한국전산망침해사고 대응팀협의회 CONCERT

작년 어느 무렵 포항공대와 한국과학기술대 사이에서 벌어진 해킹논쟁은 시사하는 바가 크다. 그만큼 해킹이나 전산망 침해사례가 우리에게 더욱 가까이 와 있음을 의미하는 것이다. 이때 우리에게 필요한 것은 무엇인가. 전문가들은 혼자의 힘으로는 이 사고를 예방하기 힘들다고 경고한다. 이런 의미에서 태동된 한국전산망침해사고 대응팀협의회(CONCERT)를 찾아 그 임무와 활동계획 등에 대해 들어봤다.

93년 영국의 A은행은 익명의 사나이로부터 협박을 당했다. 거액의 돈을 입금하지 않으면 은행의 전산망을 파괴하겠다는 협박이었다. 아무도 이를 믿으려하지 않았다. 그러나 다음날 그 은행의 전산망은 완전 마비가 되었고, 돈의 일부가 스위스 B은행의 구좌로 불법 이체된 사실이 발견됐다. A은행에서는 서둘러 거액의 돈을 입금하고 이 사실을 비밀에 부쳤다. 이 사건은 실제 일어난 일이다. 여기서 중요한 것은 이런 사건이 비단 외국만의 사례는 아니라는 점이다. 국내에서는 아직 해킹이나 그밖의 전산망침해사고가 초보적인 수준에 머물러 있지만 조만간 기하급수적으로 증가하면서 고난도의 기술이 동원될 것이라고 전문가들은 진단하고 있다.

이러한 시점에서 한국전산망침해사고 대응팀협의회(일명 콘서트 : CONsortium of CERTs)가 발족된 것은 환영할 만한 일이다. 콘서트는 지난해 4월 정보보호센터가 설립된 후 발족한 한국전산망침해사고 대응지원팀(CERTCC-KR:Computer Emergency Response Team Co-ordination Center, Korea)을 핵으로 해서 여러 회원사들로 구성되어 있다. 한국정보보호센터의 침해사고 대응지원팀과 함께 국내에서 운영되고 있는 전산망의 침해사고 대응활동을 지원하고, 전산망 운용기관 등에 대해 통일된 협조체제를 구축, 국제적 침해사고 대응을 위한 단일 창구를 제공하기 위해 설립된 협의회를 일컫는다.

콘서트의 구성

콘서트의 시작은 95년 제정된 정보화촉진법과 그 뿌리를 같이 한다. 이 법안에 의거, 96년 한국정보보호센터(Korea Information Security Agency)가 설립되었고, 같은 해 10월 침해사고 대응팀협의회 구성을 위한 준비회의가 구성되면서 본격적으로 활동하기에 이르렀다.

콘서트를 추진하게 된 주된 배경은 국내 전산망을 외부의 침입으로부터 보호하고, 다가오는 21세기 정보전쟁에 대비하기 위함이다. 즉, 한국전산망침해사고 대응지원팀과 정보 교류, 기술 공유 등의 협조체제를 통해 국내 침해사고 예방 및 피해확산의 방지를 도모함으로써 전산망의 안전한 운영에 기여함을 목적으로 하고 있다.

이러한 목적을 바탕으로 콘서트는 ▲신속한 정보교환을 위한 연락체제 구축 ▲전산망 침해사고 관련 정보 및 기술의 상호교환 ▲국제적인 전산망 침해사고 대응을 위한 제반 활동 ▲전산망 안전운영 관련 연구회 운영 ▲침해사고 대응기술력 향상을 위한 교육 및 세미나 개최 등을 수행업무로 정해두고 있다.

현재 국내에서 밝혀진 전산망 침해사고만 하더라도 손가락에 꼽을 수 있는 수준을 넘어섰다. 미국의 어느 조사기관에서는 전체 침해사고중 15%만이 신고된다고 발표할 정도로 실제 전산망 침해사고는 비일비재하게 발생하고 있는 형편이라고 할 수 있다.

현재 콘서트에는 총 58개 기관 및 업체들이 가입되어 있다〈표 1 참조〉. 협의회의 회원은 정회원과 준회원으로 구분되고, 이를 통제하는 운영위원회가 별도로 있다. 정회원은 전산망을 운영하는 기관의 침해사고 대응팀과 담당자, 대응기술 전문가 등이 해당되며, 준회원은 정보통신기기 및 S/W 제조, 판매 업체를 비롯한 기타 정보보호 관련 단체 및 기관 등이 해당된다.

