Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.6, Dec. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.6.1319

금융기관 문서 보안등급 분류에 관한 연구

강 부 일,[1†] 김 승 주[2‡]
[1]고려대학교 정보보호대학원, [2]고려대학교 사이버국방학과

Study on Security Grade Classification of Financial Company Documents

Bu il Kang,[1†] Seung joo Kim[2‡]
[1]Center for Information Security Technologies(CIST), Korea University
[2]Department of Cyber Defense/Center for Information Security Technologies(CIST), Korea University

요 약

최근 네트워크의 발달로 개인정보의 수집, 처리 등이 용이해진 반면 개인정보 유출로 인한 고객과 금융기관, 나아가 국가적 손실이 증대되고 있다. 따라서 금융기관의 개인정보 유출로 인한 정신적 피해나, 불법 유통된 개인정보를 활용한 금융거래로 인해 발생하는 추가적 피해와 관련된 방지 대책이 요구되고 있는 실정이다. 현재 금융기관에서는 중요문서(개인정보 포함)뿐만 아니라 공개문서의 열람방식에 있어서 직급이나 직위에 따른 접근통제방식을 수행하고 있다. 그리하여 기밀성을 요구하는 문서일지라도 동일 직급, 동일 직위이면 정당한 방법으로의 열람, 접근이 가능하다. 이를 개선하기 위한 방안으로 문서의 보안등급을 적용하고 보다 효과적인 접근통제를 통해 개인정보 유출 사고를 사전에 방지하고자 한다.

ABSTRACT

While the recent advance in network system has made it easier to collect and process personal information, the loss of customers, financial companies and even nations is getting bigger due to the leakage of personal information. Therefore, it is required to take a measure to prevent additional damage from the illegal use of leakaged personal information. Currently, financial companies use access control in accordance with job title or position on general documents as well as important documents including personal information. Therefore, even if a documents is confidential, it is possible for a person of the same job title or position to access the document properly. This paper propose setting up security grade of documents to improve current access control system. It will help preventing the leakage of personal information.

Keywords: personal Information, leakage of personal Information, Security grade classification of document

I. 서 론

1.1 연구배경 및 목적

오늘날 정보화 사회의 역기능이라고 볼 수 있는 보안 사고는 계속 증가하는 추세이며, 중요정보(개인정보 포함)의 유출로 인한 정신적 피해가 증가되고, 제도적 규제가 강화되는 등 기업의 윤리적·사회적 책임 이행이 요구되어 지고 있다. 금융기관들은 수집된 개인정보 유출 방지를 위한 여러 가지 노력을 기울이고 있다. 전자금융감독규정 제8조 제2항에 따르면 금융기관 IT보안 예산과 정보보호 인력 확대를 위해 2012년부터 IT보안 예산은 Table 1.과 같이 전체 IT예산

접수일(2014년 10월 16일), 수정일(2014년 11월 17일), 게재확정일(2014년 11월 19일)
† 주저자, mackbi@naver.com
‡ 교신저자, skim71@korea.ac.kr(Corresponding author)

Table 1. Current status of human resources and IT security budget of financial institutions in 2013.

(Unit : One million won, People)

Division (Bank)	Information Security budget	The security budget ratio	Security personnel it	Security staff ratio
Kookmin	33,719	10.75	55	5.01
Shinhan	29,202	10.08	37	4.96
Hana	17,824	11.59	25	5.24
Woori	21,385	7.45	48	6.06
Nonghyup	40,627	8.03	83	8.89
Korea exchange	20,040	9.77	24	5.88
Suhyup	5,521	9.00	11	5.26
Industrial	30,475	9.53	38	5.67
SC	7,100	7.52	18	5.59
Citi	13,455	14.17	29	7.53

대비 7% 이상 확보해야 하고 IT인력은 총 임직원 수의 5% 이상, 보안인력은 IT인력의 5% 이상 확보 하도록 하였다[1].

