仙台大学紀要
2005, Vol.36, No.2, pp.20-31

情報通信ネットワークにおけるセキュリティ問題

～利用者の認識不足とパスワード管理～

内　野　秀　哲

Actual Situation of Information Technology Security Problem
Caused by User's Lack of Understanding and Control of Users' Password.

UCHINO Hidetaka

The security function of an information network is effectively established by sharing the role of users and system administrators. Therefore, it is necessary for users to have the right understanding to security. This study investigated about the state of the understanding to this security and caught the problem, and simultaneously reported that the school for improving the understanding for the security is significant.

Key words：password, identification, inter net, IT-security,

1. 情報ネットワークとパスワード

1-1. 利用者の認識不足とパスワード管理の問題

インターネットは、情報化社会に代表される大規模な情報ネットワークサービスの基幹として普及し、昨今では企業の広報や通信販売などの実社会の活動が、インターネットのホームページサービスやオンラインショッピングのように、距離や時間などの制約の少ない効率的な情報ネットワークの仮想空間の中で実現され、進化を続けている。

これまでのこうした進化を顧みれば、その運用者や利用者の利便性の向上を目指したものであり、その利用者と利用機会の拡大が主な目的の背景にあると考えても間違いはない。しかし、利便性の向上とともに進化すべき安全性については未だ不十分と言わざるを得ないのが現状である。特に情報ネットワークのセキュリティ問題については、警察庁による国家公安委員会告示第９号（平成９年９月18日）の「情報システム安全対策指針」など[1~10]のように、これまでも多くの研究者によって報告されてきたが、利便性の向上とともに問題が深刻化するなど、未だに終息しないものが数多くある。

情報ネットワークのセキュリティ問題についての国際的な取り組みを見ると、主に４つの視点による取り組みが活発に行われていることが窺える。

まず第１に包括的な取り組みとして、ＣＣ(Common Criteria)を中心とした取り組みがあげられる。これは、国際的協調を目指したセキュリティ評価基準を基にした、最も大規模な情報機器のセキュリティ対策への取り組み[1]である。

第２に暗号化技術開発への取り組みがあげられる。これは通信内容の守秘を強化することに主な目的をおき、転送される情報を暗号化する技術の開発や、整備を行うことへの取り組み[2]であるといえる。

第３に、法制化への取り組み[3]があげられる。不正アクセス禁止法など、情報ネットワーク先進国ではすでに整備されている例も数多くある。第４に、情報リテラシー、情報倫理への取り組み[4]があげられる。これは情報ネットワークの持つ社会性を重視し、その社会的規範の認識修得を利用者に啓蒙する取り組みである。

国内では、こうした国際的な動きを捉えて、前述の第1、第２については旧通商産業省をはじめとした関係各所で取り組みが行われており、また、第３の法制化についても不正アクセス行為の禁止等に関する法律（不正アクセス禁止法）が平成13年２月13日より施行された。第４の取り組みについても同様に、情報倫理規定や情報ネットワーク運用のガイドラインなどが検討され、情報セキュリティ問題の不安要素が多くある大学関連においても、私立大学情報処理協会から安全な利用・運用のためのガイドライン[5]などが公開されている。その他にも有限責任中間法人JPCERTコーディネーションセンター（JPCERT/CC）や独立行政法人情報処理推進機構(IPA)などが活動の拠点となり、利用者や管理者に対しての情報提供や収集、セキュリティ対策に関する啓蒙活動、法整備や政策にむけての検討などを行っている。また、所轄当局である警察庁や旧郵政省などでは、不正アクセス禁止法や、電気通信事業法の改定等によって管理体制の整備などを進めているが、既に法整備が進んでいる情報化先進国であるアメリカやカナダ、ＥＵ諸国などの例を見ても、決定的な問題解決の手段となりにくいことが容易に想像できる。今後も情報処理の技術は進歩し、それに伴って問題性も深刻化[6]するであろうし、管理者や利用者それぞれがセキュリティ対策を厳重に行うことが、最も必要であることに変わりはない。

利用者の講ずべきセキュリティ対策[7][8]のうち、最も重要なものにパスワード管理がある。このパスワード管理によるセキュリティ対策については未だに不十分であり、不正アクセスによる被害が後を絶たない。こうした利用者のパスワード管理の不備の原因として、３つの要因を考えている。

