公的個人認証サービス普及拡大検討会
第２回　議事概要

１　日時：平成 21 年 6 月 2 日（火）9:30～12:00

２　場所：三田共用会議室　３階　大会議室

３　出席者（敬称略）

構成員

辻 井　重 男	中央大学研究開発機構教授【座長】
稲 垣　敏 弘	徳島県県民環境部地域振興総局地域情報政策課長
大 山　永 昭	東京工業大学像情報工学研究施設教授【座長代理】
小 松　文 子	独立行政法人情報処理推進機構セキュリティセンター 情報セキュリティ分析ラボラトリー長
近 藤　則 子	老テク研究会事務局長
佐々木　良一	東京電機大学未来科学部情報メディア学科教授
佐 藤　純 通	日本司法書士会連合会会長
須 藤　修	東京大学大学院情報学環教授
竹 内　雅 彦	財団法人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 IT 総合学部教授
牧 野　二 郎	弁護士
三 浦　満 雄	大阪府総務部 IT 推進課長

オブザーバー

新 井　孝 雄	総務省情報流通行政局情報流通振興課 情報セキュリティ対策室長
伊 藤　毅 志	内閣官房情報セキュリティセンター内閣参事官
川 路　暢 仁	厚生労働省政策統括官付 社会保障カード推進室室長補佐（代理出席）
栗 田　照 久	金融庁監督局総務課監督企画室長
黒 田　俊 久	経済産業省商務情報政策局情報セキュリティ政策室課長補佐
古 賀　明	国税庁長官官房企画課情報技術室長
橋 本　敏	行政管理局行政情報システム企画課情報システム企画官
吉 野　太 人	法務省民事局商事課民事局付
若 林　成 嘉	内閣官房 IT 担当室内閣参事官

民間事業者

鈴木	孝一	大和証券株式会社常務取締役
別所	直哉	ヤフー株式会社法務本部長兼 CCO
西山	晃	セコムトラストシステムズ株式会社 グループシステム部担当部長
浅野	敬	株式会社帝国データバンク営業推進部営業開発課課長補佐
高橋	章	日本電子認証株式会社システム開発部長

4　議事概要

4.1　開会

- 検討課題について事務局より資料 2 に基づき説明がなされた。

4.2　各民間事業者よりそれぞれ資料 4～8 に基づきプレゼンテーションがなされた。民間事業者のプレゼンテーションに対する主な質疑応答は以下のとおり。

- 大和証券のプレゼンテーション資料の P8 に、署名検証の証跡データを残すとの記載があるが、金融機関が OCSP や CRL からの結果を受領するだけでは不足なのか。
  →OCSP や CRL からの結果を社内で保持した場合、透明性に疑問がある。また、お客様本人が証跡確認をできるようにすることで透明性を確保する等、第三者機関が保持しているデータの方が中立性を保つことができる。

- セコムトラストシステムズのプレゼンテーション資料の P1 に電子証明書への記載内容を本人が選択できるようにする案が提案されているが、現行の電子証明書の基本 4 情報の開示の範囲を選択する方法と、最初から記載する情報を限った別の証明書を発行する方法があると考えるが、具体的にどういうイメージか。
  →証明書には氏名のみを記載し、他の情報は属性情報として、属性証明書を発行する方法、または証明書には ID のみ記載し、本人情報は認証局が保持して利用者の何らかの同意があればその際に署名検証者に開示する方法など、手段としては様々に考えられる。

- 現行の電子証明書を認証用に利用した場合、訴訟に発展するようなリスクはあるのか。
  →認証用に利用した場合でも、認証システム側で発行したランダムな値に署

名する形式をとる。したがって、悪意のあるサイトに接続してしまい例えば借用証書に署名するという事態も生じうる。

- 署名用途と認証用途の証明書の違いは、利用者にとって理解が困難であるが、分ける必要性はあるのか。
  →現行の公的個人認証の証明書はセキュリティレベルが高いが、それを認証用途に利用するとセキュリティレベルが落ちるため、署名用途の証明書と認証用途の証明書とは分けた方がよいのではないか。

- 署名と認証を別にした場合、利用者はそれらの使い分けが可能なのか。
  →１つの IC カードに 2 枚の電子証明書を格納した場合、サーバ側で一方の証明書を受け付けない等の仕組みを作れば自動で使い分けができるが、利用者側での制御は難しいのではないか。使い分けのための技術仕様を整理する必要がある。

4.3　各民間事業者のプレゼンテーションを踏まえ、検討課題について検討がなされた。主な意見等は以下のとおり。

- 国民電子私書箱構想等が議論されている中で、電子証明書が住所の異動があれば失効し、すぐに使用できなくなってしまうというのはまずいのではないか解決方策の１つとして、電子証明書の中で、氏名またはシリアル番号のみを証明することとし、住所が異動しても電子証明書を失効させないようにするという提案をしたい。

- 民間が署名検証者となる場合には、署名検証時点での住所証明までは必要ないのではないか。

- 記録媒体の拡張について、媒体へのアクセス手段の標準化も重要な検討事項である。限られたベンダしか利用できないクローズな定義では、マーケットが縮小するのではないか。

- 認証にも厳密さや強さが求められ、証跡管理が必要となる場面があるのではないか。事故があったときのトレーサビリティを確保するため、証跡管理が必要となるのではないか。

- 署名検証者の民間開放を行う際には、公的個人認証サービスに要するコスト

の一部負担についても検討すべきではないか。

- オンライン更新が実現できた場合には、鍵ペア生成装置を市町村の窓口に設置する必要がなくなるのではないか。また、民間認定認証事業者に電子証明書の発行を委託しても問題が無いのではないか。

- 基本 4 情報は本人の申請により開示されるべき情報であり、無制限な公開情報ではない。電子証明書の基本 4 情報は、行政機関のみが利用することを想定していたと考えられるから、署名検証者を民間まで開放する場合には留意が必要ではないか。

4.4　閉会

- 次回は 6 月 30 日を予定している旨、事務局より説明がなされた。

以上