패스워드 보안에 관한 실증분석

정경수* · 김기영**

< 목 차 >

Ⅰ. 서 론

오늘날 많은 기업들은 그 어느 때보다도 신뢰를 바탕으로 하는 정보시스템에 의존하게 되었으며 그것이 조직의 성공을 위한 주요한 요소라고 여기게 되었다. 급변하는 국내외의 환경변화에 능동적으로 대처하고 글로벌 경쟁에서 우위를 점하기 위해 조직은 사업공정을 합리화하고, 조직의 효과성과 생산성을 증가시키고, 경쟁우위를 가져다 줄 수 있는 정보기술을 도입하지 않을 수 없게 되었다. 그리하여 정보기술을 활용한 경영혁신, 인트라넷과 전사적자원관리(Enterprise Resource Planning: ERP)시스템의 도입, 전자상거래를 위한 시스템의 구축 등이 대부분의 조직이 번영하고 살아남기 위한 핵심과제가 되었다.

정보시스템에 대한 의존도가 커짐에 따라 많은 정보를 빨리 수집하여 처리하고 저장하여 필요한 사람들이 접근할 수 있도록 해야 했지만, 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 손실도 계속 증가하고 있는 실정이다 (Turban, McLean, Wetherbe, 1999). LA 타임즈의 보도에 의하면 1997년 한해에 미국기업의 64%가 컴퓨터관련 범죄를 경험하였다고 한다 (Los Angeles Times, March 5, 1998).

네트워크 환경에서 사용자의 인증(authentication)을 위해 패스워드가 널리 이용되고 있는데 일반적으로 패스워드는 시스템에 들어가고자 하는 사용자를 인증하거나 시스템 사용자에 대한 자료의 접근을 제한하는 용도로 이용된다. 따라서 패스워드 시스템이 불안전하다면 시스템이 위험에 빠지고 귀중한 정보가 노출 또는 변경될 수도 있으므로 패스워드의 보안은 아주 중요한 문제이다. 하지만 실질적으로 컴퓨터 시스템에 대한 침투가 패스워드와의 절충능력에 달려 있다는 사실에도 불구하고 지금까지 실제 사용하고 있는 패스워드의 특성에는 거의 관심을 가지지 않았다.

본 연구에서는 사용자가 선택한 패스워드의 특성들, 즉 패스워드 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.

* 경북대학교 경영학과
** 경북대학교 대학원 경영학과

Ⅱ. 이론적 배경

본 장에서는 패스워드의 개념과 종류 그리고 메카니즘에 대해서 알아보고 패스워드 보안에 대한 위협을 국내·국제별로 나누어 그 사례를 들었다. 또한 기존 문헌을 통하여 데이터의 속성, 패스워드의 특성, 그리고 저장방법에 관한 이론적 고찰을 하였다.

2.1. 패스워드의 개요

2.1.1. 패스워드의 정의

컴퓨터를 이용한 지능적인 범죄가 사회문제화 되어 가고 있는 환경 하에서 자료처리, 또는 정보통신분야에 있어서의 체계적 통제 수단은 기밀보호 관리와 패스워드로 알려진 비밀문자군, 사용자 식별부호, 그리고 암호와 코드의 사용에 달려있다.

Wood(1983)에 의하면 패스워드는 컴퓨터 혹은 커뮤니케이션 시스템 사용자의 신원을 확인하는데 사용되는 문자와 숫자, 특별한 기호, 그리고 제어문자의 어떤 연속물로서 정의된다. 패스워드는 사용자가 커뮤니케이션 네트워크나 혹은 원격리 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.

2.1.2. 패스워드의 종류

(1) 사용자-선택 패스워드(user-chosen password) : 사용자가 스스로 패스워드를 선택하는 방식으로, 사용자가 패스워드를 폭로하지 않는 한 비밀이 유지된다.

(2) 관리자-선택 패스워드(administrator-chosen password) : 데이터 보호 관리자에 의해 모든 패스워드가 만들어지고 운영되는 방식으로, 관리자는 무작위에 의한 패스워드 생성 및 규칙적인 변경을 행한다.

(3) 컴퓨터-선택 패스워드(computer-chosen password) : 사용자 선택방식과 관리자 선택방식의 중간 형태로서 컴퓨터가 패스워드를 만들어 내는 방식이다. 이 방식은 임의성은 있으나 사용자가 패스워드를 잊어버리기가 쉽다.

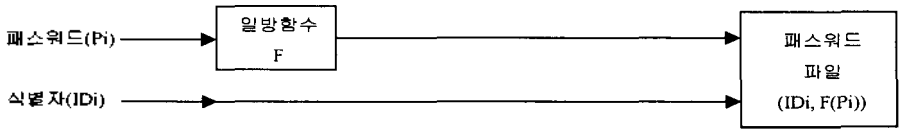
2.1.3. 패스워드 메카니즘

패스워드 시스템에서는 사용자가 자신의 식별자(identifier, ID)와 패스워드를 입력하여 자신을 인증한다. 모든 사용자들의 식별자와 패스워드는 시스템 내에 저장되어 있고 시스템은 입력된 식별자와 패스워드를 저장되어 있는 것과 비교한다. 비교결과 올바른 식별자와 패스워드가 입력되었을 경우에만 사용자에게 시스템이나 파일에 접근할 수 있는 권한을 준다.

식별자와 패스워드를 패스워드 파일에 저장하고 시스템 관리자를 제외한 모든 이에게 그 파일에 대한 접근을 제한한다. 그러나 이 방법은 시스템의 고장이나 시스템 관리자의 패스워드가 노출되는 등의 경우에 패스워드 파일이 노출될 수 있고 그때마다 모든 사용자들이 패스워드를 바꿔야 하는 문제가 있었다. 더욱 큰 문제는 시스템 관리자 자신에 대해서는 아무런 제한 조치를 할 수 없고 그가 그만둘 때 패스워드 파일을 복사해 가지고 나갈 수도 있다는 점이다.

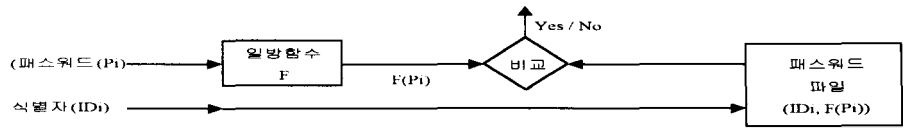
그래서 이 문제를 해결하기 위해 일방함수(one way function)를 이용한 새 방법이 고안되었다. 이 방법은 [그림Ⅱ-1] 에서와 같이 패스워드를 입력으로하여 일방함수를 계산한 결과를 식별자와 함께 패스워드 파일에 저장하는 것이다. 일방함수란 한 방향으로의 계산은 쉬운 반면 반대방향의 계산은 불가능한 함수를 말한다. 따라서 Pi를 이용하여 F(Pi)를 계산하

기는 쉬워도 F(Pi)로부터 Pi를 계산해내기는 거의 불가능하다.



[그림Ⅱ-1] 패스워드의 저장

사용자가 식별자와 패스워드를 입력하면 시스템은 그 패스워드를 일방함수를 거쳐 저장되어 있는 것과 비교하여 사용자를 인증한다. [그림Ⅱ-2]는 이러한 인증방법을 설명하고 있다. 전의 방법과 달라진 점은 역함수의 계산이 불가능하므로 패스워드 파일자체에 대한 보안이 불필요하게 된 것이다.



[그림Ⅱ-2] 패스워드의 인증

2.1.4. 패스워드보안에 대한 위협

패스워드 보안의 위협이란 사용자의 패스워드가 불법적으로 노출되는 것을 말한다. 시스템에 불법적으로 침입하려는 자는 아래의 세 가지 방법으로 사용자의 패스워드를 알아낼 수 있다.

