経済産業省補助事業

平成１６年度情報セキュリティ対策推進事業

（電子商取引（ＥＣ）技術基盤の相互運用性に関する調査研究）

PKI を利用したアプリケーションの実用化に向けての課題と方向性調査

平成 17 年 3 月

（財）日本情報処理開発協会

― 目 次 ―

1 はじめに

平成 13 年度から平成 15 年度まで「電子商取引（EC）技術基盤の相互運用性に関する調査研究」としてアジア各国/地域における PKI の相互接続実験を実施した。その結果として、PKI の相互接続が可能であることを実証することができ、「Asia PKI Interoperability Guideline v.1.0」を作成し、アジア PKI フォーラムにおいて、評価を得ることができた。しかし、PKI を利用したクロスボーダの電子取引の普及に関しては、キラーアプリケーションの掘り起こし等の課題があり、民間のビジネスに本ガイドラインを新たに適用することは容易ではない。

一方、情報技術やブロードバンドの普及により、インターネット上での大量の情報交換が行われ、インターネットの利便性は向上している。しかし、その利便性とは裏腹にネットワークセキュリティの様々な問題が表面化し、利用者への脅威・リスクは増加の一途を辿っている。安全・安心なネットワークを実現するために、電子認証基盤が重要な役割を果たすと考えられている。

電子認証基盤により各情報システムが連携したワンストップサービスを提供するには、それぞれの情報システムにおける電子認証に関するポリシーについて合意する必要がある。そのためには、電子認証に関するポリシーをどのように合意するか、そして、それぞれの情報システムにおける電子認証をどのように連携するかという課題が出てくる。このような課題の解決を目的として、近年、米国における「e-Authentication イニシアチブ」に代表されるように、電子認証に関する検討が世界的に進んでいる。そして、その一部が実際に利用されつつあるものの、国内ではようやく検討が始まった段階である。電子認証技術の可能性としては、前述の情報システム（基盤）連携の実現に留まらない。現在、フィッシング詐欺が社会問題となっており、偽サイト（クレジットカード会社の偽サイト、銀行の偽サイト等）へ個人情報（氏名、住所、ID/パスワード等）を送信してしまう被害者が増加している。このような問題の背景には、偽サイトを正しく電子認証する手段（電子認証技術）が整っていないことが挙げられ、問題解決のために電子認証技術を検討することが有効であると考えられる。

そこで本調査研究では、日本 PKI フォーラムの会員企業に対して、電子認証に関する現状調査を行い、日本国内におけるニーズを探った。そして、そのニーズの解決策を検討するためのリファレンスとして海外事例調査を行い、その結果を基に日本における電子認証の今後の方向性を検討した。

2 電子認証の現状とその課題

本報告書における“電子認証”とは、情報技術を用いた本人認証の仕組みのことをいう。本章ではコンピュータシステムに対するログイン手段に注目し、現状の電子認証に関する課題を考える。

2.1　ログイン手段の現状とその課題

2.1.1 社内システムへのログイン手段とその課題

平成17年1月～2月に日本PKIフォーラムが会員企業を対象に行った調査(以下、本調査という）の結果では、社内システムへログインする手段として、「ID/パスワード方式を採用している」という回答が多い。また、ログインを必要とする社内システムは複数あり、それぞれの社内システムを利用するたびに利用者はログインを実行している。

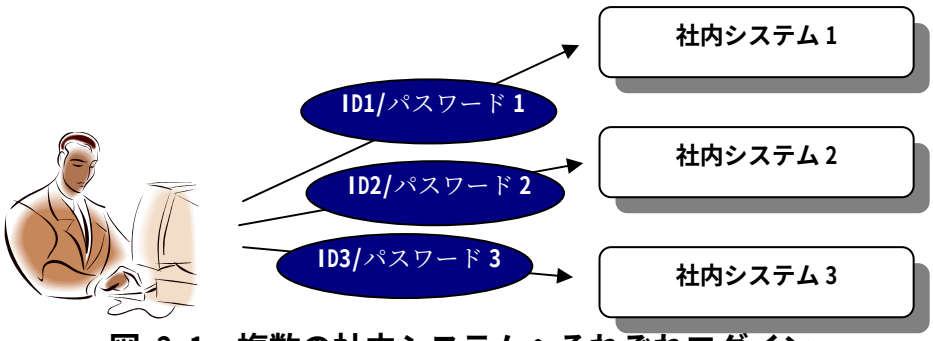


図 2.1　複数の社内システムへそれぞれログイン

本調査の結果では、このように社内システムへのログインのために複数のID/パスワードを持つことに対して、改善が必要と回答している人が多い。これは、複数のID/パスワードを管理することがシステム利用者の負担となっていることが考えられる。

2.1.2 インターネットサービスへのログイン手段とその課題

本調査では、インターネットサービス（オークションサイト、ショッピングサイト）へのログインについてもアンケートをとっている。本調査結果によると、多くの人がインターネットサービスへのログイン ID を複数保有しており、それらのログイン ID の統一を希望している。

また、本調査の結果によると、ログイン ID の取得に際し、個人情報をインターネットサービスサイトへ送信すること避けたいと考えている利用者が多い。特に、個人的に信頼できないサイトへは個人情報を送付することを避けたいと考えている回答が圧倒的であった。つまり、現状は「様々なサービスを受ける→ログイン ID を複数取得する→複数のインターネットサービスサイトへ個人情報を送付する」という図式が成り立つなかで、インターネットサービスサイトへ個人情報を送付することを、なるべく防ぐためには 1 つのログイン ID で様々なサービスを利用できることが 1 つの解として挙げることができる。

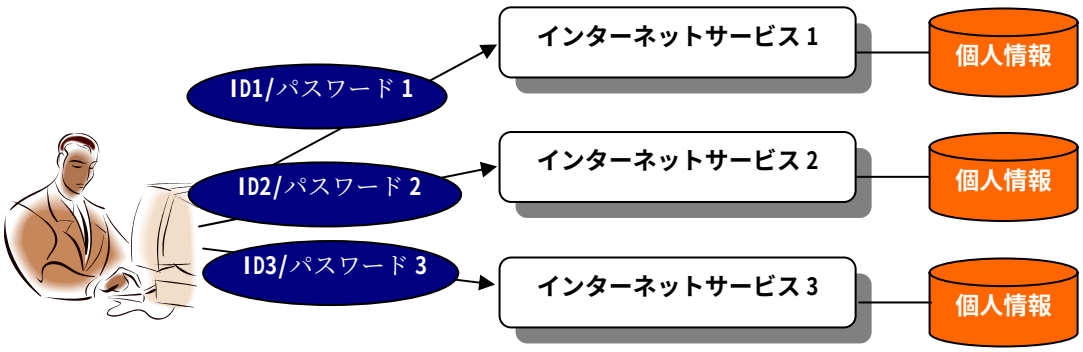


図 2.2　複数のインターネットサービスへそれぞれログイン

2.2　課題の解決に向けて

2.1 節で述べた、ログイン ID に関する利用者の要望をまとめると以下の 2 点が挙げられる。

- 1 回のログイン（認証）で、複数のシステムまたはサービスへログインしたい。
- システムまたはサービス提供者側への個人情報の送付はなるべく避けたい。

これは、日本 PKI フォーラムが会員企業に対して行った調査の結果であるが、「利用者視点にたったワンストップサービスの提供」等に注目が集まっている世の中の流れと一致しており、プライバシー保護を踏まえた、シングルサインオンが望まれている。

シングルサインオン（以下 SSO）とは、「利用者が一回の認証で、複数のサービス（システム）の利用が可能となる」ことであり、シングルサインオンにより利用者は複数の ID/パスワードを管理する必要が無くなる。

シングルサインオンの実現には、以下のステップが必要となる。

(1) 認証情報の統合
　・・・認証に関する情報を統一的に管理

(2) 認証手段の統一
　・・・認証手段（ID/パスワード）の統一

(3) アクセス制御の統合
　・・・提供を受けることができるサービスに対するアクセス制御の統合

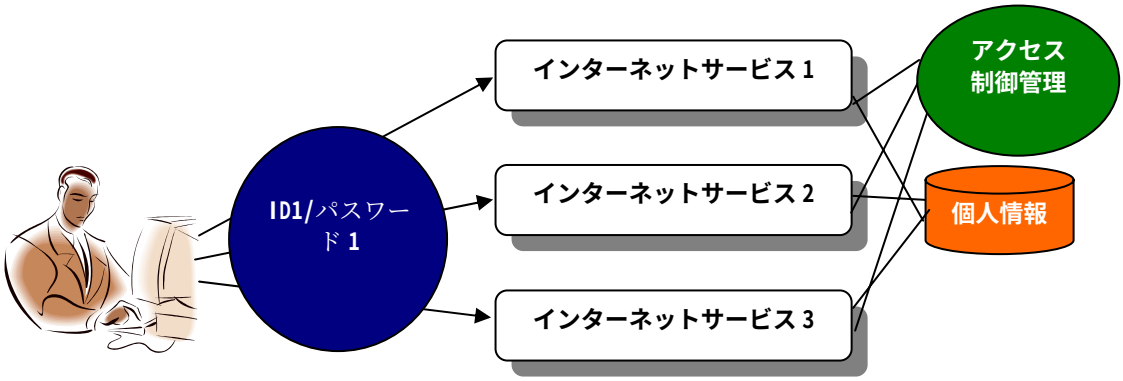


図 2.3　シングルサインオンの概念

2.2.1 シングルサインオンの現状と課題

シングルサインオンを実現するためには、「認証情報の統合」「認証手段の統一」「アクセス制御の統合」のステップが必要であることは前述したが、これには、「認証」に関する基準が必要となる。

社内システムを例にあげると、シングルサインオンを実現するためには、複数の異なるシステムが「認証」に関する社内共通的な基準に従うことが必要である。日本 PKI フォーラムの調査では、過半数の人が「ログインが必要なシステムを構築する際の社内基準を持っている」と回答している。また、調査結果では社内システムのいくつかはシングルサインオン化が進んでいるとの回答もあり、シングルサインオンの適用は今後増加していくと考えられる。

一方、インターネットサービスについて考えると、インターネットはオープンな場であり、その点で企業の社内システムとは大きく異なる。社内システムは、その企業が独自に定めた認証基準を用いることでシングルサインオン化が可能となる。しかし、インターネット上で他企業が提供するサービス同士がシングルサインオンを実現しようとする場合、各社がそれぞれの会社の認証基準によりサービスを提供している限り、認証基準の対立が生じ、シングルサインオンを実現するためのステップを実行できない。

図 2.4　認証基準の対立

この問題を解決するために共通の認証基準の設定と適用が必要となる。

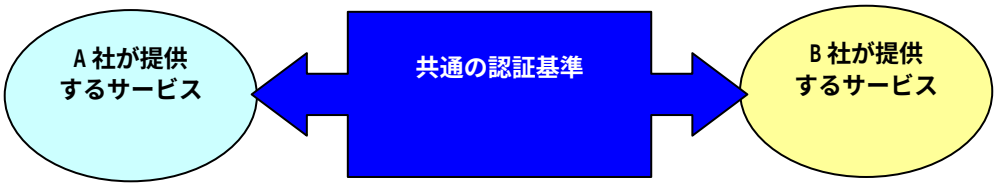


図 2.5　認証基準の共通化

しかしながら、日本国内にはこのような「認証基準」は整備されていないのが現状である。そのため、「認証基準」の整備が急がれる。

2.2.2 シングルサインオン技術の活用によるメリット

シングルサインオンの必要性と実現に向けての課題を述べたが、次に、シングルサインオンを実現することによる利用者およびインターネットサービス事業者のメリットについて述べる。

(1) 利用者のメリット

(a) 複数のログイン ID およびパスワードの管理からの開放

前述の通り、シングルサインオンを適用することにより、利用者は複数のサービスを 1 つのログイン ID/パスワードで利用できる。

(2) インターネットサービス事業者のメリット

(a) 電子認証専業サービスの利用

シングルサインオン技術を利用すると複数のインターネットサービス事業者（以下、サービス事業者）間で認証情報を共有することができる。そのため、利用者を電子認証し、その認証結果をサービス事業者へ提供する電子認証専業サービスの登場が予想できる。情報化社会の変化に迅速に対応するためには、サービス事業者にとって、経営資源の選択と集中は重要な課題の 1 つである。サービス事業者は、電子認証専業サービスを利用することで本業のサービス事業へ経営資源を集中できる。

(b) 個人情報保護法への対応

平成 17 年 4 月より個人情報保護法が施行される。サービス事業者が、利用者

認証のためだけに個人情報を収集する必要性があるのであれば、シングルサインオン技術を利用することで、収集する個人情報を必要最低限に抑えることができ、個人情報保護の管理にかかる負荷、費用を削減することができる。以下にその可能性を述べる。

(i) 電子認証専業サービスの利用

サービス事業者が電子認証専業サービスを利用した場合、電子認証に必要な個人情報の収集作業および管理は電子認証専業サービスが行う。そのため、サービス事業者は電子認証のための個人情報の収集作業および管理を行う必要が無くなる。

(ii) 他のサービス事業者との認証情報の共有

シングルサインオン技術を利用すると、他のサービス事業者が利用者を認証した情報を共有できる。そのため、認証情報の提供を受けるサービス事業者は、他のサービス事業者が電子認証する利用者の個人情報を管理する必要が無くなる。また、認証情報を共有することにより、複数の異なるサービスがシームレスにつながる可能性が広がり、各サービス間の相互運用性の向上が期待される。

(3) 利用者およびサービス事業者のメリット

(a) セキュリティレベルの標準化

複数のサービス事業者間でシングルサインオンを実現するためには、同一の認証基準が必要になることは、前述した通りである。同一の認証基準は、シングルサインオンを実現するだけでなく、サービス内容に応じて電子認証にかかわるセキュリティ要件を統一することができる。これにより、セキュリティレベルの標準化を図ることができる。

2.3 まとめ

2 章の内容をまとめると、以下の 2 点である。

- シングルサインオンは非常に有効な技術であり、利用者およびサービス事業者にとってメリットが多い。

- シングルサインオンの実現には認証基準が必要である。
  - クローズドなシステム（社内システム等）における認証基準は一部で整備が進んでいるようである。
  - オープンなシステム（インターネット上の各種サービスシステム等）でシングルサインオン化する場合、リファレンスとなる認証基準が存在しない。

しかしながら、シングルサインオンの実現には、認証基準の整備、ログイン ID の統一、認証情報の統合、認証情報の連携方法等の課題がある。これらの課題については、いくつかの海外のプロジェクトで検討が進められている。

そこで、次章以降では、海外におけるシングルサインオン、認証基準に関するプロ

ジェクトの事例調査を実施し、調査結果を紹介する。そして、日本における電子認証の今後の方向性を検討する。

3 電子認証基盤

3.1　電子認証基盤とは

人、サービス、デバイスがシームレスに接続されていくユビキタスネットワーク社会において、安全・安心を提供するサービスを実現するためには、信頼関係を確立するための認証（Authentication）が重要になる。人の認証だけでなく、サービスやデバイス等の認証も重要な役割を果たし、また、時刻（いつ）や位置（どこ）等といった認証も必要な場面がある。認証は、安全・安心なユビキタスネットワーク社会を実現するための、最も重要な要素のひとつになると考えられるが、これらの認証に対して、これまでにない多様な要求が浮上している。人の認証ということだけをとっても、プライバシー保護のための仮名による認証、人の色々な属性に関する認証が挙げられる。これらの認証が、シームレスに接続されたユビキタスネットワークにおいて、より大規模に、更に色々な組織を超えて行われることが要求されている。

様々な認証技術が登場しているものの、ユビキタスネットワーク社会で要求される個々のネットワークや組織を超えた広範囲なドメインにおける認証を実現するには、まだ大きな壁がある。それは、閉じられたローカルな認証では大きく取り上げられることのなかった、下記のような問題があるためである。

- 相互運用性の問題
  これまでの多くの認証技術は、限られた環境で動作すればよかったが、広いドメインの認証ではそれらの相互運用性が重要な問題となる。
- 認証に対するセキュリティレベルの向上
  これまでのインターネットにおける認証は当たり前に利用されているにもかかわらず、認証に対して何の評価基準もなく、実際に利用されている認証も低いセキュリティレベルのものが主流であると思われる。
- プライバシーの問題
  ドメインを超えた認証を行う場合には、利用者のプライバシーを十分に考慮する必要がある。

こうした壁を取り除き、安全・安心なサービスの連携や協調を実現するためには、電子認証基盤の整備が重要である。図 3.1 では電子認証基盤と、その基盤上で実現されるサービスとの関係を示す。電子認証基盤が広範なサービスの連携や協調のための信頼の礎となるためには、技術、ポリシー・運用、ビジネスルールを含めたフレームワークを提供することが必要である。例えば、下記に掲げた項目を提供することが必要であろう。また、このような電子認証基盤の整備は先行する海外の事例が参考となる。海外の事例や動向と日本の現状を踏まえ、日本で実現すべき電子認証基盤とはどうあるべきかを考えることが重要である。

[技術]

- 認証に関わる要素技術や実装についての調査・検討
  セキュアな認証を実現するための技術（例えば PKI やバイオメトリクス等）や実装を調査・検討し、適用する技術や実装を選定するための指針を与える。例えば、本稿 4 章で紹介する NIST の電子認証ガイドラインが参考となる。

・ 連携フレームワーク
連携フレームワークとは認証システムを相互に連携するための技術仕様である。電子認証基盤を利用するシステムの構築を容易にするための開発環境（ライブラリ等）や、相互運用性を確保するためのテストスイートの提供や、実装の評価も重要である。例えば、本稿 4 章で紹介する Shibboleth や Liberty の活動や技術仕様が参考となる。

[ポリシー＆運用]
・ 認証の評価基準
認証に対する保証レベルの規定と、その保証レベルを決定するプロセス（認証に関わるリスクアセスメント等）や、保証レベルを実現するための要件（本人確認手段や認証技術等）を与える。

・ 認証に関わる事業者に対する評価方法と認定制度
利用者の認証に関わる事業者（例えば公開鍵証明書を発行する認証局や、認証を必要とするサービスを実施する事業者等）に対する評価方法を定め、認定制度を設ける。
事業者の認定は、上記の認証の保証レベルや利用者の個人情報の取り扱いに関するプライバシーポリシー等に基づいて評価をした結果に基づくものと考えられる。

このような認証の評価基準を始めとする課題は、従来の企業内等閉じられたドメインでの認証とは異なり、組織を超えた広範な連携を行うためには特に重要である。3.3 節で改めて認証の評価基準の必要性について説明する。

[ビジネス]
・ ビジネスルール
参加する事業者に対する責任や規約等を含むビジネスルールを策定する。ビジネスルールは一意ではなく、リスクやコスト等の関係から様々なレベルの契約が存在することも考えられる。このような契約レベルは認証の保証レベル等を含めた様々な評価基準によって考えられるものである。

・ ビジネスモデル
アプリケーションや基本的なビジネスモデルを提示することにより、広範で多数の参加者による連携を促進する。

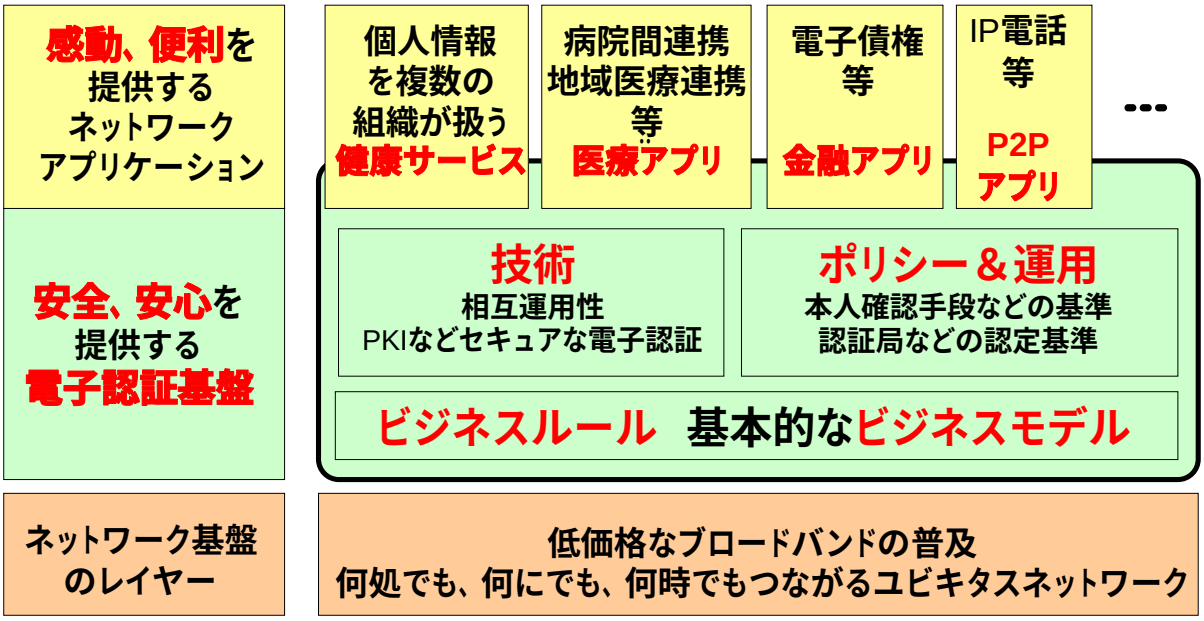


図 3.1　電子認証基盤

3.2　ID 連携（Identity federation）

これまでのインターネット上のサービスでは、利用者の認証が必要な場合に、それぞれのサービスで認証システムを構築し、自身で利用者の認証を行うものが一般的であった（図 3.2）。こうした認証システムはサービスごとに閉じられたものであり、サービス間で相互に認証システムを利用するための共通の仕組みを持たないため、利用者は利用するサービスごとに、それぞれの認証プロセスが必要であった。

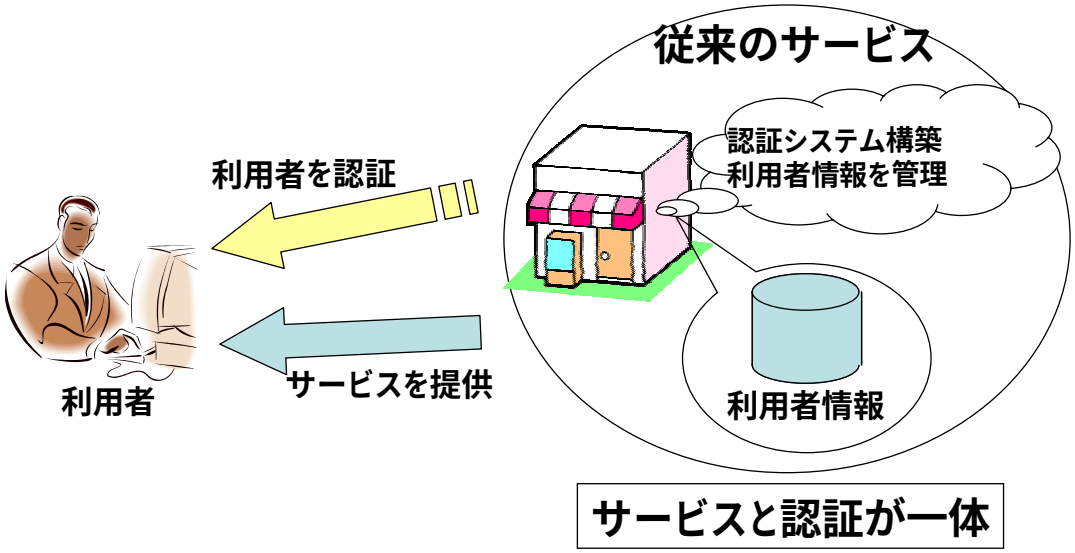


図 3.2　従来型の認証モデル

しかし、近年、OASIS により標準化された SAML（Security Assertion Markup Language）が登場し、さらに SAML の拡張として、Liberty Alliance の ID-FF 仕様や、Internet2/MACE プロジェクトの Shibboleth といったフレームワークが登場し

たことで、異なる認証システム間で利用者の認証情報を交換しシングルサインオン(SSO)を実現する ID 連携が実現可能になりつつある。Liberty と Shibbleth についての詳細は 4.2 節、4.3 節を参照のこと。

この ID 連携の仕組みにより、利用者の認証を行う役割を担う認証プロバイダーと、その認証プロバイダーから認証に関する情報を受けることでサービスを実施するサービスプロバイダーのように、サービスと認証が分離した事業者モデルを考えることができるようになった。

例えば、図 3.3 に示したモデルでは、認証プロバイダーは利用者を認証し、認証情報（例えば、いつ、どのような方法で認証したか等）をサービスプロバイダーに提供する。サービスプロバイダーはその認証情報を得ることで利用者が認証済みであると判断し、サービスを実施する。サービスプロバイダーはサービスの実施にあたり、認証情報だけでなく利用者に関する属性情報（例えば、年齢や性別等）を必要とするかもしれない。その場合には、サービスプロバイダー自身が管理する利用者の属性情報を用いるか、あるいは、他の事業者から利用者の属性情報の提供を受けることが考えられる。他の事業者との属性情報の連携のためには、さらに別の仕組み[1]が必要となるが、その仕組みは ID 連携を基礎として実施されるものである。

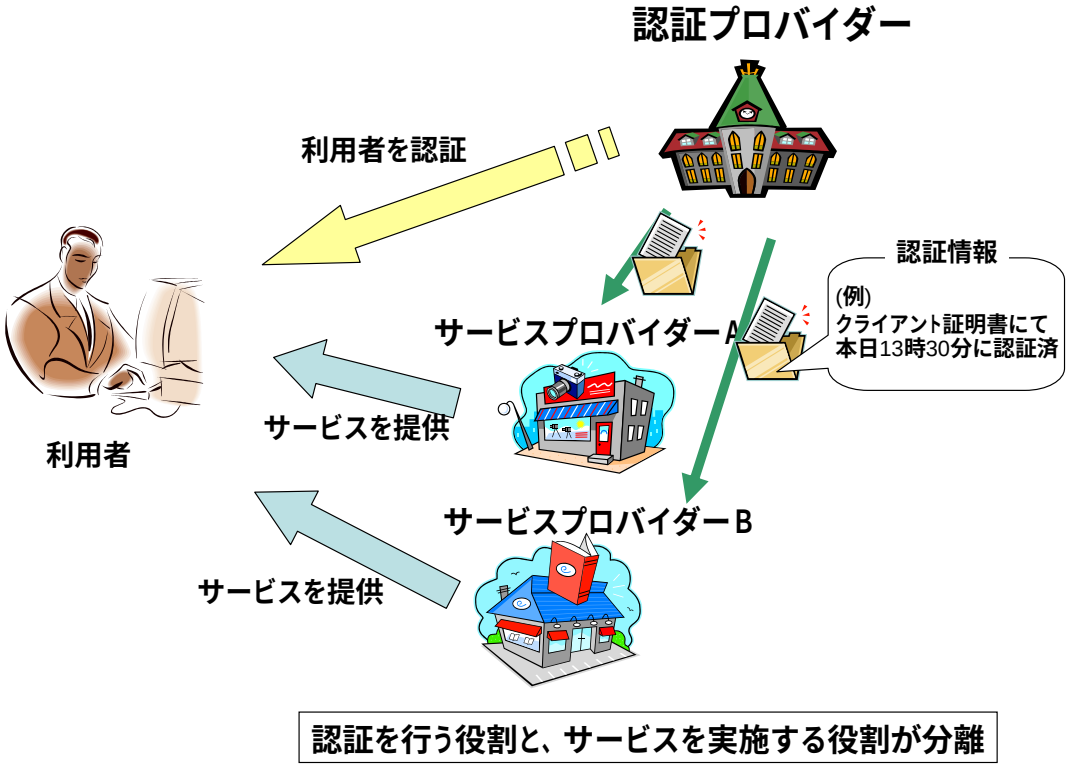


図 3.3　ID 連携による事業者モデル

SAML、Liberty、Shibboleth により実現可能となった ID 連携の仕組みは、単に利便性においてシングルサインオンを提供するという考えではなく、利用者に関する情報のセキュリティやプライバシー保護の観点にあることが重要である。利用者の情報が分散管理されることで情報漏洩時のリスクを抑えること、また、プライバシー保護の仕組みとして、利用者の同意のもとで ID 連携が行われることや、事業者間におけ

[1] 例えば Liberty の ID-WSF,ID-SIS 仕様で各事業者が持つ属性情報を連携するための仕組みを提供している。

る利用者の追跡を防ぐためにグローバルな ID を用いずに、それぞれの事業者だけに有効な ID（仮名の ID）を用いること等が考えられる。Liberty、Shibboleth のアーキテクチャについては 4.2 節、4.3 節で解説する。

認証システムの連携に関する標準化とその実用化の機運は世界的に高まっている。そして、このような ID 連携のモデルは、電子政府等にも取り入れられるような動向がある。米国電子政府においては、認証の連携を推進する e-Authentication イニシアチブが活発な活動を行っており、米国連邦政府ポータルにおいて e-Authentication イニシアチブが推進する認証の連携基盤が取り込まれようしている。また、米国では民間および官民における認証の連携を図る EAP（Electronic Authentication Partnership）が設立され、その基盤構築において認証の評価基準をはじめとする e-Authentication イニシアチブの成果を利用している。

e-Authentication イニシアチブの活動については 4.5 節で、EAP の活動については 4.6 節で紹介する。

3.3 認証の評価基準

認証に対するセキュリティレベルや保証レベルを向上し、さらに、サービスの連携を推進するためには認証の評価基準を明確にすることが重要である。

認証を必要とするネットワーク上のサービスを実施するためには、認証の脅威に対するリスクを分析し、適切な認証方法を適用することが求められる。

例えば、医療における患者情報等は機密度の高い情報であり、それを扱うサービスには高度の認証が求められなければならない。高度な認証を行うためには高いコストも要求される（図 3.4）。日本の電子署名法特定認証業務認定制度のように、認証局の認定における本人の身元確認や認証局の運用といった観点からの高度な要求を考えた場合、証明書発行コストは当然高いものとなる。一方、機密性の低いファイルをメンバー内で共有するといったサービスを考えた場合、そのサービスのためだけに高いコストをかけ、先の場合と同様の高度な認証を採用する必要性は考えにくい（図 3.5）。高度な本人確認性を必要以上に求めたためにコスト高になるだけでなく、普及を阻害することにもなる。

しかし、現状での様々なサービスにおいてはこのような認証にかかわるリスクを評価して適切な認証が行われているとは言いがたい。それは、認証の保証に関して明確な基準や指標が欠如していることがひとつの要因である。

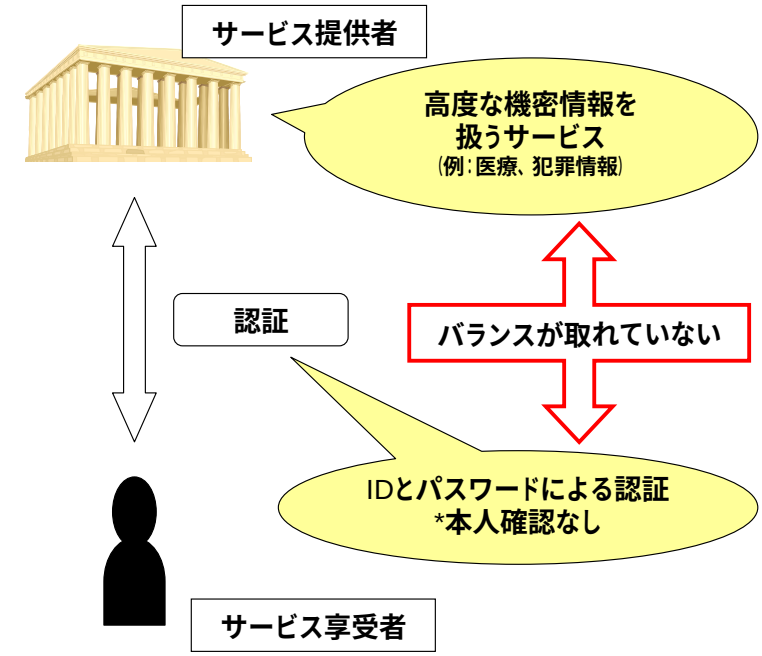


図 3.4　リスクと認証方法のバランス（1）

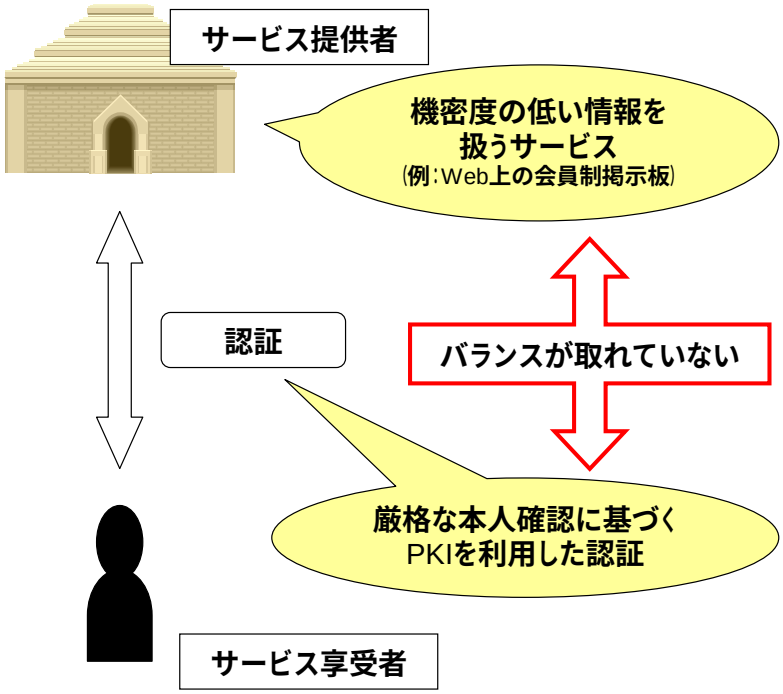


図 3.5　リスクと認証方法のバランス（2）

また、認証の評価基準の不備は、複数のサービスによる ID 連携を阻害する要因にもなりえる。これまでの認証が要求される多くのサービスは、サービス自身が認証を提供、つまりサービスと認証が一体化しており、そのため、サービスの数だけ認証シ

ステムが必要となっていた。こうした中、ID 連携によるシングルサインオンのモデルが注目されており、標準化等も急速に進展しており、電子政府等の認証基盤として取り入れようとする動きもある。

サービスと認証が一体化した従来型のモデルでは、認証の脅威に対するリスクは、一体化したサービスの主体者（サービスプロバイダー）自体が負えばよかった。一方、サービスプロバイダーと、認証の主体者、すなわち認証プロバイダーが個別に存在するモデルでは、サービスプロバイダーと、認証プロバイダー間で何らかの契約が必要である。その契約においては、認証に対するリスクを分析し、サービスに対して認証の保証レベルを適切に決定する必要があるだろう。

