情 報 保 護 學 會 誌
第 12 券 第 4 號, 2002. 8

정보통신서비스제공자의 정보보호의무

박 영 우*

요 약

오늘날 인터넷 등 정보통신망의 이용이 보편화 되면서 우리는 바야흐로 정보 및 정보시스템이 없는 생활을 생각할 수 없는 이른바 정보사회에 살고 있다. 정보사회에서는 정보가 중요한 생산수단이 되며 또 경제적 가치를 갖는다. 따라서 정보를 제대로 보호하고 또 정보가 안전하게 처리, 이용될 수 있는 환경을 마련하는 것이 중요한 국가, 사회적 과제가 된다. 이에 각 정보주체가 자신의 정보와 시스템을 내, 외부의 위협으로부터 보호할 일차적 책임을 진다. 그러나 정보통신서비스제공자는 자신의 정보와 시스템을 보호하는 정보주체로서의 일차적 책임 뿐만 아니라, 기업이나 개인과 같이 타인의 정보통신을 매개하는 사업자로서 송수신 또는 처리되는 타인의 정보를 적절히 보호하여야 할 의무가 있다. 현행 법률을 중심으로 정보통신서비스제공자의 정보보호의무의 개념과 성격 그리고 그 구체적인 내용을 살펴보았다.

Ⅰ. 서 론

정보통신기술의 발달로 21세기 사회는 이제 정보사회로 불리고 있다. 정보사회는 특히 인터넷이라는 글로벌한 정보통신 네트워크를 통하여 행정, 의료, 교육 및 상거래를 영위하게 되었다. 이러한 변화과정에서 과거 전화국으로만 표현되던 정보통신의 매개자도 다양한 형태와 내용의 서비스를 제공하는 정보통신서비스제공자로 변화하였다.

한편 정보통신기술의 발달로 현대사회는 다양한 정보통신 서비스를 이용할 수 있게 된 반면, 정보시스템이 가지고 있는 취약점과 이를 이용한 각종 위협으로 인하여 안전하고 신뢰할 수 있는 정보이용이 위협받고 있다. 이에 따라 세계 각국은 자국의 정보시스템과 글로벌 네트워크인 인터넷의 안전·신뢰성 확보를 위하여 여러 가지 정보보호 시책을 추진하고 있다. 그중의 하나가 법제도적인 측면에서 정보보호를 의무지우고 이를 지키도록 하는 것이다.

다음에서는 국내 현행법률상 정보통신서비스제공자를 중심으로 정보보호 의무에 대해 살펴본다. 다만, 개인정보 보호문제에 대하여는 독립한 글로써 다루는 것이 적절하다고 생각하여 이 글에서는 이를 제외한 일반적인 정보보호 문제를 가지고 살펴본다.

Ⅱ. 정보보호의 법률개념

현행법상 정보보호에 대한 개념정의는 정보화촉진기본법에서 정의하고 있다. 동법 제2조 제4호는 "정보보호라 함은 정보의 수집·가공·저장·검색·송신·수신중에 정보의 훼손·변조·유출 등을 방지하기 위한 관리적·기술적 수단(이하 "정보보호시스템"이라 한다)을 강구하는 것을 말한다"고 규정한다.

정보보호에 대한 이 개념정의는 앞으로 살펴보게 될 정보통신서비스제공자의 정보보호 의무와 관련해서도 유효하다고 할 수 있다. 이는 정보통신망이용촉진및정보보호등에관한법률(이하 '정보통신망법'이라 약칭한다.) 제2조제2항이 동법에서 정하는 것을 제외하고는 정보화촉진기본법의 용어정의를 따르도록 하고 있기 때문이다.

그러나 정보화촉진기본법의 정보보호의 개념정의가 과연 적절한지는 의문이다. 이는 지나치게 정보 즉 데이터(data) 중심적이며, 따라서 정보의 처리, 교환, 저장이 이루어지며 일정한 업무를 처리하는 정보시스템에 대한 보호는 포괄하지 못한다.