그러나 개인정보 유출사고는 현재까지도 진행 중에 있고, 금융기관은 중요정보의 불법유출로 인하여 심각한 손실을 경험하고 있다. 중요하고 민감한 보호 대상인 금융기관의 문서정보에 대한 자료 분류체계가 되어 있지 않아 어떤 문서가 중요문서이고, 어떤 문서를 보호해야 할지 알 수 없어 금융 보안사고가 계속해서 반복적으로 발생하고 있다. 본 연구는 이런 중요문서에 대해 보안등급을 적용함으로써 내부사용자의 불필요한 정보에 대한 접근을 제한하는 것에 목적을 두고 있다. 더구나 금융기관이 보유한 개인정보는 특정인의 생활과 관련된 여러 정보들 가운데 가장 중요하고도 내밀한 정보이기 때문에 고도의 보호수준이 요구됨은 물론 그 관리에 있어서도 매우 엄격한 제한이 필요하다는 본연적 특성을 가지고 있다[2].

따라서 중요문서에 대한 효율적이고 체계적인 분류체계가 필요하고, 그것으로 인해 내부사용자에 의한 정보유출 사고로 부터 불확실성과 위험을 감소시킬 수 있을 것이다.

1.2 연구방법 및 구성

본 연구에서는 개인정보 등을 포함한 중요한 문서들을 보안등급으로 분류하여 보호할 자산에 대해 명확한 기준을 제시함으로써 효율적인 접근제한이 될 수 있도록 제안 하고자 한다. 본 논문의 Ⅱ장에서는 개인정보 유출사고 사례 및 정보 분류체계에 대해서 Ⅲ장에서는 현재 금융기관의 문서 정보 분류와 문제점에 대해 살펴보고, Ⅳ장에서는 연구대상인 문서의 보안등급 분류, 연구가설을 설정하였으며 Ⅴ장에서는 각 요인 변수들 간의 인과관계 분석을 통해 가설을 검증하였고 마지막으로 Ⅵ장에서는 본 논문의 결론으로 끝을 맺는다.

Ⅱ. 관련연구

2.1 개인정보 의의

"개인정보"란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.('개인정보보호법 제2조')

2.2 개인정보 유출 사례

최근 몇 년간 우리는 크고 작은 개인정보 유출사고를 경험했다. 이미 전 국민의 개인정보가 한번 씩은 유출 당했다고 해도 과언이 아닐 것이다. 올 초에는 신용카드 3개회사에서 1억 4백만 개인정보가 유출되는 초대형 사고가 발생해 다시 한 번 개인정보 보호의 필요성이 대두되기도 했다. Table 2.에 따르면, 지난 3년간 연이은 대형침해사고 발생으로 인한 개인정보 침해건수가 1억 4,300만여 건에 이른다[4]. 최근 들어서는 페이스북, 트위터 등 이른바 소셜네트워크서비스(SNS)를 통한 개인정보 침해도 눈에 띄게 늘고 있다. 개인정보 침해문제는 단순한 정보주체인 개인의 문제로 국한되는 것이 아니다. 개인과 기업, 정부의 각 주체가 포함되어 전 사회적인 위험이 될 수 있다. 각 주체가 개별적으로 개인정보 침해에 대한 위험관리를 해야 하며, 전 사회적 차원의 위험관리 방안이 모색되어야 할 것이다[3].

2.3 미국의 정보 분류 체계

국내 뿐 아니라 국외에서도 정보는 국가 및 기업 운영에 있어서 중요한 자산일 뿐만 아니라 기

Table 2. Finance company from which the customer information flow

Period	company	Number of leaks	Leakage path
2011.03~05	Hanwha general insurance	More than 150,000	External hacking
2011.04	Hyundai capital services	More than 1,750,000	External hacking
2011.07	Hanaskcard	More than 90,000	Internal employee
2010.01~ 2011.08	Samsungcard	More than 800,000	Internal employee
2011.12~20 12.02	Standard Chartered Bank Korea	More than 103,000	Internal employee
2011.12~20 12.03	IBKcapital	More than 5,800	Internal employee
2013.02~05	Meritzfire	More than 160,000	Internal employee
2013.04	Citibank Korea	More than 34,000	Internal employee
2012.10~20 13.12	KBcard, Lottecard, Nonghyupcard	More than 140,000,000	Externalemployee

업의 존폐를 결정짓는 요인이 되고 있다.

