방송통신융합시스템의 보안위험분석 및 경제성분석*

김인중** · 류정아***

요 약

오늘날의 방송 및 통신시스템에서 사용되는 응용 프로그램들은 위성시스템 등 다양한 네트워크상에서 상호 연동을 하면서 복잡하게 정보를 융합해나가고 있다. 특히, 방송 및 통신시스템은 기술적으로나 규모면에서 계속 진화함에 따라, 이전에 파악하지 못한 새로운 위협 및 취약점들이 증가하고 있다.

본 논문에서는 방송통신 융합시스템에서 사용 가능한 위험분석 및 경제성 분석 방법론을 제안한다. 먼저, 위험분석에서는 기밀성(저작권), 무결성, 가용성을 기반으로 자산을 우선순위화 하는 방법과 위협 및 취약성 변화에 따른 위험도를 계산할 수 있는 모델링을 제안한다. 두 번째로는 시간에 따라 보안대책 비용에 따른 경제성을 분석할 수 있는 방법을 제시한다.

The Security Risk Analysis and Economical Estimation for Convergence of Broadcasting and Communication

InJung Kim** · JeongA Ryou***

ABSTRACT

In today's broadcasting and communication systems, many applications are converged information in a complicated manner by interworking with various networks such as satellite networks. Specifically, as broadcasting and communication systems have become more advanced in terms of technology and capacity, the increase in information assets has created new types of threats and vulnerabilities that we're not previously apparent.

This paper has proposed the following methodologies for analyzing the risks and estimating the economical that could arise in broadcasting and communication convergence systems. First, the assets are prioritized by grading them according to confidentiality(copyrights), integrity, and availability. Based on such an analysis, this paper presents a model that can be used for verifying the risk variables caused by changing threats and vulnerabilities. Second, this paper presents a method for quantitatively estimating the economical caused by countermeasure costs for each time period.

Key words : Risk Analysis, Vulnerability Analysis, Intrusion, Countermeasure

---

* 본 논문은 2008학년도 배재대학교 교내학술연구비 지원에 의하여 수행된 것임.

** 전자통신연구원 부설연구소

*** 교신저자, 배재대학교 전산수학컨텐츠학과

1. 서 론

최근 우리나라에서 방송과 통신의 융합에 대한 논의가 활발하게 이루어지고 있다. 실제로 방송과 통신이 기술적으로 융합화되어 가고 있고, 각종 방송통신 융합의 정책 및 제도[1]들이 제정되어 운영되고 있다. 융합 환경의 핵심적인 특징은 네트워크가 현재보다 더 광범위한 서비스 제공을 위한 수단으로 이용될 수 있다는 것이지만 융합에 따른 불확실성, 즉 융합에 따른 보안 위험을 분석하고 경제성을 분석하지 않고서는 서비스의 안전성을 보장할 수 없다.

현재 방송통신의 융합과 관련하여 인프라 구축에 많은 투자가 이루어지고 있지만 보안 문제도 같이 고려되어야 한다. 방송통신의 융합과 관련하여 가장 큰 고려사항은 융합으로 발생되는 해킹 피해 및 정보의 역기능이며 이를 해결하지 않으면 국민생활에 심각한 피해를 발생시키기 때문이다. 디지털 기술의 발전에 맞게 정보 보안 문제에 더욱 관심을 가져야 한다. 현재 방송분야[2]는 저작권 보호와 컨텐츠 보호 분야에 대해 역점을 두는 반면, 통신 분야[3]는 해킹, 바이러스 등 악성코드의 침해사고 예방 및 복구 대책에 더 큰 관심을 갖고 있다. 지금까지 방송통신의 융합과 관련된 보안 연구는 제대로 이루어지고 있지 않으며 융합시스템을 구축하는 데 역점을 두어 적시에 보안 대책을 수립하지 못하고 있는 실정이다. 이는 방송과 통신의 보안 관점 차이가 발생하기 때문이다. <표 1>과 같이 통신시스템은 기밀성(C), 무결성(I), 가용성(A)를 고려하여 보안 설계를 수행하지만, 방송시스템은 저작권(R), 무결성(I), 가용성(A)를 이용하여 안전성을 기반으로 하는 설계를 수행하고 있다[4]. 따라서, 단순히 네트워크 연결만으로는 서로 다른 보안 관점차이로 인하여 보안 공백 및 침해사고가 발생할 수 있으므로 방송과 통신시스템의 융합에 따른 위험을 제거해 나갈 수 있는 보안위험분석 프로세스[5]와 이에 따른 경제성 분석 연구[6]가 시급히 요구된다.

