情 報 保 護 學 會 誌
第20卷 第5號, 2010. 10

국내·외 정보보호 수준 평가 체계 및 지표 동향

이 동 희*, 여 돈 구*, 염 흥 열**

요 약

인터넷의 발달로 해킹과 같은 각종 보안위협이 증가하고 있으며 이는 국가, 기업 그리고 개인에게 심각한 위협이 되고 있다. 해킹으로 인해 유/무형적인 손실을 받을 수 있기 때문에 보안 위협에 대한 적절한 보안 대책의 수립이 필요하며, 또한 수립된 보안 대책 및 대상의 보안 수준을 확인하기 위한 다양한 정보보호 체계 및 평가 지표들이 존재하고 있다, 본 논문에서는 국내/외에서 개발된 정보보호 평가 체계와 지표, 그리고 국제 표준과 진행 동향을 살펴보고, 각 체계간의 차이점을 도출한다.

Ⅰ. 서 론

기업의 자산에 대한 기밀성, 무결성, 가용성을 실현하는 일련의 프로세스 및 활동을 일컫는 정보보호 관리체계는 조직의 자산에 대한 안전성 및 신뢰성을 향상시키고, 정보보호운영을 체계적이고 지속적으로 유지하기 위하여, "정보보호정책 수립", "정보보호관리체계 범위 설정", "위험관리", "구현", "사후관리"의 5단계를 거쳐 운영된다[1].

인터넷과 같은 정보기술의 급속한 발달을 통하여 오프라인을 통해서만 가능했던 일들을 온라인을 통하여 가능하도록 해주어 편리함을 주었지만, 이와 함께 해킹이나 바이러스 등 각종 보안위협 또한 증가하게 되었다. 기업이나 조직은 이러한 보안위협에 보다 정확하고 신속하게 대응하기 위하여 산발적인 보안 관리체계에서 종합적이고 체계적인 보안 관리체계로 변화하고 있다.

이러한 상황에서 기업과 조직의 취약점을 분석하고 평가하는 다양한 지표들이 국내/외로 개발되게 되었고, 많은 수의 기업과 조직이 자산을 관리하는 인증을 받아오고 있다.

본 논문의 2장과 3장에서는 국내/외 정보보호 관련 지표에 대하여 살펴보고, 4장에서는 정보보호 관련 국제 표준을 알아본다. 그리고 5장에서는 현재 정보보호 관련 지표들의 개선 방향을 살펴보고, 6장에서 정보보호 관련 지표들에 대한 비교를 하고, 7장에서 결론을 맺는다.

Ⅱ. 국내 정보보호 관련 평가 체계 및 지표

국내 정보보호 관련 평가 체계 및 지표는 [표 1]과 같이 정부에서 시행하는 체계 및 지표와 민간에서 시행하는 지표로 나눌 수 있다. 정부에서 운영 중인 정보보호 관련 평가 체계 및 지표는 국가정보원, 방송통신위원회, 행정안전부 주관으로 개발되었으며, 민간에 운영 중인 정보보호 관련 평가 지표는 한국정보통신산업협회의 주관으로 시행 중에 있다.

2.1 정부주도 평가 체계 및 지표

정부에서 주도적으로 시행하는 관리 체계 및 평가 지표로는 국가정보원/방송통신위원회의 국가정보보호지수[2], 국가정보원의 정보보안 관리수준 평가[3], 방송통신위원회의 정보보호 안전진단[4,5]과 K-ISMS(*KISA-Information Security Management System*)[6]을 시행하고 있으며, 행정안전부의 전자정부서비스 보안수준 실태조사[7], G-ISMS(*Government-Information Security Mana-*

본 연구는 방송통신정책연구용역사업의 연구결과로 수행되었습니다. (NIPA-2010-(1001-0035))
* 순천향대학교 정보보호학과 석사과정 (leemeca, h7ei@sch.ac.kr)
** 순천향대학교 정보보호학과 교수 (hyyoum@sch.ac.kr)

〔표 1〕 국내 정보보호 관련 체계 및 평가 지표

분류	기관	평가 지표 이름	지표 설명	
정부	국가정보원/방송통신위원회	국가정보보호 지수	목적	정부와 기업, 개인 등 부문별 정보보호 수준을 종합적으로 측정하기 위하여 도입
			대상	정부, 기업, 개인
			법률	-
			지표	2개 구분 3개 분류 12개 세부지표
	국가정보원	정보보안 관리수준 평가	목적	주요 전산망에 대한 사이버안전 역량 제고 및 정보보안 관리수준 평가하기 위하여 도입
			대상	중앙행정부처, 광역자치단체, 주요 공공기관
			법률	국가사이버안전관리 규정
			지표	9개 분야 246개 항목
	방송통신위원회	K-ISMS	목적	정보보호관리 절차와 과정을 체계적으로 수집하고 지속적으로 관리·운영하기 위하여 도입
			대상	기업
			법률	정보통신망 이용촉진 및 정보보호 등에 관한 법률, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령, 정보보호관리체계인증 등에 관한 고시
			지표	15개 분야 120개 통제사항 396개 세부통제사항
		정보보호 안전진단	목적	정보통신서비스제공자의 정보통신망의 안정성·신뢰성을 제고하기 위하여 도입
			대상	정보통신서비스제공자(ISP), 집적정보통신시설사업자(IDC) 및 쇼핑몰 등
			법률	정보통신망 이용촉진 및 정보보호 등에 관한 법률
			지표	3개 구분 11개 분야 48개 세부조치 102개 체크리스트
		PIMS	목적	개인정보와 연관성 및 관리체계의 지속적 관리를 고려하여 도입
			대상	기업
			법률	정보통신망 이용촉진 및 정보보호 등에 관한 법률
			지표	3개 분야 119개 통제 사항 325개 세부통제사항
	행정안전부	전자정부서비스 보안수준 실태조사	목적	전자정부서비스를 제공하는 기관들의 보안수준 향상을 위하여 도입
			대상	중앙행정 및 지방해정 기관의 전자정부서비스 및 주요 행정정보 서비스
			법률	전자정부법
			지표	3개 분야 12개 부문 42개 실행대상 77개 세부실행과제
		G-ISMS	목적	행정기관의 정보보호 관리수준을 보다 객관적이고 체계적으로 점검·관리하기 위하여 도입
			대상	전자정부서비스를 제공하는 행정기관
			법률	행정안전부 훈령 164호(전자정부법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 전자정부법 시행령, 행정안전부와 그 소속기관 직제)
			지표	12개 분야 44개 통제사항 145개 세부통제사항
		공공기관 개인정보보호수준 진단	목적	공공기관의 개인정보관리 수준을 개선하기 위하여 도입
			대상	중앙행정기관, 지방자치단체
			법률	공공기관의 개인정보보호에 관한 법률, 시행령, 시행규칙
			지표	3개 구분 8개 상위지표 18개 지표 75개 항목
	정보통신산업진흥원	eTRUST	목적	인터넷 거래에 대한 소비자의 신뢰성 확보 및 안전한 전자상거래 환경 구축 도모
			대상	상업적 웹 사이트
			법률	전자거래기본법 제18조
			지표	7개 심사영역 31개 평가군 112개 평가항목
민간	한국정보통신산업협회 (정보보호마크위원회)	ePrivacy	목적	개인정보보호 정책 및 관리수준을 평가를 위하여 도입
			대상	인터넷사이트를 통하여 개인정보를 수집, 취급, 관리하는 국내 사업자 및 일반인(단체)
			법률	-
			지표	7개 분야 59개 항목 (필수 17개 항목)
		i-Safe	목적	개인정보보호, 시스템 보안, 소비자 보호에 대한 평가를 위하여 도입
			대상	인터넷사이트를 통하여 개인정보를 수집, 취급, 관리하는 국내 사업자 및 일반인(단체)
			법률	-
			지표	3개 구분 10개 분야 224개 항목 (필수 79개 항목)

