활기찬 경남 행복한 도민

생산등록번호	빅데이터융합센터-554
등 록 일	2022. 7. 27.
결 재 일	2022. 7. 27.
공 개 구 분	비공개(5)

주무관	빅데이터융합센터 센터장	교무처장	총장
전미경	김형수	박태종	2022. 7. 27. 조현명
협조자	주무관 정종문	빅데이터융합센터 팀장	특별휴가

경남도립남해대학
사이버분야 침해사고 대응지침

경남도립남해대학
(빅데이터융합센터)

사이버분야 침해사고 대응지침

각종 사이버 침해사고에 의한 시스템 마비 사태를 대비하기 위한 경남도립 남해대학의 사이버분야 침해사고 대응지침임.

Ⅰ 개요

□ 목적

❍ 「경남도립남해대학 사이버분야 침해사고 대응지침」은 해킹, 바이러스 유포 등 사이버공격으로 인해 정보시스템이 위협받거나 중요자료가 유출되는 사태를 대비하여 침해사고 대응절차와 조치사항을 규정한 것임

□ 관련근거

❍ 국가 위기관리 기본지침

❍ 사이버안보 업무규정

❍ 국가사이버안전관리규정

❍ 정보통신기반 보호법

❍ 전자정부법 및 국가정보원법

❍ 보안업무규정

❍ 국가 정보보안기본지침 및 교육부 정보보안기본지침

❍ 교육부 사이버안전센터 운영규정

□ 적용범위

❍ 해킹, 바이러스 유포 등 사이버공격으로 인한 정보시스템의 마비, 중요자료 유출 등 사이버위기 상황 발생 시

❍ 대학 사이버안전 업무를 총괄하는 빅데이터융합센터의 사이버위기 대응 활동에 적용

□ 용어정의

❍ 사이버위기

- 사이버 공간에서 특정 개인 또는 단체의 전자정보 절취, 왜곡, 훼손, 전자적 수단에 의한 국가 기반시설·정보통신망 파괴 또는 오작동 유발 등의 행위로 인해 국가 안보에 중대한 영향을 미치거나 사회·경제적 혼란이 발생하고 국가 핵심기능이 지장을 받는 상황

❍ 위기관리

- 국가위기를 효과적으로 예방 및 대비하고 대응, 복구하기 위하여 국가의 자원을 기획, 조정, 집행, 통제하는 제반 활동과정

❍ 사이버공격

- 해킹, 컴퓨터 바이러스, 해킹메일, 서비스 거부 등 전자적 수단에 의하여 정보통신망을 불법 침입, 교란, 마비, 파괴하거나 정보를 절취, 훼손하는 일체의 공격행위

❍ 보안관제

- 사이버공격 정보를 실시간으로 탐지 및 분석, 대응하는 일련의 활동

II 사이버침해사고 조치사항

□ 침해사고 분류

❍ 침해사고는 중요도 및 파급 영향도 등 다양한 요소에 따라 일반침해사고, 주요침해사고, 긴급침해사고의 3단계로 분류
※ 단순 스캐닝 등 대학에 영향이 없는 단순 침입시도일 경우 조치권고로 분류

