Journal of KIIT. Vol. 18, No. 1, pp. 157-169, Jan. 31, 2020. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2020.18.1.157

중소기업의 개인정보 기술적 보호조치 방안 연구

김신석* 유혜정**

A Study on Technical Protection Measure of Personal Information in Small and Medium-sized Businesses

Sin-Seok Kim*, Hye-Jeong Yoo**

요 약

ICT의 발전으로 산업 전반에서 개인정보 이용 환경도 빠르게 변화하고 있으며, 이에 따라 개인정보를 보호하기 위한 새로운 과제가 대두되고 있다. 개인정보보호의 새로운 과제에 대한 해결 방안을 마련하기 위해서는 기업의 규모에 따라 개인정보 이용 및 보호 환경이 다르므로 이를 고려한 실제적이고 효율적인 개인정보보호 조치 방안이 마련되어야 한다. 우리나라 전체 사업체 수의 99% 이상을 차지하고 있는 중소기업의 경우 개인정보보호에 대한 인식이 저조하고, 또한 일반법 성격의 개인정보보호법을 그대로 적용하기에는 커다란 어려움을 가지고 있어 대기업과 공공기관에 비해서 개인정보보호 활동이 미흡하고 개인정보 침해사고의 비중이 높은 것이 현실이다. 따라서 본 논문에서는 기업의 규모별 개인정보보호 인식 및 환경의 차이를 분석하여 중소규모의 기업에 맞는 개인정보보호를 위한 기술적 보호조치 방안을 제안하고자 한다.

Abstract

With the development of ICT, environment for using the personal information is changing rapidly throughout the industry, and new challenges are emerging to protect personal information. In order to come up with a solution to the new challenges of protecting personal information, actual and effective personal information protection measures should be taken into account according to the size of business because the environment for using and protecting personal information depends on the size of business. In the case of small and medium-sized businesses, which account for more than 99% of the total number of businesses in Korea, they have low awareness of personal information protection and also have great difficulty in applying the Personal Information Protection Act.. So, the protection of personal information of small and medium-sized businesses is insufficient compared to big businesses and public institutions, and the proportion of personal information infringement is high. Therefore, in this paper, we analyze the difference in the recognition and environment of personal information protection by the size of the business and propose a measure for technical protection of personal information suitable for small and medium-sized businesses.

Keywords

personal information, personal information protection, small and medium-sized business, technical protection measure

* 세종사이버대학교 정보보호대학원 석사과정
- ORCID: https://orcid.org/0000-0003-3052-1491
** 세종사이버대학교 정보보호학과 교수(교신저자)
- ORCID: https://orcid.org/0000-0002-8829-7675

· Received: Dec. 17, 2019, Revised: Jan. 13, 2020, Accepted: Jan. 16, 2020

· Corresponding Author: Hye-Jeong Yoo
Dept. of Information Security, Sejong Cyber University, 121 Gunja-ro, Gwangjin-gu, Seoul, 05000, Korea
Tel.: +82-2-2204-8023, Email: hjyoo@sjcu.ac.kr

Ⅰ. 서 론

개인정보란 살아 있는 개인에 관한 정보로써 성명, 주민등록번호 및 영상 등 개인을 알아볼 수 있는 정보를 말한다. 국가 입장에서 개인정보는 공공질서 유지와 치안, 국가방위 등을 위해 이용 가능한 사회적 가치를 가진다고 할 수 있으며, 기업 입장에서 개인정보는 수익극대화 및 비용극소화 추구에 도움이 되는 경제적 가치를 가지며, 개인 입장에서 개인정보는 개인의 사생활과 밀접하게 연관되어 사적 가치를 가진다고 할 수 있다. 개인정보가 가지는 다양한 입장에서의 가치로 인해 누군가에 의해 악의적인 목적으로 이용되거나 유출되고 있으며, 이로 인해 개인의 사생활에 큰 피해를 줄 뿐만 아니라 개인의 안전과 재산에 피해를 줄 수 있기 때문에 개인정보를 보호하는 것은 매우 중요하다고 할 수 있다[1].

ICT의 발전과 진화를 기반으로 하는 제4차 산업혁명은 개인정보 환경을 변화시키고 있으며, 이에 따라 개인정보보호의 미래과제가 대두되고 있다. 제4차 산업혁명은 초연결, 초지능을 특징으로 하기 때문에 기존 산업혁명에 비해 더 넓은 범위에 더 빠른 속도로 사회 전반에 크게 영향을 끼칠 수밖에 없으며, 이로 인하여 개인정보 환경도 크게 변화되고 있다. 위치정보, 영상정보, 인터넷 접속기록 등이 새롭게 개인정보로 인식이 되고 있고, 페이스북, 트위터 및 블로그의 글 등의 막대한 정보를 통합한 빅데이터가 등장하였다[2]. 빅데이터를 인공지능이 분석하여 정보주체에 관한 판단을 내리는 경우 어떤 이유로 그와 같은 결과가 도출되었는지 파악이 불가능하며, 누가, 어디서, 어떤 방식으로 수집하여 분석하고 그 결과를 어떤 목적으로 활용할 것인지를 정보주체가 사전에 파악하여 그 권리를 행사하기가 어렵다. 사물인터넷이나 자율주행차의 경우 사물들이 상시 인터넷에 연결되어 있고, 데이터를 전송하는 통신 모듈을 내장하고 있기 때문에 보안관리가 되지 못할 경우 DDoS 공격 등에 악용될 가능성이 높다. 차량의 블루투스와 와이파이 모듈을 공격하여 원격 공격 및 제어를 하는 방식으로 GPS 정보 및 네비게이션 정보를 탈취하여 지속적으로 위치 추적을 할 수 있으며, 통화내역, 문자 메시지를 탈취할 수 있는 등 프라이버시의 침해 방법의 비약적인 진화를 가져올 수 있다. 또한, 핀테크는 금융과 정보통신기술이 결합한 서비스인 만큼 정보보안 사고 및 개인정보보호 이슈에 그대로 노출되고 있다[3].

개인정보보호의 필요성이 증가하고, 이에 대한 중요성이 커지면서 개인정보 이용환경을 분석하여 그에 맞는 적절한 보호조치 방안을 마련하는 것은 매우 중요하다. 2016년 한 해에만 신용정보 집중기관 한국신용정보원 설립, 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 정보통신망법) 및 개인정보보호법 개정, 개인정보 비식별 조치 가이드라인 시행, 개인정보 침해요인 평가제도 시행, 이동통신사 대상 개인정보 관리수준 평가제도 도입, 그리고 제3차 개인정보보호 기본 계획 수립 등 개인정보보호를 위한 기관 설치 및 제도 개선 등 개인정보를 보호하기 위한 다양한 활동이 시행되었다[3].

