情報保護學會論文誌
第20卷 第6號, 2010. 12

AHP를 이용한 SNS 정보보호 위협요인 분석

성 기 훈,[1†] 공 희 경,[2‡] 김 태 한[2]
[1]과학기술연합대학원대학교, [2]한국전자통신연구원

A Study on Threat factors of Information Security in Social Network Service by Analytic Hierarchy Process

Kihoon Sung,[1*] Hee-Kyung Kong,[2†] Taehan Kim[2]
[1]University of Science and Technology, [2]Electronics and Telecommunications Research Institute

요 약

최근 SNS 이용이 활성화됨에 따라 SNS 제공환경에서의 정보보호에 대한 관심이 증가하고 있다. 하지만 SNS 산업 환경의 급격한 성장으로 인한 가입자 유치 위주의 투자 선행과 서비스 제공자 측면에서의 SNS 정보보호 투자 효과에 대한 확신 부족, 그리고 SNS에서의 정보보호 중요위협요인에 대한 분석체계 부재로 인해 아직까지 SNS 제공환경에서의 정보보호에 대한 투자가 미흡한 실정이다. 본 논문에서는 AHP를 이용한 SNS 제공환경에서 정보보호 중요위협요인 분석을 통해 정보보호 투자 결정 기준 도출에 대한 연구를 수행하였다. 본 연구를 통해, '서비스 이미지'가 정보보호 평가기준에서 가장 중요한 항목으로 도출되었으며, '개인 프로파일 위조 및 명예훼손'과 '산업 스파이'가 중요한 SNS 정보보호 위협요인인 것으로 나타났다.

ABSTRACT

As the usage of social network service(SNS) increases recently, great attention has been shown to the information security in SNS. However, there has been little investment in SNS environment for security while preferential investment to attract subscribers has been made so far. Moreover, there is still a lack of confidence for investment effect and an absence of framework to analyze the threat factors of information security in SNS. In this paper, we propose to model for decision-making standard of SNS information security investment by the AHP. The result shows that 'service image' is the most important criterion for the decision of SNS information security. It also shows that 'Profile-squatting and reputation slander through ID thefts' and 'Corporate espionage' are important threat factors in SNS information security.

Keywords: Social Network Service, Information Security Investment, Threat Factor, AHP

I. 서 론

최근 소셜 네트워크 서비스(Social Network Service, SNS) 이용이 활성화됨에 따라 SNS에서의 정보보호에 대한 관심이 증가하고 있다. SNS에서 정보보호는 SNS 이용자의 개인 정보(privacy) 관리와 신뢰(trust)를 기반으로 한 인맥관리 및 사회 그룹 내 활동 영위를 위해 필수적인 요소로, SNS 산업의 성장과 함께 그 중요성 역시 점차 증가하고 있다. 또한 Web 2.0 환경의 정착과 스마트폰의 대중화로 인해 SNS는 최근 이용률이 급격히 증가하고 있다. Strategy Analytics(2007)는 2012년 SNS 이용자가 10억을 넘어설 것으로 전망하였다[1]. 이러한 SNS 이용자 저변 확대와 더불어 SNS 이용에 따른 정보보호 관련 문제 역시 크게 증가하고 있으나 이에 대한 전반적인 인식 및 대응 수준은 초기 단계에 머물고 있다. 국내 SNS 이용자들의 약 80%는 SNS 이용 시 불건전

접수일(2010년 9월 25일), 게재확정일(2010년 12월 13일)
† 주저자, khsung@ust.ac.kr
‡ 교신저자, konghk@etri.re.kr

정보 노출, 부정확한 정보 유통, 개인정보 및 사생활 침해 등의 정보보호 관련 불편 및 피해를 경험했지만 아직까지 이를 근절하거나 해결하기 위한 뚜렷한 대책은 없는 것으로 나타났다[2]. 이는 현재 SNS를 둘러싼 산업의 급격한 성장으로 인해 가입자 유치 위주의 투자 선행이 이루어져 상대적으로 정보보호와 관련된 투자가 미흡했기 때문이다. 또한 개방과 소통의 Web 2.0 개념을 기본으로 하는 SNS 트렌드는 많은 서비스들로 하여금 정보보호에 대한 불감증을 불러일으켰고, 전반적인 산업 관련자들조차도 SNS에서의 정보보호 문제를 부차적인 것으로 인식해왔다. 이로 인해, SNS의 정보보호 필요성을 인식하고 있지만, SNS의 특성을 고려하지 않은 채 일반적인 인터넷 서비스에서의 정보보호 문제와 유사한 수준으로 판단하고 있으며, SNS 정보보호 투자에 대한 직접적이고 가시적인 수준의 투자 효과에 대한 확신을 갖지 못하고 있다. 또한 다양하고 많은 SNS 이용환경에서 정보보호 문제가 대두되고 있는 가운데 어떤 문제가 시급하고 우선적으로 해결되어야할 것인지에 대해 객관적으로 예측할 수 있는 분석체계도 전무한 상태이다. 따라서 효율적인 SNS 정보보호 투자를 위한 위협요인에 대한 정량적, 정성적 평가기준 도출이 필요하다.

