EXPERT COLUMN

ISMS-P

정보보호 통합 인증 ISMS-P

정보보호 통합 인증, 기업 부담 줄여줄까?

지난 9월, 과학기술정보통신부와 행정안전부, 방송통신위원회가 '정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시' 전부개정안을 마련하고 9월 10일부터 행정예고 했다. 이번 개정안은 대표적인 두 가지 정보보호 관련 인증과 관련해 인증 체계와 인증 기준, 심사기관 등 인증 전반에 걸친 통합을 통해 기업의 불편과 부담을 최소화하는 것을 골자로 하고 있다.

이 글에서는 이번 개정안으로 기업의 정보보호 관리 체계 인증 심사가 어떻게 변화하는지 살펴본다.

우리나라 정보보호 인증의 양대 축이라면 '정보보호 관리체계(Information Security Management System, 이하 ISMS)' 인증과 '개인정보보호 관리체계(Personal Information Management System, 이하 PIMS)' 인증을 들 수 있다.

ISMS 인증은 과학기술정보통신부에서 주관하며, 관리과정 12개, 정보보호대책 92개 등 총 104개의 통제 항목으로 구성되어 있다. 정보보호 관리과정과 보안 대책 등 정보보호 관리체계의 적정성을 심사하는 ISMS 인증을 필수로 취득해야 하는 사업체는 전기통신사업법의 전기통신 사업자로 전국적으로 정보통신망 서비스를 제공하는 사업자(ISP)이거나 타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는 사업자(IDC)라면 모두 해당된다. 일반 사업자의 경우, 연간 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스 매출액 100억원 또는 이용자 수 100만명 이상이면 의무적으로 ISMS 인증을 받도록

되어 있고, 직전 연도 12월 31일기준으로 재학생 수가 1만명 이상인 '고등교육법' 제2조에 따른 학교나 상급 병원도 ISMS 인증 취득의 의무가 있다.

PIMS는 개인정보보호에 특화된 정보보호 인증으로, 개인정보의 수집 · 이용 · 파기 등 개인정보보호 관리 체계의 적정성을 심사하는 인증 제도다. 행정안전부와 방송통신위원회에서 주관하며, 관리과정 16개, 생명주기 및 권리보장 20개, 개인정보보호조치 50개 등 총 86개의 통제 항목으로 구성되어 있다. PIMS는 ISMS와 달리 대상자의 규모에 따라 통제 항목이 차별적으로 적용된다. 즉, 공공 기관에는 86개 항목 전부를 적용하지만 대기업은 83개, 중소기업은 74개, 소상공인은 47개 항목으로 축소 적용된다.

다른 듯 같은 ISMS와 PIMS, 문제는 이중 부담

이름이 비슷하지만 이들 두 인증은 주관 부처도 다르고 통제 항목의 수나 유형도 다르다. 그러나 세부적으로 들여다보면 유사한 부분이 상당히 많다. [표 1]은 두 인증의 통제항목 중 유사한 부분을 표시한 것이다.

ISMS			PIMS		
분야		항목	분야		항목
관리과정	1. 정보보호정책 수립 및 범위결정	2	관리과정	1.1 정책 및 범위	3
	2. 경영진 책임 및 조직구성	2		1.2 경영진 책임	1
	3. 위험관리	3		1.3 조직	3
	4. 정보보호대책 구현	2		2.1 개인정보식별	2
	5. 사후관리	3		2.2 위험관리	3
				3.1 개인정보보호체계 검토	2
				4.1 교정 및 개선 활동	1
				4.2 내부 공유 및 교육	1
정보보호대책	1. 정보보호정책	6	개인정보보호대책		
	2. 정보보호조직	4			
	3. 외부자 보안	3		7.3 위탁업무관리	3
	4. 정보자산 분류	3			
	5. 정보보호 교육	4		7.1 교육 및 훈련	1
	6. 인적 보안	5		7.2 개인정보취급자 관리	3
				9.1 영상정보처리기기 관리	2
	7. 물리적 보안	9		9.2 물리적 보안관리	3
				9.3 매체관리	3
	8. 시스템개발보안	10		8.6 개발보안	5
	9. 암호통제	2		8.5 암호화 통제	2
	10. 접근통제	14		8.1 접근권한관리	
				8.2 접속기록관리	
				8.3 접근통제영역 관리	
	11. 운영보안	22		8.4 운영보안	
	12. 침해사고관리	7		7.4 침해사고 관리	
	13. IT재해복구	3			
				5. 개인정보 생명주기 관리	16
				6. 정보주체 권리 보장	4
	합계	106		합계	86