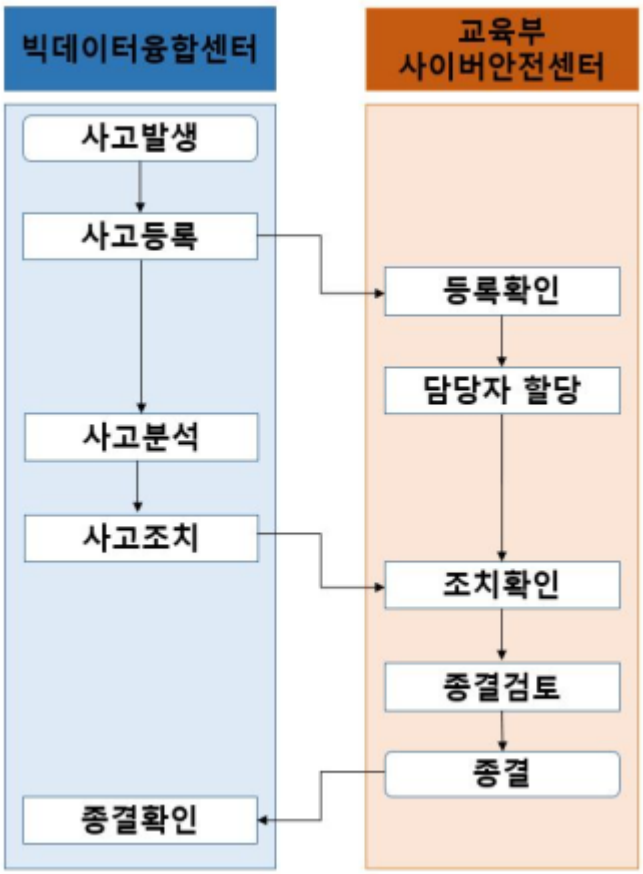
❍ 일반침해사고는 악성코드 감염 등 침해사고로 인해 업무에 지장을 받지 않고 피해확산 규모가 소규모인 경우

❍ 주요침해사고는 웹 해킹 등 중요정보(학사정보, 개인정보 등)가 노출될 가능성이 있고 서비스용 시스템 등 피해시스템이 대외 신뢰도에 큰 영향을 끼치는 경우

❍ 긴급침해사고는 피해시스템이 업무용 주요 시스템(학사관리시스템, 개인정보시스템 등)이거나 대량의 중요정보가 외부 노출될 가능성이 존재할 경우

□ 침해사고 대응 절차

❍ 침해사고 대응 절차도



- 대학에서 침해사고 탐지 시 교육부 사이버안전센터(ECSC)에 유선으로 즉각 통보하여야 하며 정보공유시스템(cyber.ecsc.go.kr)을 통해 사고 발생 이후 24시간 이내 초동조치 완료 후 신고
- 일반침해사고(악성코드 감염 등)의 경우 5일, 주요침해사고(웹 해킹 등)은 2일 이내 대상 시스템에 대하여 조치를 취하고 이를 교육부 사이버안전센터에 보고
- 긴급침해사고는 탐지 시 즉각 초동 조치 및 교육부 사이버안전센터에 유선 신고

Ⅲ 위기경보 수준별 조치사항

□ 위기경보

❍ 위기경보 수준

구 분	판 단 기 준	비 고
관심 (Blue)	- 위험도가 높은 대규모 서비스거부공격, 악성코드, 취약점 및 해킹기법 출현 - 해외 사이버공격 피해가 확산되어 국내 유입 우려 - 침해사고가 일부기관에서 발생 - 국내·외 정치·군사적 위기상황 조성 등 사이버위협 가능성 증가	위기 징후 감시 강화
주의 (Yellow)	- 일부 정보통신망 및 정보시스템 장애 - 침해사고가 다수기관으로 확산될 가능성 증가 - 국내·외 정치·군사적 위기발생 등 사이버안보 위해 가능성 고조	협조 체제 가동
경계 (Orange)	- 복수 정보통신서비스제공자(ISP)망·기간통신망 장애 발생 또는 마비 - 침해사고가 다수기관에서 발생했거나 대규모 피해로 발전될 가능성 증가	즉각 대응 태세 돌입
심각 (Red)	- 국가 차원의 주요 정보통신망 및 정보시스템 대규모 장애 또는 마비 - 침해사고가 전국적으로 발생했거나 피해범위가 대규모인 사고 발생	대응 역량 총동원

