オフィスシステム用暗号技術への取組み

Approach to Cryptographic Technologies for Office Systems

新保　淳　A. Shimbo
清水　秀夫　H. Shimizu

近年，オフィスにおけるコンピュータやネットワークの利用が推し進められ，業務上扱う情報の多くの部分がこの新たなインフラの上で扱われるようになってきた。これに伴って，情報が漏えいしたり，盗聴されたり，不正な変更を受けるといった危険も増加している。この脅威に対抗するための手段として，大きく分けて，①暗号化による情報の秘匿，②利用者認証に基づく情報へのアクセス制御がある。

ここでは，暗号化による情報の秘匿を目的とした二つのシステムを紹介する。一つは，携帯パソコン（PC）や共同利用 PC 向きで使い勝手のよさをソフトウェア技術で実現した PC ファイル暗号化システム，もう一つは，クライアント／サーバシステム向きで共同編集作業や高速なファイル更新が可能なセキュア共有ファイルである。

Computers and networks have recently become widely applied to office work. A large part of the information which is indispensable for office work is being processed on this new infrastructure. However, this situation may lead to increased risks of unauthorized disclosure and modification of data by malicious computer users. The main countermeasures against these risks are information encryption by means of cryptography, and access control by means of user authentication.

This paper describes two newly developed cryptographic systems. One is a file encryption system for personal computers used for mobile computing or joint work, in which ease of use is realized with sophisticated software techniques. The other is a secure file sharing system for client/server systems, in which concurrent editing and privacy-enhanced merging of files are efficiently achieved.

1 まえがき

オフィスや出張先において扱う多くの貴重な情報は，それ自体が高い資産価値をもつために，漏えいし悪用されたときあるいは失われたときに，その組織は大きなダメージを受けることになる。この予防策として暗号化による情報の秘匿は有効な手段である。従来から情報の暗号化システムは開発されてきたが，一般に，暗号化機能が追加された結果，システムの操作性が悪くなったり，通信速度が低下したり，共同作業の対象となるファイルの管理が困難になるなどの欠点もみられた。

ここでは，このような暗号技術の利用によって発生する使用上の問題点を回避できる新しいオフィス向け暗号化システムを紹介する。これらのシステムにより，情報のセキュリティを確保しながら，容易な操作，時間の無駄の排除などが実現され，組織の目的達成にきわめて有効である。

2 PC ファイル暗号化システム

2.1 システムの目的

ポータブル PC は手軽に持ち歩くことができる反面，デスクトップ PC がオフィスの中に据えられていた時代には考えられなかった盗難や紛失のような直接的なリスクが生じている。ポータブル PC の盗難により，ハードディスクに蓄えられた顧客情報のような機密情報が漏えいしてしまう危険性がある。

1995 年の米国における PC 盗難の被害総額は 6 億 4,000 万ドルという大きな金額であった。これは，毎日 3,855 台以上のコンピュータが盗まれている計算になる。ただし，これは PC だけの被害額であり PC に格納されている機密情報が漏えいしたことによる被害を含んだ額ではない。

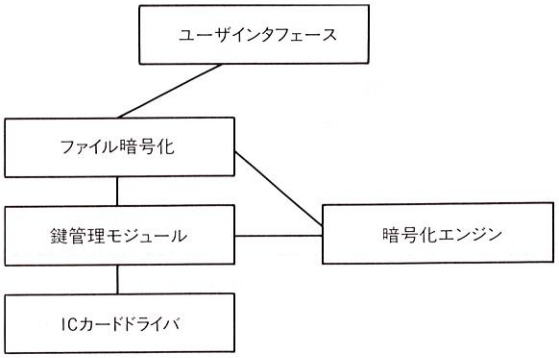

図 1．PC ファイル暗号化システムの構成　ユーザインタフェースや IC カード（鍵管理媒体）ドライバがモジュール化され，カスタマイズが容易である。

Configuration of PC file encryption system

当社では，このようなPC盗難による機密情報の漏えいというリスクへの対策技術の開発を行っている。

2.2 開発の基本方針

現在のポータブルPCはパスワード機能をもっているが，PCそのものが盗難された場合，分解してハードディスクを抜き出して他のPCに接続することで情報を読み出すことが可能である。これはハードディスクに書き込まれた情報そのものを隠さなければならないことを意味している。したがって，このシステムでは，暗号技術により情報を保護することとした。

