情 報 保 護 學 會 誌
第20卷 第1號, 2010. 2

일본 중소기업 정보보호 대책 가이드라인 동향

박 춘 식*

요 약

정보화의 진전에 따라 기업의 정보화도 급속하게 추진되고 이에 따른 역기능인 정보보호 문제도 함께 고려해야 하는 실정이다. 특히 개인 정보 유출, 영업 영보 누설, 기업 내부 핵심 기술 유출 등은 현재 중소기업이 직면하고 있는 문제이며 대기업으로 부터의 위탁 업무를 수행하거나 자체 업무를 위해서도 정보보호 대책을 마련하지 않으면 안 되는 상황임은 주지의 사실이다. 그러나 많은 통계나 보고 자료에서 알려진 바와 같이 자금 면이나 인력 면 등에서 중소기업이 정보보호 대책을 수립하고 이를 구현하여 운영하는 것은 여러 면에서 어려운 것 또한 사실이다. 이러한 중소기업의 실정을 고려하여 우리나라에서는 2006년도 정보보호진흥원(현재 한국인터넷진흥원)에서 중소기업을 위한 정보보호 가이드라인을 발행하여 중소기업의 정보 보호 대책을 수립하는 등 중소기업의 정보보호 대책을 위한 많은 지원을 해 왔다. 우리나라와 유사한 환경에 있는 일본에서도 최근 중소기업 정보보호 대책 가이드라인을 발행하였다. 이에 본고에서는 국내 중소기업 정보보호 대책 수립과 지원에 참고하고자 2009년도에 발행한 일본 중소기업 정보보호 대책 가이드라인을 소개하고 시사점을 살펴보고자 한다.

Ⅰ. 서 론

최근 정보화의 진전과 정보화의 진전에 따른 역기능의 영향은 우리나라 기업 전체 수의 99%를 차지하는 중소기업에도 많은 영향을 미쳐 사회적 관심이 높아지고 있다. 정보화의 진전으로 중소기업마다 약간의 차이는 있지만 고객관리, 경리 업무, 영업 업무 활용, 연구개발업무 등 다양한 업무에 IT가 많이 활용되고 있으며 업무 의존도도 높은 실정이다.

그러나 정보 시스템이 장애가 발생하거나 해킹 등 외부 침입에 의해 시스템이 정지되거나 데이터 손실이나 누설 또는 고객의 개인 정보 등이 유출될 경우에는 중소기업의 업무에도 커다란 영향을 미치게 된다. 고객으로부터의 신뢰를 잃어버림은 물론 중소기업의 경영에도 치명적인 위기 요소가 될 수도 있다. 또한 최근에는 위탁업무와 관련하여 개인 정보나 영업 비밀에 관련된 정보관리의 중요성에 대한 인식이 높아지고 있어, 거래처로부터 정보보호 대책이나 정보보호에 대한 자격 등을 요구하고 있으며 중소기업 자체의 선호도와 관계없이, 정보보호 대책에 대한 관심을 가질 수 밖에 없는 실정이다.

한편 중소기업은 대기업에 비교해서 자금 면이나 인력 면에서 정보 보호 대책 수립이 어려우며 여러 통계 자료에서도 이러한 실상은 나타나고 있다. 이러한 중소기업의 어려운 실정을 고려하여 우리나라에서는 2006년도 정보보호진흥원(현재 한국인터넷진흥원)에서 중소기업을 위한 정보보호 가이드라인을 발행하거나 정보보호관리체계 인증, 사이버안전관리 매뉴얼 배포, 사이버 안전 취약성 진단 등을 통하여 중소기업의 정보 보호 대책을 수립하는 데 많은 지원을 해 왔다. 우리나라와 유사한 환경에 있는 일본에서도 2009년도에 중소기업 정보보호 대책 가이드라인을 발행하였다. 이에 본고에서는 국내 중소기업 정보보호 대책 수립과 지원에 참고하고자 2009년도에 발행한 일본 중소기업 정보보호 대책 가이드라인을 소개하고자 한다.

일본의 중소기업도 우리나라와 같이 전체 기업의 99%를 차지하고 있으며 일본 산업 경쟁력의 근간을 이루고 있다. 일본 중소기업의 정보화는 많은 진전을 이루고 있으며, 이러한 정보화 진전에 따른 정보보호의 필요성도 많이 인식하고 있다. 우리나라 중소기업의 정보보호 현황처럼 일본 중소기업도 정보 보호 대책 진전은

* 서울여자대학교 정보보호학과 교수 (csp@swu.ac.kr)

다소 늦은 실정이다. 중소기업의 정보보호에 대한 인센티브나 리소스(예산, 인력 등) 제약 등이 있다고 생각되기 때문에 중소기업에 대한 정보 보호 대책에 대한 보다 구체적인 배려가 필요하다고 생각하고 있다.

일본 경제산업성 산하 독립행정법인인 정보처리추진기구, IPA(Information-Technology Promotion Agency)에서는 보다 중립적인 입장에서의 중소기업 정보보호 문제를 검토하기 위하여 2007년도부터 중소기업 정보보호 대책 연구회를 만들어 중소기업에서의 정보보호 관련 조사를 시작으로 중소기업 정보보호 수준 제고를 위한 활동을 추진해 왔다. 2008년도에는 연구회 산하에 워킹 그룹을 두어 중소기업이 직면하고 있는 문제점들에 대하여 실용적이고 적용 가능한 중소기업 정보보호 대책 가이드라인을 검토하여 2009년도에 "중소기업 정보보호 대책 가이드라인"을 발행하게 되었다. 따라서 본고에서는 일본의 중소기업 정보보호 대책 가이드라인 동향을 살펴보고 가이드라인 자체를 소개하고 그 시사점을 분석하여 우리나라 중소기업 정보보호 정책 수립이나 중소기업 정보보호 대책 향상에 참조가 될 수 있도록 하고자 한다.