第１に、現在の情報ネットワークが標準的に有しているセキュリティ機能クラスが、全ての利用国の文化に適応しているものではないという点があげられる。情報機器の発祥の地であるアメリカは、周知の通り契約社会であり、日本の社会文化と異なった性質を持っている。また、個人情報の取り扱いについても同じ事が言えよう。情報ネットワークの中核であるインターネットはそのアメリカで発祥し、その文化の下で基盤が形成された。また、現在の情報機器それ自体の基盤もアメリカの文化の下で形成されたもの[9]である。身近な例で例えれば、認証と識別に「漢字」が使えない現状が、もっとも顕著な例であろう。こうした文化の違いによるセキュリティ機能の非適応性が要因の一つと考えられる。

第２に、「法規制の実効性の問題」が考えられる。ハッカーやクラッカーなどの高度な技術を持つ者であれば、不正行為を隠滅する事も可能であろうし、また証拠となる物証も電気特性を持つものであるが故に完全に消滅させることも不可能ではない。ましてハッキングされた第三者のパスワードによる不正行為であれば、不正行為者の特定も困難である。これらの事だけで考えても、不正アクセスを法制で抑制することには限界があり、極めて困難であると考えられる。不正アクセス禁止法が制度化されている情報先進国においても、単に不正アクセスを禁止しているにとどまる例が多くある。いわば表面上で形式化し、実効性に欠ける法制では、利用者に強い社会的責任感を与えるに至らないと考えられる。

第３に、「認識不足」が考えられる。この認識不足は前述の２つの要因をも包括するが、ここでは情報倫理や情報リテラシーの観点からの「認識不足」として捉えることとする。

情報リテラシー、情報倫理への取り組みについ

ては、情報ネットワークの持つ社会性を重視し、その社会的規範の認識修得を利用者に啓蒙する取り組みが主になっていると前述したが、情報セキュリティ問題の不安要素が多くある大学関連においては特に、文部科学省や関連機関で公開しているガイドラインなどに基づき、積極的に取り組んでいく必要がある。利用者のパスワード管理について、十分な認識を与える機会を持つとすれば、こうした取り組み[10]の中で正しく啓蒙活動を進めていくことが一番現実的であろう。

情報ネットワーク利用者のパスワード管理の問題については、上述の通り３つの要因を考えているが、本稿についてはこの中から第３の要因のみを取り上げ、実態を調査・分析することによりこの要因の問題性を報告する。特に、ユーザーの講ずるパスワード管理の実態報告については、今後の情報リテラシー、情報処理倫理教育などの分野において、極めて有力な資料となる可能性があると考えている。

1-2. パスワードの評価基準

利用者が講ずべきセキュリティ対策のうち、パスワードの管理はもっとも身近でかつ重要な対策[1][2][3]であるといえる。従って、このパスワードの内容を評価することは、セキュリティに対する認識を探る上で最も効果的な指標となる。そこで、本節では、パスワードの安全性について概説し、その評価基準となりうる項目をあげる。

1) パスワードの安全性

パスワードの安全性は、そのパスワードが解析されることの困難性で判断することができる。解析されにくいパスワードの安全性は高く、解析されやすいパスワードの安全性は低いと言える。このことを解析困難性、発見困難性などの言葉で表す例[6][7][8]が多いが、ここで重要な点は、解析される可能性ではなく、どの程度解析が困難であるかを指している点である。つまり、好条件を揃えた強固なパスワードであっても解析が可能である事実をふまえ、解析されるまでに必要になるであろう探索回数の多さ（所要時間）を困難性で表している。この探索回数は、パスワードに用いる文字種と文字数によって大きく異なり、パスワードとして選択しうる組み合わせの数に等しい。また、ここでとりあげた探索方法はBrute Force Attack（全件探索）とよばれる手法によるもので、他にも探索対象を単語に絞り込んで行うDictionary Attack（辞書探索）とよばれる手法もある。

一般に利用されているキーボードでは、パスワードに設定できる文字キーが96種類ある。この96種の文字キーを８文字以内で組み合わせると、全部で7,289,831,534,994,530通りのパスワードになる。この計算については次の式で表すことができ、文字数をｎとした。

計算式

パスワードの組み合わせ数

$$= 96^{n}+96^{(n-1)}+96^{(n-2)}\cdots 96^{1}$$

$$=\sum_{i=1}^{n-1} 96^{(n-1)}$$

このように、解析困難性は、パスワードの組み合わせの多さ、つまりは文字種と文字数の多さで測ることが可能であるが、この条件の他に解析困難性を低下させる要因が存在する。利用者への指導書や、ガイドライン、セキュリティ対策基準などで取り上げている「悪いパスワード」の要素がこれにあたる。次項にその要素を評価の基準として取り上げ、解説を加えることにする。