첫째, 시스템의 패스워드 파일을 읽어내는 방법이 있다. 패스워드 파일은 일반 사용자에게 접근을 제한하며 오직 보안 관리자만이 권리를 갖게 한다. 그러나 시스템의 고장이 생겨 일반 사용자들도 패스워드 파일에 접근 가능하다거나 보안관리자가 불순한 마음을 품었을 때에는 이와 같은 패스워드시스템은 전혀 안전하지 못하다.

둘째, 사용자와 시스템간에 패스워드를 주고 받는 통신을 도청할 수 있다. 만약 보안 관리자가 패스워드 시스템에 대한 도청의 위험이 크다고 판정하면 통신되는 패스워드는 입력장소에서 암호화되어 비교 장소까지 전달되는 방법을 취해야 한다.

셋째, 패스워드가 부주의하게 만들어져 쉽게 추측할 수 있는 경우이다. 패스워드의 추측을 어렵게 하려면 사용자가 보다 무작위하게 선택하거나 자동으로 시스템에서 패스워드를 골라주는 방법이 있다.

(1) 해킹(hacking)의 개요

넓은 의미에서는 해커들이 저지르는 모든 불법적인 행위들을 해킹이라고 하며 좁은 의미에서는 정보시스템 전산망에서의 보안 침해사고를 발생시키는 행위들을 말한다.

① 불법 침입 : 인가 받지 않은 다른 정보시스템에 불법으로 접근
② 불법 자료 열람 : 허가되지 않은 불법접근을 통해 주요 정보를 열람
③ 불법 자료 유출 : 개인이나 조직의 주요 정보를 불법으로 유출
④ 불법 자료 변조 : 시스템 내의 자료나 개인의 자료를 변조
⑤ 불법 자료 파괴 : 시스템의 자료를 불법으로 파괴하는 행위
⑥ 정상 동작 방해 : 시스템의 정상적인 동작을 방해하거나 정지

이러한 경우는 대개 우리가 알고 있는 경우이며, 현재의 전산망 환경에서는 다음에 설명하는 것과 같이 보다 세분화하여 나누어 살펴볼 수 있다.

해커들의 해킹 대상을 데이터, 시스템 프로그램, 네트워크 등으로 분류하여 해커들이 저지

를 수 있는 해킹 행위들을 불법삽입, 불법유출, 불법변조, 파괴·거부 등의 행위로 나누어 다음의[표Ⅱ-1]과 같이 요약할 수 있다.

[표Ⅱ-1] 해킹과 해킹 사고 유형

대상 / 유형	데이터	시스템/소프트웨어	정보통신망
불법삽입	개인 신상에 대한 그릇된 정보등의 제공	바이러스, 웜, 백도어, 트로이 목마	시스템 과부하를 노린 행위
불법유출	주요비밀정보, 개인 신상정보 등의 유출	주요 시스템 파일의 유출	시스템 제어 정보 유출
불법변조	일반 자료 변조, 불법금융거래를 노린 변조 등	악의적 이용을 위한 프로그램/파일의 변조	통신지연, 잘못된 라우팅 유도
파괴· 거부	일반 중요 정보의 파괴	프로그램 파괴, 고장 유발행위	접근 방해, 망운영 방해

자료원 : 한국정보보호센터

통신망을 통한 주요 정보 유출사고에서 보면, 해킹 방법 중 스니퍼 등을 이용하면 네트워크를 통해 유통되는 사용자 ID, 비밀번호, 전자우편 내용 등을 감청하여 유출할 수 있고, 이러한 방법에 의한 피해는 96년 4건, 98년 5건이 알려져 있다.

전자상거래 등 시스템 해킹 정보 유출사고로 살펴보면, 사업자 시스템에 대한 해킹은 주로 관리자 권한을 부당 획득하는 방법등을 이용하면 개인 정보 등의 유출이 가능하며, 특히 사용자 ID, 패스워드 파일 등을 유출할 수 있고, ID를 도용해서 네트워크서버 취약점 공격 등으로 인한 유출이 가능하게 된다. [표Ⅱ-2]는 시스템 해킹으로 인한 중요 정보 유출건수를 보여주고 있다.

[표Ⅱ-2] 시스템 해킹으로 인한 중요 정보 유출 건수

해킹수단	년도		합계	비고
	97	98		
홈페이지 해킹	10	12	22	패스워드파일유출
네트워크서버해킹	23	39	62	패스워드파일유출
ID도용	3	9	12	일반ID 및 관자자 권한 도용
합계	36	60	96	

자료원 : 한국정보보호센터

(1) 국내 해킹 사례

우선 1998년 12월 K 대학의 한 학과에서 리눅스를 이용한 서버를 운영하던 중 외국 해커가 취약점 분석 도구인 mscan을 이용하여 시스템의 취약점을 알아낸 후, 웹서버의 PHF 버그를 이용하여 시스템의 비밀번호 파일(/etc/passwd)을 유출해 갔으며, 이를 이용해서 시스템에 침입한 후 미국에 있는 시스템으로 다시 침입하려 하였다. 또 다른 예를 살펴보면, 1999년 1월 신원미상의 외국 해커가 인천 소재 대학을 대상으로 자신의 IP주소를 임의의 IP 주소로 바꾸어 핑(ping)을 이용한 서비스 거부 공격의 하나인 스머핑(smurfing) 공격을 감행했다. 이로 인해 외부와 연동된 네트워크에 과부하가 걸려 네트워크 사용에 장애를 받았으며, 외국으로부터 항의성 메일이 수신되는 등 업무에 차질을 빚었다. 현재 인터넷에서 사용하고 있는 TCP/IP 프로토콜상의 문제점인 이 서비스 공격은 근본적인 해결 방법이 없으며, 단지 접근 제어나 라우터에서 옵션을 제거하여 임시 방편으로 대처하는 수밖에 없다.

[표Ⅱ-3]을 살펴보면, 1998년 1월부터 1999년 5월말까지 국내에서의 해킹 건수는 314건에 이르고 있고, 1999년 1월부터 5월말까지 5개월 동안에 일어난 해킹 피해 건수는 156건에 달하는데 이는 1998년 한 해 동안 발생한 건수에 육박하고 있다. 특히 학교의 피해 건수가

많은 것으로 나타나고 있다.

[표Ⅱ-3] 1998, 1999년 월별 국내 기관별 해킹 피해

월	피해기관						합계
	학교	기업	연구소	비영리 기관	정부기관	지역	
98년 1월	4	3					7
2월	10	2					12
3월	3	3					6
4월	1	1	1				3
5월	4	2					6
6월	13	8			1		22
7월	14	11		2			27
8월	6	11					17
9월	7	7					14
10월	6	5	1				12
11월	4	3					7
12월	8	13	2			2	25
99년 1월	15	12					27
2월	23	8		2		2	35
3월	17	8				1	26
4월	17	17		1		1	36
5월	11	18			1	2	32
합계	163	132	4	5	2	8	314

자료원 : 한국정보보호센터

(2) 국외 해킹 사례

Hoffer와 Straub(1989)은 다섯 군데의 조직 중 한 곳은 최소한 매 3년마다 한번의 보안침해를 경험한다는 사실을 발표하였다. 그 중 한 조직은 2백만 달러의 손실을 입었다는 보고를 하였는데, 해킹의 피해는 재정적 손실 뿐만 아니라, 컴퓨터범죄로 인해 자료의 상실과 경쟁자에게 비밀자료를 공개하게 되는 결과를 가져 올 수 있다.