회원의 자격에 대해서는 특별한 제한을 두고 있지는 않지만 그렇다고 아무 업체나 가입될 수 있는 것은 아니다. 회원의 등록은 별도의 가입양식을 작성한 다음 팩스로 신청하고, 사무국에서 가입여부를 심사하는 절차를 밟아야 한다.

CERTCC-KR의 활동

콘서트는 한국정보보호센터내의 침해사고 대응팀인 CERTCC-KR을 중심축으로 해서 운영된다. CERTCC의 목적은 국내 전산망 정보보호인데 ▲침해사고 예방을 위한 기술지원 ▲실질적인 침해사고 대응 및 분석, 피해 복구 기술지원 ▲국내 전산망 침해사고 대응팀들간 협조체제(콘서트) 운영 지원 ▲국제적 침해사고 대응을 위한 단일 창구 운영 ▲그밖의 침해사고 예방 활동 등을 수행하기 위해 한국정보보호센터내에 설립된 지원팀이다.

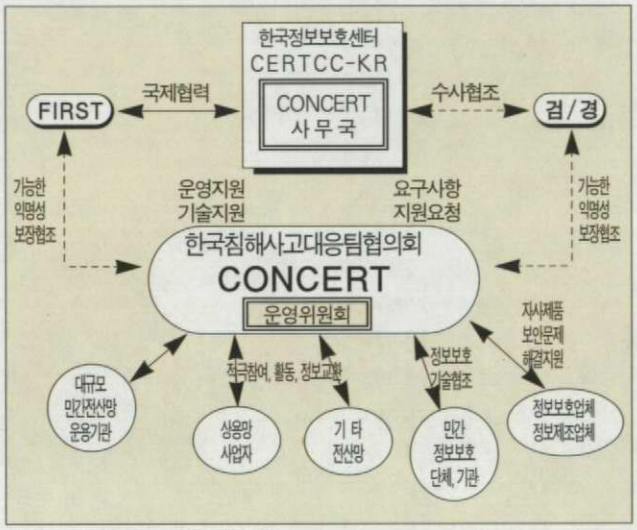
CERTCC의 주요 업무는 크게 다섯가지로 나눠볼 수 있다. 첫째는 전산망 보안침해사고 예방활동이다. 이를 위해 전산망 침해사고 예방기술 지원, 전산망 보안기술 지침 개발 및 보급, 온라인 전산망 보안진단(SECONE) 서비스 제공, 기술 세미나 지원 등을 수행한다. 둘째는 침해사고 처리 지원이다. 침해사고를 접수하고 사고의 진단 분석을 지원하는데, 독자적인 전산망 침해사고 대응팀을 갖추지 못한 기관들을 위해 침해사고 응급조치, 원인 분석, 경로 분석, 사고 재발방지 대책 등을 제공한다. 세번째는 콘서트의 운영 지원이다. 이를 위해 CERTCC 내에 콘서트 사무국을 두고 운영하고 있다. 넷째는 국제 사고대응활동 참여를 위한 창구의 제공이다. 국제적 대응팀인 FIRST(Forum of Incident Response Security Team)와 긴밀한 협조관계를 가지면서 정보보호 활동을 수행하는 것이다. 아직까지 한국은 FIRST에 정식 가입은 되지 않은 상태이고, 아태지역에서는 호주가 유일하게 가입되어 있다고 한다. 마지막 업무는 기타 활동으로서, 사고 통계 및 분석 결과 배포와 국내 유관기관과의 협력 등이 포함된다.

〈표 1〉 침해사고대응팀 협의회 가입기관 현황(97년 1월 현재)

운영위원회(16)	정회원(30)	준회원(12)
정진욱(성균관대, 위원장)	KIST(정보통신시스템실)	대정정보통신
한국과학기술원(KAIST)	SK컴퓨터통신	데이타게이트인터내셔널
나우콤	고등기술연구원	백두정보기술
넥스텔	광주과학기술원	시스코시스템즈코리아
데이콤	국립중앙도서관	ISS
삼성데이타시스템	대우통신	웹인터내셔널
시스템공학연구소(SERI)	대한항공	퀀신시스템
LG-EDS	두산정보통신	한국디지탈
충남대학교	미소테크	한국실리콘그래픽스
포스데이타	산업기술정보원	한국썬마이크로시스템즈
포항공과대학교	삼성전자	한국IBM
한국PC통신	생산기술연구원	한아시스템
한국전산원	서울대중앙전산원	
한국전자통신연구소(ETRI)	선경유통	
한국정보보호센터(사무국)	신세기통신	
한국통신멀티미디어연구소	아시아나항공	
	아이네트	
	안철수컴퓨터바이러스연구소	
	원자력안전기술연구소	
	유공	
	포항산업과학연구원	
	한국무역정보통신	
	한국무역협회	
	한국물류정보통신	
	한국원자력연구소	
	한국이동통신	
	한솔텔레컴	
	한전정보네트워크	
	현대정보기술	
	해운산업연구원	

