제20회 한국정보처리학회 추계학술발표대회 논문집 제10권 제2호 (2003. 11)

보안위험관리시스템 개발에 관한 연구

김인중*, 정윤정*, 박중길*, 원동호**
*국가보안기술연구소 취약성분석센터
**성균관대학교 전기전자및컴퓨터공학과
e-mail : cipher@etri.re.kr

A Study on Implements for Security Risk Management System

InJung Kim*, YoonJung Jung*, JungGil Park*, DongHo Won**
*Vulnerability Analysis Center, NSRI
**Dept. of Computer Engineering, SungKyunKwan University

요 약

현재 기관들은 정보통신기반시설에 대한 위험을 여러 가지 다른 방식으로 분석하고 있다. 또한, 각종 위험관리방법론, 지침 및 절차, 수준 측정 등에서 사용되는 기준들 사이에는 일관성이 없거나 서로 비교할 수가 없는 경우가 많다. 해당 기관의 보안 목표와는 상관없이 보안시스템이 설치 운영되고 있으며 그나마 없는 경우도 많다. 또한 당국에 보고하는 위험 분석 결과와 실제 기관 내에 위험 통제를 하기 위해 사용하는 위험 분석 결과도 서로 다른 경우가 흔하다. 기관 전체 차원에서의 일관성 있는 보안위험관리 방법의 부재로 말미암아 경제적으로 효율적인 위험 관리가 불가능하다고 할 수 있다.

본 논문에서는 이러한 문제점을 해결하기 위하여 정보통신기반시설에 대한 보안위험관리시스템을 제안하고 이에 대한 구현 방안을 제시한다.

1. 서론

정보화가 고도화되면서, 우리의 경제·사회 활동 기반 구조는 정보통신기반구조에 절대적으로 의존하고 있어 사이버 안전이 확보되지 않은 정보사회는 어떤 재난보다 치명적인 위험에 직면해 있다.

일례로, 2003 년 1 월 25 일 오후 해외로부터 유입된 슬래머 웜은 초당 1 만 ~ 5 만 개의 패킷(404Byte)을 대량 생성하여 뿌림으로써 네트워크 공격을 하는 악성 프로그램으로 국내에 8 천 8 백여 시스템을 급속히 감염시킴으로써 전 세계 감염시스템(약 7 만 5 천개)의 11.8%로 일본의 약 7 배, 중국의 약 2 배에 달하였다.

특히, CAIDA 의 보고에 따르면, 1 월 25 일 출현한 웜에 의해 전세계의 취약점이 존재하는(패치가 안된) Microsoft SQL 서버 2000 의 90%가 10 분 이내에 감염된 것으로 판명되었다. (CAIDA : Cooperative Association for Internet Data Analysis)

슬래머 웜은 취약점이 있는 윈도우 서버(Microsoft SQL 서버 2000)를 감염시켜 동 감염서버를 이용하는 대학, 연구소, 기업 등 이용자의 인터넷 접속경로를 차단하고 감염 서버가 자동으로 불특정 다수의 다른 컴퓨터를 공격하여 네트워크 트래픽을 폭발적으로 증가시켜 감염된 서버 주변지역의 이용자들도 인터넷 접속경로가 차단되는 결과를 초래하였다. 또한, 감염된 서버가 있는 인터넷 사이트인 경우 서비스 제공이 불가능하여 접속경로에 장애가 없는 이용자들도 인터넷 서비스를 이용할 수 없는 상황이 발생하여 결국 정보통신시설이 집적되어 있는 IDC 에서 LAN 으로 연결되어 있는 서버중의 하나가 감염된 경우 내부망 트래픽이 폭주하여 연결된 서버전체(포탈, 쇼핑몰, 게임 등)에 인터넷 접속장애가 발생하게 된 것이다. 이렇게 감염된 서버로부터 발생한 공격 패킷으로 각 ISP 의 국제 관문국에서 심한 병목현상이 발생하여 해외 인터넷 사이트 및 해외 Root DNS 에 접속할 수 없었고, Root DNS 접속 재시도를 하는 과정에서 각 ISP 들의 DNS 에 과부하가 발생하여 국내 인터넷 소통에도 지장을 초래하게 된 것이다.

