第 5 章　電子認証フレームワークのあり方

内容

- ガイドラインのターゲット
- ガイドラインの提示すべき内容
- ガイドラインの策定と維持管理のあり方
- ガイドライン策定に際して留意すべき事項

5. 電子認証フレームワークのあり方

本章では前章で示した問題意識のもと、電子認証フレームワークの中での BCP の位置づけにおいて日本国内で策定すべきガイドラインの要件について検討する。

5.1. ガイドラインのターゲット

ガイドラインの外形的要素として、対象、用途、想定利用者などのターゲットについての望ましいあり方について議論する。

5.1.1. ガイドラインの対象

電子署名については法制度が整備されつつある。従って電子認証と同様にガイドラインへのニーズは共に高いと考えられるが、電子署名には PKI の検証者がユーザ側に存在し、信頼性の構造は電子認証に比べて若干複雑である。そこで当面のターゲットは電子署名を除き、ノウハウが溜まりやすい分野を対象とする。

また、電子書名は長期保存についても考慮すべき点が通常の電子認証とは大きく異なり、統一的に扱うことが難しいことから、長期保存についてもターゲットからは除外することが適切と言える。

このほか、ガイドラインの対象とすべきターゲットについて、専門家会合において以下の意見が指摘されている。

- 自然人の領域についてはこれまでに利用されている例が多く、かつ法的な強制の適用が適切でない分野であり、ベストプラクティスに基づくガイドラインを適用することが望ましいと言える。
- レベルの高い保証レベルにおいては、ボトムアップに基づくベストプラクティスといった弱い縛りによるものは運用上の高い水準の確保の誘因にはなりにくく、強制力を持った形での適用が必要ではないか。

5.1.2. ガイドラインの用途

電子認証に関しては、現在 PKI を利用してシステムを構築している SI 業者や開発者が短期的な開発方法を繰り返すなどの結果、システムの構築過程において、ベストプラクティスといえる内容がほとんど蓄積されていない状況にある。これは開発の都度試行錯誤を行うことになるため非効率であるだけでなく、情報セキュリティの確立のために必要な要件が見落とされる可能性が高まるなど、社会基盤としての PKI の確立ならびに発展において望ましいことではない。

そこで、ガイドラインに求められる最も重要な役割は、開発者に向けて「有効で目安となる電子認証基盤の使い方」に関する情報を提示することであると考えられる。

5.1.3. ガイドラインの想定利用者

ガイドラインの想定利用者としては、電子認証フレームワークのステークホルダであればそのすべてが対象となりうる。具体的には以下の利用場面が想定される。

- サービスの調達者：電子認証サービスの機能仕様を検討する際に参照する
- サービス構築者：機能仕様をもとに電子認証機能を実装する際に参照する
- サービス提供者の団体・組織：組織間で利用すべき電子認証サービスのあり方を議論する際に参照する

これらはいずれもガイドラインの適用がふさわしい場面であるが、前項におけるガイドラインの用途を想定した場合、想定利用者としてはサービスの構築者および PKI システムの開発者が中心となることが考えられる。

5.1.4. 電子認証フレームワークにおける策定プロセスの位置づけ

前項におけるニーズに対応するための電子認証フレームワークを構築するためにふさわしい策定プロセスのあり方について検討する。

5.1.4.1. 電子認証フレームワーク策定に係る論点

前述した議論を踏まえ、電子認証フレームワークを策定するにあたって検討すべき論点を以下に示す。

（1）　電子認証フレームワークのターゲット

電子認証フレームワークのターゲットとすべき領域について、JPNIC 専門家チームメンバである松本泰氏のアイデアをもとに、以下の３種類の視点を３次元の軸としてとらえ、現在の電子署名・電子認証のターゲットを立体上に投影したもの（発案した松本氏にちなんで「松本キューブ」と呼ばれている）を示す。

- ｘ軸：認証対象（デバイス、サーバ、自然人（その他 、法人、職権なども想定））
- ｙ軸：サービスの種類（電子署名、電子認証、暗号）
- ｚ軸：レベル（低 ←レベル１・２・３・４→ 高）

