

## 指紋認証実験を取り入れた情報セキュリティ教育の試行

大久保誠也<sup>†1</sup> 湯瀬裕昭<sup>†1</sup>

情報社会となった現在、学生に情報セキュリティの重要性を理解させることは非常に重要である。本研究では、生体認証や情報セキュリティの安全性を学習させることを目的として、学生にグミ指で作成した偽指紋を利用した指紋認証装置突破の実験を行わせた。この実験は、大学院「セキュリティ特論」の講義の一部として実施した。本論文では、受講生からのアンケートやインタビューを通じて得た知見をもととして、実験を取り入れた講義を行う際の留意点や実験の効果について報告する。

### Trial of Information Security Education using Experiments of Fingerprint Authentication

SEIYA OKUBO<sup>†1</sup> and HIROAKI YUZE<sup>†1</sup>

This is important tasks to teach information security. In this trial, we introduce a experiments of fingerprint authentication to teach safety of biometrics authentication and the information security. In this paper, we discuss points to keep in mind and the effect of the lecture.

#### 1. はじめに

情報化社会となった現在、身近には情報機器が増えるとともに、日常生活でそれらの機器を適切に扱う必要が出てきた。大学等でも、情報セキュリティ関係の授業が行われるようになり、セキュリティキャンプ等、啓蒙活動も積極的に行われるようになってきている<sup>5)</sup>。これらの活動の多くでは、情報を扱う上で必要となる情報倫理や、RSA 暗号等に代表される暗号化システム、安全な通信を行うためのプロトコル等を中心とした教育されていることが

多い。

また、認証システムとして、人間が固有に持っている特徴を利用する仕組みが導入されはじめており、空港や国境をはじめ、会社や工場等、広く社会に浸透してきている<sup>2)-4)</sup>。これら生体認証システムとして利用される生体的特徴としては、虹彩や掌形、静脈、網膜、筆跡、指紋など、様々なものが利用されている。このなかでも、指紋は各個人により形が異なり、かつ生涯不変であることが旧来より知られていたため、捺印のようなかたちで認証に使われてきた。そして、現代でも生体認証システムとして広く使用されており、一般のパソコンに接続できるシステムとしても販売されている。その一方で、指紋認証を行う一部のシステムは、グミで作成した疑似指（以降、グミ指と呼ぶ）でも認証してしまう事例が指摘されており、必ずしも安全な認証を行うことができない<sup>1),6)</sup>。これら生体認証の利点ならびに欠点を理解することは、システム管理者ならびに利用者にとって、非常に重要なことである。

本取り組みでは、少人数教育を実施している大学院において、生体認証や情報セキュリティの安全性を学習させることを目的として、指紋認証装置を取り入れた講義を行った。具体的には、受講生にグミ指で作成した偽指紋を利用した指紋認証装置突破の実験を行わせた。本発表では、受講生からのアンケートやインタビューを通じて得た知見を元として、講義を行う際の留意点や講義の効果について検討を行う。

#### 2. 講義の概要と本取り組みの目的

本取り組みは、静岡県立大学大学院経営情報学研究科における「情報セキュリティ特論」の一環として行った。表1に、情報セキュリティ特論の概要を示す。概要を見てわかる通り、基本的に暗号ならびにセキュアなプロトコルに関する内容を取り扱っている。しかしながら、社会における情報セキュリティは多様化しているため、指紋認証に関するトピックを取り入れた。

指紋認証を取り入れる目的は、大きく分けて次の3つである。

- (1) 生体認証が広く普及していることを認識させるとともに、体験させることで深い理解を促す。
- (2) 世間で広く利用されている情報セキュリティ技術であっても、必ずしも安全であるわけではないことを認識させる。
- (3) 情報セキュリティ技術は、攻防一体であることを認識させ、正しい運用・評価のためには攻撃方法も知っておく必要があることを認識させる。また、それらの知識を悪用してはいけないことを認識させる。

