情 報 保 護 學 會 誌
第23卷 第4號, 2013. 8

정보통신망법 개정에 따른 기업 정보보호 제도 현황 및 정보보호 관리체계의 인증기준 비교

김 환 국*, 고 규 만**, 이 재 일***

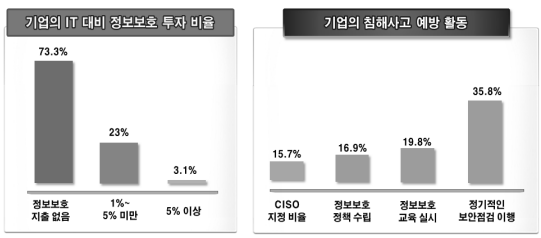
요 약

최근 사이버공격은 지능화, 대규모화되고 있는 반면, 경기침체 등으로 인해 기업의 정보보호 투자가 저조하고 인터넷 침해사고 예방활동이 미흡한 실정이다. 정부는 취약한 기업의 정보보호 환경을 개선하기 위해 정보보호 안전진단 제도를 폐지하고 정보보호 관리체계(ISMS) 인증제도로 일원화하였으며, ISMS 인증기업을 대상으로 한 정보보호 관리등급제, 정보보호 사전점검, 임원급 정보보호 최고책임자(CISO) 지정 등 신설하였다. 본 고에서는 개정 정보통신망법에 따라 신설·보완된 기업 정보보호 관련 제도현황과 변경된 정보보호 관리체계 인증기준에 대해 소개하고자 한다.

Ⅰ. 서 론

2009년 7·7 DDoS 공격, 2012년 통신사 개인정보 대규모 유출 사고, 2013년 방송 및 금융사 대상 사이버테러 등 최근 고도화된 해킹 공격에 의한 사이버 침해사고가 급증하고 있는 추세이다. 반면, 한국인터넷진흥원의 기업 정보보호 실태조사에 따르면, 국내 기업의 73.3%는 IT 예산 투자 대비 정보보호 투자가 전무하고, 기업의 정보보호 최고책임자 임명은 15.7%에 불과한 수준이다. 더욱이 절반 이상의 기업들이 정보보호 투자에 대한 필요성을 느끼지 못한다고 답하였다.[1]

정부는 급변하는 IT서비스 및 사이버 침해 환경에 능동적으로 대처하기에는 현행 정보보호 법제로는 한계가 있어, 실질적 정보보호체계 구축을 위해 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 정보통신망법) 개정(2012.2.17) 하였다. 또한, 기업에게 보다 실질적인 정보보호 활동을 유도하고, 해킹 등 사이버 위협에 대한 사전예방 조치를 강화할 수 있도록 하는 등 다양한 기업 정보보호 관련 제도들을 신설·보완하였다.[2]



〔그림 1〕 기업의 정보보호 실태조사(2013, 한국인터넷진흥원)

「정보보호 관리체계 인증 등에 관한 고시」('13.1.17 공포) : 통신사, 포털, 쇼핑몰 등 주요 정보통신서비스 제공자를 인증 의무대상자로 지정하고, 인증기준 등을 재정비하였으며, 기업의 정보보호 수준을 객관적으로 측정할 수 있는 정보보호 관리등급제를 신설하였다.

「정보보호조치에 관한 지침」 ('13.1.17 공포) : 정보보호 최고책임자 지정, 정보보호 현황 공개, 정보보호 투자 촉진(5%이상), 보안관제 운영 등 정보통신서비스 기업이 준수해야 할 조치 사항을 강화하였다.

「정보보호 사전점검에 관한 고시」 ('13.1.17 공포) : 새로운 정보통신망의 구축 또는 정보통신서비스의 제공 이전에 계획 또는 설계 과정에서 정보보호를 고려하

* 한국인터넷진흥원 보안관리팀 (rinyfeel@kisa.or.kr)
** 한국인터넷진흥원 보안관리팀 (kmko@kisa.or.kr)
*** 한국인터넷진흥원 인터넷침해대응센터 (jilee@kisa.or.kr)

여 필요한 대책을 마련토록 하였다.

