平成１２年度情報システム共通基盤整備のための連携推進事業
（オンライン制度的課題への対応）

原本性保証に係る評価・認定制度に関する調査研究

報告書

平成１３年３月

財団法人ニューメディア開発協会

はじめに

わが国は、インターネットや携帯電話を中心としたモバイル機器の普及等により、確実にデジタルネットワーク社会への道を歩んでいる。このことは文書等の形もアナログからデジタルのものへと変化していくことを意味しているが、現時点では、従来の紙媒体による文書と電子化された文書が混在している状況にあると言えよう。

電子文書の持つ特性として、改ざんが容易であり、かつ痕跡が残りにくいこと、記録媒体等の劣化による情報の消失等が起きやすいこと等が挙げられ、電子文書を安全に利用するためにこれらの脅威を克服しなくてはならない。しかしながら、文書を電子的に作成もしくは取得した場合であっても、最終的に原本として保存・管理される文書は、依然として紙媒体によるものが多いと考えられる。これらの状況を踏まえ、今後は、紙文書と同等の安全性を保つ、すなわち原本性を確保しながら、電子文書の利点である効率性や検索性の高さを失わないよう、電子文書を活用していかなくてはならない。

行政機関においては、国民への行政サービスの向上を目的に、行政事務の効率化・高度化等の行政情報化が推進されている。また、電子文書に対応した文書管理方策の整備が進められているところである。先ごろ公開された「e-Japan 重点計画(案)」においても、全府省におけるペーパーレス化（電子化）に対応した文書管理規程等の整備がうたわれている。

本報告書は、(財)ニューメディア開発協会が平成 12 年度情報システム共通基盤整備のための連携推進事業（オンライン制度的課題への対応）の一環として、経済産業省から委託を受け、当協会に設置した「原本性保証に係る評価・認定制度研究会」の検討結果をまとめたものである。本研究会では、紙文書と同等に電子文書を扱うようにするための１つの解決策である原本性保証製品について、これら製品の普及等を目的とした検討を行った。また、関連するユーザー、ベンダー双方の現状を踏まえ、原本性保証製品やシステムの評価認定制度の導入についても検討を行っている。

本研究会の開催にあたっては、東京工業大学像情報工学研究施設の喜多紘一教授を主査とし、関連団体や製品開発ベンダー、行政機関担当者の各方面からご協力を頂いた。これらの成果が、今後の原本性保証および関連製品の普及・促進の一助となれば幸いである。

平成 13 年 3 月

財団法人ニューメディア開発協会

― 目 次 ―

― 付 録 ―

原本性保証に係わる評価･認定制度研究会委員名簿

＜委員＞

主査 喜多 鉱一	東京工業大学 像情報工学研究施設 ヘルスケア情報寄付研究部門　客員教授
委員 大山 永昭	東京工業大学 像情報工学研究施設　教授
委員 山口 雅浩	東京工業大学 像情報工学研究施設　助教授
委員 国分 明男	財団法人ニューメディア開発協会　常務理事
委員 植村 泰佳	電子商取引安全技術研究組合（ECSEC）常務理事
委員 相澤 直行	財団法人医療情報システム開発センター　主任研究員
委員 奥住 啓介	財団法人データベース振興センター 事務局長兼振興部長
委員 松井 美楯	コニカ株式会社 メディカルイメージング事業本部 システムグループ　部長
委員 畠沢 菊男	日立コンピュータ機器株式会社 システム第２設計部 副部長
委員 近藤 隆	オリンパス光学工業株式会社 映像技術部開発３グループ 課長代理
委員 谷内田 益義	株式会社リコー 研究開発本部 オフィスシステム研究所 第一 OS 開発センター 主席係長研究員
委員 金井　洋一	株式会社リコー 研究開発本部 オフィスシステム研究所 第一 OS 開発センター　係長研究員
委員 風間　博之	株式会社 NTT データ　開発本部 技術開発部電子政府 PF グループ シニアエキスパート
委員 白方 貴史	株式会社 NTT データ　開発本部 技術開発部電子政府 PF グループ

＜オブザーバー＞

増井　弘一	国税庁 長官官房 企画課　主任税務分析専門官
小田　満明	国税庁 長官官房 事務管理課　主任税務分析専門官
武末　文男	厚生労働省 医政局 研究開発振興課医療技術情報推進室　室長補佐
長野　義久	厚生労働省 医政局 研究開発振興課医療技術情報推進室　管理係長
堀田　博幸	経済産業省 大臣官房 情報システム厚生課情報システム室　調整班長
楠木　真次	経済産業省 商務情報政策局 情報政策課　行政情報化係長
石井　伸治	経済産業省 商務情報政策局 情報セキュリティ政策室 セキュリティ技術一係長

＜事務局＞

財団法人ニューメディア開発協会
株式会社 NTT データ経営研究所

１． 研究会の目的

・文書や帳簿等の形態は、紙から電子（デジタル）媒体へと徐々に移行してきており、原本を電子文書とすることも容認されるようになってきている。
・それに伴い、電子化された文書等（以下「電子文書」という。）の管理上、その原本性が保証されることの重要性が高まってきている。
・経済産業省及びニューメディア開発協会では、「原本性保証電子保存システム」の基本的な機能の検討や要素技術を検討し、開発を行ってきた。
・今後、当該システムを広く普及していくためには、利用者が容易かつ安心して当該システムを調達・導入できるような、システムの確実性・信頼性を評価していく制度が必要であると考えられる。
・このような背景を踏まえ、「原本性保証評価・認定制度に係わる研究会」を発足し、評価認証スキームや制度の運用方法を出発点として、原本性保証に係わる製品の普及についての各種の検討を行うこととした。

１．１ 背景

デジタルネットワーク社会の発達に伴い、文書や帳簿等が従来の紙媒体から電子媒体へと形態が移行してきており、原本を電子文書とすることが容認されるようにもなってきている。行政機関においては、電子政府の実現に向けて、行政文書等を電子文書として受付、作成、保存・管理する動きが始まっており、書面の交付に関する情報通信技術利用のための関係法律が制定されたことなどもあり、民間においても各種文書の電子化が容認されることは今後ますます増えていくであろう。

このような動きの中で、電子文書の原本性保証対策を講じることの重要さは、企業・団体でも認識されつつある。特にエレクトロニックコマース等インターネット上で商取引を行う、銀行・証券・保険等金融機関が情報システムを利用してデータ交換を行う、医療機関等における診療録を保管する、さらには、行政機関への各種申請や届出を電子媒体で受領する、などの様々な局面において電子文書の原本性を確保することの重要性が高まってきている。

１．２ 研究会の目的

経済産業省及び（財）ニューメディア開発協会においては、これまで原本性保証電子保存システムの基本的な機能についての検討、及び要素技術の開発を行ってきた。昨年度は、原本性保証システム研究会を開催し、「電子文書の原本性保証ガイドライ

ン」、「原本性保証電子保存システム Protection Profile」（以下 PP）、「原本性保証電子保存システムインターフェース要件」を作成・作成支援を行ってきた。

今回の本研究会では、行政文書を検討の対象とし、原本性保証における評価・認定機関が具備するべき要件を抽出し、行政機関等のユーザー側が容易かつ安心して製品やシステムを導入できるように、既に取組みが進みつつある ISO/IEC15408 等への評価スキームにあてはめるか、もしくは新たな制度を創設が必要となるのかという点について検討することを出発点とし、製品やシステムの確実性・信頼性を評価する、そのための製品機能を明確にするなど、広い視点で製品の普及を目的とした検討を行った。

１．３　研究会における検討内容

１．３．１ 第 1 回研究会

第 1 回研究会では、昨年度の原本性保証電子保存システム研究会の成果を踏まえ、本研究会の目的の確認と、具体的な作業として行政機関の電子文書保存や原本性保証関連製品ベンダーの状況の把握等を行っていくことを確認した。また、評価認証機関が具備すべき要件については ISO/IEC15408 等の適応もしくは新制度創設の必要性等があることを提示しディスカッションを行った。併せて、昨年度の原本性保証電子保存システム研究会の成果物「原本性保証電子保存システム PP」のブラッシュアップを図るために PP の内容のリビジョンアップを行うことを確認した。

また、ISO15408 等のセキュリティ評価認証スキームが国際基準として確立されつつある中、原本性保証分野において「独自」制度を創設するのは適切ではないとの意見が出て、まずは制度の創設よりも原本性保証の技術的な要件定義を整理することが重要であることなどで合意した。

１．３．２ 第 2 回研究会

第 2 回研究会に先立ち、事務局にて原本性保証製品ベンダー10 社程度を対象として製品機能及びセキュリティ評価認証制度に対する意見についてインタビューを行った。また、ISO/IEC15408 及び ISO/IEC17799(BS7799 Part1)等に則ったセキュリティ評価認証制度の進捗状況及び評価コスト等について、推進団体及びベンダー各社に対しインタビューを行い、それらインタビュー結果を元に、原本性保証分野での評価・認定の適用について検討を行った。

上記で調査した各社の製品は、原本性保証機能の点で、おおよそ同様の技術を用いているものの、細部の実装技術では相違が見られた。

原本性保証で求められる要件については、あらためて事務局で整理を試みるために、「インターネットによる行政手続の実現のために」（平成 11 年 3 月共通課題研究会）や「高度情報通信社会本部制度見直し作業部会報告書」（平成 8 年 6 月同本部同作業部会）を引用したところ、両報告書において若干の表現の違いはあるが、基本的に異なるものではない。また、原本性保証要件とセキュリティ要件の対策が非常に重なる部分が多いなどから、電子文書の原本性を確保するためにユーザーとして何をすればよいのかということを今一度明確にする必要があることが分かってきた。特に「電子文書の証拠能力確保」を満足するために最低限やっておかなくてはならない要件を明確にすることが重要であると合意した。

この原本性保証対策要件、主に技術的に製品に搭載されるべき機能とは何かということを提示し、それと共に、ユーザーが製品を導入する際に製品機能を確認できるようなものが必要との意見があったことから、事務局にて原本性保証に係わるシステムのガイドラインもしくはチェックリストを作成していくこととした。

１．３．３ 第 3 回研究会

第 3 回研究会では、まず国内外の情報セキュリティ及び原本性保証に関する通達・規程類から、情報セキュリティと原本性保証要件の整理をした結果を出した。また原本性保証要件として複数存在している状況を本研究会で統一するため、主に行政文書を対象とした研究会であることから、共通課題研究会が定義した完全性・機密性・見読性を研究会で採用する要件とした。

原本性保証対策の必須技術要件を定めるための作業も行った。これは原本性を確保する際に最大の阻害要因になるであろう改ざんを挙げ、改ざんの抑止、予防、回復、検知といった観点での対策が原本性保証における必須の技術要件となり、中でも改ざん検出機能が絶対に必要となるとの議論が行われた。具体的な機能としては、改ざん検知、文書保存の時点（時刻）の特定、アクセス制御などが必要であるとの検討がなされた。

また、ユーザーが原本性保証製品を導入する際のチェックリスト案や、原本性保証に関する PP や Security　Target（以下 ST）はどのようにあるべきかなどの検討を行った。ガイドラインやチェックリストは、ユーザーが原本性保証を必要とする利用環境によって技術要件・運用要件が異なるため、各種の文書管理に関する法令、規程及びガイドラインを参考に、前提となる環境を想定して最低限必要な要件を抽出し、利用環境に沿った内容にするべきであることを確認した。

原本性保証電子保存システム PP についてはアンケート結果を盛り込んだ案を元に検討を行った。各ベンダーが想定する物理環境やネットワーク環境、想定される脅威を実際にどのように考え製品に機能として盛り込まれたのかということが分かれば、各社の共通的な機能、ひいては原本性保証システムの必須技術機能として PP に盛り込むことが可能ではないかとの意見などから、事前にベンダーにアンケートを行っている。

１．３．４ 第 4 回研究会

第 4 回研究会では、電子文書とログ/認証子をどこに保管するかという観点から改ざんされていないことを証明するスキームを 5 つほど想定し、そのうち 3 つのスキームに機能を照らし合わせて作成したガイドラインとチェックリスト(案)の検討を行った。

また、来年度以降の原本性保証システムの普及に向けた施策として、ガイドライン・チェックリストのベンダー・ユーザー双方への普及・浸透化、ISO/IEC15408 評価認証制度への適用、独自の評価・認証制度の設立、製品普及促進のためのベンダー中心の協議会の発足、モデル法の制定の 5 つの方策の検討を行った。

ユーザーが製品を選択する際、選択基準として製品の格付け等があるとよいのではないか、また格付けが必要とされる場合、格付けを行う機関としてはどのようなものがあるのかなどの検討が行われた。

今後の PP の改訂を進めるにあたり協議会等の中立的な団体が行うといったことや、ベンダーが自社製品について記述した PP を他社に開示してもらい、他社はそれらを参考にしながら PP を作っていくと、網羅的・体系的に複数の PP が出来上がり、コストも比較的低く押さえられる、といった案なども出され、それぞれ検討を行った。

２． 原本性保証に関する各種通達・報告書等

・原本性保証の考え方を整理するために、行政機関や民間企業などに向けて策定された複数の報告書等に記述されている原本性保証要件の定義を参照した。

２．１ 「インターネットによる行政手続実現のために」より（共通課題研究会最終報告書）

行政事務や手続きにおいて、文書の電子化が進められており、「インターネットによる行政手続実現のために」が発行されている。本研究会ではこの内容に従って行政機関における原本性確保の考え方について整理した。

２．１．１ 原本性確保の考え方と検討

平成 10 年 9 月に総務庁が主体となって、行政情報化の共通的な課題解決に向けて検討する研究会「共通課題研究会」を発足し、共通課題の１つである電子文書の原本性の確保方策について、制度面及び技術面からの検討が行われた。最終報告書はこの研究会により策定されたものである。

この報告書では、電子文書は紙文書と比較して、改ざんが容易でその痕跡も残りにくく、また記録媒体の経年劣化等により内容の消失が起きやすいなどの特性を有しているとし、行政機関におけるこれらの保存・管理上の問題点を明らかにし、対策を検討していく必要があるとしている。

また、この報告書においては、紙文書についても原本の意味は明確ではないので、電子文書についてのみ、法的意味での「原本」あるいは「原本性」の定義付けをする必要性は薄いという考え方が述べられている。この報告書では、「『電子文書の原本性を確保する』とは、『紙文書と比較した場合の保存・管理上の問題点が解決された状態にしておくこと』という意味で用いる」としている。

