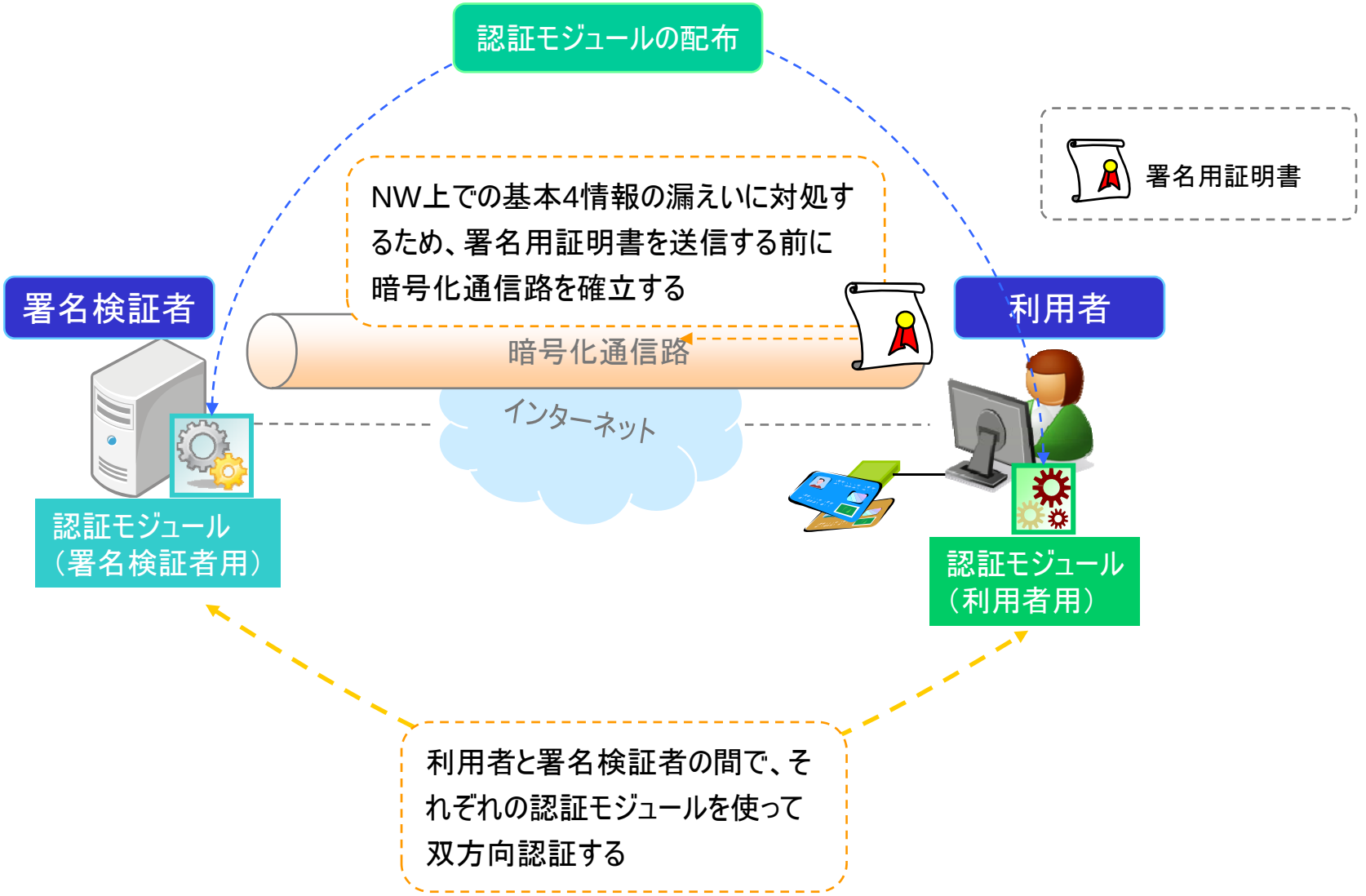
参考資料

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する ＜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する。＜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
・有効期間延長実現の方向性＜実現イメージ＞ ･･8
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準備する＜実現イメージ＞･･････････････････････････････9
・案２ 事業者基盤を整備し、民間事業者に必要なサービスを提供するイメージ＜実現イメージ＞･･････････････10
６. 利用用途の拡大（署名メール及び暗号メール）
・署名メール 個人を署名検証者にしない仕組み（共同利用設備）＜実現イメージ＞･････････････････････････11
・暗号メール 個人を署名検証者にしない仕組み（共同利用設備）＜実現イメージ＞･････････････････････････12

