総 行 マ 第 10 号
令和４年１月 31 日

各 都 道 府 県 知 事　殿
（各都道府県公的個人認証サービス担当課室扱い）

総 務 省 自 治 行 政 局 長
（　公　印　省　略　）

公的個人認証サービス事務処理要領の一部改正について（通知）

「令和３年の地方からの提案等に関する対応方針」（令和３年 12 月 21 日閣議決定）を踏まえ、公的個人認証サービス事務処理要領（平成 16 年総行自第１号総務省自治行政局長から各都道府県知事あて通知）の一部を下記のとおり改正することとしましたので、貴職におかれては内容を承知の上、域内の市町村（特別区を含む。）に周知してください。

なお、本通知は、地方自治法（昭和 22 年法律第 67 号）第 245 条の４第１項に基づく技術的助言であることを申し添えます。

記

第１　公的個人認証サービス事務処理要領の一部改正

公的個人認証サービス事務処理要領の一部を別添の新旧対照表のように改正する。

第２　実施期日

この通知は、通知の日から実施する。

担当：総務省自治行政局住民制度課
マイナンバー制度支援室
小泉係長、平間官、小山官
03-5253-5536（直通）

公的個人認証サービス事務処理要領　新旧対照表

（傍線の部分は改正部分）

改　正　前	改　正　後
第１　総説 **１　公的個人認証サービスの概要** （略） 電子証明書に係る秘密鍵及び公開鍵並びに電子証明書は、電子データとして、個人番号カードその他の総務省令で定める耐タンパ性を有する IC カードに格納され、利用者本人が設定する暗証番号と共に使用される。更にこの IC カードを利用者が厳格に管理することで、第三者に秘密鍵を読み取られることを防いでいる。こうして、高いセキュリティを実現しながら、公的個人認証サービスは全国の住民に展開される。 **２・３　（略）** **４　制度概要** （１）（略） （２）電子証明書 ア　（略） イ　規格 （ア）・（イ）（略） （ウ）記録媒体 電子証明書が記録可能な媒体は、個人番号カード及び総務省から別途通知される IC カードである（法第３条第４項、法第 22 条第４項、規則第７条、規則第 43 条、告示第６条）。 （エ）（略） ウ～オ　（略） （３）（略）	**第１　総説** **１　公的個人認証サービスの概要** （略） 電子証明書に係る秘密鍵及び公開鍵並びに電子証明書は、電子データとして、個人番号カードその他の主務省令で定める耐タンパ性を有する IC カードに格納され、利用者本人が設定する暗証番号と共に使用される。更にこの IC カードを利用者が厳格に管理することで、第三者に秘密鍵を読み取られることを防いでいる。こうして、高いセキュリティを実現しながら、公的個人認証サービスは全国の住民に展開される。 **２・３　（略）** **４　制度概要** （１）（略） （２）電子証明書 ア　（略） イ　規格 （ア）・（イ）（略） （ウ）記録媒体 電子証明書が記録可能な媒体は、個人番号カード並びにデジタル庁及び総務省から別途通知される IC カードである（法第３条第４項、法第 22 条第４項、規則第７条、規則第 43 条、告示第６条）。 （エ）（略） ウ～オ　（略） （３）（略）

（４）登場者 ア～ウ　（略） エ　署名検証者 （略） ①～④（略） ⑤電子署名及び認証業務に関する法律第２条第３項に規定する特定認証業務を行う者であって政令で定める基準に適合する者として総務大臣が認定する者 ⑥前述の①～⑤以外の者で、署名利用者から通知された電子署名が行われた情報について当該署名利用者が当該電子署名を行ったこと又は利用者証明利用者が行った電子利用者証明について当該利用者証明利用者が当該電子利用者証明を行ったことの確認を政令で定める基準に適合して行うことができるものとして総務大臣が認定するもの （略） オ～キ　（略） 第２　認証業務 １　電子証明書の発行 （略） （１）申請者／利用者による申請に基づく電子証明書の新規発行／更新（本人の場合） ア　事務手順 （ア）～（ウ）（略） （エ）IC カードの確認 A・B　（略） C　暗証番号の指定	（４）登場者 ア～ウ　（略） エ　署名検証者 （略） ①～④（略） ⑤電子署名及び認証業務に関する法律第２条第３項に規定する特定認証業務を行う者であって政令で定める基準に適合する者として主務大臣（内閣総理大臣及び総務大臣）が認定する者 ⑥前述の①～⑤以外の者で、署名利用者から通知された電子署名が行われた情報について当該署名利用者が当該電子署名を行ったこと又は利用者証明利用者が行った電子利用者証明について当該利用者証明利用者が当該電子利用者証明を行ったことの確認を政令で定める基準に適合して行うことができるものとして主務大臣が認定するもの （略） オ～キ　（略） 第２　認証業務 １　電子証明書の発行 （略） （１）申請者／利用者による申請に基づく電子証明書の新規発行／更新（本人の場合） ア　事務手順 （ア）～（ウ）（略） （エ）IC カードの確認 A・B　（略） C　暗証番号の指定

IC カードを統合端末に挿入した状態で、申請者／利用者にタッチパネルを操作させ、新規発行／更新対象の電子証明書に設定する暗証番号を指定させる。 また、更新の場合は、申請者／利用者に対して、従来の暗証番号を用いるよう案内する。	IC カードを統合端末に挿入した状態で、申請者／利用者にタッチパネルを操作させ、新規発行／更新対象の電子証明書に設定する暗証番号を指定させる。 また、更新の場合は、申請者／利用者に対して、従来の暗証番号を用いるよう案内する。
［新設］	暗証番号の設定が困難な利用者に対してはタッチパネルの操作を支援し、やむを得ない場合は代行する。なお、暗証番号の決定を代行することは認められないことから、暗証番号を代行して入力する際には、入力を代行する市区町村の職員以外の市区町村の職員が本人の意思を確認するなど、本人が暗証番号を決定したことについて十分な確認を行うものとする。
なお、申請者／利用者が経由市区町村を経由して新規発行／更新申請書を提出するときは、経由市区町村を経由して事前に暗証番号を届出させ、住所地市区町村の職員が当該暗証番号を設定することとする。	なお、申請者／利用者が経由市区町村を経由して新規発行／更新申請書を提出するときは、経由市区町村を経由して事前に暗証番号を届出させ、住所地市区町村の職員が当該暗証番号を設定することとする。
（略）	（略）
（オ）～（ケ）（略）	（オ）～（ケ）（略）
イ～コ　（略）	イ～コ　（略）
（２）（略）	（２）（略）
２～６　（略）	２～６　（略）
第３　その他附帯業務	第３　その他附帯業務
１　暗証番号の変更／初期化	１　暗証番号の変更／初期化
（１）利用者による暗証番号の変更／初期化の申請の受付（本人の場合）	（１）利用者による暗証番号の変更／初期化の申請の受付（本人の場合）
ア　事務手順	ア　事務手順
（ア）～（ウ）（略）	（ア）～（ウ）（略）
（エ）暗証番号の変更	（エ）暗証番号の変更

