

사이버위기 대응 실무 매뉴얼

2020. 12.

목 차

I . 일반사항	1
II . 침해사고 대응	3
III . 침해사고 예방	5
IV . 침해사고 정보관리	6
V . 사이버위기 대응	7
<참고 1> 사이버침해 대비 비상연락체계	13
<참고 2> 침해사고 종류별 기술적 대응 요령	16
<참고 3> 침해사고 발생 시 시스템 분석 방법	18
<참고 4> 시스템 복구 우선순위	19
<참고 5> 피해수준별 복구방법	19
<참고 6> 침해사고 대응 시나리오별 대응절차	20
<기타서식>	23

I. 일반사항

1. 목적

- 해킹·웜바이러스 유포 등 사이버공격에 한국환경정책·평가연구원(이하 연구원)이 효율적으로 대응하기 위한 대응절차와 조치사항을 규정

2. 관련 법규 등 규정

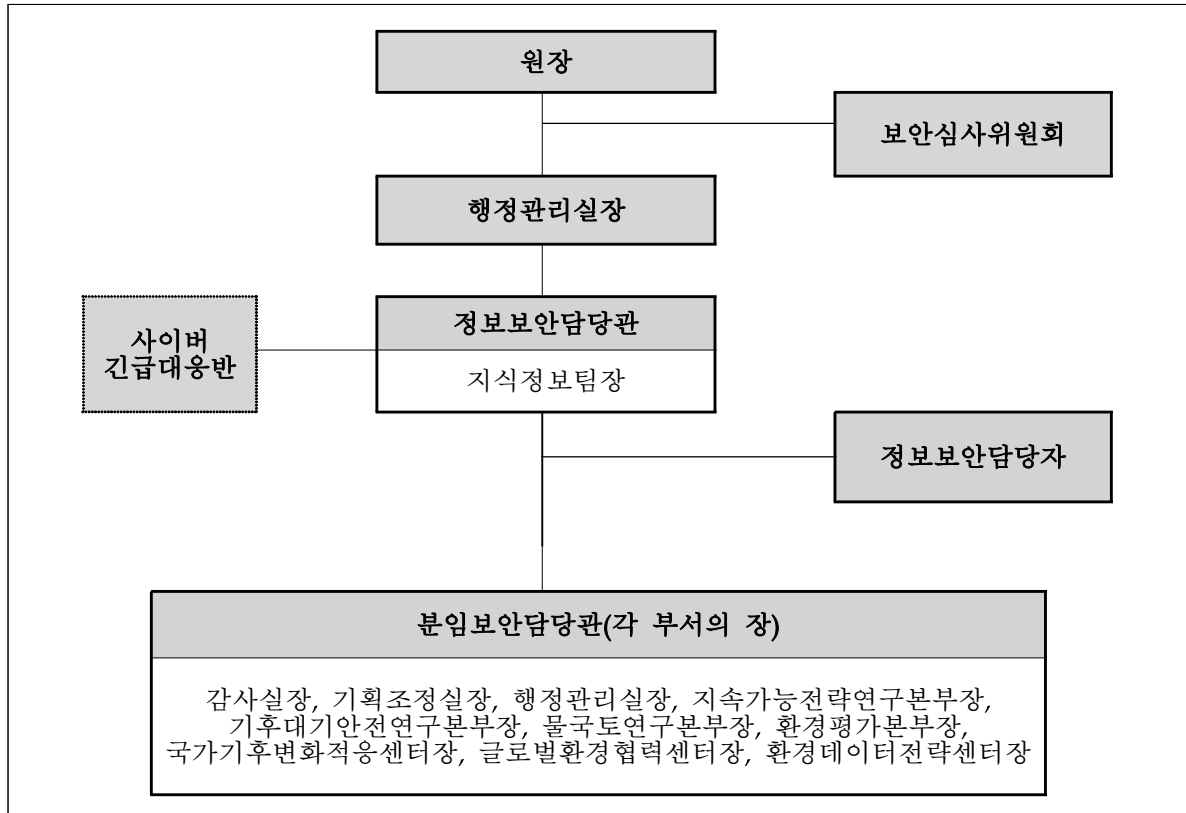
- 「국가위기관리기본지침」 (대통령훈령 제318호)
- 「국가사이버안전관리규정」 (대통령훈령 제316호)
- 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 (법률 제14080호)
- 「정보통신기반보호법」 (법률 제13343호)
- 「전자정부법」 (법률 제13459호)
- 「국가정보화기본법」 (법률 제13340호)
- 「보안업무규정」 (대통령령 제26140호)
- 「개인정보 안정성 확보조치 기준」 (행정안전부고시 제2019-47호)
- 「사이버분야 위기관리 표준매뉴얼」 (국가정보원, '13.7.29)
- 「사이버(국가·공공)분야 위기대응 실무매뉴얼」 (국가정보원, '17.1.1)
- 「국무조정실·국무총리비서실 정보보안 기본지침」 (국무조정실, '19.12.26)
- 「국가 정보보안 기본지침」 (국가정보원, '20.7.1)
- 「사이버위기대응 실무 매뉴얼」 (국무조정실, '17.2)
- 「전산보안업무규칙」 (KEI, '17.12.18)
- 「정보시스템 긴급 재난복구 계획(안)」 (KEI, '20.6.15)
- 「개인정보 침해대응 절차서」 (KEI, '20.6.30)
- 「재해·재난 대비 개인정보처리시스템 위기대응 매뉴얼」 (KEI, '20.6)

