The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 16, No. 3, pp.29-38, Jun. 30, 2016. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2016.16.3.29
JIIBC 2016-3-5

# 협동조합형 금융회사의 중앙회를 위한 정보보호 인력 및 예산의 적정성에 관한 연구

# A study on Information Protection Manpower and Budget Adequacy for Cooperative-Type Financial Company's Federation

임정환*, 김인석**

**Jung-hwan Lim*, In-Seok Kim****

**요 약** 협동조합형 금융회사란 협동조합 원칙에 따라 다수의 금융회사(일명 '조합')와 이를 지도·감독하는 중앙 조직인 중앙회로 구성되어 있다. 조합은 일정 지역 내 조합원을 바탕으로 운영되고 그 규모가 영세하기 때문에, IT 및 정보보호업무를 중앙회를 통해 위탁 구축·운영·관리하고 있다. 그러나, 금융당국은 전자금융거래법 하위규정인 전자금융감독규정을 통해 IT 및 정보보호 기준을 제시함에 있어 주식회사형 금융회사인 상업은행의 현황을 주로 고려하여 제시하였기 때문에, 협동조합형 금융회사 중 중앙회에는 적절하지 않다. 본 논문에서는 조합의 IT 및 정보보호 업무를 위탁받아 수행하는 중앙회 관점에서 정보보호 측면에서의 현황 및 고려사항을 확인하고, 개선사항을 제시함으로써, 협동조합형 금융회사의 중앙회를 위한 효율적인 정보보호 인력 및 예산 수립기준을 제안하고자 한다.

**Abstract** A financial institution operated by cooperatives, abiding by the principle set by the cooperative federation, is comprised of a numerous financial institutions. Most of these small institutions are operated within local areas, providing financial services for coop members. The Financial Supervisory Regulations that supervises security professionals, organizations, and budgets are established entirely based on commercial banks in which the application of these regulations on coop financial institutions may not be proper. This paper aims to provide an efficient IT security policy for nation-wide financial institutions operated by the Cooperative Federation by analyzing its security personnel managements and adequacy.

**Key Words :** Cooperative Federation, Financial institution operated by cooperatives, 557 Rule, The financial Supervisory Regulations

## Ⅰ. 서 론

협동조합형 금융회사란 동일 행정구역(통상 읍·면 단위) 또는 같은 직장이나 단체 등 공동유대를 같이 하는 조합원 간에 상부상조를 통해 조합원의 경제적 지위를 향상시키기 위해 설립된 것으로, 우리나라에는 5개 기관이 있다(신용협동조합법에 의해 설립된 신용협동조합, 농업협동조합법에 의해 설립된 농업협동조합, 수산업협동조합법에 의해 설립된 수산업협동조합, 산림조합법에 의해 설립된 산림조합, 새마을금고법에 의해 설립된 새

*정회원, 고려대학교 정보보호대학원 금융보안학과
**정회원, 고려대학교 사이버국방학과(교신저자)
접수일자 : 2016년 4월 15일, 수정완료일 : 2016년 5월 15일
게재확정일 : 2016년 6월 10일

Received: 15 April, 2016 / Revised: 15 May, 2016 / Accepted: 10 June, 2016
**Corresponding Author : iskim11@korea.ac.kr
Dept. of Information Security, Korea University, Korea

마을금고 등임). 이들은 각각 다른 설립 근거법에 의해 설립되었으나 5개 기관 모두 개인이 조합원의 자격으로 참여하여 설립하고, 조합원이 직접 운영하며, 참여 조합원이 책임지는 협동조합의 기본 원리에 따라 조직·운영되고 있다.

협동조합형 금융회사의 조직구성은 조합원들로 구성된 '조합' 또는 '단위조합'과 다수 개별 '조합'들을 지도·감독하는 중앙조직인 '중앙회'라는 이원 체제로 구성되어 있는데, 전국적으로 동일한 상호 및 로고를 사용하고 있다. 2014년말 기준 5개 기관 전체로 3,672개(농협: 1,154개, 수협: 90개, 산림조합: 136개, 신협: 920개, 새마을금고: 1,372개(금융감독원 통계 및 새마을금고 통계자료))의 조합과 5개의 중앙회가 있다[1].

조합의 영세성을 보완하고 규모의 경제를 실현하기 위해 중앙회를 조직하고 있으며, 중앙회는 조합들의 중앙은행 역할과 함께 경영지도, 교육, 홍보, IT 및 정보보호, 감사 등의 서비스를 제공한다. 조합은 IT 및 정보보호 업무 대부분을 중앙회에 위탁하는데, 이는 개별 조합의 공통업무를 중앙회에 위탁함으로써 공동이용에 따른 비용절감과 중앙회 인력의 전문성을 이용하여 좀 더 효율적으로 운영하도록 할 수 있기 때문이다.

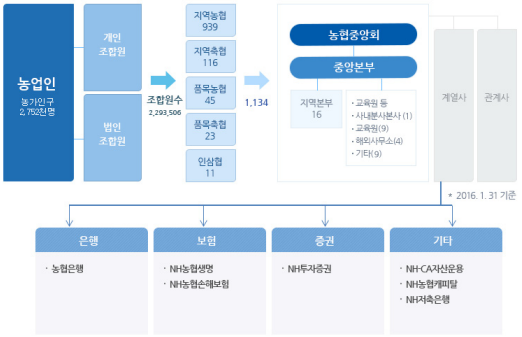


**그림 1. 농협중앙회 조직도**
**Fig. 1. Organization Chart of National Agricultural Cooperative Federation**

본래 협동조합형 금융회사는 조합원을 상대로 한 예·대 업무와 공제(보험) 업무만을 취급하였으나 1990년부터 비조합원과의 예금과 대출거래가 허용된 이후 취급업무에 대한 지속적인 규제완화 조치로 현재는 신용카드와 외환업무 등 일부 업무를 제외하고 일반 상업은행과 동일한 영업형태를 취하고 있다.