종래 ISO/IEC TR 13335-1 (IT 보안관리 가이드라인)이나 ISO/IEC 7498-2 (기본참조모델)에서 정보 및 정보시스템에서 요구되는 보안(security)

* 한국정보보호진흥원 기획단 정책연구팀(ywpark@kisa.or.kr)

요건이 정해져 있는바, 인터넷이 사회기반으로서 중요성이 커지고 있는 중에 대책을 구체적으로 검토하기 위하여 보안 요건도 기밀성, 완전성 및 가용성의 3요건 뿐만 아니라 네트워크 사회의 계약이나 절차라고 하는 정보의 고도한 이용을 전제로 한 새로운 보안요건이 필요하게 되었다. 여기서 네트워크 사회에서 필요하다고 생각되는 보안 요건을 OECD 나 ISO의 문서 등을 참고하여 정리하면 다음 8가지가 된다.[1]

(1) 기밀성(Confidentiality)
데이터 및 정보가 정당하다고 인정되는 때에 정당한 방법으로 이용하는 정당한 행위자 및 절차에만 공개되는 것 (다만, 여기서의 절차라 함은 계산처리나 데이터처리 등의 정보시스템이 행하는 처리 및 사무처리 등의 인간이 행하는 처리를 가리킨다).

(2) 완전성(Integrity)
데이터 및 정보가 정확하고 완전하며, 그 정확하고 완전한 상태가 유지되는 것

(3) 가용성(Availability)
데이터 및 정보가 정당한 행위자에 의해 요구되었을 때 언제라도 액세스 가능한 동시에 이용 가능한 것

(4) 귀속가능성(Accountability)
행위의 형적으로부터 행위자를 한번에 특정할 수 있는 것을 보증하는 것

(5) 진정성(Authenticity)
이용자, 처리방법, 시스템 및 정보가 그 실체대로 식별되는 것을 보증하는 것

(6) 신뢰성(Reliability)
의도한 동작과 결과가 실제의 동작과 결과에 모순되지 않는 것

(7) 윤리성(Ethics)
정보시스템과 그 보안기능이 다른 사람의 권리나 재산을 존중하여 공급되고 이용되는 것

(8) 리터러시(Literacy)
보안에 대한 이해와 지식을 가져 IT를 활용할 수 있는 능력

이와 같이 볼 때 현행 법률의 정보보호는 정보 즉 데이터 중심적이고 또 소극적으로 개념이 정의되어 있음을 알 수 있다. 따라서 이는 정보 뿐만 아니라 정보시스템을 보호하는 것으로 확대되어야 하며, 또한 정보가 주된 내용인 업무의 계속성을 보장하는 것을 포괄 할 수 있도록 적극적인 개념으로 바꾸어 정의할 필요가 있다.

Ⅲ. 정보통신서비스제공자의 정보보호 의무

1. 법률규정

정보통신망법 제3조제1항은 정보통신서비스제공자의 "이용자의개인정보를 보호하고 건전하고 안전한 정보통신서비스를 제공함으로써 이용자의 권익보호와 정보이용능력의 향상에 이바지할" 책무(責務)를 규정하고 있다.

또한 동법 제45조제1항은 "정보통신서비스제공자는 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 마련하여야 한다"고 규정한다. 동법 제45조제2항은 "정보통신부장관은 제1항의 규정에 의한 보호조치의 구체적 내용을 정한 정보통신서비스의 정보보호에 관한 지침을 정하여 고시하고 정보통신서비스제공자에게 그 준수를 권고할 수 있다"고 규정한다.

동법 제45조제2항의 규정에 의거하여 제정·고시된 지침이 「정보통신서비스 정보보호지침」(2002. 1. 25, 정보통신부고시 제2002-7호)이다.

2. 정보통신서비스제공자

정보통신서비스제공자라 함은 전기통신사업자와 이가 제공하는 전기통신역무를 이용한 정보제공자 및 정보제공매개자를 말한다.

전기통신사업자는 전기통신사업법에 의한 허가를 받거나 등록 또는 신고를 하고 전기통신역무를 제공하는 자를 말한다(동법 제2조제1항 제1호). 여기서 "전기통신역무"라 함은 전기통신설비를 이용하여 타인의 통신을 매개하거나 전기통신설비를 타인의 통신용으로 제공하는 것을 말한다(전기통신기본법 제2조 제7호). 이에 해당하는 사업자로는 전기통신사업법 제4조제1항의 규정에 의한 기간통신사업자, 별정통신사업자, 부가통신사업자가 있다.

