企業情報向けグループ暗号システム(1)　暗号鍵管理方式

1S－6　洲崎 誠一　伊藤 浩道　荒井 正人　梅木 久志　森藤 元
(株) 日立製作所　システム開発研究所

1．はじめに

インターネットワーキング時代の到来により，電子メールやWWWシステムを中心とするインターネット技術・サービスを積極的に取り入れ，情報共有システムや広域情報網を構築する企業が増えてきている。このようなコンピュータネットワークにより，多くのメリットが生まれる一方，情報漏洩といったセキュリティ上の問題も増加する。そのため，これら企業では情報の機密保護を目的とした暗号技術の利用機会が増えている。

以上のような動向を踏まえ，筆者らは，情報の開示先を個人名，所属，役職などのID情報やその組合せで指定可能なグループ暗号システムを開発した。本グループ暗号システムは，① セキュアカードと呼ぶ物理的に安全なモジュールを用いてグループ鍵を生成する処理（暗号鍵管理）と，② そのグループ鍵でファイルサーバやWWWサーバ上の共用ファイルを暗号化する処理（共用ファイル暗号化）からなる（図-1）。本稿では，上記暗号鍵管理方式について報告する。なお，共用ファイル暗号化方式に関しては文献1を参照されたい。

2．暗号鍵管理における課題

暗号は情報の機密保護を実現する有用な手段の一つであるが，システムが大規模化するに連れて暗号鍵の管理が煩雑になるという課題がある。この課題に対して，従来よりいくつかの方式が提案されており[2]，その一つとしてユーザーの名前などから暗号鍵を生成する，いわゆるIDベース鍵配送方式がある。一方，企業では本人よりもその人の所属や役職などにより情報にアクセスできるかどうかが決まる場合が多い。しかし，従来方式では，このように利用者の所属や役職に基づいて暗号化することは考えられていない。さらに，「部長以上全員」などといった企業の階層構造を考慮した情報の開示先指定も困難である。

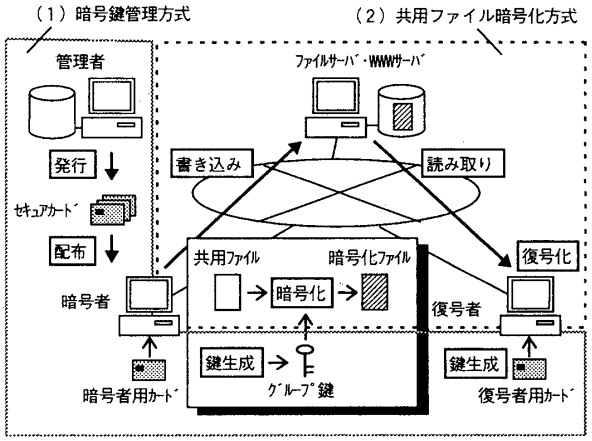

図-1　グループ暗号システム

3．実現方式

3．1　概要

上記課題を解決するため，情報の開示先である宛先リストを名前，所属，役職などの組合せによって作成し，その宛先リストを基に生成したグループ鍵で情報の暗号化を行う。また，安全性を高めるため，暗号鍵生成に係わる全ての処理はセキュアカード内部で行う。

開発にあたっては，暗号に関する専門的な知識を持たないエンドユーザーが使いやすいようGUIを具備したユーティリティも併せて開発した。

3．2　実現方式

（1）ID情報の割り当て

ID情報は，カテゴリ，データ，コードから構成した(図-2)。カテゴリ種別と各データに対応するコードは，システム導入時に管理者が決定する。各ユーザーには，そのユーザーのデータを書き込

Group Cipher Method for Enterprise Information System (1)
- Key Management -
Seiichi SUSAKI, Hiromichi ITO, Masato ARAI,
Hisashi UMEKI, Hajime MORITO
Systems Development Laboratory, Hitachi Ltd.

