정보보호 안전진단 대상자 선정 기준의 개선 방안 연구*

안 연 식**

An Enhanced Model on the Selection of Information Protection Security Diagnosis Target Firms*

Yeonshick Ahn**

■ Abstract ■

The information protection security diagnosis institution was applied services since 2004, for the leveling up of public information protection and the establishment of the stability and reliability of information communication. And this security diagnosis was implemented actually on the 142 firms in 2005, the 160 firms in 2006 and the 205 firms in 2007. But this is recognized by the some firms as one of the unnecessary regulations. And there are some difficulties with collecting the subjective and reliable source data for establishing the information protection security diagnosis target. In this research, the enhanced model on the selection of information protection security diagnosis target firms was suggested by the interview with some expert and the analysis for the related actual data. By the model which are introduced from the statistical analysis of the related data and the summary of some expert's suggestions, information protection security diagnosis target can include the information telecommunication service providers taking 5 billion won as sales in a year, and web service providers like as shopping mall site, with the personal records of 2 million subscribers.

Keyword : Information Protection Security, Information Protection Security Diagnosis

논문투고일 : 2008년 10월 21일 논문수정완료일 : 2008년 12월 06일 논문게재확정일 : 2008년 12월 08일
* 논문작성에 필요한 자료제공에 협조해주신 한국정보보호진흥원에 감사드립니다.
** 경원대학교 경상대학 경영학과 부교수

1. 서 론

인터넷을 기반으로 한 정보통신서비스에 대한 이용자수가 증가되고 있고, 서비스를 제공하는 이용자들의 정보보호 필요성은 더욱 중요해지고 있다. 그리고 홈네트워크, VoIP 등 유무선 통합 및 무선매체에 의한 서비스까지 급속하게 확대됨에 따라서 해킹, 바이러스 등 인터넷 정보침해 사고 위협뿐만 아니라 이로 인한 사회적 혼란과 경제적 피해가 증대될 것으로 예상된다[2, 6]. 2008년에도 실제로 소규모 금융기관과 대형 쇼핑몰의 고객정보 유출로 사회에 파장을 일으킨 사례가 있다[5].

정보보호 안전진단 제도는 주요정보통신서비스 제공자(ISP), 집적정보통신시설사업자(IDC), 쇼핑몰 등의 정보통신망에 대한 침해사고 예방을 위하여 정보보호조치의 관리적·기술적·물리적 보호조치를 이행하고 안전진단 수행기관으로부터 안전진단을 받음으로써 정보통신망 및 정보통신서비스에 대한 안정성 및 신뢰성을 확보하기 위한 제도이다[11]. 본 제도 시행 이후 2005년도에 142개, 2006년도에 160개, 2007년도에 205개 사업자를 대상으로 안전진단이 실시되었다. 이중에서 ISP업체는 10여개 업체, IDC/VIDC 업체는 70개 업체 그리고 쇼핑몰 등의 업체는 80여개 업체 정도이다. 이러한 실적치는 전수조사 형태를 취하고 있는 통계청의 사이버 쇼핑몰 통계조사 결과를 참고로 할 때 국내 전체 쇼핑몰의 약 5%에 해당하는 것으로 추정된다[8, 9].

〈표 1〉 2007년 국내 인터넷침해사고 통계

구 분	웜바이러스	해킹 신고				
		스팸릴레이	파싱 경유지	단순침입 시도	기타 해킹	홈피 변조
건수	5,976	11,668	1,095	4,316	2,360	2,293

(출처 : 한국정보보호진흥원, 2008).

최근 관련기관의 발표에 의하면[10], 2007년 한 해 동안 인터넷 침해사고로 신고된 건수는 2만 건 이상이다<표 1>. 최근에는 옥션(auction) 사이트는 물론 금융기관까지 해킹이 시도되고 있으며, H통신사는 고의로 고객의 개인정보를 유출시킨 이유로 피해를 입은 고객들이 해당 기업을 집단 손배소로 제소하고 있다. 이러한 부작용을 최소화하는 정부의 조치가 바로 정보보호 안전진단 제도이다.

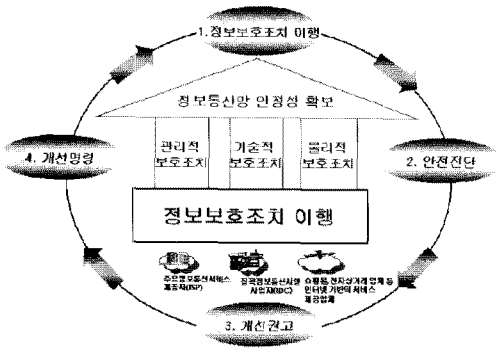
본 연구에서는 정보보호 안전진단 대상자 선정을 위해 적용되는 현행 기준이나 절차와 관련된 문제점 개선 및 개선방안 제시를 목적으로 하고 있으며, 연구 방법론은 관련 자료의 통계 분석 및 전문가의 의견 수렴을 주로 활용하였다. 관련 자료는 본 제도가 시행된 이래 2005년부터 2007년까지 관련 정부기관에 수집된 자료를 활용하였고, 전문가의 의견은 정보보호 관련 정부기관의 내부 직원 및 해당 기관에서 위촉하여 활동 중인 산업계와 학계 전문가 총 10명 규모였으며, 2007년 9월부터 2007년 12월에 걸쳐서 진행된 연구과정에서 2회에 걸친 검토회의 및 1회의 서면조사에 의한 의견제시를 통해 연구결과에 반영하였다.

