정보 보안 지침

사이버분야 위기대응실무 매뉴얼

2023. 7.

- 백 석 대 학 교 -

제1장 개 요

제1절 개 요

웜·바이러스 및 해킹 등 사이버공격에 의한 침해사고가 발생할 경우, 교내 내부의 대응절차와 조치 사항을 규정한 것임

제2절 목 적

대규모 서비스거부공격, 바이러스 유포 등 사이버공격으로 인해 정보시스템이 위협받거나 중요업무자료의 유출 및 국가기능이 지역적·부분적으로 마비되는 사태에 대비하여 우리대학교의 사이버 위기 대응절차와 조치사항을 규정한 것임

제3절 추진배경

1. 사이버 침해사고 발생건수가 지속적으로 증가하고, 교육 기관의 발생비율이 가장 높음.
2. 종합적인 조직체제 및 인프라 구축을 통한 교육 사이버 환경의 안전성 및 신뢰성 확보

제4절 추진근거

1. 「국가 위기관리 기본지침」(대통령훈령 제388호)
2. 「사이버안보 업무규정」(대통령령 제31356호)
3. 「국가사이버안전관리규정」(대통령훈령 제316호)
4. 「정보통신기반 보호법」
5. 「전자정부법」 및 「국가정보원법」
6. 「보안업무규정」(대통령령 제31354호)
7. 「국가 정보보안기본지침」 및 「교육부 정보보안기본지침」
8. 「교육부 사이버안전센터 운영규정」(교육부 훈령 제254호)
9. 「백석대학교 정보보안 지침」제4장(사이버공격 대응)

제5절 적용범위

1. 대규모 서비스거부공격, 바이러스 유포 등 사이버공격으로 인한 정보통신망의 마비, 대외비·비밀 또는 이에 준하는 업무자료 유출 등사이버위기 상황 발생시
2. 교내 단위부서에서 침해사고가 발생하여 교내 정보통신망 마비, 서비스 중단 등의 사태에 적용

백석대학교 BAEKSEOK UNIVERSITY

제6절 용어 정의

구 분	내 용
사이버위기	사이버 공간에서 특정 개인 또는 단체의 전자정보 절취·왜곡· 훼손, 전자적 수단에 의한 국가 기반시설·정보통신망 파괴 또는오작동 유발 등의 행위로 인해 국가 안보에 중대한 영향을미치거나 사회·경제적 혼란이 발생하고 국가 핵심기능이 지장을받는 상황을 말한다.
위기관리	기관의 위기를 사전에 예방하고 발생에 대비하며 위기 발생시에는 효과적인 대응 및 복구를 통하여 그 피해와 영향을 최소화함으로써 조기에 위기 이전상태로 복귀시키고자 하는 제반 활동
정보보안 (정보보호)	정보통신망 및 정보시스템을 통해 수집, 가공, 저장, 검색, 송·수신되는 정보의 유출, 위·변조, 훼손 등을 방지하기 위하여관리적·물리적·기술적 수단을 강구하는 일체의 행위로서「국가 사이버 안전관리규정」제2조 제3호의 사이버안전을포함한다.
주관부서	해당 위기에 대한 기관의 위기관리 활동에 주 책임을 지는 부서
중앙기관	해당 위기에 대한 위기관리 활동에 있어 주관부서의 활동을 지원하고 협조하는 상위 중앙행정기관의 부서
실무부서	위기관리의 대상이 되는 기능·시설을 직접 관리, 운영하고 사이버침해사고 발생시 1차적으로 대응·복구를 수행하는 부서

구 분	내 용
전문기구	보안관제·침해사고대응·정보공유분석 등 사이버안전 업무를 수행하는 기구 ※ 국가사이버안전센터, 국방정보전대응센터, 인터넷침해사고대응지원센터, 교육사이버안전센터,
정 보 통신망	「지능정보화 기본법」 제2조제8호에 따른 정보통신망을말한다.
정보통신 기반시설	「정보통신기반 보호법」 제2조제1호에 따른 정보통신기반시설을말한다
정보 시스템	「전자정부법」 제2조제13호에 따른 정보시스템을 말한다.
사이버 공 격	해킹, 컴퓨터 바이러스, 해킹메일, 서비스 거부 등 전자적수단에 의하여 정보통신망을 불법 침입·교란·마비·파괴하거나정보를 절취·훼손하는 일체의 공격행위를 말한다.
업무자료	다음 각 목의 어느 하나에 해당하는 것을 말한다. ① 「전자정부법」 제2조제6호에 따른 행정정보 및 동법 제2조제7호에 따른 전자문서 ② 「공공기록물 관리에 관한 법률 시행령」 제2조제2호에따른 전자기록물 ③ 기타 다른 법령에 의하여 공무원 등이 직무상 작성·취득하였거나 보유·관리하는 자료로서 전자적으로 처리되어부호·문자·음성·음향·영상 등으로 표현된 것
대외비	업무자료 중에서 「보안업무규정 시행규칙」 제16조제3항에 따라분류된 대외비를 말한다.
정보보호시스템	「국가정보화 기본법」 제3조제6호에 따른 정보보호시스템을말한다.
보안관제	사이버공격 정보를 실시간으로 탐지 및 분석, 대응하는 일련의활동을 말한다.

백석대학교 BAEKSEOK UNIVERSITY

제2장 위기관리 업무 체계

제1절 목 표

1. 사이버위협 조기경보체계 확립 및 사전 예방

2. 위기발생시 피해 최소화 및 신속한 복구

제2절 위기 경보 및 발령 체계

1. 위기경보 수준

구 분	판 단 기 준	비 고
관 심 (Blue)	o 위험도가 높은 대규모 서비스거부공격, 악성코드, 취약점 및해킹기법 출현으로 피해 발생 가능성 증가 o 해외 사이버공격 피해가 확산되어 국내 유입 우려 o 침해사고가 일부기관에서 발생· 국내·외 정치·군사적 o 위기상황 조성 등 사이버위협 가능성 증가	위기 징후 감시 강화
주 의 (Yellow)	o 일부 정보통신망 및 정보시스템 장애 o 침해사고가 다수기관으로 확산될 가능성 증가 o 국내·외 정치·군사적 위기발생 등 사이버안보 위해 가능성 고조	협조 체계 가동
경 계 (Orange)	o 복수 정보통신서비스제공자(ISP)망·기간통신망 장애 발생 또는 마비 o 침해사고가 다수기관에서 발생했거나 대규모 피해로 발전될가능성 증가	즉각 대응 태세 돌입
심 각 (Red)	o 국가 차원의 주요 정보통신망 및 정보시스템 대규모 장애 또는 마비 o 침해사고가 전국적으로 발생했거나 피해범위가 대규모인 사고 발생	대응 역량 총동원

※ 위험 정도가 매우 낮은 웜·바이러스, 해킹기법, 보안취약점 등에 대해서는 위기경보 이전 단계인 정상(Green) 수준으로 간주

※ 위기경보는 국가정보원(NCSC)에서 발령 교육부에서 발령사실 전파

2. 위기경보 발령 및 절차

백석대학교 BAEKSEOK UNIVERSITY

(1) 국가정보원(국가사이버안보센터)은 위기징후를 포착하거나 위기 발생이예상되는 경우, 「공공분야 사이버위기 평가회의」(이하 "사이버위기 평가회의"라 한다.)를 개최하고, 회의를 통해 도출된 평가 및 판단 결과에 따라위기 경보 발령

(2) 국가정보원(국가사이버안보센터)은 위기경보 발령 시 정보공유 시스템, 전자우편·휴대폰 문자메시지 등 기존에 구축된 상황 전파체계를 활용, 국가안보실 및 유관기관에 신속하게 통보