2.3 システムの概要

このシステムは，PCそのものが盗難されても内部の機密情報を保護する目的で，ICカード内に暗号鍵(かぎ)を封入し，ICカードがなければ暗号化された内部の情報は読み出せないような仕組みを提供している。PCを使用しない場合，ICカードは取り外して別途携帯することになる。すなわち，PC内部の情報とICカードとは，預金通帳と印鑑の関係にあるといえる。

図1にこのシステムの全体構成を示す。ユーザインタフェース部は，GUI (Graphical User Interface) および自動暗号化などのスケジュール管理を行う。ファイル暗号化部は，ユーザインタフェース部から渡されたファイル名を基にファイルを暗号化する。鍵管理モジュールは，暗号化ファイルのヘッダ情報から鍵を取り出したり，乱数を使って一時鍵を発生したりといった，鍵全般の管理を行う。ICカードドライバは，ICカードリーダライタの制御，およびICカードとのやり取りを行う $T=1$ プロトコルをサポートする。暗号化エンジンは，64ビットのブロックを暗号化したり復号する暗号化アルゴリズムを提供する。以上四つのソフトウェアモジュールがWindows® (注1) 95上で実装されている。

このシステムの対象となるPCは，PCMCIA (PC Memory Card International Association) スロットもしくはシリアルポートのいずれかをもっている，どこにでもあるPCであり，特別なハードウェアは必要としない。

図2はICカードである。図3は，PCにICカードリーダを介してICカードを装着するようすを示したものである。

2.4 システムの機能

2.4.1 ユーザインタフェース　このシステムは，多様な暗号化と復号の動作モードを用意している。それらは，ドラッグ＆ドロップによる暗号化／復号 (図4)，アイコンを右ボタンクリックしたメニューによる暗号化／復号，アイコンのダブルクリックによる復号＆アプリケーションの自動起動などである。これにより，ユーザは面倒な操作を行わずに暗号化の利点を利用できる。

以下，特徴的機能について説明する。

2.4.2 自動暗号化　暗号ファイルのアイコンをダブル

(注1)　Windowsは，Microsoft社の商標。

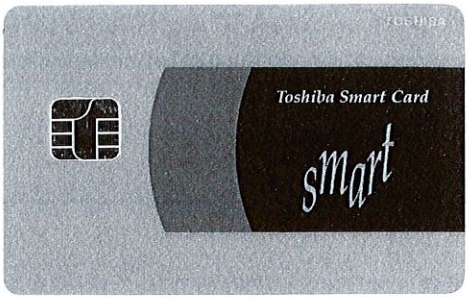

図2．ICカード　プラスチックカードの表面にICと接点をはりつけてある。Z-80相当のCPUと数Kバイト程度の記憶容量をもつ。
Smart card

図3．ICカードリーダライタ　ポータブルPCに適したPCMCIAタイプのICカードリーダライタ (FY-1300)。
Smart card reader/writer

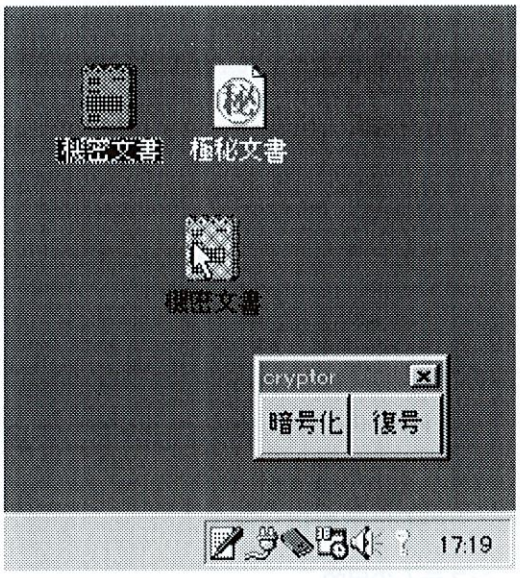

図4．ファイルの暗号化　ファイル“機密文書”のアイコンを，暗号化と書かれているボタンにドラッグ＆ドロップすることで暗号化している。
Encryption using drag and drop

