SCIS 2013 The 30th Symposium on Cryptography and Information Security
Kyoto, Japan, Jan. 22- 25, 2013
The Institute of Electronics, Information and Communication Engineers

ユーザ認証においてユーザが覚えるべき秘密情報のエントロピに関する一考察
A Study of Entropy of Authentication Information that the Users Should Remember

兼子 拓弥* 本部 栄成† 西垣 正勝††
Takuya Kaneko* Eisei Honbu† Masakatsu Nishigaki††

あらまし 計算機の能力は日々向上する．総当たり攻撃に耐性を持たせるためには，秘密情報のエントロピを計算機の進歩に伴って増加させる必要がある．すなわち，計算量的安全性に依拠するセキュリティシステムにおいては，秘密情報のエントロピの確保が必須となる．しかし，ユーザ認証においては，現在の暗号化鍵に比べて，人間が覚えることができる秘密情報（パスワード等）のエントロピが格段に小さい．このため，ユーザ認証の秘密情報のエントロピに関しては，秘密情報そのもののエントロピを十分に大きく確保するというコンセプトではなく，秘密情報のエントロピの分だけ総当たり攻撃にかかる手間を増加させるというコンセプトで，安全性設計をすることが肝要である．すなわち，秘密情報を知っている正規ユーザは総当たり試行が十分短い時間で終了するようにし，不正者は秘密情報のエントロピの分だけ正規ユーザより総当たり試行に要する時間が大きくなるように設定する．これにより，いかに計算機の能力が向上したとしても，なお，総当たり攻撃に対する耐性を持たせることが可能となる．

キーワード ユーザ認証，エントロピ強化，総当たり攻撃，記憶負荷

1 はじめに

情報システムにおけるセキュリティ技術の多くは計算量的安全性に依拠する．このようなセキュリティシステムにおいては，攻撃者の計算量が多項式時間内に収まらないようにするために，秘密情報のエントロピの確保が必須となる．例えば暗号通信などにおいては現在，共通鍵暗号の秘密情報（暗号化鍵）は 256 ビット（最近は 512 ビット），公開鍵暗号は 1024 ビット（最近は 2048 ビット）が推奨されている．

これに対し，ユーザ認証においては，what-you-know タイプの認証では人間の記憶負荷や利便性などの理由で，who-you-are タイプの認証では認証精度などの理由で，秘密情報（パスワードや生体情報）のエントロピが（暗号化鍵と比べて）格段に小さい．

ユーザ認証の総当たり攻撃に対する耐性を保つためには，秘密情報のエントロピが攻撃者の持つ計算機能力よりも大きくなるように，秘密情報を設定するべきである．しかし，計算機の能力は日々向上する．これに対し，人間が記憶可能なパスワード長や人体固有の生体情報は，一朝一夕で増えるものではなく，基本的には常に一定であると考えられる．したがって，ユーザ認証の秘密情報に関しては，秘密情報そのもののエントロピを十分に大きく確保するというコンセプトでは，総当たり攻撃に耐性を持つユーザ認証を実現することは不可能である．

そのため，我々は，秘密情報のエントロピの分だけ総当たり攻撃にかかる手間を増加させるというコンセプトで，安全性設計をすることが肝要であると考える．すなわち，正規ユーザであっても認証の際に（攻撃者と同様に）計算機を利用し，計算機の能力とユーザ自身が所有する秘密情報を併用してユーザ認証を行うという形態に移行させる．これにより，「人間は，エントロピの小さい秘密情報しか認証に利用できない」のではなく，「人間は，計算機の能力の上に，更に秘密情報の分のアドバンテージを加えた情報を認証に利用できる」ようになる．

具体的には，認証情報（サーバに登録される情報）を秘密情報（ユーザが入力する情報）と計算機能力を利用して総当たり試行によって求める補助情報によって構成

* 静岡大学情報学部 〒432-8011 静岡県浜松市中区城北 3-5-1. Faculty of Informatics, Shizuoka University, 3-5-1, Johoku, Naka Ward, Hamamatsu 432-8011, Japan.
† 静岡大学大学院情報学研究科〒432-8011 静岡県浜松市中区城北 3-5-1. Faculty of Informatics, Shizuoka University, 3-5-1, Johoku, Naka Ward, Hamamatsu 432-8011, Japan.
†† 静岡大学創造科学技術大学院〒432-8011 静岡県浜松市中区城北 3-5-1. Faculty of Informatics, Shizuoka University, 3-5-1, Johoku, Naka Ward, Hamamatsu 432-8011, Japan.

