		
Objective E：コミュニティにおいて、提出者の使用している identity の確信を提供する		
要件	ドキュメントやプロセス	
	信用レベル　A	信用レベル　B
コミュニティでの identity の利用を認証する **and** 現在か以前に使用された他の名前が、オリジナルの名前とリンクするかを認証する	もし可能であれば、名前のどのような変更についても公的な認証を提示する（例えば、結婚証明や法的な証明） **and** 次のうち少なくとも 1 つのコミュニティ利用認証の提示 ・ 運転免許証 ・ コミュニティサービスカード ・ 名前・住所・ＩＲＤナンバーがある、ＩＲＤ statement（ＩＲＤ：Inland Revenue Department） ・ 選挙人名簿登録の詳細 ・ 名前と住所の詳細を含む有効的な明細書（例えば、電話や電気） ・ 名前と住所の詳細を含む経済的な明細書 ・ 銀行カード ・ 学生ＩＤや社員ＩＤカード	もし可能であれば、名前のどのような変更についても公的な認証を提示する（例えば、結婚証明や法的な証明） **and** コミュニティでの identity の個人利用について信頼された保証人によって検証ｓれる **and** 次のうち少なくとも 2 つのコミュニティ利用認証の提示 ・ 運転免許証 ・ コミュニティサービスカード ・ 名前・住所・ＩＲＤナンバーがある、ＩＲＤ statement（ＩＲＤ：Inland Revenue Department） ・ 選挙人名簿登録の詳細 ・ 名前と住所の詳細を含む有効的な明細書（例えば、電話や電気）

	ード ・ Steps to Freedom form	・ 名前と住所の詳細を含む明細書 ・ 銀行カード ・ 学生ＩＤや社員ＩＤカード ・ Steps to Freedom form

4.11.3. 目的

本文書の目的として、以下の事項が示されている。

The Framework has been developed for New Zealand's government sector, primarily for agencies to apply when carrying out high-risk transactions with members of the public. It may also be applied to recruitment within agencies where the position being recruited to is of high-risk. Likewise, the Framework could also be helpful to organisations outside the government sector in determining the accuracy, and benefits or limitations of, different government-issued documents (as described in Appendix 3).

＜引用部の訳文＞

本フレームワークは、ニュージーランドの政府部門のために作成されたものであり、主として政府機関が公共のメンバーと高リスクの取引を行う際に適用されるものである。また、新規雇用が高リスクの位置をしめる政府機関での雇用にも適用されるかもしれない。同様にまた、政府部門外の組織が、異なる政府が発行した（Appendix 3 で述べる）文書における利益や制限の正確さを判断する際にも、フレームワークは役立つだろう。

4.11.4. 利用者

本文書の利用者として、以下の事項が示されている。利用対象者は、大多数の人々である。未成年者や認証サービス等へアクセスできない人は除いている。

The vast majority of individuals will be able to meet the EOI requirements, outlined in this Framework.

Exceptions include, for example, minors or people who cannot access the required evidence from their country of origin or where the emergency nature of a particular service makes it inappropriate to require individuals to meet the EOI requirements.

In cases like these, the Framework objectives should still be pursued where possible, but alternative EOI sources will be required. Agencies will need to apply discretion, just as they do currently.

＜引用部の訳文＞

大多数の個人は本フレームワークで概説された EOI 要件を満たしているだろう。

例外は、例えば未成年者や、要求されている証拠のうち出身国から出ているものを得られない人々、または特定のサービスの突発的に事情によって、個人への EOI 要件の適用が不適切な場合である。

これらのような場合でも本フレームワークの目標は可能な場面では追求されるべきだが、代替の EOI の情報源が必要とされるだろう。政府機関は、現在実行しているのと同様の裁量が必要であるだろう。

4.11.5. 利用方法の想定

次の図 4−5 は EOI フレームワークの利用工程である。特定のトランザクションに関して政府機関が本フレームワークを必要としているかどうかを視覚的に案内しているもので、本フレームワークをどのように使用すべきかが記されている。

