SCIS 2005 The 2005 Symposium on Cryptography and Information Security
Maiko Kobe, Japan, Jan. 25-28, 2005
The Institute of Electronics, Information and Communication Engineers

写真を使った個人認証の脆弱性に対する改善策の提案

Another approach to enhance the security of photo-based Authentication

大貫 岳人* 高田 哲司** 小池 英樹*
Takehito Onuki Tetsuji Takada Hideki Koike

あらまし「あわせ絵」の有効性評価実験により、システム特有の脆弱性と懸念される問題点がいくつか確認された。これらの問題はその起因理由により「システムの仕様に起因するもの」と「利用者の登録写真内容に起因するもの」の2つに大別される。とりわけ前者に起因する問題である、Intersection Attack（出現頻度差分攻撃）及びCombination Attack（組み合わせ攻撃）は、この種の認証システムの安全性を脅かす問題であり、その改善は必要不可欠である。そこで本論文では、現状のあわせ絵の問題点を整理し、その改善策として認証で使用する「画像集合」に着目した改善手法を提案する。そして、その手法による利点と今後の課題を述べる。

キーワード： 個人認証、画像認証、

1 はじめに

個人の写真を利用した認証システム「あわせ絵」の利便性と安全性に着目した評価実験の結果、利便性に関しては、その認証成功率／操作性／認証時間においてある程度の有効性及び実用性が認められた。しかし一方で、安全性に関しては、システム特有の脆弱性が残されていることが推測実験による検証で明らかになった。その脆弱性とは、Intersection 攻撃と Educated Guess 攻撃の可能性を意味する。実用的な認証システムとするには、それら脆弱性に対し何らかの対策を講じる必要がある。我々はその具体的な改善策として、あわせ絵のシステム仕様に起因する問題、特にその画像集合の形成方法に着目し、主に２つのシステム改善案について取り上げていくことにする。本論文では、まず第２章において、あわせ絵の現状問題点の整理として、その脆弱性の要因と攻撃手法について説明する。第３章では、提案する改善案について、その目的と経緯、具体的な対策法を紹介する。第４章では、それら改善案と現在の「あわせ絵」との比較を行った。また、画像認証において想定される様々な攻撃手法とあわせ絵に対する安全性について紹介した。最後に本提案における今後の課題にまとめついて述べた。

* 電気通信大学大学院情報システム学研究科 〒182-8585 東京都調布市調布ヶ丘 1-5-1
Graduate School of Information Systems, University of Electro-Communications 1-5-1, Chofugaoka, Chofu, Tokyo, Japan 1-5-1
** ソニーコンピュータサイエンス研究所 〒141-0022 東京都品川区東五反田 3-14-13
Sony Computer Science Laboratories, Inc. 3-14-13 Higashigotanda, Shinagawa-ku, Tokyo, Japan 141-0022

2 問題となる脆弱性について

「あわせ絵」の現状問題点とは、その安全性に関して懸念されていた２つ攻撃手法、Intersection 及び Educated Guess 攻撃を利用した“なりすまし”推測実験を試みた結果、その有効性が認められたことである[1]。これらの攻撃手法の説明と発生要因について、実験で用いたシステム仕様に則して本章にて説明する。尚、現在の「あわせ絵」に関する詳細認証手順および仕様については論文[1]、[2]を参照して頂きたい。ページ制限の都合上ここでは割愛する。

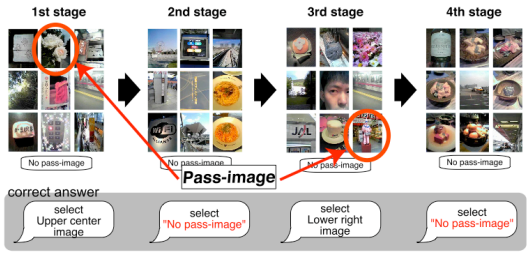

図 1: あわせ絵の認証手順

・Intersection 攻撃（出現頻度差分攻撃）

Intersection 攻撃とは、パス画像とおとり画像の出現頻度の差を利用した攻撃手法である。これは本来「パス

画像が必ず提示される」という掲示選択型認証方式における特有の弱点であった。この弱点に対し「あわせ絵」では、すでに「該当パス画像なし」という選択肢の設置により対策を図っていた(図１)。しかし、実験よりその対策をもってしても同攻撃手法による「なりすまし」が有効であることが裏付けられた[1]。