3. 적용범위

- 해킹, 웜·바이러스 유포 등 사이버공격으로 인한 중요자료 유출 등 사이버위기상황 발생 및 국무조정실 사이버위기 대응활동 시 적용

4. 정보보호 조직체계

○ 정보보안관리 조직도



- 분임보안담당관은 각 본부·실·센터의 장으로 임명, 부서의 정보 보안 업무 수행
- 정보보안담당관은 지식정보팀장으로 임명, 부서 1인을 정보보안 담당자로 임명하고 정보보안 총괄업무 수행
- 정보보안담당관은 사이버긴급대응반을 구성·운영
- 원장 직속으로 보안심사위원회를 구성·운영, 보안심사위원회는 연구운영회의를 같음하며 간사는 지식정보팀장이 수행

II. 침해사고 대응

1. 침해사고의 범위

가. 침해사고의 정의

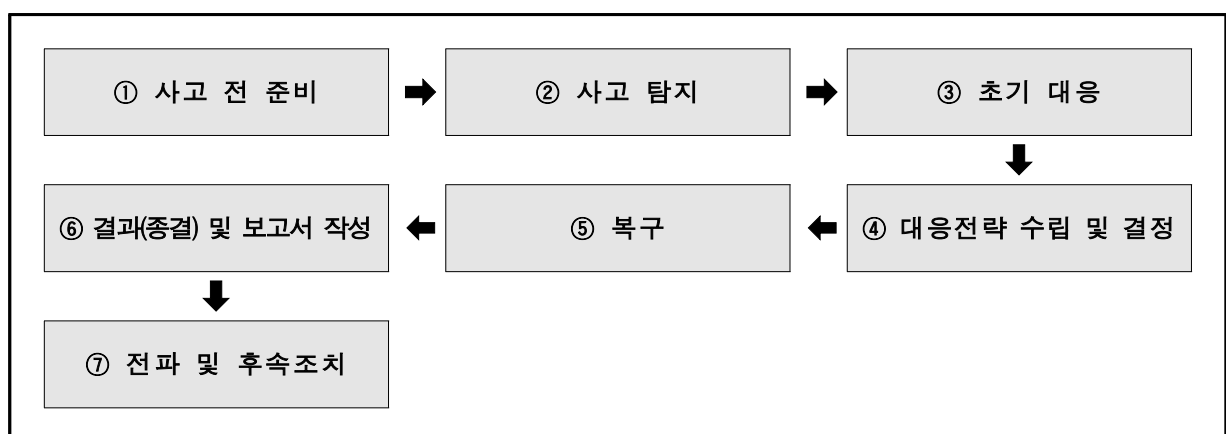
- 정보시스템에 대한 비 인가된 행위 또는 위협
 - 비인가 된 시스템 사용 또는 사용자의 계정 도용, 악성코드 유입 및 실행, 정보서비스의 방해 등
 - 국무조정실 보안정책에 위반되는 행위 포함 등

나. 침해사고의 종류(기술적 대응 요령은 참고2 참조)

- 악성 프로그램(코드)
- 서비스 거부(DoS, Denial of Service)
- 시스템 침입(비인가 된 접근)
- 오남용(비인가 된 사용)
- 정보수집 및 보안정책 위반

2. 침해사고 대응 절차

가. 침해사고 대응절차도



① 사고 전 준비

- (공통) PC, 서버 등의 시스템에 대한 항시 안전(점검 등)을 유지하고 정보보안조직도에 따라 대응체계 구축

② 사고 탐지

- (탐지자) 이상징후 탐지 즉시 정보보안담당자에게 통보
- (정보보안담당자) 침해사고 유형 및 위험도에 따라 수사기관 신고여부 판단 후 정보보안담당관 보고
- (정보보안담당관) 정보보안담당자 보고 내용 확인 후 수사기관 신고여부 결정

③ 초기 대응

- (탐지자) 피해 시스템(서버, 업무용PC 등) 네트워크 분리
- (정보보안담당자) 사고 증거 확보 및 보존, 시스템 격리 조치

④ 대응전략 수립 및 결정

- (정보보안담당자) 사고발생지 차단 및 확인, 기밀자료 유출 여부 확인 및 회수 등 사고원인 및 범위, 목적 분석
 - * 상위기관(국무조정실, 국가사이버안전센터 등) 및 유지보수 업체와 공조하여 분석
- (정보보안담당관) 사고 위험도 및 영향도에 따라 조치방안을 결정, 필요 시 상위기관에 사고경위 등에 대한 정보 제공
 - * 사고유형에 따라 법·규정을 준수하여 업무연속성 및 기술적 여건 등을 고려하여 결정

⑤ 복구

- (정보보안담당자 및 담당관)
 - 위험 우선순위(참고 4)에 따라 복구시스템 분별
 - 시스템별 피해범위에 따라 침해시스템 복구(참고 5)
 - 네트워크 및 호스트의 취약점 발견 시 조치(침입탐지시스템, 방화벽 등을 통한 패킷 통제 및 접근통제)를 실시하여 추가적인 피해 및 재발 방지

⑥ 결과(종결) 및 보고서 작성

- (정보보안담당자 및 담당관)

- 사고조치 결과 보고서(서식2) 및 피해복구 보고서 작성
- 사고 원인분석을 통해 도출된 취약점을 파악하여 개선대책 마련
- 시스템 재개 후 모니터링을 수행하며, 유사사고·침해 징후가 없는 경우 종결 처리(필요 시 상위기관 협의)

⑦ 전파 및 후속조치

- (정보보안담당자 및 담당관) 보안취약점에 대한 개선대책 등을 보고 후, 기관 내 전파

III. 침해사고 예방

1. 관리적 예방

가. 보안강화 협조 공지

- 국무조정실, 국가사이버안전센터, 연구회 사이버보안 관제센터 등에서 공지한 보안강화 협조 공지
- 보안 이슈 발생 시 관련 내용 공지를 통한 내부 직원 전파

