原本性保証電子保存システム(TrustyCabinet™)の開発

Development of Secure Electronic Document Storage System (TrustyCabinet™)

金井　洋一[*]　　谷内田　益義[*]　　小川　雅也[**]
Yoichi KANAI　　Masuyoshi YACHIDA　　Masaya OGAWA

要　　旨

電子文書を証拠として保存することが可能な新しい文書保存システムを開発した．本システムは，保存文書に対する外部からのアクセスを仲介することによって文書へのアクセスを制御するもので，システムの制御下におかれた保存文書は自動的にバージョン管理され，その修正履歴がすべて記録される仕組みになっている．更に，保存文書に対して外部から直接的に行われる不正な削除，改ざん，偽造，すり替え等の処理に対しては暗号技術を応用して対抗している．このシステムはまず行政情報システムのフィールドでの活用が期待される．

ABSTRACT

New secure document storage system that can store digital documents as evidence has been developed. The system intermediates access operations from external entities to the stored documents for controlling access to the documents. The stored documents are managed under the system and all the modification operations upon them are automatically recorded by versioning mechanism. Besides them, the stored documents are protected from direct illegal operations such as deletions, modifications, forgery, and alterations by utilizing cryptographic techniques. In the first stage, the system will be used in the field of electronic government systems.

[*] 研究開発本部 オフィスシステム研究所
Office System Research and Development Center,
Research and Development Group
[**] 販売事業本部 ソリューション計画センター
Solution Planning Center,
Marketing Group

1. 背景と目的

近年，オフィスの情報化が急速に進展し，オフィスにおける多くの業務が電子的に行われるようになりつつある．これまで紙で作成されていた書類はほとんどがパーソナル・コンピュータなどを用いて電子的に作成されるようになってきており，その作成された電子文書に対してネットワーク上でワークフロー処理をするといったシステムが開発され，順次導入が進められている．しかし，電子的に作成された書類は紙の書類に比べて，「真正性」，「見読性」，「保存性」の特性が低下する．すなわち，電子文書は改変しやすく，不可視であり，消去・劣化の可能性があることが問題となる．したがって，特に法定保存義務のある書類については電子データのまま保存することは認められず，最終的に紙に印刷して原本を保存しなければならないのが現状である．

そのような状況に対して，紙の原本が持っている性質(原本性)を電子文書にも持たせることができるようになれば，電子文書を原本，つまり証拠として保存することができることとなり，さらなる情報化が促進されペーパレスオフィス実現への基盤となりうる．

この「電子文書の原本性確保」は，今日，日本政府が強力に推進している電子政府実現のための共通課題の一つとしても認識されており，これを解決することは社会の情報化推進のためにも貢献することができる．

ここで紹介する技術は，電子文書を証明力の高い原本として安全に長期間保存管理するシステムを開発することで，上記の課題を解決することを目的としたものである．

2. 開発コンセプト

2-1 電子文書の問題点

まず，従来の紙文書に比べて電子文書が持っている問題点を以下にまとめる．

- 改ざんやすり替えが容易でそれを見分けることができない
- 完全な複製の作成が容易で原本と区別できない
- 不可視であり，目に見える状態にするのに特別なシステムが必要である
- 完全に消去することが容易である
- 時系列性がない(作成の順序が不明確，差し替えが可能)
- 一部が破損するだけで全体が復元不可能になる可能性がある
- 記録媒体が時間とともに劣化しやすい

ここに挙げた問題点のうち，いくつかは電子データの利便性の裏返しでもある．例えば完全な複製が作成可能ということは，法定保存義務という観点から見れば，どれが原本であるのかが不明確であるということになり，どの電子文書に保存義務があるのか，どの電子文書が最新の原本であるのか，といったことが不明確になることに繋がるという意味で問題となる．

2-2 解決方針

前節で述べた問題点は，電子的な原本への情報セキュリティ上の脅威と捉えることができる．脅威に対するセキュリティ対策は一般的に技術的対策と運用対策の2つに分類できる．電子データを原本として保存することについては，最終的に安全に保存・管理していたかどうか，ということに対する説明責任を当事者が負うことになると考えられる．このとき，運用によるセキュリティ対策を施している場合，それが正しく行われていたかどうかを証明することが非常に難しく，本当に電子文書(原本)に不正な改ざんやすり替えがないかどうかを証明しにくい．そこで，原本に対して，たとえシステム管理者であっても不正ができない技術的な仕組みを導入し，できる限り技術的に電子文書のセキュリティ対策を行う方針とした．そうすることで，説明責任範囲の大部分を技術的に説明することができることになる．

また，技術的なセキュリティ対策といっても様々な方法が考え得るが，電子文書を原本として保存するという機能は情報化されたあらゆる業務システムにおいて共通であるため，その機能をサブシステム化し，複数の業務システムで発生する電子原本を共通に一元管理するシステムを開発コンセプトとした．

3. 機能の概要

前節に述べたコンセプトでTrustyCabinetと呼ぶ原本性保証電子保存システムを開発した(Fig.1). ここでは, TrustyCabinetの持つ機能の概要を説明する. まず, TrustyCabinetを含む全体システムの参照モデルをFig.2に示す.

