「原本性保証システムガイドライン」

財団法人ニューメディア開発協会

平成１３年３月

＜目次＞

１． ガイドラインの目的

原本性保証システムガイドライン（以下、本ガイドラインと略）は、電子文書が紙文書と同等に扱われるようにするための方策を、情報システムとして実現するためにどのようにすべきかを提示するものである。

本ガイドラインの対象は、従来、紙文書によって組織内で重要な文書の「原本」を保管していた組織（行政機関等）が、電子文書によってその原本を保管しようとする組織・機関、それらにシステムを提供する情報システムベンダーである。これら組織が電子文書の原本性を確保するために、安心して情報システムを導入するために何を選択すればよいかという点をガイドするものである。

電子文書の原本性保証のポイントは、最終的に電子文書が証拠能力としてその効力を持ちうるのかということである。しかしながら裁判官の心証により証拠能力が推定されるため、本ガイドラインやチェックリストに則りシステムを導入し運用を行ったとしても電子文書の原本性が保証されるわけではない。情報システムが原本性を保証することは最終的に困難である。

しかしながら、裁判官の心証を良くする方向への努力として様々な原本性保証対策を講じておくことが必要であり、現在の時点で考えうる情報システムの技術が数多く実装され、強固な対策が講じられていること、それを責任を持って説明できること（説明責任）は、極めて重要である。

一般的なコンピュータシステムを導入し運用した場合と比較したときに、本ガイドラインに則った原本性保証システムを導入し運用することにより、電子文書の証拠能力はより増強されるようになると考えられる。

２． ガイドラインの構成

本ガイドラインは、原本性保証のポイントを挙げ、それをシステムによって実現するためにどのような要件が求められるのかということを提示している。現在様々なタイプの原本性保証に係わるシステムがあり、それぞれ独自の機能を搭載している。これらの中で「原本性保証電子保存システム」を中心に原本性保証システムに求められる要件と技術例を挙げている。

また原本性保証電子保存システムのチェックリストを後半に掲載している。このチェックリストに則り製品を導入し、かつシステム運用を行うことによって、電子文書に対してある一定レベルまで原本性を確保しているということができるものと考える。

３． 原本性保証とは何か

原本性保証システムに求められる要件の元となっている、行政機関と民間事業者それぞれに対して提示された通達・報告書類を見てみる。

３．１ 共通課題研究会報告書

行政機関の電子文書を保存する際の指針として出された、総務庁（現総務省）の共通課題研究会の「インターネットによる行政手続のために」（最終報告書）では、対象文書を「行政機関の職員が職務上作成し、又は取得した電子文書であって、組織として保存・管理すべきもの」とし、それら電子文書の原本性確保要件として、「完全性」・「機密性」・「見読性」を十分に確保することであり、「紙文書と比較した場合の電子文書の問題点」として以下の点を挙げている。

＜完全性＞
・改ざん、修正、すり替え等が容易で痕跡も残らない、システム障害、記録媒体の経年劣化等により内容の消失、変化のおそれがあるなど、完全性の確保に問題があること

＜機密性＞
・盗難、漏えい、盗み見が大量かつ秘密裏に行われやすいなど、機密性の確保に問題があること

＜見読性＞
・ディスプレイに表示又はプリントアウトするなどの措置を講じない限り、可視性・可読性に欠けており、見読性の確保に問題があること

３．２ 高度情報通信社会推進本部制度見直し作業部会報告書

民間事業者の電子文書を保存する際の指針として出された、高度情報通信社会推進本部の制度見直し作業部会の報告書では、電子文書の原本性保証とは、「真正性」・「見読性」・「保存性」を十分に確保することとある。

＜真正性＞
・データの故意又は過失による虚偽入力、書換え、消去及び混同を防止すること

＜見読性＞
・データの内容を必要に応じ肉眼で見読可能な状態に容易にできること

＜保存性＞
・保存期間内において復元可能な状態でデータを保存すること

３．３ 原本性保証のポイント

前出の２つの報告書では、行政機関と民間事業者のそれぞれの保存文書という違いはあるものの、原本性保証に求められる要件という点では、おおよそ一致しているものであると考えられる。