연방정보보안관리법(Federal Information Security Management Act, FISMA)에서는 정부기관이 다루고 있는 정보를 분류하고 그 정보가 유출 되었을 때 그 기관의 영향 정도를 평가하도록 하고 있다. NIST는 이런 FISMA 의 요구사항을 충족시킬 수 있는 가이드라인을 제공하는 책임을 맡고 있다. NIST는 각 급기관의 FISMA 구현을 위해 해당 표준과 지침을 전체적으로 통합하고 설명하기 위해 위험관리체계(RMF, Risk Management Framework)를 개발하고 그 위험을 관리하기 위한 활동으로 위험이 기밀성, 무결성, 가용성 관점에서 정보와 시스템에 잠재적으로 미치는 영향도에 기반을 두어 분류(Categorize), 최소보안요구사항, 비용분석 등의 요소에 기반 하여 최소 보안통제 선택(Select), 보안환경에 맞게 실제 구현(Implement), 운영 등이 원하는 결과를 도출하였는지 평가(Access), 조직운영 및 자산 등 위험을 판단하고 받아들일 수 있는지 결정(Authorize), 보안 상황 모니터링(Monitor)의 6단계로 Security Life Cycle로 분류하고 있다. FIPS PUB 199(Federal Information Processing Standards Publication 199)에서는 보안을 표현하기 위한 공통 Framework와 이해를 제공하기 위해 정보 및 정보시스템에 대한 보안 분류 기준(조직의 잠재적 영향을 기초로)을 정의하였고 기밀성, 무결성, 가용성을 보안목적으로 구분하고, 보안목적에 대한 보안침해 발생 시 개인이나 조직에서 발생되는 잠재적인 영향 도를 Table 3.과 같이 Low, Moderate, High 세단계로 정의하고 있다[5].

III. 금융기관 문서분류 체계 및 문제점

3.1 문서 분류 영향도 및 보안등급 구분

한국데이터베이스진흥원의 데이터 보안 인증 가이드에 따르면 DB정보에 대한 분류는 DB 보안정책을 수립하는데 있어서 가장 핵심이 되는 사안으로 정의하고 있다. 이 가이드를 토대로 보안 정책 수립이나 위험 평가에서 보안 대상 데이터를 분류하는 기준은 다음과 같이 보호 대상 자산(데이터)별로 총 영향 도를 산정하여 사용한다.

$$impact_a = \sum_{i=1}^{n} impact_i$$

$impact_a$: 자산a에 대한 영향도의 총합(3 ~ 9)
i: 영향받는 영역(1 ~ 3, 기밀성, 무결성, 가용성)

Fig. 1. The total effect is calculated

등급 구분을 위한 구체적인 방안은 Table 4.와 같이 3점 분류 방식을 적용하여 각 영역별 영향도 점수를 결정한 후, 이를 합산하여 총 영향도 점수를 산정하고, 산출된 총 영향도 점수에 따라 분류 등급을 결정한다. 기밀성, 무결성, 가용성 등의 영역별로 영향 수준을 평가하고 이를 반영하여 총 영향 도를 계산하면 3~9의 스코어를 얻게 되며, 이 스코어 수준에 따라 Table 5.의 사용사례 산식과 같이 영향 도에 따른 등급 분류를 산정하면 1~5등급의 분류등급을 얻을 수 있다. Table 5.은 이렇게 얻은 정보 분류를 정의한 것이다[6].

※ 적용예시
기밀성 영향 수준이 "M"이고, 무결성 영향 수준이 "H"이며, 가용성 여향 수준이 "M"인 데이터의 경우 분류 등급은 다음과 같다.
총 스코어 = [(기밀성,2) +(무결성, 3)+(가용성, 2)]
등급분류 = 7 - round(총 스코어/1.5, 0)
= 2 보안등급

Table 3. Categorization of Federal Information and Information Systems

SECURITY OBJECTIVE	Potential Impact		
	Low	Moderate	High
Confidentiality	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modi-fication or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Table 4. Impact evaluation criteria.

Division	Low	Moderate	High
Confidentiality	1	2	3
Integrity	1	2	3
Availability	1	2	3

Table 5. Definition of the grade of information classification.

