제정 2017. 02. 02.

국가기록원 훈령 제 125호

국가기록원 사이버안전센터 운영지침

국가기록원 사이버안전센터 운영에 관한 지침을 다음과 같이 제정한다.

제1장 총칙

제1조(목적) 이 지침은 「정보통신기반보호법」 제16조, 「국가사이버안전관리규정」 제4조에 따라, 국가기록원의 보안관제센터 또는 사이버안전센터 운영에 관한 사항을 정함을 목적으로 한다.

제2조(명칭) 본 센터의 명칭은 '국가기록원 사이버안전센터'라 하고 영문명은 NAK-CSC(National Archives of Korea, Cyber Security Center)라 한다.

제3조(적용범위) 이 지침은 다른 법령에 규정된 것을 제외하고 국가기록원과 그 소속기관에 대하여 적용한다.

제4조(정의) ① 이 지침에서 사용하는 용어의 정의는 다음과 같다.

1. "정보통신망"이란 「전기통신기본법」 제2조 제2호에 따른 전기통신설비를 활용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송수신하는 정보통신체제를 말한다.

2. "사이버위협"이란 해킹·컴퓨터바이러스·서비스방해 등 전자적 수단에 의하여 정보통신망을 불법침입·교란·마비·파괴하거나, 정보를 위조·변조·절취·훼손·유출하는 일체의 위협행위를 말한다.

3. "보안관제"란 전자기록물 또는 정보통신망을 대상으로 하는 사이버위협 정보를 수집·분석·전파하는 일련의 활동을 말한다.

4. "사이버안전센터"(이하 "센터"라 한다)란 일정한 수준 이상의 시설 및 장비와 이를 운영하기 위한 전문 인력을 갖추고 보안관제 업무를 수행하는 조직을 말한다.

5. "보안관제 대상기관"은 국가기록원 및 소속기관 중 센터가 사이버위협 예방 및 대응 서비스 등을 제공하는 기관을 말한다.

② 이 지침에서 사용하는 용어는 제1항에서 정하는 것을 제외하고는 「보안업무규정」(대통령훈령), 「국가정보보안지침」,「국가사이버안전관리규정」(대통령훈령)등 관계규정이 정하는 바에 따른다.

제5조(보안관제 목표) 국가기록원과 소속기관의 정보통신망에 대한 사이버위협 정보를 수집·분석하고 대응함으로써 사이버위협으로 인한 피해의 발생 또는 확산을 방지 하는데 있다.

제 2장 사이버안전센터의 설치 및 운영

제6조(조직 및 기능) ① 센터는 국가기록원 정보보호업무 담당부서에서 운영하며, 센터장은 국가기록원 정보보호 업무 담당부서의 장으로 한다.

② 센터에서 수행하는 업무는 다음 각 호와 같다.

1. 센터 업무 기획에 관한 사항

2. 센터 관련 규정 및 지침 등의 제·개정

3. 센터 운영에 관한 사항

4. 사이버위협 실시간 관제·분석 및 예·경보 전파

5. 사이버위협으로 인하여 발생한 사고의 조사 및 복구조치 지원

6. 기타 사이버위협 대응에 필요한 보안관제 대상기관과의 협력 등에 관한 사항

제7조(통합보안관제시스템 구축·운영) ① 센터장은 보안관제 업무를 효율적으로 수행하기 위하여 소관 사이버안전센터의 관제현황을 종합적으로 모니터링 할 수 있는 통합보안관제시스템을 구축·운영할 수 있다.

② 센터장은 필요한 경우 미래창조과학부장관이 지정하는 보안관제 전문업체의 인력을 활용하여 보안관제 업무를 수행하도록 할 수 있다.

제 3장 센터보안관제 업무

제8조(정보수집) ① 센터장은 보안관제 대상기관에 대한 사이버위협 정보를 수집할 수 있다.

② 센터장은 제 1항의 업무 수행에 필요한 정보 수집 장치를 보안관제 대상기관에 설치·운영할 수 있다.

제9조(사이버위기 예·경보) 센터장은 국가사이버안전센터에서 발령하는 국가사이버 위기경보 상황 등을 상시적으로 확인하고 관련 상황을 보안관제 대상기관에 신속히 전파하여야 한다.

제10조(사고보고 및 복구) ① 보안관제 대상기관은 사이버위협으로 인한 사고의 발생 또는 징후를 발견한 경우에 피해를 최소화하는 조치를 취하고 지체 없이 그 사실을 센터에 보고하여야 한다.

② 센터는 사이버위협으로 인한 사고의 발생 또는 징후를 발견하거나 제1항에 따른 보고를 받은 때에는 보안관제 대상기관 등에 사고복구 및 피해의 확산 방지에 필요한 조치를 요청할 수 있으며, 요청받은 해당기관은 특별한 사유가 없는 한 이에 협조하여야 한다.

제11조(사고조사 및 처리) ① 센터장은 보안관제 대상기관의 사이버위협으로 인하여 발생한 사고에 대하여 그 원인 분석을 위한 조사를 실시할 수 있다. 다만, 경미한 사고라고 판단되는 경우에는 보안관제 대상기관 등이 자체적으로 조사하게 할 수 있으며, 이 경우 보안관제 대상기관 등은 사고개요 및 조치내용 등 관련사항을 파악 즉시 센터에 보고하여야 한다.

② 사이버위협으로 인한 피해가 심각하다고 판단되는 경우에는 보안관제 대상기관 등 유관기관과 협의하여 합동조사 및 복구지원팀을 구성·운영할 수 있다.

제 4장 보안관리

제12조(센터 보안운영) ① 센터장은 센터는 보호구역으로 설정하여 관리하여야 하며 접근권한이 없는 자에 대한 접근 통제 및 감시를 효율적으로 수행할 수 있는 독립된 공간에 설치·운영하여야 한다.

② 센터장은 센터에서 사용되는 PC, 서버 등의 정보시스템 및 구성도, 보안관제 산출물 등의 문서 보안에 대하여 관리하여야 한다.

제13조(비상연락망) 센터장은 사이버위협에 대한 신속한 탐지 및 대응을 위

하여 국가기록원 보안관제 대상기관 등 유관기관과의 비상연락망을 현행화 하여야 한다.

제14조(비밀엄수) 보안관제 업무에 종사하거나 종사하였던 자는 그 직무상 알게 된 비밀을 타인에게 누설하거나 직무상 목적 외에 이를 사용하여서는 아니 된다.

제 5장 보칙

제 15조(운영지침) 국가기록원 소속기관에서 사이버안전센터를 설치·운영하려고 할 때에는 이 훈령에 저촉되지 아니하는 범위 내에서 소관 부문에 대한 세부 운영지침을 정할 수 있다.

제 16조(위임규정) 사이버안전센터의 효율적·체계적 운영 및 관리를 위하여 본 운영지침에 근거한 세부적인 운영규정 및 매뉴얼을 정할 수 있다.

제 6장 부칙

이 훈령은 발령한 날로부터 시행한다.