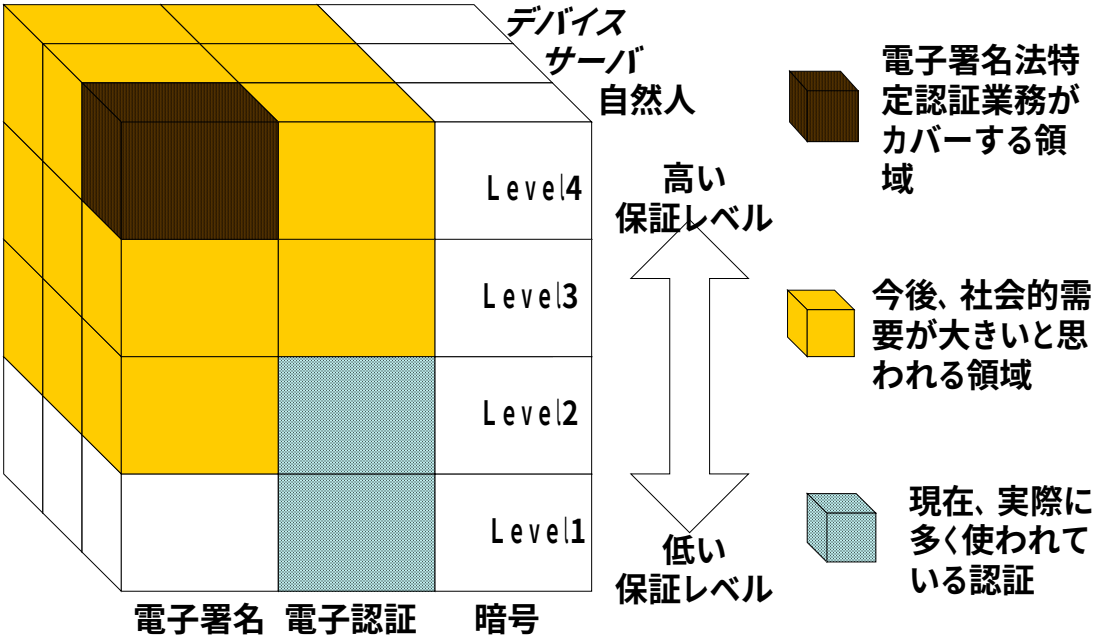

図 5－1　電子認証のターゲットについての図示例（松本キューブ）

この図は現在の電子認証における以下の状況を表象している。

- 電子署名法における特定認証業務でカバーしているのは、電子署名、自然人、レベル４のブロックに相当。
- 現在、実際に多く使われている認証は、電子認証、レベル１～２、自然人のブロックに相当。
- 今後社会的需要が大きいのは、電子署名＋電子認証、レベル２～４、デバイスやサーバの領域と思われる。

（2） 策定主体

電子認証フレームワークの策定主体になるべき組織に対しては、以下の要件が求められる。

- 民間組織であること。これは、民間主導によるフレームワークであることから必須の要件となる。
- 既存の電子認証サービス事業者において、策定主体との関係により事業者間に不公平の生ずることがないこと。

BCP はコンセンサスを基にするため、策定主体となるグループは WG の参加者に相当することになるが、実質的には WG のチェアとなる。

（3） メンテナンス主体

電子認証フレームワークをメンテナンスしていく主体については、策定主体と同一である場合、異なる場合のいずれも想定されるが、要件としては(2)で示したものと同一と考えられる。

5.1.4.2. 電子認証フレームワークを実現させるための策定プロセスのあり方

上述の論点はいずれも重要な課題であり、最適なフレームワークを策定するためには検討すべき事項も多い。ただし、フレームワークを早期に導入、活用したいというニーズも強く、策定に長時間をかけることはこうしたニーズを損ない、電子認証サービスにおける構築・運用コストやリスクの増大を招く恐れがある。

こうした状況において、ここでは電子認証フレームワークを IETF における BCP として位置づけることの可能性について検討する。

（1） BCP（Best Current Practice）としての策定が適切となる条件

IETF において BCP として公開されているドキュメントには、すでに広く利用されている手続きや規範を扱ったものが多く、ドキュメントの実用的な側面が重視されているが、Informational RFC に位置づけられるドキュメントと異なり IESG（Internet Engineering Steering Group）による承認を経ることによる公共的な性質も持ち合わせている。

