KISC 종합상황실 운영 지침

제정 2020.08.28

제1장 총칙

제1조(목적) 이 지침은 한국인터넷진흥원 KISC 종합상황실(이하“상황실”이라 한다) 운영에 필요한 사항을 규정함을 목적으로 한다.

제2조(적용범위) 상황실의 구성 및 운영 등은 법령과 다른 규정·규칙에 따로 정한 경우를 제외하고는 이 지침이 정하는 바에 따른다.

제3조(용어의 정의) ① 이 지침에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. "정보통신망"이란 「전기통신기본법」 제2조 제2호에 따른 전기통신설비를 활용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송수신 하는 정보통신매체를 말한다.
2. "사이버공격"이란 해킹·컴퓨터바이러스·서비스방해 등 전자적 수단에 의하여 정보통신망을 불법침입·교란·마비·파괴하거나, 전자문서·전자기록물을 위조·변조·절취·훼손하는 일체의 공격행위를 말한다.
3. “악성IP·도메인”이란 악성코드·악성앱 유포지, 피싱, DDoS 등 사이버 공격에 악용되는 IP와 도메인을 말한다.
4. “팀장”은 상황실 운영 업무를 하는 팀의 책임자를 말한다.

② 이 규정에서 사용하는 용어는 제1항에서 정하는 것을 제외하고는「국가 정보보안 기본지침」, 「국가사이버안전관리규정」 등 관계법령이 정하는 바에 따른다.

제2장 상황실 인력 운영

제4조(상황실 운영 방식) ① 상황실은 서울청사(연중 상시) 상황실과 나주본원(평일 주간) 상황실로 이중화하여 운영한다.

② 제1항에 의한 상황실 근무자의 주간 근무시간은 09:00부터 18:00까지, 야간 근무시간은 18:00부터 익일 09:00까지 하는 것을 원칙으로 하며, 근무 시작 시간 전 출근하여 상호 협

의된 방법으로 업무 인수인계를 하여야 한다.

③ 서울청사 상황실 근무는 팀장의 승인하에 편성된 근무 명령에 의하며 상황실 근무 최소 인원은 서울청사 3명, 나주본원 1명으로 한다.

④ 제2항과 제3항의 규정에도 불구하고 상황실의 근무시간 및 근무인원은 다음 각 호의 경우 조정하여 운영할 수 있다.

1. 사이버위기경보단계 상향 조정과 같은 특별한 상황이 있는 경우
2. 재난이 발생하였거나 발생할 우려가 있는 경우 또는 이에 준하는 상황이라고 판단되는 경우
3. 그 밖에 예외상황 발생 시 또는 효율적인 상황실 운영을 위하여 인력 조정이 필요하다고 판단되는 경우

⑤ 근무 인수인계시에는 그 내용을 팀장에게 보고하여야 한다.

⑥ 업무 태만 및 고의, 중과실 등으로 상황실 운영에 지장을 초래하거나 상황실 업무에 부적격하다고 판단되는 경우 상황실 근무에서 제외할 수 있다.

⑦ 상황실 근무자의 복무에 관한 사항 중 이 지침에서 정하지 않은 사항에 대하여는 원내 관련 규정을 준용한다.

제5조(근무자 구성) ① 상황실 근무자는 원내 침해대응 관련 업무를 수행하는 팀의 직원으로 구성하며 1명의 조장과 2명 이상의 조원을 둔다.

② 조장은 상황실 근무자 중 책임연구원 이상의 직원으로 구성하는 것을 원칙으로 하되 필요시 팀장의 판단하에 선임연구원 이하 직원 중에서도 임명 가능하다.

제6조(근무자 기본 조건) 24시간 365일 침해사고 탐지·예방·대응 등을 종합적으로 수행하는 상황실 업무 특성에 따라 근무자는 다음 각 호의 조건을 충족하여야 한다.

1. 정보보호 관련 자격증 소지자 또는 관련 업무 경험자
2. 원활한 의사소통 능력 보유자
3. 고혈압, 당뇨, 전염병 등 건강상의 문제가 없는 자

제7조(결원충원) ① 상황실 근무 인력 결원에 대한 충원은 원내 관련 규정을 준용한다.

② 단, 24시간 365일 교대 근무 형태로 운영되는 상황실 업무 특성상 신규 인력 충원 시 인사팀 등 관련 부서와 협의하여 제5조를 충족하는 적합한 인력이 투입될 수 있도록 하여야 한다

제8조(근무 기간) 상황실 근무 기간은 원내 관련 규정을 준용한다.