본 논문에서는 제 2장에서 현행의 정보보호 안전진단 제도와 문제점을 분석하고, 제 3장에서는 개선모형을 설명하되 대상자 선정 기준의 항목과 항목별 기준값의 설정에 대해서 논의하고 있으며 통계자료를 이용한 분석이 수행되었다. 그리고 제 4장에서는 결론을 제시하고 있다.

2. 현행 안전진단 제도와 문제점

2.1 현행 안전진단 제도

정보통신망법 제46조의3(정보보호 안전진단)에 의하면, 관련 정보통신서비스사업자는 안전진단 수행기관으로부터 정보통신망 또는 집적정보통신시설에 대하여 매년 정보보호지침에 따른 정보보호 안전진단을 받아야 한다고 규정하고 있다. [그림 1]은 정보보호 안전진단 절차도로서 정보보호조치 이행 여부에 대해 안전진단을 수행한 후 개선사항을 권고하고 명령하는 절차를 나타낸 것이다[11, 12].



[그림 1] 정보보호 안전진단 제도의 절차

현행 기준에서 정의한 안전진단 대상자 유형은 주요정보통신서비스제공자, 집적정보통신시설사업자, 정보통신서비스제공자 등이다[11, 12]. 주요 정보통신 서비스 제공자는 전기통신사업자로서 전국적으로 정보통신망접속 서비스인 인터넷접속 서비스 제공자와 전기통신회선설비 및 네트워크 서비스 제공자를, 집적정보통신시설사업자는 타인의 정보통신 서비스제공을 위하여 집적된 정보통신시설을 운영·관리하는 사업자(직접정보통신시설사업자)로서 공간임대 서비스(Co-location) 또는 서버임대(서버호스팅)서비스 및 네트워크 서비스 등을 제공하는 사업자와 집적정보통신시설을 임차한 재판매사업자가 포함된다. 또한 정보통신 서비스 사업자의 경우에는 연간 정보통신 서비스 매출액 100억 이상 이거나, 일일 평균 이용자가 100만 명 이상인 업체인 업체로 규정되어 있는데, 네트워크 제공 서비스(회선임대 포함), 인터넷 쇼핑몰, 포털, 게임, 예약, 종합유선방송서비스, 카드조회/지불중계, 신문·방송, 음악·교육, 전자문서교환 서비스 등을 제공하는 사업자 등이 포함된다.

이 기준에 따라 <표 2>에서와 같이, 정보통신부에 신고된 전기통신사업자 목록 및 관련 협회 자료, 신용평가기관 등의 자료를 활용하여 대상자가 선정된다. 또한 쇼핑몰 등 정보통신서비스제공자에 대해서는 매출액 100억 이상인 사업자는 국세청의 자료를, 일일평균 이용자수 100만 이상인 사업자 목록은 관련 기관에서 입수하고 있다.

〈표 2〉 현행 안전진단 대상자 선정을 위한 자료원

구 분	자료 확보	비 고
주요정보통신서비스제공자(ISP)	• 정보통신부 등록 사업자 목록 입수	
집적정보통신시설사업자(IDC)	• 정보통신부 등록 사업자 목록, 관련협회 자료 입수	
쇼핑몰 등 정보통신서비스 제공자	• 정보통신부 등록 사업자 목록, 관련협회, 신용평가기관, 랭키닷컴 등 자료 입수	국세청, 외부기관 자료 활용

2.2 현행 안전진단 대상자 선정기준의 문제점

현행 안전진단 대상자 선정에 적용되는 기준과 관련하여 관련 실태조사 자료[13, 14]와 관련 분야 전문가 의견수렴을 통해서 도출된 문제점을 정리하면 다음과 같다.

2.2.1 자율적인 기준제에 대한 인식 결여

안전진단 대상자 선정은 일정 규모 이상의 인터넷 기반의 정보통신 서비스 제공 사업자를 대상으로 하는 것으로 "자율적 기준제"를 적용한다. 이로써 제도 자체에 대한 인식이 미흡한 사업자들의 경우, 정보보호와 관련된 문제의 해결이나 사전 예방에 수동적인 자세를 갖는 경향이 있고, 안전진단 미이행 사업자를 대상으로 과태료를 부과하는 제도를 규제로 인식할 가능성이 있다.

2.2.2 금융거래 또는 사용자정보를 수집/관리하는 소규모 사업자 누락

다중이용 서비스 제공자의 경우, 현행 총매출액 100억 이상이거나, 평균 일일 이용자수가 100만 명 이상인 업체를 대상으로 하고 있다. 그러나 소규모 업체로서 사이트에서 금융거래가 이루어지거나 다수의 사용자 정보를 다루는 업체의 경우, 금융사고나 해킹사고가 발생할 경우 불특정 다수에 대한 피해를 유발할 가능성이 높기 때문에, 이러한 사업자들에 대해서도 안전진단을 받도록 하여

정보통신 서비스의 안전성을 확보할 필요가 있다.

