資料2

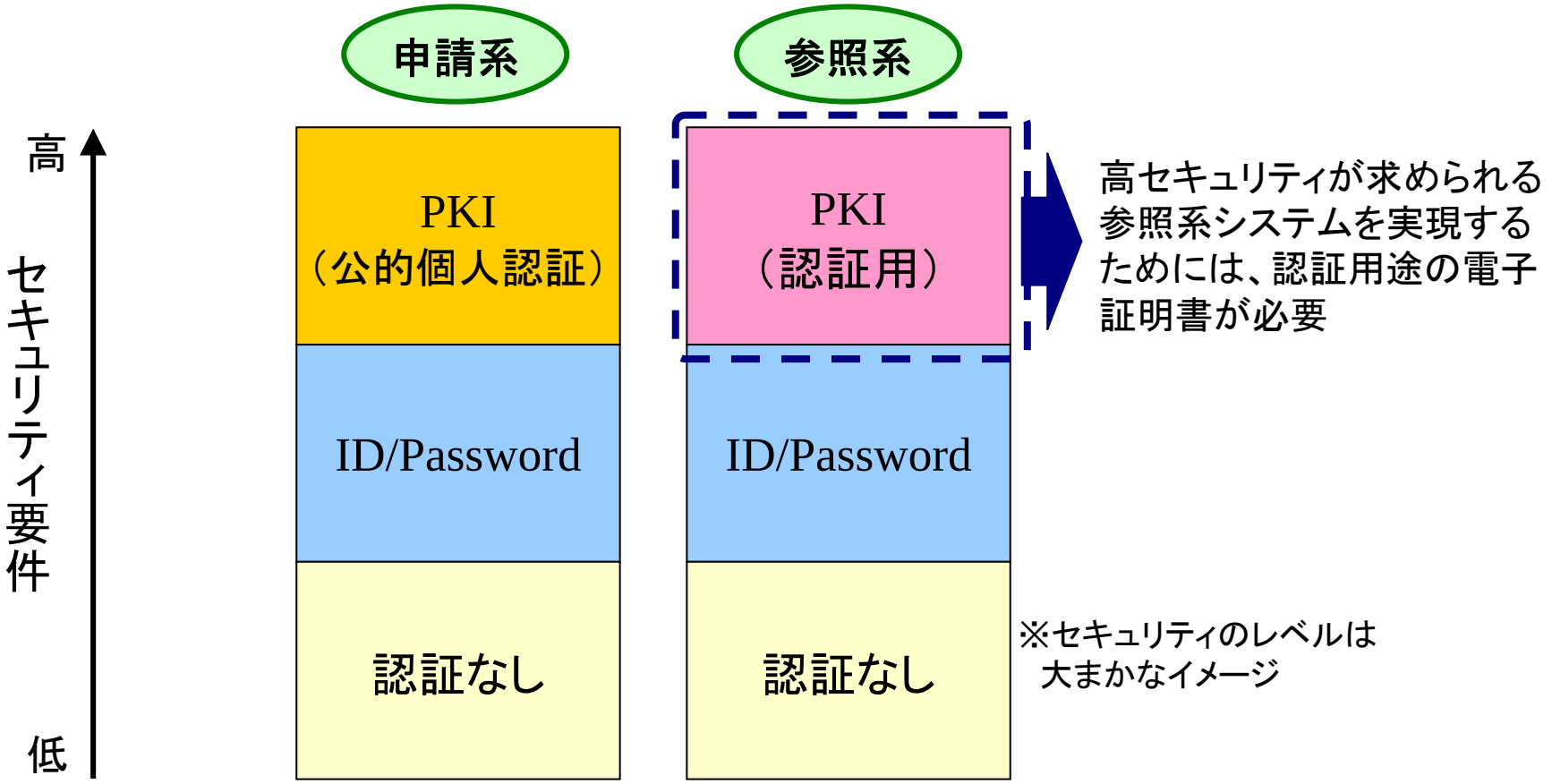
オンライン認証の実現イメージ

申請システムと参照システムにおける認証

電子行政システムは、大きく以下の2パターンに分類。

◆申請系システム：署名が要求される電子文書のやりとりを伴う手続き
◆参照系システム：行政が保管する自身の個人情報等を、必要なときにすぐに確認できるようなオンライン手続き

