특집 05

빅 데이터(Big Data)를 활용한 물리보안의 변화 현상

손상철 (대한시큐리티연구소)

목 차

1. 서 론
2. 빅 데이터에 대한 이해
3. 물리보안의 이해와 빅 데이터 활용
4. 결 론

1. 서 론

빅 데이터(Big data)를 이용한 생활 속의 사례의 한 가지인 SK텔레콤의 'T map'을 이용하여 실시간으로 빠른 길의 안내를 받으며 특정한 장소로 이동한 경험이 있을 것이다. T map 서비스는 위성항법장치(GPS)가 장착된 콜택시, 고속버스, 기업용 렌터카, 유류 운반차량 등이 수집한 전국 도로의 교통정보를 바탕으로 실시간 빠른 길을 안내하는 시스템이다. 약 5만여 대의 차량이 5분 단위로 알려오는 실시간 정보를 활용하여 가장 빠른 도로를 안내하니 도착 예상 시간도 상당히 정확한 편이라 할 수 있다.

2012년 다보스포럼(세계경제포럼・WEF)에선 '2012년 떠오르는 10대 기술' 중 첫 번째 기술로 빅 데이터가 지목되었다. 또 다보스포럼은 '빅 데이터, 빅 임팩트(Big Impact):국제 발전을 위한 새로운 가능성'이란 보고서에서 "연구자들과 정책 결정자들은 이 데이터의 홍수를 실행력 있는 정보로 바꿀 수 있는 잠재력을 깨닫기 시작했다"며, "이 정보는 저소득층의 요구를 파악하고 그들에게 서비스를 제공하거나, 위기를 예측·예방하는 데 쓰일 수 있다"고 언급하였으며, 2018년 현재에 있어서는 4차 산업을 선도하는데 매우 중요한 역할을 하고 있다.

예전에도 공공부문의 각종 통계에서부터 기업의 시장조사 보고서나 판매 현황에 이르기까지 체계적으로 분류·저장된 정보들은 많았다. 하지만 빅 데이터 분석과 활용이 이런 기존의 데이터 처리와 차별화되는 것은 자연언어 텍스트, 사진, 음악, 동영상, 위치정보 등 정형화하지 않은 데이터까지 분석 대상으로 삼아 의미를 찾아낸다는 점이다.

다양한 가치를 위해서 활용할 수 있는 빅 데이터를 21세기 화두라고 할 수 있는 '안전(安全)'을 위한 효율적인 활용적 측면에서 접근해보고자 한다. 기존에 발표된 논문, 보고서, 정책자료, 관련 교재를 토대로 작성하였으며, 빅 데이터에 대

한 이해를 통하여 안전관련 산업인 민간보안산업의 한 축인 물리보안과 빅테이터, 범죄 및 재난으로부터의 안전을 위한 빅 데이터 활용에 대하여 살펴보고, 마지막에서는 4차 산업의 중심축인 빅 데이터를 활용하면서 경계해야 할 점에 대해서 제시하고자 한다.

2. 빅 데이터에 대한 이해

4세대 무선 이동통신 기술의 발달로 인하여 유비쿼터스 및 장착형 컴퓨터, 인터넷, 클라우드 컴퓨팅, 소위 SNS라고 불리우는 소셜네트워크서비스가 확산되면서 빅 데이터는 더 이상 간과할 수 없는 존재가 되었다.

빅 데이터란 일반적으로 대량의 '데이터 군'으로서 기존의 일반적인 기술로는 관리하기 곤란한 방대한 양의 데이터로 수십 테라바이트에서 수페타바이트 정도라고 표현할 수 있다. 물론 기술이 점차 발달함에 따라 이 수치는 더욱더 증가될 것으로 보인다.