[표 1] ISMS 인증과 PIMS 인증의 유사 항목

[표 1]에서 볼 수 있는 것처럼 PIMS 인증에서 취급하는 주요 정보 자산이 '개인정보'라는 점만 제외하면 IT 시스템이나 정책수립, 조직, 인력에 대한 보안 통제항목이 대부분 ISMS의 그것과 겹친다. 그럼에도 불구하고 이들 두 인증을 각각 받아야 했던 기업으로서는 상당한 비용을 부담해야만 했다. 컨설팅 등 준비 비용과 인증심사 비용이 별도로 소요되기 때문이다. 정부에서도 이런 문제를 오래 전부터 인지하고 개선 방안을 고려한 결과 지난해 12월 'ISMS-P'라는 이름으로 인증 제도 통합 방안을 수립, 지난 9월 이에 대한 시행을 예고한 것이다.

ISMS-P, 무엇이 어떻게 달라지나

지난 9월 10일 행정예고 된 통합인증은 102개 기준으로 구성되어 있다. 만일 ISMS 인증을 신규로 취득하고자 하는 사업체(신청자)라면 정보보호 관련 80개 인증 항목에 대한 인증 심사를 받을 수 있고, 개인정보 관련 22개 항목을 추가하면 통합 인증인 '정보보호 및 개인정보보호 관리체계(ISMS-P)' 인증을 받을 수 있다.

ISMS-P의 통제항목 수가 결코 적지 않지만, 전체 통제항목을 살펴봄으로써 통합 인증체계를 개괄해보자. 우선, [표 2]는 관리 과정 부분의 공통사항이다. 눈에 띄는 것은 위험관리 영역([표 2]의 1.2) 분야에 개인정보보호 관리체계에서 중요하게 취급하는 '흐름 분석'([표 2]의 1.2.2)이 녹아들어 있다는 점이다. 개인정보보호 관리체계 인증까지 받을 것이 아니라면 굳이 개인정보 흐름 분석을 할 필요는 없겠지만 통합인증 시에는 반드시 반영해야 할 중요한 사항이다.

분야		항목	
1.1	관리체계 기반 마련	1.1.1	경영진의 참여
		1.1.2	최고책임자의 지정
		1.1.3	조직 구성
		1.1.4	범위 설정
		1.1.5	정책 수립
		1.1.6	자원 할당
1.2	위험관리	1.2.1	정보자산 식별
		1.2.2	현황 및 흐름 분석
		1.2.3	위험 평가
		1.2.4	보호대책 선정
1.3	관리체계 운영	1.3.1	보호대책 구현
		1.3.2	보호대책 공유
		1.3.3	운영현황 관리
1.4	관리체계 점검 및 개선	1.4.1	법적 요구사항 준수 검토
		1.4.2	관리체계 점검
		1.4.3	관리체계 개선

[표 2] ISMS-P 관리체계 수립 및 운영

정책과 조직 관련 통제항목은 대폭 간소화되었다. 정보보호정책 6개 항목과 조직 관련 4개 항목이 각각 1개씩으로 통합되었다. 그러나 내용이 빠졌다기 보다는 한 가지 항목 안에 다 녹여 넣은 것으로 보인다. 반면 기존에 3개 통제항목으로 구성되어 있던 외부자 보안 통제 항목([표 3]의 2.3)은 1개가 늘어 4개 항목이 되었다. 이는 최근 수년 간 발생했던 개인정보 유출 사고 중 외부자에 의한 경우가 많았다는 점이 반영된 것으로 짐작된다.

