The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 14, No. 6, pp.273-279, Dec. 31, 2014. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2014.14.6.273
JIIBC 2014-6-39

기업 보안평가 공시제도의 필요성 및 구현방안 (금융회사 중심으로)

Needs and considerrations of corporate security assessment (Focusing on financial companies)

김보*, 임종인**

Bo Kim*, Jong-In Lim**

요 약 최근 신용카드사가 보관중인 고객의 개인 및 신용 정보가 약 1억4천만 건 유출되는 국내 최대 규모의 정보유출 사고가 발생했다. 이렇게 금융회사의 개인정보 유출사고는 증가하고, 소비자의 개인정보에 대한 민원이 급속히 증가하고 있지만 아직도 뚜렷한 예방책이 없는 것이 현실이다. 따라서 금융소비자 입장에서 기업의 보안 우수성 여부를 사전에 확인 및 판단할 수 있고, 기업은 우수한 보안성을 갖추기 위해 실질적인 노력을 할 수 있는 제도적 장치가 필요한 시점이다. 본 연구는 이러한 제도적 장치를 “기업 보안평가 공시제도”라는 모델로 보고 이 제도가 왜 필요한가에 대하여 현실적이고, 객관적 입장에서 연구하고자 한다.

Abstract Recently, it was occurred in the nation's largest Information spill about 140 million cases of credit card customers' personal and credit information. As such, it was rapidly to increase in consumer complaints about the privacy of personal information in accordance with outflow of financial companies increased accident. But it is still not clear precaution. Therefore, in financial customer position, it is possible to confirm and determine in advance whether or not superior to the security company. In addition, It is time to be required institutional device that can be a real effort to equip a good security company. This report is considered a model of "Disclosure of corporate security assessment " of these devices institutional study. And We study in realistic and objective stance about why do we need this policy.

Key Words : Corporate security assessment, Security rating, Disclosure, Financial company

Ⅰ. 서 론

국내 최대 규모의 정보유출 사고가 올해 초 신용카드사에서 발생했다. 약 1억 4천만 건이면 대다수 국민들 모두의 개인정보가 유출되었다고 해도 과언이 아니다. 특히 이번 사고는 이전에 발생한 단순 개인정보 외에 신용정보라는 민감한 정보도 노출이 되어 사회적 파장을 일으켰다. 금융회사는 기본적으로 소비자와 뱅킹, 투자, 보험상품 등 금융거래를 바탕으로 하고 있다. 그러나 이번 사고로 각 금융회사들은 영업정지, 대표자 사퇴 등 영업에 큰 타격을 받은 상태이다. 그렇다면 각 금융회사들이 소비자의 개인정보 보호에 최선을 다하지 않은 것일까. 물론 수준의 차이는 있을 수 있지만 대다수의 금융회사는 상대적으로 타 업종에 비해 높은 보안 수준을 유지하

*정회원, 고려대학교 정보보호학과
**정회원, 고려대학교 정보보호학과 (교신저자)
접수일자: 2014년 11월 7일, 수정일자: 2014년 12월 7일
게재확정일자: 2014년 12월 12일

Received: 7 November, 2014 / Revised: 7 December, 2014
Accepted: 12 December, 2014
**Corresponding Author: jilim@korea.ac.kr
Dept. of Cyber Defense, Korea University, Korea

고 있다. 이것은 업무관련 별도의 감독기관(금감원 등)이 존재하여 보안 관련 감사를 정기적으로 수행하고 있으며, 금융업 자체가 신용을 바탕으로 하는 사업이기에 지속적인 보안강화 활동을 하고 있기 때문이다.

개인정보보호위원회에 따르면 지난 2013년의 개인정보관련 침해 및 상담건수가 17만 7736건으로 지난 2004년 대비 10배나 증가했다고 밝혔다. 특히 이번 신용카드사 사고와 같이 대규모 정보유출 사고가 발생한 시기를 기점으로 크게 높아지는 것으로 나타났다.

