企業情報向けグループ暗号システム

荒井正人[†] 鍛忠志[†] 伊藤浩道[†]
手塚悟[†] 佐々木良一[†]

インター/イントラネットやモバイルコンピューティングを活用した企業情報システムの普及にともない，情報セキュリティに対するニーズが高まっている．特に企業内で扱う情報には，企業の組織構造等に基づいたアクセス制御が求められる．このニーズに応えるために，報告者らは，情報開示先を組織構造やユーザのID情報に基づいて柔軟に設定可能なグループ暗号システムを開発してきた．本システムは，ユーザのID情報管理のみでなく，機密情報へのアクセス権チェックや鍵生成処理をICカードの中で行うものである．したがって，組織の編成や個人のID情報に変更が発生した場合，該当者のICカードを更新する必要があった．そこで組織情報やID情報の管理を容易化するために，前記処理をICカードの代わりにサーバマシン上のソフトウエアで実行する方式を考案した．本論文では，サーバ版の実装方式やWWWへの応用システム，および前記ICカード版との比較について記述しながら，その機能と有用性について報告する．

Group Cipher System for Enterprise Information System

MASATO ARAI,[†] TADASHI KAJI,[†] HIROMICHI ITO,[†] SATORU TEZUKA[†] and RYOICHI SASAKI[†]

Due to the rapid growth of the Internet/Intranet and mobile computing, the WWW (World Wide Web) has emerged as a means of handling enterprise information. Under such trends of the WWW, there arose strong demands on information security appropriate for enterprise organizations. As a solution for these demands, we had developed the Group Cipher System (GCS) that enables users to specify flexibly the accessible range of information based on the organizations and user's identity (ID) information. In this system, every user possesses his or her smart card, which stores the owner's ID information and has other functions, such as checking access right to information, and generating keys. This system, however, required the renewal of the card when a reshuffling of the sections or a change in one's ID occurred. To facilitate the maintenance of such information, we have developed a method that executes the functions of the smart card on the server side program instead. In this paper, we will explain about its capability and usability by describing the implementation of this method, its application to the WWW network system, and comparison with the GCS smart card version.

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企業内のみでなく企業間で構築するケースが増えてきている．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で，情報漏洩といったセキュリティ上の問題も増加する．その対策として，ファイアウォールやSSL[8]等各種セキュリティ製品や技術が発表されており，それらを実際に導入しているサイトも少なくない．これらの技術は，外部ネットワークからの侵入や情報流出の防止に有効である．

一方，企業内の情報ネットワークにおいては，上記セキュリティ対策のほかに，情報（WWWコンテンツ等）ごとのきめ細かなアクセス制御への要求が強まっている．これは，たとえばあるコンテンツについては「開発部の主任以上」のみアクセス可能とし，また別のコンテンツについては「部長全員と営業部の日立太郎」のみアクセス可能というように，企業の組織に対応した開示先設定である．

報告者らはこのようなニーズに応えるために，暗号を利用したアクセス制御技術として，情報の開示先をユーザの氏名，所属，役職等のidentity（ID）情報や，

† 株式会社日立製作所
Hitachi, Ltd.

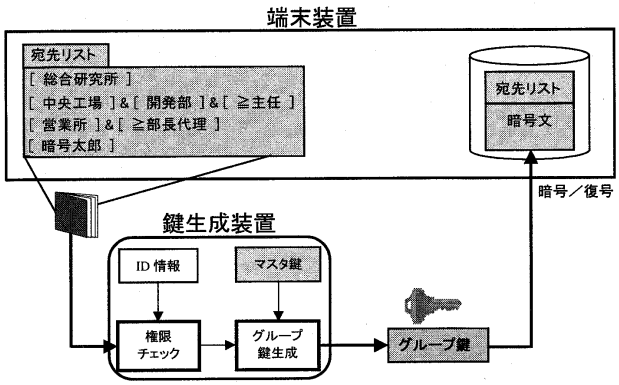

図1 グループ暗号システムの概要
Fig. 1 Overview of group cipher system.

