# 정보보호 관리체계(ISMS) 인증 제도 해설서

(version 0.1)

2013. 2.


# 목 차

# 제1장 정보보호 관리체계(ISMS) 인증대상자 및 범위

## 1.1. 인증대상자 구분

o 기존 운영되던 정보보호 안전진단 제도('13.2.18 폐지)는 실효성 문제 등으로 폐지되고, 보다 높은 수준의 정보보호 관리체계 인증 제도로 일원화 되었으며 인증 의무대상자를 지정하여 운영하게 되었다.

o 정보보호 관리체계 인증대상자는 의무적으로 인증 심사를 받아야 하는 의무대상자와 그 외 스스로 인증 취득을 희망하는 자율신청기업으로 구분된다.

**< 의무대상자 >**

o 의무대상자는 ①정보통신망서비스를 제공하는 자(ISP), ②집적정보통신시설 사업자(IDC), ③연간 매출액 또는 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 자(주요 정보통신서비스 제공자) 이다.

**관련근거**

***정보통신망 이용촉진 및 정보보호 등에 관한 법률***

**제47조(정보보호 관리체계의 인증)**
② 정보통신서비스 제공자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다. <신설 2012.2.17>
1. 「전기통신사업법」 제6조제1항에 따른 허가를 받은 자로서 대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자
2. 집적정보통신시설 사업자
3. 연간 매출액 또는 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 자

- 의무대상자는 자발적으로 대상자 여부를 확인하여 인증을 취득해야 한다.
- 의무대상자가 인증을 받지 않을 경우, 1,000만원 이하의 과태료가 부과된다.

**관련근거**

***정보통신망 이용촉진 및 정보보호 등에 관한 법률***

**제76조(과태료)**
③ 다음 각 호의 어느 하나에 해당하는 자에게는 1천만원 이하의 과태료를 부과한다.
6. 제47조제2항을 위반하여 정보보호 관리체계 인증을 받지 아니한 자

o 의무대상자는 인증시기를 매년 1월 1일부터 12월 31일까지이며, 2013년도에는 개정 망법 시행일('13.2.18.) 기준으로 2013년 2월 18일부터 2013년 12월 31일까지 인증을 받아야 한다.

**관련근거**

***정보보호 관리체계 인증 등에 관한 고시***

**제14조(인증 의무대상자 범위)**
③ 인증 의무대상자는 매년 1월1일부터 12월31일까지 인증을 받아야 한다.

- 2013년 1월 1일부터 2월 17일까지 안전진단 수검을 받았을 경우에는 2013년도에 정보보호 관리체계 인증을 받은 것으로 인정한다.

**관련근거**

***정보통신망 이용촉진 및 정보보호 등에 관한 법률***

**부칙 제3조(정보보호 안전진단의 폐지에 따른 경과조치)**
이 법 시행 당시 종전의 규정에 따라 정보보호 안전진단을 받은 사업자는 정보보호 안전진단을 받은 해당 연도에는 제47조제2항의 개정규정에 따른 정보보호 관리체계 인증을 받은 사업자로 본다.

**< 자율신청기업 >**

o 의무대상자 외의 기업이 인증 취득을 희망할 경우, 자율적인 신청을 통한 인증 심사가 가능하다.

**관련근거**

***정보통신망 이용촉진 및 정보보호 등에 관한 법률***

**제47조(정보보호 관리체계의 인증)**
① 방송통신위원회는 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계(이하 "정보보호 관리체계"라 한다)를 수립·운영하고 있는 자에 대하여 제3항에 따른 기준에 적합한지에 관하여 인증을 할 수 있다.

## 1.2. 인증 의무대상자

### < 정보통신망서비스를 제공하는 자 >

o 정보통신망서비스를 제공하는 자(ISP)란「전기통신사업법」제6조제1항에 따른 기간통신사업 허가를 받은 자로서, 정보통신망 서비스 제공지역이 '서울특별시 및 모든 광역시'인 사업자를 말한다.

**관련근거**

***전기통신사업법***

**제6조(기간통신사업의 허가 등)**
① 기간통신사업을 경영하려는 자는 방송통신위원회의 허가를 받아야 한다.

**관련근거**

***정보통신망 이용촉진 및 정보보호 등에 관한 법률***

**제47조(정보보호 관리체계의 인증)**
② 정보통신서비스 제공자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다. <신설 2012.2.17>
1. 「전기통신사업법」 제6조제1항에 따른 허가를 받은 자로서 대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자

- 인터넷 서비스, 인터넷전화 서비스, 이동통신 서비스 등 정보통신망 서비스 지역 범위가 서울특별시 및 모든 광역시를 의미한다.

※ 모든 광역시 : 인천광역시, 대전광역시, 광주광역시, 대구광역시, 울산광역시, 부산광역시

**관련근거**

***정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령***

**제49조(정보보호 관리체계 인증 대상자의 범위)**
① 법 제47조제2항제1호에서 "대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자"란 서울특별시 및 모든 광역시에서 정보통신망서비스를 제공하는 자를 말한다.

- 다만, 전국망 서비스를 제공하지 않는 ISP 사업자의 경우에는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제47조제2항제3호에 따라 연간 매출액 또는 이용자 수 기준을 적용한다.

**< 집적정보통신시설 사업자 >**

o 집적정보통신시설 사업자(IDC)란 정보통신서비스 제공을 위해 자체적으로 시설을 구축하여 운영하는 자로서, 공간 임대서비스(Co-location) 또는 서버 임대(서버호스팅) 서비스 및 네트워크 서비스 등을 제공하는 사업자이다.

**관련근거**

***정보통신망 이용촉진 및 정보보호 등에 관한 법률***

**제47조(정보보호 관리체계의 인증)**
② 정보통신서비스 제공자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다.
2. 집적정보통신시설 사업자

- 다만, 타인에 의해 구축된 집적정보통신시설에 일부를 임대하여 집적정보통신시설 사업을 하는 자(VIDC)의 경우에는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제2항제3호에 따라 정보통신서비스 부문 전년도 매출액이 100억원 이상이거나 전년도 말 기준 직전 3개월간의 일일평균 이용자수가 100만명 이상일 경우에만 포함된다.