2.2.3 총 매출액을 기준으로 한 안전진단대상자 선정

안전진단대상 중 '쇼핑몰 등 기타 정보통신서비스제공자'의 선정 기준은 100억 원 이상의 정보통신 서비스 매출액을 기준으로 하고 있지만, 실제 대부분 정보통신 서비스 매출액을 별도 구분하여 관리하지 않고 임의적으로 정보통신 서비스 매출액을 산출하고 있다. 또한 기업분할 등으로 매출액을 분리하는 방법 등을 통해서 의무를 회피하는 문제가 있다.

2.2.4 영세업체(VIDC)의 안전진단대상자 포함 여부

영세업체의 경우, 안전진단 수수료 부담, 전문적인 기술 인력의 미보유 등의 측면에서 제도에 대한 불만이 높다. 그러나 이들이 제공하는 서비스의 중단 혹은 정보통신설비의 침해사고 발생으로 고객피해는 물론, 국가 차원의 사회적·경제적인 피해 위험성이 있기 때문에, 영세업체를 고려한 보다 합리적인 방안이 마련되어야 한다.

2.2.5 일평균 접속자수를 기준으로 한 안전진단대상자 선정

일평균 이용자수는 용어상의 개념이 불일치하여 <표 3>에서와 같이 순방문자, 페이지 뷰, 시간당 방문자 수(평균치) 등 다양한 형태로 정의되어 통일된 기준을 적용하기 어렵고[7], 현재 적용중인 이용자수 데이터는 인터넷 사용자수를 샘플링(sampling) 방법으로 도출된 추정치에 근거하고 있는 문제점을 내포하고 있다.

즉, 해당 기관에서 대상자 선정에 활용하는 일평균 이용자수는 실제 데이터가 아니고, 인터넷사용자중 약 6만 명을 대상으로 그들이 접속하는 사이트를 샘플(sample)로 추정한 값이다. 이것은 실제 서비스 사용자와는 다른 값일 뿐만 아니라 정확한 통계치가 아니기 때문에 개선이 필요하다.

3. 안전진단 대상자 선정개선 모형

3.1 대상자 선정 기준항목의 개선

일반적으로 목표에 부합하는 기준항목이나 측정지표를 선정할 때 Jerry L. Harbour의 연구[1]에서 제시된 SMART 원칙을 적용한다. 여기에서 SMART란 구체화 정도(Specific), 측정 가능성(Measurable), 적용 가능성(Action-Oriented), 관련성(Relevant), 적시성(Timely) 등 지표 선정에 합리성을 검토하는 기준항목이다.

본 연구에서 다루는 주제인 안전진단 제도의 성과는 목표치를 계량화하기 어렵고, 또한 지표 관련 자료의 획득 가능성이 낮아 기준항목을 선정하기가 매우 어렵다. 따라서 본 연구에서는 다음과

〈표 3〉 일평균 사용자수에 대한 개념 비교

방법	순방문자 수	페이지 뷰	시간당 방문자 수
기준	일반적인 순위 산정방식으로 하루에 몇 번 사이트를 방문하더라도 1번으로 인정하는 절대 기준	사용자기 실제 웹 서버(web server)에 요청한 File(htm)의 수를 근거로 작성함	해당 웹사이트에 방문한 방문자수를 순위산정의 기준으로 하되 1시간 이내에 동일 사용자가 웹사이트에 방문한 내역은 새로운 방문으로 인정하지 않고 순위 산정에서 제외함
장점	조작될 염려가 없고, 객관적 기준	사용자의 로열티(loyalty) 반영 가능함	1) 페이지뷰 기준으로 순위 측정 시 발생할 수 있는 순위 왜곡 가능성 배제함 2) 사용자 로열티 반영 가능함
단점	웹사이트(Web site)별 특성 반영 안됨	객관적인 순위의 기준으로 부적합함	단, 순방문자수와 페이지뷰 기준의 단점을 완전 보완 불가능함

출처 : 정보통신윤리위원회(ICEC) 연구보고서, 2005년 1월.

같은 접근방법을 사용하였다.

우선 사업자 유형별로 제공하는 주요 서비스, 서비스의 기반이 되는 주요 자산 그리고 주요 고객 등을 식별한 후, 이를 대리할 수 있는 후보 기준항목을 <표 4>에서와 같이 선정하였으며, 후보 기준항목 중에서 입법 취지의 부합성, 산출방법의 객관성, 자료취득 가능성 및 개인정보 취급 연관성 등의 평가항목을 관련 분야의 전문가 총 8인의 서면평가로 1점에서 5점으로 평가한 결과를 이용하여, 평균치가 높은 항목인 정보통신서비스 매출액과 가입 회원수 항목을 기준항목으로 선정하였다.

