정보시스템에서 사이버 침해에 따른 잔여위험분석 및 보험산정 연구

김인중*, 정윤정*, 박중길*, 원동호**
*전자통신연구원, **성균관대학교 정보공학과
e-mail:cipher@etri.re.kr

A Study on the Residue Risk Analysis and Insurance Estimation toward Cyber-Intrusion in Information System

InJung kim*, YoonJung Chung*, JoongGil Park*, Dongho Won**
*ETRI, **ICSL, Sungkyunkwan University

요 약

중요 정보시스템에 대한 위험분석 프로세스는 자산 식별을 통해 위협, 취약성을 분석하고 이에 보호대책을 수립한다. 하지만 모든 보호대책을 적용하기에는 비용 대 효과면에서 불가능한 경우가 발생한다. 따라서, 잔여위험에 대한 분석을 통해 해결할 수 없는 위험에 대해서는 보험을 통하여 보호대책을 세워야 한다.

본 논문에서는 위험분석을 통해 계산된 피해 산정으로 사이버침해에 따른 보험 수준을 산정하는 방안을 제안하고자 한다.

Key word: Risk Analysis, Asset, Threat, Vulnerability, Safeguard, Insurance

1. 서론

네트워크와 IT 기술의 발달로 인하여 점차 유비쿼터스 시대가 도래하고 있다. 이러한 IT 시스템은 네트워크 광대역화와 컨버전스화로 기관·산업체간 경계가 붕괴되면서 기존에 보안을 고려한 폐쇄망 운영 방식이 개방화 시도를 보이고 있다. 이는 개방화를 하는 경우 비용 대 효과면에서 이익을 극대화할 수 있으며 대국민 서비스의 향상을 통해 기업의 이미지를 높일 수 있기 때문이다. 이러한 시도는 IT 서비스-인프라-제어시스템 등을 연계한 통합 솔루션을 통해 부가가치 유발효과를 노리면서 다양한 국민의 정보이용 욕구를 충족시키는데 많은 도움을 제공하게 될 것이다. 특히, 가정의 이용자가 홈 네트워크를 통해 교통, 위성, 가스, 전력, 유무선 통신의 서비스를 제공받게 된다면 막대한 경제·산업적 파급효과가 기대됨과 동시에 생활의 다양화와 편리성 증대에 기여함으로써 국가적 삶의 질을 높이고 국민의 정보이용 및 여가수준을 향상시킬 수 있을 것이다. 하지만 국가적으로 중요한 중요 정보시스템에 대한 정보화 및 컨버전스는 주요 정보 자산에 대한 노출에 따른 기밀성, 무결성 등을 충분히 고려해야 하며, 서비스 중단 등 가용성에 따른 피해가 예측가능해야 한다.

실제로 정보화 사회의 진전과 더불어 사이버 침해사고는 빠른 속도로 증가하고 있는데, 1999년에서 2003년 사이에 미국에서 발생한 침해사고는 총 137,000건으로 약 530%이상 증가하고 있다. 이러한 사이버 침해 사고에 의하여 금융부분에서만 약 2,200억 달러의 손실이 발생하였다[1].

이러한 손실을 해결하기 위하여 각종 사이버 침해에 대응하기 위한 정보보안 관리방법이 연구되고 있는데 GMITS[2]이나 ISO17799[3] 등이 있으며 기관별로 체크리스트를 활용한 방법[4]이 보편화되어 사용하고 있다. 하지만 이러한 방법론들은 위험을 분석하고 보호대책을 어떻게 해야 하는 지에 대한 절차만을 정의되어 있으며 보호대책[5]이 수립되지 못하거나 불가능한 경우에 발생될 피해 산정[6] 및 피해에 따른 대비책(보상, 보험 등)에 대한 어떠한 방법도 제시하지 못하고 있다.

본 논문에서는 이러한 정보보호 서비스에 대한 위험분석시 필연적으로 발생하는 잔여 위험[7]에 대

한 보호대책으로 피해에 대한 보험 산정 방안을 제안한다.

