제4차 세종사이버안보포럼 결과보고서

신정부의 사이버안보, 어떻게 할 것인가?

:전략 산업 인재양성 중심으로

2022. 5. 25(수) 14:30~17:30

Contents

전략 사이버안보 정책 진단과 신정부의 방향성
임종인 교수 (고려대학교, 전 청와대 안보특보)

산업 사이버보안산업 육성 위한 신정부 정책방향
윤두식 부회장 (한국정보보호산업협회)

인재양성 플랫폼 기반 정부에서의 사이버안보 인재양성
김태성 교수 (충북대학교)

세종사이버안보센터
SEJONG Institute

발제1. 사이버안보 정책 진단과 신정부의 방향성

임종인 교수 (고려대학교, 전 청와대 안보특보)

□ 사이버안보 상황

○ 랜섬웨어 위협의 급증 및 고도화

- 2021년, 미 북동부 최대 송유업체 콜로니얼 파이프라인 사에 랜섬웨어가 침투해 송유 제어시스템이 2주간 중단되었으며, 이로 인하여 미국은 지역 긴급상황이 선포되는 등 국가 차원의 혼란이 발생함
- 2017년, 워너크라이 랜섬웨어에 따른 영국 의료서비스 대란, 2019년 로빈후드 랜섬웨어 따른 볼티모어 도시 서비스 중단 등 랜섬웨어로 인한 국가기반시설 중단 사태 등은 이미 경험한 바 있음
- 최근 우리 기업과 개인들을 대상으로 위협하는 랜섬웨어는 암호화, 유출협박, 디도스 공격 등 3중 협박 형태로 진화하며 급증하는 추세를 보이고 있음

○ 고도화되고 증가하고 있는 사이버 위협의 추세

- 사이버공간에 대한 의존도 증가, 코로나19로 인한 비대면 디지털 트랜스폼 가속화 등 사이버공간의 중요성 증대로 이를 위협하는 사이버 공격은 급증하고 있으며 점차 고도화되고 있는 상황
- 국가 주체, 국가 지원을 받는 비 국가주체, 대형 범죄조직 등이 사이버 위협에서 주요 주체로 등장하고 있어 개별 국가와 기업, 개인 등이 사이버 위협에 대응하는 것은 점점 어려워지고 있는 상황
- 국가 기밀 탈취를 위한 사이버공격 역시 지속되고 있어 우리도 원자력연구원, KAI 등 국가 안보에 핵심적인 조직들이 해킹으로 정보 유출을 경험함

○ 대한민국의 모든 주체들이 사이버 위협에 노출되어 있는 상황

- (국가) 지속적인 국가주체에 의한 공공부문 정보유출 등 공격을 받고 있으나 배후에 대한 파악이나 대응 등이 이루어지지 못하고 있는 상황

※ 21년 3월 기준, 국가·공공기관 대상 사이버 위협 일평균 242만 건 발생 (국가정보원)

- (기업) 국가주체, 초국가 범죄조직 등에 의하여 기업의 첨단 기밀 등 지식재산과 영업비밀

※ 2021년 우리 기업 대상 사이버 공격 52% 증가 (체크포인트)
우리 기업들은 76%가 랜섬웨어 경험 (빔 소프트웨어)

- (개인) 모바일 메신저, 이메일을 통한 일상 소통에서도 피싱과 랜섬웨어 등 여러 위협에 노출되어 지인이 보낸 메시지도 의심해야 하는 상황

※ 2021년 기준, 지난 10년간 보이스피싱 피해액 3.2조원으로 매일 71명이 피해 (경찰)

□ 사이버안보 정책 진단

○ 최상위 리더십의 부족

- 국가 차원의 사이버안보 비전과 우선순위 확립, 회색지대 해결 등을 위해 최상위 의사결정권자의 의지와 관심이 필요
- 지난 정권에서 사이버안보 리더십은 기존 정권 대비 리더십이 강화되기보다는 약화되는 방향으로 추진되었다고 평가할 수 있음

※ 국가안보실 사이버안보비서관실이 사이버정보융합비서관실로 통폐합 (2018.07.)
임기 말 신기술·사이버안보비서관을 신설, 미국 요구에 부응하는 목적 (2021.12.)

○ 명확한 거버넌스 체계 확립 실패

- 국가 사이버안보 확립을 위해 각 부처 별 '역할과 책임 (Role & Responsibility)'을 정립하며 회색지대에 대한 명확화, 공백에 대한 대응, 분산된 역량에 대한 통합 등 거버넌스 확립을 위한 조치들이 필요함
- 2019년 국가사이버안보전략이 발표되었음에도 전략 차원에서 거버넌스 체계를 포함해 전반적으로 구체성이 떨어진다는 한계가 지적됨

※ 2019년 국가사이버안보전략은 그 자체로 미흡하며 실효성 있는 내용을 담지 못했다는 지적을 받고 있어 대대적인 보완이 필요하다는 의견
(이상민 더불어민주당 의원, 정보보호 미래비전 토론회 2021)

- 사이버안보 거버넌스 관련 전략에서 부족한 부분들을 법제화하며 세부 활동 등을 규정하기 위하여 사이버안보 관련 기본법들이 발의되었으나, 부처별 충돌이 있었으며 입법에 이르지 못하고 있는 실정

※ 조태용 의원, "사이버안보 기본법안" (2019), 김병기 의원, "국가 사이버안보법안" (2021) 윤영찬 의원, "사이버보안 기본법안" (2021) 등 사이버안보 관련 법안들이 발의되었으나 서로 충돌되는 부분도 있으며 아직 입법에 이르지 못하고 있는 상황

○ 사이버안보 역량이 발전되고 있으나 국가 전력(全力) 관점에서는 부족하다는 평가

- 국가 전반적으로 사이버보안 수준이 증가하고 있으며, 전세계에서 높은 수준을 나타내는 것으로 평가되고 있음

※ 대한민국은 2021년 ITU 국제사이버보안지수에서 194개 국가 중 4위를 차지
(ITU Cybersecurity Index 2021)

- 하지만 국가 안보 관점에서 공세적·방호적 사이버작전 역량을 비롯하여 사

이버 관련 국가 역량은 주요국 대비 부족한 것으로 평가됨

※ 대한민국 사이버안보 역량은 조사 대상 30개국 중 16위로 평가되며 일본보다 낮은 수준 (Harvard Belfer Center, National Cyber Power Index, 2020)

○ 사이버안보 관련 외교 및 국제협력에서의 한계

- 미국을 중심으로 한 자유민주주의 관점의 국가 진영들과 중국과 러시아를 중심으로 한 권위주의 국가들 간의 사이버안보 이슈에 대한 시각 차이가 있으며 우크라이나전과 기술 패권 경쟁 등으로 신냉전이 예측되고 있는 상황에서 사이버 안보 관련 외교 및 국제협력은 국익 관점에서 중요한 이슈
- 우리는 여러 사이버안보 관련 국제 규범 형성, 국제 협력 체계, 사법 공조 등에 있어 참여를 하고 있으나 성과가 없으며 일원화된 전략적 외교 및 국제 협력이 부족하다는 평가를 받고 있음