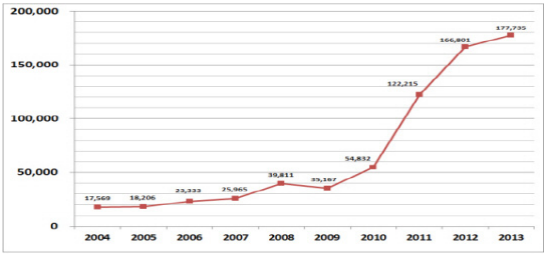

그림 1. 연도별 개인정보 침해 및 상담건수
Fig. 1. Annual Status of Privacy Complaint Counseling[1]

이렇게 소비자들의 개인정보에 대한 관심과 불안감은 높아지고 있지만 정작 본인의 개인정보가 안전하게 보관되고 있는지 여부는 사고가 발생한 후에 인지하고 있는 것이 현실이다.

본 연구는 기존의 개인정보 보안활동이 기업 내부 차원에서 알아서 하는 구조였다면, 이제는 개인정보의 주체인 소비자 관점에서 정보보호를 바라 볼 수 있게 해야 한다는 것이 주된 방향성이다. 이것은 소비자가 기업을 선택하고자 할 때 본래의 목적(투자효과,상품성 등)외에 기본적으로 해당 기업이 정보보호가 잘되어 있는지 유/무를 판단할 수 있고, 선택 후 거래 시에도 개인정보가 안전하게 운용관리 되는지 확인 할 수 있도록 하자는 것이다. 이렇게 되면 소비자측면에서 기존 사고 발생 후에 보안 Risk 인지하는 구조에서 벗어나 사전에 인지하여 기업과의 거래여부를 판단할 수 있으며, 이는 기업의 입장에서 고객 확보를 위해 실질적인 정보보호 활동을 강화할 수밖에 없을 것이기 때문이다. 이것이 바로 이번 연구의 핵심인 "기업 보안평가 공시제도" 도입에 대한 필요성을 현실적이고 객관적인 입장에서 분석해 보고자 하는 것이다.

본 논문의 범위는 금융회사를 대상으로 하며, 구성 및 분석 방법은 관련 선행학습 및 이론을 학습하여 시사점을 정리하고, 현재 금융회사의 보안공시 관련 실태조사를 통한 문제점을 점검하고, "기업 보안평가 공시제도" 도입에 대한 설문조사를 통해 소비자적 관점의 의견을 조사, 분석하여 개선방안을 찾을 수 있도록 할 것이다. 또한 결론과 더불어 이번 연구의 한계와 향후 연구과제에 대해서도 언급하겠다.

II. 관련이론 및 선행학습

1. 공시제도 및 현황

공시(Disclosure)는 사업내용이나 재무상황, 업무실적 등 기업의 내용을 투자자 등 이해관계자에게 해당 기업에 대한 권리행사나 투자판단에 필요한 정보를 의무적으로 제공하는 제도이다. 공시제도는 1985년 정부가 기업의 투명성 제고와 투자라 보호를 위해 시작한 것이 시초로 다양한 분야의 공시제도가 이후 신설되고 있다.

표 1. 공시제도 현황
Table 1. General Disclosure Status

구분	내용	도입효과	문제점
기업 공시	기업 이해관계자에게 회사관련 제공	기업경영 투명성 확보, 투자자 보호 등	허위공시에 따른 피해가능성 등
환경 정보 공시	온실가스 배출량 등 환경보호 관련 정보 제공	지구 온난화방지 등 환경 보호 향상	
교육 정보 공시	교육기관의 직원수, 취업률 등 정보 공개	교육기관의 질적.양적성장 가능	허위공시 및 교육서열화 등

상기 <Table 1>에서 보는 바와 같이 공시제도는 시행이후 다양한 측면에서 효과성을 나타내고 있다. 다만, 제도 운영상이나 기업 경쟁에 따른 일부 부작용도 발생하는 경우도 있다. "교육정보 공시제도의 경우 도입 이후 학부모(약504명)들을 대상으로 한 세베이를 한 결과 공교육 신뢰도가 상당히 향상 되었다" 라는 연구결과가 나왔다[2].

