コンピュータセキュリティ 13－4
（２００１．５．２５）

UDF(Universal Disk Format)のセキュリティ拡張

蒲田 順* 小町 祐史**

* (株)富士通研究所
** (財)光産業技術振興協会Fプロジェクト

企業内で作成される機密文書や，個人が保有するプライベートな情報等の様々な情報が電子化され，安価で大容量となった記憶媒体にファイルとして大量に蓄積されるようになるにつれて，記憶媒体上のファイルのセキュリティ確保が重要な課題となっている．とりわけ，アクセス制御，秘匿，原本性保証は最重要課題であると考えている．

我々は，多くのアプリケーションから共通に利用できる基盤として，ファイル管理の中心を担うファイルシステムでこれらの機能を実現する必要があると考え，可搬型媒体の業界標準論理フォーマットであるUDF(Universal Disk Format)をセキュリティ拡張した．

Security Enhancements for UDF(Universal Disk Format)

Jun Kamada* Yushi Komachi**

* Fujitsu Laboratories Ltd.
** F Project, Optoelectronic Industry and Technology Development Association

Security for files on storage media becomes important issue on environments that various kind of corporate documents, personal information and so on are created as electronic form, sent through high- speed network and stored on mass storage as a file. Especially, access control and data privacy functionalities for the file, and guarantee of data originality for file are very important.

We propose security enhancements of UDF(Universal Disk Format), which is de-facto standard of logical format on optical storage media, in order to provide above functionalities as common infrastructure that each application can use.

1. はじめに

企業内で作成される機密文書や，個人が保有するプライベートな情報等の様々な情報が電子化され，安価で大容量となった記憶媒体にファイルとして大量に蓄積することが一般的になってきた．

このような環境においては，記憶媒体上に格納されたファイルのセキュリティ確保が重要な課題である．とりわけ，機密情報/個人情報等を格納したファイルのアクセス制御，秘匿や，公文書ファイル等が正当なものであることを保証する原本性保証が最重要課題と我々は考えている．

このような背景から，我々は，多くのアプリケーションから共通に利用できる基盤として，ファイル管理の中心を担うモジュールであるファイルシステムでこれらの機能を実現する必要があると考え，(財)光産業技術振興協会の「光ディスク・システムの相互運用性確保のための標準化」プロジェクト(通称 F プロジェクト)において，可搬型媒体向け業界標準論理フォーマットである UDF(Universal Disk Format)のセキュリティ拡張を行った．

本稿では,このセキュリティ拡張された UDF のことを Secure UDF と呼ぶことにする.なお，***Secure UDF*** とは記憶媒体上の論理フォーマットのことを意味し，***Secure UDF ファイルシステム*** とは Secure UDF を解釈しファイルの管理を行うモジュールのことを意味する．

2. UDF

UDF[1]は，可搬型光媒体向け論理フォーマットの業界標準化団体である OSTA(Optical Storage Technology Association)により，ISO/IEC 13346[2]のサブセットとして 1995 年に策定された論理フォーマットである．現在，DVD 系，CD-R/RW が採用し，可搬型媒体の業界標準論理フォーマットとなっている．

UDF の主な特徴は以下のものである．

- 追記型媒体を書き換え可能媒体に見せる仕組み(VAT : Virtual Allocation Table)
- 性質の異なる複数区画で一つの論理ボリュームを構成する仕組み(Multi Partition)
- 複数の物理媒体で一つの論理ボリュームを構成する仕組み(Multi Volume)
- ファイル/ディレクトリに，複数の補助ファイルを関連づけて格納する仕組み(Named Stream)

今回，セキュリティ拡張のベースに UDF を選択した理由としては上記の特徴の他に，オープンな規格であるため特定企業の情報に依存せずに拡張できること，版数アップの議論が継続して行われておりセキュリティ拡張を組み込める可能性があったためである．

3. Secure UDF の提案

3.1 対象範囲

Secure UDF が対象とする機能を，現状以下のものとした．

a) アクセス制御(DAM : Digital Assets Management) : ACL(Access Control List)に基づいた，ファイルへのアクセス許可/拒否の制御
b) 秘匿(DPM : Data Privacy Management) : ファイルの暗号化/復号
c) 原本性保証(DOM : Data Originality Management) : ファイルの改竄検出とファイル操作履歴の保持/参照

なお，これら三機能を，Secure UDF ファイルシステムがファイルに適用する*セキュリティ機能*と呼ぶことにする．

3.2 コンセプト

ソフトウェアのみによる軽いセキュリティモデルから，ハードウェアアシストのあるより強力なセキュリティモデルまでを統一的に扱えるよう拡張することとする．

すなわち，Secure UDF ファイルシステムを含むそれ以下のレイヤーの物理的な構成/機能が異なっても，アプリケーションから見たときに同一に見えるようにすることである．

