정보 보안과 정보 보호 정책

Measures against Damages from Heavy Snow

글 / 洪 炅 孝
(Hong, Kyeong Hyo)
정보처리기술사,
한국CA 기술부 수석컨설턴트.
E-mail : trueman3k@gmail.com

In this paper, I introduce the definition and historical overview of information security and review the objective of information security. I describe the structure of information security risk and propose the solution against the target of protection. I review the international system of information security. I recommend several advices for the information security policy.

들어가며

온라인 게임인 리니지는 사이버 세계와 현실 세계가 구분이 안 될 정도로 실세계에서 발생하는 모든 종류의 사회 활동이 가능한 게임이다. 이 게임은 이전에도 게임에서 사용되는 아이템 거래로 인하여 신문 지상에서 많은 문제가 보도 되었는데, 이번에는 중국에서 약 100만 명에 달하는 한국 사용자의 이름과 주민번호를 불법 유출하여 불법적인 아이템 거래에 이용함에 따라 IT 강국의 정보 보호 정책에 대한 불신감이 확산 되고 있다.

또한, 국내 모 은행의 인터넷 뱅킹시스템이 해킹으로 5,000만원이 부정 인출되는 사건이 발생하였는데 이는 해킹 수준으로 보면 낮은 수준으로 취급되는 키 스토로크 방식을 이용하여 은행 예금자의 계좌 비밀번호, 보안 카드 번호 그리고 공인인증서 암호 내용을 알아내어 몰래 인출한 사건으로, 이로 인하여 대다수의 국민이 사용하는 인터넷 뱅킹에서의 보안 허점이 가장 완벽하여야 할 금융 기관에서 조차 보안 수준이 매우 취약함을 보여준 사례로 전자 금융 거래에 대한 불안감이 고조 되었다.

우리나라는 명실상부한 IT 강국으로 인식되고 있으며, 이는 초고속 인터넷을 기반으로 모든 산업의 비즈니스가 발 빠르게 e-비즈니스 진화로 인하여 인터넷 뱅킹, 인터넷 쇼핑몰, 인터넷 서점, 인터넷 극장, 인터넷 민원 발급기, 인터넷 게임 등 인터넷을 통한 비즈니스 활동이 이제는 일상화되었음을 의미한다. 그러나 인터넷을 통한 비즈니스는 편리하고 빠르다는 장점에 반하여 서로 얼굴을 상대하지 않는 비대면 거래로 인한 사용자 인증이

나 정보의 기밀성을 유지하기 위하여 정보 보안이 반드시 필요할 뿐만 아니라 완벽하게 정보 보호를 해야 된다.

완벽하게 정보 보호를 하지 않고 조금의 빈틈을 허용한다면 이는 전체 정보 보안 체인이나 인프라를 정보 위험에 노출되어 정보 보호가 일순간에 무너져 내리는 결과가 발생된다. 요즘 빈번해지고 있는 정보 보안 사고는 이런 우려를 잠재울 수 없는데, 정보 보안 위험에 효과적으로 대처하기 위해서는 정보 보안에 대해 올바른 인식을 바탕으로 정보 보호 정책에 대한 여러 논의가 필요하다.

정보 보안이란 ?

흔히 보안이라고 하면 중요한 것을 보호하기 위한 수단이나 행위들을 의미하는데 가장 가까운 곳에서 보안을 찾는다면 집 대문에 설치된 자물쇠를 볼 수 있는데, 이는 집 내부에 있는 재산이나 가족들을 보호하는 수단이 된다. 또한, 군에서는 시설보안, 통신보안 등이 상당히 중요한데 이는 중요한 시설을 보호하거나 통신상의 비밀스러운 대화를 보호하여 적으로부터 위험을 사전에 예방한다. 정보 보안은 정보가 담겨 있거나 유통되는 정보시스템 및 자료를 미래에 예상되는 바람직하지 못한 사건들로부터 효율적으로 대비하고 보호하는 것을 의미한다.