**관련근거**

***정보보호 관리체계 인증 등에 관한 고시***

**제49조(정보보호 관리체계 인증 대상자의 범위)**
② 법 제47조제2항제2호에 따라 정보보호 관리체계 인증을 받아야 하는 자 중 집적정보통신시설 사업자가 마련한 시설의 일부를 임대하여 집적정보통신시설 사업을 하는 자에 대하여는 영 제49조제2항의 기준을 준용한다.

**< 연간 매출액 또는 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 자 >**

o 연간 매출액 및 이용자 수 등 대통령령으로 정하는 기준에 해당하는 자는 쇼핑몰, 포털 등의 정보통신서비스를 제공하는 자를 말한다.

**관련근거**

***정보통신망 이용촉진 및 정보보호 등에 관한 법률***

**제47조(정보보호 관리체계의 인증)**
② 정보통신서비스 제공자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다.
3. 연간 매출액 또는 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 자

o 정보통신서비스 부문 전년도(법인의 경우에는 전 사업연도) 매출액이 100억원 이상인 자 또는 전년도 말 기준 3개월간 일일평균 이용자 수가 100만명 이상인 경우에 포함된다.

**관련근거**

***정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령***

**제49조(정보보호 관리체계 인증 대상자의 범위)**

② 법 제47조제2항제3호에서 "대통령령으로 정하는 기준에 해당하는 자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다.

1. 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 자
2. 전년도 말 기준 직전 3개월간의 일일평균 이용자 수가 100만명 이상인 자

**( 매출액 기준 : 전년도 매출액 100억 이상)**

- 정보통신서비스 부문 매출액은 정보통신서비스 제공을 통해 발생하는 연간 총 매출액의 합으로 산정하며, 여러가지 정보통신서비스를 제공할 경우에는 해당 서비스의 매출액을 모두 합하여 계산한다.

※ 매출액은 국세청 등에 신고된 금액으로 하며 이외에 내부적으로 결산자료 등을 마련하여 공인회계사 등의 검증을 거친 객관적 자료를 이용

※ 이러한 자료가 존재하지 않는다면 내부 회계자료에 대해 부서장의 승인을 거친 자료를 이용

[표1-1] 정보통신서비스 별 매출액 구분 (예시)

| 구분 | 해당 서비스 | 서비스 설명 | 정보통신서비스 부문 매출액 내역 |
|---|---|---|---|
| 신용카드검색(CCIS) 서비스 | 신용카드 | - 온라인상으로 신용카드의 도난분실, 한도초과, 연체 등을 실시간으로 확인하는 서비스를 제공하는 사업자 | - 카드조회수수료, 서비스매출, 회원수익매출, 부가수익 등 |
| 컴퓨터예약(CRS) 서비스 | 예약 | - 인터넷을 통해 서비스나 상품에 대한 예약서비스를 제공하는 사업자 | - 상품 및 서비스 판매매출, 수수료, 회원수익매출, 광고매출, 부가수익 등 |
| 전자문서교환(EDI) 서비스 | EDI | - 인터넷을 통해 전자문서교환서비스를 제공하는 사업자 | - 콘텐츠 판매매출, 수수료, 광고매출, 회원수익매출, 부가수익 등 |
| 전자지불(PG) 서비스 | PG | - 인터넷을 통해 지불중계역무를 제공하는 사업자 | - 지불중계수수료, 서비스매출, 회원수익매출, 부가수익 등 |
| 인터넷 포털 서비스 | 포털 | - 인터넷 유.무선 포털 사이트를 제공하는 사업자 | - 온라인 광고매출, 정보제공 수수료, 중계 수수료, 콘텐츠, 이용매출, 부가수익 등 |
| 인터넷 전자상거래 | 쇼핑몰 | - 쇼핑몰 역무를 제공하는 사업자 | - 판매 매출, 수수료, 광고매출, 부가수익 등 |
| 인터넷 방송 | 신문/방송 | - 인터넷을 통해 신문기사나 방송프로그램을 제공하는 사업자 | - 콘텐츠 판매매출, 수수료, 광고매출, 회원수익매출, 부가수익 등 |
| 인터넷 게임 | 게임 | - 인터넷게임서비스를 제공하는 사업자 | - 게임이용매출, 아이템 판매매출, 광고매출, 수수료, 부가수익 등 |

| | | | |
|---|---|---|---|
| 콘텐츠 제공 서비스 | 교육 | - 인터넷을 통한 교육서비스를 제공하는 사업자 | - 콘텐츠 이용매출, 수수료, 광고매출, 회원수익매출, 부가수익 등 |
| | 음악 | - 인터넷을 통한 실시간 음악 감상 서비스를 제공하는 사업자 | |
| | 기타 | - 인터넷을 통한 기타 콘텐츠제공 서비스를 제공하는 사업자 | |
| 유선방송 서비스 | Cable-SO | - 종합유선 방송서비스와 종합유선전송 서비스를 제공하는 사업자 | - 방송중계서비스 매출을 제외한 초고속인터넷서비스 매출액 등 |
| 기타 | | - 인터넷을 통한 기타 정보통신서비스를 제공하는 사업자 | |

※ 정보통신서비스 온라인 판매, 광고, 콘텐츠 이용 등으로 발생한 매출액과 부가수익, 수수료, 세금 등을 포함한 총 합계액

※ 정보통신서비스 제공을 통해 직.간접으로 발생하는 연간 국내.외 매출액

[표1-2] 쇼핑몰 판매 유형 별 매출액 구분 (예시)

| 판매 유형 | 정보통신서비스 부문에 해당되는 매출액 |
|---|---|
| 자체쇼핑몰 운영 | 자체쇼핑몰을 통한 제품 판매액 |
| 중개쇼핑몰 이용 | 해당사항 없음 |
| 중개쇼핑몰 운영 | 판매 중개수수료 + 입점료(해당하는 경우) |
| 자체쇼핑몰 운영 + 중개쇼핑몰 이용 | 자체쇼핑몰을 통한 제품판매액 |
| 중개쇼핑몰 운영 + 자체쇼핑몰 운영 | 판매 중개수수료 + 입점료(해당하는 경우) +<br>자체 쇼핑몰을 통한 제품 판매액 |
| 포인트 쇼핑몰 | 가맹점 수수료 + 고객 수수료 + 판매수수료 + 기프티콘 |

**( 이용자 수 : 전년도 말 기준 3개월 일일평균 이용자 수 100만명 이상 )**

- 일일 평균이용자는 일정 기간 동안의 주요 정보통신서비스 제공자의 홈페이지 방문자 수 등을 일평균으로 환산한 사용자 수를 말한다.

