정보 시스템 위험과 패스워드 특성간의 관계에 대한 연구

(A Study on Relationships Between Information Systems Risk and Password Characteristics)

오 창 규*, 김 종 기**, 심 윤 주**
(Chang-Gyu Oh, Jong-Ki Kim, Yun-Ju Shim)

요 약 정보시스템의 역할이 증대되고 있는 현시점에서 정보 자원에 대한 효과적인 보호는 매우 중요하다. 인터넷의 영향으로 정보 시스템의 개방화와 접속성의 증대로 인해 보다 많은 위협과 취약성에 노출되어 있으며 이들을 관리하는 것 또한 매우 중요한 이슈가 된다. 특히 정보 시스템의 사용을 위한 수단인 패스워드의 급증은 정보 보호에 더 많은 주의를 요하게 되었다. 본 연구에서는 위험분석에 사용되는 자산, 위협, 취약성 등으로부터 도출된 위험의 발생 가능성이 실제 지각된 위험에 어떠한 영향력을 행사하는가를 살펴보고, 여기서 도출된 위험이 정보보호를 위한 패스워드 특성에 어떠한 영향관계를 가지는가를 분석하였다. 이를 통해 패스워드의 효과적인 사용과 보안 대책을 수립하기 위한 방안을 제시하였다.

Abstract Information security becomes a critical attribute to corporate information systems as increased strategic and operational reliance on information systems. Current proliferation of password requires more attention on information security because its nature of external connection with password user makes information systems more vulnerable from various threats are an important element of information systems management. This study focused on two issues : (1) the relationships between risk management factors(asset, threat, vulnerability) and risk level affected by threat, (2) the relationships between risk level and key password characteristics(length, composition, lifetime, selection method).

1. 서 론

오늘날 대부분의 컴퓨터가 네트워크로 연결된 상태에서 패스워드가 비인가자에게 노출됨으로써 입게되는 자산의 손실과 사회적 피해는 엄청나다. 특히 여러 웹사이트를 접속할 때 자신의 편리를 위해서 다른 웹사이트에서도 동일한 ID와 패스워드로 등록해서 사용할 경우, 한 곳에서의 패스워드 유출은 연쇄적인 보안사고를 일으킬 수도 있다[12]. 따라서 자신의 정보보호 및 정보자산을 안전하게 관리하기 위해서는 이들을 보호하기 위한 대응 방안을 탐색해야 하는데 이것이 위험관리가 된다[15].

이에 본 연구에서는 단편적인 위험을 살펴보는 것이 아니라 정보보호를 위한 위험관리 측면에서 위험을 규명하고자 한다. 즉, 위험분석에 사용되는 자산, 위협, 취약성 등으로부터 도출된 위험의 발생 가능성이 실제 지각된 위험에 어떠한 영향력을 행사하는가를 살펴보고, 여기서 도출된 위험이 정보보호를 위한 패스워드 특성에 어떠한 영향관계를 가지는가를 분석한다. 이를 통해 패스워드의 효과적인 사용과 보안 대책을 수립하기 위한 방안을 제시하고자 한다.

2. 문헌연구

위험의 발생 가능성이 지각된 실제 위험과 어떤 관

* 부산외국어대학교 국제통상연구소
** 부산대학교 경영학부

계를 가지며, 사용자가 인지하는 위험에 따라 패스워드 특성이 어떻게 결정되는가를 규명하기 위해 위험과 패스워드에 대한 문헌연구를 실시하였다. 이 때의 위험은 정보 시스템 보안관리 측면에서의 위험관리와 위험분석을 통해 살펴보았으며, 패스워드 측면은 패스워드 시스템 보안관리 측면에서 고려되는 패스워드 특성을 중심으로 고찰하였다.

2.1. 정보 시스템 위험과 위험관리

위험(risk)이라는 것은 위협(threat)이 현실적으로 발생하여 조직에 부정적인 영향을 미칠 수 있는 가능성을 구체화한 것으로 조직의 목적에 불이익이나 손해를 초래한다[8]. 위험은 보안 위협과 취약성의 결합으로 구성된 자산이나 시스템과 관련된 잠재적인 위험도 포함되며, 조직내 존재하는 정보 자산(asset), 위협(threat), 그리고 시스템 취약성(vulnerability)의 변경이 위험을 초래한다[1,2,34].

특히 정보 시스템 위험을 산출하기 위해서는 정보자산에 대해 파악된 취약성과 이와 관계된 위협의 발생 가능성, 그리고 위협 발생시 일어나는 손실(loss)을 고려해야 한다[20]. 또한 사용자가 실제로 지각하는 정보자산에 대한 위험은 자산에 해를 입힐 수 있는 가능한 모든 것들을 규정하고 분류했을 때 이들의 발생 확률 또는 발생 빈도와 자산에 해를 입히는 정도를 통해서 알 수 있다[2]. 이렇듯 위험을 최소화하고 조직의 정보자산을 보호하기 위해서는 효과적인 위험관리가 요구된다[37].

위험관리는 조직내 정보보호 및 정보자산을 안전하게 관리하기 위한 접근 방법으로서 발생 가능한 손실을 최소화하기 위해 이들을 식별하고 추정하고 통제하는 것이다[15]. 효과적인 위험관리가 달성되기 위해서는 조직의 보안방침과 목적에 부합하는 구현전략과 시스템 보안 방침이 도출되어야 한다. 이 과정에서 다양한 보안대책이 고려되고 비용·효과 분석이 수행된다.

2.2. 위험분석과 구성 요소

위험관리에서 핵심적인 활동이 위험분석인데, 위험을 식별하고 분석을 수행함으로써 위험 수준을 낮추기 위한 보안대책을 강구하는 것이다[10]. 즉, 위험분석은 서비스중인 정보 시스템의 운영상황과 정보 시스템의 가용성(availability), 무결성(integrity), 기밀성(confidentiality)에 관한 위험의 분석결과 뿐만 아니라 필요한 대응책을 산출하고 효과를 측정하여 관리자로 하여금 의사결정 기준을 제공하는 일련의 과정이다[24]. 따라서 조직에서 사용하는 정보자산을 정보 시스템을 중심으로 파악하고 존재하는 위협을 분석하여 보안대책에 요구되는 부분이 어디인지를 살펴야 한다.

보안사고가 발생한 이후의 조치보다는 지속적인 위험분석을 통해 비용 효과적으로 위험을 감소하거나 받아들이는 수준의 보호대책을 선정할 수 있다. 위험의 발생 가능성으로부터 위험을 규정하고, 위험에 영향을 미치는 요인을 도출하기 위해 위험분석의 구성요소를 살펴보았다. 위험분석은 자산 분석, 위협 분석, 그리고 취약성 분석으로 구성된다[26,35].

