패스워드 이용에 관한 실증분석: 대학과 종합병원을 중심으로

An Empirical Study on Password Controls

정 경 수 (Kyung Soo Chung) 경북대학교 경영학부
김 기 영 (Kee Young Kim) 한국석유화학공업협회
박 종 필 (Jong Pil Park) 경북대학교 대학원

목 차

Ⅰ. 서 론
Ⅱ. 이론적 배경
Ⅲ. 연구모형 및 가설
Ⅳ. 연구분석 결과
Ⅴ. 결론 및 한계점

Keywords: *Password, Password characteristics, Password control, Authentication, Data attribute*

Ⅰ. 서 론

급변하는 국내외의 환경변화에 능동적으로 대처하고 글로벌 경쟁에서 우위를 점유하기 위해, 조직은 생산공정을 합리화하고, 조직의 효과성과 생산성을 증가시키고, 경쟁우위를 가져다 줄 수 있는 정보기술을 도입하지 않을 수 없게 되었다. 정보기술은 비즈니스의 기본틀을 바꾸기도 하고 고객에 대한 서비스나 생산과 판매전략, 그리고 유통과정 등에 엄청난 파급효과를 가져오고 있다. 그리하여 정보기술을 활용한 경영혁신, 인트라넷과 전사적 자원관리(Enterprise Resource Planning: ERP)시스템의 도입, 전자상거래를 위한 시스템의 도입과 구축 등이 대부분의 조직이 번영하고 살아남기 위한 핵심과제가 되었다.

정보시스템에 대한 의존도가 커짐에 따라 정보를 보다 빨리 수집하고, 처리하고, 저장하여 필요한 사람들이 시간과 공간의 제약을 받지 않고 활용할 수 있는 환경으로 변하고 있지만 정보기술의 확산은 불순한 의도를 가진 집단이나 개인들에게 정보시스템의 무결성과 유효성을 침해하는 기회를 가져다 주었다. 지금까지 컴퓨터를 이용한 범죄의 숫자나 종류는 상당한 비율로 증가하고 있고 컴퓨터 범죄로 인한 엄청난 손실도 계속 증가하고 있는 실정이다.

LA 타임즈에 의하면 1997년 한해에 미국기업의 64%가 컴퓨터관련 범죄를 경험하였다고 한다(LA Times, March 5, 1998).

컴퓨터관련 범죄를 막기 위해 가장 일반적으로 쓰는 방법으로 패스워드 시스템을 들 수 있다. 패스워드는 사용자의 인증이나 자료의 접근을 제한하는 등의 용도로 사용된다. 만약 패스워드 시스템이 불안정하거나 외부에 노출될 경우, 정보가 오용될 소지가 있기 때문에 패스워드의 보안은 아주 중요한 문제이다. 그러나 실질적으로 컴퓨터 시스템에 대한 침투가 패스워드와의 절충능력에 달려 있다는 사실에도 불구

하고 지금까지 많은 사람들이 우리들이 사용하고 있는 패스워드의 보안기능이나 특성에 특별한 관심을 기울이지 않았다.

본 연구에서는 사용자 선택 패스워드의 특성들, 즉 패스워드의 길이, 구성, 수명, 선택방법을 실증적으로 평가하고, 사용자가 가지고 있는 데이터 파일이 그 사람에게 얼마나 중요한지 그리고 외부로의 유출시 얼마나 민감해 질 수 있는지에 따라 패스워드의 특성에 변화가 있는지를 살펴보고, 패스워드의 특성들이 패스워드를 기억하고 기록하는데 영향을 미치는지 알아보고자 한다.

Ⅱ. 이론적 배경

본 장에서는 패스워드의 개념과 종류 그리고 메카니즘에 대해서 알아보고 기존 문헌을 통하여 데이터의 속성, 패스워드의 특성, 그리고 저장방법에 관한 이론적 고찰을 하였다.

2.1 패스워드의 개요

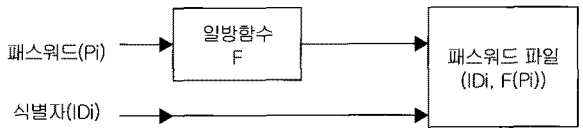
2.1.1 패스워드의 정의와 종류

Wood(1983)에 의하면 패스워드는 컴퓨터 혹은 커뮤니케이션 시스템 사용자의 신원을 확인하는데 사용되는 문자와 숫자, 특별한 기호, 그리고 제어문자의 연속물을 의미한다. 패스워드는 사용자가 커뮤니케이션 네트워크나 혹은 원거리 접속 컴퓨터에 접속할 때와 배치 컴퓨팅 업무를 초기화 할 때, 데이터베이스나 파일에 접속할 때, 그리고 특별한 시스템이나 응용프로그램을 운영할 때, 혹은 다른 어떤 제한된 컴퓨터/커뮤니케이션 자원을 요구할 때 적용될 수 있다.

패스워드의 종류에는 사용자가 스스로 패스워드를 선택하는 사용자-선택 패스워드(user-chosen password), 데이터 관리자에 의해 만들어지고 운영되는 관리자-선택 패스워드(administration-chosen password) 그리고 컴퓨터가 패스워드를 만들어 내는 형식의 컴퓨터-선택 패스워드(computer-chosen password) 방식이 있다 (Schneiner, 1996).

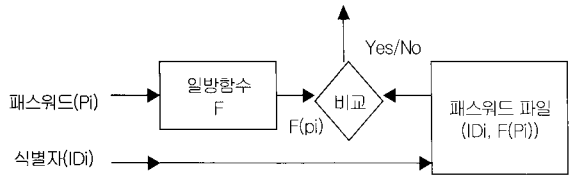
2.1.2 패스워드 메카니즘

패스워드 시스템은 기본적으로 사용자 자신의 ID (identification)와 패스워드를 입력하여 시스템에 접근하는 방법을 사용한다. 입력한 ID와 패스워드는 미리 저장된 화일들과 비교하여 사용자에게 시스템을 이용할 수 있는 권한을 부여하게 된다. 일반적으로 ID는 쉽게 바뀌지 않으며 패스워드를 변경하여 사용자의 제한을 할 수 있게 한다. 그러나 시스템의 패스워드가 노출되거나 시스템에 고장이 발생할 경우, 그 때마다 모든 시스템 사용자들이 패스워드를 바꾸어야 하는 문제가 제기되었다. 또한 시스템 관리자가 퇴직이나 이직할 경우, 패스워드 화일을 도용할 소지도 있다. 이러한 문제를 해결하기 위해 일방함수(one way function)를 이용한 방법이 사용되었다(Schneier, 1996). 일방함수는 한쪽 방향으로는 계산이 쉽지만 역으로는 계산이 불가능한 함수를 말한다. <그림 2-1>을 살펴보면, 먼저 패스워드를 입력하여 일방함수를 이용한 계산결과가 도출되면 ID와 함께 패스워드 화일에 저장하게 된다. 이때 Pi에서 F(Pi)로는 계산하기 쉬우나 F(Pi)에서 Pi로 계산하기는 불가능하다.