전기통신역무를 이용한 정보제공자 또는 정보제공매개자에 대하여 정보통신망법은 이를 구체적으로 규정하지 않고 있다. 따라서 어떤 사업자가 이에 해당하는지는 해석이 필요하나, 아직 정보제공자 또는

정보제공매개자의 범위에 대해 구체적인 분석을 한 논문이나 판결이 없는 실정이다. 다만, PC통신, 인터넷 등을 이용하여 정보 및 서비스에 관한 정보를 제공하는 자를 의미하며, 구체적으로는 인터넷 등의 정보통신망을 이용하여 방송프로그램 등의 디지털 정보를 제공하는 웹캐스팅(web casting), 신상품이나 이벤트(event)의 안내, 구직·구인 알선, 경품제공 등의 정보 및 서비스를 제공하기 위하여 회원모집 등의 방법으로 개인정보를 수집·이용하는 법인 및 개인 등이 이에 해당된다고 본다.[2] 그러나 전자서명 인증기관은 기본적으로 전자서명에 사용되는 키(데이터)의 소유자가 누구인지 확인하는 서비스를 제공하는 자로서 정보제공자 또는 정보제공매개자라고 보기 어려우며, 또한 전자서명 인증기관에 대해서는 별도의 법률(전자서명법)에서 독립하여 규정하고 있으며 매우 높은 수준의 정보보호의무를 부과하고 있다.

3. 정보통신서비스제공자의 정보보호의무의 성격

정보통신서비스제공자의 정보보호의무는 어떠한 성격의 의무인가. 먼저 정보통신망법 제3조제1항에서 규정하는 정보통신서비스제공자의 책무는 법률상 강제되는 의무가 아니다. 즉 책무란 권리자에게 자기 자신의 이익을 지키기 위하여 그 준수가 요청되는 강도가 약한 의무로서, 위반시 법률상의 이익의 상실 또는 감소라는 일정한 법적 부담이 가해질 뿐 법률상 손해배상이나 형벌 및 행정벌로써 강제되지 않는 의무를 말한다.[2] 따라서 정보통신망법은 제3조제1항의 위반에 대하여 아무런 처벌규정도 두고 있지 않다.

그러면 이와는 달리 정보통신망법 제45조제1항에서 규정하는 정보통신서비스제공자의 정보보호 의무는 진정한 법적의무인가. 그러나 이에 대해서도 동법은 그 위반에 대하여 아무런 처벌규정도 두고 있지 않을 뿐만 아니라, 동조제2항에서 정보통신부장관이 이 의무의 구체적인 내용을 정하는 '정보통신서비스의 정보보호에 관한 지침'을 정하고 그 준수를 권고할 수 있다고 규정할 뿐이다. 따라서 정보통신망법 제45조제1항의 의무도 법률상 강제되지 않는 의무 즉 책무로 해석할 수 있다. 그러나 다음과 같은 점에서 정보통신망법 제45조제1항의 의무는 동법 제3조제1항의 책무와는 달리 보아야 한다고 생각한다. 우선 정보통신망법 제45조제1항은 "보호조치를 마련하여야 한다"고 규정하였다. 이는 영업에 대한 규제인 공법적 규제이나 사업자와 이용자간의 거래관계에서 사업자가 이용자 일반에 대해 부담하는 계약상 신의성실의무의 내용을 이룬다고 본다. 따라서 이 조항에 직접 근거하여 이용자가 정보통신서비스제공자에게 정보보호조치를 요구할 수는 없으나, 정보통신서비스제공자가 정보보호조치를 게을리 하여 이용자에게 손해를 입힌 경우 안전하고 신뢰할 수 있는 정보통신서비스를 제공하여야 하는 신의성실의무를 다하지 않은 경우로 해석하고 이에 대해 배상책임을 지는 것으로 보아야 한다.