첫째, 자산 분석은 정보 시스템내의 모든 자산을 식별하고 분류해서 가치를 평가하는 것이다. 만일 정보 시스템의 보안을 위해 자산 파악을 정확하게 수행하지 못한다면 성공적인 위험 보안조치에 허점을 제공하고 올바른 위험분석을 수행할 수 없다. 그러나 자산의 식별은 상당한 시간과 비용이 요구되기에 구체적인 분석수준에 맞게 설정되어 결정해야 한다[2]. 오늘날 인터넷 기반의 네트워크 환경에 초점을 맞출 때 전산망을 통해 송·수신되는 데이터가 우선 순위가 높은 자산으로 간주되고 있다[26]. 이 때 데이터 자산의 속성은 크게 두 가지로 나눌 수 있는데 민감도(sensitivity)와 중요도(importance)이다[22]. 민감도라는 것은 데이터의 내용이 다른 사람들에게 공개될 때 문제가 발생할 수 있는 정도를 나타낸다. 중요도라는 것은 개인 사용자에 대한 데이터의 고유한 가치를 의미한다.

둘째, 위협 분석은 조직이나 자산에 해를 끼칠 수 있는 가능한 위협들을 탐색하고 적절한 방법으로 분류하여 해를 입히는 정도를 평가하는 것이다[10]. 이 때 위협은 위험분석을 위해 고려되는 자산에 해를 주거나 위험을 발생시킬 수 있는 조건, 상황, 원인 제공자로 정의될 수 있다[25]. 정보 시스템의 보안에 대한 위협요소를 파악하기 위한 보안위협 모형이 존재한다. Crockford(1980)는 정보 시스템 보안에 대한 위협 모형을 위협 요인, 상황 요인, 결과 및 자원으로 구성하였다. Parker(1981)는 원천, 동기, 행위, 그리고 결과를 포함시켜 정보 시스템 보안 위협 모형을 제안하였다. Loch 등(1992)은 원천, 가해자, 의도, 그리고 결과를 정보 시스템의 보안위협의 구성요소로 간주하였다.

셋째, 취약성 분석이다. 위험을 완전하게 파악하기 위해서는 취약성과 관련된 위협의 발생 가능성을 살

펴야 위험의 발생 가능성과 손실 정도를 예측할 수 있다[19]. 따라서 취약성 분석에 대한 논의는 필수적이다. 취약성이라는 것은 정보 시스템에 손해를 끼치는 원인이 될 수 있는 조직, 물리적 배치, 절차, 직원, 하드웨어 및 소프트웨어, 정보 등과 같은 자산이 잠재적으로 가지고 있는 약점으로 외부의 위협요인에 의해 현실화된 문제를 의미한다[2]. 즉, 취약성 자체가 손상을 초래하는 것은 아니지만, 위협이 자산에 영향을 줄 수 있는 조건은 제공한다. 따라서 취약성 분석이라는 것은 이와 같은 약점을 확인하고 분류하여 위협을 감소시키도록 하는 것이다[1].

2.3. 정보 시스템의 식별 및 인증 수단

사용자가 정보 시스템에 접근하기 위해 요구되는 인증 및 식별 수단으로 ① 사용자 ID와 패스워드를 사용해서 그 사람만이 알고 있는 사항을 이용하는 방법, ② 메모리 토큰(memory token)이나 스마트 토큰(smart token)과 같은 개인 신분카드나 키를 사용하는 방법, ③ 목소리나 지문 등과 같이 그 사람의 생체학적 특성을 이용하는 방법, ④ 사람의 무의식적인 행동양식을 이용하는 방법 등이 존재한다[4,6]. 신체적 특성의 유일성 때문에 세 번째와 네 번째 방법이 이론적으로 완벽한 것으로 생각되나, 이 방법은 구현이나 유지 및 관리 비용 측면으로 보편화 되어있지는 않다. 두 번째 방법은 개인 신분 카드나 키를 분실했을 경우 해당 기간 동안 인지할 수 없다는 단점이 있다. 또 개인 신분카드나 키는 불법적으로 복사될 수도 있다. 이런 문제들 때문에 사용자의 식별 및 인증, 그리고 주요 자원에 대한 접근제어를 위한 기초적인 보안장치가 패스워드 시스템이다[4].

이러한 패스워드 시스템은 다른 고도의 컴퓨터 보호장치 기술과 비교할 때 비교적 용이하게 구현되고 운영될 수 있으므로 가장 보편적으로 이용되고 있다[11]. 패스워드 시스템은 사용자가 사용자 ID와 패스워드 또는 암호구(passphrase), 개인식별 번호 등의 입력을 요구한다. 시스템은 입력된 패스워드와 해당 사용자 ID에 대하여 미리 저장된 패스워드를 비교하고 일치한 경우 사용자에 대한 인증이 이루어지고 접근이 허용된다.

2.4. 패스워드의 특성

정보 시스템의 정보보호를 위한 대표적인 사용자 식별 및 인증 수단으로 사용자 ID와 쌍을 이루는 패스워드는 길이, 구성, 수명, 그리고 선택 방법에서 서로 상이한 특성을 가지고 있다.

첫째, 패스워드의 길이는 패스워드 공격에 대한 방어력의 평가가 되며 다음 식에 의해 허용될 수 있는 패스워드의 수가 계산될 수 있다[14]. 패스워드 길이

$$S = Z^{l} \quad \begin{pmatrix} S = \text{가능한 패스워드의 수} \\ Z = \text{패스워드 주기} \\ l = \text{패스워드 길이} \end{pmatrix}$$

는 시스템 운영자와 보안 관리자에 의해 선택되지만, 일반적으로 보호하는 자료의 가치 또는 민감성에 비례하여 결정된다. 패스워드 길이는 구성 가능 문자와 더불어 시행 착오 공격에 대한 패스워드 시스템의 보안을 평가하는 기준이 된다. 일반적으로 5자리와 6자리의 패스워드 길이가 가장 인기가 높았으며, 대부분 4자리에서 7자리 패스워드를 사용하는 경향이 존재한다[16,18,21,33]. 또한 가장 이상적인 패스워드 길이는 6자리에서 8자리의 문자와 숫자의 조합이다[28].

둘째, 패스워드 구성이다. 패스워드 구성가능 문자는 입력장치, 저장방법 그리고 입력된 패스워드와 저장된 패스워드를 비교하는 방법과 관련된다[7]. 이 때, 생성 가능한 패스워드의 수는 시행착오 공격으로 알아낼 수 없을 만큼 커야 하며 저장이 가능하고 간편하게 입력될 수 있어야 한다[36]. 일반적으로 영어 알파벳으로만 이루어진 패스워드는 흔히 알고 있는 영어단어를 이용하는 경우가 많으므로 안전하지 못하다. 따라서 영어 알파벳에 숫자를 넣거나 그래픽 문자를 이용하면 보다 안전하게 보호할 수 있다[11].

일련의 문자들 집합에서 사용자가 선택한 패스워드의 구성 문자들을 검정하는 프로그램을 통해 패스워드를 추적하는데 걸리는 시간을 추정할 수 있다. <표 1>은 PDP-11/70에서 다양한 문자집단으로부터 n길이의 모든 가능한 문자열을 검정할 수 있는데 걸리는 시간을 추정하고 있다[30]. 이를 통해 패스워드 구성과 정보보호간에 밀접한 관련성이 존재함을 알 수 있다.

셋째, 패스워드 수명을 살펴보면, 주기적인 패스워드의 변경은 보안성을 높이는데 기초가 된다[18,25].

