컴퓨터 보안에 대한 경영전략적 접근

박 성 희*

An Approach to Computer Security from Management Strategy Perspectives

<목 차>

개 요

우리 사회가 정보화 사회로 더욱 나아갈수록 컴퓨터 시스템과 정보기술에 대한 의존도가 높아지고 있으며 이들의 사고나 실패로 인해 초래되는 반대급부가 증가하는 추세에 있다. 이 같은 이유로 오늘날 컴퓨터 보안은 보다 높은 경각심이 요구되는 중요한 분야 중의 하나이다. 특히 온라인이나 인터넷상에서의 상거래가 기업들의 중요한 일상적인 활동으로 자리 잡아가고 있는 시점에서 기업들은 컴퓨터 보안 위반으로 야기되는 수많은 위험과 위협에 심각하게 노출되어 있으며 실제로 많은

* 강남대학교 경영학부 부교수
접수일자 : 2003-4-10 게재확정일자 : 2003-12-18

기업들이 이들로 인한 손실들을 직간접적으로 경험하고 있다. 때문에 많은 기업들이 컴퓨터 보안을 위한 투자에 상당한 지출을 모색하고 있는 현실이다.

기업의 핵심적인 자산으로서 컴퓨터와 그 관련 자원들에 대한 보안은 기본적으로 특정기업이 직면해있는 컴퓨터 보안의 속성과 운영절차에 대한 정확한 이해와 함께 기업의 환경에 적합한 보안정책의 수립을 통해 이루어져야 한다. 그러나 보다 효과적인 컴퓨터 보안이 달성되기 위해서는 컴퓨터 보안에 대한 포괄적이고 통합적인 접근과 의식이 요구된다. 본 논문은 이를 위한 몇 가지의 관점을 제시한다. 그 첫째는 컴퓨터 보안에 대한 시스템적인 접근이다. 이는 과거의 컴퓨터 보안 업무가 정보기술 위주로 매우 국지적인 측면에 초점이 맞추어져 있던 문제점을 극복하기 위한 보다 진전된 접근방법을 추구하는 것이다. 둘째로는, 컴퓨터 보안관련 투자에 대한 경영자들의 의식전환이 필요하다는 점이다. 특히 컴퓨터 보안을 위한 투자에 대한 경영자의 평가에 있어서 과거의 전통적인 자본예산기법에 의한 접근에서 벗어나야 한다는 것이다. 그것은 컴퓨터 보안 분야가 목표하는 결과의 특수성 때문이다. 셋째로는, 컴퓨터 보안을 통해 기업의 경쟁력을 확보하기 위한 능동적인 접근이 필요하다는 것이다. 컴퓨터 보안을 불가피한 필요악이나 부담스러운 간접비용이라는 부정적인 시각으로 바라보는 의식으로부터 기업의 새로운 경쟁력 추구라는 능동적인 사고로의 전환이 필요하다는 것이다.

주제어 : 컴퓨터 보안, 보안정책, 보안절차, 경영전략, 보안투자 평가

I. 서 론

오늘날 컴퓨터는 개인은 물론 거의 모든 기업에서 필요불가결한 정보처리의 도구로서 폭넓게 활용되고 있으며 문명의 이기로서 그 유용성과 기여도가 갈수록 높아가고 있는 현실이다. 하지만 그 같은 높은 유용성과 기여도에도 불구하고 컴퓨터 시스템에 대한 높은 의존도와 함께 그에 따른 반대급부적인 손실위험도 함께 존재하고 있다는 사실들은 때때로 간과되곤 한다. 의도적이든 비의도적이든 컴퓨터의 기능이 마비될 경우 그에 따른 손실은 엄청난 파장을 가져온다는 것을 근래의 많은 컴퓨터 보안위반 사건이나 기능불능 사건들의 발발들을 통해 우리 사회는 자

주 경험해왔다. 이 같은 폐해를 최소화하기 위하여 컴퓨터 보안 분야는 그 중요성이 과거 그 어느 때보다도 더 커져가고 있다. 특히 이윤창출을 목표로 개방된 네트워크의 컴퓨터 환경에서 많은 활동들을 하고 있는 기업들의 경우는 그 의존도가 개인들과는 비교할 수 없을 정도로 심각하다. 경우에 따라서는 컴퓨터 보안의 부재나 결함으로 인해 기업의 지속성여부에 문제가 제기되는 극단적인 경우도 있다. 컴퓨터 보안은 효과적인 컴퓨터 시스템의 활용은 더 말할 나위없고 컴퓨터 시스템의 기능을 최적화하기위해 필수적인 관심분야이며 기업의 경쟁전략이나 경영성과에 결정적인 영향을 미칠 수 있는 분야로서 기업의 경영과 관련된 의미를 확인하는 것이 필요하다. 따라서 본 논문은 먼저 컴퓨터 보안에 관한 일반적인 배경을 컴퓨터와 관련된 보안정책과 일반원칙들을 통해 살펴보고 보안분야에서 받아들여지고 있는 효과적인 보안절차들을 정리해 보고자 한다. 더 나아가서 대부분의 기업들이 견지하고 있는 컴퓨터 보안에 대한 무조건적인 필요성이나 절대선적인 관점에서 탈피하여 기업의 전략적 목표를 달성하기 위한 하나의 과정으로서 컴퓨터 보안을 접근해야하는 근거를 살펴보고자 한다. 아울러 보다 장기적인 입장에서 컴퓨터 보안의 평가 방향을 제시하는 데 그 목적을 두고 있다.

II. 컴퓨터 보안의 속성과 보안정책

2.1 컴퓨터 보안의 정의

보안이라는 용어의 어원은 "우려나 위험, 위협으로부터 자유로움" 을 의미한다 (Cambridge Advanced Learner' s Dictionary, 2003). 따라서 컴퓨터 보안은 컴퓨터에 대한 걱정으로부터의 자유로움이라는 소극적인 의미에서부터 이를 위한 적극적인 대책이나 조치라는 적극적인 의미를 갖는다고 할 수 있다. 오늘날 우리 사회는 컴퓨터 안전에 대해 많은 우려를 안고 있다. 그것은 단순히 컴퓨터 그 자체에 대한 우려만이 아니고 컴퓨터를 중심으로 이루어지는 정보시스템과 그 관련 기술들을 모두 포함하는 것이다. 따라서 본 논문에서 컴퓨터 보안의 의미는 폭넓은 의미에서 정보시스템 보안이나 정보보안의 의미로 사용될 것이다. 너무도 익숙해져버린 컴퓨터 바이러스의 확산, 감당하기 힘들 정도로 쏟아지는 전자메일의 홍수, 은밀해야 할 개인정보의 유출 등 컴퓨터의 불법적인 활용으로 인해 발생하는 부작용들에 대해 우리 사회는 점점 더 익숙해져가고 있다. 이 부작용들에 대처하는 많은

정보기술들 역시 활발하게 개발되고 있으나 이들 간의 싸움은 매우 오랫동안 지속될 것으로 보인다.

컴퓨터 보안의 전통은 군사적인 용도에 그 기원을 찾을 수 있다. 전쟁을 승리로 이끌기 위해 필요한 정보의 기밀성을 유지하고 적의 침입을 차단하는 단계가 가장 초기의 보안사례라고 하겠다 (Schell et al, 1973). 이 같은 보안 목표들은 주로 접근통제를 통해 달성되어왔으나 보안의 대상이 보다 다양하고 확산되는 과정에서 경직된 접근통제 만으로는 보안의 기본 목적은 달성할 지언정 컴퓨터의 활용이라는 더 큰 목적이 저해되는 한계를 맞이하게 되었다. 한 단계 발전된 접근방법은 방화벽이나 침입탐지시스템과 같이 컴퓨터의 활용을 유지하는 상태에서 불법적인 접근을 적발하고 퇴치하여 그 파급효과를 최소화하는 단계이다. 이러한 방법 역시 컴퓨터 활용이라는 기능이 위축되는 면에서 컴퓨터 보안의 부정적인 인식을 불식시키지 못하는 것이 사실이다. 따라서 보다 발전된 컴퓨터 보안은 웬만한 위반이나 공격에는 견뎌 낼 수 있는 접근방법이 되어야 할 것이며, 핵심적인 기능을 위축시킴 없이 지속적으로 유지시킬 수 있는 시스템이 되어야 할 것이다. 특히나 컴퓨터 시스템의 원활한 가동과 효과적인 운영에 기업의 경쟁력 내지는 생존을 의존하고 있는 오늘날의 많은 기업들에게 있어서 컴퓨터 보안은 지대한 관심사일 수 밖에 없다.