※ 외교부에 사이버안보 전담 대사와 조직 부재, UN GGE/OEWG 창설 과정에 미참여, 2012년 WCIT에서 ITRs 찬성 사례 등

○ 경제안보 관점에서 사이버 이슈들에 대한 대응 부족

- 4차산업혁명 등 미래 산업 변화에 대응하기 위하여 대통령 직속 '4차산업혁명 위원회' 발족과 운영, 규제 샌드박스 도입 등 노력이 있었으며 '데이터 3법'통과 등 성과가 일부 있었으나 전반적으로 실패했다는 여론

※ 대통령 직속 4차산업혁명위원회 한계에 대한 지적 (이코노미스트 2022년 4월 1일 기사 등) 규제샌드박스 실효성 지적 (배달통 광고 관련 실증특례 1호 기업 실패사례 등)

- 반도체 부족 이슈, 불소 및 요소수 대란 등 IT 관련 글로벌 공급망 이슈와 화웨이 5G 장비 이슈 등 공급망 보안 등에 있어 정부가 선제적 역할에 실패
- 가상화폐, 디지털금융 등 새로운 금융과 이로 파생되는 여러 서비스 등에 있어 선제적인 규제와 정책이 부족하여 사회적 논란이 되고 있음

□ 신정부 사이버안보 방향성 제언

○ 사이버안보에 대한 강력한 리더십 확립

- 대통령이 국가 사이버안보의 최고 책임자임을 인식하고 사이버안보의 비전과 우선순위 등을 제시할 필요
- 사이버안보 관련 여러 쟁점사항에 대하여 기존의 각 부처의 의견을 수렴하여 종합하는 다운-탑 형태로는 해결이 어렵기에 대통령실에서 사이버 안보 쟁점 사항들에 대해 탑-다운으로 전략과 정책 등 대안을 제시해야 함
- 사이버안보비서관이 국가 사이버안보 실무를 총괄 이행할 수 있도록 보다 높은 권한과 역할을 부여하며 조직적인 지원이 필요함
- 국가안보실에 신설되는 '국가사이버안보위원회'를 실효성이 있으며 여러 쟁점 사항들을 해결할 수 있도록 권한과 역할을 부여하며 인력을 구성할 필요가 있음

○ 명확한 국가 사이버안보 대응체계 확립

- 국가 사이버안보 거버넌스 체계를 명확히 하여 회색지대와 공백 등이 없으며, 각 부처들이 명확한 역할과 책임을 가지고 소관 영역을 담당할 수 있도록 함
- 범부처 역량을 집중하기 위하여 통합되고 일원화된 사이버안보 공조체계 마련
- 부처 간 정보 공유와 유기적인 공조 체계를 뒷받침하기 위한 국가 사이버안보 관련 기본 법안을 제정할 필요가 있음

○ 공공 부문 사이버안보 역량 강화와 복원력(레질리언스) 확립

- (국방) 국가 차원의 사이버 위협에 대한 억지력 확보를 위해 역추적을 위한 정보수집과 기술 역량 강화, 공세적 방어 작전을 위한 무기 개발 등 군의 사이버 전략과 역량 대폭 강화
- (공공) 공공 부문과 기반시설 사이버보안 준비도 강화 및 복원력 확립을 위하여 사이버 위협 대응 역량 강화와 범부처 사이버위기 대응체계 수립 및 범부처 훈련 등을 통한 공공 보안 강화
- (외교) 사이버외교를 전담할 대사 및 조직을 신설하며, 굳건한 한-미 동맹을 바탕으로 사이버공간의 규범 형성 등 외교 활동과 주변국과 정보공유 및 공조체계 등을 확립하도록 함

※ 미국은 사이버공간 솔라리움 위원회를 통하여 국가 차원의 사이버안보 대전략을 마련했으며, 이는 (1) 외교를 통한 규범 형성, (2) 보안 강화를 통한 공격 무력화, (3) 적의 사이버 공격에 책임 부과 등 3개의 층위로 구성되는 중층적 억지 전략
(Final Report, Cyberspace Solarium Commission, 2020)

○ 국가의 사이버안보 관련 신뢰성 투명성 확보와 민간에 대한 지원

- 국가의 사이버안보 활동은 국민들의 프라이버시, 표현의 자유 등 기본권과 민주적 가치를 침해할 수 있기에 정책 수립과 집행 과정에서 투명성을 강화하고, 민감한 활동의 경우 외부 기관에 의해 승인과 감사를 받는 등 국민의 신뢰를 형성하기 위한 조치들이 필요함
- 신뢰를 바탕으로 경제 안보의 핵심축인 우리 기업들이 적국의 사이버 위협에 피해를 입지 않도록 국가가 기업 대상 위협 정보 공유, 대응 기술 지원, 공급망 보안 등을 통해 사이버 보호막을 제공할 필요

○ 사이버안보 역량에 대한 혁신적인 강화 조치

- 사이버안보는 국민의 안전과 사회의 안정, 국가의 안보 등에 핵심이며, 4차 산업혁명, 디지털 트랜스폼 등 경제 성장과 국익의 핵심이기에 사이버안보 관련 역량을 강화하기 위한 국가 차원의 혁신적인 조치들이 필요함
- 6G 등 차세대 통신, 양자컴퓨팅, 인공지능 등 신흥 기술과 파괴적 혁신에 대응하기 위하여 차세대 사이버안보 관련 연구·개발을 국가가 주도하며 민

간으로 확산
- 사이버안보의 핵심인 전문인력 양성을 위해 수도권 정원규제 예외 조치, 국가 차원의 인력 양성 등 혁신적인 조치들 강구 필요

❍ 사이버안보 관련 외교와 국제협력 강화
- 신냉전이 예상되는 국제 정세에서 기술 패권 경쟁과 사이버공간의 주도권 확보는 두 진영 간의 핵심 쟁점이 될 수 있는 분야
- 쿼드, 오커스(AUKUS), 인도태평양경제프레임워크(IPEF) 등 새로운 국제 협력에서 사이버안보는 중심 주제로 부각되고 있어 국가적 차원에서 사이버안보 관련 외교와 국제협력 전략을 수립할 필요가 있음
- UN GGE, UN PoA, UN OEWG 등 UN 중심의 사이버안보 규범 논의와 사이버 범죄 관련 부다페스트 사이버범죄 조약과 UN Ad-hoc 이슈, 인터넷 거버넌스 논의 등 여러 사이버공간 관련 외교에서 우리의 입장에 대한 정립 필요
- 동맹국, 주변국 외에도 여러 생각이 비슷한 국가들과의 지역 간, 양자 간 협력을 통해 사이버안보 국제 공조체계 확립 필요

지정토론: 김민호 교수 (성균관대학교)

□ 대통령 직속 국가사이버안보위원회

○ 신정부의 대통령 직속 국가사이버안보위원회에 대한 기대감 적음

- 지난 약 15년간 논의는 수없이 많이 있어 왔고, 사이버안보위원회가 부처 간 조정 역할 정도는 할 수 있을지 모르나, 국가 사이버안보 전체를 총괄 수행할 수 있는 기관 지정의 교통정리 없이 얼마나 실효를 거둘 수 있을지 의문 제기
- 그동안 국가 사이버안보를 담당하여 실질적인 역할을 가장 많이 수행해 왔고, 따라서 역량이 가장 높은 국가정보원에 대하여 정보기관이 (i) 사이버안보를 담당한 국제적인 사례가 없고, (ii) 국민 인권이 우려된다며 반대하는 의견은 반대를 위한 반대이지 실상에 전혀 맞지가 않음
- 실제, 영국, 호주, 미국 등 많은 국가들에서 정보기관이 사이버안보를 담당하고 있으며, 인권이 우려되면 감시 및 통제장치를 마련하면 될 일이지 덮어놓고 무조건 안 된다는 태도로 마땅한 대안조차 제시하지 않는 것은 모순