SNS 정보보호 투자에 대한 첫 단계는 '정보보호 위협요인'의 우선순위 결정에서부터 시작된다. SNS 정보보호를 효율적으로 수행하기 위해서는 무엇보다 경제적, 기술적 측면의 고려가 중요하다. 신뢰를 기반으로 이용자 간의 관계 맺기와 다양한 정보의 생성 및 공유 활동을 지원하는 SNS는, 경제적인 측면에서 가입자 유치 및 관리, 그리고 직접적인 수익원인 핵심 비즈니스 모델에 적합하면서도 효율적인 정보보호 투자가 선행되어야 한다. 또한 기술적인 측면에서도, 서비스의 성장과 함께 기하급수적으로 늘어나는 이용자들의 개인 정보와 데이터를 안전하고 효과적으로 관리할 수 있도록 해야 한다. 본 논문에서는 SNS 정보보호 투자 시 고려해야할 기준들을 제시하고 정보보호 위협요인에 대한 우선순위 분석을 수행함으로써, SNS 정보보호 투자를 위한 가이드라인을 제공하고자 한다. 연구방법은 다기준 의사결정시 널리 사용되는 계층분석기법(Analytic Hierarchy Process, AHP)을 사용하여, 정보보호 분야의 전문가들을 대상으로 설문조사를 실시하고 그 결과를 분석 및 제시하고자 한다. 본 논문의 구성은 다음과 같다. 2장에서는 본 연구에서 대상으로 하고 있는 SNS에 대한 소개와 AHP 방법론에 대한 문헌연구를 수행하였다. 3장에서는 정보보호 투자 시 고려해야할 평가기준과 SNS 이용환경에서 논의되고 있는 위협요인을 포함한 연구 모델을 제시한다. 4장에서는 연구결과를 분석하고, 마지막으로 5장에서는 본 연구의 결론 및 시사점을 제시한다.

II. 관련 연구

2.1 소셜 네트워크 서비스

SNS는 공통의 관심사를 지니고 있는 사용자들 간의 관계 형성을 통한 다양한 인적, 물적 교류를 지원하는 서비스를 의미한다. Boyd et al.(2007)은 SNS를 개인의 프로필을 구성하고, 개인들 간의 관계를 통해 형성된 연결을 공유하고, 그 연결을 바탕으로 일어나는 개인 간의 상호 작용을 지원하는 웹 기반 서비스로 정의하였다[3]. 과거 PC통신 시절부터 SNS는 버추얼 커뮤니티의 형태로 존재하였으며 본격적으로 WWW(World Wide Web)이 대중화된 시기인 2000년 이후로 인스턴트 메신저(instant messenger), 인터넷 동호회, 블로그(blog), 가상현실(virtual reality) 등의 다양한 형태로 발전해왔다. 최근에는 Facebook, MySpace 등의 인맥 중심의 복합형 블로그 형태의 서비스를 가장 많이 이용하고 있으며, 모바일 통신 환경의 발전과 스마트폰의 대중화로 단문 중심의 마이크로블로깅(micro blogging) SNS가 크게 각광받고 있다. SNS에 대한 대중들의 관심은 최근 급격히 증가하고 있다. 세계적으로 인터넷에서 이용하는 서비스 중 SNS는 12.0%로 가장 많이 이용하고 있는 서비스인 메신저(12.3%)와 거의 근접한 상태이다[4]. 대표적인 SNS라 할 수 있는 Facebook과 Twitter의 순 방문자 수는 2010년 7월 각각 1억 2천 8백만 명, 2천 9백만 명 정도 월평균 3% 이상의 증가를 보이고 있다[5]. 이러한 SNS의 성장은 주 수익원인 광고수익 현황에서도 유사하게 진행되고 있다. 2009년 세계 SNS 광고 수익은 22억 달러에 이르며, 연평균 10% 이상의 고성장률을 기록하고 있으며, 2011년에는 29억 달러에 이를 것으로 전망되고 있다[6]. 이처럼 SNS는 참여와 공유 중심의 Web 2.0 시대에 가장 적합한 인터넷 서비스로 자리매김하고 있다. 특히 다양한 콘텐츠의 생산과 유통, 공유가 손쉬운 환경으로서 SNS는, 네트워크 망외부성 효과에 의존적이기 때문에 많은 이용자를 확보할수록 서비스의 잠재적 가치가 높아지게 된다. 이는 SNS 이용자들의 참여를 통해 SNS를 통한 정보에 관한 정보(meta information)의 생성과 유통을 가속화시키게 되

어 이를 기반으로 한 다양한 비즈니스 기회를 제공하기 때문이다. 이러한 SNS의 특징은 기존 인터넷 서비스가 광고 이외의 뚜렷한 수익원을 찾지 못한 상태에서 새로운 방향성을 제시한 것으로, 향후 정보 수용자 중심의 정보 유통을 기반으로 타깃형 마케팅, 애플리케이션 내재화를 통한 원스톱 서비스 제공 등을 가능하게 할 것으로 전망된다.

2.2 계층분석기법

AHP기법은 Saaty에 의해 개발된 다기준 의사결정 모델(multi-criteria decision making model)로, 의사결정 프로세스를 체계적으로 분석하고, 여러 평가항목의 가중치를 쌍대비교(pairwise comparison)를 통해 단계적으로 도출함으로써 대안들에 대한 합리적 평가를 지원한다[7]. AHP기법은 복잡한 의사결정 문제의 계층적 구조화를 통해 부분적이며 순차적인 접근 과정을 거쳐 최종적으로 의사결정을 하도록 지원한다[7]. 즉, AHP는 계층(hierarchy)의 개념을 통해 의사결정에 필요한 여러 요소들을 계층화시켜 각 요소별, 요소간의 관계를 보다 상세히 논리적으로 보여준다. AHP기법은 일관성비율(Consistency Ratio, CR)을 기준으로 설문응답의 신뢰도를 측정할 수 있는 특성을 갖고 있기 때문에, 의사결정자의 논리적 일관성 유지 여부를 확인할 수 있으며 논리적이고 합리적인 의사결정 과정에 대한 신뢰성을 높일 수 있다[7]. 일반적으로 일관성비율의 값은 0.1(10%) 이하가 되어야 일관성과 각 항목별 가중치의 유의미를 부여할 수 있다[7]. 하지만 일부 사회과학 분야의 연구 조사에서는 설문 문항의 특성상 각 상·하위 기준간의 독립성 확보가 어렵다는 점을 감안하여 0.2(20%) 이내까지를 허용범위로 하고 있다[7, 8, 9].