従来の暗証番号を用いてタッチパネルにおいて暗証番号を変更するように促す。 暗証番号変更が困難な利用者に対してはタッチパネルの操作を支援し、やむを得ない場合は代行する。暗証番号変更の主な手順を以下に示す。 A～E　（略） （オ）・（カ）（略） イ～オ　（略） （２）（略） ２～10　（略）	従来の暗証番号を用いてタッチパネルにおいて暗証番号を変更するように促す。 暗証番号変更が困難な利用者に対してはタッチパネルの操作を支援し、やむを得ない場合は代行する。なお、暗証番号の決定を代行することは認められないことから、暗証番号を代行して入力する際には、入力を代行する市区町村の職員以外の市区町村の職員が本人の意思を確認するなど、本人が暗証番号を決定したことについて十分な確認を行うものとする。暗証番号変更の主な手順を以下に示す。 A～E　（略） （オ）・（カ）（略） イ～オ　（略） （２）（略） ２～10　（略）

（平成 16 年１月５日総行自第１号総務省自治行政局長から各都道府県知事あて通知）
＜改正＞
（平成16年３月２日総行自第42号総務省自治行政局長から各都道府県知事あて通知）
（平成 17 年２月 23 日総行自第 39 号総務省自治行政局長から各都道府県知事あて通知）
（平成 17 年４月 22 日総行自第 75 号総務省自治行政局長から各都道府県知事あて通知）
（平成 18 年 10 月 31 日総行自第 197 号総務省大臣官房総括審議官から各都道府県知事あて通知）
（平成19年９月25日総行自第141号総務省大臣官房総括審議官から各都府県知事あて通知（平成20年８月１日から施行））
（平成20年10月１日総行情第112号総務省自治行政局長から各都道府県知事あて通知）
（平成 25 年３月 19 日総行住第 22 号総務省自治行政局長から各都道府県知事あて通知）
（平成27年９月29日総行住第142号総務省自治行政局長から各都道府県知事あて通知）
（平成 27 年 11 月 26 日総行住第 188 号総務省自治行政局長から各都道府県知事あて通知）
（平成 28 年４月 14 日総行住第 85 号総務省自治行政局長から各都道府県知事あて通知）
（平成 31 年４月 24 日総行住第 63 号総務省自治行政局長から各都道府県知事あて通知）
（令和元年９月11日総行住第79号総務省自治行政局長から各都道府県知事あて通知）
（令和元年12月16日総行住第132号総務省自治行政局長から各都道府県知事あて通知）
（令和２年５月 25 日総行住第 102 号総務省自治行政局長から各都道府県知事あて通知）
（令和３年２月15日総行住第18号総務省自治行政局長から各都道府県知事あて通知）
（令和３年５月19日総行マ第14号総務省自治行政局長から各都道府県知事あて通知）

公的個人認証サービス事務処理要領

総務省

公的個人認証サービス事務処理要領　　【目次】

第１　総説

１　公的個人認証サービスの概要

平成 14 年 12 月 13 日に電子署名に係る地方公共団体の認証業務に関する法律が公布されたことに伴い、公的個人認証サービスが創設された。

さらに、平成 28 年１月から社会保障・税番号制度が開始されることに伴い、平成 25 年５月に同法が「電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律」に改正され、各都道府県知事が認証業務を行うとともに指定認証機関へ事務を委任する仕組みを廃止し、地方公共団体情報システム機構（以下「機構」という。）が認証業務を行うことが規定された。また、署名用電子証明書と、本人であることの認証手段として利用される利用者証明用電子証明書の２つの証明書を発行することとなった。

公的個人認証サービスとは、インターネット等によるオンライン手続において、なりすまし、改ざん等の危険性を防ぐための確かな本人確認手段といえる電子署名及び利用者本人であることの確かな証明手段といえる電子利用者証明を、地理的条件等による利用格差が生じないよう住民基本台帳に記録されている全国の住民に対して提供するサービスである。

公的個人認証サービスの利用を希望する者は、電子署名及び電子利用者証明を行うにあたって必要となるそれぞれの秘密鍵及び公開鍵並びに機構が発行した利用者本人の電子証明書を、住所地市区町村受付窓口において入手することが可能である。

電子証明書に係る秘密鍵及び公開鍵並びに電子証明書は、電子データとして、個人番号カードその他の主務省令で定める耐タンパ性を有する IC カードに格納され、利用者本人が設定する暗証番号と共に使用される。更にこの IC カードを利用者が厳格に管理することで、第三者に秘密鍵を読み取られることを防いでいる。こうして、高いセキュリティを実現しながら、公的個人認証サービスは全国の住民に展開される。

