グループ内メンバのための認証書更新情報配布方式[1]

5 G − 2

河内 清人, 地引 尚史, 佐納 成重, 米田 健[2]
三菱電機(株) 情報技術総合研究所[3]

1. はじめに

現在、S/MIME[1]等のセキュアメールアプリケーションを用いて組織内にセキュアメール環境を構築する動きが盛んである。企業内での使用を狙ったCAサーバ製品等も続々と登場してきている。

しかし、組織内セキュアメール環境に固有の問題が存在することは、今まで考慮されたことは無かった。本稿ではこの点に着目し、問題解決のための一手法を提案し、実装したので報告する。

2. 組織内セキュアメール環境

2.1 セキュアメール環境

本稿では公開鍵認証書を用いて従来の電子メールに暗号学的な保護を与えたものをセキュアメールと呼び、セキュアメールによる安全な情報交換を実現した環境をセキュアメール環境と呼ぶ。

一般的なセキュアメールアプリケーションは次に挙げるような機能を有している。

- 認証書の入出力
- 認証書と、人物との関連付け
- 人物の集団としてのグループの設定と、グループに対する暗号化

これらを前提として、はじめに組織内で構築されたセキュアメール環境の持つ特徴について述べる。

2.2 組織内セキュアメール環境の特徴

組織におけるセキュアメール環境においては、第一に組織外に対しての情報の漏洩を防ぐ必要がある。

それだけでなく、部外秘や課外秘、といったように、組織内のサブカテゴリー同士であっても情報の伝達を厳しく制限する必要が生じる場合もある。

そのため、組織内の全てのメンバーは、組織に関係のある人物情報・グループ情報が、常に実世界での組織形態を反映するよう保持し続けなければならない。

このように、セキュアメール環境の全てのメンバーに対して、メンバーの意志とは関係なく、更新作業が発生することが、組織におけるセキュアメール環境の最大の特徴であると言える。

2.3 組織内セキュアメール環境における問題点

2.3 節で述べた通り、組織におけるセキュアメール環境を維持していくために、メンバーは各自の認証書情報、人物・グループ情報を更新しなければならない。

さらに、大多数の企業や官公庁では、頻繁に組織の変更が行われる。従って、これらの組織では、各メンバーの更新作業も頻繁に行われなければならない。

ところが、従来のセキュアメールアプリケーションでは、ユーザーの意志とは無関係な更新作業が発生することを想定していない。そのため、メンバーは、必要とされる更新作業を全て自らが理解し、処理しなければならない。

これらの検討を踏まえ、組織におけるセキュアメール環境を構築するためには、更新作業にともなうメンバーの負担の軽減が不可欠である、との結論に達した。

そこで、本稿では、更新情報配布方式によるメンバーの更新作業の簡略化を提案する。次節で本方式について説明していく。

3. 更新情報配布方式

更新情報配布方式とは、更新作業をセキュアメー

---

[1] A Certificates Distribution Method for Organized Members
[2] KAWAUCHI Kiyoto, JIBIKI Hisashi, SANOH Narushige, YONEDA Takeshi
[3] Mitsubishi Electric Corporation, Information Technology R&D Center
5-1-1, Ofuna, Kamakura, Kanagawa, 247, Japan

ル環境の管理者が集中的に行い、結果のみを各メンバーに配布する方式である。

この方式を採用することで、組織内のメンバーは、どんな組織変更があったにしても、管理者の配布する更新情報を読み込むだけの作業しか発生しなくなる。

3.1 システム構成要素

本方式におけるシステムの構成要素を図1に示す。本方式では、暗号化メールアプリケーションに加えて、更新情報管理サーバを設ける事を特徴としている。このサーバ上で更新情報は一括生成され、ネットワーク等を通じて各メンバーに配布される。

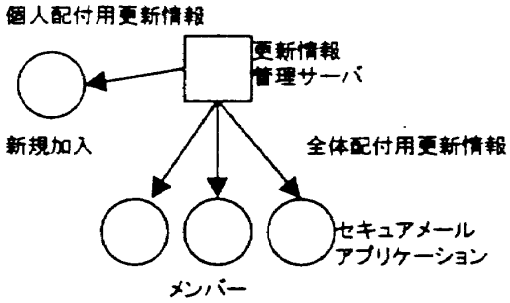

図 1 構成要素

3.2 更新情報

本方式では、2種類の更新情報を使用する。

- 新規配布用更新情報

  組織に加入してきた人物に対して生成される。この更新情報には、メンバー全員の認証書情報と、全ての組織構造情報(人物+グループ情報)が含まれる。

- 全体配布用更新情報

  組織に変更があった時に、メンバー全員に対して生成される。この更新情報には、認証書情報、組織構造情報が受けた変更に関する情報が含まれている。

全体配布用更新情報における、組織の変更の表現方法は、実装に依存する議論であるが、差分表現等を用いて極力小さくする事が望ましいと考えられる。

3.3 更新情報の保護

偽の更新情報を第三者によって配布される事で、本システムは容易に攻撃を受ける可能性がある。そのため、各更新情報には管理者によるディジタル署名を付加する必要がある。

しかし、新規配布用更新情報の場合、受信者は組織に新しく加入した人物である為、管理者の認証書に関する情報も持っていない。そのため、新規加入者に対してはあらかじめ管理者の認証書を信頼できるチャネルで配布しておく必要がある。

4. 実装

本研究では、3節で示した方式を実装し、製品化を行った。本節では実装上で行った幾つかの選択について述べる。

4.1 動作環境

サーバ、セキュアメールアプリケーションともにWindows 95, NT 4.0で動作する。

4.2 全体配布用更新情報での更新情報

認証書に関しては、変更によって新たに追加されたもののみを含むようにした。削除された認証書の情報は含まれない。これらは暗号メールアプリケーション内で組織構造情報と照らし合わせる事で検出され、削除される。

今回の実装では、組織構造情報は、毎回全組織情報を配布している。

4.3 更新情報の保護

更新情報を保護する為に、更新情報を PKCS #7 SignedData 形式で署名を行った。

この形式では、署名者の認証書を付加できる。この領域を利用して新規加入者に管理者の認証書を配布する方式を採用した。

新規加入者にはあらかじめ認証書のフィンガープリントが通知されるので、更新情報を受信した時に確認する事が可能である。

5. まとめ

組織内でのセキュアメール環境で、メンバーが行わなければならない更新作業を軽減する手法を提案した。今後は、管理者認証書のセキュアな配布方法、より効率の高い全体配布用更新情報の生成法、を検討していく予定である。

参考文献

[1] RFC 2311 S/MIME Version 2 Message Specification