정보 보안의 발전 단계를 보면, 크게 3 단계로 나눌 수 있다. 첫 번째 단계는, 1990년대 이전 단계로 국가 안보적 차원에서의 보안이 강조 되어 주요 보안시설물 등의 물리적인 개념의 보안과 비문이나 통신 보안과 같은 비밀스러운 정보에 대한 보안이다. 두 번째 단계는, 1991년에서 1998년 사이로 정보시스템에 대한 안전 및 신뢰성을 확보하기 위하여 외부로부터의 침해 방지나 정보 유출 방지에 대한 보안 단계이다. 마지막 단계로는, 1999년 이후 단계로 정보 보호에 대한 개념의 확대로 인하여 일상생활 속의 정보 보호, 전자상거래 또는 전자금융을 위한 사용자 인증 수단 제공과 개인 정보에 대한 보호가 절실하게 요구되는 단계로 발전되어 왔다.

현재 우리 사회는 산업 혁명을 지나 정보화 시대로 성숙되어 왔는데, 이로 인한 우리 사회 환경은 산업 전반에 걸친 IT 의존도 증가되고 인터넷 사용이 증가함에 반해 정보 보호 관련법과 제도는 이를 수용하지 못한 환경에서 정보 보호에 대한 의식 수준 또한 매우 취약하여 정보 보안 의식 부족, 전산망 관리 체계 부족 및 각종 데이터베이스 등의 안전성이 부족한 상태이다. 이와 대비하여 해킹 도구는 매우 발달하고 습득도 용이하게 되어 전문 해커뿐만 아니라 초보자까지 정보 시스템을 공격할 수 있게 되어 정보 보안에 대한 위협은 날로 증대되어 정보 보호에 대한 필요성이 매우 강력하게 요구되는 실정이다.

정보 보호를 위한 정보 보안의 목표는 〈표 1〉에서 보듯이 권한 있는 사용자에게만 정보를 보여주는 기밀성, 정보의 정확성을 보장하는 무결성, 정보의 이용이 가능하게 하는 가용성 그리고 전자상거래나 금융거래에서 가장 중요한 정당한 사용자임을 증명하는 인증으로 구성된다.

〈표 1〉 정보 보안 목표

정보 보안 목표	내 용
기밀성 (Confidentiality)	해당정보에 대한 권한이 부여된 자들만이 접근 가능하도록 보장하는 것으로 접근 권한이 없는 자들에 대한 정보누출의 예방. 대책 기술 : 암호화(Encryption)
무결성 (Integrity)	정보의 변조 및 파괴를 예방하고 방지하는 것으로 데이터 및 정보가 정확하고 완전하게 있는 것. 대책 기술 : 전자서명(Digital signature)
가용성 (Availavility)	해킹으로 인한 시스템 동작 불능을 예방하여, 데이터, 정보 및 정보시스템에 요구된 방법으로 적시에 이용이 가능한 것.
인증 (Authentication)	정당한 사용자임을 확인하여 이용자, 프로세스, 시스템 및 정보 또 는 자원의 신원(Identity)을 보증하는 것.

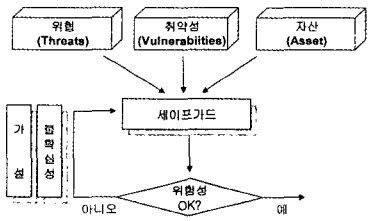
정보 보안 위험 및 정보 보안 대상

정보 보안 위험(Risk)은 정보와 정보시스템에 대한 위협(Threats)과 취약점(Vulnerabilities)의 영향과 이들의 발생 가능성으로 구성되며, 정보 보안 위험과 위협, 취약성 및 자산과의 관계는 다음과 같다.