1. 認証用途の付加

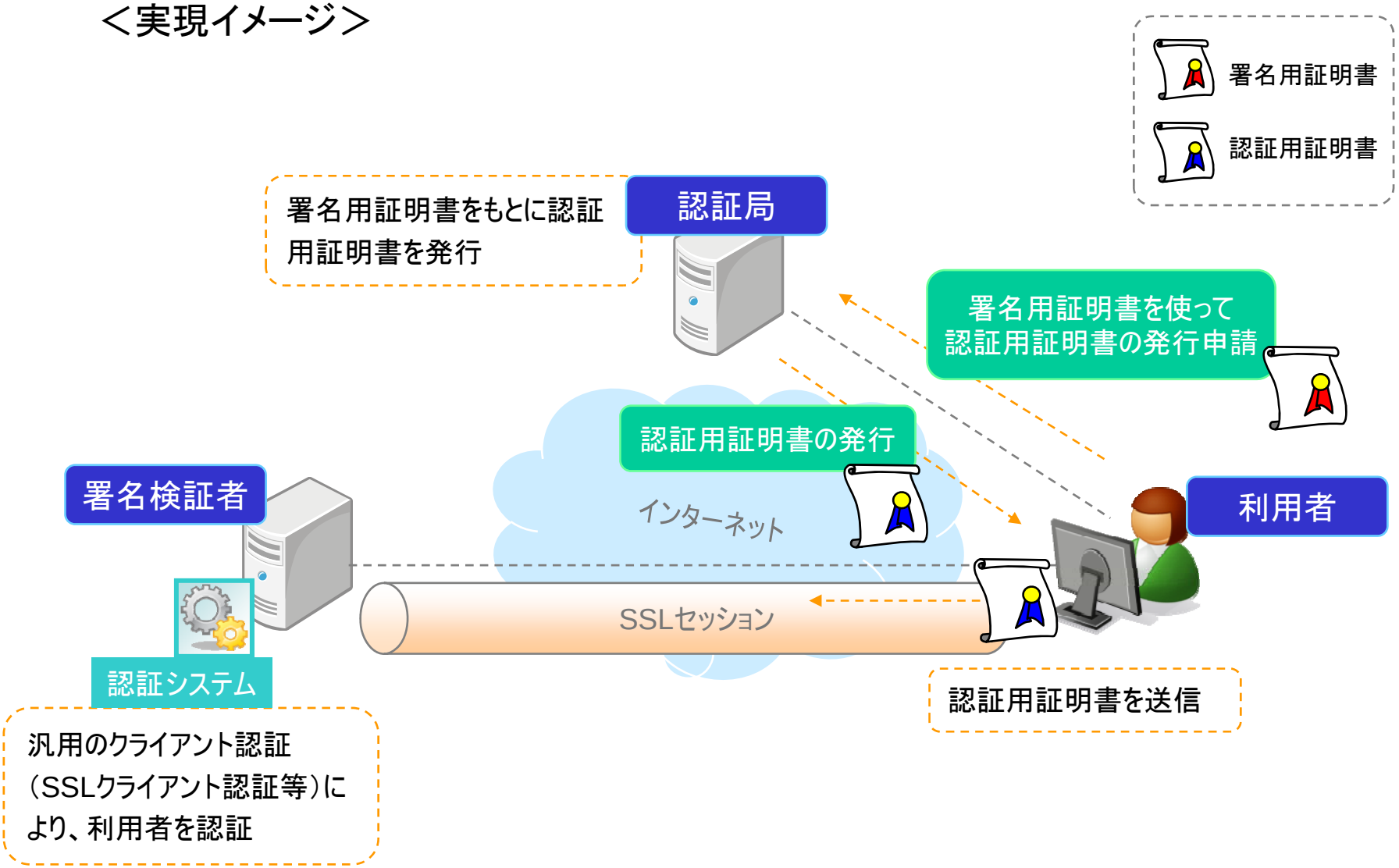
案1：現行証明書を認証用として併用する　＜実現イメージ＞



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する。

＜実現イメージ＞



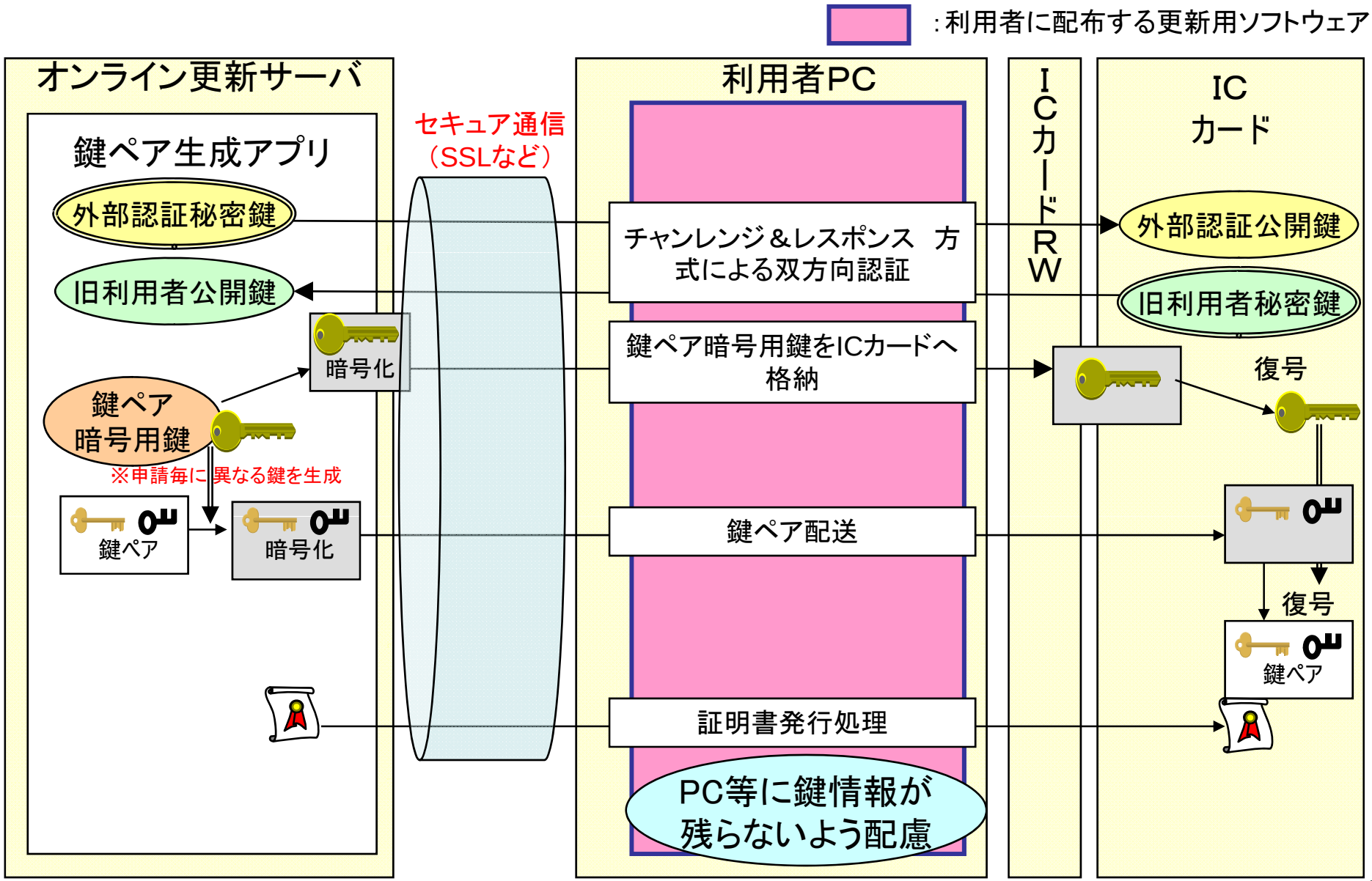
２．記録媒体の拡大

記録媒体	発行枚数等	備考
フェリカ対応交通カード （Suica及びPASMO）	４，００３万枚	・2009年4月5日時点 ・東日本旅客鉄道株式会社、 PASMO協議会、株式会社パスモ 発表資料（2009年4月23日）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