2.2 컴퓨터 보안의 속성

전통적으로 컴퓨터 보안은 그 목표를 달성하기 위하여 컴퓨터 시스템이 확보해야 할 세 가지의 속성으로서 기밀성, 무결성, 그리고 가용성 등을 강조해 왔다 (Chin, 1999). 기밀성이란 필요성에 근거한 적합한 승인 없이는 컴퓨터 관련 보안정보들을 노출시키지 않는 것이고, 무결성이란 그 정보들이 적합한 승인 없이는 수정이나 조작되지 않도록 하는 것이며, 가용성이란 합법적인 사용자들이 필요시 언제든지 그 정보들에 접근할 수 있어야 한다는 것을 의미한다.

하지만 근래 들어서 컴퓨팅 방법이나 환경의 급격한 변화로 인해서 여러 가지의 추가적인 속성들이 포함되는 경향을 보이고 있다. 그 중의 하나는 인증(authentication)이고 다른 하나는 부인 방지(non-repudiation)를 들 수 있다 (Chin, 1999). 인증이란 컴퓨터 활용자가 스스로를 밝히고 그 진실성을 검증하는 것으로서 앞에서 거론된 세 가지의 속성을 확보하는데 선결조건이 되기도 한다. 오늘날 다양한 인증 방법들의 등장으로 컴퓨터의 활용과 인증은 서로 뗄 수 없는 관계에

있다고 해도 과언은 아니다. 부인 방지는 거래의 발생 사실이나 사건의 발생 사실에 대해 제삼자가 확인할 수 있는 근거를 마련하는 것으로서 특히 법적, 재무적 거래에 있어서 매우 중요한 속성이 된다. 오늘날과 같이 인터넷을 통해 다양한 거래들이 물리적인 검증과정이나 확인없이 논리적인 온라인 상에서 이루어지는 현실에서 전자상거래나 전자자료교환과 같은 온라인 경제의 핵심활동들은 부인 방지와 같은 보안상의 대책 없이는 결코 성립될 수 없는 활동들이라고 할 수 있다.

2.3 컴퓨터 보안을 위한 보안정책

정책이란 특정한 목표달성을 위해 정해져 있는 여러 규칙들의 집합이라고 정의할 수 있다. 컴퓨터 보안정책은 컴퓨터나 그에 의해 처리되는 정보 및 관련된 개체들의 안전을 확보하기 위하여 만들어진 규칙이다 (Higgins, 1999). 또한 컴퓨터 보안정책은 기업이 소유한 정보시스템과 핵심 정보기술의 특성, 그리고 시스템 주변환경에 의해 그 토대가 이루어진다. 이런 관점에서 특정기업의 보안정책은 그 기업의 정보기술전략과 깊은 연관성을 갖게되며 더 나아가서 기업의 경영전략과도 맥을 같이 하게 된다. 아울러 컴퓨터 보안을 위한 업무기준이나 방침들은 이들 보안정책에 근거해 구체화된다는 면에서 보안정책은 컴퓨터 보안의 실무를 위해 매우 중요한 밑바탕이 된다.

일반적으로 보안정책은 시스템이나 정보의 소유자가 어떠한 목표에 관심을 갖는가에 많은 영향을 받는다. 컴퓨터 보안과 관련된 이해관계자들은 크게 두 부류로 나누어져왔다. 그 하나는 상거래와 관련된 부류이고 다른 하나는 군사에 관련된 부류이다. 후자의 경우는 오랫동안 민감한 정보에 대한 기밀성의 유지가 가장 주된 관심사로 인식되어왔다. 보안정책은 컴퓨터가 존재하기 이전부터 주요정보들을 보호하기 위해 활용되어왔으며, 컴퓨터의 도입과 함께 더 많은 위험과 잠재적인 취약점들에 대해 보안이 강화되어왔다. 특히 초기의 보안관련 연구나 개발은 군사업무와 관련하여 크게 발전하였으나 추후 상거래 관련 분야의 비중이 점진적으로 증가함으로 인해 상대적으로 그 기여도가 감소하였다 (Bort, 2002).

상거래 관련 분야의 컴퓨터 보안은 당연하게도 재무적인 자산의 보호와 함께 정보의 흐름에 많은 비중을 두게 된다. 이윤창출을 위한 적극적인 활동들은 정보의 흐름을 필요로 하고 그 과정에서 얻어지는 다양한 자료들은 거래 기업뿐만 아니라 경쟁자들에게도 매우 유용한 자원이 되기 때문이다. 따라서 상거래 상의 불법적 사취와 같은 행동을 예방하거나 적발하는데 보안정책의 일차적인 주안점이 주어지

고, 주로 응용프로그램 수준에서의 통제를 통해 정당한 사용자에게만 사용을 허락함으로써 잠재적인 불법사용을 퇴치하고 금전적인 손실의 발생을 최소화하는데 컴퓨터 보안의 초점이 맞추어진다. 이러한 상거래 시스템에서의 컴퓨터 보안은 경영통제적인 관점에서 예방적인 조치들을 위한 투자에 대해 얼마만큼의 손실을 감소시키느냐는 투자회수에 대한 의사결정에 근거하게 된다 (Ratnasingham, 1998). 하지만 오늘날 너무도 보편화 되어가고 있는 전자상거래나 온라인 환경 하에서 보다 핵심적인 컴퓨터 보안의 관심대상은 경쟁업체와 차별화된 컴퓨터보안을 통해 경쟁적 우위를 차지하는데 있다는 점도 간과할 수 없는 부분이다. 물론 이러한 전자상거래 분야에서도 경쟁자로부터 또는 외부인들로부터 보호해야하고 그 가치를 측정할 수 없는 정보자산들이 존재한다. 이들 역시 군사분야에 적용되는 기밀성 유지를 위한 보안대책들을 요구한다. 그런 면에서 군사분야와 상거래분야의 관심과 보안정책의 차이가 항상 확연한 것만은 아니라고 할 수 있다.

오늘날 통제시스템의 핵심적인 구성요소들에서 컴퓨터의 역할은 그 비중이 갈수록 증가하는 추세에 있다. 즉 고도로 발달된 네트워크에 대한 의존, 사업의 핵심활동에 대한 컴퓨터의 역할 등은 각 기업들뿐만 아니라 산업분야 전역에 걸쳐 상호의존적 관계에 놓여있다는 것이다. 또한 개별적인 컴퓨터들은 부분적으로 또는 영구적으로 다른 컴퓨터들에 연결되어서 정보를 상호교환하고 있으며 이러한 정보들과 상호 연결되어 이루어지는 이러한 기능들이야말로 컴퓨터 보안이 지켜내야 하는 그 대상이라는 것이다. 이 개별적 컴퓨터들은 각각의 사용자들을 통해 통제되고 있으며 이들에 대한 통제적 구조형태나 방법은 컴퓨터 보안에 중대한 영향을 미친다는 것이다. 이는 효과적인 컴퓨터 보안정책을 통해서 정보의 노출이나 서비스의 중단, 지연 등으로부터 발생할 수 있는 문제점들에 대한 적극적이고 폭넓은 대응이 필요하다는 것을 의미한다.

