

[研究論文]

視き見攻撃耐性を考慮した スマートフォンにおける個人認証方式の検討

市村亮太¹・野口敦弘¹・納富一宏¹・斎藤恵一²

1 博士前期課程情報工学専攻

2 国際医療福祉大学情報教育センター

A personal authentication method for smartphone against shoulder surfing

Ryota ICHIMURA¹, Atsuhiko NOGUCHI¹, Kazuhiro NOTOMI¹, Keiichi SAITO²

Abstract

In this article, we discussed features of resistant for shoulder-surfing attack on smartphone at the time of PIN code inputting. Generally, smartphone is not safe for shoulder-surfing attack, because it has large screen and operational movements of fingers are shown on the touch panel. Therefore we propose a personal authentication method and an interface against shoulder-surfing attack for smartphone. The proposed method has 3 features to defend shoulder-surfing attacks as following: 1) variable alignment of ten keys on 5x6 key matrix, 2) control of constraint display time and 3) dummy keys contained in key matrix. Using proposed interface, we experimented 20 subjects to compare our method from usual PIN code input method. Then the result of the experiment showed that proposed method can decrease more than 70% success rate of shoulder-surfing attacks. Therefore our method is available for secure login to smartphone using PIN code.

Keywords: personal authentication, shoulder surfing, smartphone, security and paired comparison

1. まえがき

近年、iPhone や Android 搭載携帯端末の登場により、スマートフォンの普及が急速に伸びている。Fig.1 に株式会社シード・プランニングが 2012 年 4 月から 7 月までの調査を行い作成した世界の携帯電話普及予測¹⁾を示す。

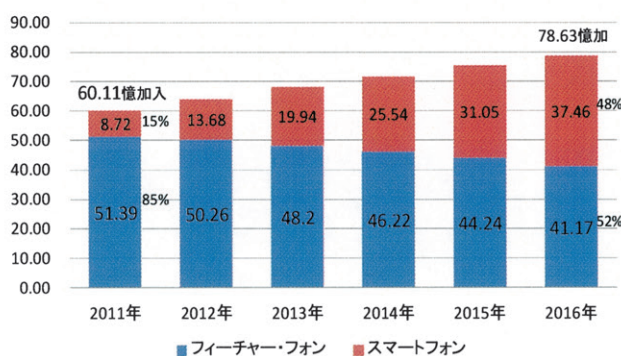


Fig.1 世界の携帯電話普及予測（単位：億加入）

この調査によると、2011 年の世界のスマートフォン普及

台数は、8 億 7200 万加入、人口普及率 12%。2016 年末では、37 億 4600 万加入、人口普及率 49%と予測している。地域別人口普及率は、北米 96%、欧州 64%、中南米 50%、アジア・太平洋 46%、中近東・アフリカ 38%となっている。また、携帯電話に占めるスマートフォン比率は、2011 年の 15%から 2016 年には約半数になると予測している。調査結果から、スマートフォンの一般ユーザへの普及は今後も世界的に拡大していくことが考えられる。

しかしスマートフォンは、タッチスクリーンデバイスであるため、入力デバイスと表示デバイスが一体化しており、フィーチャー・フォンと呼ばれる従来型の携帯電話端末に比べると画面サイズも大きく、結果として第三者によって入力情報を読み取られやすい²⁾。Fig.2 はフィーチャー・フォンとスマートフォンの PIN (Personal Identification Number) 認証時を写真で比較したものである。フィーチャー・フォンに比べ、スマートフォンの画面の視き見が容易であることがわかる。こういった問題点から、背後からの視き見攻撃を受ける危険が高いと考えられる。視き見攻撃とは、端末を操作している様子を背後から覗き込み、パスワードや重要な情報を盗む行為である。

そこで本稿では, スマートフォンにおいてもよく利用される PIN を用いた認証を行う際に, キー配置の変更, キー表示時間の制限, ダミーキーの採用によって視き見攻撃耐性を付加した認証インタフェースを提案する.

まず, 複数のレイアウトを用い, 一対比較実験を行うことによりインタフェース決定を行う. 次にその結果をもとに, 従来の認証手法と提案手法での視き見攻撃耐性の比較を行う第一視き見実験を行う. そして, 第一視き見実験において追加実験が必要だと考えられる部分において, 第二視き見実験を行なっている.