Ⅱ. 일본의 중소기업 정보보호 가이드라인

2.1 배경 및 추진 경위

중소기업은 정도의 차이는 있지만 정보화의 영향을 받고 있으며 이로 인한 정보보호 대책에 대해서도 중요성을 인식하고 있다. 게다가 서비스업이나 제조업 등에서는 중소기업이라 할지라도 거래처로부터 정보보호대책을 요구하는 경우가 많아지고 있다. 이것은 기업 규모에 불구하고 개인정보나 영업 비밀을 위탁하는 경우 정보관리의 중요성에 대한 의식이 높아지고 있는 것이 배경이 되고 있다. 이와 같이 기업에서는 싫던 좋던 정보보호대책 수립이 요구된다. 한편 중소기업은 대기업에 비교하면 자금 면이나 인재 면에서의 제약 때문에 정보보호대책 수립이 어렵다고 말해왔다. 실제로 통계상으로도 대기업과 비교하면 대책이 추진되고 있지 않은 경향이 보여 지고 있다. 반면 중소기업은 정보보호대책을 행함에 있어서 유리한 조건을 가지고 있다. 그것은 경영자를 포함한 종업원의 얼굴이 보일 정도라는 것이다. 정보보호의 첫 단계는 경영자가 정보보호의 중요성을 스스로 인식하고 그 중요성을 종업원에게 전달하고 종업원이 정보보호 대책을 수립 실행하는 의미를 이해하는 것이다. 즉, 종업원의 얼굴이 보인다는 것은 정보보호대책을 효율적으로 추진하기 위해서는 아주 유리한 조건인 것이다. 또한, 이러한 특성을 잘 이용해서 비용이 들지 않는 대책을 실현할 수도 있다. 일본의 중소기업 정보보호 대책 가이드라인은 중소기업에 필요한 정보보호 대책을 중소기업 관점에서 실현하기 위해 필요한 대책을 소개하기 위한 것이다. 일본 IPA는 2007년부터 중소기업에 있어서 정보보호 대책 촉진을 목적으로 지속적인 검토를 해 왔다. 중소기업 정보보호 대책을 고려할 경우, 위험에 따른 대책 마련이 중요하나 중소기업은 기업의 규모나 업종에 따라 다양하여 일괄적으로 정보보호 대책을 마련하거나 검토하는 것은 곤란한 점이 있음을 잘 파악하면서 추진하였다. 또한 거래 관계에 있어서도 대기업으로부터 업무 위탁을 받는 중소기업에 요구되어지는 정보보호 대책의 수준은 중소기업 자체 대책의 수준과는 동일하지 않을 가능성이 있음도 잘 파악하고 추진하였다. 따라서 IPA 연구회에서는 중소기업의 정보 보호 대책의 요건을 검토하는 경우에는 정보보호 위험의 대소에 따른 다양한 수준의 대책과 중소기업의 다양성과 그것에 기인한 정보보호 위험의 대소에 따른 고려를 기본적인 검토 방향으로 삼았다. 중소기업이 구비해야만 하는 정보보호 수준과 위탁 관계에 있어서 구비해야 하는 정보보호 수준은 서로 다른 것으로 취급하였다. 또한 다양성을 너무 고려하는 경우 오히려 중소기업 대책 마련이 곤란하여 다양성 및 단순성을 중시하였다. 중소기업 정보보호 대책 연구회에서는 2007년도 이어 2008년도에는 정보 보호를 고려한 적정한 거래 추진과 중소기업 정보보호 대책 향상의 두 가지 관점에서 검토를 행하였다. 정보보호를 고려한 적정한 거래 추진 분야는 2007년도 조사에서 나타난 결과를 중심으로 중소기업이 구비해야 하는 정보보호 수준과 위탁 관계에 있어서 구비해야 하는 정보보호 수준은 반드시 동일하지 않은 점을 고려하여 위탁 관계에 있어서 정보보호 대책의 요구 사항이 무엇인지 검토하는 것으로 정보보호를 고려한 적정한 거래의 추진을 목적으로 하였다. 두 번째의 중소기업 정보보호 대책 향상은 중소기업의 다양성을 고려하여 중소기업에서도 실시 가능한 실효성 있는 대책을 제시하여, 중소기업의 정보보호 수준 향상을 목적으로 하였다. IPA Security Center는 IPA내에

중립적 입장의 검토를 위하여 중소기업 정보보호 대책에 관한 연구회를 설치하고 2007년도의 중소기업의 실태 조사와 정보보호 문제점 등 요건 도출에 이어 2008년도에는 중소기업 정보보호 대책 가이드라인을 제정하여 2009년 3월 발표하였다. 2008년도의 연구회에서는 정보보호를 고려한 적정한 거래 추진과 중소기업 정보보호 대책 향상의 검토를 행한 후 가이드라인을 작성하였다. 일본 경제산업성도 법적인 측면과 아웃소싱에 정보보호 대책 검토 등을 통하여 연구회와 협력하여 가이드라인 작성에 참여하였다. 가이드라인 작성을 위하여 연구회 산하에 워킹그룹을 3개 설치하여 가이드라인의 구체적 작업을 추진하였다. 워킹 그룹 1은 정보보호를 고려한 적당한 거래 추진의 검토를, 워킹 그룹 2와 3은 중소기업 정보보호 대책 향상의 검토를 담당하였다. 거래처의 중요 정보를 취급하는 기업에 대해서는 워킹 그룹 1이, 조직적인 정보보호 대책이 필요한 기업에 대해서는 워킹 그룹 2, 단말 베이스의 정보보호 대책이 필요한 기업에 대해서는 워킹 그룹 3이 검토하기로 하였다. 워킹 그룹 1은 발주자와 하청자의 책임 범위를 명확히 하기 위하여 실효성 있는 대책을 구체적으로 작성하였다. ISO 27001/27002, 일본의 정보보호 관리 기준 등을 참조하고 기존의 정보보호 수준확인 체크리스트 등을 참고로 검토하여 "위탁 관계에 있어서의 정보보호 대책 가이드라인"을 정리하였다. 워킹 그룹 2는 중소기업의 규모나 업종 등에 따른 보다 구체적인 시나리오 제시 등을 고려하여 BSI IT Security Guidelines 등의 기존 가이드라인 조사와 병행하여 중소기업이 갖추어야만 하는 정보보호 대책에 대해서 검토하고 "중소기업에 있어서 조직적 정보보호 대책 가이드라인"을 작성하였다. 워킹 그룹 3은 중소기업의 정보보호 수준 향상을 위하여 정보 보호 수준 향상의 기본이 되는 "5분 만에 가능한 자사 진단 시트"를 작성하였다. 중소기업 정보보호 대책 가이드라인을 발행하였지만 이에 멈추지 아니하고 중소기업 정보보호 대책 수준 향상을 위한 프로세서와 추가적으로 향후 가이드라인 등에 포함할 항목 등에 대해서 지속적으로 검토해 나가고자 하고 있다.

2.2 가이드라인 적용 범위

가이드라인의 적용 범위는 중소기업의 경영자 및 중소기업의 정보보호 관리자를 대상으로 하고 있다. 여기서 정보보호 관리자는 IT 관리자만이 아니라 총무 기획부문 등으로 정보관리를 담당하는 자도 포함하며 또한 중소기업에 대해서도 업무를 위탁하는 기업(대기업, 중소기업 관계없이)의 계약 담당자도 대상으로 하고 있다. 일본 중소기업은, 중소기업기본법 제2조 제1항에 의한 중소기업 법령상에 [표 1]과 같이 정의하고 있다. 자본금이나 종업원중의 어느 한쪽이라도 정의를 만족하면 중소기업으로 판단된다. 계속해서, 중소기업금융공고법 등의 중소기업 관련 입법에 있어서는 시행령에 의한 고무제품제조업(일부 제외)은 자본금 3억엔 이하 또는 종업원 900인 이하, 여관업은 자본금 5천만엔 이하 또는 종업원 200인 이하, 소프트웨어업·정보처리서비스업은 자본금 3천억엔 이하 또는 종업원 300인 이하를 중소기업으로 정의하고 있다.

