침해사고대응업무 분석 및 시스템 개발[1)]

김우년, 정윤종, 박정현°, 임채호
한국정보보호센터

Development of Security Incident Response & Handling System

Woonyon Kim, Yunjong Jeong, Jeonghyun Park°, Chaeho Lim
Korea Information Security Agency

요 약

최근 해외 각국에서는 전산망 해킹 등 침해사고를 신속히 처리 및 대응할 수있는 체계적인 업무시스템의 개발과 운영을 통해 침해사고를 효과적으로 처리하고 지원할 수 있는 체계를 구축하고 있다. 하지만 국내에서는 침해사고를 종합적으로 대응할 수 있는 체제의 미비로 침해사고에 대한 효율적인 대응에 어려움이 많다. 따라서 본 논문에서는 종합적이고, 체계적인 침해사고 대응업무 시스템의 설계와 구현 및 운영을 통해 전산망 침해사고의 신속한 처리와 대응의 기반을 마련하고자 한다.

1. 서론

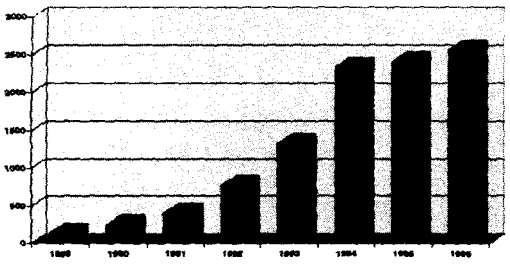
정보의 바다인 인터넷의 급속한 보급과 관련기술의 발달은 전세계를 하나의 전산망으로 묶는 중요한 매개체 역할을 하고 있지만, 이에 대한 부작용도 날로 커져가고 있고, 특히 정보유출, 불법적인 변조 및 파괴 등의 해킹이나 바이러스를 이용한 침해사고가 날로 늘어나고 있다. 최근에는 일반적인 지적탐구, 과시욕 등의 동기를 가진 일반적인 해커뿐아니라 인터넷 등 다양한 전산망을 이용한 전문적이고, 지능화된 해커들이 침해사고를 일으키고 있지만, 이러한 침해사고를 적절히 대응할 수 있는 종합적인 대응체제는 아직 미비한 점이 많다[1][2][3]. 따라서 본 논문에서는 침해사고 대응업무시스템의 개발을 통해 국내 전산망 침해사고 대응업무의 기본시스템으로 활용하여, 침해사고대응팀협의회(CONCERT) 회원기관의 침해사고에 대한 효과적인 공동협력 처리체제를 구축하고, 침해사고 처리과정을 자동화하여 침해사고 분석 및 처리 등의 효율성을 극대화할 수 있다.

1.1 해외 침해사고 현황 및 특징

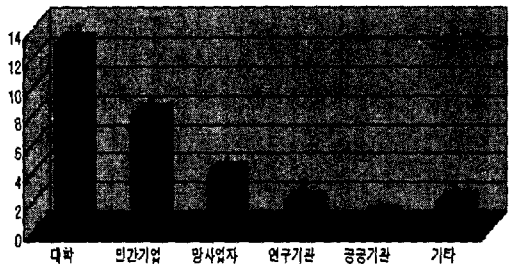
미국의 CERT/CC에서 발표한 자료(그림 1참조)에 의하면 침해사고는 인터넷 등 전산망의 보급이 일반화되기 시작한 1990년초부터 침해사고가 급속한 증가되고 있다.

침해사고에 사용되는 수법도 널리 알려져 있는 단순 취약점이나 사용자의 비밀번호를 추측하여 시스템에 접근하는 수법에서 최근에는 IP 스푸핑(Spoofing), 서비스 거부(Denial of Service)공격 등 새로운 침해수법을 사용하고 있으며, 점차적으로 Java, CGI, PERL, 브라우져 등 WWW에 관련된 보안문제가 많이 발생하고 있다.