原本性確保に対する脅威は、大まかに以下のように分類できると考えられる。

(A)改ざん
(B)システム障害による電子文書等の内容の消失・変化
(C)記録媒体の経年劣化
(D)電子文書等の盗難・漏えい・盗み見
(E)見読性の欠如
(F)電子文書保存・管理の責任やその権限の不明確化
(G)コンピュータウィルスによる破壊・消去
(H)原本と謄本・抄本の混同による、唯一性の欠如

一方で、情報セキュリティを確保することとは、OECD 情報システムセキュリティガイドラインによると、以下のように規定している。

＜可用性＞
・データ、情報、情報システムが、必要な（要求された）手順で適時にアクセスでき、利用できること

＜機密性＞
・データと情報が、正当と認められた人間、対象物、手順に対してのみ、正当と認められた時刻に、正当と認められた方法で開示されること

＜保全性＞
・データと情報が、正確かつ安全であること。また、その正確性と完全性が維持されること

原本性保証とは、情報資産（電子文書）が「あるべき姿」を保つように、かつその価値が減少しないように様々な防御を行う点において、情報セキュリティ対策の考え方と似通っているものであると考えられる。

既に原本性保証システムを導入しようとする組織において、様々な情報システム・IT 製品が導入され業務を遂行しており、それらを守るセキュリティ関連製品も導入され、かつ情報セキュリティポリシーを策定するなどして、何らかのセキュリティ対策が施されてい

るであろう。ここに新たに原本性保証システムを導入するにあたり、情報セキュリティ全般と同じように様々な対策を講じるため、その対策の全てを原本性保証システムによって補おうとすることは、コストの面から見ると得策ではない。

原本性保証とは、電子文書の証拠能力を紙文書と同様に持たせることであるとすると、民間事業者・行政機関いずれの電子文書についても裁判において証拠能力を問われた際に一番問題となるであろう、電子文書の「改ざん」が如何にしたら発生しないか、また発生したことが分かり、元の状態に戻せるかということが最大のポイントになると考えられる。

３．４ 電子文書の証拠能力を増強するための概念の整理

ある電子文書が証拠能力を持つかどうか確認する際に、その確認を著しく阻害するのが「改ざん」である。その改ざんを行う動機を持つ者は、「当事者」と「第三者」の大きく２者存在する。当事者とは電子文書の保存を行う組織に関係するいわゆる内部者で、文書の作成・保存・保管管理を行う側の立場に属し、文書作成者や文書管理者である。これらに属さないのは第三者である。第三者が行う改ざんは愉快犯的なものも多く含まれるが、文書の改ざんにより利益があるのは当事者の方である可能性が高い。よく言われるように世の中の犯罪行為は内部者が行うケースの方が、その者にとってより高い利益を生んでいることが多い。

原本性保証では、当事者・第三者の双方が行う改ざんという行為に対して対策が講じられるべきものであるが、第三者の行う改ざんの対策よりも、当事者の行う改ざんに対してより焦点が当てられるべきである。しかし証拠能力を増強するものであるため、当事者達が自らの不正行為の有無を主張する場合に、自らがその主張をするよりも、当事者以外の人間もしくはシステムによって主張される方が、より裁判官の心証を強くするであろうことが推測される。

改ざんの対策で重要な点は、当事者が行った改ざんの有無を、当事者以外の人間もしくはシステムによって説明が補完されることであり、これにより電子文書の証拠能力が増強されると考えられる。

４． 原本性保証システムの考え方

４．１ 改ざんの対策方法

原本性を保証するために最大のポイントとなる電子文書の「改ざん」について、その対策方法を分類すると、以下のようになる。

・改ざんの抑止（改ざんをできなくすること）
・改ざんの予防（改ざんが起こりにくいようにすること）
・改ざんの検出（改ざんされたことが分かること）
・改ざんの回復（改ざんされた前の状態に戻せるようにしておくこと）

上記の４つの分類を、証拠能力という観点で考えると、「改ざんされたのか、されていないのか」ということが争点であり、改ざんされていないことが証明できるのであれば証拠能力を持っていることの説明が容易となる。逆説的に言うならば、「改ざんされた事が必ず検出できるのであれば、改ざんされていないことを証明できる」と考えられる。よって、「改ざんの検出」という対策は、原本性保証システムにおいて欠くことのできないものである。