- 총매출액 항목은 산출방법의 객관성이나 자료취득성이 높아서 종합적인 관점에서 활용가치가 있으며, 향후 사업자의 정보통신서비스 부문의 매출액 자료를 획득할 수 있을 때까지 대리지표로 활용하는 것이 바람직하다.
- 정보통신서비스 매출액 항목은 안전진단 대상자 선정의 가장 효과적인 기준항목으로 판단되지만, 해당 사업자가 복합적인 영역의 매출이 있는 경우가 있고, 이 경우에도 정보통신서비스 매출액만을 분리하여 신고하지 않기 때문에, 총매출액 항목에 비교시 상대적으로 자료수집이 어려운 점이 제약점이다.
- 일평균 이용자수 항목은 앞에서 논의된 바와 같이 불특정 다수가 접속하는 많은 온라인 사이트의 접속량과 관련성이 높은 좋은 후보 항목이지만, 개념상의 통일된 이해가 아직 미흡하여 사업자마다 그리고 관련기관마다 제시하는 수치상의 불일치가 존재하고, 또한 자료수집의 어려움이 높다.
- 개인정보 수집건수(가입 회원수) 항목은 자료수집의 가능성만 확보된다면, 개념의 정의도 명확하고 특히 일평균 이용자수 항목에 비교시 상대적으로 데이터 값을 객관적으로 산출

〈표 4〉 사업자 유형별 대상자 선정 기준항목 검토

구 분	주요 서비스	주요 자산	주요 고객	대상 업체 선정 기준 항목(후보)
주요정보통신 서비스 제공자(ISP)	정보통신망 접속	정보통신설비, 회선	기업, 개인	보유설비 규모(회선용량, 설비수), 정보통신 서비스 매출액, 총 매출액
집적정보통신시설 사업자(IDC)	Co-location,서버 호스팅, 웹 호스팅	정보통신설비, 회선, 공간	기업	보유설비 규모(회선용량, 설비수), 정보통신 서비스 매출액, 총 매출액
쇼핑몰 등 다중이용 서비스 제공자	상품정보, 포털, 게임 등	상품정보	개인	가입 회원수, 거래건수, 일평균 이용자수

〈표 5〉 사업자 선정의 기준항목 후보에 대한 평가

구 분	입법취지 부합성	산출방법의 객관성	자료 취득가능성	개인정보 취급 연관성	평균점수
총매출액	4.25	4.75	4.50	1.13	14.63
정보통신 서비스 매출액	4.75	2.88	2.25	3.25	13.13
일평균 이용자수	4.88	1.25	1.63	3.75	11.50
가입 회원 수	4.63	4.63	2.38	4.88	16.50
거래 건수	4.88	4.13	1.13	3.13	13.25
회선 용량	4.63	1.38	1.88	1.00	8.88
정보통신설비수	5.00	1.25	2.38	1.38	10.00

하기 용이할 뿐만 아니라, 정보보호의 취지를 살리는데 최적의 의미를 가진 후보 항목이다. 따라서 현행 일평균 이용자수를 대체하는데 중장기적으로 가장 적합한 기준항목으로 설정할 수 있다.

- 거래건수 항목은 온라인상에서 이루어지는 모든 상거래 행위에 있어서 거래건수 데이터를 수집하기 어려울 뿐 아니라, 기술적으로 데이터를 수집할 수 있다해도 사업자의 영업비밀에 속한 사항으로 추후 검토할 수 있는 항목이다.
- 회선용량 항목은 사업자와 서비스를 제공받는 가입자들의 접속량을 추정할 수 있는 좋은 항목이지만, 회선용량의 집계 및 수시로 변경되는 용량 자료의 수집이 어렵고 진단대상자로 선정하기 위한 용량기준의 설정도 매우 난해한 항목이다.
- 정보통신설비수 항목은 회선용량과 마찬가지로 사업자가 제공할 수 있는 서비스 규모를 추정할 수 있는 좋은 항목이지만, 설비 유형과 규모, 설치 위치, 연동방식 등이 너무 다양하여 활용성이 낮은 항목이다.

따라서 현 단계에서 안전진단 대상자 선정에 적용할 기준항목으로 <표 6>과 같은 항목을 선정하였다.

3.2 대상자 선정 기준 항목별 기준값

<표 6>에서와 같이 제시된 총 매출액 항목과 개인정보수집 건수 항목의 기준값의 설정에 대해 논의하기로 한다.

〈표 6〉 사업자 유형별 대상자 선정 기준항목

구 분	대상 업체 선정 기준 항목
주요정보통신 서비스 제공자(ISP)	총 매출액
집적정보통신시설 사업자(IDC)	총 매출액
쇼핑몰 등 다중이용 서비스 제공자	개인정보 수집건수 (가입 회원수)

3.2.1 총 매출액 기준값

총 매출액은 주요 정보통신 서비스제공자(ISP)와 집적정보통신시설사업자(IDC)에 적용되는 기준항목으로서 현행 100억 원을 기준값으로 규정하고 있으나, 이 기준 값의 적정성을 판단하기는 쉽지 않고 다분히 정책적인 기준치이다.

이러한 제약요인과 가용한 자료를 고려하여 사업자별 매출액 자료와 정보보호 안전진단 제도시행 기간 중 관련 기관에 접수된 개인정보 피해 건수간의 관계를 분석한다. 분석에 사용된 자료는 본 제도의 시행 이후인 2005년부터 2007년까지 관련 기관에서 수집한 안전진단 후보군의 매출액과 정보보호 피해접수건수 자료로서, 기술적인 특성이 <표 7>에 나타나 있다.