(3) 교육부(ECSC)는 경보 접수 시 교육(행정)기관에 경보발령 사실을전자우편·휴대폰 문자메시지 등을 통해 신속히 전파

3. 위기 형태 및 피해 양상

(1) 위기 형태

가) 홈페이지·메신저·전자우편 등 활용, 악성코드 유포

- 데이터 조작·파괴·은닉·절취 및 데이터 담보 협박

나) 인터넷을 통해 업무용 전산망에 직접 침투

- 정보통신망 교란 및 재침투를 위한 백도어 설치

다) 대규모 봇넷(Botnet)구축, 광범위한 서비스거부공격

- 대량 데이터전송·부정명령 등으로 시스템 정상동작 방해나

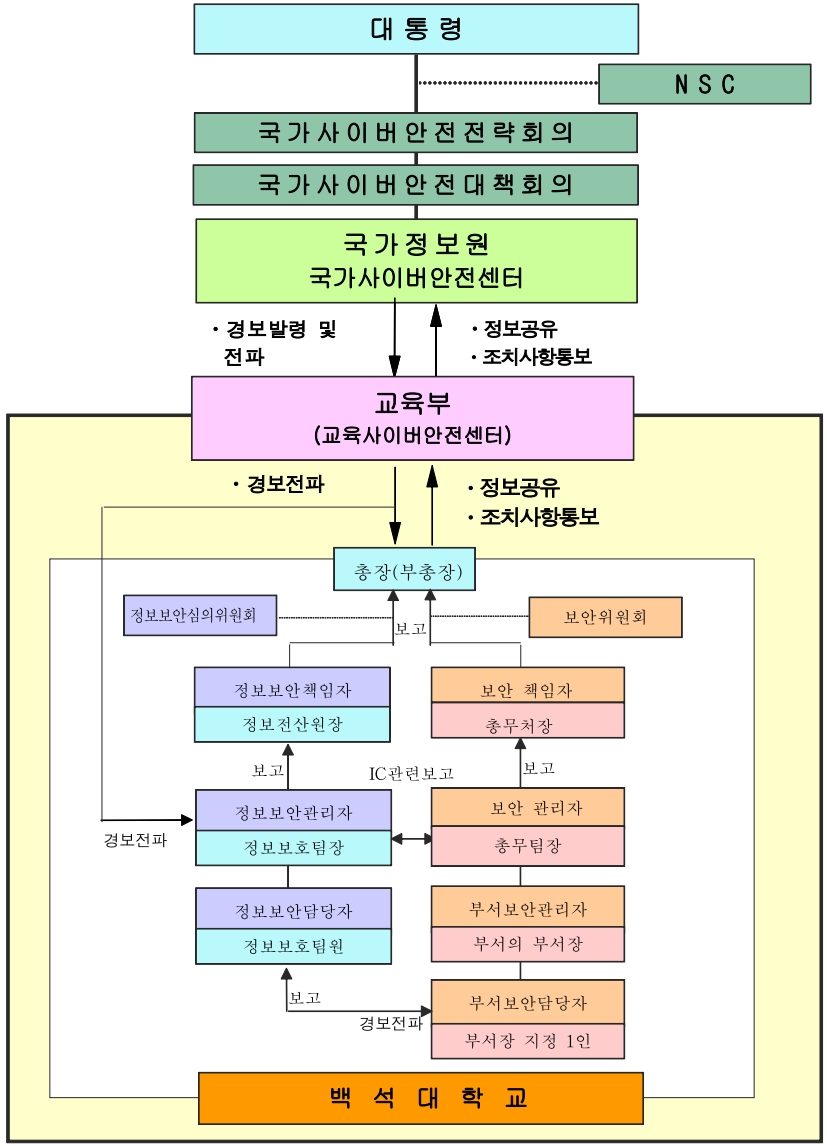
(2) 피해 양상

가) 전력·물류·교통·금융·교육·의료 등 주요정보통신기반시설 마비, 사회혼란 조장 및 국가경제 타격

나) 중요자료·국가기밀 유출, 안보공백 및 외교분쟁 야기

다) 민원·행정서비스 마비, 국민생활 불편 및 정부불신 초래

4. 위기관리 종합체계도



5. 위기관리 조직 및 역할

(1) 위기관리 조직을 다음과 같이 구성한다.

구 성	직 책	역 할	비 고
보안총괄	총장	백석대학교 및 부설기관의 보안업무 전반에 관한 지휘 감독	
보안책임자	총무처장	전반적인 보안 보안업무수행 책임자	
정보 보안책임자	정보전산원장	정보보안에 관한 감독 및 책임자	
보안 관리자	총무팀장	원활한 보안업무수행으로 보안책임자의 업무수행을 보좌함.	
정보 보안관리자	정보보호팀장	정보보안 업무수행 관리자	
부서 보안관리자	각 부서장	부서의 소관 보안업무 수행 관리자	
정보 보안담당자	정보보호팀 담당자	원활한 정보보안업무 수행을 위하여 정보보안관리자를 보좌함.	
부서 보안담당자	각 부서 보안담당	부서의 보안업무 수행 및 부서정보보안 관리자 보좌함.	

(2) 행정부서는 주관부서에서 관리하는 정보통신시스템인 경우 사안에 따라 주관부서에서 직접 보안업무를 수행할 수 있음.

제3절 비상 대응 조직도

1. 조직도

비 상 총 괄 반
o 위기대응활동의 총괄. 지휘감독
o 위기대응 계획 수립 및 대응결과 종합
o 경보에 따른 관련부서와 협조관계 유지, 상호정보교환, 지원체제 구축
o 상황에 따른 대책반을 편성하여 지휘
o 중대한사안인경우 총장및부총장 보고

비 상 대 응 반
o 모든 상황파악에 대한 실무 총괄
o 경보현상을 신속히 파악
o 경보수준별 대응 및 복구활동 총괄
o 진행상황을 체크, 기록
o 위기상황을 비상총괄반에 보고
o 대응팀과 복구팀으로 구성

2. 위기대응 기구

(1) 비상총괄반(장)

가) 구성

비상총괄반은 정보보안책임자인 정보전산원장과 보안책임자인 총무처장과 주관부서장 및 정보보안담당자로 구성되며, 비상총괄반장은 총무처장이 된다.

나) 역할

- 사이버분야 위기대응활동을 총괄 지휘 감독한다.
- 위기대응 계획 수립 및 대응결과 종합한다.
- 상황에 따른 대책반을 편성하여 지휘한다.

(2) 비상대응반(장)

가) 구성

정보보안책임자(정보전산원장), 정보보호팀장, 정보보안담당자로 구성되며,

백석대학교 BAEKSEOK UNIVERSITY

비상대응반장은 정보보안책임자가 된다.

하부조직으로는 대응팀과 복구팀으로 구성한다.

나) 역할

- 모든 상황파악에 대한 실무를 총괄한다.
- 경보현상을 신속히 파악한다.
- 경보수준별 대응업무 및 복구업무를 총괄한다.
- 진행을 체크, 기록한다.
- 위기상황을 비상총괄반에 보고한다.
- 경보에 따른 관련부서와 협조관계 유지, 상호정보교환, 지원체제 구축한다.

(3) 대응팀

가) 구성

정보보안담당자와 정보통신업무를 지원하는 정보통신 주관부서원, 전산망 관리자와 전산망 운영을 지원하는 부서원으로 구성되며, 대응팀 팀장은 정보호호팀장이 된다.

나) 역할

- 경보를 전파하고, 수준별 대응활동을 실시한다.
- 위기의 진행상황에 대한 피해확산을 차단한다.
- 피해지역을 격리시키고, 피해자를 색출한다.
- 침해사고 원인조사 및 분석업무를 수행한다.
- 위기 대응방법을 원내에 전파한다.
- 백신 업데이트 및 수동 검사 시행 안내 게시
- 각종 보안패치확인
- 로그기록 분석
- 피해상황을 종합처리하고 진행상황을 보고한다.
- 전산망의 이상징후 모니터링을 지속 실시한다.
- 합동조사팀·복구지원팀의 활동을 지원한다.
- 전원, UPS, 부대설비 등의 점검을 실시한다.
- 전원, UPS, 부대설비 등 시설피해발생시 복구 및 재설치를 이행한다.

