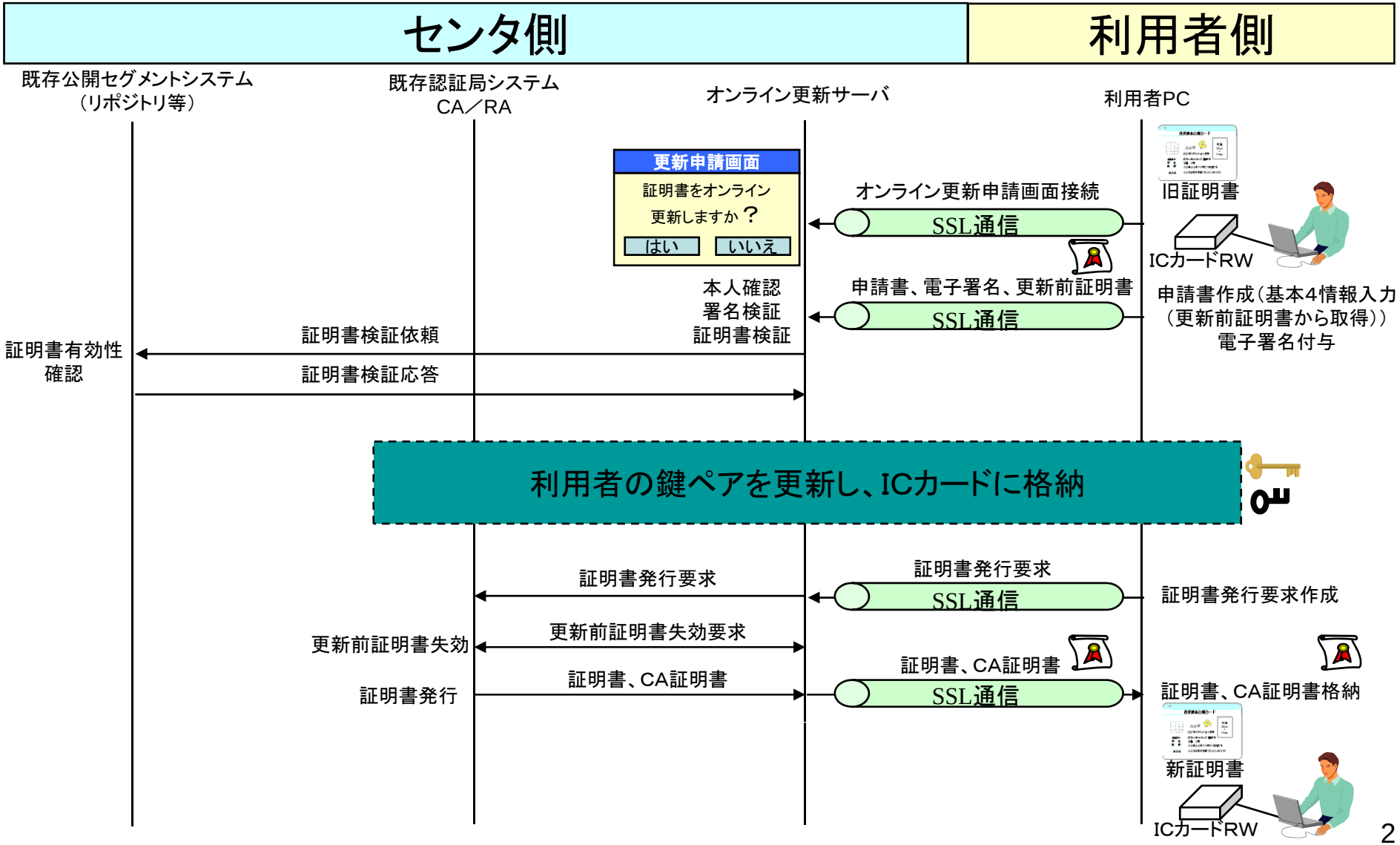
資料3

参考資料

目次

①【利便性の向上】オンライン更新

オンライン更新の流れ

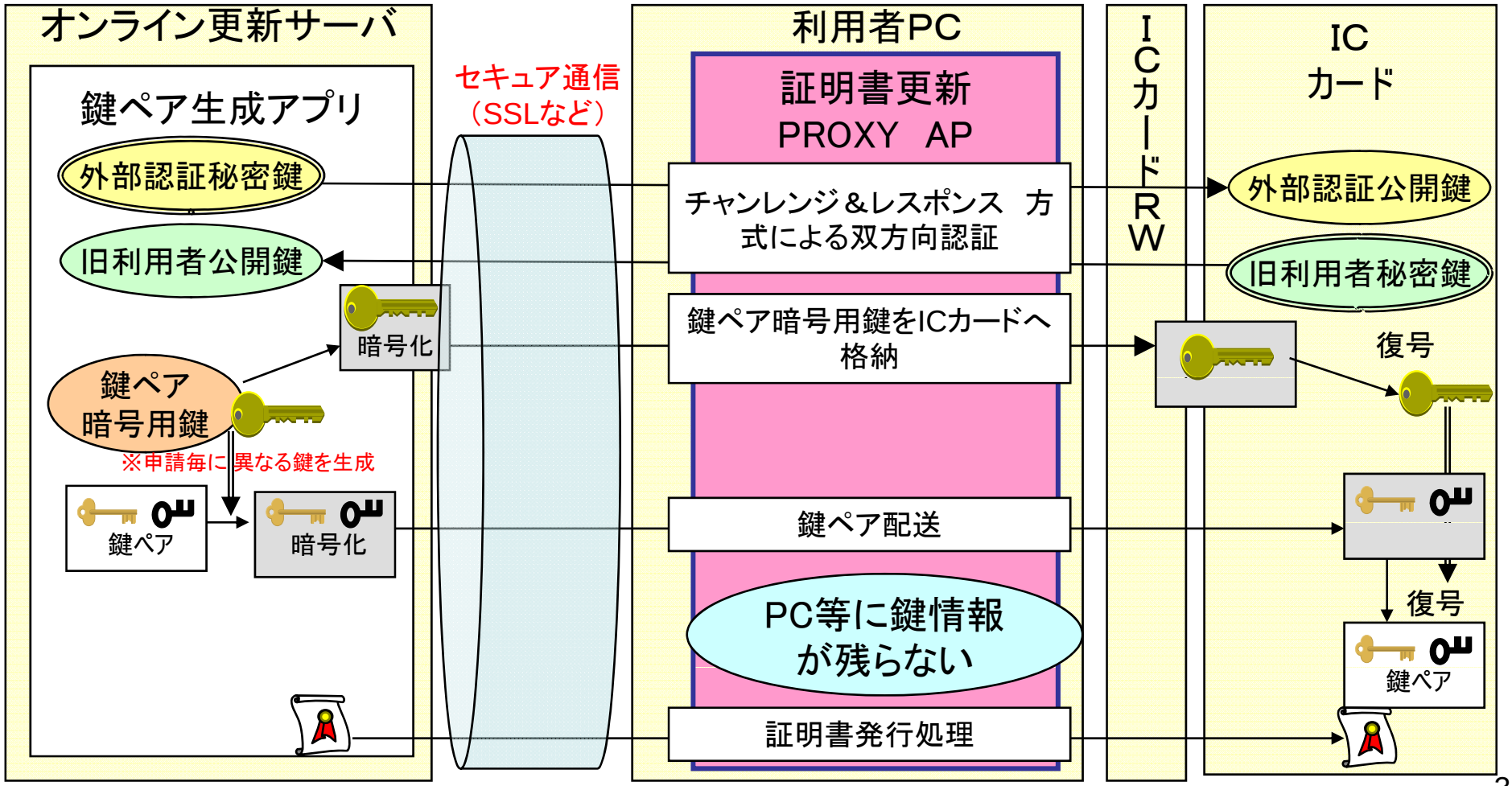


①【利便性の向上】オンライン更新

案1　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

(1)鍵ペア生成アプリの外部認証鍵ペア／旧利用者鍵ペアを使って、双方向認証を行い、ICカードに書込む準備を行う。
(2)鍵ペア暗号用鍵を旧利用者公開鍵を用いて暗号化後、利用者PCに送付し、ICカードに格納する。
(3)新しい利用者の鍵ペアを生成した後、鍵ペア暗号用鍵を使って暗号化する。
(4)暗号化された鍵ペアを利用者PCを通じてICカードに送付する。
(5)ICカード内で鍵ペア暗号用鍵を使って新しい鍵ペアの復号を行う。
(6)新利用者公開鍵に対して証明書発行処理を行う。