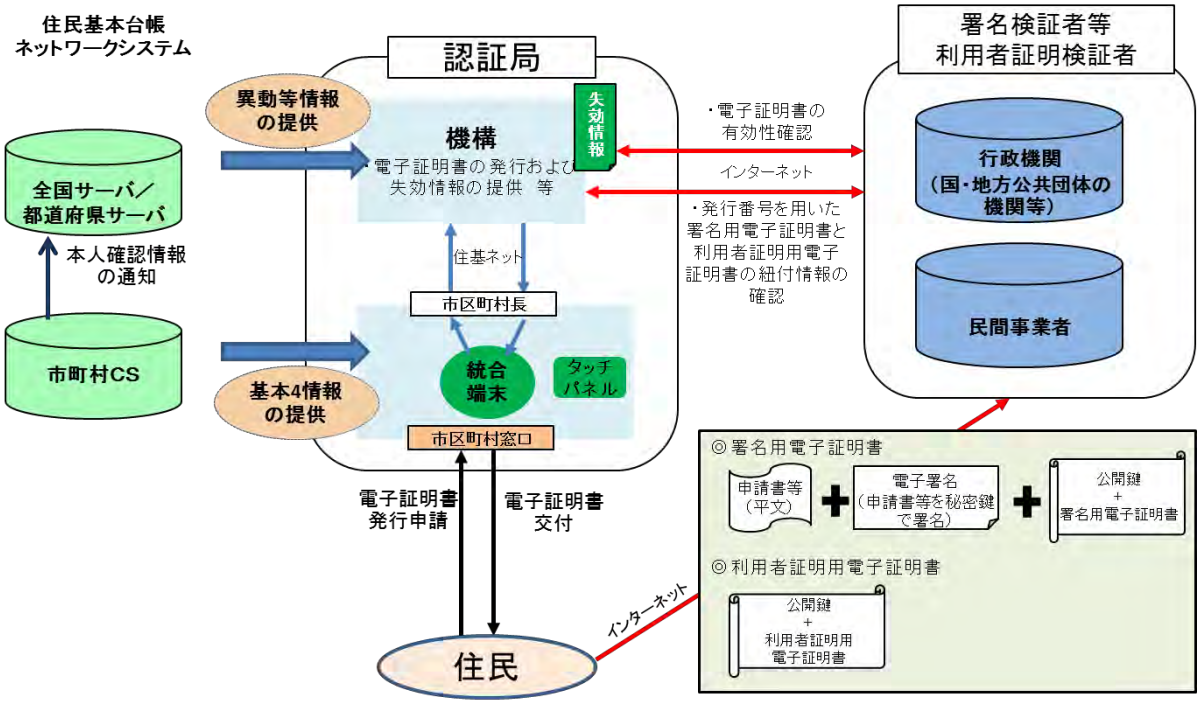


図 1-1　公的個人認証サービスの概要

2　定義

この要領において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(1)	法	電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律（平成 14 年法律第 153 号）をいう。
(2)	令	電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律施行令（平成 15 年政令第 408 号）をいう。
(3)	規則	電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律施行規則（平成 15 年総務省令第 120 号）をいう。
(4)	告示	認証業務及びこれに附帯する業務の実施に関する技術的基準（平成 15 年総務省告示第 706 号）をいう。
(5)	認証業務	法第２条第３項に規定する認証業務をいう。
(6)	秘密鍵	法第２条第４項に規定する署名利用者符号又は法第２条第５項に規定する利用者証明利用者符号をいう。
(7)	公開鍵	法第２条第４項に規定する署名利用者検証符号又は法第２条第５項に規定する利用者証明利用者検証符号をいう。
(8)	署名用電子証明書	法第３条第１項に規定する署名用電子証明書であって、同条第６項の規定により発行されるものをいう。
(9)	利用者証明用電子証明書	法第 22 条第１項に規定する利用者証明用電子証明書であって、同条第６項の規定により発行されるものをいう。
(10)	電子証明書	署名用電子証明書又は利用者証明用電子証明書をいう。
(11)	電磁的記録	法第３条第１項に規定する電磁的記録をいう。
(12)	住所地市区町村長	法第３条第２項に規定する住所地市町村長並びに地方自治法（昭和 22 年法律第 67 号）第 252 条の 19 第１項の指定都市の区長及び総合区長をいう。
(13)	電磁的記録媒体	法第３条第４項及び法第 22 条第４項に規定する電磁的記録媒体をいう。

(14)	発行記録	法第８条に規定する署名用電子証明書発行記録及び法第 27 条に規定する利用者証明用電子証明書発行記録をいう。
(15)	記録誤り等	法第 13 条に規定する署名用電子証明書記録誤り等又は法第 32 条に規定する利用者証明用電子証明書記録誤り等をいう。
(16)	発行者署名符号	法第 14 条に規定する署名用電子証明書発行者署名符号又は法第 33 条に規定する利用者証明用電子証明書発行者署名符号をいう。
(17)	失効情報	法第 16 条に規定する署名用電子証明書失効情報又は法第 35 条に規定する利用者証明用電子証明書失効情報をいう。
(18)	失効記録	特定の日における失効情報の集合物をいう。
(19)	失効情報ファイル	法第 16 条に規定する署名用電子証明書失効情報ファイル又は法第 35 条に規定する利用者証明用電子証明書失効情報ファイルをいう。
(20)	署名検証者	法第 17 条第４項に規定する署名検証者をいう。
(21)	利用者証明検証者	法第 36 条第２項に規定する利用者証明検証者をいう。
(22)	署名確認者	法第 17 条第５項に規定する署名確認者をいう。
(23)	団体署名検証者	法第 17 条第６項に規定する団体署名検証者をいう。
(24)	署名検証者等	署名検証者及び団体署名検証者をいう。
(25)	保存期間に係る失効情報	法第 18 条第１項に規定する保存期間に係る署名用電子証明書失効情報及び法第 37 条第１項に規定する保存期間に係る利用者証明用電子証明書失効情報をいう。
(26)	対応証明書の発行の番号	法第 18 条第３項に規定する対応証明書の発行の番号をいう。
(27)	保存期間に係る失効情報ファイル	法第 18 条第２項に規定する保存期間に係る署名用電子証明書失効情報ファイル及び法第 37 条第２項に規定する保存期間に係る利用者証明用電子証明書失効情報ファイルをいう。
(28)	認証業務情報	法第 44 条第１項に規定する認証業務情報をいう。
(29)	発行手数料	利用者が電子証明書の発行を受けた際に納付する手数料をいう。
(30)	個人番号カード	行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）第２条第７項に規定する個人番号カードをいう。
(31)	住基カード	行政手続における特定の個人を識別するための番号の利用等に関する法律の施行に伴う関係法律の整備等に関する法律（平成 25 年法律第 28 号）第 20 条第１項に規定する住民基本台帳カードをいう。
(32)	外国人住民	住民基本台帳法（昭和 42 年法律第 81 号）第 30 条の 45 に規定する外国人住民をいう。
(33)	統合端末	告示第１条第３号に規定する統合端末をいう。
(34)	タッチパネル	暗証番号を設定する際に利用する入力装置をいう。
(35)	鍵ペア生成装置	告示第１条第４号に規定する鍵ペア生成装置をいう。
(36)	基本４情報	住民基本台帳法第７条第１号から第３号まで及び第７号に掲げる事項（同号に掲げる事項については、住所とする。）をいう。
(37)	旧氏	住民基本台帳法施行令（昭和 42 年政令第 292 号）第 30 条の 13 に規定する旧氏をいう。
(38)	旧氏記載者	住民基本台帳法施行令第 30 条の 14 第１項に規定する旧氏記載者をいう。
(39)	通称	住民基本台帳法施行令第 30 条の 16 第１項に規定する通称をいう。
(40)	代替文字	統合端末にて表示不可能な文字に代替する文字をいう。
(41)	本人確認書類	申請者や代理人等の本人確認のために用いる書類をいう。
(42)	暗証番号	規則第６条第２項に規定する署名利用者符号を利用するために用いる暗証番号又は第 42 条第２項に規定する利用者証明利用者符号を利用するために用いる暗証番号をいう。
(43)	シリアル番号	法第７条第１号に規定する署名用電子証明書の発行の番号又は法第 26 条第１号に規定する利用者証明用電子証明書の発行の番号をいう。

3　公的個人認証サービスの運用方針

(1) 公的個人認証サービスの運用に当たっては、法第１条の趣旨に則り、電子署名及び電子利用者証明の円滑な利用の促進を図り、もって住民の利便性の向上並びに国及び地方公共団体の行政運営の簡素化及び効率化に資することを旨とし、事務処理の効率化及び合理化に努めるとともに、公的個人認証サービスの十分なセキュリティの実現を図る観点から、電子署名及び電子利用者証明に係る認証業務の適正な管理を図るものとする。

(2) 署名用電子証明書は、インターネット等によるオンライン手続における利用者の本人確認手段であり、また、利用者証明用電子証明書は、利用者本人であることの確かな確認手段であるため、その発行に当たっては、慎重かつ正確な本人確認手続をとらなければならない。電子証明書の利用者の実在性及び本人性に疑わしさが生じるようでは、その他のあらゆる要件を具備していても、住民に対する公的個人認証サービスの任務を果たし得るものではない。このために、市区町村長は次の点に留意の上、電子証明書の発行要求を行わなければならない。

ア　電子証明書は、自市区町村の住民基本台帳に記録されている者の申請によって発行されなければならない。

イ　申請者の発行申請書に記載された基本４情報（申請者が旧氏記載者である場合にあっては基本４情報及び旧氏、通称が住民票に記載されている外国人住民である場合にあっては基本４情報及び通称。以下第１において同じ。）を住民基本台帳の記録事項と照合し、当該申請者が住民基本台帳に記録されている者であることの確認を行う。