〈표 7〉 안전진단 대상 업체후보의 총매출액 규모 및 정보보호 피해접수 건수 자료

구 분	매출액	피해접수 건수 평균	대상 업체수	표준편차
1	50억 미만	3.78	23	5.40
2	~100억 미만	5.15	20	6.83
3	~500억 미만	16.49	43	35.67
4	~1000억 미만	69.67	12	194.13
5	1000억 이상	71.83	36	127.96
Total		32.24	134	93.38

이와 같이 정보통신 서비스 제공자의 개인정보 피해 접수건수를 하나의 검토 항목으로 다루는 이유는 개인정보 침해사고의 예방이 다중 정보서비스에 대한 안전진단의 목적과 부합하는 항목 중의 하나이며, 개인정보를 취급하거나 개인정보침해사고가 빈번한 정보통신 서비스 부문 제공자에 대하여 보호조치를 점검하여 개인정보침해사고를 예방할 필요가 있기 때문이다.

가. 매출액 규모와 개인정보 피해건수 간의 상관관계 분석

<표 7>에서 알 수 있듯이 사업자의 매출액이 커지면 개인정보 피해건수도 커지는 경향을 나타낸다. 그러나 매출액 규모와 개인정보 피해건수 간의 상관관계를 통계적으로 분석한 결과, 상관관계가 있다는 가설은 통계적으로 입증되지 못하였다. 그 내용을 보면 <표 8>에서와 같이 총 134개 업체 자료를 분석한 결과, 피어슨 상관계수는 0.028로서 낮게 나타나고 그것도 유의수준(sig.)이 0.751(> = 0.05)이다. 즉, 상관계수는 매우 낮은 상관관계를 나타내고, 유의수준 값은 통계적으로 유의하지 않다[3].

동일한 방법으로 총 매출액 100억 이상인 91개 업체를 대상으로 한 통계 분석에서도, 또한 총매출액 50억 이상인 111개 업체를 대상으로 한 분석에서도 피어슨 상관계수가 낮고, 통계적인 유의성이 없는 것으로 나타났다.

나. 매출액을 기준으로 한 사업자 집단별 개인정보 피해건수 간의 차이 분석

〈표 8〉 전체 사업자의 매출액과 개인정보 피해건수 간의 상관관계

구 분		매출액	피해건수
매출액	Pearson 계수	1	.028
	Sig.(2-tailed)		.751
	N	134	134
피해건수	Pearson 계수	.028	1
	Sig.(2-tailed)	.751	
	N	134	135

사업자를 매출액 규모에 따라 구분하여 집단별로 정보보호 피해접수 건수가 차이가 있는지를 분석한다. 집단 구분은 <표 7>에서 제시된 5개 구간을 기준으로, 5개 집단을 (1)과 (2), (2)와 (3) … (4)와 (5) 등 2개항으로 구분하여, 그리고 (1), (2), (3, 4, 5) 등의 3개항으로 구분하여 여러 구간을 반복적인 차이분석을 실시하였다. 그 결과, 다음에서와 같이 매출액 100억 및 50억을 기준으로 한 집단 사이에서만 유의한 결과를 보였다.

첫째로 매출액 100억 이상인 91개 업체의 정보보호피해접수 건수는 평균 45.4건이며, 매출액 100억 미만인 43개 업체의 정보보호피해접수 건수는 평균 4.4건으로<표 9a>, 2개 집단 간의 정보보호 피해접수 건수 평균차이는 41.0건으로 큰 차이를 나타낸다. 집단 간 차이분석(t-test)을 실시한 결과, 다음 <표 9b>에서와 같이 통계적으로 유의한 것으로 밝혀졌다. 또한 2개 집단의 피해건수 분포가 정규분포를 이루는지에 대한 분석결과(Levene's Test for Equality of Variances)가 유의수준(sig.)이 0.000이고 F값이 17.176으로서 고르게 분포되지 않았음을 알 수 있고, 2개 집단 간 차이가 있다는 사실에 대한 통계 분석의 유의수준(sig.)은 0.001이며 검정통계량(t 값)은 3.510로서, 피해접수 건수 차이가 존재한다는 가설이 통계적으로 유의하다[2].

둘째로, 다음과 같이 매출액 50억 이상, 50억 미만인 집단으로 구분한 평균 피해건수 차이의 차이분석 결과가 통계적으로 유의하였다<표 10a>, <표 10b>.

결론적으로 총 매출액 100억을 기준으로 한 2개 집단 간 차이 검증의 경우와, 50억을 기준으로 한 2개 집단 간 차이 검증의 결과에서, 모두 통계적으로 유의한 정보보호 피해건수의 차이가 존재할 분

〈표 9a〉 매출액 100억 이상 및 미만 사업자 집단의 개인정보 피해건수 차이

집 단	업체수	평균치	표준편차	표준오차 평균 값
100억 이상 업체	91	45.3956	111.01740	11.63779
100억 미만 업체	43	4.4186	6.07192	.92596

〈표 9b〉 매출액 100억 이상 및 미만 사업자 집단의 개인정보 피해건수 차이 분석

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	유의확률 (Sig.)	t	자유도 (df)	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									하한	상한
피해 건수	등분산이 가정됨	17.176	.000	2.414	132	.017	40.97700	16.97562	7.39754	74.55646
	등분산이 가정되지 않음			3.510	91.135	.001	40.97700	11.67456	17.78737	64.16663

주 : t-test for Equality of Means은 평균의 동질성에 대한 t-검정을 의미하며, Sig. (2-tailed)는 유의확률(양쪽), Mean Difference는 평균차, Std. Error Difference는 차이의 표준오차, 95% Confidence Interval of the Difference는 차이의 95% 신뢰구간을 의미함.

