소방청훈령 제445호

[시행 2025. 12. 4.] [소방청 훈령 제445호] [발령 2025. 12. 4.]

소방청 사이버안전센터 운영규정 일부개정훈령안

소방청 사이버안전센터 운영규정 일부를 다음과 같이 개정한다.

제27조 중 "2025년 12월 31일"을 "2028년 12월 31일"로 한다.

부 칙

이 훈령은 발령한 날부터 시행한다.

신·구조문대비표

현 행	개 정 안
제27조(유효기간) 이 훈령은 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 이 훈령을 발령한 후의 법령이나 현실 여건의 변화 등을 검토하여야 하는 2025년 12월 31일까지 효력을 가진다.	제27조(유효기간) ---------- ---------- ---------- ---------- ---------- -- 2028년 12월 31일-------- -------.

소방청 사이버안전센터 운영규정

제1장 총 칙

제1조(목적) 이 규정은 「정보통신기반 보호법」 제16조, 「국가사이버안전관리규정」 제4조 및 제10조의2에 따라 소방청 사이버안전센터의 운영 등에 관한 사항을 규정함을 목적으로 한다.

제2조(용어의 정의) ① 이 규정에서 사용하는 용어의 정의는 다음과 같다.

1. "정보통신망"이라 함은 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 활용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저정·검색·송수신하는 정보통신체제를 말한다.
2. "사이버공격"이란 해킹·컴퓨터바이러스·서비스 방해 등 전자적 수단에 의하여 정보통신망을 불법침입·교란·마비·파괴하거나, 정보를 위조·변조·절취·훼손·유출하는 일체의 공격행위를 말한다.
3. "보안관제"란 전자문서·전자기록물 또는 정보통신망을 대상으로 하는 사이버공격 정보를 수집·분석·전파하는 일련의 활동을 말한다.
4. "사이버안전센터"란 일정한 수준 이상의 시설 및 장비와 이를 운영하기 위한 전문인력을 갖추고 보안관제 업무를 수행하는 조직을 말

한다.

5. "보안관제 대상기관"이란 소방청과 그 소속기관 및 산하기관 중 사이버안전센터가 보안관제서비스를 제공하는 기관을 말한다.

② 이 지침에서 사용하는 용어는 제1항에서 정하는 것을 제외하고는 「전자정부법」, 「정보통신기반 보호법」, 「보안업무규정」, 「국가사이버안전관리규정」, 「국가정보보안기본지침」 등 관계 법령 및 규정이 정하는 바에 따른다.

제3조(적용범위) 이 규정은 소방청과 그 소속기관 및 다른 법률에 의하여 업무상 소방청장의 지도·감독을 받는 기관·단체(이하 "산하기관"이라 한다)에 적용한다.

제4조(보안관제 목표) 보안관제 목표는 보안관제 대상기관의 정보시스템 및 정보통신망에 대한 사이버공격 정보를 실시간 수집·분석하고 전파함으로써 사이버공격으로 인한 피해의 발생 또는 확산을 방지하는 데 있다.

제2장 사이버안전센터의 설치 및 운영

제5조(사이버안전센터 설치) ① 소방청장은 본청과 그 소속기관 및 산하기관을 대상으로 하는 사이버공격으로 인한 피해의 발생 또는 확산을 방지하기 위하여 보안관제 업무 등을 수행하는 사이버안전센터를 설치할 수 있다.

② 제1항에 따라 설치한 사이버안전센터의 명칭은 '소방청 사이버안전

센터(이하 "센터"라 한다)'라 하고, 영문은 NFA-CSC(National Fire Agency, Cyber Security Center)라 한다.

제6조(조직 및 기능) ① 센터는 소방청 정보보호업무 담당부서에서 운영하며, 센터장은 비상임으로서 소방청 정보통신과장이 된다.

② 센터장 업무를 보조하기 위하여 센터운영에 필요한 전담직원을 배치하여야 한다.