인터넷 해킹 사건 중 가장 유명한 사건은 "뻐꾸기 알(the cuckoo's egg)"이라는 사건이다. 이 사건은 1988년 독일 하노버에 사는 대학생 5명이 브레멘 대학교의 인터넷 계정을 이용하여 대서양 건너 미국의 어느 방위산업체 전산망에 침투한 다음 군사비밀에 해당하는 각종 정보를 입수하여 소련 KGB에 넘겨주고 그 대가로 코카인 등 마약을 받아왔던 것이다. 1년 반 이상 은밀하게 진행되던 이 해킹범행은 침투당한 방위산업체에 근무하는 클리프 스톨(Cliff Stoll)이라는 한 천문학자의 집요한 추적으로 적발되고 말았다.

중국은 은행망을 해킹하여 3만달러를 이체한 해커를 1998년 10월에 체포하였다. 중국 경찰은 중국 동부 지역에서 은행 전산망 시스템을 해킹하여 3만달러를 훔친 두 형제를 체포했다. 이들은 중국에서 체포된 최초의 사이버 은행 강도라고 Beijing Youth Daily지가 보도했다. 흥미로운 것은 98년 12월 중국의 보안당국은 이 2명의 해커들에 대해 사형을 선고하였다는 점이다.

러시아에서도 1998년 10월 29일 은행망을 침입한 해커를 검거하였는데, 남부 러시아의 Rostov-on-Don시에서 두 명의 은행 컴퓨터 해커가 체포되었다. 이 사건은 Rostov지역에서 일어난 첫 번째 은행 전산망 침입 시도였으나 실패로 돌아갔다. Rostberbank 직원으로 밝혀진 이 해커는 지난 10월 6일에 전산망을 침입하였으나 은행 전문가들이 해커 프로그램을 발견하고 해커가 만든 불법 계좌를 막았다.

(3) 국내·국제간의 피해관계

국내·국제간의 피해관계[표Ⅱ-4 참조]를 살펴보면 국내 피해는 모두 141번에 걸친 해킹이 있었고, 이 중 국외에서 국내로 침입한 경우는 123 차례나 발생하였다. 이 중 국내기관이 침입의 목표가 된 것은 34건이며, 나머지 70개 기관은 외국침입을 위한 경유지로 사용되었다. 97년에는 국외에서 국내로의 해킹이 11번 일어났는데 이에 비해 98년에는 무려 12배 정도의 증가를 보여주고 있다. 이와 반대로 국내에서 국외로의 침입경우는 모두 18건으로 작년 9건에 비해 2배의 증가율을 보이고 있다. 국외에서 국내로의 침입 및 경유가 늘어난 것은 크게 두 가지 이유를 들 수 있는데 그 중 하나는 mscan이라는 취약점 분석 프로그램이 소개되면서 사용 예에 국내의 학교 도메인인 "ac.kr"이 들어 있는 이유로 침입의 대상이 되었기 때문으로 분석할 수 있으며, 또 다른 이유로는 국제적인 침해사고의 공조체제인 FIRST에 정보통신망 침해사고 대응팀(CERTCC-KR)이 가입함으로써 국제적인 침해사고 발생시 관련 정보를 제공받음으로써 국제적인 관계가 늘어났다고 볼 수 있다.

[표Ⅱ-4] '98년 국제적 해킹사고 현황

구분	건수
국내 ⇒ 국외	18
국외 ⇒ 국내	123

자료원 : 한국정보보호센터

2.2. 선행연구

2.2.1. 이론적 고찰

(1) 데이터속성에 관한 연구

Zviran과 Haga(1999)에 의하면 데이터의 중요도는 개인 사용자에 대한 데이터의 고유한 가치를 말한다. 민감도는 만약 데이터 파일의 내용이 다른 사람에게 공개 될 때 문제가 발생할 수 있는 정도를 의미한다. 그들은 연구에서는 데이터의 속성이 패스워드의 수명, 패스워드의 선택방법에 영향을 미치는 것으로 나타났다.

(2) 패스워드 특성에 관한 연구

1) 패스워드의 길이에 관한 연구

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

$S = Z^l$ S : 가능한 패스워드의 수
Z : 패스워드 주기
l : 패스워드의 길이

Jobusch와 Oldhoeft1(989)는 패스워드 길이가 조금만 늘어나더라도 허용될 수 있는 패스워드는 굉장히 많이 늘어나게 된다라고 하였다.

Menkus(1988)는 이상적인 패스워드의 길이는 여섯에서 여덟 문자의 철자와 숫자의 조합(alphanumeric)이 되어야 한다라고 하였다.

패스워드의 길이는 시스템 운영자와 보안 관리자에 의해 선택된다. 패스워드의 길이는 최소 4문자 이상이어야 하며 10,000개 이상의 패스워드를 만들 수 있는 길이와 구성 가능 문자를 가져야 한다. 선택된 패스워드의 길이 범위는 보호하는 자료의 가치 또는 민감성에 비례하는 보안 수준을 제공해야 한다. 패스워드의 길이는 구성 가능문자와 더불어 시행착오

공격에 대한 패스워드 시스템의 보안을 평가하는 기준이 된다(이필중 · 문희철, 1991).

2) 패스워드의 구성에 관한 연구

패스워드의 구성가능문자는 입력장치, 저장방법 그리고 입력된 패스워드와 저장된 패스워드를 비교하는 방법과 연관이 있다. 구성가능문자의 최소값은 10이며 금융기관에서 이용하는 PIN(personal identification number)이 10개의 문자(0~9)로써 구성된다. 좀 더 나은 구성으로서는 10개의 숫자에 A, B, C, D, E, F를 포함하여 패스워드를 16진수로 표현하는 것이다. 16진수 문자는 하나에 4비트씩으로서 DES의 키이를 나타낼 때 이용한다. 많은 패스워드들은 영어 소문자(a~z)나 대문자(A~Z)만을 이용하여 구성된다. 그러나 영어 알파벳으로만 이루어진 패스워드는 흔히 알고 있는 영어단어를 이용하는 경우가 많으므로 안전하지 못하다. 따라서 영어 알파벳에 숫자를 넣는 방법이 좋으며 더욱 좋은 방법은 구성가능 문자로서 95개의 그래픽 문자를 이용하는 것이다. 자동 패스워드 시스템은 패스워드가 생성 또는 변경될 때 패스워드가 구성 가능 문자들로만 구성되었는지 검사할 수 있는 기능이 있어야 한다.(이필중 · 문희철, 1991)

어떤 문자들의 집단에서 사용자가 선택한 패스워드의 구성 문자들을 검정하는 프로그램을 통해 패스워드를 추적하는데 걸리는 시간을 추정할 수 있다. 아래의 [표Ⅱ-5]는 PDP-11/70에서 다양한 문자집단으로부터 n길이의 모든 가능한 문자열을 검정할 수 있는데 걸리는 시간을 추정하고 있다. 그 다양한 문자집단은 모든 소문자, 모든 소문자와 십진수의 조합, 모든 철자와 숫자의 조합, 95개의 인쇄가능한 모든 문자들, 그리고 마지막으로 128개의 ASCII 문자들을 두었다.

[표Ⅱ-5] 패스워드 구성에 따른 PDP-11/70에서 소요되는 시간

길이	26개의 영문소문자	36개의 영문소문자와 10진수	철자와 숫자의 조합	95개의 인쇄가능한 문자	128개의 모든 ASCII문자
1	30msec.	40msec.	80msec.	120msec.	160msec.
2	800msec.	2sec.	5sec.	11sec.	20sec.
3	22sec.	58sec.	5min.	17min.	44min.
4	10min.	35min.	5hrs.	28hrs.	93hrs.
5	4hrs.	21hrs.	318hrs.	112days.	500days.
6	107hrs.	760hrs.	2.2yrs.	29yrs.	174yrs.