２．１．２ 原本性確保に必要な要件と対策

電子文書の保存・管理にあたっては、完全性、見読性、機密性の確保が必要と明記している。

完全性の確保とは、電子文書が確定的なものとして作成又は取得された一定の時点以降（原簿等追記型のものについては、追記した部分について、その追記した時点以

降)、記録媒体の経年劣化等による電子文書の消失及び変化を防ぐとともに、電子文書に対する改変履歴を記録することなどにより、電子文書の改ざん等を未然に防止し、かつ、改ざん等の事実の有無が検証できるような形態で、保存・管理されることであるとしている。

機密性の確保とは、電子文書へのアクセスを制限すること、アクセス履歴を記録することなどにより、アクセスを許されない者からの電子文書へのアクセスを防止し、電子文書の盗難、漏えい、盗み見等を未然に防止する形態で、保存・管理されることであるとしている。

見読性の確保とは、電子文書の内容が必要に応じ電子計算機その他の機器を用いて直ちに表示できるよう措置されることであるとしている。

この報告書における完全性、機密性、見読性の確保の対策要件は次頁の表のとおりである。

表２－１　共通課題研究会報告書の原本性保証対策要件

対策要件の内容	対策要件の種類			対象となる文書の適用範囲
	完全性	機密性	見読性	
電子文書の保存・管理についての責任及び権限を明確化するため、管理責任者等を定めること。（組織体制）	○	○	○	○
ﾎｽﾄｺﾝﾋﾟｭｰﾀ、端末機、通信関係装置、ﾌﾟﾛｸﾞﾗﾑその他のﾊｰﾄﾞｳｪｱ及びｿﾌﾄｳｪｱの全部又は一部により構成されるものであって、電子文書を保存・管理するためのｼｽﾃﾑ(以下、電子文書保存・管理ｼｽﾃﾑ)にｱｸｾｽする者をID・ﾊﾟｽﾜｰﾄﾞ等によって識別し、認証すること。	○	○		○
電子文書を記録した媒体は、保管場所を決め、施錠して保管し、保管場所からの搬出入及び授受は管理記録を整備して行うこと。	○	○		○
電子文書保存・管理ｼｽﾃﾑに対するｱｸｾｽを監視及び記録すること。	○	○		◎
電子文書保存・管理ｼｽﾃﾑには、電子文書の内容・性格に応じて、ｱｸｾｽ権限を設定すること。	○	○		○
電子文書の保存、参照、更新、複写及び廃棄の日時並びに実施者を記録するﾛｸﾞを取得し、保存すること。当該ﾛｸﾞは、安全な場所及び媒体に一定期間保存すること。	○	○		○
電子文書の更新履歴（削除した内容、追加入力した内容等）が確認できること。当該更新履歴は、安全な場所及び媒体に一定期間保存すること。	○			◎
更新前の電子文書についても、必要に応じ一定期間保存すること。	○			○
電子文書の盗難、漏えい等に備えるとともに、改ざん等を防止するため、必要に応じ電子文書を暗号化して保管すること。	○	○		○
必要に応じ改ざん検出機能を有する電子署名を電子文書に施して保管すること。	○			○
ｼｽﾃﾑﾀｲﾏｰの設定・変更等の作業履歴が確認できること。当該作業履歴は安全な場所及び媒体に一定期間保存すること。	○			◎
電子文書のﾊﾞｯｸｱｯﾌﾟを定期的に行い、当該ﾊﾞｯｸｱｯﾌﾟを適切に保管すること。	○			○
電子文書を記録した媒体及びそのﾊﾞｯｸｱｯﾌﾟについては、定期的に保管状況及びﾃﾞｰﾀの内容が正常であるか否かの点検を行うこと。	○	○		○
外部から入手した電子文書は、ｳｲﾙｽﾁｪｯｸ後に利用すること。	○			○
電子文書の出力に必要な電子計算機、ﾌﾟﾛｸﾞﾗﾑ、通信関係装置、ﾃﾞｨｽﾌﾟﾚｲ、ﾌﾟﾘﾝﾀ等を備え付け、いつでも必要な場合には電子文書をﾃﾞｨｽﾌﾟﾚｲの画面及び書面に出力できるようにすること。			○	○
電子文書保存・管理ｼｽﾃﾑの保守、点検、改造等は計画的に行い、当該行為の期間中における電子文書の保護措置を講ずること。	○	○		○
停電、誤切断等による電子文書の消失、破壊等を防止するため、無停電電源等の必要な措置を講ずること。	○			○
ﾌﾟﾛｸﾞﾗﾑのﾊﾞｯｸｱｯﾌﾟを行い、適切に保存すること。	○		○	◎
必要に応じ、ｼｽﾃﾑ監査を実施すること	○	○	○	○

＊ 上記の表は「インターネットによる行政手続実現のために」を参照し、本研究会で作成。
＊ 適用対象となる文書の範囲：◎は消失・改ざん・漏えい等による国民の権利義務等、国民生活に重大な影響を与えるおそれのある電子文書のみ。○は対象となる全ての電子文書。

２．２ 「高度情報通信社会推進本部制度見直し作業部会報告書」より

この報告書は、高度情報通信社会推進本部の制度見直し作業部会が平成 8 年 6 月に策定したものであり、法令に基づき民間事業者等に保存が義務付けられている各種書類において、電子的な保存に関する課題と対応策をまとめ、その在り方について制度面や技術面の検討を行うこととしている。

本研究会では、民間における文書の電子保存に必要な要件を抽出するため、これを参照し、電子文書保存の観点による原本性保証の要件の整理を行った。

２．２．１ 電子文書の保存方法と留意点

この報告書では、「紙による情報の処理」から「電子化された情報の処理」への移行を実現することが重要であると述べた上で、国民の負担軽減等の観点から、法令に基づき民間事業者等に保存を義務づけている各種の書類については、電子文書による保存を原則として容認するものとしている。また、入力段階から電子化している文書は、全て電子文書保存を可能にするよう法令改正、通達発出等を行うこととしている。さらに、既に紙で作成された文書等についても、原則として電子文書による保存を可能にする措置を講じることとされている。その際に、筆跡鑑定等、紙特有の捜査が行えるという点で情報の確保に留意する必要があるという点や、書類の保存方法を各々で規定している法律等が、相互に関連している部分にも留意する必要もあると述べられている。

２．２．２ 電子保存に必要な要件と対策

電子文書保存に必要な要件として、真正性、見読性、保存性の確保の 3 要件が明記されている。

真正性の確保とは、データの故意又は過失による虚偽入力、書換え、消去及び混同を防ぐことである。

見読性の確保とは、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である。

保存性の確保とは、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である。

この報告書における真正性の確保、見読性の確保、保存性の確保の対策要件は次頁の表のとおりである。

表２－２　制度見直し部会作業報告書の原本性保証対策要件

対策要件の内容	対策要件の種類		
	真正性	見読性	保存性
改変・削除の履歴及び内容が記録され、上書きができないｿﾌﾄｳｪｱ及びﾊｰﾄﾞｳｪｱの使用	○		
電子媒体上にﾃﾞｰﾀを記録した日時、媒体製造番号等を自動的に記録し、情報の書換え、混同を防止するｿﾌﾄｳｪｱの使用	○		
ﾃﾞｰﾀ入力時に入力者や入力日時等が特定できるよう自動的に入力履歴ﾃﾞｰﾀを記録するｿﾌﾄｳｪｱの使用	○		
ﾃﾞｰﾀの不正な利用、改ざんの防止のためには、ID、ﾊﾟｽﾜｰﾄﾞ、ﾃﾞｼﾞﾀﾙ署名を管理するｿﾌﾄｴｳｱ及びﾊｰﾄﾞｳｪｱの使用	○		
ﾃﾞｰﾀの改ざん、滅失の防止のためのﾊﾞｯｸｱｯﾌﾟの作成及び保存	○		
書類の作成に際しての署名・押印を求める必要性を吟味（署名・押印）	○		
暗号技術を応用したﾃﾞｼﾞﾀﾙ署名により、電子ﾃﾞｰﾀを保存し、かつ、必要な当該署名部分の複写ができないように措置する技術が開発されていること、電子印鑑技術を利用する方法があること等の最近の技術動向に留意	○		
書類を保存すべきとされている場所に電子ﾃﾞｰﾀを保存し、かつ、必要な機器を設置して、職員の求めに応じ、時機に応じてﾃﾞｨｽﾌﾟﾚｲ装置への表示や印刷することの義務づけ		○	
必要に応じて、電子データの内容を見読容易な形態に変換し複写することの義務づけ		○	
ﾊｰﾄﾞﾃﾞｨｽｸ、FD、光ﾃﾞｨｽｸ等電子媒体の劣化、喪失、損壊の防止のための適切な管理			○
媒体上に記録されたﾃﾞｰﾀを可視化するための仕様、方法の記録・適切な管理			○
記録・管理された仕様・方法に基づき電子ﾃﾞｰﾀの内容を見読可能な状態とするための電子媒体、機器、ｿﾌﾄｳｪｱの適切な保存			○

＊上記の表は「高度情報通信社会推進本部制度見直し作業部会報告書」を参照し本研究会で作成

２．３　「診療録等の電子媒体による保存に関する解説書」より

この解説書は、厚生労働省（旧厚生省）より委託を受けた（財）医療情報システム開発センターが､診療録等の電子媒体による保存に関する技術的要件の検討について遵守すべき基準やガイドラインをまとめたものである。

診療録等の電子保存に関する原本性保証の考え方は、平成 11 年に旧厚生省より通知された「診療録等の記載方法について」の中で示されている。この通知では、高度情報通信社会推進本部制度見直し作業部会報告書に基づき､診療録等の電子化にあたっては真正性・見読性・保存性の基準を確保することが明記されている。それと同時に、留意事項として、施設管理者による運用管理規程等を定め、組織や体制の整備、患者のプライバシー保護等の対策を実施することも盛り込まれている。

また、この通知の運用を補うものとして、「法令に保存義務が規定されている診療録

及び診療諸記録の電子媒体による保存に関するガイドライン等について」が策定された。このガイドラインでは、診療録の電子保存は医療機関の自己責任において行うことを原則とした上で、真正性・見読性・保存性の確保について、各要件の技術的な対策を例示している。さらに、前述の通達の留意事項を受け、医療機関で電子保存を行う際に定めるべき運用管理規程の事例として、医療機関の規模に合わせて記述されている。病床300～400 程度の病院と、常勤医師・非常勤医師各 1 名程度の一般的な診療所の 2 種が想定されており、それぞれの施設に適した運用管理規程を作成・遵守することが記されている。

２．４ 「電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関する法律」より

この法律は、平成 10 年 3 月に財務省（旧大蔵省）令として交付され、平成 10 年 7 月に施行されたものである。電子帳簿保存法の通称で呼ばれている。

税務署の認可を受けた企業では、7 年間の保存義務のある国税関係帳簿書類を電子情報として記録媒体に保存できるようになっている。この法令は、政府の規制緩和政策の一環として、主に、税務執行の公正性を保ちながら、ペーパーレス化によるコスト削減を進め、企業側の帳簿類の保存義務軽減化を目的としたものである。

帳簿類の電子保存を実施する上では、企業側に対して真実性の確保と可視性の確保の 2 要件が求められている。真実性の確保としては、訂正／加除履歴の確保、帳簿間記録の相互追跡の確保、処理過程の文書保存の 3 点について、可視性の確保については、即時見読可能性の確保、検索可能性の確保の 2 点を守ることが必要とされている。

この法令の特徴は、電子保存された帳簿類の原本性を保証することよりも、文書管理を行うファイルシステムとして、複数の帳簿間の整合性を一致させることを重視した内容になっているという点である。

３． 原本性保証を取り巻くユーザー（行政機関）の状況

・本研究会においては行政文書を対象としたことから、行政機関の文書管理の現状を把握することとした。
・総務省の「第 34 回各省庁統一文書管理改善週間実施状況調査」によれば、省庁における文書等の電子媒体による保管割合は、平成 7 年の 48%から平成 12 年には 77%に増えている。それに伴い、電子文書の中でも原本性保証が求められる数が増加していると予想される。
・中央省庁では、「行政文書の管理方策に関するガイドライン」に則って文書管理の規定を作成し、運用することになっている。
・一部の地方自治体でも、電子文書の管理方策に関する規程等が定められている事例が見られる。

３．１ 中央省庁における文書管理の現状

３．１．１ 中央省庁の状況

総務省より公開されている「第 34 回各省庁統一文書管理改善週間の実施状況について（概要)」（平成 12 年 12 月総務庁）によれば、職員 1 人当たりの電子媒体による情報の保管割合は平成 7 年度の 48%から平成 12 年度の 77%に大幅に増加している。同時に、紙媒体で管理している文書は、平成 7 年度の 50%から平成 12 年度の 22%に大幅に減少傾向にある。現在の状況としては、紙文書と電子文書が混在して取り扱われているが、今後はさらに電子化の傾向が強くなると思われる。

３．１．２ 行政文書の管理方策に関するガイドライン

平成 11 年 5 月の「行政機関の保有する情報の公開に関する法律」の制定により、各行政機関は法第 37 条等の規定に基づいて作成された「行政文書の管理方策に関するガイドライン」（平成 12 年 2 月各省庁事務連絡申合せ）に沿って各行政機関においてルールを定め、運用することとなった。

このガイドラインでは、対象となる行政文書に電子情報も含まれており、今後の情報化の進展や諸課題の検討状況を踏まえ､必要に応じてガイドラインの適宜見直しを行うことが明記されている。

（１）行政文書ファイル

行政文書ファイルとは、「能率的な事務又は事業の処理及び行政文書の適切な保存の目的を達成するためにまとめられた、相互に密接な関連を有する行政文書（保存期間が１年以上のものであって、当該保存期間を同じくすることが適当であるものに限る。）の集合物」である。また、行政文書ファイルの帳簿（行政文書ファイル管理簿）については、原則としてネットワーク（LAN 又は省庁内ネットワーク）上の、データベースとして整備するものとされている。

（２）保存期間

行政文書の保存期間に関する基準は、本ガイドライン別表の該当する行政文書の類型を参考にして、「行政文書保存期間基準」を定めることになっている。最低保存期間の最も長いものは 30 年とされているが、必要に応じ永年保存区分（未来永劫の趣旨ではなく、不定の職務上必要な期間）を設けることができる。その保存期間の起算日は、行政文書の作成又は取得の日のほか、これらの日以後の日で、行政機関の長が適切な管理に資すると認める日とされており、満了日は、行政文書ファイルにまとめられる文書のうち、満了日が最も遅い日と定められている。

（３）記録媒体の変換

行政文書は、保存期間が満了する日まで必要に応じ記録媒体の変換を行うなどにより、適正かつ確実に利用できる方式で保存するものとされている。この方式とは、電子文書の場合、ソフトウェアやハードウェアの技術発展、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等の措置をいうとされている。

