情 報 保 護 學 會 誌
第19卷 第6號, 2009. 12

융합보안의 개념 정립과 접근방법

김 정 덕*, 김 건 우**, 이 용 덕***

요 약

현재 융합보안에 대한 개념은 물리적, 기술적, 관리적 보안을 상호 연계하여 보안의 효과성을 높이고자 하는 통합적 보안을 관리하는 개념과, 보안이 조선, 자동차 등 기타 산업과 융합되어 새로운 서비스나 제품의 안전성과 부가가치 창출을 위한 복합적 의미의 개념으로 사용되고 있다. 이러한 융합보안에 대한 상이한 개념은 향후 융합보안의 연구 및 적용에 있어 혼란을 초래할 가능성이 있다. 본 논문의 목적은 혼용되고 있는 융합보안의 개념을 재정립하고, 두 가지 차원의 융합보안 적용 시 고려해야 할 접근방법을 제시하는 것이다.

Ⅰ. 서 론

새로운 정보기술이 등장함에 따라 조직의 정보자산에 대한 위협 역시 다양해지고 있으며, 정보유출 등의 사건/사고에 따른 피해규모는 조직의 존폐에 영향을 줄 만큼 증가하고 있다. 한 예로, 최근 영국의 Sumitomo Mitsui Bank에서 해킹에 의한 도난 사건이 발생 하였고, 220만 유로의 손실을 입었다 [1]. 비록 이 은행은 강력한 IT 기술을 이용한 보안체계를 구축했음에도 불구하고, 감시망을 피해 컴퓨터 키보드에서 로그 정보를 추출할 수 있는 장치를 설치하는 등 물리적 보안의 허점을 이용한 보안 사고를 방지하지 못하였다. 이러한 물리적 보안 영역과 관리적/기술적 보안 영역의 분리에 따른 보안사건/사고는 새로운 정보보호 이슈로 부각되고 있으며, 그 해결책으로 “융합보안”이라는 개념이 등장하게 되었다.

융합보안에 대한 연구는 국외는 3년 전부터, 국내는 작년부터 활발하게 수행되고 있으며, 특정산업에 적용되거나, 솔루션으로 개발되기도 하였다. 융합보안과 관련된 국외의 연구는, 점차 다양해지고 복잡해지는 비즈니스 위협으로부터 유형자산과 무형자산을 동시에 보호하고, 점증하는 법, 규제에 효과적, 효율적으로 대응하고 보안 운영비용을 감소시키기 위해 전사적 차원에서 물리적, 기술적, 관리적 보안의 전략, 프로세스, 기능들을 융합하는 것에 초점을 두고 있다. 반면, 국내에서는 융합보안의 개념이 물리적, 기술적 보안을 통합적으로 관리하는 보안영역 내에서의 융합과 보안이 비IT기술 또는 다른 산업에 적용되어 새로운 보안 서비스 및 제품을 창출하는 보안과 기타 산업에서의 융합으로 두 가지 차원에서 혼용되고 있다. 즉, 보안과 기타 산업에서의 융합은 개별 산업 내에 어떠한 보안기술이 적용되는지에 초점을 두는 반면에, 보안영역 내에서의 융합은 조직 내에서 이미 운영 중인 물리적, 기술적 보안을 어떻게 통합하고, 누구에 의해 관리되며, 어떻게 사용할 것인가에 초점을 두고 있다. 이러한 융합보안에 대한 상이한 개념은 향후 융합보안의 연구 및 적용에 혼란을 야기할 것으로 예상된다.

따라서 본 논문에서는 국내외 융합보안에 대한 선행연구를 바탕으로, 두 가지 차원으로 혼용되고 있는 융합보안의 개념을 재정립하고, 융합보안 적용 시 고려할 수 있는 접근방법과 효율적이고 효과적으로 융합보안을 적용하기 위해 필요한 향후 연구 과제를 제시한다.

