국내 전산망 침해사고 대응체계 구축과 운영

Construction and Operation of Security Incident Response in Domestic Computer Networks

이현우, 정윤종, 신훈, 임휘성, 최운호, 임채호
한국정보보호센터

요약

인터넷을 중심으로 글로벌네트워크화 되고 있는 국내 전산망에서는 국내외 해킹 등에 의한 전산망 보안 침해사고가 매우 우려될 뿐 아니라 빈번히 발생되고 있다. 하지만 이에 대한 대책과 기술이 제대로 이루어지지 않고 있으며, 해외의 전문 침해사고대응에 비해 매우 열악한 상태에 있으므로 침해사고의 예방, 사고시 분석 및 확산 방지 및 방지책 개발과 이의 상호 정보 공유 방법을 제시하고 운영하고자 한다.

1. 배경 및 필요성

1988년 서독 간첩해커 사건[34]과 1989년 인터넷웜(Worm)사건[35]은 인터넷 등 전산망에서의 침해사고에 대한 근본적인 기술지원과 여러 전산망 기관을 경유한 침해사고에 대응하기 위해 CERT/CC(Computer Emergency Response Team/Coordination Center)가 미국방부의 지원 하에 카네기멜런대학 소프트웨어연구소 내에 만들어져 활동하기 시작하였다[1].

그리고 여러 전산망에서 CERT 와 유사한 침해사고대응팀(IRT, Incident Response Team)들이 구성되면서 상호 정보 교환 및 침해사고 공동 대응의 필요성에 따라 미 정부의 지원에 의해 NIST가 사무국을 운영하면서 FIRST(Forum of Incident Response Security Team) 이 발족되었고, 현재 북미, 유럽, 아·태지역 에서 팀들이 가입하여 총 55개 팀들이 가입한 국제적 침해사고 대응 협력기구로서 발전하고 있다.

최근 국내에서는 해킹에 의한 침해사고가 매우 늘고 있으며 일반적인 지적 탐구, 과시욕 등에 의한 일반적 해커 뿐 아니라, 인터넷 해킹을 이용한 홈뱅킹사기사건[26] 등 동기가 다양화, 지능화되고 있으며, 해외 해커에 의한 국내 기업체 및 대학 등 해킹, 우회 경로 이용하기 위한 해킹 등이 매우 우려되고 있으며, 해외에서는 무작위적인 서비스거부(Denial of Service)공격으로 인터넷 서비스제공업체의 도산 위기, 은행에 대한 공격으로 불법 예금인출[27], 미 백악관, CIA, DOJ 등 홈페이지에 대한 해킹 등 다양한 침해사고들이 나타나고 있다.

하지만 국내에서는 이러한 해킹에 의한 침해사고에 대해 전문적으로 대응할 수 있는 시스템관리자나 보안전문가가 매우 부족한 상태이며, 이를 지원해주는 기관이나 조직이 미비한 실정이다. 1995년 한국전산망협의회(KNC, Korea Network Council) 산하에 발족한 CERT-KR[28], 1996년 발족한 국내 ISP(Internet Servicce Provider) 들의 보안 협의회인 IR-Forum(Incident Response Forum) 등이 있으나 예산 부족 및 인력 부족 등으로 인하여 활동이 미비한 상태이며 전반적인 국내 전산망에 대한 활동이 미비한 상태이다.

본 논문에서는 국내 여러 전산망에서의 침해사고시 효과적인 대응을 위한 체계를 제시하고자 하며, 이를 위해 국내외에서의 현황을 살펴보고 전산망을 운영하는 기관이 어떻게 하면 침해사고 대응팀을 만들 수 있고 효율적인 운영을 할 수 있는지 제시하고자 한다.

2. 국내외 현황

2.1 국내 현황

2.1.1 한국 전산원(NCA) 대응팀[29]

한국 전산원(NCA)은 '94년 2월에 설립되어 표준본부내 보안기술팀에 네트워크 기술그룹, 시스템

기술그룹 및 위험분석 기술그룹의 기술분야 중심으로 구성되어 있다. 주요업무는 네트워크상의 보안기술 개발 및 보급, 네트워크 침해 대응기술(감지, 분석, 차단 등) 확보 및 국가기간전산망 및 정부기관 네트워크사용자의 보안의식 및 대처능력을 제고하고, 유닉스시스템 보안기술 개발 및 보급과 컴퓨터 바이러스 백신프로그램의 연구/개발을 수행하고 있다. 이외에 위험분석 기술그룹에서는 위험분석 기술확보, 위험관리 기법의 보급을 등을 담당하고 있다..

2.1.2 한국전산망협의회(KNC) / IR-Forum[30]
한국전산망협의회(KNC : Korea Network Council)와 IR-Forum(Incident Response-Forum)은 1996년 3월에 설립되었으며, 주요 업무로는 ISP(Internet Service Provider)간 보안침해정보 공유 및 침해사고에 신속하고 효율적으로 대처하며, ISP간에 보안관련 기술정보를 공유하고, 외국기술을 국내에 이전하며, 보안관련 교육과 홍보활동을 내용으로 활동하고 있다. 구성을 살펴보면 의장, 사무국 및 2개의 실무소그룹으로 구성되어 있는데, 침해사고대응 소그룹은 의사운영위원회로 구성되어 기능을 수행하고, IRF-Tech 소그룹은 IRT에 대한 기술지원을 하고 있다.

