실증단지 사이버안전
위기대응 실무 매뉴얼

본 매뉴얼은 실증단지 사이버 보안지침('10.5.)을 근거로 「사이버안전」 위기상황 발생 시 통합운영센터와 컨소시엄 운영센터가 적용할 세부 대응절차 및 제반 조치사항을 규정하여 사이버 안전에 완벽을 기하고자 작성되었음.

2011. 1.

실증단지 보안센터

- 목 차 -

<붙임>

1. 개요

제주 스마트그리드 실증단지 사이버안전 위기대응 실무 매뉴얼은 웜·바이러스 및 해킹 등 사이버공격에 의해 실증단지 정보통신망과 기기·시스템 등에 침해사고가 발생할 경우, 실증단지 통합운영센터 및 컨소시엄 운영센터의 대응절차와 조치 사항을 규정한 것임.

2. 관련근거

가. 국가위기관리기본지침(대통령훈령 제229호, '08.10.8)

나. 국가사이버안전관리규정(대통령훈령 제222호, '08.8.18)

다. 국가사이버안전매뉴얼(국가사이버안전센터, '05.10)

라. 실증단지 사이버보안 지침('10.5.)

3. 적용범위

가. 웜·바이러스, 해킹 등 사이버 공격으로 인한 실증단지 정보통신망과 기기·시스템 등의 장애 및 마비, 중요자료 유출 등 위기상황 발생 또는 발생 가능성이 있을 경우 적용

나. 통합운영센터, 컨소시엄 운영센터, 기간시스템 연계 구간에 침해사고가 발생하여 실증단지 정보통신망과 정보시스템·기기 중단 등의 사태에 적용

4. 용어 정의

구분	내용
실증단지 위기	실증단지를 구성하는 기기·정보시스템·정보통신망·통합운영센터·컨소시엄운영센터·기간시스템연계구간 등 실증단지의 핵심요소나 가치에 중대한 위해가 가해질 가능성이 있거나 가해지고 있는 상태

구분	내용
위기관리	실증단지 위기를 사전에 예방하고 발생에 대비하며 위기발생 시에는 효과적인 대응 및 복구를 통하여 그 피해와 영향을 최소화함으로써 조기에 위기 이전상태로 복귀시키고자 하는 제반 활동
위기관리 활동	① 예방 : 위기요인을 사전에 제거하거나 감소시킴으로써 위기 발생 자체를 억제하거나 방지하기 위한 일련의 활동 ② 대비 : 위기상황 하에서 수행해야 할 제반 사항을 사전에 계획, 준비, 교육, 훈련함으로써 위기대응 능력을 제고시키고, 위기발생시 즉각적으로 대응할 수 있도록 태세를 강화시켜 나가는 일련의 활동 ③ 대응 : 위기발생시 실증단지의 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
위기경보	① 관심(Blue) : 징후가 있으나 그 활동수준이 낮으며 가까운 기간 내에 실증단지 위기로 발전할 가능성도 비교적 낮은 상태 ② 주의(Yellow) : 징후 활동이 비교적 활발하고 실증단지 위기로 발전할 수 있는 일정 수준의 경향성이 나타나는 상태 ③ 경계(Orange) : 징후 활동이 매우 활발하고 전개속도, 경향성 등이 현저한 수준으로서 실증단지 위기로의 발전 가능성이 농후한 상태 ④ 심각(Red) : 징후 활동이 매우 활발하고 전개속도, 경향성 등이 심각한 수준으로서 실증단지 위기발생이 확실시 되는 상태
기기	스마트그리드 실증단지에 설치되는 스마트미터(DCU 포함), 스마트가전(홈디스플레이 포함), 전기차, 전기차 충·방전장치, 정보수집 센서, 풍력·태양력 등 신재생 발전기기
정보시스템	서버, PC 등 단말기, 보조기억매체, 네트워크 장치, 응용프로그램 등 정보의 수집·가공·저장·검색·송수신에 필요한 하드웨어와 소프트웨어

구분	내용
정보통신망	유·무선, 광선, 위성 등을 매개로 하는 다양한 정보통신 수단에 의하여 부호, 문자, 음향, 영상 등의 정보를 수집·가공·저장·검색·송수신하는 정보 전달체계
해킹	접근을 허가받지 않은 정보시스템에 불법으로 침투하거나 허가되지 않은 권한을 불법으로 갖는 행위
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
바이러스	감염파일의 실행을 통해서 확산되며, 정상적인 파일이나 부트영역에 침입하여 바이러스코드를 추가하는 형태로 파일을 감염시키는 악성 프로그램의 일종
악성코드	컴퓨터 바이러스, 웜, 트로이목마와 같이 시스템에 해를 입히거나, 시스템을 방해하기 위해 특별히 설계된 악의적인 컴퓨터 프로그램 또는 실행 가능한 코드
서비스 거부	시스템에 과도한 부하를 일으켜서 정보시스템의 사용을 방해하는 공격 방식으로서 분산서비스 거부공격 또는 분산반사서비스 거부공격 등으로 구분
트로이목마	자기복제 능력은 없으나, 정상 기능의 프로그램으로 가장하여 프로그램 내에 숨어있는 코드조각으로, 의도하지 않은 기능을 수행하는 컴퓨터 프로그램 또는 실행 가능한 코드
사이버 공격	네트워크를 통해 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 해킹, 웜·바이러스 등 악성코드 유포, 서비스거부, 도청 등을 수행하는 행위
사이버 보안	사이버 공격으로부터 실증단지 기기, 정보시스템, 정보통신망을 보호하기 위한 조치

5. 위기 전개 양상

구 분	내 용
징 후 발 견	• 보안취약점 공개 및 이를 악용한 해킹도구 발견 • 위험도가 높은 웜·바이러스 출현 • 기기 및 정보통신망에 의도적인 불법 침입 시도 탐지
초 기 진 행	• 웜·바이러스 및 해킹 피해 발생 • 정보통신망 소통량이 비정상적으로 급증
부 분 진 행	• 웜·바이러스 및 해킹 피해 증가 • 정보통신망 소통량 급증에 따른 국지적인 장애 발생 • 실증단지 핵심기반시설에서 자료유출 가능한 악성코드 감염 피해 발생
전 면 확 산	• 대규모 웜·바이러스 및 해킹 피해 발생 • 전국적으로 정보통신망 마비 확산 • 실증단지 네트워크 전역으로 정보통신망 마비 확산 • 실증단지 일부 핵심기반시설에서 자료유출 피해 발생
위 기 발 생	**• 국가 주요 정보통신망 마비** **• 실증단지 주요 정보통신망 마비** **• 실증단지 중요자료 유출**

6. 위기경보

가. 위기경보 수준

구 분	판 단 기 준	세부상황	비 고
정상 (Green)	▪ 정상상황	▪ 위험 정도가 매우 낮은 웜·바이러스, 해킹기법, 보안취약점	
관심 (Blue)	▪ 위험도가 높은 웜·바이러스 등 악성코드 및 해킹 기법 출현으로 피해 발생 가능성 증대	▪ 해외 피해 확산 등 해외 사이버위협의 국내 전파를 통한 실증단지 유입 가능성 증대 ▪ 국내 피해 확산 등 사이버위협의 실증단지 유입 가능성 증대	징후 활동 감시
	▪ 공격 시도가 발생했으나 기존 보안 대책에 의해 탐지, 차단되어 피해 발생 없음	▪ 바이러스, 트로이목마, 웜 등의 전파 시도가 탐지되어 차단됨 ▪ 기기 및 정보시스템에 대한 권한 획득 시도 차단 ▪ 기기 및 정보시스템 공격 시도가 탐지되어 차단됨	
	▪ 시스템 운영에 영향을 미치지 않는 공격 발생	▪ 네트워크를 대상으로 스캐닝	
	▪ 사이버 위협 발생이 예상되는 상황	▪ 현재는 정상상태이나 사이버위협 발생이 예상되는 상황(예, 해킹대회, 실증단지 정보시스템 및 정보통신망 시설 신규 설치 및 보수 등)	