※ 실제 인간 이용자가 아닌 PC, 스마트폰 등이 네트워크 운영을 위해 이용하는 DNS query, 기지국 등록 등의 접속은 제외

※ 자체적으로 또는 공식적으로 이용자 수 확인이 어려운 경우에는 민간 통계기관 등의 데이터를 활용

※ 가능한 웹서버는 로그 분석도구 등을 이용하여 일일평균 이용자 수를 계산

## 1.3 인증 범위

**< 인증 범위 개념 >**

o 신청기관은 제공하는 주요 정보통신서비스를 포함하여 인증 범위를 설정해야 한다.

o 인증 범위는 신청기관이 제공하는 정보통신서비스를 기준으로, 해당 서비스에 포함되거나 관련 있는 자산(시스템, 설비, 시설 등), 조직 등을 모두 포함한다.

※ 해당 서비스와 관련이 없더라도, 그 서비스의 핵심정보자산 직.간접적으로 접근한다면 포함

※ 기존 정보보호 안전진단 대상자의 경우, 안전진단 범위와 동일함

**< 인증 범위 설정 >**

o 인증 범위를 설정하기 위해서는 신청기관이 제공하고 있는 주요 정보통신서비스를 분류하고, 해당 서비스를 위한 자산 및 조직을 모두 식별해야 한다.

o 인증 범위 대상으로 식별된 모든 자산 및 조직에 대해 「정보보호 관리체계 인증 등에 관한 고시」 제18조에 따른 [별표 6] '정보보호 관리체계 인증기준'을 준수하여 보호조치를 취해야 한다.

**( 정보통신망서비스 제공자의 경우 )**

- 해당 서비스 : 서울특별시 및 모든 광역시를 통한 인터넷 서비스
- 설비 : IP기반의 인터넷 연결을 위한 정보통신설비 및 관련 서비스를 제공하기 위한 정보통신설비

[표1-3] 정보통신망서비스 제공자 서비스 분류체계 (예시)

| 구분 | 서비스 | 기능 |
|---|---|---|
| 정보통신망서비스 제공자 | 기간통신 서비스 | 인터넷 접속 서비스<br>(초고속망 서비스) |
| | | 인터넷 전화 서비스(VOIP) |
| | | 이동통신서비스(셀룰라, PCS, 3G, 4G) |

**( 집적정보통신시설 사업자의 경우 )**

- 해당 서비스 : 정보통신서비스를 제공하는 고객의 위탁을 받아 컴퓨터 장치 등 정보시스템을 구성하는 장비를 일정한 공간에 집중하여 시설을 운영・관리하는 서비스(공간임대서비스, 서버호스팅, 네트워크 서비스 등)
- 설비 : 집적정보통신시설의 관리・운영 용도로 설치된 컴퓨터 장치 및 네트워크 장비 등의 정보통신설비

[표1-4] 집적정보통신시설 사업자 서비스 분류체계 (예시)

| 구분 | 서비스 | 기능 |
|---|---|---|
| 집적정보통신시설 사업자<br>및 재판매 사업자 | 부가통신<br>서비스 | 서버 호스팅 |
| | | 스토리지 호스팅 |
| | | 코로케이션(Co-location) |
| | | 네트워크 제공 서비스<br>(회선 임대 포함) |
| | | 보안관리 서비스 (제공 시) |
| | | 도메인관리 서비스 (제공 시) |

**( 연간 매출액 또는 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 자의 경우 )**

- 해당 서비스 : 인터넷 쇼핑몰, 포털, 게임, 예약, 종합유선방송서비스, 카드조회/지불중계, 신문・방송, 음악・교육, 전자문서교환서비스 등
- 설비 : 인터넷 쇼핑몰, 포털 등의 전자상거래업을 영위하기 위해서 필요한 정보통신설비

[표1-5] 정보통신서비스 제공자 서비스 분류체계 (예시)

| 구분 | 서비스 | 기능 | |
|---|---|---|---|
| 쇼핑몰 등 | 부가통신<br>서비스 | 신용카드 검색(CCIS) 서비스 | |
| | | 컴퓨터 예약(CRS) 서비스 | |
| | | 전자문서교환(EDI) 서비스 | |
| | | 전자지불서비스 | |
| | | 전화정보 서비스(ARS) | |
| | | 인터넷<br>정보제공<br>(유선, 무선) | 인터넷 포털 서비스 |
| | | | 인터넷 전자상거래(수수료) |
| | | | 인터넷 방송 |
| | | | 인터넷 게임 |
| | | 콘텐츠 제공 서비스 | |
| 유선방송 | 방송서비스 | 유선방송서비스 | |

# 제2장 정보보호 관리체계(ISMS) 인증 기준 및 절차

## 2.1 인증기준

o 정보보호 관리체계 인증 기준은 정보보호관리과정(5단계, 12개 통제항목), 과 정보보호대책(13개 분야, 92개 통제항목)의 두가지로 구성되어 있다.

[표2-1] 정보보호 관리체계 인증 기준

| 분야 | | 통제항목 수 | 세부점검항목 수 |
|---|---|---|---|
| 관리과정 (구축단계) | 1. 정보보호정책수립 및 범위설정 | 2 | 5 |
| | 2. 경영진 책임 및 조직구성 | 2 | 5 |
| | 3. 위험관리 | 3 | 11 |
| | 4. 정보보호대책 구현 | 2 | 3 |
| | 5. 사후관리 | 3 | 8 |
| 정보보호대책 | 1. 정보보호정책 | 6 | 12 |
| | 2. 정보보호조직 | 4 | 9 |
| | 3. 외부자 보안 | 3 | 6 |
| | 4. 정보자산분류 | 3 | 9 |
| | 5. 정보보호교육 | 4 | 10 |
| | 6. 인적보안 | 5 | 14 |
| | 7. 물리적 보안 | 9 | 20 |
| | 8. 시스템 개발보안 | 10 | 32 |
| | 9. 암호통제 | 2 | 5 |
| | 10. 접근통제 | 14 | 19 |
| | 11. 운영보안 | 22 | 67 |
| | 12. 침해사고 관리 | 7 | 19 |
| | 13. IT재해복구 | 3 | 7 |
| **총계** | | **104** | **261** |

o 개정된 정보통신망법('11.12)에 따라, 기존의 실효성이 낮은 점검항목을 통합하고, 최신 보안관리 기준을 반영하는 등 인증 심사 기준의 통제항목이 137개에서 104개로 변경되었다.