(4) 복구팀

백석대학교 BAEKSEOK UNIVERSITY

가) 구성

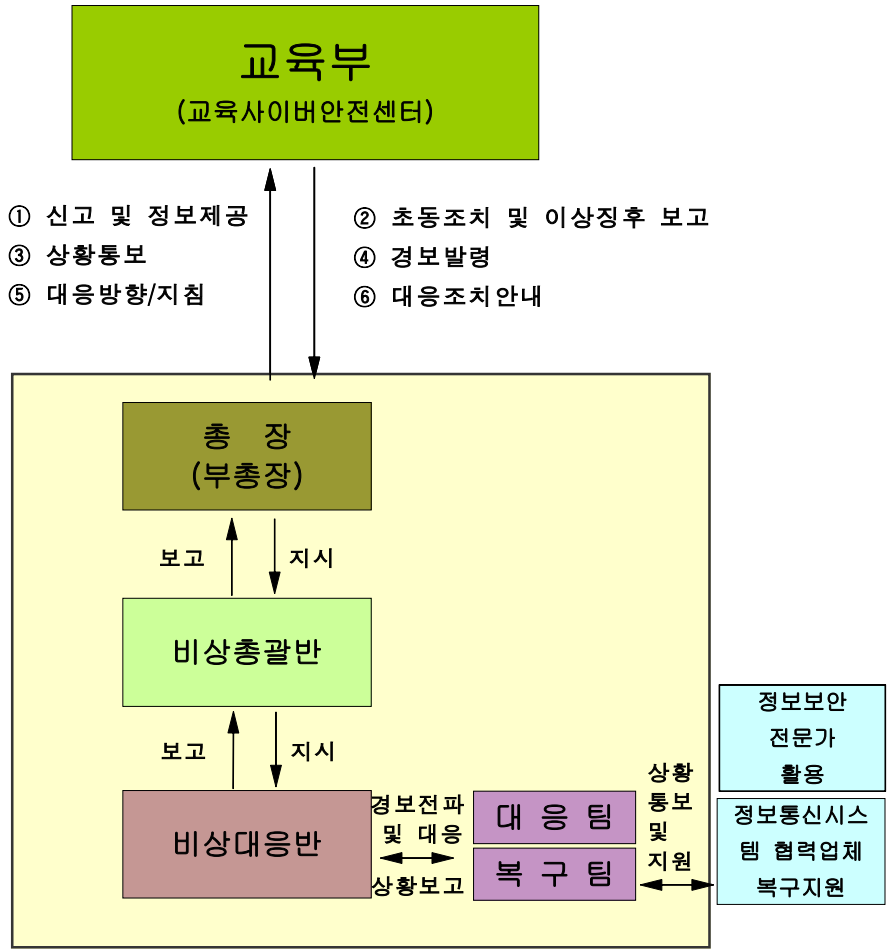
정보화 주관부서의 정보시스템담당자, DB관리자, 홈페이지 운영자 등으로 구성되며, 복구팀의 팀장은 전산개발운영팀장이 된다.

나) 역할

- 정보시스템 상태 점검를 점검한다.
- 정보시스템의 중요 데이터의 백업상태를 확인한다.
- 정보시스템의 운영체제 등 재설치 유틸리티를 확보한다.
- 백업매체를 이용한 시스템 복구를 담당한다.
- 복구된 내용을 확인하고 점검한다.

3. 임무 및 책임

구 분	임 무
비상총괄반	o 긴급대응 총괄 o 대응계획 수립 및 대응결과 종합 o 위기대응활동을 지휘 감독할 1차적인 책임과 권한 o 경보에 따른 관련부서와 협조관계 유지, 상호정보교환, 지원체제 구축 o 상황에 따른 대책반을 편성하여 지휘
비상대응반	o 모든 상황파악에 대한 실무를 총괄 o 경보현상 파악 및 위기 대응 행동지침 하달 o 대응 업무 및 복구 업무 총괄 o 진행 및 비상상황을 비상총괄반에 보고
대응팀	o 경보 전파 및 대응 o 피해확산 차단 o 사고 원인조사 및 분석 o 대응방법 전파 o 피해상황 종합처리 및 보고 o 전산망 이상 징후 모니터링 o 합동조사팀·복구지원팀과 협조 o 전원, UPS, 부대설비 등의 점검 및 복구
복구팀	o 유지보수 업체 연락처 및 비상연락망 확보 o 복구 대책의 수립 및 전파 o 시스템 상태 점검 o 운영체제 등 재설치 유틸리티 확보 o 중요 데이터 백업 확인 o 백업매체를 이용한 데이터 및 시스템 복구 o 복구된 사항의 점검



제3장 경보수준 별 대응요령

제1절 위기별 대응 조직 요약

단계	판단 기준	구성시기	구성 운영	비 고
정상 (Green)	공공분야 합동대응반	필요시	국가정보원	평시 대응
	교육부 정보보호 점검반	필요시	교육부	
	기관별 사이버위기 대응 기구	필요시	백석대학교	
관심 (Blue)	공공분야 합동대응반	필요시	국가정보원	위기 징후 감시 강화
	교육부 정보보호 점검반	필요시	교육부	
	기관별 사이버위기 대응 기구	필요시	백석대학교	
주의 (Yellow)	공공분야 합동대응반	필요시	국가정보원	협조 체제 가동
	교육부 정보보호 점검반	필요시	교육부	
	기관별 사이버위기 대응 기구	필요시	백석대학교	
경계 (Orange)	공공분야 합동대응반	필요시	국가정보원	즛각 대응 태세 돌입
	교육부 정보보호 점검반	필요시	교육부	
	기관별 사이버위기 대응 기구	필요시	백석대학교	
심각 (Red)	공공분야 합동대응반	필요시	국가정보원	대응 역량 총동원
	교육부 정보보호 점검반	필요시	교육부	
	기관별 사이버위기 대응 기구	필요시	백석대학교	

백석대학교 BAEKSEOK UNIVERSITY

제2절 관심

1. "관심" 단계 상황

◎ 웜·바이러스, 해킹기법등에 의한 피해 가능성 증가

- 신·변종 웜·바이러스 출현 후 급속 확산 징후 감지
- 일부기관의 감염피해 신고 및 정보보호업체의 피해접수 증가
- 운영체계(예:윈도우) 등 각급기관에서 다수 사용하는 범용S/W의 보안 취약점을이용한 공격코드 인터넷 공개

◎ 해외 사이버공격 피해 확산, 국내유입 우려

- 미·영·독 등 주요국 피해사례 증가, 국내 유입 가능성 증대- 해외 보안기관·업체의 위협등급 상향 조정 및 경보 발령

◎ 정보유출 등 사이버공격 시도 탐지

- 일부기관에서 유사한 유형의 비인가 접근시도 빈발- 특정기관 사용자들의 해킹용 이메일 수신사례 신고 접수

◎ 국내·외 정치·군사적 위기상황 조성 등 사이버안보 위해 가능성 증가

- 해커단체에 의한 국내 전산망 대상 공격 첩보 입수- 테러단체·적성국의 우리나라 대상 위협 발언

◎ 또는 상기 유형과 유사한 수준의 사이버위기 발생

2. "관심" 단계 조치사항 및 절차

① 위기상황 접수 및 전파

① 국가정보원(국가사이버안보센터)에서 사이버위기 '관심' 경보 발령
② '관심' 경보 지휘보고 및 상황전파

↓

② 초동조치

① 사이버위기 분석
② 교내 '관심' 경보전파 확인
③ 보안권고문 수신 및 대응요령 전파

↓

③ 긴급 대응조치

① 변종 웜·바이러스 및 추가 공격 등에 대비 보안관제 강화
② 기술·관리·물리적 보안대책 강화
③ 공격 탐지규칙 적용 및 보안관제 강화 모니터링
④ 상황 조치 결과 취합
※ '관심' 경보에 따른 대응현황을 교육부(ECSC)에 보고

↓

④ 처리상황 전파

① 위기대응 상황 종합 보고
② 국가정보원(국가사이버안보센터)에서 '관심' 경보 해제 시 전파

백석대학교 BAEKSEOK UNIVERSITY

3. '관심' 단계 조치내용

가. 위기상황 접수 및 전파

(1) 사이버위기 징후 탐지 및 경보발령

- 정보보호팀은 교내에서 이상 징후 탐지 또는 해킹사고 시 교육부 및 교육사이버안전센터에 통보
- 사이버위기 내용에 대해 정보보안책임자에 보고하고, 공문 등을 통해 각 부서에 전파

나. 초동조치

(1) 사이버위기 분석

- 정보보호팀은 현장·원격 조사를 통해 악성코드·로그기록 등 위협정보를입수하고 피해 확산 방지를 위한 초동 대응 수행
- 입수한 위협정보를 초동 분석하여 공격수법·피해가능성 등을 확인