※ 교육부에서 발령하는 위기경보 수준 적용

❍ 위기경보 대응

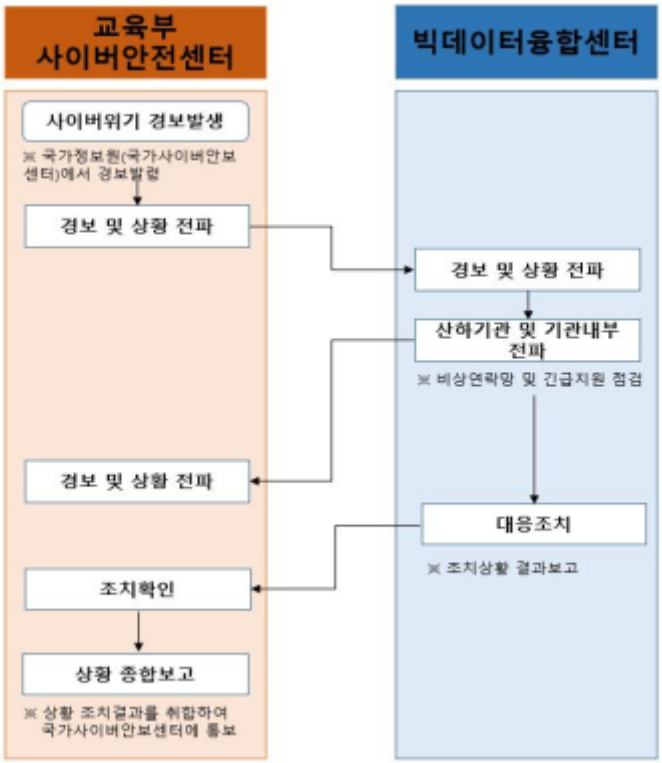
- 위기경보 수준별 대응 범위

경보단계	비상소집 범위	보고범위	소집시간	상황설명
관심	보안담당자	빅데이터융합센터장	3시간 이내	심각한 컴퓨터 웜/바이러스 징후 발생
주의	보안담당자	총장	2시간 이내	사이버침해대응센터 및 대학의 부분적 장애 발생
경계	보안담당자	총장	1시간 이내	사이버침해대응센터 전체 장애, 전국적 마비
심각	전 직원	총장	1시간 이내	

- 위기경보 수준별 이상징후 및 대응요령

경보단계	이상징후	대응요령
정상	- 전 분야 정상적인 활동 - 위험도 낮은 웜/바이러스 발생	- 신규 악성코드, 취약점 공격도구 파악 - 소프트웨어 보안 패치 업데이트 - 불필요한 서비스 차단
관심	신종 사이버위협 출현 등 피해발생 가능	- 사이버테러 관련 언론매체 보도 주시 - 네트워크 트래픽량 변화 모니터링 - 비상연락체계 확인
주의	바이러스, 해킹 출현으로 일부 피해발생	- 공격대상 시스템, 서비스 포트 등에 대한 모니터링 강화 - 악성코드 예상 유입경로 차단 - 특정 호스트에 대한 스캐닝 차단
경계	웜/바이러스 출현 등 대규모 피해발생	- 주의수준 대응요령 수행 - 집중 모니터링 대상 취약점 재점검 - 중요 자료 백업
심각	- 국내외 대규모 피해발생 - 국가적 차원에서 네트워크 사용 불가능	- 주위 및 경계수준 대응요령 수행 - 공격대상 서비스포트 차단 - 피해발생 가능성 높은 네트워크 단절

- 위기경보 발생 절차도



□ 위기경보 수준별 조치사항

❍ ‘관심’ 단계

- 위기상황
  - 웜/바이러스, 해킹기법 등에 의한 피해발생 가능성 증가
  - 해외 사이버공격 피해 확산, 국내유입 우려
  - 정보유출 등 사이버공격 시도 탐지

- 조치사항

① 위기상황 접수 및 전파
  - 국가정보원(국가사이버안보센터)에서 경보 발령
  - 경보 지휘보고 및 상황전파
  - 이상 징후 탐지 또는 사이버위협 신고접수 시 교육부 사이버안전센터 및 경상남도 사이버침해대응센터에 신고