Ⅱ. 융합보안의 필요성 및 국내외 동향

2.1 융합보안의 필요성

현재 대다수의 조직에 적용된 보안체계를 살펴보면,

* 중앙대학교 정보시스템학과 교수(jdkimsac@cau.ac.kr)
** 중앙대학교 정보시스템학과 석사과정(kunwoo.kim317@gmail.com)
*** 중앙대학교 정보시스템학과 석사과정(rage21c@naver.com)

[그림 1]과 같이 하나의 보안 관리 프로세스 아래 물리적 보안 영역, 관리적 보안영역, 기술적 보안 영역의 세 가지 영역으로 분리되어 운영되고 있다 [2] . 하지만, 이러한 보안체계는 동일한 지배구조 하에 있지만 관리자 및 관리 대상이 상이하여 서로간의 상호 연계성이 어려운 것이 사실이다. 즉, 각각의 보안체계가 잘 수립되었더라도 하나의 영역에 취약점이 발생하였을 경우, 전사적인 차원의 보안사건/사고를 미리 예방하거나 이에 대처하기 힘들다는 의미이다.

[그림 1] 현재의 보안관리 체계

따라서 이러한 보안사건/사고를 예방하고 적절하게 대처하기 위해서는 세 가지 영역을 통합적인 관점에서 관리할 필요가 있으며, 이러한 관점에서의 보안을 융합보안이라 한다. The Alliance for Enterprise Security Risk Management(AESRM)에서는 5가지 측면에서 융합보안의 필요성을 제시하고 있으며, 다음과 같다 [2] :

- 기업의 에코시스템은 빠르게 확장하고 있으며, 이는 새로운 기술 적용 및 사업 수행 방식의 변화로 조직 구조를 보다 복잡하게 만드는 요인으로 작용하고 있다. 즉, 대다수의 기업들은 비용절감을 통한 경쟁력 확보에 초점을 두고 있으며, 이를 위하여 외부의 제3자로부터 일부 IT기술을 아웃소싱하고 있으며, 이러한 제3자는 전 세계적으로 확장되고 있다.
- 정보화 사회가 고도화됨에 따라 기업에서 정보자산이 차지하는 비중은 점차 증가하고 있다. 이러한 정보자산은 대부분이 무형자산이지만, 기업에서 제공하는 물리적인 제품 즉, 유형자산 역시 정보에 의존하는 경향이 커지고 있다. 따라서, 무형자산 및 유형자산을 보호하기 위해서는 물리적 보안과 정보보호 노력이 동시에 고려되어야 한다.
- 스마트카드의 사용으로 사용자의 신원을 확인하는 동시에 위치까지 파악할 수 있는 네트워크 접근 기술이 기존의 물리적 접근 통제 기술을 대체하고 있으며, 이는 물리적 보안 영역과 관리적/기술적 보안영역의 경계가 불분명해짐을 의미하며, 통합적인 차원에서의 관리가 필요함을 뜻한다.
- 비즈니스 트랜잭션이 점차 복잡해지고 새로운 위협들이 등장함에 따라 Sarbanes-Oxley 등의 기업이 준수해야하는 최소한의 보안 수준을 요구하는 법, 규제가 등장하고 있다.
- 기업은 빠르게 변하는 위험에 대처하기 위하여 최소의 비용으로 자원을 최대한 활용하는 체계적이고 실용적인 접근법을 필요로 하게 되었다. 즉, 효율적인 보안 자원의 분배를 위해서는 위험 기반의 접근법이 필요하며, 보안전략과 관련된 투명성을 보장해야 한다는 의미이다.

이처럼, 앞서 제시한 5가지 융합보안의 필요성은 필수적인 동인으로 작용하고 있으며, 근본적으로 조직에서 보안의 역할을 변화시키고, 보안영역 내의 기능적 교차를 통하여 전체적인 측면에서 비즈니스 프로세스 또한 변화시킨다고 할 수 있다.

한편, 세계 IT보안 트렌드가 '통신상의 정보보호 경쟁'에서 '생활 속의 지식정보 보안 경쟁'으로 변화되고 확대되는 추세이다. 따라서 기존 컴퓨터 및 네트워크상의 정보보호 위주 산업 정책만으로는 변화되고 융합되는 보안 산업 트렌드에 부합되는 새로운 산업육성 전략 마련이 시급하다고 할 수 있다. 이러한 시대적 요구에 부응하고자 국내 지식경제부는 2008년부터 "지식정보보안산업" 발전전략 수립을 추진 중이며, 여기에서 지식정보보안이란, 암호, 인증, 인식, 감시 등의 보안기술이 적용된 제품을 생산하거나 관련 보안기술을 활용하여 재난·재해·범죄 등에 관한 서비스를 제공하는 것으로, 기술의 적용 영역, 제품의 특성 등에 따라 정보보안, 물리보안, 융합보안으로 세분화하고 있다 [5] . 여기에서 융합보안은 정보보안 또는 물리보안이 비IT기술 또는 다른 산업과 융합되어 창출되는 보안 제품 및 서비스를 의미한다. [표 1]은 지식경제부에서 발표한 융합보안의 적용이 필요한 산업과 적용 가능한 업종 및 제품, 기술에 대한 내용이다.

