SMART 평가법을 활용한 정보보호 관리체계(ISMS) 인증 의무대상자 선정 기준 개선 방안에 관한 연구

장상수*

요 약

2004년 도입된 정보보호 안전진단 제도는 2013년에 실효성이 보다 높은 정보보호 관리체계(ISMS) 제도로 일원화를 하였다. 기존 권고형태의 정보보호 관리체계 인증 제도가 일정 규모 이상 정보통신서비스제공자에게 의무화가 된 것이다. 이는 인터넷 침해사고로 국민생활에 영향을 미치는 정보통신서비스제공자를 대상으로 하기 때문에 책임성 등을 고려하여 의무대상자의 선정 기준을 명확히 할 필요가 있다. 그러나 현행 법 규정상 의무대상자 선정 기준 자체가 모호하여 법 적용하는데 상당한 문제가 야기 되고 있다. 더욱이 규제 제도인 인증 제도는 대상자 선정 기준이 명확해야 함에도 불구하고 객관적이지 않아 의무대상자가 제도 자체에 대한 불신과 많은 문제 제기를 하고 있다. 본 연구에서는 이를 개선하기 위하여 SMART 평가법을 적용하여 인증 의무대상자 여부를 쉽게 판단 할 수 있도록 인증 의무대상자 선정 모델을 개발하고, 개발된 모델을 통하여 실증적으로 타당성을 검증하여 제도 개선 방안을 제시하여 제도의 실효성 확보에 도움을 주고자 한다.

A Study on The Improved Selection Method of Information Security Management System(ISMS) Certification Object Applying SMART Technic

Jang Sang Soo*

ABSTRACT

Information Security Check System was Introduced in 2004, higher than in 2013, the effectiveness of Information Security Management System(ISMS) certification scheme was to unification. This is incident to the Internet affecting people's lives telecommunications service provider to target accountability because, considering the subject's duty selection criteria need to be clarified. however, Obligations under the current legislation, subject selection criteria applying the law itself is ambiguous, the result being a significant problem. Moreover, the regulatory system of certification systems subjects, although selection criteria should be clear and objectively not the obligation not to distrust the system itself and the subject was raised many issues for you. In this study, with SMART Technic in order to improve this certification you can easily determine whether a medical person authorized to develop a model for selection of medical subjects, The developed model is verified through empirical ways to improve the system by presenting the system to help, to secure the effectiveness.

Key words : SMART, ISMS, Information Security Check System, Certification Scheme, Selection Criteria, ISP, IDC.

접수일(2014년 5월 23일), 수정일(1차: 2014년 6월 27일, 2차: 2014년 6월 29일), 게재확정일(2014년 6월 30일)

* 아주대학교/지식정보보안학과

1. 서 론

2004년도 도입된 정보보호 안전진단 제도는 정보통신망 안정성 확보, 기업 정보보호 수준 제고, 정보보호 산업 활성화 등의 많은 성과를 거두었으나, 최소한의 보호조치만 의무적으로 점검하려는 태생적인 한계와 규모 및 업종별 정보통신서비스 제공자의 특성을 반영하기 어려운 점, 안전진단의 연말 쏠림으로 인한 부실진단 가능성, 나날이 진화하는 신종 침해사고 위협에 선제적·능동적으로 대처하기 어려움 등에 대한 문제점이 지속적으로 제기 되었다. 이에 따라 2013년부터 기존에 운영되던 정보보호 관리체계 제도는 폐지되고, 정보보호 관리체계(ISMS : Information Security Management System) 인증을 『정보통신망이용촉진 및 정보보호 등에 관한 법률』(이하 「정보통신망법」이라한다)개정을 통해 의무화(2013.2.18 시행)하였다. 보다 높은 수준의 ISMS 인증 제도로 일원화한 것이다[3,4].

인증대상자는 ISMS를 수립·운영하고 있는 조직으로, 자율적으로 인증심사를 희망하는 자율신청기관과 법에서 정한 의무대상자로 구분된다. 자율신청기관은「정보통신망법」제47조제1항에 의거하여 관리체계를 수립·운영하고 있는 기업(의료, 교육, 산업기밀 등 모든 산업 분야 포함)이 해당된다. 의무대상자의 경우 주요정보통신서비스제공자(ISP), 집적정보통신시설사업자(IDC), 정보통신서비스제공자(쇼핑몰 등)등으로 3가지 군으로 분류하고 있다[3,4].