最近のWebベースの情報システムに見られる3層アーキテクチャの中で, TrustyCabinetはバックエンドのデータ層の位置付けであり, ビジネスロジック層に相当する業務システムからアクセスされ, 業務の処理結果である電子原本を保存・管理するサービスを提供する.

Fig.1 Photograph of the TrustyCabinet

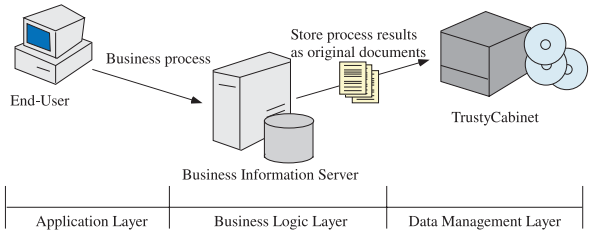

Fig.2 Reference model of TrustyCabinet integrated system

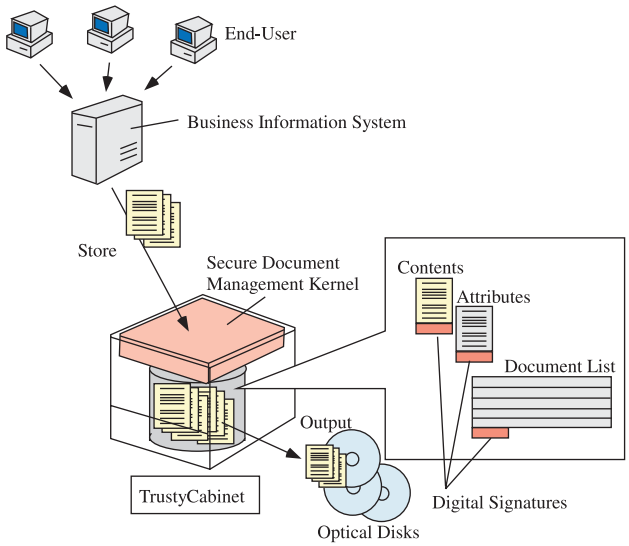

Fig.3 Schematic diagram of document storing process

TrustyCabinetによる原本の保存処理についてFig.3を元に簡単に説明する.

(1) 業務システムからTrustyCabinetに原本として保存したい電子文書をネットワーク経由で送信する.

(2) TrustyCabinetの主制御プログラム(原本性保証カーネルという)が電子文書を受け取る.

(3) 原本性保証カーネルは受け取った電子文書の属性情報(作成者, 日時, ファイル構成等)をXMLで記述, 作成する.

(4) 作成した属性情報と電子文書を原本ファイルとしてTrustyCabinetの内部ハードディスクに保存する.

(5) 原本性保証カーネルは, 原本ファイルと, 原本リスト(原本の台帳に相当)に対して公開鍵暗号方式による電子署名を自動的に付与する.

電子署名の計算に使用する秘密の署名鍵は原本性保証カーネルがTrustyCabinet内部に安全に保持しており, 原本性保証カーネルのみが正しい電子署名を算出することができる.

したがって, 万が一保存された原本に対して直接的に不正な改ざんが行われた場合でも, 公開鍵を用いた電子署名の検証に失敗するため, その改ざんが判明する. また, 原本のリストに付与している電子署名を検証することにより, 万が一原本のすり替えや削除が行われても検出可能である.