（４）保存場所

保存場所は、「組織としての管理が適切に行い得る専用の場所」とされ、フレキシブルディスク等に保存されている電子情報の場合は共用の保管庫、ホストコンピュータで管理されている磁気媒体又はサーバの共用部分、文書及び図画の場合は、事務室及び書庫の書棚とされている。

（５）管理体制

各行政機関の長は、「行政文書の管理に関する定め」を制定し、その行政文書の管理体制として、各行政機関に「総括文書管理者」、「文書管理者」及び「文書管理担当者」を置くこととされている。

総括文書管理者は行政機関毎に１人置くこととし、官房長等を指名するものとし、①行政文書の管理に関する定め等規程類の整備、②行政文書分類基準表、行政文書ファイル管理簿の整備、③行政文書の管理に関する事務の指導監督、研修等の実施を業務とする。

文書管理者は原則として各課等毎に各課等の課長等を指名し、①行政文書分類基準表、行政文書ファイル管理簿の作成、②保存期間の延長、国立公文書館

等への移管又は廃棄の各措置の実施、③課等の保有する行政文書の管理の徹底を業務とする。

文書管理担当者は原則として各課等ごとに各課等の補佐又は係長から指名し、文書管理者の補佐役を担う。

３．２ 地方自治体の文書管理にみる電子文書の取扱いの例

３．２．１ 北海道

（１）「北海道電子情報管理規程」

本規程は、電子情報としての文書の取扱いに関する条項が定められており、法制文書課長、主務課長、文書主任の各々の業務範囲が規定されている。

（２）「電子メール規程」

本規程では、通信機器を利用することができる施行文書は、公印の押印を省略できると定められている。また、文書主任は、受信した公文書を速やかに紙に出力すること等が規定されている。

３．２．２ 大阪府

（１）「大阪府庁内電子メールシステム管理運用要領」

本要領は、アクセス制御に関する条項を多く設けている。特に、システムに登録された送受信情報の保存期間は、送信の日又は開封の日から起算して 2 週間（閉庁日を含む）とすると定めている。

３．２．３ 神奈川県

（１） 「神奈川県行政文書管理規程」

本規程は、知事から法務文書課長、文書事務主任、職員等に至るまで、各権限者について細かく条項を設けている。また、電子メールに関する内容も盛り込まれている。電子文書によって処理できる範囲については、総務部法務文書課長が別に定めることになっている。

行政文書の整理保管等の事務は、総合文書処理システムを利用することを原則としているが、データの利用目的等により、受信した電子情報を当該システムに登録しない場合は、フロッピーディスク等に保存することを定めている。また、原本を紙文書で保管している電子文書については、毎年度ごと当該電子文書を削除することを定めている。

３．３ 行政機関の文書管理に関する原本性保証を取り巻く状況

行政機関から出された各種の報告書やガイドラインなどから、行政機関・民間いずれを問わず電子文書の原本性を保証できるよう対策を講じることの重要性が、非常に強く訴えられていることが分かる。「高度通信社会推進本部制度見直し作業報告書」（2 章 2 項参照）では、行政機関が所管する団体・企業等で保存すべき文書について、電子的な方法で保存する場合の要件が記述され、「インターネットにおける行政手続のために」（2 章 1 項参照）では、行政機関で保存するべき文書を対象として、電子文書の原本性確保要件が記されている。また地方公共団体では、電子文書を含む文書管理規程などによってルールが作られている。

電子文書を取り扱っていく上で文書管理規程などでルールを明確にしておくことや、原本性保証対策をしっかりと行うことは明確になってきているものの、電子文書の原本性を確保するための具体的な実効策については、未だはっきりと提示されていない状況にあるといってよいだろう。

４． 原本性保証に関するベンダーの動向

・原本性保証製品の普及の検討のため、現状の製品の動向を把握することとした。
・原本性保証製品については、製品情報の中に「原本性保証」機能が明記されているシステムや製品のベンダーを中心に、製品機能の概要・ユーザーニーズ・想定される利用者環境・保護対象資産等の意見を収集した。
・ベンダー各社は「制度見直し作業部会報告書」や「共通課題研究会最終報告書」等の原本性確保要件等を参照しているが、製品で実装している機能は多様であることがわかってきた。

４．１ 原本性保証関連製品ベンダーからの意見収集

原本性保証製品の普及を考えるに先立ち、国内の製品の動向を把握するため、各社の Web サイトや製品パンフレットに「原本性保証」機能が明記されている製品と、原本性保証の分野に関連すると思われる機能を持つ製品について調査を行った。また、該当する製品の開発ベンダー15 社の中から 10 社に対し、製品機能の概要やユーザーニーズに関するインタビューを行い、想定しているユーザーの環境、製品の機能で保護するべき情報等のアンケートを実施して、意見を収集した。

インタビューの際には、ISO／IEC15408 情報セキュリティ評価基準に則った「IT セキュリティ評価認証制度」に関する意見も収集した。

４．２ 原本性保証関連製品の機能概要

本研究会で調査対象とした原本性保証関連製品の機能概要を以下の表にまとめた（表４－１を参照）。この表は、原本性保証の機能と思われるものを中心に、それに類似する機能を記述したものである。

表４－１　原本性保証製品の機能概要

製品名	社名	機　　能
Trusty Cabinet V1	(株)ﾘｺｰ	・ユーザー固有のアカウント名とパスワードを設定し、SSL通信の上でユーザーの認証と保存装置の認証（SSLによる認証）を行う。 ・各電子文書に対するアクセスを全て文書アクセスログとして記録する。 ・保存装置へのアクセスを全て装置アクセスログとして記録する。 ・電子文書を原本として確定後は設定された保存期限内の削除を禁止する。 ・電子文書の属性情報に原本・謄本・仮原本のステータスを付与する。 ・電子文書の改訂を行うとバージョン管理が自動的に行われ、属性情報でバージョン構成が管理される。 ・電子文書と認証子(改ざん検知コード)を同フォルダの別ファイルで保存 ・長期保存のために光ディスク（保存媒体）に電子文書を書き出す。 ・管理者による時刻情報設定の履歴を記録し、タイマーIDを付与したタイムスタンプで保存文書の前後関係を保証する。 ・限定された特殊APIによるSSL通信アクセスのみを許可する。
GENPON （開発コード）	ｵﾘﾝﾊﾟｽ光学工業(株)	・ユーザー認証は、パスワード・指紋認証・IC カード等の少なくとも１つを使用する。(認証方法は、導入時に選択可能な設計となっている） ・原本アクセスログの中でコンテンツ参照のログを記録する。 ・装置アクセスログにユーザー名、ユーザーのアクセス日時等のログイン・ログアウトの情報を記録する。 ・確定操作後の電子文書の削除を禁止する。 ・電子文書の属性情報に原本、謄本、仮原本等のステータスを付与し、バージョン番号・バージョン登録日時等の情報を記録して変更履歴を管理する。 ・電子文書と認証子(改ざん検知コード）を関連付けて保存する。 ・複数の電子ファイルをまとめた単位に対しても認証子を付与する。 ・保存装置内のファイルに対しては、保存した順番に関する情報を付与する。 ・管理者による時刻情報設定毎にタイマー設定 ID を付与し、時刻の不正な変更を抑制する。 ・万一、原本が紛失した場合、謄本があればそれを原本に復旧できるが、電子文書へのアクセスログに謄本から復旧したことが明記される。 ・バックアップは基本的にシステムが自動で行う。 ・装置間、及び装置一定められた光ディスク間では原本の電子文書の移動が可能である。 ・保存する電子文書の暗号化は、設定により可能である。 ・暗号化する場合、鍵の生成・管理方法を複数の手段から選択できる。 ・限定された特殊 API による SSL(もしくは専用プロトコルの）通信アクセスのみを許可する。
製品名及び社名は非公開		・ユーザーのID、パスワードによりアクセス者を識別する。 ・ユーザー毎に許される操作(登録・更新)等のアクセス制御機能を持っている ・電子文書へのアクセスログを記録する。 ・原本となる電子文書の登録とその読出のみが可能であり、上書きは不可であるが、更新時には更新前後両方の文書を保存する。（全ての版を保存する） ・電子文書の更新毎に新たな識別情報を付与し、それらのリンクを行い、各文書の世代を管理する。 ・電子文書毎に更新可・複写可等の属性を持つことができる。 ・識別 ID（装置 ID・媒体 ID・文書 ID）で、原本と写しを区別する。 ・電子文書に改ざん検知コードを付与し、保存する。 ・光磁気ディスクにバックアップを取得する。 ・装置内にUPSを内臓している。

Digital Imaging System	ｺﾆｶ(株)	・秘密鍵を用いた相互認証プロトコルを使用し、ユーザーを認証する。 ・故意、過失に関わりなく全てのユーザーにおける書換え・消去は不可としている。 ・画像作成（発生）日時、記録した日付、時刻をログとして記録する。 ・画像情報にメッセージ認証コードを付与し、改ざんを検知する。 ・特定のドライバソフトを使用し、媒体のヘッダー情報に認証子を組み込み、媒体とドライバを相互認証することで、特定ドライバ以外のアクセスは不可としている。
ﾒﾃﾞｨｶﾙｲﾒｰｼﾞｽﾃｰｼｮﾝ （型名：P－SYMI－002）	日立ｺﾝﾋﾟｭｰﾀ機器(株)	・オリジナル（O)、オーソライズオリジナル（AO)、オーソライズコピー（AC）のデータ属性を持つ。原本およびそのコピーに相当する AO、AC 属性のデータは故意、過失に関わりなく書換え、消去および属性の変更が出来ない。 ・画像発生日時、記録日時、担当医師名などの付随データもデータ本体と同じく上記の保護を行う。 ・媒体の物理仕様、論理仕様、データフォーマットなど(財)医療情報システム開発センター（MEDIS-DC）が制定した共通規格に従ったデータの記録を行い、共通規格機器間でのデータ互換性を保証している。また共通規格以外の機器での媒体へのアクセスを抑止し、データの安全性の確保と、秘匿を支援している。 ・専用のファイルシステムでのみしか媒体へのアクセスが出来ないようにしてあり、一般 OS でのデータの書換え・消去を防いでいる。
X 線 CT 装置、画像観察・診断用装置等に搭載している原本性保証関連機能	(株)島津製作所	・オリジナル（O)、オーソライズオリジナル（AO)、オーソライズコピー（AC）のデータ属性を持つ。原本およびそのコピーに相当する AO、AC 属性のデータは故意、過失に関わりなく書換え、消去および属性の変更が出来ない。 ・画像発生日時、記録日時、担当医師名などの付随データもデータ本体と同じく上記の保護を行う。 ・媒体の物理仕様、論理仕様、データフォーマットなど MEDIS-DC が制定した共通規格に従ったデータの記録を行い、共通規格機器間でのデータ互換性を保証している。また共通規格以外の機器での媒体へのアクセスを抑止し、データの安全性の確保と、秘匿を支援している。 ・専用のファイルシステムでのみしか媒体へのアクセスが出来ないようにしてあり、一般 OS でのデータの書換え・消去を防いでいる。
eFiling Meister	(株)東芝	・アプリケーションによる ID、パスワードチェックにより、ユーザーの認証を行う。 ・ログイン、ログアウトはもちろんのこと、電子文書への登録、検索などのアクセス履歴をログとして記録することが可能である。 ・電子文書を暗号化することが可能である。 ・電子文書にデジタル署名を付与し、改ざんを検知することが可能である。
ｾｷｭｱｽﾄﾚｰｼﾞｼｽﾃﾑ ＊製品化計画中	三菱電機(株)	・秘密鍵を用いた相互認証プロトコルを使用し、ユーザーを認証する。 ・全てのユーザーの電子文書への登録・参照・削除等のアクセス履歴をログとして記録する。 ・基本的には変更・上書き・消去は不可だが、ユーザーの初期導入時の設定により、削除可能である。 ・電子文書は暗号化して保存する。 ・タイムスタンプの発行は第三者機関に依頼する。（もしくは自社内で行う第三者機関サービスで対応する） ・ユーザーの導入時の設定により自動的にバックアップを取得する。 ・オリジナル電子署名と新たな電子署名と、オリジナル認証書の有効性証明書とタイムスタンプを合わせて第二世代署名として管理し、長期にわたる有効期限を確立する。

IME ﾌﾟﾗｯﾄﾌｫｰﾑ	ﾀﾝﾌﾞﾙｳｨｰﾄﾞ・ｺﾐｭﾆｹｰｼｮﾝｽﾞ(株)	・電子文書の送信者･受信者をパスワードにより認証する。 ・電子文書が IME サーバに送信されていることを受信者へ通知し、また、そのメール発信履歴を記録する。 ・電子文書のログに作成者等の情報を記録する。 ・受信者による IME サーバへのアクセス履歴を記録する。 ・電子文書のログに、受信者によるダウンロード等の履歴を記録する。 ・送信者による文書の変更・消去は可能だが、受信者は電子文書のダウンロードのみ可能で、変更・上書き・消去等は不可とする。 ・新しい電子文書のファイル作成毎に、RC４で暗号化し、保存する。 ・タイムスタンプの発行は、第三者機関による時刻証明サービスを利用する。
Docu Touch	三井物産(株)	・インターネット経由、システム上で電子文書に電子署名（複数可）を付してアーカイブすることが可能。 ・１つのユーザー名、２つのパスワードでユーザーの本人確認を行う。また、電子署名を使用する場合には PKI の仕組みによる本人確認も行う。 ・全ての電子文書は暗号化され、ハッシュ値により原本性を確認、改ざんチェックを行っている。 ・ワークフローや電子署名等のトランザクションは全て履歴管理が可能である。 ・定期的に自動バックアップを行っている。 ・原本性を保つため保存されている電子文書をシステム上で直接修正することは出来ず、読み取りのみ可能である。編集が必要な場合には Check-out／in 機能を用いてクライアント側で編集を行う。尚、Check-out／in を行った場合には、電子文書のバージョン管理が自動的に行われる。 ・個々の電子文書にセキュリティ設定（アクセス権限など）が可能となっている。 ・フロントサーバー（WEB）とドキュメント保管サーバーを分離している。 ・API 提供により、バイオメトリクス等のセキュリティツールの追加が可能となっている。 ・PKI、RSA, SSL や HTTPS 等により、通信経路での暗号化と改ざん防止を行う。
Secure Seal	(株)NTT ﾃﾞｰﾀ	・ハッシュ値を電子文書証明センターに送り、スーパーハッシュ値や集約ハッシュ値を算出することで、改ざんを検出する。 ・ハッシュ値のみが送信されるので、原本の漏えいを防止することができる。 ・時刻をミリ秒ごとに監査情報を作成し、厳密かつ厳正な時刻を証明することが可能である。 ・センター側で 24 時間登録受付を行い、電子文書の原本性と作成時刻を保証した証明書を発行し、ユーザー企業へ送付する。 ・ユーザー企業は、電子文書本体と証明書を自身で保存する。
電子公証サービス	NTT ｺﾐｭﾆｹｰｼｮﾝｽﾞ(株)	・IC カードに組み込んだパスワードで、コンシューマの本人認証を行う。 ・導入時の設定により指紋認証も対応可能である。 ・コンシューマによる注文確認メールの取得時及びサービス企業による本人受領確認時にログを記録する。 ・受領記録、注文記録、契約書の各取引記録のログに日時・実施者（コンシューマ、サービス企業）の情報を付与する。 ・コンシューマからプラットフォームへのアクセスログを記録する。 ・コンシューマは自分の取引記録のみ参照可能とし、サービス企業は自社分の取引記録のみを参照可能とする。 ・電子文書及びタイムスタンプに電子署名を付与する。 ・定期的にバックアップを取得する。