2) 悪いパスワードと評価の基準について

前項で述べてきた内容を踏まえて、パスワードの内容を評価するための基準として以下の項目を取り上げることとする。

・少ない文字数

前項で述べたとおり、少ない文字数は、設定できるパスワードの組み合わせが限定されるため、十分な解析困難性を確保できない。

・少ない文字種

利用できる文字キー(96)の内訳は、数字(10)、記号(34)、英字(52)であるが、パスワードに単一の文字種を用いた場合、設定できる組み合わせが極端に限定される。最も数の少ない数字を例にあげれば、8文字以内でも111,111,110通りの組み合わせに限られることになる。なお、参考までに各文字種の内容は次の通りである。

数字(10)　1 2 3 4 5 6 7 8 9 0
記号(34)　␣ - ^ ¥ ! " # $ % & ' ( ) = ~ | @ [` { ; :] + * } , . / ¥ < > ? _
英字(52)　A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
a b c d e f g h i j k l m n o p q r s t u v w x y z

・単語を用いている

単語を用いたパスワードは、本人が覚えやすいばかりではなく、周囲の人からも推測されやすい。パスワード入力の際に入力キーを覗かれたり、パスワードが書かれたメモなどを見られた場合、それが一部分であったとしても解析の大きな手がかりとなる。また、ハッキングには、辞書アタックと呼ばれる解析ツールを用いた手法もあり、単語を用いたパスワードは極めて高い危険性にさらされることになる。

・個人情報や、身辺の情報を用いている

当該利用者の周囲に存在する者であれば、その利用者の氏名や年齢、住所などの個人情報、所持している車や趣味趣向などの身辺情報などは知りうるところである。したがって、後述する安易なパスワードの部類にも含まれると考えられる。また、ファクシミリの送付状や報告書、電子メールなどがデータファイルとしてコンピュータに蓄積されていれば、その中から利用者の個人情報や身辺の情報を得ることが可能である。したがって、個人情報や身辺の情報を用いることは、周囲に存在する既知の者に限らず、未知の第三者に対しても無防備な行為となり得る。

・他人が予測しやすい、あるいは覚えやすいなどの安易な設定になっている

単語の利用や個人情報なども含め、一瞬見ただけでも覚えられるような規則性のあるパスワードは、利用者本人にとっては忘れにくい便利なパスワードであろう。しかし、同時に他者に対しては、パスワード入力の際の指の動きなどから予測されやすい、あるいは覚られやすいなどの無防備なパスワードとなる。タッチパネルに残った指紋や、隠しカメラで撮影した映像からパスワードが解析されてしまうケースも多くある。

したがって、単一の文字種、少ない文字数のパスワードも同様に安易なパスワードといえる。つまり、他人が予測しやすい、あるいは覚えやすい安易なパスワードは、前述した悪いパスワードの各要素も含まれるが、単純な数字の語呂合わせや連番など、その他にも安易なパスワードになるものも考えられる。

2. パスワード設定に見られる傾向の調査

2-1. 調査の目的と方法について

本調査は情報ネットワークの利用者が設定するパスワード内容を分析することにより、セキュリティに対する認識の実態を探ることを目的としている。調査内容については、仙台大学の情報ネットワークセキュリティ講習を受講する大学生113名を対象に、その講習の直前、直後に登録を希望する利用者パスワードの内容を回答用紙に記入させた。また、講習直後の回答の際には、直前に回答したパスワード内容の自己評価についても評価基準の項目ごとに記入さ

せている。調査対象113名のうち、パスワードに設定できない文字を回答した者や、無回答者について除外し、講習前の有効回答数を104名、講習後の有効回答を109名として処理を行っている。この調査の対象に仙台大学の大学生を設定した理由については、本調査の実施によってセキュリティ崩壊を招く恐れがあることから、追跡的対策を講じる手段を確保する必要があることなどを含め、調査実施の便宜という実際的な理由があげられる。また、アンケートの回答用紙を回答欄のみのレイアウトとし、設問を全て口頭で伝えるなどによって、情報保護の対策を行ったことや、実際には、乱数によるOne Time Password（初回利用限定）を利用者に発行したことなどの対策も講じている。