：利用者がインストールするモジュール

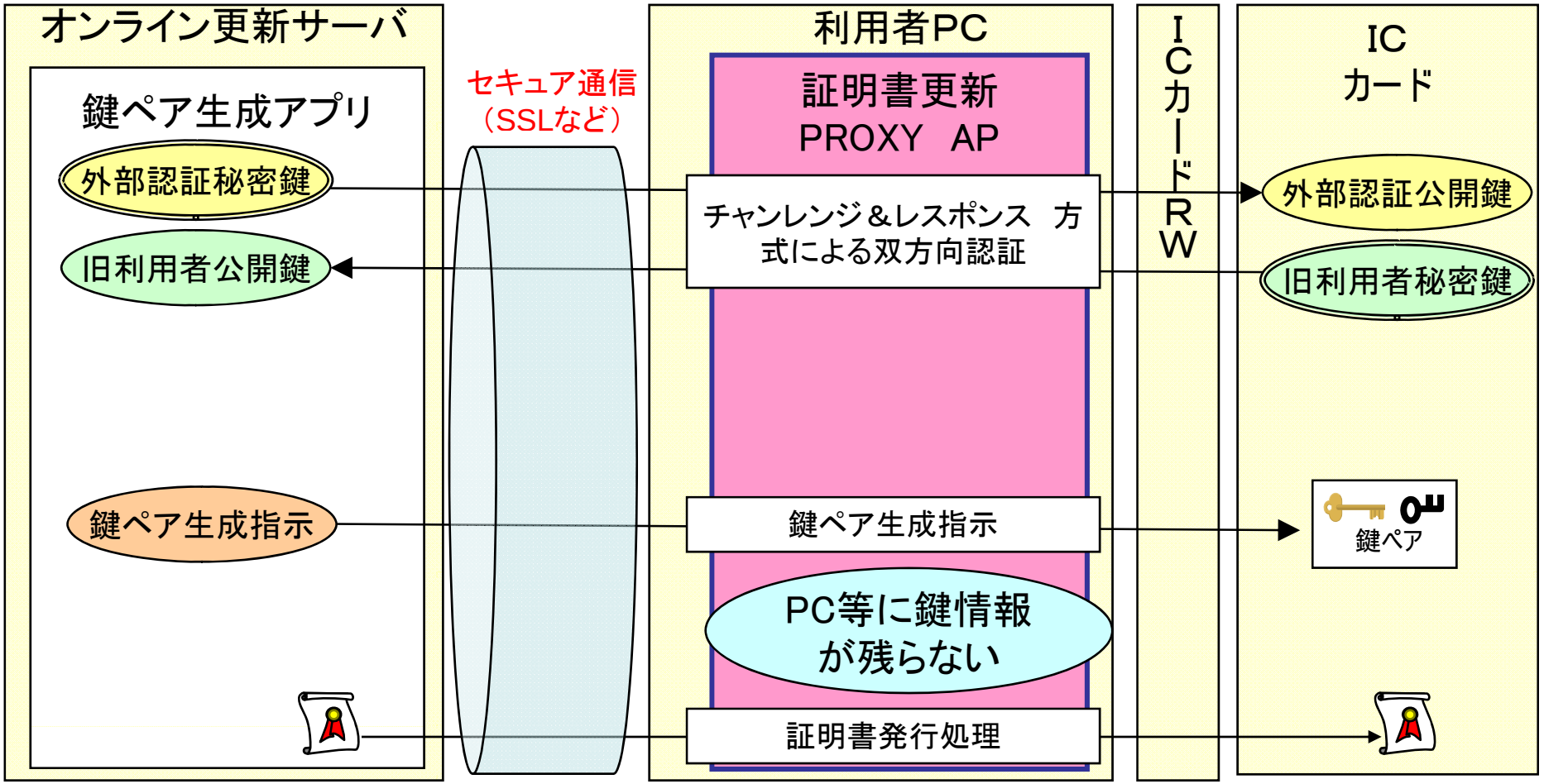


①【利便性の向上】オンライン更新

案2　ICカードで鍵ペアを生成する方式

(1)鍵ペア生成アプリの外部認証鍵ペア／旧利用者鍵ペアを使って、双方向認証を行い、鍵ペア生成指示をICカードに送信する準備を行う。
(2)鍵ペア生成指示を利用者PCを経由し、ICカードに送信する。
(3)ICカード内で鍵ペアを生成する。
(4)新利用者公開鍵に対して証明書発行処理を行う。