４．３ 製品機能からみた分類

現在国内で提供されている製品のシステム構成や機能、運用形態で大別すると、システム構成の特徴から見た「金庫型」・「ネットワーク型」と、運用形態の特徴から見た「自己型」・「第三者型」に分けられる。以下に、各分類型の種類について記述した。

分類型の種類	特徴的な機能
金庫型	・ソフトウェアもしくはハードウェアによって、電子文書を厳重に保管する機能をもつタイプである。 ・製品単独で完全性・機密性・見読性を確保できる。
ネットワーク型	・クライアント／サーバのネットワーク間でのセキュアな通信に重点を置いたタイプである。 ・ネットワーク上に存在する複数のサーバ間での文書情報の管理を可能にする。

分類型の種類	特徴的な機能
自己型	・第三者による認証や時刻証明を行わないことに特徴をもつ。
第三者型	・第三者による認証や時刻証明を行うことに特徴をもつ。

金庫型・ネットワーク型と自己型・第三者型を縦軸、横軸に当てはめて、分類を試みた(図４－１を参照)。

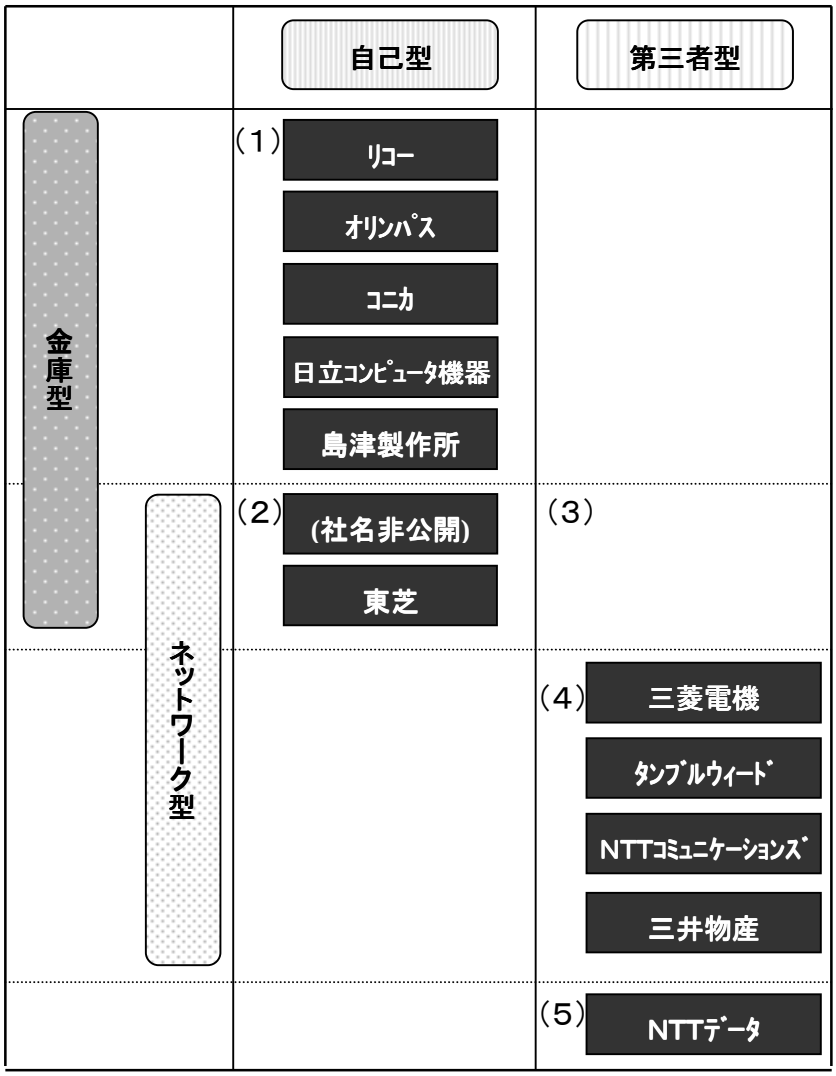

図４－１　国内で提供されている原本性保証製品の分類イメージ

（１）　金庫型／自己型

ソフトウェア及びハードウェアで厳重に電子文書を保管する。媒体間で、電子文書を移動させることに対しては、識別子により改ざんを検出するといった特徴がある。また、限定されたアプリケーション等からしかアクセスできない等の特徴をもつタイプを想定している。

（２）　金庫型／ネットワーク型／自己型

一部金庫型の機能を持つが、ネットワーク上に分散設置されたサーバ間で原本性を保証するための各種機能を持っている。

（3） 金庫型／ネットワーク型／第三者型

金庫型もしくはネットワーク型の機能を持つが、認証や時刻証明は第三者が行うことに特徴がある。

（4） ネットワーク型／第三者型

主にセキュアな通信を実現するための機能と、第三者による認証や時刻証明の機能をもっている。インターネット等オープンネットワークでの利用も想定している。

（5） 第三者型

認証や時刻証明は第三者が行うことなどに特徴がある。

4．4 共通課題研究会の最終報告書における対策要件との適合

本研究会では、「共通課題研究会最終報告書」（2 章 1 項参照）の対策要件に対応した原本性保証関連の機能について、製品に実装されているかどうかという観点で、整理を行った。その結果、「電子文書を保存・管理するためのシステムにアクセスする者をID・パスワードによって識別し、認証すること」と「電子文書の保存・参照・更新・複写及び破棄・・(中略)・・ログを取得し、保存すること」の項目については、対応している製品が多かった。さらに、「改ざん検出機能を有する電子署名を電子文書に施して保管すること」の項目については、調査の対象となった全製品が何らかの技術で改ざん検出機能を実装していることがわかった（表４－２を参照)。

表４－２　共通課題研究会最終報告書対策要件と製品機能の対応表

共通課題研究会報告書の対策要件	ﾘｺｰ	ｵﾘﾝﾊﾟｽ	某社	ｺﾆｶ	日立	島津	東芝	三菱電機	ﾀﾝﾌﾞﾙ	NTTｺﾐｭﾆ	NTTﾃﾞｰﾀ	三井物産
○ 電子文書の保存・管理についての責任及び権限を明確化するため、管理責任者等を定めること。（完、機、見）	—											
○ホストコンピュータ、端末機、通信関係装置、プログラムその他のハードウェア及びソフトウェアの全部又は一部により構成されるものであって、電子文書を保存・管理するためのシステムにアクセスする者をID、パスワード等によって識別し、認証すること。（完、機）	○	○	○	○	○	○	○	○	○	○		○
○ 電子文書を記録した媒体は、保管場所を定め、施錠して保管し、保管場所からの搬出入及び授受は管理記録を整備して行うこと。（完、機）	—											
◎電子文書保存・管理システムに対するアクセスを監視及び記録すること。（完、機）	○	○	○				○	○	○	○		○
○電子文書保存・管理システムには、電子文書の内容・性格に応じて、アクセス権限を設定すること。（完、機）	○	○	○	○	○	○	○	○				○
○電子文書の保存、参照、更新、複写及び廃棄の日時並びに実施者を記録するログを取得し、保存すること。当該ログは、安全な場所及び媒体に一定期間保存すること。（完、機）	○	○	○	○	○	○	○	○	○	○		○
◎電子文書の更新履歴（削除した内容、追加入力した内容等）が確認できること。当該更新履歴は、安全な場所及び媒体に一定期間保存すること。（完）	○	○	○				○		○			
◎更新前の電子文書についても、必要に応じ一定期間保存すること。（完）	○	○	○									○
◎電子文書の盗難、漏えい等に備えるとともに、改ざん等を防止するため、必要に応じ電子文書を暗号化して保管すること。（完、機）							○	○	○			
◎ 必要に応じ改ざん検出機能を有する電子署名を電子文書に施して保管すること（完）	○	○	○	○	○	○	○	○	○	○	○	○
◎ システムタイマーの設定・変更等の作業履歴が確認できること。当該作業履歴は安全な場所及び媒体に一定期間保存すること。（完）	○	○										○
○電子文書のバックアップを定期的に行い、当該バックアップを適切に保管すること。（完）	○		○					○		○		○
○電子文書を記録した媒体及びそのバックアップについては、定期的に保管状況及びデータの内容が正常であるか否かの点検を行うこと。（完、機）	—											
○外部から入手した電子文書は、ウィルスチェック後に利用すること。（完）												○
○電子文書の出力に必要な電子計算機、プログラム、通信関係装置、ディスプレイ、プリンタ等を備え付け、いつでも必要な場合には電子文書をディスプレイの画面及び書面に出力することができるようにすること。（見）												
○電子文書保存・管理システムの保守、点検、改造等は計画的に行い、当該行為の期間中における電子文書の保護措置を講ずること。（完、機）	—											
○停電、誤切断等による電子文書の消失、破壊等を防止するため、無停電電源等の必要な措置を講ずること。（完）			○									
◎プログラムのバックアップを行い、適切に保存すること。（完、見）												

※　原本性確保対策要件の中で原本性保証製品の機能と関連性の低いと考える項目については、対象外とし「—」で表示

※（凡例）　完…完全性、機…機密性、見…見読性

４．５ 想定されているユーザーの環境と製品の機能で保護するべき情報

本研究会では、ベンダーが原本性保証製品を開発する段階で、実際にユーザーが製品を利用する環境をどのように想定しているのか、また、製品で保護すべき情報はどのような内容を想定しているか、という前提条件が重要と判断し、アンケートを行った。

ベンダーが想定しているユーザー側の利用環境については、製品を設置する建物や部屋は、入退室管理のある施錠されたサーバルーム等を前提としているものがほとんどであった。しかし一部の製品では、不特定多数の人が出入りする一般の部屋を想定している製品があった。また、ネットワーク接続を前提としている製品のほとんどは、ファイアウォールが設置されている環境での利用を想定していた。

そして、製品によって保護するべき情報については、原本データはもちろんのことであるが、文書への処理履歴情報(ログ)やアカウント情報（製品へのアクセス者の情報）、時刻情報等がその対象とされていた。

４．６ 原本性保証関連製品ベンダーの現状

今回調査した原本性保証関連の各製品に実装されている機能は、多岐にわたっている。電子文書の保存･管理よりもネットワーク上での文書の流通を安全に行うことを重視した製品もあれば、保存・管理は文書管理システム、認証は認証システムというように、各々の機能を分散したサブシステムの複合体としてサービスを提供する製品もある。また、ユーザー毎に電子文書の書換えや消去を不可にしてアクセスを細かく制御している製品や、電子文書に認証子を付与し、改ざんを検出する製品もある。認証の方法を１つとって見ても、OS の ID・パスワードの機能を利用している製品や、それに加えて原本性保証製品のアプリケーションを起動する際に、再度ログインのための ID 等が必要になる製品等、様々である。

ベンダー各社は、開発にあたって、「共通課題研究会最終報告書」や「制度見直し作業部会報告書」に記述されている原本性確保要件を参照している。ただし、実装する機能については、各社独自に製品で保護するべき情報やユーザーのシステム環境を想定し、様々な技術を組み合わせて特徴的な製品を開発していると考えられる。

また、ベンダー側は、原本性を保証するためにどこまでの機能を盛り込めばよいのかという明確な指標がないため、何らかの基準があるとよいと考えている。一方、ユーザーにおいても、どのような機能を盛り込んだ製品を導入すれば原本性が保証されるかという確証がなく、また判断材料となるものもないため、ベンダー同様に何らかの指標があるとよいと考えている。従って、「原本性を保証する製品とはどのようなものか」という基準があれば、ベンダーは製品開発がしやすくなり、ユーザーも製品の導入が容易になるのではないかと考えられる。そのような状況が結果的に、原本性保証製品の普及につながっていくと予想される。

５． 国内におけるＩＴセキュリティに関する評価認証制度の動き

・IT セキュリティ評価認証制度（ISO／IEC15408 に準拠）は、2001 年 4 月より運用が開始されるが、実際面での評価作業は 2001 年秋頃であると見られる。
・情報セキュリティマネジメントシステム適合性評価制度（ISO／IEC17799 に準拠）も、同様に 2001 年 4 月より運用開始が予定されており、2001 年 3 月現在、原案に対するパブリックコメントを募集している。

５．１ 原本性保証評価認証制度について

原本性保証に係わる評価認証制度を検討するにあたり、来年度から開始する予定となっている２つのセキュリティ関連の評価認証制度によって原本性保証製品の評価認証制度を代替できるのかどうかという点について検討を行った。電子文書の原本性は技術と運用を組み合わせることによって保証されるようにするものであり、製品の技術に関する評価認証制度としては、ISO／IEC15408 に準拠した情報セキュリティ評価基準のスキームに基づき製品の機能をセキュリティの視点から評価する制度が予定されており、運用に関する評価認証制度としては、ISO／IEC17799（BS7799）に準拠した情報マネジメント適合性基準によって、ユーザーの利用環境も含めて評価する制度が予定されている。

原本性保証に係わる評価認証制度を検討するにあたり、ISO／IEC15408 や ISO／IEC 17799 に基づく評価認証制度に対応することで原本性保証関連製品がユーザーやベンダーにとって導入しやすいものとなるのか、もしくはこれらの制度とは別に原本性保証分野において独自の制度を必要とするのかという検証を行った。

５．２ IT セキュリティ評価認証制度への取組み

５．２．１ ISO/IEC15408 の概要

1996 年 6 月、CC（Common Criteria）プロジェクトによる CCversion2 が ISO/IEC15408（以下、ISO15408）として採用され国際基準となった。また、2000 年 7 月、日本国内においても、JIS X 5070 として日本工業規格(JIS)に認定された。ISO15408 は、セキュリティの観点から IT 関連製品や情報処理システムが適切に設計され、その設計が正しくシステム等に実装されているかどうかを評価するための基準である。