現在の「あわせ絵」では、他人数ユーザによる利用を想定し、全ユーザの写真画像を画像母集団として共有している。（図２）仮に各ユーザの保有するパスワードとなる画像（以降、パス画像とする）が４枚とすると、システムの利用者が 100 人の時、ユーザ A に対する自分以外の画像（以降、おとり画像とする）は残りの 99 人分、つまり 99×4=396(枚)となる。認証時に各照合画面に表示される画像は 9 枚で、その中の 0 枚または 1 枚がパス画像、残りがおとり画像となる（図１）。この時、ユーザ A が認証を行うと、パス画像は 4 枚の中から 1ー4 枚選ばれるが、おとり画像は 396 枚の中から 32ー35 枚となり、パス画像とおとり画像とでその出現率が大きく違うことが予想できる。攻撃者は、認証を繰り返す度に出現頻度の高い画像、すなわちパス画像を発見することが可能となる。つまり、Intersection 攻撃を引き起こす要因は、あわせ絵の画像を保持する母集団の画像数が各ユーザのパス画像数に比べ極端に差が大きい時に起こるといえる。この脆弱性は、あわせ絵の「システム仕様に起因する問題」として位置づけることができる。

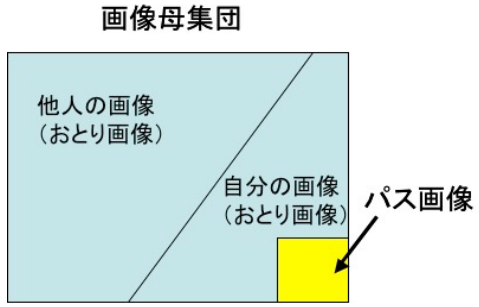

図 2: 現在の「あわせ絵」の画像集合イメージ

・Educated Guess 攻撃（推測攻撃）

Educated Guess 攻撃とは、利用者によって登録された画像内容から推測を図る攻撃手法である。この Educated Guess Attack とは、その推測に用いる情報の種類によってさらに２種類に分けられる。

- Knowledge Guess 攻撃（知識推測攻撃）
- Cognitive Guess 攻撃（認知推測攻撃）

一つは、Knowledge Guess 攻撃と呼ばれるもので攻撃対象とする相手の所有物、趣味、性格、行動情報といった“個人情報”を用いて特定の写真を絞り込み推測する手法である。これは、攻撃者の推測能力に依存する部分もあるが、何より攻撃者と被攻撃者の社会的関係の深さに影響するといえる。例えば、家族や親しい友人同士であれば、それぞれに所有する写真内容から容易に個人を特定し得る可能性がある。前回の“なりすまし”による推測実験の結果は、この Knowledge Guess 攻撃をし易い条件を攻撃者に与えてしまったことが主な原因であった。

二つ目は、Cognitive Attack（認知推測攻撃）という手法である。前者とその手法が重なる部分もあるが、大きな違いは、相手の個人情報がなくとも、写真自体の画面構成、画質、被写体との距離、被写体の種類といった共通点や類似性を見いだし、ある特定の個人に所属する画像として推測を行う方法である。

上記２種類の攻撃法は、いずれも利用者によって登録された写真内容の情報を用いて推測しているという点で「登録された写真内容に起因する問題」といえる。しかし、後者の Cognitive 攻撃に関しては、もともと他人と画像共有をしているが為に個人の特徴的な“癖”が見いだされてしまうとも考えられる。そういった意味では、この手法は「システムの仕様に起因する問題」とも言えるのである。