ウ　本人確認書類等で申請者の本人確認を行う。

エ　申請者の本人確認において、疑義が生じた場合には電子証明書の発行申請を受理しない。

オ　統合端末から取得した住民基本台帳の基本４情報をもとに電子証明書の発行要求を行う。

なお、代理人を通じての申請も可能であり、その場合、代理人に関する厳格な本人確認及び申請者本人の意思確認が必要である。

(3) 電子証明書の本人確認保証の正当性は、この制度の生命ともいうべきものである。したがって、機構はあらゆる手段を講じてその電子証明書の正当性を確保することに努めなければならない。機構は、何らかの理由により有効期間内であるにも関わらずその効力を失った電子証明書の迅速な把握に努め、その結果を失効情報として記録、管理し、署名検証者等及び利用者証明検証者に提供しなければならない。

(4) 利用者の本人確認の保証という性格上、電子証明書を利用する者は以下の点に留意して、電子証明書の厳正かつ適切な管理を行わなければならない。

ア　発行申請書、失効申請書等への正確な内容の記載

イ　秘密鍵及び当該秘密鍵を格納したICカードの安全な管理

ウ　ICカードに格納された秘密鍵を活性化する暗証番号の安全な管理

エ　秘密鍵が紛失・危殆化した場合等の速やかな失効届出

4　制度概要

(1) 公開鍵基盤

ア　公開鍵暗号方式

公開鍵暗号方式とは、電磁的方式による申請、届出等における暗号化及び電子署名というセキュリティ対策を実現可能とする暗号技術である。

（ア）暗号化

情報を暗号化し、意図しない人物に読まれることを防ぐことにより、当該情報に守秘性を付与する。

（イ）電子署名

情報の作成者を特定でき、当該情報において改変が行われていないことを確認する。公的個人認証サービスでは、公開鍵暗号方式を電子署名のための技術として利用している。公開鍵基盤の基盤技術である公開鍵暗号方式では、対となる２つの暗号鍵を用いる。ここでいう鍵とは、情報の暗号化や復号を行う際に用いるデータである。この２つの鍵はそれぞれ公開鍵と秘密鍵と呼ばれ、これら２つの鍵の組み合わせを鍵ペアと呼ぶ。

公的個人認証サービスでは、市区町村長は、鍵ペア生成装置を用いて鍵ペアを作成し、当該鍵ペアを IC カードに記録する。なお、作成された鍵ペアのうち公開鍵は住所地市区町村長を経由して、機構に通知されなければならない。

公開鍵暗号方式では、一方の鍵で暗号化した情報は、その対となる鍵でないと復号できないという性質を持つ。送信者は所有する秘密鍵を使用して情報を暗号化し、受信者に送信する。受信者は公開されている送信者の公開鍵を使用して暗号文を復号する。受信者は公開鍵で復号できることすなわち送信者の秘密鍵で暗号化されたことを確認することにより、送信者の真正性と送信されたメッセージの完全性を確認できる。

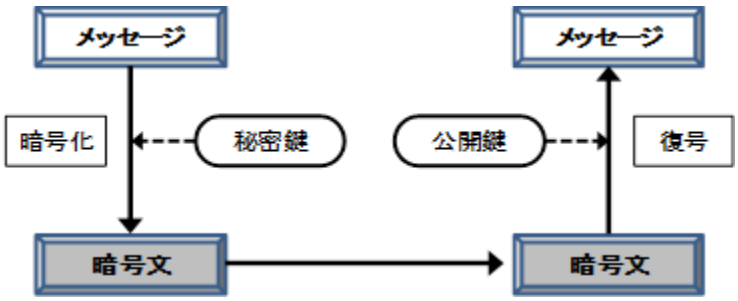


図 1-2　公開鍵暗号方式

イ　電子署名

公開鍵は誰にでも取得できるため、秘密鍵で暗号化を行っても情報の守秘性の確保にはならないが、秘密鍵は特定の個人のみ所有していることから、電子文書の認証と完全性の保証を実現することが可能である。

署名者である送信者は、署名を行いたいメッセージに対してハッシュ関数という技術を用い、ハッシュ値と呼ばれるデータに変換して出力する。電子署名とは、当該メッセ

ージのハッシュ値を秘密鍵で暗号化したものである。送信者はメッセージ、生成した電子署名及び電子証明書を受信者に送信する。受け取った受信者は、送信者の公開鍵を使用して電子署名を復号したハッシュ値と、送られてきたメッセージから生成したハッシュ値を照合することにより、送信者が署名者本人であること及びメッセージが改ざんされていないことを確認できる。

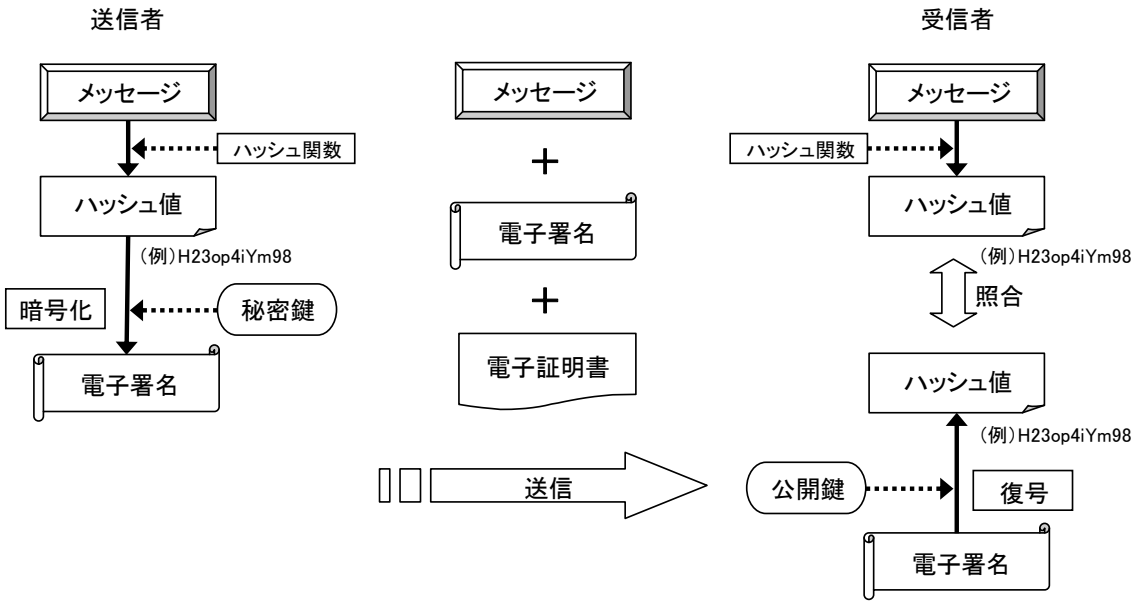


図 1-3　電子署名

ウ　署名用電子証明書を使った利用例

イで説明した電子署名技術を応用した例として、署名用電子証明書、利用者証明用電子証明書を用いた例を示す。

署名用電子証明書は、インターネットを通じたオンラインの申請や届出を行う際、他人による成りすましやデータの改ざんを防ぐために用いる本人確認の手段となる。署名用電子証明書を用いて、申請書などの情報に電子署名を付すことにより、確かに本人が送付した情報であることを示すことができる。