2.1.3 시스템공학연구소(SERI) / CERT[28]
시스템공학연구소(SERI)/CERT는 '94년에 설립되어, 활동하고 있으며, 구성은 의장(1명) 및 3 개 실무그룹으로 운영되며, 전산망 지원 그룹(SERI-CERT/Internet Support Group)에서는 국내 인터넷 망 제공자들의 지원 및 권고, 전문가 그룹(SERI- CERT/ Internet Security Expert Group)에서는 국내 보안전문가들이 자발적으로 참여하는 그룹으로서 보안문제에 대한 해결을 지원하며, 운영자 그룹에서는 전반적인 CERT활동을 총괄한다. 주요 업무로는 보안사고의 접수 및 해결 지원, 국제적 보안사고 협력, 보안사고 예방 문서서비스 그리고 보안관련 연구개발 지원과 정보서비스를 제공하고 있다.

2.1.4 경찰청 해커 수사대(Hacker Investigation Team)[31]
경찰청 해커 수사대(Hacker Investigation Team)는 '92년 "컴퓨터범죄 담당자"를 선임하여 운영되다가 '95년 10월 16일 "해커 수사 전담반"으로 확대된 뒤, '96년 2월 16일 "해커 수사대" 로 발족하여 활동 중에 있다. 그 동안 진행되어 온 주요활동상황을 보면 국제 해킹 사건은 3건을 규명하였으며, 국내 해킹 사건으로 3건에서 5명을 검거한바 있다. 해커수사대는 경찰청 한국인터폴내에 해커수사대로 구성되어, 주요 업무로는 보안에 대한 신뢰성 제고, 국내 전산망 및 전산망사용자의 안전을 보호하며, 국가정보보호, 정보화촉진 및 발전과 정보서비스 이용 활성화를 유도하고, 보안기술 발전에 능동적으로 참여하여 국가간에 있어서 정보우위를 점유하고자 한다.

2.1.5 기타
그 밖에도 서울지검에서는 정보범죄수사센터, 대검찰청에서는 정보범죄대책본부 등이 정보범죄 수사차원에서 활동하고 있다.

2.2 해외 현황

2.2.1 CERT-CC(미국)(CERT Coordination Center)(http://www.cert.org/)
미국의 CERT/CC는 1988년 발족이래 매년 2배씩 증가율을 보이는 침해사고들을 접수받아 처리하였으며 1995년에는 약 2500여건의 침해사고를 처리하고 약 16%에 달하는 침해사고를 해결하였다. 주요활동으로 긴급사태에 대응하여 연구기관망을 지원하며, 또한 사용자 보안의식, 사고대응 능력 향상, 시스템 평가, 보안 취약성의 발견 및 보안등을 담당하는 연구기관들의 연결장소로서의 기능을 가지고 있으며 주요 제공정보는 CERT Advisory, CERT FTP Archives, FAQ, Annual Report 등이 있다[1][5][11][12][19][21]

2.2.2 AUSCERT(호주)(http://www.auscert.org.au)
AUSCERT는 호주에서 유일하고 신뢰성 있는 인터넷 상의 접속점으로 보안사고와 예방기관이며, FIRST의 회원이고 US/CERT-CC, 다른 나라의 대응팀(IRTs) 그리고 호주 연방경찰과 서로 잘 연결되어 있으며, 설립목적은 전산망 침해 가능성을 줄이고 계속적인 피해의 위험을 줄이는데 있다.[23]

2.2.3 DFN-CERT(독일)(http://www.cert.dfn.de/eng/)
DFN-CERT는 1993년에 독일 최초로 국가망의 CERT로서 FIRST에 가입하였고, 설립목적으로는

보안사고와 새로운 보안취약성을 처리하고, 접수된 침해사고 처리를 지원하며, 유럽의 FIRST정보 및 연결목록(Link list)이 제공된다.[15][17]

2.2.4 CERT-IT(이탈리아)(http://idea.sec.dsi.unimi.it/cert-it.html)
1994년 2월에 설립되어 이탈리아 인터넷상의 사용자 보안문제를 해결하기 위해 밀란 대학 전산과에서 구성하였고, 또한 미국의 CERT/CC 같은 유럽 네트워크의 대응팀을 만들기 위한 TERENA (Trans European Research and Education Networking Association)에 참여하고 있다. 전세계적인 협력체제를 구축하여 알려진 침해사고를 분석하며, 이탈리아 인터넷 사용자를 위하여 보안측정 정보, 다른 CERT들과의 긴밀한 협조로 최신 정보를 제공하며, 상업용 제품의 결함을 경고하기 위하여 소프트웨어 생산자와 직접 정보를 교환한다.

2.2.5 NIST/CSRC(미국) (http://cs-www.ncsl.nist.gov/abstract.html)[25]
NIST/CSRC는 컴퓨터 보안 관련 정보를 통합하여, 그 정보가 완전하고 정확하도록 보증하며, 최신 정보를 발견하기 쉽게 하고 얻기 쉽게 제공하여 항상 최신의 정보를 제공할 목적으로 설립되었으며, 주요 관심은 컴퓨터보안 관련 위협에 대한 정보와 취약성 정보, 솔루션정보를 제공하는데 있고, Clearinghouse는 일반적인 위험, 프라이버시, 법적 문제, 바이러스, 보험, 정책, 훈련 등과 같은 다양한 주제들에 대한 컴퓨터 보안 정보에 대한 일반적인 인덱스로서의 역할에 주력하며, NIST는 FIRST와 협력하여 시스템 및 네트워크 관리자에게 새로이 알려진 보안 정보를 신속히 제공하는데 주력하고, 데이터베이스를 강력하고 액세스하기 쉽게 만들어 보안관련 자료를 제공한다. 주요 제공정보는 보안 사고 경보 시스템,뉴스레터,다른 컴퓨터 보안 서버 정보, 정책, 보안 툴, 바이러스, 보안 관련 훈련 서비스, 프라이버시, 위험, 바이러스에 대한 포럼을 제공한다.