企業の組織構造に基づいて柔軟に指定可能なグループ暗号システムを開発し，その機能とイントラネット環境での有用性について報告してきた[1)~3)]．グループ暗号システムでは，ユーザの ID 情報と暗号/復号鍵生成プログラムを IC カードに格納して配布する．したがって，組織の編成や個人の ID 情報に変更が発生した場合に，IC カードに格納された情報を更新する必要がある．前記文献 1) では，LAN を経由した ID 情報の自動更新について簡単に記述しているが，カードの所有者であるユーザが自主的に更新作業を実施する必要があり，変更がすべてにいきわたるには時間を要する．また，ユーザが IC カードのほかにカードリーダを端末に装備しておく必要があり，ユーザ数の多い大規模なシステムでは導入コストの面でも問題があった．

そこで，組織情報や ID 情報のメインテナンス容易化と導入コスト削減を図るために，ID 情報の管理と暗号/復号鍵生成機能をサーバマシン上のプログラムで行う方式を新たに考案した．本論文では，サーバ版グループ暗号システムの実装や WWW（World Wide Web）システムへの応用，および IC カード版との比較について記述しながら，その効果と有用性について記述する．

2. グループ暗号の鍵管理

2.1 概　　要

グループ暗号システムの概略を図1に示す．グループ暗号システムでは，宛先リストとシステム固有のマスタ鍵とから生成したグループ鍵を用いて情報を暗号化する．宛先リストとは，情報の開示先となるユーザ名およびグループ名のリストであり，暗号化情報のヘッダーに付加される．

表1 ユーザの ID 情報
Table 1 An user Identity information.

No.	カテゴリ	データ	コード
1	氏名	山田 一郎	
2	生年月日	1960/11/07	19601107
3	性別	男性	M
4	事業所	システム開発本部	301
5	部	製品企画部	3
6	役職	主任	9

復号化処理時には，権限チェックプログラムが暗号化情報のヘッダーから宛先リストを取り出し，復号化を試みるユーザの ID 情報が宛先リストに含まれるか否かを確認する．このとき，含まれていればグループ鍵生成プログラムがグループ鍵を生成し，含まれなければ生成しない．なお，グループ鍵は共通鍵暗号に用いる鍵であるため，復号化するときに生成する鍵は，暗号化に用いた鍵と同一である．

このように，グループ暗号システムは暗号化または復号化処理時に鍵を動的に生成するものであり，ユーザがいくつもの鍵をつねに所持しておく必要がないという特長がある．また，宛先リストはユーザ名称のほかに役職，所属部署名等が含まれ，それらが論理演算子によって連結されたものである．このように宛先リストは，企業内の任意のグループを表現可能であり，管理者があらかじめ定義しておく必要はない．

2.2 ID 情 報

ユーザには，グループ暗号システムを利用する際に必要となるユーザ識別子とパスワードを発行する．また，各ユーザ識別子には ID 情報を関連付けて管理する．ID 情報は，表1に示すようにカテゴリ，データ，コードから構成した個人情報であり，ユーザプロファイルとも呼べるものである．

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」等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，1ユーザにつき複数のID情報の登録を許すことで，同一ユーザが複数の役職を兼務するケース等にも対応可能としている．

2.3 宛先リスト

グループ暗号システムでは，ユーザが情報を暗号化する際に，情報の開示先となるユーザもしくはグループを宛先リストとして指定する．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．

をひとまとまりとし，それらをAND演算子‘^’やOR演算子‘，’で区切って並べる．その他，<，>，=，<=，>=，<>（不等号）を使えば「部長以上全員」等といった範囲指定も可能である．たとえば，製品企画部の主任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．

6C >= 9 ^ 5C = 3, 1D = "日立 太郎".

ここで，6C >= 9は，役職（カテゴリ番号6）が主任（コード9）以上のユーザを意味する．このような階層構造を考慮した開示先指定を可能とするためには，数値の大小が階層の上下を表すように，管理者があらかじめコードを割り当てておけばよい．次に5C = 3は，所属の部（カテゴリ番号5）が製品企画部（コード3）のユーザを意味する．さらに，1D = "日立 太郎"は，氏名（カテゴリ番号1）が日立太郎（データが"日立太郎"）のユーザを意味する．また，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．ユーザは，グループ暗号独自のユーティリティを利用して宛先リストを指定することとなる．またこのユーティリティは，ユーザが指定した宛先リストにユーザ本人の情報を付加する．これは，情報を暗号化したユーザが，その情報を復号化できるようにするためである．