2. 보안관련 공시제도 및 현황

보안관련 공시제도는 개인정보보호법이나 정보통신망법에 의거 금융회사가 제3자에게 제공한 정보(목적, 항목, 대상 업체 등)를 홈페이지를 통해 게시하는 수준이다.

공시 제도	대상 기관	공시매체 및 방법	공지내용	관련근거
개인 정보 보호 정책 공시	개인 정보를 수집 이용하는 모든 기관	○ 문서 : . 사업장 등에 게시 .관보, 일간신문, 간행물, 소식지 등을 통해 게시 . 계약서 등을 통해 발급	○개인정보 수집. 이용 목적, 수집 이용 항목, 안전성 조치, 개인정보보호 책임자 등 필수 공지사항	○ 개인 정보 보호법 ○ 정보 통신망 이용촉진 및 정보보호에 관한 법률
		○ 전자 : . 기관별 홈페이지 (홈페이지 우선)	○열람 청구 접수. 처리 부서 등에 선택공시 사항	

그림 2. 개인정보정책 공시현황
Fig. 2. Privacy Policy Disclosure Status

우리나라 최초 개인정보 관련 공시는 1994년1월 제정된 "공공기관 개인정보보호에 관한 법률"에 따라 1995년 총무처가 관보를 통해 게시한 건이 처음이다[3].

3. 보안평가 방식 및 현황(국내/외)

(국내) 보안평가 방식이 도입된 지는 오래되지 않았다. 1990년대 초 인터넷이 도입된 이후 공공기관 등 정부부처에서 필요성이 제기되었고, 인터넷 뱅킹이 시작되면서 금융권에서 보안평가에 대한 요구가 크게 늘어났다. 현재 평가방식은 크게 정보보호 관리체계를 기반으로 한 ISMS(Information Security Management System)와 개인정보보호 관리체계를 중심으로 PIMS(Persnal Information Management System)로 나뉜다.

(국외) 보안평가 방식으로는 영국을 중심으로 발달되어 있으며, ISO 국제표준기구를 통한 정보시스템 보안 표준규격도 구비되어 있는 상태이다.

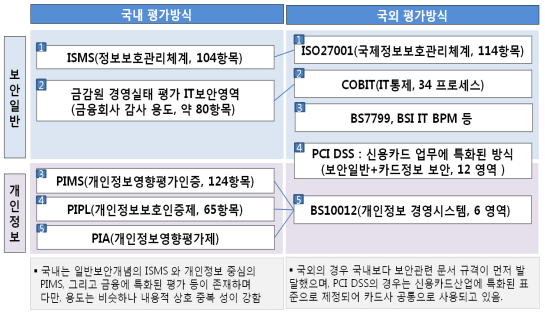

그림 3. 국내/외 보안 평가방식 현황
Fig. 3 Domestic / external security evaluation method taxonomy[4],[5],[6]

국/내외 평가방식은 대부분 기업에서 주로 활용하고 있는 것으로 금융회사의 경우 금감원의 경영실태평가(격년1회)를 의무적으로 받고 있다. 기타 평가방식 및 관련 세부사항은 다른 논문에서 많이 조사된 내용으로 본 논문의 주된 연구대상이 "보안평가 공시제도" 도입 필요성에 대한 부분임으로 여기서는 생략하도록 하겠다.

4. 선행학습 및 기타

보안평가 공시제도와 직접적으로 관련된 논문은 많지 않았다. 본 논제와 유사한 형태의 논문이라면 보안평가가 아닌 보안현황(조직, 투자, 인프라 등)에 대한 내용을 공시하는 방안으로 보안공시에 대한 타당성을 다양한 각도에서 제시하고 있었다[7]. 다만 이 논문에서 제시한 보안공시 내용을 일반 소비자측면에서 분석해 보면, 해당 기업이 보안이 좋은지 나쁜지를 판단하기에는 다소 난해하거나 어려운 항목으로 구성되어 있다. 또한 기업의 입장에서는 외부로 노출하기 꺼리는 보안사항도 포함되어 있어 이를 공시할 경우 또 다른 기업의 보안 취약성을 외부로 알리는 역기능이 존재할 수 있음을 파악할 수 있었다.이러한 부분을 보완한다면 보안공시제도에 대한 긍정적 기능을 많이 제시한 논문이기도 하다.