[표2-2] 정보보호 관리체계 인증 기준 주요 변경 내용

| 구분 | 주요 변경 내용 |
|---|---|
| 신규 항목<br>(14개) | - 경영진의 책임(예산 및 인력 지원, 의사결정 참여 등) 강화<br>- 정보보호최고책임자(CISO) 의무 지정 등 조직 구성 강화<br>- 최신기술 및 보안사고 반영 |
| 통합 또는 변경 항목<br>(128개 → 90개) | - 업무연속성관리, 물리적 보안, 전자거래보안, 검토, 모니터링 및 감사 영역 중심으로 중복 또는 유사항목 통합 |
| 삭제 항목<br>(9개) | - 적격심사, 물리적 위치 및 구조 조건, 입력 데이터/내부처리/출력 데이터 검증, 전자우편 등의 항목 실효성 부족(결함률 0)으로 삭제 |

**< 정보보호관리과정 인증 기준 >**

o 정보보호관리과정은 정보보호 관리체계 인증 심사 시 요구되는 필수 항목으로써 조직 내·외부 위협 요소의 변화 또는 새로운 취약성 발견 등에 대응하기 위하여 지속적으로 유지 관리되는 순환 주기의 형태를 가진다.

※ 5단계 관리주기 및 12개 통제항목으로 구성

[표2-3] 정보보호관리과정의 구체적인 요구사항

| 관리과정 | 요구사항 | 관련 문서 |
|---|---|---|
| 정보보호정책 수립<br>및 범위설정 | - 조직 전반에 걸친 상위 수준의 정보보호정책수립<br>- 정보보호 관리체계 범위 설정 | - 정보보호정책서<br>- 정보보호관리체계 범위서<br>- 정보자산 목록<br>(정보통신설비 목록)<br>- 네트워크 및 시스템 구성도 |
| 경영진 책임<br>및 조직구성 | - 정보보호를 수행하기 위한 조직 내 각 부문의 책임 설정<br>- 경영진 참여 가능하도록 보고 및 의사결정체계 수립 | - 정보보호조직도 |
| 위험관리 | - 위험관리 전략과 계획을 수립<br>- 위험 분석<br>- 대응이 필요한 위험 및 우선순위 결정<br>- 정보보호대책을 선택<br>- 구현 계획 수립 | - 위험관리지침서<br>- (00년)위험관리 계획서<br>- 위험 분석.평가 보고서<br>- 정보보호대책 명세서<br>- 정보보호계획서 |
| 정보보호대책 구현 | - 정보보호 대책을 효과적으로 구현<br>- 필요한 교육과 훈련을 진행함 | - 정보보호계획 이행경과 보고서 |
| 사후관리 | - 정보보호 관리체계를 운영하는 과정에서 상시적인 모니터링을 수행<br>- 정기적인 내부감사를 통해 정책 준수 상황을 확인<br>- 정보보호 관리체계를 재검토<br>- 관리 체계 개선 | - 정보보호 관리체계<br>내부감사보고서<br>- 사후관리 증적자료 |

**< 정보보호대책 인증 기준 >**

o 정보보호대책은 정보보호 관리체계 인증 심사 시 요구되는 선택 항목으로써 총 13개 분야 92개 통제항목으로 구성되어 있으며, 위험평가를 통하여 조직이 수용 가능한 위험수준을 달성할 수 있도록 통제항목을 선택한다.

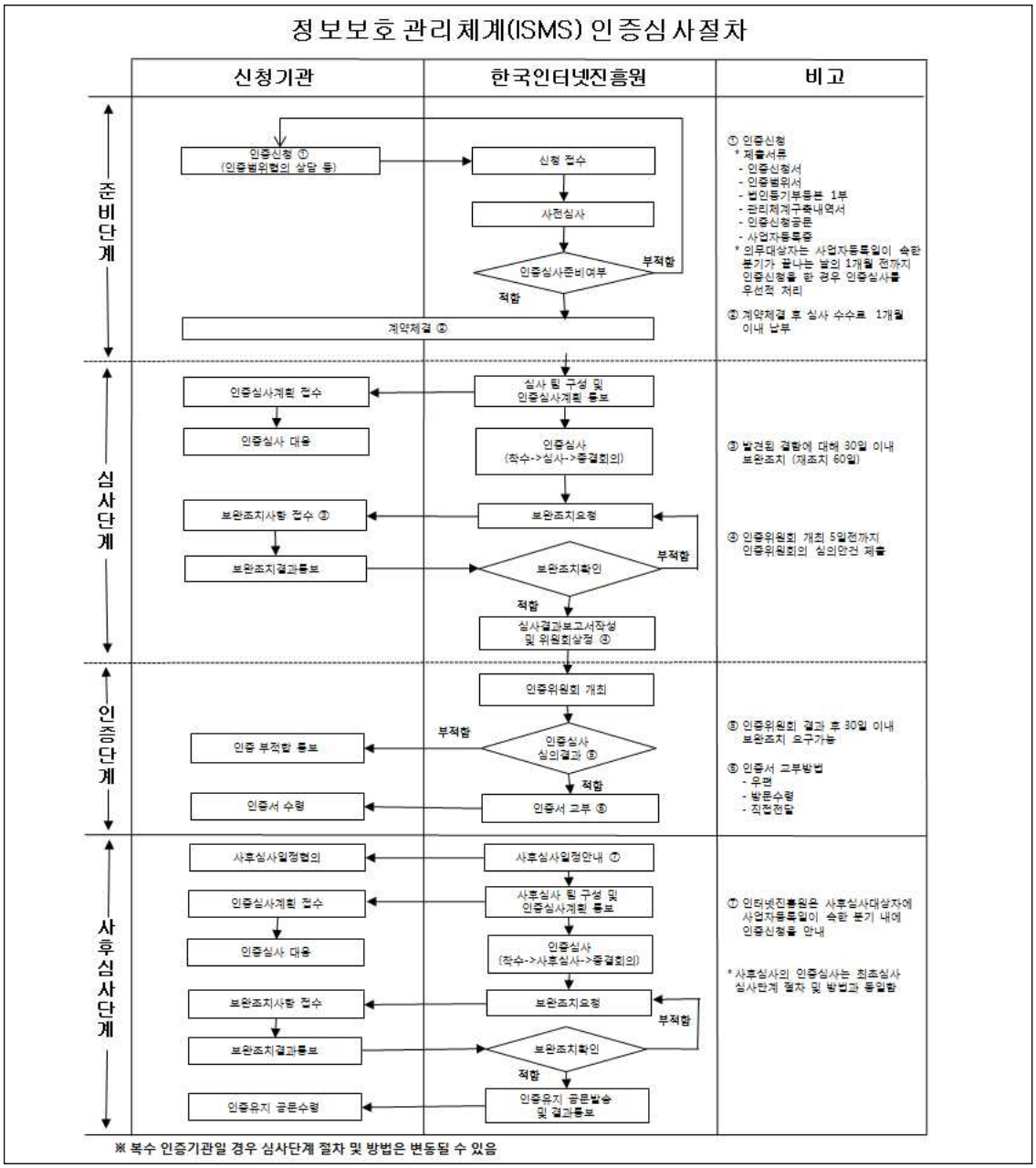
- 통제항목 중 정보보호대책 선택 시 선택하지 않은 항목은 식별되어 그 사유를 정보보호대책서에 명시하여야 한다.