2.2.6 PCERT(미국) (http://www.cs.purdue.edu/pcert/pcert.html)
보안과 컴퓨터 시스템을 강화하려는 대학내의 사람들을 지원하기 위하여 설립되었으며, 컴퓨터 보안 사고에 대비하는 각 대학별 부서간의 연락 프로토콜을 포함하여 보안문제에 대응하는 표준을 개발하고, 대학내 뿐만이 아니라 외부기관들과 컴퓨터 보안 이슈에 대한 연락처로 활동하며, 컴퓨터 시스템의 버그,설정에 대한 정보, 보안정보를 수집\배포한다.

2.3 국제적 침해사고 대응 현황 - FIRST(Forum of Incident Response and Security Teams)[10]

FIRST는 미국의 NIST를 중심으로 FIRST를 결성하여 각국의 전산망 및 정보시스템 침해사고의 방지를 위한 대응 조치의 일환으로 정부, 학계, 민간단체 등이 가지고 있는 대응능력을 체계적으로 구축하고 있으며, 각 국의 침해사고대응팀을 회원으로 구성하여 55개 기관이 FIRST에 가입하고 있다. 각국의 개별 기관들의 보안에 대한 정보공유, 일반적인 문제해결 그리고 앞으로의 전략을 계획하는 등의 일들을 함께 할 수 있는 포럼을 운영한다.

현재 년 1회 1주일 정도의 정기총회와 전자우편그룹(Mailing List)운영으로 정보를 교환하며, 회원 및 유관조직과의 공동 활동을 하고 있으며, 운영위원회, 연구회 등으로 구성되어 있다. FIRST 회원과 유관조직으로 가입하려면 기존 회원의 추천에 의하여 운영위원회 2/3이상의 찬성이 필요하다. 모든 가입기관은 운영비를 납부해야 하며, FIRST의 활동을 지원할 의무가 회원에게 있다.

2.4 해외침해사고팀의 향후 방향[32]

2.4.1 예산확보 방법의 변화
정부나 공공예산 지원이 줄어드는 경향이 있는데, 미국 CERT는 스스로 예산확보 방법을 모색 중이며, 상업화 등을 모색하려는 팀들이 있다.

2.4.2 대응팀 업무/서비스의 변화
- 인터넷 상업 비지네스와 연관된 활동이 보이고 있음.
- 자발적인 참여에서 상업적 참여로 변화 중
- 피해기관에서 보다 심도 있는 서비스를 요청하고 있음
- 새롭게 발표되는 복잡하고 큰 시스템이 더욱 취약함
- 시스템 제품들의 취약점들이 늘고 있음
- 시스템 제품들의 보안 서비스 부분이 개선되고 있지 않음

- 공개 보안도구들이 기관에서 원하는 수준의 성능 발휘가 안되고 있음
- 최근 사용자들에게는 보다 기술중심보다 사용자 편이성을 중시함
- 보안 관련 이슈에서는 주기적으로 관심분야의 변화와 혼란이 있을 것임
- 보안 문제에 대한 보도가 있어도 자신의 문제로 보지 않는 경향이 있음
- 일반 IRT 의 백업 차원으로 소규모 ISP들의 IRT 들이 나타나고 있음
- IRT 들의 집단에 많은 협력이 예상됨
- IRT 스탭들의 고용에 향후 어려움이 예상됨

2.4.3 해커들의 경향 변화
- 그룹화 되는 경향
- 지능화 되는 경향
- 공격 수법과 도구•방법들이 우수해지고, 복잡해지며, 빨라지는 경향
- 공격 지식을 초심자와 항상 공유
- 해커들 간의 통신 수단이 점점 우수해지는 경향
- 보다 강력한 동기 유발이 이루어지고 있음
- 국제적 피해가 더욱 많아지고 있음
- 해커에 의해 개발된 새로운 취약점들이 늘고 있음

2.4.4 법적인 이슈
- 프라이버시 및 비밀보호는 계속적으로 중요
- 정보의 변경 금지(Integrity)도 매우 중요
- 수사기관 신고 보다 독자적 처리를 하는 기관이 많음
- 일반 기관의 조사와 정부조사간 갈등이 예상됨

2.4.5 대응 팀의 향후 이슈
- 대응 팀간 상호 정보 공유를 어떻게 하면 잘할 것인가?
- 침입자에 대한 분석과 추적을 위한 자원을 어떻게 잘 찾을 수 있나?
- 대응팀 실무자가 어떻게 하면 효율적으로 사고 처리를 할 수 있나?
- 대응팀이나 관련 단체 등과 어떻게 통신을 잘할 수 있나?
- 대응팀이 제공하는 정보를 잘 따라할 수 있도록 하나?
- 대응팀의 예산 확보를 어떻게 보장받을 수 있나?

3. 침해사고 대응팀 구성 방안[20][25]

3.1 고려사항

3.1.1 분석

CERT의 목표는 보호 대상이 되는 기술 분야와 가입기관 등을 포함한 CERT의 업무 영역과 경계를 정의하며, 다음에 열거되는 항목들이 CERT의 목표에 포함될 수 있으며, 침해사고에 대한 중앙집중식 보고체계의 촉진, 특정 유형의 침해사고에 대한 대응활동의 조정, 직접적인 기술지원의 제공, 사용자 및 업자들에 대한 교육 및 보안의식 개선, 컴퓨터 보안 관련 정보의 총체적 제공, 침해사고 대책 수립을 위한 자료 및 기타 정보 제공, 가입기관 내의 컴퓨터 보안 정책 장려, 소프트웨어 도구의 개발 및 보급, 제품관련 문제점에 대한 업자의 대책 촉구, 사법/수사기관과의 업무 협조 등이다.

