消防予第２６９号
平成29年９月４日

各都道府県消防防災主管部長
東京消防庁・各指定都市消防長
殿

消防庁予防課長
（公印省略）

「消防同意等の電子化に向けたシステム導入対応マニュアル」の送付について

行政機関への申請手続き等の電子化については、行政手続きオンライン化関係法の施行後、様々な分野で電子化に向けた取組みが進んでいます。

建築基準法（昭和２５年法律第２０１号）第６条に基づく確認申請についても、指定確認検査機関に対する戸建住宅の確認申請を中心に電子化への対応が進んでおり、今後、消防法（昭和２３年法律第１８６号）第７条に基づく、消防同意等の手続きについても電子化が進むことにより、申請者等の負担軽減のほか、各消防本部においても紙ベースの申請書及び図面等の情報（以下「申請図書等」という。）を電子的に取り込むことができるようになり、時間的及び作業的負担の軽減につながることや大量の空間を必要とする申請図書等の保管場所が必要なくなることから、限られたスペースにおける保管場所の課題等が解決するなどのメリットが期待されます。

消防同意等の電子化については、様々な対応方策が考えられることから、実効性が高い複数のパターンを紹介するとともに、それぞれの概要や必要な準備などを示すことにより、各自治体の予算やオンラインに係る条例、要綱などに鑑みて、各自治体に適した電子化の対応方策の採用が行えるようにした、消防同意等電子化の導入に向けたマニュアルを作成しました。

各都道府県におかれましては、貴管内の市町村又は消防本部に対して消防同意等の電子化に向けたシステムの導入に向けて、具体的に検討を行うように周知をお願いします。

なお、システム導入に向けた検討を行う消防本部を把握した際には、消防庁予防課へお知らせください。

＜連絡先＞
消防庁予防課予防係
柏原・鎌倉
Tel　(03)5253-7523
Fax　(03)5253-7533
mail　t2.kamakura@soumu.go.jp

消防同意等の電子化に向けた
システム導入対応マニュアル

平成 29 年 9 月

総務省消防庁予防課

目次

1. はじめに

行政機関への申請手続き等の電子化については、平成 15 年 2 月の行政手続きオンライン化関係法の法令整備後、様々な分野で電子化に向けた取組みが進んでいる。

建築分野においては CAD(Computer Aided Design) の普及から、より効果的に 3 次元情報等を取り扱える BIM（Building Information Modeling）への普及が加速し、設計業務の電子化が進んでおり建築基準法（昭和二十五年五月二十四日法律第二百一号）に基づく確認申請については「建築確認手続き等における電子申請の取扱いについて（技術的助言）」（平成 26 年 5 月国土交通省住宅局建築指導課長）、や「建築確認検査電子申請等ガイドライン」（平成 26 年 12 月一般財団法人 建築行政情報センター）により指定確認検査機関に対する戸建住宅の確認申請を中心に電子化への対応が進んでいるところである。電子化により設計図書の電子的作成から確認申請、検査、通知報告、台帳管理、関連図書の電子保存までの官民の関連機関におけるプロセス横断的な電子化を通じて効率化され、生産性が向上しつつある。

これを受け、平成 27 年 2 月 12 日には総務省消防庁予防課より「電子申請による建築確認に係る消防同意等事務の取扱について（通知）」（消防予第 53 号）が各都道府県消防防災主管部長、東京消防庁・各指定都市消防長へ通知された。今後、消防同意等の手続きについても電子化が進むことにより、申請者が窓口まで赴く等の負担軽減、手続きにかかる時間短縮のほか、消防機関においても文書の保存スペースを削減できる、電子化入力業務の効率化や住宅用火災警報器の設置状況を電子的に把握・管理できるなど、住宅防火対策の効率化が期待される。

本書では、「電子申請による建築確認に係る消防同意等事務の取扱について（通知）」を具現化し、消防機関によって少しずつ異なる消防同意等の手続きの現状を一部または全部電子化するためにはどの手法を選択すればよいか、消防機関が実態に応じて選択できるようにすることを目的とする。また、消防同意等の手続きの電子化の導入に必要な事項を整理し、具体的な電子化方法や導入の手順を明らかにすることにより、消防機関における円滑な電子化施策の推進に資することを目的とする。

2. 用語集

用語（A～Z）	解説
ASP （ Application Service Provider・エーエスピー）	ソフトウェアをインターネット等、通じ、利用者に遠隔から利用させる事業者のこと。また、そのようなサービスを指す。
CRL（Certificate Revocation List・シーアールエル）	「証明書失効リスト」ともいう。有効期限よりも前に失効された電子証明書の一覧。失効する理由としては、秘密鍵の紛失、記載内容の変更、利用の中止等が挙げられる。
ICT （ Information and Communication Technology・アイシーティー）	「情報通信技術」と訳されることが多い。情報処理および情報通信に関する技術、産業、設備、サービスなどの総称。
ISMS （ Information Security Management System・アイエスエムエス）	情報資産のセキュリティを確保、維持するための、人的、物理的、技術的、組織的な対策を含む、経営者を頂点とした組織的な取り組みのこと。組織が保護すべき情報資産について、機密性、完全性、可用性をバランス良く維持し改善することが ISMS の要求する内容の一つとなっている。JIS Q 27001（ISO/IEC 27001）にて規格が定められている。
LGWAN（エルジーワン）	正式名称は「総合行政ネットワーク」。地方公共団体の組織内ネットワークを相互に接続し、地方公共団体間のコミュニケーションの円滑化、情報共有の高度利用を図ることを目的とする、高度なセキュリティを維持した行政専用のネットワーク。
OCSP （ Online Certificate Status Protocol・オーシーエスピー）	電子証明書の失効状態を取得するための通信プロトコル。CRL の代替として策定された。有効性を問い合わせたい証明書について「有効」、「失効」、「不明」のいずれかの応答を署名付きで返す。
PAdES-LTV （ PDF Advanced Electronic Signatures Long Term Validation・パデス エルティーブイ）	PDF ファイルの内部構造の中へ署名データを埋め込む包含形式の長期署名フォーマット。署名対象ファイルはPDF形式に限定されるが、署名された PDF ファイルを単独で扱うことができ、Adobe Acrobat Reader でも検証できる利点がある。数十年といった長い期間、電子的に署名された文書を利用または保管するために使用される。「建築確認検査電子申請等ガイドライン（平成 26 年 12 月 ICBA）」に示された形式でもある。
PDF （ Portable Document	アドビシステムズ社が 1993 年に開発したファイルフォ

Format・ピーディーエフ）	ーマット。2008 年には、国際規格（ISO32000-1:2008)で PDF のフォーマットが標準化されている。作成したドキュメントを異なるパソコン環境で元のレイアウトどおりに表示・印刷可能な特性を持つ。
S/MIME（Secure / Multipurpose Internet Mail Extensions・エスマイム）	電子メールのセキュリティを高める標準規格のこと。S/MIME として使用可能な電子証明書を利用することで、メールへの電子署名や暗号化を行うことができ、なりすましや改ざん防止、機密保護に効果がある。送信者がメールに電子署名を行うことにより受信者は送信者の本人性やメールの内容が改ざんされていないことが確認できる。また送信者はメール本文や添付ファイルを暗号化して送信することもできる。
SSL/TLS 通信（Secure Sockets Layer / Transport Layer Security・エスエスエル/ティーエルエスつうしん）	インターネット上でデータを暗号化して通信する技術。通信者はサーバー用電子証明書を参照することによって通信先を確認することができ、通信データは電子証明書による暗号化通信によって第三者からの盗聴や改ざんから守られる。Internet Explorer11 の表示では白色のアドレスバーに鍵マークが表示され、通信が暗号化されていることが表示される。最も厳格な審査の元に発行される EV 証明書を利用している場合は、Internet Explorer11 の表示で緑色のアドレスバーに鍵マークと運営組織名と認証局名が交互に表示される。このアドレスバーは、赤色の場合、フィッシング詐欺サイトの可能性があり、安全なウェブサイトと区別することができる。
SHA-1/SHA-2（シャーワン/シャーツー）	暗号処理の際に使用されるハッシュ関数の一つ。SHA-1 の生成するハッシュ値は 160 ビット、SHA-2 の場合は 256 ビット、512 ビット等がある。ハッシュ値が長いほど安全とされ、SHA-1 を使用した証明書は廃止の方向に向かっており、SHA-2 の利用に移行している。
Web サーバー（ウェブサーバー）	Web システム上で、利用者側のコンピューターに対しネットワークを通じて情報や機能を提供するコンピューター（サーバー）およびソフトウェアのこと。
XML （ Extensible Markup Language・エックスエムエル）	ソフトウェア間の通信・情報交換に用いる言語の一種。ホームページ作成の際に利用する言語である HTML に類似している。

用語（五十音順）	解説
暗号アルゴリズム	暗号化する方法・手段。
公開鍵	公開鍵暗号方式で使用される一対の鍵の一つで、一般に公開される鍵。公開鍵は他人に知られても悪用される恐れはない。秘密鍵で暗号化されたデータは一対の公開鍵でのみ復号可能となり、電子署名の検証に用いる。
失効リスト	電子証明書の失効情報を掲載するリストで「ARL（Authority Revocation List)」と「CRL（Certificate Revocation List)」の 2 種類ある。ARL は認証局自身の電子証明書の失効情報を掲載し、CRL は認証局が発行した電子証明書の失効情報を掲載する。
証明書パス	利用者の電子証明書からルート証明書までの信頼の経路。電子署名の有効性を検証する場合、この経路を元に電子証明書の信頼性を確認する。
職責証明書	地方公共団体における組織認証基盤において発行された電子証明書。地方公共団体から発信される公文書に対して電子署名を行うために利用される。
署名検証	電子署名の有効性を確認する行為。「電子署名が付与された電子データが改ざんされていないこと」「電子証明書が有効であること」「電子証明書の信頼性が確認されていること」などを確認する。
スクリプト	簡易的なプログラムのこと。機械語への翻訳を必要とせずに実行できる。
政府認証基盤（GPKI）	政府が運用する認証基盤で、官職認証局、アプリケーション認証局、ブリッジ認証局の 3 つの電子認証局から構成される。各認証局からは職責証明書、サーバー証明書、相互認証証明書などがそれぞれ発行される。
組織認証局	地方公共団体組織認証基盤（LGPKI）において、職責証明書および利用者証明書を発行する認証局。職責証明書は、地方公共団体の首長、管理職等に発行し、利用者証明書は、総合行政ネットワーク内の各種システム利用者に発行している。
タイムスタンプ	ある時刻に、ある電子ファイルが存在していたことを証明する「存在証明」と、その内容が改ざんされていないことを証明する「完全性証明」を実現する仕組みのこと。有効期間は発行時点から約 10 年で設定されている。日本データ通信協会によるタイムスタンプ認定制度がある。また、利用方法により電子署名時刻の信頼性を確保する

	「署名タイムスタンプ」と長期にわたり電子署名の真正性を継続する「アーカイブタイムスタンプ」と区別して呼ばれることもある。
タイムスタンプ局	電子証明などの手段でタイムスタンプの付与およびタイムスタンプの有効性を保証する機関。電子データの「存在証明」と「完全性証明」を実現するうえで重要な役割を果たす。「時刻認証局」ともいう。
地方公共団体組織認証基盤（LGPKI）	地方公共団体の認証基盤で、組織認証局、アプリケーション認証局、ブリッジ認証局の 3 つの電子認証局から構成される。各認証局からは職責証明書、サーバー証明書、相互認証証明書などがそれぞれ発行される。
長期署名フォーマット	電子署名とタイムスタンプを組み合わせることで電子署名の検証期間を長期間に渡り維持する仕組み。
電子証明書	利用者の公開鍵が本人に帰属していることを証明するために認証局が電子的に発行する電子ファイル、公開鍵証明書とも呼ばれる。公開鍵証明書は公開鍵そのものを含み認証局の電子署名が付されている。なお、電子証明書ファイルには公開鍵とペアになる秘密鍵を含めることもできる。有効期間は発行時点から通常 5 年を超えない範囲で設定されている。
電子署名	電子ファイルに対して署名者の秘密鍵を用いて行う電子的な署名のことで小さいサイズの電子署名データとして作成される。PDF ファイルの場合電子署名データをファイル内に格納することもできる。署名済みの電子ファイルは署名者が誰であるか、また改ざんの有無が公開鍵を用いて確認でき、これを署名検証と言う。電子ファイルに電子署名をしたものと書面に押印したものは同等として扱うことができる。
登録局	電子認証局を構成する要素の一つであり、電子証明書発行のための審査・登録を行う機関のことで、「RA（Registration Authority)」ともいう。
登録分局	地方公共団体内に設置され、証明書の発行を受け付け、発行を行っている。
認証局	電子証明書の発行と失効を行う機関のことで、「CA（Certificate Authority)」ともいう。
発行局	電子認証局を構成する一つであり、電子証明書を発行する機関のことで「IA（Issuing Authority)」ともいう。
ハッシュ関数	疑似乱数を生成する一方向関数。どのようなコンピュー

	ターでもこの関数を利用すれば同じ入力値からは全く同じ出力値（ハッシュ値）が得られるが、入力値が少しでも異なっていた場合は、異なったハッシュ値が得られる。そのため、データやファイルを送信する際、入力側と出力側でハッシュ値を求め一致すれば、途中で改ざん等が発生していないことを確認できる。
ハッシュ値	電子ファイル等を一定の長さの文字に出力するハッシュ関数を用いて出力された文字列のことをいう。元の電子ファイルを少しでも変更するとハッシュ値はまったく違うものになる。ハッシュ値は電子署名の付与・検証の際に用いられる。
秘密鍵	公開鍵暗号方式で使用される一対の鍵の一つで、利用者本人のみが保有し一般に公開されない鍵。秘密鍵が他人に知られると悪用される恐れがあるため、厳重に管理する必要がある。本人のみが所持するものなので電子署名に用いられる。
ファイアウォール	ネットワークの結節点となる場所に設けて、コンピューターセキュリティ上の理由、あるいはその他の理由により「通過させてはいけない通信」を阻止するシステムのこと。
復号	暗号化された暗号文を解いて元の平文に戻すこと。
ブリッジ認証局	国・地方公共団体等の官職等を認証する認証局（行政機関等側 CA）と国民等を認証する認証局（国民等側 CA）との間の相互認証を行い、相互認証証明書を取り交わす認証局。このことにより他の認証局から認証されている者同士で安心してデータ通信することができる。
マルウェア	マルウェア（Malware）とは、不正な悪意あるソフトウェアの総称。ウイルス、ワーム、トロイの木馬、スパイウェア、アドウェア等がこれに含まれている。
ルート証明書	ルート認証局が、自身の正当性を証明するために発行する電子証明書。
ルート認証局	他の上位の認証局から証明書を受けない最上位の認証局であり、利用用途により異なる厳格な各審査基準を満たして運用している。

3.　本書内で使用する名称・略称について

用語（五十音順）	解説
1 号建築物（いちごうけんちくぶつ）	建築基準法第六条の分類で、特殊建築物（建築基準法別表第 1（い）欄の用途のもの）かつ　床面積＞100㎡の建築物。
行政手続きオンライン化法（ぎょうせいてつづきおんらいんかほう）	行政手続等における情報通信の技術の利用に関する法律（平成十四年十二月十三日法律第百五十一号）
建築主事（けんちくしゅじ）	政令で指定する人口二十五万以上の市において、その長の指揮監督のもとに、建築基準法第六条第一項の規定による確認に関する事務をつかさどらせるために、置かなければならない公務員のこと。また、市町村（人口二十五万以上の市を除く）は、その長の指揮監督のもとに、第六条第一項の規定による確認に関する事務をつかさどらせるために、建築主事を置くことができる。
建築主事等（けんちくしゅじとう）	建築主事または指定確認検査機関。
消防機関（しょうぼうきかん）	消防本部または消防署。
3 号建築物（さんごうけんちくぶつ）	建築基準法第六条の分類で、木造以外かつ　階数≧2　延べ面積＞200㎡　のどれかにあてはまる建築物。
指定確認検査機関等（していかくにんけんさきかんとう）	特定行政庁、建築主事または指定確認検査機関。
消防長等（しょうぼうちょうとう）	消防長または消防署長。
消防通知（しょうぼうつうち）	建築基準法（昭和二十五年五月二十四日法律第二百一号）第九十三条第 4 項に基づく消防長等への通知。
消防同意依頼（しょうぼうどういいらい）	指定確認検査機関等から消防機関へ消防法（昭和二十三年七月二十四日法律第百八十六号）第七条の規定に基づく建築物の確認等に対する同意を依頼すること。
消防同意依頼書（しょうぼうどういいらいしょ）	消防同意を指定確認検査機関等から管轄する消防機関へ依頼する際に渡す書類の表紙。
消防同意通知（しょうぼうどういつうち）	消防機関から指定確認検査機関等へ消防法第七条の規定に基づく建築物の確認等に対する同意を通知すること。
消防同意通知書（しょうぼうどういつうちしょ）	消防同意を消防機関から指定確認検査機関等へ通知する際に渡す書類の表紙。
消防同意（しょうぼうどうい）	消防法第七条の規定に基づく建築物の確認等に対する同意。

消防同意期間（しょうぼうどういきかん）	消防機関は 4 号建築物の場合、消防同意を求められた日から 3 日以内に、1～3 号建築物の場合は同意を求められた日から 7 日以内に同意を与えて、その旨を当該行政庁もしくはその委任を受けた者または指定確認検査機関に通知しなければならない。その同意を求められてから指定確認検査機関等に通知をするまでの期間。
消防同意等（しょうぼうどういとう）	消防法第七条の規定に基づく建築物の確認等に対する同意および建築基準法第九十三条第 4 項に基づく消防長等への通知。
消防同意等事務（しょうぼうどういとうじむ）	消防法第七条の規定に基づく建築物の確認等に対する同意および建築基準法第九十三条第 4 項に基づく消防長等への通知に係わる事務のこと。
消防同意等書類一式（しょうぼうどういとうしょるいいっしき）	消防同意を指定確認検査機関等から消防機関へ依頼する際または、消防長等への通知の際に渡す書類の一式。消防同意依頼書、確認申請書、建築計画概要書、図面等。
特定行政庁（とくていぎょうせいちょう）	建築主事を置く市町村の区域については当該市町村の長をいい、その他の市町村の区域については都道府県知事をいう。ただし、建築基準法第九十七条の二第一項または第九十七条の三第一項の規定により建築主事を置く市町村の区域内の政令で定める建築物については、都道府県知事とする。
特定行政庁等（とくていぎょうせいちょうとう）	特定行政庁、建築主事。
2 号建築物（にごうけんちくぶつ）	建築基準法第六条の分類で、木造かつ　階数≧3　延べ面積＞500㎡　高さ＞13m　軒の高さ＞9m　のどれかにあてはまる建築物。
4 号建築物（よんごうけんちくぶつ）	建築基準法第六条の分類で、木造かつ 階数≦2、延べ面積≦500 ㎡、高さ≦13m、軒の高さ≦9mの建築物。

4. 消防同意等電子化の基礎知識

本章では、建築確認申請における消防同意および消防通知の法的根拠と現状の建築主事または指定確認検査機関と消防機関との運用手続きについて解説する。

消防同意とは、消防法第七条および建築基準法第九十三条第 1 項に基づく消防長等の同意を指し、建築確認申請や許可申請などに伴い行われる。消防通知とは、建築基準法第九十三条第 4 項において規定されている消防長等への通知を指している。

以下、消防法第七条および建築基準法第九十三条の条文を示す。

消防法（昭和二十三年七月二十四日法律第百八十六号）
第七条　建築物の新築、増築、改築、移転、修繕、模様替、用途の変更若しくは使用について許可、認可若しくは確認をする権限を有する行政庁若しくはその委任を受けた者又は建築基準法 （昭和二十五年法律第二百一号）第六条の二第一項 （同法第八十七条第一項 において準用する場合を含む。以下この項において同じ。）の規定による確認を行う指定確認検査機関（同法第七十七条の二十一第一項 に規定する指定確認検査機関をいう。以下この条において同じ。）は、当該許可、認可若しくは確認又は同法第六条の二第一項 の規定による確認に係る建築物の工事施工地又は所在地を管轄する消防長又は消防署長の同意を得なければ、当該許可、認可若しくは確認又は同項 の規定による確認をすることができない。ただし、確認（同項 の規定による確認を含む。）に係る建築物が都市計画法 （昭和四十三年法律第百号）第八条第一項第五号 に掲げる防火地域及び準防火地域以外の区域内における住宅（長屋、共同住宅その他政令で定める住宅を除く。）である場合又は建築主事が建築基準法第八十七条の二 において準用する同法第六条第一項 の規定による確認をする場合においては、この限りでない。
〇２　　消防長又は消防署長は、前項の規定によつて同意を求められた場合において、当該建築物の計画が法律又はこれに基づく命令若しくは条例の規定（建築基準法第六条第四項 又は第六条の二第一項 （同法第八十七条第一項 の規定によりこれらの規定を準用する場合を含む。）の規定により建築主事又は指定確認検査機関が同法第六条の四第一項第一号 若しくは第二号 に掲げる建築物の建築、大規模の修繕（同法第二条第十四号 の大規模の修繕をいう。）、大規模の模様替（同法第二条第十五号 の大規模の模様替をいう。）若しくは用途の変更又は同項第三号 に掲げる建築物の建築について確認する場合において同意を求められたときは、同項 の規定により読み替えて適用される同法第六条第一項 の政令で定める建築基準法 令の規定を除く。）で建築物の防火に関するものに違反しないものであるときは、同法第六条第一項第四号 に係る場合にあつては、同意を求められた日から三日以内に、その他の場合にあつては、同意を求められた日から七日以内に同意を与えて、その旨を当該行政庁若しくはその委任を受けた者又は指定確認検査機関に通知しなければならない。

この場合において、消防長又は消防署長は、同意することができない事由があると認めるときは、これらの期限内に、その事由を当該行政庁若しくはその委任を受けた者又は指定確認検査機関に通知しなければならない。
〇３　　建築基準法第六十八条の二十第一項（同法第六十八条の二十二第二項 において準用する場合を含む。）の規定は、消防長又は消防署長が第一項の規定によつて同意を求められた場合に行う審査について準用する。

建築基準法（昭和二十五年五月二十四日法律第二百一号）

（許可又は確認に関する消防長等の同意等）

第九十三条　　特定行政庁、建築主事又は指定確認検査機関は、この法律の規定による許可又は確認をする場合においては、当該許可又は確認に係る建築物の工事施工地又は所在地を管轄する消防長（消防本部を置かない市町村にあつては、市町村長。以下同じ。）又は消防署長の同意を得なければ、当該許可又は確認をすることができない。ただし、確認に係る建築物が防火地域及び準防火地域以外の区域内における住宅（長屋、共同住宅その他政令で定める住宅を除く。）である場合又は建築主事若しくは指定確認検査機関が第八十七条の二において準用する第六条第一項若しくは第六条の二第一項の規定による確認をする場合においては、この限りでない。

２　　消防長又は消防署長は、前項の規定によつて同意を求められた場合においては、当該建築物の計画が法律又はこれに基づく命令若しくは条例の規定（建築主事又は指定確認検査機関が第六条の四第一項第一号若しくは第二号に掲げる建築物の建築、大規模の修繕、大規模の模様替若しくは用途の変更又は同項第三号に掲げる建築物の建築について確認する場合において同意を求められたときは、同項の規定により読み替えて適用される第六条第一項の政令で定める建築基準法令の規定を除く。）で建築物の防火に関するものに違反しないものであるときは、同項第四号に係る場合にあつては、同意を求められた日から三日以内に、その他の場合にあつては、同意を求められた日から七日以内に同意を与えてその旨を当該特定行政庁、建築主事又は指定確認検査機関に通知しなければならない。この場合において、消防長又は消防署長は、同意することができない事由があると認めるときは、これらの期限内に、その事由を当該特定行政庁、建築主事又は指定確認検査機関に通知しなければならない。

３　　第六十八条の二十第一項（第六十八条の二十二第二項において準用する場合を含む。）の規定は、消防長又は消防署長が第一項の規定によつて同意を求められた場合に行う審査について準用する。

４　　建築主事又は指定確認検査機関は、第一項ただし書の場合において第六条第一項（第八十七条の二において準用する場合を含む。）の規定による確認申請書を受理したとき若しくは第六条の二第一項（第八十七条の二において準用する場合を含む。）の規定による確認の申請を受けたとき又は第十八条第二項（第八十七条第一項又は第八十七条の二において準用する場合を含む。）の規定による通知を受けた場合においては、遅滞なく、これを当該申請又は通知に係る建築物の工事施工地又は所在地を管轄する消防長又は消防署長に通知しなければならない。

4.1 消防同意等の紙での手続き

《消防同意》

消防同意の手順を大別すると、指定確認検査機関等から建築物の所在地の消防機関へ同意を求められる「同意依頼の受付」、建築物が防火に関する法令の規定に適合している場合に同意する「消防同意等事務」、同意する旨を伝える「同意通知」から構成される。
指定確認検査機関等は、消防機関の同意通知を待って確認済証の交付を行う。

(1) 同意依頼の受付
- (ア) 指定確認検査機関等から消防機関へ消防同意依頼書、確認申請図書の正・副本（以下、消防同意等書類一式）と消防機関が指定した書類を添えて提出する。（正・副本以外に消防用を求める消防機関もある）
- (イ) 消防同意に使用する消防同意依頼書は任意様式であるが、消防機関によっては様式を指定する場合もある。
- (ウ) 原則、消防同意等書類一式は持ち込みであるが、指定確認検査機関では信書便で消防機関に送付することが多い。

(2) 消防同意等事務
- (ア) 消防同意等書類一式を受け付けた消防機関は、対象建築物について防火に関する法令の規定に照らして審査する。
- (イ) 消防同意の審査期間中に軽微な補正が必要になった場合、不明確な点が見つかった場合は、指定確認検査機関等にその旨を通知し、図面・説明書等の提出を求める。

(3) 同意通知
- (ア) 消防法第七条 2 項、建築基準法第九十三条第 2 項に従って、消防機関は対象建築物の構造、階数、延べ面積、高さ、用途等によって同意を求められた日から三日または七日以内に「同意する」旨を指定確認検査機関等に通知する。
- (イ) 同意した旨の通知方法としては 2 種類あり、1 つ目は、同意依頼時に提出

された確認申請書一面に同意印を押印する方法、2 つ目は同意した旨を別紙にする方法である。(平成 11 年 4 月 28 日【消防予第 92 号】消防法等の一部を改正する法律等の運用について（通知))

(ウ)指定確認検査機関等は、確認申請書の一面に同意印がある場合は、同意印が押印された確認申請書一式を正本として確認済証交付後に 15 年間保存する。別紙の消防同意通知書(消防同意をする旨が記載されている通知書)が添付される場合はこれを正本と併せて 15 年間保存する。(根拠法令：建築基準法第十二条第 8 項・第 9 項、建築基準法施行規則第六条の 3（台帳の記載事項等))

《消防通知》

消防通知は、確認申請を受け付けた旨を建築主事等から消防機関に消防通知書を原則持ち込みするが、郵送する場合もある。消防通知書は任意様式である。
消防同意対象外の建築確認申請が対象となる。

4.2 消防機関、特定行政庁等、指定確認検査機関での現状の消防同意等事務について

本マニュアルを作成するにあたり、消防機関、特定行政庁・建築主事、指定確認検査機関に対して現状の消防同意事務についてヒアリングを実施した。ヒアリング結果は、以下のとおりである。

4.2.1 消防機関

(1) 申請件数

都市部では、消防同意が多く、消防通知が少ないが、それ以外の地域では、消防同意より消防通知が多い傾向にある。都市部は、防火地域・準防火地域の指定地域が広いため消防通知が行えない地域が多いためだと考えられる。なお、4 号建築物の申請が最も多い。

(2) 申請先

建物の規模により申請先が消防本部または消防署になる地域、本部で一括して行う地域が存在した。

(3) 消防同意図面の保存期間について

消防同意等事務に係わる数日間のみ保管する場合や、1 年保存、建築物が竣工するまでとしている場合が多い。地域によっては 3 年保存や永年保存していることもある。

(4) 消防不同意、軽微な補正についてのフロー

消防不同意の場合、消防機関から指定確認検査機関等へ書類の返却等を行うことが多いが、地域によっては確認申請書や図面を返却しないこともある。

「軽微な補正」については、指定確認検査機関等を経由して設計者へ伝えられるフローとなっている消防機関もあるが、指定確認検査機関の了承を得て、直接設計者とやり取りを行うこともある。

事前同意を取り入れている地域については、消防機関と設計者が直接やり取りを行っている。

一部地域では、「軽微な補正」を実施しない代わりに「不同意」を実施する。

また、「軽微な補正」を運用で実施している消防機関では、消防同意期間中、軽微な補正を行っている期間を消防同意期間に含めない運用が多く見られた。別の消防機関では、消防同意期間内で軽微な補正を実施することができなかった場合、一旦、不受理とし、再び消防同意を求める運用を実施している。

(5) 拠点間運搬

定期的、もしくは不定期に消防車等で運搬をしている。また、管轄エリアが広いほど運搬業務の手間もかかっているため、電子化するメリットがあると考えられる。

(6) 消防同意・通知の電子化促進について

電子化を進めたいと考える地域は少なく、システムを構築に要する手間や予算の確保、紙ベースの申請との併用運用について等、問題となる点があるためである。

(7) 紙文書で多い申請書

各地域、点検報告に関する申請数が非常に多い。次いで、防火管理者の届出が多いようである。

(8) 電子的に審査をするうえで必要だと考えられること

窓口であれば直接修正や差し替えができる点を、電子化を行うにあたり考慮する必要がある。独自に事前同意の運用をしている地域に関しては、電子化するにあたり、運用方法が全国統一されるのであればそれに合わせるのが望ましいと考えられる。

(9) パソコン利用状況、インターネット接続状況について

ノートPCの利用が多い傾向にある。インターネット接続については、アクセス制限をかけている地域、インターネット接続可能端末と不可能端末を切り離している消防機関がある。

(10)セキュリティ対策

市等のセキュリティ基準に則って運用している。また、インターネット接続可能な端末と接続不可能な端末を切り離すことにより、情報漏洩のリスク等を回避している。

(11)管理台帳の使用について

管理台帳に建築概要等のデータを入力し、管理している地域が多い。書面から手入力しているため、入力に一申請あたり 10 分程度の時間を要する。

4.2.2 特定行政庁・建築主事

(1) 申請件数

建築確認申請については、80-90%の割合で指定確認検査機関が実施しており、現在は計画通知が主となっている。

(2) 申請先

消防本部に申請している地域がほとんどである。

(3) 消防本部等への送付手段

文書配送委託や逓送便での手段の他に、担当者が持参で持ち込んでいる地域もある。

(4) 建築確認検査業務の電子化について

現在のモニター画面上での審査や作業については厳しいと思われる。また、建築確認件数自体が減少傾向にある中で、電子化に向けて設備投資することは難しいと考えられる。

(5) パソコン利用状況、インターネット接続状況

ノート PC を利用している地域が多く、問題点として挙げられている図面の審査において厳しさがある。インターネット接続については、アクセス制限をかけている地域、インターネット接続可能端末と不可能端末を切り離している地域がある。

