Premium Report 제76호
(2020. 10. 30)

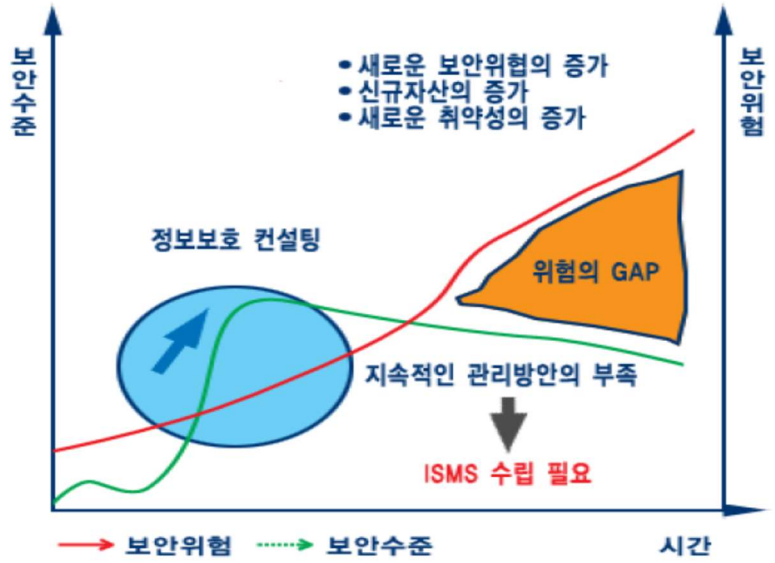
정보보호 관리체계 인증제도 이해 및 공사업체 시사점

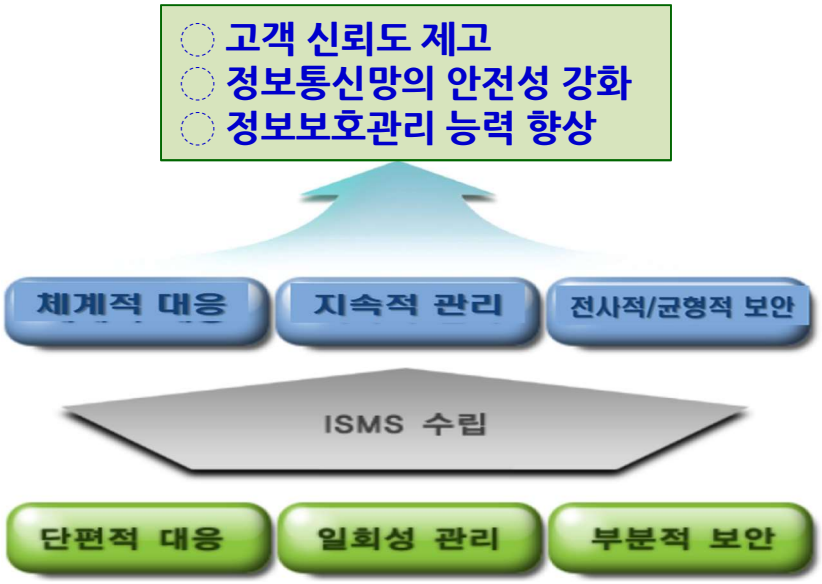
KICI 한국정보통신산업연구원

작 성 자 : 표창균 산업정책실장
내용문의 : T - (031) 231-3420 / E - capyo@kici.re.kr

1 정보보호 관리체계(ISMS) 필요한 이유

- ICT기술의 발전으로 보안대책 요구 수준이 높아지고 있지만, 지속적인 정보보호 관리 및 대응 없이는 새로운 보안위협 증가로 인해"위험의 GAP"이 점점 확대될 것임.
- 현재의 단편적 대응, 일회성 관리, 부분적 보안관리 체계보다는 정보보호 관리체계(ISMS)를 수립함으로써 "고객에 대한 신뢰도 제고, 정보통신망의 안정성 강화, 정보보호관리 능력 향상"을 위한 체계적 대응, 지속적 관리, 전사적 • 균형적 보안관리 체계 마련이 필요함.





