

公的個人認証サービスの利活用のあり方に関する検討会(第7回) 議事概要

1 日時

平成19年12月11日(木) 10:00~12:00

2 場所

三田共用会議所 大会議室

3 出席者

構成員

大山 永昭 東京工業大学像情報工学研究施設教授【座長】
多賀谷 一照 千葉大学法経学部教授【座長代理】
町田 昇 市川市情報システム部参事(井堀構成員代理)
小笠原 章 徳島県県民環境部地域振興局地域情報政策課長
亀田 繁 (財)日本情報処理開発協会 電子署名・認証センター長
竹内 雅彦 (財)自治体衛星通信機構 公的個人認証サービスセンター長
前川 徹 サイバー大学教授
村松 晃 日本認証サービス(株)代表取締役社長

オブザーバ

巻口 英司 内閣官房情報通信技術(IT)担当室参事官
山内 徹 内閣官房情報通信技術(IT)担当室参事官
中井川 禎彦 総務省行政管理局管理官(情報担当)
水野 紳志 総務省情報通信政策局情報流通振興課長
望月 明雄 総務省自治行政局市町村課住民台帳企画官
富澤 一郎 厚生労働省医政局研究開発振興課医療機器・情報室長
黒川 弘樹 厚生労働省政策統括官付社会保障カード推進室長

4 議事の概要

(1) 開会

○ 配布資料の確認

事務局より、配布資料について説明がなされた。

(2) 今後、公的個人認証サービスの利用が想定される取組み

今後、公的個人認証サービスの利用が想定される取組みとして、以下の3分野について、各担当者より資料1に沿って説明がなされた。

- ・ 社会保障カード(仮称) について
発表者 : 黒川 弘樹 厚生労働省政策統括官付社会保障カード推進室長
- ・ 電子私書箱(仮称)について
発表者 : 山内 徹 内閣官房情報通信技術(IT)担当室参事官
- ・ 次世代電子行政サービスについて
発表者 : 巻口 英司 内閣官房情報通信技術(IT)担当室参事官

【質疑応答・意見】

- まだ全然決まっていないことだが、この3つの分野を繋いで1つにしようとした場合、次世代電子行政サービスがバックオフィス部分、電子私書箱がフロント部分、社会保障カードがアクセスカードという想定も1つの形としては見えるかもしれない。

(3) オンライン認証の実現イメージ

オンライン認証の実現イメージについて、事務局より資料2に沿って説明がなされた。

【質疑応答・意見】

- P6の「検討会 論定整理(本年5月公表)より」の②のところで、公的個人認証サービスをトラストアンカーとすると、認証局は都道府県認証局に限定せずとも問題ないと思うが、今回の議論ではその点は外している理解か？
→ 公的個人認証サービスがトラストアンカーの役割を担い、民間の認証事業者の信認の原点として利用する場合も考えられるが、当面の議論としては、公的個人認証サービスにおける認証用途の電子証明書を地方公共団体において提供するとすれば、どうすべきかを議論したいと考える。公的個人認証サービスがオンライン認証を直接提供すべきか否かは、オンライン認証の利用シーンが具体化した段階での議論であると考え。
- 一般的なSSLクライアント認証ではなく、サービス専用のクライアント認証を行う場合、利用者のPCには専用の認証用クライアントソフトをインストールする必要がある。さらに、この動作環境にJRE等のソフトウェアを使用する場合には、クライアントソフト単位で利用可能なソフトウェアのバージョンが制限される問題や脆弱性対策の問題が存在する。
- SSLクライアント認証において、サーバ側(サービス提供者)から利用者側に通常送られるデータ(乱数等)の代わりに不正な契約書等を送信して、利

用者の知らないうちに署名させるようなことは、現時点では起こりえないが、技術的にはサーバのソフトを改造して行うことは可能。この問題に対して、SSLと類似のクライアントソフトを別途用意するのは非現実的であり、サーバ側の管理をしっかりとやることで解決できるのではないか。今回、想定しているサーバ側は行政やそれに準ずる公的機関であると思われるため、そのサーバ側の環境を審査し、認証することが必要だと考える。

