정보보호 준비도 평가 제도분석 및 발전방안

황명현*

전 산업영역으로 확대되고 있는 사이버 위협 속에서 정부의 노력에도 불구하고 영세 · 중소기업 및 非ICT 분야 등 정보보호 사각지대는 여전히 해소되지 않는 것이 현실이다. 우리 정부는 이미 ISMS 인증, PIMS 인증, PIPL 등의 정보보호 인증 제도를 마련하고 있지만, 이들 기업은 기업규모, 비용부담, 인식부족 등으로 인해 기존 정보보호 제도의 진입에 어려움을 겪고 있다. 기존의 진입장벽이 높은 인증제도가 아닌 효율적이고 안정적이면서 누구나 진입이 가능한 정보보호 제도가 사회적으로 요구되면서 정부는 민간주도의 「정보보호 준비도 평가」를 도입 · 시행 추진하였다.

본 기고에서는 민간 자율의 정보보호 준비도 평가의 필요성을 살펴보고 정보보호 준비도 평가의 등급모델, 평가기준, 평가방법을 소개하고 활성화 방안을 제시한다.

* 한국인터넷진흥원 정보보호관리팀 선임연구원(hwangmh@kisa.or.kr)

Ⅰ. 서론

'3.20 사이버테러',[1] '6.25 사이버공격',[2] 그리고 국내 기업들의 연이은 정보유출 사태 등 정보침해 사건들은 우리 사회 전체에 불안감을 조성하고 있다. 사이버 테러와 같은 정보침해는 서버 및 전산망 파괴, 정보유출 등으로 인한 직접적인 피해를 줄 뿐만 아니라 정보사회를 살아가는 국민들에게 불신을 안겨주어 사회적 갈등을 초래한다.

정부는 이런 문제점을 인식하고 2013년 4월 '정보보호산업 발전 종합대책',[3] 7월 '국가 사이버안보 종합대책',[4] 2014년 7월 '개인정보보호 정상화 대책',[5] 9월 '안전산업 육성 세부 이행계획'[6] 등 정보보호 및 개인정보보호를 위한 종합 대책을 마련하였다.

국회 또한 정보보호를 위한 지속적인 노력의 필요성과 정보보호 역량 강화를 위한 법적 근거를 마련하고자 「정보보호산업의 진흥에 관한 법률안」[7]을 발의하였다. 동 법률안은 정보보호 산업의 기반 구축과 경쟁력 강화, 정보보호 사각지대 해소 등을 통해 범국가적인 정보보호 인식 확산을 유도하고 안전한 사회를 구축하고자 하는 것이다. 한편, 2002년부터 시행되어온 정보보호 관리체계 인증은 2013년부터 주요정보통신서비스 제공자들을 법적 의무대상자로 포함시켜, 일정 규모 이상의 정보통신서비스 제공자는 사이버 침해사고 예방을 위해 적극적인 관심을 가지고 노력할 수 있도록 강제하고 있다.

그러나 이런 정부의 노력에도 불구하고 여전히 영세 · 중소기업 및 非ICT 분야 등 정보보호 사각지대는 해소되지 않고 있다. 정보보호 사각지대에 놓여 있는 많은 기업들은 정보보호의 중요성에 대한 인식 부족, 부족한 재정 등의 이유로 관리적 · 기술적 보호조치가 미흡한 상태이며 이로 인한 정보사고의 위험에 노출되어 있다. 이에 따라 정부는 정보보호 안심 사

1 웹서버 해킹 및 악성코드 삽입, 국내 방송, 금융사 서버 장악, 방송·금융사 내부 서버 및 PC에 악성코드 유포, 방송·금융 6개사 서버 및 PC 3만 2000여 대 마비된 사건.

2 좀비 PC를 확보하여 파급효과가 큰 국가기관의 운만을 집중적으로 DDos 공격을 했으며, 정부부처 및 언론사 및 기업 홈페이지 등의 해킹으로 사이버 테러로 일부 기업들이 피해를 입은 사건.

3 2013년 7월 4일 미래창조과학부.

4 2013년 7월 4일 미래창조과학부.

5 2014년 7월 31일 관계부처 합동.

6 2014년 9월 12일 관계부처 합동.

7 2014년 7월 7일 권은희 의원이 대표발의 하였으며, 정보보호 준비도 평가에 관한 내용을 포함하고 있음.

회 구현을 위해 2014년 2월「정보보호 등급 공시제」[8] 추진을 발표하고 8월「정보보호 준비도 평가」[9] 도입을 발표 했다. 이는 민간 주도로 국민 및 기업의 정보보호 인식강화와 정보보호 산업 활성화를 도모하고자 하는 것이다.