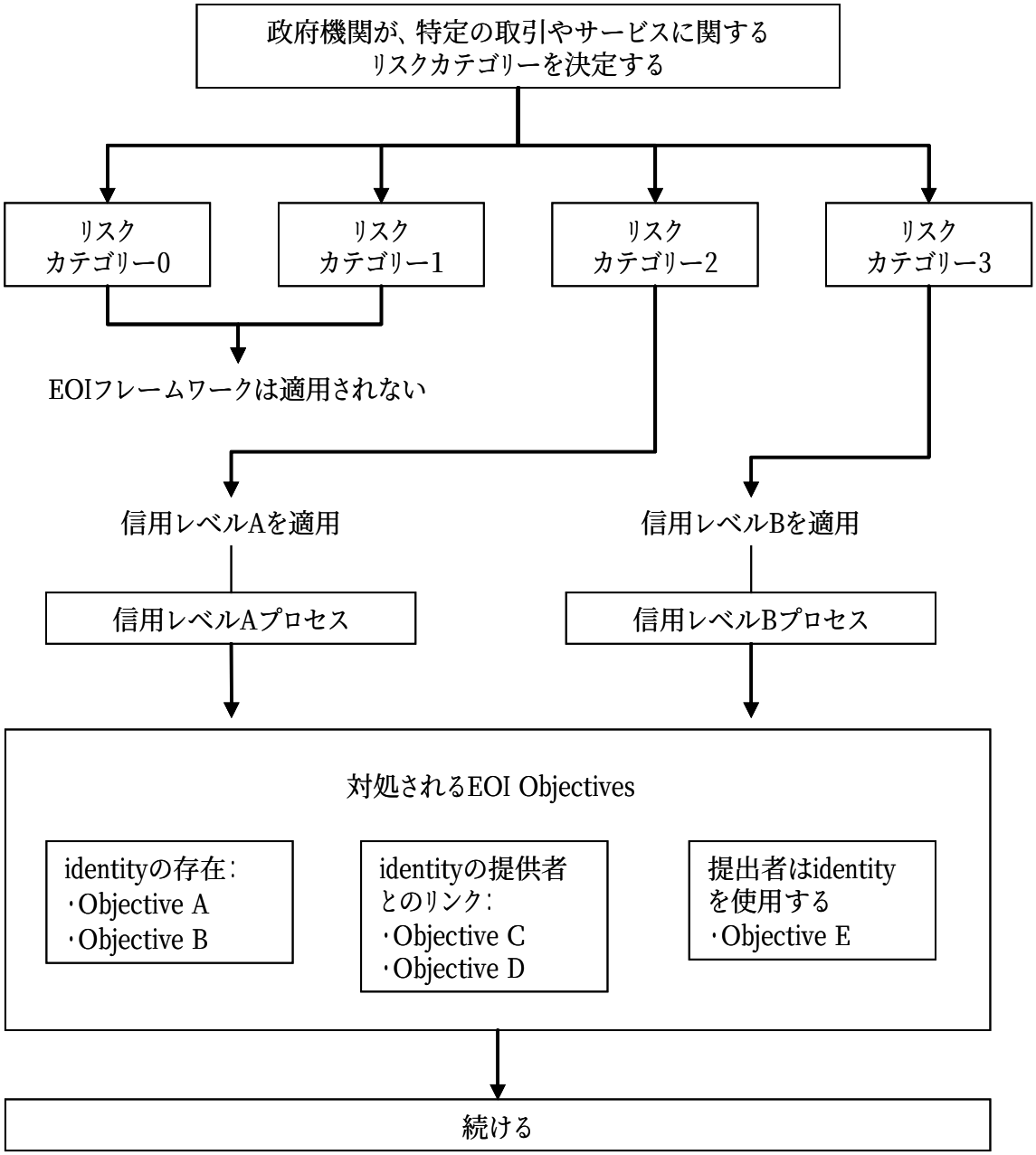


図 4−5　EOI フレームワーク利用工程

4.11.5.1. 本フレームワークの限定

EOI プロセスでも詐欺行為はありうる；結果を保証するものは扱いにくいので、（個人情報の過度な要求や政府機関の実施コストといった）コストは利益よりも優先される。

しかしながらフレームワークの目標を満たすことは、便宜主義的な者が単純な identity 詐欺行為や盗難に陥るリスクを軽減させると考えられる。例えば、信頼された証明書の検証における本フレームワークの要件は、存在しない保証人のサインの偽造のリスクを低減させるだろう。

4.11.5.2. identity ドキュメントの証拠

政府機関が自身の要件としてどの程度の頻度で関連ドキュメントを発行しておくべきかを、本フレームワークが規定しているわけではない。しかしながら、事例としては次のようなものを要求することが挙げられる。