구 분	판 단 기 준	세부상황	비 고
주 의 (Yellow)	▪ 위험도가 높은 웜·바이러스 등 악성코드 및 해킹 기법 출현으로 피해 발생 ▪ 기기 및 정보시스템에 대한 공격으로 피해 발생 ▪ 기기 및 정보시스템에 대한 대규모 공격이 발생될 것으로 예상될 때 ▪ 기기 및 정보시스템 전반에 보안태세 강화 필요	▪ 비인가된 기기 및 시스템 권한 획득 ▪ 공격에 의한 단일 시스템 장애 발생	협조 체계 가동
경 계 (Orange)	▪ 웜·바이러스 등 악성코드의 급속한 확산으로 네트워크 트래픽이 실증단지 정보통신망 전반에 걸쳐 급격하게 증가하여 대규모 피해로 발전 가능성 증가 ▪ 실증단지 운영 주요 정보시스템에 대한 공격으로 피해 발생 ▪ 다수의 시스템에 파괴적인 동작을 하는 악성코드 발견 및 피해 증가	▪ 실증단지 정보통신망 장애 ▪ 공격에 의한 주요 정보시스템 장애 발생	대비 계획 점검
심 각 (Red)	▪ 실증단지 기기 및 시스템 대상 피해 발생 ▪ 지역적·부분적 피해 발생, 전국적 확산 가능성 증대 ▪ 국가적 차원에서 공동 대처 필요	▪ 주요 기기 및 정보시스템의 주요정보 유출, 위변조, 삭제, 파괴	즉각 대응 태세 돌입

구 분	판 단 기 준	세부상황	비 고
	▪ 실증단지 운영센터에서 네트워크 사용 불가능 ▪ 실증단지 정보통신망 사용 불가능 ▪ 실증단지의 주요 정보시스템에 대한 공격으로 인한 심각한 피해 발생	▪ 웜 전파로 인하여 주요 네트워크 장비(DNS, 라우터, 백본 스위치 등)에 대한 공격으로 네트워크 운영 불가능 ▪ 대량의 네트워크 트래픽 발생으로 정보통신망 운영 불가능 ▪ 실증단지 정보통신망을 통한 주요정보 유출 ▪ 실증단지 기기 및 시스템 불법제어로 인한 전력계통 주요시설 통제 불가능	

나. 위기경보 절차

(1) 실증단지 위기경보

- 통합보안관제센터는 사고신고 접수 후, 위기경보 발령 필요성이 있을 경우 통합운영센터장에게 보고
- 통합운영센터는 보안센터 및 ES-ISAC과 위기경보 단계를 협의하고, 실증단지 위기경보 발령
- 통합보안관제센터는 각 컨소시엄 보안관제센터(보안담당)에 위기경보 전파
- 컨소시엄 보안관제센터(보안담당)는 컨소시엄 운영센터장에게 위기경보 발령 사실을 보고

(2) 국가 주요 정보통신망 위기경보

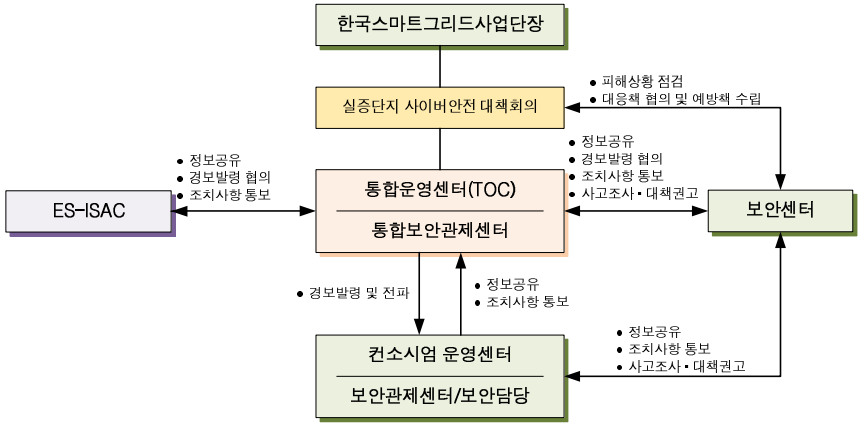
- 국가정보원(NCSC)에서 위기경보를 발령한 경우 지식경제부 사이버안전센터는 ES-ISAC에 위기경보 발령 사실을 전파
- ES-ISAC은 통합운영센터 및 보안센터와 협의를 통해 각 컨소시엄 운영센터에 위기경보 발령 사실을 전파

7. 위기관리 업무수행 체계

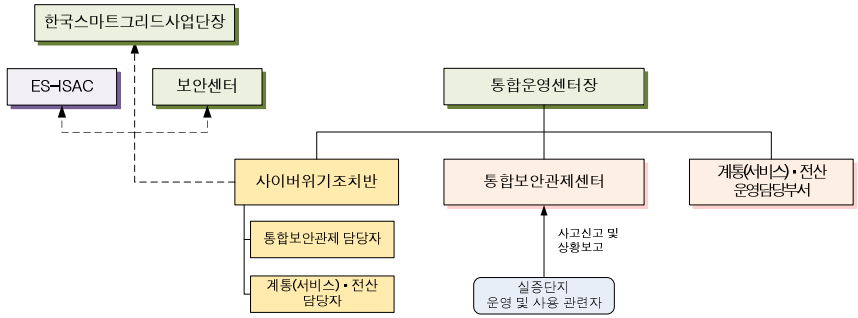
가. 기본 방침

- 사이버공격에 대한 실증단지 통합운영센터 및 컨소시엄 운영센터 간 협력체계 강화
- 사이버공격 조기경보 발령 전파 및 대응 체계 확립
- 사이버안전 관리 실태 점검 및 보완
- 대규모 위기사태 발생 시 합동조사 및 복구