gement System)[8] 그리고 공공기관 개인정보보호수준 진단[9]이 있다. 그리고 지식경제부 산하 정보통신산업진흥원에서 eTRUST[10]를 시행하고 있다. 또한 방송통신위원회는 2010년 9월 PIMS(Personal Information Management System)[11,12]의 도입 방안 마련을 추진 중에 있다.

상기 체계 및 평가 지표의 적용 대상은 크게 공공/행정기관, 일반 기업 등으로 나누어볼 수 있다. 공공/행정기관을 대상으로 하는 체계 및 평가 지표는 정보보안 관리수준 평가, G-ISMS, 공공기관 개인정보보호수준 진단이 있고, 기업을 대상으로 하는 체계 및 평가 체계 및 지표는 K-ISMS, 정보보호 안전진단이 있다. 반면, 국가정보보호지수의 경우는 보통의 지표들과는 다르게 공공/행정기관, 기업과 같이 특정한 대상으로 정보보호 평가를 하는 것이 아니라 국가 전반의 정보보호수준을 평가하는 특징이 있다.

[그림 1]의 K-ISMS 평가 항목과 [그림 2]의 G-ISMS 평가 항목은 ISO/IEC 27001[13](4장 국제 표준 참조)의 평가 항목을 바탕으로 국내의 실정에 맞도록 개선하였으므로, 두 평가 지표의 평가 항목이 다소 유사하나 K-ISMS는 일반 기업을 대상으로 하며 인증을 받고자 하는 업체가 자율적으로 신청하면 되고, G-ISMS는 행정/공공기관을 대상으로 하며 전자정부 서비스를 제공하고 있는 2010년에 30개의 정부 기관은 의무적으로 이 인증을 받아야 한다는 점에서 차이가 있다.

좀 더 자세히 살펴보면, K-ISMS는 국내 상황에 맞게 침해사고 예방, 암호화, 전자거래 항목 등을 추가하였고, G-ISMS는 암호화와 개인정보보호 항목을 추가하여 기존의 통제사항과 세부통제 항목보다 그 수가 증가하게 되었다.

G-ISMS 외에도 의무적으로 시행해야 하는 지표로는 정보보안 관리수준 평가, 전자정부서비스 보안수준 실태조사, 정보보호 안전진단, 공공기관 개인정보보호수준 진단이 있으며, 정보보호 안전진단은 안전진단대상자로 선정이 되면 의무적으로 시행해야 한다.

정보보안 관리수준 평가와 전자정부서비스 보안수준 실태조사는 평가 대상의 정보통신 시설에 대한 의존도에 따라 등급을 분류하여 등급에 따라 다른 평가 기준을 적용한다. 정보보안 관리수준 평가의 등급 분류 기준은 수행업무의 중요도, 정보시스템 및 정보 중요도, 피해분석으로 나누어지고, 평가 요소는 [그림 3]과 같다.

NO	통제내용	통제사항	세부 통제사항
1	정보보호정책	5	10
2	정보보호조직	4	11
3	외부자 보안	4	8
4	정보자산 분류	4	7
5	정보보호 교육 및 훈련	4	14
6	인적 보안	5	18
7	물리적 보안	12	36
8	시스템개발 보안	13	53
9	암호통제	3	6
10	접근통제	14	38
11	운영관리	22	99
12	전자거래보안	5	21
13	보안사고관리	7	20
14	검토, 모니터링 및 감사	11	37
15	업무 연속성 관리	7	18
	계	120	396

〔그림 1〕 K-ISMS 정보보호 대책

NO	통제분야	통제사항	세부 통제사항
1	정보보호 정책	1	2
2	정보보호 조직	1	8
3	자산관리	2	5
4	인적 보안	4	12
5	물리적 보안	2	13
6	통신 및 운영관리	10	32
7	접근통제	7	24
8	정보시스템 요구사항, 개발 및 유지보수	6	16
9	보안사고 관리	2	5
10	업무 연속성 관리	1	5
11	준거성	3	8
12	개인정보보호	5	25
	계	44	145

〔그림 2〕 G-ISMS 정보보호 대책

기관분류 기준	평가요소
수행업무의 중요도	수행업무의 국가사회적 중요도
	인원 및 서버 규모
정보시스템 및 정보중요도	정보중요도
	정보시스템 의존도
	대외업무연계 정도
피해분석	위협발생 가능성
	피해영향 정도

〔그림 3〕 정보보안 관리수준 평가 분류 기준

NO	대분류	중분류	소분류	A항목	B항목	C항목
1	정책 및 조직	2	3	10	1	1
2	계획 및 감사	2	3	5	5	0
3	정보자산 분류 및 관리	4	9	19	8	2
4	인적 보안	3	6	15	6	1
5	물리적 보안	3	8	14	2	8
6	접근 보안	5	14	48	8	9
7	운영관리	6	11	40	9	7
8	사이버 침해 사고 대응	2	5	11	5	1
9	국가용 보안시스템	3	5	11	0	0
	계	30	64	173	44	29

〔그림 4〕 정보보안 관리수준 평가

기관분류 기준	평가요소
서비스의 국가·사회적 중요도	국가단위 핵심 행정/전 국민 데이터 보유 업무
	국가단위 핵심 행정/다수 국민 데이터 보유 업무
	국민 행정/다수 국민 데이터 보유 업무
	광역 자치/규모 행정 국민 데이터 보유 업무
	기타 대 국민 생활 관련
서비스 사고 발생시 피해 영향도	전 국민 생활에 피해
	대도시 지역 주민생활에 피해
	중·소도시 지역 주민생활에 피해
	소규모 지역 주민 생활에 피해
	소규모 지역 주민 생활에 피해
수행 서비스의 온라인 의존도	전자정부서비스 접속 건수 1만건 이상
	전자정부서비스 접속 건수 5000 ~ 9999건 이하
	전자정부서비스 접속 건수 2000 ~ 4999건 이하
	전자정부서비스 접속 건수 1000 ~ 1999건 이하
	전자정부서비스 접속 건수 999건 이하