이러한 1.25 인터넷 대란의 사례는 우리에게 다음과 같은 교훈을 주었다. 첫째, 불법적 웜/바이러스를 사전에 예측하고 방지하기 위한 내부관리통제제도와 감독

당국의 적절한 감독의 중요성이 강조되었다. 둘째, 정보통신시설에 대한 보안시스템 구축에 대하여 경영층의 인식부족이 문제점으로 인식되었다. 위험부담이 없는 시설의 운영은 비현실적인 것이지만 이러한 현상 발생 시 이에 대한 원인파악 및 대응 방법이 소홀하였다. 특히, 인터넷대란과 관련하여 위험을 분석하지도 않았고 설령 분석하였다 해도 통제할 위험관리시스템이 없었다.

또 다른 보안위험관리의 실패 사례로 외국의 예를 보면 바이러스가 담긴 스팸 메일을 무차별적으로 발송하는 '소빅-F' 가 미국 동부지역 철도를 멈추게 만드는 사건이 발생했다[2]. 미 동부지역 철도를 운영하는 CSX 는 사내 정보기술 시스템이 스팸 메일 바이러스에 감염되면서 신호, 배차 시스템이 멈췄다고 밝혔다. 이에 따라 워싱턴 DC, 메릴랜드, 웨스트버지니아 인근 지역의 통근 열차와 남동부 지역 기차가 한때 운행을 중단, 아침 출근에 지장을 초래했다. 플로리다 주 잭슨빌에 본부를 두고 있는 CSX 의 신호 시스템은 이날 바이러스에 감염되면서 작동을 중단, 미시시피강 동부지역의 23 개 주를 맡고 있는 전체 CSX 시스템에 영향을 미쳤다. CSX 는 이날 낮 대부분 복구됐으나, 동부지역을 운행하는 열차들은 이날 밤까지 최고 6 시간씩 열차 운행이 지연되는 부작용을 낳았다.

만약 침해 사고에 대한 위험 상태를 볼 수 있었거나 위험 정도가 분석되고 보고가 되었더라면 이러한 상황은 발생하지 않았을 수도 있었다.

2. 보안위험분석의 관련 연구

1654 년 사람들이 E-mail 와 같은 방식을 사용하지 않고 직접 편지를 주고받는 방식을 사용할 때, 파스칼과 페르마는 확률의 기본적인 개념을 이용하여 문서를 전달하는 방법을 제시하면서 이를 위험관리 한 분야로 설명하였다. 최초에 파스칼의 의도는 도박에서 좀 더 유리할 수 있도록 하기 위함이었으나 최근에는 새로운 기법/경영의 도입에 따른 모험에 대하여 최상위자의 판단에 도움을 주고자 변경되었으며 최근 전자상거래가 도입됨에 따라 재정과 관련된 기법에 많이 적용되고 있다.

이후 경영측면에서 연구되던 위험분석 분야가 정보통신분야에서도 연구 되었는 데 관련 연구로는 미국 NIST 에서 개발한 GMIT[3]이 있고, 캐나다에서는 CSE 가 있으며 영국에서는 BS7799[4]를 제정하였다. 특히, BS7799 는 ISO17799 라는 표준을 만들어 사용하고 있다. 따라서 국내에서도 표준화를 위한 작업이 시도 되었는 데 TTA 에서 제정한 표준[5]이 있으나 대부분 GMIT 을 참고로 한 모델로써 국내 현실이 제대로 반영되어 있지 않다. 이외에도 한국전산원에서 개발한 HAWK 가 있으나 현재는 사용하지 않고 있다. 물론 정보보호컨설팅 업체나 관련 업체들이 고유의 방법론을 개발하고 적용하고 있으나 공통으로 통일화되어 있는 것은 없는 실정이다. 가장 이상적인 방법은 각각 기관마다 자체 지침을 개발하여 사용하는 것이 가장 바람직하지만 위험관리방법론을 개발하는 것이 매우 어려운 작업이므로 이에 대한 국가적 표준 가이드라인을 만들고 이에 대한 세부적인 지침을 제정하는 것이 바람직하다고 본다. 따라서, 지금이라도 위험관리과 관련한 표준화를 시작하는 것이 국내 정보통신기반시설에 대한 보호와 예방에 많은 도움이 되리라 본다.