우리나라 전체 사업체 수의 99% 이상을 차지하고 있는 중소기업의 경우 개인정보보호에 대한 인식이 저조하고, 또한 일반법 성격의 개인정보보호법을 그대로 적용하기에는 커다란 어려움을 가지고 있다. 이에 본 연구에서는 변화하는 개인정보 이용환경 분석을 바탕으로 중소기업에 맞는 개인정보보호를 위한 기술적 보호조치 방안을 제시하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 기업의 규모를 고려한 개인정보보호 방안 마련의 중요성에 대해 설명하고, 개인정보 안전성 확보조치 기준의 개정내용에 대해 소개한다. 또한 중소기업의 개인정보보호를 위한 국가적 지원에는 어떤 것이 있는지 간단히 소개하고, 이의 한계성을 설명한다. 그리고 기업의 규모별 개인정보보호 인식 및 환경의 차이를 비교함으로써 이를 통해 본 논문에서 제안하고자 하는 중소기업의 개인정보의 기술적 보호조치 방안의 필요성에 대해 알아본다. 3장에서는 본 연구에서 제안하는 중소기업의 개인정보 기술적 보호조치 방법을 기술한다. 마지막으로 4장에서는 결론 및 향후 과제에 대해 기술한다.

II. 연구의 배경 및 중요성

2.1 기업의 규모를 고려한 개인정보보호

기업의 개인정보 유출 등의 각종 침해사고는 브랜드 이미지 및 기업 신뢰의 하락으로 경영 전체를 악화시킬 수 있다. 이러한 발생 가능한 문제를 해결하기 위해서는 개인정보보호를 위한 기술적 조치 마련이 기업차원에서 필요조건이 되었다. 개인정보보호 이행이 재무, 고객, 업무, 지속성장 관점에서 기업 성과 측면에 유의한 수준에서 영향을 미치므로 개인정보보호를 위한 기술적 방안 마련은 기업의 지속적 성장을 이루기 위한 선결요건이라 할 수 있다[4].

개인정보보호법이 시행되기 전인 2011년 이전까지는 국가기관 및 공공기관에서의 개인정보보호조치 방안은 정보통신망법에 명시되어 있는 개인정보보호 조항을 준수하여 수립되었다. 그러나 2011년 9월 30일 이후 개인정보보호법이 시행되면서 개인정보를 소홀하게 관리한 기업들도 개인정보보호조치 방안을 수립할 필요가 생기게 되었다.

정보통신망법 제28조와 시행령 제9조에서는 개인정보 보호조치에 대한 사항이 명시되어 있다. 정보통신서비스 제공자 등이 개인정보를 처리할 때에는 개인정보의 분실, 도난, 유출, 위조, 변조, 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 대통령령으로 정하는 기준에 따라 개인정보를 안전하게 처리하기 위한 내부관리계획의 수립 및 시행 그리고 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 통제장치의 설치, 운영 및 접속기록의 위조, 변조 방지를 위한 조치와 개인정보를 안전하게 저장, 전송할 수 있는 암호화 기술 등을 이용한 보호조치 등의 기술적, 관리적 조치를 하여야 한다[5].

개인정보보호법은 개인정보의 수집 및 관리, 처리방침 등에 대한 사항을 명시하고 있으며, 개인정보의 관리와 관련하여 개인정보 보호원칙, 국가 및 기업의 책무, 개인정보 취급자에 대한 감독에 대한 사항 및 개인정보시스템의 안전조치에 대한 의무를 정의하고 있다[5].

정보통신망법의 개인정보 보호조치에 대한 규정은 정보통신사업자의 특이사항이 고려된 법률이며, 개인정보보호법은 민간기업의 규모 및 업종별 특이사항이 고려되지 않은 일반법 성격의 법률이라고 할 수 있다. 해당 법률에 따라 실제적인 개인정보보호가 이루어지기 위해서는 기업의 규모에 따라 예산 및 시스템 지원 등이 개인정보보호를 위한 기업의 전사적 지원 여부가 결정되므로, 기업의 규모를 고려하는 것은 매우 중요하다. 일반적으로 기업은 규모별로 1인 또는 5인 이하의 사업자인 소상공인, 상시근로자 300명 미만의 중소기업 그리고 상시근로자 수가 300명 이상인 대기업으로 분류된다. 이러한 기업의 규모에 따라 개인정보보호를 위한 지원이 달라지므로 소상공인, 중소기업 그리고 대기업에 맞는 개인정보 보호조치 방안을 수립할 수 있도록 해야 한다[5]. 중소규모의 기업에 개인정보보호법을 그대로 적용하면 개인정보보호를 위한 정책과 시스템 구축 및 운영에 대한 비용 지출에 대해서 현실적인 문제가 발생한다. 민간 기업의 경우 비용 등의 필요 요소를 자체적으로 해결해야 하고, 대기업의 경우 개인정보보호를 위하여 시스템을 구축하는 등에 대한 비용을 지출할 수 있지만 많은 중소기업의 경우 이러한 비용을 지출하는 것이 쉽지 않아 개인정보보호 방안 적용에 어려움이 크다.

따라서 현실적이고 효율적으로 개인정보를 보호하기 위해서는 기업의 규모를 고려하여 그에 맞는 개인정보보호를 위한 보호조치 방안을 수립하는 것이 반드시 필요하다고 할 수 있다.

2.2 개인정보 안전성 확보조치 기준의 개정

2019년 개인정보처리시스템의 관리기준을 명확하게 하고, 개인정보의 오·남용 및 유출사고 등 침해사고 예방 및 개인정보 침해사고 시 사후 추적 관리 강화 내용을 구체화하여 개인정보의 안전성 확보조치 기준이 개정되었다.

개인정보 안전성 확보조치 기준 제2조 제19항에서 기존에는 개인정보처리취급자가 개인정보처리시스템에 접속한 사실에 대한 기록을 정의하였으나 개인정보처리취급자가 개인정보처리시스템에 접속하여 수행한 업무내용 및 접속지 정보 그리고 정보주체정보를 추가하여 개정되었다. 개인정보취급자

등의 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무는 개인정보취급자 등이 개인정보처리시스템에 접속한 사실과 접속하여 수행한 업무내역을 확인하는데 필요한 정보를 의미한다. 계정은 개인정보처리시스템에서 접속자를 식별할 수 있도록 부여된 ID 등의 정보이며, 접속일시는 접속한 시점 또는 업무를 수행한 시점이다. 접속지 정보는 개인정보처리시스템에 접속한 자의 컴퓨터 또는 서버의 IP 주소 등이며, 처리한 정보주체 정보는 개인정보취급자가 누구의 개인정보를 처리하였는지를 알 수 있는 ID, 고객번호, 학번, 사번 등의 식별정보를 의미한다. 수행업무는 개인정보취급자가 개인정보처리시스템을 이용하여 처리한 내용을 알 수 있는 정보로 검색, 열람, 조회, 입력, 수정, 삭제, 출력, 다운로드 등이 있다[6].