〈그림 2-1〉 패스워드의 저장

<그림 2-2>는 패스워드의 인증에 대해 나타내고 있다. 사용자가 ID와 패스워드를 입력하게 되면 미리 저장되어있는 패스워드 화일과 비교하여 사용자를 인증하게 된다. 이러한 방법의 특징은 앞서 언급한 역함수에 대한 계산이 불가능하기 때문에 패스워드 화일 자체에 대한 보안이 필요하지 않게 된다. 만약 패스워드 화일이 노출될 경우라도 그 파일로부터 다른 사람의 패스워드를 알 수 없기 때문이다.



〈그림 2-2〉 패스워드의 인증

2.2 선행연구

2.2.1 데이터속성에 관한 연구

Highland(1997)는 데이터 속성(data attribute)을 민감도(sensitivity)와 중요도(importance)로 구분하였다. 민감도는 데이터 파일의 내용이 다른 사람에게 공개 될 때 문제가 발생할 수 있는 정도를 의미하고 중요도는 개인 사용자에 대한 데이터의 고유한 가치를 말한다. 그의 연구에서 민감도와 중요도가 고려되지 않은 데이터보다 이 두 가지 모두 고려된 데이터가 보다 강력한 보안으로 이루어져 있다라고 하였다.

Zviran과 Haga(1999)의 연구에서는 민감도와 중요도를 고려한 데이터의 속성이 패스워드의 수명, 패스워드의 설치 방법에 영향을 미치는 것으로 나타났다.

2.2.2 패스워드 특성에 관한 연구

1) 패스워드의 길이와 구성에 관한 연구

패스워드의 길이는 패스워드 공격에 대한 방어력의 평가가 되며 패스워드의 구성에 깊은 관련이 있다. 다음의 식에 의해 허용될 수 있는 패스워드의 수를 계산할 수 있다.

$$S = Z^{l}$$

S: 가능한 패스워드의 수
Z: 캐릭터 공간의 크기
l : 패스워드의 길이

Menkus(1988)는 이상적인 패스워드의 길이는 여섯에서 여덟 문자의 철자와 숫자의 조합(alphanumeric)이 되어야 한다라고 하였다. 또한 Jobusch와 Oldhoeft (1989)는 패스워드 길이가 조금만 늘어나더라도 허용될 수 있는 패스워드는 굉장히 많이 늘어나게 된다라고 하였다.

이에 따라, 선택된 패스워드의 길이는 보호되어야 할 자료의 가치 또는 민감성에 비례하는 보안 수준을 제공할 수 있도록 설계되어야 한다. 패스워드의 길이는 구성 가능문자와 더불어 시행착오 공격에 대한 패스워드 시스템의 보안을 평가하는 기준이 될 수 있다(이필중 · 문희철, 1991).

한편 패스워드의 구성가능문자는 입력장치, 저장방법 그리고 입력된 패스워드와 저장된 패스워드를 비교하는 방법과 연관이 있다. 구성가능문자의 최소값은 10이며 금융기관에서 이용하는 PIN(personal identification number)은 10개의 문자(0~9)로써 구성된다. 좀더 나은 구성으로서는 10개의 숫자에 A, B, C, D, E, F를 포함하여 패스워드를 16진수로 표현하는 것이다. 16진수 문자는 하나에 4비트씩으로서 DES의 키를 나타낼 때 이용한다. 대부분의 패스워드는 영어의 대문자와 소문자로 구성하는 경향이 있으므로 이를 숫자와 혼합하여 사용하는 방법이 좋다. 더욱 좋은 방법은 구성가능문자로서 95개의 그래픽 문자와 함께 이용하는 방법이 있다. 자동 패스워드 시스템은 패스워드가 생성 또는 변경될 때 패스워드가 구성 가능문자들로만 구성되었는지 검사할 수 있는 기능을 가져야 한다(이필중 · 문희철, 1991).

2) 패스워드의 수명과 선택방법에 관한 연구

일반적으로 패스워드 사용자는 패스워드를 자주 변경하지 않는 경향이 있다. 따라서 패스워드가 추측될 확률을 가지고 있는데 수식으로 표현하면 다음과 같다.

$$P = \frac{LR}{S}$$

P: 패스워드의 변경주기(수명) 이내에 추측될 확률
L: 패스워드의 수명
R: 단위 시간당 추측될 수
S: 가능한 패스워드의 수

이상과 같은 관계식을 사용하여 패스워드의 조합, 길이, 수명 등을 대입시켜 패스워드 추측 확률을 계

산할 수 있다.

패스워드의 최대 수명은 1년 이하이어야 하며 원하는 수준의 보안을 유지하면서 가장 비용이 적게드는 방향으로 수명을 결정한다. 만약 사용자가 시스템 사용권한이 없어지거나 자료접근 권한이 없어질 경우는 적어도 3일 안에 패스워드를 지우든지 유효하지 않은 패스워드로 만들어야 한다. 자동화된 패스워드 시스템은 보안 관리자가 자신을 인증한 후 사용자의 패스워드를 지우거나 교체할 수 있게 허락해야 하며 패스워드를 새로 만들거나 교체했을 때의 기록도 보존해야 한다(이필중 · 문희철, 1991).

패스워드 선택방법에 관한 연구로, Morris와 Tompson(1979)은 유닉스 환경에서 사용자 제조 패스워드의 기초 특성들을 기술하였고 이러한 패스워드에 의해 제공되어지는 보안의 수준을 분석했다.

Barton과 Barton(1988)의 연구에서는 시스템 접근을 통제하는 대부분의 방법들이 사용자-선택 패스워드를 사용한다고 하였다. 또한 대부분의 전문가들은 정보가 민감하면 할수록 더욱더 패스워드를 자주 변경해야 한다는데 동의를 하고 있다(Highland, 1997).

2.2.3 저장방법에 관한 연구

Ahituv와 Lapid 그리고 Neumann(1988)의 연구에서는 패스워드가 매우 복잡하게 설계되어 있는 경우, 사용자가 잊어버리기 쉽기 때문에, 따로 기록하게 됨으로써 도난이나 복사의 위험이 존재한다고 하였다. 반대로 패스워드가 단순한 경우, 몇 번의 시도에 의해 쉽게 추측 가능하다고 하였다. 그리고 암호 입력에 있어 타이핑 속도가 늦는다면, 타인에 의해 쉽게 노출될 수 있음을 암시하였으며 사용자들이 패스워드를 알아내고 로그인 절차를 모방하는 루틴을 운영시스템에 심어두는 사례 등을 소개하였다.

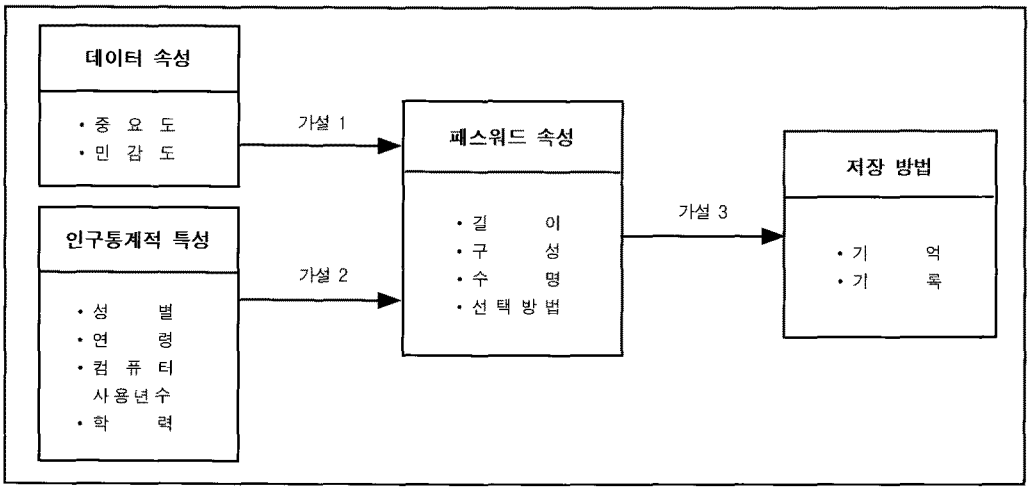
Zviran과 Haga(1993)는 '패스워드는 추측하기는 어렵지만 기억하기 쉬워야 한다' 라고 했다. 가장 안전한 보안형태로 무작위 문자열을 들 수가 있는데, 사용자들은 이러한 패스워드를 기억하기 어렵기 때문에 사용자에게 의미있는 세부사항들, 즉 이름, 별명, 생일과 같은 패스워드를 만들게 된다.