위험(Risk) = 위협(Threats) * 자산(Asset) * 취약성(Vulnerability)

위협(Threats)은 정보시스템에 손상을 끼칠 수 있는 잠재성을 가진 행동이나 의도를 의미하며 인적, 자연적, 내부, 외부, 적대적, 비적대적 등으로 분류된다. 취약성(Vulnerability)은 정보시스템이 손상을 당할 수 있는 결함이나 약점을 의미하는 것으로 잠재적 손실, 기간, 관련 정보로 구성되며 정보 시스템을 관리하면서 발생되는 실수, 누락, 정직하지 못한 직원, 불만 있는 직원 등에 의해 취약성이 발생되며 실제 통계에 의하면 외부 바이러스나 스파이에 위한 확률은 3% 미만이며 내부 직원에 의한 손실이 83%에 달하고 있다. 자산(Assets)은 정보시스템과 정보가 가지고 있는 가치로 자산의 평가는 정보자산을 성취, 재배치, 사용하지 못할 때 드는 비용으로 평가 된다.

위의 공식에 의하면 정보 보안 위험(Risk)은 위협, 자산과 취약성 중 한 개의 요소만 제로화 시킨다면 정보 보안 위험성은 소멸되는 것으로 기업이나 공공 기관의 정보 보호 정책은 위의 법칙에 따라 보안을 강화하거나 특화 시킬 수 있다.



〈그림 1〉 정보 보안 위험성 구조

정보 보안 위험성 구조인 〈그림 1〉을 보면 위협, 취약성과 자산의 정보 보호 정책이나 정보 보호 시스템들에 의해 세이프 가드에 의해 위험성이 제로화 되지 않는다면 정보 보안의 허점이 발생되므로 이는 다시 가설과 불확실성을 참조하여 세이프 가드를 강화하여 정보 보안 위험성을 제로화 될 때까지 반복하도록 한다.

정보 보안 대상은 침입 경로가 되는 인터넷이나 공중 전화망, 정보 시스템 서버나 정보가 저장된 데이터베이스, 네트워크 장비, 어플리케이션 프로

그램, 사용자에 대한 정보 보안 지침이나 정책 등이 대상이 되며 정보 보안 대상별 위협 요소와 그에 대한 기술적인 대책은 다음과 같다.

〈표 2〉 정보 대상별 위협 요소 및 기술적 대책

정보보안대상	위협 요소	기술적 대책
데이터 저장장치	삭제 복사 수정	접근제어 Secure DBMS
호스트컴퓨터 응용프로그램	OS 취약점, 서비스거부 바이러스	사용자인증 취약점 진단 전자서명 바이러스방지 Secure OS
유선망, 무선망 위성통신망	도청 위변조	비밀키 암호 공개키 암호 해쉬함수 VPN
교환기 라우터	프로토콜취약점 트래픽폭주	취약점 진단 Secure 라우터
전화기, FAX PC, W/S	신분위장 신분위장	사용자인증 생체인증 패스워드 PC 보안
카드	카드복제	사용자인증 고속암호칩

정보 보호 체제

e-비즈니스에서 u-비즈니스로 패러다임이 전환하고 있는 세계의 각 나라들은 나름대로의 정보 보호를 위해 보안 체제를 강화하고 있다. ITSEC(Information Technology Security Evaluation Criteria)은 1991년 독일, 프랑스, 네덜란드, 영국 등 유럽 4개국에서 7등급의 조직적, 관리적 통제와 보안제품의 기능성 등을 관리하며, TCSEC(Trusted Computer System Evaluation Criteria)은 1986년 미국 국방성의 정보보호평가 표준(DoDSTD 5200.28)을 기본으로 효과적인 정보보호시스템 평가기준 개발과 이러한 기준에 맞게 개발된 제품들을 평가한다.

국제 공통 평가 기준 CC는 1993년 6월 TCSEC, ITSEC, CTCPEC(캐나다 표준) 등 각 나라의 정보보호시스템 평가기준을 통합하여 단일화된 평가기준을 제정하려는 CC프로젝트가 결성되어 1999년 6월에 ISO/IEC 15408 국제 표준으로 채택되었다.

