報道資料

実はここにも 総務省

MIC Ministry of Internal Affairs and Communications

平成 21 年 1 月 26 日

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 報告書の公表

近年、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 について、暗号技術検討会等において安全性の低下により将来問題が生じる可能性が指摘されています。

このため、総務省では、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を平成 20 年 9 月 16 日から同年 12 月 18 日まで計 3 回開催し、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の必要性及び移行案、今後の検討事項等について検討を行いました。

この度、本検討会において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が取りまとめられましたので、公表します。なお、本報告書案について、平成 20 年 12 月 23 日から平成 21 年 1 月 6 日までの間、国民の皆様から広く意見を募集したところ、意見の提出はありませんでした。

公表資料

- 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
- 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の概要

参考資料

※ 本報告書案に関する意見の募集（報道資料）

※ 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について

※ 公的個人認証サービスポータルサイト

連絡先
総務省自治行政局地域情報政策室
担当：中垣内補佐、小野事務官
電話：03-5253-5586
FAX：03-5253-5529