www.calsec.or.kr
http://dx.doi.org/10.7838/jsebs.2013.18.4.301

AHP 기법을 활용한 Big Data 보안관리 요소들의 우선순위 분석에 관한 연구

A Study on Priorities of the Components of Big Data Information Security Service by AHP

수브르더 비스워스(Subrata Biswas)*, 유진호(Jin Ho Yoo)**, 정철용(Chul Yong Jung)***

초 록

IT기술의 발전은 기존의 컴퓨터 환경과 더불어 수많은 모바일 환경 및 사물 인터넷환경을 통해 사람의 삶을 편리하게 하고 있다. 이러한 모바일과 인터넷 환경의 등장으로 데이터가 급속히 폭증하고 있으며, 이러한 환경에서 데이터를 경제적인 자산으로 활용 가능한 Big Data 환경과 서비스가 등장하고 있다. 그러나 Big Data를 활용한 서비스는 증가하고 있지만, 이러한 서비스를 위해 발생되는 다량의 데이터에는 보안적 문제점이 있음에도 불구하고 Big Data의 보안성에 대한 논의는 미흡한 실정이다. 그리고 기존의 Big Data에 대한 보안적인 측면의 연구들은 Big Data의 보안이 아닌 Big Data를 활용한 서비스의 보안이 주를 이루고 있다. 이에 따라서 본 연구에서는 Big Data의 서비스 산업의 활성화를 위하여 Big Data의 보안에 대한 연구를 하였다. 세부적으로 AHP 기법을 활용한 Big Data 환경에서 보안관리를 위한 구성요소를 파악하고 그에 대한 우선순위를 도출하였다.

ABSTRACT

The existing computer environment, numerous mobile environments and the internet environment make human life easier through the development of IT technology. With the emergence of the mobile and internet environment, data is getting bigger rapidly. From this environment, we can take advantage of using those data as economic assets for organizations which make dreams come true for the emerging Big Data environment and Big Data security services. Nowadays, Big Data services are increasing. However, these Big Data services about Big Data security is insufficient at present. In terms of Big Data security the number of security by Big Data studies are increasing which creates value for Security by Big Data not Security for Big Data. Accordingly in this paper our research will show how security for Big Data can vitalize Big Data service for organizations. In details, this paper derives the priorities of the components of Big Data Information Security Service by AHP.

키워드 : 보안관리, 보안 구성요소
Big Data, Security Management, Security Elements

* First Author, Department of Business Administration, Sangmyung University(subhongiku09@gmail.com)
** Co-Author, Department of Business Administration, Sangmyung University(jhyoo@smu.ac.kr)
*** Corresponding Author, Department of Business Administration, Sangmyung University (cyjung@smu.ac.kr)
2013년 10월 10일 접수, 2013년 11월 05일 심사완료 후 2013년 11월 20일 게재확정.

1. 연구 배경

데이터를 활용한 IT 환경은 인터넷 환경을 통하여 이용자들에게 편리하게 정보를 제공하고 있다. 그러나 급격한 IT의 발달과 범위가 융합 환경과 함께 증가함에 따라서 각 기업들은 과거 아날로그 시대에 비해 해킹, 피싱 사이트, 악성코드 등의 보안의 취약점이 지속적으로 증가하고 또한 지능화 되고 있다. 최근 IT 패러다임이 IT의 환경이 생활로 스며드는 일상화가 이루어지는 스마트 시대로 변화하고 있다. 스마트 시대에 따른 데이터의 급격한 증가로 인해 -Big Data 환경은 접근이 용이하며 응용 프로그램 환경은 네트워크화 되고, 시스템 환경은 보안, 액세스 제어, 암호화 및 규정 준수를 통해 공유된다. 기업들은 기존의 정형 데이터 외에 SNS(Social Networking Service) 텍스트 및 동영상 등의 비정형 데이터까지 포함한 대용량 데이터로부터 가치를 추출하고 결과를 분석하는 Big Data 환경에 관심을 집중하고 있다. 데이터량의 급증과 비정형 데이터 분석이 가능해짐에 따라 Big Data 분석은 활용 방법에 따라 새로운 시장을 형성할 것으로 전망되고 있다. Big Data 환경의 특성으로 인하여 기존의 컴퓨팅 환경보다 체계적인 방법으로 데이터를 관리할 필요성이 제기되고 있다.