(2) '관심' 경보전파 확인

- 정보보호팀은 교내 각 부수에 경보를 전파하고, 그 결과를교 육부(ECSC)에 회신

(3) 보안권고문 수신 및 대응요령 전파

- 공격에 사용된 보안취약점, 해킹수법 및 대응방법이 포함된 보안권고문을 국가정보원(국가사이버안보센터) 및 교육부(교육사이버안전센터)로부터 제공받아 각 부서에 전파
- 필요시 교육부「정보보호 점검반」및 '긴급대응반' 요청

다. 긴급 대응조치

(1) 변종 웜·바이러스 출현 및 추가공격 대비 보안관제 강화

- '국가 사이버위협 지수'를 참고하여 신규 탐지규칙적용 등 보안 관제 강화
- 협력업체 지원 요청 실시, 자체 보안장비를 활용한 내·외부 사이버 위협에 대한 보안관제 강화

(2) 기술·관리·물리적 보안대책 강화

- 사이버공격으로 인한 피해발생 여부 점검
- 새로운 보안취약점 및 해킹수법에 대비, 보안패치 및 백신 업데이트 실시
- 불필요한 프로그램 및 서비스포트 차단, 위험 최소화

- 침입차단시스템 등 정보보호시스템의 정보통신망 접근 차단 설정 점검
- 해킹 의심메일 열람 금지 및 악성코드 유포사이트 접속 차단

(3) 공격 탐지규칙 확인 및 적용

- 국가정보원(국가사이버안보센터) 및 교육부(교육사이버안전센터)로부터 사이버 공격에 사용되는 트래픽 특성과 도구를 탐지하기 위한 탐지규칙을 제공받아 보안관제 강화 실시
- 자체 탐지 및 분석된 사이버공격 분석자료를 활용하여 탐지규칙 적용

4. 처리상황 전파

(가) 교육(행정)기관 위기대응 상황 종합 보고

- 보안관제 상황과 조치상황에 대한 대응 조치한 결과를 교육부(ECSC)에 통보

(나) 사이버위기 '관심' 경보 해제

- 국가정보원(국가사이버안보센터)에서 '관심' 경보발령 해제시정보보호팀은 교내 전파

백석대학교 BAEKSEOK UNIVERSITY

제3절 주의

1. "주의" 단계 상황

◎ 다수기관의 정보통신망 및 정보시스템 장애 발생

- 신·변종 웜·바이러스 출현 후 급속 확산
- 웜·바이러스 감염피해 발생, 사고 신고 증가
- 네트워크 접속장애 발생

◎ 다수기관의 정보유출 등 피해 발생 및 확산가능성 증가

- 해킹메일 수신 및 감염사례 빈발
- 업무자료 유출 사고 발생
- 특정 국가 또는 IP로 지속적인 데이터 전송 트래픽 발생

◎ 국내·외 정치·군사적 위기발생 등 사이버안보 위해 가능성 고조

- 국내·외 해커단체의 국내 전산망 공격 시도 발표 후 공격 착수
- 네트워크 이상트래픽 과다 탐지 및 네트워크 장애

◎ 또는 상기 유형과 유사한 수준의 사이버위기 발생

2. "주의" 단계 조치사항 및 절차

① 위기상황 접수 및 전파

① 국가정보원(국가사이버안보센터)에서 사이버위기 '주위' 경보 발령
② '주위' 경보 지휘보고 및 상황전파

② 초동조치

① 교내 '주의' 경보전파 확인
② 침해사고 원인 분석
③ 보안권고문 작성 및 대응요령 전파
④ 긴급대응반 편성 및 가동

③ 긴급 대응조치

① 교육사이버안전센터(ECSC)와 협조, 관제 강화 조치
② 피해 방생 시 사고조사 및 피해현황 파악
③ 공격 진원지·경유지 접속 차단

④ 피해복구 조치

① 피해 복구 조치
② 교내 피해복구 추진 실태 파악

⑤ 처리상황 전파

① 위기대응 상황 종합 보고
② 국가정보원(국가사이버안보센터)에서 '주의' 경보 해제 시 전파

백석대학교 BAEKSEOK UNIVERSITY

3. '주의' 단계 조치내용

가. 위기상황 접수 및 전파

(1) '주의' 경보 지휘보고 및 상황전파

- 정보보호팀은 사이버위기 내용에 대해 정보보안책임자에 보고하고, 공문 등을 통해 교내 전파

나. 초동조치

(1) '주의' 경보전파 확인

- 정보보호팀은 교내 각 부수에 경보를 전파하고, 그 결과를교 육부(ECSC)에 회신

(2) 보안권고문 수신 및 대응요령 전파

- 국가정보원(국가사이버안보센터)에서 공유된 공격에 사용되는 보안취약점, 해킹방법에 대한 정보 및 대응방법이 포함된 보안권고문을 작성, 정보공유시스템 및 이메일 등을 통해 교내에 신속 전파

다. 긴급 대응조치

(1) 교육사이버안전센터(ECSC)와 협조, 관제 강화 조치

- 국가정보원(국가사이버안보센터) 상황팀(또는 「사이버위기대책본부」구성 시 상황지원팀)에서 공유 된 공격IP·탐지룰 등 관련정보를 보안관제시스템에 적용하여 교육사이버안전센터(ECSC)와의 합동 보안관제 강화

(2) 피해현황 조사 및 파악

- 피해발생 시 국가정보원(국가사이버안보센터) 또는 교육부(ECSC)에서 현장·원격조사를 실시하여 공격기법·피해양상·경유지 등 조사
- 피해 발생 시 해당시스템 격리조치 및 피해확산 방지 조치 수행

(3) 공격 진원지·경유지 접속차단

- 공유된 공격지 및 경유지에 대한 접속 차단을 검토 및 적용

라. 피해복구 조치

(1) 피해 복구 조치 및 현황 파악

- 교내 피해 현황을 파악하고 피해복구 우선순위를 산정하여 원격·현장 복구 계획을 수립
- 「긴급대응반」으로 복구 인력을 편성하되, 필요 시 정보통신시스템 유지보수업체 등과 합동 복구 실시

(2) 피해복구 추진 실태 파악

- 교내에서 발행한 피행상황을 종합 정리
- 정보보호팀은 피해복구 추진실태를 수시파악, 복구가 더딘 사항에 인력 및 장비 등 가용자원을 집중 투입할수 있도록 피해복구 우선순위를 재설정
- 복구 우선순위 산정시 안보 및 경제 사회적 중요도를 고려해 판단

마. 처리상황 전파

(1) 대응결과 종합 및 보고

- 보안관제 상황과 조치현황에 대한 종합 보고서를 작성하고, 정보보호책임자에 종합보고
- 정보보호팀은 대응 조치한 결과를 교육부(ECSC)에 통보

(2) 사이버위기 '주의' 경보 해제

- 국가정보원(국가사이버안보센터)에서 '주의' 경보발령 해제 시 전달하는 통지문을 교내에 전파

제4절 경계

1. "경계" 단계 상황

◎ 복수 ISP망 또는 기간망에 피해 발생

- 복수 ISP망에서 이상 트래픽 급증 및 소통장애 발생
- 국내 다수정보통신망 등 중요 정보통신망의 접속지연 발생

◎ 대규모 피해 확산 가능성 증대

- 웜·바이러스 급속한 확산으로 대규모 피해 가능성 증대
- 해킹도구의 인터넷 유포로 인한 해킹사고 급증
- DNS 마비·네트워크 단절 등 주요시스템 장애 발생
- 전력·가스 등 핵심기반시스템 대상 공격 시도 급증

◎ 정보유출 등 대규모 침해사고 발생

- 국가 안보관련 기관을 대상으로 비인가 접근 시도 및 정보 유출을 위한 다양한 공격징후 발견
- 다수기관에서 대외비 이상의 비밀 등 중요정보 유출 등 침해사고 발생

