

電子公証人機能の開発と実証実験

5M-9

大越文弘

三菱電機株式会社

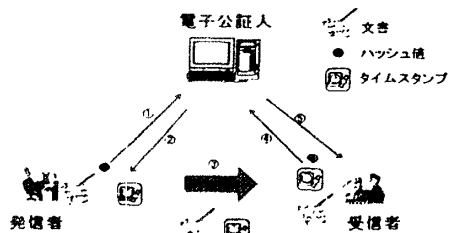
1. はじめに

近年の情報技術の発展により、社内の連絡事項、企業同士の連携・協力にコンピュータネットワークを積極的に活用するようになってきている。電子メール、WWWに代表されるオープンなコンピュータネットワークでは、迅速な情報交換が行え、また、情報が電子化されているため情報の流用が可能である。そのため、商取引にもオープンなコンピュータネットワークを導入することにより、業務の生産性、効率性の向上、本格的なペーパーレスが可能であると考えられる。しかし、コンピュータネットワークでは、電子データを対面でなくネットワークを介して交換するため、文書、取引日時のご改ざんが可能である。そのため、現状の商取引では、コンピュータネットワークを十分に活用しているとはいえない。

そこで、本研究ではネットワーク上で商取引を行うために取引事実を証明する第三者が必要と考え、取引成立日時に着目して、文書作成日時を立証するタイムスタンプ機能と、取引した内容を記述した文書のご改ざん防止に着目して、文書を複数人で秘密に保存し改ざんを不可能とする秘匿保存機能を開発した。そして、それら2つの機能が実際の商取引に有効であるか実験し、電子公証を運用する上での問題点の顕在化、ノウハウの蓄積を行うことにした。本稿では、開発した機能の概要を報告する。

2. タイムスタンプ機能

文書の作成日時を立証するための機能である。



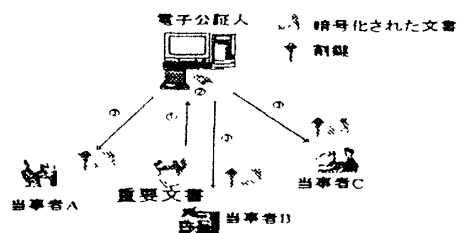
クライアント/サーバ方式を採用し、データ送受信は電子メールを利用している。また、処理の高速化と保管データのサイズを少なくするために、文

書そのものを送信・保管するのでなく、文書のハッシュ値を送信・保管している。

発信者がタイムスタンプを要求すると、クライアントで文書のハッシュ値を計算し、サーバに電子メールで送信する。サーバでは受信したハッシュ値を保管しタイムスタンプをクライアントに返送する。次に、発信者は文書とタイムスタンプを受信者に電子メールで送る。受信者がタイムスタンプの検証を要求すると、クライアントで文書のハッシュ値を計算し、ハッシュ値とタイムスタンプをサーバに電子メールで送信する。サーバは保管しているハッシュ値を検証し電子メールで結果を返す。

3. 秘匿保存機能

文書を暗号化する鍵を複数に分割することにより、当事者以外の開示を不可能とする機能である。



クライアント/サーバ方式を採用し、データ送受信は電子メールを利用している。

利用者は文書をクライアントから電子メールでサーバに送信する。文書を受信したサーバは、文書を暗号化し保管する。暗号化に用いた鍵は、k元連立方程式を用いて分割（割鍵）し、各割鍵を当事者に返す。暗号化文書の開示の際は、当事者が保持しているすべて（または一部）の割鍵からもとの暗号化に用いた鍵を再構成し暗号化文書を復号する。これにより、文書内容の修正の際は各当事者に承諾を得ないと修正不可能となる。なお、処理の履歴にはタイムスタンプを利用する。

4. おわりに

現在、2つの機能の開発は完了した。今後、実際の業務に適用して、信頼性・操作性・性能評価・運用時の問題とその対策・ニーズ等実用性を検証する。また、実験を通して、電子公証ノウハウの蓄積を行う。