구분	소속	연락처	
교육망 (학사관리, 개인정보)	교육부 사이버안전센터	전화	053-714-0777
		이메일	cert1@ecsc.go.kr
행정망 (행정시스템, 개인정보)	경상남도 사이버침해대응센터	전화	055-211-3002
		이메일	gncert@korea.kr
전체	경남도립남해대학 빅데이터융합센터	보안 담당자	055-254-2443~4

② 초동조치
  - 사이버위기 분석
  - 경보전파 확인
  - 보안권고문 수신 및 대응요령 전파

③ 긴급 대응조치
  - 변종 웜/바이러스 및 추가 공격 등에 대비 보안관제 강화
  - ‘국가 사이버위협 지수’를 참고하여 관제인력 증원 및 신규 탐지규칙 적용
  - 대응현황을 교육부 사이버안전센터에 보고

④ 처리상황 전파
  - 빅데이터융합센터장에게 보안관제 상황과 조치상황 보고
  - 국가정보원(국가사이버안보센터)에서 경보 해제 시 전파

❍ ‘주의’ 단계

- 위기상황

· 다수기관의 정보통신망 및 정보시스템 장애 발생

· 국내외 정치·군사적 위기발생 등 사이버안보 위해 가능성 고조

- 조치사항

① 위기상황 접수 및 전파

· 국가정보원(국가사이버안보센터)에서 경보 발령

· 경보 지휘보고 및 상황전파

② 초동조치

· 경보전파 확인

· 사고원인 분석

· 보안권고문 수신 및 대응요령 전파

· 긴급대응반* 편성 및 가동

* 긴급대응반 구성: 팀장 빅데이터융합센터장, 팀원 빅데이터융합센터 직원

③ 긴급 대응조치

· 보안관제센터와 협조, 관제 강화 조치

· 피해시스템 사고조사 및 피해현황 파악

· 공격 진원지 및 경유지 접속 차단

④ 피해복구 조치

· 피해시스템 목록, 피해상황 등을 작성하여 교육부 사이버안전센터 및 경상남도 사이버침해대응센터에 보고

· 긴급대응반을 구성하여 복구인력을 편성하되, 필요 시 정보통신시스템 유지보수업체 등과 합동 복구 실시

⑤ 처리상황 전파

· 보안관제 상황과 조치현황에 대한 보고서를 작성하여 총장에게 보고

· 대응조치한 결과를 교육부 사이버안전센터 및 경상남도 사이버침해대응센터에 보고

· 국가정보원(국가사이버안보센터)에서 경보 해제 시 전파

❍ ‘경계’ 단계

- 위기상황

· 복수 정보통신서비스제공자(ISP)망 또는 기관망에 피해 발생

· 대규모 피해 확산 가능성 증대

- 조치사항

① 위기상황 접수 및 전파

· 국가정보원(국가사이버안보센터)에서 경보 발령

· 경보 지휘보고 및 상황전파

② 초동조치

· 경보전파 확인

· 보안권고문 수신 및 대응요령 전파

③ 긴급 대응조치

· 보안관제센터와 협조, 관제 강화 조치

· 피해시스템 사고조사 및 피해현황 파악

· 공격 진원지 및 경유지 접속 차단

④ 피해복구 조치

· 피해시스템 복구 조치

· 피해시스템 목록, 피해상황 등을 작성하여 교육부 사이버안전센터 및 경상남도 사이버침해대응센터에 보고

⑤ 처리상황 보고

· 보안관제 상황과 조치현황에 대한 보고서를 작성하여 총장에게 보고

· 대응조치한 결과를 교육부 사이버안전센터 및 경상남도 사이버침해대응센터에 보고

· 국가정보원(국가사이버안보센터)에서 경보 해제 시 전파

· 유출자료에 대한 안보영향평가 실시 및 유출자료에 대한 효력 정지 또는 계획 변경 등 긴급조치 수행