3.1.2 대응팀 가입기관 정의

가입기관은 통상적으로 어떤 특정한 공통점을 가지는 그룹들로 이루어진다. 예를 들어 CERT의 중점 기술분야(예를 들어 특정 운영체제 또는 네트워크등)에 의해 결정될 수도 있다. 반대로, 특정 기관 전체가 가입기관으로 결정되면 대응팀의 중점기술분야는 기관 내에서 사용되는 모든 컴퓨터 기술들이 될 수 있다. 따라서 가입기관의 규모와 관련된 기술의 다양성에 의해 대응팀 업무의 규모 및 범위가 결정된다.

3.1.3 가입기관과의 통신수단 확보

가입기관은 사고의 보고, 도움의 요청, 정보의 요구 등을 위해 대응팀과의 접촉을 유지해야하는데, 가입기관간의 통신은 효율적이며, 신속할 필요가 있으며, 프라이버시정보 또는 민감한 정보를 교환할 것인지 여부를 결정하여야 하며, 이러한 정보의 교환을 위해서는 보안이 보장되는 통신 수단도 확보되어야 한다.

3.1.4 가입기관과의 업무 협조 방안의 수립
대응팀 가입기관과의 업무협조를 위해 다음과 같은 사전 준비가 필요하다. 인증된 가입기관과의 연락처 확보, 가입기관을 위한 업무협조 절차의 수립, 배포, 프라이버시준수 약속 체결 등이 수립되어야 한다.

3.1.5 정식 가입기관 및 비정식 가입기관 처리방안 확립
대응팀 업무가 활성화되고 그 활동에 대한 내용이 외부에 널리 알려지게 되면, 정식 가입기관이 아닌 다른 기관들로부터도 신고가 접수되거나 도움을 요청받게될 수도 있다. 이러한 현상은 대응팀의 업무가 효율적으로 이루어지고 있다는 증거가 될 수는 있지만 이로 인해 정상적인 업무에 영향을 받거나, 해당 기관을 직접 서비스하는 다른 대응팀과의 관계도 악화될 수 있다. 따라서 이러한 경우에 대한 방침을 사전에 수립하여두어야 한다.

3.2 효과적 운영방안

3.2.1 구조
대응팀의 구조는 전체 가입기관의 규모, 관련 기술의 다양성, 각 가입기관내의 보고체계 및 보안체계, 그리고 지리적 분포 등에 따라 다양한 형태를 가질 수 있다. 업무구조를 결정할 때는 중앙집중식 보고와 업무의 중복 방지의 목표를 염두에 두어야 한다.

3.2.2 지원 및 예산 확보
대응팀 설립과 운영에는 막대한 예산과 시간이 소요된다. 대응팀의 업무와 중앙집중식 보고체계 등의 정책에 대한 지원이 없으면, 효율적인 대응팀의 업무를 기대하기 어렵다. 나아가 구조가 열악한 대응팀은 오히려 가입기관들에 해를 가져다 줄 수도 있으며, 결과적으로 예산의 삭감 등을 초래할 수도 있다.

3.2.3 예산과 인력 관계
대응팀은 설립예산과 운영예산의 두 가지 형태의 예산을 필요로 한다. 설립예산은 컴퓨터 및 관련 장비, 새로운 직원의 고용, 통신 설비, 사무실 확보 등의 비용들을 포함한다. 운영예산은 급여 인상, 인플레이션, 출장, 워크샵 및 지원경비, 및 장비유지 등의 비용들을 포함한다. 대응팀은 최소 1인의 관리자와 2명 이상의 직원을 필요로 하며, 목표의 달성 및 업무에 대한 권태의 방지를 위해서는 최소 수준의 직원 배정이 필요하고, 초기에 직원 소요 비용을 결정한다는 것은 무리이므로 최소 인원으로 운영하여 차기 년도의 예산 산정에는 직원의 증원이 고려되어야 한다.

3.2.4 중앙집중식 사고보고 체계 확립
대응팀에 대한 지원이 확보된 후에는, 모든 컴퓨터 관련 보안사고에 대해 대응팀 핫라인 또는 전자우편 주소 등의 중앙보고창구를 통해 보고하도록 하는 정책을 발표하여야 하며, 대응팀이 효과적으로 존재하기 위해서는 중앙집중식의 보고가 필수적이다. 중앙집중식의 보고를 통해 대응팀은 모든 사고에 대응할 수 있고, 사고들이 연관이 있는지를 결정할 수 있게 된다. 또한 중앙집중식의 보고를 통해 대응팀은 가입기관 전체에 대해 보안문제의 규모, 특성, 및 범위 등에 대한 정확한 통계를 개발할 수 있다.

3.3 업무정의 및 기준개발

3.3.1 업무정의의 필요성
침해사고대응에는 역할 및 책임에 대한 혼란으로 인해 발생되는 난관들이 매우 빈번하게 제기될 수 있기 때문에 업무정의 및 기준은 이러한 마찰들과, 발생 가능한 여타의 영역에 관한 문제들에 대한 해결에 도움을 준다. 기준은 대응팀의 목표와 기능에 대한 성명서이다. 이는 운영자의 침해사고 대응업무에 대한 인식과 승인을 나타내며, 기준은 대응팀이 만족시켜야할 요구사항들을 열거하며, 업무의 경계 또는 범위를 결정한다. 이 기준은 모든 가입기관들에게 참조용으로 제공

되어야 한다.