Ⅱ. 정보보호 준비도 평가의 도입배경 및 필요성

1. 정보보호 준비도 평가 도입배경

특정 기업을 대상으로 뚜렷한 목적을 가진 지능형지속공격(APT), 지속적인 분산서비스거부(DDoS)공격, 공공기관을 사칭한 피싱사이트 증가, 사회이슈 등을 활용한 악성코드 유포증가 등 사이버위협은 그 수법이 점차 지능화 · 고도화되고 있다. 또한, 이와 같은 사이버 위협은 비단 정보통신 분야의 기업뿐만 아니라 전 산업 영역의 기업으로 확대되고 있다.

사이버 위협이 확산되자 기업의 정보자산 보호, 침해사고 대응을 위한 정보보호 역량 강화의 필요성을 제기하였고, 이를 위해서는 정부뿐만이 아니라 범국가적 차원에서 정보보호 인식 수준의 향상이 필요했다. 우리 정부는 이미 정보보호 관리체계(ISMS) 인증, 개인정보보호 관리체계(PIMS) 인증, 개인정보보호 인증(PIPL) 등의 정보보호 인증 제도를 마련하고 있지만, 많은 기업들이 기업규모, 비용부담, 인식부족 등으로 인해 제도 진입에 어려움을 겪고 있다. 기업 역시 기존의 진입장벽이 높은 인증제도가 아닌 효율적이고 안정적이면서 누구나 진입이 가능한 정보보호 제도를 필요로 하고 있다.

정부는 이런 사회적 요구와 정보보호 패러다임의 변화를 충족시키기 위해 기업의 정보보호 자율규제 문화 정착 및 자발적인 보안역량 강화의 필요성을 인지하고 민간주도의「정보보호 준비도 평가」를 도입했다.「정보보호 준비도 평가」는 기업의 보안역량 강화를 위해 정보보호 준비 수준(Readiness)을 평가하여 준비등급을 부여하는 평가이다. 기업의 정보보호 수준에 따라 등급을 부여하여 이용자가 보다 안전한 기업을 선택할 수 있는 기준을 제공하고 이를 통해 기업 간 선의의 보안경쟁을 유발하는 등 민간이 자발적으로 정보보호 역량을 강화해

8 2014년 2월 17일 미래창조과학부.

9 디지털데일리(2014.8.14.), 미래부, 올해 말 민간 자율 '정보보호 준비도 평가제' 시행

나갈 수 있도록 유도하는 것을 목적으로 하고 있다. 또한, 대기업뿐만 아니라 영세 · 중소기업 및 非ICT 분야 등 업종 및 규모를 한정하고 있지 않아 정보보호 저변을 확대하고 보안 사각지대를 해소하고자 한다. 정부는 이를 통해 민간 자율적인 보안수준 향상으로 이어지는 정보보호 자율규제 문화의 정착을 기대하고 있다.

2. 민간자율 정보보호 제도의 필요성

「정보보호 준비도 평가」는 정부가 법 · 제도적인 수단으로 강제하는 정부 주도의 규제가 아니라 민간 주도의 자율규제로써 기업이 서비스나 신뢰도 제고를 위해 자발적으로 평가를 받도록하고 있다.

정부 주도의 규제는 법적 규제로서 책임과 의무가 따르게 되며 이행하지 않는 경우 법적인 강제집행이 수반된다. 또한, 집행과정에서 정부가 부담해야하는 감시비용, 집행비용 등이 발생하게 되므로 비용 및 규제범위의 한계로 인한 집행의 사각지대가 발생하게 된다. 또한 법적 강제성으로 인해 오히려 법망을 피해가려는 과다한 기회주의적 행위요인이 발생할 수 있다.[10] 정보보호 관리체계(ISMS) 인증의 경우 정부주도의 법률 규제에 해당 된다. 정보보호 관리체계(ISMS) 인증은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조에 의거 일정 규모 이상[11]의 기업에 대해 인증취득을 의무화 하고 인증 미취득시 1000만 원의 과태료를 부과하고 있다. 이는 일정규모 이상의 정보통신서비스 사업자들에 대한 정보보호 수준을 강제로 높일 수 있는 장치가 된다. 그러나 법적 의무화로 수행하다보니 기업의 정보보호 의지까지 끌어내기에는 한계가 있다. 또한 의무대상이 아닌 영세 기업이나 非ICT기업의 경우 정보보호 관리체계(ISMS) 인증을 받을 수는 있으나 해당 기업들이 구축하여 운영하기에는 개념, 용어, 프로세스 적용 등이 쉽지 않다.