※「Suica」は東日本旅客鉄道株式会社の登録商標です
※「PASMO」は株式会社パスモの登録商標です

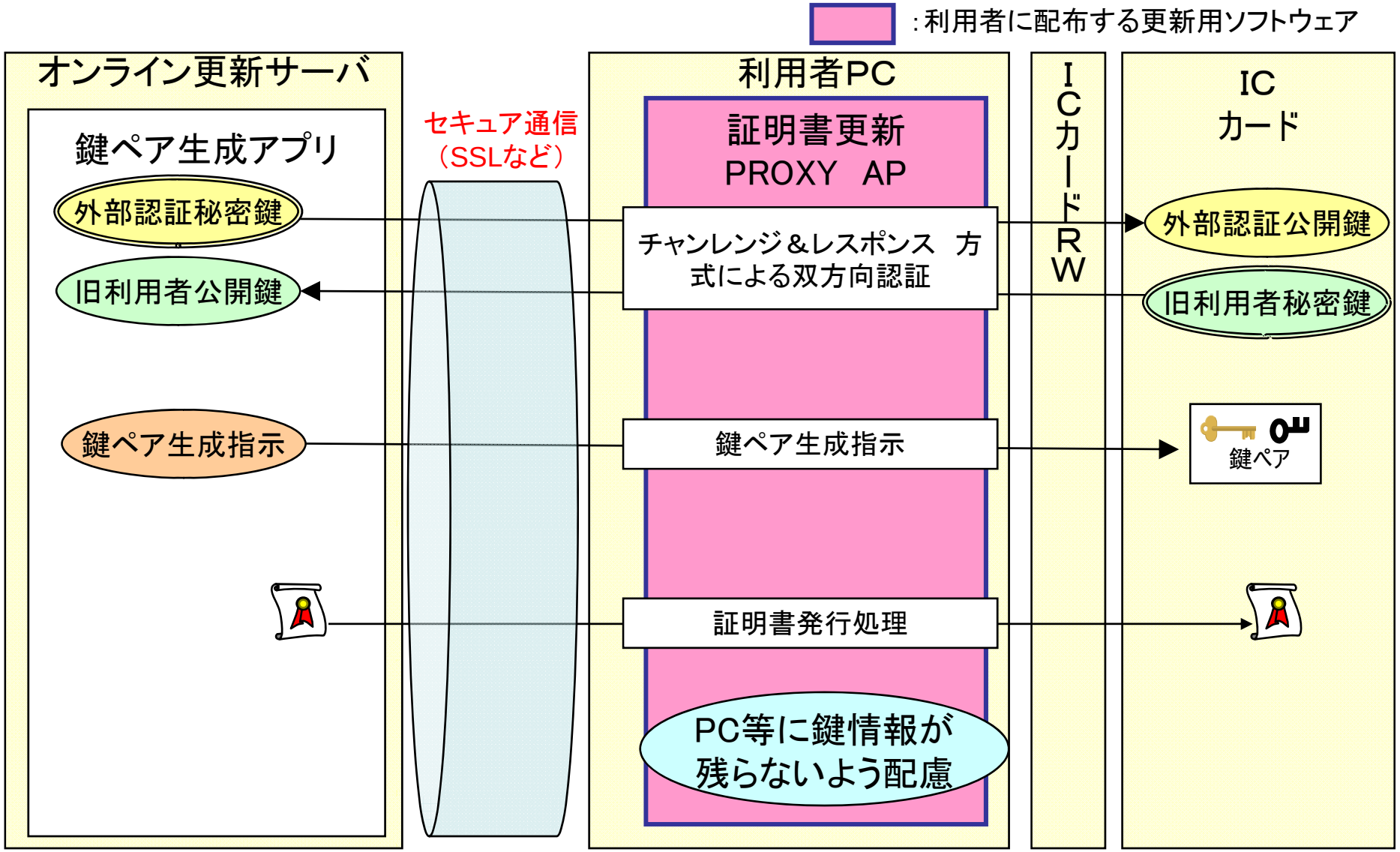
3. オンライン更新

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＞



3. オンライン更新

