2006－CE－87 (8)
2006／12／9

識別符号の秘匿強度推定におけるヒューリスティックス

福田 健
清泉女子大学 情報環境センター／司書教職課程
mailto:fkd@is.seisen-u.ac.jp

概要

パスワード（狭義の識別符号）の秘匿強度を初心者が推定する過程を探索するために3つの実験が行われた。実験1と実験2では、秘匿強度を上げる要因として、英字カテゴリに数字カテゴリが混入することの影響が過大に評価される認知的バイアスが確認された。このことから、記憶の困難度を推定することをヒューリスティックスとして用いているのではないことが推察された。実験3では、適切なヒューリスティックスが与えられた場合に、直後にはそれを自発的に用いて秘匿強度を正しく推定できるようになるが、2週間後にはその効果がなくなることが示された。

Heuristics on the estimation of the robustness of password

Takeshi FUKUDA
Information Environment Center / Librarian and Teacher Education Section,
Seisen University

Abstract

Three experiments were conducted to explore the estimating process of the robustness of password. The experiment 1 and experiment 2 showed that there is a cognitive bias that overestimates the effect of numeral within the character string to make the password stronger. It suggested that the evaluation of the difficulty of memorization is not used as heuristics. The experiment 3 showed the more adequate heuristics is used spontaneously to estimate the robustness of password, if the heuristics is pointed out. However the effect goes out two weeks later.

1 問題の所在

1.1 パスワードの秘匿強度を推定することの重要性

広範で強力な情報通信基盤に立脚する今日の社会活動においては、利用者（通信者）認証が通信の安全と有効活用を保証するために極めて重要な役割を担っている。こうした利用者認証を行う際の鍵（利用者識別認証子）としては、生体情報や物理装置が用いられることもあるが、現時点でもっとも普及している方法は識別符号[1]を鍵としたものである。

識別符号を利用者認証の鍵とする方法は、一般的には、一意性を保証するユーザIDと秘匿性を目的とするパスワードの組み合わせで実現されている。この場合、識別符号を利用した利用者認証の堅牢性は、パスワード部分の秘匿強度に依存し、それはパスワード文字列の構成により大きく変化する。

このパスワードを作成・管理する実体は、現状では各利用者自身であることが多く、した

[1] 「不正アクセス行為の禁止等に関する法律（平成十一年八月十三日法律第百二十八号）」第二条2項の定義に基づく識別符号。

がって、利用者認証の堅牢性を確保するためには、適切なパスワードを作成・管理する方法を、利用者に対して教育する必要があると思われる。しかしながら、現実に利用者に対して行われている教育処置は、不適切なパスワード文字列の典型例（生年月日・電話番号・氏名等の個人情報や実在の英単語をそのまま利用した文字列）を示すだけの場合が多い。

パスワード文字列の形式的側面（文字長・文字種など）について、利用されるシステム側で制約を課すことによって、適切なパスワードを作成するように利用者を誘導する場合があるが、この方法は、パスワード文字列が備えるべき要件とその理由との関係を説明するものではなく、また、全ての要件をシステム側で網羅的に確認することも不可能である。したがって、こうした技術的な処置は、一定程度の効果があるにせよ、効果の柔軟性や網羅性の観点から、利用者に対する教育処置にとって代わるものとはなりえない。

そもそも、適切なパスワードとは、高い秘匿強度を確保しながら利用者自身が忘却する可能性を低く抑えた文字列のことである。この両条件を満たした文字列を生成し採用するということは、利用者からみれば二律背反する制約を課せられているように思われる。それゆえ、現状では、セキュリティに関する領域知識が限られている利用者が作成するパスワードには、利用者自身に憶えやすく忘却する可能性が低いと判断された、当該利用者に由縁のある文字列（個人情報や社会関係に依存した文字列）が含まれる（秘匿強度が低い）ことが多いことが指摘されている（岡嶋 [8]）。

さらに、利用者間ではもちろんのこと、同一利用者内でも複数のパスワードが独立して運用される必要があるため、適切なパスワードを生成するための手順を一意に特定することは不可能である。すなわち、固定的な手順に無作為要因を加えたものによってパスワードの候補を生成し、それら候補について秘匿強度と自身が忘却する可能性を推定し、さらに両推定値の関係が最適に近いものを選別することで、複数の適切なパスワードを並行して利用できる。