基準の構成は、概要、機能要件、保証要件の 3 つのパートからなる。機能要件では、

ユーザーと開発者の双方が共通認識を持てるように、ユーザーのデータを保護するためのセキュリティ機能要件を示している。

保証要件では、開発者と評価者が製品やシステムのセキュリティを保証するための要件を述べている。これには PP（Protection Profile）、ST（Security Target）に対する保証要件と、TOE（Target of Evaluation）に対する保証要件がある。ISO15408 の中では、システムのセキュリティ機能及び管理者、ユーザー用のガイダンス文書を TOE、ユーザー側のセキュリティに関する要求仕様書を PP とし、PP に従って各製品で実装するベンダー側のセキュリティ機能の設計書を ST としている。

表５－１ ISO15408 で定めている機能要件及び保証要

機能要件	アクセス制御	
	識別と確認	
	ユーザデータ保護	
	セキュリティ機能保護	
	プライバシー	
	暗号利用	
	セキュリティ監査	
	可用性とリソース管理	
	高信頼性経路	
	通信／否認防止	
保証要件	評価保証クラス	構成管理
		ライフサイクルサポート
		開発と実装
		テスト
		ガイダンス文書
		配布と運用
		脆弱性評価
	保証維持クラス	保証維持

また、ISO15408 では、評価保証レベル（EAL：Evaluation Assurance Levels）を設け 7 段階に設定している。番号の大きい上位レベルは、下位レベルの要件を含んだ内容となっている。

５．２．２ IT セキュリティ評価認証制度

ISO15408 が国際的なセキュリティ評価基準として世界各国で導入が進む中で、日本においても、国際基準に準拠した形でセキュリティ基準を定めるべきとの声が高まり、

ISO15408 に則った「IT セキュリティ評価認証制度」の取組みが行われている。

国内における IT セキュリティ評価認証制度は、2001 年 4 月から制度開始されることになっている。制度の中心となる認証機関としては、独立行政法人製品技術監査機構（NITE）が設立される。この認証機関の NITE が実際の製品評価作業などを行う評価機関を認定する。NITE による評価機関の認定には、ISO／IEC17025 を採用し、かつ日本適合性認定協会(JAB)が行っている民間試験所の適合性評価制度等も参考に行われることになっている。この制度の運用にあたっては、認証・評価各々の機関が、IT セキュリティに関する知識と第三者評価ノウハウを兼ね備える必要があり、制度の開始に向けて研修等が行われている。

評価機関の候補としては、2000 年 2 月に設立された電子商取引安全技術研究組合（ECSEC）などが挙げられ、また、ISO9000/14000 関連の評価機関についても ISO15408 の評価機関として名乗りを挙げてくることが見込まれる。
制度開始当初は、評価機関によって評価する製品の専門分野が分かれる可能性があるが、将来的には 1 つの評価機関が様々な分野の製品の評価を行えることが望ましい。具体的な製品評価作業については 2001 年 9 月頃から開始されるが、それ以前も自主的な研究としてプロトタイプ開発した PP や ST の評価が進められることになっている。
評価機関の数については、海外において 1 国内で 3～5 機関程度であることから、日本においては 2～3 機関程度が適当だと考えられている。将来的には製品評価を希望するベンダー・製品の数やニーズによって決まってくるだろうとの見方である。

一方、政府の電子政府セキュリティ関連事業において製品研究などを行う際に同時に ST 開発が求められるような状況になっており、これらに呼応するように複数のベンダーが ST 開発に着手しているようである。本研究会の調査では、ベンダー側の意見として、ST 開発を行うには製品の開発工程時からドキュメントの整備や仕様の検討を行う必要があり、既に完成した製品についても開発工程を遡った見直し作業などが発生するため、多大なコストが発生する可能性があると指摘している。また、このコストは製品価格に上乗せするしかなく、製品価格の高騰を懸念する声も挙がっている。
評価認証にかかる料金やコストについては、本来評価機関の間の自由競争により評価料金が決定されるが、現時点で ST 評価料金は 1 製品評価あたり 1,000～2,000 万円程度と想定される。ただしベンダーにとっては評価料金の他に ST 開発費用がかかるので結果的に 1 製品当たり数千万円のコスト負担が発生すると予想される。PP の評価料金は、ST 評価のように実際の製品評価の工程を行わないため ST 評価料金よりは大分廉価になると予想されている。
現段階では、電子政府関連事業の一環として評価認証制度を推進している側面もあり、NITE が評価機関を認定する際や製品を認証する料金については当面無料になるら

しい。しかし NITE は独立行政法人であり、経営的に単独で成立する必要があるため、将来はこれらの料金が有料になる可能性はあると思われる。

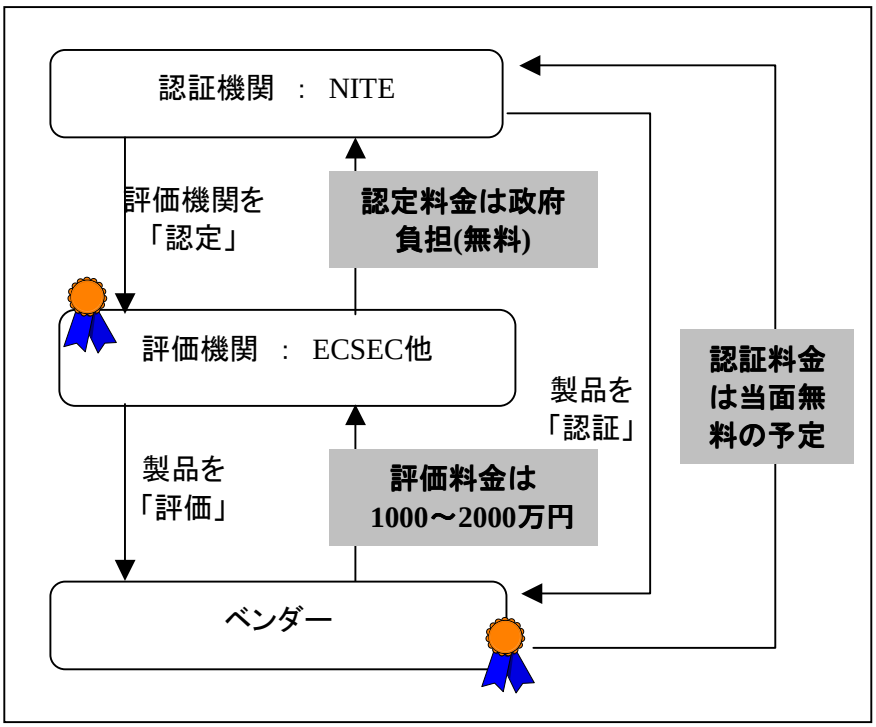

図５－１　IT セキュリティ評価認証制度のスキームと評価に係わる料金等

製品を評価するにあたり EAL レベルを設定する必要があるが、これについては EAL レベルが製品のセキュリティ強度を示すレベルであるなどと多少誤解されている面がある。また、電子政府で利用される製品の EAL レベルは 4 以上であることが望ましいとされる。現時点の国内の評価認証制度はまだ ISO15408 というものを普及していかなくてはならない段階にあり、EAL レベル 4 に対応できるよう評価機関側もベンダー側も準備を行っているが、現在直ちにレベル 4 の製品認定を国内で行うには難しい状況にあるとのことである。

日本では第三者評価という制度など馴染みがあまりなく、特にセキュリティ分野の第三者評価制度の取組みがあまり積極的にされてこなかったことなどから、今後は十分な準備とセキュリティ評価認証制度そのものの普及啓蒙についても積極的に行われて行くであろう。

５．３ 情報セキュリティマネジメントシステム適合性評価制度への取組み

５．３．１ ISO/IEC17799 の概要

ISO/IEC17799（以下、ISO17799）とは、2000 年 9 月に、BS7799-Part1 を元に認定されたものである。この BS7799 とは、情報処理システムのセキュリティ上のリスクに対応し、その管理対策の適合性を評価する基準である。また、管理対策の実施状況を検査するための基準を定め、客観的にセキュリティの方策を評価できるようにしている。また、情報処理システムが BS7799 に準拠したものであることを認証する仕組みを規定している。BS7799 は、1995 年にイギリス規格として情報セキュリティ管理対策としてまとめられたものであり、Part1「情報セキュリティ管理実施基準」と Part2「情報セキュリティマネジメントシステム仕様」から構成され、イギリス本国のみならず、スウェーデン、オランダ、デンマーク、オーストラリア等で、セキュリティ管理対策の基準として導入されている。

Part1 では、情報セキュリティ管理項目の内容を規定している。管理項目として、以下の 10 分野が挙げられている

①セキュリティポリシー
②セキュリティ組織
③資産の識別と管理
④人に対するセキュリティ
⑤環境や物理面のセキュリティ
⑥通信と運用の管理
⑦システムの開発と保守
⑧アクセス管理
⑨業務の継続のための管理
⑩セキュリティ関連の法律や規則への準拠

Part2 では、認証を受ける際に準ずるべき事項が説明されており、情報セキュリティマネジメントシステム（ISMS）の確立、実行及び文書化についての要求事項等が明記されている。

５．３．２ 情報セキュリティマネジメントシステム適合性評価制度

国内においては、ISO17799 や BS7799 に相当するものとして、情報セキュリティマネジメントシステム適合性評価制度が来年度から開始されることになっている。これは、情報処理システム安全対策実施事業所認定制度(安対制度)の廃止に伴い設立されるもので、情報セキュリティマネジメントシステム(ISMS)適合性評価制度の原案が、(財)日本情報処理開発協会（JIPDEC）より公開されている。国際的な情報セキュリティの管理対策に関する標準化動向を踏まえ、従前の安対制度における設備等の物理的な対策に加えて、運用・セキュリティマネジメントの項目も含めた評価制度となる。

評価制度のスキームとしては、以下のとおりである。制度全体の運用・維持管理には JIPDEC があたり、審査機関を指定し、登録管理を行う。また、指定審査機関による第三者評価希望事業者の審査結果に基づいて事業者の登録公表等を行う。

指定審査機関は、第三者評価希望事業者の申請を受け付け、審査を実施し、審査結果により事業者を認証する。

第三者評価希望事業者は、申請対象システムとなる ISMS を確立し、評価基準に従って審査を受け、結果に基づいて認証登録を受ける。認証を受けた事業者は、制度のマークを付けることができる。

本制度が対象とする事業者の範囲は、制度運用の初期段階においては、情報処理サービス事業者とされているが、他の事業分野への適用の拡大については、今後の検討課題とされている。ISMS ガイドライン（ドラフト版）については、従前の安対制度の項目をある程度引き継いだ上で、BS7799-Part2 の項目も追加し、現時点において必要最小限と思われるセキュリティマネジメント事項が設定されている。このガイドラインは、パイロット審査を通じて、ステップアップしていく予定とされている。

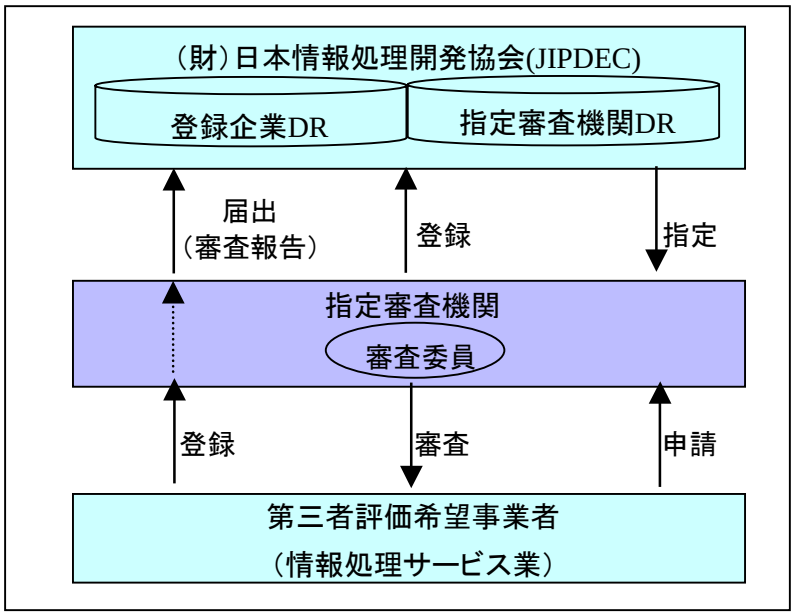

図５－２　ISMS 適合性評価制度のスキーム

５．４ ISO15408 及び ISO17799 を組み合わせた制度の検討

ISO15408 の IT セキュリティ評価認証制度は、制度そのものがまだ本格的な運用開始前であり、現状においてはユーザーが PP を作成し、ベンダーがそれに準拠した ST を作成するための素地を作っていく段階にあろう。本研究会の中では、昨年度も開発していた原本性保証製品の PP をブラッシュアップする検討の過程で、IC カードなど他のセキュリティ関連製品がそうであるように、装置自体（ハードウェア）、ファイル管理やアクセス制御（ソフトウェア）等の機能毎に分割した PP を作成することが望ましく、このことが今後ベンダー各社が行う ST 及び製品開発を容易するとの意見があがった。

原本性保証の分野の製品においても、この制度に則った製品評価を行っていくことは必要であるが、その前に、原本性保証製品に求められる機能要件を整理し、明確にしていくことが必要な段階にある。

また、情報セキュリティマネジメントシステム適合性評価制度は、審査・評価機関の体制が整うまでに、まだ少し時間を要する。また、制度運用開始の初期段階では、情報処理サービス事業者にのみ適用されるため、例えば今回ターゲットにしている行政機関等への適用はもう少し先のことになると考えられる。

いずれにしても、ISO15408 と ISO17799 の双方のスキームを組み合わせ、製品の技術要件と、ユーザーの環境や運用的な要件の両方を含めた評価認証制度に対応していくことは、原本性保証の評価認証制度のあり方を考える上で、対応すべき方法の 1 つである。

６． 原本性保証を取り巻く現況のまとめ

・「３．原本性保証を取り巻くユーザー（行政機関）の現状」、「４．原本性保証に関するベンダーの動向」、「５．国内における IT セキュリティに関する評価認証制度の動き」を踏まえ原本性保証を取り巻く現況のまとめと、研究会で検討・整理した結果について紹介していく。
・「制度見直し作業部会報告書」と「共通課題研究会最終報告書」という原本性保証を検討する際に対象となる 2 種類の報告書が主に参考とした文書であるが、民間ユーザ向けと行政機関向けという違いがあるものの、対策など要件に若干の違いがある。
・ベンダー側もこれらの報告書の定義の元に製品開発を行っているが、対策要件に対する技術の実現方法は解釈に各社の違いがあり、結果として様々な原本性保証関連機能が存在している。
・セキュリティ対策と原本性保証対策との切り分けも明確ではなく、原本性保証対策には報告書類によって若干の相違があることなどから、原本性保証対策要件および製品に求められる機能といった点では様々な解釈が存在しているのも事実である。
・ユーザー、ベンダー双方で捉えている解釈をできるだけ統一化するとともに、製品選択などを容易にするため、何らかの評価基準を定め、製品評価を行うことが望まれる。
・本研究会では、これらの現状を踏まえ、原本性保証システムガイドラインや製品チェックリストを策定することとなった。