2.4 グループ鍵生成

グループ暗号システムでは，宛先リストに乱数を連結したものを，1方向性のハッシュ関数とマスタ鍵により圧縮し，グループ鍵を生成する（**図2**）．ハッシュ関数には，MULTI2ベースのハッシュアルゴリズムを採用した[4),5)]．乱数は，宛先リストのサイズをMULTI2のブロックサイズの整数倍にするために付加する．また，乱数を付加することで同じ宛先リストでも生成するグループ鍵が毎回異なり，セキュリティを向上できる．

ここで，マスタ鍵はシステム固有の秘密数値であり，

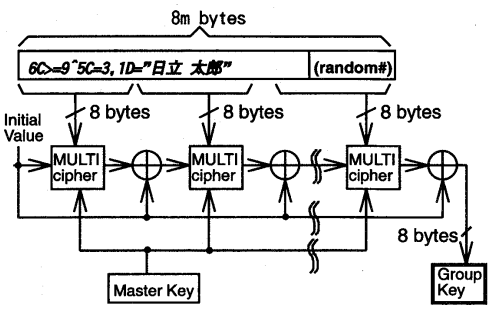

図2 グループ鍵生成
Fig. 2 Group key generation.

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，不正者によるグループ鍵生成ロジックの偽造を防いだ．

3. グループ暗号システムの実装

グループ暗号システムの構成を**図3**に示す．本システムを実現するために，以下のプログラムをWindows™ 95☆用に開発した．

(1) 管理者ユーティリティ

管理者向けに以下の機能を提供する．

- マスタ鍵の登録
- カテゴリとコードの定義
- 各ユーザのID情報登録
- ID発行：ICカード版ではICカード発行，サーバ版ではユーザ識別子とパスワード登録となる．

(2) エンドユーザユーティリティ

エンドユーザ向けに以下の機能を提供する．

- 鍵生成装置へのログイン，ログアウト
- 宛先リストの生成

(3) Secure File

グループ暗号による共有ファイルの暗号および復号機能を提供する．Secure Fileは，手動暗号機能のほかに自動暗号機能を含む．自動暗号機能は，ファイルI/Oをつねに監視し，ハードディスクへの書き込み要求があれば，グループ鍵を用いて書き込みデータを暗号化する．反対に読み出し要求があれば，グループ鍵を用いて読み出しデータを復号化する．自動暗号の対象範囲は，ユーザが任意のディレクトリ単位で指定できる．

(4) Secure WWW

プロキシサーバと同様な動作により，ブラウザとWWWサーバ間の通信データを監視し，WWWサー

☆ Windowsは米国Microsoft Corporationの商標です．

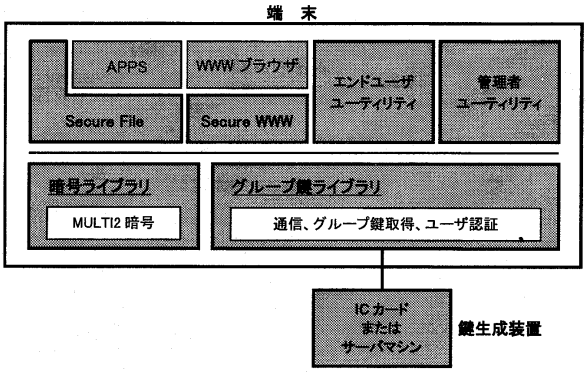

図3 グループ暗号システムの構成
Fig. 3 Group cipher system architecture.

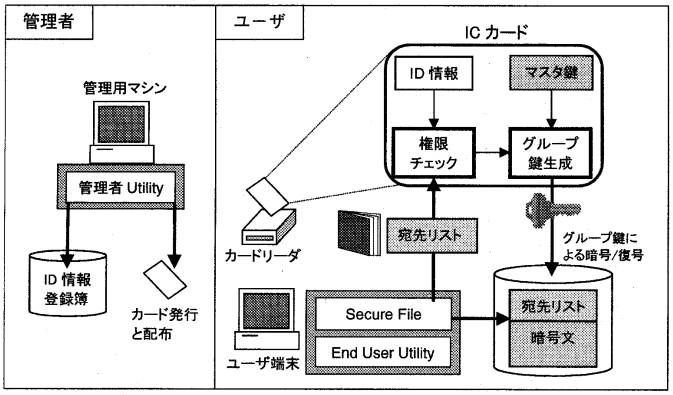

図4 IC カード版グループ暗号システムの構成
Fig. 4 Group key generation on smart card.