III. 모형 설정

본 연구모형 설정의 목적은 SNS 사업자가 정보보호투자 시 고려해야 하는 기준과 위협요인 우선순위 결정을 돕는 모델을 제시하는 것이다. SNS 정보보호 중요위협요인 선택을 위한 가이드라인이 필요한 이유는 정보보호에 대한 한정된 투자 하에서 그 투자의 효용성을 최대한 높일 수 있는 방법을 제공하기 위한 것이다.

3.1 평가 기준

이 절에서는 국내외의 연구에서 정의된 정보보호 평가 기준에 대해 고찰하고, 고려해야 할 평가 기준을 도출하고자 한다. 지금까지 정보보호투자의 효과를 분석하고 정보보호투자 시 고려해야 하는 기준에 대한 다양한 연구가 제시되어 왔다[10]. 정보보호 투자에 대한 사회적, 경제적 연구의 필요성에 대해 Soo Hoo (2000), Gordon and Loeb(2002) 등은 보험 산업과 기업에서 정보보호 문제에 대한 연구의 필요성을 분석하고 효율적인 투자 규모와 효과 등에 대한 논의의 필요성이 제기되고 있다[11, 12]. 정보보호 투자 시 고려해야하는 평가기준은 크게 경제적인 측면과 기술적인 측면으로 분류된다. 경제적인 측면의 경우, Blatchford(1995), Davis(2005), Cavusoglu et al.(2004)은 비용(costs)과 재정적 효용(financial benefits), 정보시스템 운영비용(cost of the controls), 정보보호 비용(cost of security), 신뢰도 하락(loss of credibility) 등의 평가기준을 제시하였다[13, 14, 15]. 기술적 측면에서 고려해야하는 평가기준은 크게 무결성, 가용성, 기밀성으로 나뉘는데, Gordon and Loeb(2002), Blatchford(1995), NIST(1996), Lee(2003), Bodin et al.(2005)등에 의해서 기밀성, 무결성, 가용성 등의 정보보호 목표를 효율적으로 달성할 수 있도록 하는 연구들이 이루어져 왔다[12, 13, 16, 17, 18]. 무결성은 시기적절하며, 내용이 정확하고 일관성의 수준이 유지되는

[표 1] 연구의 평가기준 선정을 위한 문헌조사

평가기준	선행연구의 평가기준	선행 연구
경제적 측면	비용(costs)	Blathchford(1995)[13]
	재정적 효용 (financial benefits)	Blathchford(1995)[13], Davis(2005)[14]
	정보시스템 운영비용 (cost of the controls)	Blathchford(1995)[13]
	정보보호 비용 (cost of security)	Davis(2005)[14]
	신뢰도 하락 (loss of credibility)	Cavusoglu et al.(2004b)[15]
기술적 측면	기밀성 (confidentiality)	Gordon and Loeb(2002)[12], Blathchford(1995)[13], NIST(1996)[16], Lee(2003)[17], Bodin et al.(2005)[18]
	데이터 무결성 (data integrity)	
	시스템 무결성 (system integrity)	
	가용성 (availability)	

것을 의미하며, 기밀성은 비 인가된 사용자의 사적인 자료 또는 기밀자료에 대한 접근을 차단하기 위한 요구사항을 뜻한다. 그리고 가용성은 인가된 사용자에 대한 서비스 보장 요구사항을 의미한다.

본 연구모형에서는 문헌조사를 통해 도출한 정보보호 평가기준에 대한 여러 선정기준들을 재분류하고 중복되는 항목들을 제거하여, 이 결과를 바탕으로 전문가를 대상으로 선정된 평가기준에 대해 델파이 조사를 실시하였다. 델파이 설문조사는 2010년 7월 31일 부터 2010년 8월 16일 까지 정보보호 관련 분야 전문가 7명을 대상으로 문헌조사에서 도출된 정보보호 평가기준에 대해 전문가들의 의견수렴을 목적으로 실시하였다. 설문에 참여한 전문가는 공공기관의 최고정보책임자 1명, 인터넷 서비스 관련기업의 CFO(Chief Financial Officer) 및 최고의사결정자 4명, 정보보호 관련학과의 대학교수 1명, 관련연구기관의 연구원 1명으로 정보보호 분야의 이론적, 실무적 경험을 보유하고 있을 뿐만 아니라 정보보호 투자 의사결정에서 영향을 줄 수 있는 전문가들로 구성하였다. 이러한 델파이 조사를 통해 도출된 평가기준은 〔표 2〕와 같다.

연구 모형의 평가기준은 크게 '경제적 측면'과 '기술적 측면' 두 가지로 범주화하였다. '경제적 측면'은 투자비용과 경제적 효과에 대한 관심의 정도로서, 서비스 제공자 내 정보시스템 관련 제품 도입 기준이다. 이는 비용 대비 효용으로 대표되는 제품 구매 자체에 초점을 맞춘 평가기준이다. '기술적 측면'은 정보보호 수준 제고에 대한 관심의 정도로서, SNS 제공환경의 특성을 반영한 제품 또는 시스템 도입 기준이다.

