1D-6

CyberTrace:共有ファイルのアクセス制御による高精度文書管理

髙橋　宏幸†　　喜田　弘司††　　坂本　久††
サーバソフトウェア事業部†　システムテクノロジーラボラトリ††
NEC システムテクノロジー株式会社

1. はじめに

近年企業内で作成される文書の大半は、電子ファイルの形式であり、ファイルサーバに保管／共有されている場合が多い。したがって、特に機密情報が含まれるファイルは、セキュアに共有する仕組みが必要である。しかし、従来のアクセスコントロールだけでは、内部からの情報漏えい対策としては不十分である。内部からの情報漏えい対策には、共有ファイルを閲覧できる手段を制限するとともに、ファイルの閲覧を許可された人物のファイルの閲覧を監視することが重要である。

本稿では、共有ファイルの情報漏えい対策に着目し、高精度な監視方式と、本方式を利用した文書の保護やログの活用方法を説明する。

2. 共有ファイルの漏えい対策の課題

従来、機密情報を記録したファイルをサーバ上で共有する場合、OS 及びファイルシステムの ACL(アクセスコントロール)や、ファイルと共に ACL を保管する技術などにより、ファイルを閲覧できる人物を制限することは可能であった。しかし、ファイルの閲覧方法には様々な方法があり、閲覧を許可された人物がファイルを閲覧した場合に確実に記録に残すのは困難であった。例えば、あるプログラム内でファイルにアクセスした記録を採取したとしても、それ以外のプログラムでファイルにアクセス手段がある場合、その操作は記録に残すことができない。(図 1)

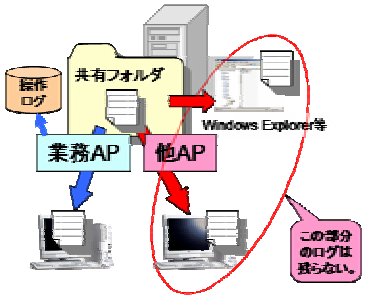

図 1．アクセスログ採取の問題

Monitoring important documents by controlling accesses in a shared file System
Hiroyuki Takahashi, Koji Kida, Hisashi Sakamoto,
NEC System Technologies, Ltd.

また、すべてのファイルアクセスをログに採取した場合、そのログは低レベルな内容となり、解析やその後の再利用が困難なものとなる。

3. 共有ファイルの監視／保護技術

共有ファイルの監視は、ファイルにアクセスする他の手段が存在すれば、特定のプログラムでログを記録していても意味のないものとなってしまう。したがって、ファイルを取得する専用のプログラム以外から、ファイルにアクセスする手段を可能な限り排除する必要がある。

以下の手段(図 2)により、機密情報を記録したファイルにアクセスできるプログラムを一つだけに限定し(以降これをファイルアクセスプログラムと呼ぶ)、他のプログラムからはアクセスできないようにすることで、権限のある人物がファイルを取得した場合に、より精度の高いログを残すことを可能とする。

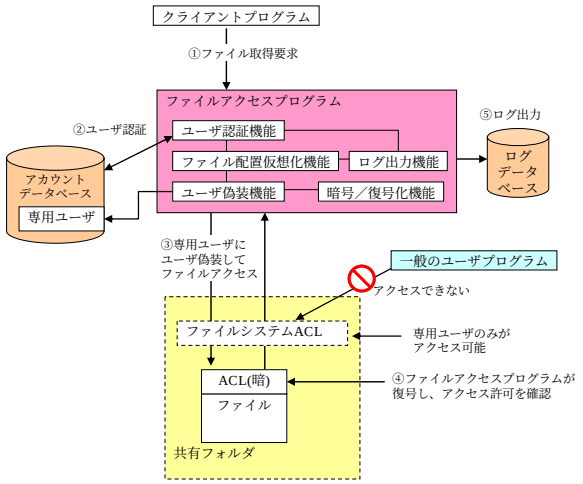

図 2．監視／保護方式

(1) サーバ上に、専用ユーザアカウントを作成する。このユーザアカウントは、OS に対話的にログオンすることができないユーザとして作成し、このユーザのパスワードは、ファイルアクセスプログラムのみが知っているものとする。
(2) ファイルのファイルシステム上の ACL は、専用ユーザのみがアクセス可能な状態にする。
(3) ファイルシステム上の ACL とは別の ACL がファイル内に付加されて保存されている。
(4) ファイルアクセスプログラムは、ユーザ認証を行った後、プロセス(スレッド)を専用ユーザアカウントに偽装してファイルを読み込み、ファイル内に付加されている ACL と認証済みのユー

ザ情報を比較し、アクセス可否を決定する。

この制限を施すことにより、一般のユーザプログラムから対象のファイルにアクセスすることはできなくなる。ただし、OS には、ファイルシステムの ACL を無視する特権が存在するため、さらに以下の保護対策が必要となる。