する．秘密情報を知っている正規ユーザは，補助情報の分の総当たり試行だけで認証情報の同定が可能であるので，十分短い時間でユーザ認証が終了する．不正者は，秘密情報の分だけ正規ユーザよりも総当たり試行に要する時間が大きくなるため，なりすましが困難となる．

2　ユーザ認証におけるエントロピの問題

2.1　パスワード認証

現在最も多く使われているユーザ認証方式は，パスワード認証方式である．パスワード認証では，個人を特定するための ID とユーザがあらかじめ設定したパスワードの入力をユーザに要求し, ID に対するパスワードが正しければ正規ユーザであると認める．

パスワード認証に対する典型的な攻撃手法に，総当たり攻撃と辞書攻撃が存在する．これらの攻撃に対して十分な安全性を確保するためには，パスワードは長く，かつランダムな文字列とすることが望ましい．しかし，長くランダムな文字列を記憶することはユーザにとって大きな負担となる．そのため，多くのユーザは短いパスワードや記憶しやすいパスワードを使用してしまい，結果としてユーザ認証としての十分な安全性を確保することができていないのが現状である[1].

2.2　画像認証

人間の画像認識能力の高さを利用し，パス「ワード」の代わりにパス「画像」を秘密情報として用いることによってユーザの記憶負荷を軽減させる画像認証方式が提案されている．画像認証には，複数の囮画像の中に紛れたパス画像を選択する Cognometric 方式[2, 3]と, 1 枚の画像の中の特定箇所（パスポイント）を選択する Locimetric 方式[4, 5]に大別される．

しかし，例えば，Cognometric 方式では，1 画面に表示できる画像数には限度があるため，総当たり数を確保が困難となっている．仮に多数の小さなアイコンを無理矢理一画面に敷き詰めることができたとしても，大量の囮画像の中に紛れるパス画像を発見することは，ユーザにとって容易ではない．また，Locimetric 方式では，例えば，1,000×800 画素の画像に対して正解領域（パスポイント）が 10×10 画素であった場合には，8,000 通りの総当たり数しか確保できないという計算になる. また，人間は画像中の特徴的な点（ホットスポット）をパスポイントとして選択する傾向があることが知られており，パスポイントの実際のエントロピは更に小さくなると推測されている[6].

以上のように，秘密情報の記憶に対するユーザの負荷を軽減するために導入された「画像の利用」が，皮肉にも，秘密情報のエントロピを低減させる結果を引き起こしてしまっている．

2.3　CAPTCHA

現在最も広く使用されている文字判読型 CAPTCHA においては，文字種別と文字数を適切に増やすことによって，総当り攻撃に対して実用的な強度を有するエントロピを確保することは可能である．ただし，解答すべき文字種別や文字数が増えるにつれて，正規ユーザにとって利便性は低下する．

また，最近の光学文字認識（OCR）技術の性能向上により，マルウェアも文字判読型 CAPTCHA の判読が可能になってきている[7]．この問題に対処するため，人間の「より高度な認知処理」に基づく CAPTCHA が種々提案されている[8, 9]が，それらの多くは人間の画像認識能力の高さを利用するものであり，2.2 節で説明した画像認証の場合と同じ理由で，総当り攻撃に対抗するに足るエントロピの確保に対する課題を残している．

2.4　生体認証

一般的に，生体情報は同一人物であっても入力の度に誤差が含まれるため，本人拒否率を抑えようとする，ある程度の他人受入れを許容する必要がある．生体情報のエントロピについては，これを正確に評価する方法は現在のところ知られていないが，実用的には「他人受入れ率の逆数」が生体情報のエントロピ（正確には，当該生体認証装置に対する生体情報のエントロピ）と考えられる[10]．仮に生体認証システムが 99.9999%の精度（他人受入れ率 0.0001%）を有していたとしても，生体情報のエントロピはたかだか 100 万通りである．したがって，生体認証においても，総当たり攻撃に対する脆弱性は大きなリスクである．

