석 사 학 위 논 문

융합 보안관제시스템 구축 활성화 방안 연구

- 공공기관 중심으로 -

2015년 6월

한성대학교 지식서비스&컨설팅대학원

융 합 기 술 학 과

IT 융 복 합 전 공

원 종 혁

석 사 학 위 논 문
지도교수 조세홍

융합 보안관제시스템 구축 활성화 방안 연구

- 공공기관 중심으로 -

A Study on Methods to Encourage the Implementation of Integrated Security Control Systems
- with a Focus on Public Organizations -

2015년 6월 일

한성대학교 지식서비스&컨설팅대학원
융 합 기 술 학 과
IT 융 복 합 전 공
원 종 혁

석 사 학 위 논 문
지도교수 조세홍

융합 보안관제시스템 구축 활성화 방안 연구

– 공공기관 중심으로 –

위 논문을 융합기술학 석사학위 논문으로 제출함

2015년 6월 일

한성대학교 지식서비스&컨설팅대학원
융 합 기 술 학 과
IT 융 복 합 전 공
원 종 혁

원종혁의 융합기술학 석사학위논문을 인준함

2015년 6월 일

심사위원장 _____ 인

심 사 위 원 _____인

심 사 위 원 _____인

국 문 초 록

융합 보안관제시스템 구축 활성화 방안 연구
– 공공기관 중심으로 –

한성대학교 지식서비스&컨설팅대학원
융합기술학과
IT융복합전공
원 종 혁

현대사회는 IT기술의 급속한 발전으로 인해 새로운 사회현상과 문화가 등장하게 되면서 다양한 분야의 융합이 이루어지고 있다. 이로 인해 정보자산의 가치도 함께 증가하게 되면서 이를 노리는 정보유출 및 보안사고에 따른 피해도 급증하게 되었다. 이러한 시대적 변화에 대응하고자 보안 분야도 더욱 변화된 보호체계가 필요하게 되었다. 과거의 보안위협으로는 비인가자 출입과 차량통제, 화재감시, 중요보안시설통제 등에 의한 물리적 영역이 대부분이었으나 최근에는 해킹과 같은 사이버공격과 중요시설 시스템 마비, 국가핵심기술 소스코드 유출 등의 지능적 범죄 피해가 증가하고 있다.

이처럼 보안에 대한 위협은 날로 커지면서 다양한 보안위협으로부터 정보자산을 보호하기 위해 물리적 보안 중심에서 정보보안 요소가 접목된 융합보안 형태의 보안관제시스템에 대한 도입에 관심이 높아지게 되었다.

그러나 아직까지 정부기관과 보안관제 전문 기업들조차 명확한 정책과 제도를 제시하지 못하고 있으며 보안사고 발생 시에 능동적인 대처가 부족하여 보안위협에 노출될 수밖에 없는 실정이다.

본 연구는 최근 들어 메가트랜드로 자리 잡고 있는 융합 보안관제시스템의 도입에 있어서 공급자 관점이 아닌 수요자 관점에서 접근하기 위해 선행연구를 통한 정부정책과 제도를 분석하였으며, 실제 구축사례를 통한 고객요구사

항과 한계점을 파악하고 실제 운영관리자와 관련업계 종사자들의 설문조사를 바탕으로 융합 보안관제시스템의 문제점과 시사점을 도출하였다.

연구대상은 융합 보안관제시스템을 도입한 고객사 중에 공공기관을 대상으로 연구하였으며, 융합 보안관제시스템을 공급하는 관련기업들의 홍보자료와 만족도 조사를 통해서 얻는 고객평가가 다소 상이함을 파악하고 이를 토대로 개선된 융합 보안관제시스템의 구축 및 커스트마이징을 위한 가이드라인을 제시하고자 한다.

본 연구는 지금까지 연구결과로 부족했던 부분인 실증분석을 보완하기 위해 실무 운영자의 인터뷰 및 설문조사를 통한 검증을 실시하였다. 설문대상자는 공공기관 보안관리자 및 관련업계 실무자들로서 인터뷰 및 설문조사를 통해서 시사점을 도출할 수 있었다. 우선 융합 보안관제시스템의 인식제고가 먼저 이루어져야 함을 제시하였으며 융합 보안관제시스템 도입 시에는 가장 우선 고려해야할 사항으로는 관련 법규 및 제도 부합여부가 중요한 이슈사항임을 제시하였다.

또한, 융합 보안관제시스템 제조사와 공급을 받는 기관의 요구사항에 대해 상이한 점을 발견하였으며, 그 이유로 현재 표준화 되어있지 않으며 도입 초기단계인 관계로 다소 시행착오를 겪으면서 문제점들을 도출하는 단계임을 판단할 수 있게 되었다.

본 연구 결과로 향후 융합 보안관제시스템 구축에 있어 좀 더 명확한 기준을 정하고 능동적인 융합보안 체계의 기틀을 마련하기 위한 가이드라인을 제시할 수 있었으며 구축 모범사례를 위해 공공기관이 선도적 역할을 함으로서 명실 공히 세계가 인정하는 IT강국으로서의 위상 제고에 기여하고자 함에 목적을 두고 연구를 하였다.

【주요어】 융합, 물리보안, 정보보안, 보안관제시스템, 지식정보보안, 융합보안관제센터, 융합보안관제시스템

목 차

표 목 차

그 림 목 차

I. 서 론

1.1 연구의 필요성과 목적

현대사회는 사회 전반에 걸쳐 급속한 발전으로 인해 유래 없이 편리하고 윤택한 생활을 하고 있다. 특히 IT 기술을 이용한 정보통신의 발전은 사회를 지식정보사회로 변화시키게 되었다. 이로 인해 전 세계 어디에서나 인터넷을 통해 지식과 정보를 공유할 수 있게 되었으며 이러한 기술 진보는 국가 경제 발전에 큰 영향을 미치게 되었다.

이러한 정보기술의 발전은 국가 및 기업 간 경쟁이 심해지면서 신기술 개발에 대해 큰 비중을 두고 투자가 이루어지고 있다. 그러나 기술을 보호하려는 인식은 상대적으로 부족하여 기술유출 및 각종 안전사고가 끊임없이 일어나고 있는 실정이다. 이에 따라 사회적 문제로 대두되는 보안 분야에 대해서도 자연스레 많은 영향을 주게 되었다. 미래학자 앨빈 토플러가 주창한 “산업스파이는 21세기 가장 큰 사업중의 하나이며, 결코 사라지지 않을 것이다.” 라는 말처럼 보안의 중요성은 더 이상 설명할 필요 없이 큰 이슈가 되고 있음이 분명하다.

과거의 보안 분야는 비인가자 출입통제, 차량통제, 화재감시, 중요보안시설 통제 등 주로 물리적 보안에 치중해 발전해 왔지만 최근 지식정보사회에 접어들면서 기업특허기술 유출, 각종 해킹으로 인한 중요시스템 마비, 국가핵심기술 소스코드 유출 등 정보보안의 중요성이 커짐으로 인해 복합적이고 통합적인 보안에 대한 요구가 증가하게 되었다. 이에 여러 기업들이나 금융기관, 정부부처 기관들은 물리적 보안 중심에서 정보보안 요소가 접목된 융합보안 형태의 보안관제시스템과 같은 솔루션에 대한 도입에 관심을 높이고 있다.

하지만 아직까지는 정부기관은 물론 보안관제 전문 업체들조차 융합보안과 관련된 명확한 가이드라인을 제시하지 못하고 있을 뿐만 아니라 능동적인 대처가 부족함으로 인해 각종 보안위협에 노출될 수밖에 없게 되었다. 융합보안에 대한 연구는 국외는 약 10년 전부터 활발하게 수행되고 있었지만, 국내는

최근 몇 년 전부터 정부기관 및 관련학회를 중심으로 논의되고 있는 수준이다.

이에 본 연구는 세계적으로 국가산업 주요과제로 떠오르면서 관심이 커지는 융합보안 및 융합 보안관제시스템에 대한 선행연구 분석을 통한 차별성을 가진 발전방안에 대한 연구를 목표로 하였다. 최근 물리적 보안과 IT기술 기반의 정보보안으로 양분화 되어 있는 영역자체가 융합되고 있는 추세이며, 이러한 융합의 중심에 있는 것이 융합보안관제라 지칭한다. 융합보안관제는 서로 개별적으로 운영 · 관리되어 왔던 물리적 보안영역과 IT기술을 접목시킨 보안관제 형태의 정보보안 영역을 하나의 관리범위 안으로 통합함으로써 보안 관리의 체계성을 확보하고 정보 유출 및 침해사고를 획기적으로 예방, 차단, 사후 추적 등이 가능하게 해준다.

따라서 본 논문은 융합보안의 발전 방향을 위해 좀 더 실질적인 문제와 이슈에 대한 분석을 목표로 관련업계 종사자 및 기업, 공공기관 보안 관리자, 보안관제 요원 등 융합보안 현장전문가들의 인터뷰 및 설문을 통해 근본적인 문제점을 다시 한 번 인식하고 향후 융합보안의 발전방향과 정책 제도화에 도움이 될 연구 자료를 확보하는데 있다.

나아가 산업 전반적인 분야에 융합기술이 적용됨으로서 자연스럽게 이슈로 떠오르게 된 융합 보안관제시스템 구축을 함에 있어 좀 더 명확한 가이드라인을 제시하여 제도정착 및 법제화를 촉진시키고 능동적인 융합보안 체계의 기틀을 마련하기 위해 공공기관이 선도적 역할을 함으로서 명실 공히 세계가 인정하는 IT강국으로서의 위상제고에 기여하고자 함에 목적이 있다.

1.2 연구의 방법 및 구성

본 논문의 연구방법은 융합보안 전반에 걸친 개념을 재정립하기 위해 선행연구를 바탕으로 한 구축동향과 정책 등을 분석하여 발전방안에 대해 연구하였고, 융합보안의 발전 방향제시를 위한 실질적인 문제와 이슈에 대한 분석을 목표로 관련업계 종사자 및 기업, 공공기관 보안 관리자, 보안관제 요원 등 융

합보안 현장전문가들의 인터뷰 및 설문을 통해 근본적인 문제점을 인식하고 향후 융합보안의 발전방향과 정책 제도화에 도움이 될 연구자료를 확보한 후 발전 방향에 대해 접근하였다.

연구방법에 있어서 기본적으로 문헌 및 사례조사를 중심으로 한 융합보안의 이론수립 통해 융합보안관제의 기술 이론을 정립하였고, 이와 관련된 융합비즈니스의 활성화 배경, 융합보안관제 분야의 구축 사례와 융합보안 정책동향을 살펴보았다. 융합보안관제 전반에 대한 내용을 살펴보기 위해 기존의 선행논문과 정부 및 민간에서 발간한 연구보고서 등 신뢰성이 높은 문헌에 대한 고찰을 중심으로 한 분석을 통해 연구를 진행하였다.[1] 현재 융합 보안관제에 대한 학계의 학술적인 자료와 정부의 심층적인 보고서 및 정책 등이 아직은 부족한 상태이며, 민간부문에서 발표된 융합보완 관련 논문과 산업자원부가 지정한 12개 보안관제 전문지정업체의 신제품 정보 및 추진전략보고서 그리고 출판된 단행본과 인터넷 검색 등 온라인과 오프라인을 통한 자료 수집을 병행하여 진행하였다. 이러한 자료들을 바탕으로 융합보안관제에 대한 개념정립과 다양한 구축사례분석 및 정책동향, 그리고 이를 토대로 하여 융합보안관제의 활성화 방안을 모색하였다.

따라서 본 연구는 경험적이고 실증적인 연구 방법을 도입하기 보다는 기존의 자료를 수집하여 분석・검토하는. 문헌연구를 기본으로 수행하였으며 동시에 융합보안관제 관련 분야의 전문가와 전문연구기관 그리고 관련 세미나 자료 등의 분석을 통한 연구방법을 수행하였다. 이와 관련된 본 논문의 구성은 다음과 같다.

제1장은 서론으로 본 연구의 필요성과 목적을 설명하였으며, 연구를 수행하는 방법과 본 연구의 구성을 기술하였다.

제2장은 이론적 고찰로서 기존에 발표된 논문 및 연구보고서를 기초로 융합보안 전반에 걸친 이론적 배경을 정의하였으며, 실제 구축사례를 검토한 후

---

1) 국내외 융합보안에 대한 선행연구논문 및 관련서적, 학회자료, 세미나자료, 인터넷정보를 얻었다. 그리고 융합보안 관련 법제도와 정책 등의 규정을 찾아 분석하였다. 특히 융합보안학회, 한국정보화진흥원, 한국인터넷진흥원(KISA)과 산업보안연구 등의 보고서를 참고하였으며 이외에 기타 정부기관의 이슈 리뷰 등 각종 학술적인 목적의 보도 자료를 살펴보았다.

본 연구의 차별성에 대해 서술하였다.

제3장은 융합 보안관제시스템의 주요현황과 정책을 조사하였으며 구축 동향 및 피해사고사례를 분석한 후 한계점 극복 및 개선방안 등을 제시하였다.

제4장은 본 논문의 핵심인 융합보안관제의 활성화 배경을 서술하였고, 관계기간 관리담당자와 관련업종 전문가들에 대해 설문조사 후 유형분석을 통해 활성화 방안을 모색하였다.

제5장은 결론의 단계로서 연구 결과를 종합적으로 정리하고, 본 연구의 시사점 및 향후 발전 방향을 제시하였다.

Ⅱ. 이론적 고찰

2.1 융합보안에 대한 선행연구

2.1.1 보안의 개념

보안(保安, Security)의 사전적 의미[2]는 위험, 손실 및 범죄가 발생하지 않도록 방지하는 상태를 말하고 있다. 보안이라는 기술적 용어는 무언가가 안전하지 않으나 안전해야 함을 뜻하며, 일반적으로 보호해야하는 대상에 대해 접근제어를 통해 안전을 도모하는 경우 보안이라는 용어를 사용한다. 보안의 목표 자체가 안전을 목표로 정의되고 있기 때문에 국내에서는 '보안'과 '안전'의 의미를 혼돈하거나 또는 그 의미를 크게 구분하지 않고 혼용하여 쓰게 되는 경우가 많이 발생하고 있다. 하지만, 보안은 피해발생의 원인이 '인간의 행위'라는 점에서 안전이라는 개념과는 엄연히 구분되어야 한다.

보안의 영역은 크게 물리적 영역과 논리적 영역의 두 가지 형태로 구분되어 정의할 수 있다. 일반적으로 물리적 영역은 '물리보안' 으로 지칭하며, 논리적 영역은 '정보보안' 으로 지칭할 수 있다.

2.1.1.1 물리적 보안 정의

사전적 의미의 물리 보안이란 물리적으로 정보, 인명, 시설을 보호하는 것을 의미한다. 이는 출입관리, 천재지변으로부터의 시설보호, 방범관리등 모든 물리적 위협에 대해 보안을 지키는 것을 의미한다. 물리적 방법이나 수단을 활용한 보안형태로서 자원이나 정보를 물리적으로 대응할 수 있는 기술적 · 환경적 통제의 범위를 의미한다.

또 다른 의미로 물리적 보안은 주요시설의 안전한 운영과 재난·재해, 범죄 등의 방지를 위한 보안제품 및 서비스로 정의할 수 있다. 대표제품으로 경비

2) 위키백과 (2015년 개정)

서비스, CCTV카메라, DVR/NVR시스템, 바이오인식(생체인식), 출입통제시스템 등이 있다. 물리적 보안 제품 중 CCTV 카메라 및 DVR 제품은 아날로그에서 네트워크 기반으로의 기술진화가 많이 진행되어 있다. 일반적으로 시설보안(physical security) 이라고도 표현되며 시대가 흐르면서 보안환경이 변하고 첨단기술이 접목되어도 그 중요성만큼은 절대 줄어들지 않고 있다.

최인호(2014)는 물리적 보안은 각종 방벽, 게이트, 창문 등의 출입문 관리 분야가 방범창, 방탄유리, 자물쇠, 금고와 같은 폐쇄형태의 분야, 그리고 출입통제시스템, 경보시스템, CCTV관리, 보안인력서비스, 침입감지시스템, 주차장 관리 등에 이르는 인력통제 분야로 분류하였다.

물리적 보안의 종류로는 크게 세 가지로 구분할 수 있는데 일반적인 경비서비스와 영상감시 시스템, 그리고 바이오 인식이다.

첫 번째, 경비서비스 산업은 사회의 범죄 예방 및 통제, 질서 유지라는 치안행정서비스의 제공은 경찰의 주요 업무영역이나, 사회의 각 부문들이 다양하게 발전하고 점차 범죄발생이 지능화·신속화·흉포화 되는 추세를 보이고 있어 안전에 대한 욕구가 증가되는 상황이다. 따라서 치안행정 서비스만으로 안전욕구를 충족시키는 것이 한계에 이르렀기 때문에 경비서비스 산업은 지속적인 성장을 보일 것으로 전망되어 진다.

두 번째, 한국산업기술진흥원(2012)은 영상감시시스템이 수집 영상에 대한 분석을 통해 물리적인 상황을 인지할 수 있는 시스템으로서, 현재는 지능형 영상인식기능이 추가된 지능형 영상보안시스템으로 발전되어 가고 있다. 최근들어 각종범죄로부터 지키기 위한 공공기관의 관심이 증가함으로 인해 관제해야 할 카메라 수가 증가함에 따라 처리해야할 연산량이 기하급수적으로 증가하게 되어 지능형 인식기능을 카메라 등에 분산하여 단계적으로 처리하는 분산형 방식으로 발전할 것으로 예상됨에 따라 향후 지능형 인식기능이 탑재된 스마트 카메라 시장 규모가 증가할 것이다.

세 번째, 바이오인식시스템은 삶의 환경이 변화함에 따라 기존제품은 사용자의 편리성을 강화시키는 방향으로 진화하고 있으며 신제품은 새로운 응용분야를 창출하는 방향으로 개발이 이루어지고 있다. 바이오기술(Bio Technology)과 정보기술(InformationTechnology)을 접목할 수 있는 유망산업으로 부상하고 있는

바이오인식 기술은 최근 정보보호의 중요성과 더불어 강조되고 있다. 인간의 신체에는 여러 가지의 특징이 있으나 그 중 얼굴, 지문, 홍채, 망막, DNA(DeoxyriboNucleicAcid)등이 바이오 인식기술에 사용되고 있으며, 이러한 신체적인 특징이 바로 개인의 고유한 비밀번호가 된다. 바이오인식 기술은 개인의 생체정보를 추출하여 정보화시키는 기술로써, 기존의 신분증, 카드, 패스워드 대신 지문, 얼굴 등의 신체적 특징을 이용하여 본인 확인을 하는 것이다.

또한, 출입통제나 개인인증을 위해 지문인식이나 홍채인식 제품들이 상용화되어 널리 사용되고 있으며, 최근 범죄 예방, 출입통제, 재난·재해 예방 등 사회 안전 목적으로 CCTV의 설치 및 운용이 급증하고 있으나, 기존의 영상을 단순 비교하여 검색하는 방법으로는 효과적인 검색을 할 수가 없다. 대용량 영상에서 효과적인 검색 및 인식을 위해 기존의 지문, 얼굴, 홍채인식 외에 걸음걸이, 옷 색상, 행위, 이벤트 등을 종합적으로 인식할 수 있는 융합형 바이오인식 기술이 요구된다. 향후에는 비제약적 환경에서 인식할 수 있는 차세대 바이오인식제품으로 발전할 것으로 예상된다고 하였다.

안황권(2011)은 기존 바이오 인식제품은 인식기에 지문이나 홍채가 정확하게 입력될 수 있도록 자세 등에 신경을 써야하는 단점이 있으므로, 사용자가 인식기에 대해 전혀 신경을 쓰지 않아도 자연스럽게 바이오정보가 입력될 수 있는 사용자 친화형의 원거리 바이오 인식기술이 활성화될 것이라고 하였다.

2.1.1.2 정보보안 정의

정보보안의 사전적 의미로는 정보의 수집, 가공, 저장, 검색, 송신, 수신 도중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적, 기술적 방법을 의미하며 정보를 제공하는 공급자 측면과 사용자 측면에서 이해할 수 있다.

공급자 측면에서는 내·외부의 위협요인 들로부터 네트워크, 시스템 등의 하드웨어, 데이터베이스, 통신 및 전산시설 등 정보자산을 안전하게 보호·운영하기 위한 일련의 행위를 말하고, 사용자 측면에서는 개인정보 유출, 남용을 방지하기 위한 일련의 행위로써 컴퓨터 또는 네트워크상의 정보의 훼손, 변조,

유출 등을 방지하기 위한 보안제품 및 서비스로 정의할 수 있다. 정보보안시장은 크게 정보보안 소프트웨어와 정보보안 하드웨어시장으로 나눌 수 있다. 보안제품 전문기업인 (주)시큐아이는 대표적인 정보보안 S/W(Software)로는 안티바이러스, 개인정보취약점분석솔루션 등이 있으며, 대표적인 H/W(Hardware)로는 방화벽(Fire Wall), 침입방지시스템(IPS : Intrusion Prevention System) 가상사설망장비 (VPN : Virtual Private Network), DDos 전용장비, 웹방화벽(Web Fire Wall) 등이 있다. 최근에는 정보보안 S/W와 H/W를 일체형의 통합보안 어플라이언스인 UTM (UnifiedThreatManagement) 개발과 출시가 보편화 되어가고 있다고 소개하고 있다. 시큐리티월드(2014)는 국내의 한정된 시장에서 점유율을 높이기 위한 전략으로 각각의 정보보안 S/W와 H/W들의 성장이 한계에 이르렀다는 사실을 나타내는 것으로 전망하고 있었다.

김영진(2012)는 정보보안 시장은 기업 IT 인프라의 안전성 보장 및 책임소재 여부에 관한 규정이나 개인 정보보호 지침이 강화될 것이 예상됨에 따라 더욱 견고한 통합보안서비스로의 시장이 확대될 것으로 전망하고 있다. IT 환경의 복잡성에 따라 견고한 보안인프라가 요구되고, 이에 따라 지속적인 수요가 기대되고 있는 실정이다. 보안제품 및 서비스의 통합화 양상은 지속될 것으로 보이고 있고, 정보보안업체의 보안과 스토리지, 시스템 및 네트워크관리 영역간 통합화도 가속화 되고 있는 실정이다. 다만, 글로벌 기업들의 시장 선점과 낮은 브랜드 인지도로 인해 해외시장에서 국내기업의 경쟁력은 매우 미미한 상황이며, 장기적인 성장 동력이 부족한 상황이다.

2.1.2 융합보안의 개념

지식경제용어사전(2015)은 융합보안(Convergence Security)의 개념을 물리적 보안과 정보 보안을 융합한 보안 개념으로 각종 내·외부적 정보 침해에 따른 대응은 물론 물리적 보안 장비 및 각종 재난·재해 상황에 대한 관제까지를 포함한다고 정의하고 있다. 현재 융합보안 개념으로 소개되는 각종 매체나 학술지의 내용은 정부가 지식정보 보안 산업을 정보보안 및 물리보안과 융합보안

등 3가지로 분류하면서 융합보안의 정의를 일반적으로 인용하고 있다. 이를 좀 더 자세히 살펴보면 2가지 관점으로 분류해볼 수 있다. 남기효(2014)는 첫째, 물리보안과 정보보안의 융합이라는 통합보안의 관점이 있다. 둘째, 非IT 산업에 보안을 적용하는 복합보안 관점과 같이 2가지 관점을 통칭하여 융합보안이라는 개념으로 정의하고 있다.

또한, ASIS(American Society for Information Science)[3] 에서는 융합보안에 대한 정의를 "기업 내에 존재하는 비즈니스 기능과 프로세스 사이의 상호 의존성 및 보안위험을 식별하고 이를 적절하게 관리할 수 있는 비즈니스 솔루션을 수립하는 것"으로 정의하고 있다. 즉, 융합보안이 단순한 기능적 활동이 아닌 기업의 전반적인 사업 미션을 위하여 가치 함축적으로 그 의미가 변하고 있다는 의미이다.

OSE(The Open Security Exchange)에서는 융합보안을 "물리적 보안과 IT 보안이 동일한 개체(Objective), 프로세스(Process), 아키텍처(Architecture)를 향하여 이동하는 것"으로 정의하고 있으며, 여기서 개체란 비용 감소, 자산 보호비용 및 운영 효율성의 향상을 의미하고 있다.

ScaletS.D(2005)는 융합보안을 "전사적 차원의 위험을 관리하기 위하여 비용효율적으로 전통적인 운영적 위험관리의 기능을 통합하는 것"이라고 정의하고 있는데 여기서 통합이란 인적 자원 보안, 사업연속성, 재난복구, 위험관리 등을 논리적, 물리적으로 통합하는 것이라고 정의하였다.

Gartner[4]는 융합보안을 물리적 보안과 정보보호가 IT위험을 관리하기 위하여 비슷하거나, 연계되거나, 혹은 동일한 프로세스와 기능을 갖추는 것이라고 정의하고 있다. COSO[5]는 융합보안을 비용 효율적으로 전사적 차원의 위험을 관리하기 위하여 전통적인 운영적 위험관리의 기능을 통합하는 것으로 여

---

3) 미국 정보과학협회 (전 미국문서협회 (American Documentation Institute))

4) 미국 코네티컷주에 본사를 둔 IT분야의 리서치 기업이다. 다국적 IT기업 및 각국의 정부기관 등을 주 고객으로 두고 있으며 설문 조사 부분의 높은 신뢰도로 공신력이 크다. 1979년에 설립되어 세계 75개국에 1,200여명의 애널리스트와 컨설턴트를 포함 3700여명의 직원을 고용하고 있다.

5) 1985년 미국에서 효과적인 내부통제 체계를 확립하기 위해 AICPA, AAA, FEI, IIA, IMA가 공동 설립한 단체다. COSO의 내부통제 프레임워크는 통제환경, 리스크평가, 통제활동, 정보 및 의사소통, 모니터링 를 통한 효과적인 업무를 수행하고 있다.

기서 통합이란, 인적 자원 보안, 사업 연속성, 재난 복구, 위험 관리 등을 논리적, 물리적으로 통합하는 것을 의미한다.