개인정보 안전성 확보조치 기준 제4조 내부관리계획은 세부적으로 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등의 내용이 추가되었으며, 전사적인 계획 내에서 개인정보가 관리될 수 있도록 최고경영층으로부터 내부결재 등의 승인을 받아 모든 임직원 및 관련자에게 알림으로써 이를 준수할 수 있도록 하고 있다. 개인정보보호책임자는 내부관리계획의 적정성과 실효성을 보장하기 위하여 연1회 이상 내부관리계획에 따른 기술적·관리적 안전조치의 이행 여부를 점검 및 관리해야 한다. 내부관리계획의 이행 실태 점검관리 결과에 따라 적절한 조치를 취하여야 하며, 중대한 영향을 초래하거나 해를 끼칠 수 있는 사안 등에 대해서는 사업주 및 대표임원 등에게 보고 후 의사결정 절차를 통하여 적절한 대책을 마련하여야 한다[6].

개인정보 안전성 확보조치 기준 제8조 접속기록의 보관 및 점검에서는 기존에는 접속기록을 6개월 이상 보관하였지만 이를 1년 이상 보관하는 내용으로 개정이 되었다. 또한, 5만 명 이상의 개인정보를 보유하고 있는 경우와 고유식별정보 또는 민감정보를 처리하는 경우에는 접속기록을 2년 이상 보관하도록 하고 있다. 그리고 개인정보의 오·남용에 대한 부분이 추가되었으며, 개인정보처리자가 개인정보를 다운로드하면 그 사유를 반드시 확인해야만 한다. 접속기록에는 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보를 기록하여야 한다. 기록하는 정보주체 정보의 경우 민감하거나 과도한 개인정보가 저장되지 않도록 하여야 하며, 검색 조건문을 통해 대량의 개인정보를 처리했을 경우 해당 검색 조건문을 정보주체 정보로 기록할 수 있으나, 이 경우 DB테이블 변경 등으로 책임추적성 확보가 어려울 수 있으므로 해당 시점의 DB를 백업하는 등 책임추적성 확보를 위해 필요한 조치를 취하도록 하고 있다. 개인정보처리자는 접속기록을 최소 보관기간 이후에도 즉시 삭제하지 않고 책임추적성을 확보하기에 충분한 기간 동안 보관·관리할 수 있도록 개인정보처리시스템에 저장된 개인정보의 중요도 및 민감도 등을 고려하여 내부관리계획에 보관기간을 정하고 이를 이행하여야 한다. 비인가자의 개인정보처리시스템 접속 시도 기록 및 정보주체에 대한 접속기록까지 보관·관리하고 정기적인 확인·감독 등을 통하여 개인정보처리시스템에 대한 불법적인 접근 및 비정상 행위 등에 대한 안전조치를 강화하도록 하고 있다[5]. 개인정보처리자는 개인정보처리시스템의 접속기록을 월1회 이상 정기적으로 점검하여야 하며, 이를 통해 비인가된 개인정보 처리, 대량의 개인정보에 대한 조회, 정정, 다운로드, 삭제, 출력 등의 비정상 행위를 탐지하고 적절한 대응조치를 할 필요가 있다. 특히, 개인정보처리시스템에 접근하여 개인정보를 다운로드 한 경우에는 내부관리계획으로 정하는 바에 따라 그 사유를 확인하고, 개인정보취급자가 개인정보의 오·남용이나 유출을 목적으로 다운로드한 것이 확인되었다면 지체 없이 개인정보취급자가 다운로드 한 개인정보를 회수하여 파기하는 등 필요한 조치를 하여야 한다[6].

2.3 중소기업의 개인정보보호를 위한 국가적 지원

통계청의 2017년 기준 영리법인 기업체 행정통계 잠정 결과에 따르면, 2017년 기준으로 국내 중소기업은 전체 사업체 수의 99.8%이며, 또한 중소기업의 종사자 수는 전체 기업규모별 종사자 수의 82%

를 차지하고 있다. 중소기업은 사업체 수 및 고용 그리고 부가가치 점유율 등에서 우리나라 경제에 차지하는 비중이 매우 높으며, 전체 산업의 다양화 및 지역경제의 균형을 이루며 발전하므로 국가의 경제적, 사회적, 정치적 안정에 기여하여 왔다고 할 수 있다.

산업 전반에 IT를 통한 기업의 정보화가 기업 경쟁력을 확보하는데 필수적인 요소가 되면서 국가에서는 중소기업을 위해서 정보화 지원 사업을 지속적으로 실시하여 중소기업이 정보화를 통해 성과가 향상될 수 있도록 하는데 기여하였다[7][8]. 국가적 지원으로 중소기업의 정보화 수준은 대기업과의 격차가 어느 정도 감소되었으나 정보보호 및 개인정보보호에 대해서는 여전히 전문지식이 부족하고, 이에 대한 투자가 미흡하기 때문에 그 수준이 낮고 취약한 것이 현실이다. 국가에서는 이러한 중소기업의 개인정보보호 문제점을 해결하기 위해 표 1과 같이 지역별 정보보호지원센터를 통한 중소기업의 정보보호 역량 강화를 위한 정보보호서비스 지원책에 포함하여 개인정보보호 활동을 지원하고 있다.