나. 업무용 전산기기 보안 강화

- 내실있는 '사이버보안진단의 날' 운영을 통해 PC 등 업무용 전산기기 보안강화

2. 기술적 예방

가. 사이버위기 대응 모의훈련 등 실시

- 직원의 위기대응능력과 보안의식 제고를 위해 모의훈련 실시
- 웹서비스 취약점 점검을 통해 안정적인 시스템 운영환경 마련

나. 정보보안 인프라 강화

- 정보시스템·정보보호시스템 보안패치 및 취약점 제거

- 백신, PMS, 내PC지키미, NAC, 보안USB, 개인정보보호SW, PC스캔 등 사용자 PC 보안 관리 철저

3. 인적 예방

가. 정보보안 교육 내실화

- 전 직원 대상 정보보안 집합교육 실시
- 맞춤형(신규직원, 정보화 용역사업 담당자(책임자) 등) 정보보안 교육 실시

IV. 침해사고 정보관리

1. 정보공개 정책

가. 침해사고와 관련된 모든 정보는 타인 혹은 타기관에 유출되지 않도록 함

나. 기관 내 정보공개 정책

- 부서 및 관련기관 침해사고 정보 공유
- 국가사이버안전센터 등 접수한 사고는 관련기관에만 정보 전달
- 타 기관에서 제공받은 정보는 명시적 “공개” 정보 이외는 비공개

2. 기록 및 파기

가. 침해사고 관련 정보는 기록·저장하고 문서 보관

- 저장된 정보는 일/월단위로 백업 저장하여 별도 보관하여야 하며, 백업본의 소산을 통하여 도난 및 재해 대비

나. 침해사고 관련 정보 파기 방법

- 파기 대상 문서는 반드시 문서 세단기를 이용하여 파기
- CD 등의 이동식 저장매체의 경우 데이터 삭제 및 물리적 파쇄를

통하여 복구 불가 상태로 파기

V. 사이버위기 대응

1. 적용범위

- 가. 웹·바이러스, 해킹 등 사이버공격으로 인한 정보통신망 마비, 기밀 자료·중요자료 유출 등 위기상황 발생 시 적용
- 나. 해킹프로그램이 은닉된 E-Mail 유포, 해커조직 공격으로 인해 홈페이지가 대량 변조되어 사회혼란 야기 및 대외 신인도 하락 등의 피해양상 발생 시 적용

2. 위기 형태 및 피해 양상

가. 위기 형태

- 인터넷을 통해 업무용 전산망에 직접 침투
- 홈페이지·메신저·전자우편 등 활용, 악성코드 유포
- 대규모 봇넷(Botnet) 구축, 광범위한 서비스 거부 공격

* 봇넷(Botnet) : 악성 봇에 감염되어 해커에 제어당하는 시스템으로 구성된 네트워크

나. 피해 양상

- 전력·물류·교통·금융 등 주요 정보통신기반시설 마비, 사회혼란 조장 및 국가 경제 타격, 민원·행정서비스 마비, 국민생활 불편 및 정부불신 초래
- 국가기밀 유출, 안보 공백, 외교분쟁 야기

3. 사이버위기 경보 수준

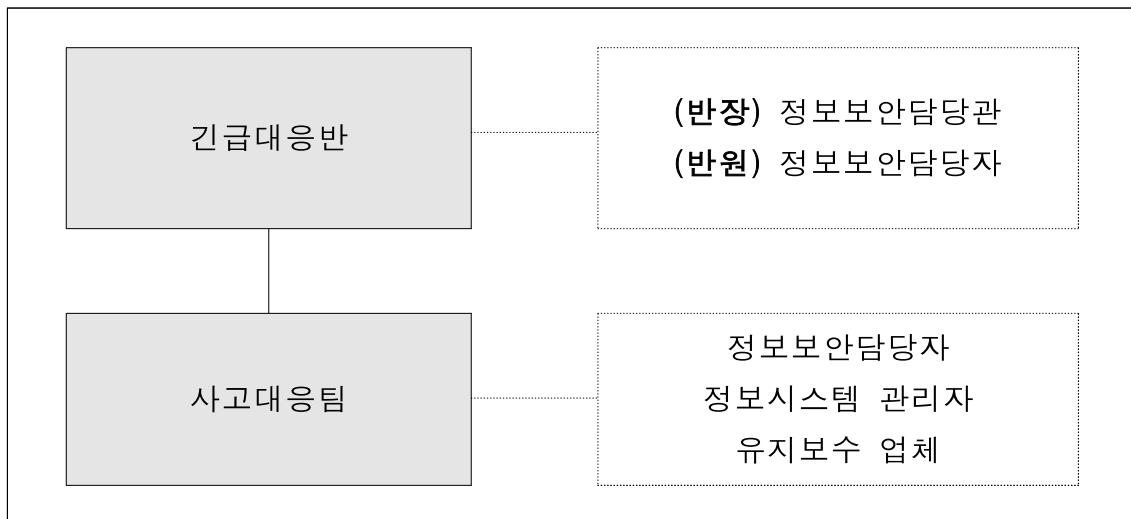
구 분	판단기준	역 할
관심 (Blue)	<ul style="list-style-type: none"> · 위험도가 높은 웜·바이러스, 취약점 및 해킹 기법 출현으로 발생 가능성 증가 · 해외 사이버공격 피해가 확산되어 국내 유입 우려 · 국내·외 정치·군사적 위기상황 조성 등 사이버위협 징후 탐지활동 강화필요 	징후 활동 감시
주의 (Yellow)	<ul style="list-style-type: none"> · 일부 정보통신망 및 정보시스템 장애 · 침해사고가 일부기관에서 발생했거나 다수기관으로 확산될 가능성 증가 · 국가 정보통신기반시설 전반에 보안태세 강화 필요 · 국내·외 정치·군사적 위기발생 등 사이버안보 위해 가능성 고조 	협조체제 가동
경계 (Orange)	<ul style="list-style-type: none"> · 복수 정보통신서비스 제공자(ISP망)·기간통신망에 장애 또는 마비 · 침해사고가 다수 기관에서 발생했거나 대규모 피해로 발전될 가능성 증가 · 다수 기관의 공조 대응 필요 	대비계획 점검
심각 (Red)	<ul style="list-style-type: none"> · 국가 차원의 중요 정보통신망 및 정보통신기반시설 운영 마비 · 침해사고가 전국적으로 발생했거나 피해범위가 대규모인 사고발생 · 국가적 차원에서 총력 대처 필요 	즉각 대응태세 돌입