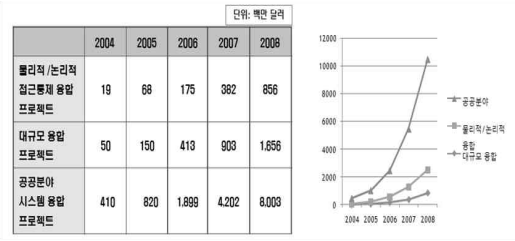
[표 1] 융합보안의 적용 분야 및 기술

운송보안 (자동차/항공/조선)	차량 지능키, 차량전자번호판, 차량블랙박스, 차량간 통신보안모듈, 차량통합보안관리, 승객용 스크리너, 조선보안
로봇보안	보안로봇, 네트워크로봇 보안
금융보안	금융ATM기기, OTP, 금융IC카드
의료보안	의료영상보안제품, 의료DB공유보안시스템
건설보안	지능형 건물/오피스 침입감지, 홈네트워크보안
국방보안	국방보안장비
산업보안	산업용 기기 보안

전 세계적으로 범죄, 테러, 재난예방을 위한 보안의 중요성이 부각되고 있으며, 응용 영역이 넓고, 여타 산업에의 파급효과가 큰 산업에 보안이 융합됨으로써 산업의 안전성 및 신뢰성을 강화할 필요가 있다. 또한 주요 산업에 필요한 융합기술 개발 주도권을 선점하는 것은 해당 분야에 있어 국가의 위상정립과 국내 관련 산업의 이익을 보호하는 차원에서 절실히 요구된다.

2.1 융합보안의 국내외 동향

정부와 기술 및 서비스 제공자를 대상으로 한 Gartner의 조사에 의하면, 2006년부터 2007년 상반기까지 단순 영상감시가 아닌 상황인지 기능을 제공하는 영상감지 시스템, 얼굴이나 지문 등으로 사람을 식별하는 바이오인식 등 물리적 보안기술에 대한 관심뿐만 아니라 융합보안에 대한 관심이 전년도에 비해 17.2% 상승한 것으로 나타났다 [3]. 또한, 물리적 보안과 기술적 보안의 통합 여부를 판단하기 위한 설문에 대한 응답으로 45%가 이미 통합되어 있다고 응답하였고, 35%는 통합을 고려하지 않고 있으며, 19%는 통합 되어있지 않지만 계획 중이라고 응답하였다 [3]. 2008년 물리적 보안과 기술적 보안의 시장규모는 약 4조 3천억 원으로 지속적으로 증가하는 추세이며, 융합보안의 시장규모 역시 증가하고 있으며, 약 1조 8천억 원의 시장규모를 형성하고 있다 [4]. 현재 물리적 보안과 기술적 보안의 시장규모가 융합보안의 시장규모보다 크지만, 증가 추세나 변화하는 정보보호 요구사항 등을 고려해보면 향후에는 융합보안이 물리적 보안과 기술적 보안의 기능을 대체하여 정보보호 시장을 주도할 것으로 예상된다. 아래의 [그림 2]는 유럽과 북미 지역의 융합보안 관련 프로젝트에 대한 지출 규모이며, 그 규모가 지속적으로 상승하는 것을 알 수 있다.



[그림 2] 유럽과 미국의 융합보안 관련 프로젝트 지출 규모

한편, 국내의 지식경제부는 보안과 기타 산업에서의 융합측면에서, 여타 산업 제품에 보안 기능을 탑재·내장되어 안전과 신뢰성을 향상시키는 융합보안 제품이 시장 수요를 창출할 것으로 예상하고 있으며, 차량, 국방, 의료, 건설, u-물류·항만 등 다양한 분야에서 융합보안 제품이 출시되고 있어 미래 Blue-Ocean 시장으로 예상하고 있다. 통계에 따르면, 융합보안 시장은 2007년 668억불에서 2014년 1,564억불로 연간 약 12.6%의 성장률을 보일 것으로 예상되며, 현재 선진국(미국, 일본, 유럽)대비 융합보안의 국내 평균 기술 격차는 1.7년, 상대 수준은 84%로 평가되었다 [5].