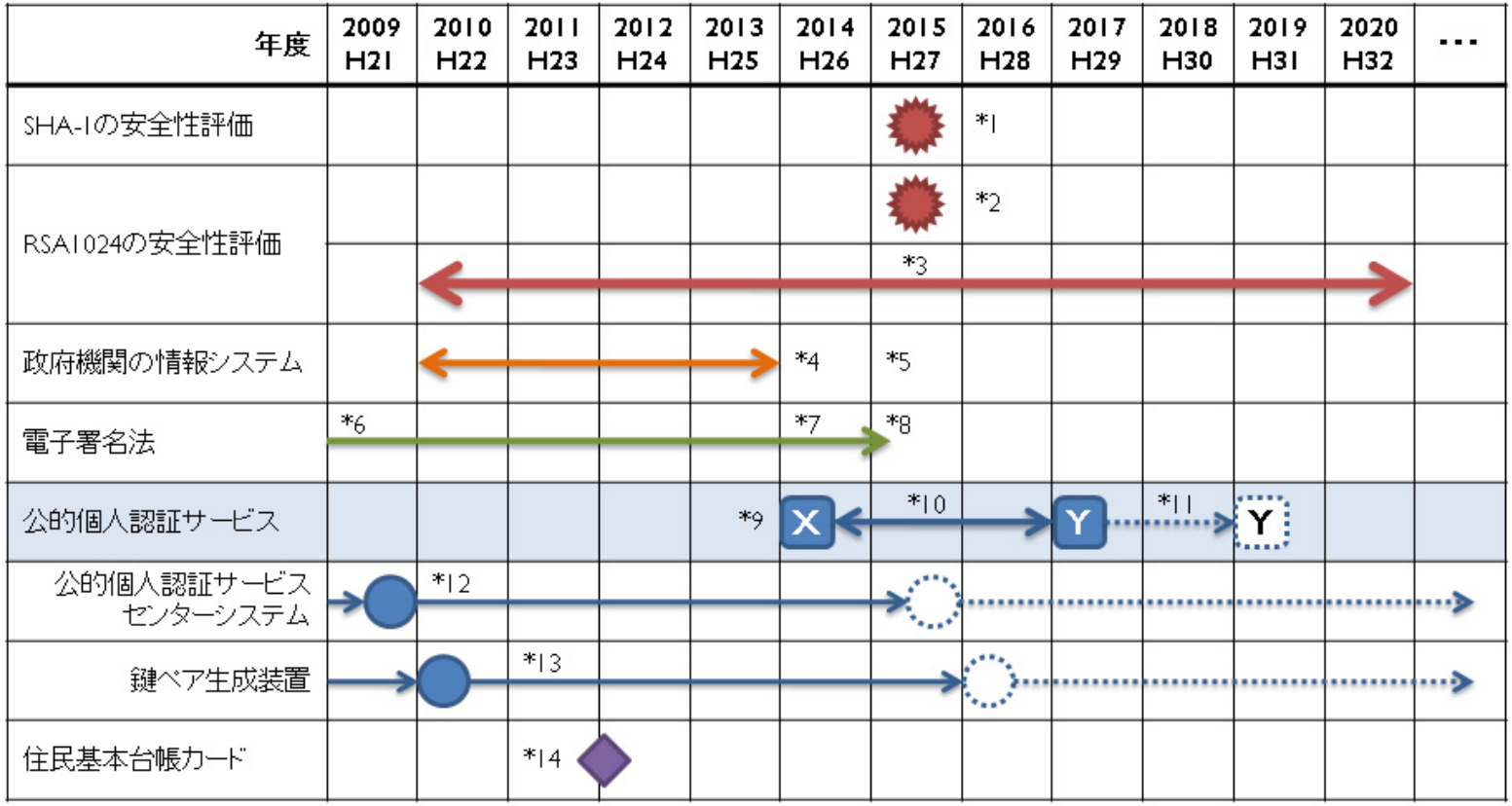
案2　双方向認証後、ICカード内で鍵ペアを生成する方式＜実現イメージ＞



※既存の住基カードでは実現が困難（ICカード内で鍵ペア生成機能を仕様追加する必要がある）
※ICカード内で鍵ペアを生成するのに要する時間はサーバ等で生成する時間に比べて長い。（2～4分程度：ばらつき有（最大7分））