署名者である利用者は、署名を行いたいドキュメントをハッシュ化し、その結果に対して署名用電子証明書に係る秘密鍵（署名利用者符号）で暗号化し、電子署名を生成する。利用者はドキュメント、生成した電子署名及び署名用電子証明書をサービス提供者（署名検証者又は署名確認者）に送信する。受け取ったサービス提供者は、利用者の公開鍵を使用して電子署名を復号したハッシュ値と、送られてきたドキュメントから生成したハッシュ値を照合することにより、利用者が署名者本人であること及びメッセージが改ざんされていないことを確認できる。

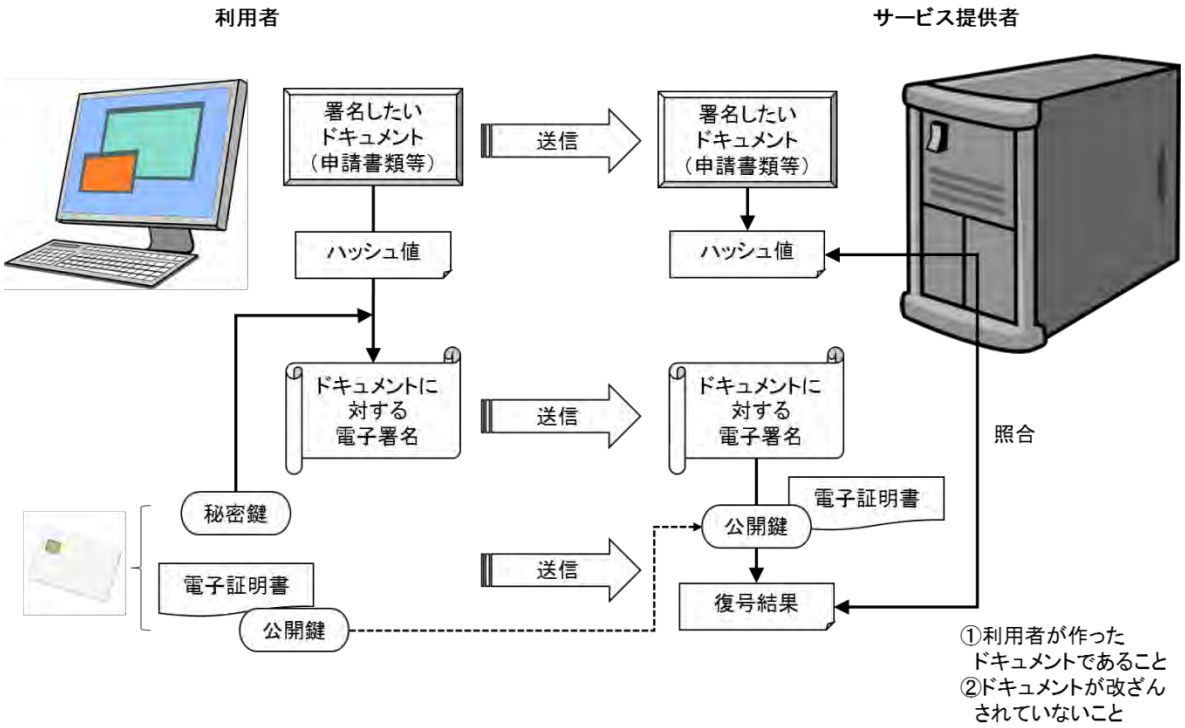


図 1-4　署名用電子証明書の利用例

エ　利用者証明用電子証明書を使った利用例

利用者証明用電子証明書は、インターネット上に提供される Web ページに対するログイン認証を ID／パスワードによるよりも安全に行うために用いる。

ログインを行う利用者には、サービスを提供するサーバーから、チャレンジコード（ログインのたびに異なる乱数）が送付される。利用者は、チャレンジコードに対して、秘密鍵を用いて暗号化し、その結果をサーバーに送信する。サービス提供者は、利用者から送られてきた情報を利用者の公開鍵で復号したものと、自身が送信したチャレンジコードを照合することで、利用者本人がログインしてきたことを確認することができる。

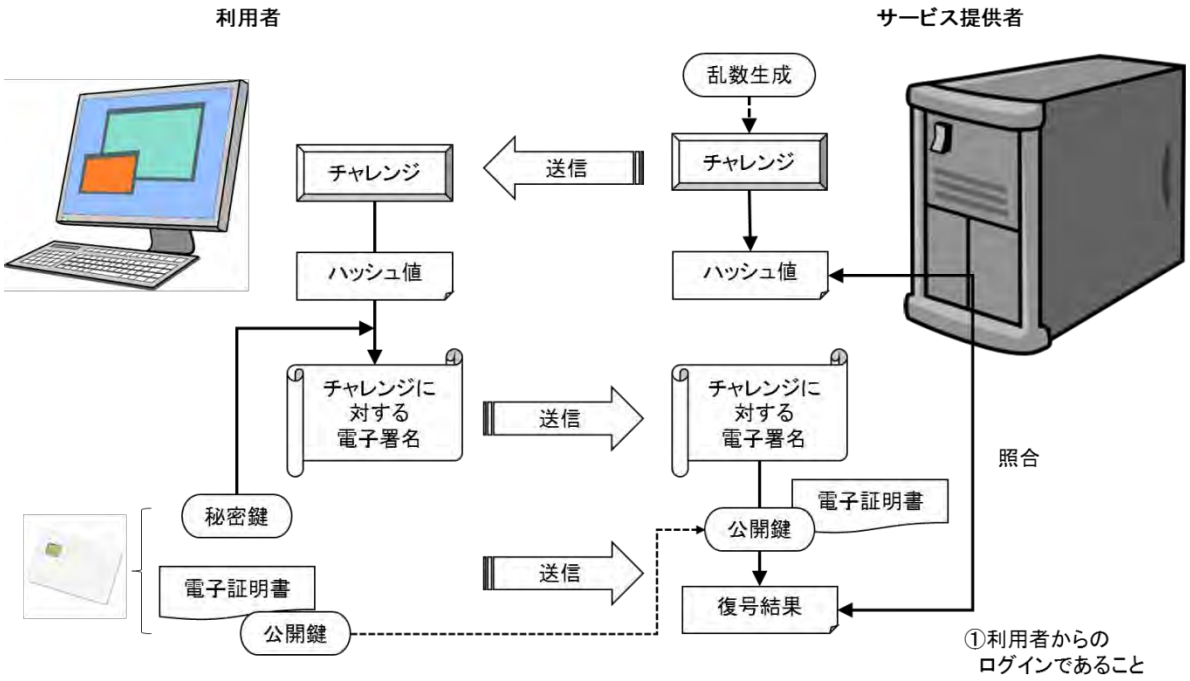


図 1-5　利用者証明用電子証明書の利用例

(2) 電子証明書

ア　意義

公開鍵暗号方式を利用する際には、受信者に公開鍵を送信する必要が生じる。しかし、ネットワーク経由での通信では通信相手を確認できないため、第三者が送信者に成りすまして公開鍵を送信する可能性がある。