3.3.2 기준과 법적 문제 고려
대응팀의 활동에는 항상 법적 문제가 따르며, 회원기관에 손해를 미칠 수 있는 경우를 고려하여, 대응팀을 대표한 활동에서 의도적이거나, 무분별하거나, 부주의한 행위의 결과로 인해 야기된 책임을 인식해야하며, 비록 대응팀이 유용한 업무를 수행하고 있는 중이라 해도 이를 부주의하게 수행한 경우, 소프트웨어 업자, 사용자, 또는 다른 사람들에 대한 책임을 지게될 수도 있다. 대응팀은 기준에서 수행하고자 하는 업무와 그렇지 않은 업무, 목표를 어떻게 수행할 것인가에 대한 문제에 개입의 한계가 어디까지인가 등을 명확히 선언함으로서 법적인 문제에 노출되는 것을 방지할 수 있다. 따라서, 대응팀의 기준 및 모든 다른 절차에 대해 법률고문의 검토를 받아야한다.

3.3.3 기준의 구성 요소들
대응팀의 기준은 목표와 업무의 범위를 설명하기 위해 다음 항목들을 포함할 수 있다.
- 개요: CERT의 존재에 대한 소개, 전반적인 임무 범위, 및 다른 기본적인 정보를 제공한다.
- 임무: CERT가 수행하고자 하는 업무와 그렇지 않은 업무에 대해 설명한다. 법적 문제에 대한 노출을 제한하기 위해 이 부분에서는 CERT의 업무의 명확한 목적을 선언하고, 기밀 문제 또는 다른 기관들이나 계약자들이 관련된 문제들에 대한 CERT의 개입 한계를 정의한다.
- 방법: CERT가 그 임무 및 요구사항들을 어떤 방법으로 성취할 것인지, 그리고 특정한 형태의 컴퓨터 보안 문제에 대해 다룰 때 사용할 일반적인 접근방법에 대해 정의한다.
- 보고체계 및 요원구성: CERT가 조직내의 위치와 지위를 설정하고, 요원구성 및 예산상의 요구는 어떠한지를 정의하며, 이것은 영역에 관한 분쟁과, 특정 유형의 컴퓨터 보안 문제를 누가 처리해야 하는지 등과 같은 다른 가능한 충돌에 대한 해결을 돕는다.

3.4 사고분석 및 처리지침

3.4.1 침해사고 대응 업무 지침 및 절차의 개발
업무를 시작하기 전에 침해사고 대응 업무들에 대한 정책과 이러한 업무의 수행 중에 참조하고 따라야할 절차들을 수립해 두어야 한다. 운영지침에는 업무에 대한 정책과 기본 수칙들이 정의되어야 하며, 지속적으로 개발될 각각의 운영절차 등에 대한 단일화된 참조자료로 사용되며, 기준과 마찬가지로, 불필요한 법적 마찰을 피하기 위해 법률고문의 검토를 받아야 한다.
- 운영 지침의 개발 : 운영지침에는 다음과 같은 항목들이 포함될 수 있다.
  - 인력구성 정보 : 연락처, 팩스, 호출기 등
  - 핫라인 사용법 : 번호, 24시간 운영을 위한 절차, 즉응 대기자 명단
  - 가입기관과의 통신 : 정보의 수신 및 발신을 위한 절차
  - 침해사고보고 : 사고의 유형, 내용, 검토결과, 검증방법 등
  - 정보 처리 : 기록, 민감한 정보, 사고요약 등
  - 대응팀 컴퓨터 장비 : 관리 정책, 구성, 절차 등
  - 행정 절차 : 지출 보고, 출장, 보안 확인 등
  - 수사기관 연락처
  - 언론의 접촉 : 언론발표, 보도 허가절차
  - 업체 연락처
  - 기타 연락 정보 : 도움 받거나 참조할 수 있는 사람들의 연락처

  ※ 운영지침은 특히 CERT 운영 초기에 자주 갱신되어야 한다.
- 세부 업무 지침의 개발 : CERT의 업무지침에 따라 세부적인 정책 및 절차를 수립해야할 업무들에는 통신 업무, 사고 처리, 현장 지원, 대외 업무 협조, 언론 관리, 정보처리, 업무 보고, 내부보안, 재난관리 등의 업무들이 포함된다:

3.4.2 사고 분석 및 처리 지침
사고 접수로부터 이의 확인, 복구, 그리고 재발 방지 및 검증에 이르는 일련의 업무에 대한 일반 지침과 기술적 절차들을 포함한다. 특히 다음과 같은 점들에 유의해야 한다.
- 사고 처리 과정중 피해의 확대 방지를 위한 대책 강구
- 법적 증거물의 유지를 위해 사고 처리 전 과정에서 증거 수집에 상응하는 절차 준수
- 추후 법적 문제에 관련되지 않기 위한 사전 대책 강구

사고 처리 지침에는 다음과 같은 내용들이 포함될 수 있다:
- 사고의 정의, 기록 유지의 범위, 사고 관련정보의 획득
- 제공된 정보를 어떻게 취급할 것인지를 연락자에게 주지
- 연락자의 교육 : 사고의 발생 원인, 재발 방지를 위해 해야할 일들
- 기록철의 유지
- 사고대응 능력의 시험
- 사후 분석의 수행

3.4.3 현장 지원 업무 절차
대응팀은 필요시 피해 기관에 요원을 파견하여 현장 지원을 제공할 수도 있다. 그러나 이 경우, 과다한 비용이 지출될 수도 있으며, 반드시 팀의 자신감을 향상시켜주지 않을 수 있으므로 다음과 같은 대안을 고려해야 한다:
- 원격 지원 가능성
- 근접한 지원그룹 이용 권장