본 고에서는 개정된 정보통신망법에 따라 신설·보완된 정보보호 사전점검, 정보보호 관리체계 인증제도, 정보보호 관리등급제 등 기업 정보보호관련 국내 제도 현황에 대해 살펴보고 정보보호 관리체계 인증기준의 주요 개정 내용을 소개하고자 한다.

Ⅱ. 기업 정보보호관련 국내 제도 현황

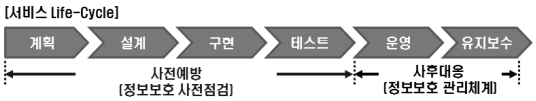
2012년 2월 정보통신망법이 개정되면서, 정보보호 안전진단 제도가 폐지되고 ISMS 인증제로 일원화되었으며, ISMS 인증기업을 대상으로 한 정보보호 관리등급제, 정보통신서비스 운영 이전에 계획·설계부터 정보보호를 고려토록 하는 정보보호 사전점검, 임원급 정보보호 최고책임자(CISO) 지정 등도 신설되었다.

〔표 1〕 국내 기업 정보보호 관련 제도

구 분	정보보호 사전점검	정보보호 관리체계 인증	정보보호 관리 등급제
시행연도	2010년	2002년	2013년
제도성격	자율 ('12년 법적근거마련)	의무 + 자율	자율 ('13.2.18 시행)
법적 근거	정보통신망법 제36조의 2	정보통신망법 제47조	정보통신망법 제47조의5
주요 대상	정보시스템 구축에 필요한 투자금액이 5억원 이상 정보화사업	의무대상자 및 자율 신청기업	정보보호관리체계 인증 취득 기업
점검항목 (인증기준)	방통위 고시 11개	104개	고시 제정준비중
유효기간	-	3년 (사후관리 연 1회)	1년
과태료	-	10백만원 이하	-

2.1 정보보호 사전점검 제도

정보보호 사전점검 제도는 기업이 정보통신서비스를 제공하기 이전에 설계, 구현, 시험 단계에서 정보보호 위협, 취약점 분석 등의 진단을 통해 사전에 취약점을 제거하고 필요한 조치를 하거나 계획을 마련하기 위한 것으로, 법적 근거가 마련되었다. 이와 유사한 제도로는 보안적합성 검증, 개인정보 영향평가 등이 있다.



〔그림 2〕 정보보호 사전전검 개념

2.2 정보보호 관리체계 인증제도

정보보호 관리체계 인증제도는 기업의 주요 정보자산 유출 및 피해를 사전에 예방하고 대처할 목적으로 기업이 수립·운영 중인 종합적인 정보보호 관리체계에 대해 인증하는 제도이다. 2013년부터 기존 정보보호 안전진단 대상자를 ISMS 인증 의무대상자로 신규 지정하여 인증을 받도록 의무화하였다.

의무대상 : 정보통신망서비스제공자(ISP), 집적정보통신시설 사업자(IDC), 정보통신서비스 매출액 100억 이상 또는 이용자수 100만명 이상 사업자

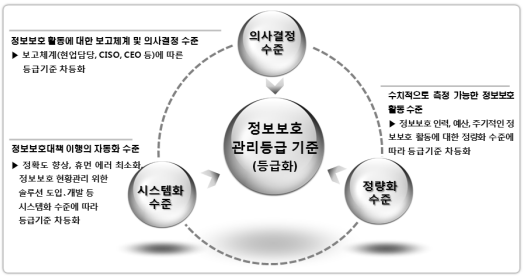
국내에서 정보보호 관리체계 인증제도는 다음 [표2]와 같이 3가지 제도가 운영되고 있다. G-ISMS 인증제도는 '2013년부터 미래창조과학부로 이관되어 운영 중이다.

