



고용노동 사이버안전센터 운영규정

[시행 2020. 10. 16.] [고용노동부훈령 제334호, 2020. 10. 16., 전부개정]

고용노동부(정보화기획팀), 044-202-7104

제1장 총칙

제1조(목적) 이 규정은 「정보통신기반보호법」 및 「국가사이버안전관리규정」에 따라 고용노동부의 보안관제센터 운영에 관한 사항을 규정함을 목적으로 한다.

제2조(명칭) 고용노동부의 보안관제센터의 명칭은 "고용노동 사이버안전센터"(이하 "센터"라 한다)라 하고, 영문 표기는 Employment and Labor Cyber Security Center(약칭은 ELCSC)라 한다.

제3조(적용 범위) 이 규정은 고용노동부와 소속기관 및 법령에 의하여 고용노동부장관의 지도·감독을 받는 산하기관 등 센터에 가입한 참가기관에 적용한다.

제4조(용어의 정의) ① 이 훈령에서 사용하는 용어의 뜻은 다음 각 호와 같다.

1. "정보통신망"이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 말한다.
2. "사이버공격"이라 함은 해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스방해 등 전자적 수단을 사용하여 정보통신망을 불법침입·교란·마비·파괴하거나 정보를 위조·변조·훼손·절취하는 행위를 말한다.
3. "보안관제"라 함은 사이버공격 정보를 실시간으로 탐지 및 분석, 대응하는 일련의 활동을 말한다.
4. "보안진단"이라 함은 정보통신망을 대상으로 취약점을 진단하는 제반활동을 말한다.
5. "탐지규칙정보"라 함은 사이버공격정보를 탐지하여 보안관제업무에 활용할 수 있는 기술정보를 말한다.
6. "인터넷 주소"라 함은 인터넷에서 국제표준방식에 의하여 일정한 통신규약에 따라 특정 정보시스템을 식별하여 접근할 수 있도록 하는 숫자·문자·부호 또는 이들의 조합으로 구성되는 정보체계로서 다음 각 목의 어느 하나에 해당하는 것을 말한다.
 - 가. 인터넷 프로토콜(IP) 주소: 인터넷에서 컴퓨터 및 정보통신설비가 인식하도록 만들어진 것
 - 나. 도메인(domain) 이름: 인터넷에서 인터넷 프로토콜 주소를 사람이 기억하기 쉽도록 하기 위하여 만들어진 것
 - 다. 그 밖에 「인터넷주소자원에 관한 법률」 제2조제1호다목에 따라 정하는 것
7. "사이버안전센터"란 일정한 수준의 시설 및 장비와 이를 운영하기 위한 전문 또는 전문인력을 갖추고 보안관제업무를 수행하는 조직을 말한다.
8. "사이버안전시스템"이라 함은 실시간 사이버공격에 관한 정보를 탐지·수집하여 보안관제 및 보안진단 업무를 수행하기 위한 정보시스템을 말한다.

9. "보안관제 전문기업"이라 함은 과학기술정보통신부 장관이 고시하는 「보안관제 전문기업 지정 등에 관한 공고」제2조2항에 따른 보안관제 전문기업을 말한다.
 10. "사이버안전서비스"라 함은 국가사이버안전관리규정 제4조에 따른 사이버안전을 위해 센터의 24시간 보안관제, 침해사고 분석 및 대응, 보안 진단 등을 말한다.
 11. "참가기관"이란 센터에 가입하여 사이버안전서비스를 받는 기관을 말한다.
- ② 이 규정에서 사용하는 용어는 제1항에서 정하는 것을 제외하고는 「전자정부법」, 「정보통신기반보호법」, 「국가정보보안기본지침」, 「국가사이버안전관리규정」, 「보안업무규정」, 「보안업무규정시행세칙」등 관계 법령이 정하는 바에 따른다.

제2장 센터

제5조(조직 및 기능) ① 센터장은 센터업무를 총괄하고 고용노동부 정책기획관으로 하며, 센터는 정보보안 업무를 담당하는 부서에서 운영한다.

② 정보보안 업무를 담당하는 부서에서는 고용노동부 및 참가기관에 대한 다음 각 호의 업무를 수행한다.

1. 센터 업무 기획 및 발전방향 수립
2. 사이버안전 관련 규정 및 제도 운용
3. 보안관제, 침해사고대응, 보안진단 업무에 대한 총괄
4. 정보통신기반시설에 대한 보호계획 수립 및 관리기관 지도·감독
5. 정보보호·사이버안전 관련 교육 및 훈련 기획
6. 정보보호·사이버안전 관련 국내외 회의, 정보교류, 학술행사 참여
7. 협의회 관련 업무

③ 센터는 고용노동부 및 참가기관에 사이버안전서비스를 제공하며 세부업무는 다음 각 호와 같다.