こうした諸条件を考慮すると、利用者が適切なパスワードを作成・管理するという問題解決にとってどのような形式的教授学習やシステム条件が有効な援助となるかについては、一定の道筋をもって検討され開発が進められる必要があることがわかる。まず、利用者がパスワードの秘匿強度をどのように推定するかを調べる必要がある。その結果、推定値の傾向として、統計的誤差では説明できない何らかの認知的バイアスが認められるとすれば、単純な練習によって推定の精度を高めることは困難であろう。すなわち、そうした認知的バイアスに拮抗する教授学習やシステム側の制約などが援助・介入として必要となるだろう。さらに、そうした援助・介入によって秘匿強度が高いパスワードを生成・採用できるとしても、その条件の中で、忘却可能性がより低いパスワードを生成・採用するための援助・介入を選別する必要もあると思われる。しかしながら、現状では、利用者がパスワードの秘匿強度をどのように推定しているのかについては、全く把握されておらず、したがって、パスワードの秘匿強度を適切に推定する方法を教授することも行われていない。

1.2 パスワードの秘匿強度の定義

本稿では、「パスワードの（理論的）秘匿強度」を、次のように定義した。パスワードの秘匿強度は、パスワードを解読するアルゴリズムに依存するが、一般的には、1) 辞書項目への抵触、2) 文字遷移の規則性への抵触、3) 既知の統計的特性への抵触、4) （想定される）文字列母集合の規模（含まれる要素数）、の 4 要因にわけて考えることができる。今回は、実験操作を簡単にするために、1)〜3) については条件をほぼ固定し（各項に抵触しない文字列を前提とする）、4) についてのみ独立変数として操作した。

4) の文字列母集合の規模については、今回は、最も単純かつ一定の実績をもつ規則によってそれを定義した。具体的には、文字列を構成する文字カテゴリとして、アルファベット大文字 (A-Z)、アルファベット小文字 (a-z)、数字

(0-9) という3種類の文字カテゴリ、さらにそれらの組み合わせからなる和集合文字カテゴリを仮定した。欧文記号文字については、被験者が欧文記号文字の要素数をいくつに見積もるのか不明であったため、今回は採用しなかった。また、それら各文字カテゴリ中に含まれる文字は、全て同一の規模素性をもつと仮定した。

したがって、あるパスワード *str* の秘匿強度は、辞書項目や統計的特性に抵触しない限りで、以下の式で定義される。

(*str* が属する文字カテゴリの要素数)$^{(str\ \text{の長さ})}$

たとえば t5zq2 というパスワード文字列の場合には、それが属する文字列母集合となる文字カテゴリはアルファベット大文字と数字の和集合であり、要素数は 26+10=36 となる。したがって、その秘匿強度は、$36^5 = 60466176$ と定義される。以下では、文字列の後に [ ] をつけてその秘匿強度を指数形式で記すことがある。

1.3 パスワードの強度推定におけるヒューリスティックスの必要性

前節のように、パスワードの強度を簡略に定義したとしても、人がその計算を行うためには高い負荷（多桁の階乗計算など）と網羅的な事前知識（記号文字種類の把握など）が求められる。したがって、負荷と事前知識が制限された一般的な状況での利用者は、パスワードの強度を推定するために、正確な強度計算を行わずに、何らかのヒューリスティックスを用いていると思われる。今回の実験を計画・設計するにあたっては、こうした利用者が用いるヒューリスティックスについて、Gigerenzer ら [7] が主張する単純ヒューリスティックス (simple heuristics) の考え方を参考にした初期仮説を設定した。

意思決定研究においては、関係する情報を十分に得られないか網羅的に考慮することが不可能な状況では、限定合理性と呼ばれる、最適化よりも満足化 (satisficing) を基準とした判断がなされることが指摘されてきた。さらに、Gigerenzer らの一連の研究 [7] は、現実場面での判断に関して、上記の限定合理性という図式をより強く推し進めた単純ヒューリスティックという図式があること、および、それに基づいた判断がうまく働くことを指摘した。単純ヒューリスティックスの考え方では、人が環境構造に関する知識を活用することを前提に、情報の探索自体を相当に限定するにも関わらず、それに基づいた判断がかなりの程度うまく機能することが主張される。この考えでは、たとえば次のような情報探索と判断の過程が想定される。