3.3 拡張内容概要

Secure UDF は論理フォーマットであるため，要約するとセキュリティ機能を適用する際に必要となる補助情報を記憶媒体上にどう配置するかに尽きる．この補助情報(以下，*セキュリティ情報*)を以下に示す．

a) ACL(Access Control List)
b) 暗号/復号アルゴリズム/鍵情報
c) 改竄検出情報，アクセスログ

拡張のキーポイントは以下の二つである．

- セキュリティ情報をいかに格納するか
- セキュリティ情報をいかに保護するか

さらに，セキュリティ情報に基づいたセキュリティ機能の適用を，Secure UDF ファイルシステムにどのように強制するかもキーポイントとなる．

これらを実現するため，それぞれ以下を規定した．

- セキュリティ情報を格納する Named Stream (*セキュアストリーム*)
- 主としてセキュアストリームを格納するための，暗号化を行う領域 (*セキュア区画*)
- ファイルに適用すべきセキュリティ機能を記述するための属性領域 (*要件拡張属性*)

これらの関係を図 1 に示す．

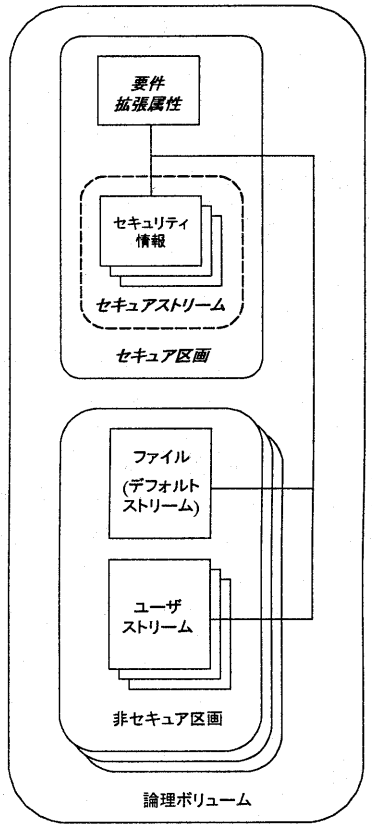

図 1 記憶媒体上の構造

なお，図 1 の配置は一例であり，求められるセキュリティレベルに応じてデフォルトストリームをセキュア区画に置いたりすることも可能

である．

3.4 セキュアストリーム

ここでは一例として，改竄検出情報を格納するセキュアストリームのフォーマットの概要を示す．他のセキュアストリームも，格納する情報が異なるだけで構造はほぼ同様である．

ストリーム名："*UDF_DataIntegrity"

ストリームフォーマット

・ ・ ・
MAC レコードの個数
MAC レコード#1
・ ・ ・
MAC レコード#n

MAC レコード欄は改竄検出情報を含んでおり，基本的にデフォルトストリームを含む全ストリームに対し，ストリームごとに用意する．

MAC レコードフォーマット

・ ・ ・
対象ストリーム名
MAC 識別子
MAC 長
MAC

MAC 欄には改竄検出情報を設定する．MAC 識別子欄は MAC 生成時に使用されたアルゴリズム，使用された鍵の種別を示す情報を含む．

MAC 識別子フォーマット

・ ・ ・
アルゴリズムタイプ
鍵タイプ

アルゴリズムタイプ欄には MAC 生成時のアルゴリズム(例えば Triple DES-MAC)を，鍵タイプ欄には鍵の種別(例えば媒体固有鍵，装置固有鍵等，CPU(システム)固有鍵)を設定する．

以上のようにストリームごとに改竄検出情報を持たせ，ファイルのオープン時に，これと再生成した改竄検出情報と比較することで，改竄の検出を行うことができる．

3.5 セキュア区画

Secure UDF ファイルシステムから見て論理的に連続した領域である区画に，区画内のデータを論理ブロック[1]単位で暗号化するセキュア区画を追加規定した．以下にセキュア区画記述子の概要を示す．

セキュア区画記述子フォーマット

・ ・ ・
実装識別子
暗号方式識別子
・ ・ ・

[1] ファイルシステムがファイルを管理する際の最小単位

実装識別子欄には"*UDF Secure Partition"の文字列が設定される．暗号方式識別子欄には，3.4 の MAC 識別子フォーマットで規定される情報が設定される．

