전산망 환경에서의 정보보호 서비스

다가오는 21세기 정보사회에서는 컴퓨터와 통신기술의 비약적인 발전과 함께 전산망이 전국적으로 확산되고 대량의 정보가 고속으로 유통되게 된다. 이미 선진 각국은 초고속정보통신망을 기반으로 하는 국가정보화를 초월하여 세계정보화 정책을 펼쳐가고 있으며, 최근 급속도로 성장하고 있는 인터넷은 전세계를 한울타리 안에 포용하면서 정보검색뿐만 아니라 광고, 판매 영역으로까지 확대되면서 미래의 경제시장으로 발돋움하고 있다.

그러나 전산망환경하에서 자연스럽게 유통되는 정보의 흐름이 항상 긍정적인 좋은 결과만을 약속해 주지는 않는다. 정부기관이나 기업체의 중요한 기밀자료가 누출되거나 변조 또는 오남용되고 개인의 프라이버시를 침해하는 역기능적 피해를 간과할 수 없는 것이다.

전산망환경이라 함은 많은 컴퓨터와 원격터미날들이 통신망을 통하여 연결되고 다시 다른 통신망과도 연결되는 통합시스템이라고 할 수 있다. 일반적으로 정보보호요소는 정보에 대한 ① 비밀성(Confidentiality), ② 무결성(Integrity), ③ 가용성(Availability)으로 나눌 수 있으며 전산망환경을 고려하여 ④ 인증성(Authenticity)과 ⑤ 부인봉쇄(Non-repudiation)를 추가할 수 있다.

그러나 정보보호는 다단계적으로 중복해서 이루어져야 하며 어느 한가지만을 믿고 의존할 수는 없는 것이다. 따라서 전산망환경에서는 다양한 정보보호 서비스를 제공할 수 있도록 하여야 한다. 여기에서는 물리적인 대책이나 법제도적으로 해커들을 규제하고 교육시키는 관리적 대책은 제외하고 기술적대책을 중심으로 전산망환경하에서 제공할 수 있는 정보보호 서비스들을 간추려서 소개하고자 한다.

남 길 현 국방대학원 교수

정보의 특성과 정보보호의 중요성

다가오는 21세기 정보사회에서는 컴퓨터와 통신기술의 비약적인 발전과 함께 전산망이 전국적으로 확산되고 대량의 정보가 고속으로 유통되게 된다. 이미 선진 각국은 초고속정보통신망을 기반으로 하는 국가정보화를 초월하여 세계정보화 정책을 펼쳐가고 있으며, 최근 급속도로 성장하고 있는 인터넷은 전세계를 한울타리 안에 포용하면서 정보검색뿐만 아니라 광고, 판매 영역으로까지 확대되면서 미래의 경제시장으로 발돋움하고 있다.

대량생산과 대량소비를 바탕으로 한 물질추구의 산업사회에서 개성을 중시하고 개인의 정신적 만족을 얻고자하는 새로운 의식과 가치관 변화를 갖고 온 정보사회로 변모함에 따라 정보는 이제 물질재화보다 더 높은 부가가치를 발휘할 수 있게 되었다. 우리가 정보의 개념을 "송신자와 수신자 사이에 전달되는 의미를 갖고 있는 기호"라고 정의 할 때 정보는 기존의 물질재화와는 다른 여러 가지 특성을 갖고 있다. 그 중에서 몇 가지만을 들어보면,

첫째, 정보 자체는 일정한 형태를 갖고 있지 않고 표현된 방식이 다양하게 존재하는 추상적인 내용이다.

둘째, 정보는 대부분 일정기간의 시효가 지나면 가치가 떨어지거나 소모되는 시한성을 갖고 있으므로 정보의 획득시점과 전달속도가 중요하게 인식된다.

셋째, 정보는 타인에게 전달하더라도 본인에게 그대로 남아 있으며 대량으로 복사될 수도 있으므로 비소모성이다.

넷째, 정보는 획득시의 정보출처의 신뢰성이 정보가치의 중요한 척도가 되는 신용 가치성을 갖고 있다.