2014년말 협동조합형 금융회사의 조합 임직원수는 149,790명이며, 자산규모는 약 502조원이다, 이는 18개 국내 시중은행의 총 임직원 수 인 135,281명보다 많으며, 자산은 시중은행의 22% 수준이다(금융감독원 금융통계정보시스템 및 새마을금고 통계). 인력이나 자산규모로 볼 때 상업은행 못지않게 상당한 비중을 차지하고 있으며, 대표적인 금융부분 감독기관인 금융감독원도 비은행 부분으로서 협동조합형 금융기관을 감독하기 위한 별도의 부서를 두고 있다.

2011년 4월 12일 금융회사 해킹피해사고로 인해 금융회사에 대한 보안문제가 대두되었고, 금융당국은 전자금융감독규정 전면개정을 통해 전자금융거래법 상 금융회사로 하여금 IT인력은 총 임직원 수 의 5% 이상을 IT인력으로, 정보보호 인력은 IT인력의 5% 이상을 보안인력으로, IT예산의 7%를 IT보안 예산으로 확보하는 것을 노력하도록 규정(이하 '5·5·7 기준'이라 함)하고 있다.

그러나, 이 5·5·7 기준은 주식회사형 금융회사인 상업은행의 IT 및 정보보호 업무 현황을 주로 고려하였기 때문에, 협동조합형 금융회사의 조직구성 형태에서는 적절하지 않는 부분이 있다. 본 논문에서는 조합의 IT 및 정보보호 업무를 위탁받아 수행하는 중앙회 관점에서 정보보호 측면에서의 현황 및 고려사항을 확인하고, 개선사항을 제시함으로써, 협동조합형 금융회사의 중앙회를 위한 효율적인 정보보호 인력 및 예산 수립 기준을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 협동조합형 금융회사의 현황 및 고려사항에 대해 설명하고, 3장에서는 개선된 정보보호 인력 및 예산 기준 개선안을 제시하며, 4장에서는 결론을 제시한다.

## II. 현황 및 고려사항

### 1. 협동조합형 금융회사의 정보보호 리스크

협동조합형 금융회사는 조합원을 중심으로 지역적인 공동유대감이 존재하고, 지역주민에게 금융편의를 제공함으로써 지역경제의 발전에 이바지하는 목적달성을 위해 존재하기 때문에, 정보보호 측면에서 상업은행과는 다른 몇 가지 고려사항이 존재한다. 구체적으로 '조직 내부통제의 한계', '조합들간 규모의 양극화로 인해 일률적인 기준의 적용이 어려움', '다수 규제기관의 관여'가 있을 수 있다.

#### 가. 고려사항 1 : 조직 내부통제의 한계

협동조합형 금융회사는 구성원 간 일체감 형성과 상

호작용이 중요시되는 조직문화와 규모의 영세성으로 인한 내부통제의 한계로 상업은행에 비해 정보보호 리스크가 상대적으로 더 높은 것으로 보인다.

구체적으로 보면 일정 지역이나 공동의 사업에 참여조합원을 중심으로 이루어지는 사업형태에서 오는 협동조합 특유의 온정적인 조직문화로 인해 정보보안과 관계깊은 업무통제, 사고통제, 접근통제를 엄격히 하는데 부담을 느낄 수 있으며, 경영감시를 소홀히 할 가능성이 있다. 특히 조합은 각각이 개별 법인으로 소속 임직원이 타법인 조합으로 이동하기 어렵고, 직원 수가 너무 적어 유착 비리나 타성에 젖은 근무형태를 방지하기 위한 직무분리, 순환보직 등 내부견제가 어려운 조합들도 많아 충분한 보안수준을 유지하기 어려운 경우도 많다[2].

조합 내부통제의 한계에 대한 대표적인 사례로 보이스피싱으로 인한 대포통장 개설 비율 측면에서 확인할 수 있다. 2014년 상반기 금융회사 별 대포통장 발급현황을 보면 지역농협, 새마을금고 등 협동조합형 금융회사가 약 40%(Table 1에서 굵게 표시된 금융회사)를 넘게 차지하는 것을 알 수 있다. 또 주로 지방에 위치한 금융기관인 우체국이나 농협은행 등을 제외하면 일반 상업은행의 비율은 채 10%가 넘지 않아 대조를 이루고 있다. 이는 내부통제가 취약한 지역의 조합을 중심으로 대포통장 개설 경로로 활용되고 있음을 알 수 있다.[3].

