「사이버안전분야」
위기대응 실무매뉴얼

과학기술부

「사이버안전분야」
위기대응 실무매뉴얼

과학기술부

이 매뉴얼은「국가위기관리기본지침(대통령훈령 제124호)」 및 「국가 사이버안전 위기관리 표준매뉴얼」을 근거로「사이버안전」 위기상황 발생 시 과학기술부가 적용할 세부 대응절차 및 제반 조치사항 등을 규정하고 있으며, 관련 기관과의 협의하에 작성되었음.

- 목 차 -

Ⅴ. 위기관리 업무수행 체계

Ⅵ. 위기경보 수준별 대응요령

Ⅶ. 위기대응 조치 및 절차

부록

붙 임

Ⅰ. 일 반 사 항

Ⅰ. 일반 사항

1. 개 요

과학기술부「사이버안전 분야 위기대응 실무 매뉴얼」은 「위기관리 표준 매뉴얼」에 따라 과학기술 소관분야에 대한 웜·바이러스 및 해킹 등 사이버공격에 의한 침해사고가 발생할 경우, 과학기술부(과학기술정보보호센터 및 실무기관 포함)의 대응절차와 조치 사항을 규정한 것임

2. 관련 법규

가. 「국가정보원법」(법률 제8050호)

나. 「국가위기관리기본지침」(대통령훈령 제124호)

다. 「국가사이버안전관리규정」(대통령훈령 제141호)

라. 「과학기술기본법」(법률 제7989호)

마. 「국가연구개발사업의 관리 등에 관한 규정」 (대통령훈령 제19872호)

3. 적용 범위

가. 웜·바이러스, 해킹 등 사이버공격으로 인한 정보통신망 마비, 중요자료 유출 등 위기상황이 발생할 경우 적용

나. 과학기술 소관 분야에 침해사고가 발생하여 과학기술부(과학기술정보보호센터 및 실무기관 포함)의 정보통신망 마비, 서비스 중단 등의 사태에 적용

4. 용어 정의

구 분	내 용
국가위기	국가 주권 또는 국가를 구성하는 정치·경제·사회·문화체계 등 국가의 핵심요소나 가치에 중대한 위해가 가해질 가능성이 있거나 가해지고 있는 상태
위기관리	국가위기를 사전에 예방하고 발생에 대비하며 위기 발생시에는 효과적인 대응 및 복구를 통하여 그 피해와 영향을 최소화함으로써 조기에 위기 이전상태로 복귀시키고자 하는 제반 활동
주관기관	해당 위기에 대한 정부의 위기관리 활동에 주 책임을 지는 정부기관 ※ 국가정보원 (국가·공공분야), 정보통신부 (민간분야), 국방부 (국방분야)는 각각 해당 분야에 주 책임 ※ 국가정보원은 국가사이버안전 정책 및 관리 총괄·조정
중앙기관	해당 위기에 대한 정부의 위기관리 활동에 있어 주관기관의 활동을 지원하고 협조하는 중앙행정기관
실무기관	위기관리의 대상이 되는 기능·시설을 직접 관리, 운영하고 사이버 침해사고 발생시 1차적으로 대응·복구를 수행하는 과학기술부 소관·정부출연연구기관 및 유관기관
전문기구	보안관제·침해사고대응·정보공유분석 등 사이버안전 업무를 수행하는 기구 ※ 국가사이버안전센터, 국방정보전대응센터, 침해사고대응지원센터, 과학기술정보보호센터
위 기 관 리 활 동	① 예방 : 위기요인을 사전에 제거하거나 감소시킴으로써 위기 발생 자체를 억제하거나 방지하기 위한 일련의 활동 ② 대비 : 위기 상황 하에서 수행해야 할 제반 사항을 사전에 계획, 준비, 교육, 훈련함으로써 위기 대응능력을 제고시키고, 위기발생시 즉각적으로 대응할 수 있도록 태세를 강화시켜 나가는 일련의 활동

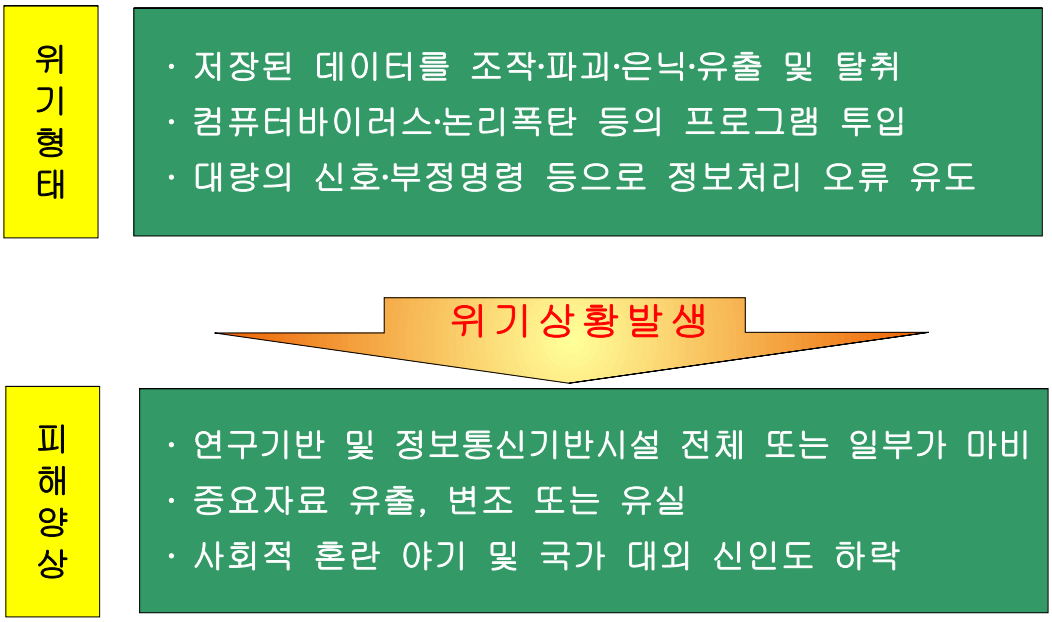
구 분	내 용
	③ 대응 : 위기 발생시 국가의 자원과 역량을 효율적으로 활용하고 신속하게 대처함으로써 피해를 최소화하고 2차 위기 발생 가능성을 감소시키는 일련의 활동 ④ 복구 : 위기로 인해 발생한 피해를 위기 이전의 상태로 회복시키고, 평가 등에 의한 제도개선과 운영체계 보완을 통해 재발을 방지하고 위기관리 능력을 향상시키고자 하는 일련의 활동
위 기 경 보	① 관심(Blue) : 징후가 있으나 그 활동수준이 낮으며 가까운 기간 내에 국가위기로 발전할 가능성도 비교적 낮은 상태 ② 주의(Yellow) : 징후 활동이 비교적 활발하고 국가위기로 발전할 수 있는 일정 수준의 경향성이 나타나는 상태 ③ 경계(Orange) : 징후 활동이 매우 활발하고 전개속도, 경향성 등이 현저한 수준으로서 국가위기로의 발전 가능성이 농후한 상태 ④ 심각(Red) : 징후 활동이 매우 활발하고 전개속도, 경향성 등이 심각한 수준으로서 위기발생이 확실시 되는 상태
정보 통신망	전기통신설비를 활용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계
정보통신 기반시설	국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 정보통신망
사이버 안전	사이버공격으로부터 정보통신기반시설을 보호함으로써 정보통신기반시설과 정보의 기밀성·무결성·가용성 등 안전성을 유지하는 상태

구 분	내 용
사이버 공격	해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스방해 등 전자적 수단에 의하여 정보통신기반시설을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 일체의 공격 행위
해 킹	접근을 허가받지 않은 정보시스템에 불법으로 침투하거나 허가되지 않은 권한을 불법으로 갖는 행위
서비스 거부	시스템에 과도한 부하를 일으켜서 정보시스템의 사용을 방해하는 공격 방식으로서 분산서비스 거부공격 또는 분산반사 서비스 거부공격 등으로 구분
악성코드	컴퓨터바이러스, 웜, 트로이목마와 같이 시스템에 해를 입히거나 시스템을 방해하기 위해 특별히 설계된 악의적인 컴퓨터 프로그램이나 실행 가능한 코드
바이러스	감염파일의 실행을 통해서 확산되며, 정상적인 파일이나 부트 영역에 침입하여 바이러스코드를 추가하는 형태로 파일을 감염시키는 악성프로그램의 일종
웜	자기 스스로 복제능력을 갖고 네트워크를 통해 생성되어 확산되는 악성프로그램의 일종으로 파일을 감염시키지는 않으며 레지스트리에 자신을 등록하는 방식으로 시스템을 감염시켜 컴퓨터가 시작될 때 스스로 동작함
트로이목마	자기복제 능력은 없으나, 정상 기능의 프로그램으로 가장하여 프로그램 내에 숨어있는 코드조각으로, 의도하지 않은 기능을 수행하는 컴퓨터 프로그램 또는 실행 가능한 코드

Ⅱ. 위기 형태 및 경보

Ⅱ. 위기 형태 및 경보

1. 위기 형태 및 피해 양상



2. 전개 양상

구 분	내 용
징후 발견	• 보안취약점 공개 및 이를 악용한 해킹도구 발견 • 위험도가 높은 웜·바이러스 출현 • 의도적인 불법 침입 시도 탐지
초기 진행	• 국내 웜·바이러스 및 해킹 피해 발생 • 정보통신기반시설 소통량이 비정상적으로 급증
부분 진행	• 국내 웜·바이러스 및 해킹 피해 증가 • 핵심기반시설에서 자료유출 가능한 악성코드 감염 피해 발생 • 정보통신기반시설 소통량 급증에 따른 국지적인 장애 발생
전면 확산	• 대규모 웜·바이러스 및 해킹 피해 발생 • 일부 핵심기반시설에서 자료유출 피해 발생 • 전국적으로 정보통신기반시설 마비 확산
위기 발생	• 국가 주요 정보통신기반시설 마비 • 국가 중요자료 유출

3. 위기 경보

가. 위기경보 수준

구 분	판 단 기 준	비 고
관 심 (Blue)	o 위험도가 높은 웜·바이러스 등 악성코드 및 해킹 기법 출현으로 피해 발생 가능성 증대 o 해외 피해확산 등 사이버위협의 국내 유입 가능성 증대	징후 활동 감시
주 의 (Yellow)	o 위험도가 높은 웜·바이러스 등 악성코드 및 해킹 기법 출현으로 피해 발생 o 과학기술분야 정보시스템 전반에 보안태세 강화 필요	협조 체계 가동
경 계 (Orange)	o 복수 국가기간망의 장애 또는 마비 o 웜·바이러스 등 악성코드의 급속한 확산으로 대규모 피해로 발전 가능성 증가	대비 계획 점검
심 각 (Red)	o 핵심기반시설·시스템 대상 피해 발생 o 지역적·부분적 피해 발생, 전국적 확산 가능성 증대 o 국가적 차원에서 공동 대처 필요	즉각 대응 태세 돌입

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

나. 위기경보 절차

(1) 국가정보원(NCSC)에서 위기 경보를 발령한 경우 과학기술부는 과학기술정보보호센터에 위기경보 발령 사실을 전파

(2) 과학기술정보보호센터는 위기경보 발령 사실을 실무기관에 전파

(3) 실무기관은 위기경보 발령 사실을 소속원에게 전파

Ⅲ. 위기관리 기본방향

Ⅲ. 위기관리 기본방향

1. 목 표

가. 과학기술분야 사이버위협 조기경보체계 확립 및 사전 예방

나. 위기발생시 피해 최소화 및 신속한 복구

2. 방 침

가. 사이버공격에 대한 과학기술부·과학기술정보보호센터·실무기관간 협력체제 강화

나. 과기부 차원의 사이버위협 정보의 수집·분석·전파의 체계화

다. 사이버공격 조기경보 발령전파 및 대응체계 확립

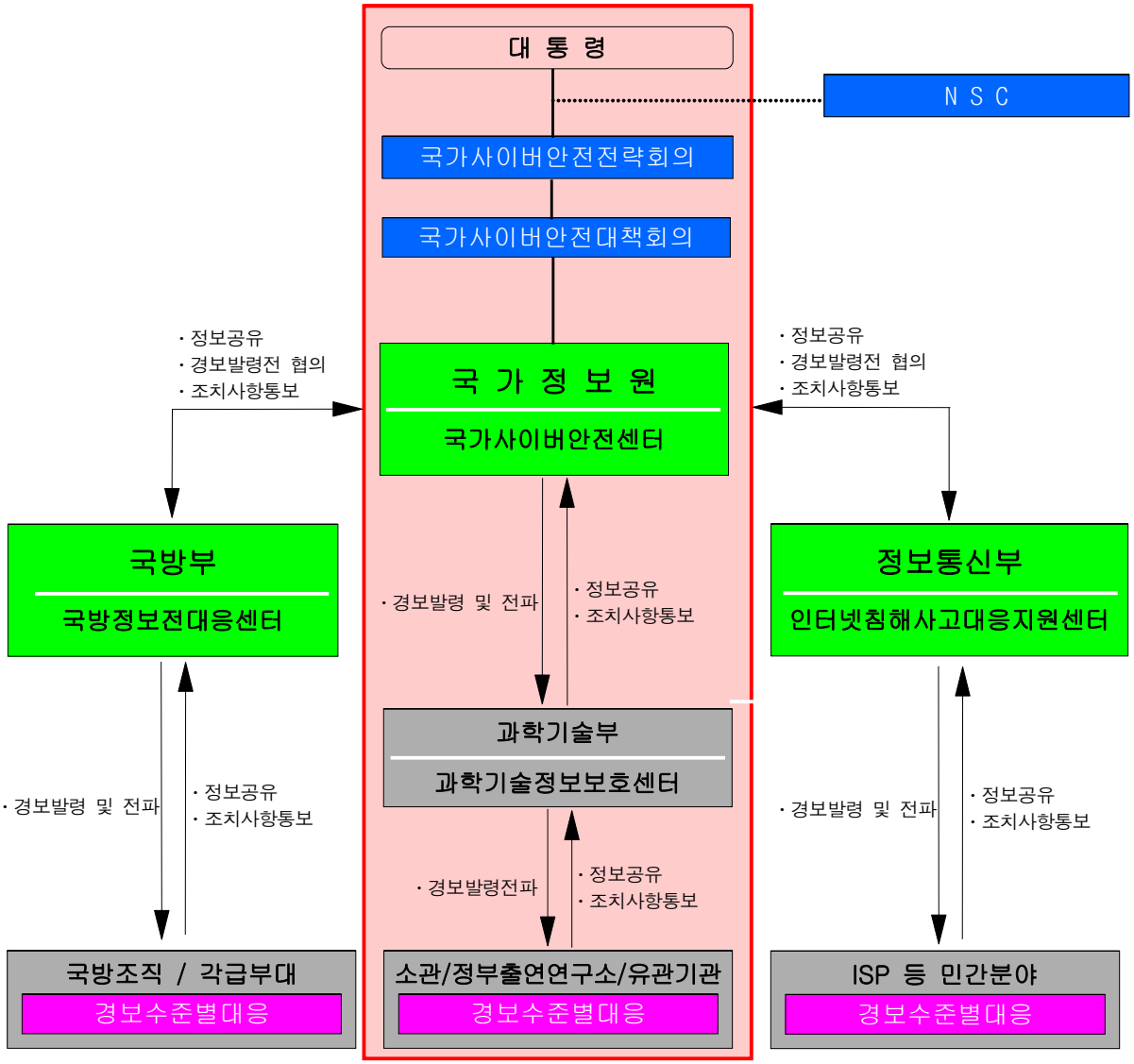
라. 과학기술 연구기반시설에 대한 사이버위협 감시 강화

마. 사이버안전 관리 실태 점검 및 보완

바. 대규모 위기사태 발생시 합동조사 및 복구

3. 위기관리체계

가. 종합체계도



나. 기관별 책임/역할

구 분	내 용
N S C	o 국가사이버안전 보호체계 구축에 관한 기획·조정 o 국가위기 경보체계 구축·운영에 관한 기획·조정 o 관련상황 모니터링 및 종합
국가사이버안전 전략회의	o 국가사이버안전체계 수립 및 개선 o 국가사이버안전 관련 정책 및 기관간 역할 조정 o 국가사이버안전 관련 대통령 지시사항에 대한 조치방안 강구 ※ 위원: 외교·법무·국방·행자·정통부 차관, NSC 사무처장
국가사이버안전 대책회의	o 국가사이버안전 관리 및 대책 방안 강구 o 전략회의의 결정사항에 대한 시행 방안 강구 o 전략회의로부터 위임받은 사항 심의 o 위기발생시 정책결정 및「합동조사팀」·「복구지원팀」지휘 ※ 위원: 전략회의 위원기관 실·국장급
국가정보원 (국가사이버안전센터)	o 국가사이버안전 정책 및 관리 총괄·조정 o 전략회의 및 대책회의의 운영에 대한 지원 o 국가·공공분야 사이버위협 위기경보 발령 및 각 분야 위기경보수준 협의 o 사이버위협 관련 정보의 총괄 관리(수집·분석·전파) o 국가·공공기관 정보통신기반시설의 안전성 확인 o 국가사이버안전매뉴얼 작성·배포 o 국가·공공분야 사고신고 접수, 사고조사 및 복구 지원 o 위기발생시 범정부적 합동조사·복구지원팀 운영계획 총괄
과학기술부 (과학기술정보보호센터)	o 과학기술 관련 사이버위협 관련 정보의 총괄 관리(수집·분석·전파) o 실무기관의 연구기반시설 및 정보통신기반시설의 안전대책 수립·시행 및 지도감독 o 사이버안전 실무매뉴얼 작성·배포 o 사고 신고 접수 및 사고 통보 o 사고 복구 및 피해확산방지를 위한 자체 사고 조사 및 복구 지원 처리 협조

구 분	내 용
국 방 부 (국방정보전 대응센터)	o 국가사이버안전 정책에 따른 국방분야 사이버안전 관리 총괄·조정 o 국방분야 위기평가/경보체계 운영, 상황종합 및 처리 o 국방분야 정보통신기반시설의 안전성 확인 o 국방분야 사이버안전 실무매뉴얼 작성·배포 o 범국가적 합동조사·복구지원팀 활동 지원(국방분야 주관)
정보통신부 (인터넷 침해사고 대응지원센터)	o 국가사이버안전 정책에 따른 민간분야 사이버안전 관리 총괄·조정 o 민간분야 위기평가/경보체계 운영, 상황종합 및 처리 o 정보통신서비스제공자와 집적정보통신시설사업자 대상 정보통신망 또는 집적정보통신기반시설 정보보호 안전진단 o 민간분야 사이버안전 실무매뉴얼 작성·배포 o 범국가적 합동조사·복구지원팀 활동 지원(민간분야 주관)
실무기관 **긴급대응반**	o 해당 기관의 연구기반시설 및 정보통신기반시설 안전 대책 수립 및 시행 o 사고 발생의 경우 적의 조치 후 과학기술부 및 과학기술정보보호센터에 통보 o 과학기술부·과학기술정보보호센터와 협조, 사이버안전 분야 위기관련 예방-대비-대응-복구 활동

Ⅳ. 위기관리 활동

Ⅳ. 위기관리 활동

1. 예 방

가. 중 점

(1) 과학기술 관련 사이버 안전대책 수립·시행

(2) 위기징후 실시간 감시, 위협정보 수집, 분석 및 전파

(3) 연구기반시설 및 정보통신기반시설에 대한 안전대책 수립

(4) 국내·외 사이버안전 관련기관과 공조

나. 세부 활동내용

(1) 평시·위기시 사이버안전대책 수립·시행

(가) 실무기관은 국가정보원에서 제공하는 평시 시스템 운용 안전기준에 따라 정기 점검을 시행

(나) 과학기술부는 안전기준의 이행 여부 확인 및 필요시 시정 조치 등을 권고

(다) 과학기술부 및 실무기관은 위기시에 대비한「위기대응 실무매뉴얼」을 작성

(2) 위기징후 실시간 감시 및 위협정보 수집·분석·전파

(가) 과학기술정보보호센터(과학기술분야)는 소관분야에 대해 24시간 사이버공격 및 위협 징후 감시

(나) 실무기관은 사이버위협 정보를 입수한 경우, 과학기술정보보호센터에 관련 정보를 통보

(다) 과학기술정보보호센터는 과학기술부에 통보

(라) 과학기술부는 국가정보원에 통보

(3) 연구기반시설 및 정보통신기반시설에 대한 안전대책 수립

(가) 실무기관은 연구기반시설 및 정보통신망 신·증설 등 환경 변화시 자체 보안대책을 강구하고 과학기술부에 보안성 검토를 의뢰

(나) 과학기술부는 실무기관의 보안성 검토 요청을 국가정보원에 의뢰

(4) 국내·외 사이버안전 관련기관과 공조

(가) 과학기술부와 과학기술정보보호센터는 국내·외 사이버안전 관련기관과 공조체제 강화 및 관련 정보 입수·전파

(나) 실무기관은 보안관제·침해사고대응·정보공유분석 등의 업무를 수행하는 과학기술정보보호센터와 협력창구 운영, 정보공유 체계 구축

다. 기관별 책임/역할

구 분	내 용
N S C 사무처	o 국가 사이버안전 위기관리 체계 구축·개선·조정 o 국가 사이버안전 위기관리 체계 부처 이행상태 확인
국가정보원 (국가사이버안전센터)	o 사이버안전 분야 국가정책 및 관리 총괄·조정 o 국가차원 사이버위협정보 총괄 관리(수집·분석·전파) o 국가·공공분야 24시간 사이버위협 및 공격 징후 감시 o 국가·공공분야 정보통신기반시설에 대한 안전성 확인 o 보안목표시설 등 중요시설에 대한 보안측정 실시 o 국가·공공분야 정보통신기반시설 신·증설시 보안성 검토
과학기술부	o 과학기술분야 정보통신기반시설에 대한 안전대책 준수 여부 확인 o 사이버 위협관련 정보입수시 국가정보원에 통보 o 위기시를 대비한 자체 사이버안전 실무매뉴얼 작성
과학기술정보보호센터	o 과학기술분야 24시간 사이버위협 및 공격 징후 감시 o 사이버 위협관련 정보입수시 과학기술부에 통보 o 사이버안전관련 산·학·연 연계체계 구축
실무기관	o 자체 사이버안전대책 수립 및 이에 따른 점검 및 예방 o 정보보호 전담 조직 및 인력 운영 o 사이버위협 관련정보 입수 및 사고 인지시 관련 내용을 과학기술정보보호센터에 통보

2. 대 비

가. 중 점

(1) 위기경보 발령 전파

(2) 실무기관 위기대응 능력 강화

(3) 사이버안전에 대한 교육 및 인식 제고

(4) 사이버 안전분야 국가위기관리 훈련/연습

(5) 위기상황 대비 Backup 및 대응책 강구

나. 세부 활동내용

(1) 위기경보 발령 전파

(가) 위기경보 발령의 경우 과학기술부는 과학기술정보보호센터에 위기경보 발령을 전파

(나) 과학기술정보보호센터는 실무기관에 위기경보 발령을 전파

(다) 실무기관은 소속원에게 위기경보 발령을 전파

(라) 문자메시지, 전자우편, 전화, 팩스, 홈페이지 등을 활용하여 신속하게 경보를 전파

(2) 실무기관 위기대응 능력 강화

(가) 백신 프로그램 및 정보보호시스템 의무적 설치

※ 정보보호시스템은 국가정보원의 인증 또는 보안성 검토를 필한 제품을 대상으로 선정

(나) 운영체제 보안패치 적용 및 응용 프로그램 업데이트

(다) 위기관리 실태 상시 점검체계 확립

(라) 사이버안전을 위한 위기관리 전담조직 운영계획 수립 자체 대응·복구를 위한 「자체대응반」 사전 구성

(3) 사이버안전에 대한 교육 및 인식 제고

(가) 과학기술부는 정보혁신협의회를 통해 실무기관 정보보호 담당자 대상으로 사이버 안전에 대한 교육과, 사이버안전에 관한 의견을 수렴하여 정책반영 수립체제 구축

(나) 실무기관은「위기대응 실무매뉴얼」에 따른 실행교육 실시

(다) 정보혁신협의회 세미나 개최 및 지원

o 사이버안전분야 민·관협의회 적극 활용

(4) 사이버 안전분야 국가위기관리 훈련/연습

(가) 국가정보원, 국회 등에서 실시하는 사이버공격 훈련/연습에 대비하여 대응계획 수립

(나) 범정부적 사이버공격 훈련/연습에 대비하여 대응계획 수립

(다) 사이버공격 훈련/연습 결과를 종합하여 보안취약점 개선·보완

(5) 위기상황 대비 Backup 및 대응책 강구

(가) 중요 자료 및 시스템의 복구를 위한 백업 실시

(나) 백업된 자료의 복구 테스트 등 비상시 시스템 복구 절차 마련

(다) 하드웨어 및 소프트웨어 업체와의 비상연락체계 점검

다. 위기경보 수준별 기관의 책임/역할

(1) 관 심(Blue)

구 분		내 용
징 후		o 위험도가 높은 웜·컴퓨터바이러스 및 해킹 기법 출현으로 피해 발생 가능성 증대 o 해외 피해확산 등 사이버위협의 국내 유입 가능성 증대
기관별 책임·역할	ＮＳＣ 사무처	o 위기징후 감시 및 모니터링 o 국가 사이버안전체계 가동 현황 점검
	국가정보원	o「자체위기평가회의」개최 및 국가·공공기관 대상 **관심** 경보 발령 o 국가차원 사이버위협 모니터링 강화 o 보안권고문 작성·배포 o 실무기관에 대처요령 및 백신 전파 o 사이버위협정보 공유(종합·분석·전파)
	과학기술부	o 과학기술정보보호센터에 **관심** 경보 전파 o 과학기술정보보호센터에 보안권고문 배포 o 자체 긴급대응반 가동 준비 및 필요시 긴급 운영 o 이상징후 및 사고발생 발견시 국가정보원에 통보 o 상황조치 관련 정보를 국가정보원에 통보
	과학기술정보보호센터	o 실무기관에 **관심** 경보 전파, 보안권고문 배포 o 과학기술부 긴급대응반 구성시 현장 지원 o 사이버위협 관제 모니터링 강화 o 새로운 악성코드, 취약점, 공격도구 정보 파악 o 상황조치 결과를 취합하여 과학기술부에 통보
	실무기관	o 소속원에게 경보전파 및 보안권고문 배포 o 자체 정보통신시스템 모니터링 강화 o 기술적 보안대책 시행 ※ 위기경보 수준별 기술적 보안대책 참조(p28)

(2) 주 의(Yellow)

구 분		내 용
징 후		o 위험도가 높은 웜·바이러스 및 해킹 기법 출현으로 피해 발생 o 네트워크 트래픽 급격 증가
기관별 책임·역할	NSC 사무처	o 모니터링 강화 및 관련기관간 협조체계 확인 o 범정부차원의 대비계획 확인
	국가정보원	o 국가·공공기관 대상 **주의** 경보 발령 o 전문기구간 협조 강화 o 피해확산 방지에 주력
	과학기술부	o 긴급운영반 운영에 대한 비상연락망 인원 및 연락처 점검 및 갱신 o 필요시 자체 긴급대응반 비상소집
	과학기술정보보호센터	o 과학기술부 긴급대응반 비상소집시 현장지원 o 실무기관과 연락체계(인원, 연락처 등) 점검 및 갱신
	실무기관	o 자체대응반 및 과학기술부·과학기술정보보호센터에 대한 비상연락망 인원 및 연락처 점검·갱신 o 기관내 정보보호시스템, 네트워크 장비등 시스템 및 프로그램 제공업체의 연락체계 점검 o 기술적 보안대책 시행 ※ 위기경보 수준별 기술적 보안대책 참조(p28)

※ 이전 단계(관심) 경보시의 조치를 지속 시행

(3) 경　계(Orange)

구　분		내　　용
징　후		o 복수 국가기간망에 피해 발생 o 웜·바이러스의 급속한 확산으로 대규모 피해로 발전 가능성 증가
기관별 책임·역할	NSC 사무처	o 국가위기수준평가회의 개최 (필요시) o 각 분야별 위기 대응태세 점검 및 조정
	국가정보원	o 국가·공공기관 대상 **경계** 경보 발령 o 범정부적 합동조사 및 복구지원팀 운영 검토 o「국가사이버안전대책회의」개최 o 실무기관 대비태세 확인 및 종합
	과학기술부	o 과학기술정보보호센터에서 제공한 사이버위협에 대한 대응요령을 모두 이행하고 있는지 재확인 o 긴급대응반 증원 및 대비계획 점검
	과학기술정보보호센터	o 실무기관에 제공한 사이버위협에 대한 대응요령을 모두 이행하고 있는지 재확인 o 과학기술부 긴급대응반 현장지원 인원 증원 o 급속한 피해 확산 우려시 네트워크 연결 차단 권고
	실무기관	o 필요시「자체대응반」운영 o 즉각적인 시스템복구를 실시하고 피해확산 차단 o 급속한 피해 확산 우려시 네트워크 연결 차단 o 기술적 보안대책 시행 ※ 위기경보 수준별 기술적 보안대책 참조(p28)

※ 이전 단계(주의) 경보시의 조치를 지속 시행

(4) 심　각(Red)

구　분		내　　용
징　후		o 핵심기반시설·시스템 대상 피해 발생 o 지역적·부분적 피해 발생, 전국적 확산 가능성 증대
기관별 책임·역할	NSC 사무처	o 국가위기수준평가회의 개최 o 각 분야별 위기대응태세 점검 및 조정
	국가정보원	o 국가·공공기관 대상 **심각** 경보 발령 o「국가사이버안전전략회의」개최 o 범정부적 합동조사 및 복구지원팀 가동
	과학기술부	o 사고대책본부를 구성하고 즉각 대응태세 돌입 o 합동조사팀, 복구지원팀 구성 o 범정부 합동조사팀, 복구지원팀 협조 및 지원
	과학기술정보보호센터	o 과학기술부 사고대책 본부 지원팀, Help-Desk팀 구성운영 o 합동조사팀, 복구지원팀 현장지원(조사 및 복구 주관)
	실무기관	o 「자체대응반」운영 및 즉각대응태세 돌입 o 기관내 PC 사용 최소화 및 오프라인 업무 권고 o 기술적 보안대책 시행 ※ 위기경보 수준별 기술적 보안대책 참조(p28)

※ 이전 단계(경계) 경보시의 조치를 지속 시행

※ 실무기관의 위기경보 수준별 기술적 보안대책

구 분	기 술 적 보 안 대 책
관 심 (Blue)	o 불필요한 서비스 점검 및 차단 또는 제거 o 백신프로그램 탐지패턴 업데이트 o 소프트웨어 보안패치 업데이트 o 라우터 및 침입차단시스템 차단규칙 점검 및 설정 o 주요시스템의 자원 사용량 및 프로세스 모니터링 o 취약시스템, 서비스 포트 등에 대한 모니터링 o 출처가 불분명한 이메일 삭제 o P2P, 메신저 등 파일교환 프로그램 사용 자제 o 중요자료에 대한 정기적 백업 실시 o 민감한 자료는 인터넷에 연결된 PC에 저장 금지 o PC내 공유폴더 사용 최소화 및 사용시 패스워드 적용
주 의 (Yellow)	o 스캐닝 활동 및 스캐닝 대상 호스트에 대한 감시 강화 o 특정 호스트에 대한 스캐닝 차단 o 악성코드 예상 유입경로 차단
경 계 (Orange)	o 서비스거부 공격 징후 포착시 공격 진행 차단 o 집중 모니터링 대상 취약점 재점검 o 중요자료 백업 실행 확인 및 복구테스트
심 각 (Red)	o 경보 관련 공격대상 서비스 포트 차단 o 국민생활에 기본이 되는 서비스를 제외한 일부 서비스 제한 o 네트워크 및 시스템에 대한 실시간 감시 및 대응

※ 각 단계는 이전 단계의 기술적 보안대책을 포함함. 단, 위기 상황에 따라 이전단계에서 다음 단계의 기술적 보안대책도 실행 가능

3. 대 응

가. 중 점

(1) 심각경보 발령의 경우 과학기술부 자체 합동조사팀을 가동하여 신속한 대응조치 및 범정부 합동조사팀 지원

(2) 과학기술정보보호센터 지원팀 구성 후 과학기술부 긴급대응반 현장지원을 통한 신속한 대응 조치

(3) 실무기관「자체대응반」에 의한 신속한 대응 조치

나. 세부 활동내용

(1) 심각경보 발령의 경우 과학기술부 자체 합동조사팀을 가동하여 신속한 대응조치 및 범정부 합동조사팀 지원

(가) 임 무

o 피해확산 차단

o 피해 상황의 종합 처리 및 보고

o 사고원인에 대한 조사 및 분석

o 실무기관「자체대응반」총괄 지휘 및 대응방법 전파

(나) 구 성

o 과학기술부, 과학기술정보보호센터, 피해기관 담당자, 산업체 전문가로 구성

- 정보보호 전문인력 풀(Pool)제 운영을 통해 산업체 정보보호 전문가 참여 유도

(다) 운 영

o 위기유형별 합동조사팀을 구성하고 합동조사를 주관

o 범정부 합동조사팀 지원

(2) 과학기술정보보호센터 지원팀 구성 후 과학기술부 긴급대응반 현장지원을 통한 신속한 대응 조치

(가) 피해기관의 사례 분석을 통해 예방 및 대응방안을 실무기관에 신속히 전파

(나) 과학기술부・실무기관간 비상연락체계 상시 가동

(3) 실무기관「자체대응반」에 의한 신속한 대응 조치

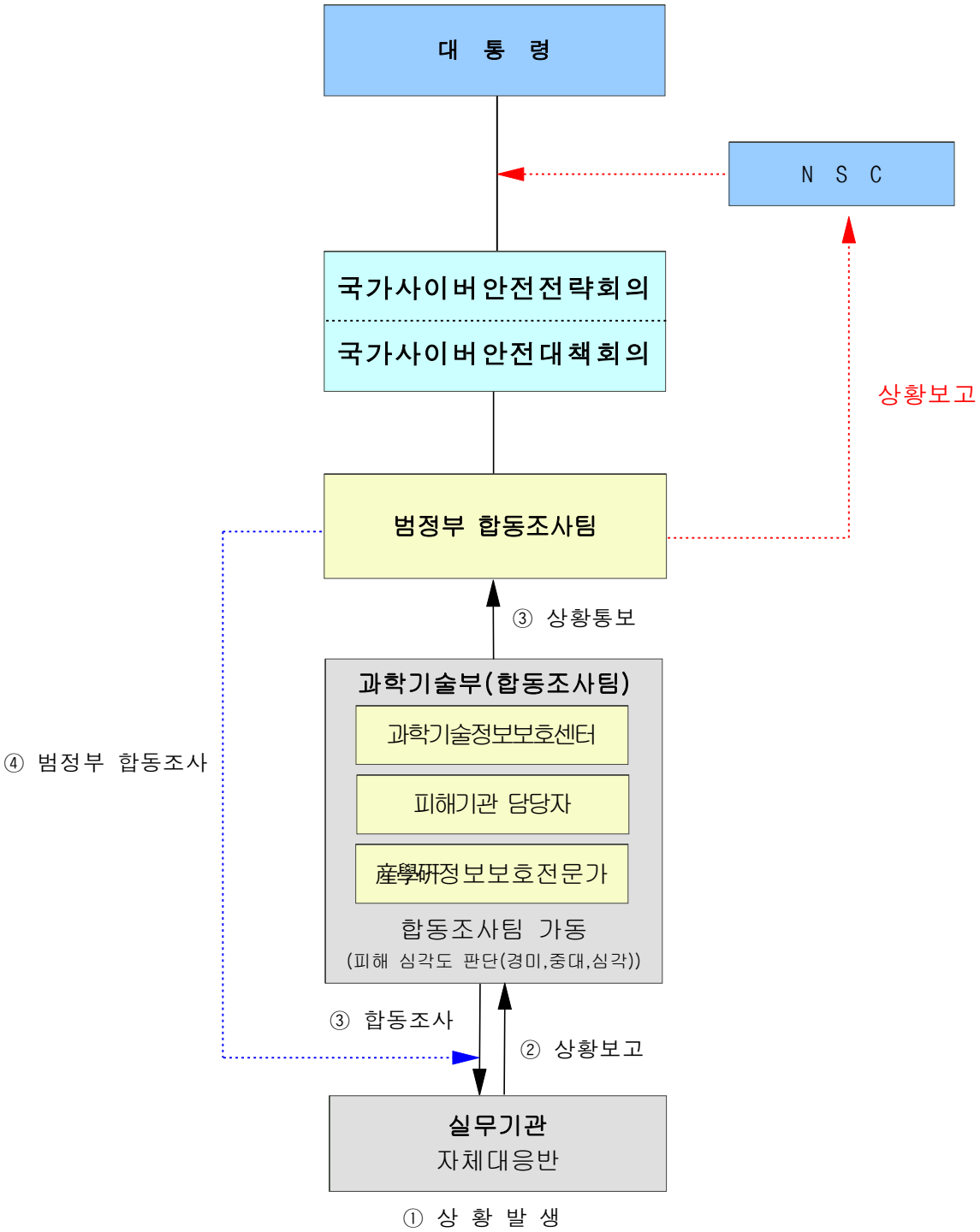
(가)「위기대응 실무매뉴얼」에 따라 상황별 대응책 적용

(나) 시스템 또는 전산센터 장애 발생시 백업시스템 또는 백업사이트 가동

(다) 사고조사 및 복구에 필요한 자료를 제공

(라) 신속한 초동조치 후 과학기술정보보호센터에 상황조치 통보

(마) 설치 및 업무수행 체계


대 통 령
N S C
국가사이버안전전략회의
국가사이버안전대책회의
상황보고
범정부 합동조사팀
③ 상황통보
과학기술부(합동조사팀)
과학기술정보보호센터
피해기관 담당자
産學硏정보보호전문가
합동조사팀 가동
(피해 심각도 판단(경미,중대,심각))
④ 범정부 합동조사
③ 합동조사
② 상황보고
실무기관
자체대응반
① 상 황 발 생