더 나아가서, 근래의 컴퓨터들은 데이터들뿐만 아니라 서로 연결되어있는 컴퓨터에 임시적으로 혹은 영구적으로 설치되어 실행될 수 있는 프로그램들을 주고받는 경우가 매우 일상화되고 있다. 이러한 프로그램이나 부분적인 프로그램의 교환이 갖는 컴퓨터 보안에 있어서의 의미는 매우 심대하다. 특히 바이러스 탐지 프로그램이나 시스템 관리 툴과 같은 기업에서 필요로 하는 보안 대책들이 그 같은 프로그램 원격설치와 같은 방법들을 활용하는 현실에서, 교환되는 모든 정보의 원천이나 그들의 무결성을 검증하는데 필수적인 프로그램의 교환을 금지한다는 것은 매우 어려운 일이기 때문이다. 오늘날 컴퓨터 보안 정책은 그만큼 분명한 영역과 한계를 규정하는 것이 매우 까다로운 과업이 되고 있다.

III. 컴퓨터 보안의 일반 원칙

기밀의 유지라는 목표는 유사 이래로 매우 중요한 대상으로 간주되어 왔으나 동시에 매우 달성하기 어려운 과제로서 인식되고 있다. 낮말은 새가 듣고, 밤 말은 쥐가 듣는다는 속담처럼 기밀의 존재 자체는 항시 노출의 위험에 놓여있다는 사실이다. 이러한 이유로 해서 보안 분야에서는 오랜 경험을 통해 얻어진 다양한 보안 원칙들을 가지고 있다. 이러한 여러 가지 경험들은 컴퓨터 보안을 위해서도 효과적으로 응용되고 있으며, 컴퓨터 보안이 갖는 특수성에 따른 보안 원칙들도 그 일반적인 틀을 갖추고 있다.

3.1 보안의 책임소재

사람들은 자신들의 행동에 대해 그 결과에 대한 책임을 져야한다는 사실을 인식하게 될 때 책임성 있게 행동한다. 이 같은 의식은 컴퓨터 시스템에도 유사하게 적용된다. 따라서 컴퓨터 시스템 상의 처리과정이나 결과에 대한 책임소재를 분명히 하기 위해서는 적절한 형태의 인증과정(authentication mechanism)이 필요하다. 더 나아가서 보안정책에 의해 통제되고 있는 시스템에서의 활동들은 적법한 승인하에 이루어져야 한다. 적법한 승인은 사용자의 신분이나 역할에 의하여 결정되는 만큼, 인증과정이 선행되어야 할 것이다. 보안상 중요한 활동들은 보안 감사를 통해서 사용자 개인 차원의 식별에 이르기까지 책임소재를 확인할 수 있어야 한다.

인증이나 승인, 감사 절차들은 기술적으로 다수의 컴퓨터 영역을 포함하는 분야로서 많은 인력과 전문성을 요하는 일들이다. 가령, 운영체제 활용에 대한 기록들에 대한 감사증적들은 많은 경우 엄청난 분량을 가지고 있거나 실무적으로 활용하기에는 너무 세분화된 기술적 자료들로 이루어져 있어서 현실적인 가치를 갖지못하는 경우가 많다. 이 같은 제약조건들에 대한 해결책들이 각 기업 별로 모색되어야 할 것이다.

3.2 최소한의 특권

최소한의 특권 원칙이란 컴퓨터의 각 프로세스에 대한 특권은 지정된 기능을 수행하는데 필요한 특권만을 제공하는데 그쳐야 한다는 것이다 (Saltzer와 Schroeder, 1975). 어떤 면에서 이 원칙은 "알 필요(need to know)" 원칙과 상관관계가 있는 듯 하나, 직책상 접근권한을 가진 사용자라 하더라도 특정 업무 수행에 필요한

경우가 아닐 경우 접근에 제한을 가할 수 있다는 면에서 보다 엄격한 접근원칙이라고 할 수 있다.

컴퓨터 시스템에서 이 원칙의 적용은 항상 이율배반적 관계를 유발한다. 즉, 완벽한 최소특권 원칙의 적용은 각 프로세스들이 특정한 목적을 위해서 필요한 화일들에 대해서 조회와 기록 등의 행위들을 사전에 세부적으로 규정하는 것이 필요한데, 이는 시스템의 운영에 지나치게 부담을 가중시킬 뿐만 아니라 프로그램의 변경이나 새로운 기능의 추가 등에 따르는 변화를 수용할 수 없다는 현실적 한계를 갖는다. 이러한 제약조건으로 해서 이 원칙은 오늘날 대부분 무시되거나 변형되어 적용되고 있는 현실이다.

3.3 보안요소의 단순화

사람이든 컴퓨터이든 간에 시스템의 보안에 영향을 미칠 수 있는 요소들은 신뢰성이 확보되어야 한다. 신뢰성의 확보는 그 요소들이 갖는 규모나 복잡성에 비례하는 노력을 필요로 한다. 즉, 다양성이나 규모, 복잡성의 최소화는 각 요소들이 설계한 대로 구현되었다는 것을 확인하는 것이 수월한 까닭으로 신뢰성 확보에 소요되는 비용이나 위험을 감소시켜준다는 것이다.

그러나 이 원칙의 적용에는 매우 조심스러운 접근이 필요하다. 단순화로 인해 얻어지는 보안효과에 비해, 시스템의 활용 상에 발생하는 제약조건들로 인해 성과상의 저해요소로 작용할 가능성이 있기 때문이다. 가령 모든 보안 점검이 중앙에 위치한 시스템 요소에 의해 모두 이루어질 경우 특정요소의 부담이 가중될 뿐만 아니라 분산된 시스템으로부터의 지나친 자원요청으로 인해 시스템의 성과를 감소시키는 결과를 가져올 것이다.

3.4 기본적 보안조치

이 원칙의 의미는 모든 시스템의 기본 사항들이 보안을 최우선으로 하여 조치되어야 한다는 것이다. 컴퓨터의 최초 취득시점부터 보안과 관련된 사항들이 엄격하게 갖추어져 있는 상태로 제공되어서, 추후 운영상의 필요로 인해 이 보안 사항들에 대한 융통성을 가미하는 것에 대한 결정은 관리자의 심사숙고에 의한 의도적인 조치에 따라 이루어져야 한다는 원칙이다. 많은 시스템들이 시스템의 성능이나 운영적 유연성을 이유로 보안이 해제된 상태로 시스템을 제공하는데, 이처럼 최소의 보안조치와 일반적으로 알려진 상태의 사용자 아이디와 기본 패스워드로 이루어진

채 제공되는 시스템들은 이 같은 원칙에 반하는 것이다. 기본적 보안조치란 앞서 거론된 최소한의 특권 원칙의 우선적 적용이라고 말 할 수 있다.

3.5 보완적 보안의 구현

컴퓨터 시스템이 내재적으로 갖게되는 결함들에 대한 완전한 해결책은 현재의 기술들로는 불가능해 보인다. 다양한 검사절차를 통해서 최소화하려는 노력에도 불구하고 많은 컴퓨터 보안사고의 대부분은 이러한 결함들을 이용한 공격으로 발생하고 있다. 따라서 시스템의 설계는 여러 가지 보완적이고 복수적인 대처 방안들을 활용하여 하나의 보안이 실패하더라도 다른 보안 방안들이 문제의 확산을 저지시킬 수 있도록 이루어져야 한다. 이는 위에서 언급된 보안요소의 단순화라는 원칙과 상충되는 부분도 있으며 오늘날의 많은 시스템 관리상의 문제가 다양한 보안 조치들로부터 기인한다는 면에서는 부정적인 면도 있다고 하겠다. 그러나 개별적인 보안 조치들이 매우 제한된 범위를 가지고 있고 그들이 나름대로의 예측하지 못한 결함들을 내포할 수 있다는 관점에서 볼 때 보완적 조치의 원칙은 오늘날의 컴퓨터 시스템 환경에서 필요할 뿐만 아니라 바람직한 것이라고 생각된다.