1. 이 논문은 정보통신부 국책기술과제인 "정보시스템 침해사고 방지기술개발"의 일환으로 진행되고 있습니다.



(그림 1) 미국CERT/CC 침해사고접수현황



(그림 2) CERTCC-KR 침해사고접수현황

특히 최근 해커들의 해킹수법은 침해수법 및 공격 수법과 도구·방법들이 우수해지고, 복잡해지며, 전반적으로 지능화, 전문화 및 그룹화되어가고 있다.

1.2 국내 침해사고 현황 및 특징

국내 침해사고대응시스템을 운영하고 있는 CERTCC-KR에서는 '97년 9월까지 해킹사고 접수 및 지원한 해킹수법의 현황 및 특징(그림 2참조)을 살펴보면, 30여개 기관에서 침해를 당했고, 침해수법과 특징은 root 계정 불법 획득(시스템 취약점), 홈페이지 변조, 패스워드 유출(스니퍼 등), 스팸메일, 메일폭탄, 서비스거부공격 등의 공격이 일어났다. 피해시스템은 주로 UNIX기종(SUN Solaris, SGI IRIX)이 대부분이고, WindowsNT도 일부 피해를 받았다.

1.3 국내침해사고 사례분석

'97년 상반기에 CERTCC-KR에 접수된 주요 침해사고 사례(표 1참조)를 분석하면 다음과 같다.

(표 1) CERTCC-KR가 접수/지원한 침해사고 사례

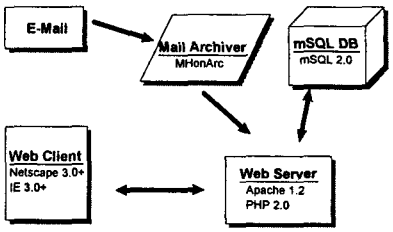
침해수법	사례분석
innd 버그 이용	'97. 8 독일에서 뉴스서버 운영중인 국내 기관의 패스워드 파일 유출
WWW 서버침입 및 패스워드유출	'97. 8 WWW서버 해킹 후 설치한 스니퍼프로그램으로 국내 모대학 패스워드 유출
홈페이지 취약점 및 서버 해킹	'97. 5 대학 전산망운영 홈페이지 자료 변조
해킹경유지 이용	'97. 7 미국에서 침입한 해커가 국내 기업의 시스템 해킹 후 각종 해킹 프로그램으로 미국 인터넷기관들을 해킹
자료 삭제	'97. 5 모대학에 침입한 해커가 각종 연구개발 자료 삭제 '97. 7 지방망사업자에 침입 서비스 중인 BBS자료 삭제
스팸메일	'97. 6 국내 기업의 Email주소를 위장하여 광고성 스팸메일을 송신하여 피해기업이 항의를 받음
Syn Flooding 공격	'97. 6 대학내 UNIX시스템 Ping Attack 으로 시스템 정지 및 Rebooting

2. 침해사고대응 업무관련 연구개발 현황

본 절에서는 침해사고대응시스템 개발현황과 해외 침해사고대응관련 기관의 업무현황에 대해 설명한다.

2.1 침해사고대응시스템 개발현황

미국의 CIAC(Computer Incident Advisory Capablility)의 IRHS(Incident and Request Handling System)은 사고처리 작업모델, 확장성, 보안성, 브라우저, 데이터베이스 독립 및 멀티사용자을 위한 매년/분기별 기록 쉽게 생성하고, 정보에 대한 요구와 사고기록 및 추적 등의 목표로 침해사고 대응업무시스템을 개발하여 수행하고 있다(그림 3 참조).



(그림 3) IRHS 시스템 구조

IRHS에서 사용하고 있는 사고정보는 일반정보와 접촉정보로 구분하여 기록하고 있고, 각 정보의 중요성, 비밀성 등에 따라 공개정보와 비공개 정보로 구분한다. 공개정보는 문서종류/상태, 공격당한 시스템/서비스, 시스템 복구방법 등이 있고, 비공개정보는 신고자(기관) 정보, 조치사항 등이 있다.

