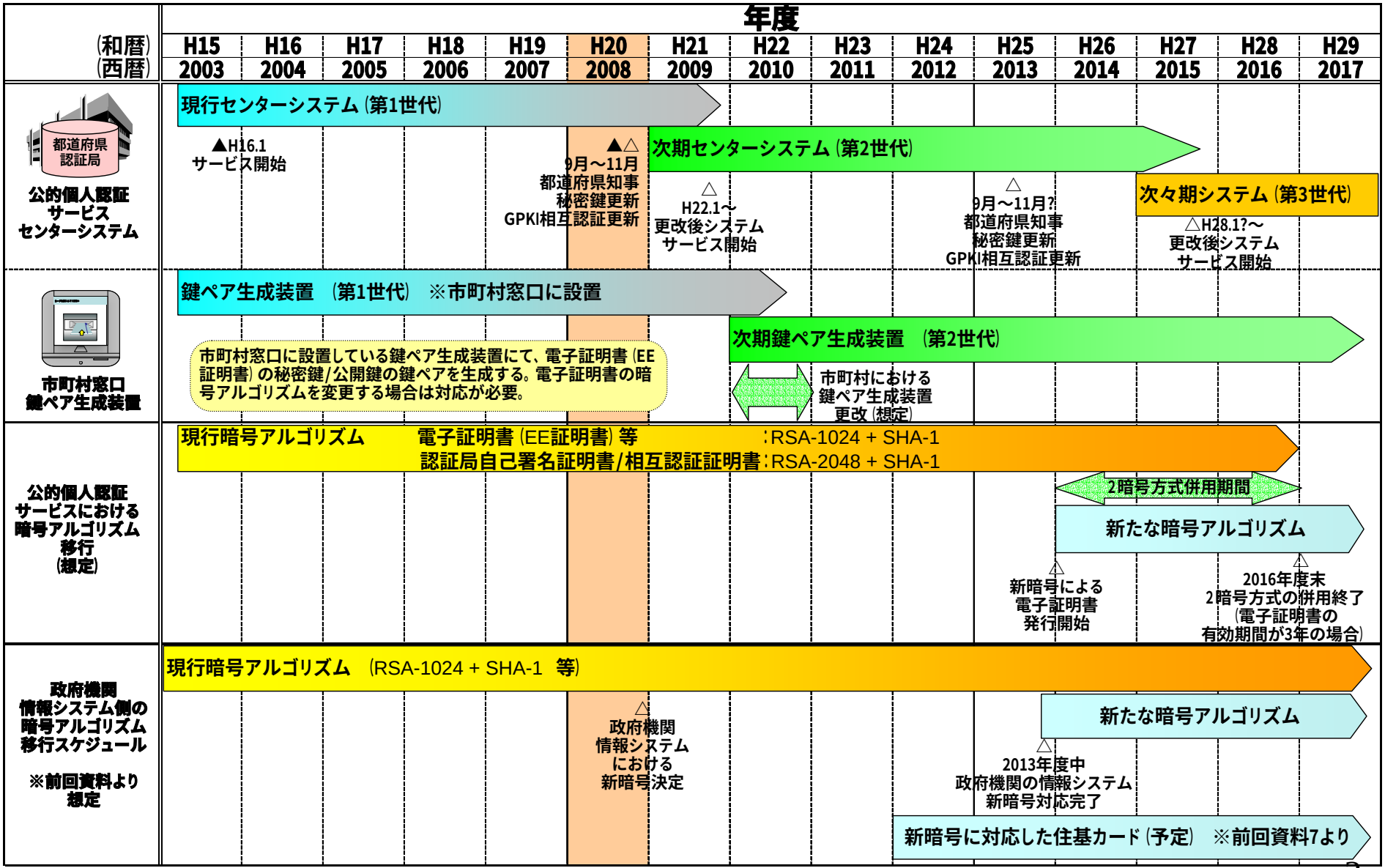
資料3

公的個人認証サービスにおける
システム更改の状況と
暗号アルゴリズムの移行にかかる影響について

平成20年10月27日

財団法人　自治体衛星通信機構
公的個人認証サービスセンター

公的個人認証サービスのシステム更改スケジュール案
(暗号危殆化対応との関連)