：利用者がインストールするモジュール



※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））

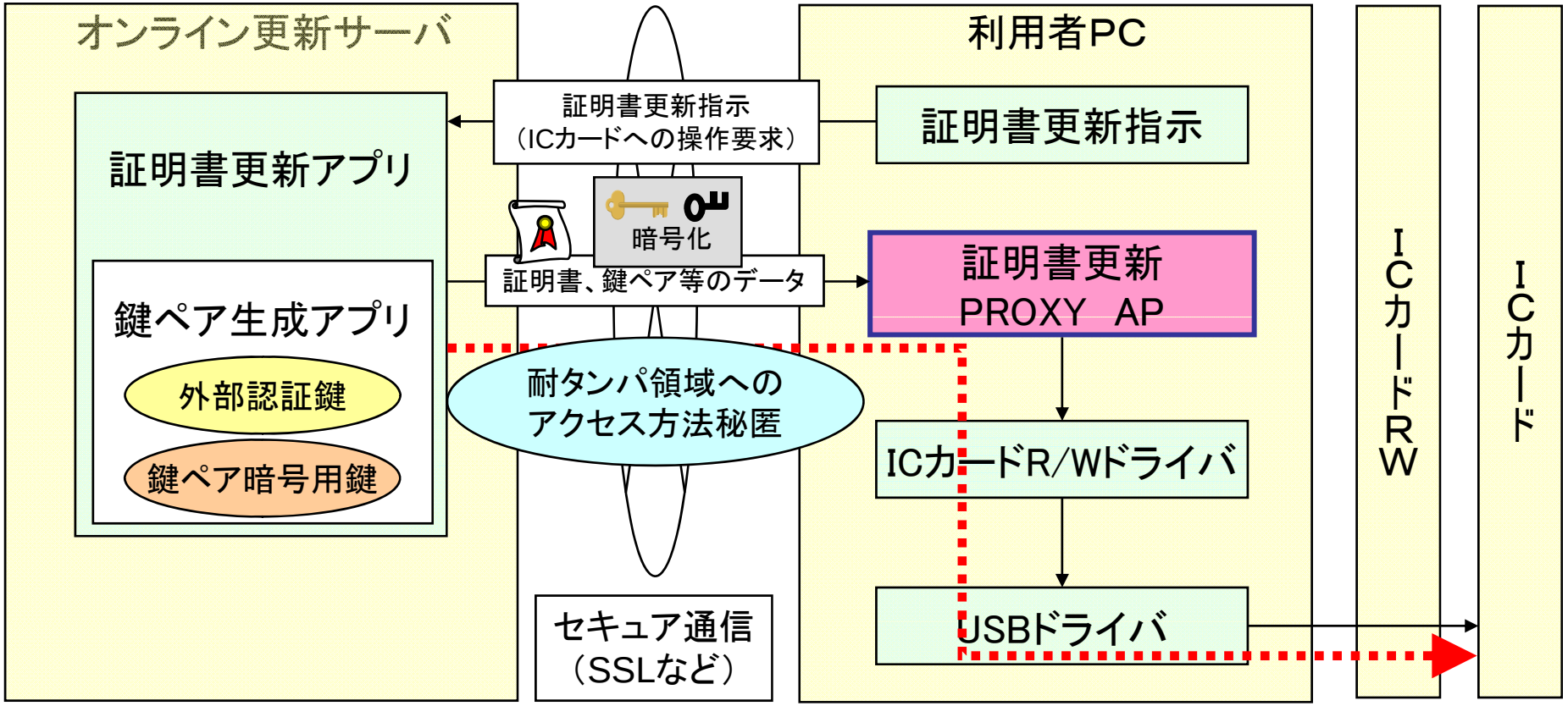
①【利便性の向上】オンライン更新

●「ICカードの耐タンパ領域へのアクセス方法を秘匿する」方式

通信経路を暗号化した上で、ICカードの耐タンパ領域への書き込み指示をサーバ側のみ行う

利用者PCに外部認証鍵を持たせずにサーバで発行した証明書や生成した鍵ペアをICカードに書込む。

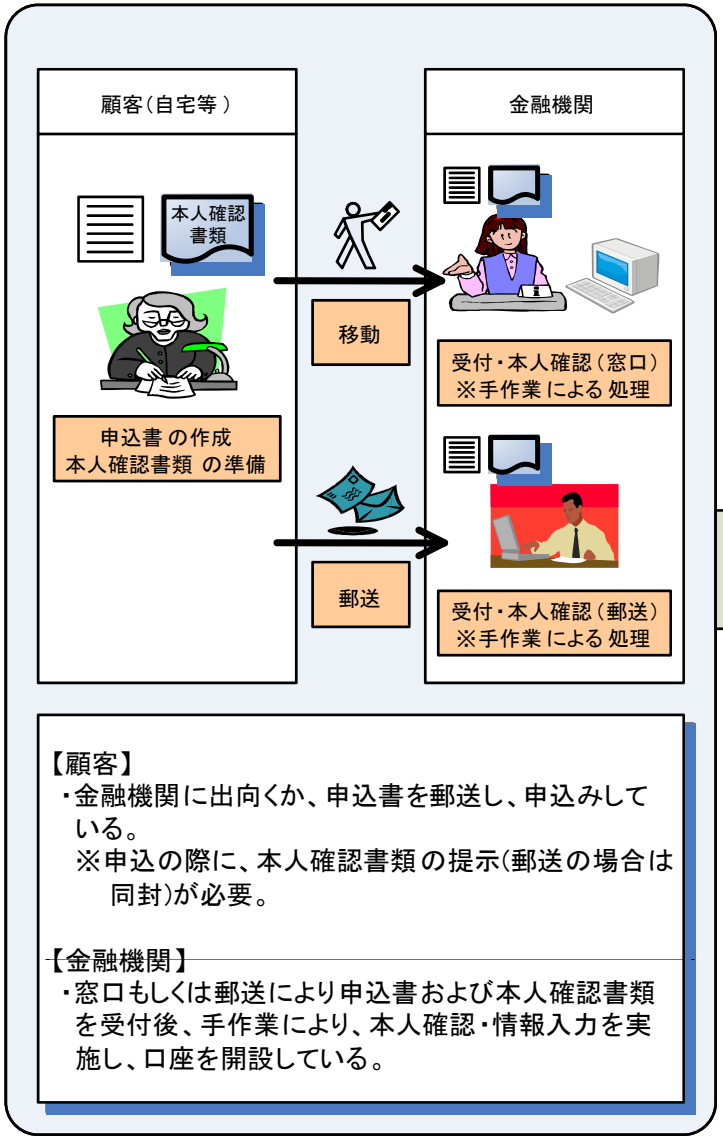
(1)利用者PCとオンライン更新サーバでオンライン更新サーバとSSLを用いた暗号通信を行う。
(2)証明書更新PROXY　APは、通信データからICカードコマンド・データを抽出し中継する。
(3)証明書更新PROXY　APは、サーバ側と協調動作するための制御を行う。
(4)証明書更新PROXY　APは、ICカードRWへのコマンドを付加して、ICカードRWと送受信する。