하지만 위험관리는 매우 어려운 것이 현실이다. 이는 자산식별이 어렵기 때문이다. 자산을 식별하기 위하여 자산의 가치를 산정하고 자산에 대한 중요도를 따지다 보면 위험분석을 시작하기도 전에 이미 많은 시간과 인력이 소요된다. 예전과 같이 간단한 시스템인 경우에는 분류가 가능하였으나 이제는 많은 종류의 시스템이 존재함에 따라 담당자조차 시설에 대한 정확한 분류가 어렵기 때문이다. 특히 예전의 시스템의 경우에는 하드웨어 자산과 소프트웨어 자산을 분류할 수 있었으나 이러한 자산의 경계도 명확하게 구분하기가 어려워진 것이 더 큰 어려움이다. 또한 데이터베이스와 관련된 자료에 대한 가치를 산정하기에는 어려운 점이 있는 것이 데이터베이스는 항상 백업을 해놓고 있으므로 데이터베이스가 파괴되거나 변조되는 일은 사실상 존재하지 않는다. 따라서 자산에 대한 식별은 현실적으로 불가능하며 이에 대한 자산 식별 및 자산 가치 산정을 어렵게 한다.

다음으로 현재 자산은 혼자 독립적으로 수행하는 것이 아니다. 서버가 중요하기는 하지만 네트워크 시스템의 하나만이라도 장애를 일으키게 되면 전 시스템이 망가지거나 불능사태를 일으킬 수 있는 것이 현재 정보통신기반시설의 가장 큰 고민중의 하나이다. 이러한 개개인의 자산들의 특징을 분류하는 것이 어려운 상황에서 보안서비스의 3 요소, 가용성, 무결성, 기밀성 등을 다시 분류한다는 것은 거의 불가능에 가깝다는 것이 다양한 위험분석 평가를 수행한 결과이다.

자산식별을 어렵게 끝내고 나면 위험 분석을 수행해야 하는 데 위험에 대한 분류 및 분석 또한 매우 어려운 것이 현실이다. 데이터에 대한 위험을 식별하기 위하여 대부분의 위험관리방법론은 인터뷰, 설문, 토론에 많이 치중하게 되며 이러한 주관적인 판단은 결국 각각의 자산을 가지고 이루어지기 때문에 엄청나게 많은 시간과 인력이 소요되는 것이다. 예를 들어 A 기관의 정보통신기반시설이 10 개의 자산을 가지고 있다고 하자. 각각의 자산에 대한 위협원을 알기 위하여 각자 가지고 있는 위협 DB 를 사용하거나 인간, 비인간, 또는 의도적, 비의도적 등으로 구분한다. 이 경우 10 * 4 = 40 가지의 경우를 고려해야 한다. 위협에 대하여 취약성이 2 개씩 존재한다면 80 가지, 이 80 가지에 대한 보안 대책을 2 개씩만 고려한다면, 160 가지의 보호대책이 나타나는 데 보안 대책이 160 가지라면 대부분의 보안 대책을 제시하였다고 할 수 있다. 이에 대한 결과에서 비용 대 효과를 제시하기 위하여 160 가지에 대한 보안 장비에 대한 비용을 구해야 하고, 만일 보안 대책을 세웠을 때와 안세웠을 때를 비교하게되면 360 가지를 가정해야 한다. 다음으로 위험이 감소되었다면 얼마나 감소 되었는 지를 분석해해야 한다. 따라서, 작은 규모의 시스템이 이러한 작업을 수행해야 하는 데 몇 백 개 아니 몇 십 개의 자산이

식별되었다면 아마도 슈퍼컴퓨터를 돌린다고 해도 결과 값을 알 수가 없게 된다. 따라서, 지금 현재 존재하는 대부분의 위험분석방법론은 이론적으로 합리적일 수 있으나 현실적으로 적용하기에는 많은 어려움이 존재하므로 컨설팅을 하는 경우 간단히 언급하는 경우에 그치고 만다.
본 논문에서는 위험관리방법론을 제정하기 위해서 다음과 같은 조건을 제시한다.