クリックすることで，自動暗号化機能を利用することができる。

自動暗号化は，次のプロセスにより実行される。

(1) ダブルクリックにより暗号ファイルが復号される。

(2) 復号されたファイルと関連づけられたアプリケーションが自動的に起動する。

(3) アプリケーションの終了後，セーブされたファイルは再暗号化される。

2.4.3 終了時暗号化機能 終了時暗号化機能は，ログオフ時にあらかじめ指定しておいたディレクトリに含まれる暗号化されていないファイルを自動的に暗号化する機能である。逆に，ログオン時に指定しておいたディレクトリに含まれている暗号化されたファイルを自動的に復号する機能ももっている。

これは，新規に作成されたファイルを暗号化する手間を省くことに役だっている。

2.4.4 誤操作防止機能 暗号化されたファイルをさらに複数回暗号化すると，その回数だけ復号しなければ平文に戻らず管理の手間が増える。セキュリティ上は一度だけ暗号化すれば十分であるため，暗号化したファイルをさらに暗号化することはできないようにしている。これは暗号化済みを示すフラグをファイルの先頭にもつことで実現している。

さらに，誤った鍵での復号によりファイルが破壊されることを防ぐために，復号しようとしている鍵が暗号化したときの鍵と同じかどうかを判定する機能をもっている。

2.4.5 IC カードに暗号鍵を保管する IC カードは，IC と外部端子をはりつけたプラスチックのカードであり，それ自体 CPU，ROM，EEPROM，RAM をもった小型のコンピュータである。IC カードの計算能力を利用することで，内容の読出し／書込みに関するアクセス制御をかけることが可能である。

このシステムでの IC カードの利用法は二通りである。

(1) 鍵を読み出すことが困難であるような鍵の入れ物

(2) IC カード内での情報の暗号化

2.4.6 ファイル暗号化方式 ファイル自体はランダムに発生した乱数を鍵（セッション鍵）として暗号化する。このセッション鍵を覚えておく必要があるが，暗号化のたびに鍵が増えていくのでは鍵の管理と記憶域の面で問題がある。IC カードの計算能力を利用することで，この問題を解決している。セッション鍵自体を IC カード内の鍵を用いて IC カード内部で暗号化し，ヘッダとして暗号化ファイルに添えている（図 5）。

この方式（間接暗号化方式）の利点は，次のとおりである。

(1) IC カード内の鍵が PC 側に読み出されることはない。

(2) ファイルごとに鍵が変わるので安全である。

(3) IC カードだけで暗号化することと比べると高速な処理が可能である。

(4) 別のマスタ鍵で再暗号化するときにヘッダだけ作りかえればよいので高速である。

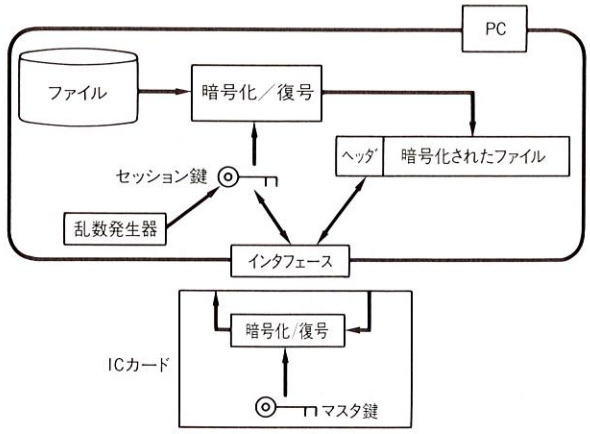

図 5．暗号化の流れ ファイルはセッション鍵によって暗号化され，セッション鍵自体は IC カード内で暗号化されヘッダとなる。
Example of file encryption

2.4.7 グループ鍵 このシステムは，たとえ機密情報であっても，情報を共有できる仕組みをもっている。すなわち，IC カードに複数の暗号鍵を格納し，複数の IC カードに同じ鍵をもたせることで情報の共有を可能にしている。

2.4.8 監査鍵 どの IC カードで暗号化したファイルであっても，復号することが可能な監査鍵を作ることができる。これはマスタ鍵に相当するもので，暗号を利用した機密の漏えいを監査することが可能である。また，緊急時の復号にも応用でき，鍵紛失対策と考えることもできる。