이렇듯 기억하기 어려운 패스워드는 사용자로 하여금 그 패스워드를 어딘가 기록하게 만든다. 따라서 조직은 기억하기 쉽고 추측하기 어렵게 할 수 있는 절충안에 관한 정책을 수립해야 한다(Paans and Herschberg, 1987).

Ⅲ. 연구모형 및 가설

3.1 연구모형의 설계

정보시스템의 보안에서 가장 널리 사용되어지고



〈그림 3-1〉 연구모형

있는 패스워드의 사용에 관한 관심사를 알아보기 위해 본 연구에서는 두 가지 연구 문제에 초점을 맞추었다. 첫째, 사용자 선택 패스워드의 특성들은 무엇인가? 둘째, 데이터의 속성과 패스워드 특성, 인구통계적 특성과 패스워드의 특성, 패스워드의 특성과 저장방법들간의 관계는 무엇인가?

본 연구에서 사용된 실증적 연구모형을 Zviran과 Haga(1999)가 사용했던 모형을 토대로 <그림 3-1>과 같이 설계하였다.

3.2 변수의 정의 및 가설의 설정

3.2.1 패스워드의 특성

본 연구에서 조사하고자 하는 패스워드의 특성들은 길이(패스워드의 문자 수), 구성(문자 영역 : 알파벳, 숫자, 알파벳과 숫자의 조합, ASCII문자 집합), 수명(패스워드 변경 빈도), 그리고 패스워드 선택방법이다. 여기서 선택방법이라는 것은 패스워드가 개인적으로 의미 있는 세부사항(사용자의 이름, 별명, 아이 이름, 혹은 기억하기 쉬운 다른 것, 개인정보), 의미 있는 세부사항의 조합(ERIC710 혹은 LOVEMARY), 소리 나는 대로 적은 문자열(2BEFREE), 무작위 문자열(H*DGFH8H), 혹은 다른 기초를 의미한다.

3.2.2 데이터의 속성과 인구통계적 특성

다음은 데이터의 속성과 인구통계적 특성이 패스워드의 특성과는 어떤 관련성이 있는지 알아보고자 한다.

첫 번째 가설은 데이터의 속성(데이터의 중요도와 민감도)과 패스워드 특성간의 관계에 관한 것이다. 데이터 중요도는 개인 사용자에 대한 데이터의 고유가치를 의미하고, 민감도는 만약 데이터 파일의 내용이 다른 사람에게 공개될 때 문제가 발생할 수 있는 정도를 의미한다. 데이터 파일의 중요도와 민감도는 그 의미에서 차이가 있다. 예를 들어, 연구논문의 데이터 파일을 고려해볼 때 그러한 파일이 공식적으로는 민감하지 않을 수도 있겠지만 관련 연구자들에게는 매우 중요한 가치가 있다. 이에 비해, 학생들의 학점을 담고 있는 데이터 파일은 그 파일 자체가 고유가치를 갖지는 않겠지만 외부로 공개되었을 경우 매우 민감한 반응을 일으킬 수 있다.

이전 연구에서는 데이터 속성과 패스워드 특성간의 관계를 거의 밝히지 않았다. Highland(1997)와 Hoffman(1997)은 보안의 수준이 보호하고자 하는 자원의 중요도와 균형을 맞추어야만 한다고 하였다. 하지만, 이러한 관계를 실증적으로 조사하지는 않았다. 본 연구에서는 데이터의 중요도와 민감도와 같은 데이터의 속성이 사용자가 만든 패스워드의 특성들과 관련성이 있는지를 살펴보았다.

가설1: 패스워드 특성(길이, 구성, 수명, 선택방법)은 보호하고자 하는 데이터의 속성(중요도와 민감도)과 관련성이 있다.

가설1a: 데이터 파일의 중요도는 패스워드 길이와 관련성이 있다.

가설1b: 데이터 파일의 민감도는 패스워드 길이와 관련성이 있다.

가설1c: 데이터 파일의 중요도는 패스워드 구성과 관련성이 있다.

가설1d: 데이터 파일의 민감도는 패스워드 구성과 관련성이 있다.

가설1e: 데이터 파일의 중요도는 패스워드 수명과 관련성이 있다.

가설1f: 데이터 파일의 민감도는 패스워드 수명과 관련성이 있다.

가설1g: 데이터 파일의 중요도는 패스워드 선택 방법과 관련성이 있다.

가설1h: 데이터 파일의 민감도는 패스워드 선택방법과 관련성이 있다.

가설2: 패스워드 특성(길이, 구성, 수명, 선택방법)은 인구통계적 특성(성별, 연령, 근무년수, 학력)과 관련성이 있다.

3.2.3 저장방법

다음 가설은 패스워드의 특성과 저장방법(기억, 기

록)간의 관계를 조사하고자 한다. 패스워드 특성은 기억에 영향을 미친다고 알려져 있다. 만약 패스워드가 기억하기 어렵다면, 기록을 하게 될 것이다. 다음의 가설을 통해 그러한 관련성을 실증적으로 확인하고자 하였다.

가설3: 패스워드의 특성(길이, 구성, 수명, 선택방법)은 패스워드의 저장방법에 영향을 미친다.

가설3a: 패스워드의 특성은 패스워드의 기억능력에 영향을 미친다.

가설3b: 패스워드의 특성은 기록에 영향을 미친다.

Ⅳ. 연구분석결과

4.1 표본의 인구 통계적 특성

본 연구는 근거리 통신망(LAN)이 구축되어 있는 영남지역 5개 종합대학교의 직원과 3개 종합병원의 직원 중 패스워드를 소유하고 있는 사람들을 표본대상으로 하였다.

한국정보보호센터에 따르면, 1999년 1월부터 12월까지 한해 동안 국내 기관별·월별 해킹 피해 건수는 총572회로 이 중 262(45.8%)회가 학교에서 248(43.2%)회가 기업체에서 발생하였다. 본 연구에서는 대상기업을 학교와 종합병원으로 선정하고 직접 방문하여 설문지를 배부하였다. 본 조사의 실증분석에는 학교기관에서 회수된 58부 그리고 병원기관에서 회수된 51부 등 총109부를 사용하였다. 수집된 설문지는 통계분석용 자료입력을 위하여 응답자별 일련 번호를 부여하였고, 각 설문항목에 대해서는 각각 그에 대한 변수값을 지정하였다.