분야		항목	
2.1	정책, 조직, 자산 관리	2.1.1	정책의 유지관리
		2.1.2	조직의 유지관리
		2.1.3	정보자산 관리
2.2	인적 보안	2.2.1	주요 직무자 지정 및 관리
		2.2.2	직무 분리
		2.2.3	보안 서약
		2.2.4	인식제고 및 교육훈련
		2.2.5	퇴직 및 직무 변경 관리
		2.2.6	보안 위반 시 조치
2.3	외부자 보안	2.3.1	보호대책 구현
		2.3.2	보호대책 공유
		2.3.3	운영현황 관리
		2.3.4	외부자 계약 변경 및 만료 시 보안
2.4	물리보안	2.4.1	보호구역 지정
		2.4.2	출입통제
		2.4.3	정보시스템 보호
		2.4.4	보호설비 운영
		2.4.5	보호구역 내 작업
		2.4.6	반출입 기기 통제
		2.4.7	업무환경 보안

[표 3] ISMS-P 보호대책 요구사항

물리보안([표 3]의 2.4)에서는 케이블 보안, 시스템 배치 및 관리로 구분되던 항목이 '정보시스템 보호'라는 항목으로 통합되었으며, 여기에 기존의 개인업무 환경 보안과 공용 업무 환경 보안이 '업무환경 보안([표 3]의 2.4.7)'으로 합쳐졌다.

분야		항목	
2.5	인증 및 권한 관리	2.5.1	사용자 계정 관리
		2.5.2	사용자 식별
		2.5.3	사용자 인증
		2.5.4	비밀번호 관리
		2.5.5	특수 계정 및 권한 관리
		2.5.6	접근권한 검토
2.6	접근통제	2.6.1	네트워크 접근
		2.6.2	정보시스템 접근
		2.6.3	응용프로그램 접근
		2.6.4	데이터베이스 접근
		2.6.5	무선 네트워크 접근
		2.6.6	원격접근 통제
		2.6.7	인터넷 접속 통제
2.7	암호화 적용	2.7.1	암호정책 적용
		2.7.2	암호키 관리

[표 4] ISMS-P 인증 및 권한 관리

분야		항목	
2.8	정보시스템 도입 및 개발 보안	2.8.1	사용자 계정 관리
		2.8.2	사용자 식별
		2.8.3	사용자 인증
		2.8.4	비밀번호 관리
		2.8.5	특수 계정 및 권한 관리
		2.8.6	접근권한 검토
2.9	시스템 및 서비스 운영 관리	2.9.1	변경관리
		2.9.2	성능 및 장애관리
		2.9.3	백업 및 복구관리
		2.9.4	로그 및 접속기록 관리
		2.9.5	로그 및 접속기록 점검
		2.9.6	시간 동기화
		2.9.7	정보자산의 재사용 및 폐기
2.10	시스템 및 서비스 보안 관리	2.10.1	보안시스템 운영
		2.10.2	클라우드 보안
		2.10.3	공개서버 보안
		2.10.4	전자거래 및 핀테크 보안
		2.10.5	정보전송 보안
		2.10.6	업무용 단말기기 보안
		2.10.7	보조저장매체 관리
		2.10.8	패치관리
		2.10.9	악성코드 통제

[표 5] ISMS-P 정보시스템 도입 및 개발보안

인증 및 권한관리는 기존 접근통제 영역에서 다루던 '사용자 인증 식별'과 '권한 관리'가 별도의 독립적인 항목으로 분류되었다. 추가되거나 변경된 부분이 있다기보다 개념적으로 유사한 항목들을 합리적으로 재배치한 것으로 보인다.

한편, 접근통제([표 4]의 2.6)에서는 실제 업무 환경에서 흔히 볼 수 있는 원격접근이나 무선 네트워크에 관한 항목을 기존 운영보안 영역에서 옮겨와 적용하였다. 암호화 적용([표 4]의 2.7)은 통제항목의 수와 내용면에서 기존과 동일하다.

정보시스템 도입 및 개발보안은 기존 ISMS의 시스템 개발보안 분야 통제항목 10가지 중에서 인증, 접근권한, 보안로그, 외주개발보안 항목을 줄여 6개가 되었다. 이 경우에도 기존 항목이 없어졌다기보다는 외주관리나 인증 통제 영역에서 해당 사항을 통제한다고 이해하면 된다.

ISMS 인증의 운영보안 영역은 통합인증 체계에서는 ▲시스템 및 서비스 운영관리([표 5]의 2.9)와 ▲시스템 및 서비스 보안 관리([표 5]의 2.10)로 나뉘어 있는데, 시스템 및 서비스 운영관리는 기존과 큰 차이가

없다. 다만, 시스템 및 서비스 보안관리에서 '클라우드 보안'과 '전자거래 및 핀테크 보안'은 새로운 기술 흐름을 적극 반영한 신규 통제 항목이라 하겠다.