〔표 2〕 정보보호 관리체계 인증제도 유형

구분	정보보호 관리체계 (ISMS)	개인정보보호 관리체계 (PIMS)	전자정부 정보보호 관리체계 (G-ISMS)
시행 시기	'02년	'11년	'09년
소관 부처	미래창조과학부	방송통신위원회	미래창조과학부 (안전행정부에서 이관)
인증 대상	민간 기업	개인정보를 보유한 민간 기업	공공·행정기관의 전자정부 대민서비스
인증 기관	KISA	KISA	KISA
자율/의무	자율 + 의무	자 율	자 율
점검항목 (인증기준)	104개 (관리과정 12, 보호대책 92)	118개 (관리과정 11, 보호대책 79, 생명주기 28)	149개 (관리과정 15, 문서화 3, 보호대책 131)

2.3 정보보호 관리등급제

국내 기업의 정보보호수준은 초기단계로서, 정보보호 활동이 전사적이 아닌 일부 중요 서비스 부분에 대해서만 이루어지고 있는 실정이다. 기업에서 제공하는 다양한 정보통신서비스에 대한 정보보호 수준을 객관적으로 측정할 수 있는 객관적 기준 및 평가 체계에 대한 필요성이 지속적으로 제기되어 정보통신망법 제47조의 5의 신설로 정보보호 관리등급제도가 시행되었다.



〔그림 2〕 정보보호 관리등급제 기준 방향

정보보호 관리등급은 기업의 정보보호 의사결정 수준, 인터넷 침해사고 예방·대응을 위한 시스템화 수준, 인력, 예산 등의 정보보호 활동 수준에 따라 등급을 부여하는 제도로서, ISMS 인증을 취득한 기업을 대상으로 권고제도이며 현재 정보보호 관리등급제 운영 및 기준을 반영한 고시안 제정을 준비 중에 있다.

Ⅲ. ISMS 인증기준의 주요 개정 내용

ICT 및 정보보호 환경의 급격한 변화에도 불구하고 ISMS 인증 기준은 2002년 ISMS 인증제도 도입 이후 기준 개정이 이뤄지지 않아 [표3]과 같이 기존의 실효성이 낮은 점검항목을 통합하고 최신 보안관리 기준을 반영한 인증기준이 변경되었다.[3]

〔표 3〕 정보보호 관리체계 인증 기준 주요 변경 내용

구분	주요 변경 내용
신규 항목 (14개)	- 경영진의 책임(예산 및 인력 지원, 의사결정 참여 등) 강화 - 정보보호최고책임자(CISO) 의무 지정 등 조직 구성 강화 - 최신기술 및 보안사고 반영
통합 또는 변경 항목 (128개 → 90개)	- 업무연속성관리, 물리적 보안, 전자거래보안, 검토, 모니터링 및 감사 영역 중심으로 중복 또는 유사항목 통합
삭제 항목 (9개)	- 적격심사, 물리적 위치 및 구조 조건, 입력 데이터/내부처리/출력 데이터 검증, 전자우편 등 실효성 부족(결함률 0%)항목 삭제

ISMS (구)인증 기준은 137개 통제항목 및 446개 세부점검항목으로, (신)인증 기준은 104개 통제항목 및 253개 세부점검항목으로 구성되었으며, 주요 변경 항목은 [표 4]와 같다.[4]

〔표 4〕 ISMS 인증기준의 주요 변경내용

분야		(구)인증 기준		(신)인증 기준	
		통제 항목 수	세부 점검 항목	통제 항목 수	세부 점검 항목
정보보호 관리 과정	정보보호 정책 수립	2	7	-	-
	관리체계 범위 설정	2	4	-	-
	정보보호정책수립 및 범위설정	-	-	2	4
	경영진 책임 및 조직구성	-	-	2	4
	위험 관리	5	19	3	11
	구현	2	7	-	-
	정보보호대책 구현	-	-	2	3
	사후 관리	3	10	3	6
	소계	14	47	12	28
문서화	문서 요건	1	1	-	-
	문서의 통제	1	1	-	-
	운영기록의 통제	1	1	-	-
	소계	3	3	-	-
정보보호 대책	정보보호 정책	5	10	6	13
	정보보호 조직	4	11	4	7
	외부자 보안	4	8	3	4
	정보자산 분류	4	7	3	7
	정보보호 교육 및 훈련	4	14	-	-
	정보보호교육	-	-	4	10
	인적 보안	5	18	5	11
	물리적 보안	12	36	9	21
	시스템 개발 보안	13	53	10	22
	암호 통제	3	6	2	8
	접근 통제	14	38	14	46
	운영 관리	22	99	-	-
	운영 보안	-	-	22	56
	전자거래 보안	5	21	-	-
	보안사고 관리	7	20	-	-
	침해사고 관리	-	-	7	14
	검토・모니터링・감사	11	37	-	-
	업무 연속성 관리	7	18	-	-
	IT재해복구	-	-	3	6
	소계	120	396	92	225
총계		137	446	104	253

