ISMSP와 PIMS 인증 제도 통합에 따른 외주인력 보안통제 방안 제시

이현석*, 원동호*
*성균관대학교 정보통신대학원 정보보호학과
e-mail:oooopsboy@nile.or.kr, dhwon@skku.edu

Proposal of Security Control Plan for Outsourcing Personnel Based on Integrated ISMS and PIMS Certification Schemes

Hyun-Seok LEE*, Dong-ho Won*
*Dept of Information Security, SungKunKwan University

요 약

국민의 편의성과 효율성 제고를 위한 온라인 대국민 서비스가 증가함에 따라 보안 사고들이 빈번하게 일어나며, 인적작원을 통해 많은 개인정보가 유출되고 있다. 이에 따라서 정부에서 ISMS와 PIMS 인증제도를 통하여 안정성을 확보하기 위한 제도를 내놓았다. 하지만 두 가지 인증제도의 중복항목으로 담당자들의 업무 부담이 늘며 이를 통합을 발표하였다. 저자는 인증제도의 인력항목을 좀 더 효율적으로 관리 할 수 방안을 제시하고자 한다.

1. 서론

국민의 편의성과 효율성을 제고를 위한 온라인 대국민 서비스는 지속적으로 증가하고 있으며 추후에도 더욱 증가할 전망이다. 증명서 발급, 행정 민원처리 등을 위해 작성된 디지털 문서에는 많은 개인정보들이 전산화되어 저장되어 있으며, 이는 해당 기업 또는 기관에서 관리·보관하고 있다. 개인정보를 포함한 디지털 정보를 관리하기 위한 정보시스템은 내·외부 인력들에 의해 구축 및 운영되는데 2012년부터 2016년까지의 개인정보 유·노출 사고의 건수는 17,204만 건이며 이중 인력에 의해 개인정보 유·노출 사고의 76%가 인력에 의해 발생한다. 이에 따라 대국민 서비스를 안정적으로 운영하기 위해 정보보호 및 개인정보 보호 체계를 확립하기 위해 ISMS, PIPL, PIMS 등 인증 제도를 운영하기 시작했다.

방송통신위원회, 행정안전부에서 운영하고 있는 PIMS, PIPL은 인증은 개인정보 보호활동을 위한 인증으로 유사 인증제도로 2014년 7월 규제개혁 일환으로 인증제도 통합을 추진하여, 2016년 1월 1일부터 PIMS로 통합되어 운영되고 있다.[1] 현재 ISMS와 PIMS 두 개의 인증제도가 운영되고 있지만 개인정보 유·노출이 지속적으로 발생하여 국가에서 ISMS의 인증 의무를 발표를 하여, 기업의 부담이 커졌다. 커진 부담에 PIMS 인증 제도를 받은 기업은 중복운영에 따른 부담에 대해 토로한 결과 2017년 12월 29일 ISMS 인증과 PIMS 인증 통합방안 확정을 밝혔다.[2]

이에 따라 저자는 ISMS와 PIMS 인증제도 통합에 따른 인력관리 항목 중 외주인력 관리방안에 중점을 두어 효율적인 보안 통제 항목이 될 수 있도록 방안을 제시 해 보고자 한다.

2. 관련법령

2.1 ISMS 법적근거

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조, 동법 시행령 제47조~54조, 정보보호 관리체계 인증 등에 관한 고시를 통해 의무기관 및 인증 신청을 받아 인증을 해주고 있다. ISMS를 통해 기업이 주요 정보자산을 보호하기 위해 수립·관리·운영하는 정보보호 관리체계가 인증기준에 적합한지 심사하여 인증을 부여하는 제도이다. 이를 통해 비즈니스 안정성 제고, 정보보호 법적 준거성 확보, 신뢰도 향상 등 많은 이점을 가지고 있다.

2.2 PIMS 법적근거

정보통신망 이용촉진 및 정보보호에 관한 법률 제47조의3, 동법 시행령 제54조의2, 개인정보보호법 제32조의2, 동법 시행령 제34조의2~제34조의 8, 개인정보보호 관리체계 인증 등에 관한 고시를 통해 인증해 주고 있다. 기관 및 기업이 개인정보보호 관리체계를 갖추고 체계적·지속적으로 보호 업무를 수행하는지에 대해 객관적으로 심사하여 기준 만족 시 인증을 부여한다. 이를 통해 기업이 보유하고 있는 개인정보를 안전하게 관리하고 인증 기업의 대외 신뢰도 향상에도 기여한다.