이와같이 물질재화와는 다른 특성을 갖고 있는 정보는 기본적으로 송신자와 수신자 사이에 어떤 전달매체를 통하여 전송되는 부형의 내용이며 이러한 정보는 전산망이라는 컴퓨터를 이용한 디지탈 통신망을 통하여 빠르고 정확한 정보를 대량으로 상대방에게 전달될 수 있게 되어 정보사회에서의 국민생활과 경제, 사회 발전의 중추적 역할을 담당하게 되었다.

그러나 전산망환경하에서 자연스럽게 유통되는 정보의 흐름이 항상 긍정적인 좋은 결과만을 약속해 주지는 않는다. 정부기관이나 기업체의 중요한 기밀자료가 누출되거나 변조 또는 오남용되고 개인의 프라이버시를 침해하는 역기능적 피해를 간과할 수 없는 것이다.

외국에서 발생된 여러 가지 컴퓨터 범죄사례를 찾아 볼 필요없이 국내에서도 최근에 정부투자 연구기관의 연구자료가 외국 해커에 의하여 국외로 유출된 사건, 은행의 온라인 홈뱅킹 서비스를 악용하여 거액의 자금을 불법적으로 이체시킨 사건, 해커가 대학 전산망에 침투하여 학사자료를 파괴하거나 정부기관의 패스워드 파일을 불법 복재하여 유출하는 사건 등 공식적으로 수사기관에 접수된 사건만도 수백 건에 이르고 있다. 대부분의 기관이나 기업체가 회사의 신뢰성을 유지하고 책임을 회피하기 위하여 외부에 발표하지 않거나 피해를 입을 사실조차 모르고 있는 경우가 많다는 사실을 고려한다면 전산망환경하에서 컴퓨터 범죄피해 수준은 의외로 심각한 수준까지 올라 있다고 할 수 있으며 정보보호의 중요성은 새삼스럽게 강조하지 않아도 충분히 수긍되는 사항이다.

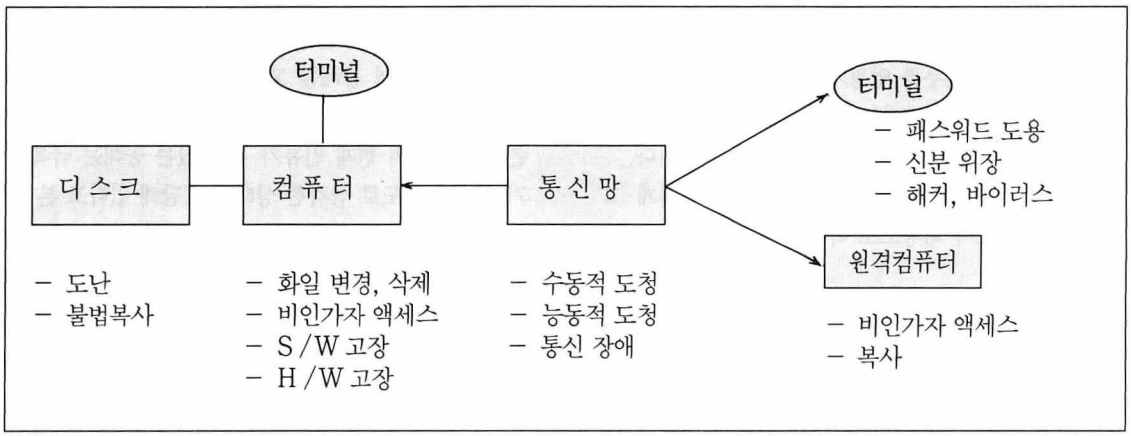
산업사회에서 공해를 고려하지 않고 중화학공업을 비롯한 공해산업 발전과 무분별한 기술개발과 자연훼손으로 인하여 현재 인류가 겪고 있는 공해는 극복되기 어려울 정도로 심각한 상태에 도달해 있다고 본다. 이와 마찬가지로 컴퓨터와 전산망이 주축을 이루는 정보사회에서 정보보호 대책을 충분히 마련하지 않고 지금과 같은 개발위주의 현상이 지속된다면 나중에 감당해야 할 역기능적 폐해는 이루 헤아릴 수 없을 것으로 추측된다.