1. 먼저 위험분석방법론은 어느 누가 해도 비슷한 결과가 나와야 한다. 예를 들어, 전문가가 할 때와 비전문가가 할 때 다르고, 같은 사람이 시간이 경과한 후에 다시 시도하였을 때 다른 결과 값이 나오고, 하나의 함수나 벡터 값을 변경함으로써 전체 결과가 바뀌게 된다면 이는 좋은 위험분석방법론이라고 할 수 없다.
2. 다른 종류의 시스템을 분석하였는 데 비슷한 결과 값이 나오게 하는 것은 좋은 위험분석방법론이 아니다.
3. 한 기관에서 정보시스템에 대하여 다른 방법론을 사용하게 되는 경우 다른 결과가 나올 수 있다. 이는 방법론의 차이에 따라 위험도가 다르게 나올 수 있으며 같은 방법론이라고 해도 컨설팅의 능력에 따라 차이가 발생할 수 있다. 이와 같이 신뢰성의 차이가 많이 발생하는 데 이러한 신뢰성을 많이 줄일 수 있는 방법론 요구된다. 이는 현재 개발되어 있는 방법론은 매우 복잡하고 어려우며 애매한 요소가 많이 존재하는 데 이는 경영측면의 방법론을 그대로 적용하기 때문에 발생하기도 한다.

3. 보안위험관리에 대한 분류

정보통신기반시설에 대한 위험관리(risk management)에 대한 논의는 보통 위험을 두 가지 또는 세 가지의 범주로 나누게 된다. 즉 정보, 데이터 등 무형자산과 관련된 위험(Immaterial risk)과 통신, 소프트웨어 등 유형자산과 관련된 위험(Material Risk)으로 나누기도 하고, 이러한 무형자산과 유형자산 이외에 이러한 시스템을 운영하는 위험(operational risk)으로 나누게 된다. 통신, 소프트웨어 등 유형 자산과 관련된 위험은 일반적으로 실체가 분명하고 감가상각, 유효기간, 개발비 등 변수의 값이 변할 때 야기되는 변동성에 따라 자산가치를 재 산정하게 되므로 이에 대한 위험관리에는 어려움이 없다.
그러나 정보, 데이터 등 무형자산과 관련된 위험의 경우에는 이것을 어떤 시각에서 보느냐에 따라 사람마다 보는 견해가 다르고 이에 따라 측정 방법과 측정된 값도 서로 다른 의미를 갖게 된다. 웹 서비스를 이용한 은행 서비스를 예로 들어본다. 네트워크를 운영하는 ISP 업체나 시스템을 관리해주는 용역업체의 침해사고로 인하여 각종 중요 자료가 변조되거나 파괴되는 경우 시스템 복구비용 및 고객의 직접적인 손해로 인하여 발생하는 피해 액만을 고려할 수 있다. 은행의 경우에는 자신들의 이익을 실현시키지 못한 부분과 거래 상대방과의 의무불이행으로 인한 손실, 은행 이미지 등을 고려할 수 있다. 고객의 입장에서는 상대방과의 업무 지연으로 인하여 발생한 물리적 피해 이외에 정신적 피해를 고려하고 타 은행 서비스로 전환하여 처리한 비용까지 고려하게 된다.
이렇게, 비록 이러한 위험 모두는 침해 사고로 인한 발생한 것이지만 해당 기관들이 위험을 분석하는 접근방법이 다른 기관의 위험 분석에도 반드시 적합하다고 볼 수 없을 것이다. 그리고, 기관마다 침해사고에 대한 위험을 분석 기준이 다를 수 있다. 예를 들어 국방과 관련된 시스템의 경우 정보에 대한 기밀성이 매우 중요하므로 다른 보안 서비스보다 더 집중하게 되며, 은행과 관련된 시스템의 경우 개인의 정보보호를 위하여 인증 및 무결성에 많은 초점을 맞추게 된다. 무역과 관련된 시스템은 가용성에 위험 분석을 강화할 것이다. 그러므로 우리나라 기관들의 경우 위험을 측정하는 시스템을 구축함에 있어서 이러한 점을 잘 이해하여 성격에 맞는 위험관리시스템을 구축하여야 할 것이다.

