D-011

履歴データ管理方式の評価
Evaluation of Log data management method

森山 令子† 平井 規郎† 郡 光則†
Ryoko Moriyama Norio Hirai Mitsunori Kori

1. はじめに

近年、IT 化の普及などを背景に、様々な場面でログを採取し蓄積し活用しようという動きが強まっている。我々は、蓄積されたログを活用するため、複数のログを統合し、各々に記録された対象の履歴を追跡するための履歴追跡型データモデル及びデータモデルの表示方式の検討を行い、履歴データ管理を実装した ([1]、[2])。

本稿では、提案する履歴データ管理方式の評価結果について報告する。

2. 履歴データ管理方式の概要

2.1 履歴追跡型データモデル

イベントによる状態変化をグラフ構造で管理し、イベントの発生順あるいは逆順で履歴追跡を実現する。

2.2 履歴追跡型データモデルの表示方式検討

履歴追跡結果はグラフ表示とし、ノード上の表示情報は追跡クラスごとに変更可能とする。また、関連情報を TIPS 表示することで内容を把握できるようにした。さらに、履歴追跡結果画面から、継続して視点を変更して再実行することも可能とする。

3. 履歴データ管理方式による履歴追跡

我々は、履歴データ管理方式を実装した。本実装方式による、履歴追跡について説明する。

3.1 履歴追跡型データの作成

まず、ログデータから追跡時の視点となるクラス情報を含む履歴追跡型データを作成する。クラスは「ユーザ」、「ファイル」などであり、クラス情報は各クラスの親子関係についてまとめたものである。ログデータと履歴追跡型データの関係の例として、２種類のログデータから履歴追跡型データを生成した例を図 1に示す。

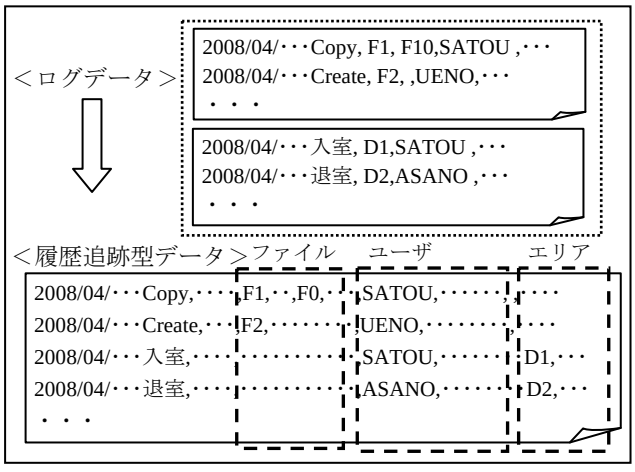

図1 ログデータから履歴追跡型データの作成

本実装方式では、図 2に示すように、点線枠で示されるクラス内関係及び履歴追跡型データの同一行情報のクラス間関係をクラス情報で管理している。また、各クラスの実際の値はインスタンスIDとして管理している。

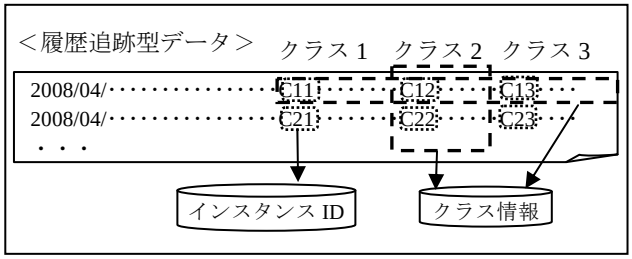

図2 本実装方式でのデータ管理

3.2 履歴追跡結果の表示と視点を変えた履歴追跡

本実装方式による画面遷移例を図 3に示す。図 3では結果表示に関する部分だけ抜粋して表示している。

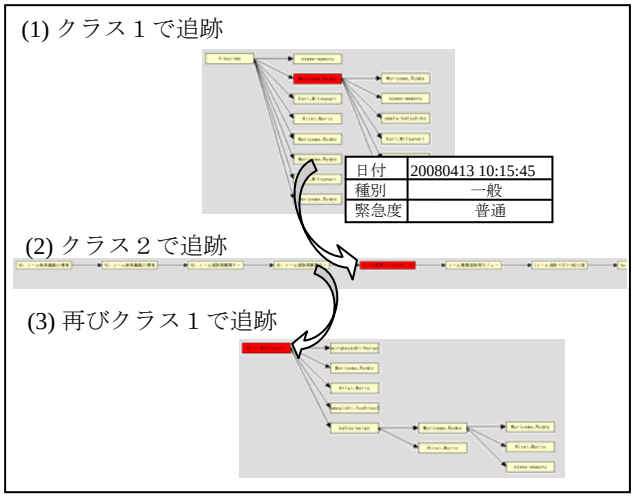

図3 履歴追跡の実行

追跡対象に対する履歴追跡結果はノードの遷移として表示する。また、ノード上に追跡クラスごとに表示する属性情報の指定が可能であり、その他の属性情報はTIPS表示する。TIPS情報は図 3の(1)に示されるような画面であり、各ノード上へのマウス移動により表示される。

ユーザは、ノード上の情報あるいは TIPS 情報を確認してから、表示結果画面より次の追跡対象を選択し、(1)→(2)→ (3)のように視点を切り替えながら、続けて履歴追跡を実行する。

† 三菱電機株式会社 情報技術総合研究所 Mitsubishi Electric Corp. Information Technology R&D Center

4. メール追跡による評価

本実装方式にメールデータを適用し、評価を行った。本実装方式でメール追跡を行う場合に、必要となる準備、及び、視点を切り替えながら履歴追跡を行うことによる効果の検証を目的とした。