그리고 미국의 네트워크장비 생산업체인 CISCO침해사고대응팀, 해커들의 주요 해킹대상인 미국의 NASA 등은 각기 침해사고를 효율적으로 접수, 분석 및 처리를 하기위해 사고접수 초기에 충분한 정보를 수집·처리하고 있다. 다음 (표 2)은 주요 침해사고대응팀에서 침해사고을 정확한 처리하기 위해 사고접수 및 처리단계에서 참고하는 기록/분석 항목이다.

(표 2) 침해사고 접수 및 분석항목

침해사고대응팀	침해사고 접수 및 분석 기록항목
ASSIST	- 고객정보(CERT#, AFCERT#), 기관정보(기관명 : 도메인명) - 사고형태(침입, 침투, 바이러스 등), 사고에 관련된 침해사고대응팀명 - 침해사고로 손상된 시스템(호스트명 : IP주소 : 하드웨어 : 운영체제 : 버전 등) - 사고 현황(침입방법, 시간, 관련정보 등) - 다른기관들과 관련된 정보(호스트 명, IP주소)
NASA	- 사고 시스템 정보(운영체제, 버전, 네트워크 주소 등) - 사고 시스템의 감사로그(사고당시 시스템 로그 정보) - 사고 정보(실지 일어난 침해사고 정보)
Uni-Cert	- 일반 정보(사고번호, 기관정보(기관명, 도메인명, 기관 성격 등) - 연락처 정보(신고자정보, 업무대행자 정보, 사고에 관련된 다른기관의 정보 등) - 피해시스템 정보(호스트명, IP주소, 네트워크 정보, 손상규모 등) - 사고정보(날짜, 시간, 대응절차, 피해시스템 이용현황 등) - 사고유형(침입수단, 침입유형, 침입방법 등) - 보안도구(보안 도구 사용여부 및 사용도구명)

2.2 해외 침해사고대응관련.기관의 업무현황

국제 침해사고대응팀 협의회(FIRST : Forum of Incident Response and Security Teams)는 미국의 NIST를 중심으로 결성되었으며, 각국의 전산망 및 정보시스템 침해사고의 방지를 위한 대응조치의 일환으로 정부, 학계, 민간단체 등 55여개기관으로 구성되어 있고, 각국의 개별 기관들의 보안에 대한 정보공유, 일반적인 문제해결 그리고 앞으로의 전략을 계획하는 등의 일들을 함께 할 수 있는 Forum으로서 역할을 수행한다.

NIST/CSRC(미국)은 컴퓨터보안 관련 위협에 대한 정보, 취약성 정보, 해결책정보를 제공하고, 주로 보안 사고경보 시스템, 뉴스레터, 다른 컴퓨터 보안 서버 정보, 정책, 보안 툴 정보, 바이러스에 대한 정보, 보안 관련 훈련 서비스 등이 있다.

CERT-CC(CERT Coordination Center, 미국)는 긴급사태에 대응하여 전산망 기술 지원하고, 사용자 보안의식, 사고대응 능력 향상, 시스템 평가, 보안취약성의 발견 및 보안 등을 담당하는 연구기관들의 협력 창구을 한다. 또한 CERT는 CERT Advisory, 보안 도구에 대한 정보, 보안 취약점에 대한 정보, FAQ, 연례보고 등의 자료를 제공한다.

AUSCERT(호주)는 호주의 유일하고 신뢰성있는 인터넷상의 보안기술서비스 접속점으로 침해사고와 예방기관의 역할을 담당하고, 침해사고 예방, 네트워크 기술 및 보안에 관련된 기술을제공한다. 또한 시스템의 취약성, 방어전략, 공격경고 등에 대한 정보를 수집, 분석, 관리 및 보안 관련 정보, 도구 및 기술의 제공처로서 활동한다.