ISP, IDC의 경우 일정규모를 고려하고 있지 않아 침해사고시에 영향이 미미한 소규모 시설을 보유하고 있는 영세업체가 포함되 공평성 문제를 가지고 있으며, 법 취지상 모든 인증 대상자는 모든 정보통신서비스제공자를 대상으로 하기 때문에 대상자 선정 기준을 서비스로 분류하는 것은 적합하지 않다. 또한 선정기준인 정보통신서비스 부문 전년도 매출액, 일일평균 이용자로 한정하고 있어 실질적으로 많은 업체가 의무 대상자임에도 빠지게 되어 대상자들로부터 선정기준의 형평성, 공평성에 대한 문제제기를 해오고 있다. 본 논문에서는 인증 의무대상자가 쉽게 본인들이 대상임을 인지하고 또한 정부에서도 보다 객관적이고 공정한 인증 의무대상자를 선정하고 인증을 받도록 의무대상자 기준 개선안을 제시하고자 하였다. 이를 위해 2013년도 인증 의무대상자 298개 업체를 대상으로 설문조사를 통해, 인증 의무대상자 여부를 쉽게 판단 할 수 있도록 인증 의무대상자 선정 모델을 개발하고, 개발된 모델을 통하여 실증적으로 타당성을 검증하여 제도 개선 방안을 제시하여 제도의 실효성 확보에 도움을 주고자 한다[3,4].

2. 관련 연구

2.1 기존 인증 의무대상자 선정 기준

인증 의무대상자의 경우는 2013년 2월 18일부터 법 개정을 통해 인터넷에 중대한 영향을 끼칠 수 있는 정보통신서비스제공자 중에서 ISP·IDC·대규모 쇼핑몰 및 포털 등의 일정규모 이상의 주요 정보통신서비스 제공자는 「정보통신망법」제47조제2항에 의거하여 의무대상자로 지정하여 관리체계를 구축하고 인증을 받아야 한다. 의무대상자의 세부적인 기준은 다음과 같다[1].

① 정보통신망서비스를 제공하는 자 (「정보통신망법」 제47조제2항제1호)
정보통신망서비스를 제공하는 자(ISP)란「전기통신사업법」제6조제1항에 따른 기간통신사업 허가를 받은 자로서, '서울특별시 및 모든 광역시'에서 정보통신망서비스를 제공하는 자를 말한다.

② 집적정보통신시설사업자 (「정보통신망법」 제47조제2항제2호)
집적정보통신시설사업자(IDC)란 타인의 정보통신서비스 제공을 위하여 자체적으로 집적된 정보통신시설을 구축하여 운영·관리하는 사업자를 말한다. 다만, 타인에 의해 구축된 집적정보통신시설의 일부를 임대하여 서비스를 재판매하는 사업자(VIDC)의 경우에는 「정보통신망법」제47조제2항제3호의 기준을 적용하여 연간 매출액 100억원 이상 또는 일평균 이용자수 100만명 이상인 자만 의무대상자에 해당한다.

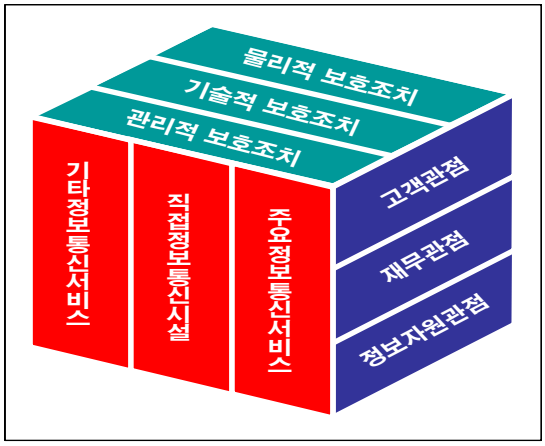
③ 연간 매출액 또는 이용자수 등이 대통령령으로 정하는 기준에 해당하는 자 (「정보통신망법」제47조제2항제3호, 시행령 제49조)

- 정보통신서비스 부문 전년도 매출액이 100억원 이상인 자
- 전년도 말 기준 직전 3개월간의 일일평균 이용자수가 100만명 이상인 자

이와 같이「정보통신망법」상 기존 인증 의무대상자 기준은 획일적이며 다양하지 못하고 구체적인 해설이나 기준이 없어 해당 이해당사자간의 많은 혼란을 야기하고 있다.

