



目, 20 日目の計 4 回認証作業を行った。実験は, 工学部の学生 5 名を対象にして行った。実験結果を表 1 にまとめる。表は実験期間中の認証作業における各認証方法の認証結果を示している。

表 1: 評価実験結果

認証方式	5 日目	10 日目	20 日目
画像認証 (エピソード記憶)		*1	*2
画像認証 (人工画像)		×*3	*3
暗証番号 (ランダムな数字)		×*4	*4
暗証番号 (ユーザ任意の設定)			

: 認証成功 / × : 認証失敗 / : 除外

\*1: 5~8 日目に認証時に表示する画像を変更。

\*2: 11~14 日目に登録キー画像を変更。

\*3: 5~9 日目でパスワードを忘却し, 再交付。その後, 手帳にパスワードを記入し保存。

\*4: 5~10 日目でパスワードを忘却し, 再交付。その後, 手帳にパスワードを記録し保存。

この実験結果から暗証番号や人工画像を利用した画像認証では, 実験開始後数日間で暗証番号や, 画像を忘れてしまい, 一度忘れた暗証番号や画像は手帳などに記録しておき, 持ち歩いている。特にこの実験のように数日間隔で認証作業を行う場合は顕著である。一方, ユーザが任意で暗証番号を決定した場合は実験最終日まで正常に認証が行えた。しかし, 実験後の調査で, この時テストユーザは自分の誕生日や所有する車のナンバー, 携帯電話番号の一部などを暗証番号として設定していたことがわかった。提案システムにおいて, ユーザ自身が所持する画像を登録し, 登録キー画像もユーザ自身が設定した場合, 実験最終日まで正常に認証作業が行えた。以上より, 人間にとってもっとも記憶しやすく, 忘れにくいエピソード記憶を利用することで, 暗証番号におけるパスワードの憶えにくさや忘れやすさを解決できたと考えられる。

## 5. 考察

提案システムでは人間の記憶負荷に着目し, 既存の認証システムに記憶負荷の軽減と利便性の要素を付加することで, 安全性と利便性の両立を実現した。パスワード認証のような既存の記憶による認証方法では, 一般に安全性と利便性は両立できないと考えられてきた。この両立できない背景として, ユーザの記憶による問題があったといえる。具体的には, 安全性を高めるためにパスワードの文字数を増やすと, ユーザが記憶しづらく, また忘れやすい。逆に, 利便性 (憶えやすさ・忘れにくさ) を追求すると, パスワードの文字数を減らす, あるいは名前の一部や誕生日など個人情報に登録してしまう。結果として攻撃の標的になりやすくなり安全性は低下する。提案システムでは, ユーザの体験による写真を用いることにより, 安全性と利便性が共に向上している。

認証システムの確率的な安全性を考える。提案システ

ムの場合, 初期設定時, 18 枚の画像の中から, 6 枚の画像を登録順に選択する。この確率を暗証番号方式のように, 数字の組み合わせに換算すると, 7 桁の以上の確率となり, 既存の数字 4 桁の暗証番号に比べて安全性が高いといえる。また, 提案システムは表示される画像枚数及び登録キー画像を増やすことが可能であり, 確率的な安全性を更に高めることができる。また, Observation 攻撃や Educated Guess 攻撃, Intersection 攻撃などさまざまな攻撃への対策も取り入れている。

画像を利用した認証システムも多く開発されている。Deja Vu[3] もその 1 つであるが, Deja Vu はコンピュータが生成した人工的な画像を用いて認証を行うものである。人工的に作られた画像の記憶はエピソード記憶の利用ではなく, 提案システムのようにエピソード記憶を利用するというコンセプトとは異なる。他にも画像認証システムは存在するが, エピソード記憶の利用を最大限に考慮した認証システムになっていない。

## 6. まとめ

ユーザの利便性と認証システムの安全性の向上を目的としてエピソード記憶を用いる認証方法を提案した。更に, 携帯電話での実装を行い, 評価実験を行った。その結果, 既存の暗証番号方式に比べ提案システムの利便性と安全性が共に向上していることがわかった。

現在, 提案システムは, NTT DoCoMo i-mode 端末での利用を前提に, ia ppli Development kit を用いて構築した ia ppli 上で動作するシステムとなっている。今後, 携帯電話のセキュリティ機能として搭載する方法としては以下の 2 点を考えている。1 つ目は現在の Java アプリケーションをベースとして, 携帯電話本体のセキュリティ機能と連携される方法である。2 つ目は, 携帯電話のオペレーティングシステム上に実装する方法である。実際に提案システムが携帯電話で動作するようになれば, 現在, 標準的に利用されている 4 桁の数字の組み合わせである暗証番号による認証システムの代替となると考えられる。暗証番号方式に比べ, 提案システムの確率的な安全性は格段に高い。それに加え, 携帯電話に搭載されているデジタルカメラの画像をそのまま認証に利用でき, エピソード記憶の利点を最大限に生かすことができる。コンピュータに対する知識がなく, 操作に不安がある初心者や記憶の保持期間が比較的に短い子供や高齢者に対しては効果が大きいと思われる。

## 参考文献

- [1] NTT DoCoMo 公式ウェブサイト DoCoMo Net, 株式会社エヌ・ティ・ティ・ドコモ (2003).  
<http://www.nttdocomo.co.jp/>
- [2] 松村健児, 白井治彦, 高橋勇, 黒岩丈介, 小高知宏, 小倉久和: イメージを利用したユーザ認証手法の検討 - エピソード記憶に基づく認証 -, 平成 15 年度電気関係学会北陸支部連合大会講演論文集, pp.392 (2003).
- [3] Dhamija, R. and Perrig, A: Deja Vu: A User Study Using Images for Authentication, 9th Usenix Security Symposium, pp.45-58 (Aug.2000).