3.1 경영진 참여 및 책임 강화

개정이전 인증기준(관리과정 1.2 조직 책임설정)에는 정보보호 활동에 대한 경영층의 명확한 지원 및 방향제시를 보증할 수 있는 조직 수립 정도가 언급되어 있는 수준으로 정보보호 활동에 대한 경영진 역할이 불분명하였다.

개정된 인증기준(관리과정 2.1 경영진 참여, 2.2 정보보호 조직 구성 및 자원할당)에는 경영진(대표이사, CISO 등)이 정보보호활동 전반의 의사결정에 참여(경영진 보고 및 의사결정 체계 마련)하도록 하고, 최고경영자가 조직규모를 고려하여 예산/인력을 지원하고 CISO지정, 실무조직을 구성하도록 명시적인 기준을 마련하였다.

3.2 정보보호 조직 구성 강화

개정이전 인증기준(보호대책 2.2.1 정보보호 관리자, 2.1.1 조직의 구성)에는 최고경영자가 정보보호 관리자를 지정하도록 하고 있으나 정보보호관리자의 위상이 불명확하고, 정보보호조직 구성을 정보보호관리자 지정으로 보고 있어 기업의 규모에 적합한 실무조직 구성 근거가 미흡하였다.

개정된 인증기준(보호대책 2.1.1 정보보호최고책임자 지정, 2.1.2. 실무조직 구성)에는 임원급 이상의 정보보호최고책임자 지정을 의무화하도록 하여 정보보호 조직의 위상을 강화하고, 정보보호 최고책임자(CISO)의 역할을 지원할 수 있는 실무조직 구성 명시적 기준을 마련하였다.

3.3 외부자 보안 강화

개정이전 인증기준(보호대책 3. 외부자 보안)에는 업무의 외부위탁 시 보안요구사항을 계약서에 명시하도록 하고 있으나 외부자 계약 만료, 외주 개발 시 준수해야 할 정보보호 대책이 미흡하게 적용되고 있었다.

- 외부자 계약 만료 시 주요 대책 : 자산반납, 접근권한 회수, 중요정보 파기 등
- 외주 개발 시 주요 대책 : 개발자 접근통제, 개발보안 절차 준수 등

개정된 인증기준(보호대책 3.2.2 외부자 계약 만료 시 보안, 8.3.1 외주개발 보안)에는 외부자 계약 만료, 업무종료, 담당자 변경 시 적용해야 할 통제기준을 마련하고, 정보시스템 외주 개발 시 보안요구사항을 계약서에 명시하고 이행여부를 관리·감독하도록 하였다.

3.4 모바일 기기 보안 강화

개정 이전 인증기준에는 업무용으로 사용되고 있는 모바일 기기(휴대전화, 노트북, PDA, 패드 등)에 대한 물리적, 논리적 접근통제에 대한 명시적인 기준이 부재하였다. 다만 “7.1.1 물리적 보호구역” 및 “11.6.1 이동컴퓨팅)의 세부점검항목에서 장비, 문서, 매체 반출입 및 휴대용 정보통신기기에 대한 보안정책 수립하도록 하는 수준이었다.

개정된 인증기준 (보호대책 7.1.5 모바일 기기 반출입, 10.4.5 모바일 기기 접근)모바일 기기 미승인 반출입에 대한 통제절차를 수립하도록 하고, 업무를 목적으로 내·외부 네트워크에 모바일기기를 연결하여 사용할 경우 접근통제 정책을 수립하도록 하였다.