〔그림 5〕 전자정부서비스 보안수준 분류 기준

NO	부문	실행대상	항목	필수	권고	선택
1	관리적 보안	4	7	3	1	3
2	제도적 보안	4	5	2	3	0
3	인적 보안	4	5	2	1	2
4	사용자 PC 보안	2	8	5	2	1
5	네트워크 보안	5	7	4	2	1
6	서버 보안	2	4	2	2	0
7	DB 보안	1	2	1	1	0
8	어플리케이션 보안	5	11	5	4	2
9	가용성	1	4	2	2	0
10	사후관리	2	4	1	2	1
11	온라인 거래 서비스 보안	6	10	10	0	0
12	증명서 서비스 보안	6	10	10	0	0
	계	42	77	43	24	10

〔그림 6〕 전자정부서비스 보안수준 평가

이 기준을 통해 기관을 가급, 나급, 다급으로 분류한 후, [그림 4]의 기준에 따라 가급은 A/B/C 항목 246개를 모두 적용하고, 나급은 A/B 항목 217개, 다급은 A 항목 173개만을 적용한다.

전자정부서비스 보안수준 실태조사의 등급 분류 기준은 제공하는 서비스의 국가·사회적 중요도, 서비스 사고 발생 시 피해 영향도, 수행서비스의 온라인 의존도로 나누며, 평가 요소는 [그림 5]와 같다. 이 기준을 통해 전자정부서비스별 보안등급을 분류하고, [그림 6]과 같이 보안 등급별로 1등급은 필수/권고/선택 77개, 2등급 필수/권고/선택일부 72개, 3등급은 필수/권고 67개, 4등급은 필수/권고일부 52개, 5등급은 필수 43개에 대해 관리적·기술적 보안기준을 적용한다.

정부를 대상으로 하는 평가 지표들이 평가 대상의 전반적인 정보보호 수준을 평가하는 것과 달리 공공기관 개인정보보호수준 진단은 평가 대상의 개인정보보호 부분만을 평가한다.

개인정보보호수준 진단은 행정기관과 지방자치단체를 대상으로 개인정보 보호수준을 진단하여 개인정보관

NO	분야		진단지표	항목
1	개인정보보호 정책환경	정책기반	4	13
		기술기반	3	14
2	개인정보 처리	수집 및 보유	4	16
		이용 및 제공	2	6
		파기	2	8
3	개인정보 침해대응	웹사이트 개인정보 노출방지대책	1	6
		개인정보유출 대응절차	1	4
		개인정보 침해구제 절차	1	4
	계		18	75

〔그림 7〕 공공기관 개인정보보호수준 진단

리 수준을 개선하기 위하여 도입한 것으로, 2단계로 평가가 진행된다. 1차에서는 각 대상이 자체적으로 평가를 진행하고, 2차에서 행정안전부가 별도로 구성한 진단전문위원회에서 1차에서 진단한 진단결과를 검증한다. 개인정보보호수준 진단의 평가 항목은 [그림 7]과 같다.

공공기관 개인정보보호수준 진단과 비슷한 지표로 민간 기업을 대상으로 하는 PIMS와 eTRUST가 있다.

PIMS에 대한 제도 도입이 2010년 8월 현재 준비 중이며, 2010년 8월에 PIMS 인증제 공청회가 열렸다. PIMS는 기업이 개인정보 보호 활동을 체계적이고 지속적으로 수행하기 위하여 개인정보보호 유관 법적 요구사항 및 전사적인 기술적·관리적 요구사항을 제시하고 있다. 현재 지표는 [그림 8]과 같이 공개되었다. 그리고 PIMS에는 [그림 9]와 같은 생명주기 준거 요구사항 영역이 존재한다. 이것은 개인정보의 수집부터 파기까

NO	도메인	통제사항	점검항목
1	개인정보보호대책	6	11
2	개인정보보호조직	5	9
3	개인정보 분류	4	7
4	교육 및 훈련	4	7
5	인적보안	3	9
6	침해사고 처리 및 대응절차	7	20
7	기술적 보호조치	36	125
8	물리적 보호조치	5	12
9	내부검토 및 감사	9	24
	계	79	224

〔그림 8〕 PIMS 보호 대책

NO	도메인	통제사항	점검항목
1	개인정보수집에 따른 조치	7	17
2	개인정보 이용 및 제공에 따른 조치	16	49
3	개인정보 관리 및 파기에 따른 조치	5	12
	계	28	78

〔그림 9〕 PIMS 생명주기 준거 요구사항

NO	심사영역	평가군	평가항목
1	공통 부문	5	19
2	쇼핑몰 부문	4	10
3	중개 부문	4	11
4	서비스 부문	3	8
5	금융 부문	4	9
6	무역 부문	5	13
7	B2B 부문	6	11
	계	31	112

〔그림 10〕 eTRUST 심사 기준

지표	심사 기준	관련 기준	구성	
ePrivacy	개인정보보호	정보통신망법, 공공기관의 개인정보보호에 관한 법률, 개인정보보호지침, i-Safe 심사기준	7개 분야 59개 항목 (필수 17개 항목)	
i-Safe	개인정보보호	정보통신망법, 개인정보보호지침, i-Safe 소비자 보호 부분	7개 분야 36개 항목 (필수 15개 항목)	
	시스템 보안	개인정보의 기술적·관리적 보호조치 기준, i-Safe 소비자 보호 부분	A그룹 3개 분야 73개 항목 (필수 58개 항목)	
			B그룹 3개 분야 66개 항목 (필수 39개 항목)	
	소비자 보호	전자상거래 소비자보호지침, i-Safe 소비자보호 부분	필수 6개 항목	A그룹 115개 항목
				B그룹 108개 항목

〔그림 11〕 ePrivacy, i-Safe 심사 기준

지의 절차에 대한 통제로, 개인정보 자체의 처리에 대한 조치를 점검한다. 이 영역은 ISO/IEC 27001과 K-ISMS에 존재하지 않는 영역으로 PIMS만의 가지는 특징이다.

ISO/IEC 27001과 K-ISMS, PIMS가 공통적으로 관리체계에 대한 지속적인 관리에 초점을 맞추고 있다. 하지만 개인정보보호에 대하여 지표를 살펴보면 ISO/IEC 27001과 K-ISMS는 개인정보와는 낮은 연관성을 가지고 있지만, PIMS는 높은 연관성을 가지고 있어 지속적인 관리가 가능하다.

eTRUST는 상업적 웹 사이트의 소비자·개인정보보호정책 및 전자상거래의 구매 전 과정에 걸친 안전성 평가를 수행한다. 평가 대상으로 종합 사이버몰, 전문 사이버몰, 직판 사이버몰, 서비스, 금융, B2B, 무역 등 8개 분야가 있고, 평가 기준은 [그림 10]과 같이 공통, 인터넷쇼핑몰, 서비스, 중개, 무역, 금융, B2B 부문으로 나누어 평가하고 있다.