〔표 1〕 일본 중소기업 정의

	제조업	도매업	소매업	서비스업	기타 산업
자본금	3억엔 이하	1억엔 이하	5천만엔 이하	5천만엔 이하	3억엔 이하
종업원	300인 이하	100인 이하	50인 이하	100인 이하	300인 이하

2.3 일본 중소기업이 직면하고 있는 정보보호 상의 과제

2.3.1 중소기업이 처해있는 환경

중소기업의 정보보호대책을 생각할 때, 중소기업에 비교적 많이 보이는 문제와 기업 전체의 문제로 나누어 생각해 볼 수 있다. 중소기업에 비교적 많이 보이는 문제로는 대기업과 비교해서 정보보호대책에 필요한 리소스(사람, 물건, 비용)의 제약, 대기업과 비교해서 정보화 진전 지연, 정보화 또는 정보보호 추진 동기 부족 등이 있다. 이들 문제에 대해서 일반적인 해결책은 없고 반드시 해결 하지 않으면 안 되는 문제는 아니지만 전자 메일이나 웹 등 인터넷으로 많은 서비스를 사용하는 이상, 타인에게 불편을 주지 않는 의미로 최저한의 대책은 필요하다.

한편, 기업 전체의 문제로써 중소기업에도 커다란 영향을 주는 문제로는 정보보호 대책 추진을 통한 기업 경쟁력 확보, 법 제도로 부터의 요청, 사회· 고객으로부터의 요청 등이 있다.

2.3.2 정보보호대책 추진을 통한 기업 경쟁력 확보

외부로부터의 요청을 고려해서 정보보호 대책을 추

진하는 것은 중요하지만, 한편으로 정보보호 대책을 통한 기업 경쟁력 향상이나 비용 삭감으로 연결되는 것이 가능하다.

2.3.3 회사·고객으로부터의 요청

회사 고객으로부터의 요청은 자사의 필요성에 기인한 것이던지, 법률에 규정되던 규정되지 않던 사회 전체가 기대하는 수준의 대책을 요구하거나 또는 고객과의 계약 등으로 대책이 요구되는 경우가 있다. 사회 기대 수준은 명확하게 정해진 것이 아니며 또한 대책을 행하고 있지 않다고 해서 바로 문제가 일어나는 것은 아니다. 그러나 일단 정보보호에 관한 사고가 일어난 경우, 최근에는 사회적인 지탄을 받는 경향이 높아지고 있다고 생각된다. 특히 사회 전반에서 기대되는 수준의 대책 실시에 게으른 경우에는 경우에 따라서는 경영에 영향을 주는 사태까지 이르게 된다는 사실은 인식할 필요가 있다. 고객으로부터의 요청은 간단하게 말하면 위탁 관계상의 정보보호대책이 요구되는 것이다. IPA 조사에 의하면 위탁 관계로 인하여 중소기업의 2/3가 정보보호 대책에 대한 요구를 받은 적이 있다고 응답하였다.

2.3.4 법제도상의 요청

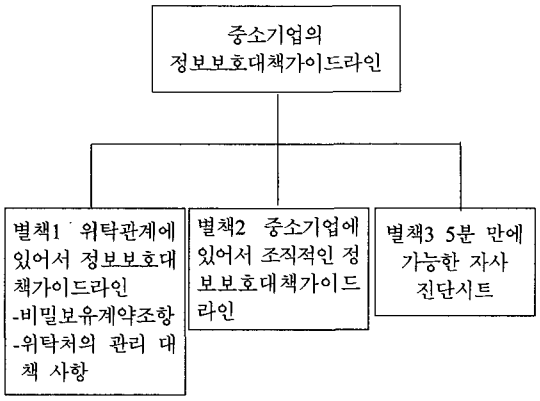
법제도로부터 요청은 간단하게 말하면 법률을 준수하기 위해 정보보호대책이 필요로 하게 되는 경우이다. 법률을 준수하기 위해 정보보호대책이 필요로 하는 경우는 주로 개인정보보호법, 금융상품거래법, 회사 내부 규정 등이다. 이들 법률은 주로 대기업을 대상으로 한 법률이지만 중소기업에도 해당하는 경우가 있다. 직접 해당하지 않는 경우일지라도, 정보의 위탁받는 곳으로서, 대기업의 자회사로서, 또는 중요한 사업거점으로서, 법률에 기준한 관리의 대상이 되는 경우가 있다는 사실에 주의할 필요가 있다.

2.4 가이드라인 사용 방법

2.4.1 가이드라인 구성과 기본적인 사용 방법

본 가이드라인은 본 가이드라인 외에 [그림 1]과 같이 3권의 별책으로 구성되고 있다.

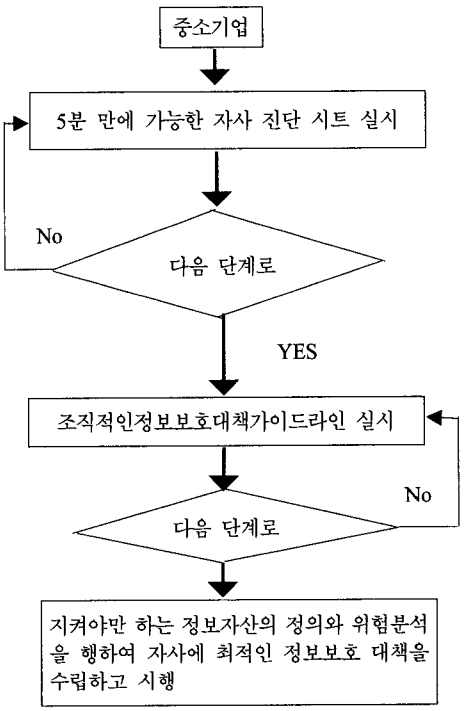
별책 1은 정보보호를 고려한 적정한 거래를 촉진하기 위하여 만들어 진 "위탁관계에 있어서 정보보호대책 가이드라인"이다. 별책1의 주요한 예정 대상층은 중소기업 등에 업무 위탁을 하는 기업의 담당자들이다. 이것은 위탁 요청 회사(또는 기관)가 정보보호 대책의 구체적인 실시 내용을 지정하지 않아 책임 관계가 애매하게 되어 결국 약한(을의) 입장에 있는 위탁 받는 곳(위탁처)이 많은 의무와 책임을 지게 되기 때문이다. 특히 중소기업은 약한 입장에 처하기 쉽다고 생각된다.



