정보보호 및 개인정보보호 관리체계 인증제도 국내 동향

이준성 _ TTA 정보보호단 책임연구원

1. 머리말

최근 우리나라는 정보통신기술의 눈부신 발전과 함께 비약적인 경제성장을 이루었고, 정보통신은 생활과 분리하여 생각할 수 없을 만큼 우리의 삶 깊숙이 들어와 영역을 확고히 굳히고 있다. 하지만 이와 동시에 1.25 인터넷 침해사고, 7.7 DDoS, 금융 및 민간기업 해킹사고, 랜섬웨어 감염, 가상통화거래소 해킹사고와 각종 개인정보 유출사고 등이 지속적으로 발생하는 등 사이버 위협은 나날이 지능화·고도화되어 그 피해는 지속적으로 증가하고 있는 추세이다. 이에 대응하고자 2001년 정보보호 관리체계(ISMS) 인증제도를 시작으로 정보보호 안전진단 제도, 전자정부 정보보호 관리체계(G-ISMS), 개인정보 관리체계(PIMS), 개인정보보호 인증제(PIPL), 금융 정보보호 관리체계(F-ISMS) 순으로 유사한 인증제도가 생성되었고, 정보보호 관리체계(ISMS) 및 개인정보 관리체계(PIMS)로 통합하여 이원화된 인증제도를 운영해 왔다. 최근 인증제도의 일원화 관리의 필요성이 대두되어 정보보호 및 개인정보보호 관리체계(ISMS-P)로 모두 통합되어 운영하고 있으며, 이에 국내 정보보호·개인정보보호 인증제도 현황 및 통합된 정보보호 및 개인정보보호 관리체계에 대해서 정리해 보았다.

2. 국내 정보보호 및 개인정보보호 인증제도 현황

2.1 정보보호 관리체계 인증제도

2.1.1 정보보호 안전진단 제도

정보보호조치, 즉 안전진단 기준인 관리적·기술적·물리적 보호조치를 이행하도록 함으로써 주요정보통신서비스제공자, 집적정보통신시설사업자 등의 정보통신망에 대한 침해사고 예방을 통해 안정적이고 신뢰성 있는 정보통신서비스를 제공하도록 한다.

안전진단대상자가 의무적으로 준수해야 할 지침에 대한 이행여부를 정보보호컨설팅전문업체로부터 확인하고 매년 일정기간 내에 정보보호 안전진단을 받도록 한 제도이다.

2.1.2 전자정부 정보보호 관리체계(G-ISMS)

전자정부 정보보호 관리체계 인증은 세계적인 우

<표 1> 국내 정보보호 및 개인정보보호 인증제도

구분		내용	인증기관	비고
정보보호	정보보호 안전진단 제도	정보통신서비스 제공자 및 집적정보통신시설 사업자에 대한 정보보호지침 준수여부를 점검	한국인터넷진흥원	ISMS 통합 (2013. 2.)
	전자정부 정보보호 관리체계(G-ISMS)	정부 및 행정기관에 대한 정보보호지침 준수여부를 심사하여 인증	한국인터넷진흥원	ISMS 통합 (2014. 11.)
	정보보호 관리체계 (ISMS)	정보통신망서비스 제공자, 집적정보통신시설 사업자, 연간 매출액 또는 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 자에 대한 정보보호지침 준수여부를 심사하여 인증	한국인터넷진흥원	ISMS-P 통합 (2018. 11.)
	금융 정보보호 관리체계 (F-ISMS)	금융권 보안 관련 규정 및 표준을 참고하여 적합한 정보보호지침 준수여부를 심사하여 인증	금융보안원	ISMS-P 통합 (2018. 11.)
개인정보보호	개인정보보호 인증제 (PIPL)	공공기관이나 민간기업에 대한 개인정보 보호조치 준수여부를 심사하여 인증	한국정보화진흥원	PIMS 통합 (2016. 1.)
	개인정보보호 관리체계 (PIMS)	개인정보보호 관리체계를 수립·운영하고 있는 사업자에 대한 개인정보 보호조치 준수여부를 심사하여 인증	한국인터넷진흥원	ISMS-P 통합 (2018. 11.)
정보보호 및 개인정보보호 관리체계 (ISMS-P)		정보통신망서비스 제공자, 집적정보통신시설 사업자, 연간 매출액 또는 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 자, 개인정보보호 관리체계를 수립·운영하고 있는 사업자에 대한 정보보호지침 및 개인정보 보호조치 준수여부를 심사하여 인증 부여	한국인터넷진흥원	현재 운영

수성을 인정받은 전자정부의 정보보호 성과 강화를 목적으로 전자정부 대민서비스의 정보보호 강화 대책 일환으로 관리체계를 도입하였다.