６．１ ユーザー（行政機関）の現状

行政機関・行政文書を対象とした原本性確保要件は「インターネットによる行政手続の実現のために－共通課題研究会最終報告書」の中で規定され、「制度見直し作業部会報告書」では民間が保存するべき文書の原本性保証について規定されている。これらの 2 種類の内容は、電子文書の原本性保証の要件を示しているという点では同じものであるが、対策要件について若干の解釈の違いがある。また、行政機関ではセキュリティポリシーを策定するなどセキュリティという視点での各種検討が進められる中で、セキュリティの対策要件と原本性保証の対策要件が非常に類似する点が多いことなどから、両者のはっきりとした違いを判断することが難しい状況などもあるようである。

本来はユーザーである行政機関の側から、原本性保証製品に求める機能を明確にベンダー側に提示する方が、ユーザーニーズに基づいた製品の機能を明確にし製品開発をしやすくするため望ましいと考えられる。原本性保証の対策要件や技術で実現される機能がまだ明確になっていない現状では、ユーザー側からこれらを提示することは難しいと思われるが、一方で、原本性保証対策への関心は高く、製品を導入する必要も迫ってき

ているため、製品の機能に関して分かりやすく説明を受けられるような基準を行政機関も望んでいる。また、その際に安心して製品を導入できるようにするため、何らかの評価を受けた製品というものがあればよく、その事から評価認証制度への期待も大きいであろう。

６．２ ベンダーの現状

ベンダーが提供する製品は、原本性保証の対策要件を満たすべく各社独自の解釈に基づく技術によって各種機能が実装されている。各社の製品機能の紹介では「原本性保証機能」とされているものでも、具体的に実現されいている機能は多岐にわたっている。原本性保証製品を利用する環境や、製品が保護対象としている情報等は、おおよそ類似しており、例えば原本性保証製品をネットワークに接続する際には必ずそのネットワークがファイアウォールで保護されている点などは各製品とも共通である。また、各製品の機能はセキュリティ強度を非常に高く設定しているものもあれば、ユーザーの利便性を考慮し強度よりも使いやすさを優先しているものもある。これらの状況が、ユーザーがどの製品を選択すべきであるか見定めることを難しくしている面がある。

６．３ 評価認証制度の状況

原本性保証の分野の製品においても、ISO15408 や ISO17799 に基づく評価認証制度に則った製品評価を行っていくことは必要であるが、その前に、原本性保証製品に求められる機能要件を整理し明確にすることが必要な段階にある。これらの評価認証制度は評価開始までにもうしばらくの時間がかかるため、その前に機能要件を整理しておくべきであろう。

近い将来に評価認証制度にベンダーが対応していくことを仮定した場合、既に ISO15408 を意識し ST 開発等に取り組んでいるベンダーもあるが、独自の考えに基づく技術によって機能を搭載した製品や ST 開発を行っており、本来 PP を参照してこれらを開発する方が望ましいことを考えると、今後はやはり原本性保証製品として搭載される技術要件を統一的に明示するためにも PP が必要になってくる。ベンダー側の意見には、ISO15408 のようなセキュリティ評価基準に則って製品評価を実施することは、製品の設計・開発工程においても相当の準備が必要であり、それらの負担を軽減するためにも PP は有用なものとなろう。

また、PP だけでなく、原本性保証製品の機能を客観的に評価し、何らかの形でユーザー側に示すことができる指標の整備が必要であるという認識は、どのベンダーからも聞かれた。

ユーザー側では、評価認証制度等が実施されることにより製品の選択がしやすくなるであろうという期待を持っている反面、評価認証制度に係わるコストが原本性保証製品等に加算され、結果的に製品価格が高価になることは好ましくないとの意見があった。

６．４ 原本性保証のガイドライン／チェックリストの必要性

原本性保証を取り巻く現状を見ると、評価認証制度を整備することはいずれ何らかの形で必要になるであろうが、その前に、原本性保証製品に求められる機能要件を整理し明確にすることが必要な段階にあることから、ユーザーが理解しやすく、製品導入の一助となるような原本性保証システムガイドライン及び原本性保証電子保存機能チェックリストを作成することとした。また、ベンダーが、これらに沿って製品機能が実装されていることをユーザーに提示することにより、ユーザーの製品判断を助けるだろうとの意見もあった。具体的には製品パンフレットに原本性保証システムガイドラインや原本性保証電子保存機能チェックリストに沿って機能が実現されていることを掲載することなどである。

本研究会で検討を重ねた結果、ガイドラインでは原本性保証の対策要件として必須であるものを明確にし、チェックリストはベンダー各社の製品機能から、できるだけ共通的な機能を見出し、各社の製品に共通的に求められる機能のチェックリストとなるようにしていく方向で意見がまとまった。

６．５ IT セキュリティと原本性保証の定義の関連性

原本性保証を取り巻くユーザーやベンダーの現状、制度的な取組み状況を見た時、共通的な問題として、IT セキュリティと原本性保証の対策要件が非常に重なる部分が多いことや、原本性保証対策要件の解釈が必ずしも同一でなかったりすることが、結果的に原本性保証製品の普及を阻害する要因の１つであるとも考えられる。

この状況を踏まえ参考までに、原本性保証に必要となる本質的な要件を見出すために、IT セキュリティと原本性保証の定義について、国内及び国外の IT セキュリティ、原本性保証関連の各種規定類から整理を試みた。

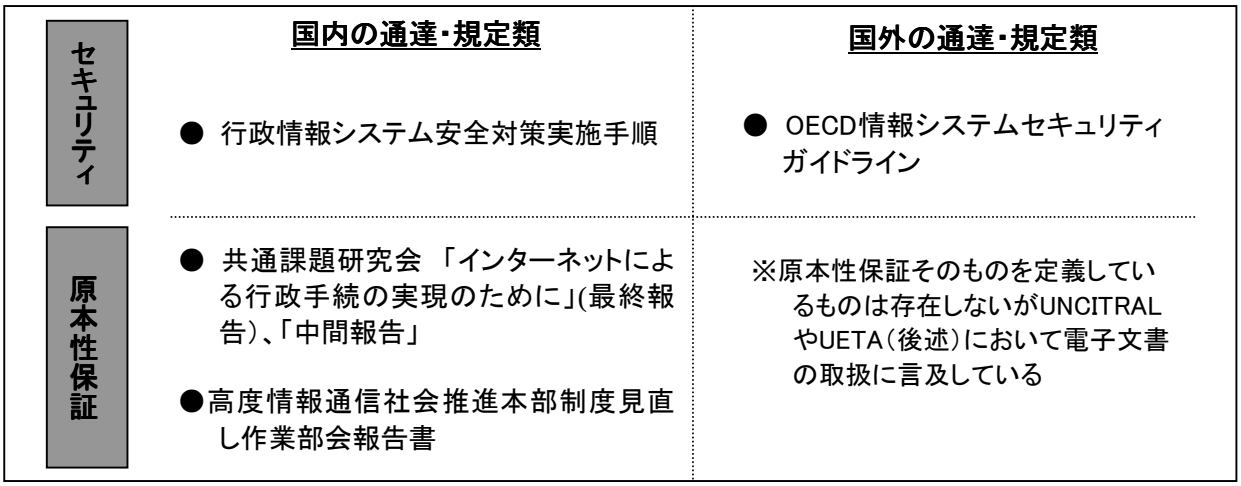

図６－１　国内外の IT セキュリティ及び原本性保証に関する通達・規定類

（１） IT セキュリティと原本性保証の整理

「行政情報システム安全対策手順」は、国内の IT セキュリティ規定の１つであり、国の行政機関において、情報システムの安全管理目標を設定する際のレベルを示すものとして利用されている。この手順の中では、データの安全性やシステムの運用上の信頼性を確保するために、正確性・機密性・継続性の視点に基づいてシステムの設計や評価を行うことが必要であると述べられている。

また、国外の規定の例として、1992 年に採択された OECD 情報システムセキュリティガイドラインでは、情報システム利用者がシステムの障害等によって不利益を受けることを防ぐために、情報システムの可用性・機密性・保全性を維持することの重要性をうたっている。

これらの規定類と、前述の原本性保証関連の報告書等を整理してみたところ、IT セキュリティの確保と原本性保証は、その概念・捉え方の上で非常に多くの重なりがある

といえる。対策要件においても両者は重複する部分が多く、明確な違いを判断することが難しい。

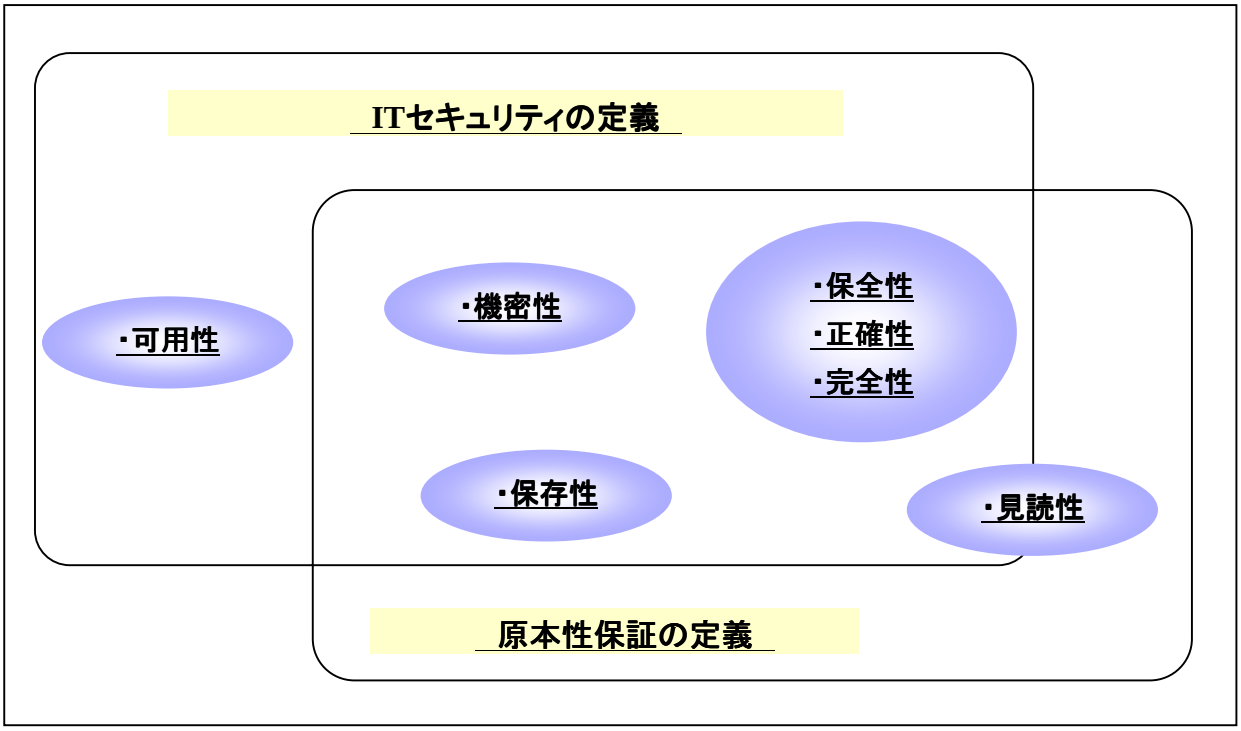

図６－２　IT セキュリティと原本性保証の関連性のイメージ図

（２） 原本性保証の定義の整理

本研究会では、原本性保証の定義を「完全性、見読性、機密性を保つこと」ととして検討を進めてきた。

対策要件に着目し、「制度見直し作業部会報告書」と「共通課題研究会最終報告書」を再度整理してみると、それぞれの報告書は対象とする文書や対策要件に見方の若干の違いはあるが、共通的な内容が多く、完全性の対策要件は、真正性・保存性の主要な対策要件を含んでいると考えられる。また、機密性の対策要件も、真正性・保存性の要件に重複する部分が多い。

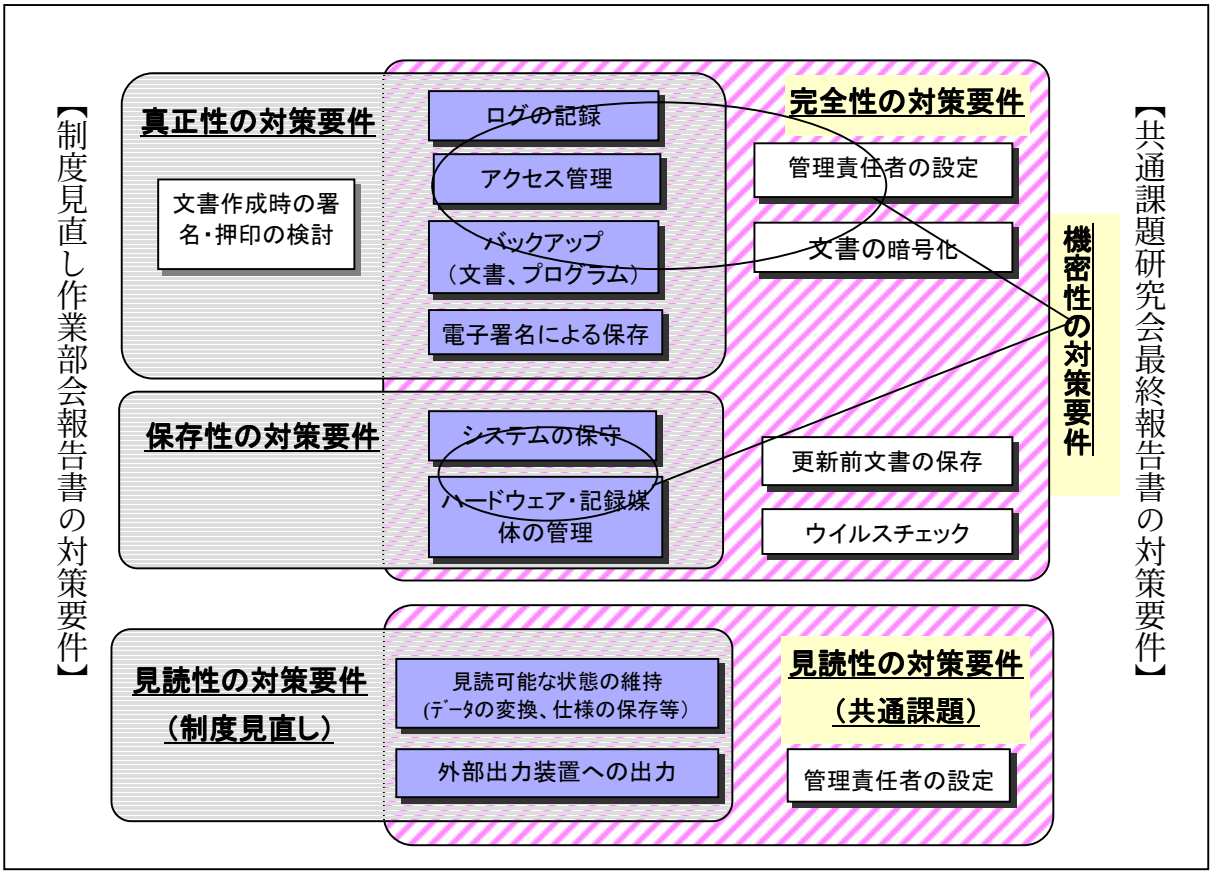

図６－３　制度見直し作業部会報告書と共通課題研究会報告書の対策要件関連イメージ図

７． 原本性保証における必須対策要件

・本研究会では、原本性保証製品やシステムを利用する行政機関及び民間における原本性保証の考え方、製品ベンダーの考え方や動向等を踏まえつつ、原本性を保証する際に必須となる機能として①改ざん検出と、②改ざん防止の大きく二つを提示した。
・「改ざん検出」、「改ざん防止」機能では、その機能によって文書の保存や作成の当事者であっても不正が行えない仕組みとなっていることが望ましい。

