資料1

検討会報告書案について

総務省 地域力創造グループ 地域情報政策室

目次

1. はじめに
2. 公的個人認証サービスにおける暗号アルゴリズムの利用
    2.1. 公的個人認証サービスにおける暗号アルゴリズムの利用
    2.2. 公的個人認証サービスにおいて利用する暗号アルゴリズムを規定する法令等
    2.3. 本検討会の検討事項
3. 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
    3.1. SHA-1及びRSA1024の安全性評価
    3.2. 政府機関における暗号アルゴリズムの安全性低下への対応
    3.3. 電子署名法に関する暗号アルゴリズムの移行
    3.4. 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
4. 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
    4.1. SHA-1及びRSA1024に代わる暗号アルゴリズム
    4.2. 暗号アルゴリズムの移行スケジュール
    4.3. 暗号アルゴリズムの移行案の見直し
5. 今後の検討事項

4.2. 暗号アルゴリズムの移行スケジュール（1）

移行スケジュール検討の必要性

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に当たっては、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、鍵ペア生成装置及び受付窓口端末の調達、公的個人認証サービスアプリケーションの開発、住基カードの交付等が必要となるため、暗号アルゴリズムの円滑な移行に向けて、移行スケジュールは予め示されることが望ましい。

具体的な検討事項

① SHA-256及びRSA2048による電子証明書（新電子証明書）の発行開始時期

② SHA-1及びRSA1024による電子証明書（旧電子証明書）の発行停止時期

③ SHA-1及びRSA1024による電子署名に係る認証業務の停止時期（SHA-1及びRSA1024の使用停止時期）

4.2. 暗号アルゴリズムの移行スケジュール（2）

① 新電子証明書の発行開始時期

以下の事項を考慮すると2014年度早期とすることが適当である。

- 電子署名法の施行状況に係る検討会報告書において、SHA-1の安全性については「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」、またRSA1024の安全性については「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」と指摘されている。
- 政府機関における暗号アルゴリズムの安全性低下への対応について、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ことが、移行指針において示されている。
- 電子署名法に関する暗号アルゴリズムの移行については、電子署名法の施行状況に係る検討会報告書においてSHA-2及びRSA2048による「電子署名についての特定認証業務の認定は遅くとも2014年度早期までに行うことが必要である」と指摘されている。
- 2012年度早期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。

4.2. 暗号アルゴリズムの移行スケジュール（3）

② 旧電子証明書の発行停止時期

新電子証明書及び旧電子証明書を併行して発行することとなった場合、公的個人認証サービスセンターシステムの運用費用及び鍵ペア生成装置の調達費用が増大すると考えられるため、新電子証明書の発行開始時期と同時期（2014年度早期）とすることが適当である。

4.2. 暗号アルゴリズムの移行スケジュール（4）

③　SHA-1及びRSA1024の使用停止時期

以下の事項を考慮すると、現段階では上記の旧電子証明書の発行停止時期（2014年度早期）及び電子証明書の有効期間（3年）を踏まえた時期（2017年度早期。ただし、電子証明書の有効期間は今後延長される可能性があり、有効期間が5年に延長された場合には2019年度早期）とすることが適当である。

- RSA1024の安全性について、「暗号技術検討会2006年度報告書」において「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」と指摘されている。
- SHA-1及びRSA1024の使用停止時期を2015年度早期又は2016年度早期とした場合、電子証明書の有効期間（3年）中に電子証明書が失効するとともに、住基カードの有効期間（10年）中に住基カードが失効するため、利用者の利便性を損なう。また、特定の時期（SHA-1及びRSA1024の使用停止時期直後等）に多くの利用者が市町村の窓口で電子証明書及び住基カードの再発行を申請することになるため、公的個人認証サービスの運営及び市町村における住基カードの発行業務に混乱が生じるおそれがある。

4.2. 暗号アルゴリズムの移行スケジュール（5）

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	
2014年度早期	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。
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）	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。