지금까지 살펴본 융합보안의 정의를 종합해 보면 융합보안이란 “비용감소 운영의 효과성 및 효율성 향상 전사적 차원의 위험을 관리하기 위하여 조직의 보안요소들이 점진적으로 통합되고 상호 협력하는 체계”라고 할 수 있다.

김민수(2011)은 융합보안의 정의로 정보보안 또는 물리보안이 IT기술 또는 산업과 융합되어 창출되는 보안 제품 및 서비스로서 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 있다고 하였다.

2.2 보안관제에 대한 선행연구

2.2.1 보안관제의 개념

관제(管制)의 사전적 의미는 “관리하여 통제함. 특히 국가나 공항 따위에서 필요에 따라 강제적으로 관리하여 통제하는 일을 이른다.” 로 정의하고 있다. 김영진(2011)은 국내에서는 1999년 최초의 보안관제 전문 기업인 안랩코코넛[6]이 보안관제 관련 업무를 시작한 이래 현재까지 명확한 정의 없이 “보안관제”라는 용어를 사용하고 있다고 하였다.

Bejtlich book Foreword by Ron Gula (2004)는 “Security Control” 또는 “Security Management Control”로 표현하고 있지만, 범위가 광범위하고 대상이 관점에 따라 달라지는 특성상 보안관제의 개념에 대한 학문적 정의는 미비한 실정이다. 미국의 Richard Bejtlich는 “Network Security Monitoring”에 대하여 “네트워크 트래픽 분석도구를 이용하여 24시간 365일 서버와 네트

6) 1999년 안철수연구소와 LG데이콤 등이 공동 출자해서 설립한 국내 최초의 보안관제 정보보호 기업. 보안관제 및 보안컨설팅 등을 주 사업으로 하는 k 기업임. 2007년 안철수연구소에 흡수 합병됨.

워크를 통해 통신한 데이터에서 잠재적인 침입자의 공격시도를 규명하고 이러한 과정에서 분석된 내용을 토대로 불명확했던 침입시도를 규명하는 일련의 행위"라고 정의 했다.

국내의 경우, 김영진(2010)은 "정보통신망이나 정보시스템에 대한사이버 공격정보 또는 보안관제 대상 자산의 안전성 판단정보를 탐지. 분석. 대응하는 일련의 활동"이라고 정의하고 있다. 이현도(2012)는 보안관제 업무에 대하여 "관제 대상기관의 정보 기술(IT)자원을 사이버공격 으로부터 보호하기 위하여 보안 이벤트 및 로그 등을 중앙 관제 센터에서 실시간으로 감시 및 분석, 대응하는 업무"로 정의하였다. 정의연(2011)은 보안 관제란 내·외부인에 의한 불법해킹, 또는 각종 유해한 요소로부터 고객이 보유하고 있는 시스템, 네트워크, 데이터 등의 손상을 막고, 피해 발생 시 원상회복 및 재발 방지를 위한 총체적인 운영관리를 말한다고 하였다.

또한, 「국가사이버안전관리규정」[7]은 "사이버공격"을 "해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스방해 등 전자적 수단에 의하여 국가정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 일체의 공격행위"라 규정하고, 이러한 사이버공격 정보를 탐지·분석하여 즉시 대응 조치를 할 수 있는 기구를 "보안관제센터"라 규정하고 있다. 그리고 「보안관제 전문업체 지정 등에 관한 공고」에서는 "보안관제" 를 "조직의 정보기술 자원 및 보안 시스템을 안전하게 운영하기 위하여 사이버공격 정보를 탐지 및 분석하여 즉시 대응하는 일련의 업무"라 규정하고 있다. 즉, 보안관제센터 업무는 사이버공격 등으로부터 공공기관의 정보자산을 안전하게 보호하는 모든 업무 및 행위를 뜻한 다는걸 알 수 있다.

한편, 한국정보통신기술협회의 IT 용어사전[8]에는 "보안 관제 서비스"를 "고객의 정보기술(IT)자원 및 보안시스템에 대한 운영 및 관리를 전문적으로 아웃소싱 하여 각종 침입에 대하여 중앙 관제 센터에서 실시간으로 감시 및 분석, 대응하는 서비스와 정보자산에 대한 보안은 전문 보안업체에 아웃소싱하고, 고객은 자신의 핵심 역량에 집중할 수 있는 선진화된 보안서비스"라 정의하고 있다. 공공기관의 아웃소싱 보안관제 업무는 공공기관이 발주하는 보안

7) 국가정보원,『국가사이버안전관리규정』대통령훈령 제316호, 2013
8) 한국정보통신기술협회 (2015) www.tta.or.kr

관제센터 위탁운영 용역사업을 수주한 보안관제 전문업체가 대행하는 업무로 정의할 수 있다. 이상 살펴본 내용을 종합해 볼 때, 본 연구에서는 “아웃소싱 보안관제”의 정의를 “공공기관의 정보자산을 사이버공격으로부터 안전하게 관리, 운영될 수 있도록 보안관제 전문업체가 수행하는 사이버 공격 정보 탐지. 분석 및 즉시 대응하는 일련의 업무”라 정의하고 있다.

2.2.2 보안관제 서비스 정의

「국가사이버안전관리규정」에서 보안관제 서비스는 고객의 정보 기술(IT) 자원 및 보안 시스템에 대한 운영 및 관리를 전문적으로 아웃소싱 하여 각종 침입에 대하여 중앙 관제 센터에서 실시간으로 감시 및 분석・대응하는 서비스 및 정보 자산에 대한 보안은 전문 보안업체에 아웃소싱하고 고객은 자신의 핵심 역량에 집중할 수 있는 선진화된 보안 서비스를 지칭한다고 하였다.

2.2.3 보안관제 관련법 및 제도

2.2.3.1 보안관제센터 운영의 근거

보안관제 센터에 관한 직접적인 법제도 차원으로는 중앙행정기관, 지방자치단체 및 공공기관이 적용대상인 대통령훈령 제316호『국가사이버 안전관리규정』이 제정되어 시행중이며 “제4조(사이버안전 확보의 책무), 제8조(국가사이버안전센터), 제10조의2 (보안관제센터의 설치・운영)”에 다음과 같은 구체적인 사항을 언급하고 있다.

제10조의2(보안관제센터의 설치·운영)

① 중앙행정기관의 장, 지방자치단체의 장 및 공공기관의 장은 사이버공격 정보를 탐지·분석하여 즉시 대응 조치를 할 수 있는 기구(이하 "보안관제센터"라 한다)를 설치·운영 하여야 한다.

-중략-

③ 보안관제센터를 설치·운영하는 기관의 장은 보안관제센터의 운영에 필요한 전담직원을 상시 배치하여야 한다.

④ 보안관제센터를 운영하는 기관의 장은 필요한 경우에는 미래창조과학부장관이 지정하는 보안관제전문업체의 인원을 파견 받아 보안관제 업무를 수행하도록 할 수 있다.

미래창조과학부 『정보통신기반 보호법』(2014) "제16조(정보공유·분석센터)에 따르면 아래와 같이 보안 관제와 유사한 업무를 수행하는 센터를 구축·운영할 수 있다고 되어 있다.

제16조(정보공유·분석센터) ①금융·통신 등 분야별 정보통신기반시설을 보호하기 위하여 다음 각 호의 업무를 수행하고자 하는 자는 정보공유·분석센터를 구축·운영할 수 있다.

1.취약점 및 침해요인과 그 대응방안에 관한 정보 제공

2.침해사고가 발생하는 경우 실시간 경보·분석체계 운영

2.2.3.2 보안관제센터 위탁에 따른 관련 법규

「금융기관의 업무위탁 등에 관한 규정」[9]에 따르면 보안관제센터를 자체 구축 및 운영 시 비용이 과다하게 소요되므로 많은 기업들은 보안관제 업무를 위

9) 『금융기관의 업무위탁 등에 관한 규정』, 금융위원회고시 제2013-18호, 2013

탁개념으로 보안관제 전문업체로부터 원격관제 서비스를 받고 있으며, 규모가 있는 정부, 공공기관, 대기업의 경우 자체적으로 구축한 보안관제센터 내에 보안관제 전문 인력을 파견 받아 관제서비스를 수행하고 있다. 보안관제 위수탁시 주요한 과업내역은 다음과 같다.

-위수탁업무의 범위(공급주기, 내용, 형태 등)
-업무수행의 수단
-정보제공 책임(수탁자 내부의 영업상 중요정보 포함)
-수탁자에 대한 감사 권한
-업무 위수탁에 대한 수수료 및 보상금
- 위탁업무에서 발생하는 자료에 대한 위탁금융회사의 소유권과 당해 금융회사의 물적 설비 및 지적재산권 등의 이용조건
-고객정보의 보호 및 비밀유지에 관한 사항
-업무의 연속성을 확보하기 위한 백업시스템 확보 등 비상계획
-면책조항, 보험가입, 분쟁해결(중재, 조정 등)방법
-수탁자의 책임한계
-계약의 파기 또는 종료(위탁금융회사의 계약해지권, 자료의 복구방법 등)에 관한 규정
-감독당국의 검사 수용의무
-수탁자가 업무 재위탁시 원계약 준수 명시
-준거법 및 관할법원(업무위수탁 상대방이 외국에 소재하는 경우)
-기타 업무위수탁에 따른 리스크관리 등을 위하여 필요한 사항 등

금융기관 이외 공공기관이나 일반 정보통신서비스를 통해 사업을 영위하는 기업들이 보안 관제를 위탁할 시 『정보통신망 촉진 및 정보보호 등에 관한 법률』과 개인정보보호법 등을 준용하고 있다.

2.3 융합 보안관제시스템에 대한 선행연구

2.3.1 융합 보안관제시스템의 개념

SJIS[10](2013)은 지금까지 융합 보안관제시스템은 방화벽, IPS, VPN, 바이러스월 등과 같은 기존의 IT보안제품과 같은 단일 솔루션에 의한 모니터링 및 방어 체계를 시작으로 위협관리시스템, 통합보안관제시스템 등의 통합형태의 발전을 보이고 있다고 보고하였다. 국가정보원(2015)는 기존의 IT 기반의 보안관제 시스템은 내부직원 또는 차량 등과 같은 출입자에 대한 모니터링 정보와 연계되어 있지 않아 물리적인 정보 유출 및 침해 사고를 예방 차단하거나, 사후 조치에 비효율적인 구조를 가지고 있다. 물리보안과 정보보안에 관련된 이벤트 정보가 정형화된 상관 분석을 하게 된다면 보다 적극적인 방어 체계로서 기대할 수 있다고 하였다.

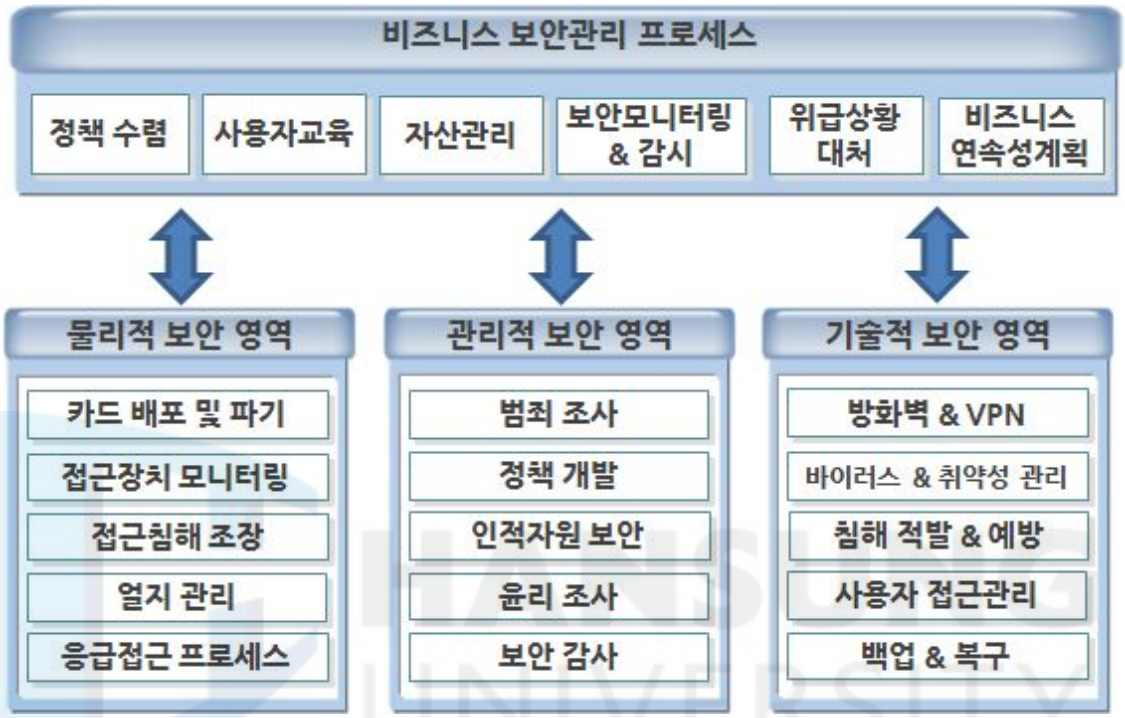
김민수(2011)는 기존의 IT기반 보안관제 시스템에서 네트워크 트래픽과 보안 이벤트를 여러 가지 방법으로 상관 분석하여 위험도를 자동화 했다면, 융합조안관제에서는 출입통제시스템과 CCTV와 같은 물리보안시스템을 통해 얻을 수 있는 이름, 출입시간, 출입위치, 출입방향, 출입차량 번호 등과 같은 출입자 정보와 기존의 보안시스템에서 얻을 수 있는 IP 및 네트워크 사용현황, PC사용정보, 문서 인쇄정보 등과 같은 다양한 이벤트 정보를 상관 분석함으로써 사고 발생 가능성을 찾아내고 이를 미연에 예방할 수 있으며, 사고 발생 시 효율적인 원인 추적이 가능하다고 하였다.

2.3.2 융합 보안관제시스템의 필요성

김정덕(2009)은 현재 대다수의 조직에 적용된 보안체계를 살펴보면서 <그림 1>과 같이 하나의 보안 관리 프로세스 아래 물리 적 보안 영역, 관리적 보안 영역, 기술적 보안 영역의 세 가지 영역으로 분리되어 운영되고 있다고 하였다. 그러나 이러한 보안체계는 동일한 지배구조 하에 있지만 관리자 및 관리

10) 삼성 SDS JOURNAL 로서 주로 컨설팅팀이 보고 자료를 발표함

대상이 상이하여 서로간의 상호 연계성이 어려운 것이 사실이다. 즉, 각각의 보안체계가 잘 수립 되었더라도 하나의 영역에 취약점이 발생하였을 경우, 전사적인 차원의 보안사건/사고를 미리 예방하거나 이에 대처하기 힘들다는 의미를 내포하고 있다고 하였다.



<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)[11]에서는 다음과 같이 5가지 측면에서 융합보안의 필요성을 제시하고 있다.

첫 번째, 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 아웃소싱

11) ASIS 에서 발간한 보안위험관리백서 (2010)

하고 있으며, 이러한 제3자는 전 세계적으로 확장되고 있다.

두 번째, 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 정보보호노력이 동시에 고려되어야 한다.

세 번째, 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.

네 번째, 비즈니스 트랜잭션이 점차 복잡해지고 새로운 위협들이 등장함에 따라 Sarbanes-Oxley 등의 기업이 준수해야하는 최소한의 보안 수준을 요구하는 법, 규제가 등장하고 있다.

다섯 번째, 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 5가지 융합보안의 필요성은 필수적인 동인으로 작용하고 있으며, 근본적으로 조직에서 보안의 역할을 변화시키고, 보안영역 내의 기능적 교차를 통하여 전체적인 측면에서 비즈니스 프로세스 또한 변화시킨다고 하였다. 이는 세계 IT보안 트렌드가 '통신상의 정보보호 경쟁'에서 '생활 속의 지식정보보안 경쟁'으로 변화되고 확대되는 추세라는 걸 의미하고 있다. 따라서 기존 컴퓨터 및 네트워크상의 정보보호 위주 산업 정책만으로는 변화되고 융합되는 보안 산업 트렌드에 부합되는 새로운 산업육성 전략 마련이 시급하며 융합 보안관제시스템의 필요성이 대두되었다.

국내에서는 시대적 요구에 부응하고자 산업자원부가 2008년부터 "지식정보보안 산업" 발전전략 수립을 추진하였다. 여기에서 융합보안은 정보보안 또는 물리보안이 비IT기술 또는 다른 산업과 융합되어 창출되는 보안 제품 및 서비스를 의미하고 있다. <표 1>은 산업자원부에서 발표한 융합보안의 적용이

필요한 산업과 적용 가능한 업종 및 제품, 기술에 대한 내용을 제시한 것이다. 제시된 융합보안의

<표 1> 융합보안의 적용 분야 및 기술

적용분야	적용기술
운송보안 (자동차/항공/조선)	차량 지능키, 차량전자번호판, 차량블랙박스, 차량 간 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

※ 출처 : 산업통상자원부 (2008) "지식정보 보안 산업" 발전전략

남기효(2014)는 융합시대에 기업 가치의 비중이 물리적 자산에서 정보자산으로 이동하는 것을 고려하여 보다 효과적인 보안 서비스를 제공하고자 하는 노력의 일환에서 발생하였으며 그 필요성이 증가하고 있다고 하였다. 과거에는 물리적 자산이 주요한 자산이었으나, 최근에는 정보시스템의 도입이 확산되면서 업무 효율성 증가를 위한 IT기술의 이용이 확대되었고, 비 IT산업에서도 정보자산의 가치가 증가하면서 보호의 중요성도 함께 커지게 되었다. 새롭게 가치가 증가한 정보자산을 보호하기 위한 방법으로 보안의 적용의 활용성이 커짐에 따라 필요성이 증가하였다.

2.4 융합 보안관제 산업 현황

2.4.1 융합보안 산업 정의

한국전자통신연구원(ETRI)은 현재 산업계에서 활발히 연구되고 있는 융합보안의 범위는 `산업+IT` 또는 `물리보안+IT`에 따른 정보보안 중심의 융합산업보안(security for convergence) 형태와 정보보안과 물리보안 영역의 기술이나 제품을 결합한 보안기술융합(convergence of security)로 나눌 수 있다고 하였다. CCTV와 IT의 융합에 따른 VPN(가상사설망) 기술의 도입, 주요기반시설을 포함한 주력산업과 IT와의 융합에 따른 정보보안 기술의 접목은 `융합산업보안`의 대표적인 예로 분류되고 있다고 하였다.

디지털타임스(2012)에서는 현재 보안업계에서 가장 활발한 융합·통합 작업이 이뤄지고 있는 분야로는 융복합관제시스템 분야 연구를 꼽을 수 있다고 하였다. IT기술의 발전과 함께 산업기밀 유출통제가 화두로 떠오르면서 물리영역의 관제와 정보보안 영역의 관제의 융합-통합이 가속화되고 있다는 것이 관련 업계의 전망이다. 이는 영상보안시스템·CCTV 등 기존 물리보안관제 기술에 회사 내부 네트워크 인증관리, 문서 보안관리, 이메일 필터링 시스템 등까지 확보된 시스템에 대한 산업계의 요구가 높아지고 있기 때문에 나타나는 현상으로 보는 관점이 지배적이라고 보도하였다.

여기에 그치지 않고 융합보안 관제분야에서는 CCTV와 출입통제시스템 등을 개별적으로 운영하던 것에서 한 발 더 나아가 PC사용정보, IP 및 네트워크 사용현황, 문서인쇄정보 등 정보보안영역의 개별 보안서비스를 함께 묶어 내외부 침입자 및 네트워크단 문제점까지 함께 살피는 서비스를 지향하고 있다. 또한, 스마트폰·태블릿PC등 스마트 기기를 활용한 외부에서의 업무 처리가 늘어나면서 임직원의 핵심 정보 유출 등 부적절한 행동을 원격으로 제어할 수 있는 기술들이 우후죽순 출시되고 있다. 그 중 가장 눈에 띄는 기술로는 회사 내부 등 정보가 유출될 수 있는 공간에 진입하면 스마트폰의 카메라나 녹음 기능을 원격 통제해 차단시키는 식으로 정보 유출 가능성을 원천적으로 차단하는 기능이다.

이와 유사한 기능으로 Push 앱을 들 수 있는데, 우리가 백화점이나 대형마트, 영화관 건물에 들어가면 자동적으로 관련쇼핑정보, 영화상영시간 등의 실시간 상황이 저절로 스마트폰에 띄워져서 자연스레 정보를 접하게 되는 기능들이 있다. 그리고 집이나 회사 등 특정장소에 배치한 PC에 클라이언트를 설치하고 이를 통해 PC 주변 중요 범위를 웹카메라로 감시하며 영상을 스마트폰으로 전송받을 수 있는 기술도 소개되고 있는데, 이 기술은 집을 비우고 장기간 여행을 떠나거나 사내주요 자산을 원격으로 감시하는데 유용한 기술로 많은 관심을 받고 있다.

안황권(2011)은 바이오인식 분야의 융합 연구도 활발하게 이뤄지고 있다. 지문, 얼굴, 홍채인식 등 다양한 바이오인식 기술을 바탕으로 출입보안, 근태관리, 전자주민증, 범죄자감식 등 다양한 영역으로 제품 및 서비스 공급을 확장하고 있는 바이오인식 기술 보유 기업들은 본인확인을 위한 바이오인식 기술을 융합한 다양한 시도를 하고 있다. 특히 `지문+얼굴`,`지문+홍채` 등 두 가지 바이오 정보를 결합한 멀티모달(Multimodal Biometrics)에 대한 연구 및 제품 출시가 한창이다. 국산 바이오인식 기술을 바탕으로 해외시장 전자주민증 및 전자투표 시스템에 진출하는 등 해외진출도 활발하게 이루어지고 있다고 하였다.

한국인터넷진흥원(2014)은 군부대 시설이나 과학기술연구소 분야도 접목 사례가 늘고 있으며, 군부대나 연구소를 둘러싼 방대한 외곽 울타리 지역에 광케이블망 장비 및 화상감시시스템을 설치해 광케이블에 인가된 자장변화를 감지하거나 외곽에 설치된 보안 와이어 주변에 물체가 접근하면 이를 즉각 감지해 원격 보안 및 통제가 가능한 기술이 활용되고 있다고 한다.

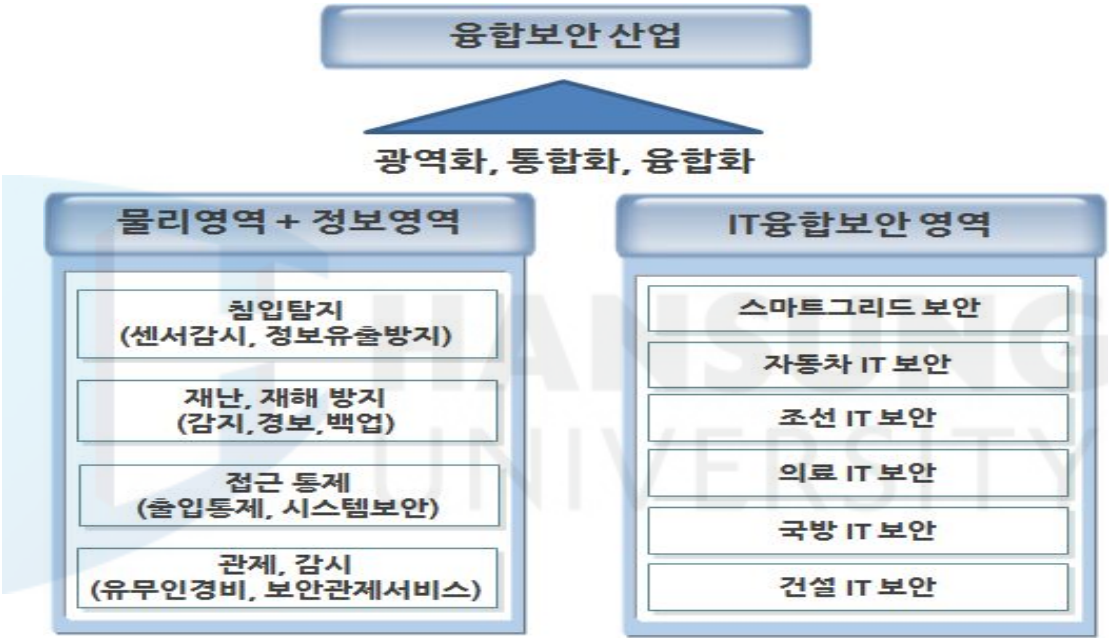
그 외에도 다양한 분야에서 융합 연구가 활발히 진행되어지고 있다. 도・감청 방지 등 통신보안 분야에서는 산업스파이를 막기 위해 사무실 내 비품 및 벽면 내에 은닉된 도청기를 찾아낼 수 있는 도청탐지기, 대화시 유리창에 진동하는 음성을 레이저파를 이용해 도청할 수 있는 기술까지 등장했다.

국가정보보호백서(2104)에서는 정부의 이 같은 흐름에 발맞춰 융합보안을 지난 2010년부터 주요 공공시장 창출 분야로 선정하고 다양한 지원정책을 펼치고 있다고 한다. 그중에 스마트워크 시스템 구축, 홈랜드시큐리티 산업 발

전전략 수립을 위해 2012년 102억원, 2013년 146억원, 2014년 150억원 등 총 약 470억원 규모의 공공 융합보안 분야 투자를 지원하고 있다.

조현숙(2013)은 관련기관에서는 "융합보안 분야 활성화를 위해서는 물리보안과 정보보안의 연계를 촉진시킬 수 있는 구체적인 법이나 가이드라인을 정부 차원에서 정립하고, 물리보안과 정보보안 내 상황정보 통합 및 공유에 대한 원천기술 R&D를 확대해야 한다."고 강조하고 있다.

삼성SDS 저널(2013)에서 소개한 융합보안 산업은 물리영역과 정보영역이 IT 융합보안 영역과의 광역화, 통합화, 융합화를 통해 이루어진다고 하였다.