❍ ‘심각’ 단계

- 위기상황

· 전국적인 네트워크 및 정보시스템 사용 불가능

· 주요 핵심기반시설의 피해로 국민혼란 발생

- 조치사항

① 위기상황 접수 및 전파

· 국가정보원(국가사이버안보센터)에서 경보 발령

· 경보 지휘보고 및 상황전파

② 초동조치

· 경보전파 확인

· 보안권고문 수신 및 대응요령 전파

③ 긴급 대응조치

· 교육부 사이버위기대책본부와의 연락 유지

· 사고조사 및 공격진원지 추적

· 피해시스템 격리조치 및 피해확산 방지 조치

④ 피해복구 조치

· 가용역량 총 동원, 신속한 피해복구 활동 추진

· 피해시스템 목록, 피해상황 등을 작성하여 교육부 사이버안전센터 및 경상남도 사이버침해대응센터에 보고

⑤ 처리상황 보고

· 보안관제 상황과 조치현황에 대한 보고서를 작성하여 총장에게 보고

· 대응조치한 결과를 교육부 사이버안전센터 및 경상남도 사이버침해대응센터에 보고

· 국가정보원(국가사이버안보센터)에서 경보 해제 시 전파

· 유출자료에 대한 안보영향평가 실시 및 유출자료에 대한 효력 정지 또는 계획 변경 등 긴급조치 수행

Ⅳ 사이버공격 유형별 조치사항

□ 사이버공격 유형별 상황

❍ 주요 업무 시스템 및 홈페이지 침해사고

- 주요 업무용 시스템 및 중요정보 보유 시스템을 침투하여 중요정보 절취
- 홈페이지의 다양한 보안취약점을 통해 홈페이지 위변조, 악성코드 유포, 자료 유출 및 경유지 악용

❍ 해킹메일 유포 침해사고

- 사회공학적 방법(지인 위장 등)을 이용하여 개인 및 금융정보 절취

❍ 분산 서비스 거부 공격 침해사고

- 특정 시스템을 대상으로 일시에 대량의 트래픽을 유발시켜 시스템의 정상 작동을 방해하거나 마비시키는 행위

□ 사이버공격 조치사항 및 절차

❍ 초동조치

- 침해사고 신고 및 증적자료 보존
  - 침해사고 발생 시 교육부 사이버안전센터에 즉시 유선 신고하고 정보공유 시스템에 등록
  - 피해시스템 전원 유지, 시스템 변경행위(OS재부팅, 자료삭제 등) 금지
  - 1년 이내 피해시스템 및 관련 보안장비 로그 확인

- 확산방지 조치
  - 피해시스템 네트워크 실질 케이블 절체 및 격리 조치
  - 피해시스템의 지속 운영이 필요한 경우 대체 시스템 사용

❍ 대응조치

- 침해사고 조사 실시
  - 1년 이내 피해시스템 및 관련 보안장비 로그 분석하여 침해 흔적 확인
  - 비정상 프로세스 및 응용프로그램 실행 여부 점검

- 시스템 복구
  - 피해시스템 포맷 후 침해사고 조사과정에서 확인된 사고 발생 이전 시점의 백업 데이터를 활용하여 복구 실시
  - 정확한 사고 발생 시점 확인이 어려운 경우 백업 데이터 복구 후 재점검 실시

- 신규 탐지규칙 적용
  - 수집된 악성파일 등을 교육부 사이버안전센터 및 경상남도 사이버침해대응센터로 발송
  - 교육부 사이버안전센터에서 개발된 신규 탐지규칙 적용

❍ 후속조치

- 결과보고
  - 침해사고 경과 및 결과를 교육부 사이버안전센터 및 경상남도 사이버침해대응센터에 보고
- 재발방지대책 수립
  - 피해시스템의 보안취약점 점검 실시
  - 자체 재발방지대책 수립 후 정보공유시스템 등록
- 보안권고문 전파
  - 상황의 중요도에 따라 이행결과를 교육부 사이버안전센터에 보고