표 1. 정보보호지원센터 정보보호서비스 현황
Table 1. Status of information protection service in the information security support center

정보보호서비스	지원내용
정보보호 서비스 현장 컨설팅	· 보안 전문 컨설턴트가 방문하여 규모별 업종별 기업 특성에 맞는 보안 컨설팅 · 보안 취약점 보호대책 마련 지원 · 각종 정보보호 양식 및 가이드 제공
웹취약점 점검	· 비밀번호 암호화 전송점검 · 관리자 페이지 노출 점검 · 10대 웹 어플리케이션 취약점 점검 · 개인정보 노출 점검
보안도구 배포	· **업무용 PC개인정보 보호조치 점검도구** · 맞춤형 전용백신 · 홈페이지 보안 강화도구
교육 및 세미나	[교육] 정보보호 침해사례 및 예방대책, SW개발보안 및 모의해킹 실습, **개인정보보호 보호조치** 등 [세미나] 정보보호 관련 법제도, 기술적·관리적 정보보호 조치 등 안내 및 발표 토론

또한, 한국인터넷진흥원은 컨설팅 및 솔루션 도입 서비스로 종합컨설팅과 약식컨설팅의 서비스 항목을 지원한다. 종합컨설팅은 보안현황 및 취약점분석, 모의해킹, 정보보호 정책기술 진단 등 중소기업별 맞춤형 정보보호 컨설팅을 지원하며, 정보보호 솔루션 및 보안제품 구입비용을 최대 300만원까지 지원한다. 약식컨설팅은 PC, 홈페이지, 이메일 등 기본적인 정보보호 수준 진단과 클라우드 기반의 보안 서비스(SECaas: SECurity as a Service) 이용료를 최대 180만원까지 지원한다[9]. 특히 개인정보보호 기술지원에 대해서는 개인정보기술지원센터를 통해 개인정보보호법에서 요구하는 의무사항 조치에 대해 비용, 기술 등의 측면에서 어려움을 느끼는 소상공인, 50인 미만의 중소사업자 및 비영리단체를 대상으로 개인정보보호 수집부터 파기까지 단계별 법적 의무사항 조치방법을 안내하고, 문서, 업무용 PC, 홈페이지 상의 개인정보를 안전하게 관리하는 방법 등 개인정보보호에 필요한 무료 컨설팅을 지원하고 있으며, 업무용 PC의 보호조치 사항을 사용자가 자율적으로 점검할 수 있는 업무용 PC 보호조치 점검도구를 제공하고 있다. 그러나 이러한 국가적 지원은 수많은 중소기업의 개인정보보호를 지원하기에는 매우 부족한 것이 현실이다.

2019 개인정보보호 연차보고서에 따르면, 암호화 대상 개인정보 보유 현황에서 공공기관은 80.8%, 대기업을 포함한 민간기업의 경우 83.7%가 가장 민감한 개인정보라고 할 수 있는 주민등록번호를 보유하고 있는 것으로 나타났다. 그러나 공공기관의 경우 78.3%가 정보화 및 정보보호(개인정보보호) 전담부서에서 개인정보보호 업무를 담당하지만, 대기업을 포함한 민간 기업에서는 62.0%가 일반 관리부서에서 담당하고 있으며, 그 중 20.0%는 개인정보보호 업무 담당부서가 없는 것으로 나타났다. 또한 가장 기본적인 개인정보보호 조치인 개인정보처리방침의 작성·공개 및 갱신에서 공공기관의 99.5%는 개인정보처리방침을 작성하여 공개하고 있으며, 최근 1년 이내에 갱신한 것으로 조사된 반면 민간기업의 경우 54.6%가 개인정보 처리방침을 갱신한지 1년 이상이었으며, 작성 이후 전혀 갱신하지 않은 기업도 19.8%나 되는 것으로 조사되었다[10].

따라서 대기업을 포함한 민간기업의 경우 기본적인 개인정보 보호조치가 부족한 것으로 나타나고 있으며, 대기업을 제외한 중소기업의 경우는 개인정보보호 환경이 더 열악하다고 할 수 있을 것이다. 개인정보보호 환경을 개선하기 위해서는 중소기업을 위한 개인정보보호에 대한 지원 규모를 확대하는 것도 필요하지만 그에 앞서 자율적으로 개인정보보호를 위한 기술적 보호조치를 수립하고 시행할 수 있도록 그에 맞는 현실적인 조치방안을 마련하여 제시하는 것이 필요하다고 할 수 있다.

2.4 기업의 규모별 개인정보보호 인식 및 환경의 차이 비교

2.4.1 개인정보 유출

표 2와 같이 기업규모별 개인정보 유출사고의 원인에 대해 조사한 자료를 분석하면 해킹 및 악성코드 등 외부공격이 42.4%로 가장 높게 나타났으며, 내부직원의 실수로 인한 유출이 26.3%, 내부직원의 고의 유출이 6.7%, 외부인 등에 의한 유출이 24.6%로 나타났다. 이와 같이 개인정보 유출사고는 외부공격(42.4%)과 내부직원의 실수 및 고의(33.0%)가 원인이 되어 높게 발생되는 것으로 조사되었다[11]. 개인정보 유출사고가 내부직원에 의해 높게 발생되는 주요 원인 중 하나로 내부직원이 USB 등 보조저장매체로 자료를 복사하여 외부로 반출하는 것을 들 수 있으며, 또한, 이메일 및 메신저 등을 이용하여 외부로 자료를 전송할 수 있는 환경이기 때문이다. 특히 중소기업에서는 USB 등 보조저장매체를 통제할 수 있는 기술적 기반이 마련되어 있지 않기 때문에 개인정보 유출을 통제할 수 없고, 특히, 외부 협력회사와 이메일 등을 주고받을 때 내부직원의 실수로 개인정보파일을 첨부하여 전송하는 등 실수로 인한 개인정보 유출의 경우도 이를 통제할 수 있는 정책적·기술적 기반이 부족한 것으로 분석할 수 있다.

개인정보 유출사고 발생 시 표 3과 같이 처벌강도가 부족하다고 조사되었는데, 특히 기업 규모가 작을수록 개인정보 유출사고 발생 시 처벌 강도가 부족하다고 응답하였다[10].

표 2. 개인정보 유출사고 원인에 대한 인식
Table 2. Recognition of the cause of personal information leakage incidents

구분	기업규모			전체
	300명 이상	50~299명	5~49명	
해킹 및 악성코드 등 외부공격	50.7 (33.0%)	69.5 (45.7%)	64.6 (49.7%)	184.8 (42.4%)
내부직원의 실수로 인한 유출	50.3 (32.8%)	35.5 (23.4%)	28.8 (22.1%)	114.6 (26.3%)
내부직원에 의한 고의 유출	7.9 (5.1%)	11.3 (7.4%)	9.9 (7.6%)	29.1 (6.7%)
외부인 등에 의한 유출	44.6 (29.1%)	35.7 (23.5%)	26.8 (20.6%)	107.1 (24.6%)
합계	153.5 (100%)	152 (100%)	130.1 (100%)	435.6 (100%)

표 3. 개인정보 유출사고 발생 시 처벌강도
Table 3. Punishment intensity for personal information leakage incidents

구분	기업규모			전체
	300명 이상	50~299명	5~49명	
부족하다	43.3 (43.3%)	56.5 (56.5%)	55.8 (55.9%)	155.6 (51.9%)
적당하다	49.0 (48.9%)	42.3 (42.3%)	41.8 (41.8%)	133.1 (44.4%)
과하다	7.8 (7.8%)	1.2 (1.2%)	2.3 (2.3%)	11.3 (3.8%)
합계	100.1 (100%)	100 (100%)	99.9 (100%)	301 (100%)

이러한 결과는 중소규모의 기업의 경우 기술적인 투자를 하는 것보다 국가의 정책으로 처벌 강도를 높여 개인정보 유출사고를 사전에 방지할 수 있게 되기를 바라는 기대심리가 투영된 것이라고 볼 수 있다. 중소기업 입장에서는 개인정보 유출을 방지하기 위한 투자비용이 부담되기 때문에 처벌을 높여 직원 및 일반 이용자의 개인정보보호에 대한 경각심을 높이기 위한 심리가 반영되어 있다고 볼 수 있다.