調査によって得られた情報は、「悪いパスワード」の評価基準となる、文字数、文字種の組み合わせ数、単語利用の有無、個人情報の有無、安易な設定などによって分析し、整理を行った。また、単語利用の有無、個人情報の有無、安易な設定については、自己評価の回答から分析し、整理を行った。

なお、この調査は、仙台大学の情報ネットワーク利用者を対象に、平成10年度から現在に至るまで継続して行っており、本稿ではその当初年度である平成10年度の実施分を対象としている。

2-2. セキュリティ講習前のパスワード設定に見られる傾向

前節で述べた「悪いパスワード」の評価基準のうち、単語利用の有無については文字種が英字に限定されるため、文字種の組み合わせと文字数の2つの基準によるものと、単語の利用の有無によるものとのを区別して調査結果の整理を行った。

1）文字種の組み合わせと文字数について

パスワードに利用できる文字種は半角表記可能なANK文字で、「0」～「9」の数字と、「A」～「Z」、「a」～「z」の英字、「！」～「”」の記号の3つの文字種類がある。パスワードに用いる文字種について、一般的には組み合わせが多い方が安全とされ、逆に単一の文字種による設定は危険であるとされている。また、文字種ごとの安全性については各文字種の内容数に比例するので、英字(52種)が最も高いことになり、次いで記号(34種)、数字(10種)の順となる。この内容数は利用環境によっても異なるが、それぞれの最大数を取り上げた。

パスワードの文字数については、推奨値を8文字以上とする例[2][5][6][7]が多いこと、キャッシュカードなどのパスワードに4文字が用いられていることをふまえて、「8文字以上」、「5～7文字」、「4文字以下」の3つに区分した。これらの組み合わせを基に、調査結果の報告を行っていくこととする。

パスワード設定に含まれている文字種については表－1－1に示したとおり、セキュリティ講習の前では、数字を設定した者が78名(75.0%)と最も多く、次いで英字を設定した者の52名(50.0%)、記号を設定した者の23名(22.1%)の順である。なお、これらの該当数は重複分を含めた数字である。

パスワード設定に用いられた文字数の内訳については表－1－2に示したとおり、8文字以上

表－1－1 設定に含まれる文字種（重複分を含む）

	講習前（n=104）	
	該当数	%
数 字	78	75.0%
記 号	23	22.1%
英 字	52	50.0%

表－1－2 各文字数別の設定

	講 習 前	
	該当数	%
8文字以上	43	41.3%
5～7文字	29	27.9%
4文字以下	32	30.8%
合 計	104	100.0%

が43名(41.30%)と最も多く、次いで4文字以下の32名(30.8%)、5～7文字の29名(27.9%)の順である。

パスワード設定に3種類の文字種を用いた者の内訳については表－2に示したとおりである。良いパスワードの推奨条件として、3種類全ての文字種を8文字以上の文字数を用いて設定をすることがあげられるが、この条件を満たしている者が7名(6.7%)程度しか見られていない。また、3種類全ての文字種を用いている者についても1名が8文字未満の悪いパスワードの条件に該当した。

パスワード設定に2種類の文字種を用いた者の内訳については表－3－1に示したとおり、8文字以上の設定が21名(20.2%)と最も多く、次いで5～7文字の設定が8名(7.7%)、4文字以下の設定が4名(3.8%)の順となっている。組み合わされた2種類の文字種について、それぞれの内訳は表－3－2から表－3－4に示したとおり、数字＋英字が20名(19.2%)、記号＋英字が12名(11.5%)、数字＋記号が1名(1.0%)の順となっている。

パスワード設定に1種類の文字種のみを用いた者の内訳については表－4－1に示したとおりである。良いパスワードの推奨条件が3種類全ての文字種を8文字以上の文字数を用いて設定することであるが、このときと同等以上の解

