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

１Ｓ－７　伊藤 浩道　洲崎 誠一　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

インターネットやモー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りつつある．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[1]を開発し，企業情報システムにおける共用ファイル暗号化に適用した．本稿では，この共用ファイル暗号化方式に関し，特徴と機能およびその仕組みについて報告する．

2. 現状の課題

共用ファイルの暗号化に，慣用暗号や公開鍵暗号方式を用いた場合，復号を許可するグループの定義毎に鍵の設定と配布が必要となり鍵の管理が容易でないという課題がある．また，OS のファイルアクセス権制御は，エンドユーザーにとっては設定が困難な上，OS の管理者が全ての情報をアクセス可能であるという課題もある．さらに，企業内文書共用にも用いられつつある WWW (World Wide Web) のセキュリティについては，幾つかの方法が提案されているが，企業の組織に対応した自由な権限設定は未だ実現されていない．

3. システムの概要

上述の課題を解決するため，クライアントまたはファイルサーバ上の共用ファイル，および WWW サーバ上の HTML (Hyper Text Markup Language) ファイルを，グループ暗号を用いて暗号化・復号化するシステムを開発した（図-1）．暗号化・復号化においては，ユーザーの ID 情報記憶とグループ暗号鍵生成を行うセキュアカードを用いて本人の認証を行う．開発にあたっては，以下の点を考慮した．

(1) ファイル共用時の安全性確保
(2) アプリケーションプログラム（AP）から透過な暗号化・復号化の実現

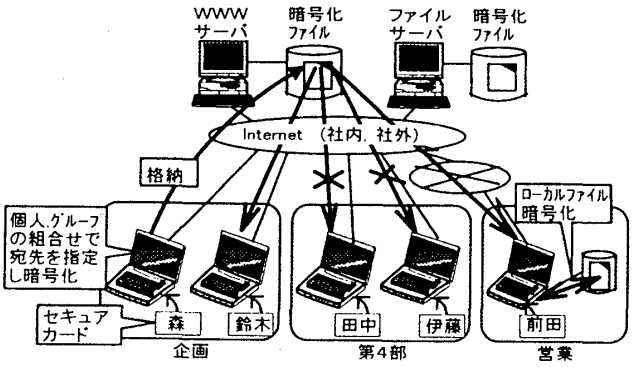

図-1　システムの概観

4. 機能と実現方式

4.1 共用ファイルの暗号化・復号化

ユーザーが明示的にファイルを指定し暗号化・復号化の操作を行う手動暗号機能と，予め設定した対象ディレクトリ内のファイルを自動的に暗号化・復号化する自動暗号機能を開発した．本稿では自動暗号機能について説明する．自動暗号機能は，宛先リストを記述したファイルを作成する機能と，ファイル I/O をフックし暗号化・復号化を行う機能から構成し，AP から透過な暗号化・復号化を実現する．

(1) 宛先リストファイル作成機能

宛先リストは，ユーザーやグループの ID 情報を登録した ID 登録簿を基に GUI を用いてインタラクティブに作成できるようにした．作成した宛先

Group Cipher Method for Enterprise Information System (2)
- Cipher Method for Shared File -
Hiromichi ITO, Seiichi SUSAKI, Masato ARAI,
Hisashi UMEKI, Hajime MORITO
Systems Development Laboratory, Hitachi, Ltd.
292 Yoshida-cho Totsuka-ku Yokohama 244 Japan

リストは，そのリストを使用する暗号化対象ディレクトリ内に，ユーザー毎の設定ファイルとして格納する．ファイルサーバ上のファイルを異なるマシンから操作した場合や，FD などのリムーバブルディスクの場合でも本機能を利用可能とするため，各対象ディレクトリの宛先リストは一括して管理せず，各ディレクトリに分散して置いた．

(2) ファイル I/O フック機能

ファイル I/O をフックすることによって，AP からの書き込みデータ暗号化と読み出しデータ復号化を行う．この処理には数 KB のブロックバッファを用い，バッファのサイズ単位で暗号化・復号化を行う．このバッファにより，ランダムアクセスへの対応，暗号文連鎖モードへの対応を可能とした．また，このバッファを先読み機能付きライトバックバッファとして機能させることによって，暗号・復号処理によるアクセス性能低下を抑えた．

さらに，暗号化前後のファイルサイズの違いを隠す機能や，別のユーザーが同一ディレクトリに異なる宛先リストで作成したファイルを操作する場合の警告機能などを設け，AP からの透過性実現とファイルの安全性，整合性維持を実現した．

4.2 HTML ファイルの暗号化・復号化

(1) HTML ファイル暗号化機能

WWW の場合，クライアントが不特定多数であり，グループ暗号に対応した復号化プログラムを搭載していないクライアントからも暗号化した HTML ファイルがアクセスされる可能性がある．このような場合に，暗号文が意味不明のバイナリ文字列として読み込まれることは安全上好ましくない．そこで，平文の HTML ファイルを暗号化したデータを，HTML のコメント文としてカプセル化し埋め込むことにした（図-2）．これによって，復号化プログラムを搭載していないクライアントのブラウザから参照した場合にも，適切な警告文を表示することができ，意味不明なバイナリ文字列が表示されることを防止できる．なお，HTML におけるコメント文終了記号“- - >”が暗号文中に現れたときは，別の乱数を実行鍵として再度暗号化を行うようにした．

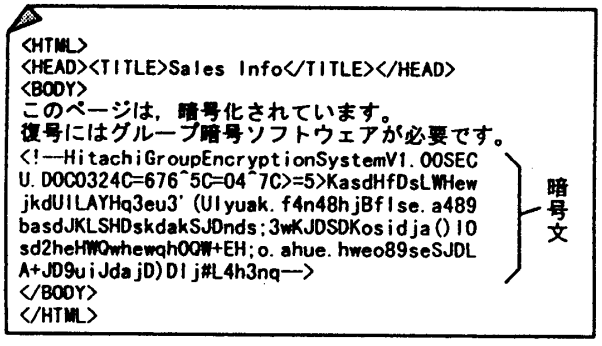

図-2 暗号文をカプセル化した HTML ファイル

(2) ブラウザ対応復号化機能

HTML ファイルの復号化は，TCP/IP ソケットをフックし，ブラウザと WWW サーバ間の HTTP（Hyper Text Transfer Protocol）通信をモニタすることによって実現した．具体的には，ブラウザが発行する HTTP の“GET”メソッドを検出し，“GET”に対応して WWW サーバから送られる HTML ファイルを復号化する．ブラウザへは，コメント文としてカプセル化されている暗号部分を復号化した結果を渡す．これによって，復号化権限を持ったユーザーが操作するブラウザからは，平文の HTML ファイルの場合と全く同様に，暗号化 HTML ファイルをブラウズすることができる．

5. おわりに

グループ暗号の共用ファイルへの適用について報告した．自動暗号化やファイルサーバ上のファイルへの対応，WWW ブラウザ対応復号化機能などを開発し，ファイル共用時の安全性確保と AP 透過な暗号化・復号化を実現した．

グループ暗号は，企業情報などユーザーの階層管理やグループ管理が必要な情報のセキュリティ実現に適した暗号方式であり，今後も新たなシステムへの適用を研究していく予定である．

参 考 文 献

[1] 洲崎，伊藤，荒井，梅木，森藤，“企業情報向けグループ暗号システム(1) 暗号鍵管理方式”，情報処理学会第 52 回大会，1S-6，1996（本大会にて発表予定）

[2] 岡本，“暗号理論入門”，共立出版，1993