2.2 민간분야 평가 체계 및 지표

민간에서 시행하는 정보보호 평가 지표로는 한국정보통신산업협회(KAIT) 산하 정보보호마크위원회[14]의 개인정보보호마크(ePrivacy)와 인터넷사이트 안전마크(i-Safe)가 있다. 개인정보보호마크와 인터넷사이트 안전마크는 행정/공공기관이나 일반 기업 모두 인증을 받을 수 있으며, 인증을 원하는 대상이 신청을 하면 심사를 받을 수 있다.

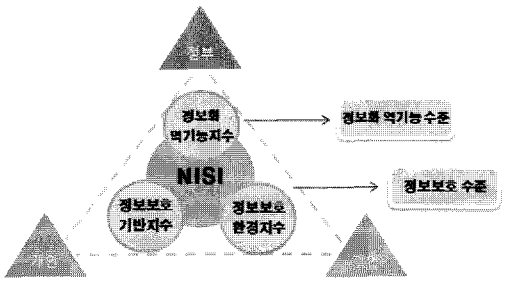
개인정보보호마크와 인터넷사이트 안전마크의 관련 기준과 지표 구성은 [그림 11]과 같다. 개인정보보호마크는 개인정보보호에 초점을 맞추어 평가를 진행하고, 인터넷사이트 안전마크는 개인정보보호 뿐만 아니라 사이트를 운영하는 시스템과 소비자 보호에 대한 부분까지 평가를 한다. 그리고 인터넷사이트 안전마크의 경우는 심사 대상을 금융, 의료부문과 기타 부분으로 나누어 다른 심사 항목을 적용함으로써 좀 더 특성화된 평가를 수행하는 특징이 있다.

2.3 국가정보보호지수

국가정보보호지수는 국가의 정보보호 수준을 측정하기 위하여 한국정보보호진흥원(KISA, 현 한국인터넷진흥원)에서 개발하였다. 국가정보보호지수는 [그림 12]과 같이 국가를 구성하는 정부, 개인, 기업 차원에서 정보보호 기반, 정보보호 환경부문을 평가함으로써 국가의 정보보호 수준을 평가하고 정보보호 활동에 대한 위협 및 침해사고 통계를 이용하여 정보화 역기능 수준을 측정한다.

국가정보보호지수는 [그림 13]과 같이 크게 정보보호 수준지수와 정보화 역기능 수준으로 나누어지며, 12개의 지표로 이루어져있다.

이 세부지표들은 계량화가 가능한 "정보보호 실태조사 및 분석", "한국 인터넷 백서", "정보화 통계집", "한



〔그림 12〕 국가정보보호지수 프레임워크

구분	분류	세부지표
정보보호수준	정보보호기반	백신 보급률
		패치 보급률
		PKI 보급률
		Firewall 보급률
		IDS 보급률
		보안서버 보급률
	정보보호환경	정보보호 예산 비율
		정보보호 전문인력 비율
		국민 보안의식 수준 비율
정보화 역기능수준	정보화 역기능	해킹 바이러스 신고 비율
		개인정보 침해 비율
		스팸 메일 수신 비율
계		12

〔그림 13〕 국가정보보호지수

국인터넷통계집", "국가 정보보호백서", "국내정보보호 산업 통계조사", "인터넷 침해사고 동향 및 분석월보" 등 지표들의 통계치를 기반으로 국가의 전반적인 정보보호수준을 평가한다.

Ⅲ. 국외 정보보호 관련 체계 및 지표

국외 정보보호 관련 지표에서는 [표 2]와 같이 미국의 NIST(*National Institute of Standards and Technology*)와 영국의 Infosecurity Europ과 PWC(*Price Waterhouse Coopers*), 대만의 정보산업연구소(*Institute for Information Industry*)에서 시행하는 지표를 살펴본다.

3.1 미국

미국은 NIST 산하 CSRC(*Computer Security Resource Center*)에서 정보보호와 관련된 개발 및 연구를 진행하고 있다. CSRC에서는 연방정부기관에서 사용하는 정보 처리 방식을 표준화한 FIPS(*Federal Information Processing Standards*)와 다양한 분야의 정보보호 가이드라인을 제공하는 SP(*Special Publications*) 800 시리즈를 발간하고 있다[15].

CSRC에 공개된 SP 800 시리즈는 총 110개(취소된 문서 46개 미포함)로 모든 SP 800 시리즈를 논문에 언급할 수 없기 때문에 이 논문에서는 정보보호 평가와 관련있는 SP 800-53 A(*Guide for Assessing the Security Controls in Federal Information Systems*)[16]와 SP 800-55 rev.1(*Performance Measurement Guide for Information Security*)[17]만을 언급한다.

SP 800-53 A는 SP 800-53(*Recommended Security Controls for Federal Information Systems*)[18]의 보안통제와 FIPS 199(*Standards for Security Categorization of Federal Information and Information Systems*)[19]의 영향 수준(Impact Level)을 통합한 것으로 정보시스템 보안통제 평가지침서이다. 이 평가지침서는 다양한 조직에서 적용이 가능하며, 정보시스템이 보다 안전하도록 하기 위해 지속적이고, 비교가 가능하도록 구성되어 있다[20].

〔표 2〕 국외 정보보호 관련 평가 체계 및 지표

분류	기관	평가 지표 이름	지표 설명	
미국	NIST (CSRC)	SP 800-53 A	목적	정보기술보안 기술 개선 및 연방 정보보안 관리법(FISMA)을 따르는 연방기관들을 돕기 위해 개발
			대상	연방기관 및 일반 조직
			법률	연방 정보보안 관리법(FISMA)
			지표	17개 분야 163개 항목
		SP 800-55 rev.1	목적	조직의 정보 시스템과 프로그램 수준의 보안수준 평가를 위한 지표 방법론을 제시하고 정보보호의 평가를 위해 개발
			대상	일반 조직
			법률	-
			지표	-
영국	PWC	ISBS	목적	영국 기업들이 직면하는 정보보호 위협에 대한 이해를 돕기 위해 실시
			대상	기업
			법률	-
			지표	33개 분류 79개 질문

NO	통제항목	통제	항목	비고
1	접근 통제	20	42	기술 통제
2	인식 및 훈련	5	6	운영 통제
3	감사 및 책임	11	25	기술 통제
4	인증, 인가 및 보안 평가	7	11	관리 통제
5	구성 관리	8	18	운영 통제
6	비상 계획	10	39	운영 통제
7	식별 및 인증	7	11	기술 통제
8	사고 대응	7	15	운영 통제
9	유지 보수	6	16	운영 통제
10	미디어 보안	6	13	운영 통제
11	물리적 환경적 보안	19	37	운영 통제
12	계획	6	7	관리 통제
13	인원 보안	8	9	운영 통제
14	위험 평가	5	9	관리 통제
15	시스템 및 서비스 인수	11	16	관리 통제
16	시스템 및 통신 보안	23	42	기술 통제
17	시스템 및 정보 무결성	12	30	운영 통제
	계	214	346	