③ 센터의 보안관제 업무를 위해 필요한 경우 과학기술정보통신부장관이 지정하는 보안관제전문업체에 업무를 위탁하여 운영할 수 있다.

④ 센터에서 수행하는 업무는 다음 각 호와 같다.

1. 사이버안전대책 수립·시행
2. 센터 관련 규정 및 지침 등의 제·개정
3. 사이버위협 실시간 관제·분석 및 예·경보 전파
4. 사이버공격 발생 시 초동대응, 지휘·보고, 원인규명 및 재발방지 조치 등
5. 사이버 위기대응훈련 및 사이버 위기대응매뉴얼 수립·시행
6. 사이버위협으로 인하여 발생한 사고의 조사 및 복구조치 지원
7. 기타 사이버위협 대응에 필요한 보안관제 대상기관과의 협력 등에 관한 사항

제7조(근무방법 등) ① 센터의 근무체계는 「소방공무원 근무규칙」 제2조제8호에 따른 상시근무체계를 유지한다.

② 관제요원의 교대근무방식은 4조2교대를 원칙으로 하되 필요한 경

우 센터장이 별도로 정하여 운영할 수 있다.

③ 국가정보원의 사이버 위기경보 발령 시에는 경보단계별로 근무인원 등을 보강하여 운영할 수 있다.

제8조(교육·훈련) ① 센터장은 보안관제요원의 능력 배양을 위해 교육·훈련계획을 수립하여 실시할 수 있다.

② 센터장은 사이버공격에 대한 대응능력 향상을 위해 정기적으로 대응훈련을 실시할 수 있다. 이 경우 국가사이버안전센터의 대응훈련과 합동으로 할 수 있다.

제9조(기록관리 등) 센터장은 평시에 보안관제상황을 일일·주간·월간 단위로 관제상황보고서(별지 제1호서식)를 작성하여 관리하고 필요 시 소방청장에게 수시로 보고하여야 한다.

제10조(통합보안관제시스템 구축·운영) 소방청장은 보안관제 업무를 효율적으로 수행하기 위하여 소방청과 그 소속기관 및 산하기관을 포괄하는 통합보안관제시스템을 구축·운영할 수 있다.

제3장 센터의 보안관제 업무

제11조(정보수집) ① 센터장은 보안관제 대상기관에 대한 사이버공격 정보를 수집할 수 있다.

② 센터장은 제1항의 업무 수행을 위하여 보안관제 대상기관의 정보통신망에 사이버공격 정보를 수집하는 장치를 설치·운용할 수 있다.

제12조(초동조치) ① 센터장은 보안관제 대상기관으로부터 수집된 사

이버공격 정보를 분석하여 정보시스템 및 정보통신망의 피해유무를 확인하고, 이를 해당 기관의 장에게 전파하여야 한다.

② 센터장은 보안관제 대상기관의 정보시스템 및 정보통신망에 대한 사이버공격 피해가 확인된 경우에는 해당 기관의 장에게 공격IP 차단, 로그자료 보존, 정보통신망에서 피해시스템 분리 등 초동조치를 요청할 수 있으며, 해당 기관은 특별한 사유가 없는 한 이에 협조하여야 한다.

제13조(정보분석 · 공유) ① 센터장은 사이버공격의 분석과 피해확산 방지대책 강구 등을 위하여 피해기관의 장에게 피해시스템과 그 사용자 등에 관하여 필요한 정보제공을 요청할 수 있으며, 해당 기관은 특별한 사유가 없는 한 이에 협조하여야 한다.

② 센터장은 피해시스템에 대한 정보분석을 통해 재발방지대책을 수립하여 이를 피해기관의 장에게 제공할 수 있다.

③ 센터장은 관련 법령에 저촉되지 않는 범위 내에서 수집·분석한 사이버 공격 정보(자체처리한 경미한 사고포함)를 국가사이버안전센터장 및 관계기관의 장에게 제공할 수 있다.