* 위험 정도가 낮은 웜·바이러스, 해킹기법, 보안취약점이 발견된 경우는 위기경보 이전 단계인 ‘정상(Green)’ 수준으로 간주

4. 위기대응 체계

가. 긴급대응반 구성

- ‘경계’ 이상의 정보 발령 또는 상황에 따라 대응반 구성·운영
- 평시에 정보보안담당관(지식정보팀장)을 긴급대응반장으로 하는 대응반 편성
- 긴급대응반 편성 인원에 대한 비상연락망 유지[참고 1]



<긴급대응반 구성>

나. 주요 임무

- 사이버 공격으로 인한 사고 발생 또는 징후 발견 시 피해 최소화
- 정보발령에 따른 대응 조치 수행
- 사고에 대한 대응책 마련, 기관 내부에 공지 등 전파
- 사고에 대한 증거확보 및 보존
- 유관기관과 긴밀한 협조체계 유지

다. 긴급대응반 역할

구 성	담 당	역 할
긴급대응반장	지식정보팀장	<ul style="list-style-type: none"> · 긴급대응반 운영 총괄 · 긴급대응반 소집 · 상황판 운영 · 대응계획 수립 및 대응결과 종합 · 피해복구계획 수립 및 복구현황 점검
사고대응팀	정보보안담당	<ul style="list-style-type: none"> · 피해상황 접수 및 초동조치 지원 등 사고 대응 · 주요 운영사이트 모니터링 · 스위치 등 네트워크 장비 보안강화 · 정보보호시스템 등을 활용, 공격차단 · 사이버위기 경보 수신시 기관내 전파 · 국정원, 국무조정실, 관제센터 등에 상황전파
	정보시스템관리자	<ul style="list-style-type: none"> · 각 시스템 보안패치 및 PC 백신 업데이트 · 네트워크 이상징후 탐지 · 신고 및 초동조치
	유지보수 업체	<ul style="list-style-type: none"> · 피해시스템 내 악성코드 샘플 채취 · 피해분석을 위한 시스템 보존 및 분석 · 피해시스템 증거 보존

5. 위기경보 수준별 조치사항

가. **관심**

- (반장) 긴급대응반 점검 총괄
- (정보보안담당자)
 - 사고인지 시 국무조정실(필요 시 국가정보원)에 통보
 - 기관 내부에 '관심' 정보 전파
 - 긴급대응반 최신 비상연락체계 점검
 - 조치결과 국무조정실에 통보
 - 시스템 유지보수 업체 연락체계 점검
 - 정보보호시스템 등 주요 시스템 모니터링 강화
 - 백업시스템 정상 작동 확인
- (정보시스템 관리자)
 - 사이버공격으로 인한 피해발생 여부 점검 및 위기징후 감시 강화
 - 새로운 보안취약점 및 해킹수법에 대비, 보안패치 및 백신 업데이트
 - 불필요한 접속, 시스템 위·변조, 접근 차단설정 등 침해 위협에 대한 시스템 모니터링 강화
 - 사고인지 시 정보보안담당자에게 신고
- (직원)
 - PC에 대한 침해시도, 해킹 등 인지 시 정보보안담당자에게 신고
 - 출처가 불분명한 이메일 수신 확인 및 열람 금지
 - PC내 공유폴더 금지

나. **주의** * 관심 단계의 대응조치 지속

- (반장) 긴급대응반 가동 준비
- (정보보안담당자)
 - 기관 내부 '주의' 정보 전파
 - 국가사이버안전센터 등의 사이버공격 분석정보에 따라 공격예상

시스템 대상 보안관리 강화

- 해킹프로그램(해킹메일·악성코드 등) 예상 유입경로 차단
- 가용가능 모든 보안시스템 설치 가동
- 유사시 신속한 전산망 복구·정상화를 위해 비상백업 및 복구 체계 점검

다. **경 계** * 주의 단계의 대응조치 지속

○ (반장) 긴급대응반 가동 및 소집, 상황판 운영

○ (정보보안담당자)

- 기관내부 '경계' 경보 전파
- 주요 정보시스템 및 데이터 백업 실시
- 피해 가능성이 높은 네트워크 단절 검토 및 비상복구체계 가동 준비
- 유지보수 업체 비상대기 요청 및 확인
- 주관기관의 상황전파 내용 이행 여부 재확인
- 사이버공격 유형에 따른 공격차단대책 확인

라. **심 각** * 경계 단계의 대응조치 지속

○ (반장) 비상대응 태세 돌입, 비상대응 결과 및 피해복구 현황 점검

○ (정보보안담당자)

- 기관내부 '심각' 경보 전파
- 기관 내 PC 사용 최소화 및 오프라인 업무 권고
- 피해발생 가능성이 높은 네트워크 연결 차단
- 백업시스템 등을 이용한 비상 복구체계 가동