◎ 복수분야에서 광범위한 피해가 발생하는 등 대규모 피해로 확대될 가능성이 높아다수기관의 공조대응이 필요한 경우

◎ 또는 상기 유형과 유사한 수준의 사이버위기 발생

2. "경계" 단계 조치사항 및 절차

① 위기상황 접수 및 전파

① 국가정보원(국가사이버안보센터)에서 사이버위기 '경계' 경보 발령
② '경계' 경보 지휘보고 및 상황전파

② 초동조치

① 교내 '경계' 경보전파 확인
② 보안권고문 작성 및 대응요령 전파

③ 긴급 대응조치

① 교육사이버안전센터(ECSC)와 협조, 관제 강화 조치
② 패히 발생시 사고조사 및 피해현황 파악
③ 공격 진원지·경유지 접속 차단

④ 피해복구 조치

① 피해 복구 조치
② 교내 피해복구 추진 실태 파악

⑤ 처리상황 전파

① 위기대응 상황 종합 보고
② 국가정보원(국가사이버안보센터)에서 '주의' 경보 해제 시 전파

백석대학교 BAEKSEOK UNIVERSITY

3. '경계' 단계 조치내용

가. 위기상황 접수 및 전파

(1) '경계' 경보 지휘보고 및 상황전파

- 정보보호팀은 사이버위기 내용에 대해 정보보안책임자에 보고하고, 공문 등을 통해 교내 전파

나. 초동조치

(1) '주의' 경보전파 확인

- 정보보호팀은 교내 각 부수에 경보를 전파하고, 그 결과를 교육부(ECSC)에 회신

(2) 보안권고문 수신 및 대응요령 전파

- 국가정보원(국가사이버안보센터)에서 공유된 공격에 사용되는 보안취약점, 해킹방법에 대한 정보 및 대응방법이 포함된 보안권고문을 작성, 정보공유시스템 및 이메일 등을 통해 교내에 신속 전파

다. 긴급 대응조치

(1) 교육사이버안전센터(ECSC)와 협조, 관제 강화 조치

- 국가정보원(국가사이버안보센터) 상황팀(또는 「사이버위기대책본부」 구성 시 상황지원팀)에서 공유 된 공격IP·탐지룰 등 관련정보를 보안관제시스템에 적용하여 교육사이버안전센터(ECSC)와의 합동 보안관제 강화

(2) 피해현황 조사 및 파악

- 피해발생 시 국가정보원(국가사이버안보센터) 또는 교육부(ECSC)에서 현장·원격조사를 실시하여 공격기법·피해양상·경유지 등 조사
- 피해 발생 시 해당시스템 격리조치 및 피해확산 방지 조치 수행

(3) 공격 진원지·경유지 접속차단

- 공유된 공격지 및 경유지에 대한 접속 차단을 검토 및 적용

라. 피해복구 조치

(1) 피해 복구 조치 및 현황 파악

- 교내 피해 현황을 파악하고 피해복구 우선순위를 산정하여 원격·현장 복구 계획을 수립
- 「긴급대응반」으로 복구 인력을 편성하되, 필요 시 정보통신시스템 유지보수업체 등과 합동 복구 실시

(2) 피해복구 추진 실태 파악

- 교내에서 발행한 피행상황을 종합 정리
- 정보보호팀은 피해복구 추진실태를 수시파악, 복구가 더딘 사항에 인력 및 장비 등 가용자원을 집중 투입할수 있도록 피해복구 우선순위를 재설정
- 복구 우선순위 산정시 안보 및 경제 사회적 중요도를 고려해 판단

마. 처리상황 전파

(1) 대응결과 종합 및 보고

- 보안관제 상황과 조치현황에 대한 종합 보고서를 작성하고, 정보보호책임자에 종합보고
- 정보보호팀은 대응 조치한 결과를 교육부(ECSC)에 통보

(2) 사이버위기 '경계' 경보 해제

- 국가정보원(국가사이버안보센터)에서 '경계' 경보발령 해제 시 전달하는 통지문을 교내에 전파

백석대학교 BAEKSEOK UNIVERSITY

제5절 심각

1. "심각" 단계 상황

◎ 전국적인 네트워크 및 정보시스템 사용 불가능

- DNS마비·네트워크 트래픽 폭주 등으로 인해 복수 ISP망에서 인터넷 등 네트워크 마비
- 국가정보통신망 등 중요 기간통신망 마비

◎ 주요 핵심기반시설의 피해로 국민혼란 발생

- 전력·가스 등 핵심기반시스템 대상 피해 발생
- 국가 주요정보통신망 및 정보시스템 사용 불가능

◎ 정보유출 등 대규모 침해사고 전국적으로 발생

- 외교·국방 등 안보관련 기관에서 비밀 대량 유출
- 다수기관에서 대규모 정보유출 발생 및 보유중인 국가 핵심자료의 훼손 발생

◎ 국가적 차원의 평가와 조치가 필요하다고 판단되는 사고 발생

2. "심각" 단계 조치사항 및 절차

① 위기상황 접수 및 전파

① 국가정보원(국가사이버안보센터)에서 사이버위기 '심각' 경보 발령
② '심각' 경보 지휘보고 및 상황전파

② 초동조치

① 교내 '심각' 경보전파 확인
② 보안권고문 작성 및 대응요령 전파

③ 긴급 대응조치

① 비상 총괄반 및 비상 대응반 가동
② 가용역량 총 동원, 사고조사 및 공격진원지 추적
③ 피해발생 가능성 높은 네트워크 단절여부 판단

④ 피해복구 조치

① 가용역량 총 동원, 신속한 피해복구 활동 추진
② 교내 피해복구 추진 실태 파악

⑤ 처리상황 전파

① 위기대응 상황 종합 보고
② 국가정보원(국가사이버안보센터)에서 '주의' 경보 해제 시 전파

백석대학교 BAEKSEOK UNIVERSITY

3. '심각' 단계 조치내용

가. 위기상황 접수 및 전파

(1) '심각' 경보 지휘보고 및 상황전파

- 정보보호팀은 사이버위기 내용에 대해 정보보안책임자에 보고하고, 공문 등을 통해 교내 전파

나. 초동조치

(1) '주의' 경보전파 확인

- 정보보호팀은 교내 각 부수에 경보를 전파하고, 그 결과를 교육부(ECSC)에 회신

(2) 보안권고문 수신 및 대응요령 전파

- 국가정보원(국가사이버안보센터)에서 공유된 공격에 사용되는 보안취약점, 해킹방법에 대한 정보 및 대응방법이 포함된 보안권고문을 작성, 정보공유시스템 및 이메일 등을 통해 교내에 신속 전파

다. 긴급 대응조치

(1) 사이버위기대책 본부 가동

- 대응역량을 집중하기 위하여「비상총괄반」 및 「비상대응반」구성·운영
- 신속한 복구 및 대응을 위하여 대응팀, 복구팀을 구성

(2) 가용역량 총 동원, 사고조사 및 공격진원지 추적

- 피해발생 시 국가정보원(국가사이버안보센터) 또는 교육부(ECSC)에서 현장·원격조사를 실시하여 공격기법·피해양상·경유지 등 조사
- 피해 발생 시 해당시스템 격리조치 및 피해확산 방지 조치 수행
- 확인된 공격진원지에 대한 접근차단 조치 요청 등 유관기관 협조 대응 실시

(3) 대응결과 종합 및 보고

- 보안관제 상황과 조치현황에 대한 종합 보고서를 작성하고 정보보안책임자에 보고하고, 교육부(교육사이버안전센터)에 통보

(4) 피해발생 가능성 높은 네트워크 단절여부 판단

- 피해확산으로 대규모 피해가 우려되는 경우, 관련네트워크 및 인터넷 단절여부 검토

라. 피해복구 조치

(1) 피해 복구 조치 및 현황 파악

- 교내 피해 현황을 파악하고 피해복구 우선순위를 산정하여 원격·현장 복구 계획을 수립
- 「긴급대응반」으로 복구 인력을 편성하되, 필요 시 정보통신시스템 유지보수업체 등과 합동 복구 실시

(2) 피해복구 추진 실태 파악

- 교내에서 발행한 피행상황을 종합 정리
- 정보보호팀은 피해복구 추진실태를 수시파악, 복구가 더딘 사항에 인력 및 장비 등 가용자원을 집중 투입할수 있도록 피해복구 우선순위를 재설정
- 복구 우선순위 산정시 안보 및 경제 사회적 중요도를 고려해 판단