3.4.4 대외 업무 협조
대응팀은 외부의 조직들과 업무상 협력해야할 필요가 있으며, 이 경우, 대응팀의 입장을 대표하게 될 수가 있으므로 사전에 정의된 절차를 통해 접촉하도록 하여야 한다. 업무 협조가 필요할 수 있는 외부 기관에는 다음이 포함된다.
- 다른 대응팀들
- 가입기관 보안 담당자,
- 법조 기관

3.4.5 언론 관리 지침
언론에의 정보 공개 시는 적절한 통제를 거쳐 꼭 필요한 내용만을 정확하게 전달하여야한다. 언론을 다루기 위한 지침에는 다음과 같은 내용들이 포함되어야 한다:
- 접촉담당: 누가 언론과의 접촉 권한을 갖는가 ?
- 기관내 홍보 부서를 통해 업무 수행
- 일관성을 유지하고, 기술적 수준은 최소한으로 유지
- 언론 발언중 추측을 배제할 것
- 증거의 보호를 위해 법조 기관과 협력할 것
- 준비되기 전에 언론 인터뷰를 강요받지 않도록 할 것

3.4.6 정보 처리
대부분의 기관은 자신들에 대한 정보, 특히 사고와 관련된 정보가 타인에게 유출되기를 원치 않으며, 필요에 의해 대응팀에 제공된 정보도 정보의 소유자와 협약되지 않은 용도로 사용되거나 공개되지 않도록 하여야 한다.

3.4.7 업무 보고
대응팀업무를 지속시키고 발전시키기 위해서는 팀의 예산을 담당하는 기관과 업무에 관심이 있는 상급기관들 또는 협력기관들에 대해 적절한 시기에 적절한 정보를 제공할 필요가 있으며, 제공 정보 선정 및 시기의 결정, 보고 형식 및 절차 등에 대한 사전 계획이 수립되어야 한다.

3.4.8 내부 보안 및 재난 관리
대응팀이 보유하고 있는 정보의 중요성과 팀의 이미지에 미치는 영향을 고려할 때, 대응팀의 내부 보안은 여타 사이트의 보안 수준보다 강화된 수준을 유지해야 한다. 내부 보안을 위해 RFC1244 등의 자료를 참조하되 최신의 보안 패치 설치, 기밀자료 보관용 금고 사용 등의 추가적인 보안대책 및 지침을 가져야 한다. 또한 자료의 보호를 위해 재난에 대한 철저한 대책과 절차의 준수가 강조되어야 한다.

3.4.9 인력 구성
전형적인 대응팀은 한사람(또는 그 이상)의 팀관리자와 두사람(또는 그 이상)의 기술요원 그리고 기능에 따른 추가인원 및 (필요시) 지원요원을 투입하며, 인원구성은 가입기관의 다양성과 규모, 그리고 가입기관 관련기술에 대한 위험의 유형에 직접 관련되므로, 전형적인 인원구성을 정의하기

는 어렵다. 제일 중요한 침해사고대응 처리자(IR Coordinator)는 일반적인 관리자의 역할에 더해, 팀 및 이에 관계된 모든 그룹간의 적극적인 업무관계의 유지에 숙련되어야 하고 또한 관계를 개선시키고 보안의식을 고취시키기 위해 가입기관 및 업자들에게 팀의 업무를 홍보하는데 많은 시간을 투자해야 한다.

3.4.10 업무 처리용 도구
대응팀의 일상적인 업무에 투여되는 시간과 노력을 줄이고 보다 중요한 업무에 투자하도록 하기 위해 업무의 효율을 높일 수 있는 도구를 개발해야한다. 이러한 도구들은 다음과 같은 것들이 있다:

- 사고 데이터베이스 관리 도구
- 일상적 업무의 자동화 도구
- 서버 상태의 점검 도구
- 서버 및 방화벽의 감시 도구
- 팀내 시스템 및 기타 자원의 보안 관리 도구

4. CERT-CC/KR 및 CONCERT 운영[33]

4.1 CERT-CC/KR(Computer Emergency Response Team-Coordination Center, Korea)

CERT-CC/KR은 국내 전산망 침해사고 처리를 위한 기술지원을 통해 안전한 전산망 운영환경을 이룬다. 이를 위해 다음과 같은 업무들이 있다.

- 침해사고방지를 위한 예방, 침해사고의 접수 및 분석, 피해복구를 위한 기술지원
- 침해사고대응팀협의회(CONCERT)를 구성하고 사무국을 운영, 지원
- 전산망 보안 점검서비스를 통한 온라인 기술지원 - SECONE : Security Emergency of Computers/Online Network Evaluation)
- 국제적 침해사고대응 활동으로서 한국을 대표하고 FIRST에 가입하여 국내외 정보교환