3　改善案について

前述したあわせ絵の現状問題点における考察をふまえて、その「システム仕様に起因する問題」である Intersection 攻撃に対する脆弱性改善にその主眼を置いた。着目したのは、あわせ絵の「画像母集団の形成方法」である。結論から先に述べると、最終的な改善案として二つのあわせ絵画像母集団を提案することになる。その詳細を説明するにあたり、我々が辿ったアプローチを PHASE１ー４の段階ごとに分けて順に説明する。

3.1　PHASE１：「母集団非共有型」の提案

Intersection 攻撃に対する具体的な改善策について考えてみる。Intersection 攻撃が発生する要因は、パス画像とおとり画像の出現頻度の差であると述べた。つまり、その差を“０(ゼロ)”にすれば、この手法は成り立たないのである。その為には、パス画像とおとり画像の出現比率を同一にする必要がある。この時、本研究で着目したのはあわせ絵における画像集合の共有形態、つまり「画像母集団の仕組み」である。この画像母集団の仕組みにおいて、その第一案である「母集団非共有型あわせ絵」を提案する。

母集団非共有型とは、パス画像とおとり画像の出現率を最初から共に一定値に固定するという方法である。現在の「あわせ絵」では、一回の認証で合計 36 枚の画像が表示されることになっている(図１)。単純に考えると、母集団の全画像が 36 枚であれば一回の認証につきどの画像も常に出現し、その出現率は一定値となる。しかし、あわせ絵では各照合画面において「パス画像無し」という選択肢があり、また照合作業を４回としてある為、「パス画像が提示されない場合」を考慮して余分に３枚（「１枚も出現しない」という条件を省く）必要となる。従って 39 枚の画像数で母集団を形成すれば、理論上出現頻度の差は限りなく 0 に近い値となり Intersection 攻撃に対する脆弱性は無くなるといえる。

ここで、39 枚という固定された画像数によって「あわ

せ絵」の現実での利用を想定してみる。現在のあわせ絵では他人との共有によって画像母集団を形成している(図２)。自分のパス画像を４枚とした場合、残りのおとり画像 35 枚を画像母集団から部分的に抽出し、39 枚による新たな母集団を形成することになる。ここで問題となるのは、この母集団の画像数が少な過ぎるということである。つまり、仮に攻撃者がなりすまし攻撃を行うとすると、まず一度の認証試行でほぼ全ての画像情報(実際には 36 枚分)を手にすることになる。そして、その僅か 36 枚の画像から特定の正規ユーザのパス画像を Educated Guess 攻撃によって推測する事は、現在の「あわせ絵」のように、数百／数千枚の中から推測することに比べ遥かに実現性が高くなってしまうからである。

そこで、その問題に対処する為に 39 枚の母集団画像を全て利用者本人のものとする条件を設置した。表示される画像が全て特定個人のものであれば、その画像内容に現れる特徴はすべて“本人のもの”となる。本人さえパス画像を記憶していれば、他人からは「どれも同一人物によるもの」ということは分かったとしても、「どれがパス画像であるか」までを推測できる可能性は極めて低くなると考える。これは、前述した Educated Guess 攻撃に対して非常に効果的な対策となる。これらの条件は結果的に、画像母集団を他人と共有しないということになる。ここでこの改善案を第一案として「母集団非共有型」と呼ぶことにする。第一案により、改善目的であった脆弱性 Intersection 攻撃の問題を解決し、さらに Educated Guess 攻撃に対しても効果が見込めると言えた。