④ 센터장은 별지 제2호 서식에 따라 사이버안전센터의 운영현황을 작성하여 매년 10월말까지 국가사이버안전센터장에게 통보하여야 한다. 다만, 운영현황을 이미 제출한 경우에는 변동사항이 있을 경우에 한하여 통보한다.

제14조(사이버침해사고 이관) 센터장은 보안관제 과정에서 수집된 사

이버공격 정보가 다른 중앙행정기관의 업무와 연관되어 있을 경우에는 해당 중앙행정기관의 장에게 별지 제3호 서식에 따라 사이버공격 정보를 신속하게 이관하여야 한다.

제15조(사고보고) ① 보안관제 대상기관은 사이버공격으로 인한 사고 발생 또는 징후를 발견한 경우에는 피해를 최소화하는 조치를 취하고 지체 없이 그 사실을 센터에 보고하여야 한다.

② 센터장은 사이버공격으로 인한 사고의 발생 또는 징후를 발견하거나 제1항에 따른 보고를 받은 때에는 보안관제 대상기관 등에 사고복구 및 피해의 확산방지에 필요한 조치를 요청하고 그 사실을 지체 없이 국가정보원장에게 통보하여야 한다.

제16조(사고조사 및 처리) ① 센터장은 보안관제 대상기관의 사이버공격으로 인하여 발생한 사고에 대하여 그 원인 분석을 위한 조사를 실시할 수 있다. 다만, 경미한 사고라고 판단되는 경우에는 보안관제 대상기관이 자체적으로 조사하게 할 수 있으며, 이 경우 보안관제 대상기관은 사고개요 및 조치내용 등 관련사항을 파악 즉시 센터에 보고하여야 한다.

② 센터장은 제1항에 따른 조사결과를 국가정보원장에게 통보하여야 한다.

③ 센터장은 사이버공격으로 인한 피해가 심각하다고 판단되는 경우에는 국가사이버안전센터, 보안관제 대상기관 등 유관기관과 협의하여 합동조사 및 복구지원팀을 구성·운영할 수 있다.

제17조(상황 전파 등) ① 센터장은 사이버공격을 탐지·분석한 결과 그 피해가 확산될 우려가 있다고 판단되는 경우에는 유관기관, 소속기관 및 사용자 등에게 이를 통보하여야 한다.

② 센터장은 국가사이버안전센터에서 발령하는 국가사이버 위기경보 상황 등을 상시 확인하고 관련 상황을 보안관제 대상기관에 전파하여야 한다.

③ 제2항의 규정에 의하여 위기경보 상황 등이 발령·전파되었을 때에는 센터장과 보안관제 대상기관의 장은 위기경보 상황 등에 적절한 계획을 수립하여 이행하여야 한다.

④ 보안관제 대상기관의 장은 제3항에 따라 수립한 계획 및 이행결과를 센터에 보고하여야 한다.

제18조(보안관제서비스 신청) ① 산하기관의 장은 「국가사이버안전관리규정」 제4조 및 제9조에 따라 정보통신망 보호를 위하여 센터장에게 사이버 보안관제서비스(이하 "서비스"라 한다)를 신청할 수 있다. 다만, 별도의 보안관제센터를 구축하여 자체적으로 보안관제 업무를 수행하는 경우에는 그러하지 아니한다.

② 제1항에 따라 서비스를 신청하고자 하는 경우에는 센터장에게 서비스 신청서(별지 제4호 서식)를 제출하여야 한다.

③ 센터장은 제2항에 따른 서비스 신청을 받으면 보안관제에 필요한 제반사항의 구비 여부를 검토하고 승인 여부를 신청일로부터 15일 이내에 신청기관에 통보하여야 한다.

제19조(보안관제회의) 센터장은 사이버안전 업무를 효율적으로 수행하기 위하여 정기 또는 수시로 보안관제 대상기관이 참석하는 회의를 개최할 수 있다.