표 4와 같이 개인정보 유출사고에 대응하기 위한 방안으로 내부 대응 프로세스 수립이 45.1%로 가장 높게 나타났으며, 별도의 대응방안 없음(28.6%) 순으로 조사되었다[11]. 내부 대응 프로세스 수립의 경우 개인정보보호법 이행을 위한 관리적 보호조치 마련의 일환으로 내부관리계획서를 수립하는 것을 의미한다. 내부관리계획서의 경우 다른 항목에 비해 상대적으로 낮은 비용투자로 적용 가능하다.

표 4. 개인정보 유출사고 대비 대응 노력
Table 4. Efforts to respond to personal information leakage incidents

구분	기업규모			전체
	300명 이상	50~299명	5~49명	
내부 대응 프로세스 수립	64.0 (46.6%)	57.0 (46.3%)	44.9 (41.9%)	165.9 (45.1%)
개인정보 배상 책임 보험 가입	23.0 (16.8%)	2.6 (2.1%)	4.0 (3.7%)	29.6 (8.1%)
준비금 등 재원 마련	3.2 (2.3%)	0.5 (0.4%)	0.2 (0.2%)	3.9 (1.1%)
개인정보보호 전문가 채용 등 인력 체계 마련	24.3 (17.7%)	18.4 (14.9%)	6.1 (5.7%)	48.8 (13.3%)
ISMS, PIMS 개인정보보호인증 취득	4.9 (3.6%)	7.7 (6.3%)	1.7 (1.6%)	14.3 (3.9%)
별도의 대응방안 없음	17.9 (13.0%)	36.9 (30.0%)	50.2 (46.9%)	105 (28.6%)
합계	137.3 (100%)	123.1 (100%)	10.71 (100%)	367.5 (100%)

별도의 대응방안 없음 항목에 대한 답변 비율을 살펴보면 대기업이 13.0%인 반면 중소규모 기업의 경우 각 30.0%, 46.9%로 답변률의 차이가 매우 크다는 것을 알 수 있으며, 이를 통해 중소규모의 기업의 경우 개인정보 유출사고 대비 대응을 위한 환경이 매우 열악함을 알 수 있다.

2.4.2 기업의 규모별 개인정보 관리 규모

기업의 규모가 클수록 직원의 수가 많고, 거래하는 협력회사 및 고객이 많기 때문에 표 5와 같이 개인정보 관리 규모가 크게 나타난다. 수집하고 있는 개인정보 유형은 기업규모에 상관없이 모두 성명이 가장 많은 것으로 나타났으며, 전화번호, 생년월일, 성별 등의 순으로 확인되었다. 중소규모의 기업의 경우 대기업에 비해 관리하고 있는 개인정보의 규모가 작지만, 5만 명 이상의 개인정보를 관리하고 있는 기업이 31.9%를 차지하고 있는 만큼 그 비율이 작다고 할 수 없으며, 우리나라 기업체의 99.8%가 중소기업인 점을 감안하면, 중소기업을 위한 개인정보 보호조치를 마련하는 것은 매우 중요하다고 할 수 있다.

표 5. 기업규모별 개인정보 관리 규모
Table 5. Scale of personal information management based on the size of businesses

구분	기업규모			전체
	300명 이상	50~299명	5~49명	
1만 명 미만	20.8%	68.1%	83.8%	57.5%
5만 명 미만	10.6%	7.5%	6.8%	8.3%
10만 명 미만	22.8%	7.8%	5.1%	11.9%
50만 명 미만	18.8%	9.6%	3.9%	10.8%
100만 명 미만	13.9%	7.0%	0.4%	7.1%

2.4.3 기업의 규모별 개인정보 침해 이슈 및 보호조치의 유사점과 차이점

기업 규모별로 개인정보 유출사고는 기업규모와 상관없이 표 2와 같이 해킹 및 악성코드 등 외부공격(42.4%)과 내부직원의 실수 및 고의(33.0%)가 원인이 되어 높게 발생되는 것으로 나타났다. 앞서 설명한 것과 같이 개인정보 유출사고가 내부에서 높게 발생하는 것은 내부직원이 USB 등 보조저장매체로 자료를 쉽게 복사하여 외부로 반출할 수 있고 이메일 및 메신저 등을 통하여 외부로 자료를 손쉽게 전송할 수 있기 때문이며, 이는 중소규모의 기업에서 더욱 빈번하게 나타난다.

기업의 규모가 클수록 외부공격에 의한 사고 비율이 낮게 나타나는데, 이는 기업의 규모가 클수록 방화벽, IPS, DDoS 솔루션 등 정보보호 솔루션에 대한 투자가 가능하기 때문이라고 할 수 있다. 기업의 규모가 작을수록 방화벽, IPS 등의 보안 솔루션 도입에 투자할 수 있는 여력이 부족하므로 외부공격에 대하여 취약할 수밖에 없다. 내부직원에 의한 고의 유출도 기업의 규모가 클수록 그 비율이 낮게 나타나데 이는 DLP, DRM 등의 보안 솔루션에 대한 투자가 이루어져 있기 때문이라고 할 수 있다.

개인정보보호 교육 등을 통해 내부 직원의 인식을 향상시키고는 있지만 여전히 개인정보보호에 대한 인식이 많이 개선되지 않다는 것을 알 수 있으며, 내부직원의 실수에 대하여 기술적인 보호조치를 더 다루어야 한다는 것을 알 수 있다. 또한, 개인정보 유출사고 원인에 대해 여전히 사회적 인식이 부족하고, 개인정보의 과다한 수집이 실수로 이어지는 것으로 볼 수 있다.