- 現在のドキュメント（法的には、これに対する例外を規定するかもしれないが）
- “ コミュニティ（フレームワークでの Objective 3.E）における identity の使用 ” の証拠のため、（現在の使用を示すために）６ヶ月前までに発行された証拠と（長期に渡って個人により使用された identity と示すために）それ以前に発行された証拠のうち少なくとも１つのソース

もし個人の EOI（例えば、ニュージーランドで発行されなかったドキュメントや評判が傷つけられているドキュメントなど）に確信が持てない又はある個人が信用レベル B の要件を満たすことができないならば、政府機関は注意をし更なる協力的な認証を要求するべきである。

4.11.5.3. identity 情報の証拠管理

本フレームワークが強固な EOI プロセスのための good practice ガイドであるが、本フレームワークは、identity 情報の収集、保存、セキュリティの確保のために必要な内部プロセスについては対象としない。（ただし、Privacy 条例に関わるところは例外とする。）

フレームワークの成功は、EOI プロセスの管理のために効果的な社内手続を政府機関が持ち合わせることにある。弱い繋がりには次のことを含む。

- 内部での詐欺によるリスク
- セキュアでないシステム

- いい加減な処理標準
- いい加減な内部統制
- 最前線のスタッフに対する適切な危機認識トレーニングの不足

identity の潜在的詐欺や盗難を示している EOI を受け取った政府機関は、それらのプロシジャーに従い、適切な当局へ警告を発するべきである。もし、EOI の特定のフォームが変更されたり誤用されたりした場合には、（フレームワークを出した）政府機関は可能な限りアドバイスをするべきである。

4.11.6. 運用方法

上記の本フレームワーク利用方法の想定に含まれる。

4.11.7. 特徴

本フレームワークを作成する際、その他海外の政府電子認証モデルを参照した。それらのモデルをニュージーランドに則した形に変更したものである。

また、認証には住所や名前、運転免許証を必要とするので、基本的には人の認証のみを扱っている。

略称 Appendix

1. 本文中で用いている略称の正式表記

BCP	Best Current Practice
BCP	Business Continuity Plan（業務継続計画）
CA	Certification Authority（認証局）
CP	Certificate Policy（認証局証明書ポリシー）
CPS	Certification Practice Statement（認証業務規定）
CRL	Certificate Revocation List（証明書失効リスト）
CSP	Credential Service Provider
EAP	Electronic Authentication Partnership
EE	End Entity
EOI	Evidence of Identity
GPKI	Governmnent Public Key Infrastructure（政府認証基盤）
IDA	Interchange of Data between Administrations
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
ML	Mailing List（メーリングリスト）
OCSP	Online Certificate Status Protocol
OID	Object ID（オブジェクト ID）
PKI	Public Key Infrastructure（公開鍵基盤）

RA	Registration Authority（登録局）
RFC	Request For Comments
SAC	Service Assessment Criteria
SNS	Social Network Service
SSL	Secure Sockets Layer
WG	Working Group

表 4-1　海外における電子認証に関わる既存ガイドラインの例

海外ガイドライン	目的	利用者	利用方法の想定	運用方法	特徴
E-Authentication Guidance for Federal Agencies―（米国）	政府機関における個人認証において適切な保証レベルを提供すること。	連邦政府関係機関	政府機関が本文書に従って保証レベルを決定することを求める。	実施日以降の一定期限内に各機関による保証レベルの設定を規定。	4 段階の保証レベルを規定。個人の身元認証と属性認証を扱うが、サーバ認証等は対象外。
Registration and Authentication ― e-Government Strategy Framework Policy and Guidelines ―（英国）	電子政府の transaction における登録と認証についての保証レベルを定めること。	電子政府サービスの入手や提供をするもの。	政府が取引相手の本人性と権限を信頼し、プライバシーや機密性の侵害、データの盗難／不正使用、その他の危害が存在しないことを確保することが必要な場合。	特に記述されていない。	中央政府省庁および政府機関は、電子取引に関して本フレームワークを満たさなければならない。
Australian Government Electronic Authentication Framework ― （オーストラリア）	政府機関が認証方法について意思決定する場合に、必ず一貫した方法が適用されるようにし、政府機関が取引の際のリスクレベルに対応した認証手段を実施することを保証する。	政府機関と企業。	政府と企業間で認証が必要となる取引において、記載されている手順を参照する。	サービスの増加に伴い、ユーザ認証方法を換え、フレームワークも更新する。	オーストラリア政府の電子認証フレームワークの公開草案であり、この草案に対する意見を募っている。