참고 1

사이버침해 대비 비상연락체계

□ 분임보안담당관

[2020.11. 기준]

구 분		구 성	비 고
1	보 안 담당관	행정관리실장 김용구	
2	일반보안 담당관	총무인사팀장 이영순	
3	정보보안 담당관	지식정보팀장 천재홍	
4	정보보안 담당자	지식정보팀 양준모	
5	분임보안 담당관	감사실장 정태영	
6		기획조정실장 강형식	
7		지속가능전략연구본부장 안소은	
8		기후대기안전연구본부장 채여라	
9		물국토연구본부장 김익재	
10		국가기후변화적응센터장 장훈	
11		환경평가본부장 문난경	
12		행정관리실장 김용구	
13		환경데이터전략센터장 이명진	
14		글로벌환경협력센터장 이현우	

「보안관리규정」 제7조(보안담당관, 분임보안담당관, 정보보안담당관, 방첩업무담당관 임명) :

①보안관련 부서장은 연구원의 보안담당관 및 방첩업무담당관, 각 부서의 장은 보직과 동시에 그 부서의 분임 보안담당관이 된다.

②효율적인 정보보안업무 수행을 위하여 정보화부서 책임자가 정보보안담당관이 되며, 정보보안담당관 업무를 보좌하기 위하여 정보화부서를 정보보안업무 전담부서로 하며, 소속원 1명을 정보보안담당자에 보한다.

□ 긴급대응반

[2020.12. 기준]

구 성	담 당	소 속	이 름	연 락 처
긴급대응반장	총괄	지식정보팀	천재홍	044-415-7406
사고대응팀	정보보안담당	지식정보팀	양준모	044-415-7466
	정보시스템관리자	지식정보팀	김영인	044-415-7602
	유지보수 업체	*대표 홈페이지 등 (플랜아이)	윤원섭	010-5125-5327
		*전자도서관 (아이네크)	이재성	02-862-3900
		*ESM (이글루시큐리티)	황건	010-9249-3343
		*보안OS (시큐브)	안민욱	010-3089-2177
		*방화벽 (아이넷시스템즈)	조동욱	010-6409-9983
		*웹방화벽 (에스티아이네트웍스)	정보람	010-6502-0428
		*백업시스템 (비즈앤블럭)	공태민	010-2354-3309
		*보안USB (비젯)	홍병기	010-6436-9847
		*PKI(인증서) (드림시큐리티)	김영대	010-3461-1262
		*백업스토리지(3Gen) (아이티트랜드)	장도원	010-5580-2992
		*DB(오라클) (위드데이터)	장형석	010-2697-0541
		*PC개인백업 (이노티움)	박한울	010-9938-4437
		*DB보안 (한컴위드)	나국환	010-2222-8693
		*전자결재 / 포털 (나눔기술)	유재홍	0103485-3470
		*DDoS차단시스템 (에코넷시스템)	임재훈	010-4051-0109
		*메일 / 스팸차단 (모비젠)	이상현	010-4805-5285
		*웹디스크 (아이티스톤)	최미리	010-9414-6504
		*ERP (크리스피드)	정연규	010-2520-0909
		*PDF변환솔루션 (이파피루스)	심택규	010-8983-4854
		*PC 등 전산기기 (유페이버정보)	권성훈	010-2836-5627
		*NAC (포엘아이티)	박순열	010-4613-5409
		*L4스위치 (오픈베이스)	김경한	010-2518-7196

□ 유관기관 연락처

기관명	URL	연락처
국가정보원 국가사이버안전센터	www.nis.go.kr service1.nis.go.kr	111 02)557-0194
국무조정실 총무과	www.pmo.go.kr	044)200-2779
검찰청 사이버범죄수사단 인터넷범죄수사센터	www.spo.go.kr	02)2480-3600(대표) 02)3480-3571
경찰청 사이버테러대응센터	www.ctr.c.go.kr	02)1566-0112 02)393-9112
한국인터넷진흥원 인터넷침해대응센터	www.kisa.or.kr www.krcert.or.kr	02)405-5114 118
경제·인문사회연구회 사이버보안 관제센터	www.nrc.re.kr	044)211-1393 ~ 5
국가과학기술연구망(CREONET) 상황실	kreonet.net	042)869-1828

참고 2

침해사고 종류별 기술적 대응 요령

구분	내용	
악성코드공격	예상 징후	새로운 취약점 출현, 백신프로그램 탐지, 특정서비스 포트 접속 증가
	피해 증상	특정프로그램 접근시 오류 발생, 특정프로세스 비정상적 작동, 침입차단시스템 등 정보보호시스템의 악성코드 탐지, 보안프로그램 강제종료
	대응	(판단)백신, 정보보호시스템 로그 분석, 특정포트 오픈 확인 (분리)포트 분리, 악성코드 분석, 포트 스캐닝, 전용백신, 침입 탐지시스템 재설정 (차단)유입경로 차단, 외부 연결시도 차단
서비스거부공격	예상 징후	새로운 서비스거부공격 도구 공개, 특정서버의 비정상적인 서비스 중단, 서비스 공격용 프로그램 발견
	피해 증상	침입차단시스템 등 정보보호시스템에서 서비스 거부 공격 탐지, 백신을 통한 서비스거부공격도구 발견, 특정서비스 중단, 네트워크 속도 저하, 이상트래픽 발견
	대응	(판단)트래픽 모니터링 도구 활용, 침입차단시스템 로그 확인 (차단)라우터 트래픽분석, 라우터 ACL설정, 침입차단시스템 활용 (결함제거)보안취약점 업데이트
비인가접근공격	예상 징후	새로운 비인가접근공격 도구 공개, 연속적인 인증실패로그 발견, 비정상적인 스캐닝 흔적 발견, 자료유출 징후 발견, 비정상적인 업무 처리 흐름발견, 물리적 비인가접근 시도
	피해 증상	침입탐지시스템 등에 비인가접근 탐지, 비정상적인 계정 발견, 비정상 동작 프로그램 발견, 데이터 위·변조 및 삭제 흔적 발견, 해킹공격 경유지 이용 탐지
	대응	(차단)피해시스템 격리 또는 서비스 중지 (백업)로그자료 백업 (결함제거)비인가공격에 사용된 계정 제거
봇넷	예상 징후	백신 프로그램 탐지, 이상 트래픽 감지, 컴퓨터 자동 작동
	피해 증상	백도어로 인한 정보 유출, 해커에 의한 조작
	대응	(판단)의심 port (6667,6668 등과 같은 IRC Port)에 연결된 IP를 확인 (차단)C&C서버와 봇의 통신을 단절 (결함제거)C&C서버와 통신하는 악성코드 제거, 신규 봇넷 정보 파악