4. 정보통신서비스제공자의 정보보호의무 내용

정보통신서비스제공자가 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위하여 취하여야 하는 보호조치는 단순히 기술적인 조치 외에 필요한 물리적 및 관리적 조치를 모두 포괄한다. 이에 대해서는 정보통신망법 제45조제2항의 규정에 의하여 정보통신부장관이 제정·고시한 「정보통신서비스 정보보호지침」이 보호조치의 구체적인 내용을 정하고 있다.

동지침에 의하면 이러한 보호조치에는 장소적 접근통제, 인적 출입제한, 전원접속, 시스템의 백업, 자연재해로부터의 방비대책 등 물리적인 요소는 물론, 전산망에 대한 접속방법과 접속절차, 사용자에 대한 이용등급의 지정, 중요자료 및 명령어에 대한 접근차단 방법 등 컴퓨터와 관련한 소프트웨어적, 하드웨어적인 기술을 모두 포함한다. 따라서 사용자의 식별코드(ID)와 계정관리(Account Administration), 전자지갑이나 전자화폐 또는 각종 통신망에서의 인증절차를 위한 전자서명, 비상복구절차, 시스템과 데이터의 백업과 지역분리 보전방법, Password Data의 보호조치, 비작동 기간중의 세션단절과 Log-on 시도 횟수 등의 제한을 통한 불법침투방지, 통신망 사용자에 대한 인증절차를 위한 토큰(Token)의 설정이나 사용자 인식번호(PIN)의 지정, 접속시도한 전화·모뎀이나 터미널의 식별장치 등을 예로 들 수 있다.[2]

5. 주요정보통신기반시설관리기관인 정보통신서비스제공자의 정보보호의무

2001년 1월 우리나라는 사회 인프라의 핵심이 되는 정보통신기반시설을 각종 전자적 침해행위 즉,

해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 또는 고출력 전자기파 등에 의한 공격행위로부터 보호하는 조치의 근거법률로서 「정보통신기반보호법」을 제정하였다. 동법에 의하면 정보통신망법의 적용대상인 정보통신망 가운데 주요정보통신기반시설로 지정되는 경우 이 법률의 적용을 받는 것으로 되어 있다(동법 제1조, 제2조 제1호, 제8조제1항). 따라서 정보통신서비스제공자는 자신이 관리하는 정보통신망이 동법에 따라 주요정보통신기반시설로 지정된 때에는 동법의 규정에 따라 취약점 분석·평가, 보호대책 수립·시행 등 특별한 정보보호조치를 취하여야 한다.

주요정보통신기반시설인 정보통신망을 관리하는 정보통신서비스제공자의 경우 정보통신망법과 정보통신기반보호법 중 어느 법률의 적용을 받는가가 문제될 수 있다. 이와 관련하여 정보통신망법 제5조는 "정보통신망이용촉진및정보보호등에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법이 정하는 바에 의한다"고 하여 정보통신망법이 일반법임을 밝히고 있다. 따라서 주요정보통신기반시설인 정보통신망을 관리하는 정보통신서비스제공자는 우선 정보통신기반보호법의 적용을 받고, 동법에서 규정하지 아니한 사항에 대하여서만 정보통신망법의 적용을 받는다.

한편 주요정보통신기반시설인 정보통신망을 관리하는 정보통신서비스제공자가 정보보호조치를 취하지 아니한 경우 이에 대한 직접적인 제재는 규정하지 않고 있으며, 보호조치 명령 위반 등을 이유로 하는 과태료의 제재가 있을 뿐이다(법 제30조제1항).

Ⅳ. IDC 사업자의 정보보호 의무

1. 법률규정

정보통신망이용촉진및정보보호등에관한법률 제46조는 "①타인의 정보통신서비스제공을 위하여 집적된 정보통신시설을 운영·관리하는 사업자는 정보통신시설의 안정적 운영을 위하여 정보통신부령이 정하는 바에 의한 보호조치를 취하여야 한다. ②제1항의 규정에 의한 사업자는 집적된 정보통신시설의 멸실, 훼손 기타 운영장애로 인하여 발생한 피해의 보상을 위하여 정보통신부령이 정하는 바에 따라 보험에 가입하여야 한다. ③정보통신부장관은 제1항의 규정에 의한 보호조치를 취하지 아니한 사업자에게 상당한 기간을 정하여 시정조치를 명할 수 있다."고 규정한다.

