# 証明書の電子化における証明書存在証明方式における一考察

高村昌興† 上島康司† 中村太一†
{takamuram, ueshimay, nakamuratic}@nttdata.co.jp
株式会社 NTT データ 技術開発本部‡

## 1.はじめに

現在の様々な契約書類において、その記載事項の正当性を証明するために、本文になる書類以外にも、多くの証明書を添付書類として付随し提出する。そのような書類に対し、提出者は添付書類の収集等、受信者は添付書類の正当性確認等が負荷として挙げられる。このような課題に対し、事例として、精算された小切手、入金依頼票のイメージファイルを参照できる仕組みも検討されている。

本稿では、このような証明書電子化が検討されている状況において、日本の商取引で必要とされる民間、及び公的証明書として望ましい電子形態を考察すると共に、上記参照方式をセキュリティ面、更には電子証明書として利用される形態を考察し、望ましい参照スキームを提案する。

## 2.証明書存在証明に関する動向

現在、国内外の官民分野においては、証明書の存在を証明する仕組みである「証明書存在証明サービス」が検討され、実際にサービスを行っているシステムも存在する。ここでは、その仕組みとサービス事例を概観する。

国内においては、財団法人ニューメディア開発協会（以下、NMDA）において、「ライセンスリポジトリ方式の制度的及び技術的課題に関する調査研究」が検討されてきた[1]。ライセンスリポジトリ方式（以下、LR 方式）とは、申請・届出に添付される書類（以下、添付書類）に対し、「添付書類を電子的な形で発行元行政機関、あるいは申請者側等に保管しておき、申請受付側の行政機関が必要に応じて閲覧することで、添付を不要にする」ことを行う方式である。これにより、流通上に生じる長大データ、イメージデータ等様々な形式、サイズの添付書類に対し、通信負荷の低減、冗長なデータ管理の低減等が可能になり、コストを削減できると考えられている。

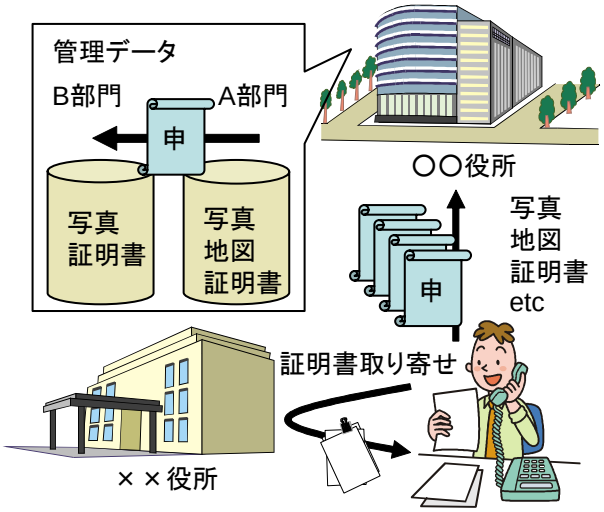


図-1. 管理情報の負荷が大きくなる要因

表-1. 証明書存在証明サービス比較

| | NMDA | BoA |
|---|---|---|
| 名称 | LR 方式（検討中） | online digital check imaging（実システム） |
| 証明内容 | 証明書、図面等資料 | 小切手、入金依頼票 |
| 対象データ形式 | あらゆるデータ形式 | イメージ |
| アクセス権 | SSL 認証<br>トークン等 | SSL 認証 |
| 証明期間 | アクセス限度回数、情報更新が生じるまで | 45 営業日 |
| 証明対象 | 申請・届出先（公的機関） | 顧客本人 |
| 運営組織 | 証明書発行者<br>添付資料作成者 | BoA |

また、海外では、米国の地方銀行であるバンク・オブ・アメリカ（以下、BoA）において、

A Case Study of the Validation Evidence adopted by the electronic License Technique
†Masaoki Takamura, Yasushi Ueshima, Taichi Nakamura
‡NTT DATA Corporation, Research and Development Headquarters

証明書を閲覧するサービスが始まっている[2]。これは、BoA が 45 日営業日以内に清算された小切手の両面、および入金依頼票のイメージデータを顧客に公開することで、照会作業が迅速化され、詐欺行為の防止が可能になると考えられている。また、この手法の特徴としては紙の削減についても述べており、安全管理上、小切手、入金依頼票を物理的に紙として残しておく手間から開放されるメリットもあると述べている。

