차세대 정보보호 기술 개발 전략


조 현 숙
한국전자통신연구원


서 동 일
한국전자통신연구원

Ⅰ. 서 론

세계적인 IT 컨설팅 업체인 가트너는 최근 2014년도 10대 전략적 기술 트렌드를 발표하였다. 특히, 가트너는 힘의 결합(Nexus of Forces)으로 소셜 네트워킹, 모바일, 클라우드, 빅데이터(즉, 정보)라는 4가지 강력한 힘의 융합이 계속해서 변화를 이끌고, 새로운 기회를 만들어 내면서 향후 3년간 기업이나 사회에 주요한 영향을 미칠 것으로 내다 봤다. 여기에 포함될 10대 전략적 기술 트렌드로는 모바일 기기의 다양성과 관리, 모바일 앱과 애플리케이션, 만물 인터넷(IoT, Internet of Everything), 하이브리드 클라우드와 서비스 브로커로서의 IT, 클라우드/클라이언트 아키텍쳐, 개인 클라우드 시대, SDx (Software Defined Anything), 웹 스케일 IT (Web-Scale IT), 스마트 머신, 3D 프린팅이라는 기술적 트렌드들이 매우 중요할 것으로 예측하였다[1]. 또한, IDG 그룹에서 전망한 2014년 IT 트렌드로는 클라우드, 모빌리티, 소셜, 빅 데이터라는 거대 트렌드와 함께 사물 인터넷, 클라우드 전략, 소프트웨어로 정의된 모든 것들, 개인용 및 퍼블릭 클라우드 서비스, 앱 스토어 등을 제시하고 있다[2].

이러한 최근의 IT 메가 트렌드에 맞물려 보안 위협 또한 전통적인 단순 바이러스 감염, 해킹 위협 뿐만 아니라 광역화, 통합화, 융합화, 지능화 되어 가고 있는 상황이다. 국내의 대표적인 보안업체중 하나인 안랩에서 예상한 2014년도 7대 보안 위협 트렌드를 보면, APT 방식의 악성코드 고도화 및 표적 확대, 전자금융사기와 사이버 범죄의 산업화 가속, 악성코드 유포 방법의 다양화 및 고도화 지속, 윈도 XP 지원 종료에 따른 보안 위협 증가, 특정 표적을 노린 소규모 모바일 악성코드, 사이버 보안에 대한 국가적 인식 변화, 펌웨어 업데이트에 악성코드 포함 시도 증가 등을 예시하고 있다[3].

또한, 최근 2014.2월 러시아 보안기업인 카스퍼스키사에서 발표한 'The Mask"라는 사이버 첩보 활동을 통한 사이버 공격 사례를 살펴보면 사이버 위협이 얼마만큼 고도화 되고 있는지를 알 수 있다. 'The Mask'로 명명된 악성코드의 주요 공격 대상은 정부기관, 대사관, 에너지/석유/가스 설비, 민간기업, 연구기관, 민간 증권사, 기타 활동기구 등 주요 공공 기관 및 국가 인프라 시설이 대부분이며, 2007년부터 전 세계를 대상으로 유포되어 민감한 정보를 수집하고 있는 가장 복잡하게 진화한 형태의 사이버 첩보 활동이다. 더욱이 'The Mask'는 악성코드, 루트킷(Rootkit), 부트킷(Bootkit) 등 복잡한 코드의 복합체로 구성되어 있으며, 윈도우즈 뿐만 아니라 맥OS, 리눅스, iOS기반 시스템, 안드로이드 모바일 플랫폼에서도 동작이 가능해 운영체제에 무관하게 활동이 가능한 최고의 기술력이 집대성되어 있는 사이버 공격 기술인 것이다. 이러한 악성코드는 현재의 백신 제품으로는 탐지가 매우 어려운 것도 현실인 것이다[4-5]. 따라서, 이러한 사이버 위협에 대비하기 위한 차세대 정보보호 기술의 개발은 매우 중요한 문제이며, 본 기고문에서는 국내외 정보보호 기술 분야의 현황 및 트렌드를 살펴보고 향후 개발 전략을 살펴보고자 한다.

최근 정보보호 기술은 사이버 융합 환경에서 암호, 인증, 인식, 감시 등 보안기술과 테러 · 재난 · 재해 · 범죄 예방 등 안전(Safety) 서비스를 제공하는 기술 및 시스템을 포괄하는 의미로 정의

전통적인 정보보호 기술은 정보의 비밀을 보장하는 기밀성(Confidentiality), 정보내용을 함부로 수정할 수 없도록 하는 무결성(Integrity), 인가된 사용자가 정보를 사용하고자 할 때 방해받지 않도록 하는 가용성(Availability)을 보장하는 기술을 의미하였다. 그러나, 최근에는 사이버(ICT) 융합 환경에서 암호, 인증, 인식, 감시 등 보안(Security) 기술과 이러한 기반 기술을 활용하여 테러 · 재난 · 재해 · 범죄 예방 등 안전(Safety) 서비스를 제공하는 기술 및 시스템을 포괄하는 의미로 정의하고 있다.