<그림 2> 융합보안 산업의 구성

2.4.2 융합보안 시장 형태

국가정보원(2015)는 보안이란 국가 · 개인 · 기업의 유 · 무형 자산 및 인적 자원의 안전과 보호를 의미하며, 보안 산업이란 이를 위한 보안제품을 생산하거나 보안 서비스를 제공하는 산업을 의미한다고 하였다. 삼성SDS(2013)은 이러한 측면에서 전통보안산업은 물리영역과 정보(IT)영역으로 구분되어 성장해 왔으나, 현재 보안 산업은 출입통제, 주차시설 관리, CCTV, 영상보안 등

물리적 환경에서 이뤄지는 전통적 물리보안 산업이 컴퓨터, 네트워크상의 정보를 보호하는 IT 정보보안 기술과의 접목을 통해 차세대 고부가가치 융합보안 서비스 산업으로 부상하고 있다. IT기술이 자동차 · 조선 · 의료 · 건설 · 전력 등 기존 산업에 활용되면서 IT와 산업간 융합에서 발생되는 보안위협을 해결하기 위한 새로운 형태의 보안제품 및 서비스가 선보이고 있다.

산업자원부(2012)는 보안 산업의 새로운 트렌드로 자리 잡은 광역화, 통합화, 융합화의 사회적 요구를 수용하기 위해 기존의 정보보호 산업을 '지식정보보안 산업'으로 새롭게 정의하였다. 지식정보보안 산업이란 암호, 인증, 인식, 감시 등의 보안기술이 적용된 제품을 생산하거나, 관련 보안기술을 활용하여 재난, 재해, 범죄 등을 방지하는 서비스를 제공하는 산업으로 정의된다.

<표 2> 지식정보보안 산업의 분류

구분	정의	대표 제품
정보보안	컴퓨터 또는 네트워크상의 정보 훼손, 변조, 유출 등을 방지하기 위한 보안제품 및 서비스	방화벽, 안티바이러스, Forensic 툴
물리보안	주요시설의 안전한 운영과 재난·재해, 범죄 등의 방지를 위한 보안 제품 및 서비스	보안관제, CCTV, 영상보안, 바이오 인식
융합보안	정보보안과 물리보안 간의 융합 또는 보안 기술이 비 IT 기술·산업과 융·복합되어 창출되는 보안 제품 및 서비스	차량 블랙박스, RFID 보안칩

※ 출처 : 산업통상자원부 (2010) 지식경제백서

지식정보보안 산업은 <표 2>에서 분류한 것처럼 기술의 적용영역 및 제품의 특성 등에 따라, 네트워크·시스템 기반의 '정보보안', 안전·안심 생활을 위한 '물리보안', 정보보안과 물리보안 간의 융합 또는 보안기술과 전통산업간 융합으로 창출되는 '융합보안'으로 세분화 된다고 발표하였다.

삼성SDS저널 및 SERI 보고서에 따르면, 융합보안시장이란 컴퓨터, 소프트웨어, 저장장치 등과 같은 IP기반의 네트워크를 사용하는 기술들과 모터, 스위치, 기타 컨트롤 장치 등 동력기반 장치들의 병행 발전에서 유래되었다고 할 수 있다. 개인, 기업, 국가의 유무형 자산 및 인적 자원 안전과 보호를 위한 제반 활동에 사용되던 전통적 물리적 보안 기술은 9·11 테러 이후 테러 및

범죄예방을 위해 CCTV를 중심으로 IP기반 기술과 지능형 영상인식 SW기술의 융합을 통해 지속적인 진화를 거듭하고 있다. 최근 물리적 보안과 IT기술 기반의 정보보안으로 양분화 되어 있는 영역자체가 융합되고 있는 추세이며, 이러한 융합의 중심에 있는 것이 융합보안관제이다. 융합보안관제는 출입통제 시스템, CCTV 등 개별적으로 운영·관리되어 왔던 물리적 보안영역과 IT 통합보안관제시스템을 하나의 관리범위 안으로 통합함으로써 보안 관리의 체계성을 확보하고 정보 유출 및 침해사고를 획기적으로 예방, 차단, 사후 추적 등이 가능하게 해준다.

한편, 융합보안 산업은 최근 이종 산업간 융·복합화의 대표적 사례로 다양한 산업분야에 보안기능이 탑재되면서 미래 Blue – Ocean으로 부상하고 있다고 해도 과언이 아니다. 다가올 유비쿼터스 사회의 차량, 국방, 의료, 건설, u-물류·항만 시스템 등의 안정과 신뢰성을 담보하는 핵심요소로 향후 엄청난 시장 수요의 예측에 대한 보고가 앞 다투어 발표되고 있다.

융합보안 시장은 2013년 기준 세계 2,700억불에 전체 지식정보보안시장의 약 74%를 차지하고 한해평균 12.7%의 성장률을 가지고 있습니다. 국내융합보안시장은 2010년 약 1조 7,000억 원으로 정보보안시장 규모인 1조 3,000억 원을 넘었으며 2018년까지 연평균 32% 성장하여 12조 8,000억 원에 이를 것으로 예상되고 있다.

한편, 융합 보안관제시스템은 이제 시장초기단계라서 시장성에 대해 정확히 보고된 자료는 없지만, 융합보안시장과 더불어 고속성장 할것이라는 데에 이견이 없다. 융합 보안관제 시스템을 도입하는 가장 큰 동기를 살펴보면 물리보안과 정보보안 사이에 존재하는 보안 공백을 제거하기 위함이며, 이러한 영역의 분리에 따른 보안사고 및 이슈는 지식정보사회의 새로운 해결과제로 부각되고 되었고, 그 해결책으로 등장한 융합 보안관제시스템의 급격한 시장 성장이 예상되어 진다.

2.4.3 융합보안 시장 규모

해양수산개발원은 융합보안 시장은 2014년 기준 세계 2424억 달러, 국내5조

5113억 원 규모의 시장이 형성되었다. 물리영역 보안시장에서 융합보안 시장으로의 전환율은 2007년에 29%, 2010년에 51%, 2013년에는 59%로 2010년을 기점으로 물리영역 내 융합보안 제품이 전체시장 규모의 50%를 상회하는 것으로 집계되었다.

<표 3> 세계보안시장 성장 규모

단위 : 억 달러

구분		2007	2010	2012	2014	2018	CAGR
정보영역		416	663	825	1,091	1,843	14.50%
물리 영역	물리보안	508	474	509	573	839	4.60%
	물리+정보	208	494	675	860	1,259	17.80%
IT 융합보안		668	1,068	1,292	1,564	2,461	12.60%
융합 보안 소계		875	1,561	1,966	2,424	3,720	14.06%

※ 출처 : 해양수산개발원 “국가 물류보안체계 확립방안”

국내 융합보안 시장은 이미 2010년에 1조 6747억 원으로 정보보안 시장규모인 1조 2727억 원을 넘어 섰으며 2018년까지 평균 32.92% 성장한 12조 8396억 원에 이를 것으로 예상되고 있다.

<표 4> 국내보안시장 성장 규모

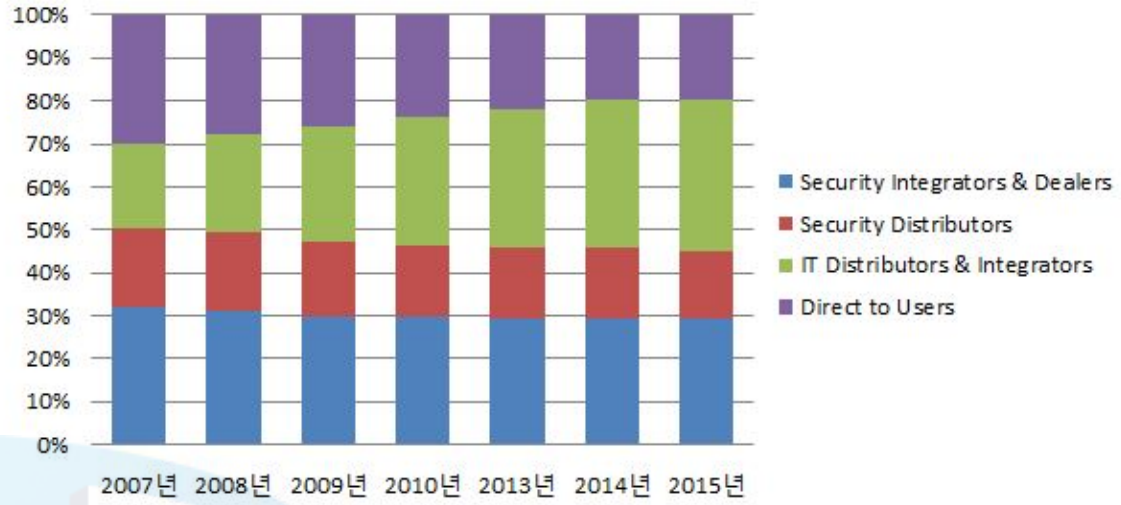
단위 : 억 원

구분		2007	2010	2012	2014	2018	CAGR
정보영역		7,431	12,724	15,401	17,541	29,145	13.05%
물리 영역	물리보안	14,924	16,247	18,069	23,281	42,814	10.12%
	물리+정보	2,922	9,616	18,910	32,149	64,222	31.60%
IT 융합보안		2,922	7,131	10,598	22,964	64,174	34.25%
융합 보안 소계		6,054	16,747	29,508	55,113	128,396	32.00%

※ 출처 : 해양수산개발원 “국가 물류보안체계 확립방안”, 시큐리티월드, KISA

J.P.Freeman이 발표한 융합보안 시장의 채널별 시장 점유율은 <그림 2>에서 알 수 있듯이 ICT 기업의 융합보안 시장 점유율이 점차 확대되고 있음을 알 수 있다. ICT 기업의 융합보안 시장 점유율이 2007년 19%에서 2015년 34%

로 증가하고, 사용자가 직접 구매하는 비중은 점차 감소할 것으로 예상하고 있다. 이렇게 융합보안 제품을 생산하는 벤처기업들이 직접 사용자에게 판매하는 형태를 떠나 점차 ICT 기업을 통한 구축이 증가하는 것은 융합보안 제품의 복잡도가 증가하기 때문으로 분석하고 있다.



<그림 3> 융합보안 시장의 채널 별 시장점유율

2.4.4 융합보안제품 구매 동기

김정덕(2009)는 융합보안 제품을 구매하는 동기를 살펴보면 물리보안과 정보보안 사이에 존재하는 보안 공백을 제거하기 위함이 가장 우선된다고 할 수 있다. 실제로 영국에 있는 일본은행인 스미토모 미쓰이 은행(Sumitomo Mitsui Bank)[12]의 경우 강력한 정보보안 기술을 이용한 보안체계를 구축하였음에도 불구하고, 해킹에 의한 도난 사건이 발행하여 약 220만 유로의 손실을 입게 되었다. 그 이유는 물리적 감시망을 피해 컴퓨터 키보드에서 로그 정보를 추출할 수 있는 장치를 설치하는 등 물리적 보안의 허점을 이용한 보안 사로를 방지하지 못한 이유가 컸었다. 이러한 물리적 보안 영역과 관리적/기술적

12) 2001년 4월 1일 스미토모 그룹의 스미토모 은행과 미쓰이 그룹의 사쿠라 은행이 합병해서 발족한 은행으로 서 본점은 도쿄 도 지요다 구에 있다.

보안 영역의 분리에 따른 보안사건/사고는 새로운 정보보호 이슈로 부각되고 있으며, 그 해결책으로 등장한 융합보안의 급격한 시장 성장이 예상된다. 이외의 융합보안 제품 구매 동기를 살펴보면 물리/IT 장비 전체 영역의 보안 이벤트를 통합하여 발생 가능한 위험을 사전 감지하고 신속 대응하기 위함이고, 보안인력 운영 효율화를 통해 보안 투자비용을 절감하기 위해서이다.

2.4.5 융합보안 시장 확대 배경

산업연구원(2014)은 융합보안 시장이 급속하게 성장하는 가장 큰 이유로는 사물인터넷(IoT)과 관련된 시장이 급속하게 성장하는 것 이외에도 스마트카, 스마트홈 등 생활에 직접적으로 연관된 기기에 대한 해킹으로 인한 다양한 피해 시나리오가 현실화될 가능성이 높다는데 있다. 국가의 핵심기반시설인 전력, 가스, 상하수도, 고속전철 등에 대해 날로 위험성이 커지는 해킹가능성이 제기되고 있다. 이러한 융합보안 피해는 이전의 정보보안보다도 피해액과 피해규모에서 월등한 차이를 보인다는 것이 지배적인 관점이다. 지금까지는 정보보안에서 문제가 일어났을 경우 실제 물리적 공간에까지 그 영향이 직접적으로 연관된 것은 아니었다. 하지만 이제는 실제 공간에까지 그 문제가 직접적으로 나타나 피해규모는 이전보다 더 커질 것으로 예상되고 있다. 구체적으로 제조업에서 보안사고가 발생한다면 제품의 신뢰성을 떨어뜨리고 해당제품에 대한 수요를 감소시킬 우려가 있다. 만일 스마트폰 또는 스마트카의 보안사고가 발생해, 국산 휴대폰의 국내 최종수요가 10% 감소한다면 연간 경제적 손실은 약 16조 원에 이를 것으로 추정된다는 보고도 있다. 그리고 국산 자동차의 경우 최종수요가 10% 감소한다면 약 24조 원 이상의 손실이 발생할 것으로 예상된다는 보고도 신중히 접할 필요가 있다. 그만큼 서비스 산업에서 보안사고가 발생한다면 해당 부문을 일정기간 서비스불가 상태로 만들고 간접적으로 다른 산업부문에도 영향을 미치게 되며 통신, 교통 또는 전력망 등의 인프라시설에서 발생한 융합보안 피해는 국가수준의 막대한 경제적 손실로 이어질 수 있다. 또한, 만일에 보안사고가 발생해 우리나라의 인터넷망에 1%의 작동불가 상태가 발생한다면 전 산업에 걸쳐 약 1조 4000억 원에 육박하는 생산차질이 발생할 것으로 추산된다. 이것은 반대로 1조

4000억 원 이하의 보안시스템에 대한 투자가 국가통신망의 안정성을 1% 높일 수 있다면 그에 대한 충분한 투자가치가 있음을 시사한 것으로 해석해볼 수 있다.

2.4.6 융합보안산업 선점을 위한 과제

산업연구원(2014) 융합보안산업은 산업 내에서 통용되는 표준기술의 선점이 중요하므로 국제표준을 선도하기 위한 방안을 마련해야 한다. 스마트카, 스마트그리드, U-헬스케어 등 IT융합 신산업 분야의 기반이 되는 보안기술에 대해 국제기구나 해외업체들은 다양한 표준수립활동을 하고 있으나 국내의 경우 일부 분야에서는 표준이 마련되어 있지 않고 정해진 국제표준을 따라가는 상황으로 국제표준 제정에 적극적으로 참여하려는 노력이 필요하다. 아직 기술개발 초기 및 표준화 단계이므로 융합사업별로 표준화 논의가 전개되고 있어 다양한 사업 기회가 존재한다. 현재 세계시장은 미국과 유럽 위주의 판도이지만 신흥시장의 성장잠재력 또한 높아지고 있다.

한국인터넷진흥원의 조사에 따르면, 현재 미국과 유럽이 세계시장의 약 90%를 점유하고 있고 시만텍, 시스코, 오라클 등의 글로벌 기업이 보안 산업을 주도하고 있는 것으로 나타났다. 하지만 향후 아시아 및 남아메리카의 비중이 상당히 증가할 것으로 예상되어 지고 있다.

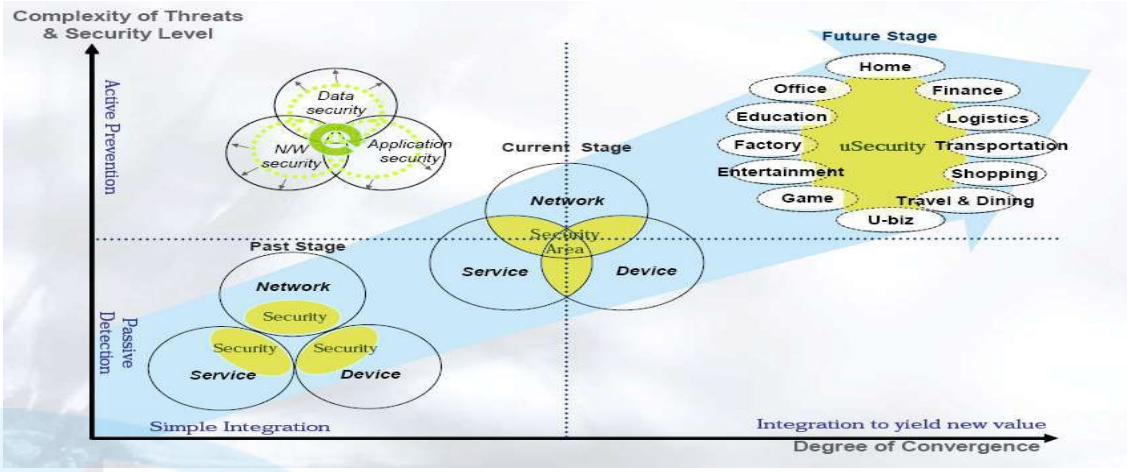
2.5 융합 보안관제시스템 기술 이론

2.5.1 융합보안 기술이론 정의

한국전자통신연구원(2015)는 융합보안 기술을 기술간 융합, 산업간 융합시 발생되는 보안취약성을 해결하는 보안기술로서 융합제품에 대한 신뢰성을 제공하여 제품 경쟁력 강화에 기여할 수 있는 기술로 정의하였다.

이글루시큐리티(2015)에서는 융합보안 기술 이론 레벨을 살펴보면 과거의 보안에 대한 개념은 네트워크보안, 정보보안, 물리적 보안, 각종 서비스 분야에 있어

서 일정한 보안·이 필요하다고 인지하는 수준이었다. 현재에 와서 이러한 분야별 보안이슈들을 통일시키는 융합형태의 보안이 정립되기 시작하였고 비로소 융합보안이라는 개념이 탄생하게 되었다. 향후 다가올 미래에는 보안이라는 관점은 예상보다 급속도로 커져서 산업 전 분야에 걸쳐서 보안이 중심이 되어야만 시스템이 구현되는 레벨이 이르게 될 것으로 전망하고 있다.



<그림 4> 융합보안 기술이론 LEVEL

2.5.2 융합보안 기술 패러다임

한국전자통신연구원(2014)은 IT기술과의 융합에 따른 네트워크 연결로 인해 기존의 해킹기술들이 융합제품에 대한 공격으로 패턴이 변화되면서 새로운 보안취약성이 발생하게 되었다. 이러한 공격패턴의 변화는 융합제품 사용자의 중요한 정보가 유출되어 개인정보보호가 노출될 가능성이 높아짐으로 인해 프라이버시 보장기술의 고도화가 이루어 져야 한다. 특히 이러한 공격패턴이 자동차, 조선, 항공분야 등 운송 분야와 의료분야 및 건설 분야에 가해진다면 우리는 경재적 피해는 물론 생명의 위협까지 느끼게 되므로 보안기술의 고도화는 우선과제가 될 수 밖에 없다. 이러한 환경적 요인으로인해 융합보안기술 패러다임은 각각 서비스 특성에 맞게 IT보안기술과 물리적 보안기술이 복합적인 요소로 활용되어 발전되어갈 것으로 예상하고 있다.

기본적으로 융합보안 기술 패러다임의 변화는 논리공간중심에서 논리공간과 물리공간의 연계 중심으로 바뀌고 있으며, 인터넷 중심의 보안영역에서 실제 현실속

공간에서의 안전으로 변화하고 있다. 정보보호 제품군들도 개별 환경에서의 정보보호에서 융합 환경에서의 정보보호 개념으로 바뀌었다. 또한 기존에 S/W 중심형 보안제품들도 S/W 와 H/W를 접목시킨 다양한 보안제품으로 변하게 되었다.

<그림 5> 융합보안기술 패러다임 변화

이처럼 다양한 분야에서 융합보안 기술은 발전방향을 논하고 있지만 종합적인 관점으로 살펴보면 논리적 중심의 개별 보안에서 물리공간을 포함한 실제 생활 공간의 안전을 통해 생명과 재산을 보호하는 형태의 기술로 발전하였음을 알 수 있다. 나아가 융합보안기술은 지식정보보안산업으로의 확대를 통해 암호, 인증, 인식, 감시 등의 보안기술이 적용된 제품을 생산하거나 관련 보안기술을 활용하여 재난, 재해, 범죄 등을 방지하는 서비스를 제공하는 산업으로 발전할 수 있는 가능성을 보이고 있음을 알 수 있었다.

2.5.3 융합보안 기술 범위

정보통신산업진흥법은 융합보안 기술을 암호, 인증, 인식, 감시 등의 보안기술이 적용된 제품을 생산하거나, 관련 보안기술을 활용하여 재난·재해·범죄 등을 방지하는 서비스를 제공하는 기술로 정의하고 있다.

이현도(2012)는 물리보안과 정보보안, 그리고 융합보안의 주요 항목별 적용

기술을 <표 5>와 같이 기술하였다.

<표 5> 융합보안 기술 범위

구분	항목	적용 기술	비고
물리보안	감시관제	무인감시, 무인경계, 치안방범, 교통통제, 환경감시, 재난재해 관제 등	
	무인전자보안	RFID, 출입통제, 스마트카드, 보안센터, 검색기기 등	
	영상보안	CCTV, 지능형 영상인식, 비디오분석, 지능형 카메라 등	
	바이오인식	홍채인식, 지문인식, 안면인식, 정맥인식, 휴먼추적 등	
정보보안	네트워크 침입	방화벽, IDS, IPS, VPN, UTM, DDos, NAC, 클라우드컴퓨팅, Vmware 보안 등	
	악성코드 대응	안티 웜바이러스, 스파이웨어, 스팸메일, 피싱, 악성봇 대응, 악성코드 자동분석 등	
	보안운영체제	커널 취약점 분석, 시스템 접근제어, 응용프로그램 버그	
	디지털 포렌식	디지털 증거 검색, 분석, 복구, e-Discovery 등	
	보안전용 칩	스마트카드, USIM, 보안토큰 등	
	접속 보안	BcN 보안, 무선랜보안, 무선단말 보안, WiBro 보안, 이동통신 보안, IPv6보안, 미래인터넷 보안 등	
	보안관리	위험관리, 취약성 분석, 보안성 평가, 보안 시각화 등	
융합보안	지능형 차량보안	차량 브랙박스, 차량통신 보안, 차량센서 보안, 차량통합보안관리 등	
	u-헬스케어 보안	의료정보 접근제어, 의료정보 공유 등	
	금융보안	금융피싱 방지, 인터넷뱅킹 보안, 온라인증권 보안 등	
	로봇보안	네트워크로봇 보안, 로봇간 통신 보안 등	
	스마트그리드 보안	AMI 암호, 인증, 프라이버시보소, AMI 인터페이스 보안, 전력망 침입탐지, 차단 등	
	주력산업보안	건설, 국방, 조선 산업보안 등	

특허청(2014)은 세계 IT보안 기술의 트렌드가 '통신상의 정보보호'에서 '개인 및 사회 안전'으로 빠르게 진화하면서 유비쿼터스 사회 진입에 따라 정보보안의 개념이 컴퓨터 및 네트워크 수준의 보안을 넘어 사회 전반의 보안으로 확장되고 있다고 하였다. 보안 기술의 영역이 단순 정보보안에서 물리보안 및 융합보안 분야로 급속히 확대하면서 지식정보보안 산업이 출현하게 되었다. 이에 따라 기존의 정보보호산업에 융합 패러다임을 반영하여 '지식정보보안산업'으로의 확대가 되었으며, 재편 및 이를 뒷받침하고 견인할 수 있는 기술개발의 필요성과 수요가 급증하게 되었다.

융합보안 기술 범위는 적용영역과 업종의 특성에 따라 정보보안, 물리보안 및 융합보안으로 구성되며, 금융, 유통, 건설, 의료, 국방 등 모든 산업의 신

뢰성과 안전성의 강화를 위하여 지식정보보안 기술이 융합되어 지속적인 경제발전을 견인하고 국민의 편안하고 안전한 삶을 보장하는 방향으로 발전하고 있음을 알 수 있었다.

2.5.4 융합 보안관제시스템 프레임워크

삼성SDS 컨설팅사업부(2013)는 융합 보안관제시스템이 End-Point에서 발생하는 다양한 이벤트를 수집하여 개별 이벤트 정보에 대한 분석 및 개별 모니터링을 지원해야 할 뿐만 아니라 수집된 이벤트의 상관관계를 분석하고 정해진 보안 규칙에 따라 적절한 보안 조치를 취할 수 있도록 기능을 제공해야 한다고 하였다. 이러한 기능을 제공하기 위해 융합보안관제 시스템이 갖추어야 할 구성을 이벤트 정보의 흐름에 따라 단계적으로 살펴보면 다섯 개의 영역으로 구분할 수 있다.

첫 번째, 융합 인터페이스 부분이다. 융합 인터페이스부는 기존에 물리, 보안, IT인프라 등으로 구분되었던 관제 대상 영역에 존재하는 다양한 종류의 보안단말(침입탐지시스템, CCTV, IC카드리더, NMS 등)이 갖는 제조사별 상이한 전송 프로토콜을 지원하며, 실시간 또는 유사 시간으로 원시형태의 보안 이벤트 수집과 PTZ 카메라 제어, 보안 정책 배포 등과 같은 보안단말 제어를 위한 프로토콜을 지원한다. 보안이벤트 로그 수집 모듈을 인프라 관제, 시설관제, 보안관제로 모듈화 하여 적용대상 사이트의 관제 범위에 따라 차별적용이 가능해야 한다.

두 번째, 관제관리는 보안단말에서 수집한 이벤트(영상, 로그든)로부터 다양한 방식의 보안패턴 분석, 이벤트 상호간의 상관관계 분석을 통해 의미 있는 정보를 획득하는 상황분석 모듈과 이벤트 원천 데이터와 분석결과 데이터의 저장, 검색, 상황처리 및 디바이스 제어 등을 담당하는 관제 지원모듈로 구성된다.