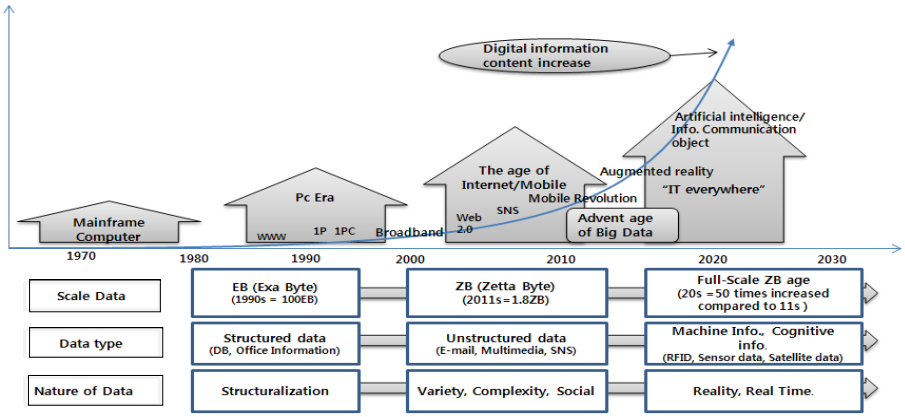
SNS 등 비정형 데이터 분석에 따른 프라이버시 침해논란과, 기업과 개인 간의 데이터 통제권 논란이 주요 이슈로 부상하고 있다. 새로운 개념 및 환경의 도입은 시장의 선진입이 중요시 되고 있어 Big Data 환경의 활성화는 기하급수적으로 늘어날 것으로 예상된다. 그러나 이에 따른 Big Data 환경의 역기능에 대한 취약성도 문제가 될 것으로 예상되고 있다. 특히 취약성에 관한 조치는 주로 사후관리로 이루어지고 있으며, 예방조치에 대한 중요성이 부각되지 못하고 있는 실정이다. 따라서 사후관리 뿐만 아닌 예상되는 상황에 대한 예방조치에 대한 보안적 관리 필요성이 제기되고 있다. 이에 따라 본 연구에서는 Big Data 서비스 활성화를 위해 Big Data의 동향에 대해 살펴보고 기존의 Big Data 관련 연구 및 보안 수준 평가 등을 통해 Big Data 서비스 활성화를 위한 보안적으로 관리 되어야 할 핵심적인 요인들을 도출하는 것을 목적으로 한다.

2. 선행 연구

2.1 Big Data의 발전 동향

Big Data는 대용량 데이터를 일컫는 의미로, 과거에는 국가적으로 수행하는 일부 통계조사에서 의도적으로 설문조사를 통해 데이터나 정보를 얻어왔다. 그러나 현재는 인터넷과 스마트폰, SNS과 Sensor 데이터를 통해 때와 장소를 가리지 않고 만들어지고 있다. Big Data에 대한 개념이 새로운 이슈가 아님에도 근래에 각광받는 이유는 정보기술의 발달로 데이터 처리능력의 발달과 저장 공간이 확대되었기 때문이다. 이에 따라 기업 또는 기관에서 데이터를 이용한 새로운 정보의 가치·지식창출을 원하게 된 것이 주된 이유라 할 수 있다.

최근에 해외 조사 기관 및 컨설팅 그룹 등은 미래의 차세대 키워드로 'Big Data'를 선정하고 경제적 가치에 주목하고 있다. <Figure



〈Figure 1〉 Tend of Increase the Amount of Information Around the World[15]

2>처럼 Big Data가 불확실해지고 있다. 그러나 Big Data의 현실적 보안 문제나 역기능에 관한 연구사례는 미흡한 실정이다. 따라서 Big Data 서비스 산업의 안정적인 활성화를 위해 핵심적으로 관리되어야 할 보안 요인들에 대한 연구가 필요한 시점이다.

2.2 새로운 컴퓨팅 환경에서의 보안관리 모델 연구

신경아 외[11]의 연구에서는 Cloud 특성에 맞는 정보보호 관리체계를 설계하기 위하여 Cloud 서비스의 핵심요소를 위험관리 영역으

Future Society characteristics and role of Big Data

Future Society characteristics	Role of Big Data
Uncertainty ⇒ Insight	- Pattern analysis and future outlook based on social phenomena real world data. - Scenario simulation for various potential. - Suggesting insights considering multifaceted situation. - Flexibly handle changing condition by the number of scenarios.
Risk ⇒ Responsiveness	- Risk analysis through pattern analysis of environment, fiction, monitoring information over signal capture. - Issues recognize from the picture, then analyze it. Based on picture analysis rapid decision making and support real time response. - Enhance transparency of companies and countries management and reduce waste elements.
Smart ⇒ Competitive	- Possible situational awareness through large scale data analysis, artificial intelligence and other services. - Personalized, intelligent services offer expand. - Support the optimal choice through the social needs analysis assessment, credit, reputation analysis. - Expand product competitiveness through the analysis of customer trend change.
Convergence ⇒ Creativity	- Creative new value through interaction of different field such as Medical information, Automobile information, Construction information, Environment information. - Complex convergence data analysis by causation, correlation to improve the safety of trial and error to minimize. - Utilizing large amount of data to create convergence market.

〈Figure 2〉 Future Society Characteristics and Role of Big Data[15]

로부터 도출하였다. 그리고 제안한 정보관리 체계는 기본적인 보안관리가 누락되지 않도록 기존 정보보호 관리체계의 모든 통제영역을 포함하고 있으며. 또는 온라인 셀프환경에 따른 서비스 이용을 지원하고 서비스계약, 제공자 사업현황을 포함하는 서비스 보안관리를 추가하여 설계하였다.