〔표 2〕 연구모형의 평가기준

상위기준	하위기준	조작적 정의
경제적 측면	비용 효율성	투자규모 대비 보안 비용의 적정한 정도 및 운영비용 절감에 기여할 것으로 기대되는 정도
	기대 수익	SNS 가입자 증가 및 수익 증대에 기여할 것으로 기대되는 정도
	서비스 이미지	잠재적 서비스 이미지 향상에 기여할 것으로 기대되는 정도
기술적 측면	기밀성	기밀성 확보에 기여할 것으로 기대되는 정도
	데이터 무결성	데이터 무결성 확보에 기여할 것으로 기대되는 정도
	시스템 무결성	시스템 무결성 확보에 기여할 것으로 기대되는 정도
	가용성	가용성 확보에 기여할 것으로 기대되는 정도

본 연구모형에서는 '경제적 측면'의 세부기준으로 비용 효율성, 기대 수익, 서비스 이미지를 제시하였으며, '기술적 측면'의 세부기준으로는 기밀성, 데이터 무결성, 시스템 무결성, 가용성을 제시하였다.

3.2 평가요소

본 논문에서 분석하고자하는 SNS 정보보호 위협요인은 SNS 이용환경에서 대두되고 있는 위협요인을 기준으로 분류하였다. 이 위협요인들은 기존의 인터넷 서비스에서 논의된 위협요인과 그 행태적 특성이 매우 상이하거나 기술적으로 새로운 방식의 것이기보다는, 신뢰기반의 관계 지향적 서비스라는 특징에 초점을 둔 것이다. 그렇기 때문에 SNS 이용환경 및 특성을 고려한 기준으로 분류체계가 재구성하는 것이 필요하다.

조찬식(2000)은 정보화 사회에서 인지가능한 정보

〔표 3〕 연구모형의 평가대안(SNS 정보보호 위협요인)

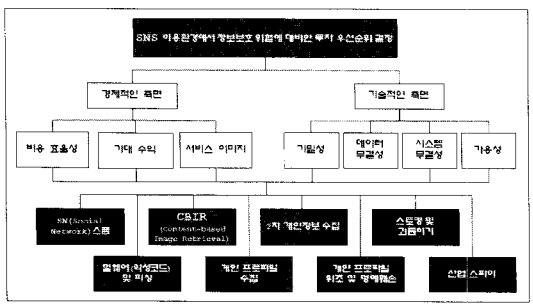
분류	평가요인	정의
기술적/매체적 위협요인	SN 스팸	자동화된 검색 도구를 통해 특정 SNS 사용자 명단 유출 및 스팸 메일 발송
	멀웨어(악성코드) 및 피싱	SNS 사이트에 게시되는 콘텐츠에 멀웨어를 심어놓아 이용자 정보 수집 및 피싱, 트래픽 과부하 등을 수행
	CBIR	특정인의 사적 이미지를 활용하여 유사 이미지 검색 및 추적으로 사용자 정보 획득 가능
의도적 위협요인	개인 프로파일 수집	SNS 상에 저장된 개인 프로파일을 수집하여 사적인 용도로 데이터화하여 사용
	2차 개인정보 수집	공개된 프로파일 이외의 2차 정보(IP주소, 접속 및 이용시간, 방문기록 등) 수집 후 사적인 용도로 데이터화하여 사용
사회/제도적 위협요인	개인 프로파일 위조 및 명예훼손	특정인의 프로파일 위조 및 허위 프로파일 작성을 통해 명예훼손 등 악의적 목적으로 사용
	스토킹, 괴롭히기	SNS를 이용한 불특정 다수를 대상으로 스토킹 및 괴롭히기 가능
	산업 스파이	특정 기업에 민감한 정보 탈취 및 지적 재산권 탈취

침해의 유형을 물리적 침해와 논리적 침해로 구분하고 트로이목마(trojan horses), 취약점 공격(exploits), 구조적 공격(infrastructure attack), 사용자 도용(impersonation), 서비스 방해 공격(denial of service attack) 등으로 분류하였다[19]. 유럽 정보보호 전문기관 ENISA(European Network and Information Security Agency)는 SNS 보안과 관련하여 기존 보안위협의 변형, 개인 프라이버시 위협, 아이덴티티 위협, 사회적 위협 등의 4개 분야로 분류하여 SN(Social Network) 스팸, CBIR(Content-Based Image Retrieval), SNS 피싱, 스토킹 등 총 15개 위협요인으로 분류하였다[20]. 이기식(2008)은 사이버보안에 영향을 미치는 위협요인을 크게 매체적(기술요소) 요인, 인간적 요인, 제도적 요인, 문화적 요인 등으로 분류하였다[21].

본 연구 모형은 ENISA에서 제안한 SNS 정보보호 위협요인을 중심으로 기존의 인터넷 서비스의 정보보호 위협요인과의 유사성 및 특성을 고려하여 [표 3]과 같이 8가지 위협요인을 채택하였다. ENISA의 정보보호 위협요인 분류는 위협요인의 목적과 위협형태의 유사성을 기준으로 분류되어있어 위협요인 간의 상호 종속성이 존재한다. 본 연구에서는 기업 측면의 SNS 정보보호 투자를 위한 위협요인의 투자우선순위에 대한 분석이기 때문에 위협요인의 독립성 보장을 우선시해야하며, 상호 종속성을 배제하지 못할 경우, 유사 위협요인에 대한 중복 투자로 이어질 수 있기 때문에 반드시 고려해야한다.