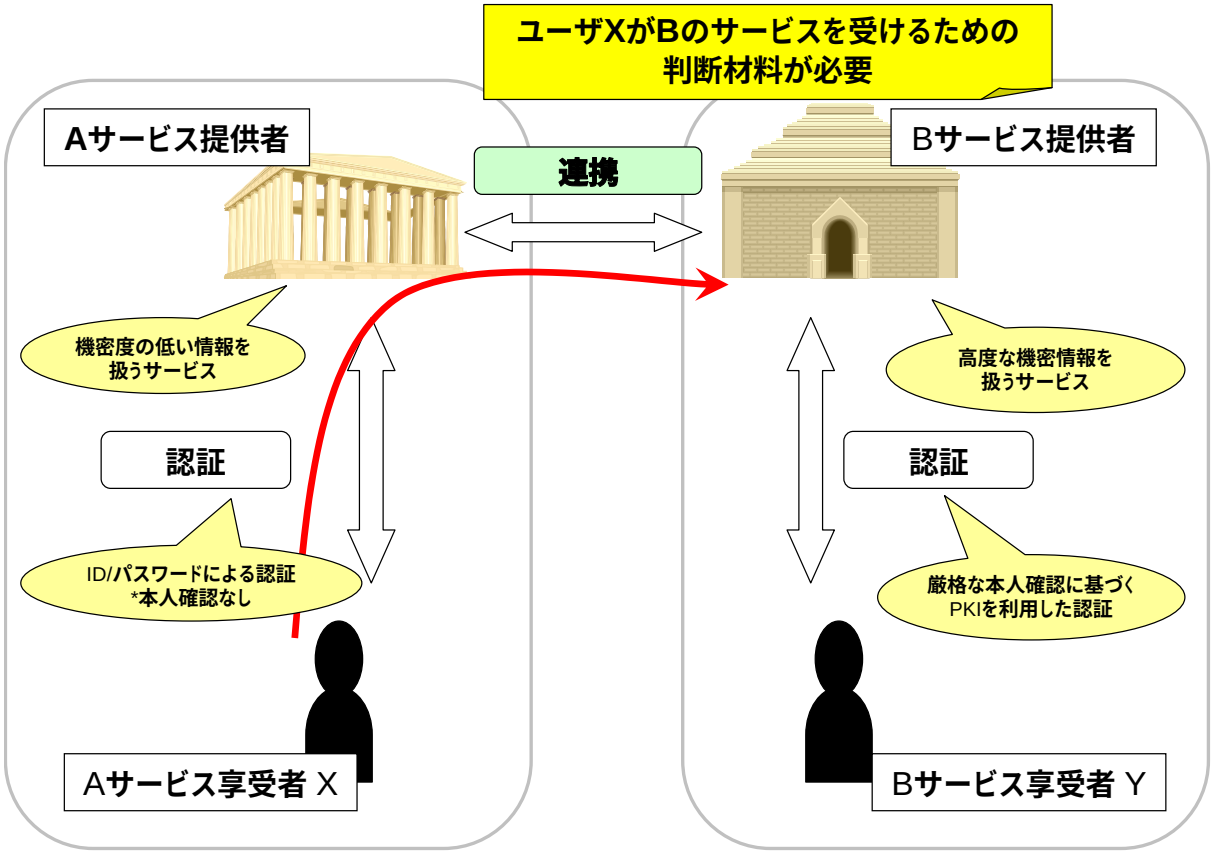


図 3.6　ID 連携と保証レベル

例えば、図 3.6 に示すように、A サービス提供者と B サービス提供者が ID 連携を行う場合を考える。A サービス提供者は自身の管理するサービス享受者 X を認証し、B サービス提供者に対してサービス享受者 X の認証結果を含んだ情報（アサーション）を発行する。B サービス提供者は A サービス提供者から得たアサーションによってサービス享受者 X へのサービス提供の認可を行う。A サービス提供者は B サービス提供者に対し認証プロバイダーとなる。このとき、A サービス提供者が認証するユーザの身元の保証と、B サービス提供者が認証するユーザの身元の保証は異なっているため、これらの認証におけるリスクを分析し、そのサービスで求められる認証の保証レベルを事前に決定する必要がある。

しかし、2 者間で多くの時間を費やし、認証に対するリスクを分析して設定したとしても、2 者間だけの連携で終わってしまう。また、もう少し範囲を広げ、業界内で

の規約や基準を作成したとしても、その業界内での連携に終わってしまう。

認証の評価基準が明確になっていれば、その評価基準を使うことにより、組織や業種を超えた認証の連携が推進されると考えられる。更に、認証プロバイダーや、サービスプロバイダーに対しての認定制度のようなものが確立すれば、異なった利害関係を持つ組織が、色々な場を共有するポータルが普及すると考えられる。

このような認証の評価基準について海外の動向を眺めると、米国の e-Authentication イニシアチブや EAP、連邦 PKI、また、オーストラリアの政府電子認証フレームワークでは、複数の保証レベルという考えがある。これらは、アプリケーションのリスクに応じた保証レベルの認証や電子署名を使い分けている。ユーザはアプリケーションの要求に応じて、クレデンシャル発行に高いコストが掛かる高い保証レベルから、比較的低いコストとなる低い保証レベルまで、適切な保証レベルの認証を利用することができる。

米国 e-Authentication イニチアチブでは保証レベルを 4 つにわけ、OMB 電子認証ガイダンスと NIST 電子認証ガイドラインにおいて、リスクを分析し保証レベルおよびその保証レベルを実現するための技術的要素を決定するプロセスを示している。これらの保証レベルについては 4.4 節で解説する。

4 事例調査

4.1 SAML

SAML（Security Assertion Markup Language）とは OASIS （Organization for the Advancement of Structured Information Standards）で策定された、認証/属性/認可といったセキュリティ情報を要求/応答するためのプロトコルである。

2002 年 11 月に version1.0 が、2003 年 9 月には version1.1 が OASIS 標準となった。さらに、Liberty Alliance の ID-FF や、Internet2 プロジェクトの成果である Shibboleth といった認証システムの仕様が取り入れられた SAML2.0 が標準化の最終フェーズにある（2005 年 2 月現在）。

SAML の基本的な概念モデルを図 4.1 に示す。

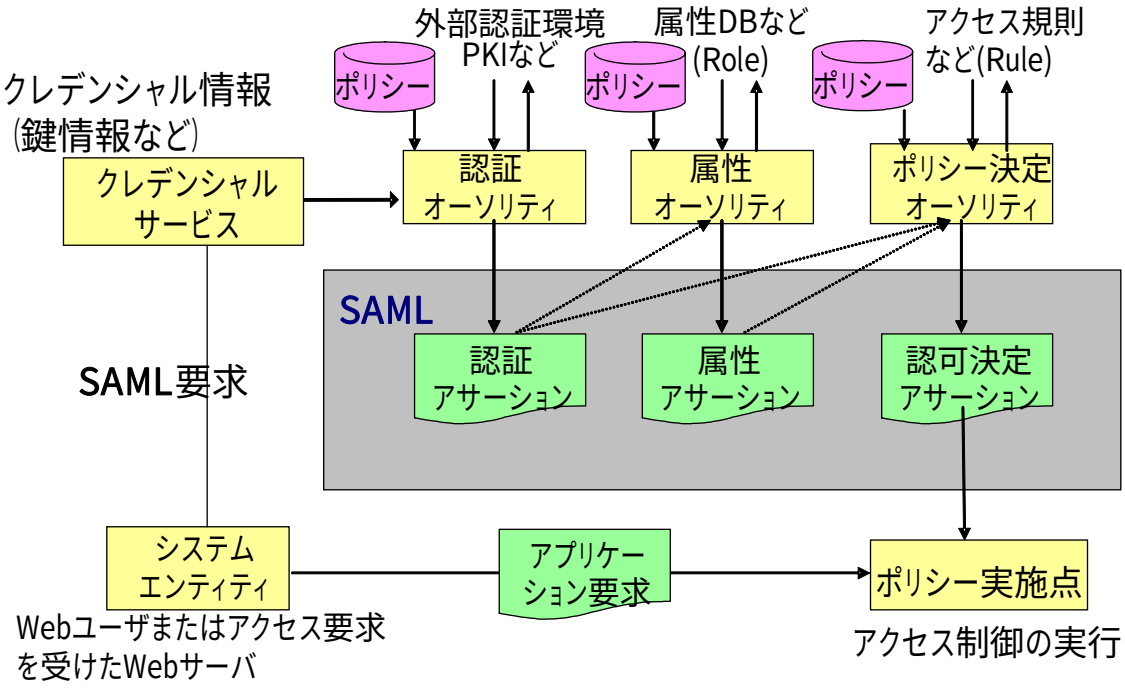


図 4.1 SAML 概念モデル

この概念モデルが示すように、SAML では、認証を行う認証オーソリティ、属性情報を提供する属性オーソリティ、認可決定を行うポリシー決定オーソリティを分け、これらを用途に応じて柔軟に配置することが可能である。従来の Web アプリケーションのアクセスコントロールでは、認証を行う役割とアクセスの認可決定を下す役割は一致しているものであった。SAML の認証、属性、認可のオーソリティという考え方によって、利用者の認証を行い、その利用者に関する属性情報を提供する認証プロバイダーと、その認証プロバイダーからの認証情報や属性情報を取得することでサービスだけを提供するサービスプロバイダーを実現することも可能になる。

SAML は認証そのものの技術とは独立した仕様となっている。認証方法を特定しないため、ID/パスワード認証から PKI のクライアント認証等様々な認証方法を適用することが可能である。利用者の認証の後に発行される認証アサーションには主に、ど

んな方法で利用者を認証したか（PKI、ID/パスワード等）を記述するが、利用者の ID 情報そのものを記述する必要はない。そのため、利用者のプライバシーを保護した形でアサーションを提供することが可能である。

シングルサインオンを実現する認証システムである Shibboleth や Liberty ID-FF は SAML をベースとした仕様となっている。これらの仕様については、4.2 節、4.3 節で紹介する。

4.2 Liberty Alliance Project

4.2.1 Liberty の概要

Liberty Alliance project（Liberty）は、2001 年 9 月に設立され、インターネット上において新しい形態での協業、商取引、通信を推進するために結成されたビジネスアライアンスである。2005 年 1 月現在、世界で 160 を超える企業や団体が参加している。Liberty では、企業間のビジネス統合や、組織間の人的交流が進む中で、これまで個別に管理してきたアイデンティティの連携や統合を実現するためのオープンな標準仕様を策定している。Liberty の仕様は、広範なネットワークアイデンティティをベースとしたコミュニケーションの支援を行い、企業に以下のことを提供する。

- 顧客およびビジネスパートナーとの関係を経済面において強化する新しい収益の機会の基盤
- 企業が顧客に対してインターネットに接続されたデバイスを使用する場合の選択肢、利便性、制御性を提供できるようなフレームワーク

Liberty の組織体制はマネジメントボードをトップに、5 つのグループが活動しており、それぞれの成果が参加メンバーに提供されるというものである。

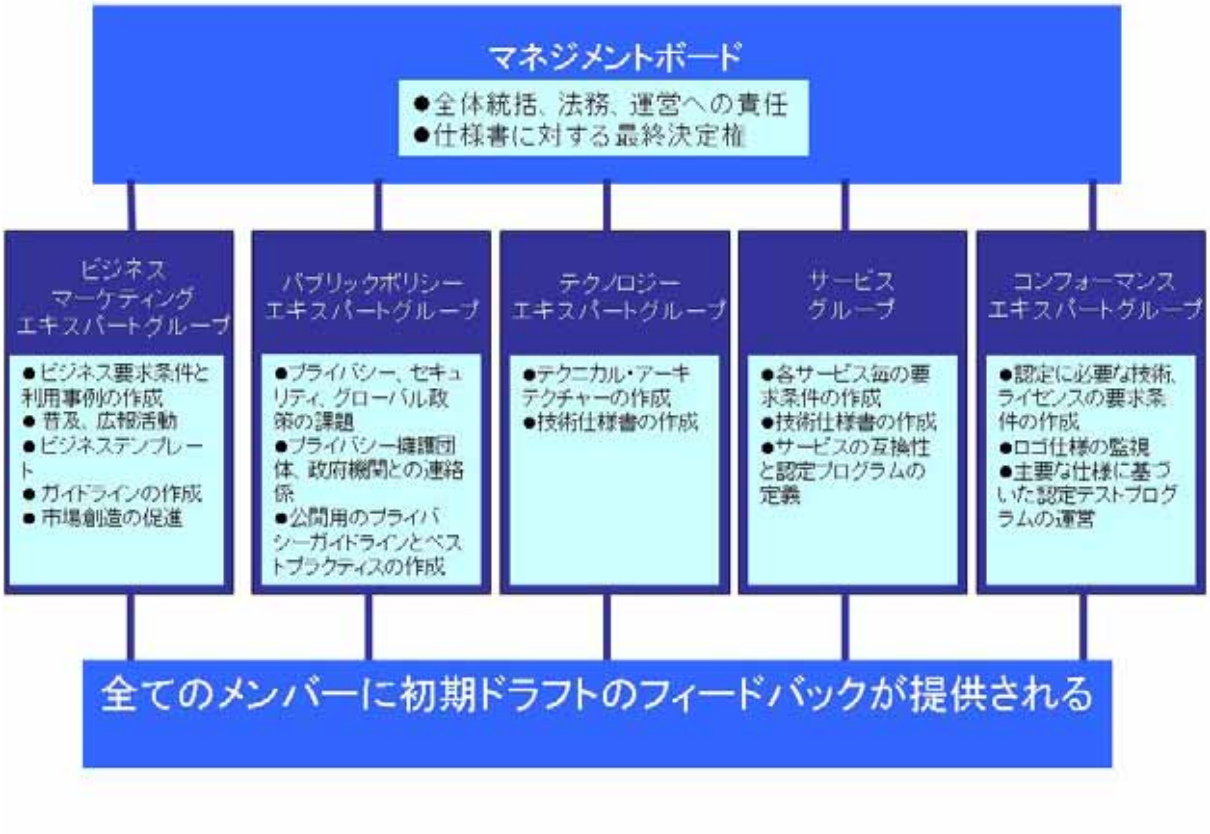


図 4.2 Liberty の組織体制

Liberty では以下のようなロードマップで様々な技術仕様を策定している。

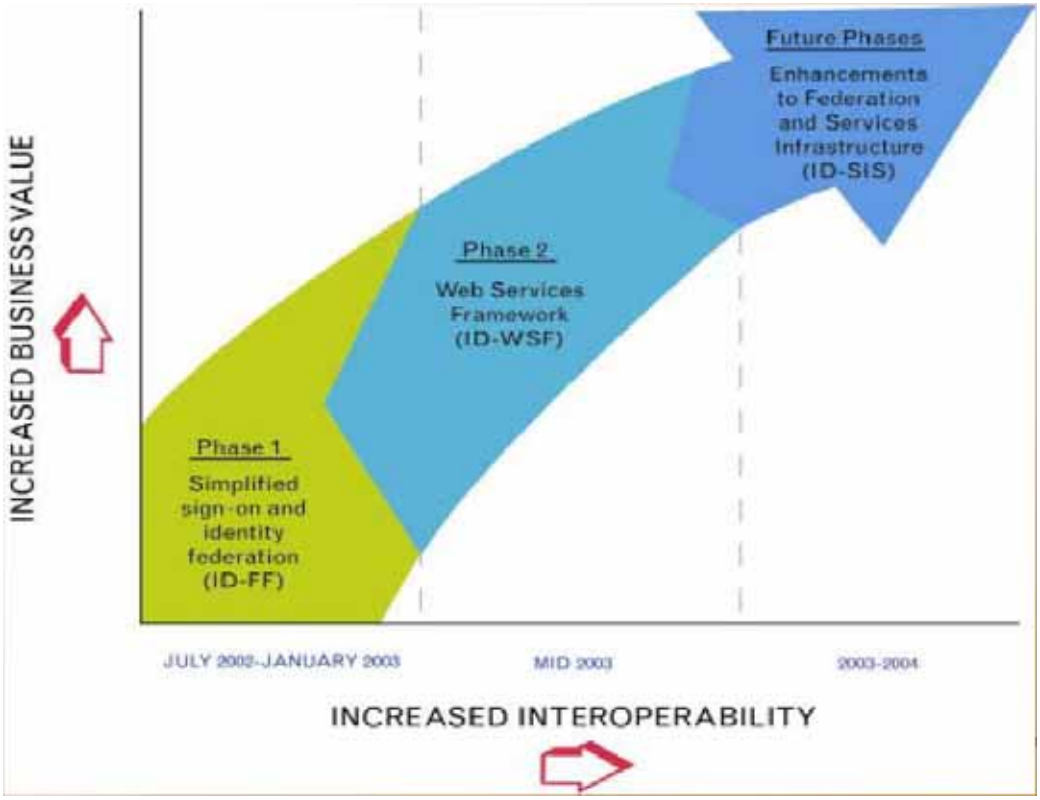


図 4.3　Liberty のロードマップ図

図 4.3 の各フェーズの内容について述べる。

- フェーズ 1　ID-FF（Identity Federation Framework）
  アイデンティティ連携とシングルサインオン技術の基盤仕様
  OASIS（Organization for the Advancement of Structured Information Standards） SSTC（Security Services Technical Committee）で策定された SAML（Security Assertion Markup Language）を拡張した認証情報の交換プロトコルや XML スキーマ定義、トランスポート層に対するバインディング方法を規定している。

- フェーズ 2　ID-WSF（Identity Web Services Framework）
  Web サービスによる個人情報の管理や交換に関する基盤仕様
  相互接続可能なアイデンティティサービスや個人の許諾に基づく属性情報の共有を構築するためのフレームワークである。

- フェーズ 3　ID-SIS（Identity Services Interfaces Specifications）
  上記 ID-WSF 上に構築する個人情報に関する基本サービスの仕様
  本フレームワークには、基本的仕様と具体的な基本サービスの仕様が含まれる。具体的な基本サービスとして、プレゼンスサービス、位置情報サービス、アドレス帳サービスが検討されている。

策定された仕様を元に実装したシステムの相互接続性を確認するコンフォーマン

ステストでは、2004 年 10 月に ID-FF、ID-WSF が行われており、仕様策定だけでなく実装化も進んでいる。市場への展開としては、ID-FF が 2003 年から 2005 年末ぐらいを想定しており、ID-WSF が 2004 年から 2007 年ぐらいを想定している。

Liberty は、2003 年 11 月に ID-FF v1.2 と ID-WSF v1.0 の仕様群を公開しており、現在は ID-FF と ID-WSF の更新、さらに ID-SIS の仕様作成を進めている。図 4.4 では ID-FF、ID-WSF、ID-SIS の関係図を示している。Liberty の仕様群は、SAML を拡張しているだけでなく、他の様々な仕様（SOAP，WSS，XML）を広く取り入れているのがわかる。また ID-FF は、ID-WSF、ID-SIS の 2 つの仕様とレイヤーが異なり、比較的独立な仕様である。

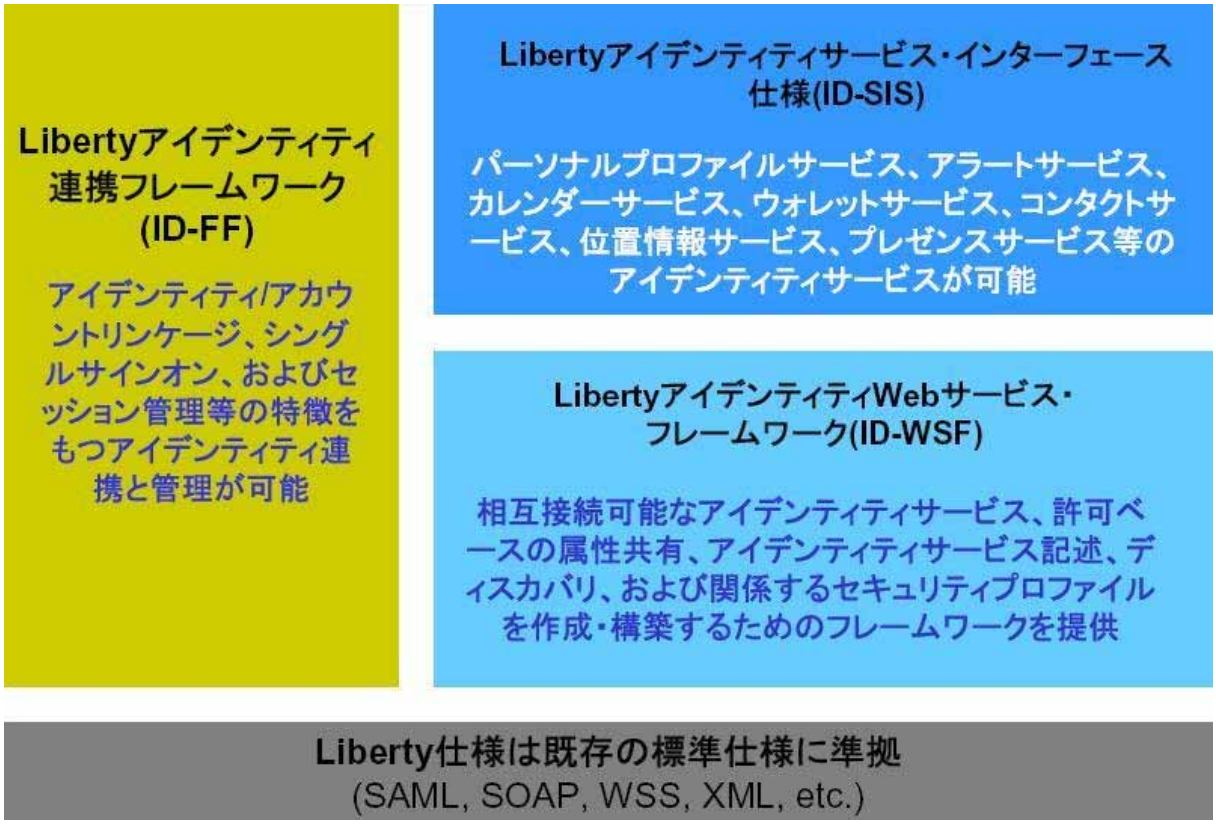


図 4.4　Liberty 技術フレームワークの図

次に Liberty ID-FF 1.2、ID-WSF 1.0 が他の仕様とどのような関係であるかを示す。

Federation の仕様には、SAML1.1 をベースにした Liberty ID-FF 1.2 と Shibboleth 1.2 の 2 つの仕様があり、他に WS-Federation の仕様がある。Federation の各仕様は、ネットワークとトランスポートの仕様群、XML とそのセキュリティの仕様群を前提に策定されている。また Identity Services は、Federation の仕様をベースに策定されている。

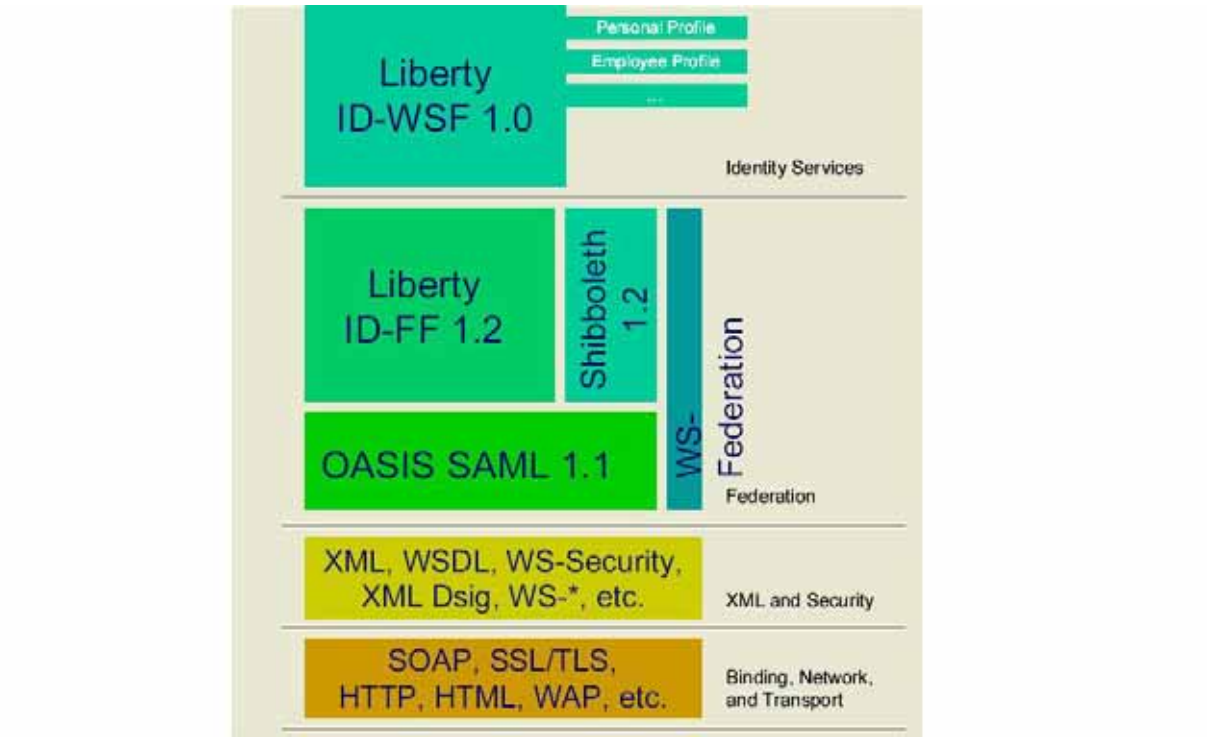


図 4.5　Liberty と関連仕様との関係図-1

4.2.2 Liberty のモデル

本節では Liberty の概要を理解するために必要なモデルについて説明する。

(1) アイデンティティとは

Liberty ではアイデンティティとは属性、認証、認可の 3 つから構成されており、「個人を特徴付ける属性情報の集合」と定義している。アイデンティティの情報とは、個人の名前、住所、電話番号、メールアドレス、クレジットカード番号、パスワード、パスポート、口座番号等、個人を特定するのに必要な情報を示す。さらに個人の嗜好（趣味、食べ物の好み等）や、履歴（購入履歴、医療履歴等）の比較的広い範囲の情報も含んでいる。またアイデンティティは、個人を特定し、その個人の属性情報の交換や、特定の属性に対してアクセス権の付与に必要な重要な情報である。Liberty では、アイデンティティがネットワーク上で安全に流通すべきものと想定しており、ネットワーク上を流通するアイデンティティを特に「ネットワークアイデンティティ」と呼んでいる。

アイデンティティは、ネットワークが発達した現在、ネットワークを通じて容易に交換することが可能であり、そのため個人のプライバシーが侵害される危険性が

ある。Liberty ではアイデンティティを確実に技術的に保護すべきとしており、アイデンティティの情報が個人の許諾に基づいて安全に流通する基盤を提供することを目的としている。

(2) Liberty アーキテクチャ

図 4.6 は Liberty の基本的なアーキテクチャを示している。Liberty のアーキテクチャは、3 つのエンティティと関連する 3 つアーキテクチャのコンポーネントから構成されている。

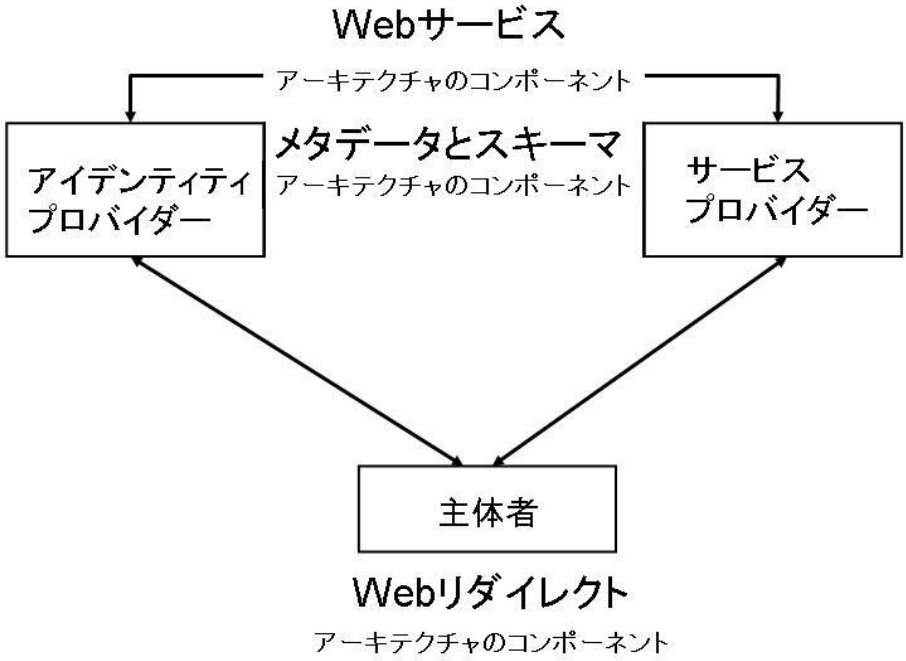


図 4.6　Liberty のアーキテクチャ図

・ 主体者（Principal）
アイデンティティを取得しており、認証結果を元に判断・決定・実施することが可能なエンティティ。ユーザ、グループ、企業、その他法人等を意味する。

・ サービスプロバイダー（Service Provider）
主体者にサービスや商品を提供するエンティティ。主体者を認証する基盤を有しておらず、アイデンティティプロバイダーにアウトソーシングしている。認証結果およびセキュリティポリシーを元に、主体者に対して特定の情報やサービスを提供する。

・ アイデンティティプロバイダー（Identity Provider）
主体者のアイデンティティ情報を生成、保管、管理し、主体者の認証を他のサ

ービスプロバイダーに提供するエンティティ。SAML の認証オーソリティ（Authentication Authority）が内部またはバックエンドに存在する。認証方式に関しては規定がなく、どの技術を採用してもよいし、既存認証基盤であってもよい。

主体者、サービスプロバイダー、アイデンティティプロバイダー以外に、Liberty では Liberty 対応クライアントまたはプロキシー（LECP）が定義されている。

・ Liberty 対応クライアント（LEC）
アイデンティティプロバイダーに関する情報を保持しており、Liberty が規定するプロトコルに従ったメッセージの送受信が可能で、SOAP による POST が可能な HTTP クライアント。

・ Liberty 対応プロキシー（LEP）
Liberty 対応クライアントをエミュレートする HTTP プロキシーである。WAP ゲートウェイが典型的なものである。

(3) トラストサークル

トラストサークルはサービスプロバイダーとアイデンティティプロバイダーの連携を示している。トラストサークル内では、サービスプロバイダーとアイデンティティプロバイダーがビジネス面と運用面において事前に合意を取り交わしており、主体者が安全でシームレスな商取引が可能である。

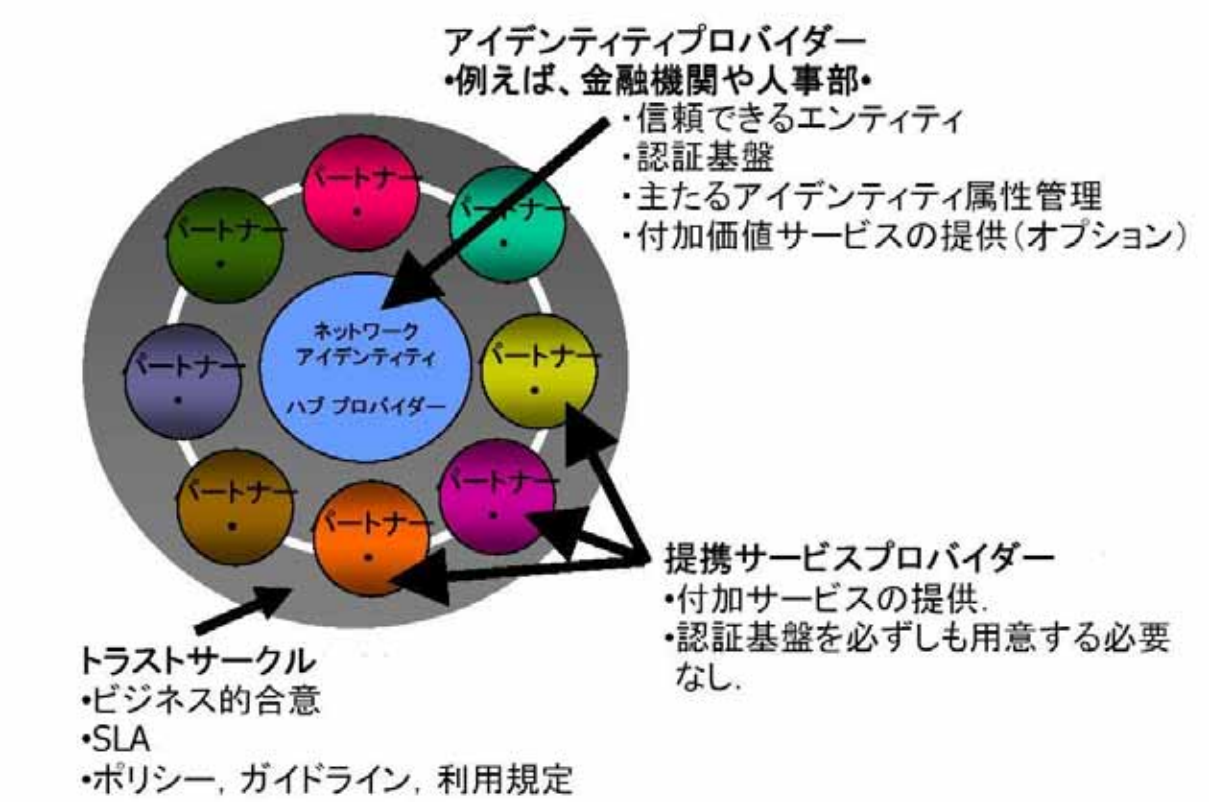


図 4.7　トラストサークル

Liberty では、主体者がアイデンティティプロバイダーにおいて一度認証されると、別のサイトで再度認証することなくアクセス可能であること（シングルサインオン）を実現する。シングルサインオンはトラストサークル内において可能である。さらにトラストサークルのアイデンティティプロバイダーと他のトラストサークルのアイデンティティプロバイダーの間においてビジネス上の合意に基づき信頼関係が成立していれば、トラストサークルを超えたシングルサインオンが可能である。

Liberty では、主体者にシングルサインオンを提供するだけでなく、シングルログアウトも提供する。シングルログアウトとは特定のアイデンティティプロバイダーによって認証されたセッションに対して一括してログアウトするものである。

(4) Liberty におけるアイデンティティ連携

アイデンティティ連携とは、個々に独立して管理されたアイデンティティを互いに関連づけることである。サービスプロバイダーはアイデンティティプロバイダーとアイデンティティを連携することにより、認証をアイデンティティプロバイダーにアウトソーシングすることが可能となる。複数のサービスプロバイダーがアイデンティティプロバイダーに認証をアウトソーシングすることで、主体者はシングルサインオンの利便性を受けることができる。ただし Liberty では、主体者の個人情報を 1 箇所に集中管理する必要がないとしており、サービスプロバイダーが複数のアイデンティティプロバイダーと連携することを想定している。

(5) 仮名

Liberty のアイデンティティ連携では、ある主体者に関して、プロバイダーが参照する際に、仮名（Pseudonyms）による名前識別子（Name Identifier）を用いる。名前識別子は、ある主体者を確認可能とするためのもので、主体者を信頼しているサービスプロバイダーまたはアイデンティティプロバイダーによって割り当てられた任意の名前である。互いに信頼しあう主体者やサービスプロバイダー、アイデンティティプロバイダー同士で共有しており、その主体者やサービスプロバイダーやアイデンティティプロバイダー同士でのみ意味を持つ。

仮名を利用することで、プロバイダーは、自身が管理している主体者のアイデンティティを通信相手のプロバイダーに対して公開せず、主体者に対してサービスの提供を可能とする。これによりプロバイダー同士が協業しても主体者を特定できない仕組みとなっている。

4.2.3 ID-FF

ID-FF は、Liberty の Federation に関する仕様群であり、OASIS の標準仕様 SAML を元にしたシングルサインオンや認証情報の交換に関する認証の枠組みを規定している。また SAML の拡張として新たに名前登録やシングルログアウト等についても規定している。

(1) プロトコルとプロファイル

Liberty ID-FF ではプロトコルとスキーマに関して次の内容を規定している。

- プロトコル
  Liberty に必要なプロトコル（要求／応答メッセージ）と XML スキーマを規定している。また各プロバイダーが受信した際の処理規則についても規定している。
- プロファイル
  プロトコル上必要となる具体的なトランスポート・バインディングとプロファイルを規定している。現在 HTTP、SOAP over HTTP 等がある。

プロトコルとプロファイルに関しては次の 7 つの仕様から構成されている。

- Single Sign-on and Federation
  アイデンティティプロバイダーとサービスプロバイダーにおいて連携確立後に、主体者がアイデンティティプロバイダーに一度サインオンすることで再度認証することなく、サービスプロバイダーを利用できる仕組み。

- Name Registration
  サービスプロバイダーとアイデンティティプロバイダーが主体者に関して互いに通信する際に利用する名前識別子を変更する仕組み。

- Federation Termination Notification
  サービスプロバイダーとアイデンティティプロバイダーが、主体者に関して確立していた連携を解除する仕組み。