公的個人認証サービスでは、機構が公開鍵の所有者に対して電子証明書を発行することにより、以下の２点について保証する。

（ア）署名用電子証明書の公開鍵と所有者の基本４情報及び署名用電子証明書の発行の番号との結びつき

（イ）利用者証明用電子証明書の公開鍵と利用者証明用電子証明書の発行の番号との結びつき

イ　規格

（ア）電子証明書の種類と用途

公的個人認証サービスでは、用途に応じて２つの電子証明書を利用することができる。

A　署名用電子証明書

文書が改ざんされていないことの確認及びインターネット等によるオンライン手続における利用者の本人確認の手段として利用される。

B　利用者証明用電子証明書

インターネット等におけるログイン等において、本人であることを証明する際に利用される。

（イ）記録事項

署名用電子証明書には、次に掲げる事項が記録される（法第 7 条、規則第 14 条）。

A　署名用電子証明書の発行の番号
B　発行年月日
C　有効期間の満了する日
D　署名利用者検証符号
E　基本 4 情報
F　当該電子証明書を発行した者の名称（機構）

等

利用者証明用電子証明書には、次に掲げる事項が記録される（法第 26 条、規則第 50 条）。

A　利用者証明用電子証明書の発行の番号
B　発行年月日
C　有効期間の満了する日
D　利用者証明利用者検証符号
E　当該電子証明書を発行した者の名称（機構）

等

（ウ）記録媒体

電子証明書が記録可能な媒体は、個人番号カード並びにデジタル庁及び総務省から別途通知される IC カードである（法第３条第４項、法第 22 条第４項、規則第７条、規則第 43 条、告示第６条）。

（エ）有効期間

電子証明書の有効期間は、電子証明書の種類に応じ、それぞれ発行の日から次に掲げる日のうちいずれか早い日までとする（法第５条、法第 24 条、規則第 13 条、規則第 49 条）。

A　署名用電子証明書の有効期間（規則第 13 条）
　(A) 発行の日後の申請者の５回目の誕生日（有効期間が満了する日までの期間が３月未満となった場合に、発行の申請を行い新たな署名用電子証明書の発行を受けるときにあっては、６回目）
　(B) 申請者が利用者証明用電子証明書の発行を受けている場合には、その有効期間が満了する日
　(C) 当該署名用電子証明書が記録された個人番号カードの有効期間が満了する日
B　利用者証明用電子証明書の有効期間（規則第 49 条）

(A) 発行の日後の申請者の５回目の誕生日（有効期間が満了する日までの期間が３月未満となった場合に、発行の申請を行い新たな利用者証明用電子証明書の発行を受けるときにあっては、６回目）

(B) 当該利用者証明用電子証明書が記録された個人番号カードの有効期間が満了する日

ウ　発行

住民基本台帳に記録されている者は、その者が記録されている住民基本台帳を備える市区町村の市区町村長を経由して、機構に対し、自己に係る電子証明書の発行の申請を行うことができる（法第３条第１項、法第 22 条第１項）。

自己に係る電子証明書の発行申請をしようとする者は、基本４情報等が記載された申請書を、住所地市区町村長に対して提出する（法第３条第２項、法第 22 条第２項）。

申請を受けた住所地市区町村長は、申請者が当該市区町村の住民基本台帳に記録されている者であることの確認を行う（法第３条第３項、法第 22 条第３項）。

住所地市区町村長は鍵ペア生成装置を利用して鍵ペアを生成し、IC カードに記録し、生成した公開鍵を機構に通知する（法第３条第４項及び第５項、法第 22 条第４項及び第５項）。

通知を受けた機構は、総務省令で定めるところにより、電子署名を行った当該申請に係る電子証明書を発行し、これを住所地市区町村長に通知する（法第３条第６項、法第 22 条第６項）。

住所地市区町村長は、発行された電子証明書を申請者の IC カードに記録する（法第３条第７項、法第 22 条第７項）。

なお、電子証明書を発行した機構は、総務省令で定めるところにより、当該電子証明書及び申請者の住民票コードを電磁的記録媒体に記録し、これを政令で定める期間（電子証明書の発行の日から当該電子証明書の有効期間の満了すべき日の翌日から起算して 10 年を経過する日まで）保存する（法第８条、法第 27 条、令第２条、令第 18 条）。

エ　失効

電子証明書は有効期間が満了した場合、その効力を失う（法第５条、法第 15 条第１項第１号、法第 24 条、法第 34 条第１項第１号、規則第 13 条、規則第 49 条）。

また、電子証明書が有効期間内であるにも関わらず、次に掲げる事項のいずれかに該当するときは、その効力を失う（法第 15 条第１項第１号から第４号まで、法第 34 条第１項第１号から第４号まで）。

（ア）利用者が任意に失効を申請した場合

（イ）秘密鍵が漏えい又は毀損等した場合

（ウ）利用者の異動等の通知があった場合

（エ）当該電子証明書に記載された事項について記録誤り等があった場合

（オ）発行者署名符号が漏えい又は毀損等した場合

オ　更新

現在有効な電子証明書を取得している者が、当該電子証明書の有効期間満了が近づいている等の理由で、当該電子証明書の失効手続と、当該電子証明書が記録されたＩＣカードへの新たな電子証明書の発行手続とを、新旧の電子証明書の基本４情報の実質的な変更（市町村合併に伴う住所の変更や住所又は氏名の代替文字の使用等は実質的な変更に含まれない。）を伴わない形で、連続的に行うことがある。この場合の連続した手続のことを事務処理上「更新」と称する場合がある。

「更新」とはあくまで事務処理上の呼称であり、これら手続の法令上の性格は通常の失効及び発行である。

なお、「更新」の場合の電子証明書の有効期間は、署名用電子証明書にあっては、イ（エ）A(A)の括弧書きに、利用者証明用電子証明書にあっては、イ（エ）B（A）の括弧書きに、それぞれ記載のとおりである。

(3) 失効情報及び失効情報ファイル

ア　意義

失効情報は、電子証明書の特定の日付における有効性を判断するためのものである。また、失効情報ファイルは失効情報のリストである失効情報の集合物であり、過去の時点における電子証明書の失効状況を確認するためのものである(法第16条、法第35条)。