2.4.9 暗号アルゴリズムの高速化 ユーザに負担をかけないために，暗号アルゴリズムは高速であれば高速であるほどよい。このシステムでは米国標準として実績のある DES（Data Encryption Standard）アルゴリズムを用いている。

当社では，現在の標準的な CPU によるソフトウェア処理だけでおよそ 10 Mbps 以上の処理速度を可能にする高速実装法を開発した。DES アルゴリズムにもともと含まれているビット演算をソフトウェアで高速に処理するために，事前に計算した表を用意している。

2.5 今後の課題

現在のこのシステムがもっている問題点を列挙する。

(1) より透明性の高いユーザインタフェース ユーザにファイルを暗号化していることを意識させないことが目標であり，まだ不十分な点が多い。

(2) IC カードの抜き忘れ対策 IC カードを挿したまま PC を紛失した場合，せっかくの保護システムがなんの役にもたたないことになる。PC と物理的に分離したまま鍵を保管できる装置は一つの解決法である。PC と物理的に分離できないような装置であっても，指紋のよ

うな個人の特徴を識別できないと作動しないような装置であってもよい。

(3) 鍵管理システム　だれがどのICカードを持っており，そのICカードにはどのような鍵が書き込まれているか，といった情報管理をサポートするシステムの整備が必要である。

(4) 通信対応　個人のPCにある情報を安全に他と交換できるような発展を考える必要がある。

3 セキュア共有ファイル

3.1 概要

セキュア共有ファイルはクライアント／サーバモデルの共有ファイルシステムである。このシステムは，暗号化や認証といったセキュリティ機能，グループによる協調作業を支援するファイルの履歴管理機能と同時編集機能，クライアントとサーバ間の通信データ量を削減する高効率通信機能を統一的に実現する。特に，携帯型計算機をクライアントとして無線回線によりファイルサーバにアクセスする場合，高効率通信とセキュリティはキーとなる技術であるため，モバイルコンピューティング環境に好適のシステムと言える。

従来，ファイルデータの暗号化などのセキュリティ強化と履歴管理など情報共有や編集に必要な管理用データの取出しには両立しない部分があった。これに対し，ファイル内のデータの位置や順序といった情報を隠さずに，しかもデータ自体は秘匿強度を保ったまま暗号化する方式を考案したことにより，以下のような特徴を備えたファイルシステムが構成可能となった。

図6にシステム構成を示す。なお，以降では，携帯PCをクライアント計算機と想定する。

3.1.1 ファイル内容の秘匿と認証機能　共有ファイルの内容は，正当な利用者以外は読めないように携帯PCが暗号化する。通信回線上はもとより，ファイルサーバでもデータは暗号化されたままである。したがって，ファイルサーバの管理者であっても内容をのぞき見ることは不可能になる。万一，サーバ上のファイルが盗難にあっても内容は判読されない。このようにファイルの内容に関し，飛躍的にセキュリティが向上する。

また，ディジタル署名技術とメッセージ認証技術（MAC：Message Authentication Code）により，不正利用者からのファイルアクセスや，通信途上のデータの改ざんを防止している。

3.1.2 高効率通信とディスコネクト機能　携帯PCでファイル編集後，ファイルサーバへのライトでは修正したファイル全体ではなく，元のファイルとの差分だけを送る。さらに，携帯PCはアクセスしたファイルのコピーをローカルなキャッシュに保持し，ファイルのリード時にはキャッシュとの差分だけをサーバから読み出す処理を行う。このようにクライアントとサーバ間の通信は，ファイルの変更部分だけで実行されるため，特に低速の回線を利用した場合に，アクセス時間短縮の効果を発揮する。