７．１ 改ざん対策の方法

電子文書が原本であることを保証することは、原本として一度作成・保存された文書が改ざんされていないことが証明されなくてはならない。原本として確定した文書が、保存後に一度でも改ざんされた形跡がある場合は「原本」とすることができない。

原本性を阻害する脅威としては、改ざんだけでなく、書換え、劣化、盗難、漏えい等が挙げられるが、中でも改ざんは最も重要となる対策を講じなくてはならない脅威である。改ざんを広く捉えるならば、電子文書が正しい状態を保てないことであるが、改ざんとは不正・故意によるものだけでなく、過失による書換えやアクセス権限者による正当な文書変更も含む場合もあると考えられる。

本研究会では、改ざん対策をセキュリティ分野で利用される対策方針の分類の考え方に基づき「抑止」「予防」「検出」「回復」にあてはめて整理した。改ざん対策にはこの４つの概念を大きく２つに分け、抑止・予防・回復を「改ざん防止」（原本性を阻害する要因をできるだけ排除すること）、検出を「改ざんの検出」（原本性を阻害されたことを後に判別できるようにしておくこと）とした（図７－１参照）。

電子文書の改ざんを 100%防止する技術を実現することは難しいものではあるが、改ざんが行われたことを検知する機能（要件）を持つことで、原本としての電子文書の証拠能力が増すことができるため、大きく２つの「改ざん防止」と「改ざん検出」の内、「改ざんの検出」がより重要であり、技術的な対策が講じられるべきとした。

司法の場で裁判官の心証形成を高めるためには、不正な第三者による脅威（犯罪）はもちろんのこと、電子文書の作成者及び管理者を含めた当事者の改ざん防止対策を行う必要があるだろう。その理由としては、文書の改ざんを行うことで、より大きな利益を得るのは、当該組織等と関係のない第三者よりも文書の作成や保存の当事者の可能性が高いと考えられるからである。

この点では、原本を保存する当事者でさえも関与できない改ざん防止機能（技術）を組み込む、また、当事者以外の信頼のおける第三者が電子文書が改ざんされていないことを証明することにより、原本性保証の機能を果たすことになると考えられる。

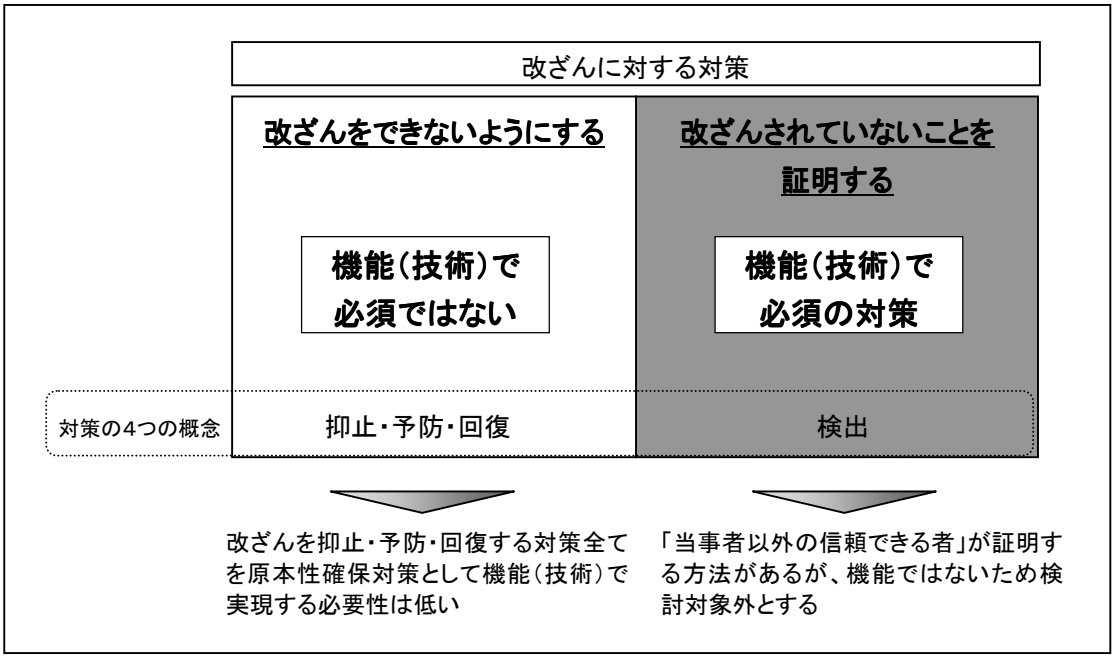

図７－１　改ざん対策のイメージ図

７．２　改ざん検出

７．２．１ 改ざん検知

電子文書に証拠能力があることを証明する場合、「改ざんされたのか、されていないのか」が重要な部分となるであろう。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より強く行えると考えられる。これは、改ざんが検知されなかったという事実があるならば、逆説的に電子文書が改ざんされずに原本のまま保存されていたことを証明できるものと捉えられる。なお、改ざん検知は、原本性保証の対策要件の中で最も重要となる機能でありかつ技術の 1 つであり、原本性保証システムと呼ぶからには必ず搭載されていなければならない機能であると考えられる。

改ざん検知機能とは、電子文書の情報が 1bit でも変化したことを検知する機能のことであり、電子文書のあらゆる変化について、その操作が行われたのはいつであるか特定できるようにする機能や、電子文書のどの原本が改ざんされたのかを一意に特定する機能等も同時に求められる。実際に検知するための手段としては、電子文書の保存等の処理記録の保存、電子文書と各種履歴への認証子の付与等が考えられる。

本研究会で行った調査では、調査対象の製品には何らかの改ざん検知機能が搭載されていた。具体的に各ベンダーが搭載する改ざん検知機能には、電子文書等にハッシ

ュ値等の認証子を付与し、改ざんを検知するなどがある。その他に、ハッシュ値等の認証子を信頼できる第三者に預け、当事者以外の第三者によって改ざん検知・非改ざんの証明を行うなどの機能もある。

７．２．２ 時点の特定

改ざんを検出するには、履歴（保存・変更・参照等を含む）情報が必要とされる。それは、改ざんを行った者の追跡を行ったり、どの時点で文書が改ざんされたのか特定できるようにするためである。

その履歴情報の内容の重要な一つの要素として時点の特定ができることが求められる。電子文書（ファイル）が変更された時点（時刻）をログ等に記録し、特定できるようにすることである。時刻情報にシステム内部のタイマーを利用する場合は、時刻情報自体を変更した時にその操作の履歴を記録する機能や、時刻情報へのアクセスを監視し、不正な操作が行われないようにする機能等も同時に求められる。

時点の特定を行う際、電子文書が確定された順序性だけを保てればよいなど限られたシステムの範囲の中などにおける相対時刻が判別できればよいという考えがある一方で、世界標準時などを保証する第三者機関が発行する正確な時刻（絶対時刻）を特定できる必要があるのではないかという考えもあるが、研究会ではどちらが必要かという結論は下せず今後も検討が必要である。

本研究会で行った調査によると、現在、各ベンダーが製品に搭載している時点の特定機能には、電子文書の保存等の時点を特定するために製品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・認証子等の時刻に付与したり、システム内の時刻証明ではなく、信頼できる第三者等が発行する時刻情報を用いて、原本データや履歴情報・認証子等の時刻を付与する方法が挙げられる。

７．３　改ざんの防止

改ざんという脅威に対して、抑止・予防・回復の対策があり、その対策には、製品用途などに合わせ様々な技術的機能が存在する。現在考えられるこれらの全て機能を原本性保証システムに搭載することは現実的ではなく、このいずれかあるいは複数の技術を組み合わせることによって、改ざんを防止することが必要である。また、改ざん防止は、ユーザーの利用環境などに合わせ、製品機能によって対策を講じるとともに、適切なシステム運用対策を行うこととのバランスを取りながら行うことが必要である。

なお、改ざん防止機能としては以下のようなものなどが挙げられる。

① 書換え・消失不可機能
　全ての者（当事者を含む）が上書き・消去できないようにする機能
② アクセス者の識別・認証機能
　アクセス者の識別・認証を行う機能
③ アクセス制御機能
　電子文書等の保存は、権限者に限定する機能
④ バックアップ機能
　電子文書をバックアップし、必要に応じて元に戻せるようにする機能
⑤ ネットワーク保護機能
　通信時もしくは保存時に文書の暗号化を行う機能
⑥ 複製制御機能
　原本と複製（謄本）が区別できるようにする機能

本研究会で行った調査によると、各ベンダーが製品に搭載する改ざん防止機能には、故意・過失に関係なく全てのユーザーによる電子文書の上書き・消去を不可とする機能や、特定の権限を与えられた権限者のみが保存・更新・削除などの操作を行うことができるようにした機能がある。また、ID・パスワードだけでなく、指紋認証を利用してアクセス制御を行う製品もあれば、原本性保証保存システムの筐体に耐タンパー性を持たせ、かつ鍵を掛けるなどして不正アクセスを防止した製品もある。

８． 原本性保証システムガイドラインと原本性保証電子保存機能チェックリスト

・原本性保証システムガイドラインは、電子文書が紙文書と同等に扱われるための方策を、情報システムの観点から提示するものである。
・ガイドラインの対象となるのは、電子文書によって原本を保管しようとする組織や機関、及び、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。
・原本性保証電子保存機能チェックリストは、ユーザーが当該システムを導入、運用する際に逐一チェックしながら製品をユーザ自身が評価できるようになっている。

８．１ 原本性保証システムガイドライン

８．１．１ 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、ガイドライン）は、電子文書が紙文書と同等に扱われるための方策について、情報システムの観点から提示するものである。

本ガイドラインは、電子文書によって原本を保管しようとする組織や機関、及び、それらにシステムを提供する情報システムベンダーを対象とし、原本性保証システムの必須機能と考えられる技術要件を明確にすることを目的に作成されている。

情報システムが原本性を保証することは最終的には困難であるが、司法の場において、裁判官の心証形成を高めるために、様々な対策を講じておくことが必要である。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がより強いものになると考える。

８．１．２ ガイドラインの構成

本ガイドラインは、ユーザー、ベンダー双方が利用することを想定しており、ユーザーに対しては、原本性保証製品を導入する際の指標となるものであり、ベンダー対しては、原本性保証をシステムによって実現するための基本的な考え方を提示するものである。現在、原本性保証に係わるシステムには様々なタイプがあるが、「原本性保証電子保存システム」を中心に、当該システムに求められる要件と技術例を挙げている。

８．１．３ ガイドラインの内容

※　付録「原本性保証システムガイドライン」を参照のこと

８．２ 原本性保証電子保存機能チェックリスト

８．２．１ チェックリストの目的

原本性保証電子保存機能チェックリスト（以下、チェックリスト）は、対象となる製品において、原本性保証の電子保存に必要なセキュリティ機能が備わっているかどうかという点について、ユーザー自身が確認できることを目的として作成した。ユーザーが本チェックリストを製品の導入・購入前に利用することで、不足している内容がある場合には、別の製品で補完するか、製品への機能を追加するなどの対策を講じるなど対応が可能になるものである。

８．２．２ チェックリストの使用方法

本チェックリストの使用方法としては、各項目について具体例を参考に、対象となる製品が該当する機能を備えているかどうかを確認する。最終的に、全ての項目にチェックが付くと、対象製品は、原本性を保証するための最低限のセキュリティ機能を備えていることになる。

８．２．３ チェックリストの前提条件と保護対象となる資産について

本チェックリストは、原本性保証電子保存システム（ソフトウエア部）Protection Profile」に対応しているため、チェックリストを意味あるものにするためには、PP と同じ前提条件を満たしていることが必要になる。その前提条件の内容については PP とチェックリストそれぞれを参照していただきたい。

また、保護対象となる資産も PP と同様の設定であるが、ユーザーのニーズに応じて資産の範囲を広げる場合には、別途技術的・運用的対策が必要であり、詳細については、「原本性保証システムガイドライン」を参照することが望ましい。

８．２．４ チェックリストの内容

※　付録「原本性保証電子保存機能チェックリスト」を参照のこと

９． 原本性保証電子保存システム（ソフトウェア部）Protection Profile

・ベンダー側が各社独自のアプローチで実装する製品機能を定めている現状を踏まえ、本研究会において検討されてきた、製品に実装するべき技術要件のうち、最低限必要となる要件を ISO/IEC15408 のセキュリティ評価基準に則った要求仕様書として作成した。

９．１ Protection Profile の目的

この Protection Profile(プロテクションプロファイル：以下、PP)は、行政文書の種類や形態について把握した上で、電子文書のセキュリティレベルや保存形態を鑑みた原本性保証電子保存システムの想定される脅威や、脅威に対する対策方針、方針を実行するためのセキュリティ技術要件について、ISO／IEC15408 に準拠した記述方式でセキュリティ仕様として策定した。

