

マイナンバーカードに格納される公的個人認証サービスについて



公開鍵暗号方式

公的個人認証サービスが採用する暗号方式。秘密鍵と公開鍵はペアとなっており、片方の鍵で暗号化されたものは、もう一方の鍵でしか復号できない性質をもつ。

署名用電子証明書

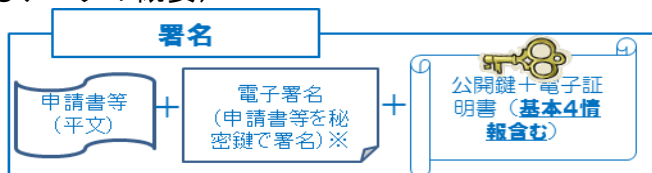
(性質)

インターネットで電子文書を送信する際などに、署名用電子証明書を用いて、文書が改ざんされていないかどうか等を確認することができる仕組み

(利用局面)

e-Taxの確定申告等、文書を伴う電子申請等に利用される。

(利用されるデータの概要)



※ 電子署名法(平成12年法律第102号)の「電子署名」に該当し、同法第3条による「真正な成立の推定」の対象になり得る。

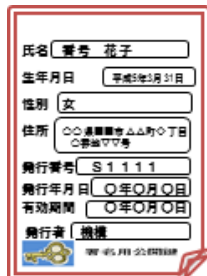


署名用
秘密鍵

※ カードの中の格納された領域から外に出ることがない

※ 秘密鍵を無理に読みだそうとすると、ICチップが壊れる仕組み

電子証明書のイメージ



※基本4情報を記録

利用者証明用電子証明書

(性質)

インターネットを閲覧する際などに、利用者証明用電子証明書(基本4情報の記載なし)を用いて、利用者本人であることのみを証明する仕組み

(利用局面)

マイナポータルログイン等、本人であることの認証手段として利用される。

(利用されるデータの概要)

利用者証明

公開鍵+電子証明書



利用者証明用
秘密鍵

※ カードの中の格納された領域から外に出ることがない

※ 秘密鍵を無理に読みだそうとすると、ICチップが壊れる仕組み

電子証明書のイメージ



※基本4情報の記録なし

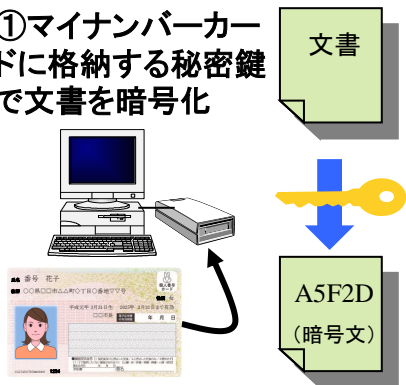
公的個人認証サービスの仕組み

【凡例】 秘密鍵： 公開鍵：

1 署名用電子証明書

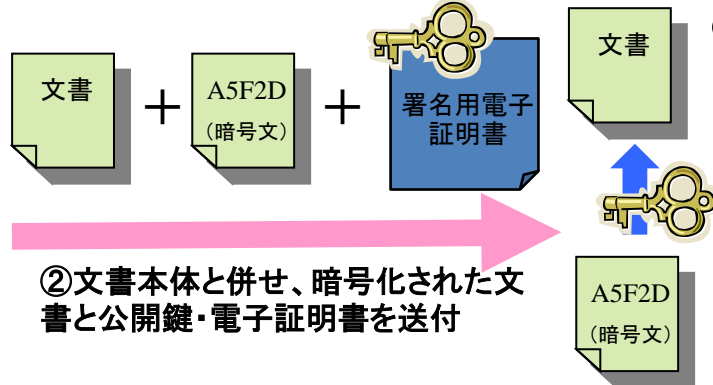
(例) e-Tax(国税電子申告・納税システム)による確定申告

①マイナンバーカードに格納する秘密鍵で文書を暗号化



発信者

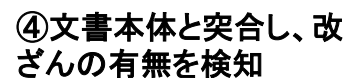
②文書本体と併せ、暗号化された文書と公開鍵・電子証明書を送付



③発信者から送付された公開鍵で暗号化された文書を復号化



④文書本体と突合し、改ざんの有無を検知



⑤電子証明書の有効性を照会

⑥電子証明書の有効性を回答

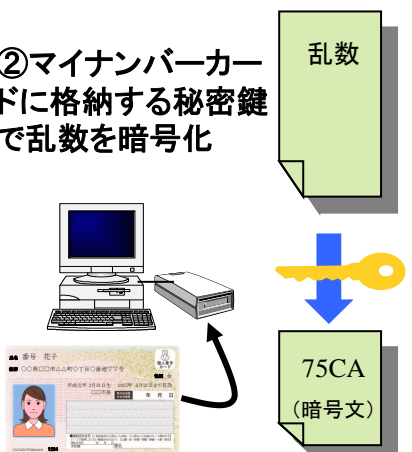
有効であれば、認証成功
確定申告を受付



2 利用者証明用電子証明書

(例) マイナポータルへのログイン(検討中)

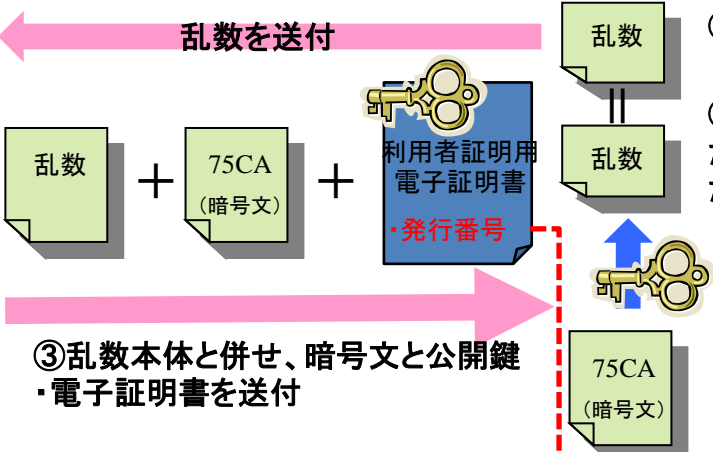
②マイナンバーカードに格納する秘密鍵で乱数を暗号化



発信者

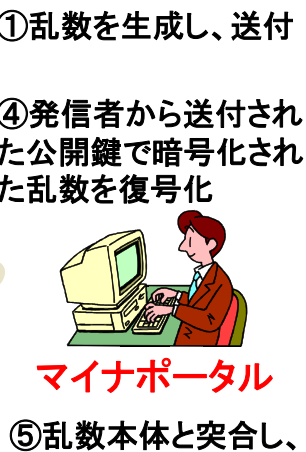
乱数を送付

③乱数本体と併せ、暗号文と公開鍵・電子証明書を送付



①乱数を生成し、送付

④発信者から送付された公開鍵で暗号化された乱数を復号化



⑤乱数本体と突合し、改ざんの有無を検知

⑥電子証明書の有効性を照会

⑦電子証明書の有効性を回答

有効であれば、認証成功
マイナポータルにログイン



・マイ・ポータルは、電子証明書に記載されている発行番号を用いて、ログインした者を特定
・氏名、住所等の基本4情報は持たず