コンピュータセキュリティ　1－3
（1998．5．29）

企業情報向けグループ暗号システム

荒井正人[1)]　鍛忠司[1)]　伊藤浩道[1)]　柴田利幸[2)]
1)（株）日立製作所　2)（株）日立情報ネットワーク

あらまし：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伴い，情報セキュリティに対するニーズが高まっている。企業内の機密情報保護には暗号化が有効であるが，一般に共有ファイルの暗号化には，エンドユーザーにとって鍵管理負担が大きくなるという問題がある。筆者らは，情報の開示先を個人名，所属，職位などのID情報および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，企業情報システムにおける共有ファイル暗号化に適用した。本稿では，この共有ファイル暗号化方式と，WWW(World Wide Web)への適用方式に関し，特徴と機能およびその仕組みについて報告する。

Group Cipher System for Enterprise Information System

Masato ARAI[1)]　Tadashi KAJI[1)]　Hiromichi ITO[1)]　Toshiyuki SHIBATA[2)]
1) Hitachi, Ltd.　2) Hitachi Information Network, Ltd.

ABSTRACT.　A group-oriented cipher communication method is developed and implemented on a WWW-based (World Wide Web) network system. In this method, a group key common to all entities of the group is generated based on the group name or the identities of entities belonging to the group. The group key, in turn, is used for encrypting the data being shared among the group via the WWW server. The data theft at the WWW cache sites on the intermediate communication line is prevented, establishing a unified feature of the good WWW cache performance and security. A prototype of our method proved the feasibility and the efficiency.

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，情報漏洩といったセキュリティ上の問題も増加する。例えば，企業情報を社内のWWWシステムを用いて共有する場合，その情報に対するアクセス制御や，通信路を流れるデータの保護が重要課題となる。

一般のWWWシステムでは，WWWサーバのアクセス制御機能を用いることで，登録されたユーザーのみが指定のファイルにアクセスできるようになる。また，WWWサーバとブラウザ間の通信データを保護する手段としては，SSL[8]による暗号化が有効である。

一方，企業内や企業間の情報システムにおいては，情報（WWWコンテンツ）毎のきめ細かなアクセス制御への要求が強まっている。これは例えば，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，またあるコンテンツについては「部長全員と営業部の山田一郎」のみアクセス可能というように，企業の組織に対応した設定である。

このようなアクセス権の設定を，暗号技術を利用して実現する場合，従来の鍵管理方式では，予めあらゆる組合せのグループを想定して暗号鍵を配布し，エンドユーザーがそれら暗号鍵を管理する必要があった。この鍵の数が膨大になることは目に見えており，エンドユーザーの負担を考えると企業情報システムにおいては現実的でないといえる。また，OSやWWWサーバが持つアクセス制御機能

を利用した場合についても，管理者が予め膨大な数のグループを登録しておく必要がある。

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，その開示先となるグループ情報と，システム固有のマスタ鍵とから，暗号化・復号化に必要なグループ鍵を動的に生成するものである。これにより，エンドユーザーの負担（暗号鍵管理）を軽減するとともに，情報作成者が開示先を指定することで，管理者によるグループの登録作業が不要となる。本稿では，このグループ鍵生成方法と，WWW(World Wide Web)への適用方式に関し，特徴と機能およびその仕組みについて報告する。

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では，宛先リストとシステム固有のマスタ鍵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ー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。

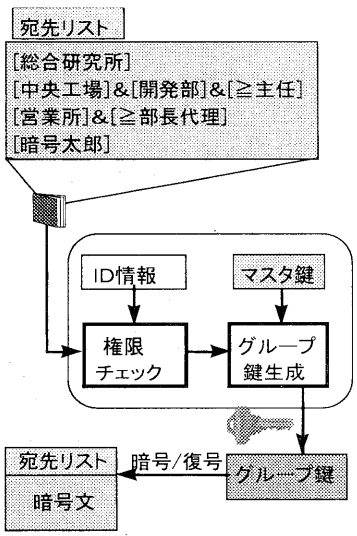


図1　グループ暗号システムの概要

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ーが宛先リストに含まれるか否かを確認する。このとき，ユーザーが含まれていれば，宛先リストから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，復号化する時に生成する鍵は，暗号化に用いた鍵と同じである。

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，ユーザーが幾つもの鍵を静的に所持する必要がないという特長がある。

また，宛先リストはユーザー名称の他に役職，所属部署名などが含まれ，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る。グループ暗号システムの概略を図1に示す。

2.2 ID情報

ID情報は，図2に示すようにカテゴリ，データ，コードから構成した。

No.	カテゴリ	データ	コード
1	氏名	日立　太郎	
2	生年月日	1960/11/07	
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