파괴 행위	예상징후	시스템의 비정상적인 작동, 오류 발생
	피해증상	웹사이트 손상, DB 파괴, 어플리케이션 오류, 시스템 부팅 실패
	대응	(판단)모니터를 통한 이상 트래픽 감지, 시스템 오류 (백업)시스템 분석 자료 백업 (결함제거)악성코드 제거, 악성코드 접근 루트 파악 및 제거, 정상적인 서비스를 위한 시스템 복구
랜섬웨어	징후	사용자 컴퓨터에 저장된 문서, 그림 파일 등을 암호화해 열지 못하도록 하고, 돈을 보내 주면 해독용 열쇠 프로그램을 전송해 준다면 금품을 요구하는 메시지 발생
	피해증상	암호화된 파일은 다시 복구되기 어렵고, 피해자가 공격자의 요구에 따라 대가를 지불해도 파일복구가 된다는 보장이 없음
	대응	랜섬웨어에 감염된 것을 발견하면 즉시 백신 프로그램으로 컴퓨터를 검사하여야 함. - 대응 가능한 백신의 개인용 무료백신 다운로드

* 복합공격은 두가지이상의 개별공격의 예상 징후가 나타나는 경우 판단가능하며, 중요도를 판별하여 각각의 사고대응 절차를 수행

참고 3

침해사고 발생 시 시스템 분석 방법

구분	내용
시스템정보분석 (Syscheck)	<ul style="list-style-type: none"> · Syscheck : 윈도우의 초기분석을 위해 국가사이버안전센터에서 제공하는 툴 · 구성요소 <ul style="list-style-type: none"> - SysTrace : 정보를 수집하는 툴로써 분석이 끝나면 결과파일을 생성 - 결과물 : '호스트이름.zip' 형식으로 생성되며 Viewer를 통해서만 읽기 가능 - Viewer : Viewer 프로그램을 설치한 후 [파일] - [열기]를 클릭하여 결과물을 선택 및 파일 로드(Load)하면 초기분석내용을 확인할 수 있음 <p>[Syscheck로 확인 가능한 내용]</p> <ul style="list-style-type: none"> - 시스템 기본정보(버전, 업데이트 목록, 네트워크 설정) - 실행중인 프로세스/DLL 정보 및 변조 유무 - 인터넷 사용 기록(다운로드 정보)
침해사고 시	<ul style="list-style-type: none"> - 네트워크 상세 연결정보 확인 : 현재 연결된 사용자 및 IP, Port 확인 - 메모리 저장 명령어 확인 : 최근 입력된 명령어 확인 - 계정, 공유, 원격 접근파일 정보 확인 - 실행중인 프로세스/DLL 정보 확인 : 특히 프로세스, 네트워크 연결중인 프로세스 확인 - 은닉 프로세스 확인 - 스케줄 작업 목록 확인 - 시작 레지스트리 확인 - 네트워크 기반 증거 수집 (IDS 로그, 라우터 로그 수집, 방화벽 로그, 중앙호스트(syslog)로 부터의 원격 로그) - 호스트 기반 증거 수집 (시스템 시간, 휘발성 데이터, 피해 시스템의 모든 파일들의 시간/날짜 정보, 출처 미확인 파일, 디스크 백업) - 그 외 증거들 수집 (증인으로 부터의 증언)
웜/바이러스 감염 시	<ul style="list-style-type: none"> - hosts 파일 설정 확인 : 파일 수정여부 확인 - 네트워크 상세 연결정보 확인 : 현재 연결된 사용자 및 IP, Port 확인 - 실행중인 프로세스/DLL 정보 확인 : 특히 프로세스, 네트워크 연결중인 프로세스 확인 - 스케줄 작업 목록 확인 - 시작 레지스트리 확인 - 인터넷 접속정보 임시파일 확인 : 감염경로 파악, 추가 악성코드 다운로드 확인 - 휴지통 파일 목록 확인 : 휴지통 폴더 내에 은닉된 파일 확인
랜섬웨어 감염 시	<ul style="list-style-type: none"> - 중요시스템 프로그램이 열리지 않음 - 윈도우 복원시점을 제거함 - 랜섬웨어가 별도의 다른 악성코드를 심음 - 백신 오작동 및 강제 삭제 또는 꺼짐 : 백신무효화 - 노트북 및 PC의 안전모드구동시 자체 안전모드로 진입 불가 - 파일의 확장자를 바꾸고 암호화함 - 모든 파일을 암호화하고 모든 파일이 암호화가 완료되면 “당신의 파일이 랜섬웨어에 걸렸다”고 통보함

참고 4**시스템 복구 우선순위**

순번	시스템명	업무등급	업무유형	비고
1	홈페이지	1등급	대국민	
2	주요 인트라넷 정보시스템 (메일, 전자결재, ERP 등)	1등급	일반행정	
3	기타	2등급	일반행정	