・ Single Logout
アイデンティティプロバイダーによって認証された主体者のすべてのセッションを一括してログアウトする仕組み。

・ Identity Provider Introduction
サービスプロバイダーとアイデンティティプロバイダーで、主体者がどのアイデンティティプロバイダーを利用しているか検索する仕組み。

・ Name Identifier Mapping
サービスプロバイダーが主体者を示す名前識別子を入手する仕組み。

・ Name Identification Encryption
暗号化する仕組み。

次に「Single Sign-on and Federation」の例として、「Browser POST プロファイル」、「Browser Artifact プロファイル」、「LECP プロファイル」の 3 つのプロファイルについて説明する。

(a) Browser POST プロファイル

認証アサーションをブラウザによりサービスプロバイダーに送る方式である。アイデンティティプロバイダーとサービスプロバイダーの直接のやりとりが不要である。

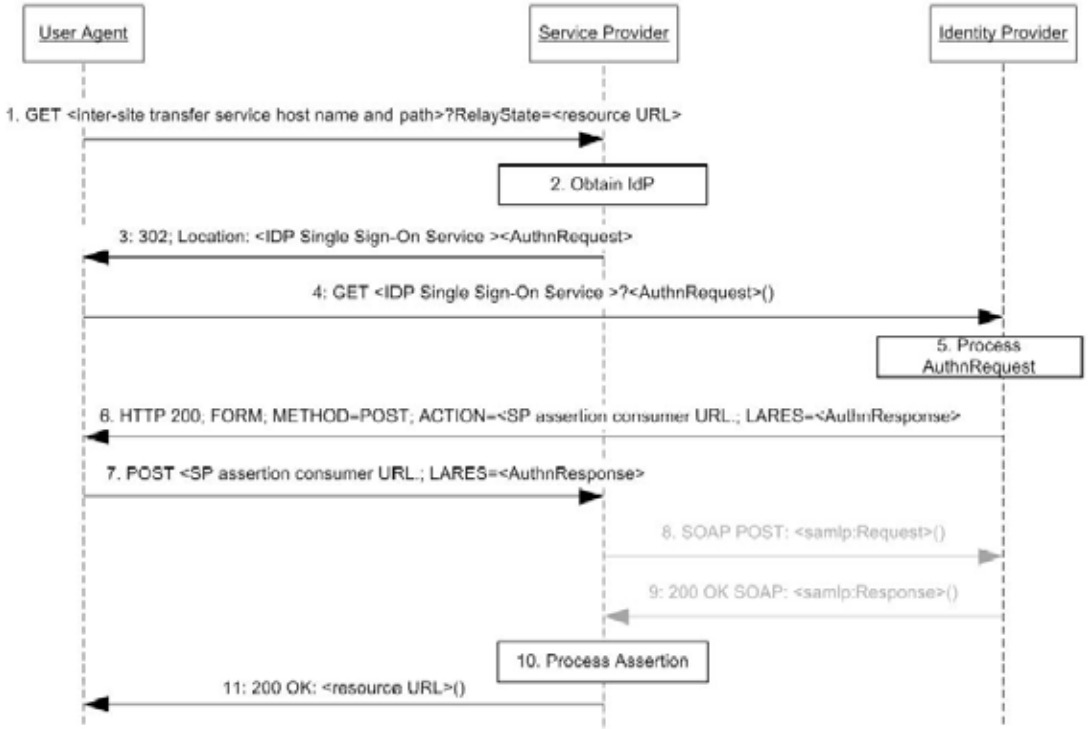


図 4.8　Browser POST プロファイルのシーケンス図

1. ユーザエージェントからサービスプロバイダーに対してアクセスする。
2. サービスプロバイダーはアイデンティティプロバイダーのアドレスを入手し、ユーザエージェントに返信する。
3. サービスプロバイダーはエージェントに対してアイデンティティプロバイダーのシングルサインオンサービスの URL に<lib:AuthnRequest>を埋め込んでリダイレクションメッセージを返信する。
4. ユーザエージェントは、アイデンティティプロバイダーのシングルサインオンサービスにアクセスする。
5. アイデンティティプロバイダーのシングルサインオンサービスは、認証要求メッセージを受信し、シングルサインオンサービスの処理を実行する。
6. アイデンティティプロバイダーはユーザエージェントの認証アサーションを発行し、HTML のフォームに格納し、HTTP 200 の返信メッセージとして返送する。
7. ユーザエージェントは、6.で受信した返信内容を含めたフォームをサービスプロバイダーに HTTP POST で送信する。
8. 不要
9. 不要
10. サービスプロバイダーは受信したアサーションの正当性を確認する。
11. サービスプロバイダーはユーザエージェントに 1.でのアクセス要求に対する返信をする。

(b) Browser Artifact プロファイル

認証アサーションをブラウザから送信するのではなく、SOAP を用いてアイデンティティプロバイダーとサービスプロバイダー間でやりとりする方式である。ブラウザを用いてシングルサインオンを実現するため、一般的に利用されるプロファイルである。

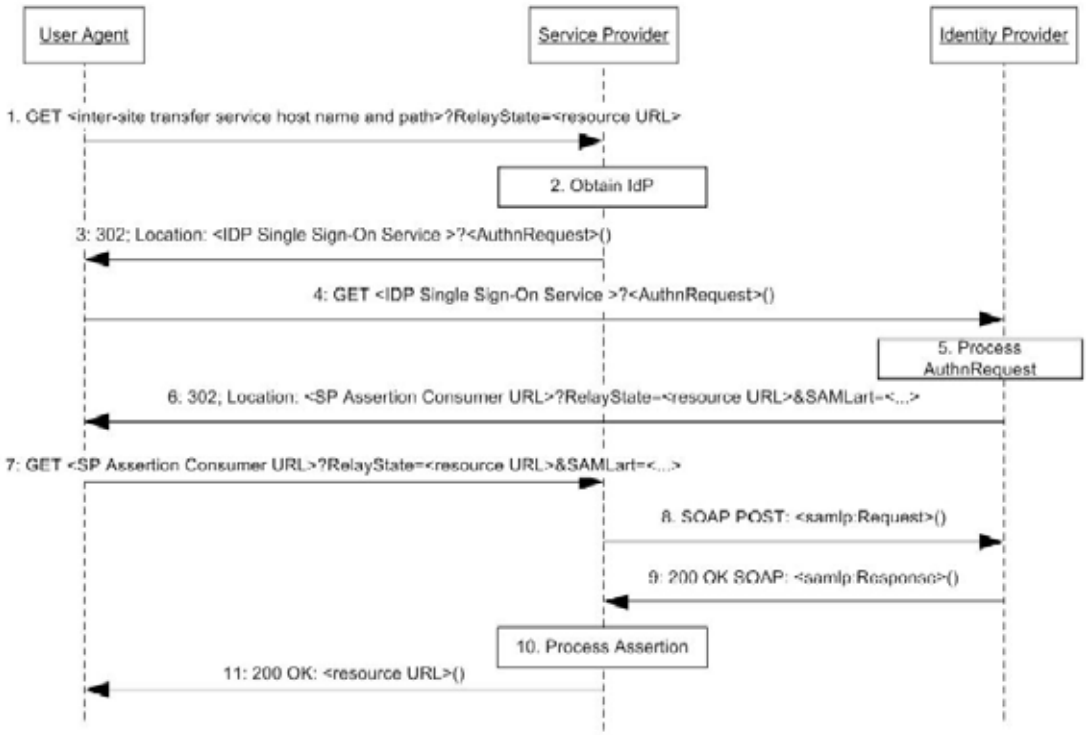


図 4.9　Browser Artifact プロファイルのシーケンス図

1. ユーザエージェントからサービスプロバイダーに対してアクセスする。
2. サービスプロバイダーはアイデンティティプロバイダーのアドレスを入手し、ユーザエージェントに返信する。
3. サービスプロバイダーはユーザエージェントに対してアイデンティティプロバイダーのシングルサインオンサービスの URL に <lib:AuthnRequest>を埋め込んだリダイレクションメッセージを返信する。
4. ユーザエージェントは、アイデンティティプロバイダーのシングルサインオンサービスにアクセスする。
5. アイデンティティプロバイダーのシングルサインオンサービスは、認証要求メッセージを受信し、シングルサインオンサービスの処理を実行する。アイデンティティプロバイダーはアーティファクトとアサーションを作成する。
6. アイデンティティプロバイダーはアサーションを付加して、ユーザエージェントに返信する。
7. ユーザエージェントは、アーティファクトを含むメッセージをサービスプロバイダーにリダイレクションする。
8. サービスプロバイダーはアイデンティティプロバイダーに対して認証アサーション要求の SOAP メッセージを送信する。
9. アイデンティティプロバイダーは認証アサーションを SOAP メッセージに格納して返信する。
10. サービスプロバイダーは受信したアサーションの正当性を確認する。

11. サービスプロバイダーはユーザエージェントに 1.でのアクセス要求に対する返信をする。

(c) LECP プロファイル

LECP は、Liberty 対応クライアント（LEC）またはプロキシー（LEP）と、サービスプロバイダー、アイデンティティプロバイダー間のやりとりを指定する。このプロファイルは、携帯電話等での利用が想定されている。

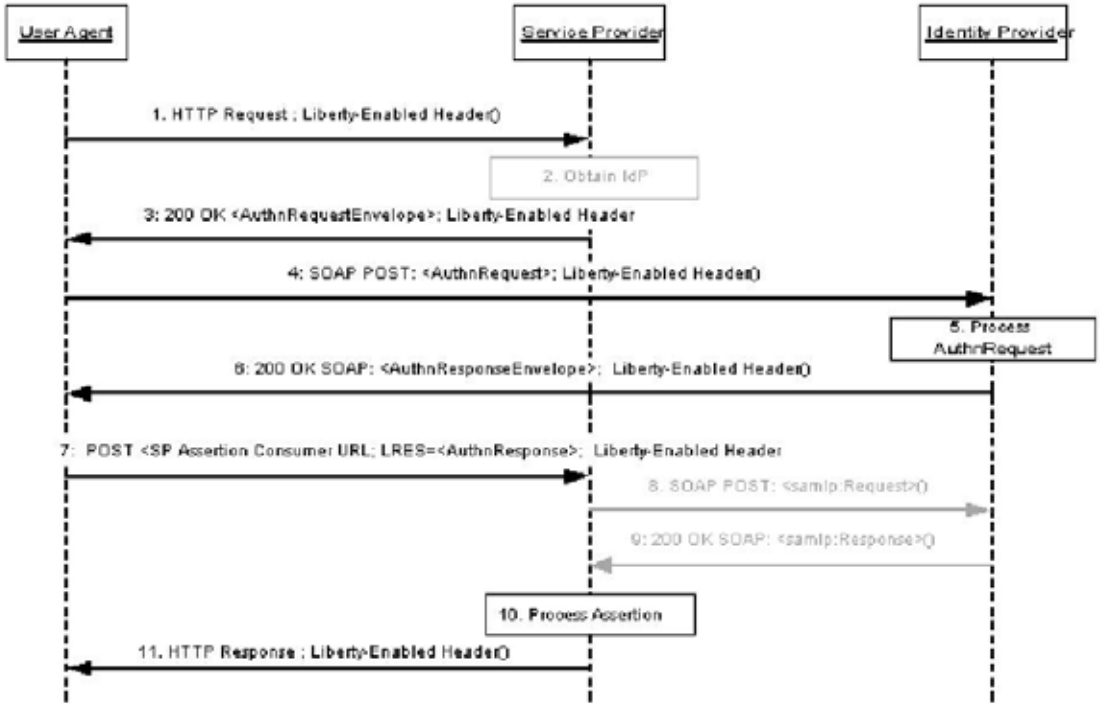


図 4.10　LECP プロファイルのシーケンス図

1. ユーザエージェントは、サービスプロバイダーに対して自らが「Liberty 準拠」であることを示すヘッダ（Liberty-Enabled Header）情報を付加して HTTP 要求を送信する。
2. 不要。LECP ではアイデンティティプロバイダーの所在等のメタ情報を事前に保持している。
3. サービスプロバイダーは、上記 Liberty 準拠ヘッダを受け取ると、返信においても Liberty 準拠ヘッダを加えて、メッセージを返信する。ここでサービスプロバイダーはアイデンティティプロバイダーリストを加えてもよい。
4. LECP は、適当なアイデンティティプロバイダーを決めて認証要求の SOAP メッセージをアイデンティティプロバイダーのシングルサインオンサービスの URL に対して送信する。
5. アイデンティティプロバイダーのシングルサインオンサービスは認証処理を行う。
6. アイデンティティプロバイダーは SOAP メッセージを LECP に対して返

信する。

7. LECP は受信した<lib:AuthnResponseEnvelope>を元に、認証要求に対する返信の SOAP メッセージをサービスプロバイダーに対して送信する。
8. 不要
9. 不要
10. サービスプロバイダーは受信したアサーションの正当性を確認する。
11. サービスプロバイダーは LECP に対して、ステップ 1.での要求に対する返信をする。

4.2.4 Liberty の状況

本節では、仕様に関連した内容として、「SAML との関係」と「Liberty の規定範囲外の項目」、「コンフォーマンス」について述べる。そして Liberty 適用に関する考察や動向等についても述べる。

(1) SAML との関係

Liberty ID-FF 1.2 は、SAML1.1 を基に拡張を行ったものである。ID-FF の開発者にとっては、SAML スキーマと、SAML を拡張したスキーマの両方を理解しなければならない。また Liberty ID-FF は、SAML で規定している属性オーソリティや認可決定オーソリティの概念が規定されていないため、実際には SAML のモデルをすべて網羅したものではない。これら 2 点から、Liberty は 2003 年 11 月に OASIS SSTC に対して次期の SAML2.0 に対して ID-FF 1.2 の仕様群と、Errata（正誤表）文書を提供することを申し入れ、受理された。Liberty は OASIS SSTC に仕様群を提供することで、SAML2.0 に Liberty の成果を反映した。

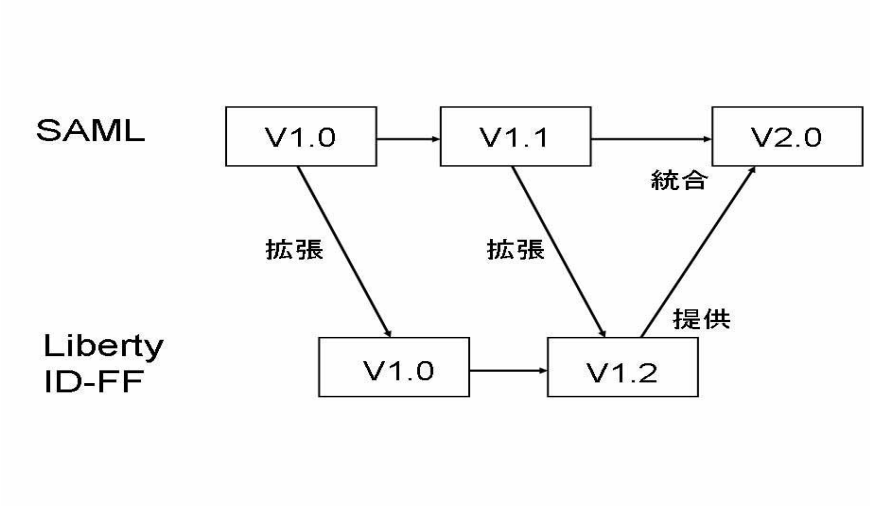


図 4.11　SAML と Liberty の仕様の関連図

SAML2.0 が、SAML1.0 をベースに Liberty や次の節で述べる Shibboleth の仕様を吸収することで、Federation の仕様群の関係は図 4.5 から図 4.12 のように変化する。SAML2.0 のコンフォーマンスに関しては、2005 年 2 月の RSA Conference 2005 において 13 社の参加によるデモンストレーションが行われている。このよう

にベンダーによる SAML2.0 の実装化が進んでいる。

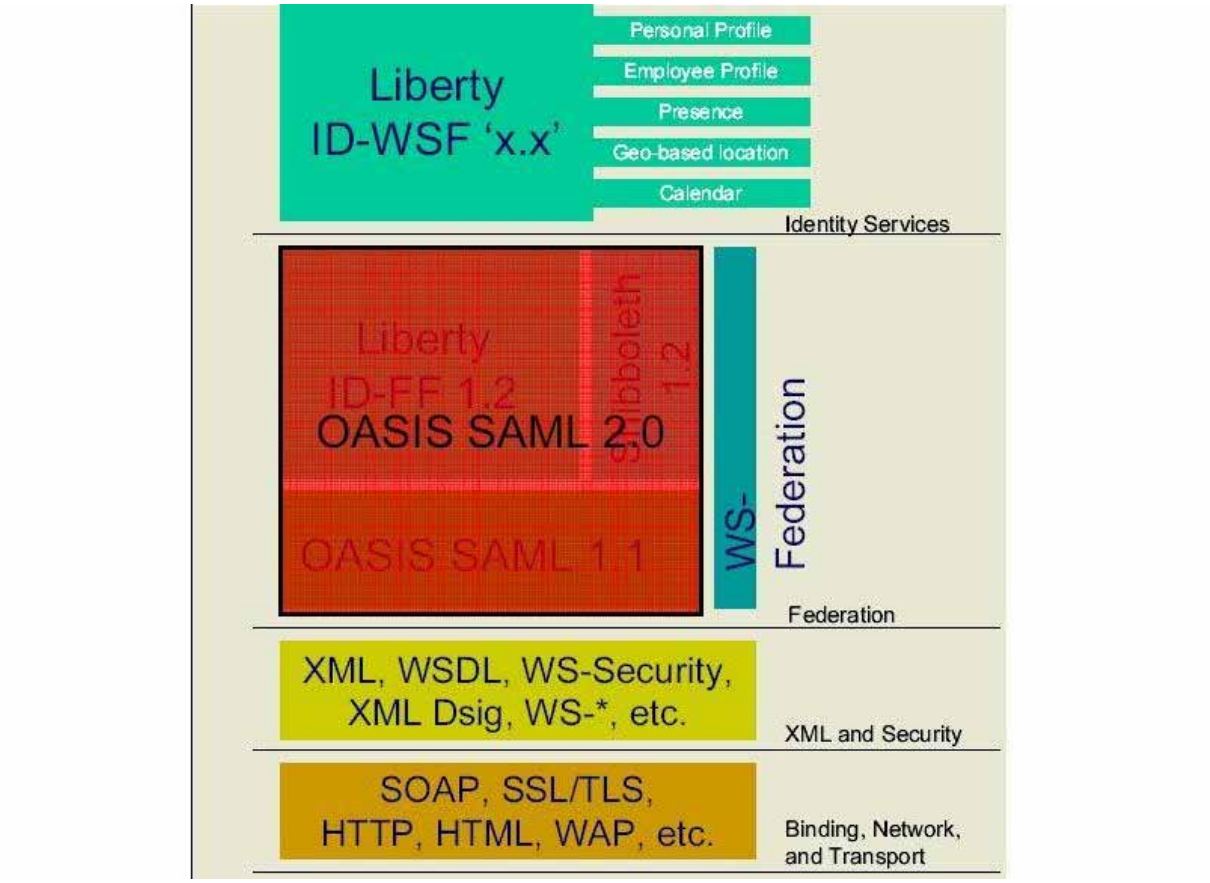


図 4.12　Liberty と関連仕様との関係図-2

(2) Liberty の規定範囲外の項目

Liberty では、アイデンティティ連携システムの構築に必要となるすべての技術を規定していない。Liberty のアイデンティティ連携システムでは、広範囲の技術領域を網羅せず、他の標準仕様を広く取り込んでいる。他の標準仕様については、Liberty の仕様内で解説せず参照のみを示しているため、前提知識の扱いとなる。そのため Liberty をすぐに理解することは容易ではない。参照されている仕様は、SAML、WS-Security、WDSL、HTTP、XML Encryption、XML Signature 等がある。

また Liberty では Liberty の普及の障害とならないように、実装に関する詳細な部分について規定していない。実装を詳細に規定しないことで、実装者が他の実装者と差別化できるように柔軟性や独自性を損なわないようにしている。ただし実装はコンフォーマンステストにおいて他の 2 つ以上の実装と接続できないと Liberty の認定が取得できない。そのため実装者は規定内容を十分満たした実装を行わなければならない。

Liberty において規定外の 4 つの項目を示しておく。

(a) 認証方式

Liberty では SAML 同様に認証連携に関するプロトコル・プロファイルについて規定しているが、認証方式に関して規定していない。SAML では、認証アサーションに主体者を認証した認証方式が記述可能であり、次の認証方式の URL が規定されている。

- パスワード
- Kerberos
- セキュアリモートパスワード
- ハードウェアトークン
- SSL/TLS 証明書ベースクライアント認証
- X.509 公開鍵
- PGP 公開鍵
- SPKI 公開鍵
- XKMS 公開鍵
- XML デジタル署名

Liberty のアイデンティティプロバイダーは、上記の認証方式を処理するシステムがバックエンドに存在していることを前提にしている。ただしすべての認証方式をサポートする必要はない。

(b) セッション管理

Liberty ではシングルサイトにおけるセッション管理方法は、実装上の課題として扱われており規定していない。しかし実装では、シングルサイトでのユーザ認証を行うための機構が必要である。その手段としては、次のようなものが考えられる。

- クッキーの利用
- セッション情報についての URL
- HTTP の POST の利用
- ハードウェアトークンの利用
- ユーザによるパスワード入力

(c) セキュリティポリシー

サービスプロバイダーやアイデンティティプロバイダーは、一般的にそれぞれセキュリティポリシーを持っており、そのセキュリティポリシーはドメイン内のセキュリティポリシーと関係している。そのため Liberty のシステム設計や実装方法は、トラストサークルや各プロバイダーのセキュリティポリシーに関係する。しかし Liberty では、アクセス制御やプライバシーに関するポリシーについて具体的に規定していない。そのため実際にアイデンティティプロバイダーとサービスプロバイダーの組織が異なる場合、4.6 節で解説する EAP 等を用いてポリシーを構築する必要がある。

(d) アサーション・アーティファクトの管理

Liberty では、SAML と同様にアサーションやアーティファクトのスキーマやプロファイルについて規定しているが、アサーションやアーティファクトの管理方法について規定しておらず実装依存となっている。たとえば携帯電話を想定す

ると、ユーザ数は何千万のオーダーになることからアイデンティティプロバイダーがアサーションやアーティファクトを大量に発行することが予想され、システムが高負荷になることが考えられる。そのためアサーション、アーティファクトの管理は、実装を行う上で重要な項目であると考えられる。

(3) コンフォーマンス

Liberty のコンフォーマンステストは、次の 4 つのプロファイルから構成されており、プロファイルごとに要求される項目（必須またはオプション）が異なる。

- IDP（アイデンティティプロバイダー）
- SP Basic（SOAP を用いないサービスプロバイダー）
- SP Complete （フル機能のサービスプロバイダー）
- LECP

表 4.1　プロファイルのコンフォーマンス項目表

Feature	IDP	SP Basic	SP	LECP
Single Sign-On using Artifact Profile	MUST	MUST	MUST	
Single Sign-On using Browser POST Profile	MUST	MUST	MUST	
Single Sign-On using LECP Profile	MUST	MUST	MUST	MUST
Register Name Identifier - (IdP Initiated) - HTTP-Redirect	OPTIONAL	MUST	MUST	
Register Name Identifier - (IdP Initiated) - SOAP/HTTP	OPTIONAL	OPTIONAL	MUST	
Register Name Identifier - (SP Initiated) - HTTP-Redirect	MUST	MUST	MUST	
Register Name Identifier - (SP Initiated) - SOAP/HTTP	MUST	OPTIONAL	MUST	
Federation Termination Notification (IdP Initiated) – HTTP-Redirect	MUST	MUST	MUST	
Federation Termination Notification (IdP Initiated) – SOAP/HTTP	MUST	OPTIONAL	MUST	
Federation Termination Notification (SP Initiated) – HTTP-Redirect	MUST	MUST	MUST	
Federation Termination Notification (SP Initiated) – SOAP/HTTP	MUST	OPTIONAL	MUST	
Single Logout (IdP Initiated) – HTTP-Redirect	MUST	MUST	MUST	
Single Logout (IdP Initiated) – HTTP-GET	MUST	MUST	MUST	
Single Logout (IdP Initiated) – SOAP	MUST	OPTIONAL	MUST	
Single Logout (SP Initiated) – HTTP-Redirect	MUST	MUST	MUST	
Single Logout (SP Initiated) – SOAP	MUST	OPTIONAL	MUST	
Identity Provider Introduction (cookie)	MUST	OPTIONAL	OPTIONAL	
Backward Compatibility	OPTIONAL	OPTIONAL	OPTIONAL	

開発ベンダーは、Liberty Alliance が主催するコンフォーマンステストに参加し、1 つ以上プロファイルを実装しており、他のベンダー2 社と接続が確認されることで、認定ロゴを取得できる。

4.2.5 Liberty に関する考察

Liberty では積極的に他の標準団体と交流し、既存の標準仕様を積極的に活用している。図 4.13 のように、標準団体、ベンダー／利用会社、政府、マスメディアと連携をとることにより、Liberty の普及促進を図っている。そのため電子認証基盤として、Liberty を採用すれば、Liberty に関係する各方面からのサポートを受けることが可能である。政府や企業、団体が認証基盤として Liberty を採用すれば、Liberty の参加団体を介して世界中にニュースとして配信されるため、他国にも影響を与えると考えられる。政府や企業、団体が Liberty を採用すると、技術面ではすでに Liberty を採用している政府、企業、団体との相互接続が比較的容易に実現可能であると予想される。

Liberty は、SAML で規定されていない部分の仕様化や機能追加が行われているため、SAML を用いるよりもすばやくシステムを構築することが可能である。そのためスピードが重要なビジネス領域において組織を超えた提携や連携を行う場合に、Liberty の採用が最適であると思われる。

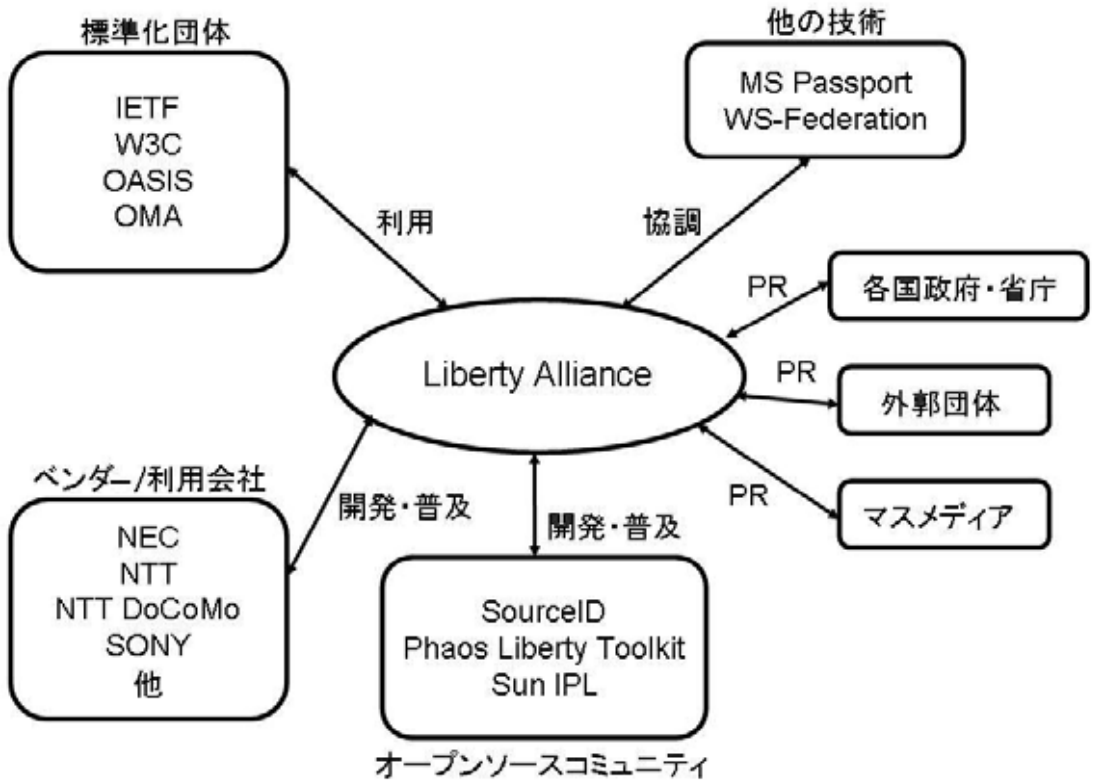


図 4.13　Liberty Alliance を取り巻く状況

Liberty Alliance のホームページでは、白書や研究事例等のドキュメントを公開しており、活動内容や成果をオープンにしている。日本語のホームページ[2]では次のドキュメントが公開されている。

- アイデンティティ連携による政府のメリット
- Liberty プロトコルとアイデンティティ盗用に関する白書
- Liberty と WS-Federation：比較概要
- 連携アイデンティティのビジネスメリット
- 総務省の EduMart 実証実験
- Communicator 社の事例
- Neuster 社の事例

昨年のトピックスとしては、IBM が 2004 年 10 月に Liberty に理事会員として参加することに合意した。IBM は Microsoft 等の大手ベンダー数社と WS-Federation の仕様を策定している。そのため IBM の Liberty 加盟は、Liberty の普及および Liberty と WS-Federation の連携促進に影響を与えると考えられる。IBM はすでに Liberty の仕様の一部に対応した Tivoli 製品を持っており、フランステレコムの子会社 Orange に提供予定である。このように市場において Liberty の適用が進んでいることから、電子認証基盤の情報収集に関して今後も Liberty の動向を注目していく必

[2] http://www.projectLiberty.org/jp/

要がある。

4.3 Shibboleth

4.3.1 Shibboleth の概要

Shibboleth は、2000 年 7 月 Internet2/MACE（Middleware Architecture Committee for Education）プロジェクト内の Shibboleth Initiative として発足した。プロジェクトでは IBM が知識や資金のサポートを行っている。Shibboleth は、アーキテクチャ、フレームワークおよび実用技術を開発しており、大学や研究機関の間でアクセス制御を必要とするリソースの共有に用いられる。Shibboleth アーキテクチャは、アクセス制御における認可情報を安全に交換するものである。

Shibboleth では、米国の約 40 の大学において運用されることで、ID を保有している生徒や教授が匿名で他の大学の施設にある情報資源にアクセスすることを可能とするシナリオを想定している。匿名に関してはビジネス分野と異なり、学術分野では学生や研究者のプライバシーを十分に考慮すべきであるという考えから取り入れられている。

Shibboleth プロジェクトでは次のコンセプトを満たすシステムの実現を目指している。

- 連携管理（Federated administration）
  利用者は所属するハンドルサービス（HS）で認証を受けることで、複数のリソース提供サイトに再度ログインする必要なくリソースにアクセスすることを可能にする。

- 標準ベース
  Shibboleth は SAML の枠組みに基づいた仕様の策定を行っている。Liberty のように SAML を拡張しているわけではない。

- 属性ベースのアクセス制御
  リソースへのアクセス権限を属性アサーションによって決定する。属性アサーションは、SAML において定義されており、属性オーソリティから発行される XML で記述された属性の認証情報である。

- プライバシーの動的管理
  利用者は利用者の属性の公開範囲のポリシーを設定可能である。そのため利用者は、リソース提供を受けるときに公開したくない属性情報をリソース提供者に知られることがない。

- 複数の信頼／ポリシー集合のフレームワーク
  ポリシーを共有する組織集合を規定している。

- 属性値の用語の定義
  人の属性に関して”eduPerson”という標準的なオブジェクトクラスを定義している。

実際 Shibboleth は、InCommon Federation において、米国の教育や研究を支援す

るためのオンラインリソースの共有に用いられている。InCommon Federation には、現在 12 の団体が参加しており、Shibboleth を使用する上で設定に必要な情報やポリシーの取り決め等を行っている。Shibboleth を用いたサービスとポリシーの情報（メタデータ）として、共通のアイデンティティ属性テーブルや、属性アサーションの保証レベル、アサーションの信頼性を定義しており、情報提供として公開されている。他の技術文書として、技術的なオペレーションや認証のオペレーションに関する情報が公開されている。

InCommon Federation への参加団体は、米国の Higher Education Institution（高等教育機関）とそれ以外のスポンサーパートナーの 2 種類ある。それぞれ InCommon Federation に参加するには、次のような費用が必要となる。

[Higher Education Institution]

申請費用	700 ドル（初回のみ）
クレデンシャルサービスプロバイダーパッケージ（アイデンティティマネージメントシステム 1 個、リソースプロバイダーID20 個を含む）	年間 1000 ドル
リソースプロバイダーの追加（20 個）	年間 1000 ドル
アイデンティティマネージメントシステム（1 個）	上記と同じ費用

[スポンサーパートナー]

申請費用	700 ドル（初回のみ）
クレデンシャルサービスプロバイダーパッケージ（アイデンティティマネージメントシステム 1 個、リソースプロバイダーID20 個を含む）	年間 1000 ドル
リソースプロバイダーの追加（20 個）	年間 1000 ドル
アイデンティティマネージメントシステム（1 個）	なし

InCommon Federation に参加することで次のような利益を得ることができる。

・ より高いセキュリティ
安全なアクセスチャネル上で強力な権限コントロールを用いたセキュリティを元にしたポリシーは、より高いレベルのセキュリティを提供する。このセキュリティでは、アイデンティティ属性と権限属性の交換においてプライバシーを確保するために安全な機構を提供する。

・ コラボレーションのための標準的な道筋を与える
共用の Web ベースのリソースへのアクセス授受のためのコレクションポイントと道筋を与える。接続に標準的な機構を使用することで、新たにコラボレーションのために繰り返されるインテグレーションの作業を減らすまたは無くすことでスケールメリットを与える。

・ アカウントのオーバーヘッドを削減
連携相手がアカウント管理の責任を持つことで、リソース提供者に所属していない利用者のアカウントの作成や管理の作業を削減できる。

・ 契約上の合意のためのスケールメリット
リソース共有の合意に必要になるポリシー、規則、要件については、連携ポリシー、合意、要件に関するドキュメント群を用いることができる。これらのドキュメントにより合意の必要性や範囲を最小限に抑えることができる。

・ オンラインリソース配信へのアクセスと監査のより細かなコントロール
IP アドレスまたは他の平易なコントロールによってリソースの制限を行っていれば、コストをベースにしたリソース配信をより細かなコントロールで認可決定を行うことが可能となる。その結果、リソースの利用状況や利用者等について矛盾のないアカウンティングが可能となる。