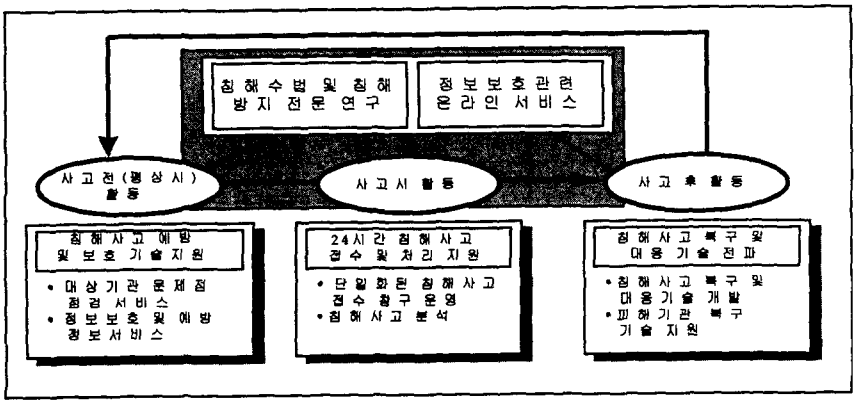

그림 1 침해사고 대응업무체계

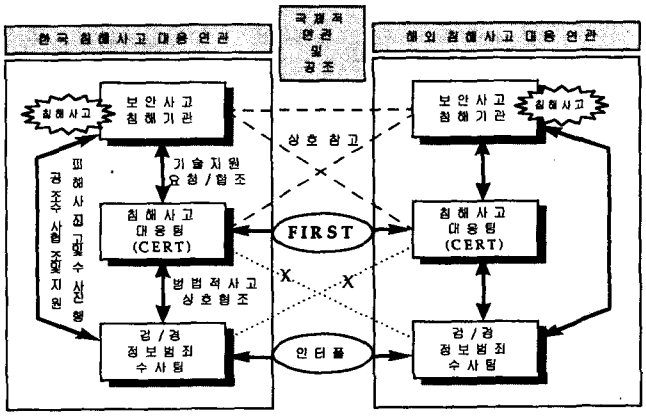

그림 2 침해사고 처리 체계

4.2 침해사고대응팀협의회(CONCERT) 운영

국내 전산망 운용기관들의 침해사고대응팀들간의 협의회로서 다음과 같은 사업을 한다.

- 전산망 침해사고 관련 상호 정보 교환 및 공동 대응
- 국제적 침해사고 공동 대응 및 협조
- 회원간 침해사고대응 기술력 향상을 위한 다음과 같은 사업
  - 세미나, 컨퍼런스, 튜토리얼 개최
  - 침해수법 공동 DB 개발 및 공유
  - 주요 대응 기술 분담 개발 및 공유, 정보 교환
- 기타 필요한 사업

가입할 수 있는 회원은 1)국내 공공전산망, 민간전산망, 업체전산망 등의 침해사고대응팀 및 담당자, 2)정보통신시스템 개발업체, 보안시스템 개발·판매업체, 비영리 학회, 연구소 등의 담당자, 3) 전산망 침해사고 대응 관련 전문가들이 참여할 수 있다.

5. 결론 및 향후 진행

이상으로 침해사고대응팀의 구성과 국내 침해사고 대응체계를 수립하고 운영, 협조하기 위한 방안들을 살펴보았는데, 이를 위해 국내외 침해사고 대응팀 현황들을 분석해 보았다. 해킹 등 침해 공격에 의한 피해는 단순한 인터넷 등 일반 전산망 뿐 아니라 상용서비스망, 금융망, 정부망 등 그 피해 대상이 다양해지며, 심각해지고 있는 경향이 있으며 이에 대한 대응 노력과 기술, 예산 등은 매우 열악한 상태에 있으므로 이 논문을 통해 국내 전산망의 침해사고 대응 방안과 협력체계를 제안하였다.

향후 CERT-CC/KR은 국내외 침해사고에 대한 접수 및 처리 지원 뿐 아니라, 이의 방지를 위한 노력과 CONCERT 사무국 운영을 통해 국내 전산망 운영기관의 대응팀 설립 지원, 협조 환경의 공간을 만들어 전반적인 국내 기술력 향상을 꾀하고자 한다.