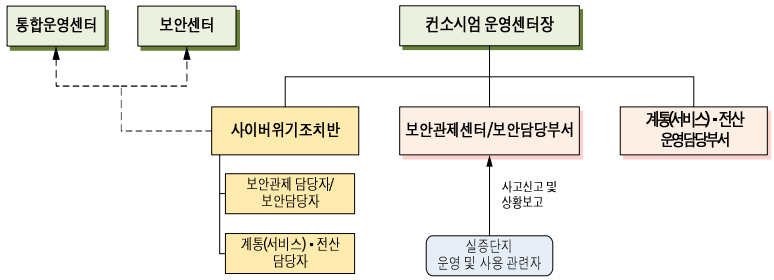
나. 실증단지 기본 체계



다. 통합운영센터 및 컨소시엄 운영센터 대응 체계

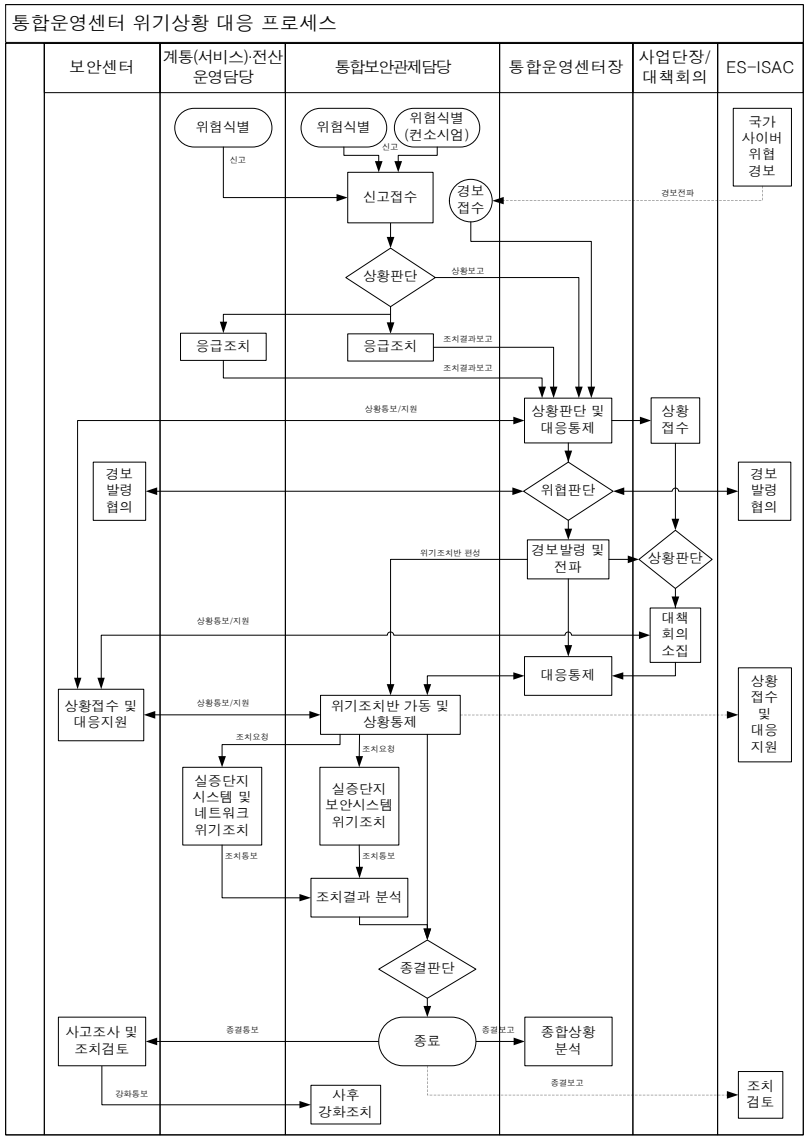


<통합운영센터>

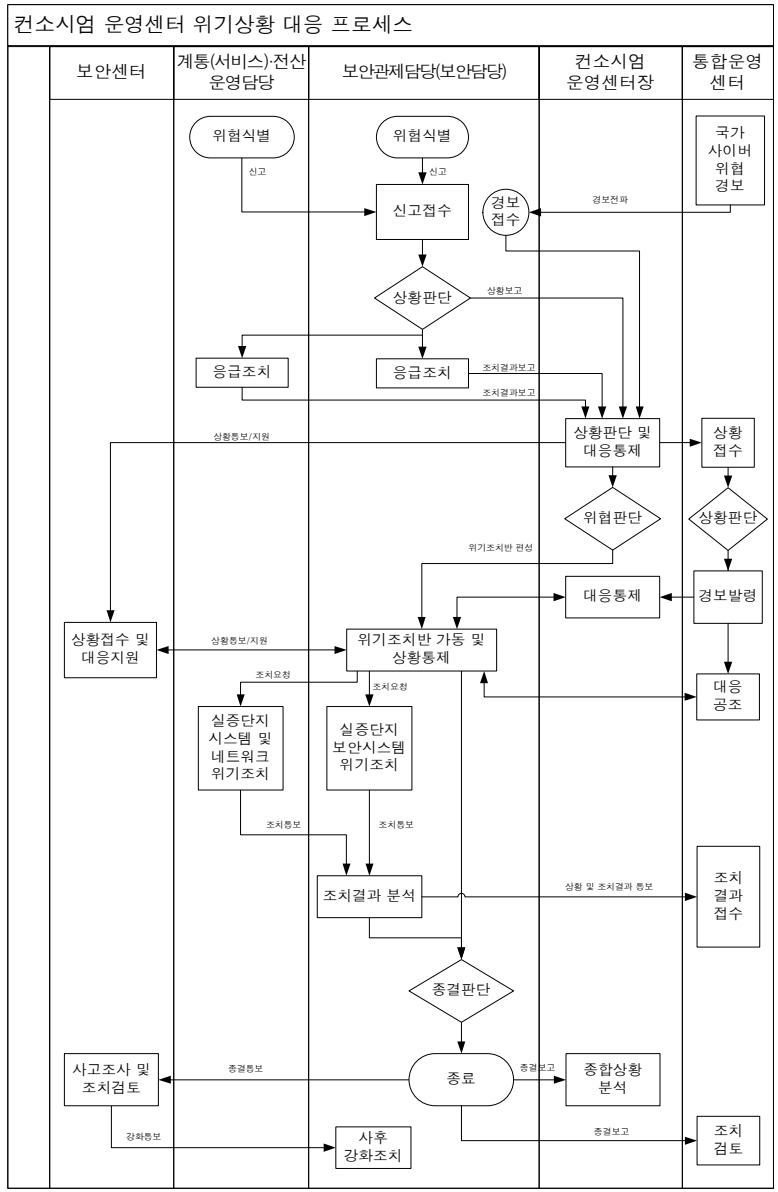


<컨소시엄 운영센터>

라. 통합운영센터 업무 흐름도



마. 컨소시엄 운영센터 업무 흐름도



바. 대응체계 구성 요소별 책임 및 역할

구 분	내 용
ES-ISAC	▪ 국가 주요 정보통신망 위기경보 발생 시 보안센터 및 통합운영센터와 실증단지 위기경보 발령 협의 ▪ 국가 주요 정보통신망 위기경보 발생 시 실증단지 관련상황 모니터링 및 종합
보안센터	▪ 국가 주요 정보통신망 또는 실증단지 위기경보 발생 시 통합운영센터 및 ES-ISAC과 실증단지 위기경보 발령 협의 ▪ 실증단지 사이버안전 위기대응 체계 수립 및 개선 ▪ 실증단지 사이버안전 위기대응 실무 매뉴얼 작성 및 배포 ▪ 정보통신망 마비 또는 자료유출 등 중대 보안사고 신고 접수, 사고조사 수행 및 복구 지원 ▪ 재발방지를 위한 보안대책 권고 ▪ 대책회의 운영에 대한 자문 제시
통합운영센터	▪ 국가 주요 정보통신망 또는 실증단지 위기경보 발생 시 보안센터 및 ES-ISAC과 협의를 통해 실증단지 위기경보 발령 ▪ 위기경보 발생 시 위기관리 업무수행 체계 구축 ▪ 실증단지 사이버안전 위기대응 실무 매뉴얼에 따른 위기대응 체계 수립 및 시행 ▪ 사이버위기 대응을 위한 위기조치반의 구성, 소집 및 운영 ▪ 실증단지 보안사고 관련 종합 모니터링 수행 ▪ 보안사고 신고 접수 및 조사 수행 ▪ 정보통신망 마비 또는 자료유출 등 중대 보안사고 발생 시 초동조치 수행 ▪ 사이버안전 분야 위기관련 예방, 대비, 대응, 복구 활동 수행