海外ガイドライン	目的	利用者	利用方法の想定	運用方法	特徴
Authentication for e-government Best Practice Framework for Authentication — （ニュージーランド）	政府機関での認証分野におけるガイドラインを提供すること。	オンライン認証プロジェクトの計画に関わる人、または要件決定を行なう人。	電子政府サービスの中でも特に認証が必要なサービスを構築する際に利用される。	認証技術と実践の変化、オンライン認証の戦略的方向性に関する政府の意思決定を反映されるため、本フレームワークは定期的に改訂される。	電子認証の実装方法について詳細に述べており、また製品やサービス選択に関する助言も含まれる。
Interchange of Data between Administrations (IDA) Authentication Policy — （EU）	IDA 認証ポリシーの定義を行なうこと。	IDA Sectoral Network で遠隔認証を必要とするもの	Sectoral Project Authentication Policy を作成する際に利用される。	特になし。	このドキュメントは、フレームワーク規約 ENTR/01/67-CONSEC の下で準備されたもの。また、米国の E-Authentication Guidance for Federal Agencies と似ている部分が多数ある。人の認証のみを扱っている。

海外ガイドライン	目的	利用者	利用方法の想定	運用方法	特徴
TRUST FRAMEWORK —（米国）	Electronic Authentication Partnership（EAP）運用および利用に関するフレームワーク作り。	EAP システムに参加する全ての人々	CSP（クレデンシャル・サービス・プロバイダー）が、EAP 認定アセスメント機関によるアセスメントを無事完了することができるために利用する。	EAP は、このビジネス・ルールを公式化するものとし、これを定期的に修正することができる。	各信頼当事者と CSP は、EAP システムへの参加の前提条件として、このビジネス・ルールによって制約されていることに同意しなければならない。
EVIDENCE OF IDENTITY FRAMEWORK —（ニュージーランド）	政府機関と公共のメンバーが高リスクの取引を行う場合のフレームワークを提供する。	大多数の人々。未成年者や認証サービスへアクセスできない人を除く。			人の認証のみを扱っている。例えば、認証時に写真による検証を行なう等。

2. IETF における Best Current Practice の一覧

表A－1　現在有効なBest Current Practiceの一覧[1]

BCP番号	標題	作成者	発行時期	バイト数	備考
3	Variance for The PPP Compression Control Protocol and The PPP Encryption Control Protocol.	F. Kastenholz.	Feb-96	14347	(Also RFC1915)
4	An Appeal to the Internet Community to Return Unused IP Networks (Prefixes) to the IANA.	P. Nesser II.	Feb-96	23623	(Also RFC1917)
5	Address Allocation for Private Internets.	Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, E. Lear.	Feb-96	22270	(Obsoletes RFC1627, RFC1597) (Also RFC1918)
6	Guidelines for creation, selection, and registration of an Autonomous System (AS).	J. Hawkinson, T. Bates.	Mar-96	22073	(Also RFC1930)
7	Implications of Various Address Allocation Policies for Internet Routing.	Y. Rekhter, T. Li.	Oct-96	34717	(Also RFC2008)
8	IRTF Research Group Guidelines and Procedures. A. Weinrib,	J. Postel.	Oct-96	27507	(Also RFC2014)

[1] 本表の内容はRFC Editorより下記にて公開されている 2006 年 2 月 26 日時点の内容に基づく。
BCP INDEX
ftp://ftp.rfc-editor.org/in-notes/bcp-index.txt