しかし、これらサービスにおいては、イメージデータやテキストデータ等を、閲覧サービスもしくは存在証明サービスとして提供しているが、そのとき限りの確認情報であり、実際に検証者が係争時に備えて確認を行ったことを証拠として残すことは難しい状況である。

これ以降は、このような状況に対し、どのように証明書存在証明サービスを提供／利用することにより、より効率的で安全な申請・届出の仕組みが実現できるのかを検討すると共に、その解決案を提示する。

## 3.証明書存在証明方式の利用モデルとその課題

LR 方式において、現在検討されている対象は、CtoG、BtoG の電子申請において、受付側で生じる添付書類閲覧サービス、もしくは証明書取得サービスである。ここでは、LR 方式の民間適用を前提とし、民間で行っている添付書類を要する手続きについて代表的なモデルを、金融、保険、産業から選択し、そこから抽出される課題を整理する。

①資金調達・融資（中小企業融資）モデル

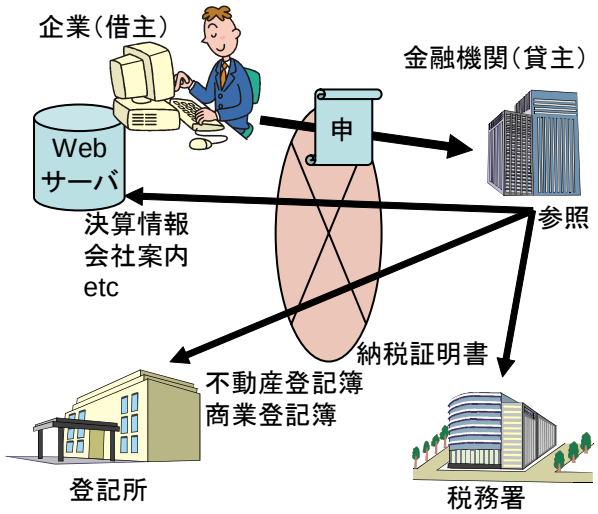


**図-2. 資金調達・融資のモデルイメージ**

中小企業における融資においては、国内経済の緊縮やペイオフ解禁など様々な要因が重なり、融資単位が小口化し、かつ融資審査のスピードアップが求められている。結果的にシステム化による融資審査業務の効率化が求められていると考えられる。

この審査過程においては、会社の存在を証明する商業登記簿謄本および印鑑証明書、収入／支払能力を示す納税証明書、担保を確認する不動産登記簿謄本、会社の規模を示すパンフレット等の提出を求められる。

②保険金請求モデル

自動車保険の請求においては、国内自動車生産数増加による保険契約の増加、および自動車増加に伴う自動車事故増加といったことが考えられ、そのような要因から請求依頼の数が増加すると考える。そのため、1 件あたりの請求審査のスピードアップが必要となると考えられる。

この審査過程においては、交通事故証明書、診断書、休業損害証明書、領収書等の提出が求められる。

③社員採用モデル

社員採用においては、定期的な新卒者に加え、近年の転職の一般化により、請求数が増加すると考える。新入社員の採用時期が一般的に決まっているため、トランザクションが集中するタイミングがあり、それ以外は転職対応等の定量的なトランザクションが発生すると考える。

この審査過程においては、履歴書、卒業証明書、成績証明書、資格証明書、住民票、年金手帳等の提出が求められる。

このようなモデルの中で必要となる添付書類を分析したとき、表-2 で示すようにまとめられる。

この表を考慮したとき、民間手続きにおいても公的証明書を添付する手続きが多く存在することが見受けられると共に、検証者が証明書の内容を見た際には、公的機関、準公的機関、企業等、証明書の発行主体の信頼性を元にその書類を受け入れ、かつ自身で管理する傾向にある。

また、公的分野の申請・届出業務と同様に、ひとつの添付書類が容量的に大きい場合、添付書類単位は小さいが高い頻度で利用される場合が存在し、民間での申請業務においてもデータ管理に対し負荷を要すると考える。

