2W-03

資料配付型の会議支援システムのセキュリティに関する提案

高根澤哲広†、横森正利†、角隆一††
†NTT 東日本、††NTT 西日本

1 はじめに

著者らは、イントラネット環境で、会議資料を共有する会議システム[1]の開発を行ってきた．現在このシステムを拡張し、インターネット環境に対応した「インターネット対応知識共有システム」の開発を進めている．このシステムは、遠隔地からの会議への参加を容易にすると同時に、遠隔講義など会議以外にも適用範囲を広げる．

インターネット環境はセキュリティが十分でない．このため本方式では、会議資料を暗号化する方式[2]によりセキュリティを確保している．本論文では、会議資料を暗号化する方式を用いて、実際に運用するときの鍵管理方法を分析し、提案する．

2 インターネット対応知識共有システム

2.1 会議資料の共有方式

本システムでは、会議資料の共有を各参加者端末に事前に会議資料を配布し、発表者端末のページ移動や、マウスポインタ等のイベント情報を全参加者に送ることで実現する．会議資料は、発表者がサーバに登録し、サーバから各参加者に配布される．

2.2 セキュリティの確保方式

インターネット環境で使用する場合、サーバに登録された会議資料がインターネットを通して窃取させるおそれがある．これを防ぐため、本システムでは、会議資料を暗号化してサーバに登録する．概要は次のとおりである．

(1). 各利用者は公開鍵と秘密鍵のペアを作成し、公開鍵をサーバに登録し、秘密鍵を参加者端末に保存する．
(2). 発表者は、共通鍵を作成し、会議資料を共通鍵で暗号化してサーバに登録する．
(3). 共通鍵は、会議に参加する各利用者の公開鍵で暗号化して、サーバに登録する．
(4). 参加者は、サーバから暗号化された会議資料と、暗号化された共通鍵をダウンロードする．
(5). 利用者の秘密鍵で共通鍵を復号化し、その共通鍵で会議資料を復号化することで会議資料を得る．

この暗号化方式でネットワークに流れるのは、公開鍵・暗号化された共通鍵・暗号化された会議資料のみである．

3 暗号化方式の運用

会議資料を暗号化する方式の場合、利用者が会議参加者かどうかの判断を秘密鍵の所持の有無で行う．そのため利用者の秘密鍵の管理が重要になる．秘密鍵の管理に必要な機能は、利用者の会議に参加する環境により異なる．ここでは、環境を端末に注目して以下の３つに分類する．

(1). 自宅や自席などにある個人専用の端末から会議に参加
(2). 会議室や教室など、複数人で共用する共用端末から会議に参加
(3). 自席端末とモバイル端末のように、１人の人が複数の端末を使いわけて会議に参加

(1)の場合は、端末の利用者と端末に保存されている秘密鍵の所有者は等しいので、従来の端末に秘密鍵を保存する管理方法で問題ない．(2)の場合は、同一端末で複数の利用者が秘密鍵を使用できる必要がある．(3)の場合は、利用者が複数の端末で秘密鍵を使用できる必要がある．

4 秘密鍵の管理方法

4.1 複数利用者の同一端末利用

この場合の秘密鍵の管理方法には、秘密鍵の管

Tetsuhiro Takanezawa, Masatoshi Yokomori,Ruichi Sumi
Nipponn Telegraph and Telephone East Corporation
Nipponn Telegraph and Telephone West Corporation
3-9-11 Midori-cho Musashino Tokyo 180-8585, Japan

理場所より以下の方法がある.

(1). 端末外に秘密鍵を保存

端末に秘密鍵を保存せず、外部に秘密鍵を保存して、端末へ秘密鍵を移動する. 鍵の保存場所としては、2つの場所がある.

(1-1). 外部記憶媒体(IC カードなど)

(1-2). ネットワーク上の秘密鍵管理サーバ

(2). 端末内に秘密鍵を保存

(2-1). 利用者ごとの秘密鍵を保存

利用者ごとの秘密鍵を、端末に保存して、利用者のユーザ認証で使い分ける.

(2-2). 端末ごとに1つの秘密鍵を保存

端末ごとの秘密鍵を作成し、利用者は端末の秘密鍵を使用して会議に参加する.

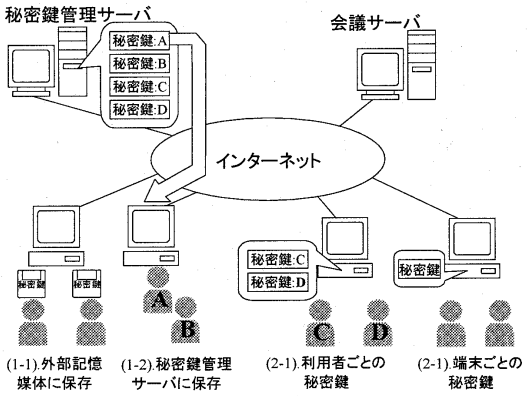

図 1:秘密鍵の管理方法

4.1.1 秘密鍵の管理方法の評価

秘密鍵の管理方法を、3章(1)の環境で秘密鍵を個人専用の端末に保存する管理方法と、セキュリティ、ユーザの操作性、システムのコストの3点について比較することで評価する.

(1-1). 外部記憶媒体に保存

媒体のコピーを防止することや、他人に使用させないなどの、媒体の管理によって、セキュリティを確保することが可能である. 使用ごとに媒体を端末にセットするだけであり、操作性は問題が少ない. フロッピーディスクの利用は低コストであるが、コピー防止などを考慮すると、IC カードなどが望ましい.

(1-2). ネットワーク上の秘密鍵管理サーバ

ネットワークに秘密鍵が流れ、セキュリティ上致命的問題がある.

(2-1). 利用者ごとの秘密鍵を端末に保存

秘密鍵が保存されている端末を複数の利用者が使用することから、3章(1)と比べセキュリティは低下するが、ユーザの操作とコストは変化しない.

(2-2). 端末ごとの秘密鍵を保存

複数の利用者が同じ秘密鍵を利用することから、利用者の区別ができない. そのため3章(1)と比べセキュリティは低下するが、ユーザの操作とコストは変化しない.

表 1. 秘密鍵の管理方法の評価

	A	B	C
(1-1)外部記憶媒体に保存	○	△	△
(1-2)ネットワーク上のサーバに保存	—	—	—
(2-1)利用者ごとの秘密鍵を保存	×	○	○
(2-2)端末ごとの秘密鍵を保存	×	○	○

A: セキュリティ
B: ユーザの操作性
C: システムのコスト

4.2 単一利用者の複数端末利用

この場合の秘密鍵の管理方法は、前述の(1-1)、(2-2)の方法である. (2-1)の方法で、複数の端末から利用可能にするには、ネットワークや外部記憶媒体を用いて秘密鍵を複数端末に保存する必要があるので、解決方法としては(1-1)や(1-2)と同じである.

5 考察とまとめ

本論文では、資料を共有する会議システムの利用者の環境に適した秘密鍵の管理方法について検討した. その結果として、外部記憶媒体に秘密鍵を保存する方法が本システムの運用に適していることが分かった.

今後は、システムに実装し有効性を検証して行く.

参考文献

[1] 横森他:“プレゼンテーション型新世代会議支援システムの実装と評価”、NTTR&D、Vol48、No.6、1999

[2] 横森他:“インターネット対応型会議支援システムにおけるセキュリティ機能に関する提案”,電気通信学会、OFS、Jun 27,2000