4. 보안위험관리시스템의 구축

이러한 여러 가지의 문제를 해결하기 위해 정보통신시스템에 대한 전사적 보안위험관리(enterprise-wide security risk management) 시스템의 개발이 요구된다. 전사적 위험관리란 말 그대로 기관 전체의 차원에서 침해요소에 대한 위험을 측정하고 관리함으로써 보안위험관리가 기관의 전체 목표와 일관되게 만드는 것을 말한다. 즉 모든 부문의 위험을 일관성 있게 측정하여 부문간 비교가 가능하도록 만들 뿐만 아니라, 합산이 가능하여 기관 전체 차원에서 위험파악과 이를 통한 보안대책 수립으로 효율적인 보안위험 관리가 가능하게 된다. 뿐만 아니라 장단기 보호대책을 세운 후 위험조정을 통하여 기관의 보안 의 극대화와 일관성 있는 기관의 보안목표를 추구할 수도 있고, 또 이를 수행함으로써 비용의 절감과 업무의 효율성을 가져올 수도 있다.
전사적 보안위험관리시스템은 CSO(Chief Security Officer)를 중심으로 문서, 인원, 정보시스템등을 관리하는 조직을 통합하여 기관의 보안과 관련한 전체 위험을 총괄 관리하는 시스템을 말한다. 전사적 보안위험관리가 성공적으로 이루어지기 위해서는 위험관리조직, 위험관리과정, 위험관리시스템의 3 박자가 갖추어져야 한다. 우선 전문적이고 유연성이 있으며 힘이 있는 위험관리 전담조직이 필요하며 이 부서는 전사적인 차원에서 위험을 다룰 수 있도록 조직도상에 위치하여야 한다. 또한 위험을 모니터하고 통합관리하는 절차를 확고히 할 수 있도록 업무의 프로세스가 변해야만 하며, 이를 과학적으로 분석하고 뒷받침할 수 있는 도구로써 시스템이 구축되어야 한다. 위험관리시스템 자체는 단지 수치를 제공하는 소프트웨어에 불과하므로 이를 운용하는 조직과 인력 및 과정이 잘 정립되어 실제 기관의 의사결정과정에 이용되어야 그 생명력이 있다고 할 수 있다.

이러한 전사적 위험관리시스템을 구축하는 과정에서 서로 다른 시스템 및 기관에서 계산된 서로 다른 위험의 비교 및 통합 문제에 직면하게 된다. 앞에서도 언급하였듯이 위험의 발생율, 파급 효과 등이 매우 가변적이기 때문이다. 특히 정보통신기반시설의 경우 파급효과가 다른 기관에 영향을 미치므로 양자간에 상관관계도 계산해야 한다.

보안위험을 통합하는 과정에서 해결하여야 하는 점은 위험에 대한 변동을 항상 확인하고 있어야 한다는 것이다. 이러한 분석 관리는 작게는 보안권고문의 확인에서부터 크게는 물리적 사회 현상까지 분석을 해야 한다는 것이다. 변화 시나리오에 대한 일관된 가정 적용 등을 위하여 위험관리 전담조직에서 실시간으로 모두를 관리하는 것이 바람직하며 이를 위한 체계적인 보안위험관리시스템의 구축이 요구된다.

5. 보안위험 데이터웨어 하우스의 개발

어떤 형태로든 위험관리를 행하는 조직들의 공통의 목표는 그들의 보안 침해에 대한 보호대책을 통해 안전한 시스템 운영이라 할 수 있다. 그런데 시스템의 다양화와 개별 업무가 복잡해짐에 따라 전체 위험을 일괄 관리하는 것은 전산시스템과 데이터시스템이 없이는 불가능해졌다. 특히 짧은 순간의 침해사고에 대하여 피해 효과가 큰 현재 시스템 구조상 실시간의 보안위험관리(real time risk management)가 필요한데 이 역시 전산시스템과 데이터시스템의 도움 없이는 불가능하다.

물론 데이터시스템의 경우 전산시스템의 일부분으로 볼 수도 있지만 굳이 구분해서 설명하는 것은 이것이 위험관리에 있어서 매우 중요하기 때문이다. 기관들이 위험관리시스템을 구축함에 있어서 직면하는 근본적 어려움은 관리하고 있는 자료로부터 필요한 정보를 어떻게 다 수집하고 또한 이용할 수 있도록 만드느냐 하는 것이다.

위험 관리자가 직면하고 있는 가장 큰 문제 세 가지는 자료의 질과 충실성, 통합된 정보의 부족 그리고 정보의 적시성이라고 하였다. 위험 관리자들은 또한 성공적 시스템의 가장 중요한 요건 중 하나로서 통합 정보의 이용가능성을 들고 있다. 이러한 분석 결과는 위험분석에 사용할 수 있는 형태의 자료를 생산하기 위한 보안위험관리시스템에 대한 개발이 필수적이다.