④【利用サービスの拡大】署名検証者の拡大（民間事業者への拡大）

金融機関の口座開設における署名検証施設を利用した業務実現イメージ

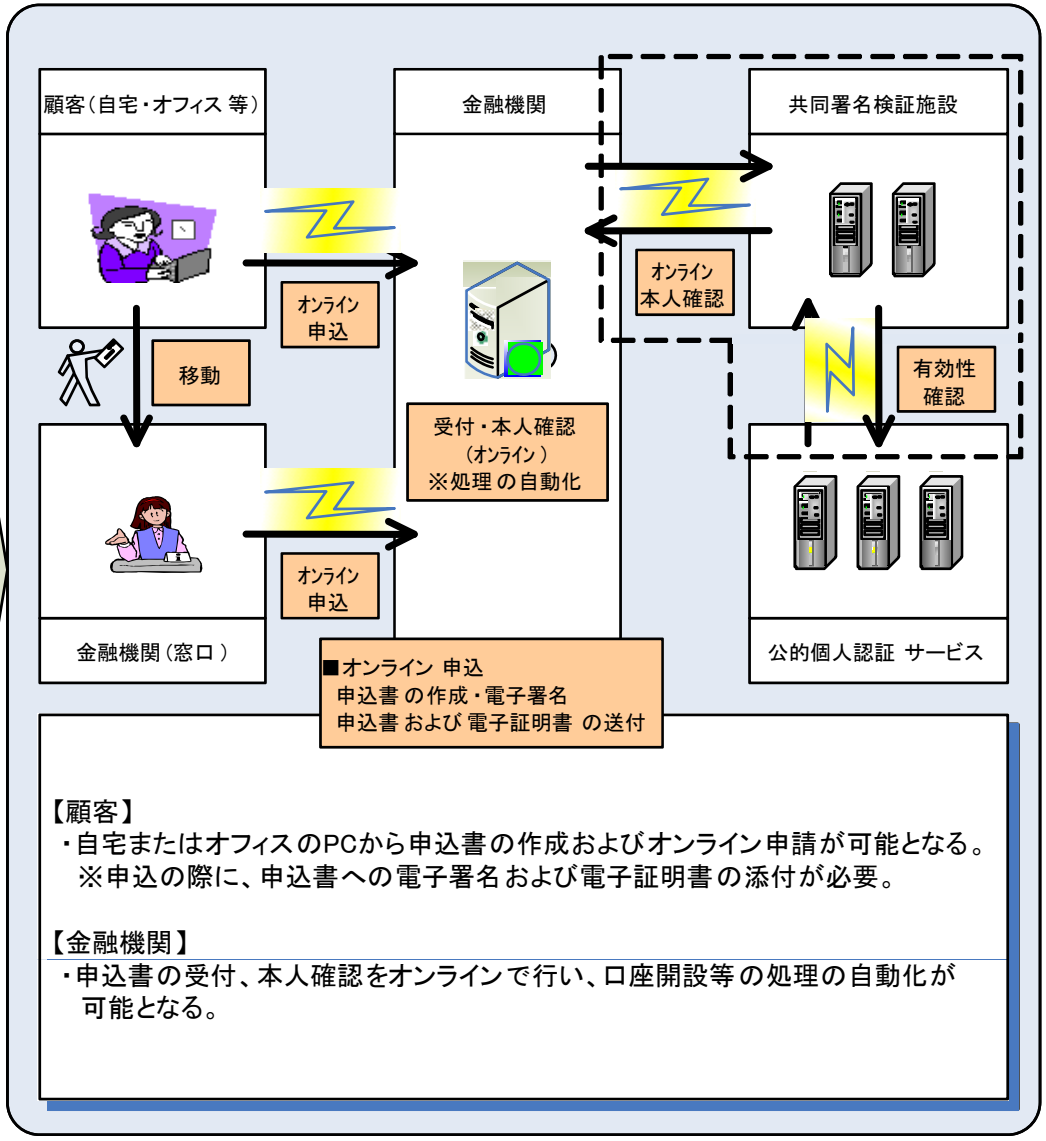
現　行



【顧客】
・金融機関に出向くか、申込書を郵送し、申込みしている。
※申込の際に、本人確認書類の提示(郵送の場合は同封)が必要。

【金融機関】
・窓口もしくは郵送により申込書および本人確認書類を受付後、手作業により、本人確認・情報入力を実施し、口座を開設している。

将　来

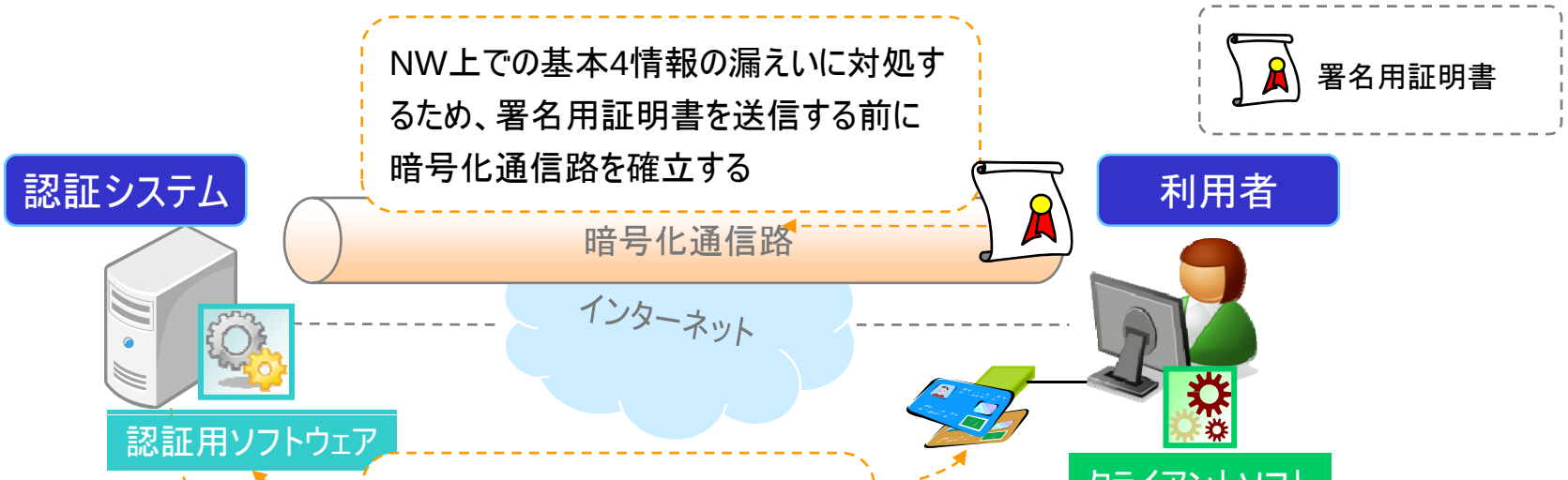


【顧客】
・自宅またはオフィスのPCから申込書の作成およびオンライン申請が可能となる。
※申込の際に、申込書への電子署名および電子証明書の添付が必要。

【金融機関】
・申込書の受付、本人確認をオンラインで行い、口座開設等の処理の自動化が可能となる。

⑤【利用サービスの拡大】利用用途の拡大(行政情報の閲覧等(認証用途))

