資料4

NISC National Information Security Center

政府機関における暗号の安全性低下への対応について

「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

2008年9月

内閣官房情報セキュリティセンター（NISC）

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

暗号の安全性低下への対応

1　現状と課題

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。

2　暗号の移行指針の概要

①技術的な対応

【政府認証基盤とそれに依存する各府省庁の情報システム】

○ 相互運用性確保のため、新旧暗号方式の双方に対応し、適切な時期に暗号方式を切り替える運用を可能に。

○ 新たな暗号方式として、SHA-256及びRSA2048を採用。

○ 移行完了前に安全性低下の影響が発生する場合に備え、緊急避難的な対応も想定。

【上記以外の情報システム】

○ 現実的な脅威となる攻撃手法が示された時点で、速やかに別の暗号方式に変更する等の対応措置を可能とする。

○ 新たな暗号方式は、より安全なものを各府省庁において判断し決定する。

②制度的な対応

○ 各府省庁において次を実施
・システムの移行時期を踏まえ、必要な対応の取りまとめ
・移行手順書の整備

③スケジュール

○ 内閣官房、総務省、法務省、経済産業省等
新たな暗号方式へ切り替える時期等を2008年度中に検討。

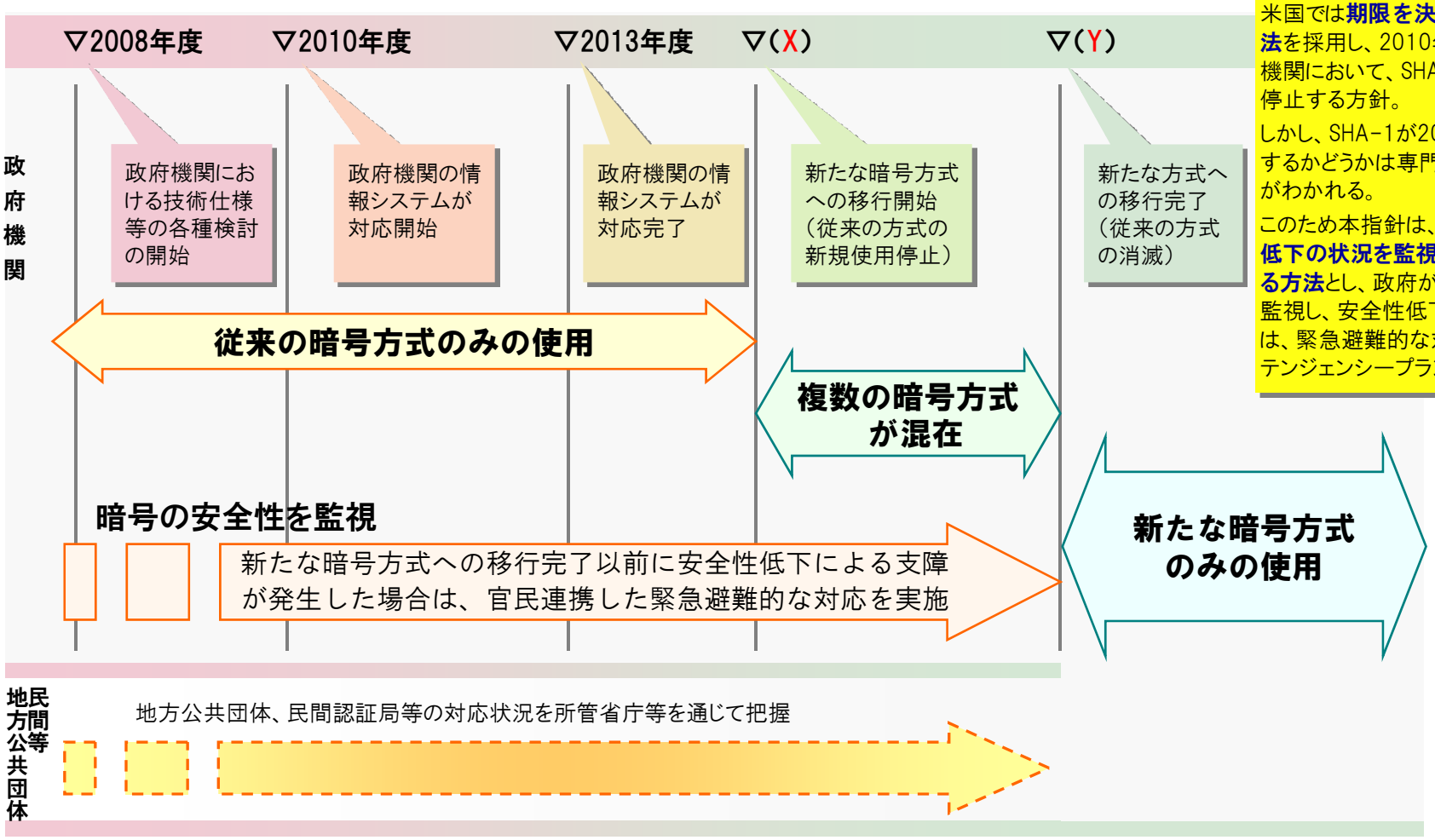
○ 内閣官房、総務省等
相互接続の技術要件、緊急避難対応等について2008年度中に検討。

○ 各府省庁
2010年から2013年までの間に、各情報システムの対応を完了。

○ 内閣官房、総務省、経済産業省
安全性の状況を監視し、必要な情報を速やかに各府省庁に提供。

移行指針に基づく暗号方式の移行完了までのスケジュール

（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）。

認証局とブリッジCAによる相互認証