정부 주도의 법적 규제와는 달리 자율규제는 규제의 주체가 정부가 아니고 정부규제에서 피규제자였던 개인 또는 기업 등이 규제의 주체가 되는 경우로, 사업자 또는 소비자보호를 위해서 또는 시장의 투명성과 신뢰를 확보하기 위해 스스로 행하는 자정노력으로서의 규제

10 한국콘텐츠진흥원, 온라인상 저작권보호를 위한 자율규제 활성화

11 전기통신사업법의 전기통신사업자로 전국적으로 정보통신망 서비스를 제공하는 사업자, 타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는 사업자, 정보통신서비스매출액 100억 또는 이용자 수 100만 명 이상인 사업자

활동이다.[12] 자율규제는 규제속도, 유연성, 시장상황에 대한 민감성, 저렴한 비용 등에서 장점이 있다. 「정보보호 준비도 평가」는 민간이 주체인 자율규제로서 정보보호 환경변화에 따른 유연성 확보가 가능하고 분야별 확장이 용이하여 신규기술 변화에 빠른 대처가 가능하다. 또한 「정보보호 준비도 평가」는 비용 및 규제범위의 한계가 없으므로 정부 주도의 법률 규제로서 해결하지 못하는 사각지대 해소의 역할을 수행하게 된다.

민간주도 자율 규제가 투명성, 신뢰성 확보가 담보되지 않는다면 이익만을 위한 활동으로 변질될 수 있다는 위험성도 안고 있다. 자율규제인 민간영역이 전통적인 정부영역에 해당되었던 규제영역에 적극적으로 참여하고, 정부영역은 이러한 민간영역의 활동과 역할에 대해서 적극적으로 협력 · 지원함으로써 규제의 합리화 및 효율성을 추구하는 규제가 된다면 정부에 의한 법적 규제와도 조화될 수 있을 것이다.[13] 법적규제와 자율규제의 상호조화를 통해 기업의 자발적 보안역량 강화를 유도하게 된다면 정보보호 인식확산과 정보보호 발전에는 더 큰 도움이 될 것이다.

〈표 1〉 규제 유형에 따른 비교 예시

구분	정보보호 관리체계 인증	정보보호 준비도 평가
규제형태	정부 주도 법률 규제	민간주도 자율규제
주체	정부	민간
대상	정보통신망법에 다른 일정 기준 이상의 의무대상자	영세 중소기업 및 非ICT 분야 등 정보보호 사각지대까지 포함
기준	고시에 따른 104개 기준 기준변경을 위해서는 고시 개정이 필요	30개의 기준 기술변화에 따른 유연한 대처가 가능하며 분야별 확장이 쉬움
미인증시 불이익	과태료 1000만 원	해당없음
부작용	법망을 피해가려는 기회주의적 행위 발생	기업이 자발적으로 참여할 수 있는 환경마련 필요

12 한국정보화진흥원, 인터넷기반서비스 내용규제 제도개선 방안연구, 2009, 41쪽

13 한국정보화진흥원, 전게 논문, 139쪽

Ⅲ. 정보보호 준비도 평가 등급모델 및 기준

1. 정보보호 준비도 평가 등급모델

「정보보호 준비도 평가」는 기업의 정보보호 인프라 확충 수준 및 정보보호활동 수행 여부 등을 고려하여 5단계의 등급으로 구분하고 있다. 준비도 평가 기준을 설계하면서 여러 차례의 시범평가를 수행하였으며 그 결과 정보보호 관리체계 인증을 받은 기업은 AA~AAA 사이의 등급이 예상됨을 확인하였다. 非ICT 기업 및 영세기업의 경우 B~BB 등급 또는 등급불가가 예상됨을 확인하였다. B, BB 등급의 경우에는 정보보호 활동에 대한 관리를 수행하고 있으며 기본적인 정보보호 준비가 된 상태인 기업을 의미한다. 정보보호에 대한 의지가 있고 어느 정도 노력을 하고 있는 기업이라면 B등급의 취득은 어렵지 않을 것이다. 그러나 A등급 이상의 경우에는 등급을 받기에 상당수준의 기준을 포함하고 있으며 BB등급에서 A등급으로 수준을 올리는 데에는 정보보호에 대한 적극적 관심 및 투자를 필요로 한다. 특히 AAA등급의 경우 정보보호 관리체계 인증을 받은 기업도 쉽게 받기는 어려운 수준으로 볼 수 있다. 정보보호 관련 인증 또는 평가를 처음 준비하는 기업은 B, BB 등급을 우선으로 목표로 하고 단계적으로 수준을 올리는 방식으로 접근할 필요가 있다. 정보보호 준비도 평가 등급 및 예상 기업은 〈표 2〉와 같다.