BCP番号	標題	作成者	発行時期	バイト数	備考
9	The Internet Standards Process -- Revision 3.	S. Bradner.	Oct-96	86731	(Obsoletes RFC1602, RFC1871) (Updated by RFC3667, RFC3668, RFC3932, RFC3979, RFC3978) (Also RFC2026)
10	IAB and IESG Selection, Confirmation, and Recall Process: Operation of the Nominating and Recall Committees.	J. Galvin, Ed..	Jun-04	76395	(Obsoletes RFC2727) (Also RFC3777)
11	The Organizations Involved in the IETF Standards Process.	R. Hovey, S. Bradner.	Oct-96	13865	(Updated by RFC3668, RFC3979) (Also RFC2028)
12	Internet Registry IP Allocation Guidelines. K. Hubbard, M. Kosters, D. Conrad, D. Karrenberg,	J. Postel.	Nov-96	28975	(Obsoletes RFC1466) (Also RFC2050)
13	Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures.	N. Freed, J. Klensin.	Dec-05	74243	(Obsoletes RFC2048) (Also RFC4288, RFC4289)
14	Key words for use in RFCs to Indicate Requirement Levels.	S. Bradner.	Mar-97	4723	(Also RFC2119)
15	Deployment of the Internet White Pages Service.	H. Alvestrand, P. Jurg.	Sep-97	31539	(Also RFC2148)
16	Selection and Operation of Secondary DNS Servers.	R. Elz, R. Bush, S. Bradner, M. Patton.	Jul-97	27456	(Also RFC2182)
17	Use of DNS Aliases for Network Services.	M. Hamilton, R. Wright.	Oct-97	17858	(Also RFC2219)
18	IETF Policy on Character Sets and Languages.	H. Alvestrand.	Jan-98	16622	(Also RFC2277)
19	IANA Charset Registration Procedures.	N. Freed, J. Postel.	Oct-00	21615	(Obsoletes RFC2278) (Also RFC2978)

BCP番号	標題	作成者	発行時期	バイト数	備考
20	Classless IN-ADDR.ARPA delegation.	H. Eidnes, G. de Groot, P. Vixie.	Mar-98	17744	(Also RFC2317)
21	Expectations for Computer Security Incident Response.	N. Brownlee, E. Guttman.	Jun-98	86545	(Also RFC2350)
22	Guide for Internet Standards Writers.	G. Scott.	Jun-98	47280	(Also RFC2360)
23	Administratively Scoped IP Multicast.	D. Meyer.	Jul-98	17770	(Also RFC2365)
24	RSVP over ATM Implementation Guidelines.	L. Berger.	Aug-98	15174	(Also RFC2379)
25	IETF Working Group Guidelines and Procedures.	S. Bradner.	Sep-98	62857	(Obsoletes RFC1603) (Updated by RFC3934) (Also RFC2418)
26	Guidelines for Writing an IANA Considerations Section in RFCs.	T. Narten, H. Alvestrand.	Oct-98	25092	(Updated by RFC3692) (Also RFC2434)
27	Advancement of MIB specifications on the IETF Standards Track.	M. O'Dell, H. Alvestrand, B. Wijnen, S. Bradner.	Oct-98	13633	(Also RFC2438)
28	Enhancing TCP Over Satellite Channels using Standard Mechanisms.	M. Allman, D. Glover, L. Sanchez.	Jan-99	47857	(Also RFC2488)
29	Procedure for Defining New DHCP Options.	R. Droms.	Jan-99	10484	(Obsoleted by RFC2939) (Also RFC2489)
30	Anti-Spam Recommendations for SMTP MTAs.	G. Lindberg.	Feb-99	53597	(Also RFC2505)
31	Media Feature Tag Registration Procedure.	K. Holtman, A. Mutz, T. Hardie.	Mar-99	24892	(Also RFC2506)
32	Reserved Top Level DNS Names.	D. Eastlake 3rd, A. Panitz.	Jun-99	8008	(Also RFC2606)
33	URN Namespace Definition Mechanisms.	L. Daigle, D. van Gulik, R. Iannella, P. Falstrom.	Jun-99	26916	(Obsoleted by RFC3406) (Also RFC2611)
34	Changing the Default for Directed Broadcasts in Routers.	D. Senie.	Aug-99	6820	(Updates RFC1812) (Also RFC2644)