패스워드의 수명주기에 영향을 미치는 요인들로서 패스워드 교체에 드는 비용, 노출되었을 때의 위험, 분배시의 위험, 패스워드를 추측할 수 있는 확률, 사용하는 횟수, 시행착오 방법을 통해 찾아낼 수 있는 확률 등이 존재한다[18]. 통상적으로 패스워드 사용자는 패스워드를 자주 변경하지 않는 경향이 존재한다.

그러나 패스워드는 주기적으로 바뀌어야 하며 노출되었다고 의심이 가거나 확신이 설 때에는 즉시 바꾸어야 한다. 또한 패스워드 시스템은 사용자나 보안 관리자가 패스워드를 교환할 수 있도록 해야 한다.

<표 1> PDP-11/70에서 패스워드를 추적하는데 소요되는 시간

길이	영문 소문자 (26개)	영문 소문자와 10진수 (36개)	철자와 숫자의 조합	인쇄가능 문자 (95개)	모든 ASCII 문자 (128개)
1	30 msec	40 msec	80 msec	120 msec	160 msec
2	800 msec	2 sec	5 sec	11 sec	20 sec
3	22 sec	58 sec	5 min	17 min	44 min
4	10 min	35 min	5 hrs	28 hrs	93 hrs
5	4 hrs	21 hrs	318 hrs	113 days	500 days
6	107 hrs	760 hrs	22 yrs	29 yrs	174 yrs

패스워드가 추측될 확률을 수식으로 표현하면 다음과 같다[25].

$$P = \frac{L \cdot R}{S}$$

(P = 변경주기 이내 추측될 확률, L = 패스워드 수명, R = 단위 시간당 추측될 수, S = 가능한 패스워드의 수)

상기와 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 적게 드는 방향으로 수명을 결정한다. 또한, 자동화된 패스워드 시스템은 보안 관리자가 자신을 인증한 후 사용자의 패스워드를 지우거나 교체할 수 있게 허락해야 하며, 패스워드를 새로 만들거나 교체했을 때의 기록을 가져야 한다[11].

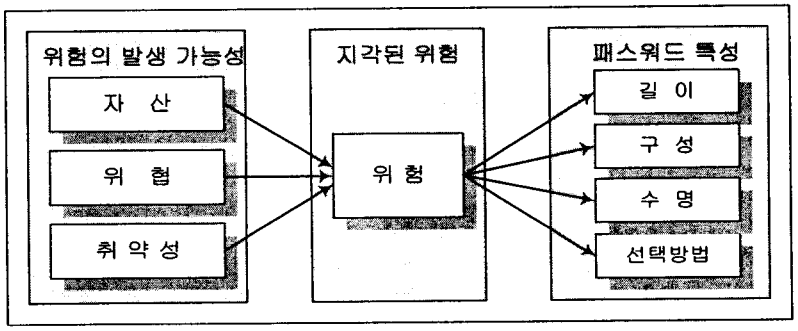
넷째, 패스워드 선택 방법이다. 패스워드의 침해는 생일이나 별명 등과 같이 사용자의 세부 신상에 관한 추측, 환경으로부터의 단서, 혹은 체계적인 침입 방법 등을 통해 이루어진다[13]. 특히 세부 신상에 관한 패스워드는 해커가 수행하는 추측이 제한되어 있기에 가장 쉽게 침해사고가 발생할 수 있다[25]. Morris와 Thompson(1979)은 유닉스 환경에서 사용자 패스워드 선택 방법에 대한 특성을 연구하였고, 3000개의 패스워드 중 85%이상이 영어사전에 있는 단어나 이러한 단어를 역순으로 배열하였거나, 이름, 거리, 도시, 전화번호 등으로 구성되어 있다는 것을 밝혔다.

패스워드의 추측 난해성과 사용자의 패스워드 기억 용이성간에는 상반관계가 존재한다. 예를 들어, 패스워드의 가장 안전한 형태로서 무작위 문자열이 제시되는데 이는 타인이 추측하기에는 힘들지만 자신이 기억하는 것 또한 어렵게 된다. 이에 패스워드가 누출이 되더라도 무용지물이 되도록 하기 위해 일회용 암호기반 패스워드가 추천되기도 한다.

3. 연구모형 및 가설

정보보호를 위한 위험관리 측면에서 위험에 따라 패스워드 특성에 어떠한 영향력이 행사되는지를 규명하기 위해 <그림 1>과 같은 연구 모형을 제시하였다. 모형으로부터 알 수 있듯이 본 연구는 크게 두 부분의 가설로 이루어져 있다.

먼저 정보보호를 위한 위험관리 측면에서 위험을 규명하고자 하였다[37]. 관리차원에서 보안에 대한 접근을 수행하기 위해서는 위험의 발생 가능성으로부터 지각된 위험이 규명되어야 한다[15]. 위험은 자산에 대한 보안 위협과 취약성의 결합으로 구성되기에, 이들 간의 관계로부터 위험을 규명한 Smith(1996)의 연구에서 구성개념을 도출하였다. 이러한 구성개념들간



<그림 1> 제안된 연구모형

의 관계는 Rainer 등(1991)과 Kim(1995)의 연구에서도 적용되었다. 위험분석을 위한 요인으로서 사용자 개인 측면에서 위험에 영향을 미치는 요인으로 자산과 취약성이, 그리고 사용자 외적 측면에서는 외부 위협이 사용되었다. 이에 본 연구에서는 위험분석을 통해 위험을 인식하는 부분으로 자산·위협·취약성의 발생 가능성에 따라 위험을 평가하고, 실제 지각된 위험과의 관계를 비교 분석할 수 있도록 관계를 설정하였다.

다음은 위험 영향 평가를 통해 도출된 지각된 위험이 패스워드 특성에 어떠한 영향력을 행사하는지를 밝히는 부분이다. 본 연구모형에서 사용된 패스워드 특성 변수인 패스워드 길이, 구성, 수명, 그리고 선택방법은 Highland(1997)와 Zviran과 Haga(1999)의 연구로부터 도출되었다. Zviran과 Haga(1999)는 데이터 속성으로 민감도와 중요도를 선정하여 패스워드 특성과의 관련성을 규명하였다. 그 결과 패스워드 길이와 유의적인 관계가 존재함을 밝혔다. Highland(1997)는 패스워드 침해를 막기위한 방안으로 패스워드 특성을 연구하였으며, 패스워드 선택방법에 따라 해킹을 당하는 정도를 줄일 수 있음을 주장하였다. 이러한 연구를 토대로 정경수 등(2001)은 보안 모형과 패스워드 특성과의 관련성을 인구통계적 변인에 따라 검증하였고, 패스워드 구성의 중요성을 피력하였다. Menkus(1988)는 위험을 최소화하기 위한 이상적인 패스워드 길이와 패스워드 수명에 대한 연구를 수행하였다. 그리고 Wood(1983)는 패스워드 수명에 영향을 미치는 요인을 탐색하여, 위험과 패스워드 수명과의 관련성을 밝힌바 있다.