(6) セキュリティ対策

市等のセキュリティ基準に則って運用している。また、インターネット接続可能な端末と不可能な端末を切り離すことにより、情報漏洩のリスク等を回避している。

(7) 管理台帳の使用について

一般財団法人　建築行政情報センター（以下、ICBA）の建築行政共用データベースを利用している地域と、独自に開発した台帳システムを利用している地域、そのほか、既存製品であるパッケージソフトウェアを使用する地域がある。

(8) ICBA の建築行政共用データベースシステム利用状況

主に利用している機能としては、「建築士・事務所の登録」「処分状況チェック」「法令・大臣認定データベース」であり、「通知・報告配信システム」の利用は少なかった。

4.2.3　指定確認検査機関

(1) 申請先

事前に消防機関に問い合わせをし、申請先を把握している。

(2) 消防本部等への送付手段

郵便で送付している指定確認検査機関がほとんどだが、一部持参している指定確認検査機関もあった。

(3) 建築確認申請手続きの電子化を検討しているか

事前申請を含め、本申請を電子化している指定確認検査機関や、事前申請のみを電子化している指定確認検査機関があり、建築確認申請の手続きを電子化する動きについては、積極的であった。

(4) 電子化を進めるにあたって重要だと考えていること

電子証明書の取得を簡素化し低価格化することで、申請者にとって電子証明書の取得そのものの敷居を低くすることが必要だと考えている。また、書類の一部が書面だと電子の意義が薄れると考えられ、委任状の電子化も進められると良いという意見があった。

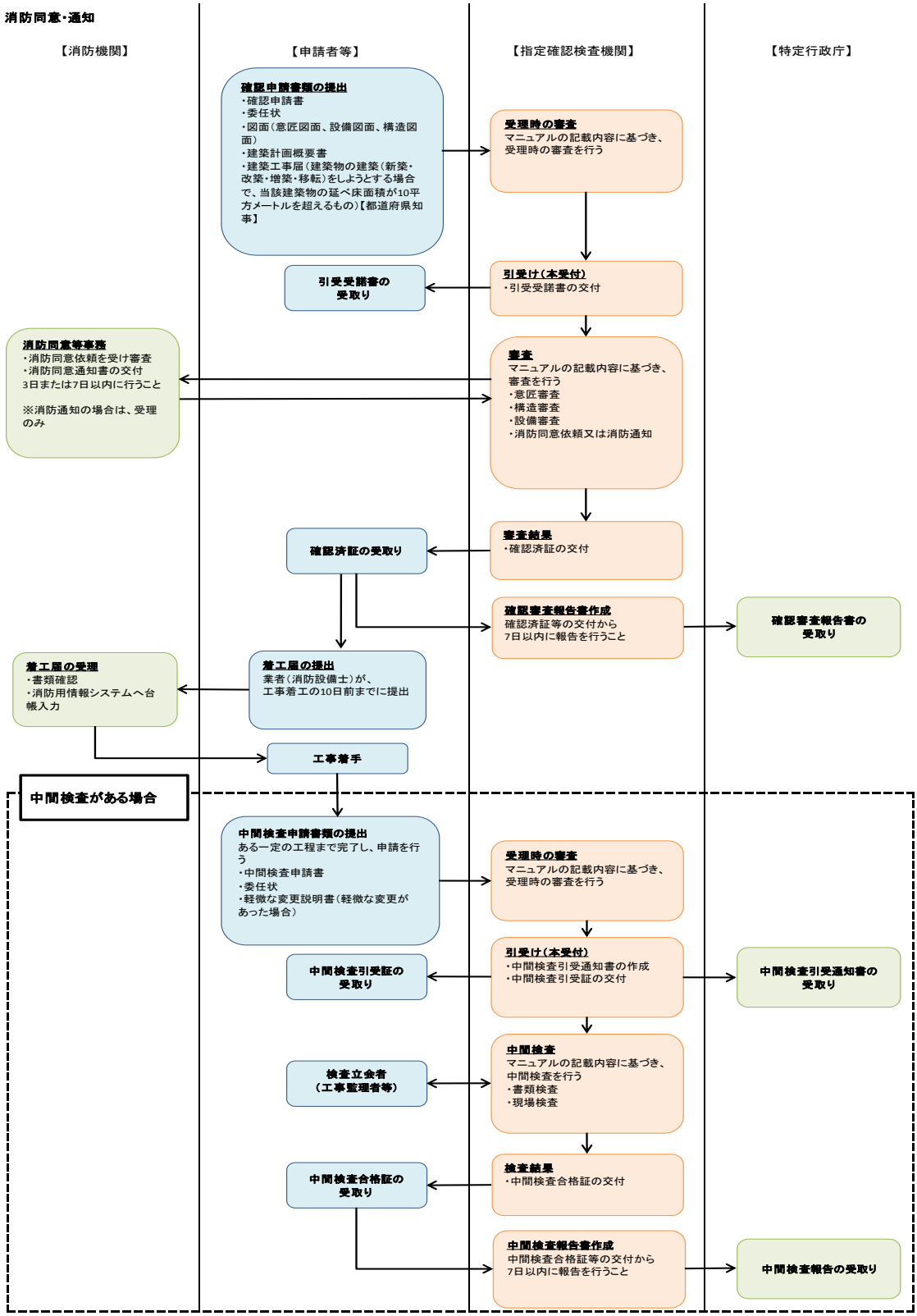
(5) セキュリティについて

確認申請を行っている指定確認検査機関では、ISMS で必要とされているセキュリティ事項をルールとして決めていることが多い。しかし、ISMS の認証取得は、手間とコストがかかるため、取得まで行っている指定確認検査機関は無かった。

(6) データ活用

台帳管理の使用について、大きく分けて二種類あり、ICBA の建築行政共用データベースシステムの台帳を利用している指定確認検査機関と、独自に開発したシステムを利用している機関に分かれる。比較的、規模の多い指定確認検査機関では、独自システムを利用している割合が高い。

4.2.4　一般的な消防同意事務を含むフロー



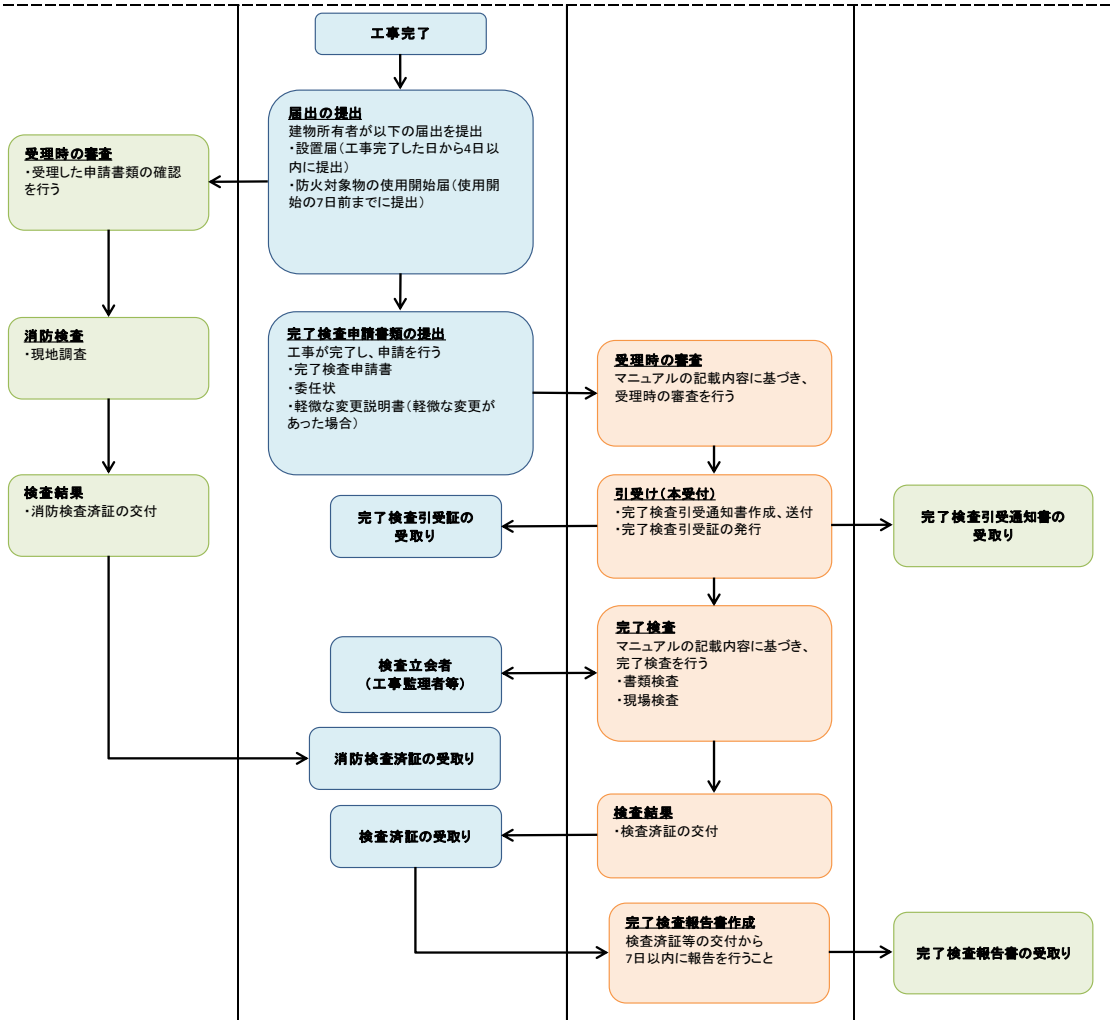


図 1　消防同意事務を含むフロー

4.3 建築確認申請の電子化について

建築確認申請の電子申請は、平成 26 年 5 月 7 日 国住指第 394 号の国土交通省住宅局建築指導課による技術的助言にて、建築確認申請の電子申請の取扱いが示された。その後、平成 26 年 12 月 17 日「建築確認手続き等における電子申請の実施にあたって（情報提供）」においては具体的な申請の手続きについて ICBA 作成の「建築確認検査電子申請等ガイドライン」が提示された。このような背景もあり、平成 26 年 12 月以降、指定確認検査機関による建築確認申請においては、4 号建築物を中心に電子証明書を利用した電子申請が普及し始めている。

建築確認申請の電子申請では、申請書や図面が紙から PDF 形式の電子ファイルに置き換わり、申請者や設計者の押印の替わりにそれぞれの電子証明書で署名される。

指定確認検査機関は、情報通信インフラを構築しオンラインで電子ファイルを受付けして審査し、当該電子ファイルを正本として法定保存期間である 15 年間保存する。

建築確認申請が書面から電子ファイルに代わったことにより、申請者が負担している郵送費用の削減、郵送日数が短縮され、建築主へのサービス向上につながっている。

一方、消防同意については平成 27 年 2 月 12 日 消防予第 53 号の総務省消防庁予防課による「電子申請による建築確認に係る消防同意事務の取扱について（通知）」において、建築確認申請の電子化に伴い、消防同意における情報通信技術を使用した同意の方法と、建築確認検査機関で電子申請を印刷して消防同意に送付する方法が提示された。同通知では、消防通知の情報通信利用の方法も提示されている。

しかしながら、消防同意および消防通知を実施するための情報通信インフラが整備されていないことから、電子申請された建築確認申請は確認検査機関によって書面に印刷して送付する方法のみが実施されている。

電子申請された建築確認申請の「消防同意」の手続きは以下のとおり運用されている。

《消防同意》

① 同意依頼の受付

(ア)建築確認申請を電子申請で行う場合、指定確認検査機関は管轄消防機関へ送付するため消防同意等書類一式を電子ファイルから印刷する。この際、申請者から電子申請された申請図書を取り違い防止のため識別番号を記載し、正・副本に相当する分として 2 部印刷する。電子申請において図面は PDF 形式の電子ファイルで申請されるが、委任状や確認申請書一面が書面で申請される書面と電子ファイルの混合申請の場合においては、指定確認検査機関が書面をスキャンして PDF 形式の電子ファイルに変換して図面とともにモニターで審査することがあるため、電子ファイルの図面とスキャンした委任状等に識別番号を記載した印刷物を併せて消防同意に提出する。

(イ)消防同意等事務、同意通知については「4.1 消防同意等の紙での手続き」と同様の手順になる。

② 消防同意等事務（図面等の確認）

(ア)書面による建築確認申請と同様。

③ 同意通知

(ア)消防同意通知書の返却までは書面による建築確認申請と同様。

(イ)消防同意通知書返却後、建築確認申請が電子申請の場合、同意手続きに使用する消防同意等書類一式は指定確認検査機関による電子正本の印刷物になるので、これに同意印が押印されている場合は、同紙を書面のまま 15 年間保存する。消防同意通知書が別紙の場合は、同紙を書面のまま 15 年間保存する。

《消防通知》

「4.1 消防同意等の紙での手続き」と同様の手順になる。

4.4 消防同意等の電子化に向けて

本書を作成する中で各消防機関や指定確認検査機関からヒアリングした結果、現状の紙媒体での消防同意手続きについては、以下の課題が判明した。

《課題》

① 持参または郵送にかかるコストおよび時間

(ア)指定確認検査機関が、消防機関へ同意を求める書類の持参または郵送にかかる時間、消防機関から指定確認検査機関へ同意通知する際、受領するため赴く時間または郵送にかかる時間が負担となり、建築確認手続きの中で時間短縮を阻害する要因となっている。

(イ)同意通知の際に、消防機関が指定確認検査機関へ消防同意等書類一式の返却作業が発生するため、作業手間が発生している。

(ウ)指定確認検査機関が、持参または郵送する際のコストは、最終的に申請者の負担となっている。

② 消防機関の台帳入力

(ア)消防機関では台帳管理しており、消防同意に提出された消防同意等書類一式から手入力するため、一申請あたり 10 分程度の入力作業の負担が発生している。(消防機関)

(イ)指定確認検査機関では、消防機関によって、消防同意時に特定の様式の書類提出を求める場合があり、これが申請者の負担となっているが、消防機関側の台帳入力の効率を上げるためという側面もある。

③ 消防機関管内の移送

(ア)消防機関によっては、管轄内での消防同意等書類一式の移送が発生する場合があり、費用や移送にかかる時間が負担となっている。

④ 正・副本の比較作業

(ア)消防機関では、消防同意等書類一式に正本と副本が含まれる場合、双方の比較作業が発生している。

一方、消防同意等を紙媒体から電子媒体にする際の懸念点も挙げられた。

《課題》

① インフラ

(ア)消防機関では、インターネット環境はセキュリティ対策されており、閲覧可能なサイトを限定しているほか、ネットワークを業務システムと切り離して運用している。このため、台帳システムへの自動入力をする場合、USB メディア等を介したデータ移動が必要になると考えられている。

② 電子審査

(ア)図面等をモニターで審査するに際して、モニターのサイズに図面が収まら

ない大型モニターを用意する必要がある。

③ 消防同意システムの多面化

(ア)消防機関が各指定確認検査機関独自の消防同意システムを使用する場合、指定確認検査機関ごとに ID を使い分ける必要があり、消防機関での業務が煩雑化する懸念がある。

建築確認申請では電子活用が整いつつあり、官民データ活用基本推進法からも消防同意等の情報通信インフラの整備は喫緊の課題である。

消防機関で台帳入力する項目について電子化された確認申請の手続きで使用しているフォーマットを参考にあらかじめ標準仕様を定め、当該データを指定確認検査機関等から受理して消防機関の台帳システムに取り込めば、入力作業の軽減と誤入力の防止などが期待される。同様に消防同意を電子申請した場合、確認済証にかかる発行日数の短縮という効果が期待される。

反面、紙申請での消防同意等事務の質を担保する対策が必要であることを考慮すると、4 号建築物および 2 号建築物（住宅）、3 号建築物（住宅）で、図面のサイズが A3 サイズ以下に限定して電子化を進めることが、消防機関、指定確認検査機関等の業務効率の向上につながると考えられる。また、4 号建築物、2 号建築物（住宅）、3 号建築物（住宅）を対象とすることについては、全確認申請数の約 7 割を占めているため、多くの案件が対象となると考えられる。

建築確認申請の電子申請には副本が無いため消防同意を電子化した場合には、指定確認検査機関等が消防同意に提出する書類については、消防機関と指定確認検査機関等であらかじめ協議が必要である。消防同意等を電子的に行う場合、提出する電子ファイルは指定確認検査機関等が正本に準ずると認める電子ファイルであり、「電子的に作成された、または紙書類をスキャンして作成された消防同意等書類一式」とすることが望ましい。

消防通知については、消防通知書と建築計画概要書（建築基準法別記第 3 号様式）以外に添付する書類が無いため、電子システムで建築主事等から消防機関へ通知する仕組みを構築することで持参または郵送にかかる手間と費用の軽減が期待される。

消防同意が電子化された場合は、これを指定確認検査機関等が電子保存する方法が想定される。

5. 想定される電子化手法

消防同意等を電子化する場合の基本的な考え方は、「電子申請による建築確認に係る消防同意等事務の取扱について（通知）」（平成 27 年 2 月 12 日消防予第 53 号）に以下のとおり示されている。

> 電子申請による建築確認に係る消防同意等事務の取扱について（通知）（平成 27 年 2 月 12 日消防予第 53 号）
> １ 消防同意について
> 消防同意に係る事務手続きを、指定確認検査機関と消防長等との間で情報通信の技術を利用して行う場合は、電磁的記録に**双方が電子署名を付与すること等の適切な方法により電磁的記録を作成した本人の確認をするとともに、通信途中での電磁的記録の情報漏洩、改ざん等を防止した上で**実施されたい。この場合、指定確認検査機関と消防長等は事前に実施方法を協議し、合意した上で行うこと。
> ・・・中略・・・
> ２ 消防長等への通知について
> 建築基準法第 93 条第４項に基づく通知を、指定確認検査機関と消防長等との間で情報通信の技術を利用して行う場合は、消防長等から指定確認検査機関に通知する手続きがないため、消防長等は電子署名の付与の手続き等を行う必要はない。消防長等への通知を情報通信の技術を利用して行う方法としては、**指定確認検査機関のサーバーにアクセスして電子署名を検証（正当な認証局が発行している本人の電子証明書であること、電子証明書の有効期限が切れていないこと、電子証明書が失効していないこと、署名対象データが改ざんされていないこと）し、電磁的記録をダウンロードする方法等が考えられる。**この場合、指定確認検査機関と消防長等は事前に実施方法を協議し、合意した上で行うこと。
> ・・・中略・・・
> ３ その他
> ・・・中略・・・
> (3) 防火対象物の点検及び報告の特例申請等を情報通信の技術を利用する方法で行う場合は、原則、**総務省関係法令に係る行政手続等における情報通信の技術の利用に関する法律施行規則**（平成 15 年総務省令第 48 号）に規定する電子証明書を送信しなければならないとされていることから、**消防同意等事務を情報通信の技術を利用する方法で行う場合も当該規則を参考のこと。**

5.1 電子署名および電子証明書の基本

電子署名とは、書面におけるサイン（署名）や印影と同等の役割を果たすものである。

消防機関が公印を押印した書面は、消防機関が電子署名を電子ファイルに付与したものと同じ効力をもったものとなる。

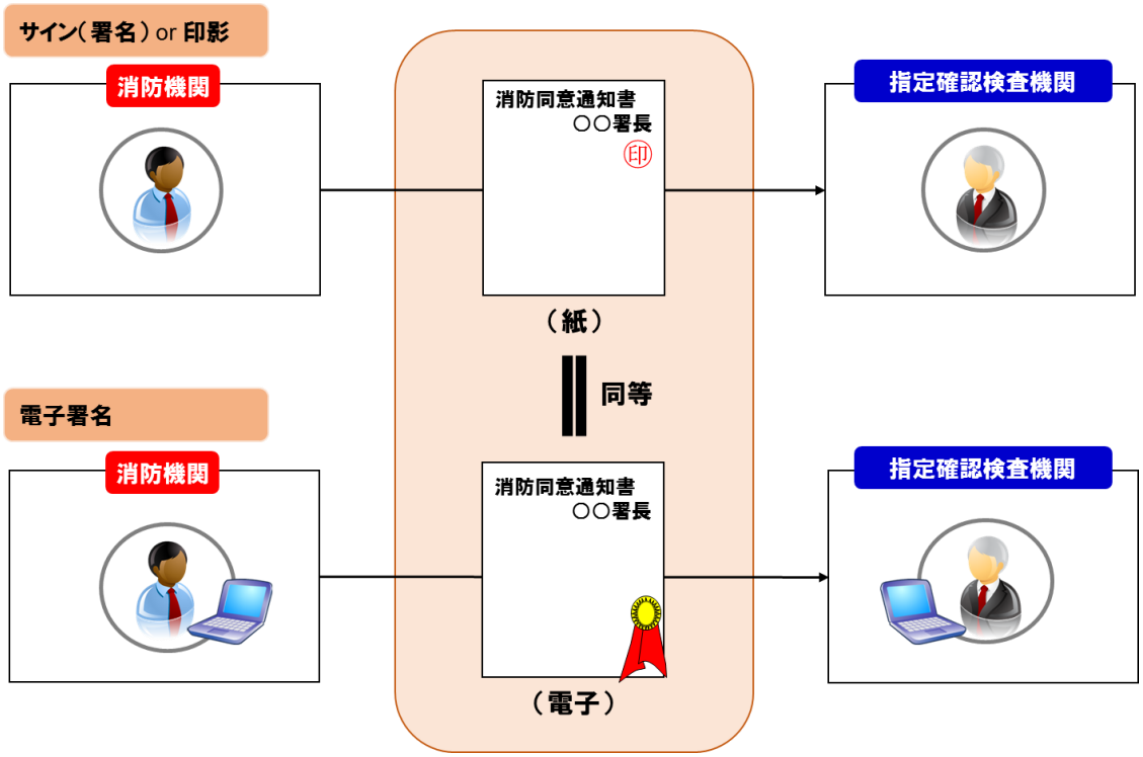


図 2　電子署名について

電子証明書とは、電子署名が本人であることを確認するために用いられ、書面における印鑑登録証明書等と同等の役割を果たす。

実印を秘密鍵（電子署名に使用）とするならば、印影が公開鍵（秘密鍵と対で発行され検証に使用）に相当し、印鑑登録証明書等は、電子証明書（電子認証局で発行され公開鍵の所有者を証明）に相当すると考えられる。

印影と印鑑登録証明書を照合することにより本人が押印したことを証明できるのと同様に、公開鍵と電子証明書で本人より作成された電子ファイルであることを検証することができる。

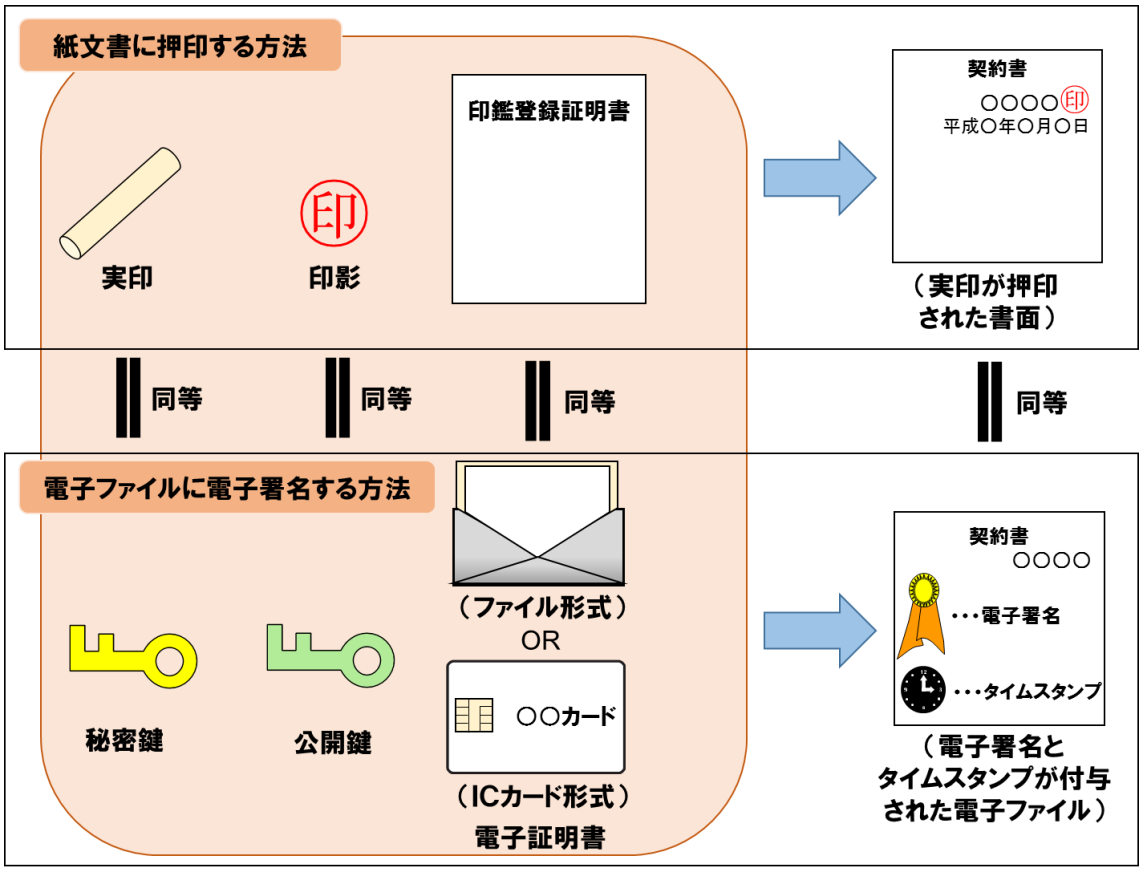


図 3　書面に押印する方法と電子署名を用いる方法の比較

5.2 建築確認手続き等における申請者の電子署名に用いる電子証明書

現在、指定確認検査機関における建築確認手続き等の電子申請については、「行政手続きオンライン化法」を根拠法として、関連省令、告示等の定めるところにより認められている。「建築確認手続き等における電子申請の取扱いについて（技術的助言）」（平成 26 年 5 月 7 日付け国住指第 394 号）では、国土交通省住宅局建築指導課長から、各都道府県建築行政主務部長および地方整備局長または指定確認検査機関に対して、建築確認手続き等における電子申請等の取扱いを明確化する観点から、留意点が示されている。

電子申請等に使用する電子証明書の要件としては、以下のように記載されている。[1]

> 建築確認手続き等における電子申請の取扱いについて（技術的助言）（平成 26 年 5 月 7 日付け国住指第３９４号）
> ２．電子署名の要件について
> 建築確認手続き等の電子申請の仕組みを支障なく安定的に運用するため、電子署名を付与する際には電子証明書を使用する必要があるが、規則第 3 条第 3 項において規定する電子証明書のうち、既に他の行政関連手続きの電子申請でも広く用いられている次に掲げる電子証明書のいずれかを使用すること。
> ①商業登記法（昭和 38 年法律第 125 号）第 12 条の 2 第 1 項及び第 3 項の規定に基づき登記官が作成した電子証明書
> ②電子署名に係る地方公共団体の認証業務に関する法律（平成 14 年法律第 153 号）第 3 条第 1 項に規定する電子証明書
> ③告示第 3 条第 1 号に規定する電子証明書

従って、申請者が指定確認検査機関に建築確認手続き等を電子申請により行う場合は、上記①、②、③の電子証明書を使用し確認申請書類に電子署名をする必要がある。また、消防機関も消防同意依頼書に添付された消防同意等書類一式には上記①、②、③の設計者の電子署名がされていることを検証することになる。

上記①、②、③は以下の電子証明書である。

①. 商業登記に基づく電子認証制度の電子証明書

②. 公的個人認証サービスによる電子証明書

③. 政府認証基盤のブリッジ認証局と相互認証している民間認定認証局から発行される電子証明書になる。

上記①、②、③を「図 4　政府ブリッジ認証局（BCA）と接続する官民の認証基盤」に示す。

5.3 指定確認検査機関の電子署名に用いる電子証明書

「総務省関係法令に係る行政手続等における情報通信の技術の利用に関する法律施行規則」（平成十五年三月二十四日総務省令第四十八号）では、電子申請を行う場合、記名・押印に代わる措置として電子署名を行い電子証明書とともに送信する方法等により、電磁的記録を作成した本人の確認や、通信途中での電磁的記録の情報漏洩、改ざん等を防止したうえで実施する必要があるとされている。なお、その際に使用が認められている電子証明書は下記の同規則（第二条 2 項二号）により行政機関等の使用に係る電子計算機から認証できるものであって以下となっている。

また、消防同意等の手続きが規定されている消防法第 7 条は、従来は官からの手続きの

[1] 建築確認検査電子申請等ガイドライン 平成 26 年 12 月 一般財団法人 建築行政情報センター（ICBA）

規定であるが、現在は民間の指定確認検査機関からの手続きも含まれるため、消防同意等の手続きを電子化するにあたり、同規則の適用範囲と準ずる扱いをするのが相当であると考えられる。

総務省関係法令に係る行政手続等における情報通信の技術の利用に関する法律施行規則（平成十五年三月二十四日総務省令第四十八号）
第二条 2
二　電子証明書　次に掲げるもの(行政機関等が情報通信技術利用法第三条第一項 に規定する行政機関等の使用に係る電子計算機から認証できるものに限る。）をいう。
イ　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第三条第一項 に規定する署名用電子証明書
ロ　電子署名及び認証業務に関する法律第八条 に規定する認定認証事業者が作成した電子証明書（電子署名及び認証業務に関する法律施行規則 （平成十三年総務省・法務省・経済産業省令第二号）第四条第一号 に規定する電子証明書をいう。）
ハ　商業登記法（昭和三十八年法律第百二十五号)第十二条の二第一項 及び第三項 の規定に基づき登記官が作成した電子証明書
第三条　この省令は、別表の上欄に掲げる法令の同表の下欄に掲げる規定に基づく手続等について適用する。
・・・中略・・・
別表　（第三条関係）
【上欄】消防法（昭和二十三年法律第百八十六号）
【下欄】第八条の二の三第二項、第十三条の十三第一項及び第三項（第十七条の九第四項において準用する場合を含む。)、第十三条の十四（第十七条の九第四項において準用する場合を含む。)、第十六条の十七第一項、第十六条の三十五第一項、第十六条の四十二、第十七条の三の三、第二十一条の三第二項、第二十一条の四第一項、第二十一条の三十七第一項並びに第二十一条の四十

従って、指定確認検査機関が消防同意依頼を電子申請により行う場合は、上記イ、ロ、ハの電子証明書を使用し消防同意依頼書に電子署名をする必要がある。また、消防機関は消防同意依頼書に電子署名された電子証明書が上記イ、ロ、ハに該当することを検証する必要がある。なお、「5.2 建築確認手続き等における申請者の電子署名に用いる電子証明書」にて申請者が電子署名をした場合には、消防同意依頼書に添付される文書に申請者の電子署名と指定確認検査機関の電子署名がされるケースがある。

