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３回　議事概要

1　日時：平成 20 年 12 月 18 日（木）10:00～12:00

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】
井 堀　幹 夫	市川市 CIO 情報政策監
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

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
梶　原　　亮	総務省情報通信国際戦略局通信規格課標準推進係長（代理）
小 高　久 義	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課長補佐（代理）
正 野　直 子	総務省自治行政局市町村課（代理）
畠 山　啓 以	国税庁長官官房企画課情報技術室システム研究官（代理）
花 田　高 広	経済産業省商務情報政策局情報セキュリティ政策室係長（代理）
山 西　浩 仁	法務省民事局商事課電子認証係長（代理）

4　議事概要

4.1　開会

4.2　検討会報告書案について、事務局（総務省自治行政局地域政策課地域情報政策室小野）より資料 1 及び資料 2 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。

- 住基ネット全体の機器更改等と合わせて新しい住基カードの開発を検討しており、2012 年度の当初（一部の市町村においては 2011 年度末）ぐらいから新しい住基カードを交付することができると考えている。

- 現在、市町村窓口の鍵ペア生成装置は日立製と富士通製である。2 社が 2010 年度以降は現在の鍵ペア生成装置を保守できないと話しているため、2010 年度には鍵ペア生成装置を更改する必要がある。

- 新旧暗号アルゴリズムの併用期間（2014 年度早期から 2017 年度早期まで）の運用費用がなるべく小さくなるよう今後検討したい。（事務局）

- 公的個人認証サービスにおける暗号アルゴリズムの移行スケジュールについては、次世代電子行政サービスの引越ワンストップ、電子私書箱及び社会保障カードのスケジュールを踏まえぜひ調整していただきたい。

- 「電子署名に関する現在の運用においては、電子署名に利用する暗号アルゴリズムの移行に伴い、SHA-1 及び RSA1024 による電子署名の検証が将来できなくなるため」（資料 2（20 頁））とあるが、将来にわたり電子署名を検証できる制度的な保証は現在もないのではないか。

- 本検討会は本日（第 3 回会合）で閉会し、「今後の検討事項」については都道府県、LASCOM 及び総務省で検討していきたいと考えている。（事務局）

- 社会保障カード、電子私書箱等の将来的な構想もあり、現時点では不確定要素が多いため、今後、検討していただいた移行スケジュールを基本として合理的な判断をしていく必要がある。（事務局）

- 公的個人認証サービスの利用者のパソコンも新しい暗号アルゴリズムに対応する必要があり、利用者の環境についても注視すると良いのではないか。

- 事務局より報告書案に関する意見を募集する旨の提案があり、了承された。

4.3　まず暗号移行のための残された検討課題について東京電機大学教授佐々木様より資料 3 に基づき説明があり、次に公的個人認証サービスに関するリスク整理について NTT コミュニケーションズ株式会社佐藤様より資料 4 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。

- 急激な危殆化が起こった場合の対応について、移行指針においてコンティンジェンシープランを作成する旨記載しており、検討を始めている。

- SHA-1 に関して、第二原像攻撃は「なりすまし攻撃」と言い、衝突計算攻撃は「たまたま一致攻撃」と言えば良いのではないか。

- 衝突計算攻撃については、問題の大きさを過大に評価しているのではないか。

- 長期署名については、最終的に標準化及び法制化を考える必要があり、組織的に研究することが望ましい。

- フランスの事例（資料 4（3 頁））については、IC カードの安全性の問題ではなく、RSA（300 ビット程度）の問題だったことを確認していただきたい。

- 日本の公証と欧米のノータリーは意味が違う。長期署名については欧米のノータリーと同様に整理し、署名検証した状態を第三者が保証する仕掛けをつくる必要があるのではないか。

- 長期署名について、電子文書の内容を保証する、電子文書の改ざんを検知する仕組みをつくることは可能である。

- 楕円曲線暗号については、なかなか普及しなかったものの、RSA2048 に対して 210 ビット程度で足り、指数関数時間の攻撃法しか判明していない。このため、仮に RSA3072 の利用を検討するのであれば、RSA3072 ではなく楕円曲線暗号を利用すると良いのではないか。

- 「② アメリカでは政府システムにおいて 2010 年に RSA1024 および SHA-1 の運用が終了する」（資料 4（2 頁））とあるが、検証を含めて全て終了することを意味しているのか確認していただきたい。

- 日本の予算制度の中で、2010 年に全ての政府機関の情報システムを更新することはできない。現在、政府機関の情報システムについては 2014 年から新たな暗号アルゴリズムに切り替えたいと考えている。

- 電子文書そのものを無くしてしまう場合、電子文書を正しく保存することについて電子署名の力は及ばないため、利害関係のない者に電子文書を渡す方法が一番良い。今後、医療分野において健康情報等の長期利用が予測される。

- 法的問題に備え証拠を保全及び開示できるよう、技術、法制度、管理及び運営を含め総合的に体制を整備することがデジタルフォレンジックである。

- データの証拠性の問題が大事である。データの証拠性については、デジタルフォレンジックの分野であり、電子署名を上手に使う、ハードウェアで解決する、又は相互チェックの仕組みをつくる方法がある。

4.4　閉会

- 本検討会を閉会する旨、事務局より説明がなされた。
- 総務省自治行政局地域政策課地域情報政策室長井上より挨拶がなされた。
- 辻井座長より挨拶がなされた。

以上