다. 기관별 책임/역할

구 분	내 용
N S C 사무처	o 위기상황 모니터링, 범정부 이행상태 종합 보고 o 부처·기관의 위기대응체계 가동 실태 확인
국가정보원	o 범정부적「합동조사팀」운영 총괄지원 및 결과 보고 o 필요시 국가사이버안전전략회의·대책회의 개최 o 국가차원 사이버공격 대응조치 강구 o 국내외 전문기구간 정보협력 강화
과학기술부	o 긴급대응반 및 과학기술부 합동조사팀 구성 운영 o 국가정보원(NCSC) 및 과학기술정보보호센터와 비상연락체계 유지 o 과학기술분야 피해 상황 종합 o 범정부 합동조사팀 지원
과학기술정보 보호센터	o 보안관제 강화 및 초기대응 o 과학기술부 합동조사팀 지원(과학기술분야 조사주관)
실무기관	o 자체대응반 구성운영 o 과학기술부 및 과학기술정보보호센터와 비상연락체계 유지 o「위기대응 실무매뉴얼」에 의거 단계별 대처요령 수행 o 사고조사 및 복구에 필요한 자료제공

4. 복 구

가. 중 점

(1) 과학기술부・과학기술정보보호센터・실무기관간 긴밀한 협조

(2) 복구 절차에 따른 피해복구 수행

(3) 사고 재발 방지를 위한 보안대책 수립 및 시스템 개선

(4) 심각경보 발령의 경우 과학기술부 자체 복구지원팀 가동 및 범정부 복구 지원팀 지원

나. 세부 활동내용

(1) 과학기술부・과학기술정보보호센터・실무기관간 긴밀한 협조

(가) 경미한 사고는 피해 기관이 자체 복구

※ 피해복구 및 상황처리 완료시 과학기술정보보호센터에 통보, 과학기술정보보호센터는 과학기술부에 통보

(나) 중대한 사고는 과학기술부(과학기술정보보호센터) 지원하에 복구

(다) 심각한 사고는 범정부「복구지원팀」에 의해 복구

(2) 복구 절차에 따른 피해복구 수행

순서	절 차	세 부 내 용	
1	복 구 범 위 결 정	데이터 복구	o 시스템 내 데이터만 손상
		소프트웨어 복구	o 시스템 내 프로그램 및 운영체제에 오류 발생
		운영체제 재설치	o 운영체제 복구 불가능
		하드웨어 교체	o 시스템의 하드웨어 손상
2	우 선 순 위 결 정	복수의 피해복구 대상에 대한 복구 우선순위를 결정	
3	피 해 복 구	데이터 복구	o 백업 데이터로부터 자료 복원
		소프트웨어 복구	o 백신프로그램을 이용, 악성코드 제거 o 공격에 이용된 취약점 제거 o 응용프로그램 재설치 o 운영체제 복구
		운영체제 재설치	o 운영체제 및 응용프로그램 재설치 o 백업 데이터로부터 자료 복원 o 운영체제 재설치 완료 후 정상상태 복귀 확인
		하드웨어 교체	o 파손된 하드웨어 교체
4	사 후 관 리	o 시스템 재가동 후 일정기간 동안 모니터링 실시 o 처리결과 보고서 작성 o 일정기간동안 시스템 및 네트워크 주기적 재점검	

(3) 사고 재발 방지를 위한 보안대책 수립 및 개선

(가) 사고 원인 분석에 따라 보안취약점 검사 및 개선

(나) 사이버안전대책의 실효성 점검 및 수정·보완

(4) 심각경보 발령의 경우 과학기술부 자체 복구지원팀 가동 및 범정부 복구 지원팀 지원

(가) 임 무

o 피해 상황의 파악 및 복구 절차 수립·시행

o 심각한 피해의 경우 범정부「복구지원팀」과 연계, 복구활동 지원

o 피해 복구 및 사후 처리 결과 종합 보고

(나) 구 성

o 과학기술부, 과학기술정보보호센터, 피해기관 담당자 및 산업체 전문가로 구성

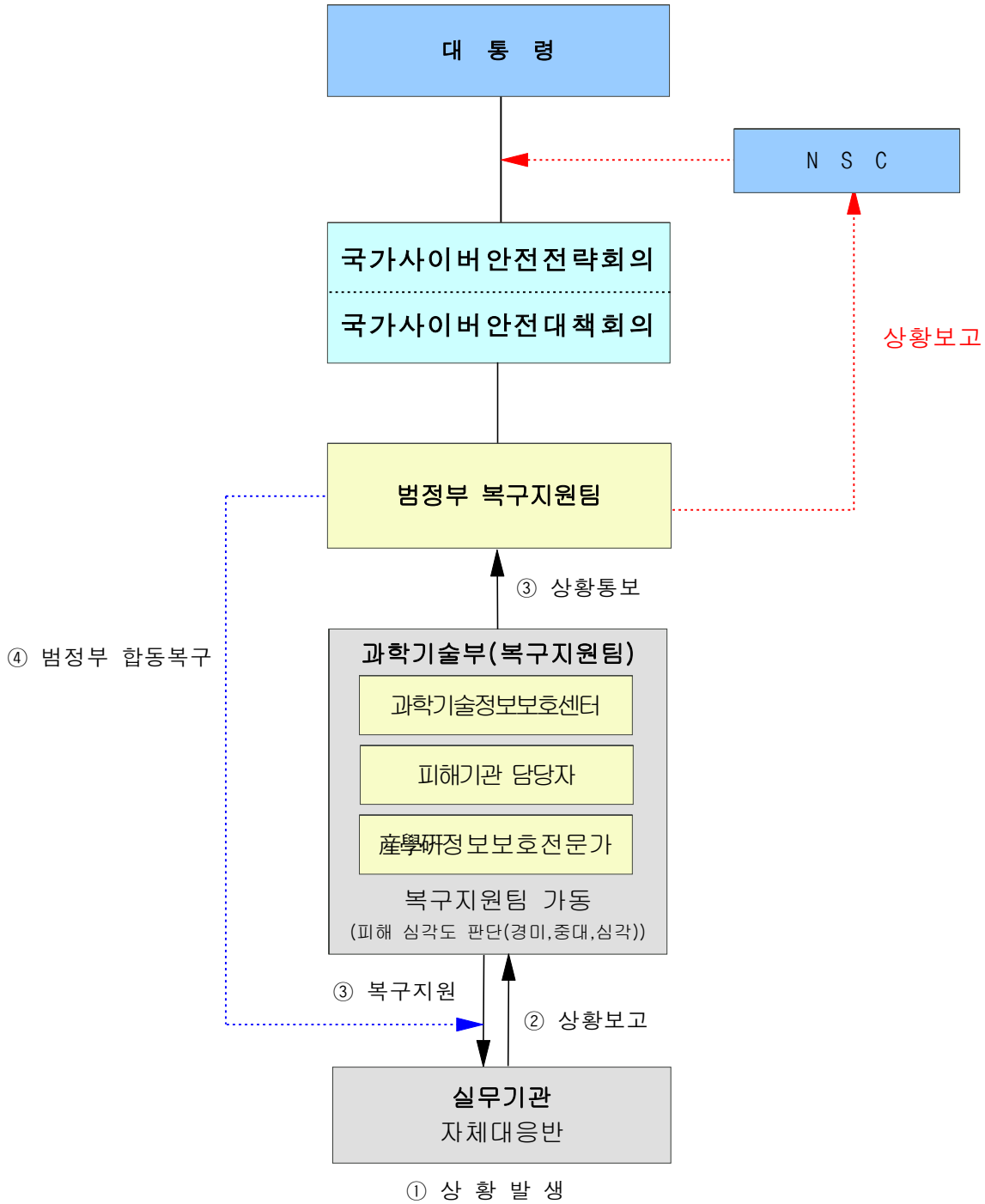
- 정보보호 전문인력 풀(Pool)제 운영을 통해 산업체 정보보호 전문가 참여 유도

(다) 운 영

o 복구유형에 따라 복구지원팀을 구성하고 합동복구를 주관

o 범정부 복구지원팀 지원

(라) 설치 및 업무수행 체계


대 통 령
N S C
국가사이버안전전략회의
국가사이버안전대책회의
상황보고
범정부 복구지원팀
③ 상황통보
④ 범정부 합동복구
과학기술부(복구지원팀)
과학기술정보보호센터
피해기관 담당자
産學硏정보보호전문가
복구지원팀 가동
(피해 심각도 판단(경미,중대,심각))
③ 복구지원
② 상황보고
실무기관
자체대응반
① 상 황 발 생

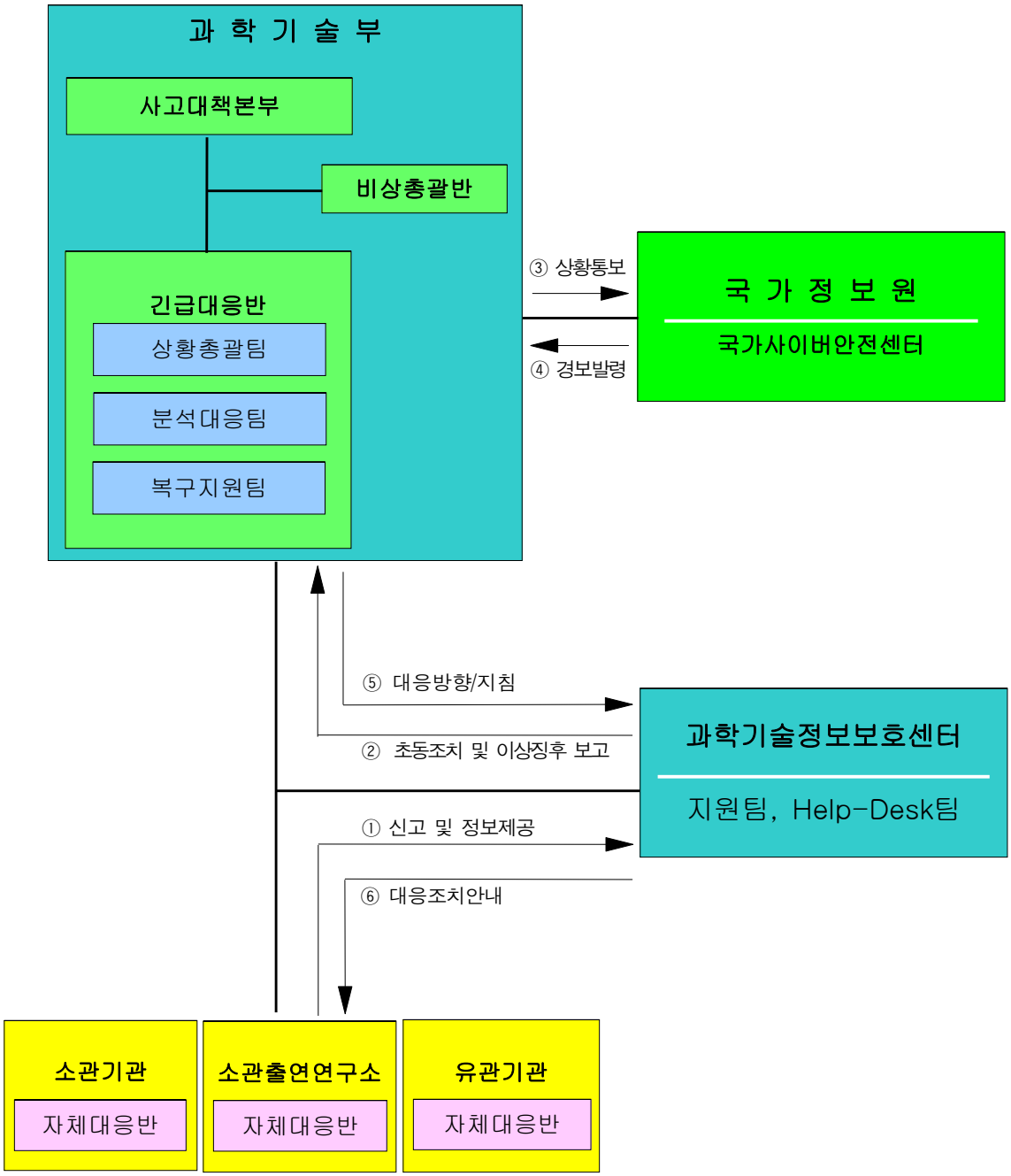
다. 기관별 책임/역할

구 분	내 용
N S C 사무처	o 피해 및 복구현황 종합 보고 o 범정부적 사이버안전 위기관리 체계 개선책 기획·조정
국가정보원	o 범정부적「복구지원팀」운영 주관 및 결과보고 o 필요시 국가사이버안전전략회의·대책회의 개최 o NSC와 정보 공유 o 피해복구 절차 수립 및 정보보호 전문인력 POOL제 운영
과학기술부	o 과학기술부 복구지원팀 구성 운영 o 국가정보원(NCSC) 및 과학기술정보보호센터와 비상연락체계 유지 o 과학기술분야 연구기반시설 및 정보통신기반시설 피해복구 o 과학기술분야 피해복구 상황 종합
과학기술정보 보호센터	o 보안관제 강화 및 초기대응 o 과학기술부 복구지원팀 지원(복구주관)
실무기관	o 자체대응반 구성운영 o 과학기술부 및 과학기술정보보호센터와 비상연락체계 유지 o「위기대응 실무매뉴얼」에 의거 단계별 대처요령 수행 o 복구에 필요한 자료제공 및 관련업무 지원

V. 위기관리 업무수행 체계

V. 위기관리 업무수행 체계

1. 위기대응 체계



2. 위기대응 기구

가. 과학기술부 사고대책본부

(1) 구성

(가) 위기 수준이 **심각**, 또는 그에 준하는 경우에 **사고대책본부(본부장 : 정책홍보관리실장)**를 구성·운영

(나) 사고대책본부 아래 **비상총괄반, 긴급대응반**(분석대응팀·복구지원팀·상황총괄팀)을 구성·운영

(다) 과학기술정보보호센터는 사고대책본부(긴급대응반) 지원

(라) 운영 장소 : 과학기술부 전산실(2동 7층 전산실 712호)

(2) 역할

(가) 피해현황 파악 및 피해복구 활동 총괄

(나) 사이버위협 정보수집·분석 및 우선조치사항 도출·조치

(다) NSC, 국정원 등 사이버 유관부처 등과 협조체제 유지

(3) 세부 임무

구 분	임 무
본 부 장 (정책홍보관리 실장)	o 과학기술정보보호센터 및 과기부내 사이버안전 관련 기능 총지휘 o 과학기술부 장·차관 보고
비상총괄반 (비상계획담당관)	o 위기관리계획 수립 및 긴급대응반 지원
긴급대응반 (정보화담당관)	o 긴급대응반 총괄 o 대응계획 수립 및 대응 결과 종합 o 보고서 작성 종합
상황총괄팀	o 피해신고 접수 및 보안관제 실시 o 위기경보 발령 및 해제 전파 o 유관기관 관제센터(NCSC, KrCERT 등)와 협력 o 보도자료 작성 및 언론 대응 o 사이버안전 유관기관과의 협조체계 구축
분석대응팀	o 사고원인 조사 및 피해규모 확인 o 공격기법·파급영향 분석 o 공격진원지 파악 및 차단대책 강구 o 범정부 합동조사 지원
복구지원팀	o 복구대책 수립 및 전파 o 현장파견 신속한 복구 및 보안기술 지원 o 정보보호 전문기관(백신업체 등)과의 정보 협력 o 사이버안전 유관기관 협력 o 범정부 복구지원 협조
과학기술정보보호센터 (팀장:과학기술정보보호센터장)	o 긴급대응반 현장지원 o 위기경보 발령 및 해제 전파 o 공격기법·파급영향 분석 o 복구 및 보안기술 현장지원
실무기관 (자체대응반)	o 자체 안전대책 수립·시행 o 사고에 대한 긴급 조치 및 조치결과 통보 o 자체대응반 구성·운영 o 기술적 보안대책 시행

나. 과학기술부 비상총괄반

(1) 구성

(가) 위기경보수준이 **심각**의 경우 **비상총괄반(반장 : 비상계획담당관)**을 구성·운영

(2) 역할

(가) 비상사태 및 위기관리에 관한 계획 수립 및 이에 따라 긴급대응반 지원과 부내·외 상황보고

(나) 경보발령에 따른 대응조치 수행 현황 모니터링 관리

(다) 중요시설의 지정과 보호 대책 수립 및 시행

다. 과학기술부 긴급대응반

(1) 구성

(가) 위기경보수준이 **관심** 이상인 경우 필요시 **긴급대응반**을 구성·운영

o 긴급대응반은 상황총괄팀, 분석대응팀, 복구지원팀 구성·운영, 분석대응팀은 합동조사팀 구성시 합동조사팀으로 역할전환

(나) 긴급대응반 반장을 **정보화담당관**으로 하고, 긴급대응반 아래 **정보화담당관실 사무관**을 **팀장**으로 부내 네트워크·시스템관리자·실무자와 유지보수업체 및 과학기술정보보호센터 전문인력 등이 참여하는 상황총괄팀, 분석대응팀, 복구지원팀을 각각 편성·운영

(2) 역할

(가) **심각** 수준의 위기경보가 발령될 경우 **사고대책본부** 구성

(나) 사이버 위협 경보에 따른 대응계획 수립 및 조치결과를 종합하여 사고대책본부장에게 상황보고

(다) 사이버공격으로 인한 사고 발생 또는 징후 발견시 국가정보원(사이버안전센터)에 신고

(라) 사고에 대한 증거 확보 및 보존

(마) 긴급대응반 편성 인원에 대한 비상연락망 유지

라. 과학기술정보보호센터

(1) 구성

(가) 과학기술분야 핵심연구정보 보호체계를 체계적으로 지원하기 위한 종합상황실, **지원팀** 구성·운영

(나) **관심** 수준 이상의 사이버위협 경보가 발령될 경우 현장기술을 지원할 수 있는 Help-desk팀 구성·운영

(2) 역할

(가) Non-Stop(365일/24시간) 모니터링하고 각종 위협정보 분석 및 대응

(나) 사이버위협 경보가 발령될 경우 **실무기관에 사이버위협 경보 발령 및 해제 전파**

(다) 사고원인 조사 및 피해규모 확인 지원

(라) 공격기법, 해킹방법 분석후 대응방안 마련 및 전파

(마) 침해사고 원인분석 및 대응방안 강구 지원

(바) 현장 조사 및 복구 지원

(사) 조치결과 취합 및 종합 보고서 작성지원

(3) 세부 임무

구 분		임 무
과학기술정보보호센터	상황관제	o 24시간 종합상황실 운영 o 실무기관 대상 경보 발령 및 해제 전파 o 과학기술정보보호 대상기관 네트워크 모니터링 o 국내·외 주요 보안사이트 모니터링 o 침해사고 초동대응 o 침해사고 전화접수 및 대응 지원
	분석대응	o 침해사고 원인분석 및 기술적 대응방안 강구 o 웜·바이러스 샘플 채취 및 파급영향 분석 o 해킹 방법 분석 o 공격진원지 파악 및 차단대책 강구 o 피해규모 확인
	복구지원	o 복구 대책 수립 및 전파 o 해킹 대응기술 전파 o 해킹사고 현장조사 및 기술지원 o 정보보호 전문기관(백신업체 등)과의 정보 협력 o 대응결과 종합

마. 실무기관

(1) 구성

(가) 정보 및 정보보호책임자(팀장급 이상)를 반장으로 하는 **자체 대응반** 구성·운영

o 정보통신시스템실무자 및 협력사 등이 참여

(2) 역할

(가) 과학기술정보보호센터에서 사이버 위협 경보가 전파된 경우 기관내 소속원에게 즉시 경보 발령 및 해제 전파

(나) 자체 네트워크·시스템 등 모니터링 및 수시 점검

(다) 조치결과 및 피해상황 등을 과학기술정보보호센터에 통보

(라) 자체 위기상황 탐지·대응결과 및 피해상황 등의 보고

(마) 침해사고 원인 분석을 위한 현장 조사 및 복구 협조

(바) 기관 특성에 적합한 **사이버안전 분야 위기대응 실무 매뉴얼** 작성·운영

Ⅵ. 위기경보 수준별 대응요령

Ⅵ. 위기경보 수준별 대응요령

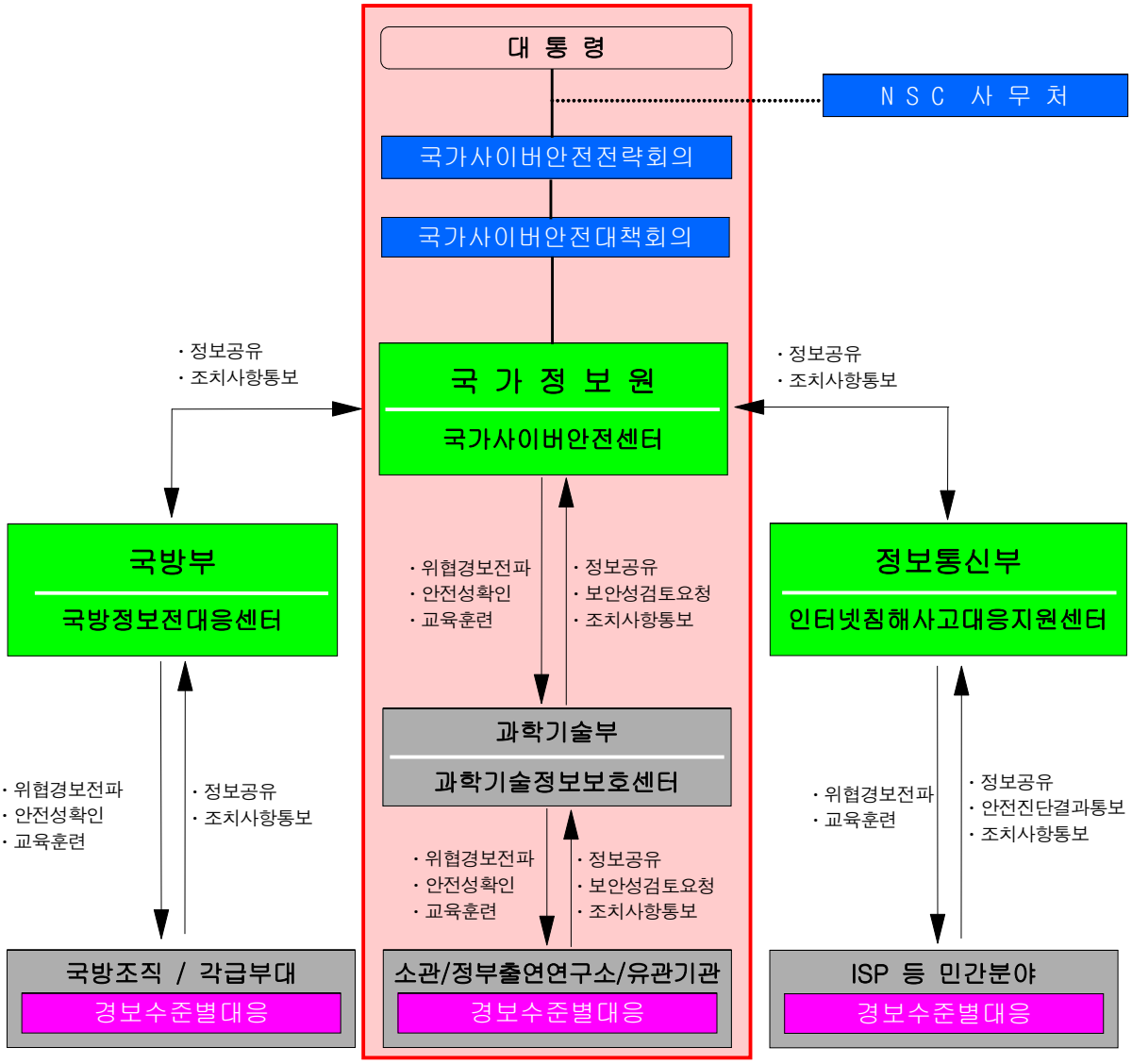
사이버위협 경보수준은 관심·주의·경계·심각의 4단계로 구분된다. 과학기술부는 국가정보원으로부터 경보발령을 접수한 경우에는 본 장에 수록된 경보수준별 대응요령을 수행하여야 한다.

□ 경보수준별 대응요령 요약

단계		대응요령 요약
경보	심각	○ **경계** 경보 조치 지속 시행 ○ 국가차원의 즉각 대응 태세 돌입 ○ 과학기술부 합동조사 및 복구지원팀 가동
	경계	○ **주의** 경보 조치 지속 수행 ○ 과학기술정보보호센터는 비상 대응 체계 가동 ○ 과학기술부는 긴급대응반, 실무기관은 자체대응반 가동
	주의	○ **관심** 경보 조치 지속 수행 ○ 분야별 사이버안전 유관기관 및 보안업체와 공조체계 확인 ○ 과학기술부는 긴급대응반, 실무기관은 자체대응반 가동 준비 (필요시 소집)
	관심	○ 보안권고문 등 보안조치 이행 ○ 이상 징후 탐지시 초동대처 후 국가사이버안전센터에 통보 ○ 사고발생 대비 긴급대응반, 자체대응반 연락체계 확인 ○ 사이버공격 여부 감시 강화
정상		○ 과학기술부(과학기술정보보호센터) 홈페이지 및 SnT Net 등 정보공유시스템의 최신 정보 지속 확인 ○ 보안취약점 발굴 및 실무기관간 공유체계 활성화 ○ 과학기술분야 사이버안전 위기대응 매뉴얼에 의거 정기적 점검 실시 ○ 사고발생 대비 긴급대응반 구성, 실무기관은 자체대응반 구성 ○ 사이버안전 모의훈련 실시 및 취약점 개선·보완 ○ 정보혁신협의회를 통한 사이버안전 교육 및 훈련 실시

1. 평시 예방활동

가. 평시 업무체계



과학기술부와 과학기술정보보호센터(보안관제, 침해사고대응, 정보공유분석 등 사이버안전 업무를 전담하는 기구)는 다음의 임무를 수행

(1) 과학기술부는 소관분야 실정에 맞는 보안관리 기준을 수립

(2) 국가정보원은 과학기술부의 정보통신망 안전성을 확인할 수 있고, 과학기술부 실무기관의 정보통신망에 대한 안전성 확인은 과학기술부 장관과 협의하여 수행

(3) 과학기술정보보호센터는 24시간 사이버공격 및 위협 징후 감시, 침해사고대응, 정보공유분석 등의 업무를 수행

평시 실무기관은 다음의 임무를 수행

(1) 실무기관의 장은 사이버위협으로부터 관할 정보통신망의 보호를 위해 부록 Ⅲ.「평시 안전점검 체크리스트」를 참조하여 정기적으로 보안점검을 시행

(2) 정보통신망 신·증설 등 정보화사업 추진시 자체 보안대책을 강구하고 과학기술부에 보안성 검토를 의뢰

(3) 과학기술부는 실무기관의 보안성 검토 요청을 국가정보원에 의뢰

(4) 실무기관은 대규모 사이버공격 발생시 신속하고 효과적으로 대응하기 위하여 정보보안 전문인력으로 자체대응반을 구성

※ 자체대응반 구성 및 운용은 부록 Ⅰ. 「2-나-(3) 실무기관의 자체 사고조사 (p160)」 참조

나. 예방활동

(1) 사이버안전대책 수립

(가) 과학기술부는 국가사이버안전매뉴얼을 바탕으로 과학기술부 실정에 맞게 소관분야 안전대책(사이버안전분야 매뉴얼 포함)을 수립하고, 이를 소속 및 산하기관에 배포하여 활용

(나) 과학기술부는 소관분야 안전대책을 수립·시행할 경우에는 국가정보원에 통보

(다) 실무기관은 과학기술부의 안전대책에 따라 자체 안전대책을 수립·시행

(2) 안전성확인 및 점검조치

(가) 안전성 확인 및 정기점검

- o 과학기술부는 자체 수립한 안전대책에 따라 소관분야 정보통신망에 대한 안전성과 안전대책 이행여부에 대해 정기점검을 실시할 수 있음
- o 과학기술부는 국가정보원과 협의하여 실무기관에 대해 현장방문 또는 원격 측정을 통하여 사이버안전대책 이행여부와 정보통신망의 안전성 확인할 수 있음
- o 실무기관은 자체적으로 정보통신망에 대한 안전대책의 적절성 이해 여부 등에 대해 정기적으로 점검 실시

(나) 안전성 확인의 시정 조치

o 국가정보원장은 과학기술부 및 실무기관에 대한 정보통신망의 안전성과 안전대책 이행여부에 대해 확인을 실시한 경우에 필요한 시정조치를 권고할 수 있음

o 과학기술부 장관 및 실무기관의 장은 국가정보원이 제시한 시정 권고사항에 대해 조속히 조치를 취하고, 그 결과를 국가정보원장에게 통보

(3) 위협정보 수집·분석 및 전파

(가) 위협정보 공유체계 구축

o 과학기술부는 국가차원의 사이버위협 정보가 종합 수집·분석될 수 있도록 사이버위협 정보수집의 보안관제망 연동 지원

o 과학기술정보보호센터는 국가정보원에서 주관하는 사이버위협 정보수집 시스템을 연동한 기관을 대상으로 보안관제 및 정보공유 등을 위한 협의체(회의체) 참석

(나) 사이버위협 정보 수집

o 과학기술정보호호센터는 사이버위협 정보 또는 이상징후 정보 등과 같은 다양한 위협정보를 수집하기 위해 과학기술부 및 실무기관의 전산망을 대상으로 24시간 공격 및 위협 징후 모니터링

o 과학기술정보보호센터와 실무기관은 보안관제시스템 또는 오프라인 등을 통해 사이버위협 정보를 인지한 경우에는 초동조치 후 과학기술부에 통보하고 과학기술부는 국가정보원에 통보

(다) 보안정보 및 대응책 작성·배포

o 과학기술부는 국가정보원에서 발표한 보안권고문 또는 취약점 분석정보를 과학기술정보보호센터에 배포하고 과학기술정보보호센터는 실무기관에 배포

o 실무기관은 보안정보, 보안권고문 또는 취약점 분석정보를 바탕으로 보안 업데이트 및 대응조치를 수행하고, 기관 내부에 배포

(라) 사이버위협 인지 또는 사고 발생시 신고 및 조사

o 실무기관은 과학기술정보보호센터와 위협정보 전파 및 사고신고 연락체계를 구성 유지

o 사이버 사고 또는 징후 발생시 실무기관은 과학기술정보보호센터에 통보하고 과학기술정보보호센터는 과학기술부에 통보

o 사이버 사고 또는 징후 발생시 과학기술부는 국가정보원(NCSC)에 통보

o 국가 기밀문서가 저장된 정보시스템에 해킹 사고가 발생했을 경우에는 의무적으로 신고

(4) 사이버안전 관련기관과 정보공유

(가) 사이버안전 전문기구와의 정보공유 및 공조체계

o 과학기술정보보호센터는 사이버안전 전문기관과 정보공유 및 협력체계를 구축하고 관계 전문가 회의에 참석

(5) 정보통신망에 대한 보안성 검토 및 보안측정

※ 보안성 검토 및 보안측정은 「국가정보보안기본지침」 참조

(가) 정보통신망 보안대책 수립 및 보안성 검토

o 실무기관은 정보통신망 신·증설 등 정보화 사업을 추진하는 경우 자체적으로 보안대책을 수립

o 실무기관은 자체 수립한 보안대책의 적절성 여부에 대해 과학기술부에 보안성검토를 요청

o 과학기술부는 실무기관이 자체 수립한 보안대책의 적절성 여부에 대해 국가정보원에 보안성검토를 요청

o 국가정보원은 각급기관이 요청한 보안대책에 대한 보안성을 검토하여 적합한 대책을 제시

(6) 사이버안전에 대한 교육·홍보 및 훈련 등

(가) 사이버위협 대응 교육 및 훈련 강화

o 과학기술부 정보보안담당관(자)은 국가정보원에서 실시하는 국가 정보보안설명회에 참석

o 실무기관은 사이버위협에 대비하여 정기적인 교육 및 훈련을 통해 소속직원의 보안의식 제고와 보안관리 요령을 전파

(나) 사이버공격 대응훈련

o 실무기관은 국가정보원이나 국회 등에서 실시하는 사이버안전 모의훈련을 통해 발견되지 않았던 새로운 취약점이나 관리가 허술했던 부분을 찾아내고 이를 보완하기 위하여 적극 협조

o 실무기관은 기관의 보안취약성을 진단하기 위해 필요한 경우 국가정보원에 수시 모의훈련 실시를 요청할 수 있음

(다) 사이버안전기술 확보

o 과학기술부는 소관분야 정보통신망을 보호하기 위해 사이버안전 기술 연구개발의 소요를 국가정보원에 제기할 수 있음

(7) 기본점검 활동

(가) 사이버위협 동향 파악

o 실무기관은 과학기술정보보호센터 등 사이버안전 전문기구 및 보안업체의 홈페이지를 수시방문, 관련내용을 파악

o 국내외 방송이나 언론의 사이버위협 관련 보도 주시

(나) 주요 정보시스템의 정기점검

o 웹서버, 메일서버 등의 정보시스템이 정상적으로 운영되는지 또는 불법침입자에 의한 중요 데이터의 파괴 및 위·변조가 발생되었는지 여부를 정기적으로 점검

(다) 업무와 관련 없는 P2P등의 인터넷 연결 프로그램 사용 자제

o P2P 등의 파일공유프로그램은 웜이나 트로이목마 등과 같은 악성프로그램을 전파할 가능성이 있으므로 가급적 사용을 자제

(라) 백신 탐지 패턴 및 소프트웨어 보안패치 업데이트 실시

o 악성프로그램의 특성은 계속적으로 변하기 때문에 백신프로그램의 엔진은 항상 최신버전으로 업데이트

o 사용 중인 소프트웨어의 보안패치사항이 발표된 경우 해당패치를 수행하여 취약점을 최소화 하도록 노력

(마) 네트워크 트래픽량 변화 모니터링

o 라우터, 침입탐지시스템 등을 이용하여 트래픽량이 급증하는지를 지속적으로 모니터링

o 네트워크 트래픽량 모니터링을 통해 서비스거부 공격, 웜 확산 등의 이상 징후 발생여부를 관찰

(바) 출처가 불분명한 이메일 삭제

o 출처가 불분명한 이메일을 통해 웜·바이러스가 감염될 우려가 있으므로 의심되는 이메일은 열지 않고 삭제

o 사용자가 이메일을 미리보기만 하더라도 악성코드가 사용자 PC에 사용자도 모르는 사이에 설치될 우려가 있으므로 미리보기 기능을 삭제

(사) 폴더 및 파일 공유 사용 자제

o 자료 교환 등을 위해 사용하는 컴퓨터 폴더 및 파일 공유를 통해 사이버공격이 발생될 우려가 있으므로 폴더 및 파일 공유 사용을 자제

(아) 복잡한 패스워드 사용 및 주기적인 변경

o 컴퓨터의 불법적인 접근을 방지하기 위해 유추하기 힘든 복잡한 패스워드를 사용하며, 반드시 특수문자를 포함

※ CMOS 패스워드, 계정 패스워드, 화면보호기 패스워드, 공유 패스워드, 네트워크 접근 등 컴퓨터에서 사용하는 패스워드

o 계정 패스워드는 월 1회 이상 주기적으로 변경

2. 관 심

가. 상 황

o 위험도가 높은 웜·바이러스 등 악성코드 및 해킹 기법 출현으로 피해 발생 가능성 증대

o 해외 피해확산 등 사이버위협의 국내 유입 가능성 증대

나. 기관별 대응요령

(1) 과학기술부

(가) NCSC에서 위기경보를 발령할 경우 과학기술정보보호센터에 경보발령 전파

※ 경보발령 양식은「붙임 1」참조

△ 전파대상 : 과학기술정보보호센터

△ 전파수단 : SMS, FAX, 전화, 전자우편 및 홈페이지

(나) 과학기술정보보호센터에서 이상징후 또는 사고 발생이 통보된 경우 과학기술부는 NCSC에 관련사항을 통보

< 과학기술부 연락처 >

o 전화 02-503-7619/ FAX 02-2110-3609

o 전자우편 cert@most.go.kr 또는 홈페이지 www.most.go.kr

< NCSC 연락처 >

o 전화 111 또는 02-557-0716/ FAX 02-3432-0463(24시간)

o 전자우편 cert@ncsc.go.kr 또는 홈페이지 www.ncsc.go.kr

※ 사고신고서식 및 사고조치 양식은「붙임 3, 4」참조

(다) 보안권고문 및 보안조치 이행 권고문이 NCSC에서 배포된 경우 과학기술정보보호센터에 배포

※ 경보발령 양식은「붙임 1」참조

△ 전파대상 : 과학기술정보보호센터

△ 전파수단 : SMS, FAX, 전화, 전자우편 및 홈페이지

(라) 긴급대응반 가동 준비 및 필요시 긴급대응반원 비상소집

(마) 실무기관 상황조치 관련 정보를 취합하여 NCSC에 통보

※ 상황조치 양식은「붙임 2」참조

(2) 과학기술정보보호센터

(가) 과학기술부 긴급대응반이 가동될 경우 신속한 현장지원

(나) 과학기술부에서 위기경보를 전파할 경우 실무기관에 전파

※ 경보발령 양식은「붙임 1」참조

△ 전파대상 : 실무기관

△ 전파수단 : SMS, FAX, 전화, 전자우편 및 홈페이지

(다) 실무기관에서 이상징후 또는 사고 발생이 통보된 경우 과학기술부에 관련사항을 통보

< 과학기술정보보호센터 연락처 >

o 전화 032-869-0808/ FAX 042-869-0809(24시간)

o 전자우편 sntsec@kisti.re.kr 또는 홈페이지 www.sntsec.or.kr

※ 사고신고서식 및 사고조치 양식은「붙임 3, 4」참조

(라) 보안권고문 및 보안조치 이행 권고문이 과학기술부에서 배포된 경우 실무기관에 배포

※ 경보발령 양식은「붙임 1」참조

△ 전파대상 : 실무기관

△ 전파수단 : SMS, FAX, 전화, 전자우편 및 홈페이지

(마) 새로운 악성코드, 취약점, 공격도구를 파악하여 실무기관에 대응요령 배포

(바) 긴급대응반 가동될 경우 신속한 현장지원

(사) 실무기관 상황조치 관련 정보를 취합하여 과학기술부에 통보

※ 상황조치 양식은「붙임 2」참조

(3) 실무기관

(가) 과학기술부에서 위기경보를 전파할 경우 소속원에게 경보발령 전파

(나) 이상징후 또는 사고가 발생한 경우 과학기술정보보호센터에 관련사항을 통보

※ 사고신고서식 및 사고조치 양식은「붙임 3, 4」참조

(다) 과학기술정보보호센터에서 배포한 새로운 악성코드, 취약점, 공격도구 대응요령에 따른 보호대책 이행

(라) 보안 권고문은 일정수준 이상의 위험성을 갖고 있는 웜·바이러스, 보안 취약점, 해킹기법 등 사이버위협 요소에 대한 특성과 적절한 대응방법을 제공하고 있으므로 이에 따라 보호대책 이행