バから受信した暗号化ファイルを復号化してからブラウザへ転送するプログラム．これにより，復号権利を持つユーザは，通常の HTML ファイルへのアクセスと同様にして暗号化 HTML ファイルを閲覧できる．

(5) 暗号ライブラリ

共通鍵によるデータ暗号・復号用 API を提供する．暗号アルゴリズムには MULTI2 を採用したが，本システムにおける鍵管理は暗号アルゴリズムの種類に依存しないので，他の共通鍵暗号アルゴリズムと置き換えることも可能である．

(6) グループ鍵ライブラリ

鍵生成装置へのユーザ認証処理やグループ鍵要求等のコミュニケーションに必要な機能を提供する．

(7) 鍵生成装置

鍵生成装置には，マスタ鍵や ID 情報のほか，権限チェックやグループ鍵生成機能を搭載する．鍵生成装置として IC カードを利用した方式についてはすでに報告している[1)~3)]．IC カード版グループ暗号システムでは，ID 情報とマスタ鍵のほか，権限チェックプログラムとグループ鍵生成プログラムを，管理者が IC カードに格納してユーザへ配布する．このシステムの特徴は，IC カード自身が持つ耐タンパー性により，上記プログラムや情報を不正アクセスから保護できることと，IC カードの演算機能を用いてグループ鍵を生成するところにある．また，IC カードにはユーザパスワードを設定し，システム利用の際にはパスワード入力によるユーザ認証を行う．IC カード版グループ暗号システムの構成を図 4 に示す．

この IC カード版に加え，鍵生成装置として通常のサーバマシンを利用したシステムを新たに設計・開発した．4 章では，サーバ版グループ暗号システムについて報告する．

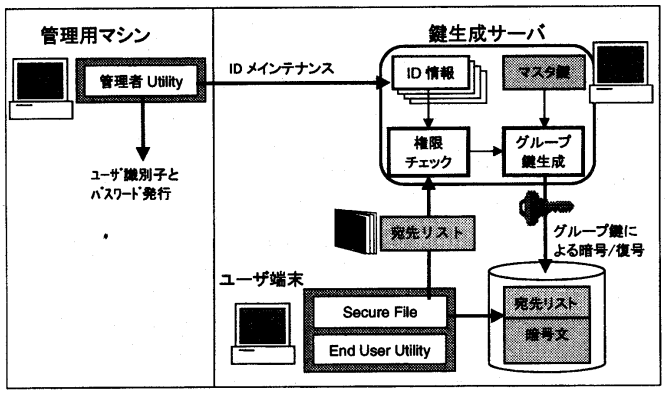

図5 サーバ版グループ暗号システムの構成
Fig. 5 Group key generation on server machine.

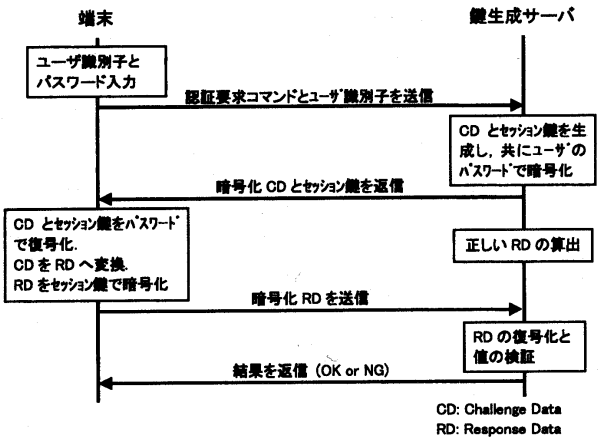

図6 CHAP によるユーザ認証
Fig. 6 User authentication based on CHAP.

4. サーバを利用したシステム

4.1 システム構成

サーバ版では，たとえば社内の部門サーバ等に前記鍵生成装置の機能を実装する．このサーバを鍵生成サーバと呼び，図5に示すように，権限チェックプログラムとグループ鍵生成プログラムを格納し，マスタ鍵と ID 情報を集中管理する．また，ユーザへは IC カードの代わりにユーザ識別子とパスワードを発行する．なお，サーバ OS としてはファイルのアクセス制御機能や監査機能を持つ Windows^{TM} NT を採用した．

4.2 鍵生成サーバの機密性

サーバ版のシステム構成では，鍵生成サーバを物理的に安全な部屋に設置するとともに，サーバ OS が持つアクセス制御機能により上記プログラムや情報を不正利用されないよう保護することで，上記プログラムや情報の不正な書き換えおよび読み取りを防止できる．

