P2P セキュアファイル共有システムにおける新共有機能の実現

―安全で安心な共有ファイルの更新とバックアップ―

１．　背景

近年、わが国の高度情報化社会の発展に伴って PC の普及率が高まり、それに伴ってネットワーク技術も飛躍的に進歩してきている。個人ユーザにおいてもデータを電子化して取り扱う機会が増え、専用のファイル共有ソフトやファイルサーバを用いて、複数のユーザと、ファイルを交換・共有したり、個人のファイルを自宅と会社の PC 間で送受信したりする技術が進歩し、普及してきた。

しかし、現在広く普及しているファイルサーバは運用コストが高いか、高度な管理知識を必要としているため、大規模な企業や学術機関であれば導入は容易であるが、大学の研究室や企業のプロジェクトチームといった小規模な組織での導入は難しいといえる。

現存するファイル共有ソフトは、その種類によっては匿名のままファイルを共有することが可能なため、著作権の侵害となる違法なファイルが共有される場合がある。さらに、ファイル共有ソフト特有のコンピュータワームも存在するため、セキュリティに対する意識の低いユーザや、知識の乏しいユーザにソフトを利用されることで重要なデータが流出してしまう事件も見受けられるようになっている。

また、近年の PC は HDD の容量が大きく、ファイルを保存するには十分なディスク容量を持っている。しかし、その容量を有効に活用しているユーザは少数であり、余剰ディスクスペースをもてあましているユーザが多いのが現状といえる。年々増加してゆくデータの整理やバックアップには多くの時間を割く必要があり、個人におけるファイル管理は困難になってきている。

２．　目的

本プロジェクトでは、小規模なグループの PC を、P2P 技術を用いて安全に連携させることによりファイル管理コストを低減し、ネットワークに参加している各 PC の通信帯域と余剰ディスクスペースをシステム全体で共有するファイル保存システムの構築を目標とする。本提案システムでは、ファイル保存先はユーザが普段使用する PC のディスクスペースであるため、ファイル保存の際は暗号化・アクセス権制御・秘密分散の諸技術を用いて、特殊な権限を持つ管理者不在での安全なファイルの保存・復元・共有を実現している。さらに、ステガノグラフィ技術を応用することによって、文書データを含むファイルとファイル復元情報を持つファイルの区別が第三者にはつかない仕組みを導入する。システムログイン時には、公開鍵暗号方式によって認証・ファイル保存情報の管理を行うため、万が一重大な情報が外に漏れてしまった場合でも責任の所在を明らかにすることができ、迅速な対処も行える。

３．　開発の内容

今回開発のベースとしている P2P ファイル分散保存システムは、図 1 のように大学の研究室内や企業のプロジェクトチーム内などに設置されている小規模なローカルエリアネットワークを対象に、各 PC を P2P で連携し、それらの PC にファイルを分散保存するシステムである。

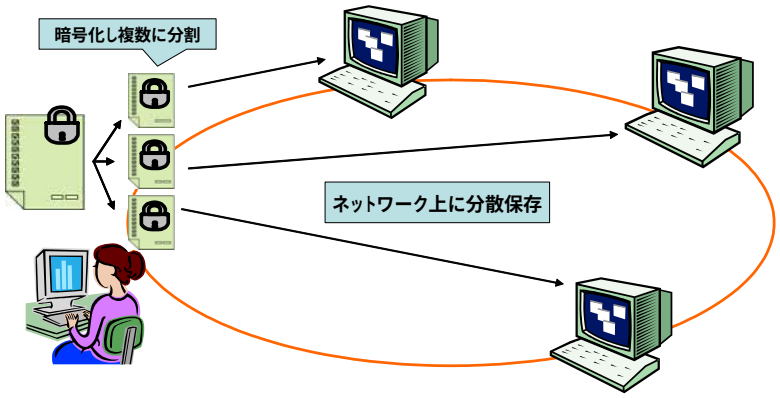

図 1　システム概要

本システムでは、個人利用 PC の余剰ディスクスペースにファイルを保存しているが、冗長性を持たせたファイル分割と暗号化により情報の秘匿性を保っている。以下の図 2 にファイル分割アルゴリズムの例を示す。