Ⅳ. 효과적인 컴퓨터 보안을 위한 접근 절차

4.1 컴퓨터 보안 영역의 설정

컴퓨터 시스템에 대한 효과적인 보안을 위해서는 컴퓨터 자원들과 관련된 보안 정책들을 적용하기 위해 시스템 내의 자원들을 분리하는 접근이 필요하다. 이 같은 분리된 자원들을 별개의 보안 영역이라고 할 수 있고 이들은 주로 컴퓨터 자료들과 이 자료들을 처리하는 컴퓨터의 요소들이라고 할 수 있다. 가령, 컴퓨터가 처음 구동되기 시작되는 시점에서 초기의 보안 영역을 어떻게 설정하는가 하는 것은 컴퓨터 전반의 안전한 보안을 위해서 매우 중대한 조치가 되기도 한다. 많은 컴퓨터 바이러스들이 이러한 이유로 해서 처음 구동과 함께 컴퓨터 시스템을 통제할 수 있는 방법을 탐색하는 것이다. 나아가서 컴퓨터 보안 영역의 설정뿐만 아니라 설정된 영역들간의 상호 통제를 위한 조치들 역시 중요하다. 컴퓨터 보안 영역은 컴퓨터 하드웨어가 내장하고 있는 기능들이나 소프트웨어의 기능들을 활용하여 설정할 수 있다. 하드웨어의 입출력 통제나 컴퓨터의 특권적 상태의 변경, 가상적 기억

장치로부터 물리적 기억장치 주소로의 맵핑 등과 같은 특권적 지시사항들로의 접근을 통제하는 방법들은 가장 기본적인 수준에서의 영역설정에 관건이 되는 것들이다.

4.2 사용자와 보안영역의 연결

컴퓨터 보안을 위해서는 모든 시스템에서 이루어진 활동들이 특정 사용자들에게 그 근원을 추적해 나갈 수 있어야 한다. 즉 사용자와 보안영역들을 연결하는 작동절차에 대한 필요성이 제기되는 것이다. 사용자의 신원확인과 인증은 이 같은 연결관계를 정립하는데 필요한 과정이라고 할 수 있다. 사용자 아이디와 패스워드의 제시가 가장 보편적인 신원확인과 인증 방법이었으나, 인증카드와 같은 증거물, 생체인식 등과 같은 방법들도 갈수록 그 용도가 넓어지고 있다. 대부분의 인증과정에서 사용되는 방법들은 주로 세 가지 원칙에 그 근거를 두고 있다. 첫째는 패스워드와 같이 사용자가 "알고 있는" 것, 둘째는 인증카드와 같이 사용자가 "소유하고 있는" 것, 셋째는 지문이나 홍채와 같이 사용자 "자신을 나타내는" 것 등이다. 일반적으로 이 인증 방법들은 여러 가지 방법들이 중복되어 사용될수록 더욱 보안의 신뢰성을 높일 수 있다고 인식되고 있다.

하지만 무엇보다도 인증과정 상에서 핵심이 되는 요소는 인증 데이터의 출처와 검증결정 구성요소 간에 안전한 경로가 보장되어야 한다는 것이다. 경로상의 취약성은 인증을 위해 결정적인 정보의 신뢰성을 보증할 수 없고 이는 인증과정의 오류를 초래할 수 있다. 도청이나 가로채기와 같은 위협에 대처하기 위하여 일부 인증 프로토콜들은 매 인증에 따른 기대 반응이 달라지는 도전-반응의 절차를 도입하기도 한다 (Tipton & Krause, 2003).

오늘날 대부분의 인증절차는 성공 또는 실패로서 그 결과를 제시할 뿐, 인증과정에서 얻어진 증거들에 대해 별도의 분석이 이루어지지 않거나 증거의 수집조차 이루어지지 않는 경우가 허다하다. 그것은 인증과정에서 얻어지는 자료의 방대함으로 해서 자료분석이 매우 번거롭거나 자료분석을 통해 얻을 수 있는 보안상의 효익이 그리 크지 않기 때문이다. 그러나 공개 키 기반구조의 확산으로 인한 인증 공개키의 활용은 사용자의 인증수준이나 인증기관의 신뢰도 수준의 비교를 통해 훨씬 더 깊이 있는 자료들을 제공할 수 있을 것으로 보여진다.

일단 사용자의 신원이 특정 영역에 연결이 되면, 일반적으로 영역 내에서 설정된 사용자의 권한이 제공된다. 그러나 사용자의 아이디가 여러 사람들에 의해 공

유될 수 있을 경우 사용자와 영역간의 연계성은 심각하게 약화될 수 밖에 없다. 인증과정을 적법하게 통과한 사용자가 실행한 특정 행동들에 대해서 어느 특정인에게 그 책임을 귀착시키는 것이 매우 어렵기 때문이다. 따라서 아이디 공유에 대한 명확한 원칙과 절차를 규정함으로써 무원칙적으로 공유되는 아이디로 인해서 발생할 수 있는 부작용이나 폐해를 예방하고 규제하는 것이 필요하다.

4.3 시스템 접근의 승인 통제

사용자와 특정 보안영역의 연결이 이루어지면, 그 다음 단계는 특정 자원에 접근하려는 프로그램의 시도를 승인할 것인지의 여부를 결정하는 것이다. 이 같은 승인은 조직의 보안 정책을 시행하도록 설계된 참조 모니터(reference monitor)라는 시스템 요소를 통해 그 프로그램의 요구가 보안정책에 위배되는지 여부를 판단하게 된다. 가령 승인 대상 객체가 화일일 경우 특정 사용자들에게 허용된 읽기, 쓰기, 실행 권한을 구체화한 접근통제목록(access control list)이 일반적으로 존재한다. 따라서 특정 프로그램이 특정화일을 읽기 위해 접근요청을 하면, 참조 모니터는 사용자가 요구한 작업에 대한 권한 여부를 판단하여 적법한 경우 화일 접근을 허용하여 필요한 작업을 할 수 있도록 하거나 적법하지 않은 경우 접근을 불허하고 특정 형태의 오류 메시지를 보내게 된다.

이러한 참조 모니터가 효과적으로 실행되기 위해서는 우선 모든 접근 요청들을 중재할 수 있어야 하고, 둘째 작고 단순한 형태를 갖추어서 주어진 기능들을 오류없이 실행할 것이라는 신뢰성이 있어야 하고, 셋째 외부적인 조작이나 변조로부터 스스로를 방어할 수 있도록 만들어져야 한다. 효과적인 참조 모니터의 세 가지 요구조건인 완전한 중재, 무오류 기능, 변조불능 등을 충족하기 위하여는 별도의 독립적인 영역을 가진 중앙통제식 보안시스템 요소를 필요로 하게 된다. 문제는 이러한 모니터가 여러 영역들을 빈번하게 오고 가야하는 필요를 유발하고 이는 다시 전체 시스템의 성과 문제를 야기한다는 점이다 (Tipton & Krause, 2003).

전형적으로 승인 정책과 그 실행절차는 컴퓨터 시스템 내의 여러 단계에 걸쳐 존재하게 된다. 로그인 절차를 통해 특정 사용자가 시스템 사용에 대한 권한을 부여받았는지 여부를 확인하고, 화일 시스템을 통해 적법하게 로그인한 사용자가 특정 화일에 접근할 수 있는 권한을 소유하고 있는지 여부를 검증하며, 데이터베이스 관리시스템과 같은 프로그램을 통해 사용자에게 허용된 부분이 화일의 어떤 필드인지 여부를 검증하는 것이 그 같은 단계별 승인절차 실행의 예가 될 것이다. 만약

특정 사용자가 데이터베이스 프로그램을 거치지 않고 데이터베이스에 접근하여 화일을 불러올 수 있다면 이는 데이터베이스의 보안통제의 결함으로서 데이터베이스가 참조 모니터로서의 완전한 중재 기능을 실패한 경우가 될 것이다. 이러한 이유로 해서 응용 프로그램 관련 보안통제에 완벽을 기하고자 하는 개발자들의 경우, 그 프로그램이 실행되는 상황이나 운용체제 내에서 이루어지는 승인 작동절차에 대해서 정확하게 이해하는 것이 필수적이다.