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



出展:「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

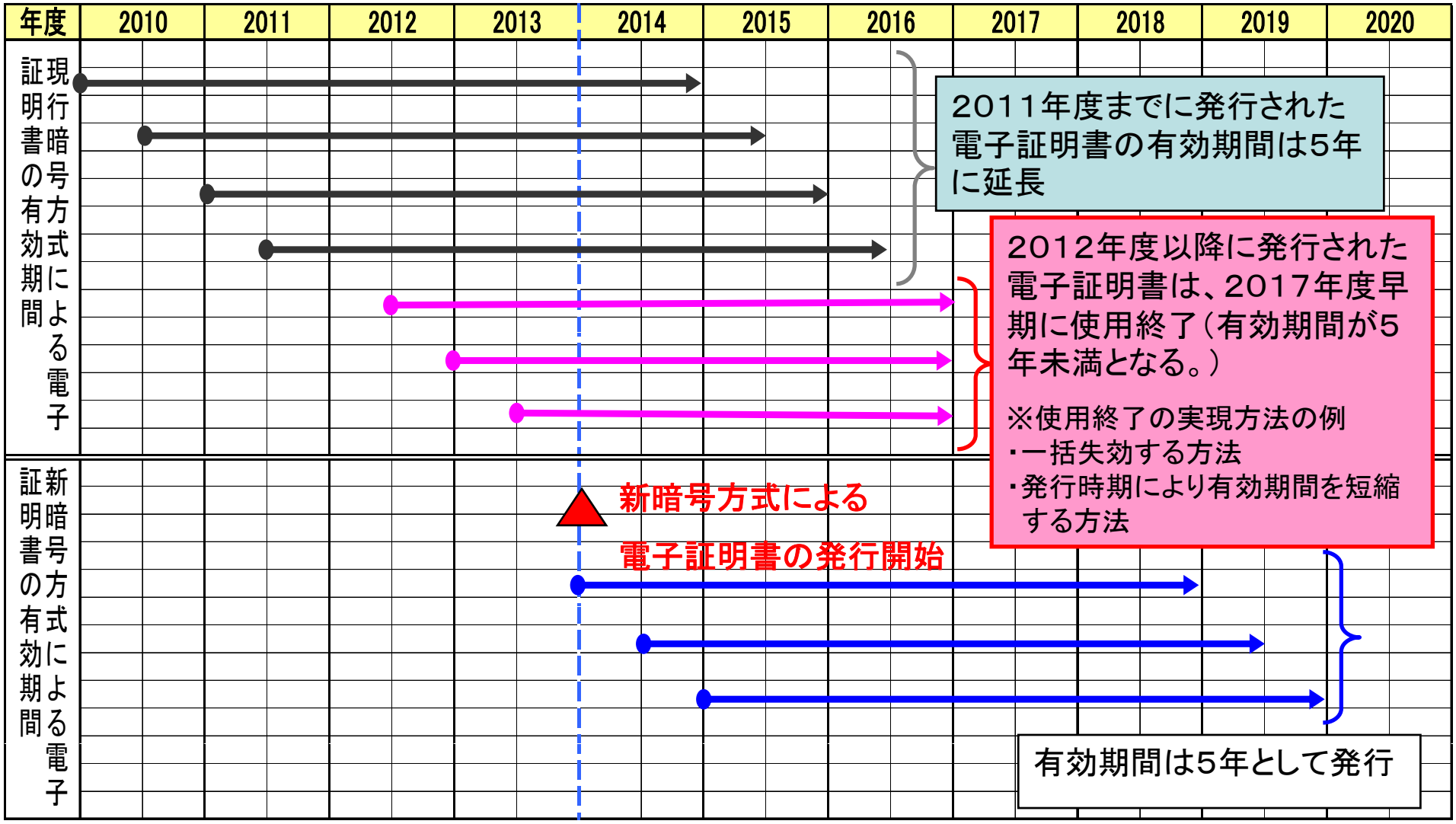
公的個人認証サービスにおける暗号アルゴリズムの移行スケジュール（注釈）

*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。