**표 1. 대포통장 개설 금융기관 상위 10개 사(2014.1~6)**
**Table 1. Top 10 Depot Bankbooks number by Financial Institution of Korea(2014.1~6)**

| 순위 | 은행 | 대포통장 수 | 대포통장 비율(%) | 피해액 (백만원) |
|---|---|---|---|---|
| **1** | **지역농협** | **3,408** | **30.75** | **25,961** |
| 2 | 우체국 | 2,403 | 21.68 | 18,152 |
| 3 | 농협은행 | 1,554 | 14.02 | 11,939 |
| **4** | **새마을금고** | **1,115** | **10.06** | **7,870** |
| 5 | 증권사 | 623 | 5.62 | 6,405 |
| 6 | 우리은행 | 354 | 3.19 | 4,585 |
| 7 | 하나은행 | 274 | 2.47 | 2,268 |
| 8 | 신한은행 | 232 | 2.09 | 1,762 |
| 9 | 기업은행 | 232 | 2.09 | 1,828 |
| **10** | **신협** | **174** | **1.57** | **1,135** |

### 나. 고려사항 2 : 조합들 간 규모의 양극화로 인한 일률적인 기준의 적용이 어려움

조합들 간 규모의 양극화가 점점 심화됨에 따라, 대규모 조합과 소규모 조합 간 규모의 격차로 인해 정보보호 측면에서 위험의 차이가 있을 수 밖에 없음에도, 규제기준이 일률적으로 적용됨으로써 과소 또는 과대 규제감독으로 인한 문제가 일어날 수 있다.

정보보호 분야 법률에 있어서는 전자금융거래법 시행령 제11조 제3항에서 정보보호최고책임자를 임원급으로 임명해야 하는 금융회사의 규모를 '총자산 2조원 이상이고, 상시 종업원 수 300명 이상'으로 정하고 있는데 이는 대부분의 협동조합형 금융회사에는 적용이 되지 않는다.

이에 반해 금융 분야 법률은 대표적으로 신용협동조합법 시행령 제14조의2에서 총 자산 1,500억원 이상의 대형조합과 부실조합으로 나누어 상임이사 설치를 의무화하고, 총 자산 2,000억원 이상의 조합은 상임감사를 둘 수 있도록 하는 등 조합의 자산분포에 따라 규제 적정성을 고려하여 법률 실효성을 높이고 있다.

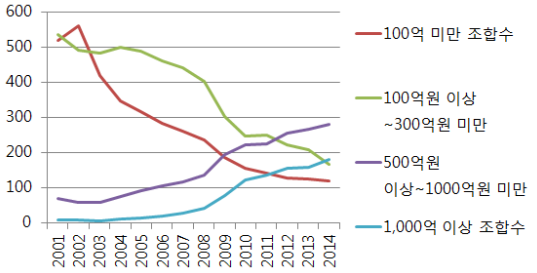


**그림 2. 자산규모에 따른 신협 수 변화(2001-2014)**
**Fig. 2. Institution Number of National Union Federation of Korea by Asset Size (2001-2014)**

### 다. 고려사항 3 : 다수 기관의 관여

우리나라의 경우 설립목적, 조직구조가 유사하지만 설립 근거법이 서로 다른 협동조합형 금융회사들이 각기 다른 기관으로부터 규제를 받는다. 각 기관의 설립 근거법과 규제는 표 2와 같다.

**표 2. 협동조합 형 금융회사의 특별법과 감독기관**
**Table 2. Supervisory Organization & Law of Financial institution operated by cooperatives**

| 기관명 | 특별법 | 감독기관 | | |
|---|---|---|---|---|
| | | 경제 | 금융 | 공제 |
| 농협 | 농협법 | 농림축산 식품부 | 금융감독원 | 농림축산 식품부 |
| 수협 | 수협법 | 해양 수산부 | | 해양 수산부 |
| 산림조합 중앙회 | 산림 조합법 | 산림청 | | 산림청장 |
| 신협 | 신협법 | 금융위원회 | 금융위원회 | 금융위원회 |
| 새마을 금고 | 새마을 금고법 | 행정자치부 | | |

규제기관이 협동조합형 금융회사마다 상이하기 때문에, 규제기관의 입장에 따라 정보보안에 대한 기준이 달라질 수도 있으며, 협동조합 금융회사들이 서로 경쟁하면서 어느 한 기관에 의해 규제가 완화되면 형평성 차원에서 다른 기관의 규제도 완화되어야 한다는 요구가 제기되어 결국 규제관용의 수준을 어디까지 허용하여야 하는지에 대한 문제점을 발생시킨다.

이에 따라 금융위원회는 2013년부터 신협, 농협, 수협, 산림조합 및 새마을금고 등 상호금융 관계기관들이 참석한 '상호금융정책협의회'를 개최하여 기관 간 정책공조 강화와 '동일기능 동일규제' 원칙에 따른 금융감독업무 체계화를 위해 노력하고 있으나 IT 또는 정보보안 분야가 별도로 논의된 적은 없다.

## 2. 국내외 정보보호 인력 및 예산 관련 기준 및 동향

본 장에서는 국내외 정보보호 인력 및 예산 관련하여 규정 또는 기준 및 동향에 대해 설명한다.

### 가. 정보보호 인력 기준 및 동향

(1) 전자금융감독규정 상 정보보호 인력 기준

전자금융거래법 하위규정인 전자금융감독규정 제8조에 따르면, 금융회사 또는 전자금융업자는 인력 및 예산에 관하여 정보기술부문 인력은 총 임직원수의 100분의 5 이상, 정보보호 인력은 정보기술부문 인력의 100분의 5 이상, 그리고, 정보보호예산을 정보기술부문 예산의 100분의 7 이상이 되도록 노력하도록 규정하고 있다.

이 규정에서 총 임직원 수를 산정하는 기준으로 금융회사 등의 상시 종업원으로 하되, 1년 이상 장기휴직자와 외주(outsourcing)인력은 제외하도록 하고 있으며, 정보기술인력부문 산정 시 "금융회사의 총임직원 중 내부 규정에 따라 IT 기획·개발·운영·정보보호 등 정보기술부문의 업무를 처리하는 사람", 그리고, "IT업무를 담당하는 상시 종업원 중 해당 금융회사의 IT업무를 적법한 절차에 의해 수행하는 사람으로서, 이 규정 제60조제1항제13호에 의한 업무수행인력 관리방안에 따라 관리되고 있는 사람으로 정하고 있다."으로 정하고 있다.