また, 紙原本の場合に後から修正が可能なように, 保存された電子原本に対しても修正が可能である. ただし, 原本

の修正要求を受け取ると，原本性保証カーネルは修正した原本のコンテンツファイルを原本の新しい版として記録する．つまり自動的に版管理を行い，原本に対する修正履歴がすべて改ざん，取り消しのできない状態で記録される．これにより，紙の原本と同等な証明力(真正性)を確保している．

そして最終的には，例えば年度の切り替わり時期などに前年度の原本を全てハードディスクからCD-Rなどの光ディスクに書き出す機能を持っており，長期保存性を確保している．

このシステムで重要なことは，保存された原本やそれを管理するデータをすべて電子署名技術で保護していることにより，原本への様々な処理が，すべて原本性保証カーネルを介してしか実行できない技術的な仕組みにしていることである．原本性保証カーネルを介さずに原本に対して直接不正処理を行うとそれが検出されることになる．

4. TrustyCabinet™の技術

前節までにTrustyCabinetが持つ機能の概要を説明した．ここではその機能を実現する技術について説明する．

4-1 原本の真正性確保

Fig.4を用いて真正性を確保する技術の詳細を説明する．TrustyCabinetに保存された各原本には，原本性保証カーネルによって電子署名が計算され，付与される．そして，その原本の識別番号(原本ID)と電子署名が，一定の目的で管理される文書の集合である文書空間(DocSpace)ごとに作成される原本リストに対して，エントリとして加えられる．できあがった原本リストには原本性保証カーネルによって電子署名が計算され，付与される．そして，その文書空間の識別番号(メディアID)と原本リストの電子署名が，TrustyCabinetごとに存在する文書空間リストのエントリとして加えられる．最後に文書空間リストに対して原本性保証カーネルが電子署名を付与する．

これにより，原本，文書空間，TrustyCabinetという単位で改ざんの検出が可能になる．付与された電子署名については，まず起動時に文書空間リストの整合性を，次に文書空間にアクセスする際に原本リストの整合性を，最後に各原本にアクセスする際にその原本の整合性を検証するという形で自動的に内部で処理が行われる．

TrustyCabinetでは一つの文書空間は一枚のメディアに相当しており，原本と原本リストは個々のメディアに記録される．そして，TrustyCabinetで扱うすべてのメディアの管理情報である文書空間リストは，TrustyCabinetの内部ハードディスクに保存する．

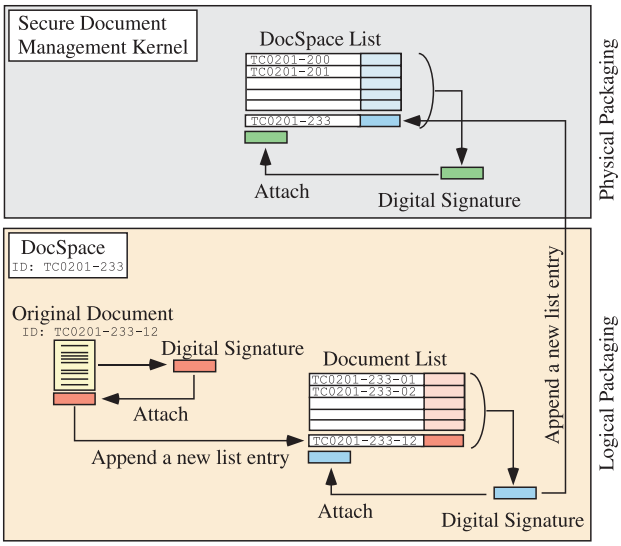

Fig.4 Mechanism of keeping trustworthiness of documents

その他にも，原本が保存・修正された時系列性が保たれるように，TrustyCabinetのシステムタイマの設定を変更するとその変更履歴についても記録するようにしている．

前節からここまでを通して，基本的に保存する原本を対象として暗号技術を駆使したセキュリティ処理について説明しているが，原本性保証カーネルに対する改ざん，実行環境(オペレーティングシステム)の改ざん，ウィルスの混入，ハードウェアへの細工，といったことが行われないよう，原本性保証カーネルそのものに対するセキュリティ対策も必要である．

TrustyCabinetは原本性保証カーネルを含む実行環境そのものを物理的な耐タンパー性のある筐体に格納した(Fig.1)．基本的にシステム管理者であっても原本性保証カーネルには触れることはできず，サービスマンのみが内部のメンテナンスを行うことができる位置付けとした．

物理的耐タンパー性についてどこまで高いレベルを求めるかについては，TrustyCabinetを誰でも物理的にアクセスできる環境に設置するのか，入退室管理されたコンピュータ

ルームに設置するのか，といった運用環境のセキュリティレベルに依存する．

Fig.4にあるように，TrustyCabinetではこの耐タンパー筐体への格納を物理的パッケージ化(Physical packaging)と呼んでおり，その原本性保証カーネルの物理的パッケージ化と，暗号技術の組み合わせによって論理的に不正アクセスが不可能になったメディアの状態を，メディアの論理的パッケージ化(Logical packaging)と呼んでいる．