出展：「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

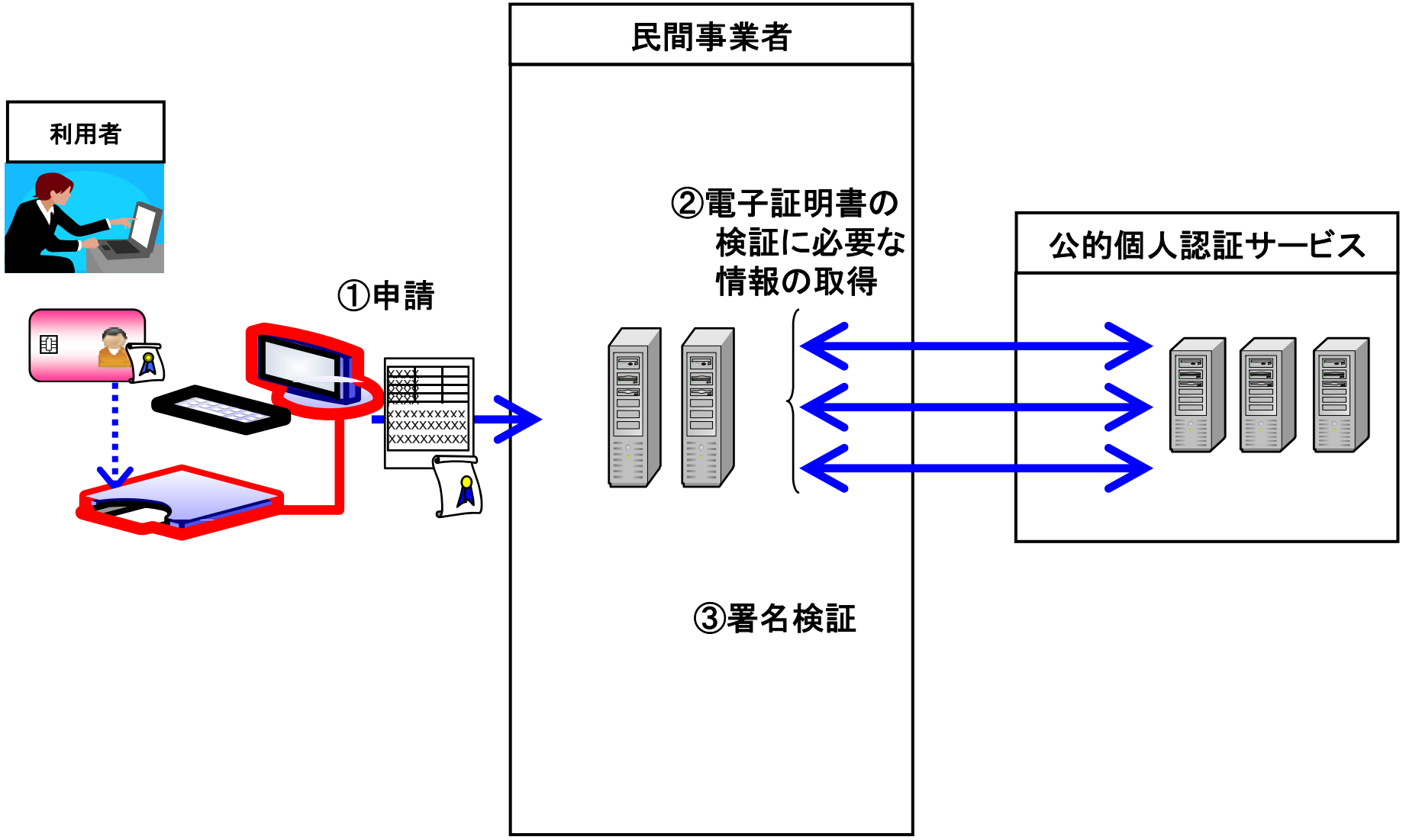
有効期間延長実現の方向性＜実現イメージ＞



※2010年度当初より有効期間が5年に延長された場合を想定

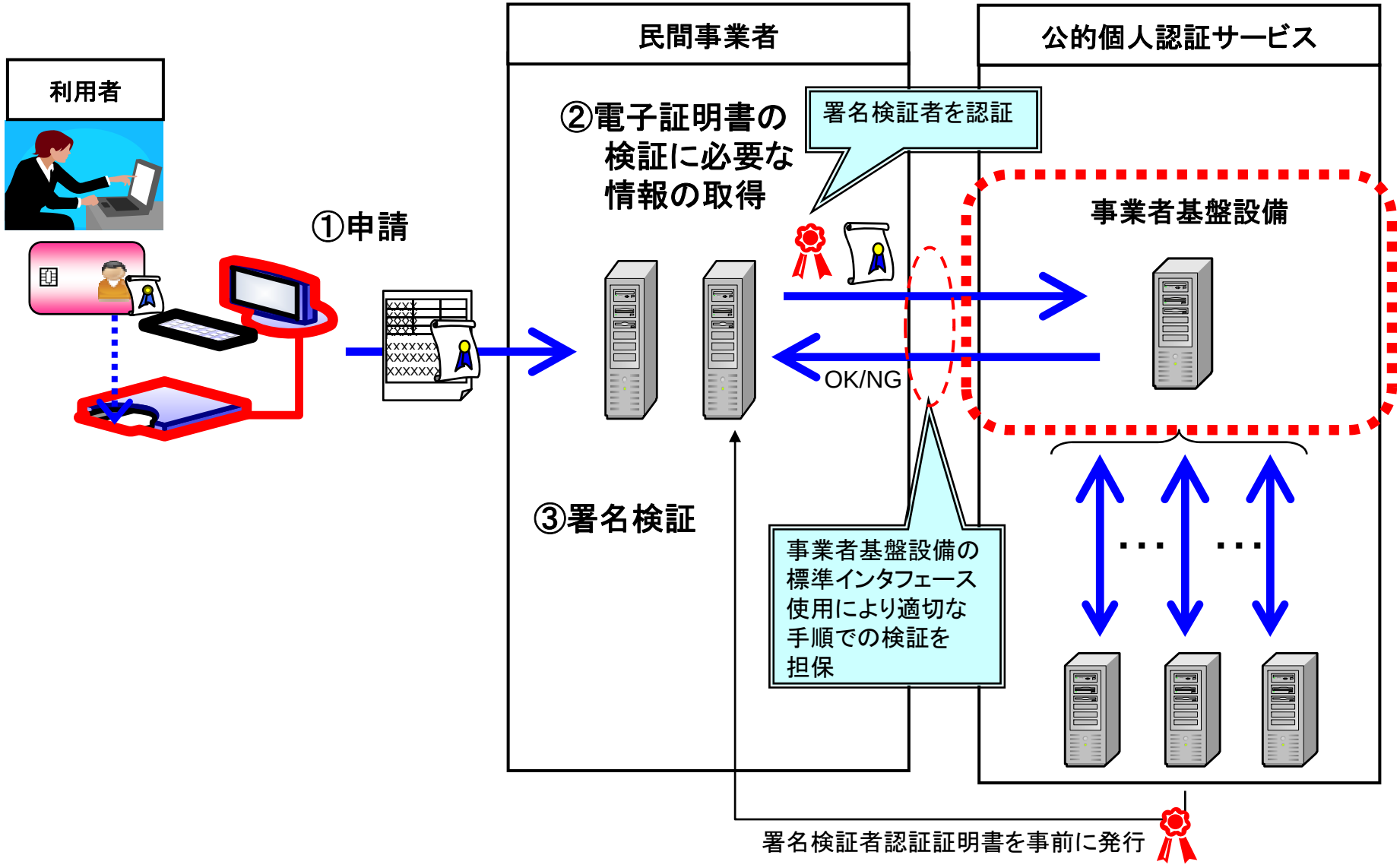
５．署名検証者の拡大（民間事業者への拡大）

案１　署名検証に必要な設備は民間事業者において準備する＜実現イメージ＞