빅 데이터는 '데이터양'외에도 인터넷의 텍스트 데이터, 위치정보, 동영상 등 다양한 데이터를 바탕으로 한 관계형 데이터베이스의 구조화되지 않은 데이터로 유용한 지식을 얻을 수 있는 '다양성'과 시시각각으로 변화하고 발생하는 데이터에 대한 분석처리인 '속도'의 중요한 요소로 지니고 있다. 이처럼 빅 데이터는 넓은 의미에서의 소위 3V(데이터 양(volume), 다양성(variety), 속도(velocity))를 포함하여 데이터를 축적하고 처리하고 분석하는 기술과 인재와 조직을 포함하기도 한다. 그리고 좁은 의미로는 개인과 밀접한 관계가 있는 구체적인 데이터를 활용하는 것이라고 일컫는다.

3. 물리보안의 이해와 빅 데이터 활용

3.1 보안의 구분

보안(security)이란 사전적인 의미로 어떤 위협으로부터 안전을 유지한다는 뜻이다. 안전(safety)은 위험하지 않거나, 위험이 없는 상태를 의미한다. 따라서 보안이라 함은 위험, 손실 및 범죄가 발생하지 않도록 방지하는 상태를 가리킨다.

3.1.1 물리보안

물리보안(physical security)의 정의를 위키피디아 백과사전에서 찾아보면 "물리적으로 정보, 인명, 시설을 보호하는 것을 의미하며, 이는 인가자 및 비인가자의 출입관리, 천재지변으로부터의 시설보호, 방범관리 등 모든 물리적 위협에 대해 보안을 지키는 것을 의미한다. 국내에도 물리보안 전문 업체가 여럿 있으며, 도난 예방중심으로 보안활동을 하고 있다."라고 기술되어 있다. 보다 구체적인 물리보안은 범죄 등 고의적 위협(threat)으로부터 인명, 정보, 시설 등 자산(asset)을 보호하기 위해 물리적 취약성(vulnerability)을 통제하는 활동이다. 그 통제수단은 건축물이나 보안관련 설비 등의 구조적(structural) 요소, 보안시스템 등의 전자적(electronic) 요소와 보안요원 등의 인적(human) 요소로 구성된다."

3.1.2 정보보안

정보보안(information security)이란 "정보의 수집, 가공, 저장, 검색, 송신, 수신 도중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적, 기술적 방법을 의미한다. 정보보안을 위해서는 물리적인 방법과 비(非)물리적인(소프트웨어적인) 방법이 사용될 수 있다. 물리적인 방법 중 대

표적인 것은 자물쇠의 사용이나 보초의 활용 등을 들 수 있으며, 비물리적인 방법 중 대표적인 것은 암호화 기술을 사용하는 것이다."로 정의되어 있다.

3.1.3 융합보안

융합보안(convergence security)이란 물리보안과 정보보안을 융합한 보안 개념으로, 각종 내·외부적 정보 침해에 따른 대응은 물론 물리보안 장비 및 각종 재난·재해 상황에 대한 관제까지를 포함한다. 미래에는 물리보안과 정보보안의 구분이 없이 통합보안(total security) 개념으로 안전과 안심을 추구하는 방향으로 진행될 것으로 예상한다.

3.2 보안시장의 규모

최근 안전위협 요인의 증대, 보안의식의 증대, 보안기술의 첨단화로 보안 분야에 대한 시장이 날로 확대되고 있다. 각종 시장분석 자료를 종합해 보면 향후 2020년까지의 보안시장 규모는 〈표 1〉과 같이 예측하고 있다. 2020년경 기계경비 분야는 전 세계 시장규모가 98조 원, 국내시장 규모는 약 2.1조 원으로 예상하며, 인력경비 분야는 각각 191조 원과 2조 원, 기타 서비스 분야는 81조 원과 0.3조 원으로 예상한다. 기타는 현금호송 등의 서비스를 포함한 내용이다. 시스템에 의한 기계경비 분야는 인력경비 분야와 비교하면 세계시장 규모는 작지만, 국내는 거의 동등한 수준의 시장규모로 예상한다.