Ⅲ. 융합보안의 개념 정립

3.1 융합보안의 정의

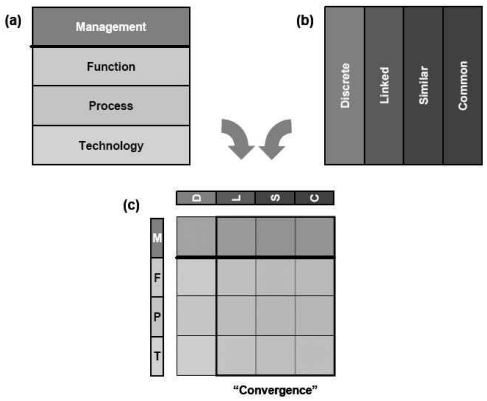
현재 융합보안에 대한 정의는 국제적으로 표준화되지 않았지만, 다양한 연구기관에서 제시되고 있다. 우선, ASIS(American Society for Information Science) International에서는 “융합”에 대한 정의를 “기업 내에 존재하는 비즈니스 기능과 프로세스 사이의 상호의존성 및 보안 위험을 식별하고, 이를 적절하게 관리할 수 있는 비즈니스 솔루션을 수립하는 것”이라고 내리고 있으며 [6], 이러한 정의는 보안이 단순한 기능적인 활동이 아닌 기업의 전반적인 사업 미션을 위하여 가치 함축적으로 그 의미가 변하고 있다는 의미이다. OSE(The Open Security Exchange)에서는 융합을 “물리적 보안

과 IT보안이 동일한 개체(objective), 프로세스, 아키텍처를 향하여 이동하는 것"이라고 정의하고 있으며, 여기서 개체란 비용 감소, 자산 보비용및 운영 효율성의 향상을 의미한다[7E]. TGartner에서는 융합보안을 물리적 보안과 정보보호가 IT위험을 관리하기 위하여 비슷하거나, 연계되거나, 혹은 동일한 프로세스와 기능을 갖추는 것이라고 설명하고 있으며 [3] , COSO online에서는 융합보안을 비용 효율적으로 전사적 차원의 위험을 관리하기 위하여 전통적인 운영적 위험관리의 기능을 통합하는 것으로 여기서 통합이란, 인적자원 보안, 사업 연속성, 재난 복구, 위험 관리 등을 논리적, 물리적으로 통합하는 것을 의미한다 [8] .

상기에서 살펴본 융합보안의 정의를 종합해 보면 융합보안이란 "비용 감소, 운영의 효과성 및 효율성 향상, 전사적 차원의 위험을 관리하기 위하여 조직의 보안 요소들이 점진적으로 통합되고 상호 협력하는 체계"라고 할 수 있다.

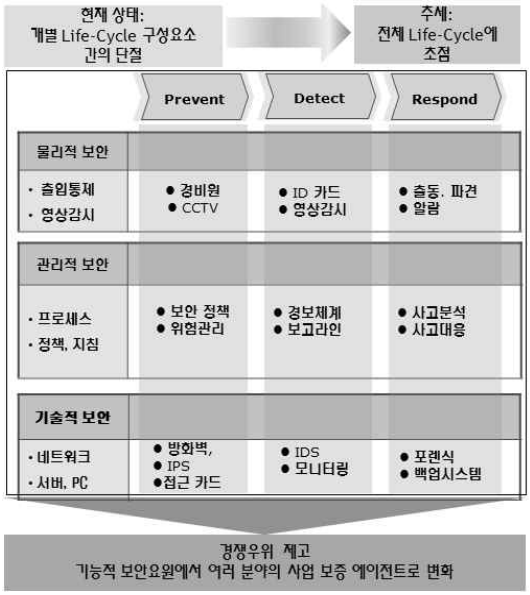
3.2 융합보안의 개념 모델

앞서 설명하였듯이, 현재 대부분의 조직에서는 물리적, 기술적, 관리적 보안이 서로 다른 프로세스와 기능들로 운영되어 왔다. 이러한 보안 구조는 중복 투자 및 관리 시간의 증가로 운영비용의 증가를 초래하였다. 이와 같은 문제점을 극복하기 위한 융합보안의 개념적 모델 중 아래의 [그림 3]과 같이 Gartner에서 제시한 융합보안의 모델은 각각의 영역의 기능, 프로세스, 기술이 서로의 연계된 정도에 따라 세 가지 수준으로 융합되어 하나의 영역에서 관리되어짐을 보여준다.



