NISC National Information Security Center

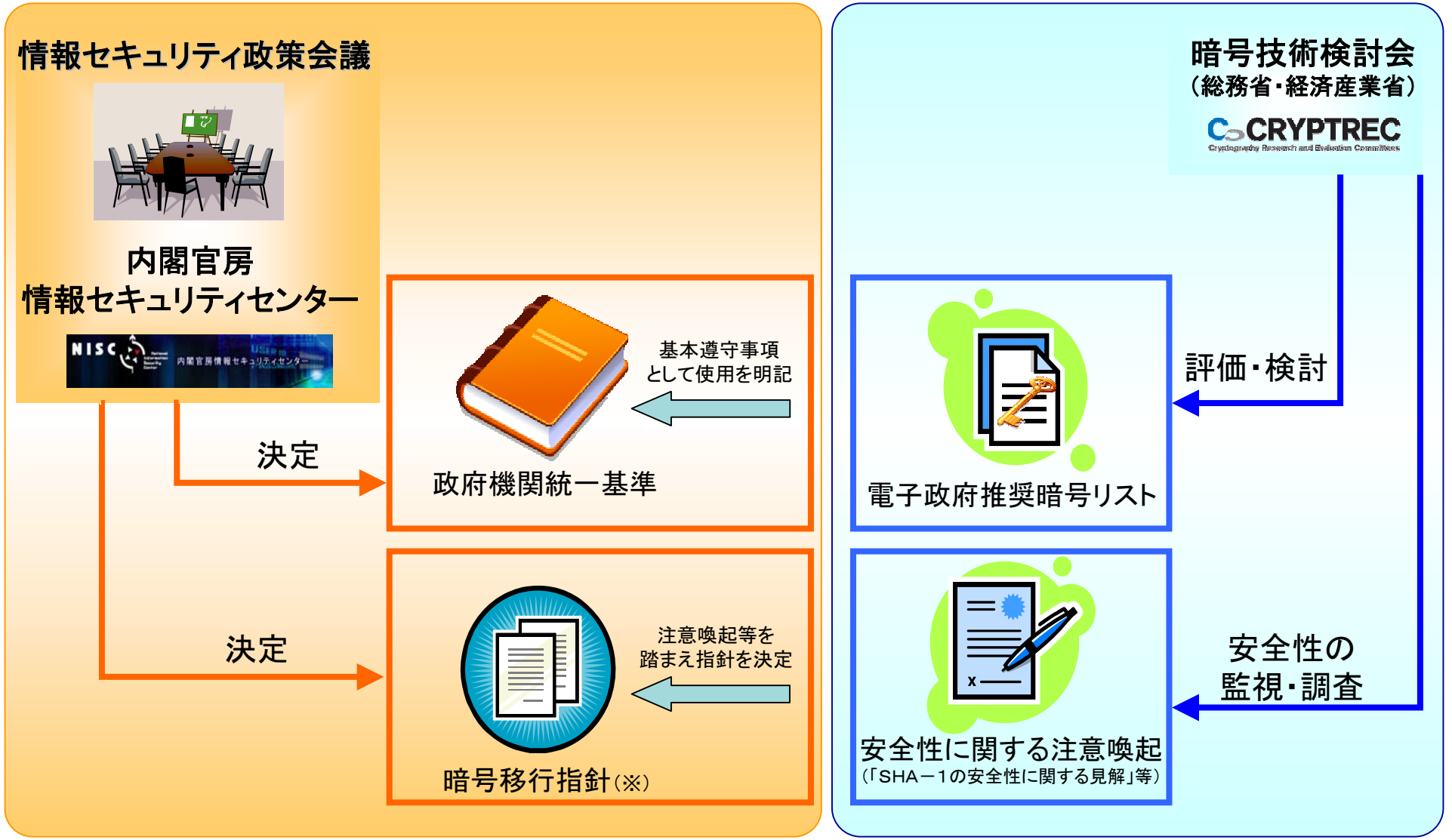
政府機関における安全な暗号利用の推進について

2009年2月18日

内閣官房情報セキュリティセンター（NISC）

http://www.nisc.go.jp/

政府機関における安全な暗号利用に関する現在の体制



※:「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」(平成20年4月22日情報セキュリティ政策会議決定)