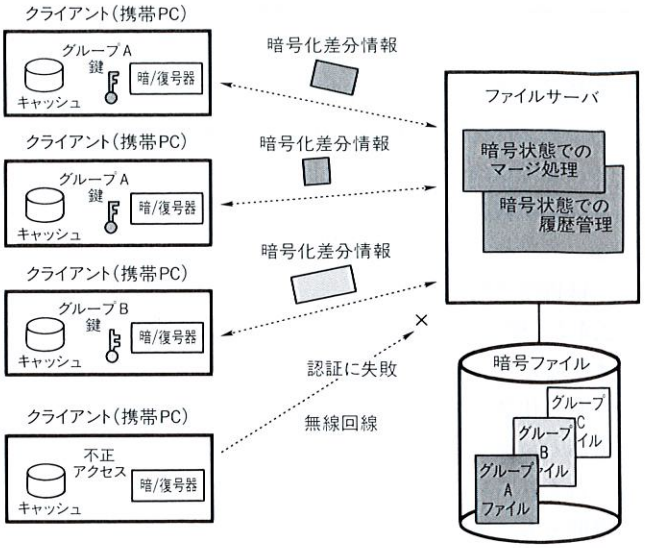

図6．セキュア共有ファイルのシステム構成　携帯PCが暗号機能をもち，ファイルサーバは暗号状態でのマージ処理，履歴管理機能をもつ。

System architecture of secure file sharing system

さらに，携帯PCは対象ファイルのリード／ライト時だけサーバとの接続を行うため，ファイルの編集中はサーバとの接続は不要である。したがって，編集中に通信が突然切断されても編集を継続できる。このように必要なときにだけサーバとの接続を行い，ローカルに編集を行うディスコネクト編集が可能である。

3.1.3 同時編集と履歴管理機能　複数のユーザが書込みを行う共有ファイルではファイルの一貫性管理の問題がある。例えば，同一のファイルをアクセスし，編集中のユーザAとBがいたと仮定すると，先にAが編集結果を保存し，あとからBが別の編集結果を保存するようなことが生ずる。この場合，通常のシステムではBが保存しようとするときに，すでにファイルが更新済みである旨をBに通知して，Bの保存を拒否する。セキュア共有ファイルではこのような利用法以外に，同時編集という利用モードも備えている。

これは，先の例でBの保存時にファイルサーバがAの編集内容とBの編集内容の両方を組み合わせたものを最新のファイル内容とするものである。このときのサーバの処理を“マージ処理”と呼ぶことにするが，この処理ではファイルの履歴管理が必要であり，この機能も同時に実現している。

3.1.4 暗号処理の軽減

以上の機能はサーバ上のファイルを暗号化したままで実現されている。ファイルの作成や更新時には，新たに書き加えるデータは暗号化するが，それ以前に書かれていたデータの再暗号化は不要である。データの削除時には対象データに削除のタグを付けるだけである。このようにすべてのデータは最初の書込み時に一度だけ暗号化されること，もともとサーバ側には暗号・復号能力はないためサーバ側での暗号処理がいらないことなど，暗号化のオーバヘッドが必要最低限で済むようにくふうされている。

3.2 メカニズム

3.2.1 同時編集と履歴管理

同時編集は，共有ファイルの任意の時点でのバージョンに対する，携帯PCによる編集結果を受信したサーバが，それをどのように現時点でのファイル内容に反映させるかという問題に帰着する。セキュア共有ファイルでは，利用者による編集をデータの挿入とデータの削除に分解してとらえ，これらの行為が必ず反映されることを保証することにしている。例えば，図7のように元のファイルに対して携帯PC-Aは“研究会@東京”を“展示会@幕張”に変更し，携帯PC-Bは“懇親会”を追加した場合を想定する。このときのマージ版は“展示会@幕張”と“懇親会”を残した内容としている。なお，携帯PC-Bにとって“研究会@東京”がマージ版で変更されることが不都合な場面も予想されるので，ある携帯PCからのライト要求によりマージが行われた場合には，サーバからその事実を携帯PCに通知する。

以上のマージ処理は，新規の挿入ブロックに対して生成時刻と消去時刻のタグ情報を用意し，編集が行われる都度，新規の挿入や新規の削除ごとにブロックの分割・挿入・タグ情報の管理を行うことで実現される。図7の同時編集に対応したファイルサーバ上のマスタファイルの推移を図8に示した。このデータ構造では任意の時点でのファイルの内容を各データブロックのタグ情報を基に再生可能であるため，履歴管理も同時に実現されている。