なお、特定の日における失効情報の集合物である失効記録があわせて作成される。

イ　情報内容

（ア）記録事項

失効情報は、失効した電子証明書のシリアル番号、失効した年月日、失効事由であり、当該情報は失効記録に記録される。失効事由には以下の事項が挙げられる。

(A) 利用者の秘密鍵の危殆化
(B) 発行者署名符号の危殆化
(C) 証明書記録事項の変更
(D) 更新のための失効
(E) 利用者の意思によるサービスの停止

失効記録は、失効情報のリスト、失効記録の発行者及び発行者署名等から構成される。有効期間満了となった電子証明書に係る失効情報は失効記録には記載されない。

失効情報ファイルは、失効情報のリストである失効情報の集合物であって、失効情報を電子計算機を用いて検索することができるように体系的に構成したものをいう。

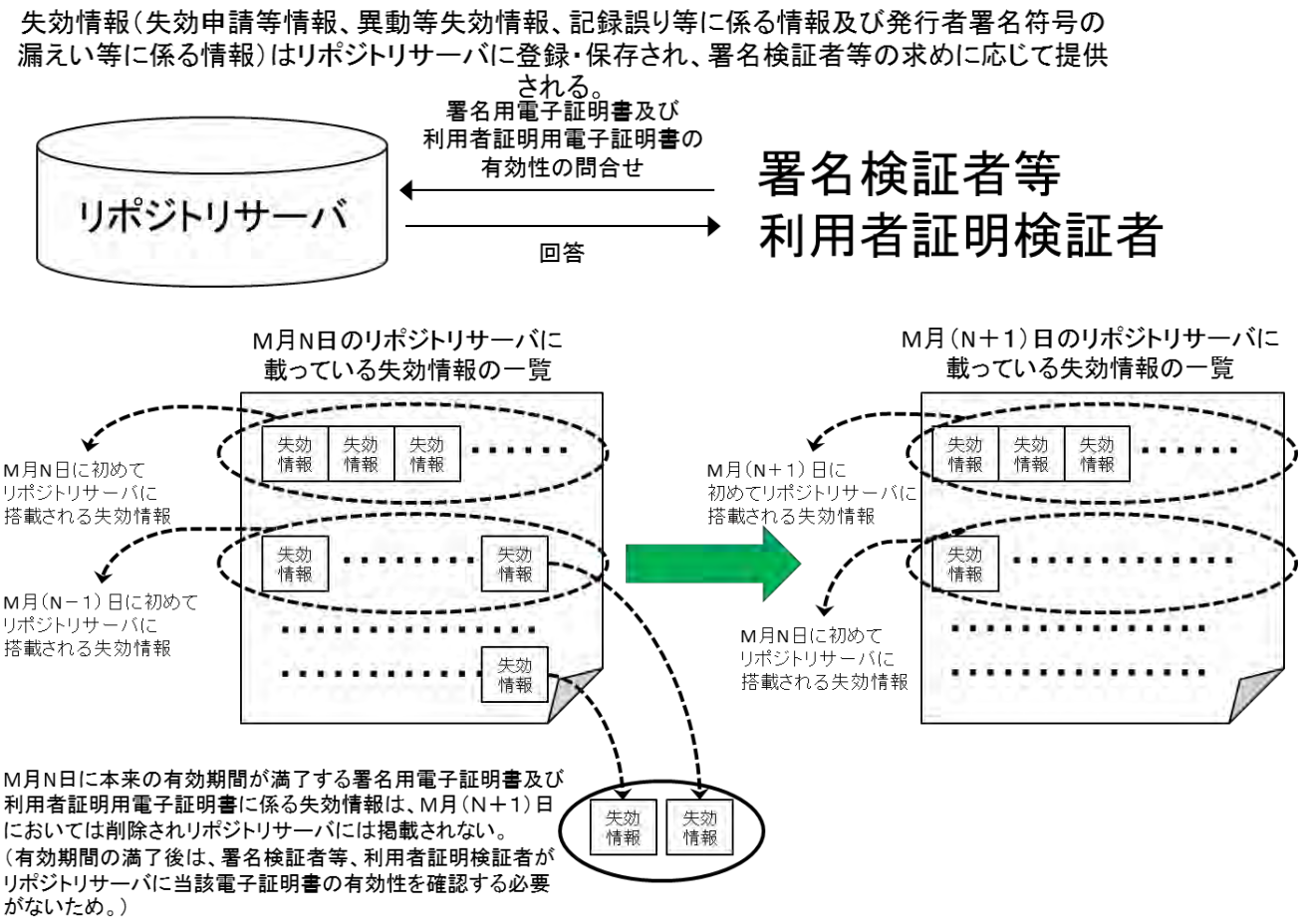
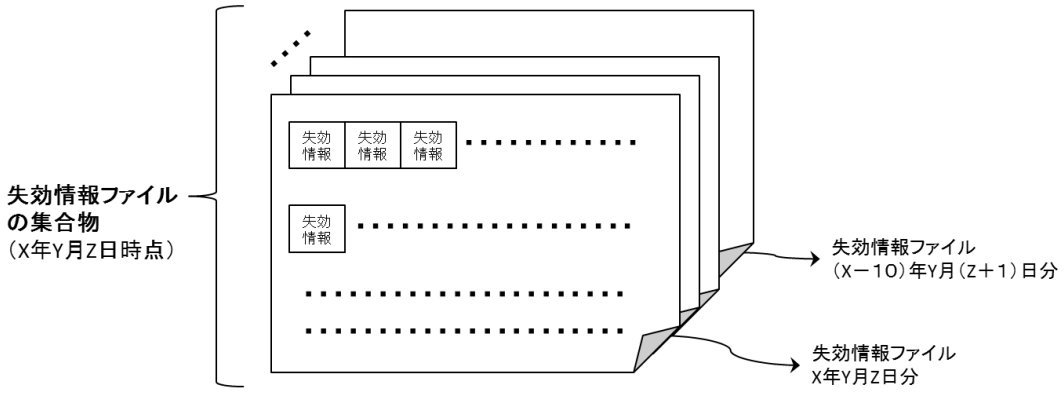


図 1-6　失効情報及び失効記録



失効情報ファイルは、ある日における失効情報の一覧表ともいうべきもので、24時間ごとに作成され、後日紛争が生じたときの証拠となるものとして、作成された日から10年間保存される。署名検証者等及び利用者証明検証者は、後日、紛争の証拠とするため、保存期間に係る失効情報ファイルの提供を求めることができる。

図 1-7　失効情報、失効記録及び失効情報ファイル

（イ）保存期間

失効情報は当該失効情報の記録を開始した日から、当該失効情報に係る電子証明書の有効期間の満了する日まで保存される（令第３条から第６条まで、令第 19 条から令第 22 条まで)。

また、失効情報ファイルは、作成した日から 10 年間保存される（令第７条、令第 23 条)。

ウ　提供

電子証明書が有効期間内であるにも関わらず、その効力を失った場合、機構は総務省令の定めるところにより、当該失効情報を電磁的記録媒体に記録し、これを当該記録を開始した日から当該失効情報に係る電子証明書の有効期間の満了する日まで保存し（法第 11 条から第 14 条まで、法第 30 条から第 33 条まで、令第３条から第６条まで、令第 19 条から第 22 条まで)、電子証明書の有効性の確認をしようとする署名検証者等及び利用者証明検証者の求めがあったときは、政令で定めるところにより、速やかに、保存期間に係る失効情報の提供を行う（法第 18 条第１項、法第 37 条第１項、令第 13 条、令第 24 条)。

また、機構は、総務省令の定めるところにより、失効情報ファイルを定期的に作成し、これを作成した日から 10 年間保存し（法第 16 条、法第 37 条、令第７条、令第 23 条)、署名検証者等及び利用者証明検証者の求めに応じ、政令で定めるところにより、提供する（法第 18 条第２項、法第 37 条第２項)。

署名検証者等及び利用者証明検証者は有効性を確認したい電子証明書に関して、OCSP レスポンダと呼ばれるサーバに対してリアルタイムに問い合わせをすることが可能である（告示第 33 条第１項、告示第 36 条第１項)。