公的個人認証サービスにおける主な暗号アルゴリズム利用状況

主な暗号アルゴリズム利用箇所	
都道府県認証局 ブリッジ認証局	公開鍵証明書の鍵ペア及び署名 ・電子証明書（利用者用証明書） ・認証局自己署名証明書 ・相互認証証明書（ブリッジ認証局～都道府県認証局間、対政府認証基盤（ＧＰＫＩ））
失効情報提供サービス （CRL提供方式（リポジトリ））	失効情報リストに対する署名 ・CRL（電子証明書の失効情報リスト） ・ARL（自己署名証明書等の失効情報リスト）
失効情報提供サービス （OCSPレスポンダ照会方式）	OCSPレスポンスに対する署名
	CRL取り込みの際の署名検証
官職証明書検証サービス	レスポンスに対する署名
	リクエストに付与された利用者の署名検証
	官職証明書等の検証
オンライン窓口　（有効性確認、オンライン失効申請）	オンライン失効申請に対する署名
市町村受付窓口端末	ICカード認証用署名
	鍵ペア生成装置の署名検証
鍵ペア生成装置	電子証明書（利用者証明書）の鍵ペア生成及び署名
利用者クライアントソフト	電子署名付与機能 ・電子申請文書等への署名付与 ・官職証明書検証サービス利用要求（リクエスト）への署名
その他	・都道府県知事自己署名証明書やブリッジ認証局自己署名証明書のフィンガープリント ・センター内外の通信暗号化（SSL通信） ・運用機能における利用

※ICカード（現在は住基カードのみ）や、署名検証者（電子申請・申告等システム）における影響点は考慮していない。

公的個人認証サービスで暗号アルゴリズムを変更する際に考慮が必要となる主な外的要因（その1）

●政府認証基盤（GPKI）

署名検証者（府省庁・地方自治体）が運営する電子申請・申告等システムにおける電子証明書の有効性確認は、GPKIが公的個人認証サービスを相互認証先としていることで担保されている。

GPKIが定める相互認証基準（相互運用性仕様）において、相互認証先認証局が満たすべき暗号アルゴリズム（鍵長等）が規定されている。

暗号アルゴリズム変更後もGPKIと相互認証するためには、暗号アルゴリズム変更後の相互認証基準に公的個人認証サービス側認証局が準拠する必要がある。

（電子証明書だけではなく、認証局の鍵長（RSA-2048）の変更も考慮が必要）

●ICカード（住基カード）

電子証明書及び利用者秘密鍵を安全に格納する媒体であることから、暗号アルゴリズム変更後の鍵長等に対応されていることが必須である。

公的個人認証サービスで暗号アルゴリズムを変更する際に考慮が必要となる主な外的要因（その2）

●鍵ペア生成装置

市町村窓口において利用者の鍵ペア（秘密鍵・公開鍵）を生成し、ICカード（住基カード）に格納する手段となるもので、市町村毎に製造事業者等から購入または借入（リース）している。

暗号アルゴリズムを変更する場合は、変更後アルゴリズムに対応した機器を市町村毎に導入する必要がある。

●ICカードリーダライタ

市町村窓口端末や利用者パソコンに接続し、

- ICカードに対する電子証明書の格納（電子証明書発行時）
- ICカード内の電子証明書の取り出し・秘密鍵を用いた電子署名値の受け渡し（電子証明書利用時）

等のために必要となるもので、市町村や利用者が製造事業者等から購入または借入（リース）している。

暗号アルゴリズムを変更することによる影響の見極めが必要である。