〈표 2〉 정보보호 준비도 평가 등급

등급	설명	예상기업
AAA	정보보호 준비 정도가 우량하며 환경변화 및 침해위협에 대한 예방적 대처까지 가능한 기업	국가 사회적 파급력이 큰 대국민서비스 제공 기업
AA	정보보호 준비 정도가 양호하며 환경변화 및 침해위협 시 적절한 대처가 가능한 기업	다량의 개인정보보유 기업
A	정보보호 준비 정도가 양호하나 환경변화 및 침해위협 정도에 따라 대처능력이 제한적인 기업	非ICT분야 대기업, 일정규모 이상의 정보통신 서비스 제공자
BB	정보보호 준비 정도가 보통이며 환경변화 및 침해위협 정도에 따라 대처능력이 제한적인 기업	인터넷을 이용해 주된 사업을 영위하는 ICT 분야 중소 · 중견 기업
B	기본적인 정보보호 관리활동이 준비된 기업	인터넷을 보조로 활용해 사업을 영위하는 非ICT 분야 중소 · 영세 기업

2. 정보보호 준비도 평가 기준 및 평가 방법

「정보보호 준비도 평가」는 필수항목(기반지표 · 활동지표)과 선택항목으로 구성되어 있다.

필수항목은 기반지표와 활동지표로 구성되어 있으며 등급을 결정하는 주요 지표가 된다. 기반지표는 정보보호 리더쉽과 자원관리항목으로 구성되어 있으며 정보보호를 수행할 수 있는 환경마련에 중점을 두고 있다. 활동지표는 관리적, 물리적, 기술적 정보보호 활동 현황에 대한 지표이며 실질적인 정보보호 행위에 대하여 평가한다. 선택항목은 선택적으로 적용할 수 있는 지표로서 금융, 교육, 의료 및 기타 산업별 요구사항에 맞추어 필수지표에 추가하여 평가할 수 있는 지표이다. 현재 선택지표는 개인정보보호 지표만을 포함하고 있으나 향후 산업별 요구사항에 맞는 선택지표를 확장 가능하도록 설계하였다. 〈표 3〉은 기반지표, 활동지표, 선택지표를 구분한 표이다.

〈표 3〉 정보보호 준비도 평가 지표 구분

구분	설명	주요항목
기반지표 (필수)	정보보호 정책 · 경영 · 의사결정 구조(리더십)와 보안투자 및 인력 · 조직 등 필수적인 보안 인프라(자원관리)를 평가(7개)	정보보호 최고책임자의 자격 및 역할, 정보보호 의사결정 과정 · 구조, 정보보호 계획 수립 · 이행, 정보보호 예산 및 집행, 정보보호 인력 · 조직 보유 등
활동지표 (필수)	관리적 · 물리적 · 기술적 정보보호조치 현황 및 체계적인 보안활동 수행 여부를 평가(16개)	연간 임직원 정보보호 교육(횟수, 시간), 내 · 외부자 보안관리, 연간 취약점 점검 수준 및 횟수, 침해사고 대응체계(모의훈련 실시 등) 구축, 백업 및 복구체계 구축
선택지표	선택지표는 기업이 선택 할 수 있는 지표로서 금융, 교육, 의료 및 기타 산업별 요구사항에 대하여 확장가능하게 운영할 수 있도록 설계	개인정보보호 지표의 경우 「개인정보보호법」및 「정보통신망법」에서 규정하는 개인정보보호 필수항목에 대한 준수 여부를 평가(7개)

필수 지표인 기반지표 및 활동지표는 23개의 세부 평가지표로 구성되어 있으며 각 세부 평가지표는 점수를 가진다. 선택지표인 개인정보보호는 7개의 세부 평가지표로 구성되어 있으며 점수 형태가 아닌 Pass or Fail 구조이다. 이는 개인정보보호는 법적 요구사항이라 점수화하여 구현하는데 어려움이 있음을 반영한 것이다. 정보보호 준비도 평가기준은 정보보호 관리체계(ISMS) 인증 심사항목(104개) 대비 경량화된 평가기준으로 개발하였다. 이는 평가에 소요되는 비용 · 인력 절감을 통해 평가 자체에 대한 기업의 부담을 완화하기 위함이다. 정보보호 관리체계 인증이 보안활동 별 계획수립 및 실행과 이에 따른 보완 · 개선 사항 등 프로세스 전반에 걸쳐 심사하는 방식이라면, 정보보호 준비도 평가는 객관적인 기준에 따라 보안활동의 특정 시점 또는 행위를 중심으로 평가하여 평가기간 및 인력을 단축시켰다.