政府機関の情報セキュリティ対策のための統一基準（第4版）

（2009年2月3日情報セキュリティ政策会議決定）

1.5.2.4 暗号と電子署名の標準手順

（1） 暗号と電子署名に係る規定の整備

【基本遵守事項】

（a） 統括情報セキュリティ責任者は、府省庁における暗号化及び電子署名のアルゴリズム及び方法を、以下の事項を含めて定めること。

（ア）**電子政府推奨暗号リストに記載されたものが使用可能な場合には、それを使用すること。**

（イ）情報システムの新規構築又は更新に伴い暗号化又は電子署名を導入する場合には、**電子政府推奨暗号リストに記載されたアルゴリズムを使用すること。**ただし、使用するアルゴリズムを複数のアルゴリズムの中から選択可能とするよう暗号化又は電子署名を実装する箇所においては、当該複数のアルゴリズムに、**少なくとも一つは電子政府推奨暗号リストに記載されたものを含めること。**

参考1：政府機関統一基準（第4版）における関連部分

2.1.1.6 暗号と電子署名（鍵管理を含む）

（1） 暗号化機能及び電子署名機能の導入

【強化遵守事項】

（g） 情報システムセキュリティ責任者は、暗号化又は電子署名の付与又は検証を行う必要があると認めた情報システムにおいて、選択したアルゴリズムがソフトウェア及びハードウェアへ適切に実装され、暗号化された情報の復号又は電子署名の付与に用いる鍵及び主体認証情報等が安全に保護された製品を使用するため、暗号モジュール試験及び認証制度に基づく認証を取得している製品を選択すること。

解説：アルゴリズムの実装状況及び鍵等の保護状況を確認するに当たり、ISO/IEC 19790に基づく暗号モジュール試験及び認証制度による認証を取得している製品を選択することを求める事項である。

アルゴリズム自体が安全であっても、それをソフトウェアやハードウェアへ実装する際、生成する疑似乱数に偏りが生ずる等の理由で疑似乱数が推測可能であったり、鍵によって処理時間に統計的な偏りが生ずる等の理由で鍵情報の一部が露呈したりすると、情報システムの安全性が損なわれるおそれがある。

なお、「適切に実装されている」とは、アルゴリズム自体の安全性だけではなく、疑似乱数の推測、鍵情報の一部露呈等の脅威に対応して実装していることをいい、その確認には、独立行政法人　情報処理推進機構(IPA)により運用されている暗号モジュール試験及び認証制度（JCMVP：Japan Cryptographic Module Validation Program）等が利用可能である。

参考2：SHA-1及びRSA1024の移行

「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」の決定

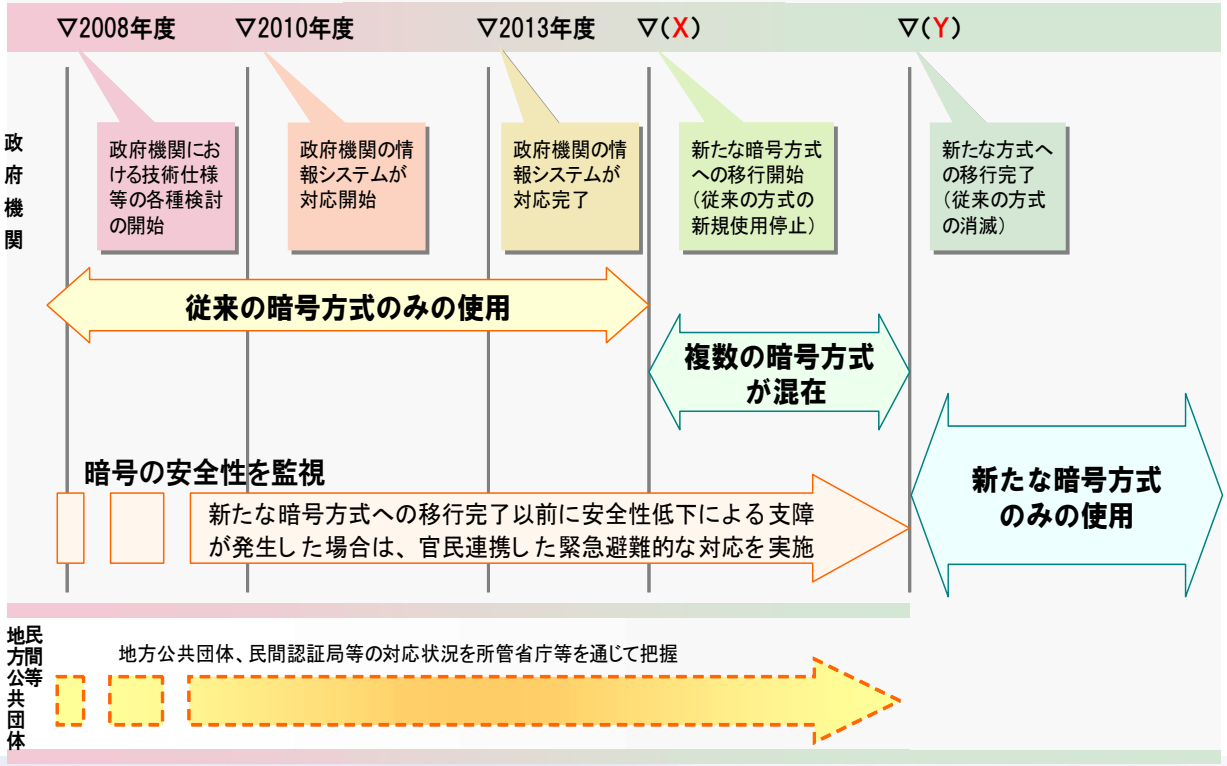
①電子政府システムでは、電子署名等のために暗号が使用されており、SHA-1及びRSA1024と呼ばれる暗号方式を広く使用。