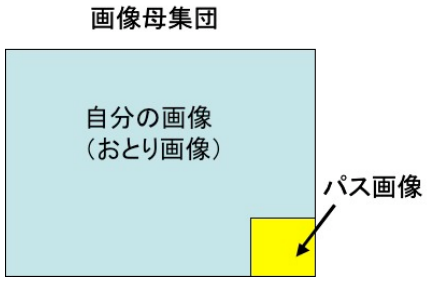

図３:「母集団非共有型」あわせ絵の画像集合イメージ

3.2 PHASE 2:「Combination 攻撃」の発見

「母集団非共有型」あわせ絵に対して更なる安全性の考察を行った結果、その改善によって新たな脆弱性が発生した。それは Combination Attack（組み合わせ攻撃）と呼ぶものである。まずは、その攻撃手法の原理から説明する。

・Combination Attack（組み合わせ攻撃）

Combination 攻撃とは、パス画像が２枚以上登録されている時、「パス画像同士は同一照合画面に出現しない」という条件を利用して、母集団の全画像情報から同一照合画面内に表示された全ての画像ペア（組み合わせ）を消去していき、より最終的にペアとして存在しなかった画像群をパス画像として絞り込んでいく手法である。

図４を用いてこの攻撃手法の概念を詳しく説明する。

まず、攻撃者は何らかの手段により、母集団非共有型の全画像情報(39 枚)を知ったとする。この時、全画像数に対応した、39×39 のマトリクス表を用意する(作業①)。この表に、各照合画面にて表示された９枚の画像群全てに対し、１対１の画像ペアを作り（作業②）、該当する各ペアのセルを順に消去していく（作業③）。こうすると、最終的に消去されずに残った画像ペアがそれぞれパス画像として割り出せることになる。では、実際に何回目の認証作業でパス画像を絞り込むことができるのか計算してみることにする。まず、このマトリクス表のセル数は 39×39-39=1482(個)存在する。各セルは１つの画像ペアに対して必ず２つのセルに対応しているので、組み合わせとしては全セル数の半分の 741 通り存在することになる。1 つの照合画面で掲示される画像は９枚なので、それぞれの画像ペアの組み合わせ数は $_9C_2$=36 通り存在する。そして１回の認証試行で、照合画面が４回現れるとすると、39×4=156 通りの組み合わせが一度の認証で判明することになる。となると 741 通り全ての組み合わせが判明する最短認証回数は、741÷144=5.146 となり、（母集団画像が 39 枚、パス画像が４枚、照合画面の表示画像数９枚、照合回数が４回という条件において）理論上６回目の認証試行でパス画像を絞り込める可能性があるということになる。

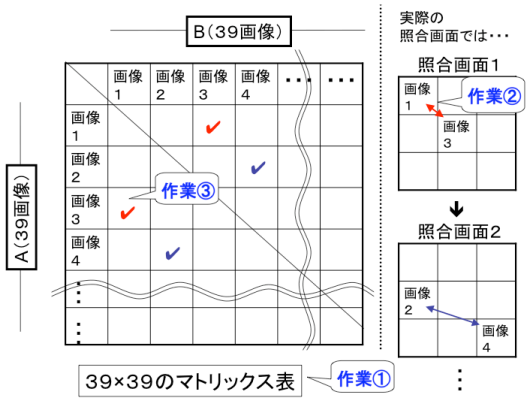

図４: Combination 攻撃の攻撃手法の概念

しかし、現実的には６回の認証試行でパス画像を特定することは不可能と言ってよい。何故なら、あわせ絵システムは認証の度に画像をランダムな組み合わせで各照合画面に掲示しており、さらに、使用されるパス画像も1ー3 枚と変動するからである。とはいっても、理論的にはその可能性が示されており、決して無視できる問題ではない。数回の認証試行では不可能であっても、数十回、数百回のデータを採取すれば、実行可能であると言える。

3.3 PHASE 3:「母集団限定共有型」の提案

Combination 攻撃が発生した経緯とその要因について整理する。今回の「母集団非共有型」あわせ絵の改善案に伴い、現行のあわせ絵より変更した部分は、母集団の画像数を 39 枚に固定した点と母集団の画像共有を“非

