한국인터넷진흥원 침해사고 분석 절차 안내서

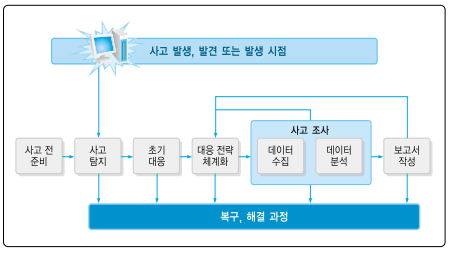
챕터 2. 단계별 침해사고 분석 절차

BoB7기 취약점분석 정성조

# 사고대응 방법론

침해사고의 최근 경향

* 다수의 서버를 공격
* 다수의 서버로 공격
* 대중화
* 범죄적 성향



# 사고대응 전 준비과정

**임기응변**이 가능하도록 관리자와 긴밀한 협조관계와 각 직책별 행동방안을 구축해야함

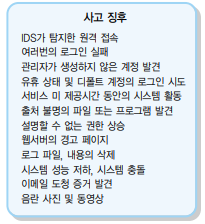
+ 대응 기술 개발, 도구 준비, 사전 보안 조치

방안

* 호스트 및 네트워크 기반 보안 측정
* 사용자 교육
* 침입탐지 시스템 설치
* 강력한 접근 통제(whitelist, blacklist ..)
* **규칙적인 백업**
* 침해사고 대응팀과의 비상 연락망 구축

# 사고 탐지

IDS(Instrusion Detection System) – 예기치 못한 시스템 동작 탐지



**초기 대응 점검표**

* 현재 시간과 날짜
* 사건보고 내용과 출처
* 사건 특성
* 사건 일시
* 관련 하드웨어, 소프트웨어
* 네트워크 연결 지점

# 4절 초기대응

수행되는 모든 행동을 문서화하여 기록

* 로그 분석, 패킷 분석, whitelist, blacklist 분석, etc

# 5절 대응전략 수립

환경의 **전체적** 고려

* 중요도
* 정보의 민감성
* 공격의 크기
* 경제적 피해
* ETC

대응 방법에 따라 기업이 영향을 받을 수 있으니 대응 전략은 조직의 업무 목표를 고려해야 함

* 시스템 다운 시간 및 영향
* 대외 이미지 및 업무 영향
* 지적 재산권 및 경제적 영향

# 6절 사고 조사

**육하원칙**에 따라 조사함

데이터 수집

* 디지털 데이터
* 빅 데이터

수집한 정보는 호스트 기반 정보, 네트워크 기반 정보 등으로 나뉠 수 있음

호스트 기반 정보

* 현재 날짜, 시간
* 소켓(포트)
* 네트워크 인터페이스 상태

네트워크 기반 증거

* (IDS/ 라우터, 인증 서버, 방화벽, etc)의 **로그**
* 합의된 모니터링
* 증거 손상이 가능한 관련자 격리

데이터 분석

모든 수집된 정보의 전체적인 조사

Ex) 로그, 시스템 conf, 웹 브라우저 history, 이메일 메시지와 첨부 파일, etc

# 7절 보고서 작성

컴퓨터를 모르는 사람도 읽을 수 있도록 6하원직에 따라 객관적으로 서술

# 8절 복구 및 해결 과정

* 취약점에 대한 조치
* 시스템 개선이 이루어지고 있는지 추억
* 위험 우선순위 식별