그리고, 정보보호 인력은 "금융회사의 총임직원 중 내부 규정에 따라 정보보호 업무를 처리하는 사람", 그리고, "정보보호 업무를 담당하는 상시 종업원 중 해당 금융회사의 정보보호 업무를 적법한 절차에 의해 수행하는 사람으로서, 전자금융감독규정 제60조제1항제13호에 의한 업무수행인력 관리방안에 따라 관리되고 있는 사람"으로 정하고 있다.

또한 전자금융감독규정 <별표1>의 제2항의 나(4) 및 제3항의 나(4)에서는 조합의 정보기술부문 인력과 정보보호인력의 정의와 관련한 특례조항이 있는데, 예컨대 중앙회가 조합의 전자금융기반시설에 대한 운영을 공동수탁하는 경우, 중앙회에서 IT업무를 수행하는 상시 종업원에 대하여 각 조합의 운영비용 분담비율에 따라 산정한 인력에 대하여는 각 조합의 정보기술부문 인력으로 간주할 수 있는데, 또한 동 규정 제3항에서는 각 조합은 전자금융감독규정 제8조 제2항의 인력과 예산의 구비 여부를 확인할 때 동 규정 <별표1> 및 <별표2>의 내용을 준수하여야 한다.

### (2) 국내 금융회사의 정보보호 인력 동향

한국은행의 2014년 금융정보화 추진현황에 따르면 국내 155개 금융회사를 대상으로 조사한 결과 금융IT인력이 총 임직원수에서 차지하는 비중은 3.8%로 전년말 대비 0.4%p 증가하였으며, 정보보호 인력이 IT인력에서 차지하는 비중은 8.4%(총 임직원수 기준 0.3%)를 기록하였다[5].

**표 3. 금융기관의 총 임직원 수, IT인력 수, 정보보호 인력 수 (기준, 명, %)**

**Table 3. Total Staff & IT Staff Number of Korean Financial Institute (Unit: People, %)**

| 연도 | 총 임직원 | IT인력 | 정보보호 인력 |
|---|---|---|---|
| 2012 | 240,191 | 8,202 (3.4) | 447 (5.4) |
| 2013 | 242,545 | 8,356 (3.4) | 574 (6.9) |
| 2014 | 239,539 | 9,136 (3.8) | 770 (8.4) |

일반은행, 지방은행, 특수은행을 포함한 전체 국내 상업은행 임직원 수는 2013년 124,904명을 기록하였으며 전년말 대비 0.8% 감소하였다. 그러나 금융IT인력은 전년말 대비 9.2% 증가한 4,077명으로 나타났다.

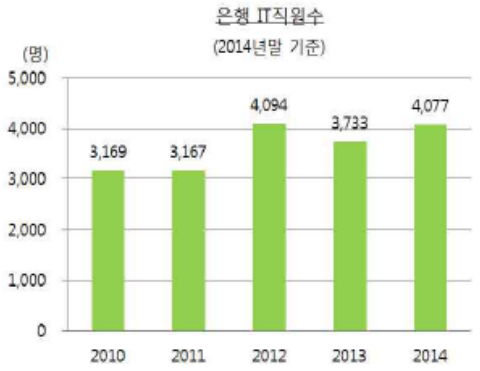


그림 3. 전체 은행 IT직원 수, 2010-2014
Fig. 3. Total Banking IT Staff Number. 2010-2014

한편, 보안 전담인력인 정보보호관리 인력의 비중은 전체 IT인력의 7.5%로 나타났다.

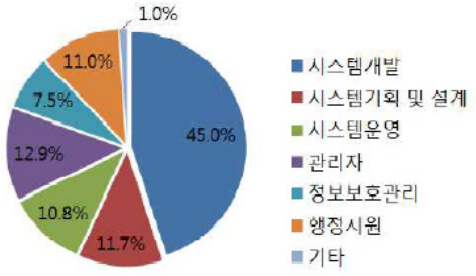


그림 4. 은행 IT직원 중 업무별 인력비중 2014
Fig. 4. Ratio of Banking IT Staff Number 2014

2014년 보안인력이 크게 증가한 이유로 한국은행은 은행의 신규 전산투자 및 시스템 개발이 확대되면서 전체 IT인력이 다소 증가하였고, 특히 은행권의 정보보호 노력으로 IT보안 전담인력이 크게 증가한 것으로 보고 있다.

### (3) 국외 정보보호 인력 동향

2014년 Gartner 자료[4]에 따르면. IT정규직(Full-Time Equivalent) 근무자를 기준으로 IT 인프라와 애플리케이션 보안과 일반적인 IT리스크 관리, IT 컴플라이언스, IT 사내 보안 등을 담당으로 하는 인력은 전체 IT인력 중 7.7%에 해당한다고 보았다.

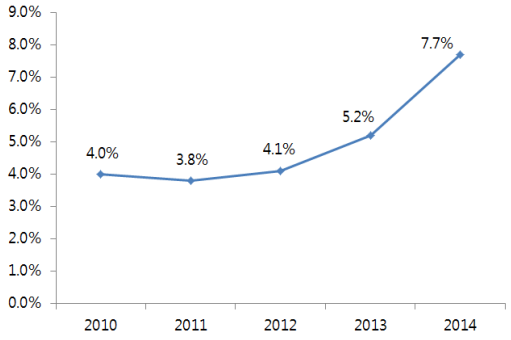


그림 5. 전체 IT인력 중 정보보호 인력 비중, 2010-2014
Fig. 5. Total IT Security Support FTEs as a Percent of Total IT FTEs, 2010— 2014

금융분야(Banking and financial Services)에 대해서는 2014년 전체 IT인력 중 10.0%가 보안인력으로 조사되었다.

