

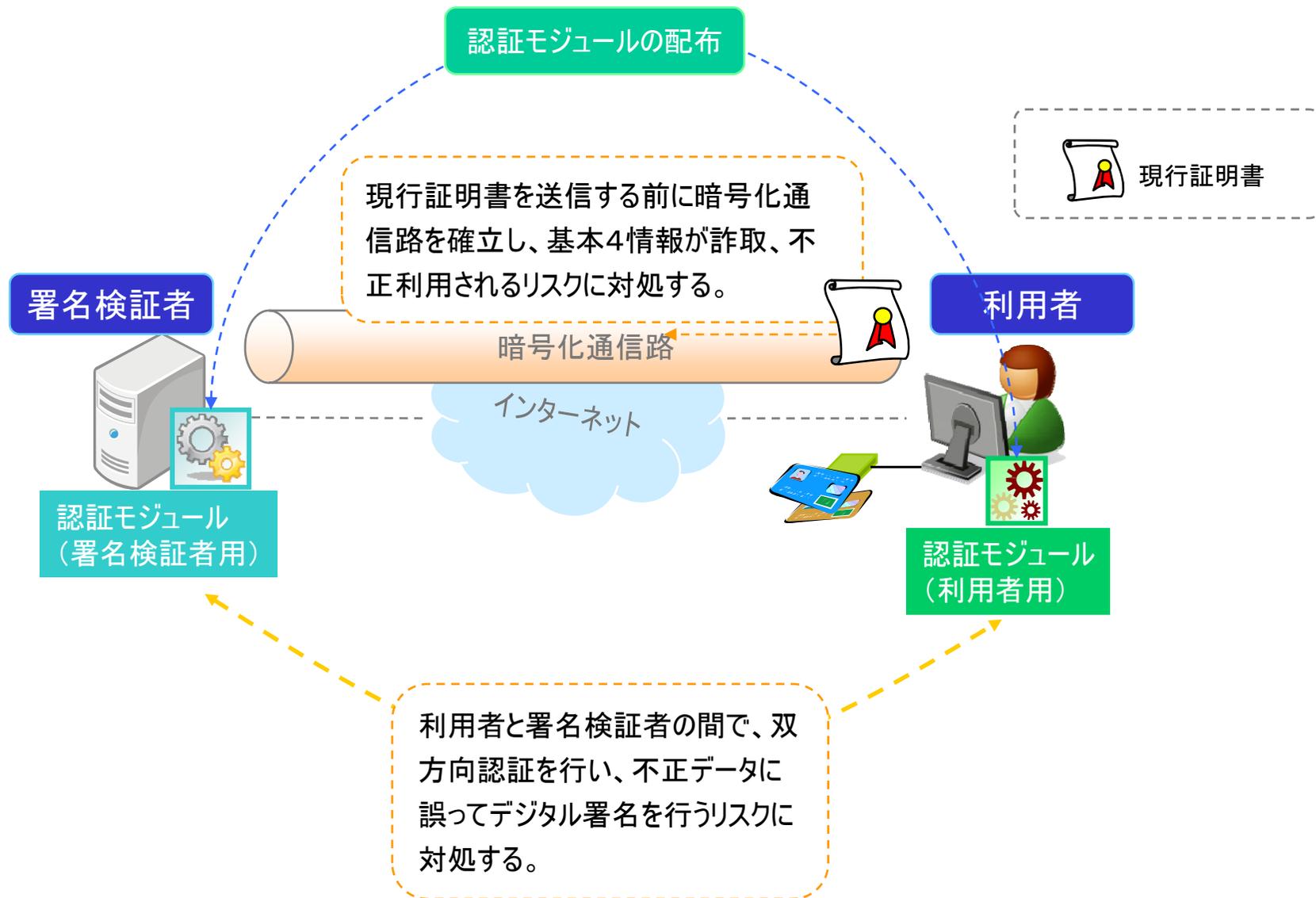
参考資料

目次

1. 認証用途の付加	
・案1：現行証明書を認証用として併用＜実現イメージ＞	1
・案2：現行証明書とは別に、基本4情報の一部のみを記載する認証用証明書を発行＜実現イメージ＞	2
2. 記録媒体の拡大	
・主要な記録媒体の普及状況	3
3. オンライン更新	
・案1 双方向認証後、サーバ側で鍵ペア生成後、暗号化してICカードまで送信する方式＜実現イメージ＞	4
・案2 双方向認証後、ICカードで鍵ペアを生成する方式＜実現イメージ＞	5
4. 有効期間の延長	
・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	6
・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)	7
・案1 <実現イメージ>	8
・案2 <実現イメージ>	9
・方向性＜実現イメージ＞	10
5. 署名検証者の拡大(民間事業者への拡大)	
・案1 署名検証に必要な設備は民間事業者において整備＜実現イメージ＞	11
・案2 事業者基盤設備を整備し、民間事業者に必要なサービスを提供＜実現イメージ＞	12
6. 利用用途の拡大(署名メール及び暗号メール)	
・案 署名メール(共同利用設備を設置し、必要なサービスを提供)＜実現イメージ＞	13
・案 暗号メール(共同利用設備を設置し、必要なサービスを提供)＜実現イメージ＞	14
・ISP等が公的個人認証サービスを利用して署名メール用の電子証明書を発行＜実現イメージ＞	15
・ISP等が公的個人認証サービスを利用して暗号メール用の電子証明書を発行＜実現イメージ＞	16