<sup>†1</sup> 静岡県立大学経営情報学部

School of Administration and Informatics, University of Shizuoka

表 1 情報セキュリティ特論概要

情報化社会を迎え、多くの情報がインターネットを介してやり取りされるようになってきている。そして、安全に情報をやり取りするためには、暗号技術は必須の技術である。本講義の目的は、暗号技術を中心として情報セキュリティに関する知識と理解を深めることである。本講義では、現代暗号の理解に必要な基本的事柄や、代表的な暗号の実装方式を取り扱う。また、実際に使用されている場面や、現在研究が行なわれている将来の暗号技術についての議論を行なうことにより、暗号を考える上での方法論を身につける。必要となる数学的知識は、適時説明を行なう。なお、講義形式ならびにディスカッションを中心として行なう。

前半は現在広く使用されている暗号技術について、後半では現在研究が行なわれている暗号技術について行なう。以下のトピックを、各 1～3 回にわたって取り扱う。

- (1) イントロダクション
- (2) 公開鍵暗号と秘密鍵暗号
- (3) 公開鍵暗号：RSA 暗号等
- (4) 秘密鍵暗号：DES 等
- (5) 電子署名：MD5 等
- (6) 量子暗号：量子鍵配送
- (7) まとめ

1 番目の目標を達成するために、本講義では座学だけではなく実験も取り入れることとした。また、2 番目ならびに 3 番目の目的を達成するために、グミによる疑似指作成を行うこととした。暗号技術を用いて同様のことを行いたい場合、高度な数学的知識が必要となる。一方、グミ指作成は、必要となる知識が少なくともよい上、機材の数を揃えるのも容易である。

大学で不正アクセス技術を伴う実験を行う場合、学生に不正アクセスのための教育をしていると見なされないように注意する必要がある。本取り組みで取り入れたグミ指による不正アクセス手法は、すでに Web 等でも広く知られている手法であるため、この問題には当たらないものと考えている。

### 3. 事前準備と実験概要

講義時間に行う関係上 1 時間半で座学による説明と演習が収まり、かつ、ノウハウを持たない受講生でもグミ指作成に成功する必要がある。そこで、事前準備としていくつかの機材で実験し、成功率の高い機材の組み合わせを選定した。また、今回の取り組みでは、実際に使用されているセキュリティ機器でも突破できる場合があることを体験させるため、一般に市販されている特徴点抽出方式の指紋認証装置を利用している。これらの結果をふまえた講義手順書を作り、講義当日に配布した。参考として A.2 に示す。

実際の講義においては、前半では座学による生体認証について説明し、後半では指紋認証実験を実施した。座学では、生体認証の一般的なことや、各種手法、各種施設での利用事

例、ならびに指紋認証はグミ指で突破される場合があることを説明した。実験では、手順書を配布し、教員も実演しながら、グミ指作成を行った。また、指紋情報は重要な個人情報でもあるので、作成した指紋と型の廃棄についての指導を行った。なお、講義は 2009 年 7 月 23 日 5 限目に行われ、4 名の大学院生が受講し、全員がグミ指による Windows へのログインに成功した。

講義中、アンケートを座学前ならびに座学後、実験後の 3 回に分けて行った（以後、それぞれを事前アンケート、中間アンケート、事後アンケートと呼ぶ）。アンケート内容ならびに結果を A.1 に示す。

### 4. アンケート結果

事前アンケート項目 1 では、他のセキュリティに関する講義の受講経験を問うた。結果が示す通り、受講生は他にセキュリティ関係の講義を受けた経験が無く、本講義（情報セキュリティ特論）がはじめての受講である学生が多くを占めている。

事前アンケート項目 2 ならびに 3 では、各種セキュリティ技術を聞いたことがあるか、ならびに利用経験を問うた。指紋認証は、多くの受講生が知っているだけではなく、体験もしている結果となった。