구 분	내 용
	▪ 중대 보안사고 발생 시 보안센터에 통보하고, 위기관련 업무 수행 시 보안센터와 협조
컨소시엄 운영센터	▪ 위기경보 발령 시 위기관리 업무수행 체계 구축 ▪ 실증단지 사이버안전 위기대응 실무 매뉴얼에 따른 위기대응 체계 수립 및 시행 ▪ 사이버위기 대응을 위한 위기조치반의 구성, 소집 및 운영 ▪ 컨소시엄 보안사고 관련 종합 모니터링 수행 ▪ 보안사고 신고 접수 ▪ 정보통신망 마비 또는 자료유출 등 중대 보안사고 발생 시 초동조치 수행 ▪ 사이버안전 분야 위기관련 예방, 대비, 대응, 복구 활동 수행 ▪ 중대 보안사고 발생 시 통합운영센터 및 보안센터에 통보하고, 위기관련 업무 수행 시 보안센터와 협조
대책회의	▪ 사업단장은 사이버위기 상황에 효과적으로 대응하기 위하여, 위기경보가 경계 단계 이상으로 격상되거나, 협조체계 가동을 통한 대응이 필요한 경우 대책회의 소집 ▪ 피해 상황 점검, 대응책 협의 및 예방책 수립 ▪ 기타 실증단지 지원을 위한 요구사항 및 지원책 강구 등 예방 및 조치에 필요한 사항 제시 ▪ 대책회의 구성 : 사업단장, 보안센터장, 통합운영센터장, 각 컨소시엄 운영센터장, 위기조치반장
위기조치반	▪ 위기조치반은 기본적으로 보안담당부서(통합보안관제센터 또는 보안관제센터), 계통(서비스)·전산 운영담당부서를 중심으로 구성하고 필요한 경우 다른 부서의 지원을 받음

구 분	내 용
	▪ 위기조치반의 반장은 보안담당부서장으로 하되, 사이버 위기상황을 고려하여 가장 적합하다고 판단되는 직원을 반장으로 선임 가능 ▪ 위기조치반이 주관하여 사이버위기 대응 ▪ 사이버위기 관련 정보 취득 및 분석 등 기술적 조치 수행 ▪ 실증단지에 대한 황색 및 적색 등급 이상의 사고가 발생하여 조치가 완료된 경우, 보안센터와 협조하여 네트워크 및 시스템에 대한 사고조사 실시 ▪ 보안담당 : 업무의 총괄적 수행, 유관기관과 연락체계 담당, 사고 위협판단, 위기조치반 가동 및 상황통제, 보안시스템 위기조치, 위기조치결과 분석, 사고조사 ▪ 계통(서비스)·전산담당 : 계통 및 서비스 관련 시스템 및 정보통신망 위기조치 ▪ 대책회의의 결과를 반영하여 위기조치반 운영

사. 위기관리 활동

단계	중점	세부활동	역할
예방	▪ 실증단지 관련 사이버 안전대책 수립·시행	▪ 국가 및 한전 정보보호 기본지침, 실증단지 운영규정 (사이버 보안지침 및 보안가이드라인) 등의 평시 시스템 운용 안전기준에 따라 정기 점검 시행 ▪ 위기시에 대비한 「위기대응 실무매뉴얼」 시행	▪ 자체 사이버안전 대책 수립 및 이에 따른 점검 및 예방 ▪ 정보보호 전담 조직 및 인력 운영
	▪ 위기징후 실시간 감시, 위협정보 수집, 분석 및 전파	▪ 사이버위협 정보를 보안센터에 통보 (컨소시엄 운영센터는 통합운영센터에도 통보)	▪ 사이버위협 관련정보 입수 및 보안사고 인지 시 관련 내용을 상호 공유
	▪ 실증단지 핵심기반 시설 및 정보통신망에 대한 안전대책 수립	▪ 증단지 핵심기반시설 및 정보통신망 신·증설 등 환경 변화 시 자체 보안대책을 강구하고 기간시스템과 연계되는 부분에 대해서는 국가정보원에 보안성 검토 의뢰	
	▪ 국내외 사이버안전 관련기관과 공조	▪ 통합운영센터, 컨소시엄 운영센터, 보안센터와 정보공유 체계 구축	

단계	중점	세부활동	역할
대비	▪ 위기경보 발령 전파	▪ 통합운영센터는 ES-ISAC 및 보안센터와 협의를 통해 실증단지에 위기경보 발령 ▪ 위기경보 발령을 문자메시지, 전자우편, 전화, 팩스, 홈페이지 등을 활용하여 위기경보를 컨소시엄 운영센터에 신속하게 전파	<관심> ▪ 경보전파 및 보안권고문 배포 ▪ 정보통신 시스템 모니터링 강화 ▪ 기술적 보안대책 시행
	▪ 위기대응 능력 강화	▪ 백신 프로그램 및 정보보호시스템 의무적 설치 ▪ 운영체제 보안패치 적용 및 응용 프로그램 업데이트 ▪ 위기관리 실태 상시 점검체계 확립 ▪ 사이버안전을 위한 위기관리 전담조직 운영계획 수립 자체 대응·복구를 위한 자체대응반 사전 구성	<주의> ▪ 자체대응반 및 위기관리 체계에 대한 비상연락망 인원 및 연락처 점검 갱신
	▪ 사이버 안전에 대한 교육 및 인식 제고	▪ 실무매뉴얼에 따른 실행교육 실시	▪ 기기·시스템, 네트워크 장비 등 시스템 및 프로그램 제공업체의 연락체계 점검
	▪ 사이버 안전 위기관리 훈련	▪ 사이버공격 훈련 대응계획 수립과 훈련 결과를 종합하여 보안취약점 개선 및 보완	▪ 기술적 보안대책 시행

단계	중점	세부활동	역할
	▪ 위기상황 대비 Backup 및 대응책 강구	▪ 중요 자료 및 시스템의 복구를 위한 백업 실시 ▪ 백업된 자료의 복구 테스트 등 비상시 시스템 복구 절차 마련 ▪ 하드웨어 및 소프트웨어 업체와의 비상연락체계 점검	<경계> ▪ 필요시 자체 대응반 운영 ▪ 즉각적인 시스템 복구를 실시하고 피해확산 차단 ▪ 급속한 피해 확산 우려 시 네트워크 연결 차단 ▪ 기술적 보안대책 시행 <심각> ▪ 자체대응반 운영 및 즉각 대응 태세 돌입 ▪ 기관 내 PC 사용 최소화 및 오프라인 업무 권고 ▪ 기술적 보안대책 시행