1. 認証用途の付加

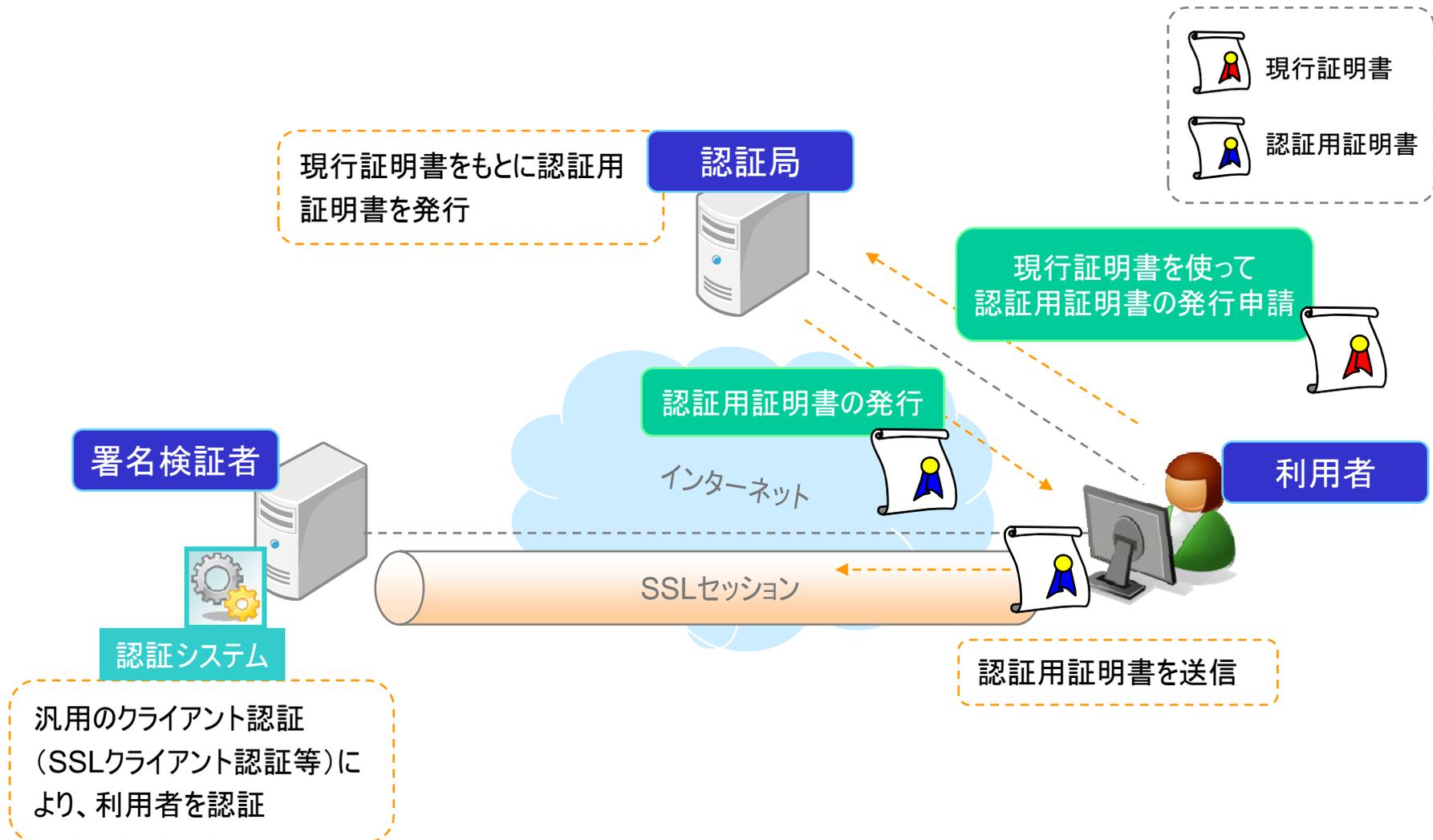
案1： 現行証明書を認証用として併用＜実現イメージ＞



1. 認証用途の付加

案2： 現行証明書とは別に、基本4情報の一部のみを記載する認証用証明書を発行

<実現イメージ>



2. 記録媒体の拡大

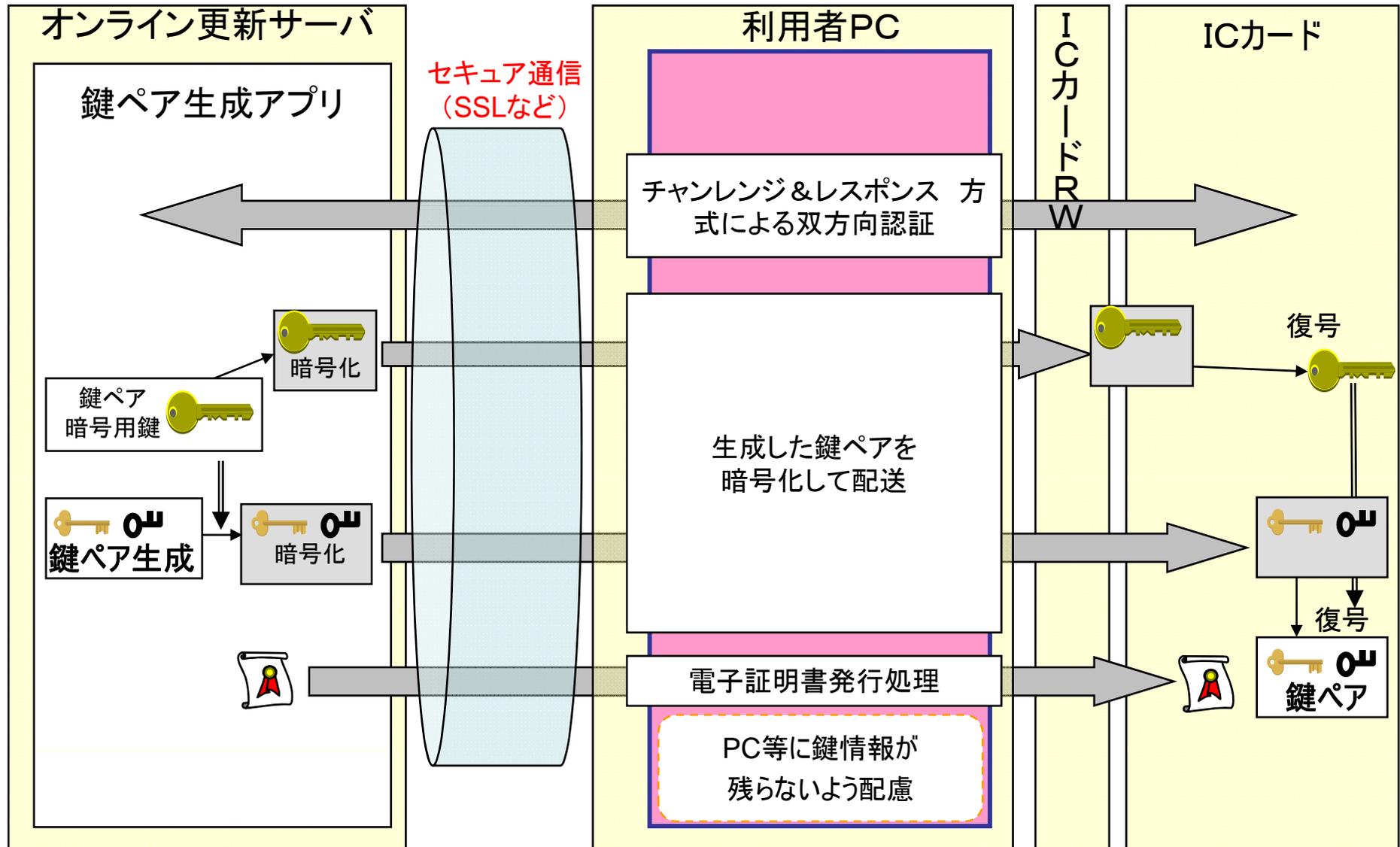
主要な記録媒体の普及状況

記録媒体	発行枚数等	備考
非接触ICカード技術方式 “FeliCa”対応の媒体 (Edy、Suica、PASMO、 nanaco、WAON、ICOCA)	1億1017万枚	・2009年5月末時点 2009年6月26日「日経流通新聞」7面 「主要6電子マネーの普及状況(前払い方式)」より
携帯電話(第三世代)	8,810万加入	・2008年3月末時点 ・平成20年版 情報通信白書より