이러한 정보보호 기술은 정보보호 제품 특성과 활용 분야에 따라서, 네트워크 · 시스템 및 데이터 · 콘텐츠 보호를 위한 정보보안 기술, 안전 · 안심 생활을 지원하는 물리보안 기술, 보안 기술로 IT-융합 전통산업의 안전성과 신뢰성을 제공하는 융합보안 기술로 구분 된다. 즉, 컴퓨터 또는 네트워크상의 정보의 훼손, 변조, 유출 방지와 사이버 범죄/테러 예방을 위한 보안 제품 및 서비스를 정보보안 기술이라 하며, 전통적인 정보보호 기술은 이러한 정보보안 기술을 의미하였다. 정보보안 기술은 정보통신망에서 정보의 안전한 송수신 및 보관 · 처리, 상대방의 신원 확인 및 정보에 대한 무결성을 보장하는 프리미티브 기술인 암호/인증 기술, 유무선 통합 망에서 다양한 사이버 공격에 대응하기 위한 직접적인 방어 기술 및 침해사고 정보공유, 실시간 통합제어 기술 뿐만 아니라 악성코드의 수집 및 분석, 자동분류, 경유/유포지 탐지 기술을 의미하는 유무선 네트워크 보안 기술, 플랫폼의 무결성 및 안전한 실행 환경을 제공하고 악성코드의 탐지 및 대응 기술 등을 통해 단말/서버 시스템의 중요 정보 유출 방지 및 안전한 보안 서비스 실행을 보장하는 단말/서버시스템 보안 기술, 콘텐츠 보호, 개인정보 유출과 프라이버시 침해 문제해결, IT기반 범죄 증거 확보 등 다양한 ICT 응용 및 서비스를 위한 콘텐츠 및 응용보안 기술 등으로 세분화 할 수 있다.

또한, 물리보안 기술은 물리적 접근으로 발생되는 테러, 재난 · 재해, 범죄로부터 안전 · 안심 생활을 지원하는 보안 제품 및 서비스를 의미한다. 여기에는 영상에서 자동 검출/추적된 객체를 표현하고 다른 객체와 구별할 수 있는 특징을 추출하여 분류, 식별, ID부여, 식별 코드화 등을 수행하는 인식 기술, 카메라 또는 센서를 이용하여 감시 대상인 객체의 정보를 보다 용이하게 획득, 저장, 관리/보호 및 모니터링 할 수 있도록 하는 감시 기술로 세분화 할 수 있다. 융합보안 기술은 보안 기술이 비(非) IT기술 · 산업과 융합되어 창출되는 보안 제품 및 서비스를 말하며, IT와 융합된 산업 자동화 및 제어 시스템의 적절한 작동에 있어서 의도적 또는 비의

도적인 방해를 야기하는 이벤트를 예방 또는 탐지하는 제어시스템 보안 기술, IT 기반의 차량, 의료 등의 산업에 대한 안전성과 신뢰성 향상을 위해 개인정보 노출, 사이버테러 등 내외부 침해사고를 예방 또는 탐지하는 산업보안 기술로 세분화 할 수 있다.

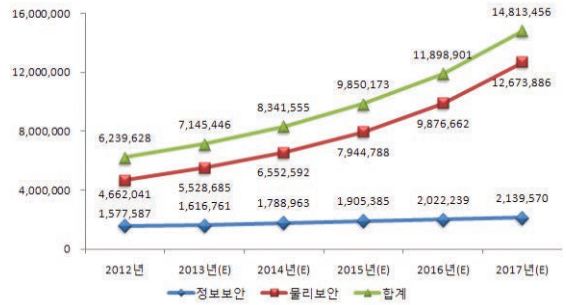
본 기고문에서는 이러한 정보보호 기술 분야에 있어서 중장기적인 차세대 정보보호 기술 개발 전략 방안을 제시한다. 제2장과 3장에서는 국내외 시장 및 산업동향, 국내외 기술개발 동향을 알아보고, 제4장에서 향후 미래 사회에 적합한 중장기적인 보안기술 개발 전략을 제시한다. 마지막으로 결론 및 향후 전망을 살펴본다.

Ⅱ. 국내외 시장 및 산업 동향

1. 국내 현황

2013년 국내 정보보호 산업의 매출은 7조 1,454억원으로, 2012년 대비 14.5% 증가하였다. 이중 정보보안 매출은 2012년 대비 2.5% 증가한 1조 6,168억원이며, 물리보안 매출은 2012년 대비 18.6% 증가한 5조 5,287억원 정도이다. 정보보호 산업의 2017년 매출 전망은 연평균 증가율(CAGR, Compound Annual Growth Rate) 18.9%를 기록하며, 그림 1과 같이 2017년 14조 8,135억원으로 성장할 것으로 전망된다[6].

국내에는 233여 개의 정보보안 업체와 385여 개의 물리보안 업체가 존재하며, 융합보안 분야 전문 기업은 극히 드문 상황이다. 또한 전체 업체들 중 약 70%가 자본금 10억원 미만의 중소기업이며, 100억원 이상인 기업은 겨우 4%에 불과한 실정이다. 종업원 규모를 봤을 때에도 10인 미만 기업이 25%, 10인 이상 50인 미만 기업이 50% 정도일 정도로 영세한 상황이다[6].



〈그림 1〉 국내 정보보호 산업 규모 전망 (백만원)[6]

그러나, 국내에서도 최근 대규모 개인정보 누출 사고 등 지속적인 사이버 공격이 발생되면서 점차적으로 정보보호의 중요성에 대한 인식이 높아지고 있으며, 개인 및 기업 뿐만 아니라 국가 안보적 측면의 중요성이 부각되면서 향후 국내의 정보보호 산업 규모는 더욱 더 확장될 것이며 기업 규모 또한 점차적으로 대규모화 될 것으로 예측되고 있다.