4.3 端末と鍵生成サーバ間の経路保護

サーバ版のシステム構成では，ユーザ端末と鍵生成サーバを結ぶネットワーク上を宛先リストやグループ鍵が転送されるため，通信データの盗聴・改ざん等によるセキュリティ脅威が発生する．そこで，システム利用の際には，たとえば CHAP (Challenge-Handshake Authentication Protocol)[6]によりパスワードを平文で送信することなくユーザ認証を行うとともに，端末と鍵生成サーバ間でセッション鍵（一時的に利用する鍵）を共有し，以後の通信データをすべて暗号化することとした．CHAP の概略を図6に示す．

表2 ICカード版とサーバ版の評価
Table 2 Evaluation of the smart card version and the server version.

#	評価項目	ICカード	サーバマシン
1	マスタ鍵とID情報の安全性	A（ICカードの特性に依存）	C（運用や環境に依存）
2	マスタ鍵とID情報の管理負担	D（分散管理）	A（集中管理）
3	導入コスト	D	B
4	モバイル対応	A	D
5	ユーザ認証の安全性	B（所有 + 知識）	C（知識）

評価の見方 A：非常に優れている，または最適
B：優れている
C：特に問題なし
D：問題あり，または不適

5. 方式比較

前記ICカード版とサーバ版を，5つの項目について比較する．また，報告者らによる主観的かつ相対的な評価を**表2**に示す．

5.1 情報の機密性と完全性

ICカードの場合，その媒体としての耐タンパー性[10]により，マスタ鍵やID情報を不正アクセスから保護できる点で優れている．一方，サーバ方式の場合は鍵生成サーバのOSが有するセキュリティ機能の強度やサーバの管理方法，および物理的な環境等によって強度が変化するといえる．

5.2 管理の容易さ

ICカードを企業内あるいは企業間システムで使用する場合，役職や所属部署名等個人のID情報が変更されたときにカードの回収と再発行が必要となる．文献1)では，LANを経由したID情報の自動更新について簡単に記述しているが，カードの所有者であるユーザが自主的に更新作業を実施する必要があり，変更がすべてにいきわたるまでには時間を要する．企業では，組織や人事の変更にともなうID情報の書換えが頻繁に起こりうるため，企業情報システムには鍵生成サーバによるID情報の集中管理が特に有効であるといえる．

ただし，氏名や性別，個人識別番号，生年月日等，一生を通じて変更されない，あるいは変更の頻度が少ない情報のみをID情報として登録するならば，ICカードを利用しても管理上大きな支障はないと考える．

5.3 導入コスト

ICカードを利用する場合，すべてのユーザにカードを配布し，すべての端末にカードリーダを装備することになる．したがって，ユーザ数の多い大規模なシステムでは導入コストの面で問題がある．一方，サーバ方式の場合，現在使用しているサーバ機器があればソフトウェアをインストールするだけでよい．

5.4 モバイル環境への対応

インターネットを経由して社内のリソースへアクセスする場合，ICカードを利用すれば権限チェックとグループ鍵生成を端末側で実行できるが，サーバ方式であれば，暗号化情報へアクセスするたびにインターネット側から鍵生成サーバへの通信が発生する．システム全体のセキュリティを考慮すれば，インターネット側に提供するサービスはファイアウオール等を利用して極力少なくすることが望ましい．つまり，鍵生成サーバへのポートもインターネット側には提供しないことが望ましいことから，モバイル環境ではICカード版が適しているといえる．

5.5 ユーザ認証の安全性

ICカード版におけるユーザ認証は，ICカードを所持していること（所有）と，パスワードを知っていること（知識）の2つの条件が揃っている場合に成立する．したがって，ユーザ識別子とパスワードを知っている（知識）だけで認証が成立するサーバ版と比べ，セキュリティ面で優れているといえる．

ただし，グループ暗号システムにおける権限チェック処理とグループ鍵生成処理は，ユーザ認証手段に依存しないメカニズムとなっている．したがって，ユーザ認証手段として，パスワードの代わりに指紋等の生体認証を組み込むことも技術的には可能である．

5.6 総合評価

ID情報の集中管理が可能であることから，ユーザが数百人，数千人規模のシステムでは，サーバ方式が適している．一方，モバイルコンピューティングやスタンドアロンの環境でファイル暗号・復号を行うにはICカード方式が適している．今後，ICカードが普及すればコストの問題も解消されるかもしれないが，現