上記イ、ロ、ハは以下の電子証明書である。

イ. 公的個人認証サービスによる電子証明書

ロ. 政府認証基盤のブリッジ認証局と相互認証している民間認定認証局から発行される電子証明書

ハ. 商業登記に基づく電子認証制度の電子証明書

上記イ、ロ、ハを「図 4　政府ブリッジ認証局（BCA）と接続する官民の認証基盤」に示

す。

5.4 消防長等の電子署名に用いる電子証明書

「行政手続きオンライン化法」では、行政機関等が行う電子的な処分通知や作成の際、署名等をすることとしているものについては「当該法令の規定にかかわらず、氏名又は名称を明らかにする措置であって主務省令で定めるものをもって当該署名等に代えることができる。」（第四条 4 項、第六条 3 項）とされており、当該署名とは電子署名のことを指すため、電磁的記録による作成等の場合、署名等は電子署名に代えて行うことが定められている。また、「消防法等の一部を改正する法律等の運用について（通知）」（平成 11 年 4 月 28 日　消防予第 92 号）別添 2「指定確認検査機関に係る消防同意事務等標準処理マニュアル」により、以下のとおり同意の通知または不同意の通知を行う際は、必ず消防長等の官職の者が同意または不同意したことを明らかにする必要がある。

「消防法等の一部を改正する法律等の運用について（通知）」（平成 11 年 4 月 28 日　消防予第 92 号）別添 2「指定確認検査機関に係る消防同意事務等標準処理マニュアル」
(1)　同意の通知
審査を行った結果、同意を与える場合は、次に掲げる方法により担当者の氏名及び連絡先を付して指定確認検査機関に通知すること。
ア　建築基準法施行規則別記第２号様式の第１面に準ずる書式による文書が添付されている場合は、**消防長等の官職及び交付の日付が明らかになるよう、当該文書の同意欄に消防長等が定める同意印を押印**等し、交付する方法
イ　ア以外の場合は、同意する旨、**消防長等の官職、建築主の氏名等の事案を特定するために必要な事項、交付の日付等を記載**した文書を交付する方法
(2)　不同意の通知
審査を行った結果、同意を与えない場合は、**同意できない旨、抵触する法令の規定及び当該抵触の内容、消防長等の官職、建築主の氏名等の事案を特定するために必要な事項、交付の日付等を記載**した文書に担当者の氏名及び連絡先を付して交付する方法により指定確認検査機関に通知すること。

従って、消防長等が使用する電子証明書の属性情報（記載内容）には消防長等の職責を記載する必要がある。なお、消防長等の職責が記載できる電子証明書は、地方公共団体組織認証基盤（LGPKI）の組織認証局から電子文書を送信する地方公共団体職員の職責等に対し発行される「職責証明書」に限られる。[2]また、「職責証明書」であれば、同意の通知または不同意の通知を受け取った指定確認検査機関等が消防長等の電子署名を検証する際に、明らかに消防長等の電子証明書であり、信頼された機関から発行された電子証明書である

[2] 地方公共団体情報システム機構「地方公共団体における組織認証基盤（LGPKI）について（https://www.j-lis.go.jp/lgwan/lgpki/summary/cms_15410842.html）

ことが検証できる。

「地方公共団体組織認証基盤の運営に関する基本綱領」の第 7 条第 3 項において認証局運営組織（LGWAN 運営主体）は、登録分局に証明書の発行、申請等の業務を委任している。登録分局は、市町村の「総務局」「総務部」「総務課」「行政情報課」などの部署で担っていることが多く、その部署で、消防長等向けの職責証明書が発行されている。

実際に消防機関で消防長等の職責証明書を取得する際には、各市町村の当該部署へ問い合わせ電子証明書を発行する手続きを行う必要があるが、市町村によっては現在の登録分局の規程上消防長等向けに発行することが想定されておらず、規程に定められていない可能性がある。その場合は、登録分局の規程を変更してもらう等対応が必要な場合も考えられる。

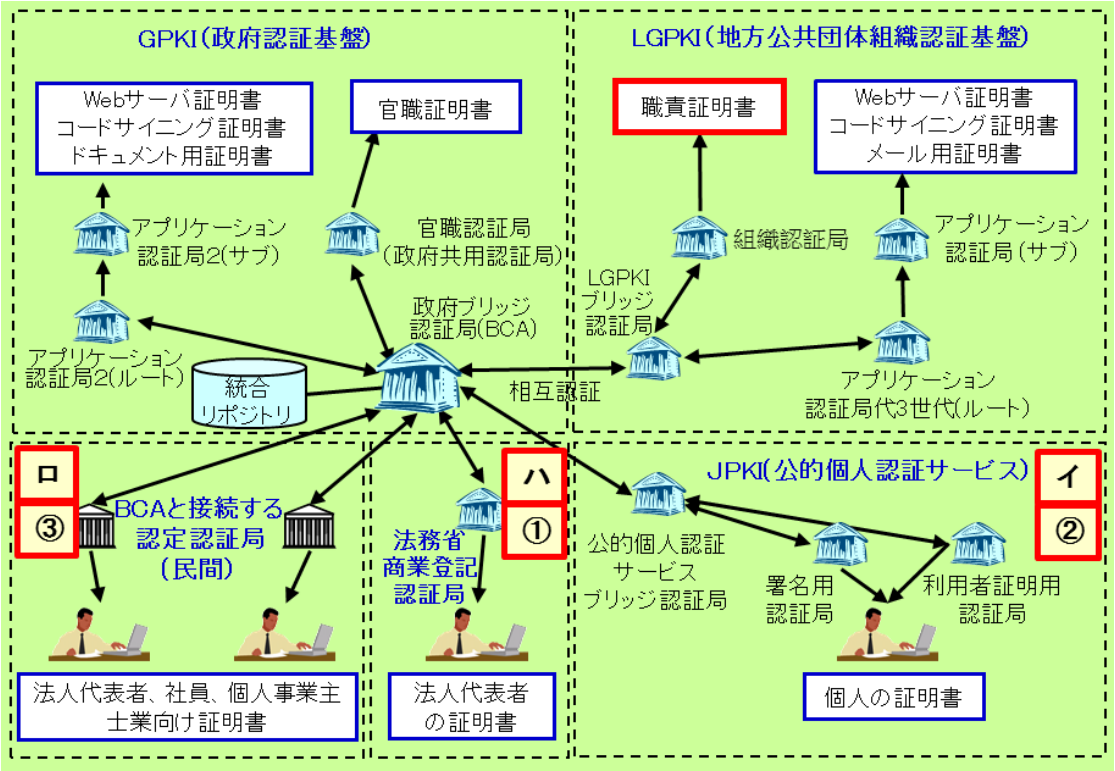


図 4　政府ブリッジ認証局（BCA）と接続する官民の認証基盤

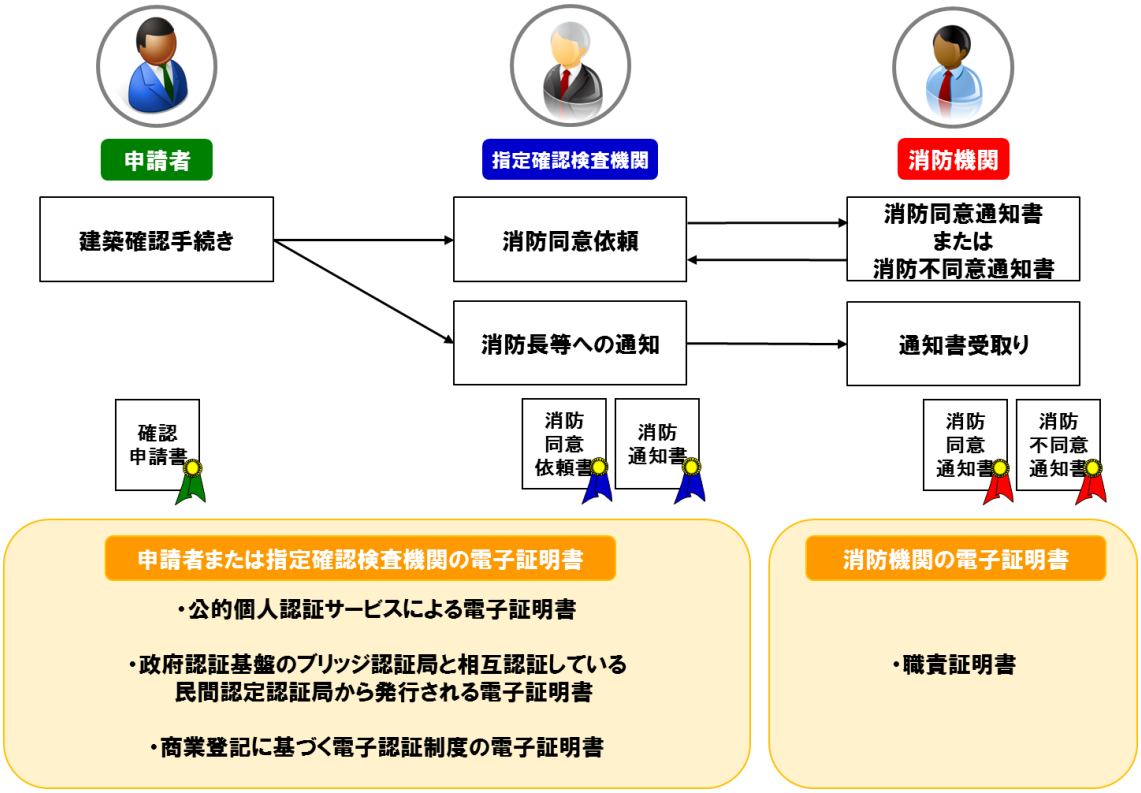


図 5　電子署名に用いる電子証明書

5.5 消防同意等事務を電子化する場合のシステムについて

実際に消防同意等事務を電子化しようとした場合、消防機関と指定確認検査機関等の間で電子署名済みの電子ファイルを転送する必要がある。なお、この際の電子ファイルは PDF ファイルとし、長期署名方式は、PAdES-LTV 形式とする。この実現方法として、

(1) ファイルのアップロードやダウンロードが行える電子システムを利用したファイル転送

(2) 電子メールの添付ファイルによるファイル送信

が考えられる。 (1)の場合には既存の電子システムを改修して活用または新たに電子システムを導入することが考えられ、いずれの場合も ID、パスワード、電子証明書等により利用者の確認を行い、情報セキュリティに留意してシステム構築・運用を実施する必要がある。システム構築・運用を企業に依頼する場合は、当該企業が ISMS 認証取得していること等を確認することが望ましい。

また、ファイル転送を行う電子システムではファイルのアップロード時に送信先へ、ダウンロード時に送信元にメール等で通知することにより、消防機関と指定確認検査機関等の間でスムーズにやり取りができ、更に互いの進捗状況把握や作業漏れ防止に効果がある。(2)の場合には、既存のメールシステムが利用できるが、通信回線の安全性、誤送信リスク、標的型電子メール等のセキュリティ侵害などへの対策に留意したうえで運用する必要がある。

本章後半に電子化するための各々の手法とメリット、デメリット、コストを記載する。それを元に、導入について検討・判断していただきたい。なお、消防機関で電子システムを導入するにあたり、電子データをモニターで審査するための資材準備（審査端末・大きいモニター等）、台帳システムなどの既存システムへの連携費用、電子決裁システムの導入費用が考えられ、これらには別途費用がかかる。

5.6 消防同意等事務を電子化する場合の基本的な流れ

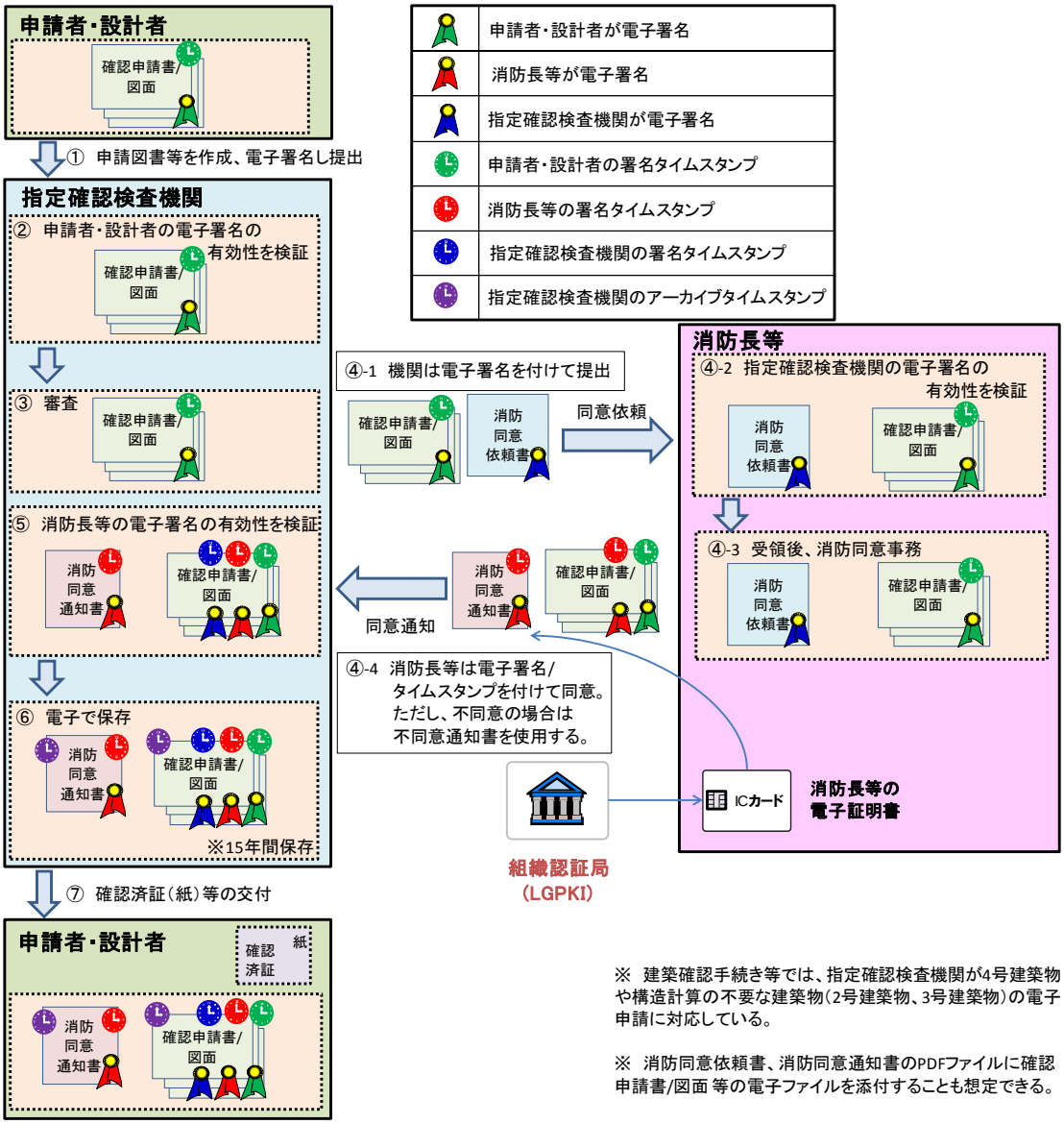


図 6　電子的な消防同意フロー図

申請者はこれまで書面に押印して確認申請書等を提出していたが、電子の場合は「電子署名」を付与して電子ファイルを送信する。指定確認検査機関は、持参や郵送していた消防同意依頼に係わる電子文書に「電子署名」を付与し消防機関に即日送信が可能となり、消防機関が消防同意する際も「電子署名・タイムスタンプ」を付与した電子ファイルを即日送信することにより、従来の事務作業にかかっていた郵送時間の削減ができ、指定確認検査機関の確認済証の発行期間短縮につながる可能性が高く、住民サービスの向上につながる。指定確認検査機関は、消防同意済みの電子ファイルに「アーカイブタイムスタンプ」を付与し、法定保存期間である 15 年間保存する。確認申請書等の副本については、電子ファイルで申請者に返送可能となる。

5.7 既存の電子システムを活用する場合

5.7.1 地方公共団体にて運用している既存の電子申請システムの利用拡大

指定確認検査機関等からの消防同意等には、地方公共団体が運用している「電子申請システム」の申請種別を拡大し利用することが考えられる。

＜必要となること＞
・既存の電子申請システムの改修。
・日本データ通信協会認定のタイムスタンプの利用。
・行政側ユーザーに消防長等、消防機関の担当者を登録。
・消防機関への行政端末の配備。
＜メリット＞
・地方公共団体が管理をするため、消防機関や指定確認検査機関等が独自で負担するコストはない。
・既存システムのためセキュリティ対策を新たに講じる必要がない。
＜デメリット＞
・地方公共団体の協力体制が必要。
・既存システムの仕組みによっては、改修費が多額になる恐れがある。
＜コスト＞
・既存システムの仕組み、改修業者の対応などにより数百万円～数千万と幅広くなることが想定される。

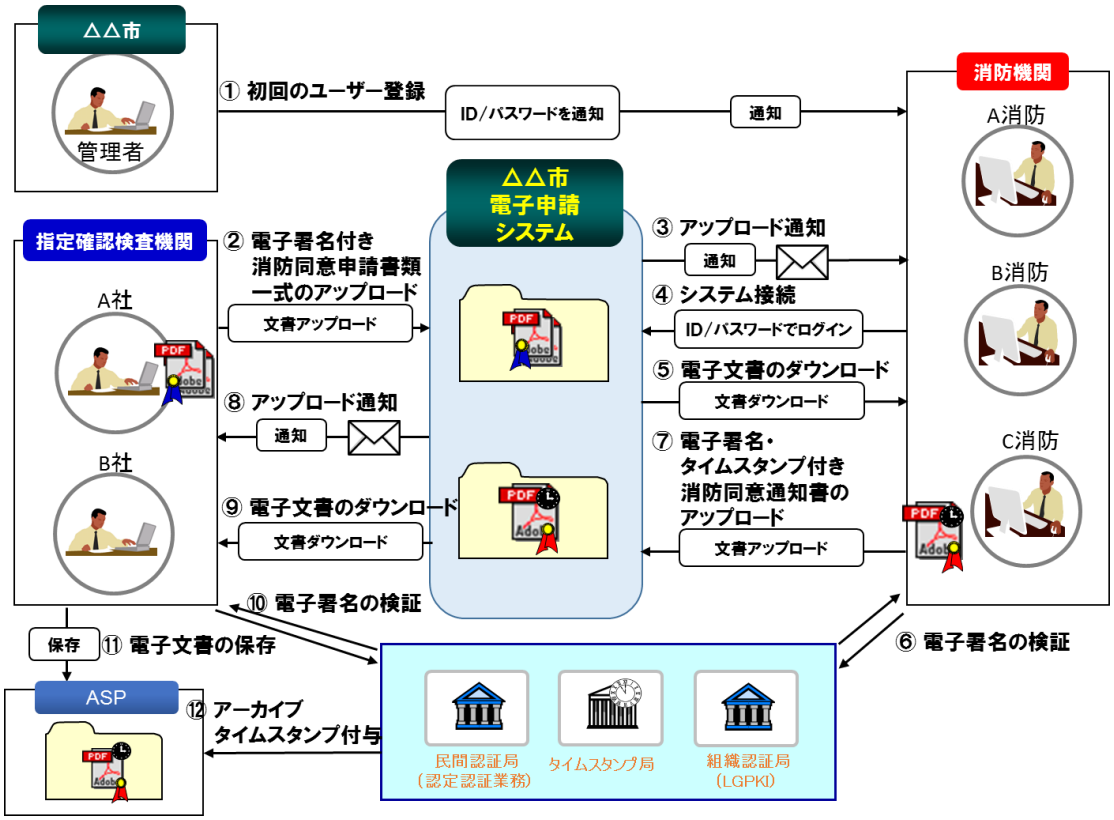


図 7　既存の電子システムの利用拡大

5.7.2 指定確認検査機関のファイル転送システムを消防機関が利用

現在、指定確認検査機関が建築確認手続き等で利用しているファイル転送システムを消防機関が利用し、指定確認検査機関との間で消防同意等のファイル転送を行うことが考えられる。

＜必要となること＞
・指定確認検査機関にて消防長等、消防機関担当者を登録。
・指定確認検査機関と消防機関でメールおよびインターネット接続が行える端末。
・ファイル転送システム自体に電子署名、タイムスタンプを付与する機能がない場合、別途電子署名やタイムスタンプを付与するための Adobe 社「Acrobat」やスカイコム社「SkyPDF」等の LGPKI の電子署名に対応した PDF 閲覧・編集ソフトウェアを用意し、日本データ通信協会認定のタイムスタンプの利用契約を結ぶ必要がある。
＜メリット＞
・電子システムの改修等がないため電子化しやすい。
・管理や費用負担は指定確認検査機関となるため消防機関の費用が発生しない。
・サイズの大きい電子ファイル転送が可能。（ファイルサイズの上限は各サービスにて要確認）
＜デメリット＞
・ファイル転送システムを利用していない指定確認検査機関がある。
・指定確認検査機関ごとにアクセス先や ID/パスワードを使い分け、操作性が異なる可能性がある。
・単純なファイル転送サービスの場合、タイムスタンプをシステム上で付与できないため、PDF 閲覧・編集ソフトウェアで付与する必要がある。
＜コスト＞
・指定確認検査機関のファイル転送システムでタイムスタンプを利用していない場合は、消防機関でタイムスタンプ利用料が発生する。
（利用料の例）月間 1,000 スタンプ以内で 1 万円程度。
・PDF 閲覧・編集ソフトウェア（PAdES-LTV 対応）を利用する場合、メーカーにより価格は異なるが、1 万円程度から 4 万円程度で購入可能。

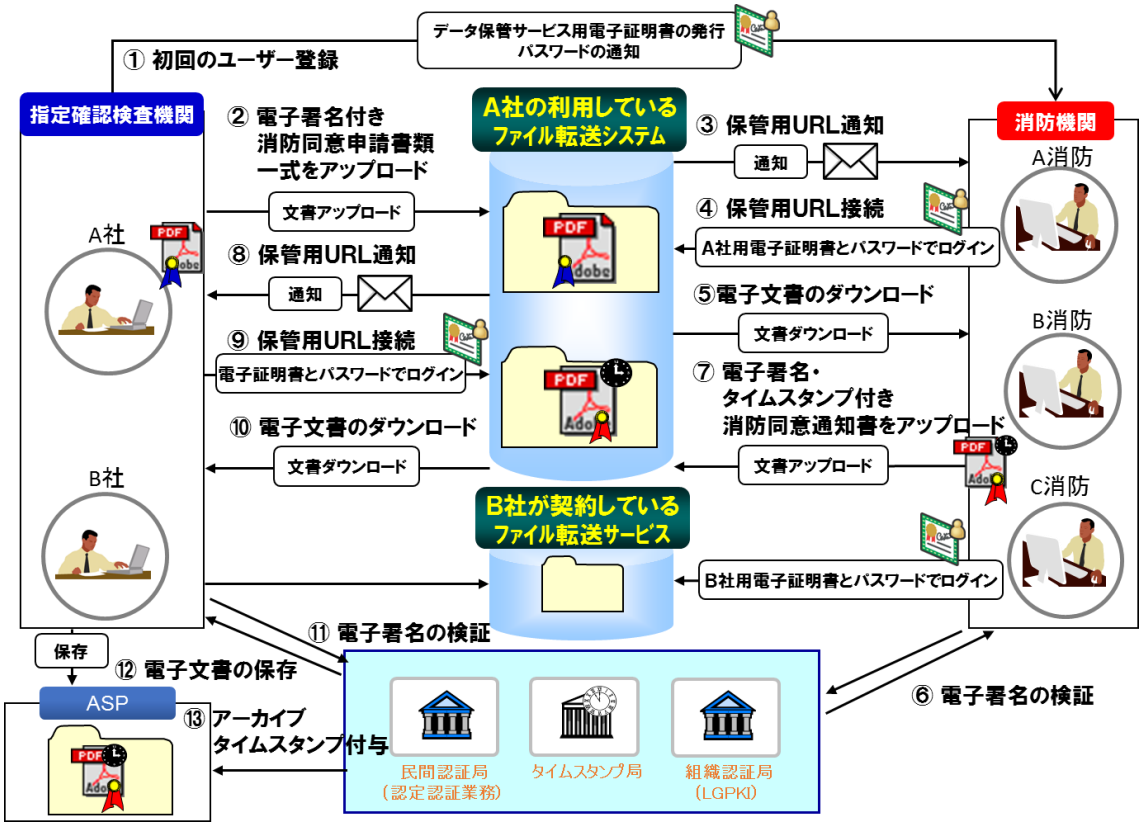


図 8　指定確認検査機関のデータ保管サービスを介したファイル交換

5.7.3 電子メールによる添付ファイル送信

指定確認検査機関と消防機関において消防同意等書類一式を電子メールにて送信することは、送受信相手の数や通信文の量が多く誤送信リスクや標的型電子メール等のセキュリティ上の問題がある。そのため、消防同意等の電子ファイルをメールで送信する場合は、セキュリティ上、標的型電子メール攻撃などへの対策が必要となり、なりすまし防止、改ざん防止、ウイルス感染対策、情報漏洩対策などを行う必要がある。

そのため、S/MIME（エスマイム）による電子署名・暗号メールの利用が必要と考えられる。S/MIME を利用するには対応するメールソフトウェアおよびメール用証明書（S/MIME 用証明書）を双方、用意する必要がある。

消防機関は、登録分局または民間の認証局へメール用証明書の発行を依頼し用意する必要がある。指定確認検査機関は、信頼された認証局から本人確認を行ったうえで発行されるメール用証明書を用意する必要がある。

S/MIME 方式の署名暗号化メールを行う場合は以下の手続きによる。

(1) メールソフトウェアにメール用証明書を登録し、電子署名・暗号化を行うための設定をする
(2) 通信相手の電子署名の付いたメールを受信し、通信相手の公開鍵を登録する
(3) メールを作成し、メールが電子署名・暗号化設定されていることを確認し送信する

この場合、通信途中、第三者に内容を見られることや改ざんの心配はない。しかし、公開鍵は、誰でも入手可能なので、送信相手がメールを暗号化しているから安全とは言えないので、受信メールの電子署名を検証し、予め決められた送信者からの送信であることを確認する必要がある。また、添付ファイルの安全性をウイルス対策ソフト等で確認する必要があるが暗号化されたメールの場合は復号後の添付ファイルに対してウイルスチェックを行うことが必要となる、このような運用が許可されない場合はメールの暗号化は採用できない。更に、送信先が開封したことを確認するためにメールソフトウェアで開封通知が届く設定にしておくか、受領返信をするなどの運用も行うことが望ましい。

その他、電子メールは送信先のメールサーバーで受信ファイルサイズの上限が定められている。消防同意依頼書や消防同意通知書を送信する際にファイルサイズが上限を上回っている場合、ファイル分割をする必要が発生し作業が煩雑になる恐れがある。ただし、消防通知の場合は、比較的ファイルサイズが小さくメールでの添付には、消防同意より適していると思われる。

＜必要となること＞
・指定確認検査機関と消防機関とでメールおよびインターネット接続が行える端末。
・指定確認検査機関と消防機関の双方でメール用証明書を取得。
・指定確認検査機関と消防機関の双方で S/MIME に対応したメールソフトウェア（Microsoft Outlook、Mozilla Thunderbird、Shuriken、Mac Mail 等）を利用。
・電子署名やタイムスタンプを付与するための Adobe 社「Acrobat」やスカイコム社「SkyPDF」等の LGPKI の電子署名に対応した PDF 閲覧・編集ソフトウェアを用意し、日本データ通信協会認定のタイムスタンプの利用契約を結ぶ必要がある。
＜メリット＞
・電子システムの改修等がないため電子化しやすい。
・費用が安価に抑えられる。
＜デメリット＞
・電子データのファイルサイズが大きい場合、送受信できないため、分割して複数送信する必要がある。（サイズの大きいファイルを分割するフリーソフトウェアもある）
・電子データのファイルサイズが小さいものでないと現実的な運用が考えにくい。
・指定確認検査機関の数や消防同意の件数が多いと煩雑となる。
・メールに付与された電子署名の署名検証が作業負担となる。
・S/MIME に対応したメールソフトウェアおよびその利用が消防機関で許可または対応されていない場合、利用できない。
＜コスト＞
・指定確認検査機関のファイル転送システムでタイムスタンプを利用していない場合は、消防機関でタイムスタンプ利用料が発生する。
（利用料の例）月間 1,000 スタンプ以内で 1 万円程度。
・PDF 閲覧・編集ソフトウェア（PAdES-LTV 対応）を利用する場合、メーカーにより価格は異なるが、1 万円程度から 4 万円程度で購入可能。
・地方公共団体の登録分局で発行されるメール用証明書を利用する場合は、費用なし。民間の認証局で発行されるメール用証明書を利用する場合は、年間基本料金は数万円程度発生する。

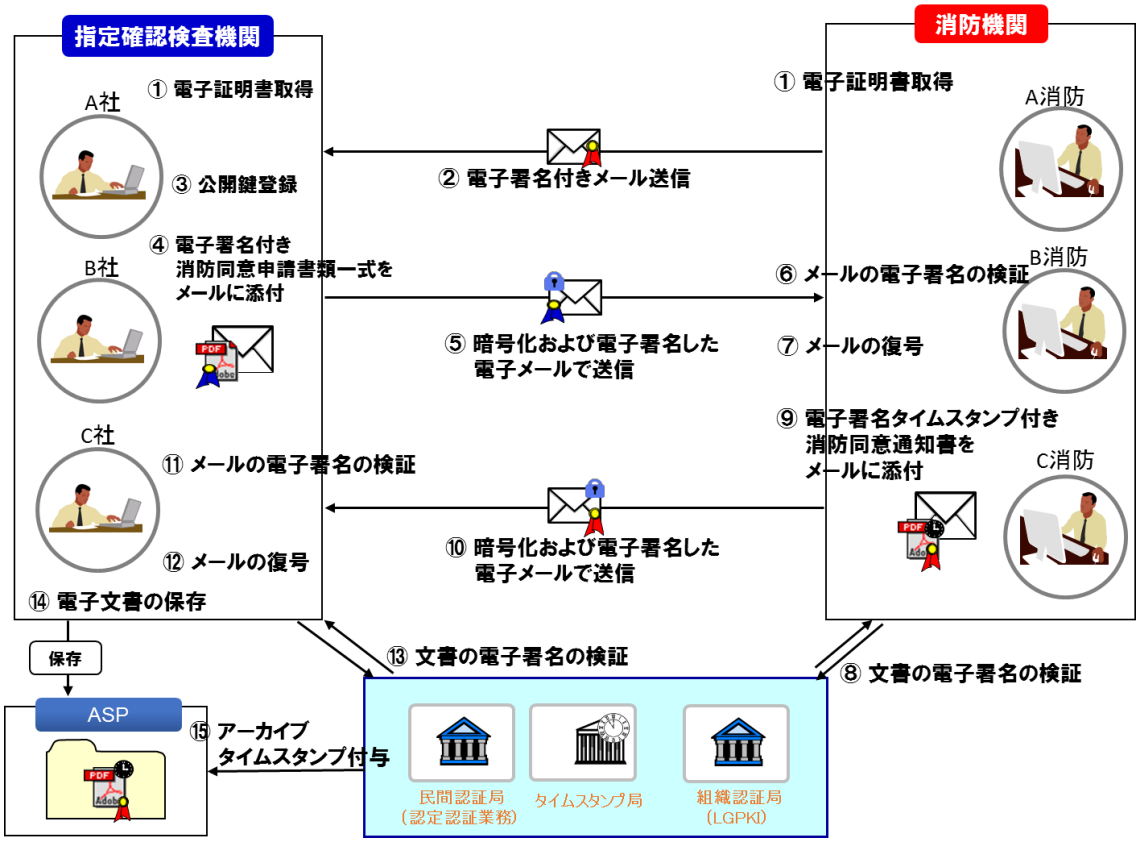


図 9　電子メールによる添付ファイル送信

5.7.4 特定行政庁とのイントラネットを利用したファイル送信

消防機関と特定行政庁との間で消防同意等事務を行う場合、地方公共団体のイントラネット経由の通信が利用できると考えられ、安全性が確保される。特定行政庁から消防同意を受ける場合は、アクセス制限のあるファイルサーバーを介するファイル交換や電子決裁システム等をはじめとするイントラネットを利用した運用が考えられる。なお、イントラネット経由の通信を利用する場合はセキュリティ上外部のネットワークと切り離されており、環境がイントラネット内に閉じていることを確認したうえで実施する必要がある。