역할 기반 접근통제(role-based access control) 또는 과업 기반 보안통제(task-based security control) 정책과 절차의 개발은 응용프로그램과 관련된 정책들의 복잡성을 조직화하고 개별 사용자보다는 작업과 관련된 사용자들의 역할들을 관련된 접근권한에 연결시키고자 하는 시도의 한 결과이다 (Bellettini, et al., 2001; Steinke, 1997). 이를 통해서 사용자들은 미리 설정된 복잡한 응용프로그램 관련 승인 사항들을 특정한 역할을 근거로 승인을 받아 실행하는 것이 가능해 지는 것이다.

4.4 시스템 감사의 운영

소프트웨어나 컴퓨터 설비의 오작동의 경우 감사 로그들이 시스템 관리와 유지를 위해 매우 유용하게 활용된다. 컴퓨터 보안에 있어서도 감사 로그의 사용은 보안 관련 활동들에 대한 명확한 책임소재를 제공함으로써 컴퓨터 보안의 중요한 연결고리의 역할을 한다. 일반적인 경우 시스템의 사용자가 감사 로그를 제거한다거나 변조한다는 것을 생각하기는 어렵지만, 침입자가 시스템에의 침입이 성공하고 시스템 내에서의 활동들을 숨기고자 한다면, 감사 절차를 무력화시키는 것은 가장 일차적으로 원하는 바가 될 것이다. 감사 절차는 이러한 시도나 공격에 견뎌낼 수 있어야 할 것이다. 감사 절차가 보호될 수 없다고 한다면 시스템의 보안도 장담할 수 없는 것은 당연하다. 그러나 대부분의 침입자들이 보안 감사 절차에 대해 상세한 지식을 갖기가 어렵고 그것을 무력화시키는 것은 그리 손쉬운 일은 아니다. 더군다나 많은 감사 로그나 감사증적들은 수정불능 미디어에 기록되거나 별도의 원거리 화일에 보내지는 등 침입자가 조작이나 변경하는 것을 막을 수 있도록 설계되곤 한다.

보안 감사의 현실적인 문제점은 로그에 기록된 자료들로부터 추가적인 감사 대상을 선별하거나 효과적으로 점검할 수 있도록 내용을 관리하는데 있다. 운영시스템 수준에서의 감사가 시스템 전체와 관련하여 일관성있는 자료를 제공하고 가장

보편적인 작업이 되겠지만 로그 기록들의 양에 비해서 얻을 수 있는 내용은 매우 제한되는 것이 보통이다. 즉, 외부로부터의 침투가 일단 확인되었다고 할 경우 로그 기록을 통해서 침입자의 활동 내역을 재구성할 수는 있겠지만, 로그 기록의 점검을 통해서 침투가 발생했는지 여부를 알아낸다는 것은 그리 현실성이 없는 편이다. 반면에 응용 프로그램 수준에서 이루어지는 감사의 경우 일련의 시스템 명령에 대한 의미를 찾아내는 것은 상대적으로 수월하다고 하겠다. 그러나 이 경우에도 각 응용 프로그램들이 만들어내는 감사 로그들은 각기 다른 내용과 형식을 갖는다는 어려움이 존재한다 (McHugh, 2001). 그럼에도 불구하고 응용프로그램들과 관련된 감사의 접근이 보다 효과적인 결과를 가져올 것으로 판단된다. 보안 감사 로그는 그 존재 자체로 인해서 사용자들에게 경각심을 불러일으키고 불법적인 활동을 예방하는 효과를 가지며 나아가서 자동화된 침입탐지시스템을 위한 자료의 원천이 된다는 점에서 컴퓨터 시스템 보안에 매우 유용한 도구의 역할을 한다 (Alexander, et al, 2001).

4.5 보안을 위한 암호법의 활용

암호화는 오늘날의 정보보안에 있어서 없어서는 안될 매우 핵심적인 기술이다. 암호화 알고리즘은 평범한 자료를 암호화 키를 통해 복호화 키에 의해서만 본래의 형태로 전환시킬 수 있는 암호문으로 변환시킨다. 암호화 키와 복호화 키가 같은 경우 이를 대칭형 키라고 하고 그 둘이 서로 다를 때 이를 비대칭형 키라고 일컫는다. 비대칭형 키 알고리즘의 경우 서로 다른 키를 소지함으로써 하나의 키는 비밀키로서 한 사람만이 소유하고, 다른 하나는 공개키로 많은 사람이 소유할 수 있도록 만들어진다. 비밀키로 암호화된 자료의 경우 공개키를 소유한 누구라도 복호화를 할 수 있으나 암호화는 비밀키의 소유자만이 할 수 있다라는 사실은 매우 중요한 의미를 지니게 된다. 즉, 자료나 문서의 출원지로서 비밀키를 소유한 사람에게 연계시킬 수 있다는 사실로 인해 전자서명 (digital signature)을 생성하는데 핵심적인 방법으로 사용될 수 있다는 것이다. 그러나 비대칭키 알고리즘은 대칭키 알고리즘에 비해 훨씬 많은 양의 연산을 필요로 하기 때문에 비교적 적은 양의 자료를 암호화하는데 적용되는 것이 일반적이다.

컴퓨터 보안 문제와 관련된 암호법의 적용은 지난 10여 년 간 계속 증가해왔다. 그 가운데에서도 과거 어느 때보다도 더 광범위하게 암호법이 활용되고 있는 곳은 전자상거래의 정보보안과 검증 분야에서 찾아볼 수 있다 (Liddy, 1997). 인터넷 상

에서 이루어지고 있는 상거래들을 암호화하는데 사용되는 대표적인 암호법으로는 SSL(Secure Socket Layer)나 TLS(Transport Layer Security)를 들 수 있다. 이들은 전자상거래에서 사용되는 신용카드 번호와 같은 정보들이 통신상에서 도청에 의해 노출되는 것을 막기 위한 암호화를 위해 사용되는 세션키들을 생성하고 전달하기 위하여 공개키 암호체계를 활용한다. 그러나 이 프로토콜들은 통신의 양쪽 끝에 위치해있는 컴퓨터 시스템들을 보호하는 데에는 별다른 효과를 발휘하지 못한다는 허점을 가지고 있다. 즉, 컴퓨터 시스템들에 보관되어있는 키들에 대한 관리는 컴퓨터 통신보안에 대한 문제이전에 컴퓨터 보안의 문제라는 것이다 (Schneier, 1998).

4.6. 보안조치에 대한 효과검증

컴퓨터 보안이 별개의 프로세스로서 시스템 내에서 작동한다고 할 때, 바람직한 보안은 사용자들이 의식하지 못하거나 불편을 야기시키지 않도록 하는 것이다. 정상적으로 가동되고 있는 시스템 내에서 보안 절차로 인해서 사용에 걸림돌이나 장애요소로 작용할 경우, 사용자들은 그 같은 불편을 해소하기 위하여 보안과 관련된 작동장치나 절차들을 무력화시키거나 무시할 가능성을 가져오게 될 것이다. 작업을 자주 중단시키는 보안조치나 자주 나타나는 대화창구는 사용자의 주의를 끌지 못하게 되고 경우에 따라서는 심각하게 받아들여야 할 조치들조차도 무시되고 간과되는 결과를 초래할 수 있다. 즉, 보안조치들이 제대로 작동함으로 인해서 이루어지는 경우와 보안조치들의 불필요한 간섭으로 인해 생겨나는 경우들을 구분하는 것이 매우 어려워지는 상황을 가져올 수 있다는 것이다. 이를 위해서 필요한 것은 보안과 관련된 설계와 구현에 대한 계량화 할 수 있는 확신도를 검증하는 것이다.