한편, 한국정보보호센터 CERTCC는 지난 1월 30일 인터네트에 홈페이지(http://www.certcc.or.kr/)를 개설했

〈그림 1〉 한국정보보호센터 침해사고대응팀에서 개설한 홈페이지 화면.



〈그림 2〉 콘서트의 운영형태

다. 이 홈페이지는 국내 전산망 운영기관과 보안담당자에게 해킹 등 전산망 침해사고에 대응과 관련한 정보를 효율적으로 제공하기 위함이다〈그림 1〉.

이번에 홈페이지를 개설함에 따라 전산망침해사고 대응지원팀의 활동을 보다 활성화하기 위한 계기를 마련하게 되었으며, 국제침해사고대응협조기구 FIRST에 한국을 대표하여 가입함으로써 국내의 전산망 침해사고 관련 정보 교환창구 역할을 담당하게 될 것이라고 CERTCC의 최운호 선임연구원은 밝힌다.

이 홈페이지는 침해사고대응팀의 활동사항과 해킹 등 침해사고 지원요청 방법과 절차는 물론 효과적인 대응기술자료를 제공하고 있으며, 아울러 침해사고 예방 및 방지에 필요한 국내외 각종 자료를 찾아볼 수 있다. 또한 콘서트의 활동사항과 회칙, 가입안내 등의 정보를 제공하고 있으며 국내외 정보보호관련 최신 동향과 뉴스, 행사 및 공지사항 등도 함께 보여준다.

콘서트의 활동

콘서트는 추진원칙을 정해두고 있다. 현재 16개 기관 및 업체로 구성된 운영위원회를 활성화시킴과 더불어 신뢰성있는 협조, 연락체제를 구축하고, 보안지침과 방화벽, 해킹방지기술 등의 연구 활성화를 통해 기술력 향상을 목표로 하고 있다.

이처럼 원활한 운영을 위한 세부 방안으로는 ▲신속한 침해사고 상호협력 ▲국제적 침해사고 상호협력 ▲대응기술력 상호 공유 및 향상 ▲회원들의 협의회에 대한 공헌 기대 ▲프라이버시 보장 원칙 등을 제시하고 있다. 구체적인 운영형태는 그림 2와 같다.

특이한 점은 한국정보보호센터 내에 검찰, 경찰, 안기부 등 정보 보안과 관련된 기구들이 특별 파견되어 있다는 것이다. 사건이 발생할 경우 수사협조 의뢰가 들어오는 경우 개별 기관들의 프라이버시를 최대한 존중해주고, 익명성을 보장해주는 조건하에 수사에 협조하도록 되어 있다. 한마디로 중립성을 최대한 지키는 범위에서 모든 업무를 수행한다는 원칙이다.

CERTCC의 최운호 선임연구원은 "콘서트의 역할은 소방서와 같다고 할 수 있다. 화재가 일어났을 경우 불을 꺼주는 것이 주요 임무이겠지만 미연에 화재를 방지하는 것도 중요한 임무 중의 하나다. 콘서트도 마찬가지다.

침해사고의 사후처리도 중요하겠지만 더욱 중요한 것은 사전 예방이다. 그리고 어떤 기술을 가지고 침입했다는 사실이 중요한 것이 아니라 침입 대비에 관련된 지침서를 마련하는 것이 가장 절실히 요구된다"고 밝히면서 "모든 업체 및 기관에게 가입을 권유한다.

보안과 관련된 사항은 개인이나 팀의 힘으로 감당할 수 없는 경우가 많다. 그리고 꼭 회원으로 가입하지 않더라도 연락이나 정보공유는 대단한 힘을 발휘할 수 있다"고 권한다. 콘서트는 3월경에 운영위원회를 소집해 세미나 등 향후 일정에 대한 승인절차를 밟을 것이라고 한다.

〈 김완선 객원기자〉