제9조(수당 및 특근매식) 상황실 근무자의 수당 및 특근매식은 원내 관련 규정을 준용한다.

제3장 상황실 임무

제10조(침해대응 임무) ① 상황실 근무자는 다음 각 호의 임무를 수행한다.

1. 국내 민간분야 사이버공격 이슈 실시간 모니터링 및 전파
2. 국내외 보안 사이트 모니터링 및 정보 공유
3. 악성 IP·도메인 접속 차단 및 해제
4. 국내 민간분야 홈페이지 변조 여부 실시간 모니터링 및 대응
5. 침해사고 신고 접수 및 대응
6. 인터넷서비스제공자, 보안관제 기업 등 관련 업체의 네트워크 이상 유무 정기 점검
7. 공공·국방분야로부터 이관받은 민간분야 침해사고 대응
8. 보안 관련 기사 요약 및 전파
9. 상황실 운영에 필요한 시스템 관리 및 점검
10. 그 밖에 침해사고 대응 및 상황실 운영에 필요하다고 판단되는 사항

② 사이버위기경보단계 상향 등 비상시에는 다음과 같은 업무를 추가로 수행한다.

1. 주요 사이트 모니터링 강화
2. 경찰청, 국정원 등 유관기관 비상 공조체계 가동
3. 위기평가회의 가동 및 운영지원
4. 전체 피해현황 집계 및 대응
5. 그 밖에 과학기술정보통신부 민간분야 사이버위기대응 실무 매뉴얼에서 정하는 사항

③ 조장은 제1항과 제2항의 임무 및 팀장으로부터 지시받은 업무를 조원에게 분담할 수 있고 조원은 조장의 지시에 따라 임무를 수행한다.

제11조(기록유지 임무) ① 상황실 근무자는 사고상황, 파급피해·영향 및 수습상황 등 주요 위기사항을 작성·보고하고 그 기록을 유지·관리하여야 한다.

② 위기상황과 관련된 문서·대장 등의 보존 및 관리는 원내 관련 규정에 따른다.

③ 상황실 근무자는 위기상황보고·전파체계도와 관계부처 및 유관기관 연락처, 상황실 근무수칙 등을 상황실에 비치하고 수시로 정비·관리하여야 한다.

제12조(평상시 보고 및 전파 등 임무) ① 상황실 근무자는 제10조에 따른 임무 수행 결과를 작성하여 보고체계에 따라 정기적으로 보고하여야 한다.

② 상황실 근무자는 제1항의 규정에도 불구하고 긴급한 보고가 필요하다고 판단하는 경우 수

시로 보고하여야 한다.

③ 상황실 근무자는 정기·수시 보고시 파악된 사고상황, 파급피해·영향 및 대응 사항 등의 주요 사항을 소관부서 및 유관기관에 전파하여야 한다.

제4장 비상시 운영

제13조(비상시 상황보고 등) ① 상황실 근무자는 다음 각 호의 비상 상황에서 신속한 보고 및 조치가 필요하다고 판단되는 때에는 팀장에게 지체없이 보고하여야 한다.

1. 침해사고 발생으로 종합상황실 시스템 및 업무 중단
2. 사이버위기경보단계 상향 조정
3. 재난, 재해 등으로 인한 상황실 업무 지장 초래

② 팀장은 제1항에 의하여 보고받은 내용을 보고체계에 따라 보고하여야 한다.

제14조(비상상황 전파 및 대응) ① 상황실 근무자는 비상 상황이 파악되면 해당 기업 및 관련 기관에게 그 사실을 전파하여 신속한 대응·복구가 이루어질 수 있도록 하여야 한다.

② 상황실 근무자는 지속적인 상황관리를 위하여 필요시 해당 기업·기관에 파급피해·영향, 향후 전망 및 조치사항 등 관련 정보 파악을 위해 노력하여야 한다. 이 경우 상황실 근무자는 시간대별 조치 및 확인 사항을 기록·관리하여야 한다.

제15조(비상소집 등) ① 팀장은 내용에 따라 비상소집이 필요하다고 판단하는 경우 비상 소집 인력 계획을 본부장에게 보고 후 해당 부서장의 승인하에 관련 업무를 수행하는 직원을 비상 소집할 수 있다.

② 팀장은 제1항에 의해 비상소집된 인력에 대하여 평소에 부여된 임무 외 개별임무를 지정할 수 있다.

부 칙<2020. 8. 28>

제1조(시행일) 이 지침은 경영기획본부장의 승인을 얻은 날로부터 시행한다.