しかし、改ざんの対策として「改ざんの検出」ができるだけでなく、改ざんの「抑止」・「予防」・「回復」についても対策を講じないことには、原本性保証システムとして不足であろう。

本ガイドラインでは、改ざんの検出を「改ざん検出機能」、改ざんの抑止・予防・回復を「改ざん防止機能」と呼ぶこととする。

４．２ 技術で必須の機能

改ざん検出機能は、原本性保証システムに必ず搭載されてなくてはならない機能の１つであると考える。

しかし、改ざん防止機能については、全ての要件が技術的に対策が講じられていることは必要なく、いずれかの技術もしくは複数の技術を組み合わせて実現されていることが望ましい。また原本性保証システムの技術によって対策が講じられない場合は、適切なシステム運用が行われていることが必要となる。

５． 原本性を確保する機能

４章で見たように、「改ざん検出機能」と「改ざん防止機能」の２つが原本性保証というシステムに求められる重要な２機能である。本章では２つの機能と、その他原本性確保のために必要となる機能を見ていく。

※本ガイドラインでは、「改ざん検出機能」と「改ざん防止機能」を兼ね備えたシステムの一例として、「原本性保証電子保存機能チェックリスト」を付属している。

５．１ 改ざん検出機能

（１） 改ざん検出機能（必須）

＜要件＞
電子文書データ（ファイル）の変化を検出できるようにすること

＜具体的な技術例＞
○電子文書データ（原本データ）の保存等処理のログを記録する。ログには保存等処理の操作者、時刻関連情報、などを含む。
○原本データと各種履歴については、改ざん検出用データ（認証子）を付与し、改ざんの有無を判別する。改ざん検出用データは、ハッシュ関数を利用してハッシュ値を生成し、原本データとハッシュ値を一体として保存する。ハッシュ値は一つの原本データから、唯一の値しか取ることができないため原本データを一意に特定でき、元の原本データが少しでも変化すると値が大きく変化するという特性から、改ざんの有無の判別が可能となる。
○ログや認証子は、原本データの保存年限に見合った期間に渡って保存できるよう保存期間設定をする。

○改ざん検出用データを信頼できる第三者機関に預け、改ざんが起こったことを後に第三者機関が検出する。当事者以外の第三者が改ざん検出を行うことにより、より信頼性の高い非改ざんの証明を行う。
○改ざん検出用データを暗号化し管理する。また電子署名・PKI の仕組みを利用し、暗号化した改ざん検出用データを信頼できる第三者に預けることで、より信頼性の高い非改ざんの証明を行う。

（２） 時点の特定機能（必須）

＜要件＞
電子文書データ（ファイル）の変更した時点もしくは時刻を特定できるようにすること

＜具体的な技術例＞
○電子文書データ（原本データ）の保存等の時点を確定するために、システム内部にシステムタイマーを保有し、原本データや履歴情報・認証子などに時刻を付与する。システムタイマーの時刻は適宜調整を行う。
○原本データ時刻情報の変更内容を記録し、複数の時刻情報間での前後関係を保証する

○信頼できる第三者機関等が発行する標準時刻を用いて、原本データや履歴情報・認証子などにその時刻を付与する。

５．２ 改ざん防止機能

改ざんを広く解釈するならば、電子文書がその状態を保てないことである。保てなくなる脅威としては、改ざんという不正なイメージのものだけでなく、過失による書換えや、システムダウン、媒体の劣化などがあるが、これらが発生しても結果的に電子文書の状態は元の正しい状態ではなくなる。

これらのようなことを防ぐために様々な方策が考えられるが、これに対応するように用途に合わせて様々な機能が存在する。これらは、全てが技術的機能として対策が講じられていることは必要なく、いずれかの技術もしくは複数の技術を組み合わせて実現されていることが望ましい。また、原本性保証システムの技術によって対策が講じられない場合は、適切なシステム運用が行われていることが必要となる。

(A)改ざん
(B)システム障害による電子文書等の内容の消失・変化
(C)記録媒体の経年劣化
(D)電子文書等の盗難・漏えい・盗み見
(E)見読性の欠如
(F)電子文書保存・管理の責任やその権限の不明確化
(G)コンピュータウィルスによる破壊・消去