2. 국외 현황

세계 정보보호 산업의 시장 규모는 2012년 기준 1,732억달러로 연평균 약 10.5%대의 높은 성장률이 예상되고 있다. 특히, 물리보안 및 융합보안 시장의 성장세에 힘입어 2017년경 정보보호 산업의 시장은 표 1과 같이 2,851억달러 규모로 약 1.7배 증가할 전망이다[8]. 이는 미국, 서유럽 주요국, 일본 등이 정보보호를 국가 핵심 현안으로 인식하고 관련 분야 예산을 확대하며 국가 차원의 안보 체계를 구축하는 데 많은 영향을 받고 있다. 또한, 타 산업 분야에서 안전과 신뢰성에 대한 요구가 증가하면서 융합보안 산업의 고성장세가 지속될 전망이며, 차량·국방·의료·금융·건설·물류·항만 등 이종 산업과 통신망에서의 핵심 가치로서의 융합보안 수요가 급증할 것이다. 또한, 미국, 유럽, 일본 등 3대 시장이 지금까지 세계 시장의 대부분을 차지하고 있었으나 그 비중은 점차 축소될 것으로 보이며, 중국의 경우에는 물리보안 시장에서 매년 20% 이상의 성장률을 보이고 있어 향후 최대의 물리보안 시장으로 부상할 것이다.

〈표 1〉 세계 정보보호 시장 현황 및 전망 (억달러)[8]

	2012	2013	2014	2015	2016	2017	CAGR
세계시장 합계	1,732	1,900	2,097	2,305	2,547	2,851	10.5%
정보보안	496	548	601	651	714	783	9.6%
물리보안	1,184	1,290	1,420	1,562	1,723	1,934	10.3%
융합보안	52	62	76	92	110	134	20.9%

Ⅲ. 국내외 기술 동향

1. 정보보안

정보보안 기술 분야의 기술경쟁력은 미국 등 기술선진국과 1~2년 정도의 기술격차를 보이고 있다[8-11].

암호/인증 기술 분야의 경우, IBM 등의 세계 최고 연구 기관과 경쟁 수준의 기술력을 보유하고 있으나, 암호 안전 설계, Homomorphic encryption, Post-Quantum Cryptography 등 新암호화 기법에 대한 기술 격차는 여전히 높은 편에 있는 것으로 판단된다. 전자상거래의 활성화로 인해 공인인증 인프라(PKI), 멀티팩터인증, 멀티채널인증에 대한 세계적 수준의 기술력을 보유하고 있으나, 인증 인프라의 취약점을 이용하는 지능형 공격에 대한 근본적인 대응은 미흡한 실정이다.

유무선 네트워크보안 기술의 경우, 방화벽/IDS/IPS, 통합보안 제어 등 국산 네트워크보안 제품의 시장 점유율은 높여가고 있지만, 지능형 SIEM[1], STAP[2] 제품등 신기술이 접목된 하이엔드 보안 제품의 기술 경쟁력은 여전히 선진국 대비 미흡한 실정이다. '시그니처리스(signatureless)' 기반의 악성코드 탐지를 위한 샌드박싱 기술, 이상 행위 탐지를 위한 빅데이터 분석 기술 등이 기존 네트워크보안 제품 측면에서 경쟁력이 미흡하며, 무선 DoS/피싱 공격 대응이 불가능한 저속/저용량/저가 공유기 형태의 국내 무선랜 제품 경쟁력은 높은 편이나, 무선침입공격 방지와 스위치 기능이 내장된 고성능 AP제품의 경쟁력은 미흡한 상황이다.

> 암호 안전 설계, Homomorphic encryption, Post-Quantum Cryptography 등 新암호화 기법에 대한 기술 격차는 여전히 높은 편

단말/서버시스템 보안 기술의 경우, 모바일 단말 보안, 가상화 보안 등 新 서비스 보안 제품의 시장 지배력 및 기술 경쟁력은 취약하나, M2M 보안은 태동기로써 핵심기술 경쟁력 확보가 가능할 것으로 판단된다. 특히, 이러한 신 기술 분야는 국내 출연(연)을 중심으로 국가 아젠더로서 신속한 기술 확보와 시장의 선진입을 통한 국제 경쟁력 확보가 필요할 것으로 판단된다.

콘텐츠 및 응용보안 기술의 경우, 저작권보호용 DRM 제품은 세계 시장 경쟁력을 확보하고 있으나, 빅데이터/클라우드 보안 기술 및 디지털 포렌식 제품군의 기술 경쟁력은 여전히 선진국 대비 부족한 편이다. 개인정보보호 기술은 유출방지 기술이 있으나, 주민번호 등 단순한 패턴의 개인정보만을 탐지할 수 있고, 지능화된 내부자 유출을 탐지할 수 없는 등 기술력이 미흡한 편이다.

