

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

1 はじめに

近年、政府機関の情報システムにおいて使用されている一部の暗号アルゴリズム（ハッシュ関数¹SHA-1²（以下「SHA-1」という。）及び公開鍵暗号方式³RSA 1024⁴（以下「RSA1024」という。))の安全性低下が指摘されている。一般的に、暗号アルゴリズムは、電子計算機の能力の向上などにより、安全性が時間の経過とともに低下するものであるが、暗号技術検討会⁵などにおいては、それら暗号アルゴリズムの安全性の低下により、近い将来に現実的な問題が生じる可能性について指摘しているところである。

SHA-1 及び RSA1024 は、電子申請、電子入札等を行うための政府機関の情報システムにおいて、その安全性及び信頼性を確保するための技術の一要素として広く使用されている暗号アルゴリズムである。政府機関の情報システムの安全性及び信頼性を確保するためには、これらの暗号アルゴリズムについて、情報システムのライフサイクル等を踏まえつつ、適時により安全なものに移行する必要がある。その際、関係する情報システム間における相互運用性を確保する観点や政府機関全体の情報セキュリティ向上の観点から、政府統一的な対応が必要である。

そこで、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 について、より安全な暗号アルゴリズムに移行するための指針を、以下のとおりとりまとめることとした。

2 対象機関

内閣官房、内閣法制局、人事院、内閣府、宮内庁、公正取引委員会、国家公安委員会（警察庁）、金融庁、総務省、法務省、外務省、財務省、文部科学省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省及び防衛省とする。

¹ 与えられたデータから固定ビット長の値を生成する関数。本指針では、一方方向性（当該関数の演算の非可逆性）及び衝突困難性（同一の数値を生成する異なるデータの発見困難性）の両性質を持つものとする。

² ハッシュ関数 SHA の一つ。与えられたデータから 160 ビットの値を生成する。

³ 関連した 2 つの鍵（公開鍵と秘密鍵）を使用する暗号方式であり、一方の鍵（公開鍵又は秘密鍵）で暗号化したデータは他方の鍵（秘密鍵又は公開鍵）でのみ復号できるようになっている。2 つの鍵は、公開鍵が与えられても、秘密鍵を導き出すことが計算上困難な特性を持っている。

⁴ 公開鍵暗号方式の一つで、暗号アルゴリズムを RSA、鍵の長さを 1024 ビットとしたもの。

⁵ 総務省大臣官房技術総括審議官及び経済産業省商務情報政策局長の私的研究会として毎年度開催。

3 内容

(1) 情報システムの設計要件

情報システムにおける暗号アルゴリズムの用途を踏まえつつ、それぞれの情報システムにおいて、以下のように設計を行う。

ア 政府認証基盤（GPKI）⁶及び商業登記認証局⁷

- (ア) 電子証明書⁸の発行に使用する暗号アルゴリズムを複数の中から選択可能とする構成とし、使用する暗号アルゴリズムを特定の時期に切替可能とする。
- (イ) 電子証明書の検証に使用する暗号アルゴリズムを複数の中から選択可能とする構成とし、それぞれの暗号アルゴリズムごとに、検証を行う期間の開始及び終了時期を設定可能とする。
- (ウ) (ア)及び(イ)においては、以下の暗号アルゴリズムを含める。
 - a.電子証明書の発行及び検証に使用する暗号アルゴリズムについては、ハッシュ関数 SHA-1 及び公開鍵暗号方式 RSA2048⁹（以下「RSA2048」という。）の組合せ並びにハッシュ関数 SHA-256¹⁰（以下「SHA-256」という。）及びRSA2048の組合せ。
 - b.電子証明書の発行対象者¹¹の鍵ペア¹²に使用される暗号アルゴリズムについては、RSA1024 及びRSA2048。

イ 政府認証基盤に依存する情報システム

- (ア) 文書ファイルへの電子署名及びその検証に使用する暗号アルゴリズムを複数の中から選択可能とする構成とし、暗号アルゴリズムごとに電子署名及び検証を行う期間の開始及び終了時期を設定可能とする。
- (イ) (ア)においては、以下の暗号アルゴリズムを含める。
 - a.ハッシュ関数については、SHA-1 及びSHA-256。
 - b.公開鍵暗号方式については、RSA1024 及びRSA2048。

ウ ア及びイ以外の情報システム

- (ア) SHA-1 又は RSA1024 に対して現実的な脅威となる攻撃手法が示さ

⁶ Government Public Key Infrastructure：国民等と行政機関との間でやり取りされる文書ファイルについて、内容が改ざんされていないことや、その文書ファイルが真にその名義人によって作成されたかを確認できるようにするための仕組み。