〈표 1〉 방송 및 통신시스템의 차이

	통신시스템	방송시스템
보안 요소	기밀성>무결성>가용성	가용성>무결성>저작권(인증)
정보(컨텐츠) 보호 수준	등급별 차등 암호 자산 접근통제 다단계 인증	저작권 수준 스크램블 과금 수준의 인증
신뢰성 요구	백업, 이중화 대책 등 응답 시간 요구	QoS 실시간 요구
운영체제와 프로토콜	Windows, UNIX 등 TCP/IP, Ethernet 등	업체 운영체제 방송 프로토콜
자산	정보, 정보통신장치	컨텐츠, 방송장비
보호대상	서버, 라우터 등	주파수 등
전송 대상	1 : 1, 1 : N	불특정 다수
단말 장치	PC, PDA 등	TV, 라디오 등

한편, 방송통신 융합시스템에서 정보(컨텐츠)의 유통 및 연동은 기존에 존재하지 않았던 새로운 형태의 정보 보안 사고를 낳게 되었다. 정보 자산 가치의 중요성을 인식하는 만큼 사고에 대한 위험의 인지는 부족한 것이 현실이다. 사실, 대부분의 기관들이 관리하고 있는 융합시스템이 사고발생 이후의 피해 파악에 앞서 사전에 어떠한 위협 요인들이 존재하였으며 어느 정도 위험에 노출되었는지 조차 파악하지 못하고 있는 경우가 많다. 따라서 보안사고의 예방을 위하여 방송통신 융합시스템을 운영·관리하는 기관은 해당 자산들이 융합에 의해 어느 정도 위험에 노출되어 있는지를 정확히 파악하고 인지하는 과정이 절대적으로 필요하다[7].

방송통신 융합시스템에 대한 정확한 보안위험분석은 적절한 보안 대응책 선정을 가능하게 하여 결과적으로 위험 발생 가능성을 크게 감소시켜 차후에 실제적으로 발생될 수 있는 보안 사고의 피해 규모를 크게 감소시키게 된다. 보안위험분석 과정

은 이와 같이 사전에 사고를 예방하기 위한 의미가 크다고 할 수 있다.

이에 반해 경제성 분석은 어느 수준으로 보안대책을 수립할 것인가를 판단하기 위한 과정이다. 모든 위험에 대하여 해결하고 대응할 수 있는 것이 바람직하겠지만 이는 천문학적인 비용이 들어도 해결하지 못하는 경우가 발생한다. 비용대비 효과를 분석하여 위험을 수용할 것인지, 회피할 것인지, 법/규정에 의하여 처리할 것인지를 판단하기 위해서는 경제성 측면에서 바라봐야 한다. 융합시스템에 대한 안정적인 운영 관리를 위해서는 시설에 대한 보호계획에 앞서 위험 대처를 위한 경제성 분석 기준이 마련되어야 한다. 그러나 사이버 침해 요인에 대한 이해 부족과 침해 규모에 대한 정확한 분석 기준이 없어 서로 다른 방식에 의하여 분석 결과를 발표하고 있다. 이는 상이한 결과로 인하여 궁극적으로는 보호 예산 및 피해 규모가 과대 또는 과소평가되어 정확한 상황 판단을 어렵게 만들기도 한다.

본 논문에서는 방송통신융합시스템에 적합한 객관적이고 현실적인 보안위험분석 및 경제성분석 방안을 제시하기 위하여 다음과 같이 구성한다.

먼저, 보안위험분석 및 경제성분석을 위하여 국내외 보안위험분석 프로세스 및 경제성 분석 모델을 수립하고 분석하여 방송통신 융합시스템에 적합한 측정 요소를 발굴한다.

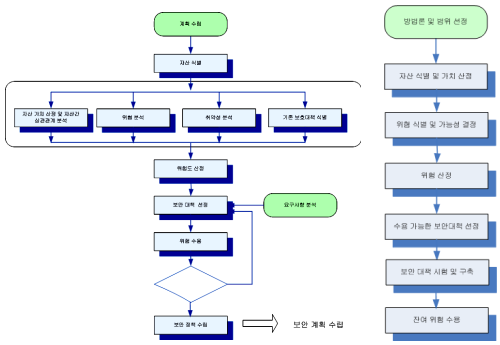
둘째, 방송통신 융합시스템에 적합한 자산, 위협, 취약성분석을 통해 위험도를 계산하고 이를 통하여 보호대책을 수립하는 보안위험분석 프로세스를 제안한다. 이는 시스템을 모델링하는 기법을 통해 시간변화에 따라 위험도 변화를 즉시 분석이 가능하게 된다.

셋째, 방송통신 융합시스템과 같이 다양한 정보자산들이 밀집되어 있고 연동되는 시스템에 대하여 효과적인 경제성 분석 설계에 대한 방안을 제시한다.

2. 관련 연구

2.1 보안위험분석 프로세스

일반적인 정보시스템에서 사용되는 위험분석 프로세스는 (그림 1)과 같다.



(그림 1) 일반적인 위험분석 프로세스 (GMITS[8]과 NIST 방법론[9])

계획수립 단계는 시스템의 구축 및 운영과 관련한 범위, 목적 등을 상세히 기술하고, 어떤 방식 또는 어떻게 접근하여 위험분석을 수행할 것인지 심도 있게 논의한다. 또한 조직의 물리적인 구조나, 보안과 관련된 정책적인 문서 등 정보를 수집하며, 컴퓨터 운영자 또는 관리 책임자나 부서장 및 관련 사용자들과의 인터뷰 또는 서면 질의를 통해 다양한 데이터들을 수집한다. 수집된 자료를 토대로 자산의 파악 및 가치 평가, 위협 파악 및 위협에 따른 취약성 분석, 그리고 그에 따른 보안대책을 수립하게 된다. 자산분석 단계는 조직에서 보호되어야 할 핵심적인 자산을 파악하고 식별하는 단계이다. 모든 자산을 우선 식별한 후 위험평가의 범위 설정에 따라 좀 더 세부적으로 어느 수준까지 자산을 보호할 것인지를 식별한다. 자산은 기밀성, 무결성, 가용성을 고려하여 중요도를 매긴다. 이때 자산의 구입 또는 유지비용뿐만 아니라 가치로 나타내기 어려운 기업의 이미지나 대외신인도와 같은 가치를