□ '외교'와 '외교부'의 구분

○ 사이버 외교 및 국제협력에 대한 논의에서 임종인 교수가 외교부의 노력과 사이버안보대사의 임명 등을 주장한 것과 관련하여, 모든 외교를 반드시 외교부가 해야 하는 것은 아니며 실제 외교부가 그 많은 다양한 분야들의 외교를 다 담당할 수도 없음

○ '사이버안보 외교전문가'가 하면 될 일이며, 인권 분야에서 국가인권위원회가 여러 인권 관련 외교 및 국제협력을 주도적으로 담당하는 것이 좋은 예임

□ 사이버안보 인력양성

○ 사이버안보 인력양성에 대해서도 전체적인 수급의 고려뿐만 아니라 수도권의 정원 조정과 지방인재 육성방안을 거국적으로 모색해야 함

발제2. 사이버보안산업 육성 위한 신정부 정책방향

윤두식 부회장 (한국정보보호산업협회)

□ 붙임 PPT 대체

지정토론: 최동근 사장 (센스톤, 전 CISO 협회장)

□ 붙임 PPT 참조

○ 1인 기업 및 사용자도 모두 보호해야 한다는 의견

○ 시장, 즉 수요기관인 기업들이 보안에 대한 투자를 그동안 제대로 하지 않았기 때문에 한국의 정보보호업체들이 영세하다는 분석
- 정보보호산업이 70년대 초반부터 산업화 과정에서 함께 시작되었다면 기본 인프라(HW, SW, 기본인력)에 대한 부분이 형성되었겠지만, 한국의 보안시장은 2000년대 초 전자상거래가 시작되면서 갑자기 형성된 것이라 갑자기 보안에 대한 투자를 하려고 보니 투자액 자체가 너무 커진 상태
- 기업들은 '뭐 그동안도 투자 안하고 잘 지내왔는데' 라는 안이한 생각을 하게 되고 정부도 익숙하지 않은 분야라 잘 챙기지 못한 것이 합쳐져서 정보보호산업의 영세화를 불러왔다고 평가

발제 3. 플랫폼 기반 정부에서의 사이버안보 인재양성

김태성 교수 (충북대학교)

□ 사이버안보의 회복탄력성 확보의 주체가 바로 사이버안보 인재

○ 지능정보사회의 정보보호 위협이 가파르게 증가하고 있고 정보보호의 대상이 개인정보에서부터 민감한 군사정보에 이르기까지 매우 광범위해져, 숙련된 보안 전문인력의 역할은 더욱 커지고 있음[1)]

- 대응 전담팀을 별도로 운영하는 것이 매년 증가세에 있는 데이터 유출로 인한 피해를 감소시키는 가장 효과적인 방법으로 제기되고 있으며[2)], 이로 인해 전문역량을 보유한 인력의 확보가 중요

○ (ISC)² 는 2021년 발표한 조사보고서에서 세계적으로 272만 명의 정보보호 인력이 부족하다고 보고[3)]. 2020년 부족분은 312만 명이었는데 줄어든 이유는 2020년 이후 신규인력이 대거 진입했기 때문으로 분석

- 정보보호 전문가로 가기 위한 경력경로가 변화하고 있는데, 여전히 IT 배경을 가지고 있는 것이 일반적이지만(응답자의 47%), 진입경로가 다양해지고 있다고 분석. 약 15%는 정보보호 정규 교육과정으로 교육받았고 15%는 정규과정 이외의 수단을 이용하여 정보보호 교육을 받고 진입

○ 보안 인력은 전 산업에서 활동하며, 기본적인 IT 배경에 정보보호 전문성을 결합하여 전문인력으로서 역할을 수행

- 지능정보 사회로 진입하는 문턱에서 기업들은 인공지능, 사물인터넷 등의 지능정보 기술의 이해와 이에 대한 보안 위협에 대응하는 숙련된 전문성을 모두 갖춘 인력을 희망
- 더욱이, 사회 · 경제 기반의 IT 의존도가 높아져 감에 따라 정보보호가 정보보호 산업이나 IT산업만의 문제가 아닌 전 산업에 내재하는 문제로 자리잡고 있고, 이에 따라 일상적인 업무 처리 과정에서 발생하는 반복적인 정

1) https://www.cyberseek.org/index.html#aboutit (미국 CyberSeek 홈페이지; 2022.02.22. last visited)
2) Ponemon Institute, 2018 Cost of a Data Breach Study: Global Overview, 2018.
3) ISC², Cybersecurity Workforce Study, 2021.

보보호 관리나 개인정보보호에 대한 일반인들의 교육 수요도 증가

○ 인공지능과 사물인터넷의 발전으로 사이버안보를 위협하는 주체와 방법과 대상이 광범위하게 확대되고 고도화되면서, 사이버안보 문제는 얼마나 빠르게 회복탄력성(resilience)을 발현하느냐에 달렸으며 이를 이끄는 것이 바로 인재

□ 사이버안보 인재양성의 한계

○ 고도화된 지능정보 사회로의 진입을 준비하고 있는 현재 정부는 디지털 신산업 분야 핵심 인재 양성 및 확보를 목표로 다각도로 접근해 왔음

- 한국형 디지털 뉴딜 정책의 성공을 위해 인재 확보가 우선이라고 보고, 기업 수요 기반의 '실무형 인재' 양성을 위한 K-Digital Training (디지털 신기술 핵심 실무인재 양성훈련) 추진
- 데이터(D)·네트워크(N)·인공지능(A) 신산업 분야 핵심인재 양성 정책도 '기업이 원하는 인재 양성 체계' 구축과 K-Digital Training 확대 위주로 추진해 옴
- 윤석열 정부는 110대 국정과제에 사이버보안 역량 강화를 위해 보안클러스터 모델의 지역거점 확산으로 기업 성장을 지원하고, 10만 사이버보안 인재를 양성하겠다고 공식 발표

○ 기본적으로 국내 정보보호 인력 양성 및 교육 정책은 정보보호 산업 진흥 차원에서 추진되고 있기에, 정보보호 산업의 상황에 영향을 받으며 정보보호 산업의 내실성 및 직업 매력도가 인재 확보의 관건

- 현재 정보보호 기업의 89.4%가 100인 미만 규모

〈 2019년 말 기준 국내 정보보호 기업 종사자 규모별 현황 (단위: 개, %) 〉

구분	정보보안		물리보안		합계	
	기업 수	비율	기업 수	비율	기업 수	비율
20인 미만	218	41.1	437	58.1	655	51.1
20~100인 미만	237	44.6	254	33.8	491	38.3
100~200인 미만	43	8.1	27	3.6	70	5.5
200인 이상	33	6.2	34	4.5	67	5.2
합계	531	100.0	752	100.0	1,283	100.0

출처 : 국가정보원 등, 2021 국가정보보호백서, 2021.5.