2.2 인증 의무대상자 선정 기준 개선 모형

본 연구에서는 인증 의무대상자 선정을 위한 모형을 개발하고, 이 모형을 기반으로 인증 의무대상자가 보다 명확한 기준하에서 법규를 준수할 수 있도록 하고 기업의 노력과 수고가 헛되지 않도록 정보통신망의 안정성 및 정보의 신뢰성 확보라는 제도의 취지를 고려하였다. 또한 법 규정에서 정의하고 있는 의무대상자 기준을 보다 객관적이고 명확한 기준을 마련하기 위해 인증 의무대상자 선정 모델은 대상자 선정에 영향을 미칠 수 있는 요소로 정보통신서비스 영역, 정보보호지침(물리적, 기술적, 관리적 보호조치) 영역, 대상자 선정 기준 영역 등 3가지 주요 요소를 선정 모델로 설정하여 분석한다. 대상자 선정 기준 모델은 가장 중요한 요소로 판단되는 입법 취지 부합성, 산출방법의 객관성, 개인정보 취급 연관성, 자료 확보의 가능성 등을 고려하였다. 제도 취지상 많은 기업들이 정보보호 관리체계를 구축하고 인증을 받도록 하여 침해사고에 대한 예방 및 대응 능력을 제고하고자 대상자 선정 기준을 보다 객관적이고 다양한 접근 방법을 고려하였다. 특히, 대상자 선정을 위한 관점에서는 고객관점(이용자수, 고객(회원수), 재무관점(총매출액, 정보통신매출액), 정보자산 관점(보유설비수, 종업원수) 등에 대하여 세부적인 내용을 분석하여 의무대상자 선정 모델을 개발하였다. (그림 1)은 정보보호 관리체계 의무대상자 선정 모델을 제시하고 있다.



(그림 1) ISMS 의무대상자 선정 모델

2.2.1 보호조치영역(인증심사기준)

보호조치 영역인(물리적, 기술적, 관리적 보호조치) 인증심사 기준 측면에서는 <표 1>과 같이 대상에 따라 분야별 또는 서비스별 준수해야할 보호대책들은 별도로 분류하고 있지 않으며, 업종이나 서비스 구분 없이 모두 적용 가능하도록 설계되었다. 위험관리를 통해 대상자가 스스로 수준에 맞도록 통제항목을 선택하는 방식이다. 따라서 보호조치 영역인 인증심사기준은 대상자 선정에 영향을 미치지 않는 것으로 분석되었다[2].

<표 1> 인증심사기준

분야		통제 항목 수	세부 점검 항목
관리적	1. 정보보호 정책 수립 및 범위설정	2	4
	2. 경영진 책임 및 조직구성	2	4
	3. 위험 관리	3	11
	4. 정보보호대책 구현	2	3
	5. 사후관리	3	6
	1. 정보보호 정책	6	13
	2. 정보보호 조직	4	7
	3. 외부자 보안	3	4
	4. 정보자산분류	3	7
	5. 정보보호 교육	4	10
	6. 인적 보안	5	11

물리적	7. 물리적 보안	9	21
기술적	8. 시스템 개발 보안	10	22
	9. 암호통제	2	8
	10. 접근통제	14	46
	11. 운영 보안	22	56
	12. 침해사고 관리	7	14
	13. IT재해복구	3	6
총계		104	253

2.2.2 대상자의 정보통신 서비스 범위 영역

2013년도 의무 인증 대상자 중에서 의무대상 범위를 서비스별로 구분하면 <표 2>와 같이 분류할 수 있다. 정보통신서비스 영역은 「정보통신망법」상의 대상서비스는 크게 ISP, IDC, 쇼핑몰 등을 분류하고 있으나, ISP나 IDC에 대한 서비스 구분은 오히려 혼란을 줄 수 있고 기존 정보통신서비스매출액이나 이용자수 기준에 모두 포함되고 있으므로 별도로 구분할 필요가 없는 것으로 분석되었다[3].

<표 2> ISMS 의무대상자의 서비스 범위

서비스	수단 및 기능	형태	서비스 내역	대상자 영역
기간통신	주요정보통신서비스제공자	초고속 인터넷 서비스	케이블 모뎀 서비스	ISP
			xDSL 서비스	
			기타 초고속 인터넷 서비스	
		초고속 가입자망 서비스		
		기타 초고속 통신 서비스		
		무선데이터접속 서비스		
부가통신	직접정보통신시설사업자	서버호스팅		IDC
		스토리지호스팅		
		코로케이션		
		네트워크 제공 서비스(회선임대포함) 등		
부가통신	쇼핑몰 등	인터넷접속 기반서비스		매출액 또는 이용자수
		카드조회. 지불중계 등		
		컴퓨터예약(CRS) 서비스		
		전자문서교환(EDI)		
		네트워크 제공 서비스		
		인터넷 포털 서비스		
		인터넷 전자상거래		
		신문/방송, 음악/교육 등		
		인터넷 게임		
		기타 인터넷 정보제공 서비스		
	유선방송	Cable-SO 등		