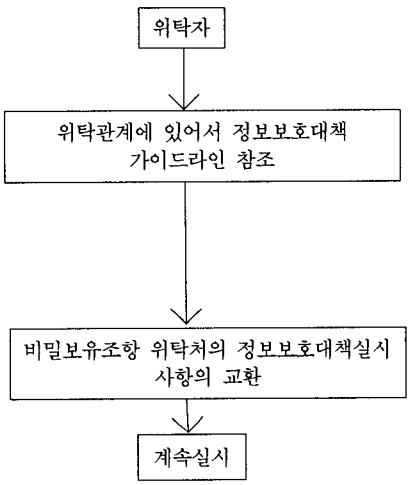
〔그림 1〕 가이드라인 구성

별책 2는 중소기업의 정보보호 대책을 높이기 위한 중소기업의 조직적인 정보보호대책 가이드라인이다. 이것은 일정 이상의 정보보호 상의 위험에 노출되어 있거나 또한, 일단 정보 누설 등의 사고가 발생한 경우, 자사 업무에 영향이 미칠 뿐만이 아니라 거래처 등에 대해서도 커다란 불편을 줄 가능성이 있는 중소기업을 주요 대상으로 하고 있다. 별책 3은 중소기업의 정보보호 대책 수준을 높이기 위해 필요한 "5분 만에 가능한 진단 시트"다. 이것은 중소기업 전체의 정보보호 대책의 출발점으로, 최저한으로 실시해야 하는 것이며 경영자나 관리자가 자주 점검하기 위한 것이다.

먼저 가이드라인 이용자가 중소기업 자신인지([그림 2]), 위탁 요청 회사인지 ([그림 3])에 따라 2가지로 나누어진다. 독자가 중소기업 자신의 경우는 먼저 별책 3의 "5분 만에 가능한 자사 진단 시트"를 실시하고 충분한 대책이 되었다고 판단한 경우는 별책 2의 "조직적인 정보보호 대책 가이드라인"을 실시한다. 다시 충분한 대책이 되었다고 판단한 경우는 ISMS 등을 이용하여 최적의 정보보호 대책을 책정하고 실시한다[그림 2]. 독자가 위탁 요청 회사(또는 기관) 입장인 경우는 별책 1의 위탁 관계에 있어서 정보보호 대책 가이드라인을 참



〔그림 2〕 가이드라인 사용 방법(1)

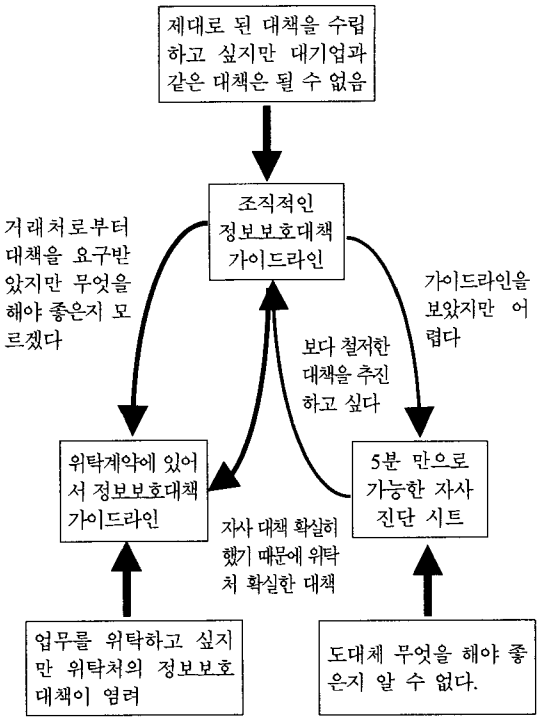


〔그림 3〕 가이드라인 사용 방법(2)

조한다[그림 3].

2.4.2 보다 높은 수준의 활용 방법

가이드라인의 기본적인 사용 방법은 2.4.1에서 보였지만 반드시 이와 같은 방법으로만 한정된 것은 아니다. 예를 들면, 위탁 요청 회사로 부터 정보보호 대책을 요



〔그림 4〕 다양한 가이드라인 활용법

구받았을 때, 조직적인 정보보호 대책 가이드라인을 활용하는 것도 생각되며, 조직적인 정보보호 대책 가이드라인의 보조로써 "5분 만에 가능한 자사 진단 시트"를 활용해도 좋다[그림 4]

또한 가이드라인보다도 높은 수준의 대책을 마련하고자 하는 경우는 IPA의 정보보호 대책 벤치마크랑, 국제표준인 ISMS 이용이나 인증 취득 등의 방법도 고려될 수 있다. 특히, IPA의 정보보호 대책 벤치마크는 중소기업도 고려하여 설계되어 있으며, 또한 가이드라인은 정보보호 대책 벤치마크와의 정합에도 유의해서 작성되어 있기 때문에 가이드라인의 다음 단계로는 최적의 것인 셈이다.

Ⅲ. 위탁관계에 있어서 정보보호 대책 가이드라인

3.1 개요

본 가이드라인은 업무 위탁에 있어서 비밀 정보를 제공하는 경우, 위탁 요청 회사로부터 위탁을 받는 위탁처에 대해서, 비밀 정보의 지정 또는 보관에 필요한 정보보호 대책의 구체적인 내용이 명시되지 않는 경우가

있다. 이러한 상황에서는, 비밀 정보의 누설 방지를 위한 적절한 대책을 기대할 수가 없다. 업무 위탁에 있어서 비밀 정보의 제공은, 위탁을 요청하는 회사로부터 위탁을 받는 위탁 처에 제공되는 경우 외에, 위탁 처에서 위탁 요청 회사에 제공하는 경우, 상호간에 제공하는 경우가 있지만, 여기에서는 비밀 정보를 위탁하는 회사가 위탁 처에 제공하는 경우만을 주로 검토하였다. 그리고 거래기본계약서, 개별계약서, 각서, NDA(Non-Disclosure Agreement), 협의나 구두에 의한 확인, 또는 매매계약서, 대리점계약서 등, 또는 발주서, 규격서 등을 통해서 실행되는 비밀 정보의 취급에 관한 사항을 위탁 요청 회사가 해야만 하는 사항도 포함하여 "업무 위탁 계약에 관한 비밀관리 조항(예)"으로 정리하였다. 더욱이 위탁 요청 회사로부터 제공을 받은 비밀 정보에 관해서 위탁처가 기업이 실시하는 정보보호 대책 사항인, "위탁 처의 정보보호 대책 사항"에 대해서 몇 개의 기업으로부터 실무에 사용하고 있는 사례들을 수집하여 보다 구체적으로 대책 사항의 예시를 제시하였다. 위탁 요청 회사는 본 자료를 참조하여, 위탁을 받는 위탁 처와 협의하여 비밀 정보의 지정 및 보관에 필요한 정보보호 대책의 구체적인 실시 내용을 명시하는 것이 바람직하다.

