3次元形状モデルを用いた認証システムの試作*

5W−7

村田　篤則　　新藤　義昭　　松田　郁夫
日本工業大学

1・はじめに

インターネット、パソコン通信等の計算機ネットワークの普及に伴い、近年では認証システムが重要視されてきている。そこで、パスワードとして暗証文字列や暗証番号を用いる従来の認証システムの問題点を検討し、3次元形状モデルを利用した認証方法の試作開発を行った。

2・認証システムの問題点

現在の認証システムは、パスワードとして暗証文字列や暗証番号を用いている。しかし、計算機の非専門家が、パスワードを用いる認証システムを使用した場合、次のような問題点が挙げられる。

(1) 複雑なパスワードを設定すると自分が忘れてしまうため、記憶しやすい単語が使われる。
(2) 簡単なパスワードを設定すると他人に解除されやすい。
(3) 暗証文字列は、記憶しやすい単語である事が多いため、口伝いに漏洩しやすい。

計算機の非専門家は、パスワード漏洩の結果引き起こされる惨事の大きさについて認識があまいようである。最も効果的なパスワードは、乱数的で人間にとって意味不明な長い文字列である。しかし、このようなパスワードは、設定者が記憶するのが困難である。

これらの問題を解決するパスワードの設定及び認証の方法として、3次元仮想空間内に配置された3次元形状モデルと対話することによって認証を行うシステムを提案する。本論文では、この認証システムをVisual Software Agent Security check Interface（以後VSASIと記す）と名付けた。また、VSASIの評価ソフトウェアを開発した。

3・VSASIの操作パラダイム

本論文で提案するVSASIの操作パラダイムを次に述べる。

(1) ＶＲ技術を用いて構築した3次元仮想空間に生物型エージェントを配置する。
(2) ユーザは、マウス等のデバイスを用いて、このエージェントに、**立ち居振舞いを振り付ける**。この振り付け結果が、**認証文字列に変換**される。
(3) (2)で生成される文字列は、人間にとっては無意味で乱数的な長い文字列である。
(4) パスワードの認証は、再度エージェントに立ち居振舞いを振り付けることで行う。
(5) この際、振り付け精度を制御することによって、認証レベルを変化させることができる。

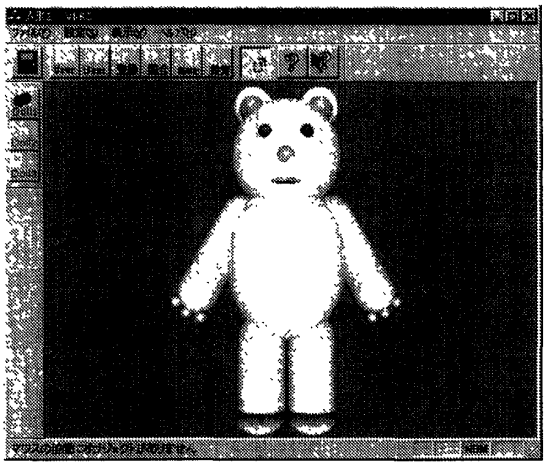

図 1 VSASIの画面例

VSASIの画面例を図1に示す。この例では、**熊型**エージェントの 顔、肩（左右）、腕（左右）、手（左右）、胴体、足（左右）、足先（左右）、尻尾、目、鼻、口などのホットスポットをマウスなどのポインティングデバイスでダブルクリックすることにより、予めホットス

---

* A Security Check Interface Using 3D-Model
Atsunori MURATA, Yoshiaki SHINDO, Ikuo MATSUDA
Nippon Institute of Technology
4-1 Gakuendai, Miyashiro, Minamisaitama, Saitama, 345, Japan

ポットに定義されている動作を行う。それにより、立ち居振舞いを振り付けることができる。
認証文字列の生成は、ホットスポットに文字コードを乱数的に割り当てることにより行う。

図 2 エージェントの様子

振り付けによって形状の変化したエージェントの様子を図２に示す。この結果生成される文字列を人間が記憶するのは困難であるが、エージェントの立ち居振舞いは視覚的であり記憶可能である。

4・パスワードの設定

文字入力によるパスワード設定では、画面への文字表示を隠蔽して近傍にいる他人に盗み見されないような配慮をしている。VSASI では、同様な隠蔽機能として振り付け時に次のような情報も取得している。

(1) **マウスボタン**（プライマリとセカンダリ）
(2) **キイボード**

これらの情報と画面の振り付けを同時に盗み見することは困難であると考えられる。

5・VSASI の特徴

この VSASI の特徴は次の通りである。

(1) 認証データ（パスワード）を視覚的に記憶することができる。
(2) 認証情報である立ち居振舞いは、言葉で表現し難いので、口伝いの漏洩の可能性が低い。

また、不正アクセス防止策として、度重なる認証行為の再試行を検出した際、次のような防衛行動をとる。

・認証行為の繰り返しに対する防衛行動

(1) エージェントの形状そのものを徐々に変化させる。
(2) エージェントとの距離が離れていくことにより、ホットスポットを探索し難くしていく。

・不正な認証行為の検出に対する防衛行動

(1) エージェントが周囲に援助を求める。
（VSA の援助要請行動）
(2) 認証行為そのものを不能にする。

不正な認証行為の判定は、

(1) 一定以上の認証行為の繰り返しを検出した場合
(2) 立ち居振舞いが明らかにかけ離れている場合

を不正な認証行為とする。
「VSA の援助要請行動」は、音声、画像等を最大限駆使して、周囲の人間（計算機の近傍にいる操作者以外の人）に「不正アクセス」が行われようとしている緊急事態を通報する新しい試みである。これは、オフィスや学校などでの効果が期待できる。

6・おわりに

本論文では、３次元形状モデルを用いた認証システム、「VSASI」を提案した。
今後は、さらにシミュレーション実験により、操作方法の改善等を行う予定である。