정보보호 및 개인정보보호 관리체계(ISMS-P) 인증 제도에서 중소기업 기반 평가항목 도출에 관한 연구

박혁규[1] · 강완석[2] · 신광성[1,*]

[1]원광대학교 · [2](주)비제오테크

A Study on the Derivation of SME-based Evaluation Items in ISMS-P Authentication Systems

Hyuk Gyu Park[1] · Wan Seok Kang[2] · Kwang Sung Shin[1,*]

[1]Wonkwang University · [2]Vigeotech Com

E-mail : hgpark7@wku.ac.kr / stone@vigeotech.com / waver0920@wku.ac.kr

요 약

중소기업 실태조사에 따르면, 기술보호역량 수준은 매년 나아지고 있으나, 기술유출 및 피해는 지속적으로 발생하고 있다. 이는 중소기업 임직원의 보안의식 강화와 보안수준을 지속적으로 유지할 수 있는 보안관리 및 감독체계가 필요함을 보여준다. 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증 제도가 이와 관련된 최신 기준인데, 이 제도는 ISP, IDC, 병원 및 학교, 중소기업 등 인증 대상 기관의 유형을 고려하지 않고 동일한 인증 기준을 적용하는 문제점이 있다. 본 논문에서는 ISMS-P 인증과 개인정보보호 관리체계(PIMS) 인증을 참고하여 중소기업에 특화되어 적용할 수 있는 73개 평가 항목을 도출하였다. 연구 결과는 기존의 ISMS-P 인증에 비해 평가 항목 수가 28.4% 줄었음을 보여준다.

ABSTRACT

According to a survey on the infringement of SMEs, the level of technology protection capability is improving every year, but technology leaks and damage continue to occur. This shows that there is a need for a security management and supervision system that can strengthen the security awareness of SME executives and employees and maintain the security level continuously. The Personal Information & Information Security Management System(ISMS-P) authentication systems is the latest related standard, which has the problem of applying the same certification criteria without considering the types of certification target organizations such as ISPs, IDC, hospitals and schools, and SMEs.. In this paper, 73 evaluation items that can be specialized and applied to SMEs were derived by referring to ISMS-P certification and Personal Information Protection Management System (PIMS) certification. The results of the study show that the number of evaluation items decreased by 28.4% compared to the existing ISMS-P certification.

키워드

ISMS-P, PIMS, ISMS, Security Management System

Ⅰ. 서 론

중소기업의 기술보호 수준, 기술침해 현황 등에 대한 실태조사에 따르면, 기술보호역량 수준은 매년 나아지고 있으나, 기술유출 및 피해는 지속적으로 발생하고 있다. 중소기업 기술보호역량수준 실태조사(2019)에 따르면, 최근 5년간(2015～19년)의 기술유출 총 피해금액은 4,242억원이며, 기술자료 복사·절취, 핵심인력 스카웃, 이메일 및 휴대용 장치 이용 순으로 기술자료 유출이 일어났다고 한다. 또한 최근 3년 간 중소기업에서 유출사고가 발생하는 주된 이유는 보안관리 및 감독체계 미흡이 가장 높고, 다음으로 임직원 보안의식 부족, 보안투자 미흡 순으로 나타나고 있다. 이 조사 결과는

* corresponding author

중소기업 임직원의 보안의식 강화와 보안수준을 지속적으로 유지할 수 있는 적절한 보안관리 및 감독체계가 필요함을 보여준다.

본 논문에서는 이와 관련된 국내 · 외 정보보호 관리체계를 살펴보고, 현행 인증 제도의 문제점을 제시하고, 중소기업에 특화되어 적용할 수 있는 평가 항목을 정보보안 중소기업과 함께 도출하였다.

II. 국내 · 외 정보보호 관리체계

국내·외 정보보호 관리체계를 살펴보면, 국제표준인 ISO/IEC 27001 인증은 정보보호 정책, 통신 및 운영, 접근통제, 정보보호 사고대응 등 정보보호 관리 14개 분야와 114개 항목에 대해 평가한다.