Fig.2 PIN 認証時の画面比較

2. 理論

2.1 PIN

PIN はクレジットカードやキャッシュカードの利用の際に, 持ち主を確認するために使用される暗証番号のことである. 多くの場合, 4桁のPINが用いられる.

入力中のパスワードを表示しないタイムシェアリング時代から続けられている従来の手法は, 視き見攻撃への対策としては有効である. しかし, 新しいパスワードの入力を行う際にも文字がまったく表示されないため, 新しいパスワードを覚えるのが大きな負担になるという問題がある³⁾.

提案手法では, 入力したパスワードを一定時間表示する機能を設けており, この問題を解決するとともに, パスワードを表示することによって視き見攻撃者にPINを読み取らせない仕掛けを用意している. 詳しくは3章で述べる.

2.2 一対比較

複数の試料を比較しようとするとき, 順序法と呼ばれるすべての試料を一度に順位づける方法では困難な場合がある. このような場合, 試料の中から2個ずつ取り出して対にして比較していき, すべての試料を比較して評価する方法を一対比較法と呼ぶ^{4), 5)}. 主な一対比較法を Table 1 に示す. 本実験では, 平均的な価値判断からの偏りを測定するために Thurstone の一対比較法を用いた.

Table 1 主な一対比較法

判断方法	求まる尺度	手法
順位を付ける	順位尺度	一意性の係数
		一致性の係数
	間隔尺度	Thurstone の一対比較法
差の程度を評点で示す	比例尺度	Bradley の一対比較法
	間隔尺度	Scheffe の一対比較法 (各変法を含む)

3. 視き見攻撃耐性を考慮した個人認証方式

3.1 キー配置の変更

PIN を用いた従来の認証手法では, 3列4行のキー配置が一般的である. 提案手法では5列6行分のキー配置とし, Fig.3 のようにランダムな配置でテンキーを表示する. テンキーが表示されている以外のキーをダミーとすることで, 視き見攻撃耐性の向上を実現する. ダミーキーについての詳細な説明は2.3節で行う.

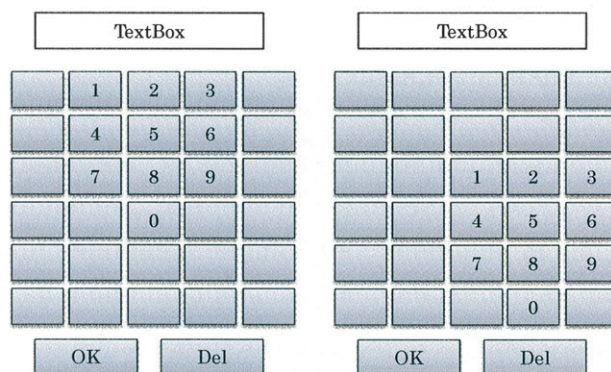


Fig.3 テンキーの配置

3.2 キー表示時間の制限

2.1節で説明したテンキーの表示時間を制限することにより, テンキーとダミーキーの識別が困難になる. Fig.4 のようにテンキーが表示された後, 数字表記が消える. 認証開始時から一定時間はテンキーが表示されるため, 被認証者はテンキーが表示されている間にその配置を記憶する必要がある.

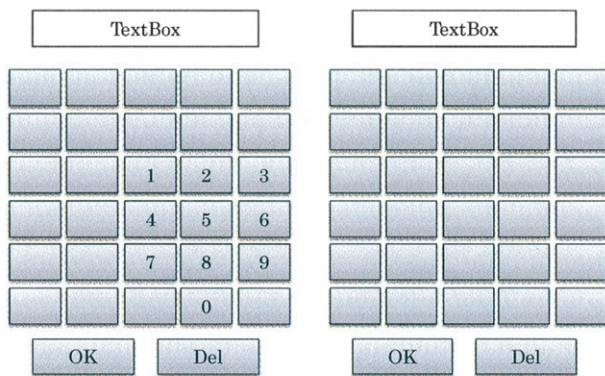


Fig.4 キー表示時間の制限

3.3 ダミーキー

認証開始時に表示されたテンキー以外のキーは、Fig.5に示すようにすべてのキーがダミーとなる。Dはダミーキーであることを示している。キー表示時間の制限により数字表記が消えることで、視き見攻撃者はどのキーがダミーキーなのかが分からなくなる。ダミーキーを押下した場合、0～9までのランダムな数字がTextBox内に表示される。