응답자의 인구통계적 특성은 <표 4-1>에서 나타난 바와 같다. 먼저 학교기관을 살펴보면, 남성과 여성의 구성비율이 비슷하고 연령은 26세에서 30세 그리고 31세에서 35세가 다소 높은 구성비율을 차지하고 있지만 어느 정도 골고루 분포된 것으로 보인다. 컴퓨터 사용년수는 10년 이하가 대부분이며 교육수준은 대졸이상이 71.9%로 대부분을 차지하고 있다. 다음으로 병원기관을 살펴보면, 남성과 여성의 구성비율이 비슷하고 연령에서는 31세에서 35세가 다소 높은 구성 비율을 보이고 있고, 교육수준은 대졸이상이 74%

〈표 4-1〉 응답자의 인구통계적 특성

특성	구분	학교		병원	
		응답자 빈도	구성비(%)	응답자 빈도	구성비(%)
성 별	남 자	31	53.4	28	54.9
	여 자	27	46.6	23	45.1
연 령	20세~25세	8	13.8	3	6.2
	26세~30세	15	25.9	11	22.9
	31세~35세	11	18.9	18	37.5
	36세~40세	16	27.6	6	12.5
	41세~45세	5	8.6	7	14.7
	46세 이상	3	5.2	3	6.2
컴퓨터 사용년수	1년~5년	27	47.4	22	44.9
	6년~10년	25	43.8	21	42.9
	11년 이상	5	8.8	6	12.2
교 육 수 준	중 졸	0	0.0	1	2.0
	고 졸	5	8.8	2	4.0
	전문대졸	11	19.3	10	20.0
	대 졸	37	64.9	27	54.0
	대학원 이상	4	7.0	10	20.0

로 가장 많은 비율을 차지하고 있다. 이상에서 보는 바와 같이 두 기관은 비슷한 구성을 보여주고 있다.

분석기법은 SPSS패키지를 통해 ANOVA, Kruskal-Wallis, Spearman's rho, t-test, Mann-Whitney, 빈도분석, 로지스틱 회귀분석을 수행하였다.

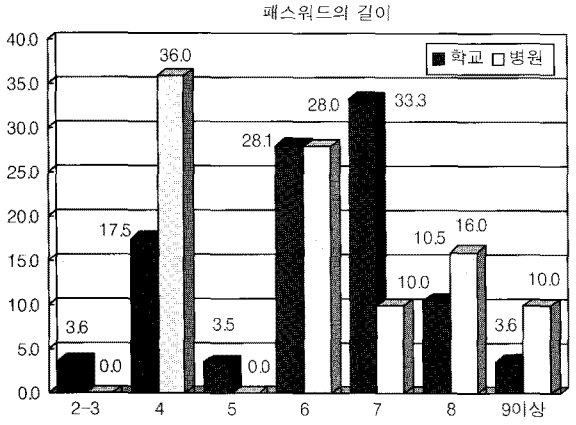
4.2 사용자 패스워드의 특성

4.2.1 패스워드 특성

(1) 패스워드의 길이

<그림 4-1>에서 보듯이 학교기관에서는 6~7단위가 61.4%로 대부분을 차지하고 있는데 이는 Menkus (1988)가 권고하고 있는 8단위에 근접하고 있다. 이에 비해 병원기관에서는 4단위가 36%로 가장 많은 비율을 차지하고 있다. 따라서 두 기관 모두 패스워드의 길이가 짧은 것으로 드러나고 있다.

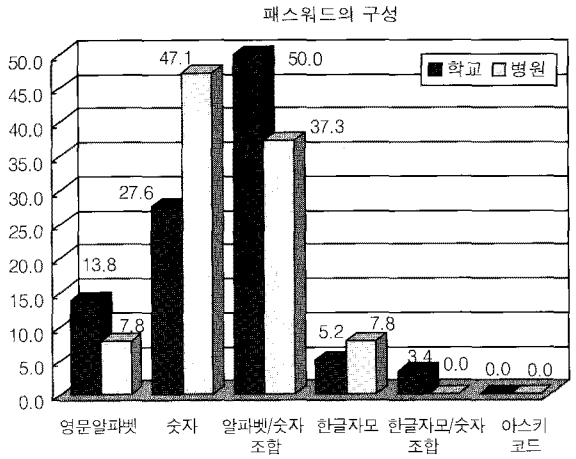
참고로 Windows NT와 Unix는 패스워드 길이를 15문자까지 지원하고 있으며, RSA는 32문자까지 지원하고 있다. Morris와 Thompson(1979)은 패스워드의 길이가 짧으면 침입자가 사용자의 패스워드를 쉽게 알아낼 수 있다라는 사실을 제시하고 있다.



〈그림 4-1〉 패스워드의 길이

(2) 패스워드의 구성

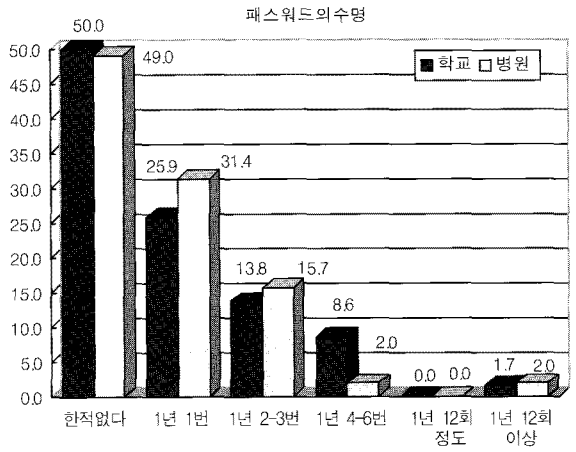
<그림 4-2>에서 보면 학교기관에서는 응답자의 50%가 알파벳과 숫자의 조합(alphanumeric)을 그리고 27.6%가 숫자로 구성된 패스워드를 선호하는 것으로 나타나고 있으며, 이에 비해 병원기관은 47.1%가 숫자만을 선호하는 것으로 나타났다. 보다 복잡한 체계라 할 수 있는 한글 자모체계와 숫자의 조합 그리고 ASCII코드를 패스워드로 사용한다는 응답자는 거의 없었다. 본 연구 결과를 보면, 구성할 수 있는 방법이 다양하게 있음에도 불구하고, 사용자들은 단순한 패스워드를 선호한다는 Morris와 Thompson(1979)의 연구를 뒷받침해주고 있다.



〈그림 4-2〉 패스워드의 구성

(3) 패스워드의 수명

정기적인 패스워드 변경은 기초적인 보안 수단이

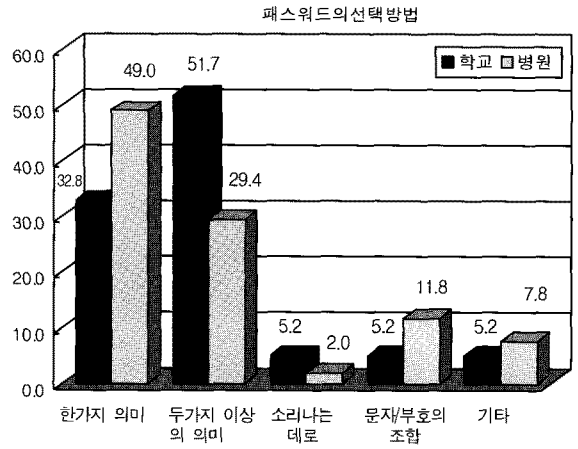


〈그림 4-3〉 패스워드의 수명

라 할 수 있다. Wood(1983)는 패스워드는 해마다 바꿔어야한다고 주장하였고, Menkus(1988)는 매달 바꿔어야 한다고 주장했는데 이는 패스워드를 자주 변경해줌으로써 침입자가 쉽게 패스워드를 추측할 수 없도록 하기 위함이다. 그러나 <그림 4-3>에서 보는 바와 같이 두 기관 모두 한번도 변경해 본적이 없다라는 답변이 50%와 49%를 차지하고 있다. 이러한 결과를 보면 두 기관 모두 사용자들이 패스워드를 바꾸기 싫어하는 경향을 엿볼 수 있다.