기관이 수립하고 구축한 종합적인 정보보호 관리체계를 제3자가 객관적으로 심사하여 인증을 부여하는 제도이며, 정부 및 행정기관 등의 조직 및 서비스 특성에 적합하게 수립된 종합적인 정보보호 관리체계를 의미한다.

일반적으로 인증범위를 조직 전체로 선정해야 하나 일부 기관의 규모와 특성에 따라 인증범위를 조직의 일부 또는 서비스 단위로 나누어 추진하고 향후 단계적으로 인증범위를 확대할 수 있다.

2.1.3 정보보호 관리체계(ISMS)

정보보호 관리체계는 조직이 보존해야 할 정보자산의 기밀성·무결성·가용성을 실현하기 위한 절차와 과정을 체계적으로 수립하여 지속적으로 관리하고 운영하는 제도이다.

인증운영은 정보보호정책 수립 및 범위 설정, 경영진 책임 및 조직구성, 위험관리, 정보보호대책 구현, 사후관리의 5단계를 거쳐 수립·운영되고, 정보보호대책 요구사항(선택항목)으로는 정보보호 관련 위험을 통제하기 위해 관리과정 5개 분야 12개 통제항목, 정보보호대책 13개 분야에 대해 92개 통제항목을 제시하고 있다.

모든 기관 및 기업의 경우 인증대상이며, 정보통신망서비스제공자, 집적정보통신시설 사업자, 연간 매출액 또는 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 자는 의무적으로 인증을 취득해야 한다. 인증 획득 시 그 인증의 유효기간은 3년이며, 매년 1회 중간심사를 통과해야 인증이 유효하다.

2.1.4 금융 정보보호 관리체계(F-ISMS)

정보보호 관리체계(ISMS) 기반으로 금융 보안관

<표 2> 정보보호 관리체계(ISMS)와 금융 정보보호 관리체계(F-ISMS) 세부항목 비교

구분		관리과정	보호대책	합계
정보보호 관리체계(ISMS)		28	225	253
금융 정보보호 관리체계 (F-ISMS)	유지	19	128	324
	변경	9	96	
	추가	3	69	
	합계	31	293	

련 규정 및 표준 등을 참고하여 금융권에 특화된 절차와 과정을 체계적으로 수립하여 관리 및 운영하는 제도이다. 금융 정보보호 관리체계는 정보보호 관리체계(ISMS)와 104개 통제항목은 같으나 세부항목이 기존 253개에서 324개로 강화하여 금융보안원이 운영하고 있다.

2.2 개인정보보호 관리체계 인증제도

2.2.1 개인정보보호 인증제(PIPL)

개인정보보호 인증제는 「개인정보보호법」을 기반으로 개인정보처리자의 개인정보보호 관리체계 구축 및 개인정보 보호조치사항을 이행하고 일정한 보호수준을 갖춘 경우 인증마크를 부여하는 제도이다.

업무를 목적으로 개인정보를 처리하는 공공기관, 민간기업, 법인단체 및 개인 등 모든 공공기관 및 민간 개인정보처리자를 대상으로 한다.

개인정보보호 인증과정을 통해 개인정보보호 관련 법령에서 요구하는 기준을 기관 내부에서 준수하는 여부를 점검하고, 조직 내부 구성원에게 개인정보보호에 대한 중요성을 전파하고, 인식 및 역량을 제고할 수 있다.

개인정보를 수집·이용하고 있는 공공기관 및 민간기업이 「개인정보보호법」에서 요구하는 보호조치와 활동을 이행하고 일정수준 이상 달성했는지를 승인하는 제도로 인증대상은 공공기관·대기업·중소기업·소상공인으로 하고 있는 자율 인증제도이다.

2.2.2 개인정보 관리체계(PIMS)

개인정보 관리체계는 방송통신위원회 의결 및 「정보통신망법」을 기반으로 국민들에게는 개인정보를 안전하게 관리하는 조직을 객관적으로 식별할 수 있는 기준을 제시하고 조직 스스로 개인정보 유·노출 및 개인정보의 수집·보관·이용 등 취급 절차상에서 발생할 수 있는 침해 요인을 파악하고 이를 미연에 방지하도록 하는 체계적이고 종합적인 관리체계이다.

