



政府機関における安全な暗号利用の促進

「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2月4日(月)

内閣官房情報セキュリティセンター(NISC)

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

1 現状と課題

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。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**。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(案)の概要

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。

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

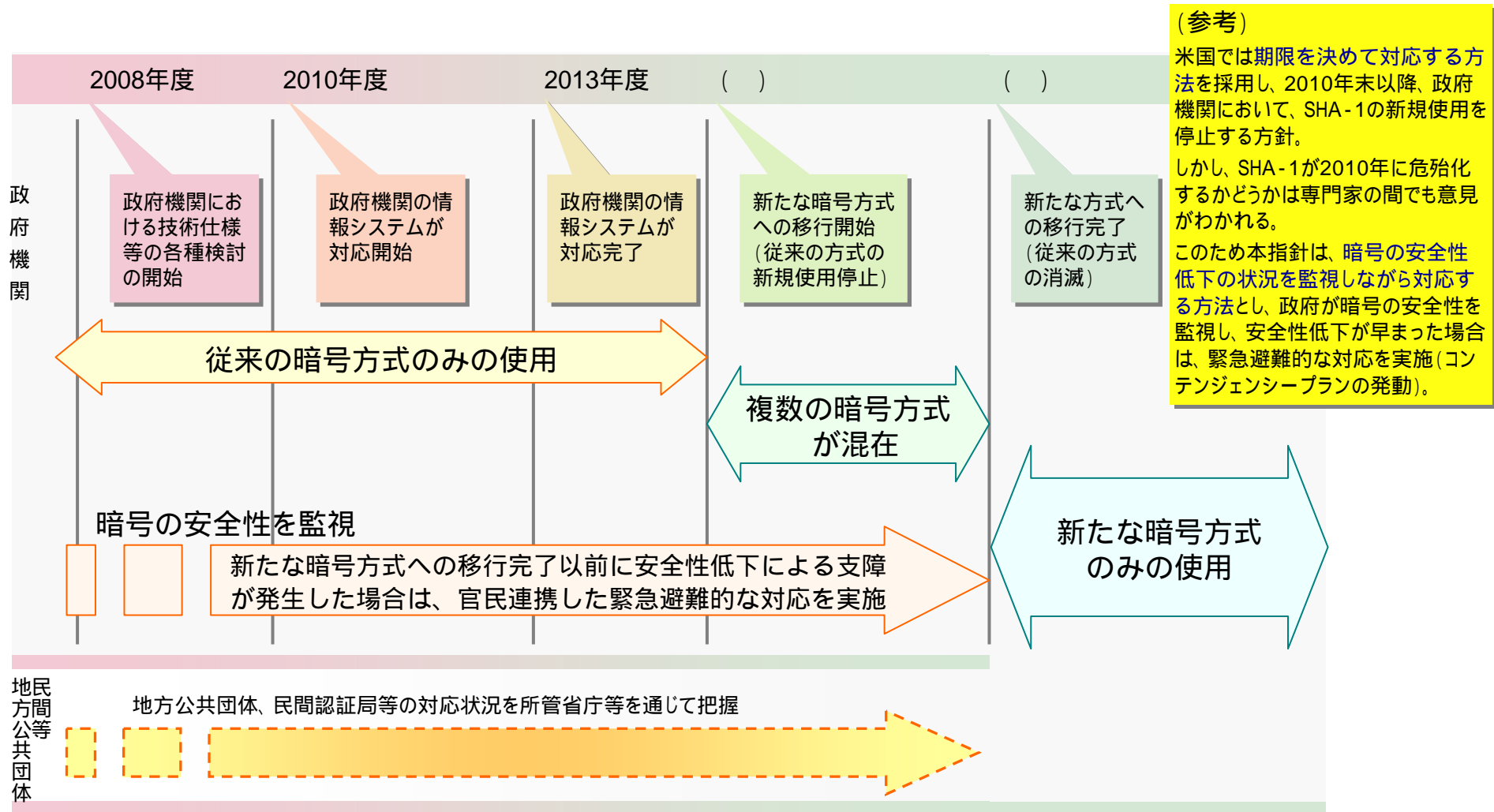
スケジュール

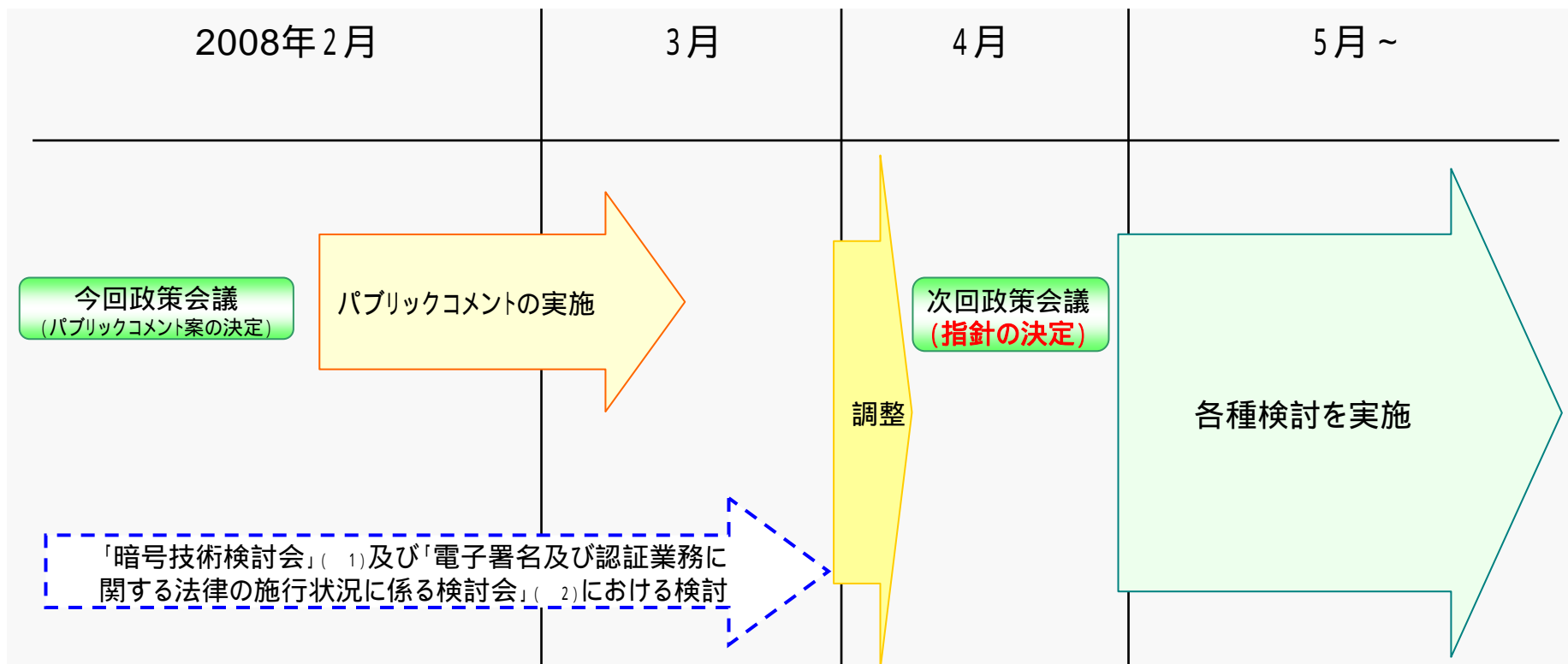
- 内閣官房、総務省、法務省、経済産業省等
新たな暗号方式へ切り替える時期等を2008年度中に検討。
- 内閣官房、総務省等
相互接続の技術要件、緊急避難対応等について2008年度中に検討。
- 各府省庁
2010年から2013年までの間に、各情報システムの対応を完了。
- 内閣官房、総務省、経済産業省
安全性の状況を監視し、必要な情報を速やかに各府省庁に提供。

移行指針(案)に基づく暗号方式の移行完了までのスケジュール



():関係機関との調整を図りながら、
2008年度中に時期を検討





(1) 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
 (2) 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