こうした BCP として策定することが適切となる条件としては、以下の要素が想定される。

- すでに実践に供されている規範、成功事例がある
  BCP は現行の取りうる方策の中で最善であることが前提であるため、電子認証フレームワークで規定される内容はいずれも実践に供され、成功事例といえる成果を得ていることが求められる。
- 内容をあらかじめ最適化することが困難
  最適化することが可能な方策の場合は、BCP という手法をとらなくとも、当初から最適案で合意形成が可能なことが多い。

（2） BCP（Best Current Practice）としての策定することによる利点

BCP として策定することによる利用者への利点としては、以下が挙げられる。

- スピーディーな提供が可能
  既存の実践例をもとにドキュメント化し、関係者の合意を得た上で公開する手続きとなるため、新たに根本から方法を議論する場合と比較して策定に必要な期間が短い。
- 分野を超えた利用が可能
  BCP としての位置づけを与えることで、何らかの分野の中で適用可能な BCP があれば、分野に拘ることなくその成果を相互利用できるメリットを期待することが可能となる。

（3） BCP が成立するための条件

電子認証フレームワークを BCP として策定する方法には(2)で示したような利点がある反面、これを成立させるために以下のような条件を満足させる必要がある。

- 成功事例が存在していること
  BCP は現状におけるベストプラクティスとしての意味づけをもつため、ここに盛り込まれる内容については、これまでの実践において成功を得た事例が存在する必要がある。ただし、これはフレームワークにおいて想定しているターゲットと同一である必要はなく、今回の例であれば海外の同様のドキュメントなどを参考にすることで条件を満たすことも可能である。
- 想定ターゲットとなるフレームワークの利用者が策定プロセスに参加もしくは委任すること
  BCP の公正性、客観性等は策定メンバーの構成と策定プロセスの公開によって保証されることになるため、策定に際しては想定ターゲットとなるフレームワークの利用者が策定プロセスに参加することが望ましい。ただし、利用

者が策定プロセスに参加するために必要な知識を持ち合わせているとは限らないため、策定プロセスへの委任を得ることによっても差し支えない。

5.2. ガイドラインの提示すべき内容

ここでは、前項の対象に向けたガイドラインにおいて、「経験上有効で目安となる使い方」の情報として、具体的に提示すべき内容について検討する。

5.2.1. 開発・構築関連

電子認証サービスの開発・構築の際に有効な BCP として、以下の内容を規定することが想定される。

5.2.1.1. 認証の保証レベル

電子認証サービスにおける保証レベル（assurance level）については、海外ではすでに広く利用されているにもかかわらず日本では GPKI（Government Public Key Infrastructure - 政府認証基盤）などを含めても準拠可能なレベルの規定がなく、ガイドラインで提示する内容の中で最も高いニーズがあると考えられるものの１つである。反面前例がないだけに、ガイドラインにおいてその概念について十分な説明を行うことが必要となる。

保証レベルに関してガイドラインにおいて言及すべき内容を、以下に列挙する。なお、ここでは民間用途を想定し、政府認証基盤における保証レベルの扱いについてはガイドラインで定める内容の対象外とする。

（1） 保証レベルの定義

レベルについては認証対象を限定せずに規定する。段階数については、海外との共通性の観点から、４段階程度に分割することが想定される。

2.2 節において示した通り、米国政府による“ E-Authentication Guidance for Federal Agencies ”における保証レベルの区分は下表のようになっている。

表 5－1　"E-Authentication Guidance for Federal Agencies"が定める保証レベル

レベル	保証の程度	定義
1	最低限の保証	正当性への信頼はほとんどまたは全くない
2	低い保証	正当性に対する若干の信頼がある
3	中程度の保証	正当性への信頼は高い
4	高い保証	正当性への信頼は非常に高い

（2） 認証の対象と保証レベルとの対応

(1)で認証対象を限定せずに保証レベルを規定した上で、本項で認証対象との対応関係を検討することで柔軟な適応性を実現する。認証対象としては、以下を想定する。

- 個人
- サーバ
- 機器に割り当てられた IP アドレス

このうち個人認証については、(1)で示した米国政府のガイダンスでは以下の 2 種類の区分を想定している。

- 身元（identity）認証
- 属性認証（例：退役軍人、米国市民、等）

このほか、個人認証については、扱う情報がセンシティブ情報かどうかでさらに細分化することも考慮の対象となる。

（3） 保証レベル決定のための必要作業と手続き

新たな電子認証サービスにおける保証レベルを決定する手順として、以下の項目についての対応方法を定めることが想定される。

- 電子認証サービスに対するリスク評価（リスクアセスメント）の手続き
- 用いるべきリスク分析手法
- 評価結果と保証レベルとの対応づけに関する合意形成プロセス

（4） 既存の制度と補償レベルの対応関係

電子署名法の要件に準拠したシステムなど、一定の情報セキュリティ要件を満たした場合に、自動的に一定の保証レベルを割り当てることについても、保証レベルの検討とあわせて考慮する必要がある。