以上の A～G を脅威と捉え、原本性保証システムで特に対策が講じられた方がよいと考えられるものを挙げる。

＜特に原本性保証システムの機能で対策を講じることが望ましい脅威＞
・特に内部者による組織内部等の LAN ネットワークを経由した、もしくは直接原本性保証システムの操作による不正アクセスによる改ざんなど
・操作や保存の権限のない原本データに対する不正な利用者のアクセス
・正しい利用者としての権限を持つ者が原本データの消去・改変・すり替えなどを行う
・システム管理者が誤って操作ミス等を行い、原本データが変化・消去する

＜原本性保証システムの周辺環境で対策を講じてもよいと考えられる脅威＞
・外部ネットワーク等から侵入するコンピュータウィルスによる破壊・消去
・電子文書等の盗難・漏洩・盗み見
・見読性の欠如
・電源断等システム障害による電子文書等の内容の消失・変化

（1） 書換・消去不可機能

＜要件＞
保存期間内の電子文書データ（原本データ）は、あらゆるアクセス者が上書き・消去などできないようになっていること。

＜具体的な技術例＞
－確定操作－
○保存すべき原本データを確定するために、確定操作機能を設ける。
○確定操作を行った原本データは、変更・上書き・削除ができないようにし、データを変更する際は追記とする。
○版管理・バージョン管理機能として、改変された文書を新しい版とすることで、文書の改変履歴や古い版の参照を可能とする。

－追記ディスク－
○原本データを書き込むディスクは、追記・書換えの場合、追記・書換え前の情報はそのまま残し、新たな情報として記録する。
○原本データを書き込むディスクは、一度しか書き込みができない。

－ハードウェア等の機能－

○特定のプロトコルやネットワークコマンド、特定のインターフェースのみ接続できるようにする。

○原本性保証システムの筐体は耐タンパー性を持ち、かつ鍵がかかるようにするなどし、物理的な不正アクセスを防ぐ。

○原本性保証システムの筐体を開ける、ディスクを挿入する、各種インターフェースに装置を接続する、などの操作の記録が全て残るようにする。

（２） アクセス者の識別・認証

＜要件＞

利用者の権限による原本データへのアクセスを制御するために、原本性保証システムの操作以前にアクセス者の識別・認証を行うこと

＜具体的な技術例＞

○アクセス者を ID・パスワードで識別・認証する。

○アクセス者の情報を IC カード等に格納し、IC カードへのアクセス者登録管理を行うと共に、システムの利用毎に識別・認証する。

○アクセス者を公開鍵基盤技術を用いた電子認証によって識別・認証する。

○IC カードと共に、ID・パスワード、電子認証を用いることにより、アクセス者の識別・認証の信頼性をより増すことができる。

○上記の各種識別・認証機能を、原本性保証システムを利用するクライアントシステムでアカウントを発行し、クライアントシステム側で識別・認証を行う。その場合、認証した情報が原本性保証システムに確実に引き継がれ利用できるようにする。

（３） アクセス制御

＜要件＞

電子文書データ（原本データ）の保存・参照・更新などの操作について、利用権限を持つアクセス者のみに限定できるようにすること。

＜具体的な技術例＞

○全てのアクセス者は、原本データの参照しかできない。特定の権限を与えられた管理者

等のみが保存・更新・削除などの操作を行うことができるようにする。
○原本データへのアクセス制御は、読み込み／書き込み、読み込みのみ、の２つの権限設定によって管理する。
○原本性保証システムへのアクセスのログインやログアウトの記録を残るようにする。

（４） バックアップ

＜要件＞
電子文書データ（原本データ）が元の状態に戻せるようにバックアップを取得する

＜具体的な技術例＞
○原本性保証システム内部の原本データや履歴データは、自動的にミラーリングし、かつ外部記憶媒体へのバックアップを作成する。
○原本データを可搬型媒体（CD-R など）へバックアップし、媒体識別番号を付与して管理する。