3. オンライン更新

案1 双方向認証後、更新サーバ側で鍵ペアを生成し、暗号化してICカードまで送信する方式<実現イメージ>

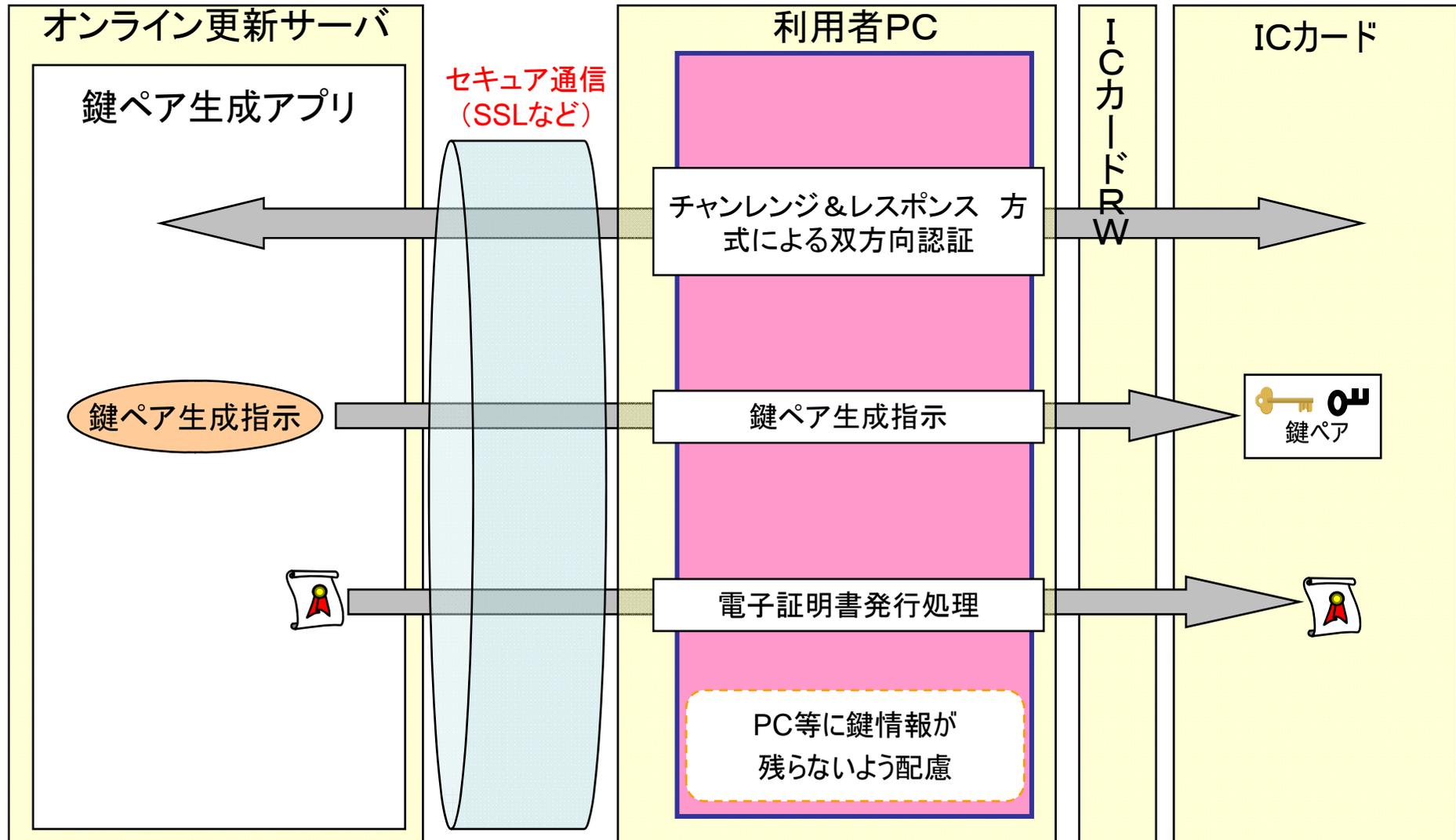
 : 利用者に配布する更新用ソフトウェア



3. オンライン更新

案2 双方向認証後、ICカード内で鍵ペアを生成する方式<実現イメージ>

 : 利用者に配布する更新用ソフトウェア



4. 有効期間の延長

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

年度	2009 H21	2010 H22	2011 H23	2012 H24	2013 H25	2014 H26	2015 H27	2016 H28	2017 H29	2018 H30	2019 H31	2020 H32	...	
SHA-1の安全性評価								*1						
RSA1024の安全性評価								*2						
政府機関の情報システム						*4	*5							
電子署名法	*6						*7	*8						
公的個人認証サービス						*9	*10			*11				
公的個人認証サービス センターシステム		*12												
鍵ペア生成装置														
住民基本台帳カード			*14											

出典:「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報告会」報告書
(平成21年1月26日)