The total influence score	Security (risk) grade		Description
9	1	High Confidential	As top grade, Level allowed only very limited small number
7~8	2	Confidential	As senior grade, Level allowed only personnel with limited access to services such as security managers
6	3	High Restricted	Departments and the top administrator, Security department only allowed access
4~5	4	Restricted	Internal staff and allow access only to a group of employees that the company does not apply to special restrictions in the corporate
3	5	Public	No matter the External open

3.2 현재 금융기관 문서분류 체계 및 문제점

금융기관의 문서 분류 체계를 알아보기 위해 국내 A은행에서 현재 사용하고 있는 문서 분류 방법을 '피해예상 경중'에 따라 Table 6.과 같이 분류 하였다. 문서분류를 '피해예상경중'에 따라 분류하므로 고객 개인정보 유출 등 보안 사고에 노출되어 있다. 왜냐하면 Table 6.과 같은 분류방식은 개인정보에 대한 분류가 되지 않아 개인정보 유출 등 보안 사고에 취약하다고 볼 수 있다. 2013.12 발생한 카드사 개인정보 유출과정을 보면 외부직원에게 개인정보 접근을 허용하였고, 은행 영업점에서 고객이 작성한 개인정보가 포함된 신청서를 관리 소홀로 인하여 고객민원을 발생시켰다. 이와 같이 개인정보에 대한 체계적인 보안 분류체계가 없다보니 문서보안에 대한 관리 및 통제가 없고 그것으로 인해 개인정보 유출사고로 이어졌다고 볼 수 있다. 또한 금융기관 정보자산인 문서에 대해 보호하여야할 대상을 구분하지 못해 정보보호를 차등 할 수 없어 안전하게 보호·운영 되어야 하는 개인 정보 등을 유출이나 남용으로 부터 방지하기 위한 일련의 행동을 할 수 없어 정보보안의 목표인 기밀성,무결성 등을 유지하기에 어려움이 있다.

Table 6. Classified according to the severity of the expected damage

Division	Classification standard
Top-secret documents	- External leakage, the company document that can bedeadly and had tremendous damage - Documents that could have a significant impact on the strategy and management of the bank - Document data that has been registered for reporting management council, Financial Strategy Council (ALCO), Risk Management Committee, of expanding executive meeting, Board of Directors, Crisis Management Committee, the system is included
Confidential document	- Except for a top secret grade, When an external leakaged, The documents damages to the company, employee, and individuals. - Document contain information of value that deserves to affect the bank's ROE - Legal remedy from the external companies and organizations, The document is exposed to the civil or criminal, accuse, charge of threat. - The document contain information about unreleased new goods and business development of the bank - Document information related to the introduction of IT resources / new technology is included
General	The documents are not included in the above document

3.3 문서 보안등급 분류의 필요성

금융기관들은 복잡하고 다양한 상품을 판매하면서 여러 개인정보를 수집하고 있지만, 정작 수집된 개인정보를 포함하는 중요문서에 대한 관리 및 보호 수준은 비교적 체계적이지 않다. 만약 중요문서에 대한 등급 분류가 명확하게 구분되지 않는다면 다음과 같은 위험들이 존재할 수 있다.

첫째. 보호할 자산에 대한 불명확성이다. 현재 많은 보안인력과 예산을 집행하고 있지만 내부보안 사고는 계속 발생하고 있다. 이런 원인은 보호할 자산에 대한 리스트가 충분하지 않기 때문이다. 둘째. 업무의 비효율성이다. 현재 개인정보가 포함하지 않은 상품안내장 및 단순제안서조차도 보안문서로 잠겨 있어 불필요한 반출승인 절차를 따르고 있어 영업력을 반감 시키고 있다. 마지막으로 정보보호를 위한 비용이 증가한다. 명확한 분류기준이 없는 상태에서 적당한 기준에 따라 정보를 분류한다면 불필요한 정보에 과도한 보안조치로 인한 비용을 증가시킬 수 있다.

IV. 제안하는 문서의 보안등급 분류

4.1 주요 금융기관 문서 분류

문서에 대한 보안등급을 분류하기 위하여 주요 3개 은행의 영업점 및 본부부서에서 사용하고 있는 문서를 조사하여 각 문서에 포함하고 있는 항목을 Table 7.과 같이 분류 하였다. 문서 분류 기준은 각 은행마다 분류기준이 비슷하여 공통된 카테고리(Category)로 묶었다. 개인정보보호법 개정(공포 2013.8.6.)에 의하면 2014.8.7일부터 법령상 근거 없이 불필요하게 주민번호를 수집하는 행위가 엄격히 제한됨에 따라 앞으로 주민번호를 문서에 작성하는 일은 없을 것 같아 문서 분류에 주민등록번호를 제외시켰다.