共有”とした点である。それらをふまえると、この Combination 攻撃を引き起こす要因は、その母集団の全画像情報から消去して行くという手法からして、母集団の画像数の少なさにあるといえる。さらに、母集団の画像が少ないということは全ての画像リストを盗まれ易いということも言える。このことから、Combination 攻撃に対処する有効的手段は、母集団の画像数を増やすことであると言える。しかし、簡単には増やせない大きな理由がある。その理由とは、単純に母集団の画像数を増やすとパス画像とおとり画像の出現頻度が偏り、再び Intersection 攻撃を招いてしまうおそれがあるからである。では、どのような基準で母集団の画像を増やせば良いのか。その問題点に対し我々は再びあわせ絵の画像集合に着目した。その結果、２つ目の改善案である「母集団限定型」あわせ絵を提案するに至った。これは、“母集団非共有型”の「パス画像数とおとり画像数を始めから一定値に固定する」という方法に対し「利用者の登録するパス画像数に合わせて、おとり画像数も変化させる」という方法である。では、その「母集団限定型」あわせ絵の画像集合の仕組みから説明する。

「母集団限定型あわせ絵」では、その画像母集団は現在の「あわせ絵」と同じ枠組み（母集団）を利用し、その中に限定された母集団(以降、小母集団と呼ぶ)を置いた(図 5)。画像母集団を現状のあわせ絵と同じ“共有型”としたのには理由がある。それは、利用者の登録するパス画像数の変化に伴い必要となるおとり画像数や小母集団形成の多様化に幅広く対応可能とする為である。この小母集団は、パス画像数の変更に応じて動的に適正なおとり画像数を母集団から割り当て再形成されるもので、そのおとり画像数は可変となる。

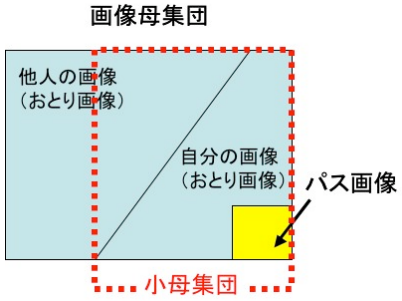

図 5:「母集団限定共有型」あわせ絵の画像集合イメージ

まず実際の認証作業において、システムが行う手順から述べる。始めにユーザがパス画像を登録すると、そのパス画像の総数 P を調べる。次に、その P から各パス画像の出現率 Pr を算出する。そして、Intersection 攻撃を防ぐために、Pr と出現率が等しくなるような最適なおとり画像数 D を求め、その画像数 D を母集団からランダムに確保し、小母集団として形成する。ここで出現率 Pr と適正なおとり画像数 D の算出例について以下に示した。

[現在の「あわせ絵」の仕様における、任意のパス画像の出現率 Pr とおとり画像数 D の算出例]

仕様条件：ユーザの登録するパス画像 P：4 枚 (P_1~P_4)
照合画面の表示画像数 9 枚
照合回数数 4 回

１回の認証試行における P の出現枚数 1~4 枚によってそれぞれ場合分けを行う。

(i) 1 回の認証試行に P が 1 枚出現するとき
まず、システムはその認証試行において P を何枚つかうかを決める。その選択肢は「1~4 枚」と「0 枚（該当画像なし）」の計 4 通りある。従って、

・ 選択肢の中から P を 1 枚使用する確率は 1/4

となる。また、

・ P_1~P_4 で任意の P(以降、P_1 とする)が抽出される確率は 1/4

となる。よって(i)の場合 P_1 の出現確率は

$1/4 \times 1/4 = \underline{\mathbf{1/16}}$

同様に、(ii) 1 回の認証試行に P が 2 枚出現するときを考える。

(ii) 1 回の認証試行に P が 2 枚出現のとき

・ システムが P を 2 枚使用する確率は 1/4
・ 2 枚の P の中で P_1 が 1 枚目に出る確率は 1/4
・ 2 枚の P の中で P_1 が 2 枚目に出る確率は 3/4×1/3