장은영 외[12]의 연구에서는 모바일 Cloud 서비스는 모바일 서비스와 무선네트워크, Cloud 서비스가 융합된 서비스로 다양하고 확장된 안전한 서비스를 배포하고 위협 발생 시 적절하게 대응하기 위한 방안에 대한 필요성을 제기하였다. 모바일 단말 무선 네트워크, Cloud 컴퓨팅 서비스의 위협을 분석하여 모바일 Cloud 서비스의 위협과 위협에 대응하기 위한 방안을 정의하였으며, 위협 시나리오를 기반으로 잠재된 위협을 예상하고 대응할 수 있는 방안을 제시하였다.

노봉남[13]의 연구에서는 3-screen, 가상화, 네트워크 기반의 어플리케이션 등 On-demand 형태의 다양한 서비스가 제공되면서 해당 환경에서 발생할 수 있는 보안 위협을 탐지, 예방하기 위한 보안기술의 필요성을 제시하였다. 세부적으로 Cloud 컴퓨팅 환경에서 해결해야 할 보안 문제에 대하여 이슈와 사례를 기술하고 이용자 입장에서의 Cloud 컴퓨팅 보안 평가 요소를 제시하였다.

박춘식[14]의 연구에서는 Cloud 서비스 사용자(기업 등)들은 Cloud 컴퓨팅 특성에 의한 여러 가지 위험들에 대해서 Cloud 컴퓨팅 환경으로 인한, 보안을 포함한 여러 가지 주요 이슈들에 대하여 검토하였다. 그리고 보안에 관한 문제들을 보다 구체적으로 분석하고 Cloud 컴퓨팅에 관한 위협들을 식별하여 보안 위험을 줄일 수 있는 대략적인 대응책들을 제안하였다.

이와 같은 선행 연구를 기반으로 본 연구에서는 Big Data의 동향과 특성을 조사하고 최근 Big Data의 보안적 이슈에 대한 연구 및 Big Data의 보안적 이슈들을 바탕으로 Big Data 서비스 활성화를 위한 보안관리 측면에서의 연구를 진행하고자 한다.

2.3 Big Data 보안이슈

Big Data의 보안적 관점에서 보았을 때 “Security by Big Data”가 아닌 “Security for Big Data” 관점의 연구는 현재까지 미흡한 상황이다. Big Data의 처리 및 컴퓨팅 인프라를 보다 안전하게 만들기 위해 Cloud Security Alliance[15]와 SOPHOS[20]에서는 Big Data의 보안 문제점을 다음과 같이 6가지로 분석하였다.

첫째 Big Data 환경에서는 분산 처리를 위해 다수의 정보처리를 위하여 파일 및 데이터를 서버 등에 저장하는 과정에서 분산 데이터의 위·변조와 같은 보안적 위험이 존재할 가능성이 있다.

둘째 Big Data 환경에서는 스마트폰, 노트북, 태블릿 PC와 같은 BYOD(Bring Your Own Device)들이 쉽게 접속 할 수 있다. 이와 같은 많은 휴대용 기기 또는 장치를 통하여 입력되는 데이터의 유효성에 대한 실시간 관리가 어렵다.

셋째 Big Data 환경에서는 다양한 기기 또는 장치를 통하여 대량의 데이터를 양산함에 있어서 사용자들이 단순 또는 오남용의 비의

도적 행동으로 발생되는 사고(바이러스 유입 등)에 대하여 보안성을 강화하고 사고를 예방할 수 있는 24/7 모니터링이 어렵다.

넷째 기존의 환경과 같이 모든 데이터를 암호화 하여 관리하기 어려워짐에 따라, Big Data 환경의 경우에는 end-to-end에서 필요한 부분을 선별적으로 암호화하기 때문에 데이터 보안에 취약해질 수 있다.

다섯째 Big Data 환경에서는 접근통제관점에서 가능한 많은 데이터를 공유하며 해당 데이터에 대한 체계적인 접근통제를 할 필요성이 있다. 사용자의 접근권한을 세분화하여 자산을 체계적으로 관리하는 것이 중요하다.

여섯째 Big Data 환경에서는 보안사고 원인파악에 시간과 노력이 상대적으로 더 필요하기 때문에 어떤 공격이 일어났는지, 취약점은 무엇인지 알기 위해 감사를 더욱 세분화하여 시행해야 할 필요가 있다.

이처럼 기존의 컴퓨팅이 Big Data 환경으로 변함에 따라 새로운 취약점이 나타나고 있다. 때문에 기존과 달리 Big Data 환경에서 보안적 요소를 적용하기 위한 각 요소들을 차별적으로 적용하기 위한 방안이 필요하다.