それぞれのシステムにおいて必要な認証技術は下図のようなイメージ。



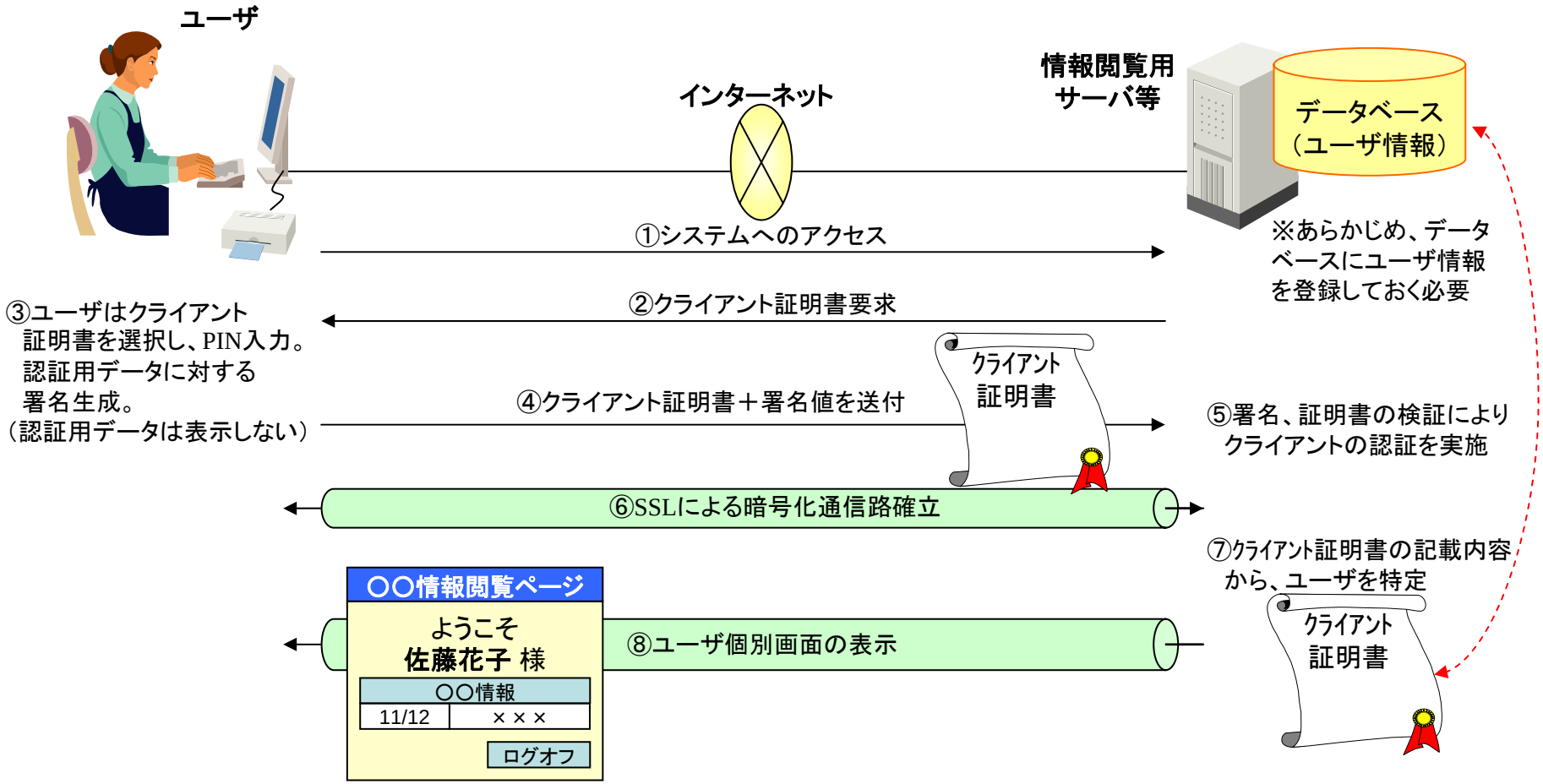
※参照系であっても、申請系の手続き（情報参照の申請）として構成することは可能。

電子署名とオンライン認証の相違点

	電子署名	オンライン認証
位置付け・性格	電子署名が付された文書に、本人がその意思をもって作成した文書として、署名・押印のある文書と同一の法的効力を付するもの。併せて、電子署名の有効性を保証するための厳格な本人確認機能を提供。	特定の人・もの・法人等について、その本人等であって、なりすましではないことを、保証する機能を提供。
主な用途	署名・押印が要求される電子文書（申請書類、届出書類など）のやりとりを伴うオンライン・オフライン手続	機器やシステム、サービスを利用するためのアクセス許可（基本的に、電子文書のやりとりを伴わない）を要求するオンライン手続
効果・ねらい	以下の脅威から手続を保護する 〇電子文書の作成者のなりすまし 〇電子文書の改ざん 〇電子文書の作成者の否認	以下の脅威から手続を保護する 〇機器やシステム、サービスの利用者のなりすまし
法律上の定義	電子署名及び認証業務に関する法律（電子署名法）上で定義が明文化されている。 （公的個人認証法では電子署名法上の定義を引用。）	オンライン認証（なりすましの防止）のみを取り上げて電子署名と区別した規定は、現行法上ではなされていない。