(마) 새로운 보안취약점이 발표되거나 위험도가 높은 웜·해킹 기법에 대한 피해 발생 가능성이 높은 상태이므로 지속적으로 모니터링 하여 피해 발생 여부를 체크하고 위기징후 감시

(바) 해외에서 피해가 확산되는 경우 사이버위협의 국내 유입 가능성이 높아지므로 이에 대한 감시 철저

(사) 업무수행에 반드시 필요한 서비스를 제외한 일반적인 시스템 서비스에 대해서는 해당 프로세스의 실행을 중지시키거나 서비스 포트를 차단하여 취약점에 대한 위협을 최소화

(아) 라우터의 CAR(Committed Access Rate), ACL(Access Control List) 설정 내용과 스위치, 침입차단 시스템의 IP주소 또는 포트번호에 대한 허용 및 차단 규칙을 확인

(자) 서비스 포트를 허용할 때는 서비스를 제공하는 특정 포트만을 허용 하도록 설정하였는지 점검

(차) 상황조치 관련정보를 과학기술정보보호센터에 통보

※ 상황조치 양식은「붙임 2」참조

3.주 의

가. 상 황

o 위험도가 높은 웜·바이러스 등 악성코드 및 해킹 기법 출현으로 피해 발생 o 과학기술분야 정보시스템 전반에 보안태세 강화 필요

□ **관심**경보 조치 지속적 수행

나. 기관별 대응요령

(1) 과학기술부

(가) 평시에 긴급대응반 운영계획(반장, 인원, 역할, 연락처 등) 수립 유지

(나) 긴급대응반 운영에 대한 비상연락망 인원 및 연락처를 점검하여 최신 내용으로 갱신

※ 긴급대응반 비상연락망 양식은「붙임 5」참조

(다) 경보발령 체계도에 따른 연락체계 확인

(라) 필요시 긴급대응반원을 비상소집

(2) 과학기술정보보호센터

(가) 과학기술부, 사이버안전 유관기관 및 실무기관 연락체계(인원, 연락처) 점검 및 갱신

※ 실무기관, 사이버안전 유관기관 비상연락망 양식은「붙임 6, 8」참조

(3) 실무기관

(가) 자체대응반 운영에 대한 비상연락망 인원 및 연락처를 점검하여 최신 내용으로 갱신

※ 자체대응반 비상연락망 양식은「붙임 7」참조

(나) 과학기술부 및 과학기술정보보호센터 연락체계 점검 및 갱신

※ 자체대응반 비상연락망 양식은「붙임 7」참조

(다) 기관 내에서 사용 중인 정보보호시스템, 네트워크 장비 등 시스템 및 프로그램을 제공한 업체 간의 연락체계 점검

※ 정보시스템 협력업체 연락처 양식은「붙임 9」참조

(라) 악성코드, 취약점, 공격도구 등에 대한 분석정보가 발표될 경우, 공격대상이 될 수 있는 시스템, 서비스 포트번호 등을 예상

(마) 공격대상 시스템의 IP주소 또는 공격대상 서비스 포트번호의 차단 상태 확인

(바) 침입차단시스템, 침임탐지시스템 등을 이용하여 공격대상 시스템, 서비스 포트번호 등에 대하여 모니터링 강화

(사) 악성코드의 유입경로가 이메일의 첨부물을 통한 것인지, 웹 사이트의 이동코드를 통한 것인지, 특정한 소프트웨어의 배포를 통한 것인지 판단

(아) 이메일이나 웹을 통해 악성코드에 감염될 경우, 침입차단시스템, 침입탐지시스템, 이메일 서버 및 클라이언트 프로그램, 웹 프록시 서버 등에 차단규칙 추가

(자) 특정 소프트웨어 배포를 통해 악성코드에 감염될 경우, 해당 소프트웨어를 해지하고 추가적 설치를 금함

4. 경 계

가. 상 황

o 복수 국가기간망의 장애 또는 마비 o 웜·바이러스 등 악성코드의 급속한 확산으로 대규모 피해로 발전 가능성 증가

□ **주의**경보 조치 지속적 수행

나. 기관별 대응요령

(1) 과학기술부

(가) 과학기술정보보호센터가 실무기관에 사이버위협에 대한 대응요령을 모두 전파하였는지 또한 NCSC, 백신업체에서 제공하는 사이버위협에 대한 대응요령을 모두 이행하고 있는지 재확인

(나) 긴급대응반 증원 및 대비계획 점검

(2) 과학기술정보보호센터

(가) 실무기관이 과학기술정보보호센터에서 제공하는 사이버위협에 대한 대응요령을 모두 이행하고 있는지 재확인

(나) 긴급대응반 현장파견 인원 증원

(다) 급속한 피해확산이 우려되는 경우 과학기술부에 통보하고 실무기관에 네트워크 연결 차단 권고

(3) 실무기관

(가) 필요시 자체대응반 운영

(나) 피해가 예상되거나 피해상황 추이에 따라 자체대응반을 투입, 즉각적인 시스템복구를 실시하고 피해확산 차단조치

(다) 서비스거부공격에 대한 이상 징후를 포착한 경우 정보보안담당자는 신속하게 라우터, 침입차단시스템 등의 차단규칙을 재설정하여 공격 진행을 차단

※ 서비스거부공격 이상징후 포착시 공격전개 차단에 대한 자세한 방법은 국가사이버안전매뉴얼 부록 참조(p249)

(라) 중요 정보자료를 갖고 있는 서버 및 중요한 서버의 자료를 백업하여 네트워크와 단절된 안전한 곳에 보관

(마) 악성코드, 취약점, 공격도구 등에 대한 분석정보에 따른 공격대상 시스템의 IP 주소 또는 공격대상 서비스 포트번호의 차단 상태를 수시로 확인

(바) 침입차단시스템, 침입탐지시스템 등을 이용하여 취약점을 재점검하여 발견된 취약점 제거

(사) 피해발생 가능성이 높은 네트워크를 대상으로 물리적인 케이블 분리 등의 단절시행 여부를 검토하고, 필요할 경우 기관장의 승인하에 단절

5. 심 각

가. 상 황

o 핵심기반시설·시스템 대상 피해 발생 o 지역적·부분적 피해 발생, 전국적 확산 가능성 증대 o 국가적 차원에서 공동 대처 필요

□ **경계**경보 조치 지속적 수행

나. 기관별 대응요령

(1) 과학기술부

(가) 정책홍보실장을 본부장으로 하는 사고대책본부를 구성하여 즉각 대응태세 돌입

(나) 비상계획 담당관을 반장으로 하는 비상총괄반 구성

(다) 과학기술부 합동조사팀, 복구지원팀 구성 운영, 분석대응팀 역할 전환

o 과학기술부「합동조사팀」임무

- 피해확산 차단
- 피해 상황의 종합 처리 및 보고
  ※ 피해상황 종합 양식은「붙임 10～13」참조
- 사고원인에 대한 조사 및 분석
- 실무기관「자체대응반」총괄 지휘 및 대응방법 전파

o 과학기술부「합동조사팀」구성

- 과학기술부, 과학기술정보보호센터, 피해기관 담당자, 산업체 전문가로 구성

- 정보보호 전문인력 풀(Pool)제 운영을 통해 산업체 정보보호 전문가 참여 유도

o 과학기술부「합동조사팀」운영

- 위기유형별 합동조사팀을 구성하고 합동조사를 주관
- 범정부 합동조사팀 지원

o 과학기술부「복구지원팀」임무

- 피해 상황의 파악 및 복구 절차 수립·시행
- 「긴급대응반」과 연계, 복구활동 지원
- 피해 복구 및 사후 처리 결과 종합 보고

※ 피해상황 종합 양식은「붙임 10～13」참조

o 과학기술부「복구지원팀」구성

- 과학기술부, 과학기술정보보호센터, 피해기관 담당자, 및 산업체 전문가로 구성
- 정보보호 전문인력 풀(Pool)제 운영을 통해 산업체 정보보호 전문가 참여 유도

o 과학기술부「복구지원팀」운영

- 복구유형에 따라 복구지원팀을 구성하고 합동복구를 주관
- 범정부 합동복구팀 지원

(라) 사이버 위협에 대한 철저한 원인 분석을 통해 피해규모 및 적절한 대응 방법 등을 제시

(마) 피해규모를 판단하여 범정부 차원의 합동조사팀, 복구지원팀 협력 요청

(2) 과학기술정보보호센터

(가) 과학기술부 사고대책본부를 지원하기 위한 지원팀, Help-Desk팀 가동하고 즉각 대응태세 돌입

(나) 과학기술부 합동조사팀, 복구지원팀 현장지원(조사 및 복구지원 주관)

(3) 실무기관

(가) 자체대응반을 가동하고 즉각 대응태세 돌입

(나) 악성코드, 취약점, 공격도구 등에 대한 분석정보가 발표될 경우, 라우터·스위치 및 침입차단시스템의 차단규칙을 추가 설정하여 공격대상 서비스 포트를 차단

※ 공격대상 서비스 포트 차단에 대한 자세한 방법은 국가사이버안전매뉴얼 부록 참조(p249)

(다) 기관 내 PC사용을 최소화하여 만약에 발생할 수 있는 잠재적인 사고를 미연에 방지

(라) 서비스거부공격 및 웜 발생을 확실하게 예상할 수 있거나 내부 시스템 및 네트워크에 대규모 피해 확산을 예상할 수 있는 경우, 기관장의 승인을 받고 물리적인 케이블 분리 등을 통해 피해대상 네트워크를 단절

(마) 피해를 당한 해당 기관의 정보보안담당자는 사고와 관련된 데이터뿐만 아니라 데이터백업 및 로그관리 등 사고조사 및 복구에 필요한 자료를 제공

o 경미한 사고는 피해 기관이 자체 복구

※ 피해복구 및 상황처리 완료시 과학기술부 및 과학기술정보보호센터에 통보

o 중대한 사고는 과학기술부(과학기술정보보호센터) 지원 하에 복구

o 심각한 사고는 범정부「복구지원팀」에 의해 복구

Ⅶ. 위기대응 조치 및 절차

Ⅰ. 악성 웜·바이러스에 의한 과학기술 중요문서 유출

1. 관심의 경우 조치사항 및 처리절차

가. 상 황

□ 개 요

o 윈도우즈 운영체제의 최신 취약점을 이용하여 시스템을 마비시키고, 시스템내의 파일을 특정 서버로 유출시키는 AA-1웜이 미국에서 최초 발견된 이후 수 시간 만에 캐나다 등 인접국 및 유럽까지 급속히 확산됨에 따라 미국 등 국외 연구소와 협업하고 있는 연구소등을 통해 국내 유입이 우려되고 있음

□ 세부 내용

o 사고신고 일시 및 내용 : 7월 6일 10:30
- 현재까지 AA-1웜과 관련된 국내 사고는 보고되지 않음
- 미국 DHS(국토안보부)로부터 AA-1웜 주의를 요청하는 메일 수신
- 영국의 NISCC(국가기반시설보안조정센터)로부터 AA-1웜 주의를 요청하는 메일 수신
- 국가정보원 국가사이버안전센터(NCSC)에서 **관심** 경보 발령을 통해 AA-1웜 주의 요청

o 피해 현황
- 미국 주요 관공서 및 은행 등 국가·공공기관의 시스템이 마비되어 수 시간 동안 인터넷 서비스가 이루어지지 않음
- 영국, 프랑스 등 유럽 국가의 공공기관 및 연구시설의 시스템이 마비되고 내부 정보가 유출된 사고가 발생함

나. 조치사항 및 절차

(1) 조치 목록

조치사항	세부 내용
위기상황 접수 및 보고/전파	o 보고 및 내부 상황전파
초동조치	o 사이버위협 분석 o 「관심」경보 발령 전파 ※ 과학기술부는 경보발령 내용 접수시 과학기술정보보호센터 및 실무기관 등에 신속히 전파 o 보안권고문 및 보안조치 등 이행 권고문이 NCSC에서 배포된 경우 전파/보호대책 이행
긴급대응조치	o 백신 및 탐지룰 업데이트 배포 o 과학기술부 차원의「긴급대응반」가동 준비 및 필요시 긴급대응반 비상소집 o 국내외 유관기관 동향 파악 및 협조 o 모니터링 강화 o 불필요한 서비스 차단 및 차단규칙 점검 o 상황 조치 결과 취합 ※ 과학기술부는 실무기관 등의 조치결과를 취합, NCSC로 통보 o 피해 발생시 주의 단계 조치 수행
처리상황 보고	o 조치상황 종합 및 보고

다. 조치 내용

(1) 위기상황 접수 및 보고/전파

(가) 보고 및 내부 상황전파

o NCSC에서 관심 경보 발령의 경우 긴급대응반 상황총괄팀은 사이버 위협 내용을 상부에 보고하고 과학기술부 전 직원에게 신속히 전파

※ 보고내용 및 양식은「붙임 1」참조

(2) 초동조치

(가) 사이버위협 분석

o 긴급대응반 분석대응팀은 공격기법 및 피해 가능성 등을 분석

o 긴급대응반 상황총괄팀은 AA-1 웜에 대한 피해 가능성이 높은 상태이므로 지속적으로 모니터링하고 위기 징후를 감시

o 정보보호 제품 공급 社와 상황공유 및 업데이트 의뢰

- 긴급대응반 분석대응팀은 정보보호 제품 공급社(침입차단·탐지시스템 제작업체, 백신업체 등)에 정보제공 및 웜·바이러스 백신 탐지룰 업데이트 요청

※ 악성코드 샘플 제공할 정보보호업체 목록은「붙임 9」참조

(나) **관심** 경보 발령 전파

o **관심** 경보 발령의 경우 접수 후, 반장에게 보고하고 과학기술정보보호센터 및 실무기관에 신속히 전파

- 긴급대응반 상황총괄팀은 사이버 위기경보를 반장에게 보고하고, NCSC의 **관심** 경보 발령사실을 과학기술정보보호센터에 신속히 전파

△ 전파대상 : 과학기술정보보호센터

△ 전파수단 : SMS, FAX, 전화, 전자우편 및 홈페이지

- 과학기술정보보호센터는 실무기관에 **관심** 경보 발령 사실을 신속히 전파

△ 전파대상 : 실무기관

△ 전파수단 : SMS, FAX, 전화, 전자우편 및 홈페이지

- 실무기관은 위기경보를 접수하고 신속히 기관내 소속원에게 **관심** 경보 발령 사실을 전파

※ 경보발령 양식 및 상황조치 작성양식은「붙임 1, 2」참조

(다) 보안권고문 및 보안조치 등 이행 권고문이 NCSC에서 배포된 경우 전파/보호대책 이행

o 긴급대응반 상황총괄팀은 보안권고문 및 보안조치, 대응요령 등 이행 권고문이 NCSC에서 배포된 경우 이를 과학기술정보보호센터에 전파하고, 과학기술정보보호센터는 실무기관에 전파

o 실무기관은 보안권고문 및 보안조치, 대응요령 등 이행 권고문에 따른 보호대책 이행

(3) 긴급대응 조치

(가) 백신 및 탐지룰 업데이트 배포 및 적용

o 백신 및 탐지룰이 제공되는 경우 과학기술정보보센터를 통하여 실무기관에 배포

o 실무기관은 배포된 백신 및 탐지룰을 자체 시스템에 적용

(나) 긴급대응반 가동 준비 및 필요시 긴급대응반 비상소집

o 긴급대응반 반장은 상황을 예의 주시하고 긴급대응반 가동 준비 및 필요시 긴급대응반 비상소집

o 과학기술정보보호센터는 긴급대응반이 가동될 경우 신속한 현장 지원

(다) 국내외 유관기관 동향 파악 및 협조

o 국가사이버안전센터(NCSC), 정보통신부 등 보안관제를 수행하는 기관에 대한 동향 파악 및 상호협조

(라) 모니터링 강화

o AA-1월에 대한 피해 발생가능성이 높은 상태이므로 지속적으로 모니터링 및 위기징후 감시 강화

- 과학기술정보보호센터 및 실무기관은 사이버 위협에 대한 모니터링 및 위기징후 감시체제 강화

(마) 불필요한 서비스 차단 및 차단규칙 점검

o 업무수행에 반드시 필요한 서비스를 제외한 일반적인 시스템 서비스에 대해서는 해당 프로세스의 실행을 중지시키거나 서비스 포트를 차단하여 취약점에 대한 위협을 최소화

o 라우터의 CAR(Committed Access Rate), ACL(Access Control List) 설정 내용과 스위치, 침입차단 시스템의 IP주소 또는 포트번호에 대한 허용 및 차단 규칙을 확인

o 서비스 포트를 허용할 때는 서비스를 제공하는 특정 포트만을 허용 하도록 설정하였는지 점검

(바) 상황조치 결과 취합

o 실무기관은 경보발령에 따른 대응조치 수행 후 과학기술정보보호센터 기술지원팀에 상황통보

※ 상황조치 통보서는「붙임 2」참조

o 과학기술정보보호센터 기술지원팀은 상황조치 결과를 취합하여 과학기술부 상황총괄팀에 보고

o 긴급대응반 상황총괄팀은 상황조치 결과를 취합하여, 반장에게 보고하고 국가정보원(NCSC)에 통보

(사) 피해 발생시 **주의** 단계 조치 수행

o 피해가 발생되어 NCSC에서 **주의** 단계로 상향조정하는 경우 **주의** 단계 조치 시행(P81 참조)

(4) 처리상황 보고

(가) 조치상황 종합 및 보고

o 긴급대응반 상황총괄팀 및 분석대응팀은 피해 및 대응현황을 종합·정리하여 보안관제 상황과 조치현황에 대한 종합 보고서를 작성하여 반장에게 보고

2. 주의의 경우 조치사항 및 처리절차

가. 상 황

□ 개 요

o 윈도우즈 운영체제의 최신 취약점을 이용하여 시스템을 마비시키고, 시스템내의 파일을 특정 서버로 유출시키는 AA-1웜이 미국 연구소등과 협동 과제를 수행하고 있는 국내 일부 연구소로 전자우편을 통해 전파되어 중요 연구정보 일부가 유출되는 피해가 발생함

□ 세부 내용

o 사고신고 일시 및 내용 : 7월 6일 16:30
- OOO연구원 등 일부 연구소에서 전자우편을 통해 전파된 웜 바이러스에 의하여 감염 시스템이 마비되는 사고 신고접수됨
- 과학기술정보보호센터(S&T-SEC)에서 OOO연구원 등 일부 연구소 내에서 발생하고 있는 트래픽 이상 현상 탐지
- 과학기술정보보호센터에서는 탐지 및 신고 접수된 현황을 국가사이버안전센터에 통보
- 국가정보원 국가사이버안전센터(NCSC)에서 “주의” 경보 발령을 통해 AA-1웜에 대한 보안태세 강화 요청

o 피해 현황
- OOO연구원등 일부 연구소에서 AA-1웜에 감염된 시스템이 마비되어 업무 장애가 발생하고 중요 연구정보 자료 일부가 유출된 것으로 확인됨
- AA-1웜에 감염된 OOO연구원 등에서 내부 네트워크를 통한 AA-1웜 전파 시도로 인하여 다량의 트래픽이 발생하여 인터넷 장애가 발생함

나. 조치사항 및 절차

(1) 조치 목록

조치사항	세부 내용
위기상황 접수 및 보고/전파	o 관심 단계에서 피해발생 및 사고 신고
초동조치	o 사고원인 분석 o「주의」경보 발령 전파 ※ 과학기술부는 경보발령 내용 접수시 과학기술정보보호센터 및 실무기관 등에 신속히 전파
긴급대응조치	o 필요시 긴급대응반 비상소집 o 국내외 유관기관 동향 파악 및 협조 강화 o 피해현황 파악 및 사고조사 o 공격 진원지·경유지 접속 차단 및 보안대책 시행 o 피해 확산시 경계 단계 조치 수행
피해복구 조치	o 피해확산 방지 및 복구 조치 o 기관별 피해복구 추진 실태 파악
처리상황 보고	o 관심 경보단계 조치 수행
후속조치	o 재발 방지대책 수립·전파

관심 경보 조치 지속적 수행

다. 조치 내용

(1) 위기상황 접수 및 보고/전파

(가) 관심단계에서 피해발생 및 사고신고

o 실무기관에서 AA-1 웜에 대한 피해가 발생하여 관련 사실을 과학기술정보보호센터에 신고

o 과학기술정보보호센터는 AA-1 웜에 대한 피해발생 사실을 과학기술부에 보고

o 과학기술부는 피해사실을 NCSC에 통보

※ 사고신고 양식은「붙임 3」참조

(2) 초동조치

(가) 사고 원인분석

o 긴급대응반 분석대응팀은 피해기관에 출동, 공격기법·피해양상 등을 분석하고, 상황총괄팀은 관제시스템에 탐지룰 적용

(나) **주의** 경보 발령 전파

o **주의** 경보 발령의 경우 접수 후, 반장에게 보고하고 과학기술정보보호센터 및 실무기관에 신속히 재전파

- 긴급대응반 상황총괄팀은 사이버 위기경보를 반장에게 보고하고, NCSC의 **주의** 경보 발령사실을 과학기술정보보호센터에 신속히 재전파

△ 전파대상 : 과학기술정보보호센터

△ 전파수단 : SMS, FAX, 전화, 전자우편 및 홈페이지

- 과학기술정보보호센터는 실무기관에 **주의** 경보 발령 사실을 신속히 재전파

△ 전파대상 : 실무기관

△ 전파수단 : SMS, FAX, 전화, 전자우편 및 홈페이지

- 실무기관은 위기경보를 접수하고 신속히 기관내 소속원에게 **주의** 경보 발령 사실을 재전파

※ 경보발령 양식 및 상황조치 작성양식은「붙임 1, 2」참조

(3) 긴급대응 조치

(가) 필요시 긴급대응반 비상소집

o 긴급대응반 반장은 평시 긴급대응반 운영계획을 수립유지

o 긴급대응반 운영에 대한 비상연락망 인원 및 연락처를 점검하여 최신 내용으로 갱신

o 경보발령 체계도에 따른 연락체계 확인

o 필요시 긴급대응반 비상소집

o 과학기술정보보호센터 및 실무기관 등도 비상연락망 및 연락처를 점검하여 최신 내용으로 갱신

o 실무기관은 정보보호시스템, 네트워크 장비 등 시스템 및 프로그램을 제공한 업체간의 연락체계 점검

(나) 국내외 유관기관 동향 파악 및 협조 강화

o 국가사이버안전센터(NCSC), 정보통신부 등 보안관제를 수행하는 기관에 대한 동향 파악 및 상호협조 강화

(다) 피해현황 파악 및 사고조사

o 과학기술부 실무기관 정보보호담당자는 해당 기관에 사고 발생시 즉시 과학기술정보보호센터에 피해내용을 통보하고, 자체 조사 및 복구 수행, 결과를 과학기술정보보호센터에 통보

※ 사고신고 및 사고조치 작성양식은「붙임 3, 4」참조

o 과학기술정보보호센터는 과학기술부에 피해 내용을 보고

o 과학기술부는 피해내용을 NCSC에 통보

o 긴급대응반 상황총괄팀·분석대응팀·복구지원팀은 피해현황을 파악하고 사고조사 계획을 수립하는 등 대응조치

o 긴급대응반 분석대응팀은 사고 조사를 수행하여 원인을 분석하고 공격·경유지 등을 확인

(라) 공격진원지·경유지 접속 차단 및 보안대책 시행

o 긴급대응반 분석대응팀은 피해확산 방지를 위해 공격지 및 경유지에 대한 접속 차단을 긴급대응반장에 건의

o 긴급대응반 상황총괄팀은 NCSC에 공격·경유지에 대한 접속을 차단토록 요청

o 공격대상 시스템의 IP주소 또는 공격대상 서비스 포트번호의 차단 상태 확인

o 침입차단시스템, 침임탐지시스템 등을 이용하여 공격대상 시스템, 서비스 포트번호 등에 대하여 모니터링 강화

o 악성코드의 유입경로가 이메일의 첨부물을 통한 것인지, 웹사이트의 이동코드를 통한 것인지, 특정한 소프트웨어의 배포를 통한 것인지 판단

o 이메일이나 웹을 통해 악성코드에 감염될 경우, 침입차단시스템, 침입탐지시스템, 이메일 서버 및 클라이언트 프로그램, 웹 프록시 서버 등에 차단규칙 추가

o 특정 소프트웨어 배포를 통해 악성코드에 감염될 경우, 해당 소프트웨어를 해지하고 추가적 설치를 금함

(마) 피해 확산시 **경계** 단계 조치 수행

o 피해가 확산되어 NCSC에서 **경계** 단계로 상향조정하는 경우 **경계** 단계 조치 시행(P88 참조)

(4) 피해복구 조치

(가) 피해확산 방지 및 복구조치

o 긴급대응반 분석대응팀은 피해기관 목록 작성 후 피해복구 우선순위를 산정하고 원격·현장 복구계획을 수립

※ 피해기관 목록 작성 양식은「붙임 10～13」참조

o 복구 우선순위 산정 시 피해기관의 연구정보자원의 중요도, 경제·사회적 중요도 등을 고려해 판단

o 긴급대응반(과학기술정보보호센터 중심)으로 복구 인력을 편성하되, 필요시 피해기관 전산망 유지보수 업체등과 합동 복구 실시

(나) 기관별 피해복구 추진실태 파악

o 긴급대응반 복구지원팀은 기관별 피해복구 추진실태를 수시파악, 복구가 미흡한 기관에 인력·장비 등 가용자원을 집중 투입할 수 있도록 피해복구 우선순위를 재설정

o 긴급대응반 분석대응팀은 상황 조치 결과를 취합해 피해범위 및 피해예방조치 현황을 파악하는 한편, 조치가 미흡한 기관에 대해서는 보완을 권고

(5) 처리상황 보고

(가) 관심 경보단계 조치 수행

o 관심 경보단계 조치 수행

(6) 후속조치

(가) 재발 방지대책 수립·전파

o 긴급대응반 분석대응팀은 사고원인이 된 AA-1 웜에 대한 보안취약점 분석결과, 도출된 문제점 개선 및 재발 방지대책을 수립·전파

3. 경계의 경우 조치사항 및 처리절차

가. 상 황

□ 개 요

o 윈도우즈 운영체제의 최신 취약점을 이용하는 AA-1웜 발생이후 전자우편 및 메신저를 통해 전파되는 변종(AA-1a) 웜바이러스가 추가 발생하여 초고속연구망을 이용하는 연구소를 대상으로 시스템이 마비되고 중요 연구정보가 유출되는 피해가 발생함

□ 세부 내용

o 사고신고 일시 및 내용 : 7월 7일 20:30

- △△△연구원 등 다수의 연구소에서 전자우편 및 메신저를 통해 전파되는 웜바이러스에 의하여 원내 대다수의 시스템이 마비되었다는 사고가 신고 접수됨
- 과학기술정보보호센터(S&T-SEC)에서 △△△연구원 등 다수의 연구소내에서 발생하고 있는 트래픽 이상 현상 탐지
- 과학기술정보보호센터에서는 탐지 및 신고 접수된 현황을 국가사이버안전센터에 통보
- 국가정보원 국가사이버안전센터(NCSC)에서 “경계” 경보 발령을 통해 AA-1웜 및 변종에 대한 보안 공조대응 요청

o 피해 현황

- △△△연구원등 다수 연구소에서 AA-1웜 및 AA-1a웜에 감염된 시스템이 마비되어 업무 장애가 발생하고 중요 연구정보 자료 일부가 유출된 것으로 확인됨
- AA-1웜 및 AA-1a웜에 감염된 다수의 시스템이 발생하는 트래픽에 의하여 일부 기관의 백본 네트워크가 다운되어 인터넷이 불통되는 장애가 발생함

나. 조치사항 및 절차

(1) 조치 목록

조치사항	세부 내용
위기상황 접수 및 보고/전파	o 주의 단계에서 피해확산 및 사고 신고
초동조치	o「경계」경보 발령 전파 ※ 과학기술부는 경보발령 내용 접수시 과학기술정보보호센터 및 실무기관 등에 신속히 전파
긴급대응조치	o 긴급대응반 증원 운영 o 실무기관은 필요시 자체대응반 운영 o 피해 확산시 경계 단계 조치 수행
피해복구 조치	o 주의 경보단계 조치 수행
처리상황 보고	o 주의 경보단계 조치 수행
후속조치	o 유출 자료에 대한 안보영향평가 실시

주의 경보 조치 지속적 수행

다. 조치 내용

(1) 위기상황 접수 및 보고/전파

(가) 주의 단계에서 피해확산 및 사고 신고

o 실무기관에서 AA-1 웜 및 AA-1a 웜에 대한 피해가 확산되어 관련 사실을 과학기술정보보호센터에 신고

o 과학기술정보보호센터는 AA-1 웜 및 AA-1a 웜에 대한 피해확산 사실을 과학기술부에 보고

o 과학기술부는 피해확산 사실을 NCSC에 통보

※ 사고신고 양식은「붙임 3」참조

(2) 초동조치

(가) **경계** 경보 발령 전파

o **경계** 경보 발령의 경우 접수 후, 반장에게 보고하고 과학기술정보보호센터 및 실무기관에 신속히 재전파

- 긴급대응반 상황총괄팀은 사이버 위기경보를 반장에게 보고하고, NCSC의 **경계** 경보 발령사실을 과학기술정보보호센터에 신속히 재전파

△ 전파대상 : 과학기술정보보호센터

△ 전파수단 : SMS, FAX, 전화, 전자우편 및 홈페이지

- 과학기술정보보호센터는 실무기관에 **경계** 경보 발령사실을 신속히 재전파

△ 전파대상 : 실무기관

△ 전파수단 : SMS, FAX, 전화, 전자우편 및 홈페이지

- 실무기관은 위기경보를 접수하고 신속히 기관내 소속원에게 **경계** 경보 발령 사실을 재전파

※ 경보발령 양식 및 상황조치 작성양식은「붙임 1, 2」참조

(3) 긴급대응 조치

(가) 긴급대응반 증원 운영

o 긴급대응반 반장은 증원 및 대비계획 점검

o 과학기술정보보호센터는 긴급대응반 현장파견 인원 증원

o 과학기술부는 실무기관이 NCSC 및 백신업체에서 제공한 AA-1 웜 및 AA-1a 웜 대응요령을 모두 이행하고 있는지 재확인

o 과학기술정보보호센터는 급속한 피해확산이 우려되는 경우 과학기술부에 통보하고 실무기관에 네트워크 연결 차단 권고

(나) 실무기관은 필요시 자체 대응반 운영

o 과학기술부는 피해확산이 예상되거나 피해상황 추이에 따라 시스템 복구 및 피해확산 차단을 위해 실무기관에 자체 대응반 가동을 독려

o 피해가 예상되거나 피해상황 추이에 따라 자체대응반을 투입, 즉각적인 시스템복구를 실시하고 피해확산 차단조치

o 서비스거부공격에 대한 이상 징후를 포착한 경우 정보보안 담당자는 신속하게 라우터, 침입차단시스템 등의 차단 규칙을 재설정하여 공격 진행을 차단

※ 서비스거부공격 이상징후 포착시 공격전개 차단에 대한 자세한 방법은 국가사이버안전매뉴얼 부록 참조(p249)

o 중요 정보자료를 갖고 있는 서버 및 중요한 서버의 자료를 백업하여 네트워크와 단절된 안전한 곳에 보관

o 악성코드, 취약점, 공격도구 등에 대한 분석정보에 따른 공격대상 시스템의 IP 주소 또는 공격대상 서비스 포트번호의 차단 상태를 수시로 확인

o 침입차단시스템, 침입탐지시스템 등을 이용하여 취약점을 재점검하여 발견된 취약점 제거

o 피해발생 가능성이 높은 네트워크를 대상으로 물리적인 케이블 분리 등의 단절시행 여부를 검토하고, 필요할 경우 기관장의 승인하에 단절

(다) 피해 확산시 **심각** 단계 조치 수행

o 피해가 확산되어 NCSC에서 **심각** 단계로 상향조정하는 경우 **심각** 단계 조치 시행(P94 참조)

(4) 피해복구 조치

(가) 주의 경보단계 조치 수행

o 주의 경보단계 조치 수행

(5) 처리상황 보고

(가) 주의 경보단계 조치 수행

o 주의 경보단계 조치 수행

(6) 후속조치

(가) 유출 자료에 대한 안보영향평가 실시

o 대외비 이상의 비밀이 유출된 경우 과학기술부는 해당 비밀 자료의 국가안보상 파급효과 분석을 위해 해당기관 담당자 및 관련 분야 전문가를 소집, 안보영향평가 실시

o 안보에 영향이 있다고 판단된 경우, 피해기관은 해당 비밀에 효력정지 및 취소 등의 조치 수행

4. 심각의 경우 조치사항 및 처리절차

가. 상 황

□ 개 요

o 초고속연구망을 중심으로 전파되던 AA-1웜 및 AA-1a웜이 전자정부통합망과 KT, 데이콤 등 국내 주요 ISP까지 확대 전파되어 인터넷을 통한 전자정부서비스, 전자상거래서비스, 인터넷뱅킹 서비스등이 마비되는 피해가 발생함

□ 세부 내용

o 사고신고 일시 및 내용 : 7월 8일 06:30
- 대다수의 국가·공공기관 및 인터넷서비스업체, 은행등의 네트워크가 마비되었다는 사고가 신고 접수됨
- 과학기술정보보호센터(S&T-SEC), 전자정부통합센터등에서 전국적으로 발생하고 있는 이상 트래픽 탐지
- 과학기술정보보호센터에서는 탐지 및 신고 접수된 현황을 국가사이버안전센터에 통보
- 국가정보원 국가사이버안전센터(NCSC)에서 “심각” 경보 발령을 통해 AA-1웜 및 변종에 대한 국가적 차원의 공동대처 요청

o 피해 현황
- 대다수의 공공기관 및 연구기관에서 AA-1웜 및 AA-1a웜으로 인한 트래픽 증가로 시스템 접속장애 발생
- 국가기관의 중요자료가 인터넷에 유출, 외교 및 안보관련 기관의 일부 민감한 자료로 인해 외교문제 발생 가능성 높음
- 연구기관의 중요 연구 비밀정보 자료가 해외로 유출됨에 따라 막대한 경제적 국가경쟁력 손실 우려

나. 조치사항 및 절차

(1) 조치 목록

조치사항	세부 내용
위기상황 접수 및 보고/전파	o 경계 단계에서 피해확산 및 사고 신고
초동조치	o「심각」경보 발령 전파 ※ 과학기술부는 경보발령 내용 접수시 과학기술정보보호센터 및 실무기관 등에 신속히 전파
긴급대응조치	o 사고대책본부 구성 운영 o 비상총괄반 구성 운영 o 과기부차원의 합동조사팀 구성 운영 o 과학기술정보보호센터 지원팀, Help-Desk팀 가동 o 실무기관은 자체대응반 가동 o 피해발생 가능성이 높은 네트워크 단절여부 판단
피해복구 조치	o 과기부차원의 복구지원팀 구성 운영
처리상황 보고	o 경보해제 및 하향조정 전파 o 종결보고
후속조치	o 사고재발 방지대책 수립 및 전파