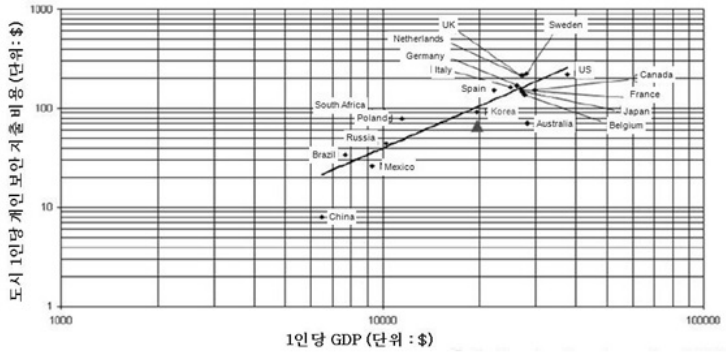
선진국일수록 시스템에 의한 기계경비에 대한 수요가 높음을 알 수 있다. (그림 1)에서와 같이 1인당 GDP가 큰 나라일수록 1인당 월평균 보안지출비용이 더 높다. 미국, 영국, 스웨덴과 같은 선진국은 개인 1인당 보안지출비용이 약 $200으로 제일 높으며, G7 국가들은 대부분 $150 정도 지출한다. 한국은 보안지출비용이 약 $100 이하로 선진국과 비교하면 여전히 적은 비용을 지출

〈표 1〉 년도별 보안시장 규모

(단위 : 兆 원)

구분	분야		2010년	2015년	2020년
물리보안	보안서비스	기계경비 (국내)	46(1.2)	67(1.6)	98(2.1)
		인경비 (국내)	93(1.3)	133(1.6)	191(2.0)
		기타 (국내)	41(0.2)	58(0.2)	81(0.3)
		계 (국내)	180(2.7)	258(3.4)	370(4.4)
	보안솔루션	출입통제 (국내)	11(0.4)	24(0.6)	56(1.1)
		영상감시 (국내)	30(0.4)	50(0.5)	80(0.8)
		침입감지 (국내)	2(0.3)	3(0.5)	4(0.8)
		계 (국내)	43(1.1)	77(1.6)	140(2.7)
	계 (국내)		223(3.8)	335(5.0)	510(7.1)
정보보안	서비스 (국내)		36(0.2)	78(0.3)	172(0.5)
	솔루션 (국내)		34(0.8)	56(1.1)	94(1.8)
	계 (국내)		70(0.9)	134(1.4)	226(2.3)
전체 계 (국내)			293(4.7)	469(6.4)	776(9.4)

Freedonia, Frost & Sullivan, IDC 2011년 자료



(그림 1) 1인당 GDP에 따른 도시 1인당 보안지출비용 관계

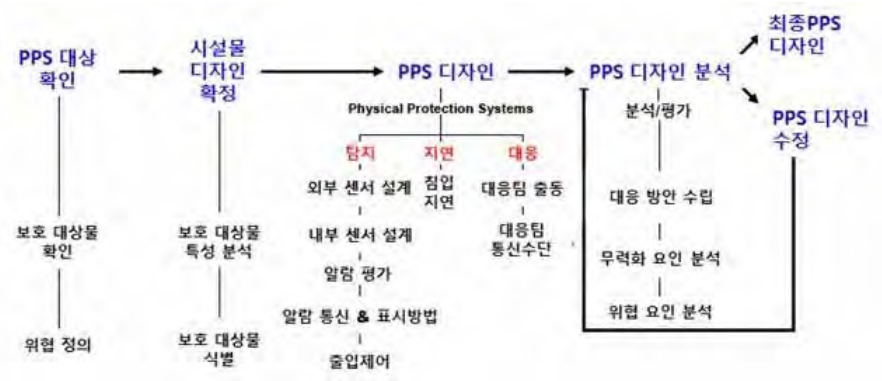
하고 있다. 반면 중국은 보안지출비용이 매우 낮은 상태이나, 향후 성장세가 가장 높을 것으로 예상한다.(The Freedom Group, Inc. 2005년)