Ⅲ. 현황 및 문제점

1. 보안공시 현황

국내 보안관련 의무공시의 경우 정보통신망법 및 개인정보보호법에 의거 제3자에게 정보제공 시 정보제공 기관 등 관련내용을 외부에 의무공시하게 되어 있다. 주요 금융회사별 공시여부를 확인한 결과 홈페이지를 통해 개인정보취급방침, 개인정보처리방침을 명시하고 정보제공사 등 관련 내용을 게시하고 있다.

표 2. 주요 금융회사의 개인정보 제공 공시현황
Table 2. Major financial company providing private information disclosure status

구분	은행(5)	증권(5)	보험(5)	카드(5)
공시 여부	O(5)	O(5)	O(5)	O(5)
방법	홈 페이지	홈 페이지	홈 페이지	홈 페이지
공시 내용	정보 제공 항목 등	정보 제공 항목 등	정보 제공 항목 등	정보 제공 항목 등

다만, 홈페이지 화면에서 공시내용을 찾기가 쉽지 않았으며, 게시된 제3자에 대해서만 제공되는지 여부는 확인할 수 없었다. 또한 금융소비자가 느끼기에 해당 금융회

사의 보안상태가 잘되어 있는 지 여부를 평가할 만한 공시 요소는 찾을 수 없었다.

미국의 증권거래위원회(Securities and Exchange Commission, SEC)에서는 기업의 재정적 손실을 가져올 수 있는 보안사고가 발생한 경우 관련 정보를 외부에 공시하도록 하는 가이드라인을 제정하여 운영하고 있다[8]. 이것은 의무이행 사항은 아니지만, 정보보안 관련 기업이 소비자에게 리스크 예방차원에서 제공하는 일종의 공시제도 라 볼 수 있을 것이다.

2. 보안평가 현황

금융회사의 경우 보안평가의 경우는 금감원의 경영실태평가(IT보안영역)와 정보기술(IT)영역에 대한 통제기술서 형태로 평가를 받고 있다. 또한 일부 회사에서는 사설 보안인증 획득을 위해 ISO27001 등 정보보호 관리체계에 의해 평가를 받고 있는 것으로 파악되었다. 신용카드사의 경우 해외 Visa, Master, Amex 카드 등과 제휴시에는 정기적으로 지불결제산업 데이터보안 표준(PCI DSS)을 기준으로 보안평가를 받고 있다[9]. 이 경우 해외 카드사가 평가주체가 되어 시행하는 것으로 제휴대상 기업이 관련 자료제출 및 인터뷰를 하는 방식으로 점검하고 있다.

표 3. 주요 금융회사의 보안평가 현황
Table 3. Major financial company security assessment status

구분	공시유무	은행 (5)	증권 (5)	보험 (5)	카드 (5)
금감원 경영실 태평가	미 공시	O(5)	O(5)	O(5)	O(5)
회계 감사평 가	미 공시	O(5)	O(5)	O(5)	O(5)
인증 평가획 득	공시	O(4) X(1)	O(1) X(4)	O(4) X(1)	O(3) X(2)
PCI DSS	미 공시	X(5)	X(5)	X(5)	O(5)

Ⅳ. 설문조사 분석 및 고려사항

1. 개요

이번 설문조사의 목적은 연구대상인 금융회사의 “기업 보안평가 공시제도” 도입에 대한 여론 및 시행 시 어떤 방식으로 가야하는지에 대한 방향성을 찾고자 하는 것이다. 대상은 회사원, 주부, IT종사자, 교사 등 금융거래를 이용하는 다양한 소비자들이며, 인터넷을 통해 총 60명을 대상으로 무작위 표본조사 형태로 진행하였다. 조사항목은 총27개로 현 금융회사에 대한 보안 신뢰도 및 제도 시행에 대한 의견을 구하는 형식으로 진행하였다.