2. 국내 침해사고 보험 현황 및 정의

최근 개인신용정보의 보안이 중요시되는 은행 증권 신용카드 등 금융회사들이 사이버 위험보험을 많이 가입하고 있다. 이에따라, 2004년 국내 모증권사는 전산실 직원의 프로그램 운영 과실로 온라인거래가 일시중단된 적이 있어 보험사로부터 7,000만원을 지급받았다. 또 증권사의 사이버거래 시스템 오류로 고객이 제때 주식매도 주문을 내지 못해 발생한 손실 5,600만원도 보상해줬다. 2000년 10월에는 인터넷정보관리업체 직원의 실수로 보조전력장치가 가동되지 않아 이를 이용하는 온라인쇼핑업체가 손실을 봤고 보험금 7,300만원을 받았다. 이러한 사이버 위험에 따른 배상한도는 보험료와 보장하는 위험에 따라 다르지만 손해 범위가 워낙 넓어 대부분 사고당 5억~10억원이며 최고한도는 20억원 수준이다. 보험료는 1000만원에서 수 억원까지 다양하다. 한 통신업체는 총 보상한도를 20억원으로 정했을 때 연간 보험료가 6,300만이었다.

이러한 보험의 유형은 전산시스템의 미비 등 전산시스템 운영자의 잘못에 따른 배상책임과 관련된 것이 대부분이다. 이는 관리적인 측면과 가용성 측면만을 고려한 것으로 침해에 따른 기술적인 측면과 기밀성, 무결성에 따른 피해를 고려하지 않고 있다. 다만 일부 인터넷데이터센터(IDC)가 입주한 업체를 대상으로 해킹 등으로 정보가 훼손되거나 서버 기능에 문제가 생기는 피해를 입었을 때 일부 비용을 지급하는 보험을 이용하고 있다. 하지만 해킹에 따른 피해를 사전에 가늠하기 어려워 보험요율 산정이 쉽지 않으므로 보험회사에서 배상부담을 기피하거나 지급을 반대할 가능성이 있다. 또한 국가적 중요정보시스템에 대해서는 보험 산정에 대한 논의조차 이루어고 있지 않다. 하지만 앞으로 인터넷이 점점 더 생활의 큰 부분을 차지하고 컨버전스화되면 예기치 못한 사고로 발생할 손실규모도 커질 것으로 예상돼 침해사고에 대한 보험에 대한 관심이 요구되고 있는 실정이다.

본 논문에서 제시하는 기본적인 보험의 성립요건은 중요 정보시스템의 컴퓨터 네트워크에 해커가 침입, 운영정보를 빼내 불법행위에 이용했거나 컴퓨터 바이러스로 각종 고객정보가 손상돼 기관이나 제3자가 피해를 봤을 때, 정보시스템의 잘못된 정보로 인하여 생활에 불편이나 피해가 발생하였을 때 금전적 손해를 보상해주는 것을 기본으로 한다. 또한 온라인 관련기관의 서버가 바이러스에 감염된 것을 모르고 사용자가 접속했다가 정보나 데이터베이스, 프로그램 등이 손상되면 재산상 손실은 물론 복구비용까지 물어주는 것을 포함한다.

3. 사이버침해에 따른 잔여위험분석

앞으로 중요 정보시스템을 운영하는 기관에서는 전자거래 및 전자 정보에 대한 침해 피해에 대해 배상책임을 질 것으로 보인다. 이는 비밀번호 등 접근장치의 위/변조 또는 정보의 전자 전송/처리 과정에서 발생한 사고로 인한 이용자 손해에 대해서는 원칙적으로 해당 기관에서 책임을 부담해야 하며 해킹 피해의 책임 주체를 해당기관에서 규정해야 하기 때문이다. 이에따라, 사이버 침해에 대한 배상을 위한 준비를 해야 한다. 이러한 배상 부담을 피하기 위하여 보험을 고려하게 되는 데 보험 산정을 위해서는 정확하게 현 시스템에 대한 위협과 취약성이 무엇인지 확인해야 한다.