〔그림 14〕 SP 800-53 A

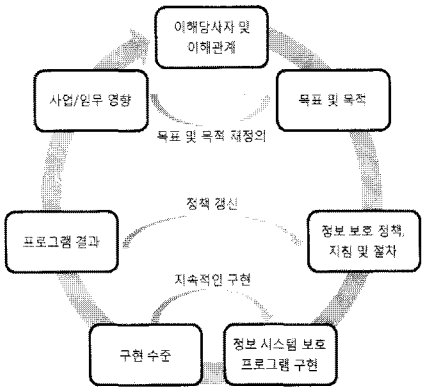
보안 객체	영향		
	낮음	중간	높음
기밀성	한정	중대	심각
무결성	한정	중대	심각
가용성	한정	중대	심각

〔그림 15〕 SP 800-53 A의 영향 수준

[그림 14]는 SP 800-53 A의 통제 항목을 나타낸 것으로 크게 기술 통제, 운영 통제, 관리 통제로 분류된다. 기술 통제는 시스템에 의해 자동적으로 수행되는 것에 대한 통제 분류로 접근 통제, 식별 및 인증, 감사 및 책임, 시스템 및 통신 보안 항목으로 구성되고, 운영 통제는 사람에 의해 수행되는 것에 대한 통제 분류로 인식 및 훈련, 구성 관리, 비상 계획, 사고 대응, 유지 보수, 미디어 보안, 인원 보안, 물리적·환경적 보안, 시스템 및 정보 무결성 항목으로 구성된다. 관리 통제는 시스템 관리와 보안을 위한 통제 분류로 인증·인가 및 보안 평가, 계획, 위험 평가, 시스템 및 서비스 인수 항목으로 구성된다.

FIPS 199의 영향 수준은 [그림 15]과 같이 기밀성, 무결성, 기용성에 대한 조직과 개인의 잠재적인 영향을 낮음(low), 중간(moderate), 높음(high)으로 나타낸다.

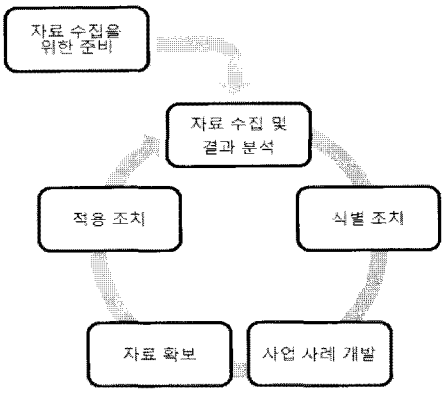
- 낮음: 기밀성, 무결성, 가용성의 손상이 조직의 운영, 조직의 자산 또는 개인적인 것에 한정된 역효과
- 중간: 기밀성, 무결성, 가용성의 손상이 조직의 운영, 조직의 자산 또는 개인적인 것에 중대한 역효과
- 높음: 기밀성, 무결성, 가용성의 손상이 조직의 운영, 조직의 자산 또는 개인적인 것에 심각한 역효과



〔그림 16〕 정보보호 대책 개발 절차

SP800-55 rev.1은 SP800-55(*Security metrics Guide for Information Technology systems*)[21]와 SP800-80 (*Guide to Developing Performance Metrics for Information Security*)[22]을 통합하고 조직의 보안수준 평가를 위한 지표 및 지표 개발 방법론을 제시하는 정보보호 성능 평가지침서이다.

이 평가지침서에서는 [그림 16]과 같은 7단계의 정보보호 대책 개발 절차와 [그림 17]과 같은 6단계의 정보보호 측정 프로그램 구현 절차를 제시하고 있다. 그리고 [그림 18]과 같은 19개의 지표의 샘플을 제시하고 있다. 샘플은 SP 800-53 통제에서 프로그램 수준은 SA-2 자원의 할당, RA-5 취약성 스캐닝, AT-3 보안 교육, CA-6 보안 승인, CM-2 기준 구성, CM-3 구성 변화 통제, CP-4 비상 계획 테스트 및 훈련, RE-6 물리적 접근 모니터링, 유효한 암호의 사용 항목을 사용하고, 시스템 수준은 AC-17 원격 접근, AU-6 감사 모니터링/분석/보고, AC-2 계정 관리, AC-3 접근 강제, IA-2 유저 확인



〔그림 17〕 정보보호 측정 프로그램 구현 절차

분류	지표	평가 타입	실행 증거
프로그램 수준	보안 예산	영향성	2
	취약성 관리	효율성	2
	인식 및 훈련	이행	6
	보증, 인가 및 보안 평가	유효성	5
	구성 관리	이행	4
	긴급 사태 계획	유효성	3
	시스템 및 통신 보안	이행	3
시스템 수준	접근 관리	유효성	6
	감사 및 책임	효율성	3
	식별 및 인증	유효성	2
	유지 보수	효율성	3
	위험 평가	효율성	5
프로그램/시스템수준	사고 대응	유효성	4
	미디어 보안	유효성	4
	물리적 환경	유효성	2
	계획	이행	3
	인적 보안	이행	2
	시스템 및 서비스 인수	이행	2
	시스템 및 정보 무결성	유효성	6
	계		67

〔그림 18〕 SP 800-55 rev.1 샘플

및 인증, MA-2 관리된 유지 보수, MA-6 적절한 유지 보수, CA-5 조치 및 마일드스톤의 계획 항목을 사용한다. 그리고 프로그램/시스템 수준은 IR-6 사고 보고, MP-6 미디어 처리 및 처분, PL-4 행동의 규칙, AC-2 계정 관리, PS-3 인적 심사, SA-4 인수, SI-2 흐름 개선 항목을 사용한다.

NO	분류	항목
1	조사 방법	3
2	정보 보호에 대한 태도	3
3	신뢰	3
4	보안 인식	2
5	위험 평가 및 규정 준수	3
6	BS 7799 (ISO 27001) 채택	3
7	보안 기술과 전문 지식	2
8	보안에 대한 투자	3
9	보안 경비에 대한 사업 사례	2
10	아웃소싱 및 해외 이전	2
11	최악에 대한 준비	3
12	Carried away	2
13	안티-바이러스 통제	3
14	이메일 및 웹 사용	3
15	신원 및 접근 관리	3
16	확장 네트워크	3
17	웹사이트 보안	3
18	최근 기술	3
19	보안 위반의 발생률	3
20	다른 보안 조사와 비교	3
21	보안 사고의 유형	2
22	바이러스와 악성 소프트웨어에 의한 감염	3
23	정보 시스템의 직원 남용	3
24	외부인에 의한 승인되지 않은 접근	2
25	컴퓨터 절도 및 사기	2
26	시스템 오류 및 데이터 손상	1
27	위반의 영향	1
28	사업 중단	2
29	사고 대응 비용	2
30	직접적인 재정 손실	1
31	평판 피해	1
32	사고의 총 비용	2
33	사고 대응 및 긴급 사태 계획	2
	계	73

〔그림 19〕 ISBS 2008

3.2 영국

영국의 경우 기업들을 위해 정책적으로 지원하는 내각 부서인 BERR(*Department of Business, Enterprise & Regulatory Reform*)-우리나라의 지식경제부-에서 2009년까지 ISBS(*Information Security Breaches Survey*)[23,24]의 조사를 담당하였으나, 2010년부터는 영국의 대학교육과 과학 등을 담당하는 DIUS(*Department of Innovation, University and Innovation*)이 DBIS(*Department of Business, Innovation and Skills*)와 통합·개편되면서, Infosecurity Europ과 PWC가 ISBS의 조사를 담당하게 되었다.