4.2 제안하는 금융권 문서분류체계

문서분류는 보안등급 정책을 수립하는데 있어서 가장 핵심이 되는 사안으로 금융기관에서 수집된 정보에 따라 보안등급별로 분류하여 보호하여야 할 자산과 그렇지 않을 자산을 나눠 민감한 정보유출로 인하여 발생 할 수 있는 위험을 최소화하는 것을 목표로 하여 등급을 분류 하였다. Table 7.과 같이 문서의 보안등급 분류기준을 상세히 설명하면 ①업무담당자 의견의 분류기준은 Table 3.에서 제시된 미 연방정보 보안관리법의 정보 및 정보시스템분류에 의해 각 규정별 업무담당자가 기밀성, 무결성, 가용성별로 등급을 분류하였고, ②스코어는 기밀성, 무결성, 가용성의 등급을 Table 4.에서 제시된 한국데이터베이스 진흥원의 분류 점수에 의해 산출하였고, ③위험등급은 스코어 점수를 기초로 Table 5.에서 제시된 한국데이터베이스 진흥원의 위험등급에 의해 분류하였다. 문서의 작성된 항목 및 내용에 대해 정보시스템분류를 살펴보면 기밀성은 특성상 아주 민감해서 주의 깊은 통제와 보호를 요구하는 항목인지를 판단하였다. 예시로 개인식별정보, 직원정보, 은행의 경영이나 전략이 노출되었을 때 은행에 중대한 영향을 미칠 수 있는 정보인지

Table 7. Risk assessment and classification of security evaluation of financial institutions document.

Type of documents	Work	①Charge of the business opinions			②Score	③Risk rating	Document content
		C	I	A			
Regulation	Loans	L	M	L	4	4	Documents about the manipulation of the task such as Real-name financial transactions and bank, banking regulation and taxation provisions of law provision, Act ensure confidentiality, the rules regarding the housing supply, trade law, business and other areas of the Framework Act on Electronic Commerce.
	Receive	L	M	L	4	4	
	Foreign exchange	L	M	L	4	4	
	Fund /Trust	L	M	L	4	4	
	Investment / Bancassurance	L	M	L	4	4	
	Retirement annuity	L	M	L	4	4	
	Risk	L	M	L	4	4	
	The articles of association	L	M	L	4	4	
	The Board of Directors	L	M	L	4	4	
Guidelines	Loans	L	M	L	4	4	Working rules such as each business process of operations and selling goods such as accounting standard for coaching methods or a person to guide you right directions.
	Receive	L	M	L	4	4	
	Foreign exchange	L	M	L	4	4	
	Fund /Trust	L	M	L	4	4	
	Investment / Bancassurance	L	M	L	4	4	
	Retirement annuity	L	M	L	4	4	
	Privacy protection	L	L	L	3	5	
	Risk	L	L	L	3	5	
	Electronic financial management	L	L	L	3	5	
Terms/ Goods Guide	Loans goods	L	L	L	3	5	Goods manuals to help understand about the product, such as users and reference.
	Receive goods	L	L	L	3	5	
	Foreign exchange goods	L	L	L	3	5	
	Fund/Trust goods	L	L	L	3	5	
	Investment / Insurance goods	L	L	L	3	5	
	Retirement annuity	L	L	L	3	5	
Work manual	Loans goods	H	M	L	6	3	Method of processing business and the use of each work-specific
	Receive goods	H	M	L	6	3	
	Foreign exchange goods	H	M	L	6	3	
	Fund/Trust goods	H	M	L	6	3	
	Retirement annuity	H	M	L	6	3	
	Investment / Bancassurance goods	H	M	L	6	3	
	Retirement annuity	H	M	L	6	3	
	IT operations	H	M	L	6	3	M/F, Server etc, each device setup and management tasks required to Treatment Methods