3. ISMS 및 PIMS 인증제도 인력 통제 항목

3.1 ISMS 인증제도 인력에 대한 통제 항목

ISMS의 인증제도는 정보보호 관리과정 12개, 정보보호 대책 92개 항목으로 총 104개 항목으로 구성되어지고 있으며, 인력 통제에 관한 항목은 외부자보안, 인적보안

등으로 구성되어 있다. 세부적인 항목은 표1과 같으며, 5개 분야에, 30개의 통제사항을 분류가 된다.[3]

<표 1> ISMS 인력 통제 분야

No.	통제분야	통제목적	통제사항
1	외부자 보안	보안요구사항 정의	외부자 계약 시 보안요구사항
		외부자 보안 이행	외부자 보안 이행 관리
			외부자 계약 만료 시 보안
2	인적 보안	정보보호 책임	주요직무자 지정 및 감독
			직무 분리
			비밀유지서약서
		인사 규정	퇴직 및 직무변경 관리
			상벌규정
3	물리적 보안	물리적보호 구역	출입통제
			모바일기기 반출입
		사무실보안	개인업무 환경보안
			공용업무 환경보안
4	시스템 개발 보안	구현 및 이관 보안	개발과 운영 환경 분리
			시험데이터 보안
			소스 프로그램 보안
		외주 개발 보안	외주 개발보안
5	접근통제	접근통제 정책	접근통제 정책 수립
		접근권한 관리	사용자 등록 및 권한부여
			관리자 및 특수 권한 관리
			접근권한 검토
		사용자 인증 및 식별	사용자 인증
			사용자 식별
			사용자 패스워드 관리
			이용자 패스워드 관리
		접근통제 영역	네트워크 접근
			서버 접근
			응용 프로그램 접근
			데이터베이스 접근
			모바일기기 접근
			인터넷 접속

3.2 PIMS 인증제도 인력 통제 항목

PIMS의 인증제도는 개인정보보호 관리과정 16개, 생명주기 및 권리보장 20개, 개인정보 보호조치 50개 총 86개의 유형이 있으며, 각 적용 유형별로 인증 기준이 다르다. PIMS의 인력통제 항목은 개인정보보호 보호대책 인증기준에 속해 있으며, 3개 영역 26개 항목으로 세부항목은 표2와 같다.[4]

<표 2> PIMS 인력 통제 분야

No.	인증기준	영역	항목
1	개인정보 보호대책 인증기준	관리적보호조치	보안 서약서
			퇴직 및 직무변경 관리
			외부 위탁 계약
			위탁자 관리·감독
2		기술적보호조치	접근통제 정책 수립
			개인정보취급자 등록
			개인정보취급자 권한 관리
			특수권한관리
			개인정보취급자 접근 권한 검토
			개인정보취급자 인증 및 식별
			비밀번호 관리
			네트워크 접근
			서버 접근
			응용 프로그램 접근
			데이터베이스 접근
			인터넷 접속 통제
			직무분리
			보안 시스템 설치·운용

			모바일 기기 관리
			개발 시 보안조치
			개발과 운영환경 분리
			외주개발 보안
3		물리적 보호조치	개인 업무 환경 보안
			개인정보처리시스템 저장 매체 관리
			휴대용 저장매체 관리
			이동컴퓨팅 관리

4. 외주인력 통제 분야 비교 분석

두 가지 인증제도의 인력 통제항목 중 가시적으로 외주인력 보안 통제분야는 ISMS에서는 7개 통제사항이 있으며, PIMS에서는 5개의 통제사항이 있으며 각각 표3과 표4와 같다.

