ユーザモデルを利用した継続的認証システムについて*

6 B − 4

高井 英樹　佐藤 究　宮崎 正俊†

東北大学大学院情報科学研究科宮崎研究室‡

e-mail: takai@dais.is.tohoku.ac.jp

1　まえがき

従来の主な認証方法として、パスワード方式、生物学的特徴（指紋、網膜のパターンなど）を利用した方式、携帯認証装置（磁気カードなど）を利用した方式、セッション暗号化方式などがある。しかしこれらは、次に挙げる問題点すべてを解決することはできない。1. パスワードの盗聴および推測の可能性 2. 継続的な認証が難しいこと 3. 使いやすさ 4. 管理の手間。

そこで筆者らは、ユーザモデルを利用した継続的な認証システムを提案する。このシステムでは、特定ユーザの計算機利用における特徴、癖、タスクの傾向等を反映したユーザモデルに基づき、実利用者の操作やタスクとユーザモデルから推論される操作やタスクにおける差異を感知することにより利用時の継続的ユーザ認証を行なう。

本稿は、まず 2 章において提案認証システムの概要を述べる。次に 3 章において、このシステムの構成要素それぞれについて詳しく述べる。4 章はまとめである。

2　概要

本章では, 認証システムの概要について述べる（図 1）。ユーザが計算機を利用しているとき、そのユーザが正当なユーザか不正なユーザかの認証は次のようにして継続的に行なう。

ユーザの入力・操作はユーザインタフェースを通して取り込まれる。ここでユーザの入力・操作とは、具体的には次のものを意味する。

- 使用したコマンド
- コマンド中で使用したオプション
- コマンドの組合せ
- 参照ファイル
- 使用時間
- キータイプの速さ

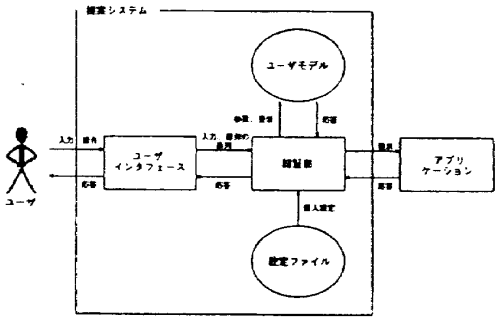

図 1: システム概要

本システムにおけるユーザモデルは、特定ユーザの計算機利用時における特徴、癖、タスクの傾向等を反映した、仮想的なユーザの利用のモデルである。このモデルから、ある状況における特定ユーザの操作、利用のパターンや傾向を引き出すことができる。またこのモデルは、最初に原型が用意されており、ユーザが計算機を利用していくにつれてそのユーザの特徴をとらえた、ユーザ特有のものとなっていく。つまりユーザモデルは継続的に更新される。

認証部はまず、ユーザインタフェースが取り込んだ入力、操作を受け取る。次にユーザモデルを参照しながら、実利用者が正当なユーザか否かを判定する。この判定は、ユーザが何らかの入力または操作を行なう度に行なわれる。またあらかじめ読み込まれた個人設定も利用される。正当なユーザであると認証された場合、ユーザモデルの更新を行なうとともにコマンドや操作の実行を許可する。また不正なユーザであると認証された場合、実行禁止と適切なメッセージの表示命令を出す。