このような状況は、民間も官側証明書の参照を多く要するため、民間へ LR 方式の技術、およびサービスの開放が課題として挙げられる。

また、前章で示したように、LR 方式以外にも、民間企業が発行する証明書に関しては参照する仕組みができつつもあるが、それは銀行等限定されたドメインの中での仕組みであるため、そのドメイン以外での証明能力に乏しい状況である。この場合においては、あくまでも顧客への参照機能の提供であり、その証明情報を第三者に提供することを前提としていない理由であることも挙げられる。

**表-2. 利用モデルで必要とされる証明書**

| | 資金調達・融資 | 保険金請求 | 社員採用 |
|---|---|---|---|
| 本人存在確認 | ― | ― | 住民票（公的機関） |
| 会社存在確認 | 商業登記謄本（公的機関） | ― | ― |
| 有資格確認 | ― | 保険契約書（企業） | 卒業証明書、成績証明書、資格証明書（教育機関） |
| 所在地確認 | 商業登記謄本（公的機関） | ― | ― |
| 支払行為確認 | 納税証明書（公的機関） | 領収書 | ― |
| 健康状態確認 | ― | 健康診断証（医療機関） | 健康診断証（医療機関） |
| その他確認書類 | 不動産登記簿謄本（公的機関）、決算書（企業）、試算表（企業）等を添付 | 事故証明書（公的機関）、休業損害証明書（企業）等を添付 | 履歴書（本人）、成績証明書（教育機関）、年金手帳（公的機関）等を添付 |

注：（）は書類発行主体

LR 方式の中にも、イメージデータを公開する、テキストで情報を公開する仕組み等が存在するが、それらはあくまでもそのとき限りの参照データを前提としているために、普遍的な証拠書類としては扱えない状況である。

例えば、現在の住所の確認、現在の資格の確認という観点であれば、申請業務の審査過程において現在の確認を行い、その結果を持って処理を行うという「運用」で対応できる場合も考えられるが、係争時を考慮したならば「参照先の情報で確認した」証拠を残すことが重要と考える。

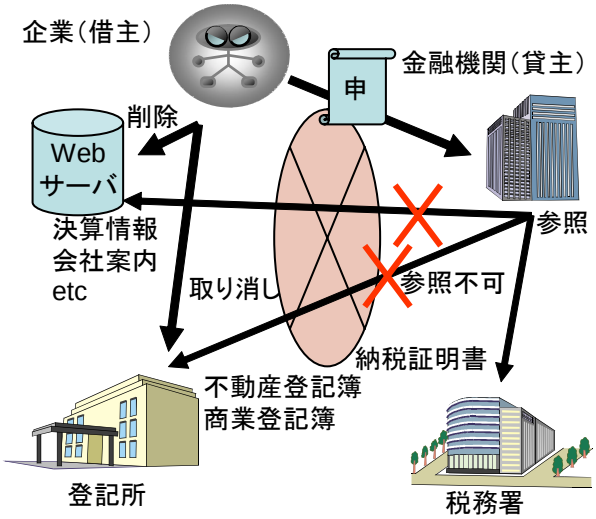


**図-2. 契約成立後の情報更新による影響**

そのため、イメージデータ、テキストデータ等データの種別に寄らず、利用者／提供者のどちらかで、その時間に参照した結果と実績が証拠として残せる仕組みが重要と考える。

## 4.提案方法

将来的には、CtoB、BtoB 等民間分野での規制緩和から、公的機関発行の証明書の利用が可能となると考えるので、ここでは技術的な課題、特に前章で示した「その時間に参照した結果と実績が証拠として残せる仕組み」について焦点をあてることとする。

これまで示した証明書存在証明サービスでは、それぞれのサービスとして情報を参照するのみ、もしくは情報そのものをダウンロードする仕組みであった。前者は証拠が残らない、後者は利用者（検証者）も最終的には情報を持つという効率の悪さという課題であった。

①証拠への対応

民間分野と公共分野での運用の違いは、係争時において公共分野は法制度的に運用をサポートしているのに対し、民間分野では自己責任で証明を要する部分が強く、自身で証明データを確保する必要がある。証拠として利用できるためには、表-3 で示す要素が必要と考える。