- 정보보호산업 인력 수는 총 5.4만 명(2019년 12월 말 기준). 7년 미만 기술자가 58.8%를 차지하여 인력의 전문적인 숙련도 확보를 위한 지속적인 경력 계발이 어려운 것으로 파악됨. 이는 업무환경의 매력도가 낮은 데에 따른 인력의 직군 이탈, 인력 단가가 낮음에 따른 숙련인력 유지 어려움 등이 원인일 수 있음
- 2021년 정보보호 기업체의 신규 채용 계획 인원은 총 4,009명으로, 이 중에서 신입은 2,213명(55.2%), 경력은 1,796명(44.8%)

❍ 정보보호를 포함하여 지능정보 기술과 관련된 산업 분야의 경우, 업무 자체의 범주와 담당인력에 대한 수요명세가 유동적이고 비정형적
- 농업, 임업, 건축 등과 같이 역사가 오래된 산업은 업무수행에 필요한 지식 및 기술이 정형적이고 한번 익히면 거의 변동이 없기에 정규교육 기관이 산업이 필요로 하는 인력을 양성하는 데에 어려움이 적음
- 수요산업의 경기에 밀접하게 관련된 산업이나 기반이 되는 기술 자체의 변화 주기가 빠른 산업의 경우, 업무 범위가 수요나 기술의 변화에 따라 수시로 변하기 때문에 인력에 대한 지속적인 향상성 교육 지원 필요
- 정보보호의 경우, 특히 산업에서의 인력 수요가 유동적. 비정형적(보안사고 및 보안 관련 규제에 민감)이며, 보유기술 및 지식을 기반으로 해당 인력의 업무 고유성이 확보된다는 점에서 인력 유입 경로가 매우 다양하기에 교육 대상과 내용 모두가 한정적이지 않아 인재 양성이 쉽지 않음

❍ 2020년 대학·대학원의 정보보호 관련 학과를 조사한 결과에 따르면, 전문대학 24개, 대학교 53개, 대학원 67개 학과 등 총 149개 학과가 운영 중[4)]
- 2020년 전문대학 이상 정규 교육기관의 재적학생 수는 11,920명이며, 정규 교육기관이 배출한 정보보호 인력은 총 1,522명
- 공공·민간 부문 및 정부지원 사업 등으로 이루어지는 정규교육 기관 이외의 교육은 주로 재교육 형태로 진행 중. 이외 자격증 교육이나 취업준비과정 위주로 진행하고 있는 민간 교육기관을 통한 인력양성이 있음. 모두 연간 교육생 규모는 정확하게 알 수 없음

❍ 미국과 영국은 국가 사이버보안 인력양성을 위한 표준 프레임워크를 개발하고 이를 토대로 사이버보안 분야 정규 및 민간 교육기관의 교육과정 운영은 물론 사이버보안 분야에 관심이 있는 또는 재직 중인 인력이 지속적인 자기계발을 할 수 있도록 인력 전문성 관리까지 가이드

4) 국가정보원 등, 2021 국가정보보호백서, 2021.5.

- 미국은 NICE Framework (https://niccs.cisa.gov/), 영국은 CyBOK (Cyber Security Body of Knowledge; https://www.cybok.org/) 등의 사이버보안 분야의 업무를 상세히 구분하고 정의
- 국가에서 제공하는 초중고부터 대학(원) 및 재직자 재교육 과정의 모든 사이버보안 교육·훈련의 컨텐츠를 표준화하고자 노력하고 있으며, 실제 사이버보안 업무 현장에서의 실무를 가상체험하거나 인턴십 등을 통해 체화하도록 하는 프로그램을 지속 발굴 중

□ 사이버안보 인재양성을 위한 국내 정부지원사업 현황

❍ 정보보호영재교육원 (교육부, 2014년 개시)
- 「정보보호 교육센터」(2012년 개시)와 연계 [교육(행정)기관의 개인정보보호 업무 담당자 전문교육 기회 확대를 목표로 온·오프라인 센터를 권역별로 지정]
- 영재교육원은 수도권, 충청권, 영남권, 호남권으로 권역별 센터(서울여자대학교, 목포대학교, 대구대학교, 건양대학교)를 통해 "정보보호에 흥미를 가진 꿈과 끼가 있는 대한민국 초등학교 6학년부터 고등학교 2학년까지 누구나" 지원 가능

❍ 사이버 가디언즈 (과기부, 2016년 개시)
- 「사이버 시큐리티 인력양성 종합계획」 실행사업으로 개시
- 가디언즈 보안캠프 ☞ 중학생 대상 사이버 보안과 정보보호에 대한 관심과 흥미 유발을 위해 이론과 실습 체험형으로 구성한 교육 프로그램
- 지도자 양성교육 ☞ 중·고교 교사 대상으로 정보보안 교수 역량 제고를 목적으로 만든 프로그램. 한국정보기술연구원 주관
- 정보보안 교육 운영 지원 ☞ 2021년 지원 대상 학교는 한국디지털미디어고등학교, 세명컴퓨터고등학교, 성남테크노과학고등학교, 선린인터넷고등학교, 덕영고등학교, 경북소프트웨어고등학교 등 6개교

❍ 대학정보보호동아리연합회(KUCIS) 지원사업(과기부, 2006년 개시)
- 정보보호 인재 페스티벌, 산업현장 전문가 특강 및 멘토링, 정보보호 실습교육, 프로젝트 결과발표회 등의 프로그램으로 운영
- 한국정보보호산업협회 주관 (대학정보보호동아리 지원사업은 2006년부터 한국인터넷진흥원 주관으로 개시. 중간에 중단된 적도 있음)
- 2021년 24개 정보보호 동아리를 대상으로 평가하여 우수동아리 3개 선정 (서울여자대학교 SWING, 백석대학교 HUB, 국민대학교 PEPSI)

❍ 차세대 보안리더 양성 프로그램 Best of the Best(BoB) (과기부, 2012년 개시)
- 과학기술정보통신부 주최, 한국정보기술연구원(KITRI) 주관
- 정보보안 기술과 산업의 미래를 이끌어 나갈 차세대 리더 양성 목표
- 고등학생 및 대학생이 지원하여 1년여간 교육을 받음

❍ K-Shield Jr. (과기부, 2018년 개시)
- 고등학교나 대학교 졸업자 또는 졸업예정자로서 관련 분야로 취업을 희망하는 미취업자는 모두 지원 가능
- 고용계약형 석사과정 및 차세대보안리더(BoB) 수료생도 지원 가능
- 과학기술정보통신부 주최, 한국인터넷진흥원 주관
- 정보보호 분야 취업시 현장실무를 즉각 수행할 수 있는 사이버보안 전문 주니어 인력양성을 목표로 하는 프로그램
- 국가직무능력표준(NCS)에 맞춘 실습 중심의 교육과정 운영. 운영기관별 100명씩 총 200명을 선발하여 200시간 이상의 교육과정 이수 후 취업까지 지원하는 실무 맞춤형 교육과정