Q. X市（たとえば新潟市）とY市（たとえば福島市）について、どちらの方が人口が多いか？

（両市について十分に知らない場合）

A. step 1 どちらか片方の都市の名前だけを知っている場合

→ 名前を知っている都市の方が人口が多いと判断して終わる。

A. step 2 たとえば、どちらか片方の都市が県庁所在地である（と知っている）場合

→ 県庁所在地の都市の方が人口が多いと判断して終わる。

A. step 3 たとえば、どちらか片方の都市にプロサッカーチームがある（と知っている）場合

→ プロサッカーチームがある都市が人口の方が多いと判断して終わる。

A. step N （後略）

上記の例では、判断内容に関わる環境構造を反映した差分情報が一つだけ探索・採用され、それに基づいて判断が行われ、その結果、かなり高い正解率を得ることが示されている。

この単純ヒューリスティックスの考え方と、利用者がパスワードを作成する際にその文字列を忘却する可能性を推定するという事実を考え合わせると、「パスワードの秘匿強度は、憶えやにくさ（記憶困難度）を鍵として推定される」という作業仮説を導くことができる。

これは、すなわち、パスワード文字列を憶えようとした場合の難しさをシュミレーション評価し、それを秘匿強度の推定値に代えることで、高い負荷と網羅的な前提知識を必要とせずにパスワードの秘匿強度を推定する、というヒューリスティックスを想定するものである。以下では、これを「記憶困難度に基づくヒューリスティックス」と呼ぶ。

2 研究計画

ここまでで、パスワードの秘匿強度を利用者が推定することについて、どのような過程とヒューリスティックスが用いられることでどのような結果（認知的バイアス）が生じているいるかを明らかにし、それを教授学習に生かす必要があること、しかしながら現状ではそれが行われていないこと、などを示してきた。こうした問題を踏まえ、本稿では、まず、パスワードの利用について一定の経験をもちながらも、その秘匿強度を推定する方法を教授されたことがない者を被験者として、パスワードの秘匿強度を推定させる課題を課し、その結果と実際の秘匿強度とを比較し、秘匿強度を推定する際の認知的バイアスの内容を明らかにする実験を行った（実験1・実験2）。そして、その結果から示唆される認知的バイアスに拮抗する可能性をもつヒューリスティックスを利用者に教示し、その効果を評価した（実験3）。

3 実験1

3.1 目的

複数のパスワードの秘匿強度を相互比較する際に、パスワード文字列内のどのような属性が、秘匿強度を上げる（下げる）要因として評価されるかを抽出する。

3.2 課題

パスワードとして提示された5種の文字列について、推定した秘匿強度が高い順にそれらを並べ替させる秘匿強度推定課題と、それとは別に提示された5種の文字列について、推定した記憶困難度が高い順にそれらを並べ替えさせる記憶困難度推定課題が用いられた。

提示された5種の文字列は、秘匿強度が最大のものが最小のものの10倍以内に収まり、かつ、4〜6文字長で、かつ、属する文字カテゴリが相互に異なるものである。また、同一の5種の文字列は、被験者間要因で、秘匿強度推定課題と記憶困難度推定課題の両方に用いられた。提示された5種の文字列の例を以下に示す。

u3fw	aK3b	857423	axhq	zNfS
YGZCE	3640758	kNhjW	ER9X7	HumB9
ANJW	sYQk	VD8Z	cZs5	972485

3.3 被験者

日常的にパスワードを利用し、かつ、過去8週間以内に、パスワード文字列の禁忌条件と生成方法の例（略語法）を形式的に教授され、かつ、その方法に基づいて、課題対象の文字列に準じたパスワードを自身で生成・採用した経験をもつ、四年制大学1年次生110名が採用された。

3.4 手続き

被験者は、4群に等分割され、群ごとに異なる課題項目が印刷された質問紙を同時に配布され、一斉に課題が実施された。実施時間は約10分であった。

3.5 結果

秘匿強度推定課題について、各被験者の順位評価を被験者間で算術平均して真の順位評価を推定した。その結果、

u3fw[1.6+e6]=2.4 難：易 zNFS[7.3+e6]=2.5

dw5r8[6.0+e7]=1.9 難：易 ArDKs[3.8+e8]=2.8

のように、実際の秘匿強度とは逆の順位を示す項目対として、「英大文字と英小文字」対「英大文字（または英小文字）と数字」が全6対のうち5対に観察された。すなわち、英大文字