경계 경보 조치 지속적 수행

다. 조치 내용

(1) 위기상황 접수 및 보고/전파

(가) 경계 단계에서 피해확산 및 사고신고

o 초고속연구망 중심으로 피해가 확산되던 AA-1 및 AA-1a 웜이 민간 ISP 및 국가공공망으로 확산되면서 국내 전체로 피해확산

o 실무기관에서 AA-1 웜 및 AA-1a 웜에 대한 피해가 확산되어 관련 사실을 과학기술정보보호센터에 신고

o 과학기술정보보호센터는 AA-1 웜 및 AA-1a 웜에 대한 피해확산 사실을 과학기술부에 보고

o 과학기술부는 피해확산 사실을 NCSC에 통보

※ 사고신고 양식은「붙임 3」참조

(2) 초동조치

(가) **심각** 경보 발령 전파

o **심각** 경보 발령의 경우 접수 후, 반장에게 보고하고 과학기술정보보호센터 및 실무기관에 신속히 재전파

- 긴급대응반 상황총괄팀은 사이버 위기경보를 반장에게 보고하고, NCSC의 **심각** 경보 발령사실을 과학기술정보보호센터에 신속히 재전파

△ 전파대상 : 과학기술정보보호센터

△ 전파수단 : SMS, FAX, 전화, 전자우편 및 홈페이지

- 과학기술정보보호센터는 실무기관에 **심각** 경보 발령 사실을 신속히 재전파

△ 전파대상 : 실무기관

△ 전파수단 : SMS, FAX, 전화, 전자우편 및 홈페이지

- 실무기관은 위기경보를 접수하고 신속히 기관내 소속원에게 **심각** 경보 발령 사실을 재전파

※ 경보발령 양식 및 상황조치 작성양식은「붙임 1, 2」참조

(3) 긴급대응 조치

(가) 사고대책본부 구성 운영

o 정책홍보실장을 본부장으로 하는 사고대책본부를 구성하여 즉각 대응태세 돌입

- 관제인력 증원 및 탐지룰 적용 등 보안관제 강화

- 각 분야·부문별 관제센터와 수시 연락 및 동향파악 강화

※ 사고대책본부 구성, 역할, 세부임무는(P42~43) 참조

(나) 비상총괄반 구성

o 비상계획 담당관을 반장으로 하는 비상총괄반 구성 운영

o 비상사태 및 위기관리에 관한 계획 수립 및 점검

(다) 과학기술부 차원의 합동조사팀 구성 운영

o 피해범위 및 복구시간 등에 따라 다수의 반으로 구성

o 피해현황 파악 및 사고조사

- 합동조사팀은 피해규모를 파악하고 현장·원격조사 계획 수립 및 이행

- 웜에 감염된 시각, 침입차단시스템 로그에 기록된 자료 유출량 및 기간, 피해 PC내 저장된 문서 등을 종합 분석

※ 합동조사팀 임무, 구성, 운영방법은 (P68~69) 참조

(라) 과학기술정보보호센터 지원팀 및 Help-Desk팀 가동

- 과학기술부 사고대책본부를 지원하기 위한 지원팀, Help-Desk팀을 가동하고 즉각 대응태세 돌입
- 과학기술부 합동조사팀 현장지원(조사 주관)

(마) 실무기관은 자체 대응반 가동

o 실무기관은 자체대응반을 가동하고 즉각 대응 태세 돌입

o 악성코드, 취약점, 공격도구 등에 대한 분석정보가 발표될 경우, 라우터·스위치 및 침입차단시스템의 차단규칙을 추가 설정하여 공격대상 서비스 포트를 차단

※ 공격대상 서비스 포트 차단에 대한 자세한 방법은 국가사이버안전매뉴얼 부록 참조(p249)

o 기관 내 PC사용을 최소화하여 만약에 발생할 수 있는 잠재적인 사고를 미연에 방지

o 서비스거부공격 및 웜 발생을 확실하게 예상할 수 있거나 내부 시스템 및 네트워크에 대규모 피해 확산을 예상할 수 있는 경우, 기관장의 승인을 받고 물리적인 케이블 분리 등을 통해 피해 대상 네트워크를 단절

o 피해를 당한 해당 기관의 정보보안담당자는 사고와 관련된 데이터뿐만 아니라 데이터백업 및 로그관리 등 사고조사에 필요한 자료를 제공

(바) 과학기술정보보호센터는 급속한 피해확산이 우려되는 경우 과학기술부에 통보하고 실무기관에 네트워크 연결 차단 권고

(4) 피해복구 조치

(가) 과학기술부 차원의 복구지원팀 구성 운영

o 피해상황의 파악 및 복구 절차 수립·시행

o 심각한 피해의 경우 범정부 복구지원팀과 연계하여 복구 활동 지원

o 피해복구 및 사후 처리 결과 종합 보고

※ 복구지원팀 임무·구성·운영 방법은 (P69) 참조

o 경미한 사고는 피해 기관이 자체 복구

※ 조치 상황을 과학기술부 및 과학기술정보보호센터에 통보

o 중대한 사고는 과학기술부 복구지원팀 지원 하에 복구

o 심각한 사고는 범정부「복구지원팀」에 의해 복구

(5) 처리상황 보고

(가) 경계 경보단계 조치 수행

o 경계 경보단계 조치 수행

(나) 경보해제 및 하향 조정

o NCSC에서 경보 해제 또는 하향 조정이 전파된 경우 반장에게 보고하고 경보 해제 또는 하향 조정전파

※ 전파절차 및 전파수단·대상은 발령의 경우와 동일

(다) 종결보고

o 경보 해제 또는 하향 조정의 경우 종결보고 실시

o 보고체계 : 사고대책본부장 → 과학기술부 장관

o 보 고 자 : 사고대책본부장(정책홍보관리실장)

o 보고방법 : 내부보고 양식에 따라 종결보고

※ 합동조사팀 및 복구지원팀 운영결과 반영

o 보고 종료 후 상황해제 및 사고대책본부 해체

(6) 후속조치

(가) 사고재발 방지대책 수립 및 전파

o 기밀자료 유출 사고발생 기관에 대한 전산망 보안강화 대책, 유포된 기밀자료에 대한 효력정지 방안을 마련

o 예산 인력이 수반되는 국가차원의 대책에 대해서는 유관 기관(국가정보원, 기획예산처, 행정자치부)에 지원 요청

Ⅱ. 홈페이지 대량 변조 사고

1. 관심의 경우 조치사항 및 처리절차

가. 상 황

□ 개 요

o 국내 공공기관, 인터넷쇼핑몰, 개인사용자 홈페이지 등 국내에서 가장 많이 쓰이고 있는 AA-Board 게시판 프로그램의 취약점이 해외 유명 해킹정보 사이트(www.securiyfocus.com)에 등록됨에 따라 국내 홈페이지에 대한 변조 및 정보유출을 시도하는 해킹 공격이 우려되고 있음

□ 세부 내용

o 사고신고 일시 및 내용 : 7월 6일 18:30

- AA-Board 게시판 프로그램의 취약점이 해킹 정보 사이트(www.securityfous.com)에 등록되었음이 과학기술정보보호센터(S&T-SEC)에 신고 접수됨
- 현재까지 AA-Board 게시판 프로그램의 취약점을 이용한 홈페이지 공격에 의한 사고는 보고되지 않음
- 국가정보원 국가사이버안전센터(NCSC)에서는 AA-Board 게시판 프로그램의 중요성을 고려하여 “관심” 경보 발령을 통해 홈페이지 사용에 대한 주의를 요청함

o 피해 현황

- AA-Board 게시판은 프로그램은 국내에서 개발되어 주로 사용됨에 따라 해외에서 사고 발생보고는 없음
- AA-Board 게시판 프로그램의 취약점 패치가 개발되고 있음

나. 조치사항 및 절차

(1) 조치 목록

조치사항	세부 내용
위기상황 접수 및 보고/전파	o 보고 및 내부 상황전파
초동조치	o 사이버위협 분석 o 「관심」경보 발령 전파 ※ 과학기술부는 경보발령 내용 접수시 과학기술정보보호센터 및 실무기관 등에 신속히 전파 o 보안권고문 및 보안조치 등 이행 권고문이 NCSC에서 배포된 경우 전파/보호대책 이행
긴급대응조치	o 백신 및 탐지룰 업데이트 배포 o 과학기술부 차원의「긴급대응반」가동 준비 및 필요시 긴급대응반 비상소집 o 국내외 유관기관 동향 파악 및 협조 o 모니터링 강화 o 불필요한 서비스 차단 및 차단규칙 점검 o 상황 조치 결과 취합 ※ 과학기술부는 실무기관 등의 조치결과를 취합, NCSC로 통보 o 피해 발생시 주의 단계 조치 수행
처리상황 보고	o 조치상황 종합 및 보고

다. 조치 내용

(1) 위기상황 접수 및 보고/전파

(가) 보고 및 내부 상황전파

o NCSC에서 관심 경보 발령의 경우 긴급대응반 상황총괄팀은 사이버 위협 내용을 상부에 보고하고 과학기술부 전 직원에게 신속히 전파

※ 보고내용 및 양식은「붙임 1」참조

(2) 초동조치

(가) 사이버위협 분석

o 긴급대응반 분석대응팀은 공격기법 및 피해 가능성 등을 분석

o 긴급대응반 상황총괄팀은 해킹조직의 공격에 대한 피해 가능성이 높은 상태이므로 지속적으로 모니터링하고 위기 징후를 감시

o 정보보호 제품 공급 社와 상황공유 및 업데이트 의뢰

- 긴급대응반 분석대응팀은 정보보호 제품 공급社(침입차단·탐지시스템 제작업체, 백신업체 등)에 정보제공 및 탐지룰 업데이트 요청

※ 악성코드 샘플 제공할 정보보호업체 목록은「붙임 9」참조

(나) **관심** 경보 발령 전파

o **관심** 경보 발령의 경우 접수 후, 반장에게 보고하고 과학기술정보보호센터 및 실무기관에 신속히 전파

- 긴급대응반 상황총괄팀은 사이버 위기경보를 반장에게 보고하고, NCSC의 **관심** 경보 발령사실을 과학기술정보보호센터에 신속히 전파

△ 전파대상 : 과학기술정보보호센터

△ 전파수단 : SMS, FAX, 전화, 전자우편 및 홈페이지

- 과학기술정보보호센터는 실무기관에 **관심** 경보 발령 사실을 신속히 전파

△ 전파대상 : 실무기관

△ 전파수단 : SMS, FAX, 전화, 전자우편 및 홈페이지

- 실무기관은 위기경보를 접수하고 신속히 기관내 소속원에게 **관심** 경보 발령 사실을 전파

※ 경보발령 양식 및 상황조치 작성양식은「붙임 3, 4」참조

(다) 보안권고문 및 보안조치 등 이행 권고문이 NCSC에서 배포된 경우 전파/보호대책 이행

o 긴급대응반 상황총괄팀은 보안권고문 및 보안조치, 대응요령 등 이행 권고문이 NCSC에서 배포된 경우 이를 과학기술정보보호센터에 전파하고, 과학기술정보보호센터는 실무기관에 전파

o 실무기관은 보안권고문 및 보안조치, 대응요령 등 이행 권고문에 따른 보호대책 이행

(3) 긴급대응 조치

(가) 백신 및 탐지룰 업데이트 배포 및 적용

o 백신(취약점 패치) 및 탐지룰이 제공되는 경우 과학기술정보보호센터를 통하여 실무기관에 배포

o 실무기관은 배포된 백신(취약점 패치) 및 탐지룰을 자체 시스템에 적용

(나) 긴급대응반 가동 준비 및 필요시 긴급대응반 비상소집

o 긴급대응반 반장은 상황을 예의 주시하고 긴급대응반 가동 준비 및 필요시 긴급대응반 비상소집

o 과학기술정보보호센터는 긴급대응반이 가동될 경우 신속한 현장 지원

(다) 국내외 유관기관 동향 파악 및 협조

o 국가사이버안전센터(NCSC), 정보통신부 등 보안관제를 수행하는 기관에 대한 동향 파악 및 상호협조

(라) 모니터링 강화

o 해킹에 대한 피해 발생가능성이 높은 상태이므로 지속적으로 모니터링 및 위기징후 감시 강화

- 과학기술정보보호센터 및 실무기관은 사이버 위협에 대한 모니터링 및 위기징후 감시체제 강화

(마) 불필요한 서비스 차단 및 차단규칙 점검

o 업무수행에 반드시 필요한 서비스를 제외한 일반적인 시스템 서비스에 대해서는 해당 프로세스의 실행을 중지시키거나 서비스 포트를 차단하여 취약점에 대한 위협을 최소화

o 라우터의 CAR(Committed Access Rate), ACL(Access Control List) 설정 내용과 스위치, 침입차단 시스템의 IP주소 또는 포트번호에 대한 허용 및 차단 규칙을 확인

o 서비스 포트를 허용할 때는 서비스를 제공하는 특정 포트만을 허용 하도록 설정하였는지 점검

(바) 상황조치 결과 취합

o 실무기관은 경보발령에 따른 대응조치 수행 후 과학기술정보보호센터 기술지원팀에 상황통보

※ 상황조치 통보서는「붙임 2」참조

o 과학기술정보보호센터 기술지원팀은 상황조치 결과를 취합하여 과학기술부 상황총괄팀에 보고

o 긴급대응반 상황총괄팀은 상황조치 결과를 취합하여, 반장에게 보고하고 국가정보원(NCSC)에 통보

(사) 피해 발생시 **주의** 단계 조치 수행

o 피해가 발생되어 NCSC에서 **주의** 단계로 상향조정하는 경우 **주의** 단계 조치 시행(P107 참조)

(4) 처리상황 보고

(가) 조치상황 종합 및 보고

o 긴급대응반 상황총괄팀 및 분석대응팀은 피해 및 대응현황을 종합·정리하여 보안관제 상황과 조치현황에 대한 종합 보고서를 작성하여 반장에게 보고

2. 주의의 경우 조치사항 및 처리절차

가. 상 황

□ 개 요

o AA-Board게시판 프로그램을 사용하고 있는 OOO연구원, OOO 국가기관 및 소규모 인터넷 쇼핑몰 등 100여개의 국내 홈페이지가 해외 해커에 의하여 변조되는 피해가 발생함

□ 세부 내용

o 사고신고 일시 및 내용 : 7월 7일 20:30

- AA-Board게시판 프로그램을 사용하고 있는 OOO 연구원의 메인 홈페이지 변조사고가 과학기술정보보호센터에 신고 접수됨
- AA-Board게시판 프로그램을 이용하는 50개 공공기관 및 인터넷 쇼핑 홈페이지 변조 사고가 www.zone-h.org에 게시되었음을 과학기술정보보호센터에서 탐지

  ※ www.zone-h.org : 홈페이지 해킹 결과를 과시하는 해킹사이트
- 과학기술정보보호센터에서는 탐지 및 신고 접수된 현황을 국가사이버안전센터에 통보
- 국가정보원 국가사이버안전센터(NCSC)에서 “주의” 경보 발령을 통해 AA-Board 게시판 프로그램 사용자에 대한 주의요청

o 피해 현황

- AA-Board게시판 프로그램을 사용하고 있는 OOO 연구원 홈페이지가 브라질 해커그룹 “△△△그룹“에 의하여 변조되는 사고가 발생함
- 아직까지 AA-Board 취약점 패치 파일이 개발되지 않아 대량의 피해가 우려되고 있으며 피해발생 증가 추세임

나. 조치사항 및 절차

(1) 조치 목록

조치사항	세부 내용
위기상황 접수 및 보고/전파	o 관심 단계에서 피해발생 및 사고 신고
초동조치	o 사고원인 분석 o「주의」경보 발령 전파 ※ 과학기술부는 경보발령 내용 접수시 과학기술정보보호센터 및 실무기관 등에 신속히 전파
긴급대응조치	o 필요시 긴급대응반 비상소집 o 국내외 유관기관 동향 파악 및 협조 강화 o 피해현황 파악 및 사고조사 o 공격 진원지·경유지 접속 차단 및 보안대책 시행 o 피해 확산시 경계 단계 조치 수행
피해복구 조치	o 피해확산 방지 및 복구 조치 o 기관별 피해복구 추진 실태 파악
처리상황 보고	o 관심 경보단계 조치 수행
후속조치	o 재발 방지대책 수립·전파

관심 경보 조치 지속적 수행

다. 조치 내용

(1) 위기상황 접수 및 보고/전파

(가) 관심단계에서 피해발생 및 사고신고

o 실무기관에서 AA-Board 게시판 프로그램을 사용하고 있는 홈페이지 등에 대한 피해가 발생하여 관련 사실을 과학기술정보보호센터에 신고

o 과학기술정보보호센터는 연구기관의 홈페이지에 대한 피해 발생 사실을 과학기술부에 보고

o 과학기술부는 피해사실을 NCSC에 통보

※ 사고신고 양식은「붙임 3」참조

(2) 초동조치

(가) 사고 원인분석

o 긴급대응반 분석대응팀은 피해기관에 출동, 공격기법·피해양상 등을 분석하고, 상황총괄팀은 관제시스템에 탐지룰 적용

(나) **주의** 경보 발령 전파

o **주의** 경보 발령의 경우 접수 후, 반장에게 보고하고 과학기술정보보호센터 및 실무기관에 신속히 재전파

- 긴급대응반 상황총괄팀은 사이버 위기경보를 반장에게 보고하고, NCSC의 **주의** 경보 발령사실을 과학기술정보보호센터에 신속히 재전파

△ 전파대상 : 과학기술정보보호센터

△ 전파수단 : SMS, FAX, 전화, 전자우편 및 홈페이지

- 과학기술정보보호센터는 실무기관에 **주의** 경보 발령 사실을 신속히 재전파

△ 전파대상 : 실무기관

△ 전파수단 : SMS, FAX, 전화, 전자우편 및 홈페이지

- 실무기관은 위기경보를 접수하고 신속히 기관내 소속원에게 **주의** 경보 발령 사실을 재전파

※ 경보발령 양식 및 상황조치 작성양식은「붙임 1, 2」참조

(3) 긴급대응 조치

(가) 필요시 긴급대응반 비상소집

o 긴급대응반 반장은 평시 긴급대응반 운영계획을 수립유지

o 긴급대응반 운영에 대한 비상연락망 인원 및 연락처를 점검하여 최신 내용으로 갱신

o 경보발령 체계도에 따른 연락체계 확인

o 필요시 긴급대응반 비상소집

o 과학기술정보보호센터 및 실무기관 등도 비상연락망 및 연락처를 점검하여 최신 내용으로 갱신

o 실무기관은 정보보호시스템, 네트워크 장비 등 시스템 및 프로그램을 제공한 업체간의 연락체계 점검

(나) 국내외 유관기관 동향 파악 및 협조 강화

o 국가사이버안전센터(NCSC), 정보통신부 등 보안관제를 수행하는 기관에 대한 동향 파악 및 상호협조 강화

(다) 피해현황 파악 및 사고조사

o 과학기술부 실무기관 정보보호담당자는 해당 기관에 사고 발생시 즉시 과학기술정보보호센터에 피해내용을 통보하고, 자체 조사 및 복구 수행, 결과를 과학기술정보보호센터에 통보

※ 사고신고 및 사고조치 작성양식은「붙임 3, 4」참조

o 과학기술정보보호센터는 과학기술부에 피해 내용을 보고

o 과학기술부는 피해내용을 NCSC에 통보

o 긴급대응반 상황총괄팀·분석대응팀·복구지원팀은 피해현황을 파악하고 사고조사 계획을 수립하는 등 대응조치

o 긴급대응반 분석대응팀은 사고 조사를 수행하여 원인을 분석하고 공격·경유지 등을 확인

(라) 공격진원지·경유지 접속 차단 및 보안대책 시행

o 긴급대응반 분석대응팀은 피해확산 방지를 위해 공격지 및 경유지에 대한 접속 차단을 긴급대응반장에 건의

o 긴급대응반 상황총괄팀은 NCSC에 공격·경유지에 대한 접속을 차단토록 요청

o 공격대상 시스템의 IP주소 또는 공격대상 서비스 포트번호의 차단 상태 확인

o 침입차단시스템, 침임탐지시스템 등을 이용하여 공격대상 시스템, 서비스 포트번호 등에 대하여 모니터링 강화

o 특정 소프트웨어를 통해 악성코드에 감염될 경우, 해당 소프트웨어를 해지하고 추가적 설치를 금함

(마) 피해 확산시 **경계** 단계 조치 수행

o 피해가 확산되어 NCSC에서 **경계** 단계로 상향조정하는 경우 **경계** 단계 조치 시행(P114 참조)

(4) 피해복구 조치

(가) 피해확산 방지 및 복구조치

o 긴급대응반 분석대응팀은 피해기관 목록 작성 후 피해복구 우선순위를 산정하고 원격·현장 복구계획을 수립

※ 피해기관 목록 작성 양식은「붙임 10~13」참조

o 복구 우선순위 산정 시 피해기관의 연구정보자원의 중요도, 경제·사회적 중요도 등을 고려해 판단

o 긴급대응반(과학기술정보보호센터 중심)으로 복구 인력을 편성하되, 필요시 피해기관 전산망 유지보수 업체등과 합동 복구 실시

(나) 기관별 피해복구 추진실태 파악

o 긴급대응반 복구지원팀은 기관별 피해복구 추진실태를 수시파악, 복구가 미흡한 기관에 인력·장비 등 가용자원을 집중 투입할 수 있도록 피해복구 우선순위를 재설정

o 긴급대응반 분석대응팀은 상황 조치 결과를 취합해 피해 범위 및 피해예방조치 현황을 파악하는 한편, 조치가 미흡한 기관에 대해서는 보완을 권고

(5) 처리상황 보고

(가) 관심 경보단계 조치 수행

o 관심 경보단계 조치 수행

(6) 후속조치

(가) 재발 방지대책 수립・전파

o 긴급대응반 분석대응팀은 사고원인이 된 AA-Board게시판 프로그램에 대한 보안취약점 분석결과, 도출된 문제점 개선 및 재발 방지대책을 수립・전파

3. 경계의 경우 조치사항 및 처리절차

가. 상 황

□ 개 요

o AA-Board게시판 프로그램을 사용하고 있는 OOO연구원, OOO 국가기관 및 인터넷 쇼핑몰 등 200여개의 국내 홈페이지가 해외 해커에 의하여 변조되는 피해가 발생함
특히, 해당 게시판 프로그램의 취약점 상세설명과 취약점을 공격하는 자동화된 해킹툴이 사용방법 설명과 함께 유명 해킹정보 사이트(www.securityfoucs.com)에 공개됨에 따라 국내의 홈페이지에 대한 대량 피해가 예상되고 있음

□ 세부 내용

o 사고신고 일시 및 내용 : 7월 9일 10:30

- AA-Board게시판 프로그램을 사용하고 있는 △△△연구원 등 50여개 연구원의 메인 홈페이지 변조사고가 과학기술정보보호센터에 신고 접수됨
- AA-Board게시판 프로그램을 이용하는 100여개 공공기관 및 인터넷 쇼핑 홈페이지 변조 사고가 www.zone-h.org에 게시되었음을 과학기술정보보호센터에서 탐지
  ※ www.zone-h.org : 홈페이지 해킹 결과를 과시하는 해킹사이트
- 과학기술정보보호센터에서는 탐지 및 신고 접수된 현황을 국가사이버안전센터에 통보
- 국가정보원 국가사이버안전센터(NCSC)에서 “경계” 경보 발령을 통해 공조 대응을 요청함

o 피해 현황

- AA-Board게시판 프로그램을 사용하고 있는 △△△연구원 등 200여개의 홈페이지가 변조되는 사고가 발생함

나. 조치사항 및 절차

(1) 조치 목록

조치사항	세부 내용
위기상황 접수 및 보고/전파	o 주의 단계에서 피해확산 및 사고 신고
초동조치	o「경계」경보 발령 전파 ※ 과학기술부는 경보발령 내용 접수시 과학기술정보보호센터 및 실무기관 등에 신속히 전파
긴급대응조치	o 긴급대응반 증원 운영 o 실무기관은 필요시 자체대응반 운영 o 피해 확산시 경계 단계 조치 수행
피해복구 조치	o 주의 경보단계 조치 수행
처리상황 보고	o 주의 경보단계 조치 수행
후속조치	o 유출 자료에 대한 안보영향평가 실시

주의 경보 조치 지속적 수행

다. 조치 내용

(1) 위기상황 접수 및 보고/전파

(가) 주의 단계에서 피해확산 및 사고 신고

o 실무기관에서 AA-Board 게시판 프로그램을 사용하고 있는 홈페이지 등에 대한 피해가 확산되어 관련 사실을 과학기술정보보호센터에 신고

o 과학기술정보보호센터는 연구기관의 홈페이지에 대한 피해확산 사실을 과학기술부에 보고

o 과학기술부는 피해확산 사실을 NCSC에 통보

※ 사고신고 양식은「붙임 3」참조

(2) 초동조치

(가) **경계** 경보 발령 전파

o **경계** 경보 발령의 경우 접수 후, 반장에게 보고하고 과학기술정보보호센터 및 실무기관에 신속히 재전파

- 긴급대응반 상황총괄팀은 사이버 위기경보를 반장에게 보고하고, NCSC의 **경계** 경보 발령사실을 과학기술정보보호센터에 신속히 재전파

△ 전파대상 : 과학기술정보보호센터

△ 전파수단 : SMS, FAX, 전화, 전자우편 및 홈페이지

- 과학기술정보보호센터는 실무기관에 **경계** 경보 발령사실을 신속히 재전파

△ 전파대상 : 실무기관

△ 전파수단 : SMS, FAX, 전화, 전자우편 및 홈페이지

- 실무기관은 위기경보를 접수하고 신속히 기관내 소속원에게 **경계** 경보 발령 사실을 재전파

※ 경보발령 양식 및 상황조치 작성양식은「붙임 1, 2」참조

(3) 긴급대응 조치

(가) 긴급대응반 증원 운영

o 긴급대응반 반장은 증원 및 대비계획 점검

o 과학기술정보보호센터는 긴급대응반 현장파견 인원 증원

o 과학기술부는 실무기관이 NCSC 및 프로그램 제작업체에서 제공한 AA-Board 게시판 프로그램에 대한 대응요령을 모두 이행하고 있는지 재확인

o 과학기술정보보호센터는 급속한 피해확산이 우려되는 경우 과학기술부에 통보하고 실무기관에 네트워크 연결 차단 권고

(나) 실무기관은 필요시 자체 대응반 운영

o 과학기술부는 피해확산이 예상되거나 피해상황 추이에 따라 시스템 복구 및 피해확산 차단을 위해 실무기관에 자체 대응반 가동을 독려

o 피해가 예상되거나 피해상황 추이에 따라 자체대응반을 투입, 즉각적인 시스템복구를 실시하고 피해확산 차단조치

o 서비스거부공격에 대한 이상 징후를 포착한 경우 정보보안 담당자는 신속하게 라우터, 침입차단시스템 등의 차단 규칙을 재설정하여 공격 진행을 차단

※ 서비스거부공격 이상징후 포착시 공격전개 차단에 대한 자세한 방법은 국가사이버안전매뉴얼 부록 참조(p249)

o 중요 정보자료를 갖고 있는 서버 및 중요한 서버의 자료를 백업하여 네트워크와 단절된 안전한 곳에 보관

o 악성코드, 취약점, 공격도구 등에 대한 분석정보에 따른 공격대상 시스템의 IP 주소 또는 공격대상 서비스 포트번호의 차단 상태를 수시로 확인

o 침입차단시스템, 침입탐지시스템 등을 이용하여 취약점을 재점검하여 발견된 취약점 제거

o 피해발생 가능성이 높은 네트워크를 대상으로 물리적인 케이블 분리 등의 단절시행 여부를 검토하고, 필요할 경우 기관장의 승인하에 단절

(다) 피해 확산시 **심각** 단계 조치 수행

o 피해가 확산되어 NCSC에서 **심각** 단계로 상향조정하는 경우 **심각** 단계 조치 시행(P120 참조)

(4) 피해복구 조치

(가) 주의 경보단계 조치 수행

o 주의 경보단계 조치 수행

(5) 처리상황 보고

(가) 주의 경보단계 조치 수행

o 주의 경보단계 조치 수행

(6) 후속조치

(가) 유출 자료에 대한 안보영향평가 실시

o 대외비 이상의 비밀이 유출된 경우 과학기술부는 해당 비밀 자료의 국가안보상 파급효과 분석을 위해 해당기관 담당자 및 관련 분야 전문가를 소집, 안보영향평가 실시

o 안보에 영향이 있다고 판단된 경우, 피해기관은 해당 비밀에 효력정지 및 취소 등의 조치 수행

4. 심각의 경우 조치사항 및 처리절차

가. 상 황

□ 개 요

o AA-Board게시판 프로그램의 취약점이 추가로 유명 해킹정보 사이트(www.securityfoucs.com)에 공개되면서 AA-Board를 이용하는 국내 대부분의 홈페이지가 변조됨에 따라 국가 행정서비스, 전자상거래 서비스등에 장애가 발생하여 국내 인터넷 사용에 심각한 장애가 발생함

□ 세부 내용

o 사고신고 일시 및 내용 : 7월 10일 12:00

- AA-Board 게시판 프로그램을 사용하고 있는 대다수의 국가·공공기관 및 인터넷서비스업체, 은행등의 홈페이지 변조 사고가 신고 접수됨
- 과학기술정보보호센터에서는 탐지 및 신고 접수된 현황을 국가사이버안전센터에 통보
- 국가정보원 국가사이버안전센터(NCSC)에서 “심각” 경보 발령을 통해 AA-Board 게시판 취약점 제거 및 홈페이지 변조에 대응하기 위한 국가적 차원의 공동대처 요청

o 피해 현황

- AA-Board 게시판 프로그램을 사용하고 있는 국내 대다수 홈페이지가 변조되어 정상적인 서비스가 불가능함
- 대부분의 국가기관 홈페이지가 변조됨에 전자정부 서비스 장애 및 국가 신뢰도에 대한 악영향이 우려됨
- 인터넷쇼핑몰 및 인터넷 뱅킹 등의 홈페이지가 해킹 사고로 인한 서비스 장애로 막대한 경제적 손실이 우려됨

나. 조치사항 및 절차

(1) 조치 목록

조치사항	세부 내용
위기상황 접수 및 보고/전파	o 경계 단계에서 피해확산 및 사고 신고
초동조치	o「심각」경보 발령 전파 ※ 과학기술부는 경보발령 내용 접수시 과학기술정보보호센터 및 실무기관 등에 신속히 전파
긴급대응조치	o 사고대책본부 구성 운영 o 비상총괄반 구성 운영 o 과기부차원의 합동조사팀 구성 운영 o 과학기술정보보호센터 지원팀, Help-Desk팀 가동 o 실무기관은 자체대응반 가동 o 피해발생 가능성이 높은 네트워크 단절여부 판단
피해복구 조치	o 과기부차원의 복구지원팀 구성 운영
처리상황 보고	o 경보해제 및 하향조정 전파 o 종결보고
후속조치	o 사고재발 방지대책 수립 및 전파

경계 경보 조치 지속적 수행

다. 조치 내용

(1) 위기상황 접수 및 보고/전파

(가) 경계 단계에서 피해확산 및 사고 신고

o 일부기관을 중심으로 피해가 확산되던 AA-Board 게시판 변조 공격이 국내 전체로 피해확산

o 실무기관에서 AA-Board 게시판 프로그램 변조 공격에 대한 피해가 확산되어 관련 사실을 과학기술정보보호센터에 신고

o 과학기술정보보호센터는 연구기관의 홈페이지 변조에 대한 피해확산 사실을 과학기술부에 보고

o 과학기술부는 피해확산 사실을 NCSC에 통보

※ 사고신고 양식은「붙임 3」참조

(2) 초동조치

(가) **심각** 경보 발령 전파

o **심각** 경보 발령의 경우 접수 후, 반장에게 보고하고 과학기술정보보호센터 및 실무기관에 신속히 재전파

- 긴급대응반 상황총괄팀은 사이버 위기경보를 반장에게 보고하고, NCSC의 **심각** 경보 발령사실을 과학기술정보보호센터에 신속히 재전파

△ 전파대상 : 과학기술정보보호센터

△ 전파수단 : SMS, FAX, 전화, 전자우편 및 홈페이지

- 과학기술정보보호센터는 실무기관에 **심각** 경보 발령 사실을 신속히 재전파

△ 전파대상 : 실무기관

△ 전파수단 : SMS, FAX, 전화, 전자우편 및 홈페이지

- 실무기관은 위기경보를 접수하고 신속히 기관내 소속원에게 **심각** 경보 발령 사실을 재전파

※ 경보발령 양식 및 상황조치 작성양식은「붙임 1, 2」참조

(3) 긴급대응 조치

(가) 사고대책본부 구성 운영

o 정책홍보실장을 본부장으로 하는 사고대책본부를 구성하여 즉각 대응태세 돌입

- 관제인력 증원 및 탐지룰 적용 등 보안관제 강화

- 각 분야·부문별 관제센터와 수시 연락 및 동향파악 강화

※ 사고대책본부 구성, 역할, 세부임무는 (P42~43) 참조

(나) 비상총괄반 구성

o 비상계획 담당관을 반장으로 하는 비상총괄반 구성 운영

o 비상사태 및 위기관리에 관한 계획 수립 및 점검

(다) 과학기술부 차원의 합동조사팀 구성 운영

o 피해범위 및 복구시간 등에 따라 다수의 반으로 구성

o 피해현황 파악 및 사고조사

- 합동조사팀은 피해규모를 파악하고 현장·원격조사 계획 수립 및 이행

- 홈페이지 변조 시각, 정보보호시스템에 기록된 각종 로그, 피해 시스템내 이벤트 로그 등을 종합 분석

※ 합동조사팀 임무, 구성, 운영방법은 (P68~69) 참조

(라) 과학기술정보보호센터 지원팀 및 Help-Desk팀 가동

- 과학기술부 사고대책본부를 지원하기 위한 지원팀, Help-Desk 팀을 가동하고 즉각 대응태세 돌입
- 과학기술부 합동조사팀 현장지원(조사 주관)

(마) 실무기관은 자체 대응반 가동

o 실무기관은 자체대응반을 가동하고 즉각 대응 태세 돌입

o 악성코드, 취약점, 공격도구 등에 대한 분석정보가 발표될 경우, 라우터·스위치 및 침입차단시스템의 차단규칙을 추가 설정하여 공격대상 서비스 포트를 차단

※ 공격대상 서비스 포트 차단에 대한 자세한 방법은 국가사이버안전매뉴얼 부록 참조(p249)

o 기관내 홈페이지 AA-Board 게시판 프로그램 사용을 최소화하여 만약에 발생할 수 있는 잠재적인 사고를 미연에 방지

o 해커 공격으로 인해 확실하게 예상할 수 있거나 내부 시스템 및 네트워크에 대규모 피해 확산을 예상할 수 있는 경우, 기관장의 승인을 받고 물리적인 케이블 분리 등을 통해 피해대상 네트워크를 단절

o 피해를 당한 해당 기관의 정보보안담당자는 사고와 관련된 데이터뿐만 아니라 데이터백업 및 로그관리 등 사고조사에 필요한 자료를 제공

(바) 과학기술정보보호센터는 급속한 피해확산이 우려되는 경우 과학기술부에 통보하고 실무기관에 네트워크 연결 차단 권고

(4) 피해복구 조치

(가) 과학기술부 차원의 복구지원팀 구성 운영

o 피해상황의 파악 및 복구 절차 수립·시행

o 심각한 피해의 경우 범정부 복구지원팀과 연계하여 복구 활동 지원

o 피해복구 및 사후 처리 결과 종합 보고

※ 복구지원팀 임무·구성·운영 방법은 (P68) 참조

o 경미한 사고는 피해 기관이 자체 복구

※ 조치 상황을 과학기술부 및 과학기술정보보호센터에 통보

o 중대한 사고는 과학기술부 복구지원팀 지원 하에 복구

o 심각한 사고는 범정부「복구지원팀」에 의해 복구

(5) 처리상황 보고

(가) 경계 경보단계 조치 수행

o 경계 경보단계 조치 수행

(나) 경보해제 및 하향 조정

o NCSC에서 경보 해제 또는 하향 조정이 전파된 경우 반장에게 보고하고 경보 해제 또는 하향 조정전파

※ 전파절차 및 전파수단·대상은 발령의 경우와 동일

(다) 종결보고

o 경보 해제 또는 하향 조정의 경우 종결보고 실시

o 보고체계 : 사고대책본부장 → 과학기술부 장관

o 보 고 자 : 사고대책본부장(정책홍보관리실장)

o 보고방법 : 내부보고 양식에 따라 종결보고

※ 합동조사팀 및 복구지원팀 운영결과 반영

o 보고 종료 후 상황해제 및 사고대책본부 해체

(6) 후속조치

(가) 사고재발 방지대책 수립 및 전파

o 기밀자료 유출 사고발생 기관에 대한 홈페이지 보안강화 대책, 유포된 기밀자료에 대한 효력정지 방안을 마련

o 예산 인력이 수반되는 국가차원의 대책에 대해서는 유관기관(국가정보원, 기획예산처, 행정자치부)에 지원 요청

Ⅲ. 국제 사이버테러 단체에 의한 국가망 DDoS 공격

1. 관심의 경우 조치사항 및 처리절차

가. 상 황

□ 개 요

o 2007년 9월 개최되는 UN정기총회 고위급 본회의 시점에 맞추어 국제적 사이버테러단체로부터 UN전산망 및 미국 주요전산망을 대상으로 사이버테러 경고메일이 발송되었으며, 본회의 개최날인 9월 16일 UN전산망 및 미국 주요 전산망으로 DDoS 공격이 발생되어 약 2시간 가량동안 전산망이 마비되는 사고가 발생함에 따라 국내 중요 전산망에 대한 공격도 우려되고 있음