정보통신망법 제46조제1항의 규정에 의거하여 정보통신망법시행규칙 제4조(집적된 정보통신시설의 보호조치)는 "①타인의 정보통신서비스제공을 위하여 집적된 정보통신시설을 운영·관리하는 사업자가 법 제46조제1항의 규정에 의하여 정보통신시설의 안정적 운영을 위하여 취하여야 하는 보호조치는 다음 각호와 같다.

1. 정보통신시설에 대한 접근 권한 없는 자의 접근 통제 및 감시를 위한 기술적·관리적 조치
2. 정보통신시설의 지속적·안정적 운영을 확보하고 화재·지진·수해 등의 각종 재해와 테러 등의 각종 위협으로부터 정보통신시설을 보호하기 위한 물리적·기술적 조치
3. 정보통신시설의 안정적 관리를 위한 관리인원 선발·배치 등의 조치
4. 정보통신시설의 안정적 운영을 위한 내부관리계획(비상시 계획을 포함한다)의 수립 및 시행

②정보통신부장관은 관련 사업자의 의견을 수렴하여 제1항의 규정에 의한 보호조치의 구체적인 기준을 정하여 고시한다. ③정보통신부장관은 제1항의 규정에 의한 보호조치의 이행확인을 하는 과정에서 다른 기관이 수행하는 업무와 관계되는 때에는 해당 기관과 미리 협의하여야 한다."고 규정하고 있다. 그리고 정보통신망법시행규칙 제4조제2항의 규정에 의거하여 「집적정보통신시설보호지침」(2001. 9. 26, 정보통신부 고시 제2001-83호)이 제정·고시되었다.

또한 정보통신망법 제46조제2항에 의거하여 동법 시행규칙 제5조(보험가입)는 "①타인의 정보통신서비스제공을 위하여 집적된 정보통신시설을 운영·관리하는 사업자는 법 제46조제2항의 규정에 의하여 사업 개시와 동시에 책임보험에 가입하여야 한다. ②제1항의 규정에 의하여 사업자가 가입하여야 하는 책임보험의 최저보험금액은 별표와 같다."고 규정하고 있다.

2. IDC 사업자

타인의 정보통신서비스제공을 위하여 집적된 정보통신시설이란 바로 인터넷 데이터 센터(Internet Data Center)를 말한다. 이 인터넷 데이터 센터

를 운영·관리하는 사업자(이하 "IDC 사업자"라 한다)는 정보통신망법에서 말하는 정보통신서비스제공자는 아니다. 따라서 IDC 사업자의 정보보호조치 의무를 따로 규정하고 있는 것이다.

3. IDC 사업자의 정보보호의무 내용

IDC 사업자의 정보보호 의무는 정보통신서비스제공자의 정보보호 의무와는 다르다. 첫째, 규정형식면에서 IDC 사업자에 대해 별도로 규정하고 있고, 둘째 정보보호 의무와 관련하여 보험가입의무가 부과되고 있다.

IDC 사업자가 집적정보통신시설의 안정적 운영을 위하여 취하여야 하는 보호조치는 다음과 같다.

- 정보통신시설에 대한 접근 권한 없는 자의 접근 통제 및 감시를 위한 기술적·관리적 조치
- 정보통신시설의 지속적·안정적 운영을 확보하고 화재·지진·수해 등의 각종 재해와 테러 등의 각종 위협으로부터 정보통신시설을 보호하기 위한 물리적·기술적 조치
- 정보통신시설의 안정적 관리를 위한 관리인원 선발·배치 등의 조치
- 정보통신시설의 안정적 운영을 위한 내부관리계획(비상시 계획을 포함한다)의 수립 및 시행

이들 보호조치의 구체적인 기준은 앞에서 언급한 「집적정보통신시설보호지침」(2001. 9. 26, 정보통신부 고시 제2001-83호)에서 상세히 정하고 있다.

한편 IDC 사업자는 사업개시와 동시에 매출액이 100억 이상인 경우 10억원, 10억 이상 100억 미만인 경우 1억원, 10억 미만인 경우 5천만원을 최저보험금액으로 하는 책임보험에 의무적으로 가입하여야 한다(시행규칙 제5조제2항). 이 때 매출액은 책임보험에 가입하여야 할 연도의 직전사업연도의 매출액을 말하며, 직전사업연도의 매출액이 없거나 매출액 산정이 곤란할 경우에는 당해 사업자가 예측한 향후 1년간 매출액을 말한다.