〈표 2〉

소분류	한국	미국	일본	유럽	중국
암호 및 인증	2.0	0.0	1.5	0.5	2.5
유무선 네트워크보안	1.7	0.0	1.3	0.9	2.5
단말/서버 시스템 보안	1.7	0.0	1.3	0.9	2.5
콘텐츠 및 응용보안	1.2	0.0	1.3	1.0	2.0

1) SIEM : Security Information Event & Management

2) STAP : IDC가 정의하고 있는 보안 분야 Market Segment로서, 사이버 스파이 행위나 데이터 유출을 목표로 한 은밀한 악성코드 기반의 공격을 감지하는 제품은 특수한 보안 시장 영역으로 간주해야 하며, 이 새로운 보안 분야를 'STAP(Specialized Threat Analysis and Protection)'으로 정의

2. 물리보안

물리보안 기술 분야에서, 휴먼/바이오인식 기술은 미국 대비 75%수준 및 3.0년의 기술격차를 보이고 있으며, CCTV 감시/관제 분야는 85%수준 및 2.0년의 기술격차를 보이는 것으로 판단된다[8-11].

미국은 지문인식, 얼굴인식, 홍채인식, 스마트카드 분야의 대표적인 업체들의 M&A를 통하여 L1 Identity Solutions社(현, MorphoTrust USA)를 설립하고 휴먼/바이오인식 기술 및 세계 시장을 선도하고 있는 상황이다.

〈표 3〉

소분류	한국	미국	일본	유럽	중국
휴먼/바이오 인식	3.0	0.0	1.5	1.0	2.5
CCTV 감시/관제	2.5	0.0	1.0	0.5	2.5

〈표 4〉

핵심기술	기술 선도국 및 기관	상대적 수준(%)
휴먼/바이오 인식	– MorphoTrust USA (미국) – Google, IBM (미국) – iOmniScient (호주) – NEC (일본)	70~80
CCTV 감시/관제	– Axis Communications (미국) – Pleco (미국) – Milestone (덴마크) – ObjectVideo (미국) – Bosch (독일)	80~90

영상인식 기반 물리보안 기술은 인식 활용도를 높이기 위한 사용자친화형/원거리/모바일 바이오인식 기술로 진화하고 있는 추세이며, 지문인식 위주의 바이오인식에서 얼굴, 귀 모양, 걸음걸이 등 CCTV 환경에서 사람식별 및 검색을 위한 소프트 바이오인식(Soft-Biometrics) 기술 개발이 추진되고 있는 상황이다.

얼굴인식은 대부분의 경우 DB에 저장된 영상과 근거리에서 획득된 얼굴영상 만을 주로 이용하고 있어, 실시간 환경에서 객체정보 획득 등 전처리 기술 수준이 미흡하며, CCTV 감시/관제 영상보안 기술은 기존 서버 중심에서 분산화 기반 하이브리드 분석 방식으로 발전함에 따라 대규모 영상을 동시에 고속/고성능 분석하기 위한 패러다임으로 진화 발전되고 있는 추세이다.

3. 융합보안

융합보안 기술에서, 산업보안 분야는 독일 대비 2.0년의 기술격차가 있고, 헬스케어 보안 분야는 1.7년의 기술격차를 보이는 것으로 판단된다[8-11].

운송보안, 홈랜드보안, 경계감시 분야에서는 미국과 유럽이 전체 IPR의 90% 이상을 보유한 것으로 판단되며, 의료, 바이오, 로봇 보안 또한 미국과 유럽이 대부분의 IPR을 보유하고 있다.

또한, 제어시스템 네트워크 경계 위협 방지보다는 네트워크 내부위협을 방지할 수 있는 제어기 단위로 방어할 수 있는 기술로의 신시장이 AllenVault, Byres Security 등의 글로벌 회사를 중심으로 빠르게 변화되고 있다. 이외에도 산업제어시스템과 정보통신 기술 격차가 7년인 점을 감안하여 보면 해외 산업제어시설용 특수방화벽 제품의 기술격차도 7년 이상으로 판단된다.

〈표 5〉

소분류	한국	미국	일본	유럽	중국
기반시설 보안	2.0	0.0	0.9	0.7	2.9
산업 보안	2.0	0.5	1.5	0.0(독일)	3.0

운송보안, 홈랜드보안, 경계감시 기술 분야의 경우, 미국 Lockheed Martin, Boeing, 유럽 NorControl사, 독일 ATLAS 등이 시장을 선도하고 있으며, 항공관제 시스템 분야는 미국 Lockheed Martin 등 기술력이 우수한 기업들이 시장을 주도 중이고, 전신 스크리너 등 고난이도 융합제품은 선진 업체 대비 여전히 5~6년 이상의 격차가 존재하는 것으로 판단된다.

해상관련 기술은 노르웨이, 영국, 러시아 등 유럽이 강세이며, 국내 기술 수준에는 4~5년 격차가 존재하나 최근 출연(연)등 국내에서 해당 분야의 IT융합 기술 개발로 그 격차가 급격히 축소되고 있는 상황이다.

운송보안 중 시장이 가장 큰 자동차보안시장의 경우 유럽의 EVITA 프로젝트가 선도하고 있으며, EVITA프로젝트는 독일을 주축으로 독일내 자동차 OEM사와 부품제조사들이 참여한 프로젝트로 3가지 등급의 솔루션을 제안하고 있다. 이러한 자동차보안 분야에서 국내 기술 수준은 차내 네트워크에 대한 보안기술에 있어서는 4~5년 기술 격차가 존재하는 것으로 보이며, 차외 네트워크연동에 대한 보안 기술에 있어서는 2~3년 정도의 기술 격차가 존재할 것으로 판단된다.