표 6. 개인정보의 안전한 관리를 위한 조치[11]
Table 6. Measures for the safe management of personal information

구분	기업규모			전체
	300명 이상	50~299명	5~49명	
내부관리계획 수립·시행	87 (17.9%)	86.6 (24.4%)	80.9 (32.3%)	254.5 (23.3%)
접근통제 시스템	71.3 (14.7%)	40.7 (11.4%)	25.2 (10.1%)	137.2 (12.6%)
접근권한 차등 부여 제한	48.6 (10.0%)	32.2 (9.1%)	27.4 (10.9%)	108.2 (9.9%)
개인정보보호 암호화 기술	52.3 (10.8%)	38.0 (10.7%)	17.1 (6.8%)	107.4 (9.8%)
송수신 암호화 기술	34.2 (7.0%)	13.8(3.9%)	7.8 (3.1%)	55.8 (5.1%)
접속기록 보관	40.8 (8.4%)	21.3(6.0%)	8.0 (3.2%)	70.1 (6.4%)
보안프로그램 설치·갱신	65.3 (13.5%)	51.0 (14.3%)	27.6 (11.0%)	143.9 (13.2%)
잠금장치 보관	60.6 (12.5%)	56.6 (15.9%)	48.4 (19.3%)	165.6 (15.2%)
재해재난 대비	25.4 (5.2%)	15.3 (4.3%)	8.0 (3.2%)	48.7 (4.5%)
합계	485.5 (100%)	355.5 (100%)	250.4 (100%)	1091.4 (100%)

개인정보의 안전한 관리를 위하여 기업들은 내부 대응 프로세스를 수립하여야 한다. 표 6과 같이 기업의 규모에 상관없이 개인정보의 안전한 관리를 위한 조치로 내부관리계획의 수립·시행이 가장 높게 나타났다. 기업 규모별로 차이점은 300명 이상의 대기업의 경우 고가의 보안 솔루션인 접근통제시스템에 투자하여 개인정보가 안전하게 관리될 수 있도록 하는 것이 두 번째로 높은 개인정보 보호조치로 선택된 반면, 300명 미만의 중소규모의 기업은 잠금장치보관을 꼽았다는 것이다. 기업의 규모가 작을수록 데이터 파일보다 서류에 개인정보를 관리하는 경우가 많아 개인정보가 적힌 서류를 서고의 잠금장치를 통해 보관을 하고, 기업의 규모가 큰 300명 이상의 기업에서는 서류 대신 파일 형태로 저장되어 있는 개인정보 관리 환경을 일정 부분 반영한 것이라고 할 수 있다. 그러나 업무의 전산화 및 정보의 디지털화는 일부 규모가 큰 기업에만 적용되는 것이 아닌 우리 사회의 일반적인 현상이 된 현재, 개인정보보호 조치 마련의 기업 규모별 경제적 차이점을 뚜렷하게 보여주는 것이라고 할 수 있을 것이다.

현재의 내부 대응 프로세스를 보면 기업의 규모가 클수록 보안 솔루션에 대한 투자가 이루어져 안전하게 개인정보가 관리되고 있지만 기업의 규모가 작을수록 보안 솔루션에 대한 투자가 제대로 이루어지지 않고, 낮은 비용으로 개인정보를 관리하는 있는 것을 확인할 수 있다. 이와 같이 개인정보를 안전하게 관리하기 위해서는 기술적인 보호조치가 반드시 필요하며, 비용 투자에 부담을 가지고 있는 규모가 작은 기업에 대해서는 자율적으로 개인정보보호를 위한 기술적 보호조치를 수립하고 시행할 수 있도록 그에 맞는 현실적인 조치 방안을 마련하여 제시하는 것이 필요하다는 것을 알 수 있다.

III. 중소기업의 개인정보 기술적 보호조치

개인정보를 보호하기 위한 기술적인 조치에는 접근권한 관리, 접근통제, 암호화, 접속기록의 보관 및 점검, 악성프로그램 방지 등이 있으며, 이를 크게 네트워크 보안, PC 보안, 서버 보안의 3개의 보안 영역으로 구분할 수 있다.

3.1 개인정보보호를 위한 일반적인 기술적 보호조치

3.1.1 네트워크 보안

개인정보의 안전성 확보조치 기준에 따르면, 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 인가받지 않은 접근을 제한하고 불법적인 개인정보 유출 시도를 탐지 및 대응하여야 한다. 또한, 취급 중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 조치를 하여야 한다.

개인정보보호를 위한 안전성 확보조치 기준을 만족시키기 위해서는 개인정보보호를 위한 네트워크 영역에서는 표 7과 같이 방화벽, IPS, 웹 방화벽, VPN을 통하여 기술적 보호조치가 가능하다.

표 7. 안전성 확보조치 기준에 따른 네트워크 보안 영역에서의 개인정보보호를 위한 일반적인 기술적 보호조치
Table 7. General technical protection measures for personal information protection in network security area according to criteria for securing personal information safety

조항	안전성 확보조치 기준	기술적 보호조치
6조 1항	개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol)주소 등으로 제한하여 인가받지 않은 접근을 제한하여야 한다.	방화벽
6조 1항	개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응하여야 한다.	IPS, 웹 방화벽
6조 2항	개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 가상사설망(VPN: Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다.	VPN

표 8. 안전성 확보조치 기준에 따른 PC 보안 영역에서의 개인정보보호를 위한 일반적인 기술적 보호조치
Table 8. General technical protection measures for personal information protection in PC security area according to criteria for securing personal information safety

조항	안전성 확보조치 기준	기술적 보호조치
6조 3항	개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근통제 등에 관한 조치를 하여야 한다.	DLP
7조 1항	개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.	DRM
7조 5항	개인정보처리자는 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.	DRM
7조 6항	개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립시행하여야 한다.	암호키 관리
7조 7항	개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.	DRM
9조	개인정보처리자는 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 한다.	백신 프로그램

외부 네트워크에서 내부 네트워크로 유입되는 트래픽 또는 내부 네트워크에서 외부 네트워크로 나가는 트래픽에 대하여 IP 및 포트로 허용하거나 차단할 수 있는 기능을 고려하여 방화벽으로 보호조치를 하고, 외부 네트워크로부터 내부 네트워크로 침입하는 트래픽을 공격패턴 시그니처로 제어하는 기능을 고려하여 IPS로 보호조치를 할 수 있다. 또한 일반적인 방화벽과는 달리 웹 트래픽을 분석하여 공격을 탐지하고 차단하는 기능을 고려하여 웹 방화벽으로 보호조치를 한다. 웹 방화벽의 경우 정보 유출 방지 및 웹사이트 위·변조 방지에 대한 기능도 보유하고 있다. 그리고 공중망 구간 암호화 통신 기능을 고려하여 VPN으로 보호조치를 한다.

3.1.2 PC 보안

개인정보의 안전성 확보조치 기준에 따르면, 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 업무용 컴퓨터에 암호화하여 저장하여야 하며, 개인정보가 열람권한이 없는 자에게 공개되거나 유출되지 않도록 보호조치를 하여야 한다.

