政府機関の暗号アルゴリズムに係る移行指針の改定概要

資料 3-1

1　経緯

①電子政府システム（入札・申請等）において電子署名等のために広く使用されているSHA-1及びRSA1024と呼ばれる暗号方式の安全性の低下が指摘

②より安全な暗号方式（SHA-256及びRSA2048）への移行が必要であることから、「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」を策定

（H20年4月22日　情報セキュリティ政策会議決定）

2　政府機関における移行に向けた準備スケジュール

- 各府省庁が保有する情報システムの新たな暗号方式への対応時期　⇒「2013年度末まで」
- 新たな暗号方式による電子証明書の発行開始可能時期　⇒「2014年度早期」
- 従来の暗号方式による電子証明書の検証（有効性の確認）終了可能時期　⇒「2015年度早期」

（H21年2月3日　情報セキュリティ政策会議決定）

3　移行指針の改定概要

- 切替時期について各認証基盤との調整結果を踏まえ、以下のとおり改定

  政府認証基盤及び電子認証登記所が発行する電子証明書については、

  a.「2014年9月下旬以降、早期に」新たな暗号方式に切替

  b.「2015年度末までに」従来の暗号方式によって発行された証明書の検証を終了

  ただし、発行済み電子証明書の有効期間が残存し、やむを得ない場合は、「2019年度末まで」検証可

（参考）政府機関における暗号移行スケジュール