불순한 의도를 가진 자가 길이가 5단위(문자) 이하의 소문자로 구성된 PDP-11/70에 접근하는 것은 문제가 아닌 것으로 나타났다. 길이가 6단위(문자)라 하더라도 몇 주안에 접근이 가능하다라는 것을 Morris와 Thompson(1979)이 밝혔다.

3) 패스워드의 수명에 관한 연구

통상적으로 패스워드 사용자는 패스워드를 자주 변경하지 않는 경향이 있다. 패스워드의 주기는 여러 가지 변수들에 의해 결정되는데 그 변수들을 열거하면 다음과 같다.

㉮ 패스워드 교체비용
㉯ 불의의 타협과 관련되는 위험
㉰ 분배에 따른 위험
㉱ 패스워드를 추측할 수 있는 확률
㉲ 패스워드 이용횟수
㉳ 완벽한 시행착오 방법을 통한 패스워드의 검색

패스워드가 추측될 확률을 수식으로 표현하면 다음과 같다.

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

P : 패스워드의 변경주기(수명) 이내의 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 계산할 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 교체해야 한다. 자동화된 패스워드 시스템은 보안 관리자가 자신을 인증한 후 사용자의 패스워드를 지우거나 교체할 수 있게 허락해야 하며 패스워드를 새로 만들거나 교체했을 때의 기록을 가져야 한다.(이필중 · 문희철, 1991)

4) 패스워드 선택방법에 관한 연구

Barton, B.F.와 Barton, M.S.(1988)에 의하면 시스템 접근을 통제하는 대부분의 방법들은 사용자 선택 패스워드를 포함한다. 아직까지 컴퓨터 초보자들, 사실상 전문가들에게도 패스워드 선택에 관한 지침서를 제공하는 문헌은 거의 없다. 보안에 초점을 맞추고 있는 "하라"와 "하지마라"라는 임시적인 목록이 오히려 기여한 바가 있다고 할 수 있다. 일반적으로 "하라"라는 목록은 길고, 무작위 문자로 구성하고, 그리고 변경이 빈번한 패스워드를 권하고 있다. "하지마라"라는 목록은 대개 이름, 이니셜, 날짜, 그리고 특히 사용자에게 중요한 숫자를 사용하지 않도록 권유하고 있다. 환경적인 실마리 뿐만아니라 이러한 항목의 역 사본을 사용하는 것을 금지한다.

Highland(1997)에 의하면 대부분의 전문가들은 정보가 민감하면 할수록 더욱더 패스워드를 자주 변경해야하고 패스워드를 선택하는 방법이 적절할 때 가능하다라고 했다.

Morris와 Tompson(1979)은 유닉스 환경에서 사용자 제조 패스워드의 기초 특성들을 기술하였고 이러한 패스워드에 의해 제공되어지는 보안의 수준을 분석했다. 3000개의 패스워드를 조사한 후에, 그들은 85%이상이 다음에 따르는 범주 중 한 곳에 포함되어졌다: 영어사전에 있는 단어, 사전에 있는 단어를 거꾸로 철자화, 성씨 혹은 이름, 거리명, 도시, 그리고 전화번호. 이러한 것들은 대부분의 패스워드가 추측하기 쉽고 그들이 보호하려는 시스템의 충분한 보안수준을 제공하지 못했다는 것을 제시하고 있다.

(3) 저장방법에 관한 연구

Zviran과 Haga(1993)는 패스워드는 추측하기는 어렵지만 기억하기 쉬워야 한다라고 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.

Ahituv와 Lapid 그리고 Neumanm(1988)은 가장 일반적인 기법이라 할 수 있는 패스워드

의 사용은 많은 제약 조건이 따른다고 했다.

㉮ 패스워드가 매우 복잡하게 설계되어 있는 경우, 사용자는 패스워드를 잊어버리기 쉽다. 따라서 사용자는 어딘가에 기록을 해두게 되고 결과적으로 도난이나 복사가 될 수 있다.

㉯ 패스워드가 단순한 경우, 사용자와 관련된 것 중 흔하게 볼 수 있는 것이다. 예를 들자면 생일 같은 것을 기반으로 패스워드를 설계하게 된다. 그래서, 몇 번의 시도에 의해 쉽게 추측이 가능할 수가 있다.

㉰ 암호 입력에 있어서 타이핑 속도가 늦는다면, 그 패스워드가 스크린에 반복되어 나타나지 않더라도, 타인에 의해 쉽게 노출될 수가 있다.

㉱ 패스워드는 일반적으로 운영시스템 소프트웨어의 테이블에 저장되고, 침입자에 의해 검색되어질 수 있다.

㉲ 사용자들로부터 패스워드를 알아내고 또한 로그인 절차를 모방하는 루틴을 운영시스템에 심어두는 여러 사례들 또한 있다.

Menkus(1988)에 의하면 패스워드는 추측하기도 어렵고 기억하기 쉬워야 하는데 추측하기가 어렵도록 하기 위해서는 광범위한 분야에서 추출되어야 한다. 하지만 만약에 추측하기 어렵도록 패스워드를 만든다면, 또한 기억하기도 어려울 것이다. 패스워드의 가장 안전한 형태로 무작위 문자열을 제시하고 있는데, 패스워드를 길고, 무작위로 만들게 되면 다른 사람이 추측하기가 힘들겠지만, 일반적으로 사용자들 또한 그것들을 기억하기가 어렵게 된다. 따라서 대부분의 사용자들은 그 시스템이 인식할 수 있는 최소한의 문자수를 택하게 될 것이다. 그리고 그들의 이름, 별명, 이니셜, 생일과 같은 의미가 있는 세부사항들을 사용한다.

2.2.2. 패스워드 보안에 관한 Zviran과 Haga(1999)연구

이 연구는 미국 캘리포니아에 있는 미국의 국방부에 종사하고 있는 컴퓨터 사용자들을 대상으로 패스워드의 특성들을 조사하였다. 조사 방법은 내부 메일링시스템을 이용하여 2000명의 사용자들에게 설문지가 배부되었고, 997부를 회수하였다. 이 논문에서는 비교적 추측하기 쉬운 패스워드를 사용한다는 것이 밝혀졌다. 또한 시스템 사용자들의 보안의식을 향상시킬 수 있는 교육의 효과성에 문제점을 제시하고 있고, 조직은 사용자들이 패스워드를 만들 때 감독할 수 있는 메카니즘을 보유해야 하고 사용자 선택 패스워드를 채택하고 사용하는 규범의 필요성을 밝히고 있다.

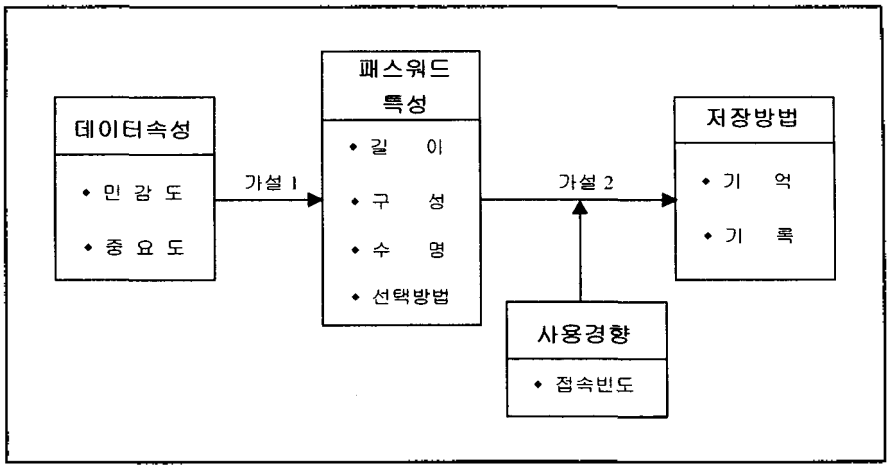
Ⅲ. 연구모형 및 가설

3.1. 연구모형의 설계

경영에 있어 가장 잘 알려진 패스워드 사용에 관한 관심사를 기술하기 위해, 이 연구는 두 가지 연구 질의에 초점을 맞춘다. 첫째, 사용자 선택 패스워드의 특성들은 무엇인가? 둘째, 주요 패스워드 특성들간의 관계는 무엇인가?