3.5 주요 직무자 인터넷 접속 제한

개정이전 인증기준(보호대책 11.3.2 인터넷 접속관리)에는 침입차단시스템을 통한 인터넷 접속 정책을 수립하도록 하고 있으나 업무 중요도에 따른 주요직무자(DBA, DB운영자, 개발자, 중요정보 취급자 등)별 인터넷 접속 제한 통제(망분리, 웹메일/메신저/P2P/웹하드/유해사이트 차단 등)는 미흡한 수준이었다.

개정된 인증기준(보호대책 10.4.6 인터넷 접속)에 인사정보, 영업비밀, 산업기밀, 개인정보 등 중요정보를 대량으로 취급·운영하는 주요직무자에 대한 접속 제한, 망분리 등의 정책을 수립하도록 하였다.

상기 인증기준 이외에도 주요 변경내용은 다음 [표 5]와 같다.

〔표 5〕 ISMS 인증기준의 주요 변경내용

구분	관련 기준	내용
DDoS 보안	12.1.1 침해사고 대응절차 수립 (강화)	DDoS 등 침해사고 유형별 중요도 분류, 유형별 보고·대응·복구 절차, 비상 연락체계, 훈련 시나리오 등을 포함한 침해사고 대응 절차를 수립하여야 한다.
무선네트워크	11.2.7 무선네트	무선랜 등을 통해 무선인터넷을 사용하는 경우 무선 네트워크 구간에 대한 보안

구분	관련 기준	내용
보안	워크 보안 (신규)	을 강화하기 위해 사용자 인증, 송수신 데이터 암호화 등의 보호대책을 수립하여야 한다.
스마트 워크 보안	11.2.6 스마트워크 보안 (신규)	재택근무, 원격협업 등과 같은 원격 업무 수행 시 이에 대한 관리적·기술적 보호대책을 수립하고 이행하여야 한다.
패치 관리	11.5.2 패치관리 (신규)	소프트웨어, 운영체제, 보안시스템 등의 취약점으로 인해 발생할 수 있는 침해사고를 예방하기 위해 최신 패치를 정기적으로 적용하고 필요한 경우 시스템에 미치는 영향을 분석하여야 한다.
개발 보안	8.1.4 접근권한 기능 (신규)	정보시스템 설계 시 업무의 목적 및 중요도에 따라 접근권한을 부여할 수 있도록 하여야 한다.
보안 관제	11.6.4 침해시도 모니터링 (신규)	외부로부터의 침해시도를 모니터링하기 위한 체계 및 절차를 수립하여야 한다.
사용자 보안 강화	10.3.1 사용자 인증 (신규)	정보시스템에 대한 접근은 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 의해 통제되어야 하고 필요한 경우 법적요구사항 등을 고려하여 중요 정보시스템 접근 시 강화된 인증방식을 적용하여야 한다.
	10.3.2 사용자 식별 (신규)	정보시스템에서 사용자를 유일하게 구부할 수 있는 식별자를 할당하고 추측 가능한 식별자 사용을 제한하여야 한다. 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하고 책임자의 승인을 받아야 한다.

Ⅳ. 결 론

사이버공격은 특정 기업의 기밀이나 개인정보 등 특정 정보를 목표로 하루가 다르게 지능화, 고도화되고 있다. 이는 기업의 첨단기술의 유출, 기업 신뢰도 하락과 고객 이탈, 주가 하락뿐만 아니라 집단소송과 대규모 피해보상 등 사회·경제적인 측면에서 큰 문제를 발생시켰다. 이러한 문제점에 대해 기업의 사회적 책임성이 더욱 요구되기에 이르렀으며, 기업의 정보보호 수준을 강화할 수 있는 종합적 관리체계의 구축이 필요하게 되었다.

정보통신망법 개정에 따라 기업 경영진 차원에서 상시 모니터링 체계 구축 등 체계적 정보보호 관리를 유도하기 위하여 기존 운영되던 정보보호 안전진단 제도는 폐지되고, 보다 높은 수준의 ISMS 인증 제도로 일원화 하여, 일정규모 이상의 정보통신서비스제공자는 의무적으로 인증을 받도록 강화하였다.