분야		항목	
2.11	사고 예방 및 대응	2.11.1	사고 예방 및 대응체계 구축
		2.11.2	취약점 점검 및 조치
		2.11.3	이상행위 분석 및 모니터링
		2.11.4	사고 대응 훈련 및 개선
		2.11.5	사고 대응 및 복구
2.12	재해복구	2.12.1	재해·재난 대비 안전조치
		2.12.2	재해 복구 시험 및 개선

[표 6] ISMS-P 침해사고 예방 및 대응

침해사고 예방 및 대응 관련 통제항목도 '예방'과 '대응'이라는 관점에서 일관되게 정리되었다. 항목은 7개에서 5개로 줄었지만 기존 내용을 모두 포함하고 있으며, 특히 침해사고 예방에서 중요한 취약점 점검 및 조치를 추가한 것은 매우 적절한 배치라 할 수 있겠다.

신규로 정보보호 인증을 취득하려는 기업이라면

향후 신규로 ISMS 인증을 받고자 하는 사업체(신청자)라면 위에서 언급한 80개 기준에 대해서만 심사를 준비하면 될 것이다. 만일 개인정보보호 인증까지 통합하여 받고자 한다면 [표 7]의 22개 항목을 추가로 준비하면 된다.

분야		항목	
3.1	사고 예방 및 대응	3.1.1	개인정보 수집 제한
		3.1.2	개인정보의 수집 동의
		3.1.3	주민등록번호 처리 제한
		3.1.4	민감정보 및 고유식별정보의 처리 제한
		3.1.5	간접수집 보호조치
		3.1.6	영상정보처리기기 설치·운영
		3.1.7	홍보 및 마케팅 목적 활용 시 조치
3.2	개인정보 보유 및 이용 시 보호조치	3.2.1	개인정보 현황관리
		3.2.2	개인정보 품질보장
		3.2.3	개인정보 표시제한 및 이용 시 보호조치
		3.2.4	이용자 단말기 접근 보호
		3.2.5	개인정보 목적 외 이용 및 제공
3.3	개인정보 제공 시 보호조치	3.3.1	개인정보 제3자 제공
		3.3.2	업무 위탁에 따른 정보주체 고지
		3.3.3	영업의 양수 등에 따른 개인정보의 이전
		3.3.4	개인정보의 국외 이전
3.4	개인정보 파기 시 보호조치	3.4.1	개인정보의 파기
		3.4.2	처리 목적 달성 후 보유 시 조치
		3.4.3	휴면 이용자 관리
3.5	정보주체 권리 보호	3.5.1	개인정보처리방침 공개
		3.5.2	정보주체 권리보장
		3.5.3	이용내역 통지

[표 7] 개인정보 처리 단계별 요구사항

위의 [표 7]에서 강조된 항목들은 개정 법령 내용을 반영하여 통합인증 체계에 추가 보완된 통제항목이다. 기존 인증에서 전혀 다루지 않았던 내용이 아니라 세부 점검사항으로 포함되어 있던 것을 독립 항목으로 격상시켜 그 중요성을 강조한 것으로 이해하면 된다. 특히, 기업의 비즈니스가 클라우드 시스템과 글로벌로 확장되는 추세에 따라 개인정보의 국외 이전([표 7]의 3.3.4)은 최근 더욱 심각한 이슈가 되고 있는 만큼 꼭 인증 취득 목적이 아니더라도 각별히 유의해야 하는 영역이다.

2018년 10월 30일 현재, 정보보호 및 개인정보보호 관리체계 통합인증(ISMS-P)의 개정 고시는 아직 발효되지 않았다. 또한 고시가 발효되더라도 고시 시행 후 6개월까지는 개정 이전의 기준에 따라 인증을 신청할 수 있고, 기존 인증 기준에 따라 인증을 취득한

경우에는 해당 인증의 유효기간까지 기존 인증기준으로 사후 심사를 받을 수 있다고 한다.

필자 사견으로는 이번 개정안은 아주 현실적이고 합리적인 기준으로 정비되었다. 기왕이면 이번 기회에 더 많은 기업과 기관이 통합된 ISMS-P 인증을 취득하여 더욱 체계적이고 안정적인 사업환경을 갖추기를 기대해본다.