従って、

$1/4(1/4+3/4\times1/3) = \underline{\mathbf{2/16}}$

同様に、計算すると(iii) の P が 3 枚出現するときは、

$1/4(1/4+3/4\times1/3+3/4\times2/3\times1/2) = \underline{\mathbf{3/16}}$

(iv) の P が 4 枚出現するときは、

$1/4\times1 = 1/4\ (= \underline{\mathbf{4/16}})$

これらの結果より、任意の P_1 が出現する確率 Pr は、

$\therefore \mathbf{Pr} = 1/16+2/16+3/16+4/16 = \underline{\mathbf{5/8}}$

となる。

ここで、おとり画像数を D とすると、1 回の認証試行で出現するおとり画像数は 32~35 枚で、その平均は 33.5 枚となる。すると任意のおとり画像の出現率 D_r は

$D_r = 33.5/D$

と表すことができる。従って、パス画像とおとり画像の出現率が等しくなる D を求めるには、

$Pr = D_r = 33.5/D = 5/8$

より、$\underline{\mathbf{D = 53.6}}$　　$\therefore \mathbf{D=54}$

上記の算出結果より、“現行のあわせ絵”の仕様（パス画像が 4 枚、照合画面の表示画像数 9 枚、照合回数が 4 回という条件）において、その最適なおとり画像数は 54 枚であることが分かった。この算出方法を利用すれば、ユーザの登録するパス画像数に合わせて、自動的に最適なおとり画像数を割り当て、Intersection 攻撃を無効とすることが可能となる。また、Combination 攻撃に対しては、ユーザの所有するパス画像を増やせば、それに伴いおとり画像が増員され、結果的に母集団画像数が増えたことになり脆弱性が強化されることになる。

3.4 PHASE 4 : Combination 攻撃に対するさらなる強化法

“非共有型”から“母集団限定型”を提案することによって、Combination 攻撃に対して“利用者のパス画像の増加”により防御率が高められることが分かった。しかし、それでも根本的な解決とは言えない。参考データとして、前節での仕様条件（パス画像 4 枚、おとり画像 54 枚）で図 4 の概念を用いて Combination 攻撃の評価を行うと、理論上最低 11 回の試行回数でパス画像が絞り込まれてしまうということが分かった。では逆に、100 回の試行回数に耐えるにはという問いに対しては、約 10 枚のパス画像と約 160 枚のおとり画像数が必要であることが分かった。これらの結果に対し、利便性と安全性のバランスにおいて実用性を満たした改善策とは言い難い。

そこで、我々はシステム仕様に関して新たに「専用おとり策」と呼ぶ機能の付与を考えた。この「専用おとり策」とは、Combination 攻撃で利用される条件「パス画像同士は同一照合画面に出現しない」に着目し、反対にその条件を利用不能にすることである。その方法とは、パス画像設定時に、ある特定のパス画像とおとり画像に対し、もしくは特定のおとり画像同士に対し「同一照合画面には出現しない」という条件を適用することである。その結果、攻撃者はパス画像の絞り込みが不可能となる。この機能に対しては、試行回数による制限がないため、非常に有効な改善法となる。さらに、この「専用おとり策」の実装においては、母集団非共有型／母集団限定共有型の双方に適応可能なものである。この「専用おとり策」機能を実装することによって Combination 攻撃によるパス画像の特定は理論上不可能となったと言える。

4 提案手法の利点と限界

4.1 改善案と現行「あわせ絵」との比較

提案した２つの改善案を現在の「あわせ絵」と比較し予想される効果、利点、特徴について整理する。今回、「非共有型」と「限定共有型」という２種類の画像集合体系を紹介したが、この母集団の概念によって分類すると、現行のあわせ絵は「完全共有」という分類に位置づけることができる。