3.3 물리보안과 범죄예방 및 손실예방

물리보안의 개념적 키워드는 물리적으로 차단하고, 침입자를 사전에 감지하고, 침입이 감지되면 즉각 퇴치하는 것이다. 선진국에서는 1960년대부터 첨단 센서를 이용한 물리보안시스템이 도입되기 시작했다. 물리보안시스템은 감시하고자 하는 주요 시설물에 적절한 센서를 설치하고, 센서들에서 발생한 이상 신호를 컨트롤러(controller)를 통해 중앙관제센터에 실시간 전송하는 시스템이다. 중앙관제센터에 이상 신호가 접수되면 각 지역에서 근무하는 순회요원에게 출동지시를 내리거나 가까운 인근 경찰서 또는 소방서에 통보하여 범죄확산의 예방 및 손실을 예방(risk prevention)할 수 있는 시스템으로 발전되었다.

3.3.1 PPS(Physical Protection System)의 이해

물리보안시스템에서 가장 중요한 역할을 하는 것이 센서(sensor)이다. 이를 위해 센서를 어떻게 설치를 해야 하는지 기준이 필요한데, 이러한 기준이 되는 것이 바로 PPS이다. PPS는 Physical Protection System의 약자이며, 번역하면 물리방호시스템이 된다. PPS 설계 프로세스는 (그림 2)



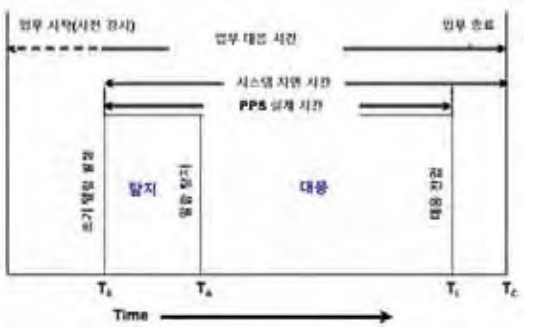
(그림 2) PPS 설계 프로세스

와 같다. 우선 보호 대상물(대부분 주요 건물 또는 핵심 시설 단지)이 정의가 되면, 대상물에 침입하는 경로인 위협을 파악해야 한다. 그 다음은 보호 대상물의 성격을 정확히 정의한 후 본격적인 디자인을 하게 된다.

PPS 디자인은 탐지, 지연, 대응이라는 3가지 기준으로 설계를 한다. 여기서 탐지 부분에서 적합한 센서를 지정하고 설치하는 작업을 하게 된다. 디자인이 끝나면 분석과 평가를 거쳐 무력화 요인 및 위협요인을 분석하여 수정을 하게 되고, 최종 이상이 없으면 PPS 디자인을 확정하게 된다.

3.3.2 PPS설계시 고려사항

PPS 설계에 있어 고려해야 할 사항은 (그림 3)과 같이 탐지 및 대응까지 소요되는 시간을 고려해야 한다는 것이다. 첫 번째 시간은 알람탐지 시간이다. 이것은 초기 알람이 발생하고, 그로부터 오보인지 실제 침입신호인지를 판단한 후 침입임을 확정하기까지의 시간이다. PPS 설계에서 가장 중요한 고려사항이 바로 알람탐지 시간이다. 이 시간을 최소로 줄이는 것이 PPS 설계의 핵심이다. 두 번째 시간은 침입으로 확정판정이 되면, 침입자에 대응할 수 있는 방안을 고려하여 최대한 빠른 시간 내에 대응이 가능하도록 시스템을 설계해야 한다. 이와 같이 알람탐지와 대응