Ⅳ. 차세대 기술개발 전략

1. 기본 전략

앞서 제2장 및 3장에서 살펴본 바와 같이 국내 정보보호 산업의 국제 경쟁력은 매우 미흡한 게 사실이다. 따라서, 이러한 국내의 정보보호 기술 경쟁력을 향상시키기 위해서는 정보보호 원천 기술의 확보와 국제 경쟁력을 보유한 국내 정보보호 산업 규모 확대를 주요 목표로 하여 국가 출연(연)을 중심으로 한 중장기적인 원천기술 확보 전략 및 민간 정보보호 산업 규모를 확

대하기 위한 국가적 정책이 중점 추진되어야 할 것으로 판단된다. 여기에는 2013년도 12월 발표된 정보보호 일류제품 개발을 위한 기술 개발(안) 등이 매우 유효 적절한 정책일 것이다.

예를 들어, 단기적으로는 시장에서 시급히 요구하는 수입대체형 정보보호 제품의 상용화가 필요하며, 중장기적으로는 수출주도형 및 고난이도의 미래 성장형 제품의 발굴과 관련 기술 개발이 매우 중요할 것이다. 또한, 국가 출연(연)의 과제 기획 단계부터 기술개발/특허/표준 등을 상호 연계하여 국가 연구개발 성과물에 대한 시장 상용화 및 확산 정책을 적극적으로 추진하여야 할 것이다.

추가적으로 이러한 중장기적인 원천기술 확보 및 산업 경쟁력 확보를 위한 정책 추진에는 매우 많은 예산이 소요될 것으로 판단되나, 현실적으로 대규모의 단기적인 예산 확보는 매우 어려운 것도 사실이다. 따라서, 기존의 다양한 정부의 정책적 프로그램 예산 들을 적극 활용하여야 하며, 국제적인 연구개발 프로젝트 참여도 적극적으로 고려하여 열악한 예산 규모의 한계를 극복 할 수 있도록 하여야 할 것이다.

최근에는 필요로 하는 인가 대상에게는 정보의 기밀성을 유지하면서 더욱 편리한 사용을 가능케 하는 Homomorphic Encryption 기술에 대한 연구개발이 적극적으로 이루어지고 있어

2. 정보보안

앞서 분류된 정보보안 기술 분야에는 암호/인증 기술, 유무선 네트워크 보안 기술, 단말/서버시스템 보안 기술, 콘텐츠 및 응용보안 기술 등으로 세분화 되어 있다.

정보보안 분야의 가장 기반이 되는 암호/인증 기술은 사이버 환경에서 다양한 정보를 안전하고 신뢰성 있게 접근·이용·보관·처리·유통하기 위한 기반 기술이며, 정보의 안전한 송수신 등 유통을 위한 암호기술, 사용자의 신원확인 및 유통되는 정보에 대한 무결성을 보장하기 위한 인증기술, 불법적인 정보접근을 통제하기 위한 접근제어 기술, 이용자 중심의 개인정보 관리 및 보호 기술 등으로 세분화할 수 있다.

암호기술은 중요 정보가 인가되지 않은 대상에게 불법적으로 노출되지 않도록 기밀성을 보호하기 위해 사용하는 기술이다. 기존에는 비트수를 늘려 안전성을 강화하는 블록 암호 알고리즘 기술을 주로 개발하였다면, 현재는 양자컴퓨터와 같은 미래 컴퓨팅 환경을 대비하여 양자 암호기술, 경량화 암호 알고리즘 기술 등을 개발하고 있다. 최근에는 보호개념 이외에 꼭 필요로 하는 인가 대상에게는 정보의 기밀성을 유지하면서 더욱 편리한 사용을 가능케 하는 Homomorphic Encryption 기술이 적극적으로 연구 개발되고 있는 상황이다. Homomorphic 암호화 기술은 암호화된 데이터에 대한 임의의 연산을 보존하는 암호 기술로, 2009년 Gentry에 의해 처음으로 해결책이 제시되었으며, 국내에서는 정부 출연(연)을 중심으로 활발한 연구 개발이 이루어지고 있는 상황이다.

인증기술은 사이버 환경에서 적법한 사용자를 식별하기 위한 신원확인을 비롯하여 유통되는 정보의 무결성을 보장하는 기술이다. 일반적인 ID/패스워드와 같이 기존 사용자의 신원확인 기술에서부터 다양한 단말기의 진위성 여부를 보장하기 위한 디바이스 인증기술, 익명의 사용자를 추적할 수 있는 익명 인증기술, 매번 비밀번호를 변경하는 OTP(One Time Password) 인증 기술 등으로 세분화 된다. 최근에는 온·오프라인 인증기술을 상호 유기적으로 결합하여 무결성을 보장하면서도 더욱 편리한 사용을 가능케 하는 스마트지갑 및 스마트 인증 기술이 연구 개발되고 있다.

유무선 네트워크 보안 기술, 단말 및 서버시스템 보안 기술은 인터넷과 같은 개방형 네트워크 환경에서 전달되는 정보의 위조, 변조, 유출, 무단침입 등을 비롯한 불법 행위로부터 정보를 보호하는 네트워크 보안과 정보통신 시스템의 안전성과 가용성을 향상시키는데 필요한 단말 및 시스템 보안기술 등으로 세분화 할 수 있다.