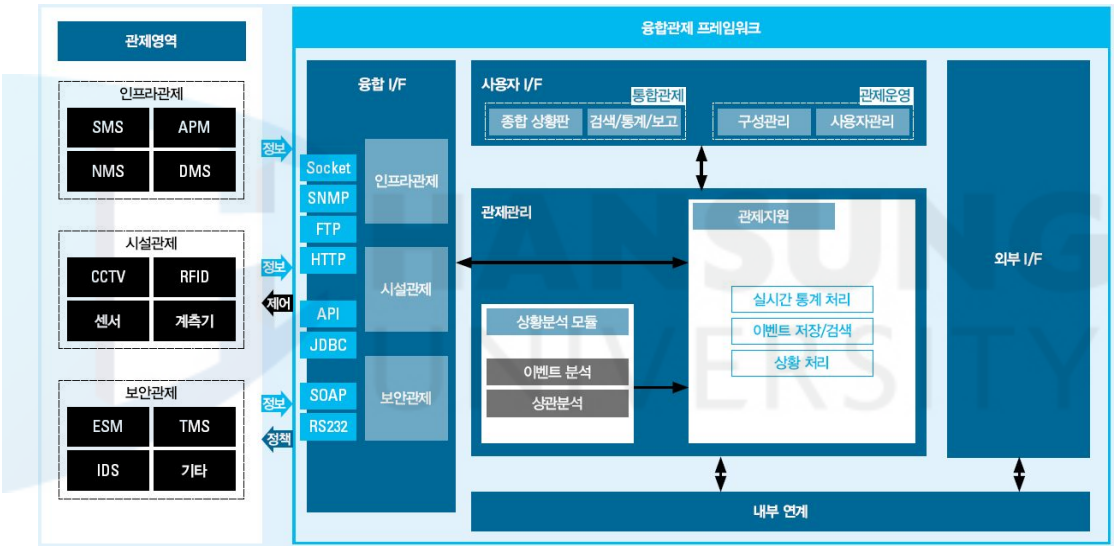
세 번째, 내부연계는 보안이벤트가 발생하면 동기방식으로 메시지를 처리할 수 있도록 융합보안관제 시스템 구성요소간 메시지의 흐름을 제어하는 역할을 담당하게 된다. 이러한 동기식 처리는 보안사고 처리 프로세스와 같이 조직에서 규정하고 있는 업무 프로세스에 따라 이벤트를 처리할 수 있도록 해준다. 이를 위

해 메시지 관리, 메시지 라우팅, 트랜잭션 처리 등의 기능이 구현되어야 한다.

네 번째, 사용자 인터페이스는 종합상황판를 통해 각종 장애, 상황, 정책 등을 관리하는 통합 관제와 관제 대상 보안단말의 구성, 관제 사용자 권한관리, 상황실 운영관리 등 관제운영으로 구성된다.

다섯 번째, 외부 인터페이스는 프로토콜 및 메시지 변환을 통해 E-mail, Mobile 뿐만 아니라 기업 정보시스템 등과의 시스템 연계를 수행한다.

삼성SDS가 제시하는 융합보안관제 시스템의 Framework는 <그림 6>과 같으며 융합 보안관제 기술 동향에서 제시하고 있는 다섯 가지 구성 요소 중 모듈화 설계, 분석데이터 표준화 및 클라우드 컴퓨팅 기술 접목, Rule Based 관제 모델 기반 제공 등을 포함하고 있다.



<그림 6> 융합 보안관제시스템 프레임워크

2.5.5 모듈화 설계

김민수(2012)는 융합보안관제 대상 별 관제 영역이 인프라 관제, 시설관제, 보안관제 등으로 상이 또는 통합될 수 있으므로 환경에 따라 관제 형태별 구성이 가능하도록 모듈 설계되었다. 또한 인터페이스 연동방식 및 컴포넌트 별로 유닛을 쉽게 추가·변경할 수 있도록 플러그인 형태로 설계되어 시스템의

확장성과 유연성이 향상되었다고 하였다. 기본적으로 IT인프라 관제 + 보안 관제, 보안 관제 + 시설관제, 시설 관제 유닛들의 선택적 통합이라고 표현할 수 있다. 그리고 IT인프라, 시설, 보안 시스템 등에서 발생한 이벤트는 Socket, SNMP, FTP, HTTP, API, JDBC, SOAP, RS232 등의 표준화된 프로토콜로 각 모듈에 제공 된다. 인프라 관제 모듈은 관제 데이터 처리를 위한 컴포넌트로 구성되며, 시설 관제 모듈은 시설물 데이터 처리를 위한 컴포넌트와 디바이스제어를 위한 컴포넌트로 구성된다. 데이터 처리 컴포넌트에는 행동분석, 얼굴인식, LRP 등의 유닛이, 디바이스 제어 컴포넌트에는 PTZ, 음향제어, 밸브제어 등의 유닛이 플러그인 형태도 제공된다. 보안관제 모듈은 보안 장비 데이터 처리를 위한 컴포넌트와 정책 분배를 위한 컴포넌트로 구성된다고 하였다.

2.5.6 분석 데이터 표준화 및 클라우드 컴퓨팅 기술 접목

김민수(2012)는 다양한 관제 대상 정보의 체계적인 분석과 이 기종간 정보의 연계 분석 및 검색 지원을 위해 분석 데이터 표준이 수립이 필요하다고 하였다. 분석 데이터는 XML 기반의 표준에 맡게 작성되어 타 모듈간 연계 분석을 지원하며 CCTV영상, 음성 등과 같은 관제 원본데이터와 영상분석정보, LRP 등의 분석 데이터는 분리 보관되어 사용자가 원하는 정보를 신속하게 검색할 수 있도록 지원한다. 관제 데이터의 양, 복잡도, 관제소의 수가 증가함에 따라 소규모 단위의 클라우드 컴퓨팅 기술을 활용하여 개인, 사무실 단위의 효율적 관리와 지역단위 관제 센터의 통합이 가능해졌다. 각 지역의 관제소는 개별 시스템을 구축하여 운영하며, 각 지역 관제소의 상황을 중앙 관제소에서 통합 관리/검색 하는 서비스가 가능해진다. 현재 경찰청과 도로공사에서 이와 같은 통합 관제센터를 운영 중에 있다.

2.5.7 Rule Based 관제 모델

임명성(2014)는 물리와 IT의 연계 데이터 분석 방안 및 통계 분석 모델을

수립하고, 기존 Infra 및 IT보안관제 중심으로 수립된 관제모델을 통합적 관제 관점으로 재구성함으로써 Rule Based 기능을 활용한 통합 관제 프로세스의 자동화가 이루어진다. 물리와 IT관제 데이터의 상관관계 및 Rule Base의 Trigger를 정의함으로써 기존에 간과되었던 정보들을 활용한 새로운 징후 파악이 가능해졌으며, 뿐만 아니라 Rule Based 자동화 관제가 가능해져 실시간 장애 위치, 상태 파악을 통한 조기 조치 및 장애 예방이 가능해졌다고 하였다.

2.6 선행연구 검토 및 본 연구 차별성

현재까지 진행되고 있는 융합 보안관제시스템의 활성화 방안에 대한 연구는 크게 정보보안관제의 기술적 부분의 개선방안과 물리보안관제의 환경개선 분야에 대한 전략에 대한 연구로 구분 할 수 있다. 이에 본 연구에서는 선행논문으로 정보보안과 물리보안을 접목시킨 융합 보안관제시스템의 활성화 방안을 위해 '시큐리티 환경변화에 따른 융합보안의 대두와 물리보안업체의 대응 (안황권, 2011)', '융합보안을 연계한 기계경비산업 발전방안에 관한 연구 (최인호, 2014)', '융합보안관제시스템 개선에 관한 연구 (이동휘, 2011)' 를 검토하였다. 그리고 아직은 제도화 되지 못한 융합 보안관제시스템 관련 정책연구를 위해 '개인정보보호기술의 최신 동향과 향후 전망 (남기효, 2014)', '산업보안의 개념적 정의에 관한 고찰 (이창무, 2011)', '산업보안을 위한 융합보안관제시스템에 관한 연구 (하옥현, 2009)', '융합보안 강화를 위한 정보보안 정책 효과성 측정도구 개발 (임명성, 2014)', '보안환경변화에 따른 융합보안 발전방향 (김민수, 2012)', '융합보안시장 동향 보고 (최진묵, 2010)' 를 검토하였으며, 이를 통해 새로운 활성화 전략을 수립할 수 있었다. 또한, 공공기관과 일반기업, 외국계열회사 등의 구축사례를 검토한 후 관련 업계 동향을 살펴보았다. '기밀유출방지를 위한 융합보안 관제 체계 (이창훈, 2010)', '내부정보유출방지 관점에서의 보안수준 평가 (장항배, 2009)', '내부정보 유출 징후 분석을 통한 유출방지체계 구축에 관한 연구 (이기혁, 2009)' 검토를 통해

융합 보안관제시스템의 취약점을 분석하고 근본적인 대책마련이 필요하다는 시사점을 도출하였다. 본 연구는 향후 국가산업발전에 크게 기여할 융합보안관제 산업의 활성화 방안에 있어서 관련 산업 종사자 및 공공기관 관리자와의 인터뷰 및 설문조사를 통해 지금까지 구체적으로 제시하지 못했던 융합보안관제시스템 구축시 우선 고려해야할 사항과 향후 발전방향을 제시하고자 한다.

Ⅲ. 융합 보안관제시스템 구축 동향

3.1 융합보안 정책

3.1.1 국외 융합보안 정책

우광제(2015)는 선진국들은 이미 융합보안을 포함한 지식정보보안 관련 규제와 지원을 추진 중에 있으며, 지식정보보안 관련 규제와 지원을 위한 통합적인 조직체계를 갖추어 왔다. 우선 미국은 국토안보부법에 의거 설립된 국가안보부에서 민·관·군을 구별하여 기관별로 임무를 분담하지 않고 통합적으로 운영하고 있다고 하였다. 그리고 EU는 집행위원회의 정보사회 미디어국과 유럽네트워크 정보보안청이 사이버 보안과 관련한 역할을 주도적으로 수행하고 있으며, 일본은 정보보안 정책의 기본 전략을 결정하는 '정보보안 정책 회의'를 정례화하고 그 수행 기관으로 내각관방 정보보안센터(NISC)를 설치하여 정보보안 정책을 총괄하는 임무를 부여하고 있다. 이처럼 세계 각국은 지식정보보안산업을 육성하기 위해 전략적 투자를 추진하고 있으며 특히 정보보호 인력양성을 위해 체계적인 지원을 하고 있다.

미국은 사이버보안진흥법(Cyber Security enhancement Act)을 기반으로 지식정보보안산업 육성을 위해 전략적 투자를 추진하고 있고 정보보호 인력 양성을 위해 다양한 대학 교육 지원 프로그램을 운영하고 있다.

EU는 공동 연구개발정책인 7차 프레임워크 프로그램(7th Framework Programme)에서 지식정보보안 분야에 약 9,000만 유로의 예산을 투입할 정도이다.

일본은 2010년 '국민을 지키는 정보보안 전략'을 발표하고 '정보보안 정책회의' 를 통해 국가 정보보안 관련 전략 수립하였다. 2012년 6월 회의에서 정보보안로드맵을 작성하여 4대 전략 분야와 12대 과제에 대한 구체적인 목표와 시기를 명시하였으며 2013년 3월 회의에서 민·관 통일적·상호보완적인 정보보안 정책 추진을 주 내용으로 하는 아베 정부의 '새로운 정보보안 전략'

을 수립하여 법제화 하였다.

3.1.2 국내 융합보안 정책

국내는 지식정보보안 총괄기관이 없고 정부의 지속적인 지원 역시 부족한 실정이다. 특히, 국내의 정보보안 분야 관리·감독 체계는 분야별로 분산되어 있어 국가 수준의 복합적 보안사고 발생 시 기관 간의 정책 혼선이 우려될 수준이다. 사이버 보안을 위해 국가·공공 분야는 국가정보원의 국가사이버안전센터, 민간 분야는 방송통신위원회의 한국인터넷진흥원 인터넷침해사고대응센터, 국방 분야는 국군사이버사령부에서 각각 분야별 임무를 분담하고 있다. 국가적인 중요 사이버사고 발생 시에는 국가정보원, 국방부, 미래부 등 범정부 차원에서 '민·관·군 합동대응팀'을 임시 소집하여 후속 조사를 하고 있으며 그 외의 사고에는 '민·관 합동조사단'이 활동하는 것을 원칙으로 하나 원활히 운영되고 있지 않는 실정이다.

정부는 지식정보보안과 관련된 산업진흥정책을 마련하고 있으나 지속적인 투자가 이루어지지 못하고 사이버사고 발생 후의 일시적인 수준에 그치고 있는 안타까운 실정이다. 그리고 산업자원부에서 '지식정보보안산업 진흥 종합계획 Securing Knowledge Korea 2013 (2008~2013)'을 추진하였고, 이를 보완하여 미래창조과학부에서 '정보보호산업 발전 종합대책(2013~2017)'을 발표하였으며 정보보호산업진흥법(안)을 추진 중에 있다. 한편, 정보보안분야 예산은 2009년 7.7 DDoS 사이버 공격으로 IT 전체 예산의 8.2%로 상승하였다가 국민적 관심이 떨어지면서 2011년에는 6.2%로 감소, 이후 사이버사고를 겪으면서 2012년에 IT 예산의 8.1%까지 다시 상승했으며, 2014년 까지 꾸준한 상승세를 보이고 있다.

또한 관련학회인 한국인터넷진흥원과 한국융합보안학회 에서는 꾸준한 컨퍼런스 개최를 통해 국내 최고의 보안기술 전문가와 IT법·정책 전문가들을 학회에 참여시키고 있으며, 관계부서에 관심을 촉구하는 활동을 지속적으로 하고 있다.

현행 보안적합성 검증(CC 인증), 정보보호 관리체계(ISMS) 인증, 개인정보

보호 관리체계(PIMS) 인증 등이 있으나 세부검증 사항에서 융합보안 분야에 대한 보완이 필요하며, IT산업 전체의 육성에 초점을 맞춘 법령인 '정보통신 진흥 및 융합 활성화에 대한 특별법'과 '정보통신산업 진흥법'이 있으나 정보보안 분야를 강화하는 방향으로 개정이 요하며 현재 추진 중인 '정보보호산업 진흥법(안)'의 제정이 시급한 실정이다.

물론 '정보통신 진흥 및 융합 활성화에 관한 특별법'의 기본계획에 이러한 정보보안에 관한 사항이 언급되어 있지만, 3년 단위로 계획이 수립되므로 융합보안 정책체계 확립에는 한계가 있을 수밖에 없다.

또한, '정보통신산업 진흥법' 중에 '지식정보보안산업의 육성'이 있지만, 이또한 정보보안 분야에만 치중되어 있어서 융합보안에 대한 고려가 미흡함을 알 수 있다. 결론적으로 산업별 · 제품별 보안인증제도, 보안 사고에 대한 보상 및 보험 관련 규정, 국가 핵심 기반시설에 대한 보안규정 강화 등 융합보안 관련 법률 마련이 시급히 필요한 시점이라고 판단되어 진다.

미래부(2015)는 융합보안 정책이 이토록 미흡한 이유로 가장 설득력 있는 말로는 산업형성 초기이다 보니 현재 구축되어 운영 중인 융합보안관련 시스템들이 적절하게 구축되어 있는지에 대한 의문에서 시작되었다고 하였다. 그래서 미래부는 산 · 학 · 연 보안전문가로 구성된 '융합보안 코디네이터'를 두어, 과제의 기획, 수행, 종료까지 전 단계에 걸쳐 자문 및 검증을 받을 수 있도록 할 예정이라고 하니 좀 늦었지만 어느 정도 효과를 거둘 수 있기를 희망할 수 있게 되었다.

3.2 융합 보안관제시스템 구축 사례

3.2.1 A 공사

A공사는 방대한 시스템 운영에 있어 위험에 대한 체계적이고 적절한 대처의 필요성이 대두됨에 따라 융합 보안관제시스템을 도입하였다. 본사 외에도 지방에 본부와 연구소가 있는 A공사의 관리서버에 구축하고 데이터서버에 저장된 데이터베이스를 활용하여 건물 내·외부에 위치한 보안 대상물과 보안 시스템 등의 정확한 위치와 상태를 한 번에 표시하여 관리할 수 있도록 하여 통합적으로 3D시각화를 통해 모니터링 할 수 있는 환경이 구축되었다.[13)]

<그림 7> A공사 융합 보안관제시스템 구축 사례

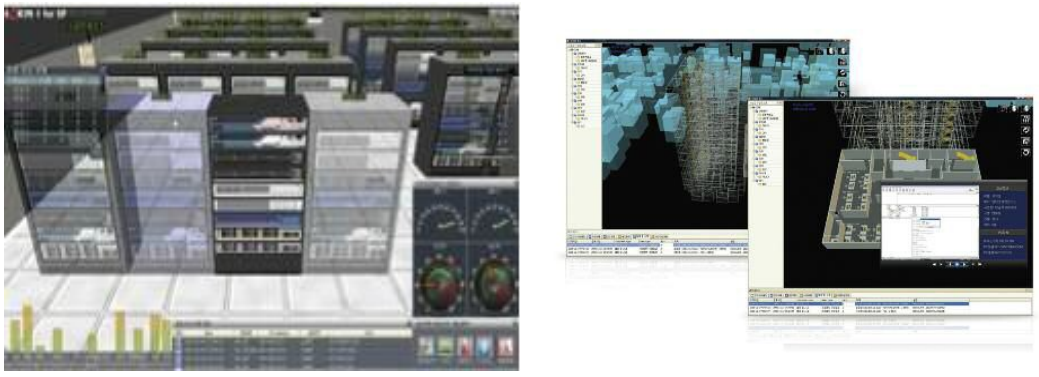
A공사의 정보통신 및 정보보안 관리자의 요구사항 수렴 후 반영한 결과물로 직관적인 관리GUI와 함께 통합적인 3D 시각화 모델로 외부 위험에 효율적 대처가 가능하게 되었다. 이렇게 관제시스템의 시각화된 3D통합공격분석시스템 모델은 시각화된 3D모델 설계방법' 기술로 건물 내·외부에 위치한 보안 대상물과 보안시스템의 정확한 위치와 상태를 3D입체영상으로 주시하고 관리할 수 있으며 간단한 적층, 선정 작업에 의해 건물 외곽 및 내부 3D단면도를 관리 (생성, 수정, 삭제, 복사) 할 수 있다. 또한 보안좌표만으로도 해당 보안좌표대상물의 위치와 종류를 식별할 수 있고 표시부에 즉각적으로 표시하여

13) 이글루시큐리티 융합보안연구소 (2015)

관제시스템의 시각화된 3D모델을 제공함으로써, 외부로부터 발생하는 보안위험을 효율적으로 관리할 수 있도록 해 주게 되었다. 이에 따라 관제시스템 관리 및 유지비용은 물론, 인력비용 감소 효과를 발생시켰다. 또한, A공사에 설치된 실사의 3D 전산실 조감도를 통해 보안 이벤트 발생 시에는 내부 조감도와 연계된 상황을 표출하여 장애 발생 탐지 및 장애 예측을 통한 신속한 대응이 가능하며 UPS, 항온 항습기, 온도, 습도, 누수, 화론 소화기 등과 연동되어 설비 장애 발생 시 현장 카메라로의 자동 연동으로 인한 지능적인 장애 대응 처리가 가능해지게 되었다. 결국 시스템 관리 및 유지비용 절감은 물론 물리보안, 시설물 관리를 통합관제 함으로써 보안관제의 인력비용이 감소되는 효과를 보였다.

3.2.2 B 건설

B건설은 실시간 분양시스템 운영 및 설계도 등 중요문서에 보안에 관심이 커짐에 따라 융합 보완관제시스템을 도입하였다. 전국 각지에 산재해 있는 건축물을 관리하고, 특허공법등에 대한 중요문건에 대한 보안 사고유출로 인해 보안관제에 대해 한 단계 강화된 관제시스템의 도입이 시급했었다. 이에 관리서버에서 각종 DB서버를 관리하며, 문서유출관리에도 보안을 강화함은 물론 서버룸 출입자에 대해서도 24시간 철저히 할 수 있게 되었다.[14)]



<그림 8> B건설 융합 보안관제시스템 구축 사례

14) 이글루시큐리티 융합보안연구소 (2015)

3.2.3 C 호텔

C호텔은 외국계 호텔로서 도심에 위치한 특성상 객실손님 외에도 로비나 식당, 카페에 방문하는 불특정 다수인원에 대한 감시 및 보안에 대한 고심이 커지자 융합 보안관제시시템을 도입하게 되었다. 각 층의 적재적소에 설치되어 있는 센서장치로부터 실시간으로 정보를 수집함으로서 적은 수의 관리인원으로도 넓은 건물 내부의 분산된 시설물에 대한 감시가 가능하게 되었다. 또한, 출입문 에서부터 각층에 산재해 있는 관계자출입장소에 대한 보안 강화를 통해 화재 및 각종 테러 위협으로부터 안전한 보안관리체계를 구축하게 되었다.[15)]

<그림 9> C호텔 융합 보안관제시스템 구축 사례

3.2.4 D문화재 관리소

최근 빈번하게 발생하는 국가 주요 문화재 손실 사고는 모든 국민에게 문화재 관리의 문제점을 인식하는 계기를 제공하였다. 우리나라의 국보 1호이자 상징이었던 숭례문이 하루아침에 전소되는 막대한 피해가 발행하지 않도록 주요 문화재에 대한 좀 더 과학적이고 체계적인 관리를 위한 방안이 대두되고 있다. 융합 보안관제시스템은 정보보안 뿐 아니라 시설물 감시를 동시에 할 수 있어 주요 문화재 관리를 위한 최적화된 커스트마이징을 통해 한 단계

15) 이글루시큐리티 융합보안연구소 (2015)

발전한 관리체계를 구축할 수 있었다.[16)]

<그림 10> D문화재 관리소 융합 보안관제시스템 구축 사례

즉, 문화재 내부와 외부에 다기능 파노라마 카메라, 회전형 카메라, 열화상 카메라, 화재감시 카메라, 출입구 카드 리더기 등을 설치하여 화재예방 및 외부인의 불법침입에 의한 문화재 도굴, 도난, 훼손을 예방하고 추가적인 사고에 대한 예측으로 세계적인 문화재 손실을 최소화 할 수 있도록 해 주는 것이다. 이렇게 수집된 모든 정보는 관리소 관제센터에 자동 통보되고 3D, E-MAP, 현장영상 및 장비 위치정보 등을 효과적으로 구성하여 입체적인 통합관제 기능을 구현하여 운영자 중심의 직관적인 화면을 구성하여 표출해 주고 있다. 또한 이상상황 발생 시, 이벤트 영상을 자동으로 확대 표출하고 자동으로 저장하며 현장에 1차 경광등을 이용한 경고, 2차 자동 경고방송 수행 및 센터 내 경광등, 스피커 등으로 상황을 전파하며, 3차로 라이브 경고방송, 유관기관 SMS통보 등을 통해 현장대응을 함으로써 위험상황에 대한 통합 관리가 가능하게 되었다.

3.2.5 E 생명보험

E 생명보험사는 본사 사옥건물에 대한 통합관리체계를 구축하기 위해 융합

16) 이글루시큐리티 융합보안연구소 (2015)

보안관제시스템을 도입하게 되었다. 기본적으로 원하던 관리방식인 출입통제, CCTV감시, 구역순찰관리, 엘리베이터 관리, 화재감시, 주차장감시 등의 기능 외에 조명등 자동제어시스템, 비상구 출입통제는 물론, 전력, 공조, 방재에 이르는 지능형 융합 보안관제시스템을 통해 적은 인력으로도 포괄적인 관리체계를 구축할 수 있게 되었다.[17)]

<그림 11> E생명보험 빌딩관리 융합 보안 관리시스템 구축

3.2.6 미 국방성

미군은 스마트카드 기반의 융합보안체계를 이미 구축완료 하였으며 현재까지 지속적인 발전방안을 추진하고 있다. 스마트카드로 개인식별을 통합 관리하는 시스템으로서 한 장의 카드로 출입, 네트워크 접근, 프린팅 등의 보안을 관리 통을 위한 표준지침 운영하고 있다.[18)]

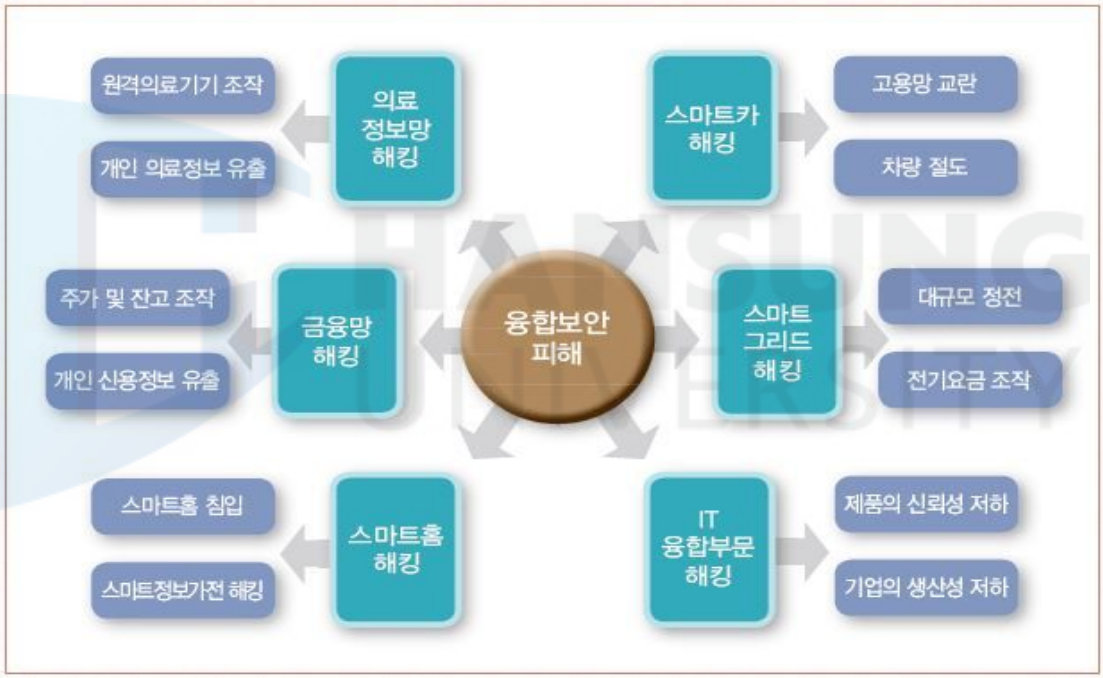
17) 이글루시큐리티 융합보안연구소 (2015)
18) 롯데정보통신 (2014)

<그림 12> HSPD (Homeland Security Presidential Directive)-12

3.3 융합보안 피해사고사례 및 문제점 분석

3.3.1 융합보안 피해 유형

산업연구원(2015)에서 발표한 융합보안산업은 최근 IT산업과 이종 산업의 융·복합화 경향에 따라 다양한 산업분야에 보안기능이 탑재되면서 시장수요가 급증할 것으로 전망되어지고 있다. 그 이유는 융합보안산업은 현재 산업발전 단계상 초기이고, 신흥국 시장의 수요가 점차 증가하고 있어 새로운 사업 기회를 제공할 여지가 충분하다고 판단하고 있다.