Fig.6は「D, 9, 4, D, D, 2, 9」と入力した際のTextBox内の表示である。実際には入力されたキーが一度TextBox内に表示され、1.5秒が経過、または次のキーを入力することにより米印表記に変わる。Fig.6に示すように、ダミーキーを入力した位置には0～9までのランダムな数字が表示されている。ダミーキーによる入力は見かけ上入力されているように見えるが、ダミーキーは暗証番号の照合の際には考慮されない仕掛けとなっている。

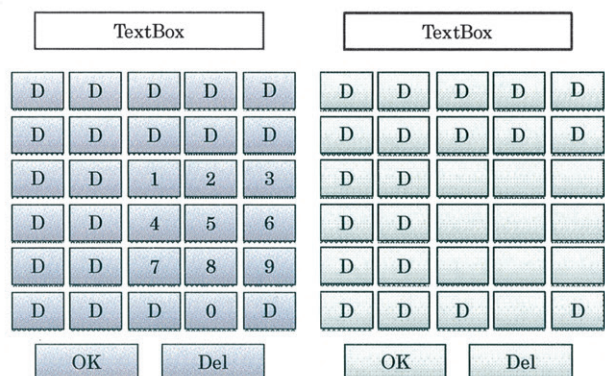


Fig.5 ダミーキー



Fig.6 ダミーキー入力時の TextBox

4. 一対比較実験

4.1 実験目的

今回提案した手法において、キーのサイズや配置間隔、また、情報提示時間に明確な基準が存在しないため、インタフェースを一対比較実験を行うことにより決定する。

4.2 実験機器

実験に使用したスマートフォンをFig.7に、スペックをTable 2に示す。



Fig.7 実験に使用したスマートフォン

Table 2 実験機器

型番	OS	タッチパネルサイズ
ISW11SC	Android 2.3.6	4.7 インチ

4.3 実験条件

キー配置のレイアウトを2パターン、キー表示時間を3パターン用意し、本学学生の被験者10名にスマートフォンを用いて提案手法での認証を行ってもらった。入力してもらったキーは「D, 9, 4, D, D, 2, 9」の順で統一した。普段通りに使用してもらい、直観的な判断を可能にするため、持ち方、入力方法について特に指示はしていない。実験の様子をFig.8に示す。また、レイアウトパターンをFig.9, Fig.10に示し、パターンごとの条件をTable 3に示す。

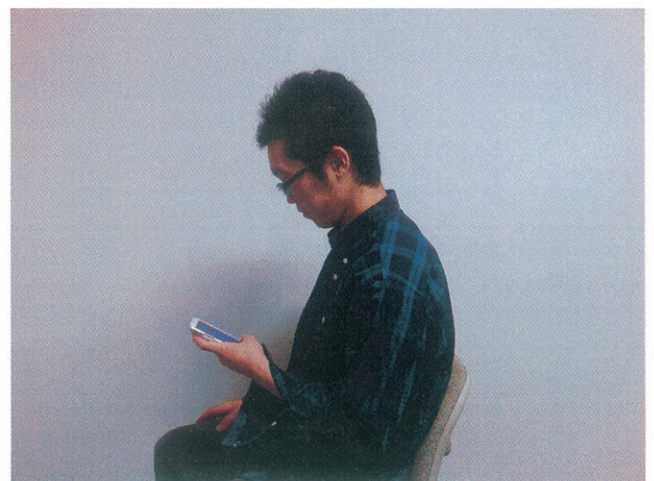


Fig.8 実験の様子

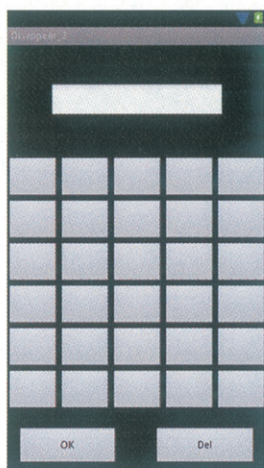


Fig.9

レイアウト Btn (L)

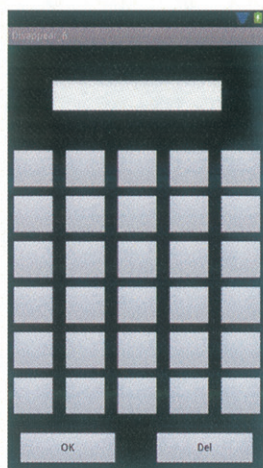


Fig.10

レイアウト Btn (S)