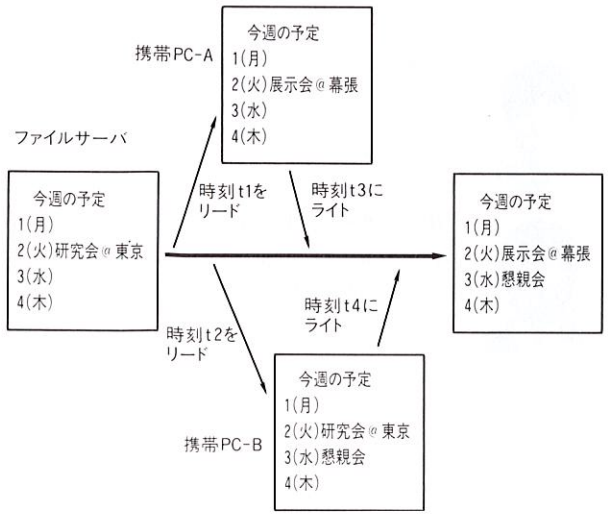

図7．同時編集の例　セキュア共有ファイルで，利用者AとBが共有ファイルを同時編集した場合の内容の変化の一例を示す。

Example of concurrent editing

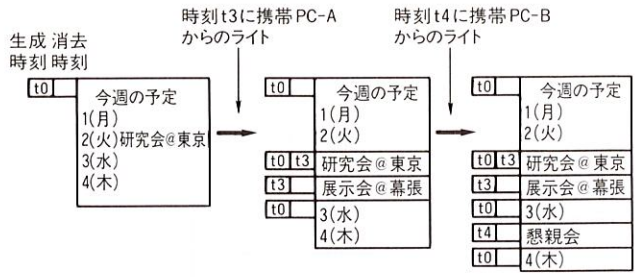

図8．同時編集によるマスタファイルの推移　携帯PCでのファイル編集によりファイルサーバのデータのブロック分割，タグ情報の記録が行われる。

Example of concurrent editing and file transition

3.2.2 暗号方式と暗号状態でのマージ処理

共有ファイルはファイルごとにファイル鍵FKで暗号化するが，先のマージ処理に適した暗号方式と共有ファイルのデータ構造が必要である。検討の結果，「ファイルの構造は見せるが内容は見せない」方針で暗号化することと，暗号化されたデータブロックに対し，復号せずに任意の箇所でキャラクタ単位に分割可能な暗号方式の利用が条件であることが判明した。すなわち，図8のブロック構造は残したまま，タグ情報は暗号化せず，ブロック単位に自己同期型ストリーム暗号で暗号化する方法を考案した。標準的な自己同期型ストリーム暗号にDESの8ビットCFB（Cipher FeedBack）モードがある（図9）。この暗号方式では，暗号文を連鎖させて1バイト単位に暗号化するので，同一のキャラクタであ

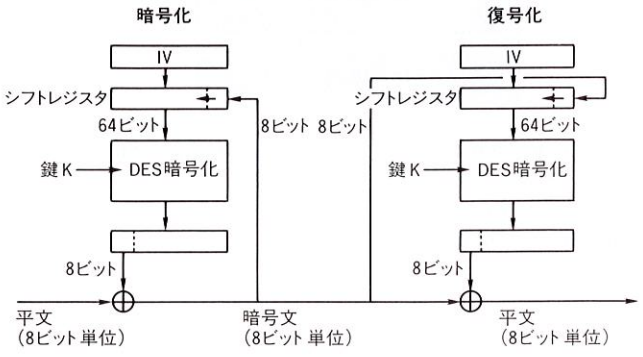

図9．DESの8ビットCFBモード　暗号文を8ビットずつシフトレジスタに供給しながら，暗号化／復号化する。シフトレジスタの初期値IVが必要。

DES in 8-bit CFB mode

っても異なる暗号文に変換される。さらに，ある暗号キャラクタの復号にはそのキャラクタ以前の8バイトの暗号キャラクタだけが必要となる性質がある。この暗号方式では，シフトレジスタの暗号化初期値IV（Initial Vector）が必要であり，このシステムではブロックごとにIVを設けている。

新規挿入ブロックの暗号化は携帯PCがランダムにIVを定めて暗号化する。ブロックの分割により生ずる断片ブロックのIVは，分割前のブロックの後ろ8バイトをサーバがコピーする。この処理で断片ブロックごとに復号が可能となる。図10は暗号状態でのマージ処理の処理例である。また，図11はこれらの機能を実現するデータ構造である。