□ 세부 내용

o 사고신고 일시 및 내용 : 10월 10일 15:00

- 미국 DHS(국토안보부)로부터 국제사이버테러단체의 DDoS 공격에 대한 관련 내용을 메일로 수신
- 영국의 NISCC(국가기반시설보안조정센터)로부터 국제사이버테러단체의 DDoS 공격과 동일한 패턴의 공격에 대한 탐지 관련 내용을 메일로 수신
- 현재까지 국내에서 국제사이버테러단체의 DDoS와 동일한 패턴의 공격시도는 탐지되지 않고 있음
- 국가정보원 국가사이버안전센터(NCSC)에서 “관심” 경보 발령을 통해 국제사이버테러단체의 DDoS 공격에 대한 주의 요청

o 피해 현황

- UN전산망에 대한 국제사이버테러단체로부터의 DDoS 공격이 발생하여 약 2시간 동안 전산망이 마비되어 인터넷 서비스가 이루어지지 않음
- 영국, 프랑스 등 유럽 국가의 국가 중요 전산망에 대한 동일 패턴의 소규모 DDoS 공격이 발생함

나. 조치사항 및 절차

(1) 조치 목록

조치사항	세부 내용
위기상황 접수 및 보고/전파	o 보고 및 내부 상황전파
초동조치	o 사이버위협 분석 o 「관심」경보 발령 전파 ※ 과학기술부는 경보발령 내용 접수시 과학기술정보보호센터 및 실무기관 등에 신속히 전파 o 보안권고문 및 보안조치 등 이행 권고문이 NCSC에서 배포된 경우 전파/보호대책 이행
긴급대응조치	o 백신 및 탐지룰 업데이트 배포 o 과학기술부 차원의「긴급대응반」가동 준비 및 필요시 긴급대응반 비상소집 o 국내외 유관기관 동향 파악 및 협조 o 모니터링 강화 o 불필요한 서비스 차단 및 차단규칙 점검 o 상황 조치 결과 취합 ※ 과학기술부는 실무기관 등의 조치결과를 취합, NCSC로 통보 o 피해 발생시 주의 단계 조치 수행
처리상황 보고	o 조치상황 종합 및 보고

다. 조치 내용

(1) 위기상황 접수 및 보고/전파

(가) 보고 및 내부 상황전파

o NCSC에서 관심 경보 발령의 경우 긴급대응반 상황총괄팀은 사이버 위협 내용을 상부에 보고하고 과학기술부 전 직원에게 신속히 전파

※ 보고내용 및 양식은「붙임 1」참조

(2) 초동조치

(가) 사이버위협 분석

o 긴급대응반 분석대응팀은 공격기법 및 피해 가능성 등을 분석

o 긴급대응반 상황총괄팀은 국제사이버테러단체로부터의 DDoS 공격에 대한 피해 가능성이 높은 상태이므로 지속적으로 모니터링하고 위기 징후를 감시

o 정보보호 제품 공급 社와 상황공유 및 업데이트 의뢰

- 긴급대응반 분석대응팀은 정보보호 제품 공급社(침입차단·탐지시스템 제작업체, 백신업체 등)에 정보제공 및 웜·바이러스 백신 탐지룰 업데이트 요청

※ 악성코드 샘플 제공할 정보보호업체 목록은「붙임 9」참조

(나) **관심** 경보 발령 전파

o **관심** 경보 발령의 경우 접수 후, 반장에게 보고하고 과학기술정보보호센터 및 실무기관에 신속히 전파

- 긴급대응반 상황총괄팀은 사이버 위기경보를 반장에게 보고하고, NCSC의 **관심** 경보 발령사실을 과학기술정보보호센터에 신속히 전파

△ 전파대상 : 과학기술정보보호센터

△ 전파수단 : SMS, FAX, 전화, 전자우편 및 홈페이지

- 과학기술정보보호센터는 실무기관에 **관심** 경보 발령사실을 신속히 전파

△ 전파대상 : 실무기관

△ 전파수단 : SMS, FAX, 전화, 전자우편 및 홈페이지

- 실무기관은 위기경보를 접수하고 신속히 기관내 소속원에게 **관심** 경보 발령 사실을 전파

※ 경보발령 양식 및 상황조치 작성양식은「붙임 3, 4」참조

(다) 보안권고문 및 보안조치 등 이행 권고문이 NCSC에서 배포된 경우 전파/보호대책 이행

o 긴급대응반 상황총괄팀은 보안권고문 및 보안조치, 대응요령 등 이행 권고문이 NCSC에서 배포된 경우 이를 과학기술정보보호센터에 전파하고, 과학기술정보보호센터는 실무기관에 전파

o 실무기관은 보안권고문 및 보안조치, 대응요령 등 이행 권고문에 따른 보호대책 이행

(3) 긴급대응 조치

(가) 백신 및 탐지룰 업데이트 배포 및 적용

o 백신(취약점 패치) 및 탐지룰이 제공되는 경우 과학기술정보보호센터를 통하여 실무기관에 배포

o 실무기관은 배포된 백신(취약점 패치) 및 탐지룰을 자체 시스템에 적용

(나) 긴급대응반 가동 준비 및 필요시 긴급대응반 비상소집

o 긴급대응반 반장은 상황을 예의 주시하고 긴급대응반 가동 준비 및 필요시 긴급대응반 비상소집

o 과학기술정보보호센터는 긴급대응반이 가동될 경우 신속한 현장 지원

(다) 국내외 유관기관 동향 파악 및 협조

o 국가사이버안전센터(NCSC), 정보통신부 등 보안관제를 수행하는 기관에 대한 동향 파악 및 상호협조

(라) 모니터링 강화

o 국제사이버테러단체로부터의 DDoS 공격에 대한 피해 발생 가능성이 높은 상태이므로 지속적으로 모니터링 및 위기징후 감시 강화

- 과학기술정보보호센터 및 실무기관은 사이버 위협에 대한 모니터링 및 위기징후 감시체제 강화

(마) 불필요한 서비스 차단 및 차단규칙 점검

o 업무수행에 반드시 필요한 서비스를 제외한 일반적인 시스템 서비스에 대해서는 해당 프로세스의 실행을 중지시키거나 서비스 포트를 차단하여 취약점에 대한 위협을 최소화

o 라우터의 CAR(Committed Access Rate), ACL(Access Control List) 설정 내용과 스위치, 침입차단 시스템의 IP주소 또는 포트번호에 대한 허용 및 차단 규칙을 확인

o 서비스 포트를 허용할 때는 서비스를 제공하는 특정 포트만을 허용 하도록 설정하였는지 점검

(바) 상황조치 결과 취합

o 실무기관은 경보발령에 따른 대응조치 수행 후 과학기술정보보호센터 기술지원팀에 상황통보

※ 상황조치 통보서는「붙임 2」참조

o 과학기술정보보호센터 기술지원팀은 상황조치 결과를 취합하여 과학기술부 상황총괄팀에 보고

o 긴급대응반 상황총괄팀은 상황조치 결과를 취합하여, 반장에게 보고하고 국가정보원(NCSC)에 통보

(사) 피해 발생시 **주의** 단계 조치 수행

o 피해가 발생되어 NCSC에서 **주의** 단계로 상향조정하는 경우 **주의** 단계 조치 시행(P133 참조)

(4) 처리상황 보고

(가) 조치상황 종합 및 보고

o 긴급대응반 상황총괄팀 및 분석대응팀은 피해 및 대응현황을 종합·정리하여 보안관제 상황과 조치현황에 대한 종합 보고서를 작성하여 반장에게 보고

2. 주의의 경우 조치사항 및 처리절차

가. 상 황

□ 개 요

o 2007년 11월 아시아태평양경제협력체(APEC)가 부산에서 개최됨에 따라 국가정보원(NIS)에서 국제사이버테러단체로부터의 각종 테러위험에 주의를 요청함

o 국내 OOO연구원 등 일부 출연 연구원의 백본 라우터에 이상 트래픽이 급증하는 사고로 인하여 내부 네트워크가 마비되는 피해가 발생함

□ 세부 내용

o 사고신고 일시 및 내용 : 10월 21일 10:30
- OOO연구원 등 일부 연구소에서 급격한 백본전산망의 트래픽 증가와 함께 백본전산망 전체가 마비되는 신고가 접수됨
- 과학기술정보보호센터(S&T-SEC)에서 OOO연구원 등 일부 연구소에서 발생하고 있는 비정상적인 트래픽 증가 현상 탐지
- 과학기술정보보호센터에서는 탐지 및 신고 접수된 현황을 국가사이버안전센터에 통보
- 국가정보원 국가사이버안전센터(NCSC)에서 “주의” 경보 발령을 통해 DDoS에 대한 보안태세 강화 요청

o 피해 현황
- OOO연구원등 일부 연구소에서 백본라우터의 갑작스러운 트래픽 증가로 인하여 네트워크가 마비되어 업무 장애가 발생함
- OOO연구원등 일부 연구원의 홈페이지 서버가 다운되어 약 3시간 동안 홈페이지 접속에 대한 장애가 발생함

나. 조치사항 및 절차

(1) 조치 목록

조치사항	세부 내용
위기상황 접수 및 보고/전파	o 관심 단계에서 피해발생 및 사고 신고
초동조치	o 사고원인 분석 o「주의」경보 발령 전파 ※ 과학기술부는 경보발령 내용 접수시 과학기술정보보호센터 및 실무기관 등에 신속히 전파
긴급대응조치	o 필요시 긴급대응반 비상소집 o 국내외 유관기관 동향 파악 및 협조 강화 o 피해현황 파악 및 사고조사 o 공격 진원지·경유지 접속 차단 및 보안대책 시행 o 피해 확산시 경계 단계 조치 수행
피해복구 조치	o 피해확산 방지 및 복구 조치 o 기관별 피해복구 추진 실태 파악
처리상황 보고	o 관심 경보단계 조치 수행
후속조치	o 재발 방지대책 수립·전파

관심 경보 조치 지속적 수행

다. 조치 내용

(1) 위기상황 접수 및 보고/전파

(가) 관심단계에서 피해발생 및 사고 신고

o 실무기관에서 DDoS 공격으로 추정되는 백본라우터의 비정상적인 트래픽 증가로 백본전산망이 마비되는 피해가 발생하여 관련 사실을 과학기술정보보호센터에 신고

o 과학기술정보보호센터는 DDoS 공격에 대한 피해발생 사실을 과학기술부에 보고

o 과학기술부는 피해사실을 NCSC에 통보

※ 사고신고 양식은「붙임 3」참조

(2) 초동조치

(가) 사고 원인분석

o 긴급대응반 분석대응팀은 피해기관에 출동, 공격기법·피해양상 등을 분석하고, 상황총괄팀은 관제시스템에 탐지룰 적용

(나) **주의** 경보 발령 전파

o **주의** 경보 발령의 경우 접수 후, 반장에게 보고하고 과학기술정보보호센터 및 실무기관에 신속히 재전파

- 긴급대응반 상황총괄팀은 사이버 위기경보를 반장에게 보고하고, NCSC의 **주의** 경보 발령사실을 과학기술정보보호센터에 신속히 재전파

△ 전파대상 : 과학기술정보보호센터

△ 전파수단 : SMS, FAX, 전화, 전자우편 및 홈페이지

- 과학기술정보보호센터는 실무기관에 **주의** 경보 발령 사실을 신속히 재전파

△ 전파대상 : 실무기관

△ 전파수단 : SMS, FAX, 전화, 전자우편 및 홈페이지

- 실무기관은 위기경보를 접수하고 신속히 기관내 소속원에게 **주의** 경보 발령 사실을 재전파

※ 경보발령 양식 및 상황조치 작성양식은「붙임 1, 2」참조

(3) 긴급대응 조치

(가) 필요시 긴급대응반 비상소집

o 긴급대응반 반장은 평시 긴급대응반 운영계획을 수립유지

o 긴급대응반 운영에 대한 비상연락망 인원 및 연락처를 점검하여 최신 내용으로 갱신

o 경보발령 체계도에 따른 연락체계 확인

o 필요시 긴급대응반 비상소집

o 과학기술정보보호센터 및 실무기관 등도 비상연락망 및 연락처를 점검하여 최신 내용으로 갱신

o 실무기관은 정보보호시스템, 네트워크 장비 등 시스템 및 프로그램을 제공한 업체간의 연락체계 점검

(나) 국내외 유관기관 동향 파악 및 협조 강화

o 국가사이버안전센터(NCSC), 정보통신부 등 보안관제를 수행하는 기관에 대한 동향 파악 및 상호협조 강화

(다) 피해현황 파악 및 사고조사

o 과학기술부 실무기관 정보보호담당자는 해당 기관에 사고 발생시 즉시 과학기술정보보호센터에 피해내용을 통보하고, 자체 조사 및 복구 수행, 결과를 과학기술정보보호센터에 통보

※ 사고신고 및 사고조치 작성양식은「붙임 3, 4」참조

o 과학기술정보보호센터는 과학기술부에 피해 내용을 보고

o 과학기술부는 피해내용을 NCSC에 통보

o 긴급대응반 상황총괄팀·분석대응팀·복구지원팀은 피해현황을 파악하고 사고조사 계획을 수립하는 등 대응조치

o 긴급대응반 분석대응팀은 사고 조사를 수행하여 원인을 분석하고 공격·경유지 등을 확인

(라) 공격진원지·경유지 접속 차단 및 보안대책 시행

o 긴급대응반 분석대응팀은 피해확산 방지를 위해 공격지 및 경유지에 대한 접속 차단을 긴급대응반장에 건의

o 긴급대응반 상황총괄팀은 NCSC에 공·경유지에 대한 접속을 차단토록 요청

o 공격대상 시스템의 IP주소 또는 공격대상 서비스 포트번호의 차단 상태 확인

o 침입차단시스템, 침임탐지시스템 등을 이용하여 공격대상 시스템, 서비스 포트번호 등에 대하여 모니터링 강화

(마) 피해 확산시 **경계** 단계 조치 수행

o 피해가 확산되어 NCSC에서 **경계** 단계로 상향조정하는 경우 **경계** 단계 조치 시행(P140 참조)

(4) 피해복구 조치

(가) 피해확산 방지 및 복구조치

o 긴급대응반 분석대응팀은 피해기관 목록 작성 후 피해복구 우선순위를 산정하고 원격·현장 복구계획을 수립

※ 피해기관 목록 작성 양식은「붙임 10~13」참조

o 복구 우선순위 산정 시 피해기관의 연구정보자원의 중요도, 경제·사회적 중요도 등을 고려해 판단

o 긴급대응반(과학기술정보보호센터 중심)으로 복구 인력을 편성하되, 필요시 피해기관 전산망 유지보수 업체등과 합동 복구 실시

(나) 기관별 피해복구 추진실태 파악

o 긴급대응반 복구지원팀은 기관별 피해복구 추진실태를 수시파악, 복구가 미흡한 기관에 인력·장비 등 가용자원을 집중 투입할 수 있도록 피해복구 우선순위를 재설정

o 긴급대응반 분석대응팀은 상황 조치 결과를 취합해 피해범위 및 피해예방조치 현황을 파악하는 한편, 조치가 미흡한 기관에 대해서는 보완을 권고

(5) 처리상황 보고

(가) 관심 경보단계 조치 수행

o 관심 경보단계 조치 수행

(6) 후속조치

(가) 재발 방지대책 수립・전파

o 긴급대응반 분석대응팀은 사고원인이 된 DDoS 공격에 대한 보안취약점 분석결과, 도출된 문제점 개선 및 재발 방지 대책을 수립・전파

3. 경계의 경우 조치사항 및 처리절차

가. 상 황

□ 개 요

o 국제사이버테러단체로부터 부산에서 열리는 아시아태평양경제협력체(APEC)가 개최되는 11월 12일 국내 주요 전산망에 대한 DDoS 공격을 감행하겠다는 경고 메일과 사전에 시범적인 공격을 수행하겠다는 메일이 국가사이버안전센터(NSCS)에 전송됨

o 국내 초고속연구망에 대한 DDoS 공격으로 추정되는 이상 트래픽의 급증으로 인하여 백본라우터의 서비스 장애 등 초고속연구망 전체가 마비되는 피해가 발생함

□ 세부 내용

o 사고신고 일시 및 내용 : 11월 3일 20:30

- 초고속연구망이 운영되고 있는 △△△연구원의 백본라우터의 트래픽이 급속히 증가함과 동시에 연구망 전체가 마비되는 사고가 발생함
- 과학기술정보보호센터에서는 탐지 및 신고 접수된 현황을 국가사이버안전센터에 통보
- 국가정보원 국가사이버안전센터(NCSC)에서 “경계” 경보 발령을 통해 DDoS 공격에 대한 보안 공조대응 요청

o 피해 현황

- 국내 과학기술 전용 전산망인 초고속연구망의 라우터가 국제사이버테러단체의 DDoS 공격으로 전산망 전체가 약 10시간 동안 마비되어 업무장채 및 인터넷 서비스 장애가 발생함
- 해외 연구소와 협동과제를 수행하고 있는 국내 일부 연구소들의 경제적 손실 및 대외 신뢰도 하락이 우려됨

나. 조치사항 및 절차

(1) 조치 목록

조치사항	세부 내용
위기상황 접수 및 보고/전파	o 주의 단계에서 피해확산 및 사고 신고
초동조치	o「경계」경보 발령 전파 ※ 과학기술부는 경보발령 내용 접수시 과학기술정보보호센터 및 실무기관 등에 신속히 전파
긴급대응조치	o 긴급대응반 증원 운영 o 실무기관은 필요시 자체대응반 운영 o 피해 확산시 경계 단계 조치 수행
피해복구 조치	o 주의 경보단계 조치 수행
처리상황 보고	o 주의 경보단계 조치 수행
후속조치	o 유출 자료에 대한 안보영향평가 실시

주의 경보 조치 지속적 수행

다. 조치 내용

(1) 위기상황 접수 및 보고/전파

(가) 주의 단계에서 피해확산 및 사고 신고

o 실무기관에서 DDoS 공격에 대한 피해가 확산되어 관련 사실을 과학기술정보보호센터에 신고

o 과학기술정보보호센터는 DDoS 공격에 대한 피해확산 사실을 과학기술부에 보고

o 과학기술부는 피해확산 사실을 NCSC에 통보

※ 사고신고 양식은「붙임 3」참조

(2) 초동조치

(가) **경계** 경보 발령 전파

o **경계** 경보 발령의 경우 접수 후, 반장에게 보고하고 과학기술정보보호센터 및 실무기관에 신속히 재전파

- 긴급대응반 상황총괄팀은 사이버 위기경보를 반장에게 보고하고, NCSC의 **경계** 경보 발령사실을 과학기술정보보호센터에 신속히 재전파

△ 전파대상 : 과학기술정보보호센터

△ 전파수단 : SMS, FAX, 전화, 전자우편 및 홈페이지

- 과학기술정보보호센터는 실무기관에 **경계** 경보 발령사실을 신속히 재전파

△ 전파대상 : 실무기관

△ 전파수단 : SMS, FAX, 전화, 전자우편 및 홈페이지

- 실무기관은 위기경보를 접수하고 신속히 기관내 소속원에게 **경계** 경보 발령 사실을 재전파

※ 경보발령 양식 및 상황조치 작성양식은「붙임 1, 2」참조

(3) 긴급대응 조치

(가) 긴급대응반 증원 운영

o 긴급대응반 반장은 증원 및 대비계획 점검

o 과학기술정보보호센터는 긴급대응반 현장파견 인원 증원

o 과학기술부는 실무기관이 NCSC 및 정보시스템 장비·프로그램 제조업체에서 제공한 DDoS 공격 대응요령을 모두 이행하고 있는지 재확인

o 과학기술정보보호센터는 급속한 피해확산이 우려되는 경우 과학기술부에 통보하고 실무기관에 네트워크 연결 차단 권고

(나) 실무기관은 필요시 자체 대응반 운영

o 과학기술부는 피해확산이 예상되거나 피해상황 추이에 따라 시스템 복구 및 피해확산 차단을 위해 실무기관에 자체 대응반 가동을 독려

o 피해가 예상되거나 피해상황 추이에 따라 자체대응반을 투입, 즉각적인 시스템복구를 실시하고 피해확산 차단조치

o 서비스거부공격에 대한 이상 징후를 포착한 경우 정보보안 담당자는 신속하게 라우터, 침입차단시스템 등의 차단 규칙을 재설정하여 공격 진행을 차단

※ 서비스거부공격 이상징후 포착시 공격전개 차단에 대한 자세한 방법은 국가사이버안전매뉴얼 부록 참조(p249)

o 중요 정보자료를 갖고 있는 서버 및 중요한 서버의 자료를 백업하여 네트워크와 단절된 안전한 곳에 보관

o 악성코드, 취약점, 공격도구 등에 대한 분석정보에 따른 공격대상 시스템의 IP 주소 또는 공격대상 서비스 포트번호의 차단 상태를 수시로 확인

o 침입차단시스템, 침입탐지시스템 등을 이용하여 취약점을 재점검하여 발견된 취약점 제거

o 피해발생 가능성이 높은 네트워크를 대상으로 물리적인 케이블 분리 등의 단절시행 여부를 검토하고, 필요할 경우 기관장의 승인하에 단절

(다) 피해 확산시 **심각** 단계 조치 수행

o 피해가 확산되어 NCSC에서 **심각** 단계로 상향조정하는 경우 **심각** 단계 조치 시행(P146 참조)

(4) 피해복구 조치

(가) 주의 경보단계 조치 수행

o 주의 경보단계 조치 수행

(5) 처리상황 보고

(가) 주의 경보단계 조치 수행

o 주의 경보단계 조치 수행

(6) 후속조치

(가) 유출 자료에 대한 안보영향평가 실시

o 대외비 이상의 비밀이 유출된 경우 과학기술부는 해당 비밀 자료의 국가안보상 파급효과 분석을 위해 해당기관 담당자 및 관련 분야 전문가를 소집, 안보영향평가 실시

o 안보에 영향이 있다고 판단된 경우, 피해기관은 해당 비밀에 효력정지 및 취소 등의 조치 수행

4. 심각의 경우 조치사항 및 처리절차

가. 상 황

□ 개 요

o 2007년 11월 12일 국제사이버테러단체의 DDoS 공격으로 판단되어지는 다량의 트래픽이 해외 관문국 라우터를 통해 국내 인터넷 교환노드인 KIX(Korea Internet Exchange), BIX(Busan Internet Exchange)로 유입되면서 해당 백본 라우터가 마비되는 피해가 발생함

□ 세부 내용

o 사고신고 일시 및 내용 : 11월 12일 06:00

- 국내 인터넷 교환노드인 KIX, BIX의 백본 라우터를 공격 목표로 하는 대량의 트래픽이 급속히 증가함에 따라 KT, 데이콤 등 국내 ISP간 인터넷 통신 및 해외로의 인터넷 통신이 마비되는 사고가 발생하여 신고 접수됨
- 국가정보원 국가사이버안전센터(NCSC)에서 “심각” 경보 발령을 통해 DDoS 공격에 대한 국가적 차원의 공동대처 요청

o 피해 현황

- 국내 인터넷 교환노드인 KIX, BIX 전산망 마비로 약 10시간 동안 국내 ISP간 및 해외로의 인터넷 통신이 마비됨
- 국제적 중요 행사시기의 사이버테러사고 발생으로 인하여 국제적 신뢰도 및 국가 이미지 하락이 우려됨
- 국내 ISP를 이용하고 있는 인터넷쇼핑몰 및 인터넷뱅킹 등의 서비스 장애로 막대한 경제적 손실이 우려됨

나. 조치사항 및 절차

(1) 조치 목록

조치사항	세부 내용
위기상황 접수 및 보고/전파	o 경계 단계에서 피해확산 및 사고 신고
초동조치	o「심각」경보 발령 전파 ※ 과학기술부는 경보발령 내용 접수시 과학기술정보보호센터 및 실무기관 등에 신속히 전파
긴급대응조치	o 사고대책본부 구성 운영 o 비상총괄반 구성 운영 o 과기부차원의 합동조사팀 구성 운영 o 과학기술정보보호센터 지원팀, Help-Desk팀 가동 o 실무기관은 자체대응반 가동 o 피해발생 가능성이 높은 네트워크 단절여부 판단
피해복구 조치	o 과기부차원의 복구지원팀 구성 운영
처리상황 보고	o 경보해제 및 하향조정 전파 o 종결보고
후속조치	o 사고재발 방지대책 수립 및 전파

경계 경보 조치 지속적 수행

다. 조치 내용

(1) 위기상황 접수 및 보고/전파

(가) 경계 단계에서 피해확산 및 사고 신고

o 초고속연구망 중심으로 피해가 확산되던 국제사이버테러 단체로부터의 DDoS 공격이 민간 ISP 및 국가공공망으로 확산되면서 국내 전체로 피해확산

o 실무기관에서 국제사이버테러단체로 추정되는 공격근원지로부터의 DDoS 공격에 대한 피해가 확산되어 관련 사실을 과학기술정보보호센터에 신고

o 과학기술정보보호센터는 DDoS 공격에 대한 피해확산 사실을 과학기술부에 보고

o 과학기술부는 피해확산 사실을 NCSC에 통보

※ 사고신고 양식은「붙임 3」참조

(2) 초동조치

(가) **심각** 경보 발령 전파

o **심각** 경보 발령의 경우 접수 후, 반장에게 보고하고 과학기술정보보호센터 및 실무기관에 신속히 재전파

- 긴급대응반 상황총괄팀은 사이버 위기경보를 반장에게 보고하고, NCSC의 **심각** 경보 발령사실을 과학기술정보보호센터에 신속히 재전파

△ 전파대상 : 과학기술정보보호센터

△ 전파수단 : SMS, FAX, 전화, 전자우편 및 홈페이지

- 과학기술정보보호센터는 실무기관에 **심각** 경보 발령 사실을 신속히 재전파

△ 전파대상 : 실무기관

△ 전파수단 : SMS, FAX, 전화, 전자우편 및 홈페이지

- 실무기관은 위기경보를 접수하고 신속히 기관내 소속원에게 **심각** 경보 발령 사실을 재전파

※ 경보발령 양식 및 상황조치 작성양식은「붙임 1, 2」참조

(3) 긴급대응 조치

(가) 사고대책본부 구성 운영

o 정책홍보실장을 본부장으로 하는 사고대책본부를 구성하여 즉각 대응태세 돌입

- 관제인력 증원 및 탐지룰 적용 등 보안관제 강화

- 각 분야·부문별 관제센터와 수시 연락 및 동향파악 강화

※ 사고대책본부 구성, 역할, 세부임무는 (P42~43) 참조

(나) 비상총괄반 구성

o 비상계획 담당관을 반장으로 하는 비상총괄반 구성 운영

o 비상사태 및 위기관리에 관한 계획 수립 및 점검

(다) 과학기술부 차원의 합동조사팀 구성 운영

o 피해범위 및 복구시간 등에 따라 다수의 반으로 구성

o 피해현황 파악 및 사고조사

- 합동조사팀은 피해규모를 파악하고 현장·원격조사 계획 수립 및 이행

- 웜에 감영된 시각, 침입차단시스템 로그에 기록된 자료 유출량 및 기간, 피해 PC내 저장된 문서 등을 종합 분석

※ 합동조사팀 임무, 구성, 운영방법은 (P68) 참조

(라) 과학기술정보보호센터 지원팀 및 Help-Desk팀 가동

- 과학기술부 사고대책본부를 지원하기 위한 지원팀, Help-Desk팀을 가동하고 즉각 대응태세 돌입
- 과학기술부 합동조사팀 현장지원(조사 주관)

(마) 실무기관은 자체 대응반 가동

o 실무기관은 자체대응반을 가동하고 즉각 대응 태세 돌입

o 악성코드, 취약점, 공격도구 등에 대한 분석정보가 발표될 경우, 라우터·스위치 및 침입차단시스템의 차단규칙을 추가 설정하여 공격대상 서비스 포트를 차단

※ 공격대상 서비스 포트 차단에 대한 자세한 방법은 국가사이버안전매뉴얼 부록 참조(p249)

o 기관 내 PC사용을 최소화하여 만약에 발생할 수 있는 잠재적인 사고를 미연에 방지

o 서비스거부공격 및 웜 발생을 확실하게 예상할 수 있거나 내부 시스템 및 네트워크에 대규모 피해 확산을 예상할 수 있는 경우, 기관장의 승인을 받고 물리적인 케이블 분리 등을 통해 피해 대상 네트워크를 단절

o 피해를 당한 해당 기관의 정보보안담당자는 사고와 관련된 데이터뿐만 아니라 데이터백업 및 로그관리 등 사고조사에 필요한 자료를 제공

(바) 과학기술정보보호센터는 급속한 피해확산이 우려되는 경우 과학기술부에 통보하고 실무기관에 네트워크 연결 차단 권고

(4) 피해복구 조치

(가) 과학기술부 차원의 복구지원팀 구성 운영

o 피해상황의 파악 및 복구 절차 수립·시행

o 심각한 피해의 경우 범정부 복구지원팀과 연계하여 복구 활동 지원

o 피해복구 및 사후 처리 결과 종합 보고

※ 복구지원팀 임무·구성·운영 방법은 (P69) 참조

o 경미한 사고는 피해 기관이 자체 복구

※ 조치 상황을 과학기술부 및 과학기술정보보호센터에 통보

o 중대한 사고는 과학기술부 복구지원팀 지원 하에 복구

o 심각한 사고는 범정부「복구지원팀」에 의해 복구

(5) 처리상황 보고

(가) 경계 경보단계 조치 수행

o 경계 경보단계 조치 수행

(나) 경보해제 및 하향 조정

o NCSC에서 경보 해제 또는 하향 조정이 전파된 경우 반장에게 보고하고 경보 해제 또는 하향 조정전파

※ 전파절차 및 전파수단·대상은 발령의 경우와 동일

(다) 종결보고

o 경보 해제 또는 하향 조정의 경우 종결보고 실시

o 보고체계 : 사고대책본부장 → 과학기술부 장관

o 보 고 자 : 사고대책본부장(정책홍보관리실장)

o 보고방법 : 내부보고 양식에 따라 종결보고

※ 합동조사팀 및 복구지원팀 운영결과 반영

o 보고 종료 후 상황해제 및 사고대책본부 해체

(6) 후속조치

(가) 사고재발 방지대책 수립 및 전파

o 기밀자료 유출 사고발생 기관에 대한 전산망 보안강화 대책, 유포된 기밀자료에 대한 효력정지 방안을 마련

o 예산 인력이 수반되는 국가차원의 대책에 대해서는 유관기관(국가정보원, 기획예산처, 행정자치부)에 지원 요청

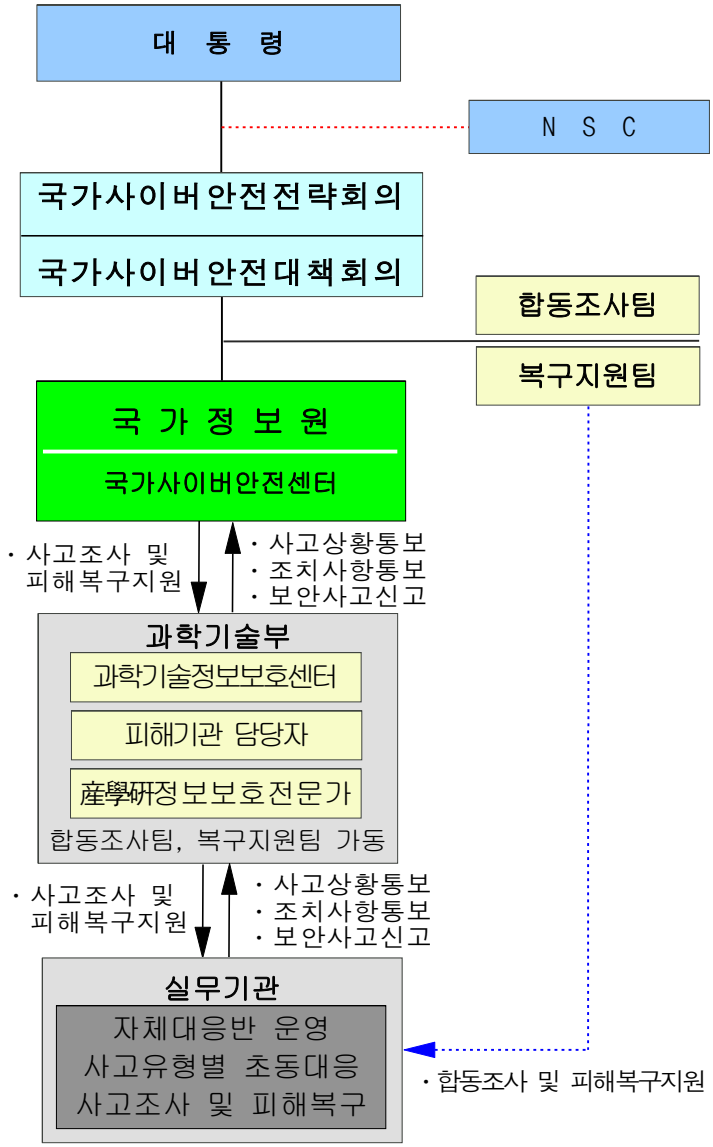
부 록

Ⅰ. 사고조사 및 복구

1. 사고조사 및 피해복구 체계

가. 업무체계도

(1) 사이버공격으로 인해 발생한 정보통신망 보안사고 또는 사이버 침해사고에 대해 공격기법과 사고원인을 분석하는 일체의 행위를 지칭하며, 피해확산 차단 및 유사사고재발 방지를 위한 보안대책을 수립하고자 함



나. 사고조사 및 복구 절차

(1) 사이버위협 경보가 **심각** 수준으로 발령된 경우에는 범정부적으로 구성된 합동조사팀·복구지원팀과 연계하여 사고조사 및 피해복구를 수행하며, 해당 기관의 장은 이에 필요한 인력 및 관련 자료를 지원

(2) 자체적으로 사고원인 규명, 공격자 추적, 공격 증거확보 등의 조사를 실시하거나 피해를 복구 할 때에는 다음과 같은 절차에 따라 실시하며, 사고 조치결과를 작성·유지

(3) 사고조사 결과, 범죄 혐의가 있다고 판단되는 경우 실무기관은 과학기술정보보호센터에 통보하고 과학기술정보보호센터는 과학기술부에 통보, 과학기술부 장관은 국각정보원장에게 통보

1단계	
사고신고 사고대응	○ 사고신고 및 초동대응 ※ 사고신고 양식은「붙임 3」참조

2단계	
증거확보 및 보존	○ 증거자료 백업 ※ 부록 Ⅰ.「2.마. 증거확보 및 보존요령(p162)」참조

3단계	
사고조사	○ 공격유형별 사고조사 ○ 사고원인 규명 및 공격근원지 추적 ※ 필요시 과학기술부 합동조사팀 연계 조사 ○ 범죄여부 판단(실무기관→과학기술정보보호센터→과기부) ※ 필요시 과학기술부장관이 국가정보원장에 수사요청

4단계	
피해복구	○ 피해복구 ※ 부록 Ⅰ.「2.사. 피해복구 절차(p166)」참조 ※ 필요시 과학기술부 복구지원팀 연계 복구

5단계	
보고서작성	○ 사고 조치결과 통보 ※ 사고 대응조치 결과통보 양식은「붙임 4」참조
	○ 사고처리결과보고서 작성 ※ 사고처리결과보고서는 초동조치, 증거확보, 사고조사, 피해복구 결과 과학기술부 합동조사팀 및 복구지원팀 연계 조사 내용을 기술

2. 사고조사 및 복구 요령

가. 사고 신고

(1) 사고발생에 따른 신고

(가) 정보보안사고

o 보안사고가 발생한 실무기관의 장 또는 사고를 범하였거나 이를 인지한 자는 지체없이 사고의 일시·장소·사고내용 및 현재 취하고 있는 조치를 과학기술정보보호센터에 통보

o 실무기관의 장은 국가정보보안기본지침에 나열된 정보보안사고가 발생한 때에는 즉시 피해를 최소화하도록 조치를 취하고 과학기술정보보호센터 통보

o 과학기술정보보호센터는 실무기관의 보안사고 사실을 과학기술부에 통보

o 과학기술부는 보안사고 사실을 국가정보원에 통보

(나) 사이버 침해사고 및 공격징후 발견

o 과학기술부 장관은 국가정보통신망에 대한 사이버공격의 계획 또는 공격사실, 사이버안전에 위협을 초래할 수 있는 정보를 입수한 경우에는 지체 없이 그 사실을 국가정보원장에게 통보

o 과학기술부 장관은 사이버공격으로 인한 사고의 발생 또는 징후를 발견한 경우에는 피해를 최소화하는 조치를 취하고 지체없이 그 사실을 국가정보원장에게 통보

o 실무기관의 장은 사이버공격으로 인한 사고의 발생 또는 징후를 발견한 경우에는 피해를 최소화하는 조치를 취한 후 그 사실을 과학기술정보보호센터에 통보해야 하고, 과학기술정보보호센터는 과학기술부에 통보하고, 과학기술부 장관은 이를 지체 없이 국가정보원장에게 통보

나. 사고조사의 실시

(1) 정보보안사고 전말조사

(가) 보안사고 전말조사는 실무기관의 업무용 PC에 불법 침입이 발생하여 대외비이상의 비밀자료가 유출된 경우에도 해당

(나) 보안사고는 이에 대한 전말조사가 종결될 때까지 공개하여서는 안됨

(다) 경비한 사고의 경우에는 실무기관의 장에게 사고조사를 위임할 수 있음

(2) 사이버 침해사고 조사

(가) 경미한 사고라고 판단되는 경우에는 실무기관의 장이 자체적으로 조사하게 할 수 있음

(나) 실무기관에 대한 사이버공격이 특히 다음 각 호에 해당되는 경우 보안사고에 준하여 사고조사를 실시

o 대외비 이상의 비밀자료를 입력, 출력, 열람에 활용되거나 과거에 활용된 이력이 있는 업무용 PC에 저장된 자료유출을 목적으로 하는 사이버공격

o 대외비 이상의 비밀자료를 입력, 출력, 열람하는 업무를 현재 수행 또는 과거에 수행했던 공무원 또는 임직원의 업무용 PC에 저장된 자료유출을 목적으로 하는 사이버공격