Table 3 ボタンレイアウトと表示時間

パターン	レイアウト	キー表示時間[秒]
Btn (L1)	Btn (L)	1
Btn (L2)	Btn (L)	2
Btn (L3)	Btn (L)	3
Btn (S1)	Btn (S)	1
Btn (S2)	Btn (S)	2
Btn (S3)	Btn (S)	3

4.4 実験結果

Fig.11 に対比較実験の結果を示す。尺度値が大きいほど順位は高く、使いやすいことを示す。Btn (S3)、Btn (S2)、Btn (L2) は順位が高く、Btn (L3)、Btn (S1)、Btn (L1) は順位が低かった。

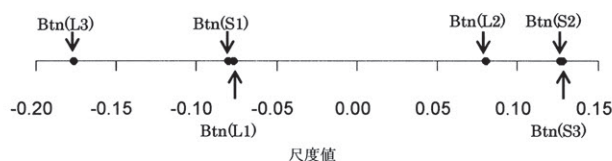


Fig.11 一対比較結果

4.5 考察

キー表示時間が1秒のものは、順位が低い結果となった。1秒ではキー配置を覚えるのには不足だと感じた被験者が多かったため、このような結果になったと考える。しかし、実験終盤になると1秒のものを選択する被験者もいたことから、慣れによりキー表示時間を減らすことが可能だと考えられる。慣れてくることで、今回の実験において順位が高い結果となった Btn (S3) の順位は低くなることが予測できる。レイアウトは Btn (S) の順位が Btn (L) に比べて高かった。これは Btn (S) のほうが Btn

(L) に比べてボタン間の間隔が広く、押し間違えにくいという安心感があったためだと考える。

5. 第一視き見実験

5.1 実験目的

実際に提案手法において視き見攻撃に耐性があることを調査するため、第一視き見実験を行った。一対比較実験において得られた結果のうち、順位の高かった Btn (S3) と Btn (S2) を用いて視き見実験を行った。

5.2 実験機器

実験機器は一対比較実験で使用した機器と同一である。

5.3 実験条件

入力被験者を1名、視き見被験者を20名とし、視き見被験者には計7回視き見を行ってもらった。入力被験者は椅子に座った状態でスマートフォンを左手に持ち、親指でキー入力を行う。視き見被験者は入力前に視き見可能な位置へ移動してもらい、一試行ごとに入力された暗証番号を紙に記入してもらう。実験の様子を Fig.12 に示し、各試行の条件を Table 4 に示す。従来手法において、キー表示時間が常に表示となっているが、これはキー表示時間の制限が従来手法には存在しないためこのようにしている。また、視き見被験者には連続で視き見を行ってもらうため、同一の数字ではパターンが読み取られてしまうと考え、入力内容の数字を一部変更している。従来手法は、実験機器であるスマートフォンに搭載されている画面ロック解除を行うための PIN 認証とした。Fig.13 に入力画面を示す。従来手法において、入力されたキーが TextBox 内に表示され、1.5 秒経過または次のキーを入力すると米印になる。提案手法はこれと同じ仕組みとしている。

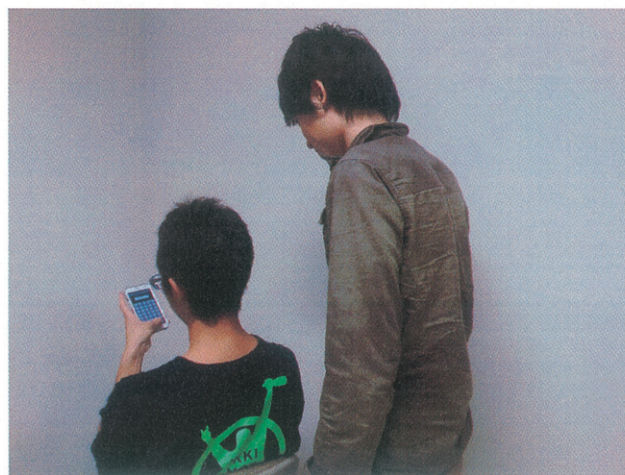


Fig.12 実験の様子

Table 4 実験で用いた PIN パターン

手法	入力内容	キー表示時間[秒]
従来	6128	常に表示
提案 (a)	6128	3
提案 (b)	D94DD29	3
提案 (c)	D32DD32D	2
提案 (d)	6128	2
提案 (e)	D32DD32D	3
提案 (f)	D94DD29	2



