7N-5　分散型ソフトウェア開発環境における ユーザ利用経路追跡アルゴリズム

筒井宏史　貫井春美　三原幸博
株式会社 東芝　システム・ソフトウェア技術研究所

1．まえがき

ソフトウェア開発支援システムＩＭＡＰ(Integrated Software MAnagement and Production Support System)が前提としている分散型ソフトウェア開発環境におけるネットワーク管理の研究に着手し、１つの組織内のＬＡＮにおける管理情報を把握するネットワークモニタシステムを提案した[1]。しかし、複数のＬＡＮが相互接続された場合、ＬＡＮ外部への対応が課題であった。ＬＡＮを相互接続することは、ユーザに対してそれだけ広域な資源を利用できるという利点を与えるが、その反面、遠隔から不正なユーザに侵入される等、いくつかの問題点も生じる。

本稿では、複数のＬＡＮを相互接続したコンピュータネットワークで、ユーザの利用経路を把握するアルゴリズムについて報告する。

2．対象ネットワークの前提条件

分散型ソフトウェア開発環境の特徴の１つである構成の柔軟性を踏まえて、ターゲットとするネットワークの前提条件を以下のように定める。［図１］

・一つの組織単位のＬＡＮを管理ドメインと定義する。管理ドメインは相互に接続可能で、ネットワーク全体を管理ドメインの集合として捉える。

・管理ドメインの中の各ノードはユニークに識別され、ノード間で相互に通信が可能である。

・各管理ドメインは直接自身と接続された管理ドメインのみを認識している。すなわち、隣接しているドメインは相互にユニークに識別される。

・経路追跡の対象となるノードはコンピュータネットワーク上の１つのコンピュータシステムであり、他のコンピュータシステムからネットワークを介して利用可能なものとする（他のコンピュータシステムから利用できないものはターミナル同様の扱いとする）。

・各ノードは以下の管理情報を提供できる。

i)ユーザ情報　…ノードを利用しているユーザ名、そのユーザの利用時刻（ログイン時刻）、利用端末名、進入元ノード名（リモート利用の場合、どのノードから利用しているか）

ii)プロセス情報…ノードで起動されているプロセス名（パラメータ含む）、そのプロセスの起動された時刻、起動したユーザ名、起動端末名

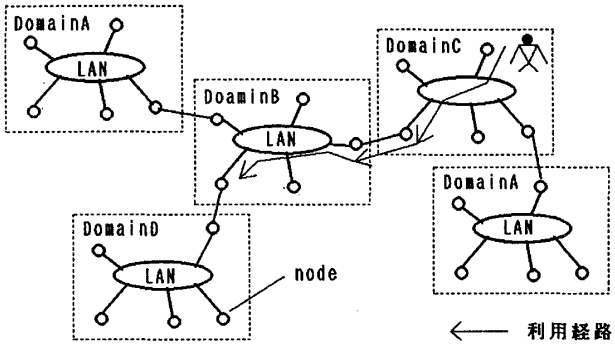

図１　対象ネットワーク

3．ユーザ利用経路追跡アルゴリズム

3-1.基本アルゴリズム

利用経路の追跡を以下の２段階で行う。

(1)管理ドメイン内の追跡

管理ドメイン内で経路を把握する。すなわち、１つの管理ドメイン内を利用しているユーザの経路は、その管理ドメインで確実に把握する。隣接する管理ドメインから進入しているユーザについては、どのドメインに属するどのノードから進入しているかまで把握する。

(2)管理ドメイン間の追跡

隣接するドメインから利用経路が及ぶ場合には、ドメイン間で追跡情報を交換し、追跡を依頼する。

以下にその詳細を示す。

3-2.管理ドメイン内アルゴリズム

各ノード間では、先に示した管理情報を相互に要求・転送する手段を持つ。また、自ノードがリモートから利用される時に使用可能なプロセスを把握している。

ユーザ情報より、追跡対象ユーザがリモートノードから利用しているか否かを判断する。リモートノードから利用している場合には、そのリモートノードに、ユーザ名、コネクションプロセス、利用時刻、システム時刻を送信し、追跡を依頼する。これを順次繰り返し、対象ユーザがローカルに存在するノードで追跡は終了する。

しかし、以下の場合には経路を一意に決定できず、追跡が無限ループに陥り収束しないといった問題がある。［図２］

(a)１つのノードを対象ユーザが複数利用している

"User Tracking Algorithm in Distributed Software Developing Environment"
Hiroshi Tsutsui, Harumi Nukui, Yukihiro Mihara
TOSHIBA Corp. Systems & Software Engineering Lab.