중요 정보시스템에 대한 보험을 들기 전에 위험분석을 실시하여 위험의 수준과 보호대책의 범위를 파악한다. 위험을 분석하기 위하여 일반적으로 사용되고 있는 방법론은 그림 1과 같다. 일반적으로 위험분석을 실시한 후에 보호대책을 선택하고 위험 수락(risk acceprance)을 한다. 하지만, 사이버 침해에 대한 발생은 현실적으로 위협과 취약성이 계속 증가하므로 100% 보안 대책을 수립한다고 해서 해결될 사항이 아니다. 예를들어, 서버가 윈도우즈 시스템이기 때문에 주기적으로 새로운 취약성이 발견된다고 해서 이상적인 새로운 보안 운영체제의 도입을 도입할 수는 없다.

따라서, 비용 대 효과를 극대화하는 시점에서 보호대책을 수립하여 운영·관리하면서 나머지 부분에 대해서는 보안정책과 지침을 통해서 꾸준히 위험요인을 제거해 나가야 한다. 그럼에도 불구하고 사이버 침해로 인하여 피해가 발생하게 되면 피해 산정 후 보험을 통한 피해 보상을 통해 꾸준한 정보보호 대책을 수립해야 나가야 한다. 다만 보험 가입이 모두 허용하는 것이 아니고 보험이 필요한 경우를 다음과 같은 환경으로 제한한다.

- 위험에 대한 보호대책을 수립하는데 예산이 즉시 반영되지 않는 경우
- 위협 및 취약성이 발생할 확률이 극히 낮은 경우

- 피해 발생시 기밀성, 무결성에 영향이 없으나 가용성 복구에는 많은 시간이 걸리는 경우
- 요구되는 보호대책 비용이 상대적으로 많은 경우
- 보호대책 수립 전 시스템 변경/이전하는 경우 등

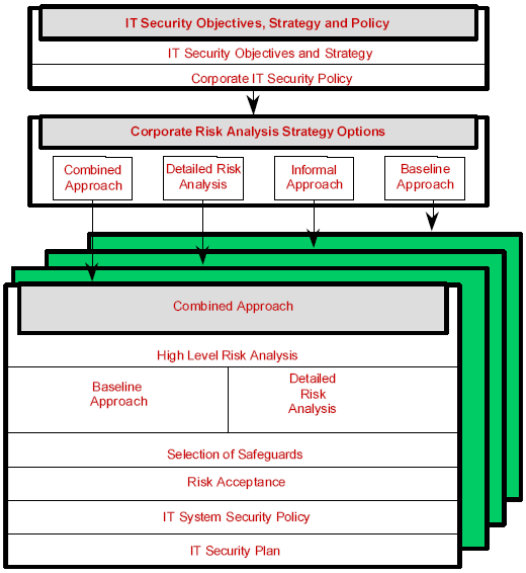

그림 1. GMITS 위험분석 프로세스

4. 사이버침해에 따른 보험 비용 산정

보험을 통해서 중요 정보시스템에 대한 개방화 및 연동이 가능하지를 분석하는 기법이 중요하다. 예를 들어, 정보보호수준이 약하거나 보완해야 하는 경우에는 사이버침해에 따른 보험을 제한할 수 있어야 한다. 특히, 정보에 대한 가치는 상황적, 상대적이므로 정보에 대한 피해 발생시 보험 가액을 정하는 것이 정성적일 수밖에 없다. 이러한 차이점이 기존 생명보험이나 재해보험과의 차이점이라고 볼 수 있다. 표 1은 기존 보험과의 차이점을 보여주고 있다.