(다) 국가정보원장은 사이버공격으로 인한 사고의 발생 또는 징후를 발견한 경우 과학기술부 장관에게 사고복구 및 피해의 확산방지에 필요한 조치를 요청할 수 있음

(라) 실무기관의 장은 국가정보원장이 사고 조사시 원인분석을 위하여 정보통신망의 접속기록 등 관련 자료의 제공 및 피해시스템에 잔존한 해킹프로그램의 채증 등 증거확보를 요청할 경우 적극협조(구두설명 또는 전자우편으로 갈음 할 수 있음)

(마) 과학기술부 장관은 특별한 사유가 없는 한 이에 협조하여야 한다. 특별한 사유라 함은 현행법령에 의하여 금지되어 있거나 정보제공 절차가 서명에 의해야 한다고 규정된 경우

(바) 사고조사에 대한 실무 지원은 정보보안 책임자 및 실무자가 수행하는 것을 원칙으로 함

(3) 실무기관의 자체 사고조사

(가) 실무기관의 장은 경보가 발령되었을 때에 경보발령과 관련된 사고 대응을 위해 자체대응반을 편성 운영

(나) 실무기관의 자체대응반장은 정보보안책임자가 겸임하는 것을 원칙으로 하며, 자체대응반원은 정보보안 실무자를 중심으로 편성

(다) 실무기관의 자체대응반장은 사이버공격으로 인한 사고의 발생 또는 징후 발견시 피해 최소화 조치를 취해야 함

(라) 경미한 사고라고 판단되는 경우에는 실무기관의 장이 자체적으로 조사하게 할 수 있음

(마) 실무기관의 장이 자체적으로 사고조사를 실시한 경우에는 사고조사를 완료한 후 사고조치 서식에 의거하여 사고조치결과 보고서를 작성 유지하고, 사본 1부를 과학기술정보보호센터에 통보, 과학기술정보보호센터는 과학기술부에 통보, 과학기술부는 국가정보원에 통보

다. 합동조사팀 및 복구지원팀 지원요청

(1) 사이버공격으로 대규모 피해가 발생한 경우 과학기술부가 범정부 합동조사팀 및 복구지원팀에 지원요청

라. 사고조사 결과

(1) 조사결과 처리

(가) 국가정보원장은 보안업무규정에 의한 전말조사를 실시한 경우 그 결과를 실무기관의 장에게 통보

(나) 실무기관의 장은 조사결과에 대하여 필요한 조치를 취하고, 사고 관련자에 대해서는 관계법규에 의거 징계토록 하며 처리 결과에 대해서는 국가정보원장에게 통보

(2) 안보영향평가

(가) 실무기관장은 보안사고의 전말조사 결과에 의하여 비밀의 효력 정지 또는 취소 등의 필요한 조치를 취함(보안업무규정시행규칙 제63조)

마. 증거확보 및 보존요령

1단계

증거자료 백업	○ 피해 장비(컴퓨터)의 백업파일 생성 - 로그자료 - 프로세스 정보 - 네트워크 연결상태 - 파일 시스템 정보 ※ 주의사항 : 피해 장비의 전원차단 실시 등 운영 장비 정지로 사고원인의 증거 발견이 불가능해지지 않도록 주의

2단계

컴퓨터 하드웨어 파악	윈도우 시스템	○ 내 컴퓨터 등록정보를 이용, 하드웨어 정보파악
	유닉스 시스템 리눅스 시스템	○ dmesg 명령어 이용, 하드웨어 정보 파악

3단계

해당 소프트웨어 파악	윈도우 시스템	○ 제어판의 프로그램 추가/삭제 기능을 통해 시스템에 설치된 프로그램 현황을 파악 ※ 주의사항 : 레지스트리(Registry)정보를 통해 세부 사항도 확인
	유닉스 시스템 리눅스 시스템	○ 운영체제에 맞는 명령어를 사용하여 파악 - Linux : RPM(RedHat Package Manager) 명령 실행 - Solaris(SUN O/S) : pkgadd, pkgrm, pkginfo 명령 실행 - HP-UX : swinstall 명령 실행 - SCO OpenServer : pkgadd, pkgrm, custom 명령 사용 - FreeBSD : pkg_add, pkg_delete, pkg_info 명령 사용

4단계

파일목록 작성 및 조사	윈도우 시스템	○ 모든 파일의 검색 - 검색옵션을 모든 파일을 볼수 있도록 선택하고 탐색기를 사용하여 전체 파일 현황을 파악 ○ 특정 파일의 검색 - 검색옵션을 특정 파일을 볼수 있도록 선택하고 탐색기 이용, 특정 파일 현황을 파악
	유닉스 시스템 리눅스 시스템	○ 모든 파일의 검색 -「ls」명령어를 사용하고「-a」또는「-al」옵션을 사용하여 전체 파일의 목록을 확인 ○ 특정 파일의 검색 -「find」명령어를 사용하여 특정파일의 위치를 확인

5단계

증거자료 추출	○ 증거자료 백업매체 - 원본과 동일한 형태, 동일 모델로 저장 보관 ○ 증거자료 추출분석 - 원본 같은 이미지 복사본을 사용 - 하드웨어적 이미지 복사 : Encase등과 같은 하드디스크 복사기로 복사(고가의 정밀수사에 사용) - 소프트웨어적 복사 : 「고스트」 프로그램 사용 ○ 증거자료 분석환경 - 컴퓨터 범죄가 일어난 환경과 동일하게 준비(예를 들어, 동일환경의 하드웨어 준비 등)

6단계

증거자료 분석·확보	○ 일반적 문서파일 - 특정 키워드가 포함된 문서 검사 ○ 회계 파일 - 사용한 회계용 프로그램 파일 분석 ○ 데이터베이스 파일 - 원본 데이터베이스 무결성 검사 - 데이터베이스 구조, 테이블 구성 조사

바. 사이버공격 유형별 사고조사 요령

(1) 악성코드공격 사고조사 요령

(가) 악성코드 사본 수집 및 보존

o 악성코드 분석 및 추후 사고조사를 위해 악성코드 사본을 수집하여 보존

o 수집된 악성코드를 과학기술정보보호센터에 통보, 과학기술정보보호센터는 과학기술부에 통보, 과학기술부는 국가사이버안전센터에 통보

(나) 사고 처리 내역을 기록 유지

o 사후 법적 증거로 활용하거나 상황보고 및 사고 처리 활동에 대한 사후 검토를 위해 악성코드로 인한 사고 발생시 대응요령 수행 내역에 대한 기록을 유지

(2) 서비스거부공격 사고조사 요령

(가) 트래픽 분석을 통한 공격자 추적

o 스니퍼와 같은 트래픽 분석 도구를 이용하여 감시되는 트래픽으로부터 공격 근원지를 식별

o 라우터의 트래픽 분석기능과 스위치의 MAC 주소 테이블을 이용하여 서비스거부공격의 공격자를 추적

※ 네트워크 장비를 이용한 서비스거부공격 추적 및 차단에 대한 자세한 정보는 국가사이버안전매뉴얼 부록5.「5.2」참조

o 정보통신 서비스 제공자(ISP)에게 공격자 추적 요청

o 서비스거부공격이 호스트를 손상시킨 방법을 파악

o 시스템 및 네트워크의 대량 로그 엔트리를 분석

o 피해시스템과 동일 IP대역을 사용하고 있는 컴퓨터의 로그를 조사

(나) 후속 공격에 대한 대비책 강구

o MRTG(Multi Router Traffic Grapher)와 같은 네트워크 트래픽 모니터링 도구를 이용하여 복구활동이 시작되기 전까지 꾸준한 네트워크 모니터링

o 네트워크 모니터링으로 후속 공격 발생시, 서비스거부 공격 발생 대응요령을 이용하여 공격자를 추적하고 추가적인 증거를 확보

(3) 비인가접근공격 사고조사 요령

(가) 관련 로그 및 증거 자료 확보

o 침입탐지시스템, 침입차단시스템, 피해시스템의 로그 등과 같은 사고 관련 로그 및 증거 자료 확보

o 침입사실을 확인하기 위하여 lsof(유닉스용) 또는 fport (윈도우즈용)와 같은 도구를 이용하여 열려진 포트와 매칭하는 프로세스를 찾아냄

(나) 물리적 상황 증거 확보

o 사고기간 중 전산실, 사무실 등의 출입통제시스템의 로그를 확보

(4) 복합구성공격 사고조사 요령

(가) 개별적 공격에 대한 사고조사 수행

o 복합구성공격에 의하여 사고가 발생한 경우 일어난 사고 각각에 대해 사고조사를 수행

사. 피해복구 절차

1단계

피해복구 범위결정	단순 데이터복구	○ 피해사고가 발생한 시스템의 데이터만 손상이 발생
	소프트웨어복구	○ 피해사고가 발생한 시스템의 프로그램 및 운영체에 단순 오류 발생
	시스템 재설치	○ 피해사고가 발생한 시스템의 운영체제에 복구 불가능한 심각한 오류 발생
	하드웨어 교체	○ 피해사고가 발생한 시스템의 하드웨어 손실 발생

2단계

피해복구 우선순위 결정	○ 피해복구 대상 시스템이 두 개 이상인 경우, 이들 대상에 대한 복구 우선 순위화
	○ 즉시 조치해야 할 복구 내용과 중장기적인 계획에 의해서 수행해야 할 복구 내용 결정

3단계

피해복구	단순 데이터복구	○ 피해사고 발생 전에 백업하였던 데이터로 복구 ○ 백신 프로그램을 이용한 악성코드 탐지 및 치료
	소프트웨어복구	○ 소프트웨어 패치를 이용한 공격에 이용된 취약점 제거 ○ 응용프로그램 재설치 ○ 운영체제 CD를 이용한 운영체제 복구
	시스템 재설치	○ 운영체제 CD를 이용한 운영체제 재설치 ○ 필요한 운영프로그램 설치 ○ 먼저 백업한 자료를 이용한 데이터 복원 ○ 시스템을 완료 후 정상상태 복귀 확인
	하드웨어 교체	○ 파손된 하드웨어 부품 교체

4단계

사후관리	○ 시스템 재개 후 일정기간 동안 모니터링 강화 ○ 피해복구에 관한 보완 보고서 작성 및 일정기간동안 시스템 및 네트워크의 주기적인 재점검 ○ 사건처리에 대한 회의 개최 ○ 책임부과 여부 검토

Ⅱ. 사이버공격 유형별 대응

1. 사이버공격 유형

가. 개요

실무기관의 정보보안 책임자(실무자)가 사이버공격 징후 인지 또는 사이버공격으로 인한 사고 발생시 이를 효율적으로 처리할 수 있도록 사이버공격 유형을 악성코드공격, 서비스거부공격, 비인가접근공격, 복합구성공격 4가지로 분류

최근의 사이버공격의 특징을 요약하면 다음과 같음

(1) 사이버공격의 지능화, 다양화, 복합화 및 자동화

(2) 파일공유, 메일, P2P 등을 통해 다른 시스템으로 매우 빠른 전파

(3) 사회공학적인 기법과 다양한 기술적 방법이 결합된 사이버공격 도구 출현

(4) 침입차단시스템, 침입탐지시스템 등의 정보보호시스템을 우회하거나 무력화하는 공격 출현

(5) 보안취약점이 공개되면 당일 이를 이용하는 공격도구 출현 (Zero-Day Attack)

(6) 역연결(Reverse Connection)을 이용하여 원격제어 하는 악성코드 출현

(7) 금전적 이득을 위한 개인정보를 유출하는 공격 출현

나. 사이버공격 유형 분류

(1) 악성코드공격

악성코드공격이란 컴퓨터바이러스, 웜, 트로이목마, 백도어, 봇(BOT), 스파이웨어 등이 사용자의 동의 없이 컴퓨터에 설치되어 사용자의 정보를 탈취하거나 컴퓨터를 오작동 시키고 네트워크를 마비시킬 수 있는 악의적인 행위

(2) 서비스거부공격

서비스거부공격(Denial of Service)은 시스템에 과도한 부하를 유발하여 정상적인 서비스를 차단하거나 성능을 저하시키는 행위. 서비스거부공격은 TCP 프로토콜을 이용하여 요청메시지에 대한 응답메시지를 보내지 않음으로써 피해 시스템의 TCP 세션을 불완전한 상태로 연결하여 수용능력을 포화시켜 피해 시스템의 서비스를 불가능하게 만든다. 공격자는 소스 IP정보를 위조하거나 봇과 같은 악성코드에 감염된 시스템을 이용함으로써 자신의 위치를 노출시키지 않음

(3) 비인가접근공격

비인가접근공격은 네트워크, 시스템, 응용프로그램, 데이터 또는 기타 자원 등에 인가를 받지 않은 자가 논리적 또는 물리적으로 불법 접근하는 공격유형을 의미
공격자는 자신이 직접 해킹을 시도할 수도 있고, 악성프로그램을 이용하여 사용자의 중요정보를 자동으로 수집한 후 정상적인 방법으로 해킹을 시도할 수도 있음

(4) 복합구성공격

복합구성공격은 악성코드공격, 서비스거부공격, 비인가접근공격 등의 요소를 복합적으로 이용하는 공격유형을 의미함. 봇 계열의 악성코드가 서비스거부 공격을 수행하거나 비인가 접근을 위한 피싱 등의 경우가 이에 해당

2. 사이버공격 유형별 탐지

가. 악성코드공격 탐지·분석

(1) 악성코드공격 예상 징후[1)]

악성코드공격 예상 징후
○ 새로운 취약점의 출현 - 과학기술정보보호센터 및 과학기술부 등 사이버안전 유관기관 웹 사이트 및 각종 보안정보 웹 사이트를 통해 확인 - 취약점이 발표되면 단기간에 해당 취약점을 공격하는 공격도구 또는 악성코드가 배포되므로 즉시 보안패치를 수행 ※ 악성코드 : 웜 ·바이러스, IRC 봇, 트로이목마, 백도어, 스파이웨어 등 ○ 새로운 악성코드의 출현 - 국가사이버안전센터 웹 사이트 및 각종 보안정보 웹 사이트를 통해 확인 ○ 백신 프로그램의 감염 파일 탐지 ○ 특정 서비스 포트로의 비정상적인 접속 시도 증가 ○ 침입탐지시스템, 침입차단시스템, 네트워크 장비, 시스템 로그 등을 통해 확인 ※ 비정상적인 접속 시도 포트의 예 : 1434/udp (Slammer 웜), 135/tcp (Welchia 웜) 등

악성코드공격의 징후를 발견하였을 경우에는 다음과 같이 사고 발생을 감시하고 초동조치를 수행

(가) 새로운 악성코드 및 취약점에 대한 정보 수집 및 관련 보안패치

(나) 비정상 접속이 시도되고 있는 시스템에 대한 지속적인 감시

1) 징후란 사이버공격이 일어날 조짐을 의미한다.

(2) 악성코드공격의 피해증상

악성코드공격 피해증상

○ 백신 소프트웨어의 악성코드 발견 경고 발생
○ 파일 또는 프로그램의 삭제 및 손상
  - 문서 열람 또는 프로그램 실행시 오류 발생
  - 보안관련 프로그램 실행시 자동 종료
○ 특정 프로세스의 비정상적인 작동
  - 해당 프로세스의 CPU 사용량 증가
  - 피해시스템의 네트워크 사용량 폭증
  - 출처가 불분명한 원격시스템과 피해시스템간의 네트워크 연결 탐지
○ 의도하지 않은 화면 출력
  - 화면에 이상한 메시지나 그림 출현
  - 인터넷 사용시 의도하지 않은 웹 사이트로 연결
○ 침입탐지시스템, 침입차단시스템 등 정보보호시스템에서 악성코드 침입시도 관련 내용 탐지

위와 같은 악성코드공격에 의한 증상을 발견하였을 경우에는 사고 발생여부를 판별하고, 부록 Ⅱ. [3.가. 악성코드공격 대응요령(P176)]을 참조하여 사고에 대응하며, 필요시 과학기술정보보호센터 등 사이버안전 전문기구에 도움 요청

나. 서비스거부공격 탐지·분석

(1) 서비스거부공격 예상 징후

서비스거부공격 예상 징후

○ 인터넷상에 새로운 서비스거부공격 도구 공개
- 국가사이버안전센터 웹 사이트 및 각종 보안정보 웹 사이트를 통해 확인

※ 서비스거부공격 도구의 예 : TFN, Trinoo, Stacheldraht, TFN2Kt 등

○ 기관내 특정 서버의 비정상적인 서비스 중단
- 서비스거부공격의 대상은 대부분 서버급 장비이며 이러한 서버에서 비정상적으로 서비스가 중단되는 경우에는 서비스거부공격으로 의심

○ 침입탐지시스템, 침입차단시스템 등 정보보호시스템에서 스캐닝 활동 탐지
- 서비스거부공격과 관련된 스트링이 포함된 트래픽 발견 (에이전트 검색 메시지, 공격 시작 메시지등)

○ 서비스거부공격을 위해 대기하고 있는 프로그램 발견
- 프로세스 확인 유틸리티, 열린 포트 확인 유틸리티, 악성프로그램 탐지 소프트웨어 등을 통해 확인

※ 서비스거부공격 에이전트 사용 포트의 예 : 27444/udp(Trinoo), 18753/udp(Shaft), 9325/udp(Mstream), 6838/udp(Mstream 변종)

서비스거부공격 예상 징후를 발견하였을 경우에는 다음과 같이 사고발생을 감시하고 초동조치 수행

(가) 서비스거부공격 도구에 대한 정보 수집 및 관련 보안 패치

(나) 스캐닝 등이 이루어지고 있는 대상 시스템에 대한 지속적인 감시

(다) 서비스거부공격을 위한 에이전트 탐색 및 제거

(2) 서비스거부공격 피해증상

서비스거부공격 피해증상

○ 침입탐지시스템, 침입차단시스템 등 정보보호시스템에서 서비스거부공격 침입시도 관련 내용 탐지
○ 백신 소프트웨어에 의한 서비스거부공격도구 발견
○ 기관내 특정 서버의 서비스 중단
  - 서비스거부공격 발생시 과도한 트래픽 집중으로 인하여 소프트웨어/하드웨어 오류가 발생되어 서비스가 중단
○ 네트워크 속도 저하
  - 피해시스템의 네트워크 사용량 폭증으로 인한 네트워크 속도 저하
  - 출처가 불분명한 다수의 원격시스템과 피해시스템간의 네트워크 연결 탐지
○ 네트워크 트래픽의 이상패턴 발견
  - 패킷의 발신/수신 IP 주소가 없거나 존재하지 않는 IP 주소로 변조
  - 일정한 패턴의 발신/수신 IP 주소를 갖는 일련의 트래픽 발견
  - 비대칭형 네트워크 트래픽 패턴 다수 발생

위와 같은 서비스거부공격 피해증상을 발견하였을 경우에는 사고 발생 여부를 판별하고, 부록 Ⅱ. [3.나. 서비스거부공격 대응요령(p179)]을 참조하여 사고에 대응하며, 필요시 과학기술정보보호센터 등 사이버안전 전문기구에 도움 요청

다. 비인가접근공격 탐지·분석

(1) 비인가접근공격 예상 징후

비인가접근공격 예상 징후

○ 인터넷상에 새로운 서비스거부공격 도구 공개
- 국가사이버안전센터 웹 사이트 및 각종 보안정보 웹 사이트를 통해 확인

○ 침입탐지시스템의 관련 경고 또는 로그 발견
- telnet등 특정 서비스에 대한 지속적인 접속 시도 발견
- '/bin/sh'과 같은 공격내용을 포함한 스트링을 포함한 트래픽 발견
- 연속적인 인증 실패 로그 발견

○ 사회공학적 기법을 이용한 공격 시도 탐지
- 관리자나 타 사용자를 사칭하여 민감한 정보, 시스템설정 변경, 특정 프로그램 수행 요구
- 다량의 피싱 메일 수신

○ 비정상적인 스캐닝 흔적 발견
- 웜, 바이러스 및 서비스거부공격을 위한 스캐닝 이외의 패턴 발견
- 업무용 애플리케이션 서비스 포트에 대한 스캐닝 발견

○ 자료 유출 징후와 관련된 로그 발견
- 특정 자료 열람 횟수의 비정상적 증가
- 업무와 관계없는 사용자에 의한 자료 열람 로그 발견

○ 비정상적인 업무 처리 흐름 발견
- 일반적인 업무 흐름 패턴과 다른 업무 처리 내용 발견
- 업무 처리 데이터의 불일치 발견

○ 물리적인 비인가접근 시도를 포착
- 잠겨진 배전함 및 배선함을 열려는 시도
- 정체불명의 사람에 의한 말소된 신분증 및 인증카드 사용 시도

비인가접근에 의한 공격의 징후를 발견하였을 경우에는 다음과 같이 사고발생을 감시하고 초동조치 수행

(가) 새로운 비인가접근관련 취약점에 대한 정보 수집 및 관련 보안패치

(나) 비인가접근이 시도되고 있는 시스템에 대한 지속적인 감시

(다) 비정상적인 업무 흐름에 대한 감시 및 물리적 인가조치에 대한 검토

(2) 비인가접근공격 피해증상

비인가접근공격 피해증상

○ 침입탐지시스템, 침입차단시스템 등 정보보호시스템에서 비인가접근에 의한 침입 시도 관련 내용 탐지
○ 비정상적인 사용자계정 발견
- 동시에 다양한 원격지로부터 접속중인 사용자계정 발견
- 관리자 수준의 새로운 사용자 또는 그룹 계정 발견
○ 비정상으로 동작하는 프로그램 발견
- 레지스트리 혹은 시작 파일 목록 등에서 정체불명의 프로그램 리스트 발견
- 비정상적으로 실행중인 프로세스 발견
○ 데이터 위·변조 및 삭제 흔적 발견
- 중요자료의 위·변조 및 삭제 흔적 발견
- 문서, 프로그램등의 권한설정 및 시각 변경
- 시스템 중요설정파일의 변경사항 발견
- 시스템 부하, 네트워크 사용량, 로그 기록량, 파일시스템 사용량 등 시스템 운용상의 심각한 변화 발생
○ 해킹 공격의 경유지 이용 탐지
- 타 기관으로부터 공격 경유지 등으로 이용되고 있다는 사실을 통지
- 특정 호스트에 대한 경유지 이용으로 유추할 수 있는 네트워크 트래픽 탐지
※ 사용자가 중요정보를 입력하도록 유도하는 메일 다수 발견 (피싱)

위와 같은 비인가접근에 의한 공격의 증상을 발견하였을 경우에는 사고 발생 여부를 판별하고, 부록 Ⅱ. [3.다. 비인가접근공격 대응요령(p180)]을 참조하여 사고에 대응하며, 필요시 과학기술정보보호센터 등 사이버안전 전문기구에 도움 요청

라. 복합구성공격 탐지·분석

(1) 복합구성공격의 예상 징후

개별 공격에 대한 예상 징후를 분석하여 두 가지 이상의 징후를 나타내는 경우 복합구성공격의 예상 징후로 판단할 수 있으며, 각 유형별 사고발생 감시 및 초동조치를 시행

(2) 복합구성공격의 피해증상

복합구성공격의 증상은 두 가지 이상의 사고가 발생하였거나 현재 발생하고 있는 상태에 대한 정보를 의미한다. 따라서 상기 주요 공격기법 탐지·분석요령을 바탕으로 개별 사고 증상을 분석하여 두 가지 이상의 증상이 발견된 경우 부록 Ⅱ. [3. 사이버공격 대응요령(p176)]의 내용을 참고하여 사고에 대응하고 필요시 과학기술정보보호센터 등 사이버안전 전문기구에 도움 요청

사이버공격으로 인한 사고 발생시 해당 공격을 긴급히 차단하고 피해를 최소화시키기 위한 주요 공격 유형별 대응요령은 다음과 같음

3. 사이버공격 대응요령

가. 악성코드공격 대응요령

(1) 악성코드공격 판단

(가) 웜・바이러스 계열의 악성코드는 메일, 공유폴더 또는 취약점스캐닝을 통해서 은밀하고 빠르게 전파되므로 백신프로그램, 침입탐지시스템, 침입차단시스템 등 정보보호시스템과 네트워크 장비의 로그자료 등을 주시

(나) 트로이목마나 봇 계열의 악성코드는 외부에서 접근이 가능하도록 특정포트를 오픈하고 있거나, 주기적으로 특정 사이트 또는 특정 시스템으로 접속을 시도하므로 시스템들의 네트워크 설정 및 구성 상태를 확인

(2) 감염시스템 분리

(가) 감염된 호스트를 식별 후 네트워크에서 분리하여 악성코드를 분석

(나) 백신프로그램의 경고 메시지를 참고하여 악성코드를 식별할 수 있지만 백신 프로그램이 모든 악성코드 감염을 탐지하지는 못하므로 다음과 같이 사고내용을 조사. 감염된 호스트가 식별이 되면 해당 호스트를 네트워크에서 분리한 후 아래의 악성코드 분석과정을 수행

- o 알려진 트로이목마 및 백도어 포트를 통한 연결을 탐지하기 위해 감염이 의심되는 호스트에 대해 포트 스캐닝을 수행
- o 백신업체에서 긴급히 제공하는 특별한 탐지 및 치료 도구를 사용

o 개별 호스트의 로그 기록뿐만 아니라, 악성코드 유입 경로에 있는 이메일 서버, 침입차단시스템, 프락시 서버 등의 로그 기록을 검토

o 악성코드 사고와 관련된 행위를 식별할 수 있도록 침입탐지시스템을 재설정

o 수행되고 있는 프로세스들이 정상적으로 동작하고 있는지 확인하기 위해 무결성 검사 및 감사 자료를 검토

(3) 감염경로 차단

(가) 악성코드 유입 경로를 차단

o 피해확산 방지를 위해 이메일 서버 및 클라이언트 프로그램은 특정 제목, 발신인 주소, 첨부물 명칭, 악성코드 속성 등을 기준으로 차단규칙을 추가 설정

o 수백 대 이상의 시스템이 악성코드에 감염되고 이메일 등의 전파수단을 통한 접근 시도로 인하여 전파 매개 서버 시스템이 서비스를 제공할 수 없게 될 경우, 이메일 서버 등 전파 매개 서버 시스템을 폐쇄

o 악성코드가 특정 서비스의 취약점을 이용하여 내부 네트워크로 유입될 경우, 침입차단시스템, 스위치 또는 라우터의 차단규칙 설정을 통한 내부 네트워크의 유입을 차단

(나) 외부로의 연결시도를 차단

o 특정 IRC 서버 또는 백도어 마스터 시스템으로 접속을 시도하고 있는지 여부를 확인하기 위해 시스템에서 주기적으로 외부로 나가는 패킷이 있는지 여부를 확인

o 내부 피해 시스템의 악성코드가 외부 시스템으로 연결을 시도하는 경우 라우터나 침입차단시스템의 차단규칙 설정을 이용하여 해당 연결 시도를 차단

※ 예) 내부 호스트의 슬래머웜 감염시 침입차단시스템에서 외부로 나가는 패킷 중 도착지 포트번호가 1434 포트인 패킷을 차단하여 내부에서 외부로의 공격을 차단

(4) 외부 네트워크와의 연결 차단

(가) 대규모 피해를 유발하는 악성코드공격으로 인하여 침해사고가 발생한 경우나 많은 트래픽 발생으로 인해 기관의 인터넷 접속 자체가 불가능한 경우에 실무기관은 기관의 인터넷 접속 경계에서 접속 단절을 권고

(5) 미확인 악성코드 대처

(가) 감염이 의심되나 현재까지 알려지지 않은 악성코드는 과학기술정보보호센터 등 사이버안전 전문기구에 도움 요청하여 조치

o 현재 보유하고 있는 백신 프로그램으로 탐지되지 않는 악성코드로 인하여 사고가 발생하였거나 의심되는 경우 과학기술정보보호센터, 국가사이버안전센터 및 백신업체에 연락하여 조치

(6) 사고통보

(가) 실무기관의 장은 악성코드공격으로 인한 사고 발생의 경우 과학기술정보보호센터에 통보하고 과학기술정보보호센터는 과학기술부에 통보

(나) 과학기술부 장관은 소관분야 정보통신망이 악성코드 공격으로 인하여 사고가 발생한 경우에 그 사실을 국가정보원장에게 통보

나. 서비스거부공격 대응요령

서비스거부공격에 의한 사고 발생의 경우 해당 공격근원지로부터의 모든 트래픽을 차단해야 하며 세부 대응요령은 다음과 같음

(1) 서비스거부공격 유형 판단

(가) 정보보안책임자(실무자)는 공격자의 서비스거부공격의 유형을 판단하기 위하여 MRTG(Multi Router Traffic Grapher)와 같은 트래픽 모니터링 도구를 이용하여 네트워크 트래픽 모니터링

(나) 라우터, 침입차단시스템, 침입탐지시스템 등으로 부터의 로그 기록정보를 참조하여 공격 증상을 확인

(2) 네트워크 장비를 이용한 서비스거부공격 추적·차단

(가) 라우터의 트래픽 분석기능을 이용하여 서비스거부 공격의 근원지를 추적

(나) 공격의 특성에 맞게 라우터나 스위치에 CAR 또는 ACL을 설정하여 해당공격을 차단

※ 네트워크 장비를 이용한 서비스거부공격 추적·차단에 대한 자세한 정보는 국가사이버안전매뉴얼(p257) 참조

(다) 공격의 특성에 맞게 침입차단시스템의 차단규칙을 설정하여 해당 공격을 차단

※ 예) 슬래머 웜을 통한 서비스거부공격 발생시 침입차단시스템에서 1434 포트로 유입되는 패킷 차단

(3) 정보통신서비스제공자(ISP) 차단규칙을 통한 공격 차단 및 추적

(가) 외부 호스트로부터의 서비스거부공격으로 인하여 기관의 인터넷 라우터가 정지 및 오동작하는 경우에 해당 기관은 공격 차단 및 공격자 추적 등을 과학기술정보보호센터에 요청

(나) 과학기술정보보호센터는 과학기술부를 통하여 실무기관의 요청사항을 관계기관에 통보하고 협조요청

(4) 피해시스템의 위치 재배치 및 중요자료 백업

(가) 특정 호스트가 공격 대상이 되고 다른 서비스거부 공격 대응 전략이 효과가 없는 경우, 해당 호스트를 다른 IP 주소로 대체

(나) 피해시스템의 빠른 복원을 위하여 가능한 빨리 백업 도구를 이용하여 CD나 저장테이프 등 보조기억장치에 시스템의 데이터를 백업

(다) 특정 호스트가 공격 대상이 되고 다른 서비스거부 공격 대응 전략이 효과가 없고 공격에 대한 피해가 크다고 판단될 경우, 기관장의 승인을 득한 후 공격 대상 네트워크를 분리

(5) 악용되고 있는 보안취약점 또는 결함 제거

(가) 취약점이 존재하는 시스템의 서비스를 이용하는 서비스 거부공격의 경우, 해당 서비스 포트로 패킷이 유입되지 않도록 침입차단시스템이나 라우터에서 차단규칙을 설정하여 패킷을 차단

(나) 유사공격의 재발을 방지하기 위하여 보안패치 되지 않은 시스템은 해당 취약점을 각 운영체제별 패치 사이트에서 패치를 다운받아 설치

다. 비인가접근공격 대응요령

(1) 피해시스템 격리 또는 관련 서비스 중지

(가) 시스템의 추가적 피해 및 피해 확산 방지를 위해 가능한 사고 시스템을 물리적, 논리적으로 분리

(나) 비인가접근공격 근원지를 식별하고, 라우터·스위치·침입차단시스템의 차단규칙 및 서버시스템의 네트워크 차단규칙 설정을 통하여 사후 비인가접근을 차단

(2) 로그 자료 백업

(가) 비인가접근공격 근원지를 식별하고, 원인 파악을 위한 중요한 단서로 사용 될 로그 자료를 안전하게 백업 및 보관

(3) 비인가접근공격에 사용된 계정 제거

(가) 공격에 이용된 계정을 식별하고 윈도우시스템의 사용자 관리 도구와 유닉스 시스템의 'userdel' 명령어를 이용하여 해당 사용자계정을 사용 중지 또는 제거

(나) 내부 사용자가 외부 조직을 공격하는 것과 같은 부적절한 행위를 발견할 경우 이 사용자를 찾아내어 추가적인 피해를 방지

(다) 외부에서 내부 네트워크로 비인가접근공격 시도를 발견한 경우, 과학기술정보보호센터와 협력하여 불법접근 사용자계정의 제거 또는 점검

(4) 사고통보

(가) 실무기관의 장은 비인가접근공격으로 인한 사고 발생의 경우 그 사실을 과학기술정보보호센터에 통보하고 과학기술정보보호센터는 과학기술부에 통보

(나) 과학기술부 장관은 소관분야 정보통신망이 비인가접근 공격으로 인하여 사고가 발생한 경우에 그 사실을 국가정보원장에게 통보

라. 복합구성공격 대응요령

사고별 대응요령을 나열하고 중요도를 판별하여 우선순위에 따라 공격기법별 사고 대응절차를 모두 수행

Ⅲ. 평시 안전점검 체크리스트

1. 점검분야

대분류	중분류	소분류
가. 정보보안 관리체계	(1) 정보보안정책	(가) 정보보안지침
		(나) 검토 및 평가
	(2) 정보보안조직	(가) 정보보안 조직
		(나) 정보보안 협력
		(다) 정보보안 인력
나. 정보보안계획 및 활동	(1) 정보보안계획	(가) 활동계획 수립
		(나) 정보보안 활동 수행
	(2) 개인정보보안 활동	(가) 개인별 직무책임
		(나) 보안사고 보고
	(3) 정보보안사고 예방 및 대응	(가) 예방활동
		(나) 대응체계 구축
		(다) 재발방지 대책
	(4) 정보보안감사	(가) 정보보안 감사
다. 정보자산통제	(1) 정보취급 절차	(가) 분류지침
		(나) 자산목록
		(다) 비밀보안대책
	(2) 정보자산 도입 및 폐기	(가) 정보자산 승인
		(나) 안전한 폐기 및 사용
		(다) 가용성 보장 계획
	(3) 매체관리	(가) 기억매체 관리
라. 인적보안	(1) 인원보안	(가) 직무책임
		(나) 직무분장
		(다) 인원선발 정책
		(라) 보안규정 준수
	(2) 정보보안교육 및 훈련	(가) 정보보안교육 및 훈련
	(3) 정보보안의식 및 환경조성	(가) 정보보안의식 및 환경조성

대분류	중분류	소분류
마. 물리적 보안	(1) 시설보안	(가) 물리적 보호구역
		(나) 출입통제
		(다) 물품배달・수령
		(라) 보호구역에서의 작업
		(마) 도청 예방 활동
	(2) 재난복구대책	(가) 재난복구대책 수립
		(나) 재난복구대책 검토
		(다) 장비보호
		(라) 전원공급
		(마) 통신회선 보호
바. 접근 보안대책	(1) 접근 보안지침	(가) 접근 보안지침
	(2) 네트워크 보안	(가) 네트워크 사용에 관한 정책
		(나) 원격 사용자 인증
		(다) 시스템 인증
		(라) 네트워크상의 분리
		(마) 네트워크 연결 정책
		(바) 네트워크 관리
		(사) 무선통신망 보안
	(3) 정보시스템 보안	(가) 시스템 접근통제
		(나) 중요시스템 격리
		(다) 공유자원 제한 통제
		(라) 시스템 유지 보수
	(4) 사용자 인증 및 계정관리	(가) 사용자 인증
		(나) 사용자 계정관리
		(다) 패스워드 사용
		(라) 로그온 절차
	(5) 응용프로그램 접근통제	(가) 응용프로그램 접근통제

대분류	중분류	소분류
사. 운영관리	(1) 운영상의 변경통제	(가) 운영상의 변경통제
	(2) 서비스 관리	(가) 필요서비스 관리
		(나) 전자우편 보안
		(다) 서비스 보안
	(3) 정보보호시스템 보안	(가) 정보보호시스템 설치 및 구성
		(나) 정보보호시스템 활용 및 보호
	(4) 악성코드 관리	(가) 악성코드 관리
	(5) PC보안 관리	(가) PC보안 관리
	(6) 로그 및 모니터링	(가) 로그
		(나) 시스템 사용 감시
		(다) 시스템 감사기록 보안
	(7) 백업	(가) 백업
아. 시스템 개발 및 유지보수	(1) 시스템 개발 및 정보보안 요구사항	(가) 정보보안 요구사항분석
		(나) 시스템 시험 및 평가
		(다) 개발환경 보호
	(2) 운영소프트웨어 보안	(가) 운영소프트웨어의 통제
		(나) 변경통제 절차
		(다) 기술적 검토
	(3) 외주관리	(가) 외주관리
자. 보안시스템	(1) 암호사용	(가) 암호사용지침
		(나) 암호취급인가
		(다) 암호실 사용
	(2) 암호장비	(가) 암호장비 사용
		(나) 관리자 지정 및 변경
		(다) 암호장비 운용관리
	(3) 암호자재	(가) 등록 및 관리
		(나) 취급 및 파기
	(4) 암호논리	(다) 암호논리

2. 점검항목

가. 정보보안 관리체계

(1) 정보보안정책

(가) 정보보안지침

보안대책 : 국가사이버안전관리규정, 국가정보보안기본지침 등 국가정보보안 정책을 기본으로 각급기관 자체 지침을 작성하고 기관장이 승인하여야 하며, 모든 직원에게 배포되고 주기적으로 교육을 실시하여야 한다.