(4) 패스워드의 선택방법

패스워드의 해킹은 컴퓨터 게시판에 올라와 있는 정보, 즉 개인의 세부신상에 관한 추측에 의한 실마리를 이용해서 알아낼 수 있다. 세부신상의 예를 들자면, 이름, 별명, 자식이름, 애완동물 이름, 약혼자 이름, 자동차이름, 생일 등을 들 수 있다. 이러한 항목은 사용자에게 특별한 의미를 부여하고 있기 때문에 기억력을 향상시켜준다. 어쨌든, 사용자의 세부신상에 관한 것을 패스워드로 선택하면, 해커는 쉽게 해킹을 하게 된다. 그 이유는 그 해커가 해야할 추측이 제한되어있기 때문이다. <그림 4-4>에서는 두 기관 모두 한가지 의미와 두 가지 이상의 의미를 조합한 패스워드를 선호하는 것으로 나타났는데, 이는 패스워드를 쉽게 추측할 수 있는 발판이 된다고 할 수 있다.



〈그림 4-4〉 패스워드의 선택방법

4.3 측정도구의 신뢰성과 타당성 검증

본 연구의 설문지는 문헌연구를 토대로 하여 예비설문지를 작성, 2회에 걸쳐 예비조사를 실시하였다. 본 연구에서 사용된 변수들은 기존의 연구에서 사용되어 어느 정도 신뢰성과 타당성이 있는 것으로 입증되었고, 응답자가 이해하는데 어려움이 있는 어휘들은 보다 쉽고 명확하게 수정하여 사용하였다.

신뢰성(reliability)이란 동일한 개념에 대해 측정을 반복했을 때 동일한 측정값을 얻을 가능성이다. 이러한 신뢰성을 측정하는 방법으로는 재검사법(test-retest method), 복수양식법(multiple forms technique), 반분법(split-half method), 내적일관성(internal consistency reliability) 등이 있다.

본 연구에서는 재검사법(test-retest)을 통해 신뢰성을 검증하였는데, 설문조사는 3주간의 간격을 두고 교직원을 상대로 무작위로 선택된 20명의 사용자로 나누어서 두 번에 걸쳐 이루어졌다. 개별항목에 대한 재검사법(test-retest)에 의한 상관관계 계수는 $r = 0.62 (p < 0.05)$에서 $r = 0.91 (p < 0.05)$까지의 신뢰범위를 보였다.

타당성(validity)은 조사자가 측정하고자 하는 개념을 얼마나 정확히 측정하였느냐에 관한 것이며, 본 연구의 측정도구에서는 하나의 질문으로 얻고자 하는 정보가 충분하므로 복수가 아닌 단일 문항으로 질문을 하였다. Scarpello와 Campbell(1983)은 사용자의 만족도에 관한 태도를 측정하는데 있어서 한 항목을 측정하는 것이 여러 항목을 측정하는 것보다 더욱 더 포괄적인 측정이라는 것을 입증했다. Galletta와 Lederer (1989)는 사용자 정보 만족도의 포괄적인 측정을 위해서 세부적이고 독립적인 항목들의 합산은 타당하지가 않다고 하였다. 포괄적인 측정을 위해서는 포괄적인 질의가 보다 적절하다고 하였다.

Kappelman과 McLean(1991)은 이러한 한 항목 접근법을 검정하였는데, 단일항목이 포괄적인 사용자 만족도 구성에 있어서 가장 신뢰가 있고 타당한 방법이라 하였다. 본 연구에서는 타당성이 입증된 Zviran과 Haga(1999)의 측정도구를 이용하여, 두 번에 걸친 예

비조사를 통한 보완 등으로 도구의 타당성을 입증하였다.

4.4 가설 검증

4.4.1 패스워드의 특성과 데이터 속성과의 관련성

> 가설 1: 패스워드의 특성(길이, 구성, 수명, 선택방법)은 보호하려고 하는 데이터의 속성(중요도와 민감도)과 관련성이 있다.

<표 4-2>에서는 패스워드의 특성과 데이터 속성간의 관련성(가설1)을 8가지 하위가설로 나누어 검증한 결과를 보여주고 있다.

학교기관에서는 데이터의 중요도와 민감도에 따라 패스워드의 길이를 선택하는데는 차이가 있는 것으로 나타났다(가설1a, 가설1b). 다시 말해 데이터의 중요도와 민감도는 패스워드의 길이를 선택하는데 영향을 미치는 것으로 나타났다.

사후검정으로 던넷의 다중검정치를 이용하여 민감도에 따라 2집단과 6집단이 유의적인 차이가 있는 것으로 나타났는데, 이는 사용자가 가지고 있는 데이터 파일이 외부로 유출시 민감해 질 수 있는 경우에는 세심한 주의를 가지고 패스워드를 만들고 있다는 것을 의미한다. 데이터의 중요도와 민감도는 패스워드의 구성과는 관련성이 없는 것으로 나타났다(가설1c, 가설1d). 그리고 데이터의 중요도와 민감도는 패스워드의 변경주기와 약한 상관관계를 보여주고 있는데(가설1e, 가설1f), 이는 패스워드를 선택할 때 추측하기 어렵게 해야하고 민감하고 중요한 데이터를 보호하기위해 패스워드를 자주 변경하여야 한다는 Highland(1997)의 연구를 입증하고 있다. 또한 데이터의 민감도에 따라 패스워드의 선택방법에 차이가 있는 것으로 나타났다.

이에 비해 병원기관에서는 데이터의 민감도에 따라 패스워드의 길이의 선택과 패스워드의 수명을 선택하는데 있어서 차이가 있는 것으로 나타났고 나머지는 모두 기각되었다. 이는 상대적으로 학교 기관보다 병원기관에 있는 사용자들이 패스워드를 만드는데 있어서 다양하지 못함을 보여주고 있고 패스워드에 대한 보안의식이 약한 경우로 보여진다.

4.4.2 패스워드의 특성과 인구통계적 특성과의 관련성

> 가설 2: 패스워드의 특성(길이, 구성, 수명, 그리고 선택방법)은 인구통계적 특성과 관련성이 있다.