❍ 정보보호 특성화대학 지원사업 (과기부, 2015년 개시)
- 「K-ICT 시큐리티 발전전략」 최고 인재양성을 위한 실행사업으로 실시
- 정보보호 주요직무별 특화된 교육과정을 통해 현장 맞춤형 정보보호 실무 인력을 양성하는 것이 목표
- 1차사업 2015년~2021년
(서울여자대학교, 아주대학교, 고려대학교 (15년~20년), 충북대학교(16년~21년))
- 2차사업 2021년~2025년(예정). 21년 2개교(고려대학교(세종), 세종대학교) 신규 선정, 25년까지 8개교로 확대 예정

❍ 고용계약형 석사과정 지원사업 (과기부, 2009년 개시, 2018년 종료)
- 대학과 기업들이 컨소시엄을 구성해 석사과정을 개설하면, 정부가 지원
- 석사과정 졸업 후 학생들은 입학시 매칭된 업체에서 최소 2년의 계약 기간 동안 의무적으로 근무하여야 함
- 건국대학교, 고려대학교, 단국대학교, 동국대학교, 상명대학교, 성균관대학교, 순천향대학교, 숭실대학교, 아주대학교, 조선대학교, 중앙대학교, 충북대학교

❍ 지역전략산업 융합보안 핵심인재 양성사업 (일명 융합보안대학원지원사업, 과기부, 2018년 개시)
- 지역전략산업과 연계한 문제해결형 과제 중심의 교육과정 운영을 통해 현

장 맞춤형 융합보안 핵심인재를 양성하고, 지역 생태계 조성을 목표로 개시
- 2019년 고려대(스마트공장), 전남대(에너지산산업), KAIST(스마트시티) 선정. 2020년 강원대, 성균관대(디지털헬스케어), 부산대(핀테크), 순천향대(자율주행차), 충남대(스마트시티) 선정

□ 사이버안보를 위해 어떻게 인재를 확보해 나갈 것인가

○ 첫째, 보안 업무를 설명하여 딱 필요한 인재를 양성할 수 있는 기준인 보안 업무 표준 프레임워크 개발 필요
- 이는 모든 교육과 인재 양성의 기본 뼈대로 활용할 수 있기 때문
- 기업은 어떤 업무에 인력이 필요한 것인지를 설명하는 기준이며, 교육기관은 무엇을 가르쳐야 할지를 설명하는 기준. 인력은 경력계발 방향을 설정하고 학업계획을 수립하는 기준이 됨

○ 둘째, 縱(전문성)과 橫(보편성)의 방향으로 보안 인재를 확보해 나가야 함
- 전문성을 갖춘 숙련된 인재 양성과 모두가 보안인력이 될 수 있는 보편적인 보안 교육 확대가 동시에 이루어져야 함
- 국가 차원의 사이버공격이 발생했을 때 빠르게 회복탄력성(resilience)을 발휘하려면, 사회 전반에 걸쳐 보안의 중요성과 필요성을 인식하고 행동할 수 있는 체계를 구축하는 것이 필요하며 이는 지속적인 (재)교육을 통해 가능

○ 셋째, 교육기관의 인재 양성 주체로서의 역량 강화 필요
- 고등학교 및 대학(원) 등의 인재 공급자로서의 종합적인 역할이 중요
- 현재의 교육시스템은 인재 수요 및 기술 흐름을 파악하여 교육과정을 즉시 수정하고 학위를 수여하는 과정을 운영할 수 있는 자체적인 역량이 부족
- 기술을 중심으로 발전하는 지능정보사회에서는 개인들도 단일 전공만으로는 강점을 확보하기 어려움. 복수전공이나 협동과정 이수 등이 있으나 명확한 취업 분야에 대한 명세가 없어 학생 스스로 준비하는 데에 한계가 있음
- 지역별로 산재해 있는 특성화고, 전문대학, 대학(원) 정보보호 전공.학과를 연계하고, 기존 정부 지원사업들을 연결하여 통합관리체계를 구축하는 것이 급선무. 인재 양성의 속도도 빨라질 수 있고 인재 양성의 범주도 넓어질 수 있으며 사업간 중복 문제도 해결할 수 있음
- 취업 분야를 명세화하여 제시하고 갖춰야 하는 지식 및 기술을 중심으로 교과목들을 편집하여 학습할 수 있도록 함으로써[국가 주도로 개발하는 보안 업무 표준 프레임워크 기반], 교과목별로 전공 수준의 전문성을 갖춘 인재를 시장에 보다 빠르게 공급하는 체계 구축 가능

❍ 넷째, 보안 업무 또는 산업이 매력적인 경력계발 분야임을 인식시키기 위한 노력 필요

- 평생직장의 개념이 사라진지 오래이며 긱이코노미(Gig Economy)의 영향으로 긱워커(Gig Worker) 개념까지 등장. 보유한 기술을 자산화하여 하나의 직장에 얽매이지 않고 다수의 계약관계로 일하는 방식으로서, 정규직 채용·유지에 부담을 느끼는 업체들도 이러한 간접 고용을 선호
- 개인 차원에서 장기적인 경력계발의 타임라인 내에서 보안 업무가 성장에 있어 유리한 경력요소가 될 수 있음을 보여주어야 함. 이를 위해서는 보안 전문가 인증, 보안 전문 자격제도 확대 등이 필요
- 이는 국가 주도로 개발하는 보안 업무 표준 프레임워크를 기반으로 인력의 표준 경력계발 경로를 제시해 주는 작업이 함께 필요

지정토론: 유지연 교수 (상명대학교)

□ 사이버안보 분야 인재양성은 양적 인재양성 뿐만 아니라 질적인 일정 '표준'이 필요

○ 사이버보안 업무 위주로 미니멈이 맥시멈이 된다라는 인식은 사이버안보의 전체 틀 안에서는 한계가 있으므로 보다 큰 틀의 프레임워크를 만들어야 함

○ 인력의 역량 분석 체계를 우선 만들고 (ex. 호주의 ASD Framework) 인력구성과 역량, 필요역량 등을 매칭하는 작업이 요구됨

□ 사이버안보 인재양성 '전략' 방향 설정

○ 산업을 위한 인재양성인지, 공세적 대응을 위한 인재양성인지 등 보다 구체적인 인재양성의 성격과 방향을 규정하여 설계할 필요
→ 인력의 분포 및 배분과 직결되는 문제

○ 인력의 역할 및 활용 방안이 함께 구체화되어야 함 (화이트해커 10만 ? 과연 그 인원이 그 역할에 필요한 것인가?)

□ 재교육 체계 반드시 마련

○ 표준 교육 형태를 갖춤과 동시에 교육기관마다의 특수성을 가미

○ 표준 교과과정 + 재교육

□ 공공기관의 사이버보안 전담 인력 확보

○ 정원규제로 인한 어려움을 정보보호 인원 별도 정원 운영 제도 등의 마련으로 돌파

*본고의 내용은 세종연구소의 입장과 무관합니다.