참고문헌

[1] 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.
[2] CEC, "Incident Reporting - A European Structure: Database Structures" Commission of the European Communities(CEC/DGX111-B). - Report No. 19733(S2003/WP08). - Oct. 1992.
[3] CEC, "Incident Reporting - A European Structure: Final Feasibility and Strategy Report" Commission of the European Communities (CEC/DGX111-B). - Report No. 19733 (S2003/WP09-10). - Dec.1992.
[4] "Computer Emergency Response Team System (CERT System): Operational Framework" Members of the CERT System. - Nov. 16, 1990.
[5] "The CERT Coordination Center FAQ", CERT/CC, CMU, Revision 7. - January 1993.
[6] "CERT-NL Operational Framework", CERT-NL. SURFnet. Utrecht, NL. V2.1., Jun, 1992.
[7] "Frequently Asked Questions about CERT-NL" CERT-NL. SURFnet. Utrecht, NL. Feb, 1993.
[8] "Invitational Workshop on Computer Security Incident Response", CMU, SEI, PA. Aug,1991
[9] "DARPA establishes Computer Emergency Response Team" DARP, Dec., 1988.
[10] "Forum of Incident Response and Security Teams (FIRST) Operational Framework", FIRST, Sep. 1992.
[11] "CERT Incident Response and the Internet" K. T. Fithen and B. Y. Fraser (CERT/CC, US). - INET'93. - 1993.
[12] 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.
[13] P. Holbrook (CICNet, US) and J. Reynolds (ISI, US), "Site Security Handbook", RFC1244, FYI8. Jul. 1991
[14] "IT Security Incident Analysis Services (IAS)" International Organization for Standardization ISO/IEC JTC1/SC27/WG1. SC27/N882, SC27/WG1/N457Rev. May 1994.
[15] Klaus-Peter Kossakowski, "The DFN-CERT Experience: Building up a new CERT within Europe" DFN-CERT, Univ. of Hamburg. JENC5/INET '94 Prague, June 1994.
[16] Klaus-Peter Kossakowski, "The European Situation: The future of CSIH in Europe" DFN-CERT, Univ. of Hamburg. 6th FIRST Workshop, Boston, Jul. 1994.
[17] Klaus-Peter Kossakowski, "The Funding Process: A challenging task", DFN-CERT, Univ. of Hamburg. 6th FIRST Workshop, Boston, Jul. 1994.
[18] Thomas A. Longstaff, "Results of a Workshop on Research in Incident Handling" CERT/CC, CMU, PA. Special Report CMU/SEI-93-SR-20. Sep. 1993.
[19] Richard D. Pethia and K. R. van Wyk, "Computer Emergency Response : An International Problem", CERT/CC, CMU, PA.
[20] E. Eugene Schultz Jr., David S. Brown and Thomas A. Longstaff, "Responding to Computer Security Incidents", CIAC, LLNL, CA. Jul. 1990
[21] E. Eugene Schultz Jr., Richard D. Pethia, J. R. Dalton, "Computer Emergency Response Teams : Lessons Learned", CIAC, CERT/CC, AT&T, 13th NCSC, Md. NIST, 1990
[22] E. Eugene Schultz Jr, "The Computer Emergency Response Team System CERT-SYSTEM", CIAC, LLNL, CA. Oct, 1991.
[23] Danny Smith, "Forming an Incident Response Team", AUSCERT, Univ. of Queensland. Brisbane, Qld. - Jul. 1994.
[24] 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.
[25] John P. Wack , "Establishing a Computer Security Incident Response Capability (CSIRC)", NIST, NIST, Md. - NIST Special Publication 800-3, Nov. 1991.
[26] 조선일보 1996년 9월 24일자 기사
[27] 조선일보 1996년 6월 10일자 기사
[28] http://www.cert-kr.or.kr
[29] 한국전산원, 국가기간전산망 보안침해사고 대응체계 구축보고서, 1995.12
[30] IR-Forum 개인접촉자료 1996.9
[31] 경찰청, 해킹방지기법, 1996.7
[32] Katherin T. Fthen, " Future of Incident Response" 8th FIRST workshop, July 1996
[33] 한국정보보호센터, 정보시스템 해킹현황 및 대응, 1996.11
[34] "The Cuckoo's egg", Clifford Stoll, 1989, DOUBLEDAY
[35] GAO, "Virus Highlights Need for improved Internet Management", IMTEC-89-57, Jun. 1989

첨부 : FIRST 회원 기관명 목록

MIL: Militery, COM : Company, GOV:Government, EDU: Education

지역	회원명(팀명)	서비스 대상 영역	비고
북미 (41)	AFCERT	MIL	미국 공군
	ANSCERT	COM	기업체(ANS CO+RE)
	Apple	COM	기업체(애플, Apple Computer)
	Bellcore	COM	기업체(AT&T Bellcore)
	BCERT	COM	기업체(보잉사, Boeing)
	CERT	모든영역	미국 CERT - 미국방성 지원
	CISCO	COM	기업체(CISCO)
	DISA	MIL	미국방성Defence Infor. System Agency
	ASSIST	MIL	미국방망(DOD Internet)
	CIAC	GOV	미에너지성(DOE, ESnet)
	SSRT	COM	기업체(디지탈, Digital)
	DOW	COM	기업체(DOW)
	EDS	COM	기업체(EDS)
	GE	COM	기업체(General Elec.)
	Goddard SFC	GOV	미공우주국(Space Flight Center(NASA))
	Goldman	COM	기업체(Sachs)
	HP	COM	기업체(HP)
	IBM	COM	기업체(IBM)
	JP Morgan	COM	기업체(JP Morgan)
	MCI	COM	기업체(MCI)
	Motorola(MCERT)	COM	기업체(Motorola)
	MxCERT	MX	멕시코(Mexican CERT)
	NASA	GOV	미항공우주국(NASA Ames Res. Center)
	NASIRC	GOV	미항공우주국(Auto.Sys.Incid.Resp.Capab)
	NAVCIRT	MIL	미해군(Naval Computer Incid. Resp. Team)
	NCSA-IRST	EDU	미슈퍼컴응응센터
	NIST	GOV	NIST/CSRC
	Northwestern U.S	EDU	북서대학교
	Ohaio S. U.	EDU	오하이오 대학교
	Pennsylvania S.U.	EDU	펜실베니아 대학교
	PCERT	EDU	퍼듀 대학교
	SAIC	COM/GOV	기업체(보안관련 업체, SAIC)
	SGI	COM	기업체(Silicon Graphics)
	SBACERT	GOV	미중소기업청(Smaill Business Admin)
	Stanford U.	EDU	스탠포드 대학교
	SUN Micro	COM	기업체(썬마이크로)
	TRW	COM	기업체(TRW)
	UCERT	COM	기업체(Unisys)
	Sprint	COM	기업체(SPRINT)
	Veteran's H. A.	GOV	미재향군부(Veteran's Health Administration)
	Westinghouse	COM	기업체(웨스팅하우스)
유럽 (13)	BSI/GISA	DE	독일(GISA)
	CARNET-CERT	HR	크로아티아
	CCTA	UK	영국(정부,CCTA)
	CERT-IT	IT	이탈리아
	CERT-NL	NL	네덜란드
	DRA	GB	영국(국방성)
	DFN-CERT	DE	독일
	Israel	IL	이스라엘
	JANET-CERT	UK	영국(대학)
	Micro-Bit VC	DE	독일(바이러스센터)
	NORDUnet	DK	노르웨이
	Renater	FR	프랑스
	SWITCH-CERT	CH	스위스
아·태 (1)	AUSCERT	AU	호주