마. 처리상황 전파

(1) 대응결과 종합 및 보고

- 보안관제 상황과 조치현황에 대한 종합 보고서를 작성하고, 정보보호책임자에 종합보고
- 정보보호팀은 대응 조치한 결과를 교육부(ECSC)에 통보

(2) 사이버위기 '심각' 경보 해제

- 국가정보원(국가사이버안보센터)에서 '경계' 경보발령 해제 시 전달하는 통지문을 교내에 전파

백석대학교 BAEKSEOK UNIVERSITY

제4장 사이버공격 유형별 대응 및 조치사항

제1절 개요

1. 개요

정보통신기술 사용이 많아짐에 따른 다양한 사이버공격도 함께 증가하고, 기법 또한 지능화·은밀화 됨에 따라 국민생명과 국가안보에 직결되는 문제로심각성이 점차 커지고 있음이에 따라 사이버공격 발생 시 이를 신속히 탐지·차단하고 사고원인을규명해 재발방지대책을 수립하는 일련의 대응 및 조치활동이 매우 중요함

2. 사이버공격 유형별 상황

(가) 주요 업무 시스템 및 홈페이지 침해사고

- 주요 업무용 시스템 및 중요정보(개인정보 등) 보유 시스템을 침투하여중요정보 절취 등
- 홈페이지의 다양한 보안취약점을 통해 홈페이지 위변조, 악성코드 유포, 자료 유출 및 경유지 악용 등

(나) 해킹메일 유포 침해사고

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

(다) 서비스 시스템 DDoS 침해사고

- 특정 시스템을 대상으로 일시에 대량의 트래픽을 유발시켜 시스템의정상 작동을 방해하거나 마비시키는 행위 등

백석대학교 BAEKSEOK UNIVERSITY

3. 사이버공격 조치사항 및 절차

절차	구분	근거조항
1. 침해사고 신고 및 증적자료 보존	초동조치	① 정보보안기본지침 제39조, 40조 ② 교육부 사이버안전센터 운영규정 제5조, 제8조, 제9조, 제10조
2. 확산방지 조치		
3. 침해사고 조사 실시	대응조치	
4. 시스템 복구		
5. 신규 탐지규칙 개발 및 적용		
6. 결과종합 및 보고	후속조치	
7. 재발방지대책 수립		
8. 보안권고문 전파		

제2절 사이버공격 유형별 대응 및 조치

1. '홈페이지' 공격 조치내용

(가) 초동조치

(1) 침해사고 신고 및 증적 자료 보존

- 정보보호팀은 침해사고 발생 시 정보보호책임자에게 보고하고 교육부(ECSC)에 즉시 유선 신고 및 정보공유시스템에 등록
- 피해시스템 전원 유지, 시스템 변경행위(OS재부팅, 자료삭제 등) 금지
- 1년 이내 피해시스템 및 관련 보안장비 로그 확보

(2) 확산방지 조치

- 피해시스템 네트워크 절체 및 격리 조치 실시하고 지속 운영이 필요한경우 대체 시스템 사용

※ 네트워크 절체 시 방화벽을 이용한 논리적 절체가 아닌 실질 케이블 절체 필요

(나) 대응조치

(1) 침해사고 조사 실시

- 1년 이내 피해시스템 및 관련 보안장비 로그 분석하여 침해 흔적 확인
- 홈페이지 내 악성파일(웹쉘 등)생성 여부 확인
- DB내 데이터 변경 및 확인되지 않은 계정 등 여부 확인

※ 피해시스템과 연동된 DB의 경우 ID/PW 변경 실시

- 비정상 프로세스 및 응용프로그램 실행 여부 점검
- 현장 확인이 필요하다고 판단되는 경우 교육부 「정보보호 점검반」 요청

(2) 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

(3) 신규 탐지규칙 개발 및 적용

- 수집된 악성파일(웹쉘 등)을 교육부(ECSC)로 발송

- 신규 탐지규칙 개발 후 교내 적용

(다) 후속조치

(1) 결과종합 및 보고

- 침해사고 경과 및 결과 종합 보고 실시

(2) 재발방지대책 수립

- 피해시스템의 보안취약점 점검 실시
- 정보보호팀은 재발방지대책을 수립하여 정보보안책임자 보고 및 교육부(ECSC) 통보

(3) 보안권고문 전파

- 추가 피해 발생 및 중요 사안일 경우 차단 가능한 정보를 포함하여 교내 보안권고문 전파 실시
- 상황의 중요도에 따라 이행결과 확인

2. '해킹 메일' 조치내용

(가) 초동조치

(1) 침해사고 신고 및 증적 자료 보존

- 정보보호팀은 침해사고 발생 시 정보보호책임자에게 보고하고 교육부(ECSC)에 즉시 유선 신고 및 정보공유시스템에 등록
- 피해시스템 전원 유지, 시스템 변경행위(OS재부팅, 자료삭제 등) 금지
- 1년 이내의 피해 PC 및 보안장비(스팸차단솔루션 등) 로그 확보
- 수신된 해킹메일의 경우 별도로 삭제하지 말고 EML파일의 형태로별도 보존 및 신고 시 필수 포함, 사고 조사 후 삭제 등 후속처리

(2) 확산방지 조치

- 수신 메일 계정 비활성화 및 피해 PC 점검 실시
- 해킹메일 발신 계정에 대한 차단정책 적용 및 추가 수신 메일 여부 확인 후해당 PC점검 실시
- 피해 PC 네트워크 절체 실시

※ 네트워크 절체 시 방화벽을 이용한 논리적 절체가 아닌 실질 케이블 절체 필요

(나) 대응조치

(1) 침해사고 조사 실시

- 비정상 프로세스 및 응용프로그램 실행 여부 점검
- 1년 이내 수·발신 내역 확인 및 첨부파일 분석실시
- 메일 원문 및 첨부파일 등 분석을 통해 악성코드감염 여부 확인
- 메일 계정(사용자 및 관리자)관리 현황 확인
- 현장 확인이 필요하다고 판단되는 경우 교육부 「정보보호 점검반」 요청

(2) 시스템 복구

- 해킹메일 삭제 실시
- 피해PC 포맷 및 메일 계정 변경 등 추가 조치 권고

(3) 신규 탐지규칙 개발 및 적용

- 수집된 악성파일 및 원본 메일 등 관련 자료 교육부(ECSC)로 발송
- 신규 탐지규칙 개발 후 교육(행정)기관에 적용

(다) 후속조치

(1) 결과종합 및 보고

- 침해사고 경과 및 결과 종합 보고 실시

(2) 재발방지대책 수립

- 피해시스템의 보안취약점 점검 실시
- 정보보호팀은 재발방지대책을 수립하여 정보보안책임자 보고 및 교육부(ECSC) 통보

(3) 보안권고문 전파

- 추가 피해 발생 및 중요 사안일 경우 차단 가능한 정보를 포함하여 교내 보안권고문 전파 실시
- 상황의 중요도에 따라 이행결과 확인

3. '서비스거부공격' 조치내용

(가) 초동조치

(1) 침해사고 신고 및 증적 자료 보존

- 정보보호팀은 침해사고 발생 시 정보보호책임자에게 보고하고 교육부(ECSC)에 즉시 유선 신고 및 정보공유시스템에 등록
- 공격IP 차단(DDoS대응장비 등) 및 네트워크장비(QOS, 스위치 등)에서트래픽 분산 처리
- 보안장비 및 네트워크 장비 자료(로그 등) 보존 실시

(2) 확산방지 조치

- ISP(인터넷 회선 사업자)에 회선 모니터링을 통해 공격 IP차단 요청
- 보안장비를 활용하여 공격 IP 차단
- 임시 회선 증설, QoS 설정 변경 등 가용 트래픽 증가 설정 적용
- 공격 유형 분석 후 관련 패턴 업데이트 및 적용
- 공격 IP, 공격 기법에 대하여 교육(행정)기관에 전파하여 추가 피해 및확산 방지 조치 실시