3.2 업무위탁계약에 관한 비밀 보관 조항

업무 위탁을 행하는 데 있어서 거래기본계약서, 개별계약서, 각서, NDA, 협의나 구두에 의한 확인, 또는 매매계약서, 대리점계약서 등, 또는 발주서, 규격서 등을 통해서 행해지는 비밀 정보의 취급에 관한 사항을 "업무 위탁 계약에 관한 비밀 보관 조항(예)"로써 정리한 것이다. 업무적으로는 업무 위탁의 내용, 취급하는 정보의 성질 등에 의해서 조항 및 조항의 내용을 취사선택하고, 또한 운용상의 공부 등에 의해 부족함이 없는 실효성 있는 비밀 정보 관리를 하지 않으면 안 된다. 또한, 업무 위탁처가 해외에 있는 경우, 법률, 상업 습관, 사회적 관습 등이 서로 다르기 때문에 오해가 발생하지 않도록 명확하게 기술할 필요가 있다. SaaS나 ASP 등의 서비스를 이용하는 경우라 할지라도 업무 위탁 계약서나 SLA(Service Level Agreement)로 비밀 보관에 관한 사항을 보증할 필요가 있다. 업무 위탁 계약에 관한 비밀 보관, 재위탁과 관련되어 계약서 형태의 샘플을 해당 위탁 요청자나 위탁 수행 담당인 위탁처가 필요 시 사용할 수 있도록 가이드라인에서 소개하고 있다.

3.3 위탁 처에 있어서 정보 보호 대책 사항

위탁 요청 회사로부터 위탁 처에 제공하는 비밀 정보의 관리에 관해서, 위탁 처가 실행하는 정보보호 대책 사례를 나타낸다. 구체적으로 많은 사례를 나타내기 위해 사례 상호간의 정합성은 보증되어 있지 않기 때문에 적절하게 선택하도록 한다. 위탁 계약에서는 비밀 정보의 취급과 적절한 안전 관리 조치에 대해서, 위탁자, 수탁자 쌍방이 동의한 내용을 사전에 구체화 할 필요가 있다. 구체적인 실시 대책이 없고, 위탁 요청 측이 위탁 처에 대해서, 사고가 발생한 경우의 손해 배상에 대해서만 계약에 포함시키는 것은 바람직하지 않다. 이들 사례를 참고로 비밀 정보의 종류, 업무 위탁 관계 등의 제반 조건을 고려하여 위탁 요청 기관은 위탁 처와 협의함과 동시에 위탁처가 실시할 적절한 정보 보호 대책을 지시해야만 한다. 정보 보호 대책의 주요 사항은 다음과 같다.

3.3.1 정보보호에 대한 조직적 대처

(1) 비밀 정보의 관리 취급 절차
-비밀 정보는 다른 정보와 구별해서 보관
-비밀 정보의 관리자 지정
-비밀 정보 접근 가능자의 범위 설정
-종사자 관리 대장 관리
-비밀정보관리대장 기록 관리
-비밀 복제 등 위탁 요청 기관의 사전 승인
-비밀 반출 시 위탁 요청 기관 등 사전 승인
-비밀 반출 시 파일 암호화
-비밀 저장 기억 매체 안전 열쇠 기능
-비밀 폐기 및 소각 철저
-백업 규정을 정하고 정기적 실시
-비밀 포함한 이면지 사용 금지
-비밀 서류 장시간 방치 금지 규정 운영
-정보 보호 운용 상태 정기적 확인
-정기적 비밀 취급 업무 내부 점검 실시 등

(2) 비밀 정보에 관한 업무의 재 위탁 사항
-업무 재 위탁 시 위탁 요청 기관 사전 승인
-비밀에 관한 절차 문서화

-재 위탁 처의 정보보호의 운영 정기적 확인
-재 위탁 처의 비밀 전달 기록 관리
-재 위탁 처에 비밀 전달 시 암호화 등
-재 위탁 요청 기관과 비밀 보관에 관한 계약 체결

(3) 비밀 정보 취급 종사자 의무 및 교육
-비밀에 관한 준수 사항을 종사자에게 주지
-정기적 교육 실시 등

3.3.2 물리적 보호

(1) 비밀 보관소의 출입 및 시건 장치 관리
-비밀 정보 보관 및 취급 구역 설정
-비밀 보관소 침입 방지 대책
-비밀 보관소 출입 제한 및 기록
-시건 장치가 있는 캐비닛 등에 비밀 관리
-서버 룸의 출입 및 작업 기록 보관
-시건 장치 등의 정기적 점검
-출입기록의 정기적으로 점검

(2) 비밀 보관소의 개인 물품 반입 금지
-개인 소유 기록 매체 등의 반입 금지
-개인 소유 기록 매체 등의 업무 이용 금지
-개인 소유 PC의 사내 네트워크 접속 금지

3.3.3 정보 시스템(비밀 관련)의 운용 관리

-바이러스 대책 소프트웨어 도입
-바이러스 대책 소프트웨어 기능 활용
-정기적으로 바이러스 검사
-노트 PC의 암호화 소프트웨어의 도입
-허가되지 않은 소프트웨어 설치 금지
-기억 매체 접속 금지
-정보 시스템의 시각 정기적 동기 조정
-업무에 불필요한 웹 사이트 접근 제한
-최신의 패치를 적용하는 등 취약성 대책 등

3.3.4 비밀 정보 접근 제어

-ID와 패스워드에 의한 식별과 인증
-ID의 등록이나 삭제에 관한 규정 정비
-안전한 패스워드 사용
-스크린 세이버의 패스워드 이용
-비밀 접근 권한 재 평가 실시 및 조치 등

3.3.5 정보보호 관련 사고 대응

-비밀 누설 발생 시의 체제 및 연락망 정비
-누설 발생 의심 시 비밀관리자에게 보고
-비밀 누설 시, 위탁 요청기관에 신속 보고 등

Ⅳ. 중소기업에 있어서 조직적인 정보보호 대책 가이드라인

4.1 개요

본 가이드라인은 일정 이상의 정보보호 상의 위험에 노출되거나 또는 정보 누설 등의 사고가 발생한 경우, 자사 업무에 영향을 주는 것은 물론이고 거래처 등에 대해서도 커다란 불편을 끼칠 가능성이 있는 중소기업을 대상으로 하고 있다. 그 때문에 일정한 비용을 들여서 정보보호 대책을 행할 필요가 있지만, 중소기업의 다양함(규모, 업종 등)을 고려하면 구체적으로 어떻게 대책을 행해야 하는 지에 대해서 일정한 기준을 만드는 것은 곤란하다. 이 때문에 본 가이드라인은 중소기업이라면 공통으로 실시해야만 하는 대책과, 기업 마다 제각기의 특징을 고려해서 실시해야만 하는 대책의 2가지로 나누어서 설명하였다. 공통으로 실시해야만 하는 대책만으로도 상당한 효과가 있다고 생각되지만, 충분한 대책을 취하기 위해서는 기업 마다 고려해야 하는 대책에 대해서 각자 검토를 행하고 필요한 대책을 취하는 것이 바람직하다. 게다가 본 가이드라인에 기초한 대책을 행한 중소기업은 정보보호대책 벤치마크를 이용하기 때문에 구하고자 하는 대책의 달성 상황을 파악하거나 다양한 기업 가운데에서 자사의 위치를 파악할 수 있다. 이것에 의해 부족한 대책이 판명되었을 때는 다시 본 가이드라인을 참조하여 필요한 대책에 대해서 검토하는 것이 중요하다.