（５） ネットワーク保護

＜要件＞
通信経路上での不正な改ざん・盗み見・盗難などが起こらないよう、通信時もしくは保存時に暗号化処理を行う

＜具体的な技術例＞
○電子文書データに暗号化処理を行う機能を搭載する。

（６） 複製制御

＜要件＞
原本とその複製（謄本）が区別できるようにする

＜具体的な技術例＞
○原本とその複製を区別するために、それぞれのステータスを管理する。

５．３　今後技術的な解決を考慮すべき課題

・電子文書の保存期間が長期に渡る場合、文書フォーマットや媒体フォーマットを、数年・数十年先であっても、常に利用できるようにしておかなくてはならないこと
・電子文書の保存期間が長期に渡る場合、証明技術に利用するための暗号化技術等を長期に渡って証明に利用できるよう、適切・安全に利用できるようにすること

６． 原本性保証システム利用にあたっての運用条件

原本性保証システムを利用するにあたり、本システムも情報システムの一つであることを認識し、以下のような対策を講じておく必要があることに注意して頂きたい。

＜情報システムセキュリティの運用として対策が講じられるべき脅威＞

・組織外部の者により、物理的に侵入する、もしくはネットワークを経由した論理的に侵入して行う、改ざん、盗難、システム障害などあらゆる不正行為
・外部の事業者等により、メンテナンス作業時等において、対象システムに物理的にアクセスして行う、改ざん、盗難、などあらゆる不正行為
・電子文書の保存・管理の責任やその責任所在が不明確であるために発生する脅威
・地震・火事などの災害や電源断によって引き起こされるシステム障害により、電子文書等の内容の消失・変化が発生すること

（１） 組織と管理者

システム管理者が定められていること。システム管理者は、文書管理者及び文書管理担当者とは別の職員とし、システム管理者と文書管理者の責任と権限の範囲を明確に定めておくこと。
システム管理者、システム利用者、その他第三者を区分し、各々の利用権限や守るべきセキュリティのルールなどを定めていること
システム管理者は定期的に交代し、長期間に渡って同一人物が管理を行わないようになっていること。
電子文書管理に関して、情報セキュリティの責任、管理実施手順などを明確にしておくこと。
情報システムの事故が発生した場合には、システム管理者と文書管理者が対処にあたること。

（２） 情報資産の管理

セキュリティを確保すべき保護対象資産について、原本となる電子文書のファイル、および格納するハードウェアや過搬型保存媒体などを明確に管理すること
保護対象資産である電子文書のファイル、およびそれらを格納するハードウェアや過搬型媒体などを不正に持ち出されないよう適切に管理すること

（3） 利用者

利用者に対して、システムを利用する上で必要なセキュリティに関する知識を周知していること。知識とは離席時や帰宅時は情報を放置していないこと、ハードウェアソフトウェア、電子データの各情報資産の移動は一定の手順に従って行われていること。
利用者に対して、電子文書管理に関する知識や技術の周知、修得を進めていること。
利用者には、システムを利用するための ID・パスワードなどの登録情報を安易に他人に教えたり、人目に触れる場所に書き留めたりしないこと、などの周知が徹底されていること

（4） 物理的及び環境的セキュリティ

システムを設置する建物は、鉄筋コンクリートのビルディングであり、耐震・耐火設備、消化設備など、災害対策の設備を設けていること
システムを設置する建物の入り口には、警備員が常駐しているか、もしくは警備システムなどが設置され、組織に無関係の人間が容易に建物に侵入できないようになっていること
原本性保証に係わるシステムを設置する部屋は、入退室管理が行えるよう施錠が出来、情報システムを設置するための専用の部屋になっていること
原本性保証に係わるシステムを設置する部屋は、部屋内で使用するシステムに電源断による障害が発生しないよう、無停電電源装置等の対策が施されていること
情報システムを設置するための専用の部屋の鍵は、システム管理者もしくは文書管理者によって適切に管理されていること
電子文書の保存等の操作を行うための組織内 LAN に接続されている端末を設置する事務室等については、無人の時や夜間及び休日は施錠できるようになっていること
電子文書の保管場所については、原本性保証に係わるシステムのハードウェア内部、もしくは過搬型媒体の場合は情報システム専用の部屋に設置される保管庫に保管していること。なお保管庫についても施錠管理できる方が望ましい。