[그림 3] Gartner의 융합보안 모델

또한, AESRM에서는 아래의 [그림 4]와 같이, 서로 다른 조직의 인적자원, 프로세스, 기술들이 물리적, 기술적, 관리적 보안사고 예방, 탐지, 대응 주기와 서로 기능적으로 교차하는 융합보안 모델을 제시하였다. 이를 통해 조직은 보안비용을 감소시키고, 기능적 보안요원을 비즈니스 활동에 참여시킴으로써 일상적인 보안활동이 가능하게 된다.



[그림 4] AESRM의 융합보안 모델

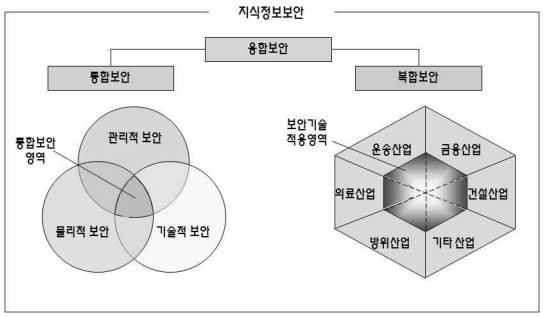
위와 같은 Gartner와 AESRM의 융합보안 모델은 융합의 방법에는 차이가 있으나, 개별적으로 수행되는 물리적, 기술적, 관리적 보안 기능 및 활동들을 상호 연계하여 통합적으로 관리한다는 공통점이 존재한다.

3.3 융합보안의 개념 재정립

상기에서 살펴본 국외 융합보안의 정의 및 개념모델은 다소 차이는 있으나 기존의 서로 다른 영역에서 수행된 보안 활동을 연계하여 하나의 영역에서 관리되어짐을 알 수 있다. 하지만 현재 국내에서 연구되고 있는 융합보안은 두 가지 차원에서 혼용되고 있으며, 그 의미가 상이한 만큼 적용 영역이나 기술체계도 다르다고 할 수 있다. 이는 향후 연구 및 적용에 혼란을 가져올 우려가 있으므로, 이에 대한 개념을 재정립 할 필요가 있다. 우선 국내 지식경제부에서 추진 중인 지식정보보안산업은

정보보안, 물리보안, 융합보안으로 구성되어 있으며, 정보보안은 컴퓨터 또는 네트워크상의 정보의 훼손, 변조, 유출 등을 방지하기 위한 보안제품 및 서비스를 의미하고, 물리보안은 주요 시설의 안전한 운영과 재난·재해 등의 방지를 위한 보안제품 및 서비스를 의미한다. 여기에서 정보보안은 보안 영역에서 다루어지는 관리적/기술적 보안의 개념과 유사하고, 정보보안 및 물리보안의 융합과 국외에서 연구되고 있는 관리적/기술적 보안과 물리적 보안을 통합적으로 관리하는 융합보안이 개념적으로 일치한다고 할 수 있다. 즉, 지식경제부에서 제시한 융합보안의 개념은 국외에서 사용되고 있는 융합보안에 대한 개념을 포함하지 않는 협의의 개념으로 사용되고 있다. 따라서 현재 국내외에서 혼용되고 있는 융합보안의 개념을 확장하는 한편, 구분을 위해 그 개념을 명확히 하여 서로 다른 접근방법을 사용해야 할 것이다.