매길 수 없는 것들도 고려한다. 위협분석 단계는 전 단계에서 이루어진 식별된 자산을 토대로 조직에 발생될 수 있는 위협을 파악한다. 위협의 파악과 함께 위협의 발생 빈도 등을 분석한다. 이런 과정은 다음 단계인 취약성 분석과 함께 이루어진다. 취약성 분석 단계에서는 조직에서 일어나는 위협에 의한 손실발생 가능성 또는 피해 규모를 늘릴 수 있는 취약성을 파악한다. 위험도 평가 단계는 앞서 평가가 이루어진 위협과 취약성을 토대로 하여 이러한 위협과 취약성이 조직에 미치는 불확실한 사건들의 발생 여부와 이에 따라 발생될 파장을 측정하는 단계이다. 위험도는 위협이나 취약성들의 유형, 발생빈도 및 예상 손실액 등을 고려하여 측정한다.

여러 가지 위협에 따라 위험을 분석하고 난 뒤에는 취약성을 제거하여 위험을 최소화 할 수 있는 보안대책을 수립한다. 보안대책 분석 단계에서 이루어지는 현재 상황에서 어떠한 보안대책이 가장 적절한 지를 식별한다. 그리하여 조직에 악영향을 미칠 수 있는 침해 사고 발생을 방지하고 발생한 사건에 대해서는 영향이 미치지 못하도록 적절히 제어할 수 있는 것이다.

3.2 경제성분석 모델

방송통신융합시스템에 보안대책을 수립하기 위해서는 경영자가 보안의 필요성을 이해 할 수 있도록 해야 한다. 이를 위하여 경제성 분석이 요구되며 보안 구축비용 대 효과를 반드시 검토해야 한다. 아무리 좋은 보안대책이라고 해도 비 경제적이거나 고비용인 경우에는 수립이 불가능하기 때문이다. 대부분의 보안과 관련한 경제성 분석은 피해 분석을 통해 이루어진다. 시스템 가동 중단에 따른 1차 피해와 대외 서비스 제공 불가 및 대외 이미지 손실 등에 따른 2차 피해로 나누어 계산하게 되는 데 <표 2>와 같이 구분한다[10].

〈표 2〉 피해규모 산출

<table>
<tr><td colspan="2">간접비용</td><td colspan="2">예방을 위해
투자한 비용</td><td>이미지 손상
추가 하락</td></tr>
<tr><td rowspan="2">직접
비용</td><td>기대
손실</td><td>매출이익
손실</td><td>생산효율
저하로 인한
손실</td><td rowspan="2">잠재적인
법적
책임 비용</td></tr>
<tr><td>추가
비용</td><td>복구 비용</td><td>복구 불가능한
데이터의 가치</td></tr>
<tr><td colspan="2"></td><td colspan="2">명시적 비용</td><td>잠재적 비용</td></tr>
</table>

〈표 3〉 비용 산출 계산적 측면의 비교

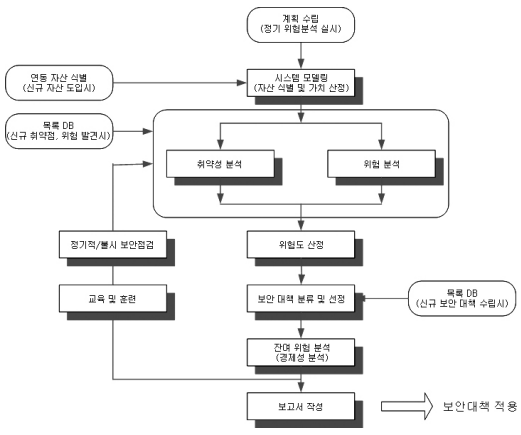
비교 항목	미국 ICAMP	일본 피해액 산출 방법
피해 복구비용	내부근로자의 시간당 인건비(노동력+시설물)	인건비 중심
손실이익	추가 인건비(근로자+사용자)의 28%	명확한 경우만 계산. 대체수단 등의 모호한 손실 이익은 업무마비에 따른 피해액으로 간주
업무마비에 따른 피해액	사용자 측면에서 계산한 것으로 시간당 인건비 이용	IT 관련 부분만 세부적으로 계산
이미지 하락	(피해복구비용+손실이익+사용자 피해액)의 52%	없음
적용 환경	대학 캠퍼스 등	일반기업
특징	IT 침해사고를 정량적 수치화하는 기본 개념 제시	피해 관련 세부적인 계산법 제시
문제점	손실이익, 간접피해액 산출시 사용되는 수치(28%, 52%)의 근거 미비	피해액에 큰 영향을 미치는 파라미터의 수치를 주관적으로 선정
	사례 적용은 가능하지만 그 결과에 대한 검증이 없으며 실제 피해액과의 편차가 클 수 있음	실제 사례에 적용하려면 자세한 데이터 필요
공통점	자산 중심 보다는 피해 복구에 투입된 사람과 그 사고의 영향을 받은 사람을 중심으로 기준 금액과 시간을 이용해 비용 계산	

이와 관련하여 미국에서는 ICAMP(Incident Cost Analysis and Modeling Project) 연구[11]를 추진하였고, 일본에서는 2001년부터 보안 대책 연구개발 등 사업의 일환으로서 일본 네트워크 보안 협회(JNSA)가 사고에 의한 피해액 및 대책비용의 산출 모델[12]을 제시하였다. 두 피해액 산출 모델에 대한 주요 내용은 다음 <표 3>과 같다.