정보보호요소와 보안 취약성

전산망환경이라 함은 많은 컴퓨터와 원격터미날들이 통신망을 통하여 연결되고 다시 다른 통신망과도 연결되는 통합시스템이라고 할 수 있다. 일반적으로 정보보호요소는 정보에 대한 ① 비밀성(confidentiality), ② 무결성(integrity), ③ 가용성(availability)으로 나눌 수 있으며 전산망환경을 고려하여 ④ 인증성(authenticity)과 ⑤ 부인봉쇄(non-repudiation)를 추가할 수 있다.

비밀성이란 정보가 도청이나 비인가자의 엑세스에 의하여 부당하게 외부로 누출되지 않는 것을 말하며, 무결성이란 비인가자가 정보를 임의로 변경시키거나 생성 또는 삭제를 하지 못하도록 하는 것이다. 가용성이란 인가된 사용자가 정보를 사용하고자 할 때 항상 정보가 활용될 수 있도록 유지시켜주는 것을 뜻하며 정보의 파괴나 손상을 막아주는 것이다. 한편 인증성과 부인봉쇄는 광의의 무결성에 포함된다고 볼 수도 있으나 전산망환경에서는 매우 중요한 요소이므로 따로 분류해 본 것이다. 인증성이란 통신망을 통하여 다른 시스템에 접속하거나 정보를 송수신할 때 서로 상대방이 적법한 상대임을 확인할 수 있도록 하는 것이며, 부인봉쇄란 서로 정보교환이 이루어진 후에 송신

〈그림〉 전산망환경에서의 보안취약성



또는 수신 사실을 부인하지 못하고 메시지 내용에 대해서도 부정한 행위를 할 수 없도록 하는 것이다.

그러나 최근 확산되고 있는 인터넷을 비롯한 LAN, WAN 등의 각종 전산망환경에서는 악의적인 해커나 바이러스 또는 불법 침입자 등에 의하여 그림과 같은 여려가지 취약점을 내포하게 된다.

근래의 인터넷환경에서는 해커들에 의한 여러 가지 불법행위가 큰 문제가 되고 있다.

초기의 해커는 특별히 나쁜 의도를 갖지않고 호기심, 능력과시용, 영웅적 심리등의 이유로 컴퓨터시스템의 취약한 부분을 공격하였으나 이제는 전산망을 통하여 컴퓨터시스템에 허가없이 무단침입하여 서비스를 무료로 사용하고 중요자료를 누출하거나 변조 또는 파괴시켜서 의도적으로 해악을 끼치는 컴퓨터 범죄행위자로 인식되고 있다. 또한 도청이라 함은 유무선뿐만 아니라 위성통신까지 포함되는 전산망에 불법적으로 접속하여 정상적인 정보의 흐름을 방해하는 행위로서 가만히 정보를 청취하기만 하는 수동적 도청과 거짓 정보를 보내거나 정보를 변조하고 흐름을 방해하는 능동적 도청으로 구분된다.

이와같이 전산망환경에서 발생되는 보안의 취약성은 특히 인터넷의 사용자가 급속도로 확산됨에 따라 더욱 가속화되고 있으며 그 이유는 인터넷이 침입자들에게 매우 취약할 수 밖에 없는 몇가지 특성을 갖고 있기 때문으로 추측된다.

첫째, 인터넷의 개방성이다. 인터넷은 기본 목적이 전세계 어디에서나 정보교환을 빠르고 원활하게 할 수 있도록 서비스를 제공하며 누구나 쉽게 활용할 수 있도록 하고 있기 때문에 해커들도 쉽게 접속이 가능하고 전산망과 전산망을 연결하는 인터넷 여행을 할 수 있도록 되어있다.

둘째, UNIX 운영체제와 TCP/IP 전송 프로토콜의 소스가 개방되어 있다. 인터넷에 연결된 시스템은 대부분 UNIX를 기본으로 하고 있으며 정보교환을 위해서는 TCP/IP 프로토콜을 사용하고 있으나 이 두가지는 소스 프로그램이 거의 완벽하게 공개되어 학교나 연구소에서 연구 목적으로 활용되고 있기 때문에 해커들이 이들을 악의적으로 연구하여 취약점을 찾아내고 이를 역이용할 수 있는 여건을 제공하고 있다.