1. 사이버공격의 실시간 관제·분석
2. 사이버공격으로 발생한 사고의 조사 및 복구 지원
3. 정보통신망 보안진단 및 이행점검
4. 사이버안전시스템 운영
5. 정보보호·사이버안전 교육 및 훈련 서비스 제공
6. 정보보호·사이버안전 관련 국내·외 기술 연구·조사 및 각종 간행물 발간
7. 그 밖에 협의회에서 정한 업무

제6조(협의회 운영) 센터장은 다음 각 호의 사항을 심의·의결하기 위하여 고용노동 사이버안전센터 운영 협의회(이하 "협의회"라 한다)를 운영할 수 있다.

1. 센터 관련 규정 및 제도 마련
2. 센터 관련 중요 정책사항 결정

3. 센터 관련 정보 공유 및 발전방향 수립
4. 그 밖에 의장이 필요하다고 판단한 사항

제7조(협의회 구성) ① 협의회 의장은 정책기획관으로 하고, 간사는 정보보안 업무를 담당하는 부서의 장이 되며, 위원은 참가기관의 정보보안책임관으로 구성한다.

- ② 협의회 의장은 제5조제2항 및 제3항의 각 호의 업무에 대하여 심의·결정 등 필요하다고 인정되는 경우에는 협의회를 소집할 수 있다.
- ③ 협의회는 재적위원 과반수 이상의 출석으로 개최하고, 출석위원 과반수 이상의 찬성으로 의결한다.
- ④ 협의회 의장은 제3항에도 불구하고 협의회를 소집하기 곤란하거나 긴급을 요하는 경우에는 서면회의를 개최할 수 있다.

제8조(사이버안전시스템 구축·운영) ① 센터장은 사이버안전서비스를 제공하기 위한 시스템(이하 "사이버안전시스템"이라 한다)을 구축·운영하여야 한다.

- ② 센터장은 센터운영에 필요한 인력 및 예산 확보 방안을 마련하여야 한다.

제9조(센터시설운영) ① 센터장은 접근 통제 및 감시를 효율적으로 수행할 수 있는 독립된 공간에 센터를 구축·운영하여야 하며 제한구역으로 설정하여 관리하여야 한다.

- ② 센터장은 보안관제 업무를 수행하기 위한 정보통신망을 별도로 구축·운영하여야 하며 다른 정보통신망(인터넷 포함)과 분리·운영하여야 한다.

제10조(예·경보 전파) ① 센터장은 사이버공격에 대한 관심·주의·경계·심각등 수준별 예·경보가 발령된 경우에는 즉시 그 내용을 참가기관의 장에게 전파하여야 한다.

- ② 제1항에 따라 예·경보가 발령·전파되었을 때에는 참가기관의 장은 예·경보 수준에 맞는 적절한 계획을 수립하여 이행하여야 한다.

제11조(공격정보 탐지·수집) ① 센터장은 참가기관에 대한 사이버공격에 관한 정보를 탐지·수집하여야 한다.

- ② 센터장은 제1항의 업무를 수행하기 위하여 참가기관의 장과 협의하여 사이버공격에 관한 정보를 실시간 수집하는 장비 및 소프트웨어를 참가기관의 정보통신망에 설치·운영하거나 탐지규칙정보를 제공하여 관련 정보를 실시간 수집할 수 있다.
- ③ 센터장은 사이버공격에 관한 정보를 탐지·수집하기 위하여 불가피한 경우 다음 각 호에 해당하는 정보를 처리할 수 있다.
 1. 공격 주체 및 피해자를 식별하기 위한 IP 주소, 전자우편 주소, 정보통신서비스 이용자 계정 정보, 피해자의 성명 및 연락처
 2. 피해 시스템 관련 로그기록
 3. 사이버공격의 방법 및 피해 확인에 필요한 정보

제12조(탐지규칙정보 개발 및 배포) ① 센터장은 센터 자체 개발 및 국가사이버안전센터에서 배포한 탐지규칙정보를 활용하여 보안관제업무에 활용 할 수 있다.

- ② 센터장은 긴급성이 요구되는 사이버공격에 대한 탐지규칙정보를 참가기관에게 적시에 배포하여야 한다.
- ③ 센터장은 제1항에 따른 탐지규칙정보를 「공공기관의 정보공개에 관한 법률」 제9조제1항에 따른 비공개 대상 정보 및 「국가정보자료관리규정」 제2조제1호에 따른 국가정보자료로서 취급·관리하여야 한다.
- ④ 탐지규칙정보는 다음 각 호에 해당하는 방법으로 관리하고 매월 1회 이상 보안관리 실태를 점검하여야 한다.
 1. 암호화 저장·전송
 2. 인터넷을 통한 평문 송·수신 금지
 3. 인터넷 등 외부유출 금지
 4. 탐지규칙정보 관리시스템의 원격 접속 금지
- ⑤ 탐지규칙정보를 배포받은 참가기관의 장은 탐지규칙정보가 유출된 경우 즉시 그 사실을 센터장에게 통보하여야 한다.