BCP番号	標題	作成者	発行時期	バイト数	備考
35	Registration Procedures for URL Scheme Names.	R. Petke, I. King.	Nov-99	19780	(Obsoleted by RFC4395) (Also RFC2717)
36	Guidelines for Writers of RTP Payload Format Specifications.	M. Handley, C. Perkins.	Dec-99	24143	(Also RFC2736)
37	IANA Allocation Guidelines For Values In the Internet Protocol and Related Headers.	S. Bradner, V. Paxson.	Mar-00	18954	(Also RFC2780)
38	Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing.	P. Ferguson, D. Senie.	May-00	21258	(Obsoletes RFC2267) (Updated by RFC3704) (Also RFC2827)
39	Charter of the Internet Architecture Board (IAB).	Internet Architecture Board, B. Carpenter, Ed..	May-00	15984	(Obsoletes RFC1601) (Also RFC2850)
40	Root Name Server Operational Requirements.	R. Bush, D. Karrenberg, M. Kosters, R. Plzak.	Jun-00	21133	(Obsoletes RFC2010) (Also RFC2870)
41	Congestion Control Principles.	S. Floyd.	Sep-00	43823	(Also RFC2914)
42	Domain Name System (DNS) IANA Considerations.	D. Eastlake 3rd, E. Brunner-Williams, B. Manning.	Sep-00	22454	(Also RFC2929)
43	Procedures and IANA Guidelines for Definition of New DHCP Options and Message Types.	R. Droms.	Sep-00	13631	(Obsoletes RFC2489) (Also RFC2939)
44	Use of HTTP State Management.	K. Moore, N. Freed.	Oct-00	18899	(Also RFC2964)
45	IETF Discussion List Charter.	S. Harris.	Nov-00	5682	(Also RFC3005)
46	Recommended Internet Service Provider Security Services and Procedures.	T. Killalea.	Nov-00	27905	(Also RFC3013)
47	Tags for the Identification of Languages.	H. Alvestrand.	Jan-01	26522	(Obsoletes RFC1766) (Also RFC3066)

BCP番号	標題	作成者	発行時期	バイト数	備考
48	End-to-end Performance Implications of Slow Links.	S. Dawkins, G. Montenegro, M. Kojo, V. Magret.	Jul-01	39942	(Also RFC3150)
49	Delegation of IP6.ARPA.	R. Bush.	Aug-01	5727	(Obsoleted by RFC3596) (Updates RFC2874, RFC2772, RFC2766, RFC2553, RFC1886)(Also RFC3152)
50	End-to-end Performance Implications of Links with Errors.	S. Dawkins, G. Montenegro, M. Kojo, V. Magret, N. Vaidya.	Aug-01	36388	(Also RFC3155)
51	IANA Guidelines for IPv4 Multicast Address Assignments.	Z. Albanna, K. Almeroth, D. Meyer, M. Schipper.	Aug-01	15389	(Also RFC3171)
52	Management Guidelines & Operational Requirements for the Address and Routing Parameter Area Domain ("arpa").	G. Huston, Ed..	Sep-01	18097	(Also RFC3172)
53	GLOP Addressing in 233/8.	D. Meyer, P. Lothberg.	Sep-01	8225	(Obsoletes RFC2770) (Also RFC3180)
54	IETF Guidelines for Conduct.	S. Harris.	Oct-01	7413	(Also RFC3184)
55	Guidelines for Evidence Collection and Archiving.	D. Brezinski, T. Killalea.	Feb-02	18468	(Also RFC3227)
56	On the use of HTTP as a Substrate.	K. Moore.	Feb-02	34785	(Also RFC3205)
57	IANA Considerations for IPv4 Internet Group Management Protocol (IGMP).	B. Fenner.	Feb-02	6473	(Also RFC3228)
58	Defining the IETF.	P. Hoffman, S. Bradner.	Feb-02	6401	(Also RFC3233)
59	A Transient Prefix for Identifying Profiles under Development by the Working Groups of the Internet Engineering Task Force.	M. Rose.	Jul-02	7916	(Also RFC3349)

BCP番号	標題	作成者	発行時期	バイト数	備考
60	Inappropriate TCP Resets Considered Harmful.	S. Floyd.	Aug-02	46748	(Also RFC3360)
61	Strong Security Requirements for Internet Engineering Task Force Standard Protocols.	J. Schiller.	Aug-02	16411	(Also RFC3365)
62	Advice to link designers on link Automatic Repeat reQuest (ARQ).	G. Fairhurst, L. Wood.	Aug-02	66097	(Also RFC3366)
63	Session Initiation Protocol for Telephones (SIP-T): Context and Architectures.	A. Vemuri, J. Peterson.	Sep-02	49893	(Also RFC3372)
64	Internet Assigned Numbers Authority (IANA) Considerations for the Lightweight Directory Access Protocol (LDAP).	K. Zeilenga.	Sep-02	45893	(Also RFC3383)
65	Dynamic Delegation Discovery System (DDDS) Part Five: URI.ARPA Assignment Procedures.	M. Mealling.	Oct-02	19469	(Also RFC3405)
66	Uniform Resource Names (URN) Namespace Definition Mechanisms.	L. Daigle, D. van Gulik, R. Iannella, P. Faltstrom.	Oct-02	43707	(Obsoletes RFC2611) (Also RFC3406)
67	Change Process for the Session Initiation Protocol (SIP).	A. Mankin, S. Bradner, R. Mahy, D. Willis, J. Ott, B. Rosen.	Dec-02	26234	(Updated by RFC3968, RFC3969) Also RFC3427)
68	Layer Two Tunneling Protocol (L2TP) Internet Assigned Numbers Authority (IANA) Considerations Update.	W. Townsley.	Dec-02	9135	(Also RFC3438)
69	TCP Performance Implications of Network Path Asymmetry.	H. Balakrishnan, V. Padmanabhan, G. Fairhurst, M. Sooriyabandara.	Dec-02	108839	(Also RFC3449)
70	Guidelines for the Use of Extensible Markup Language (XML) within IETF Protocols.	S. Hollenbeck, M. Rose, L. Masinter.	Jan-03	64252	(Also RFC3470)