（５） ネットワーク環境及びアクセス管理

インターネットや霞ヶ関 WAN などの組織外部のネットワークと組織内のネットワークを接続する場合には、ファイアウォールを設置して不正なアクセスを防止していること
組織内 LAN 等の利用者端末が原本性保証に係わるシステムとネットワークを介して接続されている場合には、利用者は端末上で ID・パスワードなどによって認証され、それらの履歴が記録・管理されていること
システム管理者によって、利用者を認証するための ID・パスワードの発行・管理が適切に行われ、電子文書に対するアクセス権限の範囲等が明確にされていること

（６） システムの開発及びメンテナンスなど

システムの障害等が発生しないよう、メンテナンス作業を行っていること
電子文書の記録媒体の変換等については、ソフトやハードの技術発展、記録媒体そのものの耐用年数等に対応するため、同一又は他の種別の記録媒体への変換、データ・ファイル形式の変更、定期的なバックアップなどの措置を適切に講ずること。また記録媒体の変換等を行ったことは管理簿等に記入して管理しておくこと。
1 日に 1 回程度の定期的な電子文書のバックアップを行っていること。
ウイルス検出ソフトウエアをシステムに装備する、もしくは電子文書の保存等の操作を行う前には必ずウィルスチェックを行うなどにより、コンピュータウィルスを検出でき、ウィルスが含まれる電子文書が保存されないようになっていること
外部事業者等がシステムのメンテナンス作業等を行う場合は、システム管理者の管理監督の元に作業を行い、作業後にはその内容等を報告させること。

７．　原本性保証システム導入例①：行政機関の文書管理における利用環境の想定

行政機関においては、「バーチャル・エージェンシーの検討結果を踏まえた今後の取組について」（平成 11 年 12 月 28 日高度情報通信社会推進本部決定）の「iii　行政事務のペーパーレス化（電子化）」の中で行政機関の内部事務のうち一定の事務について計画期間内に電子化を実現することとしており、また、「申請・届出等手続の電子化推進のための基本的枠組み」（平成１２年３月３１日行政情報システム各省庁連絡会議了承）においても、申請・届出等手続のオンライン化を強力に推進するとされている。これらの状況を鑑みても、今後文書の電子化という流れの中で必然的に文書の電子的保存が求められるという状況にある。

紙と電子を同等に扱っていくために電子文書の原本性を確保し、行政機関においても説明責任を果たせるようにすべきであるが、原本性を確保することは技術もしくは運用による両面の対策によって適切に行われることが求められる。

原本性保証システムを導入する場合の一例として、以下のような行政機関の利用環境を想定した。

７．１　　行政機関のシステム環境における原本性保証

ある省庁では機密度が高く厳重に保存されるべき紙文書を次のような環境と運用方法によって保管・管理している。

・保存すべき文書は、全て官房・文書管理課に集められ、承認などのしかるべき処理の後、保存される。
・保存すべき文書は、職員しか場所を知り得ない省庁内の倉庫で保管されている。倉庫の入り口のドアは１つであり、施錠可能で、窓など他の入り口はない。鍵は文書管理課等の管理職相当の管理者が保管している。
・省庁の入居するビルには玄関および入り口に守衛が立ち、身分証等の提示によりビルに入ることが可能となる。