5.2.1.2. 電子認証サービスで用いる情報システムの要件と保証レベルとの対応づけ

各保証レベルに対応する、電子認証サービスで用いる情報システムにおいてあるべき要件について、以下の観点から整理する。

（1） 本人確認手段

個人を認証する場合、サービス提供事業者が行う本人確認の確認方法と、保証レベルとの対応を定める。

本人確認手段としては、以下の２種類について検討する必要がある。

- 登録時（対面、確認文書、証明者、等）
- サービス利用時（PIN・パスワード、認証デバイス（IC カード、トークン等）、バイオメトリクス等）

策定内容の参考として、EU の“IDA Authentication Policy”が本人確認手段として定めるトークンの例を示す。

表 5－2　保証レベルに応じたトークンの種類

トークンの種類	保証レベル（○＝使用可能、×＝使用不可）			
	1	2	3	4
ハード暗号トークン（認証を必要とするスマートカード等）	○	○	○	○
ソフト暗号トークン（メディアに保存された暗号鍵等）	○	○	○	×
ワンタイムパスワードデバイストークン	○	○	×	×
パスワードまたは PIN トークン（利用者が暗記した文字列）	○	×	×	×

（2） 認証結果の有効期限

認証に成功した結果を、どの程度の期間有効と認めるかの基準について定める。(1)と同様、EU の“ IDA Authentication Policy ”における有効期限の例を示す。

表 5－3　保証レベルに応じた有効期限

有効期限	保証レベル（○＝使用可能、×＝使用不可）			
	1	2	3	4
24 時間	○	×	×	×
12 時間	○	○	×	×
2 時間	○	○	○	×
直ちに	○	○	○	○

（3） システムにおけるアクセス制御措置

電子認証に関わるシステムで利用するサーバにおけるアクセス制御に関する措置との対応関係を定める。アクセス制御方式としては、以下が想定される。

- OS における強制アクセス制御
- 管理者権限の分割・最少化
- デュアルコントロール（複数の管理者の同席を前提とした制御）

（4） システムを構成する機器における認証取得

認証に関わるシステムの構成製品が取得している情報セキュリティ評価・認証制度（ISO/IEC15408 - Common Criteria）の認証レベルとの対応関係を定める。

5.2.1.3. 電子認証サービスのマネジメントと保証レベルとの対応づけ

各保証レベルに対応する、電子認証サービスのマネジメントにおいてあるべき要件について、以下の観点から整理する。

（1） 情報セキュリティマネジメントシステム（ISMS）

各保証レベルに応じた、電子認証サービスにおける情報セキュリティマネジメントシステム（ISMS）についての要件について定める。

（2） セキュリティ監査の方法

各保証レベルに応じた、情報セキュリティ監査として実施すべき要件について定める。

（3） 失効情報の取得と検証

保証レベルに応じた失効情報の扱いについて規定する。なおこの扱いに関して、すでに保証レベルに基づいた運用を行っている米国の Federal PKI においては、低いレベルにおいては失効情報そのものを扱っていないことを考慮し、本ガイドラインにおいても保証レベルにより失効情報の取り扱いの有無を含めた検討を行うものとする。

5.2.1.4. 電子認証サービスの構成要素毎のベストプラクティス

（1） 信頼点（トラストポイント）

信頼点に関しては、相互認証を円滑に実現するなどの視点から共通の規範をベースに提供されていることが望ましい。そこで、RFC3647、RFC4158 の内容などを考慮しつつ、以下に示す項目について提示することで、信頼点の設定に関する共通化を促すものとする

