暗号を用いた文書通信管理方式の検討

6P－7

大田 幸由，萱野 忠

ＮＴＴ通信網研究所

１．はじめに

機密文書として扱われる情報を通信する場合，情報自体の隠蔽のほかにも，情報漏洩時の経路追及などのため情報の通信履歴を明確にしておく必要がある．

我々は，ネットワーク上のデータベースを用いて機密文書情報を通信する形態を想定して，データベースに情報登録を行った者が通信相手を制限し，同時に通信相手が通信の事実を否定できない方式を検討した．その結果について本稿で報告する．

２．文書の通信管理

文書通信を管理する上で，通信に関する事実を，文書の送信者，受信者とも，後日否定できないことは重要なことである．特に，文書に対する機密性が求められるほど，その要求は高くなると考えられる．本稿では，機密文書の通信を想定し，この概念を実現する方式を検討する．ここでは，データベースを用いた文書通信モデルを対象に検討を行う．検討対象となるモデルは次のようなものである．

あるユーザが機密文書をデータベースに保管し，この文書に対する正当な参照権を有するユーザが読み出しを行う．

以下では，データベースに文書を保管する者を送信者，データベースから文書を読み出す者を受信者と呼ぶことにする．図１に概念図を示す．

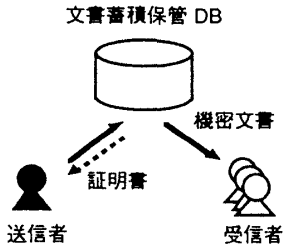


図１　検討モデル

機密文書のこのような通信形態において，次のサービスを実現する．(1) については，文書の機密性から当然必要となるサービスである．

(1) 情報を暗号化してネットワーク上での情報の漏洩，改ざんを防止する．

(2) 送信者が，受信者を特定して通信の事実に関する証明を得られる．

これらにより，送信者は，受信者へ安全に情報を伝えることができ，文書の通信を管理することができる．受信者は，通信の事実を否定することはできなくなる．

2.1 従来方式との比較

このように通信の事実を証明する方式は，電子メールシステム上では，すでにいくつか提案されている[1][2][3]．一般に，これらの方式では調停者と呼ばれる者を介して，送信者が電子メールに関する内容，配達証明を得ることができるようになっている．しかし，いずれの方式も，単一の受信者を想定しているので，複数の受信者へ向けて電子メールを送る場合には，送信者が同一の処理を繰り返す必要がある．

本稿では，この問題を解決するために，機密文書を一旦，データベースに保管することにより，送信者が機密文書自体を送る手続きは１回限りで済ませて，各受信者へは調停者を介すことなく通常の電子メールを送れるようにする．これにより，送信者はデータベースに機密文書を保管してもらう時に内容証明が得られ，受信者が機密文書を読み出す度に，その都度，配達証明が得られる．

３．提案方式

２章で述べたサービスを実現する方式を以下に示す．まず，機密文書を保管するためのデータベースを管理する文書サーバを定義する．この文書サーバは，文書の保管以外に，文書の内容，配達証明書を発行する調停者としての役割も果たす．提案方式では，文書サーバに対する信頼性，機密性を仮定しておく必要がある．この仮定に基づき，以下の項目を文書サーバの前提条件とする．