3　総当り攻撃に対する既存研究

総当たり攻撃に対してユーザ認証の耐性を保つためには，秘密情報のエントロピが攻撃者の持つ計算機能力よりも大きくなるように，秘密情報を設定する必要がある．この実現のためには，秘密情報のエントロピを増大させるアプローチと攻撃者の攻撃効率を低下させるアプローチが存在する．この実現のためには，秘密情報のエントロピを増大させるアプローチと，攻撃者の攻撃効率を低下させるアプローチが存在する．ここでは，これらに関する既存手法を幾つか紹介する．

3.1　秘密情報のエントロピを増大させるアプローチ

3.1.1.　語呂合わせ

パスワードは，十分なエントロピを持ち，かつランダムな文字列であることが望ましい．しかしながら，ランダムな文字列をユーザが記憶することは大きな負担とな

る．そこで，一見ランダムに見えるパスワードに対して語呂合わせなどによって意味づけを行い，長いパスワードを比較的小さな記憶負荷によって覚えるという方法がある[11].

3.1.2. パスワード管理ツール

ユーザのパスワード管理を支援する方式として，パスワード管理ツール[12]が挙げられる．パスワード管理ツールは，ユーザの代わりに複数の（ID と）パスワードをユーザ PC 内で管理する．これによって，ユーザはそれらの認証情報を記憶することなくパスワード認証を行うことができる．認証情報の記憶が不要となるため，ユーザは，十分に長いランダムなパスワードをサービスごとに個別に設定することが可能となる．

パスワード管理ツールに登録されている認証情報は暗号化によって安全にユーザ PC 内に保管される．ユーザがパスワード管理ツール自体にログインすることで，ツールに登録されているすべての認証情報の使用が許可される．すなわち，ユーザはパスワード管理ツールにログインするための ID とパスワードを 1 組覚えるだけで，サービスごとに異なる認証情報を利用することが可能となる．

この方式では，パスワード管理ツール自体へのログインは，通常のパスワード認証を用いることとなる．すなわち，ツールに対するログイン情報に対してはエントロピの課題は解決されず，この部分が脆弱ポイントとして残る．ツールにログインするためのパスワードが漏洩してしまうと，ツールに登録されているすべての認証情報が不正者に手に渡るため，被害が深刻となる．

3.1.3. 認証を繰り返し行う方法

1 度の認証では十分なエントロピを確保できない場合に，複数回認証を行うことでエントロピの確保を達成することが可能である．例えば，画像認証においてパス画像を選択するという行為を複数回行う方法や，指紋認証において 2 本以上の指紋を提示する方法がこれに当たる．当然ながら，繰り返しの回数が増すごとに，ユーザの利便性が損なわれることになる．

3.1.4. what-you-have タイプの認証

what-you-have タイプの認証であれば，ユーザが所持する IC カードなどのトークンの中に，十分長く，ランダムな認証情報を記録することが可能である．ただし，トークン自体の盗難や紛失に対するリスクがあるため，ユーザにトークンの管理徹底が求められる．

3.2 攻撃者の攻撃効率を低下させるアプローチ

3.2.1. タールピット

タールピットとは，認証に失敗した場合，一定時間が経過しないとリトライできない仕組み[a]のことである[13]．総当たり攻撃は，正しい秘密情報を発見するまで認証を繰り返すことによって行われるため，タールピットを仕掛けて一定時間のリトライを禁止することによって，総当たり攻撃に要する時間を膨大にすることができる．また，規定回数以上の認証失敗の場合には，アカウントを無効化（アカウントロックアウト）するという方法[13]も採れる．

ただし，タールピット（やアカウントロックアウト）が有効に機能するのは，オンラインで実行される総当たり攻撃に対してのみとなる．

3.2.2. bcrypt

Provos らは，ハッシュ値を求めるための計算量を意図的に多くすることで，ユーザ認証の総当たり攻撃に対する耐性を向上させる方法を提案した[14]．bcrypt と名付けられたこの手法は，Blowsifh[15]型のブロック暗号における部分鍵生成演算の繰り返し回数を可変とすることで，ハッシュ計算に要する時間をコントロールできるように設計されている．

ハッシュ計算に時間を要するようになれば，認証試行 1 回（認証時に入力された情報のハッシュ値が登録されているハッシュ値と一致するか否かの検査）当たりの所要時間が増加し，その分，不正者が単位時間当たりに実行可能な認証試行回数が減少する．すなわち bcrypt は，認証アルゴリズムそのものにタールピットを仕掛け，不正者の総当たり攻撃能力を減衰させる方式であるといえる．