- 証明書検証者への情報提供方法
- 信頼点の認証局の信頼性担保の仕組み

（2） 登録局（RA）

認証局については、以下の内容が想定される。

- 登録局で行うべき業務の内容
- 保証レベルの区分への対応

（3） 証明書

特殊な証明書についての情報提供を行うことが想定される。

- 職権証明書
- 仮名証明書（欧州で利用）

（4） リポジトリ

認証局などが有するリポジトリの相互利用に関して、その整合性を確保するための複製や連携の方法などについて規定することが考えられる。

（5） ユーザ環境

ガイドラインにおいてユーザ環境について規定すべき項目としては、以下が想定される。

- 鍵ペアの運用環境のあり方
- 失効情報の取得と検証

このうち失効情報についてはエンドユーザにおける対応に関して現状で問題点が多いことから、ガイドラインで規定することが有用と考えられる。

5.2.1.5. 失効情報の取得と検証

失効情報を扱う際に考慮すべき項目として、以下を想定する。

- 失効情報の伝達方法の特徴（OCSP と CRL の違い：データサイズ、伝達時間の長さ等）
- 失効情報の取り扱いの期限
- 失効情報の受付方法（例：ポータルにアクセスすると失効情報がチェックされるなど）

5.2.1.6. 証明書利用者（EE）への情報提供

証明書利用者に対して、以下の項目についての情報提供を行う。

- 信頼点の証明書、検証パス、ポリシーの相互運用
- オブジェクト識別子（OID）とは

- オブジェクト識別子の取り方、管理方法

5.2.1.7. 分野別の要件（保健医療、金融、教育等）

以上の項目のほか、分野別のベストプラクティスとして、以下の各分野についての規定事項を追加することが想定される。

- 保健医療分野
- 金融分野
- 教育分野

こうした分野別の項目は、本来共通にすべきであるが経緯上複数の規範が存在するような場合の打開策としても適用が可能である。

5.2.1.8. コストとの関係

電子認証に関するサービスレベルを決定する際に、構築・運用に要するコストと運用時のリスクについて情報を提供することは有用と考えられる。ただし、分野を特定しない状態で定量的な議論を行うことは困難であることもあり、コストとリスクに関する要因とその相互作用についての指摘にとどまることも想定される。

5.2.2. 運用関連

電子認証サービスを運用もしくは保守していく際の BCP として、以下の内容を規定することが想定される。なお、これらの事項をとりまとめ、運用規程のテンプレートとして提供することも考慮することが望ましい。

5.2.2.1. 失効情報の取扱い

保証レベルの箇所でも言及しているが、失効情報についてはこれまでの認証サービスにおいて適切に扱われてきたとは言えない。ガイドラインにおいては、一定の保証レベル以上で運用する場合、最新の失効情報を反映させることを求めることになる。

5.2.2.2. 危機管理対応

電子認証サービスにおける緊急事態発生時の危機管理（Crisis Management）として

対応すべき対応（緊急時対応、業務継続計画（Business Continuity Plan））について定めるものである。想定される緊急事態の例としては、以下のケースを想定する。

（1） 秘密鍵の漏洩

認証局等において管理している秘密鍵に関する機密性が破られた場合に関係者が行うべき対策とその実施手順を規定する。

（2） 暗号アルゴリズムの危殆化

暗号アルゴリズムそのもの、もしくは認証サービスにおいて利用している実装において欠陥が発見され、認証サービスにおける機密性や完全性が確保されない恐れが生じた場合に講じるべき対策とその実施手順について規定する。

（3） 認証局サーバへの不正アクセス、悪意のソフトウェアの侵入

認証局を運用しているサーバへの不正アクセスやコンピュータウイルス、ワーム等の侵入が発生、ないし発生する恐れがある場合の対策とその実施手順について規定する。

5.2.2.3. 証明書利用者（EE）に必要とされること

これまでは、証明書利用者のうち、いわゆるエンドユーザを対象にセキュリティ確保を目的として何らかの義務を課したりすることは困難とされてきた。ただし、電子認証サービスにおいて一定の保証レベルを確保するためにはすべての参加者が安全管理を行うことが欠かせなくなるため、以下に示すような事項の遵守をもとめることについて規定する。遵守を規定する方法としては、こうした内容について了解した旨を同意書の形式で提供することなどが考えられる。