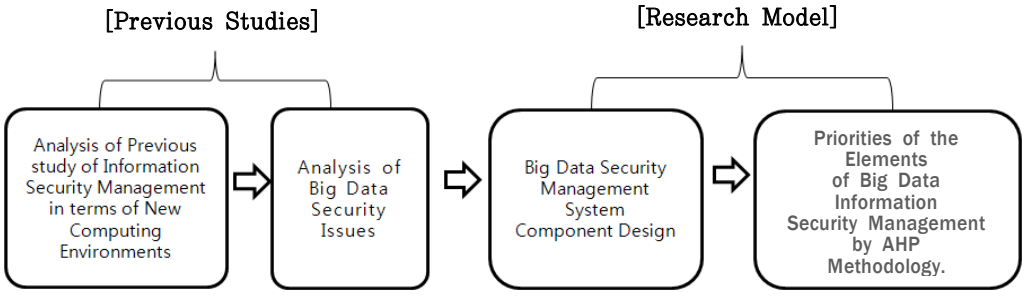
3. Big Data 정보보안 구성요소 우선순위 분석

3.1 연구모형 설계

기존의 다른 연구사례를 바탕으로 유사 연구 사례를 통해 Big Data의 보안관리와 관련된 보안적 요소들을 도출하고, 도출된 지표를 바탕으로 설문 및 AHP 분석을 통해 각 지표들 중 Big Data 보안관리에 필요한 요소들 중 가장 우선시 되어야할 요소를 분석하고자 한다. 본 연구에서는 Veiga and Eloff[17]의 연구를 바탕으로 기존의 기업 정보보안 수준평가 지표 연구 논문들을 Mapping하여 새로운 Big Data 보안관리 요소들을 도출하고자 한다.

3.2 Big Data를 위한 정보보안 구성요소 조사 및 분석

Veiga and Eloff[17]의 연구에서는 보안을 4개의 단계로 나누었다. 보안의 1, 2차 단계는 IT 환경 보안에 대한 지극히 기술적인 접근법으로 특징지어졌으나 시간이 흐르면서 조직의



〈Figure 3〉 Priorities of the Components of Big Data Information Security Service Research Methodology

거버넌스가 보안관리에 있어 중요한 역할을 하며 최고 경영진들이 관여해야 한다는 것을 인지함에 따라 기술적 보호 메커니즘과 경영진 관여로 불리는 이 두 단계의 병행이 지속되어왔다. 보안의 3차 단계는 보안을 하나의 생활양식으로 만들어 조직 내 효과적인 보안 문화를 조성하기 위해 각자가 행하는 보안활동을 업무의 하나로 편입해야 한다는 것에 중점을 두었으며, 보안 문화를 인식・태도와 관련된 가정으로 정의할 수 있으며(Martins and Eloff, 2002), 4차 단계에서는 핵심 요인 중 하나로 사회공학적 리스크들을 방지하는 것이며 기술의 결함보다는 사람의 실수가 대부분의 보안 침입의 근본 원인으로 언급했다(PWC, 2004). Von Solms[21]는 적절한 보안 거버넌스가 이러한 리스크들을 다루는 필수 요소라는 점을 강조했다. 위에서 설명한 Veiga and Eloff [17]의 연구를 바탕으로 정보보안 수준평가 연구 논문들을 Mapping하여 새로운 Big Data 보안관리 요소들을 도출하였다. 정보보안 관리 및 수준평가 연구 논문들의 설명은 다음과 같다.

오남석[1]의 연구에서는 정보통신 서비스 제공 기관 및 업체가 현재의 보안 상태를 단계별로 등급화 된 지표에 따라 평가하고, 지속적으로 정보보호 수준을 상위 단계로 개선해 나갈 수 있도록 정보보호 수준 평가방법을 제안하였다. 이를 위해 SP800-26의 17개 분야, SP800-53의 3개 분야, ISMS 15개 분야, ISO27001의 10개 분야를 분석하여 중복적 분야를 제거하고 전문가 회의를 통해 54개의 평가항목을 도출하였다.

이희명[2]의 연구에서는 첨단기술과 핵심정보의 불법적 유출로 인해 피해사례가 증가하고 있으나, 기업의 보안사고 방지와 예방 체제는 일부 영역에 국한되어 효율적인 대응을 하지 못하고 있다고 분석하였다. 일부 기업에서 안전장치로 ISMS를 도입하여 운영하고 있으며 정보보호 활동의 성과를 정량적으로 평가하여 대응방안 수립에 활용 가능하도록 사례연구와 실용성에 초점을 맞추어 모델을 개발하였다.

이영규[3]의 연구에서는 정보보안 평가와 관련이 있는 기존연구들을 검토하여 평가지표를 제시하면서 보안담당자와 보안컨설턴트 등 정보보안전문가들을 대상으로 정보보안 평가가 내용의 타당성과 평가의 용이성 그리고 평가의 신뢰성 측면에서 얼마나 적합한지에 대해 일련의 부합성 분석(coincidence analysis)을 실시하여 평가목적에 부합하는 정보보안 평가지표를 선정하여 제시하였다. 고미현[4]의 연구에서는 기업 프로세스의 전사적 차원에서 정보보호 수준을 체계적으로 측정할 수 있도록 균형성과 표를 활용한 평가 모형의 개발 및 수준단계의 진단을 위한 정보보호 수준 통합 평가체계를 제시하였다. ISO[5], Eloff and Eloff [5], McCarthy and Campbell[7] and Tudor[8] 각 연구에 따르면, ISO/IEC 17799와 McCarthy and Campbell의 조직 성숙도 평가 모델 구성요소들은 보안 구성요소들의 범위를 다루는데 있어 가장 포괄적이며 Eloff and Eloff[6] 연구의 접근법은 윤리적 가치를 언급하는 유일한 연구이다. Tudor[8]의 연구에서는 경영진이 직원들을 신뢰하고 직원들이 경영진을 신뢰한다면, 새로운 절차를 시행하고 보안에 따른 행동 변경을 지시하기 더 쉬워지는 가설을 세워 유일하게 신뢰를 보안요소로 제시하였다. KISA[9] and NISTIR[40]의 연구에서는 정보자산의 기밀성, 무결성, 가용성을 달성하기 위하여 각종 보안 대책을 관리하고,