2.2.3 대상자 선정 기준 영역

대상자 선정 기준 관점에서는 고객관점, 재무관점, 정보자원관점으로 분류하고 전문가의 검토를 통해 추가적인 대상선정의 다양한 방법으로 후보 기준항목을 도출하였다. 또한 선정 기준항목이 신뢰성, 파악 용이성, 객관성, 공정성, 투명성 등이 중요한 요소로 이를 고려하였다. 또한 ISP, IDC 분류는 대상 범위의 서비스로만 분류하고 대상자 선정기준으로는 적합하지 않아 새로 제시하는 대상선정 기준안으로 포함하였다. ISP, IDC 기준을 제외하고 기존 정보통신서비스매출액과 이용자수 이외 총 매출액, 정보통신설비수 등 <표 3>과 같이 10개의 대상선정 기준(안)을 도출하였다[3].

<표 3> 대상자 선정 기준(안) 도출

구분	선정 기준(안)	정의	비고
고객관점	고객 회원수	정보통신서비스를 제공받기 위해서 등록한 회원수 또는 개인정보 보유 건수	추가
	일일 이용자수	전년도 말 이전 3개월간의 평균 일일 이용자수	기존
재무관점	총매출액	직전년도 연간 총매출액	추가

	정보통신서비스 매출액	정보통신서비스부문 연간 매출액	기존
	정보화 투자액	직전년도 IT 업무에 투자한 투자액	추가
	정보보호투자액	직전년도 정보보호 업무에 투자한 투자액	추가
	거래 건수	온라인 상의 모든 상거래 행위 건수	추가
정보자산 관점	총 종업원수 (직원)	직전년도 상시근무 직원수	추가
	정보통신 직원수	직전년도 정보통신 분야 전담 직원수	추가
	정보보호 직원수	직전년도 정보보호 분야 전담 직원수	추가
	정보보호대상 정보통신 설비수	정보보호대상 정보통신설비 총 보유수	추가
	인터넷 회선 용량	인터넷 회선 접속 총 용량	추가

2.3 인증 의무대상자 선정 기준 개선안 평가

본 연구에서는 목표에 부합하는 기준항목이나 측정지표를 선정할 때 평가방법으로 활용되고 있는 SMART(Specific, Measurable, Attainable, Realistic, Timeline) 평가법을 활용하였다. 스마트(SMART) 평가법은 정당의 공약을 평가하기 위해 영국에서 처음 개발된 지표다. 구체성(S·specific), 측정 가능성(M·measurable), 달성 가능성(A·aimed), 적절성(R·relevant), 시간 계획성(T·timed)을 종합한 평가 방식이다. 본 연구에서는 후보 기준 항목중에서 SMART 평가법에 <표 4>와 같이 입법 취지 부합성, 산출방법의 객관성, 개인정보 취급 연관성, 자료 확보의 가능성 등을 고려한 접근방법을 사용하였다.

<표 4> 대상자 선정 판단기준 및 등급구분

판단기준	설명	등급	의미
Specific	항목 설정에 대한 목표가 구체적 (입법 취지 부합성)	5	아주 명확하게 구별되고 산출물도 생성도 충분함
Measurable	항목 설정목표가 측정이 가능 (산출방법의 객관성)	4	약간 명확하게 구별되고 산출물도 생성도 약간 충분함
Attainable	항목 설정값이 활용이 용이 (개인정보 취급 연관성)	3	보통 명확하게 구별되고 산출물도 생성에 약간 어려움
Realistic	항목이 현실적으로 적용이 가능 (자료 확보의 가능성)	2	명확하게 구별되지 않고 산출물도 생성 약간 곤란
Timeline	기간내에서 정확히 판단 가능	1	명확하게 구별되지 않고 산출물도 생성 아주 곤란

의무대상자를 선정을 위하여 선정된 후보 기준항목을 관련분야 전문가 총 10명의 서면평가로 1점에서 5점으로 평가한 결과를 이용하여 평균치가 높은 항목(4.0 이상)을 <표 5>와 같이 선정하였다.