んだものをセキュアカードに入れて配布する。コードは，宛先リストのデータ量削減，および「部長以上全員」などといった企業の階層構造を考慮した開示先指定を可能とするために設けた。また，一人のユーザーが複数の ID 情報を持つことを許すことで，役職の兼務などに対応可能とした。

	カテゴ	データ	コード
1	氏名	日立太郎	
2	生年月日	19650101	
3	性別	男性	M
4	社員番号	871010001	
5	事業所	東京本社	001
6	部	総務部	S
7	課	経理１課	K1
8	役職	係長	7
⋮	⋮	⋮	⋮

図-2　ID 情報

（2）宛先リストの作成

宛先リストは，各カテゴリを条件式で連結した形で表現した。具体的には，

カテゴリ番号　演算子　データまたはコード

を一纏まりとし，それらを‘^’や‘,’で区切って並べた。これらは AND 演算および OR 演算である。例えば，上記 ID 情報構成で，東京本社総務部の係長以上全員と日立太郎を開示先とする場合，以下のような宛先リストを生成する。

5C=001^6C=S^8C<=7, 1D=日立太郎

ここで，カテゴリ番号の次の‘C’および‘D’は，演算子に続くものがコードであるかデータであるかを意味する。

（3）グループ鍵の生成

① 宛先リストと ID 情報との照合

入力された宛先リストの各条件について，セキュアカード内に格納されたカード所有者の ID 情報と合致するかどうかチェックする。条件を満たすときは処理を継続し，それ以外はグループ鍵を生成せずに処理を終了する。

② グループ鍵の生成

宛先リストとマスタ鍵を連結したものを，MULTI2 暗号[3]をカスケード接続したハッシュ関数を用いて圧縮し，グループ鍵を生成する(図-3)。このマスタ鍵は，セキュアカード内に格納された全カード共通の秘密数値であり，管理者がシステム導入時に決定する。これをグループ鍵の構成要素とすることで，不正者がセキュアカード外部に偽のグループ鍵生成ロジックを作ることを防いだ。

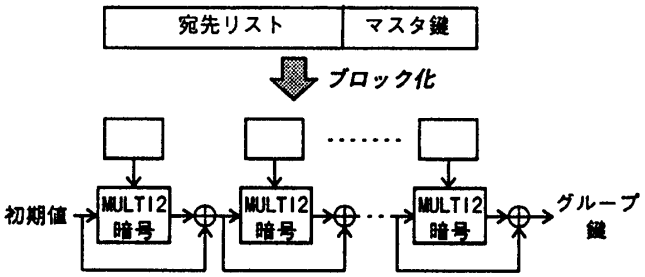

図-3　グループ鍵の生成

（4）暗号化情報の構成

グループ鍵で情報を直接暗号化した場合，情報の開示先を変更する度に再暗号化が必要となる。そこで，ランダムに生成したデータ鍵をグループ鍵で暗号化し暗号化情報のヘッダ部に付加することとした。これにより，情報の開示先変更がヘッダ部の再暗号化のみで対処可能となった。

4．おわりに

本稿では，グループ暗号システムの暗号鍵管理方式について述べた。本方式に対する攻撃手段としては，宛先リストチェックの無効化や ID 情報の改竄，マスタ鍵の漏洩等が考えられるが，それら全てをセキュアカード内に閉じこめることで上記不正を防いだ。これにより，安全性を確保しつつ，情報の開示先を個人名，所属，職位およびそれらの任意の組み合わせで指定可能にするなど，ユーザーの利便性向上も図れた。

参　考　文　献

[1] 伊藤，洲崎，荒井，梅木，森藤，“企業情報向けグループ暗号システム(2)共有ファイル暗号化方式”，情報処理学会第 52 回全国大会，1S-7，1996(本大会にて発表予定)

[2] 岡本，“暗号理論入門”，共立出版，1993

[3] 宝木ほか，”マルチメディア向け高速暗号アルゴリズム Hisecurity-Multi2 の開発と利用方法，1989 年情報理論とその応用，暗号と情報セキュリティジョイントワークショップ資料，電子情報通信学会，167-173(平 1-8)