이에 본 연구에서는 위험분석을 통해 확인된 요소(자산, 위협, 취약성)들의 발생 가능성과 실제 위험과의 차이를 검증하고, 이렇게 규명된 위험이 패스워드 길이, 패스워드 구성, 패스워드 수명, 그리고 패스워드 선택방법 등에 어떠한 영향력을 행사하는 지를 밝히고자 하였다. 이를 토대로 안전한 패스워드 관리를 위한 현실적인 시사점을 제공하고자 하였다.

4. 데이터 분석 및 가설 검증

4.1. 자료 수집과 표본 구성

본 연구의 목적은 위험이 발생할 가능성과 사용자가 지각하는 실제 위험과의 관계로부터 도출된 위험이 패스워드 특성에 어떠한 영향력을 행사하는지를 규명하는 것이다. 보다 효과적인 규명을 위해 상대적으로 낮은 수준의 정보보호 의식을 가지고 있는 단순 정보이용 웹사이트에서 지각하는 위험과 패스워드, 그리고 보다 높은 수준의 정보보호 의식을 가지고 있는 이뱅킹(e-banking) 웹사이트에서 지각하는 위험과 패스워드에 대해 사용자 지각 데이터를 수집하였다. 이는 사전 조사를 통해 중요도를 구분한 결과에 바탕을 둔 것이었다. 또한 설문에 대한 응답을 위해 일정기간 동안 지속적인 방문을 수행한 경험을 가지고 있는 단순 정보이용 웹사이트와 이뱅킹 웹사이트가 선정되도록 하였다.

설문 응답자들은 정보보호에 대한 기본적인 의식은 가지고 있으며, 단순 정보이용 웹사이트와 이뱅킹 웹사이트를 모두 사용하고 있는 부산·경남 지역의 학생과 직장인으로 구성되었다. 2002년 10월 21부터 약 1개월 동안 총 171부의 설문이 회수되어 분석에 이용되었으며, 성비는 남자 116명(67.8%), 여자 55명(32.2%)이었다. 또한 컴퓨터 사용 경험을 볼 때, 1년~2년은 10명(5.8%), 3년~4년은 34명(29.9%), 5년~6년은 41명(24.0%), 7년~8년은 40명(23.4%), 그리고 9년 이상은 46명(26.9%)으로 집계되었다.

설문 응답자들이 패스워드 시스템에서 사용하는 패

<표 2> 응답자들의 전체 패스워드 개수와 사용 방법

패스워드 사용방법	전부 같은 패스워드	33	19.3
	일부 같은 패스워드	136	79.5
	전부 다른 패스워드	2	1.2
사용하는 전체 패스워드 개수	1개 ~ 5개	126	73.7
	6개 ~ 10개	28	16.4
	11개 ~ 15개	10	5.8
	16개 ~ 20개	4	2.3
	20개 이상	3	1.8

스워드 개수와 사용 방법과 관련된 기술통계량을 <표 2>에 요약하였다. 사전 조사에서 대부분의 사람들이 접속하는 시스템의 중요도에 따라 패스워드를 다르게 사용하고 있음을 발견하였다. 그리고 본 연구에서 중요도에 따른 패스워드 선택 방법을 고찰한 결과 79.5%(136명)가 일부는 같고 일부는 다른 패스워드를 사용함으로써 기억하기 용이하도록 자신이 생각하는 척도에 따라 패스워드를 선택함을 알 수 있었다. 그러나 결과표로부터 알 수 있듯이 대부분의 사람들(73.7%)이 5개 이하의 패스워드로 자신이 사용하는 모든 시스템에 접속하고 있으며, 비록 많은 숫자는 아닐지라도 모든 시스템에 동일한 패스워드를 사용하고 있는 사람도 19.3%에 달하고 있다. 이를 통해 개인의 정보보호를 위한 완벽한 패스워드 관리는 이루어지고 있지 않음이 드러났으며, 위험의 지각에 따라 패스워드가 가지는 특성을 밝히는 본 연구를 통해서 현재 사용자들에게 패스워드 시스템 관리에 대한 시사점을 제공할 수 있다.

4.2. 측정 도구의 평가

선행연구의 고찰을 통해 도출된 개념을 측정하고, 연구모형에 대한 가설 검증을 위해 측정도구의 신뢰성 평가는 수행되어져야 한다. 본 연구에서 수행된 신뢰성 평가는 내용 타당성(content validity), 개념 타당성(construct validity), 내적 일관성(internal consistency) 등이다.

<표 3> 측정 변수의 조작화

변 수		측 정 항 목		척 도	참 고 문 헌
위험의 발생 가능성	자 산	· 자산의 중요도(악용으로 인한 피해정도) · 자신의 민감도(데이터의 고유가치)	[asst1] [asst2]	리커트 척도	Wood(1983) Jobusch & Oldhoeft(1989) Zviran & Haga(1999)
	위 협	· 패스워드 입력과정의 노출 가능성 · 외부 침입자의 패스워드 도청 가능성 · 외부 침입자의 패스워드 파일 도용 가능성 · 내부 침입자의 패스워드 불법사용 가능성	[thrt1] [thrt2] [thrt3] [thrt4]	리커트 척도	Crockford(1981) Guarro(1988)
	취약성	· 패스워드의 추측의 가능성 · 패스워드의 망각의 가능성 · 정보 유출의 가능성 · 패스워드 운용 과정 정도	[vuln1] [vuln2] [vuln3] [vuln4]	리커트 척도	Guarro(1998) Gilbert(1991)
지각된 위험	위 험	· 보안사고로 인해 불이익을 당한 빈도 · 보안사고가 자산에 미치는 정도	[risk1] [risk2]	리커트 척도	김종대 외(1994) Guarro(1998)
패스워드 특성	길 이	· 패스워드의 문자 수		등간 척도	Fort(1985) Highland(1997) Zviran & Haga(1999)
	구 성	· 알파벳 · 숫자 · 알파벳과 숫자의 조합 · 한글 자모와 숫자의 조합 · ASCII문자 집합		명목 척도	Morris & Thompson(1979) Zviran & Haga(1999)
	수 명	· 패스워드 변경 빈도		서열 척도	Wood(1983) Highland(1997) Zviran & Haga(1999)
	선택방법	· 한 가지 의미 · 두 가지 이상의 의미 조합 · 한글을 영어자판으로 표기 · 소리나는 대로 적은 문자열 · 무작위 문자열		명목 척도	Seeley(1989) Highland(1997) Zviran & Haga(1999)

(1) 내용 타당성 분석

내용 타당성(content validity)이라는 것은 측정도구 자체가 측정하고자 하는 속성이나 개념을 측정할 수 있도록 되어 있는가를 평가하는 것이다. 일반적으로 측정도구가 측정 대상이 가지고 있는 무수한 속성들 중의 일부를 대표성 있게 포함하고 있으면 해당 측정

도구는 내용 타당성이 높다고 말할 수 있기에 평가문항이 도출된 과정을 살펴봄으로써 신뢰성을 검증할 수 있다[38].