반면 기업은 빠른 속도로 변화하고 있는 IT 환경 및 정보보호 컴플라이언스 요구에 부담이 가중되고 있어, 기업이 정보보호 투자가 저조한 것도 현실이다. 이는 기업의 보안관리 취약점 ToP 10[5]을 살펴보아도, 패스워드 관리 소홀, 주요 자산 식별 미흡, 접근통제 미흡 등 기본적인 정보보호 활동이 미흡한 것으로 알 수 있다.

〔표 6〕 기업 보안관리 취약점 ToP 10

1	패스워드 암호화 및 관리 미흡
2	주요 자산에 대한 보안등급 부여 및 취급방안 미흡
3	백업관련 지침 부재 및 미준수
4	개인정보보호 등 법적 요구사항 미준수
5	정보보호 교육 계획 부재 및 사후 교육 미흡
6	비인가자 접근통제에 대한 주기적 검토 미흡
7	계정 공통 사용 및 관리 미흡
8	내부망에 대한 연결통제 규정 미준수
9	주요 정보자산 식별 및 위험 분석/평가 미흡
10	물리적 보호구역 미정의 및 반출입 관리 미흡

이제는 기업의 정보보호를 지출해야 하는 비용의 개념이 아니라, 비즈니스 기회를 예측하고 현재와 미래의 위험에 적절히 대응할 수 있는 핵심 경쟁력인 동시에, 예상하지 못한 위기상황에서 기업전반의 비즈니스 안정성을 유지하고 정보자산을 적절하게 보호하기 위한 경영활동의 일부로 보아야 한다.

기업의 임원급 정보보호 최고 책임자를 지정하여 임명하고, 경영진은 자사의 정보보호 전략 및 정책 수립 등 의사결정에 적극적인 참여가 필요하다. 또한 정보보호 전담조직 구성, 정보보호 교육 실시 등 내부 직원의 역량을 강화하도록 지원하고, 자사의 정보보호 활동에 지속적인 모니터링(내부 감사 등) 체계를 구축하고 외주업체에 대한 보안을 강화하여 해킹사고 대비 위험관리 능력 확보가 필요하다.

참고문헌

[1] 한국인터넷진흥원, “2012년 기업 정보보호 실태조사”, *한국인터넷진흥원 발간 보고서*, 2013

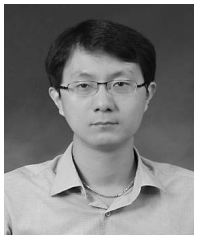
[2] 방송통신위원회 고시 제2013-3호, 제2013-4호, 제2013-5호, Jan. 2013

[3] 한국인터넷진흥원, “정보보호관리체계 인증제도 해설서”, *한국인터넷진흥원 발간 보고서*, 2013
[4] 한국인터넷진흥원, “ISMS 인증기준 세부점검 항목”, http://isms.kisa.or.kr, 2013
[5] 한국인터넷진흥원, “2012년 ISMS 인증심사 결과분석”, *한국인터넷진흥원 내부보고서*, 2013

〈著者紹介〉

김 환 국 (Kim Hwan Kuk)
정회원

2000년 8월 : 한국항공대학교 컴퓨터공학과 석사 졸업
2001년~2006년 : 한국전자통신연구원 정보보호연구단 연구원
2009년 3월~2011년 2월 : 고려대학교 정보보호대학원 박사과정 수료
2007년~현재 : 한국인터넷진흥원 보안관리팀 책임연구원
<관심분야> 정보보호, 클라우드 보안, 정보보호 관리체계 인증체계



고 규 만 (Ko Kym Man)
정회원

2002년 2월 : 연세대학교 컴퓨터과학과 석사
2007년 3월~2009년 2월 : 전남대학교 정보보호산학협동과정 박사 수료
<관심분야> (개인)정보보호 관리체계
2002년 1월~현재 : 한국인터넷진흥원 보안관리팀 책임연구원

이 재 일 (Lee Jae Il)
정회원

서울대학교 계산통계학과 학사
서울대학교 계산통계학과 석사
연세대학교 컴퓨터과학과 박사
1996년 6월 : 한국 IBM
1996년 7월~현재 : 한국인터넷진흥원 인터넷침해대응센터본부장
<관심분야> 정보보호