〈Table 1〉 Mapping between Info. Security Governance and Info. Security Evaluation level Components

Code	Information Security Components	NamSeok Oh[1]	Hee Myung Lee[2]	Yeongku Lee[3]	Mi Hyun Ko[4]	ISO[5]	Eloff[6]	McCarthy[7]	Tudor[8]	KISA[9]	NISTIR[10]	%
1	Corporate governance					O				O	O	30%
2	Info. security strategy		O	O				O				30%
3	Leadership in terms of guidance and executive level representation					O	O	O	O			40%
4	Security organization	O	O	O	O	O	O	O	O	O	O	100%
5	Security policies, standards, and guidelines	O	O	O	O	O	O	O	O	O	O	100%
6	Measurement/Metric/Return on investment				O		O	O				30%
7	Compliance and monitoring	O	O	O		O	O	O	O	O	O	90%
8	User management	O	O	O	O	O		O		O	O	80%
9	User awareness, training and education	O	O	O	O	O	O	O	O	O	O	100%
10	Ethical values and conduct						O					10%
11	Trust								O			10%
12	Certification against a standard			O		O	O					30%
13	Best practice and baseline consideration					O	O	O	O			40%
14	Asset management	O	O	O	O	O	O		O	O	O	90%
15	Physical and environmental controls	O	O	O	O	O	O	O	O	O	O	100%
16	Technical operations control	O	O	O	O	O	O	O	O	O	O	100%
17	Business continuity planning	O	O	O	O	O		O	O	O	O	90%
18	Disaster recovery planning	O	O	O	O			O	O	O	O	80%
19	Risk assessment process	O	O	O	O	O		O		O	O	80%

위험기반 접근방법에 기초하여 구축, 운영, 모니터링 및 검토, 개선 등의 주기를 거쳐 정보보호를 관리하고 운영하는 주요 추진체계, 구축 및 운영 방법 등을 제시하였다. 이와 같은 연구들은 Big Data 환경을 고려한 것이 아니기 때문에 Big Data 환경을 위한 보안관리 요소를 도출하기 위에서 <Table 1>과 같이 각 연구에서 제시하고 있는 핵심적인 보안 요소에 대하여 공통적인 특성을 가진 요소들을 맵핑하고 도출하였다.

Veiga and Eloff[17]의 연구에서 제시된 '프라이버시'에 대한 정보보안 요소는 해당 연구분야가 넓으며 개인정보를 포함하여 현재 다른 연구자들의 연구에서 활발하게 이루어지고 있기 때문에 본 연구에서는 프라이버시에 대한 항목은 보안관리 요소에서 보안 전문가 회의를 통해 제외 하였다. 각 논문에 언급된 이슈 및 보안구성요소들을 나열하여 선행연구와 비교하여 <Table 2>과 같은 보안구성 요소를 도출하였다. <Table 1>의 보안구성 요소를 유사연구에서 언급하는 보안구성 요소들과 Mapping하여 연관성이 높은(60% 이상) 구성 요소를 도출하였으며 본 연구의 Mapping 결과 항목은 모두 절대적인 기준에서 보안 지표 항목으로 타당한 것으로 나타났다. 절대적인 수준은 3.0(60%)을 기준으로 사용하였다[19]. <Table 2>는 도출한 Big Data 보안관리의 11개 구성요소이다.

Big Data 보안관리의 각 구성요소들을 Mapping한 결과 보안조직 및 역할, 보안정책 및

〈Table 2〉 Big Data Security Components

Code	Big Data Security Components											
3	Security organization	O	O	O	O	O	O	O	O	O	O	100%
4	Security policies, standards, and guidelines	O	O	O	O	O	O	O	O	O	O	100%
6	Compliance and monitoring	O	O	O		O	O	O	O	O	O	90%
7	User management	O	O	O	O	O		O		O	O	80%
8	User awareness, training and education	O	O	O	O	O	O	O	O	O	O	100%
14	Asset management	O	O	O	O	O	O		O	O	O	90%
15	Physical and environmental controls	O	O	O	O	O	O	O	O	O	O	100%
16	Technical operations control	O	O	O	O	O	O	O	O	O	O	100%
17	Business continuity planning	O	O	O	O	O		O	O	O	O	90%
18	Disaster recovery planning	O	O	O	O			O	O	O	O	80%
19	Risk assessment process	O	O	O	O	O		O		O	O	80%

지침, 사용자 인식제고 및 교육, 물리적/환경적 통제, 기술적 들이 모두 100%로 가장 높게 나왔으며, 법적준거성 확인 및 교육, 자산식별 및 관리, 업무 연속성 계획이 90% 뒤를 이었다. 마지막으로 사용자 관리, 위험분석 및 보안사고 관리, 재해복구 계획이 80%로 나타났다.

