정보사회와 정보보안

김홍근
한국정보보호센터

1. 정보사회와 보안 취약성

가. 정보사회

오늘날 우리는 급속도로 발전하는 정보 사회에 살고 있다. 정보 사회는 정보의 생성, 저장, 처리, 가공, 운반, 검색 기능이 상호 연결된 다양한 통신망 환경에서 다양한 형태의 정보 서비스가 이루어지는 사회이다. 정보통신 기술의 급속한 발전, 세계 구석구석을 거미줄처럼 이어주는 인터넷 망은 이러한 정보 및 정보화 서비스를 산업계 전반에 걸쳐 다양한 형태로 제공하여 주고 있다. 원하는 정보를 언제라도 손쉽게 얻을 수 있도록 해주는 것이 바로 정보 사회인 것이다. 자신이 있는 곳이 바로 세계의 중심이며, 정보의 집결지이다. 유닉스로 대변되어지는 클라이언트/서버 환경은 점차 정보화 시대의 주역으로 떠오르고 있으며, 초고속정보통신망의 구축은 이러한 인터넷상의 서버들을 더욱 더 빠르게 엮어주고 있다. 정보 사회에서 정보의 수집, 분석 및 활용 능력은 한 나라의 국익이나 경쟁력을 좌우하는 중요한 자산이 되고 있다.

나. 정보 사회의 보안 취약성

새로운 문명의 탄생 및 발전은 인류에게 그 편리함과 유익성이라는 혜택을 제공하는 한편 자연적으로 파생되는 역기능으로 인한 폐해를 가져다 준다. 정보통신이라는 문명의 이기에 대해서도

유사한 문제가 점차 대두되고 있다. 그 편리함과 유익성에 반비례하여 매우 위험하고 파괴적인 역기능이 뒤따르고 있는 것이다. 정보 사회에서는 모든 산업활동과 사람들의 생활에서, 정보 그 자체가 주요한 자산의 원천이 된다. 그러나 정보를 취급하는데서 오는 취약성으로 인하여 정보에 대한 무단 유출 및 파괴, 변조와 같은 공격이 자행되고 있다.

또한 우리는 인가 받지 않은 불법 사용자로 인한 정보시스템의 파괴, 개인 신상 비밀의 누설 및 유출, 불건전 정보의 유통 등과 같은 정보시스템의 오남용으로 인해 고통받고 있다. 자신이 원하는 정보를 언제 어디서든지 손쉽게 얻을 수 있게 되었지만, 정보화의 부작용으로 인해 생기는 피해 또한 막대한 것이다. 자신이 소유하고 있는 정보가 자신도 모르는 사이에 침해받고 있으며, 적절하게 보호되지 못하는 정보들로 인해 하루아침에 막대한 피해를 볼 수도 있는 것이다. 지금 이 순간에도 원치 않는 방법으로 중요기밀 또는 개인 신상 자료가 전 세계 네트워크를 타고 유출되고 있을지도 모르는 일이다. 이와 같이 갈수록 첨예해지는 국가간의 경쟁, 기업간의 경쟁에서 정보 자산의 보호는 중요한 현안으로 떠오르고 있다.

다. 정보 보안의 의미

정보란 컴퓨터에 존재하는 데이터 뿐만 아니라 이 데이터로부터 유추해 낸 자료를 포함하는 것으로 정의할 수 있다. 정보 보안은 이러한 유·무형의 정보를 내부 또는 외부의 위협으로부터 보호하고자 하는 것이다. 우리 나라도 크고 작은 유형의 정보 범죄가 매년 급속한 추세로 증가하고 있는 실정이다. 한국전산원에서 발간된 '95년 정보화 역기능 현황 및 분석 보고서에 의하면 1995년 일년동안 집계된 국내 정보화 역기능 사례는 총100건으로서, 10억 이상의 피해를 입힌 역기능 사례도 5건이나 되는 것으로 알려져, 해당 기관에 심각한 소실을 초래한 것으로 밝혀졌다. 그러나 많은 보안 사고가 보고되지 않고 그냥 지나가거나 피해 입은 사실 자체를 모르고 있다는 점을 고려한다면 실제 피해 사례는 훨씬 더 많고 광범위할 것으로 보인다. 정보통신 시스템과 네트워크가 더 개방되고, 용량과 성능 그리고 연결성이 강화될수록, 그 취약성도 비례하여 증대될 것이다.

