미국 IT감사통제 분야의 최근 연구동향 - ISACA를 중심으로

권호열

강원대학교 컴퓨터학부

New Trends in IS Audit and Control Researches of ISACA

Kwon, Ho Yeol

Dept. of Computer Science and Engineering

Kangwon National University

E-mail : hykwon@kangwon.ac.kr

요 약

IT서비스의 품질을 보장하기 위한 IT감사통제의 최근 연구동향을 소개한다. 이를 위하여 IT감사통제 분야에서 전세계적으로 가장 큰 네트워크를 형성하고 있으며 이 분야를 실질적으로 이끌고 있는 미국 ISACA의 최근 10 년간 주요 출판물을 분석하였다. 그리고 정보시스템 감사통제 분야의 현안들과 현안의 해결을 위한 노력에 대하여 분석하고, 향후 발전방향에 대한 시사점을 도출하였다.

1. 서론

정보시스템이 복잡화, 대규모화하면서 이러한 정보시스템 품질을 심사하여 문제점을 식별하고 해결방안을 권고하는 전문가에 대한 요구가 크게 증가하고 있다. 이에 따라 기술사 뿐 만 아니라 정보시스템감사사(CISA), 정보시스템감리사, 전보보안전문가(CISSP), 정보보호전문자격(SIS) 등 다양한 전문자격제도가 출현하여 운영되고 있다.[1-4] 이들 가운데 CISA 자격은 1978년에 시작된 후 지금까지 전 세계 160개국에서 86,000 명의 자격자를 배출하였으며, 미국 국방성에서도 정보보증(IA) 전문가로 인정받는 자격이다. 또한 CISA 자격은 최근 보안관리자(CISM), 거버넌스전문가(CGEIT) 등의 자격제도로 분화하는 등 발전을 거듭하고 있다.

본 연구에서는 IT서비스의 품질을 보장하기 위한 IT감사통제의 최근 연구동향을 소개한다. 이를 위하여 IT감사통제 분야에서 전세계적으로 가장 큰 네트워크를 형성하고 있으며 이 분야를 실질적으로 이끌고 있는 미국 ISACA의 최근 10 년간 주요 출판물을 분석하여. 감사통제 분야의 현안들과 이러한 현안의 해결을 위한 노력에 대하여 분석하고, 향후 정보시스템감리의 발전방향에 대한 시사점을 도출하였다.

2. 본론

2.1 감사통제 현안 추세의 분석

정보시스템 감사통제 현안 추세를 분석하기 위하여 사용한 자료는 정보시스템 감사통제 분야의 현황을 시기적절하게 반영하는 것으로 알려진 ISACA Journal 의 특집 기사로서, 최근 10 년간 (2000.1-2009. 10) 출판된 총 434 편의 기사이다.[7]

본 연구에서는 이러한 특집기사를 ISACA의 표준화된 지식범주인 6 개의 CISA 도메인(표 2 참조)으로 분류하여 시간의 경과에 따른 도메인별 비중의 변화와 주요 변화에 대한 시사점을 도출하였다. 표 1 은 ISACA Journal 특집기사의 CISA 도

메인별 분포이며, 각 도메인별 현안의 상대적인 변동은 그림 1 과 같다.

년도	CISA 도메인						소계
	1	2	3	4	5	6	
2000	2	10	14	2	7	0	35
2001	1	3	22	3	16	0	45
2002	6	7	7	2	16	1	39
2003	8	15	9	3	15	2	52
2004	7	15	12	0	18	0	52
2005	3	18	7	1	9	1	39
2006	12	18	3	2	9	0	44
2007	5	19	10	0	10	3	47
2008	12	18	11	1	4	0	46
2009	6	17	6	0	6	0	35
합계 (백분율)	62 (14.3)	140 (32.3)	101 (23.3)	14 (3.2)	110 (25.3)	7 (1.6)	434 (100.0)

표 1. ISACA Journal 특집기사의 CISA도메인별 분포

2.2 ISACA의 현안 대응과 시사점

감사통제의 도메인별 현안의 변동과 ISACA의 대응으로부터 다음과 같은 시사점을 얻는다.

- 2001년 911 테러 직후 재해 상황에서도 기업활동이 지속될 수 있도록 보장하는 비즈니스 연속성과 재해복구에 대한 관심이 증가하였다.