4. Big Data를 위한 정보보안 구성요소 우선순위 도출

4.1 우선순위 도출을 위한 조사 설계

계층적 의사결정(AHP) 기법은 Tomas Saaty (1977)에 의해 개발된 다 기준 의사결정모델(multicriteria decision making model)로, 의사결정 프로세스를 체계적으로 분석하고, 여러 평가항목의 가중치를 쌍대비교(Pairwise comparison)를 통해 단계적으로 도출함으로써 대안들에 대한 합리적 평가를 지원한다. 이 방법은 의사결정에 필요한 여러 요소들을 계층화시켜 각 요소별, 요소간의 관계를 보다 상세히 논리적으로 보여주는 기법이다. Big Data 정보보호 구성요소들의 중요도를 측정하기 위해 AHP의 쌍대비교 분석을 하고자 설문조사를 진행하였다. Big Data 보안관리 구성요소의 우선순위를 도출하기 위한 AHP의 쌍대비교를 통해 11개의 Big Data 보안관리 항목들의 가중치를 산출하였다. 설문조사는 정보보호 분야 전문가 25명(국내 정보보호 관련 교수 4인, 현업 10년 이상 경력의 기술적 보안관리 전문가 6인, 물리적 보안관리 전문가 6인, 관리적 보안

	Security Organization	Security Policy	Compliance & Monitoring	User Management	User Awareness	Assets Management	Physical Control	Technical Control	BCP	DRP	Risk Management
Security Organization	1	2.018	1.5368	2.2036	0.8325	1.5692	1.5887	1.6686	0.8687	0.7056	1.4685
Security Policy		1	1.34	1.4685	1.7532	0.9475	0.7411	0.9161	1.5574	1.0553	0.6322
Compliance & Monitoring			1	0.9258	0.9475	1.3852	0.6607	0.5949	1.1962	0.671	1.5123
User Management				1	0.7201	1.5439	1.4051	1.4479	1.0134	1.0914	1.4931
User Awareness					1	1.1279	1.2457	1.4479	1.4182	1.0149	0.5419
Assets Management						1	1.8828	1.4479	1.509	1.0614	1.3769
Physical Control							1	1.4479	0.7904	0.7761	0.3261
Technical Control								1	1.4073	1.5574	1.8027
BCP									1	1.1486	0.7489
DRP										1	1.2624
Risk Management											1

〈Figure 4〉 The Geometric-mean value of Big Data Security Components

								Consistency Index			0.067
	Security Organization	Security Policy	Compliance & Monitoring	User Management	User Awareness	Assets Management	Physical Control	Technical Control	BCP	DRP	Risk Management
Weight	0.120	0.091	0.080	0.091	0.093	0.093	0.075	0.091	0.077	0.092	0.097

〈Figure 5〉 Weight of Big Data Security Components

관리 전문가 5인, 그리고, 현업 10년 이상 경력의 보안 컨설턴트 4인)을 대상으로 실시하였다.

4.2 Big Data를 위한 정보보안 구성요소 도출

AHP 분석의 경우, 중요도 평가과정에 집단이 참가하여 그 의견을 취합하는 방법은 집단의 동의를 구하여 단일의 중요도를 계산하는 방법과 개별적으로 중요도를 평가한 후 통합하는 방법이 있으나, 본 연구에서는 후자의 방법을 택하였고 25명 전문가의 의견을 기하평균(geometric mean)을 사용하여 집단의견의 중요도를 산출하였다. 중요도 산출을 위해서는 AHP 분석 프로그램 Expert Choice 2000을 사용하였다. <Figure 4>은 25개 설문지의 의사결정을 일관성 있게 통합하기 위하여 산출된 기하평균이다.

<Figure 5>은 기하평균을 토대로 산출된 가중치 결과이다. Consistency Index 값이 0에 가까울수록 응답자의 일치성이 높아서 그 결과의 신뢰성이 높아진다. 실험적으로 전문가들의 응답결과는 0.10 이하의 Inconsistency Index를 보이는 것으로 나타났으며, 0.10 이하의 값은 일치성을 신뢰할 수 있음을 의미한다. 본 연구에서는 25개 설문지의 영역별로 평가기준의 일관성 비율을 산출하였고, 일치성비율은 0.067로 유의한 수준의 응답으로 판단하였다. <Figure 6> 일치성 지수의 수식은 다음과 같다.