[표2-4] 정보보호관리 통제사항

| 통제분야 | 통제목적 | 통제사항 수 |
|---|---|---|
| **정보보호정책** | - 정책의 승인 및 공표, 정책의 체계, 정책의 유지관리 | 6 |
| **정보보호 조직** | - 조직의 체계, 책임과 역할 | 4 |
| **외부자 보안** | - 계약 및 서비스수준협약 보안관리, 외부자 보안 실행관리 | 3 |
| **정보자산 분류** | - 정보자산의 조사 및 책임할당, 정보자산의 분류 및 취급 | 3 |
| **정보보호 교육 및 훈련** | - 교육 및 훈련 프로그램 수립, 시행 및 평가 | 4 |
| **인적 보안** | - 책임할당 및 규정화, 비밀유지, 적격심사 및 주요 직무 담당자 관리 | 5 |
| **물리적 보안** | - 물리적 정보보호대책, 데이터 센터 정보보호, 장비보호, 사무실 보호 | 9 |
| **시스템 개발 보안** | - 분석 및 설계 보안관리, 구현 및 이행 보안관리, 변경관리 | 10 |
| **암호 통제** | - 암호 정책 수립, 암호 사용, 키관리 | 2 |
| **접근통제** | - 접근통제 정책, 사용자 접근 관리, 접근통제 영역 | 14 |
| **운영관리** | - 운영 절차와 책임, 시스템 운영, 네트워크 운영, 매체 및 문서관리, 악성 소프트웨어 통제, 이동컴퓨팅 및 원격 작업 | 22 |
| **침해사고 관리** | - 대응 계획 및 체계, 대응 및 복구, 사후관리 | 7 |
| **IT재해복구** | - IT재해복구 체계 수립, 영향분석에 따른 복구대책 수립 시험 및 유지관리 | 3 |
| **합 계** | | 92 |

## 2.2 인증 절차

o 인증 심사 절차는 (그림2-1)와 같으며, 준비단계, 심사단계, 인증단계, 사후심사 단계로 나누어진다.




(그림2-1) 인증 절차도

## < 준비단계 >

### ( 인증 신청 )

- 신청기관은 인증 신청서 등의 제출서류와 함께 공문 접수(전자문서 포함)를 통하여 인증 신청을 해야 한다.

- 인증기관은 신청서류를 접수하고 접수증을 교부한 후 신청 서류의 기재사항을 검토하여 미비점이 있을 경우 보완을 요청할 수 있다.

※ 보완요청을 받은 신청기관은 요청받은 날로부터 10일 이내에 이를 보완하고 신청서류를 재구비하여 신청하여야 함

- 의무대상자의 인증신청 연말 쏠림현상을 방지하기 위해 회사 사업자 등록일이 속한 분기가 끝나기 1개월 전에 인증 신청을 한 경우, 인증심사를 우선적으로 처리하도록 한다.

※ 대상자는 사업자 등록일을 기준으로 3개월 전에 인증신청을 해야 함

**관련근거**

***정보보호 관리체계 인증 등에 관한 고시***

**제16조(인증의 신청 등)**

③ 인터넷진흥원 또는 인증기관은 제14조에 따른 인증 의무대상자가 사업자 등록일이 속한 분기가 끝나는 날의 1개월 전까지 인증 신청을 한 경우 인증심사를 우선적으로 처리할 수 있다.

- 인증 신청 시에는 정해진 신청서와 정보보호 관리체계 명세서를 제출하여야 하며 법인의 경우 법인 등기부 등본을 추가로 제출해야 한다.

**관련근거**

***정보통신망 이용 촉진 및 정보보호 등에 관한 법률 시행령***

**제47조(정보보호 관리체계 인증의 방법·절차·범위 등)**

① 법 제47조제1항 또는 제2항에 따라 정보보호 관리체계의 인증을 받으려는 자는 정보보호 관리체계 인증신청서(전자문서로 된 신청서를 포함한다)에 다음 각 호의 사항에 대한 설명이 포함된 정보보호 관리체계 명세서(전자문서를 포함한다)를 첨부하여 인터넷진흥원 또는 방송통신위원회가 지정한 기관(이하 "정보보호 관리체계 인증기관"이라 한다)에 제출하여야 한다.