オンライン認証のイメージ（SSLクライアント認証の例）

オンライン認証のイメージとして、民間において一般に行われている、SSLクライアント認証の例を以下に示す。

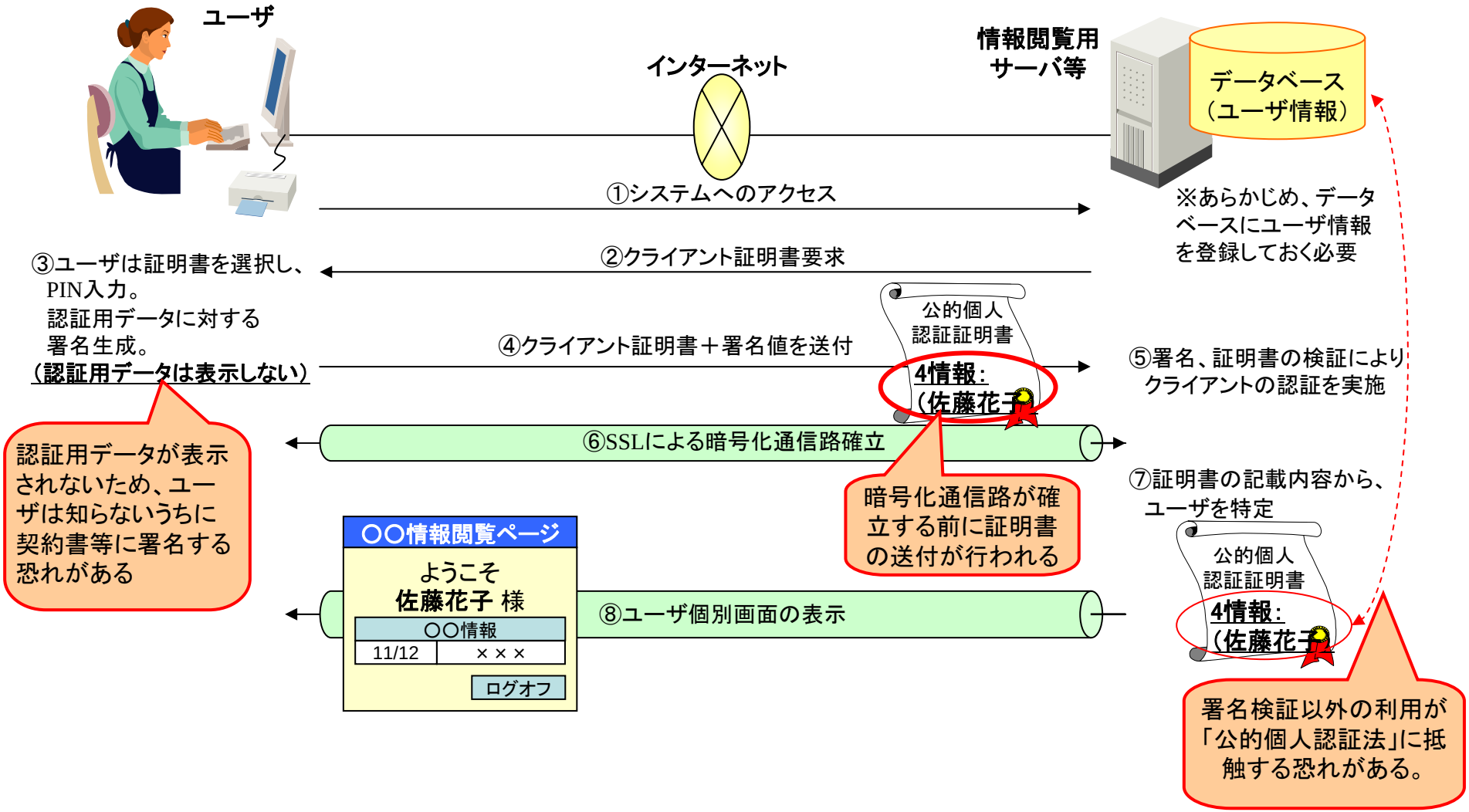


※　一般的なWebサーバとWebブラウザにおける、標準機能でSSLクライアント認証を実施した場合の利用イメージ。

※　SSL通信においてやり取りされる情報のうち、クライアント認証に注目した場合の流れ。

公的個人認証サービスにおいてSSLクライアント認証をそのまま適用した場合に生じる課題

公的個人認証サービスにおいてオンライン認証を行う場合、SSLクライアント認証をそのまま適用した場合、例えば、以下の課題が生じるものと考えられる。



公的個人認証サービスにおいてSSLクライアント認証をそのまま適用した場合に生じる課題

公的個人認証サービスにおいてオンライン認証を行う場合、SSLクライアント認証をそのまま適用した場合に生じる課題を表にまとめると以下のとおり。なお、ここに掲げた課題以外にも様々な課題が生じる可能性がある。

分類	課題
法制度面	「公的個人認証法」において、電子証明書の目的は下記のように記述されている。 ***署名検証者は、利用者から通知された電子証明書を、当該電子証明書とともに通知された情報について行われている電子署名が当該電子証明書に記録された利用者署名検証符号に対応する利用者署名符号を用いて行われていることの確認以外の目的に利用してはならない。（電子署名に係る地方公共団体の認証業務に関する法律第19条第2項）*** → SSLクライアント認証では、証明書記載事項を署名検証以外の目的（例：ユーザの属性確認）に用いることがあるが、そのことが「公的個人認証法」で禁止する目的外利用の疑いがある。
技術面	○SSLクライアント認証では、暗号化通信路確立前にクライアント証明書が送付されてしまうため、電子証明書に記載された情報の流出を防ぐ措置を講じておく必要がある。 ○SSLクライアント認証では、サーバから送付される認証用データが画面で表示されないことが通常であるため、ユーザにとって、自分が何に対して署名生成を行っているのか分かりづらい。
運用面	ユーザが引っ越した場合等に際し、電子証明書が失効するため、その都度、ユーザ登録等の処理が必要となる。