（同意書の記述項目の例）

- サービス利用に先立って認証局証明書を確認すること
- 秘密として扱うべき情報を漏洩させてはいけないこと

5.3. ガイドラインの策定と維持管理のあり方

これまでの議論をもとに、IETF における BCP の策定プロセスを日本国内で適用した場合の、ガイドラインの策定とその後の維持管理のあり方について検討する。

5.3.1. ガイドラインの策定プロセス

前節で示したように、IETF における BCP ドキュメントの策定プロセスは以下の手順で行われる。ここでは、確認のためそれぞれのプロセスの要旨を示す。

（1） Internet-draft の提出

誰もが自由に投稿できるドキュメントとして、Internet-draft が提出される。

（2） Internet-draft の公開

提出されたドキュメントを、IETF は自らのサーバを通じて６ヶ月間公開する。

（3） 支持に基づく IESG への申請

公開中の意見をもとに、広くインターネット業界に有用な情報を含んでいると判断された場合、BCP にすることについての IESG への申請が行われる。

（4） IESG によるレビュー・承認

申請をもとに、IESG が申請内容をレビューし、BCP とすることが適切と判断された場合は承認の手続きが行われる。

（5） BCP としての登録・公開

申請が承認されると、ドキュメントには RFC 番号（あるいは BCP 番号）が割り当てられ、公式に IETF の FTP および Web サーバを通じて恒常的に参照可能なドキュメントとして扱われるようになる。

これと同様の手続きを経るべく、ガイドラインの策定プロセスとしては以下の手順を想定する。

（1） 民間におけるニーズに基づく趣意の表明

電子認証フレームワークの一環として電子認証に関わるガイドラインを策定する旨の趣意の表明を行う。

（2） 趣意の内容の公開

以下の項目を含んだ趣意を公開し、関係者（ステークホルダ）からのコメントを集める。

- 文書化の目標
- 利用対象者
- 策定作業期間
- レビュ対象者

（3） 趣意に基づく活動の実施

外部からのコメントをもとに、ワーキンググループ等の活動を通じてガイドライン案の作成作業を行う。

（4） ガイドラインの策定

作成されたガイドライン案を公開し、コメントを得た上で承認プロセスを経て策定に至る。

（5） 新たなニーズに基づく更新

運用・マネジメントのプロセスとして、ガイドラインの実施を通じて得られた影響、反応、意見等を踏まえ、ガイドラインの更新プロセスを継続的に実施することになる。

5.3.2. ガイドラインの展開のあり方

ガイドライン策定後の展開として、ある分野を対象とした BCP を電子認証フレームワークを通じて別の分野に適用すべく改良することが想定される。この関係を次図に示す。派生的な BCP について議論する手段としては、直接ワーキンググループ（WG）会合を通じて行うだけでなく、メーリングリストやソーシャルネットワークサービス（SNS）を使って行うことも想定される。

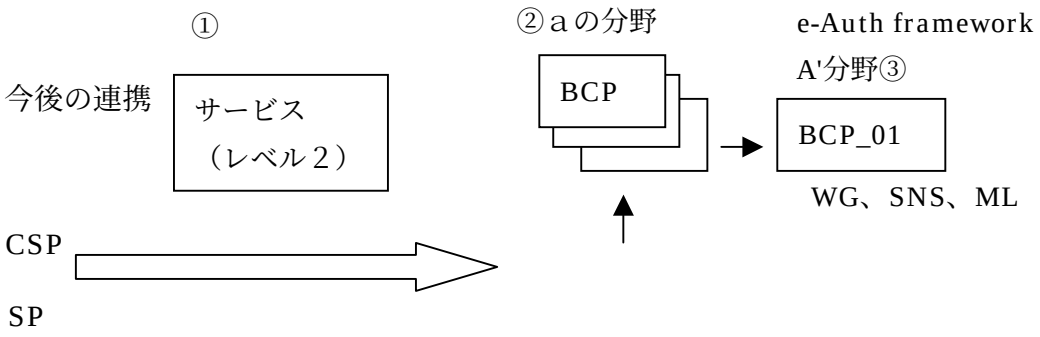

図 5−2　他分野への BCP を通じた連携

5.4. ガイドライン策定に際して留意すべき事項

これまで議論してきたガイドラインが有効に機能する範囲について確認する。

5.4.1. ガイドラインが機能しない条件

日本国内における電子認証分野において、本ガイドラインの適用対象外、もしくは適用対象であっても有効に機能しないと考えられる条件について考察する。

5.4.1.1. ガイドラインの適用対象外となる事例

電子認証サービスのうち、以下の事例については本ガイドラインの適用対象外となるものと考えられる。

（1）　電子認証の仕様や運用に関する規程が独自に定められている分野

分野を限定して、電子認証に関して独自の規程を適用することが定められている場合は、本ガイドラインの適用対象にはなり得ない。現時点においては日本国内においてこうした分野の事例はないが、「保健医療福祉分野 PKI 認証局 証明書ポリシ」が 2005 年に策定されるなど、独自の規程を策定しようとする動きが見られる。