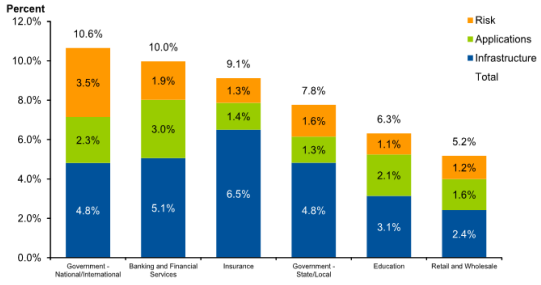


그림 6. 산업별 전체 IT인력 중 정보보호 인력 비중, 2014
Fig. 6. IT Security Support FTEs as a Percent of Total IT FTEs by industry. 2014

## 나. 정보보호 예산 기준 및 동향

### (1) 전자금융감독규정 상 정보보호 예산 기준

전자금융거래법 하위규정인 전자금융감독규정 제8조에 따르면, 금융회사 또는 전자금융업자는 예산에 관하여 정보기술부문 예산의 100분의 7 이상이 되도록 노력하도록 규정하고 있다.

### (2) 국내 금융회사의 정보보호 예산 동향

2014년 금융회사의 총 예산은 66조 2,482억원이며 그 중 IT예산은 5조 4,982억원으로 전년 대비 IT예산은 13.8% 증가한 것으로 나타났다. 한편 금융회사의 정보보호 예산은 5,668억원으로 IT예산 중 10.3%의 비중을 차지하여 금융당국이 제시한 정보보호 예산비중(IT예산 중

정보보호 예산을 7% 이상으로 편성)을 크게 상회하는 것으로 나타났다.

**표 4. 국내 금융회사의 총 예산, IT예산, 정보보호 예산 (단위 : 백만원, %)**

Table 4. Total Budget, IT & IT Security Budget of Korean Financial Institute. 2012-2014 (Unit : Ten Billion, %)

| 연도 | 총 예산 | IT예산 | 정보보호 예산 |
|---|---|---|---|
| 2012 | 63,925 | 5,229 (8.2) | - |
| 2013 | 58,778 | 4,833 (8.2) | 443 (9.2) |
| 2014 | 66,248 | 5,498 (8.3) | 567 (10.3) |

국내 은행권의 경우 2014년 총예산은 전년대비 2.8% 증가한 21조 8,826억원으로 나타났으며, IT예산은 전년대비 7.5% 증가한 2조 1,754억원으로 나타났다. 은행의 IT인력 증가 등에 따라 은행 총 예산 중 IT예산이 차지하는 비중이 2013년 9.5%에서 2014년에는 9.9%로 증가하였다. 한편 IT예산의 9.7%에 달하는 2,102억원이 정보보호를 위해 배정된 것으로 나타났다.

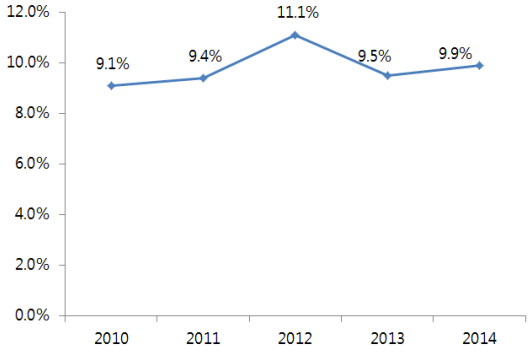


**그림 7. 연도별 전체 예산 중 IT예산 비율, 2010-2014**

Fig. 7. Ratio of IT Budget as a Percent of Total Budget, 2010-2014

### (3) 국외 정보보호 예산 동향

2014년 Gartner 자료[4]에 따르면, 전체 IT투자액 중 보안분야에 대한 투자액은 2011년 이후 계속 증가 추세로 2014년은 전체 IT투자액의 6.1%로 조사되었다.

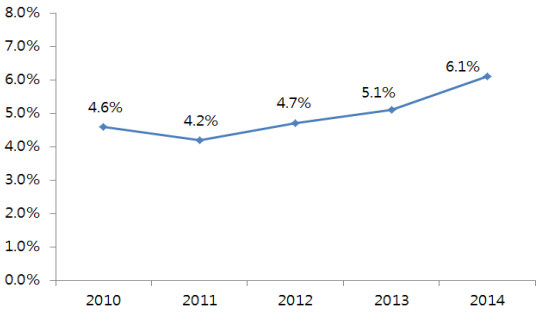


**그림 8. 연도별 전체 IT예산 중 정보보호 예산 비율, 2010-2014**

Fig. 8. Total IT Security Spending as a Percent of IT Spending, 2010-2014

특히 금융분야(Banking and financial Services)에 대해서는 2014년 전체 IT투자액 중 9.6%에 해당한다고 설명하고 있다.