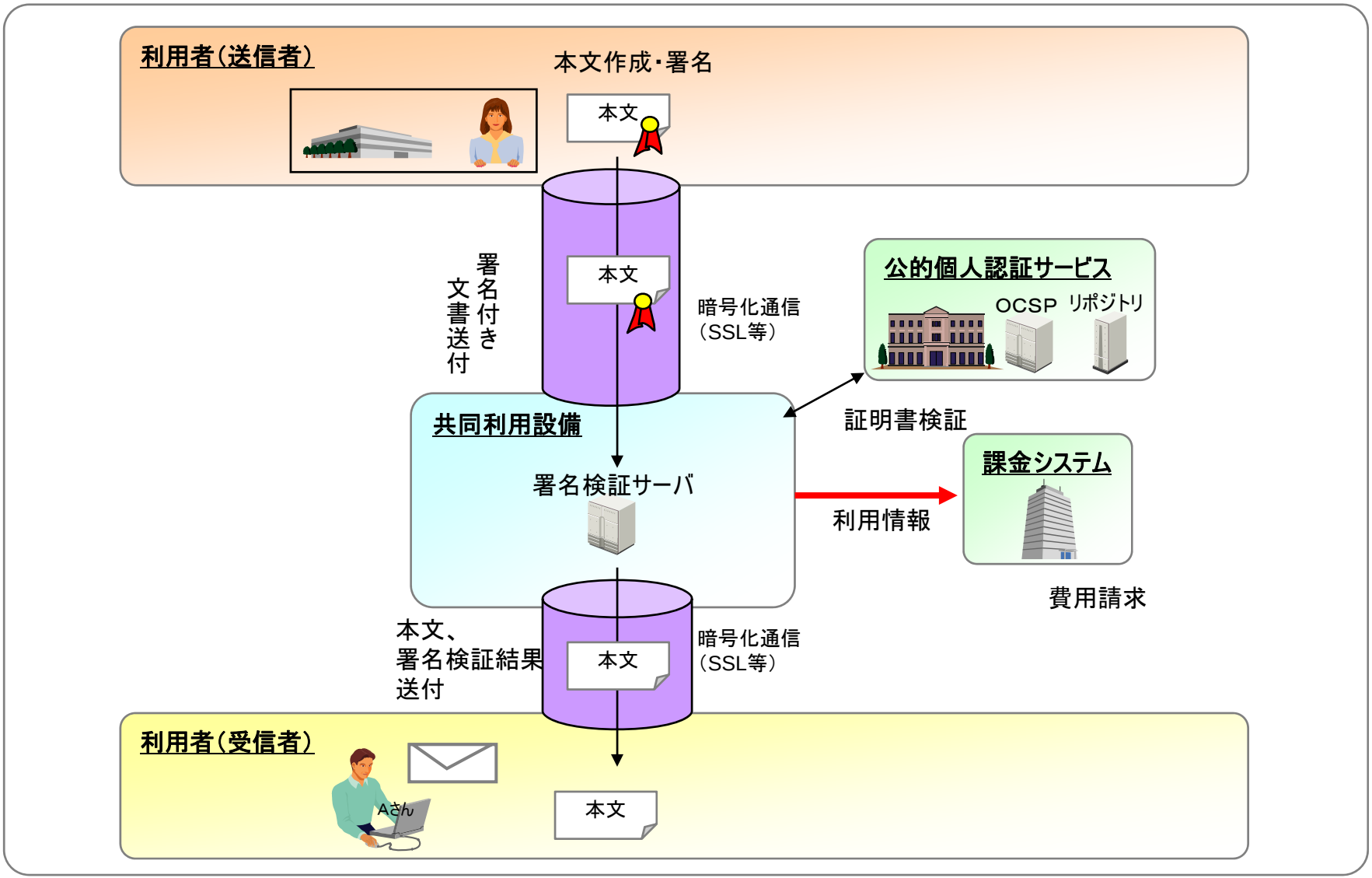
5. 署名検証者の拡大（民間事業者への拡大）

案2　事業者基盤を整備し、民間事業者に必要なサービスを提供する＜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）

署名メール　個人を署名検証者にしない仕組み（共同利用設備）＜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）

暗号メール　個人を署名検証者にしない仕組み（共同利用設備）＜実現イメージ＞