表－2　3種類の文字種による設定

	講　習　前	
	該当数	%
8文字以上	7	6.7%
5～7文字	1	1.0%
4文字以下	0	0.0%
合　計	8	7.7%

表－3－1　2種類の文字種による設定

	講　習　前	
	該当数	%
8文字以上	21	20.2%
5～7文字	8	7.7%
4文字以下	4	3.8%
合　計	33	31.7%

表－3－2　数字＋記号による設定

	講　習　前	
	該当数	%
8文字以上	1	1.0%
5～7文字	0	0.0%
4文字以下	0	0.0%
合　計	1	1.0%

表－3－3　数字＋英字による設定

	講　習　前	
	該当数	%
8文字以上	12	11.5%
5～7文字	6	5.8%
4文字以下	2	1.9%
合　計	20	19.2%

表－3－4　記号＋英字による設定

	講　習　前	
	該当数	%
8文字以上	8	7.7%
5～7文字	2	1.9%
4文字以下	2	1.9%
合　計	12	11.5%

表－4－1　1種類の文字種による設定

	講　習　前	
	該当数	%
8文字以上	15	14.4%
5～7文字	20	19.2%
4文字以下	28	26.9%
合　計	63	60.6%

表－4－2　数字のみによる設定

	講　習　前	
	該当数	%
8文字以上	11	10.6%
5～7文字	13	12.5%
4文字以下	25	24.0%
合　計	49	47.1%

析困難性を単一の文字種で求めた場合、英字のみ（単語利用の危険性を考慮しない）で10文字以上、記号のみで11文字以上、数字のみでは16文字以上が必要となる。このことから考えれば、悪いパスワードは単一の文字種で少ない文字数ということになる。この悪い条件に当たる4文字以下の設定が28名(26.9%)、5～7文字の設定が20名(19.2%)と非常に多く存在している。この2つのケースを加算すると、実に48名(46.2%)にもなり、ほぼ2.2名に1名の割合で悪い条件に当たるパスワードを設定していることになる。また、8文字以上の設定が15名(14.4%)存在するが、悪い条件に当たっていることに違いはなく、これも全体から見れば少なくない数字である。

用いられた文字種については表－4－2から表－4－4に示したとおり、数字が49名(47.1%)と最も多く、次いで英字が12名(11.5%)、記号が1名(1.0%)の順となっている。また、4文字以下の設定で最も多かったのが数字による設定の25名(24.0%)であった。

2) 単語利用の有無について

パスワードハッキングに、辞書アタックという手段があるが、これは辞書と呼ばれる単語が記録されたデータベースとハッキングツールを用いてパスワードハッキングを行うものであり、そのデータベースには一般の辞書に掲載されているものから代表的な人名、流行語などの多くの単語が登録され、また更新されている。こうしたツールによる不正な認証が、1秒に1回試行されたと仮定すると、10万語の辞書でも約28時間弱で完了することになる。また、単語などの覚えやすい文字は、パスワード入力の際に一瞬見られるなどしても容易に推測されてしまう可能性がある。一般に良いパスワードの条件として単語を設定しないことを推奨している。本調査では単語の利用の有無を設問によって回答させた。その結果は表－5に表したとおり、こうした単語をパスワードに用いた者が9名(8.7%)存在した。仮に本調査の対象者全員に対してこの辞書アタックが行われた場合、確実に9名はハッキングの被害に遭うことになる。

3) 自己評価に見られたパスワード設定の反省点について

セキュリティ講習会を受講した後、それぞれが事前に設定したパスワードに対する自己評価を記入させた。この中より文字種、文字数、単語の有無、個人情報の有無などを反省点としてあげているものを表－6に表した。最も多く見

表－4－3 記号のみによる設定

	講習前	
	該当数	%
8文字以上	0	0.0%
5～7文字	1	1.0%
4文字以下	1	1.0%
合 計	2	1.9%

表－4－4 英字のみによる設定

	講習前	
	該当数	%
8文字以上	4	3.8%
5～7文字	6	5.8%
4文字以下	2	1.9%
合 計	12	11.5%

表－5 単語を用いた設定

講習前	
該当数	%
9	8.7%

表－6 自己反省点（重複あり）

	該当数	%
文字種について	10	9.6%
文字数について	38	36.5%
単語を利用	9	8.7%
個人情報を利用	58	55.8%
安易であった	54	51.4%

られたのが個人情報を用いたという反省点をあげた58名(55.8%)であった。次いで覚えやすい簡単なパスワードであったという54名(51.4%)、文字数について38名(36.5%)、文字種について10名(9.8%)、単語の利用について5名(4.8%)の順である。

