公的個人認証サービスにおける暗号方式等の移行に関する検討会報告書の概要

開催背景

- 近年、公的個人認証サービスにおいて利用されているハッシュ関数SHA-1及び公開鍵暗号方式RSA1024について、暗号技術検討会等において安全性の低下により将来問題が生じる可能性が指摘されている。
- このため、公的個人認証サービスにおける暗号方式等の移行に関する検討会は、平成20年9月16日から同年12月18日まで計3回開催され、公的個人認証サービスにおける暗号アルゴリズムの移行の必要性及び移行案、今後の検討事項等について検討を行った。

公的個人認証サービスにおける暗号アルゴリズムの移行案

- SHA-1及びRSA1024に代わる暗号アルゴリズムとしてSHA-256及びRSA2048を利用することが適当である。
- 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である。ただし、このスケジュールについてはSHA-1及びRSA1024の急速な安全性低下を前提としていないため、今後、コンティンジェンシープランを検討する必要がある。また、利用者の利便性及び「今後の検討事項（右下を参照のこと。）」に十分配慮して移行を進める必要がある。
- 暗号アルゴリズムの移行案については、暗号アルゴリズムの監視状況等を踏まえ、必要に応じて見直しを行う必要がある。

暗号アルゴリズムの移行スケジュール

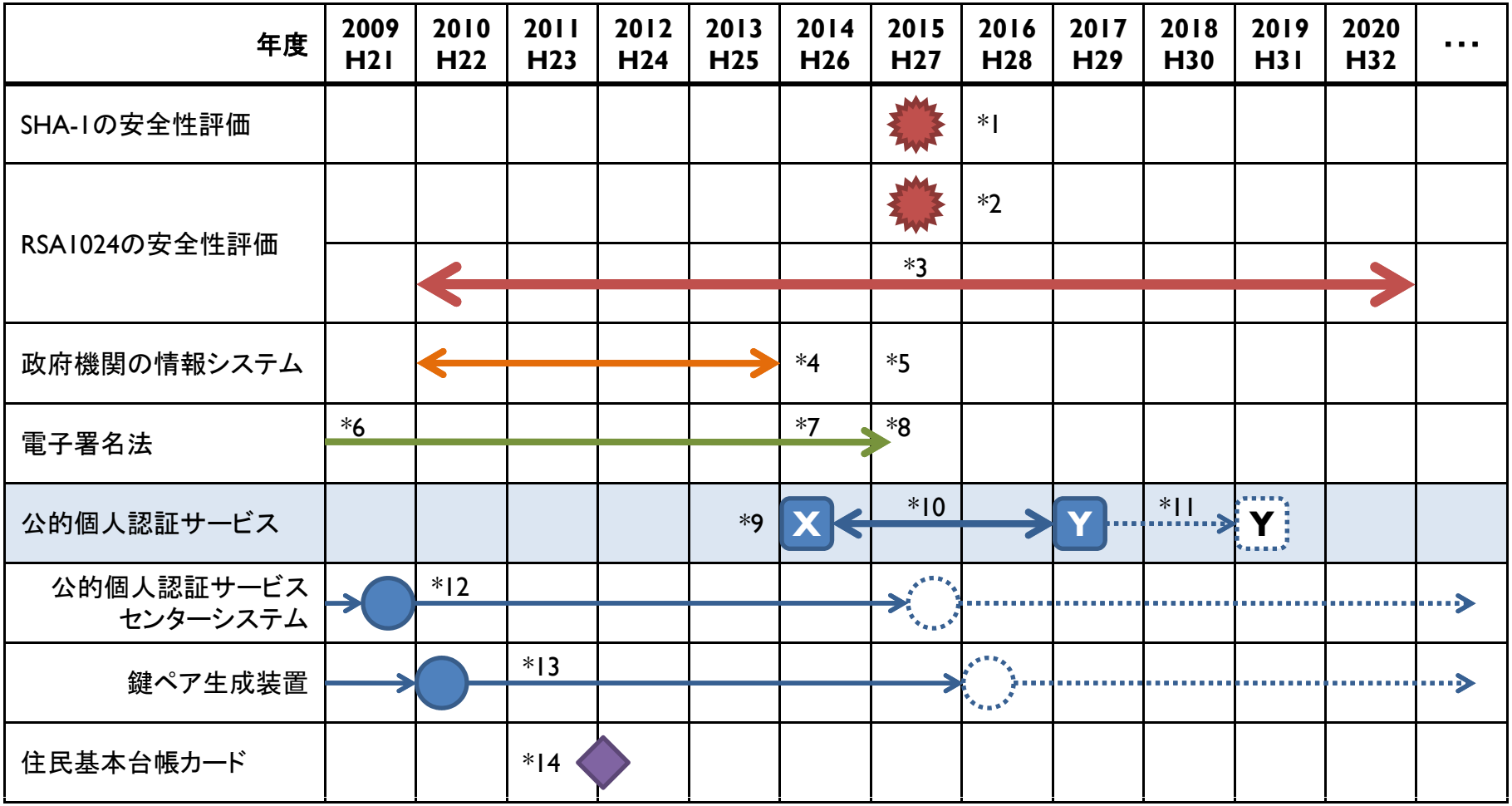
2014年度早期	新電子証明書の発行を開始するとともに、旧電子証明書の発行を停止する。
2017年度早期（電子証明書の有効期間が5年に延長された場合には2019年度早期）	旧電子証明書の有効期間後に、SHA-1及びRSA1024の使用を停止する。