4. 有効期間の延長

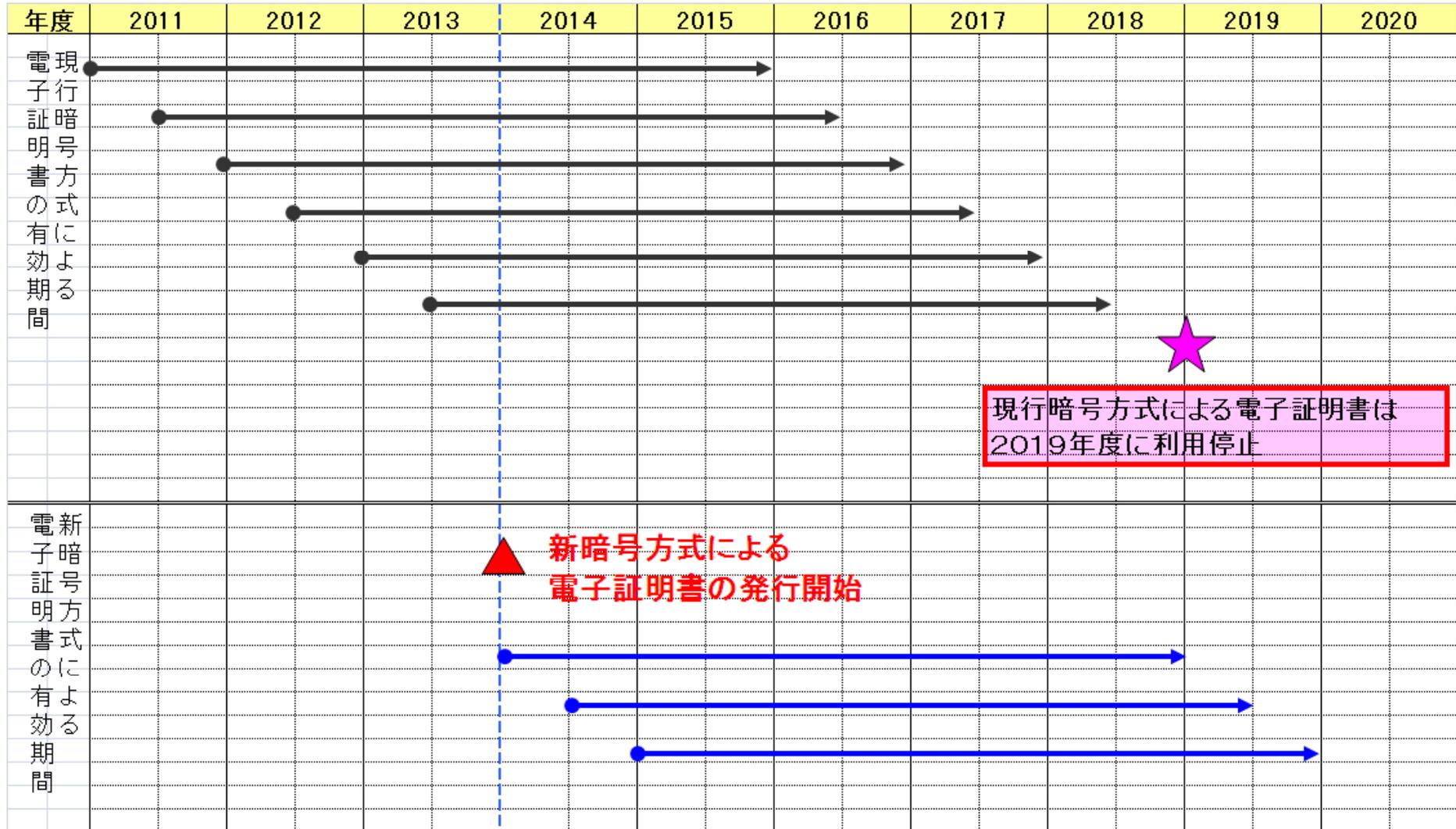
公的個人認証サービスにおける 暗号アルゴリズムの移行スケジュール（注釈）

*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。

出典:「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報告会」報告書
(平成21年1月26日)