이러한 문제는 기관, 운영시스템, 컴퓨터 하드웨어에 관계없이 어떤 유형의 정보든 다양한 정보원으로부터 수집될 수 있도록 도와주는 보안위험데이터웨어하우스의 구축을 통해서 성공적으로 해결될 수 있다. 이는 원하는 만큼 자주 정보를 수집할 수 있게 해줄 뿐만 아니라 일관성 있고 쉽게 이용할 수 있는 포맷으로 정보를 변환시킬 수 있게 해준다. 데이터웨어 하우스는 시장 및 포지션 자료를 포함하고 있는 각각의 시스템으로부터 단순히 자료를 추출하는 것보다 훨씬 더 많은 것을 제공해준다. 전사적 보안위험관리는 '우리 기관의 발생한 취약점은 현재 얼마인가?' 또는 '전세계에 걸친 취약점은 얼마나 되는가?' 등의 질문에 답하기 위해 정확한 자료를 필요로 한다. 위험관리자들은 효율적인 데이터웨어하우스를 구축함으로써 자료의 타당성에 대해 확신을 가지고 기관 전체 차원에서의 위험분석과 관리를 수행할 수 있을 것이다.

6. 결론

포괄적인 위험분석과 보고는 위험관리의 양대 축이다. 대부분의 기관은 운영하고있는 시스템의 안정성을 보장해야만 하는데, 그와 같은 안정성은 기관이 노출되어 있는 위험의 성질에 달려있다. 지금까지의 솔루션들은 정보통신기반시설에 대한 보안위험관리와 관련하여 어떠한 정보도 제공하지 못했다. 또한 현 시스템에 위험관리를 적용하지 못하고 극히 일부 취약점 분석 평가를 통하여 일부 적용한 것이 전부이다. 이러한 제한적 접근법들은 위험의 특정한 측면들을 알게 해주는 기능이 있는 것은 사실이지만 전사적 관점에서는 별 도움이 되지 않았던 것이 사실이다. 그러나 기관의 증대와 각종 시스템의 발달로 인해 전사적 차원에서 위험을 측정하고 보고하는 것은 일상적이고 필연적인 기관의 업무가 된 것이다.

지속적인 컴퓨터 능력의 혁신과 인터넷의 발달은 전세계적 시스템의 완전 자동화 및 24 시간 운영을 수행하고, 기관과의 연동이 광범위하게 추진되고 있다.

이제 과거의 취약점분석 상황을 제공하는 것 대신에 미래에 대한 전망 리포트로 대체하고, 위험 감소 및 잔여 위험분석을 통한 기관이 가진 위험과 보호대책 수립간의 관계에 따라 복합적으로 결정해야 한다. 기관들은 위험을 적절히 관리할 수 있어야만 보다 많은 서비스를 수행할 수 있다. 미래의 기관들은 위험관리 기능을 단순한 비용 지출이 아닌 반드시 필요한 요소로 바꿔 생각해야 할 것이며, 심각한 보안 위험은 제거하고 해결 가능한 위험은 허용하는 것이 바람직하다.

한편, 기관도 중요하지만 국가에서 사용할 수 있는 위험분석 방법론의 표준화가 필요하다고 본다. 현재 위협요소는 새로이 많이 발생하고 있고 이러한 위협에 대하여 적절하고 신속하게 대응하기 위해서는 많은 시나리오를 작성하고 이 시나리오에 따라 대응할 수 있는 교육이 이루어져야 한다. 이를 위하여 적절한 방법론이 만들어져야 하고 방법론에 필요한 각종 데이터베이스를 구축해야 한다. 자산, 취약성, 위협에 대한 데이터웨어하우스를 구축하고 보호대책을 세울 수 있는 표준화 계획이 요구된다.

참고문헌

[1] 정보통신부, "정보통신망 침해사고 조사결과", www.mic.go.kr, 2003.2.18.

[2] http://www.cbsnews.com/stories/2003/08/21/tech/main569418.shtml, 2003.8.21

[3] ISO/IEC13335, Guidelines for the Management of IT Security(GMITS), 1996

[4] ISO/IEC17799, Code of Pratics for Information Security Management, 2000.

[5] TTAS.KO-12.0007, "공공정보시스템 보안을 위한 위험분석 표준-위험분석방법론 모델," 2000.