D-045

行動履歴追跡機能を備えた統合ログ管理システム
Integrated Log Management System with Behavior Trace Function

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

1. はじめに

近年、法令順守やセキュリティ管理意識の高まりから、外部からの不正侵入や内部からの情報漏えいに関する情報を管理する統合ログ管理システムの重要性が高くなっている。

我々は、履歴追跡型ログ DB [1]を統合ログ管理システムに適用することで、行動履歴追跡機能を備えた統合ログ管理システムを実現した。本稿では、統合ログ管理システムの強化機能と評価結果について報告する。

2. 課題

従来の統合ログ管理システムには以下の課題がある。

- ログから条件に合うイベントを検索して行動一覧を得ることは容易であるが、検索したログの関連付けがわからない。
- 内部情報流出の原因究明などを目的に、複数のイベントを順序付けて定義した行動パターンでログを検索することが困難。

3. 行動履歴追跡機能

以上のような課題に対し、我々は、行動履歴追跡機能を備えた統合ログ管理システムを提案し、実装した。これは、図 1に示すように、統合ログ管理基盤[2]に、履歴追跡型ログDBを適用したものである。

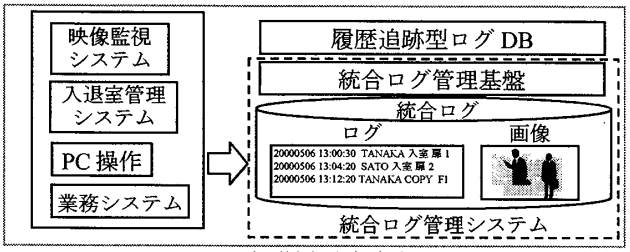

図1 行動履歴追跡機能

統合ログ管理基盤では、映像監視システムのスナップショット画像（以下、画像）を入退室管理システムなどその他のログと関連づけることで、一元管理を行う。

3.1 追跡機能

ログに分散する情報を関連付けた行動履歴として結果を取得する追跡機能を実現した。

以下、追跡対象となるカテゴリをクラス、クラス内で一意に識別可能な ID をインスタンス、ログに含まれる動作をイベントと呼ぶ。我々は、ログに含まれるイベントとイベントの前後で遷移するインスタンスの状態について、クラス内関係とクラス間関係をグラフ構造で効率的に管理する履歴追跡型データモデルを提案した。これを履歴追跡型ログ DB で実装することで、追跡を可能とした。

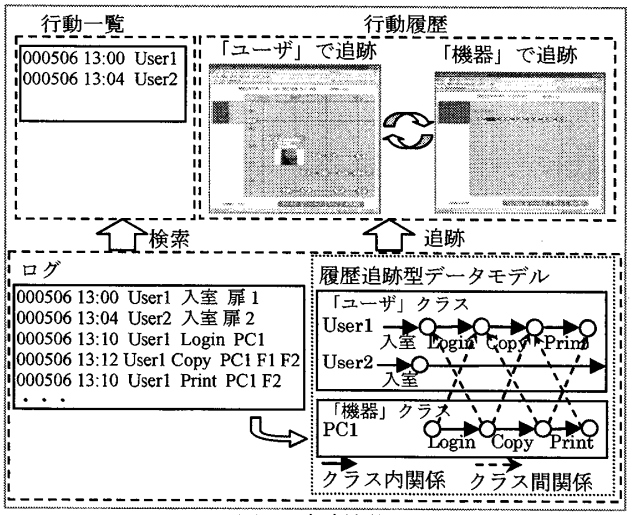

図2 追跡機能

図 2のようなユーザ、機器クラスの場合、User1 やUser2、PC1 についてイベントによる状態の遷移をクラス内関係で、User1 とPC 1 の関係をクラス間関係で管理する。これにより、User1 で履歴追跡の実行や、User1 の行動履歴からクラス間関係を持つPC1 の履歴追跡の実行が可能となる。また、行動履歴は、ログに含まれる日付や画像など任意の項目を関連情報として属性に持つという特長を持つ。さらに、クラスを変更して追跡ができるという特長も持つ。