<표 4-3>에서는 인구통계적 특성 중 성별이 패스워드를 선택하는데 관련성이 있는지를 검증하였다. 우선 두 기관 모두 성별에 따라 패스워드의 길이를 선택하는데는 차이가 없는 것으로 나타났다. 학교기

〈표 4-2〉 패스워드의 특성과 데이터 속성간의 관련성

가 설	데이터 속성	패스워드 특성	검 정 기 법	학 교			병 원		
				검증값	p	연구가설	검증값	p	연구가설
가설1a	중요도	길 이	ANOVA	3.758	.004	**채 택**	1.699	.155	기 각
가설1b	민감도	길 이	ANOVA	3.719	.004	**채 택**	1.999	.097	**채 택**
가설1c	중요도	구 성	Kruskal- Wallis	2.837	.829	기 각	4.600	.467	기 각
가설1d	민감도	구 성	Kruskal- Wallis	8.336	.213	기 각	1.920	.860	기 각
가설1e	중요도	수 명	Spearman's rho	.229	.084	**채 택**	- .073	.613	기 각
가설1f	민감도	수 명	Spearman's rho	.228	.085	**채 택**	.214	.092	**채 택**
가설1g	중요도	선택방법	Kruskal- Wallis	6.603	.359	기 각	4.296	.508	기 각
가설1h	민감도	선택방법	Kruskal- Wallis	15.176	.019	**채 택**	3.924	.560	기 각

관을 살펴보면, 남·여의 집단에 따라 패스워드의 구성을 선택하는데는 차이가 있는 것으로 나타났는데, 남자가 여자 보다 복잡하게 구성하는 것으로 나타났다. 또한 남·여의 성별이 선택방법에도 영향을 미치는 것으로 나타났는데 남자가 여자보다 복잡하게 구성하는 것으로 나타났다. 다음으로 병원기관을 살펴보면, 구성, 수명, 선택방법이 유의한 것으로 나타났는데, 결론적으로 두 기관 모두 남·여의 성별에 따라 패스워드 특성의 선택이 달라진다는 것을 의미하며, 남성이 여성보다 상대적으로 패스워드에 대한 보안의식이 강한 것으로 보인다.

<표 4-4>에서는 인구통계적 특성 중 연령은 패스워드를 선택하는데 있어서 거의 관련성이 없는 것으로 나타났다. 이는 나이에 따라 패스워드를 선택하는데는 거의 차이가 없는 것으로 나타났다.

<표 4-5>에서는 인구통계적 특성 중 컴퓨터 사용년수가 패스워드 선택과 관련성이 있는지를 검증하였다. 학교기관에서는 컴퓨터의 사용년수가 패스워드 길이를 선택하는데 영향을 미치는 것으로 나타났는데, 차이검증에 대한 사후검증 결과, 사용년수가 가장 긴 집단이 그렇지 않은 집단들 보다 패스워드 길이가 긴 것으로 나타났다. 또한 컴퓨터 사용년수에 따라 패스워드 구성과 패스워드 선택방법을 채택하는데도 영향을 미치는 것으로 나타났다. 하지만 병원기관에서는 컴퓨터 사용년수가 패스워드를 선택하는 것과는 관련성이 없는 것으로 나타났다.

〈표 4-3〉 성별과 패스워드 특성과의 관련성

인구통계적 특성	패스워드 특성	검정기법	학교			병원		
			검증값	p	연구가설	검증값	p	연구가설
성별	길이	t - test	.230	.819	기각	.604	.548	기각
	구성	Cramer's V	.412	.043	**채택**	.446	.017	**채택**
	수명	Mann -Whitney	391.000	.643	기각	146.000	.000	**채택**
	선택방법	Cramer's V	.445	.022	**채택**	.413	.069	**채택**

〈표 4-4〉 연령과 패스워드 특성과의 관련성

인구통계적 특성	패스워드 특성	검정기법	학교			병원		
			검증값	p	연구가설	검증값	p	연구가설
연령	길이	ANOVA	1.615	.153	기각	2.443	.035	**채택**
	구성	Kruskal-Wallis	9.239	.236	기각	7.173	.411	기각
	수명	Spearman's rho	- .083	.536	기각	.038	.797	기각
	선택방법	Kruskal-Wallis	5.601	.587	기각	7.298	.399	기각

〈표 4-5〉 컴퓨터 사용년수와 패스워드 특성과의 관련성

인구통계적 특성	패스워드 특성	검정기법	학교			병원		
			검증값	p	연구가설	검증값	p	연구가설
컴퓨터 사용년수	길이	ANOVA	4.736	.013	**채택**	.770	.469	기각
	구성	Kruskal-Wallis	6.632	.036	**채택**	1.348	.510	기각
	수명	Spearman's rho	.176	.190	기각	.181	.214	기각
	선택방법	Kruskal-Wallis	5.054	.080	**채택**	.001	.999	기각

〈표 4-6〉 학력과 패스워드 특성과의 관련성

인구통계적 특성	패스워드 특성	검정기법	학 교			병 원		
			검증값	p	연구가설	검증값	p	연구가설
학 력	길 이	ANOVA	.974	.412	기 각	3.736	.011	**채 택**
	구 성	Kruskal-Wallis	3.071	.381	기 각	1.864	.601	기 각
	수 명	Spearman's rho	.089	.509	기 각	.028	.845	기 각
	선택방법	Kruskal-Wallis	2.210	.530	기 각	3.789	.285	기 각

<표 4-6>에서는 인구통계적 특성 중 학력은 패스워드 선택에는 거의 영향을 미치지 않는 것으로 나타났다.

4.4.3 패스워드의 특성과 저장방법과의 관련성

> 가설 3: 패스워드의 특성(길이, 구성, 수명, 그리고 선택방법)과 패스워드의 저장방법은 관련성이 있다.

종속변수가 명목척도이므로 로지스틱 회귀분석을 이용하였다. 이에 앞서 독립변수 중 패스워드의 구성과 선택방법은 명목척도로 이루어져 있으므로 더미변수(dummy variables)로 변환하여 분석을 실시하였다. 로지스틱 회귀분석은 종속변수와 독립변수간의 인과관계를 추정하는 기법으로서 패스워드의 특성과 저장방법간의 인과관계를 밝혔다.

<표 4-7>에서 모형적합도는 0.0170, 0.0005로서 학교와 병원 두 기관 모두 통계적으로 유의한 것으로 나타났다. 모형을 구성하는 계수들을 이용하여 각 독립변수가 종속변수에 미치는 영향을 살펴보면, 패스워드의 길이는 학교와 병원 두 기관 모두 음(-)의 영향을 미치는 것으로 나타났는데, 이러한 결과는 두 기관 모두 패스워드의 길이가 길어질수록 사용자가 기억하기 어렵다는 것을 말해주고 있다. 또한 알파벳과 숫자의 조합은 학교기관에서 그리고 두 가지 이상의 의미 조합은 병원기관에서 기억하기 어려운 것으로 나타났다.

<표 4-8>에서 모형적합도는 0.0846, 0.0222로서 두 기관 모두 통계적으로 유의한 것으로 나타났다. 모형을 구성하는 계수들을 이용하여 각 독립변수가 종속변수에 미치는 영향을 살펴보면 다음과 같다.