しかし，bcrypt のように暗号関数そのものに手を加える方法においては，安全性の証明までを考えると，その設計負荷は比較的高いものとなる．また，使用するハッシュ関数が固定されてしまうことは，認証アルゴリズムのバラエティが限定されるという弊害につながるだけでなく，万一このハッシュ関数がブレイクされてしまった場合には代替が効かないという問題をはらむ．

3.2.3. ソルト

通常，パスワード認証システムにおいては，パスワードはハッシュ化された状態で保管されており，認証時に入力されたパスワードのハッシュ値が登録されているハッシュ値と一致するか否かによって認証の可否が判定される．ハッシュ関数の一方向性によって，パスワードのハッシュ値が万一漏洩したとしても，ハッシュ値からパスワードを逆算することは難しい．

しかし，レインボーテーブル（平文のすべての組み合わせに対するハッシュ値を事前に計算して，平文とハッシュ値の対応を表にしたもの）が用意されていた場合には，不正者はテーブルルックアップによって実時間内にハッシュ値からパスワードを知ることができる[16]．現在，70～80 ビット程度以上のパスワードでなければ，レ

[a] 一般的にはアカウントのロックアウトの一種として知られている．本稿では特にアカウントの無効化との区別を行うために，「タールピット」という言葉で呼称する．

インボー攻撃に脆弱であるといわれている[17]．しかし，レインボーテーブルの作成は不正者によってアンダーグラウンドで常に行われており，レインボー攻撃に耐性を持たせるために必要となるパスワードのエントロピは絶えず増加していく．

レインボー攻撃に対する対策としてソルトが知られている[18]．ソルトとは，パスワードのエントロピを増加させるためにパスワードに付加する乱数のことである．ソルトの付加によってパスワードのエントロピが増加し，レインボーテーブルの作成に天文学的な時間を要するようになる．

なお，ソルトの値そのものは，パスワードのハッシュ値とともに平文で保管されることになる．このため，正規ユーザの記憶負荷は増加しない．すなわちソルトは，パスワードのハッシュ値の逆計算に対するエントロピを増加させているだけであり，パスワードの総当り攻撃に対するエントロピを増加させているわけではない．

4　提案方式

計算機の能力は日々向上するため，秘密情報のエントロピを増大させるアプローチには限界がある．また，攻撃者の攻撃効率を低下させるアプローチに関しては，タールピットはオフラインによる総当たり攻撃には対抗できない．bcrypt は，暗号設計の負荷の高さが課題として残る．ソルトは，パスワードの総当り数そのものを増加させるものではない．

そこで本稿では，正規ユーザであっても認証の際に（攻撃者と同様に）計算機を利用し，計算機の能力とユーザ自身が所有する秘密情報を併用して認証を行うというコンセプトに基づくユーザ認証方式を提案する．これにより，「人間は，エントロピの小さい秘密情報しか認証に利用できない」のではなく，「人間は，計算機の能力の上に，更に秘密情報の分のアドバンテージを加えた情報を認証に利用できる」ようになる．

4.1　コンセプト

総当たり試行には，全パターンを試行するために必要となる時間は認証情報のビット長に応じて指数関数的に増加するという特徴がある．そのため，あるビット長以下の認証情報に対する総当たり試行にかかる時間は短いが，それ以上のビット長の認証情報に対する試行にかかる時間は膨大となる．この特徴を用いて，ユーザに認証情報の一部のみを入力させ，残りの情報を総当たり試行によって補完することで，ユーザ認証におけるエントロピの不足を緩和するとともに，実用時間内での認証完了を達成する．以降，認証情報の内，ユーザが入力する情報を「秘密情報」，総当たり試行によって保管する情報を「補助情報」と呼ぶ．すなわち認証情報とは，秘密情報と補助情報を連結した情報となる．