네트워크 침해대응은 기존의 방화벽기술, 침입탐지기술, 침입억제기술, 분산서비스거부공격 대응 기술과 같은 정보보호 기술이며, 주로 네트워크 접근제어, 역

추적 영역까지 포함한다. 이동통신 및 모바일 보안은 실제 서비스를 위한 사용자의 정보보호 이슈 및 부가서비스에 대한 정보보호 영역을 포함한다. 무선랜(근거리 통신망) 보안기술은 무선랜에 참여하는 각 개체들의 권리, 이익, 프라이버시 등을 보호하고, 나아가서는 무선랜 자체를 각종 공격으로부터 보호하는 기술이다. 보안분석/관리는 기업의 보안관리, 위협관리, 패치관리, 로그관리/분석, 취약점 분석, 지능형 통합보안관리 영역을 말한다. 미래인터넷(Future Internet)은 통신·방송·컴퓨팅·센서가 융합된 인프라로 현 인터넷의 다양한 요구사항(광대역, 이동성, 안정성, 유비쿼터스, 경제성 등)을 수용하는 새로운 미래 네트워크이다.

클라우드 컴퓨팅은 컴퓨팅 자원을 사용한 만큼 비용을 지불하도록 하는 개념으로 시작된 기술로 가상화 기술을 기반으로 자원을 공유 혹은 분산 사용이 가능하도록 하고 있으며 컨텐츠, 네트워크, 플랫폼, 디바이스 등 4가지의 서비스를 포함하여 전체 레벨에서의 정보보호를 제공하는 체계를 가진다. 이외에도 차세대 휴먼 디지털 정보기기로써 인간 친화적인 유비쿼터스 컴퓨팅 환경 제공에 수반되는 차세대 퍼스널컴퓨팅 플랫폼, 웨어러블 네트워크, 휴먼-컴퓨터 상호작용(HCI) 기술 및 개인화 서비스 기술 들이 필요하다. 보안 칩셋 기술은 스마트카드, MTM(Mobile Trusted Module), USIM, 보안토큰 등을 말한다. 특히, MTM 보안 기술은 기존의 소프트웨어적인 보안 기술에서 하드웨어 적인 스마트 단말 보호 기술을 제공하기 위한 것으로 향후 중점적인 상용화 추진이 필요할 것으로 판단된다. 디지털 포렌식 기술은 사이버 범죄, 정보유출 등과 관련된 디지털 증거가 법적 증거력을 갖게 하기 위해 디지털 데이터를 수집, 보관, 분석, 보고하는 과학적이고 논리적인 절차와 방법을 의미한다. 악성코드 대응이나 봇넷 대응과 같은 기술은 다양한 악성코드나 봇넷(botnet)[3]을 대응하기 위한 기술과 사이버공격 역추적 및 보안 관리에 대한 기술들이 향후 중점 개발되어야 할 것이다.

이외에도 최근의 ICT 메가 트렌드에서 알 수 있듯이 소셜 컴퓨팅 영역, 모바일 영역, 클라우드 서비스 영역, 빅 데이터 영역에서의 정보보안 기술 개발 전략이 필수적으로 소요될 것이다. 더욱이 이러한 메카 트렌드는 필연적으로 민감한 개인정보 들을 중점적으로 사용될 것이므로 빅데이터의 분석과 활용시 개인정보의 보호를 위한 기술의 개발은 매우 중차대한 문제로 대두될 것이다.

3. 물리보안

앞서 분류된 물리보안 기술 분야에는 인식 기술, 감시 기술 등으로 세분화 되어 있다.

휴먼/바이오 인식 기술의 경우, 국내 산업의 92%가 지문인식 분야일 정도로 큰 영역을 차지하고 있으며, 이외에 얼굴인식, 홍채인식, 원거리 휴먼인식 등 지문 이외의 바이오인식 시시장 창출이나 기술 개발에는 매우 취약한 구조이다. 그러나 점차적으로 세계 시장에서는 아직까지는 지문 인식이 높은 비중을 차지하고 있으나 점차 얼굴인식, 홍채인식, 정맥인식, 걸음걸이 인식 등 타 기술 분야로 시장이 확대되고 있으므로 이에 대비할 수 있는 원천 기술 확보 전략이 필요할 것이다. CCTV 감시/관제와 같은 감시 기술 분야에서는 기존의 CCTV/DVR 제품의 국제 경쟁력이 점차 하락하는 추세이다. 더욱이 차세대 영상 감시 제품에 대한 준비 부족으로 인하여 국내의 지능형 영상인식 제품 기술은 외국 기술에 크게 의존하고 있는 실태이다.

따라서, 향후의 국제 경쟁력 확보를 위해서는 인식 기술 분야 중에서도 원거리 휴먼인식 기술, 사용자 친화형 바이오 인식 기술, 비제약적 인식 기술, 개인 식별 및 고성능의 바이오 검색 기술 등을 확보 하여야 할 것이다. 또한 지능형 영상 인식 기술 중에서도 배경 모델링 기술, 이동객체 추적기술, 실시간 프라이버시 마스킹 기술 등과 같은 공공기관의 수요가 클 것으로 예측되는 분야의 기술 뿐 만 아니라 재난/재해 방지용 지능형 영상 감시 기술이나 3D와 같은 더욱더 효율적으

3) 일종의 군대처럼 악성 봇에 감염되어 명령, 제어 서버에 의해 제어당하는 대량의 시스템들로 구성된 네트워크로 수십에서 수만대의 시스템에 동시에 명령을 전달받아 실행하여 대규모의 네트워크 공격 등 다양한 악의의 행위가 가능한 기술이다.