＜必要となること＞

・アクセス制限のあるファイルサーバーを介するファイル交換または電子決裁システムを利用したファイル交換などイントラネット内にファイル交換できる方法があること。

・電子署名やタイムスタンプを付与するための Adobe 社「Acrobat」やスカイコム社「SkyPDF」等の LGPKI の電子署名に対応した PDF 閲覧・編集ソフトウェアを用意し、日本データ通信協会認定のタイムスタンプの利用契約を結ぶ必要がある。

＜メリット＞

・特定行政庁と消防機関にて共有しているイントラネット用の既存サーバーを利用できるためサーバー利用の費用がかからず、セキュリティの心配がない。

・既存の機能を利用できれば、改修費用がかからない場合がある。

＜デメリット＞

・指定確認検査機関が利用できない。

・サイズの大きい電子ファイルに既存サーバーが対応できるか検討が必要。

・状況確認のため電子ファイルの受取状況、進捗状況を確認できる運用を別途検討する必要がある。

＜コスト＞

・費用は改修しない場合と既存機能を改修する場合があるため、0 円～数百万円と想定される。

・PDF 閲覧・編集ソフトウェア（PAdES-LTV 対応）を利用する場合、メーカーにより価格は異なるが、1 万円程度から 4 万円程度で購入可能。

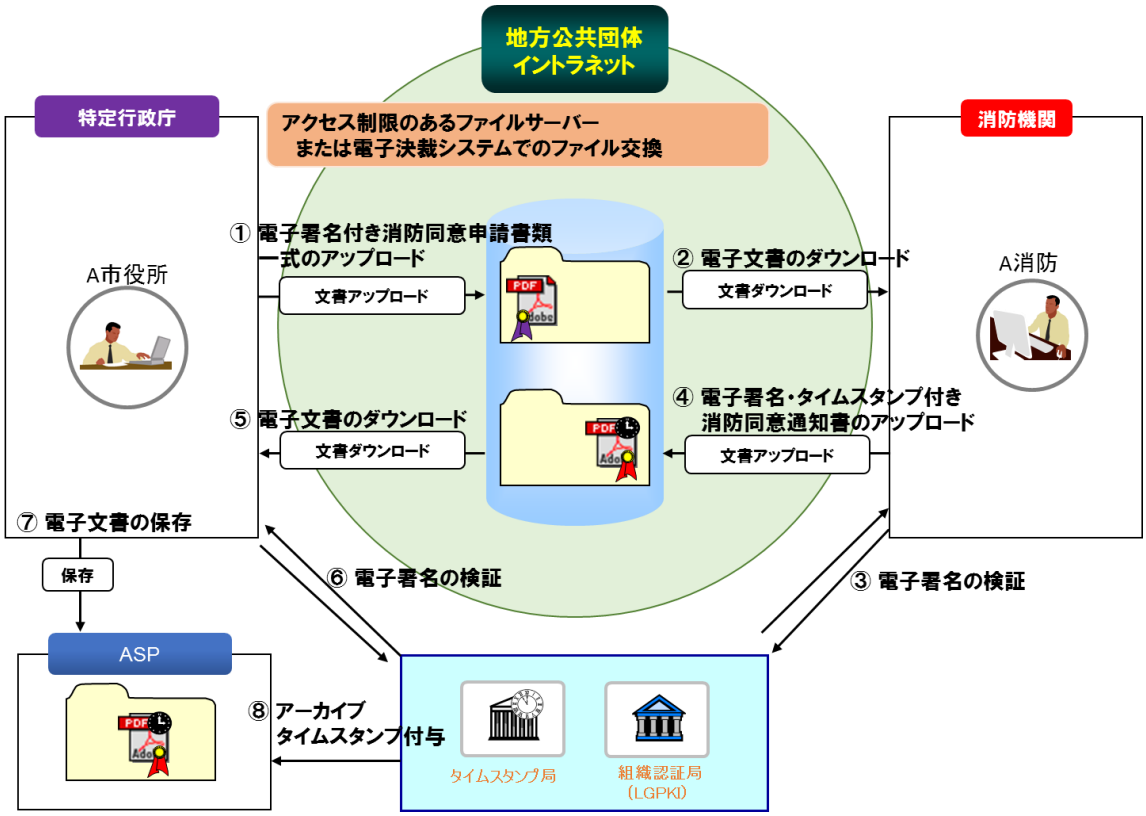


図 10　特定行政庁からイントラネットを利用したファイル送信

5.8 新規に電子システムを導入する場合

5.8.1 全国統一的な新規電子システムの利用

新規に電子システムを導入する場合は、消防機関、特定行政庁、指定確認検査機関で一元管理できる同一の電子システムを利用することにより、効率的な運用が期待できる。そのため、全国の消防機関で利用可能な統一的な電子システムを消防機関単位で導入できることが望ましい。例として、全国の消防機関で利用可能な統一的な電子システムが提供され、それを消防機関が契約して利用料を支払えば電子システムの利用が開始できるなどが考えられる。

各々の地方公共団体や消防機関ごとに閉じた個別システムの形では、指定確認検査機関側でアカウントを使い分ける（個別システムごとにアクセスする URL や利用者確認のための ID、パスワード、ログインに用いる電子証明書などが異なる）必要があるため煩雑となる。

全国の消防機関で利用可能な統一的な電子システムを導入する場合は、セキュリティが確保された ASP 利用が考えられる。

主な機能要件は下記となる。

(1) インターネット経由で SSL/TLS 通信等により安全性を確保した通信経路により消防機関、指定確認検査機関、特定行政庁の許可された者のみがアクセスできる。

(2) 消防同意、消防通知に必要な電子ファイルをアップロードし、指定した送信先だけが閲覧、ダウンロード可能である。

(3) 文書アップロードの際に送信先にメール通知が行うことができる。

(4) アップロードする電子ファイル（PDF ファイル）に必要に応じて電子署名、タイムスタンプが行うことができる。

(5) 電子署名の方式は PAdES-LTV 形式に準拠する。(「建築確認検査電子申請等ガイドライン（平成 26 年 12 月　ICBA)」に示された方法)

(6) 電子署名とタイムスタンプの検証機能を有する。特に業務の効率化のため複数の電子署名済みファイルに対して一括して検証ができる機能を有すことが望ましい。

(7) 電子証明書は､「総務省関係法令に係る行政手続等における情報通信の技術の利用に関する法律施行規則　第二条 2 項二号」のイ、ロ、ハのうちいずれか 1 つ以上、および LGPKI の電子証明書が利用できる。(「図 5　電子署名に用いる電子証明書」を参照)

＜必要となること＞
・新規電子申請システムの利用契約。
・電子申請システムの消防機関の管理者を登録。
・消防機関の管理者により消防長等、消防機関担当者を登録し ID/パスワードを付与。
・指定確認検査機関と消防機関とでメールおよびインターネット接続が行える端末。
＜メリット＞
・消防機関と指定確認検査機関等で同一システムを利用することにより一元管理ができ効率的な運用が期待できる。
・消防同意等事務以外の紙申請についても電子化が進むことが考えられる。
・セキュリティが確保しやすい。
・ファイルサイズの大きい電子データの交換ができる。
・新規電子システム側で電子署名・タイムスタンプの機能を用意できるため、消防機関個別に準備する必要はない。
＜デメリット＞
・消防機関や指定確認検査機関ごとに細かいカスタマイズが難しい。
・指定確認検査機関等で同一システムの利用が必要。
・同一システム利用のコンセンサスが必要。
＜コスト＞
・初期コストとして数十万円。
・利用料として 1 消防機関あたり月々の基本料は数万円程度、ファイルの送受信料は 1 ファイルに付き 100 円程度と想定される。指定確認検査機関にとっては郵送費が削減できるため、ファイルの送受信料は指定確認検査機関側に求めることも想定できる。

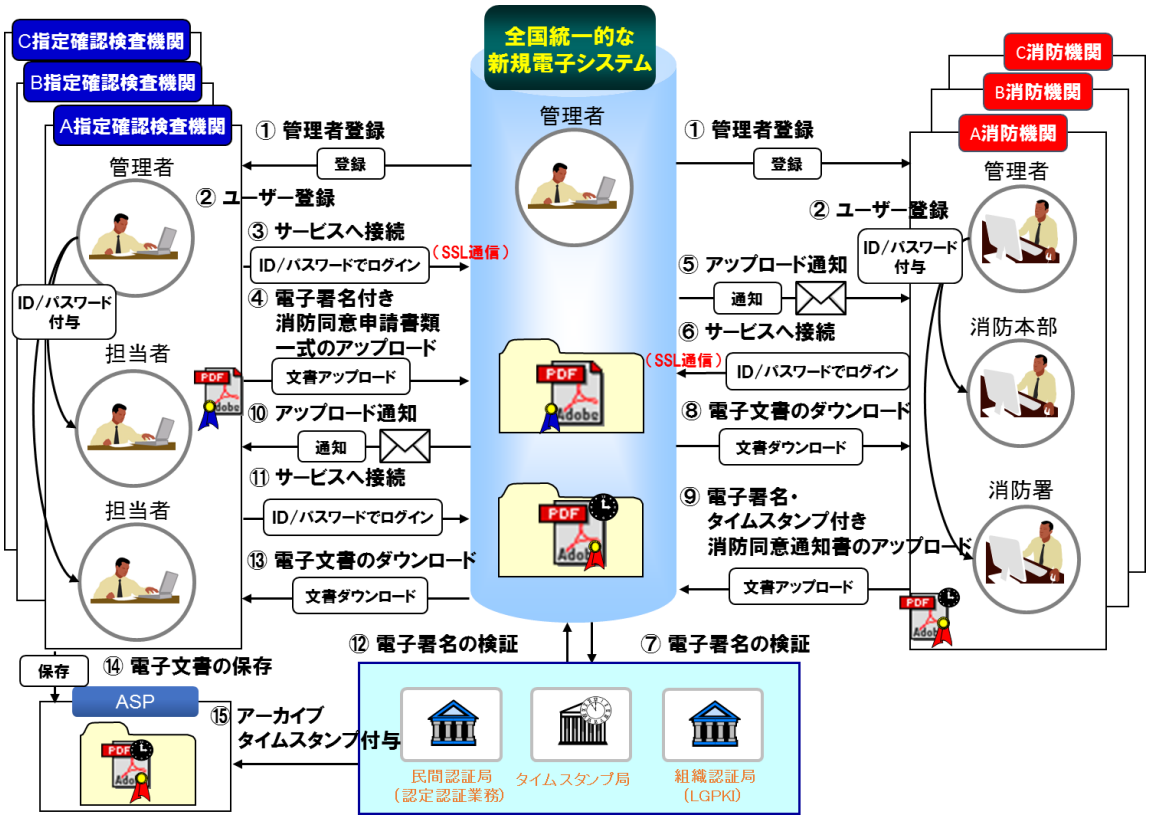


図 11　Web 上の電子文書交換サーバーを介したシステムイメージ

5.8.2　各消防機関個別の電子システムを利用

Web 上でファイル転送ができるサービスには、ファイル転送のみに特化したファイル転送サービスやファイル転送以外にも電子署名・タイムスタンプ・長期電子保存などの機能も含まれたサービスがある。なお、サービスによっては、ファイル送信はできるがファイル受信できないサービスもあるため、双方で送受信できるサービスを利用する必要がある。

ここでは、消防機関がこれらのサービスから任意に選択して利用することを想定する。指定確認検査機関等は消防機関が選択した個別の電子システムを利用するため、指定確認検査機関等にとっては煩雑になることが考えられる。

＜必要となること＞
・消防機関にてファイル転送サービス等を行っている業者と契約。
・消防機関にて消防長等、消防機関担当者を登録。
・指定確認検査機関等を登録するなどの作業が必要かどうかはサービスによって異なる。
・消防機関と指定確認検査機関等でメールおよびインターネットが行える端末を準備。
・ファイル転送サービス自体に電子署名、タイムスタンプを付与する機能がない場合、別途電子署名やタイムスタンプを付与するための Adobe 社「Acrobat」やスカイコム社「SkyPDF」等の LGPKI の電子署名に対応した PDF 閲覧・編集ソフトウェアを用意し、日本データ通信協会認定のタイムスタンプの利用契約を結ぶ必要がある。
＜メリット＞
・サービスによっては安価に抑えられる。
・消防機関が契約するため、指定確認検査機関等が契約する場合と異なり消防機関にとっては煩雑にならない。
・ファイルサイズの大きい電子データの送受信ができる。（ファイルサイズの上限は各サービスにて要確認）
＜デメリット＞
・指定確認検査機関等は消防機関ごとにアカウントを使い分ける（個別システムごとにアクセスする URL や利用者確認のための ID、パスワード、電子証明書などが異なる）必要があるため煩雑になる。
・指定確認検査機関等に利用してもらうよう協力体制が必要。
・単純なファイル転送サービスの場合、タイムスタンプをシステム上で付与できないため、PDF 閲覧・編集ソフトウェアで付与する必要がある。
・無料サービスの転送サービスも存在するがウイルス検知機能などのセキュリティ面での保障がないため推奨しない。
＜コスト＞
・初期コストとして数十万円。
・利用料として 1 消防機関あたり月々の基本料は数万円程度、ファイルの送受信料は 1 ファイルに付き 100 円程度と想定される。指定確認検査機関にとっては郵送費が削減できるため、ファイルの送受信料は指定確認検査機関側に求めることも想定できる。
・PDF 閲覧・編集ソフトウェア（PAdES-LTV 対応）を利用する場合、メーカーにより価格は異なるが、1 万円程度から 4 万円程度で購入可能。

図 12　消防機関のデータ保管サービスを介したファイル交換

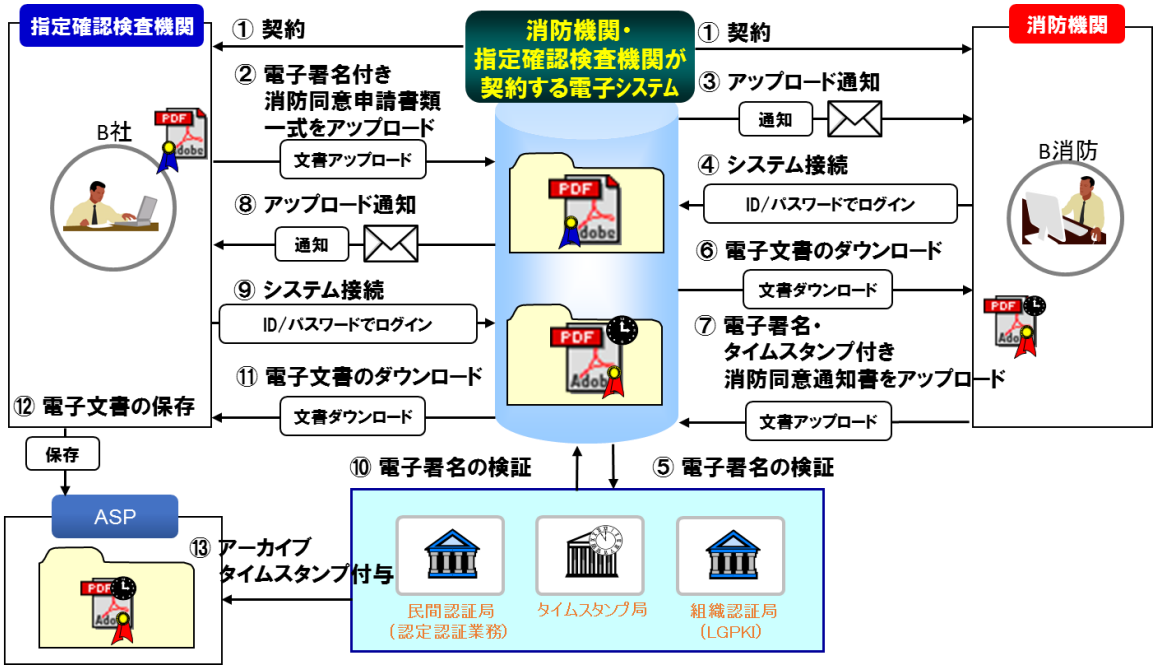


図 13　消防機関・指定確認検査機関が契約するシステムを介したファイル交換

5.9 消防同意等をすべて電子化する場合と一部を電子化する場合

「消防法等の一部を改正する法律等の運用について（通知）（平成 11 年 4 月 28 日　消防予第 92 号)」では、同意を与える方法として「ア」、「イ」の 2 つの方法が示されており（「5.4 消防長等の電子署名に用いる電子証明書」を参照)、それぞれの場合で電子化の方法を示す。

5.9.1　消防同意を電子化する場合

(1)　確認申請書に消防長等の電子署名を付与し交付する方法

「ア」は、確認申請書の第 1 面の同意欄に消防長等が定める同意印を押印等し交付する方法である。電子的に行う場合、指定確認検査機関等から受領した確認申請書の PDF ファイルに消防長等の電子署名を行い交付する方法となり、消防機関の消防同意事務処理規程等にて「確認申請書に消防長等の電子署名を付与することにより同意したものとする」等を定めるものとする。その方法については以下に示す。

① 指定確認検査機関等では消防同意依頼書を PDF ファイルにて作成し担当者の電子署名を行い、対象となる確認申請書、設計図書の PDF ファイル（申請者が建築確認申請手続を書面で行った場合は、「建築確認検査電子申請等ガイドライン」に準拠し、スキャナーにて「解像度は原則として 300dpi 以上で、書面等に打ち出した際に明確に表示できること」とし、スキャナー画像ファイルに指定確認検査機関等の電子署名を行ったもの)、委任状を受領している場合にはそのスキャン画像とともに消防機関に送信する。

② 消防機関は受領した消防同意依頼書に付与された指定確認検査機関等の電子署名を検証し、問題なければ受理、審査する。

③ 審査結果に問題が無ければ、消防同意等書類一式の PDF ファイルに消防長等の電子署名を行い、タイムスタンプを付与し、指定確認検査機関等に返送する。なお、確認申請書には申請者の電子署名のみが付されている場合と申請者の電子署名および指定確認検査機関等の電子署名が付されている場合がある。このため、電子署名された確認申請書に同意、不同意の処分内容、コメント、同意番号などを追記した場合、電子署名が検証できなくなる。従って、処分内容、コメント、同意番号などの追記が必要な場合には必要に応じて付帯的な文書を別途作成して添付することが考えられる。

④ 不同意を通知する場合は、消防同意等書類一式には消防長等の電子署名は行わず、別に「消防不同意通知書」を PDF ファイルにて作成し消防長等の電子署名を行い返却するものとする。消防不同意通知書には、同意できない旨、不同意事由、消防長等の官職、建築主の氏名等の事案を特定するために必要な事項、交付の日付、担当者の氏名、連絡先等を記載するものとする。

また、電子署名自体には印影は無いが PDF ファイルに電子署名を行う場合は印影の代わりに任意の画像を「可視署名」として補助的に付けて表示することができる。なお、「可視署名」で表示する画像には「電子署名済み」であることを表示

したものが望ましく、実際の印影イメージを用いると書面に押印したもののコピーと誤認される恐れがあるため、用いるべきではない。「図 14　電子署名を行った確認申請書（サンプル PDF）のイメージ」に示す。

⑤　指定確認検査機関等では、受領した③の消防長等の電子署名とタイムスタンプの検証を行い、問題がなければ③に必要に応じて指定確認検査機関の電子署名を行った後、アーカイブタイムスタンプを付与し電子保存する。

・PDFへ電子署名（可視署名必須）

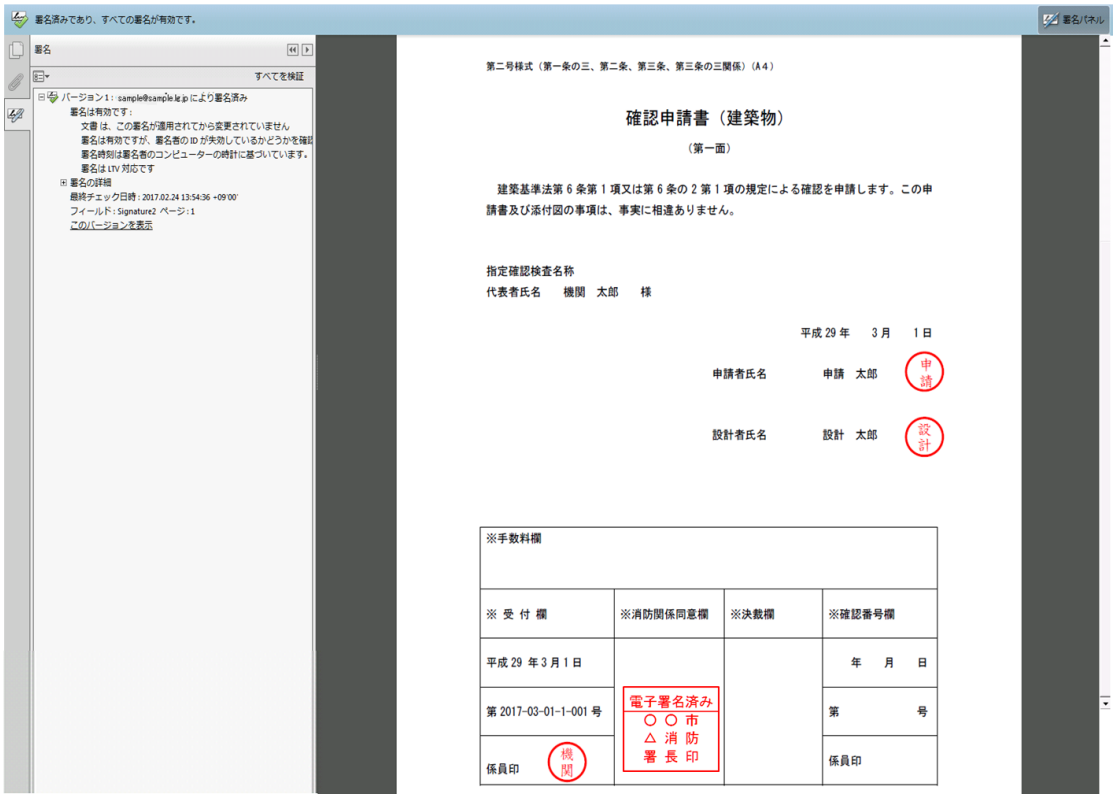


図 14　電子署名を行った確認申請書（サンプル PDF）のイメージ

(2)　消防同意通知書に消防長等の電子署名を付与し交付する方法

「イ」は、同意する旨、消防長等の官職、建築主の氏名等の事案を特定するために必要な事項、交付の日付等を記載した文書を交付する方法である。

この方法による場合は、消防長等の官職、建築主の氏名等の事案を特定するために必要な事項、交付の日付等を記載した「消防同意通知書」等の文書を電子的に作成し、消防長等の電子署名を行い交付する方法となる。なお、消防機関の消防同意事務処理規程等にて「消防同意通知書に消防長等の電子署名を付与することにより同意したものとする」等を定めるものとする。その方法については以下に示す。また、消防同意通知書等のサンプル書式を「14.2 消防同意通知書サンプルフォーマット」に記載する。

① 指定確認検査機関等では消防同意依頼書を PDF ファイルにて作成し担当者の電子署名を行い、対象となる確認申請書、設計図書の PDF ファイル（申請者が建築確認申請手続を書面で行った場合は、スキャナーにて 300dpi 以上で読み取った画像ファイルに指定確認検査機関等の電子署名を行ったもの)、委任状を受領している場合にはそのスキャン画像とともに管轄する消防機関に送信する。

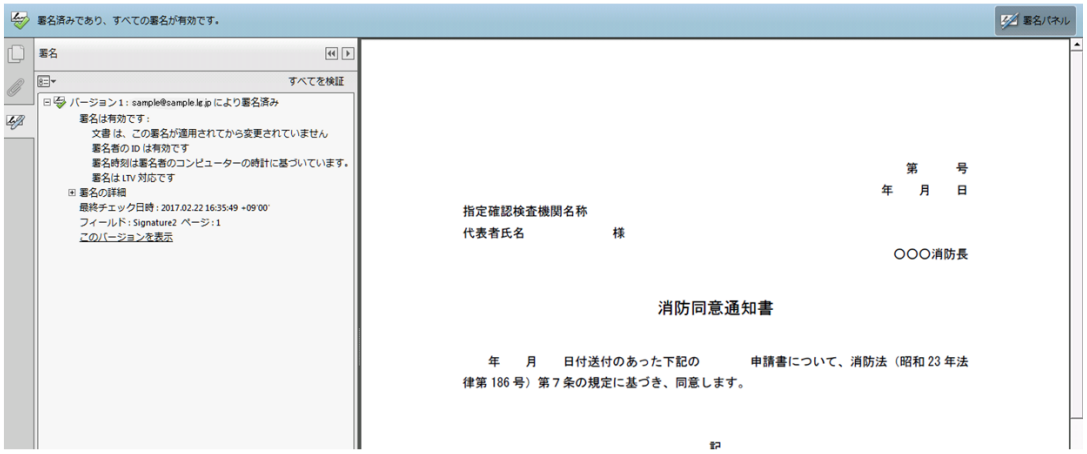
② 消防機関は受領した消防同意依頼書に付与された指定確認検査機関等の電子署名を検証し、問題なければ受理、審査する。

③ 審査結果に問題が無ければ、対象となる確認申請書を特定する識別番号等の情報、同意する旨、消防長等の官職、建築主の氏名等の事案を特定するために必要な事項、交付の日付、同意番号等を記載した消防同意通知書を PDF ファイルにて作成する。

④ 消防同意通知書、消防同意等書類一式の PDF ファイルに消防長等の電子署名を行い、タイムスタンプを付与し、指定確認検査機関等に返送する。なお、消防同意通知書の PDF ファイルの中に対象となる消防同意等書類一式を添付ファイルとして格納したうえで、消防長等の電子署名とタイムスタンプを付与することも可能であり、一回の署名タイムスタンプで PDF ファイル全体に電子署名とタイムスタンプを付与したことになるため効率的である。

⑤ 指定確認検査機関等では、受領した④の消防長等の電子署名とタイムスタンプの検証を行い、問題がなければ③にアーカイブタイムスタンプを付与し電子保存する。

・消防同意通知書へ電子署名



・消防不同意通知書へ電子署名

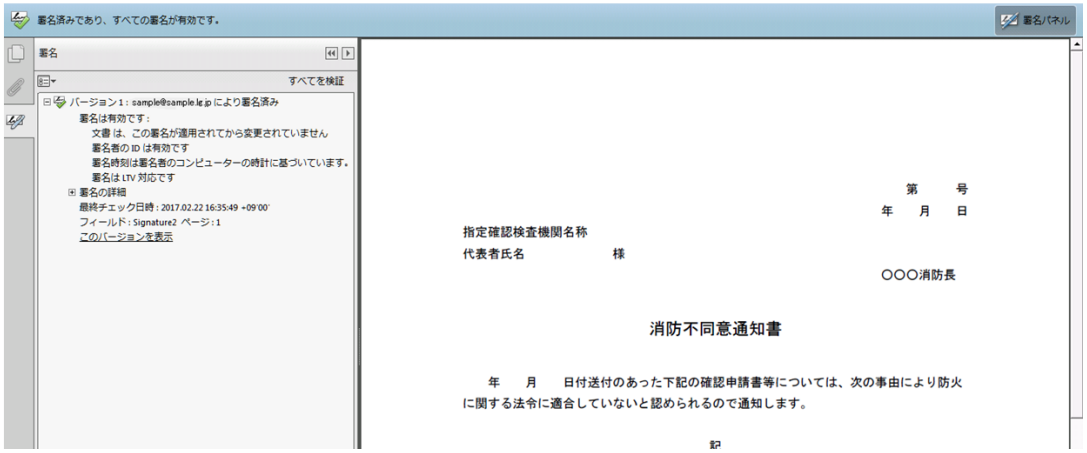


図 15　消防同意通知書の作成イメージ

(3)　消防同意依頼書のみ電子化し消防同意は書面で交付する方法

消防同意依頼書のみ電子化する場合は、消防同意の通知は書面で行うものであるか（1）の①、②を電子化する方法と同様に行えばよいと考えられる。消防同意の方法は従来どおり書面にて行うものとする。「ア」の確認申請書に同意印を押印する方法では、確認申請書の PDF ファイルをプリントアウトして同意印を押印する必要がある。

消防同意の通知を電子化しない場合は、消防長等の電子署名は不要となる反面、受領した電子ファイルを消防側でプリントアウトをする手間がかかり、通知の郵送にかかる時間も短縮されないため効率化の効果は限られたものとなる。

5.9.2　消防通知を電子化する場合

消防通知を電子化する方法について以下に示す。

(1)　指定確認検査機関等では消防通知書を PDF ファイルにて作成し担当者の電子署名を行い、対象となる申請図書等の PDF ファイル（申請者が建築確認申請手続を書面で行った場合は、スキャナーにて 300dpi 以上で読み取った画像ファイルに指定確認検査機関等の電子署名を行ったもの）を消防機関に送信する。

(2)　消防機関は受領した消防通知書に付与された指定確認検査機関等の電子署名を検証し、問題なければ受理する。

5.10既存のデータベースと連動させる場合および非連動の場合

(1) 既存のデータベースと連動させる場合

多くの消防機関では、独自開発のシステムや市販のパッケージシステムを採用している。

このシステムでは、確認申請書等の記載事項を入力しており、消防機関の既存のデータベースとなっている。そのため、既存のデータベースと連動させるべく、消防機関に対し、指定確認検査機関等から電子化した消防同意等書類一式とともに確認申請書等の記載事項データを送信してもらい、そのデータを消防機関のデータベースに取り込むことができれば、従来、紙の確認申請書等を見て手入力していた作業を省略することが可能となる。このように既存のデータベースと連携させることにより、消防機関の消防同意事務を効率化できる。

確認申請書等の記載事項を電子化する際の標準フォーマットとして、ICBA の「申請プログラム」で確認検査・建物の申請時に作成される XML ファイルまたはそれと同等のフォーマットの XML ファイルを推奨する。データ連携用の XML ファイルは消防同意等書類一式の電子ファイルとともに指定確認検査機関等から消防機関へ送信されるものとする。消防機関のデータベースに取り込む際は ICBA の Web サイトで公開されている当該 XML の仕様を参考にされたい。