보안 인증 부문에서는 영국표준협회(British Standards Institution) 주관으로 1993년부터 산업계의 보안 관련 표준을 수렴하여 1998년까지 제정한 정보보안에 대한 표준규격인 BS7799 (British Standards 7799)는 ISO/IEC 17799가 되어 정보 보안 표준 인증으로 사용되고 있다.

우리나라의 정보 보호 평가 기준으로 K0~K7 등급을 기준으로 1996년 8월 제정된 정보화 촉진 기본법 제15조 및 동법 시행령 제15, 16조를 근거로 1998년 2월 정보통신망 침입차단시스템 평가기준 및 평가지침서를 제정 고시하여 한국정보보호센터에서 침입차단/탐지시스템에 대한 평가를 시행하고 있으며, 정보통신망 이용촉진 및 정보보호 등에 관한 법률에서는 최근 문제가 되고 있는 개인 정보 보호를 위해 '개인정보의 기술적 · 관리적 보호조치 기준'이 고시되어 시행 중이다.

정보 보호 정책 제언

아주 빠르게 성장한 IT 강국의 이면에는 이전

성수대교 붕괴나 삼풍백화점 붕괴처럼 가슴 아픈 인재와 같은 유형의 보안 사고들이 곳곳에서 도사리고 있으며, 또한 세계는 정보전과 해킹전으로 양상이 변하고 있는데 적국으로부터의 인터넷 비즈니스의 기반을 붕괴시키는 해킹 공격이나 정보 보안 테러는 얼마든지 실현 가능한 시나리오로, 이는 자칫하면 IT 강국을 일순간에 붕괴시킬 수도 있는 강력한 힘을 가지고 있다.

최근 개인 정보 유출 사태나 인터넷 뱅킹 불법 금액 인출 사건 등을 보면 우리의 정보 보호 정책의 실효성에 대한 의문을 지울 수 없는데, 이에 다음의 세 가지 정보 보호 정책에 대한 제언을 드린다.

첫 번째, 개인 신상 정보 보호 수단으로 비실명 인증 제도를 적극 검토하기 바란다. 즉, 주민번호를 대체하는 인증으로 인하여 원천적으로 개인 정보의 노출을 방지 할 수 있다.

두 번째, 기업과 공공 기관에서 정보보호 투자를 적극적으로 하기 바란다. 이는 현재의 인프라나 인터넷 비즈니스 규모에 모자란 보안 예산 및 인력에 대한 현실화를 해 적극적인 정보 보호로 '소 잃고 외양간 고치는 식'이 아닌 사전 예방을 통해 안정적이고 지속적인 인터넷 비즈니스를 가능하게 한다.

마지막으로, 정보 보호를 위한 법과 제도의 개·제정 시 현실 및 시장상황을 감안하기 바란다. 이는 일률적인 법과 제도의 적용으로 인하여 역차별 받거나 비즈니스 상황이 얼어붙는 상황을 최소화하기 위하여 급변하는 시장 상황에 맞게끔 공청회를 통한 각계각층의 의견을 수렴해야 한다.

지금까지 IT 강국을 위한 정부의 정책과 시장의 상황이 제대로 구축되었다면 이제는 이를 육성하고 좀 더 차원을 높이기 위하여 발 빠른 정보 보호 정책과 투자에 대한 현실화를 통해 안정적이고 지속적인 IT 강국으로 한층 더 업그레이드 할 수 있으리라 전망된다.

(원고 접수일 2006년 3월 15일)

〈참 고 문 헌〉

[1] 한국정보보호진흥원 "2005년 일본의 정보보호 정책"

[2] 한국정보보호진흥원 "일본의 차세대 정보보호 정책방향과 최근 동향"

[3] KISA "2006년 01월 인터넷 침해사고 동향 및 분석 월보"

[4] 안철수 연구소 "2006년 10대 보안 이슈"

[5] 한국전자통신연구원 "국내 정보 보호 관련 법규 분석"

[6] 한국정보산업연합회 " IT보안 메커니즘"

[7] 전자신문 , 디지털타임 다수 기사 참고