4-2　原本の管理方法

Fig.4では電子文書を概念的にひとつの塊で示しているが，HTMLで記述された文書に代表されるように，一つの文書は複数のファイルで構成されることが一般的になりつつある．そのため，TrustyCabinetは複数のコンテンツファイルを一つの原本として管理することを可能とし，その原本のファイル構成について改ざんされないように電子署名の技術を使って保護している．

具体的にはAIIM(The Association for Information and Image Management)が定めているDMA(Document Management Alliance)という文書管理アーキテクチャの文書オブジェクトモデルを簡易化したものを原本のコンテンツファイルの管理方法として採用している．

Fig.5に示すように，一つの原本は原本の属性ファイル，署名ファイル，アクセスログファイルとコンテンツファイルで構成している．原本に対して修正が施されると，修正されたコンテンツファイルのみが新しいバージョンとして記録され，修正されていないコンテンツファイルについては以前のバージョンのファイルへのリンクを張る形で管理する．原本のファイル構成は，原本の属性ファイルの中に記述して管理しており，原本が修正されるごとに原本の構成変化が属性ファイルに反映される．

また，署名ファイルには原本を構成する各ファイルのハッシュ値を格納しており，そのハッシュ値のリストに対して電子署名を付与している．

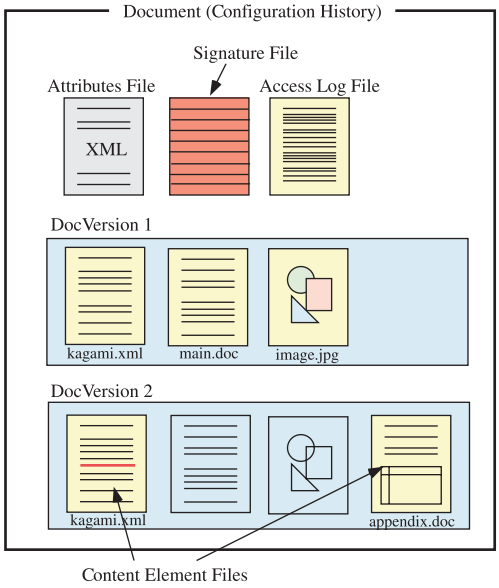

Fig.5　Structure of a stored original document

4-3　原本の移動・謄本の作成

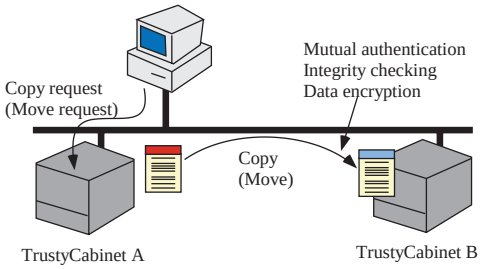

Fig.6　Moving or copying documents to other storage systems

紙原本の場合，原本を他の部署や業務に渡すといったことが可能である．同じようにTrustyCabinetでもFig.6にあるように，別のTrustyCabinetに対して原本を移動したり，複製である謄本を作成したりすることが可能である．原本の移動等では原本の電子データそのものがネットワーク上を流れることになるが，通信はSSL(Secure Sockets Layer)をベースにして相互認証，改ざん検知，暗号化を行うことにより，成りすまし，改ざん，盗聴を防いでセキュリティを確保している．

原本を移動すると移動元のTrustyCabinetには当該原本を移動したことを示す履歴と移動先TrustyCabinetの識別番号が記録される．

4-4　属性に応じたアクセス制御

TrustyCabinetは保存している電子文書に対して，「仮原本」，「原本」，「謄本」といった属性を付与して管理している．それぞれの属性の関係はFig.7に示す通りである．まず，外部から保存要求とともに渡される電子文書は，「仮原本」，もしくは，「原本」という属性を付与することができる．「原本」の属性が付与された電子文書については，自動的に修正履歴が記録され，指定された保存期限を過ぎるまで削除することはできない．その一方，「仮原本」の属性が付与された電子文書は，「原本」と同じく修正履歴が記録され改ざんすることはできないが，仮の原本という位置付けであるため削除はできるようになっている．そして後で属性を「原本」に変更することができる．一度「原本」の属性に変更した後は保存義務が発生した文書という位置付けになるため，保存期限を過ぎるまでは削除できず，もちろん「仮原本」の属性に戻すこともできない．これをワークフロー上で活用することで，決裁が済んだ文書のみを「原本」の属性にすることで保存義務のある文書のみを適切に保存・管理することができる．