로 감시 할 수 있는 다중 객체 추적 기술, 다중센서 연동 추적 기술, 방범/방재 지능형 영상 감시 기술 등을 적극적으로 확보 할 수 있도록 하여야 할 것이다.

4. 융합보안

앞서 분류된 융합보안 기술 분야에는 제어 시스템 보안 기술, 산업 보안 기술 등으로 세분화 되어 있다. 물론, 산업보안 기술에는 자동차 보안 기술, 헬스케어 보안 기술, 항공 보안 기술, 해양 보안 기술 등과 같이 비IT 산업과의 융합화에 따른 보안 문제 해결 기술 들이 모두 포함되어 있다.

전반적으로 제어시스템 보안 제품은 외국의 기술 의존도가 매우 높은 편이며, 현재까지 정보보안 위주의 정보보호 기술 발전으로 인하여 제어 시스템 보안 분야의 원천기술 확보는 매우 미흡한 상황이다. 더욱이 제어 시스템 분야는 범 부처 성격인 경우가 많아서 다양한 기술 분야 간의 기술적 융합이 필수적으로 소요되는 높은 기술적 난이도를 가지고 있다. 또한, 산업 보안 기술 분야는 자동차 보안 분야 및 해양 보안, 항공 보안 분야의 일부 기술 개발이 이루어 지고 있으나 대부분의 비IT 제품과의 융합화에 따른 보안 문제 해결은 아직까지 매우 미흡한 상황이다.

따라서, 제어시스템 보안 기술의 경우, 스마트그리드 네트워크 트래픽 분석, 접근제어, 상호 인증 기술 개발이 필요하며, 원자력 분야의 이상징후 탐지 및 제어, 침해사고 탐지 등과 같은 보안 기술 개발이 필요할 것이다.

산업보안 분야의 경우, 고령화 사회 대비 생체 의료기기 해킹 방지 기술이나 임베디드 의료기기 악성코드 방지 기술, 산업보안 분야의 침해사고 포렌식 기술 등의 선제적 기술 개발 전략이 필요할 것으로 판단된다.

Ⅴ. 결론 및 향후 전망

기밀성, 무결성, 가용성 보장을 위한 전통적인 정보보호 기술 분야에서 최근에는 테러 · 재난 · 재해 · 범죄 예방 등 안전(Safety) 서비스까지를 포함하는 포괄적인 개념의 정보보호 기술로 발전하고 있음이 최근의 기술적 트렌드이다.

최근의 고 지능화된 사이버 공격에 대응하는 사이버 보안 위협 대응은 점차적으로 기존 산업적 문제에서 국가 안보적 문제로 인식되어 지고 있는 상황이며, 사이버 공격의 대응 또한 국부적인 조기 탐지 및 대응에서 침해 정보의 공유를 통한 다자간 협력 대응으로 확산을 조기 차단하고, 공격 근원지 식별/추적 및 선제적 대응을 통해 적극적으로 사이버 공격을 조기 경보/예방하는 방식으로 발전되고 있다. 보안 기술 및 시스템 또한 기존의 단순 모니터링 위주의 노동집약적 보안감시에서 벗어나, 지능적/자율적 보안 감시 기술로 효율성이 극대화될 수 있도록 발전되고 있다.

유무선 네트워크 보안 분야에 있어서 침해정보의 공유를 기반으로 네트워크 공격을 고속 탐지/차단하는 기술에서 APT(Advanced Persistent Threat) 공격의 예측, 공격자 식별 · 위치 추적 및 선제적 공격 대응으로 발전하고 있다. 이는 기존의 1채널 감시/탐지 기반의 저속 (54M급) 무선 침입 방지 및 40G급 DDoS(Distributed Denial of Service) 공격 차단기술에서 기가(Giga)급 무선 · 4G 모바일망 침해방지 및 미래인터넷 보안, 빅데이터 보안 분석 기반의 지능형 보안기술로 발전한다는 것을 의미한다. 단말/서버 시스템 보안기술은 스마트카드, USIM(Universial Subscriber Identity Module), TPM/MTM(Trusted Platform Module/Mobile Trusted Module), 모바일 단말 관리 기술, 모바일 백신 기술, 안티 스팸, 안티 피싱, 악성코드 분석과 같은 보안 소프트웨어/하드웨어 기술에서 스트리밍 데이터 동적 프라이버시 보호, 사물통신 보안 관리, 가상화 보안, 초고신뢰 수준의 멀웨어 대응, 자동분석 엔진 및 리커버리 기술과 같은 스마트 액티브 보안기술로 발전될 것이다. 온/오프라인 포렌식 분석, 단말기 종속형 콘텐츠 DRM(Digital Right Management), 업로드/다운로드 유해물 유통차단, 암호화 및 접근 권한제어에 의한 개별 개인정보 보안을 근간으로 하는 현재의 콘텐츠 및 응용보안 기술 분야에서는 포렌식 데이터 가시화 및 연관분석, N스크린 공

유 콘텐츠 DRM, 스트리밍 유해물 유통 차단, 클라우드/빅데이터 프라이버시 보호와 같은 분산환경 (클라우드/빅데이터) 대응 보안 기술로 발전할 것이다. 암호/인증 기술 분야는 기존의 AES, RSA, ECC와 같은 고속/경량 암호 구현 및 부채널 공격 방지 기술에서 Homomorphic Encryption, White Box, 양자 암호와 같은 키누출 방지형 암호 구현 및 프라이버시 보호형 암호 기술로 진화할 것으로 전망된다.