や英小文字（全26種）よりも数字（全10種）の方が、文字列に混在した場合に秘匿強度を上げる効果が過大評価される、ということである。実際の秘匿強度とは逆の順位を示す項目対は他にも見られたが、上記以外の安定した傾向は見出せなかった。

記憶困難度推定課題について、各被験者の順位評価を被験者間で算術平均して真の順位評価を推定し、それと、秘匿強度推定課題についても同等の処理をした結果とを比較すると、一定の順位相関が確認された（Spermanの順位相関係数 r_S=0.41〜1）。しかし、秘匿強度と記憶困難度推定値の間には、秘匿強度と秘匿強度推定値との間にみられたような特定の傾向は見いだせなかった。

被験者間でのKendallの順位一致計数 W_s を算出すると、秘匿強度推定課題では $W_s = .81$〜.93、記憶困難度推定課題では $W_s = .44$〜.84であった。

3.6 考察

パスワード文字列について、秘匿強度値順に並べたものと秘匿強度の推定値順に並べたものとの差分を、秘匿強度値順に並べたものと記憶困難度の推定値順に並べたものとの差分と比較すると、両者は異なる内容であった。

また、秘匿強度の推定値順に並べたものは、記憶困難度の推定値順に並べたものに比べて、被験者間でのばらつきが小さかった。

文字列の記憶困難度の決定関数を定義することは困難であるが、一つの近似解として、「文字列を慣習的な音声ラベルを用いて、復号可能な状態に符号化（表現）した際の最小の容量」を想定することができる。この近似解に従うと、たとえば同じ4文字の文字列でも、u3fwは大文字と小文字が混在していないため「小文字でゆー・さん・えふ・だぶりゅ」と比較的小さな容量で済むのに対し、zNfSは大文字と小文字が混在しているため「小文字のぜっと・大文字のえぬ・小文字のえふ・大文字のえす」と大きな容量を必要とする。すなわち、英大文字と英小文字からなる文字列の方が、英大文字（または英小文字）と数字からなる文字列に比べて憶えにくいはずである。したがって、秘匿強度の推定に記憶困難度に基づいたヒューリスティックスが用いられているとすれば、英大文字と英小文字の和集合から構成されたパスワードの方が、英大文字（または英小文字）と数字カテゴリの和集合の場合に比べて、秘匿強度が高いと推定されるはずであるが、実際にはそのようになっていなかった。

これらのことから、本実験前に設定した初期仮説である「パスワードの秘匿強度は、憶えやにくさを鍵として推定される（記憶困難度に基づくヒューリスティックス）」という仮説は、少なくともそれ単独では説明力が低く棄却されると考えられる。

この実験1の課題では、秘匿強度と記憶困難度を推定する対象として、相互の類似性が低い文字列（文字列間で文字の重複は極力回避されていた）を5種提示した。こうした課題では、各文字列ごとに秘匿強度を推定し、次に、各文字列の推定結果を比較する、という問題解決過程が想定される。一方、現実に利用者がパスワードの秘匿強度を推定する場面では、パスワード文字列を利用者自身が生成しそれに対して秘匿強度が推定される。この場合、秘匿強度の推定結果に基づいてパスワード文字列を部分修正し、さらに、修正前のパスワード文字列と修正後のパスワード文字列とを比較しながら秘匿強度を再推定する、という手順になる。実際、福田 [1]、福田 [2] は、所定の秘匿強度を確保するパスワード文字列が作成される過程を分析した結果、文字列の一部分を変更する作業が、文字列を大幅に変更する作業に比べて、時間・回数ともに大きく上回ることを示している。

このように、比較対象となるパスワード文字列間の類似性が高い場合には、両パスワード文字列の差の部分だけが注目される。その結果、両文字列の差の部分が秘匿強度に与える影響を演繹的に計算または推論するという、実験1の課題とは異なる問題解決過程が想定される。そこで、こうした状況においても実験1の結果が再現されるかどうかを確認するため、実験2を行った。

4 実験2

4.1 目的

実験1で確認された、数字カテゴリと英字カテゴリが混在したパスワード文字列が、英大文字カテゴリと英小文字カテゴリが混在したパスワード文字列よりも、高い秘匿強度をもつと推定される傾向について、類似性が高い二つのパスワード文字列を題材とした場合でも再現できるか、確認する。

