침해사고 분석 절차 안내서

담당 멘토	김종현 멘토님
작성일	2025.08.20
기수	Best of the Best 14th Digital Forensics
이름	최우정

내용

1. 침해사고 분석 절차 안내서 (2010-8 호)

1-1 개요

본 보고서는 한국인터넷진흥원에서 2010 년 발간한 침해사고 분석 절차 안내서이다. 해킹 피해 기관이나 개인이 침해사고를 당했을 경우 적절히 대응할 수 있도록 분석 절차와 기술, 그리고 주요 사고 사례를 제시한다. 특히 악성봇 감염 PC 와 홈페이지 악성코드 은닉 사고 분석에 중점을 두었으며, 운영체제, 네트워크, 데이터베이스에 대한 구체적 분석 기법과 실제 해킹 사례를 통해 실무자가 참고할 수 있는 지침을 제공한다.
10 년 이상 지난 문서이지만, 침해사고 대응의 기본 원칙과 절차를 체계화한 점에서 여전히 유의미하며, 이후 국가 차원의 사고 대응 체계 정립에 기여한 바 있다. 다만 오늘 날 클라우드, IoT, 랜섬웨어, 공급망 공격 등 최신 위협에는 한계가 있다.

1-2 서론

최근 인터넷 침해사고가 금전적 이익을 목적으로 지능적이고 복합적으로 진화하면서 분석과 대응이 어려워지고 있다. 국내 홈페이지 해킹, 개인정보나 게임 정보 유출, 피싱, 악성봇 감염으로 인해 DDoS 공격 및 스팸 발송 등이 주요 피해 유형이다. 본 안내서에는 이에 대응할 수 있도록 분석 절차와 기술을 제공하며, 특히 악성봇 감염 PC 와 홈페이지 악성코드 은닉 사고 분석에 초점을 맞추고 있다.
당시 사이버 공격의 범위와 양상을 포괄적으로 설명했으며, 공격자의 동기가 경제적 이득으로 이동했음을 지적한 점이 인상적이다. 현재도 이러한 추제는 이어지고 있으나, 클라우드 및 모바일 중심 위협은 다루지 못한 한계점이 존재한다.

1-3 침해사고 분석 절차

침해사고 대응은 7 단계로 체계화 된다.

1) 준비 : 대응팀 협조 체계, 도구 준비, 보안 조치
2) 탐지 : IDS, 방화벽, 로그 등으로 이상 징후 식별
3) 초기 대응 : 정보 수집, 사건 유형 식별, 인수인계

4) 대응 전략 : 정책, 법률, 업무, 기술적 요인 고려
5) 조사 : 호스트 기반(로그, 휘발성 데이터, 메모리 등), 네트워크 기반 증거, 기타 증언 확보
6) 보고서 작성 : 명확하고 객관적인 보고
7) 복구 : 원인 제거, 취약점 보완, 재발 방지

위 절차는 현대 디지털 포렌식 절차와 상당히 유사하며, 증거 수집, 분석, 보존의 중요성을 강조한 점이 돋보인다. 오늘날 요구되는 전자증거법, 개인정보 보호법 등 최신 법적 규제 요건 반영은 부족하다고 느껴진다.

1-4 침해사고 분석 기술

운영체제, 네트워크, 데이터베이스별 구체적인 분석 기법이 제시된다.

1) Windows : 시스템, 프로세스, DLL, 네트워크, 레지스트리, 자동 실행, 이벤트 로그, MAC 타임 분석, 루트킷 탐지, 임시 인터넷 파일 분석 등
2) Linux : 프로세스, 포트, 계정, 로그 분석, 루트킷 탐지, 파일 무결성 검증, 웹 로그 통한 취약점 및 웹쉘 확인
3) 네트워크 : 트래픽 모니터링, 패킷 캡처, 공격 패턴 분석
4) 데이터베이스 : MySQL, MSSQL 취약점 점검(계정 패스워드, 권한 관리, SQL Injection 흔적, 보안 패치, 로그 점검 등)

실무에서 즉시 활용 가능한 도구와 명령어 중심으로 구성되어 당시 분석가들에게 유용했을 것 같다. 오늘날에는 사용하기에는 대부분 구식 도구로 보여지고, EDR/XDR, 클라우드 로그 분석 등 최신 기법과는 차이가 난다.