サーバにとってファイルの内容は暗号化されているが各ブロックの生成・消去時刻や順序は把握できるため，履歴管理や高効率通信といった特徴は保存されていることがポイントである。

正当なメンバだけがファイル鍵FKを取得可能とするため，各ファイルの先頭には各メンバの公開鍵でFKを個別に暗号化したフィールドがある。このフィールド内の暗号化鍵情報は共有ファイルの所有者が最初に作成し，共有ファイルのメンバの変動があったときに変更する。

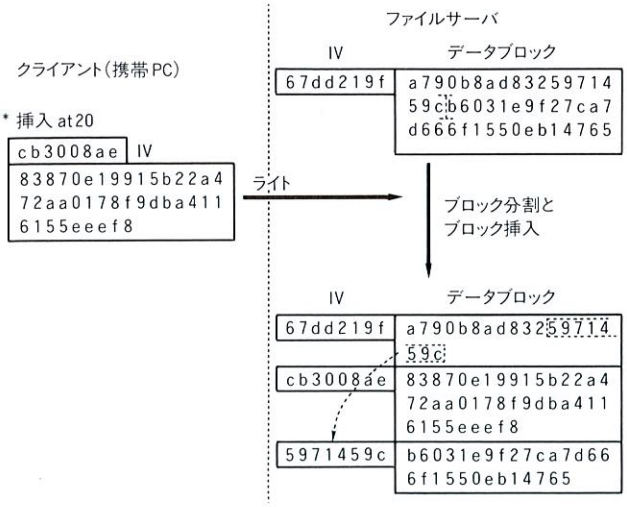

図10. 暗号化マージ処理の例　ファイルサーバでは暗号状態のままデータブロックの分割，IV情報の更新が行われる。

Example of privacy-enhanced merge processing

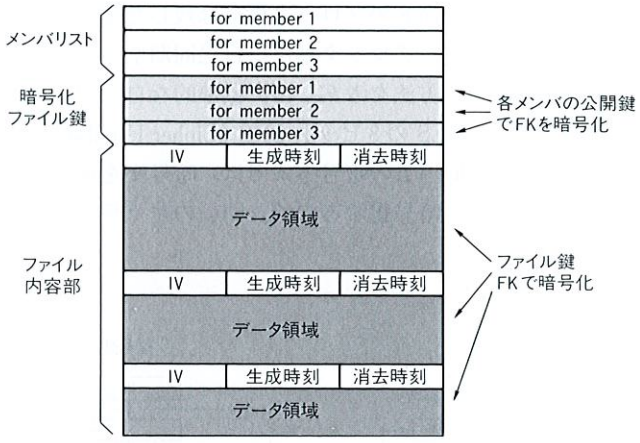

図11. セキュア共有ファイルのマスタファイルのデータ構造　暗号化ファイル鍵とファイル内容部から構成される。各データブロックにはIV情報を設定する。

Data structure of master file

4 あとがき

PCに格納した機密情報を保護するために，暗号技術を使用したファイル暗号化システムについて述べた。パーソナルユースとして，また携帯・共同利用PCなどオフィスシステムのためのツールとして用いることができる。また，暗号によるファイルデータの保護機能と非同期型の共有ファイルを融合させ，暗号化マージ処理という新たな特長をもつセキュア共有ファイルを開発した。クライアント／サーバ型のアプリケーションとしての試作が完了し，社内で試用を開始している。

文　献

(1) A. Shimbo, et al: Security Mechanism of Privacy Enhanced Shared File System suitable for Mobile Access, IEICE Trans., Vol. E79-A, No. 1, pp. 102-109 (Jan. 1995)

新保　淳　Atsushi Shimbo

研究開発センター 情報・通信システム研究所研究主務。暗号・情報セキュリティの研究・開発に従事。電子情報通信学会，情報処理学会会員。

Communication & Information Systems Research Labs.

清水　秀夫　Hideo Shimizu, D.Eng.

研究開発センター 情報・通信システム研究所，工博。暗号・情報セキュリティの研究・開発に従事。電子情報通信学会，セキュリティマネジメント学会会員。

Communication & Information Systems Research Labs.