Fig.13 従来手法とした PIN 認証

5.4 実験結果

Fig.14 に視き見実験の結果を示す。従来手法での視き見攻撃成功率は 100%となった。提案手法 (a) と提案手法 (d) のダミーキーを含めない入力内容のものでは、提案手法 (a) が 70%, 提案手法 (d) が 75%となり、ダミーキーを含めた場合の視き見攻撃成功率は 0%となった。

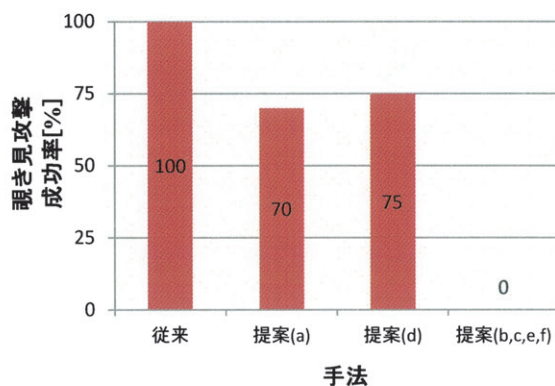


Fig.14 第一視き見実験結果

5.5 考察

従来手法での視き見攻撃成功率は 100%となり、視き見

攻撃に対し非常に危険であることがわかる。視き見攻撃成功率は提案手法 (a) が 70%, 提案手法 (d) が 75%となったことから、キー表示時間の制限とキー配置の変更により、従来手法に比べると 25~30%の視き見攻撃への耐性ができたといえる。提案手法 (b, c, e, f) でのダミーキーを含めた場合の視き見攻撃成功率は 0%となったが、これはダミーキーなどの仕掛けを視き見攻撃者に教えていなかったため、このような結果になったと考える。また、ダミーキーを含めた場合にすべての視き見被験者が暗証番号を 4 桁よりも多く紙に記入していた。これは、入力部分を見るのではなく TextBox 内を見ていたため、暗証番号を読み取ることができなかったといえる。視き見攻撃者が仕掛けを理解していた場合に、どの程度提案手法が視き見攻撃への耐性を示せるのかを調査する必要がある。

6. 第二視き見実験

6.1 実験目的

第一視き見実験において、提案手法 (b, c, e, f) での視き見攻撃成功率は 0%となったが、これはダミーキーなどの仕掛けを視き見攻撃者に教えていなかったためにこのような結果になったと考えられる。視き見攻撃者が仕掛けを知っていた場合の視き見攻撃成功率を調査する必要があると考え、この第二視き見実験を行った。第一視き見実験により、Btn(S3) と Btn (S2) では視き見攻撃成功率の差は 5%と誤差程度であった。一対比較実験により、慣れることで Btn (S2) が Btn(S3)の順位を上回ることがわかったため、第二視き見実験では、レイアウト Btn (S2) のみを用いている。

6.2 実験機器

実験機器は一対比較実験、第一視き見実験で使用した機器と同一である。

6.3 実験条件

入力被験者を 1 名、視き見被験者を 20 名とし、視き見被験者被験者には計 4 回視き見を行なってもらった。各試行の条件を Table 5 に示す。その他の条件については第一視き見実験と同様である。従来手法において入力桁数を 8 桁にしたのは、提案手法において 4 桁の PIN に 4 桁のダミーキーを混合させたものとの比較を行うためである。

Table 5 実験で用いた PIN パターン

手法	入力内容	キー表示時間 [秒]
従来	23565682	常に表示
提案 (A)	D94DD29D	2
提案 (B)	D5301DD3980D	2
提案 (C)	D61DD28DD25DD3D6	2

6.4 実験結果

Fig.15 に第二視き見実験の実験結果を示す。従来手法である暗証番号 8 桁の際の視き見攻撃成功率は 50%となった。提案手法 (A) の暗証番号が 4 桁、ダミーキー 4 桁の場合の視き見攻撃成功率は 30%となった。提案手法 (B) の暗証番号が 8 桁でダミーキーが 4 桁のものと、提案手法 (C) の暗証番号が 8 桁でダミーキーが 8 桁のものの視き見攻撃成功率は 5%となった。