인증체계는 개인정보관리과정, 개인정보보호대책 및 개인정보생명주기 3개 분야의 124개 통제항목으로 구성된다. 인증대상은 개인정보를 처리하는 기업 및 기관, 개인으로 하고 있는 자율 인증제도이다.

3. 정보보호 및 개인정보보호 관리체계 (ISMS-P) 인증제도

정보보호 및 개인정보보호 관리체계는 조직의 각종 보안위협으로부터 주요 정보자산을 보호하기 위해 정보보호 및 개인정보보호 관리 절차, 관리적·기술적·물리적 보호대책을 체계적으로 수립하여 지속적으로 운영·관리하기 위한 종합적인 체계이다.

3.1 추진배경

정보보호 관리체계(ISMS)는 2001년 제도 도입 이

[그림 1] ISMS 및 PIMS 통합추진 경과

[그림 2] 법령과의 관계

후 정보보호 안전진단 제도와 전자정부 정보보호 관리체계(G-ISMS)가 통합되어 2015년 인증 의무대상을 확대하게 된다.

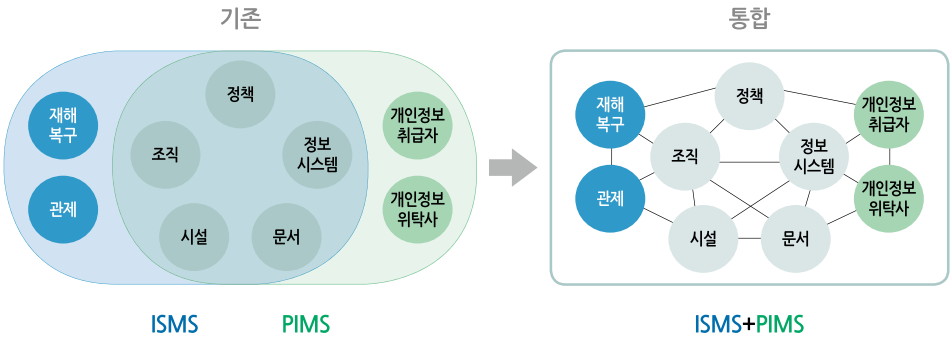
개인정보보호 관리체계(PIMS)는 2010년 제도 도입 이후 2016년 개인정보보호 인증제(PIPL)와 통합되었다.

두 인증제도 간 정보서비스 및 개인정보보호 및 관리를 위해 연계가 필요하게 되었고, 정보보호 관리체계와 개인정보보호 관리체계 내 통제항목이 일부 유사하고 개별 운영에 따른 기업의 혼란 및 재정·인력상 부담이 발생하게 되어 정보보호 관리체계 및 개인정보보호 관리체계의 통합 추진이 이루어지게 되었다.

이에 과학기술정보통신부, 방송통신위원회, 행정안전부는 기존 정보보호 관리체계 인증 등에 관한 고시(「정보통신망법」), 개인정보 관리체계 인증 등에 관한 고시(「개인정보보호법」)로 이원화되어 운영되던 제도를 일원화하기 위하여 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시로 통합하여 개정하였다.