4. IDC 사업자의 정보보호의무 위반에 대한 제재

IDC 사업자의 경우에도 직접적인 정보보호의무 위반에 대해서는 아무런 제재규정이 없다. 그러나 정보통신망법 제46조제2항의 보험가입의무에 위반하거나 동법 제46조제3항의 시정조치명령에 위반한 경우 이에 대해 500만원 이하의 과태료를 부과한다(법 제67조제1항).

V. 결 론

이상 살펴본 바와 같이 우리나라의 현행법률은 다른 나라와 비교하여 정보보호에 대하여 상세히 규정한 편이라고 할 수 있다.

그러나 우선 정보보호의 개념이 해당 법률에서 보호하고자 하는 것이 정보 즉 데이터 자체에 국한되는지 또는 이것뿐만 아니라 정보시스템 더 나아가서는 이를 기반으로 하는 업무의 계속성을 보장하려는 것인지가 잘 구분되고 있지 않다. 따라서 각각의 경우에 보호대상이 무엇인지를 우선 분명히 할 필요가 있다.

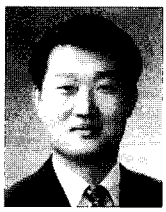
또한 정보통신서비스제공자의 경우 일부는 정보통신기반보호법 및 전자서명법의 적용도 받게 되어 이중 또는 삼중의 의무를 부담하게 될 수도 있는데, 이와 관련하여 해당법률들 간의 적용관계가 분명하지 않다. 한편 정보통신서비스제공자라 하여도 제공하는 서비스의 종류, 규모 및 보유하는 정보시스템 등이 반드시 동일하지는 않다. 그럼에도 불구하고 현재 법률 특히 각종 지침은 이를 구분하지 않고 획일적인 정보보호기준을 제시하고 있다고 생각되며, 또 상이한 조건이나 환경을 모두 포괄할 수 있는 융통성있는 기준으로는 생각되지 않는다. 그렇기 때문에 법률 스스로 해당규정이나 이에 근거한 각종 지침을 그 준수를 당사자의 임의에 맡기는 '권고적 성격'으로 규정할 수 밖에 없는 것이다. 법은 이를 준수하여야 할 자가 불가능한 것을 기대하지는 않는다. 따라서 각 사업자에게는 그 사업자의 사업종류, 영업규모 및 보유시스템 등의 조건에 맞추어 그에 알맞은 정보보호가 의무지워질 필요가 있다. 이를 위하여는 모든 사업자에게 공통적으로 적용할 수 있는 기본기준을 일반적이고 추상적으로 제시하고 각 사업자는 이를 자신에게 맞는 정보보호정책으로 구체화하도록 한 다음, 각 사업자의 정보보호정책과 그 실현내용 및 결과를 토대로 정보보호의무의 준수여부를 판단하는 것이 타당하리라고 본다.

참고문헌

[1] 정보통신이용에관한시큐리티보호에관한검토회,

정보통신이용에관한시큐리티보호에관한검토회 보고서 - 네트워크사회의 취약성 극복을 위하여 -, 2000. 11.
[2] 정보통신부/정보보호진흥원, 개인정보보호지침해설서, 2002. 4.
[3] 김형배, 채권총론, 박영사, pp.44-45, 1992.
[4] 사법연수원, 전자거래법, p.406, 2001.
[5] 夏井高人, 네트워크사회의문화와법, 일본평론사, 1997.

〈著者紹介〉



박 영 우 (Young-woo Park)
1985년 2월 : 고려대학교 법과대학 졸업
1988년 8월 : 고려대학교 대학원 법학과 석사과정 수료, 법학석사
1995년 8월 : 고려대학교 대학원 법학과 박사과정 수료, 법학박사
1995년 1월~1998년 6월 : 법무부 법무자문위원회 연구위원
1998년 7월~현재 : 한국정보보호진흥원 선임연구원
관심분야 : 정보보호 정책, 정보법학