関連 URL：http://www.icba.or.jp/DBkyougikai/renkei.html

一般財団法人　建築行政情報センター（ICBA）

建築行政共用データベースシステム

申請用サンプルファイル　…確認申請書 XML

送受信用サンプルファイル　…建築計画概要書 XML

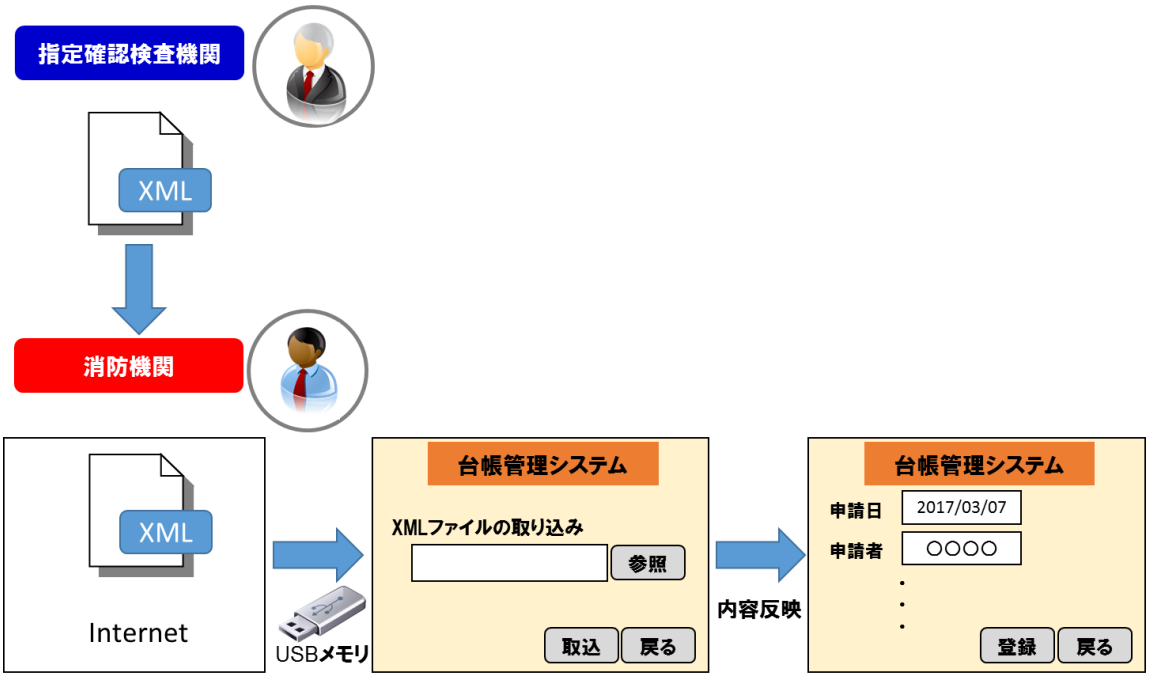


図 16　既存データベースと連動する場合の運用例

(2) 既存のデータベースと非連動の場合

消防機関で導入されているシステムに確認申請書等の記載事項データ等を手入力している場合、この既存のデータベースと非連動となると、消防機関では、消防同意等書類一式を電子申請で受信しても確認申請書等の記載事項は手入力することとなり、消防同意等事務の電子化に伴う効率化が限定的なものとなる。

5.11消防同意等以外の消防法関係の手続きも合わせて電子化する場合

消防同意等以外の消防法関係の手続きが既に電子化されているもの、今後電子化を進めたいと考えられているものを以下に例示する。

(1) 既に電子化されているもの

実際、以下のような申請を電子申請で受け付けているが、その申請数は、紙による申請数と比較すると著しく少ないことから、今後の課題として、電子証明書の普及等が挙げられる。

電子申請可能な申請の例
≪法令に基づく届出≫ 消防計画作成（変更）届出 統括防火・防災管理者選任（解任）届出書 全体についての消防計画作成（変更）届出書

防火・防災管理者選任（解任）届出書 完成検査済証の再交付申請 危険物製造所等品名、数量又は指定数量の倍数変更の届出 危険物保安督者の選任、解任の届出 防災管理者（副防災管理者）選任・解任の届出 危険物製造所等の工期又は所有者等の名称、住所等の変更の届出 ※ 上記以外に、その他火災予防条例等に基づく届出

(2) 今後電子化を進めたいと考えられているもの

① 防火対象物の使用開始の届出等（火災予防条例（例）第四三条）

建物や建物の一部を使用する場合、使用を始める 7 日前までに、建物を使用する者が、管轄する消防機関に届け出する必要がある。

多くの場合、直接持参が条件であるが、防火対象物の使用開始の届出等を電子申請する場合、申請後に電話やメール等で使用検査の日程調整を行うなどの運用になることが考えられる。

② 民泊の電子申請

今後、電子申請が検討されている民泊での手続きについても、消防機関の電子化対応に含める。現時点で、民泊は、旅館業法が適法され、消防法上では宿泊施設となり「消防法令適合通知書」が必要となる。今後そういった民泊関係の手続きにおいて電子申請への対応が想定できる。

5.12消防同意等以外の消防法関係の手続きも合わせて電子化する場合の基本的な留意事項

消防同意等以外の消防法関係の手続きを電子化する場合、申請対象者が多く、定期的に提出される申請を中心に電子化を進めていくと、申請者の利便性に寄与する効果がより大きいものとなる。

現状では、紙申請を受け付けた場合、消防職員が紙の申請書類を見て台帳システムに入力する作業が存在するため、入力項目の多い申請を電子申請に採用することも消防機関側の省力化に貢献できると考えられる。

現状一般的な電子申請システムにおいては、記名・押印に代わる措置として電子署名を行う必要があるため、消防法関係の手続きを電子化する場合においても電子署名に対応したシステム構築が求められる。

5.13文書保存、図面等の保存を電子化する場合

電子申請において、受領した文書や図面等の電子ファイルを電子的に保存する場合は、電子ファイルが原本となるため、長期的な真正性（正当に作成されたものであることが明確で作成以後改ざんされていないことが確認できること）や見読性（保存期間を通じで見

読可能な状態を維持すること）や保存性（記録の滅失の防止ができていること）を確保する必要がある。

具体的な対応策としては以下の内容が挙げられる。

長期的な真正性の確保としては、電子署名の有効性を長期間、確認可能にする標準技術「長期署名フォーマット」を活用して、必要な期間、電子署名の検証を継続して「真正性」を確保することが必要となる。

長期的な見読性の確保としては、記録の所在管理や検索機能、システムの維持管理、システム障害対策としてのシステムの冗長化など保存期間を通じて見読性の維持に必要な対策を講ずることが必要である。

長期的な保存性の確保としては、マルウェアや不正アクセスなどによる記録の滅失の防止対策、バックアップとその履歴の管理、復元手段の確認などの対策等が必要となる。

また、電子ファイルの保存量に適したサーバーのストレージ領域を確保する必要がある。

(1) 文書保存の電子化

消防同意通知書等も確認申請書等と同様に指定確認検査機関等では 15 年保存が義務付けられている（建築基準法第十二条第 8 項、第七十七条の二十九第 2 項等）。電子でも同様の扱いが必要だが、消防機関では法定保存義務は特にない。内規等で電子保存する際は保存年数を定め、アクセス権限管理や情報漏洩対策を行ったうえで保存することが必要となる。

(2) 図面等保存の電子化

消防同意で添付されている図面をスキャン等行い、電子で保存する消防機関は少数であり、紙での保存も竣工後、1 年間程度という状況が多い。目的は、建物完成後の検査で利用するのが最後の利用で、それ以降は、防火対象物の使用開始の届出等で提出された図面を最新図面として保存しているケースが主である。図面を電子で保存している場合、災害発生時、消防車の車載端末からのアクセス、また庁内端末からアクセスできるというメリットが挙げられる。紙図面で保存している場合は、建物図面は、所轄消防署に保存されているものだけとなり、災害発生時等、建物図面を現場に持参することがある。また、災害現場へ図面を持参せず、無線で指示を受ける場合もある。

5.14その他

現在、指定確認検査機関では、4 号建築物を中心に電子で確認審査業務が実施され始めており、タブレット等を用いた検査業務で実績を上げつつある。しかし、大規模な建物の場合、現状では紙で印刷した図面での確認審査が一般的である。従って、4 号建築物を中心とした小型物件から電子化を進めていくことが導入を容易にすると考えられる。

6.　図面等の補正等に関する解説および手続き等運用

本章では、建築確認申請における消防同意および消防通知時に図面等の軽微な補正等が必要となった際に申請者、指定確認検査機関および消防機関との運用手続きについて解説する。

6.1 消防同意等補正の解説

消防同意に係る図面等の補正等については、建築基準法第六条第 1 項で規定する建築基準関係規定にとどまらず、消防法、消防法施行令（昭和三十六年三月二十五日政令第三十七号）、火災予防条例に関する規定の内容もあるため、軽微な補正を含めると多くの確認申請時の計画が補正の対象となり、軽微な補正であっても構造計算等に影響を及ぼす可能性があるため、補正等の通知は迅速に行う必要がある。

消防通知に係る図面等の補正については、ほとんど存在せず、手交または郵送された書類不足による対応のみと思われるため、以降の記載は消防同意の手続きのみとする。

6.2 手続き（建築確認申請および消防同意等が書面による場合の対応）

消防同意に係る補正の手続きについては、「消防法等の一部を改正する法律等の運用について」（通知）（平成 11 年 4 月 28 日　消防予第 92 号）の別添 2「指定確認検査機関に係る消防同意事務等標準処理マニュアル」の第 2 図書の審査等　1 同意期間 (2)終了日 イ.「同意期間中に図書の不備等があると認める場合は、指定確認検査機関に対して電話等の手段によりその旨を通知したうえ、通知した当日から図書の不備等が補正される日までの間は、同意期間から除くこととし、その旨連絡すること。」とあり、消防機関と指定確認検査機関等との手続きであることが原則となる。

具体的には、以下の手続きとなる。

(1) 消防機関より補正等を求める内容を指定確認検査機関等へ対面または電子メール等（FAX を含む）で通知する。
(2) 指定確認検査機関等は補正等を求める内容を確認し申請者へ通知する。(消防機関から直接申請者へ通知する場合については、消防機関は指定確認検査機関等へ確認してから行う）

指定確認検査機関等は補正等を求める内容を確認する際に、副本があれば内容の確認を行うことができるが、正本、副本が消防機関にある場合は、内容の確認は行うことができないため、補正等を求める通知があった経過事実の確認のみとなる。

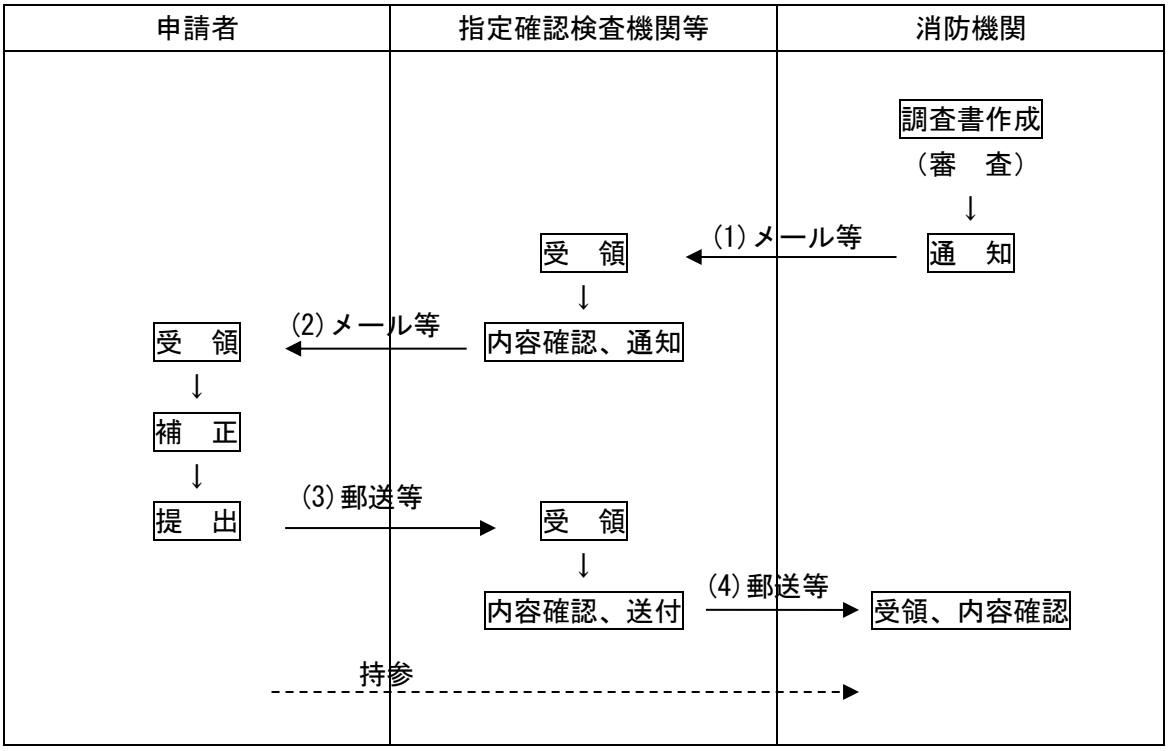
図面等の補正等については、原則、申請者は補正した図面等を指定確認検査機関等へ提出することになる。申請者が直接、消防機関へ図面等を持参し補正する場合は、指定確認検査機関等は同意後に消防機関から補正等を行った図面等を受け取ることになる。

申請者が直接、消防機関へ図面等を持参し補正する理由としては、補正等の内容を消防

機関に直接確認したいためや、補正等を行った図面等を指定確認検査機関等経由で郵送するための時間等の節約が考えられる。

具体的には、以下の手続きとなる。
(3) 申請者が補正等を行った図面等は、申請者より指定確認検査機関等に提出される。
(4) 指定確認検査機関等は補正等の内容を確認し消防機関へ図面等を持参または郵送する。
　補正等を行った図面等の提出の手続きについては、今回ヒアリングを行った消防機関では原則のとおりの運用のほか、申請者が直接、消防機関へ赴き補正等を行う場合もあるとの回答があった。

《補正等に関する手続きフロー》



6.3 手続き（建築確認申請が電子で消防同意等が書面による場合の対応）
　建築確認申請を電子申請で行う場合、図面等は設計者等が電子署名した電子ファイルであり、電子署名後の電子ファイルを変更することはデータの改ざんにあたるため、行うことができない。(書面でいう追記や訂正ができない)
　補正等が必要となる場合は、設計者等は補正等を行った電子ファイルに元の電子ファイルを含めた全体に対して新たに電子署名を付与して提出するか、補正等を行った電子ファイルのみに電子署名を行い提出する必要がある。

「電子申請による建築確認に係る消防同意等事務の取扱いについて」(平成 27 年 2 月 12 日消防予第 53 号）の通知により、指定確認検査機関等と消防長等は事前に実施方法を協議

し、合意したうえで行うこととある。しかしながら現状の消防同意等事務の運用は書面にて行われている。このため、指定確認検査機関等は取り違え防止のための識別番号を記載した電子ファイルを書面に出力して消防機関へ送付する方法をとっており、電子化による利便性が損なわれている状況である。

ただし、書面による運用と異なり、確認申請時の図面等（電子ファイル）が指定確認検査機関等に残っているため、消防機関より補正等を指定確認検査機関等に通知した際に、指定確認検査機関等は補正等の内容を容易に確認することができる。

図面等の補正等を行った電子ファイルについては、指定確認検査機関等が新たに取り違え防止のための識別番号を記載した電子ファイルを書面に出力して、消防機関へ送付することが必要となるため、申請者は必ず指定確認検査機関等に提出することとなるが、指定確認検査機関等から消防機関までの郵送のための時間が軽減されず、申請者にとっては電子化による利便性が損なわれたままである。

また、申請者が直接、消防機関へ電子ファイルではなく、書面による補正等を行う場合は、「書面による運用」と同じ方法となる。また、このとき指定確認検査機関等は図面等の補正等の内容を確認することができない。

6.4 手続き（消防同意等が電子化された場合の対応）

電子化の利便性が損なわれないためには、申請者と指定確認検査機関との間だけでなく、指定確認検査機関と消防機関との間でも消防同意等が電子的に行える仕組みの整備が必要となる。

消防同意等が電子化されることにより、指定確認検査機関等から消防機関までの郵送時間（経費を含む）の軽減が見込まれるとともに、消防機関内で図面等の送付がある場合についても、電子化により書面での運用の際に必要となる運搬のための手間や時間を軽減することができ、消防同意等事務のための時間を確保することができる。

申請者が補正した図面等（電子ファイル）を提出する際も、申請者と指定確認検査機関等との間で情報通信技術を利用することで郵送時間の軽減となる。指定確認検査機関等は提出された図面等（電子ファイル）の補正された内容を確認することができ、消防機関との情報通信技術を利用することで更なる郵送時間の軽減となり、消防機関は消防同意等事務を再開できることとなる。

ただし、書面による運用と同様に消防機関と申請者との間で補正内容を確認するために、申請者が直接消防機関へ図面等を持参し内容を確認することは今後も考えられるが、申請者から指定確認検査機関等を経由して消防機関までの情報通信技術が整備されていれば、消防機関へ書面で提出しなくとも最低限の時間で図面等が送付できるため、申請者の利便性は確保でき、住民サービスの向上につながる。

また、補正等により消防機関で記録する台帳等の変更がある場合についても、指定確認

検査機関等から提供する確認申請書等の情報を電子ファイルで受領することにより台帳等へ必要な情報を取り込むことができる。

7. PDF ファイルを利用した電子署名の運用例

本章では、PDF ファイルを利用した電子署名の運用例を示す。

なお、本章では、以下の略称を利用している。

例えば、「署名＝機関」と記載されている場合は、「指定確認検査機関が電子署名を付与したファイル」という意味になる。

【署名者の略称】

機関…指定確認検査機関

申請者等…申請者および設計者（委任状がある場合は、設計者のみ）

設計者…建築図面を作成した建築士

消防…消防機関

署名…電子署名

ＴＳ…タイムスタンプ

また、確認申請書等データ（XML）は、必須ではなく任意とし、事前に指定確認検査機関等との調整事項となり、建築計画概要書データになることも想定される。

本章では、図面は 1 ファイル内に複数の図面が存在する前提となっているが、実際の運用では、1 図面 1 ファイルの運用も考えられる。

消防通知の場合は、消防同意依頼書の代わりに消防通知書を使用するものとする。

複数ファイル送信する場合、複数ファイルをそのまま送信する方法と PDF ファイルの中に添付して送信する方法が考えられる。「図 17 消防同意依頼書にファイルを添付するイメージ」では、PDF ファイルに添付したイメージ図を示し、消防同意依頼書の PDF ファイルに確認申請書、確認申請書等データ、建築計画概要書、図面一式が添付されているイメージを表している。

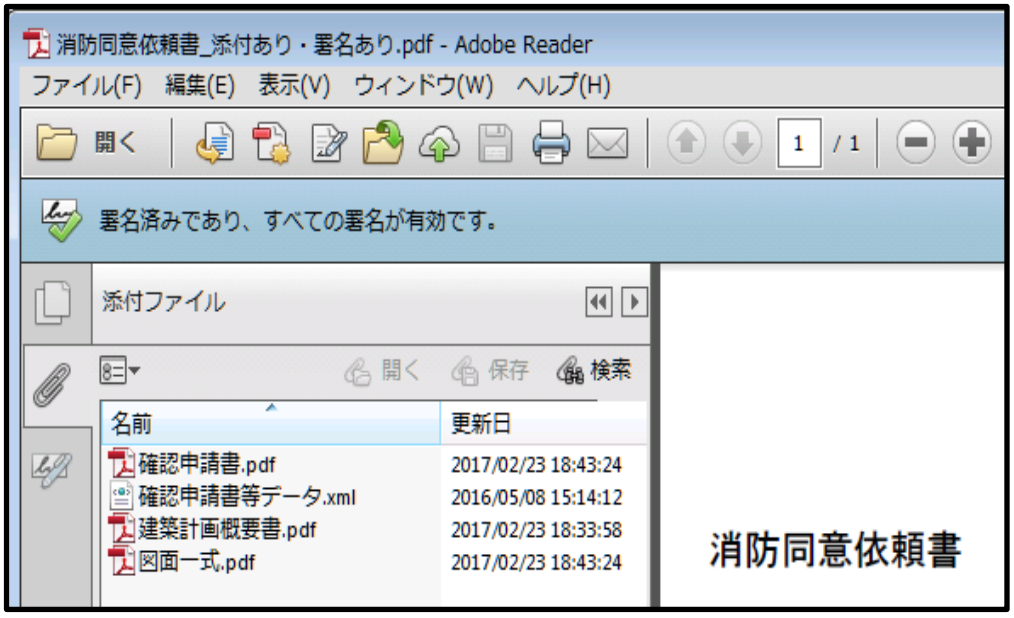
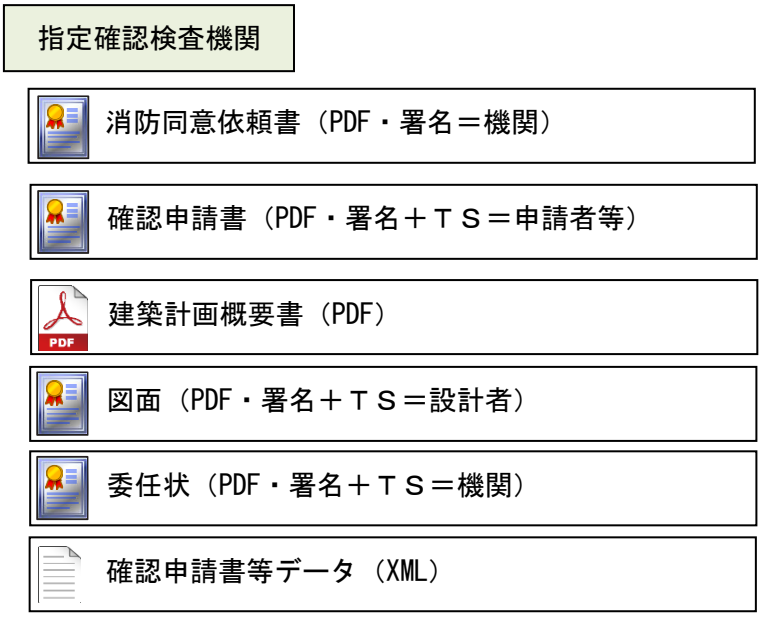


図 17　消防同意依頼書にファイルを添付するイメージ

7.1 指定確認検査機関から消防同意依頼書を送信する場合

7.1.1 指定確認検査機関が消防同意等書類一式を個別ファイルにて送信する方法

指定確認検査機関が消防同意依頼書および委任状をスキャンした電子ファイルに電子署名・タイムスタンプを付け、それ以外の PDF ファイルとともに送信する方法となる。各ファイルには以下のように電子署名が付されている。消防機関で受領後は、消防同意依頼書に付された確認検査機関の電子署名の正当性の検証および、それ以外のファイルに付された電子署名の検証を行う必要がある。



(1) メリット

処理が単純化でき PDF 閲覧･編集ソフトの添付ファイル機能を必要としない。

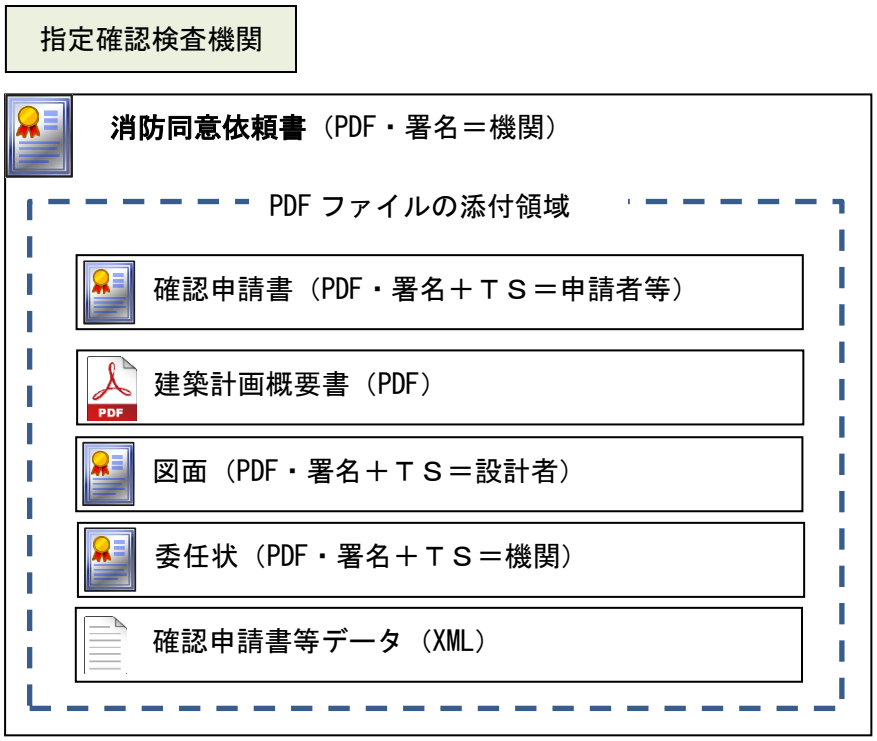
(2) デメリット

PDF 閲覧・編集ソフトの添付ファイル機能を使わないため、送信ファイル数が多くなる。

消防機関では、消防同意依頼書に付された確認検査機関の電子署名の正当性の検証および、それ以外のファイルに付された電子署名の検証を行う必要がある。

7.1.2　指定確認検査機関が消防同意依頼書に消防同意等書類一式を添付する方法

指定確認検査機関が消防同意依頼書に消防同意等書類一式（委任状は指定確認検査機関でスキャンした電子ファイルに電子署名・タイムスタンプを付与）を添付したうえで、電子署名を付け送信する方法となる。各ファイルには以下のように電子署名およびタイムスタンプが付されている。



(1) メリット

消防機関では、消防同意依頼書に付された確認検査機関の電子署名の正当性の検証だけ行えばよい。

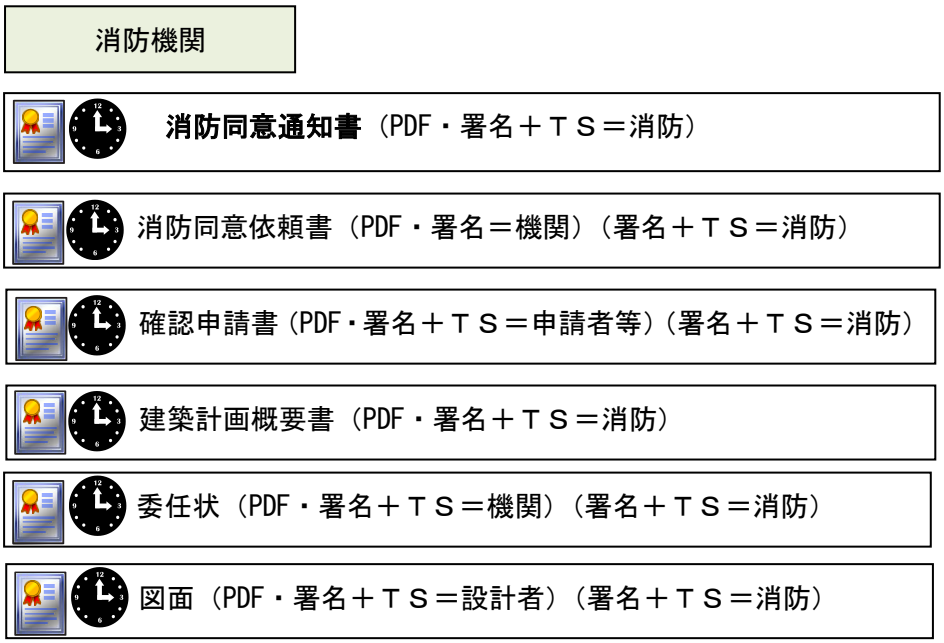
(2) デメリット

PDF 閲覧・編集ソフトの添付ファイル機能を必要とし、添付ファイルの内容確認をする場合に PDF ファイルから取り出す必要がある。

7.2 消防機関から消防同意通知書を送信する場合

7.2.1　消防機関が消防同意等書類一式を個別ファイルにて送信する方法

消防機関が消防同意通知書および消防同意等書類一式に電子署名とタイムスタンプを付け、ファイルとともに送信する方法となる。各ファイルには以下のように電子署名およびタイムスタンプが付されている。



(1) メリット

処理が単純化できPDF閲覧･編集ソフトの添付ファイル機能を必要としない。

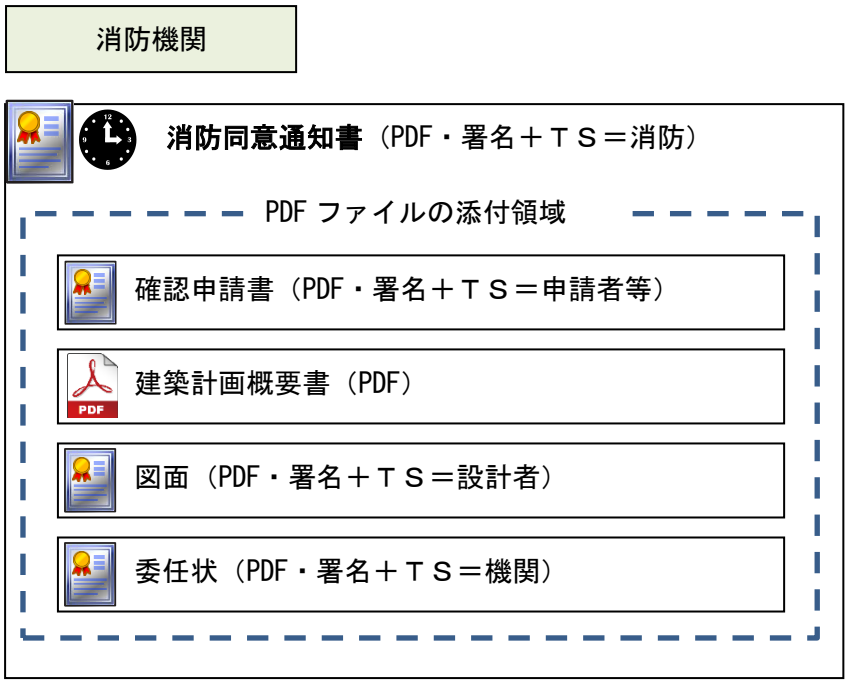
(2) デメリット

PDF閲覧・編集ソフトの添付機能を使わないため、電子署名・タイムスタンプを付与した送信ファイル数が多くなる。

消防機関では、消防同意通知書および、それ以外のファイル個別に電子署名を行う必要がある。

7.2.2　消防機関が消防同意通知書に消防同意等書類一式を添付する方法

消防機関が消防同意通知書に消防同意等書類一式を添付したうえで、電子署名およびタイムスタンプを付け送信する方法となる。各ファイルには以下のように電子署名およびタイムスタンプが付されている。



(1) メリット

消防機関では、消防同意通知書にのみ、電子署名およびタイムスタンプを付与すれば済む。

(2) デメリット

PDF 閲覧・編集ソフトの添付ファイル機能を必要とし、添付ファイルの内容確認をする場合に PDF ファイルから取り出す必要がある。

7.3 電子署名の検証方法

(1) Adobe Acrobat Reader（無償）での検証方法

インターネットに接続された環境で、PDF ファイルを開くと、以下のように青い四角で囲まれた電子署名に関する表示を確認することができる。インターネット接続しないと、失効状態を認証局へ確認できないので検証が完了できない。