점 검 항 목	구분
정보보안에 관련된 정책 및 지침이 규정화되어 있는가	A
정보보안정책은 관련법령 및 규정, 지침, 상급기관의 정보보안정책을 모두 수용하고 있는가	B
정보보안정책은 기관장에 의해 승인되었는가	A
정보보안정책 또는 지침은 직원에게 배포하였는가	A
직원에게 정보보안정책을 이해시키기 위하여 교육을 실시하고 있는가	B

(나) 정보보안정책 검토 및 평가

보안대책 : 새로운 위험 및 취약성의 대두, 기술변화에 따른 중요 정보시스템의 환경변화를 반영하기 위해, 정보보안지침을 주기적으로 검토해야 한다.

점 검 항 목	구분
정보보안정책 또는 지침은 주기적으로 검토하고 있는가	A

(2) 정보보안조직

(가) 정보보안조직 구성 및 역할

보안대책 : 정보보안 관리를 위한 전담조직이 구성되어 있으며, 보안심사위원회는 종합적인 정책, 지침의 검토와 승인, 주요 정보자산의 변화, 보안사고 검토와 모니터링, 정보보안관련 주요안건의 승인 등의 임무를 수행해야 한다.

점 검 항 목	구분
정보보안 전담조직이 있는가	C
보안심사위원회는 구성되어있는가	A
보안심사위원회의 활동이 활발히 수행되고 있는가	A
정보보안 업무를 수행하는 부서는 업무 처리시 타부서로부터 독립적인가	B

(나) 정보보안 협력

보안대책 : 정보보안 역할과 책임, 위험평가와 보안의식 제고 계획 등 조직차원의 협력에 필요한 사항을 조정하고 보안사고 대응을 위한 국가정보원, 중앙행정기관, 관련업체 등과 적절한 협력관계를 유지해야 한다.

점 검 항 목	구분
관련부서와의 업무분장 및 협조체계가 수립되어 있는가	B
국정원, 중앙행정기관, 관련업체 등과 적절한 조직간 협력 관계가 유지되는가	A
보안대책의 자문을 위해 전문기관이나 외부 전문가의 도움을 받을 수 있는 방안이 있는가	C

(다) 정보보안 인력

보안대책 : 정보보안 역할과 책임배정이 명확히 정의되어 있고, 각 자산의 보안을 위해 보안절차와 점검책임을 부여해야 한다.

점 검 항 목	구분
정보보안 전담인력이 있는가	B
정보보안과 관계된 모든 활동에 책임지는 관리자가 있는가	C
자산보호 및 정보보안절차 수행과 책임을 명확히 정의하였는가	B

나. 정보보안계획 및 활동

(1) 정보보안계획

(가) 활동계획수립

보안대책 : 정보보안활동 추진계획을 수립·시행하여야 한다.

점 검 항 목	구분
연간 보안활동 추진 계획이 수립되어 있는가	A
정보보안활동 계획은 관련 조직이나 기관장, 책임자에 의해 심사, 승인되었는가	A
전년도 보안활동 추진 결과에 대한 심사분석을 하고 있는가	A

(나) 정보보안 활동 수행

보안대책 : 정보보안 활동은 추진계획에 의거하여 차질없이 수행되어야 한다.

점 검 항 목	구분
정보보안활동은 계획대로 추진되고 있는가	B
보안활동 추진 계획이 주기적으로 검토되고 조정되는가	B

(2) 사용자 정보보안 활동

(가) 개인별 직무책임

보안대책 : 정보보안 관리책임을 숙지하여 관리책임이 있는 정보자산을 보호하고 일상의 보안에 대하여 점검해야 한다.

점 검 항 목	구분
직원들은 본인의 보직에 관련된 정보보안규정을 숙지하고 있는가	A
퇴근 전 기본적인 정보보안 점검을 수행하는가	A
직원은 개인이 관리하는 정보자산에 대하여 정보보호 생활수칙을 준수하는가	B

(나) 보안사고 보고

보안대책 : 모든 직원은 보안사고 조치절차를 숙지하여, 보안사고에 대한 대응조치와 공식적인 보고를 수행해야 한다.

점 검 항 목	구분
직원은 정보보안사고시 가장 먼저 보고(통보)하여야 할 사람이 누구인지 알고 있는가	A
직원은 사이버 공격 등 정보보안 사고시 조치사항을 알고 있는가	A

(3) 정보보안사고 예방 및 대응

(가) 정보보안 예방활동

보안대책 : 정보보안 사고를 최소화하기 위하여 보안취약점을 분석하고 보안대책을 수립해야 한다.

점 검 항 목	구분
정보보안 예방활동에 관한 지침, 매뉴얼이 있는가	A
시스템 또는 서비스에서 발견되거나 의심되는 보안 취약점 및 위협을 보고하는가	B
주기적으로 자체 취약점 점검을 실시하는가	B
정보시스템에 대한 정보보안 취약점 분석·평가를 실시하는가	B

(나) 정보보안사고 대응체계 구축

보안대책 : 정보보안 사고대응 및 조치절차를 수립·교육하고 대내외 비상연락체계를 구축하고 정보를 공유해야 한다.

점 검 항 목	구분
정보보안사고 대응계획 및 보고, 조치 절차를 수립하였는가	A
정보보안사고에 대비한 비상연락체계를 유지하고 있는가	A
정보보안사고에 대비하여 사이버안전 전문기구와 협조체계를 유지하고 있는가	A
정보보안사고 중요도 등급에 따른 대응요령을 준수하는가	A
정보보안사고 발생시 대응절차에 관한 훈련을 전직원이 받고 있는가	B

(다) 사고 재발방지 대책

보안대책 : 보안사고와 장애를 감시하고 재발 여부 및 영향력을 확인하며 향후 발생빈도나 피해를 감소시킬 수 있는 대책을 마련해야 한다.

점 검 항 목	구분
정보시스템 기능장애를 보고하기 위한 절차가 수립되어 있는가	C
정보보안사고와 기능장애를 분석하고 유사사고가 반복되지 않도록 재발방지 대책을 수립·시행하는가	B

(4) 정보보안감사

(가) 정보보안감사 시행

보안대책 : 정보보안 감사는 정기적으로 수행하고, 감사결과 도출된 미비점은 지속 보완하여야 한다.

점 검 항 목	구분
정보보안정책의 적절성 평가 및 시행여부 확인을 위한 정보보안감사 및 활동에 관한 규정이 있는가	A
정보보안감사는 정기적으로 수행되는가	A
정보보안감사 결과 도출된 미비점에 대한 보완조치를 하고 있는가	B

다. 정보자산통제

(1) 정보취급 절차

(가) 정보자산 분류지침

보안대책 : 모든 정보자산은 국가정보통신보안기본지침에 의거 분류되고 분류체계를 정기적으로 검토해야 한다.

점 검 항 목	구분
모든 정보자료 및 자산은 관리자가 지정되어 있으며 관리자의 임무가 명시되어 있는가	A
정보자료 및 자산의 분류와 관리에 관한 규정이 있는가	A

(나) 자산목록 관리

보안대책 : 모든 정보자산에 대한 목록이 작성되고 관리되어야 한다.

점 검 항 목	구분
정보자산은 중요도에 따라 구분하고 관리번호를 부여하여 관리하고 있는가	A
정보자료 공개시 보안심사위원회 또는 보안담당과 등 자체규정에 의거 보안성검토를 받고 있는가	A

(다) 비밀보안대책

보안대책 : 기밀이나 중요한 정보로 분류된 정보자산에 대하여 보안대책이 강구되어야 한다.

점 검 항 목	구분
비밀자료 보안을 위한 지침, 절차가 있는가	A
컴퓨터에서 문서 및 보조기억매체로 출력된 비밀자료(대외비 포함)는 관리대장 및 로그에 기록되어 관리되고 있는가	A
P2P 등의 프로그램이나 정보통신설비, 음성, 팩스 및 비디오의 사용을 통한 정보유출을 방지하기 위한 보안대책을 수행하고 있는가	C
비밀 및 중요문서 전송시 인가되지 않은 접근, 오용 또는 변조로부터 보호되는가	A
출력물을 통해 중요정보가 유출되지 않도록 적정등급의 비밀을 표기 하고 주기적으로 이상유무를 점검하는가	C

(2) 정보자산 도입 및 폐기

(가) 정보자산 승인

보안대책 : 새로운 정보자산에 대한 승인절차가 있으며 정보보안 정책 또는 지침의 적용여부, 호환성에 대한 검토가 고려되어야 한다.

점 검 항 목	구분
새로운 정보자산에 대하여 인가 또는 승인하는 과정이 수립되어 있는가	A
인가된 장비(H/W, S/W)만을 사용하도록 규정하고 이에 따른 책임을 정의하고 있는가	C
새로운 정보시스템,업그레이드 및 새로운 버전에 대한 승인기준이 수립되어 있는가	A
정보통신보안담당관은 새로 구축된 정보통신시스템의 정보보안체계가 부적절하다고 판단시, 그 시스템의 사용 연기나 문제점에 대한 조치를 요구할 수 있는가	C

(나) 정보자산 폐기

보안대책 : 중요정보를 저장한 정보시스템이나 저장매체를 안전하게 폐기하기 위한 적절한 절차가 있어야 한다.

점 검 항 목	구분
시스템 고장 및 수리시 내장된 자료유출 방지를 위한 보안대책이 수립·시행되는가	B
정보자산의 외부 반출입은 통제되고 있는가	A
컴퓨터 등 자료 저장기능이 있는 장비를 안전하게 폐기하기 위한 절차가 있는가	A

(다) 가용성 보장

보안대책 : 업무를 지원하는 중요 시스템과 네트워크 장비의 성능, 구성, 장애 등을 관리하고 적정한 가용성을 보장해야 한다.

점 검 항 목	구분
정보시스템의 저장용량, 네트워크 대역폭 등 가용성 요구사항에 대한 계획을 수립하고 있는가	B

(3) 매체관리

(가) 기억매체 관리

보안대책 : 기억매체의 안전한 관리를 위해 구입·관리·저장 등에 대한 보안관리가 이루어지고, 소각·절단 등 재생 불가능한 방법을 이용하여 폐기해야 한다.

점 검 항 목	구분
기억 매체에 대한 구입, 관리, 저장 및 파기에 대한 통제가 이루어지고 있는가	A
비밀(대외비 포함)처리 및 저장에 기억매체 사용 시 보안대책이 수립·시행되고 있는가	A
기억매체 파기시 자료를 확실하고 안전하게 삭제하고 있는가	A

라. 인적보안

(1) 인원보안

(가) 역할 및 책임 규정

보안대책 : 정보보안 정책 또는 지침에 따라 직원들의 역할과 책임을 적절하게 규정해야 한다.

점 검 항 목	구분
내부 및 외부인원의 보안통제에 관한 규정이 있는가	A
정보보안규정·지침은 관리자 및 일반사용자의 정보보안과 관련한 직무 책임범위를 명시하고 있는가	A
모든 신입직원에게 보안 유의사항과 그들의 책임에 대한 설명이 충분히 이루어지고 있는가	B

(나) 직무분장

보안대책 : 특정 직무의 관리나 시행 또는 책임분야를 명확히 분리하여 적절한 권한을 주어야 한다.

점 검 항 목	구분
개인의 보직 및 임무에 따라 정보자산에 대한 상이한 권한이 주어지는가	A
역할에 따라 직원의 직무를 명확히 분리·운영하고 있는가	A

(다) 인원선발 및 관리정책

보안대책 : 인원선발시 신원조사 등 충분한 검증조사를 시행하고, 인사이동시 접근권한도 신속하게 변경하여야 하며, 중요정보를 관리하는 직원에 대하여 정기적인 확인을 수행해야 한다.

점 검 항 목	구분
직원선발시 직무에 따른 신원조사는 철저히 수행되는가	A
비밀 등 중요정보를 다루는 직원에 대해서 비밀취급인가, 보안서약서 징수 등 보안대책 수행하는가	A
인사 변동에 따른 접근권한 조정이 신속하게 이루어지는가	A

(라) 보안규정 준수

보안대책 : 직원의 보안규정 준수를 독려하기 위해 보안규정 이행여부를 직원평가에 반영해야 한다.

점 검 항 목	구분
직원평가시 정보보안에 관련된 규정준수 여부가 반영되어 있는가	B
직원의 보안규정 위반에 따른 징계 절차가 있는가	A
특권을 가진 직원에 대한 주기적인 점검이 이루어지는가	C

(2) 정보보안교육 및 훈련

(가) 정보보안교육 및 훈련실시

보안대책 : 정보보안 정책 및 절차에 대해 주기적 교육 및 훈련을 실시하여 보안의식을 제고토록 하여야 한다.

점 검 항 목	구분
정보보안교육, 정보보안의식 고취 및 환경 조성에 관한 내용이 규정되어 있는가	A
연간 정보보안교육계획을 수립하여 수행하는가	A
일반직원을 대상으로 기초 정보보안교육은 정기적으로 시행되고 있는가 (수단:소집교육, 유인물 배포, 정보통신망 게재 등)	A
정보보안담당자 및 시스템관리자의 역량강화를 위한 전문 보안교육을 수행하는가	B

(3) 정보보안의식 및 환경조성

(가) 정보보안 환경조성

보안대책 : 정보보안 준수환경을 조성하기 위해 지속적인 의식 강화 활동을 수행해야 한다.

점 검 항 목	구분
사용자에게 정보보안관련 경각심을 줄 수 있는 홍보활동을 하고 있는가	A
기관장에게 진행중인 정보보안계획과 정보보안 문제를 정기적으로 보고하고 있는가	A
기관의 장과 각 부서의 책임자는 정보보안 강화관련 메시지(문서, 메일, 게시판 등)를 지속적으로 전파하고 있는가	B

마. 물리적 보안

(1) 시설보안

(가) 보호구역 지정 및 관리

보안대책 : 보호구역을 지정하여 운영하는 각급기관장은 비인가자의 무단 출입 및 침투를 방지하기 위한 보안대책을 강구해야 한다.

점 검 항 목	구분
보호구역의 물리적 접근통제에 대한 내용이 규정되어 있는가	A
주요 정보자산을 보호하기 위하여 보호구역을 설정하였는가	A
보호구역에서의 작업에 대한 지침이 있는가	B

(나) 출입통제

보안대책 : 보호구역에 대한 출입을 출입목적에 따라 인가하고 출입일시를 기록하며 감독해야 한다.

점 검 항 목	구분
보호구역 분류에 따른 보안대책을 수립하여 수행하고 있는가	A
중요 정보시스템은 보안 및 환경적 위험으로부터 물리적으로 보호되고 있는가	A
보호구역에 대한 접근권한을 출입목적에 따라 인가하고 있는가	B
보호구역에 대한 접근권한은 정기적으로 검토 및 갱신되고 있는가	A
보호구역은 경비원 또는 CCTV등에 의해 출입이 모니터되고 있는가	A
출입통제 기록을 관리하고 있는가	A
물리적 접근에 대한 감시와 사고조사 및 교정 노력이 행해지는가	C

(다) 물품 반입 통제

보안대책 : 물품배달·수령은 통제되어야 하며, 인가되지 않은 접근을 피하기 위하여 보호구역으로부터 떨어져 있어야 한다.

점 검 항 목	구분
물품배달 및 수령은 통제되고 있는가	C

(라) 보호구역내 작업통제

보안대책 : 보호구역에서의 작업시 비인가된 접근 등 자료유출 차단을 위한 보안대책이 있어야 한다.

점 검 항 목	구분
보호구역에서 근무하는 외부인력의 작업은 항상 감시되고 있는가	A
보호구역에 주기적으로 출입하는 외부인에 대한 보안서약서를 징수하는가	B

(마) 도청 예방 활동

보안대책 : 도청에 대한 보안대책이 있어야 한다.

점 검 항 목	구분
내부로 유입되는 각종 장비 및 물품 등에 대해 도청장치 은닉여부를 보안검색을 하는가	B
중요회의 및 협상시 해당장소에 대해서 도청 위해 요소 제거 등 보안대책을 강구하는가	B
은닉된 도청장치 탐색을 위한 활동계획을 수립 시행하는가	B

(2) 재난복구대책

(가) 재난복구대책 수립

보안대책 : 재난발생에 대비하여 재난복구대책을 수립, 시행해야 한다.

점 검 항 목	구분
재난·재해 및 사이버공격 등에도 기관업무가 지속될 수 있는 재난복구대책이 수립되어 있는가	A
비상사태 발생시 대피 우선순위를 부여한 소산 절차서가 있는가	A
복구에 대한 책임 할당 등 복구절차가 수립되어 있는가	A
비상시 데이터 복구, 시스템 복구 등을 위하여 시스템 공급업체와 유지보수 계약이 체결되었는가	A

(나) 재난복구대책 검토

보안대책 : 재난복구대책을 정기적으로 시험하여 영향평가를 실시한다.

점 검 항 목	구분
재난복구대책을 정기적으로 시험하고 검토하는가	B
재난·재해시 업무지속성에 대한 영향분석을 실시하는가	C
재난·재해시 취할 보안 절차에 관한 훈련을 받고 있는가	A

(다) 장비보호

보안대책 : 정보자산은 재난·재해에 대비하여 보호하여야 한다.

점 검 항 목	구분
정보통신실은 온도,습도,방진 등에 있어 시스템이 운영될 수 있는 적합한 환경을 유지하고 있는가	B
중요 장비가 사용 불가능하게 될 때 이를 대체할 장비가 있는가	B
네트워크 장애 또는 마비시 네트워크 복구가 가능한가	B

(라) 전원공급

보안대책 : 장비는 정전 및 기타 전기적 이상으로 부터 보호해야 한다.

점 검 항 목	구분
지속적인 전원 공급 지원을 위한 대책을 강구하고 있는가	B
전력선, 전원장비에 대한 주기적인 위험요소와 고장 여부를 검토하는가	B

(마) 통신회선 보호

보안대책 : 정보를 전달하는 통신회선은 재난·재해, 악의적 절단, 도청으로부터 보호해야 한다.

점 검 항 목	구분
통신회선 보호를 위한 대책이 있는가	C
정보통신 설비도면의 구성에 관한 최신자료를 유지·관리하고 있는가	C

바. 접근 보안대책

(1) 접근 보안지침

(가) 접근 보안지침 수립

보안대책 : 접근 보안대책은 업무 필요성과 연계 승인, 문서화하고, 접근 보안 정책에 따라 접근을 제한하여야 한다.

점 검 항 목	구분
접근 보안지침을 규정화하고 있는가	A
관리자는 사용자 접근을 통제하기 위하여 사용자의 접근권한을 정기적으로 검토하는가	A
시스템 및 네트워크 장비 제작·용역업체의 초기설정을 변경하였는가	B
시스템 및 응용프로그램에 대한 정보 접근을 제한하기 위하여 시스템 관리자와 사용자의 권한을 명확히 구분하여 통제하고 있는가	B

(2) 네트워크 보안

(가) 네트워크 보안정책

보안대책 : 네트워크 보안정책은 접근허가와 비인가된 네트워크 서비스 접근시도에 대한 인증절차, 연결 서비스에 대한 보안절차 등을 포함해야 한다.

점 검 항 목	구분
네트워크 서비스 사용에 관한 접근통제 규정이 있는가	A
네트워크 장비에 대한 원격관리시 접근권한이 적절히 설정되어 있는가	B
정보통신망 신·증설시 보안대책을 강구하고 있는가	B
네트워크의 노드에 할당된 주소는 규정에 따라 체계적으로 관리하는가	B

(나) 원격 사용자 인증

보안대책 : 원격 사용자를 인증하기 위한 보안대책이 있어야 한다.

점 검 항 목	구분
원격접속을 인가하고 통제하기 위한 규정이 존재하는가	A
원격 사용자의 접근을 인증하기 위한 인증서, IP인증 등의 통제절차가 있는가	B

(다) 시스템 인증

보안대책 : 원격 컴퓨터 시스템에 대한 연결을 인증해야 한다.

점 검 항 목	구분
네트워크 장비는 네트워크내 타 노드로의 접속에 대하여 접근통제를 수행하는가	A
중요 시스템에 대한 원격 연결은 제한된 시스템에서만 가능하도록 시스템 인증을 수행하고 있는가	B

(라) 네트워크상의 분리

보안대책 : 정보서비스, 사용자 및 정보시스템 중요도, 업무 연관성 등을 고려하여 네트워크내 보안대책을 강구하고, 허용된 네트워크내에서만 접근 가능해야 한다.

점 검 항 목	구분
네트워크 중요도에 따라 네트워크를 분리하여 운영하고 있는가	A
내부망과 인터넷·상용망은 물리적으로 분리되어 있는가	C
네트워크 장비의 원격관리는 신뢰된 주소로 제한하여 접근통제를 수행하고 있는가	A

(마) 네트워크 연결 정책

보안대책 : 접근통제 정책에 따라 사용자의 접속은 공유된 네트워크내로 제한해야 한다.

점 검 항 목	구분
네트워크의 접근을 제한하기 위하여 통제수단(네트워크 접근통제 정책, 침입 차단시스템 등)이 있는가	A
네트워크 연결에 대한 보안대책은 적절하게 유지되고 주기적으로 검토되는가	B
불필요한 신뢰관계(r-서비스, nfs 등)로 연결된 시스템이 존재하지 않는가	C
내부 네트워크 정보(IP, 시스템 정보, 구성도 등)를 외부로부터 보호하고 있는가	C
모뎀을 이용한 내부망 접속 시 보안대책을 강구하고 통제하는가	C

(바) 네트워크 관리

보안대책 : 네트워크상의 에러 또는 보안문제를 파악하기 위해 보안관리를 수행해야 한다.

점 검 항 목	구분
통신 회선은 충분한 용량을 가지고 있으며 네트워크 구성과 운영에 문제가 없는가	B
네트워크 장비들의 버그나 보안취약점을 패치하였는가	B
네트워크상의 에러등을 파악하기 위해 네트워크 관리 시스템을 설치 운영하고 있는가	B

(사) 무선통신망 보안

보안대책 : 무선통신망을 이용시 사용자 접근, 인증 및 전송 자료에 대한 보안 대책을 강구해야한다.

점 검 항 목	구분
무선통신망 구축시 도청, 전파월경 등에 대한 보안대책은 강구되었는가	B
무선랜 사용시 비인가자에 의한 무단접속 등에 해킹에 대비 보안대책은 강구 되었는가	B

(3) 정보시스템 보안

(가) 시스템 접근통제

보안대책 : 정보시스템에 대한 접근통제가 정의되어 사용자가 감시되어야 한다.

점 검 항 목	구분
정보시스템에 대한 접근통제가 정의되어 있는가	A
정보시스템에 대한 권한부여 및 사용은 통제되고 감시되는가	A
시스템의 비인가 사용자에 대한 처벌 규정(사용자에 대한 책임과 절차)을 적용하고 있는가	B

(나) 중요시스템 격리

보안대책 : 중요시스템을 분류하여 접근을 엄격히 제한하여야 한다.

점 검 항 목	구분
중요 시스템에 대하여 격리된 전용 컴퓨팅 환경을 제공하고 있는가	B
관리자 권한으로 접속하는 단말기는 제한, 지정되어 있는가	B

(다) 공유자원 제한 통제

보안대책 : 시스템 자원을 공유할 경우에는 적절한 보안대책을 강구해야 한다.

점 검 항 목	구분
공유 시스템 자원(공유 폴더, 파일 등)에 대한 접근통제는 적절하게 수행되고 있는가	A
일반사용자의 특정 시스템 유틸리티 프로그램 및 명령어 사용을 제한하고 있는가	C
멀티유저 환경에서 타 사용자 정보열람, 변경을 제한하고 있는가	C

(라) 시스템 유지 보수

보안대책 : 시스템 유지/보수시 외부직원에 대한 통제와 보안대책을 강구해야 한다.

점 검 항 목	구분
주요 시스템에 대해 외부업체의 원격 작업을 허용하고 있지 않은가	B
시스템 유지 또는 보수에 대한 절차가 있는가	B

(4) 사용자 인증 및 계정관리

(가) 사용자 인증

보안대책 : 적절한 사용자 인증 대책을 강구해야 한다.

점 검 항 목	구분
정보시스템에 대한 안전한 연결을 보장하기 위한 사용자 인증절차가 있는가	A
중요서비스 제공시 사용자 인증을 위해 안전성이 입증된 인증메커니즘을 사용하고 있는가	B
전자서명인증체계를 사용하고 있는가	C
부인방지 서비스를 제공하는가	C
모든 멀티유저 정보시스템과 서비스에 대한 접근을 승인하기 위한 정형화된 사용자 관리절차가 있는가	A

(나) 사용자 계정관리

보안대책 : 사용자 계정관리에 대한 절차가 있어야 한다.

점 검 항 목	구분
사용자 계정 관리에 대한 절차가 규정되어 있는가	A
정보자산에 사용자 계정을 부여받을 때 본인임을 증명하는 절차가 있는가	B
모든 사용자는 해당 정보시스템 접근시 고유의 계정을 소유하고 있는가	A
사용자 계정관리 지침에 따른 주기적인 점검 및 갱신이 수행되고 있는가	B
예외적인 상황 또는 일시적인 계정이용은 정보통신보안담당관 또는 보안책임자의 승인하에 사용되는가	C

(다) 패스워드 사용

보안대책 : 패스워드의 선택과 사용에 대한 올바른 보안요구사항을 적용하고, 사용자 교육을 실시해야 한다.

점 검 항 목	구분
비밀번호의 선택과 사용에 대한 올바른 보안 요구사항(비밀번호 비밀유지, 최소 6자이상 조합된 비밀번호의 선택, 정기적 변경, 개인 비밀번호 공유 금지 등)이 적용되고 있는가	A
비밀번호파일은 암호화등의 보호메커니즘을 통하여 보호되는가	A
비밀번호는 사전에 존재하는 단어나 연상, 추측이 용이한 단어를 사용하지는 않는가	B

(라) 시스템 접근절차

보안대책 : 정보시스템에 대한 안전한 접근을 통제하기 위한 절차가 있어야 한다.

점 검 항 목	구분
로그온 진행 중 스니핑 등을 통한 민감 정보의 누출을 방지하고 있는가	C
로그온시 허용되는 세션유지, 재시도 간격 등의 최대시간과 최소시간을 제한하여 서비스 거부공격, 무작위 로그온 시도 등으로부터의 안전하게 운영하고 있는가	C
정상적인 로그인 후 일정기간동안 아무 행위를 발생하지 않으면 자동으로 로그아웃하는 기능을 수행하는가	B
로그온 실패횟수(3회 권장)를 제한하고 있는가	B
로그 On-Off에 대한 모든 기록을 유지 관리하고 있는가	B

(5) 응용프로그램 접근통제

(가) 응용프로그램 접근통제

보안대책 : 중요한 응용프로그램에 대하여 보안대책을 강구해야 한다.

점 검 항 목	구분
응용프로그램이 관리자에 의한 통제하에 서비스 되는가	A
중요 응용프로그램이 다중 사용자 환경에서 운영될 경우에 읽기·쓰기·실행 등의 권한이 적절하게 부여하여 운영하는가	C
원격접속자에 대해 시스템에 접근할 수 있는 시간을 제한하고 있는가	C

사. 운영관리

(1) 운영상의 변경통제

(가) 운영상의 변경통제

보안대책 : 정보시스템 운영중 변경에 대해 통제 하여야 한다.

점 검 항 목	구분
운영절차를 문서화하고 유지하는가	A
정보시스템 운영에 대한 변경을 통제하고 있는가	B

(2) 서비스 관리

(가) 필요서비스 관리

보안대책 : 보안위험을 감소시키기 위해 불필요한 서비스를 제거하고 보안패치를 주기적으로 수행해야 한다.

점 검 항 목	구분
중요 정보시스템의 필요한 서비스(포트)가 정의되어 있는가	A
불필요한 서비스를 제거하기 위해 주기적으로 검토하는가	A
사용하는 서비스, 시스템에 대한 보안 패치를 지속적으로 수행하고 있는가	A

(나) 전자우편 보안

보안대책 : 전자우편 운영절차를 수립하고 보안대책을 마련해야 한다.

점 검 항 목	구분
전자우편을 사용함으로써 발생할 수 있는 보안위험(정보유출, 변조 등)을 감소시키기 위한 대책이 존재하는가	A
스팸, 피싱메일을 비롯하여 트로이목마, 웜, 바이러스 등이 포함된 악성메일에 대한 보안대책은 존재하는가	A

(다) 서비스 보안

보안대책 : 외부로 서비스되는 정보를 보호해야 한다.

점 검 항 목	구분
외부로 서비스되는 정보의 무결성을 보장하는 방안이 존재하는가	C
정보시스템에 등록된 주민등록번호와 같은 개인정보를 보호하기 위한 보안대책이 존재하는가	C

(3) 정보보호시스템 보안

(가) 정보보호시스템 설치 및 구성

보안대책 : 정보보안 요구사항을 충족하도록 침입차단시스템 등 정보보호시스템을 설치해야 한다.

점 검 항 목	구분
정보보호시스템은 국가기관용의 정보보안 요구사항을 만족하는 인가, 승인된 제품을 선정하였는가	A
외부망 연결시 침입차단시스템 등 정보보호시스템이 설치되어 있는가	A
정보보호시스템의 구성은 가용성을 보장하는가	B
정보보호시스템 구성은 정보보안 요구사항을 충족하는가	A

(나) 정보보호시스템 활용 및 보호

보안대책 : 보안취약점에 대응할 수 있도록 정보보호시스템을 관리하고 동시스템에 대한 보안대책을 강구해야 한다.

점 검 항 목	구분
정보보호시스템에 대한 원격관리에 대한 보안대책이 있는가	A
정보보호시스템은 최신의 취약점에 대하여 대응할 수 있도록 주기적으로 업그레이드되고 시험되는가	A
정보보호시스템은 필요한 서비스만 제공되고 설치목적 외 다른 용도로 사용되지 않는가	A

(4) 악성코드 관리

(가) 악성코드 탐지·제거관리

보안대책 : 악성코드로부터 보호하기 위한 탐지, 방지수단을 도입하여 정기적인 검사를 수행해야 한다.

점 검 항 목	구분
외부에서 유입되는 악성코드(바이러스, 웜, 트로이목마 등)의 예방, 탐지, 대응을 위한 보안대책은 수립되었는가	A
정보시스템에 백신 프로그램이 설치되어 운영되고 있는가	A
백신 프로그램은 정기적으로 업데이트되고 있는가	A
백신프로그램, 보안 진단도구 등을 이용하여 주기적으로 악성코드 검사를 수행하는가	A

(5) PC보안 관리

(가) PC보안 관리

보안대책 : PC보안 지침을 작성하고 각 직원별 PC를 보호해야 한다.

점 검 항 목	구분
PC보안에 관한 내용이 규정화 되어 있는가	A
공유폴더 및 파일에 대한 통제내용이 명시되어 있는가	A
비인가자의 PC접근을 차단하기 위한 보안대책(화면보호기, 부팅통제, 비밀번호 설정 등)을 사용하고 있는가	A
PC의 자료 보호를 위해서 PC보안 소프트웨어(백신, PC방화벽, 암호화 등)를 설치 운영하고 있는가	A
버그 및 보안취약점에 대한 최신패치를 지속적으로 수행하는가	A
노트북 컴퓨터 등 이동 가능한 장비에 대한 보안대책을 강구하고 있는가	B
비밀 등 중요자료를 처리하는 단말기가 인터넷 및 상용망에 분리되어 있는가	B

(6) 로그 및 모니터링

(가) 로그 관리

보안대책 : 운영기록 및 시스템 오류를 기록하고 운영절차에 따라 보고하여야 한다.

점 검 항 목	구분
정보시스템 운영에 대한 기록(로그)을 보관하도록 규정하고 있는가	A
정보시스템에 대한 예외상황 및 오류를 기록하여 보고하도록 규정화되어 있는가	A
중요 정보시스템으로의 접속시도에 대한 로그 정보를 관리하는가	B
로그인 성공 시, 이전 로그인에 대한 날짜, 시간정보가 제공되며, 실패한 로그인등에 대한 정보가 제공되는가	B
데이터베이스에 대한 모든 질의와 개정작업은 로그에 기록되는가	B
주기적으로 로그를 점검하고 보고하는가	B
네트워크 장비 및 정보보호시스템의 로그정보를 보관·관리하고, 정기적으로 검토하고 있는가	B

(나) 시스템 사용 감시

보안대책 : 정보시스템의 사용을 감시하는 절차를 수립하고 감시활동의 결과를 정기적으로 검토해야 한다.

점 검 항 목	구분
침해사고시 중요 로그정보는 사고조사를 위해 관계법령, 규정, 지침에 의거 보존하는가	B
정보시스템의 사용을 감시하고 그 결과를 정기적으로 검토하는가	A
장애의 감지 및 복구를 위해 운영상황을 감시하는가	A

(다) 시스템 감사기록 보안

보안대책 : 운영시스템에서 생성·기록된 로그, 모니터링 등 감사기록에 대한 보안대책이 수립되어야 한다.

점 검 항 목	구분
감사기록 검토에 대한 책임과 역할 분담이 규정되었는가	A
감사기록의 비인가된 열람, 변경, 삭제 등에 대비하여 보안대책이 규정되어 있는가	B
감사기록을 효율적으로 분석하기 위하여 적절한 감사기록의 설계, 감사도구 및 유틸리티의 사용이 구현되고 있는가	C

(7) 백업

(가) 백업 관리

보안대책 : 안전한 백업시설을 확보하고 백업계획을 수립하여 정기적으로 백업을 수행해야 한다.

점 검 항 목	구분
중요 데이터파일과 운영요소들이 식별되고 백업계획이 규정되어 있는가	A
필수적인 소프트웨어 및 데이터에 대한 백업이 정기적으로 이루어지고 시험되는가	A
백업 데이터에 대한 보안대책이 수립되어 있는가	B
백업 시설은 전산실과 물리적으로 떨어진 안전한 장소에 설치하여 물리적인 테러, 재난·재해에 대비하고 있는가	B

아. 시스템 개발 및 유지보수

(1) 시스템 개발 및 정보보안 요구사항

(가) 정보보안 요구사항 분석

보안대책 : 시스템 개발 및 변경시 설계와 요구사항 정의단계에서 정보보안 요구사항에 대한 분석이 수행되어야 한다.

점 검 항 목	구분
시스템 개발 및 개선시 정보보안 요구사항에 대한 분석이 수행되고 보안성 검토가 이루어지고 있는가	A
새로운 위협, 취약성이 발견되거나 새로운 정보기술을 시스템에 적용할 때 정보보안 요구사항이 재검토되는가	C
각 부서에서 정보시스템 구축시 정보보안대책과 관련하여 계획단계부터 정보보안부서와 협의 하는가	B

(나) 시스템 시험 및 평가

보안대책 : 정보보안 요구사항을 충족하는지 시험평가를 수행하여야 한다.

점 검 항 목	구분
시스템 시험절차에서 정보보안 요구사항에 대한 평가 및 시험을 수행하는가	A
소프트웨어의 설치 운영 이전에 악의적 코드와 백도어 등을 탐지하기 위한 시험평가를 수행하는가	B
버퍼오버플로우, 크로스 사이트 스크립팅 등 보안취약점에 대비하여 응용프로그램에 대한 데이터 입력이 검증되는가	B
응용 프로그램으로부터의 데이터 출력이 적합한지 검증하는가	B

(다) 개발환경 보호

보안대책 : 개발중인 시스템 및 소스코드에 대한 접근을 통제하고 운영환경과 분리해야 한다.

점 검 항 목	구분
소프트웨어 기능시험시 시험 데이터 및 시스템에 대한 보안 대책을 강구하는가	B
개발중인 소스 프로그램에 대한 접근을 통제하는가	B
소프트웨어 운영환경과 개발 환경이 분리되어 있는가	B
소프트웨어 수정, 신규개발시 배포와 실행은 문서화되고 검토되는가	B

(2) 운영소프트웨어 보안

(가) 운영소프트웨어의 통제

보안대책 : 운영 시스템상에서 소프트웨어 구현을 통제하기 위한 절차를 갖춰야 한다.

점 검 항 목	구분
운영시스템상에서 소프트웨어 구현을 통제하고 시스템의 손상위험을 최소화하기 위한 관리지침이 있는가	A

(나) 변경통제 절차

보안대책 : 정보시스템 변경은 공식적인 통제절차에 의해 엄격히 통제해야 한다.

점 검 항 목	구분
정보시스템의 손상을 최소화하기 위하여 변경 시행에 대하여 엄격한 통제를 실시하는 공식적인 변경통제 절차가 있는가	A
운영 소프트웨어 패키지의 변경이 요구될 경우, 변경을 통제하는 절차가 있는가	B
운영 소프트웨어의 패키지 변경이 필수적인 경우, 원본 소프트웨어를 보관하고, 확인한 복사본에 변경사항을 적용하고 있는가	B

(다) 기술적 검토

보안대책 : 변경이 발생되는 경우 응용프로그램을 검토하고 시험해야 한다.

점 검 항 목	구분
운영시스템의 기술적 변경시 운영이나 보안상 영향을 확인하기 위한 검토 절차를 적용하고 있는가	B

(3) 외주관리

(가) 외주관리 보안

보안대책 : 외주용역에 의한 정보시스템 개발, 운영시 쌍방간이 합의한 계약서에 의해 엄격한 보안대책이 적용되어야 한다.