본 연구에서 사용될 실증적 연구모형을 Zviran과 Haga가 사용했던 모형을 토대로 [그림 Ⅲ-1]과 같이 설계하였다.

3.1.1. 연구모형



[그림Ⅲ-1] 연구모형

3.1.2. 변수의 정의 및 가설의 설정

(1) 패스워드 특성

첫 번째 질의는 실제 패스워드의 질적인 구현에 초점을 맞춘다. 조사가 이루어지는 패스워드의 특성은 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 성씨, 이름, 별명, 아이이름, 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.

(2) 데이터 속성

두 번째 질의는 데이터의 속성과 패스워드 특성간 그리고 패스워드의 특성과 기억능력·기억간의 관계라고 할 수 있다.

첫 번째 가설은 데이터의 속성(데이터의 중요도와 민감도)과 패스워드 특성간의 관계에 관한 것이다. 데이터의 중요도는 개인 사용자에 대한 데이터의 고유가치를 말한다. 민감도는 만약 데이터 파일의 내용이 다른 사람에게 공개될 때 문제가 발생할 수 있는 정도를 의미한다. 데이터 파일의 중요도와 민감도를 구분하기 위해, 예를 들어, 이 연구논문의 텍스트를 포함하는 데이터 파일을 고려해보자. 그것은 공식적으로는 민감하지 않을지도 모르지만, 본 연구자에게는 중요한 가치가 될 수도 있을 것이다. 비교해서 보면, 학생의 학점을 포함하고 있는 어떤 교수의 데이터 파일에 대한 고유가치를 거의 가지지 않을 것이지만 외부로 유출될 경우 매우 민감한 반응을 일으킬 수 있다.

본 연구에서는 데이터의 중요도와 민감도와 같은 데이터의 속성이 사용자 제조 패스워드의 특성들과 관련성이 있는지를 검증할 것이다. 가설1에서의 관련성은 인과관계를 의미하는 것은 아니다.

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

가설1a : 데이터 파일의 민감도에 따라 패스워드의 길이에는 차이가 있다.

가설1b : 데이터 파일의 중요도에 따라 패스워드의 길이에는 차이가 있다.
가설1c : 데이터 파일의 민감도에 따라 패스워드의 구성에는 차이가 있다.
가설1d : 데이터 파일의 중요도에 따라 패스워드의 구성에는 차이가 있다.
가설1e : 데이터 파일의 민감도에 따라 패스워드의 수명은 차이가 있다.
가설1f : 데이터 파일의 중요도에 따라 패스워드의 수명은 차이가 있다.
가설1g : 데이터 파일의 민감도에 따라 패스워드의 선택방법에는 차이가 있다.
가설1h : 데이터 파일의 중요도에 따라 패스워드의 선택방법에는 차이가 있다.

다음 가설은 패스워드 특성과 저장방법(기억, 기록)간의 관계를 조사하고자 한다. 패스워드 특성은 기억에 영향을 미친다고 제안되어져 왔다. 다음에 따르는 가설을 통해 그러한 관련성을 실증적으로 확인하고자 한다.

가설2 : 패스워드의 특성(길이, 구성, 수명, 그리고 선택방법)은 패스워드의 저장방법에 영향을 미칠 것이다.
가설2a : 패스워드의 특성은 패스워드의 기억능력에 영향을 미칠 것이다.
가설2b : 패스워드의 특성은 기록에 영향을 미칠 것이다.

Ⅳ. 연구분석결과

4.1. 표본 및 자료의 기술적 특성

4.1.1. 표본의 설계 및 자료의 수집

본 연구는 근거리 통신망(LAN)이 구축되어 있는 T지역 5개 종합대학교의 직원 중 패스워드를 소유하고 있는 자를 표본대상으로 하였다. 한국정보보호센터에 따르면, 1998년 1월부터 1999년 5월까지 국내 기관별 해킹 피해 건수는 총314회로 이 중 163(52%)회가 학교가 그 대상이었다. 이에 본 연구인은 설문지를 각 대상기관에 직접 방문하여 배부하였다. 본 조사용 설문지는 총 250부가 배부되었는데 이 중 223부가 회수되어 92.8%의 회수율을 보였다. 이 중 분석에 부적당하다고 판단되는 설문지 8부를 제외하고 총 210부(84%)를 본 연구의 실증분석에 이용하였다. [표Ⅳ-1]은 응답자의 인구 통계적 특성을 보여주고 있다.

[표Ⅳ-1] 응답자의 인구통계적 특성

특 성	구 분	응답자 빈도	구성비(%)
성 별	남 자	108	51.7
	여 자	101	48..3
연 령	21세~25세	33	16.0
	26세~30세	43	20.9
	31세~35세	44	21.4
	36세~40세	44	21.4
	41세~45세	29	14.1
	46세 이상	13	6.3
컴퓨터 사용년수	1년~5년	99	48.3
	6년~10년	84	41.0
	11년 이상	22	10.7
교 육 수 준	고졸	24	11.7
	초대졸	37	18.0
	대졸	117	57.1
	대학원 이상	27	13.2

분석기법은 SPSS패키지를 통해 ANOVA, Kruskal-Wallis, Spearman's rho, 상관관계분석, 빈도분석, 로지스틱 회귀분석을 수행하였다.

4.2. 측정도구의 신뢰성과 타당성 검증

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

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=9.1까지의 신뢰범위를 보였다.

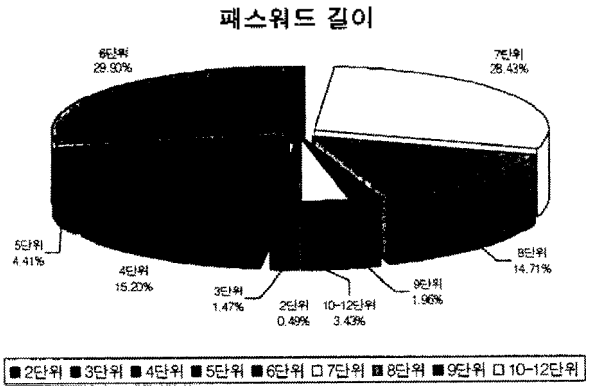
본 연구의 측정도구에서는 하나의 질문으로 얻고자 하는 정보가 충분하므로 복수가 아닌 단일 문항으로 질문을 하였다. Scarpello와 Campbell은 사용자의 만족도에 관한 태도를 측정하는데 있어서 한 항목을 측정하는 것이 여러 항목을 측정하는 것보다 더욱 더 포괄적인 측정이라는 것을 입증했다. Galletta와 Lederer(1989)는 사용자 정보 만족도의 포괄적인 측정을 위해서 세부적이고 독립적인 항목들의 합산은 타당하지가 않다고 하였다. 포괄적인 측정을 위해서는 포괄적인 질의가 보다 적절하다고 하였다.

