公的個人認証サービスにおける暗号方式等の移行に関する検討会
第１回　議事概要

1　日時：平成 20 年 9 月 16 日（火）14:00～16:00

2　場所：全国町村議員会館 2 階会議室

3　出席者

構成員

辻 井　重 男	情報セキュリティ大学院大学学長【座長】
大 山　永 昭	東京工業大学像情報工学研究施設教授
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	財団法人日本情報処理開発協会電子署名・認証センター長
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
鈴　木　　豊	東京都総務局行政部副参事（振興調整担当）
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
山 戸　康 弘	大分県企画振興部 IT 推進課長

オブザーバー

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
大 嶋　裕 一	国税庁長官官房企画課情報技術室情報技術係長（代理）
岡 本　好 史	総務省行政管理局行政情報システム企画課 情報システム管理室長
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（代理）
杉 浦　直 紀	法務省民事局商事課補佐官（代理）
中 村　高 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 課長補佐（代理）
望 月　明 雄	総務省自治行政局市町村課企画官（代理）

4　議事概要

4.1　開会

- 井上知義地域情報政策室長より挨拶がなされた。
- 事務局より構成員の紹介があり、各構成員より挨拶がなされた。
- 事務局より本検討会の運営について説明がなされた。
- 辻井座長より挨拶がなされた。

4.2　公的個人認証サービスにおける暗号方式等の移行に関する検討会の開催について、事務局より資料 2 に基づき説明がなされた。

4.3　SHA-1 及び RSA1024 の安全性評価について、総務省情報通信国際戦略局通信規格課標準化推進官荻原様及び独立行政法人情報通信研究機構情報通信セキュリティ研究センターセキュリティ基盤グループ黒川様より資料 3 に基づき説明があり、検討がなされた。この説明に関する主な意見等は以下のとおり。

- 暗号の移行に関して、あまり議論されていない論点が 2 点ある。1 点目は、既存の署名付き文書について有効性の確認が将来できなくなる運用になっていることである。2 点目は、セキュリティホールを作らないためにどのように暗号方式等を移行するのかという運用の問題である。

- 1 点目の論点については、暗号方式等の移行に当たっての留意事項として（本検討会）第 3 回会合で検討したいと考えている。なお、本検討会の報告書としては、この論点について問題提起に止めることも考えられる。（事務局）

- ISO15408（コモンクライテリア）、ISMS 及び ISO19791 があるものの、運用（2 点目の論点）については公式に実質的な検討を行う必要がある。

- 暗号の移行については説明が難しい。現在利用している暗号はかなり安全だが、かといって暗号を移行しないのは困る。一方、現在利用している暗号が安全ではないから暗号を移行すると説明すると、いかにも現在の暗号で事故が起こるような、事故前提社会という言葉が出てくる。

- SHA-1 について、衝突発見に要する時間の目安が約 7 年以下とは、当時（2006 年 4 月現在）の国内最高速のスパコンで衝突発見に約 7 年かかると見積もったということ。スパコンの性能は向上しているため、例えば 2010 年のスパコンだと衝突発見に 7 年はかからない。

4.4　まず政府機関における暗号の安全性低下への対応について内閣官房情報セキュリティセンター内閣参事官伊藤様より資料 4 及び資料 5 に基づき説明があり、次に「電子署名及び認証業務に関する法律」に関する暗号アルゴリズムの移行について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黒田様より資料 6 に基づき説明があり、最後に住民基本台帳カードの対応について総務省自治行政局市町村課企画官望月様より資料 7 に基づき説明があり、検討がなされた。これらの説明に関する主な意見等は以下のとおり。

- 電子政府推奨暗号リスト（平成 15 年 2 月 20 日）は、10 年程度は安心して使える暗号のリストとして公表したもの。

- 電子署名は安全性及び信頼性が担保されていないと使ってもらえないため、暗号の危殆化に当然対応していかなければならないと思っているが、経済的な問題もあり、次の暗号方式等の検討に当たっては、暗号の移行が公的個人認証サービスを運営している都道府県及び市町村にとって大きな財政負担になることも考慮していただきたい。

- 暗号の危殆化のパターンがいくつかある。計算機がどんどん速くなることによる危殆化については RSA2048 が 20 年や 30 年は大丈夫だと言えるが、新しい攻撃方法が出てくることによる危殆化については何とも言えない。ただし、新しい攻撃方法が出てくることによる危殆化についても 10 年程度は大丈夫だろうから、10 年ごとに見直すというのが現状である。

- コストの問題は大きな問題であるが、技術レベル、システムの運用レベル及びマシンのサイクルを総合的に判断すると、CRYPTREC が想定した 10 年は常識的な期間であると考える。

- 暗号移行の容易なソフトフェアがあったほうがいいという考え方もある。一方で、ソフトフェアは複雑にすればするほど、ダウンしやすく、セキュリティホールができて攻撃されやすいという問題がある。

- 内閣官房情報セキュリティセンターでまとめて予算要求をして、暗号の移行に当たって各省庁及び地方公共団体が利用できるパッケージをつくっていただけないか。

- 内閣官房で移行指針をまとめ、各情報システムを所管している省庁でそれぞれこの指針に従って予算を要求し対応していただこうと考えている。

- 暗号の移行は初めて経験することである。既存の署名付き文書について有効性の確認が将来できなくなる運用になっていること等についても1個1個解決していかなければいけない問題だと認識している。いろいろな方のご知見をいただきながら、スムーズな暗号移行の第1例としたい。

- 住基カードの発行手数料の無料化と住基カードの更改について、整合性をとっていただけないか。

- 利用が伸びている e-Tax の電子申告については、現在の住基カードの機能で十分であるから、現在の段階で住基カードの発行手数料を無料化して、e-Tax の電子申告に住基カードを利用していただくことは問題ないと考えている。

- 現在の住基カードは最大 RSA1024 までの対応となっており、新しい住基カードで RSA2048 に対応することを検討している。製品開発、評価等が相当順調に進んだ場合、新しい住基カードは 2012 年に発行できるだろう。なお、新しい住基カードの新規発行に当たっては、それまでに発行した住基カードの有効期間が 10 年であることに留意する必要がある。

4.5　閉会

- 次回は 10 月中下旬を予定している旨、事務局より説明がなされた。

以上