제13조(초동 조치) 참가기관의 장은 사이버공격으로 인한 피해 최소화 및 확산 방지를 위하여 다음 각 호의 사항을 포함한 조치를 취하여야 한다.

1. 사이버공격 경유지(사이버공격에 악용되거나 악용될 우려가 있는 웹사이트 주소, IP주소, 전자우편 주소를 말한다) 및 공격 IP주소 차단
2. 피해 시스템을 정보통신망으로부터 분리하거나 악성프로그램의 동작을 정지시키는 조치
3. 사고원인 규명을 위한 피해 시스템 및 로그 기록의 보존

제14조(사고보고 및 복구) ① 참가기관의 장은 사이버공격으로 사고발생 또는 징후를 발견한 경우에 피해를 최소화 하는 조치를 하고 그 사실을 지체 없이 센터장에게 보고하여야 한다.

- ② 센터장은 사이버공격으로 사고발생 또는 징후를 발견하거나 제1항에 따른 보고를 받은 경우에 참가기관의 장에게 사고복구 및 피해의 확산방지에 필요한 조치를 지시할 수 있으며, 해당 기관은 이에 따라야 한다.

제15조(사고조사 및 처리) ① 센터장은 사이버공격으로 발생한 사고발생에 대하여 그 원인 분석을 위한 조사를 실시할 수 있다. 다만, 경미한 상황인 경우에는 피해 기관의 장이 자체적으로 조사하게 할 수 있으며, 이 경우 피해 기관의 장은 사고 개요 및 조치내용 등 관련 사항을 센터장에게 즉시 보고하여야 한다.

- ② 센터장은 사이버공격으로 피해가 심각하다고 판단되는 경우에 국가사이버안전센터, 피해 기관 등과 협의하여 합동조사 및 복구지원팀을 구성·운영할 수 있다.
- ③ 센터장은 사이버공격으로 인한 사고의 원인 분석 및 재발 방지를 위하여 피해 기관의 장에게 각 호의 해당하는 자료 제출을 요청할 수 있다.
 1. 공격 주체 및 피해자를 식별하기 위한 IP 주소, 전자우편 주소, 정보통신서비스 이용자 계정 정보, 피해자의 성명 및 연락처
 2. 사이버공격에 사용된 악성프로그램 및 공격 과정에서 생성·변경 또는 복제된 디지털정보
 3. 공격 주체가 절취한 디지털정보
 4. 공격 주체의 행위가 기록된 내역 또는 로그기록

- ④ 제3항에 따른 자료 제출을 요청받은 피해 기관의 장은 관계 법규에 저촉되지 않는 범위 내에서 해당 자료를 제출하여야 하며 센터장은 제출 받은 자료를 사이버공격에 대한 예방 및 대응과 관련한 목적으로만 사용하여야 한다.
- ⑤ 피해 기관의 장은 사고 원인을 규명할 때까지 피해 시스템에 대한 증거를 보존하고 임의로 관련 자료를 삭제하거나 포맷하여서는 아니 된다.
- ⑥ 민간 클라우드컴퓨팅서비스의 공공 전용 클라우드를 이용하는 기관의 장은 공공 전용 클라우드에서 사고가 발생한 경우 센터장과 합동으로 조사반을 구성하여 클라우드컴퓨팅서비스제공자에 대하여 계약의 범위 내에서 자료의 보존 및 제출요구, 현장 조사 등 필요한 조치를 취하여야 한다.

제16조(재발방지대책) ① 센터장은 제15조에 따른 조사 결과 및 재발방지를 위한 보안조치 사항을 피해 참가기관의 장에게 통보하여야 한다.

- ② 제1항에 따라 조사 결과를 통보받은 기관의 장은 관계법규에 따른 개선대책 수립·시행 등 필요한 조치를 취하여야 한다.

제17조(지도점검) ① 센터장은 참가기관의 정보보호 및 사이버안전과 관련한 운영현황 등을 지도·점검할 수 있다.

- ② 참가기관은 제1항에서 지도·점검한 결과에 대하여 필요한 조치를 성실하게 하여야 한다.

제18조(관제업무의 위탁) ① 센터장은 사이버침해의 탐지·분석·대응 등 보안관제 업무의 원활한 수행을 위하여 보안 관제 전문기업에 사이버안전서비스 운영업무를 위탁할 수 있다.