학교기관에서는 패스워드의 수명이 기록에 음(-)의 영향을 미치는 것으로 나타났는데, 이는 패스워드를 자주 바꿀수록 기록하게 된다는 것을 말해주고 있다. 이에 비해 병원기관에서는 패스워드의 길이가 기록에 영향을 미치는 것으로 나타났다. 패스워드의 길이가 길어지면 기억하기가 어렵고 따라서 기록하게 되는 것으로 보인다. 하지만 기록을 하게 되는

〈표 4-7〉 패스워드의 특성과 기억능력간의 관련성

종속변수	독립변수	학 교			병 원		
		계수(B)	p	연구가설	계수(B)	p	연구가설
기억능력	패스워드 길이	- .6381	.0815	**채 택**	- .7014	.0725	**채 택**
	알파벳과 숫자의 조합	- 3.1383	.0246	**채 택**	- 5.0702	.9489	기 각
	두 가지 이상의 의미 조합	- .1792	.8692	기 각	2.3899	.0883	**채 택**
	패스워드 수명	- .0078	.9818	기 각	- .6913	.3094	기 각

〈표 4-8〉 패스워드의 특성과 기록간의 관련성

종속변수	독립변수	학 교			병 원		
		계수(B)	p	연구가설	계수(B)	p	연구가설
기 록	패스워드 길이	- .4470	.1552	기 각	- .7494	.0134	**채 택**
	알파벳과 숫자의 조합	- .5828	.6056	기 각	1.4787	.3945	기 각
	두 가지 이상의 의미 조합	- 1.1074	.3001	기 각	1.1925	.3754	기 각
	패스워드 수명	- .4144	.0992	**채 택**	.1187	.7857	기 각

경우 분실의 위험도 있고 따라서 그 조직에 나쁜 영향을 미칠 수도 있다.

V. 결론 및 한계점

5.1 결 론

조직의 정보관리에 있어서 보안에 대한 경영진의 관심은 감소하고 있는 것으로 나타나고 있다. Ball과 Harris(1982)의 연구에 의하면 가장 중요하게 여기는 정보관리의 주제로서 자료 보안은 12번째 순위였다. 그리고 1987년의 Brancheau와 Wetherbe(1987)의 연구에서는 18위였고, 1991년의 Neiderman과 Brancheau 그리고 Wetherbe(1991)의 연구에서는 19위였다. 또한 1996년의 Brancheau와 Wetherbe(1996)의 연구에서는 MIS의 상위 20개 분야에서 보안에 관한 이슈가 포함되지 못했다. 이는 보안에 대한 중요성이 줄어들었거나 혹은 더욱더 강력한 시스템 통제가 이루어졌다는 것을 의미한다고 볼 수 있다.

본 연구에서는 사용자가 선택한 패스워드의 특성들을 실증적으로 평가하고, 이러한 패스워드의 특성들과 데이터의 속성 그리고 패스워드 저장방법간의 관련성을 알아보았다. 실증분석을 위해 근거리 통신망이 구축되어 있는 영남지역 5개 종합대학과 3개 종합병원에 종사하고 있는 직원을 대상으로 설문조사를 실시하였다.

본 연구의 시사점을 살펴보면 다음과 같다.

첫째, 패스워드의 특성들에 대한 연구결과를 살펴보면, 사용자 선택 패스워드는 학교와 병원 두 기관 모두 비교적 추측하기 쉬운 것으로 드러났다. 상대적으로 학교 기관의 종사자가 보다 복잡하게 구성하는 것으로 나타났지만 여전히 두 기관의 종사자 모두 패스워드에 대한 보안의식이 약한 것으로 보인다. 패스워드의 길이는 비교적 짧고, 단순하게 구성되어 있고, 패스워드의 변경은 거의 이루어지지 않고 있으며, 패스워드가 개인에게 의미 있는 세부사항들의 특성으로 구성되어져 있는 것으로 드러났다. Morris와 Thompson(1979)의 연구결과와 비교하여 보면 개인용 컴퓨터시대 이전부터 인터넷 시대에 이르기까지 사용자 선택 패스워드의 특성들은 그렇게 많이 변하지 않은 것으로 보인다.

둘째, 인구통계적 특성 중 성별은 두 기관 모두 관련성이 있는 것으로 나타났는데, 패스워드를 만들 때 남성이 여성보다 복잡하게 구성하는 것으로 나타났다. 연령과 학력은 두 기관 모두 패스워드를 만드는 것에 영향을 미치지 않는 것으로 드러났고, 학교기관에서는 컴퓨터의 사용년수가 길수록 패스워드가 복잡해지는 것으로 나타났다. 하지만 병원기관에서는 관련성이 없는 것으로 조사되었다.

셋째, 패스워드의 특성과 데이터의 속성간의 관련성에서는 두 기관 모두 데이터 속성이 패스워드의 길이를 정하는데 영향을 미치는 것으로 나타났다. 그중 학교 기관 대부분은 패스워드 선택에 있어서 데이터의 속성에 의해 영향을 받는 것으로 나타났지만, 병원 기관은 학교기관 보다 많은 영향을 받지 않는 것으로 나타났다. 추가적으로 본 연구에서 사용자의

22.0%가 데이터 파일은 중요하지 않다라고 응답했고, 32.8%가 민감하지 않다라고 하였다. 데이터 파일이 중요하고 민감한 경우 사용자들은 패스워드를 선택하고 사용할 때 주의해야 한다.

넷째, 패스워드의 선택방법 중 두 가지 이상의 의미 조합이 기억능력에 영향을 미치는 것으로 나타났고, 패스워드를 자주 변경할수록 기록하는 경향을 보였다.

결론적으로 두 대상기관을 비교해 보면, 병원기관의 종사자들이 학교 기관의 종사자보다 패스워드에 대한 보안의식이 약한 것으로 나타났다. 이는 학교기관의 종사자들은 조직의 외부 환경에서 인터넷을 통하여 데이터로의 접근이 가능하므로 패스워드 보안에 관한 의식화가 어느 정도 이루어져 있는 반면에, 병원 기관은 많은 자료에 대하여 외부로부터의 접속을 완전히 차단하고 있으므로 패스워드의 보안이 중요하게 고려되지 않고 있거나 패스워드 보안에 관한 교육이 제대로 시행되고 있지 않다고 볼 수 있다. 실제 대부분의 병원기관에서는 부서간의 시스템 또한 통합되어 있지 않아서 병원내의 자료공유가 제대로 이루어지지 않고 있는 실정이다. 이는 패스워드의 원래목적이 제대로 이루어지지 않고 있음을 의미하는데, 궁극적으로 인트라넷/엑스트라넷으로 통합된다면 패스워드의 활용도는 더욱 확고해 질 수 있을 것이다. 왜냐하면, 패스워드의 해킹을 통한 자료의 변조, 수정, 삭제와 같은 직접적인 영향 뿐만 아니라 경유지로 이용함으로써 조직에 상당한 피해를 유발시킬 수 있기 때문이다.

본 연구결과에서는 컴퓨터 사용자들은 패스워드를 만들고 사용하는데 있어서 보안의식이 매우 낮은 것으로 판단되며, 또한 쉽게 추측할 수 있는 패스워드를 만드는 경향을 보여주었다.

외부침입자 혹은 내부침입자에 의한 해킹의 피해가 기하급수적으로 증가하고 있는 오늘날, 모든 해킹의 첫 관문이라고 할 수 있는 패스워드에 대한 보안교육이 철저하게 이루어져야 할 것이며, 조직은 패스워드의 선택과 사용에 관한 규범을 제정해야 할 필요가 있는 것으로 판단된다.

5.2 연구의 한계점 및 연구방향

본 연구의 한계점과 향후 연구의 방향을 제시하면 다음과 같다.