〈표 4〉 정보보호 준비도 평가 세부 평가지표

지표	구분	세부 평가지표		점수
기반지표	1. 정보보호 리더십	1.1	정보보호 최고책임자(CISO) 지정	5
		1.2	정보보호 의사소통 및 정보제공	5
		1.3	정보보호 운영방침	4
	2. 정보보호 자원관리	2.1	정보보호 추진계획	4
		2.2	정보보호 인력 및 조직	4
		2.3	정보보호 예산 수립 및 집행	4
		2.4	정보보호 이행점검	4
활동지표	1. 관리적 보호활동	1.1	정보보호 교육 수행	5
		1.2	자산관리	4
		1.3	인적보안	4
		1.4	외부자 보안	5
	2. 물리적 보호활동	2.1	정보통신시설의 환경 보안	4
		2.2	정보통신시설의 출입 관리	4
		2.3	사무실 보안	4
	3. 기술적 보호활동	3.1	취약점 점검	5
		3.2	정보보호 사고탐지 및 대응	5
		3.3	시스템 개발 보안	4
		3.4	네트워크 보안	4
		3.5	정보시스템 및 응용프로그램 인증	5
		3.6	자료유출 방지	4
		3.7	시스템 및 서비스 운영 보안	5
		3.8	백업 및 IT재해복구	4
		3.9	PC 및 모바일기기 보안	4
	합계			100
선택지표	개인정보보호	1	개인정보 최소수집	P
		2	개인정보 수집 고지 및 동의획득	P
		3	개인정보취급방침	P
		4	이용자 권리 보호	P
		5	개인정보의 관리적 보호조치	P
		6	개인정보의 기술적 보호조치	P
		7	개인정보 파기	P

정보보호 준비도 평가기준 개발 초기에는 정보보호 성숙도 측면에서 접근하였다. 그러나 평가기준 개발 단계에서 기업을 대상으로 시범평가를 수행한 결과 국내 기업 현실에서는 정보보호 활동이 단계적인 수준으로 적용되는 기업은 많지 않았다. 낮은 수준의 정보보호 활동을 수행하고 있지 않으나 높은 수준의 정보보호 활동은 수행하고 있어 성숙도와는 반대되는 보안활동 형태가 발생하여 성숙도 산정에 어려움이 있었다. 이에 따라 국내 기업에서는 정보

보호 수준을 성숙도 측면에서 접근하기에는 어려움이 있다는 결론을 내리게 되었다. 그 결과 정보보호 준비도 평가기준은 기존의 성숙도 측면이 아닌 활동중심의 항목으로 재구성하고 항목별 점수화하여 점수를 충족하는 방식으로 구현하였다.

〈표 5〉는 기반지표의 '1. 정보보호 리더십' 항목의 세부 평가지표 및 평가내용의 일부분이다. 평가내용을 보면 각 항목마다 세부배점이 있으며 평가내용의 활동 정도에 따라 세부 점수를 할당하게 된다.

〈표 5〉 기반지표의 세부 평가지표 및 평가내용 예시

구분	세부 평가지표		평가내용	배점	평가점수
1. 정보보호 리더십	1.2 정보보호 의사소통 및 정보제공	정보보호에 관한 의사소통 및 정보제공이 이루어지는가?	정보보호조직(또는 담당자)은 임직원에게 주기적으로 정보보호 관련 정보를 제공(뉴스레터, 정보보안 실천퀴즈, 정보보안 실천가이드 등)하고 있다. (반기1회 : 0.5점 분기1회 : 1점)	1	
			정보보호 기술, 관련 법률에 대한 외부 전문가 자문 또는 인증(준비도 평가 제외)을 연 1회 이상 수행하고 있다.	1	
			정보보호 관련 담당자와 이해관련 부서의 실무자가 정보보호 관련 사항에 대해 주기적인 의사소통 활동을 수행하고 있다. (반기1회 : 0.5점 분기1회 : 1점)	1	
			정보보호최고책임자와 경영진 또는 이해관련 부서 책임자가 참여하여 주요 정보보호 사안을 결정하는 자리를 정기적으로 마련하고 있다. (반기1회 : 0.5점 분기1회 : 1점)	1	
			최고경영자(CEO)에게 정보보호활동 보고를 정기적으로 수행하는 등 최고경영자와 정보보호조직(또는 담당자)간의 주기적인 의사소통을 하고 있다. (반기1회 : 0.5점 분기1회 : 1점)	1	
			합계	5	
	1.3 정보보호 운영방침	국내외 관련 규정을 검토하여 정보보호 운영방침(또는 정책, 지침 등)을 정하고 모든 구성원에게 공표하는가?	정보보호 운영방침을 문서화하고 있으며 다음의 사항을 포함하고 있다. 경영진의 정보보호 운영방침 준수의지(0.25) 정보보호 관련 법규에서 요구하는 정보보호 준수사항(0.25) 관리적인 측면의 정보보호 준수사항(0.25) 기술적인 측면의 정보보호 준수사항(0.25)	1	
			정보보호 운영방침은 최고경영자 서명과 시행일을 명기하여 공표하고 모든 구성원이 쉽게 접할 수 있는 방식으로 공개하고 있다.	1	
			정보보호최고책임자는 조직의 운영방침 적합여부 및 법령의 변화 등을 확인하여 연1회 이상 개정하고 있다.	1	
			문서화된 인사규정 등에 정보보호운영방침 위반에 따른 상벌규정을 명시 및 시행하고 있다.	1	
			합계	4	

〈표 6〉은 활동지표의 '1. 관리적 보호활동' 항목의 세부 평가지표 및 평가내용의 일부분이다.