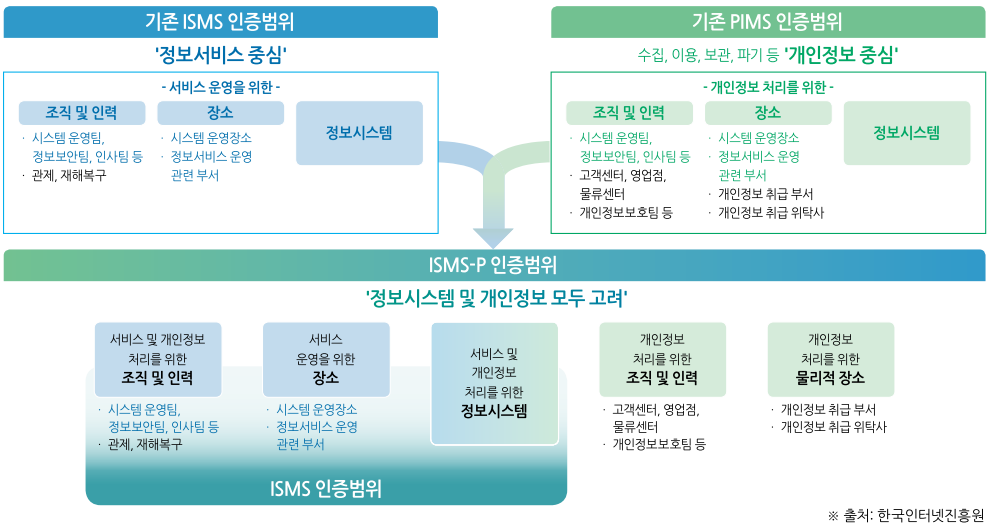
3.2 통합인증 내용

정보보호 관리체계(ISMS)와 개인정보보호 관리체



※ 출처: 한국인터넷진흥원

[그림 3] 정보보호 관리체계(ISMS) 및 개인정보보호 관리체계(PIMS) 통합 방안



※ 출처: 한국인터넷진흥원

[그림 4] 정보보호 및 개인정보보호 관리체계(ISMS-P) 통합인증 범위

계(PIMS) 내 정책, 조직, 시설, 문서, 정보시스템 등 중복된 통제항목을 도출하여, 단일제도에서 정보보호 및 개인정보를 체계적으로 관리할 수 있도록 인증제도 통합 방안을 도출하였다.

3.2.1 통합인증 범위

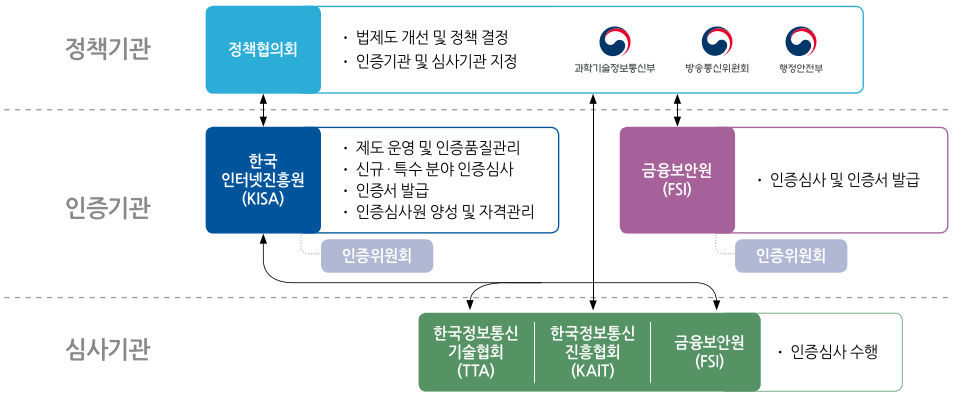
기존 정보서비스 중심의 정보보호 관리체계(ISMS) 인증범위와 개인정보 중심의 개인정보보호 관리체계(PIMS) 인증범위를 모두 고려하여 정보시스템 및 개인정보 중심으로 인증범위를 통합하였다.

정보서비스를 위한 조직·인력·장소, 개인정보처리를 위한 조직·인력·장소, 정보서비스와 개인정보처리를 위한 정보시스템으로 범위를 선정하고, 기존 인증과 유사한 정보보호 관리체계(ISMS) 인증범위와 개인정보보호를 추가한 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증으로 범위를 크게 구분하였다.

통합인증은 ISMS-P(정보보호 및 개인정보보호 관리체계)와 ISMS(정보보호 관리체계)로 인증범위를 구분하여 인증신청 할 수 있도록 제도화하였다.

<표 3> 통합 인증 구분

구분	내용	대상
정보보호 및 개인정보보호 관리체계 (ISMS-P)	개인정보의 흐름과 정보보호 영역을 모두 인증하는 경우	보호하고자 하는 정보서비스가 개인정보의 흐름을 가지고 있어 개인정보 처리단계별 보안강화가 필요한 조직
정보보호 관리체계 (ISMS)	정보보호 중심으로 인증하는 경우	기존 의무대상 기업·기관, 개인정보를 보유하지 않거나 개인정보 흐름의 보호가 불필요한 조직



※ 출처: 한국인터넷진흥원

[그림 5] 정보보호 및 개인정보보호 관리체계(ISMS-P) 담당기관

3.2.2 담당기관 및 체계

기존 정보보호 및 개인정보보호 관리체계 담당기관인 과학기술정보통신부와 방송통신위원회, 행정안전부가 정책협의회를 구성하여 법제도 개선 및 정책을 결정하고, 인증기관은 한국인터넷진흥원 및 금융보안원, 심사기관은 한국정보통신기술협회(TTA), 한국정보통신진흥협회(KAIT), 금융보안원이 담당하고 있다.