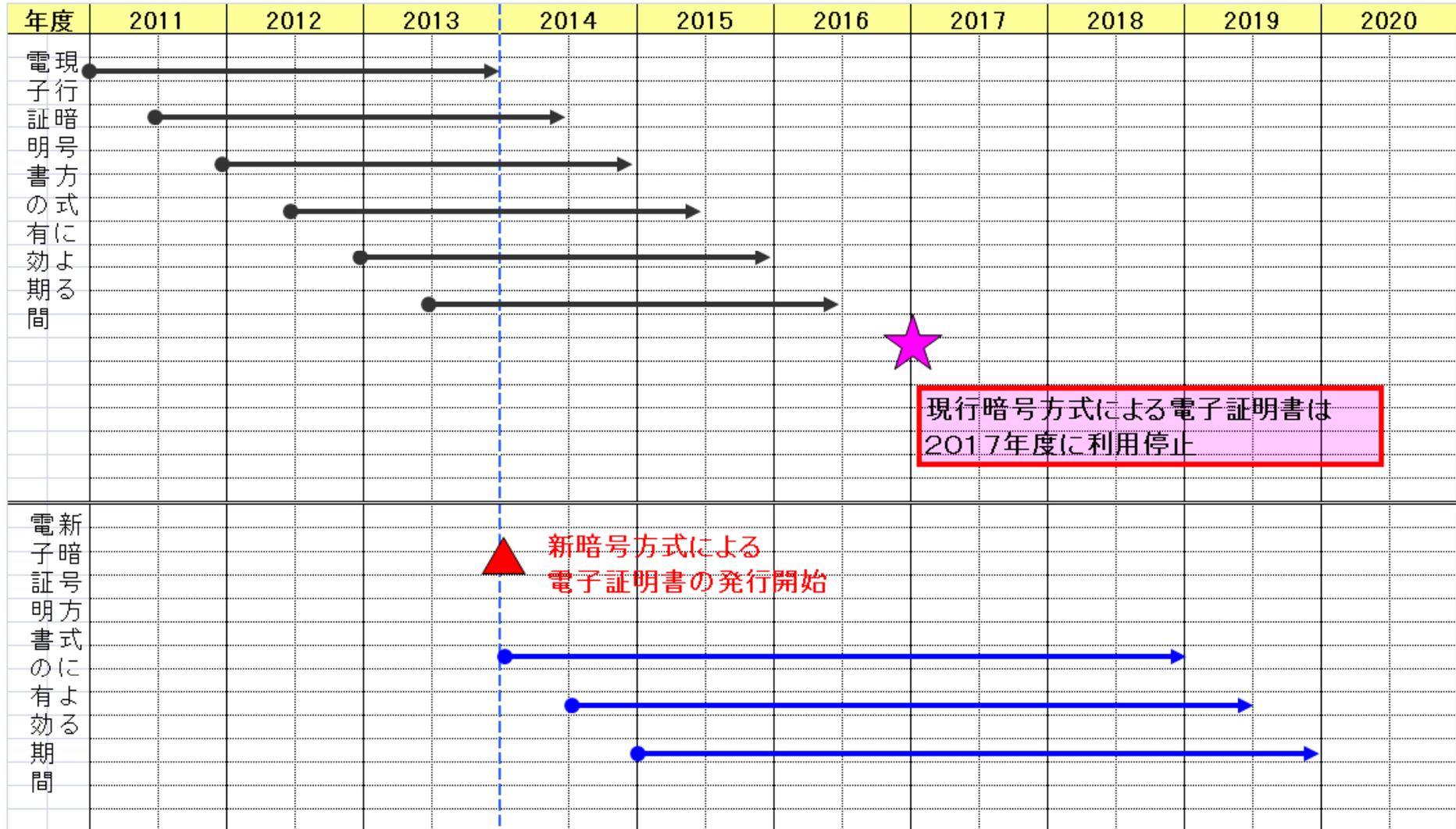
4. 有効期間の延長

案1 <実現イメージ>



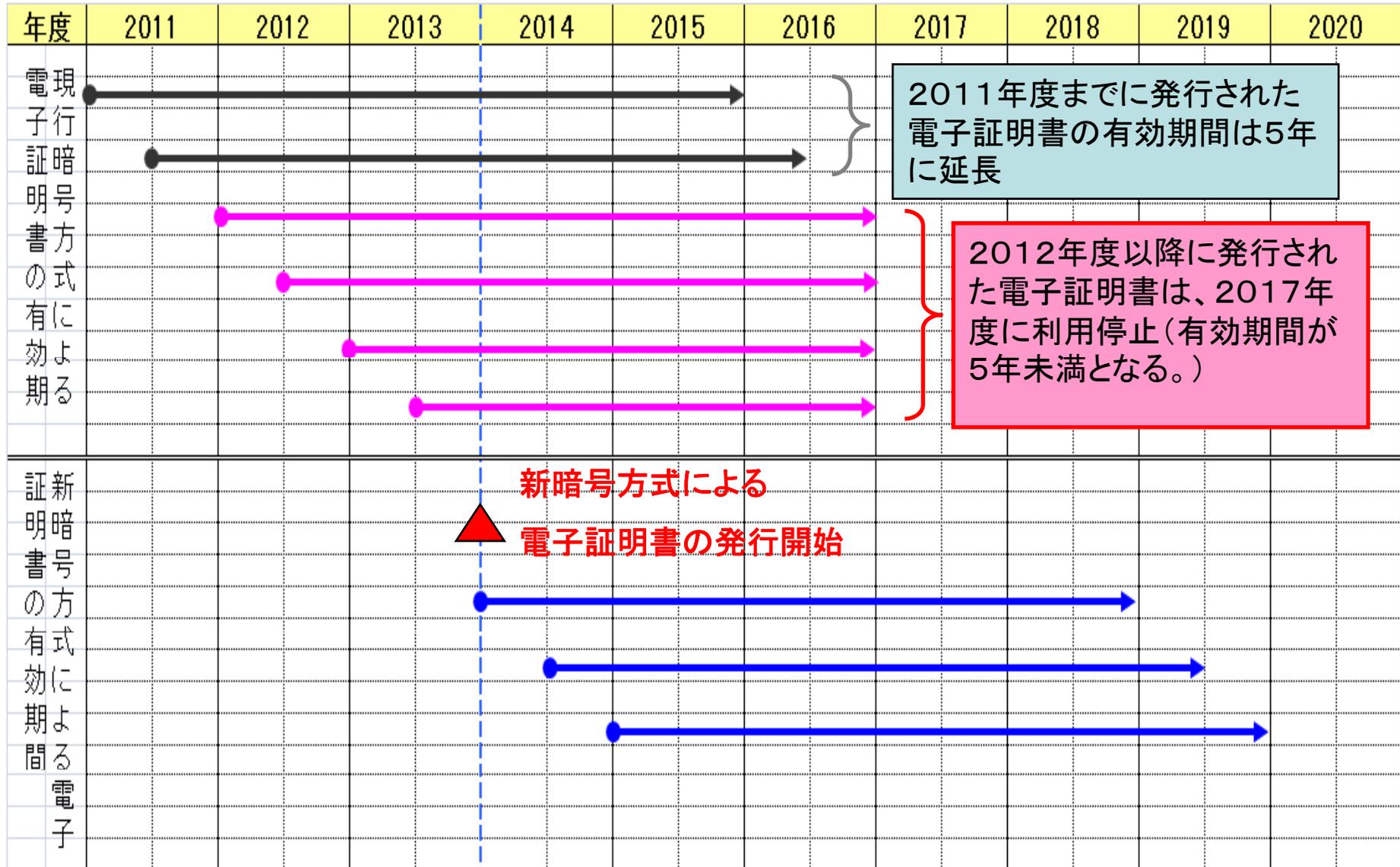
4. 有効期間の延長

案2 <実現イメージ>



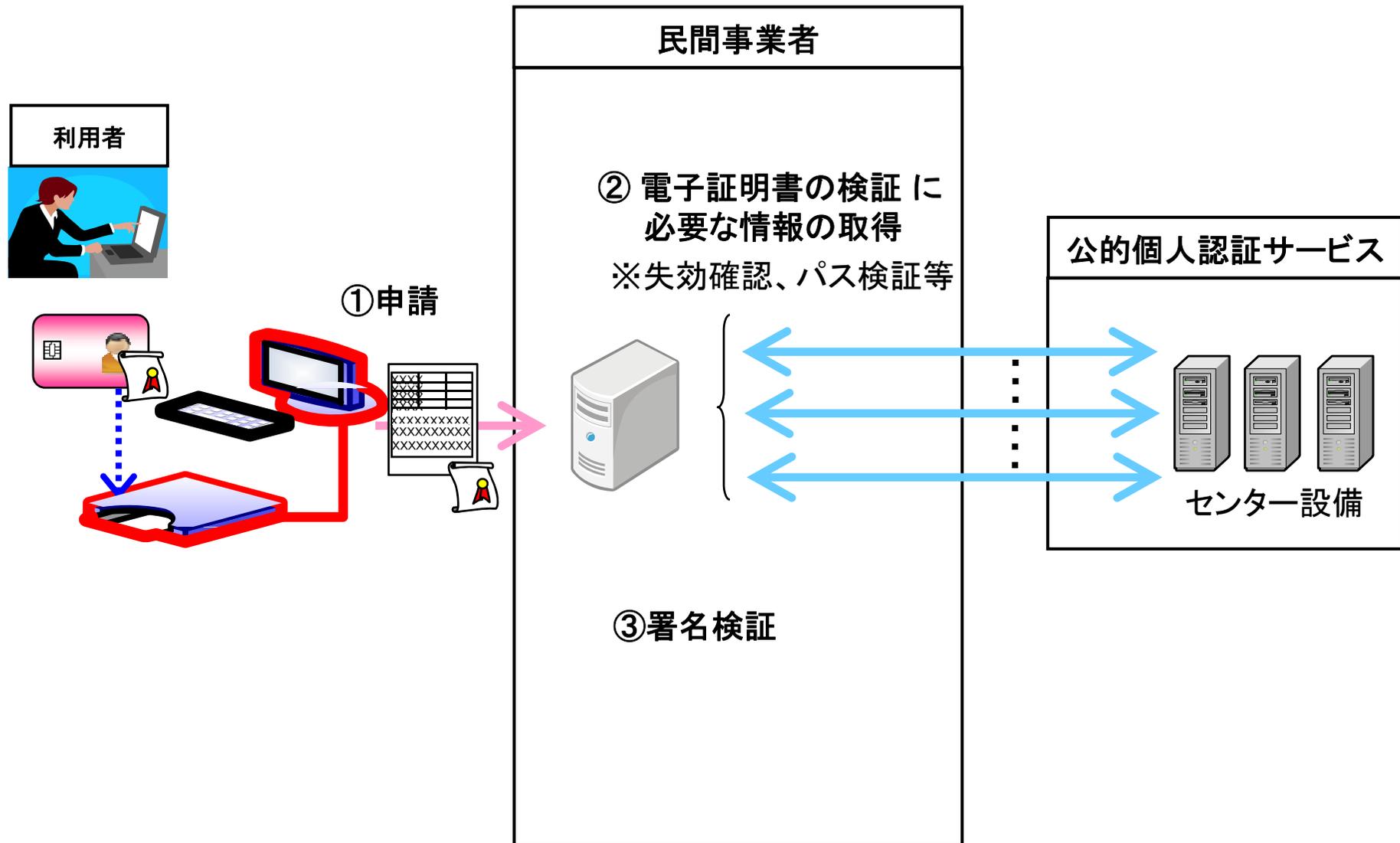
4. 有効期間の延長