지식경제부에서 제시하는 융합보안의 의미는 보안이 비IT기술 또는 다른 산업에 적용되어 새로운 보안 서비스 및 제품을 창출하는 것으로, 산업에서 생산되는 제품 및 서비스에 보안 기능이 탑재되어 제품 및 서비스의 신뢰성과 안전성을 향상 시킬 뿐, 이러한 제품 및 서비스 본연의 기능이 변하거나 생산 프로세스나 조직 구성이 변하는 것은 아니다. 따라서 산업에서 생산되는 제품 및 서비스에 보안 기능이 탑재되어 서로 개별적인 기능을 수행하므로 이를 “복합보안”이라고 명명하는 것이 적절하다고 판단된다. 또한 국외에서 사용되고 있는 융합보안은 물리적, 기술적, 관리적 보안의 기능 및 프로세스를 통합하여 동일한 영역에서 관리하는 개념으로 “통합보안”이라고 명명하는 것이 바람직할 것이다. 다시 말해, 통합보안과 복합보안은 모두 융합보안에 해당되며, 결국 지식정보보안이란 통합보안과 복합보안을 모두 포함하는 포괄적인 개념이라고 할 수 있다. 아래의 [그림 5]는 지식정보보안의 구성요소인 통합보안과 복합보안의 개념을 도식화한 것이다.



[그림 5] 통합보안과 복합보안의 개념

Ⅳ. 융합보안 접근방법

4.1 통합보안 측면

통합보안의 접근방법 중 조직구성 측면을 살펴보면, 우선 최근 이슈화 되고 있는 “Converged CSO"의 적용을 들 수 있다. Converged CSO는 물리적/기술적 보안 조직 및 프로세스, 통제 활동에 대한 충분한 지식을 소유한 통합보안의 책임자로, 최고 경영층으로 구성된 위원회에 참여하여 정보보호와 조직의 목표를 연계시키기 위한 중요한 역할을 수행한다. 또한, Converged CSO는 조직의 시스템이 복잡하고, 통합보안의 구현을 위한 자원이 부족할 경우, 기존의 물리적/기술적 보안 프로세스를 통합하지 않고, 각각의 보고체계를 구성하여, 개별적인 물리적/기술적 보안 프로세스를 통합적으로 관리할 수 있다. 한편, 기존의 물리적/기술적 보안 프로세스를 통합하였을 경우, 통합보안 전담 부서를 구성하여 정보보호 프로세스 및 통제를 효율적으로 평가, 모니터링 할 수 있다. 이러한 통합보안 전담 부서는 조직의 물리적/기술적 위험을 통합적인 시각으로 식별하고, 평가하며, 위험을 허용수준 이내에서 관리할 수 있도록 한다. 뿐만 아니라, 통합보안 적용 시 조직의 비즈니스 프로세스를 고려하는 것 또한 중요하다고 할 수 있다. 통합보안을 단순히 물리적 보안과 기술적 보안을 통합하는 개념으로 인식하는 것에는 한계점이 존재한다. 기존의 물리적/기술적 보안을 통합하여 관리하는 것도 중요하지만, 이것을 비즈니스 프로세스와 연계시켜 보안을 일상적인 업무수행의 일환으로 인식하고 수행하는 것이 중요하다고 할 수 있다. 즉, 조직의 일상적인 업무수행 프로세스에 존재하는 취약점을 식별하고, 이러한 취약점이 향후 보안사건 및 사고에 미칠 영향을 최소화하기 위해 통합된 물리적/기술적 보안 활동을 업무수행 프로세스에 반영할 필요가 있다.

4.2 복합보안 측면

앞서 살펴보았듯이 복합보안은 제품 및 서비스의 안전성과 신뢰성 향상을 위해 보안이 산업에 융합되어 산업의 부가가치를 높이는 것이라고 할 수 있다. 하지만, 단순히 제품 및 서비스에 보안기능을 추가하는 것은 여전히 한계점을 내포한다. 즉, 복합보안은 산업에서 창출

된 최종 결과물인 제품 및 서비스뿐만 아니라, 산업의 원천기술 및 지식, 인적자원 역시 보호해야 한다는 의미이다. 따라서 이와 같은 접근방법은 산업 내 존재하는 다양한 가치사슬을 고려하여 가장 많은 부가가치를 창출하는 요소를 식별하고, 이를 우선순위에 따라 보호해야 한다. 산업의 본원 적인 활동을 생산, 운송, 마케팅, 판매, 물류, 서비스 등과 같은 현장업무라 한다면, 이러한 본원적 활동을 지원하는 구매, 기술개발, 인사, 재무, 기획 등의 제반업무가 필요하다. 이러한 현장업무와 제반업무를 가치 활동이라 하였을 때, 원재료, 부품, 서비스 등을 제공하는 공급자의 가치사슬과 최종 산출물인 제품 및 서비스를 구매하는 구매자의 가치사슬에는 보안 취약점이 존재하며, 이러한 취약점으로 인해 산업 기술 및 지식이 유출될 위험이 존재할 수 있다. 따라서 우선적으로 산업보안 협의체를 구성하여, 여타 산업에 파급효과가 큰 사업을 선별하여 가치사슬 경로의 취약점을 식별하고, 비용-효과를 고려하여 우선순위에 따라 적절한 통제를 구현하고 운영한다면 신뢰성 및 안전성은 물론 시장수요 증진을 통해 산업의 부가가치를 향상시킬 수 있을 것으로 예상된다.