참고 5**피해수준별 복구방법**

피해수준	복구방법	복구 절차
데이터 손상	데이터 복구	<ul style="list-style-type: none"> 백업 데이터로부터 자료 복원
운영체제/프로그램 오류발생	어플리케이션 복구	<ul style="list-style-type: none"> 백신프로그램을 이용, 악성코드 제거 공격에 의한 취약점 제거 어플리케이션 소스 및 DB 복원을 통한 수정·재설치 어플리케이션 복구 확인
운영체제 복구불가능	운영체제 재설치	<ul style="list-style-type: none"> 운영체제 및 응용프로그램 재설치 백업 데이터로부터 자료 복원 운영체제 재설치 완료 후 정상상태 복귀 확인
하드웨어 손상	하드웨어 교체	<ul style="list-style-type: none"> 동일 하드웨어로 교체

참고 6

침해사고 대응 시나리오별 대응절차

□ 외부수준

- 서비스 거부 공격
- 웹서버를 통한 중요정보 노출
- 웹서버를 통한 DMP 구간 점령
- DMZ 구간에서 내부 망으로의 권한획득
- 메일 시스템을 통한 해킹 위협
- 방화벽 설정 오류를 통한 권한획득
- 악의의 사용자에게 의한 바이러스/웜 유포

□ 내부수준

- 서비스 거부 공격
- 내부 사용자에게 의한 권한획득 위협
- 내부 사용자에게 의한 바이러스/웜 유포 등

□ 상세 침해 시나리오 목록

구분		번호	침해 시나리오
외 부 수 준	서비스 거부 공격	# 1	분산 서비스 공격
		# 2	Syn Flooding 공격
		# 3	열려진 서비스를 통한 서버다운 공격
		# 4	기본 계정을 통한 네트워크 장비다운
	웹서버를 통한 중요 정보 노출	# 5	부적절한 파라미터의 처리
		# 6	테스트 파일, 백업 파일, DB정보를 포함한 파일 획득
		# 7	웹 관리자 권한 획득
	웹서버를 통한 DMZ 구간 점령	# 8	악성코드 업로드를 통한 권한획득
		# 9	침해 웹서버를 통한 경유 공격
		# 10	웹서버 엔진 취약점을 통한 권한획득
	DMZ구간에서 내부 망으로의 권한 획득	# 11	방화벽 설정 오류를 통한 내부권한 획득
		# 12	DB포트를 통한 DBA 권한 획득
		# 13	SNMP를 통한 라우팅 정보 파악
	메일 시스템을 통한 해킹 위협	# 14	악성 첨부파일 Reverse Connection 시도
		# 15	URL 링크 유도를 통한 Reverse Connection 시도
		# 16	스팸메일 발송을 통한 네트워크 부하

구분		번호	침해 시나리오
	방화벽 설정 오류를 통한 권한 획득	# 17	외부 불필요한 서비스를 통한 로그인
		# 18	SNMP를 통한 인터페이스다운
		# 19	외부 공인 Ipff 통한 시스템 침해
		# 20	무선 데이터 통신을 통한 해킹 위협
	악의의 사용자에게 의한 바이러스/웜 유포	# 21	사용자 PC 감염으로 인한 웜/바이러스 유포 (known)
		# 22	악의적인 바이러스 제작에 의한 유포 (unknown)
내부 수준	서비스 거부 공격	# 23	Ping Sweep을 통한 네트워크 부하
		# 24	서비스 거부 취약점을 이용한 시스템다운
		# 25	DBA 권한 획득으로 인한 DB 다운
	내부 사용자에게 의한 권한획득 위협	# 26	시스템 취약점을 통한 권한획득
		# 27	스니핑을 통한 권한획득
		# 28	웹 관리 서버를 통한 웹 관리자 권한획득
		# 29	SNMP 스캐닝을 통한 라우팅 정보 파악
		# 30	바이러스/웜 제작을 통한 배포

□ 침해사고 상황별 분석 방법 목록

구분		침해 시나리오
네트워크	패킷 스니핑을 통한 네트워크 분석	
	스니핑 탐지	Ping 이용
		ARP 이용
		DNS 이용
		네트워크 관리
	IDS/Firewall/IPS 분석	IDS에 네트워크 Scanning 감지
	인터넷 방화벽 룰셋 및 IDS 분석	
	네트워크 장비 분석	Default 패스워드 체크
		로깅 기능 체크
		트래픽 분석을 통한 서비스 거부공격 추적
	SNMP Community String 값 확인	룰을 이용한 확인
UNIX 시스템 상세 분석	해킹 여부 판단	
	피해 시스템 백업	
	피해 시스템 상태 분석	숨겨진 파일 또는 디렉토리 점검
		Root 소유의 SUID 설정파일 점검
	Step 별 백도어 점검 방법	
	유형별 백도어 거색 기법	패스워드 백도어 검색