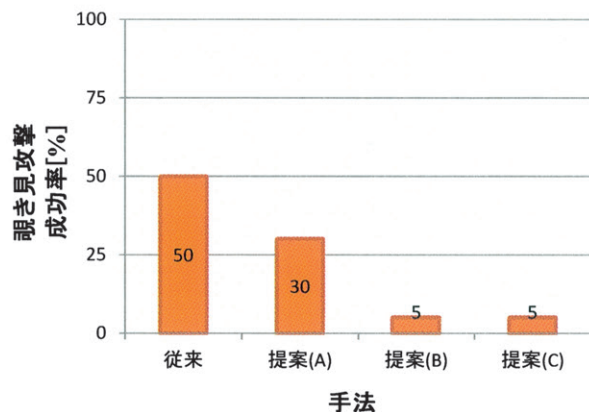


Fig.15 第二視き見実験結果

6.5 考察

従来手法での視き見攻撃成功率は 50%、提案手法 (A) の視き見攻撃成功率は 30%となったことから、従来手法において桁数を 8 桁にする場合に比べ、提案手法において桁数 4 桁にダミーキー 4 桁を加える場合の方が視き見攻撃に耐性があることがいえる。これにより、利用者が暗証番号を覚える桁数を減らし、利用者の負担を軽減することが可能になると考える。また、提案手法 (B)、提案手法 (C) においての視き見攻撃成功率は 5%となっていることから、暗証番号を 8 桁に設定し、更にダミーキーを混ぜて入力することで、ダミーキーの仕組みを知られている場合であっても視き見攻撃に大きな耐性をもつことがいえる。ダミーキーの仕掛けに加え、キー配置の変更、キー表示時間の制限の機能が加わったことによりこのような結果となったと考える。

7. まとめ

本稿では、一対比較によるインタフェース決定と、第一視き見実験、第二視き見実験における従来の認証手法と提案手法での視き見攻撃耐性の比較を行った。

第一視き見実験において、暗証番号が 4 桁の場合に、従来手法において視き見攻撃成功率が 100%となり、非常に危険であることがわかった。提案手法は従来手法に比べ、ダミーキーを含めない場合だと 25~30%、ダミーキーを含めることで 100%視き見攻撃への耐性ができた。

第二視き見実験において、従来手法での暗証番号 8 桁の際には視き見攻撃耐性が 50%なのに対し、提案手法で

の暗証番号 4 桁ダミーキー 4 桁の際、視き見攻撃耐性が 70%となっている。これは、視き見攻撃に耐性をつくることを考えた場合に、従来手法に比べ、覚えなければならぬ暗証番号が減ることになる。結果として利用者の負担を減らすことにも繋がると考える。しかし、キー表示時間中にテンキー配置を覚え、暗証番号にダミーキーを混ぜながら入力するという提案手法は現段階において、従来手法に比べると利用者側に煩わしさを感じさせることが考えられる。

暗証番号が 4 桁の場合の第一視き見実験、第二視き見実験の結果から、視き見攻撃成功率が従来手法では 100%、提案手法のダミーキーを混ぜて入力した場合ではダミーキーを知られていない場合に 0%、知られていた場合でも 30%まで軽減することができた。このことから、ダミーキーを混ぜて入力することが提案手法において、視き見攻撃耐性の向上をするうえで重要であることがいえる。

今後は、利用者にかかる負担を軽減させ利便性の向上を考慮したうえで、視き見攻撃者が暗証番号を読み取ることができない工夫をしていきたい。

参考文献

- [1] 株式会社シード・プランニング：世界のスマートフォン普及予測、
<http://www.seedplanning.co.jp/press/2012/2012072601.html>, (2012)。
- [2] 野口敦弘, 高橋雅隆, 納富一宏, 斎藤恵一：自己組織化マップを用いたタッチスクリーンによるキーストローク認証手法 ～暗証番号桁数増加によるキーストロークリズムの影響評価～, 電子情報通信学会 2011 年度 HCG シンポジウム C3-1, pp.255-260, (2011.12)。
- [3] Richard E Smith：認証技術 パスワードから公開鍵まで, pp.146-149, オーム社 (2003)。
- [4] 有賀千裕, 納富一宏, 斎藤恵一, 斎藤大輔：自己組織化マップを用いた Web の可読性の分析-文字数と改行幅による一対比較, バイオメディカル・ファジィ・システム学会 第 21 回年次大会講演論文集, pp.32-33 (2008)。
- [5] 長沢伸也, 川栄聡史：Excel でできる統計的官能評価法 順位法 一対比較法 多変量解析からコンジョイント分析まで, pp.161-163, pp.169-217, 日科技連出版社 (2008)。