4. 제안하는 위험분석 및 경제성 분석 방법론

4.1 보안위험분석 프로세스

먼저 본 논문에는 방송통신융합시스템에 적합한 보안 위험분석 프로세스를 제안한다. 기본적인 보안위험프로세스는 (그림 2)와 같이 나타낸다. 기존 프로세스와의 차이점은 시스템 모델링을 통해 융합자산의 자산 가치를 산정하며, 잔여위험분석에서 경제성 분석 절차를 포함시켰다. 또한, 신규 자산 도입, 신규 취약점 및 위협 발견 시, 신규 보안대책 수립 시에도 위험분석을 실시할 수 있도록 하고 있다. 이렇게 하는 것은 지금까지 수행한 위험분석 관련 정보들이 모두 종합적이고 체계적으로 관리되어야 하기 때문이다.



(그림 2) 제안하는 보안 위험분석 프로세스

먼저 자산분석에서는 단위 자산별로 자산을 식별하고 이에 대한 자산의 가치 및 중요도를 산정하는 방식에서 벗어나 업무 유형별로 자산을 그룹화 한다. 그룹화 하기 위해서는 시스템을 다음 절에 나타난 것과 같이 시스템을 모델링하여 중요도를 산정한다.

기존에는 위협분석을 위하여 위협원, 위협빈도 등으로 구분하거나 위협 트리를 만드는 작업을 하였으나 이러한 방식은 평가자의 주관적인 사항에 많은 영향을 받게 된다. 따라서, NIST 800-53의 보안통제항목[13]을 바탕으로 위협 목록을 작성한다. 취약성 분석은 CERT 권고문에 나타난 CVE (Common Vulnerabilities and Exposure)[14]를 바탕으로 등급을 매긴다. 마지막으로 위험도는 기밀성(저작권), 무결성, 가용성을 기반으로 각각 5등급으로 정한 후 매트릭스 테이블을 통해 융합시스템의 위험도를 계산한다.

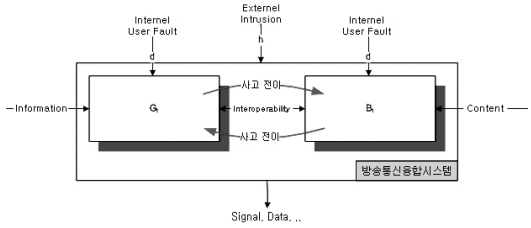
본 논문에서 제시한 보안위험분석 프로세스와 기존의 프로세스를 비교하면 <표 4>와 같다.

〈표 4〉 방송통신 융합시스템을 위한 보안위험분석 프로세스 비교

	제안한 보안위험분석	기존 위험분석
자산 분석	융합 자산에 대한 연관성 분석을 통한 중요도 선정	단위 자산을 통한 자산의 중요도 산정
위협 분석	NIST 800-53 보안통제항목	일반 위협 목록
취약성 분석	CERT의 CVE 취약점 목록	위협과 같은 분류
경제성 분석	가능	불가능
이전 위험분석 결과 비교	용이함	복잡함
환경 변화에 따른 대응	즉시 확인 가능	인력과 시간이 소요

4.1.1 융합시스템 모델링

일반적으로 모델링을 위해서는 대상 시스템과 자산을 정의하고 시스템의 목적, 구성 등 시스템의 기능적 한계에 대한 명확한 정의가 수행되어야 하나 본 논문에서는 시스템의 구성요소 간의 상호 의존성과 각 운용 내용에 대하여 시스템의 위협 요소가 동작하는지의 여부를 나타내기 위한 것으로 정보시스템을 하나의 블록으로 묶어서 표현한다. 따라서, 방송통신융합시스템 실제 시스템에 대한 모델은 (그림 3)과 같이 표현한다. 방송통신시스템은 어떤 주어진 목적을 달성하기 위하여 상호작용을 하는 여러 개의 요소가 모여 하나의 복합체를 이루고 있는 실체이며, 주위환경으로부터 시스템에 요구되는 사항을 입력이라고 하며, 그 입력에 의하여 시스템에 나타나는 결과를 출력이라고 한다.