公的個人認証サービスにおけるオンライン認証の実現イメージ

検討会　論点整理（本年5月公表）より

公的個人認証サービスが認証用途の電子証明書を発行する形態としては、以下のようなパターンが考えられる。

① 現行の公的個人認証サービスの署名用途の電子証明書を認証用として併用する。

② 現行法を改正し、公的個人認証サービスの都道府県認証局から、署名用途の電子証明書とは別に認証用途の電子証明書を発行する。

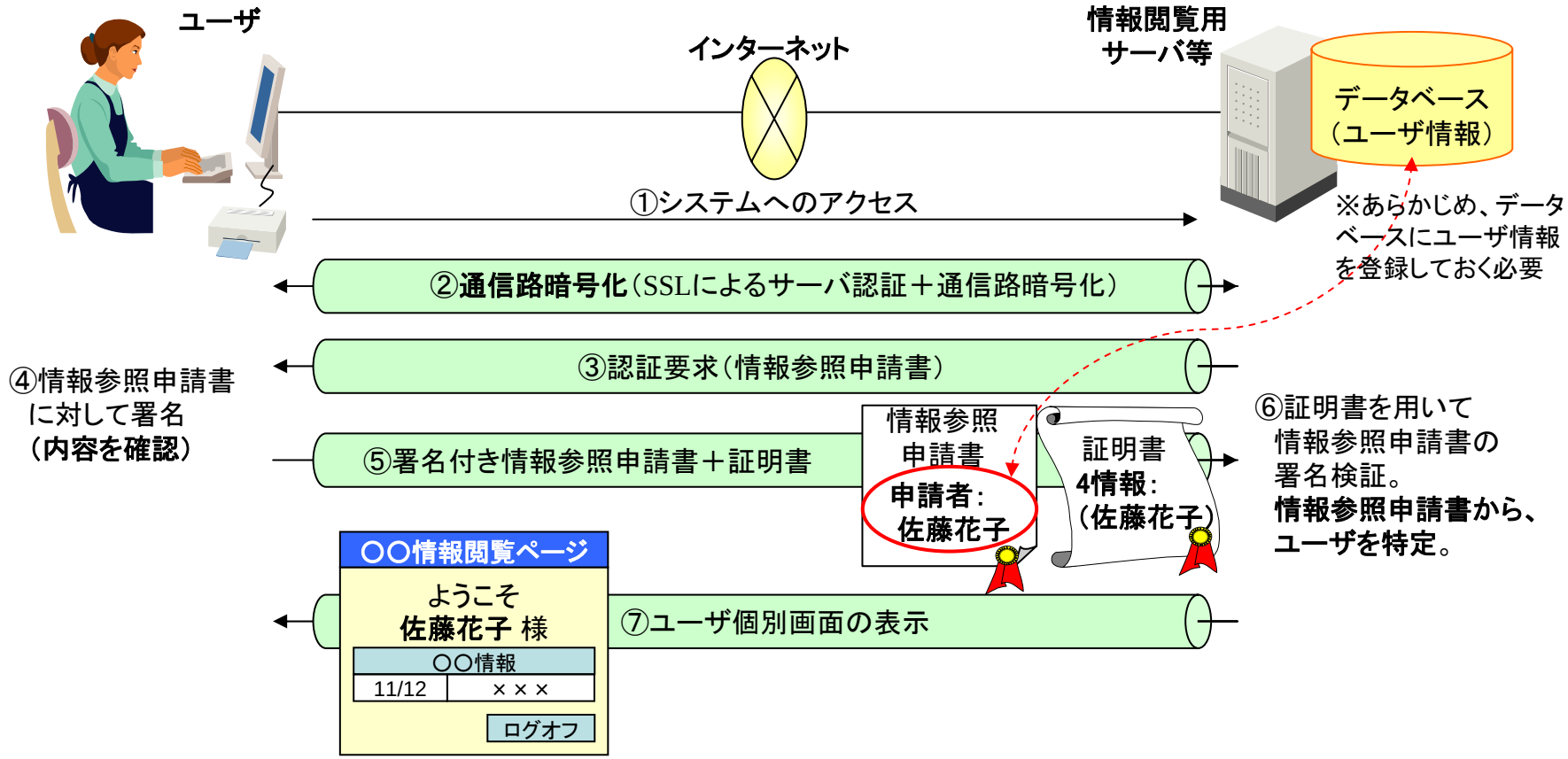
公的個人認証サービスにおいてオンライン認証を実現するにあたって、SSLクライアント認証をそのまま適用した場合には、様々な課題が生じるものと思われる。

それらの課題を解決し、オンライン認証を実現し得る手段として様々な方法が考えられ、現時点で一つに絞り込むのは困難であるところ、実現イメージとして、上記の論点整理に示したパターン毎に、その例を次ページ以降に示す。

【イメージ1】現行の公的個人認証サービスの電子証明書を認証用にも併用

公的個人認証サービスの電子証明書を認証用にも併用する形でオンライン認証を実現するのであれば、例えば、以下の方法により、技術面の課題は解決できる可能性。（ただし、制度面の課題は別途、検討が必要）

〇署名対象となる認証用データ（下図では情報参照申請書）の内容を表示する
〇証明書を送付する前に通信路の暗号化を行う
〇証明書以外のもの（下図では情報参照申請書）によりユーザを特定する



【イメージ2】現行の証明書とは別に、オンライン認証用途の証明書を発行

現行の証明書とは別に、認証用途の証明書を新たに発行した場合、認証用証明書に記載する内容や認証用証明書の利用目的の設定次第では、SSLクライアント認証のスキームと同様になる。