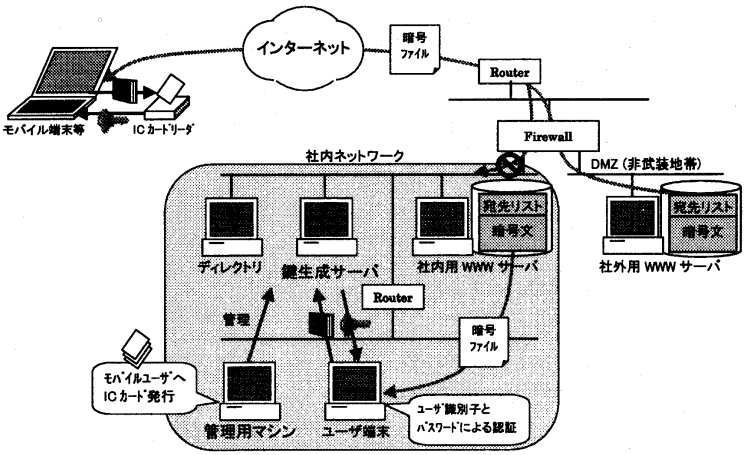

図7 WWWへの適用例
Fig. 7 Example of an application for WWW system.

時点でのICカードやそのリーダの価格と，一般的なサーバ機器の価格を考慮すると，ユーザ数が数十人程度の小規模なシステムで，かつサーバ機器を安全に管理する環境がなければ，ICカード版が適していると考える．このように，どちらが優れているか一概にはいえず，システムの規模や環境，および用途によってICカード方式とサーバ方式を使い分けることが望ましい．このICカードと鍵生成サーバの混在システムを，WWWへの適用例として6章で記述する．

6. WWWへの適用例

グループ暗号システムの適用例として，WWWコンテンツのアクセス制御について以下に記述する．なお，WWW環境におけるグループ暗号システムの有効性については，文献1)，3)ですでに報告済みである．本論文では，ICカード版とサーバ版が混在するシステムを例示しながら，用途に応じた使い分けとその効果について記述する．

6.1 モデルシステムの構成

機密情報を社内（イントラネット）だけでなく，社外（インターネット）からもグループ暗号を用いて安全に共有可能なシステムをモデルとして説明する．

モデルシステムでは，**図7**に示すように，共有する機密情報をすべて暗号化してWWWサーバに格納しておく．WWWサーバについては，社内用と社外用に分け，ファイアウオール等を用いて社外用WWWサーバのみ社外からアクセス可能となるよう配置する．

また，社内から機密情報へアクセスする際には，鍵生成サーバを用いてグループ鍵を生成し，社外から機密情報へアクセスする際にはICカードを利用する．したがって，社外で利用する端末にはICカードリーダを装備することとなる．さらに，端末の環境設定ファイルの中に，現在有効な鍵生成装置のタイプを記述しておく．たとえば，社外で使用する場合は，ICカードリーダへの通信ポートを記述しておき，社内で使用する場合は，鍵生成サーバのIPアドレスとポート番号を記述することになる．前記グループ鍵ライブラリは，この情報を基にアクセス対象となる鍵生成装置を識別できる．

6.2 運用イメージ

鍵生成サーバは物理的に安全な部屋に設置し，部屋への入退室を厳重に管理する．

管理者は，管理者ユーティリティを用いて組織情報を定義し，所属名や役職等にコードを割り当てる．また，社内ユーザ向けにはID情報登録を実施するとともに，ユーザ識別子とパスワードを発行する．

本モデルシステムでは，組織情報やID情報を，全社的なディレクトリサービスを活用して集中管理するため，ID情報に変更が発生した場合，管理者はディレクトリの内容を更新するだけでよい．

一方，社外からイントラネットへアクセスする必要があるユーザは，あらかじめ管理者にICカード借用を申請する．これには，出張者や他社へ出向中の者，あるいは在宅勤務等のモバイルユーザが該当する．管理者は，社外からアクセスする必要のあるユーザからの申請を受けて，申請者のID情報や各種プログラムをICカードに格納し，パスワードを設定した後でカードリーダとともにユーザへ期限付きで貸し出す．