특정 애플리케이션이나 도구가 계획한대로 작동하는지 여부에 대한 확신은 몇 가지의 증거를 근거로 한다. 그 중 하나는 그 도구가 잘 훈련되고 필요한 능력을 지닌 사람에 의해 만들어졌는가에 대한 증거이고 또하나는 세부사항들이 정해진 절차에 따라 적절히 이루어졌는가에 대한 증거이며 또다른 하나는 그 도구 자체에 대한 분석과 검사를 통해서 그 적정성 여부에 대한 증거를 확인하는 것이다. 그러나 이 증거들 중에서 가장 중요하고 확실한 증거는 도구 자체에 대한 증거일 것이다. 누가 어떻게 만들었는가에 관계없이 작동 결과가 기대한 대로라면 그것으로 그 도구에 대한 확신은 성립될 수 있기 때문이다. 하지만 오늘날의 컴퓨터들, 하드웨어나 소프트웨어들, 모두 그 복잡성은 과거와 비교할 수 없이 높다. 따라서 이들에

대한 철저한 분석과 검사는 근본적으로 한계를 갖고 있다는 것이다.

범용적 컴퓨터 시스템들에 대한 보안 검증 문제를 공식적으로 다룬 것은 소위 "오렌지 문서"라고 불리우는 미 국방성의 '컴퓨터 시스템의 신뢰성 평가 기준'이다. 이 문서는 보안절차와 확신에 필요한 요구조건들에 대해 등급별로 분류가 가능하게 하는 기초적 틀을 제시하였다 (Barnard & Solms, 1998). 이 같은 기준을 통해 컴퓨터 시스템에 필요한 다양한 보안관련 요구사항들을 구체화하는 것이 가능해졌고, 컴퓨터산업에서는 이에 따른 보안조치와 기능들을 모색하고 그 결과를 객관화된 근거와 인증을 토대로 사용자들에게 제시할 수 있게 되었다. 이러한 평가와 검증이 초기에는 주로 군사적인 또는 공공적인 분야에서 주로 전개되었으나 그 여파는 민간분야에서도 보편화되고 이는 컴퓨터 시스템의 보안평가를 중요한 정보시스템의 요소로 인식하게 만드는 토양을 제공하게 되었다. 이들 평가기준의 목표는 다양한 컴퓨터 시스템들이 갖추어야 할 공통적인 보안요구사항들의 확보와 시스템들을 평가하는데 필요한 객관적인 척도들을 구체화하는 것이라고 할 수 있다. 이들을 근거로 사용자들이나 고객들은 자신들이 필요로 하는 보안수준에 맞는 컴퓨터 시스템을 획득하고 그 보안성에 대한 신뢰성을 담보할 수 있기 때문이다. 나아가서 이러한 보안평가에 대한 발전은 미국 이외의 여타 국가로도 파급되어 많은 국가들이 각국 나름대로의 환경과 여건에 적합한 평가기준들을 제정하고 활용하는데 기여하게 되었다 (Barnard & Solms, 1998).

V. 컴퓨터 보안의 경영전략적 관점

5.1 컴퓨터 보안의 시스템적 관점

많은 기업들이 컴퓨터 보안과 관련된 도전들에 일상적으로 접하고 있다. 세간에 크게 화제가 되곤 하는 컴퓨터바이러스의 침입과 전파로 인한 피해로부터 내부 구성원들의 고객정보 유출과 같은 기업의 신뢰성에 부정적인 영향을 미치는 사건들의 돌출 등과 같은 정보시대의 어두운 그늘들로 인해 컴퓨터 시스템의 관리자들뿐만 아니라 경영관리자들은 컴퓨터 보안의 심각성을 인식해가고 있다. 그러나 컴퓨터 보안은 단순한 일과성 사건의 문제가 아니고 보다 근본적인 시스템의 문제라는 것을 이해하는 것이 타당성 있는 해결책을 찾기 위해 매우 중요하다. 즉, 많은 컴퓨터 보안 사고의 원인들이 부적합한 컴퓨터 시스템의 관리에 기인하고 있다는 것

이다 (Wood, 1995).

게다가 갈수록 높아가고 있는 사용자들의 컴퓨터 활용능력이나 기능은 컴퓨터 보안 전문가의 부족과 함께 컴퓨터 보안 분야가 직면하고 있는 심각한 문제점의 하나이다. 컴퓨터 소프트웨어 개발회사들의 수익을 보장하기 위한 계속적인 기능추가와 버전 변경도 컴퓨터 시스템의 안정성을 위협하는 매우 중대한 요소 중의 하나이다. 늘어나는 기능과 다양성에 비해 이의 안정성을 확보하는데 필요한 시간과 경비는 현실적으로 불충분한 것이 대부분이고 이에 따른 프로그램의 취약점들이 컴퓨터 해커들이나 범죄자들에게는 더할 수 없는 기회를 제공하고 있다는 것이다. 아이러니컬하게도 이 취약점들의 발견이나 수정이 해커들의 열성과 노력으로 인해 이루어지고 있는 것은 오늘의 컴퓨터 보안이 안고 있는 또하나의 근본적인 정보시스템의 문제점이라고 할 수 있다 (Furnell et al., 2001).

근래 들어 인터넷의 보편화와 함께 눈에 띄는 컴퓨터 응용프로그램의 추세 중의 하나는 소규모의 프로그램들이 인터넷 사이트로부터 전달되어 클라이언트 시스템에 설치되고 활용된다는 것이다. 즉, 매크로 프로그램이나 스크립트들, 플러그인들, 자바 애플렛들 등과 같은 모빌코드라고 하는 프로그램들이 바로 그 예이다. 특별한 통제나 검증이 거의 없이 일상적으로 전달되고 활용되는 이 프로그램들은 사용자들로 하여금 매우 심각한 보안상의 취약점을 갖게 하는 인터넷 활용 실태라고 할 수 있다 (Furnell et al., 2001). 이는 오늘날의 사용자들이 컴퓨터 보안에 관해 과거에 비해 매우 방만하거나 그 중요성에 대해 매우 의식이 낮은 때문일 것이다. 언제 어디에서도 쉽게 접할 수 있는 컴퓨터 활용의 환경과 전세계 어느 곳에 존재하는 컴퓨터일지라도 쉽게 접근할 수 있는 개방된 인터넷의 환경이 오늘의 컴퓨터 사용자들의 보안에 대한 무관심과 무의식에 최적의 토양을 제공했을 것으로 판단된다. 나아가서 바이러스 탐지 프로그램의 보편화와 이들에 대한 과신은 단지 이 같은 유형의 프로그램 개발회사의 과대선전 때문만은 아닐 것이다. 하루하루 증가하는 새로운 형태의 바이러스 프로그램들이 백신프로그램 개발회사들의 치솟는 주식가격이나 매스컴에서의 각광에도 불구하고 항상 이들을 비웃듯이 앞서가고 있다는 사실은 그리 신비스러운 것만은 아닐 것이다.

오늘날 주목을 받고 있는 컴퓨터 보안의 첨병 중의 하나는 침입탐지시스템을 들 수 있다. 과거에 발생한 다양한 컴퓨터 공격에 대한 분석과 경험을 토대로 불법적인 컴퓨터 접근을 사전에 예방하고자 활용되는 이 시스템들은 아직도 그 발전의 초기단계에 머물고 있다고 할 수 있다. 더욱이 과거의 경험을 통해서 알려진 흔적(signature)들을 토대로 해서 미래에 발생할 침입을 탐지한다는 점에서 바이러스 방

어프로그램과 유사한 한계점을 갖고있는 것이다. 즉, 계속해서 진화하고 변모하는 침입의 방법과 형태들을 전향적으로 발견하고 대처한다는 것은 그 자체가 내재적인 한계를 갖는다는 것이다. 게다가 잘못된 경고나 서비스 거절은 시스템의 가용성이나 효율성을 떨어뜨리고 기업의 신뢰성에 부정적인 효과를 초래할 수 있다. 따라서 상당한 수준의 침입탐지시스템이 개발되기 전까지는 민감한 보안의 필요성과 정보처리의 생산성 사이의 딜렘마는 지속될 것으로 보인다.