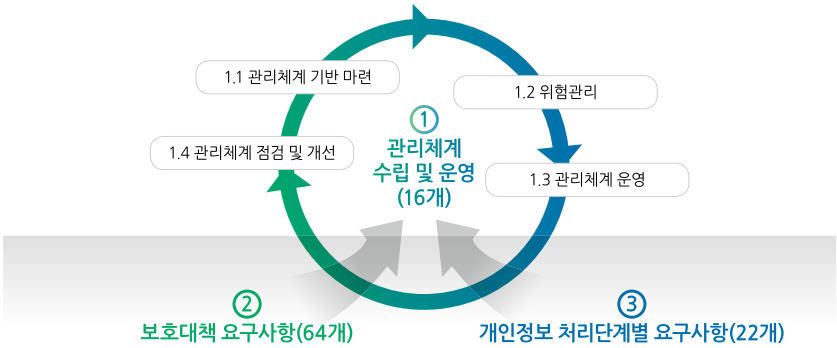
3.2.3 통합 인증기준

정보보호 및 개인정보보호 관리체계(ISMS-P) 인증기준은 크게 3개 영역(관리체계 수립 및 운영, 보호대책 요구사항, 개인정보 처리단계별 요구사항)에서 총 102개의 인증기준으로 구성되어 있다. 정보보호관리체계(ISMS) 인증을 받고자 하는 기업 및 기관은 2개 영역(관리체계 수립 및 운영, 보호대책 요구사항) 80개의 인증기준을 적용받게 되며, 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증을 받고자 하는 기업 및 기관은 3개 영역 102개 인증기준을 적용받게 된다.

3.3 기대효과

정보보호 관리체계(ISMS) 및 개인정보보호 관리체계(PIMS) 인증제도 내 개별 운영 중인 행정 및 인증심사 절차를 통합하여 신청기관이 인증에 소요되는 비용·행정·인력에 대한 부담을 절감하고 복수 인증제도 운영에 따른 기업의 혼란을 해소할 수 있다.

정보시스템의 안정성과 정보서비스 및 개인정보 흐름을 중점적으로 분석을 통한 내재된 위험성을 관리하여 융합화·고도화되는 사이버 침해 및 위협에



※ 출처: 한국인터넷진흥원

[그림 6] 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증기준(3개 분야 102개 기준)

효과적으로 대응이 가능하다.

4. 맺음말

정보보호 및 개인정보보호 관리체계(ISMS-P) 통합 인증 제도는 유사하거나 중복된 항목을 단순하게 통합 및 재배치하는 것이 아니라 최신 기술 및 이슈, 법 개정에 따른 요구사항을 반영하여 인증기준을 강화하였다. 특히 정보서비스 및 개인정보 흐름 분석, 클라우드 및 핀테크 서비스 보안강화, 개인정보 관련 강화된 보호조치 등을 반영하였다. 최초 정보보호 관리체계(ISMS)가 시행되었을 때부터 현재까지 정보보호 인증 제도에 대한 실효성 논란은 있지만, 통합된 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증을 신청한 기업 및 기관은 내·외부 사이버 위협으로부터의 보증수표가 아닌 정보보호 및 개인정보보호를 위한 최소한의 관리체계를 갖추기 위한 시작이며 지속적으로 발전시킬 수 있도록 활성화시켜야 할 필요가 있다.

[참고문헌]

[1] 인증제도 통합에 따른 고시 개정사항 안내, KISA
[2] 정보보호 안전진단 제도 소개, KISA
[3] 전자정부 정보보호관리체계(G-ISMS)인증 안내서, 행정안전부
[4] ISMS-P를 통해 본 개인정보보호 및 정보보호 정책의 흐름 변화, 김성동
[5] 개인정보 보호 인증(PIPL) 안내서, NIA
[6] 통합 PIMS 인증제도 및 인증기준 안내교육, KISA
[7] 정보보호관리체계 구축 및 활용(장상수 외)

[주요 용어 풀이]

- G-ISMS(Government Information Security Management System): 전자정부 정보보호 관리체계
- ISMS(Information Security Management System): 정보보호 관리체계
- PIPL(Personal Information Protection Level): 개인정보보호 인증제
- PIMS(Personal Information Management System): 개인정보보호 관리체계
- ISMS-P(Personal Information & Information Security Management System): 정보보호 및 개인정보보호 관리체계