단계	중점	세부활동	역할
대응	▪ 심각경보 발령의 경우 통합운영센터, 컨소시엄 운영센터, 보안센터 간 협력하여 신속한 대응조치 및 지원 ▪ 위기조치반에 의한 신속한 대응 조치	▪ 통합운영센터, 컨소시엄 운영센터, 보안센터 간 협력하여 피해확산 차단, 피해 상황의 종합 처리 및 보고, 사고원인에 대한 조사 및 분석, 대응방법 전파 ▪ 시스템 또는 전산센터 장애 발생 시 백업시스템 또는 백업사이트 가동 ▪ 사고조사 및 복구에 필요한 자료 제공 ▪ 위기대응 실무매뉴얼에 따라 상황별 대응책 적용	▪ 자체대응반 구성운영 ▪ 위기관리 체계 구성원 간 비상연락 체계 유지 ▪ 사고조사 및 복구에 필요한 자료제공 ▪ 위기대응 실무매뉴얼에 의거 단계별 대처요령 수행
복구	▪ 보안센터·통합운영센터 간 긴밀한 협조 ▪ 복구 절차에 따른 피해복구 수행	▪ 경미한 사고는 피해 기관이 자체 복구 – 필요시 컨소시엄 운영센터는 통합운영센터에 통보 ▪ 중대 보안사고 발생 시 보안센터에 상황 통보 (컨소시엄 운영센터는 통합운영센터에도 상황 통보) ▪ 중대 보안사고 발생 시 보안센터 지원 하에 복구	▪ 자체대응반 구성운영 ▪ 위기관리 체계 구성원 간 비상연락 체계 유지 ▪ 위기대응 실무매뉴얼에 의거 단계별 대처요령 수행 ▪ 복구에 필요한 자료제공 및 관련업무 지원

단계	중점	세부활동	역할
	▪ 사고 재발 방지를 위한 보안대책 수립 및 시스템 개선	▪ 사고 원인 분석에 따라 보안취약점 검사 및 개선 ▪ 사이버안전대책의 실효성 점검 및 수정·보완	

아. 위기경보 수준별 기술적 보안대책

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

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

자. 복구 절차에 따른 피해복구 수행

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

8. 위기경보 수준별 대응요령

가. 경보수준별 대응요령 요약

단계		대응요령 요약
경보	심각	○ **경계** 경보 조치 지속 시행 ○ 실증단지 통합 관리 차원의 즉각 대응 태세 돌입 ○ 보안센터 사고조사 및 복구지원팀 가동
	경계	○ **주의** 경보 조치 지속 수행 ○ 위기조치반 가동
	주의	○ **관심** 경보 조치 지속 수행 ○ 통합운영센터, 컨소시엄 운영센터, 보안센터 간 공조체계 확인 ○ 위기조치반 가동 준비 (필요시 소집)
	관심	○ 보안권고문 등 보안조치 이행 ○ 이상 징후 탐지 시 초동대처, 중대사고 발생 시 보안센터에 통보 ○ 사고발생 대비 위기조치반 연락체계 확인 ○ 사이버공격 여부 감시 강화
정상		○ 정보공유시스템의 최신 정보 지속 확인 ○ 보안취약점 발굴 및 실무기관 간 공유체계 활성화 ○ 사이버안전 위기대응 매뉴얼에 의거 정기적 점검 실시 ○ 위기조치반 구성 ○ 사이버안전 모의훈련 실시 및 취약점 개선·보완

나. 단계별 조치 사항

1) 공통조치사항 (청색, 황색, 적색단계 해당)

대응 업무	주무부서
○ 침입 시도 발생에 따른 처리 절차 1. 침입탐지 정보에서 근원지 IP 주소의 whois 정보 파악 2. 침입차단시스템에서 해당 IP 주소의 접근을 차단하고 통합운영센터와 보안센터에 신고 ("별표 3"참고) 3. 해당 기관(사용자)으로 항의 전화 연락 및 메일 발송 4. 피해발생 또는 이에 준하는 침입, 지속적인 침입일 경우, 조치 요청 공문을 해당 기관장에게 발송 가. 의도적인 해킹 시도일 경우, 통합운영센터장 및 컨소시엄 운영센터장 명의로 항의 서한을 해당 기관장에게 발송 나. 침입이 지속적으로 발생할 경우, 항의 메일을 3일 간격으로 발송, 단 근원지 IP 주소가 국외인 경우 항의 메일만 송부 5. 침입시도가 없고 해당 기관으로부터 조치 완료 통보를 받은 후, 침입차단시스템 차단을 해제하고 처리 완료	통합 운영센터 및 컨소시엄 운영센터

2) 단계별 조치사항

단계	대응 업무	주무부서
정상	○ 정보시스템 보안에 대한 계획 수립 – 주요 자산에 대한 자산 목록표 작성 및 현황 유지 – 네트워크 구성 최신 현황 유지 (내·외부 연계 현황 포함) – 정보보안 시스템 운영 지침 수립	보안담당부서
	○ 일상적인 정보보안 업무 수행 – 사용자, 관리자, 경영자 대상 교육 및 모의 대응 훈련 수행 – 시스템 내부의 불필요 계정 삭제	보안담당부서 전부서

단계	대응 업무	주무부서
	– 패스워드 관리 지침에 의거한 패스워드 관리 수행	전부서
	– 내부적인 취약성 점검, 외부 취약성 점검주기적 실시	보안담당부서
	– 바이러스 백신, 방화벽, 침입탐지시스템 보안 제품 운영	전부서
	– 네트워크 모니터링 도구를 이용한 네트워크 트래픽 분석	보안담당부서
	– 주요 정보 시스템 데이터의 주기적 백업 수행	전부서
	– 주기적인 취약점 정보 확인 및 패치 수행	전부서
	– 방화벽, 침입탐지시스템, 스위치, 라우터 등의 보안감사 자료	보안담당부서
	– 정보보안 업무 수행 결과 기록, 분석 및 관리자 보고	보안담당부서
관심	○ 단순 해킹사고 대응 업무 수행	보안담당부서
	– 사이버테러 대응 요원이 대응 조치 시행 및 보고	
	○ 유관 기관과의 협조 체제 유지	
	– 유관기관 협조 및 연락 체계 구성	전부서
	– 주기적 회의를 통한 정보수집 및 공유	전부서
	○ 상위 단계 조치에 대한 주기적인 검토 및 시행 준비	전부서
주의	○ 이전 단계의 모든 조치 시행	
	○ 피해 시스템/네트워크에 대한 조치 (피해상황 분석 및 긴급 상응 보안 조치 수행)	
	– 필요시 공격당한 시스템/네트워크 세그먼트 분리	전부서
	– 공격자 IP 또는 수상한 IP 주소 접근 통제	보안담당부서
	– 공격당한 서비스 중지	전부서
	– 정보보호 제품의 로깅 강화, 규칙, 엔진 등 업데이트 수행	보안담당부서
	– 패스워드가 유출되었거나 비인가 계정 삭제	해당부서
	– 위변조 파일 식별 및 복구	보안담당부서
	– 긴급 취약성 경고 수신시 권고대응조치 수행	보안담당부서
	– 취약점 패치 수행	보안담당부서