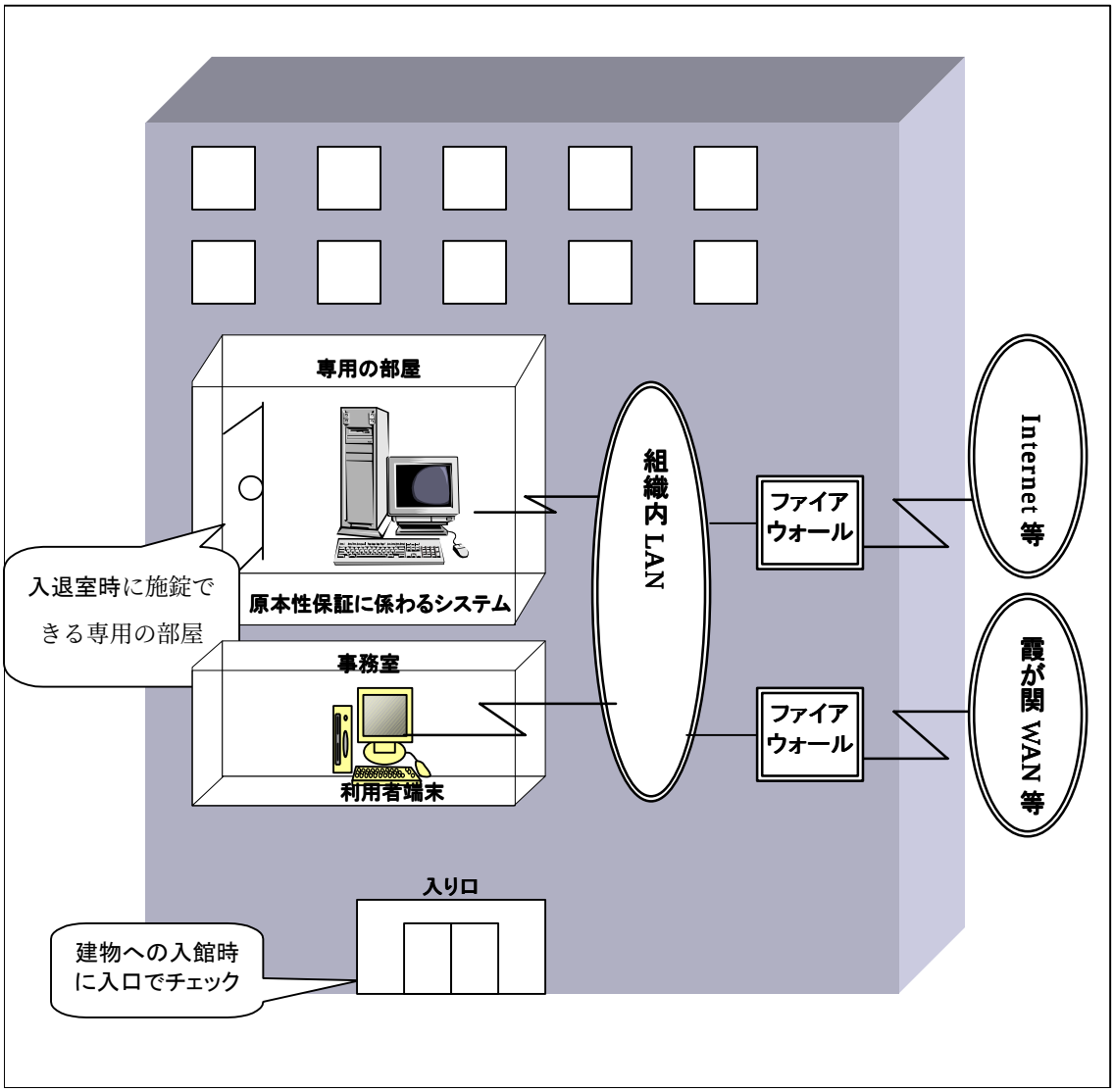

図１　行政機関のシステム利用環境想定図

以上のようなシステム利用環境において、原本性保証システムの要件に則り、また原本性保証電子保存機能チェックリストに照らし合わせてシステムを導入し、かつ情報セキュリティ対策を行うことにより、電子文書の原本性は一定のレベルで確保されたものになると考えられる。

８． 原本性保証システム導入例②：汎用電子申請システム

汎用電子申請システムにおける原本保存の場所やタイミングの捉え方を紹介する。汎用電子申請システムは、他の行政機関において電子申請および電子申請に係わる文書の原本性保証について検討する上で参考になるものだと考えられる。

８．１　個別手続のオンライン化（汎用電子申請システム）

個別手続のオンライン化に関し、経済産業省では 2003 年度までに所管法令等に係わる 2001 件の申請・届出等手続のオンライン化を実現するという計画である。

個別手続のオンライン化に係わるシステムは専用と汎用の２種類に分かれ、専用システムは特許電子出願や貿易管理システムなど他の行政事務と比較して規模が大きい特殊性を持ち、汎用システムは、専用システムが取り扱う範囲外の共通的な行政事務における申請システムである。