②しかし、このSHA-1及びRSA1024は、安全性の低下が指摘されており、より安全な暗号方式への移行が必要。

③より安全な暗号方式への移行にあたっては、情報システムの相互運用性確保や政府全体の情報セキュリティの向上のため、政府統一的な移行指針を策定することが必要。

「新たな暗号方式としてSHA-256及びRSA2048を採用すること」などを規定した移行指針を情報セキュリティ政策会議において決定

移行指針に基づく暗号方式の移行スケジュール



（X，Y）：関係機関との調整を図りながら、2008年度中に時期を検討

（参考）

米国では**期限を決めて対応する方法**を採用し、2010年末以降、政府機関において、SHA-1の新規使用を停止する方針。

しかし、SHA-1が2010年に危殆化するかどうかは専門家の間でも意見がわかれる。

このため本指針は、**暗号の安全性低下の状況を監視しながら対応する方法**とし、政府が暗号の安全性を監視し、安全性低下が早まった場合は、緊急避難的な対応を実施（コンテンジェンシープランの発動）。

参考3：第2次情報セキュリティ基本計画における関連部分

第2次情報セキュリティ基本計画
（2009年2月3日情報セキュリティ政策会議決定）

第3章 今後3年間に取り組む重点政策

第1節 対策実施4領域における取組みの推進と政策目的の着実な実現

（1）対策実施4領域

① 政府機関・地方公共団体

［政府機関］

（ア）全ての政府機関において能動的に情報セキュリティ対策に取り組む体制の確立

5）技術面の知見を蓄積・活用する仕組みの構築

情報セキュリティ対策の推進に当たって、我が国における情報セキュリティに係る技術的・専門的な知識や経験の利用を図るため、関連する独立行政法人や情報セキュリティ関係団体などの研究者・実務家の知見を集合的に活用するための仕組みの構築を推進する。

（カ）その他個別の情報セキュリティ対策の推進

3）政府機関における安全な暗号利用の推進

電子政府の安全性及び信頼性を確保するため、政府機関で使われている推奨暗号について、その安全性を継続的に監視・調査するとともに、技術動向及び国際的な取組みを踏まえ、現行の「電子政府推奨暗号リスト」の2013年度改訂に向けて、関係機関において所要の作業を進める。また、「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」の策定時の経験を適切に継承し、安全性が低下した暗号について速やかに安全な暗号への移行を進める。

電子政府推奨暗号リスト及びCRYPTRECへの期待

電子政府推奨暗号リストの在り方について

- 今回、単一のリスト方式から「推奨暗号候補リスト」や「互換性維持暗号リスト」など複数のリスト方式に細分化され、安全性のレベルについて、よりユーザーが理解しやすくなったものと認識。
- 今後は、リストの評価及びリスト間の移動が適切に行われることを期待。
- 特に、暗号の移行は一朝一夕には行かないため、調達側が調達サイクル等を踏まえて「互換性維持暗号リスト」などを適切に活用できるように、移動する際の基準について、予め明確にしていただく、又は、移動する際に理由・根拠を明確に公表していただきたい。

CRYPTRECの在り方について

- 暗号分野の研究については、情報セキュリティ分野の中でもより専門性が高いため、CRYPTRECの監視活動やリストガイド作成等の活動に期待。
- 海外で研究発表が行われるケースも多く、CRYPTRECでは、これらの情報収集活動を行っていると承知しているが、状況の変化があった場合には、暗号技術監視委員会などの定例の会議に加えて、リアルタイムに情報を共有してもらえることも期待。
- また、今回のSHA-1及びRSA1024の移行に当たっては、これらの急激な安全性の低下に備えた監視活動が必須であることから、その情報共有については、特にお願いしたい。