4.2 課題

課題は、文字列 *str1* 中の1文字を異なる文字カテゴリの文字に置換して文字列 *str2* にする、という文脈つきで *str1* と *str2* を提示し、置換前後での秘匿強度の高低変化を強制選択させた。文字の置換条件として以下の4種類を設定した。

英字→数字（数字添加）で秘匿強度が高くなる
　例：TjqK → Tj7K

英字→数字（数字添加）で秘匿強度が低くなる
　例：yWne → y4ne

数字→英字（数字排除）で秘匿強度が高くなる
　例：y4ne → yWne

数字→英字（数字排除）で秘匿強度が低くなる
　例：Tj7K → TjqK

各問題は、その置換方向を反転しただけのものが、被験者間要因で交換して用いられた。

4.3 被験者

被験者は、実験1と同様の条件で選ばれた別の個体110名。

4.4 手続き

被験者は4群に等分割され、群ごとに異なる課題項目が印刷された質問紙を同時に配布され、一斉に課題が実施された。実施時間は約5分であった。

4.5 結果

数字添加文字列の秘匿強度が高い問題（表1）と数字排除文字列の秘匿強度が高い問題（表2）のいずれにおいても置換方向の効果は見られなかった（2 × 2直接確率計算法）。

また、表1の課題では、理論的な正解にあたる数字添加文字列の秘匿強度を高いと推定した回答が有意に多い（2 × 1直接確率計算法: $p < .01$）が、表2の課題では、理論的な正解に当たる数字排除文字列の秘匿強度を高いと推定した回答は多くなく、有意差がない（逆方向置換）か逆方向の有意傾向すらみられた（順方向置換）。

4.6 考察

比較対象文字列間の類似性が高い場合、すなわち、文字列内の一部文字の変化に注目して秘匿強度の変化を推定する課題条件でも、実験1と同様に、英大文字や英小文字に比べて数字が文字列に混在する場合に秘匿強度を過大評価するという認知的バイアスが確認された。

仮に、記憶困難度に基づくヒューリスティックスが用いられれば、こうした認知的バイアスは見られなくなる。すなわち、記憶困難度の推定値を秘匿強度の推定値に代用することを教示し、学習者がそれを用いたとすれば、先の認知的バイアスを軽減できる可能性がある。また、これまでの各課題に用いられた文字列について、その母集合文字列の要素数を概算することが本当に困難であるかどうかについても確認する必要がある。そこで、上記の仮説と問題点を検討するために実験3を行った。

5 実験3

5.1 目的

記憶困難度に基づくヒューリスティックスがパスワードの秘匿強度を推定するために受け入れられるかどうかを確認する。また、文字列長が4〜6文字のパスワードについて、その母集合文字列の要素数を計算する（数え上げる）ことが可能かどうかを確認する。

表 1: 数字添加文字列の方が秘匿強度が高い文字列ペア

	高いと判断された文字列	
	数字添加	数字排除
順方向置換（英字→数字）	175	41
逆方向置換（数字→英字）	182	34

表 2: 数字排除文字列の方が秘匿強度が高い文字列ペア

	高いと判断された文字列	
	数字添加	数字排除
順方向置換（英字→数字）	118	95
逆方向置換（数字→英字）	101	112

5.2 課題

課題1は、与えられた2つの文字列（4組とダミー2組の6組で、文字列長が4〜6文字）について、E群用課題1では、場合の数が多いと推定した文字列を選択するように、M群用課題1では、記憶困難度が高いと推定した文字列を選択するように、それぞれ指示が記されている。

課題2は、与えられた2つの文字列（4組とダミー2組の6組で、文字列長が4〜6文字）について、パスワードとして秘匿性強度が高いと推定した文字列を選択するように、指示が記されている。課題1と課題2では与える文字列が独立である。また、課題2には、「課題1を解法として利用するように」などの指示や「課題2を解法として利用できる」などの課題1と課題2との関係を示す情報は含まれていない。