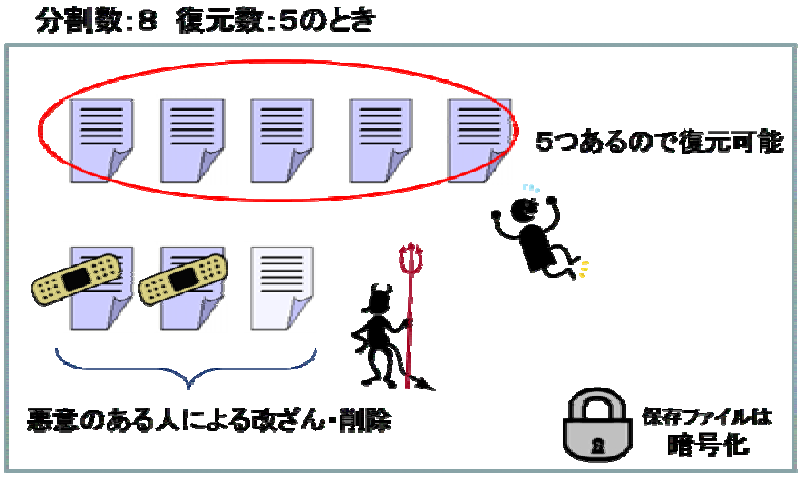

図 2　ファイルの分割と復元アルゴリズム

このようにネットワーク上に散在する PC の余剰ディスクスペースに、安全にファイルを保存することがシステムの基本コンセプトである。もちろん、PC の余剰領域が少ないユーザもファイルの保存、バックアップを行うことができる。また、PC が故障した場合にも、ファイル保存時の冗長性によりファイル内容が失われることはない。

ファイルを共有する場合は、複数の人物がファイルに対するアクセス権を有するため、ファイルの保存場所や更新情報、アクセス権を持つユーザの管理が重要となる。本システムでは共有されるファイルの情報を一括管理することで、共有ファイルの安全性を向上させている。

本システムは、ファイルの保存および復元情報に関しても、分割保存されているファイル本体と同様にネットワーク上に保存するという複雑な手法を用いてはいるが、ユーザはこの仕組みを理解する必要はなく、ネットワークに接続できる環境さえ整っていれば誰でも簡単にシステムを利用できる。また、分散保存されている情報は、それが分割されたファイルの断片であるのか、暗号化された重要なアクセス管理情報であるのかについて、正当なアクセス権を持つユーザ以外には秘匿にする手法を用いているため、本システムの仕組みを理解している第三者が悪意を持って情報を盗み出そうとした場合においても、重要な情報に対象を絞って短時間で攻撃を行うことはできない。以下の図 3 に起動時のシステムの状態を示す。

①ユーザID表示ウィンドウ　②保存ファイル一覧
③保存履歴ダイアログ　④ユーザ入力ボックス
⑤状態表示ウィンドウ

図 3　システム運用時の状態

４．　従来の技術（または機能）との相違

ベースとしている既存システムでは、共有ファイルの復元情報はユーザそれぞれが自身の公開鍵によって暗号化して管理しているため、共有ユーザが増加すると復元情報を暗号化する演算回数が増え、効率の悪化を招いていた。また、ファイルが保存されるたびに、新たな復元情報が含まれるファイルが作成されていたことも問題であった。つまり初回に test.txt を保存したときと、再編集後に test.txt を保存したときとでは全く別物の復元情報ファイルが生成されるため、保存対象外となるファイル数がファイル更新ごとに増加してしまう。

そこで本システムでは、既存システムのボトルネックであった復元情報ファイルをユーザ全員で共有することで、演算回数を減少させ、システム効率の向上を図っている。また、同名の保存ファイルであれば、ファイルの復元情報を追記していくことで無駄なファイルの増加を防げる。

さらに本システムでは、共有ファイルへのアクセスログを残しているため、情報漏洩時や改竄時における責任の所在を明確にすることができ、問題に対する迅速な対応が期待できる。

５．　期待される効果

本システムの利用環境は、大学の研究室や SOHO における小規模な LAN である。本システムを運用することで、サーバや管理者を必要とすることなく、低コストで簡単にファイルの共有、更新、バックアップを行うことができる。本システムはサーバなどの特別な追加機材を必要としないため、結成と解散を繰り返す企業のプロジェクトチームなどでもファイル共有を行いやすいといえる。

６．　普及（または活用）の見通し

今後は本システムを Linux に移植し、Windows と Linux の両 OS で使用できるようなものを考えている。さらに、より直観的に利用できるようドラッグ＆ドロップだけでファイルの保存・復元ができるようにユーザインタフェースの改良を行っていく予定である。開発成果の一部をオープンソースソフトウェアとして公開することを考えており、本プロジェクトの開発成果が普及し社会貢献となることを望んでいる。

ファイル共有における手法についても改良を重ねる必要があるため、これからも学会の研究会やシンポジウムなどを通してより多くの人から意見を取り入れて開発を続けていきたい。

７．　開発者名（所属）

東森ひろこ（東京工科大学コンピュータサイエンス学部 4 年　宇田研究室）