方向性<実現イメージ>



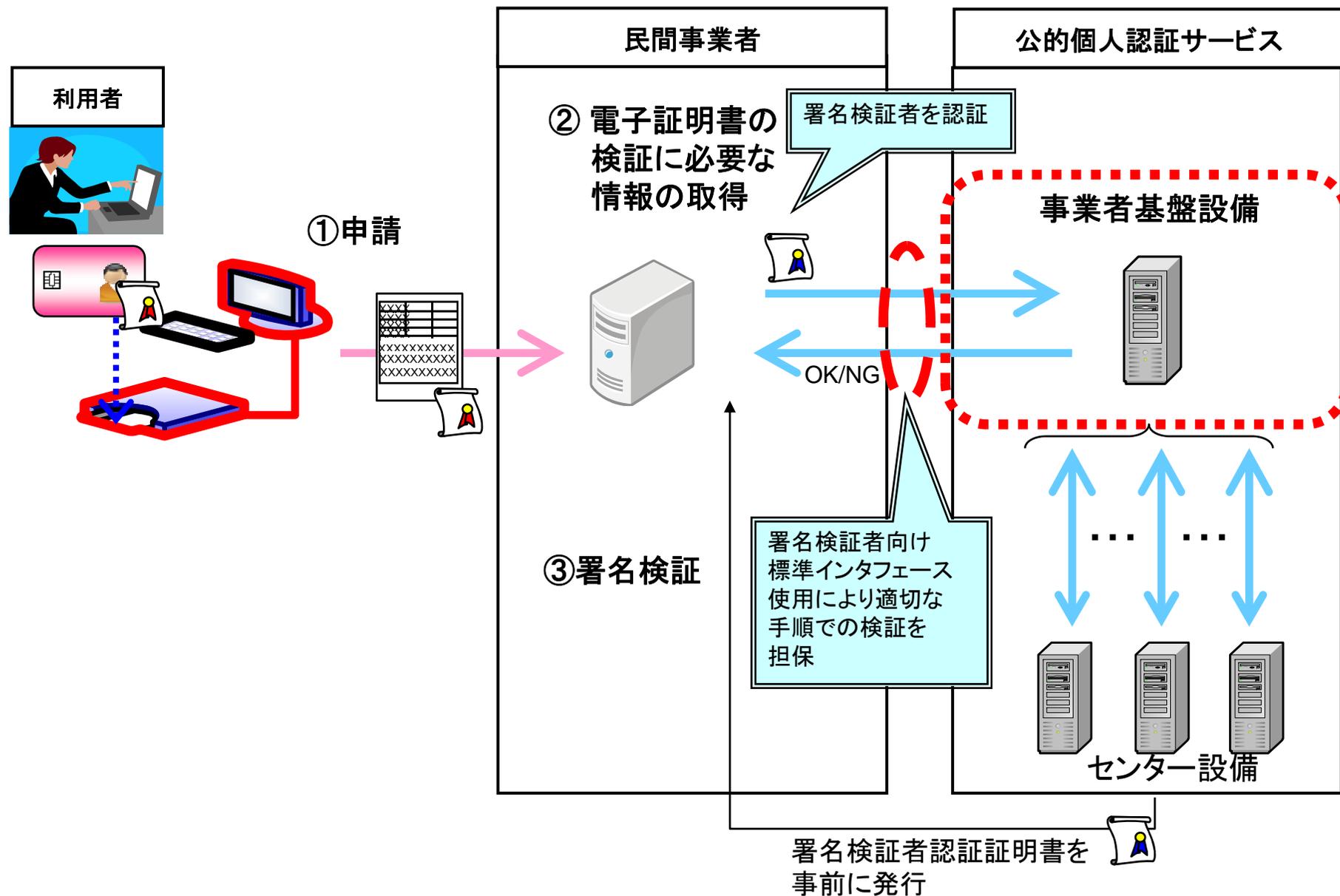
5. 署名検証者の拡大(民間事業者への拡大)

案1 署名検証に必要な設備は民間事業者において整備<実現イメージ>



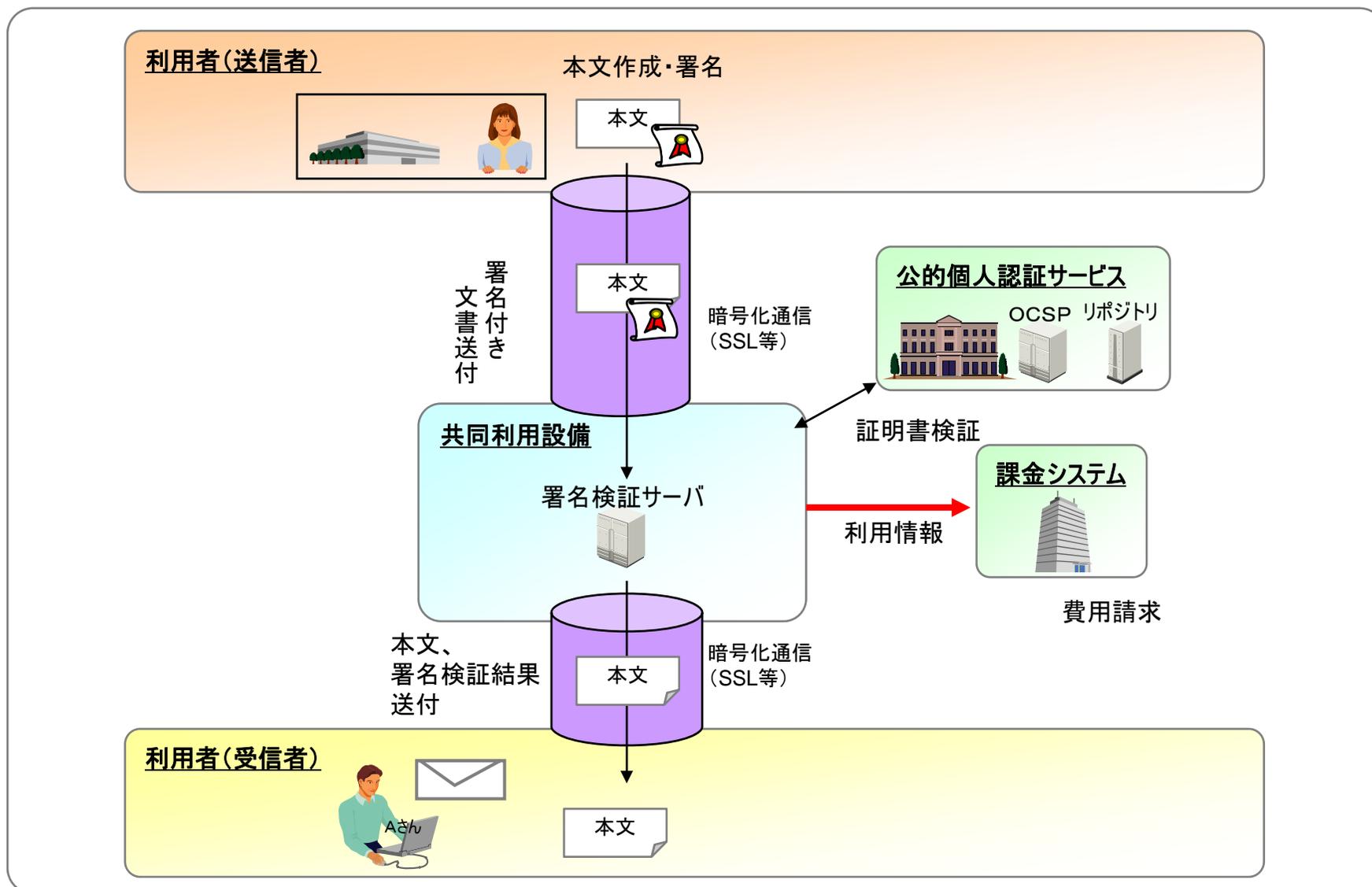
5. 署名検証者の拡大(民間事業者への拡大)