ISBS는 2년 주기로 조사되며, 조사를 담당하던 주체가 바뀌면서 몇몇 설문 대상, 방법론, 설문 내용 등이 변경되게 되었다. BERR이 담당하였을 때는 엄선된 기업들에 대하여 설문이 이루어졌지만, 2010년 조사부터는 광범위한 기업에 대하여 설문이 이루어지게 되었다. 또한 전화를 이용하던 설문 방식 또한, 온라인을 통해 설문으로 개선이 되었다.

그리고 분류와 항목의 수에 변화가 있었는데, 이것은 ISBS 2008을 통해 향상된 결과를 얻지 못하였고, 비용을 감소시킬 수 있는 부분을 제대로 반영하지 못하고 있기 때문에 분유와 항목이 새로 추가되거나 수정되었다. 이에 따라 ISBS 2008는 [그림 19]과 같이 33개 분류 73개 항목이 있었지만, ISBS 2010에서는 [그림 20]와 같이 21개 분류, 40개 항목으로 그 수가 줄었다. 21개의 분류 중 14개 분류는 ISBS 2008과 동일하게 유지되었고, 7개 분류는 수정되거나 새롭게 추가되었다.

ISBS는 이러한 설문을 통해 정보보호에 대한 기업의

NO	분류	항목
1	정보 보호에 대한 태도	3
2	변화하는 환경	3
3	보안 문화	3
4	보안에 대한 투자	3
5	보증에 대한 수요	2
6	데이터 유출 방지	2
7	보안 위반의 발생률	3
8	보안 사고의 유형	2
9	바이러스와 악성 소프트웨어에 의한 감염	2
10	시스템 오류 및 데이터 손상	1
11	컴퓨터 절도 및 사기	2
12	직원에 의한 다른 사고 아기	2
13	외부인에 의한 비인가 접근	3
14	위반의 영향	1
15	사업 중단	2
16	사고 대응 비용	1
17	직접적인 재정 손실	1
18	간접적인 재정 손실	1
19	평판 피해	1
20	사고의 총 비용	1
21	긴급 사태 계획	1
	계	40

〔그림 20〕 ISBS 2010

관점	주요 영역	핵심성과지표	후행지표
보호요구	노출 취약성 감소	3	4
	고급 침해사고 처리 대응	2	6
심층 기술 구현	최종 사용자 보안	5	6
	서버 보안	8	9
ISMS 수립	ISMS 구현	4	22
인식제고 및 교육	최종사용자 인식제고	1	1
	IS 관련 직원 능력	1	1
	경영층 지원	1	1
계		25	50

〔그림 21〕 Cyber health check

인식도나 실태를 설문 조사한 결과를 비교하여 정보보호 수준을 확인한다.

3.3 대만

대만은 정보산업연구소에서 기업의 정보보호 성능을 측정하기 하기 위해 ISO/IEC 27001과 Cyber health check 시스템을 함께 사용하는 지표를 [그림 21]과 같이 제안하고 측정기준을 제시하였다.

Cyber health check[25]는 인식제고 및 교육, ISMS 수립, 심층 기술 구현, 보안 요구의 4단계를 거치는 정보시스템 보안과 정보시스템 보안 관리 전략 수립을 통해 잠재적인 정보시스템 문제 확인 및 사이버 보안 리스크를 감소시킨다. 그리고 Cyber health check는 실제로 여러 사람들을 대상으로 실험 메일을 전송하고, 그 응답 비율을 측정하며, 평가기준과 지표의 순위를 매기고 10개 등급으로 분류한다.

Ⅳ. 국제 표준

현재 정보보호 관련 국제 표준으로는 ISO/IEC에서 제정한 ISO/IEC 27000 시리즈가 있다. 이것은 정보보호관리시스템(ISMS)에 대한 표준으로 27000(용어 정의), 27001(요구사항), 27002(실행 지침), 27003(구현 지침), 27004(측정 평가), 27005(위험 관리), 27006(심사인증기관 요구사항)까지 표준이 제정되었으며, 27007(심사 지침)에 대한 표준 작업이 진행 중이다.

그리고 현재 ITU-T에서도 정보보호 관련 표준 지표에 대한 작업을 진행 중이다.

4.1 ISO/IEC 27001, 27002

ISO/IEC 27001과 27002는 영국 BSI(British Standard Institute)에서 개발한 BS 7799의 Part 1과 Part 2를 표준화 한 것으로, 먼저 Part 2가 ISMS의 요구사항에 대한 표준인 27001으로 표준이 되고, 이후에 Part 1이 실행 지침인 27002로 표준화되었다.

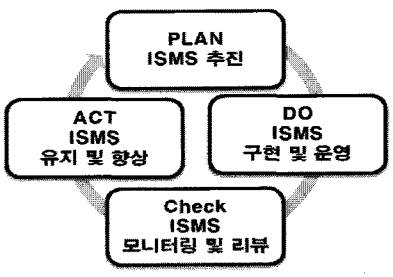
ISO/IEC 27001는 현재 정보보호 분야에서 가장 널리 인정받고 있는 국제인증으로 ISMS에 대한 이행, 감시 및 검토, 유지, 개선에 필요한 요구사항을 정의하고 있으며, 정보보호가 필요한 기업에 정보보호관리체계를 수립하고 운영할 수 있는 [그림 22]과 같은 Plan-Do-Check-Ack(PDCA) 모델을 제공하고 있다. 이 표준에서는 대상을 특정 산업이나 규모 등으로 제한하지 않는다. 그리고 ISO/IEC 27002는 ISMS을 위한 정보보호 관리의 모범 사례 권고안을 제공하며, 기밀성·무결성·가용성을 중심으로 한 표준화된 실무 규약이다.

ISO/IEC 27002의 지표 구성을 살펴보면 [그림 23]와 같이 11개 통제분야, 39개 통제항목, 133개 세부통제항목으로 이루어져 있다.

4.2 ITU-T X.CSI(Cyber Security Index)

현재 ITU-T에서는 지난 SG17 회의(2010년 4월 7일~4월 16일) 사이버 보안 지수에 관한 가이드라인에 대한 신규 워크아이템 제안(*A proposal for establishing a new work item on guidelines for Cybersecurity Index(CSI)*)[26]의 기고서가 제출되어 채택되었다.