첫째, 본 연구에서 사용된 측정방법이나 측정도구로 사용된 설문자체가 완벽한 것이 아니므로 이에 대한 더 많은 연구가 요구되며, 단일 항목으로 한 변수를 설명하는 것으로 국한되어 있으므로 정확한 측정과 설문지의 신뢰성과 타당성을 높이기 위한 정교한 측정방법의 개발이 요구된다.

둘째, 본 연구에 제시된 연구모형과 척도는 외국문헌을 바탕으로 개발되었으므로, 연구결과를 한국의 상황에 적용하기 위해서는 한국적 상황에 더욱 적합한 연구모형과 측정항목의 개발이 요구된다.

셋째, 보안정책이 잘 정립된 조직과 그렇지 못한 조직간의 패스워드 보안에 관한 의식에는 큰 차이가 있을 것이다. 실제로 본 논문에서 가설의 기각이 많은 이유 중 하나가 보안에 대한 의식화가 제대로 이루어지지 않았기 때문인 것으로 판단된다.

끝으로, 대상기업을 학교와 병원기관으로 국한하였기 때문에 본 연구의 결과를 일반화하는 데에는 한계가 있다. 앞으로의 연구는 일반기업 등으로 확대해 수행한다면 보다 다양한 결과를 도출할 수 있으리라 판단된다.

참 고 문 헌

이필중, 문희철, 패스워드 시스템의 보안에 관한 고찰, 한국통신보호학회지, 제1권 제1호, 1991, pp. 109-118.

정충영, 최이규, SPSSWIN을 이용한 통계분석, 무역경영사 제 3판, 1998.

Ahituv, N., Lapid, Y. and Neumann, S., "Verifying the authentication of an information system user," *Computers and Security*, Vol. 6, No. 2, 1988, pp. 152-157.

Ball, L. and R. Harris, "SMIS member: a membership analysis," *MIS Quarterly*, Vol. 6, No. 1, 1982, pp. 19-38.

Barton, B. F. and M. S. Barton, "User-friendly password methods for computer-mediated information systems," *Computers and Security*, Vol. 3, No. 3, 1988, pp. 186-195.

Bishop, M. and D. V. Klein, "Improving system security via proactive password checking," *Computers and Security*, Vol. 14, No. 3, 1995, pp. 233-249.

Brancheau, J. C. and J. C. Wetherbe, "Key issues in information systems management," *MIS Quarterly*, Vol. 11, No. 1, 1987, pp. 23-36.

Brancheau, J. C. and J. C. Wetherbe, "Key issues in information systems management: 1994-95 SIM/ Delphi results," *MIS Quarterly*, Vol. 20, No. 2, 1996, pp. 225-242.

Galletta, D. F. and A. L. Lederer, "Some cautions on the measurement of user information satisfaction," *Decision Sciences Journal*, Vol. 20, 1989, pp. 419-438.

Highalnd J. H., "Demise of passwords," *Computers and Security*, Vol. 9, No. 4, 1990, pp. 196-200.

Highland J. H., "How to prevent the use of weak passwords," *EDPACS*, Vol. 18, No. 9, 1991, pp. 7-12.

Highland J. H., "Changing passwords," *Computers and Security*, Vol. 16, No. 3, 1997, pp. 183-184.

Hoffman, L. J., *Modern Methods for Computer Security and Privacy*, Prentice-Hall, Englewood Cliffs, NJ, 1977.

Jobusch, D. L. and A. E. Oldhoeft, "A survey of password mechanisms: weakness and potential improvements, part 1," *Computers and Security*, Vol. 8, No. 7, 1989, pp. 587-604.

Kappelman, L. A. and E. R. McLean, "The respective roles of user participation and user involvement in information system implementation success," *Proceedings of the Twelfth International Conference on Information Systems*, New York, NY, December 1991, pp. 339-349.

Los Angels Times, March 5, 1998.

Menkus, B., "Understanding the use of passwords," *Computers and Security*, 1988, Vol. 7, No. 2, pp. 132-136.

Morris, R. and K. Thompson, "Password security: a case history," *Communications of the ACM*, Vol. 22, No. 11, 1979, pp. 594-597.

Neiderman, F., J. C. Brancheau, and J. C. Wetherbe, "Information systems issues for the 1990s," *MIS Quarterly*, Vol. 15, No. 4, 1991, pp. 475-502.

Paans, R., and I. S. Herschberg, "Computer security: the long road ahead," *Computers and Security*, Vol. 6, No. 5, 1987, pp. 403-416.

Scarpello, V. and J. P. Campbell, "Job Satisfaction: Are All the Parts There?" *Personnel Psychology*, Vol. 36, 1983, pp. 577-600.

Schneier. B., Applied cryptography, John Wiley & Sons. Inc., 1996.

Spafford, E., "The internet worm : crisis and aftermath," *Communications of the ACM*, Vol. 32, No. 6, 1989, pp. 700-703.

Turn R and W. H. Ware "Privacy and security issues in information systems," *IEEE Transactions on Computers*, Vol. C-25, No. 12, 1976, p. 1353

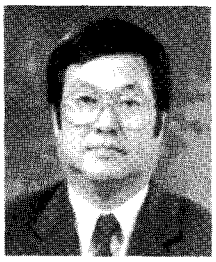
Wood, C. C., "Effective information system security with password controls," *Computers and Security*, Vol. 2, No. 1, 1983, pp. 5-10.

Zviran, M. and W. J. Haga, "Cognitive passwords: the key for easy access control," *Computers and Security*, Vol. 9, No. 8, 1990, pp. 723-736.

Zviran, M. and W. J. Haga, "A comparison of password techniques for multilevel authentication mechanisms," *The Computer Journal*, Vol. 36, No. 3, 1993, pp. 227-237.

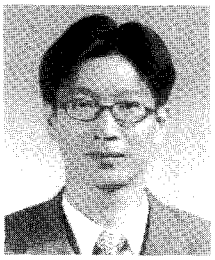
Zviran, M. and W. J. Haga, "Password security: an empirical study," *Journal of Management Information Systems*, Vol. 15, No. 4, 1999, pp. 161-185.

◐ 저 자 소 개 ◑



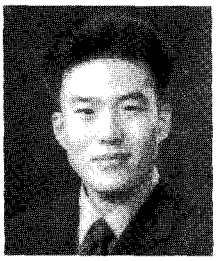
정 경 수 (kschung@knu.ac.kr)

공동저자 정경수는 연세대 경영학과를 졸업하고 뉴욕주립대(SUNY at Buffalo)에서 경영학석사, University of Texas at Austin에서 경영학박사를 취득하였다. 현재 경북대 경영학부에 재직하고 있으며 주요관심분야로는 경영정보시스템, 정보윤리, 전자상거래 등이 있다.



김 기 영 (kykim@mail.kpia.or.kr)

공동저자 김기영은 경북대 대학원에서 석사학위를 취득하고 현재 한국석유화학공업협회에 근무하고 있다. 주요관심분야로는 정보시스템, 네트워크보안, Data Analysis, CRM 등이 있다.



박 종 필 (mis@ssc.or.kr)

공동저자 박종필은 계명대학교 경영정보학과를 졸업하고 현재 경북대학교 대학원 경영학과에 재학중이다. 관심분야는 경영정보시스템, 지식경영, 전략경영 그리고 IT가 조직성과에 미치는 영향 등이다.