6X-03

パスワード認証とパターン認証の安全性に関する比較評価

君塚　悠†　岡本　剛†
神奈川工科大学†

1. はじめに

パスワード認証には，ユーザが単純なパスワードを登録したことが原因で，辞書攻撃により不正にログインされたり，パスワードを複数のサービスで使い回すことが原因で，リスト型アカウントハッキングにより不正ログインされたりする危険性がある．

一方，パターン認証は，パスワード認証に代わる，または併用される認証方式である．これは，予め登録したパターンにより本人であることを確認する認証方式であるが，パスワードと同様，人の記憶に基づくため，パスワード認証と同様の脆弱性があると考えられる．そこで，本研究では，パスワード認証とパターン認証の安全性の比較を行った．

2. パターン認証

パターンは，パターン認証において，ユーザ自身が考え，記憶する必要がある．特徴として，以下のものが挙げられる．

- パスワードとは違い，文字や数字の列ではなく，パターンを記憶する必要がある
- パターンに割り当てられた英数字や文字をワンタイムパスワードとして利用する

例えば，最上層，中間層，最下層に分かれた乱数表から，ユーザが設定したパターンのセルに割り当てられた数字を抜き出し，それをパスワードとするパターン認証がある．その認証画面の例を図1に示す．

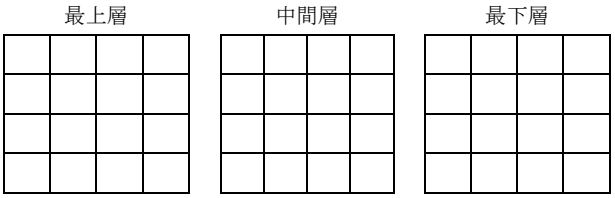

図1　パターン認証画面の例

パターン認証では，各セルに疑似乱数が割り当てられており，事前に登録したパターンのセルに割り当てられた文字を抜き出し，ワンタイムパスワードとする．このことから，従来のパスワード認証よりも，盗み見や盗聴に対する安全性は高い．しかし，パターン認証は，パスワードと同様に，推測しやすい単純なパターンを設定する傾向があることが予想されるが，パスワードのように安全でないパターンはまだ明らかでない．また，パターンはパスワードよりも記憶しやすい [1]とあるが複雑なパターンでも記憶しやすいかどうかは明らかでない．

3. パスワードとパターンの収集

パスワードとパターンの安全性を比較するため，18 歳から21 歳の学生から，パスワードとパターンを収集した．パスワードは，4 文字以上 8 文字以下とし，大文字と小文字のアルファベットと，数字，記号から選べることとした．パターンは，図 1 に示したセルから 4 個以上 8 個以下のセルを選べることとした．

パスワードとパターンを収集する前に，パスワードの安全性の問題点を解説した上で，その時点で，使用していない新しいパスワードとパターンを設定させた．その結果，229 名から収集し，有効数は 186 個であった．

4. 安全性の比較評価

4.1. 辞書攻撃に対する安全性評価

収集したパスワードのうち，単純なパスワードの割合を調査するため，辞書攻撃に使用される辞書と照合し，一致するパスワードの割合を調査した．使用した辞書は，John The Ripper の提供サイトで公開されているデータ [2]であり，データの総数は3,917,116 個である．この辞書には，英単語以外に，世界各国でよく使用される氏名や，ユーザがよく設定する文字列などが含まれる．この辞書データと収集したパスワードを照合した結果，収集したパスワードの 4.2%が合致した．

パスワードの辞書攻撃と同様にパターン認証で安全性を評価するために，辞書データとして，図 2 に示す規則性のある単純なパターンのすべての組み合わせを使うことにした．なお，セルを共有する 2 つの規則的なパターンの組み合わせは除外した．その結果，組み合わせ総数は，2,844 通りとなる．

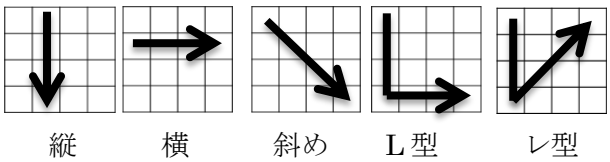

図2　規則的なパターン

これらの規則的なパターンと収集したパターンを照合した結果，収集したパターンの約 63%が合致した．この結果から，1 人のユーザに対し，2844 通りのパターンを試した場合に，約 63%の確率で認証に成功することになる．この成功率はパスワード

Comparative evaluation of security for password-based and pattern-based authentication
†Yu Kimizuka, Takeshi Okamoto,
Kanagawa Institute of Technology

の成功率と比べて、極めて高い成功率である.

4.2. パターンの複雑さの評価

収集したパターンの複雑さを定義し，パターンの複雑さを明らかにする. パターンの複雑さは, 収集したパターンを調査する中で, 使用される傾向にあるパターンの形や座標を考慮して, 次のように定義した. この定義で，図 3 のパターンの複雑さを計算すると 8 となる.