영상 인식/감시와 같은 물리 보안 분야에서는 강압식 바이오인식 기술, 유인화 감시/관제 기술에서 대용량/비제약적 휴먼인식, 무인화/지능형 감시/관제 기술로 발전할 것이다.

융합보안 분야에서는 기존 IT 보안기술의 단순 적용이나 EMR/EHR(Electronic Medical Record/Electronic Health Record) 보호, 수동적인 개별 차량 보안에서 기간산업의 안전성과 보안성이 강화될 수 있는 장치간 네트워크 보안/인증이나 지능형 통합 보안관제, 능동적 차량보안, PHR(Personal Health Record), 생애 전주기의 토탈 의료 보안과 같은 방향으로 발전될 것이다.

이와 같은 정보보호 기술의 발전 전망과 더불어 더욱 더 안전하고 행복한 삶의 질을 추구하는 사회적 기대효과에 부응할 수 있는 정보보호 기술의 개발은 국가적 국부 창출을 위한 필수 불가결한 요구사항 일 것이다. 따라서, 암호/인증, 네트워크 및 시스템 보안, 응용 보안 등을 포괄하는 정보보안 기술 분야, 휴먼 바이오 인식과 영상 감시 등과 같은 물리 보안 기술 분야, 제어 시스템 보안이나 비IT 제품과의 융합화에 따른 융합보안 기술 분야에 있어서 중장기적인 기술 개발 전략을 수립하고 이를 추진하는 것은 매우 중요할 것으로 판단된다.

본 기고문에서는 최근의 ICT 메가 트렌드에 따른 정보보호 기술의 확장된 개념에서부터 국내외 산업 및 기술 동향을 분석하고 향후 필요로 하는 차세대 정보보호 기술 개발 전략을 각 기술 분야별로 수립하였으며, 기술 분야별 향후 전망을 예측하였다. 이를 바탕으로 국가 출연(연)을 포함하여 학계, 산업계의 역량을 집결하여 국제적인 기술 경쟁력을 확보할 수 있는 정보보호 기술 개발에 적극 노력하여야 할 것이다.

암호/인증, 네트워크 및 시스템 보안, 응용 보안 등을 포괄하는 정보보안 기술 분야, 휴먼 바이오 인식과 영상 감시 등과 같은 물리 보안 기술 분야, 그리고 융합보안 기술 분야에 있어서 중장기적인 기술 개발 전략의 수립과 추진하는 것은 매우 중요

참 고 문 헌

[1] 가트너(Gartner), www.gartner.com
[2] IDG, “2014년 IT 전망 보고서”, 2013.12월
[3] 안랩, “2014년 예상 7대 보안위협 트렌드”, 2014.1월
[4] KISA, Cyber Security Issue (2014.1월, 2월호), 2014.3월
[5] Kaspersky Lab, “Unveiling careto – The Masked APT“, 2014.2.11
[6] 지식정보보안산업협회(KISIA), 한국디지털CCTV연구조합(KDCA), 2013 국내 정보보호산업 실태조사, 2013.12월
[7] KISA, 2012 국내 지식정보보안산업 실태조사, 2012.11월
[8] 미래창조과학부, ICT R&D 기획-소분과보고서(정보보호분야), 2013.9월
[9] 미래창조과학부, 정보보호 일류제품 개발을 위한 기술 개발(안), 2013.12.12
[10] 국가정보원, 미래창조과학부, 방송통신위원회, 안전행정부, 2013 국가정보보호백서, 2013.4월
[11] 지식경제부, 지식정보보안산업 진흥 종합계획, 2012.12월
[12] 방송통신위원회, 행정안전부, 지식경제부, 2012 국가정보보호백서, 2012.5월
[13] 시만텍, www.symantec.co.kr
[14] 한국인터넷진흥원, www.kisa.or.kr
[15] 인터넷침해대응센터, www.krcert.or.kr
[16] 이동범, 곽진, “미국 정부의 사이버 공격에 대한 보안 전략”, 정보보호학회지 24권 1호, 2014.2월
[17] 포티넷코리아, www.fortinet.co.kr
[18] 국가사이버안전센터(NCSC), service1.nis.go.kr (www.nis.go.kr)

조 현 숙

1979년 2월 전남대학교 수학과 (학사)
1989년 2월 충북대학교 (석사)
2001년 2월 충북대학교 전산학과 (박사)
2004년~2007년 UST 정보보호공학과 전공책임교수
2011년~현재 국방부정책자문위원 등 정부위원다수 활동
1982년 3월~현재 한국전자통신연구원, 본부장

〈관심분야〉
암호학, 인터넷 보안, 보안 프로토콜, 네트워크보안

서 동 일

1989년 2월 경북대학교 전자공학과 (학사)
1994년 2월 POSTECH (석사)
2004년 8월 충북대학교 전산학과 (박사)
1994년 3월~현재 한국전자통신연구원, 책임연구원
1994년 3월~현재 TTA 표준화 위원
2011년 3월~현재 UST 겸임교수

〈관심분야〉
인터넷 정보보호, 미래인터넷 보안 등