Type of documents	Work	①Charge of the business opinions			②Score	③Risk rating	Document content
		C	I	A			
Statement / Formatting	Loans	H	H	L	7	2	Name , home address , home phone number , mobile phone , E - receiving mail, work address , work phone number, office Fax, workplace /department name, about SMS, whether the prohibition of telephone, postal Suryoncho , passport English ,nationality, passport number, payment account number, wedding anniversary, type of occupation , annual income , signed
	Receive	H	H	L	7	2	
	Foreign exchange	H	H	L	7	2	
	Fund/Trust	H	H	L	7	2	
	Investment / Bancassurance	H	H	L	7	2	
	Retirement annuity	H	H	L	7	2	
	The consent of personal information collection	L	L	L	3	5	Name , signature
Report /Guidance	Loans goods	L	L	L	3	5	Reference materials to help each task an understanding of the goods, and important contents of the terms
	Receive goods	L	L	L	3	5	
	Report all sorts of goods	L	L	L	3	5	
Sample form of foreign exchange	Foreign currency sample form	L	L	L	3	5	A description of the World countries currency that helpful to identify a counterfeit coin on to the naked eye
	Foreign currency counterfeiting	L	L	L	3	5	
Proposal	Proposal by industry.	L	L	L	3	5	Proposal forms for wholesale, retail industries such as transportation, electronics, each for, oil prices, interest and foreign exchange derivatives
	Derivatives proposals	L	L	L	3	5	
Drafting paper	Action copy, Original proposal, Cooperation statement(general)	H	M	L	6	3	Customer information, information, not the general business strategy document
	Ministry of strategy and planning, financial planning, the secretariat document (and other management strategies)	H	H	H	9	1	Documents which significant impact on bank's management and strategy.
Business Report	Management consulting, management accounting report for the (official)	H	H	H	9	1	Reporting the Management council, financial strategy committees and board meeting.

판단하였다. 무결성에 대해서는 데이터의 완전성, 일관성, 정확성, 유일성, 유효성 등 데이터의 품질 기준으로 판단했으며, 예시로 공시되지 않은 재무상태, 회계보고서, 위·변조 등의 영향을 받는 항목인지를 고려하였다. 마지막으로 가용성은 응답시간의 지연, 접근불능, 데이터 손실, 파괴, 도난 등의 발생에 대한 의사결정불능, 업무처리 불가 등을 기준으로 삼았다. 예시로는 은행의 경영이나 전략에 중대한 영향을 미치는 문서가 손실, 도난 등으로 인하여 의사 결정 및 업무처리가 불가 될 수 있는 내용인지를 기준으로 삼았다.

V. 제안하는 문서분류체계의 타당성 분석

5.1 연구방법

연구 자료의 수집을 위해 설문 대상자는 3개 금융기관 정규 직원 중 개인정보를 취급 하는 업무담당자에 한해서 전체 150명(A은행: 90, B은행: 30, C은행: 30)을 대상으로 조사를 실시하여 설문결과를 작성하였다. 조사기간은 2014년08월 18일부터 8월22일까지 5일 동안 수행 되었으며 직접방문 하는 방법으로 근무처, 직위, 직무, 경력 등이 한쪽으로 치우치지 않도록 사전에 조정 후 조사를 실시하였다. 본 연구에서는 IBM SPSS Statistics 18 통계 분석 프로그램을 사용하여 가설의 실증분석을 하였다.

5.2 연구가설 및 요인설정

중요(개인정보 포함)정보 유출에 영향을 미치는 요인들은 여러 가지 요인들이 상호 연관되어 다양하게 나타난다. 본 연구에서는 문서의 보안등급이 직관적으로 위험을 인지하고 중요정보 유출방지에 어떠한 영향을 미치는지 알아 볼 것이다. 또한 '피해예상경중'에 따라 분류되어 있는 현재 문서분류체계와도 영향이 미치는지도 연구할 것이다. 따라서 문서 보안등급분류에 대해 결정짓는 요인들의 차이와 영향이 미치는 정도를 살펴보기 위한 연구가설은 다음과 같다.

H1: 문서의 보안등급분류는 중요정보 유출방지와 정(+)의 영향을 미칠 것이다.

보호자산인 문서를 차등적으로 보호하게끔 하여 보다 명확한 유출방지와 보안예산 비용을 절감 시킬 것으로 기대된다.

H2: 문서의 보안등급분류는 '피해예상경중'에 따라 분류되는 현 문서분류체계와 부(-)의 영향을 미칠 것이다.

현 문서분류체계에서 미처 반영하지 못한 개인정보영역에 대한 불가피한 보완이 필요 할 것이다.