事前、中間、事後アンケートのそれぞれにおいて、生体認証に対する安全性の認識ならびに指紋認証に対する安全性の認識を問うた。「生体認証がどのぐらい安全そうだと思うか、10 段階評価でお答え下さい」という問いに対する回答結果を図 1 に示す。続いて、「指紋認証がどのぐらい安全そうだと思うか、10 段階評価でお答え下さい」という問いに対する回答結果を図 2 に示す。図 1 と図 2 の A から D は、4 名の受講生を表している。生体認証に関しては、個々の学生に認識の違いはあまり無く、また、講義が進んでも安全性の認識にあまり変化は見られなかった。一方、指紋認証に関しては、Web 等で情報が広まっているため、事前アンケートの時点で安全性を信用していない学生がおり、個々の認識にばらつきがあった。また、全体的な傾向としては、講義が進むにつれ、大きく信用度が落ちていることがわかる。事前アンケートと中間アンケートの間の落ち込みは、座学中にグミ指による偽指のことを講義したため、そして中間アンケートと事後アンケートの間の落ち込みは、実験のためと考えられる。この結果から、グミ指作成実験により、学生は危険性をより深く理解したものと考えられる。

事後アンケート項目 3 では、本講義で知識が深まったかを問うた。平均 4.25 と、学生自身はあまり深まったと感じていない結果となった。また、事後アンケート項目 4 で、実験が

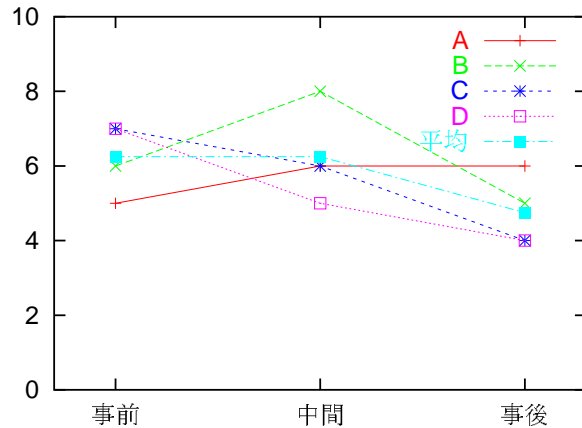


図 1 生体認証の安全性についての認識の変化

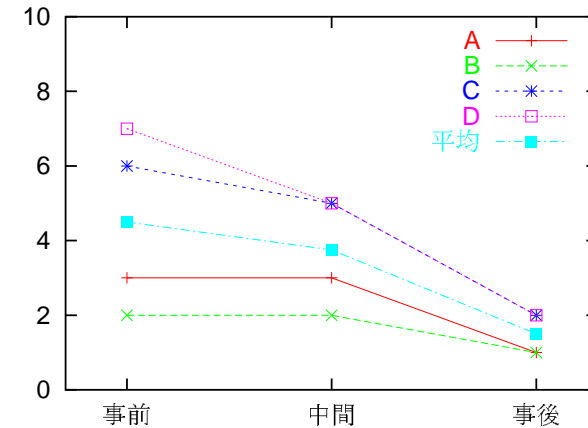


図 2 指紋認証の安全性についての認識の変化

理解を深めるのに役立つかを問うたところ、ばらつきが出てしまっている。その一方で、実験自体は興味深いと感じたらしく、今後の実験への参加意欲を問うた事後アンケート項目 5 や実験の必要性を問うた事後アンケート項目 6 では、高い得点を得ている。また、項目 6 ならびに 7 の記述項目にある、『必ずしも、安全ではないことが実感できた』等の記述より、こちらの意図通りの結果が得られているように見える。これらのことから、学生は知識が深まった実感は得ていないものの、実験自体は関心を持っており、また、ある程度の理解を深める助けになっていると考えられる。

## 5. おわりに

本取り組みでは、生体認証や情報セキュリティの安全性を学習させることを目的として、指紋認証装置を取り入れた講義を行い、アンケートを通じて有効性を検証した。また、その際に必要となった事前準備について紹介した。今回の取り組みは、少人数の大学院生に対する講義ということもあり、受講生全員が初体験にも関わらず、講義時間中に全員がグミ指の作成に成功した。アンケートでは、本取り組みは知識の定着にある程度有用であり、学生も興味は持っているが、その一方で学生自体は知識の定着の実感を持っていないこととなった。今後の課題としては、学生が知識の定着を認識できる講義の実現や、大人数の学部生に対して同様の目的を達成する講義の実施が挙げられる。

