

---

## 認証基盤の適用に関する検討

---

# 1. 認証基盤の適用に関する検討の概要

## 検討のポイント

インターネット等のネットワークを利用して申請を行うOSSにおいては、なりすまし、否認、改ざんという脅威が存在し、それらを解決するために、公開鍵暗号方式を用いた認証基盤の適用が不可欠である(公開鍵暗号方式を用いた認証基盤については参考資料に示す)。認証基盤の適用においては、申請者及び行政機関において、どの認証基盤を利用することが望ましいかについて検討を行った。

申請者(個人)の認証基盤

申請者(法人)の認証基盤

行政機関(運輸支局長、警察署長、都道府県知事等)の認証基盤 (ただし、どの電子文書に電子署名(認証基盤)を適用するかについては今後検討が必要である)

## 検討の方向性

申請者(個人)の認証基盤

実印 + 印鑑登録証明書等と同様の信頼性を要するため、本人確認の厳格性、電子証明書に記載される個人情報の信頼性(氏名や住所の変更を把握できるか)、普及等の観点から「公的個人認証サービス」を利用する方向で検討する(概要については次ページを参照)。

申請者(法人)の認証基盤

実印 + 印鑑登録証明書等と同様の信頼性を要するため、本人確認の厳格性、電子証明書に記載される法人情報の信頼性(登記情報の変更を把握できるか)、普及等の観点から「商業登記認証基盤」を利用する方向で検討する(概要については次ページを参照)。

行政機関の認証基盤

平成15年度から稼働が予定されている以下のような認証基盤の利用を前提とする。

運輸支局長： 政府認証基盤(GPKI)

警察署長： 政府認証基盤(GPKI)又は地方公共団体認証基盤(LGPKI)

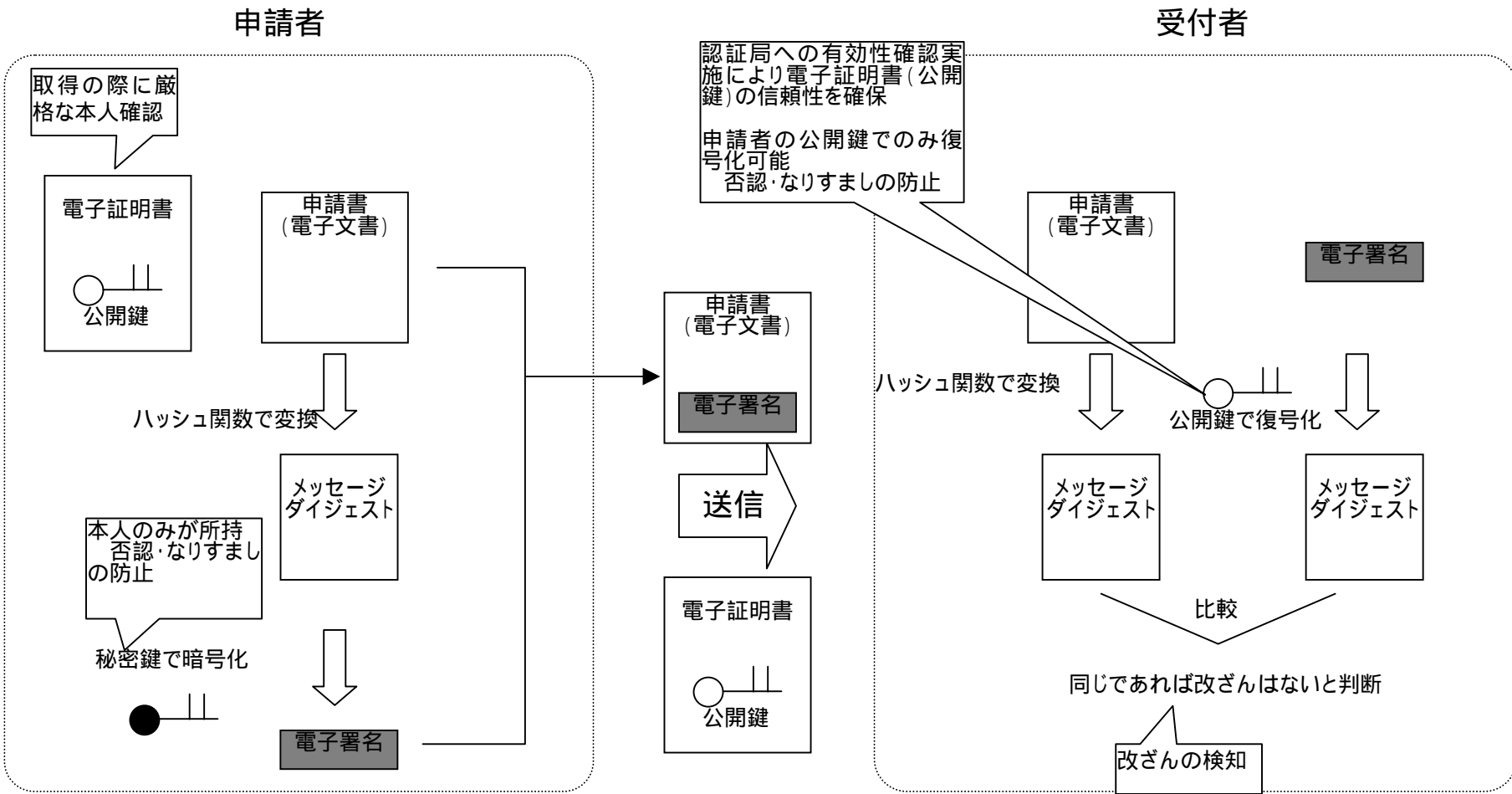
都道府県知事、都道府県税事務所長： 地方公共団体認証基盤(LGPKI)

## 2. 公的個人認証サービスと商業登記認証基盤の概要

### 公的個人認証サービスと商業登記認証基盤の概要

	公的個人認証サービス	商業登記認証基盤
認証局の設置主体	都道府県 (ただし、本人確認事務は市町村が実施)	法務省
電子証明書を受けることができる者	住民基本台帳に記録されている者	法人代表者(登記所に印鑑を提出した者)
本人確認の厳格性	住所地の市町村において対面審査による厳格な本人確認を実施	登記所に印鑑を提出した法人代表者が出頭するか、委任状を持つ代理人が出頭して申請
電子証明書に記載されている本人(登記)情報の信頼性	住所等、住民基本台帳の個人情報に変更があった際には、住民基本台帳ネットワークシステム等と連携することで電子証明書が失効される。そのため、有効である電子証明書の情報の信頼性は確保される	登記情報に変更があった場合には、管轄登記所からの通知によって知らされ、電子証明書が失効される。そのため、有効である電子証明書の信頼性は確保される
電子証明書に記録される本人(法人)に関する情報	・氏名 ・住所 ・生年月日 ・性別	・会社の商号 ・会社の本店 ・会社代表者の氏名 ・会社代表者の資格 等
稼働時期	平成15年度に稼働予定	平成12年度から稼働

# (参考) 公開鍵暗号方式を用いた認証基盤の概要



秘密鍵・公開鍵: 秘密鍵によって暗号化されたものは、そのペアである公開鍵でのみ復号化可能  
 ハッシュ関数:  $y = f(x)$  において  $x$  から  $y$  を求めるのは簡単であるが、 $y$  から  $x$  を求めるのは事実上困難であり、かつ  $x$  から同一の  $y$  を生成するのが計算上不可能である関数のこと