DFN-CERT(독일)은 1993년에 독일최초로 국가망의 CERT로, 보안사고의 접수 및 처리업무를 수행하여 접수된 침해사고 등을 지원하고, 유럽의 FIRST정보와 WWW 연결, WWW 서버, FTP 서버 등을 운영한다.

CERT-IT(이태리)는 1994년 인터넷상의 사용자 보안문제 해결위해 밀란대학 전산과에서 구성되어 있고, 국내외 침해사고를 분석, 이탈리아 인터넷 사용자를 위해 보안점검 분석정보 제공한다.

CERT-NL(네덜란드)는 네덜란드 연구교육망인 SURFnet의 컴퓨터사고대응팀으로 해킹, 보안 취약성 및 바이러스와 관련있는 컴퓨터 및 네트워크상의 사고 처리하고, 보안관련 BBS, 보고서, 논문, 도구, FAQ 등을 제공한다.

3. 침해사고 대응업무 분석

3.1 침해사고 업무분석

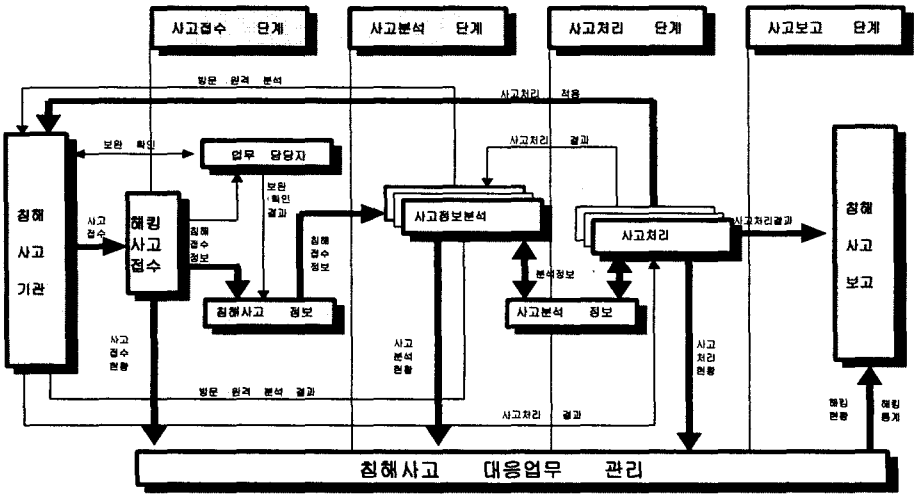
침해사고 대응팀의 일상적인 업무(그림 4참조)는 사고접수, 사고내용 분석, 사고결과 처리 및 필요한 사항을 보고하는 단계로 크게 나눈다.

① 사고접수 단계

사고 접수단계에서 사고기록의 작성은 프라이버시를 유지하면서 사고처리와 관련된 모든 활동 및 수집된 주요 정보들은 사고 문서, 복구 또는 사후 참조 및 증거 자료로서 기록해야 한다.

② 사고분석 단계

사고 분석단계는 사고의 재발방지, 사고의 근원 및 침입경로 파악 등을 위해 침입수법, 가해수단, 침



(그림 4) 침해사고대응업무 처리과정

입경로 등을 파악해야 하고, 점검 및 분석과정을 체계적·반복적으로 하여 그에 따른 평가결과를 피드백(feedback)을 통해 분석절차를 개선해야 한다.

사고분석을 정확히 하기위해 다음 순서로 분석한다.

- o 사고접수된 내용을 적시 파악
- o 미비한 사항 사고기관에 원격/방문 확인/재요청 등을 통해 상세한 사고 내용 파악
- o 임시초치할 수 있는 사고분석 결과 도출
- o 분석결과 검토, 최종분석 결과 도출, 분석결과 보고

③ 사고처리 단계

사고 처리단계에서는 분석한 결과정보를 가지고 침해사고가 발생한 기관에 조치한 내용을 기술하고, 조치사항는 간단 명료해야 하며, 사용자의 기술 수준에 따라 조절한다. 그리고 사고처리에 관련된 모든 활동 및 수집정보들은 사고의 분석, 복구, 또는 사후 참조 및 증거 자료로서 기록되어야 하고, 사고에 대한 필요한 조치사항은 다음과 같다.