먼저 위험의 발생 가능성으로서 자산(asset)의 경우 본 연구에서는 데이터 자산의 속성으로 민감도(sensitivity)와 중요도(importance)로 구분 지었다[21]. 즉, 개인 사용자에 대한 데이터의 고유 가치와 만약 데이터 파일의 내용이 타인에게 공개될 때 문제가 발생할 수 있는 정도로 조작화 하였으며, 이는 기존 연구에서도 검증된바 있다[e.g. 25,39,40]. 정보 시스템의 보안에 대한 위협(threat)을 파악하기 위한 보안위협 모형이 존재한다. 본 연구에서 사용된 위협은 Crockford(1981)가 제시한 모형에 초점을 맞추어 정보 시스템을 저해할 수 있는 위협 요인을 조작화하였다. 취약성(vulnerability)은 Guarro(1998)와 Gilbert(1991)의 연구로부터 도출된 보안대책의 결핍(absence of safeguards) 및 위험공격에 노출되어 있는 시스템의 상태로 범위를 정하였다.

사용자가 실제로 지각하는 정보자산에 대한 위험(risk)은 자산에 해를 입힐 수 있는 가능한 모든 것들을 규정하고 분류했을 때 이들의 발생 확률 또는 발생 빈도와 자산에 해를 입히는 정도를 통해서 알 수 있다[2]. 이에 지각된 위험을 보안사고로 인해 불이익을 당한 빈도와 보안사고가 자산에 미치는 정도로 보았다.

본 연구에서 조사하고자 하는 패스워드의 특성 요인들의 측정도구는 Highland(1997)와 Zviran과 Haga(1999)의 연구에서 검증된 설문 항목을 이용하였다. 길이(패스워드의 문자 수), 구성(문자영역 : 알파벳, 숫자, 알파벳과 숫자의 조합, ASCII 문자 집합), 수명(패스워드 변경빈도), 그리고 패스워드 선택방법이다. 여기서 선택방법이라는 것은 패스워드가 개인적으로 의미 있는 세부사항(사용자의 이름, 별명, 개인정보, 혹은 기억하기 쉬운 다른 것), 의미 있는 세부사항의 조합(ERIC710 혹은 KILLME), 한글을 영어자판으로 표기(한글로 '한국'을 영어자판으로 'gksrnr'로 표기), 소리나는 대로 적은 문자열(RUSURE), 혹은 무작위 문자열(H*DGHG8H)을 의미한다. 이에 본 연구에서는 기존 문헌에서 사용된 측정 도구를 본 연구에 맞게 조작화하였으며, <표 3>에 정리를 하였다.

(2) 개념 타당성과 내적 일관성 분석

개념 타당성(construct validity)이라는 것은 어떤 척도가 해당 변수를 정확하게 측정하고 있는가를 의미한다. 이를 위해 수렴 타당성(convergent validity) 개념을 위주로 검토를 수행하였다. 수렴 타당성은 동일한 개념을 측정하기 위하여 서로 상이한 두 가지 측정방식을 개발하고 이에 의하여 얻어진 측정치들간에 높은 상관관계가 존재해야 함을 의미한다. 본 연구에서는 이론변수에 대한 측정치들의 요인적재량 값을 살펴봄으로써 척도의 수렴 타당성을 확보하고 있는지를 살펴보았고, <표 4>에 제시하였다. 그 결과 모든 요인들의 아이겐 값이 허용치인 1.0을 상회함으로써

<표 4> 구성 개념의 요인분석 결과표

구 분		요 인				크론바-α
		위협	취약성	자산	위험	
위 협	thrt3	**0.885**	0.087	0.043	0.131	0.74644
	thrt2	**0.877**	0.0789	0.192	0.059	
	thrt4	**0.758**	0.285	0.140	0.016	
	thrt1	**0.613**	0.226	-0.098	0.281	
취약성	vuln3	0.062	**0.808**	0.170	0.099	0.78139
	vuln4	0.156	**0.758**	0.055	0.025	
	vuln2	0.099	**0.683**	-0.137	-0.015	
	vuln1	0.210	**0.668**	0.290	0.091	
자 산	asst2	0.133	0.056	**0.885**	0.081	0.85404
	asst1	0.065	0.104	**0.876**	0.059	
위 험	risk1	0.131	0.069	0.035	**0.892**	0.81054
	risk2	0.138	0.103	0.120	**0.871**	
분산값(%)		32.253	14.192	11.768	8.936	설명정도 67.148
아이겐값		3.870	1.703	1.412	1.072	

<표 5> 위험 관련 측정변수의 기술 통계량

측정 변수		표본수	정보이용 패스워드		이뱅킹 패스워드	
			평균	표준편차	평균	표준편차
위험의 발생 가능성	자 산	171	3.4034	0.9491	4.0701	0.8630
	위 협	171	2.6002	1.0415	2.9049	1.1026
	취약성	171	3.3350	0.9195	3.6339	0.9766
지각된 위험	위 험 (영향평가)	171	1.8982	1.0907	1.2514	0.9503

적정한 유의 수준을 제시하고 있다. 또한 요인 적재량 값이 최저 0.613에서 최고 0.892의 범위로서 비교적 높은 값으로 제시되기에 본 연구에서 채택한 측정 척도가 높은 수준의 개념 타당성을 확보하고 있음을 알 수 있다. 또한 전체분산의 67.148%를 설명함으로써 설명력도 존재한다고 볼 수 있다.

연구 변수로서 사용되기 위해서는 측정문항들이 해당 개념을 정확히 반영하고 있어야 한다. 이를 위해 측정도구에 대한 신뢰성 평가를 실시하였다. 내적 일관성 분석을 위해 크론바-α(Cronbach's alpha) 계수값을 나타낸 표를 역시 <표 4>에 제시하였다. 결과에서 알 수 있듯이 모든 신뢰성 계수가 0.75 이상을 기록하고 있다. 따라서 상기 결과를 토대로 본 연구의 조사를 위한 측정도구는 신뢰할 수 있다고 볼 수 있다.

4.3. 분석 결과

(1) 연구 변수의 기술통계 분석

본 연구에 포함된 위험(자산, 위협, 취약성)의 발생 가능성과 지각된 위험(위험의 영향평가) 수준 변수들에 대한 기술통계 분석 결과를 <표 5>에 정리하였다. 리커트 5점 척도가 사용되었으며, 숫자가 클수록 위험 발생 가능성과 위험이 높음을 나타낸다.

먼저 전체적인 측면에서 기술 통계량을 살펴보면, 위험의 발생 가능성 측면은 이뱅킹 패스워드가 단순 정보이용 패스워드보다 더 높은 수치를 보이고 있다. 반면, 위험 영향 평가를 통한 지각된 위험 수준은 단순 정보이용 패스워드보다 이뱅킹 패스워드가 더 낮은 것으로 분석되었다. 즉, 사전 조사에서 나타난 바와 같이 설문 응답자가 가장 중요하게 생각하는 이뱅킹 시스템에서 실제적인 보안 사고는 적게 발생되는 것으로 인지되었지만, 위험 발생 가능성은 높다는 결과는 다음의 시사점을 제공한다. 첫째, 자산의 중요성과 민감도가 은행에서 더욱 크기에 보다 철저한 보안 정책과 강력한 보안이 이루어지고 있음을 알 수 있다. 둘째, 실제 패스워드와 관련된 위험에 대해 사람들이 인식하는 것과 실제와는 차이가 난다는 것이다. 그러나 결과표에서 나타난 수치를 받아들임에 있어 보다 조심스러운 해석이 요구된다. 본 연구에서 실시한 지각된 위험 수준은 사용자가 단순하게 해당 정보 시스템의 최종 사용자로서 지각한 것일 뿐 실제 사용자가 모르는 상태에서 발생한 정보유출, 해킹 혹은 바이러스로부터도 안전하다는 것을 나타내지는 않는다.