No	설문내용
1~5	귀하의 연령대/업종/직업/업무/직급?
6~7	금융서비스 이용여부/종류?
8~9	귀하가 이용하는 금융회사의 안전유무/안전하지 않다면 이유는?
10~11	최근 신용카드사 정보유출사고시 유출여부/이후 조치사항은?
12	금융회사의 보안사고가 계속 발생하는 이유는?
13~14	신용카드사 외 정보유출 유무/이후 조치는?
15~16	사고발생 회사와 기업에 거래여부/사고회사와 거래하기 전제 위한 조건은?
17~18	금융회사 선택 시 우선고려사항/정보보호 안전성을 판단하는 기준 또는 방법은?
19~20	보안평가 공시제도 도입 찬성여부/이전 답변이유?
21	제도 도입 시 공시내용을 보고 회사 선택할 경우 참고할 것인지?
22	제도 도입 시 상대적으로 평가가 낮을 경우 타사로 이동여부?
23~26	선호하는 공시매체/평가결과에 대한 유형/평가주체/주기/?
27	제도 도입 시 반영하고 싶은 사항은?

그림 4. 소비자 설문조사 항목
Fig. 4. Consumer survey items

2. 결과분석

설문항목은 총27개 중 금융회사 신뢰도 및 공시제도를 중심으로 4가지 주요영역을 중심으로 결과를 분석해 보도록 하겠다. 첫째로 현재 금융회사의 정보보안에 대한 신뢰도 및 정보유출 사고가 증가하는 이유에 대한 조사내용이다. 응답자의 97%가 본인이 거래하는 금융회사에 대한 보안관련 신뢰는 하지 않는 것으로 나타났으며, 그 이유는 기업 내부통제 미흡(61%), 해킹기술의 발달(36%), 고객부주의(3%) 순으로 응답했다.

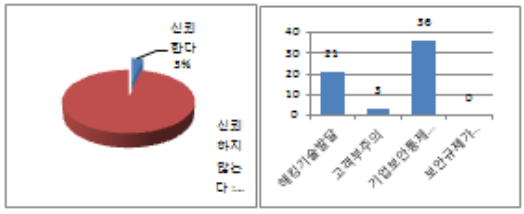

그림 5. 금융회사 신뢰여부 및 사고원인
Fig. 5. Financial institutions trust and causes of accident

둘째로 지난 신용카드사 정보유출 사고 시 정보유출 여부에 대해 응답자 77%가 유출되었으며, 이중 유출 이후 45%가 해당 금융회사와 거래를 중지하거나 카드를 재발급 받은 것으로 나타났다. 또한 8%는 법적 소송을

진행 중이다. 다만 47%가 아무 조치를 취하지 않은 것으로 밝혀져 소비자들의 개인정보 사고대응에 대한 태도는 아직 소극적인 것으로 파악되어 진다.

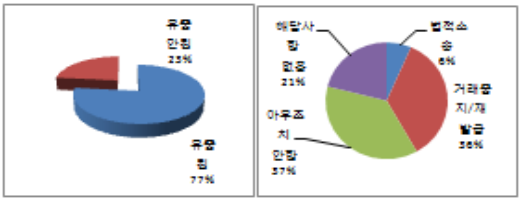

그림 6. 정보유출 여부 및 대응방식
Fig. 6. Information disclosure and whether your coping status

셋째로 "보안평가 공시제도" 도입에 대한 질문에 응답자 97%가 찬성하였으며, 다만 반대한 응답자도 3%나 되었는데, 이는 해당 업무에 종사하는 보안담당 직군으로 업무 과부하를 들어 반대하는 것으로 나타났다. 또한 제도 시행 후에 금융회사를 선택할 때 참고하겠냐는 질문에는 모든 응답자 100%가 참고하겠다고 응답했으며, 기존 거래하는 금융회사가 타사 대비 상대적으로 보안평가가 안 좋을 경우에는 타사도 이동하겠다가 92%로, 이동을 고려하겠다가 5%, 그냥 있겠다 가 3%로로 나타났다. 이번 결과에 의하면 향후 이 제도가 시행될 경우 금융회사를 선택하는 기준이 기존의 투자 수익률이나 금융상품 선호도 외에도 정보보안 평가결과를 함께 고려한다는 의미로 금융회사의 영업환경에도 많은 변화가 올 것으로 보인다.