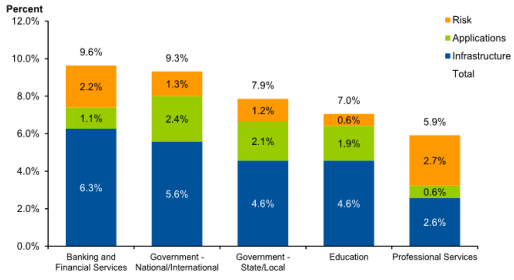


**그림 9. 산업별 전체 IT예산 중 정보보호 예산 비율, 2014**

Fig. 9. IT Security Spending as a Percent of IT Spending by Industry. 2014

## Ⅲ. 협동조합형 금융회사의 중앙회를 위한 정보보호 인력 및 예산 기준 개선방안

### 1. 인력 측면

#### 가. 중앙회의 성격을 고려한 보안인력 분리 필요

조합의 정보보호 인력을 산정하기 위하여 조합 중 신용사업, 특히 전자금융업무를 수행하는 조합은 전자금융거래법 제2조 제3호 마목 및 동법 시행령 제2조 제5호에 따른 금융회사로 취급되므로, 달리 특별한 예외규정이 없는 한 각 조합별로 전자금융감독규정 제8조 제1항에 따라 인력 및 조직을 운영하고, 동조 제2항에 규정된 인력 및 예산에 관하여서도 각 조합별로 인력과 예산 구비기준을 준수하는 것이 타당할 것으로 생각된다. 중앙회도 독립적인 사업을 수행하는 독립법인으로 각 특별법에

따라 별개의 법인격을 인정하고 있고, 상호금융사업을 영위하는 경우에는 신용협동조합법에 따른 신용협동조합의 중앙회로 보아 전자금융거래법상 금융회사로서 전자금융거래법이 적용된다고 보는 것이 합리적이다. 또한 전자금융감독규정은 전자금융거래법의 시행에 필요한 사항을 규정하는 것을 목적으로 하므로 전자금융거래법에 관한 의무와 금융회사로서 법적 주체를 종합적으로 고려하면 전자금융감독규정 제8조 제2항에서 규정하고 있는 "금융회사"가 준수해야 할 인력, 조직 및 예산에 관한 기준을 중앙회도 준수해야할 것으로 생각된다.

그러나 협동조합형 금융회사의 중앙회는 1개의 법인으로 성립하는 것일 뿐, 각 개별 법인인 조합의 IT 위탁을 받은 연합회로서 성립하는 것이 아니므로, 전자금융거래법상 '금융회사'의 의무를 부담하고 그 효과를 받게 되는 법적 주체는 중앙회라는 1개의 법인으로 보는 것이 논리적이다. 따라서, 협동조합형 금융회사의 중앙회는 그 자체로 전자금융거래법상 금융회사이므로 중앙회 전체 임직원을 기준으로 전자금융감독규정의 인력 및 예산규정을 충족해야 할 것으로 생각된다. 이와 같이 중앙회는 조합의 연합회로서의 역할을 수행하고 있음에도 보안인력의 산정은 조합의 임직원 수가 반영되지 않은 상황이다.

또한 농협중앙회 및 수협중앙회의 경우 각각의 계열사인 농협은행 및 수협은행이 IT 및 정보보호 인력을 공동으로 사용하고 있는데 중앙회는 개별 조합들의 정보보호 관련 리스크를 상시로 관리·감독을 위해 중앙회 내 조합들의 정보보호 리스크를 전담할 조직과 인력이 강화하여 개별 조합들에 대한 상시적인 내부통제·취약점 점검, 보안 교육 등이 실행되어야 하며, 조합을 위한 정보보호 기능이 중앙회의 다른 사업기능과 이행 상충의 여지가 있으므로 분리 독립성을 확보할 필요가 있다.

### 나. 정보보호 인력 산정방식 개선

금융감독원은 2014년 6월 "금융회사 정보기술(IT)부문 보호업무 이행지침"을 제정하여 전자금융감독규정 제8조 제2항 제1호에 따른 정보기술부문 인력(5%) 및 정보보호 인력(5%)을 산정 기준을 제시하고 있는데, 이 기준에 따른 정보기술부문 인력은 다음과 산정된다.

상업은행의 경우 전자금융감독규정 제8조에 의해 운용할 수 있는 최소 정보보호인력은 총 임직원수의 0.25%(총 임직원수 의 5% × 정보기술부문 인력의 5%)이다.

**표 5. 정보기술부문 인력 산정 기준**
Table 5. Calculation Method of Regulation Observance IT Staff number

| | |
|---|---|
| 금융회사 내부인력 | ① |
| 전산자회사 등의 인력 | ② |
| 금융회사 외주인력 | ③ |
| 내부정보기술부문 인력 | ⓐ = ① |
| 인정 전산 자회사 인력 | ⓑ = ② - (재하청 인력) |
| 인정 외주 인력 | ⓒ = (③ ≥ ①) |
| 정보기술부문 인력 | ⓓ=ⓐ+ⓑ+ⓒ |
| 금융회사 총 임직원 수 × 0.05 | Ⓐ |
| 규제 준수 여부 | Ⓐ ≤ ⓓ |

조합도 상업은행과 마찬가지로 기본적으로 금융업무를 할 수 있도록 되어 있으며, 전자금융감독규정에서 요구하는 사항은 금융사업에 국한되고 있다. 그러나 조합은 금융·비금융 업무를 모두 하고 있기 때문에 해당 조합법인은 감독대상이 되며, 또한 중앙회도 조합과 관련한 상호금융 업무를 수행하고 있으므로, 당연히 중앙회도 감독 대상된다.

그에 따라 중앙회 보안인력에 대한 기준은 중앙회 자체 정보보호 최소 인력에 조합에 대한 정보보호 최소인력이 추가로 산정해야 한다.