H3: 문서의 보안등급분류는 보안정책에 정(+)의 영향을 미칠 것이다.

제안한 보안등급분류로 현재 시행되고 있는 보안정책과 상호 보완적 관계가 될 것으로 기대된다.

5.3 신뢰도와 타당성 분석

연구 가설에 포함되어 있는 변수의 측정항목들의 신뢰성(reliability)과 구성타당성(construct validity)을 탐색적 요인분석(exploratory factor analysis)으로 평가하였다. 내적일관성은 크롬바흐 알파계수(Cronbach`s α)를 사용하여 분석하였다. 크롬바흐 알파계수가 0.7 이상이면 각 변수의 측정이 내적일관성이 있다고 판단된다. Table 8.에서는 연구 변수들에 대한 측정 항목들의 요인 적재값, 고유값(Eigen value), 크론바흐 알파 값을 보여준다. 모든 측정변수는 구성요인을 추출하기 위해서 주성분분석(principle component analysis)을 사용하였으며, 요인적재치의 단순화를 위하여 배리맥스(varimax) 방법에 따른 직교회전 방식을 채택하였다. 그 결과 Table 8.에서와 같이 4개의 요인으로 구분되었다. 측정 항목들의 요인 적재 값은 대부분 0.4 이상으로 측정 항목들의 집중타당성이 있는 것으로 나타났다. 신뢰도 분석의 결과는 Table 8.에서 알 수 있듯이 모든 연구변수의 크롬바흐 알파계수가 0.7 이상으로 각 측정항목은 신뢰성이 있다고 볼 수 있다.

5.4 결과분석

어떤 한 요인들이 연구가설에 영향을 미치는지, 그리고 가설검증을 하기 위해서 다중 회귀분석(Multiple Regression Analysis)을 시행하였다.

문서의 보안등급 분류로 인한 보안정책의 변화가 있는지 알아보기 위해 유출방지, 현재 문서분류체계, 보안정책을 독립변수로 입력하여 종속변수인 문서 보안등급에 대한 회귀 분석을 실시하였다. Table 9.의 다중 회귀분석 결과를 살펴보면, 중요정보 유출방지와 보안정책에 대해 정(+)의 영향이 미쳤음을 알 수 있

Table 8. Exploratory factor analysis

Number	Factors				Cronbach's α
	1	2	3	4	
Q13	**.875**	.091	.136	.100	0.834
Q14	**.864**	.152	.073	.164	
Q16	**.850**	.087	.018	.238	
Q15	**.815**	.149	.004	.259	
Q9	.151	**.815**	.156	.080	0.73
Q11	.145	**.809**	.206	.147	
Q10	.089	**.770**	.341	-.040	
Q12	.105	**.755**	.322	-.025	
Q3	-.012	.217	**.829**	-.046	0.866
Q4	.147	.276	**.733**	.155	
Q1	.102	.324	**.722**	.008	
Q2	.025	.346	**.681**	.048	
Q6	.203	.140	-.060	**.810**	0.903
Q7	.242	-.066	.169	**.762**	
Q5	.248	.126	-.015	**.760**	
Q8	.000	-.116	.470	**.475**	
Eigenvalue	5.453	3.044	1.530	1.105	
Propriety standard formation of Kaiser-Meyer-Olkin measure					0.768
The Spherical Test of Bartlett			Approximate square contingency.		1393.922
			Freedom		120

다(가설 1, 3 채택). 반면, 현재 문서분류에 대해서는 유의수준 0.564로 귀무가설이 지지가 된다(가설 2 기각). 그러므로 문서의 보안등급 분류체계와 '피해예상경중'에 따른 분류체계는 상당히 관련이 있다고 할 수 있다.