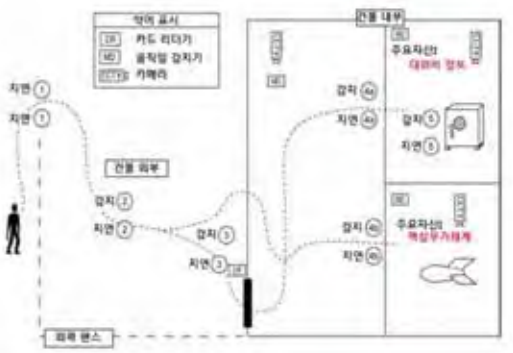


(그림 3) PPS 설계시 고려해야 할 지연 시간 정의

시간을 합친 시간이 PPS 설계시간이 된다. 그 다음 대응이 완료가 되면 업무가 종료가 되는데, 이에 소요되는 총 시간을 업무대응 시간이라 한다.

(그림 4)는 주요자산을 보유하고 있는 건물 내부와 건물을 보호하는 외곽펜스로 구성된 물리보안 시스템에서 침입자가 침입하는데 소요되는 시간을 시뮬레이션한 사례이다. 외곽펜스는 침입자의 침입을 지연시키기 위해 필요한 시설물이고, 펜스를 지난 후에 여러 종류의 장애물을 마당에 설치하여 침입자가 건물로 진입하는 시간을 최대한 지연시켜야 한다. 마찬가지로 건물 내부로 침입한 이후에도 주요자산이 있는 위치까지 침입자가 쉽게 도달하지 못하도록 각종 장애물을 설치하는 것도 중요하다.

장애물이 없는 경우, 침입자가 펜스로부터 주요자산 탈취에 소요되는 시간을 추정해 보면 〈표 2〉와 같다. 약 10분이면 외부에서 침입하여 주요자산을 탈취할 수 있다. 그러므로 센서에 의한 조기 감지도 중요하지만, 장애물을 설치하여 지연시키는 것도 물리적 보안에서 아주 중요한 항목이다.



(그림 4) PPS 디자인 사례

〈표 2〉 장애물이 없는 경우 주요자산 탈취에 소요되는 시간 추정

단계	지연 옵션	추정 지연 시간	감지 옵션
1	펜스 기어오르기	20초	PISD
2	건물외부에서 달리기 (예, 약 180m)	40초	공간감지 센서
3	문, 창문, 벽을 부수고 침입	2분	공간감지 및 진동감지 센서
4	핵심시설 부수고 침입	4분	진동감지 센서
5	주요자산 탈취	3분	공간감지 센서
총 지연 시간		10분	

3.4 물리보안과 빅 데이터의 활용

4차 산업혁명을 견인하고 있는 사물인터넷(IoT), 인공지능(AI), 클라우드, 빅 데이터 등 정보통신기술(ICT)이 영상보안 등 물리보안과 결합하며 보안시장의 근본적 변화(Deep Change)를 이끌고 있다. 기존의 방범용 CCTV가 영상을 저장하고 저장된 영상을 발생한 사고의 사후처리를 위해 사용되는데 그쳤다면, 이제는 딥러닝 기반의 AI 기술을 만나면서 사고를 예방할 수 있는 사전적 보안을 통해 더욱 안전한 사회를 만드는데 활용될 전망이다.

점차 보안의 형태는 총체적 대응이 가능한 형태로 발전하게 될 것이고, 이러한 발전에 따라 보다 다각적 위험에 대한 예측이 가능하고, 정확한 사고 징후 또한 탐지할 수 있어야 할 것이다. 이를 위해서는 물리보안, 정보보안, 방재안전, 환경안전, 유·무선 통신 이력 정보 등의 모니터링 데이터 융합과 각종 정보에 대한 상관관계, 패턴 및 이상 상황 분석 등을 통해 이루어질 수 있을 것이다.

예를 들면, 기존의 통합로그관리시스템(SIEM, Security Information and Event Management)으로부터 분석된 이상 행위자의 출문 시, 검색 요원에 의한 정밀 검색이 이루어지도록 하기 위한 시스템으로 IT보안 시스템과 물리적 보안검색 시스템과의 융합된 보안 형태로 볼 수 있다.

