4ZC-02

細粒度バックアップを用いたファイル復元可能なファイルサーバの設計

永野凛太郎† 稲村浩† 石田繁巳† 中村嘉隆‡

†公立はこだて未来大学システム情報科学部, ‡京都橘大学 工学部情報工学科

1 はじめに

マルウェアの一種であるランサムウェアは猛威を振るっている [1]. 情報セキュリティ白書 2022 中の情報セキュリティ10 大脅威,「組織」向け脅威の順位では「ランサムウェアによる被害」が 1 位となっている [2]. 令和 3 年度における国内の組織向けランサムウェア被害事例の中で 1000 万円以上を負担した割合は 40%以上である [3].

ランサムウェアなどのマルウェアによりファイルサーバ上のファイルを破壊されファイル復元を行う際，手動でファイル復元を行うことは煩雑で困難である．手動でバックアップとファイル復元を行う場合，バックアップをとった時期によっては完全な状態のファイルを復元できない．手動でファイル復元作業をする場合には担当者にバックアップ方法に関する知識が要求される上，ファイル復元作業時には担当者のミスも起こりうる．したがって，自動でバックアップとファイル復元を行うシステムが必要となる．

自動バックアップを行う際，ファイルサーバ側からマルウェアが実行されるタイミングを知ることは難しい．文献 [4] ではランサムウェアプロセスの開始を契機として暗号化されたファイルを自動的に復元する手法が報告されているが，ファイルサーバ上ではクライアント端末上のプロセスを区別できない．このため，ファイルサーバ上で全てのファイルアクセスに対し細粒度にバックアップを取得し，マルウェアの実行タイミングを特定することなくマルウェアによる変更を元に戻す．

本稿では，悪意あるファイル変更からの自動復元を目指すにあたり前提となる，細粒度バックアップ機能と，それを用いたファイル復元機能を備えたファイルサーバを設計したことを報告する．

Design of a File Server Capable of Restoring Files using Detailed Backup

Rintaro Nagano†, Hiroshi Inamura, Shigemi Ishida†, Yoshitaka Nakamura‡

†School of Systems Information Science, Future University Hakodate, Japan,

‡Kyoto Tachibana University, Japan

†{b1019239, inamura, ish}@fun.ac.jp

2 細粒度バックアップシステム

細粒度バックアップシステムを構成するにあたり，ファイルサーバ上のファイルを操作した際に実行される関数に注目する．本研究では，この関数のことをファイル操作関数と呼ぶ．

ファイルサーバ内部ではファイル操作が起こる度に対応するファイル操作関数が呼びだされる．例えば NFS プロトコルに基づくファイルサーバではファイルサーバをマウントしたクライアント端末上でファイル操作を行うとファイルサーバ上では NFS プロトコルで定義されるファイル操作を行うための関数が実行される．この時実行されるファイル操作関数は OS のシステムコールとほぼ一対一で対応するものである．

細粒度バックアップシステムではクライアント端末から送信されたファイル操作のパラメータを時系列順に並べた「ファイル操作列」を記録することでファイルの復元を可能にする．記録するパラメータは実行されたファイル操作関数により異なるが，大別して次の 3 つの情報から構成される．

一つ目は実行されたファイル操作関数の種類である．この情報は実行されたファイル操作をどのようにロールバックするかを決めるために必要となる．

二つ目は実行したファイル操作関数の引数である．例えば，多くの場合で復元に必要となる引数として絶対パスがあげられる．ほぼすべてのファイル操作関数は操作の対象となる絶対パスを引数に指定する．ファイル操作をロールバックする際，削除されたディレクトリを再生成する場合にはディレクトリの絶対パスが，ファイルに加わった変更を元に戻す場合にはファイルの絶対パスが必要となる．他にもファイル名変更操作を元に戻す際には，引数に指定される元のファイル名と変更後のファイル名の両方が必要である．

