履歴追跡結果の表示方式の検討[1]

森山令子[2]　郡光則[3]　平井規郎[4]
三菱電機株式会社　情報技術総合研究所[5]

1. はじめに

蓄積されたログデータの活用のため、関連する複数のデータを統合し、イベント発生による状態遷移をグラフ構造で表現することで、効率よく履歴追跡を行うデータモデルの検討を進めている([1])。

本稿では、PC 上で対話的に履歴追跡を行い、実行結果をわかりやすく表現することでユーザの理解を深め、また、スムーズな操作の実現を目的とした表示方式の提案を行う。

2. 結果表示に関する課題

一例として、図１の PC の操作ログから得られた履歴追跡結果を表すデータモデルの表示方法として、図２のようなリスト形式がある。

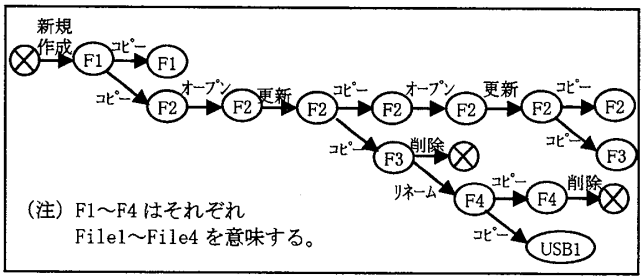

図１．履歴追跡結果（データモデル）

```
(タイムスタンプ　　ｲﾍﾞﾝﾄ　ユーザ　引数１　引数２)
2007/12/01 09:05:20 新規作成　A　File1
2007/12/01 09:30:13　コピー　　B　File1　　File2
  2007/12/01 09:32:40 オープン　B　File2
  2007/12/01 11:53:36　更新　　B　File2
  2007/12/01 21:22:02　コピー　　C　File2　　File3
      2007/12/01 21:35:26 リネーム　C　File3　　File4
        2007/12/01 21:38:54　コピー　　C　File4　　USB1
        2007/12/01 21:42:29　削除　　C　File4
  2007/12/02 15:47:39 オープン　B　File2
  2007/12/02 16:14:08　更新　　B　File2
  2007/12/03 07:48:21　コピー　　D　File2　　File5
```

図２．ファイル操作の履歴追跡結果表示例

この方法では、追跡対象に関係する全ての操作が混在して表示されるため、どのような経緯で遷移したか一見してわかりにくく、また、全体との関係がつかみにくいという問題があった。

1 Visualization for Results of Traceability
2 Ryoko Moriyama 3 Mitsunori Kori 4 Norio Hirai
5 MITSUBISHI ELECTRIC CORPORATION INFORMATION TECHNOLOGY R&D CENTER

3. 結果表示方式の提案

本稿では以上のような履歴追跡結果の表示方法について提案する。

3.1. 複数のインスタンス関係の表示

本提案の前提となるデータモデルでは、インスタンスがイベントの前後で１対１に対応する順序関係と１対多、あるいは多対１に対応する階層関係を想定する。前者の例としてファイルのオープン及び削除、後者の例としてファイルのコピーや結合がある。データモデルで表現した例を図３に、履歴追跡結果の表示例として図４に示す。

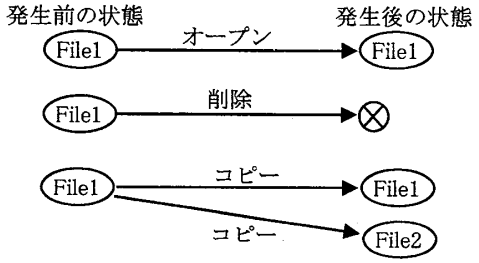

図３．データモデルによる表現

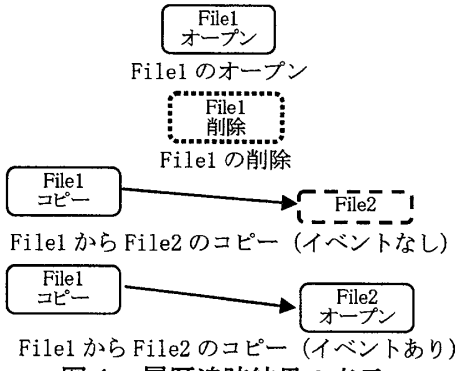

図４．履歴追跡結果の表示

図４では、インスタンスとイベントを１つのノードでまとめて表示する。ファイルコピーなど、新たなインスタンスが発生する場合には、ノードの Y 座標をずらすなど親子関係を示すインデントをつけた表示方法とする。また、新たに発生したインスタンスに対応するイベントの有無や、ファイル削除などターミネータに対する表示方法もノードの枠を点線表示や破線表示にするなど異なる表示方法で区別を明確にする。