（2）　セキュリティ対策の不十分な認証サービスを許容している分野

当然ながら、本ガイドラインの定める内容を満たすことを前提としない認証サービスにおいては、一部組織が本ガイドラインに準拠しても全体のサービスレベルは本ガイドラインの想定している水準を満たさない。このようなサービスについては本ガイドラインの適用対象外となる。

5.4.1.2. ガイドラインの適用対象であっても有効に機能しない事例

前項とは別に、ガイドラインの適用対処とすることは可能であるが、実際には有効に機能しないと判断される分野の事例を挙げる。

（1）　高度なセキュリティを規定する必要がある分野

通常と比較して極めて高度なセキュリティを要求される分野については、各組織が本ガイドラインに準拠する形で、電子認証サービスにおいて必要なセキュリティを確保す

ることは容易ではない。これは、ベストプラクティスに基づいて要件を定める方式が、高いレベルのセキュリティ要件の規定には適していないことによる。このような条件の場合は、強制力をもった規程を定め、サービスの参加組織にこれを遵守させることが必要となる。

（2） 高度なセキュリティを規定する必要がある分野

ここで対象としているガイドラインは民間主体で策定するものであるが、国をはじめとする行政機関、公的機関において、本ガイドラインに基づいた電子認証サービスの構築、運用を行うことを妨げるものではない。ただし、一般に行政の提供するサービスには行政固有の要件を必要とする場合が多く、電子認証サービスにおいてもそうした要件を行政において独自に規定する場合は、本ガイドラインに準拠しているとみなすことは難しくなる。

このほか、以下の条件が満たされる場合も、行政機関等が独自のガイドラインの策定する動機となり得る。

- ガイドラインの策定主体、策定プロセスが中立的とみなしにくい場合
- 何らかの理由の結果、本ガイドラインの維持・管理が将来的に継続的に行われることへの信頼感が得にくい場合

5.5. まとめ

日本における電子認証サービスにおいては、幅広く利用可能で保証レベルを定めたガイドライン的な役割を担うドキュメントが存在せず、本来必要であるべき安全性が確保されないまま PKI システムの構築が進んでいく恐れがある。

こうした中で、IETF の Best Current Practice の考え方をもとに、電子認証フレームワークの中で「経験上有効で目安となる使い方」をまとめたガイドラインの作成を推進していくことが求められている。

5.6. 今後の展望

電子認証フレームワークにおいてガイドラインを作成していくのに向けて、今後の展望を示す。

5.6.1. 関連機関との連携

日本 PKI フォーラムにおいて、調査で提案しているガイドラインと同様、レベル分けを含む内容をもった電子認証ポリシーガイドライン検討が進められている。電子認証の利用者の視点からは、日本 PKI フォーラムが証明書ポリシー（CP）、JPNIC が認証業務規程（CPS）をそれぞれ策定するイメージがあるとの意見もあり、これらが重複した作業になることを避けるためにも両者の知見を交え、それぞれの立場からベストプラクティスを提示、共有していくことが考えられる。

5.6.2. ガイドラインの構築に向けた取組み

実際にガイドラインを作成するのに際しては、以下のような取組みが考えられる。

（1）　ベストプラクティスの集成

これまでに実施されている電子認証サービスの構築・運用事例のうち、優れた効果を示しているものや利用者・運用者の評価が高いものについて、実施者の協力を得てその構築・運用時に用いたドキュメントやノウハウの収集、整理を行う。

（2） 保証レベル区分の導入の影響に関する調査

今回策定するガイドラインの主たる特徴となる保証レベルについて、導入した場合の影響や事前に考慮しておくべき対策について調査を行うことが望ましい。

（3） 策定プロセスの実施

以上(1)(2)の結果を踏まえ、策定プロセスに則ってガイドラインの検討が行われることになる。