단계	대응 업무	주무부서
	– 백신 엔진 업데이트 및 점검	보안담당부서
	– 필요시 백업 시스템 가동	전부서
	– 공격기법 등에 대한 분석 및 보안조치 결과 보고	보안담당부서
	○ 정보보호 업무수행 강화	
	– 주요 정보 시스템에 대한 백업 주기 단축	전부서
	– 주요 시스템, 보안 시스템, 네트워크 장비 로그 레벨 강화	전부서
	– 로그 검토 및 로그 분석자료 상위기관 보고	전부서
	– 주요 시스템들에 대한 취약점 점검	보안담당부서
	– 정보시스템 사용자, 관리자들에게 상황 전파 및 인식 제고	보안담당부서
	– 새로운 취약점 확인 및 패치 주기 단축	보안담당부서
	– 정보보호 업무 수행 결과 기록 및 보고 수행 강화	보안담당부서
	○ 상위 단계 조치에 대한 주기적인 검토 및 시행 준비	전부서
경계	○ 이전 단계의 모든 조치 시행	전부서
	○ 피해 시스템/네트워크에 대한 조치 (피해 상황 분석 및 긴급/상응 보안 조치 수행)	
	– 필요시 공격당한 시스템/네트워크 세그먼트 분리	전부서
	– 업무 공백을 취소화하기 위한 백업 시스템 가동	전부서
	– 주요 정보시스템의 지속적인 서비스를 위한 백업 채널 가동	전부서
	– 공격자 IP 또는 수상한 IP 주소 접근 통제	보안담당부서
	– 공격당한 서비스 중지	전부서
	– 정보보호 제품 로깅수준 강화, 규칙, 엔진 등 업데이트 수행	보안담당부서
	– 패스워드가 유출되었거나 비인가된 계정 삭제	해당부서
	– 위변조 파일 식별 및 복구	보안담당부서
	– 긴급 취약성 경고 수신시 권고 대응조치 수행	보안담당부서
	– 취약점 패치 수행	보안담당부서

단계	대응 업무	주무부서
	– 백신 엔진 업데이트 및 점검	보안담당부서
	– 공격 기법 등 분석 및 보안조치 결과 보고	보안담당부서
	○ 정보보호 업무 수행 강화	
	– 주요 시스템에 대한 보안감사, 검토의 즉각적 시행	보안담당부서
	– 주요 파일에 대한 즉각적 백업 실시	전부서
	– 상황 총괄하는 상황데스크 설치 및 운영	보안담당부서
	– 컴퓨터, 통신선로, 운영 장소의 물리적 통제를 통한 사고전파 방지	전부서
	– 시스템 운영 필수 계정을 제외한 계정의 일시적인 폐쇄	전부서
	– 피해 상황 파악 및 대상 정보 시스템에 대한 즉각적 복구 조치 수행	보안담당부서
	– 필요시 업무 연속성 보장을 위한 오프라인 업무 수행 대비	전부서
	○ 주요 시스템, 보안 시스템, 네트워크 장비 등의 조치 사항 등을 보안센터에 통보 (컨소시엄 운영센터는 통합운영센터에도 통보)	보안담당부서
	○ 상위 단계에 대한 검토 및 준비 강화	전부서
심각	○ 이전 단계의 모든 조치 시행	전부서
	○ 적절한 보안 조치 시행	
	– 각종 로그의 실시간 검토	보안담당부서
	– 해당 S/W 벤더 접촉을 통한 최신 패치 상태 유지	전부서
	– 내부 네트워크의 외부 접점 단절	전부서
	– 업무 연속성 보장을 위한 오프라인 업무 수행	전부서
	○ 주요시스템, 보안시스템, 네트워크 장비 등의 로그 실시간 분석, 해당 조치사항 등을 보안센터에 실시간 통보 (컨소시엄 운영센터는 통합운영센터에도 통보)	보안담당부서

9. 사고 조사 요령

가. 사고신고

절 차	세 부 내 용
사고 신고	(1) 정보보안사고, 사이버침해사고 및 공격징후 발견 시 사고 일시·장소·사고내용 및 현재 취하고 있는 조치를 보안센터에 통보 (컨소시엄 운영센터는 통합운영센터에도 통보) (2) 사고신고 연락처는 붙임참조

나. 사고 조사 실시

절 차	세 부 내 용
사고 조사 실시	(1) 정보보안사고 전말조사 (가) 보안사고 전말조사는 통합운영센터 및 컨소시엄 운영센터 내 시스템에 불법침입이 발생하여 중요자료가 유출된 경우, 실증단지 정보통신망 장애 및 마비, 기간연계시스템을 통한 불법침입 등 중대 보안사고가 발생한 경우에 해당 (나) 전말조사가 종결될 때까지 관련 내용을 공개하여서는 안 됨 (다) 전말조사는 통합운영센터 및 컨소시엄 운영센터 지원 하에 보안센터가 수행하는 것을 원칙으로 함 (2) 사이버 침해사고 조사 (가) 사이버공격이 특히 다음 각 호에 해당되는 경우 보안사고에 준하여 사고조사 실시 o 기기·시스템·정보통신망 장애 및 마비를 목적으로 하는 사이버 공격 o 기기·시스템에 저장된 중요 자료 유출을 목적으로 하는 사이버 공격

절 차	세 부 내 용
	(나) 통합운영센터장 및 컨소시엄 운영센터장은 보안센터가 사고 조사 시 원인 분석을 위하여 정보통신망의 접속기록 등 관련 자료의 제공 및 피해시스템에 잔존한 해킹 프로그램의 채증 등 증거확보를 요청할 경우 적극협조(구두설명 또는 전자우편으로 갈음할 수 있음) (다) 사고조사는 통합운영센터 및 컨소시엄 운영센터 지원 하에 보안센터가 수행하는 것을 원칙으로 함 (3) 자체 사고조사 (가) 경미한 사고로 판단되는 경우, 정보보안사고 전말조사 및 사이버 침해사고 조사를 보안센터와 협의하여 통합운영센터 및 컨소시엄 운영센터가 자체적으로 사고조사 수행

다. 사고 조사 결과

절 차	세 부 내 용
사고 조사 결과	(1) 조사결과 처리 (가) 통합운영센터장 또는 컨소시엄 운영센터장이 자체적으로 사고조사를 실시한 경우에는 사고조사를 완료한 후 사고조치 서식에 의거하여 사고조치결과 보고서를 작성 유지하고, 사본 1부를 보안센터에 통보 (나) 통합운영센터장 및 컨소시엄 운영센터장은 조사결과에 대하여 필요한 조치를 취하고, 사고 관련자에 대해서는 관계법규에 의거 징계토록 하며 처리 결과에 대해서는 보안센터장에게 통보 (컨소시엄 운영센터장은 통합운영센터장에게도 통보)

라. 증거확보 및 보존 요령

※ 증거확보 및 보존을 위한 세부내용 수행은 보안센터와 협의 후 진행

절차	세 부 내 용	
증거 자료 백업	○ 피해 장비(컴퓨터)의 백업파일 생성 – 로그자료 – 프로세스 정보 – 네트워크 연결 상태 – 파일 시스템 정보 ※ 주의사항 : 피해 장비의 전원차단 실시 등 운영 장비 정지로 사고원인의 증거 발견이 불가능해지지 않도록 주의 (예, 피해 장비의 전원을 차단할 경우 사고원인 및 이상징후를 판단을 위한 증거확보가 어려우므로, 네트워크에서 분리)	
컴퓨터 H/W 파악	윈도우 시스템	○ 내 컴퓨터 등록정보를 이용, 하드웨어 정보파악
	유닉스 시스템 리눅스 시스템	○ dmesq 명령어 이용, 하드웨어 정보 파악
해당 S/W 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
파일 목록 작성 및	윈도우 시스템	○ 모든 파일의 검색 – 검색옵션을 모든 파일을 볼 수 있도록 선택하고 탐색기를 사용하여 전체 파일 현황 파악

