

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

開催要領

1. 目的

公的個人認証サービスにおいて利用されているハッシュ関数 SHA-1 及び公開鍵暗号方式 RSA1024 の安全性に懸念が生じる可能性が指摘され、国際的にも新たな暗号方式等への移行が進んでいることから、公的個人認証サービスの信頼性を引き続き確保するため、暗号方式等の移行について学識経験者・関係機関等による検討を行う。

2. 検討事項

- 公的個人認証サービスにおける暗号方式等の移行方針について

3. 構成及び運営

- 検討会の構成は別紙のとおりとする。
- 検討会には座長 1 名を置く。
- 会議資料及び議事要旨は、総務省ホームページに掲載することにより公表する。

4. 開催期間

平成 20 年 9 月から平成 20 年 12 月まで計 3 回の開催を予定。

5. 事務局

総務省自治行政局地域政策課地域情報政策室が検討会の庶務を担当する。

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

構成員・オブザーバー名簿

構成員

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
辻井重男	情報セキュリティ大学院大学学長 【座長】
山戸康弘	大分県企画振興部IT推進課長

オブザーバー

相澤哲	法務省民事局商事課長
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
江畑賢治	総務省自治行政局市町村課長
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
古賀明	国税庁長官官房企画課情報技術室長
田中宏	総務省情報通信国際戦略局通信規格課長
三角育生	経済産業省商務情報政策局情報セキュリティ政策室長

(敬称略・五十音順)