3.2 行動検索機能

行動パターンを検索条件として、一致するインスタンス一覧を取得する行動検索機能を実現した。

例えば、「イベント A の後にイベント B を 2 回実行」などの条件に一致するインスタンス一覧を取得する。

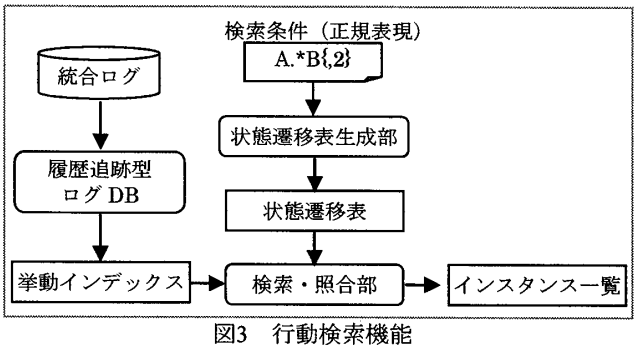

図3 行動検索機能

† 三菱電機株式会社 情報技術総合研究所
MITSUBISHI ELECTRIC CORPORATION
INFORMATION TECHNOLOGY R&D CENTER

図 3に示すように、履歴追跡型ログDBでは、統合ログの状態遷移に含まれるイベントや状態をユニークなID値に変換してから挙動インデックスを生成する。挙動インデックスとは、3.1で説明した履歴追跡型データモデルを実体化したものである。

また、正規表現で指定された検索条件は、状態遷移表生成部で状態遷移表に変換される。検索・照合部で、sDFA 文字列照合方式[3]により、挙動インデックスを走査して状態遷移表と照合し、インスタンス一覧を得る。sDFA 文字列照合方式は、DFA 方式の必要メモリ量を削減することで高速照合を実現した。

4. 適用評価

4.1 既知の事実からの追跡

追跡機能が関連する行動や原因となる事実の追跡に有効であり、ログの内容把握が効率化できることを検証する。

例えば、あるユーザが紛失した ID カードで印刷したことがわかっているケースを考える。

まず、図 4①のように時期やユーザID、「印刷」イベントから該当ログを検索し、ユーザIDで行動履歴追跡を実行する。実行結果より、IDカードの不正使用で、印刷以外にコピーや、入室／退室記録を残していないといった一連の行動が把握できる。その際、画像で確認することにより、IDカードの使用者が本人でないことの確認も可能となる。

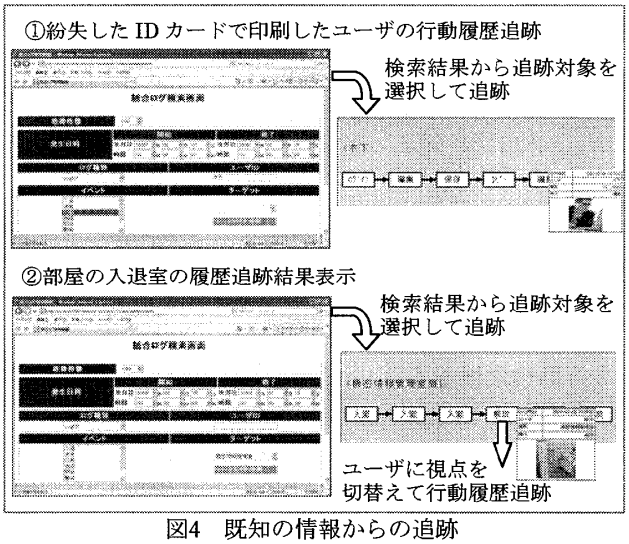

図4　既知の情報からの追跡

次に不正入室に関する事実を確認する。図 4②のように不正入室が行われた可能性のある時間と部屋を指定してログを検索し、部屋の扉の行動履歴追跡結果を得る。部屋の扉が解放され、その前後は正常な入退室のみであることより、不正入室の原因が扉の解放であったことが確認できる。続けて、扉を解放したユーザに着目し、ユーザの行動履歴追跡を実行する。それにより、発覚した扉の解放以外に、不正につながる行動の有無が確認できる。