［共有形態］	［完全共有］	［半共有］	［非共有型］
［攻撃手法］	母集団共有型 現行あわせ絵	母集団限定型 あわせ絵	母集団非共有 型あわせ絵
Intersection攻撃	×	◎	◎
Educated Guess攻撃	△	△	○
Combination攻撃	○	◎	○

◎:有効である ○:ある程度効果が見込める △:どちらとも言えない
×:効果はない

図 6: 改善による攻撃手法に対する有効性の評価

図６は本論文にて扱った「あわせ絵」特有の各種攻撃手法に対し、現在のあわせ絵及び改善案１、２の母集団型において予想される有効性の評価をしたものである。

・Intersection 攻撃

今回の改善によってその攻撃手法をほぼ無効とすることができた。これにより「出現頻度が高い画像＝パス画像」という条件は成立しなくなる。

・Educated Guess 攻撃

おとり画像も本人の画像となる「母集団非共有型あわせ絵」では、利用者を特定できても、パス画像までを特定することは困難となる為、Cognitive Attack に対しては効果があると見込まれる。しかし、一般的にこの攻撃手法はあわせ絵においてもっとも懸念される点であるが、決定的な解決策が見つかっていない。やはりユーザに依存する要素が多い問題である。しかし、ユーザの訓練や意識によっては、その登録画像を利用して反対に攻撃者を惑わす“道具”として機能することも考えられる。

・Combination 攻撃

「専用おとり策」機能によって「母集団限定型」および「母集団非共有型」あわせ絵の両方で効果がある。しかし“非共有型”あわせ絵では、“限定共有”に比べ元々の母集団の画像数が固定で少ないのと、パス画像の増加による強化が行えないというのが、有効性において万全とは言えない理由である。

4.2 想定される他の攻撃手法とその安全性

掲示型画像認証方式に対して想定される各種攻撃手法について紹介する。これらの脆弱性に対して更なる考察や実験による検証は不可欠である。図 7 は、それら攻撃手法の性質と予想される脅威の度合いによって整理した。なお、各攻撃手法について、中には、その攻撃方法や要因がまだ明らかになっていない部分もあり、その攻撃手法の要因として着目する部分によって解釈の仕方が様々であり、あくまで目安としての分類として理解して頂きたい。

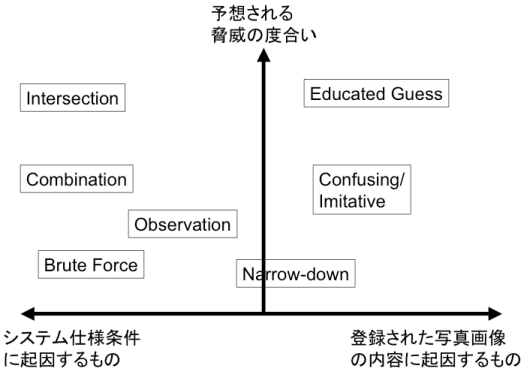

図 7: 想定されるさまざまな脆弱性の分類

・Narrow-down 攻撃(絞り込み攻撃)

照合画面のおとり画像を特定の画像で埋め尽くし、結果的に特定個人のパス画像がむき出しになってしまう攻撃手法である。この手法を使うには、母集団の画像を攻撃者の画像で埋め尽くす必要がある。母集団の画像数が少ない時は、攻撃者一人で実行可能だが、現実的には多人数による攻撃でないと不可能である。

・Confusing/Imitation 攻撃 (模倣攻撃)

同一または非常に類似した画像を登録することによって、正規ユーザのパス画像の判断を混乱させる攻撃手法である。攻撃者の目的は、攻撃対象者のパス画像を知ることではなく、ユーザの認証行為やサービス利用を妨害することにある。いわゆるDOS攻撃の一種である。この攻撃手法も母集団の画像数が多ければ脅威とはならないが、他のユーザが無意識に類似した画像を登録してしまった場合は別の問題として考慮する必要がある。関連研究では画像ヒストグラムを利用し類似した画像を自動識別するという解決法を提案している[3]。