## 謝 辞

本取り組みを実施する際、電気通信大学情報通信工学科の太田和夫教授に、非常に有用なご意見を頂きました。この場を借りてお礼申し上げます。

## 参 考 文 献

- 1) 浩二山田, 弘之松本, 勉 松本: ISEC2000-45 指紋照合装置は人工指を受け入れるか, 電子情報通信学会技術研究報告. ISEC, 情報セキュリティ, Vol.100, No.213, pp. 159-166 (20000718).
- 2) 独立行政法人情報処理推進機構: 情報セキュリティ教本, 実教出版 (2009).
- 3) 独立行政法人情報処理推進機構: 情報セキュリティ読本, 実教出版 (2009).
- 4) 独立行政法人情報処理推進機構: 情報セキュリティ白書 2009, 毎日コミュニケーションズ (2009).
- 5) 杉井学, 小柏香穂理, 因幡哲男, 王躍, 市川哲彦, 永井好和, 糸長雅弘: 情報セキュリティ教育のための e ラーニング教材の開発について (情報教育研究), 教育実践総合センター研究紀要, Vol.23, pp.181-190 (20070325).
- 6) 青山奈保子: 指紋画像からの人工指作製 (その 3): デジタルカメラを用いた場合, 2003 年暗号と情報セキュリティシンポジウム (SCIS2003), Jan., pp.393-398 (2003).

## 付 録

### A.1 アンケートならびに集計結果

#### 事前アンケート

- (1) 以前、情報セキュリティに関する授業や講義を受けたことがありますか？  
ある方は、どのようなときに、どのような内容を教わったか教えてください。

ある	ない
1人	3人

- 学部の講義で、DES や公開鍵暗号について学んだ。

- (2) 以下の認証方式の中で、聞いたことがあるものに丸をつけてください。聞いたことがあるものについては、どこで聞いたか教えてください。

指紋認証	静脈認証	虹彩認証	網膜認証	筆跡認証	顔認証
4人	2人	2人	2人	0人	3人
中国 TV			アニメ		アニメ

- インターネットや TV 等で聞いたことがある。

- (3) 以下の認証方式の中で、経験したことがあるものに丸をつけてください。経験したことがあるものについては、どこで経験したか教えてください。

指紋認証	静脈認証	虹彩認証	網膜認証	筆跡認証	顔認証
3人	0人	0人	0人	0人	1人
中国 中部国際空港 携帯 パソコン					シアトルの空港

- (4) 生体認証がどのぐらい安全そうだと思うか、10段階評価でお答え下さい（0がもっとも危険で、9がもっとも安全）。

0	1	2	3	4	5	6	7	8	9	平均 6
					1人	2人	1人			

- (5) 指紋認証がどのぐらい安全そうだと思うか、10段階評価でお答え下さい（0がもっとも危険で、9がもっとも安全）。

0	1	2	3	4	5	6	7	8	9	平均 4.5
		1人	1人			1人	1人			

#### 中間アンケート

- (1) 生体認証がどのぐらい安全そうだと思うか、10段階評価でお答え下さい（0がもっとも危険で、9がもっとも安全）。

0	1	2	3	4	5	6	7	8	9	平均 6.25
					1人	2人		1人		

- (2) 指紋認証がどのぐらい安全そうだと思うか、10段階評価でお答え下さい（0がもっとも危険で、9がもっとも安全）。

0	1	2	3	4	5	6	7	8	9	平均 3.75
		1人	1人		2人					

- (3) 思ったこと、感じたことを、率直にお答え下さい。
- 指紋認証が、もし悪人が指を切って使うと危険だと思った。
  - 指紋は双子でも違うことにビックリした
  - 結構いろんなところが人とは違う部分があることにビックリした
  - 何だったら確実に安全な生体認証ができるのだろうかと思った。無理かもしれないけど。
  - 具体的にどのように危険なのかわからないけど、完璧ではない気がする。