4.3.2 Shibboleth のモデル

(1) システムの構成要素
Shibboleth の構成要素は次のようなものである。

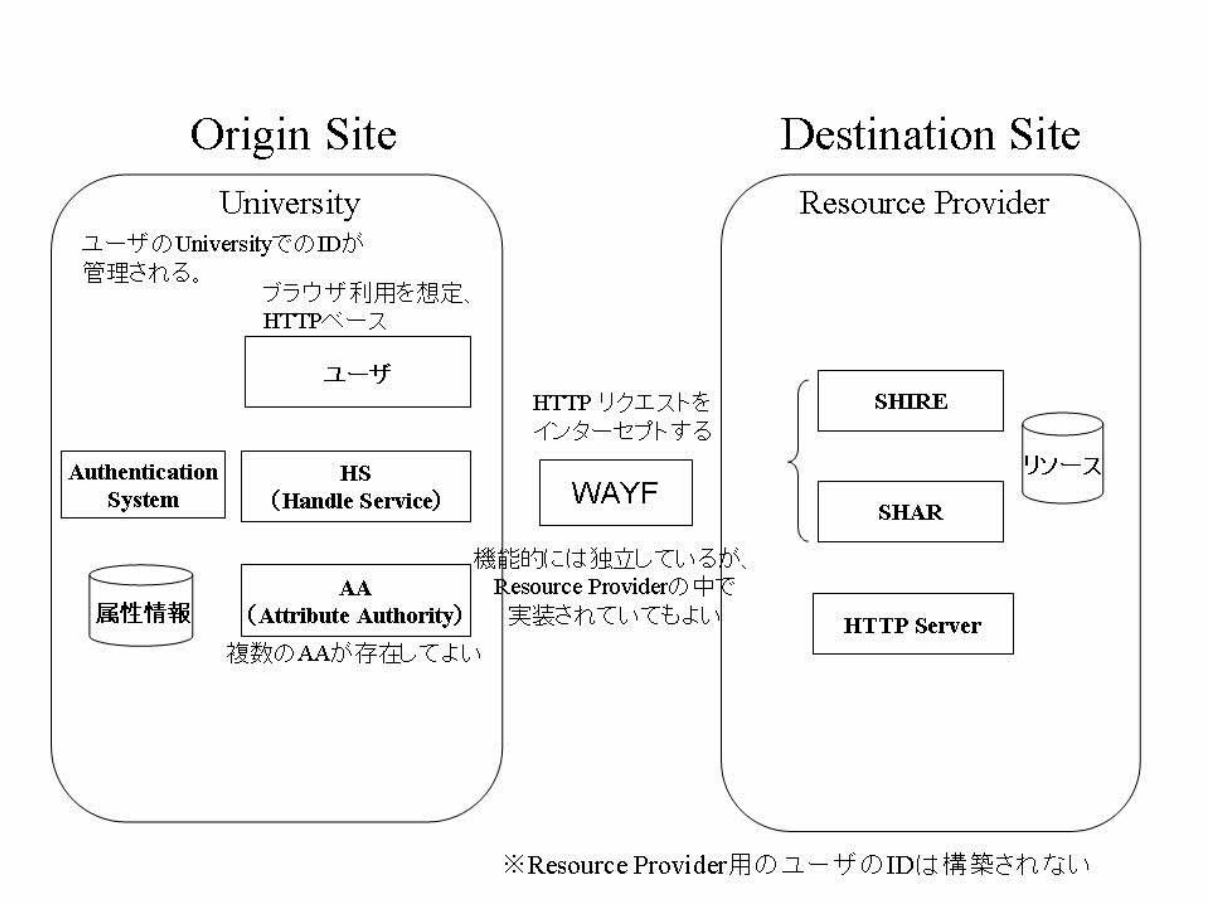


図 4.14　システム構成図

- オリジンサイト（Origin Site）
  リソースプロバイダーのリソースを利用する大学

- ディスティネーションサイト（Destination Site）
  大学にリソースを提供するリソースプロバイダー

- 認証システム（Authentication System）
  大学に所属するユーザを認証する基盤

・ 属性情報
大学に所属するユーザの属性情報
複数の属性情報の項目を管理

・ ハンドルサービス（Handle Service）
ハンドル（仮識別子）を作成し、マッピング
ローカルサイトでユーザを認証

・ 属性オーソリティ（Attribute Authority）
SAML で規定されている属性オーソリティ

・ WAYF （Where Are You from）
ユーザが所属する大学の HS を検索するサービス
ハンドルサービスの名前と URL をマッピング

・ SHIRE（Shibboleth Indexical Reference Establisher）
ユーザのアクセス元サイトと HS を特定してハンドルを取得
ハンドルの検証

・ SHAR（Shibboleth Attribute Requester）
属性オーソリティに属性情報を要求し、属性オーソリティから属性情報を取得

・ リソース
リソースプロバイダーが提供するサービスや情報

(2) 処理フロー

Shibboleth は図 4.15 のフローによって、大学のユーザがリソースプロバイダーからサービスを受けることが可能となる。リソースプロバイダーは、大学と信頼関係を築いており、大学にその大学の所属ユーザであるか問い合わせることで、リソース提供を行うかどうかを決定している。

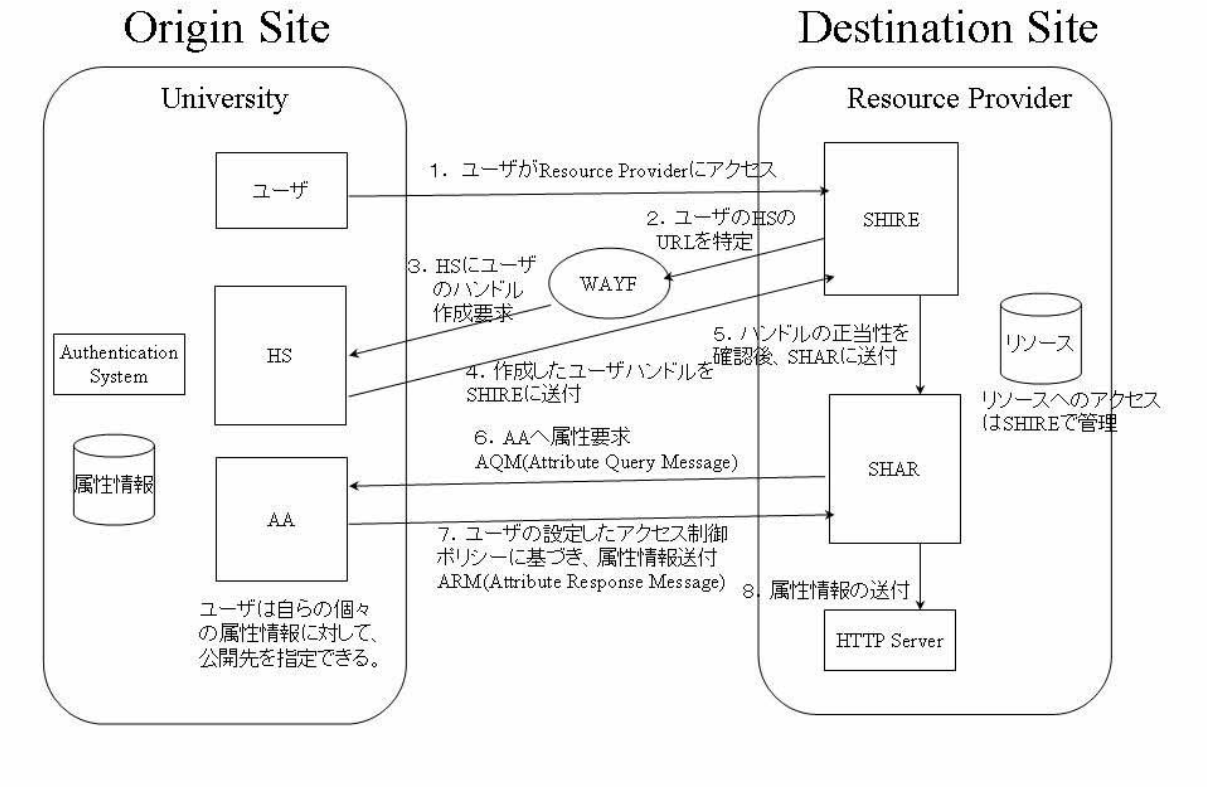


図 4.15　Shibboleth の処理フロー

1. ユーザはリソースプロバイダーにアクセスする。リソースプロバイダーは SHIRE でユーザのアクセスを受信する。
2. SHIRE は WAYF にユーザをリダイレクションすることでユーザの所属するハンドルサービスの URL を解決する。
3. WAYF はユーザと通信してユーザが所属するハンドルサービスの URL を特定する。その後 WAYF は、ハンドル作成要求（Attribute Query Handle Request）を作成し、ユーザをハンドルサービスにリダイレクションする。
4. ハンドルサービスは利用者の認証に成功するとハンドルを作成する。ハンドルサービスはハンドルを作成し、ユーザを SHIRE にリダイレクションする。
5. SHIRE はハンドルの正当性を確認して、その結果を SHAR に送信する。

6. SHAR は、ハンドルを元に属性オーソリティに属性情報を要求するため、AQM（Attribute Query Message）を送信する。
7. 属性オーソリティはユーザが設定したアクセス制御ポリシーに基づき、SHAR に公開可能な属性情報を受け渡すために、ARM（Attribute Response Message）を送信する。
8. SHAR は HTTP Server に属性情報を送信する。

4.3.3 Shibboleth のアーキテクチャ

Shibboleth の特徴としては、ブラウザのユーザのみに注目している点と、属性アサーションを用いてリソースにアクセスするユーザを特定しない点であり、これらを SAML の枠組みでうまく実現している。

(1) アイデンティティプロバイダー

アイデンティティプロバイダーは、図 4.14 のハンドルサービス、認証システム、属性オーソリティ、属性情報のデータベースを含むものであり、主体者の認証とアサーションの生成を行う。アイデンティティプロバイダーは SAML ドメインモデルの認証オーソリティと属性オーソリティの機能コンポーネントから構成されている。アイデンティティプロバイダーは次の 5 つの機能を有している。

- 認証オーソリティ
- 属性オーソリティ
- シングルサインオンサービス
- インターサイト転送サービス
- アーティファクト解決サービス

(2) サービスプロバイダー

サービスプロバイダーは、図 4.14 のリソースプロバイダーにあたり、SHIRE、SHAR、リソースデータベース、HTTP サーバを含むものである。サービスプロバイダーはセキュリティコンテキストを元にした権限またはカスタマイズを行った Web ベースのサービス、アプリケーション、または、リソースを与える。サービスプロバイダーは次の 2 つの機能を有している。

- アサーションコンシューマーサービス
- 属性リクエスター

(3) WAYF（Where Are You from?）

「4.3.2 (1) システムの構成要素」で説明した WAYF と同じものである。Shibboleth では、ユーザエージェントがサービスプロバイダーにアクセスしたときに、サービスプロバイダーがユーザエージェントの証明するアイデンティティプロバイダーが特定できない場合がある。このときサービスプロバイダーはユーザエージェントを WAYF にリダイレクションし、WAYF においてユーザエージェントが所属するアイデンティティプロバイダーに転送する。

(4) プロトコルとプロファイル

Shibboleth では、SAML の Browser/POST プロファイルまたは Browser/Artifact プロファイルを用いる。Shibboleth ではユーザが Browser をベースにしてサービ

スプロバイダーからリソース提供をうけることが特徴の 1 つである。次に Shibboleth の各エンティティ間のシーケンス図を示す。

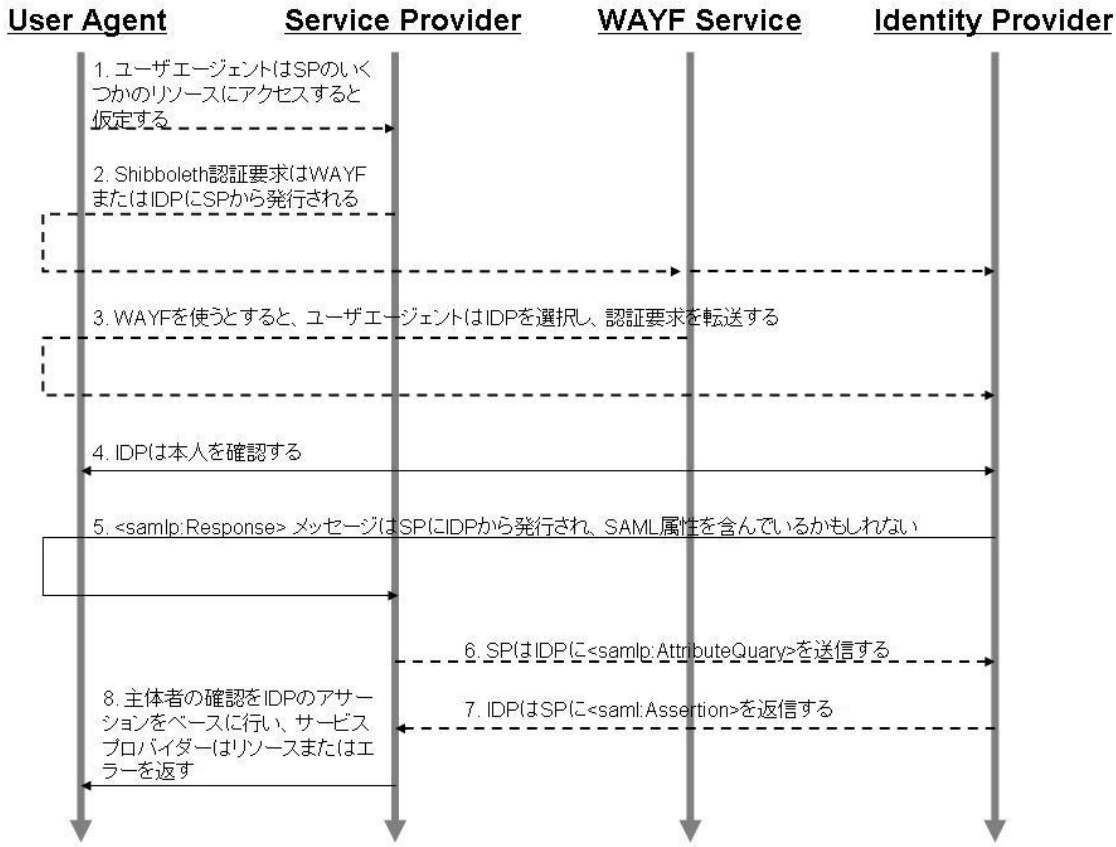


図 4.16　Shibboleth のシーケンス図

以下で図 4.16 の流れを解説する。

1. ユーザエージェントはサービスプロバイダーのリソースにアクセスする。
2. サービスプロバイダーは、アイデンティティプロバイダーにユーザエージェントを介して認証要求をリダイレクションする。このときサービスプロバイダーはリダイレクション先のアイデンティティプロバイダーが不明である場合、WAYF サービスにユーザエージェントを介して認証要求をリダイレクションする。
3. サービスプロバイダーが WAYF を利用する場合、ユーザエージェントはアイデンティティプロバイダーを選択する。WAYF は認証要求を対象のアイデンティティプロバイダーにユーザエージェントを介して認証要求をリダイレクションする。
4. アイデンティティプロバイダーは、ユーザの本人確認をする。
5. アイデンティティプロバイダーは、<samlp:Response>メッセージを生成して、ユーザエージェントを介してサービスプロバイダーに転送する。<samlp:Response>メッセージには、アーティファクトまたはアサーションが格納されている。
6. サービスプロバイダーは、<samlp:Response>メッセージのアーティファクトまたはアサーションを元に、アイデンティティプロバイダーに<samlp:AttributeQuery>を送信する。
7. アイデンティティプロバイダーは、<samlp:AttributeQuery>を元に属性アサーションを含んだ<saml:Assertion>を返信する。
8. サービスプロバイダーはアイデンティティプロバイダーの属性アサーションを元にユーザの確認を行い、ユーザにリソースまたはエラーを返す。

4.3.4 Shibboleth の状況

本節では、仕様に関連した内容として、「セキュリティの考察」と「SAML との関係」、「コンフォーマンス」について述べる。そして Shibboleth の適用に関する考察や動向等についても述べる。

(1) セキュリティの考察

Shibboleth では、セキュリティに関する注意点として次のようなことを挙げている。悪意のあるユーザが、アイデンティティプロバイダーやサービスプロバイダーになりすますことがないように、SAML プロトコルやアサーションに署名をつけた方がよいとしている。またユーザがサービスプロバイダーのどのリソースにアクセスしているかをアイデンティティプロバイダーに知られないような機能を要求している。他にはセキュリティ基盤において時刻同期が重要であり、UTC に比べて５秒未満のずれであることが望ましいとしている。

(2) SAML との関係

Shibboleth は SAML で規定している範囲内においてプロトコルやプロファイルを定義しており、SAML の枠組みを元にアサーションを用いてセキュリティを確保している。Shibboleth で用いられるアサーションは、SAML の属性アサーションを使用している。また Shibboleth の AQM／ARM のメッセージは、SAML プロトコルを使用している。そのため Shibboleth の仕様を理解する上でベースとなる SAML の仕様を事前に理解しておく必要がある。

SAML の仕様を読んだだけでは、実際にどのようなシステムが構築可能であるか想像することが難しい。

(3) コンフォーマンス

Shibboleth では次のプロファイルについて相互接続性が確保されれば認定を受けることができる。Shibboleth のコンフォーマンステストには、米国以外の大学が参加することが可能かどうか不明であるが、米国以外の大学が米国の大学と連携してリソースを共有する場合には、Shibboleth を用いることになると思われる。

- Browser Authentication Request
- Browser/POST Authentication Response
  SAML で定義されている Browser/POST と同じ。
- Browser/Artifact Authentication Response
  SAML で定義されている Browser/Artifact と同じ
- Attribute Request/Response/Syntax
- Transient NameIdentifier Format
- Metadata Profile

それぞれアイデンティティプロバイダーとサービスプロバイダーの必須、オプションの項目に関しては以下の表で示しておく。

表 4.2　コンフォーマンス項目表

Profile/Protocol	IdP	SP
Browser Authentication Request	MUST	MUST
Browser/POST Authentication Response	MUST	MUST
Browser/Artifact Authentication Response	MUST	MUST
Attribute Request/Response/Syntax	MUST	OPTIONAL
Transient NameIdentifier Format	MUST	MUST
Metadata Profile	MUST	MUST

4.3.5 Shibboleth に関する考察

Shibboleth の特徴としては、属性アサーションを用いてサービス提供することにより利用者のプライバシーを損なうことなくセキュリティを確保しているところである。そのため Shibboleth を用いた認証基盤は、プライバシーを重視したシステムに

適用することが望ましい。ビジネスの場では、プライバシーよりもセキュリティを重視する傾向があるため、米国のように学術的な場において利用されるのが一般的だと考えられる。Shibboleth の学術系への適用という観点では、先に述べた米国の InCommon Federation 以外に、スイスの The Swiss Education & Research Network が存在する。またイギリスの JISC（The Joint Information Systems Committee）においても導入が検討されている。

Shibboleth は、SAML の枠組みで部品をうまく組み合わせ、SAML で示されているシングルサインオンのシーケンスの例と異なるものを実現している。そのため SAML をベースにした特徴のあるシングルサインオンのシステム仕様を検討する際に参考になると思われる。また InCommon 等、すでに Shibboleth を用いて運用している組織のドキュメントからポリシーや運用に関する情報を得ることが可能であるため、SAML を採用する際のコンセプトやプレイヤー等について参考にできると思われる。

Shibboleth は学術系に関する特徴を比較的強く持っているため、特定領域に特化したシステム構築で SAML を用いる際に、よい実例として扱われるのではないかと考えられる。

4.4　米国標準技術局電子認証ガイドライン

4.4.1 米国連邦政府の動向と電子認証ガイドライン

本節では米国の標準技術局（NIST : National Institute of Standards and Technology）が発行した電子認証ガイドライン（以下 NIST ガイドライン）[1] について述べる。NIST ガイドラインは、行政管理予算局（Office of Management and Budget : OMB）が発行した連邦政府機関向け電子認証ガイダンス（以下 OMB ガイダンス）[2] で示された認証の保証レベルに対する技術要件を示したものである。これら 2 つの文書は、米国電子政府戦略の中での成果である。本節ではまず米国電子政府戦略における電子認証の動向を概説し、その後 NIST ガイドラインの位置づけを示すことで全体像の把握を狙う。

その後、4.4.2 節において OMB ガイダンスで示された認証の保証レベルとその決定プロセスについて解説を行い、4.4.3 節で NIST ガイドラインにおける技術要件を詳細にわたり解説する。最後に NIST ガイドラインに関する動向調査を 4.4.4 節で示し、4.4.5 節でまとめる。

図 4.17　米国電子政府戦略の分類

(1) 米国連邦政府における電子政府戦略

2001 年秋以降、米国ブッシュ政権は電子政府の実現にむけて 24 のイニシアチブを制定した。24 のイニシアチブはそれぞれのサービス対象によって G2C （政府機関対国民：Government　to Citizen）、G2G（政府機関対政府機関：Government to Government）、G2B（政府機関対企業：Government to Business）、IEE（内部効率化：Internal Efficiency & Effectiveness）と分類され、また、すべてのイニシアチブに横断するイニシアチブとして、安全で強固な認証を提供する e-Authentication イニシアチブが位置づけられている（図 4.17）。e-Authentication イニシアチブの成果は、文書やツール等が一般に公開されている。（図 4.18）

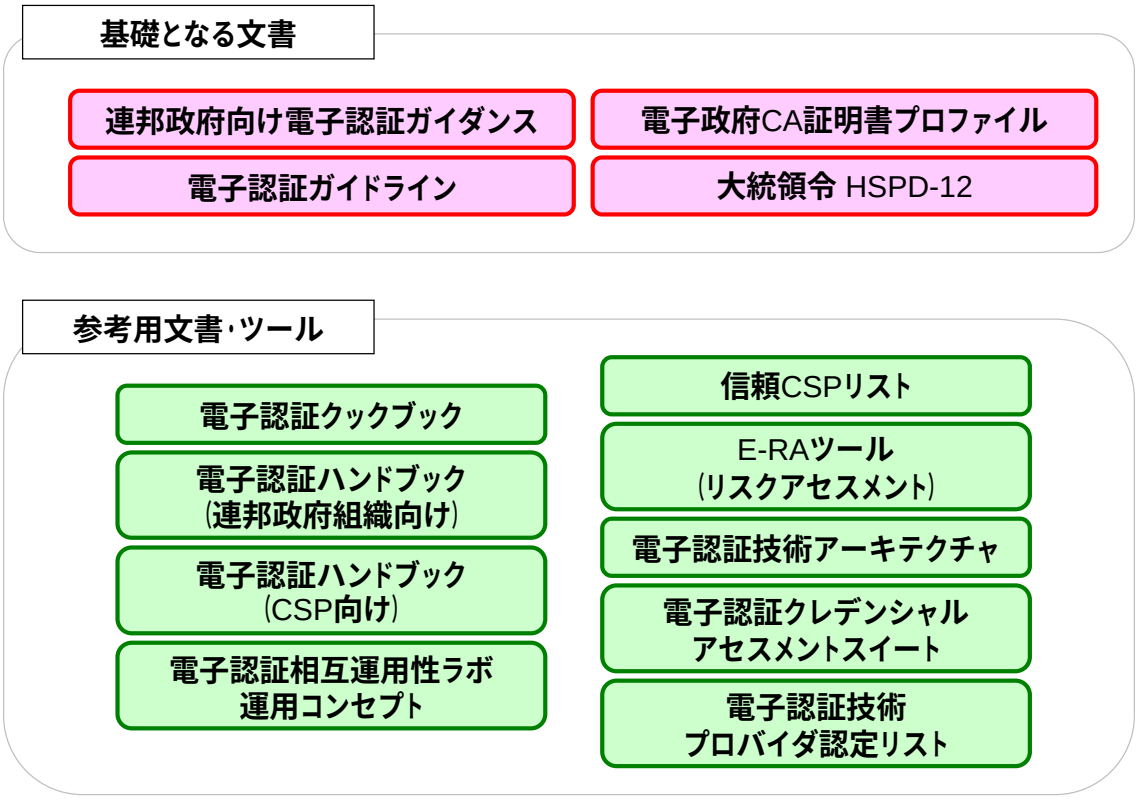


図 4.18　e-Authentication イニシアチブ成果物

すでに米国の政府機関の多くでは、電子的にサービスを提供していた。当然それらのサービスを提供する前の段階で、サービス享受者に対して何らかの認証をしなければならないが、現状ではそういった本人認証のシステムを個々のサービスがそれぞれ構築を行っており、その構築コストに相当な負担を強いられていた。また、互いに連携したサービスや同じユーザ情報を共有したサービス形態等が行われていないために、個別での構築コストがかかり政府全体としても相当なコスト負担がかかっていることに加え、サービス享受者としてもいくつもの認証形態に応じて、複数の本人を認証する手段を持たなければならずその負担は小さなものではなかった。

個々の認証システム構築のコスト、また連携したサービス展開、そしてユーザの利便性等を考慮し、e-Authentication イニシアチブが計画された。

(2) 電子認証ガイドライン

e-Authentication イニシアチブの成果として、OMB は OMB ガイダンスを発表した。OMB ガイダンスでは認証において 4 つの保証レベルを規定しており、サービスの機密度合い等により適切な認証方法を指定することの重要性を示している。OMB ガイダンスは同時に保証レベルと認証方法を決定するプロセスも示している。しかし、そこでは技術的な要素については触れておらず、その部分を NIST ガイドラインが受け持つ形になっている（図 4.19)。NIST ガイドラインは、認証時におけるリスクと脅威、さらにその対策を踏まえレベル別に技術要件を示している。

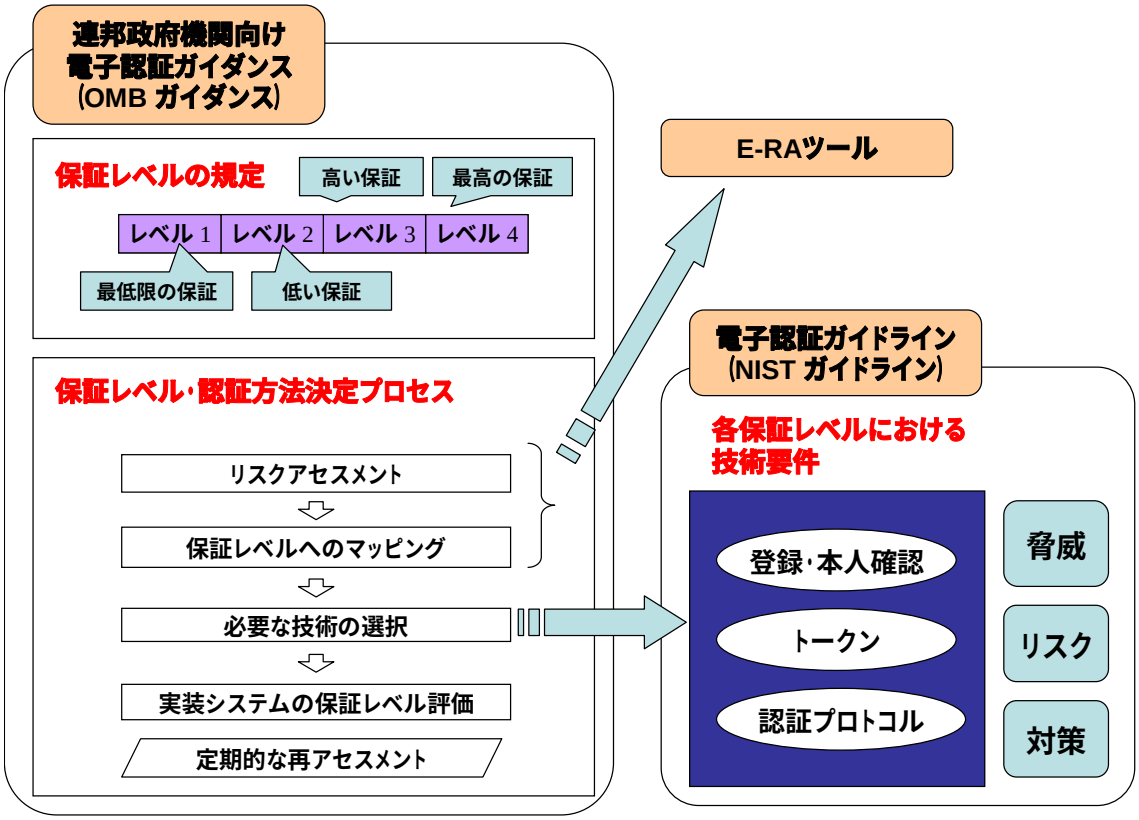


図 4.19　OMB ガイダンスと NIST ガイドラインの関係性

NIST ガイドライン自体は、OMB ガイダンスを補助する形での文書としての位置づけがあると共に、NIST の文書として「NIST Special Publication 800-63」という識別がされている（図 4.20）。NIST ではコンピュータセキュリティに関するガイドラインや推奨としての文書として Special Publication（SP） 800 シリーズを発表しており、NIST ガイドラインもその中のひとつである。2005 年 2 月の段階では草案を含め 77 の文書が発表されており、本人確認や医療、さらにはインシデントハンドリング等その対象とする領域は広い。SP 800 シリーズは、主に米国電子政府におけるセキュリティの為に発表されている文書ではあるが産業界への影響も強く、また米国だけにとどまらず世界の各国より多く参考にされている文書となっている。

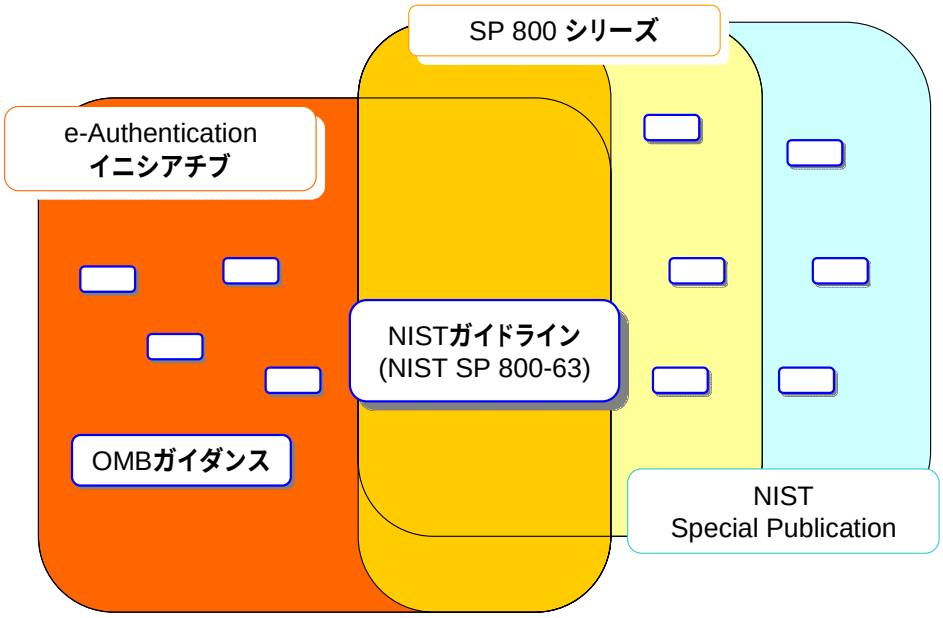


図 4.20　NIST ガイドラインの位置づけ

4.4.2 認証における保証レベル

必要なサービスレベルに応じて、必要な認証方法を適切に提供することの必要性についてはすでに 3 章において述べた。ここでは、適切な認証方法を提供するにあたって必要である認証の保証レベルについて、OMB ガイダンスが規定した保証レベルの解説を行う。OMB ガイダンスでは認証におけるリスクとその影響度、さらに誤認証の発生確率を考慮して 4 つの保証レベルを定義し、それぞれのレベルにおける要件を述べている。また連邦政府機関がシステムを構築する際に保証レベルと認証方法を決定するためのプロセスも提示している。

OMB ガイダンスでは、その対象部分をいくつか限定している。まず認証（Authentication）と認可（Authorization）に関して、認証のみを考慮し認可は考慮していない。また認証は人間ユーザのみに適用され、サーバや他の機械、ネットワークコンポーネント等の認証には適用されない。さらにクレデンシャルの電子署名での利用や、正しい署名者による「故意の署名（Intent to Sign）」に関連した問題については論じておらず、あくまで人間の認証にのみ論点を絞っている。ここで言うクレデンシャルとは、認証処理時に検証者（Verifier）に提示することで検証される対象のことを言う。

(1) 保証レベル

OMB ガイダンスでは、保証の定義を以下のようにしている。

- クレデンシャル被発行者のアイデンティティ調査プロセスにおける信用の程度
- クレデンシャル利用者がクレデンシャル被発行者であるという信用の程度

保証の 4 つのレベルは以下のように定義される。

- レベル 1） 主張するアイデンティティの正当性の信用が（ほとんど）ない
- レベル 2） いくらかの信用性
- レベル 3） 高い信用性
- レベル 4） とても高い信用性

それぞれのレベルの解説を行う。

(a) レベル 1

主張するアイデンティティの正当性の信用が（ほとんど）ない状態。例えば、自己登録 ID とパスワードの利用によるサービスの利用等がこれにあたる。

(b) レベル 2

全般的に見てある程度の正当性が主張するアイデンティティに存在する状態。初期にアイデンティティの確認を必要とする公的サービスにおいて広く適用が可能である。誤認証によって起こる影響が一時的なもので済むような場合等がこれにあたる。

(c) レベル 3

アイデンティティの正当性主張において高い信頼性を必要とする処理に適している。例えば特許申請時での特許情報の送信等、秘密情報の開示が競合相手に大きな利益を生ませるような場合に適用される。また、その財政ロスは重大ではあるが、壊滅的ではなくレベル 4 は妥当ではない場合等。

(d) レベル 4

アイデンティティ正当性の主張において大変に高い信頼性を必要とする処理に適している。例えば法執行機関における犯罪情報を含んだデータベースへのアクセス等、情報が開示したときに多大な問題を起こす場合等。

(2) 保証レベルと認証方法の決定プロセス

実際に認証システムを構築する際に、その保証レベルと認証方法を決定しなければならないが、OMB ガイドラインではその決定プロセスも合わせて提示している。そのプロセスを以下に示す。

- リスクアセスメント
- リスクの保証レベルへのマッピング
- 必要な技術の選択
- 実装システムの保証レベル評価
- 定期的な再アセスメント

- リスクアセスメント

リスクアセスメントの方法については、OMB が発表している GPEA（米国政府ペーパーワーク削減法）実装ガイダンスや NIST のガイダンスを参照することが可能である。それらのガイダンスを利用することにより、アイデンティティの誤認証における潜在的な被害と影響に対してそれぞれの深刻度を測ることができる。リスクアセスメントは、技術的な失敗のみならず、悪意のある第 3 者、一般的な誤解、人的な誤操作等様々な要因を考慮しなければならない。またその際、リスクを低く評価するよりは高く評価するほうが望ましい。リスクアセスメントの結果が得られれば、特定のリスクに対してはシステムの見直しにより誤認証の発生頻度を減らすことも可能である。

- リスクの保証レベルへのマッピング

リスクアセスメントで得られた各カテゴリのリスクを表 4.4 に適用することで適切な保証レベルを選択する。

- 必要な技術の選択

必要な保証レベルが決定した後は、NIST ガイドラインに従い、適切な技術の選択を行う。NIST ガイドラインについては次節で解説する。

- 実装システムの保証レベル評価

実装システム上では、複数のリスクが複合的に生じることがある。そのためシステムは実装した後にあらためて保証レベルの要件を満たしているかを評価す

る必要がある。

- 定期的な再アセスメント
  システムの実装が終わり、評価も終われば、システムとして一応の完成を見る。しかし技術の進歩や組織のビジネスプロセスの変更等の要求から、認証を行う情報システムとその周りの環境は変化することが十分に考えられる。その場合、以前のリスクアセスメントの結果とそれに対応した認証の要件により得られた保証レベルが保たれているとは限らない。そのために、認証を行う情報システムに対して定期的なリスクアセスメントが必要となる。

実際にここで示されたプロセスに沿って保証レベルを決定していくのだが、e-Authentication イニシアチブではプロセスにおける「リスクアセスメント」と「保証レベルへのマッチング」を行う E-RA ツールを提供している。認証の保証レベルを決定するにあたり、まず E-RA を用いて保証レベルのマッチングを行った後、NIST ガイドラインに従い適切な技術を選択することが具体的な認証システムの実現方法となろう。

(3) 潜在インパクトとリスク

認証を受けるユーザがそのアイデンティティの正当性を主張してくる場合、認証を行う組織はそのアイデンティティの正当性保証を適切にレベル付けする必要があることはすでに述べた。そのレベル付けは、まず認証における潜在的なリスクを考慮し、誤認証が発生した場合により悪い状況を引き起こすものに関しては、高い保証レベルの認証を行わなければならない。OMB ガイダンスにおいて、認証におけるリスクは 2 つの要因からなるとしている。1 つ目は潜在的な被害と影響、2 つ目が被害の発生度合である。さらに OMB ガイダンスでは、潜在的な被害と影響を 6 つのカテゴリに分け、それぞれにおいてリスクを評価することで、その保証レベルを適切に設定する指標を与えている。それぞれのカテゴリは、Low、Moderate、High と 3 段階の影響度で評価をされる。このリスク評価は NIST が策定した連邦政府情報と情報システムにおけるセキュリティ分類標準（FIPS 199）[3] に従うものである。以下に 6 つのカテゴリを示す。また各カテゴリにおけるそれぞれの影響度の説明を表 4.3 に示す。

- 不便性、災難、身分や評判への損害
- 金銭的ロス、組織の責務
- 組織計画や公益への被害
- 機密（sensitive）情報の未許可開示
- 個人の安全
- 民事上あるいは刑事上の違反（Civil or criminal violations）