인공지능, 빅데이터, 클라우드, IoT, 모바일 등으로 대변되는 4차산업혁명시대 도래와 함께 새로운 취약점 증가, 신규 체계의 증가 등 보안위협 요소가 증가할 것이며, 정보통신 산업과 기업 현장에서 필요한 정보보호 관리체계를 마련하고, 인증을 통해 체계적인 대응 마련이 필요한 실태임.

2 정보보호 관리체계 인증제도 개념

- 공공업무/정보서비스를 제공하는 기관이나 기업을 대상으로 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 승인된 인증기관이 증명하는 제도
- 정보보호 중심의 ISMS 인증과 정보보호 및 개인정보보호 인증 등 모두를 포함한 ISMS-P 인증으로 구분됨.

정보보호 관리체계 인증(ISMS)

정보보호의 정책/조직/관리적/기술적 대책에 대하여 인증하는 경우

정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 인터넷진흥원 또는 인증기관이 증명하는 제도

정보보호 및 개인정보보호 관리체계 인증(ISMS-P)

ISMS + 개인정보보호(-P) 대책을 모두 포함하여 인증하는 경우

정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 인터넷진흥원 또는 인증기관이 증명하는 제도

자료: 한국인터넷진흥원 (https://isms.kisa.or.kr/main/ispims/intro/).

최근 개인정보보호 관리의 중요성이 대두됨에 따라 안전행정부에서 운영하던 개인정보보호 관리체계 인증제도와 통합된 ISMS-P로 정보보호 관리체계 인증제도가 시행되고 있음

3 정보보호 관리체계 법적 근거

➢ 정보보호 관리체계의 활성화를 위해 “정보통신망 이용촉진 및 정보보호에 관한 법률(정보통신망법) 제47조과 동법 시행령 제47조~제54조, 개인정보보호법 제32조의 2”에 따라 “정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시”로 통합되어 법적 근거가 마련됨.

4 정보보호 + 개인정보보호 관리체계 인증제도 통합 추진 경과

➢ **정보보호 관리체계는 2018. 11월에 ICT환경이 융합 및 고도화된 다양한 침해 위협에 효과적으로 대응하고, 기업의 중복된 인증 심사 및 유지에 대한 부담을 경감하기 위해 정보보호(ISMS), 개인정보보호(PIMS)가 ISMS-P로 통합되어 적용 중임.**

ISMS *Information Security Management System*

정보보호 관리체계 인증

2001 ISMS 인증제도 도입
2002 인증기준 고시 제정
2013 인증 의무화
※ 정보보호 안전진단 제도 폐지
2014 인증기관 심사기관 추가 지정
2015 인증 의무대상 확대

PIMS *Personal Information Management System*

개인정보보호 관리체계 인증

2010 방통위 의결 기반 PIMS 시행
2012 정보통신망법에 법률적 근거 마련
※ 대상 : 정보통신서비스 제공 사업자
2013 개인정보보호법 기반 PIPL 제도 시행
※ 대상 : 공공기관/대기업, 중소기업, 소상공인
2016 PIMS, PIPL 인증제도 통합

융합화, 고도화되고 있는 침해위협에 효과적인 대응을 위해
정보보호와 개인정보보호의 연계 필요

심사항목이 유사하고 개별 운영에 따른 **기업의 혼란 및 재정·인력상 부담 발생**

ISMS, PIMS 통합 추진

5 정보보호 관리체계의 인증 의무 대상

➢ **정보통신망 이용촉진 및 정보보호에 관한 법률(정보통신망법) 제47조 2항에 따라 ISMS인증 의무 대상자와 자율 신청자로 구분되어 인증 획득을 위한 심사가 진행됨.**

* **인증 의무 대상자 : 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 아래 표에서 기술한 의무대상자 기준에 하나라도 해당되는 자**

대상자 기준	세부분류 (정보통신서비스제공자)	비고
(ISP) 전기통신사업법의 전기통신사업자로 전국적으로 정보통신망 서비스를 제공하는 사업자	인터넷접속서비스, 인터넷전화서비스 등	서울 및 모든 광역시에서 정보통신망서비스 제공 (SKT, SK 브로드밴드, KT, LGU+ 등)
(IDC) 타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는 사업자	서버호스팅, 코로케이션 서비스 등	정보통신서비스 부문 전년도 매출액 100억 이하인 영세 IDC 제외
(매출액 및 이용자 기준) 연간 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스매출액 100억 또는 이용자 수 100만명 이상인 사업자	인터넷쇼핑몰, 포털, 게임, 예약, Cable-SO 등	정보통신서비스 부문 저년도 매출액 100억 이상 또는 전년도 말 기준 직전 3개월간 일일 평균 이용자 수 100만명 이상 사업자
	상급종합병원 대학교	「의료법」 제3조의4에 따른 상급종합병원 직전연도 12월 31일 기준으로 재학생 수가 1만명 이상인 「고등교육법」 제2조에 따른 학교