事後アンケート

- (1) 生体認証がどのぐらい安全そうだと思うか、10段階評価でお答え下さい(0がもっとも危険で、9がもっとも安全)。

0	1	2	3	4	5	6	7	8	9
				2人	1人	1人			

平均 4.75

- (2) 指紋認証がどのぐらい安全そうだと思うか、10段階評価でお答え下さい(0がもっとも危険で、9がもっとも安全)。

0	1	2	3	4	5	6	7	8	9
	2人	2人							

平均 1.5

- (3) 本講義で、生体認証に関する知識がどのぐらい深まったかを教えてください。

0	1	2	3	4	5	6	7	8	9
			1人	2人		1人			

平均 4.25

- (4) 本日の実験は、生体認証に関する知識を深めるのにどのぐらい役に立ったかを教えてください。

0	1	2	3	4	5	6	7	8	9
			1人		2人		1人		

平均 5

- (5) 今後もこのような実験があったら参加したいと思いますか？

0	1	2	3	4	5	6	7	8	9
						3人		1人	

平均 7.5

- (6) 本日の実験で思ったこと、感じたことを、率直にお答え下さい。
- 指紋さえ採取できればグミ指は作成できるのかなと思いました。
  - PCに本当にログインできることにビックリした。

- 実際に指紋が作れてしまうことはすごいと思った。
- 実際にそこら辺をさわったときに指紋が残ってしまうので、それを利用してグミ指が作成できてしまうと、安全でなくなると感じた。

- (7) この講義に実験等は必要だと思いますか？  
理由も教えてください。

0	1	2	3	4	5	6	7	8	9
						1人	2人		1人

- 実験と通じて、本当のことがわかります。
- 例えばそれが指紋認証ならそれが必ずしも安全でないことの理解が深まると思います。
- 暗号が絶対でないとか、偽造できてしまうとか、安全ではないことが実感できた。
- 実体験することで、関心は高まる。

A.2 実験手順書

実験概要

現在、生体的特徴により個人を特定／認証する生体認証が広く使用されている。生体認証で採用される生体的特徴としては、指紋／光彩／静脈等があげられる。

指紋は各個人で異なる形状を持っており、終生形が変化しない性質を持っている。そのため、指紋により個人を認証することが古くから行われている。

本実験の目的は、実際に指紋認証を体験するとともに、グミによる偽指を作成することで、現在の指紋認証装置の利点と欠点をより深く理解することである。

実験に当たっての注意

- 『セキュリティに関する正しい知識』と『セキュリティに関する不正行為をするための知識』は紙一重／表裏一体である。本実験／授業で身につけた知識を悪用してはいけない。
- 型ならびにグミ指は、あなたの指紋という重要な情報を持っている。その扱いには十分気をつける必要がある。特別な理由がないなら、授業終了後に確実に破壊し、処分すること。
- 熱湯を使用するので火傷に注意する。

### 使用する機材について

本実験では、以下の機材を使用する（図3参照）。他に、湯沸かしポットと冷蔵庫を使用する。

- 自由樹脂  
60度以上のお湯につけることで、自由に形を変化させることができるプラスチック。冷えると固まる。  
指の型を取るのに使用する。1人15～20g程度。
- ゼラチンリーフ  
ゼラチンが固まったもの。湯煎で溶かして使用する。冷えると固まる。  
型に流し込み固めることで、グミ指となる。1人5g程度。  
ゼラチンには粉状のものもあるが、時間内に固くするため、今回はゼラチンリーフを使用する。
- 陶器の器  
自由樹脂をお湯につけて柔らかくするとき使用する。
- プラスチックコップ  
ゼラチンリーフを溶かすのに使用する。
- プラスチックの器  
プラスチックのコップを湯煎するのに使用する。
- 計量スプーン
- 割りばし
- はさみ
- 指紋認証装置ならびにパソコン  
指紋認証を行うのに使用する。