⁷ 商業登記に基づく電子認証制度に係る電子証明書を発行する認証局。

⁸ 認証局により発行された電子署名の検証用公開鍵が真正であることを証明するデータ。

⁹ 公開鍵暗号方式の一つで、暗号アルゴリズムをRSA、鍵の長さを2048ビットとしたもの。

¹⁰ ハッシュ関数SHAの一つ。与えられたデータから256ビットの値を生成する。

¹¹ 電子証明書を利用する実体（個人、組織等）をいう。いわゆる「エンドエンティティ」。

¹² 公開鍵暗号方式で使用する「秘密鍵」と「公開鍵」の対となる2つの鍵のこと。

れた時点で、速やかに別の暗号アルゴリズムに変更する等の対応措置を可能とする。

(例)

- ・ 暗号モジュール¹³を、交換できるようにコンポーネント化して構成する。
 - ・ 複数の暗号アルゴリズムを選択可能とする。
- (イ) 複数の暗号アルゴリズムを導入する場合は、以下のものを含める。
- a. ハッシュ関数に SHA-1 以外を導入する場合には、SHA-256 相当以上の暗号強度を持つもの
 - b. 公開鍵暗号方式に RSA1024 以外を導入する場合には、RSA1152¹⁴相当以上の暗号強度を持つもの。
- (ウ) SHA-1 及び RSA1024 以外の暗号アルゴリズムを導入した後は、新たなアルゴリズムで電子署名を行うこととし、検証等暗号アルゴリズムの移行が完了するまでの間に必要となる場合においてのみ SHA-1 及び RSA1024 を使用することが可能な構造とする。

エ その他

新たな暗号アルゴリズムへの移行が完了する以前に、SHA-1 又は RSA1024 の安全性の低下による影響が発生する状況（発生が予測された場合を含む。以下同じ。）に備え、緊急避難的に、電子証明書の失効、再発行等を積極的に活用し、情報システムが提供する業務が継続して運用できる構造とする。

(2) 計画等の策定

- ア 各府省庁は、(1)に定める暗号アルゴリズムの安全性向上に必要な対応について、情報システム全体の更改前の部分的な実施も検討した上で、情報システムごとの移行時期を踏まえ、必要となる対応を 2008 年度中にとりまとめる。
- イ 既に発行済みの電子署名付き文書ファイル及び電子証明書について、暗号アルゴリズムの移行に伴い、失効、再発行等の対応が必要となる場合に備え、それぞれの手続きごとに、当該対応に係る手順書の整備等必要な措置を講ずる。
- ウ 新たな暗号アルゴリズムへの移行が完了する以前に、SHA-1 又は RSA1024 の安全性の低下による影響が発生する状況に備え、情報システムの停止等に伴う国民への影響を最小限とするために必要な措置を

¹³ ハードウェア、ファームウェア及びソフトウェアにおいて、暗号化、復号、電子署名等の暗号化機能を実装した構成要素のこと。

¹⁴ 公開鍵暗号方式の一つで、暗号アルゴリズムを RSA、鍵の長さは 1152 ビットとしたもの。

講ずる。

(3) スケジュール

ア 各府省庁は、(2)アにおいて取りまとめた内容の概要について、2008年度中に内閣官房に報告する。

イ 内閣官房、総務省、法務省、経済産業省及び関係府省庁は、アの報告等を基に、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。

ウ 内閣官房、総務省及び関係府省庁は、政府認証基盤と他の認証局との相互接続に必要となる技術要件及び新たな暗号アルゴリズムへの移行が完了する以前に安全性の低下による影響が発生する状況に備えた官民共同の電子証明書の失効等の仕組みについて、2008 年度当初に検討に着手する。

エ 内閣官房、総務省及び関係府省庁は、新たな暗号アルゴリズムに対応した情報システムの相互運用性の検証を可能とする環境の整備について 2008 年度当初に検討に着手し、2009 年度の構築を目指す。

オ 各府省庁は、上述の検討結果を踏まえ、原則として、2010 年度に新規に構築（更改を含む。以下同じ。）する情報システムから 3(1)の設計要件を組み入れ、2013 年度までに各情報システムを当該要件に適合させるものとする。ただし、2009 年度に構築する情報システムについては、3(1)ウの仕様を適用する。

カ 総務省及び経済産業省は、SHA-1 及び RSA1024 の安全性について監視し、内閣官房は、必要な情報を速やかに各府省庁に提供する。

4 本指針の見直し

本指針は、暗号技術検討会及び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¹⁵の検討状況のほか、各府省庁の対応状況等を踏まえ、必要に応じて見直しを行う。

¹⁵ 総務省政策統括官（情報通信担当）、法務省民事局長及び経済産業省商務情報政策局長の私的検討会として開催。