만 아니라, 검정통계량을 나타내는 t값이 전자<표 8b>의 3.510에서 후자<표 9b>의 3.537로 증가하였다. 이것은 50억을 기준값으로 설정했을 때에서 100억을 기준으로 했을 때보다 더 피해차이가 명확하다는 것을 보여주고 있다.

따라서 주요 정보통신 서비스 제공자 (ISP)와 집적 정보통신시설 사업자(IDC)중 안전진단 대상 사업자 선정시 적용되는 총매출액 기준값으로는 현행 100억에서 50억으로 조정하는 것이 더 타당성이 있음을 알 수 있다.

3.2.2 개인정보수집 건수 항목의 기준값

가. 개인정보수집 건수(가입 회원수) 항목의 기준값 추정

개인정보수집 건수는 현행의 일평균 사용자수보다 개념이 명확하고, 쇼핑몰 등 다중 정보서비스 제공자에게 적용할 수 있는 매우 유용한 기준항목이다. 그러나 사이트별 개인정보수집 건수는 업체의 영업 기밀에 속하는 자료이기 때문에, 부풀린 값 또는 개략치만을 제시하거나 공개를 거부

〈표 10a〉 매출액 50억 기준 사업자 집단의 개인정보 피해건수 차이

구 분	N	Mean	Std. Deviation	Std. Error Mean
50억 이상 업체	111	38.1441	101.65368	9.64854
50억 미만 업체	23	3.7826	5.40165	1.12632

〈표 10b〉 매출액 50억 기준 사업자 집단의 개인정보 피해건수 차이분석

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
피해 건수	등분산이 가정됨	7.738	.006	1.616	132	.109	34.36154	21.26582	-7.70435	76.42742
	등분산이 가정되지 않음			3.537	112.914	.001	34.36154	9.71406	15.11607	53.60700

〈표 11〉 사이트별 가입자 수 통계

(단위 : %)

구 분		업체수 (N)	1만명 이하	1~5 미만	5~10 미만	10~20 미만	~100 미만	~200 미만	~400 미만	400 이상	평균 (만명)
전 체		50	-	-	8.0	4.0	16.0	8.0	12.0	52.0	719.34
정보통신 서비스제공 역무별	포 탈	16	-	-	-	-	-	-	6.3	93.8	1512.63
	온라인게임	7	-	-	-	-	-	-	42.9	57.1	709.00
	웹 스토리지	15	-	-	20.0	13.3	33.3	13.3	-	20.2	150.67
	채 팅	12	-	-	8.3	-	25.0	16.7	16.7	33.3	378.50

하는 등 실제로 파악하기가 쉽지 않은 점이 문제이다.

다만, 정보통신윤리위원회(ICEC)에서 총 54개 정보통신서비스 제공자를 대상으로 한 조사 결과 <표 11>을 보면, 대부분의 포털 사이트(16개 업체), 온라인게임 사이트(7개 업체)는 가입자 수가 200만 명 이상으로 나타났으며, 웹 스토리지의 30%와 채팅 사이트의 66% 정도는 100만 명 이상의 가입자수를 확보하고 있다[7]. 향후 지속적인 통계분석이 필요한 상황이지만 대체로 회원수를 200만 이상 보유한 사업자로 정한다면 대형 포털사이트와 온라인게임 사이트의 100%, 그리고 웹스토리지의 20%, 채팅 사이트의 50% 정도를 안전진단 대상 사업자로 포함시킬 수 있다고 판단된다.

나. 개인정보수집 건수(가입 회원수) 항목의 기준값 활용 가능성

개인정보수집 건수는 법제도의 보완이 되지 않은 상태에서는 사업자들로부터 수집하기 매우 어려운 항목이다. 그러나 업체나 관련 기관에서 용어 자체의 개념이 달라서 혼동을 일으킬 문제는 전혀 없다. 또한 국가인권위원회의 인권 관련 정부통계현황 보고서[4]에서도 개인정보의 수집과 보유를 법으로 규정해야 한다고 강조하고, 국가인권 수준의 향상을 위해서 추가로 개발되어야 한다고 하는 통계(지표)항목에도 각 포털 사이트의 개인정보 보호실적과 유출건수 등을 제시하고 있어, 법 규정에 의한 수집 항목으로 설정되는 경우 매년 정확한 보유 회원수를 의무적으로 제출받을 수 있어서 본 제도와 연계되면 효과를 기대할 수 있다.

다. 개인정보수집 건수(가입 회원수) 항목의 기준값 활용을 위한 법제도적인 보완

개인정보보호와 관련하여 관련 입법사례를 보면, 정보통신 서비스 사업자에 대한 개인정보의 수집 및 관리를 강화하는 추세이다. 2005년 12월에는 피싱(Phishing)과 같이 정보통신망을 통해 속이는 행위로 타인의 개인정보를 수집한 자 및 동일한 방법으로 개인정보 제공을 유인한 자에 대한 처벌 규정이 반영되었고, 2006년 12월에 『정보통신망법』이 재개정되어, 개인정보의 수집·이용·제공 시 동의절차를 대폭 강화되었다.