案2 事業者基盤設備を整備し、民間事業者に必要なサービスを提供<実現イメージ>



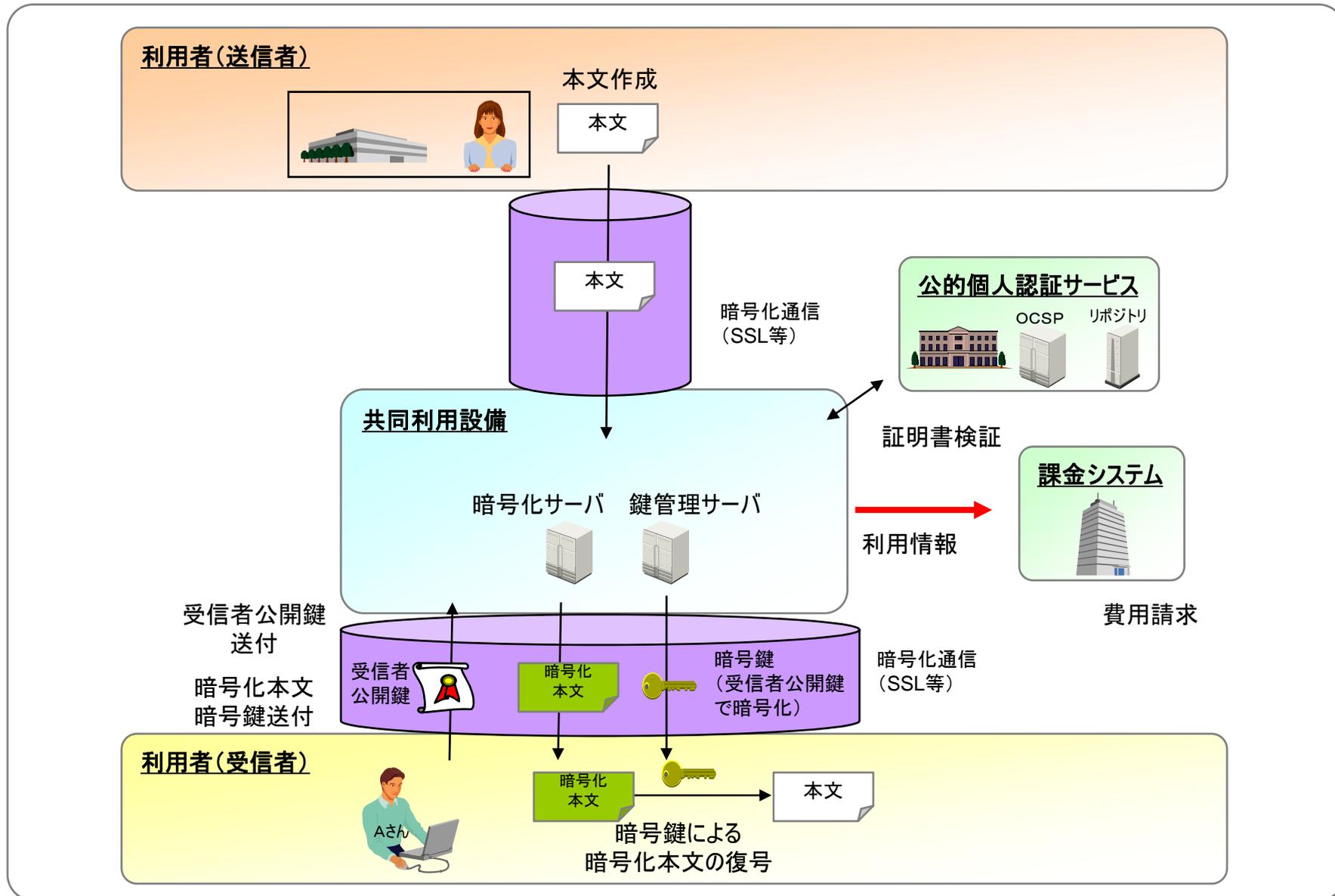
6. 利用用途の拡大(署名メール及び暗号メール)