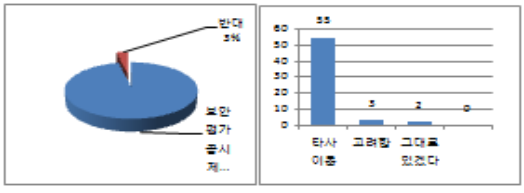

그림 7. 보안평가 공시제도 도입여부 및 금융회사 이동여부
Fig. 7. Security Assessment and financial disclosure whether the company introduced Whether moving

넷째로 보안평가를 시행할 경우 평가 주체가 누가 되어야 하느냐에 대한 부분이다. 응답자 중에 59%가 금감원 등 감독기관에 해야 한다고 답변했다. 이는 금융회사의 상급기관인 금감원 등에서 실제 영업정지나 기타 관리감독 권한을 가지고 있어 제도 시행 시 철저한 감사자 입장에서 제도를 정착해야 한다는 의견으로 보여 진다. 그리고 보안전문 업체 17%, 사설 인증기관 16%로 나타났다. 특히 평가주체가 독립된 권한과 객관성을 확보 할 수 있는 별도의 기관이어야 한다는 의견이 8%로 향후 신용평가사와 같은 별도의 기구가 만들어 질 수 있을지는 지켜봐야 할 거 같다. 또한 평가결과의 공시매체에 대한 의견으로는 홈페이지가 25%, 핸드폰 문자 8%, 이메일 2%, 사업장 3%로 하나의 매체를 통해 공시하는 것보다 모든 매체 및 사업장에 게시해야 된다가 62%로 압도적으로 많았다.

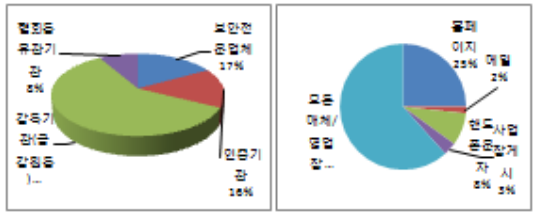

그림 8. 보안평가기관 유형 및 공시방법
Fig. 8. Security Evaluation Facility Type and disclosure methods

기타 의견으로는 평가공시 주기는 1년이 52%, 6개월이 31%로로 1년 이하를 가장 선호했으며, 평가결과 방식은 1,2,3 또는 A,B,C 등의 등급화가 43%, 100점 기준의 점수화가 30%로 소비자입장에서 이해하기 쉽고 타 회사와 비교가 가능한 표준화된 방식을 원하는 것으로 나타났다.

이제까지 "금융회사 보안평가 공시제도" 도입에 대한 다양한 소비자들의 의견을 수집하여 조사. 분석해 보았다. 종합 정리해 보면 금융 소비자들은 현재 금융회사 보안수준에 대해 신뢰하지 않고 있으며, 보안수준이 어느 정도인지 확인하고 싶지만 객관적으로 알 수 있는 방법이 없는 것으로 나타났다. 또한 이 제도가 시행될 경우 금융회사를 선택 또는 이동시 고려하겠다가 대다수인 만큼 본 제도에 대한 시행 및 구체적인 방안에 대해 논의가 필요할 것으로 보인다.