1. 정보보호 관리체계의 범위
2. 정보보호 관리체계의 범위에 포함되어 있는 주요 정보통신설비의 목록과 시스템 구성도
3. 정보보호 관리체계를 수립·운영하는 방법과 절차
4. 정보보호 관리체계와 관련된 주요 문서의 목록
5. 정보보호 관리체계와 관련된 국내외 품질경영체제의 인증을 취득한 경우에는 그 명세

**( 사전 인증심사 )**

- 인증기관은 인증심사의 진행 여부를 판단하기 위하여 신청기관에 방문하여 인증심사 준비 여부를 확인하는 사전인증심사를 실시할 수 있다.
- 인증기관은 신청기관의 준비가 미비하여 인증심사를 진행할 수 없는 경우, 30일 이내에 이를 보완하도록 요청할 수 있다.
- 신청기관이 인증기관으로부터 보완을 요청받은 날로부터 30일 이내에 인증심사를 진행할 수 있도록 보완하지 못하는 경우, 인증기관은 신청기관의 인증신청을 무효화할 수 있다.

**( 계약 체결 )**

- 인증기관은 인증 신청서류 접수 여부 및 신청기관의 인증심사 준비현황을 파악한 후 신청기관과 인증심사 계약을 체결한다.
- 신청기관은 인증기관과 협의한 후 심사기간, 심사인원, 인증 수수료, 인증의 범위 등을 포함하는 인증심사계약을 체결하고, 인증심사 계약체결 후 인증심사 수수료를 1개월 이내에 납부해야 한다.
- 수수료 납부 방법은 인증 심사 계약 시 신청기관과 협의하여 일괄 또는 분할 납부 방법으로 조정할 수 있다.

**관련근거**

***정보보호 관리체계 인증 등에 관한 고시***

**제27조(수수료의 납부)**

① 신청기관은 최초심사, 사후심사 및 갱신심사 신청 시 수수료를 납부한다. 다만, 수수료 납부 방법(일괄 또는 분할)은 인증심사 계약 시 신청기관과 협의하여 조정할 수 있다.

② 신청기관은 인증심사 계약을 체결한 날로부터 1개월 이내에 인증 수수료를 인터넷진흥원 또는 인증기관에 납부하여야 한다.

- 중소기업법 제2조에 따른 중소기업이 인증을 신청하는 경우, 수수료 감면 혜택을 부여한다.

※ 수수료의 할인율에 대하여는 향후 공지 예정

**관련근거**

***정보보호 관리체계 인증 등에 관한 고시***

**제26조(수수료의 산정)**

② 인터넷진흥원 또는 인증기관은 제1항에 따라 산정된 인증 수수료를 공지하여야 한다. 다만,「중소기업기본법」제2조에 따른 중소기업이 인증을 신청하는 경우 수수료 감면 등 필요한 지원을 할 수 있다.

③ 인터넷진흥원 또는 인증기관은 신청기관의 인증범위가 정보보호 관련 타 인증과 중복될 경우 신청기관과 협의하여 수수료를 조정할 수 있다.

< 심사단계 >

( 인증심사팀 구성 및 인증 심사계획 통보 )

- 인증기관에서 인증심사를 위한 인증심사팀 구성 시 인증심사 품질 제고 및 책임성 강화를 위해 심사팀장은 인증(심사)기관의 소속직원 중 심사원 이상으로 선정한다.

- 인증심사의 공정성, 객관성 확보를 위해 인증심사팀 구성 시 인증대상기관의 컨설팅 참여직원은 배제한다.

**관련근거**

***정보보호 관리체계 인증 등에 관한 고시***

**제19조(인증심사팀 구성)**

② 인증심사팀 구성 시 심사팀장은 인터넷진흥원 또는 인증기관 소속의 심사원 이상으로 선정하여야 한다.

③ 신청기관의 정보보호 관리체계 인증을 위한 컨설팅에 참여한 인증심사원 또는 신청기관의 소속직원은 인증심사팀의 구성원에서 배제하여야 한다.

- 인증기관은 인증 수수료가 납부된 날로부터 10일 내에 인증심사 기간, 심사팀 구성 등을 명시한 인증심사 계획서를 작성하여 신청 기관에 통보한다.

[표2-5] 심사계획 통보 내용

| 구분 | 내용 |
|---|---|
| 심사 일정 | - 착수회의<br>- 서면심사<br>- 현장심사<br>- 주요 시스템(업무지원 시스템, 정보보호시스템 등) 시연<br>- 현장심사 및 현장확인 (담당자 인터뷰 및 현장실사)<br>- 결과 확인 및 종결회의 |
| 심사팀 구성 | - 심사팀장<br>- 심사팀 인원 |
| 심사 준비사항 | - 심사 공간 및 비품<br>- 인증심사 관련 자료 및 이행 증적자료심사 지원<br>- 담당자 지정 |

( 인증심사 대응 )

- 신청기관은 원활한 인증심사를 위하여 통보받은 계획에 따라 표3-5 기재된 내용으로 심사 준비를 해야 한다.

- 신청기관은 인증심사를 수행하기 위하여 필요한 장소와 세부 문서, 운영기록 등의 자료를 제공하고 담당자 면담을 주선하는 등 필요한 협조를 제공해야 한다.

[표2-6] 심사 준비사항

| 구분 | 내용 |
|---|---|
| 심사 공간 | - 회의실<br>- 빔프로젝트 |
| 비품 | - 전화<br>- 네트워크 회선<br>- 화이트 보드 |
| 인증심사 관련 자료<br>및 이행 증적자료 | - 상위 정책서, 직무기술서, 정보보호계획서, 정보보호 관리체계 범위정의서, 담당자 연락처 (사본 각 4부)<br>- 정보보호대책명세서 (원본 1부, 사본 3부)<br>※ 운영현황/관련문서/증적자료는 상세하게 작성<br>- 각종 지침/절차/매뉴얼 (원본 1부, 사본 2부)<br>- 위험분석 보고서, 내부 감사 결과보고서, 교육계획서 등 각종 보고서/계획서 (원본 1부, 사본 2부)<br>- 각종 점검 및 관리대장 등 이행증적자료 (원본 1부) |
| 심사 지원<br>담당자 지정 | - 조직도 및 연락처 등<br>- 관련문서 열람 및 관계자 면담 등에 대한 협조 |

**( 인증심사 )**

- 인증심사는 관리체계의 인증심사 기준인 관리과정과 관리적, 기술적, 물리적 보호조치로 구성된 정보보호대책 통제항목이 적절히 이행되고 있는지 확인한다.
- 인증심사 수행은 서면심사와 현장심사를 병행하여 실시한다.
- 서면심사에서는 인증 신청기관의 관리체계 관련 문서인 정책과 지침, 절차 등 내부규정을 갖추고 있는지, 해당 내부규정이 인증기준에서 제시하고 있는 요구사항(통제항목)을 충족하고 있는지 심사한다.