「電子申請による建築確認に係る消防同意等事務の取扱について（通知）」（平成 27 年 2 月 12 日消防予第 53 号）において、以下の項目について検証することとしている。「図 18　署名の検証確認」、「図 19　Adobe Acrobat Reader の証明書ビューア」にて、検証項目部分を示す。

① 正当な認証局が発行している本人の電子証明書であること
② 電子証明書の有効期限が切れていないこと
③ 電子証明書が失効していないこと
④ 署名対象データが改ざんされていないこと

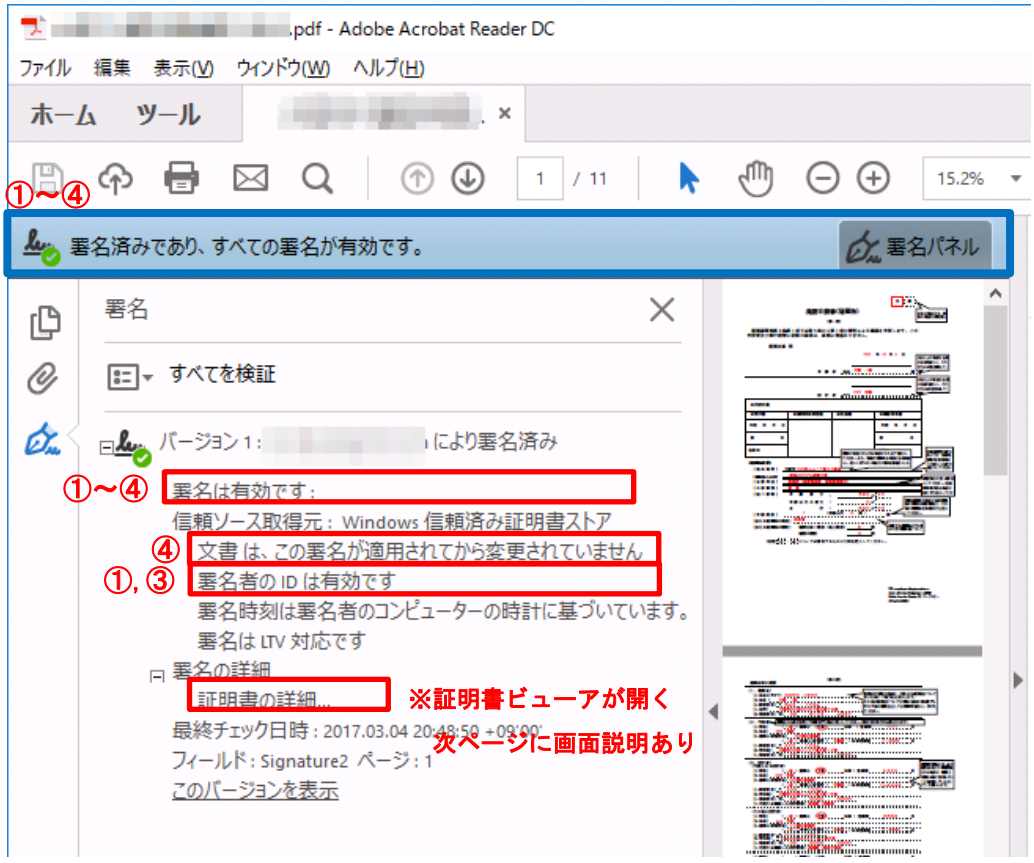


図 18　署名の検証確認

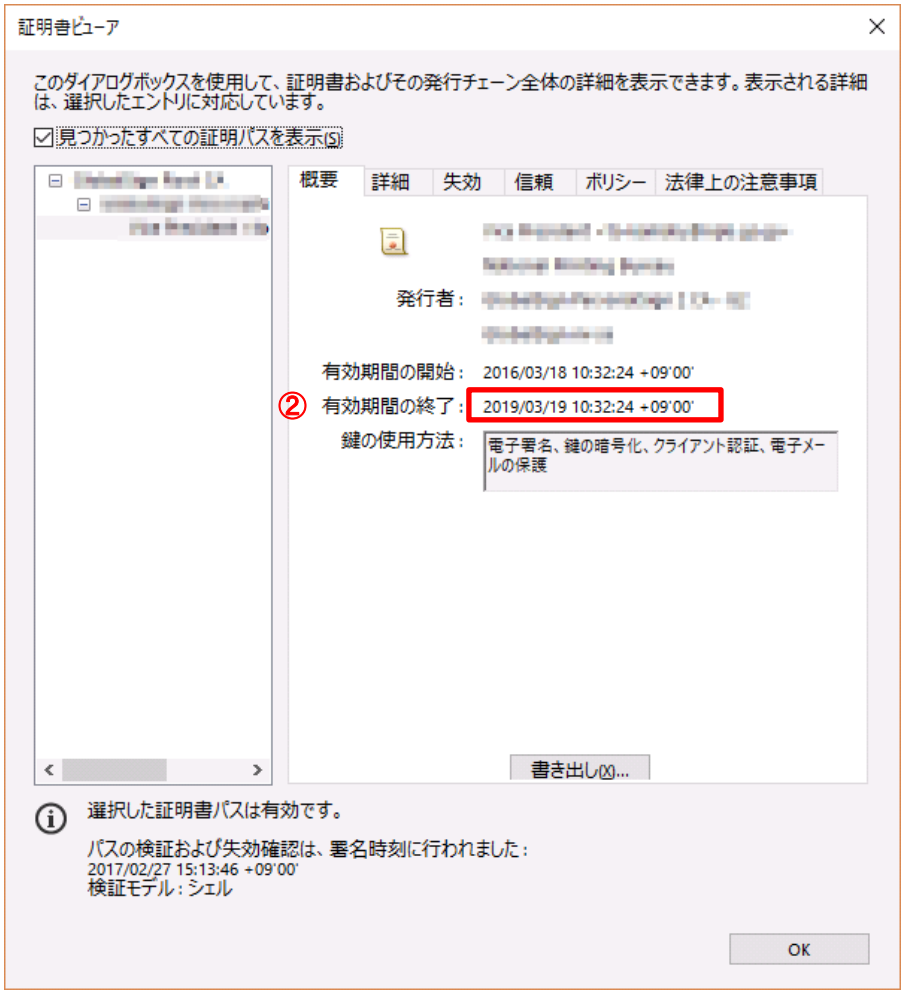
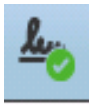


図 19　Adobe Acrobat Reader の証明書ビューア

電子署名状態のアイコンは、「図 20　Adobe Acrobat Reader のアイコン説明」に示す種類がある。電子署名状態アイコンを確認することで、電子署名に利用された電子証明書の信頼性が確認できる。

パターン1			
署名済みであり、すべての署名が有効です。			
 Adobe Reader XI	 Adobe Acrobat Reader DC	信頼された認証局から発行されているか	○
		有効期間内か	○
		失効されていないか	○
		電子署名後に変更されていないか	○

パターン2			
署名済みであり、すべての署名が有効です。 ただし、最終署名の後に署名されていない変更があります。			
 Adobe Reader XI	 Adobe Acrobat Reader DC	信頼された認証局から発行されているか	○
		有効期間内か	○
		失効されていないか	○
		電子署名後に変更されていないか	×

パターン3			
少なくとも1つの署名に問題があります。			
 Adobe Reader XI	 Adobe Acrobat Reader DC	信頼された認証局から発行されているか	?
		有効期間内か	?
		失効されていないか	?
		電子署名後に変更されていないか	?

パターン4			
無効な署名があります。			
 Adobe Reader XI	 Adobe Acrobat Reader DC	信頼された認証局から発行されているか	○
		有効期間内か	○
		失効されていないか	×
		電子署名後に変更されていないか	?

パターン5			
検証が必要な署名があります。			
 Adobe Reader XI	 Adobe Acrobat Reader DC	信頼された認証局から発行されているか	?
		有効期間内か	?
		失効されていないか	?
		電子署名後に変更されていないか	?

図 20　Adobe Acrobat Reader のアイコン説明

パターン 3 については、電子証明書の何について問題があるのかを実際に確認する

必要がある。

「失効情報にアクセスできない、または、電子署名に利用された電子証明書が有効期間外となっている」場合には、有効期間の確認を行う。問題がない場合は、認証局の失効情報にアクセスできていないことになるため、CRL 配布点を確認し、その URL にアクセスできるかを確認する。

「電子署名に利用された電子証明書は、信頼された認証局から発行されていない」と表示される場合は、Adobe Acrobat Reader 等に、電子署名に利用された電子証明書を発行した認証局の証明書が、信頼済み証明書の一覧に存在していないためである。信頼された認証局からの発行であることが確認できる場合は、その認証局の証明書をインストールする必要がある。

パターン 5 については、Adobe Acrobat Reader 等が文書内の署名を検証していない状態であるため、「すべてを検証」をクリックすると、1 から 4 のパターンに変化する。

参照[3]

[3] 電子認証局会議　電子証明書利用時の操作方法 http://www.c-a-c.jp/operation/

8.　各消防機関における電子化の対応に必要なセキュリティ対策

本章では、電子化することによって起こりうるセキュリティの脅威および対策について解説する。

8.1 セキュリティ脅威とその対策

消防同意等の電子化を行うにあたり、インターネットと接続した端末で建築の情報や建築図面を送受信する状況が想定される。この際に、まず、留意しなければならない点が、情報漏洩である。

平成 27 年 6 月、日本年金機構の複数の端末がウイルスに感染し、政府関係機関の被害としては、最大規模となる 125 万件の個人情報が漏洩した。これは、添付ファイル付きメールや外部 URL が記載されたメールを開封し、実行したことが感染原因とされた。その後、攻撃者がウイルスを使ってネットワーク内の情報を探索し、個人情報の搾取を行ったとみられている。この際、攻撃の検知は、外部機関からの指摘で発覚した。このように情報漏洩は、気が付かないうちに行われていることがあることを認識し、セキュリティ対策を行うことが必要である。

ここでは、消防同意等事務を行う一般職員向けと情報システム管理者向けのセキュリティ対策に分け、対策方法を示す。

8.1.1　一般職員および情報システム管理者のセキュリティ対策

(1) ソフトウェアの脆弱性対策

OS やアプリケーションの脆弱性が起因した攻撃の一つとして、ゼロデイ攻撃が挙げられる。これは、脆弱性情報が公開された場合、その欠陥を解消するための修正プログラム等が公開されるが、脆弱性が発見されてから、修正プログラム等の対策が提供されるまでの時間差を利用して行われる攻撃のことである。これを予防するためには、ソフトウェア会社等から一時的な回避策が提示されている場合があるので、その回避策に従い対応を検討することが必要となる。

一般職員の対策としては OS、Adobe Flash Player、Java、ウイルス対策ソフト等のソフトウェアの更新が行われる設定になっているか確認し定期的に最新の状態に保つ必要がある。

情報システム管理者の対策としては、システムが自動で更新されるような設定にすることや、脆弱性情報を定期的に入手し、ゼロデイ攻撃の可能性がある場合は回避策を一般職員へ周知徹底することが必要となる。

(2) ランサムウェア対策

ランサムウェアとは、電子メール、URL、添付ファイル等により標的とされたパソコン等をウイルス感染させ、保存された電子ファイルを暗号化し、利用者のアクセスを不可能な状態にし、暗号化を解除するため、身代金として金銭を要求する悪意あるソ

フトウェアである。近年急増している攻撃である。たとえ、身代金を支払ったとしても、利用不可能にされたデータが元に戻る保証はないため、ランサムウェアの被害にあわないように注意する必要がある。

一般職員の対策としては、OS、ウイルス対策ソフトを含むソフトウェアを最新の状態に保つ必要がある。また、不用意に電子メールの添付ファイルは開かないことが挙げられる。

情報システム管理者の対策としては、保存データを異なるネットワーク上の端末へ定期的にバックアップすることや「8.1.4 総務省の取り組み」に記述してある、一般職員向けパソコンをインターネット接続系ネットワークから分割する対策が挙げられる。

(3) Web サイト改ざんからのウイルス対策

Web サイトからウイルスに感染させる手口の一つとして、Web サイトに配信される広告に、不正なコードを混入させ、閲覧した利用者を悪意あるサイトに誘導する「マルバタイジング」と呼ばれる攻撃が確認されており、アプリケーションソフトやブラウザの脆弱性を悪用するものである。

一般職員の対策としては、OS、ウイルス対策ソフトを含むソフトウェアを最新の状態に保つ必要がある。また、問題の解決に至るまではアプリケーションソフトを無効化することも防御対策の一つである。

情報システム管理者の対策としては、ウェブアプリケーションに脆弱性があるか定期的に調査し最新の状態に保つ必要があるほか、運用している Web サーバーに改ざん検知システムを導入する等の対策が挙げられる。

(4) マクロウイルス対策

マクロウイルスとは、Microsoft Office に搭載された単純作業を自動化するためのマクロという機能を悪用して感染するウイルスである。1990 年代後半から 2000 年代前半頃に流行し、その後はほとんど確認されていなかったが、平成 26 年からマクロウイルスによる攻撃が再び発生し、増加傾向にある。増加した要因として、実在の組織をかたり、不特定多数にマクロウイルスを添付したメールをばらまく攻撃に利用されたことが挙げられる。

一般職員の対策としては、OS、ウイルス対策ソフトを含むソフトウェアを最新の状態に保つ必要がある。また、不用意に電子メールの添付ファイルは開かないことが挙げられる。

(5) フィッシング詐欺対策

主にインターネットバンキング等の各種サービスの認証情報を盗むことを目的としたフィッシング詐欺が継続している。インターネットバンキングに限らず、インターネット上で利用するサービスの ID・パスワードは、攻撃者に狙われている状況にあることを認識し、適切な管理が求められる。

一般職員の対策としては、少しでも不審なメールに返信しないことや、信頼される送信者以外からのメール本文中にあるリンクはクリックしないよう注意する必要がある。また、SSL/TLS を使用し暗号化されたサイトの場合、正規のサイトであるかを確認するため、Internet Explorer 等のブラウザでサーバー証明書を確認してウェブサイトの所有者等で問題のないことを確認したのち、ID・パスワードの入力を行うことが有効な対策となる。

(6) 内部者による情報の不正な持ち出し対策

組織内の機密情報の持ち出しといった内部不正は、社員や職員等の正規の権限を有する者によって行われるため、これを防ぐことは容易ではない。不正に持ち出された機密情報は、金銭を得るために売買の対象にされ、組織にとっては信用や利益に直接影響を与える重大な脅威である。情報の持ち出し手段は「USB メモリ」が 43.6%と最も多く、電子メールやパソコンを用いるケースが続いている。

項目	1 位		2 位		3 位	
不正行為の動機	ルールを知っていたが、うっかり違反した	40.5%	ルールを知らずに違反した	17.5%	業務が忙しく終わらせるため持ち出した	16.0%
対象情報	顧客情報	52.3%	技術情報	35.8%	営業計画	26.2%
持ち出し手段	USB メモリ	43.6%	電子メール	34.3%	パソコン	25.5%

表 1 情報持ち出しの動機、対象情報、手段（出展：IPA「内部不正による情報セキュリティインシデント実態調査」を元に編集）

一般職員の対策としては、USB メモリを持ち帰らないなど利用ルールを遵守する必要がある。

情報システム管理者の対策としては、パソコン等で USB メモリの利用制限を検討することや情報セキュリティルールの周知を定期的に行うこと、定期的に情報セキュリティ教育を実施することが必要だと考えられる。また、ネットワークの利用制限を設けることや、アクセスログでの監視、庁内ネットワークの監視体制を強化することなどが考えられる。

(7) 電子メールの取り扱いについて

通常の電子メールは、暗号化されていない文章である平文で通信することが一般的であり、すべて第三者に見られている可能性があると認識してやり取りを行うことが重要である。平文で通信を行うことにより、盗聴やなりすまし、改ざんの危険性が出てくる。また、秘密にしたい内容を送付する際、1 通目に添付ファイルを ZIP ファイル等で暗号化し、2 通目にパスワードのみを送付する場合、第三者に見られている可能性を考えると、この方法はセキュリティに対して不十分である。パスワードは、電子メ

ール以外の方法で事前にルールを決めておき、それを利用するか、その都度、電子メール以外の方法で伝達することが望ましい。また、電子メールの署名・暗号化方法としては、S/MIME が挙げられ、必要に応じて利用することが望ましい。S/MIME とは、Secure Multipurpose Internet Mail Extensions の略で、電子メール用のセキュリティ技術で、認証局が発行する「電子証明書」によって送信者の本人性を確認することが可能となる。送信者によるメールへの電子署名と暗号化の機能を利用することができる。

8.1.2 情報システム管理者によるセキュリティ対策

(1) 不正アクセスによる情報漏洩対策

管理や対策が不十分なサーバーに存在する脆弱性を狙った、外部からの不正アクセスによる情報漏洩が発生している。個人情報だけでなく、クレジットカードの情報も窃取されている事例もある。代表的な攻撃手段として、「SQL インジェクション攻撃」がある。多くのサーバーは、データベースとの通信に SQL と呼ばれる言語を使用しており、データベースと連携した Web アプリケーションの多くは、利用者からの入力情報を基にデータベースへの命令文を組み立てている。攻撃者は、Web アプリケーションと連動しているデータベースへ問い合わせを行うパラメータとして、不正な SQL 文を与えることにより、情報を改ざんまたは、不正に引き出すことを試みる。発生しうるリスクとしては、以下のものが挙げられる。

・非公開情報が閲覧されてしまうことによる情報漏洩
・情報の改ざんや消去
・ユーザーID やパスワードが漏洩することによる不正アクセスの助長

対策としては、サーバーにおける基本的なセキュリティ対策（セキュリティパッチの適用、不要なアカウントの削除、ログの取得等）やデータベースの保護（ユーザーの一元管理、格納データ暗号化、監査機能等）、ファイアウォールの設定が重要となる。また、アプリケーションを開発する際に、プログラミングの時点から不正な SQL 文を実行しないよう対策することも必要である。

基本的な内容ではあるが、パスワードに大文字・小文字・数字・記号を混ぜて使用することや、最低 8 文字以上の長さにする設定も有効な対策である。

(2) Web サーバーの脆弱性診断による対策

Web サイトに潜む脆弱性は多種多様に存在し、セキュリティの専門技術者による診断により適切な対策方法を講じることが望ましい。Web アプリケーション診断サービスを用いることにより、様々な脆弱性や潜在要因を洗い出して適切な対策方法の策定ができ、不正アクセス等の脅威を低減することが可能になる。Web アプリケーション診断サービスのほか、サーバー・ネットワーク機器の脆弱性診断サービスも合わせて実施することが望ましい。

(3) Web サーバーへのアクセスを不可能にする攻撃への対策

Web サーバーへのアクセスを不可能にする攻撃として、DoS（Denial of Service）攻撃がある。サーバーに大量のデータを送信して多大な負荷をかけ、サーバーのパフォーマンスを低下させたり、機能停止に追い込んだりする攻撃のことである。公開 Web サーバーへの DoS 攻撃としては「DDoS 攻撃」が挙げられる。複数のネットワークに分散する大量のコンピューターが一斉に特定のネットワークやコンピューターへ接続要求を送出し、通信容量を溢れさせて機能を停止させてしまう。攻撃対象になった場合の対策としては、ネットワーク回線の増強や、複数のサーバーによる負荷分散が可能な CDN（Contents Delivery Network）の利用等で悪影響を緩和できる場合がある。そのほか、ネットワーク上の振る舞いをチェックし、分析することで悪意あるアクセスを検知し、接続を遮断する DoS 対策装置の導入も検討できる。攻撃者によっては、攻撃停止の対価として金銭を要求してくる場合があるが、金銭要求に対して支払うことは得策ではない。また、攻撃者にサーバーを踏み台にされないための対策としては、最新バージョンのソフトウェアを使用する、必要最低限のアクセスのみ許可する等の基本的なセキュリティ対策が必要である。

(4) 庁内の CSIRT（情報セキュリティに関する統一的な窓口）を有効活用した対策

サイバーセキュリティ基本法（平成二十六年十一月十二日法律第百四号）第 5 条では「地方公共団体は、基本理念にのっとり、国との適切な役割分担を踏まえて、サイバーセキュリティに関する自主的な施策を策定し、及び実施する責務を有する。」とされている。また、総務省発行の「地方公共団体における情報セキュリティポリシーに関するガイドライン(平成 27 年 3 月版)」では、CSIRT の設置が求められている。

平時より CSIRT を活用し、サイバー攻撃の予兆をつかむためのログ監視、情報セキュリティルールの制定・見直し、情報セキュリティに関する周知活動、情報セキュリティ事故を想定した訓練等を行うことが重要だと考えられる。

総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン(平成 27 年 3 月版)」 [4]

情報セキュリティに関する統一的な窓口(「庁内の CSIRT (Computer Security Incident Response Team)」以下、「庁内の CSIRT」という。)の設置

情報システムに対するサイバー攻撃等の情報セキュリティインシデントが発生した際に、情報セキュリティインシデントのとりまとめ、CISO・CIO への報告、報道機関等への通知・公表、関係機関との情報共有など、情報セキュリティインシデントに関するコミュニケーションの核となる体制を危機管理等の既存の枠組み等を活用するなどして構築する必要がある。

また、地方公共団体情報システム機構(自治体 CEPTOAR)等の関係機関や他の地方公共団体の同様の窓口機能、外部の事業者等と連携して体制を強化することが求められる。

8.1.3 情報セキュリティマネジメントシステムの構築

情報セキュリティマネジメントシステム(ISMS:Information Security Management System)は、情報資産のセキュリティを確保、維持するための、人的、物理的、技術的、組織的な対策を含む、経営者を頂点とした組織的な取り組みのことである。コンピューターウイルスによる被害や情報漏洩等、情報資産を脅かす要因が著しく増加しており、これらの脅威に対して適切にリスクアセスメントを実施して、組織における総合的な情報セキュリティを確保するためには、ISMS の構築・運用が重要となっている。ISMS が達成すべきことは、リスクマネジメントプロセスを適用することによって情報の機密性、完全性および可用性をバランス良く維持・改善し、リスクを適切に管理しているという信頼を利害関係者に与えることにある。そのためには、ISMS を、組織のプロセスおよびマネジメント構造全体の一部とし、かつその中に組み込むことが重要である。ISMS を効率よく行うための手法が、PDCA(Plan - Do - Check - Act の略)である。品質改善や環境マネジメントでよく知られた手法で、次のステップを繰り返す。

1. Plan:問題を整理し、目標を立て、その目標を達成するための計画を立てる
2. Do:目標と計画をもとに、実際の業務を行う
3. Check:実施した業務が計画通り行われて、当初の目標を達成しているかを確認し、評価する
4. Act:評価結果をもとに、業務の改善を行う

[4] 総務省 地方公共団体における情報セキュリティポリシーに関するガイドライン (http://www.soumu.go.jp/denshijiti/jyouhou_policy/)

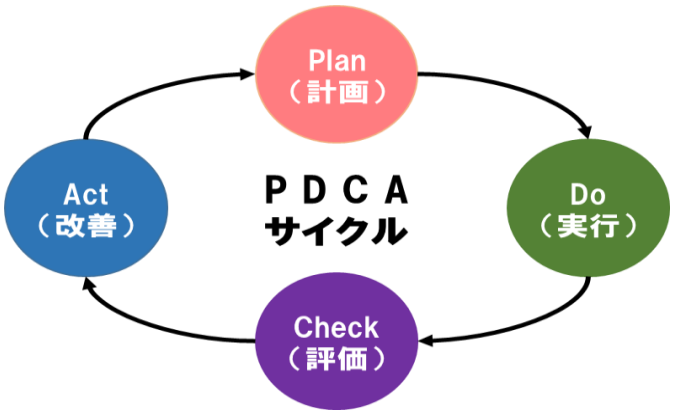


図 21　PDCA サイクル

情報セキュリティ対策は一度行ったら終わりではなく、常に積極的に対策を行っていかなければ、新たな脅威に対応できないという側面を持っているため、環境の変化に合わせて絶えず見落としと改善が求められる。組織のセキュリティ対策における目標達成レベルを継続的に維持改善するために PDCA サイクルを繰り返すのである。

8.1.4　総務省の取り組み

日本年金機構における個人情報流出事案を受けて、総務省から、以下文書が各都道府県知事、各市区町村長宛てに送付され、情報セキュリティ対策の強化を図ることが必要であるとの通達があった。

平成 27 年 12 月 25 日 総行情第 77 号「新たな自治体情報セキュリティ対策の抜本的強化について」 以下の三層からなる対策で、情報セキュリティ対策の抜本的強化を図る自治体を支援。 ①マイナンバー利用事務系では、端末からの情報持出し不可設定等を図り、住民情報流出を徹底して防止 ②マイナンバーによる情報連携に活用される LGWAN 環境のセキュリティ確保に資するため、LGWAN 接続系とインターネット接続系を分割 ③都道府県と市区町村が協力して、高度な情報セキュリティ対策を講じるため、自治体情報セキュリティクラウドを構築 【Ｈ２７補正予算 ２５５億円】

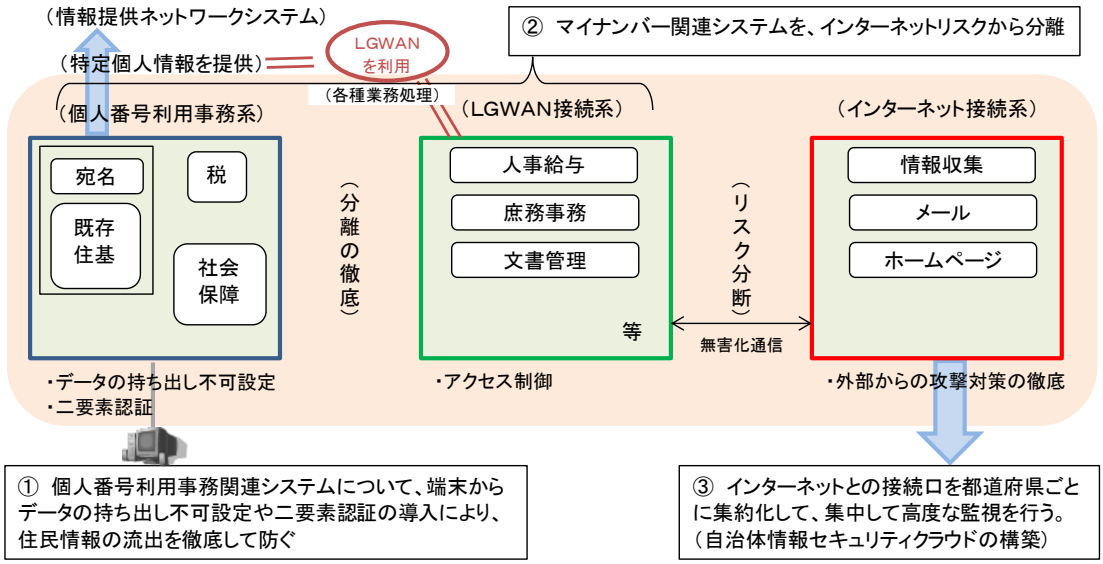


図 22　情報セキュリティ対策強化 [5]

LGWAN 接続系とインターネット接続系を分割する方法として、以下の 2 つが考えられる。

(1) 端末の物理的な分離

LGWAN 接続系とインターネット接続系で端末を物理的に分ける方法。

(2) 仮想ブラウザによる分離

仮想ブラウザとは、OS の機能等に依存せず、完結した環境で動作する Web ブラウザ。ウイルスの攻撃の他、個人情報やパスワードの窃盗を試みるスクリプトが存在していても、情報を遮断できる。

[5]平成 27 年 12 月 25 日 総行情第 77 号「新たな自治体情報セキュリティ対策の抜本的強化について」　自治体情報セキュリティ強化対策事業

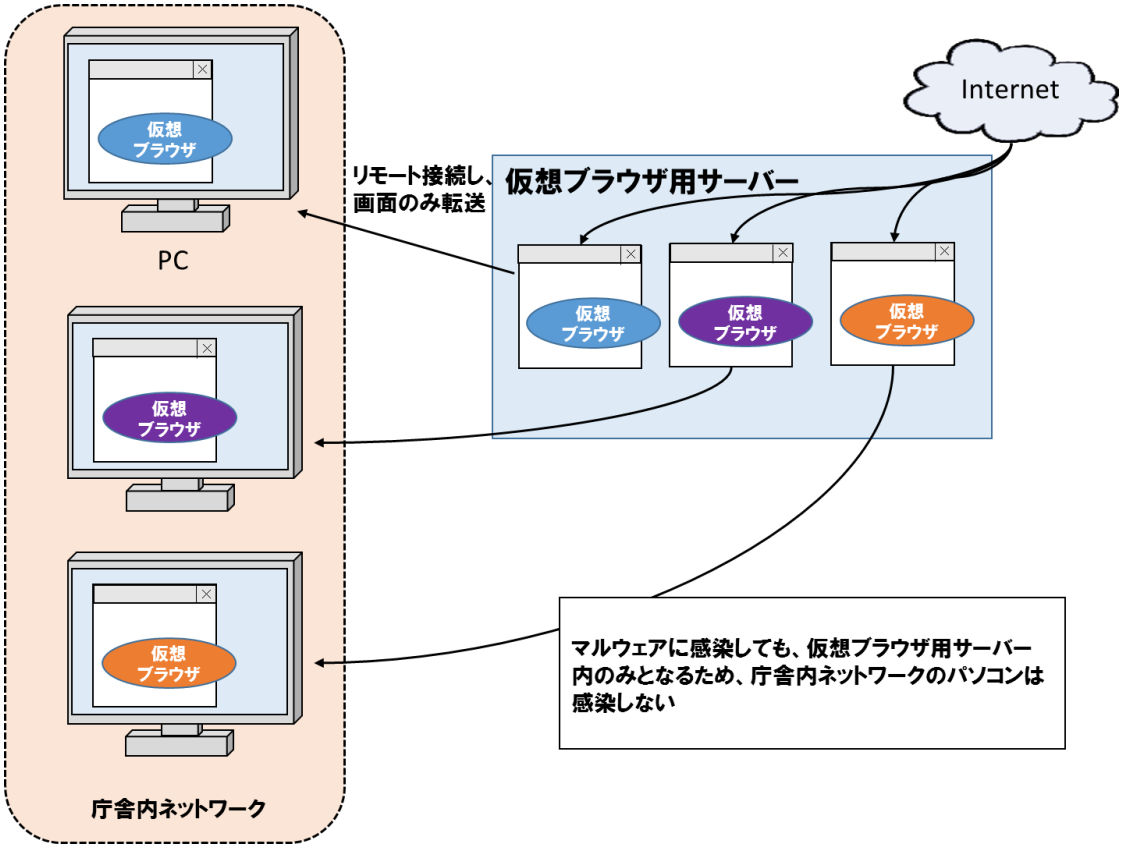


図 23　仮想ブラウザ概念図

しかしながら、上記のような対策を実施したとしても、セキュリティ脅威は残留する。考えられる脅威としては、暗号化されたファイルをメールで受信した場合である。ZIP ファイル等の圧縮ファイルに関しては、ウイルスを検出することができるが、パスワードにて暗号化されていた場合はウイルス検出が不可能となるため注意が必要である。また、ネットワークを介さないデータの受け渡しの際には、USB メモリの利用も考えられる。デバイスの紛失や盗難の可能性、許可されたデバイス以外（私物 USB メモリ等）を使用することによるウイルス感染の可能性が残るためである。インターネットを分離したといえ問題は残るため、対策については各地方公共団体等で検討する必要があると考えられる。