작성자 : 신소현

사이버보안산업 육성을 위한 신정부 정책방향

– 세종 사이버 안보 포럼 –

- 일시 : 2022. 5. 25 (수)
- 장소 : 서머셋팰리스 서울 (2층 세미나 룸)

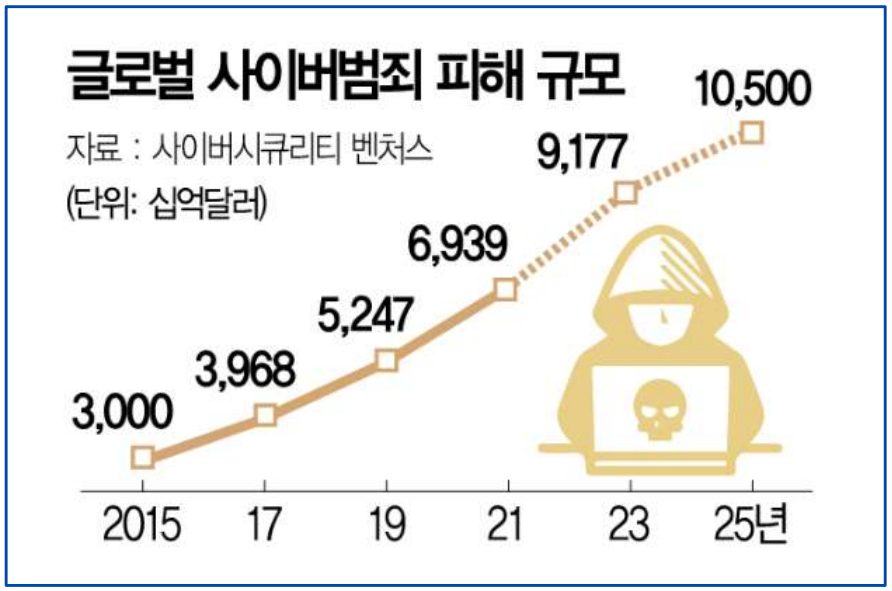


kisia
한국정보보호산업협회
Korea Information Security Industry Association

1. 사이버 침해 실태 및 정보보호산업의 현주소

사이버 침해 실태 및 정보보호산업의 현주소

① (글로벌) 사이버범죄 피해 매년 증가 예측





- ✓ 글로벌 사이버 범죄 피해액 **6조 9,390억 달러**
- ✓ **2025년 10조 달러까지 커질 것으로 예측**
- ✓ 미국 '21년 상반기 약 7,000억 원의 복구비용 지불
- ✓ 전년 대비 약 42% 증가한 수치
- ✓ 미 백악관은 한국, 영국, 프랑스, 독일, 일본 등 전세계 우방 30개국과 '랜섬웨어 대응 이니셔티브 화상회의 개최' → **사이버 집단 안보체제 구축 의지**

☞ 2013년 시만텍 '노턴 사이버 범죄보고서',

연간 사이버 범죄 피해 금액이 3,880억 달러로 2,880억 달러인 세계 마약 시장을 추월했다고 보고한 바 있음

사이버 침해 실태 및 정보보호산업의 현주소

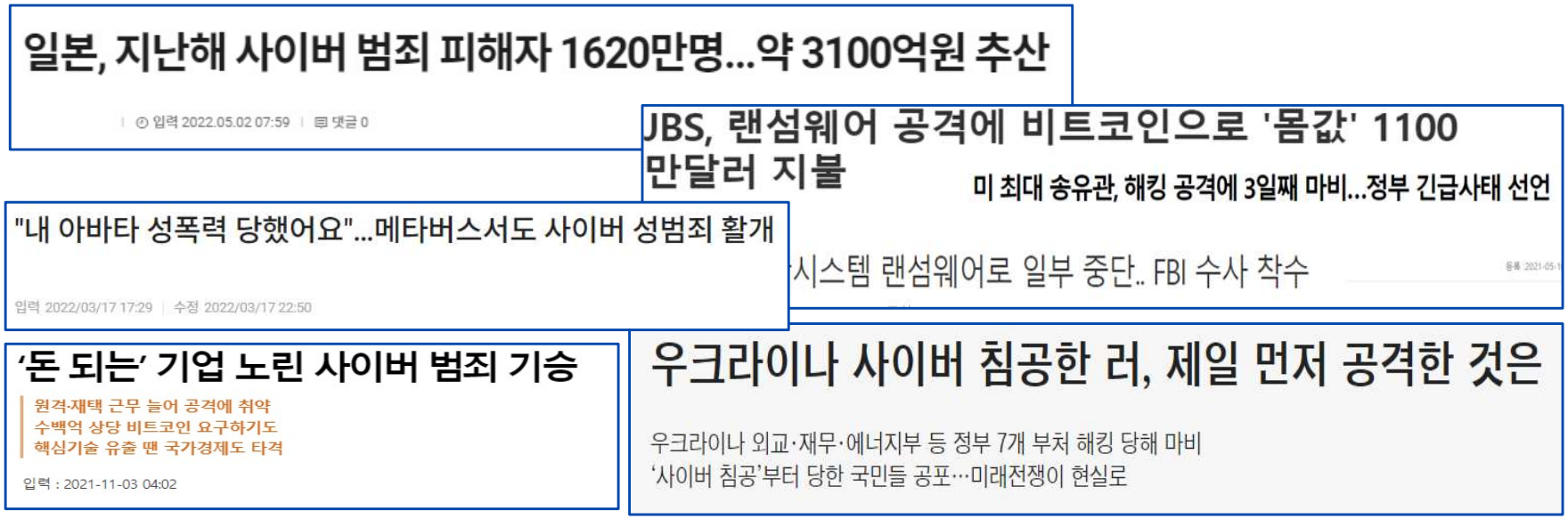
② (글로벌) 사이버범죄 대상 범위 다양화

✓ 국가 기반시설과 국민 생활에 밀접한 분야에 대한 사이버 공격 확대

☞ 송유관회사 '컬로니얼 파이프라인', 랜섬웨어 공격 긴급사태 선포

☞ 세계 최대 육가공업체 'JBS', 사이버공격 '글로벌 공급망' 위협

☞ 뉴욕시 법무과 전산시스템 랜섬웨어 공격, 서비스 일부 중단

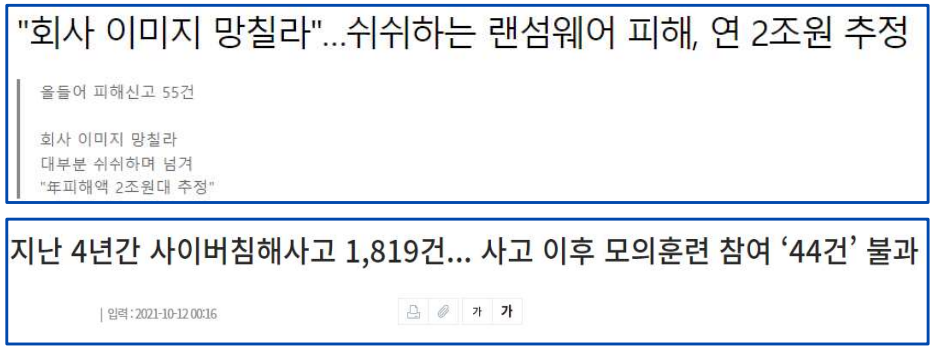


사이버 침해 실태 및 정보보호산업의 현주소

③ (국내) 사이버 침해 피해 현황

- ✓ 최근 5년간 전체 범죄는 13.4% 감소, 사이버 범죄는 20년도 18만 건으로 전년 대비 약 24.8% 증가
- ✓ 21년 국내 랜섬웨어 피해 기업 10곳 중 9곳은 중소기업
- ✓ ① 자신들이 사이버 침해 피해를 입었는지 인지하지 못하는 경우가 많으며
- ✓ ② 자신들이 사이버 침해 피해를 입더라도 이를 드러내지 않고, 관련 기관에 신고하지 않는 경우가 많음