<그림 13> 융합보안피해 유형

허진(2014)은 사물인터넷(Internet of Things) 기술이 확산되면서 보안취약성도 증가할 수밖에 없는데 가장 큰 이유로 사물이 네트워크에 연결되는 사물인터넷 현상은 우리가 생각하는 것보다 훨씬 더 다양한 분야에 적용될 것으로 전망되고 있다. 시스코(Cisco)는 세계 사물인터넷 기기가 2013년 87억 개에서 2020년 500억 개로 늘어나고 2040년 이전에는 1억 5천만 개 까지 늘

어날 것으로 전망하고 있다. 그리고 자동차, 물류, 의료, 가전, 금융, 전력, 환경 등 다양한 분야에 적용되어 실시간 정보, 원격 제어, 빅데이터 분석 등의 서비스를 제공한다.

다양한 기기들이 인터넷을 통해 연결됨에 따라 보안 취약성에 대한 이슈가 제기되고 있는 중이며, 사물인터넷의 단말(센서, CCTV 등)은 패스워드 정도의 낮은 보안수준만 적용된 것이 대부분이기 때문에 해킹에 취약할 수밖에 없는 실정이다. 또한, 보안소프트웨어 기업 시만텍(Symantec)은 2014년 주목해야 할 보안시장 트렌드로 '사물인터넷의 보안 취약성 대두'를 언급하였다. 이는 가상의 사이버 환경이 물리적인 환경으로 확장되면서 다양한 형태의 보안 위협 대두될 수 있음을 경고하고 있다. 스마트카, u-헬스케어, 스마트홈 등 생활에 직접적으로 연관된 기기에 대한 해킹으로 인해 다양한 피해 시나리오가 현실화될 가능성이 있다. 그뿐만이 아니라, 국가의 SCADA (Supervisory Control and Data Acquisition) 시스템을 통해 관리하고 있는 핵심기반시설인 전력, 가스, 상하수도, 고속전철 등에 대한 해킹 가능성도 제기되고 있을 정도이다. 그리고 전산망을 해킹해 취득한 접속 권한으로 개인정보 유출, 악의적 기기 제어, 인프라 시스템 마비 등의 이차적인 피해범위가 물리 공간으로 확대되면서 경제적 피해규모는 대폭 증가할 것으로 예상되고 있다. 현재, 융합보안 관련 해킹 가능성에 대한 연구가 보안관련 연구소를 중심으로 이루어지고 있으며 실제 다양한 피해 사례가 보고되고 있는 중이다. 가장 큰 피해사례로는 IT융합 정도가 높고 사물인터넷의 활용도가 높은 스마트카, 스마트그리드, 의료정보망, 스마트홈에 대한 해킹 시연을 하거나 사고사례가 보고되고 있다.

2013년 노턴 보고서(Norton Cybercrime Report 2013)[19]에 따르면 전 세계 사이버 범죄 피해 규모가 연간 1,130억 달러에 달했으며 매일 100만 명 이상이 사이버 범죄 피해를 입은 것으로 발표 하였다.

국내에서는 정부·기업의 홈페이지와 금융 통신망에 대한 공격이 증가하고 있으며 정보보안의 실제 피해 빈도와 규모가 확대되고 있다. 2003년 1·25 인터

19) 전세계 1위의 정보보안 전문기업으로서 1982년 게리헨드릭스가 국립과학재단의 보조금으로 서립한 회사이다. 부설 보안연구소에서 발표한 보고서이다. (www.symantec.co.kr)

넷 대란(1,600억 원)을 시작으로 2009년 7.7 DDos 공격(363~544억 원), 2011년 4월 농협 전산망마비(150억~200억 원), 2013년 3·20 전산 대란, 6.25 사이버 공격(8,823억 원) 등 대규모 통신망에 대한 사이버 공격이 증가하고 있음을 알 수 있다.

아직까지는 융합보안 피해 사례가 많지 않기 때문에 경제적인 피해규모 측정에는 어려움이 있으나 기존의 보안 피해규모보다 월등히 증가할 것으로 예상되고 있다. 아직까지 융합보안 사고가 실제 경제적인 피해로 이어진 경우는 많지 않으나 향후 발생 시 기존의 정보보안 피해보다 광범위한 피해가 발생하고 피해규모 역시 증가할 것으로 전망되어 진다.

3.3.2 융합보안 피해 규모 및 파급효과

국가정보원(2015)발표한 국내 융합보안 피해는 GDP 규모 및 인터넷 보급률을 기초로 대략적으로 추정하였을 때 2015년 13조 4,000억 원, 2020년 17조 7,000억 원, 2030년 26조 7,000억 원 예상되며 국가 신용도 하락, 2차 피해 등을 고려한다면 더욱 증가할 것으로 예상하고 있다.

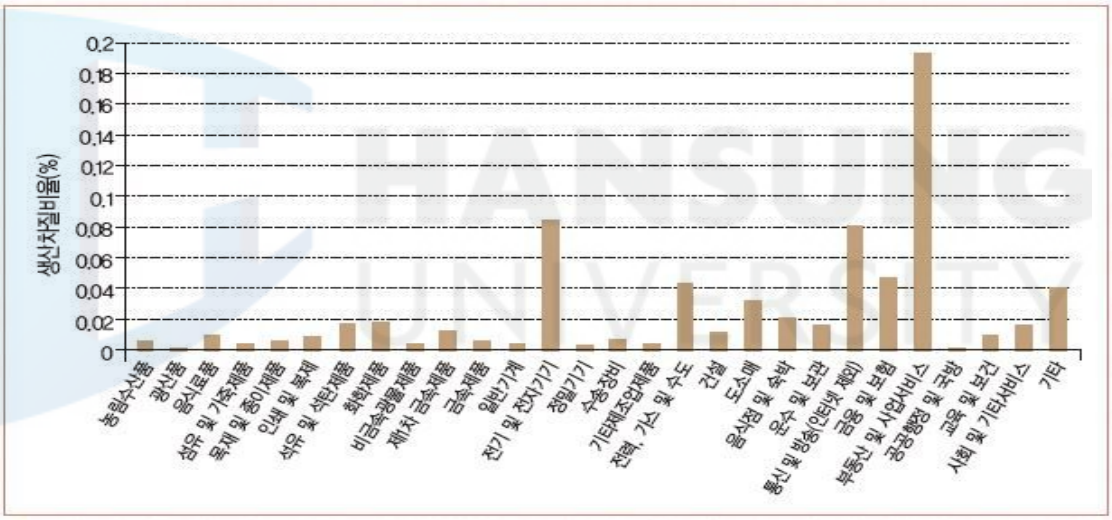
산업연구원(2014)는 실제로 융합보안 피해사고의 파급효과로는 산업전반에 걸쳐 그 파장이 크다는 것을 생산차질비율(Inoperability)을 통해 알 수 있다. 우선 제조업에서 보안사고가 발생한다면 제품의 신뢰성을 떨어뜨리고 해당 제품에 대한 수요를 감소시킬 우려가 있다. 만일, <그림 14>을 참고로 스마트폰 또는 스마트카의 보안사고가 발생하여 국산 휴대폰의 국내 최종수요가 10% 감소한다면 연간 경제적 손실은 약 16조원에 이를 것으로 추정되며, 국산 자동차의 경우 최종수요가 10% 감소한다면 약 24조원 이상의 손실 발생할 것으로 예상된다. 서비스산업에서 보안사고가 발생한다면 해당 부문을 일정 기간 서비스불가(inoperability) 상태로 만들고 간접적으로 다른 산업 부문에도 영향을 미치게 된다고 하였다.

만일, 금융기관에 대한 보안 공격으로 인해 금융 산업에서 1%의 지장을 받게 된다면 금융 산업 자체에 1조 7,000억 원 피해가 예상되며, 전 산업에 걸쳐 간접적으로 6,000억 원 경제적 손실이 발생할 것으로 추정하고 있다. 그리

고 통신, 교통 또는 전력망 등의 인프라시설에서 발생한 융합보안 피해는 국가수준의 막대한 경제적 손실로 이어질 수 있음을 알 수 있다.

그리고 보안사고가 발생하여 우리나라의 인터넷망에 1%의 작동불가 상태가 발생한다면 전 산업에 걸쳐 약 1조 4,000억 원에 육박하는 생산차질이 발생할 것으로 추산되고 있다. 이것은 반대로 1조 4,000억 원 이하의 보안시스템에 대한 투자가 국가 통신망의 안정성을 1% 높일 수 있다면 그에 대한 충분한 투자가치가 있음을 시사한다. 인터넷이 마비될 경우, 생산차질비율 관점에서 보면, '부동산 및 사업서비스' 부문의 생산차질이 가장 클 것으로 추정하고 있다.

손해비용 관점으로 보면, '전기 및 전자기기' 부문에서 약 3,000억 원에 이르는 가장 큰 경제적 손실 발생할 것으로 예상된다고 한다.



<그림 14> 인터넷 마비로 인한 산업별 생산차질비율

갈수록 정보유출이 두려운 세상이 다가오고 있다고 한다. 새로운 기술이 등장함에 따라 개인 및 조직의 정보자산에 대한 위협 역시 다양해지고 있는 현실이다. 최근 자주 일어나는 개인정보 유출 등의 사건/사고에 따른 피해규모는 조직의 존폐와 개인의 인권까지 영향을 줄 만큼 증가하고 있는 현실이다.

3.3.3 보안 피해사고사례 및 문제점 분석

3.3.3.1 국외 피해사고사례

3.3.3.1.1 스미토모 미쓰이 은행 해킹 사건

영국에 있는 일본은행인 스미토모 미쓰이 은행[20](Sumitomo Mitsui Bank)의 경우 강력한 정보보안 기술을 이용한 보안체계를 구축하였음에도 불구하고, 해킹에 의한 도난 사건이 발행하여 약 220만 유로의 손실을 입게 되었다c. 그 이유는 물리적 감시망을 피해 컴퓨터 키보드에서 로그 정보를 추출할 수 있는 장치를 설치하는 등 물리적 보안의 허점을 이용한 보안 사로를 방지하지 못한 이유가 컸었다. 이러한 물리적 보안 영역과 관리적/ 기술적 보안 영역의 분리에 따른 보안사건/ 사고는 새로운 정보보호 이슈로 부각되고 있으며, 그 해결책으로 등장한 융합보안의 급격한 시장 성장이 예상된다. 이외의 융합보안 제품 구매 동기를 살펴보면 물리/IT 장비 전체 영역의 보안 이벤트를 통합하여 발생 가능한 위험을 사전 감지하고 신속 대응하기 위함이고, 보안인력 운영 효율화를 통해 보안 투자비용을 절감하기 위해서이다. (위키 백과, 검색일 2015. 5. 28)

3.3.3.1.2 소니픽처스 엔터테인먼트 해킹 사건

2014년 11월 24일에 발생한 소니 픽처스 엔터테인먼트[21]의 해킹 사건은 회사 관계자 간의 전자 메일, 직원의 개인 정보, 미공개 영화 본편의 복사 등 다양한 정보의 유출을 초래하였다. 유출된 전자 메일을 통해 소니 픽처스의 공동 회장 히라이 카즈오와 에이미 파스칼이 《디 인터뷰》에서 김정은 암살 장면을 "완화"하도록 지시하고 있었던 것이 밝혀졌다. 이메일 외에 2015년에

20) 2001년 4월 1일 스미토모 그룹의 스미토모 은행과 미쓰이 그룹의 사쿠라 은행이 합병해서 발족한 은행으로 서 본점은 도쿄 도 지요다 구에 있다.

21) 소니 픽처스 엔터테인먼트(Sony Pictures Entertainment, Inc., SPE)는 소니의 자화사인 미국의 다국적 기술 및 미디어 회사이며 텔레비전 및 영화 제작/배급 기업이다.

공개가 예정되어 있는 《007 스펙터》의 각본의 사본이 유출되었다. 해커 집단은 《디 인터뷰》 미국 공개 일인 2014년 12월 25일에 새로운 정보를 공개한다고 예고하였다. 《디 인터뷰》를 한 때 공개를 취소했었으나 12월 25일 미국전역 개봉 및 인터넷 유료결재로 공개하였다. 한편, 2014년 12월 15일 직원의 사회 보장 번호나 의료 정보를 유출의 원인은 보안 대책의 부족이 원인인 것으로 두 전직 소니 픽처스 직원이 소송을 제기한 사건이다. (위키백과, 검색일 2015. 5. 28)

3.3.3.1.3 Bank of America 기밀정보 유출 사건

2010년 10월 BankofAmerica[22]에서 근무한 전직 프로그램 개발자에 의해 회사 기밀정보가 유출된 사건으로 회사 손익상태, 트레이딩 포지션, 신용보고서 등 총21개 기밀 파일을 유출하였다. BankofAmerica는 직원 이메일의 대용량 전송에 대한 모니터링 과정에서 이를 적발하였다. 전직 프로그램 개발자가 퇴사 이전에 회사 기밀정보를 유출하였다. 내부 정보유출 경로를 사전에 차단하는 대책과 사후 모니터링의 중요성을 보여준 사건으로 내부정보 유출 방지 및 불법 행위 모니터링 시스템 도입 등이 시급히 필요하게 되었다. (홍시환, 2011).

3.3.3.2 국내 피해사고사례

3.3.3.2.1 “1.25” 인터넷 대란

2003년 1월 25일 대한민국 인터넷 망이 마비된 사건이다. 마이크로소프트사 SQL 서버의 허점을 이용하는 슬래머 웜 이 이 사건을 일으켰다. 이 사건은 슬래머 웜에 감염된 PC들이 대량의 데이터를 생성해 KT 혜화전화국에 있는 DNS 서버에 인터넷 트래픽을 집중시키면서 시작되었다. KT 혜화전화국이

22) 미국의 대형 금융회사로 미국 전역을 포함해 전 세계 40개 이상의 나라에서 영업을 하고 있다.

공격에 의해 마비되자, 전국적인 인터넷 트래픽이 다른 백본망으로 우회하기 시작했고, 다른 DNS 서버도 순차적으로 마비되어 갔다. 한편, 대기업의 인터넷 회선이 아닌 백본망을 빌리는 형태로 서비스를 제공하는 중소업체의 인터넷 회선은 대기업의 회선에 비해 마비의 정도가 덜했다. 이 사건으로 피해를 입은 인터넷 사용자들은 KT를 상대로 피해보상소송을 제기하기도 한 피해사례이다. (위키 백과, 검색일 2015. 6. 2)

3.3.3.2.2 삼성전자 핸드폰 설계도 유출 사건

2006년 3월 발생한 (주)삼성전자 선임연구원이 시도한 최신형 국내 휴대폰 설계회로를 카자흐스탄 통신업체에 유출 기도 사건이 있었다. 삼성전자 무선사업부 선임연구원 이○○는 연구개발비 약 26억 5천만원이 투입된 최신형 PCS휴대폰[SPH-S1300]및 셀룰러 슬림 휴대폰[SCH-V740]의 회로도 및 배치도 등이 들어있는 파일을 사내 통신망을 통해 다운로드 받은 다음 이를 A4용지 15장에 출력하여 가지고 나와 카자흐스탄의 유력정보통신사인 'NURSAT'사의 관계자들에게 열람시킨 후 샘플로 회로도 사본 각 1장을 교부하고 가격조건을 절충하던 중 적발되었다. 피의자는 사내 보안검색대를 통과하자 출력물을 접어 점퍼 속주머니에 넣고 관심을 다른 데로 돌리고자 직원교육용 사내자료인 'RTOS' 제작 책자를 가지고 나오는 등 지능적인 방법을 사용하였다. 위와 같은 사건이 일어나게 된 원인을 살펴보면, IT 강국으로 부상함에 따른 경쟁력 있는 기술 분야의 급성장에 따른 역효과를 들 수 있다. IT 분야 수출총액의 전체 수출액의 30%에 육박하고 있고,후발국가인 중국·대만을 비롯하여 미국 등 선진국에서도 탐내는 기술이 생겨나기 시작하였고 그 역작용으로 해외 산업스파이가 반발하기 시작하였다. 또한 IMF이후 평생직장 개념이 없어진 현재 고용불안감으로 퇴직 전 한몫 챙기자는 의식이 팽배해져 이에 따라 회사의 중요한 기밀문서를 별도로 보관하는 풍조가 생겼으며, 기술인력에 대한 관리 소홀, 기술자들의 도덕적 해이가 그 원인이라 하겠다. (남상봉,2011:15)

3.3.3.2.3 옥션 개인정보 유출 사건

2008년 옥션 전체회원 1863만여 명의 개인 정보가 유출되었다. 옥션은 자체적으로 2008년 2월 4일에 자사의 정보가 유출된 사실을 감지하였으나, 실제 피해규모보다 적은 1081만 명의 정보만이 유출된 것으로 파악했다. 경찰은 조사 결과를 2010년 1월 말 옥션 측에 넘겨졌으나 옥션은 이를 2개월여가 지난 2010년 3월 25일에 발표하였다. 옥션 측에서는 피해 데이터를 일일이 수작업으로 확인하느라 발표가 늦어졌다고 해명했다. 이 사건은 중국의 해커에 의해 이루어진 것으로 추정되며, 사이트간 요청 위조(CSRF) 공격 방식을 이용한 것으로 알려졌다. 해커는 옥션의 관리자들에게 공격 코드가 포함된 전자 우편을 대량으로 송신하였다. 관리자가 전자 우편을 읽는 순간 거기에 포함된 코드를 실행하게 되었고, 그 결과 해커는 관리자의 인증 정보를 얻었다. 해커는 이를 이용하여 옥션에 가입된 사용자들의 정보를 빼내었으며, 이후 유출된 개인정보를 인질로 옥션 측에 금전을 요구하였다. (위키 백과, 검색일 2015. 6. 2)

3.3.3.2.4 “7.7” DDoS 공격

7·7 DDoS 공격 또는 777 DDoS 공격은 2009년 7월 7일을 기점으로 대한민국과 미국의 주요 정부기관, 포털 사이트, 은행 사이트 등을 분산 서비스 거부 공격(DDoS, 디도스)하여 서비스를 일시적으로 마비시킨 사건이다. 한국 일부와 미국의 경우 이 공격을 1차 공격으로 명명하여 전체적으로 1차~4차의 4단계로 구분한다. 이 공격은 2009년 7월 5일, 미국 시간으로 2009년 7월 4일인 독립 기념일에 시작되었다. 백악관을 비롯한 미국의 27개 사이트를 공격했다. 한편, 2009년 7월 4일 국가정보원과 방송통신위원회는 대한민국과 미국에서 DDoS 공격 징후를 파악했지만, 적절한 대응을 하지 않았다는 것이 밝혀졌다. 먼저, 대한민국을 타깃으로 한 1차 공격은 2009년 7월 7일 오후 6시 경에 시작되고 약 24시간동안 지속되었다. 대한민국과 미국의 주요 26개 사이트를 공격했는데, 청와대 및 백악관, 그리고 대한민국의 주요 언론사와

주요 정당, 포털의 홈페이지 등이 공격리스트에 포함되어있었다. 2차 공격은 2009년 7월 8일 오후 6시에 시작되고 약 24시간동안 지속되었다. 1차 공격 리스트에 있었던 사이트 일부와 주요포털 사이트의 메일서비스를 대상으로 공격을 했다. 공격 대상이 된 사이트는 16개이다. 3차 공격은 2009년 7월 9일 오후 6시에 시작되었다. 이로 인해 국가정보원과 일부 금융기관 홈페이지가 장애를 빚었지만 약 3시간 만에 정상화되었다. 4차 공격은 2011년 1월 6일에도 발생했는데, 같은 달 28일 경찰은 수사를 통해 '남북한 사이버 전쟁'을 촉발시킨 분산서비스거부(DDos) 공격이 네티즌의 관심을 끌려는 10대의 '1인 자작극'이었음을 밝혔다. (위키 백과, 검색일 2015. 6. 2)

3.3.3.2.5 “2010년 삼일절” 사이버 공격

2010년 한·일 삼일절 사이버 공격 사건은 2010년 3월 1일에 대한민국의 웹사이트 디시인사이드를 중심으로 하여 웃긴 대학, 루리웹, 엽기 혹은 진실, 오늘의 유머, 다음 아고라등의 커뮤니티 사이트들이 연합하여 세운 네이버의 ‘테러대응연합’ 회원들이 일본의 웹사이트 2채널을 공격한 사건이다. 디시인사이드와 2채널 이 두 사이트는 2004년 이후 크고 작은 싸움을 벌여왔다. 2010년 3월 1일은 대한민국의 경축일인 삼일절이며, 한일 병합 조약이 발효된 지 딱 100년이 되는 해이기도 하다. 2009년 겨울에 러시아에서 발생한 한국인 구타사망 사건과 2010년 동계올림픽 김연아 선수의 금메달 수상에 따른 비방이 도를 넘어서자 우리나라 네티즌 사이에서 "정당한 테러 대응 카페"(이하 테대연)가 개설되며 단 하루 만에 회원 수 1만 2천 명을 돌파했다. 결국 테대연 연합은 3월 1일 오후 1시에 F5리로드 등의 방식으로 일제히 공격을 가해 2채널 전 서버가 다운되었다. 3월 2일 현재 파악된 피해 금액은 약 250만 달러 이상으로 추정된다. (위키백과, 검색일 2015. 6. 2)

3.3.3.2.6 농협 전산망 마비 사태

2011년 4월 12일 농협 전산망에 있는 자료가 대규모로 손상되어 수일에 걸쳐 전체 또는 일부 서비스 이용이 마비된 사건이다. 사건 초기에는 협력 업체에 의한 사고 가능성이 제기되었으나, 이후 농협 측에서는 내부 전문가의 사이버 테러일 가능성이 높다고 발표했다. 그 후 4월 26일에 대한민국 검찰은 조선민주주의인민공화국의 소행이라고 발표했으나 여러 가지 부분에서 의문점이 지적되었다. 농협 측의 사건 처리가 미흡했다는 지적이 있었으며, 농협의 일부 업무는 4월 13일 오후, 모든 업무는 여러 차례 연기 끝에 18일만인 4월 30일에 정상화되었다. (위키백과, 검색일 2015. 6. 2)

3.3.3.2.7 “3.20” 전산 대란

3·20 전산 대란(－電算大亂)은 2013년 3월 20일 대한민국의 주요 언론과 기업의 전산망이 마비되고, 다수의 컴퓨터가 악성코드에 감염되어 피해를 입은 사건이다. 악성코드의 유포로 3만 2천여 대의 시스템이 감염된 것으로 알려져 있다. 방송통신위원회는 사건 당일 브리핑에서 "피해 기관으로부터 채증한 악성코드를 분석한 결과 특정 업체의 업데이트 관리 서버(PMS)에서 악성코드가 유포된 것으로 추정된다."고 설명했다. 다음날인 21일 브리핑에서는 단일 조직에 트로이 목마를 통해 사전에 유입된 악성코드에 공격당한 것으로 추정되며, 일부 기업의 악성코드 유입 경로 추적 결과 중국 소재 IP 주소가 발견되었다고 발표했다. 하지만 22일 중국이 아니라 농협은행의 것으로 정정했는데 '101.106.25.105'라는 사설 IP 주소가 중국의 국제 공인 IP 주소와 같아 잘못 판단했다고 한다. (위키 백과, 검색일 2015. 6. 2)

3.3.3.2.8 개인정보 대량유출사건

2014년 대한민국 개인정보 대량유출사건은 대한민국의 주요 카드사의 1억 4000만 건이 넘는 개인정보가 유출된 사건을 말한다. 2013년 6월경에 개인

정보가 유출되었으나, 2014년 1월에 뒤늦게 밝혀져 큰 이슈로 번졌다. 이 사건은 2013년 6월 경 KCB 신용평가사 직원 한 명이 카드사로 파견을 나가 주요 카드사 (국민, 롯데, 농협)의 고객 개인정보를 유출시켜 대출광고업자와 대출모집인에게 정보를 넘겼다. 하지만 카드사는 7개월 동안 인지를 못하였다가 2014년 1월에 검찰의 발표로 알려지게 되었다. 그리고 KCB 신용평가사 직원과 정보를 구입한 대출광고업자를 검찰에 구속 기소하고 정보를 구입한 대출모집인을 불구속 기소하였다. (위키백과, 검색일 2015. 6. 3)

3.3.3.2.9 경비업체 농협금고 털이 사건

2013년 3월 23일 충남 당진 농협 금고에서 현금 1억 원을 훔친 사건이 발생했다. 범인은 전직 경비업체 직원으로서 내부사정을 잘 알고 있었다고 한다. 경비업체 근무시절에 미리 만들어 둔 예비 보안카드로 경비를 해제한 뒤 3분 만에 금고를 털어 달아난 사건이다. 농협측도 휴일엔 업무 편의를 위해 경비업체 직원에게 금고문을 열어 둔 채로 맡길 정도로 관리가 허술했다는 경찰 조사 결과가 있었다. (위키백과, 검색일 2015. 6. 3)

Ⅳ. 융합 보안관제시스템 발전 방안

4.1 융합 보안관제시스템 활성화 배경

4.1.1 융합 보안관제 체계 패러다임의 변화

산업보안협회(2015)가 발표한 <그림 15>의 융합보안관제체계 구축 패러다임을 살펴보면 2011년에 보안관제센터 인프라 구축 및 관제운영 프로세스의 확립을 통한 도입기를 거치며 2012년 발전기를 통해 산업기밀 추적 및 관리서비스 강화를 위해 현장대응팀을 운영하게 되었다. 2013년과 2014년에는 On-Line 취약점 분석 및 위험관리체계 수립 및 지역, 분야별 관제센터와 유기적 연계체계 수립 등을 이루며 성숙기를 맞이하게 되었다. 2015년에 이르러 융합보안관제체계가 구축되었음을 알 수 있다.