今後の検討事項

- 暗号技術検討会等の意見等を踏まえコンティンジェンシープランを検討する必要がある。
- SHA-256及びRSA2048に対応する公的個人認証サービスセンターシステムの構築、鍵ペア生成装置の調達、住基カードの交付等について、手順、スケジュール、所要の経費等を検討する必要がある。
- 電子署名を行う電子文書の長期利用に関する対策及び暗号アルゴリズムの安全な移行方法について検討する必要がある。

公的個人認証サービスにおける暗号方式等の移行に関する検討会報告書　www.soumu.go.jp/menu_03/shingi_kenkyu/kenkyu/kouteki_kojin/

公的個人認証サービスにおける暗号アルゴリズムの移行スケジュール



公的個人認証サービスにおける暗号アルゴリズムの移行スケジュール（注釈）

*1	「衝突計算攻撃による脅威は、2015年前後には現実的になることが想定される」。
*2	「概ね2015年以降に、危殆化のおそれが高まってくることが示されている」。
*3	「1年間の計算によって攻撃可能になる時期については、2010年～2020年の間と推定することができた。」
*4	各府省庁は、2010年度から2013年度までの間に各情報システムの対応を完了する。
*5	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。
*6	特定認証業務に係る電子署名の基準にSHA-2を追加する。（2008年度）
*7	SHA-2及びRSA2048による電子署名についての認証業務を開始する。（ 2014年度早期まで）
*8	SHA-1及びRSA1024による利用者電子証明書の有効期間後に、特定認証業務に係る電子署名の基準からSHA-1及びRSA1024を削除する。（ 2014年度末前後を目途）
*9	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。（2014年度早期）
*10	新旧暗号アルゴリズム（SHA-1及びRSA1024並びにSHA-256及びRSA2048）の併用期間。
*11	SHA-1及びRSA1024による電子証明書の有効期間後に、SHA-1及びRSA1024による電子署名に係る認証業務を停止する。（2017年度早期（電子証明書の有効期間が5年に延長された場合には2019年度早期））
*12	公的個人認証サービスのセンターシステムを更改し、次期センターシステムによるサービスを開始する。（2010年1月）
*13	市町村窓口の鍵ペア生成装置を更改する。（2010年度（想定））
*14	2011年度末を目途に新たな暗号アルゴリズムに対応する住基カードの交付を開始することが検討されている。