(1) 文書を保管し，この内容に関する内容証明書を送信者へ送る．

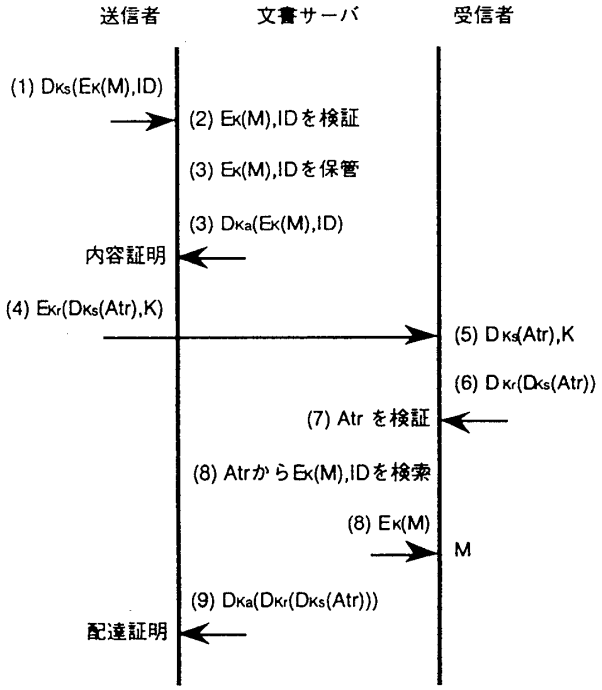
(2) 受信者の読み出しトークンに基づいて，保管されている文書を受信者へ送る．

(3) 受信者への送信を保証する配達証明書を送信者へ送る．

3.1 方式手順

提案方式の具体的な処理手順を以下に示す．図２はこの処理を表わしている．

A Study of Communication Management for Secret Documents Based on Cryptosystem
Yukiyoshi OHTA , Tadashi KAYANO
NTT Telecommunication Networks Laboratories
1-2356 Take, Yokosuka-Shi, Kanagawa 238-03, Japan.



記号説明
M：機密文書
Atr：文書属性
ID：文書情報 (ID∈Atr)
Ks：送信者の秘密鍵（公開鍵暗号）
Kr：受信者の秘密鍵（公開鍵暗号）
Ka：文書サーバの秘密鍵（公開鍵暗号）
K：文書の暗号化鍵（共通鍵暗号）

図２　提案方式の処理手順

文書番号：（文書ごとに設定）
配布番号：（受信者ごとに設定）
送信者：
受信者：
文書作成日：

図３　文書属性の例

(1) 送信者は，ある鍵で暗号化した文書にディジタル署名を行い，これを文書サーバへ送る．（暗号化した文書には，文書番号，送信者などの情報をつけておく．これは文書と後述する文書属性とを対応づけるためである．）
(2) 文書サーバは，受け取った文書に対して送信者のディジタル署名を検証する．
(3) 署名の正当性を検証した後，この文書を保管するとともにディジタル署名を行い，これを内容証明書として送信者へ送る．
(4) 送信者は，受信者ごとに定義した文書属性にディジタル署名を行い，これと文書を暗号化した鍵を各受信者の公開鍵で暗号化し，受信者へ直接メールで送信する．文書属性は例えば図３に示すものである．
(5) 受信者は，受け取ったメールを自分の秘密鍵で復号することにより，文書属性および文書を暗号化している鍵を得る．
(6) 受信者は，文書属性にディジタル署名を行い，これを文書の読み出しトークンとして文書サーバへ送る．
(7) 文書サーバは，受け取った文書属性に対して受信者，送信者のディジタル署名を検証する．
(8) 署名の正当性を検証した後，文書属性に基づいて保管しておいた文書を受信者へ送る．この時，文書に付与された文書番号以外にも文書の送信者を調べるなどして，これが異なれば，送らないようにする．（これにより，他のユーザの文書を読み出すことはできない．）
(9) さらに，文書サーバは，文書属性にディジタル署名を行い，これを配達証明書として送信者へ送る．

４．安全性の検討

この方式は，３章の文書サーバに関する前提条件の上で実現されている．文書サーバが不正を行う場合を想定し，この方式の安全性について検討する．

(1) 文書は暗号化されているので，漏洩の心配はない．
(2) 正当なユーザ以外に文書を送信したとしても，文書の暗号化鍵を知らない限り復号されることはない．
(3) 配達証明書には送信者，受信者のディジタル署名が含まれるので，証明書を発行しないことはできても，偽造することはできない．

５．おわりに

本稿では，機密文書に対する文書属性を定義して，これを受信者の読み出しトークンとして利用すると同時に，送信者に対する配達証明として発行する方式を提案した．この方式を用いると，送信者が複数の受信者へ機密文書を送信する時に，内容，配達証明を得る手続きを簡略化できることがわかった．

今後は，この方式が実システムへと適用される場合を想定して，手順の詳細化，安全性に対する十分な検討などを行う予定である．

参考文献

[1] 中尾：”メッセージ内容証明サービスにおける暗号の適用”，第２回暗号と情報セキュリティ（CIS）研究会資料（1985）．
[2] 田中，内田，秋山：”暗号を用いた内容証明・配達証明サービス”，信学論，Vol.J70-D，NO.2，pp.423-431（1987）．
[3] 安達，杉村：”電子メイルにおける配達証明・内容証明の実現に関する一考察”，信学技報，ISEC93-16，PP.1-6（1993）．