本稿で提案するシステムは、今後の実装、実験を通して改良していく予定である。つまり現時点での提案システムは、今後の改良のためのプロトタイプである。

3　システム構成

3.1　ユーザインタフェース

提案システムのユーザインタフェースは、既存の高機能シェル tcsh を変更したものである。そして、入力・

---

*Continual Authentication System by Using Usermodel

†Hideki TAKAI, Kiwamu SATO, Masatoshi MIYAZAKI

‡Graduate School of Information Sciences, Tohoku University

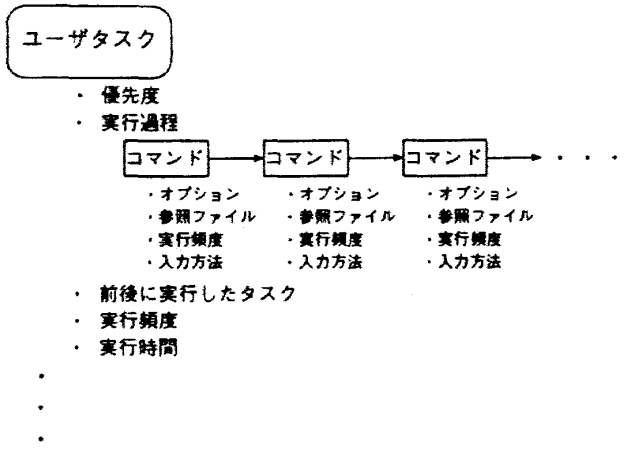

図 2: ユーザモデルの構造

操作の取り込み、構文解析、意味解析、ジョブ制御、メッセージの表示等を行なう。

3.2 ユーザモデル

本研究におけるユーザモデルは、次の要件を満足する必要がある。1. ユーザの特徴、癖を正確に、詳しく定義できること 2. ユーザの「成長」に対応できること。ここで「成長」とは、ユーザが計算機を使用していくにつれて、計算機使用時における特徴や癖が変化することを意味する。

計算機使用時におけるユーザの特徴・癖とは、タスクの実行に際して観測されるその実行過程や実行時の状況と言える。よってユーザモデルには、ユーザが過去に実行したタスクおよびそのタスクの実行過程、実行時の状況を記録する必要がある。本提案システムにおけるユーザモデルの構造を、図2に示した。ここでユーザタスクやコマンドは、認証部によってクラスター分析されている。また本研究におけるユーザタスクとは、いくつかのコマンドおよびその入力方法や実行時刻、実行頻度等の組み合わせからなり、計算機使用時における特定ユーザのタスクを反映したものである。例えばプログラムの開発というユーザタスクは、ディレクトリの移動コマンド、ソースファイルの編集コマンド、コンパイルコマンド、デバッグコマンド、実行コマンドおよびそれぞれの入力方法、実行時刻そして実行頻度等の情報からなる。またユーザタスクは、ユーザの特徴や癖の変化に対応するために、1日または1週間のサイクルにおけるユーザタスクの実行時刻、ユーザタスク間の組合せ、優先度等の情報に基づき認証部によって動的に作成、変更される。

3.3 設定ファイル

一般的にセキュリティの強化と使いやすさとの間にはトレードオフが存在する。本システムにおける設定ファイルは、そのトレードオフの関係をカスタマイズするためのものである。つまり指定対象の単位、判定基準、指定内容それぞれについて次のような設定が可能である。

1. 指定対象の単位
   入力コマンド単位、またはユーザタスク単位で対象を指定することができる。
2. 判定基準
   判定基準として、頻度、実行の過程または実行時間のデータを指定することができる。
3. 指定内容
   不正なユーザと判定された場合の対応について、実行禁止または強制ログアウトを選択することができる。

3.4 認証部

提案システムにおける認証部はまずユーザの入力・操作の系列をユーザインタフェースから受けとる。次にそれをクラスタリング解析し、ユーザタスクを生成する。次にそれをユーザモデルに渡し、対応する既存のユーザタスクに関する情報を受けとる。そしてこの情報およびあらかじめ読み込まれた個人設定をもとに、実利用者の認証を行なう。最後に実行要求およびユーザモデルの更新、または禁止、メッセージの表示命令を出す。

4 まとめ

以上第2章から第3章まで、我々が提案する認証システムについて述べた。今後実装および実験を行ない、この提案システムのプロトタイプを改良していく予定である。また、ユーザの過去の入力パターンと関係のない入力・操作（初めて実行するコマンドや気まぐれに行なう入力）への対応も、今後の課題として考えている。

参考文献

[1] 大槻 説平, 山本 米雄, 保原 信, 山村 陽一 ：小特集：知的ＣＡＩ最近の動向, 情報処理 VOL.29, NO.11, 1988年.