<표 3> ISMS 외주인력 통제 분야

No.	통제분야	통제목적	통제사항
1	외부자 보안	보안요구사항 정의	외부자 계약 시 보안 요구사항
		외부자 보안 이행	외부자 보안 이행 관리
			외부자 계약 만료 시 보안
2	인적 보안	정보보호 책임	직무 분리
			비밀유지서약서
		인사 규정	퇴직 및 직무변경 관리
3	시스템 개발 보안	외주 개발 보안	외주 개발보안

<표 4> PIMS 외주인력 통제 분야

No.	인증기준	영역	항목
1	개인정보 보호대책 인증기준	관리적보호조치	보안 서약서
			외부 위탁 계약
			위탁자 관리·감독
2		기술적보호조치	특수권한관리
			외주개발 보안

두가지 인증제도에서 점검하는 항목에 대해 가시적으로 외주인력 통제 보았을 때, 외주인력에 대한 전반적인 점검 항목은 인력통제 분야를 통해 행해지고 관리되고 있다. 외주인력에 관해 가시적으로 보이는 항목들은 대부분 사업 수행 시 작성 및 생성되는 보안서약서, 비밀유지계약서 등이 작성되고, 결재가 되었는지를 확인하는 항목들이다.

5. 외주인력 통제 강화 대책

사업 수행 시 작성되고 생성된 서류들을 결재를 통해 확인한다는 관점보다 외주인력으로 인한 내부자료 유출 등 보안위협을 통제하기 위해 물리적 대책, 인적보안관리, 관리적 대책, 기술적 대책으로 구분하여 외주인력을 통제해야 한다.[5]

5.1 물리적 대책

외주인력이 중요정보가 보관된 장소에 대한 접근 통제와 같은 물리적 보안대책을 위해 물리적 접근통제, 출입이력 관리, 이동매체 반·출입통제를 한다.

5.2 인적보안관리

외주인력 신원확인 등과 같은 인적보안관리가 필요하다. 상주 유지보수 인력의 신원확인, 보안의식 강화를 위한 보안교육을 실시, 보안구역 출입 통제를 해야 한다.

5.3 관리적 대책

정보시스템과 연관되어 있는 인원, 조직, 기술상에 대한 전반적이고 총체적인 보안대책이다. 작업내역 관리, 시스템 접근권한 관리, 정보시스템 관리, 조직체계 정비 및 검사를 실시한다.

5.4 기술적 대책

외주인력 통제를 위한 접근 통제와 저장 매체 통제 등의 기술적인 대책이다. 접근관리, 출력물 유출방지, 네트워크 제한, 반·출입 매체관리 등 기술적으로 유출에 대한 방지를 통제한다.

6. 결론

두 가지의 인증제도 통합에 따라 정보보안 및 개인정보보호 담당자들의 업무 부담은 많이 줄어들 것이다. 하지만 조금 더 효율적으로 운영하기 위해 통제항목 중에서도 인력분야, 그 중 외부인력 통제항목에 대해서 조금 더 구체적인 대책 마련이 필요하다.

외부자 보안, 외주개발보안 등 명시하지 않고 인적보안으로 통합하여 관리하면 조금 더 담당자들이 인증을 받는데 있어 수월 할 것이다. 그 외 외부자 관리에 있어 계약체결 및 수행에 있어 필요한 보안서약서, 비밀유지계약서 등 행정적인 업무는 시스템 사업관리 통제항목을 개설하여 사업을 체계적으로 관리 할 수 있는 방안이 효과 적이다.

그러나 제안하는 외주 인력통제에 있어 효과적인 체계를 위해 통제항목에 대한 외주인력 통제 강화대책, 데이터 관점, 시스템관점 등 각각의 관점에 대한 연구가 세부적으로 필요하다.

참고문헌

[1] 디지털데일리, http://www.ddaily.co.kr/news/article.html?no=137003

[2] 정부24, https://www.gov.kr/portal/ntnadmNews/1286470

[3] 한국정보보호심사원협회, 인포더북스 “인증심사원 자격시험과 정보보안 실무자를 위한 ISMS 실무가이드”, (2015.8):22-23

[4] 한국인터넷진흥원, “PIMS 인증제도 안내서 | 인증기준 편”, (2017.4): 7-10

[5] Eun-Sub Lee, Sin-Ryeong Kim, Young-Kon Kim, “A Study on Enhancing Security Management of IT Outsourcing for Information System Establishment and Operation”, The Journal of The Institute of Internet, Broadcasting and Communication(JIIBC), Vol. 17, No. 4, pp.27-34