특히 보안 위험성이 높은 대상에 대해 보안자

(그림 5) 융·복합 보안 시스템 구성 (출처 : LG CNS)

〈표 3〉 기밀유출 대응 시나리오

기밀 유출 단계	이상 징후 탐지 방법	보안대응
경쟁사 접촉 시도 및 사전 공모	이메일 등 통신 모니터링	경쟁사 메일 도메인 송수신 등 이상 징후 예측
정보 유출 시도	정보 시스템 접근 행위, 보안 위반 이벤트 수집과 분석	① 시나리오 및 상관 분석 등을 통한 이상행위, 일탈 행위에 대한 이상 징후 포착 ② 물리적 보안 시스템 연계 알람
정보 획득 후 출문 시도	이상 징후자 출문 시 알람 이벤트 수신	출문 보안 검색 강화를 통한 유출 적발 및 차단

원을 집중하기 때문에 보안검색에 대한 효율성이 높아지게 되고, 뿐만 아니라 실시간 데이터 처리를 통해 잠재적인 보안 위험성에 대한 사후 추적이 아닌 즉각적이고 능동적인 대처가 가능하다는 점에서 효과적인 보안관리라고 할 수 있다.

최근 사례를 보면 대부분의 보안사고가 전/현직 직원의 내부 유출을 통해서 발생하고 있다. 이러한 유출사고는 보통 정당한 권한을 가지고, 정당한 업무행위로 이루어지고 있어서 적발해 내기 쉽지가 않기에 빅 데이터를 통한 여러 가지 정보들을 종합하여 통합적인 시선으로 보안의 위협을 찾아내고 예방하게 되는 것이다.

물리적 보안뿐만 아니라 모든 보안기술들이 나날이 발전하고 있으며, 새로운 보안솔루션 역시 지속적으로 생겨나고 있다. 그러나 보안 전문가인 브루스 슈나이어(Bruce Schneier)가 지적했듯이 '절대적으로 안전한 시스템이란 존재하지 않는다.'라는 사실을 잊지 말아야 할 것이다. 보안기술이 날로 발전할수록 침해 및 해킹 기술도 함께 진화하고 있기 때문이다.

3.5 물리보안과 통합관제를 통한 융합보안

전통적으로 보안은 물리보안과 정보보안으로 구분되어 따로 발전해 오는 과정에서 정보보안

(그림 6) 기술 유출의 주체 (출처 : 국가정보원 산업기밀보호센터)

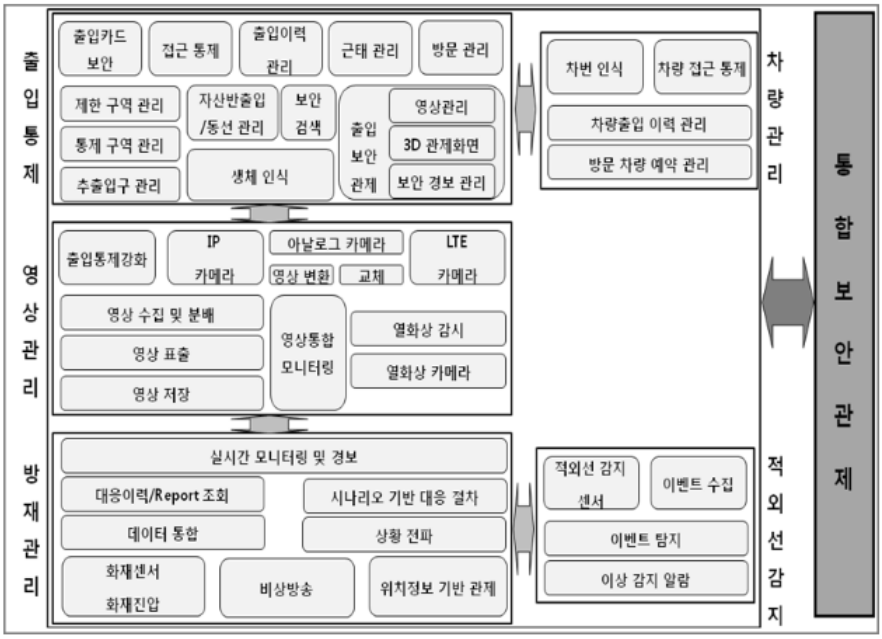
의 중요성으로 인하여 물리보안의 중요성을 낮게 보는 경향이 있었으나 물리보안의 허점으로 인하여 손실이 발생하는 사건들을 경험하면서 가장 기초가 되는 물리보안이 취약하면 다른 보안들의 안정성도 보장할 수 없다고 인식되기 시작했다.