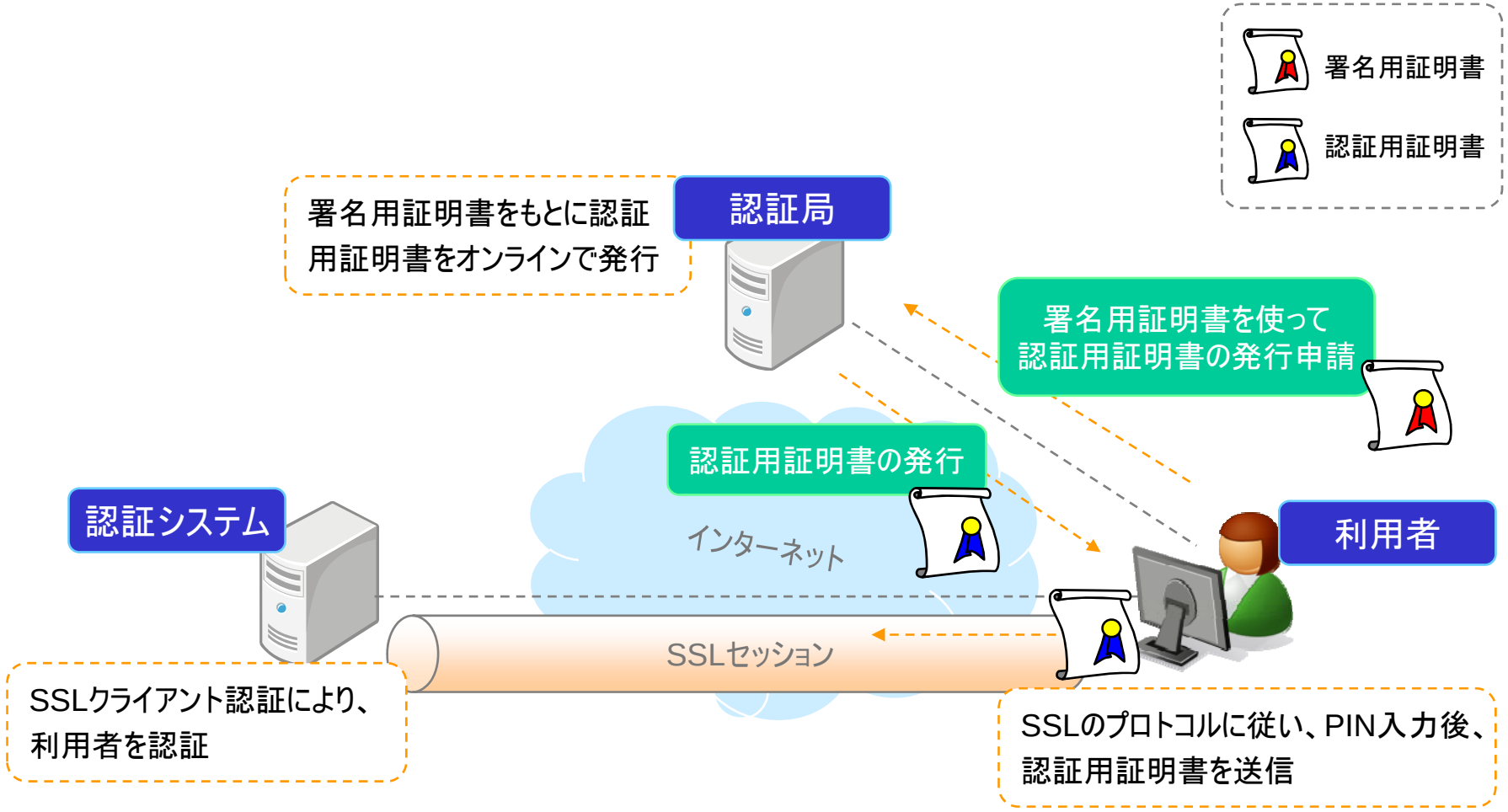
<パターン① 現行の署名用の電子証明書(以下、署名用証明書)を認証用として併用方策案の実現イメージ>



※墨塗り技術を利用して、署名用証明書の基本4情報を秘匿する案も考えられる。この案を実現する場合は、各署名検証者等のシステムを含むシステム全体への影響を考慮する必要がある。

⑤【利用サービスの拡大】利用用途の拡大(行政情報の閲覧等(認証用途))