점 검 항 목	구분
외주용역에 의해 정보시스템을 개발하거나 운영시에는 보안요구사항에 대해 쌍방간에 합의한 문서가 있는가	A
임시고용인, 컨설턴트, 계약업자 등의 외주업체 직원이 중요 정보시스템에 접근할 때 위험을 식별하여 엄격한 보안통제가 이루어지는가	A
안전한 외주 소프트웨어 개발을 위한 통제절차의 수립과 적용을 수행하는가	B

자. 보안시스템

(1) 암호사용

(가) 암호사용지침

보안대책 : 정보자료의 보안을 위하여 암호장비를 사용하고자 할 경우에는 암호통제에 관한 내용이 규정화되어야 한다.

점 검 항 목	구분
정보보안을 위한 암호의 사용에 관한 내용이 규정화되어 있는가	A
암호장비 및 자재에 대한 보안대책이 규정화되어 있는가	A
비밀 등 중요자료 소통을 위해 보안시스템을 사용하고자 할 경우 국정원장이 개발제작하거나 승인한 제품을 사용하고 있는가	A
보안시스템의 무단복제 및 타기관이나 개인으로의 임의대여를 엄격히 금지하고 있는가	A

(나) 암호취급인가

보안대책 : 암호체계를 연구개발하거나 보안시스템을 취급하고자 하는 자는 암호취급을 인가받아야 하며, 관련업무를 수행하지 않을 경우 즉시 암호취급 인가를 해제해야 한다.

점 검 항 목	구분
암호체계 연구개발자 및 보안시스템 취급자는 암호취급을 인가받았는가	A
암호취급인가를 받은 자가 타부서 전출, 휴직 등으로 암호체계 관련 업무를 수행하지 않는 경우에 즉시 암호취급인가를 해제하는가	A

(다) 암호실 사용

보안대책 : 암호실을 설치하고자 하는 경우 출입을 통제하고 경비조치를 취하며, 폐쇄할 경우 암호장비 및 암호자재를 반납해야한다.

점 검 항 목	구분
암호작업이 필요하여 암호실을 설치한 경우 보안대책을 강구하였는가	A
암호실을 폐쇄한 경우 기관장의 책임하에 행하고 암호장비 및 자재를 지체없이 배부기관에 반납하였는가	A
암호실의 인가자만 출입할 수 있도록 통제되어 있는가	A

(2) 암호장비

(가) 암호장비 사용

보안대책 : 비밀 등 중요 정보자료의 안전한 전송을 위해 인가된 암호장비를 사용해야 한다.

점 검 항 목	구분
비밀 및 중요자료의 전송을 위해 암호장비 또는 암호자재를 사용하고 있는가	A
암호장비 사용시, 인가된 암호장비를 사용하고 있는가	A

(나) 암호장비 관리자 지정 및 변경

보안대책 : 암호장비의 보안관리를 위해 관리자를 지정하고, 관리자 교체시 인수인계가 적절히 이루어져야 한다.

점 검 항 목	구분
암호장비의 보안관리, 정,부 관리자가 지정 운영되고 있는가	A
관리자 교체시 암호장비 인수인계를 실시하고, 인수인계 사항을 기록 유지 하고 있는가	A

(다) 암호장비 운용관리

보안대책 : 암호장비의 운용을 위해 필요한 보안대책을 수립하고, 주기적인 점검을 수행해야 한다.

점 검 항 목	구분
암호장비의 동작여부를 주기적으로 점검하도록 절차를 수립하고, 절차에 따라 주기적으로 점검하는가	A
암호장비 키 저장, 사용, 변경, 파기 절차가 있는가	A
암호장비 고장시 정비범위 및 정비절차를 수립, 시행하고 있는가	A

(3) 암호자재

(가) 암호자재 등록 및 관리

보안대책 : 암호자재에 대한 보안대책을 위하여 모든 자재를 등록하고 주기적인 점검을 수행해야 한다.

점 검 항 목	구분
암호자재는 암호실내 별도 금고 또는 비밀 캐비냇에 보관되고 있는가	A
현용을 제외한 미래용, 과거용 암호자재는 봉인하여 보관하고 있는가	A
암호자재에 대해 주1회 주기적으로 이상유무 점검을 실시하는가	A

(나) 암호자재 취급 및 파기

보안대책 : 암호자재 배부 및 회수, 인수인계, 파기를 위한 보안대책을 수립해야 한다.

점 검 항 목	구분
암호자재 수발시 인감등록자가 업무를 수행하는가	A
암호자재의 인수인계를 실시하고, 인수인계 사항은 기록, 유지 되고 있는가	A
비상시 암호자재에 대한 긴급파기계획을 문서로 작성하고 각 부서에 전달 시행하고 있는가	A
암호자재를 임의 복사, 복제하여 사용하지 않는가	A

(4) 암호 논리

(가) 암호논리 사용

보안대책 : 암호논리 설치 및 운용관리를 위한 보안대책을 수립해야 한다.

점 검 항 목	구분
암호논리의 키를 안전하게 관리하며 주기적으로 키를 변경하는가	A
암호논리를 지급하는 자는 암호취급인가를 받았는가	A
암호논리가 내장된 정보통신시스템이 설치된 장소는 보호구역으로 설정하고 암호장비에 준하여 관리하거나 이에 상응한 보안대책을 강구하였는가	A

붙 임

1. 경보발령문(과학기술부 → 과학기술정보보호센터 → 실무기관)

경 보 발 령 문

제 목	○○○○○○ 관련 '관심' 경보 발령
발 령 일	0000년 00월 00일 00시 00분
개 요	○
대 응 책	○ 실무기관 대응책 1. 2. 3. ○ 개인 사용자 1. 2. 3.
관련정보	○ ○

※ 제목과 발령일 부분은 경고발령 수준에 따라 해당 경보수준 색으로함

관심 - 주의 - 경계 - 심각

2. 상황통보문(실무기관 → 과학기술정보보호센터 → 과학기술부)

상 황 통 보

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	o 기관내 사용자에게 대응책을 작성, 배포 o 전자우편 서버의 Filter를 적용 o 기관내 감염피해 확인 (피해대수 및 감염PC의 IP)		
조치대상 목록			
조치결과			
특이사항			

※ 이 양식은 과학기술정보보호센터 홈페이지(www.sntsec.or.kr)에서 내려 받을 수 있습니다.

※ Fax 042-869-0809 또는 sntsec@kisti.re.kr로 0000년 00월 00일 00시 00분까지 통보 바랍니다.

※ 제목과 발령일 부분은 경고발령 수준에 따라 해당 경보수준 색으로함

관심 - 주의 - 경계 - 심각

3. 사고신고 서식(실무기관→과학기술정보보호센터→과학기술부)

사 고 신 고

기 본 정 보			
기 관 명	00연구원	부 서	정보전산과
성 명	홍 길 동	직 위	과장
전자우편	hong@aaa.re.kr		
연 락 처	전화: 042-555-2837 H.P:010-310-9876 Fax: 042-555-2830		
사 고 내 용			
사고 일시	2006년 8월 17일 09시 15분	피해IP주소	146.52.34.21
피해시스템 용도	사, 아 * 뒷장의 '가.시스템 분류' 기호 입력	운영체제	■ 윈도우 □ 유닉스 □ 네트워크장비 상세버젼정보: Windows XP/2003
사고 유형	D * 뒷장의 '나.사고 유형' 기호 입력	피해범위	146 대 * 피해시스템이 여러대인 경우 피해숫자 기입
사고 내용	본연구원 홈페이지 자유게시판에 악성 유언비어 게시		
조 치 내 용			
공격자 정보	공격자 ID : jgsew, 접속IP : 43.12.56.77		
피해 현황	우리 정부를 비난하는 내용		
긴급조치 실시사항	게시자 ID 삭제 및 게시물 삭제		
관련보안제품 운영현황	웹 방화벽		
그 밖에 사고 관련 내용을 구체적으로 서술			
없음			

가. 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
차	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 타 시스템에 접속한 기록이 발견되었을 경우
B	자료훼손 및 유출	내부 시스템의 자료가 변조가 되었거나, 대량의 데이터가 외부로 무단송신된 흔적이 발견되었을 경우
C	단순침입 시도	지속적인 스캐닝 공격이 발생할 경우
D	웜바이러스 피해	기관내의 PC에서 웜바이러스가 발견되었을 경우
E	홈페이지 변조	기관의 홈페이지가 변조되었을 경우
F	홈페이지 접속 불가능	기관의 홈페이지 서버 또는 네트워크 이상으로 인해 홈페이지 접속이 불가능 할 경우
G	서비스거부공격 피해	불특정 다수의 IP로부터 접속시도 또는 대량 트래픽이 일시에 유입될 경우
H	기타	위의 사고유형에 포함되지 않을 경우 서술식으로 기술

4. 사고조치 서식(실무기관→과학기술정보보호센터→과학기술부)

사 고 조 치

기 본 정 보			
기 관 명		부 서	
성 명		직 위	
전자우편			
연 락 처	전화: Fax:	H.P:	

사 고 내 용			
사고 일시	년 월 일 시 분	피해IP주소	
피해시스템 용도	* 사고신고시와 동일하게 작성	운영체제	□윈도우 □유닉스 □네트워크장비 상세버전정보:
사고 유형	* 사고신고시와 동일하게 작성	피해범위	OO 대 * 피해시스템이 여러대인 경우 피해숫자 기입
사고 내용			

조 치 내 용 요 약	
사고원인	* 자체긴급대응반, 합동조사팀의 사고조사에 대한 내용을 요약 작성
피해현황	* 사고대응 조치 전의 피해현황을 요약 작성
사고대응 조치사항	* 자체 긴급대응반, 복구지원팀의 피해복구 조치에 대한 내용을 요약 작성
피해복구결과	* 사고대응 조치 후의 현황을 요약 작성
* 자세한 사항은 사고원인 · 피해현황 · 조치내역 · 향후 개선대책 등을 망라하여 '사고처리결과보고서' 작성	

※ 이 양식은 과학기술정보보호센터 홈페이지(www.sntsec.or.kr)에서 내려 받을 수 있습니다.

※ Fax 042-869-0809 또는 sntsec@kisti.re.kr로 사고를 신고하시기 바랍니다.

5. 긴급대응반 비상연락망(과학기술부)

과학기술부 긴급대응반 비상연락망

갱신일 : 07.04.16

구성원	상황별 담당자		이 름	연락처
반 장	정보보안담당관		성기억	010-000-1234
기술 전문가	라우터 및 스위치 취약점 발표	네트워크 관리자	김 ○ ○	010-000-1234
	DB 프로그램 취약점 발표	데이터베이스 관리자	김 ○ ○	010-000-1234
	그룹웨어 프로그램 취약점 발표	그룹웨어 관리자	김 ○ ○	010-000-1234
	이메일 필터링 및 점검필요	이메일 시스템 관리자	김 ○ ○	010-000-1234
	홈페이지 및 웹서버 사고빈발	홈페이지 관리자	김 ○ ○	010-000-1234
	특정IP 공격시도 및 탐지이벤트 확인. 정보보안 프로그램 취약점 발표 등	보안시스템 관리자	김 ○ ○ 박 ○ ○	010-000-1234 010-000-1234
	주요 데이터 및 시스템 백업	데이터베이스 관리자 주요 시스템 관리자 백업시스템 관리자	김 ○ ○ 김 ○ ○ 김 ○ ○	010-000-1234 010-000-1234 010-000-1234
	그 외	각 시스템별 관리자	김 ○ ○	010-000-1234
대응 요원	과학기술정보보호센터		김 ○ ○ 김 ○ ○ 김 ○ ○ 김 ○ ○ 김 ○ ○	010-000-1234 010-000-1234 010-000-1234 010-000-1234 010-000-1234

※ 기술전문가는 사이버위협 유형에 따라 선택 구성함

6. 실무기관 비상연락망

과학기술정보보호 대상기관 비상연락망

갱신일 : 07.07.10

구분	기관명	담당부서	담당자	연락처				
				전화번호	FAX	휴대폰번호	전자메일	
과기부 직할 (10)	과학기술부	정보화담당과	심원무	02-2110-3601	02-2110-3609	011-9284-3070	wmsim@most.go.kr	
	한국과학기술원	정보통신팀	노부술	042-869-2419	042-869-2450	010-9678-9878	boosulro@kaist.ac.kr	
			손형탁	042-869-5688	042-869-2450	011-437-9648	cosmos@kaist.ac.kr	
	(부설)고등과학원	학부지원팀	이영진	02-958-3824	02-958-3790	010-3156-8218	yjlee@kias.re.kr	
			최병호	02-958-3771	02-958-3790	016-298-5728	bhchoi@kias.re.kr	
	광주과학기술원	전산팀	이규대	062-970-2071	062-970-2079	010-9451-9071	kdlee@gist.ac.kr	
			박양수	062-970-2076	062-970-2079	011-9614-1729	frog@gist.ac.kr	
	대구경북과학기술원	사업협력실	황규석	053-430-8640	053-430-8669	019-237-2017	sio2@dgist.ac.kr	
			김종배	053-430-8663	053-430-8669	019-891-5650	jerome74@dgist.ac.kr	
	한국과학재단	정보관리팀	여무성	042-869-6700	042-869-6777	010-6376-7163	msyeu@kosef.re.kr	
			채수일	042-869-6709	042-869-6777	011-407-6290	csi0926@kosef.re.kr	
	한국과학기술기획평가원	정보분석팀	김주호	02-589-2957	02-589-2191	011-9885-8090	ahwi@kistep.re.kr	
			배상태	02-589-2876	02-589-2191	016-9626-4370	stbae@kistep.re.kr	
	한국원자력의학원	전산정보팀	민효기	02-970-2027	02-974-4351	011-306-7069	min@kcch.re.kr	
			정재우	02-970-2070	02-974-4351	016-795-9602	jwjung@kcch.re.kr	
	한국원자력안전기술원	지식정보실	정윤형	042-868-0245	042-868-0069	011-787-5884	k078cyh@kins.re.kr	
			진형식	042-868-0522	042-868-0069	016-451-0522	k356jhs@kins.re.kr	
	과학기술연합대학원대학교	교학처	김정흠	042-865-3975	042-864-5554	018-451-7271	kimjh@ust.ac.kr	
			정 윤	042-865-3988	042-864-5554	018-407-6087	haro1033@ust.ac.kr	
	한국원자력통제기술원	정보관리실	신익현	042-866-6691	042-861-8819	019-274-7243	ihshin@kinac.re.kr	
기초 기술 연구회 (7)	기초기술연구회							
	한국과학기술연구원	정보통신담당	강명관	02-958-6284	02-958-6299	011-9704-3612	kmk@kist.re.kr	
			최수용	02-958-6283	02-958-6299	011-721-1374	sychoi@kist.re.kr	
	한국기초과학지원연구원	전산운영팀	민안기	042-865-3570	042-865-3542	017-427-4313	commin@kbsi.re.kr	
			차종환	042-865-3577	042-865-3542	010-2423-0085	snowmir@kbsi.re.kr	
	(부설)핵융합연구센터	지식정보관리팀	고호은	042-710-1826 042-870-1590	042-870-1599	016-595-3216	hyperkhu@nfrc.re.kr	
			이도섭	042-870-1591	042-870-1599	010-3033-8005	netko@nfrc.re.kr	
	(부설)국가수리과학연구소	연구지원실	김병학	042-864-5702	042-864-5706	011-9562-5547	bhkim@khu.ac.kr	
			홍희준	042-864-5705	042-864-5706	010-3455-5205	dono@nims.re.kr	
	한국생명공학연구원	전산정보과	정호석	042-860-4570	042-860-4575	019-472-4572	hsjeong@kribb.re.kr	
			김대겸	042-860-4573	042-860-4575	016-9292-5865	kdkmy@kribb.re.kr	
	한국천문연구원	전산정보팀	신재식	042-865-3208	042-861-5610	016-407-7007	asshin@kasi.re.kr	
			남현웅	042-865-3210	042-861-5610	011-829-2024	hwnam@kasi.re.kr	
	한국한의학연구원	한의학정보화사업단	송미영	042-868-9454	042-861-9421	018-217-2615	smyoung@kiom.re.kr	
			이선우	042-868-9548	042-861-9421	011-439-8820	swlee@kiom.re.kr	
산업 기술 연구회 (8)	산업기술연구회							
	한국전자통신연구원	정보관리팀	진병운	042-860-0740	042-861-1033	010-9557-1754	bwjin@etri.re.kr	
			임정일	042-860-0745	042-861-1033	018-286-1293	jiyim@etri.re.kr	
	(부설)국가보안기술연구소	총무팀	김강섭	042-860-5472	042-860-5656	016-443-8715	kks@etri.re.kr	
			서인석	042-860-1412	042-860-5656	010-9437-3946	isseo@etri.re.kr	
	한국화학연구원	정보전산실	김종한	042-860-7780	042-860-7699	011-429-7050	jhkim@krict.re.kr	
			유영근	042-860-7783	042-860-7699	011-9405-5739	ygyu@krict.re.kr	

	(부설)안전성평가연구소	전산통계팀	나재열	042-610-8161	042-610-8171		jyna@kitox.re.kr	
			박진수	042-610-8165	042-610-8171	010-9977-0122	icemaker@kitox.re.kr	
	한국생산기술연구원	지식정보팀	김기중	041-589-8093	041-589-8099	016-9848-1138	gjkim@kitech.re.kr	
	한국전기연구원	지식정보과	하회두	055-280-1104	055-280-1179	011-818-4150	hdha388@keri.re.kr	
			한옥수	055-280-1178	055-280-1179	018-792-5267	oshan@keri.re.kr	
	한국기계연구원	지식정보팀	이규옥	042-868-7648	042-868-7646	011-9060-7638	kolee@kimm.re.kr	
			신동우	042-868-7638	042-868-7646	011-9811-7638	dwshin@kimm.re.kr	
	한국식품연구원	지식정보팀	김태규	031-780-9252	031-780-9255	010-9133-0391	kfriktg@kfri.re.kr	
			최대관	031-780-9253	031-780-9255	011-9441-9904	spade@kfri.re.kr	
공공기술연구회 (10)	**공공기술연구회**							
	한국과학기술정보연구원	연구망사업팀	이혁로	042-869-0517	042-869-0509	010-3481-4574	leehr@kisti.re.kr	
			이행곤	042-869-0513	042-869-0509	010-3078-0519	hglee@kisti.re.kr	
	한국표준과학연구원	지식정보팀	이상태	042-868-5422	042-868-5423	016-462-0624	stlee@kriss.re.kr	
			민복기	042-868-5427	042-868-5423	010-2845-9507	bkmin@kriss.re.kr	
	한국항공우주연구원	정보지원팀	서광식	042-860-2161	042-860-2169	016-403-5375	ksseo@kari.re.kr	
			배석	042-860-2153	042-860-2169	019-680-8131	sbae@kari.re.kr	
	한국철도기술연구원	정보화팀	문진한	031-460-5142	031-460-5139	010-2016-0678	jhmoon@krri.re.kr	
			이규선	031-460-5144	031-460-5139	011-9942-1189	ksun_lee@krri.re.kr	
			강석주	031-460-5144	031-460-5139	010-2413-5599	sjkang@krri.re.kr	
	한국건설기술연구원	정보전산실	김승균	031-910-0040	031-910-0085	011-9997-9148	skkim@kict.re.kr	
			남기형	031-910-0046	031-910-0085	016-707-2804	khnam@kict.re.kr	
	한국에너지기술연구원	전산관리과	안상규	042-860-3733	042-860-3374	011-773-6180	softahn@kier.re.kr	
			김순환	042-860-3722	042-860-3374	011-536-2241	shkim@kier.re.kr	
	한국지질자원연구원	지식정보과	안창인	042-868-3491	042-861-3280	016-400-1710	anci@kigam.re.kr	
			전상준	042-868-3492	042-861-3280	011-452-0624	sjjeon@kigam.re.kr	
			유민수	042-868-3495	042-861-3280	011-408-8843	ans@kigam.re.kr	
	한국해양연구원	경영정보팀	권순철	031-400-6056	031-406-1647	011-9965-9812	sckwon@kordi.re.kr	
	(부설) 극지연구소	혁신기획팀	진동민	032-260-6040	032-260-6039	011-9737-1611	dmjin@kopri.re.kr	
			이민철	032-260-6014	032-260-6039	011-435-0700	leemc@kopri.re.kr	
	한국원자력연구원	정보통신팀	이해초	042-868-2095	042-861-9315	010-6488-2095	hclee@kaeri.re.kr	
			황혜선	042-868-8796	042-861-9315	010-7676-9552	hyeseon@kaeri.re.kr	
산하기관 및 단체 (3)	**산하기관 및 단체**							
	한국과학문화재단	경영지원실	윤승재	02-559-3866	02-555-0702	011-9088-5546	pulse@ksf.or.kr	
			김진만	02-559-3829	02-555-0702	019-337-2985	funnyman@ksf.or.kr	
	한국과학기술단체총연합회	정책조사팀	윤호식	02-3420-1221	02-553-2170	011-9094-8121	hsyoun@kofst.or.kr	
			김선일	02-3420-1223	02-553-2170	017-311-2617	kofst@kofst.or.kr	
	한국산업기술진흥협회	전산정보팀	한성희	02-3460-9161	02-3460-9116,7	017-396-8133	shhan@koita.or.kr	
			배재기	02-3460-9162	02-3460-9169	017-306-7215	jgbae@koita.or.kr	

구분	기관명	담당부서	담당자	연락처				
				전화번호	FAX	휴대폰번호	전자메일	
산업기술연구회(8)	**산업기술연구회**							
	한국전자통신연구원	정보관리팀	진병운	042-860-0740	042-861-1033	010-9557-1754	bwjin@etri.re.kr	
			임정일	042-860-0745	042-861-1033	018-286-1293	jiyim@etri.re.kr	
	(부설)국가보안기술연구소	총무팀	김강섭	042-860-5472	042-860-5656	016-443-8715	kks@etri.re.kr	
			서인석	042-860-1412	042-860-5656	010-9437-3946	isseo@etri.re.kr	
	한국화학연구원	정보전산실	김종한	042-860-7780	042-860-7699	011-429-7050	jhkim@krict.re.kr	
			유영근	042-860-7783	042-860-7699	011-9405-5739	ygyu@krict.re.kr	
	(부설)안전성평가연구소	전산통계팀	서정은	042-610-8160	042-610-8171	016-426-5509	jesuh@kitox.re.kr	
			박진수	042-610-8165	042-610-8171	010-9977-0122	icemaker@kitox.re.kr	
	한국생산기술연구원	지식정보팀	김기중	041-589-8093	041-589-8099	016-9848-1138	gjkim@kitech.re.kr	
	한국전기연구원	지식정보과	하회두	055-280-1104	055-280-1179	011-818-4150	hdha388@keri.re.kr	
			한옥수	055-280-1178	055-280-1179	018-792-5267	oshan@keri.re.kr	
	한국기계연구원	지식정보팀	이규옥	042-868-7648	042-868-7646	011-9060-7638	kolee@kimm.re.kr	
			신동우	042-868-7638	042-868-7646	011-9811-7638	dwshin@kimm.re.kr	
	한국식품연구원	지식정보팀	김태규	031-780-9252	031-780-9255	010-9133-0391	kfriktg@kfri.re.kr	
			최대관	031-780-9253	031-780-9255	011-9441-9904	spade@kfri.re.kr	
공공기술연구회(9)	**공공기술연구회**							
	한국과학기술정보연구원	연구망사업팀	이혁로	042-869-0517	042-869-0509	010-3481-4574	leehr@kisti.re.kr	
			이행곤	042-869-0513	042-869-0509	010-3078-0519	hglee@kisti.re.kr	
	한국표준과학연구원	지식정보팀	이상태	042-868-5422	042-868-5423	016-462-0624	stlee@kriss.re.kr	
			민복기	042-868-5427	042-868-5423	010-2845-9507	bkmin@kriss.re.kr	
	한국항공우주연구원	정보지원팀	서광식	042-860-2161	042-860-2169	016-403-5375	ksseo@kari.re.kr	
			배석	042-860-2153	042-860-2169	019-680-8131	sbae@kari.re.kr	
	한국철도기술연구원	정보화팀	문진한	031-460-5142	031-460-5139	010-2016-0678	jhmoon@krri.re.kr	
			이규선	031-460-5144	031-460-5139	011-9942-1189	ksun_lee@krri.re.kr	
			강석주	031-460-5144	031-460-5139	010-2413-5599	sjkang@krri.re.kr	
	한국건설기술연구원	정보전산실	김승균	031-910-0040	031-910-0085	011-9997-9148	skkim@kict.re.kr	
			남기형	031-910-0046	031-910-0085	016-707-2804	khnam@kict.re.kr	
	한국에너지기술연구원	전산관리과	안상규	042-860-3733	042-860-3374	011-773-6180	softahn@kier.re.kr	
			김순환	042-860-3722	042-860-3374	011-536-2241	shkim@kier.re.kr	
	한국지질자원연구원	지식정보과	안창인	042-868-3491	042-861-3280	016-400-1710	anci@kigam.re.kr	
			전상준	042-868-3492	042-861-3280	011-452-0624	sjjeon@kigam.re.kr	
			유민수	042-868-3495	042-861-3280	011-408-8843	ans@kigam.re.kr	
	한국해양연구원	경영정보팀	권순철	031-400-6056	031-406-1647	011-9965-9812	sckwon@kordi.re.kr	
	(부설) 극지연구소	혁신기획팀	진동민	032-260-6040	032-260-6039	011-9737-1611	dmjin@kopri.re.kr	
			이민철	032-260-6014	032-260-6039	011-435-0700	leemc@kopri.re.kr	
산하기관 및 단체(3)	**산하기관 및 단체**							
	한국과학문화재단	경영지원실	윤승재	02-559-3866	02-555-0702	011-9088-5546	pulse@ksf.or.kr	
			김진만	02-559-3829	02-555-0702	019-337-2985	funnyman@ksf.or.kr	
	한국과학기술단체총연합회	정책조사팀	윤호식	02-3420-1221	02-553-2170	011-9094-8121	hsyoun@kofst.or.kr	
			김선일	02-3420-1223	02-553-2170	017-311-2617	kofst@kofst.or.kr	
	한국산업기술진흥협회	전산정보팀	한성희	02-3460-9161	02-3460-9116,7	017-396-8133	shhan@koita.or.kr	
			배재기	02-3460-9162	02-3460-9169	017-306-7215	jgbae@koita.or.kr	

7. 자체대응반 비상연락망(실무기관)

실무기관 자체대응반 비상연락망

갱신일 : 07.04.16

구성원	상황별 담당자		이 름	연락처
반 장	정보전산실 팀장		김 ○ ○	010-000-1234
기술 전문가	라우터 및 스위치 취약점 발표	네트워크 관리자	김 ○ ○	010-000-1234
	DB 프로그램 취약점 발표	데이터베이스 관리자	김 ○ ○	010-000-1234
	그룹웨어 프로그램 취약점 발표	그룹웨어 관리자	김 ○ ○	010-000-1234
	이메일 필터링 및 점검필요	이메일 시스템 관리자	김 ○ ○	010-000-1234
	홈페이지 및 웹서버 사고빈발	홈페이지 관리자	김 ○ ○	010-000-1234
	특정IP 공격시도 및 탐지이벤트 확인. 정보보안 프로그램 취약점 발표 등	보안시스템 관리자	김 ○ ○ 박 ○ ○	010-000-1234 010-000-1234
	주요 데이터 및 시스템 백업	데이터베이스 관리자 주요 시스템 관리자 백업시스템 관리자	김 ○ ○ 김 ○ ○ 김 ○ ○	010-000-1234 010-000-1234 010-000-1234
	그 외	각 시스템별 관리자	김 ○ ○	010-000-1234
관계기관 연락처	과학기술부		김 ○ ○ 김 ○ ○ 김 ○ ○	010-000-1234 010-000-1234 010-000-1234
	과학기술정보보호센터		김 ○ ○ 김 ○ ○ 김 ○ ○	010-000-1234 010-000-1234 010-000-1234

※ 기술전문가는 사이버위협 유형에 따라 선택 구성함

8. 사이버안전 유관기관 비상연락망

사이버안전 유관기관 비상연락망

갱신일 : 07.04.16

구분	기관명	연락처	홈페이지
공공 분야	과학기술부 과학기술정보보호센터	042-869-0808	www.sntsec.re.kr
	외교통상부	02-3703-2114	www.mofat.go.kr
	법무부	02-503-7023	www.moj.go.kr
	행정자치부 전자정부본부	02-3703-3287	www.mogaha.go.kr
	한국전산원 통합위탁운영팀	02-2131-0758	www.nca.or.kr
	국가보안기술연구소	042-864-5030	www.nsri.re.kr
국방 분야	국방 CERT (국군통신사령부 CERT상황팀)	02-748-0896	-
	기무사 국방정보전대응센터	02-731-0118	www.dsc.mil.kr
수사	대검찰청 인터넷범죄수사센터	02-3480-3600	www.spo.go.kr
	경찰청 사이버테러대응센터	02-3939-112	www.ctrc.go.kr
민간 분야	증권 ISAC	02-767-7285(주) 02-767-7381(야)	www.koscomisac.co.kr
	금융 ISAC	02-531-1623	www.kftc.or.kr
	통신 ISAC	02-405-5651	www.tisac.or.kr
	인터넷침해사고대응지원센터	02-405-5114	www.krcert.or.kr
	안철수연구소(A-SEC)	02-2186-7930	www.ahnlab.co.kr
	하우리	02-828-0850	www.hauri.co.kr

9. 정보시스템 협력업체 연락처

정보시스템 협력업체 연락처

갱신일 : 07.04.16

구분	업체명	담당자명	연락처	비고
정보보호시스템	정보보호기술	김 ○ ○	010-000-1234 02-222-3456	
	기타	김 ○ ○	010-000-1234 02-222-3456	
네트워크 장비	시스코	김 ○ ○	010-000-1234 02-222-3456	
	쌍용정보통신	김 ○ ○	010-000-1234 02-222-3456	
	기타	김 ○ ○	010-000-1234 02-222-3456	
백신업체	안철수	김 ○ ○	010-000-1234 02-222-3456	
	하우리	김 ○ ○	010-000-1234 02-222-3456	
	기타	김 ○ ○	010-000-1234 02-222-3456	
시스템 및 소프트웨어	마이크로소프트	김 ○ ○	010-000-1234 02-222-3456	
	하우리	김 ○ ○	010-000-1234 02-222-3456	
	기타	김 ○ ○	010-000-1234 02-222-3456	
회선사업자	KT	김 ○ ○	010-000-1234 02-222-3456	
	하나로텔레콤	김 ○ ○	010-000-1234 02-222-3456	
	기타	김 ○ ○	010-000-1234 02-222-3456	

10. 피해기관 종합 목록표

과학기술분야 피해기관 종합 목록표

갱신일 : 07.04.16

기관명	정보통신망 중요도	지원형태			우선순위	처리결과
		현장출동	원격복구	현장·원격		
○○연구소	B		○		하	완료

※ 정보통신망 중요도는 국가사이버안전매뉴얼 보안관리수준평가를 참조(p74)

※ 우선순위는 상-중-하로 구분함

11. 피해현황표 Ⅰ(사고건수)

과학기술분야 피해현황표 Ⅰ

갱신일 : 07.04.16

기 관 명	구 분	사고건수	피해현황	기밀유출
○○○연구소	본원			
	분원(서울)			
총 계				

12. 피해현황표 II (유해트래픽, 악성이벤트 탐지현황)

과학기술분야 피해현황표 II

갱신일 : 07.04.16

기 관 명	전체트래픽	특정Port 트래픽	이벤트 변화량	비고
○○○연구소				

※ 기준시간은 24시간 이전대비 변화량을 측정(상황에 따라 조정)

※ 부문별 보안관제를 수행하는 기관은 지속적으로 추가

13. 피해현황표 Ⅲ (특정IP 흔적 및 백신탐지 기록)

과학기술분야 피해현황표 Ⅲ

갱신일 : 07.04.16

기관명	구 분	공격IP	특정 Port	백신 탐지명	이메일 수신여부
○○○연구소	본원				
	분원(서울)				
총 계					

※ 기관단위로 피해증상 파악시 활용

실무기관 사이버안전분야 위기대응 실무매뉴얼 작성 요령

Ⅰ. 일반사항

1. 개요

o 실무기관의 사이버안전 분야 위기대응 실무 매뉴얼 작성 개요에 맞추어 간략히 작성

2. 적용범위

o 사이버안전 분야 위기대응 실무 매뉴얼의 적용범위를 기술

3. 용어정의

Ⅱ. 위기관리 활동

1. 예방

o 실무기관은 평시 사이버 위협에 대한 자체 위기관리 예방활동을 체계적으로 구축하기 위해 아래와 같은 중점사항에 대한 세부 활동내역을 실무기관의 실정에 맞게 작성하고 이행

(1) 실무기관의 실정에 맞는 사이버 안전대책 수립·시행

(2) 위기징후 실시간 감시 방안

(3) 연구기반시설 및 정보통신기반시설에 대한 안정성 확인 방안

(4) 과학기술정보보호센터와 정보공유체제 구축

2. 대비

o 실무기관은 사이버 위협에 대한 대비체제를 구축하기 위해 아래와 같은 중점사항에 대한 세부 활동내역 및 위기경보 수준별 관리자·실무자의 책임/역할을 실무기관의 실정에 맞게 작성하고 이행

(1) 위기경보 발령시 전파 방안

(2) 위기대응 능력 강화 방안

(3) 사이버안전에 대한 교육 및 인식 제고 방안

(4) 사이버안전 분야 위기관리 훈련/연습 방안

(5) 위기상황 대비 Backup 및 대응책 강구

3. 대응

o 실무기관은 사이버 공격에 의한 사고 발생이나, 피해발생시 즉각 대응하기 위한 체제를 구축하기 위해 아래와 같은 중점사항에 대한 세부 활동내역을 실무기관의 실정에 맞게 작성하고 이행

(1)「자체대응반」에 의한 신속한 대응 조치 방안 및 과학기술정보보호센터 및 과학기술부 등 비상연락체계 구축

※ 과학기술부 사이버분야 위기대응 실무 매뉴얼 부록 1.「사고조사 및 복구」참조

4. 복구

o 실무기관은 사이버 공격으로 인해 사고 발생이나 피해발생시 피해의 규모를 판단하여 자체복구 방안을 마련하고 과학기술부 및 과학기술정보보호센터와 긴밀한 협조를 통해 복구 체제를 구축하기 위해 아래와 같은 중점사항에 대한 세부 활동내역을 실무기관의 실정에 맞게 작성하고 이행

(1) 복구절차에 따른 피해복구 수행 방안

(2) 사고재발 방지를 위한 보안대책 수립 및 시스템 개선 방안

※ 과학기술부 사이버분야 위기대응 실무 매뉴얼 부록 1.「사고조사 및 복구」참조

Ⅲ. 위기관리 수행업무 체계

1. 위기대응 체계

o 실무기관은 위기경보에 따른 기관내 정보보호관리자, 시스템 및 네트워크 관리자 등을 중심으로 위기대응 체계를 구축

2. 위기대응 기구(자체대응반)

o 실무기관은 위기경보에 따른 기관내 정보보호관리자, 시스템 및 네트워크 관리자 등으로 편성된 자체대응반을 구성하고 각각의 세부 역할을 기술

Ⅳ. 위기경보 수준별 대응요령

1. 예방활동

(1) 실무기관은 자체 안전대책을 수립하여 시행

※ 국가사이버안전매뉴얼 부록 1.「평시 안전점검 체크리스트」를 기관의 실정에 맞게 작성·시행

(2) 정보통신망에 대한 안전대책에 따른 정기적 점검 실시 계획 수립

(3) 위협정보 전파시 대응책 마련 및 사이버 위협 인지 또는 발생시 신고 및 초동조치 방안 마련

(4) 정보통신망에 대한 보안성 검토 및 보안측정 방안마련

※ 보안성 검토 및 보안측정은 「국가정보보안기본지침」참조

(5) 사이버안전에 대한 교육·홍보 및 훈련 등 계획수립

(6) 기본점검 활동 수립(정기점검, 동향파악 등)

2. 관심

o 관심 경보에 대한 실무기관의 대응요령 수립

※ 과학기술부「사이버분야 위기대응 실무 매뉴얼」및「국가사이버안전매뉴얼」 참조

3. 주의

o 주의 경보에 대한 실무기관의 대응요령 수립

※ 과학기술부「사이버분야 위기대응 실무 매뉴얼」및「국가사이버안전매뉴얼」 참조

4. 경계

o 경계 경보에 대한 실무기관의 대응요령 수립

※ 과학기술부「사이버분야 위기대응 실무 매뉴얼」및「국가사이버안전매뉴얼」 참조

5. 심각

o 심각 경보에 대한 실무기관의 대응요령 수립

※ 과학기술부「사이버분야 위기대응 실무 매뉴얼」및「국가사이버안전매뉴얼」 참조

실무기관별 사이버분야 위기대응 실무 매뉴얼 작성은 실무기관의 사이버안전대책을 수립하는 것으로 사이버안전대책 수립·시행할 경우에는 과학기술부에 1부를 통보하여야 한다.

과학기술부 사이버안전 분야 위기대응 실무 매뉴얼(http://www.sntnet.or.kr)을 바탕으로 실무기관의 실정에 맞게 수립하여야 한다.

국가사이버안전매뉴얼(http://www.ncsc.go.kr) 또는 사이버안전 분야 위기관리 표준매뉴얼 등을 참조.