(b)対象ユーザが途中でユーザIDを変更している
(c)経路がループしている

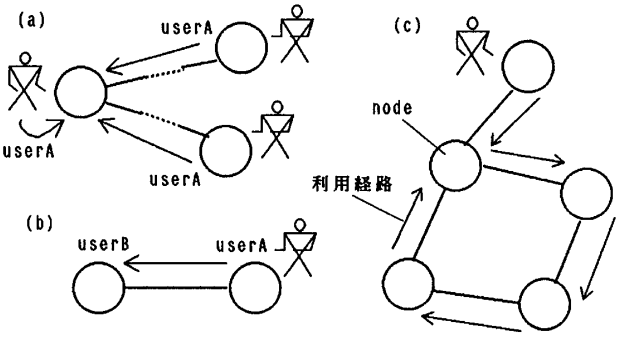

図２　利用経路例

このような問題を解決するために、ノード間でリモート利用ユーザを一意に対応づける。そのためにユーザ情報だけでなく、プロセスと時間の情報を組み合わせて利用する。進入先ノードでの利用時刻とリモート利用のために起動されたプロセス名により、進入元ノードで対応するプロセスを検出し、そのプロセスを起動しているユーザを対象ユーザと判断する。これにより、ユーザの利用経路は一意に決定され、確実に追跡は収束する。

進入元ノードが隣接ドメインに属する場合、管理ドメイン間のアルゴリズムに進む。

3-3.管理ドメイン間アルゴリズム

管理ドメインには、ドメイン内の情報を収集し、他のドメインに転送する役割を担うノード（＝ドメインマスタ）を置く。

各管理ドメインは、隣接するドメインのドメインマスタの名前を把握しており、通信を行う手段を持つ。

リモート利用ユーザの進入元ノードが隣接するドメインに属する場合、その隣接ドメインのドメインマスタに経路追跡を依頼する。依頼されたドメインマスタは、3-2章の手順により、指定されたノードから利用経路追跡を開始し、収集した情報をまとめて依頼元のノードに転送する。

以上のアルゴリズムをまとめて図３に示す。

3-4.ノード間の時計の同期

ノード間で追跡対象ユーザをユニークに対応づけるために利用開始時刻を用いている。この方法では、各ノード間の時計の誤差が問題となる。

本アルゴリズムでは以下のような方式により、時計の誤差に対応する。

追跡の要求プロトコル内に、進入先ノードと進入元ノード間の時計誤差のチェックを組み込み、その誤差を差し引いてリモート利用時刻とプロセス起動時刻の対応を図る。さらに、修正時刻で対応しない部分については、リモート利用の時刻順にシリアル番号をふり、その番号により吸収する。

この方式により、より確実な経路の対応づけが行える。

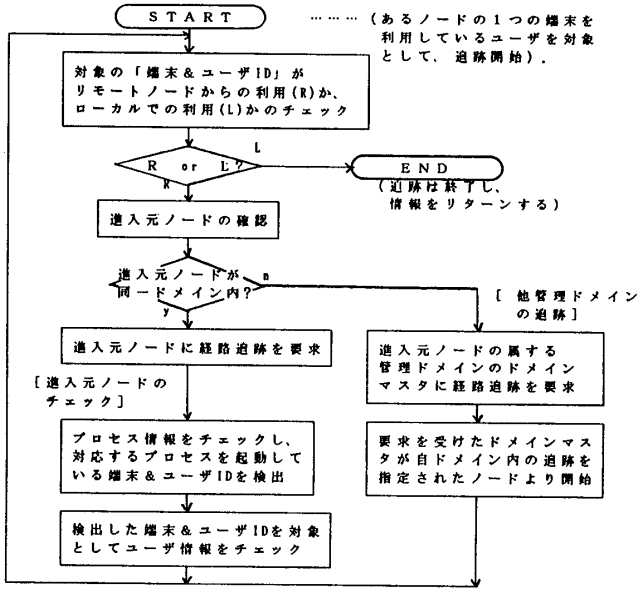

図３　利用経路追跡アルゴリズム

４．効果

分散型ソフトウェア開発環境においてユーザの利用経路を把握することにより、以下の効果が期待される。

＜不正ユーザの侵入検出＞

把握した利用経路から”不審なユーザ”と考えられる利用形態（同一ユーザが物理的に離れた場所に同時に存在する、リモート利用時に不当にユーザIDを変更している、等）を抽出し、そのユーザに警告を発する、サービスを停止する等のアクションをとるためのトリガーとする。これにより不正なユーザの侵入防止の一助とする。

５．まとめ

分散型ソフトウェア開発環境においてネットワーク全体を把握することなく、隣接するドメインのみを認識するだけでユーザの利用経路を一意に把握するアルゴリズムを提案した。

今後、このアルゴリズムに基づいたユーザ利用経路追跡システムを試作し、評価を行う。

［参考文献］

[1]筒井、他：「水平分散環境におけるネットワーク管理」
情報処理学会　第37回全国大会予稿集
[2]G.Skinner,etc., "RESOURCE MANAGEMNET IN A DISTRIBUTED INTERNETWORK ENVIRONMENT."
ACM comm., April,1988.
[3]塚本、他：「分散処理」昭晃堂