(그림 3) 방송통신융합시스템 모델

통신시스템이 $G = g_1, g_2, \cdots, g_i, \cdots, g_n$라고 할 때, g_i는 단위 자산이다. 예를들어, PC, 서버, 라우터 등을 의미한다. 통신시스템 G의 단위 자산들은 시간 t에 따라 자산의 가치가 변화될 수 있으므로 시간변수에 따른 자산의 가치를 함수화하여 $\overline{g_t^{(i)}}(h, d)$로 표현할 수 있다. h는 해킹, 악성코드 등에 의한 외부 침해사고를 의미하며, d는 작업자의 과실, 장비의 노후화 등에 따른 사고이다. 통신시스템의 총 자산 가치는 g_i의 자산 가치의 합을 다음과 같이 표현된다.

$$\overline{G_t}(h, d) = \sum_{i=1}^{n} \overline{g_t^{(i)}}(h, d), \quad i = 1, \cdots, n$$

방송시스템도 통신시스템과 마찬가지로 표현할 수 있다. 방송시스템이 $B = b_1, b_2, \cdots, b_i, \cdots, b_m$으로 표현하며, 방송시스템의 총 자산가치도 다음과 같이 표현한다.

$$\overline{B_t}(h, d) = \sum_{i=1}^{m} \overline{b_t^{(i)}}(h, d), \quad i = 1, \cdots, m$$

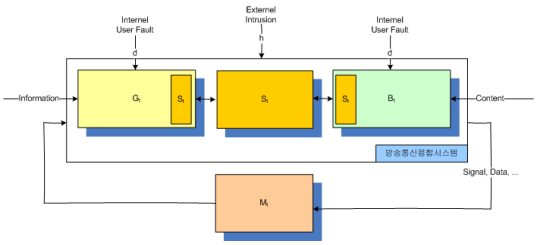
방송통신시스템의 융합으로 인하여 총 자산 가치는 시너지 효과로 인하여 상승하는 부분이 있는데 반하여, 중복 요인 또는 호환성으로 인하여 폐기되는 부분도 발생한다. 여기서 고려해야 할 사항은 융합으로 인하여 자산의 가치의 변화는 침해사고 및 해킹문제에 밀접하게 관련된다는 것이다. 먼저, 방송통신 융합으로 인하여 상승되는 자산의 가치 부분을 $\oplus$로 표시하고, 보호 대책으로 발생되는 자산의 가치를 $\ominus$로 표현하면 다음과 같이 나타난다.

$$\overline{C_t} = \overline{G_t}(h, d) + \overline{B_t}(h, d) + [\overline{G_t}(h, d) \oplus \overline{B_t}(h, d)] - [\overline{G_t}(h, d) \ominus \overline{B_t}(h, d)]$$

만일, $\overline{G_t}(h, d) \oplus \overline{B_t}(h, d) \leq \overline{G_t}(h, d) \ominus \overline{B_t}(h, d)$으로 나타나게 된다면 융합에 따른 효과가 발생되지 않는다는 것을 의미한다.

4.1.2 융합보호시스템 및 모니터링시스템

위에서 설명한 방송통신융합시스템에 대하여 보호대책을 수행하기 위하여 (그림 4)와 같이 표현한다. 먼저, 융합보호시스템은 S_t로 표현하고, 모니터링시스템(보안관제)은 M_t로 나타낸다. 단, 여기서 나타내는 융합보호시스템은 융합과 관련되어 위험이 발생할 수 있는 자산만을 보호하기로 한다.

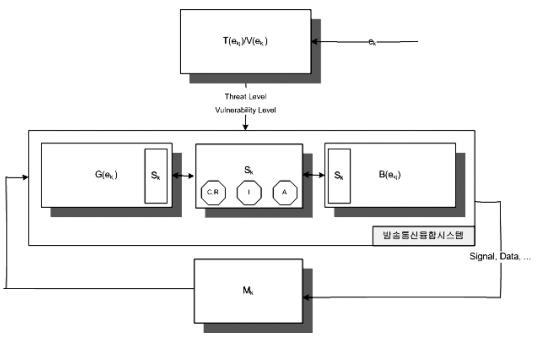


(그림 4) 융합보호시스템을 고려한 방송통신융합 시스템 모델

S_t는 정보시스템에 대한 안전한 운용 및 관리를 위하여 보안서비스 요소인 기밀성(C), 무결성(I), 가용성(A)등으로 구분할 수 있다. 단, 방송시스템 관점에서 바라보는 경우에는 기밀성(C) 대신에 저작권(R)으로 표현한다. M_t은 융합시스템에 대한 각종 정보 흐름 및 접속결과 등을 분석하여 불법 침입 또는 잘못된 접근이 발생하였는 지를 확인하여 침해 사고에 대한 대응 및 복구를 제공한다. S_t와 M_t는 시간에 따라 자산의 가치가 변할 뿐, 해커로 인한 공격 h나 내부자에 의한 사고 d에 의한 영향을 받지 않는다고 가정한다. 따라서, S_t와 M_t의 자산의 가치는 각각 $\overline{S_t}$, $\overline{M_t}$로 표현하게 된다.

4.1.3 보안위험분석 위험도 산정

해킹의 위협 및 바이러스의 변종으로 인하여 방송통신 융합시스템의 위협 및 취약성들은 계속해



(그림 5) 위험도 산정을 위한 블록 다이어그램

서 발생하게 되면 이에 관련한 위험은 수시로 변화하게 된다. 따라서, 단 한 번의 위험분석 프로세스가 아닌 변화되는 자산, 위협, 취약성에 따라 위험이 수시로 변화됨에 따라 자동으로 대응 결과에 따라 (그림 5)와 같은 위험도를 조정할 수 있는 자동화 프로세스를 구축한다.

