「政府機関の情報システムにおいて使用している暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」に基づく検討状況について

～SHA-1及びRSA1024の切替えに係る検討状況について～

2009年2月3日

内閣官房情報セキュリティセンター（NISC）

資料5－2

移行スケジュールの検討状況

経　　緯

第17回情報セキュリティ政策会議（H20.4.22）

電子政府システムにおいて、電子署名等のために広く使用しているSHA-1及びRSA1024と呼ばれる暗号方式の安全性の低下が指摘されていることを受け、より安全な暗号方式への移行するため、「政府機関の情報システムに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」を決定。

○ 移行に当たっては、相互運用性の確保等のため、政府機関以外の関係機関との調整が必須であることから、当該移行指針においては、「新たな暗号アルゴリズムへの切替時期並びにSHA-1及びRSA1024の使用停止時期について、2008年度中に検討する」こととされている。
○ 今回、政府機関の検討状況等について、経過報告をするもの。

政府機関における検討状況

- 昨年、各府省庁の情報システム及び申請手続の状況を調査。
- 認証基盤全体の切り替え時期を調整するに当たり、まず、政府機関において対応可能な時期を検討することとし、その方針の概要は以下の通り。
  - 新たな暗号アルゴリズムによる電子証明書の発行開始可能時期は、「2014年度早期」とする。（※1）
  - 従来の暗号アルゴリズムによる電子証明書の検証終了可能時期は、「2015年度早期」とする。（※2）
  - GPKI及び商業登記認証局の切替時期については、他の関係機関を踏まえた認証基盤全体としての切替時期に合わせることとする。ただし、上記時期にも対応可能とするため、必要となる対応をあらかじめ検討しておくこととする。

※1：政府機関の情報システムの対応が終了する2013年度末から一定の事務作業時間がかかることを考慮したもの。
※2：政府機関が電子署名を付した文書を発行後、最長1年間、当該電子文書の検証が必要である手続きが存在することを考慮したもの。

参考：移行スケジュールの検討状況（関係機関等）

電子署名法関係における検討状況（総務省・法務省・経済産業省）

- 昨年度、電子署名法の施行状況に係る検討会を開催（H19.12～20.3）し、暗号アルゴリズムの移行を含めた検討を行い、結果を報告書として公表。
- 概要は以下の通り。
  - 以下のスケジュール案を基本として、制度改正作業等を進めていくことが適当。
    - 2008年度に特定認証業務に係る電子署名の基準にSHA-2を追加。
    - 2014年度早期までに、認定認証事業者は、SHA-2及びRSA2048bitによる電子署名に係る特定認証業務を開始。
    - 2014年度末前後を目途として、特定認証業務に係る電子署名の基準から、SHA-1、RSA1024bitを削除。

公的個人認証サービス（JPKI）関係における検討状況（総務省）

- 昨年、暗号の移行に関する検討会を開催（H20.9～12）し、結果を報告書として公表。
- 概要は以下の通り。
  - 現段階では、以下のスケジュールを基本として、暗号アルゴリズムの移行を進めていくことが適当。
    - 2014年度早期に、SHA-256及びRSA2048による電子証明書の発行を開始するとともに、SHA-1及びRSA1024による電子証明書の発行を停止する。
    - SHA-1及びRSA1024による電子証明書の有効期間後（2017年度早期（※3））に、SHA-1及びRSA1024による電子署名に係る地方公共団体の認証業務を停止する。

その他

- 地方公共団体組織認証基盤（LGPKI）については、政府機関、公的個人認証サービスにおける検討状況などを参考に、現在、対応を検討中。
- 政府機関及び各関係機関とも、急激な安全性の低下に備えて、あらかじめ緊急避難的な対応（コンテンジェンシープラン）を検討することとしている。

※3：電子証明書の有効期間（現在3年）が5年に延長された場合には2019年度早期（電子証明書の有効期間に係る検討は、2009年度に検討する予定）。

参考：移行指針に基づく暗号方式の移行スケジュールの検討状況の概要