米国アイデンティティ管理エコシステム政策（NSTIC）のゆくえ

宮川 寧夫 †　　松本 泰 †

† 独立行政法人 情報処理推進機構
isec-info@ipa.go.jp

あらまし　米国のオバマ政権において今年から施行されているアイデンティティ管理についての政策は，生態系になぞらえて「エコシステム」と呼ばれている．民間が主導するアイデンティティ管理サービスを政府部門が認定しながら，官民が共通的に利用する枠組みを模索しているかのように見える．国民のアイデンティティ情報についての権威ある源泉は，多くの国々においては現在も政府によって管理されているので，必ずしもアイデンティティ管理サービスの「適者生存」を見守るのみではアイデンティティ管理政策は成り立たない．本稿においてはアイデンティティ管理の官民連携における政府の役割について整理を試みる．

A Commentary on US NSTIC

Yasuo Miyakawa†　　Yasushi Matsumoto†

†Information-technology Promotion Agency (IPA)
isec-info@ipa.go.jp

Abstract　In the United States, an identity management strategy has been announced in this April, and it is stating about “Identity Ecosystem”. It seems that the US is trying to find out suitable framework in which the federal government and the citizens can use identity management systems together, by certifying identity management services within the framework. As the authoritative source of citizen’s identity information is managed by government in a lot of nations, the identity management policy doesn’t necessarily work well only by certifying ”Survival of the fittest” as the identity management service. In this paper, we will try to clarify the role of the government within the federation with the private sector in identity management.

1　はじめに

1.1　NSTIC とは

今年 4 月に米国連邦政府の「NSTIC（National Strategy for Trusted Identities in Cyberspace）」[1] がホワイトハウスから正式に発表された．この国家戦略は，ビジョンとして「確実性，プライバシ，選択の自由およびイノベーションを促進するような作法で，オンラインサービスにアクセスするために個々人や組織体が，セキュアで，効果的で，使い易く，かつ相互運用可能なアイデンティティ管理サービスを利活用できるようにすること」を掲げており，このビジョンが実現する理想型を「アイデンティティエコシステム（Identity Ecosystem）」と呼んでいる．

1.2　エコシステム

なぜ，NSTIC において「エコシステム（生態系）」というメタファが使われているのであろうか？近年，わが国においては一般的に，新たな産業体系を構成しつつある発展途上の分野に

おける企業間の連携関係全体を指して「エコシステム」と呼ぶようになっている．米国の産業界においても ‘business ecosystem’ という用語が同様の意味をもって定着している[1]．

NSTIC には，アイデンティティエコシステムが準拠すべき「指導原則（Guiding Principle）」として，下記の 4 つの事項を掲げてられている．

1. よりプライバシを保護し，ユーザが自発的に選択するものとする
2. セキュアかつ弾力的（resilient）なものとする
3. ポリシーについても技術的にも相互運用可能なものとする
4. 費用対効果が高く，使い易いものとする

この種のアイデンティティ管理サービスには，随意的な信頼モデルをもち，複数の利害関係者が参画して機能するというエコシステム的な特徴を備えているものがある．NSTIC は，民間で開発されているアイデンティティ管理サービスを，ある種の政策フレームワーク内に位置づけるための認定制度を公式に支持したものである．したがって，NISTIC が意図する「エコシステム」には複数の利害関係者が参画する循環系であるという特徴のみならず,「適者生存」をも示唆するメタファになっている可能性がある．

この政策フレームワークは，本人認証システムについて，そのトランザクションに想定されるリスクに基づいて複数レベルの技術的な要件を掲げる基準を設けて，相応の運用を承認するものである．このような政策フレームワークが成立すれば，複数の適するサービスが同時並行的に認定されて，利用されることが想定されている．ここに「適者生存」のような意味合いがある可能性がある．これまでの米国の連邦政府の情報セキュリティに関する政策の多くが，政府調達の要件を規定していたのみであったのに対して，NSTIC は官民が連携する内容を含んでいる．

[1] http://lexicon.ft.com/Term?term=business-ecosystem

1.3 NSTIC における政府の役割

連邦政府の役割として，民間のアイデンティティエコシステムの開発を支援し，それらが「指導原則」に則ったものとなるように提携する役割があるとされている．特にプライバシーの保護に関しては，FIPP（Fair Information Practice Statement）[10] への準拠性が目標として掲げられている．そして，既存の民間アイデンティティエコシステムを利活用して先行事例を作ることによって，民間活動を導くことも掲げられている．

州政府等の役割として，概ね連邦政府と同様の役割を担うと記述されている．ただし，構成員である市民とより密接に接する位置にあり，市民の啓発を重視するように促されている．