다음으로 위험의 발생 가능성 측면에서 세부 항목에 대한 기술 통계를 살펴보면, 일반 사용자들은 사용하고 있는 정보 시스템의 위협과 취약성으로부터 야기되는 위험의 발생 가능성에대한 인지 정도는 낮은 것으로 분석되었다. 이는 실제 운용되고 있는 시스템과 네트워크 상황이 안전하다라고 설명하기보다는 정보보호를 위한 위협과 취약성에 대한 인식 수준이 상대적으로 낮다는 것으로 이해해야 할 것이다. 따라서 정보 시스템의 효과적인 위험관리를 위해 향후 정보보호 인식 및 교육, 훈련이 반드시 요구됨을 시사하고 있다.

다음으로 패스워드 특성을 살펴보기 위해 패스워드 관련 측정변수의 기술 통계량을 단순 정보이용 패스워드와 이뱅킹 패스워드에 관해 요약하였으며, 그 결과를 <표 6>에 제시하였다. 첫째, 패스워드 길이를 살펴보면, 단순 정보이용 패스워드에서는 6자리~7자리의 패스워드(48.5%)를, 이뱅킹 패스워드에서는 8자리~9자리(41.5%)를 주로 사용하고 있음이 나타났다. 이는 Menkus(1988)가 권고하는 6자리~8자리에 포함되고는 있다. 그렇지만 대체적으로 단순 정보이용 패스워드의 길이가 이뱅킹에 비해 짧은 경향을 보임으로써 위험 발생 가능성이 높을수록 패스워드 길이가 길어짐을 알 수 있다.

둘째, 패스워드 구성 측면에서는 다음과 같다. 알파벳과 숫자의 조합이 정보이용 관련 패스워드(51.5%)와

<표 6> 패스워드 관련 측정변수의 기술 통계량

측정항목		정보이용 패스워드		이뱅킹 패스워드	
		도수	백분율(%)	도수	백분율(%)
패스워드 길이	4자리~5자리	12	7.0	30	17.5
	6자리~7자리	83	48.5	60	35.1
	8자리~9자리	62	36.3	71	41.5
	10자리~11자리	10	5.8	9	5.3
	12자리	4	2.3	1	0.6
패스워드 구성	알파벳	21	12.3	12	7.0
	숫자	40	23.4	46	26.9
	알파벳과 숫자조합	88	51.5	95	55.6
	한글자모와 숫자조합	15	8.8	11	6.4
	ASCII 문자 집합	7	4.1	7	4.1
패스워드 수명	변경하지 않음	121	70.8	121	70.8
	일년에 3번 이하 변경	41	24.0	35	20.5
	일년에 4번~6번 변경	3	1.8	3	1.8
	매달 변경	3	1.8	9	5.3
	한달 이내에 변경	3	1.8	3	1.8
패스워드 선택방법	한가지 의미	59	34.5	55	32.2
	두 가지 이상의 의미조합	80	46.8	89	52.0
	한글을 영어 자판으로 표기	21	12.3	12	7.0
	소리나는 대로 적은 문자열	2	1.2	0	0
	무작위 문자열	9	5.3	15	8.8

이뱅킹 관련 패스워드(55.6%)에서 많이 사용됨을 볼 수 있다. 반면 응답자의 약 36% 정도는 단순하게 알파벳만을 사용하거나 숫자만으로 구성된 패스워드를 보유함으로써 단순한 패스워드를 선호하는 과거의 Morris와 Thompson(1979)의 연구를 크게 벗어나지 못하고 있다. 비록 응답자 비율을 낮지만, 보다 복잡한 체계라 할 수 있는 한글자모와 숫자의 조합이 각각 8.8%와 6.4%, 그리고 ASCII 문자 집합은 4.1%로 조사되었다. 물론 연구 여건과 인구통계적 상황이 다른 환경에서 단순 비교는 무리겠지만, 복잡한 체계로 패스워드 구성을 하는 응답자가 없었던 Zviran과 Haga(1999)의 연구에 비출 때, 사용자들의 정보보호에 대한 관심이 예전에 비해서는 높아지고 있다고 조심스러운 해석을 내릴 수 있다.

셋째, 패스워드 수명 측면에서 살펴 볼 때, 주기적인 패스워드 변경은 정보보호 수단의 기초가 된다[18]. 그럼에도 불구하고 단순 정보 이용과 이뱅킹 패스워드 모두 한번도 변경해 본적이 없다는 응답이 71%나 차지하였다. 따라서 보다 안전한 정보보호를 위해서는 패스워드 시스템의 변경주기를 통해 위험을 줄일 수 있는 장치가 마련되어야 할 것이다. 이 때 사용의 편의성 측면에 고려된 수명주기 정책이 결정되어야 할 것이다.

넷째, Highland(1997)는 보호해야 하는 정보가 민감할수록 패스워드를 선택하는 방법이 적절해야 한다는 것을 강조하였다. 특히 이름이나 이니셜, 날짜, 사용자에게 중요한 숫자는 사용하지 않음으로써 환경적인 실마리가 원천적으로 봉쇄되기를 권고하고 있다. 그럼에도 불구하고 단순 정보 이용 패스워드의 81.3%, 이뱅킹 패스워드의 84.2%의 응답자들이 쉽게 추측할 수 있는 한 가지 의미이거나 의미 조합으로 패스워드를 선택하는 것으로 드러났다. 물론 패스워드의 기억 용이성 때문이겠지만, 패스워드의 적절한 선택 방법을 통해 위험을 최소화하도록 노력해야 할 여지가 많다.

(2) 연구 모형의 검증

본 연구 모형을 실증적으로 검증하기 위해 SAS 8.01을 이용하여 설문 결과를 분석하였다. 위험관리 측면에서 위험에 대한 규명은 회귀분석을 통해 살펴보았고, 지각된 위험과 패스워드 특성의 관련성은 설문 척도에 맞는 분산분석을 실시하였다.

먼저 자산, 위협, 취약성 등과 같은 위험의 발생 가능성이 위험 영향평가로부터 도출된 위험에 어떠한 영향력을 미치는지를 밝히기 위해 다중 회귀분석

<표 7> 위험에 영향을 미치는 위험의 발생 가능성

종속변수	독립변수	표준회귀계수	T-value	p>|T|	R^2	F-value	p>|F|
지각된 위 험	자 산	0.8709	1.749	0.0810	0.7840	49.484	0.0001***
	위 협	0.2470	4.488	0.0001***			
	취약성	0.4411	0.624	0.5330			
	상 수	0.5600	2.184	0.0300			
* : p < 0.05 ** : p < 0.01 *** : p < 0.001							

(multiple regression)을 실시하였다. 이 때 각각의 문항값의 평균값을 사용하여 분석이 실시되었고, 그 결과를 <표 7>에 요약하였다.