<표 5> 대상자 선정 후보 기준항목 평가

선정 기준(지표)	등급구분					평균	선택
	S	M	A	R	T		
고객 회원수	5	3	5	3	5	4.2	선정
일일 이용자수	5	3	5	5	3	4.2	선정
총매출액	5	5	5	5	3	4.6	선정
정보통신서비스 매출액	5	5	5	5	3	4.6	선정
정보화투자액	3	3	3	3	3	3.0	제거
정보보호투자액	3	3	3	3	3	3.0	제거
거래 건수	4	3	4	3	2	3.2	제거
총 종업원수(직원)	5	5	5	5	5	5.0	선정
정보통신 직원수	3	5	3	3	3	3.4	제거
정보보호 직원수	3	5	3	3	3	3.4	제거
정보보호대상 설비수	5	5	3	5	5	4.6	선정
인터넷 회선 총 용량	5	4	3	2	3	3.4	제거

3. ISMS 인증 의무대상자 기준 개선(안)

3.1 의무대상자 선정 기준 후보항목 검증

<표 5>와 같이 SMART 평가법으로 확정된 의무대상자 선정 기준 개선(안)을 검증하기 위하여 2013년도 인증 의무대상자에 대한 설문조사 방법을 활용하였다. 설문조사 범위는 전체 대상 298개 업체 중에서 설문에 응답한 116개 업체에 대하여 분석하였다. 대상자 선정 기준 모형에 따라 영역을 고객관점, 재무관점, 정보자원관점을 중심으로 분석하였다. 의무대상자 선정의 주요항목으로 고객관점에서는 이용자수와 기업별 보유하는 고객수를 중심으로 분석하였으며, 재무관점에서는 총매출액과 정보통신매출액을 중심으로 분석하였고, 정보자산관점에서는 보유설비수와 종업원수를 중점으로 분석하였다.

3.2 고객관점의 의무대상자 선정 방안

3.2.1 이용자수 분석

이용자수는 기업에서 보유중인 고객정보와는 다른 성격을 갖고 있다. 특정 정보를 제외하고는 대부분의 정보는 공개되어 있는 것이 사실이나 이러한 공개된 정보의 왜곡은 사회적으로 국가적으로 크나 큰 문제를 야기할 수 있다. 고객 회원수와는 별도로 접속자수나 일일 이용자수를 단순 사용자로 구분되어서는 안된다. <표 6>은 설문조사 결과 2013년 의무대상자 중 이용자수가 100만명을 초과하는 업체가 14.77%(무응답 제외)였다. 민간 통계 업체인 랭키닷컴의 3개월 일평균 순방문수 10만명 이상 웹사이트 207개(2013년 12월기준)이며 중복을 배제한 179개 기업의 인증 의무대상자 여부를 분석한 결과, 27.93%인 50개 기업이 의무대상자에 해당한다. 제도 취지상 많은 대국민 서비스를 수행하는 기업이 해당하지 않고 있기 때문에, 대상자 확대를 위해서 3개월 일평균 순이용자수 기준을 100만명 단위에서 10만명 단위의 소단위로 확대할 필요가 있다[10].

<표 6> 서비스 이용자수 분석

이용자수 (만명)	업체수 (개)	구성비(%)		이용자수(명) 평균값
		무응답 포함	무응답 제외	
100초과	13	11.21	14.77	17,770,460
75~100	1	0.86	1.14	800,000
50~75	3	2.59	3.41	656,667
25~50	12	10.34	13.64	353,060
10~25	18	15.52	20.45	169,818
1~10	22	18.97	25.00	53,317
1 이하	19	16.38	21.59	2,883
무응답	28	24.14	-	-
	116	100	100	-

3.2.2 고객회원수 분석

고객 회원수는 실 사용자로 볼 수 있으며많은 개인정보를 포함하고 있어 침해사고시 엄청난 피해손실이 발생할 수 있다. 고객회원수는 명시적으로 산출하는 것이 가능하지만 다양한 고객이 존재한다. 고객이나 회원수를 고려하여 고객 비율(직접, 간접, 대행), 고객의 성격(기업, 개인, 또는 둘다), 고객에게 제공된 서비스의 종류 등을 고려하여 관리가 이루어져야 한다. <표 7>은 2013년 인증 의무대상자 중 회원수가 1,000만명을 초과하는 업체가 15.46%(무응답 제외)를 차지하고 있다. 회원수 질문항목에 모두 답변한 97개 업체를 대상으로 총매출액 중 정보통신서비스 부문 매출액이 차지하는 비율을 분석하였다. 10만명 이상의 회원수를 차지하는 비율은 83.6%로 분석되었다.