1.4 正式版公開までの経緯

NSTIC のドラフト [2] が 2010 年 6 月 25 日に発行されていた[2]．今年の 4 月に公表された正式版との間には，内容な差異が複数ある．

- 上述の「指導原則」を掲げる順序も変わり，よりプライバシを保護し，自発的な（ユーザによって選択される）ものとする」ことが目立つように配置された．
- この政策の実施する際の調整の役割を担う組織として，商務省に NPO（National Strategy Office）が設置されることが明記された．
- ドラフト段階では，ビジョンと共に便益を説明するために，3 つのレイヤー（実施（Execution），管理（Management）および統治（Governance））ごとに説明されていたが，正式版においては削除されてしまった．
- ドラフトには「権威ある源泉（authoritative source）」についての記述が 4 箇所，存在していたが，正式版においては，それらのすべての箇所が修正されて，このキーワードが無くなった．本稿の後方においては，この「権威ある源泉」について検討する．

[2] http://www.whitehouse.gov/blog/2010/06/25/national-strategy-trusted-identities-cyberspace

2 LoA フレームワークの系譜

NISIC のフレームワークが想定している「LoA（Level of Assurance：保証レベル）」について，これを規定しようと試みてきた仕様の系譜を振り返る．現時点において NSTIC の政策フレームワークとして用いられることが想定されていると見受けられるのは，2003 年に OMB（Office of Management and Budget）から発行された M-04-04[11] に定義されている 4 層の LoA である．このような 4 層のレベルが一朝一夕に定義されたわけではない（図 1）．

2.1 ブリッジ CA の CP フレームワーク

複数レベルの保証要件という発想の原型は，PKI 技術におけるブリッジ認証局（Bridge Certification Authority）の CP（Certificate Policy）に由来する．

複数の PKI ドメインをブリッジさせるときには，同等の保証レベルの PKI ドメインと信頼関係を構築する必要があるため，証明書上の CP 項目に基づいて同等性を判定する．国際的な標準化活動の中で，CP 項目のフレームワークについて規定する IETF の RFC 2527[16] は 1999 年 3 月に発行された．この RFC は，CP のみならず CPS（Certificate Practices Statement）についても，そのフレームワークを規定したものである．

これをきっかけとして，同年に米国連邦政府の FPKI（Federal PKI）のブリッジ CA が発行する証明書の CP について，4 つの保証レベル（Assurance Level）が検討されて発行された [12]．具体的に，X.509 証明書上に，このような CP 情報を収めて渡すものとして規定されている．この CP についての参照フレームワークは，M-04-04[11] のフレームワークの中では，高位の「レベル 3」および「レベル 4」が規定されたことに形跡が残っている．また，この頃，米国においては官民連携させるためのブリッジ PKI が検討されていた [12]．

国際的な標準化案件の中にレベルについての記述が現れるのは，RFC 3647[17] 以降である．このフレームワークの中に複数レベルの CP を設定することができ，この仕様にはカナダ政府の PKI における CP 設定の用例が示されている．

ちなみに，同 2000 年日本の電子政府の GPKI のポリシー設計を記述した『GPKI 相互運用性仕様書』[8] の策定の際には，米国 FPKI の証明書プロファイルや CP からの影響を受けたが，それらの CP としては，ひとつのみを規定したので複数のレベルを備えているわけではない．

2.2 連邦政府調達フレームワーク

既述のように，2003 年 12 月，OMB から M-04-04 というメモランダム [11] が発行されたが，これは連邦政府システム調達における本人認証に関する要件についてのものである．

これを受けて，NIST が SP 800-63: “Electronic Authentication Guideline” の策定に着手し，これが 2006 年 10 月に発行された [15]．これは，卑近なパスワードによる本人認証や，台頭してきた SAML 等の連携認証を含めて，それらが，どのレベルの要件に適合するのかを指し示す基準として策定されたものである．

同時並行的に，e-Authentication Initiative のもと，官民が連携する EAP（Electric Authentication Partnership）が民間側に編成されて，ポリシー等のフレームワークが検討された．これが，Liberty alliance に移管されて，今日の Kantara INITIATIVE における EAP の活動となっている．

PKI 以外の本人認証サービスを，このフレームワークに具体的に当てはめようとする活動として，ICAM（Identity, Credentials, and Access Management）[3] が政府側で活動している．

このように，LoA の定義は連邦政府調達における業務要件として定義されている．

2.3 トラストフレームワーク策定の困難性

2010 年 2 月に発行された Kantara INITIATIVE の IAF（Identity Assurance Framework）[13] は，アイデンティティ管理サービスを認定するためのフレームワークを SP 800-63[15] に基