<그림 15> 융합 보안 관제체계 발전 패러다임

4.1.2 보안위협의 증가

과거의 보안위협은 시설경비, 출입통제에 국한되는 물리보안이 주요 관심사였지만, 1980년대를 지나 1990년대 접어들면서 컴퓨터의 발달과 인터넷의 보급으로 인해 정보보안의 필요성이 커지게 되었다. 현재에는 산업기술의 발달과 IT기술의 접목을 통해 정보전달의 중요성이 급속히 증가하면서 기업기밀정보 유출 및 금융기관의 해킹, 공공기관의 서비스 업무 중단 등 날로 지능화되어가는 보안위협 속에서 살고 있다. 특히 국제적인 해킹피해로 인해 우리나라 기업들과 금융기관들을 금전적 피해는 물론 기업이미지에 큰 타격을 받게 되는 것을 불안해하고 있는 실정이다.

하나대투증권(2013)은 2013년 2월 글로벌 보험회사인 AIG가 258명의 최고경영자(CEO)들을 상대로 경영상 위험요인에 대해 조사한 결과 응답자의 85%가 해킹을 선택했다고 보도하였다. CEO들은 실적 감소, 자산가치 하락, 주가와 투자 위험보다도 기업경영에 해킹이 더 큰 위험요소라고 본 것이다. 또한 응답 CEO의 69%는 재무적 위기보다도 해킹에 따른 평판하락이 기업에 더 심각한 위협이 되고 있다고 대답하였다.

국정원 산업기밀보호센터의 보고 자료[23]에 의하면 국가핵심기술의 해외 유출 사고는 2013년 6건에서 2014년 63건으로 10배 이상 증가하였으며, 기술유출로 인한 우리나라의 예상 피해액이 연평균 50조원에 이른다고 하였다. 기술유출 분야는 전기전자, 정밀기계, 정보통신, 화학, 생명공학 등 다양한 분야에서 위협을 받고 있으며 기술유출 산업스파이의 80%가 전, 현직 직원을 통해 발생한다는 보고는 시사 하는 바가 크다. 이러한 피해사고는 매년 지속적으로 증가하고 있으며, 이러한 보안 위협에 대응체계를 마련이 시급한 실정이다.

4.1.3 융합보안 시장의 성장

융합보안 시장은 2007년 이후 연평균 14%의 고속 성장세를 보이며 2014년

23) 국정원 산업기밀보호센터 (2015), 끝나지 않은 위협, 경제안보

기준 세계 2424억 달러, 국내5조 5113억 원 규모의 시장이 형성되었다. 2000년 이전에는 물리보안 시장의 규모가 우의를 차지하였지만 2000년대 들어서는 정보보안 시장을 중심으로 시장이 성장하였다. 특히 최근 들어 융합보안 시장의 성장세가 눈에 띄게 달라졌으며, 2010년을 기점으로 물리영역 내 융합보안 제품이 전체시장 규모의 50%를 상회하는 것으로 집계되었다. 국내 융합보안 시장은 세계시장보다 성장 규모가 훨씬 가팔랐으며, 이미 2010년에 1조 6747억 원으로 정보보안 시장규모인 1조 2727억 원을 넘어 섰으며 2018년까지 평균 32.92% 성장한 12조 8396억 원에 이를 것으로 예상되어진다. 이처럼 융합보안 시장의 성장세는 고속성장을 거듭하고 있다는 것을 알 수 있었다. 가트너가 발표한 자료에 의하면 세계 융합보안 시장의 국가별 비중에서 우리나라는 1.4% 수준이어서 비중이 매우 작지만, 매년 성장속도가 급속히 증가하고 있음에 유의해야 한다고 한다.

4.2 융합 보안관제시스템 개선점 설문조사

4.2.1 설문조사 결과분석

공공기관의 보안관제 관리 담당자, 보안관제 관련기업 보안담당자 및 관련 종사자들에게 융합보안관제시스템 발전 방안에 대한 연구에 대한 의견을 수렴하기 위해 설문조사를 실시하였다.

4.2.2 설문조사 대상

설문조사 대상은 공공기관에서 근무하는 물리보안 담당자 22명, 정보보안 담당자 28명과, 보안관제 산업 종사자 40명, 보안관제실 요역업체 근무요원 22명을 대상으로 <표 5> 과 같이 2015년 5월 15일부터 5월 29일까지 실시하였으며, 설문조사 항목과 지표는 명목척도법을 사용하여 일반사항을 조사하였으며, 제2장 이론적 고찰과 제3장 융합보안관제시스템 구축 동향에서 논의한 융합보안관제센터와 융합 보안관제시스템에 대한 개선점과 기능적 요구사항은 리커트척도법을 참고하여 작성하였으며, 조사결과는 MS-Excel 을 사용하여 표현하였다.

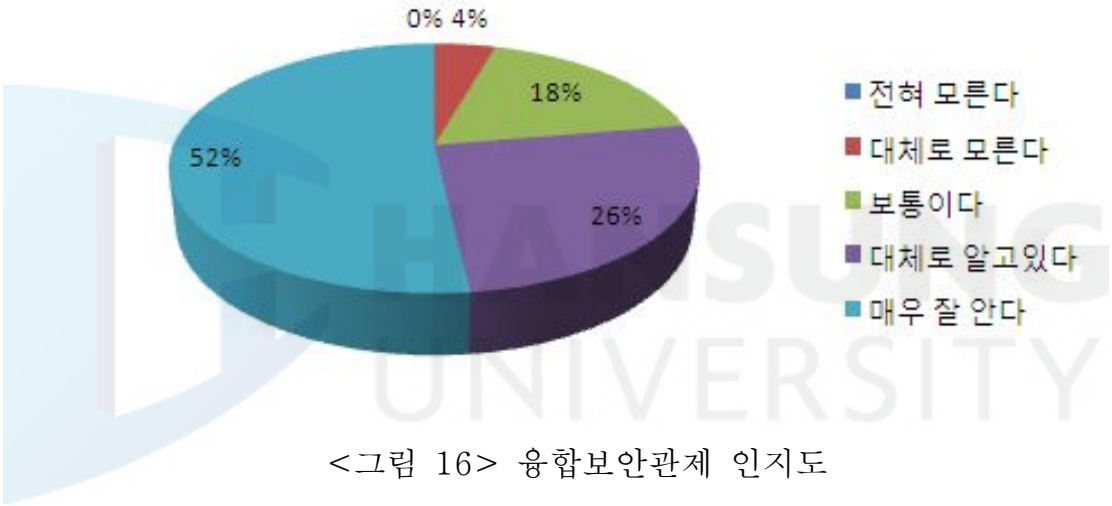
<표 5> 설문조사 응답자 현황

구분	보안관제 관리 담당자			보안관제 산업 종사자					합계
	공공기관		소계	관련기업				소계	
	물리보안 담당자	정보보안 담당자		물리 보안 담당자	정보 보안 담당자	융합 보안 담당자	관제 근무요원		
응답 자수	22	28	50	13	17	10	22	62	112

4.2.3 융합보안관제 인지도에 관한 설문조사 결과분석

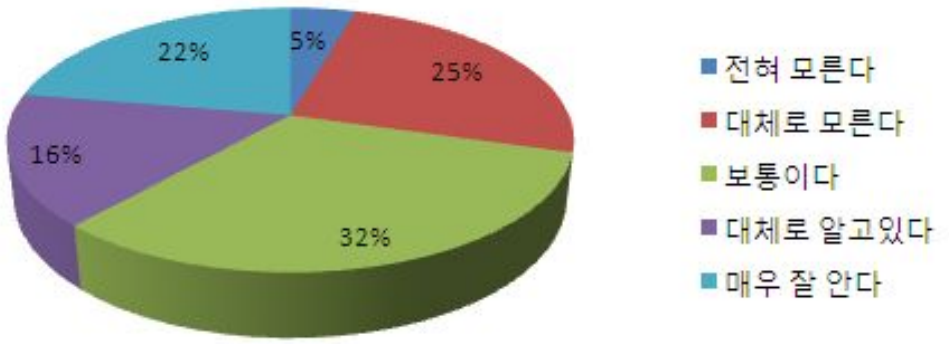
공공기관의 보안관제 관리 담당자 및 보안관제 산업 종사자를 대상으로 한 설문조사 결과를 설문 항목별 분석한 결과 다음과 같았다.

융합보안관제에 대해 알고 있는지에 대한 질문에는 <그림 16>와 같이 응답자의 과반수인 (78%)가 긍정적으로 응답하였으며 그중 52%는 매우 그렇다. 26%는 대체로 그렇다. 18%는 보통이라고 응답하였고, 4%는 부정적인 의견을 제시한 것으로 보아 융합보안관제에 대한 인지도는 대체로 높으며 과반수가 인지하고 있음을 알 수 있었다.



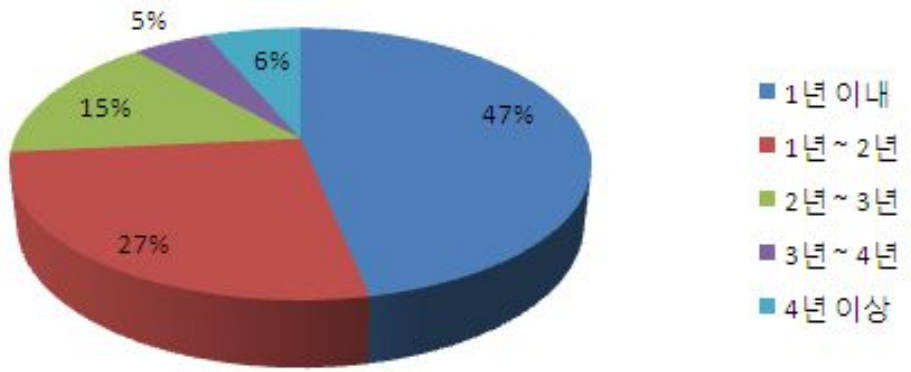
<그림 16> 융합보안관제 인지도

융합 보안관제시스템에 대해 알고 있는지에 대한 질문에는 <그림 17>와 같이 응답자의 과반수에 못 미치는 (38%)가 긍정적으로 응답하였으며 그중 22%만이 매우 그렇다. 16%는 대체로 그렇다. 32%는 보통이라고 응답하였고, 33%는 부정적인 의견을 제시한 것으로 보아 융합 보안관제시스템에 대한 인지도는 대체로 높지 않다는 것을 알 수 있었으며, 잘 모르겠다는 의견도 33%에 이르는 것으로 미루어 융합 보안관제시스템의 구체적인 기술검토와 발전방향이 이루어지 위해서는 사전에 인지도부터 높일 필요가 있다는 것을 알게 되었다.



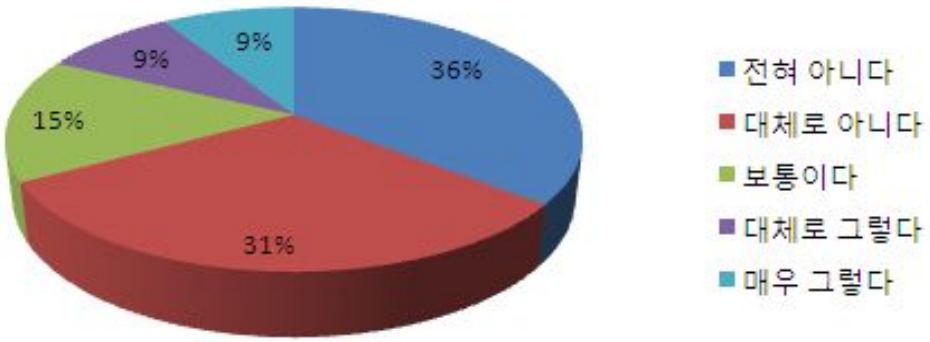
<그림 17> 융합 보안관제시스템 인지도

융합 보안관제시스템을 알게 된 시기에 대한 질문은 <그림18> 긍정적인 답변과 보통이라는 답변을 한 대상자에 한해서 설문을 받은 결과이다. <그림12>와 같이 응답자의 과반수에 근접한 (47%)가 1년 이내에 처음 알게 되었다고 응답하였으며 1년~2년 은 27% 응답자가 의견을 제시했다. 2년~3년은 15%, 3년~4년은 5%였으며, 4년 이상 된 응답자는 전체의 6%에 머무는 응답을 얻었다. 본 설문문항 결과로 보아 융합 보안관제시스템은 국내에서 인지도가 많이 없다보니, 실제 담당자들이 알게 된 시기도 생각보다 최근이라는 것을 알게 되었다.



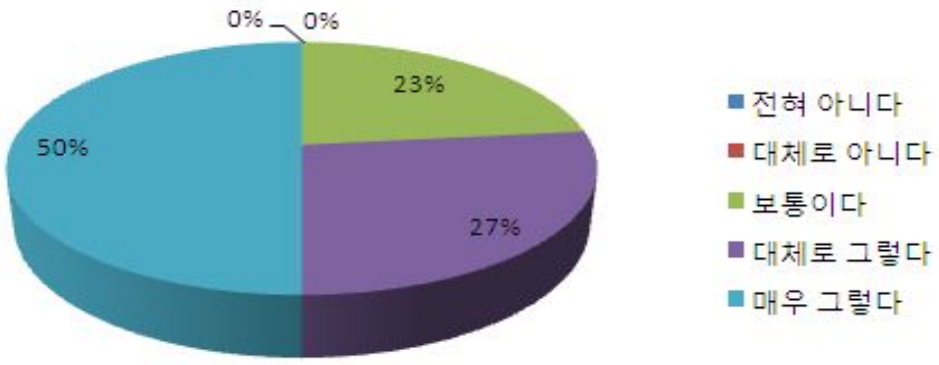
<그림 18> 융합 보안관제시스템을 알게 된 시기

현재 소속되어 있는 회사에 융합 보안관제시스템이 구축되어 있는지에 관한 질문에는 <그림 19>과 같이 응답자의 과반수가 넘는 (67%)가 부정적으로 응답하였으며 15%는 보통이라고 응답하였고 18%만이 그렇다고 응답을 제시하였다. 현재까지는 융합 보안관제시스템 도입이 미비한 실정임을 알 수 있었다.



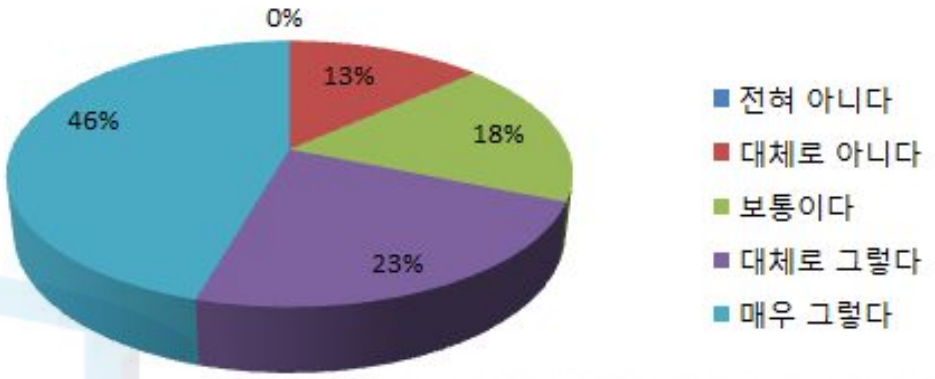
<그림 19> 융합 보안관제시스템 구축 여부

융합 보안관제시스템 구축이 된다면 보안성 향상에 기여할 것인가에 대한 질문에는 <그림 20>과 같이 응답자의 과반수가 넘는 (77%)가 긍정적으로 응답하였으며 그중 50%는 매우 긍정적이라는 답변을 제시하였다. 보통이라는 답변은 23%였으며, 부정적인 답변은 전혀 없었다. 도입이 된다면 보안성 향상에 도움이 될 것이라는 인식을 가지고 있음을 알 수 있었다.



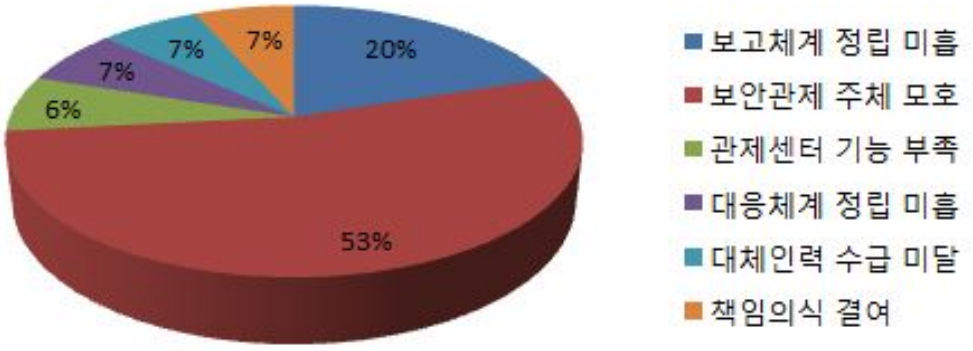
<그림 20> 구축후 보안성 향상에 기여 가능성

융합 보안관제시스템 구축후 보안침해 위협으로부터 안전해질 것인가에 대한 질문에는 <그림 21>과 같이 응답자의 과반수가 넘는 (69%)가 긍정적으로 응답하였으며 그중 46%는 매우 긍정적이라는 답변을 제시하였다. 보통이라는 답변은 18%였으며, 부정적인 답변은 13%를 차지하였다. 앞선 질문과 연관성이 있는 유사한 질문이었지만 의외로 부정적인 응답을 제시한 사람이 있었다. 대체로 안전해질 것이라는 의견이 많았지만 부정적인 응답에 대해 자세히 알아볼 필요가 있었다.



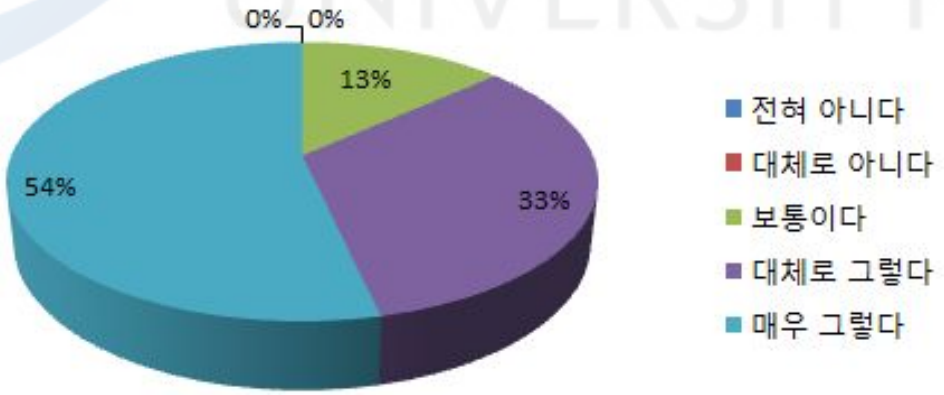
<그림 21> 구축후 보안위협으로부터 안전 여부

융합 보안관제시스템 구축후 보안침해 위협으로부터 안전하지 못하다고 생각하는 이유에 대한 질문에는 <그림 22>과 같이 응답자의 과반수가 넘는 (53%)가 보안관제 주체의 모호함을 지적하였다. 보고체계 정립 미흡에 대해선 20% 응답제시가 있었으며, 그 외에 관제센터 기능 부족, 대층체계 정립 미흡, 대체인력 수급 미흡, 책임의식 결여 등의 응답이 있었다. 이를 통해서 부정적인 응답을 제시한 사람들의 의견이 대체로 융합보안관제시스템 구축시 보안관제 주체에 대한 정립이 먼저 이루어져야하며, 보고체계 정립 또한 사전에 정립해야 함을 알 수 있었다. 또한 기능적 부분과 책임의식 부분에서도 우려의 시선이 있음을 알 수 있었다. 이런 부정적 의견은 향후 융합 보안관제시스템의 구축에 대한 발전 방향을 잡기위해 반드시 고려하고 설계해야 하는 부분임을 알 수 있었다.



<그림 22> 보안위협으로부터 안전하지 못한 이유

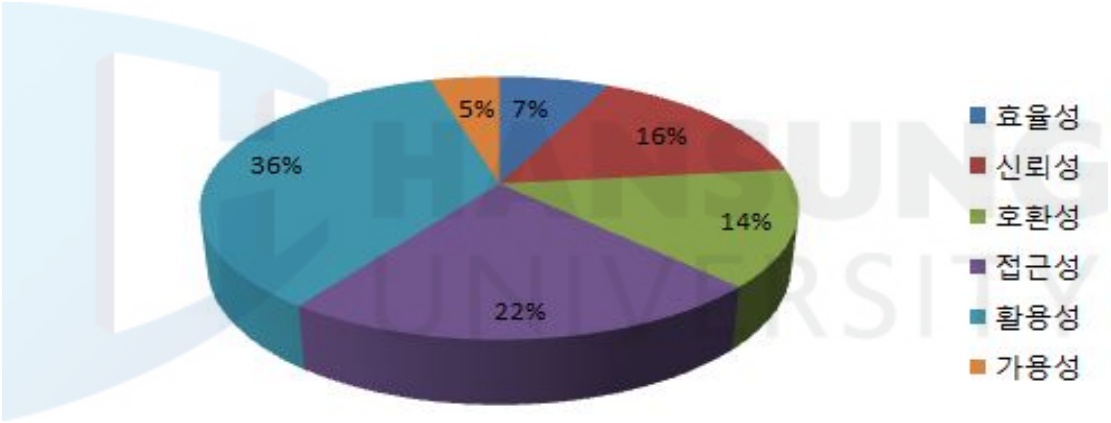
융합 보안관제시스템 구축후 반드시 필요하다고 생각하느냐는 질문에는 <그림 23>과 같이 응답자의 대다수 비중의 (87%)가 긍정적인 응답을 제시하였다. 그중 54%는 매우 긍정적인 응답을 하였으며, 보통이라고 생각하는 응답자는 13%였다. 부정적인 응답을 제시한 사람은 전혀 없었다. 이를 통해 융합 보안관제시스템 구축은 대다수의 응답자가 그 필요성을 높이 보고 있다는 것을 알 수 있었다.



<그림 23> 융합보안관제시스템 구축의 필요 여부

4.2.4 융합 보안관제시스템 도입 시 고려사항에 대한 설문조사 결과분석

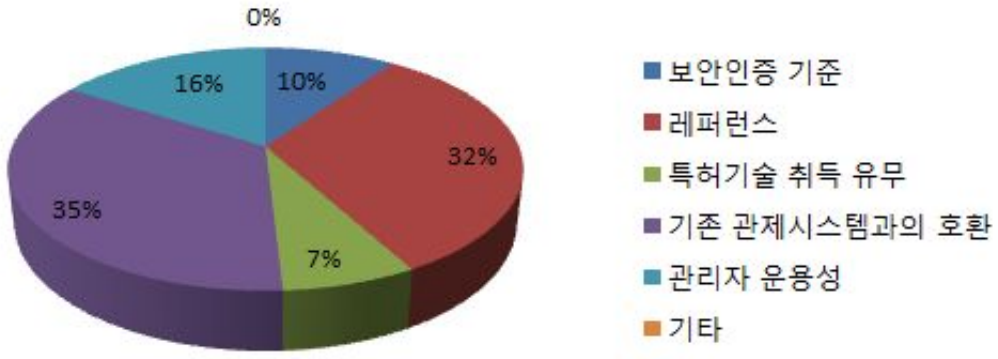
융합 보안관제시스템 도입 시 가장 중요하게 생각하는 부분은 어떤 것인가에 대한 질문에는 <그림 24>과 같이 활용성이(36%)이 가장 많은 응답을 제시하였다. 그다음 접근성(22%), 신뢰성(16%), 호환성(14%), 활용성(7%), 가용성(5%) 순으로 응답을 제시하였다. 이를 통해 융합관제시스템 도입 시 활용성과 접근성이 과반수가 넘는 (58%)를 차지함으로서 실질적 운영에 필요한 부분을 고려하고 있음을 알 수 있었다. 그 외에도 다양한 의견이 비교적 골고루 나타남으로서 레퍼런스 및 대외적인 평가가 많지 않음으로 인해 운영 관리자 및 관련업체 종사사들 조차도 의견이 분분함을 단적으로 보여주었다고 판단되며, 실제 도입 시 필요한 기준을 정하기에 어려움이 예상된다고 보여진다.