<표 7> 회원수 분석

번호	회원수 범위	업체수	구성비(%)		회원수(명) 평균값
			무응답 포함	무응답 제외	
1	1천만명 초과	15	12.93	15.46	19,069,347
2	5백만명 초과1천만명 이하	8	6.90	8.25	6,972,500
3	1백만명 초과5백만명 이하	18	15.52	18.56	3,142,489
4	5십만명 초과1백만명 이하	11	9.48	11.34	775,669

5	2십만명 초과5십만명 이하	14	12.07	14.43	340,394
6	1십만명 초과 2십만명 이하	11	9.48	11.34	149,954
7	5만명 초과 1십만명 이하	10	8.62	10.31	78,290
8	1만명 초과 5만명 이하	5	4.31	5.15	36,548
9	1만명 이하	5	4.31	5.15	2,959
10	무응답	19	16.38		
합계		116	100	100	

3.3 재무관점의 의무대상자 선정 방안

3.3.1 총매출액 분석

총매출액은 기업의 온라인과 오프라인을 포함한 모든 매출액을 의미한다. 총매출에 대한 고려사항은 기업의 관점에서 보면 정보통신 분야의 매출이 발생하지 않을 가능성이 존재하기 때문에 정보통신 기술을 이용한 서비스 관점을 고려하지 않을 수 없으므로 이에 대한 비율 내지는 기여 정도를 고려할 필요가 있다. 따라서 총매출액에 대한 정보통신서비스 기술 활용정도, 총매출액에 대한 정보통신서비스 점유비율 등이 매출액에 영향 미친다. <표 8>와 같이 2013년 인증 의무대상자인 중 총매출액이 100억을 초과하는 업체가 96.46%(무응답 제외)를 차지하고 있다[6].

<표 8> 총매출액 분석

번호	매출액 범위	업체수(개)	구성비(%)		총매출액(억원) 평균값
			무응답 포함	무응답 제외	
1	1,000억 초과	36	31.03	31.86	17,266
2	100억 초과 1,000억 이하	73	62.93	64.60	361
3	10억 초과 100억 이하	3	2.59	2.65	83
4	10억 이하	1	0.86	0.88	7
5	무응답	3	2.59		
합계		116	100	100	

3.3.2 정보통신서비스 매출액 분석

정보통신매출액은 일부 사업자의 경우에 전체 또는 일부로 존재하며, 이에 따라서 정보통신 매출액의 비중 또한 제도 취지를 고려 할 때 중요하다고 할 수 있다. 선정 기준은 총매출액에 대한 정보통신 매출비율, 순수한 정보통신 매출액(비용기준), 매출액 대비 정보통신서비스를 제공하기 위한 비용 투입비율, 매출액 대비 정보보호서비스를 제공하기 위한 비용 투입비율 등이 명확하게 설정될 필요가 있다. 2013년 의무대상자 중 <표 9>는 정보통신서비스 부문 매출액이 100억을 초과하는 업체가 93.69%(무응답 제외)를 차지하고 있다[6].

<표 9> 정보통신서비스 매출액 분석

번호	매출액 범위	업체수(개)	구성비(%)		정보통신서비스 부문 매출액(평균값)
			무응답 포함	무응답 제외	
1	1,000억 초과	22	18.97	19.82	4,397
2	100억 초과 1,000억 이하	82	70.69	73.87	286
3	10억 초과 100억 이하	6	5.17	5.41	85
4	10억 이하	1	0.86	0.90	3
5	무응답	5	4.31	-	0
합계		116	100	100	

3.4 정보자산관점의 의무대상자 선정 방안

3.4.1 정보통신 설비 수 분석

의무대상자의 인증 범위는 대국민 대상 인터넷 관련 정보통신서비스로 그 대상 설비는 해당 서비스 제공을 위한 유무형의 모든 정보자산이 해당되며 서버, 네트워크 장비, 정보보호시스템 등이 해당된다. 일반적으로 인터넷에 연결되지 않고 내부업무를 위한 서버와 네트워크 장비 등 대 국민서비스가 아닐 경우 인증 범위에서 제외된다. 인증 대상설비에 대한 고려사항은 먼저 타인 또는 대 국민 대상 서비스인지 파악하고 인터넷 접속장비 인지, 내부 업무용과 외부 서비스용 장비를 구분해야 한다. <표 10>은 2013년 인증 의무대상자의 정보통신 설비수 조사 결과 평균 전체 50개를 초과하는 업체가 78.02(무응답 제외)를 차지하고 있다[5].