그러나 실제로 다수의 사이트에서 개인정보의 등록을 요구하고 있고[1], 고객의 개인정보를 취급하는 사업자들이 경각심을 갖고 보호 및 유지관리 시스템을 갖추도록 이를 더욱 강화할 필요가 있으며, 개별 사업자로부터 사이트별 일일 평균 이용자수나 개인정보 수집건수에 대해서 년1회 정도의 자료 제출을 의무화할 수 있으면 활용의 효과가 기대된다.

이와 관련 『정보통신망법』에서는 정보주체로부

1) 2006년 정보통신부는 총 24,500개 사업자를 대상으로 사업자 개인정보 관리 현황을 조사한 결과 홈페이지를 운영하는 경우는 19,213개였으며, 이 중 전체의 65%에 해당하는 12,495개 사업자가 개인정보를 수집하고 있었음[6].

터 개인정보를 수집하는 경우, 관리 책임자, 수집·이용목적, 이용·보유기간, 개인정보의 동의 철회(회원탈퇴) 방법, 정보의 열람 및 정정에 관한 사항 등을 필수적으로 사전에 고지하고 동의를 받도록 규정하고 있다. 또한 관련 기관에서는 웹사이트에서 개인정보를 수집·이용하는 사업자가 개인정보 수집 이전에 이러한 의무고지 사항들을 준수하고 있는지 모니터링 함으로써 사업자의 개인정보보호 준수실태를 점검하고 있다. 이러한 제도에 추가하여 개별 사업자로부터 사이트별 일일 평균 이용자수나 개인정보 수집건수에 대한 자료를 제출하도록 하고, 관련 기관에서 이를 수집하는 체계의 구성이 필요하다. 모든 정보통신 서비스 제공사업자를 대상으로 개인정보 수집건수 등을 파악하기 위해서는 법제화가 필요하기 때문에, 단기적으로는 현행의 제도 하에서 『정보보호 안전진단 결과보고서』의 서식에 이들 항목을 포함시켜 조사하고 자료의 축적 및 분석을 위해 활용하도록 개선이 필요한 것으로 판단된다.

이상에서 논의된 안전진단 대상 사업자를 선정하기 위해 적용할 기준값을 정리하면 <표 12>와 같다.

3.3 기타 대상자 선정기준 개선방안

앞에서 논의한 사항 이외에, 안전진단 대상자 선정시 보완되어야 할 추가적인 개선방안은 다음과 같다.

첫째, 자율적으로 안전진단 활동에 적극 참여하고, 평가결과가 우수한 사업자에 대한 안전진단 면제 대상자 확대가 필요하다. 안전진단 대상 사업자로서 과거 3년 간의 안전진단 결과 정보보호 수준이 우수하며, 관련 전문 인력을 보유하고 있고, 사업자 스스로 안전진단 활동을 철저히 수행하고 있는 사업자들에 대해서는, 소정의 검토절차를 거쳐서 향후 3년간 안전진단 면제 대상자로 지정하는 방안을 검토할 필요가 있다. 이러한 조치는 자율적인 안전진단 제도의 참여는 물론 사업자 스스로 정보보호 수준을 향상하고 안정적인 정보통신 서비스 제공을 위해 매우 바람직하다고 판단된다.

〈표 12〉 안전진단 대상자 선정 기준항목별 기준값

구 분	대상업체 선정 기준 항목
주요정보통신 서비스 제공자(ISP)	총 매출액 50억 이상
집적정보통신시설 사업자(IDC)	총 매출액 50억 이상
쇼핑몰 등 다중이용 서비스 제공자	개인정보수집 건수 (가입 회원수) 200만명 이상

둘째, 안전진단 대상이 되는 후보 업체에게 정기적으로 안내문을 발송하거나 혹은 안전진단 제도에 대한 설명회 개최가 필요하다.

셋째, 대상자 확인 및 대상 선정에 이의가 있는 업체에 대한 민원 처리를 위한 법적근거가 마련되어야 한다. 또한 악의적으로 제도를 피해갈 수 있는 다양한 편법(예 : 상호분할, 자업자분할, 기업분할, 접속정량제 시행, 고의적 서버다운 등)이 예상되므로 추가적인 요건 정의가 필요하다.

그리고 소규모 VIDC 사업자 등에 대한 적용상의 문제와 관련하여 개선방안에서는 사업자 유형에 따른 적용기준 항목을 총매출액 50억 이상으로 설정했기 때문에 상당수의 소규모 VIDC 사업자들은 제외될 가능성이 높다. 저비용의 안전진단 수검비용을 산정해 적용하는 방안, 일부 국고 보조나, 관련 기관을 통한 일괄적인 안전진단을 추진하는 방안도 추가로 검토하면 좋을 것이다.

4. 결 론

정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위해 도입된 안전진단 제도는 정착단계로 진입하고 있다. 그러나 안전진단 제도가 국내의 정보통신 서비스 제공자의 정보보호 수준을 향상하며, 체계적이고 효율적으로 제도가 운영될 수 있도록 하기 위해서 특히 사업자 선정기준에 대해서

본 연구에서는 현행 제도에서의 현황 및 문제점을 바탕으로 개선방향을 도출하였다.