4.2 정보·정보자산과 정보보호

정보보호란 정보의 기밀성, 완전성 및 가용성을 유지

하는 일. 게다가 진정성, 책임 추적성, 부인방지 및 신뢰성 등을 유지하는 것도 정의되어 있지만 간단히 말하면 기업의 경우 기업 비밀이나 개인정보 등의 정보를 어떻게 지키는 가 또는 그 정보를 취급하는 정보시스템을 어떻게 지키는 가이다. 기업이 반드시 지켜야만 하는 정보에는 전자적인 정보만이 아니라 종이 정보도 포함된다. 게다가 예를 들면 제조업이라면 시작품이나 금형 등, 순수한 정보만이 아니라 물건으로 구체화된 정보도 포함되는 경우가 있다. 이와 같은 물건으로 구체화된 정보는 특허 등으로 지키는 것은 어렵고 비밀정보로 관리하는 것이 적절한 경우가 있기 때문이다. 정보와 유사한 말에 정보자산이라는 단어가 있다. 정보와 정보자산은 거의 유사한 의미로 사용되는 경우도 많지만 정보자산은 다양한 정보 가운데, 기업으로써 관리해야만 하는 대상으로서 선택된 것을 말한다. 이것은 기업 가운데에서 난무하는 정보를 모두 관리하는 것은 불가능하며 또한 의미가 없기 때문이다. 또한 정보시스템 등도 정보자산에 포함되는 경우가 있다. 정보보호의 첫걸음은 제 각각의 기업이 자사의 정보자산이 무엇인지 파악하는 것이다.

4.3 공통으로 실시해야만 하는 대책과 기업마다 고려해야만 하는 대책

본 가이드라인에는 중소기업에 있어서 공통으로 실시해야만 하는 대책과 기업 마다 고려해야만 하는 대책의 2가지로 나누어 설명한다. 공통적인 대책에서는 본 가이드라인의 대상이 되는 기업이라면 그 기업의 규모나 업종에 관계없이 필요로 하는 대책에 대해서 예를 들어 가면서 설명되어 있다. 기업 마다 고려해야만 하는 대책에 대해서는 중소기업에 있어서 중점적으로 대처해야만 하는 다양한 시나리오를 제시하여 공통 대책의 철저한 시행과 경우에 따라서는 필요로 하는 고도의 대책에 대해서도 설명하였다. 이것은 기업마다 자신 업무 내용 등을 고려해 필요로 하는 대책을 선택하는 데 도움을 주고자 하는 것을 목적으로 하고 있다. 구체적으로는 기업이 자사가 직면할 위험이나 문제점(정보보호 위험)에 대한 주의를 주기 위해 몇 개의 전형적인 시나리오 가운데에서 자사에 적합한 것을 선택하고 그것에 대응하는 대책을 스스로 선택하게 한다. 모든 대책을 시행하는 것은 불가능하기 때문에 어떠한 생각으로 대책의 취사선택을 해야만 하는 지에 대한 기본적인 검토 방법도 제시하였다. 본 가이드라인에 제시된 다양한 대책 가운데에는 기본적으로 필요한 대책 항목과 최근의 위협에 대한 대책으로써 필요한 항목이 포함되어 있다.

4.4 공통으로 실시해야만 하는 대책

중소기업이라면 공통으로 실시해야만 하는 대책에 대해서 제시한다. 여기에서는 규모나 업종에 의하지는 않지만 중소기업 가운데에서도 기업으로서 조직적인 대책을 취할 기업을 염두에 두고 있다. 공통으로 실시해야만 하는 대책에는 다음의 5가지 분류에 따라서 관리 대책을 정리하고 있다.

(1) 정보보호에 대한 조직적인 취급: 경영자 또는 경영관리자가 정비해야만 하는 회사내 체제나 규정 정비에 관한 항목
(2) 물리적 보호 : 물리나 기억 매체 등, 물리적인 물건의 관리에 관한 항목
(3) 정보시스템 및 통신 네트워크 운용 관리: PC나 네트워크 등의 관리에 관한 항목
(4) 정보시스템의 접근제어 상황 및 정보시스템 개발, 보수에 대한 정보보호대책: 정보나 정보시스템에 대한 접근제어에 관한 항목과 정보시스템의 도입시에 고려해야 할 항목
(5) 정보보호상의 사고 대응: 정보보호에 관한 사고가 발생한 경우의 준비에 관한 항목

4.4.1 정보보호에 대한 조직적인 대처

-정보보호에 관한 경영자의 의도 전파
-정보보호 대책 책임자 및 담당자 명시
-중요 정보자산 구분
-중요한 정보의 취급 절차
-계약서 등에 정보 취급 주의사항 표기
-종업원(파견 포함)에 대한 정보보호 주지
-정보보호 교육 기회 제공

4.4.2 물리적 보호

-중요한 정보 보관 관리
-중요한 컴퓨터나 배선의 안전한 배치 및 설치
-도난방지대책이나 확실한 폐기 등

4.4.3 정보시스템 및 통신 네트워크 운용관리

-정보시스템 운용에 관한 운용 규칙 제정
-정보 시스템(비밀 관련)의 운용 관리
-최신 패치 등 취약성 대책
-통신 데이터의 암호화 등 보호 대책
-기억매체 보호 대책

4.4.4 정보시스템의 접근제어 상황 및 정보 시스템의 개발, 보수에 관한 정보보호대책

-비밀 정보 접근 제어
-중요한 정보에 대한 접근 제한 설정
-인터넷 접속에 관한 부정 접근 대책 마련
-무선 LAN의 정보보호 대책
-정보보호를 전제로 한 시스템 전반의 관리

4.4.5 정보보호 관련 사고 대응

-시스템 장해 시 업무 재개 위한 업무파악
-긴급 사태 시 수행 업무 파악

4.5 기업별로 고려해야만 하는 대책

중소기업에 있어서 중점적으로 다루어야만 하는 다양한 시나리오를 제시하면서 "공통으로 실시해야만 하는 대책"의 철저와 경우에 따라서 필요로 하는 고도의 대책에 대해서 설명하였다.

4.5.1 기업의 다양한 위협과 위협에 대한 대책

가이드라인에서 제시한 사례들의 시나리오 전반부를 읽고, 자신의 회사 입장에서 봤을 때, 어떤 사고가 발생할까, 어떠한 위험이 있을까를 예상해 본다. 그런 다음 "발생한 사고"를 읽어보고 자신의 회사가 안고 있는 위험성(리스크)에 관심을 갖거나 또는 재확인하는 것이 효과적이다. 시나리오 자체가 자사 업무에 해당하지 않는 경우는 건너뛰어도 좋다. 가이드라인에는 10가지의 시나리오를 소개하고 있다.

4.5.2 기업 정보보호의 기본적인 방법

(1) 정보 자산의 조사 파악

앞에서 설명한 바와 같이 정보보호의 첫걸음은 기업들이 자사의 정보자산이 무엇이 있는 지 파악하는 것이다. 정보 자산은 다양한 정보 가운데, 기업으로서 관리해야 할 대상으로서 선택된 것을 말한다. 이것은 기업 가운데에서 넘쳐나는 정보를 모두 관리하는 것은 불가능하며 또한 의미가 없다. 그러면 어떠한 정보를 중요한 정보자산으로 파악할 수 있을까라고 한다면 이것은 기업마다, 업종마다 서로 다르기 때문에 한마디로 말할 수는 없지만 예를 들면 다음과 같은 정보는 중요한 정보자산이라 말할 수 있다.