8.2 ISO/IEC27001（ISMS）体制の構築

(1) 地方自治体の ISO/IEC27001（ISMS）対応

地方自治体において、情報セキュリティ基準を設けていることは、多い。ISMS で求められている内容を現在の地方自治体で定めている情報セキュリティ基準が満たしているか確認し、もし満たしていない場合、新たな規程の追加、情報セキュリティ基準の改定を実施する必要がある。

(2) 地方公共団体における情報セキュリティポリシーに関するガイドライン

総務省より「地方公共団体における情報セキュリティポリシーに関するガイドライン」が公開されている。地方公共団体においても情報セキュリティポリシーを策定する必要がある。総務省が公開している「地方自治情報管理概要」によると以下の内容が実施率の低いものとして挙げられるため、強化していく必要がある。

① 主要な情報資産についてのセキュリティ対策実施手順の策定
② 主要な情報資産についての調査およびリスク分析
③ 緊急時対応訓練の実施
④ 緊急時対応計画を策定
⑤ 情報システムの運用等の外部委託先に対する指導・監査
⑥ 情報セキュリティポリシー等の遵守状況についての自己点検
⑦ 情報セキュリティについて内部監査
⑧ 情報セキュリティについて内部監査および外部監査

対策実施率（都道府県は 47、市区町村は 1741）		
対象項目	都道府県	市区町村
情報セキュリティ責任者や管理者等の任命	100.0%	95.6%
主要な情報資産についてのセキュリティ対策実施手順の策定の有無	97.9%	51.9%
情報セキュリティポリシーの策定	100.0%	97.9%
重要な情報資産について、無断での持ち出しやメール等による送付を禁止している	100.0%	96.3%
主要な情報資産について調査およびリスク分析を行っている	55.3%	33.0%
サーバー等の停電対策を実施している	100.0%	99.2%
サーバー室等の入退室管理を行っている	100.0%	98.3%
重要情報を含む紙媒体を適切に管理している	100.0%	93.9%
CD-R、USB メモリ等の持ち出しを制限している	97.9%	87.2%
情報セキュリティ研修を職員に対して実施している	100.0%	77.2%
緊急時対応訓練を実施している	46.8%	18.8%
不正プログラムへの対策ソフトウェアの導入や定義ファイルのアップデート	100.0%	100.0%
重要なデータのバックアップを取得	100.0%	99.5%
機器や外部記憶媒体を破棄する際、重要なデータを抹消	100.0%	97.9%
重要なデータへのアクセス制限を実施	100.0%	96.7%
許可されていないソフトウェアの導入を禁止	100.0%	94.1%
重要な情報システムのアクセスログを保存し、検査	95.7%	86.1%
重要なデータを暗号化し保存	63.8%	35.7%
委託事業者に対し、情報漏洩防止策を契約等により義務付けている	100.0%	99.1%

緊急時対応計画を策定	97.9%	56.6%
情報システムの運用等の外部委託先に対する指導・監査を実施している	61.7%	48.5%
情報セキュリティポリシー等の遵守状況について、自己点検を実施	83.0%	46.2%
情報セキュリティについて内部監査のみを実施	48.9%	25.2%
情報セキュリティについて内部監査および外部検査を実施	31.9%	6.2%
情報セキュリティについて外部監査のみを実施	0%	4.4%

「8 各消防機関における電子化の対応に必要なセキュリティ対策」参考文献[6] [7] [8] [9]

[6] 独立行政法人情報処理推進機構（IPA）「情報セキュリティ白書 2016」
[7] 独立行政法人情報処理推進機構（IPA）「大企業・中堅企業の情報システムのセキュリティ対策～脅威と対策～ 分冊６」
（http://www.ipa.go.jp/security/fy18/reports/contents/enterprise/html/611.html）
[8]独立行政法人情報処理推進機構（IPA）「情報セキュリティマネジメントと PDCA サイクル」
（http://www.ipa.go.jp/security/manager/protect/pdca/index.html）
[9] 一般財団法人日本情報経済社会推進協会（JIPDEC）「情報セキュリティマネジメントシステム（ISMS）とは」
（https://www.isms.jipdec.or.jp/isms/）

9. 電子署名およびタイムスタンプの方法等

本章では、電子署名およびタイムスタンプについて解説する。

9.1 電子署名の方法

電子署名とは、電磁的記録（電子文書）に付与する電子的な署名であり、書面における印影やサイン（署名）に相当する役割を果たす。以下の内容を確認するために用いる。

・署名者本人の意志が確認できること（本人が確かにその文書に署名をしたことが確認できること）

・同一性の確認（その文書が改ざんされていないこと）

電子署名を実現する仕組みは、国際的な標準技術である「公開鍵基盤」(PKI：Public Key Infrastructure）が利用されている。

(1) 認証局と電子証明書

公開鍵基盤を利用した「公開鍵暗号方式」は、「秘密鍵」(Private key）と「公開鍵」（Public key）の１組の鍵ペアによる暗号技術がベースとなっており、「電子署名」の生成に秘密鍵を、その検証に公開鍵を用いる。電子文書の本人性を確保するうえでの前提事項は以下の 2 点である。

① 署名者本人以外が秘密鍵を使用できないこと

② 公開鍵が署名者の所有する秘密鍵とペアとなるものであることが証明できること

ここで、公開鍵の所有者を保証することが重要となる。信頼できる第三者機関（Trusted Third Party）として公開鍵の所有者を保証する機関が認証局であり、認証局は利用者の本人確認を実施したうえで公開鍵の所有を証明する「公開鍵証明書」の発行を行い、秘密鍵と公開鍵の紐付けを保証する。公開鍵証明書には発行元の認証局の電子署名が付与され、一般的には「電子証明書」とも呼ばれる。

また、署名者は秘密鍵を本人以外が使用できないよう安全に管理する必要がある。秘密鍵の紛失や、電子署名を行う際に用いるパスワードの漏洩等により、万一、秘密鍵が本人性の証明に使用できなくなる状態（危殆化）となった場合、署名者は認証局に失効申請を行い、これを受けた認証局は無効となった証明書のシリアル番号を記載した失効情報に認証局の電子署名を付与して開示している。なお、失効情報は CRL（Certification Revocation List）や失効リストと呼ばれている。

(2) 電子署名の基本要件

電子署名のメカニズムは、電子ファイルに対し「ハッシュ関数」にて演算をし、得られた「ハッシュ値」を公開鍵暗号方式により署名者の秘密鍵を用いて暗号化したものが、「署名値」となる。

ハッシュ関数とは、文字や大きいサイズの電子ファイルであっても、一定の長さの文字を出力する関数のことである。

現在、最も多く利用されている SHA-2 の SHA256 というハッシュ関数に以下の文字を

入力した場合、ハッシュ値（64 文字）が出力される例を示す。

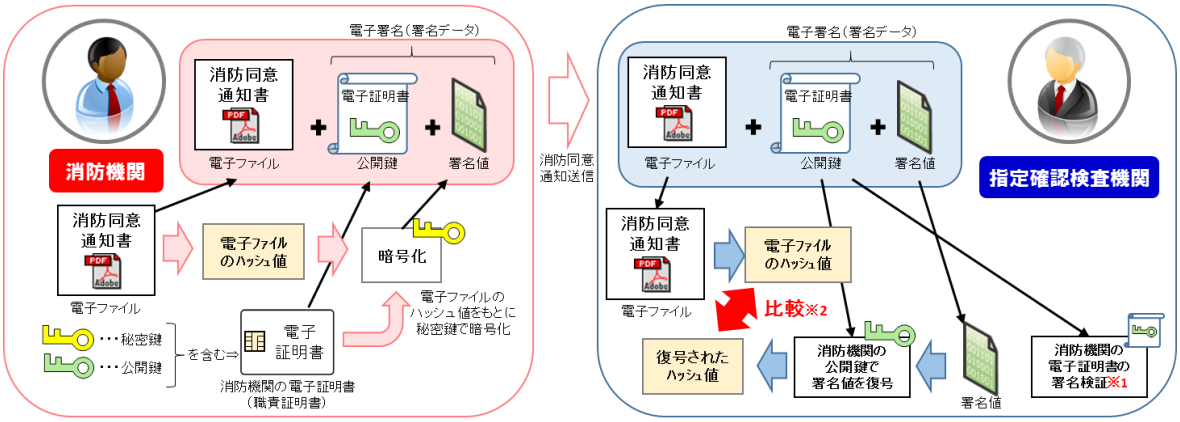
入力 →出力（ハッシュ値）

JAPAN→82a13f46dd02c304e228fd163259cf310817d2653f0fc209a75205b9a3d38568

JAPAn→a655f85c27151a3ad0e80ff962ecee8893248bb1708452b88d30a8bf968011d6

このように一字、異なっただけでまったく異なったハッシュ値が得られるため、ハッシュ値から電子ファイルを特定することも可能となる。ただし、ハッシュ値から元のファイルを復元することはできない。

電子署名の有効性を検証する際は、署名値を署名者の公開鍵で復号して得られたハッシュ値と、電子ファイルをハッシュ関数で演算をして得られるハッシュ値を比較することにより確認できる。双方が一致する場合は、公開鍵と秘密鍵の紐付け、および電子ファイルが改ざんされていないことが確認できるため、電子署名の本人性、非改ざん性を検証することが可能となる。



※1･･･正当な認証局が発行している本人の電子証明書であること、電子証明書の有効期限が切れていないこと、電子証明書が失効していないことが確認できる。
※2･･･ハッシュ値が一致すれば電子ファイルが改ざんされていないこと、電子ファイルの作成者と送信者が同一であることが確認できる。

図 24　署名と署名検証（RSA 署名の場合）

また、電子署名を実施する際には、その目的に応じ、以下の項目に留意した適切な利用が必要となる。

① 署名文書の利用用途に応じた適切な電子証明書を用いること

目的に応じて利用できる証明書の範囲が示されている場合はそれに従う必要がある。例えば、指定確認検査機関が電子ファイルに電子署名を行う場合は、電子署名法(電子署名及び認証業務に関する法律：法律第百二号)に基づき認定認証事業者の発行する電子証明書等を利用する必要がある。また、認証局が開示する「証明書ポリシー」(CP：Certificate Policy) に発行基準や用途が規定されている。

② 電子証明書の有効期間内に電子署名を行うこと

電子証明書の有効期間は発行時点から通常 5 年を超えない範囲で設定されている。電子署名を実施する時点において、この有効期間を超えていないことが必要である。

③　失効していない電子証明書を用いること

署名時点で失効していない電子証明書の秘密鍵を用いる必要がある。認証局では「失効情報」を公開している。そこで電子署名に用いた秘密鍵に対応する「電子証明書」の「シリアル番号」が「失効情報」に掲載されていないことを確認する。ただし、ほとんどの認証局では、有効期間満了前に失効した電子証明書のシリアル番号は、有効期間を超えた時点で、「失効情報」から削除しているため、電子署名の有効性検証は有効期間内に限られる。

④　署名文書の利用期間を通じて、電子署名の正当性が確認可能であること

法定保存期間等、署名文書の真正性の維持が必要な期間、電子署名の有効性が確認できる必要がある。署名の有効期間を超える場合は、タイムスタンプを併用した長期署名方式を採用する必要がある。

(3) 署名検証の基本要件

電子署名の検証は、署名者の本人性と署名された文書の非改ざん性を立証するための基本要素となる。前述の①～④を適切に確認し、また、署名文書が改ざんされていないことが確認できる必要がある。

・証明書検証（本人性の確認、前述①、②、③の確認）

署名に用いた証明書が正当な認証局から署名者本人に対して発行されたもので（①）、署名当時に有効期間が切れておらず（②）、失効していない有効な証明書（③）であることを確認。

・署名値の検証（非改ざん性の確認）

電子署名が署名者の公開鍵とペアになっている秘密鍵で行われており、また、署名文書が改ざんされていないことをハッシュ値の比較で確認。

・電子署名の有効性検証の継続

署名文書の利用期間を通じて、電子署名の有効性を確認。（前述④）

証明書検証においては、署名時点での証明書の有効性が問われる。ここで署名時刻を保証する客観的な時刻情報が必要となる。署名のみの場合、署名時刻は、署名者のコンピューターの時計に基づくため時刻の信頼性が高くなく、この役割を担うのが、タイムスタンプである。

9.2 タイムスタンプの方法

タイムスタンプとは、電子データが「ある日時に存在していたこと」および「その日時

以降に改ざんされていないこと」を証明する電子的な時刻証明書である。

電子署名の有効性を確認できる期間は電子証明書の有効期間内に限られ、最長 5 年が限度となる。しかし、タイムスタンプを併用した「長期署名フォーマット」を利用することで、より長期にわたり電子署名の有効性を継続して確認することが可能となる。

(1) 長期署名とは

電子証明書には有効期間があり、有効期間後には失効情報を取得できない問題があるが、電子署名とタイムスタンプを組み合わせることで、署名データだけでは無く、証明書や失効情報を1つにまとめて管理して証明書の有効期間後でも検証できる仕組みである。なお、タイムスタンプは、IETF RFC 3161（Time-Stamp Protocol）および ISO/IEC 18014 で標準化されている。

(2) 長期署名の手順

法定保存期間が定められた電子署名文書を保存する場合は、その文書が将来にわたり一定期間、署名検証が可能であることが必要である。その際、特に「証明書検証の継続性」に対して留意する必要があり、証明書検証では以下の 4 点を確認することになる。

① 署名文書の利用用途に応じた適切な証明書を用いること
② 署名当時に証明書の有効期間が切れていないこと
③ 失効していない証明書を用いて署名していたこと
④ 署名文書の利用期間を通じて上記①～③が確認可能であること

②および③を確認するためには、まず署名時刻が何時であったのか客観的に示せることが必要となるためタイムスタンプを利用する。また、署名時点での証明書の有効性を確認するためには、「失効情報」を保存する必要がある。

通常、認証局は証明書の有効期間を超えて失効情報の公開はしていない。失効情報には失効した証明書のシリアル番号が記載されているが、ほとんどの認証局では失効情報の肥大化を避けるため、失効した証明書の有効期間が過ぎるとそれらのシリアル番号は失効情報から消去している。従って、証明書の有効期間を超えて証明書の有効性を確認できないということである。

このような問題を解決するために、電子署名の有効性を証明書の有効期間や失効、さらには署名に用いた暗号アルゴリズムが脆弱化した後も維持できる署名規格として、「長期署名フォーマット」がある。その手順の概要は、以下となる。

① 署名対象データに電子署名を付与する
② 署名直後にタイムスタンプ（署名タイムスタンプ）を付与し、署名時刻を特定する
③ 証明書検証に必要となる以下の検証情報を収集格納する
  ・タイムスタンプ局の証明書
  ・署名者の証明書
  ・証明書パス上の認証局の証明書

・上記すべての認証局の失効情報

④　上記の署名対象文書や署名値、検証情報全体に対してタイムスタンプ（アーカイブタイムスタンプ）を付与する

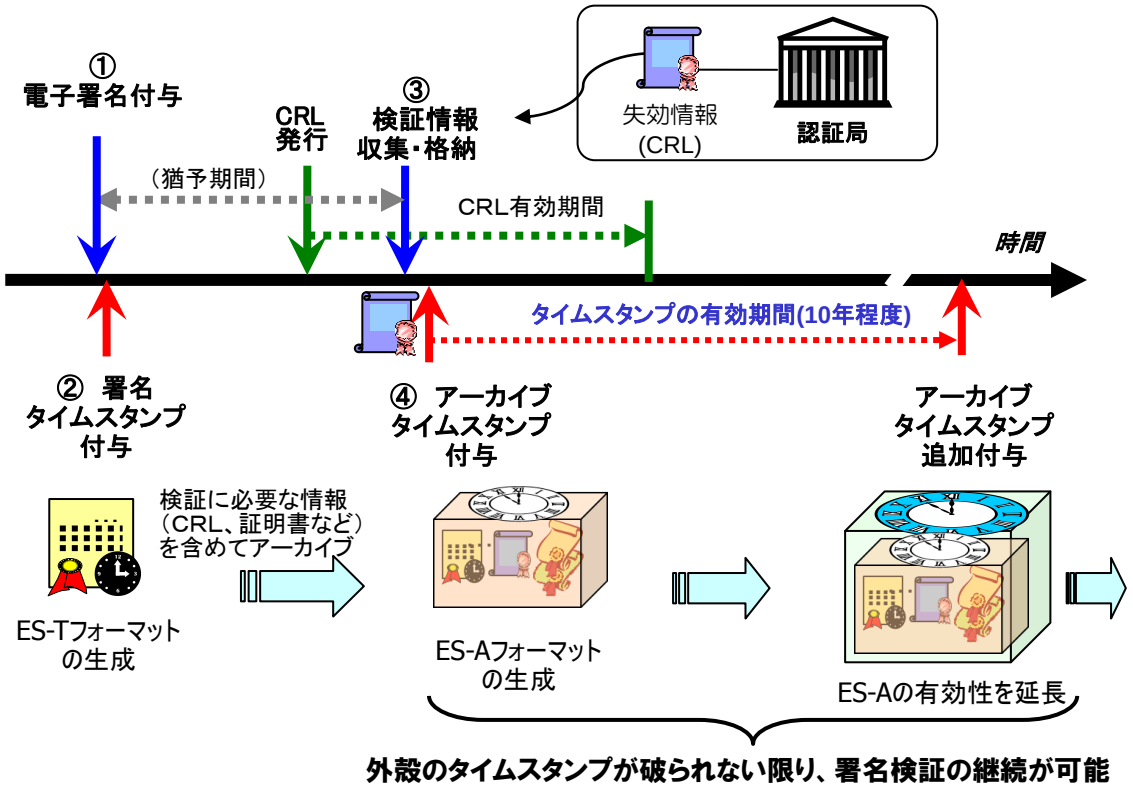


図 25　長期署名フォーマットについて

ここでの各タイムスタンプの役割は、

・署名タイムスタンプ

　電子署名時刻の信頼性を確保する

・アーカイブタイムスタンプ

　署名文書と失効情報をタイムスタンプの暗号アルゴリズムにより保護し、長期にわたり電子署名の真正性を継続する

ことにある。すなわち長期署名フォーマットとは、タイムスタンプにより署名時刻を特定して検証基準時刻とし、その時刻において、有効な証明書を用いて署名したことを後日検証可能とするものである。

なお、これらのタイムスタンプの有効期間は概ね 10 年間である。署名タイムスタンプ時刻で電子証明書が有効であったことが署名後 10 年間、確認および検証が可能となる。

従って、15 年間電子的に保存する必要がある場合、アーカイブタイムスタンプの有

効期間が切れる前にタイムスタンプを再付与することにより、電子署名された電子文書の署名検証を約 20 年間維持、継続することが可能となる。

(4) 署名データの形式と長期署名フォーマットの種類

署名対象データと署名データは一つのファイルに統合して作成可能だが、独立した二つのファイルとして作成可能となる。署名対象データと署名データの形式には、以下の三つに大別でき、利用形態に応じて選択する。

① 分離形式（Detached 型）

署名対象データとは独立して署名データを作成する形式である。署名対象データの種別は問わず、あらゆるファイル形式に対して署名データが作成できる。既存アプリで署名対象データを取り扱っている場合など、アプリ側への影響が少なく済む一方で、署名対象データと署名データを紐付けて管理する必要がある。

② 内包形式（Enveloping 型）

署名データの中に署名対象データを格納（内包）して作成する形式。署名対象ファイルと署名データが一つのファイルとなり扱いやすい一方、アプリ等で署名対象データを利用する場合、署名データから署名対象データを取り出す必要がある。

③ 包含形式（Enveloped 型）

署名データが署名対象データの中に含まれる（包含）形で作成する形式である。②と同様に一つのファイルで管理するため、扱いが容易である。一方で、署名対象データのファイル形式が電子署名をサポートしていることが必要となり、作成できるファイル形式に制限がある。（例：PDF や XML 等）

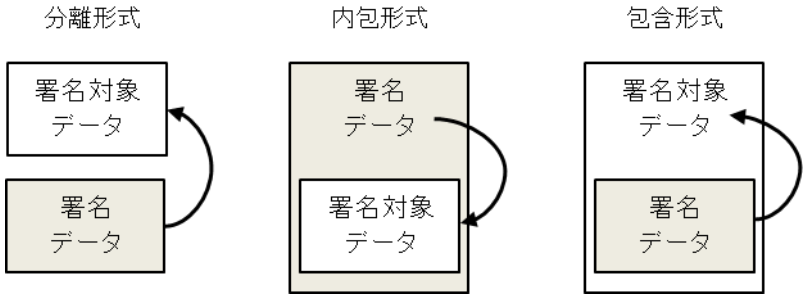


図 26　署名データの形式

また、長期署名フォーマットには、上記の署名形式や署名対象ファイル種別に応じて以下の種類がある。

・CAdES（CMS Advanced Electronic Signatures）

汎用的な署名ファイル形式である CMS（Cryptographic Message Syntax）をベース

とした長期署名フォーマット。署名対象データのファイル形式は限定されないため、広く様々なファイルへ電子署名を付与できる。分離形式、内包形式の電子署名に用いられる。

・XAdES（XML Advanced Electronic Signatures）

XML ファイルを対象とした電子署名形式である XML 署名をベースとする長期署名フォーマット。分離形式、内包形式、包含形式のすべてに用いることが可能。

・PAdES（PDF Advanced Electronic Signatures）

PDF ファイルの内部構造の中へ署名データを埋め込む包含形式の長期署名フォーマット。署名対象ファイルは PDF 形式に限定されるが、署名された PDF ファイルを単独で扱うことができ、Adobe Acrobat Reader 等でも検証できる利点がある。

一般的に、分離形式の電子署名はスキャナー保存等、ファイル形式を限定せずに社内で電子保存する際に向いており、PAdES のような包含形式の電子署名は、電子契約のように署名文書を社外に提出する必要がある場合に適していると言える。

9.3 消防長・消防署長向け電子証明書（職責証明書）の取得

消防長、消防署長の職責証明書を消防組織が属する市町村の登録分局にて発行の手続きを行うことにより、発行可能である。また、一部の市町村では、消防長に対し既に発行しているケースも存在する。現状の規程で職責が限定されている場合は、規程を改定する必要性がある。

(1) 消防に関する記載のある規程

以下は、規程の改定は必要ないと思われる登録分局の規程の例である。証明書発行対象として消防本部が含まれているため問題ないと思われる。

（登録分局の所掌事務）

登録分局は、総合行政ネットワーク運営主体からの委任に基づき、次の各号に定める業務を行うものとする。

(1) 市長部局、消防本部、市立病院、上下水道局、教育委員会事務局、選挙管理委員会事務局、審査委員事務局、農業委員会事務局および議会事務局の鍵情報等の発行、更新および失効に係る申請の受付および審査

(2) 消防に関する記載のない規程

以下は、ある電子証明書を発行する対象の職員が定められており、消防職員が含まれていないため、規程の改定の必要があると思われる登録分局の規程の例である。「消防本部の職員」を追記する必要がある。

（登録分局の役割）
　登録分局は、次に掲げる職員で使用する鍵情報等の発行申請、更新申請、失効申請に関する受付、審査および発行などの事務を遂行するものとする。
(1) 町長の事務部局の職員
(2) 議会の事務部局の職員
(3) 教育委員会の事務部局の職員
(4) 選挙管理委員会の事務部局の職員
(5) 監査委員の事務部局の職員
(6) 農業委員会の事務部局の職員
(7) 水道事業の職員

(3) 特別限定されていない規程
　以下は、規程の改定は必要ないと思われる登録分局に関する規程の例である。特に証明書発行の職責を限定していないので問題ないと思われる。

（登録分局の設置）
　市は､地方公共団体組織認証基盤の運営に関する基本綱領第8条第2項の規定により、地方公共団体組織認証基盤における証明者の利用および管理並びに基本綱領第7条第3項各号に定める委任業務を遂行するため、登録分局を設置する。
2　登録分局は、次に掲げる業務を行う。
(1) 証明書利用者からの証明書発行等申請における実在性および同一性の確認
(2) 登録局への証明書の発行、更新および失効申請
(3) 発行局が発行した証明書利用者への完了通知および証明書の配付
(4) 登録分局に関する総合行政ネットワーク運営主体（以下「LGWAN運営主体」という。）への届出
(5) 登録分局の運営に必要な書類の整理
(6) 登録分局の監査対応

参考文献[10]

[10]月刊IM 2016-10月号、11月号（公益社団法人日本文書情報マネジメント協会）

10. 電子化に伴う各消防機関で定められている関連規定

10.1文書保存規程、決裁規程、事務処理規程等の改正等の必要性

(1) 文書保存規定・公文書管理規定

公文書の作成、決裁、公印、登録、保存、廃棄について記載されているが、電磁的記録についての規定がなければ、改定が必要になると考えられる。

以下は、消防機関の公文書管理規程のサンプルで、電磁的記録について記載されている個所について抜粋している。規程内において、電磁的記録以外と電磁的記録についてその特性に応じて分類して規定する必要がある。

公文書管理規程のサンプル

（文書の取扱い）

文書（図画及び電磁的記録を含む。以下同じ。）は、条例、規則及びこの規程の定めるところにより、適正に管理しなければならない。

（電気通信回線を通じて到達した電磁的記録の収受等）

電気通信回線を通じて到達した電磁的記録の収受等に関し必要な事項は、別に定める。

（電磁的記録の管理）

電磁的記録を保存する主管課長は、電磁的記録の特性を考慮して、漏えい、滅失、き損、改ざん等が生じないよう必要な措置を講じ、適正に管理しなければならない。

2　電磁的記録を記録する媒体が持ち運び可能な場合は、主管課長が指定する施錠可能な場所で適正に管理しなければならない。

(2) 決裁規定・事務処理規定の変更箇所について

以下は、消防同意・事務処理規程のサンプルである。

消防同意・事務処理規程のサンプル

（同意等の通知）

建築主事等への同意等の通知は、同意等の区分に応じ、次の各号に定めるところにより行うものとする。

(1) 同意の場合

ア　申請書の計画及び現場の状況が防火の規定に適合しているものについては、申請書の消防関係同意欄（以下「同意欄」という。）に、同意する旨（別表）並びに申請書の審査に係る決裁完了年月日及び消防同意受付番号（以下「決裁日等」という。）を併記したうえ、公印規則に規定する建築同意用消防長印（以下「同意用印」という。）を押印すること

・・・略・・・

(2) 不同意の場合

ア　同意欄に、同意できない旨（別表）及び決裁日等を併記したうえ、同意用印を押印すること

イ　不同意通知書に、違反している法令の規定及び当該違反の内容並びに決裁日等を記載したうえ、同意用印を押印し、処理申込票等の裏面に貼付し、貼付箇所に同意用印を用いて割印すること

別表

1. 同意できない旨

年　月　日 第　　号
同 意 で き な い
○ ○ 市 消 防 長

2. 同意する旨

年　月　日 第　　号
同　意　す　る
○ ○ 市 消 防 長

同意の場合は、申請書の「消防関係同意欄」に「同意する旨」と「決裁完了年月日」、「消防同意受付番号」を併記し、「建築同意用消防長印」を押印すると規定されている。また、不同意の場合も同様、同意欄に「同意できない旨」および決裁日等を併記し、「同意用印」を押印するとしている。いずれも書面に追記や押印することが前提になっている。そのため、消防同意等を電子化する場合、申請書に対して、「同意する」旨と「決裁完了年月日」、「消防同意受付番号」を記載した電子文書を発行し、電子署名を行うとした、電子化対応の規程変更が必要になる。

11. 電子化に伴うシステムの取扱いの職員教育

本章では、指定確認検査機関等や消防機関の消防同意等の電子化に伴う職員教育について記述する。

11.1教育方法

電子化に伴う教育として、職員に対し業務に必要な知識および技能を習得させ、かつ情報セキュリティの意識を向上させることが必要である。特に、電子化にあたっては、消防職員に対し、OA 機器、情報セキュリティ対策、電子証明書の取り扱い、ICT 等の知識を効果的に得られ、効率的な教育方法にする必要がある。

効率的な方法としては、教育担当者が全職場に対して実施するのではなく、まずは教育担当者が各拠点のリーダーを集めて集中的に教育を行い、次にリーダーが各職場の職員に教育を行うことが考えられる。また、職員向けの教育資料に専門用語集を加えることにより職員に基礎知識を理解させることも有効である。なお、イントラネットを活用できる場合は教育資料とテスト項目をイントラネットに公開し、システム的に自動教育を実施することも考えられる。

11.2初回教育

初回教育は、消防同意等電子化システムが導入されることによる基礎知識の教育と運用開始のための教育が必要となる。基礎知識の教育はセキュリティ教育以外にも電子署名、タイムスタンプに関する基礎的教育などが考えられ、運用開始のための教育は、消防同意等電子化システムの操作方法、消防同意等電子化システムから取得したファイルを庁内システムへ移動し、既存の消防システムへ読み込ませる方法など実運用を考慮した実践的な教育となる。

11.3定期的な教育

教育は定期的に行うことで職員の電子化業務に関する認識の徹底、セキュリティ事故を起こさないような意識改革、自己啓発につながる。そのため、事務処理要領等に教育の方針、目的、対象、教育時期、教育計画および教育実施記録の策定等について明記したうえで、定期的に実施することが望ましい。なお、教育時期については、職員の新規任命時以外にも年次の定期教育、事務処理要領等の規程・マニュアルに変更があった場合にも実施するとよい。また、教育の体制を整える必要があるため、予め教育責任者、教育担当者を任命しておくとよい。

セキュリティ、電子署名、タイムスタンプの最新動向（例えば、SHA1 から SHA2 に移行するような情報）も確認のうえ、必要であれば教育に含める。

11.4教育資料

電子化にあたりシステム導入または改修が想定されるが、運用に際しては規程、マニュアルの作成または修正が必要となる。これらの規程、マニュアルを教育資料として利用す

ることで、職員の理解をより深めることができると考えられる。

事務処理要領には消防同意等を電子化した場合の運用手続きについて記載し、正常ケースだけでなく、紙と電子が混在する場合や補正、不同意の場合等、発生し得る異常ケースを考慮したうえで記載する必要がある。

その他、教育資料として規程、マニュアルに記載すると望ましいと考えられる項目を以下に列挙する。

教育資料（例）

・設備とネットワーク
・情報セキュリティ対策（定期的な Windows Update、ソフトウェアのセキュリティ更新プログラムの適用、ウイルス検知付きの USB メモリの使用、不正ログの調査等）
・個人情報の取り扱い
・アクセス権限・パスワードの付与・変更・削除に関する管理業務
・障害対応手順
・電子ファイルの持込・持出
・電子ファイルの保存期間と廃棄方法
・消防同意等電子化に関する概要
・電子署名・タイムスタンプの知識
・システムの操作方法
・システムの利用環境