3. 고려사항 및 기대효과

앞서 분석한 결과에서도 나타났듯이 금융소비자들은 금융회사의 정보보호를 신뢰하지 않고 있다. 이것은 현재도 정보유출 사고는 계속발생하고 있는데, 지금 거래하는 금융회사가 안전한지에 대한 정보를 어디서도 얻을

수 없기 때문이다. 따라서 이에 대한 문제점을 해결하기 위해서는 먼저 소비자들에게 금융회사에 대한 보안 수준을 객관적으로 평가하여 보여 줄 수 있는 제도가 필요하다는 것이다. 이렇게 되면 현재 금융회사가 추진하고 있는 소비자 중심의 영업과 연계되어, 회사는 소비자의 개인정보를 안전하게 보관하는지 유무를 객관적으로 평가받기 위하여 소비자의 정보보호에 사활을 거는 영업환경이 자연스럽게 조성될 것이고, 이에 따라 회사의 보안 리스크는 지금보다는 크게 개선될 것이기 때문이다.

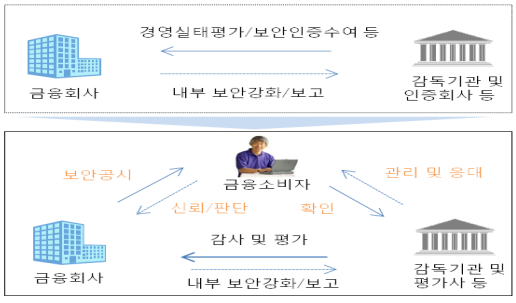

그림 9. 보안평가 개선방식
Fig. 9. Improving security assessment structure

그리고 설문조사 결과, 공시제도를 시행할 경우 평가주체에 대해 금감원 등 감독기관을 선호하는 비율이 59%이상 차지한 것을 보면, 평가주체에 대해 초기에는 신뢰가 갈 수 있는 기관이 주체로 추진되어야 신뢰성을 유지할 수 있을 것으로 보이며, 평가 방식에 있어서도 일반적인 표준화된 보안점검 사항들 외에 금융회사가 가진 특수한 규제(5.5.7제도 등, 금융회사 IT보호업무 이행지침)[10]를 반영한 금융전용 평가방식을 도입하는 것이 효과적인 보안 리스크 제거와 운영 관리상에도 효율적일 것이다.

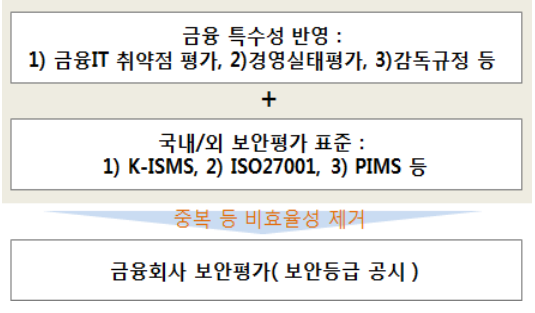

그림 10. 보안평가 이행방안
Fig. 10. Security Assessment Implementation

따라서 평가방식은 Fig 10과 같이 현재 금융회사가 평가받고 있는 금융IT 취약점분석 및 IT경영실태평가 항목(69개) 등을 기반으로 하고, KISA의 ISMS(104개) 및 PIMS(118개) 등 다른 정보보호 인증체계와 비교, 분석하여 금융의 필수항목 및 각 평가방식의 중복적 요소를 제거하여 최종적으로 평가 항목으로 하고 이를 기반으로 소비자가 이해하기 쉬운 등급제 형태로 공시하는 평가방식이 고려되어야 할 것이다.

표 4. 보안평가 공시 후 개선효과
Table 4. Security evaluation performed after disclosure Benefits

구분	현재	제도 시행 후
소비자 측면	- 금융회사 선택/거래 시 보안수준을 판단할 근거가 없다 - 금융회사의 보안을 신뢰하지 않음	- 금융회사 선택 시 보안수준평가 가능(소비자 권리) - 지금보다 보안 신뢰도 향상
금융회사측면	- 영업중심 사업으로 보안에 대한 인식 및 투자 미흡 - 지속적 사고발생	- 소비자신뢰성 회복 - 보안활동 강화 - 보안리스크 감소에 따른 사고 예방

V. 결 론

지금까지 금융회사의 “보안평가 공시제도” 도입 필요성에 대하여 선행학습과 관련 현황 및 소비자 설문조사 분석 등을 통해 알아보았다. 이번 연구는 금융회사의 대규모 정보유출 사고가 계속 발생하고 있고, 뚜렷한 해법을 찾지 못하는 상황에서 업무적, 기술적 보안의 한계를 넘어서 기업의 정보보호에 대한 개념을 다른 각도에서 조명할 수 있는 부분이라고 생각한다.