1-5 주요 해킹 사고별 분석 사례

1) 악성코드 은닉 사이트 : iframe/object 코드 삽입, DB 값 변조 등 다양한 웹 해킹 기법과 대응 절차(악성코드 삭제, 로그 분석, 백도어 제거, 취약점 보완, 서비스 재개, 모니터링)
2) 악성봇 C&C 서버 : IRC 기반 봇넷 운영 방식, 분석 도구(sniffer, fport, tcpview, rootkit 탐지 도구), 감염 PC 및 서버 분석, 시스템 원상복구 절차
3) ARP Spoofing 사례 : 감염 PC 가 동일 세그먼트 내 다른 PC 공격, iframe 삽입 및 USB 전파 기능, 네트워크 장애 유발, arpwatch 등 대응 방안

당시 국내외에서 빈번히 발생하던 대표 위협들을 구체적으로 다루어 훈련 자료로 가치가 높았을 것 같다. 그러나 오늘날 공격 양상과는 괴리가 있으며, 최신 위협 사례로 보완할 필요가 있다.

1-6 결론

침해사고 분석 절차를 표준화 및 체계화할 필요성을 강조하며 향후 기술과 환경 변화에 따라 절차와 도구도 고도화해야 함을 언급한다. 이 자료를 통해 실제로 국가 차원의 사이버 사고 대응 지침 및 체계 수립에 영향을 주었다고 볼 수 있다. 다만 기술적 세부 내용과 도구는 상당 부분 구식이므로, 오늘날에는 최신 위협과 도구를 반영한 보완이 필요하다.

2. 정보통신분야 침해사고 대응 안내서(2024.09)

본 안내서는 한국인터넷진흥원이 2024 년 발간한 최신 대응 지침으로, 정보통신서비스 제공자, 기업 정보보호 담당자, 개인 이용자를 대상으로 사이버 침해사고 예방 및 대응 요령을 제시한다.

대한민국이 ICT 강국으로서 IoT, 빅데이터, AI 등 신기술을 빠르게 도입하는 환경 속에서, 사이버 공격의 지능화, 고도화, 대규모화에 따른 피해가 증가하고 있음을 배경으로 한다. 침해사고의 정의와 신고 절차, 법적 의무, 유형별 대응 방법, 시스템별 보안 조치 방안 등을 체계적으로 정리하였으며, 개인부터 기업까지 적용 가능한 범용 지침이라는 점이 특징이다.

2-1 개요

대한민국은 OECD 국가 중 ICT 기술 도입률이 높고, 코로나 19 이후 디지털 전환으로 초연결 사회에 진입했다. 해킹, 악성코드, DDoS, 개인정보 유출, 산업기밀 탈취 등 사이버 위협이 지능화 및 고도화되어 매년 피해가 증가하고 있다. 안내서의 목적은 기업, 개인 모두가 사이버 침해사고에 예방적으로 대응할 수 있도록 지침을 제공하는 데 있으며, 적용 범위는 정보통신서비스 제공자, 기업, 개인, PC 방 등이다.

ICT 환경과 사이버 위협의 변화상을 시의성 있게 설명하여 독자의 공감과 필요성 인식을 높인다. 다만 전체적으로 배경 설명이 많고 구체적인 대응이 부족한 것 같아 실무자보다는 정책 담당자에게 적합한 듯하다.