절차	세 부 내 용	
조사		○ 특정 파일의 검색 – 검색옵션을 특정 파일을 볼 수 있도록 선택하고 탐색기 이용, 특정 파일 현황 파악
	유닉스 시스템 리눅스 시스템	○ 모든 파일의 검색 – Is」 명령어를 사용하고 「–a」 또는 「–al」 옵션을 사용하여 전체 파일 목록을 확인 ○ 특정 파일의 검색 – 「find」 명령어를 사용하여 특정 파일의 위치를 확인
증거 자료 추출	○ 증거자료 백업매체 – 원본과 동일한 형태, 동일 모델로 저장 보관 ○ 증거자료 추출분석 – 원본과 같은 이미지 복사본을 사용 – 하드웨어적 이미지 복사 : 「Encase」 등과 같은 하드디스크 복사기로 복사 (고가의 정밀수사에 사용) – 소프트웨어적 복사 : 「고스트」 프로그램 사용 ○ 증거자료 분석환경 – 컴퓨터 범죄가 일어난 환경과 동일하게 준비(예를 들어, 동일 환경의 하드웨어 준비 등)	
증거 자료 분석 및 확보	○ 일반적 문서파일 – 특정 키워드가 포함된 문서 검사 ○ 회계 파일 – 사용한 회계용 프로그램 파일 ○ 데이터베이스 파일 – 원본 데이터베이스 무결성 검사 – 데이터베이스 구조, 테이블 구성 조사	

마. 사이버공격 유형별 사고조사 요령

구분	세 부 내 용	
악성 코드 공격	악성코드 사본 수집 및 보존	o 악성코드 분석 및 추후 사고조사를 위해 악성코드 사본을 수집하여 보존 o 수집된 악성코드를 통합운영센터 및 보안센터에 통보
	사고 처리 내역을 기록 유지	o 사후 법적 증거로 활용하거나 상황보고 및 사고 처리 활동에 대한 사후 검토를 위해 악성코드로 인한 사고 발생 시 대응 요령 수행 내역에 대한 기록 유지
서비스 거부 공격	트래픽 분석을 통한 공격자 추적	o 네트워크 스니퍼, MRTG(Multi Router Traffic Grapher) 같은 트래픽 분석 도구를 이용하여 감시되는 트래픽으로부터 공격 근원지를 식별 o 라우터의 트래픽 분석 기능과 스위치의 MAC 주소 테이블을 이용하여 서비스거부공격의 공격자를 추적 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
	후속 공격에 대한 대비책 강구	o 네트워크 트래픽 모니터링 도구를 이용하여 복구활동이 시작되기 전까지 지속적인 네트워크 모니터링 o 네트워크 모니터링으로 후속 공격 발생시, 서비스거부공격 발생 대응요령을 이용하여 공격자를 추적하고 추가적인 증거를 확보
비인가자 접근 공격	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

구분	세부 내용	
	물리적 상황 증거 확보	o 사고기간 중 전산실, 사무실 등의 출입통제시스템의 로그를 확보
복합 구성 공격	개별적 공격에 대한 사고조사 수행	o 복합구성공격에 의하여 사고가 발생한 경우 일어난 사고 각각에 대해 사고조사를 수행

10. 사이버공격 유형별 대응

※ 사고조사에 필요한 자료가 삭제되지 않도록 주의하고, 필요시 보안센터와 협의하여 조치 및 증거보존 수행

가. 악성코드 공격 대응 요령

단계	대응요령
악성 코드 공격 판단	▪ 웜·바이러스 계열의 악성코드는 메일, 공유폴더 또는 취약점스캐닝을 통해서 은밀하고 빠르게 전파되므로 백신프로그램, 침입탐지시스템, 침입차단시스템 등 정보보호시스템과 네트워크 장비의 로그자료 등을 주시 ▪ 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
감염 시스템 분리	▪ 감염된 호스트를 식별 후 네트워크에서 분리하여 악성코드를 분석 ▪ 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 유입경로에 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

단계	대응요령
감염 경로 차단	▪ 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 전파 수단을 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 ▪ 외부로의 연결시도를 차단 o 특정 IRC 서버 또는 백도어 마스터 시스템으로 접속을 시도하고 있는지 여부를 확인하기 위해 시스템에서 주기적으로 외부로 나가는 패킷이 존재하는지 여부를 확인 o 내부 피해 시스템의 악성코드가 외부 시스템으로 연결을 시도하는 경우 라우터나 침입차단시스템의 차단규칙 설정을 이용하여 해당 연결 시도를 차단
외부 네트워크와의 연결 차단	▪ 대규모 피해를 유발하는 악성코드공격으로 인하여 침해사고가 발생한 경우나 대량의 트래픽 발생으로 인해 기관의 인터넷 접속 자체가 불가능한 경우에 기관의 인터넷 접속 경계에서 접속 단절을 권고
미확인 악성코드 대처	▪ 감염이 의심되나 현재까지 알려지지 않은 악성코드는 보안센터에 도움을 요청하여 조치 o 현재 보유하고 있는 백신 프로그램으로 탐지되지 않는 악성코드로 인하여 사고가 발생하였거나 의심되는 경우 보안센터 및 백신업체에 연락하여 조치

단계	대응요령
사고 통보	▪ 악성코드공격으로 인한 사고 발생의 경우 보안센터에 통보 (컨소시엄 운영센터는 보안센터에도 통보)

나. 서비스거부 공격 대응 요령

단계	세부 내용
유형 판단	▪ 보안담당부서 책임자(담당자)는 공격자의 서비스거부공격의 유형을 판단하기 위하여 MRTG와 같은 트래픽 모니터링 도구를 이용하여 네트워크 트래픽 모니터링 ▪ 라우터, 침입차단시스템, 침입탐지시스템 등으로 부터의 로그 기록 정보를 참조하여 공격 증상을 확인
네트워크 장비를 이용한 추적·차단	▪ MRTG 등의 트래픽 모니터링 도구 및 라우터의 트래픽 분석기능을 이용하여 서비스거부공격의 근원지를 추적 ▪ 공격의 특성에 맞게 라우터나 스위치에 CAR 또는 ACL을 설정하여 해당공격을 차단 ▪ 공격의 특성에 맞게 침입차단시스템의 차단규칙, 라우터의 필터링 기능을 설정하여 해당 공격을 차단 ▪ IP 주소를 이용한 공격차단이 스푸핑 공격 등을 통하여 실효성이 적은 경우에는 MAC 주소를 분석하여 차단
정보통신서비스 제공자(ISP) 차단 규칙 적용	▪ 외부 호스트로부터의 서비스거부공격으로 인하여 실증단지 통합운영센터 또는 컨소시엄 운영센터의 인터넷 라우터가 정지 및 오동작하는 경우에 해당 운영센터는 공격차단 및 공격자 추적 등을 보안센터에 요청 ▪ 보안센터는 국가정보원 NCSC를 통하여 각 운영센터의 요청을 관계기관(ISP)에 통보하고 공격차단 및 공격자 추적 등이 사안에 대한 협조 요청

단계	세부 내용
위치 재배치 및 중요 자료 백업	▪ 특정 호스트가 공격 대상이 되고 다른 서비스거부공격 대응 전략이 효과가 없는 경우, 해당 호스트를 다른 IP 주소로 대체 ▪ 피해시스템의 빠른 복원을 위하여 가능한 빨리 백업도구를 이용하여 CD나 저장테이프 등 보조기억장치에 시스템의 데이터를 백업 ▪ 특정 호스트가 공격 대상이 되고 다른 서비스거부공격 대응 전략이 효과가 없고 공격에 대한 피해가 크다고 판단될 경우, 통합운영센터장 또는 컨소시엄 운영센터장의 승인을 득한 후 공격대상 네트워크를 분리
보안 취약점 또는 결함 제거	▪ 취약점이 존재하는 시스템의 서비스를 이용하는 서비스거부공격의 경우, 해당 서비스 포트로 패킷이 유입되지 않도록 침입차단시스템이나 라우터에서 차단규칙을 설정하여 패킷을 차단 ▪ 유사공격의 재발을 방지하기 위하여 보안패치 되지 않은 시스템은 해당 취약점을 각 운영체제별 패치 사이트에서 패치를 다운받아 설치