不正者が認証情報全体を総当たり攻撃するのに要する時間が 1 年（$\fallingdotseq 3 \times 10^7$秒）以上であれば安全であり，かつ，正規ユーザが認証に要する時間が 1 秒以下ならば利便性が損なわれないとする．例えば，現在の計算機が 1 秒間に10^8通りの総当たりが可能だとすると，秘密情報を知らない不正者が総当たり試行に 1 年以上を要するようにするためは，認証情報全体のエントロピとして $3 \times 10^7 \times 10^8 = 3 \times 10^{15}$通りを確保する必要がある．一方で，秘密情報を知っている正規ユーザであれば 1 秒で総当たり試行が終了するようにするためは，補助情報のエントロピを10^8通りに抑える必要がある．以上より，秘密情報のエントロピを3×10^7通り，補助情報のエントロピを10^8通りとして，認証情報全体のエントロピを 3×10^{15}通りにしてやれば，「不正者による認証情報全体の総当たり攻撃に要する時間は 1 年，かつ，正規ユーザによる認証に要する時間は 1 秒」の制約を満たすことが分かる．

ここで，提案方式においては，補助情報のエントロピを調整することによって，認証情報全体のエントロピが任意に設定できることに注意されたい．これにより，将来，計算機速度が向上し，総当たり試行に要する時間が短縮されたとしても，正規ユーザが入力する秘密情報を増やすことなく，総当たり攻撃に対する耐性を維持することができる．例えば，上記の例において計算機速度が 10 倍（1 秒間に10^9通りの総当たりが可能）になった場合には，補助情報のエントロピを 10 倍（10^9通り）にして，認証情報のエントロピを 10 倍（3×10^{16}通り）にする．（正規ユーザが入力する秘密情報のエントロピは 3×10^7通りのままである．）これにより，「不正者による認証情報全体の総当たり攻撃に要する時間は 1 年，かつ，正規ユーザによる認証に要する時間は 1 秒」の制約はそのまま維持される．

この関係を図 1 と図 2 に模式的に示した．時代とともに計算機の性能は向上し，不正者が攻撃のために割ける時間（ここでは 1 年と仮定する）の範囲内で実行可能な総当たり攻撃回数もそれに応じて増加する（図 1 の①）．すなわち，計算機の時間感覚としては，性能の向上とともに「一瞬」という時間が日を追って短くなっていく（図 2 の⑥）．これに対し，人間の時間感覚は時が移っても大きく変化することはなく，例えば「1 秒」を感じる時間の長さは，現在（図 1，図 2 の t1）も次世代（図 1，図 2 の t2）もほぼ同じ時間を保つ（図 2 の⑤）．以上より，正規ユーザが一瞬と感じる時間（ここでは 1 秒と仮定する）の範囲内で実行可能な総当たり試行回数は，計算機の性能向上と歩調を合わせて増加することが分かる．よって，「補助情報に対する 1 秒間の総当たり試行」という計算機の援用をユーザ認証に組み込むことにより，不正者の攻撃能力（図 1 の①）は 1 秒間の総当たり試行の分だけ減じられ，不正者の実効的な攻撃能力は時代によらず一定値になる（図 1 の④）．

秘密情報のエントロピがこの値（図 1 の④）を超えて

いれば，ユーザ認証の安全性が確保されることになる．人間の記憶力や生体認証装置の精度も時を越えてさほど変化することはない（図１の③）が，提案方式によって不正者の実効的な攻撃能力（図１の④）が一定となるため，常にユーザ認証の安全性を確保することが可能である．

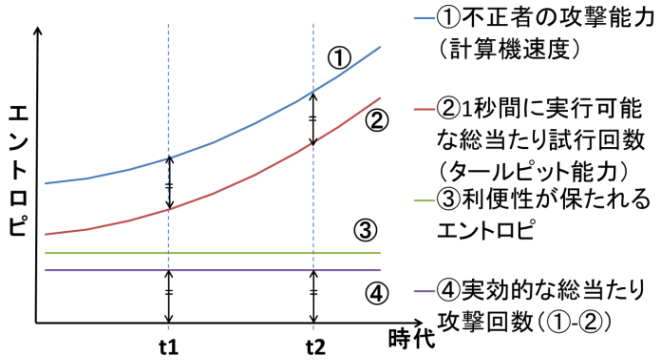

図 1　時代による処理能力（エントロピ）の推移

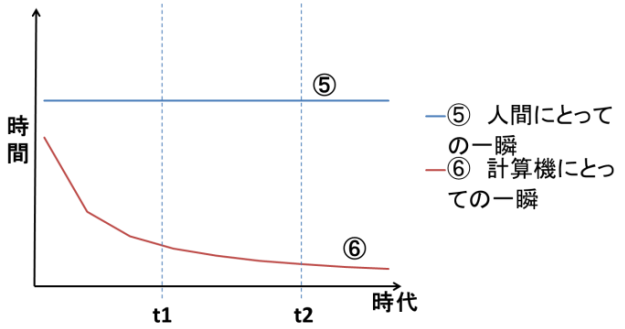

図 2　時代による処理時間の推移

4.2　基本的な認証手順

提案方式による具体的な認証の手順を以下に記す（図3）．なお，提案方式における秘密情報は，パスワード認証においてはパスワード，CAPTCHA においては提示された問題に対してユーザが入力する解答，生体認証においては生体情報である．