2-2 사이버 침해사고 신고

침해사고는 정보통신망법에 따라 해킹, 악성코드, DDoS, 서비스 거부, 정보 위변조, 공격 경유지 이용 등 정보통신망 보호 절차를 우회하는 모든 행위가 해당된다. 사고 인지 시 24 시간 이내 과학기술정보통신부 또는 KISA 에 신고해야 하며, 미신고 시 3 천만원 이하 과태료를 부과한다. 개인정보 처리자는 유출 사실을 알게 된 때로부터 72 시간 이내에 KISA 또는 개인정보보호위원회에 신고하고, 정보 주체에게 개별 통지해야 한다. 통지 내용에는 항목, 규모, 시점, 경위, 대응 조치, 연락처 등이 포함되어야 한다.

법적 근거와 절차를 명확히 규정하여 실무 적용성이 높다. 특히 개인정보 유출 시 72 시간 내 신고, 통지 의무는 GDPR 과 유사해 글로벌 규제 수준을 반영했다.

다면 법률 용어가 많아 중소기업 및 일반 사용자가 이해하기 어렵다는 한계가 있다.

2-3 침해사고 조치 가이드

1) 개인 이용자
   보안 카드 전체 요구, 로그인 알림, PC 성능 저하 등 이상 징후를 침해사고 신호로 보고 대응한다.
   대응 방안으로는 정품 소프트웨어 사용, OS/소프트웨어 패치 자동 업데이트, 백신 설치, 데이터 주기적 백업, 공유기 관리자 비밀번호 변경, 사이트별 다른 ID/비밀번호 사용 등이 있다.
2) 기업
   서버, 네트워크, DB, 어플리케이션별 점검 항목과 보안 조치를 제시한다.
   웹서버에는 최신 패치 적용, 관리자 계정 최소화, DMZ 배치, 접근제어 강화, 로그 최소 6 개월 보관, Inbound 트래픽 최소화를 적용한다.
   네트워크 영역에서는 원격 접근 제한, SNMP community 문자열 변경, ACL 설정, 불필요한 서비스 중단. 보안 패치 적용을 할 수 있다.
   DB 영역에서는 기본 패스워드 변경, 원격 접속 차단, 사용자 권한 최소화, test 계정 삭제, MS-SQL 은 게스트 계정 비활성화, 포트 변경, xp_cmdshell 제거 등을 할 수 있다.

개인부터 기업까지 계층적 대응 방안을 제시하여 범용성이 높다. 특히 최신 위협을 반영했다는 점이 장점이다. 그러나 KISA 제공 서비스와 도구 중심으로 서술되어, 글로벌 기업이나 클라우드 기반 보안 운영 환경에는 다소 적용 한계가 있다.

2-4 결론

2024 년 안내서는 2010 년 안내서에 비해 법적 의무와 최신 위협을 반영했다는 점에서 실무적 가치가 높다. 특히 24 시간, 72 시간 내 신고 및 통시 의무는 GDPR 등 글로벌 기준을 수용했다는 점에서 의미가 크다. 개인과 기업을 모두 대상으로 한 점검 항목과 조치 방안을 제공하여 현장 활용도가 높다.
다만 기술적 부분은 여전히 표준 가이드 수준에서 머물고 있고, 클라우드나 모바일, AI 위협에 대한 구체적 대응 전략은 미흡하다. 따라서 본 안내서는 법적

준수와 기본 대응 지침으로는 유용하지만, 최신 SOC 운영이나 클라우드 기반 보안 전략에는 보완이 필요하다.
최근 "공대에 미친 중국, 의대에 미친 한국"이라는 영상을 보게 되었는데, 한국은 세계적인 IT 강국임에도 불구하고 IT 기술자에 대한 지원이 충분하지 않아 인재들이 해외로 빠져나가는 경우가 많은 것 같다. 사이버 위협은 국가 경쟁력과 직결되기 때문에 기술적 대응 지침뿐 아니라 IT 보안 인재의 육성과 지원이 병행되어야 한다고 생각한다. 장기적으로는 기술 발전뿐 아니라 인적 자원의 유출을 막고, 전문성을 강화하는 정책적 지원이 절실한 때인 것 같다.