Kappelman과 Mclean(1991)은 이러한 한 항목 접근법을 검정했고, Bailey와 Pearson, Ives et al(1991) 또한 단일항목과 다항목 도구를 검정하였는데, 단일항목이 포괄적인 사용자 만족도 구성에 있어서 가장 신뢰가 있고 타당한 방법이라 하였다. 이에 본 연구에서는 타당성이 입증된 Zviran과 Haga(1999)의 측정도구를 이용한 점, 두 번에 걸친 예비조사를 통한 보완 등으로 도구의 타당성을 입증하였다.

4.3. 가설 검증

4.3.1 패스워드 특성

(1) 패스워드 길이

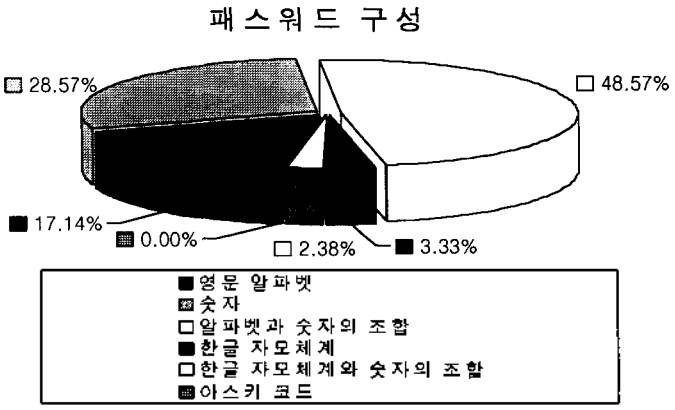


[그림Ⅳ-1] 패스워드 길이

[그림Ⅳ-1]에서 보듯이 패스워드의 길이가 6~7문자가 58.3%를 차지하고 있다. Menkus는 이상적인 문자(단위)의 수로 8문자를 권고하고 있는데, 21.6%의 응답자는 그이하의 문자수를 사용하고 있는 것으로 나타나고 있다. 참고로 Windows NT와 Unix는 패스워드 길이를 15문자까지 지원하고 있으며, RSA는 32문자까지 지원하고 있다. Morris와 Thompson은 패스워드의 길이가 짧으면 침입자로 하여금 사용자의 패스워드를 쉽게 알아낼 수 있게 한다라

고 제시하고 있다.

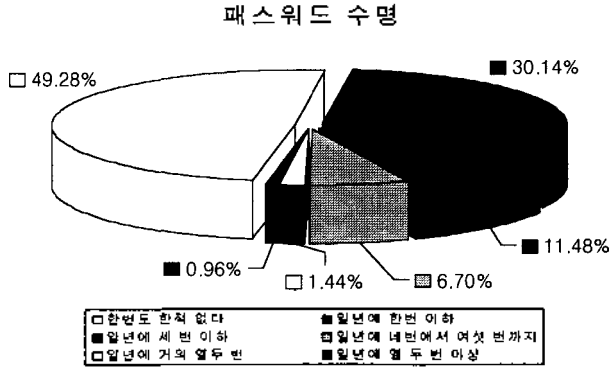
(2) 패스워드 구성



[그림Ⅳ-2] 패스워드 구성

[그림Ⅳ-2]에서 보면 응답자의 48.6%가 알파벳과 숫자의 조합(alphanumeric)을 그리고 28.6%가 숫자로 구성된 패스워드를 선호하였고, 한글 자모체계는4.0%, 한글 자모체계와 숫자의 조합은 3.3%의 선호도를 보였고, ASCII코드를 패스워드로 사용한다는 응답자는 아무도 없었다. 본 연구 결과를 보면, 구성할 수 있는 방법이 다양하게 있음에도 불구하고, 사용자들은 단지 알파벳과 숫자의 조합이라든가, 숫자만으로 구성된 패스워드를 사용한다는 Morris와 Thompson의 연구를 뒷받침해주고 있다.

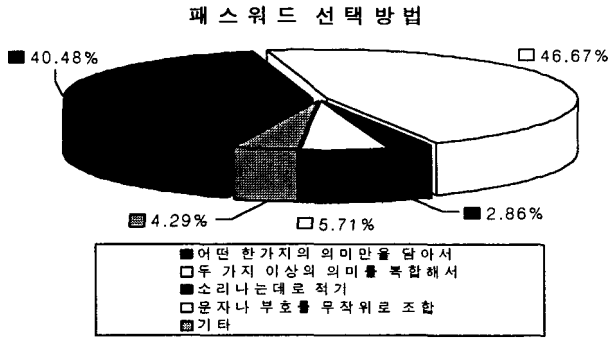
(3) 패스워드 수명



[그림Ⅳ-3] 패스워드 수명

정기적인 패스워드 변경은 기초적인 보안 수단이라 할 수 있다. Wood는 패스워드는 해마다 바꿔어야한다고 주장하였고, Menkus는 매달 바꿔어야 한다고 주장했다. 본 연구에서는 패스워드를 자주 변경해줌으로써 침입자로 하여금 패스워드의추측을 어렵게 한다고 했지만, [그림Ⅳ-3]에서 보면 49.3%가 한번도 한적없다, 30.1%가 단 한번 한적 있다라고 응답을 하였다.

(4) 패스워드 선택방법



[그림Ⅳ-4] 패스워드 선택방법

패스워드의 절충은 컴퓨터 게시판에 올라와 있는 정보, 즉 개인의 세부신상에 관한 추측에 의한 실마리, 그리고 체계적인 침입으로 인해 일어난다. 세부신상의 예를 들자면, 이름, 별명, 자식이름, 애완동물 이름, 약혼자, 자동차이름, 생일 등등을 들 수 있다. 이러한 항목은 사용자에게 특별한 의미를 두고 있기 때문에 기억력을 향상시켜준다. 어쨌든, 사용자의 세부신상에 관한 것을 패스워드로 선택하게 되면, 해커는 쉽게 해킹을 하게 된다. 그 이유는 그 해커가 해야할 추측이 제한되어있기 때문이다. [그림Ⅳ-4]는 응답자의 40.5%가 어떤 한가지 의미만을 담아서, 46.7%가 두 가지 이상의 의미를 복합해서 패스워드를 만들었다는 것을 보여주고 있다.

본 연구에서는 패스워드 특성과 저장방법간의 관계가 제 3의 변수에 의해 설명되어지는 것을 방지하기 위해 접속빈도를 통제변수로 두었다. [표Ⅳ-2]에서 보는 바와 같이 신뢰수준 90%에서 통제변수와 저장방법간에는 상관관계가 없는 것으로 나타났다.

[표Ⅳ-2] 통제변수와 저장방법간의 스피어만서열 상관계수

종속변수 / 통제변수	기억		기록	
접속빈도	상관계수	유의확률	상관계수	유의확률
	.071	0.097	.171	0.014

4.3.2. 가설 1의 검증

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

가설1의 검증에서 관련성은 인과관계를 의미하는 것은 아니다.

[표Ⅳ-3] 패스워드 특성과 데이터 속성간의 관련성

가설	데이터 속성	패스워드 특성	척도	검정기법	검정값	유의확률	연구가설
가설1a	민감도	길이	등간	ANOVA	2.199	.045	채택
가설1b	중요도	길이	등간	ANOVA	1.318	.251	기각
가설1c	민감도	구성	명목	Kruskal- Wallis	9.430	.151	기각
가설1d	중요도	구성	명목	Kruskal- Wallis	2.496	.869	기각
가설1e	민감도	수명	서열	Spearman's rho	.314	.000	채택
가설1f	중요도	수명	서열	Spearman's rho	.253	.000	채택
가설1g	민감도	선택방법	명목	Kruskal- Wallis	4.041	.671	기각
가설1h	중요도	선택방법	명목	Kruskal- Wallis	.825	.991	기각

[표Ⅳ-3]에서는 패스워드 특성과 데이터 속성간의 관련성(가설1)을 8가지 하위가설로 나누어 검증한 결과를 보여주고 있다.