4) 調査・分析によって得られたその他の結果について

本調査の分析にあたり、数名の対象者に聴き取りを行い、調査・分析の参考としたが、その中でポケベルのメッセージコードをパスワードに用いた例が存在している。

ポケベルでは相手へのメッセージを数値に変換し、電話機のプッシュ信号で送信するが、この際に用いられるのがポケベルのメッセージコードである。このコードを基にして、調査結果を分析したところ、明らかにメッセージコードを用いた例として講習前、講習後ともに4名存在している。メッセージコードを用いた場合、全て数字で表記され、かつ文字数は偶数の桁数となる。また、母音となる1、2、3、4、5の出現が多くなることが予測できるので、規則性が発生することが考えられる。本調査で確定できた例は少ないが、数字の組み合わせの中に潜在している可能性は高いと考えている。これらの現象が見られたのは、本調査の対象となった大学生の中にポケベルが普及した世代が含まれているからであるが、その他世代にも、あるいは今後ともこうした時代・世代的背景に影響を受けた事例が現れることは十分に考えられる。しかも他者から容易に推測し得るという意味では注意すべきパスワード情報であることに違いはない。

3. セキュリティの認識・意識改善による効果の分析

パスワードの管理は、利用者が講ずべきセキュリティ対策の最も必要不可欠な要素であることは周知のことであるし、これまでも随所で述べてきたところである。また大学等においては、情報セキュリティ問題の不安要素が多くある[5][10]ことも事実であり、調査の対象となった仙台大学の大学生についてもＩＤに学籍番号を用いるなど、セキュリティ不安の要素があることは否めない。従って、利用者の利便性の確保のために、利用者のパスワード管理等のセキュリティに対する認識に、より一層、依存せざるを得ない状況にある。

セキュリティ講習は、平成10年11月4日、ＯＡ関連商社であるＮ事務機のインストラクタＳ氏により、同学内のマルチメディア講義室にて午後4時30分から行われた。内容はセキュリティ問題の事例について解説を行い、パスワード管理の要件について一通りの説明を行うものであった。コンピュータによる教材提示によって進行し、およそ35分ほどで終了した。本研究は、この講習内容の分析を行うものではないので、講習内容の評価については言及しないが、パスワード管理に関する必要な情報を伝えるには十分な内容であったと考えている。本考察については、パスワード設定の要件について、一通りの情報伝達があったことを前提に述べていく。

セキュリティ講習前のパスワード管理の状況については、次の特徴があきらかになっている。全体的に見ても数字の利用は78名(75.0%)と多く、数字のみを用いたものが49名(47.1%)と最も多い。その中でも25名(24.0%)が4文字以下の設定になっている。数字を用いた設定が極端に多いことが講習前の大きな特徴としてあげられる。約1.3人に1人の割合で数字を用い、2.1人に1人の割合で数字だけを用いている。また、約4人に1人の割合で4文字以下の極端に悪いパスワードを設定していることになる。ここで解析困難性を基にこのケースを考えてみると、4文字以下の数字であればそのパスワードの組合せは11,110通りであり、仮にハッキングツール等を用いて1秒に1回解析が

行われたとすれば、3時間程度で完了することになる。

4文字以下の数字を用いるパスワードといえば、キャッシュカードの類の暗証番号が連想されるが、こうした実生活からくる慣習が、この現象を引き起こす要因の一つと考えられる。また、前章第2節でポケットベルのメッセージコードの可能性を提示したが、潜在的な要因としてこの暗証番号と同様に考えることができる。確かに、実生活においてこの数字4文字の暗証番号に支えられているところは大きいであろうが、キャッシュディスペンサのように解放され、人目に付くスペースで利用されるものと、密室で利用されることが多い情報端末とでは極端にその状況は異なる。また、キャッシュカードの場合は、あくまでも暗証番号であり、言い換えるならばパスナンバーである。予め数字に限定されている暗証番号と、96種の文字キーがある情報端末のパスワードではあきらかに安全性に違いがある。インターネット上でも、実社会と同様の経済活動が繰り広げられるようになってきた現在、インターネットの利用は、キャッ

表－7－1　パスワード設定の講習の前後差

		文字種内訳				文字数内訳			単語の利用	
		該当数	%			該当数	%		該当数	%
数字	前	78	75.0%	8以上	前	43	41.3%	前	9	8.7%
	後	74	67.9%		後	90	82.6%	後	17	15.6%
	差	-4	-7.1%		差	47	41.2%	差	8	6.9%
記号	前	23	22.1%	5～7	前	29	27.9%			
	後	27	24.8%		後	15	13.8%			
	差	4	2.7%		差	-14	-14.1%			
英字	前	52	50.0%	4以下	前	32	30.8%			
	後	87	79.8%		後	4	3.7%			
	差	35	29.8%		差	-28	-27.1%			
無効	前	9	8.7%	合計	前	104	100.0%			
	後	4	3.7%		後	109	100.0%			
	差	0	-5.0%		差	5	0%			