Consistency Index: CI

$$CI = \frac{\lambda max - n}{n-1}$$

- CI <0.1 accept
- CR – CI/RI < 0.1 accept
  (CR= Consistency Ratio)
- RI = Random Index

〈Figure 6〉 Consistency Index

<Table 3>는 영역별 상대적 가중치를 구한 결이다. “보안조직 및 역할”이 0.120으로 가장 높았으며, 그 다음 “위험분석 및 보안사고 관리”의 가중치가 0.097, “사용자 인식제고 및 교육”과 “자산 식별 및 관리”가 0.093으로 같았으며, “재해복구 계획”이 0.092, “사용자 관리”와 “기술적 통제”가 0.091로 같았다. 그리고 “법적 준거성 확인 및 교육”이 0.080, “업무연속성계획”이 0.077, “물리적/환경적 통제”가 0.075로 나타났다. 전체 대상자의 30%에게 정성적인 인터뷰와 문헌 분석 결과, 보안조직과 위험분석이 각각 1, 2순위로 책정된 것은 첫째, 정보보호관리 활동을 수행하고 검

〈Table 3〉 Priorities of Big Data Security Components

Big Data Security Components	Weight	Priorities
Security organization	0.120	1
Security policies, standards, and guidelines	0.091	5
Compliance and monitoring	0.080	6
User management	0.091	5
User awareness, training and education	0.093	3
Asset management	0.093	3
Physical and environmental controls	0.075	8
Technical operations control	0.091	5
Business continuity planning	0.077	7
Disaster recovery planning	0.092	4
Risk assesment process	0.097	2

증하는 인력(사람)들에 대한 책임, 권한 및 상호연관 관계를 정의하고 문서화 하는 것과 조직의 위험을 관리할 보안 조직의 구성이 가장 중요하며 둘째, 구성된 보안 조직에 의해 기업의 위험분석(식별된 정보자산에 영향을 줄 수 있는 모든 위험과 취약성, 위험을 식별하고 분류해야 하며 정보자산의 가치와 위험을 고려하여 잠재적 손실에 대한 영향을 식별·분석)이 다른 보안 요소들 보다 선행적으로 수행되어야 하기 때문인 것으로 분석되었다. 본 연구의 시사점으로 Big Data 보안관리에서는 기술적 측면보다 조직구성, 정책수립, 등이 거버넌스 측면의 노력이 더 중요한 평가기준으로 인식되는 것으로 나타났다.

5. 결 론

본 연구에서는 Big Data의 동향과 특성을 조사하고 최근 Big Data의 보안적 이슈에 대한 연구, 그리고 Big Data의 보안 이슈들을 바탕으로 Big Data 서비스 활성화를 위한 보안관리 측면에서의 연구를 진행하였다. 현재의 Big Data 보안 연구는 “Security for Big Data”가 아닌 “Security by Big Data”가 주를 이루고 있었으며, 그에 따라 기존의 Big Data 보안 연구의 내용만으로는 얻고자 하는 Big Data 서비스 활성화를 위한 보안관리 측면의 요소들을 도출하는데 한계가 있었다. 따라서 본 연구에서는 기존 연구사례를 바탕으로 유사한 사례에서 Big Data 서비스의 보안관리에서 필요한 11가지의 요소들을 도출하였으며, 도출된 11가지 요소들의 주요 활동을 정의하고 Big Data 정보보안 관리 구성 요소의 우선순위를 도출하기 위해 AHP의 쌍대비교를 통해 11개의 Big Data 정보보안 관리 항목들의 가중치를 구하여 우선순위를 제시하였다. 본 연구에서는 한계점으로는 AHP 방법론을 통하여 설문 응답자의 전문성이 중요시되고 있지만, 설문 대상이 다양하지 않아 폭넓은

분석이 제한된 측면이 있었다. 그리고 현재 Big Data 보안관리에 대한 연구가 많이 이루어지지 않았기 때문에 도출한 11개의 요소들의 세부항목에 대해 추가적인 연구가 필요하며, Big Data의 서비스 활성화를 위한 정보보안관리 체계의 적용이 실제 부족하다는 점이다. 본 연구는 Big Data의 서비스 활성화를 위한 정보보안관리 연구가 현재까지 많이 이루어지지 않고 있는 “Security for Big Data” 측면에서 Big Data 보안관리에 대한 새로운 지표와 Big Data의 보안관리 방향을 제시하는데 의미를 두고자 한다. 본 연구의 분석 결과에 따르면 Big Data의 보안 이슈들을 해결하기 위해서 기술적인 접근도 중요하지만 관리적, 정책적, 거버넌스적 접근이 중요하며, Big Data의 보안 이슈에 대한 현실적인 사용자 관리 및 사용자 교육, 현실적인 보안 이슈에 대한 정확한 인식제고가 중요하다고 판단된다. 최근 보안 이슈는 역시 점차 지능화되고 있으며 양적인 문제만이 아니라 질적인 측면에서도 피해의 규모가 날로 심각해지고 있다. 따라서 이런 이슈들을 극복하기 위한 치밀한 보안조직과 보안정책 및 지침, 사용자 교육 양성 및 인식 제고가 매우 중요하다고 판단된다. 마지막으로, 물리적, 관리적, 기술적 부분으로 나뉘어 관리되어온 보안과 관련된 이슈들의 기반에는 “사람”이 핵심으로 분석되기 때문에 향후 많은 양의 불특정한 데이터를 다루는 Big Data 보안관리에 있어, 기반이 되는 사람에 대한 연구와 지표 개발은 필수가 될 것이다. 따라서 향후 연구로는 Big Data 보안관리 개선을 위하여 “사람”의 의식 기반에 관련된 지표를 탐색해보고자 한다.