図2　ユーザーのID情報

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。ID情報とは，各カテゴリにデータやコードを割り当てた個人情報である。各ユーザーには，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ーIDおよびパスワードを発行する。

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，1ユーザーにつき複数のID情報の登録を許すことで，同一ユーザーが複数の役職を兼務するケースなどにも対応可能とした。

2.3 宛先リスト

グループ暗号システムでは，ユーザーが情報を暗号化する際に，情報の開示先となるユーザー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演算子およびOR演算子である。その他，<, >, =, <=, >=, <>(不等号)を使えば「部長以上全員」などといった範囲指定も可能である。例えば，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，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。エンドユーザーは，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，ユーザーが指定した宛先リストにユーザー本人の情報を付加する。これは，情報を暗号化したユーザーが，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，宛先リストと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3)。

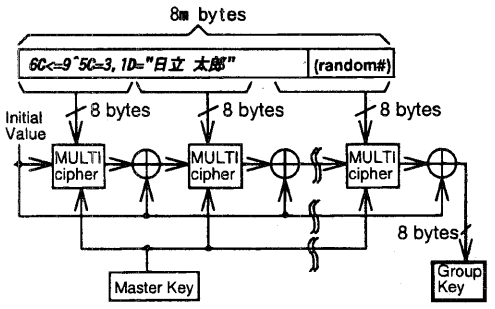


図3 グループ鍵生成方法

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[3][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正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，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，不正者が偽りのグループ鍵生成ロジックを作ることを防いだ。

3. グループ暗号システムの実装

本グループ暗号システムを構成するための主なプログラム及び情報は下記の通りである。

(1)主要プログラム
- ID登録と発行
- ユーザー認証
- 権限チェック
- グループ鍵生成
- アプリケーション（ファイル暗号など）

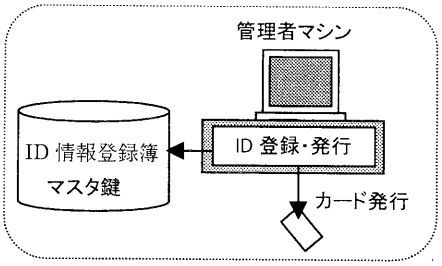
(2)情報
- ID情報
- マスタ鍵

このうち，ＩＤ情報とマスタ鍵については，不正なアクセスから保護する必要がある。また，権限チェックとグループ鍵生成のプログラムについても，改ざんや不正利用ができないよう保護する必要がある。

これらを保護する手段として，ICカードのセキュリティ機能を利用するものと，物理的に安全な部屋に設置したサーバを利用するものの2つのシステムを設計・開発した。

3.1 ＩＣカードを利用したシステム[1]

ICカードの演算機能を用いてグループ鍵を生成する。前記ID情報とマスタ鍵の他，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，ICカードに格納してシステム利用者へ配布する。このシステム構成では，ICカードがもつセキュリティ機能により，上記プログラムや情報の不正な読み取りを防止できる。また，ICカードには利用者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ー認証を行う。



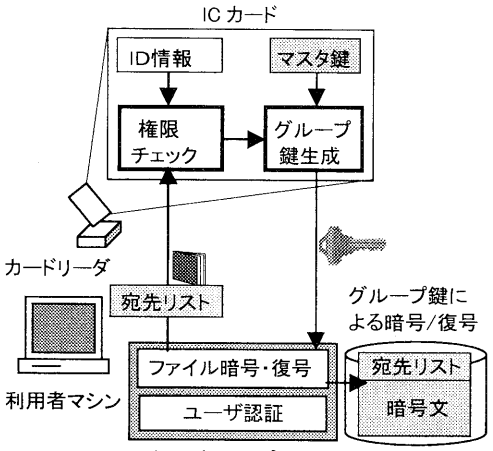


図4 IC カード版グループ暗号システムの構成

3.2 サーバを利用したシステム[2]