- 本来、公開鍵証明書は公開しても問題ないことが前提である。問題があるとするれば、証明書の内容が署名検証以外の目的に使用されることである。今回、想定している署名検証者は行政側であるため、そのような問題は発生しないと考えるが、行政側であっても無制限に実施するやり方は法律違反になるので、それなりの法整備は必要と考える。
- 公的個人認証サービスでは署名検証の範囲が限定されるため、公的個人認証サービスにおける公開鍵証明書と一般的なPKIにおける公開鍵証明書とでは、考え方が異なると思われる。
- 公的個人認証サービスで署名検証の範囲が制限されている旨をP7には、記載しておいた方がよいと考える。

(4) 海外事例の紹介

海外事例の紹介について、事務局より資料3-1および資料3-2および参考資料に沿って説明がなされた。

【質疑応答・意見】

- 海外事例にあるような認証レベルの規定を国内で作るべきだという議論は日本ではまだ出ていないようだ。
- 1枚の電子証明書で署名、認証、暗号化などの用途に対応しているところもあれば、機能別に電子証明書を分けている国もあるが、各国における電子証明書(署名、認証、暗号化)の利用率や利用数は分かるか？
 - 現在、事務局ではその情報を持っていないため、調べておく旨発言
- デンマークでは、電子証明書が2つ存在している。1つは「クウォリファイド」という電子証明書で、日本の電子署名法で規定しているような厳しい基準を満たしたものであり、もう1つは「アドバンスト」という電子証明書で、資料3-2の事例におけるレベル4相当には耐えられないが、インターネットから簡単に取得、利用できるものである。当初、デンマークでは「クウォリファ

イド」のみを発行していたが、使いづらい等の理由から国民に浸透することなく、ほとんど発行されなかったが、「アドバンス」を発行して、ある程度の安心安全に利用できる環境を作ったところ、一般市民に多く使われるようになった。

- 韓国では、電子政府のサービス利用時の還付制度を設けていたり、民間のいくつかのオンラインサービスに電子証明書の利用を義務付けていることもあり、電子証明書が大変、普及している。秘密鍵は様々な媒体に格納することを許されているが、基本的に複数の認証手段を組み合わせているので、今のところ、盗難によるなりすまし等の大きな問題は発生していないようである。

(5) オンライン認証機能の取扱いに係る検討のポイント

オンライン認証機能の取扱いに係る検討のポイントについて、事務局より資料4に沿って説明がなされた。

【質疑応答・意見】

- 現在、電子証明書の発行は市町村窓口での対面処理で行っているが、発行の際には住民の方に一度、窓口にお越しいただく必要があるというような課題や、窓口運用時間の課題もある。ぜひ、住民サービス向上につながるようなかたちで議論を進めていただきたいと考える。

(6) 質疑応答、意見交換

- 社保卡や電子私書箱などにおいて、認証用途という新たな面での公的個人認証サービスの普及を考える上では、各面での検討状況を意識しながら速やかに対応していくことが求められている。
- 資料2のP7のフロー図では、1つのアプリケーション上のステータスが完結しておらず、特に情報参照時における本人確認の部分で誤解を与える部分がある。したがって、サービスを適用する側から見た整理を1度やっていただいた方がいいと考える。例えば、社会保障カードでよく話に出てくる話題として、年金記録やレセプト情報、資格情報の閲覧および確認といったサービスを想定例として考えてもよいのではないかと考える。
- 今日に関連省庁から、アプリケーション側で公的個人認証サービスとの連携について、どのような検討が進んでいるか説明していただいたが、事務

局としては、そちらの検討状況を見ながら、当検討会の今後の予定を決めていきたいと考えている。資料4で羅列した検討ポイントを提示しているが、残りの3回の検討会で、その全てのポイントを詳細に検討することは想定していない。

(7) 閉会

次回、第8回の検討会は2008年1月中を予定している旨、事務局より話がなされた。

以上