패스워드의 길이와 데이터의 민감도[가설1a]간에는 관련성이 있다는 연구가설은 유의 확률 0.05보다 적으므로 95%신뢰수준에서 채택되었다. 그리고 패스워드의 길이와 중요도[가설1b]간에는 관련성이 있다는 연구가설은 유의확률 0.05보다 크므로 95% 신뢰수준에서 기각되었다. 본 연구결과를 보면, 사용자가 가지고 있는 데이터파일이 외부로의 유출시 민감하다고 생각 될 때에는 세심한 주의를 가지고 패스워드를 만들어야 한다는 가정을 입증하고 있다. 하지만 중요도는 길이와 상관없는 것으로 나타났다.

패스워드의 구성과 데이터의 민감도[가설1c] 그리고 패스워드의 구성과 중요도[가설1d]간에는 관련성이 있다는 연구가설은 유의확률 0.05보다 크므로 95%신뢰수준에서 기각되었다. 데이터 속성과 패스워드의 구성간에는 관련성이 없다는 결과가 나왔다.

패스워드의 수명(패스워드의 변경 빈도)과 데이터의 민감도[가설e] 그리고 패스워드의 수명과 데이터의 중요도[가설f]간에는 관련성이 있다는 연구가설은 유의확률 0.05보다 작으므로 95%신뢰수준에서 채택되었다. 데이터 속성과 패스워드 수명간에는 관련성이 있는 것으로 나타났으며, 패스워드를 선택할 때 추측하기 어렵게 해야하고, 민감하고 중요한 데이터를 보호하기 위해 패스워드를 자주 변경해야한다는 Highland의 연구를 입증해 주고 있다.

패스워드의 선택방법과 데이터의 민감도[가설1g] 그리고 패스워드의 선택방법과 데이터의 중요도[가설1h]간에는 관련성이 있다는 연구가설은 유의 확률 0.05보다 크므로 95%신뢰수준에서 기각되었다. 패스워드의 선택방법과 데이터의 속성간에는 관련성이 없는 것으로 나타났다. 이러한 결과가 나온 것은 사용자가 패스워드를 선택시 그들이 저장해야 할 자료가 얼마나 중요하고 외부로의 유출시 얼마나 민감한지에 관하여 인식이 부족한 탓이라고 추측이 된다. 일단 사용자들이 그들이 보호하려는 자료의 특성을 이해하게 된다면, 그들은 적절히 패스워드를 바꾸게 될 것이라 생각된다.

4.3.3. 가설 2의 검증

가설2 : 패스워드의 특성(길이, 구성, 수명, 그리고 선택방법)과 패스워드의 저장방법은 관련성이 있다.

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

[표Ⅳ-4] 패스워드 특성과 기억능력간의 관련성

독립변수	종속변수	계수(B)	유의도	연구가설
패스워드 길이	기억능력	.0545	.6061	기각
숫자		.0843	.6646	기각
알파벳과 숫자의 조합		.2255	.6646	기각
한글 자모 체계		-.4704	.6405	기각
한글 자모 체계와 숫자의 조합		1.3932	.0933	채택
두 가지 이상의 의미 조합		.4292	.0745	채택
소리나는데로 적기		.6386	.5567	기각
문자/부호의 무작위 조합		.3648	.5857	기각
패스워드 수명		.1441	.0812	채택

[표Ⅳ-4]의 검증 결과를 로지스틱 회귀식으로 나타내면 다음과 같다.

패스워드의 기억능력 = 1.2212 + .0545(패스워드 길이) + .0843(숫자) + .2255(알파벳과 숫자의 조합) - .4704(한글 자모 체계) + 1.3932(한글 자모 체계와 숫자의 조합) +.4292(두 가지 이상의 의미 조합) +.6386(소리나는데로 적기) +.3648(문자/부호의 무작위 조합) +.1441(패스워드 수명)

위의 식에 대한 유의 확률은 .0611로서 10%의 유의 수준에서 통계적으로 유의함을 보여주고 있다. 따라서 패스워드 특성이 기억능력에 영향을 미치는 것으로 나타났다. 패스워드의 구성 중 한글 자모 체계와 숫자의 조합, 패스워드의 선택방법 중 두 가지 이상의 의미 조합 그리고 패스워드의 수명이 기억능력에 영향을 미치는 것으로 나타났다.

[표Ⅳ-5] 패스워드 특성과 기록간의 관련성

독립변수	종속변수	계수(B)	유의도	연구가설
패스워드 길이	기록	-.0128	.9076	기각
숫자		-.6292	.0884	채택
알파벳과 숫자의 조합		-.6451	.2300	기각
한글 자모 체계		-1.3154	.2391	기각
한글 자모 체계와 숫자의 조합		-.6634	.6088	기각
두 가지 이상의 의미 조합		.8248	.0674	채택
소리나는데로 적기		1.1243	.3613	기각
문자/부호의 무작위 조합		.6044	.3838	기각
패스워드 수명		.3984	.0081	채택

[표Ⅳ-5]의 검증 결과를 로지스틱 회귀식으로 나타내면 다음과 같다.

패스워드의 기록 = 2.7522 - .0128(패스워드의 길이) - .6292(숫자) - .6451(알파벳과 숫자의 조합) - 1.3154(한글 자모 체계) - .6634(한글 자모 체계아 숫자의 조합) + .8248(두 가지 이상의 의미 조합) + 1.1243(소리나는데로 적기) + .6044(문자/부호의 무작위 조합) + .3984(패스워드의 수명)

위의 식에 대한 유의 확률은 .0731로서 10%의 유의 수준에서 통계적으로 유의함을 보여주고 있다. 따라서 패스워드 특성이 기록에 영향을 미치는 것으로 나타났다. 패스워드의 구성 중 숫자, 패스워드의 선택방법 중 두 가지 이상의 의미 조합 그리고 패스워드의 수명이 패스워드의 기록에 영향을 미치는 것으로 나타났다.

Ⅴ. 사용자의 보안 의식

사용자는 패스워드를 생성할 때 어떠한 제한으로 만들 것인가를 결정해야 하며 패스워드 시스템을 스스로 보호해야 한다는 의무감을 가져야한다. 누군가에 의해 보안의 위협이 있을 때에는 시스템 보안관리자에게 즉시 보고하는 자세가 필요하다. 또한 패스워드를 잊거나 타인에게 노출되지 않도록 세심한 주의를 가질 필요가 있다.

다음은 사용자가 패스워드를 선택하는 경우 주의해야할 사항들이다.

4.1. 패스워드를 기억해야 한다.

사용자는 시스템에 로그인을 할 때마다 패스워드를 입력해야 하므로 자신의 패스워드를 꼭 알고 있어야 한다. 패스워드를 어딘가에 기록할 수도 있지만 분실의 위험이 따르기 때문에 그 기억장소에 대한 보안이 필요하게 된다. 따라서 반드시 기억해야 한다.

4.2. 패스워드의 추측 가능성을 줄여야 한다.

패스워드를 사용자가 선택해서 만들게 되는 경우 타인에 의한 추측이 어렵도록 해야 한다. 일반 사용자들은 기억하기 쉽도록 하기 위해 자신의 신상과 관련된 생일, 전화번호, 주민등록번호, 주소, 혹은 주변인물의 이름, 생일 등을 이용하여 패스워드를 만드는 경향이 있다. 이런 경우 불순한 의도를 가진자가 그 사용자의 정보를 많이 가지고 있다면 그 사용자가 속한 조직에 미치는 영향은 상당할 것이다. 따라서 사용자들은 무작위로 패스워드를 선택할 필요가 있다.