- o 사고 이전 상태로의 복원, 사고의 재발 방지 및 사고의 근원 및 침입경로 파악
- o 조치단계에 대한 피해당사자의 요구사항, 사고의 규모, 예상되는 소요인력 파악
- o 현재 가용한 인력 등을 종합적으로 고려하여 지원방침을 결정

3.2 침해사고 대응절차

효과적으로 침해사고 대응업무을 수행하기 위해서는 정책 및 절차 수립, 사고접수, 분석, 조치, 보고, 피해복구 등 단계적으로 수행해야 한다. 다음과 같은 침해사고 대응절차가 필요하다.

- o 침해사고대응정책 및 절차수립 : 물리적, 기술적, 관리적 측면을 고려한 정책 및 절차 수립
- o 사고 접수 : 신고자/접수자 정보, 피해상황, 지원내용 등을 침해사고 양식에 의해 상세히 기록 접수하고, 반드시 접수한 사람과 기관을 확인해야 한다.
- o 사고의 분석 : 접수내용을 바탕으로 체계적으로 원격 또는 방문 등을 이용 사고를 분석
- o 사고조치 및 결과 보고 : 접수된 침해사고를 적절히 조치하고 결과는 사고기관(기업) 또는 관련 기관(필요시) 등에 보고 조치
- o 그리고 동일 사고재발 방지를 위한 대책의 수립 및 검증이 필요하다,

3.3 침해사고 대응 기술

현재 국내 전산망은 침해사고에 대해 대응하기 위한 전문인력들이 부족하고, 각각의 전산망 운영 기관들은 침해사고에 대비한 정보보호 기술의 구현과 관리보다 전산망의 운영에 급급하기 때문에 전산망에 대해 정보보호가 이루어지지 않아 외부의 침입에 대해 거의 무방비 상태라고 볼 수 있다. 이러한 배경에서 침해사고대응은 전문적인 침해사고 대응지원팀에서 이루어져야하며 주요 임무는 다음과 같다.

- o 침해사고 예방을 위한 기술지원,
- o 침해사고의 접수, 분석을 위한 기술지원,
- o 침해사고 확산 방지를 위한 침입자 분석, 추적,
- o 침해사고 예방을 위한 권고문서의 작성 및 배포

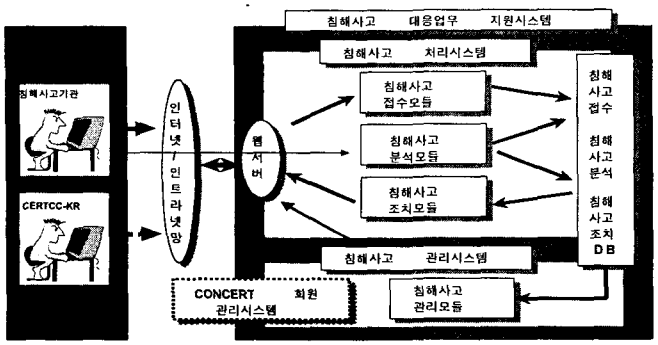
대응팀의 구조는 전체 대상기관의 규모, 관련 기술의 다양성, 각 대상기관내의 보고체계 및 정보보호 체계, 그리고 지리적 분포 등에 따라 다양한 형태를 가질 수 있다. 구조로는 모든 대상기관이 집중적으로 침해사고 보고하여 하나의 대응팀이 업무를 지원하는 경우인 중앙집중형, 기관수, 서비스가 많거나, 기관별 성격이 달라서 하나의 대응팀이 업무를지원하기 어려울 때 구성되는 분산형, 중안집중형과 분산형 절충절충형으로 구분할 수 있다.