* **자율신청자 : 의무대상자 기준에 해당하지 않으나, 자발적으로 ISMS-P를 구축·운영하는 기업·기관은 임의신청자로 분류하며, 희망할 경우 자율적으로 신청하여 인증심사를 받을 수 있음.**

6 정보보호 관리체계의 인증 업무 수행 체계

➢ 정보보호 관리체계 인증업무 수행체계로는 인증 심사를 진행하기 위하여 과기부로 부터 지정된 심사기관과 심사결과에 대해 인증/인증서 발급하는 인증기관, 관련 법제도 개선 및 정책 결정 등의 업무를 수행하는 정책기관으로 구성됨

7 정보보호 관리체계 인증심사를 위한 인증기준

➢ 2010년부터 운영된 개인정보보호관리체계(PIMS)와 정보보호 관리체계(ISMS)을 2018년에 서로 중복된 사항을 통합하여, 정보보호(ISMS : 80개)와 개인정보 처리요구사항(22개)로 구성된 ISMP-P로 인증기준을 마련함.

구분		인증분야	인증 세부 분야(인증기준 개수)	
ISMS-P (102개)	ISMS (80개)	1.관리체계 수립 및 운영(16)	1.1 관리체계 기반 마련(6) 1.3 관리체계 운영(3)	1.2 위험관리(4) 1.4 관리체계 점검 및 개선(3)
		2.보호대책 요구사항(64)	2.1 정책, 조직, 자산 관리(3) 2.3 외부자 보안(4) 2.5 인증 및 권한 관리(6) 2.7 암호화 적용(2) 2.9 시스템 및 서비스 운영관리(7) 2.11 사고 예방 및 대응(5)	2.2 인적보안(6) 2.4 물리보안(7) 2.6 접근통제(7) 2.8 정보시스템 도입 및 개발 보안(6) 2.10 시스템 및 서비스 보안관리(9) 2.12 재해복구(2)
	-P (22개)	3.개인정보 처리단계별 요구사항(22)	3.1 개인정보 수집 시 보호조치(7) 3.3 개인정보 제공 시 보호조치(3) 3.5 정보주체 권리보호(3)	3.2 개인정보 보유 및 이용 시 보호조치(5) 3.4 개인정보 파기 시 보호조치(4)

* [참고] 정보통신 시공현장에서 운영되는 CCTV 설치/운영에 대한 인증기준은 통합인증 3장 개인정보 처리단계별 요구사항 분야, 3.1 개인정보수집시 보호조치, 3.1.6 “영상정보처리기기 설치/운영”에서 인증기준으로 제시되어 있어서, 인증기준에 부합된 설치 및 운영이 되도록 함

8 정보보호 관리체계의 인증기준 적용 사례

➢ 인증기준(3.1.6 영상정보처리기 설치·운영) 확인사항 및 현장 적용 사례(예시)

인증기준	영상정보처리기기를 공개된 장소에 설치·운영하는 경우 설치 목적 및 위치에 따라 법적 요구사항(안내판 설치 등)을 준수하고, 적절한 보호대책을 수립·이행하여야 한다.
주요 확인사항	• 공개된 장소에 영상정보처리기기를 설치·운영할 경우 법적으로 허용한 장소 및 목적인지 검토하고 있는가? • 공공기관이 공개된 장소에 영상정보처리기기를 설치·운영하려는 경우 공청회·설명회 개최 등의 법령에 따른 절차를 거쳐 관계 전문가 및 이해관계인의 의견을 수렴하고 있는가? • 영상정보처리기기 설치·운영 시 정보주체가 쉽게 인식할 수 있도록 안내판 설치 등 필요한 조치를 하고 있는가? • 영상정보처리기기 및 영상정보의 안전한 관리를 위한 영상정보처리기기 운영·관리 방침을 마련하여 시행하고 있는가? • 영상정보의 보관 기간을 정하고 있으며, 보관 기간 만료 시 지체 없이 삭제하고 있는가? • 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우 관련 절차 및 요건에 따라 계약서에 반영하고 있는가?
관련 법규	• 개인정보 보호법 제25조(영상정보처리기기의 설치·운영 제한)