6.3 適用効果

WWW向けのセキュリティプロトコルやシステムとして，S-HTTP[7]やPCT[9]等様々なものがある．しかし，WWWブラウザの種類に依存したり，プロキシサーバにキャッシュされるファイルの安全性等の問題がある．また，SSL[8]では暗号化により通信データの機密性は保てるものの，プロキシサーバ上のキャッシュファイルの共有が不可能である．これらの技術と比べ，グループ暗号システムには以下のような利点がある．

- WWWブラウザの種類に依存しない．
- WWWサーバやプロキシサーバの種類に依存しない．
- HTTPやHTMLの仕様拡張が不要である．
- キャッシュファイルの共有と機密性を実現する．

さらに，社外からアクセスするユーザは，自己の端末に保存しているファイルをSecure Fileにより暗号化しておくことで，端末の紛失や盗難時にも機密情報の漏洩を防ぐことができる．特に，WWWブラウザがキャッシュするファイルを，Secure File自動暗号機能により暗号化しておくことは，閲覧した企業情報の漏洩を防ぐのに有効である．

7. アクセス制御技術としての考察

本章では，企業情報システムにおけるアクセス制御技術として，グループ暗号システム（ICカード版とサーバ版共通）が持つ有効性についてまとめる．

6章で示したように，WWW環境において特定のユーザやグループのメンバだけに情報を開示するのであれば，グループ暗号システムを使わなくとも，アクセス制御機能を標準で具備するOSやWWWサーバを利用する方法もある．しかし，その場合多くの企業情報システムでは以下の点で問題があると考える．

(1) マルチベンダ環境での実現が困難

実際の企業情報システムの場合，その多くが様々な種類のOSやWWWサーバが混在するマルチベンダ環境である．したがって，あるベンダのWWWサーバでACL（Access Control List）の設定をしたファイルを，異種WWWサーバの環境下に格納する場合，移動後にACLを再設定する必要がある．シームレスなアクセス制御を実現するためには，ネットワーク内で使用するOSやWWWサーバ等を統一する必要がある．

(2) 開示先の指定・定義が困難

ACLの設定とは，ユーザ単位，グループ単位にアクセス権を与えることである．管理者は，ユーザだけでなくグループについてもあらかじめ定義しておく必要がある．定義されていないグループに対してアクセス権を与える場合，そのグループのメンバに対して個別にアクセス権を与えるか，管理者に新規グループを定義してもらってから当該グループにアクセス権を与える必要がある．情報の種類によって，その共有範囲が多様に変化しうる環境にはふさわしくない．

(3) 管理者のアクセス制限が困難

一般的にファイルサーバやWWWサーバの管理者権限があれば，その中に格納されたファイルに対してアクセスが制限されていないため，本来読んではならない情報にもアクセスできてしまう．

グループ暗号システムでは，これらの課題を以下に示すように解決できる．

(1) マルチベンダ環境への対応

開示範囲を宛先リストとして暗号化情報のヘッダーに付加することで，ファイルサーバやWWWサーバの種類に依存しないアクセス（開示）制御が可能となる．ただし，端末側に実装するプログラムは，端末のOSの種類に応じて用意しなければならない．

(2) 柔軟な開示先設定

情報発信者がその開示先を組織情報やID情報から任意に定義可能とすることで，管理者があらかじめすべてのグループや鍵を定義する必要がなくなるという利点がある．

(3) 管理者のアクセス制限

情報を暗号化することで，ファイルサーバやWWWサーバの管理者であっても，宛先リストに含まれなければ復号化できないため，情報を読むことができない．

8. おわりに

ファイルの共有範囲を，企業の組織にあわせて柔軟に設定可能とするグループ暗号システムを開発した．特に，従来ICカードに実装していた機能をサーバマシンに実装することで，大規模システムにおけるID情報のメインテナンス容易化と，導入コスト削減を達成できた．また，ICカード版とサーバ版の特長を明確にし，その特長を活かしながら互いに共存できることをWWWへの適用例を用いて示した．さらに，マルチベンダ環境に対応できるアクセス制御技術であることを示した．

一方課題としては，暗号化によりWWWコンテンツのメインテナンスが煩雑になりやすいことがあげられる．これについては，暗号化情報に対する宛先確認ツールやファイル再暗号処理の自動化等により対処できると考える．また，WWWへの適用には，CGI等

が生成するアクティブコンテンツへの対応が不可欠であるが，本論文で報告した方式では十分に対応できない．これについては，宛先リストに基づいたアクセス制御機能をWWWサーバ側に組み込む等，その実現方式を引き続き検討していきたい．