4.1 メールデータの変換

メールサーバに蓄積したメールデータを使用する。また、メールはヘッダとボディから成るが、ヘッダを抽出してから、履歴追跡型データに変換したものを使用した。ヘッダ抽出の際には、1 通のメールを送信者、受信者総数と複数データに分割し、「１人がN人に送信した」場合、「N個のイベントが発生した」ものと扱う。また、受信者総数はTo/Cc/Bccの合計とした。図 4に例を示す。

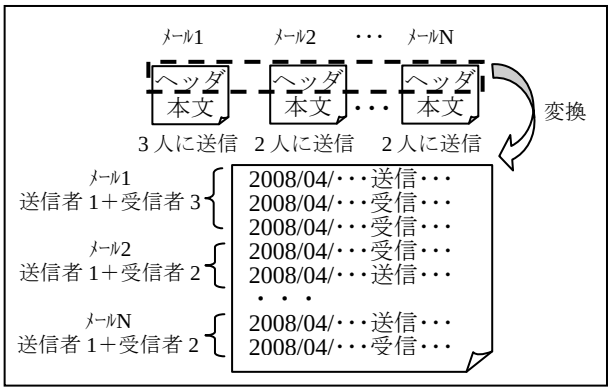

図4　メール用履歴データの作成

4.2 メール用履歴追跡型データの作成

「メッセージ」と「ユーザ」の２つのクラスを定義してメール用の履歴追跡型データを作成した。「メッセージ」はヘッダのMessageID、「ユーザ」は、送信時はFromの値、受信時はTo/Cc/Bccいずれかの値とする。図 5にメール用の履歴追跡型データの例を示す。

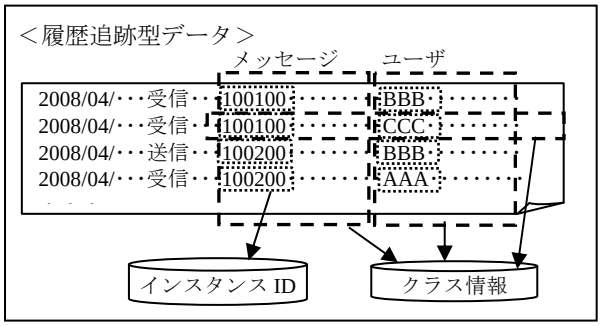

図5　メール用の履歴追跡型データ

4.3 メール追跡での評価

追跡対象として選択したメールを、メッセージで履歴追跡した結果の例を図 6に示す。図 6ではノード上にユーザ名が表示されている。先頭ノードのユーザが６人にメールを送信し、その中の一人が６人に返信、次に５名に返信する、と４回返信を繰り返す様子を表している。

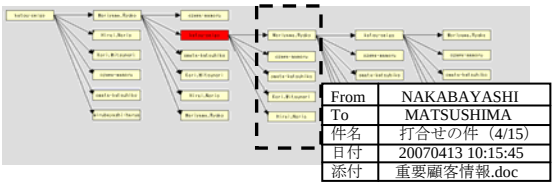

図6　メッセージクラスでの履歴追跡結果例

例えば、追跡対象が送信したメールに、図 6のTIPSに示されるようなファイルが添付され、その添付ファイルの伝播経路を知りたい場合を考える。図 6の点線枠内のノードにはTIPS情報で添付ファイルが表示される。それ以降のノードで添付ファイルがない場合も、追跡対象のメールの返信が繰り返される範囲で伝播していないだけである。その場合、ファイルを伝播する可能性が高い添付ファイルを受信した点線枠内の各ユーザについて、視点をユーザに切り替えて履歴追跡を実行することで、添付ファイルの送信を確認することができる。その際は、点線枠内のノードを順に選択し、視点をユーザに切り替えて履歴追跡を行い、図 7のような履歴追跡結果画面を得る。

図7　ユーザクラスでの履歴追跡結果例

図 7において、点線枠内のノードが、ユーザが添付ファイルを受信した以降のメールに関する操作を意味する。添付ファイルの送信の有無をTIPS画面で確認することで、受信した添付ファイルの送信の可能性が把握できる。続けて図 7の点線枠内の添付ファイルを送信したノードで、メッセージに視点を切り替えて追跡することで、さらなる伝播の可能性が把握できる。

以上のように、メッセージクラスだけでは独立した履歴であるものを、履歴追跡結果の情報を確認しながらユーザクラスという視点に切り替えて履歴追跡を行い、さらに視点をメッセージクラスに切り替えた履歴追跡結果の情報確認を行うことで、関連付けを把握できるという効果を得た。

5. おわりに

本稿では、履歴データ管理方式の実装により、履歴追跡型データモデルを適用し、履歴追跡結果の表示及び視点を切り替えた操作が可能であることを確認した。さらに、メールデータを適用した評価では、視点を切り替えた履歴追跡と履歴追跡結果の確認により、１つの視点では独立した複数の履歴を関連付けて把握できる効果を得た。

今後は、実用化に向けた研究開発を進める予定である。

参考文献

[1]平井 規郎，森山 令子，郡 光則，“履歴追跡に適応するデータモデルの検討”,IPSJ 70 回全国大会講演論文集,3B-6(2007).
[2]森山 令子，郡 光則，平井 規郎，“履歴追跡結果の表示方式の検討”,IPSJ 70 回全国大会講演論文集,3B-7(2007).