表－7－2　組合せた文字種の差

		1　種		2　種		3　種	
		該当数	%	該当数	%	該当数	%
8以上	前	15	14.4%	21	20.2%	7	6.7%
	後	30	27.5%	47	43.1%	13	11.9%
	差	15	13.1%	26	22.9%	6	5.2%
5～7	前	20	19.2%	8	7.7%	1	1.0%
	後	9	8.3%	6	5.5%	0	0.0%
	差	-11	11.0%	-2	-2.2%	-1	-1.0%
4以下	前	28	26.9%	4	3.8%	0	0.0%
	後	4	3.7%	0	0.0%	0	0.0%
	差	-24	-23.3%	-4	-3.8%	0	0.0%
合計	前	63	60.6%	33	31.7%	8	7.7%
	後	43	39.4%	53	48.6%	13	11.9%
	差	-20	-21.1%	20	16.9%	5	4.2%

シュカードの利用以上の危機管理を持たなければならない。その上、キャッシュカードやクレジットカードでは、不正利用による被害を救済する保険等もあるが、不正アクセスによって受ける個人の権利への侵害については、救済する保険も制度もまだ十分に整備されていない。こうした認識不足については早期に解消する必要があるだろう。

セキュリティ講習後については回答数の推移を中心に特徴を考察した。講習前後の差については表－７－１～４に示す。

講習前については数字を用いた設定が78名(75.0%)と最も多かったが、講習後は英字の87名(79.8%)が最も多く、講習前52名(50.0%)との差は35名(29.8%)である。数字についての講習後は74名(67.9%)で、その差は-4(-7.1%)であり、英字の増加から見れば大きな差はない。記号についても27名(24.8%)で、その差は4(2.7%)であり、大きな差はなかった。文字数については８文字以上が90名(82.6%)に増加しており、その差は47名(41.2%)と最も大きい。逆に５～７文字の設定

表－７－３　単一の文字種を用いた設定の前後差

		数字のみ		記号のみ		英字のみ	
		該当数	%	該当数	%	該当数	%
８以上	前	11	10.6%	0	0.0%	4	3.8%
	後	15	13.8%	0	0.0%	15	13.8%
	差	4	3.2%	0	0.0%	11	9.9%
５～７	前	13	12.5%	1	1.0%	6	5.8%
	後	5	4.6%	1	0.9%	3	2.8%
	差	-8	-7.9%	0	0.0%	-3	-3.0%
４以下	前	25	24.0%	1	1.0%	2	1.9%
	後	1	0.9%	0	0.0%	3	2.8%
	差	-24	-23.1%	-1	-1.0%	1	0.8%
合計	前	49	47.1%	2	1.9%	12	11.5%
	後	21	19.3%	1	0.9%	21	19.3%
	差	-28	-27.8%	-1	-1.0%	9	7.7%

表－７－４　２種の文字種を用いた設定の前後差

		数字＋記号		数字＋英字		記号＋英字	
		該当数	%	該当数	%	該当数	%
８以上	前	1	1.0%	12	11.5%	8	7.7%
	後	0	0.0%	35	32.1%	12	11.0%
	差	-1	-1.0%	23	20.6%	4	3.3%
５～７	前	0	0.0%	6	5.8%	2	1.9%
	後	0	0.0%	5	4.6%	1	0.9%
	差	0	0.0%	-1	-1.2%	-1	-1.0%
４以下	前	0	0.0%	2	1.9%	2	1.9%
	後	0	0.0%	0	0.0%	0	0.0%
	差	0	0.0%	-2	-1.9%	-2	-1.9%
合計	前	1	1.0%	20	19.2%	12	11.5%
	後	0	0.0%	40	36.7%	13	11.9%
	差	-1	-1.0%	20	17.5%	1	0.4%

が15名(13.8%)、4文字以下が4名(3.7%)と、共に減少している。特に4文字以下の差は-28名(-27.1%)であり、その差は大きい。同様に、表－7－2～4の表した内訳を見ると、数字と英字の組合せで8文字以上の設定が35名(32.1%)で、その差が23名(20.6%)と増えているのに対し、4文字以下の数字の設定が1名(0.9%)にまで減少し、その差も-24名(-23.1%)と大きい。