- パターンの形は, セル間の最短距離を移動させることで構成する
- セルと層は周期的境界条件を満たす
- セル間の移動を加点する（セルを縦，横，斜めに 1 つ移動する度に， 1 点の加点とする）
- 層間の移動は， 1 度につき 1 点の加点とする
- セルは周期的境界条件を満たすが, 端から端へ移動するパターンの場合，斜めに移動することはできない. ただし, 角から角へは移動できる
- 同じ箇所を使用する場合，2 回の使用は 2 点の加点，3 回の使用は加点なし，4 回目以降は，使用する度に 2 点の減点とする. 4 回ならば 2 点の減点，8 回ならば 8 点の減点とする

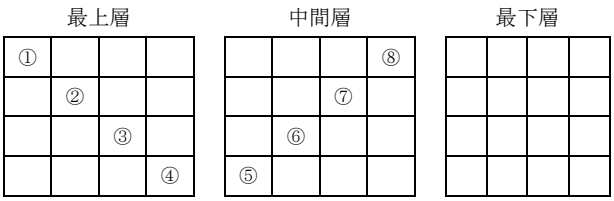

図 3　パターンの例

複雑さを計算した結果，18 歳代の複雑さの平均値は 7.188 であり，19 歳代は 8.259 であり，20 歳代は 7.256 であった. また, 4 章で作成した規則的なパターンと一致したパターンの複雑さは，平均で 7.064 であり，規則的なパターンと一致しなかったパターンの複雑さは 8.243 であった. これらの結果から，19 歳代は，複雑なパターンが多く含まれていることがわかる.

4.3. エントロピーの比較

収集したパスワードの各文字とパターンの各セルの使用割合からエントロピーを計算した. パスワードのエントロピーは, 5.457 であり，パターンは 5.392 であった. つまり，パターンよりパスワードの方が複雑であることがエントロピーからも確認できる.

5. パスワードとパターンの特徴分析

パスワードやパターンは，使用する文字やセルに偏りがある場合, 推測しやすくなる. ユーザがパスワードやパターンを設定するときに, 使用されない傾向にある文字種, セルの層を分析した. パスワードの文字の使用割合を図 4 に，パターンに利用される各層の使用割合を図 5 に示す. これらの結果から，使用されていない傾向のあるアルファベットの大文字や記号，最下層を使用することにより，パスワードやパターンの安全性が改善されると考えられる.

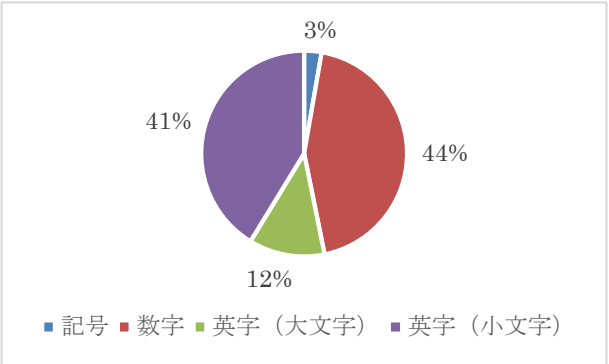

図 4　パスワードの文字種毎の使用割合

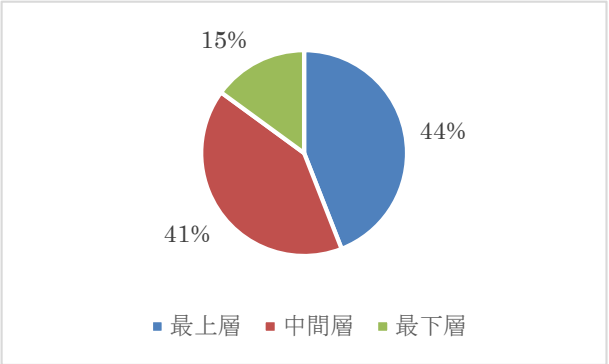

図 5　パターンの層毎の使用割合

6. おわりに

本研究では，パスワードとパターンの安全性の比較評価を行った. パターンでは、ユーザの約 63%が規則的なパターンと一致した. また, 収集したパスワードとパターンでは, パスワードの複雑さがわずかに勝っていた. したがって, 人間が設定するパターン認証はパスワード認証よりも安全性が低い.

パターン認証の安全性を改善するために，規則的なパターンの使用を禁止させ，使用するセルの偏りが少なくなるようにさせる工夫が求められる.

参考文献

1) 株式会社シーエスイー：マトリクス認証のしくみ, https://www.cseltd.co.jp/products/smx/

2) John The Ripper password cracker: Openwall wordlists, http://mirrors.kernel.org/openwall/wordlists/all.gz