VI. 결 론

6.1 결론

본 연구는 문서의 보안등급 분류이다. 위 내용을 요약해보면 문서의 보안등급 1등급인 경우는 은행의 경영이나 전략에 중대한 영향을 미칠 수 있는 문서, 2등급은 개인식별정보가 포함한 문서, 3등급은 각 업무별 사용방법 및 업무처리방법에 관한 문서, 4등급은 은행의 규정, 지침 등 법률에 관한 문서, 5등급은 약관, 상품설명서, 안내장, 보고서, 일반기안문 등으로 분류했다. 금융기관의 중요정보 유출이 중요한 문제가 되고 있고 이에 따른 관리 방안이 여러 방면으로 연구되고 있다. 특히 금융기관의 고객 개인정보가 유출되어 피해사례가 끊임없이 반복 이어지고 있다. 앞으로는 금융기관 CEO 등에 해임 등 징계권고 사유가 될 만큼 사안이 중요하고 시급하다. 본 연구에서는 금융기관 문서의 보안등급을 반영하여 중요정보 유출을 방지시킬 수 있는 방안을 연구하였다. 연구 결과 문서의 보안등급 분류는 중요정보 유출방지와 보안정책에 정(+)의 영향을 미치는 것으로 나타났다. 또한 '피해예상경중'에 따른 분류체계도 제안한 문서의 보안등급 분류체계와 연관성을 가지는 것으로 나타났다.

본 연구에서는 금융기관 문서의 보안등급을 분류하였고 통계학적으로 증명 하였지만 향후, K-ISMS, ISO27001 등 일반적이고 다양한 위험평가 방법으로 선행 연구한 논문을 기반으로 금융기관 문서 특성을

Table 9. Results of Regression Analyses for Hypotheses Testing

Model		The counter with nonstandardized		Coefficient of standardization	t-value	Instructiveprobability	Durbin-Watson	R Square
		B	Standard error	Beta				
Subordination variable : Grade Classification of Documents	-	.950	.356		2.670	.008	2.194	.389
	Leakage Prevention	.604	.071	.564	8.453	.000		
	measure of damage	-.052	.080	-.047	-.645	.520		
	Security policy	.223	.077	.212	2.908	.004		

R = .624, modified R^2=.377 F=31.018, $p < 0.05$ attention.

반영한다면 보다 명확한 보안등급 분류기준을 제시 할 수 있을 것이다.

References

〔1〕 The Financial News Daily available at, "http://www.kbanker.co.kr/news/articleView.html?idxno=41062",〔Accessed: February 8, 2014〕

〔2〕 Gil-Yong Oh, Due to the leakage personal information, emergency debate, January 27, 2014

〔3〕 The Security News Daily, available at, "http://www.boannews.com/media/view.asp?idx=32178&kind=1",〔Accessed: July 19, 2012〕

〔4〕 The Korea Economic Daily, available at,"http://www.hankyung.com/news/app/newsview.php?aid=2014010820061",〔Accessed:January 8, 2014〕

〔5〕 NIST, Guide for Mapping Types of Information and Information Systems to Security Categories, "http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf", p20

〔6〕 DQC, available at, "http://www.dqc.or.kr/guideline/6-2-3.html"

〈저자소개〉

강 부 일 (Bu-il Kang) 정회원
1997년 2월: 전주대학교 수학과 학사
1997년 1월~2001년 2월: KB국민카드
2001년 3월~현재: KB국민은행 전산정보 본부
2013년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 금융정보보안, 유가증권 자산평가
E-mail: mackbi@naver.com

김 승 주 (Seungjoo Kim) 종신회원
1994년~1999년: 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년 12월~2004년 2월: KISA(舊한국정보보호진흥원) 팀장
2002년~현재: 한국정보통신기술협회(TTA) IT 국제표준화전문가
2004년 3월~2011년 2월: 성균관대학교 정보통신공학부 조교수, 부교수
2011년 3월~현재: 고려대학교 사이버국방학과/정보보호대학원 정교수
2004년~현재: 한국정보보호학회 이사
2005년~2006년: 교육인적자원부 유해정보 차단 자문위원
2007년: 국가정보원장 국가사이버안전업무 유공자 표창
2007년~2009년: 전자 정부 서비스 보안 위원회 사이버 침해사고대응 실무위원회 위원
2010년: 방송통신위원회 정보통신망 침해사고 민관합동조사단 위원
2012년 3월~2012년 6월: 선관위 디도스 특별검사팀 자문위원
2013년 4월~2013년 12월: IT보안인증사무국 자문위원
2013년 9월~현재: 중앙선거관리위원회 자문위원
2014년 3월~현재: 헌법재판소 자문위원
〈관심분야〉 보안공학,암호이론,정보보증,정보보호제품 보안성 평가, IoT보안, HCISecurity, Cyber-Physical Security
E-mail: skim71@korea.ac.kr