# 電子署名法に基づく認定認証業務で用いる暗号アルゴリズムの移行について
## （平成２３年度電子署名法研究会報告 別紙）

平成２４年２月２２日
電子署名法研究会※

## １．背景

電子署名等のために広く使用されている暗号アルゴリズム SHA-1 及び RSA1024 については、暗号技術検討会や平成１９年度の電子署名及び認証業務に関する法律の施行状況に係る検討会（以下、「附則第３条検討会」という。）等において安全性が低下しているとの指摘がある。これに関連し、情報セキュリティ政策会議は「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」を平成２０年４月に決定し、関係府省は使用する当該暗号アルゴリズムについて、より安全な暗号アルゴリズムに移行することとしている。

## ２．移行スケジュール

電子署名及び認証業務に関する法律（平成１２年法律第１０２号）に基づき、国の認定を受けた特定認証業務を行う者（以下「認定認証事業者」という。）が発行する電子証明書は、政府機関の情報システムにおける電子申請、電子入札等に広く用いられており、これら政府系情報システムと、認定認証事業者における暗号アルゴリズムの移行に関しては、協調して実施される必要がある。

当研究会は、認定認証事業者の暗号アルゴリズムの移行に関し、移行指針、附則第３条検討会の検討結果、認定認証事業者等の関係機関の移行スケジュールに関し調査した結果等を踏まえ、以下のとおり確認する。

### （１）移行時期

認定認証事業者は、平成２６年度早期までに、より安全な暗号アルゴリズムによる電子証明書を発行することが必要である。また、本件に関する変更認定のための指定調査機関の調査については、一時期に集中することのないよう、平準化を図る必要がある。

### （２）関係機関との連携

認定認証事業者の暗号移行については、平成２２年度の電子署名法における暗号アルゴリズム移行研究会の検討内容を踏まえ、関係機関が連携し、滞りなく移行関連作業を進めることが必要である。

※「電子署名法研究会」は、経済産業省委託事業「平成２３年度企業・個人の情報セキュリティ対策促進事業（電子署名・認証業務利用促進事業（暗号アルゴリズムの移行等に関する調査研究））」に基づき、設置された研究会である。