〈표 6〉 활동지표의 세부 평가지표 및 평가내용 예시

구분	세부 평가지표		평가내용	배점	평가점수
1. 관리적 보호활동	1.1 정보보호 교육 수행	전체 임직원을 대상으로 정보보호 교육을 수행하는가?	교육대상, 교육시간, 교육방법, 교육내용, 불참자 관리방안 등을 포함한 연간 정보보호 교육계획을 수립하고 이에 따라 교육을 수행하고 있다. (계획대비 70%이상 : 0.5점, 90%이상 : 1점)	1	
			전체 임직원 및 외부위탁사를 대상으로 정보보호 교육을 수행하고 있다. – 주요 업무수행자 대상 정보보호 교육수행(0.3점) – 전체 임직원 대상 정보보호 교육수행(0.6점), – 외부위탁사 포함 정보보호 교육수행(1점)	1	
			정보보호 교육의 내용을 대상자의 직위 및 업무 특성에 따라 구분하여 수행하고 있다. 일반직원 대상 정보보호 교육(0.25) 임원 대상 정보보호 교육(0.25) 정보기술부문 직원대상 정보보호 교육(0.25) 외부 위탁사 대상 정보보호 교육(0.25)	1	
			정보보호 교육 참여율, 만족도, 개선사항을 포함한 교육 결과 보고서를 작성하여 정보보호 최고책임자에게 보고하고 있다. (단순보고 0.3점, 참여율 70%이상: 0.5점, 90%이상: 1점)	1	
			전체 임직원의 교육 참여율을 높이기 위하여 인센티브 또는 제재 방안을 마련하여 시행하고 있다.	1	
			합계	5	

준비도 등급 산정은 각 평가내용에 따른 평가점수를 모두 합산하여 준비등급을 부여한다. 등급은 점수 별로 구간을 두고 부여하게 되며 항목별 정보보호 수준의 균형을 맞추기 위해 항목별 최소점수를 반영하고 있다. B등급 이상의 경우 23점 이상의 점수를 받아야 하며 23개의 세부 평가지표의 모든 항목을 1점 이상 충족하여야 한다. A등급 이상의 경우 60점 이상의 점수를 받아야 하며 23개 세부 평가지표의 모든 항목을 2점 이상 반드시 충족하여야 한다. 선택지표인 개인정보보호 항목은 별도의 점수 배점이 없으며 전체 항목을 만족하여야 P(ass)가 부여된다. 기준 충족여부를 평가한 후 준비등급에 'P'를 표시하게 된다.