각종 전산 침해 사고를 방지하기 위해서는 외부 침입에 대비한 효율적인 정보 보호 시스템을 개발하여야 함은 물론이지만, 그보다는 정보 보안에 대한 정책 수립과 정보 보안 마인드가 우선해야 할 것이다. 정보 보안이 제대로 이루어지지 않을 경우 국가 및 개인이 입게될 손해도 심각하겠지만 국가 또는 기업간의 치열한 정보 사회 경쟁에서도 뒤쳐지게 될 것이다.

2. 정보 보안의 기본 목표

정보 보안에 대한 요구는 처리되어질 정보의 속성에 따라서 다양할 수 있지만, 크게 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)의 3가지로 나누어 생각할 수 있다. 이는 정보 보안의 속성일 뿐만 아니라 정보 보안의 목표이기도 하다. 정보 보안이라는 것 자체가 내부 또는 외부의 침입자에 의해 저질러지는 각종 정보의 파기, 변조 및 유출 등과 같은 정보 범죄로부터 중요 정보를 보호하자는 것이 그 기본 목표이기 때문이다.

가. 기밀성

기밀성이란, 정보는 소유자가 원하는 대로 비밀이 유지되어야 한다는 원칙이다. 정보는 소유

자의 인가를 받은 사람만이 알아야 하며 인가되지 않은 정보의 공개는 절대로 방지되어야 함을 뜻한다.

기밀성은 그 특성에 따라 핵무기나 방어전략과 같은 국가 기밀성 자료, 비밀 첩보원이나 정보제공자와 같은 법률적 특성의 자료, 영업 또는 연구자료와 같은 기업적 성격의 자료, 신용도나 병력과 같은 개인 신상에 관한 자료를 포함한다. 기밀자료의 경우 그 기밀성이 노출되지 않도록 반드시 인가된 자에 의해서만 접근이 가능해야 한다. 이러한 기밀성을 보장하기 위한 메카니즘으로 접근 제어와 암호화를 들 수 있다.

나. 무결성

무결성이란, 정보는 정해진 절차에 의해 그리고 주어진 권한에 의해서만 변경될 수 있다는 것을 의미한다. 정보는 항상 일정하게 유지되어야 하며, 단지 인가 받은 방법에 의해서만 변경될 수 있다. 정보에 대한 정확도의 정도가 자세하게 명시되어 있어야만 하며, 무결성에 대한 정책에는 정보 변경에 대한 통제뿐 아니라 오류나 태만으로부터의 예방도 포함하고 있어야 한다.

즉 정보는 우발적이건 고의적이건 간에 허가없이 변경되어서는 안됨을 의미한다. 무결성 제어를 위한 메카니즘으로는 물리적 통제(Physical Control)와 접근 제어(Access Control)를 들 수 있다. 또 이미 변경됐거나 변경 위험이 있을 때는 이를 탐지해 복구할 수 있는 메카니즘도 필요하다.

다. 가용성

가용성은 정보 시스템이 적절한 방법으로 작동되어야 하며 정당한 방법으로 권한이 주어진 사용자에게 정보 서비스가 거부되어서는 안된다는 것이다. 다양한 응용 프로그램에 대해 적당한 반응시간이 결정되어 있어야만 한다. 비행기 제어나 병원의 응급 시스템과 같이 생명이 관계된 상황에서는 적시에 주어지는 자원의 가용성은 무엇보다도 중요한 요소이다. 소유 정보를 적시에 적절하게 사용할 수 없다면 그 정보는 이미 소유의 의미를 잃게 되거나 정보 자체의 가치를 상실하게 되기 때문이다. 가용성을 확보하기 위한 통제 수단으로는 자료의 백업, 중복성 유지, 물리적 위협요소로 부터의 보호 등이 있다.

그러나 이같은 통제 수단의 적용은 시스템 외적인 것이 대분이기 때문에 보안 관련 시스템 아키텍춰 설계시 제외되기도 한다. 보안성과 가용성은 상호 이율 배반적인 면이 있으므로 컴퓨터 보안에 적절한 수준으로 균형을 이루도록 절충하는 것이 바람직하다.

3. 우리의 정보 보안 현황

각종 컴퓨터 범죄 관련 보도와 연구를 통하여, 정보 사회의 역기능적 부작용의 해결은 고도 정보사회 진입을 위해 선결되어야 하는 당면 과제로 인식되고 있다. 그러나, 우리의 현실은 정보화 역기능에 대해 효과적으로 대처하지 못하고 있다 할 수 있다. 이러한 이면에는 다음과 같이 법·제도적, 기술적, 관리적, 윤리적 문제점이 지적될 수 있다.