案 署名メール(共同利用設備を設置し、必要なサービスを提供) <実現イメージ>



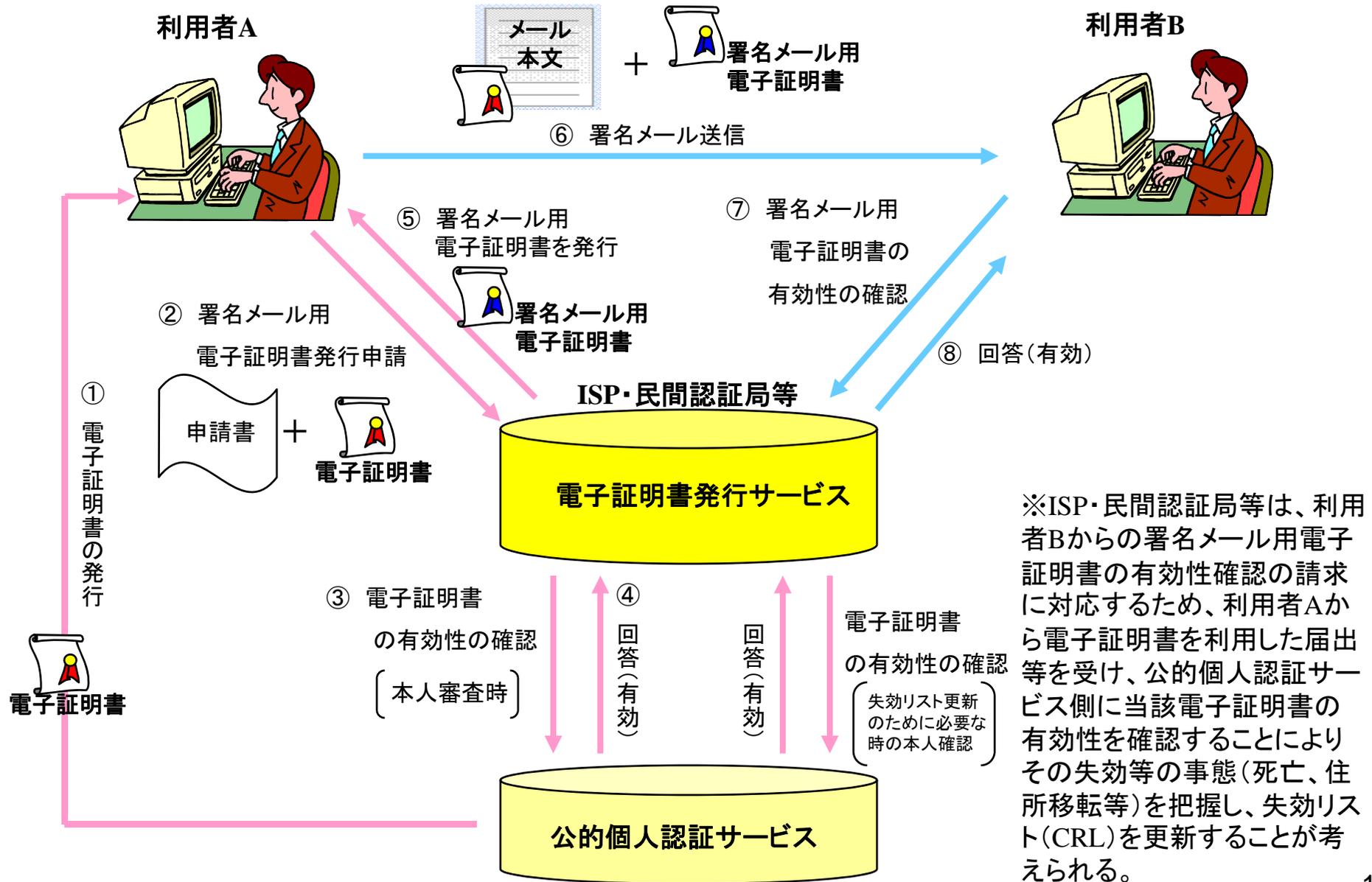
6. 利用用途の拡大(署名メール及び暗号メール)

案 暗号メール(共同利用設備を設置し、必要なサービスを提供) <実現イメージ>



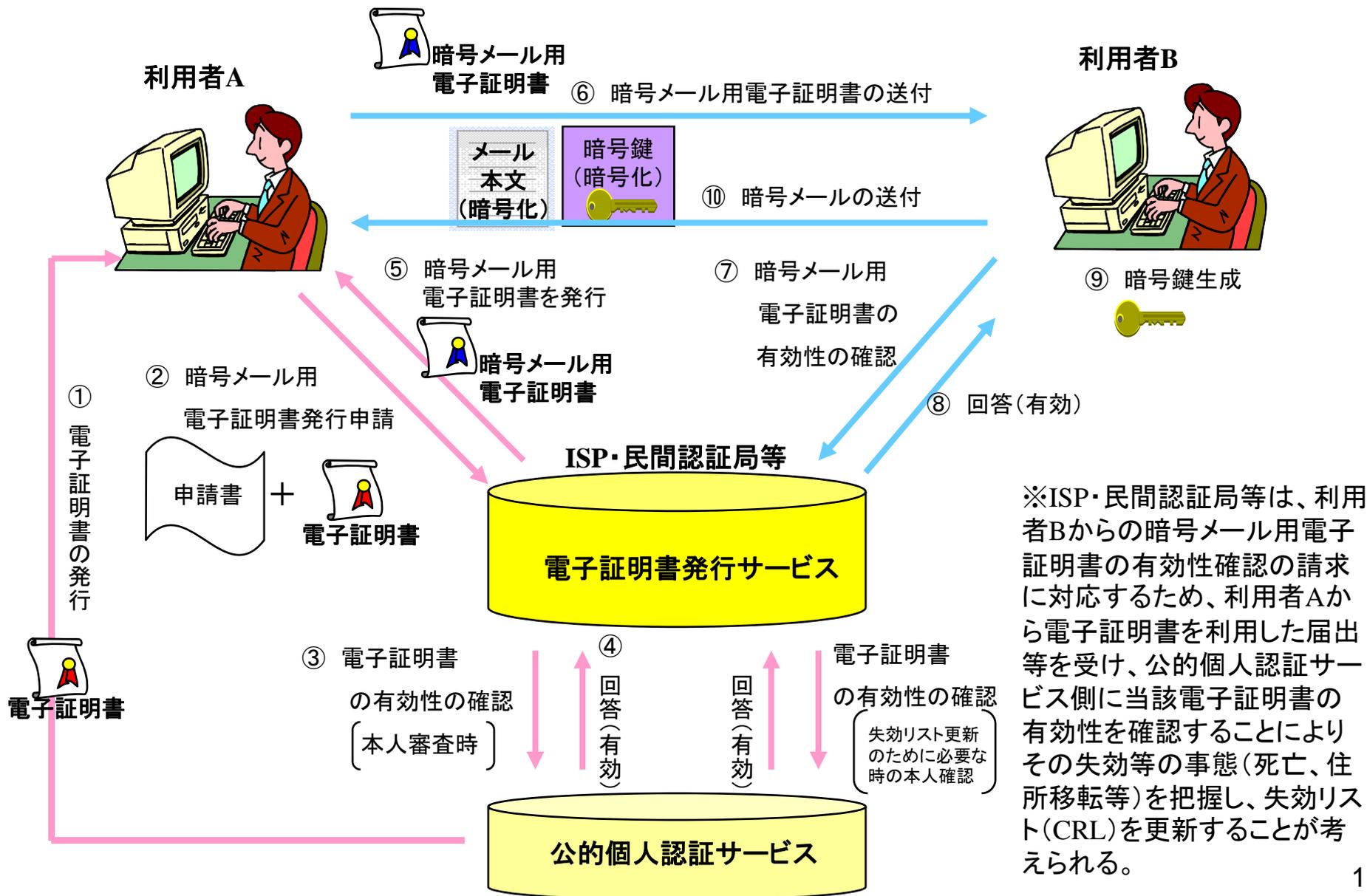
6. 利用用途の拡大(署名メール及び暗号メール)

ISP等が公的個人認証サービスを利用して署名メール用の電子証明書を発行<実現イメージ>



6. 利用用途の拡大(署名メール及び暗号メール)

ISP等が公的個人認証サービスを利用して暗号メール用の電子証明書を発行<実現イメージ>



※ISP・民間認証局等は、利用者Bからの暗号メール用電子証明書の有効性確認の請求に対応するため、利用者Aから電子証明書を利用した届出等を受け、公的個人認証サービス側に当該電子証明書の有効性を確認することによりその失効等の事態(死亡、住所移転等)を把握し、失効リスト(CRL)を更新することが考えられる。