조합에 대한 정보보호 인력 산정방식은 상업은행의 보안인력 산정방식과 마찬가지로 조합의 총 임직원수를 감안하되 조합의 IT인력은 없으므로 총 임직원 수의 0.25%를 계산 한 후 업무분담 인력비율을 차감하여 산정함이 적정한 것으로 판단된다.

이를 조합 총 임직원수로 계산했을 때 정보보호 업무에 필요한 최소인력 기준과 과부족 인력은 Table 8과 같다.

**표 6. 협동조합 형 금융회사의 최소 정보보호인력**
Table 6. Minimum Security Staff of Financial institution operated by cooperatives
**(* 신협통계 및 농협중앙회 내부자료, ** 각 협동조합형 금융회사 내부자료)**

| | 농협 | 신협 | 수협 | 새마을금고 | 산림조합 |
|---|---|---|---|---|---|
| 조합 총 임직원 수ⓐ (단위:천명) | 63 | 10 | 7 | 30 | 2 |
| ⓑ=ⓐ× 0.0025 | 158 | 25 | 18 | 75 | 5 |
| 정보보호 인력ⓒ * | - | 9 | - | 25 | 3 |
| 과부족 | ▲158 | ▲16 | ▲18 | ▲50 | ▲2 |

위에서 조사된 결과를 보면 일부 금융회사의 중앙회는 조합만을 위한 정보보호인력은 없거나(농협중앙회, 수협중앙회), 상업은행의 절반 이하 수준으로 정보보호 인력이 운영됨을 알 수 있다.(신협, 새마을금고, 산림조합)

또한 중앙회 또는 중앙회의 계열사가 자체사업을 가지고 있으면서 IT 및 정보보호 업무를 수행하는 농협중앙회·수협중앙회의 경우에는 정보보호 업무 분담율에 해당하는 정보보호 인력은 인정해 주어야 하는데, 이는 금융회사 정보기술(IT)부문 보호업무 이행지침에서 전산자회사의 경우에는 전산자회사의 재하청인력을 제외하고 운영비용 분담율에 해당하는 인력을 정보보호 인력으로 인정하고 있다.

### 다. 정보보호 인력산정 비율 개선

2013년 전자금융감독 규정 개정 당시 정보보안에 대한 미비한 투자가 일련의 정보보안 사고의 원인으로 제기되었고, 그에 따라 감독당국은 해외 수준으로 단기간에 높여야 하는 필요성이 제기되었다. 이에 따라 당시 해외 금융회사의 평균 보안투자 수준이 국내 최소기준으로 설정하게 되었으며, 현 시점에도 보안분야에 대한 투자는 해외 추이를 따라가는 상황이 계속되고 있다.

앞서 현황에서 살펴본 바와 같이 정보보호 인력에 대한 글로벌 투자 추세는 2012년 말 IT인력대비 보안인력은 평균 비율은 4.1%이며, 한국은행 자료에 의한 2012년 국내 155개 금융회사도 평균 5.4%였다. 이후 정보보호에 대한 중요성이 인식되면서 2014년 말에는 글로벌 평균 7.7%, 국내 평균은 8.4%까지 높아졌다. 따라서 2013년 전자금융감독규정 개정 시 기준으로 삼은 2012년 말 기준보다 3% 이상 높아졌음을 알 수 있다.

따라서 현재 시점에서 전자금융감독규정 제정당시와 같은 논리로서 정보보안의 최소 인력비율을 산정한다면 2014년말 글로벌 평균 비율인 7.7%를 감안하여 8%로 설정 하는 것이 합리적이라 생각된다.

### 2. 예산 측면

정보보호 예산은 2011년 6월 금융감독원 "금융회사 IT보안강화 종합대책"을 마련하면서 IT 보안예산 비율을 5% 이상 유지토록 권고하고 있다고 밝히고 있었으며, 당시 2010년말 은행권은 정보보안 예산비중은 3.4%(금융권 전체로는 3.2%)였다[6], 따라서 당시 규제기관의 의도는 글로벌 평균인 4.6% 수준까지 IT보안 예산비율을 올리려 했던 것으로 파악된다.

2014년말 글로벌 IT보안분야에 대한 투자는 전체 IT투자액의 6.1%로 조사되었고, 특히 금융분야의 경우는 9.6%이다. 또한 한국은행 자료에 따르면 국내 금융회사의 경우는 이보다 더 높은 10.3%의 비중을 차지하고 있다.

현재 시점에서는 정보보호 인력산정 비율 때 고려했던 방법과 마찬가지로 2014년 말 금융분야의 글로벌 IT투자 기준인 9%로 설정하는 것이 합리적이라 생각되며, 실제로 금융감독원은 2011년 6월 "금융IT보안강화 종합대책" 에 의해 IT 보안인력 비율을 일정 수준 이상 유지토록 의무화 하고, 구체적인 비율 수준은 총 자산규모, 직원 수, 전자금융거래규모, 고객 수, 국제기준 등을 감안하여 결정하되, Road Map에 따라 단계적으로 높여나갈 예정이라고 밝힌 바 있다[7].

### 3. 자산규모에 따른 보안 기준 차등화

대규모 조합과 소규모 조합 간 규모의 격차로 인해 정보보호 측면에서 위험의 차이가 있을 수 밖에 없음에도, 규제기준이 일률적으로 적용됨으로써 과소 또는 과대 규제감독으로 인한 문제가 일어날 수 있다. 이러한 문제를 감소시키기 위해서는 자산규모에 따라 통제범위나 보안 기준 등을 차등화 하여 적용할 필요가 있어 보인다. 그러나 감독당국의 수많은 개별 조합에 대한 감독기능에는 한계가 있으므로, 법제 개정을 통해서 개선하기 보다는 협동조합형 금융회사의 중앙회가 중간·자율 감독기구로서의 조합에 대한 사전적 정보보호 감독 기능을 수행함으로써 개별 조합들에 대한 상시적인 내부통제·취약점 점검, 보안 교육 등이 실행됨이 바람직하다.