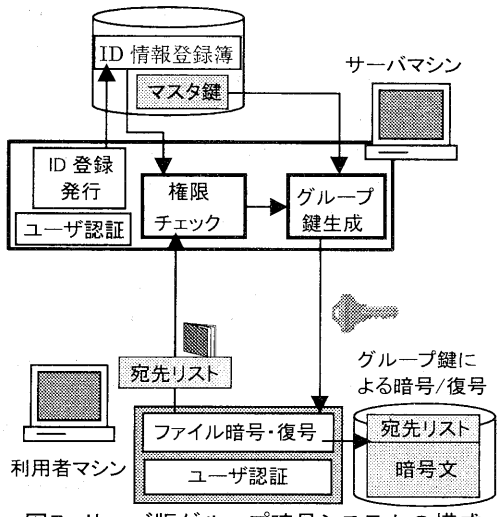


図5 サーバ版グループ暗号システムの構成

例えば，社内の部門サーバにグループ鍵生成機能を実装する。図5に示すように，前記ID情報とマスタ鍵の他，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，サーバマシンに格納し，システム利用者へはIDとパスワードを発行する。このシステム構成では，サーバマシンを物理的に安全な部屋に設置すると共に，サーバのアクセス制御機能により上記プログラムや情報を不生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読み取りを防止できる。また，システム利用の際には，例えば 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ー認証を行うとともに，クライアントーサーバ間でセッション鍵を配布し，以後の通信データを全て暗号化する。

3.3 方式比較

前記IC カード版とサーバ版の比較を表1に示す。

表1 IC カードとサーバ方式の比較

#	比較項目	IC カード	サーバ
1	マスタ鍵と ID 情報の管理負担	× (分散型)	○ (集中型)
2	マスタ鍵と ID 情報の安全性	◎	△ (運用に依存)
3	導入コスト	×	○
4	Mobile 対応	◎	△
5	ユーザー認証	○ (ｶｰﾄﾞ+ﾊﾟｽﾜｰﾄﾞ)	△ (ID+ﾊﾟｽﾜｰﾄﾞ)

IC カードの場合，マスタ鍵や ID 情報をより安全に保護できる点で優れている。しかし，企業内あるいは企業間で使用する場合，役職や所属部署名などの個人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。企業では，組織や人事の変更に伴う ID 情報の書換えが頻繁に起こり得るため，企業情報システムにはサーバ方式が適している。一方，モバイルコンピュータやスタンドアロンのコンピュータでファイル暗号・復号を行うには IC カードが適している。今後，IC カードが普及すればコストの問題も解消されると予想でき，環境や用途によって IC カードとサーバを使い分けることが望ましいと考える。

4. WWW への適用

グループ暗号システムを利用したアプリケーションの例として，WWW コンテンツのアクセス制御について以下に記述する。

4.1 概要

WWW 向けのセキュリティプロトコルやシステムには，S-HTTP[7]や SSL[8], PCT[9]など様々なものがある。しかし，特定の WWW ブラウザに依存したり，平文がプロキシサーバにキャッシュされるなどの問題がある。そこで，グループ暗号により予め暗号化した HTML(Hypertext Markup Language)ファイルを WWW サーバに格納することとした。開発における基本方針は下記の通りである。

- 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(Hypertext Transfer Protocol) や HTML の拡張は無しとする
- キャッシュファイルの安全性を維持する

4.2 HTML ファイルの暗号化

WWW の環境では，グループ暗号の復号プログラムを持たないクライアントからもブラウザを利用して暗号化HTML ファイルにアクセス可能である。このとき，クライアントの画面上に意味不明の暗号文，つまりバイナリデータが表示されることは，WWW ブラウザソフトの安定動作を維持するためにも好ましくない。この対策法として，HTML ファイルの暗号化の際には，暗号文を Base64 でエンコードすると共に HTML のコメント文としてカプセル化することとした。具体的には，前記ファイル暗号プログラムにおいて，対象ファイル名の拡張子が.htm または.html であれば，暗号文を Base64 でエンコードし，先頭と後尾にそれぞれ HTML のコメント開始文字列（<！—— ）と終了文字列（——>）を付加する。エンコード後の文字列には「−」や「>」が含まれないため，暗号文の途中に上記コメント終了文字列が出現することはない。

図 6 に暗号化 HTML ファイルの一例を示す。復号プログラムを持たないクライアントがこの HTML ファイルを受信すると，画面には，「このページは暗号化されています。復号化するにはグループ暗号ソフトウェアが必要です。」というメッセージが表示され，暗号文は表示されない。このように，暗号文の外にメッセージを付加することにより，グループ暗号のソフトウェアを持たないユーザーに対するメッセージを書き込める。

```
================================
<HTML>
<HEAD><TITLE>
営業情報
</TITLE></HEAD>
<BODY>
このページは暗号化されています。
復号化するにはグループ暗号ソフトウェアが
必要です。
<!--GCSv1.00
6hEyX8YCzXtPoamwVpYVnZr0zJ9SoHYuy
N62UzQ/iw3+IYpgkWuwfvERSUjK2abLBD
J9P+ZTb3WSI61enmcjWzPTME4aQrCRZqo
eTi2zVSt56++++sE58JKadUL2HNYGq3X9
k+1JN/JF4Z2H3/0++++sQqy6UnNvXgG++
+U0+wpMgZ4QlsmQadK
-->
</BODY>
</HTML>
================================
```