Ⅵ. 결 론

본 논문에서는 국외에서 연구되고 있는 융합보안의 개념을 기반으로 국내에서 혼용되고 있는 융합보안의 개념을 재정립하였다. 또한 융합보안을 통합보안과 복합보안 측면에서 분석함으로써 향후 융합보안 적용 시 고려해야할 접근 방법을 제시하였다.

효과적으로 융합보안을 구현하기 위해서는 하향식 접근법을 사용해야 한다. 이는 융합보안의 방향 설정, 구현, 지원이 상위 관리자에서 시작해서 중간관리자, 일반 사용자로 적용되어야 함을 의미한다. 따라서 이러한 하향식 접근법은 기업의 자산을 책임지고 있는 최고 경영층이 통합의 정도를 결정하고, 올바르게 역할과 책임을 할당한 후, 개선 여부를 파악하여 조직의 목표달성에 기여해야 할 것이다. 또한, 기존의 물리적, 기술적, 관리적 보안이 융합되었을 경우, 통합된 시각에서 성과를 평가 할 수 있는 척도나 기법들을 개발할 필요가 있다. 이는 융합보안이 기존의 보안체계의 문제점을 극복하여 어느 정도 효과적이고, 효율적인지 판단하기 위해 필수적이라 할 수 있다.

끝으로 본 논문에서 제시된 융합보안의 개념을 올바르게 이해하고 적용하였을 때 비로소 비용-효과적인 정보보호 활동을 수행할 수 있을 것으로 판단된다.

참고문헌

[1] Watson, James. “Physical and IT Security Must Go Together.” Computing, May 4, 2005.

[2] Booz, Allen, Hamilton, "Convergence of Enterprise Security Organizations", The Alliance for Enterprise Security Risk Management (AESRM), November 8, 2005.

[3] Nicole S. Latimer-Livingston, “Let's Get Physical What Clients Are Asking About the Integration of Physical and Logical (IT) Security", Gartner, November 9, 2007.

[4] Hunt Steven. “Trends 2005: Security Convergence Gets Real.” Forrester Research. January 11, 2005.

[5] “지식정보보안산업 발전전략", 지식경제부, 2008.

[6] Deloitte, “The Convergence of Physical and Information Security in the Context of Enterprise Risk Management”, The Alliance for Enterprise Security Risk Management, 2007.

[7] The Open Security Exchange (OSE), “Physical/IT Security Convergence: What It Means, Why It’s Needed, and How to Get There”, 2007.

[8] Scalet S.D., “Convergence: Case Study”, COSO online, 2005.

<著者紹介>

김 정 덕 (Kim Jungduk)
종신회원

1979년 : 연세대학교 정치외교학과, 학사
1981년 : 연세대학교 경제학과 대학원, 석사
1986년 : University of S. Carolina, MBA
1990년 : Texas A&M University, Ph.D. in MIS
1991년~1993년 : 한국전산원, 선임연구원
1993년~1995년 : 원광대학교, 조교수
1995년~현재 : 중앙대학교, 교수
<관심분야> 정보보호 거버넌스, 정보보호 관리, IT 감사, 정보시스템의 전략적 응용 등

김 건 우 (Kim Kunwoo)

2008년 8월 : 중앙대학교 정보시스템학과, 학사
2008년 9월~현재 : 중앙대학교 정보시스템학과, 석사과정
<관심분야> 정보보호 관리, 정보보호 거버넌스, 시스템 감사

이 용 덕 (Lee Yongduk)

2008년 2월 : 중앙대학교 정보시스템학과, 학사
2008년 3월~현재 : 중앙대학교 정보시스템학과, 석사과정
<관심분야> 정보보호 관리, 정보보호 거버넌스, 전사적 정보보호 아키텍처