(나) 대응조치

(1) 침해사고 조사 실시

- 공격 IP 현황 및 공격 방법 분석
- 보안장비 정책 확인
- 현장 확인이 필요하다고 판단되는 경우 교육부 「정보보호 점검반」 요청

(2) 시스템 복구

- 보안장비 임계치 조정
- 피해시스템 및 연계시스템 서비스 점검 실시

(3) 신규 탐지규칙 개발 및 적용

- 공격 IP현황 및 공격 탐지 로그 등 관련 자료 교육부(ECSC)로 발송
- 신규 탐지규칙 개발 후 교내 적용

(다) 후속조치

(1) 결과종합 및 보고

- 침해사고 경과 및 결과 종합 보고 실시

(2) 재발방지대책 수립

- 피해시스템의 보안취약점 점검 실시
- 정보보호팀은 재발방지대책을 수립하여 정보보안책임자 보고 및 교육부(ECSC) 통보

(3) 보안권고문 전파

- 추가 피해 발생 및 중요 사안일 경우 차단 가능한 정보를 포함하여 교내 보안권고문 전파 실시
- 상황의 중요도에 따라 이행결과 확인

4. '악성코드 감염' 조치내용

(가) 초동조치

(1) 침해사고 신고 및 증적 자료 보존

- 정보보호팀은 침해사고 발생 시 정보보호책임자에게 보고하고 교육부(ECSC)에 즉시 유선 신고 및 정보공유시스템에 등록
- 피해 PC 전원 유지, PC 변경행위(OS 재부팅, 자료삭제 등) 금지
- 1년 이내의 보안장비(방화벽, IPS 등) 로그 확보

(2) 확산방지 조치

- 네트워크 절체 등 피해 PC 격리 및 백신 점검 실시

※ 네트워크 절체 시 방화벽을 이용한 논리적 절체가 아닌 실질 케이블 절체

(나) 대응조치

(1) 침해사고 조사 실시

- 1년 이내 보안장비 로그 분석 실시
- 악성 파일 경로 확인 및 샘플 채증
- 비정상 프로세스 및 응용프로그램 실행 여부 점검
- 백신 점검 결과 분석
- 현장 확인이 필요하다고 판단되는 경우 교육부 「정보보호 점검반」 요청

(2) 시스템 복구

- 피해PC 포맷 및 백신 점검 실시

(3) 신규 탐지규칙 개발 및 적용

- 수집된 악성 파일 등 관련 자료 교육부(ECSC)로 발송
- 신규 탐지규칙 개발 후 교내 적용

(다) 후속조치

(1) 결과종합 및 보고

- 침해사고 경과 및 결과 종합 보고 실시

(2) 재발방지대책 수립

- 피해시스템의 보안취약점 점검 실시
- 정보보호팀은 재발방지대책을 수립하여 정보보안책임자 보고 및 교육부

백석대학교 BAEKSEOK UNIVERSITY

(ECSC) 통보

(3) 보안권고문 전파

- 추가 피해 발생 및 중요 사안일 경우 차단 가능한 정보를 포함하여 교내 보안권고문 전파 실시
- 상황의 중요도에 따라 이행결과 확인

부 칙

이 지침은 2003년 4월 1일부터 시행한다.

부 칙

이 지침은 2004년 8월 1일부터 시행한다.

부 칙

이 지침은 2005년 9월 1일부터 시행한다.

부 칙

이 지침은 2006년 3월 1일부터 시행한다.

부 칙

이 지침은 2007년 3월 1일부터 시행한다.

부 칙

이 지침은 2008년 3월 1일부터 시행한다.

부 칙

이 지침은 2009년 3월 10일부터 시행한다.

부 칙

이 지침은 2009년 3월 7일부터 시행한다.

부 칙

이 지침은 2010년 3월 7일부터 시행한다.

부 칙

이 지침은 2011년 3월 7일부터 시행한다.

부 칙

이 지침은 2013년 5월 1일부터 시행한다.

부 칙

이 지침은 2016년 7월 1일부터 시행한다.

부 칙

이 내규는 2018년 9월 1일부터 시행한다.

부 칙

이 지침은 2019년 1월 1일부터 시행한다.

부 칙

이 지침은 2020년 5월 15일부터 시행한다.

부 칙

이 지침은 2022년 2월 1일부터 시행한다.

부 칙

이 지침은 2023년 7월 18일부터 시행한다.

백석대학교 BAEKSEOK UNIVERSITY

붙임

1. 침해사고 대응 조직도

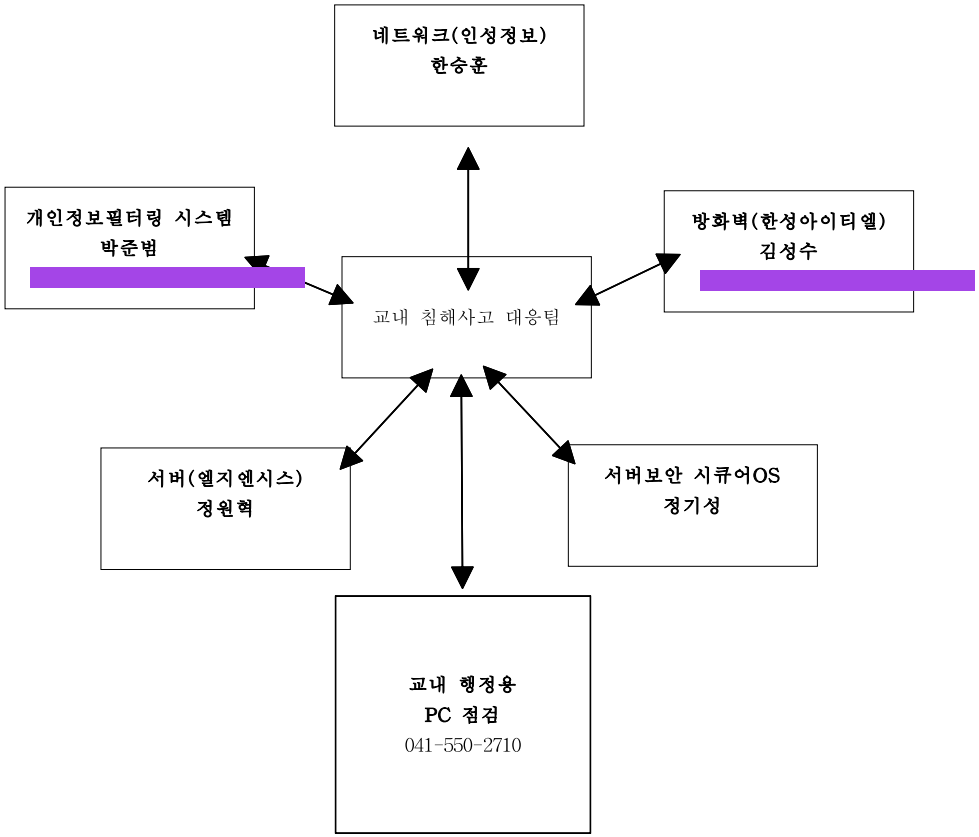
가. 자체대응반 비상연락망

갱신일: 20223.07.

구성원	담당	직급명(업무)	담당자	연락처	email
비상 총괄반	반장	보안담당관 (총무처장)	주희철	010	.kr
	반원	총무팀장	육경철	010	kr
	반원	정보보안담당관 (전산정보원장)	홍경호	010	.kr
	반원	전산정보원 부원장	이수연	010	.kr
	반원	정보보호팀장	이문재	010	kr
	반원	전산개발운영팀장	노남철	010	kr
비상 대응반	반장	정보보안담당관 (전산정보원장)	홍경호	010	.kr
	대응팀 총괄	정보보호팀장	이문재	010	kr
	복구팀 총괄	전산개발운영팀장	노남철	010	kr
	대응팀	DB	홍승우	010	c.kr
		네트워크	김상원	010	c.kr
		홈페이지	심수옥	010	.kr
	복구팀	DB	유재성	010	kr
		네트워크	김동근	010	.kr
		홈페이지	심수옥	010	.kr

백석대학교 BAEKSEOK UNIVERSITY

나. 교내 서비스 관련 업체 비상 연락망



서비스명	담당자	연락처	email	업 체
방화벽	김성수	010	kr	한성아이티엘
웹방화벽	정기성	010	21.com	에이텍정보기술
개인정보필터링	박준범	010	i.com	이지서티
서버	정원혁	010	s.com	엘지엔시스
서버보안	정기성	010	21.com	에이텍정보기술
네트워크	한승훈	010	o.co.kr	인성정보
V3	최준태	010	om	(주)위포

다. 국가 기관 연락처

기관명	신고전화	비고
국가정보원	☎ 111	
교육사이버안전센터	☎ 053-714-0777	

라. 정보시스템(정보전산원) 복구 순위

1. 정보시스템의 중요도 평가 기준

정보자산의 중요도 평가는 정보보호의 3대 요소인 기밀성, 무결성, 가용성의 정도를 고려하여 수행합니다.