図6 暗号化 HTML ファイル

4.3 受信データの復号化

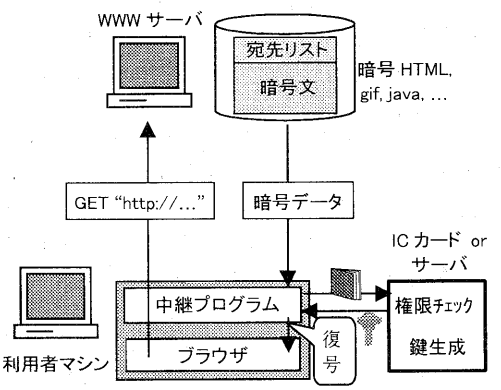


図7 中継プログラムによる復号処理

WWW ブラウザが受信したファイルの復号については，幾つかの方式が考えられる。1 つは，ブラウザが呼び出すヘルパーアプリケ

ーションによる復号である。しかし，ヘルパーアプリケーションにより復号化したデータは，HTMLとしてブラウザが処理できないため，その用途は限定される。他の方式として，CCI(Common Client Interface)[10] を利用した復号が考えられるが，API が標準化されていないため，ブラウザの種類に依存するという問題がある。

そこで，HTTP のトラップによる復号方式を採用した。具体的には，図7に示すようにクライアントに通信の中継プログラムを常駐させ，送受信データを監視することで実現できる。中継プログラムは，WWW ブラウザが HTTP の"GET"メソッドを発行すると，それに対する WWW サーバからの受信データをチェックする。受信データがグループ暗号により暗号化されていれば復号処理を実行し，平文データについてはそのままブラウザに渡す。これにより，復号権利を持つユーザーは，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。

8. まとめ

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。本方式は，企業情報システムにおける共有ファイルのアクセス制御の他，電子メールなどの1対Nの安全なデータ送信にも有効であると言える。

特に WWW への適用では，エンドユーザーの操作性を損なうことなく WWW のセキュリティを高めることができる。更に，WWW サーバには，予め情報提供者によって暗号化したファイルを格納するため，WWW サーバの管理者であっても復号権利がなければ情報を取得できないという特長がある。企業情報システムにおいては，情報提供者とサーバ管理者とが必ずしも一致しないことからも，これは有効であると言える。また，プロキシサーバがキャッシュするファイルも暗号化されているため，キャッシュファイルへの攻撃にも対処できる。ただし，暗号化により WWW コンテンツの管理が困難にならないよう，アクセス権確認ツールなどを提供する必要があると考える。

謝辞：本研究の推進に当たってご支援，ご指導頂いた関係者の方々に深く感謝する。

参考文献

[1] H. Ito, S. Susaki, M. Arai, M. Koizumi, and K. Takaragi, "Group Cipher System for Intranet Security," IEICE Trans. Vol. E81-A, No. 1, January 1998, pp. 28-34.

[2] M. Arai, H. Ito, S. Susaki, H. Umeki, and T. Kaji, "Group Cipher System For Extranet System," CALS Expo INTERNATIONAL, Tokyo, TS12-1, 1997, pp. 1-6.

[3] K. Takaragi, K. Hashimoto, and T. Nakamura, "On Differential Cryptanalysis," IEICE Trans. Vol. E74, No. 8, August 1991, pp. 2153-2159.

[4] IPA/Hitachi Ltd., "MULTI2," ISO/IEC 9979 register of cryptographic algorithm, {iso standard 9979 multi2 (9)}, NCC, UK, Nov. 1994.

[5] K. Takaragi, R. Sasaki, and F. Nakagawa, "Development of Multi-media Encryption Algorithm HISECURITY-MULTI2 and Its Operation Mode," Proceedings of the 1989 Joint Workshop in Information Theory and it's Applications, Cryptography and Information Security, Atami, Japan, August 1989.

[6] W. Simpson, "PPP Challenge Handshake Authentication Protocol (CHAP)," Request for Comments 1994, Network Working Group, August 1996.

[7] E. Rescorla and A. Schiffman, "The Secure Hyper Text Transfer Protocol," July 1995.

[8] K. Hickman and T. Elgamal, "The SSL Protocol," Internet-draft, June 1995.

[9] J. Benaloh, et al., "The Private Communication Technology Protocol," Internet-draft, October 1995.

[10] D. Thompson, "Common Client Interface Protocol Specification," April 1995. http://www.ncsa.uiuc.edu/SDG/Software/XMosaic/CCI/cci-spec.html,