[별표 10] 주요정보통신기반시설 사고신고서(제21조 관련)

사 고 신 고 서

기 본 정 보			
기 관 명		부 서	
성 명		직 위	
전자우편			
연 락 처			
사 고 내 용			
사고 일시		피해IP주소	
피해시스템 용도		운영체제	
사고 유형		피해범위	
사고 내용			
조 치 내 용			
공격자 정보			
피해 증상			
긴급조치 실시사항			
관련보안제품 운영현황			
그 밖에 사고 관련 내용을 구체적으로 서술			

o 시스템 분류 목록

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

o 사고 유형 목록

기호	사고 유형	설명
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 무단 송신된 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