課題3は、課題2と同じ問題構造で、具体的な課題項目が課題2と異なるものになっている。

課題1と課題2に用いられた文字列のペアは2セット用意され、それらは被験者間の無作為要因として、課題1と課題2の間で交換して用いられた。

課題1〜課題3で用いられた文字列のペアは、実験1の結果から、秘匿強度と秘匿強度の推定値が逆転するもの、および、それと同じ文字列カテゴリをもつものが採用された。たとえば、

英大文字+英小文字で5桁 (UL5):
kNhjW[3.8+e8]
と
英小文字+数字で5桁 (LN5):
dw5r8[6.0+e7]

がペアとして採用された。この場合、両者の秘匿強度を推定して比較した結果は、特段の教示がなければ「UL5<LN5」となると予想されるが、課題1で教示された各ヒューリスティックスが用いられるとすれば「UL5>LN5」となると予想される。

5.3 被験者

被験者は、実験1・2と同様の条件で選ばれた別の個体117名。

5.4 手続き

被験者は、E群（場合の数に基づくヒューリスティックス群）61名とM群（記憶困難度に基づくヒューリスティックス群）56名の2群に等分割され、群ごとに異なる課題項目が印刷された質問紙を同時に配布され、一斉に課題が実施された。上記の方法で課題1と課題2が同時に行われた後、2週間後に同様の方法で課題3が行われた。課題1と課題2をあわ

せた実施時間は約5分間、課題3の実施時間は約5分間であった。

5.5 結果

課題1のE群（数え上げ値を概算する課題）について全問題を平均した正答率は.83、また、課題1のM群（記憶困難度を推定する課題）について全問題を平均した予想一致率（予想された結果と一致した反応）は.75であった。

課題2（秘匿強度を推定する課題）について全問題を平均した正答率は、E群で.69、M群で.69であった。

課題3（秘匿強度を推定する課題）については、課題1について4組中3組以上、かつ、課題2について4組中3組以上、正しい（課題1のM群では予想通りの）結果を示した被験者（E群43名、M群41名）だけを分析対象とした。その結果、課題3について全問題を平均した正答率は、E群で.33、M群で.29であった。

5.6 考察

課題1の結果から、高々6文字からなるパスワード文字列については、記憶困難度の推定だけではなく、数え上げ値を概算することについても、比較的正しく行えることが確認された。すなわち、パスワード文字列について、数え上げ値を算出することが困難であることが理由で、秘匿強度の推定値がそれと異なっているわけではないことが示唆された。

また、課題1と課題2の結果から、パスワードの秘匿強度を推定するためのヒューリスティックスとして、直前に用いた問題解決操作を自発的に利用する傾向があることが確認された。しかし、このヒューリスティックスを外部から教示した効果は2週間後にはかなり消失していることが、課題3の結果から示された。

6 今後の課題

パスワードの秘匿秘匿推定でみられた認知的バイアスの背景にあるヒューリスティックスの内容、および、秘匿強度をより適切に推定するヒューリスティックスの教示の効果が一時的なものである理由について、今後検討する必要がある。

また、今回の実験とは異なる知識・経験・認知能力をもつ利用者、たとえば、十分な教授学習を経験した者や、年少者や高齢者などを対象とした場合に、今回と同様の結果が得られるか否かについても確認する必要もあるだろう。

参考文献

[1] 福田健:問題解決過程における大域戦略と局所戦略の転換. 日本発達心理学会弟16回大発表論文集, p.290(2005).

[2] 福田健：識別符号の秘匿性強度に対する初心者の概念. 平成16年度情報処理教育研究集会講演論文集, pp.708-711(2005).

[3] 福田健：識別符号の秘匿強度推定における認知的バイアス. 日本認知科学会第23回大会発表論文集, pp.344-345(2006).

[4] 福田健：認証符号の秘匿強度の推定における方略教示の効果. 日本認知心理学会第4回大会発表論文集, p.182(2006).

[5] 福田健：識別符号の秘匿強度に対する初心者の概念. 日本心理学会第70回大会発表論文集, p.941(2006).

[6] 福田健：識別符号の秘匿強度推定における認知的バイアスと方略教示の効果. 平成17年度情報教育研究集会講演論文集, pp.296-299(2006).

[7] Gigerenzer, G, Todd, P. M., and The ABC Research Group (Eds.) : *Simple Heuristics that makes us smart,* Oxford Univ. Press(1999).

[8] 岡嶋裕史：暗証番号はなぜ4桁なのか？, 光文社 (2005).