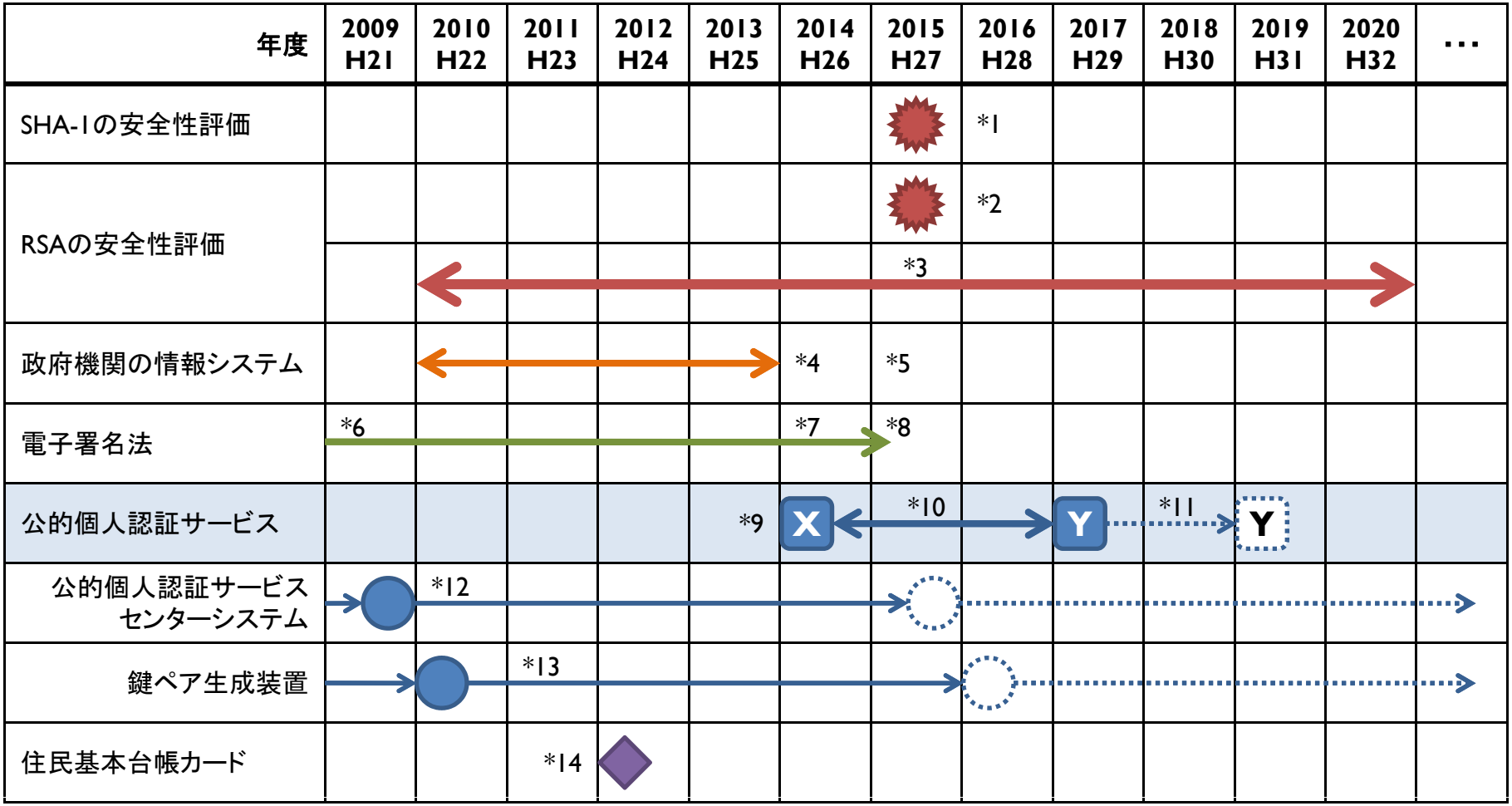
総務省において、現段階では上記の移行スケジュールを基本として施行規則及び技術的基準の改正作業等を進めていくことが適当である。ただし、このスケジュールについてはSHA-1及びRSA1024の急速な安全性低下を前提としていないため、今後、SHA-1及びRSA1024の使用停止時期以前にSHA-1及びRSA1024の安全性低下により問題が生じる状況に備え、暗号技術検討会等の意見等を踏まえコンティンジェンシープランを検討する必要がある。また、利用者の利便性及び「5. 今後の検討事項」に十分配慮して公的個人認証サービスにおける暗号アルゴリズムの移行を進める必要がある。

4.3. 暗号アルゴリズムの移行案の見直し

暗号アルゴリズムの移行案については、暗号技術検討会等における暗号アルゴリズムの監視状況、政府機関における暗号アルゴリズムの安全性低下への対応状況、電子署名法に関する暗号アルゴリズムの移行状況、公的個人認証制度の改正状況等を踏まえ、必要に応じて見直しを行う必要がある。

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

参考資料



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）

参考資料

*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	2012年度早期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。

5. 今後の検討事項

- SHA-1及びRSA1024の使用停止時期以前にSHA-1及びRSA1024の安全性低下により問題が生じる状況に備え、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、鍵ペア生成装置及び受付窓口端末の調達、公的個人認証サービスアプリケーションの開発、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。
- 電子署名に関する現在の運用においては、電子署名に利用する暗号アルゴリズムの移行に伴い、SHA-1及びRSA1024による電子署名の検証が将来できなくなるため、対策を検討する必要がある。また、暗号アルゴリズムの移行に当たってセキュリティホールを作らないよう、暗号アルゴリズムの安全な移行方法を検討する必要がある。