현재 기업의 보안 니즈는 재물, 재화의 도난 방지에서 정보 자산의 유출 방지까지 확대되고 있다. 또한 사생활 보호, 건강, 환경, 에너지까지 보안을 지키고자 하는 대상으로 부각되기 시작했다. 그리고 발생 가능한 위협이 복합화된 형태로 발생하고 있다. 침입, 도난, 테러와 같은 물리보안 위협과 정보 유출, 변조, 해킹 등의 정보 보안 위협이 합쳐지고, 환경안전과 에너지 고갈 또한 신종 위협으로 등장했다.

최근 IP 카메라 등 영상 감시 시스템 및 출입관리 시스템이 TCP/IP의 개방형 네트워크를 수용하게 되면서 물리보안에도 IT가 다양하게 적용되기 시작했다. 또한 개별적인 출입통제, 주차시설관리, CCTV 영상보안 같은 물리적 보안장비에 대한 통합관리, 각종 재난· 재해 상황에 대한 관제까지 포함하는 물리보안과 정보보안이 상호 보완적으로 융합되어 통합관리 형태로의 변화가 최근의 물리보안 트렌드라고 볼 수 있다.

4. 결 론

4차 산업시대를 맞이하여 보안은 경영의 선택이 아닌 필수요소로 초기 단계서부터 보안을 고려해야 할 것이다. 즉 경영의 핵심 축으로 자리매김해야 한다. 빅 데이터가 성장세가 계속 진행되는데 무엇이든지 상상할 수 있다. 이를 테면 다양한 산업에서 적용되면서 우리의 삶이 어떻게 바뀔 것인지 다양한 상상을 할 수가 있을 것이다. 따라서 빅 데이터를 안전하게 유지하는 것에 대한 혁신적인 방안을 요구하게 될 것이다.



(그림 7) 물리보안 및 통합보안관제를 통한 융합보안의 기본 틀 구성(예시) (출처 : LG CNS)

보안은 생각하는 것보다 훨씬 넓고 포괄적이며 끊임없이 변화하며 중요하게 다가올 것이다. 그러므로 기업 및 많은 조직들이 지속적인 보안 투자와 함께 보안에 대한 관심, 적절한 대응 조치를 이해하고 있어야 할 것이다. 따라서 빅 데이터, lot, AI 등을 보안과 접목하여 언제 발생할지 모르는 손실을 예측할 수 있게 되고, 예측에 따라서 손실의 예방 가능성을 높일 수 있게 된다. 부득이 손실을 예방하지 못한 경우가 발생하게 된다면 그 손실을 최소화 시킬 수 있게 될 것이다. 결과적으로 빅 데이터 등을 보안과 효과적으로 접목시키게 되면 손실을 예방하게 되고, 손실의 예방은 새로운 생산을 의미하는 것을 주목해야 한다. 더욱이 보안은 기술적인 대책만으로 대응이 불가능한 조직의 문화와 관습에 관한 구성원의 인식문제이기 때문에 '사람' 중심의 근본적인 보안수준 개선 대책이 요구되고 있음을 간과해서 안 될 것이다.