이 기고서는 사이버 보안 지수와 관련하여 현재 글로벌 차원에서 합의된 지수가 없으며, 변화하는 기술반전 추이와 개도국이나 저개발국의 현황을 고려한 지수 개발이 요구되고 있으나 국제표준화 기구에서 표준화가 수행이 되고 있지 않기 때문에, 지수의 지표 데이터에 대한 신뢰성을 확보하면서 사이버보안 지수를 대표할



〔그림 22〕 PCDA 모델

NO	통제분야	통제항목	세부통제항목
1	보안정책	1	2
2	정보보안 조직	2	11
3	자산 관리	2	5
4	인원 보안	3	9
5	물리적 환경적 보안	2	13
6	통신 및 운영 관리	10	32
7	접근 통제	7	25
8	정보시스템 취득, 개발, 유지보수	6	16
9	보안 사고 관리	2	5
10	사업 연속성 관리	1	5
11	준거성	3	10
	계	39	133

〔그림 23〕 ISO/IEC 27002 정보보호 대책

수 있는 지표 선정과 정보보호 정책의 집행 효과를 측정하기 위하여 사이버보안 지수의 개발이 제안되었다.

X.CSI의 기고서는 현재 순천향대학교 염흥열 교수가 메인에디터로 선정되어 표준화 작업을 수행하고 있다. 현재 작성중인 X.CSI 권고 초안은 2010년 10월 라포쳐 회의를 거쳐, 2010년 12월에 개최 예정인 ITU-T SG17 회의에 제출될 예정이다.

현재 개발 중인 사이버 보안 지수에는 한국의 국가정보보호지수 및 대표 정보보호 평가 지표와 선진국 및 개도국의 실정이 반영되어, 국가의 전반적인 보안 수준을 측정할 수 있고, 조직 및 국가의 실정에 맞는 평가 지표를 선택 할 수 있는 방법론을 개발 중에 있다.

V. 평가 지표의 통제항목 비교

이번 장에서는 국제 표준인 ISO/IEC 27002의 지표와 한국의 K-ISMS, 미국의 SP 800-53 A의 지표를 비교한다. 영국의 ISBS를 제외한 이유는 ISBS의 경우 조직의 정보보호 수준 평가 기준이 실무자의 설문에 의존하기 때문이다.

각 지표의 통제항목의 수를 보면 [그림 24]과 같이 SP 800-53 A가 분야와 항목의 수에서 다른 지표에 비해 많지만, 세부항목을 보면 K-ISMS가 396개로 가장 많다. 그리고 ISO/IEC 27002는 분야, 항목, 세부항목에서 다른 두 지표에 비해 그 수가 가장 적다.

다음으로는 평가 대상에서 차이를 보인다. 이 두 지

	ISO/IEC 27001	K-ISMS	SP 800-53 A
분야	11	15	17
항목	39	120	214
세부항목	133	396	346

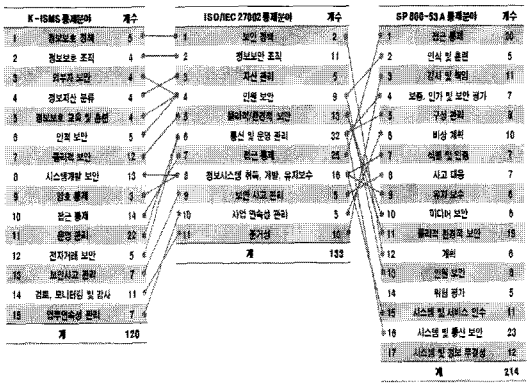
〔그림 24〕 각 통제항목의 비교

통제분야	설명
보안 정책	정보보안에 대한 경영방침과 지원사항에 대한 통제 구조 확인
정보보안 조직	조직 내에서 보안을 효과적으로 관리하기 위한 보안 조직 구성 및 책임과 역할에 대한 규정
자산 관리	조직 자산에 대한 분류 및 이에 따른 적절한 보호 프로세스 검토
인원 보안	사람에 의한 실수, 절도, 부정 수단이나 설비의 잘못 사용으로 인한 대응방안 확인
물리적/환경적 보안	비인가된 접근, 손상, 사업장과 정보에 대한 영향 대응책 여부
통신 및 운영 관리	정보처리 설비의 정확하고 안전한 운영방안 여부
접근 통제	정보 접근 통제 방안 여부
정보시스템 취득, 개발, 유지보수	정보시스템 보안이 수립되었음을 보장하는 방안 존재 여부
보안 사고 관리	정보보안 사고와 취약점이 허용기간 내에 교정과 의사전달이 되는지 여부
사업 연속성 관리	사업활동의 방해요소를 완화시키며 주요 실패 및 재해의 영향으로부터 주요 사업 활동을 보호하기 위한 프로세스 존재 여부
준거성	법률 및 민사상의 법률, 규정 또는 계약 의무사항 및 보안 요구 사항의 불일치를 회피하는 방안 존재 여부

〔그림 25〕 ISO/IEC 27002 통제분야 설명

표는 일반 기업의 정보보호 관리체계를 대상으로 기업의 정보에 대한 보안 수준 정도를 평가하는 것이고, SP 800-53 A는 정보시스템 자체에 대한 평가이기 때문에 다른 두 지표에 비해 평가 대상이 한정적이다.

통제분야를 비교하기 위해서 [그림 25]과 같이 ISO/IEC 27002의 통제분야 대한 내용을 기준으로 비교하였다. 3개의 지표를 비교하면 [그림 26]과 같이 ISO/IEC 27002의 인적 보안, 물리적/환경적 보안, 통신 및 운영관리 등과 같은 통제분야들이 SP 800-53 A에서는 세분화되어 나타나고 있다. 그에 비해 K-ISMS는 ISO/IEC 27002의 통제항목을 대부분 쓰고 있으며, ISO/IEC 27002의 인원 보안, 통신 및 운영 관리, 정보시스템 취득/개발/유지보수 통제분야를 세분화하였다.



〔그림 26〕 통제항목 비교[11]

Ⅵ. 평가 체계 및 지표의 개선방향

지금까지 살펴본 체계 및 지표들은 공공기관 이나 일반 기업 등 특정 분야에서만 적용할 수 있도록 개발이 되어 다른 분야에 적용하기가 어렵다. 또한 몇몇 체계 및 지표들은 서로간의 지표 항목이 유사하여 동일한 평가 분야의 중복이 발생하고 있고, 유사한 인증 제도가 운영됨으로 해서 실효성이 저하되는 문제가 발생한다. 이와 같은 문제를 해결하기 위해 다양한 분야의 전반을 평가할 수 있는 통합된 지표의 개발이 필요하다.

또한 진단항목이 개선되지 않는 문제가 있는데, 최근에 개발된 지표가 아니라면 최근 정보보호 이슈에 대한 점검항목이 없거나 새롭게 필요한 평가항목이 없는 경우가 있다. 이러한 문제는 지속적으로 국내/외에서 발생하는 보안이슈를 파악하고, 평가하여 그 결과를 반영할 수 없으므로 주관기관은 평가항목을 지속적으로 개선해야 한다.