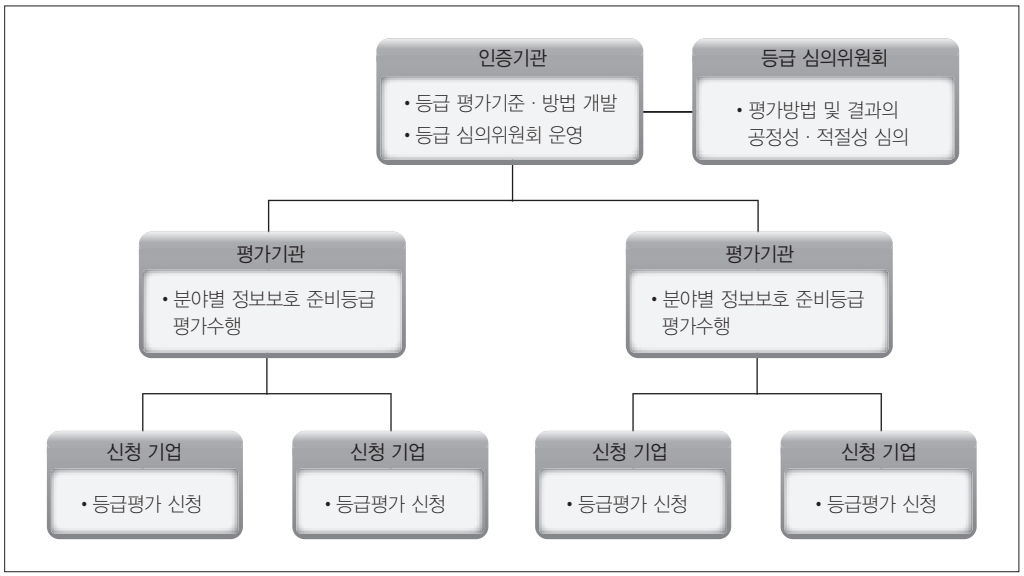
〈표 7〉 정보보호 준비도 평가 점수별 등급

환산점수	100 ~ 90점	89 ~ 80점	79 ~ 60점	59 ~ 40점	39 ~ 23점	개인정보보호
준비등급	AAA	AA	A	BB	B	P

Ⅳ. 정보보호 준비도 평가 사업화 현황

「정보보호 준비도 평가」는 한국인터넷진흥원이 등급모델, 평가기준 · 방법 등을 설계 및 개발하고 민간에 기술이전[14]하는 방식으로 사업화를 진행하였다. 기술이전을 위해 정보보호 유관 민간단체 및 기업을 대상으로 기술이전 및 사업화과제 공모[15]를 위한 기술설명회를 개최하였으며 한국정보방송통신대연합(ICT대연합), 한국정보통신기술협회(TTA), 한국정보통신진흥협회(KAIT), 한국침해사고대응팀협의회(CONCERT)가 수행기업으로 선정되었다.

평가체계는 평가기관과 인증기관으로 나누어 운영된다. 평가기관은 정보보호 준비도를 평가하는 업무를 전담하며, 인증기관은 평가결과에 대한 최종 검증 · 심의를 거쳐 준비등급을 부여하는 역할을 한다. 또한 평가결과의 최종 검증 · 심의를 담당하는 「등급 심의위원회」를 외부전문가로 구성하여 등급부여의 공정성과 투명성을 강화하였다. 인증기관은 한국정보방송통신대연합(ICT대연합)이 수행하고 있으며 평가기관은 정보통신기술협회(TTA), 한국정보통신진흥협회(KAIT), 한국침해사고대응팀협의회(CONCERT)가 수행한다.



[그림 1] 정보보호 준비도 평가 사업운영 체계

14 중소기업 등의 기술 경쟁력 강화 및 미활용 기술의 활용을 확대를 목적으로 출연연 또는 공공기관이 보유한 특허 및 기술(무형의 지재권 포함) 등을 기업에 양도

15 기술이전 양수기관(수행기관)의 안정적인 제도 운영을 검증하기 위하여, '사업화 과제 공모'를 통해 수행능력 및 운영계획, 향후 발전방안 등에 대한 평가를 실시

한국인터넷진흥원은 이들 기업과 기술이전 계약을 마친 상태이다. 선정된 기업은 본격적인 제도 시행에 따른 홍보 등을 위하여 정보보호 준비도 평가 출범식을 10월에 개최[16]하였으며 11월부터 본격적으로 기업을 대상으로 평가를 수행하고 있다. 2014년 기준 189명의 평가사를 양성하였으며 19개 기업이 평가를 받은 상태이다.

Ⅴ. 정보보호 준비도 평가 활성화를 위한 향후 과제

이제 첫걸음을 시작한 정보보호 준비도 평가가 민간자율 정보보호 평가제도로서 성공적으로 자리매김 하기 위해서는 다양한 시각에서의 노력이 필요하다. 우선 준비도 평가의 활용도를 높일 수 있는 방안을 연구하여야 한다. 준비도 평가의 활성화를 위해서는 기업이 쉽게 접근할 수 있는 환경이 갖춰져야 한다. 건강검진과 같이 기업이 정기적으로 기업의 정보보호 상태를 검진할 수 있는 진단도구로 활용될 수 있도록 홍보되어야 할 것이다. 또한 중소기업이 정보보호 준비도 평가에 관심을 가질 수 있는 기본여건을 마련하여야 한다. 이를 위해서는 관련 기관과 연계하여 정보보호 관련 전문성이 부족한 중소기업 담당자들도 준비도 평가를 준비할 수 있도록 교육이나 관련 자료들을 보급하는 활동이 필요하다.

규모가 크고 협력사 및 수탁사가 많은 기업은 수탁사 또는 협력사의 정보보호 수준관리에 대한 어려움이 많다. 수탁사 또는 협력사에 대한 점검의 방법으로 정보보호 준비도 평가를 이용하는 것도 좋은 활용 안이 될 것이다. 정보보호 준비도 평가는 선택지표를 추가할 수 있어 기업이 특정 요구사항을 추가한 형태의 평가가 가능하다. 추가 점검항목을 선택항목으로 의뢰하고 필수항목과 선택항목을 포함하여 수탁사 또는 협력사가 점검받을 수 있도록 활용한다면 규모가 크고 협력사 및 수탁사가 많은 기업의 경우 관리를 위한 노력과 비용을 절감할 수 있을 것이다. 개인정보관련 법률이 강화되어 수탁사가 법률을 위반한 경우에도 업무를 위탁한 기업이 책임져야하므로 정보보호 준비도 평가는 수탁사 정보보호 점검을 위해서 좋은 도구가 될 수 있다.