참 고 문 헌

[1] 곽관훈, 기업의 빅 데이터(Big Data) 활용과 개인정보의 보호의 조화, (일감법학 제27호(2014)

[2] 경찰청·한국디지털포렌식학회, 디지털증거 처리 표준 가이드라, (경찰청, 2006)

[3] 국립재난안전연구원, 소셜 빅데어터 재난관리 운영방안 및 이슈 탐지기법 연구, (국립재난안전연구원, 2013)

[4] 권건보, 개인정보보호와 자기정보통제권, (경인문화사, 2005)

[5] 권오걸, 스마트 형법각론, (형설출판사, 2011)

[6] 김대호·김성철·나은영·심용운·이상우·이재신·장병희·진달용·최선규·최준호, 소셜미디어, (커뮤니케이션북스, 2012)

[7] 김용수, 리스크 커뮤니케이션. (씨앤아이북스, 2012)

[8] 김은미·이동후·임영호·정일권, SNS혁명의 신화와 실제, (나남출판사, 2011)

[9] 미래전략연구본부 재난관리연구실, 빅데이터와 재난관리, (한국행정연구원, 2013)

[10] 손상철외, 재난안전관리론(도서출판 진영사, 2018)

[11] 옥진아. 진창종, 빅데이터로 경기도의 안전을 지킨다, 2015

[12] 윤평중, '災難 유토피아'에서 희망을 꿈꾸다, (조선일보, 2014)

[13] 이예림, 국가재난안전정책과 향후계획, (안전행정부 안전관리본부, 2013)

[14] 이재현, 빅 데이터와 사회과학: 인식론적, 방법론적 문제들, 커뮤니케이션

[15] 이진형, 데이터 빅뱅, 빅 데이터의 동향, (Journal of Communications & Radio Spectrum, 2013)

[16] 이창범, 개인정보보호법제 관점에서 본 빅 데이터의 활용과 보호방안, 법학논총 제37권 제1호, 2013)

[17] 정용찬, 빅 데이터, (커뮤니케이션북스, 2013)

[18] 정지형· 김강훈, 한국과 미국의 공공부문 빅 데이터 활용 현황 분석, (한국정보과학회, 2012)

[19] 방송통신위원회, 스마트워크 활성화 추진계획, 2012

[20] 정용찬. 빅데이터 혁명과 미디어 정책 이슈(KISDI Premium Report 12-02). (정보통신정책연구원. 2012)

[21] 정용찬, 빅데이터, 빅브라더. KISDI 전문가컬럼. (정보통신정책연구원. 2012)

[22] 빅토르 마이어 쇤베르거·케네스 쿠키어, 이지연(옮김), 빅 데이터가 만드는 세상(21세기북스, 2013)

[23] 토비아스 징엘슈타인·피어 슈톨레, 윤재왕(역), 안전사회: 21세기의 사회통제(한국형사정책연구원, 2012)

[24] 찰스 두히그, 강주헌 (옮김), 습관의 힘, (갤리온, 2012),

[25] 한국지역개발원, "빅 데이터 시대의 데이터 활용과 전략", 지역정보화 동향분석, 2012의 자료를 재인용

[26] 한국지역정보개발원, 빅데이터를 활용한 지방자

치단체의 재난안전관리 거버넌스 구축연구, (한국지역정보개발원, 2013)
[27] 한국행정연구원, 빅데이터와 재난관리, (한국행정연구원, 2013)
[28]日本学術会議 情報学委員会 E-サイエンス・データ中心科学分科会, ビッグデータ時代に対応する人材の育成, 2014
[29] Ratcliffe, J. H., "The Structure of strategy thinking", in J. H. Ratcliffe, (ed.), [30]Strategic Thinking in Criminal Intelligence Sydney: Federation Press, 2009
[30] https://blog.lgcns.com/856 https://blog.naver.com/iotsensor/221120586921

저 자 약 력

손 상 철

이메일 : kojison@naver.com

- 대한시큐리티연구소(KSI) 소장
- 국제구명구급협회(IEMA) 한국본부장
- 한국시큐리티연구원 상임이사
- 대한민국탐정협회 상임회장