IV. 실증 분석

4장에서는 앞서 제시한 연구모형을 토대로 정보보호분야 전문가들을 대상으로 실시한 설문조사 결과를 분석하고자 한다. 본 연구모형은 제 1계층은 모델의 목표, 제 2계층은 2개의 상위평가기준, 제 3계층은 7개의 하위평가기준, 제 4계층은 8개의 평가 대안으로 구성되어있다.



[그림1] SNS 정보보호 투자 우선순위 결정을 위한 계층도

[그림 1]의 계층도를 기반으로 전문가 대상 설문조사를 수행하여 연구모형을 분석하였다. 설문조사는 정보보호 관련 분야 전문가 9명을 대상으로 실시하였다. 회수된 응답지 9부 중 일관성비율이 0.2 이상인 응답지와 결손치가 있는 응답지 2부를 제외한 총 7부를 유효 데이터로 판단하여 분석 자료로 활용하였다. 유효 설문 응답자들의 일관성비율은 각각 0.05, 0.19, 0.17, 0.06, 0.07, 0.11, 0.05로 나타났다. AHP 분석의 경우, 중요도 평가과정에 집단이 참가하여 그 의견을 취합하는 방법은 집단의 동의를 구하여 단일의 중요도를 산출하는 방법과 개별적으로 중요도를 평가한 후 통합하는 방법이 있으나, 본 연구에서는 후자의 방법을 택하였고 7명 전문가의 의견을 기하평균(geometric mean)을 사용하여 집단의견의 중요도를 산출하였다[9]. 본 연구는 AHP 분석 프로그램 Expert Choice 2000을 이용해 상위기준과 하위기준 간 우선순위 분석, 대안간 상위기준별 우선순위 분석, 대안간 하위기준별 우선순위 분석, 응답자별 분석을 통해 연구모형에 대한 실증분석을 수행하였으며, 그룹의 일관성비율은 0.05로 유의한 수준의 응답으로 판단하였다.

[표 4]는 상위기준(main criteria) 및 하위기준(sub criteria)간 우선순위(priority)에 대한 정보보호분야 전

[표 4] 상위기준 및 하위기준 간 우선순위 분석 결과

상위 기준	상위 기준 간 상대적 중요도	하위기준	상위기준 대비 하위기준 간 상대적 중요도	전체 하위기준 간 상대적 중요도
경제적 측면	0.644	비용 효율성	0.368 (2순위)	0.237 (2순위)
		기대 수익	0.214 (3순위)	0.138 (3순위)
		서비스 이미지	0.418 (1순위)	0.269 (1순위)
기술적 측면	0.346	기밀성	0.379 (1순위)	0.131 (4순위)
		데이터 무결성	0.223 (3순위)	0.077 (6순위)
		시스템 무결성	0.283 (2순위)	0.097 (5순위)
		가용성	0.115 (4순위)	0.040 (7순위)
총 합	1.000		2.000	1.000

문가들의 의견을 보여주고 있다. 우선 상위기준 간 쌍별 비교 결과는 경제적 측면의 중요도와 기술적 측면의 중요도가 각각 64%와 35%로 경제적 측면의 중요도가 더 큰 것으로 나타났다. 상위기준 대비 하위기준 간의 상대적 중요도는 경제적인 측면에서 서비스 이미지가 41.8%로 1위를, 비용 효율성이 36.8%로 2위를, 기대 수익이 21.4%로 3위를 기록했다. SNS에서 서비스 이미지는 가입자 유치 및 충성도 제고와 밀접한 관계를 가지고 있기 때문에 정보보호 투자에서 우선적으로 고려해야하는 것으로 분석된다. 그 다음으로 중요한 평가기준인 비용 효율성은, SNS의 정보보호 투자 시 서비스 운영 제반에 있어서 정보보호 침해로 인한 피해를 방지함과 동시에 서비스의 운용에 있어서 중요한 투자 기준임을 나타내고 있다. 다음으로 중요한 정보보호 투자 평가기준은 기대 수익인 것으로 분석되었다. 이는, 조직에서 정보보호 투자효과를 가장 가시적이고 정량적으로 판단할 수 있는 기준이 기대 수익에 대한 기여도이기 때문인 것으로 분석된다. 이들 기준들의 순위를 보면, 정보보호 투자라는 것이 기대 수익에 대한 직접적인 효과성 측면보다는 SNS 제공환경에서의 기업 이미지 향상과 정보시스템 운영비용의 감소를 통한 비용 효율성 측면이 더욱 강조되고 있는 것을 알 수 있다.

기술적인 측면에서의 상위기준 대비 하위기준 간의 상대적 중요도는 기밀성이 37.9%로 1위, 시스템 무결성이 28.3%로 2위, 데이터 무결성이 22.3%로 3위, 가용성이 11.5%로 4위를 각각 기록했다. 전통적인 정보보호 침해는 기밀성을 달성하지 못하게 하는 형태로, SNS 제공환경에서 기밀성은 서비스 이용자가 가장 기본적으로 제공받아야하는 부분이기 때문에 그 상대적 중요도가 높게 나온 것으로 분석된다. 시스템 무결성은 데이터 무결성과 가용성을 보장하기 위한 선제적 평가기준이기 때문에 위와 같은 결과가 나온 것으로 판단된다.

전체 하위기준 간의 상대적 중요도는 경제적 측면 기준에서 서비스 이미지가 가장 높은 순위를 기록하였으며, 이는 SNS 제공환경에서 정보보호 투자의 가장 중요한 목적과 고려되는 우선순위가 서비스 이미지 제고라는 것을 보여주는 결과이다. SNS 제공환경에 적합한 정보보호 투자는, 정보화 역기능들로부터 정보시스템을 보호하고 효율적으로 관리함으로써, 안정적인 서비스 제공과 동시에 향후 서비스 이미지 제고를 통한 신뢰도 증대에 기여할 수 있을 것으로 기대하고 있는 것으로 해석된다.

