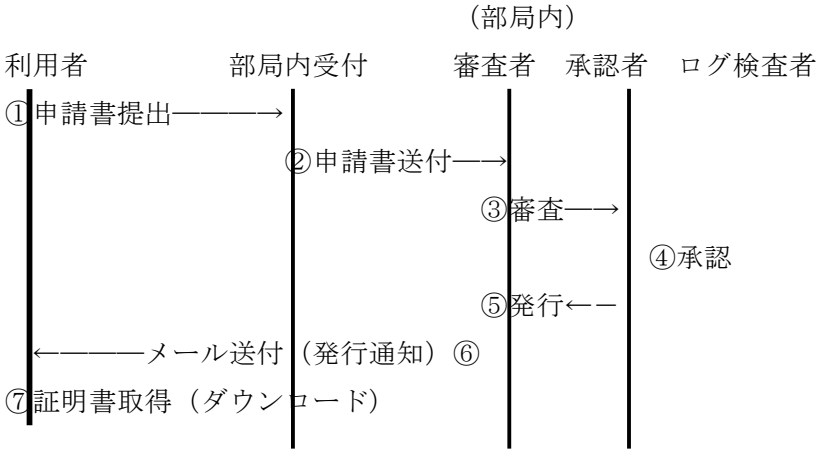
電子証明書発行デモ説明

電子証明書を発行する場合、発行に信頼がおけること（匿名携帯電話の混乱は記憶に新しい)、発行業務が従来業務の流れに乗ること（当然)、業務負荷が重くないこと（いかに便利だとわかっていても、発行にコストがかかりすぎれば誰も発行側に回りたがらない）が求められます。

今回構築した CA では、発行に必要な利用申請の審査、承認の業務を部局（またはいくつかの部局が集まって適正な規模になった集合体）の中で行います。業務を行う権限は、中央から委譲されています。この「委譲」は、IC カードの交付という形で実現されています。

デモにおける登場人物は次のようになっています。シナリオは、利用者が電子証明書を取得するために、部局の交付担当者に連絡を取ることからはじまります。部局には審査者と承認者が割り当てられています。



審査者と承認者は RA クライアントから RA コネクタに接続して業務を行います。部局ごとに接続できる利用者 DB を分割することで複数部局にわけた登録業務が可能になります。

デモで示すように、審査者と承認者は、それぞれ一人だけでは発行業務が行えません。この相互牽制ルールが、発行される電子証明書の信頼性に直結しています。

なお、今回のデモでは利用者が直接 IC カードに電子証明書を格納するシナリオになっています。利用者がどういう場面でどう電子証明書を使うのかによって、この部分はさらなる検討が必要になります。

ログ検査者は、RA に残されたログを定期的、不定期的に検査して、審査者と承認者の作業に不正がないかのチェックを行います。これも電子証明書の信頼性の一部になっています。