구분		침해 시나리오
		설정 파일을 이용한 백도어 검색
		Crontab 백도어 검색
		.profile 백도어 검색
	Rootkit 점검	Lsof를 이용한 시스템 파일 점검
		시스템 파일의 파일 크기, timestamp 확인
		MD5를 이용한 무결성 검사
	해킹기법 분석	Messages 분석
		Xferlog 분석
		Access_log, error_log 분석
	분석도구	Lsof
		Nc
		Nmap
		Md5
		Md5-tool
윈도우 시스템 분석	해킹 진행여부 판단	Netstat 명령어를 이용한 세션 연결 상태 분석
		Sniffing 툴을 이용한 세션상태 분석
	피해시스템 상태분석	Fport를 이용한 백도어 점검
		계정 및 스케줄러 점검
		네트워크 공유정보 점검
		악성프로그램 점검
	해킹기법 분석	이벤트 로그 분석
		IIS 로그 분석
		SQL 로그 분석
		Ms Exchange 로그 분석
	분석도구	IRIS
		Fport
		ntlast
웹	해킹진행 여부 및 상태분석	Netstat 명령어를 이용한 세션 연결 상태 분석
		웹 페이지를 이용한 백도어 검색
	해킹 기법 분석	중요정보 노출 측면
		권한획득 위협 측면
		SQL Injection 공격 유형의 웹로그 분석
		XSS 공격 유형의 웹로그 분석
		부적절한 파라미터 조작 가능성 확인
		관리자 페이지 ID/Password 취약 유형 점검
DB	DB Connection 로그 분석	Oracle listener audit trail
	DB 관련 로그 분석	Oracle DBMS History situation
	계정 운용 적정성 분석	DBMS 유저 정보 확인

서식 #1~#7

- 서식 #1 사고신고서
- 서식 #2 사고조치보고서
- 서식 #3 상황통보문
- 서식 #4 피해기관 현황표 I
- 서식 #5 피해기관 현황표 II

[서식1] 사고신고

사 고 신 고 서

기 본 정 보			
기 관 명		부 서	
성 명		직 위	
전자우편			
연 락 처	전화:	H.P:	Fax:
사 고 내 용			
사고일시	년 월 일	피해 IP 주소	
	시 분		
피해시스템 용 도	* 시스템 분류 목록 입력	운영체제	<input type="checkbox"/> 윈도우 <input type="checkbox"/> 유닉스 <input type="checkbox"/> 네트워크장비
			상세버전정보:
사고유형	* 사고유형 목록 입력	피해범위	대 * 피해시스템의 수량 기입
사고내용			
조 치 내 용			
그 밖에 사고 관련 내용을 구체적으로 서술			

[첨부]

가. 시스템 분류 목록

기호	시스템 분류	설명
가	웹서버	기관의 홈페이지 운영 및 웹서비스 제공을 하는 서버
나	전자우편 서버	전자우편 송수신을 위해 운영하는 서버
다	DB/업무 서버	홈페이지 및 업무지원을 위한 데이터베이스 서버
라	개발/임시서버	개발 및 운영테스트를 위하여 사용하는 임시서버
마	통신전송장비	라우터, 스위치 등 통신전송장비 일체
바	보안장비	방화벽, IDS, VPN 및 백신서버 등 정보보안제품 일체
사	개인/업무 PC	기관 내 사용자의 PC
아	임시PC	공용 작업을 위해 여러 명이 사용하는 PC
자	기타	시스템 분류가 없는 경우(서술식 기술)

나. 사고 유형 목록

기호	사고유형	설명
가	경유지 악용	타 기관으로부터 해킹시도 항의를 받았거나, 시스템 점검 중 해킹 흔적 또는 해킹툴이 설치되어 타 시스템에 접속한 기록이 발견되었을 경우
나	자료훼손 및 유출	내부 시스템의 자료가 변조되었거나, 대량의 데이터가 외부로 무단 송신된 흔적이 발견되었을 경우
다	단순 침입 시도	지속적인 스캐닝 공격이 발생할 경우
라	웜 바이러스 피해	기관내의 PC에서 웜 바이러스가 발견되었을 경우
마	홈페이지 변조	기관의 홈페이지가 변조되었을 경우
바	홈페이지 접속 불가능	기관의 홈페이지 서버 또는 네트워크 이상으로 인해 홈페이지 접속이 불가능할 경우
사	서비스거부 공격피해	불특정 다수의 IP로부터 접속 시도 또는 대량 트래픽이 동시에 유입될 경우
아	기타	사고유형에 포함되지 않을 경우(서술식 기술)

[서식2] 사고조치보고서

사 고 조 치 보 고 서

기 본 정 보			
기 관 명		부 서	
성 명		직 위	
전자우편			
연 락 처	전화:	H.P:	Fax:
사 고 내 용			
사고일시	년 월 일	피해 IP 주소	
	시 분		
피해시스템 용 도	* 시스템 분류 목록 입력	운영체제	<input type="checkbox"/> 윈도우 <input type="checkbox"/> 유닉스 <input type="checkbox"/> 네트워크 장비
			상세버전정보:
사고유형	* 사고유형 목록 입력	피해범위	대 * 피해시스템의 수량 기입
사고내용			
조 치 내 용 요 약			
사고원인			
피해현황			
사고대응 조치사항			
피해복구결과			
기 타			

[서식3] 상황통보문

상 황 통 보 문

기 관 사 항			
기 관 명		부 서	
성 명		직 위	
전자우편			
연 락 처	전화:	H.P:	Fax:
조 치 사 항			
경보수준			
발 령 일	0000년 00월 00일	수 신 일	0000년 00월 00일
	00시 00분		00시 00분
조치사항 요약	<ul style="list-style-type: none"> ○ 기관내 사용자에게 대응책을 작성, 배포 ○ 전자우편 서버의 Filter를 적용 ○ 기관내 감염피해 확인(피해대수 및 감염PC의 IP) 		
조치대상 목록			
조치결과			
특이사항			

※ 제목과 발령일 부분은 경고발령 수준에 따라 해당 경보수준 색으로 함

관심
-
주의
-
경계
-
심각

[서식4] 피해현황표 I(사고건수)

번호	구 분	사고건수	피해현황	기밀유출
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				

[서식5] 피해현황표 II(특정 IP 흔적 및 백신탐지 기록)

번호	구 분	공격 IP	특정 Port	백신 탐지명	이메일 수신여부
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					