<그림 24> 도입 시 중요하게 생각해야하는 부분에 대한 설문

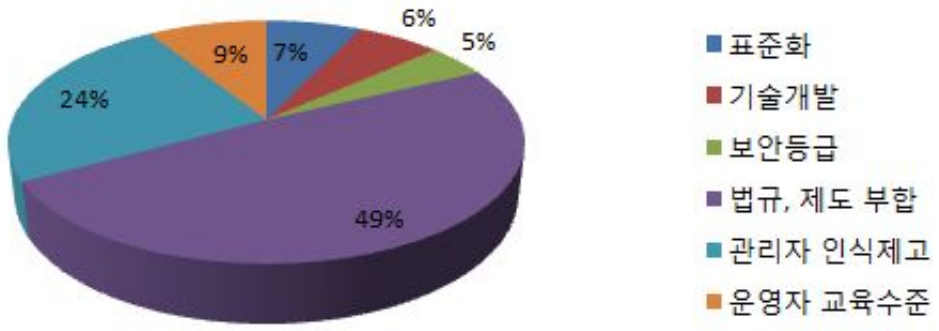
융합 보안관제시스템 도입 시 우선 고려해야할 사항이 무엇인가에 대한 질문에는 <그림 25>과 같이 기존 관제시스템과의 호환(35%)이 가장 많은 응답을 제시하였다. 그다음 레퍼런스(32%), 관리자 운용성(16%), 보안인증(10%), 특허기술 보유(7%) 순으로 응답을 제시하였다. 이를 통해 융합관제시스템 도입 시 우선 고려해야할 부분은 기존 관제시스템과의 호환 및 타 기관에 구축된 레퍼런스를 통해 안정적 운영을 가장 원한다는 것을 알 수 있었다. 그 외에도 관리자 운용성 측면과 보안인증 기준 및 특허기술 보유 유무도 우선 고

려대상임을 알 수 있었다.



<그림 25> 도입 시 우선 고려해야 할 부분에 대한 설문

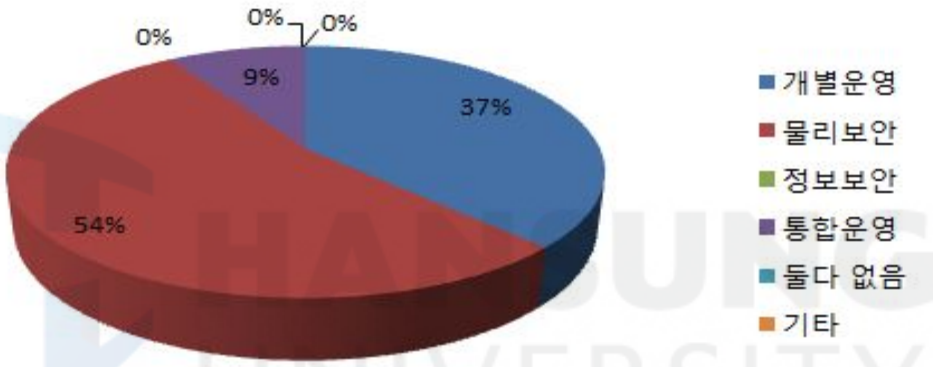
융합 보안관제시스템 도입 시 가장 고려해야할 사항이 무엇인가에 대한 질문에는 <그림 26>과 같이 법규, 제도 부합여부(49%)가 가장 많은 응답을 제시하였다. 그다음 관리자 인식제고(24%), 운영자 교육수준(9%), 표준화 기술(7%), 기술개발(6%), 보안등급(5%) 순으로 응답을 제시하였다. 이를 통해 융합관제시스템 도입 시 가장 고려해야할 부분은 법규, 제도 부합여부가 과반수에 가까운 (49%) 응답을 제시함으로서 가장 고려해야 할 부분이라는 것을 알 수 있었다. 그리고 관리자 인식제고와 교육수준도 중요한 요소임을 알 수 있었다. 이와 같이 융합 보안관제시스템에 대한 견해는 관련 법규 및 제도의 기준이 모호하기 때문에 어느 범위까지 보안관제의 기준을 삼는지 여부가 가장 중요한 고려사항임을 알 수 있었다.



<그림 26> 도입 시 가장 고려해야 할 부분에 대한 설문

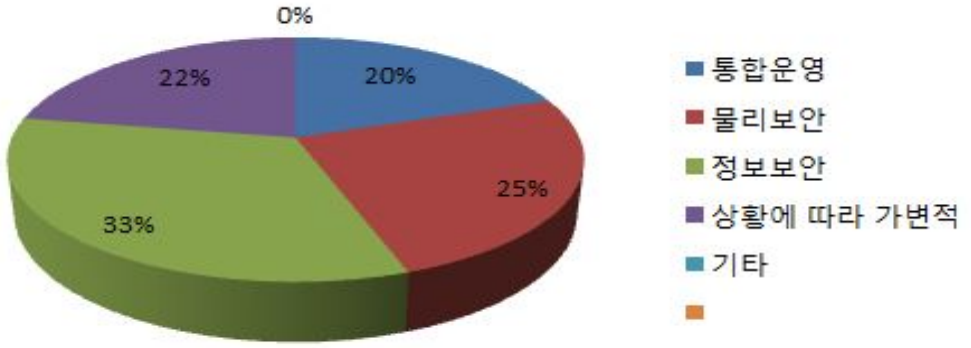
4.2.5 융합보안관제시스템 운영 실태에 관한 설문조사 결과분석

현재 보안관제가 어떤 형태로 운영되고 있는지에 대한 질문에는 <그림 27>과 같이 과반수인 (54%)가 물리보안센터만 운영한다고 응답하였으며 37%는 물리보안센터와 정보보안센터를 개별 운영한다고 응답하였다. 그리고 9%는 통합운영을 한다고 응답하였다. 정보보안센터만 별도로 운영하는 곳은 한곳도 없었으며 모든 응답자가 물리보안센터는 운영하고 있다고 응답하였다. 이를 통해 물리보안센터는 기본적으로 모두 운영하고 있으며 일부는 정보보안센터만 개별 운영하는 것을 알 수 있었다. 그리고 통합운영을 하는곳은 굉장히 미비함을 알 수 있었다.



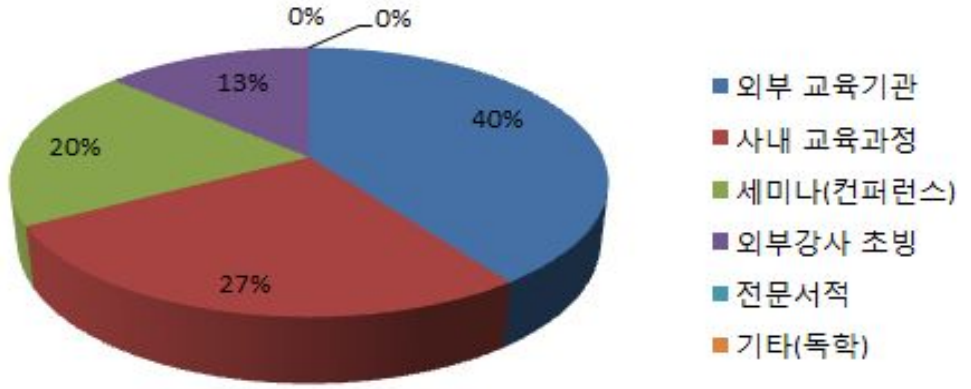
<그림 27> 보안 관제센터 운영형태에 대한 설문

융합보안업무중 어느 분야가 중요하며 우선시 되어야 한다고 생각하는지에 대한 질문에는 <그림 28>과 같이 33%는 정보보안 분야를 25%는 물리보안 분야를 22%는 상황에 따라 가변적이라는 응답을 하였으며, 20%는 통합적 운영이 중요시 되어야 한다고 응답하였다. 이를 통해본 결과로 의견이 다양하게 제시되었으며, 운영센터별 또는 업무별로 융합보안업무의 중요성에 대한 인식의 차이가 많음을 알 수 있었다. 이는 아직 융합보안분야가 관제센터 관리자 및 관련업체 종사자들에게 인지도가 부족하고 구체화된 구축사례가 많이 않음으로 인해서 주관적인 견해가 많음을 알 수 있었다. 해당 설문문항은 본 연구의 배경이 되었으며, 발전방향에 대한 시사점을 도출하기에 매우 중요한 설문이었다.



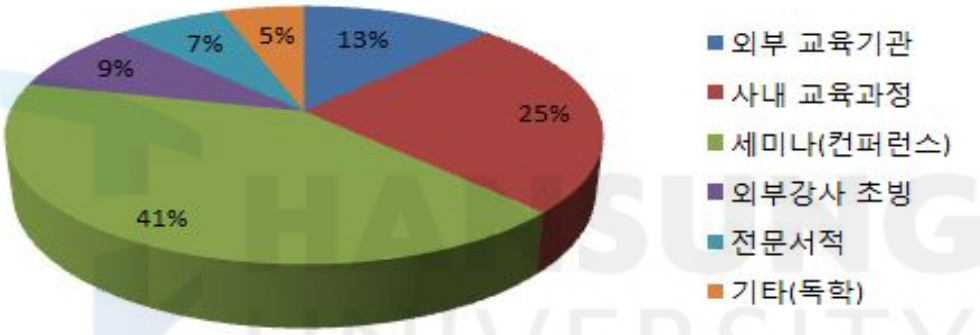
<그림 28> 융합보안업무중 중요시 되어야 하는 분야에 대한 설문

융합보안관련 기술력 습득은 어떤 매개체를 통한 교육이 가장 좋다고 생각하는지에 대한 질문에는 <그림 29>과 같이 40%가 외부 교육기관을 통해서 지식 및 기술력 습득을 희망하였으며 27%가 사내 교육과정을 선호하였고 20%는 관련분야 세미나 및 컨퍼런스를 통한 기술력 습득으로 응답하였다. 13%는 외부강사 초빙을 통한 지식전달에 응답하였다. 지식전달을 희망하는 대상자들의 선호도 조사를 통해 본 결과는 특정한 매개체에 치중하지 않았으며 다양한 방법을 통한 기술력 습득을 희망하고 있음을 알 수 있었다. 해당 설문을 받는 동안 중복체크를 하고자 하는 의견을 가장 많이 받았던 설문 문항이었다. 이를 통해 융합보안분야 관리자 및 관련업체 종사자들은 지식정보 습득 및 기술력습득에 많은 노력과 관심을 기울이고 있음을 알 수 있었다.



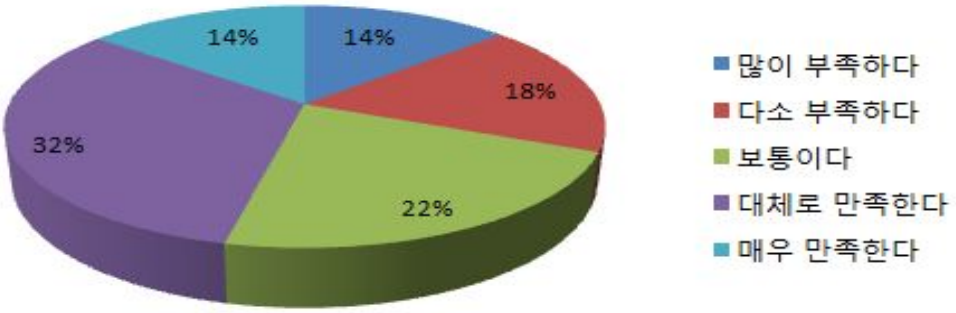
<그림 29> 융합보안관련 기술력 습득을 위한 매개체에 대한 설문

융합보안관련 기술력을 습득은 어떠한 매개체 통해 받았는지에 대한 질문에는 <그림 30>과 같이 41%가 세미나 및 컨퍼런스를 통해서 지식 및 기술력 습득을 했다고 응답하였으며, 25%가 사내 교육과정이라고 응답하였다. 13%는 외부 교육기관을, 9%는 외부강사 초빙을 통해 습득하였다고 응답하였다. 그리고 7%는 전문서적을, 5%는 독학등의 방법으로 기술력을 습득하였다는 응답하였다. 제시된 응답을 통해 본 결론으로는 응답자들이 실제로 기술력을 습득한 매개체중 세미나 및 컨퍼런스가 가장 많았으나 희망하는 매개체는 외부 교육기간이 가장 많았다. 이를 통해 융합보안분야 기술습득을 위한 매개체가 많이 않으며 현재까지는 세미나 및 컨퍼런스에 많이 의존하고 있음을 알 수 있었다.



<그림 30> 융합보안관련 기술력을 습득한 매개체에 대한 설문

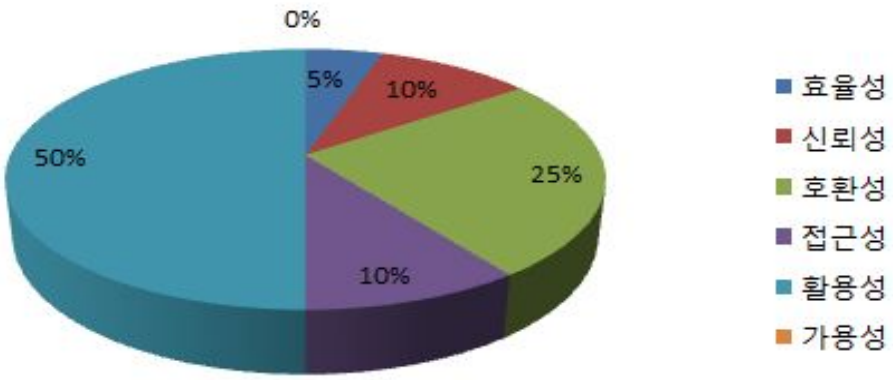
융합보안관련 교육 내용이 충분한지에 대한 질문에는 <그림 31>과 같이 과반수에 못 미치는 (46%)가 긍정적인 응답을 제시하였으며 그중 14%만이 매우 만족한다고 응답하였다. 22%응답자가 보통이라고 답변하였으며, 32% 응답자는 부정적인 응답을 제시한 것으로 보아 융합보안관련 교육에 대한 만족도가 전반적으로 높지 않음을 알 수 있었다. 이를 통해 현재까지 융합보안관련 전문교육기관 등의 지식정보전달 매개체의 전문성 부족으로 인해 융합보안관제분야 관제요원들의 기술력 습득에 대한 욕구를 충족시켜주기가 어려운 현실이며, 활성화를 위해서는 제도정착 및 정부지원 프로그램 등의 지원이 시급함이 필요함을 알 수 있었다.



<그림 31> 융합보안관련 교육 내용이 충분한지에 대한 설문

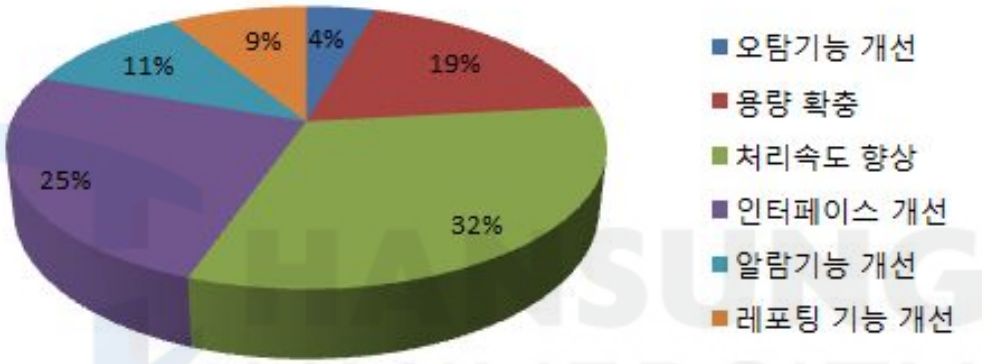
4.2.6 융합 보안관제시스템 기능에 관한 설문조사 결과분석

융합 보안관제시스템이 구축되어 운영 중인 기관에 대한 설문으로서 시스템 사용기능중 가장 중요한 부분은 무엇인가에 대한 질문에는 <그림 32>과 같이 과반수에 해당하는 (50%)가 활용성에 대해 응답을 제시하였다. 그리고 25%는 호환성이 중요하다고 응답하였고, 10%는 접근성과 신뢰성을 5%는 효율성을 중요한 기능이라고 응답하였다. 이러한 응답자의 제시를 통해 시스템 도입 전 고려사항과 실제 도입후 운영에 있어서 상이한 요소를 발견할 수 있었다. 해당 설문을 통해 본 논문의 가장 중요한 기능 도입 시 고려해야할 부분과 상이한 부분을 발견할 수 있었다. 또한 해당 설문문항을 통해 본 연구의 발전 방향에 대한 매우 중요한 시사점을 얻을 수 있었다.



<그림 32> 융합 보안관제시스템의 가장 중요한 기능에 대한 설문

융합 보안관제시스템의 개선이 필요한 기능에 대한 질문에는 <그림 33>과 같이 32%가 처리속도 향상에 대해 응답을 제시하였으며, 25%가 인터페이스의 개선을 19%가 용량 확충에 대한 의견을 제시하였다. 11%는 알람기능 개선을 9%는 레포팅 기능 개선을 4%는 오탐기능 개선에 대한 의견을 제시하였다. 이러한 응답자의 제시를 통해 시스템 도입후 기능적인 문제와 향후 개선사항에 대한 요소를 확인 할 수 있었다. 융합 보안관제시스템을 직접 운영하고 있는 기관에서는 안전성 및 보안강화의 효과를 느끼고는 있지만 그에 반해 개선사항이 다양하게 요구되고 있음을 통해 시스템의 안정화에 필요한 부분을 발견할 수 있었다.



<그림 33> 융합 보안관제시스템의 개선이 필요한 기능에 대한 설문

4.3 융합 보안관제시스템 발전방안

융합 보안관제시스템의 발전방향을 제시하기 위해 공공기관의 물리보안 및 정보보안 관리자와 관련기업 보안관리담당자, 그리고 보안관제 파견요원들에 대한 설문을 통해 추출한 결과를 분석하였다. 본 논문의 연구대상이 되었던 공공기관 융합 보안관제시스템 활성화 방안에 대해 다음과 같은 발전방향을 도출할 수 있었다.

첫 번째, 융합 보안관제시스템에 대한 인지도 부분에서 얻은 시사점은 대체적으로 인지도가 낮음을 알 수 있었다. 시스템이 구축되어 있는 기관이 적은 이유도 있지만, 인식하게 된 시점이 2~3년 이내라는 응답이 대부분을 차지하였다. 구축을 희망하는 긍정적인 답변이 많이 나왔으며, 구축후 보안위협으로부터 안전하게 되어(69%) 보안성 향상에 기여할 것이라는(77%) 응답이 많이 나왔다. 이를 통해 물리보안과 정보보안이 서로 개별로 분리되어 운영되고 있어서 낭비되는 공간적, 시간적, 인력적 소비를 줄일 수 있다는 장점으로 공공기관에 적합한 형태의 관제시스템 이라는 것을 알 수 있었다.

두 번째, 융합 보안관제시스템 도입 시 고려사항에 대한 설문을 통해 얻은 시사점은 도입 시 우선 고려해야 할 부분으로는 기존 관제시스템과의 호환성과 구축 레퍼런스가 65%를 차지하였다. 이는 공공기관의 특성상 기존에 구축되어 운영 중인 검증된 관제시스템인지 여부와 각종 솔루션과의 호환성을 가장 유념해야 한다는 것을 알 수 있었다. 구축 레퍼런스도 호환성과 같은 맥락에서 이해하면 되기 때문에 기존 시스템들과의 완벽한 호환성을 바탕으로 안정적 운영이 가능한 시스템을 선호한다는 것을 알 수 있었다.

세 번째, 융합 보안관제시스템 도입 시 중요한 요소로는 접근성과 활용성이 과반수(58%)가 넘는 응답을 제시했다. 그다음으로 호환성, 신뢰성을 중요시하였는데, 이를 통해 시스템 도입 시 관리자의 접근성을 높이기 위해 맞춤형 GUI 구현과 기존 분산되어 운영 중인 각종 관제솔루션들의 연계를 통한 활용성을 높여야 한다는 것을 알 수 있었다.

네 번째, 융합 보안관제시스템 운영시 가장 중요하다고 선택한 요소는 활용성이 수(50%)를 차지하였다. 그리고 호환성 및 접근성이 35%를 차지한 것을

통해 도입전, 후 운영하면서 느끼는 중요성이 다소 상이하다는 것을 알 수 있었다. 실제 운영을 해본 후 필수사항으로 활용성이 높게 선별된 이유는 융합보안관제시스템이 과도하게 많은 기능과 인터페이스를 보유하고 있어서이다. 당장 사용하지 않는 기능요소가 많다는 것을 의미한다. 향후 증가되는 시스템들과 연동을 위해 꼭 필요한 요소이지만, 너무 많은 기능은 관리자의 관제능력을 저해할 수 있기 때문에 시스템 도입 시 자주 사용하는 중요기능 위주로 커스트마이징한 제품을 제공하고, 향후 추가되는 기능은 간편하게 적용할 수 있는 모듈식 구조 형태의 제품으로 개발해야 할 것이다.

다섯 번째, 현재 공공기관의 보안담당자들의 직군은 통신직군과 전산직군으로 구분할 수 있다. 두 직군 모두 보안과 관련된 전문가임에는 틀림이 없지만, 본연의 주 업무가 분명히 존재하고 있음으로 지속적인 보안업무 수행에 어려움이 있었다. 이에 정보보안 직군의 임용을 통해 향후 정부부처는 물론 전국 지자체 단위에 정보보안 직군의 인사배정과 임무를 부여함으로서 융합보안관제시스템의 활성화 증대를 기대함으로서 더욱 안전하고 신뢰성을 높은 대민서비스 만족도를 높일 수 있기를 기대한다.

이처럼 공공기관 도입 시 중요한 요소를 파악하기 위한 설문조사를 시행 후 분석을 통해 융합보안관제시스템의 발전방향을 도출하게 되었다. 향후 지속적으로 성장하는 융합보안관제분야의 중요한 시스템으로서 좀 더 보완하고 해결해야하는 과제들이 아직은 많이 있지만, 지속적인 기술개발은 물론 고객사별 커스트마이징을 필수요소로 인식해야 할 것이다. 특히 물리보안 분야와 정보보안 분야를 통합하여 관제하는 특성상 다양한 보안관제 시스템들의 로그정보를 모으고 분석하는 기능도 좀 더 개선되어야만 할 것이다. 결국 융합 보안관제시스템의 안정화를 통해 투자비용을 줄여서 예산절감 효과를 얻을 수 있으며, 개별로 분산 운영되어 있는 시스템들을 통합함으로서 운영의 효과성 및 관제효율성을 향상시킴으로서 전사적 관제능력을 보여줄 수 있을 것으로 기대한다.

V. 결 론

지금까지 공공기관의 보안관제 형태는 비인가자 출입통제, 차량통제, 화재감시, 중요 시설보안, CCTV카메라, 지문인식 등 의 물리적 형태의 보안 분야와 방화벽, IPS, DDoS, 바이러스월 등 정보보호를 다루는 정보 분야로 구분되어 운영하고 있다. 이 두가지 분야는 개별적으로 관제센터 및 관제실을 운영하고 있고, 관제인력 또한 개별적인 임무를 수행하고 있다. 이렇게 분산된 형태의 관제체계는 공간적, 시간적, 인력적 낭비를 초래하는바 공공기관의 특성상 가장 민감하게 요구되는 예산절감 요구에 부합되는 통합형태의 융합보안관제시스템의 도입 필요성이 최근 제기되었다. 또한, 각종 보안위협으로 인해 공공기관의 정보자산을 보호하기 위해서도 융합 보안관제시스템의 도입이 필요하게 되었다. 하지만 현재 출시되고 있는 시스템들은 아직 초기단계로서 고객사의 요구사항을 만족시키기엔 부족한 부분이 있으며, 이러한 부분들을 개선하기 위해 검증단계의 절차가 필요하게 되었다. 특히 물리보안 분야와 정보보안 분야의 관제실 운영과 관제형태가 상이함으로 인해 통합운영시 발생되는 부작용을 최소화하기 위한 기초수립계획을 세우고 활성화 방안을 마련하게 되었다.

본 논문에서는 융합 보안관제시스템 발전 방안을 도출하기 위한 기반마련을 위해 융합보안관제 산업을 파악하고 관련 정책을 조사하였으며 활성화 배경과 국내외 융합 보안관제시스템 구축사례 분석과 공공기관 보안관제 관리자 및 관련업계 종사자들의 설문조사를 통한 발전 방향 도출에 초점을 맞추어 연구를 수행하였다. 기존에 개별적으로 구축되어 운영 중이던 물리보안 분야와 정보보안 분야의 상관관계와 이해관계를 검토함으로서 융합보안관제의 패러다임의 변화를 바탕으로 한 최적의 구축방안을 마련할 수 있었다.

먼저, 공공기관 융합 보안관제시스템 도입 시 사전에 필요한 중요 요소를 파악하고 도입 시 우선시 고려할 점을 도출하여 실제 구축시 만족도를 높이기 위해 설문조사를 실시하였다. 설문조사 대상으로는 공공기관의 물리보안 관리자, 정보보안 관리자와 보안관제 전문 업체 물리보안 관리자, 정보보안 관리자 및 융합보안관제 파견관제요원들을 선정하였다. 그 결과 융합보안관제시스

템에 대한 인지도 및 운영방식에 대한 인식이 매우 부족하다는 사실을 알게 되었다. 그리고 융합 보안관제시스템 구축후 기대효과에 대한 조사에서는 대부분 긍정적인 반응을 보여 왔다. 하지만 일부 부정적인 답변을 제시한 응답자들을 대상으로 어떠한 요소가 보안위협으로부터 안전하지 못한 이유에 대한 설문을 실시하였다. 그 결과는 과반수의 응답자가 보안관제 주체가 모호하다는 지적을 하였으며, 보고체계 정립의 미흡함을 그다음 이유로 들었다. 그 외에도 관리자 책임의식 결여, 대체인력 수급문제, 대응체계 정립 미흡, 관제센터 기능 부족 등 다양한 이유가 제기되었다.

이처럼 융합 보안관제시스템 구축에 앞서 많은 관심과 우려를 동시에 가지고 있음을 알 수 있었다. 특히 도입 시 가장 고려해야 할 부분에서는 과반수가 법규 및 제도 부합여부를 제시하였고, 그다음 관리자 인식제고 부분을 제시하였다. 이를 통해 공공기관의 제한적인 업무 특성의 독특함 때문에 관련법규 및 제도가 우선 정착되어야 함을 알 수 있었다. 해당 시스템을 출시하는 여러 제조사들의 홍보자료와 카탈로그 등을 참조하였을 때에는 도입되는 모든 기관들이 매우 만족하다는 내용으로 일관하였으나, 실제 구축되어 운영중인 기관에서는 다소 상이한 응답 결과가 나왔다. 그 이유로는 현재 융합 보안관제시스템이 표준화 되어 있지 않았으며, 메가 트랜드 이슈는 분명하지만 아직 초기단계인 관계로 시행착오를 겪고 있다는 판단이 들었다. 현재까지의 연구 자료를 검토해 보아도 발전방향에 대한 의견과 가이드라인 제시일 뿐 실무자를 통한 실증분석은 부족하였다. 이에 본 연구를 통한 발전방향 제시를 통해 향후 공공기관에 구축될 예정인 융합 보안관제시스템의 기능 향상과 고객 만족을 위해서 사전에 충분한 검토를 이행할 수 있기를 희망한다.