하나는 소비자측면에서 기업의 보안을 바라본다는 것과 다른 하나는 기업의 입장에서 소비자중심의 보안정책을 추구하면서 얻게 되는 실질적인 보안기능의 강화가 사회적 이슈인 보안사고 예방에 크게 기여할 수 있다는 것이다. 따라서 “보안평가 공시제도”가 금융회사에 도입이 된다면 기존에 소비자가 가지고 있던 보안에 대한 불신이 줄어들 것이고, 기업 내부에서의 보안은 단순 지원업무가 아닌 회사 전략상 중요한 업무로 인식되어 적극적인 정보보호 강화 활동을 통해 결과적으로 보안리스크 감소 및 사고예방에 직접적인 영향을 줄 것이기 때문이다.

끝으로 본 연구를 위해 기존 선행연구를 학습하면서

"기업 보안평가 공시제도"에 대한 관련 논문이나 자료가 의외로 많지 않아 추후 지속적인 연구가 필요할 것으로 보이며, 보수적인 금융회사의 보안에 대한 정보나 자료가 많지 않아 일정부분 연구의 한계가 있었다. 또한 이번 연구범위가 "보안평가 공시제도" 도입이 왜 필요한가에 대한 당위성에 대한 분석을 중심으로 했기에 추가적으로 보안평가에 대한 구체적인 방법론이나 기준 및 관리체계에 대해서는 향후 연구가필요하다.

References

[1] Annual Status of Privacy Complaint Counseling, From personal Information Protection Commission
[2] Yeon-Ju Lee, The factors of the School of Information Disclosure,influencing enhance confidence in public education, Dec. 2013
[3] Jae-Geun Lee "An Estimation Model of the Personal Information Protection Performance Level using the Privacy Policy Disclosure Data", Dec. 2013
[4]http://www.fss.or.kr/fss/kr/bbs/list.jsp?bbsid=12073 96397643&url=/fss/kr/1207396397643
[5]http://isms.kisa.or.kr/kor/notice/dataList.jsp?p_No=4 8&b_No=48
[6]http://www.iso.org/iso/home/standards/management -standards/iso27001.htm
[7]Hyo-Jung Jun, "A Feasibility Study on Introduction of Information Security Disclosure", Dec. 2012
[8]http://www/sec.gov/diisions/corpfin/guidance/cfguid ance-topic2.htm (SEC "Guidance concerning cyber incident disclosure)
[9]https://www.pcisecuritystandards.org/security_stand ards
[10]http://www.fss.or.kr/fss/kr/bbs/list.jsp?bbsid=1207 396397643&url=/fss/kr/1207396397643, July. 2014
[11]Woo-Jun Kang. "2014 An Efficient Privacy Preserving Method based on Semantic Security Policy Enforcement", Dec. 2013

저자 소개

임 종 인(회원)

- 1986년 : 고려대학교 수학과 이학박사
- 現 고려대학교 정보보호대학원장,개인정보보호위원회위원,국방부정보화책임관자문위원 등

<관심분야 : 사이버국방, 정보법학, 디지털포렌식, 개인정보보호, 융합기술보안 등>

김 보(회원)

- 2008년 : 고려대학교 정보경영공학과 (석사)
- 2013년 : 고려대학교 정보보호대학원 박사과정
- 現 고려대학교 정보보호연구원 금융보안연구센터 수석연구원

<관심분야> 금융보안, 전자결재보안, 보안정책, 융합보안 등