4.3. 패스워드를 자주 변경해야 한다.

패스워드의 노출 가능성이 있을 때 사용자는 즉시 패스워드를 바꾸어야한다. 또한 패스워드를 자주 바꾸어 줌으로써 그 노출 가능성을 줄일 수 있다. 마이크로 소프트 엔티에서는 시스템 관리자가 패스워드의 수명을 제한 할 수 있다.

4.4. 패스워드를 입력할 때에는 타인에게 노출되어서는 안된다.

패스워드를 시스템에 입력하는 전형적인 방법은 키보드를 이용하는 것이다. 만약 키보드 입력이 느린 경우 타인에 의해 노출될 수가 있으므로 반드시 주위를 둘러보고 타이핑을 빨리 할 필요가 있다.

4.5. 패스워드의 생생 및 분배

초기 시스템 로그인시 일반적으로 사용자는 패스워드를 생성하도록 요구되며 이 때 사용자는 반드시 패스워드를 만들어야 한다. 또한 시스템 관리자에 의해 패스워드를 할당 받는 경우 사용자는 빨리 자신이 선택한 패스워드로 바꾸어야 한다.

VI. 결론 및 한계점

패스워드의 사용은 시스템 보안에 있어서 일부분에 지나지 않지만, 대부분의 시스템에서는 패스워드를 이용해서 사용자를 인증하고 자료에 대한 접근을 통제하고 있으므로 패스워드의 사용법은 아주 중요한 문제라고 할 수 있다.

본 연구에서는 사용자 선택 패스워드의 특성들을 실증적으로 평가하고, 이러한 패스워드의 특성들과 데이터의 속성 그리고 패스워드의 특성들과 패스워드의 저장방법간의 관련성을 알아보았다.

본 연구의 시사점을 살펴보면 다음과 같다.

첫째, 사용자 선택 패스워드는 비교적 추측하기 쉬운 것으로 나타났다. 둘째, 사용자가 가지고 있는 데이터 파일의 민감도에 따라 패스워드의 길이는 달라질 수 있다는 것을 보여 주었다. 또한 패스워도의 수명은 데이터의 중요도와 민감도에 의해 영향을 받는다는 사실은 매우 중요하다. 만약 사용자가 가지고 있는 데이터 파일이 매우 중요하고 민감한 데이터파일이라면 더욱더 자주 패스워드를 변경하게 될 것이다. 셋째, 패스워드의 특성이 기억능력과 기록에 영향을 미치는 것으로 나타났다.

최근에 정보시스템 보안에 대한 경영진의 관심은 크게 감소한 것으로 나타났다. 1981년에 발표된 Ball과 Harris의 연구에서 보면 가장 중요하게 여기는 정보관리의 주제로서 자료 보안은 12번째의 순위였다. 그리고 1986년의 Neiderman, Brancheau,그리고 Wetherbe의 연구에서는 19위였고, 1995년 Brancheau는 그의 연구에서 MIS중역진들은 보안에 관한 이슈를 MIS의 상위 20개에서 제외시켰다라고 했는데, 이는 보안에 대한 중요성이 줄어들었거나 혹은 더욱더 강력한 시스템 통제가 이루어졌다 것을 의미한다라고 제시했다.

외부침입자 혹은 내부침입자에 의한 해킹의 피해가 기하급수적으로 증가하고 있는 오늘날, 모든 해킹의 첫 관문이라고 할 수 있는 패스워드에 대한 보안 교육이 철저하여야 하고, 조직은 패스워드의 선택과 사용에 관한 규범을 제정해야 할 것으로 본다.

본 연구는 앞에서 언급한 다양한 시사점을 지니고 있음에도 불구하고 연구결과의 해석을 제한하는 몇 가지의 한계점을 포함하고 있다.

첫째, 측정도구에 있어서 단일 항목으로 한 변수를 설명하는 것으로 국한되어 있으므로 정확한 측정과 설문지의 신뢰성과 타당성을 높이기 위한 정교한 측정방법의 개발이 요구된다. 둘째, 본 연구에서 제시된 연구모형과 척도는 외국 문헌을 바탕으로 개발되었으므로, 연구결과를 한국의 상황에 적용하기 위해서는 한국적 상황에 더욱 적합한 연구모형과 측정항목의 개발이 요구된다. 셋째, 본 연구는 표본의 대표성에 관련된 문제점을 지니고 있다. 원칙적으로는 전국적인 모집단을 대표할 수 있는 엄밀한 확률표본이 선정되어야 함에도 불구하고 표본이 일부지역에 국한되어 추출되었다. 또한 다양한 조직에서 이루어진다면 더욱 더 좋은 연구가 될 것이다. 넷째, 보안정책이 잘 정립된 조직과 그렇지 못한 조직간의 패스워드 보안에 관한 의식에는 큰 차이가 있을 것이다. 실제로 본 논문에서 가설의 기각이 많은 이유 중 하나는 보안에 대한 의식화가 제대로 이루어지지 않았기 때문으로 보여진다.

참 고 문 헌

김재문, 개선된 패스워드 보안 방법 및 구현, 경북대학교 석사학위논문, 1988.

김종구, System Security에 관한 연구, 고려대학교 경영대학원 석사학위 논문, 1987.

박우일, 자동생성 패스워드에 의한 시스템 접근통제에 관한 연구, 숭실대학교 정보과학대학원 석사학위논문, 1990.

신종태, 김대호 자동패스워드의 생성 시스템에 관한 연구, 한국통신보호학회지, 제 4권 제4호, 1994, pp. 5-11.

이필중, 문희철, 패스워드 시스템의 보안에 관한 고찰, 한국통신보호학회지, 제 1권 제1호, 1991, pp. 109-118.

임채호 외, 98 정보시스템 해킹현황 및 대응, 한국정보보호센터, 1998.

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

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

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

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

Brancheau, J.C. and Wetherbe, J.C., "Key issues in information systems management," *MIS Quarterly*, Vol. 12, No. 1, 1987, pp. 23-36.

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

Edward J.G. and G. Lawrence S., *Information Systems Success Measurement*, IDEA GROUP PUBLISHING, 1998, pp. 66-78.

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.

Hoffer, J. and Straub, D.W., "The 9 to 5 underground: are you policing computer crimes?", *Sloan Management Review*, Vol. 30, No. 4, 1989. 11. pp. 35-43.

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

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

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

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

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

Porter, S.N., "A password extension for human factors.", *Computers and Security*, Vol. 1, No. 1, 1982, pp. 54-56.

Seely, D., "Password cracking : a game of wits.", *Communications of the ACM*, Vol. 32, No. 6, 1989.

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

Stoll, C., "Stalking the willy hacker.", *Communications of the ACM*, Vol. 31, No. 5, 1988, pp. 484-497.

Straub, D.W. and Nance, W.D., "Discovering and disciplining computer abuse in organizations : a field study", *MIS Quarterly*, Vol. 14, No. 1, 1990, pp. 45-60.

Turban, E., McLean, E., Wetherbe, J., *Information Technology for Management*, John Wiley & Sons Inc., New York, 1999.

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

Wu, T.C. and Sung, H. S., "Authenticating passwords over an insecure channel.", *Computers and Security*, Vol. 15, No. 5, 1996, pp. 431-439.

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

Zviran, M. and Haga, W.J., "Password Security : An Empirical Study", *Journal of Management Information Systems*, Vol. 15, No. 4, 1999, pp. 161-185.

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