・Brute Force 攻撃

画像の選択パターンを変えつつ繰り返し攻撃を行う手法で、別名 Random 攻撃または Dictionary 攻撃とも呼ばれる。この場合、その選択パターンが何らかの知識情報に基づいているならばEducated Guess 攻撃となるが、基本的には画像選択時の画面インターフェースに依存する攻撃手法である。現状のあわせ絵では照合画面数と解答選択肢から正当確率は1/9999となり、4桁の暗証番号認証とほぼ同じ強度である。一定時間内においてある試行回数で認証ロックがなされる機能を導入すれば、脅威とはならないと考えられる。

・Observation 攻撃

Shoulder Surfing、またはReplay Attackとも呼ばれる手法で、認証時の作業内容や秘密情報を物理的にあるいは通信データの盗聴によって入手し、その情報を使って”なりすまし”を行う手法である。基本的にChallenge-Response方式の認証であれば、ある程度防ぐ事ができる攻撃である。

5 今後の課題

今後の課題として、まず挙げられるのは今回提案した改善案に基づく実際の評価と検証である。前回のあわせ絵評価実験と同様に、その安全性を検証する評価は必要不可欠である。その為には、これらの提案に基づくシステムの実装が必要である。改善案１、２ともその実装における実現性は高いと予想されているが、その構築段階で新たな問題点や脆弱性が発見される可能性もある。また、実際問題としていくつかの脆弱性については、その条件や環境設定の準備が困難なものも想定される。例えば、前回のなりすまし実験においても、厳密にIntersectionとEducated Guess攻撃の分離による測定が困難であった。またその一方で、実際の攻撃者はいくつかの攻撃手法を併用して攻撃を行う可能性が高く、単純に各々の脆弱性が低いからといっても軽視できない要素があることも考慮しなければならない。その様な問題に対しても、有効な解決／代替策などを図って行く必要がある。

6 おわりに

本研究では、前回の“あわせ絵”評価実験において検証された脆弱性について、主に２つの改善案を提案した。Intersection攻撃に対し、「母集団非共有型あわせ絵」を提案し、その提案により発生した新しい攻撃手法Combination 攻撃に対しては、「母集団限定共有型あわせ絵」によって改善を試みた。後者の提案により、若干の改善が見込まれたが、十分な対策ではないとして、最後に「専用おとり策」機能を提案した。これらの提案により、あわせ絵システムの仕様に起因する脆弱性については改善が図られたといえる。一方、利用者の登録画像内容に起因する問題、Educated Guess攻撃については、「母集団非共有型あわせ絵」では効果が見込まれるものの、依然として画像認証における脅威として未解決に終わった。考察として、今回の改善案と現行のあわせ絵の比較を行いその改善効果を示した。今後の課題としては、改善案の実装とその有効性評価が必要であると同時に、画像内容に起因する問題についても評価を行う必要があるということを述べた。

7 参考文献

[1] 大貫岳人、高田哲司、小池英樹: 画像認証システム「あわせ絵」の有効性実証のための評価実験, to appear, SCIS2005, (Jan 2005).

[2] 高田哲司、小池英樹 : あわせ絵:画像登録と利用通知を用いた正候補選択方式による画像認証方式の強化法, 情報処理学会論文誌 Vol. 44 No.8, pp.2002-2012 (2003)

[3] Trevor Pering, Murali Sundar, John Light, and Roy Want: Photographic Authentication through Untrusted Terminals, IEEE Pervasive computing 1536-1268 (2003).

[4] Dhamija, R. and Perrig, A.: Deja Vu: A User Study Using Images for Authentication, 9th Usenix Security Symposium, pp.45-58(Aug. 2000).

SCIS2005 事務局
Email: scis2005-query@xxx.xxx.jp