<표 10> 정보통신 설비수 분석

설비수 범위	업체수(개)	구성비(%)		설비수(개)(평균값)
		무응답 포함	무응답 제외	
10,000개 초과	2	1.72	2.20	146,486
1,000개 초과 10,000개 이하	9	7.76	9.89	2,765
500개 초과 1,000개 이하	10	8.62	10.99	671
100개 초과 500개 이하	33	28.45	36.26	221
50개 초과 100개 이하	17	14.66	18.68	72
50개 이하	20	17.24	21.98	28
무응답	25	21.55	-	
합계	116	100	100	

3.4.2 종업원 수 분석

전사적으로 조직 구성원은 의무대상자를 선정함에 있어 중요한 요소 중에 하나이다. 정보보호는 실제로 기술부분 외에 관리적인 부분이 중요한 부분으로 조직 규모를 판단함에 있어서 종업원수와 매출액이 중요한 항목이다. 보호업무의 대상과 성격에 따라서 보호업무를 추진하기 위한 직원수가 결정되게 된다. 전 직원들의 정보보호 인식 수준이 그 조직의 보안수준을 결정하게 되므로 순수한 정보보호 참여인력도 중요하지만 전체적인 직원을 산정하는 것도 정보보호 측면에서 중요한 요소로 고려해야 한다. <표 11>는 2013년 인증 의무대상자 중 종업원수가 100명을 초과하는 업체가 70.18%(무응답 제외)를 차지하고 있다[5].

<표 11> 종업원수 분석

종업원수 범위	업체수(개)	구성비(%)		종업원수(명)(평균값)
		무응답 포함	무응답 제외	
10,000명 초과	4	3.45	3.51	19584.00
1,000명 초과 10,000명 이하	8	6.90	7.02	2372.75
500명 초과1,000명 이하	10	8.62	8.77	825.40
100명 초과 500명 이하	58	50.00	50.88	229.05
50명 초과 100명 이하	21	18.10	18.42	83.38
50명 이하	13	11.21	11.40	34.31
무응답	2	1.72	-	
합계	116	100	100	

3.5 기존 선정 방안과 제안된 선정방안 비교

기존의 인증 의무대상자 선정 방안인 ISP, IDC, 일일 이용자수, 정보통신서비스제공자 등 4가지 방식에서 본 연구에서 제시하는 개선 방안은 고객회원수, 총매출액, 정보통신설비, 종업원수를 추가하는 방안을 제시하였다. <표 12>는 기존 선정방안과 제안안 선정방안에 대한 비교와 정성적 평가 내용을 설명하고 있다. 다만, 일정 규모 선정 기준(단위)은 대상자 수와 관계가 있기 때문에 사회적 상황, 기업의 여건 등 여러 가지를 고려하여 정부의 정책적 판단에 따라야 할 것이다.

<표 12> 선정 기준항목 비교

기존 선정방안(4개)		제안 선정방안(6개)	평가
ISP		제외	정보통신서비스제공자에 모두 포함되며 형평성 등을 고려 일정규모 이상의 사업자를 선정하는 것이 바람직
IDC		제외	정보통신서비스제공자에 모두 포함되며 형평성 등을 고려 일정규모 이상의 사업자를 선정하는 것이 바람직
기타 정보통신서비스	-	고객 회원수	개인정보보호 유출 방지 등 법 제도 취지에 부합
	일일 이용자수	유지	정보통신망 안정성 확보 등 법 제도 취지에 부합
	-	총매출액	법의 형평성, 취지 등에 부합
	정보통신서비스 매출액	유지	정보통신망 안정성 확보 등 법 제도 취지에 부합

	-	총 종업원 수 (직원)	법의 형평성, 취지 등에 부합
	-	정보보호대상 설비수	정보통신망 안정성 확보, 공평서 등에 부합

3.6 기대 효과

기존 선정 기준항목의 문제점으로 지적되어온 기준항목의 형평성, 공평성, 제도 취지 부합성, 획일적이고 다양하지 못한 기준항목 등으로 대상자로부터 많은 불만을 야기하였다. 본 연구에서 제시한 개선 방안은 SMART 평가법을 적용하여 기준항목의 구체성, 객관성, 측정가능성, 활용성, 적시성 등을 고려하여 기준항목을 선정하였기 때문에 기존의 문제점을 다소 해소하였다. 이는 대상자입장에서는 스스로 판단하여 대상여부를 판단하기 쉽고, 정부입장에서는 기준항목의 다양화에 따라 보다 많은 대상자들이 인증을 받도록 하여 국가 정보보호 수준을 높일 수 있다는 것이 장점이다. 또한 제도 시행의 타당성과 실효성 확보가 가능하여 보다 안정적인 제도 운영과 대상자 선정 기준을 탄력적으로 적용이 가능하다는 것이다.

