暗号アルゴリズムの移行スケジュール案

総務省 地域力創造グループ 地域情報政策室

移行スケジュール案の検討について

移行スケジュール案検討の必要性

- 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、新たに採用する暗号アルゴリズムに対応した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、住民基本台帳カードの発行等の準備が必要となるため、暗号アルゴリズムの円滑な移行に向けて、移行スケジュール案は予め示されることが望ましい。

具体的な検討事項

- 移行スケジュール案の検討に当たって、具体的には新たな暗号アルゴリズムを利用する電子署名に関する認証業務の開始時期（新たな暗号アルゴリズムを利用する電子証明書の発行開始時期、移行指針（＊）中「新たな暗号アルゴリズムへの切替時期」に対応するもの）、SHA-1及びRSA1024を利用する電子証明書の発行停止時期、SHA-1及びRSA1024を利用する電子署名に関する認証業務の停止時期（移行指針中「SHA-1及びRSA1024の使用停止時期」に対応するもの）を検討する必要がある。

＊「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」
（平成20年4月22日情報セキュリティ政策会議決定）

移行スケジュール案

X：新たな暗号アルゴリズムを利用する電子署名に関する認証業務の開始時期
（新たな暗号アルゴリズムを利用する電子証明書の発行開始時期）
（移行指針中「新たな暗号アルゴリズムへの切替時期」に対応するもの）
Z：SHA-1及びRSA1024を利用する電子証明書の発行停止時期
Y：SHA-1及びRSA1024を利用する電子署名に関する認証業務の停止時期
（移行指針中「SHA-1及びRSA1024の使用停止時期」に対応するもの）

案	X	Z	Y
A案	2014年度早期	2014年度早期 （Xと同時）	2015年度早期 （Z＋1年）
B案	2014年度早期	2014年度早期 （Xと同時）	2017年度～2019年度早期 （Z＋3～5（＊）年）
C案	2014年度早期	2022年度早期 （2012年度早期＋10年）	2025年度～2027年度早期 （Z＋3～5（＊）年）

＊　電子証明書の有効期間（3年）は今後延長される可能性がある。

Xについて（各案共通）

新たな暗号アルゴリズムを利用する電子署名に関する認証業務の開始時期（新たな暗号アルゴリズムを利用する電子証明書の発行開始時期、移行指針中「新たな暗号アルゴリズムへの切替時期」に対応するもの）については、以下の事項を考慮すると2014年度早期が適当ではないか。

関係する情報システムとの連携について

- 政府機関の情報システムについて、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。（移行指針）
- 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。（電子署名法の施行状況に係る検討会報告書（＊））

SHA-1及びRSA1024の安全性低下について

- RSA1024が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。（「暗号技術検討会2006年度報告書」）
- SHA-1の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。（電子署名法の施行状況に係る検討会報告書）

＊「電子署名及び認証業務に関する法律の施行状況に係る検討会報告書」（平成20年3月）

Ｙ・Ｚについて（各案の特徴）

A案（Z：2014年度早期、Y：2015年度早期）　〔電子署名法に関する暗号アルゴリズムの移行スケジュール案（2014年度末前後を目途に、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。）に対応。〕

- SHA-1及びRSA1024の使用停止時期は2015年度早期。（安全性の観点から検討が必要。）
- 電子証明書の有効期間（3年～5年（＊））中に、電子証明書の再発行が必要。（住民の利便性等の観点から検討が必要。）
- 住基カードの有効期間（10年）中に、住基カードの再発行が必要。（住民の利便性等の観点から検討が必要。）

B案（Z：2014年度早期、Y：2017年度～2019年度（＊）早期）　〔電子証明書の有効期間（3年～5年（＊））に対応。〕

- SHA-1及びRSA1024の使用停止時期は2017年度～2019年度早期。（安全性の観点から検討が必要。）
- 住基カードの有効期間（10年）中に、住基カードの再発行が必要。（住民の利便性等の観点から検討が必要。）

C案（Z：2022年度早期、Y：2025年度～2027年度（＊）早期）　〔新たな暗号アルゴリズムに対応した住基カードの発行スケジュール（2012年度早期を目途に検討中。）及び住基カードの有効期間（10年）に対応。〕

- SHA-1及びRSA1024の使用停止時期は2027年度早期。（安全性の観点から検討が必要。）
- 新旧の電子証明書を併行して発行する期間が生じる。（運営費用の観点から検討が必要。）

Ｚ：SHA-1及びRSA1024を利用する電子証明書の発行停止時期

Ｙ：SHA-1及びRSA1024を利用する電子署名に関する認証業務の停止時期

＊　電子証明書の有効期間（3年）は今後延長される可能性がある。

移行スケジュール案（まとめ）

	X （発行開始時期）	Z （発行停止時期）	Y （使用停止時期）	主な特徴
A案	2014年度早期	2014年度早期 （Xと同時）	2015年度早期 （Z＋1年）	● 電子署名法に関する暗号アルゴリズムの移行スケジュール案に対応。 ● 電子証明書の有効期間（3年～5年（＊））中に電子証明書の再発行が必要。 ● 住基カードの有効期間（10年）中に住基カードの再発行が必要。
B案	2014年度早期	2014年度早期 （Xと同時）	2017年度～ 2019年度早期 （Z＋3～5（＊）年）	● 電子証明書の有効期間（3年～5年（＊））に対応。 ● 住基カードの有効期間（10年）中に住基カードの再発行が必要。
C案	2014年度早期	2022年度早期 （2012年度早期 ＋10年）	2025年度～ 2027年度早期 （Z＋3～5（＊）年）	● 新たな暗号アルゴリズムに対応した住基カードの発行スケジュール（2012年度早期を目途に検討中。）及び住基カードの有効期間（10年）に対応。 ● 新旧の電子証明書を併行して発行する期間が生じる。

SHA-1及びRSA1024の安全性低下について

- RSA1024が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。（「暗号技術検討会2006年度報告書」）
- SHA-1の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。（電子署名法の施行状況に係る検討会報告書）

＊　電子証明書の有効期間（3年）は今後延長される可能性がある。