이 같은 컴퓨터 보안의 제반 난제들에 대한 효과적인 접근방법은 어떻게 이루어져야 할 것인가? 흔히 컴퓨터보안이 갖는 전문성이나 특수성으로 인해 많은 컴퓨터보안의 실무들이 국소적이고 기술적인 접근을 취해왔던 것이 현실이다. 그러나 특정한 기술 분야에 국한된 혁신이나 개선을 통해서만으로는 오늘날과 같이 고도의 다면화된 정보기술의 컴퓨터 시스템에 대한 효과적인 보안을 달성할 수는 없다. 컴퓨터 보안의 연결고리를 이루고 있는 제 분야가 체계적으로 연계되어 특정 기업이나 조직의 환경에 적합한 총체적인 보안 대책이 수립되어야만 타당성있는 결과를 얻을 수 있을 것이다. 즉, 기업의 여건에 적합한 보안정책의 수립에서부터 보안을 우선으로 한 시스템 아키텍쳐의 개발과 검증, 통합적인 보안절차와 도구의 구축 및 집행, 시스템 요원들뿐만 아닌 사용자들의 교육과 훈련, 지속적인 감사와 평가 등 총괄적이고 체계화된 보안시스템의 개발과 구현이 요구된다고 하겠다 (Dhillon, 1999).

5.2 컴퓨터 보안의 경영전략적 관점

빈번하게 세간의 주목을 집중시키고 있는 해킹사고, 바이러스 침입에 따른 시스템 마비, 내외부적 사고나 재해로 인한 정보시스템의 중단 등 오늘날 기업들이 크게 의존하고 있는 컴퓨터 시스템의 보안문제들로 인해 이들에 대한 기업들의 관심이 갈수록 높아져가고 있는 현실이다. 이에 따라서 기업들은 바이러스 탐지, 방화벽 설치, 첨단 암호법의 도입, 침입탐지시스템의 구축, 가상사설망의 설치, 자동 백업장치의 구입 등 새롭게 개발되고있는 보안기술들에 많은 투자를 하고있다. 기업이 처한 시스템 환경에서 컴퓨터 보안에 대한 최적의 투자 해결책을 모색하는 것은 매우 중요한 경영의 과제라고 할 수 있다. 즉, 증가하는 자원의 투입에 따르는 통제의 필요성과 함께 효율적인 보안을 위해 보다 체계적인 투자의 우선순위 결정의 중요성이 강조되는 것이다 (Ekenberg, 1995; Gallagher, 1998; Verton, 2001). 한편 Wood (1995)는 많은 보안전문가들이 컴퓨터 보안의 문제를 정보기술적인 문제로만

파악하는 것을 비판하며 기술문제가 아닌 경영문제로 인식할 것을 주장한다. 즉, 경영자의 전면적인 지원, 보안에 대한 명확한 정책, 구성원들의 중요성 인식, 그리고 정보자산에 대한 통합적인 관리 통제 등과 같이 기술적인 접근을 뛰어넘는 경영적 접근이 이루어져야 컴퓨터 보안 투자로부터 기대하는 성과를 가져올 수 있다는 것이다.

경영자들의 투자의사결정에 있어서 컴퓨터 보안 분야에 대한 관심은 투자에 따른 가치의 회수로 귀착된다. 즉, 컴퓨터 보안 시스템의 구현과 활용은 여타 기업의 자본투자와 마찬가지로 투자회수의 대상인 것이다. 컴퓨터 시스템에 대한 투자는 매우 철저한 자본예산과정에 따른 의사결정이 이루어지며, 유사하게 컴퓨터 보안의 투자에 대한 의사결정 역시 효익과 비용분석이라는 방법론에 근거할 수 밖에 없다. 문제는 컴퓨터 보안투자의 효익은 여타 자산의 투자와 달리 가시적인 결과를 제시하는 것이 어렵다는데 있다. 성공적인 컴퓨터 보안의 가치는 크게 두 가지로 요약될 수 있다. 하나는 보안위반에 따른 손실의 발생을 최소화하거나 손실을 사전에 예방하는 것이고, 다른 하나는 보안 강화된 기업의 시스템이 전자화된 경쟁시장에서 경쟁력 우위로 나타나는 것이다 (Stahl, 1992; Parker, 2000; Higgins, 1999).

컴퓨터 보안의 투자에 대한 평가로서 일차적인 부가가치는 손실의 최소화와 잠재적인 손실의 예방이다. 이것은 발생할 가능성과 발생하지않은 결과 사이의 인과관계를 검증하는 것으로서 측정이 매우 어려운 부분이다. 또한 과거에 발생한 사실과 미래에 발생할 가능성 사이에서 현재의 미발생을 보안의 효과로 파악하는데는 많은 어려움이 따르는 것이다. 오늘날 컴퓨터 보안의 투자효과에 대한 부정적인 시각은 이 같은 문제에 그 근원을 두고 있다. 더구나 급속도로 변화해 가는 정보기술의 환경 하에서 컴퓨터 보안은 타 자산에의 투자와 달리 기업의 요구변화나 기술적 변화에 따라 급격한 수익체감의 현상을 보이는 특성이 있기 때문이다 (Ross, 2002). 따라서 컴퓨터 보안과 관련된 단기적인 비용의 절감이나 수익의 창출과 같은 전통적인 투자회수의 기대는 평가기준으로서 적합하지 않다.

컴퓨터 보안의 실질적인 투자가치는 정보네트워크화된 오늘의 경제 여건 하에서 최소한의 생존전략이라는 측면과 보안 경쟁력의 효과로 나타날 장기적인 경쟁력 우위에 있다고 하겠다. 기업의 핵심기술 유출, 악성프로그램 침입으로 인한 돌발적인 정보시스템의 마비, 고객의 정보유출로 인한 기업이미지 추락 등과 같은 보안위반 사례들은 기업의 생존 자체를 위협하는 엄청난 손실을 초래할 수 있다. 이러한 위협들에 직접적으로 대응하는 생존전략은 최소한의 투자를 추구하고 상황 반응적인 접근으로서 항상 "뒤쫓아가는" 전략이라고 할 수 있다. 반면에 기업의 핵심기술

이나 정보시스템의 안전보장, 네트워크 상에서의 거래에 대한 고객의 신뢰, 위협적인 컴퓨터 환경 하에서의 신뢰성있는 시스템 가동 등은 궁극적으로 기업의 명성과 경쟁력 우위라는 장기적인 효과로서 가시화될 것이다. 이것은 단편적인 재무제표상의 수치로는 표시될 수 없는 내재적이고 함축적인 가치라고 할 수 있다. 다시 말하면, 보안전략을 경쟁전략과 연계시킴으로써 기업의 경쟁력 우위를 추구하고 나아가서는 이를 토대로 한 새로운 사업분야의 개척이나 진출을 가능케 하는 것이다. 이를 위해서는 네트워크 시대에서 컴퓨터 보안이 갖는 의미와 가치를 능동적으로 기업의 경영전략에 결합시킬 수 있는 경영자의 의식전환이 필요할 것이다.

VI. 결 론

오늘날과 같이 첨단정보화되어있는 기업들의 경영통제시스템 구조하에서 컴퓨터가 갖는 기능이나 역할은 그 어느 때보다도 더 중요하다. 즉, 개별기업 내 다양한 기능적 부서들 간의 통합적인 상호관계, 공급자와 최종소비자에 이르는 공급망의 한 부분을 이루는 기업 내외부 간의 긴밀한 협력관계와 의존관계, 그리고 통신네트워크를 통해 횡적, 종적으로 그리고 물리적, 논리적으로 연계되어있는 통제시스템으로서의 컴퓨터 시스템들은 기업의 경쟁력과 핵심역량으로까지 인식되고 있는 현실이다. 따라서 컴퓨터 보안은 이 같은 기업의 경쟁력과 핵심역량에 지대한 영향을 미칠 수 있는 분야로서 그에 걸맞는 관심과 투자가 필요할 것이다.