정보보호관리체계(ISMS: Information Security Management System) 인증 제도는 각종 위협으로부터 정보자산을 보호하기 위해 종합적인 체계를 세우고, 심사를 통해 도출된 위협올 관리하여 기업 및 개인의 보안 위협을 관리하는 것이다. 이 제도는 정보통신망법을 근거로 기업·기관이 보호해야 할 필요가 있는 중요 정보의 보호를 위해 연 1회 심사를 통해 인증을 부여한다. 인증기준은 정보보호 관리과정 5개, 통제 분야 12개, 정보보호 대책 13개, 통제 분야 92개 등 총 104개 항목으로 구성되어 통제항목들에 대한 적합성 여부를 평가한다.

개인정보보호관리체계(PIMS: Personal Information Management System)[1] 인증 제도는 기업이 개인정보보호 활동을 체계적으로 수행하기 위해 필요한 일련의 개인정보 보호조치 체계이며, 기업의 유형별로 인증 기준을 달리한다. 이 제도는 개인정보보호법과 정보통신망법을 근거로 기업·기관이 취급하고 있는 개인정보를 보호하기 위해 연 1회 심사를 통해 그 적절성을 평가하고 인증을 부여한다. PIMS 인증기준은 개인정보보호 관리과정 4개 분야 16개 통제항목, 생명주기 및 권리보장 인증기준 2개 분야 20개 통제항목, 개인정보 보호대책 인증기준 3개 분야 50개 통제항목 등 총 9개 분야 86개 통제항목으로 구성되어 있으며 공공기관 86개, 대기업 83개, 중소기업 74개, 소기업 47개의 통제항목들에 대한 적합성 여부를 평가한다.

III. ISMS-P에서 중소기업 평가항목 도출

정보보호 및 개인정보보호 관리체계(ISMS-P)[2]는 2018년 11월 시행된 최신 표준으로, ISP, IDC, 병원 및 학교, 중소기업 등 인증 대상 기관의 유형을 고려하지 않고 동일한 인증 기준을 적용한다. ISMS-P 인증 기준 구성 항목은 102개 항목이며, 원래 ISMS 항목인 관리체계 수립 및 운영 16개 항목, 보호대책 요구사항 64개 항목에 더해 개인정보처리 단계별 요구사항 22개 항목이며 자세한 인증기준개수는 표 1과 같다.

표 1. ISMS-P 인증기준

통합인증	분야(인증기준 개수)
관리체계 수립 및 운영(16)	1 관리체계 기반 마련(6) 2 위험관리(4) 3 관리체계 운영(3) 4 관리체계 점검 및 개선(3)
보호대책 요구사항 (64)	1 정책, 조직, 자산 관리(3) 2 인적보안(6) 3 외부자 보안(4) 4 물리보안(7) 5 인증 및 권한 관리(6) 6 접근통제(7) 7 암호화 적용(2) 8 정보시스템도입 및 개발 보안(6) 9 시스템 및 서비스 운영관리(7) 10 시스템 및 서비스 보안관리(9) 11 사고 예방 및 대응(5) 12 재해복구(2)
개인정보 처리단계별 요구사항 (22)	1 개인정보 수집 시 보호조치(7) 2 개인정보 보유 및 이용 시 보호조치(5) 3 개인정보 제공 시 보호조치(3) 4 개인정보 파기 시 보호조치(4) 5 정보주체 권리보호(3)

이 기준을 중소기업에 적용하기에는 무리가 있어, 본 연구에서는 ISMS-P과 PIMS 인증을 참고하여 중소기업에 적합한 평가항목을 도출하였다.

IV. 결 론

본 연구는 정보보호 전문 중소기업인 (주)비제오테크와 함께 ISMS-P과 PIMS 인증을 참고하여 중소기업 현장에 적합한 73개 평가 항목을 도출하였다. 연구 결과는 기존의 ISMS-P 인증에 비해 평가항목 수가 28.4% 줄었음을 보여준다. 도출한 영역과 인증기준 항목을 열거하면 1. 관리체계 수립 및 운영(7개), 2. 보호대책 요구사항(45개), 3. 개인정보처리 단계별 요구사항(21개)이다.

Acknowledgement

이 논문은 한국연구재단(과학기술정보통신부)의 지원에 의함(No. NRF-2019R1G1A1087290).

References

[1] KISA, Introduction to PIMS [Internet]. KISA, c2019, [cited July, 28, 2019]

[2] KISA. ISMS-P Introduction of KISA ISMS-P [Internet]. KISA, c2019 [cited July,28, 2019]