- ② 제1항에 따른 사이버안전서비스 운영업무를 위탁받은 기업(이하 "수탁기관"이라 한다)은 사이버공격에 대하여 24시간 탐지분석·대응할 수 있는 근무체계를 구축·운영하여야 한다.
- ③ 수탁기관은 보안관제 인력이 근무를 교대할 때에 근무 중에 발생한 주요 상황을 명확하게 인계인수하도록 하여 업무의 연속성을 유지하여야 한다.

제19조(비상연락체계) ① 센터장은 사이버공격에 대한 신속한 탐지 및 대응을 위하여 참가기관 및 국가사이버안전 센터 등 유관기관의 비상연락망을 현행화하여야 한다.

- ② 참가기관의 장은 제1항에 따른 비상연락망 변동시 센터장에게 즉시 통보하여야 한다.

제20조(교육) ① 센터장은 센터 업무담당자에 대한 교육 계획을 수립·시행하여야 한다.

- ② 센터장은 센터 업무담당자가 매년 10시간 이상 보안관제 관련 교육을 이수하도록 하여야 한다.

제3장 참가기관

제21조(가입 및 탈퇴) ① 「국가사이버안전관리규정」제4조 및 제9조에 따라 고용노동부 산하 공공기관은 정보보호 및 사이버안전을 위하여 센터에 가입하여야 한다.

- ② 고용노동부 소관 업무를 법령에 의하여 위임·위탁받아 수행하는 기관은 정보보호 및 사이버안전을 위하여 센터에 가입할 수 있다.

- ③ 제2항에 따라 센터에 신규로 가입하려는 기관은 참가신청서(별지 제1호서식)를 제출하여 센터장의 승인을 받아야 한다.
- ④ 제2항에 따라 가입한 참가기관이 센터를 탈퇴하려는 경우 탈퇴신청서(별지 제2호서식)를 제출하여 센터장의 승인을 받아야 한다.
- ⑤ 센터장은 제2항에 따라 가입한 참가기관이 제22조제3항에 따라 정보보호 및 사이버안전을 위한 의무를 성실히 수행하지 않는다고 판단될 경우 해당 기관을 탈퇴시킬 수 있다.

제22조(권리와 의무) ① 참가기관은 가입과 동시에 제2항 및 제3항의 권리와 의무를 갖게 되며, 협의회에 참여할 수 있다.

② 참가기관의 권리는 다음 각 호와 같다.

1. 센터로부터 사이버안전서비스를 제공받을 권리
2. 협의회에 출석하여 의견을 제시하고 회의에 참여할 권리

③ 참가기관의 의무는 다음 각 호와 같다.

1. 센터의 규칙 및 결정사항 준수
2. 참가기관의 사이버안전 전담조직·인력 및 비상연락망 제공
3. 해킹·바이러스 등 침해사고 발생내역 및 대응 관련 자료 제공
4. 관제서비스 대상 장비현황 등 정보기술 설비현황 자료 제공
5. 침해사고 발생시 조사 및 처리가 필요한 경우 네트워크·시스템 관리자 및 유지보수업체 인원 등이 참여하여 센터와 공동대응

제23조(전담 조직 및 인력) 참가기관의 장은 소관 정보통신망의 사이버안전 업무를 전담할 조직 및 전문 인력을 확보하는 등 필요한 조치를 하여야 한다.

제4장 비밀유지

제24조(비밀유지) ① 센터에 종사하는 사람 또는 종사하였던 사람은 그 직무상 알게 된 정보 및 자료 등을 센터운영 목적 외 사용하거나 누설하여서는 아니된다. 다만, 다음 각 호의 경우에는 센터장의 승인을 거쳐 공개·사용할 수 있다.

1. 해당 참가기관의 동의가 있는 경우
2. 통계 및 학술목적 등으로 특정기관이 나타나지 않도록 가공·사용할 경우
3. 법령에서 정한 규정에 따라 적법한 절차를 거쳐 정보를 제공하는 경우

② 참가기관은 센터 가입을 통해 알게 된 각종 정보 및 자료 등을 센터장의 허가 없이 사용하거나 누설하여서는 아니 되며, 탈퇴 이후에도 동일하게 적용된다. 다만 해당 기관 관련 정보 또는 공개가 가능한 자료의 활용에 대해서는 그러하지 아니하다.

③ 제1항 및 제2항에 따라 센터에 종사하는 사람, 참가기관 센터 업무 담당자는 비밀유지 서약서(별지 제3호서식)를 제출하여야 한다.

제5장 보칙

제25조(재검토기한) 이 훈령은 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 2020년 1월 1일 기준으로 매3년이 되는 시점(매 3년째의 12월 31일까지를 말한다)마다 법령이나 현실여건의 변화 등 그 타당성을 검토하여 이 규정의 개선 등의 조치를 하여야 한다.

부칙 <제334호,2020.10.16.>

이 규정은 발령한 날로부터 시행한다.