ファイルの世代管理による情報流制御の提案

松山　竹次郎[†1]　新城　靖[†2]　佐藤　聡[†2]
中井　央[†3]　板野肯三[†2]

1. はじめに

近年，P2P ファイル共有ソフトウェアによる機密文書漏洩などのユーザの意図しないファイル流出が頻繁に起きている．その対策として，P2P ソフトウェアをインストールさせないようにしたり，ソフトウェアが用いる通信路を制限をするなど，ネットワークシステムに対して規制を設ける方式が一般的である．これは流出そのものを止めようとする方式である．しかし現実には機密文書は流出してしまい，流出元を特定して処罰を行うといった事態が報道されている状況にあり，社会的に大きな問題となっている．既存のファイル保護の方法の一つにファイル暗号化がある．しかし復号化のための鍵情報を管理する必要があり，これが大量に必要となってしまうので管理が煩雑になる．また，IP アドレスによる送信先の固定や無線 LAN の ESSID によるファイルの送信先を認証する方式[3] も提案されている．しかしどちらの方式も，利用者のシステムに対する理解が必要であり，利用すること自体が難しい．そこでより簡易にファイルを保護できるシステムが求められていると言える．

本研究では，ユーザの意図しないファイル流出を制御する為，ファイルシステム自体に制限機能を持たせ情報流の制御を行う．

2. 想定される本システムの使用状況

まず具体的に想定される流出局面を，大学においての成績管理を例として示す．ファイルを扱うことになる人間は，3 種類いる．成績データを管理する成績管理者，成績を決定する教員およびテストの採点を行い成績を算出する Teaching Assistant（学生．以後 TA と記す）の 3 者である．成績表データは教員が作成する．テストの採点を複数人の TA に依頼し，成績表データを配布する．TA はテストの点数から成績を算出し，成績表データに記入して教員に返す．教員は複数の成績表データをマージし成績を決定，最終的な成績表データを成績管理者へと渡す．この時，教員は成績表データに対する責任があり，TA が成績表データを適切に扱い，漏洩や不正コピーが行われていない事を把握しておく必要がある．しかし TA の行動を全て把握することは難しい．TA が個人所有のノート PC で作業を行おうと，ファイルをコピーする可能性がある．管理対象でない PC にファイルがコピーされたとき，安全である保証はどこにもない．本研究では，保護対象とするファイルへのコピーや編集操作を制限・記録することで，ファイルへのアクセス内容を把握し，ユーザの意図しないファイル流出を防ぐ．

†1 筑波大学第三学群情報学類
†2 筑波大学システム情報工学研究科コンピュータサイエンス専攻
†3 筑波大学図書館情報メディア研究科

3. ファイルの世代管理による情報流制御システムモデル

本研究で作成するシステムを，Information flow Control FileSystem（以後 ICFS と記す）と呼ぶ．本研究では，リモートの OS は信用出来るものと仮定する．またトラストチェーンを作り，その範囲内である計算機は信用出来るものとする．トラストチェーンは，例えばスカイプを用いてこれを形成する．

本研究では，ユーザの意図しないファイル流出を防ぐ為に，保護対象としたファイルに対するアクセスをユーザが検知出来るようにする．その為ファイルへのアクセスを，コピーと編集の 2 種類に分類する．コピーは専用のプログラムを作成し，そのプログラムを通して行う．それ以外のファイルアクセスは全て編集と見なす．編集する時，開こうとしているソフトウェアが許可されたものであるか否かの検査を行い，コピー時にはコピー回数の制限を行う．ファイルには保護のための追加情報として，作成者名，世代情報，コピー可能回数，許可ソフトウェア一覧，コピー履歴および追加情報のチェックサムの 5 種類の情報を持たせ

表 1　ICFS 内でのファイルのやりとりの制限

コピー元＼コピー先	作成者	閲覧者
作成者	特になし	世代情報インクリメント
閲覧者	世代情報クリア コピー可能回数 クリア	・世代情報インクリメント ・既に閲覧者間でコピー されていればコピー不可 ・コピー可能回数デクリメント

る．

コピープログラムは送信と受信の 2 つの機能を持つ．コピープログラムはユーザ情報を持ち，それにより送受信時にどこへコピーされるかを判定する．ファイルを作成したユーザを作成者，それ以外のユーザを閲覧者として区別する．

編集時の処理を述べる．ソフトウェアがファイルを開くとき許可ソフトウェア一覧情報と照合し，一覧に存在するソフトウェアであれば編集することを許可する．一覧に無い場合ダイアログボックスを表示し，ユーザに可否を尋ねる．ユーザが許可した場合許可ソフトウェア一覧へ追記し，編集を許可する．許可しなかった場合には編集させない．