### 実験手順

- (1) 指紋の登録
  - (a) Windowsに指紋情報を登録する。今回は、人指し指を登録する。
  - (b) Windowsに指紋でログインできることを確認する。
- (2) 型の作成
  - (a) 陶器の器に沸騰したお湯を入れる。
  - (b) 自由樹脂を約20g、陶器の器に入れる（計量スプーンの10gのもの2杯ぐらい）。
  - (c) 全体がお湯につかるように、浮かんでしまっている自由樹脂を割りばしで沈

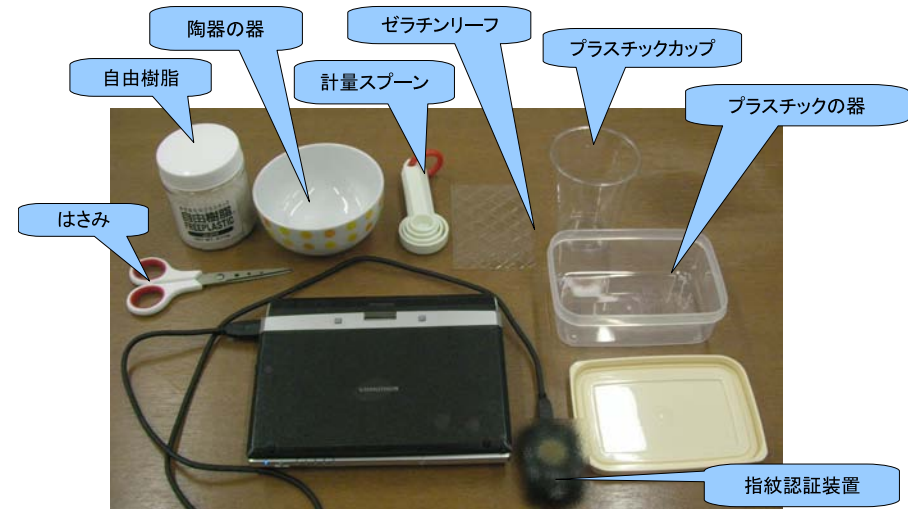


図3 使用機材

める。

- (d) 自由樹脂全体が透明になるまで待つ。
  - (e) 透明になったら、割りばしを利用して自由樹脂を一塊にし、すくいあげ、直に触れるぐらいまで冷えるのを待つ。
  - (f) 冷えたら、両手を使って自由樹脂を団子状にする。
  - (g) じっと掴んでいても火傷しないぐらいの温度になるまで待つ。
  - (h) 冷えたら、机の上に自由樹脂を置き、人指し指で上から押さえ付ける。ゼラチンを注いだときにこぼれないように、斜めから押し付ける感じで行うのがよい。押さえ付けた状態を、15分ほど維持する。徐々に固まってくる。指を動かすと型が正常に取れないので注意、図4参照。
  - (i) 指を離す。
- (3) グミ指の作成
    - (a) プラスチックコップをハサミで裁断し、高さをプラスチックの器と同じぐらいにする。
    - (b) ゼラチンリーフをハサミで細かく切り刻み、プラスチックのコップに入れる。



図 4 型のサンプル

- (c) プラスチックの器に、半分の高さまで熱湯を注ぐ.
- (d) 計量スプーンでを用いて、プラスチックの器からお湯を 5g 程度とり、プラスチックカップに注ぐ.
- (e) プラスチックカップをプラスチックの器に入れて湯煎する. 蓋をして、15 分ほど待つ.
- (f) ゼラチンリーフがネットリとしてくる (まだ、ゼラチンとお湯は分離している). 割りばしを用いて溶かす. ある程度粘度のある液体ができる.
- (g) 型に注ぐ.
- (h) 5 分程度そのままにする.
- (i) 冷蔵庫で 15 分ほど冷やす.
- (j) 固まったのを確認して、ゼラチンを型から取り外す. 取り外したものがグミ指となる. 弾力性があるが簡単には崩れないグミが望ましい.

#### 認証実験

- (1) Windows にログインできるか確認する.