평가와 인증은 공정성과 신뢰성이 담보가 되어야 한다. 그러나 민간 주도의 평가 및 인증은 수익과 연계되어 있어 이익을 위한 활동으로 변질될 수 있는 위험성을 항상 안고 있다. 인

16 매일경제(2014.10.29), ICT대연합, 민간 자율 정보보호 준비도 평가 시행

증 또는 평가기관이 이익을 위해 공정성과 신뢰성을 져버린다면 부실평가가 될 수밖에 없다. 실제 민간 인증제도의 경우 인증서 남발 등으로 인한 부작용 사례로 기사화[17]된 적이 있다. 그러므로 평가 및 인증기관은 스스로 자정작용을 할 수 있는 체계를 갖추고 지속적으로 유지할 수 있는 노력을 하여야 한다. 예를 들어 중앙일보 대학평가, 한국능률협회컨설팅(KMAC)이 주관하는 한국산업의 고객만족도(KCSI) 조사의 경우 민간에서 운영하지만 꾸준히 신뢰받고 운영되는 사례가 된다. 더불어 평가 및 인증기관이 전문성을 갖추어 정보보호 기술변화, 산업분야의 다양성 등을 고려한 지속적이고 적극적인 기준개선작업을 수행한다면 국민이 신뢰할 수 있는 평가가 될 수 있을 것이다.

마지막으로 정부가 민간 자율 정보보호 제도의 활성화를 위해 정보보호 준비도 평가의 활동과 역할에 대해서 적극적으로 협력하고 지원하게 된다면 운영의 효율성이 갖춰져 더 큰 기폭제가 될 것이다. 그 첫 번째가 정보보호 공시제도[18]이다. 기업의 신용평가와 같이 정보보호 공시제도가 시행 된다면 기업이 적극적으로 관심을 가질 수 있는 환경이 마련될 것이다. 또한 대기업이 자발적으로 참여하게 되므로 협력업체와 경쟁업체가 따라올 수 있게 된다. 또한 공시를 통해 선의의 경쟁을 유도할 수 있으며 기업이 협력사, 수탁사와 계약 시 사전에 보안수준을 확인 할 수 있게 되므로 많은 기업들이 정보보호 수준을 높이기 위해 더욱 노력할 것이다. 두 번째는 인센티브이다. 정보보호 준비도 평가는 의무제도가 아니므로 기업의 자발적인 준비등급 취득을 유도하기 위하여 인센티브가 필요하다. 인센티브는 경영진의 관심을 높일 수 있어야 하고 혜택 또한 다양화되어야 한다. 정부의 정보보호 투자활성화 대책[19]에 정보보호 준비도 평가를 받은 기업에 대한 혜택을 포함시켜 정보보호를 위해 노력하는 기업이 다양한 혜택을 받을 수 있도록 노력할 필요가 있다.

본고에서는 정보보호 준비도 평가의 필요성과 기준 및 평가방법을 살펴보고 그 활성화 방안을 알아보았다. 이제 첫걸음을 시작한 정보보호 준비도 평가의 성공적인 정착을 위해서는 지속적인 관심과 노력이 필요하다. 해당 노력이 수반된다면 정보보호 준비도 평가로 인해 기업의 정보보호 인식 확산과 수준향상에 도움이 될 것으로 기대한다.

---

17 서울신문(2009.3.21), ISO 인증 발급도 관리도 엉터리
전자신문(2013.11.27), 내년 1월부터 ISO 부실인증 기관에 법적 조치
파이낸셜뉴스(2013.10.23), 친환경농산물 부실 인증 처벌 강화

18 연합뉴스(2014.6.17), 기업 보안수준 공개 '보안등급 공시제' 도입 추진

19 이데일리(2014.7.31), 정부, 정보보호 투자 활성화 대책 "2017년까지 시장규모 2배"

참고문헌

디지털데일리 (2014.8.14.). 미래부, 올해 말 민간 자율 '정보보호 준비도 평가제' 시행
보안뉴스 (2014.10.20). 전문가 7인이 말하는 '정보보호 준비도 평가' 개선방안
매일경제 (2014.10.29). ICT대연합, 민간 자율 정보보호 준비도 평가 시행
서울신문 (2009.3.21). ISO 인증 발급도 관리도 엉터리
연합뉴스 (2014.6.17). 기업 보안수준 공개 '보안등급 공시제' 도입 추진
이데일리 (2014.7.31). 정부, 정보보호 투자 활성화 대책 "2017년까지 시장규모 2배"
전자신문 (2013.11.27). 내년 1월부터 ISO 부실인증 기관에 법적 조치
파이낸셜뉴스 (2013.10.23). 친환경농산물 부실 인증 처벌 강화
한국인터넷진흥원 (2014). 정보보호 등급모델 개발 및 표준화 추진
한국인터넷진흥원 (2014). 정보보호 준비도 평가 사업화 방안 연구
한국콘텐츠진흥원 (2010). 온라인상 저작권보호를 위한 자율규제 활성화