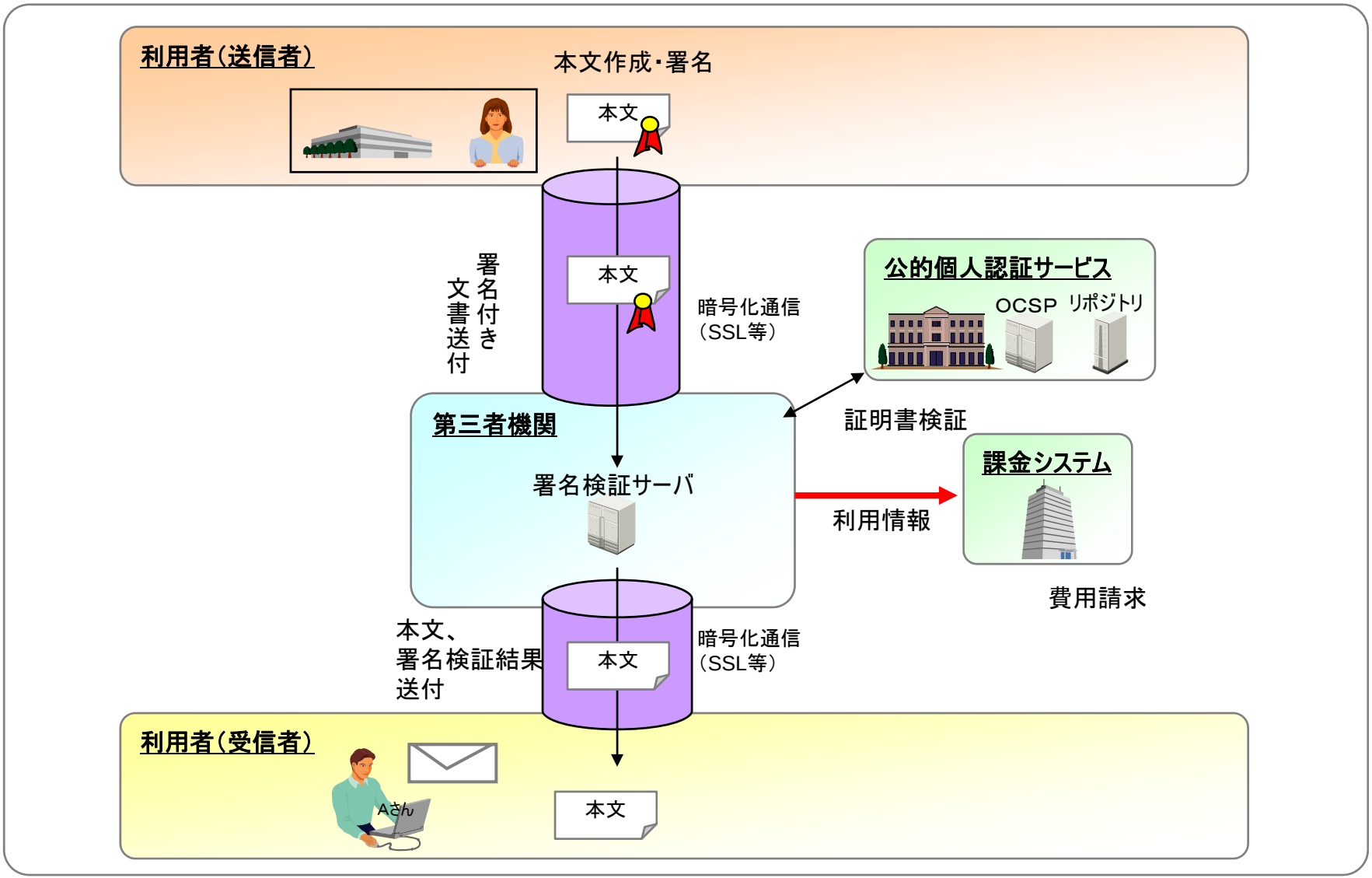
＜パターン②新たに認証用証明書を発行　方策案の実現イメージ＞



※　ここでは、署名用証明書をもとに認証用証明書をオンラインで発行する方式案を記載。この場合、署名用証明書の利用用途拡大にもつながる。

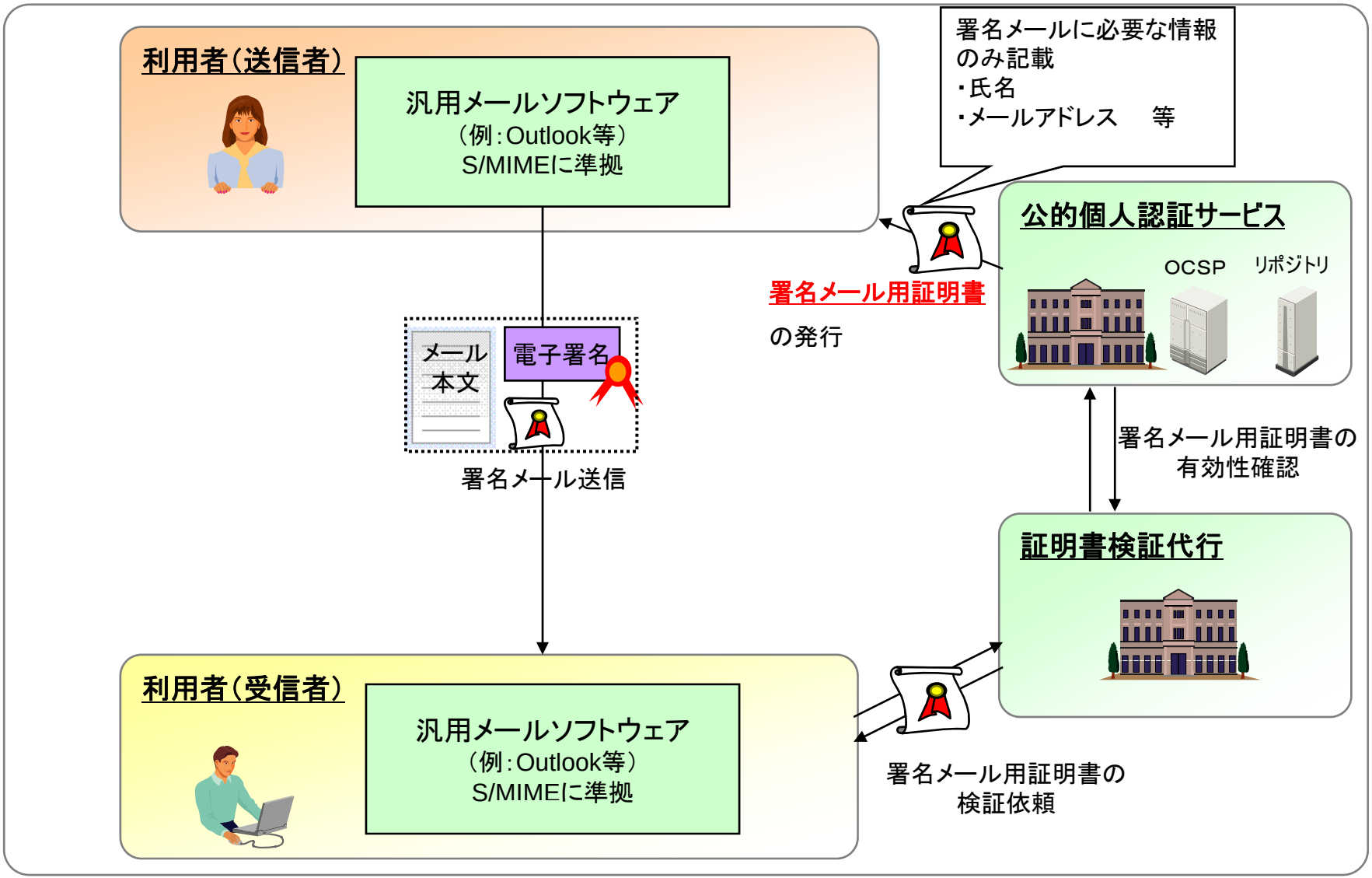
⑥【利用サービスの拡大】利用用途の拡大（署名メール）

署名メール　個人を署名検証者にしない仕組み１（第三者機関設置）実現イメージ