表 4.3　潜在的な被害と影響

	Low	Moderate	High
不便性、災難、身分や評判への損害	短期間における限定した損害	短期間における深刻な損害、あるいは長期間における限定した損害	長期間における深刻あるいは非常に厳しい侵害
金銭的ロス、組織の責務	あまり重要でない、取るにたらない回復不可能な金銭的ロスあるいは組織の責務	深刻な回復不可能な金銭的ロスあるいは組織の責務	非常に厳しいまたは壊滅的な金銭的ロスあるいは組織の責務
組織計画や公益への被害	組織運用や資産、公益に対して限定されている逆の効果の波及	組織運用や資産、公益に対して深刻な逆の効果の波及	非常に厳しいまたは壊滅的な逆の効果の波及
機密情報の未許可開示	影響度の低い機密性損失における個人的、米国政府機密、商業上の機密情報の未許可組織への開示	影響度が中程度の機密性損失における個人的、米国政府機密、商業上の機密情報の未許可組織への開示	影響度の高い機密性損失における個人的、米国政府機密、商業上の機密情報の未許可組織への開示
個人の安全	医療措置を必要としない傷害	たいしたことのない傷害の中程度のリスク、あるいは医療措置を必要とする限定したリスク	深刻な障害あるいは死のリスク
民事上あるいは刑事上の違反	通常は法執行を受けることのない民事上あるいは刑事上違反のリスク	法執行をうける民事上あるいは刑事上違反のリスク	法執行計画において非常に重要な民事上あるいは刑事上違反のリスク

OMB ガイドラインでは各カテゴリのリスクレベルと保証レベルの対応を示した（表 4.4）。認証システムの保証レベルを決定する際は、まずシステムのリスクアセスメントを行い各カテゴリのリスクレベルを導き出す。各カテゴリのリスクレベルに合わせて表 4.4 と照らし合わせ、すべてのリスクレベルを満足する最小の保証レベルを選択することで認証システムの保証レベルを決定する（図 4.21）。

表 4.4　潜在的な影響度と認証の保証レベルのマッチング

認証エラーによる潜在的な影響のカテゴリ	保証レベル			
	1	2	3	4
不便性、災難、身分や評判への損害	Low	Mod	Mod	High
金銭的ロス、組織の責務	Low	Mod	Mod	High
組織計画や公益への被害	N/A	Low	Mod	High
機密（sensitive）情報の未許可開示	N/A	Low	Mod	High
個人の安全	N/A	N/A	Low	High Mod
市民や犯罪の違反	N/A	Low	Mod	High

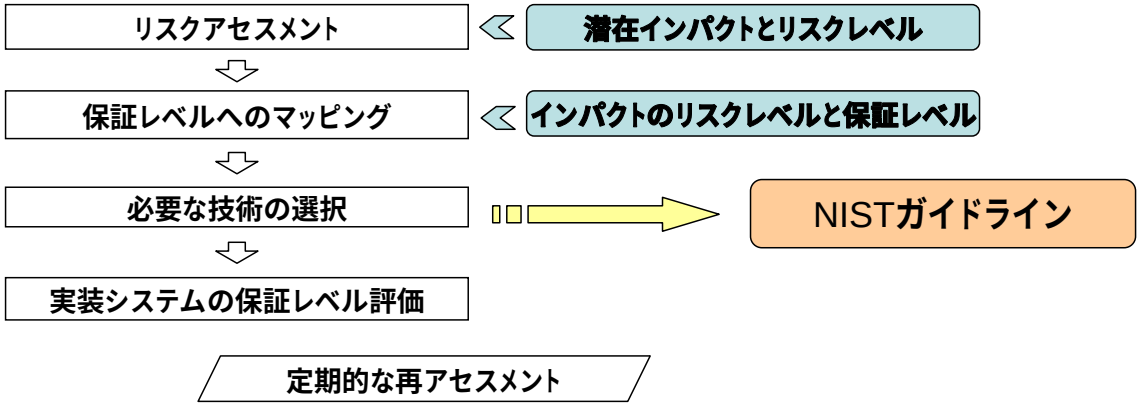


図 4.21　各表が利用される段階

4.4.3 各保証レベルにおける技術要件

NIST ガイドラインでは、OMB ガイダンスで定めた 4 つの保証レベルについて、技術要件を示している。技術要件という性格上、用語の定義や技術を適用する対象については細かく規定されている。本節ではまず NIST ガイドライン内における用語の定義と認証のモデルについて解説を行う。また NIST ガイドラインでは認証における技術として 3 つの要素が考慮されている。1 つ目が本人認証に用いるトークン、2 つ目が登録作業とアイデンティティの確認、そして 3 つ目に認証プロトコルである。本節ではそれぞれについても解説を行う。最後に保証レベルごとでの要件の概観を示す。

(1) 用語の定義

NIST ガイドラインでは OMB ガイダンスと比較して用語の定義が厳密にされている。ここでは、文書内での意味を統一し読者の誤解のないよう、NIST ガイドラインに従った用語の定義を抜粋して説明する。またこの用語の意味は、本節のみに限定したものとする。

- アイデンティティ（Identity）
  個々の人が持つ唯一の名称。法的な氏名は重複する可能性があるので、唯一性を保つために個人のアイデンティティは氏名に加え付加的な情報（住所、口座番号や社員番号等の唯一の識別子）を含まなければならない。

- 認証（Authentication）
  要求者アイデンティティの信頼確立プロセス

- 認証プロトコル（Authentication Protocol）
  仕様が策定されているメッセージ交換プロトコル。このプロトコルを用いてリモートからの要求者認証を行う。

- 要求者（Claimant）
  認証プロトコルによりそのアイデンティティが検証される人。

- 加入者（Subscriber）
  CSP よりクレデンシャルまたはトークンを受領し、認証プロトコル上での要求者となる人。

- トークン（Token）
  要求者のアイデンティティを認証するために、要求者が所持し管理するもの。パスワードや、PKI の公開鍵等がこれにあたる。

- クレデンシャル（Credential）
  トークンと、その所持と管理をしている人のアイデンティティを厳密に結びつける対象。X.509 電子証明書や、Kerberos チケット等はクレデンシャルの例である。

- CSP（Credential Service Provider）
  加入者のトークン発行または登録作業、加入者へのクレデンシャル発行作業を行う主体。PKI であれば認証局がこれにあたる。

- 登録（Registration）
  CSP の加入を申請した者に対し、RA（Registration Authority）が CSP に代わり申請者のアイデンティティを検証するプロセス。

- CA（Certification Authority）
  公開鍵証明書の発行と失効を行う機関。

- RA（Registration Authority）
  CSP に対し、申請者のアイデンティティ保証を行う信頼された主体。RA は CSP における必須部分である場合もあれば、独立した主体である場合もある。独立主体の場合においても CSP とは関連のある主体となる。

- 検証者（Verifier）
  認証プロトコルを通じ要求者のトークン所持を検証することで要求者アイデンティティを検証する主体。検証するために、トークンとリンクされる要求者のクレデンシャルの検証と状態チェックを行う必要がある。

- リライングパーティー（Relaying Party）
  加入者のクレデンシャルを信頼し、業務処理実行や情報、システムに対してのアクセス権を与える主体。

- PIN（Personal Identification Number）
  10 進数のみを含むパスワード。

- トークンの所持と管理（Possession and Control of a token）
  認証プロトコルにおいてトークンの活性化と利用が可能であること。

- 所持証明プロトコル（Proof of Possession protocol）
  要求者が検証者に対し、トークンの所持と管理を証明するプロトコル。

- アサーション（Assertion）
  検証者よりリライングパーティーへ送られる、加入者のアイデンティティ情報を含んだ情報。

(2) 電子認証のモデル

NIST ガイドラインでは、認証に関連した役割を細かく規定している。図 4.22 にあるのがそのモデル概観である。

まず認証のシステムへの参加を希望するユーザ（申請者）は、登録機関 RA に対し CSP の加入者になることを申請する。その際に RA に対し申請者はアイデンティティの証明を行う。RA によってアイデンティティの証明がなされたら RA は CSP に対しその申請者のアイデンティティを保証する。RA の保証により、CSP は申請者を加入者とする。CSP は加入者に対し、クレデンシャルとトークンの発行もしくは登録を行う。トークンとクレデンシャルは CSP が発行してもよいし、加入者がすでに持っているものを登録してもらってもよい。

CSP の加入者となったユーザは、認証システムにおいて何らかのサービスを受ける資格を得たことになる。加入者は、サービスを提供する主体であるリライングパーティーからサービスを受ける場合、まず検証者に対して認証の要求を行う。この場合、加入者は検証者に対しての要求者という呼びかたをされる。検証者と要求者間での認証のプロセスは、認証プロトコルを通して行われる。検証者は、要求者がトークンの所持と管理をしているかを確認し、要求者のアイデンティティを確認する。

実際にサービスを提供するリライングパーティーは、検証者による認証要求の結果をアサーションとして受け取る。そのアサーションにより要求者に対して提供するサービスの決定を行う。

これらが一連の電子認証のモデルとなっている。

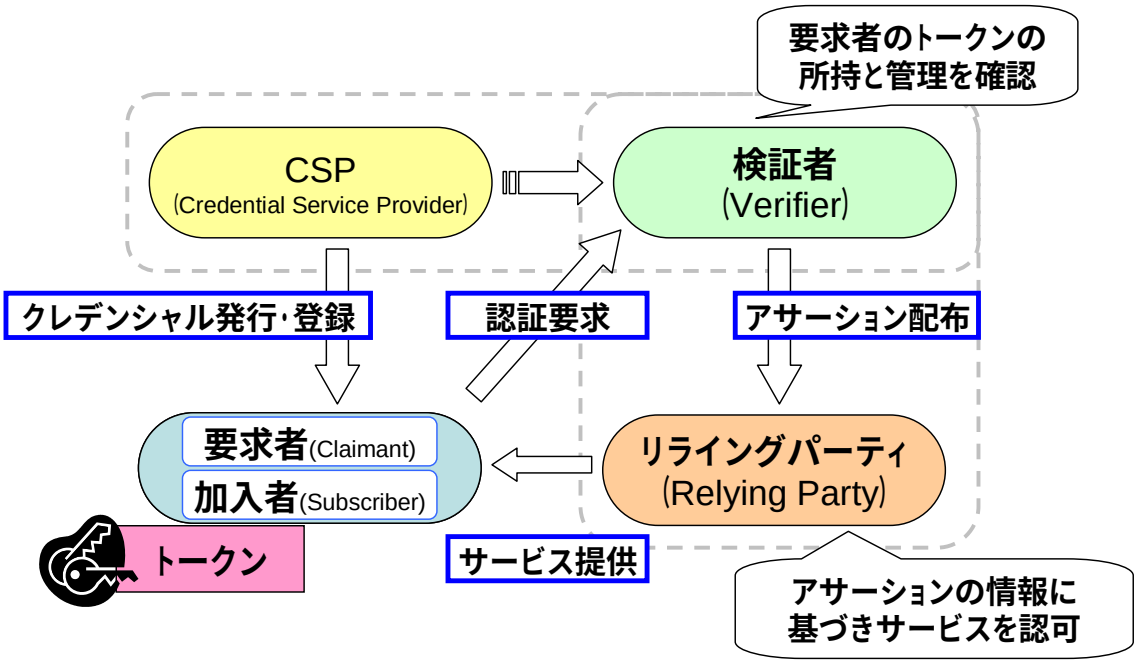


図 4.22　認証システムを構成する主体

電子認証のモデルにおいて役割は細かく分けられているものの、それらが必ずしも分離している必要はない。例えば図 4.22 では RA の記述がないが、実際は CSP と関連の深い役割であり一般的には同一主体における別作業機構として運用されていることから図上では省略してある。また検証者とリライングパーティーが同じ役割を示す状況、つまり認証とサービスを同じ主体が行う場合も十分にある。また RA、CSP、検証者、リライングパーティーが全て同じ主体によって運営されることもある。

(3) トークン

要求者のアイデンティティ認証を行うときに、要求者が所持そして管理していることがわかる何らかの物をここではトークンと言う。要求者のアイデンティティ認証を行う場合、その認証要素は 3 つからなる。その 3 つを以下に挙げる。

- 記憶：何を知っているか（Something you know）
- 所持：何を持っているか（Something you have）
- 生体情報：誰であるか（Something you are）

「何を知っているか」は例えばパスワード等がこれにあたり、また「何を持っているか」は社員証等 ID を示すものや暗号鍵の所持等がこれにあたる。「誰であるか」は生体情報に関するもの等があたる。当然これらに対してはそれぞれに異なる脅威が潜んでおり、それらを整理することで対策をしなければならない。記憶はそれを他人に知られてしまえば認証の要素として意味を失うものであるし、所持も盗難や複製等の脅威を持つ。生体情報は他に比べて脅威は少ないかもしれないが、複製という脅威は存在する。さらに生体情報は取替え可能な情報ではないため、一度漏洩した場合の影響も大きく、特に注意すべき脅威である。

トークンは、これらの要素の 1 つ以上を持つものである。例えばこれら 3 つの要

素から複数の要素を利用するシステムは、当然単独の要素しか利用しないシステムよりも強固であることが言え、保証レベルが高くなれば複数の要素、特に 2 つの要素を用いた認証（2 要素認証）を用いることが要件となる。また脅威に対する対策としては、盗難を困難にする機構や、盗難されても利用あるいは情報の開示を困難にする機構等の物理的なセキュリティメカニズムを持つことも対策となる。他の対策としては、複雑なパスワードの導入や、システムとネットワークでのセキュリティコントロールを行うこと等が挙げられる。

e-Authentication イニシアチブでは 4 種類のトークンを扱っている（表 4.5）。パスワードトークンはいわゆるパスワードや PIN といった要求者が記憶する秘密情報を指す。ワンタイムパスワード（OTP）デバイストークンは認証で用いる OTP を生成するハードウェアであり、入力パッドや生体情報リーダにより活性化させ OTP を生成させる 2 要素認証として利用される。ソフトウェアトークンは HDD や CD-ROM 等ディスクや他メディア上に格納された暗号鍵のことを指す。鍵自体はそのままでは利用できず、パスワード等により活性化されるような 2 要素認証で用いるべきである。ハードウェアトークンは、暗号鍵を格納したハードウェアデバイスであり高いセキュリティを実現する。ハードウェアトークンとソフトウェアトークンに関しては、NIST ガイドライン上で FIPS 140-2[4] 認定が必須とされている。FIPS 140-2 に関しては「参考資料：暗号モジュール評価基準 FIPS 140-2」で解説しているのでそちらを参考願いたい。

表 4.5　トークンの種類

トークンの種類	概要
パスワードトークン	文字列等
ワンタイムパスワードデバイストークン	ワンタイムパスワードを生成するハードウェア
ソフトウェアトークン	メディア等に格納された暗号鍵
ハードウェアトークン	特別なハードウェアデバイスに格納された暗号鍵。要 FIPS140-2 認定。

各トークンはセキュリティ面を考えそれぞれ利用できる保証レベルが定められている（表 4.6）。パスワードトークンは使いやすい反面、危険であるためにレベル 3 以上では使用が認められていない。レベル 3 以上に関しては 2 要素認証が必須となっており、ハードウェアトークンのみがレベル 4 での使用を認められている。

表 4.6　保証レベルごとの利用可能トークン

トークンの種類	レベル 1	レベル 2	レベル 3	レベル 4
ハードウェアトークン	√	√	√	√
ワンタイムパスワードデバイストークン	√	√	√	
ソフトウェアトークン	√	√	√	
パスワードトークン	√	√		

(4) 登録作業とアイデンティティ証明

リモートからの認証の場合、相手のアイデンティティ保証を考えるにあたっては、システムへの登録作業とそれにかかわるアイデンティティの証明も重要な部分となっている。アイデンティティ証明の保証を低いレベルで行い保証の高いトークンと認証プロトコルを提供しても全体としては低い保証の認証しか得られることができない。

各保証レベルにおける登録の要件を考えるには、まず登録時の脅威を考慮しなければならない。登録時の脅威を以下に挙げる。

- 登録者へのなりすまし
- 登録者本人による事後否認
- 登録基盤の不正・侵害

NIST のガイドラインでは登録基盤の不正・侵害に関しては対象外とし、なりすましと事後否認にのみ焦点を絞り脅威とその対策を考慮している。ユーザ（申請者）は RA に登録申請を行い、審査の結果 CSP の加入者として登録されるが、実際の登録にあたりその申請者のアイデンティティ保証ができるように以下のことが要求される。

- 登録申請者の主張する属性を持つ人物が存在し、それが唯一の人物を識別するのに十分である。
- トークン登録者が ID に示された人物である。
- 登録申請者は登録の事実を事後否認できない。

e-Authentication イニシアチブでは登録時に直接本人が登録に訪れるケースとリモートからの登録の双方を認めているが、保証レベル 4 ではリモート登録を認めていない。各保証レベルにおける登録要件を表 4.7 に示す。

表 4.7　保証レベル別登録作業要件

	直接登録	リモート登録
レベル 1	要件なし	要件なし
レベル 2	政府機関の発行する写真つき ID（住所や国籍付き）。ID の正しさと写真と申込者の一致を確認し、住所の確認が取れたら発行。	政府機関の発行する ID の番号と、金融機関の口座番号。それぞれ該当機関へ照会、名前・生年月日・住所・その他個人情報を確認。住所へ通知を送付するか、住所確認後の発行、または住所への連絡後発行。
レベル 3	政府機関の発行する写真付き ID。ID について該当機関へ照会。ID 番号・生年月日・住所・その他個人情報を確認。住所を確認後、発行。	政府機関の発行する ID 番号と金融機関の口座番号。それぞれ該当機関へ照会、名前・生年月日・住所・その他個人情報を確認。住所確認後の発行、または住所への電話連絡（要録音）後発行。
レベル 4	レベル 3 に該当する ID や口座を 2 つ必要とする。一番主要なものは公的な写真付き ID であること。主要なものに関して該当機関へ照会。写真比較、ID 番号・生年月日・住所を記録。2 つ目に関しては、ID の正しさと写真と申込者の一致を確認、あるいは金融機関へ照会し名前・生年月日・住所・その他個人情報を確認。生体情報を記録（否認防止の為）。住所の確認。以上を終えて初めて発行。	不許可

(5) 認証プロトコル

認証プロトコルは、その認証モデルにおいて CSP の加入者がサービス提供者に対してサービスを受けるべく、その認証を検証者に依頼する作業工程である。検証者は、要求者がトークンの所持と管理を行っていることを検証し、その結果の情報をサービス提供者であるリライングパーティーにアサーションとして返す。リライングパーティーはアサーションの情報に基づき要求者（加入者）に対してサービスを提供する。

本節では認証プロトコルにおけるレベル別技術要件を示す。技術要件を示すにあたり、「クレデンシャルの状態（有効期間、失効）」「アサーション」「長期共有機密情報の保護」「パスワード」の 4 つの視点よりそれぞれ要件を示している。まず技術要件に先立ち認証プロトコルの脅威とその対策を考える。その後、4 つの視点からの認証メカニズム要件を示す。

(a) 認証プロトコルの脅威と対策

認証プロトコルに対する脅威としては、盗聴、なりすまし、セッションハイジャックがある。セッションとは 2 者による通信の単位であり、例えば HTTP ではサーバとクライアントのデータ転送が通信しどちらかが切断するまでの一連の通信のことを言う。

盗聴は一般的にはトークンの取得を狙って行われる。なりすましは、要求者になりすまして推測したトークンを試行するものと、検証者になりすまして正しい要求者からトークンを窃取するものの 2 つのケースが存在する。またセッションハイジャックにも 2 つのケースが存在する。その双方ともが検証者から機密情報を窃取、または検証者へ不正な情報を入力あるいは出力することを目的としている。1 つ目のケースが要求者になりすますケースで、2 つ目のケースがリライングパーティーになりすますケースである。

脅威に対する対策もやはりそれぞれの脅威に従っていくつかの対策が存在する。例えば、暗号化等盗聴耐性のあるプロトコル設計をすることで盗聴への対策を行う。またパスワードの推測攻撃に対する対策としては、エントロピーの高いパスワードの使用や、パスワードの試行回数を制御する等の対策が可能である。さらに、前の認証メッセージを記録して再送することで認証を通過するリプレイ攻撃に対しては、同じ主体が認証を行う場合でもメッセージが異なるようなプロトコルを設計することで対策ができる。またセッションハイジャックの対策としては、メッセージ内容が挿入や消去あるいはルート変更されている場合に検知が可能なようにセッションごとに共有する秘密情報を利用することで対策が可能である。

その他の脅威としては、不正なコードを利用した攻撃により認証トークン自身を侵害することや、要求者（加入者）、CSP、検証者等の認証に参加する主体自身への侵入行為を行うこと、またソーシャルエンジニアリングや、「ショルダーサーフィン」と呼ばれる肩越しからの覗き見、そして故意にトークンを侵害する等の脅威があるが、これらの脅威は NIST ガイドラインでは認証プロトコルの脅威とは考えず、対象外としている。

(b) 認証プロトコル技術要件

ここでは認証プロトコルの技術要件を示す。ここではトークンはすでに登録されているものとし、またアイデンティティ確認と登録もすでにされているものとする。技術要件は以下に示す 4 つの視点より規定される。

- クレデンシャルとトークンの管理
- アサーション発行
- 長期共有秘密情報（Long-Term Shared Secret）管理
- パスワード強度

クレデンシャルとトークンは、その有効期間や状態、失効に関しての要件がレベル別に示される。さらに、リライングパーティーが受け取るアサーションの発行に関しての要件がある。長期共有秘密情報は制御や格納に関しての要件、最後にパスワードはその強度についての要件が示される。

- クレデンシャルとトークンの管理

  クレデンシャルとトークンの技術要件として、その有効期限、状態、失効等が挙げられている。要件としては検証可能状態の有無や、クレデンシャルやトークンが利用不可能な状態になった後の失効処理までの時間等がある。検証可能な状態とは、失効リストやオンライン検証サーバの存在等があたる。表 4.8 に要件を示す。レベル 1 では規定は特にない。レベル 2 以上では、クレデンシャルとトークンの検証が可能になっていなければならず、また失効までの時間も定められている。レベル 4 ではさらに機密情報の扱いや、一時的あるいは短時間の暗号鍵の有効期間にも触れられている。

表 4.8　保証レベル別クレデンシャルとトークン管理要件

	クレデンシャルとトークンの有効期限、状態、失効
レベル 1	（規定なし）
レベル 2	・CSP はクレデンシャル検証のための安全な仕組みを提供しなければならない。 ・クレデンシャルやトークンの 72 時間以内の失効。
レベル 3	・CSP はクレデンシャル検証のための安全な仕組みを提供しなければならない。 ・クレデンシャルやトークンの 24 時間以内の失効。
レベル 4	・CSP はクレデンシャル検証のための安全な仕組みを提供しなければならない。 ・クレデンシャルやトークンの 24 時間以内の失効。 ・機密情報の送信は暗号化され、一時的あるいは短時間の暗号鍵の有効期間は 24 時間以内。

- アサーション発行

  リライングパーティーが受け取るアサーションの要件を表 4.9 に示す。レベル 1 以上においてアサーションは信頼できる主体からのデジタル署名が付与されているか、または信頼できる主体から安全なプロトコルを通じて直接取得することが要件とされている。ここで信頼できる主体とは検証者等を指す。レベル 2、3 ではさらにアサーションが発行されてからの有効期限が決められている。レベル 4 については NIST ガイドライン中には記述がなく、アサーションが利用できるかどうかも判断できないが、利用できないと考えたほうが妥当であろう。

表 4.9　保証レベル別アサーション要件

	リライングパーティーが受け取るアサーション要件
レベル 1	・(a)、(b) いずれかの要件を満たす。 (a) 信頼できる主体からのデジタル署名付き (b) 信頼できる主体から安全なプロトコルを通じての直接取得
レベル 2	・(a)、(b) いずれかの要件を満たす。 (a) 信頼できる主体からのデジタル署名付き (b) 信頼できる主体から安全なプロトコルを通じての直接取得 ・発行より 12 時間までの有効期限
レベル 3	・(a)、(b) いずれかの要件を満たす。 (a) 信頼できる主体からのデジタル署名付き (b) 信頼できる主体から安全なプロトコルを通じての直接取得 ・発行より 2 時間までの有効期限
レベル 4	（記述なし）

- 長期共有秘密情報管理

長期共有秘密情報の保護に関する要件を表 4.10 に示す。全てのレベルにおいて、必要とされるアプリケーションと管理者のみがアクセスできるようにアクセス制御により保護されていなければならない。長期共有秘密情報の格納については、ハッシュ化や暗号化、さらには暗号に用いる暗号モジュールに関しての規定、秘密分散法の適用等レベルごとに詳細にわたっている。レベル 3 とレベル 4 の要件は同じとなっている。なお暗号モジュールの評価基準 FIPS140-2 に関しては「参考資料：暗号モジュール評価基準 FIPS 140-2」を参照されたい。

また、一時セッション鍵の生成については、その方法や鍵強度等も別途定められている。

表 4.10　保証レベル別長期共有秘密情報要件

	長期共有秘密情報の保護
レベル 1	・秘密情報ファイルは任意のアクセス制御により制限される。 ・秘密情報ファイル内には平文パスワードを含まない。
レベル 2	・CSP と要求者（加入者）以外には秘密情報は開示されない（セッション用の一時共有秘密情報は CSP より検証者に渡される）。 ・秘密情報ファイルは任意のアクセス制御により制限される。 ・以下（a）、（b）、（c）いずれかの要件を満たす。 (a) ファイル内には平文パスワードを含まない。 (b) パスワードと Salt[3]またはユーザ名を連結し、認定アルゴリズムによりハッシュ化しファイルに格納。 (c) 認定アルゴリズムにより暗号化しファイルに格納。
レベル 3	・秘密情報ファイルは任意のアクセス制御により制限される。 ・秘密情報ファイルは暗号化される。 ・以下（a）、（b）、（c）いずれかの要件を満たす。 (a) 鍵は FIPS 140-2 レベル 2 以上の認定を受けたハードウェアモジュールか FIPS140-2 レベル 3 以上の認定を受けたモジュールに格納されている。 (b) 秘密情報は FIPS 140-2 レベル 2 以上の認定を受けたハードウェアモジュールか FIPS140-2 レベル 3 以上の認定を受けたモジュールに格納され、平文ではエクスポートされない。 (c) 秘密情報は m 個に秘密分散され、そのうち n 個（2 以上 m 以下）以上の分散情報により認証を可能にする。 ・長期共有秘密情報より生成される一時セッションキーは第 3 者の検証者へ渡されるが、長期共有秘密情報自身は渡されない。
レベル 4	・秘密情報ファイルは任意のアクセス制御により制限される。 ・秘密情報ファイルは暗号化される。

[3] Salt：パスワードのハッシュ化の際、ハッシュ化の前にパスワードに連結する乱数値。Salt の利用により、より乱数化された値（鍵）が生成可能となる。

	・以下（a)、(b)、(c）いずれかの要件を満たす。 (a) 鍵は FIPS 140-2 レベル 2 以上の認定を受けたハードウェアモジュールか FIPS140-2 レベル 3 以上の認定を受けたモジュールに格納されている。 (b) 秘密情報は FIPS 140-2 レベル 2 以上の認定を受けたハードウェアモジュールか FIPS140-2 レベル 3 以上の認定を受けたモジュールに格納され、平文ではエクスポートされない。 (c) 秘密情報は m 個に秘密分散され、そのうち n 個（2 以上 m 以下）以上の分散情報により認証を可能にする。 ・長期共有秘密情報より生成される一時セッションキーは第 3 者の検証者へ渡されるが、長期共有秘密情報自身は渡されない。

- パスワード強度

パスワードについてはその強度に関して要件が定められている。パスワードの強度はユーザ名が既知である等の前知識の有無により変わるが、レベル 1 では前知識なしでのパスワード推測の成功確率が 1024 回に 1 回未満であることが要件になっている。レベル 2 では同様に確率が 16384 回に 1 回未満であることが要件になっている。レベル 2 ではさらに、前知識がある場合でも最低限 10 ビットのエントロピー（前知識なしで 1024 回に 1 回の成功確率相当）を持つパスワード強度が要件として定められている。

なおレベル 3 と 4 に関してはパスワードの利用は認められていない。

表 4.11　保証レベル別パスワード強度要件

	パスワード強度
レベル 1	・前知識無し（ただしユーザ名既知）の状態でオンラインパスワード推測の成功確率が 1/1024 を超えない。
レベル 2	・前知識無し（ただしユーザ名既知）の状態でオンラインパスワード推測の成功確率が 1/16384 を超えない。 ・少なくとも 10 ビットのエントロピー。
レベル 3	（利用できない）
レベル 4	（利用できない）

(6) 保証レベル別の技術要件概要

ここまでにおいて、電子認証システムを構成する各要素によって保証レベルごとの要件を解説した。ここでは、それらの要素の要件を保証レベルごとにまとめ、各保証レベルで必要とされる技術要件の概要を示す。

- レベル 1

アイデンティティ証明はないが、同一の要求者が保護されている処理またはデータにアクセスしているという保証をする。広範囲の認証技術が利用でき、レベル 2 以上のどのトークン方法も利用可能である。認証の成功には、要求者がその

トークンを制御していることをセキュアな認証プロトコルを通じて証明することが必要である。

このレベルでは、ネットワークを介して平文のパスワードや秘密は送信されない。また、盗聴者によるオフライン攻撃を阻む暗号方法も必要とされない。例えば、単純なパスワードチャレンジレスポンスプロトコルは許可される。多くの場合において、盗聴者は直接的な辞書攻撃によりパスワードを見つけることが可能である。

長期共有秘密情報が検証者に漏れる。認証成功時の要求者に関して発行されたアサーションも、認定された方法を利用してリライングパーティーにより暗号的に認証される。または、アサーションはセキュアな認証プロトコルを通じて信頼できる主体より直接得られる。

- レベル 2

  レベル 2 は単一要素のリモートネットワーク認証を提供する。アイデンティティ証明の要件がある。広範囲の認証技術が利用可能である。パスワードや PIN と同様に、レベル 3 以上のどのトークン方法も利用可能である。認証の成功には、要求者がそのトークンを所持・管理していることをセキュアな認証プロトコルを通じて証明することが必要である。盗聴者、リプレイ、オンライン推測攻撃は防御される。

  長期共有秘密情報が利用されるのであれば、その情報は任意の主体に漏らされることはない。ただし、要求者と、CSP により運営される検証者は除く。ただ一時的なセッション共有鍵は CSP により独立した検証者に提供される。認証成功時の要求者に関して発行されたアサーションも、認定された方法を利用してリライングパーティーにより暗号的に認証される。または、アサーションはセキュアな認証プロトコルを通じて信頼できる主体より直接得られる。

- レベル 3

  レベル 3 は複数要素のリモートネットワーク認証を提供する。アイデンティティ証明の手続きは情報や物を識別する検証が要求される。レベル 3 の認証は、暗号プロトコルを通しての鍵かワンタイムパスワードの所持の証明に基づく。レベル 3 の認証では、盗聴・リプレイ・オンライン推測・検証者なりすまし・中間者攻撃（man-in-the-middle）等の脅威により主な認証トークンの侵害を防ぐ暗号的な耐性メカニズムが要求される。また、最低 2 つの認証要素が要求され、ソフトウェアトークン、ハードウェアトークン、ワンタイムパスワードデバイストークンといった 3 種のトークンが利用される。

  認証は要求者がそのトークンを制御していることをセキュアな認証プロトコルを通じて証明することが必要であり、パスワードか生体情報によりまずトークンを解除しなければならない。または、2 要素認証を確立するためにセキュアな認証プロトコル上でパスワードも利用しなければならない。長期共有秘密情報が利用されるのであれば、その情報は任意の主体に漏らされることはない。ただし、要求者と、CSP により運営される検証者は除く。ただ一時的なセッション共有鍵は CSP により独立した検証者に提供される。認定暗号技術がすべての動作に利用される。また、認証成功時の要求者に関して発行されたアサーションも、認定された方法を利用してリライングパーティーにより暗号的に認証される。または、

アサーションはセキュアな認証プロトコルを通じて信頼できる主体より直接得られる。

- レベル 4

レベル 4 は最も高い実際的なリモートネットワーク認証保証を提供する。レベル 4 の認証は、暗号プロトコルを通しての鍵の所持証明に基づく。レベル 4 はレベル 3 と似ているが、FIPS 140-2 暗号モジュール認定を受けたハードウェアトークンのみが許可される。その後の重要なデータ送信は認証プロセス経由の鍵により認証される。トークンは、FIPS140-2 のレベル 2 以上の認定を全体で受け、さらに物理セキュリティでは FIPS140-2 のレベル 3 以上の認定を受けたハードウェアモジュールであるべきである。物理的トークンの要求により、それらは容易にはコピーできず、FIPS140-2 はオペレータ認証のレベル 2 以上を要求するので、このレベルは良い 2 要素リモート認証を保証する。

また、主体間の全機密データ送信と全主体の認証に強力な暗号の認証を必要とする。公開鍵と共通鍵の両方とも利用する。認証は要求者がそのトークンを制御していることをセキュアな認証プロトコルを通じて証明することが必要である。プロトコルの脅威としては、盗聴・リプレイ・オンライン推測・検証者なりすまし・中間者攻撃が防御される。長期共有秘密情報が利用されるのであれば、その情報は任意の主体に漏らされることはない。ただし、要求者と、CSP により運営される検証者は除く。強力な認定暗号技術が全ての動作において利用される。すべての重要なデータ送信は認証プロセス経由の鍵により認証される。

さらに、参考として各保証レベルにおいて利用可能なトークンタイプを表 4.12 に、対策されるべき脅威を表 4.13 に、パスワード強度を表 4.14 に、またその他重要な差異を表 4.15 に示す。

表 4.12　利用可能なトークン

トークンタイプ	レベル 1	レベル 2	レベル 3	レベル 4
ハードウェアトークン	√	√	√	√
ワンタイムパスワードデバイストークン	√	√	√	
ソフトウェアトークン	√	√	√	
パスワードトークン	√	√		

表 4.13　各レベルで対策される脅威

対策	レベル 1	レベル 2	レベル 3	レベル 4
オンライン推測攻撃	√	√	√	√
リプレイ攻撃	√	√	√	√
盗聴		√	√	√
検証者のなりすまし			√	√
中間者攻撃			√	√
セッションハイジャック				√

表 4.14　パスワード強度要件

	レベル 1	レベル 2
攻撃対象を定めたパスワード推測攻撃（前知識なし）	1/1024	1/16384
攻撃対象を定めないパスワード推測攻撃		1/1024

表 4.15　その他の要件

	レベル 1	レベル 2	レベル 3	レベル 4
CSP と検証者は第 3 者へ共有秘密情報を開示しない		√	√	√
複数要素認証			√	√
機密データ送信での認証				√

4.4.4 電子認証ガイドライン関連動向

本節では、NIST ガイドラインに関連する動向を紹介する。まず近年の米国動向として、政府機関での ID カードに関する動向、医療系での動向等を紹介する。

また、OMB ガイダンスや NIST ガイドラインは米国以外でも大きな影響を与えており、各国での関連する動向もまとめた。

(1) 米国政府 ID カード関連動向

2004 年 7 月に大統領によりサインされた大統領令 HSPD-12[5] は、テロ対策として連邦政府施設等へのアクセス管理と、連邦政府の職員と契約者の本人確認の厳格さを定めている。それを受けて NIST では FIPS 201 “ 連邦組織の従業員と契約者の PIV（個人アイデンティティ検証）”[6] を策定、2005 年 2 月末に発表した。FIPS（Federal Information Processing Standard）は NIST が発行する規格で米国連邦政府機関における調達基準となっており、その影響は極めて大きい。さらにその影響は米国のみにとどまらず、世界的にも事実上の標準規格になる場合もある。その FIPS 201 では、認証の保証レベルとして OMB ガイダンスと NIST ガイドラ

インを参照している。
さらに FIPS 201 では発行されるクレデンシャルとして IC カードを挙げている。その中で IC カードに関しての規格も示され、IC カードの業界への影響も大きなものになっており、業界団体である SmatCard Alliance でもたびたび FIPS 201 に関する議論が交わされている。FIPS 201 ではその技術要件として NIST ガイドラインを参照しており、NIST ガイドラインもまた注目を浴びている。