三つ目はファイル操作関数によって変更する前のファイルのテキストまたはバイナリ情報である．書き込み

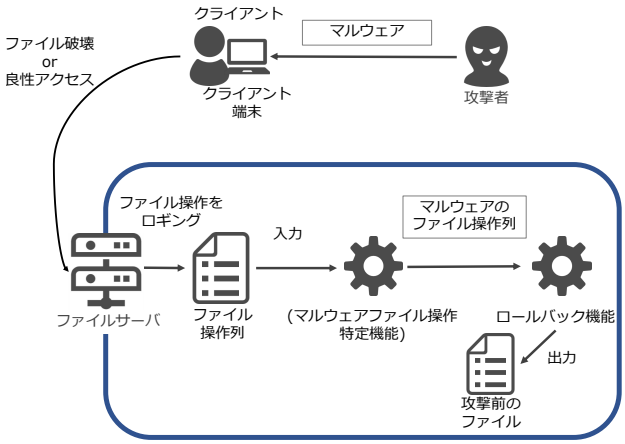

図 1: ファイル破壊から復元までの流れ

などのファイル操作が行われ，ファイルの内容が変更された際，ファイルの状態を元に戻すためには変更前のデータが必要である．

3 実装

細粒度バックアップシステムは記録されたファイル操作列の中からマルウェアによる操作であると判定されたものを選択的にロールバックし，ファイル破壊攻撃からのファイル復元を実現する．

構成するシステムにマルウェアのファイル操作を特定する機構を加えた最終的な流れを図 1 に示す．マルウェアによるファイル操作をロールバックするために，クライアント端末から送信される個々のファイル操作単位で操作列の 1 レコードを定義する．ファイル操作列は次の 4 つ組レコードのリストとして定義される．

```
{TS, file_op_proc, args, op_target}
```

ここで TS はファイル操作の実行タイムスタンプ，file_op_proc はファイル操作関数，args はその引数，op_target は file_op_proc(args) の呼び出しによって変更される対象データの変更前の値である．

細粒度バックアップシステムでファイル操作の選択的なロールバックを行う場合，ロールバック対象のファイル操作列を指定する．ファイル操作列を TS に対して逆順にソートし，その順で各レコードに対して以下の手続きを実行する．

```
reverse_file_op_proc(file_op_proc, args,
                     op_target)
```

ここで，reverse_file_op_proc は file_op_proc の逆の操作を行う手続きである．

4 実装と評価

本研究では，オープンソースのファイルサーバである UNFS3 [5] を拡張する形で実装を行い，実験に用いるファイルサーバを開発する．UNFS3 は NFS ver3.0 [6] プロトコルを実現したファイルサーバ実装であり，ユーザースペースで動作する．したがって本研究におけるファイル操作関数は NFS ver3.0 の手続きに対応するものである．

今後，提案システムの性能を評価する予定である．実際に構成したシステム上で特定のファイル操作を行い，ファイル操作の記録に伴う処理時間の増分などの提案システムの性能を評価する．

5 おわりに

本稿では，細粒度バックアップ機能とファイル復元機能を備えたファイルサーバの設計について報告し，今後の評価にも触れた．次の課題として，ファイルサーバ上のファイルを破壊するマルウェアによる攻撃からのファイル復元の検証を行う予定である．

参考文献

[1] 独立行政法人情報処理推進機構（IPA）セキュリティセンター：コンピュータウイルス・不正アクセスの届出状況 (2022).

[2] 独立行政法人情報処理推進機構（IPA）：情報セキュリティ白書 2022 (2022).

[3] 警察庁：令和 3 年におけるサイバー空間をめぐる脅威の情勢等について (2022).

[4] Continella, A., Guagnelli, A., Zingaro and et al.: ShieldFS: A Self-Healing, Ransomware-Aware Filesystem, *Proc. 32nd Annual Conference on Computer Security Applications (ACSAC)*, pp. 336–347 (2016).

[5] Schmidt, P.: UNFS3: User-space NFSv3 Server, https://unfs3.sourceforge.net/ (参照 2022-12-22).

[6] Staubach, P., Pawlowski, B. and Callaghan, B.: NFS Version 3 Protocol Specification, RFC 1813 (1995).