References

[1] Oh, N. S., Han, Y. S., Eom, C. W. Oh, K. S., Lee, B. G., “Developing the Assessment Method for Information Security Level,” Journal of the Society for e-Business Studies, Vol. 16, No. 2, pp. 159-169, 2011.

[2] Lee, H. M., Lim, J. I., “A Study on the Development of Corporate Information Security Level Assessment Models,” Korea Institute of Information Security and Cryptology, Vol. 18, No. 5, pp. 161-170, 2011.

[3] Lee, Y. K., Kim, S. H., “A Development of Evaluation Indicators for Information Security by means of the Coincidence Analysis,” Korea Society of IT Services, Vol. 7, No. 3, pp. 175-198, 2008.

[4] Ko, M. H., Kong, H. K., Kim, T. S., “Using a Balanced Scorecard Framework to Evaluate Corporate Information Security Level,” Telecommunication Review, Vol. 19, No. 6, pp. 925-935, 2009.

[5] ISO/IEC 17799(BS 7799-1), “Information technology, Security techniques, Code of practice for information security,” 2005.

[6] Eloff, j. H. P. and Eloff, M., “Integrated Information Security Architecture,” Computer Fraud and Security, pp. 10-16, 2005.

[7] McCarthy, M. P. and Campbell, “Security Transformation,” McGraw-Hill : New York, 2001.

[8] Tudor, J. K., “Information Security Architec-

ture-An integrated approach to security in an organization," Boca Raton, FL : Auerbach, 2000.

[9] KISA, MSIP, "Korea Information Security Management System Guideline(ISMS)," March, 2013.

[10] NISTIR 7628, "Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security," sep. 2010.

[11] Shin, K. A., Lee. S. J., "Information Security Management System on Cloud Computing Service," Journal of The Korea Institute of Information Security and Cryptology, Vol. 22, No. 1, pp. 155-167, 2012.

[12] Jang, E. Y., Kim, H. J., Park, C. S., Kim, J. Y., Lee. J. I., "The study on a threat countermeasure of mobile Cloud services," Journal of The Korea Institute of Information Security and Cryptology, Vol. 21, No. 1, pp. 177-186, 2011.

[13] Noh, B. N., Choi, J. G., "Security Technology Research in Cloud Computing Environment," Journal of Security Engineering, Vol. 8, No. 3, pp. 371-383, 2011.

[14] Park, C. S., "Study on Security Considerations in the Cloud Computing," Journal of academia-industrial technology, Vol. 12, No. 3, pp. 1408-1416, 2011.

[15] National Information Society Agency (NIA), "Big Data era opening a new future," 2013.

[16] "CSA Big Data Working Group Releases Top 10 Big Data Security and Privacy Challenges Report," Cloud Security Alliance, 2012.

[17] Da Veiga, J. H. P. Eloff, "An Information Security Governance Framework," Information Systems Management, Vol. 24, pp. 361-372, 2007.

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

[19] Kim, H. S., "A Study on the Quantification of Information Security Level," The Korea Society of Management information Systems, Vol. 9, No. 4, pp. 182-201, 1999.

[20] SOPHOS, "New platform and Changing threats," Security Threat Report, 2013.

[21] Von Solms, S. H., "Information Security-The fourth wave, Computers and Security," Vol. 25, pp. 165-168, 2006.

[22] Martins, A. and Eloff, J. H. P., "Information Security Culture, In Security in the information society," Boston : Kluwer Academic Publishers, IFIP/SEC, pp. 203-214, 2002.

저 자 소 개

Subrata Biswas (E-mail : subhongiku09@gmail.com)
2006년 상명대학교 경영학과 (학사)
2010년~현재 상명대학교 경영학과 (석사)
관심분야 경영정보, Big Data 분석, 정보보안관리체계, 경영정보보호

유진호 (E-mail : jhyoo@smu.ac.kr)
1992년 고려대 이과대학 수학과 졸업
1994년 고려대 일반대학원 통계학과 (석사)
2010년 고려대 정보경영공학전문대학원, 정보경영공학과 (박사)
현재 상명대학교 경영학과 교수
관심분야 정보보호, 인터넷윤리, MIS

정철용 (E-mail : cyjung@smu.ac.kr)
1982년 서울대학교 경제학과 졸업
1985년 Univ. of Washington MBA
1992년 Univ. of Texas at Austin MIS (박사)
현재 상명대학교 경영학과 교수
관심분야 금융IT 및 보안, 비즈니스 인텔리젼스