(2) 米国医療系動向
近年、医療の世界でも情報セキュリティへの要求は高まっており、とくに患者の個人情報等機密度の高い情報を扱う際の制約が厳しくなっている。米国では 1996 年に医療保険の相互運用性と説明責任に関する法律（HIPAA：Health Insurance Portability and Accountability Act）が制定され、患者の情報とプライバシーの高いセキュリティを求めている。さらに、HIPAA ではセキュリティやプライバシー等に対して基準あるいは規制を設けている。
NIST では HIPAA の基準の中の 1 つ HIPAA セキュリティルールについての実装ガイドライン（NIST Draft SP 800-66）[7] の草案を作成している。その文書の中で、情報へのアクセス制御や人等の認証に関して、NIST ガイドラインを参照している。

(3) その他の米国動向
米国においてはその他にも NIST ガイドラインを参照している事例が多い。全米州 CIO 協議会（NASCIO）のプライバシー委員会は、2004 年 12 月に「電子認証とプライバシーの問題」に関しての調査報告を行った。そこでは州政府と電子取引をする人を認証するにはどのレベルの本人確認を行えば十分かという議論がされており、そこで OMB ガイダンスや NIST ガイドラインが参照されている。
テキサス州では EA（Enterprise Architecture）の一環として ACE（Architecture Components for the Enterprise）を行っている。EA とは効率のよい組織運営のための方法論で、業務手順や情報システム、組織の最適化等を行う。2004 年 7 月、ACE の小委員会の 1 つである相互運用性小委員会において NIST ガイドラインをベストプラクティスとして採用したい旨が、同じく小委員会のセキュリティ小委員会内のレビューの結果、全員一致の賛同が得られた。

(4) 他の海外動向
NIST ガイドラインは米国だけではなく、他の国の電子認証動向にも影響を及ぼしている。ここでは米国以外での NIST ガイドラインの参照動向を伝える。
ヨーロッパの情報社会に関する標準化活動の統制を行う団体 CEN/ISSS に、IC カードを利用した電子認証に関する Workshop がある。そこでは電子認証に関していくつかの文書を公開しており、その中の「ヨーロッパ市民の電子 ID に向けて」では電子 ID カードを利用した電子認証等、特に電子政府での利用に貢献するためのビジョン[8] が書かれている。そこではビジョンを実現させるための技術要件の記述もあり、NIST ガイドラインを参照している。文書内でも OMB ガイドラインと同様に 4 段階の保証レベルを規定しており、影響の強さをうかがわせる。
OMB ガイダンスや NIST ガイドラインを参照としていない文書の中でも、関連が深いものも多い。英国では電子政府戦略の 1 つとして電子認証があり、そこで電

子認証における登録と認証についてのガイドラインを示している。OMB ガイダンスや NIST ガイドラインは直接参照していないものの、4 段階の保証レベルの規定等、共通項も多い。またオーストラリア政府の電子認証フレームワーク草案[9] では 4 段階の評価という視点から電子認証が示されており、内容的にも NIST ガイドライン等の影響が見て取れる。さらにニュージーランドの電子政府では信頼レベルという 4 つのレベルを示した認証のベストプラクティスのフレームワークを文書化しており[10] 、参照こそないものの技術要件の内容等で同様に NIST ガイドラインの影響を見ることができる。

4.4.5 電子認証ガイドラインに関する考察

本節では米国政府機関のための電子認証ガイドラインを中心に解説し、さらにその動向等の調査も付記した。

米国の行政管理予算局（Office of Management and Budget：OMB）が策定した OMB ガイダンスでは認証における 4 つの保証レベルを定義し、それぞれのレベルにおける要件を述べている。また連邦機関がシステムを構築する際に保証レベルと認証方法を決定するためのプロセスも提示している。OMB ガイダンスで示された 4 つの保証レベルでの技術要件を示しているのが、NIST が発行した NIST ガイドラインである。

OMB ガイダンスで示された 4 つの保証レベルは、潜在的な被害と影響度とそのリスク、さらにはその発生確率により決定づけられる。潜在的な被害と影響度として 6 つの要素を挙げ、それぞれについてリスクを 3 段階で考慮し、4 つの保証レベルへとマッピングしている。

NIST ガイドラインでは OMB ガイダンスで示された 4 つの保証レベルの技術要件を示している。技術要件はトークン、登録作業とアイデンティティ証明、認証プロトコルの 3 つの視点より詳細に示されている。

これらの文書により、認証を必要とするシステムにおいて、適切な保証レベルを与える認証技術を選択することが可能になる。適切なレベルの認証技術を提供することの重要性は、現在の電子認証技術の利用においては理解がされていない部分であり、ともすれば高いレベルの認証だけをやればよいという考えを持ちがちな現状では優れた指標となるであろう。適切な認証のレベルを与え、適切なシステムが出来上がることが、あらためて電子認証をこれからの世の中の基盤として整備していくためには必要不可欠である。

現実に、OMB ガイダンスや NIST ガイドラインは米国内の公的分野においてすでに影響が出ている。さらにその影響は米国内にとどまらず、海外でもこれらが参照されているものもある。また実際に参照はされていなくとも、電子政府の認証として保証レベルを定め始めた国も多く、その中心にこれらの文書があるのは間違いないであろう。しかし、多くの認証クライテリアは人間の認証に関してのものであり、機器やネットワークコンポーネントの認証は考慮されていない。これから多くなることが予想されるこれらの認証に関してのクライテリアも望まれるところである。

明確な指標が存在することで電子認証が官民を問わず世の中全般にさらに浸透していく様子がうかがえる一方で、日本ではいまだこういった認証のクライテリアが存在しておらず、電子認証分野における検討が十分でないのが現状である。今後日本での認証クライテリア構築はもはや必須と言ってよく、早急な構築はサービスの提供者と享受者を問わずに望まれていることであろう。

日本での認証クライテリアを構築する際には、いくつもの考慮すべき点が存在する。そのひとつに、暗号モジュールの評価制度の問題がある。NIST ガイドラインでは、高いレベルの保証を持たせる場合に、そのトークンには FIPS 140-2 の認定を要求している。FIPS 140-2 の認定は日本でも数社が取得しているものの、米国の企業が認定を取得することに比べ、文書の作成や、認定機関との折衝等、困難な部分が見て取れる。その困難さは、日本に認定機関がないことが大きな原因であると考えられる。認証クライテリア確立を考慮した場合、高いレベルの保証には当然暗号モジュールの評価が不可欠になることから、これら認定機関についても考慮しなければならない。さらに、人間だけではなく機器やネットワークコンポーネントも包含した形で認証クライテリアが構築できれば望ましい。

4.4.6 参考資料：暗号モジュール評価基準　FIPS 140-2

米国では NIST が連邦政府情報処理規格（Federal Information Processing Standards：FIPS）を発行している。FIPS は政府の調達基準となっているために非常に影響が大きい。

FIPS 140-2 は暗号モジュールの安全な設計と実装のための要件を示しているものであり、FIPS 140 として発行されたものが改訂を繰り返し現在の FIPS 140-2 となっている。FIPS 140-2 では暗号モジュールに対して以下の観点から要件が示されている。

- 無権限の情報利用からの保護
- 重要な（Critical）セキュリティパラメータの保護
- 未検知改ざんの防止
- 認定セキュリティ手法の採用
- モジュール操作状態の表示（Indication）
- エラーの検知、表示

FIPS 140-2 は、13 の規定分野に関してそれぞれ要件を示している。また保護されるデータや使用状況等を考慮し、4 段階のセキュリティレベルを設けている（図 4.23）。認定を受ける製品は、それぞれの規定分野について項目別評価を受け、レベル付けされる。さらに 13 分野の中で一番低いレベルを全体評価のレベルとしている。

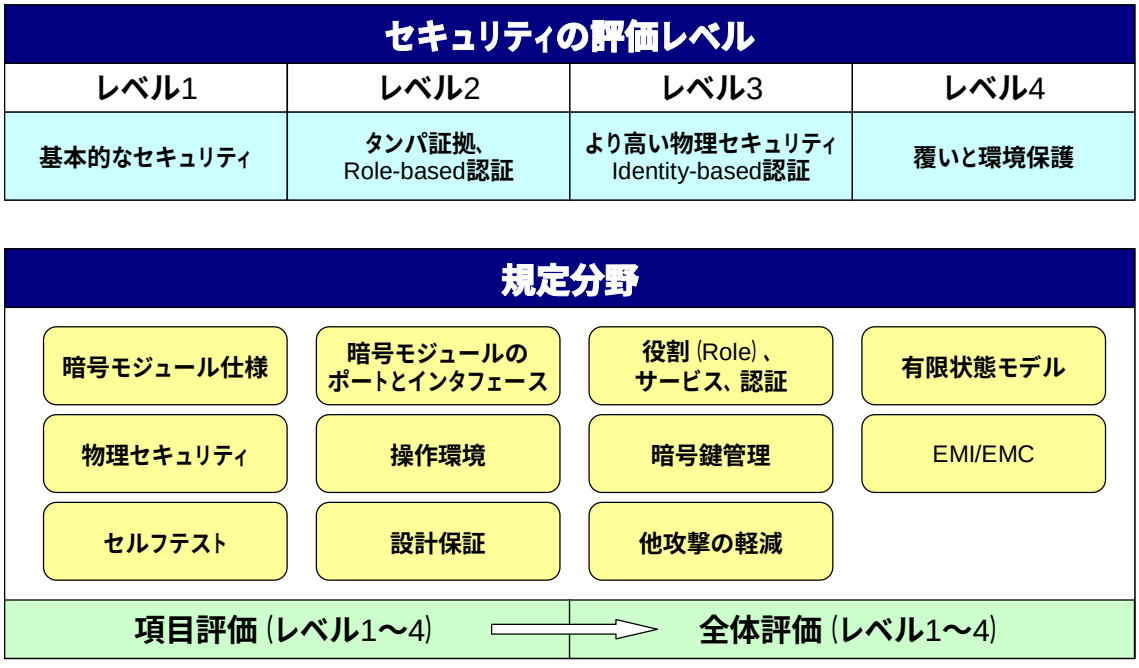


図 4.23　FIPS 140-2 の評価レベルと規定分野

FIPS 140-2 は米国にとどまらずカナダや英国でも標準として採用される等、さまざまな政府で採用されている。さらには公的機関にとどまらず民間でもその利用は広まっている。

NIST ガイドラインの中では、トークンにおいて、また、長期共有秘密情報の格納に関して FIPS 140-2 の認定が必要になる部分がある。

まずトークンについては、OTP デバイストークンとソフトウェアトークン、ハー

ドウェアトークンについて FIPS 140-2 の認定が要求される場合がある。それぞれのトークンで FIPS 140-2 の認定が要求されることはレベルにより異なる。

OTP デバイストークンは、保証レベル 3 での使用において、FIPS 140-2 全体レベル 1 以上の認定を受けた製品であることが要求される。なお OTP デバイストークンは保証レベル 4 での使用は認められていない。

ソフトウェアトークンも OTF デバイストークンと同様に、保証レベル 3 での使用において、FIPS 140-2 全体レベル 1 以上の認定を受けた製品であることが要求され、保証レベル 4 では使用が認められない。

ハードウェアトークンは保証レベル 3 と 4 について異なる FIPS 140-2 認定要件が課されている。保証レベル 3 では、全体でレベル 1 以上の FIPS 140-2 認定と「役割、サービス、認証」分野でのレベル 2 以上の認定が必要とされる。保証レベル 4 では、全体でレベル 2 以上の FIPS 140-2 認定と、物理セキュリティ分野でのレベル 3 以上の認定が必要とされる。

次に、長期共有秘密情報の格納に関しては、保証レベル 3 の長期共有秘密情報において、その格納は FIPS 140-2 のレベル 2 以上の認定を受けたハードウェア暗号モジュールあるいは FIPS 140-2 レベル 3 以上の認定を受けた暗号モジュールによって暗号化されていなければならない。あるいは、秘密情報自身が FIPS 140-2 のレベル 2 以上の認定を受けたハードウェア暗号モジュールあるいは FIPS 140-2 レベル 3 以上の認定を受けた暗号モジュールの暗号鍵として格納されていることでも可能である。

4.4.7 参考文献

[1] "Electronic Authentication Guideline", W. Burr, D. Dodson, T. Polk, June 2004, http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf

[2] "E-Authentication Guidance for Federal Agencies", J. Bolten, December 2003, http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

[3] "Standards for Security Categorization of Federal Information and Information Systems", Compouter Security Division, Information Technology Laboratory, NIST, Deceomber 2003, http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

[4] "Security Requirements for Cryptographic Modules", Information Technology Laboratory, NIST, May 2001, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[5] "Policy for a Common Identification Standard for Federal Employees and Contractor", G. Bush, August 2004, http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html

[6] "Personal Identity Verification （PIV） of Federal Employees and Contractors", Compouter Security Division, Information Technology Laboratory, NIST, February 2005, http://csrc.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf

[7] "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act （HIPAA） Security Rule", P. Bowen, A. Johnson, J. Hash, C. Smith, D. Steinberg, May 2004, http://csrc.nist.gov/publications/drafts/DRAFT-sp800-66.pdf

[8] "Towards an electronic ID for the European Citizen, a strategic vision", CEN/ISSS Workshop eAuthentication, October 2004, http://www.cenorm.be/cenorm/businessdomains/businessdomains/isss/activity/eauthstrategicvision.pdf

[9] "Australian Government Electronic Authentication Framework", Information Management Office, Australian Government, May 2004, http://www.agimo.gov.au/__data/assets/file/30609/AGAF_Overview_for_Business.pdf

[10] "Authentication for e-government:Best Practice Framework for Authentication", Authentication Team, E-government Unit, State Services Commission, April 2004, http://www.e-government.govt.nz/docs/authentication-bpf/bpf.pdf

4.5 e-Authentication

4.5.1 e-Authentication 概要

(1) e-Authentication の位置づけ

米国政府が提唱している e-Authentication イニシアチブでは、電子政府の FEA（連邦政府エンタープライズアーキテクチャ）に対応した認証フレームワークであり、政府機関を横断したシングルサインオン（SSO）の実現を目指している。複数の認証プロバイダーが連携するモデルであり、SAML 等の技術を統合している。

また、認証情報の連携対象を民間事業者に拡げることで、民間サービスと公的サービスとを連続的に利用することも可能とするものである。

e-Authentication と政府各組織との関係を図図 4.24 に示す

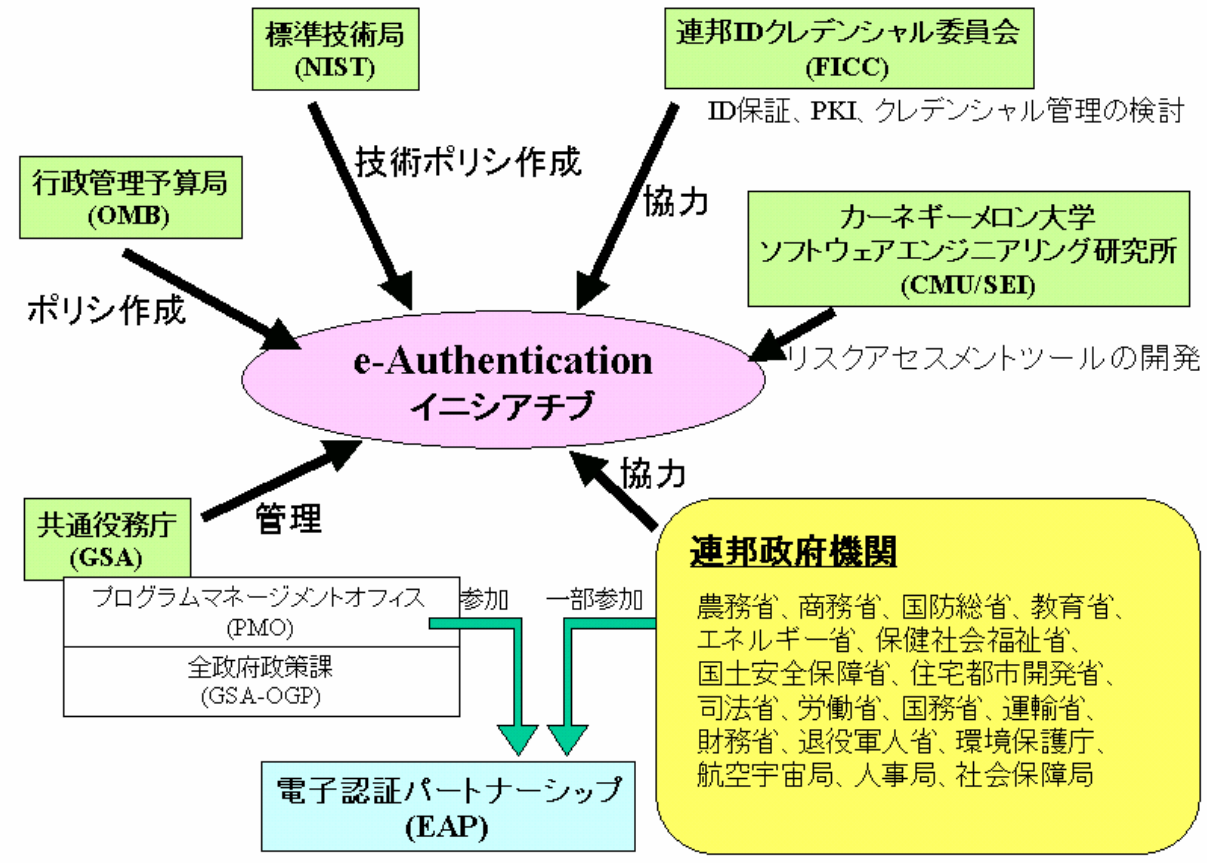


図 4.24 e-Authentication と各組織との関係

なお、e-Authentication では、利用者認証を必要とする各行政サービスに対して FirstGov によるポータルが提供され、また認証ゲートウェイにより認証窓口が一本化され、認証処理の一元化が図られている。

また、利用者の認証手段については、NIST の保証レベルに基づき、ID/パスワードや PKI に基づく認証等の手段が選択される。

(2) e-Authentication 目的

e-Authentication を適用することで、これまで各行政サービスが独自に決めていた認証手順やポリシーの基準が明確となり、行政サービス間の連携が容易となることが見込まれている。

e-Authentication の適用前後のイメージを図 4.25 に示す。

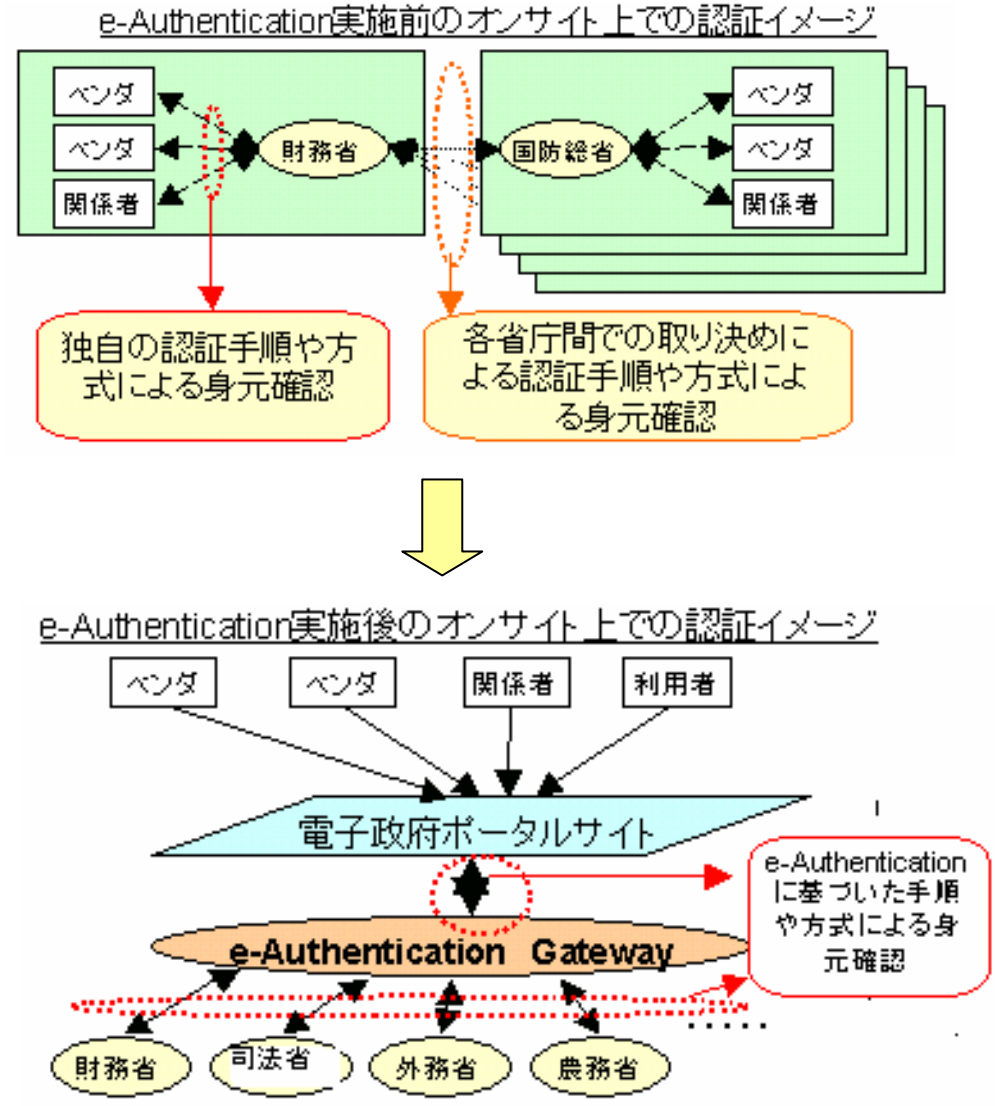


図 4.25　e-Authentication 実施前後の認証イメージ

また、e-Authentication では、以下の実現が期待されている。

(a) 「利用者の利便性の向上による e-Government の普及促進」

e-Government 構築の進展に伴い、複数のサービスがオンラインで利用可能となりつつある。しかし、個々のサービスが独自の認証手段を持ち、個別に利用者の管理を行ってしまうと、利用者はサービスごとに異なるインターフェイスを使い分け、異なる ID を使い分けることになり利便性は低下することが懸念される。

e-Authentication では、FirstGov によるポータルを経由することで認証が必要なサービスのワンストップ化と認証ゲートウェイによる認証処理の一元化と SSO により、サービスの利用者が認証手続の煩雑さから開放されることが期待される。

加えて、SAML や Liberty Alliance Project のフレームワークを活用し利用者の認証情報の連携を実現することで、個々のサービスにおいて利用者管理ポリシーの独立性は維持され、また共通 ID によるプライバシー問題の回避が図れるとされている。

(b) 「認証ポリシーやリスク分析手順、製品やサービスの認定等の共通化による民間企業、市民、政府の負担の軽減」

利用者をどのような手段で認証するかといった認証ポリシーや、個々のサービスにどういった認証手段が必要かといったリスク分析手順が一元的に管理されることで、認証を必要とするサービスを構築する民間企業や行政機関の負担が軽減される。

また、製品を相互接続性等に基づき認証する手続きも Interoperability Laboratory により管理され、製品の開発や製品の選択等の負担も軽減される。

(c) 「セキュリティ基準の明確化による安全性向上」

適切な認証メカニズムが明確となることで、各サービスに必要十分な認証レベルとの対応をとりやすくなり、セキュリティの改善が見込まれる。

なお、e-Authentication における認証対象は、e-Government システムの利用者（自然人）とされており、機器やサーバの認証は対象とされていない。

また、サービスの認可や、X.509 証明書を発行する認証局等の運営についても対象外とされている。

(3) e-Authentication の現在のステータス

現在の主な作業は、そのコンセプトの実証を行っている段階となっている。この中では、利用者のアイデンティティの連携（Federation）技術の実装も含まれている。

また、実証に際しては Interoperability Laboratory による関連する市販製品やサービスの相互運用性も検証され、検証されたものは、随時、認定がなされている。

具体的な情報は以下の通り。

- Grant.gov および eTravel. で SAML1.0 プロトコルを活用した、保証レベル 1 と 2 での ID 認証のパイロットテスト中

- FedTeDS と eOffer が政府指定ベンダーとのオファー提出等において、PKI 活用可能アプリケーションのパイロットテスト中

- 環境保護局の中央データ交換、 National Park Service のアプリケーションで電子署名を必要とするフォームのパイロットテスト中

- 財務省、退役軍人局で企業を含めた e-Authentication の導入のための土台のパイロットテスト保留中

- 財務省と共通役務庁で PKI レスポンスを SAML へ変換するトランスレータを活用して、パスワードによって保護されているリソースへアクセスする方法で、PKI クレデンシャルを使う可能性についてテスト中

4.5.2 e-Authentication のアーキテクチャ

(1) e-Authentication モデルの構成

e-Authentication の基本的なモデルとして、行政サービスを受ける際に他の行政機関の認証結果を利用することでサービスの利用を求めるというパターンがあげられる。この場合のモデルの構成を図 4.26 に示す。

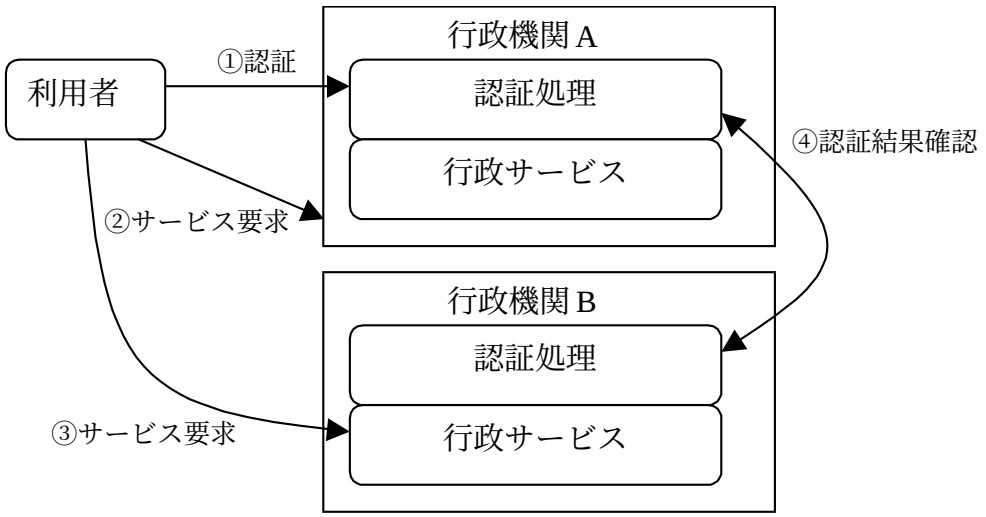


図 4.26　e-Authentication の基本的なモデル構成

これは、利用者が各行政機関の提供する認証機能を利用するモデルである。利用者にはよく利用する行政サービスがあり、そのサービスを起点として他のサービスに移る際に行政機関同士で認証結果（ログイン状態に関する情報等）を確認し合うことで、利用者に対して SSO を実現する。

このモデルの背景として、e-Government で提供される行政サービスのうちのいくつかは、既に多くの利用者が利用しており、そのサービスが提供する認証機能や利用者のアカウント管理の機構を活用することが、認証手段の共有には有効であるとの考え方がある。

しかし、上記のモデルではフレームワークに参加する行政サービスが増加すると、図 4.27 に示すように、認証情報の共有の仕組みが複雑になる可能性がある。

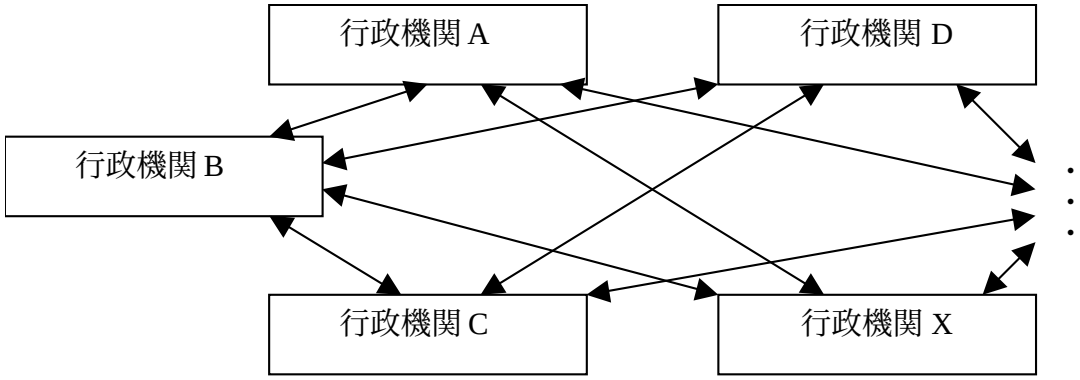


図 4.27　行政機関同士が相互にポリシーを共有する場合

そこで、図 4.28 に示すように、複数の行政サービスに対してハブの役割を持つ認証ゲートウェイを定義することで、行政サービスの追加や構成変更等の対応を容易とするとともに、利用者にとっても認証窓口が一本化されることで利便性が向上することとなる。

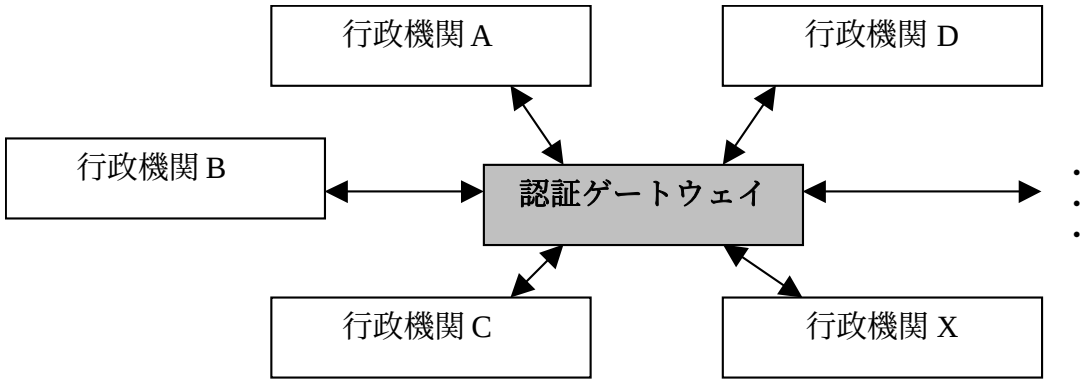


図 4.28　認証ゲートウェイを通じてポリシーを共有する場合

各行政サービスに対して共通の認証ゲートウェイを利用する場合のモデルを図 4.29 に示す。

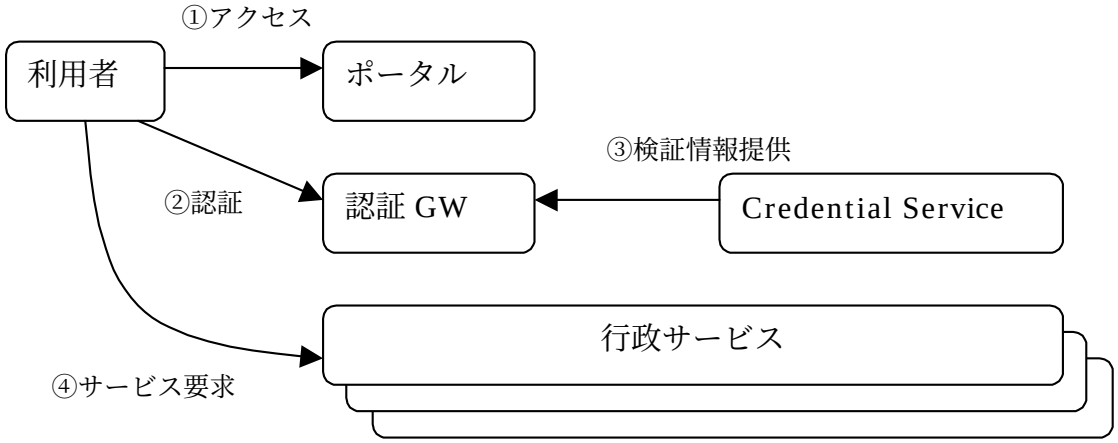


図 4.29　認証ゲートウェイを利用した利用モデル

利用者は各行政サービス共通の窓口であるポータルを経由し認証ゲートウェイに誘導され、そこで利用する行政サービスに応じた認証手段で認証される。
認証結果（ログイン状態に関する情報等）は、目的の行政サービスに伝えられ、利用者は行政サービスが利用可能となる。
なお、このモデルでの運用が始まったとしても、各行政機関が個別に認証する方法は併存して提供されることとなっている。

利用者が複数の行政サービスを一度の認証で利用する SSO のためには、認証ゲートウェイや各行政機関の認証機能と行政サービスの間で認証結果（ログイン状態に関する情報等）が伝達されなければならない。現時点では、その伝達手段として X.509 証明書を直接流通させ各行政サービスが共通の Validation サービスを利用する等して利用者の認証情報を共有する方法と、SAML のアサーションにより認証結果を共有する方法とを利用することとされている。
しかし、今後、SAML の複数バージョンのサポートや Liberty Alliance Project の仕様や WS-Federation 等の仕様との併存等、この伝達手段についても複数の方式を利用することが求められてくると考えられている。
これについては、図 4.30 に示すように、Scheme Translator と呼ぶサービスを仲介させ、そこで各行政サービスが必要とするプロトコルに変換し情報を共有するモデルも検討されている。

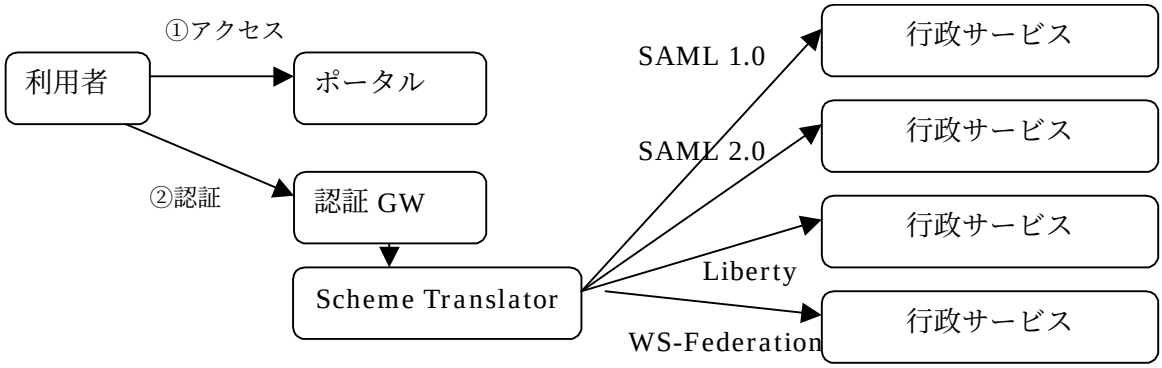


図 4.30　Scheme Translator を用いた利用モデル

(2) e-Authentication における認証の流れ

e-Authentication では、認証情報の流れとして複数のパターンに対応できることとされている。以下にその例を示す。

（参考：GSA:Technical Approach for the e-Authentication Service Component）

(a) 基本的な例

① 利用者はポータルサイト（FirstGov）にアクセスをする。
② 利用者は、アクセスしたい行政サービス（Agency Application）を選択すると、それに適応した認証サービス（Credential Service）に転送され、そこで認証処理を行う。
③ 利用者は、行政サービスに対して認証サービスが発行した認証情報（SAML Assertion 等）を提示し、サービスをうける。