次にコピー時の処理を述べる．ファイルコピーの世代管理を行う．その機能を地上デジタル放送などで用いられている CPRM（Content Protection for Recordable Media ）のコピー・ワンス[2] を参考にして設計する．地上デジタル放送の録画時に，コピーワンスやダビング 10 といった制限方法がある．これは放送データを，1 回ないし 10 回までしかコピーさせず，コピーした先のデータは再コピー不能となる世代管理機能である．本研究では，ファイル作成者でないユーザが保護対象となったファイルを扱う場合に世代管理を行う．ファイルのコピー回数に制限を持たせる事で，不正なファイルコピーが行われたとしても制限以上のコピーを行なわせず，それ以上の拡散を防ぐ．ファイルは暗号化して保護し，閲覧時には ICFS で自動的に復号化を行う．

また，本研究では ICFS が適用される領域とそれ以外を区別し，その内外で処理を変える．ICFS の範囲外へ移動，又はコピーを行う場合，復号化せず，暗号化状態のままで行う．

ICFS の範囲内である場合の処理を**表 1** に示す．作成者が操作する場合，作成者の所有する領域へのコピーであれば特別な判定は行わない．そうでない領域（閲覧者の領域）へのコピーである場合，世代情報をインクリメントしてコピーを行う．閲覧者が操作する場合，コピー操作時に残りコピー可能回数を検査し，0 でなければコピー元のコピー可能回数のデクリメントと，コピー先の世代情報のインクリメントを行い，コピーする．残りコピー可能回数が 0 であるファイルおよび世代情報が 2 度インクリメントされたファイルは，コピー操作が不可となる．コピーを行ったとき，その記録はファイルの制御情報に残される．

4. ICFS の実装

ICFS では，2 章で述べた世代管理に必要な情報を各ファイルに持たせておき，ファイルアクセス時に世代管理情報に従ったアクセスの制限を行う．また，対象ファイルを暗号化することにより ICFS 以外からのファイルの閲覧を制限する．これによりファイルへアクセスする時点で，暗号化またはファイルシステムによるコピーの判定を行う事ができ，ファイル単位で情報流を制御できる．

本研究では ICFS を Linux のファイルシステムとして実装する．ICFS は実際のディスク管理は行わず，既存のファイルシステム上へ領域を確保し，そこに保護対象のファイルを格納する．この方式では，既存ファイルシステムへの通常のアクセス時にもファイルが見えてしまうが，ファイル名及びファイル内容を暗号化することでこれに対処する．ユーザプロセスから ICFS までの間は復号化されたデータのやりとりを，ICFS と実際のファイルシステムとの間では暗号化されたデータのやりとりを行う．

ファイルの暗号化の仕組みとして，共通鍵暗号方式である AES 暗号を CTR モードで利用する．暗号を適用するのは，保護対象とするファイル名及びファイル内容である．

次に，コピー用プログラムの実装についてを記す．これは，ファイルシステムと通信して実際のファイルコピーを行うためのプログラムである．このプログラムは，シェル上のコマンドとして実装を行う．

5. おわりに

現在までに，テストとして FUSE（Filesystem in USEr space）[1] によるアクセス対象の暗号化までの実装を行った．FUSE とは，ファイルシステムの内部を理解する必要がなく，カーネルモジュールプログラミングを学習しなくてもユーザー空間ファイルシステムを開発出来るフレームワークである．

今後は ext3 のような通常のファイルシステムの調査を行い，本システムの実装を行う．またファイルコピー時に制限情報に従い，コピーの可不可を判定する部分および各ファイルに対して制限情報を設定するための GUI プログラムの実装を行う．

参考文献

1) Lonczewski, F. and Schreiber, S.: The FUSE-System: an Integrated User Interface Design Environment, *in Proc. CADUI, J. Vanderdonckt (Ed*, pp.37–56 (1996).
2) 社団法人 電波産業会 ARIB(AssociationRadio Industries，Businesses)：4.1 コンテンツ保護に関する運用規定，ARIB TR-B14 3.6 版（第三分冊），p.304 (2008).
3) 鈴来和久，一柳淑美，毛利公一，大久保英嗣：Privacy-Aware OS Salvia におけるデータアクセス時のコンテキストに基づく適応的データ保護方式，情報処理学会論文誌, Vol.47 No.SIG3，pp. 1–15 (2006).