3.2.履歴追跡結果の表示

図１の履歴追跡結果に対し、全体を表現する際に、ユーザが注目したい属性情報をノード上に表示することでユーザの理解度を深める。ファイルクラス ID、ユーザクラス ID、イベント、日時、等インスタンスの持つ属性情報から任意の情報を選択して表示する。

例えば、図１の履歴追跡結果について、ノード上にユーザクラス ID とイベントを表示すると図５のようになる。

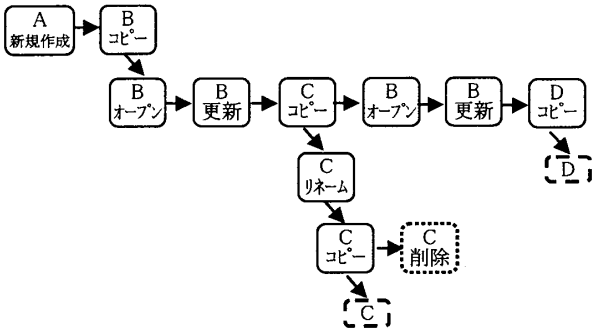

図５．履歴追跡結果の表示例１

ユーザ A が作成したファイルが、ユーザ B,C,D にコピーされ、ユーザ C でリネーム後にさらにコピーされ削除、ユーザ D ではコピーに続くイベントが無しであることが示されている。

3.3. 視点の切替え

図１の履歴追跡結果はファイルクラスで履歴追跡を行った例であるが、例えば図５の状態で、続けてユーザ C の履歴に注目したい場合にはユーザクラスで履歴追跡を行い、結果を表示する。ユーザＣに関連したデータモデルでは、ファイルクラスとユーザクラスを図６のように表現することができる。図６において順序関係を実線、クラス間関係を破線で示す。

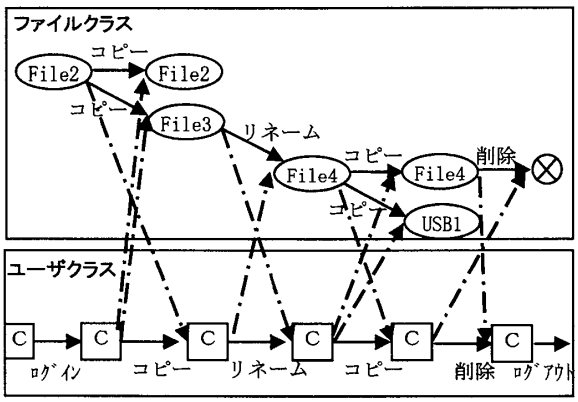

図６．ユーザＣの操作（データモデル）

ユーザＣをユーザクラスで履歴追跡を行うとログイン、コピー、リネーム、コピー、削除、ログアウトの順序関係を持つ。これを本稿の履歴追跡結果で表示しノード上にイベントと引数１を表示すると図７のようになる。

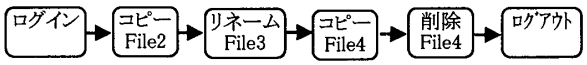

図７．履歴追跡結果の表示例２

このように、クラスを切替えて履歴追跡を行い、それぞれの履歴追跡結果を表示する手段を提供することで、ファイルで履歴追跡（図５）→ユーザで履歴追跡（図７）→再び図７より別ユーザでの履歴追跡、といった操作も可能となり、追跡対象に関係した各ユーザの振る舞いの把握が可能となる。

3.3. 条件と一致するノードの強調表示

履歴追跡結果に対し、「タイムスタンプが『22 時～5 時』、かつイベントが『コピー』」などといった条件と一致するものを強調表示する機能により、多数のノードが存在する場合に操作性の向上が期待できる。例えば図８に示すように多数のノードが存在する場合に、表示色を変えるなど強調表示する。これによりユーザは強調表示されたノードに対しユーザクラスで追跡するなど、対話的な操作性が実現できる。

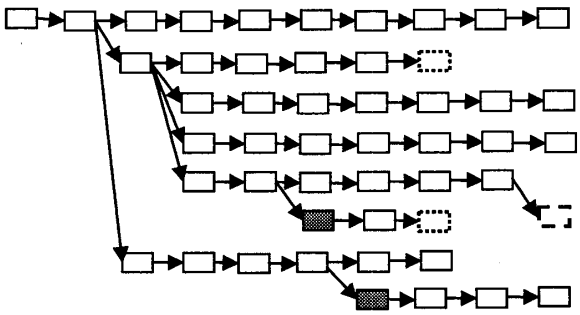

図８．履歴追跡結果の強調表示例

４．おわりに

本稿では、履歴追跡結果を表示する方法を提案した。今後は様々な分野のデータを使用した履歴追跡結果に対し本提案の表現方式を適用することで評価のフィードバックを行い、ユーザの理解度を深める表示方法の研究開発を進める予定である。

参考文献

[1] 履歴追跡に適応するデータモデルの検討, 平井, 森山, 郡, IPSJ 70 回全国大会予稿集