제20조(비상연락체계) ① 센터장은 사이버공격 정보의 신속한 전파 및 대응을 위하여 센터와 보안관제 대상기관 간 비상연락체계를 구축·운영하여야 한다.

② 보안관제 대상기관의 장은 제1항의 규정에 따른 비상연락체계를 최초 구축하거나 변동이 발생한 경우 비상연락망(별지 제5호 서식)을 작성하여 센터장에게 통보하여야 한다.

제4장 보안관리

제21조(시설보안) ① 센터장은 센터를 보호구역으로 설정하여 관리하여야 하며, 접근 권한이 없는 자에 대한 접근 통제 및 감시를 효율적으로 수행할 수 있는 독립된 공간에 설치·운영하여야 한다.

② 센터장은 센터 출입인가자의 범위를 설정하고 비인가자에 대한 접근 통제 대책을 마련하여야 한다.

③ 센터장은 외부로부터 시찰·견학 요청을 받은 경우에는 핵심시설에 대한 사진촬영을 제한하고 보안관제와 관련된 세부 정보의 제공을 금지하는 등 출입 인원에 대한 보안대책을 마련하여야 한다.

제22조(인원보안) ① 센터장은 외부 인력을 보안관제 업무에 활용하고자 하는 경우에는 다음 각 호의 보안대책을 수립·시행하여야 한다.

1. 계약서에 보안 주의사항과 위반 시 책임한계 명시

2. 보안서약서 징구(별지 제6호 서식)

3. 보안관리 책임자 지정

4. 업무와 무관한 정보통신망 접속 금지 등 업무범위 명확화

5. 업무와 무관한 정보통신실 등 중요시설에 대한 출입 제한

6. 기타 필요하다고 인정되는 보안대책

② 센터장은 외부 인력에 대하여 매월 1회 이상 정기 또는 수시로 보안점검과 보안교육을 실시하여야 한다.

제23조(문서보안) ① 보안관제 업무를 수행하는 PC·서버 등 정보시스템에 대외비 또는 비밀을 보관·유통하여서는 아니 된다.

② 센터 내에 설치한 인터넷 접속이 가능한 PC·서버 등 정보시스템에 보안관제 대상기관의 업무와 관련된 문서를 보관·유통하여서는 아니 된다.

③ 누구든지 보안관제 업무와 관련된 세부적인 사항이 포함된 문서를 대외에 임의로 공개하거나 공개된 장소에 무단으로 방치하여서는 아니 된다.

제24조(비밀유지) ① 센터에 근무하는 자 또는 근무하였던 자는 업무수행 중 알게 된 정보 및 자료 등을 센터의 운영 용도 이외에 다른 목적으로 사용하거나 누설하여서는 아니 된다.

② 보안관제 대상기관은 센터장이 통보하는 보안관제 관련 사항을 외부에 임의로 공개·누설 또는 제공하여서는 아니 된다.

③ 제1항 및 제2항과 관련하여 센터에서 근무하는 자 및 보안관제 대상기관의 정보보호업무 담당자는 비밀유지서약서(별지 제7호 서식)를 센터장에게 제출하여야 한다.

제5장 보칙

제25조(운영지침) 소속기관 및 산하기관에서 사이버안전센터를 설치·운영하려고 하는 경우 이 훈령에 저촉되지 아니하는 범위 내에서 소관 부문에 대한 세부 운영지침을 정할 수 있다.

제26조(준용) 이 지침에 명시되지 않은 사항은 다음 각 호의 관련 법령 및 규정에 따른다.

1. 「전자정부법」 및 같은 법 시행령
2. 「정보통신기반 보호법」 및 같은 법 시행령
3. 「보안업무규정 시행규칙」
4. 「국가사이버안전관리규정」
5. 「국가정보보안기본지침」
6. 그 밖의 관계 법령

제27조(유효기간) 이 훈령은 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 이 훈령을 발령한 후의 법령이나 현실 여건의 변화 등을 검토하여야 하는 2028년 12월 31일까지 효력을 가진다.