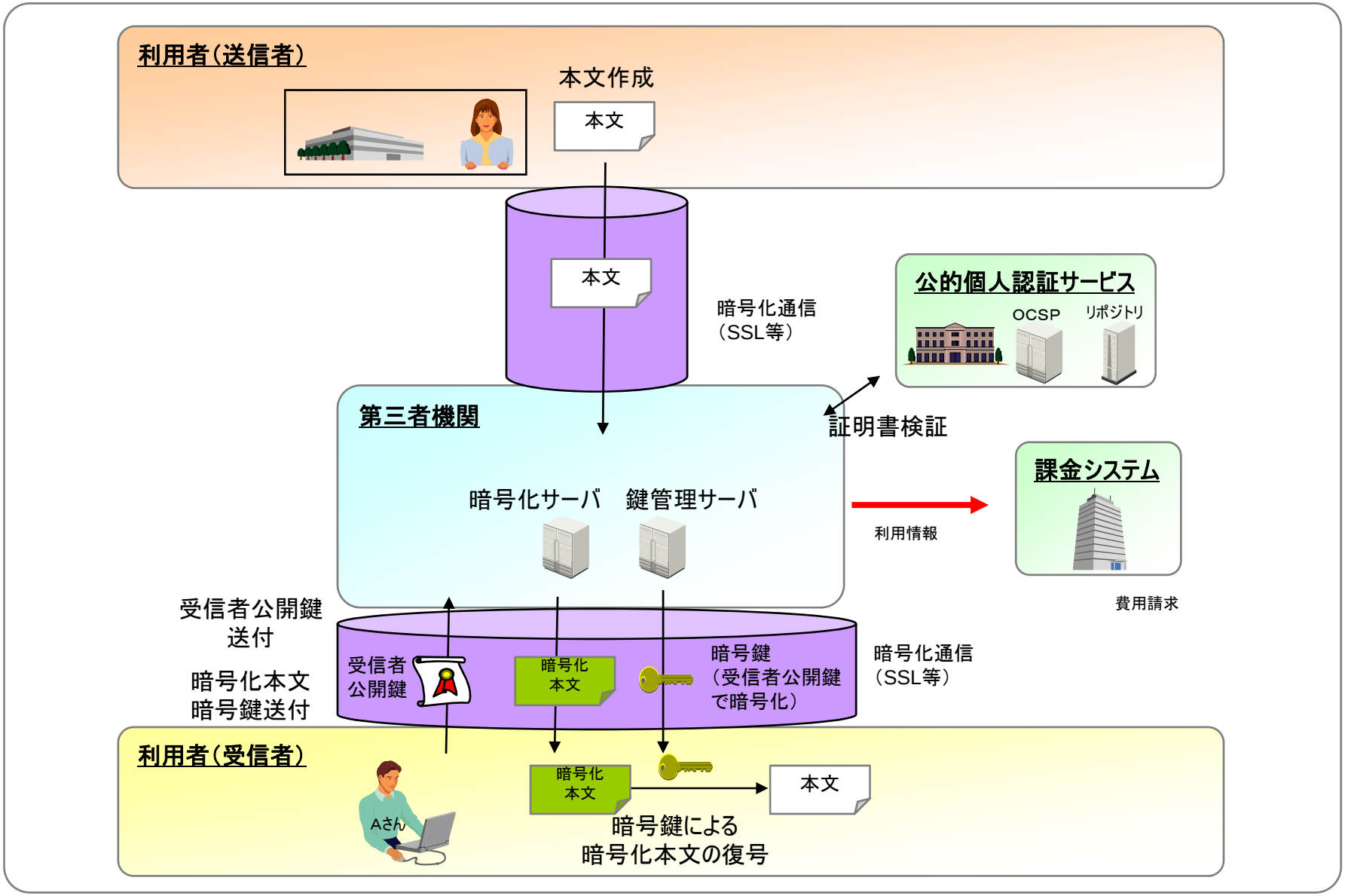
⑥【利用サービスの拡大】利用用途の拡大（署名メール）

個人を署名検証者にしない仕組み２（汎用メールソフトウェア利用） 実現イメージ



⑥【利用サービスの拡大】利用用途の拡大（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（第三者機関設置）実現イメージ



⑥【利用サービスの拡大】利用用途の拡大（暗号メール）

個人を署名検証者にしない仕組み２（汎用メールソフトウェア利用） 実現イメージ