暗号化の鍵として媒体固有鍵を使用した場合には，媒体上の全データを他の媒体に不正にデッドコピーされても，媒体固有鍵が異なるため利用できない．また，CPU(システム)固有鍵を使用した場合には，媒体を不正に持ち出しても他システムでは利用できない．このように求められる要件に応じて鍵を選択することが可能である．

3.6 要件拡張属性

要件拡張属性のフォーマットを以下に示す．

要件拡張属性フォーマット

・ ・ ・
要件機能長
要件機能
・ ・ ・

要件機能欄には，適用すべきセキュリティ機能がビットごとの論理和で設定される．現在，第0ビットがアクセス制御,第1ビットが秘匿，第2ビットが改竄検出，第3ビットがアクセスロギングとして定義されている．ビットが1に設定されている場合，対応するセキュリティ機能をファイルに適用する必要があることを示す．

要件機能長欄には要件機能欄の長さが設定される．

3.7 ハードウェア連携

図2は,記憶媒体上の一部の領域(*セキュア領域*)の暗号化/復号を，記憶装置が持つTRM(Tamper Resistance Module)が行い，この領域をセキュア区画にマッピングする場合を示している．

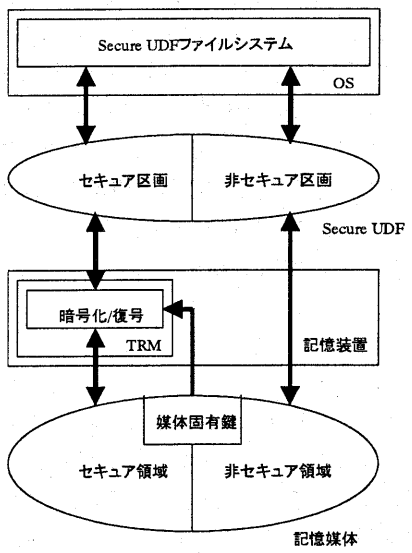

図2 ハードウェア連携の例

媒体固有鍵を記憶装置外に取り出す手段を与えなければ，たとえセキュア区画のデータを他媒体に不正にデッドコピーされたとしても利用することはできない．さらに，Secure UDF ファイルシステムと記憶装置が相互認証を行った上でのみセキュア区画にアクセスできるよう記憶装置を構成することで，デッドコピーを不可能にすることもできる．

4. 試作システム

Secure UDF の有効性を実証するため，Linux 上に Secure UDF ファイルシステムおよ

びSecure UDFフォーマッタ等のツールを試作した．試作した機能は以下の通りである．

- 改竄検出，操作履歴保持/参照機能のためのセキュアストリームサポート
- セキュア区画を含む複数区画サポート
- 要件拡張属性サポート[2]

これらにより，正当な権限を持つユーザが悪意を持ってファイル操作を行った場合には，確実に操作履歴が残るため不正行為の抑止となること，正当な権限を持たないユーザがSecure UDFファイルシステムをバイパスして記憶媒体上のファイルを直接改竄した場合にも，確実に改竄行為があったことを検出できることが確認でき，その効果が実証された．

5. まとめ

多くのアプリケーションから共通に利用できるファイルシステムでアクセス制御，秘匿，原本性保証を行うことのできるよう，業界標準論理フォーマットのUDFをセキュリティ拡張し，Secure UDFとして規定した．さらに，本仕様に基づく試作システムをLinux上に実装し，その効果を実証した．

本仕様は，(財)光産業技術振興協会Fプロジェクトの活動において策定し，UDFの策定元であるOSTAに国際標準化提案したものである．2001年3月のOSTA本会議において，正式に仕様書として発行することが承認され，現在最終校正作業を行っている．さらに本仕様をJISタイプIIの標準情報[3]として公表するため，申請手続き中である．また，本仕様のための拡張ファイルシステムAPI(Application Programming Interface)も同プロジェクトにおいて規定し，JISタイプII標準情報[4]として申請中である．

謝辞

本仕様策定の検討に参加いただいた，Fプロジェクトメンバー各位に感謝の意を表します．

参考文献

[1] Optical Storage Technology Association, "Universal Disk Format Revision 2.01", Mar. 14, 2000

[2] ISO/IEC 13346:1995 Volume and file structure of write-once and rewritable media using non-sequential recording for information interchange

[3] TR X 0040:2001, ユニバーサルディスクフォーマット(UDF)のセキュリティ拡張（原案）

[4] TR X 0041:2001, ユニバーサルディスクフォーマット(UDF)に基づくファイルシステムの応用プログラムインタフェース（原案）

[2] 試作した時点での版数に基づいているため，最新の仕様と若干異なった実装となっている．