-정보가 누설되었을 때, 회사 경영에 커다란 영향이 있는 것(예: 개인정보)
-정보가 변경되었을 때, 회사 경영에 커다란 영향이 있는 것(예: 재무 회계 정보)
-정보가 분실되었거나 이용될 수 없게 되었을 때 회사 경영에 커다란 영향이 있는 것(예: 설계 도면)

더구나 정보자산에는 전자적인 정보만이 아니라 종이 정보나 정보 시스템을 포함하는 것이 있다. 정보 자산을 파악할 때에 자주 이용되는 것은 정보 자산 관리 대장이다.

(2) 사고 가능성과 영향

중요한 정보 자산을 파악할 수 있다면, 다음으로 행하는 것은 정보 자산이 어떠한 위협에 있는 지를 검토하는 것이다. 구체적으로는 다음과 같은 위협이 생각되어진다.

-외부의 요인(예: 컴퓨터 바이러스, 부정 접근, 서비스 방해)
-내부의 요인(예: 정보보호 대책 준비 안 됨, 소프트웨어 결함, 조작 실수)

또한, 이들 위협이 어느 정도 일어나는가에 대해서 간단한 평가를 행한다. 예를 들면 1) 빈번하게 일어난다(월 1회 정도), 2) 간혹 일어난다(년 1회 정도), 3) 전혀 발생하지 않는다(몇 년에 1회) 등. 다음으로 위협이 실제로 발생했을 때, 정보 자산이 어느 정도 영향을 받을까에 대해서, 예를 들면, 1) 영향도 대 (회사의 존망이 걸려 있다), 2) 영향도 중(업무가 정지한다), 3) 영향도 소(업무 효율이 저하한다) 등, 3단계 정도로 나누어 생

각한다.

영향의 크기를 측정하는 지표로써 피해액 등을 고려하는 방법도 있지만, 목적이나 편리함에 따라서 결정하면 좋다. 어느 것을 하던지 발생 빈도, 영향 크기를 엄밀하게 구할 필요는 없고 대략적인 목표로써 생각하면 충분하다.

(3) 대응 방침의 결정

모든 위협에 대해서 대책을 모두 취하는 것은 비용도 많이 소요되므로 현실적이지는 않다. 따라서 업무에 영향을 주거나 어느 정도 발생 가능성이 있는 것에 정보보호 대책의 투자를 집중하는 것이 바람직하다. 자주 이용되는 방법으로는 다음과 같은 4가지 대응 방침으로 분류하는 것이 추천되고 있다.

-영향도가 중간 정도로 간혹 발생하는 경우, 정보보호 대책을 실시함으로써 영향이나 발생 확률을 낮추는 대응 방침(위험 감소)

-영향도가 대 정도로 빈번하게 발생하는 경우, 경영상에도 큰 문제가 있기 때문에 하는 방법을 바꾸거나 그와 같은 업무를 실시하지 않는 대응 방침(위험 회피)

-영향도가 대이지만, 전혀 발생하지 않는 경우, 다른 회사에 위탁하거나 보험 등에 들어두는 대응 방침(위험 이전)

-영향도가 소 정도로 전혀 발생하지 않는 경우, 무시하는 대응 방침(위험 보유)

어떠한 영역을 정보보호 대책의 대응 범위로 할지는 비용 문제도 포함하여 각각의 회사가 판단하는 것이지만 합리적인 대처 방침을 생각하는 경우에는 이와 같은 수법이 참고가 된다.

(4) 정보보호 파급효과

정보보호 대책 실시에는 비용이 들지만 한편으로 정보보호 대책을 실시함으로써 업무 효율화 등을 통해서 결과적으로는 전체 비용의 삭감으로 이어지는 경우가 있다. 다음은 그와 같은 예제들이다.

-정보보호 대책을 위해 업무 흐름이나 시스템 재평가에 의해 드러내지 않아도 좋은 사람에 대한 데이터의 은폐나 동일한 데이터의 복잡한 인력 등의 불필요한 작업을 없앨 수 있다. 이것에 의해서 작업 효율을 높이고 실수 축소로 연결되는 경우가 있다.

-정보보호 대책을 엄격하게 행하기 위해서 관리 대상이 되는 서버를 통합하여 삭감하면 시스템 운용 비용의 삭감 등으로 연결된다.

이와 같이 정보보호를 단순히 비용으로 보지 않고 비용 절감의 도구로 한다든지 기업 가치의 창조로 연결되는 것으로 보는 것도 중요하다.

V. 5분 만에 가능한 자사 진단 시트

중소기업 정보보호 대책 가이드라인의 구성 중 별첨 3인 "5분 만에 가능한 자사 진단 시트"에 대한 설명으로 자사 진단 시트를 소개한다. 중소기업의 정보 보호 관련하여 입문 수준의 기본적인 활동으로 최초로 해야 하는 정보보호 대책의 수단이다. 진단 시트는 [표 2]와 같으며 경영자 또는 관리자만이 시트의 설문에 대한 응답을 하나만 선택하여 기입하는 것으로 자신 회사의 정보보호 대책 수준을 재점검 해보는 것이다. 물론 진단 시트의 대책 방법만으로 정보보호 대책이 충분하다는 것이 아니며, 이 결과에 따라 가이드라인의 활용이나 보다 높은 수준의 정보보호 대책을 마련하는 데 활용할 수 있도록 제공하고 있다.

VI. 시사점 및 결론

본고에서는 일본의 중소기업 정보보호 대책 가이드라인을 집중적으로 소개하였다. 일본의 중소기업 정보보호 대책 가이드라인은 가이드라인 작성 연구회와 연구회 산하의 워킹 그룹들에 의하여 체계적이며 지속적으로 작성되었다. 이는 중소기업 현장에서의 현황 파악과 현실적으로 필요하면서도 저 비용으로 구현할 수 있는 방안들을 모아 가이드라인으로 제시하였다. 또한 중소기업에서 고려해야 할 정보보호 분야를 기술적 보호 대책 중심보다 위탁 업무에서의 정보 보호, 조직적 정보보호, 간단하게 중소기업의 정보보호 수준을 파악해 볼 수 있도록 실무적이고 직접 적용 가능한 관리적, 정책적, 기술적 대책을 전반적으로 소개하였다. 중소기업 스스로가 정보보호의 중요성을 인식하고 중소기업 스스로의 힘으로 특히, 경영자가 직접 정보보호 대책을 점검해 보고 관리해 보도록 하여 가이드라인이 중소기업 스스로의 정보 보호 대책 구현에 많은 도움이 되도록 만들어 진 점이 눈에 띄었다. 향후, 우리나라에서 제시한 중소기업 정보보호 가이드라인과 일본에서 제시한 중소기업 정보보호 대책 가이드라인과의 체계적인 비교 분석