また失効記録は、リポジトリと呼ばれるサーバに格納され、署名検証者等及び利用者証明検証者に提供される。署名検証者等及び利用者証明検証者は定期的にリポジトリサーバから失効記録を取得することで、当該電子証明書の有効性を確認することも可能である（告示第 33 条第１項、告示第 36 条第１項)。

更に機構は、署名検証者等及び利用者証明検証者の求めに応じ、保存期間に係る失効情報ファイルを提供する（令第 14 条)。

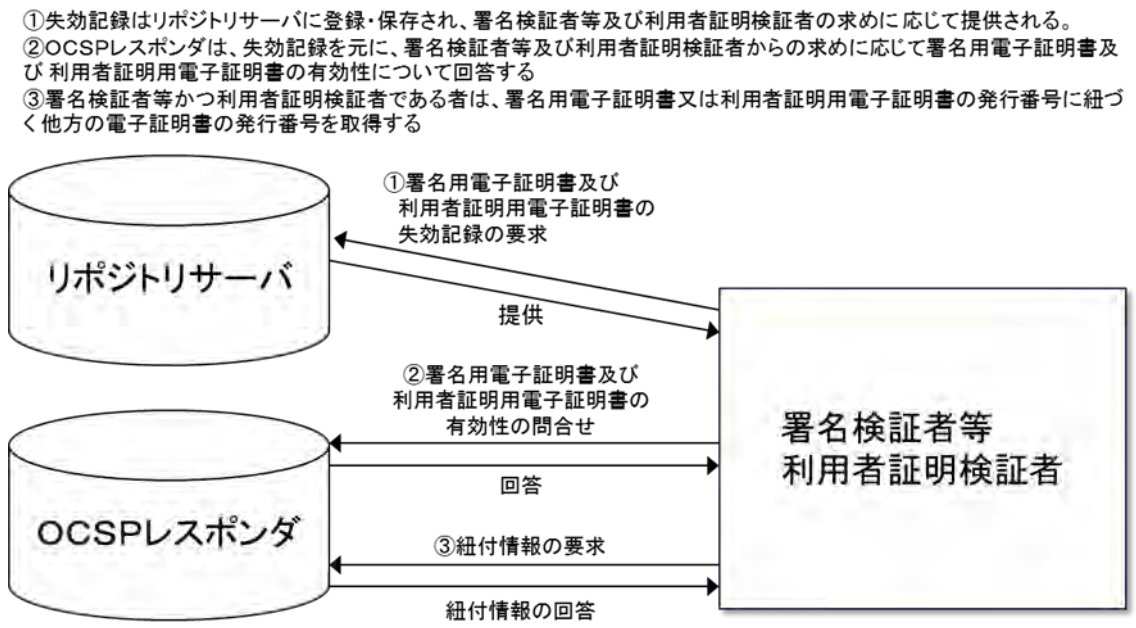


図 1-8　リポジトリサーバ及び OCSP レスポンダ

(4) 登場者

ア　機構

機構は、市区町村長と相互に連携・協力して、電子証明書その他証明書の発行、発行記録の記録及び保存、電子証明書の失効申請／届出の受付及び処理、失効情報の記録及び保存、失効情報ファイルの作成及び保存、電子証明書の有効性を確認する手段の提供、対応証明書の発行の番号の提供等の業務を行う。

また、利用者に対して、利用者が国又は地方公共団体の機関からオンラインで受け取った文書の電子署名の検証に必要となる官職及び職責証明書の有効性を確認する手段を提供する。

イ　市区町村長

市区町村長は、電子証明書の発行申請及び失効申請の受付、申請者の本人性の確認、機構の発行した電子証明書の申請者への交付等の業務を行う。

ウ　利用者

住民基本台帳に記録されている者で、電子証明書の発行を受けた者のことをいう（電子証明書の発行を受けるまでは申請者という）。国又は地方公共団体等との間のオンライン申請・届出等や民間事業者との間のオンライン取引等において、電子証明書を利用することができる。

また、機構に対して自己に係る認証業務情報について、その開示及び当該開示に係る認証業務情報について訂正等を請求することができる。（開示請求及び訂正等請求は、サービスの利用を取りやめた後も認められる。）

また、国又は地方公共団体の機関からオンラインで受け取った文書の電子署名の検証において、官職及び職責証明書の有効性を確認する。

エ　署名検証者

次の者のうち、署名用電子証明書の有効性を確認する手段の提供を受けることについて法第 17 条第１項の規定に基づき機構にあらかじめ届け出て、アクセス権を付与された者をいう。

①情報通信技術を活用した行政の推進等に関する法律（平成 14 年法律第 151 号）第３条第２号に規定する行政機関等

②裁判所

③行政機関等に対する申請、届出その他の手続に随伴して必要となる事項につき、電磁的方式により提供を受け、行政機関等に対し自らこれを提供し、又はその照会に応じて回答する業務を行う者として行政庁が法律の規定に基づき指定し、登録し、認定し、又は承認した者

④電子署名及び認証業務に関する法律（平成 12 年法律第 102 号）第８条に規定する認定認証事業者

⑤電子署名及び認証業務に関する法律第２条第３項に規定する特定認証業務を行う者であって政令で定める基準に適合する者として主務大臣（内閣総理大臣及び総務大臣）が認定する者

⑥前述の①～⑤以外の者で、署名利用者から通知された電子署名が行われた情報について当該署名利用者が当該電子署名を行ったこと又は利用者証明利用者が行った電子利用者証明について当該利用者証明利用者が当該電子利用者証明を行ったことの確認を政令で定める基準に適合して行うことができるものとして主務大臣が認定するもの

署名検証者は、機構から失効情報の提供等署名用電子証明書の有効性を確認する手段の提供を受け、利用者より受信した電子申請／届出に添付された署名用電子証明書の有効性を検証する。

オ　利用者証明検証者

エの①から⑥までに掲げる者で、利用者証明用電子証明書の有効性を確認する手段の提供を受けることについて法第 36 条１項の規定に基づき機構にあらかじめ届け出て、アクセス権を付与された者をいう。

利用者証明検証者は、機構から失効情報の提供等利用者証明用電子証明書の有効性を確認する手段の提供を受け、利用者より受信した利用者証明用電子証明書の有効性を検証する。

カ　団体署名検証者

次の団体又は機関のうち、署名用電子証明書の有効性を確認する手段の提供を受けることについて法第 17 条第５項の規定に基づき機構にあらかじめ届け出て、アクセス権を付与された者をいう。

①法律の規定に基づき他人の依頼を受けて行政機関等及び裁判所に対する申請、届出

その他の手続を行う者が所属する団体で政令で定めるもの

②行政機関等及び裁判所に対する申請、届出その他の手続に必要な電磁的記録を提供する者が所属する団体又は機関で政令で定めるもの

団体署名検証者は、機構から失効情報の提供等署名用電子証明書の有効性を確認する手段の提供を受け、署名確認者より受信した利用者に係る電子申請／届出に添付された署名用電子証明書の有効性を検証し、その結果を署名確認者に回答する。

キ　署名確認者

カの①の団体に所属する者及び同②の団体又は機関に所属する者であり、法第 20 条第１項の規定により、団体署名検証者を通じて署名用電子証明書の有効性を確認できる者をいう。