(0)　サーバに，認証情報P(= $P_u|P_r$)のハッシュ値H(P)が格納されている．ここで，P_uはユーザが入力する秘密情報，P_rは総当たり試行によって同定する補助情報を表す．
(1)　サーバは，H(P)をクライアントに送信する．
(2)　ユーザは，P_uをクライアント端末に入力する．
(3)　クライアント端末は，H($P_u|P_r$)がH(P)と一致するP_rを総当たり試行によって求める．
(4)　クライアント端末は，$P_u|P_r$をサーバに送信する．
(5)　サーバは，受け取った$P_u|P_r$のハッシュ値H($P_u|P_r$)とH(P)が同一であれば認証成功とし，一致しなければ認証失敗とする．

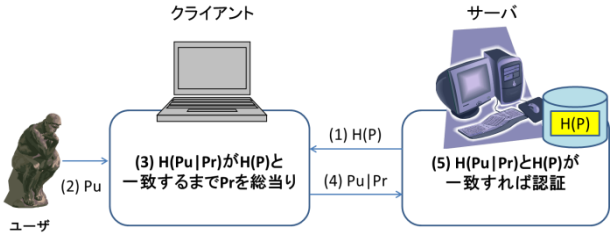

図 3　基本方式

4.3　ソルトを加えた拡張方式

レインボー攻撃[16]への攻撃耐性を考慮し，4.2 節の認証手順を，ソルトを加えた手順へと拡張する．ソルトを加えた拡張方式の認証手順を以下に記す（図 4）．

(0)　サーバに，認証情報P(= $P_u|P_r|S$)のハッシュ値H(P)およびソルトSが格納されている．ここで，P_uはユーザが入力する秘密情報，P_rは総当たり試行によって同定する補助情報を表す．
(1)　サーバは，H(P)とSをクライアントに送信する．
(2)　ユーザは，P_uをクライアント端末に入力する．
(3)　クライアント端末は，H($P_u|P_r|S$)がH(P)と一致するP_rを総当たり試行によって求める．
(4)　クライアント端末は，$P_u|P_r$をサーバに送信する．
(5)　サーバは，受け取った$P_u|P_r$にSを加えてハッシュ化した値H($P_u|P_r|S$)とH(P)が同一であれば認証成功とし，一致しなければ認証失敗とする．

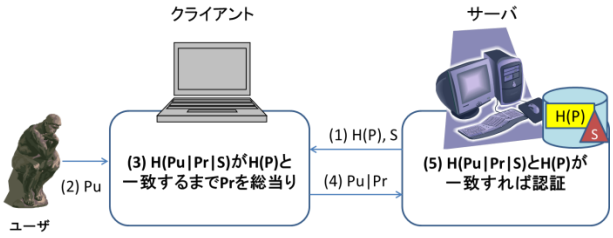

図 4　拡張方式

5　安全性の評価・考察

5.1　総当たり攻撃に対する耐性の評価

提案方式では，認証情報全体P（=$P_u|P_r$）の総当たりに対しては膨大な時間を要し，補助情報P_rのみの総当たりに対しては正規ユーザがストレスなく待てる時間内で終了するように，秘密情報P_uおよび補助情報P_rのエントロピを設定する．