보안 요구사항	내 용	보안 등급
기밀성	허가되지 않은 사용자(개체)에게 민감하거나 중요한 정보가 노출되지 않는 것을 말한다.	3단계 분류
무결성	허가되지 않은 사용자(개체)에 의한 정보의 변경, 삭제, 생성 등을 방지하는 것을 말한다.	3단계 분류
가용성	정상적인 사용자(개체)가 시스템을 사용하고자 할 때 거부해서는 안 된다는 것을 말한다.	3단계 분류

구 분	기 준	보안 등급
기밀성	매우 제한적인 권한 설정에 따라 이용이 통제되는 민감한 정보, 학교기밀정보, 학사정보, 입찰정보 등	3
	결재선상(담당, 팀장 등 직속관리자)에 있는 임직원에게만 허용되는 정보, 방화벽 규칙, 견적서 등	2
	외부에 공개되더라도 큰 영향을 주지 않는 정보	1
무결성	정보를 불법적인 방법으로 변경하거나 손상시키는 경우 업무에 매우 큰 영향을 주며 자칫 업무 기능 전체의 마비에까지 이를 수 있음	3
	정보를 불법적인 방법으로 변경하거나 손상시키는 경우 업무에 큰 영향을 끼침	2
	정보를 불법적인 방법으로 변경하거나 손상시키더라도 업무에 큰 영향을 주지 않음	1
가용성	매일 95% 이상의 시간 동안 정보, 시스템, 네트워크에 대한 인가된 접근이 가능해야 함	3
	모든 근무일에 걸쳐 표준 근무 시간 동안 정보, 시스템, 네트워크에 대한 정상적인 접근이 가능해야 함	2
	모든 근무일에 걸쳐 표준 근무 시간의 25% 이상 시간동안 정보, 시스템, 네트워크에 대한 정상적인 접근이 가능해야 함	1

2.

정보시스템의 복구 우선 순위(정보전산원)

분류 등급	분류 기준	대상 시스템	비고
1등급	학사 행정 서비스	메인 DB, 백본 네트워크, DNS 등	
2등급	행정 업무 서비스	대표 홈페이지, 가상서버 등	
3등급	행정 업무 지원 서비스	정보보호시스템, 물리적 장치 등	
4등급	기타 서비스	그 외 서비스 서버 등	

【 별지 제1호 서식 】

사 고 신 고

기 본 정 보			
기 관 명		부 서	
성 명		직 위	
전자우편			
연 락 처			
사 고 내 용			
사고 일시	년 월 일 시 분	피해IP주소	
피해시스템 용도	* 뒷장의 '가.시스템 분류' 기호 입력	운영체제	■ 윈도우 □ 유닉스 □ 네트워크장비 상세버젼정보:
사고 유형	* 뒷장의 '나.사고 유형' 기호 입력	피해범위	대 * 피해시스템이 여러대인 경우 피해숫자 기입
사고 내용			
조 치 내 용			
공격자 정보			
피해 현황			
긴급조치 실시사항			
관련보안제품 운영현황			
그 밖에 사고 관련 내용을 구체적으로 서술			
0000			

※ 이메일(webmaster@bu.ac.kr) 또는 Fax(041-550-0866)로 사고신고 바랍니다.

1. 시스템 분류 목록

기호	시스템 분류	설 명
가	웹서버	기관의 홈페이지 운영 및 웹서비스를 제공하는 서버
나	전자우편 서버	전자우편 송수신을 위해 운영하는 서버
다	DB/업무서버	홈페이지 및 업무지원을 위한 데이터베이스 서버
라	개발/임시서버	개발 및 운영 테스트를 위하여 사용하는 임시 서버
마	통신전송장비	라우터, 스위치 등 통신전송장비 일체
바	보안장비	방화벽, IDS, VPN 및 백신서버 등 정보보안제품 일체
사	개인/업무PC	기관내 사용자의 PC
아	교육/임시PC	교육장 또는 공용 작업을 위해 여러 명이 사용하는 PC
자	기타	위의 시스템 용도에 없는 경우 서술식으로 기술

나. 사고 유형 목록

기호	사고 유형	설 명
A	경유지 악용	타기관으로부터 해킹시도 항의를 받았거나, 시스템 점검 중 해킹흔적 또는 해킹툴이 설치되어 타시스템에 접속한 기록이 발견되었을 경우
B	자료훼손 및 유출	내부 시스템의 자료가 변조가 되었거나, 대량의 데이터가 외부로 무단송신된 흔적이 발견되었을 경우
C	악성코드 감염	기관내의 서버 PC에서 악성코드가 발견되었을 경우
D	홈페이지 변조	기관의 홈페이지가 변조되었을 경우
E	홈페이지 접속 불가능	기관의 홈페이지 서버 또는 네트워크 이상으로 인해 홈페이지 접속이 불가능 할 경우
F	서비스거부공격 피해	불특정 다수의 IP로부터 접속시도 또는 대량 트래픽이 일시에 유입될 경우
G	시스템 파괴	내부 시스템의 자료가 삭제되어 사용이 불가능한 경우
H	해킹메일	해킹메일 열람 및 해킹메일 내 악성파일 실행의 경우
I	기타	위의 사고유형에 포함되지 않을 경우 서술식으로 기술

【 별지 제2호 서식 】

경 보 문

제 목	이라크테러단체의 사이버위협 관련 '관심' 경보 발령
발 령 일	2023년 00월 00일 14시 00분
개 요	◦ OOO의 한 테러단체가 사이버공격을 위하여 Liberation 웜을 첨부파일로포함하는 전자우편을 대량 살포하고 있으므로, 전자우편 확인시 주의 요망
대 응 책	◦ 교육(행정)기관 보안담당자 1. '개인사용자 대응책'을 참고하여, 기관내 사용자에게 대응책을 작성, 배포 2. 전자우편 서버의 Filter를 전송하여 송신자 도메인이 state.gov인 경우, 수신하지 않도록 설정 3. TCP 25, 139 포트의 트래픽에 대해 모니터링을 강화하고, 해당 포트에 대한패킷을 대량 발송하는 IP를 확인하여 백신으로 점검 - 중간 생략 - ◦ 개인 사용자 1. state.gov로부터 전자우편 수신 가능성이 없는 사용자는 해당 전자우편을열어보지 말고 즉시 삭제할 것 2. 'netstat-an'을 이용하여 TCP 139 연결세션이 대량 3. 공유폴더 사용시 영문·숫자·기호를 혼합한 패스워드 사용
관련정보	◦ OOO 웜 급속 확산, 위협등급 상향조정

※ 제목과 발령일 부분은 경고발령 수준에 따라 해당 경보수준 색으로함

관심 - 주의 - 경계 - 심각

【 별지 제3호 서식 】

상 황 통 보 문

기 관 사 항			
기 관 명		부 서	
성 명		직 위	
전자우편			
연 락 처	전화:	H.P:	Fax:

조 치 사 항			
경보수준	관 심		
발 령 일	0000년 00월 00일 00시 00분	수 신 일	0000년 00월 00일 00시 00분
조치사항 요약	◦ 기관내 사용자에게 대응책을 작성, 배포 ◦ 이메일 서버의 Filter를 적용 ◦ 기관내 감염피해 확인 (피해대수 및 감염PC의 IP)		
조치대상 목록			
조치결과			
특이사항			

※ 이메일(webmaster@bu.ac.kr) 또는 Fax(041-550-0866)로 사고신고 바랍니다.

※ 제목과 발령일 부분은 경고발령 수준에 따라 해당 경보수준 색으로함

관심 - 주의 - 경계 - 심각

【 별지 제4호 서식 】

피해 정보시스템 목록표

시스템명	중요도	설명			우선순위	처리결과
		현장복구	원격복구	현장 · 원격		
00시스템	B	O			상	완료

※ 우선순위는 상-중-하로 구분함

백석대학교 BAEKSEOK UNIVERSITY