  ※ 각종 문서 및 이행 증적자료 검토, 보호대책 적용 여부 확인 등의 방법으로 관리적 요소를 심사
- 현장심사에서는 문서에서 명시한 통제사항들이 실행되고 있는지 확인하고, 서면심사에서 발견된 문제점의 원인을 현장실사를 통해 기술적 대책, 물리적 대책이 이행되고 있는지 확인한다.

※ 이행에 따른 증적자료 또는 전자적 기록 점검 등

**관련근거**

***정보보호 관리체계 인증 등에 관한 고시***

**제20조(인증심사 방법 및 보완조치)**

① 인증심사는 신청기관을 방문하여 서면심사와 현장심사를 병행한다.

② 서면심사는 인증기준에 적합한지에 대하여 정보보호 관리체계 구축·운영 관련 정보보호 정책, 지침, 절차 및 이행의 증적자료 검토, 정보보호대책 적용 여부 확인 등의 방법으로 관리적 요소를 심사한다.

③ 현장심사는 서면심사의 결과와 기술적·물리적 보호대책 이행 여부를 확인하기 위하여 담당자 면담, 관련 시스템 확인 및 취약점 점검 등의 방법으로 기술적 요소를 심사한다.

- 인증심사 후 심사원들은 서면심사 및 현장심사를 통하여 도출된 문제점에 대해 결함보고서를 작성하고, 최종적으로 신청 기관의 담당자들과의 "결과확인 회의"를 통하여 결함 내용을 확인한다.
- 인증기관은 인증심사에서 알게 된 비밀을 타인에게 누설하거나 업무 외 목적으로 사용하지 않는다.

**( 보완조치 요청 )**

- 인증기관은 정보보호 관리체계 결함보고서를 신청기관에 전달하고, 결함보고서에 기술한 결함에 대해 신청기관에게 보완조치 요청서를 작성하여 통보한다.
- 신청기관은 보완조치 요청을 받은 날로부터 30일 이내에 보완조치를 수행하고 정보보호 관리체계 보완조치 내역서를 작성하여 인증기관에 제출해야 한다.
- 인증기관은 신청기관이 제출한 결과에 대하여 현장 확인이 필요하다고 판단될 경우 현장을 방문하여 결과를 확인할 수 있다.
- 인증기관이나 인증위원회에서 보완조치결과가 미흡하다고 판단할 경우, 재조치를 요구할 수 있으며 추가적으로 60일 이내에서 보완조치 기간을 연장할 수 있다.
- 신청기관이 추가적으로 보완조치에 대한 요청을 받은 날로부터 60일 이내에 보완조치에 대한 결과물을 제출하지 못하는 경우, 보완이 이루어지지 않은 것으로 판단한다.

**관련근거**

***정보보호 관리체계 인증 등에 관한 고시***

**제20조(인증심사 방법 및 보완조치)**

④ 인터넷진흥원 또는 인증기관은 인증심사에서 발견된 결함에 대해 최대 90일(재조치 요구 60일 포함) 이내에 보완조치를 완료하도록 신청기관에게 요청할 수 있다.

⑤ 인터넷진흥원 또는 인증기관은 인증위원회 심의결과에 따라 30일 이내에 보완조치를 요구할 수 있다.

( 심사 결과보고서 작성 및 인증위원회 상정 )

- 인증심사원은 서면심사 및 기술심사를 통하여 발견한 결함에 대한 보완조치의 결과 확인이 이루어지면, 심사 결과보고서를 작성한다.
- 인증심사팀이 수행한 심사결과에 대한 객관성과 공정성 확보 및 일정수준 이상의 품질 확보를 위하여 한국인터넷진흥원의 장이 구성·운영하는 인증위원회에 심사 결과보고서를 상정한다.

**관련근거**

*정보보호 관리체계 인증 등에 관한 고시*

**제22조(인증위원회의 운영)**

① 인터넷진흥원 또는 인증기관의 장은 인증위원회의 심의안건을 검토하여 위원회 개최 5일 전까지 인증위원회에 제출한다.

② 인증위원회 위원장은 제21조제1항 각 호의 사항에 대한 심의·의결 결과를 인터넷진흥원 또는 인증기관의 장에게 제출한다.

< 인증단계 >

( 인증심사 결과 심의·의결 )

- 위원장은 인증위원회의 업무를 통할하며 위원회를 대표하여 정보보호 관리체계 인증기관의 장에게 인증심사원이 실시한 인증심사 결과가 인증심사기준에 적합한지 여부를 심의하고 그 결과를 제출한다.
- 정보보호 관리체계 인증위원회를 운영함으로써 심사와 심의·의결을 분리하여 부실 논란을 없애고 실효성을 확보한다.

**관련근거**

*정보보호 관리체계 인증 등에 관한 고시*

**제20조(인증심사 방법 및 보완조치)**

① 법 제47조제5항에 따라 인터넷진흥원 또는 인증기관의 장은 다음 각 호의 사항을 심의·의결하기 위하여 인증위원회를 설치·운영하여야 한다.

1. 최초심사 또는 갱신심사 결과가 인증기준에 적합한지 여부
2. 사후심사 결과 법 제47조제8항 각 호에 해당하는 사유를 발견한 경우에 그 결과의 적합성 여부
3. 그 밖에 정보보호 관리체계 인증과 관련하여 위원장이 필요하다고 인정하는 사항

② 인증위원회는 5인 이상 10인 이내의 위원으로 구성하되, 위원은 정보보호전문가, 정보시스템감리사, 기술사, 대학교수 등 정보보호분야에 학식과 경험이 있는 자 중에서 인터넷진흥원 또는 인증기관의 장이 위촉하며, 위원장은 위원 중에서 호선한다.