셋째, 인터넷의 거대성이다. 현재 인터넷은 세계 170여개국을 연결하여 400만대 이상의 호스트와 5천만명을 넘어서는 사용자를 보유하고 있는 방대한 규모의 전산망을 형성하고 있다. 따라서 인터넷에서

는 검열이 거의 불가능하며 해커들이 여러 나라를 통과할 경우 역추적이 매우 어렵고 해커들 상호간의 정보교환이 은밀하고 손쉽게 이루어져서 정보보호 대책을 마련하더라도 조그마한 빈 틈이 있으면 빠르게 전파되어 공격을 시도하고 있다. 따라서 인터넷을 포함하는 전산망환경에서의 정보보호 대책은 더욱 어려워질 수밖에 없는 현실이라고 볼 수 있다.

전산망 정보보호 서비스

효율적인 정보보호 대책을 마련하기 위해서는 정보보호를 해야하는 대상을 식별하고 전산망과 컴퓨터시스템의 취약성을 분석하여 제공되는 대안들 중에서 최선의 선택을 하도록 해야 한다.

일반적으로 정보보호 대책을 물리적대책, 관리적대책, 기술적대책으로 분류할 수 있다. 물리적대책은 시설물이나 통신선로를 보호하고 출입자를 통제하거나 자물쇠를 이용하는 등의 물리적인 방법을 이용하는 것이고, 관리적대책은 법·제도적인 장치와 교육, 조직 및 인사관리, 비밀등급관리, 보안감사 등의 관리적 방법을 뜻한다. 기술적 대책은 패스워드 관리나 엑세스 제어를 하는 운영체제 또는 데이터베이스 시스템을 비롯하여 보안 모뎀이나 보안장비를 이용하거나 암호화기법을 이용하는 기술적인 방법으로 정보를 보호하는 방법이다.

특히 도청과 도난으로부터 정보를 보호하고 원격인증이나 부인봉쇄를 위한 기술적인 방법에는 암호화기법이 가장 적합한 방법으로 인식되고 있으며 최근에 개발되고 있는 IC카드(스마트 카드)를 이용한 여러 가지 서비스도 활발하게 연구되고 있다.

그러나 정보보호는 다단계적으로 중복해서 이루어져야 하며 어는 한가지만을 믿고 의존할 수는 없는 것이다. 따라서 전산망환경에서는 다양한 정보보호 서비스를 제공할 수 있도록 하여야 한다.

여기에서는 물리적인 대책이나 법제도적으로 해커들을 규제하고 교육시키는 관리적대책은 제외하고 기술적대책을 중심으로 전산망환경하에서 제공할 수 있는 정보보호 서비스들을 간추려서 소개하고자 한다.

원격인증(Remote Authentication) 서비스

단순한 컴퓨터시스템에서 사용자를 인증하기 위해서는 패스워드 방식이 가장 일반화되어 있다. 그러나 전산망으로 연결되는 원거리에 있는 사용자나 컴퓨터시스템 상호간에 상대를 인증하기 위해서는 단순한 패스워드 방식을 신뢰성이 매우 낮아지게 된다. 따라서 공개키 암호방식을 이용하거나 제삼자의 확인을 받는 방법 등의 더욱 보안성이 높은 인증서비스를 필요로 한다.

액세스제어(Access Control)서비스

액세스제어는 정보나 시스템보호를 위한 가장 기본적인 기술로서 어떤 사용자 가 어떤 자원을 사용하고자 할 때 적절한 권한이 허용되어 있는지 확인을 거쳐서 사용을 허가하는 것이다. 이러한 자원 이용에 대한 엑세스 허용여부를 결정하는 권한확인서버는 정보보호정책과 적절한 메카니즘에 의해서 엑세스제어 서비스를 제공하게 된다. 특히 인터넷과 같이 수많은 사용자를 상대로 할 때는 더욱 조심하여야 하며 보호자원의 보안등급에 따라 필요한 수준의 서비스가 이루어져야 한다.