PC 보안에 대하여 DLP 및 DRM 그리고 백신 프로그램으로 [표8]과 같이 개인정보보호조치를 할 수 있다. 이메일 등에 첨부하여 전송하는 파일을 차단하고, 인가되지 않은 보조저장매체를 차단하는 기능을 고려하여 DLP로 보호조치를 한다. 문서의 암호화를 통해 허가된 사용자만이 문서를 활용할 수 있

도록 DRM으로 보호조치를 할 수 있다. 그리고 PC에 침입한 악성코드를 치료하는 기능을 가진 백신 프로그램으로 보호조치를 한다.

3.1.3 서버 보안

개인정보의 안전성 확보조치 기준에 따르면, 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 개인정보처리시스템에 암호화하여 저장하여야 하며, 업무 수행에 필요한 접근권한을 최소한의 범위로 업무 담당자에 따라 차등 부여해야 한다.

개인정보보호를 위한 안전성 확보조치 기준을 만족시키기 위해서는 서버 보안에 대하여 DB 접근제어 및 DB 암호화로 표 9와 같이 개인정보보호를 위한 기술적 보호조치를 할 수 있다. DB 접근자의 접속 시간대별 제어 및 SQL 구문별 권한을 제어하고 데이터 마스킹 및 감사로깅 기능을 고려하여 DB 접근제어로 보호조치를 하고, DB 서버 내의 개

인정보 파일을 암호화해서 관리할 수 있는 DB 암 호화로 보호조치를 한다.

3.2 규모를 고려한 개인정보 기술적 보호조치

개인정보에 대한 실제적인 안전성 조치가 이루어질 수 있도록 개인정보 안전성 확보조치 기준에서는 그림 1과 같이 개인정보 보유 현황 및 기업의 규모에 따라 완화형, 표준형, 강화형의 3가지 유형으로 차등적으로 분류하여, 해당 유형에 따라 개인정보의 안전조치 기준을 적용할 수 있도록 하였다. 유형3인 강화형의 경우는 개인정보 안전조치 제4조부터 제13조의 조치사항을 모두 적용해야 하며, 유형2인 표준형은 제4조부터 제11조, 제13조를 그리고 유형1인 완화형은 제5조부터 제11조, 제13조의 적용을 받는다. 이렇게 차등하게 분류된 안전조치 기준에 따르면 중소규모의 기업은 유형1부터 유형3까지 개인정보 보유량에 따라 모든 유형에 해당할 수 있다.

그림 1. 개인정보 보유량 및 기업 규모에 따른 안전조치 기준 차등

Fig. 1. Different standards of safety measures according to the amount of personal information and the size of the businesses

표 9. 안전성 확보조치 기준에 따른 서버 보안 영역에서의 개인정보보호를 위한 일반적인 기술적 보호조치

Table 9. General technical protection measures for personal information protection in server security areas according to criteria for securing personal information safety

조항	안전성 확보조치 기준	기술적 보호조치
5조 1항	개인정보처리자는 개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.	DB 접근제어
5조 3항	개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.	DB 접근제어
5조 5항	개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.	DB 접근제어
7조 1항	개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.	DB 암호화
7조 2항	개인정보처리자는 비밀번호 및 바이오 정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.	DB 암호화
9조	개인정보처리자는 악성프로그램 등을 방지치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 한다.	백신 프로그램

개인정보보호를 위한 일반적인 기술적 보호조치와 규모를 고려한 중소기업 대상인 유형2의 개인정보보호를 위한 기술적 보호조치에 대한 차이점으로 제7조 6항의 암호키 관리부분이 제외되었다. 기업의 규모로 개인정보 안전성 확보조치 기준을 완화하였다고 하더라도 기술적인 보호조치에서는 특별히 효과를 볼 수 있다고 할 수 없다.

이를 개선하기 위해서는 단순하게 개인정보 보유량으로 유형을 분류하는 것보다는 개인정보를 민감정보와 간접정보로 분류하여 민감정보의 관리 보유량과 간접정보 관리 보유량으로 유형을 분류하여야 한다. 소상공인, 중소기업 및 대기업에 따른 간접 개인정보 보유량에 대한 유형은 대기업을 제외하고 소상공인과 중소기업의 유형을 동일하게 적용해도 개인정보보호 상의 큰 문제가 없으면서 이를 통해 중소규모의 기업에서도 기본적인 보호조치를 할 수 있도록 유도할 수 있다. 이러한 기준이 확립된다면 중소기업에서는 개인정보보호를 위한 투자비용에 큰 부담 없이 개인정보를 효율적으로 관리할 수 있을 것이다. [표10]은 간접 개인정보만을 보관하는 중소기업이 개인정보 안전성 확보조치 기준을 충족하도록 하는 개인정보보호 기술적인 보호조치로 개인정보처리시스템을 보유하고 있는 경우를 고려하였다.

네트워크 보안에서 UTM은 방화벽 및 IPS 그리고 VPN 기능을 보유하고 있으며, 일부 웹 방화벽의 기능을 보유하고 있으므로, 민감 개인정보의 보유량이 적은 중소기업에서는 고가의 IPS 및 웹 방화벽을 설치하지 않아도 된다. 다만, UTM의 웹 방화벽 기능은 OWASP TOP10 취약점 및 국가정보원의 8대 취약점을 모두 방어하지는 못하지만 가장 많이 발생하는 인젝션 공격 등을 방어할 수 있기 때문에 UTM으로 적정 수준에서 웹 공격에 대해 방어를 할 수 있다. 그리고 기업 내부에 웹 서버가 존재하지 않는다면 공유기를 사용해도 외부의 공격에 대해 방어할 수 있으므로 공유기보다 고가인 UTM을 설치하지 않아도 된다. 이러한 경우 보안 강도는 다소 낮아지더라도 중소기업에서는 낮은 비용으로 보안 솔루션을 도입할 수 있다.

PC 보안에서 업무용 컴퓨터의 접근통제는 Cloud DLP를 사용한다. 전형적인 DLP는 DLP 관리 서버를 별도로 구축하고, 업무용 컴퓨터에 Agent를 설치하여 매체제어를 수행하므로 많은 비용이 발생하지만 Cloud DLP의 경우에는 별도의 DLP 관리 서버를 구축하지 않고, 업무용 컴퓨터에만 Agent를 설치하여 매체제어를 수행하므로 전형적인 DLP와 비교해도 기능적인 문제없이 비용을 절감하여 보호조치를 할 수 있다. 또한, 로그기록에 있어서 DLP 관리 서버에서 저장 공간이 부족한 경우 이를 해결하기 위해 별도의 비용을 지불하여 문제점을 조치해야 하지만 Cloud DLP의 경우에는 이러한 문제에 유연하다.