보안에 관한 오랜 역사와 경험에도 불구하고 본격적으로 정보사회로 나아가고 있는 오늘날의 현실에서 컴퓨터 보안은 아직도 수많은 과제들과 미지의 도전들에 직면하고 있다. 특히나 성공적인 시장 경쟁력을 위해서 고객과 사업파트너들, 그리고 조직구성원들로 하여금 자유롭게 시스템에 접근할 수 있도록 정보인프라와 네트워크를 개방해야하는 현실은 보안전문가들에게 매우 중대한 과제를 던져주고 있다. 아울러 갈수록 복잡해져가는 운영체제와 시스템 구조, 새로운 정보기술들의 출현으로 인한 기술적 진보에 후행적으로 쫓아가는 보안기술들, 컴퓨터 보안을 부담스러운 간접경비나 필요악으로 간주하는 경영자들의 부정적인 의식 등은 보안전문가들이 우선적으로 극복해야 할 중대 과제라고 할 수 있다.

많은 경영자들이 컴퓨터 보안을 단순히 새로운 정보보안기술의 도입과 활용으로만 인식하는 경향은 매우 위험한 것이다. 오늘날의 개방화된 통신네트워크와 컴퓨

터 시스템 하에서 국지적이고 기술지향적인 컴퓨터 보안의 접근 만으로는 기업의 신경적 중추로서 다면화된 컴퓨터 시스템의 기능과 역할을 충족시킬 수 있는 해결책을 얻을 수 없다. 개별적으로 운용되고 있는 컴퓨터 보안의 기능과 자원을 통합하여 시스템적으로 접근하는 체계의 구축이 효과적인 보안을 위해 요구된다. 아울러 컴퓨터 보안투자에 대한 전통적인 자본예산기법의 적용은 컴퓨터 보안의 특성상 매우 부적합하다. 바람직한 컴퓨터 보안은 컴퓨터 자산들에 대한 전략적 가치를 고려하고 기업의 필요에 적합한 보안전략 및 정책의 수립과 아울러 이들 자산의 공유와 보호에 관련된 위험들을 평가하고 이들을 관리하기 위한 보안통제의 구현을 필요로 한다. 이를 위해서는 시대상황에 대한 최고경영자의 정확한 이해와 장기적인 경쟁력 확보 차원에서 컴퓨터 보안의 가치를 인식하는 것이 무엇보다도 필요하다. 최고경영자의 미래에 대한 비전과 리더십 그리고 경영전략에서 출발하여 정보기술전략을 매개로 하여 보안전략으로 이어지는 정보네트워크와 인터넷 시대의 가치를 십분 지향하는 것이 성공적인 기업으로 나아가는데 중요한 토대가 될 것이다.

참 고 문 헌

Alexander, D; Bean, L.; & Harrast, S. "Information Protection Program," *Internal Auditing*, Vol.16, No.2, 2001, pp.8-12.

Barnard, L. & Solms, R. "The Evaluation and Certification of Information Security Against BS 7799, *Information Management & Computer Security*, Vol.6, No.2, 1998, pp.72-77.

Bellettini, C; Bertino, E.; & Ferrari, E. "Role Based Access Control Models", *Information Security Technical Reports*, Vol. 6, No.2, 2001, pp.21-29.

Bort, J. "Time for a New Security Model," *Network World*, Vol. 19, No. 30, July 29, 2002, pp. S6-8.

Cambridge Advanced Learner's Dictionary, Cambridge University Press, 2003.

Chin, S. "High-Confidence Design for Security", *Communications of the ACM*, July 1999, Vol.42, No.7, pp.33-37.

Davis, C. "An Assessment of Accounting Information Security", *The CPA Journal*, March 1997, pp.28-34.

Dhillon, G. "Managing and Controlling Computer Misuse," *Information Management & Computer Security*, Vol.7, No.4, 1999, pp.171-175.

Ekenberg, L.; Oberoi, S; & Orci, I. "A Cost Model for Managing Information Security Hazards", *Computers & Security*, Vol.14, No.8, 1995, pp.707-717.

Furnell, S; Chiliarchaki, P.; & Dowland, P. "Security Analyser: Administrator Assistants or Hacker Helpers?" *Information Management & Computer Security*, Vol.9, No.2, 2001, pp.93-101.

Gallagher, S. "Control will Cost You," *Information Week*, Feb. 23, 1998, pp.56-72.

Gordon, L. & Loeb, M. "Economics of Information Security Investment", *ACM Transactions on Information and System Security*, Vol.5, No.4, November 2002, pp.438-457.

Herold, R. "Case Study: An Information Security Program," *Computer Security Journal*, Vol.10, No.2, Fall 1994, p.17.

Higgins, H. "Corporate System Security: Towards an Integrated Management Approach," *Information Management & Computer Security*, Vol.7, No.5, 1999, pp.217-222.

King, C.; Dalton, C.; & Osmanoglu, T. *Security Architecture: Design, Deployment & Operations*, Osborne/McGraw-Hill: New York, 2001.

Kovacich, G. "Protecting 21st Century Information It's Time for a Change," *Computers & Security*, Vol.20, No.3, 2001, pp.207-213.

McHugh, J. "Intrusion and Intrusion Detection," *International Journal of Information Security*, Vol.1, 2001, pp.14-35.

Liddy, C. "Commercialization of Cryptography," *International Journal of Information Security*, Vol.5, No.3, 1997, pp.87-89.

Parker, D. "Risk Reduction Out, Enablement and Due Care In," *Computer Security Journal*, Vol.16, No.4, 2000, pp.37-41.

Ratnasingham, P. "Trust in Web-based Electronic Commerce Security," *Information Management & Computer Security*, Vol.6, No.4, 1998, pp.162-166.

Ross, S. "IS Security Matters: Vive le ROI," *Information Systems Control Journal*, Vol.2, 2002, pp.10-11.

Saltzer, J. & Schroeder, M. "The Protection of Information in Computer Systems," *Proceedings of IEEE*, Vol.63, No.9, 1975, pp.1278-1308.

Schell, R.; Downey, P.; & Popek, G. *Preliminary Notes on the Design of Secure Military Computer Systems*, Directorate of Information Systems Technology: Bedford, MA, 1973.

Schneier, B. "Security Pitfalls in Cryptographic Design," *Information Management & Computer Security*, Vol.6, No.3, 1998, pp.133-137.

Stahl, R. "Information Security for the Client/Server Environment," *Chief Information Officer Journal*, Vol.5, No.2, Fall 1992, pp.43+

Steinke, G. "A Task-based Approach to Implementing Computer Security," *Journal of Computer Information Systems*, Fall 1997, pp.47-54.

Tipton, H. & Krause, M. *Information Security Management Handbook, Vol.4 (4th Ed.)*, Auerbach Publication: Boca Raton, 2003.

Trompeter, C. & Eloff, J. "A Framework for the Implementation of Socio-ethical Controls in Information Security," *Computer & Security*, Vol.20, 2001, pp.384-391.

Verton, D. "Firm Tracks Threats, Not Vulnerabilities," *Computerworld*, July 9, 2001, p.10.

Wood, C. "The Charles Cresson Wood File," *Information Management & Computer Security*, Vol.3, No.4, 1995, pp.23-26.

ABSTRACT

An Approach to Computer Security from Management Strategy Perspectives

Park, Seong-Whoe*

The role and contribution of computers are beyond the question in this information-based society. Sometimes the high dependence on the computers are regarded as considerable threats to the businesses. One of such threats is the violation of computer security. While businesses in on-line network and Internet are becoming a main stream activities in many companies, they are exposed to many risks due to open computing infrastructures like Internet. Investments in computer security are in vogue because of expanding businesses in computer network and management's concern for such environments.

Management's expectation from such investments encounters a lot of disappointment in practice. It is due to the fact that traditional justification of investment in computer security does not lend itself to adequate outcome from Return on Investment perspectives. However, this does not mean those investments are ineffective for the money. Instead, the assessment of such investments should differ from traditional value measurements because security outcomes are mostly unmeasurable and invisible prevention and avoidance of losses.

This paper discusses the broad issues of computer security and investment in such areas. The argument forwarded is the justification of computer security should be based more on long-term and strategic pursuit such as competitive competence in e-commerce and open network environments. This requires the top management's foresight and vision for the business leadership in the future.

KeyWord : *Computer Security, Security Policy, Security Procedures, Management Strategy, Security Investment Assessment*

---

* Associate Professor, School of Management, Kang Nam University