謝辞 本研究の推進にあたり，(株) 日立製作所システム開発研究所片岡雅憲所長をはじめ関係者各位のご指導に深謝する．

参考文献

1) Ito, H., Susaki, S., Arai, M., Koizumi, M. and Takaragi, K.: Group Cipher System for Intranet Security, *Trans. IEICE*, Vol.E81-A, No.1, pp.28–34 (1998).
2) 洲崎ほか：企業情報向けグループ暗号システム (1) 暗号鍵管理方式，第52回情報処理学会全国大会論文集 (4)，1S-6, pp.355–356 (1996).
3) 伊藤ほか：企業情報向けグループ暗号システム (2) 共用ファイル暗号化方式，第52回情報処理学会全国大会論文集 (4)，1S-7, pp.357–358 (1996).
4) Takaragi, K., Hashimoto, K. and Nakamura, T.: On Differential Cryptanalysis, *Trans. IEICE*, Vol.E74, No.8, pp.2153–2159 (1991).
5) IPA/Hitachi Ltd.: MULTI2, ISO/IEC 9979 register of cryptographic algorithm, *iso standard 9979 multi2 (9)*, NCC, UK (Nov. 1994).
6) Simpson, W.: PPP Challenge Handshake Authentication Protocol (CHAP), RFC 1994, Network Working Group (Aug. 1996).
7) Rescorla, E. and Schiffman, A.: The Secure Hyper Text Transfer Protocol, Internet-draft (July 1995).
8) Hickman, K. and Elgamal, T.: The SSL Protocol, Internet-draft (June 1995).
9) Benaloh, J., et al.: The Private Communication Technology Protocol, Internet-draft (Oct. 1995).
10) Security architecture of financial transaction systems using integrated circuit cards, ISO 10202-4:1996 Financial transaction cards, Part 4, Secure application modules.

(平成11年6月1日受付)
(平成11年9月2日採録)

荒井 正人（正会員）

1990年日本大学理工学部電子工学科卒業．1992年同大学院理工学研究科博士前期課程修了．同年（株）日立製作所入社．マイクロエレクトロニクス機器開発研究所を経て，システム開発研究所に勤務．インターネット，イントラネットにおけるセキュリティ技術の研究開発に従事．

鍛 忠司

1996年大阪大学大学院基礎工学研究科情報工学分野博士前期課程修了．同年（株）日立製作所入社．システム開発研究所にて企業情報システム，分散オブジェクトシステムのセキュリティに関する研究開発に従事．

伊藤 浩道（正会員）

1984年大阪大学工学部精密工学科卒業．1986年同大学院精密工学科修士課程修了．同年（株）日立製作所入社．マイクロエレクトロニクス機器開発研究所でのパーソナルコンピュータのハードウェアの研究開発，ネットワークシステムの研究開発，システム開発研究所でのインターネット，イントラネットにおけるセキュリティ技術の研究開発を経て，現在デジタルメディア開発本部に勤務．同開発本部主任技師として携帯情報端末，家庭用情報端末およびそのシステムに関する研究開発に従事．

手塚 悟（正会員）

1984年慶応義塾大学工学部数理工学科卒業．同年（株）日立製作所入社．マイクロエレクトロニクス機器開発研究所に勤務し，パーソナルコンピュータのオペレーティング・システム，デバイス・ドライバ，LANシステム等の研究開発に従事．その後，システム開発研究所に勤務，同研究所主任研究員．以来，パーソナルコンピュータを中心としたLANシステムの構築・運用管理の研究開発，さらにセキュリティシステムの研究開発に従事，現在に至る．

佐々木良一（正会員）

1971年東京大学卒業．同年（株）日立製作所入社．システム開発研究所にてシステム高信頼化技術，セキュリティ技術，ネットワーク管理システム等の研究開発に従事し，製品化に貢献．同研究所第4部部長等を経て現在主管研究長兼セキュリティシステム研究センタ長．工学博士（東京大学）．1983年電気学会論文賞受賞．1998年電気学会著作賞受賞．著書に，「情報科学入門教養としてのコンピュータ」日本理工出版会1995年，「インターネットセキュリティ基礎と対策技術」（共著）オーム社1996年，「インターネットセキュリティ入門」岩波新書1999年等．IEEE，電子情報通信学会，電気学会各会員．