[표 5]와 [표 6]에서는 상위 기준 및 하위 기준 별로 각 대안간의 상대적 중요도를 보여주고 있다. SNS 제공 시 정보보호 투자를 하는 경우, 경제적인 측면에서는 '산업스파이'가 상대적 중요도가 가장 높은 위협요인으로 나타났으며, 기술적인 측면에서는 '개인 프로파일 위조 및 명예훼손'이 중요도가 높은 것으로 나타났다. '산업 스파이' 위협 요인은 크게 두 가지 측면에서 매우 위협적인 정보보호 침해를 발생할 수 있는 것으로 보인다. 첫째, SNS 자체의 데이터베이스, 즉 서비스 이용자 정보 및 기술, 콘텐츠의 유출 가능성에 대한 위협이며, 둘째는 SNS 이용자의 중요 기밀 정보 누출로 인한 연계 피해이다. 전자의 경우는 막대한 이용자 정보를 가지고 있는 SNS 제공자에게 있어서 가장 치명적인 정보보호 침해로, 최근 몇몇 인터넷 서비스의 이용자 정보 유출 등과 같은 피해를 야기할 수 있다. SNS 제공환경에서는 단 한 번의 정보보호 침해만 발생하게 되더라도 이용자들이 대거 이탈할 수 있게 되기 때문에 SNS 제공자 입장에서 매우 중요한 위협요인이 될 것으로 판단된다. 후자의 경우, SNS가 관리하고 있는 이용자의 중요 정보가 유출되어 2차적인 피해를 야기하는 문제로, 이와 같은 문제가 발생하게 되면 서비스 이미지 실추는 물론 2차 피해에 대한 막대한 손해배상까지 감수해야만 하는 상황이 될 수 있다. 즉, '산업 스파이'는 SNS 제공자 입장에서 침해가 발생하는 순간 서비스 운용에 치명적 손실이 불가피하여 매우 위험도가 높은 위협요인이라 할 수 있다. '개인 프로파일 위조 및 명예훼손'은 기술적 측면에서 가장 중요한 위협요인이지만, 경제적 측면에서도 '산업 스파이'와 거의 유사한 수준의 중요도를 갖는다. '개인 프로파일 위조 및 명예훼손'은 정보보호 침해 사례 중 악의적 해킹, 즉 크래킹에 가까운 침해 유형으로, 인터넷 서비스 정보보호 에서 가장 기본적인 위협요인이다. SNS는 서비스 제공 기업의 정보보호에 대한 신뢰도가 매우 중요하기 때문에 '개인 프로파일 위조 및 명예훼손'은 SNS 이용자들의 정보를 보호하기 위한 가장 기본적이고 시급히 대처해야할 위협요인인 것으로 나타났다. 그 밖에 '2차 개인정보 수집', '개인 프로파일 수집', 'CBIR' 등의 위협요인은 SNS 자체적 보안 정책 및 이용자의 권한 설정 등을 통해 1차적으로 관리 가능한 위협요인으로 상대적으로 중요도가 낮은 것으로

〔표 5〕 대안간 상위기준별 우선순위 분석 결과

대 안	경제적 측면	기술적 측면	전체 순위
SN 스팸	0.055 (8순위)	0.057 (8순위)	0.055 (8순위)
멀웨어 및 피싱	0.077 (7순위)	0.138 (3순위)	0.099 (6순위)
CBIR	0.078 (6순위)	0.109 (6순위)	0.089 (7순위)
개인 프로파일 수집	0.115 (5순위)	0.127 (5순위)	0.119 (5순위)
2차 개인정보 수집	0.124 (4순위)	0.134 (4순위)	0.127 (4순위)
개인 프로파일 위조 및 명예훼손	0.195 (2순위)	0.185 (1순위)	0.192 (1순위)
스토킹 및 괴롭히기	0.161 (3순위)	0.090 (7순위)	0.135 (3순위)
산업 스파이	0.196 (1순위)	0.161 (2순위)	0.183 (2순위)

〔표 6〕 대안간 하위기준별 우선순위 분석 결과

대안	경제적인 측면			기술적인 측면				전체 순위
	비용 효율성	기대 수익	기업 이미지	기밀성	데이터 무결성	시스템 무결성	가용성	
SN 스팸	0.065 (7순위)	0.043 (8순위)	0.051 (8순위)	0.045 (8순위)	0.053 (8순위)	0.070 (8순위)	0.072 (8순위)	0.055 (8순위)
멀웨어 및 피싱	0.093 (6순위)	0.075 (7순위)	0.064 (7순위)	0.107 (5순위)	0.136 (3순위)	0.169 (1순위)	0.163 (2순위)	0.099 (6순위)
CBIR	0.060 (8순위)	0.087 (6순위)	0.088 (6순위)	0.091 (7순위)	0.114 (6순위)	0.134 (5순위)	0.098 (7순위)	0.089 (7순위)
개인 프로파일 수집	0.131 (4순위)	0.119 (4순위)	0.098 (5순위)	0.118 (3순위)	0.129 (5순위)	0.147 (3순위)	0.106 (5순위)	0.119 (5순위)
2차 개인정보 수집	0.126 (5순위)	0.135 (3순위)	0.116 (4순위)	0.117 (4순위)	0.139 (2순위)	0.155 (2순위)	0.128 (4순위)	0.127 (4순위)
개인 프로파일 위조 및 명예훼손	0.175 (2순위)	0.223 (1순위)	0.200 (2순위)	0.203 (2순위)	0.217 (1순위)	0.135 (4순위)	0.184 (1순위)	0.192 (1순위)
스토킹 및 괴롭히기	0.139 (2순위)	0.110 (5순위)	0.205 (1순위)	0.104 (6순위)	0.081 (7순위)	0.073 (7순위)	0.102 (6순위)	0.135 (3순위)
산업 스파이	0.210 (1순위)	0.207 (2순위)	0.178 (3순위)	0.215 (1순위)	0.131 (4순위)	0.117 (6순위)	0.146 (3순위)	0.183 (2순위)

판단된다.