このうち汎用システムは、「汎用電子申請システム」として平成 12 年度中に開発されることになっている。また、汎用電子申請システムでは「原本保存」をシステムによって行われることが仕様に盛り込まれている。

８．２　電子申請における原本文書の保存の場所とタイミング

汎用電子申請システムでは、申請者からの申請・届出文書を行政側のシステムで処理を行った後、申請者に許認可等文書として送信する。（図２参照）

＜申請書受信から許認可等文書送信までの流れ＞

受信→原本保存→受付→認証・検証→手数料→審査支援→電子決裁→発行→原本保存→送信

原本保存は、申請者からの受信直後と、申請者への送信直前の２つの場面で行われている。受信直後は一時保存という仮の状態であり、その後に認証や審査・決裁などの処理を経た後、確定された文書として許認可等文書の形になり送信直前に原本として保存される。

また原本として保存された許認可等文書は、文書内容の修正なども考えられるため、上記の各処理中に参照できるようにしておく必要もあろう。

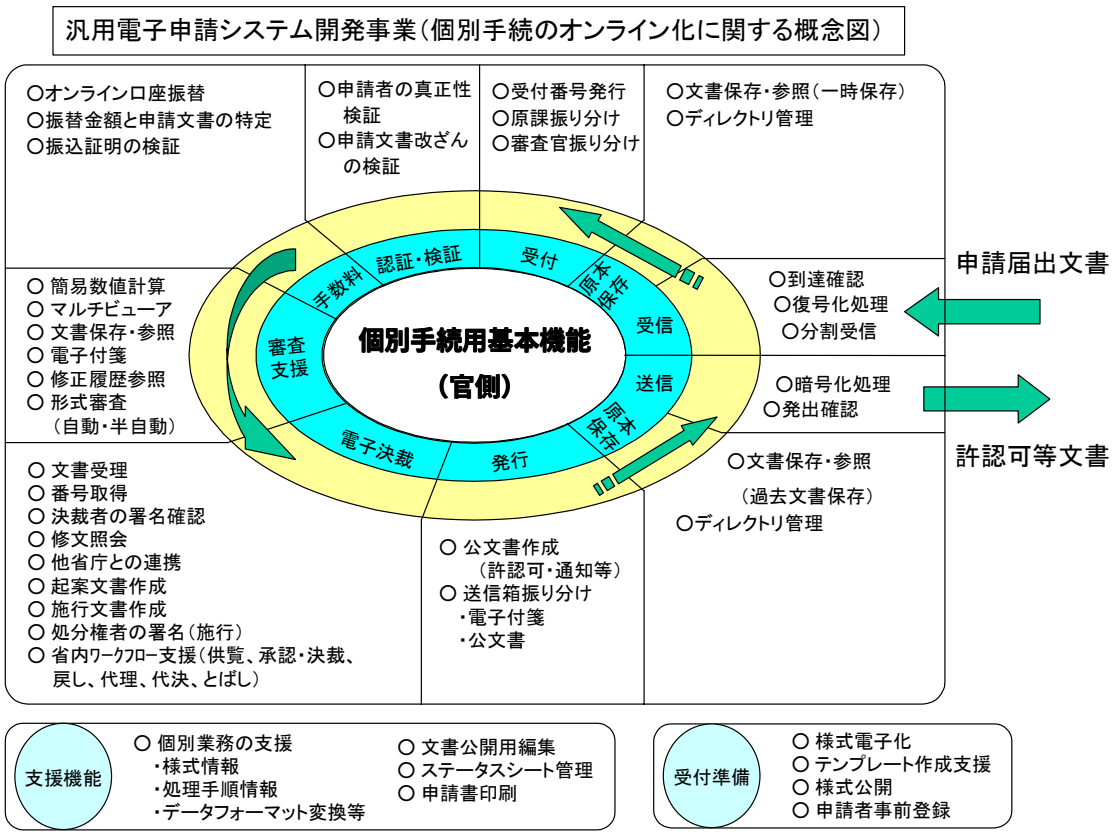

図２　汎用電子申請システム開発事業（個別手続のオンライン化に関する概念図）※

※経済産業省・商務情報政策局情報政策課「個別手続のオンライン化について」より抜粋