다. 비인가자 접근 공격 대응 요령

단계	세부 내용
격리 또는 서비스 중지	▪ 시스템의 추가적 피해 및 피해 확산 방지를 위해 가능한 사고 시스템을 물리적, 논리적으로 분리 ▪ 비인가 접근공격 근원지를 식별하고, 라우터・스위치・침입차단시스템의 차단규칙 및 서버시스템의 네트워크 차단규칙 설정을 통하여 사후 비인가 접근을 차단
로그 자료 백업	▪ 비인가 접근공격 근원지를 식별하고, 원인 파악을 위한 중요한 단서로 사용될 로그 자료를 안전하게 백업 및 보관
공격에 사용된 계정 제거	▪ 공격에 이용된 계정을 식별하고 윈도우 시스템의 사용자관리 도구와 유닉스 시스템의 'userdel'명령어를 이용하여 해당 사용자계정을 사용중지 또는 제거 ▪ 내부 사용자가 외부 조직을 공격하는 것과 같은 부적절한 행위를 발견할 경우 해당 사용자를 찾아내어 추가적인 피해를 방지 ▪ 외부에서 내부 네트워크로 비인가 접근공격 시도를 발견한 경우, 보안센터와 협력하여 불법접근 사용자계정의 제거 또는 점검 ※ 사용자 계정 제거 등은 사고조사 시 증거확보 등에 필요한 사항이므로, 보안센터와 협의하여 수행
사고 통보	▪ 비인가 접근공격으로 인한 중대 보안사고 발생의 경우 그 사실을 보안센터에 통보 (컨소시엄 운영센터는 통합운영센터에도 통보)

라. 복합구성 공격 대응 요령

세부 내용
사고별 대응요령을 나열하고 중요도를 판별하여 우선순위에 따라 공격기법별 사고대응절차를 모두 수행

붙 임

1. 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	관 심			
발 령 일	0000년 00월 00일 00시 00분	수 신 일	0000년 00월 00일 00시 00분	
조치사항 요약	o 기관 내 사용자에게 대응책을 작성, 배포 o 전자우편 서버의 Filter를 적용 o 기관 내 감염피해 확인 (피해대수 및 감염PC의 IP)			
조치대상 목록				
조치결과				
특이사항				

※ 제목과 발령일 부분은 경고발령 수준에 따라 해당 경보수준 색으로 함

관심 - 주의 - 경계 - 심각

2. 사고신고 서식

사 고 신 고

기 본 정 보			
기 관 명	00운영센터	부 서	보안담당
성 명	홍 길 동	직 위	과장
전자우편	hong@aaa.co.kr		
연 락 처	전화: 064-111-2222 H.P:01X-111-2222 Fax: 064-111-2222		
사 고 내 용			
사고 일시	2011년 1월 17일 09시 15분	피해IP주소	1.1.1.1
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	6 대 * 피해시스템이 여러대인 경우 피해숫자 기입
사고 내용	홈페이지 자유게시판에 악성 유언비어 게시		
조 치 내 용			
공격자 정보	공격자 ID : jgsew, 접속IP : 2.2.2.2		
피해 현황	실증단지 운영 장애 내용		
긴급조치 실시사항	관련 IP 차단		
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	기관 내 사용자의 PC
아	교육/임시PC	교육장 또는 공용 작업을 위해 여러 명이 사용하는 PC
자	기타	위의 시스템 용도에 없는 경우 서술식으로 기술

나. 사고 유형 목록

기호	사고 유형	설 명
A	경유지 악용	타기관으로부터 해킹시도 항의를 받았거나, 시스템 점검 중 해킹흔적 또는 해킹툴이 설치되어 타시스템에 접속한 기록이 발견되었을 경우
B	자료훼손 및 유출	내부 시스템의 자료가 변조가 되었거나, 대량의 데이터가 외부로 무단송신된 흔적이 발견되었을 경우
C	단순침입 시도	지속적인 스캐닝 공격이 발생할 경우
D	웜·바이러스 피해	운영센터 내의 PC에서 웜·바이러스가 발견되었을 경우
E	홈페이지 변조	운영센터의 홈페이지가 변조되었을 경우
F	홈페이지 접속 불가능	운영센터의 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

3. 사고조치 서식

사 고 조 치

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			
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, 위기조치반, 합동조사팀의 사고조사에 대한 내용을 요약 작성		
피해현황	* 사고대응 조치 전의 피해현황을 요약 작성		
사고대응 조치사항	* 자체긴급대응반, 위기조치반, 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			

4. 사고신고 연락처

사고신고 연락처

기관명	전화	팩스	전자우편	홈페이지
ES-ISAC				
통합운영센터				
보안센터	042-870-2177	042-870-2222	bgmin@ensec.re.kr	
한전 S/P				
KT S/P				
SKT S/P				
LG S/P				
한전 S/T				
SKE S/T				
GS칼텍스 S/T				
한전 S/R				
현대중공업 S/R				
포스코ICT S/R				
한전 S/PG				

5. 실증단지 위기대처 비상연락망

실증단지 위기대처 비상연락망

갱신일 : 11.01

구성원	담당자	이 름	연락처
운영센터	운영센터장		
위기조치반	위기조치반장		
	보안담당		
	계통(서비스)·운영 담당		
통합보안 관제센터 · 보안센터 (보안담당부서)			
계통(서비스)· 전산운영 담당부서			

6. 실증단지 사이버안전 유관기관 비상연락망

실증단지 사이버안전 유관기관 비상연락망

갱신일 : 11.01

구분	기관명	연락처	홈페이지
사업단	사업단장		
	사업단		
보안 센터	보안센터장		
	보안센터	042-870-2177	-
ES-ISAC	ES-ISAC		
통합운영 센터	통합운영센터		
	통합보안관제센터		
컨소시엄	한전 S/P 운영센터		
	한전 S/P 보안담당		
	KT S/P 운영센터		
	KT S/P 보안담당		
	SKT S/P 운영센터		
	SKT S/P 보안담당		
	LG S/P 운영센터		
	LG S/P 보안담당		
	한전 S/T 운영센터		
	한전 S/T 보안담당		
	SKE S/T 운영센터		
	SKE S/T 보안담당		
	GS칼텍스 S/T 운영센터		
	GS칼텍스 S/T 보안담당		
	한전 S/R 운영센터		
	한전 S/R 보안담당		
	현대중공업 S/R 운영센터		
	현대중공업 S/R 보안담당		
	포스코ICT S/R 운영센터		
	포스코ICT S/R 보안담당		
	한전 S/PG 운영센터		
	한전 S/PG 보안담당		

7. 정보시스템 업체 연락처

정보시스템 지원 업체 연락처

갱신일 : 2011.01

	업체명	이름	연락처	목적
Net, PC유지보수, UPS,항온항습기, 기타 업무				
전자결재시스템/ 통합정보시스템				
IT 인프라, 업무포털, 홈페이지				
정보보안,메일 및 인터넷관리				

PC A/S 업체 연락처

순번	업체명	엔지니어	연락처
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			