この場合の処理の流れを図 4.31 に示す。

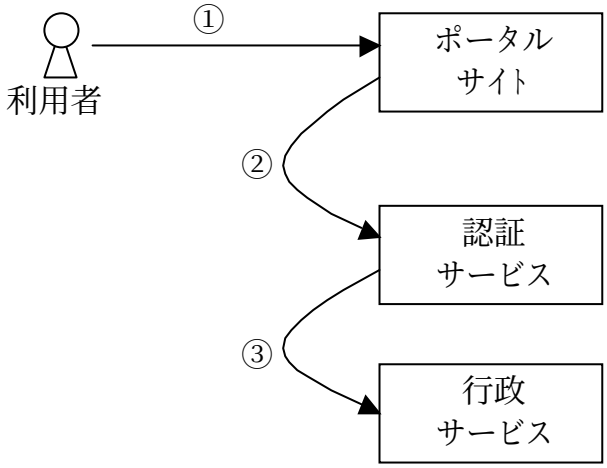


図 4.31　e-Authentication の基本フロー

このほかに、ポータルを利用せず、利用者が Agency Application や Credential Service に直接アクセスすることも認められている。

(b) 行政サービスからポータルサイトにリダイレクトされる例

① 利用者は、まず利用したい行政サービス（Agency Application）にアクセスする。

② 利用者は行政サービスにアクセスするとポータルサイト（FirstGov）に転送される。

③ 利用者は、アクセスしたい行政サービスに適応した認証サービス（Credential Service）にポータルサイトによって転送され、そこで認証処理を行う。

④ 行政サービスに対して認証サービスが発行した認証情報（SAML Assertion 等）が提示され、利用者はサービスをうける。

この場合の処理の流れを図 4.32 に示す。

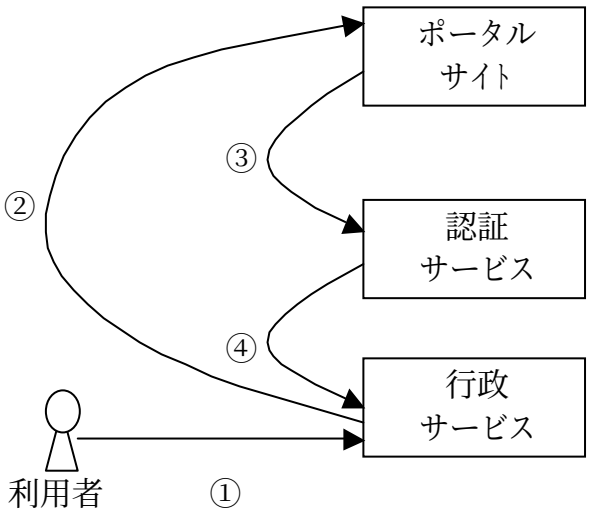


図 4.32　基本フローに対するバリエーションの例

(c) 異なるプロトコルをスキーマ変換サービスにより併用する例

① 利用者はポータルサイト（FirstGov）からスキーマ変換サービス（Scheme Translator）に転送される。
② 利用者はそこで認証処理を行う。
③ この時に使用するプロトコルは認証サービス（Credential Service）が使用可能なプロトコルとする。
④ 利用者が行政サービス（Agency Application）を利用する場合は、スキーマ変換サービスにより、行政サービスが利用可能なプロトコルに変換して認証情報（ログイン状態情報等）を転送する。

この場合の処理の流れを図 4.33 に示す。

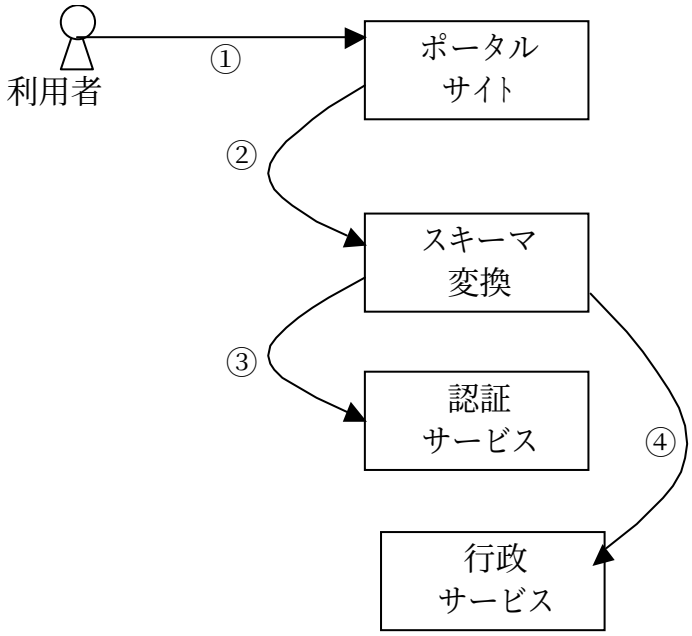


図 4.33　スキーマ変換サービスを用いた場合のフロー例

(d) 認証手段として証明書を使う例

① 利用者はポータルサイト（FirstGov）にアクセスをする。
② 利用者は、アクセスしたい行政サービス（Agency Application）を選択すると、該当の行政サービスにリダイレクトされる。
③ 利用者はその行政サービスでの認証に必要な利用者証明書が要求され、それを送付する。（SSL や TLS を利用する方法等がある）
④ 行政サービスは、検証サービス（Validation Service）を用いて、証明書を検証し利用者を認証する。
（検証サービスを利用せず、行政サービスがローカル環境で検証することも可能である）

この場合の処理の流れを図 4.34 に示す。

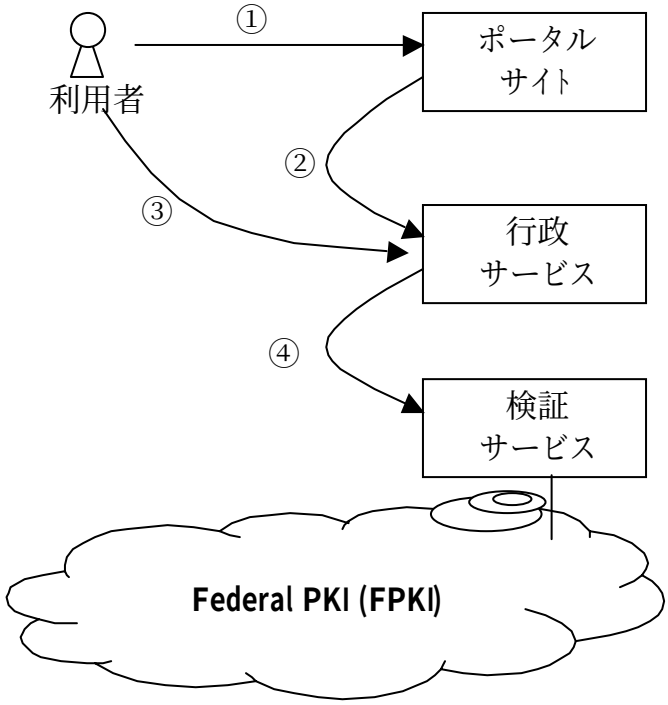


図 4.34　証明書を利用する場合のフロー例

(e) Assertion ベースの行政サービスに対して証明書を使う例

① 利用者はポータルサイト（FirstGov）にアクセスをする。
② 利用者は、スキーマ変換サービス（Scheme Translator）に誘導される。
③ スキーマ変換サービスでは必要な利用者証明書が要求され、利用者はそれを送付する。（SSL や TLS を利用する方法等がある）
④ スキーマ変換サービスは、検証サービス（Validation Service）を用いて、証明書を検証し利用者を認証する。
（検証サービスを利用せず、行政サービスがローカル環境で検証することも可能である）
⑤ 認証結果は SAML Assertion を用いて行政サービスに伝達される。

この場合の処理の流れを図 4.35 に示す。

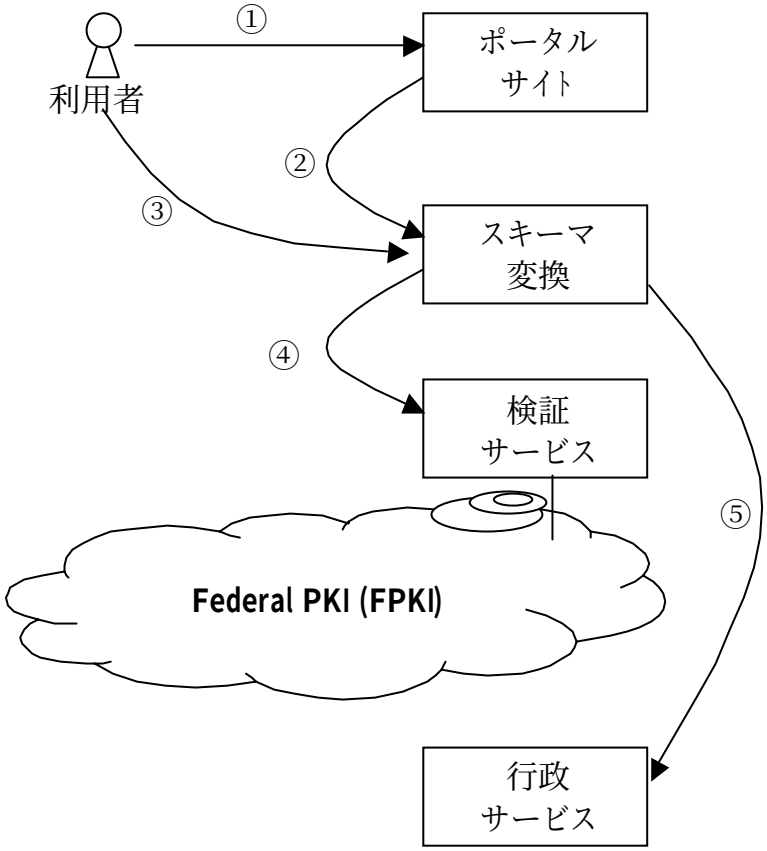


図 4.35　証明書による認証結果を Assertion で伝達する場合のフロー例

4.5.3 e-Authentication における適合性検証について

e-Authentication において、それぞれの認証サービス（Credential Service）や行政サービス（Federal Agencies）が、相互に接続するために、それぞれの運用ポリシーが適合しているか、またそれぞれの保証レベルはどれにあたるか等を事前に確認しておくことが重要となる。

本節では、それぞれの適合性検証の手順をまとめる。

また、あわせて、利用される製品に対する適合性検証についても記述する。

(1) Credential Service Provider（CSP）のアセスメント

認証情報を提供する Credential Service Provider（CSP）は、まず、OMB M-04-04 に従い、自身が適合する保証レベルを確認する。

その後、保証レベルに応じて、CEWG が提供するアセスメントパッケージを利用して、適合性のアセスメントを受ける。

また、あわせて、Memorandum of Understanding （MOU）や Memorandum of Agreement （MOA）への適用も求められる。

具体的な手順は以下の通り。

（参考資料：GSA 「E-A Handbook for CSPs」）

① Credential Manager を通じて手続きを行う。
Credential Manager とは、e-Authentication の Program Management Office（PMO）において Program Manager（PM）より任命される担当者である。

② 適用する保証レベルを決定する。
保証レベルの考え方は「OMB M-04-04」および「NIST SP 800-63」に基づく。
確認をする主な観点は以下の通り。
・実装方式
・管理
・保守
・認証手続

③ Credential Service Assessment を受ける。
保証レベルに適した運用がされるか、その運用ポリシー（手順や規則等）の評価を受ける。

④ Memorandum of Understanding （MOU）や Memorandum of Agreement （MOA）を適用する。

・CSP が提供する認証情報の受け渡し方式として、以下の 2 方式がある。

[SAML Assertion で提供する方式]
CSP あるいは認証ゲートウェイが認証し、その結果を SAML Assertion で Federal Agency に提供する。e-Authentication では、SAML Artifact Profile を採用している。

[X.509 証明書を用いる方式]
CSP は認証局として証明書を発行する。
検証者（検証サーバを含む）に対しては、検証に必要な情報（CRL 等）を提供する。

(2) Service Provider（Federal Government Agencies）のアセスメント

Federal Government Agencies は、e-Authentication に対応するにあたり以下の手順を踏むこととされている。

（参考資料：GSA 「E-A Handbook for Federal Agencies」）

① Agency Relationship Manager を通じて手続きを行う。
Agency Relationship Manager とは、e-Authentication の Program Management Office（PMO）において Program Manager（PM）より任命される担当者である。

② 該当のアプリケーションの保証レベルを決定する。
保証レベルの考え方は「OMB M-04-04」および「NIST SP 800-63」に基づく。主な考慮点は以下の通り。

・サービスに対する信頼や評価の低下
・経済的損失
・公益への影響
・個人の安全への影響
・犯罪への影響

なお、リスク分析については、e-Authentication で提供されるツール”e-Authentication Requirements and Risk Assessment tool（e-RA）”が利用できる。e-RA ツールは、カーネギーメロン大学ソフトウェアエンジニアリング研究所（CMU/SEI）が開発し、e-Authentication イニシアチブが政府の IT システムに対して認証リスクを評価する際に使用するものであり、現在入手可能なバージョンは 1.4B である。すでに、政府機関の主要なシステムの評価が開始されており、2004 年度中に評価を終了する予定である。

e-RA により、その行政サービスに求められる保証レベルが明確にされると、その保証レベルに適した CSP（Credential Service Provider）の中から利用するものを選択する。
なお、CSP も前項の記述の通り、e-RA を用いて対応可能な保証レベルが明確となっている。

③ Memorandum of Understanding （MOU）や Memorandum of Agreement（MOA）を適用する。
なお、Federal Agencies が利用する認証情報の受け渡し方式として、以下の 2 方式のいずれかを実装することとなっている。

[SAML Assertion を受け入れる方式]
認証ゲートウェイや他の Federal Agency が認証し、その結果を SAML Assertion で受け入れる。e-Authentication では、SAML Artifact Profile を採用している。

[X.509 証明書を用いる方式]
Credential 発行者である認証局の証明書を基に認証する方式。
検証サーバを利用することで、一元的な検証も実現可能。

(3) CSP および Federal AA の認定状況

現在までに認定された CSP および Federal AA の状況は表 4.16 の通りである。

表 4.16　認定済みの AA と CSP

	AA(Agency Application)	CSP(Credential Service Provider)
Level 4 (Very High)	政府機関調査官の前科者DBや 個人情報DBへのアクセス	Department of the Treasury PKI Level 4 Department of Defense PKI Level 4
Level 3 (High)	米特許商標局　機密特許情報の電子提出	Department of the Treasury PKI Level 3 NASA PKI Level 3 USDA-NFC PKI Level 3 Department of Defense PKI Level 3 Department of Energy PKI Level 3 ACES-DST PKI Level 3 State of Illinois PKI Level 3
Level 2 (Some)	米連邦政府 the Gov Online Learning Center (www.golearn.gov)	USDA E-Authentication Svc. Password Level 2 ORC, Inc. Password Level 2
Level 1 (Less or No)	米教育省　My.ED.Gov	ORC, Inc Password Level 1 USDA E-Authentication Svc. Password Level NSF FastLane Password Level 1

分析手順e-RA(e-Authentication Risk and Requirements Assessment)に従い分析されたサービスの例。
米OMB資料"M-04-04:E-Authentication Guidance for Federal Agencies"より引用

E-Authentication Program Management Office(PMO)により認定されたCSPの全リスト。(2004年7月16日時点)
認定基準については、下記ドキュメントに記載されている。
・"Interim Credential Assessment Guidance" および Credential毎のProfile
・"NIST Electronic Authentication Guideline 800-63"

(4) Product の相互接続保証

製品の相互接続性保証は、「e-Authentication Interoperability Lab」で実施することとされている。「e-Authentication Interoperability Lab」の構成概要は図 4.36 の通りである。

（参考資料：「E-A Interoperability Lab Concept of Ops」）

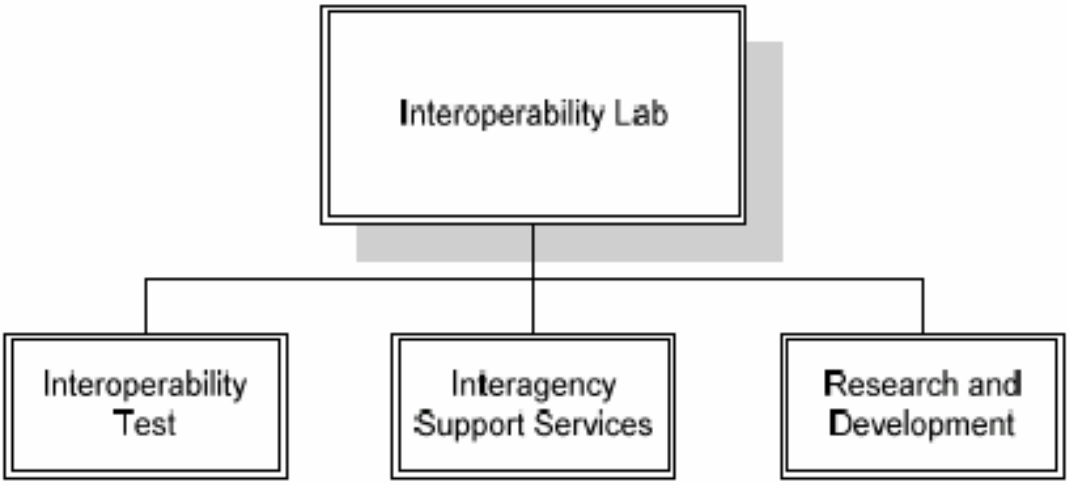


図 4.36 Interoperability Lab **の構成**

Interoperability Laboratory では製品「Commercial off the Shelf（COT)」、スキーム、標準の評価を実施する。

適合性の基準とされる文書には以下のものがある。

- Office of Management and Budget e-Authentication Guidance for Federal Agencies
- Memorandum （OMB M-04-04）
- National Institute for Standards and Technology Recommendation for Electronic
- Authentication （NIST SP 800-63）
- Federal PKI Bridge Certificate Policy （CP）
- GSA Information Technology （IT） Security Policy
- Credential Assessment Framework
- Federal Identity Credentialing Component

Interoperability Laboratory で評価が終わり、e-Authentication フレームワークの中で利用可能とされる製品は e-Authentication 適合製品リスト（The Approved e-Authentication Technology Provider List）で公開される。

現在、評価が終わっている製品として表 4.17 に示すものが挙げられている。

表 4.17　認定済みの市販製品

提供元	製品名
Entegrity	AssureAccess v3.0.0.4
Entrust	GetAccess v7.0 SP 2 Patch 3
Hewlett-Packard	Select Access v5.2
IBM	Tivoli Federated Identity Manager v5.1.1
Netegrity	Site Minder 6.0.1.04
Oblix	ShareID 2.0
RSA Security	Federated Identity Manager v2.5LA
Sun Microsystems	JES Identity Server
Trustgenix	IdentityBridge 2.1

4.5.4 e-Authentication に関する考察

行政機関、民間事業者にかかわらず、ネットワークを利用したサービスは急速に広まりつつある。これに従い、サービスはより多用化され、また、非常に重要な業務にも適用されてきている。

このような状況では、利用者のなりすましを防止する認証が適切に行われることが必須な要件であることは共通認識となっていると言ってもよいと思われ、実際、これまでに、電子署名法に基づく特定認証業務や公的個人認証等において、利用者を特定することに対する基準や仕組みは整備されてきている。

しかし、利用者認証を適切に行うためには多くのコストと運用ノウハウが必要なことも事実である。

そのため、「そのサービスにとって必要十分な認証手段は何か」「安全に（プライバシー保護も含む）認証手続きを共有する方法はないか」という課題は、今後、ますます重要となると考えられる。

この課題に対する考え方のひとつとして、e-Authentication のコンセプトは有用となりうる。

e-Japan 政策に従い、今後、整備されていくアプリケーションや地方自治体の行政サービス等、現在、個々の省庁や自治体が個別に判断している保証レベルや必要十分な認証手順に関して、ガイドラインを示すことで、安全性と効率性が向上すると見込まれ、有益であると考える。

なお、e-Authentication 自体は図 4.37 に示す通り主に行政サービスを対象としたものである。

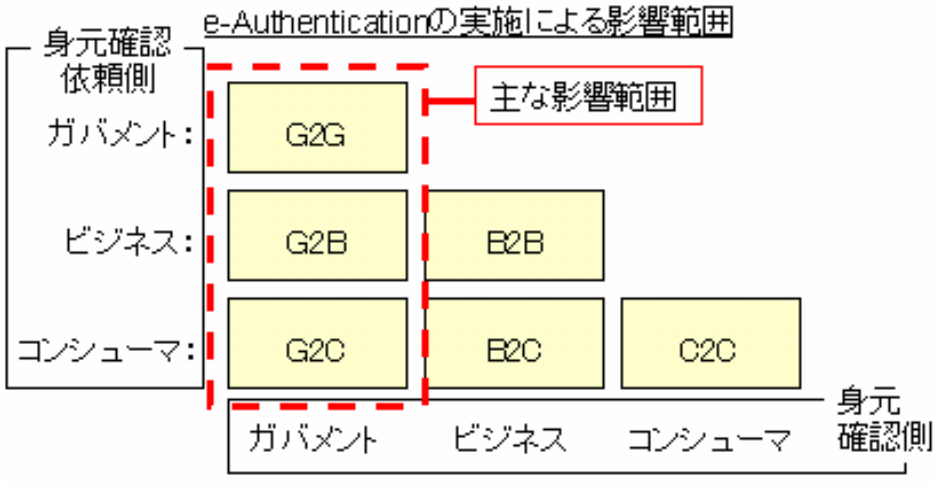


図 4.37　e-Authentication の対象範囲

このコンセプトを参考に、民間サービスにも適用可能な保証レベルの考え方の整備と分析手段の提供が行われると、認証を必要とするサービスの適切な運用が容易となる。

さらに、各サービスが抱える認証処理に伴うコストやリスクを肩代わりできる電子

認証を専業とするサービスのようなものが利用できれば、サービス事業者にとっては運用コストの削減や新しいサービスの誘発の要因となる。また利用者にとっても、これにより認証手続きが共通化され操作性が向上することになる。

これらの結果、電子認証がより適切にかつより容易に活用できるようになるといったことが期待できると考えている。

4.6 Electronic Authentication Partnership （EAP）

米国では、連邦政府が進めている電子認証（Authentication）の基盤e-Authentication[4]と平行して、政府だけでなく民間においても電子認証の基盤を構築しようとしているElectronic Authentication Partnership （EAP）[5]が存在する。

EAP は、公的および民間の電子認証システムの相互運用を可能にすることをタスクとして作られた、多産業パートナーシップである。産業界を横断してセキュアな電子処理を行うシステムを構築・運営していくためには、電子認証システムの相互運用性が必要不可欠な要素であるという考えが EAP 設立の背景にある。

本節では、EAP の設立経緯とその目的、組織構成を紹介する。その後、EAP のフレームワークについて解説を行う。最後に、EAP の活動と照らし合わせながら、日本でこのような活動を計画する際の問題を検討する。

4.6.1 設立経緯と目的

米国では、2001 年の大統領アジェンダにより、電子政府の実現に向けて、e-Authentication イニシアチブが制定された。これと同時期に、ワシントン DC にある戦略国際問題研究所（CSIS : Center for Strategic and International Studies）とジョーンズ・ホプキンズ大学が、公的部門と民間部門での電子認証の相互利用の分析のためのワーキンググループを召集した。2003 年春には、CSIS が公的な管理機構に関する報告書を、ジョーンズ・ホプキンズ大学が民間の管理機構に関する報告書をそれぞれ完成させた。その後、これらの報告書の内容を受けて CSIS が官民協業の体制を作ろうと動き、EAP が設立されることになった。EAP の設立発表は、2003 年 12 月、行政管理予算局（OMB : Office of Management and Budget）の電子政府 IT 室の Karen Evans 氏によって行われた。

EAP の最終目標は、国民や顧客に対し、様々な電子認証システムによって発行されたデジタルなクレデンシャルを信頼することができる簡単な手段を提供することである。ここでいうクレデンシャルとは、認証処理時に提示して検証される対象のことである。この目標を達成するためには、電子認証システムの相互運用性が不可欠だが、EAP は電子認証システムの相互運用性について、次のように考えている。

ある組織がユーザに対してクレデンシャルを発行して本人かどうかを認証しているような場合に、別の組織において、前者の組織で使われている認証プロセスを信頼し利用することである。後者の組織においては、ユーザを再度認証する必要がなくなる。

クレデンシャルを発行して認証プロセスを提供する側をクレデンシャルサービスプロバイダー（CSP : Credential Service Provider）、CSP のサービスを利用してユーザを認証する側をリライングパーティー（RP : Relaying Party）として話をすると、このような信頼関係を構築する場合、二者間であれば、CSP と RP が互いに合意書を取り交わせばよい。しかし、大規模な相互運用を考えた場合、RP が利用したい CSP とそれぞれ個別に二者間合意を取り交わすことは難しくコストもかかる。そこで、

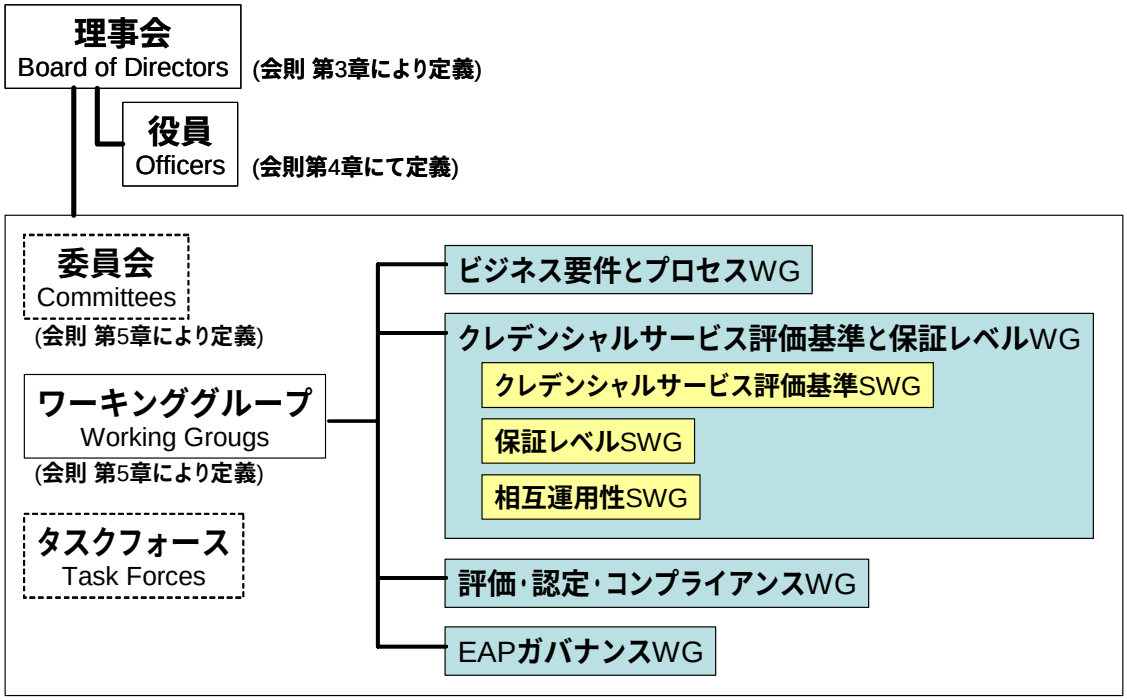
[4] [URL] e-Authentication, http://www.cio.gov/eauthentication/
[5] [URL] Electronic Authentication Partnership, http://www.eapartnership.org/

EAP において、EAP の機構に加わる CSP や RP が合意できるようなルールを作る。そのルールに従って運営している CSP や RP は、EAP に参加している他の CSP や RP と合意書を取り交わしたことになり、多者間で信頼関係を結べる。

EAP では、このような相互運用を実現するために、二者間合意に代わるルールを作り、認証に対して階層的な保証レベルを定義する。そして、CSP によって発行されるクレデンシャルに対しては、評価基準を示し、どの保証レベルを満たしているかを評価し認定する機構を用意する。

4.6.2 組織構成

EAP は、デラウェア州法に基づいて組織された非株式・非営利活動法人であり、正式名称が「Electronic Authentication Partnership, Inc.」である。EAP の組織構成は会則によって定めており、図 4.38 に示すように理事会と委員会、ワーキンググループで構成されている。しかし、設立当初は暫定的な組織体制で活動していたため、委員会やタスクフォースは 2005 年度より活動を始めることになる。また、共通役務庁（GSA : General Services Administration）と契約した全米自動決済協会（NACHA : NACHA - The Electronic Payments Association）が事務局を務めている。2005 年 2 月には、会則に従って、初代の理事会となる、投票権を持つメンバー15 名と投票権を持たない政府機関からの顧問 1 名が選出された[6]。



(注) WG = ワーキンググループ, SWG = サブワーキンググループ

図 4.38　EAP の組織構成

[6] “Electronic Authentication Partnership Elects First Board, Will Test Rules for Interoperability of Online Authentication”, http://www.eapartnership.org/docs/020705_NR_Board_election.doc

ワーキンググループの活動は非常に活発であり、EAP 全体会合も月 1 回程度のペースで開催されている。成果物として、2004 年 9 月に会則（Bylaws）[7]を採択し、2005 年 1 月に信頼フレームワーク（Trust Framework）を公開した。

会員資格には、ビジネスメンバーと非ビジネスメンバーの 2 種類がある。ビジネスメンバーとは、事業に携わる、すなわち、営利目的の企業、会社、法人、事業体等である。非ビジネスメンバーとは、事業に携わらない、すなわち、政府機関、非営利組織団体等である。どちらにしても、電子認証に関心を有する、個人や組織団体に広く参加を呼びかけている。

2005 年 2 月現在、参加メンバーは、民間企業・政府機関・その他の組織団体を合わせて、150 を超える。その内の 50 を超える組織団体が、EAP の会員として会費を支払い、投票権を得ることに同意する旨の同意書（Letter of Intent : LOI）に署名している。当初は政府資金で活動してきたが、2004 年 9 月に正式に承認された会則に基づき、会員団体の会費での運営へ移行した。

参加組織団体を簡単に紹介すると、民間企業では、RSA Security、ActivCard、Entrust、Microsoft、Oracle、VeriSign、各種銀行、信用調査会社等が参加している。非政府機関では、Shibboleth や Smart Card Alliance、CSIS、ジョーンズ・ホプキンズ大学等が参加している。また、連邦政府機関では、e-Authentication イニシアチブのプログラムマネジメントオフィス（PMO）、GSA、OMB、国防総省、教育省、保健社会福祉省、環境保護庁環境情報局、社会保障局、米国雇用機会均等委員会、下院議会、郵政省等が参加しているが、連邦政府機関で LOI に署名したのは GSA のみである。

EAP と e-Authentication イニシアチブやその他の組織団体との関係を図 4.39 に示す。

[7] “BYLAWS of Electronic Authentication Partnership - Adopted September 2, 2004”, http://www.eapartnership.org/docs/CompletedEAPBylaws_v1.0.doc

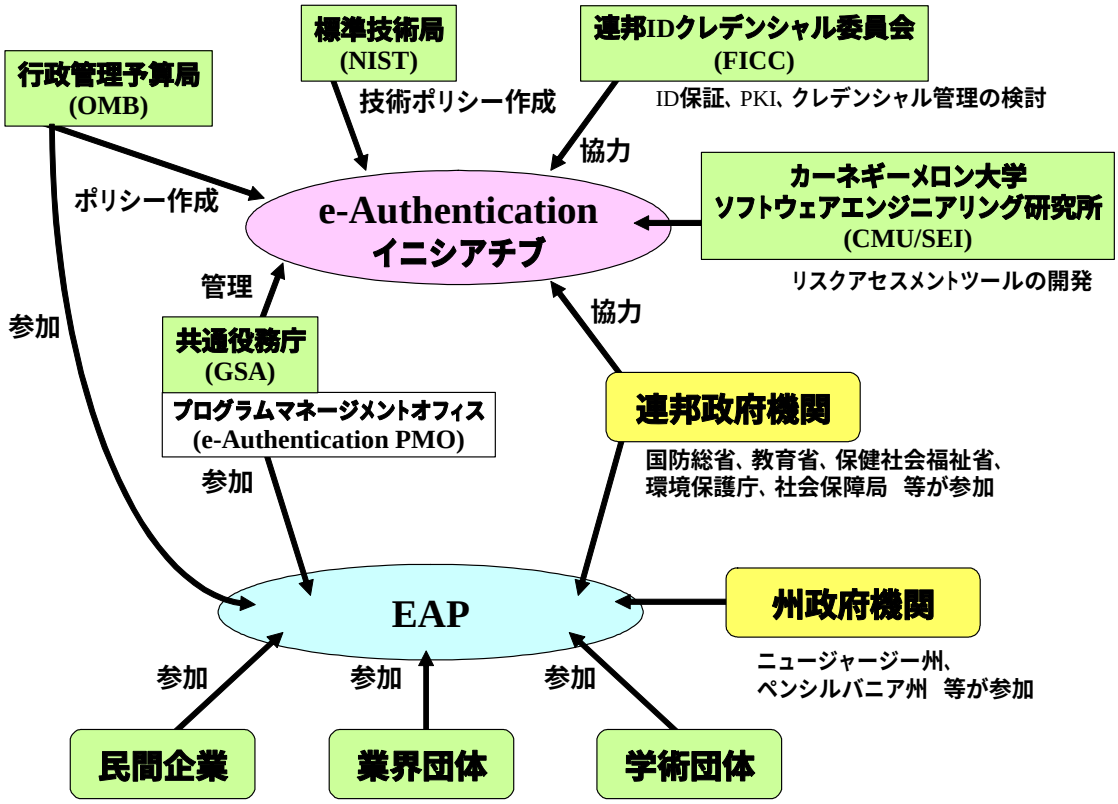


図 4.39　組織関係図

EAP が活動を行う中で、参照している文献一覧を表 4.18 に示す。

表 4.18　EAP の参考文献

タイトル （原文タイトル）	出版元	発表時期
管轄区域を超えた電子商取引の中で使用できる証明書の発行のための APEC ガイドライン （APEC GUIDELINES FOR SCHEMES TO ISSUE CERTIFICATES CAPABLE OF BEING USED IN CROSS JURISDICTION eCOMMERCE）	APEC 電気通信・情報ワーキンググループ eSECURITY タスクグループ	2004 年 10 月
暫定報告・認証システムにおけるプライバシー原則 （Interim Report, Privacy Principles for Authentication Systems）	認証プライバシー原則 WG	2003 年 5 月
連邦政府に対する電子認証ガイダンス （e-Authentication Guidance for Federal Agencies）[11]	OMB	2003 年 12 月
21 世紀における ID 管理システムとガバナンス （Identity Management Systems and Governance in the 21st Century）	ジョーンズ・ホプキンズ大学,	2003 年 4 月
NIST SP 800-53 連邦情報システムにおいて推奨されるセキュリティコントロール （Recommended Security Controls for Federal Information Systems）	NIST	2005 年 2 月
NIST SP 800-63 電子認証ガイドライン（Electronic Authentication Guideline） [12]	NIST	2004 年 6 月（9 月改訂）
ガバナンスと認証：あいまいなものと ID 連携 （Governance and Authentication: Ambiguous Bits and Federated Identity）	CSIS	2003 年 5 月
アイデンティティの不正行為：重大な国内と世界の脅威 （Identity Fraud: A Critical National and Global Threat）	ユティカ大学経済犯罪研究所、LexisNexis	2003 年 10 月
認証局向けの WebTrus プログラム （WebTrust Program for Certification Authorities）	米国公認会計士協会、カナダ公認会計士協会	2000 年 8 月
FAST フェーズ 1 最終報告書 （Financial Agent Secure Transaction （FAST） Phase 1 Final Report White Paper）	金融サービス技術コンソーシアム（Financial Services Technology Consortium： FSTC）	2000 年 9 月

CSIS の報告書とジョーンズ・ホプキンズ大学の報告書が EAP 設立のきっかけになった文書であり、OMB ガイダンスや NIST 電子認証ガイドラインやその他、電子認証にかかわる文献を参考にしたり、その成果を利用したりしている。

Burton Group という調査会社が作成し、2004 年 9 月に e-Authentication イニシアチブから公開された、e-Authentication イニシアチブと EAP の活動について調査報告し提言を寄せる報告書[13] もあるので参照されたい。