암호화 서비스

개인의 프라이버시 보호와 중요정보의 노출이나 도청을 방지하기 위해서는 암호화해서 저장하거나 전송할 수 있어야 한다. 또한 암호화하기 위해서 필요한 비밀키를 공동으로 보유하기 위해서도 암호화 방식이 사용된다. 기존에 널리 사용된 암호방식에는 암호화할 때 사용한 키와 복호화할 때 사용한 키가 같아야 하는 대칭형 비밀키 암호방식으로서 DES(Data Encrytion Standard)가 가장 널리 사용되고 있는 암호기술이다. 그러나 전산망환경에서는 사용자가 많고 수시로 암호키를 변경시켜 주어야 하며 최초키의

분배 등 비밀키 관리문제가 매우 중요하게 인식됨에 따라 암복호화시에 각각 상이한 키를 사용하는 비대칭형 공개키암호 방식이 더욱 적합하게 활용될 수 있다.

디지탈서명(Digital Signature)서비스

전산망환경에서 디지틀문서를 교환할 때 종이문서에서의 인감도장과 같은 기능을 수행할 수 있는 디지탈서명 기술은 계약이나 부인봉쇄를 위하여 매우 활용성이 높고 필수적인 기술이라고 할 수 있다. 통상적인 사내결재 시스템에서 제공되는 결재시스템은 결재자의 패스워드를 이용한 확인정도의 서비스를 제공하기 때문에 재편집이 가능한 디지탈문서에서 중요한 사항에 대해서는 위조나 변조의 가능성이 내재되어 있다.

그러나 디지탈서명은 메시지내용에 따라 수시로 서명이 변경되므로 위조나 차후에 부인할 수 없는 특성을 갖고 있다.

디지탈서명은 국제표준화가 진행되고 있으며 국내에서도 표준화작업이 일부 마무리되고 있는 상태이고 실용화되기 위해서는 IC카드를 이용하는 방법이 가장 효과적으로 연구되고 있다.

방화벽(Firewall) 서비스

방화벽시스템은 외부전산망과 연결되는 케이트웨이(gateway)에서 비인가자의 불법접근이나 트래픽을 통제할 수 있도록하며 철저한 신분확인절차나 발신지확인을 수행하여 내부 전산망과 시스템자원을 보호하는 기술이다.

방화벽시스템은 해외에서 인터넷에 가장 많이 사용되는 기술이며 기본적인 기능은 공개되어 있고 추가적인 기능을 보강하여 여러회사에서 다양한 제품을 상품화하고 있다.

감사증적(Audit-trail)서비스 및 해커탐지 기술

감사라고 하면 보통 관리적인 대책에 포함시키고 있으나 전산망환경에서 특히 해커와 같은 불법침입자를 탐지해내고 근원지를 역추적하거나 훼손된 정보를 원상복구하기 위해서는 충분한 감사자료가 필요하며 고도의 해커탐지기술이 필요하다. 해커탐지기술도 여러가지 형태로 분류할 수 있으나 새로운 방법으로 해킹을 시도하는 해커를 탐지하는 것은 매우 어려우며 더군다나 실시간 탐지는 시스템의 성능저하를 유발하는 직접적이 원인이 되기도 한다.

결론

본고에서는 정보사회에서 정보보호의 중요성을 살펴보고 전산망환경에서 필요한 정보보호서비스들을 간단하게 고찰하여 보았다. 정보사회를 향하여 국내외가 온통 인터넷 열기로 가득하고 고급화된 정보서비스 제공을 위하여 노력하고 있으나, 정보보호분야에 대해서는 그 동안의 사회적 분위기에 휩싸여 남의 일처럼 생각하고 충분한 연구와 대비책을 갖고 있지 못한 실정이다.

특히 정보보호를 위한 암호화장비나 프로그램은 공개를 하지 않기 때문에 타첨단 과학기술과는 다르게 외제품의 모방이나 수입이 극히 제한될 수밖에 없으며 우리가 독자적으로 연구개발하여야 한다는 어려움을 안고 있다.

그러나 아무리 어려운 문제일지라도 정보보호대책은 우리나라가 선진국과 함께 정보사회로 진입하기 위해서는 선결되어야 할 필수과제임을 명심하여 정부와 산학연이 합심하여 연구에 참여하고 지원을 확대하여야 할 것이다.

다행스럽게도 지난 4월에 한국정보보호 센타가 정보통신부 산하기관으로 발족되어 정보보호분야의 연구와 개발을 선도하고 정책지원을 펴나갈 수 있으리라 기대하는 바이다.