위험을 계산하기 위하여 이전에 서술한 자산의 가치를 다음과 같이 위험도 수식으로 나타낸다. 먼저 통신시스템은 보안서비스인 기밀성, 무결성, 가용성을 기반으로 표현하고, 방송시스템은 저작권, 무결성, 가용성으로 표현한다. 침해가 발생하는 단계를 k로 표시한다. k번째 발생하는 침해는 e_k라 하면, g_i의 k_j에서 기밀성으로서의 위험도는 $\widehat{g_C^{(i)}}(e_{k_j})$, 무결성으로서의 위험도는 $\widehat{g_I^{(i)}}(e_{k_j})$, 가용성으로서의 위험도는 $\widehat{g_A^{(i)}}(e_{k_j})$로 표현한다. 이때 각각의 결과 값은 3등급(상, 중, 하)으로 구분한다.

$$\widehat{g_C^{(i)}}(e_{k_j}),\ \widehat{g_I^{(i)}}(e_{k_j}),\ \widehat{g_A^{(i)}}(e_{k_j})\ \in\ 1, 2, 3$$

이때, g_i의 k_j에서 위험도 $\widehat{g^{(i)}}(e_{k_j})$는 $\widehat{g_C^{(i)}}(e_{k_j})$, $\widehat{g_I^{(i)}}(e_{k_j})$, $\widehat{g_A^{(i)}}(e_{k_j})$의 3차원 매트릭스 테이블 값의 합으로 계산할 수 있다. 따라서, 통신시스템 G의 위험도 $\widehat{G}(e_{k_j})$는 $\widehat{g^{(i)}}(e_{k_j})$들의 평균이다.

$$\widehat{G}(e_{k_j})\ =[\frac{\sum_{n}^{i=1}\widehat{g^{(i)}}(e_{k_j})}{n}]\ \in\ 1, 2, 3, 4, 5$$

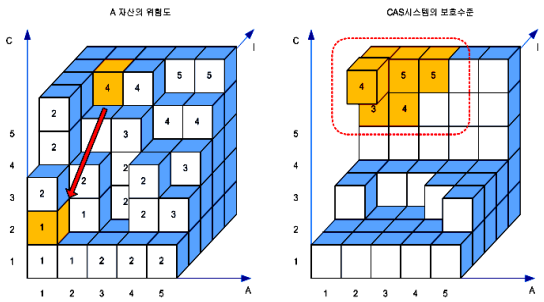
여기서, 등급화의 정수화를 위하여 [] 가우스 함수 처리를 한다. 방송시스템 B의 위험도도 마찬가지로 계산할 수 있다.

$$\widehat{B}(e_{k_j})\ =[\frac{\sum_{n}^{i=1}\widehat{b^{(i)}}(e_{k_j})}{n}]\ \in\ 1, 2, 3, 4, 5$$

최종적으로 방송융합시스템의 위험도는 $\widehat{C}(e_{k_j})$

$= \hat{\hat{G}}(e_{k_j}) \oplus \hat{\hat{B}}(e_{k_j})$으로 표현하여, 여기서 ⊕는 n차원 매트릭스 테이블이다.

잔여 위험분석은 융합보호시스템 및 모니터링 시스템을 통해 수행하게 되는데 보호 대책을 통해 위험도를 감소시키는 영향을 분석한다. 예를 들어, 방송통신융합시스템에서 사용자에게 과금과 관련된 업무와 관련된 자산 A를 보호하고 싶은 경우, 자산 A에 대하여 기밀성과 무결성을 요구하지만 가용성에는 낮은 등급을 갖으므로 위험도가 4로 평가된다. 위험도를 1로 줄이기 위하여 과금과 관련한 개인정보보호를 위한 보호시스템을 선정시 CAS(Conditional Access System)을 선정할 수 있다. 이렇게 되면 기밀성과 무결성에 대한 위험이 (그림 6)과 같이 줄게 되는 것을 쉽게 분석할 수 있게 되는 것이다.

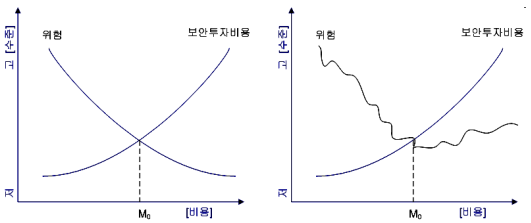


(그림 6) 자산별 위험도 및 보호시스템 간 상관관계도

이상과 같이 모델링을 통한 위험 분석을 통해 위험도 산정 및 보안대책 제시가 단시일 내에 이루어지면서 상관관계를 파악할 수 있게 된다.

4.2 경제성 분석

이전의 통신시스템이나 방송시스템의 경우 보안대책을 수립하기 위하여 예산을 투입하게 되면 (그림 7)의 왼쪽 그림처럼 위험은 감소하게 되므로 최적의 투자비용(M_0)을 산출할 수 있었다. 하지만 방송통신융합시스템의 경우에는 보안에 많은 예산을 투자해도 새로운 취약점이 발견되거나 침해 위협이 융합으로 인하여 발생하게 되면 (그림 7)의 오른쪽 그림처럼 위험은 증가하게 된다. 따라서, 이제는 투자비용과 위협과의 상관관계만으로는 비용분석이 불가능하다.