5. 결 론

현재 정보통신망법에서 적용하고 있는 ISP, IDC, 대상자 선정 기준은 ISMS 인증기준 자체가 정보통신서비스별로 구분하고 있지 않기 때문에 ISP, IDC는 정보통신서비스 매출액이나 이용자수 기준을 적용하는 것이 바람직 해 보인다. 본 연구에서 도출된 대상자 선정 기준 풀에서 2013년도 인증의무대상자에 대한 설문조사를 통해 검증한 결과 <표 13>와 같이 의무대상자 선정항목 기준 개선안을 개발하였다. 법 취지상 잠재 대상자는 모든 정보통신서비스제공자이기 때문에 기존의 ISP, IDC 등 서비스 분류방식은 적합하지 않아 제외하고 정보통신서비스매출액 기준과 이용자수는 제도 취지상 문제가 없어 유지하고 추가 기준으로 4개의 새로운 기준(고객회원수, 총매출액, 정보통신설비, 종업원수)이 가장 적정한 기준으로 분석되었다.

<표 13> 의무대상자 선정항목 기준 개선안

관점	항목	단위	현재	단위 조정	추가 여부
고객 관점	이용자수	명	100만명 이상	10만명 이상	기존
	고객 회원수	명	없음	10만명 이상	추가
재무 관점	총매출액	억원	100억 이상	100억 이상	추가
	정보통신 매출액	억원	100억 이상	100억 이상	기존
정보 자산	설비수	대	없음	50대 이상	추가
	종업원수	명	없음	100명 이상	추가

이와 같이 의무대상자를 선정하는 기준의 가장 중요한 요소로는 입법 취지 부합성, 산출방법의 객관성, 개인정보 취급 연관성, 자료 확보의 가능성 등이다. 또한 선정 기준항목이 신뢰성, 파악 용이성, 객관성, 공정성, 투명성 등이 중요한 요소로 본 연구에서는 이를 반영하였다.

본 연구에서는 보다 명확한 기준을 도출하여 대상자에게 제시하여 선정된 대상업체가 자율적으로 대상여부를 판단하고, 스스로 ISMS를 구축하고 인증을 받도록 하였다. 또한 제도의 실효성 확보와 의무대상자 선정의 적정성과 투명성 확보를 하고자 하였다.

이상으로 본 연구에서는 ISMS 인증 제도의 의무대상자 선정을 위한 현황을 분석하고, 의무대상자 선정 모델을 개발하였으며, 2013년도 의무대상자에 대한 설문을 통해 의무대상자 선정항목을 분석하여 적정성을 검증하였다. 적정성을 검증하는 과정에서 항목의 가중치나 척도기준을 반영하였다. 의무대상자 선정을 위하여 많은 기업들이 인증 대상에 포함되도록 산정하는 방법을 법 취지를 고려하여 보다 과학적이고 신뢰성 있는 접근 방법을 제시하였다.

향후 정보통신망 및 서비스의 안정성 확보와 정보통신망법 적용의 근거를 명확하게 하기 위해서는 정보통신서비스에 대한 분류체계와 분류 방법을 표준화하고 국내 정보통신서비스제공자에 대한 정확한 현황

파악과 기준 마련에 대한 연구가 추가 되어야 할 것이다.

참고문헌

[1] 법제처, “정보통신망 이용촉진 및 정보보호 등에 관한 법률 및 시행령”, 2013.
[2] 미래창조과학부, “정보보호 관리체계 인증 등에 관한 고시”, 2013.
[3] 한국인터넷진흥원, 정보보호 관리체계 인증 제도 안내서, 2013.
[4] 한국인터넷진흥원, "정보보호 관리체계(ISMS) 구축 및 운영 교육 교재“, 2013.
[5] 한국인터넷진흥원, ‘기업정보보호실태조사’ 2013.
[6] 한국정보통신진흥협회, ‘정보통신산업실태조사’ 2013.
[7] 박용성, “AHP에 의한 의사결정 이론과 실제,” 교우사, 2009.
[8] Thomas L Saaty, "The Analytic Hierarchy Process," New York: McGraw Hill. International, Translated to Russian, Portuguese, and Chinese, Revised editions, Paperback (1996, 2000), Pittsburgh: RWS Publications, 1980
[9] http://www.expertchoice.co.kr
[10] www.rankey.com

[저 자 소 개]

장 상 수 (Sang-soo Jang)

1989년 2월 한국항공대학교 학사
2003년 2월 동국대학교 석사
2011년 8월 전남대학교 박사
현재 아주대학교 지식정보보안학과 특임교수

email : ssjang0116@gmail.com