〔표 2〕 5분 만에 가능한 자사 진단 시트

No	항목	내용	체크			
다음 항목에 대해서 모든 사원이 실시하고 있는 대답해주시기 바랍니다. 일부 사원이 실시하고 있는 경우에는 "일부실시하고 있다"를 선택해주시기 바랍니다.			실시	일부실시	실시않음	모름
1	보관	중요 정보를 책상 위에 방치하지 않고 열쇠부착 캐비닛에 보관하고 열쇠를 잠그는 등 중요 정보가 함부로 취급되지 않도록 잘 하고 있는가?				
2	반출	중요 정보를 회사 밖으로 반출할때는 패스워드를 거는 등 도난 분실 대책을 하고 있는가?				
3	폐기	중요한 서류나 CD 등을 폐기하는 경우는 세절기로 절단하는 등 중요 정보가 읽어볼 수 없도록 처분을 하고 있는가?				
4		중요정보가 들어있는 컴퓨터ㅖ 기억매체를 폐기하는 경우는 소거 소프트웨어를 이용하거나 업자에게 소거를 의뢰하는 등 전자 데이터가 읽혀지지 않도록 처리를 하고 있는가?				
5	사무실	사무소에서 잘 모르는 사람을 만나면 누구인지 물어보는 등 허가 없이 출입하는 사람이 없도록 하고 있는가?				
6		노트북 이용자는 퇴사시에 책상 위의 노트북을 서랍 속에 정리하는 등 도난 방지 대책을 하고 있는가?				
7		최종 퇴실자는 사무실을 잠그고 퇴실 기록(일시,퇴실자)를 남기는 등 사무실의 시건장치를 관리하고 있는가?				
8	개인 컴퓨터	Window Update를 행하는 등 항상 소프트웨어를 안전한 상태로 하고 있는가?				
9		파일 교환 소프트웨어가 들어오지 않게 하는 등 파일이 유출될 위험성이 높은 소프트웨어의 사용을 금지하고 있는 가				
10		사내외에서 개인 컴퓨터의 업무 사용을 허가제로 하는 등 업무에서 개인 컴퓨터의 사용을 명확히 하고 있는가?				
11		퇴사시에 컴퓨터의 전원을 끄는 등 다른 사람이 사용하지 않도록 하고 있는가?				
12	패스워드	패스워드는 자신의 이름을 피하는 등 다른 사람들이 추측하기 어려운 것을 사용하고 있는가?				
13		패스워드를 다른 사람에게 보이는 곳에 부착해두지 않도록 하는 등 다른 사람에게 알 수 없도록 관리하고 있는가?				
14		로그인용의 패스워드를 정기적으로 변경하는 등 다른 사람에게 간파 당하지 않도록 하고 있는 가?				
15	바이러스 대책	컴퓨터에는 바이러스 대책 소프트웨어를 설치하는 등 의심스러운 웹사이트나 전자 메일을 통한 바이러스로부터 컴퓨터를 지키기 위한 대책을 행하고 있는가?				
16		바이러스 대책 소프트웨어의 바이러스 정의 파일을 자동 갱신하는 등 항상 최신 바이러스 정의 파일이 되도록 하고 있는가?				
17	메일	전자 메일을 보내기 전에 수신 주소의 확인을 하는 등 잘못된 수신처로의 송신 실수를 방지하는 방법을 철저히 하고 있는가?				
18		상호간에 메일 주소를 알지 못하는 많은 사람들에게 메일을 보내는 경우는 Bcc 기능을 활용하는 등 메일주소를 잘못해서 다른 사람들에게 전하지 않도록 하고 있는가?				
19		중요 정보를 메일로 보내는 경우는 암호 메일을 사용하던지, 중요 정보를 첨부파일로 패스워드로 보호하는 등 중요 정보의 보호를 하고 있는가?				
20	백업	중요 정보의 백업을 정기적으로 하는 등 고장이나 오 조작 등에 대비하여 중요 정보를 소실하지 않도록 하는 대책을 하고 있는가?				
다음 항목에 대해서는 당신 회사에서 실시하고 있는 지 답해 주시기 바랍니다.			실시	일부실시	실시않음	모름
21	종사자	채용 시에 비밀준수의무가 있다는 사실을 주지시키는 등 종사자에게 비밀을 지키도록 하고 있는가?		-		-
22		정보 관리의 중요성 등을 정기적으로 설명하는 등 종사자에게 의식을 고취시키고 있는가?		-		-
23	거래처	계약서에 비밀 보유(비밀준수의무) 항목을 추가하는 등 거래처에 비밀 준수를 요구하고 있는가?		-		-
24	사고대응	중요 정보의 유출이나 분실,도난이 있는 경우의 대응 절차서를 작성하는 등 사고가 발생한 경우를 대비한 준비를 하고 있는가?		-		-
25	규정	정보보호 대책을 회사 규정으로 하는 등 정보보호 대책의 내용을 명확하게 하고 있는가?		-		-

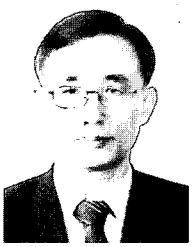
A: 실시 개수	B: 일부 실시 개수	합계점수=C+D
A 개	B 개	합계
C=A4	D=B2	
C 점	D 점	점

을 통하여 보다 실용적이고 적용 가능한 중소기업 정보보호 대책용 가이드라인이 만들어 질 필요가 있다.

참고문헌

[1] 한국정보보호진흥원/정보통신부, "중소기업 정보보호 가이드라인", 2006. 4.
[2] IPA, 일본 중소기업정보보대책가이드라인 보고서, 2009. 3.
[3] IPA, 일본 중소기업정보보호대책가이드라인, 2009. 3.
[4] 한국정보보호진흥원, 기업정보보호담당자용 민간사이버안전매뉴얼, 2004. 8.
[5] 한국정보보호진흥원, 기업직원용 민간사이버안전매뉴얼, 2004. 8.
[6] 박춘식 등, "정보보안 관리 평가 방법론 고찰", 정보보호학회지, 제11권, 제3호, pp.38-48, 2001. 6.
[7] 한국인터넷진흥원, 산업육성 중소 IT서비스 기업 지원, "http://www.kisa.or.kr/jsp/business/protect/protect6.jsp".
[8] 한국인터넷진흥원, 정보보호관리체계인증 ISMS, "http://isms.kisa.or.kr/isms/jsp/isms.jsp".
[9] 일본 경제산업성, SaaS SLA 가이드라인, 2008. 1.

〈著者紹介〉



박 춘 식 (Park Choon-Sik)
종신회원
1995년: 일본동경공업대 공학박사
1982년~1999년: 한국전자통신연구원 책임연구원
2000년~2008년: 국가보안기술연구소 책임연구원, 소장
2009년 3월~현재: 서울여자대학교 정보보호학과 교수
<관심분야> 개인정보보호기술, 클라우드컴퓨팅보안