このようなデータ構成を持つことで、誰によって生成されたドキュメントであるのか、確認

内容（ドキュメント ID から取り出せるドキュメント）とハッシュ値が対応しているのか（検証した対象は何であるのか）、そしてデータを検証した時間はいつであるのかを証明することが可能となると考える。

このとき、申請・届出データに係争が生じる可能性もあるため、この情報が 7 年、10 年といった長期間の保証を求めることになる。PKI といった技術においては、有効期限が切れてしまう関係上あまり意味を成さないため、証明書存在証明サービスを受ける側は証拠データの証拠 ID のみを管理することとし、係争時には、その ID を基にその証拠データを抽出する運用を考える。このとき署名を付与することになるが、通信路のセキュア化としてそのとき有効な秘密鍵で署名を付与して提供することを考える。

その際に、サービス提供側での注意点としては、長期間のデータ管理にはデータ更新が生じることは否めないが、更新履歴を十分なセキュリティを持って管理することで、そのときの状態へ証拠能力を持って戻すことが可能である。

**表-3．証拠データ構成**

| 構成 | 内容 |
|---|---|
| 証拠 ID | 本証拠データのトランザクション ID |
| ドキュメント保有者名 | ドキュメント保有者名称 |
| ドキュメント ID | ドキュメント保有者がドキュメント発行時に付けたトランザクション ID（ドキュメントがない場合は空） |
| ハッシュ値 | ドキュメントのハッシュ値（ドキュメントがない場合は空） |
| 照会結果 | ドキュメントを照会した結果（有効／無効） |
| 時間 | 問い合わせを実施した時間 |
| 署名 | データ保有者による署名 |

②効率向上への対応

現行の運用、法制度との親和性から、申請・届出データに添付書類データが付随している流通方式、もしくはダウンロードする参照方式が望ましい。しかし、ネットワークの普及に伴い、通信の効率化、ディスク容量の効率化を考慮するべきであり、それを考慮した際には、検証側にはデータ本体を確保しない照会方式が望ましいと考える。

現行の運用、および法制度とのギャップを考慮し、次に示す図のように、データを添付して申請する方式、申請先でデータをダウンロードする方式、申請先でデータの存在を確認する方式へと段階を経て効率的な方式へと変更していくべきと考える。

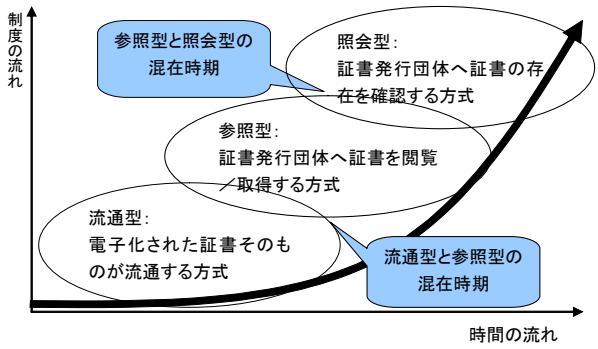


**図-3.時間と制度による機能の成長**

## 5.まとめ

本稿では、係争時等証明書の検証を行ったことを証明する必要があるとき、「確かに参照先の情報で確認した」という証拠を残すことの必要性があること、及びその解決案を述べた。

実装を考慮した際には、証拠データの利用権限を保障するためにも、発行された証拠データの利用回数を制限する仕組み、対象者のみ利用できる仕組み等、DRM(Digital Rights Management)技術を応用して、証拠データに対し更なるセキュリティを設けることも可能であるため、そのような機能拡張の検討も必要である。

また、民間モデルの検討を行った際には、公的証明書を利用している手続きが多々あり、手続きの電子化にあたっては公的証明書電子化を行われることが切望されている状況でもある。このような背景においては、民間市場の活性化に向けて、規制緩和、法制度整備も重要な課題と思われる

## 参考文献

[1]ライセンスリポジトリ方式の制度的及び技術的課題に関する調査研究,ニューメディア協会, http://www.nmda.or.jp/nmda/soc/1-1/1_1all.pdf
[2]online digital check imaging, Bank of America, http://www.bankofamerica.com/newsroom/press/press.cfm?PressID=press.20021127.01.htm