③ 위원장은 인증위원회의 업무를 통할하며 위원회를 대표한다.

( 인증서 발급 )

- 인증위원회는 인증기관에서 수행한 인증심사결과(관리체계 인증 기준 적합 여부 등)를 심의·의결하고, 그 결과에 따라 인증기관은 인증서 발급한다.

**관련근거**

*정보보호 관리체계 인증 등에 관한 고시*

**제23조(인증서 발급)**

인터넷진흥원 또는 인증기관의 장은 제22조제1항에 따라 인증위원회의 심의·의결 결과를 제출받은 때에는 신청기관의 정보보호 관리체계가 이 고시에서 정한 인증기준에 적합하다고 판단된 경우 별지 제11호서식의 정보보호 관리체계 인증서를 발급하여야 한다.

## < 사후심사단계 >

( 사후심사 )

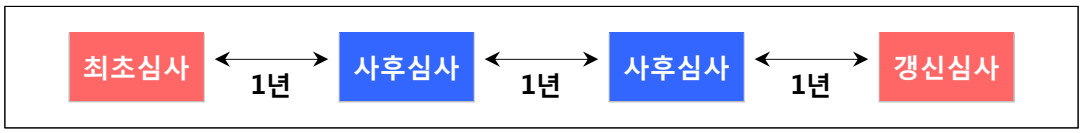
- 정보보호 관리체계 인증을 받게 되면 그 인증은 3년간 유효하고 관리체계의 지속적인 유지운영을 위해 1년에 한번 이상 관리체계를 점검하는 사후관리를 해야 한다.

**관련근거**

*정보보호 관리체계 인증 등에 관한 고시*

**제47조(정보보호 관리체계의 인증)**

⑥ 한국인터넷진흥원 및 정보보호 관리체계 인증기관은 정보보호 관리체계의 실효성 제고를 위하여 연 1회 이상 사후관리를 실시하고 그 결과를 방송통신위원회에 통보하여야 한다.




(그림2-2) 인증 심사 주기

## 2.3 인증 고려사항

### < 소요기간 >

o 의무대상 기업들은 단계별 소요기간을 확인하여 인증 취득을 준비해야 한다.

- 인증 절차는「준비 → 심사 → 인증」단계로 이루어지며, 인증 소요기간은 내부 준비부터 인증까지 약 6개월 이상이 소요되므로, 연내 취득을 위해서는 일정을 역산하여 조기에 인증 준비를 하는 것이 필요하다.
- 정보보호 관리체계 인증 신청을 위해서는 정보보호 관리체계 구축 후 최소 2개월 이상 운영하여야 한다.

**관련근거**

***정보보호 관리체계 인증 등에 관한 고시***

**제15조(신청기관의 사전 준비사항)**
신청기관은 정보보호 관리체계 인증을 신청하기 전에 인증기준에 따른 정보보호 관리체계를 구축하여 최소 2개월 이상 운영하여야 한다.

[표2-7] 인증 절차 및 소요기간표 (예시)

| 인증절차 내용 | ① 준비 | | | ② 심사 | | | | | ③ 인증 | |
|---|---|---|---|---|---|---|---|---|---|---|
| | ISMS 구축 | ISMS 운영 | 인증 신청 | 심사 준비 | 인증 심사 | 보완 조치 | 조치 확인 | 심사 결과보고서 작성 | 인증위원회 심의 준비 | 인증위원회 심의 및 인증서 교부 |
| 소요시간 | 1~3개월 | 2개월 (최소) | 5일 | 30일 | 5일 | 30일 | 5일 | 5일 | 30일 | 2일 |

- 인증시기는 매년 1월1일부터 12월 31일까지이므로, 의무대상자는 인증서 부여날짜 기준으로 최소 2개월 전에 인증심사가 완료되어야 한다.
- 특정 시기에 인증심사가 집중되는 경우, 사업자 등록일을 기준으로 인증심사가 우선 처리될 수 있으므로 조기에 인증 신청을 할 필요가 있다.

**관련근거**

***정보보호 관리체계 인증 등에 관한 고시***

**제16조(인증의 신청 등)**
③ 인터넷진흥원 또는 인증기관은 제14조에 따른 인증 의무대상자가 사업자 등록일이 속한 분기가 끝나는 날의 1개월 전까지 인증 신청을 한 경우 인증심사를 우선적으로 처리할 수 있다.

### < 심사 유형 >

o 정보보호 관리체계 인증심사 종류는 최초심사, 사후심사, 갱신심사로 이루어진다.

**관련근거**

***정보보호 관리체계 인증 등에 관한 고시***

**제2조(용어의 정의)**

9. “최초심사”란 처음으로 인증을 신청하거나 인증의 범위에 중요한 변경이 있어서 다시 인증을 신청한 때 실시하는 인증심사를 말한다.
10. “사후심사”란 정보보호 관리체계 인증(인증이 갱신된 경우를 포함한다)을 받고난 후 매년 사후관리를 위하여 실시하는 인증심사를 말한다.
11. “갱신심사”란 유효기간 만료로 다시 인증을 신청한 때 실시하는 인증심사를 말한다.

[표2-8] 인증심사 종류

| 심사 구분 | 내용 |
|---|---|
| 최초심사 | - 처음으로 인증을 신청하거나 인증의 범위에 중요한 변경이 있어서 다시 인증을 신청한 때 실시하는 인증심사<br>※ 인증취득기관의 인증 취소, 기업 결합.분할 등의 경우, 최초심사로 다시 신청하고 인증위원회에서 심의하여 인증 부여 |
| 사후심사 | - 정보보호 관리체계 인증(인증이 갱신된 경우를 포함)을 받고난 후 매년 사후관리를 위하여 실시하는 인증심사<br>※ 인증취득기관의 상호.주소.대표자 변경, 관리체계 범위의 일부 변경 등의 경우, 사후심사로 진행 |
| 갱신심사 | - 인증취득기관이 운영중인 정보보호 관리체계 인증의 유효기간 만료로 유효기간 연장을 위해 다시 인증을 신청한 때 실시하는 인증심사 |