4.6.3 フレームワーク

EAP では、電子認証システムの相互運用性を確立するために、EAP の運営規則やフレームワークの整備を行っている。本節では、EAP が整備する EAP フレームワークについて説明する。フレームワークとは、EAP の会員が相互運用する時に合意すべきことや要件等をまとめたものである。EAP の会員がどのように EAP というパートナーシップを構築するかのガバナンス、相互運用に加わる会員が共有すべきビジネスルールや、電子認証に失敗した場合のリスクや保証すべき認証のレベルの定義、互いに利用するクレデンシャルに対して求められる要件やそのクレデンシャルがその要件をきちんと満たしているかどうかを検証し認定するプロセスのルール等を確立しなくてはならない。

EAP フレームワークの概念を図 4.40 に示す。

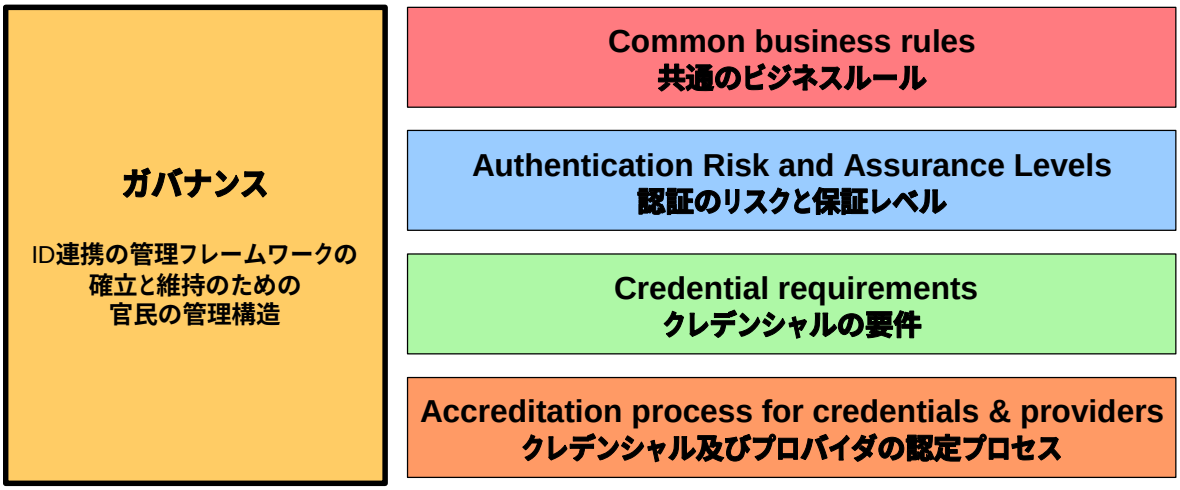


図 4.40　EAP フレームワーク

EAP フレームワークの開発アプローチを図 4.41 に示す。政府や民間企業、教育機関や保健機関等が、これまでそれぞれで作ってきた、クレデンシャルの標準や運用のプロセスやルール、評価プロセスを利用して、EAP における信頼のフレームワークを開発するというアプローチである。また、世の中の状況変化に合わせていくために、定期的な更新を行うことも前提にしている。

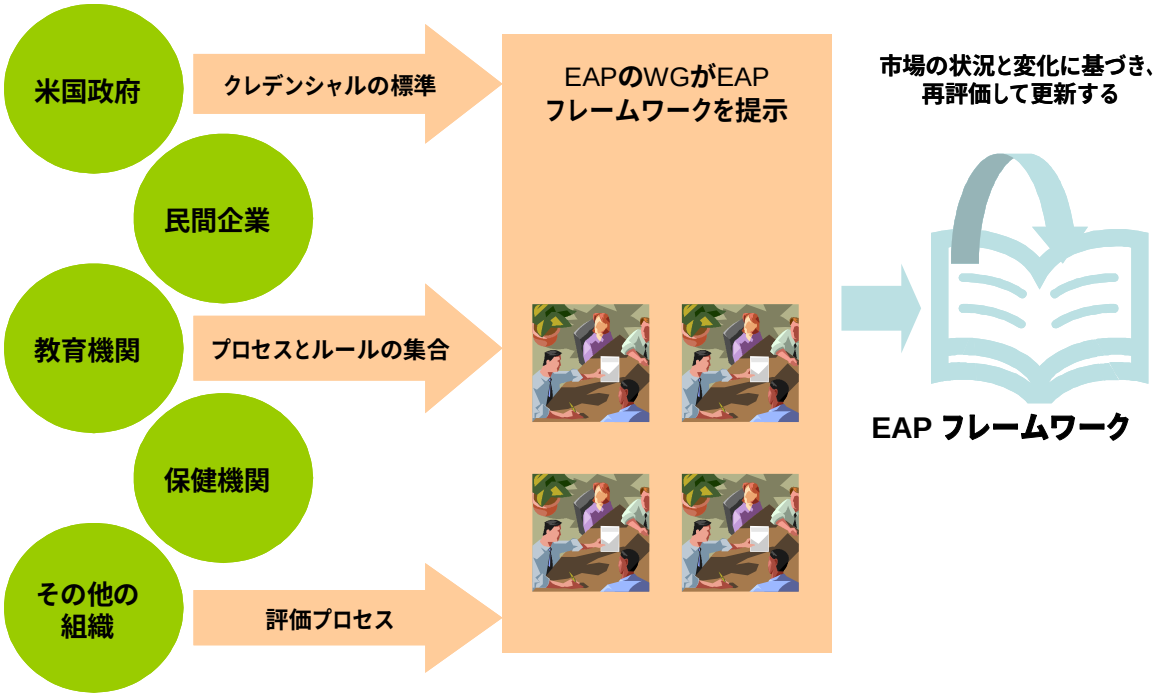


図 4.41　EAP フレームワークの開発アプローチ

このアプローチで開発される EAP フレームワークの要素は、次の 5 つである。

・ ビジネスルール（Business Rules）

・ 保証レベル（Assurance Levels）
・ アセスメントフレームワークとクライテリア（Assessment Framework, Criteria）
・ 評価と認定とコンプライアンス（Evaluation, Accreditation and Compliance）
・ EAP ガバナンス（EAP Governance）

以下、順番に解説する。

(1) ビジネスルール

EAP の電子認証システム連携のための運用規則について規定したものである。このビジネスルールの検討は、ビジネス要件とプロセス（BRP : Business Requirements and Processes）ワーキンググループが行っている。

ビジネスルールには、EAP、クレデンシャルサービスプロバイダー（CSP）、リライングパーティー（RP）、クレデンシャルの EAP 認定を担当する評価機関の役割と義務が定義される。また、EAP 認定のクレデンシャルを用いて問題が生じた際の対応についても定義されている。

EAP の認証連携のシステムに参加するには、次のことを定義しているビジネスルールに合意することが前提になっている。

・ 認証を目的として、EAP 認定のクレデンシャルを使用、有効性検証をする。
・ クレデンシャルの認定、アセスメントを担当する機関の認定に関して、本ビジネスルールを遵守する。

EAP は次のことに責任を持つことになる。

・ EAP システムに加わる、RP や CSP や評価機関への参加承認
・ CSP が発行するクレデンシャルの認定
・ クレデンシャルの EAP 認定において CSP の評価を行う評価機関の認定
・ ビジネスルールのメンテナンス

EAP が認定したクレデンシャルは、ビジネスルールに合意し、信頼関係にある RP によって利用されることになる。CSP からクレデンシャルを発行されるユーザは、本ビジネスルールを直接合意しないので、CSP との契約で利用することになる。

(2) 保証レベル

EAP においても、e-Authentication イニシアチブの OMB ガイダンス[11] や NIST 電子認証ガイドライン[12] と同様、4 つの保証レベル（Assurance Level : AL）を定義している（表 4.19）。これは、政府と非政府のシステムを接続する際に、EAP 立ち上げ当初は、e-Authentication イニシアチブのアプローチを使うのが良い、という考えからである。OMB ガイダンスと NIST 電子認証ガイドラインに記載されている保証レベルについては、4.4 節を参照されたい。

表 4.19　保証レベル

e-Authentication イニシアチブ	EAP		説明
レベル 1	AL1	Minimal	主張されたアイデンティティの有効性に対する確信がほとんどない（最低限の保証）
レベル 2	AL2	Moderate	主張されたアイデンティティの有効性に対する確信がいくらかある（低い保証）
レベル 3	AL3	Substantial	主張されたアイデンティティの有効性に対する確信が高い（高い保証）
レベル 4	AL4	High	主張されたアイデンティティの有効性に対する確信が大変高い（最高の保証）

また、認証が失敗した場合の潜在的な影響と保証レベルのマッチングについても定義している（表 4.20）。

4 つの保証レベルで定義している点は OMB ガイダンスと同じであるが、リスクのマッピングは OMB ガイダンスが Low/Moderate/High の 3 つのレベルで示しているのに対し、EAP では Minimum/Moderate/Substantial/High と４つのレベルで示している。OMB ガイダンスのマッチング（表 4.4）と比較されたい。

表 4.20　潜在的な影響と保証レベルのマッチング

認証エラーによる潜在的な影響のカテゴリ	保証レベル			
	1	2	3	4
不便性、災難、身分や評判への損害	Min	Mod	Sub	High
金銭的ロス、組織の責務	Min	Mod	Sub	High
組織計画や公益への被害	N/A	Min	Mod	High
機密（sensitive）情報の未許可開示	N/A	Min	Sub	High
個人の安全	N/A	N/A	Min	Sub High
市民や犯罪の違反	N/A	Min	Sub	High

*Min=Minimum; Mod=Moderate; Sub=Substantial; High=High

Sub の部分が、表 4.4 と異なる部分である。

(3) アセスメントフレームワーク

クレデンシャルを発行する CSP をアセスメントするフレームワーク、サービスアセスメントクライテリア（Services Assessment Criteria : SAC）と呼ばれる評価基準を開発する。SAC は次の 3 つで構成されている。

- 共通組織サービスアセスメントクライテリア
  （Common Organizational Service Assessment Criteria : CO-SAC）
- アイデンティティ証明サービスアセスメントクライテリア
  （Identity Proofing Service Assessment Criteria : ID-SAC）

・ クレデンシャル管理サービスアセスメントクライテリア
（Credential Management Service Assessment Criteria : CM-SAC）

この 3 つの SAC の内容を簡単に紹介する。

(a) CO-SAC
各保証レベルにおいて、クレデンシャルサービスやクレデンシャルサービスプロバイダーのビジネス全般や組織の適合性に関する要件を規定する。この基準は、他の基準（ID-SAC や CM-SAC）と組み合わせて使用される。

(b) ID-SAC
各保証レベルにおけるアイデンティティ証明の技術的な適合性に関する要件を規定する。この基準は、EAP が認定する、電子信頼サービス（Electronic Trust Service ： ETS）や関連の電子信頼サービスプロバイダー（Electronic Trust Service Provider : ETSP）のアイデンティティ証明サービスに適用される。ただし、アイデンティティ証明の後の段になる、クレデンシャルの配布に関する部分はこの基準の範囲外である。後述の CM-SAC の扱いとなる。

(c) CM-SAC
各保証レベルにおけるクレデンシャルの管理サービスやプロバイダーの機能の適合性に関する要件を規定する。

CO-SAC、ID-SAC、CM-SAC は、適応すべき保証レベルごとに、要件を複数の領域に分類して定義している。

SAC の検討は、クレデンシャルアセスメントクライテリア（CSAC : Credential Services Assessment Criteria）サブワーキンググループが行っている。
CSAC SAG は e-Authentication イニシアチブの電子認証クレデンシャルアセスメントスイートをはじめ、OMB ガイダンス、NIST 電子認証ガイダンス、米国抵当銀行協会（MBAA : Mortgage Bankers Association of America）や連邦ブリッジ認証局（FBCA : Federal Bridge Certification Authority）や t-Scheme の成果を参照・利用している（表 4.21）。

表 4.21　CSAC WG の参考文献

タイトル （原文タイトル）	出版元	発表時期
証明書ポリシー（Certificate Policy Requirements Document）	MBAA	2003 年 6 月
アイデンティティの不正行為：重大な国内と世界の脅威 （Identity Fraud: A Critical National and Global Threat）	ユティカ大学経済犯罪研究所、LexisNexis	2003年10月
テキサス大学電子 ID （UT EID）	テキサス大学	-
連邦政府に対する電子認証ガイダンス （e-Authentication Guidance for Federal Agencies）[11]	OMB	2003年12月
電子認証クレデンシャルアセスメントスイート（e-Authentication Credential Assessment Suite）	e-Authentication イニシアチブ	2003年12月
NIST SP 800-63 電子認証ガイドライン（Electronic Authentication Guideline） [12]	NIST	2004 年 6 月（9 月改訂）

アイデンティティの基盤（Identity Infrastructure）	NECCC[8]	2003年11月
SISACリライングパーティー:SISACのセキュアなIDクレデンシャルを使用する場合のガイダンスとベストプラクティス（SISAC Relying Parties: Guidance and Best Practices for Implementing Use of SISAC Secure Identity Credentials）	MBAA-SISAC[9]	2003年10月

ここで、参考資料の中のひとつである、e-Authenticationイニシアチブのクレデンシャルアセスメントスイート（Credential Assessment Suite）について紹介する。クレデンシャルアセスメントスイートは、クレデンシャルアセスメントフレームワーク（Credential Assessment Framework : CAF）とクレデンシャルアセスメントガイド（Credential Assessment Guide : CAG）とクレデンシャルアセスメントプロファイル（Credential Assessment Profile : CAP）から構成されている（図4.42）。

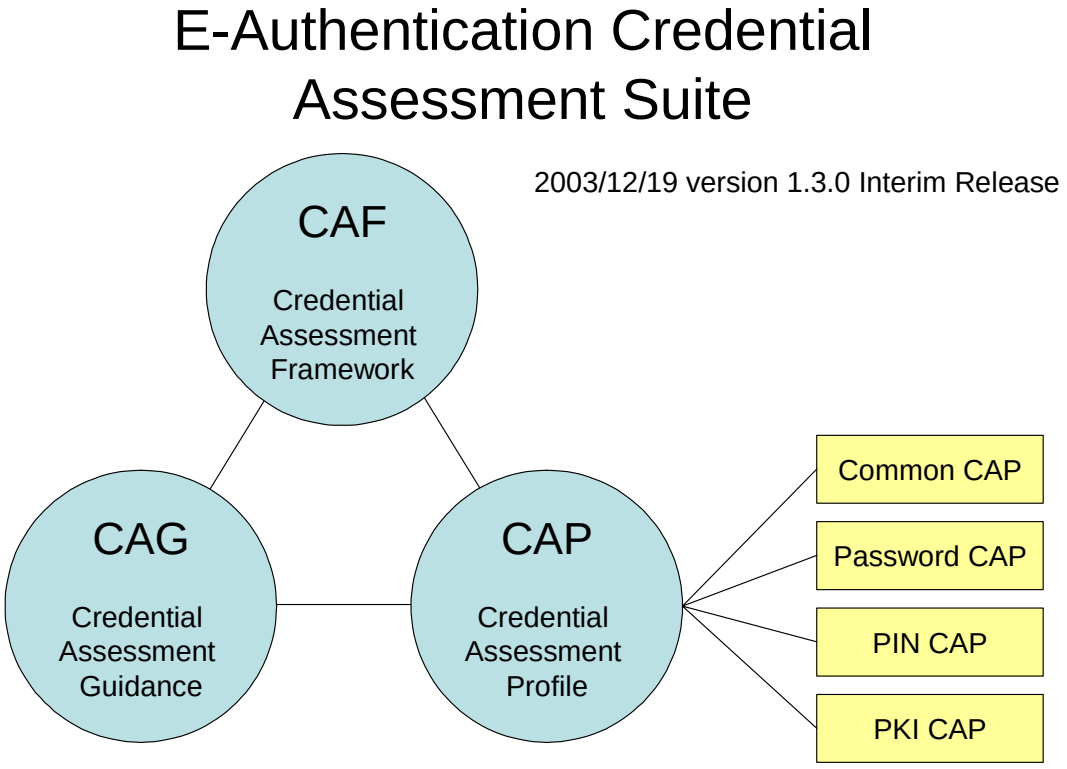


図 4.42　e-Authentication クレデンシャルアセスメントスイート

CAF とは、クレデンシャルアセスメントの手法について書かれた文書である。アセスメントに登場する組織の役割、アセスメントの流れが記載されている。

CAG とは、クレデンシャルのアセスメントに関わるものに対するガイドラインである。アセスメントの概要や評価レポートの内容の説明が記載されている。

CAP とは、クレデンシャルが定義された保証レベルに適合するかを評価するチ

[8] NECCC = National Electronic Commerce Coordinating Council
[9] MBAA-SISAC = Secure Identity Services Accreditation Corporation, a subsidiary of MBAA

ェックシートである。パスワード用の「Password CAP」、PIN 用の「PIN CAP」、PKI 用の「PKI CAP」、PKI 以外のクレデンシャルに共通な項目について記載された「Common CAP」の 4 つの CAP から構成されている。表 4.22 は、この 4 つの CAP の評価基準を抜粋して一覧にしたものである。

表 4.22　CAP 評価基準一覧

共通	Level 1	Level 2
Organizational Maturity	☐ Established ☐ Authorization to Operate ☐ General Disclosure	☐ Documentation ☐ Staffing ☐ Subcontracts ☐ Helpdesk ☐ Audit ☐ Risk Mgt ☐ COOP ☐ Logging ☐ Configuration Mgt ☐ Network Security ☐ Physical Security
Identity Proofing		☐ IVP Disclosure ☐ Records At least one of: ☐ Confirmed Relationship ☐ In Person Proofing ☐ Remote Registration
Authentication Protocol	☐ Secure Channel ☐ Proof of Possession ☐ Session Authentication ☐ Stored Secrets ☐ FIPS Crypto	☐ Protected Secrets
Token Strength	☐ Uniqueness	
Status Management	☐ Credential Validity	☐ Credential Status ☐ Credential Invalidation
Credential Delivery		☐ Confirming Delivery

パスワード	Level 1	Level 2
Token Strength	☐ Basic Password ☐ Modifiable	☐ Strong Password
Status Management		☐ Inactivity Expiration

PIN	Level 1	Level 2
Token Strength	☐ Basic PIN ☐ Modifiable	☐ Strong PIN

PKI	Level 1	Level 2	Level 3	Level 4
Authentication Protocol	☐ Proof of Possession			
Token Strength		☐ FPKI Rudimentary	☐ FPKI Basic	☐ FPKI Medium

この CAP を用いて評価され、承認された CSP の CSP 名とクレデンシャルのタイプ、認定日の一覧が、図 4.18 の「信頼 CSP リスト（Trusted Credential Service Providers List）」として公開される。2005 年 2 月現在、この信頼 CSP リストには、パスワード、PIN、PKI のクレデンシャルタイプの CSP がリストされている。政府機関がなんらかのサービスを提供する場合に、この信頼CSP リストを参照して、そのサービスに求められる保証レベルを満たしている CSP を選択すればいいので

ある。

現時点ではまだだが、EAP においても同様に、SAC を用いて EAP ブランドの信頼 CSP リストを作ることを構想に入れている。

(4) 評価と認定とコンプライアンス

EAP は CSP に対して認定制度をとり、EAP に認定された CSP しかクレデンシャルを提供できない。また、CSP を認定するのは評価機関であり、EAP に認定された評価機関だけが評価認定することができる。この評価（Accreditation）と認定（Certification）に関するルール、評価機関と CSP の評価と認定に関するプロセスと基準を定義する。この検討は、連邦 ID クレデンシャル委員会（Federal Identity Credentialing Committee : FICC）の資料[10・11]を参考にして、評価・認定・コンプライアンス（EAC : Evaluation, Accreditation, and Compliance）ワーキンググループで行われた。

(5) ガバナンス

EAP の統合構造を定義するものである。どのように EAP を運営していくのか、会則と予算について取り組んでいる。ガバナンスについての検討作業は、EAP ガバナンスワーキンググループで行われた。会則は 2004 年 9 月 2 日に正式に採択されている。

以上、フレームワークの要素概念について紹介してきたが、ビジネスルール、保証レベル、サービスアセスメントクライテリア、認定と証明の 4 つで構成される信用フレームワーク（Trust Framework）のワーキングドラフト（バージョン 1.0）[12]は、2005 年 1 月に公開されている。構成を図 4.43 に示す。

[10] “FICC Audit Standards for PKI Shared Service Provider Entities”, http://www.cio.gov/ficc/documents/AuditStandards.pdf

[11] ” FICC Shared Service Providers (SSP) Subcommittee Documents”, http://www.cio.gov/ficc/ssp_documents.htm

[12] “Electronic Authentication Partnership Trust Framework Working Draft Version 1.0”, http://www.eapartnership.org/docs/Trust_Framework_0105.pdf

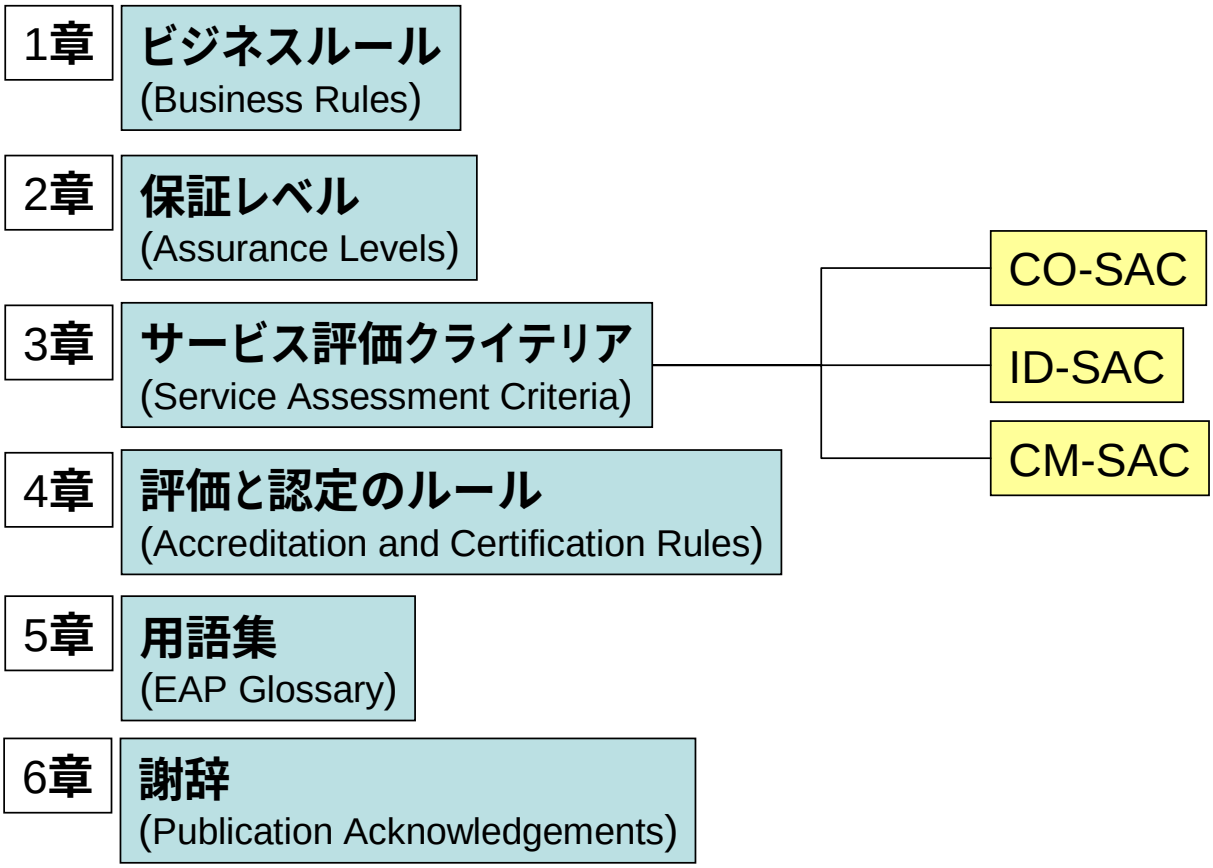


図 4.43　Trust Framework の構成

1 章でビジネスルール、2 章で保証レベル、3 章でサービス評価クライテリア、4 章で評価と認定のルールが定義され、5 章ではフレームワークで使われる用語の説明がある。

このワーキングドラフトで一番の比重があるのは、3 章の SAC の部分である。CO-SAC、ID-SAC、CM-SAC の評価基準の識別子は、「ALn_{CO,ID,CM}_ZZZ#999 name」のように表記される。この表記において、n は基準が適応される保証レベルを、CO/ID/CM で SAC の種別を示す。また、ZZZ の部分は基準の領域を示す略語が、999 の部分は基準のタグシーケンス番号が入り、name が基準のショート記述名となる。この評価基準の記述子に対して、要件が詳細に記載されている。

4.6.4 EAP に関する考察

本節では、米国の EAP の活動について、設立経緯から目的、組織構成、EAP のフレームワークについて解説してきた。図 4.44 に、EAP の活動をまとめた。

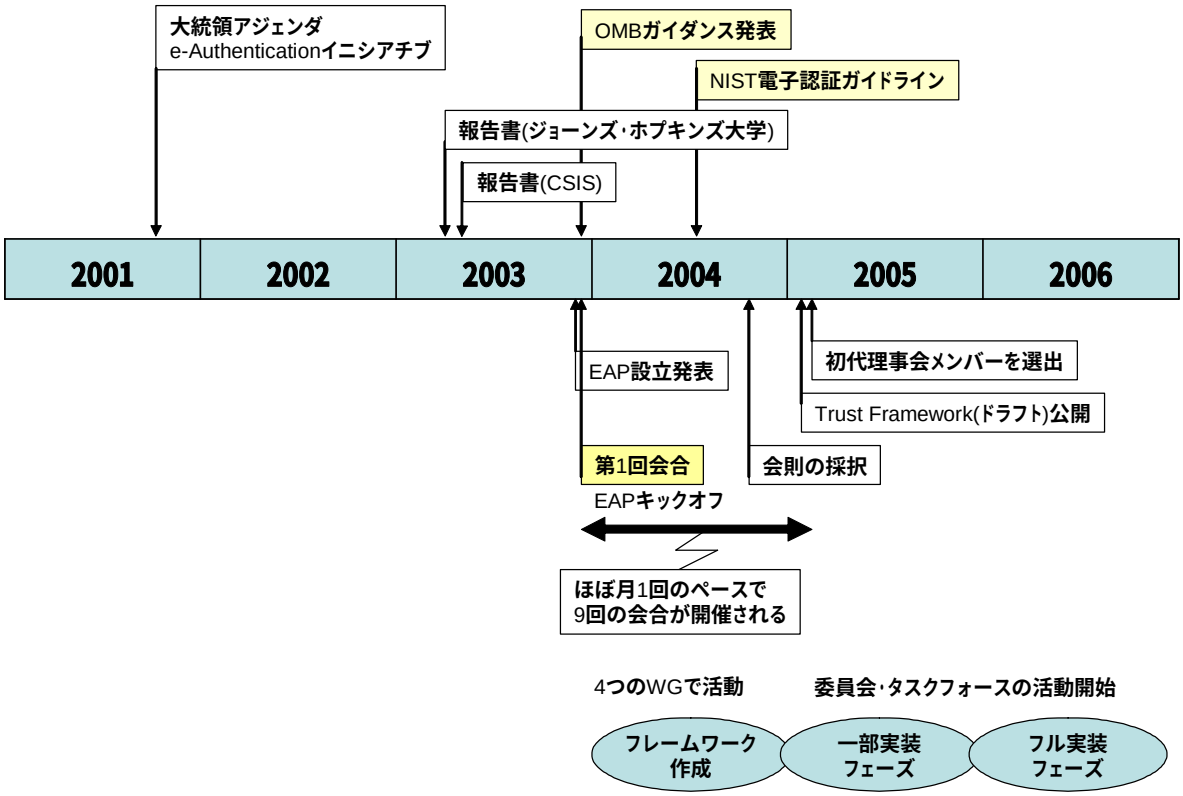


図 4.44　EAP の活動状況

2005 年 2 月に開催された EAP の全体会合では、今後の予定が示され、2004 年に作成したフレームワークを踏まえ、2005 年にはテストを開始し、2006 年にはフル実装しようと計画している。ワーキンググループだけでなく、委員会やタスクフォースの立ち上げも計画している。

EAP は 2003 年末に発足して活動を始めたが、約 1 年で、正式な会則の採択や信用フレームワークのワーキングドラフトを公開する等、早期に立ち上がっている。これは、暫定体制ながらも、EAP 全体の会合を月 1 度の頻度で開催し、4 つのワーキンググループが大変活発な活動をしているからである。その活動を進める上で、e-Authentication イニシアチブをはじめとする、他の団体組織が作成した、これまでの成果物を有効活用している。活動資金にしても、最初の 1 年は政府予算で運営し、正式な会則が採択された後は、EAP の活動に賛同して会員の会費から運営へ移行する形をとった。また、参加を募るにしても、まずは電子認証に興味のある団体に官民を問わず呼びかけて参加してもらい、その上で、会員になるかどうかの判断を仰ぎ、会員になるならば LOI に署名するという手法をとっている。非会員であっても、投票権がないだけで、ワーキング活動や会合に参加することができる。このような背景もあるためか、参加団体も多種多様である。連邦政府機関や州政府機関、大学や各種業界団体、システムインテグレータやサービス業と幅広く、既に 150 を超える団体が参加し、会員も 50 を超えている。結びつきの強い政府機関としては、設立発表をした OMB や EAP の事務局を務める NACHA と契約し、e-Authentication イニシアチブを管轄する GSA だろう。情報提供という面をみても、会合資料やワーキンググループのドラフトや参考文献を一般公開している。正式な会則の採択後は会合資料の一

部が会員限定になってしまったが、それでも多くの資料を参照できる。

米国における EAP の活動を見てきたが、EAP の活動に鑑みると、日本において電子認証システムの連携を行う場合には次の課題が考えられる。

課題 1：EAP では、e-Authentication イニシアチブの成果を利用することができたが、日本には e-Authentication イニシアチブに該当するような政府主導のプロジェクトはない。既存の成果物を利用できないので、認証の保証レベルや評価基準を考える場合に、認証に対する深い理解が必要になり、調査・検討の場を推進していかなければならない。

課題 2：連携を進めるためには、多種多様の組織団体の参加が必須である。偏らず広い参加を呼びかけるためには、参加に対するメリットを示す必要があるだろう。そのために、認証に対する啓蒙活動、基本的なビジネスモデルやアプリケーションの提示等も考えられる。

課題 3：電子認証システムの連携は、特に民間の場合は、日本国内だけで閉じるものではなく、米国の EAP や欧州の関連団体とのリエゾンが必要になる。少なくとも、他国の動向を踏まえ、相互運用が可能なフレームワークが望まれる。

上に示した課題を解決するためにも、日本においても、連携を見据えた電子認証システムの整備を推進する活動の場が必要である。

4.6.5 参考文献

[11] “E-Authentication Guidance for Federal Agencies”, J. Bolten, December 2003, http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

[12] “NIST Special Publication 800-63: Electronic Authentication Guideline”, W. Burr, D. Dodson, T. Polk, Version 1.01, September 2004, http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf

[13] “Burton Group Report on the Federal E-Authentication Initiative”, August 2004, http://www.cio.gov/eauthentication/documents/BurtonGroupEAreport.pdf

5 電子認証の今後の方向性

インターネットを経由した取引では、公開鍵証明書を利用した取引も普及が進んでいる一方で、ID とパスワードによる本人確認による取引が依然として大半を占めている。PKI を利用した本人確認方法は、ID、パスワードを利用した本人確認よりも高いセキュリティを提供できる。高額な取引については、より高い安全性が要求されるので、PKI を導入することが妥当である。PKI の導入コストは、まだ、比較的高いので、今後のコストダウンやリスクの増大により、PKI の導入投資に対する効果が高まり、一層の普及が予測される。

PKI による本人確認と ID・パスワードによる本人確認では、セキュリティ上の差こそあれ両社とも本人確認の機能を提供することに変わりはなく、ビジネス上のアプリケーションが要求するセキュリティレベルを満たしていれば、認証の方式がすべて同じである必要はない。認証の方式が異なる場合には、アプリケーションが要求するフォーマットに変換することにより、技術的には、認証の相互運用性が確保される。

異なる複数の認証方式が同一のサービスで利用されている場合、そのサービスの要求するセキュリティレベルはその中で一番低いレベルを採用していることになる。2 つ以上のサービス適用者が相互に連携する場合にも、セキュリティレベルは一番低いレベルに合わせることになるので、高いセキュリティレベルを要求しているサービスを利用している利用者が、低いセキュリティレベルを要求しているサービスを利用できても、低いセキュリティレベルを要求しているサービスを利用している利用者が、高いセキュリティレベルを要求しているサービスを利用することはできない。

このような考え方のもとに、ネットワークを利用したビジネスを発展させるためには、本人確認に関する連携サービスの興隆や認証機能に関わるコストダウンが必須であり、新たな認証に関する仕組みづくりが必要である。

以下に、調査結果を踏まえ、今後、認証サービスや日本におけるネットワークを利用した産業の発展のために留意すべきことを述べる。

5.1　認証機能のサービス事業化

これまでは、1 つのサービスプロバイダーが初めから終わりまでの完結したサービスを提供することが多かった。しかし、サービス内容の高度化・競争の激化により、企業は投資する資源を集中せざるを得なくなってきている。本人確認等といったどこの企業でもサービスを提供する際に共通して必要なサービスは、それらを専門に取り扱うサービス提供者と連携した方が、マーケット全体としては投資コストを抑え、日本の産業の競争力が強まることが期待できる。

5.2　認証セキュリティレベルの相互運用性

電子署名法に準拠する特定認証業務については、一定のセキュリティレベルが確保されているが、それ以外の方法（ID、パスワードや特定認証業務以外の PKI 等）については、全体的に整理されておらず、認証を専門とするサービスが誕生するには、セキュリティレベルの相互運用性を確保することが必要である。

電子商取引の安全性は、利用するアプリケーションによって決められるべきであり、

すべてのアプリケーションが必ずPKIを利用しなければならない必然性は無い。ID、パスワードの利用や特定認証局でない認証局が発行する公開鍵証明書も、今後とも利用されて行くであろうから、これらの環境を踏まえて、認証に係わるセキュリティレベルの相互運用性の確保を進める必要がある。

認証の相互運用性が確保されることにより、ネットワーク上のビジネス連携が容易になり、経済がより活性化することが期待できる。また、利用者は、ID やパスワードあるいは、PKI 証明書をサービスごとに分けて利用することも不要になり、利便性が向上する。

5.3　認証サービス提供構造の実体化

EAP に見られるように、ネットワーク上の本人確認を連携して行うための仕組みが、技術面だけではなく、ビジネスの仕組みをも考慮しつつ、進行している。クレジットカードの仕組みが決済構造や商慣習の違いにより日本と米国では異なるように、認証サービスを利用したネットワーク上の構造も米国と日本では異なってくることが予想される。日本においては、どのような認証サービス連携がビジネスとして確立可能であるのかを見極め、投資に見合うだけの連携がどの分野で発生するのかについての市場予測も必要である。また、クレジットカードビジネスが国際化しているように、今後の認証連携サービスの国際化も視野に入れた戦略の立案が必要である。

5.4　オープンな技術仕様による実装

事例調査の中で、e-Authentication、 Liberty、 Shibboleth 等を見てきたが、いずれも一定の前提や目的に基づいて構築されている。e-Authentication は、米国政府から見た本人確認のスキームであり、Liberty は、SAML をベースとした技術志向のスキームであり、Shibboleth は、大学間のリソースの有効利用を目的としたスキームである。

実際のシステムを構築する際には、市場で調達可能ないずれかの技術を採用することになるが、長期間にわたって利用可能な認証のスキームを構築するためには、オープンな仕様に基づく技術を利用することが望ましい。

5.5　個人情報保護への対応

平成 17 年 4 月より、個人情報保護法が民間企業に対して適用される。認証の連携においては、個人を特定するための情報や個人を特定したことを証明する情報がネットワーク上で交換される。相手により、開示してよい情報と開示してはいけない情報を明確に区別する必要があり、これらの機能をどのように実装するかについても、慎重な検討が必要である。特に、欧州においては、ネットワーク上で個人情報をどのように保護すべきかに関する研究や実験が進んでおり、参考とすべきである。