첫째, 법·제도적 장치의 미흡이다. 제도, 법령, 기관, 업무처리 등에 대한 조정 기능 및 역할 분담 등의 관리 체계가 적절히 설정되어 있지 않으므로 해서 당면 과제에 대한 시기 적절한 대응이 어렵다. 최근에 들어 제정된 정보화촉진기본법과 시행령, 개인정보보호법과 컴퓨터 범죄 처벌 조항이 강화된 형사법의 개정 등 정보 보안와 관련 법과 규정이 많이 보강되고 있으나, 대부분 규제 사항만 강조하고 정보 보안 서비스 제공은

언급하지 못하는 등의 문제점을 가지고 있다.

둘째, 정보 보안 기술 개발 및 연구 인력의 부족과 연구 능력의 부족이다. 지금까지 우리나라에서 정보통신 기술과 같은 첨단 기술은 대부분이 선진 외국 기술을 모방하거나 도입하는 방식이었으나, 정보 보안 기술이나 장비 개발은 보안이라는 특수성과 자국의 기술 보호주의에 의해 모방이나 선진 핵심 기술의 도입은 불가능 하였다.

게다가 정보 보안에 대한 사회적 투자 인식 결여로 교육기관에서의 전문 인력 양성이 부족하여 자체적으로 정보 보안 기술을 국산화 하기에는 많은 어려움이 있다. 그나마 국내에서 정보 보안에 관한 선도적 기술 그룹은 국가 보안에 관련되어 있어 그 업무의 성격상 폐쇄적으로 운영될 수 밖에 없어서 민간으로의 관련 기술 확산은 원천적으로 봉쇄되어 있었다.

셋째, 정보 보안에 대한 인식의 부족이다. 정보화 초기 단계에 있어 정보 보안을 위해서는 관리적 대책이 중심이 될 수 밖에 없으나 이러한 관리적 대책이 실효성을 갖기 위해서는 정보시스템 관리자·이용자의 정보 보안 의식

즉, 정보 보안의 필요성과 중요성에 대한 인식이 관건이다. 이러한 정보 보안 의식이 미흡할 경우 관리적 대책은 불필요하고 불편한 절차로 인식되어 정보 보안 조치가 형식화되고 오히려 활발한 정보통신 시스템 이용에 저항을 유발한다. 정보통신 기술이 정보 사회와 국가 발전에 주도적 역할을 담당하고 있는 현실을 고려할 때, 이제는 정보시스템 관리자 및 이용자 모두가 실질적인 정보 보안 담당자가 되어야 함을 인식해야 한다.

넷째, 새로운 범죄에 대한 사회적인 도덕 관념의 결여이다. 우연한 동기로 혹은 호기심이나 성취감을 동기로 하여 시작된 시스템의 침입 시도나 불법 접근은 사소한 침해의 경우 범죄 의식보다는 오히려 시스템에 대한 우월심을 갖는 등 문서 체계에서는 당연히 침입 행위가 되었던 것들이 익명성과 비가시성 등으로 희석되어지곤 하며, 우리나라의 전통적인 공동체 의식과 협조 의식들이 이러한 환경에서 악용되는 경우가 많아 개인 프라이버시 침해 등의 문제를 낳고 있다.

4. 결론

올 4월부터 정부는 정부가 추진하고 있는 정보 사회를 향한 역기능 예방 및 방지를 위한 정보 보안 대책이 효율적이고 균형있게 추진될 수 있도록 전담 기관인 한국정보보호센터를 설립하여 정부·공공기관에서 민간기관인 산·학·연에 이르기까지 법·제도적, 관리적 그리고 기술적 정보 보안 대책을 지원하도록 하고 있다. 이를 통해 국가기간전산망의 안전성과 개인 및 기업 정보를 보호하고 개방화에 대비하는 자주적인 정보 보안 기술을 확보하기 위해 중장기적인 시각에서 정보 보안 장비의 개발·평가·공급·사용에 관한 체계 정립과 정보 보안 기술 연구·개발의 지원, 정보 보안에 관한 욕구 수렴·창출 등이 연동적으로 이루어 질 수 있도록 하여야 할 것이다.

아울러 정보통신 시스템 침해 사고와 범죄에 대한 도덕성과 책임성에 대한 근본적인 인식을 갖도록 대국민 교육 및 홍보를 강화해야 할 것이다. DC