〔표 7〕은 각 응답자별 대안선정 결과이다. '산업 스파이'와 '개인 프로파일 위조 및 명예훼손'을 가장 중요한 위협요인으로 인식하고 있으며, 'SN 스팸'을 가장 낮은 순위로 인식하는 것으로 나타났다. 이는 스팸이 이미 오랜 기간 인터넷 서비스에서 공통적으로 직면하고 있는 정보보호 위협요인으로 인식되고 있으며, 타 위협 요인에 비해 직접적이거나 경제적인 피해를 야기하는 수준이 낮기 때문이다. 또한 최근 SNS 이용실태를 살펴보면 이용자 간의 자체적인 스팸 정화 능력이 타 인터넷 서비스에 비해 높은 수준이며, 현 서비스 시스템의 필터링 능력으로도 충분히 대응 가능하기 때문인 것으로 판단된다.

V. 결 론

본 연구의 결과가 SNS 제공시 정보보호 투자 의사결정에 대하여 제시하고 있는 시사점은 다음과 같다. 첫째, 기업에서 정보보호 목적을 달성하기 위해 투자하는 경우 경제적 측면의 중요도가 기술적 측면보다

〔표 7〕 대안간 응답자별 우선순위

구 분		응답자 1	응답자 2	응답자 3	응답자 4	응답자 5	응답자 6	응답자 7	집단의견
일관성 비율(CR)		0.05	0.19	0.17	0.06	0.07	0.11	0.05	0.05
대안별중요도	SN 스팸	0.054 (8순위)	0.103 (5순위)	0.024 (8순위)	0.069 (7순위)	0.055 (8순위)	0.054 (8순위)	0.076 (7순위)	0.055 (8순위)
	멀웨어 및 피싱	0.110 (4순위)	0.043 (8순위)	0.041 (7순위)	0.195 (2순위)	0.96 (6순위)	0.070 (6순위)	0.172 (1순위)	0.099 (6순위)
	CBIR	0.116 (3순위)	0.095 (6순위)	0.061 (6순위)	0.095 (6순위)	0.69 (7순위)	0.060 (7순위)	0.060 (8순위)	0.089 (7순위)
	개인 프로파일 수집	0.085 (7순위)	0.088 (7순위)	0.172 (3순위)	0.110 (4순위)	0.133 (3순위)	0.104 (3순위)	0.141 (3순위)	0.119 (5순위)
	2차 개인정보 수집	0.092 (6순위)	0.173 (2순위)	0.200 (1순위)	0.059 (8순위)	0.130 (4순위)	0.085 (4순위)	0.140 (4순위)	0.127 (4순위)
	개인 프로파일 위조 및 명예훼손	0.255 (1순위)	0.169 (3순위)	0.194 (2순위)	0.103 (5순위)	0.176 (2순위)	0.267 (2순위)	0.168 (2순위)	0.192 (1순위)
	스토킹 및 괴롭히기	0.191 (2순위)	0.141 (4순위)	0.148 (5순위)	0.153 (3순위)	0.128 (5순위)	0.083 (5순위)	0.115 (6순위)	0.135 (3순위)
	산업 스파이	0.097 (5순위)	0.178 (1순위)	0.162 (4순위)	0.215 (1순위)	0.214 (1순위)	0.276 (1순위)	0.128 (5순위)	0.183 (2순위)

높으며, 경제적 측면의 하위기준인 서비스 이미지를 가장 중요한 평가기준으로 인식하는 것으로 나타났다. SNS는 신뢰기반의 관계지향성 서비스로, 이용자 수에 따른 망외부성 효과가 극명하게 나타나는 특성을 갖고 있기 때문에, 서비스 이미지 확보는 직접적으로 서비스 이용자 유치 및 관리에 영향을 주게 된다. 이러한 환경에서 SNS 제공자는 정보보호 침해로 인한 서비스 이미지 실추를 방지하기 위해 가장 우선적으로 투자를 해야 하는 것으로 나타났다. 둘째, 기술적 측면에서는 전통적인 정보보호 평가기준인 기밀성의 중요도가 가장 높게 나타난 것은 SNS 제공환경에서 기밀성은 가장 기본적으로 이용자에게 제공해야하는 선결조건이며 동시에 이용자의 서비스 만족도 향상을 통해 서비스 이미지 제고에 효과적이기 때문이다. 셋째, SNS 제공환경에서 정보보호 투자 시 위협요인 도출에 대한 다양한 이해관계자들의 의견에 일관성을 검증함으로써 의사결정 과정에서의 불확실성을 제거하고 효율적인 의사결정을 도와주는 기준을 마련하였다.