９．２ Protection Profile の方針

今回作成した PP は、昨年度の成果物である「原本性保証電子保存システム Protection Profile」をソフトウェア部、ハードウェア部等に分割し、今年度は原本性保証のコアとなるソフトウェア部のブラッシュアップを行ったものである。

９．３ 本研究会での検討経緯

本研究会においては、前述の PP の作成方針を提示し、検討を行った。今回の PP 作成にあたって、原本性保証に係わる製品のベンダーに製品を利用する際に想定した環境や製品が保護対象とする情報資産についてアンケートを実施し、その結果から共通的な脅威や対策方針の洗い出しを行い、原本性保証製品のコアとなるセキュリティ対策要件を構成することを提案した。

PP のコンセプトを明確にするために、前提条件となる物理的環境を想定し、守るべき資産を「原本データ」、「時刻関連情報」とし、また、原本データへの不正操作と時刻関連情報への不正操作に関する技術的な対策案を提示した。具体的には、原本データ及び時刻関連情報へのアクセスの制御、原本データ及び時刻関連情報の処理履歴の記録、改ざんの検知、時刻関連情報の取得機能の保護、上書き不可の各機能を提示し、検討を行った。

９．４ プロテクションプロファイルの内容

※　付録　「原本性保証電子保存システム（ソフトウェア部）Protection Profile」を参照のこと

１０． 原本性保証の普及啓蒙に向けて

・本研究会ではガイドラインやチェックリストを策定したことが一つの大きな成果であったが、今後さらに原本性保証および関連製品を普及していくための方策として、中長期的な内容も含め複数の方策を提示した。
・ガイドラインやチェックリストの普及策としては、原本性保証製品のパンフレット等にガイドラインに掲載されている機能が実装されていることを記載してもらうことなども策の一つである。
・製品の PP については、製品のハードウェア PP、媒体への保存に関する PP 等、機能毎に作成し、登録作業を進めていくことが必要である。
・ガイドラインやチェックリストの普及を促進するために、独自の評価認証制度によってガイドラインやチェックリストを何らかの機関が認定するといったことを検討していく必要がある。
・これら上記 3 つの方策における課題の解決や、さらなる原本性保証関連の技術的な研究を目的とした中立的な組織の設立を計画すること検討した。
・また、将来的には電子文書の証拠能力を確保するための対策を講じることの重要性を明文化した「モデル法」の制定も視野に入れるべきとの検討を行った。

１０．１ 原本性保証関連製品の普及へ向けて

原本性保証のニーズは、今後行政機関などに限らず紙文書から電子文書へ移行を考えるあらゆる業種・業界の組織において大きくなっていくはずである。例えば、民間企業でも電子商取引等を行う場合、契約書等の電子文書の保存・管理をするときに、原本性の保証が必要になってくることなどがある。

本研究会において作成された「原本性保証システムガイドライン」、「原本性保証保存機能チェックリスト」及び「原本性保証電子保存システム(ソフトウェア部)Protection Profile」を公開し、原本性保証の機能要件の本研究会での考え方を広め、製品の普及を進めていくことが必要である。

ガイドライン等を普及していくだけでなく、広く原本性保証対策の重要性を啓蒙していくことや、製品の普及のために、具体的に 5 つの方策を提案した。

１０．２ 今後の具体的な方策

１０．２．１ ガイドライン・チェックリストの普及・浸透化

ユーザー自身が製品の機能を確認し、導入することができるように、ガイドライン及びチェックリスト、PP を公開することが 1 つの方法として挙げられ、これはぜひともやらなくてはならないことである。

今回作成したガイドラインは、ベンダー各社からインタビューした結果をベースとした原本性保証の機能要件の事例である。さらに詳細な技術レベルや製品の必須機能要件に関して、ベンダー側のコンセンサスを得る必要もあり、今後継続的にベンダーの開発担当者達が連携し、密接なコミュニケーションをとりつつ、ガイドラインなどのリファインを行っていくことが望ましいと考える。

また、ガイドラインやチェックリストを公開するだけでなく、ベンダー各社の製品のパンフレット等に、ガイドラインに準拠していることやチェックリストの機能を満たした製品である旨を記載してもらうことがユーザー側の安心感を生み、積極的な製品の導入につながっていくと思われる。

中央省庁については、「e-Japan 重点計画（案）」の中で、2001 年度中に全府省が電子情報の保存・管理に関する規程等を定めることが盛り込まれており、この中に、原本性保証の技術要件を反映してもらえれば、これからの原本性保証製品の普及に大きなインパクトを与えることができると考えられる。

１０．２．２ ISO／IEC15408 情報セキュリティ評価基準への適用

今回作成した PP は、ユーザーの利用環境等の前提条件を考慮し、原本性保証システムといった中でも保存に特化したシステムの機能に絞った内容になっている。PP の作成にあたっては対象となるシステムを特定する必要があるためと、原本性保証の機能をより明確にするために一般的なシステム利用環境を前提条件とし製品の物理的な強度に関するハードウェア部は除き、ソフトウェア部をその対象としたなどの理由からである。

原本性保証システムは電子文書の保存だけでなく、電子文書の流通等の場面において利用することに重きを置いたシステムもあることから、原本性保証流通やその他関連するシステムの PP も順次作成していくべきであると考える。また、ソフトウェア部に限らず、ハードウェア部の PP や、原本性保証保存に必要な様々な機能要件を含む、ハードウェア部とソフトウェア部の複合的な PP の作成も今後は必要になってくるであろう。

これら各種の PP のリファイン及び追加作成にあたっては、ベンダー各社の製品開発

担当者による中立的な組織を設立し、原本性保証に必要となる要件をより技術的に詳細に検討することも考えられる。

また、各ベンダーで製品や ST を開発する際に、PP と近い設計書のようなものや PP そのものを作成することも予想される。その作成された各社独自の製品特徴を反映した PP を公開し、ISO15408 のスキームに従い PP が数多く登録されるようになると、原本性保証製品の認知度も上がってくると考えられる。中立的な組織の役割としては、公開された PP が、ガイドラインやチェックリストの要件に即しているかどうかを判断し、各ユーザーの環境に適応した PP を推奨していくといった内容が想定される。

１０．２．３ 原本性保証評価認証制度の設立に向けて

中長期的な視点に立った場合、ISO15408 に基づくセキュリティ評価認証制度とは別に、独自スキームによる原本性保証評価認証制度の確立も必要になってくると考えられる。

具体的な独自制度の活動内容としては、評価認証制度に則って認証された製品に、原本性保証要件に適合した機能を実装しているシステムであることを認定する何らかのマークを付与するなどがある。

ただし、現時点ではまだ課題が多く残され、さらなる検討が必要である。1 つには、製品に対してマークを付与するために、どのレベルまで原本性保証の技術要件を求めるのかという点である。例えばユーザーは原本性保証製品を安心して導入するために「この製品を導入すれば原本性が保証される」ということをマーク付き製品に求めるが、どのレベルの技術を搭載しても製品が原本性を保証することは難しい。どのような製品であればマークを付与することができるのかということは、技術動向を考慮し、継続的に、適宜見直しを計っていかなければならない。またマークを付与することで、結果的に認証機関がどこまで製品に責任を負うかという点についても、製品やその技術・機能が原本性を保証できない以上、同時に充分検討する必要がある。研究会では、電子文書の改ざんなどによって発生するであろう損害賠償責任などに対して、ベンダーや制度の運営機関の責任範囲を明確にする必要があるかもしれないといった意見や、将来的に、電子文書の改ざんによるリスクの算定が可能であるならば、ユーザー・ベンダー間で係争が発生した場合に備え、拠出金を募り保険機構を整備し、仲裁機関としての役割を持たせるということも考えられるかもしれないという意見があった。

１０．２．４ 原本性保証製品普及のためのベンダー協議会の発足

原本性保証システム開発ベンダー各社、行政機関、ユーザー団体等から構成される組織として「原本性保証システム普及協議会」(案)を発足させることが、今後の普及方策の土台となるものとして重要であると考えられる。

予想される主な活動内容は、技術的な研究として、原本性保証要件、仕様書の策定、長期保存に係わる諸問題の研究、ガイドライン及びチェックリストのリファイン、PP 登録支援、ST 開発指導等が挙げられる。また、制度面の研究として、国外の原本性保証関連の法制度の調査､原本性保証認定マーク制度の導入検討､制度上の諸問題の検討、独自の評価認証制度の検討等が考えられる。そして、製品の利用促進に関連し、普及啓蒙のための広報活動や、行政機関への提言活動、電子政府・医療・金融等のユーザー分野別のサブディスカッショングループによる利用促進の検討等が想定される。

この協議会は、技術的な研究、制度面の研究、利用促進の検討といった 3 つの方策を円滑に進め､各々の方策の中で生じるであろう諸問題の解決のための機関としての役割を担うものと考えられる。ただし、協議会の運営主体や運営方法、活動のための資金調達、団体としての法人格の取得等、発足にあたっては、検討すべき項目が多々あり、母体となる団体もしくはベンダーの協力が必要不可欠になると考えられる。

１０．２．５ 国内におけるモデル法の確立

UNCITRAL による電子商取引モデル法や電子トランザクション共通法(UETA)等、国際的にも電子文書の証拠能力を確保する方策を定めるモデル法が整備されている中で、国内においても、同様に明文化することにより、原本性保証対策の重要性を醸成することも重要であると考えられる。

国内におけるモデル法の成立に向けては､国内の電子情報を取り扱う諸法令の動向を合わせて考慮し、充分検討することが重要である。

〔参考〕

～国外の電子文書についての規定～

（１） 電子商取引モデル法

国連の国際商取引法委員会(UNCITRAL)は､1996 年に各国が電子商取引に関する国内立法にあたってのモデル法として､各国の既存の法的な障害を除去することを目的に「電子商取引モデル法（Uncitral Model Law on Electronic Commerce)」を採択した。

このモデル法は、企業間の取引に関するものであるが、法令内で適用される「データメッセージ」の概念は広く、EDI、電子メール、電報、テレックス、ファクシミリによる情報の送受信等に及んでいる。

また、第 1 部第 2 章の 8 条には原本性に関連すると考えられる記述や、9 条には証拠能力等に関する記述がある。9 条の第 1 項では、いかなる法的手続きであっても、その証拠がデータメッセージであるというだけの理由や、証拠を提出する物が入手しうる最善の証拠である場合には､それがオリジナルではな

いという理由によって、データメッセージの証拠としての承認を否定するような証拠法則を適用してはならないという内容が記されている。第 2 項では、データメッセージの形態の情報には、適切な証拠能力を与えなければないとされている。さらにその証明力を評価する際には、当該データメッセージが作成・保存・伝達された方法の信頼性、情報の完全性が維持された方法の信頼性、作成者が特定された方法、その他関連する要素が考慮されなければならないとされている。

（2） 電子トランザクション共通法

1999 年、アメリカの統一州法全国会議（NCCUSL）において、「電子トランザクション共通法（Uniform Electronic Transaction Act、略称 UETA）が採択され、各州への立法化が勧告された。統一州法全国会議は、州政府の連携による会議体であり、法律家や有識者を交えてこの法令が策定された。各州は UETA の全部もしくは一部を採用し、州法として定めるものであり、2001 年 2 月現在、22 州が採択している。

UETA は、遺言や統一商事法典（UCC）等の特別な規定がある事項等の例外を除き、あらゆる電子的な取引に関する電子記録及び電子署名に適用され、当事者間での取り決めや取引範囲・契約方法等を推奨している雛型である。

7 条では、電子記録及び電子署名が法的な有効性、契約の有効性を満たすための要件に関する規定がおかれている。一方で、9 条においては、電子記録及び電子署名はそれを行った者に帰属するとした上で、実際に記録等を行ったかどうかという点については、個別の事情に照らし合わせて認定されるが、帰属の推定等に関する法的効果には明確な規定がなされていない。

さらに 13 条の証拠の許容性には、「電子記録及び電子署名の証拠性は、それらが電子的なものであるという理由によって排除されるものではない」という一文が含まれている。

１０．３ まとめ

原本性保証の普及方策としては、中長期的な計画も含め、大きく 5 つの方策を提示した。

1 つは、できるだけ早い段階で本研究会で作成したガイドライン及びチェックリストを公開し、ベンダー、ユーザー双方への普及・浸透化を図り、ベンダーにチェックリストに記載されている機能であることを製品パンフレット等に記載してもらい、ユーザーがそれを参照する、などである。

１つは、ガイドラインやチェックリストと一緒に参照してもらいたいと考える PP についても、他のセキュリティ製品と同様に、各機能毎の PP を複数作成し、登録作業を進めていくという方策が挙げられる。

１つは、ガイドライン・チェックリスト・PP の普及を支援するための独自の制度による製品評価認証の実施について検討を進めていくことである。

１つは、製品ベンダーが集まり、製品の普及に向けた方策を検討・実施して行く中立の機関として、原本性保証システム普及協議会（案）といったベンダーフォーラムの設立を行うことで、諸課題の解決を図っていく方策である。

１つは、電子商取引モデル法のような、電子文書の証拠能力を確保するための法令を明文化するアプローチを行うことにより、社会全体に対して、原本性保証の重要性を啓蒙していくことも考える必要があると思われる。

１１． むすびに

電子商取引や電子政府の推進のためには、できるだけ早く「紙情報」と「電子情報」を同等に扱うことのできる世の中にならなければいけない。
政府の「e-Japan 戦略」等において、このための法制度整備は急速に行われつつあるが、ユーザーが電子情報をリスクなく利用していくためには、「原本性保証」という条件をクリアしていかなければならない。

一方、現時点では残念ながら「原本性保証」という定義、具体的に必要な対策については、様々な解釈が入り乱れており、明確なものは存在していない。そのため、ベンダー側は原本性保証システムにどのような機能を盛り込むべきか判断がつかず、ユーザー側もどのようなシステムを利用すればいいのかが判断できない状況にある。

今回とりまとめた「原本性保証システムガイドライン」、「原本性保証電子保存機能チェックリスト」、「原本性保証電子保存システム（ソフトウェア部）Protection Profile」が、現況を打破するために多少なりとも役立つことができれば、これにまさる幸せはない。

また、これに留まらず、本研究会で示された、いくつかの原本性保証製品普及方策についても、継続検討の上、行政・民間が一体となって、何らかの形で実現されることを切に望んでいる。

平成１２年度情報システム共通基盤整備のための連携推進事業
（オンライン制度的課題への対応）

原本性保証に係る評価・認定制度に関する調査研究
報告書

平成１３年3月

発行　　財団法人ニューメディア開発協会
〒108-0073　東京都港区三田１－４－２８
TEL　　０３－３４５７－０６７２