정보보호 평가체계에 대한 이해도가 낮은 경영층의 경우, 평가를 통한 감사행위의 보증수준이 기대치와 다르거나, 정성적 평가의 경우 심사원 또는 심사환경에 따라 그 결과가 달라질 수 있기 때문에 수치화 가능한 정량적 지표에 의한 정보보호 평가체계가 개발되어야 한다.

국가정보보호지수의 경우 국내에서만 통용되는 지수이기 때문에 글로벌 차원의 표준화 기구를 통한 국제적으로 합의가 될 필요가 있다. 하지만 현재 지수에서는 기술적, 정책적 성숙도를 평가할 수 있는 지표가 없기 때문에 국가의 정보보호 전반을 측정할 수 있도록 다양한 지표의 개발이 필요하다.

또한 효과적인 지수화를 위하여 자동화된 툴 개발이 필요하며, 이미 수집된 신뢰할 수 있는 통계를 활용할 수 있어야 한다. 앞서 언급했던 진단항목이 개선 문제 또한 선택 가능한 지표들(Pool)을 구성하여, 지속적으로 국내외 보안 이슈를 평가항목에 반영할 필요가 있다.

Ⅶ. 결론

정보보호 평가는 평가 대상의 정보보호 수준을 전반적이고 객관적으로 살펴볼 수 있는 방법이다. 이러한 평가를 통해 평가 대상은 자신의 정보보호 수준을 확인함으로써 보다 나은 정보보호 대책을 세울 수 있다.

본 논문에서는 국내/외에서 사용되고 있는 정보보호 관련 평가 체계 및 지표와 정보보호 관련 국제 표준을 살펴보고 현재 지표들의 개선방향에 대해 서술하였다.

향후 각 분야에 특화된 항목을 가지면서 하나의 지표를 통해 정보보호 전반을 평가를 할 수 있는 지표가 개발되어 기업 및 조직, 개인의 정보보호 수준이 향상되기를 기대해보며, 그리고 국가정보보호지수의 개선을 위하여 추가적인 연구가 진행되어야 할 것이다.

참 고 문 헌

[1] 권영관, 염흥열, "컨택센터의 정보보호관리체계 적용에 관한 연구," 정보보호학회지, 18(5), pp. 99-111, 2008년 10월.

[2] 한국정보보호진흥원, "국가 정보보호수준 평가지수 모델개발 및 활용에 관한 연구," 2005년 12월

[3] 국가사이버안전센터, "국가 사이버 안전 매뉴얼," 2005년 10월.

[4] 한국인터넷진흥원, "정보보호 안전진단 해설서," 2010년 3월.

[5] 한국인터넷진흥원, "정보보호 안전진단 업무 안내서," 2010년 3월.

[6] 한국인터넷진흥원, "정보보호 관리체계 브로슈어," 2010년 3월.

[7] 행정안전부, "전자정부서비스 보안수준 개선대책," 2008년 4월.

[8] 행정안전부, "전자정부 정보보호관리체계 인증 등에 관한 지침," 2010년 6월.

[9] 행정자치부, "개인정보보호수준 진단," 2008년 4월.

[10] eTrust인증, www.etrust.or.kr

[11] 방송통신위원회, 한국인터넷진흥원, "개인정보보호관리체계(PIMS) 인증제 공청회," 2010년 8월.

[12] 방송통신위원회, 한국인터넷진흥원, "개인정보보호관리체계(PIMS) 인증 심사항목 리스트," 2010년 8월.

[13] ISO27k infosec management standards, www.iso27001security.com

[14] 정보보호마크 인증위원회, www.eprivacy.or.kr

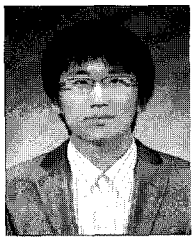
[15] NIST CSRC, http://csrc.nist.gov

[16] NIST, "Guide for Assessing the Security Controls in Federal Information Systems," Jul 2008

[17] NIST, "Performance Measurement Guide for

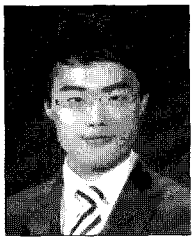
Information Security," Jul 2008
[18] NIST, "Recommended Security Controls for Federal Information Systems," Feb 2005
[19] NIST, "Standards for Security Categorization of Federal Information and Information Systems," Feb 2004
[20] 이영규, "정보보안 평가지표의 부합성 및 중요도에 관한 실증연구," 2008년 2월.
[21] NIST, "Security Metrics Guide for Information Technology Systems," Jul. 2003.
[22] NIST, "Guide to Developing Performance Metrics for Information Security," Jun. 2007.
[23] BERR, "Information Security Breaches Survey 2008," April. 2008.
[24] PricewaterhouseCoopers, Infosecurity Europe, "Information Security Breaches Survey 2010," April. 2010.
[25] III, http://web.iii.org.tw/
[26] ITU-T, "Proposal for the 4th revised text on ITU-T X.usnsec-1|ISO CD 29180: Security framework for ubiquitous sensor network," http://www.itu.int/md/T09-SG 17-C-0125/en, Sep. 2009.

〈著者紹介〉



이 동 희 (Dong-Hee Lee)
학생회원

2010년 2월: 순천향대학교 정보보호학과 졸업
2010년 3월~현재: 순천향대학교 정보보호학과 석사과정
<관심분야> 정보보호, 역추적



여 돈 구 (Don-Gu Yeo)
학생회원

2009년 2월: 순천향대학교 정보보호학과 졸업
2009년 3월~현재: 순천향대학교 정보보호학과 석사과정
<관심분야> 정보보호, USN 보안, 클라우드 컴퓨팅 보안, IPTV 보안, 역추적

염 흥 열 (Heung-Youl Youm)
종신회원

1981년 2월: 한양대학교 전자공학과 졸업
1983년 2월: 한양대학교 대학원 전자공학과 졸업(석사)
1990년 2월: 한양대학교 대학원 전자공학과 졸업(박사)
1982년 12월~1990년 9월: 한국전자통신연구소 선임연구원
1990년 9월~현재: 순천향대학교 공과대학 정보보호학과 정교수
1997년 3월~2000년 3월: 순천향대학교 산업기술연구소 소장
2000년 4월~2006년 2월: 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재: 한국정보보호학회 총무이사, 학술이사, 교육이사, 논문지편집위원(역), 수석부회장(현)
2005년~2008년: ITU-T SG17 Q.9 Rapporteur(역)
2006년 11월~2009년 2월: 정보통신연구진흥원 정보보호전문위원
2009년 5월~현재: 국정원 암호검증위원회 위원
2009년~현재: ITU-T SG17 부의장/SG17 WP2 의장
<관심분야> 인터넷보안, USN 보안, IPTV 보안, 홈네트워크 보안, 암호프로토콜