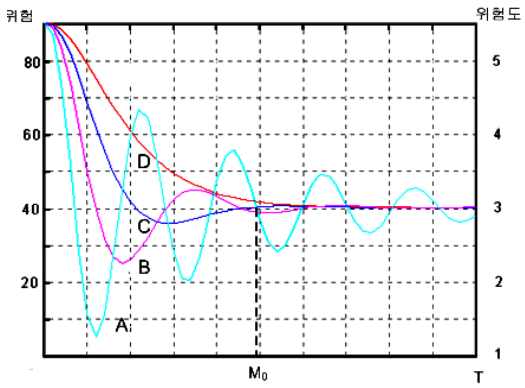


(그림 7) 위험대비 비용투자비용 상관관계

이에 따라 본 논문은 위험 대비 보안 투자비용과 관련하여 방송통신융합시스템에 적합한 새로운 경제성 분석 모델을 제시하고자 한다. 이 모델은 비용측면에서 보는 것이 아닌 시간 측면에서 분석한다. 일정한 보안비용이 계속해서 투자된다면 총 위험은 꾸준히 감소하게 되지만 일부 신규 취약점 발견 및 위협으로 인하여 위험이 순간적으로 증가할 수 있게 된다. 위험의 함수는 (그림 8)과 같이 여러 형태로 나타날 수 있다. 예를 들어, 바이러스 및 웜과 같은 악성코드 함수(A)의 경우처럼 빈번하게 발생하면서 한번 감염되면 위험도가 갑자기 증가하게 되지만, 백신 처리로 인하여 안전성을 회복할 수 있다. 사용자의 부주의한 사고(D)의 경우는 지속적인 교육 및 훈련으로 인하여 완만하게 위험을 줄여나갈 수 있다. 어느 정도 단위 자산의 위험도 3을 기준으로 보호대책을 조정해 나간다. 전체 위험도 3을 기준으로 위험도가 변경되지 않는 예산(M_0) 내에서 투자 예산을 조정해 나가면 된다.

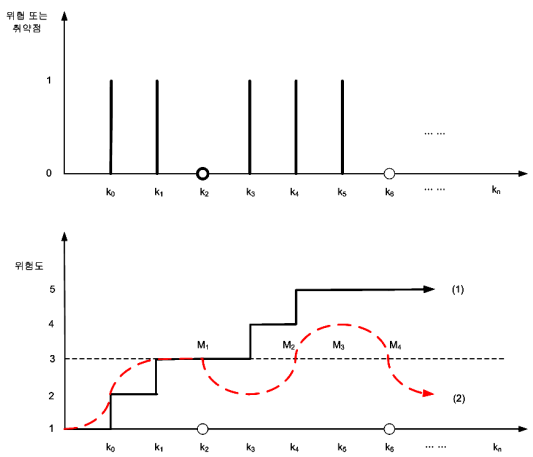
보안 예산은 일정한 액수로 계속 투입되지만 위협과 취약점은 수시로 발생한다. 먼저 위협과 취약성은 일정한 주기로 발생하며, 새로 발견된 위협/취약성은 이전에 발생한 위협/취약성과 다르다고 가정한다. 또한, 발견된 위협/취약성에 대하여 보

호 대책을 수립하면 더이상 동 위협/취약성으로 인하여 위험도가 증가하지 않는다고 가정한다.



(그림 8) 시간 측면에서 바라본 일정 보안 예산 투입시 위험 흐름도

융합시스템에 대하여 위협/취약성들이 계속 주기적으로 발생하게 되면 이와 관련한 시스템의 전체 위험도는 증가하게 된다. 이러한 위험도는 대응책에 따라 감소하거나 더 이상 위험도가 증가하지 않는다. 이러한 상태를 (그림 9)와 같이 예를 들어 표현하며, 다음과 같이 수식으로 표현할 수 있다.



(그림 8) 위협/취약성에 따른 위험도 변화

$$K_n : T(K_n) = t_n$$

$$\sum_{i=0}^{n} T(k_i) \oplus \sum_{j=1}^{n_j} M_j = R+1 \quad \downarrow \; M_{n_j+1}$$

$$\sum_{i=0}^{n} T(k_i) \oplus \sum_{j=1}^{n_j+1} M_j = R \qquad \sum_{i=0}^{n} T(k_i) \oplus \sum_{j=1}^{n_j} M_j = R$$

$$K_{n+1} : T(K_{n+1}) = t_{n+1}$$

여기서, n_j 는 k_n까지 보안 예산 투입 횟수이고, $\oplus$는 보안 예산 투입 후 위험도의 합이다.