그 내용을 요약하면, 전체 정보통신 서비스 사업자를 일괄적으로 총매출액 100억 이상, 또는 일평균 사용자수 100만 이상인 사업자를 안전진단 대상 사업자로 규정했던 현행 기준을, 사업자 유형에 따라서 구분하여, 기준항목을 달리 적용하도록 하였다. 즉, 주요 정보통신서비스 제공자(ISP)와 집적 정보통신시설 사업자(IDC)에 대해서는 현행 안전진단 대상 사업자 기준으로 적용하고 있는 총매출액 100억 이상인 사업자에서 50억 이상으로 조정하여 개인정보 피해사례를 줄일 수 있도록 제도를 강화하고, 쇼핑몰 등 다중이용 서비스 제공자에 대해서는 개인정보수집 건수 즉, 가입 회원수가 200만 명 이상인 사업자를 대상으로 적용하는 방안이 바람직하다고 판단된다.

이러한 기준을 적용하기 위해서는 연간 1회의 개인정보 수집건수를 자료로 제출하도록 하는 법규정의 제도화가 선행되어야 하므로, 현행 제도의 연속성을 유지하는 차원에서 잠정적으로는 사업자의 일평균 사용자수를 적용하는 경과조치를 포함할 수도 있을 것이다.

본 연구의 제약사항으로는 안전진단 제도의 성과인 사업자들의 정보보호 수준향상 정도를 계량적으로 측정하기 위해 필요한 정보가 사업자의 내부 보안 또는 영업 기밀에 속하는 사항으로서 접근이 어렵기 때문에, 분석 대상 자료가 제한적이어서 결과 해석에 유의해야 할 것으로 판단된다.

본 연구에서 제시한 개선방안들을 적용함으로써 기대되는 효과는 첫째, 현행보다 더 높은 정보보호 수준을 유지하도록 함으로써 안정성을 제고하고, 둘째, 소규모 집적시설 사업자(VIDC)에 대해서는 정보통신 매출액 규모를 통해서만 적용하므로 일부 영세 사업자에 대해서 합리적인 예외성을 허용하며, 셋째, 현행 일평균 사용자수 항목보다 명확한 개념을 가진 개인정보 수집건수(즉, 가입 회원수) 항목으로 변경하여 합리성을 높이는 것은 물론, 기타 사업자들이 자발적인 참여의지를 가지고 평가 결과가 우수한 수준으로 나타난 경우 향후 3년간 안전진단 대상에서 유예하는 방안 등을 통해서 자발적으로 정보보호 수준을 높이는 제도 정착의 효과를 기대할 수 있다.

참 고 문 헌

[1] Harbour, Jerry L., The Basics of Performance Measurement, Quarterly Resource, 1997.

[2] 강병서 · 김계수, 사회과학 통계분석, 한나래, 2005, p.238.

[3] 강병서 · 김계수, 사회과학 통계분석, 한나래, 2005, p.95

[4] 국가인권위원회, 인권 관련 정부통계 현황에 대한 실태조사 (2005년도인권상황 실태조사 연구용역보고서), 2005.

[5] 안연식, 서정훈, 장상수, 정보보호 안전진단 대상자 선정기준의 개선 연구, 한국IT서비스학회 2008년 춘계학술대회 발표논문집, 2008, pp.572-577.

[6] 정보통신부, 2007년 정보화에 관한 연차보고서, 정보통신부, 2007.

[7] 정보통신윤리위원회, 2004년도 정보통신서비스 제공자 실태조사, 2005.

[8] 통계청, 사이버 쇼핑몰 통계조사 결과, 2007.

[9] 한국정보보호진흥원, 2004년도 정보보호 안전진단 대상자 현황조사 결과 보고서, 2004.

[10] 한국정보보호진흥원, 인터넷 침해사고 동향 및 분석 월보, 인터넷침해사고대응지원센터, 2008.

[11] 한국정보보호진흥원, 정보보호 안전진단 기준 해설서, 2007.

[12] 한국정보보호진흥원, 정보보호 안전진단 방법 · 절차 · 수수료에 관한 해설서, 2007.

[13] 한국정보보호진흥원, 정보보호 안전진단 제도 개선 및 발전방안 연구, 2005.

[14] 한국정보보호진흥원, 정보보호 안전진단을 통한 기업보안 수준 강화전략, 2007.

◈ 저 자 소 개 ◈

안 연 식 (ahndreo@kyungwon.ac.kr)

현재 경원대학교 경상대학 경영학과 교수로 재직중이며, 연세대학교에서 전자계산학 전공(석사), 국민대학교 정보관리학부에서 경영정보시스템을 전공(박사)하였다. 한국전력공사와 한전KDN(주)에 재직하며 소프트웨어 엔지니어와 IT컨설턴트로 활동하였고, 전자계산조직응용기술사와 정보시스템감리사 자격을 보유하고 있다. 연구결과는 정보처리학회지, 경영학연구, 정보통신정책연구, 한국IT서비스학회지, Information System Research, Journal of Software Maintenance and Evolution 등의 국내외 학술지 게재와 한국데이터베이스학회, 한국경영과학회, 경영정보학회, International Conference on the Software Engineering and Data Engineering 등의 학술대회에서 논문으로 발표하였으며, 한미간 FTA체결이 우리나라 소프트웨어산업에 미치는 영향 등 다수의 연구과제를 수행한 바 있다. 주요 관심분야는 기술경영, 정보시스템 평가 등이다.