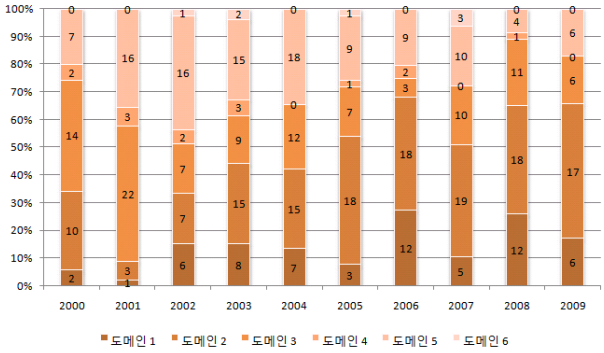

그림 1. CISA 도메인별 현안의 상대적 변동 추세

- 6 개의 CISA 도메인 중 최근 들어 가장 많은 관심을 모은 도메인 2 (IT거버넌스, 32.3%)와 도메인 5 (정보자산의 보호, 25.3%) 는 보다 높은 전문성을 위하여 각각 거버넌스전문가(CGEIT) 및 보안관리자(CISM)로 분화 독립하였다. 표 2 는 CISA, CGEIT, CISM과 함께 정보시스템감리사, 보안전문가(SIS) 및 CISSP 등의 응시자격과 전문지식 도메인을 비교한 것이다.
- 세번째로 비중있게 다루어진 도메인 3 (시스템 및 인프라 수명주기 관리, 23.3%)은 감사통제 전

전문자격 (발행처)		CISA (ISACA)	CGEIT (ISACA)	CISM (ISACA)	정보시스템감리사 (NIA)	SIS (1급) (KISA)	CISSP ((ISC)^2)
응시자격		- 5년 이상 IS 감사,통제,보증 또는 보안 경력자	- 5년 이상 IT거버넌스 자문, 감독, 지원 경험자	- 5년 이상 정보보안 경력자	- 학사학위자로 정보처리실무경력 9년 이상인 자	- 4년제 대학졸업(예정)자로 정보보호과목 12학점이상 이수자	- 5년 이상 보안전문가 경력자
CISA 도메인	1	• IS 감사 프로세스 (10)			• 감리		
	2	• IT 거버넌스(15)	• IT 거버넌스 프레임워크(25) • 전략적 연계(15) • 성과 측정(12)	• 정보보안 거버넌스(23)			• 정보보안 거버넌스 및 위험관리
	3	• 시스템 및 인프라 수명주기 관리(16)	• 자원 관리(13)	• 정보보안 프로그램 개발(17)	• S/W 공학 • 사업관리 • 데이터베이스		• 응용개발 보안
	4	• IT 서비스 제공 및 지원(14)	• 가치 인도(15)	• 정보보안 프로그램 관리(24)	• 시스템 구조		• 보안 아키텍처 및 설계 • 운영 보안
	5	• 정보 자산의 보호 (31)	• 위험 관리(20)	• 정보위험성 관리 (22)	• 보안	• 시스템 보안 • 네트워크 보안 • 어플리케이션 보안 • 정보보호론	• 접근 통제 • 암호학 • 법률,규정,조사 및 적합성 • 물리(환경) 보안 • 통신네트워크 보안
	6	• 비즈니스 연속성 및 재해복구(14)		• 사고관리 및 대응 (14)			• 비즈니스 연속성 및 재해 복구

표 2. 정보시스템감사통제 관련 전문자격의 비교

문가들이 감사기법만 아니라 감사의 대상이 되는 기술의 흐름과 변화에 대하여 매우 민감하게 반응하고 있다는 것을 알 수 있다.

- 또한 정보시스템의 도입과 구축, 운영 측면에서 강조되던 IT거버넌스를 IT의 가치와 기업경영에 보다 밀접하게 연계시킬 필요성이 제기됨에 따라 Val-IT가 새로 제안되어 발전하고 있다.

3. 결론

본 연구에서는 IT서비스의 품질을 보장하기 위한 IT감사통제의 최근 연구동향을 소개하였다. ISACA의 성공적인 경험을 국내의 정보시스템 감리에 적용하면 다음과 같은 시사점이 얻어진다.

첫째, 정보시스템감리의 발전을 위해 감리대상인 사회적 수요 및 IT서비스 산업의 요구변화를 반영하여 감리 지식체계를 지속적으로 재조직 및 개선하는 구조가 필요하다. 둘째, 신기술 출현 또는 국가/사회적 현안 발생에 의하여 특정 영역의 감리 지식에 대한 수요가 장기적으로 크게 증가할 것이 예상되는 경우 보다 전문화된 자격제도의 도입을 고려할 수 있다.

[참고문헌]

[1] CISA® 시험 및 자격증에 대한 응시자 안내서, ISACA, 2009.

[2] 2009년도 정보시스템 감리사 자격검정 안내, 한국정보화진흥원, 2009. 5.

[3] CISSP for Professionals, $(ISC)^2$, 2009.

[4] 2009년도 정보보호전문가(SIS) 자격검정, 한국인터넷진흥원, https://www.kisa.or.kr/, 2009.

[5] CISM® 시험 및 자격증에 대한 응시자 안내서, ISACA, 2009.

[6] Candidate's Guide to the CGEIT™ Exam and Certification, ISACA, 2009.

[7] ISACA Journal, ISACA, 2000. - 2009.