(5) ファイル、およびファイルに付加されている ACL は暗号化して保存し、ファイルアクセスプログラムのみが復号可能とする。

(6) ファイルの配置構造を仮想化し、実際のファイル名は、ユーザから見えるファイル名とは異なる名前で保存する。

4. 本技術を利用したシステム例

前節の方式を利用したファイルの保護とログの記録(監視)を実現するシステム例を説明する。

4.1 ファイルの保護

ファイルアクセスプログラムを経由しないプログラムは、ファイルが特定できず、また閲覧もできないよう保護する。ファイルシステムフィルタドライバにより対象ファイルへのイベントを監視し、ファイルアクセスプログラム以外のプロセスからのアクセスを拒否する技術の併用により、さらに強度を上げることも可能である。まず、ファイルアクセスプログラム専用のクライアントプログラムを用意する。サーバ共有フォルダ内ファイルは、図 3 のように、クライアントプログラムに対して、ファイルを仮想的にフォルダのツリー構造として見せる。

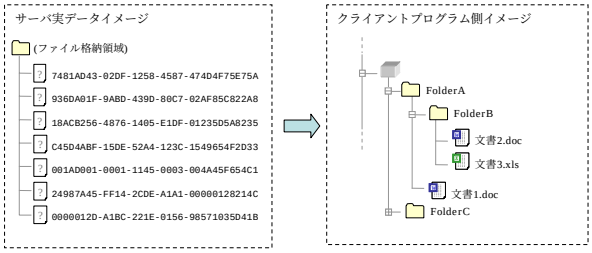

図 3. ファイル構成の仮想化

図 4 のように、クライアントプログラムでの仮想的なフォルダは、実際には XML ファイルとして格納する。XML ファイルは暗号化して格納され、ファイルアクセスプログラムのみが復号できる。このファイルには以下が記述される。

- 仮想フォルダ配下に含まれるファイル、およびサブ仮想フォルダのリスト。このリストにはクライアントプログラムから見える仮想的なファイル名、またはフォルダ名と、それに該当するサーバ上の実ファイル名がペアで記述される。
- 仮想フォルダの ACL。

また、クライアントプログラムから見た仮想的なファイルは、サーバのフォルダ内ではファイルのデータに ACL を付加した形で格納される。

なお、ファイルのデータおよび、ACL は暗号化機能により暗号化されて格納される。

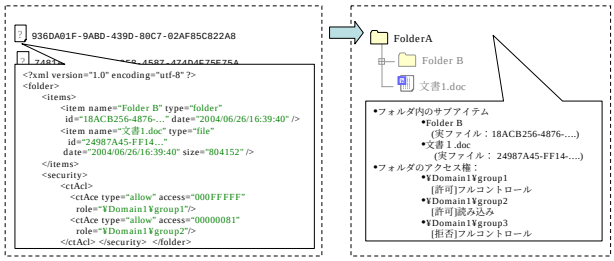

図 4. 仮想フォルダ定義ファイルのイメージ

4.2 ログの記録

権限のある人物がファイルを取得した場合、ファイルアクセスプログラムはクライアントプログラムとの連携により、日時やユーザ名、クライアントマシンの情報(マシン名、IP アドレス等)とともに、どのファイルをクライアントのどこ(保存フォルダ名等)に持ち出したかをログデータベースに記録する。これにより、高精度な監視ログを残すことが可能となる。

4.3 ログの活用

ログの記録により、ファイルが、いつ、誰がどこに持ち出したかを特定できる。また、クライアントマシン上で操作を監視し、ログを記録するシステムが多数存在する。ログビューアプログラムを用意し、両者のログを連携して表示させることにより、持ち出されたファイルがその後どうなったかを特定することも可能となる。

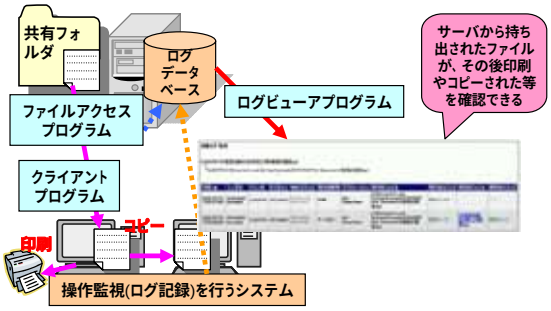

図 5. ログの活用例

5. まとめ

本稿では、権限のある人がファイルを取得した場合に精度の高いログを残せる方式を提案した。特長は、ファイルを取得する専用のプログラムを提供することと、他のプログラムからファイルにアクセスできないようにする技術を有している点である。本方式は、企業内部の人物からの漏えい抑止や高度にセキュリティが要求されるファイルの管理等の用途に有効である。