BCP番号	標題	作成者	発行時期	バイト数	備考
71	TCP over Second (2.5G) and Third (3G) Generation Wireless Networks.	H. Inamura, Ed., G. Montenegro, Ed., R. Ludwig, A. Gurtov, F. Khafizov.	Feb-03	61528	(Also RFC3481)
72	Guidelines for Writing RFC Text on Security Considerations.	E. Rescorla, B. Korver.	Jul-03	110393	(Also RFC3552)
73	An IETF URN Sub-namespace for Registered Protocol Parameters.	M. Mealling, L. Masinter, T. Hardie, G. Klyne.	Jun-03	14815	(Also RFC3553)
74	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework.	R. Frye, D. Levi, S. Routhier, B. Wijnen.	Aug-03	115222	(Obsoletes RFC2576) (Also RFC3584)
75	Session Initiation Protocol (SIP) Basic Call Flow Examples.	A. Johnston, S. Donovan, R. Sparks, C. Cunningham, K. Summers.	Dec-03	163159	(Also RFC3665)
76	Session Initiation Protocol (SIP) Public Switched Telephone Network (PSTN) Call Flows.	A. Johnston, S. Donovan, R. Sparks, C. Cunningham, K. Summers.	Dec-03	200478	(Also RFC3666)
77	IETF ISOC Board of Trustee Appointment Procedures.	L. Daigle, Ed., Internet Architecture Board.	Dec-03	13008	(Also RFC3677)
78	IETF Rights in Contributions.	S. Bradner, Ed..	Mar-01-05	43574	(Obsoletes RFC3667) (Updates RFC2026) (Also RFC3978)
79	Intellectual Property Rights in IETF Technology.	S. Bradner, Ed..	Mar-01-05	41366	(Obsoletes RFC3668) (Updates RFC2026, RFC2028) (Also RFC3979)
80	Delegation of E.F.F.3.IP6.ARPA.	R. Bush, R. Fink.	Jan-04	7137	(Also RFC3681)

BCP番号	標題	作成者	発行時期	バイト数	備考
81	The IETF XML Registry.	M. Mealling.	Jan-04	17325	(Also RFC3688)
82	Assigning Experimental and Testing Numbers Considered Useful.	T. Narten.	Jan-04	15054	(Updates RFC2434) (Also RFC3692)
83	A Practice for Revoking Posting Rights to IETF Mailing Lists.	M. Rose.	Mar-04	15698	(Also RFC3683)
84	Ingress Filtering for Multihomed Networks.	F. Baker, P. Savola.	Mar-04	35942	(Updates RFC2827) Also RFC3704)
85	Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP).	J. Rosenberg, J. Peterson, H. Schulzrinne, G. Camarillo.	Apr-04	77308	(Also RFC3725)
86	Determining Strengths For Public Keys Used For Exchanging Symmetric Keys.	H. Orman, P. Hoffman.	Apr-04	55939	(Also RFC3766)
87	Use of Interior Gateway Protocol (IGP) Metric as a second MPLS Traffic Engineering (TE) Metric.	F. Le Faucheur, R. Uppili, A. Vedrenne, P. Merckx, T. Telkamp.	May-04	17475	(Also RFC3785)
88	IANA Considerations for the Point-to-Point Protocol (PPP).	V. Schryver.	Jun-04	6321	(Also RFC3818)
89	Advice for Internet Subnetwork Designers.	P. Karn, Ed., C. Bormann, G. Fairhurst, D. Grossman, R. Ludwig, J. Mahdavi, G. Montenegro, J. Touch, L. Wood.	Jul-04	152174	(Also RFC3819)
90	Registration Procedures for Message Header Fields.	G. Klyne, M. Nottingham, J. Mogul.	Sep-04	36231	(Also RFC3864)
91	DNS IPv6 Transport Operational Guidelines.	A. Durand, J. Ihren.	Sep-04	10025	(Also RFC3901)