4.1 節で説明したように，提案方式の総当たり攻撃に対する耐性は，将来計算機速度が向上した場合にも保た

れる．コンピュータの誕生以来，CPU 性能は飛躍的に向上しており，計算機速度は 10 年で約 9 倍になっている[19]．計算機速度が向上すると，総当たり試行に要する時間は短くなるため，その分だけ総当たり攻撃に対する攻撃耐性が低下してしまう．認証情報全体のエントロピをE，秘密情報P_uのエントロピをE_u，補助情報P_rのエントロピをE_rとし，仮に計算機速度が 2 倍になった場合を想定する．このとき，計算機速度に伴い，P_rの総当たりに要する時間は 1/2 となる．このため，P_rのビット数を増加させてE_rのエントロピを 2 倍にしても，正規ユーザが行うP_rの総当たり試行に要する時間は維持される．また，$\mathrm{E} = E_u \times E_r$なので，$E_r$を 2 倍にすることにより，Eも 2 倍となり，不正者が実行すべき認証情報$P_u|P_r$全体の総当たり試行に要する時間も維持される．

このように，秘密情報P_uを知っている正規ユーザと知らない不正者の間における認証情報Pの総当たり試行に要する時間の差は，計算機速度に関係なく，秘密情報P_uのエントロピの大きさE_uに依存するため，十分な攻撃耐性を持つ秘密情報P_uを 1 度設定すれば，その後の計算機速度の向上に左右されず，安全にユーザ認証を行うことができる．

5.2 秘密情報のエントロピの考察

4.1 節の試算によれば，提案方式における秘密情報P_uのエントロピは3×10^7通りである．本節では，各種のユーザ認証における秘密情報P_uのエントロピに対して，その妥当性を考察する．

5.2.1. パスワード認証

一般に，パスワードとして使用可能な文字 95 種から記憶情報を作成する場合，$95^3 \fallingdotseq 8.6 \times 10^5$，$95^4 \fallingdotseq 8.1 \times 10^7$より，ユーザが秘密情報$P_u$として 4 文字以上を記憶することで総当たり攻撃に対する攻撃耐性が保たれることが分かる．

5.2.2. 画像認証

例えば，Cognometric 方式において，15 枚の画像の中から 7 枚の画像を正しい順序で選択する場合，認証試行 1 回当たりのエントロピは${}_{15}\mathrm{P}_7 \fallingdotseq 3.2 \times 10^7$となる．しかし，この場合は，ユーザは秘密情報として 7 枚の画像とその順番を記憶しなければならない．画像認証において，ユーザが覚えるべき秘密情報に対して3×10^7通りのエントロピを確保するためには，何らかの工夫が必要である．

5.2.3. CAPTCHA

画像ベースの CAPTCHA においては，15 枚の画像の中から 7 枚の画像を正しい順序で選択するような問題を生成することができれば，認証試行 1 回当たりのエントロピは${}_{15}\mathrm{P}_7 \fallingdotseq 3.2 \times 10^7$となる．例えば，赤ちゃんから老人までの様々な年齢の男性 8 人と女性 7 人の顔画像を表示し，その中から「女性を若い順にクリックせよ」というような CAPTCHA 問題を構成してやれば，総当たり攻撃に対する攻撃耐性が保たれることが分かる．

5.2.4. 生体認証

例えば，指紋 1 指を用いて 99.99%の精度（他人受入れ率 0.01%）で本人認証を行うことができる指紋認証システムがあったとする．このシステムに指紋 2 指を登録し，AND 型の認証を行った場合，その他人受入れ率は1×10^{-8}となるため，1×10^8通りのエントロピを確保できることになる．したがって，提案方式であれば，生体認証においても，実用的な運用範囲（2 指の利用）内で総当たり攻撃に対する攻撃耐性が保たれると期待される．

また，現在，理論的な観点からも生体情報のエントロピの評価が進められており，例えば文献[20]では，虹彩認証においては，虹彩情報のエントロピが最低でも 100 ビット程度（$\fallingdotseq 1.2 \times 10^{30}$通り）であることが報告されている．この点からも，提案方式を利用するにあたっての要件となる3×10^7通りのエントロピの確保は可能であると考えられる．

6 まとめと今後の課題

本稿では，ユーザ認証に対する攻撃手法である総当たり攻撃を逆に利用して認証情報の一部を補完することによって安全性と利便性を両立するユーザ認証方式を提案し，ユーザ認証における秘密情報のエントロピに関して考察した．

提案方式であれば，ユーザが3×10^7通りのエントロピを持つ秘密情報を入力するだけで，総当たり攻撃に十分な耐性が確保できることを示した．ただし，例えばパスワード認証において，ユーザが秘密情報として推測しやすい文字列を設定してしまうと，辞書攻撃等による脆弱性が顕在化する．このため，提案方式においても，既存のパスワード認証と同様に，推測されにくいパスワードを設定することがユーザに求められる．