4. 침해사고 대응업무 지원시스템

침해사고 대응업무 지원시스템은 인터넷을 통해 침해사고기관이 사고접수를 할 수 있도록 WWW환경에서 수행하는 것으로 크게 침해사고 접수모듈, 침해사고 분석 모듈, 침해사고 분석 모듈, 침해사고 처리모듈의 침해사고 처리시스템과 침해사고 현황파악/통계자료/보고서 작성 지원 모듈 등의 침해사고 관리시스템으로 구성된다(그림 5참조). 그리고 침해사고대응팀협의회 회원관리 업무를 수행하는 시스템도 포함한다.

침해사고 대응업무시스템의 주요기능은 다음과 같다.

- o 침해사고 접수/분석/조치 과정에 관련된 내용을 정형화하여 저장(DB)하는 기능
- o 침해사고 접수/분석/조치를 위해 기존정보를 활용할 수 있도록 하는 검색기능
- o 침해사고 접수/분석/조치 과정 및 결과에 대한 현황, 통계 및 보고기능
- o 침해사고대응팀 협의회 회원의 등록/수정/삭제/통계 및 보고기능
- o 침해사고 접수상황 알람(삐삐, 경보 등)기능
- o 접수 건당 문서번호 자동할당 기능

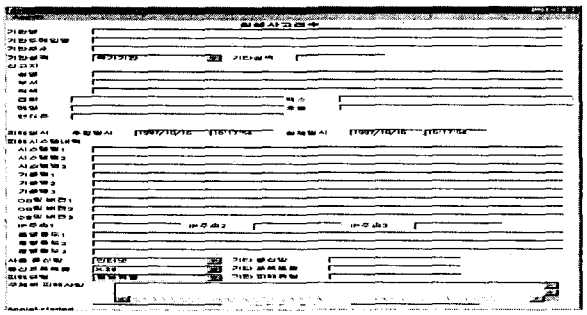


(그림 5) 침해사고 대응업무시스템 구조

4.1 침해사고 처리시스템

4.1.1 침해사고 접수모듈

침해사고 접수모듈은 침해사고 처리/관리시스템을 접근하기 위한 모듈로 시스템관리자, 접수담당자 또는 침해사고 처리/관리시스템의 접근이 허락된 침해사고 기관 및 관련담당자에게만 접근을 허락한다. 이때 침해기관에서 접수한 사고정보는 침해사고를 당한 기관(사용자)의 피해시스템/네트워크의 정보, 피해사항, 신고자 일반정보 등의 정보가 있다. 주요기능은 접수내용을 자동적으로 DB화하는 기능, 사전 등록 기관(자)을 접수시 관련정보 자동 입력기능을 가지고 있다.

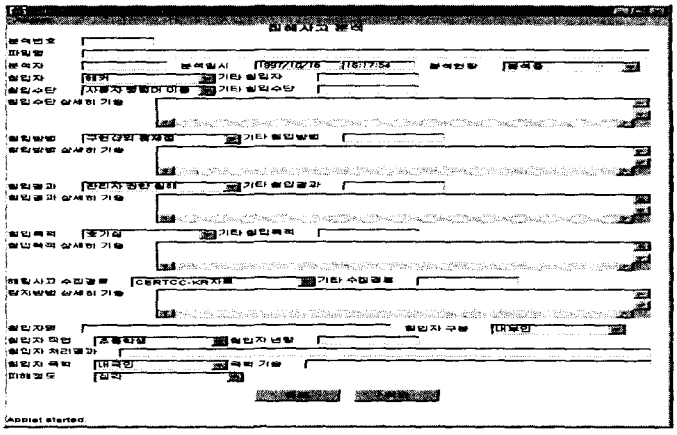


(그림 6) 침해사고 접수화면

4.1.2 침해사고 분석모듈

침해사고 분석모듈은 침해사고 접수된 사항과 현장방문 등에 의한 획득한 정보들을 바탕으로 침해사고를 분석하는 모듈이다. 그리고 침해사고 분석은 사고접수된 시점부터 사고가 정확히 종료되는 시점까지 철저한 분석을 통해 침해사고 재발방지를 원칙으로 한다. 주요기능은 사고접수 내용 접근/편집 기능, 침해사고 DB 활용기능 등이 있고, 분석정보 항목은 분석자명 등의 일반정보와 분석도구, 분석방법 및 분

