# 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 2 回　議事概要

1　日時：平成 20 年 10 月 27 日（月）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】 |
| 大 山　永 昭 | 東京工業大学像情報工学研究施設教授 |
| 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 |
| 船 田　美 幸 | 徳島県県民環境部地域振興局地域情報政策課課長補佐（代理） |
| 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 |
| 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<br>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） |
| 平 野　友 貴 | 総務省情報流通行政局情報流通振興課<br>情報セキュリティ対策室調整係長（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　まず政府認証基盤（GPKI）における暗号方式等の移行について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小高様より資料 2 に基づき説明があり、次に公的個人認証サービスにおけるシステム更改の状況と暗号アルゴリズムの移行に係る影響について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竹内様より資料 3 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。

- 今後、公的個人認証サービス制度に関して、電子証明書の有効期間の延長、オンライン更新、格納媒体の拡大及びオンライン認証について検討したいと考えている。このため、暗号アルゴリズムの移行スケジュールの検討に当たっては、柔軟性のある移行スケジュールを検討する必要がある。（事務局）

- 電子署名法では署名の長期化について制度的な対応は明示されていない。なお、電子署名法では本人の真偽確認が特定認証業務の認定を受けている場合に義務付けられている。電子的な利用申請を受け付けている認定認証業務においては、電子的に提出された利用申請書にタイムスタンプを付与するとともに、署名検証及び内容確認したという記録に認証局の担当者の電子証明書を用いて電子署名を行い、その電子文書を長期保管している。

- GPKI は平成 20 年 1 月に機器を更改し、当該更改においては 48 ヵ月で機器を調達しているため、次の更改は平成 24 年 1 月に予定されている。

- 政府機関では 2013 年度までに各情報システムの対応を完了することとしており、X-day は 2014 年度以降になるだろう。SHA-1 等の急速な安全性低下の対応策は別途考える予定であるが、X-day を前倒しすることは考えていない。

- Y-day については NISC で検討しており、今年度中に結論を出したいと思っている。X-day と Y-day の間は短くする方向で検討したいと考えている。

4.3　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 4 及び資料 5 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。

- 例えば RSA1024 を RSA2048 に変更すること自体については、プログラムの改変に要する費用は比較的少ないだろう。システム全体の動作検証を含めた費用については何とも言えない。

- 予め SHA-2 及び RSA2048 を用意し選択できるようにしておくことも可能である。セキュリティホールを作らないようにすることが重要だが、大きな

問題ではないだろう。

- SHA-1 及び RSA1024 のみを利用する前提でアプリケーションが作成されている場合、全面的な改修が必要になる。一方、利用する暗号アルゴリズム（SHA-1、SHA-2 等）を指定できる仕様でアプリケーションが作成されている場合、比較的有利である。

- リスク対応の常道として、どういう情報資産を守るのか、どういう脅威があるのか、その確率はどのくらいか、そして緊急対応にいくらお金がかかるのかまで考えないといけない。アプリケーションの実態については専門家が集まって検討しないといけないだろう。

- 電子政府推奨暗号リストは 10 年毎に再検討することになっており、今後リストに新たな暗号アルゴリズムが追加されることも十分あるものの、それによって SHA-1 及び RSA1024 に代わる暗号アルゴリズムとして SHA-256 及び RSA2048 を採用することが変わることはないだろう。

- 平成 22 年度には市町村の鍵ペア生成装置を更新する必要がある。新しい鍵ペア生成装置の耐用年数の途中で暗号アルゴリズムが切り替わるため、新旧両方の暗号アルゴリズムに対応した鍵ペア生成装置を検討する必要がある。

- 新しいバージョンの住基カードについては、今年度暗号アルゴリズムを決め、その後、製品開発、ISO の評価及び動作確認を行う。製品開発、ISO の評価及び動作確認に 2 年近く時間を要するため、製品化を平成 24 年度より早くすることはかなり難しい。

- 住基カードのメーカーと鍵ペア生成装置のメーカーが相談し、前もってテストできるよう調整するのではないか。

4.4　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 6 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。

- 現在、次期公的個人認証サービスシステムの仕様を作成している。今回の更新は提案型で調達することを予定しており、仕様に暗号アルゴリズムの移行を明記して、提案者からいい提案を受けたいと考えている。

- 本検討会の報告書については都道府県及び市町村に情報提供する予定である。（事務局）

- 今後、有効期間の延長、オンライン更新、格納媒体の拡大、オンライン認証等の検討課題が出てくるだろう。都道府県の費用負担の問題は避けられないものの、公的個人認証サービスの利便性向上及びセキュリティ確保の要請にも応える必要があるため、公的個人認証サービスシステムの更改にあたっては、上記の検討課題に対応できる仕様を目指していただきたい。（事務局）

- A 案及び B 案では、暗号アルゴリズムの移行に、住基カードを再発行する費用を伴うことになるのではないか。

- 安全面及び様々な要因を考慮して Y-day を検討する場が必要ではないか。

- NISC は、CRYPTREC の評価を踏まえて、いかなる情報資産に対していかなる脅威があるのか、その確率はどのくらいか、エマージェンシーレスポンスにどのくらい手間とお金がかかるのかを総合的に判断して、Y-day を決めるといいのではないか。

- 暗号アルゴリズムの危殆化の影響を直接受けないよう、制度的な裏付けも含めてシステム全体の配置を検討する必要がある。

- 現在、第 2 次情報セキュリティ基本計画の検討に当たって、暗号アルゴリズムの危殆化等のリスクをどのように許容する社会をつくる必要があるのか考えている。

- A 案は電子証明書を有効期限前に失効させてしまうこととなり混乱が大きく、C 案は X と Y の期間が長すぎて難しいだろう。結果的に B 案が最も妥当ではないか。

- 相互認証の更新時期については、各省会議に方針を諮った後、民間認証局にも意見を聞きたいと考えている。

4.5　閉会

- 次回は 12 月中旬を予定している旨、事務局より説明がなされた。

以上