講習後の大きな特徴としては、第1にパスワードの文字数が増加したことと、英字を用いた設定が増えたことがあげられる。第2は数字の設定が多いという講習前の特徴を踏襲しながらも、4文字以下の数字の設定が減少していることであり、いわば、最も悪いパスワードの部類に入る例がほとんど見られなくなったことである。これを講習による効果として考えれば、パスワードの要件に関する情報を提供することにより、安易に悪いパスワードを設定する例が減少するということになる。

4. まとめ

本調査の結果からはセキュリティ講習の受講による効果が顕著にみられており、あらためてこのような講習の機会と、その質の向上を目指すことの必要性が窺えた。また、その効果については今後、講習内容との関わりなどを含めて調査を続ける予定である。従来から情報セキュリティ問題の不安要素が多くあるといわれる大学などでは、利用者のＩＤが学籍番号などで設定されている例が多く、利用者とＩＤを特定しやすい環境にある。また、利用者登録などのパスワード管理についても、やむを得ず学籍番号等をパスワードとして用いている例もある。教育機関では、こうした作業が一時期に集中するため、このようなケースがみられても致し方がないのだが、電気通信事業法の改定によって否応なく改善を求められる可能性がある。また、利用者の講ずるセキュリティ対策は、利用者個人の権利を保護する目的だけではなく、他者の保護あるいは社会秩序の維持をする義務にあたるという認識を今後はより強く持たなければならない。とりわけ、ガイドラインや倫理規定などは、整備が急がれるところであろう。

利便性と安全性の両立は、情報通信ネットワークサービスを運用する上では不可欠なことであり、また常に利用者と管理者（あるいは運営者）との対峙の中で実現せざるを得ない。情報セキュリティを効果的に確立させるためには、利用者とシステム管理者のセキュリティの対策義務の役割分担を明確にする必要があると考えられる。技術革新や法制化によるセキュリティの確立も大切な事ではあるが、情報ネットワーク社会も実際の社会生活同様に社会的規範をもち、全ての利用者がお互いに役割を遂行することが最も現実的で有効な手段ではないだろうか。

参考文献

[1] (C) 電子協1997年コンピュータセキュリティ委員会：コンピュータセキュリティ基本要件･機能編【第2版】，日本電子工業振興協会，1997

[2] 佐々木良一：インターネットセキュリティ入門，岩波新書，1999

[3] 堀部政男：プライバシーと高度情報化社会，岩波新書，1994

[4] 越智貢，土屋俊，水谷雅彦：「情報倫理学」，ナカニシヤ出版，2000.7

[5] 社団法人私立大学情報教育協会　情報倫理教育振興研究委員会：ネットワークの運用体制に関するガイドライン，社団法人私立大学情報教育協会，1998
http://www.shijokyo.or.jp/LINK/rinri.pdf

[6] 黒田　豊：インターネット･セキュリティ　ころばぬ先の知恵，丸善ライブラリー，1997

[7] 警察庁：情報システム安全対策指針　国家公安委員会告示第9号，平成9年9月18日
http://www.npa.go.jp/soumu2/kokuji.htm

[8] 通商産業省：報道発表資料本文「コンピュータ不正アクセス対策基準について」
http://www.miti.go.jp/press-j/past/c60806a2.html

[9] 今井賢一：情報ネットワーク社会，岩波新書，

1993
[10] 文部科学省・和歌山大学：「平成13年度情報処理教育研究集会講演論文集」，文部省・和歌山大学，2001.10
林英輔，久保美和子，大塚秀治，牧野晋：情報システムの不適切利用者に関する情報倫理教育，pp11
中山幹夫：情報ネットワーク社会を核とした情報教育論，pp15
辰巳丈夫，楠元範明：情報科の教員養成における「情報倫理」と「情報職業」，pp32
木川裕：ネット環境における学生の情報関連補記の認識，pp107
河本進，渡邉透，細谷順二：学生のインターネット意識の傾向について，pp111
橋本恵子：大学生の情報行動における男女差，pp125
工藤英男，内田眞司，武村泰宏，吉川博史：インターネットにおける情報倫理に関する意識調査(6)，pp135
永田清，柴木恒一，青木智子：学生の個人情報とセキュリティ意識(2)，pp151
山口栄作，鈴木斉：アンケート調査に基づく利用者のセキュリティ意識向上計画，pp167

(平成17年1月20日受付,平成17年2月1日受理)