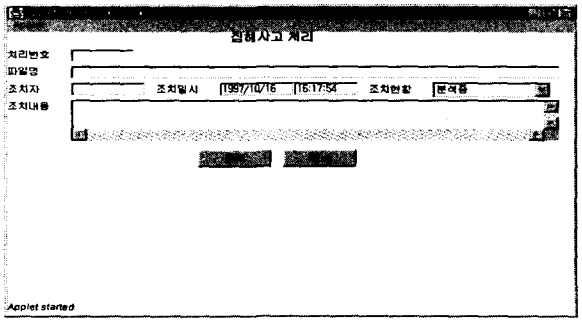
석내용 등의 분석정보를 가지고 있다.



(그림 7) 침해사고 분석화면

4.1.3 침해사고 처리모듈

침해사고 처리모듈은 침해사고 분석모듈에 분석한 정보를 가지고 침해사고가 발생한 기관에서 처리한 내용을 기술하는 모듈이다. 주요기능은 사고분석 내용 접근/편집 기능, 처리결과 정보 DB화 기능 등이고, 사고처리 정보항목은 처리자명 등의 일반정보와 처리도구, 처리방법 및 처리내용 등의 처리정보를 가지고 있다.

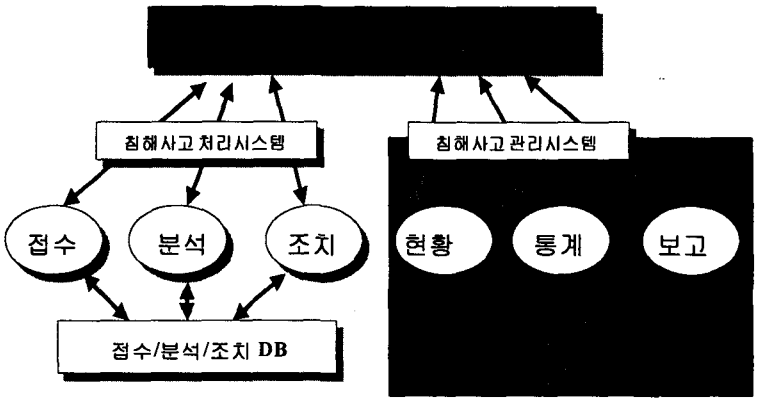


(그림 8) 침해사고 처리화면

4.2 침해사고 관리시스템

침해사고 관리시스템은 침해사고 대응업무의 전과정을 침해사고 대응업무 담당자/관리자가 현황을 파악할 수 있고, 현황 분석, 현황 통계 등을 통해 불법침입자들의 동향을 파악, 침해수법 연구 등의 기초자료로 활용할 수 있는 시스템이다.

주요기능은 침해사고 기간별 현황 파악기능, 침해사고 주간/월간/년간 통계 기능 및 침해사고 접수/분석/조치 보고기능이다. 특히 통계자료는 국내 정보시스템 해킹·바이러스 현황 및 국내외 관련 기술동향 파악, 침해사고 방지대책 수립시 활용할 수 있는 기초자료로 매우 중요하다.



(그림 9) 침해사고 관리시스템

5. 결론 및 향후계획

본 연구를 통하여 인터넷 등 전산망에서의 해킹과 불법침입에 대한 침해사고 현황 및 이에 대한 대응업무시스템 설계 및 구현에 대해 살펴보았다. 국내에서는 다소 미비한 대응체계시스템 구축으로 효과적이고 구체적인 대응업무 진행에 차질이 많고, 자체적인 관련기술력 확보와 제품이 발표되지 못하여 이 연구를 통해 보다 안정적인 국내 망운영과 침해사고에 대한 대응체제 확보에 노력하고자 한다.