また，「原本」の属性が付与された電子文書の複製を要求すると，複製された文書には自動的に「謄本」の属性が付与される．「謄本」はその時点での原本の完全な複製であることを保証した文書であり，保存義務の対象ではないため削除は許可するが，複製であるため修正は許可しない．

一般的なオペレーティングシステムでは主にユーザ(グループ)と対象オブジェクトの関係によってアクセス権限が決定される仕組みでアクセス制御が行われるが，TrustyCabinetでは上記のように対象オブジェクト(文書)に付与されている属性に応じてアクセス権限が決まるアクセス制御法則を採用している．

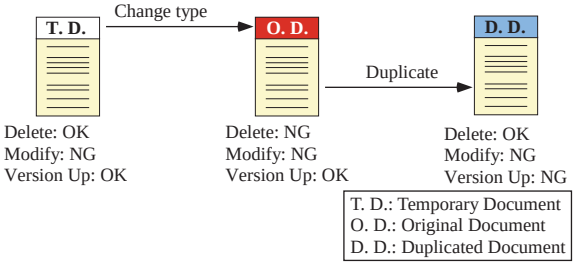

Fig.7　Document type based access control

4-5　原本の長期保存性確保

特に法的に保存義務のあるような文書の場合，その種類によっては保存期限が10年から30年というような長期間にわたる場合がある．一般にハードディスクのような磁気記録メディアよりもCD-Rのような光ディスクの方が長期保存には適しているため，TrustyCabinetでは原本の電子文書を光ディスクに書き出して保存できるようにしている．暗号技術を応用した改ざん検知処理を行っているため，光ディスクは書き換え型であっても追記型であっても構わないが，不用意な削除や書き換えに対抗するためにも追記型のメディアを採用することが望ましい．

4-6　原本の見読性確保

TrustyCabinetは，保存された電子文書について，作成者，作成日時，ファイル構成，修正履歴等を記述した属性情報を原本ごとに自動的に作成・記録する．この属性情報はXMLで記述されており，テキストデータであるため長期にわたる見読性に優れている．さらにXMLをRDF(Resource Description Framework)に準拠させているため，これを原本に関するメタデータとして将来にわたって情報システムで処理しやすい状態としている．

また，原本を構成するファイル群は一般的なファイルシステム上にフォルダ階層を作成して分かりやすく配置して記録し，保存ファイルの配置を見れば直感的に原本の構成が分かるようにしている．多くの場合，システムよりもメディアの寿命の方が長いため，特別なシステムでしか理解できない形で記録してしまうことはデータの消失につながる恐れがある．そのため，直感的に分かりやすい記録方式は原本の見読性にとって重要なこととなる．

このようにしてTrustyCabinetは原本の長期にわたる見読性確保をできるだけ技術的にサポートするようにしている．

5. まとめ

暗号技術，XML，光ディスク等を組合せ，電子文書を証明力の高い原本として安全に長期間保存・管理するTrustyCabinetの技術について紹介した．

このTrustyCabinetはすでにインターネット電子申請の実

証実験などにおいて利用されていることもあり，電子文書のセキュリティに敏感な電子政府，電子商取引システム，医療情報システムといったフィールドから順に本技術が活用されていくことが期待できる．

6. 今後の展開

現在，財団法人ニューメディア開発協会を中心として原本性保証電子保存システムに求められるセキュリティ要件を，国際的な情報技術セキュリティ評価基準ISO/IEC 15408に準拠した形で定義する活動が行われている．リコーはその活動に参画しており，TrustyCabinetが原本性保証電子保存システムとして認証を受けられるように活動していく予定である．原本性保証電子保存を行っていることが国際標準に準拠した形で公的に認証されれば，利用者は更に安心してTrustyCabinetを電子原本の保存のために利用することができるようになる．

謝辞

本技術紹介にある原本性保証電子保存システムは，特殊法人情報処理振興事業協会において創造的ソフトウェア育成事業の一環で実施された「原本性保証電子保存システムの開発」プロジェクトの成果に基づいている．

プロジェクトにおいて技術的な指導をいただいた財団法人ニューメディア開発協会の国分明男常務理事ならびに，東京工業大学の大山永昭教授に謝意を表する．

また，TrustyCabinetの開発に尽力してくださった関係者の皆様と，特に先端技術を駆使して開発を進めてくださったリコーシステム開発(株)の皆様に謝意を表する．

参考文献

1) 国分, 谷内田, 山口：(特)情報処理振興事業協会 創造的ソフトウェア育成事業 最終成果発表会論文集,(1998)pp.341-348

2) 金井：行政&ADP, Vol.34,(1998)pp.10-17