[3] http://www.gsa.gov/portal/content/105208

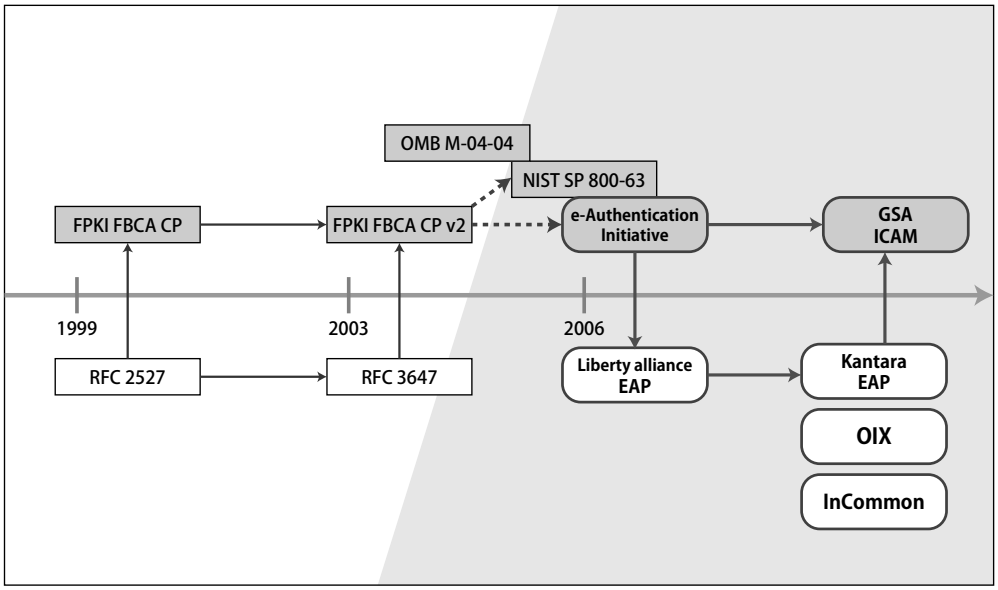

図 1: LoA フレームワークの系譜

づいて規定しようとしてしている．このような各レベル要件に基づく認定制度のためのフレームワークは，トラストフレームワークと呼ばれている．OIX（Open Identity eXchange）も，トラストフレームのモデルを作成しようとしている[4]．トラストフレームワークを実現するためには，その過程を証明するための監査制度が必要となり，その設計は容易ではない．

アイデンティティ管理サービス産業を「レモン市場」にしないようにするためには，レベルを技術的に規定する基準や，基準に則った認定制度が重要な役割を果たす．一般に，広い範囲の技術を対象とするようにすると，それらの技術の多様性に起因して技術基準が複雑になってしまう．今般のアイデンティティエコシステムの分野においては，おそらくこのような複雑性に起因して，PKI のブリッジ CA の CP についての RFC 3647[17] に相当する技術的な参照フレームワークが，対象範囲とする技術に渡って存在していない．技術的にも，制度設計上も，困難な検討課題が残されている．

また，後述する「権威ある源泉」が，曖昧なままでは，均等なトラストフレームワークの運用が想定し難い．広域ドメインに適用することを想定すると，国や州の制度の違い等に起因して，本人確認の証拠資料の証拠力が異なるシステムを，同等に扱ってしまう制度となる懸念が残る．

「エコシステム」として運用する制度を設計するためには，すべての利害関係者に何らかのインセンティブがあるような構造に設計する必要があろう．

3　政府の他の役割：権威ある源泉

そもそも「公的なアイデンティティとは何か?」は，国の文化に拠る．国民のアイデンティティ情報についての「権威ある源泉」は，多くの国々においては現在も国によって管理されているが，米国はその例外となる．

[4] urlhttp://openidentityexchange.org/what-is-a-trust-framework

3.1 米国

一般に，本人確認に関する事項は州法において規定されているようであり，米国連邦政府の公文書において「権威ある源泉」について記述することに関しては難しいようである．既述のように，今回の正式版からも「権威ある源泉」についての記述が削除されている．今回の NSTIC 以外にも，例えば，NIST がアイデンティティクレデンシャル仕様について草稿していた SP 800-103 という案件が頓挫してしまっている例もある．

3.2 欧州

EU（European Union）の域内各国においては,「電子署名指令」に基づいて，電子署名アプリケーションの相互運用可能性の論点が重視されてきた [7]．そのような電子署名アプリケーションにおいて，個人のアイデンティティ情報を何らかの法的な根拠に基づいて表現する際の X.509 証明書のプロファイルとして QC（Qualified Certificate）が規定されてきた [4].

この QC が，公的なアイデンティティを示す X.509 証明書項目の基準となっており，この証明書に基づくディジタル署名が，否認防止用に利用されている．さらに，近年，QC プロファイルをもつ本人認証用の証明書も発行・利用されるようになってきた [14].