결과로부터 알 수 있듯이 사용자 인지 측면에서 살펴보았을 때 위험 변수에 영향을 미치는 요인은 자산이나 취약성보다는 위협에 보다 큰 영향력이 행사됨이 나타났다. 자산과 취약성 부분은 사용자 개인 측면에 의존하는 반면, 패스워드 입력과정이 노출되거나 외부 침입자에 의한 도청 및 도용 가능성 등은 사용자 외적 측면이 보다 강하다. 따라서 패스워드 시스템을 이용하는 사용자는 외적 환경 측면에서 보다 큰 위험을 인지하고 있는 것으로 분석될 수 있다.

다음으로 사용자가 정보 시스템에 대해 지각하는 위험수준과 패스워드 특성간의 관계를 분석하였으며, 그 결과를 <표 8>에 제시하였다.

먼저 지각된 위험수준과 패스워드 길이와의 관계는 집단의 분산분석을 비모수적 방법으로 수행한 Kruskal-Wallis 검증을 통해 살펴보았다. 일반적으로 비모수적 통계 방법은 표본수가 부족하거나 측정값이 명목자료이거나 순위자료일 경우에 주로 행해지는 기법이다. 분석된 결과를 살펴보면, 사용자가 지각하는 위험에 따라 패스워드 길이가 달라짐을 알 수 있다. 즉, 위험 발생 가능성이 높고, 지각되는 위험이 클수록 사용자는 패스워드 길이를 길게 하는 것으로 분석되었다. 이러한 결과는 앞 절에서 살펴본 기술 통계 분석에서와 같은 시사점을 제공한다.

둘째, 사용자가 지각하는 위험수준과 패스워드 구성과의 관계를 살펴보기 위해 역시 집단의 분산분석을 비모수적 방법으로 수행한 Kruskal-Wallis 검증을 실시하였다. 그 결과 위험의 영향 평가와 패스워드 구성간에는 유의적인 관련성을 발견할 수 없다. 일반적으로 패스워드 구성은 개인이 보다 간편하게 입력할 수 있는 방식으로 이루어지기에 사용자들이 위험에 대한 지각을 할 때, 패스워드 길이는 바꾸더라도 구성은 바꾸려 하지 않는다는 것으로 분석될 수 있다. 이는 현실적으로 매우 중요한 시사점을 제공한다. 복잡한 체계로 패스워드를 구성하는 응답자가 매우 적었던 기술 통계 분석의 결과를 미루어 볼 때, 조직내 정보 자산을 보호하기 위한 패스워드 관리 지침을 제공함에 있어 패스워드 구성 측면이 강조되어야 함을 시사한다.

<표 8> 위험과 패스워드 특성간의 분석 결과

독립변수	종속변수	통계 측정치		
지각된 위 험	패스워드 길 이	χ^2	DF	p>|χ^2|
		23.784	3	0.0001***
	패스워드 구 성	χ^2	DF	p>|χ^2|
		0.815	3	0.846
	패스워드 수 명	상관계수(위험⇔수명)		p>|R|
		-0.106*		0.049*
	패스워드 선택방법	χ^2	DF	p>|χ^2|
		10.946	3	0.012*
* : p < 0.05 ** : p < 0.01 *** : p < 0.001				

셋째, 사용자가 지각하는 위험수준과 서열척도로 측정된 패스워드 수명과의 관계를 살펴보기 위해 Spearman 상관 분석을 실시하였다. 결과로부터 알 수 있듯이 위험의 지각 수준이 높을수록 패스워드는 더 자주 변경되어야 한다는 것을 인지하고 있다. 그러나 앞 절에서 실시한 기술 통계 분석에서 실제 많은 응답자들이 패스워드를 잘 변경하지 않음을 살펴보았다. 이는 조직내 정보보호를 위한 교육이나 훈련도 중요하지만, 정보보호에 대한 인식(awareness)에 대한 강조가 선행되어야 함을 시사한다고 볼 수 있다.

마지막으로 사용자가 지각하는 위험수준과 패스워드 선택방법과의 관계를 살펴보기 위해 Kruskal-Wallis 검증을 실시하였다. 분석 결과 지각된 위험의 영향 평가에 따라 패스워드 선택방법이 달라짐을 확인할 수 있다. 즉, 위험의 수준이 높다고 지각될 때 보다 추측하기 어려운 패스워드를 선택해야 함이 드러났다. 그러나 현실적으로 패스워드의 추측 난해성과 사용자의 패스워드 기억 용이성간에는 상반관계가 존재하기에 사용의 편의성 측면이 고려된 선택방법이 강구되어야 할 것이다.

5. 결 론

본 연구에서는 정보 시스템 사용자가 선택한 패스워드 특성을 실증적으로 평가하고 이러한 패스워드 특성들과 위험간의 관련성을 살펴보았다. 특히 위험을 도출하는 과정에서 위험관리 메커니즘을 도입하여 자산, 위협, 그리고 취약성을 가지고 위험이 발생할 것이라는 가능성을 평가하였다. 또한 위험에 대해 영향평가를 통해 실제 사용자들이 경험한 인지된 위험과 위험의 발생 가능성간의 차이점을 검증하였다. 보다 효과적인 검증을 위해서 사전 조사를 통해 낮은 수준의 정보보호 중요성을 가지고 있는 단순 정보이용 웹 사이트와 높은 수준의 정보보호 의식을 가지고 있는 이뱅킹 패스워드 시스템을 대상으로 응답된 설문을 분석하였다. 그 결과 단순 정보이용 패스워드와 이뱅킹 패스워드 시스템에서 발생 가능한 위험과 실제 위험간의 차이점을 규명하였으며, 패스워드 사용자들이 패스워드를 선택하고 관리함에 있어 실제 위험이 패스워드의 길이와 수명, 그리고 선택방법에 영향을 미친다는 것을 밝혔다. 또한 위험의 발생 가능성과 지각된 위험에 대한 기술통계 분석과 연구 모형의 분석을 병행하였다. 그 결과 조직내 정보 자산을 보호하기 위한 패스워드 관리 지침을 제안하였다. 아울러 조직내 정보보호를 위한 교육이나 훈련도 중요하지만, 정보보호에 대한 인식에 대한 강조가 선행되어야 함을 시사하였다.

그러나 본 연구에서 실시된 지각된 위험 수준은 사용자가 단순하게 해당 정보 시스템의 최종 사용자로서 지각한 것이다. 또한 본 연구의 설문에 응답한 사람들은 학생과 직장인들로서 일반인들에 비해 보안에 대한 인식이 어느 정도 정립되어 있다고 예상된다. 따라서 향후 실제 발생한 보안 위험에 대해 패스워드 특성과의 관련성을 탐색하는 연구가 수행되어야 할 것이다. 또한 전자상거래와 관련된 패스워드에 대해 일반인을 대상으로 연구가 진행된다면 보다 일반적인 결론을 유도할 수 있을 것이다.