끝으로 본 연구의 한계점으로는 융합보안관제란 용어가 생소함으로 인해 선행연구가 부족하였고, 자료수집에 일관성이 결여되었으며 구축사례를 통한 만족도가 예상보다 부족한데서 보다 심층적인 연구를 하는데 어려움이 있었다. 하지만 다행이도 제도 정착이 몇 년밖에 않되었지만 관련제도 및 법령이 어느 정도 명확히 존재하였고, 정부기관 및 보안업계에서도 적극적인 활성화 방안을 위해 노력하는 모습을 볼 수 있어서 향후 융합 보안관제시스템의 발전방향이 다양하게 제시되고 실현되리라는 확신을 가질 수 있었다.

참 고 문 헌

1. 국내문헌

공병석 外 (2014) 복합적 보안위협에 따른 기계경비 개선방안 연구

권대혁 (2014) 정보보안과 물리보안의 연관시나리오를 이용한 융합보안 관제 수준 향상 방안에 관한 연구

권대혁, (2014) 정보보안과 물리보안의 연관시나리오를 이용한 융합보안 관제 수준향상 방안에 관한 연구

김경탁 (2010) 기계경비시스템의 발전방안에 관한 연구

김민수 (2011) 보안환경변화에 따른 융합보안 발전방향, 경기대학교 석사 논문

김민수 (2012) 보안환경변화에 따른 융합보안 발전방향

김민준 (2010) 정보보안 거버넌스 프레임워크에 관한 연구

김영진 (2010) 국가 정보통신망에 대한 체계적인 보안관제 수행을 위한 모델 연구

김정덕 外 (2009), 융합보안의 개념 정립과 접근방법, 정보보호학회지 제 19권 제 6호 2009, pp.68~74

남기효 (2014) 개인정보보호기술의 최신 동향과 향후 전망

노경민 (2014) mVOIP 융합서비스 활용전략에 관한 연구

문정민 (2014) 융합기술을 활용한 스마트그리드 촉진전략에 대한 연구

박성주 (2012) 개인정보 유출방지를 위한 SRI(Security Risk Indicator) 기반 모니터링 시스템 개발

안황권 (2011) 시큐리티 환경변화에 따른 융합보안의 대두와 물리보안업체의 대응

우강섭 (2012) 우리나라의 u-헬스 서비스의 인지도 및 전략에 관한 연구

우광제 (2015) 융합보안전문가의 핵심과업 및 직무역량 요구분석

윤인수 (2007) 내부자에 의한 정보유출 방지를 위한 보안시스템 구축에

관한 연구
이기혁 外 (2009) 내부정보 유출 징후 분석을 통한 유출방지체계 구축에 관한 연구
이대성 外 (2010) 정보유출 방지 연구기술 동향 ??정보보호학회논문지, 제 20 권, 제 1 호??
이동휘 (2011) 융합보안관제시스템 개선에 관한 연구
이재명 (2013) 보안관제 위탁운영의 감리 방안에 관한 실증적 연구
이창무 (2011) 산업보안의 개념적 정의에 관한 고찰
이창훈 (2010) 기밀유출방지를 위한 융합보안 관제 체계
이현도 (2012) 공공분야 보안관제 업무에 대한 평가지표 개발 연구
임명성 (2014) 융합보안 강화를 위한 정보보안 정책 효과성 측정도구 개발
장항배 (2009) 내부정보유출방지 관점에서의 보안수준 평가
장희선 (2014) ICT 융합 서비스 키워드 트렌드 분석
전정훈 (2012) 보안 프로그램의 취약성 및 문제점에 관한 연구
정병수 (2009) 산업보안의 연구경향 분석 [한국치안행정논집] 9권 베2호 195 ~ 215p
정진욱 (2001) 정보보안 기술을 이용한 공항 보안 시스템 구축 방안에 관한 연구
정진홍 外 (2011) 융합보안에 있어서 스마트폰 기능의 과학적 적용에 관한 연구
채승엽 (2013) 스마트카 분야의 융합보안 시장 전망
최인호 (2014) 융합보안과 연계한 기계경비산업 발전방안에 관한 연구
최인호 (2014) 융합보안을 연계한 기계경비산업 발전방안에 관한 연구
최정일 (2014) 지식정보보안 산업의 현황과 전망
최진묵 (2010) 융합보안시장 동향 보고
하옥현 (2009) 산업보안을 위한 융합보안관제시스템에 관한 연구
한종욱 (2010) 융합보안기술 현황 및 전망, ETRI
허 진 (2014) 사물인터넷(IoT) 융합비즈니스 촉진전략에 대한 연구
황규현 (2014) 중소기업 융합교류 특성과 기술사업화

황동욱 (2014) 융합보안관제환경을 위한 아키텍처 구축 및 활용 방안에 대한 연구

황원식 外. (2014) 사물인터넷 시대 안전망, 융합보안산업 ??e-KIET 산업경제정보??

2. 국외문헌

AESRM (The Alliance for Enterprise Security Risk Management) (2010)

Bejtlich book Foreword by Ron Gula (2004)

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

J.P.Freeman, "The 2008 U.S Converged Security/IT system Market"

McAfee 연구소 (2014) www.mcafee.com/November2014ThreatsReport 2015년 보안 위협 전망

Nicole S. Latimer-Livingston (2007)

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.

RichardBejtlichForeword by Ron Gula.“TheTAO ofNetwork Security Monitoring: Beyond Intrusion Detection”. Addison -Wesley,2004.

ScaletS.D (2005)

The Open Security Exchange (OSE) (2007)

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

Watson, James. “Physical and IT Security MustGo Together.” Computing, May 4, 2005.

3. 단행본 및 기타문헌

『금융기관의 업무위탁 등에 관한 규정』, 금융위원회고시 제2013-18호,
21세기 산업보안론 (2009) 진영사
국가사이버안전매뉴얼 (2015) 국정원
국가정보보호백서 (2013) 안전행정부
국가정보보호백서 (2014) 안전행정부
국가정보보호백서 (2015) 안전행정부
국가정보원 (2013)『국가사이버안전관리규정』대통령훈령 제316호
국가정보원 (2015)
국정원 산업기밀보호센터 (2015), 끝나지 않은 위협, 경제안보
기업 정보보안 가이드 2013 v.8 (2013) 화산미디어
미래창조과학부 (정보보호정책과),『정보통신기반 보호법』
산업기술 보호론 (2013) 성문사
산업보안 이론 (2013) 성문사
산업자원부 (2008) "지식정보 보안 산업" 발전전략
산업통상자원부(2012)
삼성SDS 저널 (2013)
삼성경제연구소 (2015) SERI.org
스마트 시대 정보봉 전략과 법 제도 (2011) 한국학술정보
예선당 (2009) 산업보안 이대로 좋은가
월간시큐리티월드(2015)
이글루시큐리티 융합보안연구소 (2015)
전 세계 기술규격 사전인 ASIS(AmericanSociety forInformationScience)
정보보안의 이해 (2012) BJ퍼블릭
정보보호의 살아있는 역사 (2007) 한국정보보호진흥원
정보통신산업진흥법 제32조제1항
조현숙 (2013), 한국전자통신연구원 사이버융합보안연구단장

(주)메트로컴넷 부설 ICT연구소 (2011) 정보보호시스템을 이용한 네트워크 연동 및 관리시스템 구축

(주)메트로컴넷 부설 ICT연구소 (2015) 스마트 모바일 융복합 보안 관제시스템 구축

지식경제용어사전 (2015) 산업통상자원부

지식정보보안산업 발전전략 (2008) 지식경제부

최진묵 外. (2010) 융합보안시장 동향 보고 ??Samsung SDS Vol.7 / No.2W??

특허청 (2014), 물리, 융합보안 산업 IP 경쟁력 제고방안

한국인터넷진흥원 (2011) 2010 정보보호 실태조사(기업편)

한국정보통신기술협회 (2015) www.tta.or.kr

4. Web Site

ADT캡스 : www.adtcaps.co.kr

SK인포섹 : www.skinfosec.com

삼성테크윈 : www.samsungtechwin.co.kr

시큐아이 : www.secui.com

에스원 : http://www.s1.co.kr

윈스 : www.wins21.co.kr

이글루시큐리티 : wwww.igloosec.co.kr

인콘 (구 윈포넷) : www.win4net.com

케이에스아이 : www.itksi.com

한국정보통신기술협회 http://word.tta.or.kr

부 록

【설 문 지】

안녕하십니까?

먼저 바쁘신 중에도 설문에 응해주심에 감사의 말씀을 드립니다.

저는 한성대학교 지식서비스&컨설팅 대학원 융합기술학과에서 “융합 보안관제시스템 발전 방향에 대한 연구”를 주제로 석사학위 준비를 하고 있습니다.

본 설문은 전세계적으로 큰 이슈가 되어 메가트랜드로 급부상중인 “융합보안 산업”의 분야중 “융합 보안관제시스템”의 활성화를 위해 현재의 문제점을 파악하고 개선점을 도출함으로서 향후 국가산업으로 발전할 융합보안산업의 중요한 척도로서 활용가치가 있는 발전방향 제시를 위해 작성되었습니다.

또한 본 설문은 융합보안관제 산업의 활성화를 위해 필요한 정부정책 및 발전방향 모델을 제시함으로서 전세계적으로 IT 강국으로서 전세계적으로 지속적으로 선도할 수 있는 기반을 마련에 도움이 되고자 합니다.

본 설문을 통해 수집된 정보는 비밀을 유지하고 통계 목적으로만 활용될 것이며, 본 연구목적 이외의 다른 용도로는 절대 사용하지 않을 것임을 약속드립니다.

귀하께서 답변하신 내용들은 모두 귀중한 연구 자료로 이용 될 것이므로 가능한 성실한 응답을 부탁드리며, 빠진문항 없이 답변해주시길 부탁드립니다.

문항은 총 25개 문항으로 되어 있으며, 작성을 완료 하시는데 10분정도 소요될 것입니다.

본 설문조사에 협조해 주심에 다시 한 번 깊은 감사를 드립니다.

2015년 6월

한성대학교 지식서비스&컨설팅대학원 융합기술학과

지도교수 : 조 세 홍

연 구 자 : 원 종 혁

연 락 처 : 010-3950-7199

arisulove@nate.com

1. 다음 은 일반사항에 관한 내용입니다. 일치하는 곳에 √ 체크를 해주시기 바랍니다.

1.1 귀사(기관)의 주요 업종은 어떻게 되십니까?

① 정보통신(정보보호)
② 전자, 전기, 계측
③ 기계
④ 연구소
⑤ 공공기관
⑥ 기타

1.2 귀하의 직무는 어떻게 되십니까?

① 경영기획부서 (기획, 홍보, 마케팅)
② 경영관리부서 (인사, 노무, 재무)
③ 연구개발부서
④ 생산기술부서
⑤ 품질부서
⑥ 기타

1.3 귀하의 근무연수는 어떻게 되십니까?

① 1년 이하
② 1년이상 ~ 5년이하
③ 5년이상 ~ 10년이하
④ 10년이상 ~ 15년이하
⑤ 15년이상 ~ 20년이하
⑥ 20년 이상

1.4 귀사(기관)의 종업원수(인력규모)는 어떻게 되십니까?

① 10명 미만

② 10명이상 ~ 50명 미만
③ 150명 이상 ~ 100명 미만
④ 100명 이상 ~ 200명 미만
⑤ 200명 이상 ~ 500명 미만
⑥ 500명 이상

2. 다음은 융합보안관제 인지도에 관한 내용입니다. 중요도에 대한 설문으로서 귀하의 의견과 일치하는 곳에 √ 체크를 해주시기 바랍니다.

2.1 융합보안관제에 대해 잘 알고 계십니까?
① 전혀 모른다.
② 대체로 모른다.
③ 보통이다.
④ 대체로 알고 있다.
⑤ 매우 잘 안다.

2.2 융합 보안관제시스템에 대해 잘 알고 계십니까?
① 전혀 모른다.
② 대체로 모른다.
③ 보통이다.
④ 대체로 알고 있다.
⑤ 매우 잘 안다.

2.3 융합 보안관제시스템에 대해 언제 처음 알게 되었습니까?
① 1년 이내
② 1년 이상 ~ 2년 이내
③ 2년 이상 ~ 3년 이내

④ 3년 이상 ~ 4년 이내

⑤ 4년 이상

2.4 현재 융합 보안관제시스템이 구축되어 있습니까?

① 전혀 아니다.

② 대체로 아니다.

③ 보통이다.

④ 대체로 그렇다.

⑤ 매우 그렇다.

2.5 융합 보안관제시스템 구축이 귀사(기관)의 보안성 향상에 도움이 될것으로 생각하십니까?

① 전혀 아니다.

② 대체로 아니다.

③ 보통이다.

④ 대체로 그렇다.

⑤ 매우 그렇다.

2.6 융합 보안관제시스템 구축후 보안침해 위협으로부터 안전해질 것이라고 생각하십니까?

① 전혀 아니다.

② 대체로 아니다.

③ 보통이다.

④ 대체로 그렇다.

⑤ 매우 그렇다.

2.7 융합 보안관제시스템 구축후 보안침해 위협으로부터 안전하지 않을것이라는 이유는 무엇이라고 생각하십니까?

① 보고체계 정립 미흡

② 보안관제 주체 모호
③ 관제센터 기능 부족
④ 대응체계 정립 미흡
⑤ 대체인력 수급 미달
⑥ 책임의식 결여

2.8 융합 보안관제시스템 구축이 귀사(기관)에 꼭 필요하고 생각하십니까?
① 전혀 아니다.
② 대체로 아니다.
③ 보통이다.
④ 대체로 그렇다.
⑤ 매우 그렇다.

3. 다음은 융합보안관제시스템 도입시 고려해야 할 사항에 관한 내용입니다. 귀하의 의견과 일치하는 곳에 √ 체크를 해주시기 바랍니다.

3.1 융합 보안관제시스템 도입시 가장 중요하게 생각하는 부분은 어떤것입니까?
① 효율성 (도입비용 및 유지관리비용)
② 신뢰성 (레퍼런스)
③ 호환성 (커스트마이징)
④ 접근성 (GUI)
⑤ 활용성 (DB연동)
⑥ 가용성 (성능)

3.2 융합 보안관제시스템 도입시 우선 고려해야할 사항은 어느부분이라고 생각하십니까?

① 보안인증 기준
② 레퍼런스
③ 특허기술 취득 유무
④ 기존 관제시스템들과의 호환성
⑤ 관리자 운용성 (GUI)
⑥ 기타

3.3 융합 보안관제시스템 도입시 가장 고려해야할 부분은 무엇이라고 생각하십니까?
① 표준화
② 기술개발
③ 보안등급
④ 법규, 제도 부합
⑤ 관리자 인식제고
⑥ 운영자 교육수준

4. 다음은 융합 보안관제센터 운영실태에 관한 내용입니다. 귀하의 의견과 일치하는 곳에 √ 체크를 해주시기 바랍니다.

4.1 보안관제센터 근무 년수는 어떻게 되십니까?
① 1년 이내
② 1년 이상 ~ 2년 이내
③ 2년 이상 ~ 3년 이내
④ 3년 이상 ~ 5년 이내
⑤ 5년 이상 ~ 10년 이내
⑥ 10년 이상

4.2 보안관제센터는 어떤 형태로 운영되고 있습니까?

① 물리보안센터와 정보보안센터 개별운영

② 물리보안센터만 운영

③ 정보보안센터만 운영

④ 물리보안센터와 정보보안센터 통합운영

⑤ 둘 다 운영하지 않는다

4.3 융합보안업무중 어느 분야가 중요하고 우선시 되어야 한다고 생각하십니까?

① 물리적 보안 분야

② 정보보안 분야

③ 둘 다

④ 이슈 발생 시 상황에 따라 다르다

4.4 융합보안관제센터는 운영방식중 어느분야가 중심이 되어 운영중이라고 생각하십니까?

① 물리보안센터

② 정보보안센터

③ 둘 다

④ 둘 다 해당없음

⑤ 이슈 발생시 상황에 따라 다르다

4.5 융합보안관련 기술력 습득은 어떤 매개체를 통한 교육이 가장 좋다고 생각하십니까?

① 외부 교육기관

② 사내 교육과정

③ 세미나 (컨퍼런스 등)

④ 외부강사 초빙

⑤ 전문서적 및 연구결과 보고서 참고

⑥ 기타 (독학 등)

4.6 융합보안관련 교육을 받으셨다면 어떤 매개체를 통해 받으셨습니까? (중복체크 가능)

① 외부 교육기관

② 사내 교육과정

③ 세미나 (컨퍼런스 등)

④ 외부강사 초빙

⑤ 전문서적 및 연구결과 보고서 참고

⑥ 아직 받지 못함

4.7 융합보안관련 교육 내용이 충분하다고 생각하십니까?

① 많이 부족하다

② 다소 부족하다

③ 보통이다

④ 대체로 만족한다

⑤ 매우 만족한다

4.8 융합 보안관제시스템 보수교육은 년간 몇회를 받으셨습니까?

① 1회

② 2회

③ 3회

④ 4회

⑤ 5회 이상

⑥ 받지 않았다

5. 다음은 융합 보안관제시스템 기능에 관한 내용입니다. 귀하의 의견과 일치하는 곳에 √ 체크를 해주시기 바랍니다.

5.1 현재 융합 보안관제시스템이 도입 되어 있습니까?

① 도입 완료
② 곧 도입 예정
③ 향후 도입 예정
④ 도입 검토중
⑤ 도입계획 없음

5.2 융합 보안관제시스템 기능중 무엇이 가장 중요하게 활용되고 있습니까 ?

① 효율성
② 가용성
③ 확작성
④ 내구성
⑤ 기능성

5.3 융합 보안관제시스템 기능중 개선이 필요한 분야는 무엇이라고 생각하십니까?

① 오탐기능 개선
② 용량 확충
③ 처리속도 향상
④ GUI 표현 개선
⑤ 알람기능 개선
⑥ 레포팅 기능 개선

ABSTRACT

A Study on Methods to Encourage the Implementation of Integrated Security Control Systems

- with a Focus on Public Organizations -

Won, Jong-Hyuk
Major in IT Integration
Dept. of Convergence Technology
Graduate School of Knowledge Service Consulting
Hansung University

Due to the rapid development of IT technology in modern times, as new social circumstances and cultures emerge, the integration of various industries is taking place. The value of information assets has seen an accompanied increase with this phenomenon followed by a dramatic increase in damaging cases of information leakage and security related breaches. In order to address such changes in the information age frontier, there is a need for appropriate changes to the security systems in the security industry. Previous security threats were limited to the physical domain such as access by unauthorized personnel and vehicles, monitoring of fires, and the restriction of main security facilities, but recently there has been an increase in damagse from intelligence crimes such as cyber attacks in the form of hacking, the overloading of core

security systems, and breaches and leaks of sensitive national intelligence and core technology source code etc.

The threat against security grows larger day by day, and in moving away from security implemented through physical measures and to protect against these diverse threats, there is an increase in interest to implement integrated security type security control systems that are dedicated to information security. But governments and specialized security control corporations still have yet to establish clear policies and guidelines, and in the case of a security related accident, due to the lack of active reactionary measures, the reality of the state of security cannot help but leave our systems exposed to security threats.

This research takes the perspective not of the supplier for the recently trending implementation of integrated security control systems, but approached this issue from the perspective of the demanding customer, and through analyzing government policies and guidelines through previous research, and by determining the needs of the customer and the limitations of the systems through case studies on actual implementations of security solutions, and finally, based on survey research of hands on system administrator and professionals in related industries, the problematic issues and potential suggestions for integrated security control systems were deduced.

The research was conducted towards public organizations that had implemented integrated security control systems, and it was determined that there was a difference between the customer evaluations included in the marketing materials of companies related to supplying the implementations of integrated security control systems and the customer evaluations of satisfaction surveys, and based on this difference, a guideline for the improved implementation of integrated security control systems and their customization is provided.

In order to complement previous research with empirical analysis that

had not been included, verification based on interviews with hands on systems administrators and research surveys was conducted. The survey targets were systems administrators of public organizations and hands on personnel of related companies, and through the interviews and research surveys new suggestions were able to be deduced. It was first proposed that there needs to be an improvement on the recognition of integrated security control systems, and when implementing integrated security control systems, it was proposed that the most important consideration to make is whether or not the system is compliant with related laws and policies.

Differences between the requirements by the organization implementing the integrated security control system and the supplier were discovered, which were caused due to the lack of standardization, and it was possible to determine that the integrated security control system industry was currently in the early stages of implementation and going through a mild trial and error stage.

Based on the results of this research, it was possible to present clearer standards for the future implementation of integrated security control systems and also to establish guidelines for an active integrated security system framework, and by having public organizations lead the way as best practice and implementation cases of integrated security control systems, this research has the objective of contributing to improving the status of Korea both in name and practice as a globally recognized Information Technology superpower.

[Keywords] integrated, physical security, information security, security control system, intelligence information security, integrated security control center, integrated security control system

감사의 글

대학원 생활을 시작한지가 엊그제 같은데, 어느덧 시간이 흘러 2년의 시간이 흐르고 석사 과정을 마무리하는 시간이 다가왔습니다. 먼저 본 논문이 완성되기까지 자상한 격려로 이끌어 주신 존경하는 조세홍 교수님께 감사의 말씀을 드립니다. 그리고 지난 2년동안 한결같은 믿음으로 이끌어 주신 존경하는 임욱빈 교수님께 진심으로 깊은 감사를 드립니다. 또한 바쁘신 일정 속에서도 기꺼이 시간을 내주시어서 논문을 심사해 주신 노광현 교수님께 감사의 말씀을 드립니다.

논문을 무사히 마칠 수 있도록 도움을 주신 지식서비스&컨설팅연구원 분들께 감사를 드립니다. 특히 바쁜 업무 중에도 우리들의 학사일정과 행사를 늘 챙겨주신 김봄시내 연구원님, 조민수 연구원님, 조민정 연구원님, 박소민 연구원님, 그리고 융합기술학과 동기이며 언제나 일심동체로 의기투합했던 평생 있지 못할 우인형님, 병희형님, 황용형님, 경기형, 정훈이형, 원일이형, 태원, 성민, 문봉이에게 진심으로 고마움을 전합니다. 저희학과 선배로서 아낌없는 조언을 해주신 임은희, 허진, 문정민 선배님, 대학원 생활에 큰 도움을 주셨던 지식서비스&컨설팅학과 이명원 팀장님, 이영성 계장님께 깊은 감사의 말씀을 드립니다. 그리고 원우회 사무국장 임무를 병행하면서 힘든 가운데에서도 대학원 생활의 추억을 남겨주신 이철규회장님, 박남규회장님, 김봉수회장님, 윤혜란국장님, 그 외에도 교육대학원 최숙현회장님, 뷰티예술대학원 박지수회장님, 경영대학원 유승철회장님, 부동산대학원 유재욱회장님, 행정대학원 김근래회장님, 모든 분들께 감사의 말씀을 드립니다. 여러분들의 많은 도움이 있었기에 논문통과라는 큰 기쁨을 얻을 수 있었습니다.

그리고 회사업무와 학교생활을 병행하느라 일에 소홀함이 있었는데도 제 업무를 많이 도와주시고 아낌없는 지도와 격려를 해주신 부설 ICT 연구소장님, 항상 인생의 올바른 길의 표본을 보여주시며 인격적으로 이끌어주신 최요한

팀장님, 제가 바쁠 때마다 업무적으로 큰 도움을 주신 김호진 차장님, 본인의 바쁜 박사과정 중에서도 오히려 나의 논문 완성을 도와주기 위해 귀중한 시간을 할애해준 멋있는 후배 은섭이, 또한 논문 준비하면서 바쁜 와중에도 내가 힘들 때 마다 큰 위로를 해준 시립대학교 원서연 박사님, 특히 회사에 입사한 후 지금까지 14년이 넘도록 저를 칭찬해주시고 늘 관심가지며 독려해주시고 위로해주신 존경하는 최선민 대표이사님, 이상철, 홍성재, 김은겸 전무이사님께 깊은 감사의 말씀을 드립니다. 아울러 바쁠 때 업무의 빈자리를 메워준 회사 관계자 모든 분들께 감사를 드립니다.

오늘이 있기까지 언제나 기도로 잘되길 기원해주신 사랑하는 아버지, 어머니, 늘 부족한 사위지만 언제나 친아들처럼 대해주시고 자랑스러워 해주시는 장인어른, 장모님께 깊은 감사의 말씀을 드립니다. 멀리 미국에서 박사논문 준비하느라 바쁜 가운데도 늘 기도와 염려를 해주는 종유와 매제, 조카인 주열이와 주담이, 그리고 언제나 우리가족과 함께 기쁨과 슬픔을 나누며 신경써주고 챙겨주는 고마운 큰 처제와 큰동서, 조카 민지와 연수, 작은 처제와 작은동서, 조카 경준이와 유리, 저 멀리 광양에서 주경야독하며 늦은 나이지만 더 높은 꿈을 향해 노력하는 멋진 처남 수하와 처남댁, 조카 윤슬이, 그리고 남편과 자식 뒷바라지를 해주면서 힘들어도 언제나 따뜻한 말로 감싸주고 자랑스러워 해주며 끝까지 믿어준 사랑하는 아내 박선하, 아빠의 바쁜 회사일과 학교생활로 함께 있어줄 시간이 부족해서 늘 마음에 걸렸는데, 오히려 아빠가 늦은 밤 논문 쓰는데 수고하신다며 기운내시라고 웃으며 나를 격려해 주던 듬직한 아들 세연이와 함께 이 기쁨을 나누고 싶습니다.

– 6월 어느 늦은밤 낙산공원에서 –

2015년 6월
원 종 혁