본 연구에서 사용된 설문 응답자는 SNS에 대한 전반적인 이용실태 및 서비스 특성 및 정보보호 기술 전반에 대한 폭넓은 이해를 갖춘 실무자나 조직의 정보보호 투자관련 의사결정에 영향을 미칠 수 있는 최고정보책임자 혹은 최고정보보호책임자이어야 하므로, 설문결과를 확보하는데 많은 어려움이 있었다. AHP 방법론에서는 설문 응답자의 전문성이 중요시되고 있지만, 본 연구에서는 설문 대상이 다양하지 않아 폭넓은 분석이 제한된 측면이 있었다. 또한 SNS에 대한 정보보호 측면에서의 연구가 미비한 상태에서, 본 연구에서 제시된 정보보호 위협요인에 대한 평가대안은 대안들 사이의 관계에 대한 상호 독립성 및 대체가능성에 대한 한계가 존재한다. 추후 연구에서는 SNS의 규모와 유형별로 정보보호 투자 목적에 적합한 정보보호 대안을 선정할 수 있는 모형을 제시하고자 한다. 또한 향후 연구에서는 서비스 제공자 측면이 아닌 서비스 이용자 측면에서 중요하게 고려하는 정보보호 요인을 분석하여 보다 가시적이고 객관적으로 SNS 제공환경에서의 정보보호 투자 의사결정을 지원할 수 있는 연구를 수행할 계획이다. 이러한 연구를 바탕으로 SNS 제공환경에서 정보보호에 대한 투자 의사결정 시 고려되는 작용원리와 의사결정에 미치는 영향을 체계적으로 분석할 수 있을 것이다.

참고문헌

[1] Martin Olausson, The People's Revolution: Implications of Web 2.0 and Social Media Applications, Strategy Analytics, Report, Dec. 2007.

[2] 한국인터넷진흥원, 인터넷이용자의 SNS이용실태조사, 연구보고서, 2009년 7월.

[3] D.M. Boyd and N.B. Ellison, "Social Network Sites : Definition, History, and Scholarship," Journal of Computer-Mediated Communication, vol. 13, no. 1, pp.210-230, Dec. 2007.

[4] comScore, The comScore Data Passport - First Half 2010, Data Passport, Feb. 2010.

[5] Compete, http://siteanalytics.compete.com

[6] eMarketer, http://www.emarketer.com/blog/index.php/future-social-media/

[7] T.L. Saaty, The Analytic Hierarchy Process, McGraw Hill, New York, 1980.

[8] T.L. Saaty, "How to Make a Decision: The Analytic Hierarchy Process," European Journal of Operation Research, vol. 48, pp.9-26, 1990.

[9] T.L. Saaty and G.V. Luis, "Diagnosis with Dependent Symptoms: Bayes Theorem and the Analytic Hierarchy Process," Operations Research, vol 46, no. 4, pp.491-502, 1998.

[10] 공희경, 전효정, 김태성, "AHP를 이용한 정보보호 투자 의사결정에 대한 연구," Journal of Information Technology Applications & Management, 15(1), pp.139-152, 2008년 4월.

[11] K.J. Soo Hoo, How much is enough? A Risk-Management Approach to Computer Security, Stanford University, 2000.

[12] L.A. Gordon and M.P. Loeb, "The Economics of Information Security Investment," ACM Transactions on Information and System Security, vol. 5, no. 4, pp.438-457, Nov. 2002.

[13] C. Blatchford, "Information Security Controls - Are They Cost-effective," Computer Audit Journal, vol 3, pp.11-19. 1995.

[14] A. Davis, "Return on Security Investment- Proving It's Worth It," Network Security, vol 2, pp.8-10, Nov. 2005.

[15] H. Cavusoglu, B. Mishra and S. Raghunathan, "A Model for Evaluating IT Security Investments," Communications of the ACM, vol 47, no. 7, pp.87-92, Jul.. 2004.

[16] NIST, An Introduction to Computer Security, NIST Special Publication 800-12, 1996.

[17] Vincent C.S. Lee, "A Fuzzy Multi-criteria Decision Model for Information System Security Investment," LNCS 2690, pp.436-441, Mar. 2003.

[18] L.D. Bodin, L.A. Gordon and M.P. Loeb, "Evaluating Information Security Investments Using the Analytic Hierarchy Process," Communications of the ACM, vol 48, pp.79-83, Feb. 2005.

[19] 조찬식, "정보사회에서의 정보보안에 관한 연구," 한국문헌정보학회지, 34(1), pp.155-180, 2000년 3월.

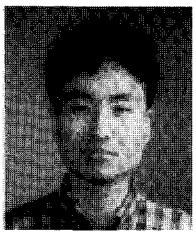
[20] ENISA, Security Issues and Recommendations for Online Social Networks, ENISA Position Paper No.1, Oct. 2007.

[21] 이기식, "인터넷시대 사이버보안의 인식양태 및 정책대안," 한국공공관리학보, 22(4), pp.99-127, 2008년 12월.

〈著者紹介〉

성 기 훈 (Kihoon Sung) 학생회원
2004년 8월: 한국과학기술원 산업공학과 학사
2004년 9월~현재: 과학기술연합대학원대학교 정보통신기술경영학과 통합(박사)과정
〈관심분야〉 기술경제성분석, 주파수 정책, 소셜미디어 등

공 희 경 (Hee-Kyung Kong) 정회원
2008년 8월: 충북대학교 경영정보학과 졸업
2008년 8월: 충북대학교 경영학 박사
2009년 3월~현재: 한국전자통신연구원 기술전략연구본부
〈관심분야〉 정보보호, 기술경영, 기술경제성분석



김 태 한 (Taehan Kim)
1996년 2월: 서울대학교 경영학과 졸업
2005년 2월: 한국과학기술원 산업공학과 박사
2004년 12월~현재: 한국전자통신연구원 기술전략연구본부 선임연구원
〈관심분야〉 전파자원 활용정책, 모바일 비즈니스 모델 등