12. 電子化に伴い必要となる特定行政庁および指定確認検査機関との調整等

12.1電子システムの採用と運用に関する調整

消防機関と指定確認検査機関等の間で消防同意等に利用する電子システムについて、消防機関と指定確認検査機関等双方でどの電子化手法を採用するか調整する必要がある。具体的には電子システム、ファイル転送サービスまたはS/MIMEメールなど採用するシステムに関する調整や、その運用に関する調整が必要となる。また、電子ファイルの添付方法、使用する電子証明書等、ならびに双方の費用負担等の調整が必要になると考えられる。

(1) 消防同意の申請を受け付ける際の電子ファイルの調整

電子化を行う際、消防機関が受け入れる電子ファイルは電子署名済み電子ファイル、確認申請書等の電子ファイルが想定される。そのファイルのフォーマットについて予め調整を行う必要があると思われる。

① 電子署名された文書（例：電子署名されたPDFファイル）

確認申請書、委任状、図面等のファイルについて押印が不要である点、電子署名が必要である点を調整する必要があると考えられる。

② 確認申請書等の記載事項データファイル（例：XMLファイル形式）

指定確認検査機関等から消防同意等が行われる際、確認申請書等の記載事項データファイルの送付の有無、送付する場合はその形式を調整する必要がある。形式については「5.10 既存のデータベースと連動させる場合および非連動の場合」を参照するものとする。記載事項データファイルを送付していただくことにより、消防機関が従来、紙の確認申請書等を見ながら手入力していた項目を自動入力することができる。これにより、入力にかかる時間の削減、誤入力が防止可能となり、消防同意等電子化の大きなメリットの一つとなり得る。

(2) 使用する電子証明書に関する調整

消防機関と指定確認検査機関等の間で、指定確認検査機関等が消防同意等を電子化するうえで使用する電子証明書を調整する必要がある。使用する電子証明書の詳細については「5.3指定確認検査機関の電子署名に用いる電子証明書」を参照するものとする。

12.2申請先の公開に関する調整（消防機関）

現状では、建築物のある住所や建築物の規模等によって申請先が消防本部または消防署等にて予め決められているため、申請先をホームページ等で公開し、変更があればタイムリーに更新することが望ましい。

13. 図面審査を電子端末で実施するための方法

本章では、先に電子申請の活用が進む指定確認検査機関において、電子申請の審査手法について例示する。

指定確認検査機関では平成 26 年 12 月に ICBA から発行された「建築確認検査電子申請等ガイドライン」に従って、4 号建築物等を中心に、構造計算適合性判定が不要な建築物（建築基準法第 6 条第 1 項第 2 号、第 3 号の建築物で構造計算適合性判定が不要な建築物を含む）など図面のサイズが小さく枚数も少ない申請を電子申請の対象として審査している。

《書面にて審査する方式》

電子申請された申請書および図書類を、書面に印刷して審査を行う。留意点として、印刷洩れや印刷物の取り違い等を防止するため、印刷物には識別番号とページ総数とページ番号を出力して、印刷後に書面と電子ファイルの整合確認を行う。

審査を実施した書面については、書面を保存する方式と、台帳に電子ファイル毎に審査した方式、審査日、審査者、補正内容を記録し書面を破棄する方式とがある。

《モニターにて審査する方式》

審査一回目のみ書面にて審査し、差し替え申請については差し替え該当電子ファイルをモニターで審査する方式と、一つの申請について一貫してモニターのみで審査を行う方式がある。

差し替え該当ファイルのみを審査する方式においては、差し替えされたファイルと変更の無いファイルが識別可能な仕組みを構築し、審査者は差し替えファイルのみを容易に識別して審査を行う。補正事項と差し替えファイルの内容が整合するかをモニターで判断する方法や新旧の PDF を差分比較するソフトウェア等を利用して、審査を行う。審査内容については、台帳に電子ファイル毎に審査した方式、審査日、審査者、補正内容を記録する。

モニターは 25 インチ以上であれば、A3 サイズを等倍に表示可能であるが、普及して廉価な 23 インチや 24 インチモニターを複数台使用する場合が多い。（参考費用：モニターは廉価製品の市場価格は 2 万円。差分比較ソフトウェアは 1 万円～。）

一つの申請を一貫してモニターで審査する方式においては、PDF ファイルの特性を利用し、審査時のメモや補正事項を PDF 提出ファイルのレイヤーに書き込み、審査の履歴を管理する指定確認検査機関も存在する。本方式の利点は、電子署名された原本とは別に、原本の複製にメモ等を入力し審査履歴として電子ファイルで保存できることである。

《タブレットで審査する方式》

現場検査での利用が多いが、タッチパネル対応のタブレット端末にて申請書や図書を確認して審査を行う。タブレットはパソコンモニターに比べて小型の製品が多いが、タッチパネルにて直感的に拡大や図書の切り替えができ、メモや補正事項について手書きで図書に書き込むことが可能である。

本方式を利用する場合、申請書一式が同じフォルダ内に格納される仕組みなどで小型の

タブレットでも容易に図書一式を閲覧できるような工夫と、メモ書きした PDF ファイルを審査のエビデンスとして保存する仕組みの構築が求められる。
（参考費用：タブレットを購入する場合、5 万円程度から。レンタルする場合は、通信費込みで月額 4 千円～。PDF に追記する機能については、Adobe Acrobat（有料）や Adobe Acrobat Reader（無料）等の注釈（Annotation）機能を搭載したソフトウェアを利用。）

14. 付録

14.1 消防同意依頼書サンプルフォーマット

指定確認検査機関から消防機関へ発行される。

第　　号
年　　月　　日

消防局長

指定確認検査機関会社名
代表取締役　　社長名

消防同意依頼書

建築基準法第六条の二第１項の規定により、下記の建築物の確認審査の申請を引き受けたので、消防法第七条、建築基準法第九十三条第１項の規定に基づき同意を依頼します。

記

1. 受付年月日：　　年　　月　　日
   受付番号：第　　号

2. 建　築　主：
   住　　所：

3. 建築場所：

4. 建築主からの申請方法：　■電子申請　　□電子申請以外
   ＊別添の確認申請書、図書・書類は、申請された電子文書の謄本であり、
   電子文書の記録内容と相違はありません。

5. 図書の返却方法：■電子　　□その他（　　）

6. 連　絡　先：指定確認検査機関会社名　　担当者名：
   電話番号：　　メールアドレス：
   識別番号：第　　号

14.2消防同意通知書サンプルフォーマット
消防機関から指定確認検査機関へ発行される。

第　　号
年　　月　　日

指定確認検査機関名称
代表者氏名　　様

消防長

消防同意通知書

年　　月　　日付送付のあった下記の　　申請書について、消防法（昭和二十三年七月二十四日法律第百八十六号）第七条の規定に基づき、同意します。

記

1. 建 築 場 所
   地 名 地 番 :
   住 居 表 示 :
2. 名　　称:
3. 申　請　者:
4. 用　　途:消防法施行令　別表第１　　項　（　　）
5. 規模・構造等:　　造　　地上　　階　地下　　階
   延べ　　㎡

【消防管理情報】
1. 受付年月日 :　　年　　月　　日
2. 同意年月日 :　　年　　月　　日
3. 同意番号等 :第　　号

【指定確認検査機関管理情報】
1. 受理年月日 :　　年　　月　　日
2. 指定確認検査機関受付番号:第　　号

14.3消防不同意通知書サンプルフォーマット
消防機関から指定確認検査機関へ発行される。

第　　号
年　　月　　日

指定確認検査機関名称
代表者氏名　　様

消防長

消防不同意通知書

年　　月　　日付送付のあった下記の確認申請書等については、次の事由により防火に関する法令に適合していないと認められるので通知します。

記

1. 建 築 場 所
   地名地番：
   住居表示：

2. 申　請　者：

3. 不同意事由：

【消防管理情報】
1. 受付年月日 ：　　年　　月　　日
2. 不同意年月日 ：　　年　　月　　日
3. 同意番号等 ：第　　号

【指定確認検査機関管理情報】
1. 受理年月日 ：　　年　　月　　日
2. 指定確認検査機関受付番号：第　　号

14.4 総務省消防庁　通知・通達

通知・通達を次頁以降に示す。

(1) 消防法等の一部を改正する法律等の運用について（通知）（平成 11 年 4 月 28 日　消防予第 92 号）

(2) 電子申請による建築確認に係る消防同意等事務の取扱について（通知）（平成 27 年 2 月 12 日　消防予第 53 号）

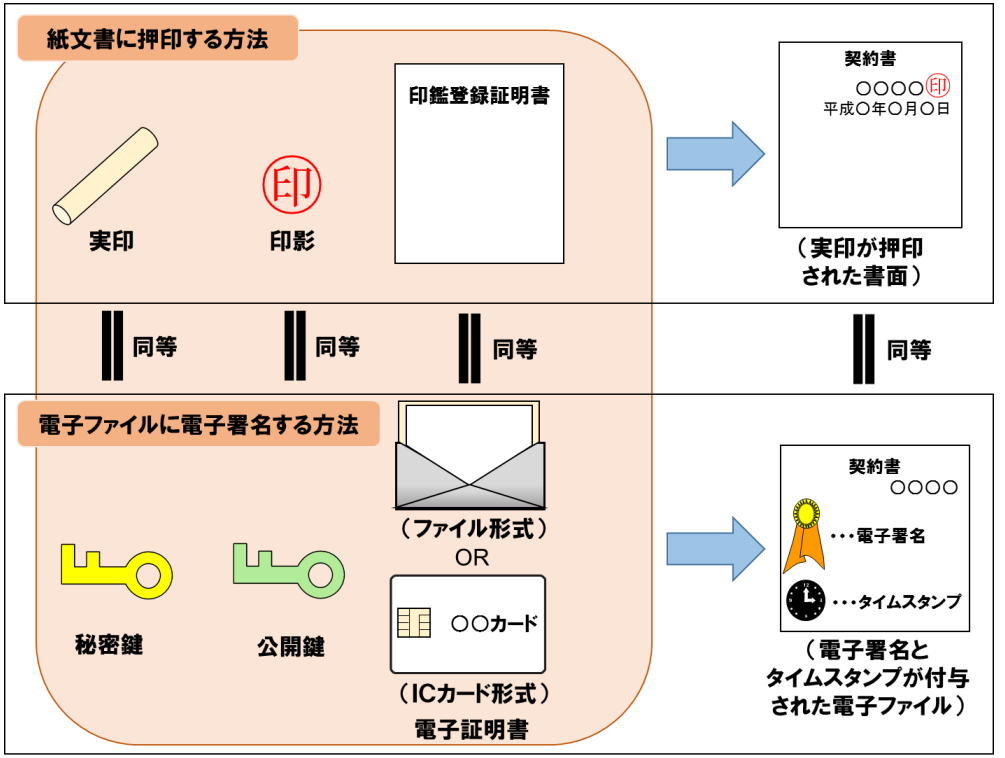
消防同意等の電子化に向けたシステム導入対応マニュアル
＜概要版＞

本書は、「消防同意等の電子化に向けたシステム導入対応マニュアル」の概要版です。
これまで書面で行われていた消防同意等事務を電子化する上ではいくつかの方法があり、電子化に関する基本事項や各方法別にメリット、デメリット、コスト、必要な作業や準備について概要を記載しました。各消防機関において、「電子申請による建築確認に係る消防同意等事務の取扱について（通知）」（平成 27 年 2 月 12 日　消防予第 53 号）を具現化し、電子化するためにはどの手法を選択すればよいか、実態に応じて選択できるよう検討の糸口として参考にしてください。
なお、詳しくはマニュアル本編をご参照ください。

平成 29 年 ９月
総務省消防庁予防課

◆電子署名に関する用語の解説

用語	説明
電子証明書	利用者の公開鍵が本人に帰属していることを証明するために認証局が電子的に発行する電子ファイル、公開鍵証明書とも呼ばれる。公開鍵証明書は公開鍵そのものを含み認証局の電子署名が付されている。なお、電子証明書ファイルには公開鍵とペアになる秘密鍵を含めることもできる。有効期間は発行時点から通常 5 年を超えない範囲で設定されている。
公開鍵	公開鍵暗号方式で使用される一対の鍵の一つで、一般に公開される鍵。公開鍵は他人に知られても悪用される恐れはない。秘密鍵で暗号化されたデータは一対の公開鍵でのみ復号可能となり、電子署名の検証に用いる。
秘密鍵	公開鍵暗号方式で使用される一対の鍵の一つで、利用者本人のみが保有し一般に公開されない鍵。秘密鍵が他人に知られると悪用される恐れがあるため、厳重に管理する必要がある。本人のみが所持するものなので電子署名に用いられる。
電子署名	電子ファイルに対して署名者の秘密鍵を用いて行う電子的な署名のことで小さいサイズの電子署名データとして作成される。PDF ファイルの場合電子署名データをファイル内に格納することもできる。署名済みの電子ファイルは署名者が誰であるか、また改ざんの有無が公開鍵を用いて確認でき、これを署名検証と言う。電子ファイルに電子署名をしたものと書面に押印したものは同等として扱うことができる。
タイムスタンプ	ある時刻に、ある電子ファイルが存在していたことを証明する「存在証明」と、その内容が改ざんされていないことを証明する「完全性証明」を実現する仕組みのこと。有効期間は発行時点から約 10 年で設定されている。日本データ通信協会によるタイムスタンプ認定制度がある。 また、利用方法により電子署名時刻の信頼性を確保する「署名タイムスタンプ」と長期にわたり電子署名の真正性を継続する「アーカイブタイムスタンプ」と区別して呼ばれることもある。
ハッシュ値	電子ファイル等を一定の長さの文字に出力するハッシュ関数を用いて出力された文字列のことをいう。元の電子ファイルを少しでも変更するとハッシュ値はまったく違うものになる。ハッシュ値は電子署名の付与・検証の際に用いられる。

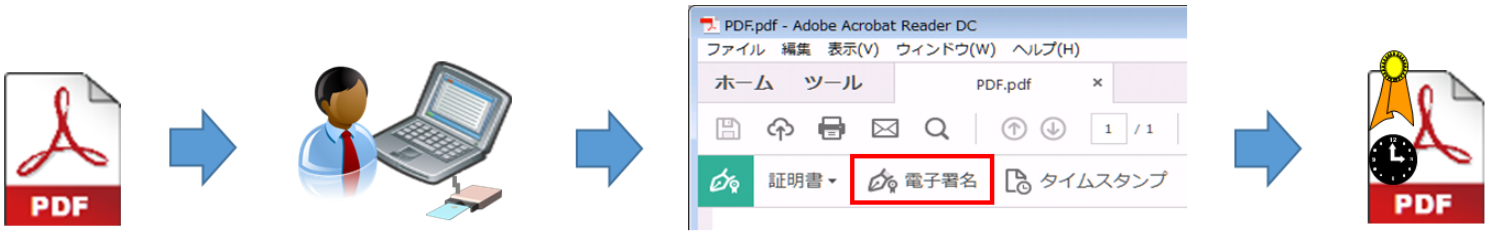


◆電子署名について

電子署名を行う場合、まず電子証明書を準備する必要がある。消防長等が利用する電子証明書は、地方公共団体の登録分局に申請すれば入手することができ、職責証明書と呼ばれ、IC カード形式で発行される。IC カードには公開鍵と秘密鍵が含まれる。秘密鍵は公印と同様の効力を有するため、IC カードは公印同様の取扱いが必要とされる。IC カードの利用にはパソコンに基本ソフトをインストールし、パソコンと接続された IC カードリーダーに IC カードを挿入すれば利用することができる。

また、IC カードと Adobe Acrobat 等の署名プログラムを用いて PDF ファイルに電子署名を行う操作をすると、自動的に PDF ファイルのハッシュ値が計算され、職責証明書に含まれる秘密鍵で暗号化され「署名値」となる。「署名値」は、「職責証明書に含まれる公開鍵」とともに 電子署名（署名データ）として、PDF ファイルに埋め込まれる。

◆電子署名・タイムスタンプの付与方法（PDF 閲覧・編集ソフトを利用する場合）



電子署名したい PDFファイルを 用意する。

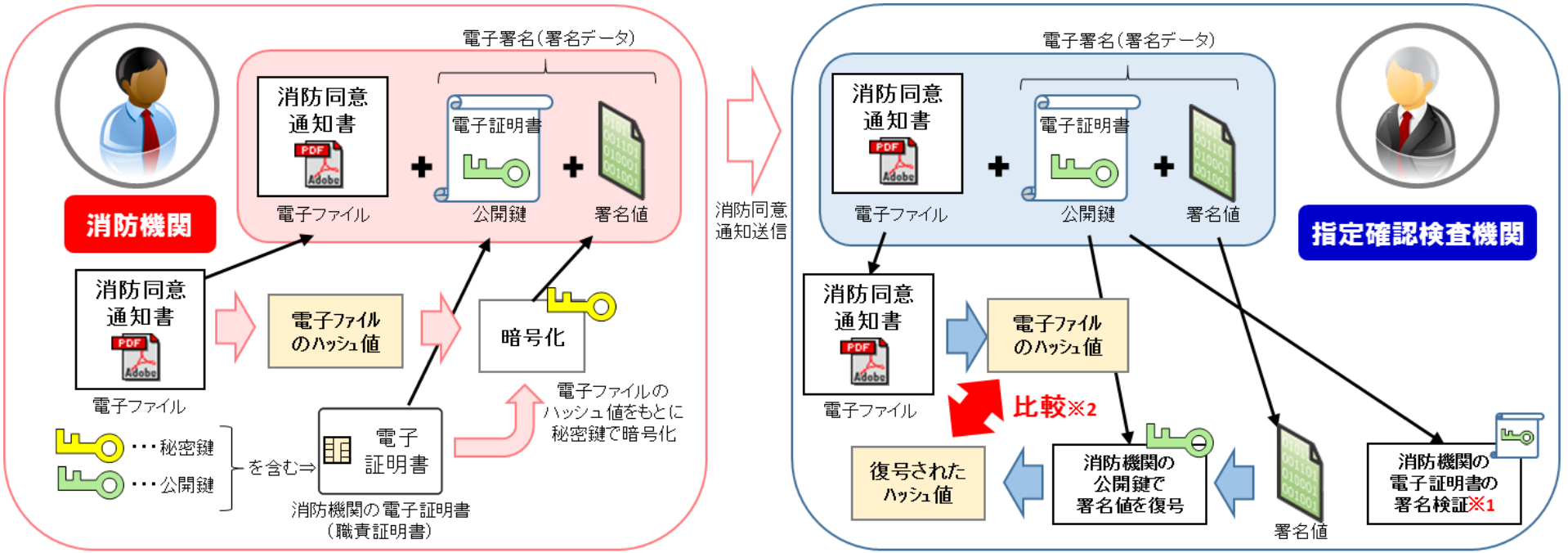
職責証明書ICカードをICカードリーダーにセットする。

PDF閲覧・編集ソフトにてPDFファイルを開き、「電子署名」ボタンをクリックし、証明書の種類、署名内容等を設定すると電子署名およびタイムスタンプが付与される。もし、タイムスタンプの設定がされていない場合は電子署名のみになる。

電子署名・タイムスタンプの付与が 完了する。

※ 事前にICカードリーダーのドライバーインストール、電子署名・タイムスタンプに対応したPDF閲覧・編集ソフトのインストール・設定等が必要となる。ソフトウェアの種類により名称、操作方法は異なる。

◆電子署名の付与および検証方法（概念図）



※1・・・正当な認証局が発行している本人の電子証明書であること、電子証明書の有効期限が切れていないこと、電子証明書が失効していないことが確認できる。
※2・・・ハッシュ値が一致すれば電子ファイルが改ざんされていないこと、電子ファイルの作成者と送信者が同一であることが確認できる。

◆消防同意を電子化するための手法

【初期コストを抑えたい場合】

No.	方法	メリット	デメリット	コスト
1	**指定確認検査機関が既に建築確認検査電子申請で利用している電子ファイル転送システム**を消防機関が利用する方法 【運営主体】 指定確認検査機関	・既存システム利用のため、電子化が容易 ・費用負担は指定確認検査機関で、消防機関のコスト負担がない。 ・サイズの大きい電子データ転送が可能。 ・ファイル転送システムに署名・タイムスタンプ機能がある場合、消防機関で新たなタイムスタンプ契約が不要。	・ファイル転送システムを利用していない指定確認検査機関がある。 ・指定確認検査機関ごとにアクセス先やID/パスワードを使い分ける必要があり、また操作性が異なる可能性がある。	消防機関初期コスト：なし。 消防機関ランニングコスト：電子ファイル転送システムにタイムスタンプ契約が付いている場合は不要。契約が付いていない場合は、タイムスタンプ料金が必要。
2	**消防機関が民間の電子ファイル転送システム**を利用する方法 【運営主体】 消防機関	・サービスによっては初期コスト・ランニングコストが抑えられる。 ・複数の確認検査機関から送付される消防同意依頼等を一つのシステムからすべて確認でき、作業が煩雑にならない。 ・サイズの大きい電子データ転送が可能。 ・ファイル転送システムに署名・タイムスタンプ機能がある場合、消防機関で新たなタイムスタンプ契約が不要。	・指定確認検査機関等に利用してもらうよう協力体制が必要。 ・単純なファイル転送サービスの場合、タイムスタンプをシステム上で付与できないため、PDF閲覧・編集ソフトウェアで付与する必要がある。 ・無料ファイル転送サービスの利用は、ウイルス検知、災害対策等のセキュリティ面での保証がないため推奨しない。	消防機関初期コスト：電子ファイル転送システム利用の初期費用。（数十万円程度） 消防機関ランニングコスト：1消防機関あたり月間基本料金は数万円程度。 ファイル送受信料は1ファイルにつき100円程度。 電子ファイル転送システムにタイムスタンプ契約が付いている場合は不要。契約が付いていない場合は、タイムスタンプ料金が必要。
3	署名暗号化メール(S/MIME方式)を利用する方法 【運営主体】なし S/MIME（エスマイム）方式とは受信者が送信者の本人性やメールの内容が改ざんされていないことを確認できる仕組み。	・ファイル転送システムを利用しないため電子化しやすい。 ・初期コストを安価に抑えられる。	・サイズの大きい電子データの場合、メールサーバーにて送受信が制限されるため、分割してメール送信をする必要がある。 ・メールの電子署名検証が作業負担となる可能性がある。 ・署名暗号化メール(S/MIME方式)に対応したメールソフトウェア（Microsoft Outlook、Mozilla Thunderbird、Mac Mail等）およびその利用が消防機関で許可または対応されていない場合、利用できない。	消防機関初期コスト：なし。 消防機関ランニングコスト：タイムスタンプ料金。 地方公共団体の登録分局で発行されるメール用証明書を利用する場合は、費用なし。 民間の認証局で発行されるメール用証明書の場合は、年間基本料金は数万円程度。

【地方公共団体の既存システム活用の場合】

No.	方法	メリット	デメリット	コスト
1	既存の**電子申請システム**を改修して利用する方法 【運営主体】 地方公共団体	・地方公共団体が管理をするため、消防機関や指定確認検査機関等の初期コストがない。 ・既存システムのためセキュリティ対策を新たに講じる必要がない。	・地方公共団体の協力体制が必要。 ・既存システムの仕組みによっては、改修費が高額になる恐れがある。	地方公共団体初期コスト：数百万円～数千万円。（既存システムの仕組み、改修業者の対応などによりコストは大きく変わる可能性がある） 消防機関ランニングコスト：既存の電子申請システムにタイムスタンプ契約が付いている場合は不要。契約が付いていない場合は、タイムスタンプ料金が必要。

【特定行政庁との場合】

No.	方法	メリット	デメリット	コスト
1	外部と切り離されている**イントラネットを利用**してファイル転送を行う方法 【運営主体】 地方公共団体	・特定行政庁と消防機関にて共有しているイントラネット内の既存サーバーを利用するため、費用がかからず、セキュリティ上も問題がない。 ・既存の機能を利用できれば、初期コストがかからない場合がある。	・指定確認検査機関が利用できない。 ・サイズの大きい電子データに既存サーバーが対応できるか検討が必要。 ・状況確認のため電子データの受取状況、進捗状況を確認できる運用を別途検討する必要がある。	地方公共団体初期コスト：0円～数百万円。改修しない場合と既存機能を改修する場合があるため。 消防機関ランニングコスト：ファイル転送システムにタイムスタンプ契約が付いている場合は不要。契約が付いていない場合は、タイムスタンプ料金が必要。

【消防機関の共通した作業・費用負担】

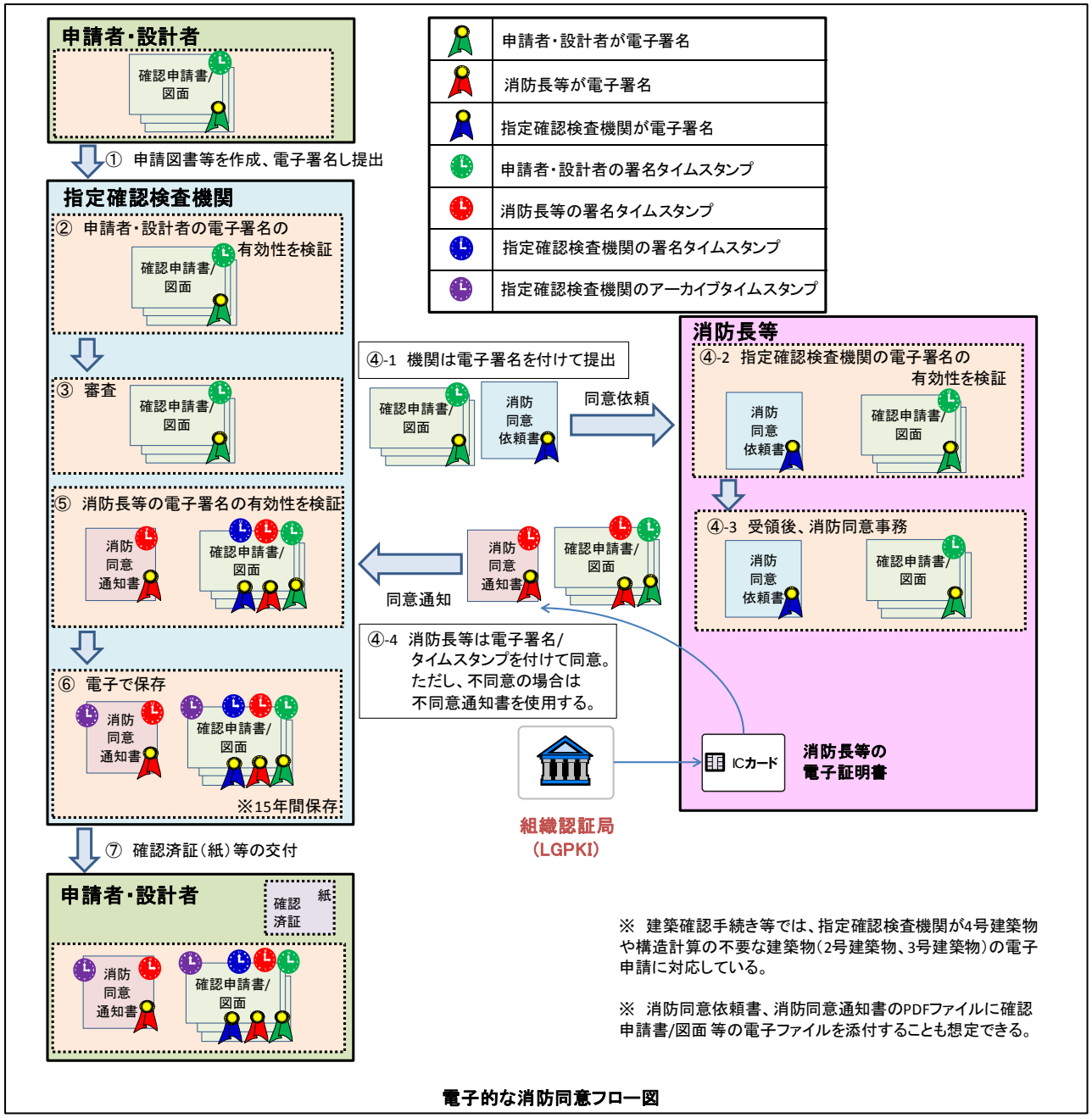
【必要項目】＜合計　約16万円＞
◎インターネット接続できるパソコン。（10万円以下）
◎大型ディスプレイ・解像度フルHD 1920x1080 約24インチ程度。（2万円/台）
◎PDF閲覧・編集ソフトウェア。（LGPKIの電子署名およびPAdES-LTV対応・1万円～4万円。ただし、既に持っている場合は不要。）
◎地方公共団体の登録分局に申請し職責証明書、ICカードリーダーを取得。（無料）

【必要に応じて準備する項目】
・消防同意事務（図面確認等）を行うパソコン。（10万円以下）
　パソコンがディスプレイ2台構成に対応であれば、2台構成がより望ましい。
・タイムスタンプ契約を行う場合は、月間料金約1万円。（月間1,000スタンプ以内の場合）

【対応すると業務効率に貢献できる項目】
・台帳入力の手間を省く場合、確認申請書または建築計画概要書のファイルを読み込む改造費用。
（利用している台帳システム開発会社に確認が必要）
・消防機関内で消防同意決裁を行うための電子決裁システム導入。

【確認項目】
消防同意・事務処理規程等にて消防同意等の電子化を行えるか確認。出来ない場合は、規程の改定が必要。

◆電子的な消防同意事務の流れ



※ 建築確認手続き等では、指定確認検査機関が4号建築物や構造計算の不要な建築物（2号建築物、3号建築物）の電子申請に対応している。

※ 消防同意依頼書、消防同意通知書のPDFファイルに確認申請書/図面 等の電子ファイルを添付することも想定できる。

電子的な消防同意フロー図

消防同等電子化のフロー説明

申請者はこれまで書面に押印して確認申請書等を提出していたが、電子の場合は「電子署名」を付与して電子データを送信する。指定確認検査機関は、持参や郵送していた消防同意依頼に係わる電子文書に「電子署名」を付与し消防機関に即日送信が可能となる。消防機関が消防同意する際も「電子署名・タイムスタンプ」を付与した電子データを送信することにより、従来の事務作業にかかっていた郵送時間の削減ができ、指定確認検査機関の確認済証の発行期間短縮につながる可能性が高く、住民サービスの向上につながる。指定確認検査機関は、消防同意済みの電子データに「アーカイブタイムスタンプ」を付与し、法定保存期間である 15 年間保存する。また、確認申請書等の副本については、電子データで申請者に返送する。

消防同意の電子化メリット

消防同意依頼に係わる文書の保存が電子でできるため、やり取りにかかる時間の短縮、保存スペースが不要となる。

消防同意事務において、紙運用の場合、消防職員が確認申請書や建築計画概要書等を見ながら台帳システムへ手入力する作業が発生していたが、消防同意の電子化が進み、確認申請書や建築計画概要書が電子データで受領可能となれば、台帳システムへ自動入力することができる。これにより、これまで入力にかかっていた時間の削減、誤入力防止につながる。

紙運用の場合、一部の消防機関では、消防同意依頼に係わる書類一式を消防本部と消防署などの間で運搬をしていたが、消防同意の電子化が進めば運搬業務が不要となり、消防同意にかかる日数の削減、作業効率の改善につながる可能性が高い。