표 1. 기존 보험과 사이버침해보험과의 구분

	기존 보험	사이버침해보험
자산의 형태	유형	무형
자산의 흐름	고정	변동
자산의 가치	감소	증가
패해 산정	자산가치 비율	정보가치 비율
보험 가액 요인	자산 규모	정보보호 수준
주요 보험 수가 항목	하드웨어 구입비용 또는 재활비용	복구비용, 기관 이미지
피해 원인 예측	가능	불가능

시스템을 관리하는 기관은 보호대책비용과 보험비용을 포함하여 전체비용을 계산하며 전체비용이 가장 낮은 지점에서 정보보호 설계를 수행한다. 그림 2는 이에 대한 보호대책비용 대 효과 분석 그래프이다.

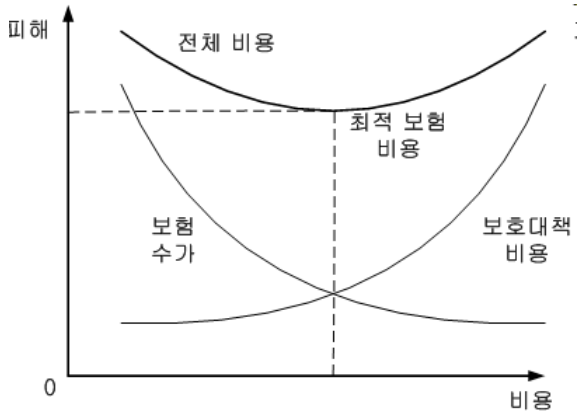

그림 2. 보호대책 비용 대 최적의 보험 비용

이러한 비용을 산정하기 위해서는 자체 통제항목을 개발하여 해당 항목에 대한 점수를 계산한다. 보험비용은 해당 침해 사고가 통제항목에서 이미 해결된 것인지 아닌지에 많은 영향을 미치게 된다. 통제항목의 개발을 위하여 각종 정보보호 지침이나 검사기준들을 활용하며, 컨설팅을 통해 얻을 수 있다. 또한 보호대책을 세워야 할 부분과 보험으로 해결해야 할 부분을 정하고 보험의 경우 해당 자산에 대한 취약성/위협이 발생할 확률을 정확하게 계산하여 피해액을 산출한다.

- 피해액 = 자산의 가치 * 해당 위협 발생 확률
- 보험비용 = 전체 피해액 * 보험수가

고려해야할 항목으로 가용성 측면을 고려한 보험에 대한 정량적 수치 계산은 가능하나 정보에 대한 기밀성/무결성 측면은 수치 계산이 어렵다. 따라서, 기밀성/무결성에 대한 정량적 수치 계산은 기관 담당자와 위험분석 담당자, 보험 설계사간의 델파이 기법을 이용한 토론으로 피해 비용을 조정한다.

5. 사이버침해에 따른 피해 산정

기존 보안대책에서 수립된 상황에서 피해가 발생한 경우에는 기관의 부주의한 실수에 의한 것이므로 이때는 보험 지급을 거절할 수 있으나, 불가항력적이거나 새로운 위협 및 취약성으로 인한 위험손실인 경우에는 피해로 인정해야 한다. 이를 위하여 컴퓨

터 포렌직스를 이용하거나 관련기관과의 공동조사를 통하여 원인을 파악한다. 단, 차후에 동일한 피해가 발생하지 않도록 복구 대책을 동시에 적용시키는 것을 보험 내에 포함시키도록 한다.

5.1 자산의 분류

자산의 분류 방법은 여러 가지 방법이 존재하지만 건물, 인력 등을 제외한 정보자산에 대하여 피해를 산정한다. 즉, 사용 여부에 관계없이 재산적 가치를 지니고 있는 건물과 같은 시설을 비롯하여 기계/기구 및 장치, 저장 또는 보관중인 동산, 구축물 등은 제외하며, 정보 및 정보시스템, 그리고 정보를 보관하는 장치 등을 모두 자산으로 분류한다. 자산의 분류 방식은 기밀성, 무결성, 가용성 측면으로 구분한다.