今日，欧州（EU）は，広く市民に手元トークン（IC-ID カード）をもたせる施策をとっている．EU 政策は，域内のどの国においても同様に，カウンター越しに手元トークンによって身元を証明できるようにすることと，域内各国のインターネットサーバー上の電子商取引を同様に行えるようにすることを重視している．このようなことが，QC プロファイルを生んだ背景にある．身元確認の厳密さを求める故,「公的なアイデンティティ」を各国の政府が証明することが前提とされている．

3.3 日本

わが国における本人確認に関する「権威ある源泉」に相当するものとして，戸籍および外国人登録の制度がある [3]．それらの「権威ある源泉」は地方自治体によって管理されているが，法的には国の役割が市町村長によって管掌されている構造にある [5]．そもそもアイデンティティ情報が紙で管理されていた時代には，それらは民間側には無かった．

政府が管理するアイデンティティ情報についての「権威ある源泉」としての役割をアウトソースすることは，現状では想定し難い．わが国においてトラストフレームワークのような政策フレームワークについて制度設計を行う際には,「権威ある源泉」を管理するという政府の役割についても考慮する必要がある．

4 まとめと展望

米国の NSTIC は，わが国の今後の政策フレームワークを検討する際に参考になるが，単純に模倣できない部分もある．

わが国の『オンライン手続におけるリスク評価及び電子署名・認証ガイドライン』[6] を策定した際には，米国連邦政府の LoA に基づいて検討した経緯があるので，今般の NSTIC とも親和性がある．ただし，NSTIC の「エコシステム」も始まったばかりであり，そのトラストフレームは一朝一夕には仕上がらない．

NSTIC には「エコシステム」達成のために，国際的な関係の重要性と，他国との相互運用可能性に関する民間支援について明記されている．国際的な標準化案件として，具体的に ISO/IEC JTC 1/SC 27 においては，29115[5] という案件があり，米国が主導している．このような案件について長期的な視野で注視していく必要があるとともに，参画していく必要もある．

一方、わが国においては,「権威ある源泉」についての政府の役割についても整合的に制度設計する必要がある．

[5] http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45138

参考文献

[1] The White House, “NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE” (15 April 2011) http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

[2] DHS, DRAFT “National Strategy for Trusted Identities in Cyberspace” (25 June 2010) http://www.dhs.gov/xlibrary/assets/ns_tic.pdf

[3] 宮川 寧夫, 松本 泰, 須川 賢洋,「わが国の本人確認に関する諸法の現状と課題」,『CSS2010 予稿集』(2010 年 10 月)

[4] 宮川 寧夫, 松本 泰,「QC プロファイルの整合的な利用法」,『CSS2009 予稿集』(2009 年 10 月)

[5] 中村 秀治, 「 『国民 ID』としての新たな社会基盤の必要性」, Web, <http://www.mri.co.jp/NEWS/localweb/report/2030312_2091.html>

[6] 各府省 CIO 連絡会議,『オンライン手続におけるリスク評価及び電子署名・認証ガイドライン』(2010 年 8 月 31 日) http://www.kantei.go.jp/jp/singi/it2/guide/guide_line/guideline100831.pdf

[7] 電子政府ガイドライン作成検討会,『セキュリティ分科会報告書』: 29–31 (2010 年 2 月) http://www.kantei.go.jp/jp/singi/it2/guide/security_guide_line/siryou2.pdf

[8] 基本問題専門部会, 『政府認証基盤相互運用性仕様書』(2001 年 4 月 25 日) http://www.gpki.go.jp/session/CompatibilitySpecifications.pdf

[9] Nelson E. Hastings, W. Timothy Polk, “Bridge Certification Authorities: Connecting B2B Public Key Infrastructures” (2000) http://csrc.nist.gov/groups/ST/crypto_apps_infra/documents/B2B-article.pdf

[10] Federal Trade Commission, “Fair Information Practice Principles” (Last Modified: 25 June 2007), Web, <http://www.ftc.gov/reports/privacy3/fairinfo.shtm>

[11] OMB, M-04-04: “E-Authentication Guidance for Federal Agencies” (16 December 2003) www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf

[12] FPKIPA, “X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA)”, Version 1.12 (27 December 1999) http://www.pubklaw.com/ecomm/fbcacp03122001.pdf

[13] kantara INITIATIVE, “Identity Assurance Framework: Overview” (February 2010) http://kantarainitiative.org/confluence/download/attachments/38371432/Kantara+IAF-1000-Overview.pdf

[14] Stork Project, 2.3D: “Quality authenticator scheme” (3 March 2009) https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=577

[15] NIST, SP 800-63: “Electronic Authentication Guideline” (April 2006) http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

[16] IETF, RFC 2527:“Certificate Policy and Certification Practices Framework” (March 1999) http://tools.ietf.org/html/rfc2527

[17] IETF, RFC 3647:“ Certificate Policy and Certification Practices Framework” (November 2003) http://tools.ietf.org/html/rfc3647