(그림 9)에서 위협/취약성이 시간에 따라 계속 발생하게 되면 위험도는 선 (1)과 같이 증가하게 된다. 최적의 보호 예산(M_0)을 통하여 보안 대책을 수립하고 있는 상태에서 위협이 3등급 이상이 되면 대응책이 고려되며, 대응책을 통하여 위험 수준은 선 (2)와 같이 감소하게 된다. 대응책은 위협/취약성이 나타난 후에 일정기간 후에 발생하므로 위험이 계속 증가하지 않도록 사전 예방 대책이 지속적으로 이루어져야 한다. 감소된 효과는 선 (1)과 선 (2)의 차이에 나타난 영역에 해당한다. 보안 예산과 관련된 경제성 분석은 선 (1)과 선 (2) 사이의 크기이며, 자산 분석시 계산된 자산 가치를 고려하여 계산한다.

5. 결 론

본 논문은 방송통신 융합시스템을 운영하는 조직의 체계적인 보안활동에 도움을 주기 위하여 예방 및 대응측면에서 2가지 프로세스를 제시하였다. 첫 번째 예방활동 측면에 대한 프로세스로는 방송통신 융합시스템을 운영하는 조직의 보안활동을

하기 위한 필수요소인 보안위험분석 프로세스를 제안하고, 두 번째 대응활동 측면에 대한 프로세스로는 위협 및 취약성 발견에 따른 위험도 증가와 관련하여 보안 예산 투입에 따른 위험도 감소 수준을 통한 경제성 분석 모델을 제시하였다.

좀 더 상세하게 제안한 프로세스를 살펴보면, 첫 번째 제안한 예방차원의 보안위험분석은 실제 방송통신 융합시스템에 적용이 가능하도록 단계별 알고리즘을 포함한 프로세스를 기술하였다. 정보자산의 중요도를 분석하기 위하여 연동 자산에 대하여 기밀성, 무결성, 가용성을 통해 중요도로 등급화하여 어느 자산이 더 중요한지 우선 순위화 할 수 있도록 하고, 위협 분석에서는 위협원 식별이 주관적일 수 있으므로 NIST의 800-53 보안 통제 항목을 기반으로 위협을 분류하였다. 이를 기반으로 위협/취약성의 변화에 따라 위험도의 변화를 즉시 파악할 수 있게 되었다.

두 번째 제안한 대응차원의 경제성 분석 모델은 보안 예산 비용에 따른 위험 수준에 대하여 시간대로 분석하는 방안을 제시하였다.

이상으로, 본 논문에서는 방송통신 융합시스템에서 사이버 침해로부터 발생할 수 있는 피해를 최소화하고 신속한 대응활동을 위한 보안위험분석과 경제성 분석 기법을 제시함으로써 체계적이고 종합적으로 정보보호 영향 및 수준을 분석할 수 있는 기틀을 마련하게 되었다.

참 고 문 헌

[1] 윤석민 외, “정책연구 제2005-9호, 방송통신 융합관련 법제도 정비방안 연구”, 방송위원회 정책연구 제2005-9호, 2006.

[2] 전한얼 외, “방송통신 기술동향 연구 : 디지털 콘텐츠”, 방송위원회 제2006-5호, 2007.

[3] 국가정보원, “2008 국가정보보호백서”, 2008.

[4] 류정아, “방송과 통신의 융합에 따른 취약점 분석 프로세스 연구”, 제29회 정보처리학회 춘계학술대회논문집, 2008.

[5] Hoh Peter In, Young-Gab Kim, Taek Lee, Chang-Joo Moon, Yoonjung Jung, Injung Kim, “A Security Risk Analysis Model for Information Systems”, Proceeding of Asia-Sim2004, Springer-Verlag, pp. 505-513, Oct. 2004.

[6] Young-Gab Kim, Taek Lee, Hoh Peter In, Yoon-Jung Chung, InJung Kim, Doo-Kwon Baik, “A Probabilistic Approach to Estimate the Damage Propagation of Cyber Attacks”, Proceeding of ICISC2005, Springer-Verlag, Dec, 2005.

[7] JeongA Ryou, “A Security Design for Information Sharing between Control System and Information System”, Proceedings of Security and Management(SAM)2008. July 2008.

[8] MICTS(Previously GMITS), ISO/IEC 27005 ISMS Risk Management. 2005.

[9] NIST, Federal Information Technology Security Assessment Framework. http://csrc.nist.gov/organizations/guidance/framework-final.pdf, 2000.

[10] Gordon, L. A. and Loeb, M. P, “Managing Cybersecurity Resources : A Cost-Benefit Analysis, 2006.

[11] CIC IT Security Working Group, “Incident Cost Analysis and Modeling Project Report”, A Report to the USENIX Association, 2000.

[12] JNSA, “Information security Incident survey Report Fiscal 2003”, 2003. http://www.jnsa.org/houkoku2003/incident_survey1_e.pdf.

[13] NIST, “Recommended Security Controls for Federal Information Systems”, SP pp. 800-53 Rev. 2. Dec. 2007. http://csrc.nist.gov/publications/PubsSPs.html.

[14] US-CERT and CERT/CC, “US-CERT Vulnerability Notes Database”, http://www.kb.cert.org/vuls/.

김 인 중

2006년 성균관대학교 전기전자컴퓨터공학과 (공학박사)

1992년~2000년 국방과학연구소 선임연구원

2000년~현재 전자통신연구원부설연구소 팀장

류 정 아

2001년 충남대학교 수학과(이학박사)

2006년~2007년 충남대학교 강의전담교수

2008년~현재 배재대학교 전임강사