BCP番号	標題	作成者	発行時期	バイト数	備考
92	The IESG and RFC Editor Documents: Procedures.	H. Alvestrand.	Oct-04	17093	(Updates RFC2026, RFC3710) (Also RFC3932)
93	A Model for IETF Process Experiments.	J. Klensin, S. Dawkins.	Nov-04-04	14409	(Also RFC3933)
94	Updates to RFC 2418 Regarding the Management of IETF Mailing Lists.	M. Wasserman.	Oct-04	8488	(Updates RFC2418) (Also RFC3934)
95	A Mission Statement for the IETF.	H. Alvestrand.	Oct-04	16639	(Also RFC3935)
96	Procedures for Modifying the Resource reSerVation Protocol (RSVP).	K. Kompella, J. Lang.	Oct-04	15314	(Updates RFC3209, RFC2205) (Also RFC3936)
97	Clarifying when Standards Track Documents may Refer Normatively to Documents at a Lower Level.	R. Bush, T. Narten.	Dec-04	12251	(Also RFC3967)
98	The Internet Assigned Number Authority (IANA) Header Field Parameter Registry for the Session Initiation Protocol (SIP).	G. Camarillo.	Dec-04	20615	(Updates RFC3427) (Also RFC3968)
99	The Internet Assigned Number Authority (IANA) Uniform Resource Identifier (URI) Parameter Registry for the Session Initiation Protocol (SIP).	G. Camarillo.	Dec-04	12119	(Updates RFC3427) (Also RFC3969)
100	Early IANA Allocation of Standards Track Code Points.	K. Kompella, A. Zinin.	Feb-22-05	13706	(Also RFC4020)
101	Structure of the IETF Administrative Support Activity (IASA).	R. Austein, Ed., B. Wijnen, Ed., B. Carpenter, Ed., L. Lynch, Ed..	Jan-06	55589	(Also RFC4071, RFC4371)
102	IAB Processes for Management of IETF Liaison Relationships.	L. Daigle, Ed., Internet Architecture Board.	Apr-25-05	18360	(Also RFC4052)

BCP番号	標題	作成者	発行時期	バイト数	備考
103	Procedures for Handling Liaison Statements to and from the IETF.	S. Trowbridge, S. Bradner, F. Baker.	Apr-25-05	38816	(Also RFC4053)
104	Terminology for Describing Internet Connectivity.	J. Klensin.	May-11-05	24522	(Also RFC4084)
105	Embedding Globally-Routable Internet Addresses Considered Harmful.	D. Plonka.	Jun-05	22656	(Also RFC4085)
106	Randomness Requirements for Security.	D. Eastlake, 3rd, J. Schiller, S. Crocker.	Jun-03-05	114321	(Obsoletes RFC1750) (Also RFC4086)
107	Guidelines for Cryptographic Key Management.	S. Bellovin, R. Housley.	Jun-05	14752	(Also RFC4107)
108	IP Performance Metrics (IPPM) Metrics Registry.	E. Stephan.	Aug-05	23074	(Also RFC4148)
109	Deprecation of "ip6.int"	G. Huston.	Aug-05	5353	(Also RFC4159)
110	Tunneling Multiplexed Compressed RTP (TCRTP).	B. Thompson, T. Koren, D. Wing.	Nov-05	48990	(Also RFC4170)
111	Guidelines for Authors and Reviewers of MIB Documents.	C. Heard, Ed..	Sep-05	102521	(Also RFC4181)
112	Prioritized Treatment of Specific OSPF Version 2 Packets and Congestion Avoidance.	G. Choudhury, Ed..	Oct-05	34132	(Also RFC4222)
113	The IETF Administrative Oversight Committee (IAOC) Member Selection Guidelines and Process.	G. Huston, Ed., B. Wijnen, Ed..	Dec-05	15396	(Also RFC4333)
114	BGP Communities for Data Collection.	D. Meyer.	Feb-06	26078	(Also RFC4384)
115	Guidelines and Registration Procedures for New URI Schemes.	T. Hansen, T. Hardie, L. Masinter.	Feb-06	31933	(Obsoletes RFC2717, RFC2718) (Also RFC4395)