☞ 정확한 현황 파악 및 대응 방안을 수립하지 못하는 현실, 정확한 피해규모 파악 불가


"회사 이미지 망칠라"...쉬쉬하는 랜섬웨어 피해, 연 2조원 추정

올들어 피해신고 55건

회사 이미지 망칠라
대부분 쉬쉬하며 넘겨
"年피해액 2조원대 추정"

지난 4년간 사이버침해사고 1,819건... 사고 이후 모의훈련 참여 '44건' 불과

| 입력 : 2021-10-12 00:16


[단독] "신고해도 실익 없다"...대기업, 해킹 피해 '쉬쉬'

입력 2021.10.18 17:00 | 수정 2021.10.19 01:20 | 지면 A16

"복구 지원 못 받고 이미지 손실"
랜섬웨어 신고 건수 4년간 6건

- ✓ 글로벌 해커조직(7,000명) 보유한 북한 ☞ 잠재적 보안 위협 존재

※ 美 바이든 행정부, '국가의 사이버 보안 강화를 위한 행정명령'과 '핵심 인프라 제어 시스템을 위한 사이버 보안 개선에 관한 국가 보안 각서' 발표 → 사이버 침해사고 발생시 중요 인프라 기업의 신고 및 보고 의무화

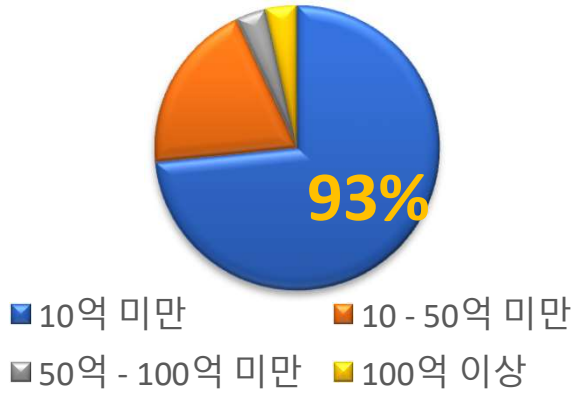
사이버 침해 실태 및 정보보호산업의 현주소

⑤ 국내 사이버 보안 시장 규모 (기업 현황)

〈 국내 정보보안기업 자본금 규모별 현황 〉

구분	10억 미만	10억 이상~ 50억 미만	50억 이상~ 100억미만	100억 이상	합계
기업수(개)	390	104	18	19	531
비율(%)	73.4	19.6	3.4	3.6	100

정보보안 기업규모 (자본금)



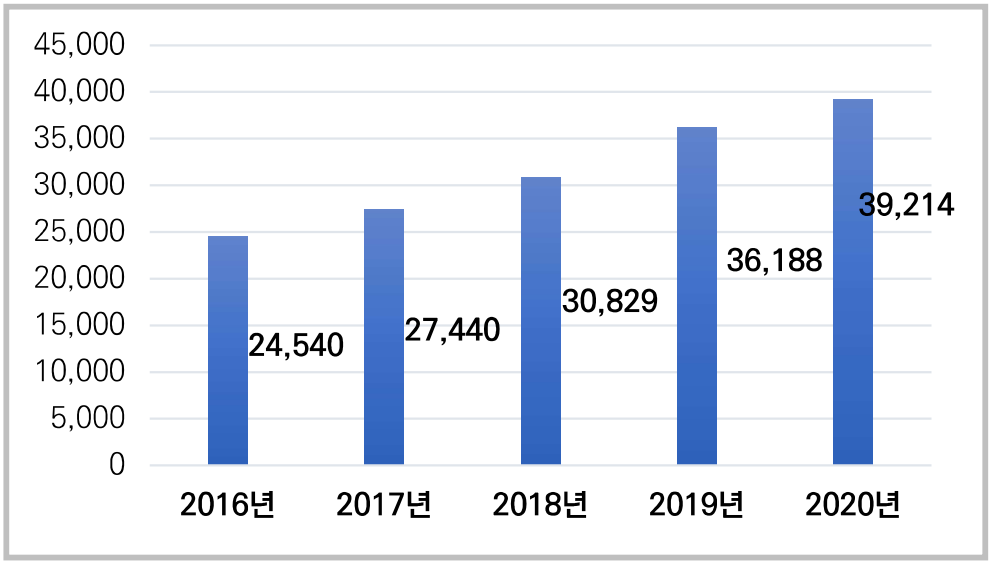
"22년 정보보호 기업 규모 자본금 10억 미만 기업 971개(75.7%)로 기업 규모 영세 "

전체 기업수 1,283개 중 10억 미만 기업이 대다수로(75.7%),
10억 이상 50억 미만 기업(17.5%)를 합하면
전체 93.2%가 영세한 기업에 속한다.

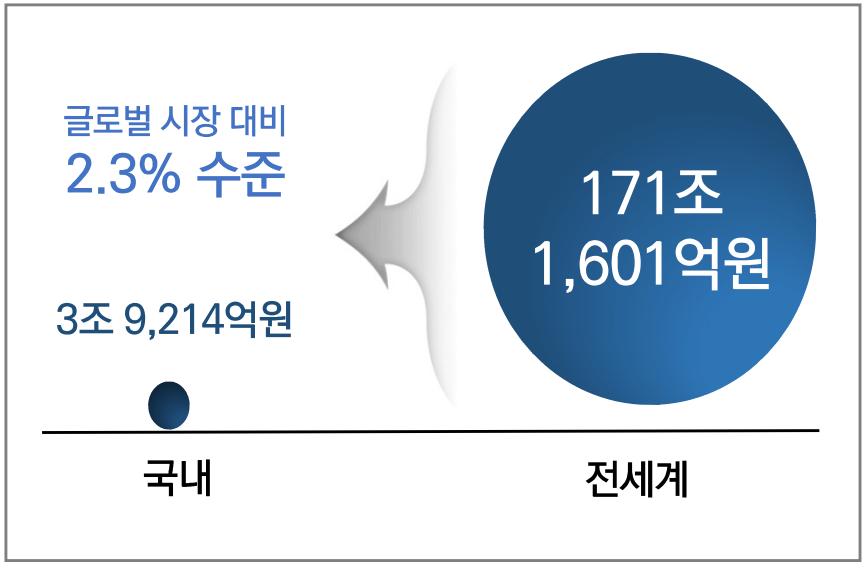
사이버 침해 실태 및 정보보호산업의 현주소

⑤ 국내 사이버 보안 시장 규모 (매출 현황)

국내 정보보안산업 매출액 현황(억원)