참 고 문 헌

[1] 김법진, "CRAMM을 이용한 정보시스템을 위한 위험분석과 관리," 한국과학기술원 석사논문, 1996.

[2] 김종대, 김기윤, 김정덕, 김종기, 김현배, 남길현, 류재철, 박태환, 신동익, 이경석, 이재권, 이필중, 임채호, "전산망 보안을 위한 위험관리지침서", 연구보고서(NCA III-RER-9432), 한국전산원, 1994. 12.

[3] 이동수, 정보시스템 감사이론 및 실무 매뉴얼-정보기술 자가진단, 이한 출판사, 1996.

[4] 이만영, 전자상거래 보안기술, 생능출판사, 1999.

[5] 이서로, 파워 해킹 테크닉, 파워북, 1995.

[6] 이석호, 데이터 베이스론, 정익사, 1985.

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

[8] 이형원, 정보시스템 안전대책, 영진 출판사, 1993.

[9] 정경수, 김기영, 박종필, "패스워드 이용에 관한 실증분석: 대학과 종합병원을 중심으로," Information Systems Review, 제3권, 제1호, pp. 143-157, 2001.

[10] 한국전산원, "전산망 보안을 위한 위험관리 지침서," 1994.

[11] 한국정보보호센터, "정보보호총서," 1996, 12.

[12] Anderson, R.J., "Why Cryptosystems Fail," Communications of the ACM, Vol. 37, No. 11, pp.

32-40, 1994.

[13] Avame, S., "How to Find out a Password," Data Processing & Communication Security, Vol. 12, No. 2, pp.16-17, 1988.

[14] Browne, P.S., Security: Checklist for Computer Center Self-Audits, Arlington, VA : American Federation of Information Processing Societies, 1984.

[15] Caelli, William, Dennis Longley, and Michael Shain. Information Security Handbook. New York, NY: Stockton Press, 1991.

[16] Cooper, J.A., Computer and Communi -cations Security — Strategies for the 1990s, New York, McGraw-Hill, 1989.

[17] Crockford, N., "An Introduction to Risk Management," Woodhead-Faulkner Limited, Cambridge, England, 1980.

[18] Fort G.M., "Department of Defense Password Management Guideline," CSC-STD-002-85, Library No. S-26, 994, 12 April 1985. http://comsec.theclerk.com/CISSP/green.htm.

[19] Gilbert, I.A., "Risk Analysis : Concepts and Tools," Datapro Reports on Information Security, Risk Analysis, pp. 101-112, 1991.

[20] Guarro, S., "Analytical and Decision Models of Live," Risk Management Model Builders Workshop, pp. 49-72, 1998.

[21] Highland, J.H, "Demise of Passwords," Computers and Security, Vol. 9, No. 4, pp. 196-200, 1990.

[22] Highland, J.H., "How to Prevent the Use of Weak Passwords," EDPACS, Vol. 18, No. 9, pp. 7-12, 1995.

[23] Highland, J.H., "Changing Passwords," Computers and Security, Vol. 13, No. 3, pp. 183-184, 1997.

[24] Jackson, K.M. and Hruska, J., "Computer Security Reference Book," British Library Cataloging in Publication Data, pp. 227-263, 1992.

[25] Jobusch, D.L. and Oldhoeft, A.E., "A Survey of Password Mechanisms, Weaknesses and Potential Improvements," Computers and Security, Vol. 8, No. 8, pp. 675-689, 1989.

[26] Kim, J.K., "An Empirical Study on Information Systems Security Effectiveness Model," Journal of the Korean OR/MS Society, Vol. 20, pp. 77-104, 1995.

[27] Loch, K.D., Houston, H.C., and Merrill, E.W., "Threats to Information System : Today's Reality, Yesterday's Understanding," MIS Quarterly, Vol. 17, No. 2, pp. 173-186, 1992.

[28] Menkus, B, "Understanding the Use of Passwords," Computers and Security, Vol. 7, No. 2, pp. 132-136, 1988.

[29] Miller, H.E. and Engemann, K.J., "A Methodology for Managing Information-Based Risk," Information Resources Management Journal, Vol. 9, No. 2, pp. 17-24, 1996.

[30] Morris, R., and Thompson, K., "Password Security: a Case History," Communications of the ACM, Vol. 22, No. 11, pp. 594-597, 1979.

[31] Moses, R.H., "The CCTA Risk Analysis and Management Methodology (CRAMM) -Risk Management Model," Working Paper, 1988.

[32] Parker. D.B., "Computer Security Management," Creston VA : Reston Publishing Company, pp. 115-166, 1981.

[33] Pfleeger, C. P., "Security in Computing," Prentice-Hall. Englewood Cliffs. NJ. 1997.

[34] NIST, "An Introduction to Computer Security: The NIST Handbook," NIST Special Publication 800-12, 1999.

[35] Rainer, R.K., Snyder, C.A., and Carr, H.H., "Risk Analysis for Information Technology," Journal of Management Information Systems, Vol. 5, No. 1, pp. 129-147, 1991.

[36] Seeley D., "Password Cracking, a Game of Wits," Communications of the ACM, Vol. 32, No. 6, pp. 700-703, 1989.

[37] Smith, H.J., "Information Privacy: Measuring Individuals' Concerns About Organizational Practices," MIS Quar- terly, Vol. 20, No. 2, pp. 165-195, 1996.

[38] Straub, D.W., "Validating instruments in MIS research," MIS Quarterly, Vol. 13, No. 2, 1989, pp. 147-170.

[39] Wood, C.C., "Effective Information System Security with Password Controls," Computers and

Security, Vol. 2, No. 1, pp. 5-10, 1983.
[40] Zviran, M., and Haga, W.J., "Password Security: an Empirical Study," Journal of Management Information Systems, Vol. 15, No. 4, pp. 161-185, 1999.

오 창 규 (Chang-Gyu Oh)

1996년 8월 : 부산대학교 경영학부 졸업
1999년 2월 : 부산대학교 경영학과 석사
2002년 8월 : 부산대학교 경영학과 박사
2001년 3월 ~ 2003년 2월 : 부산외국어대학교 국제통상지역원 전임강사(강의전담)
2003년 3월 ~ 현재 : 부산외국어대학교 국제통상연구소 선임연구원
<관심분야> 조직내 정보기술채택, 정보시스템 보안관리, 전자상거래

김 종 기 (Jong-Ki Kim)

1987년 : 부산대학교 경영학과 학사
1988년 : Arkansas State University, MBA
1992년 : Mississippi State University, Ph.D. in MIS
1993년 3월 ~ 1998년 12월 : 국방정보체계연구소 선임연구원
1999년 3월 ~ 현재 : 부산대학교 경영학부 조교수
<관심분야> 정보시스템 보안관리, 전자상거래, 프로젝트 관리

심 윤 주 (Yun-Ju Shim)

2001년 2월 : 동서대학교 국제물류학과 졸업
2003년 2월 : 부산대학교 경영학과 석사
<관심분야> 전자상거래 보안