提案方式は，ユーザ PC 側で総当たり試行を行うために，サーバに大きな負荷がかからないという利点を持つ．しかし，これは同時に，認証情報全体のエントロピがユーザ PC の処理能力に依存して設定されることを意味する．そのため，処理能力の低いクライアントで認証することを前提として設定された認証情報に対して，処理能力の高いマシンを用いて総当たり攻撃を仕掛けた場合，想定された攻撃耐性を保つことができないことが考えられる．今後はクラウドコンピューティング等を用いて，ユーザ側の計算機の処理能力に依らず，提案方式の効果が発揮されるような方法を検討したい．

謝辞　本稿を執筆するにあたり，株式会社日立製作所横浜研究所高橋健太様から，有益なるご助言を頂きました．心より感謝申し上げます．

参考文献

[1] Scary Logins: Worst Passwords of 2012 – and How to Fix Them（2012 年 12 月 14 日取得）
http://splashdata.com/press/PR121023.htm

[2] Two Factor Authentication, Graphical Passwords – Passfaces（2012 年 12 月 14 日取得）
http://www.realuser.com/

[3] Tetsuji TAKADA, Takehito ONUKI and Hideki KOIKE, " Awase-E: Recognition-based Image Authentication Scheme Using Users' Personal Photographs," Innovation in Information Technology, November 2006

[4] ピクチャ パスワードでサインインする – Microsoft Windows（2012 年 12 月 14 日取得）
http://windows.microsoft.com/ja-JP/windows-8/picture-passwords#1TC=t1

[5] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy and Nasir Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system, " International Journal of Human-Computer Studies 63 (2005), pp.102-127

[6] Sonia Chiasson, Alain Forget, Robert Biddle and P.C. van Oorschot, "User interface design affects security: Patterns in click-based graphical passwords." International Journal of Information Security, Volume 8, Number 6, December 2009, pp.387-398

[7] PENtcha – Caca Labs（2012 年 12 月 14 日取得）
http://caca.zoy.org/wiki/PWNtcha

[8] T Yamamoto, T Suzuki and M Nishigaki, "A Proposal of Four-panel cartoon CAPTCHA, " Advanced Information Networking and Applications March 2011, pp.159-166

[9] ASIRRA – Microsoft Research（2012 年 12 月 14 日取得）
https://research.microsoft.com/en-us/um/redmond/projects/asirra/

[10] 高橋健太, "テンプレート保護と生体認証基盤," 第 2 回バイオメトリクス研究会 2012 年電子情報通信学会ソサエティ大会

[11] 佐藤優人, 加藤貴司, ベッド B. ビスタ, 高田豊雄, "画像連想語呂合わせパスワードを利用したパスワード作成支援システムの改良手法の提案," SCIS 2010

[12] パスワード管理ソフト ID Manager（2012 年 12 月 14 日取得）
http://www.woodensoldier.info/soft/idm.htm

[13] IPA ISEC セキュア・プログラミング講座 : Web アプリケーション編 第 2 章 アクセス制限対策 : ユーザー認証（2012 年 12 月 14 日取得）
https://www.ipa.go.jp/security/awareness/vendor/programmingv2/contents/101.html

[14] Niels Provos and David Mazieres, " A Future-Adaptable Password Scheme, " USENIX Annual Technical Conference, 1999

[15] Bruce Schneier, " Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)," Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag, 1994, pp.191-204

[16] How Rainbow Tables work（2012 年 12 月 14 日取得）
http://kestas.kuliukas.com/RainbowTables/

[17] ニーモニックニュース：ニーモニックニュース 2012 年 6 月第 2 号（2012 年 12 月 14 日取得）
http://mneme.blog.eonet.jp/default/2012/06/post-b03a.html

[18] Rovert Morris and Ken Thompson, "Password Security: A Case History," Communications of the ACM November 1979 Volume22 Number11 , pp.594-597

[19] 青山貞一, 鷹取敦, "究極のパソコン活用 ～3 次元流体計算の可能性と課題～," 武蔵工業大学 環境情報学部 情報メディアセンタージャーナル第 8 号, 2007, pp.95-100

[20] 赤尾直彦, 披田野清良, 小松尚久, "最小距離エントロピーを用いた虹彩情報の情報量推定に関する一考察," SCIS 2011