## Ⅳ. 결 론

보안사고는 현재까지 연구되어 온 다양한 방식의 인력보안 기준과 투자에도 불구하고 지속적으로 증가하고 있다. 특히 본 논문에서는 금융회사 중 협동조합형 금융회사의 중앙회가 가지는 특성을 감안하여 정보보호 인력 및 예산의 적정성을 검토하였다.

협동조합형 금융회사는 본문에서 지적한 '조직 내부통제의 한계', '조합들간 규모의 양극화로 인해 일률적인 기준의 적용이 어려움', '다수 규제기관의 관여' 와 같은

이유로 시중은행이 가진 정보보호 리스크 외에도 고려해야 할 사항이 있음에도 불구하고, 현행 전자금융거래법 하위규정인 전자금융감독규정이 모든 금융회사의 환경을 고려할 수 없다는 점에 있어 협동조합형 금융회사의 중앙회가 최소한의 IT보안인력 보유하도록 규제하는데 다소 부족한 부분이 있었던 것으로 생각된다.

그러므로 본 논문에서는 협동조합형 금융기관의 특성을 반영하여, 전자금융감독규정에서 정하고 있는 정보보호 인력 및 예산을 다음과 같이 개선할 것을 제안한다.

첫째, 협동조합형 금융회사의 중앙회는 자체사업을 위한 정보보호인력 외 개별조합의 정보보호를 위한 인력을 별도로 구성해야 하며, 그 인력은 조합의 총 임직원수를 감안하여 0.25%를 계산 한 후 업무분담 인력비율을 차감하여 산정해야 한다.

둘째, 정보보호 인력 및 예산비율은 협동조합형 금융회사의 중앙회도 최근 국·내외 관련업체 평균을 감안하여 인력비율은 8%까지, 예산비율은 9%까지 높여야 하며, 이는 중앙회 뿐만 아니라 상업은행과 동일한 기준으로 봐야 하므로 금융회사 전체적으로 적용될 수 있도록 전자금융감독규정 일반의 개정이 필요하다.

셋째, 규제기관은 전국에 산재해 있는 수많은 조합을 직접 감독하는 방식은 효율적이지 못하므로 중앙회가 내부통제·취약점 점검 등 기능을 할 수 있도록 중간 감독기구의 역할을 수행할 수 있도록 해야 한다.

## References

[1] Credit Union Research Laboratory, “2014 Credit Union Statistics”, http://research.cu.kr, pp. 97-98, Jun. 2015.

[2] Chung-Ok Koo, “Risk Profile of Cooperative Financial Institution and Its Supervisory Implications”, Korean Society for Cooperative Studies vol. 30. no. 3, pp 133-142, Dec. 2012.

[3] The Financial Supervisory Service Press Release, “Parliamentary Inspection of the Administration 2014”, http://tfnews.co.kr/news/article.html?no=3621, Jun. 2014.

[4] Gartner, “IT Key Metrics Data 2015: Key IT Security Measures: Multiyear”, http://www.gartner.com/document/2935417?ref=solrAll&refval=165027587&qid=088dcc4d6e4b936c015f1c2aa7379ef6, Dec. 2014

[5] The Bank of Korea, “2014 Current State of Financial Informatization”, July, 2015.

[6] Seong-Heon Lee, “Parliamentary Inspection of the Administration 2010”, ETNEWS, www.etnews.com/201104140136, 14. Apr. 2011

[7] The Financial Supervisory Service Press Release, “Comprehensive Measures of Financial Institution IT Security Policy”, 23 June. 2011

[8] Chung-Ok Koo, “Risk Profile of Cooperative financial Institution and Its Supervisory Implications”, Feb. 2012

[9] Ha-Gyeong Bang. “A study of security personnel managements and adequacy by state-owned company”, Jun. 2011

[10] The Financial Supervisory Service Press Release, “Open the Mutual Finance Policy Council”, 18. Jan. 2013

[11] The Financial Services Commission “Regulation on Supervision of Electronic Financial Transactions”, Revison 2015-18, 24. Jun. 2015

[12] Financial Statstics Information System, “Monthly Financial Statistics Bulletin”, http://fisis.fss.or.kr/fss/fsi/id/fssview04.jsp, Dec. 2014

[13] MG Korean Federation of Community Credit Cooperatives, “The Statistics of Community Credit Cooperative”, 31. Dec. 2014

[14] Kyung-Hee Han, In-Seok Kim, “A Study on Threat Analysis of PC Security and Countermeasures in Financial Sector”, The Journal of The Institute of Internet, Broadcasting and Communication(JIIBC), VOL .15, No. 6, pp. 238-290, Dec. 31. 2015,

## 저자 소개


### 임 정 환(정회원)

- 2000년 원광대학교 전자공학과(공학사)
- 2015년 3월~현재 : 고려대학교 정보보호대학원 금융보안학과 석사과정

<주관심분야 : 전자금융보안, 보안정책, 전자금융법규 등>

### 김 인 석(정회원)

- 2008년 고려대학교 정보경영공학과 박사
- 2009년 ~ 현재 : 고려대학교 정보보호대학원 교수
- 現 FDS산업포럼 회장, 한국사이버정보전학회 운영위원 등

<주관심분야 : 전자금융보안, IT감사, 전자금융법규 등>