以上のように、ログに関連付けを持たせて管理することで、行動履歴として追跡することが可能となる。それにより、既知の情報から関連する行動の把握や、対象となる行動の原因究明に有効であり、ログの内容把握の効率化を確認できた。

4.2 ユーザ定義の行動からの追跡

行動検索機能が、これまで見つけることができなかった事実の把握や、状況の把握に有効であり、ログの内容把握が効率化できることを検証する。

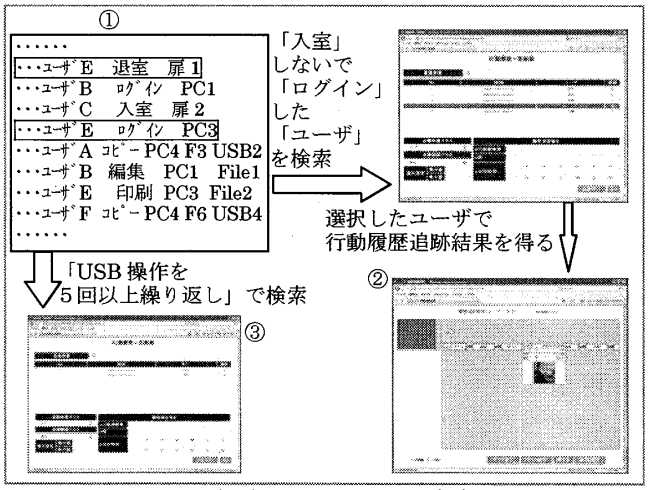

図5　行動パターンからの追跡

例えば図 5①のようなデータに対し、不正行動パターンとして「入室しないでログイン」を定義する。

まず、行動検索機能で、定義した不正行動パターンに該当する「ユーザ」一覧を検索し、検索されたユーザの行動履歴追跡を実行する。実行結果より、図 5②のようにコピー、印刷と組み合わせた操作で重要ファイルの不正印刷を行った事実が明らかになるなど、複数のログを組み合わせた行動の確認で不正行為の把握が可能になる。

また、「機器」に対し、不正行動につながる操作として「USB操作を５回以上繰り返し」と定義して検索することで、図 5③のように不正行動の発生しやすい機器やユーザの把握が可能となる。

以上のように、行動パターンを定義して行動検索を実行することで、従来では発見できなかった事実や状況の把握が可能となり、ログの内容把握の効果化を確認できた。

5. おわりに

我々は、行動履歴追跡機能を統合ログ管理システムに実装し、行動履歴追跡実行、及び、定義した行動パターンによる行動検索を実現した。

ログを関連付けて管理することで、既知の事実から関連する事実の把握や原因究明のための追跡に有効であることを確認した。また、行動検索機能により、行動パターンによる検索を実現することができ、さらに追跡機能で、関連する事実や状況の把握も可能になることを確認した。行動履歴追跡機能を備えた統合ログ管理システムにより、ログの内容把握の効率化に有効であるという結論を得た。

参考文献

[1]平井 規郎, 森山 令子, 郡 光則, “履歴追跡型データモデルの評価”, 日本データベース学会論文誌, Vol.7, No3, pp.73-78(2008).
[2]山岸 義徳, 郡 光則, “入退管理・映像監視システム向け統合ログ管理方式”, 第 7 回情報科学技術フォーラム, D-034(2008).
[3]中村隆顕, 郡 光則, “大規模正規表現の高速照合方式”, 情報処理学会全国大会第 67 回, 4F-5 (2005).