5.2 피해 비용 산정

피해산정은 자산이 침해로 인하여 중단 및 정지, 노출 및 도난, 변조등의 피해가 발생하였을 때 그 가치의 감소 또는 파급 정도가 얼마나 발생하였는지를 알기 위하여 매우 중요하다.

자산에 대한 피해산정은 피해가 발생한 때와 위치에 따라 다를 수 있다. 따라서, 피해 가액 평가시에는 자산에 대하여 매년 위험분석을 통해 시가를 산출한다. 피해에 대한 분류는 다음과 같다.

- 침해에 따른 직접비용
- 침해에 따른 복구비용
- 침해에 따른 대체비용

또한, 사이버침해에 따른 피해를 산정하기 위해서는 어느 정도 범위를 선정해야 한다.

- 피해로 인한 서비스 중단 손해
- 서비스 중단으로 인한 사용자의 불편/피해 손해
- 복구에 따른 복구비용
- 복구 기간 동안 대체 비용
- 복구 후 포렌직 수사 및 정밀 위험분석 비용
- 정보보호시스템 도입 비용
- 관리적 비용 - 지침, 절차 개발, 교육, 훈련
- 물리적 비용 - 접근통제장치, CCTV 등

6. 결론

국가기관 정보시스템 정보화전략계획(ISP) 프로젝트 결과를 분석해보면 국내 중앙행정기관은 332종의 전산시스템과 1,691대의 서버를 운영하고 있으나 전산환경이 열악하고, 장애관리·재해복구 등의 대응체계가 미흡할 뿐만 아니라 정보화 투자 효율성도 낮은 것으로 조사됐다[8]. 전체 기관의 55%가 30평 미만의 소규모 전산실을 보유하고 있으며, 시스템의 18.1%가 과부하, 19.2%가 저활용 상태인 등 구축해 놓은 시스템의 활용성도 낮은 것으로 나타났다. 특히 시스템의 절반에 가까운 49%는 매월 1회 이상의 장애가 발생하고, 43%는 월평균 30분간 장애를 일으키는 등 만성적인 문제를 갖고 있었다. 따라서, 위험분석을 통해 예산 범위 내에서 정보보호대책을 수립하고 보험 산정을 하여 안전하고 신뢰성 있는 중요 정보시스템 운영이 가능하도록 해야 한다.

본 논문에서는 중요 정보시스템의 위험분석을 통한 피해 산정으로 수락하기 어려운 보호대책에 대해서는 보험을 통한 방안을 제시하였다. 이러한 개념은 유비쿼터스 서비스 환경을 구축하는 데 안심하고 정보시스탬 개발 및 운영할 수 있도록 해주며 품질보장 및 다양한 응용 서비스를 개발하는 데 여건 조성에 많은 도움을 줄 것이다.

참고문헌

[1] 국가사이버안전센터, http://www.ncsc.go.kr.

[2] ISO/IEC TR 13335, Information technology - Guidelines for the management if IT Security: GMITS, 1998.

[3] ISO/IEC, International Standard ISO/IEC 17799:200 - Code of Practice for Information Security Management, 2000.12.1

[4] Young-Hwan Bang, Yoon-Jung Jung, InJung Kim, Namhoon Lee, Gang-Soo Lee: The Design and Development for Risk Analysis Automatic Tool. ICCSA (1) 2004: 491-499

[5] InJung Kim, Yoon-Jung Jung, JoongGil Park, Dongho Won: A Study on Security Risk Modeling over Information and Communication Infrastructure. Security and Management 2004: 249-253

[6] Yoon-Jung Jung, InJung Kim: The Development for the Risk Assessment Methodology of Spiral Model. Security and Management 2003: 334-336

[7] Hoh Peter In, Young-Gab Kim, Taek Lee, Chang-Joo Moon, Yoonjung Jung, Injung Kim: A Security Risk Analysis Model for Information Systems. AsiaSim 2004: 505-513

[8] 행정자치부 전자정부지원센터, http://www.gcc.go.kr.