정상사례

• 안내판 및 홈페이지 게재 내용(예시)

CCTV 설치 안내

- ◆ 설치목적 : 범죄 예방 및 시설안전
- ◆ 설치장소 : 출입구의 벽면/천장, 엘리베이터/각층의 천장
- ◆ 촬영범위 : 출입구, 엘리베이터 및 각층 복도(360° 회전)
- ◆ 촬영시간 : 24시간 연속 촬영
- ◆ 관리책임자 : 0000과 홍길동(02-000-0000)
- ◆ 위탁관리자 : 0000업체 박길동(02-000-0000)

(설치 · 운영을 위탁한 경우)

〈출처〉 민간분야 영상정보처리기기 설치 · 운영 가이드라인(행정안전부)

결함사례

- 사례 1 : 영상정보처리기기 안내판의 고지 문구가 일부 누락 되어 운영되고 있거나 영상정보처리기기 운영·관리 방침을 수립·운영하고 있지 않는 경우
- 사례 2 : 영상정보처리기기 운영·관리 방침을 수립 운영하고 있으나 방침의 내용과 달리 보관기간을 준수하지 않고 운영되거나, 영상정보 보호를 위한 접근통제 및 로깅 등 방침에 기술한 사항이 준수 되지 않는 등 관리가 미흡한 경우
- 사례 3 : 영상정보처리기기의 설치·운영 사무를 외부업체에 위탁을 주고 있으나 영상정보의 관리 현황 점검에 관한 사항, 손해배상 책임에 관한 사항 등 법령에서 요구하는 내용을 영상정보처리기기 업무 위탁 계약서에 명시하지 않은 경우
- 사례 4 : 영상정보처리기기의 설치·운영 사무를 외부업체에 위탁을 주고 있으나 영상정보처리기기 안내판에 수탁자의 명칭과 연락처를 누락하여 고지한 경우

영상정보처리기 설치사례와 같이 정보통신공사 설계/시공시 인증기준에 부합한 시공/운영이 요망됨.

9 정보보호 관리체계 인증제도의 공사업체 시사점

다양하고, 지능화된 사이버침해로 부터 안전한 정보통신 환경 조정이 선제적으로 필요함. 이에 따라, 정보통신공사업체는 효과적이고, 안정적인 정보보호 관리체계의 구축 및 인증 제도 활용을 위해 ISMS-P에 대한 이해와 관심이 요망되며, 다음과 같은 시사점을 제시함

- [사이버 침해 대응에 대한 필요성 인식] 공공기관 및 주요정보통신기반시설, 금융기관 등 정보통신공사업 현장에서 사이버 침해 대응은 전문성과 체계적인 대응이 요구됨에 따라, ISMS-P 등 인증제도를 통한 체계적인 정보보호 관리체계 활용이 필요함.
- [법령에 의한 인증제도 의무 적용 / 활용] 정보보호 관련 법령에 따라 정보보호 침해 대응에 대한 의무사항이 제시되고 있으며, ISMS-P 인증기준을 반영한 정보통신 설계기준 및 표준공법 마련 등 개선이 필요함
- [인증제도에 의한 정보보호 대응체계 마련] 다양한 정보통신환경에서 효과적인 사이버 침해 대응을 위해 정보보호관리체계 인증기준에서 제시된 기술적 대책과 CCTV/정보통신보안체계 설치 등 물리적 대책, 보안지침에 의해 통제되는 관리적 대응까지 다양한 공종이 적용된 시공현장까지 정보보호 관리를 위한 세부적인 대응체계 마련이 요망됨
- [지속적인 거버넌스 대응] 정보보호 관리체계 인증의 일회성 대책이 아닌 정보보호 거버넌스 마련을 위한 조직의 정책 마련과 정보보호 조직 역량 강화, 정보보호 업무절차 마련, 대책에 대한 지속적인 훈련과 대응이 요망됨