표 10. 규모를 고려한 개인정보 기술적 보호조치
Table 10. Technical protection measures for personal information protection considering the size of the businesses

영역	조항	고려사항	기술적 보호조치
네트워크 보안	6조 1~2항	· 외부 공격자로부터의 침입 방지 및 웹 공격에 대해 방어 · 본/지사 간 통신 시 가설사설망을 활용	UTM (내부에 웹 서버 부재 시 공유기 사용)
PC 보안	6조 3항	업무용 컴퓨터 등에 접근통제 조치	Cloud DLP
	7조 1,5,7항	외부 반출 시 개인정보의 유출을 방지하기 위한 파일의 암호화	오피스 파일 암호화 기능 사용
	9조	업무용 컴퓨터의 개인정보 파일을 보호하기 위한 악성 프로그램 방지 및 치료	백신 프로그램
서버 보안	5조 1~6항	· 개인정보처리시스템에 접근 권한을 차등 부여 · 개인정보처리시스템의 접근 권한을 변경 또는 말소 · 접근권한의 부여, 변경 및 말소에 대한 내역을 3년간 보관 · 비밀번호를 일정 횟수 이상 잘못 입력한 경우 접근제한	DB 접근제어
	8조 1,3항	개인정보의 접속기록 보관 및 유출, 위·변조 대응	DB 접근제어
	9조	서버의 개인정보 파일을 보호하기 위한 악성 프로그램 방지 및 치료	백신 프로그램

개인정보의 안전한 송신 및 전달 등을 위해 암호화 기술을 사용할 수 있으며, 이때, 개인정보의 암호화를 위해서 고가의 DRM을 구축하는데, 간접 개인정보의 경우 교육을 통해 오피스 파일을 생성할 때마다 암호화 기능을 통해 문서를 암호화 하는 정책을 구현할 수 있다. 서버 보안에서 접근 권한 및 기록을 위해 DB 접근제어를 구축해야 한다. DB 접근제어 솔루션에는 어플라이언스 솔루션과 소프트웨어 솔루션이 존재하며, 소프트웨어 솔루션의 경우 상대적으로 적은 비용으로 도입할 수 있으므로, 민감 개인정보 보유량이 낮은 중소기업의 경우 간접 개인정보에 대해서는 소프트웨어 DB 접근제어를 구축하여 보호조치를 하도록 한다.

Ⅳ. 결 론

우리나라의 전체 사업체 수의 99% 이상을 차지하고 있는 중소기업의 경우 개인정보보호에 대한 인식이 저조하고, 또한, 개인정보보호법에 따른 개인정보 안전성 확보조치 기준을 그대로 적용하기에는 비용 및 기술면에서 커다란 어려움을 가지고 있다. 이에 본 연구에서는 변화하는 개인정보 이용 환경 분석을 바탕으로 중소규모의 기업에 맞는 개인정보 기술적 보호조치 방안을 제안하였다.

안전성 확보조치 기준에 따른 개인정보를 보호하기 위한 일반적인 기술적인 보호조치를 네트워크 보안, PC 보안, 서버 보안의 세 개의 영역으로 구분하여 제시하고, 이를 각각 중소규모의 기업에 적합하게 제안했다는 점에서 의미가 있다고 할 수 있다.

IDC에 의하면 의료 데이터의 양이 2012년 500PB에서 2020년에는 25,000PB로 약 50배가 증가할 것이라고 전망하였다. 향후, 이와 같이 폭발적으로 증가하는 스마트의료 분야에서 중소형 의료기관에 적용할 수 있는 개인정보보호를 위한 기술적 보호 조치 방안에 대한 연구를 진행할 계획이다.

References

[1] Korea Internet & Security Agency(KISA) Online Personal Information Protection Portal, https://www.i-privacy.kr/jsp/user4/intro/define1.jsp. [accessed: May 12. 2019]

[2] Kyoung-Hwan Choi, "Personal Information Protection of Medical Area", Smart Medical Treatment Information Security Conference, pp. 8, 2016.

[3] Personal Information Protection Commission, "Annual Report on Personal Information Protection", pp. 17-17, 2017.

[4] Chang-Soo Moon and Sun-Hyung Kim, "An Empirical Study on the Impact of Enterprise's Performance on Personal Information Protection Execution", Journal of Korean Institute of Information Technology, Vol. 14, No. 3, pp. 97-106, Mar. 2016.

[5] Jinhyung Kim and Hyung-Jong Kim, "A Study on the way for Handling for Personal Information Protection considering the Scale and Characteristic of Companies' Status", Journal of Security Engineering, Vol. 9, No. 1, pp. 101-106, Feb. 2012.

[6] KISA, "Criteria for Securing Personal Information Safety", No. 2019-47, 2019.

[7] Hyun-Soo Han, Kiho Kim, and Hee-Dong Yang, "SME Informatization Attributes Based Analysis for their Criticalness, Status and Policy Implication", Journal of Information Technology Application and Management, Vol. 20, No. 4, pp. 97-110, Dec. 2013.

[8] Seong-JIn Lee, "The Need of SME - Focusing on Taiwannese Companies", 2006.08.24., http://jobdahan.net/management/7855. [accessed: Jun. 15. 2019]

[9] KISA, "Local SME Information Protection Support",https://www.kisa.or.kr/business/infor/inforlev1.jsp. [accessed: Jun. 15. 2019]

[10] Personal Information Protection Commission, "2019 Annual Report on Personal Information Protection", pp. 35-46, 08, 2019.

[11] Ministry of the Interior and Safety, Personal Information Protection Commission, "Personal Information Protection research on the actual condition", 11-1312000-000035-10, 2018.

저자소개

김 신 석 (Sin-Seok Kim)

2001년 8월 : 명지대학교
전기전자공학부(공학사)
2019년 10월 ~ 현재 :
세종사이버대학교
정보보호대학원 석사과정
2012년 4월 ~ 현재 : ㈜영우디지탈
매니지드사업부 근무
관심분야 : 개인정보보호, 네트워크 보안, 시스템보안

유 혜 정 (Hye-Jeong Yoo)

1997년 2월 : 고려대학교
수학과(이학사)
1999년 2월 : 고려대학교
수학과(이학석사)
2002년 8월 : 고려대학교
수학과(이학박사)
2004년 1월 ~ 현재 :
세종사이버대학교 정보보호학과 교수
관심분야 : 사용자인증, 개인정보보호, 콘텐츠보안