본 연구에서는 국내외 침해사고 현황 및 침해사고 관련업무을 분석하고, 이를 바탕으로 침해사고대응업무 기본시스템을 설계·구현하였다. 여기에서 제시되고 연구된 기술들은 국내 전산망의 안정화와 침해사고에 대해서 신속한 처리와 대응업무를 자동화할 수 있는 기반을 마련할 것이다.

본 연구과제에서 제시된 기본시스템 구현을 바탕으로 '97년까지 기본시스템을 구현 및 운영하고, '98년까지 종합적이고 체계적인 침해사고 대응업무 시스템을 개발할 예정이다.

[참고문헌]

[1] 한국정보보호센터, 정보보호총서, 1996.12
[2] 임채호외 6명, "정보시스템 해킹방지 기술 현황 및 시스템 설계", '97 WISC논문집, 1997, 10
[3] 한국정보보호센터, 정보시스템 해킹현황 및 대응, 1996.11.
[4] Russell L. Brand, oping with the Threat of Computer Security Incidents : A Primer from Prevention through Recovery", CERT/CC, CMU, PA. CERT V0.6. Jun. 1990.
[5] Danny Smith, "Forming an Incident Response Team", AUSCERT, Univ. of Queensland. Brisbane, Qld. - Jul. 1994.

[6] John P. Wack , "Establishing a Computer Security Incident Response Capability(CSIRC)", NIST, NIST, Md. - NIST Special Publication 800-3, Nov. 1991.
[7] "Computer Emergency Response Team System (CERT System): Operational Framework" Members of the CERT System. - Nov. 16, 1990.
[8] "The CERT Coordination Center FAQ", CERT/CC, CMU, Revision 7. - January 1993.
[9] "Forum of Incident Response and Security Teams (FIRST) Operational Framework", FIRST, Sep. 1992.
[10] E. Eugene Schultz Jr., David S. Brown and Thomas A. Longstaff, "Responding to Computer Security Incidents", CIAC, LLNL, CA. Jul. 1990.
[11] E. Eugene Schultz Jr, "The Computer Emergency Response Team System CERT- SYSTEM", CIAC, LLNL, CA. Oct, 1991.
[12] G. S. Stewart and D. Sylvester, "Potential Liabilities Of Computer Security Response Centers Arising From Notification To Publishers And Users Of Security Deficiencies In Software" . Dec. 1989.
[13] B. Y. Fraser and R. D. Pethia, "The CERT/CC Experience: Past, Present, and Future" CERT/CC, INET'92. - Kobe, Japan. - June 15-18, 1992. - p. 203-208.
[14] P. Holbrook (CICNet, US) and J. Reynolds (ISI, US), "Site Security Handbook", RFC1244, FYI8. Jul. 1991.
[15] CEC, "Incident Reporting - A European Structure: Database Structures" Commission of the European Communities (CEC/DGX111-B). - Report No. 19733(S2003/WP08). - Oct. 1992.
[16] "IT Security Incident Analysis Services (IAS)" International Organization for Standardization ISO/IEC JTC1/SC27/WG1. SC27/N882, SC27/WG1/N457Rev. May 1994.
[17] Katherin T. Fthen, " Future of Incident Response" 8th FIRST workshop, July 1996.
[18] Sandy Sparks & Rich Pethia, "Practical Intrusion Dection Introdution", 1997. 6, FedCIRC
[19] John Fisher, "Incident and Request Handling System", 9th FIRST workshop, June 1997.
[20] http://www.certcc.or.kr
[21] http://www.cert.org
[22] http://www.auscert.org.au
[23] http://www.cert.dfn.de/eng
[24] http://idea.sec.dsi.unimi.it/cert-it.html
[25] http://www.nic.surfnet.nl./surfnet/security
[26] http://cs-www.ncsl.nistgov/abstract.html
[27] http://www.first.org