2020년 국내 및 전세계 정보보안산업 규모



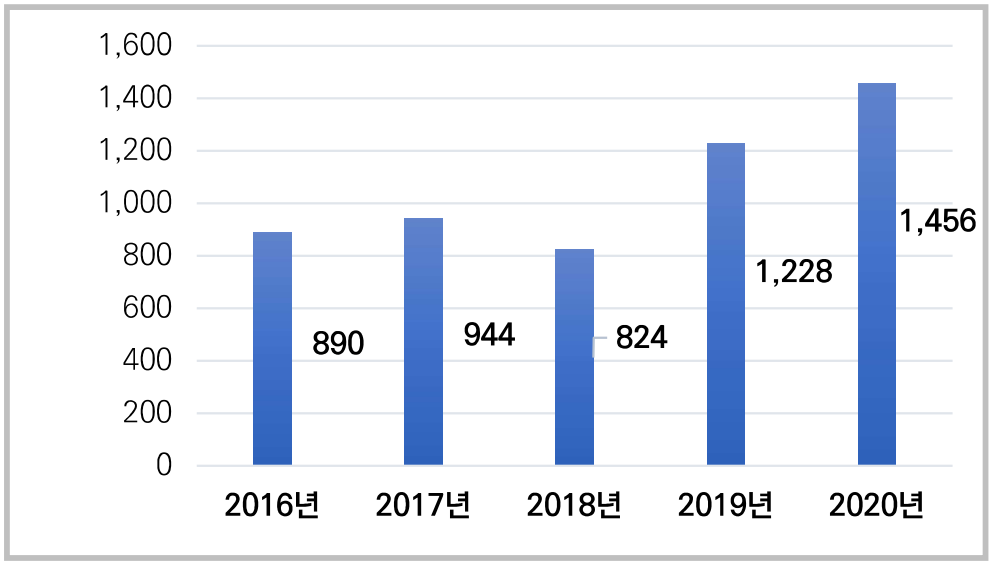
❖ 출처 : 2021 정보보호산업 실태조사(KISIA), 2020 글로벌 정보보호 산업시장 동향조사(KISA)

2020년 국내 정보보안 매출액은 3조 9,214억원으로 2019년 대비 8.4% 증가하였으나 여전히 세계시장의 2.3% 수준으로 나타남

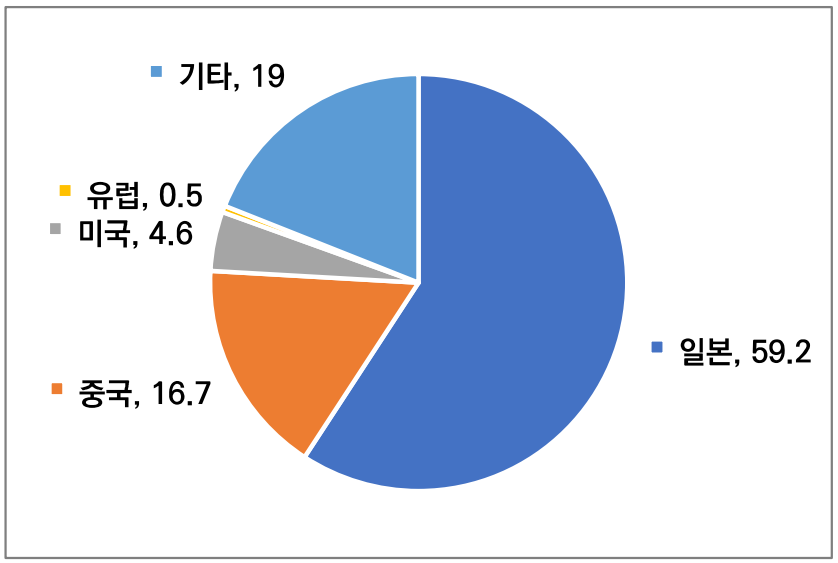
사이버 침해 실태 및 정보보호산업의 현주소

⑤ 국내 사이버 보안 시장 규모 (수출 현황)

국내 정보보안산업 수출액 현황(억원)



2020 정보보안산업 국가별 수출 현황(%)



❖ 출처 : 2021 정보보호산업 실태조사(KISIA)

- ❖ ’20년 정보보안 수출액은 1,456억원
- ❖ 매년 소폭 상승하고 있으나 일부 기업의 수출 실적에 의존
- ❖ 특정 기업의 수출 감소시 전체 매출액에 타격 발생

※ 정보보안 수출은 전세계 10% 비중에도 미치지 못하는 일본시장(약 13조원)에 집중되어 (2020년 59.2%)있으며 최대 시장인 미국으로의 수출은 4.6% 수준

사이버 침해 실태 및 정보보호산업의 현주소

⑥ 보안산업 유니콘기업

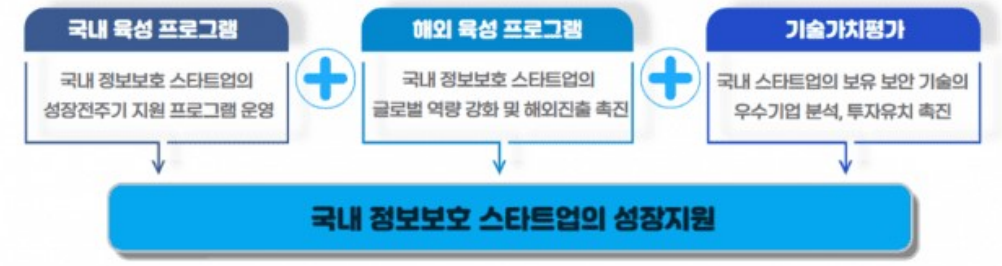
✓ 21년 사이버보안 분야 신규 글로벌 유니콘 기업 Top10 현황

– 미국(6개)과 이스라엘(3개) 캐나다(1개) 기업이 차지

<전세계 사이버 보안 유니콘 기업 수 (CB Insight) '21.12.31. 기준>

국가	미국	이스라엘	캐나다	영국	스위스	중국	합계
유니콘 기업	31개	6개	2개	1개	1개	1개	42개

✓ 글로벌 경쟁력을 갖춘 대형 신생 보안 기업 육성



✓ **새로운 시장에서의 성장 지원**

– AI 기반 보안, 융합보안, 블록체인, IoT 등

– 새로운 시장에 대한 선점을 위해 유관 분야 협력 필요

✓ **산업 내 M&A 및 투자 유지 확대 지원**

– 안정적인 기업 성장을 위한 투자 및 M&A 지원 확대

✓ **핵심 기술 확보를 위한 R&D 강화**

– 정부의 R&D 투자를 통한 기술 이전, 기술 협력의 확대

– 기술 경쟁력 확보를 통한 세계 무대 진출 지원

2. 사이버 침해에 대한 선도적 대응

사이버침해에 선도적 대응 필요

1 **사이버보안의 사회 이슈화**

(사이버 범죄와의 전쟁 선포) 국가 차원의 사이버 보안 강화 의지 표현

2 **국가 사이버보안 총괄 컨트롤 타워 구축**

(컨트롤타워 구축) 민, 관, 군을 총괄할 수 있는 체계 마련

3 **랜섬웨어로부터 중소기업의 해방**

(중소기업 지원 및 홍보 수행) 다양한 중소기업 맞춤 솔루션 지원 및 대국민 홍보 수행

4 **메타버스 등 웹 3.0 인터넷 전환 대응**

(표준 모델 및 지재권 보호 강화) 디지털 환경에서의 권리 및 자산 보호를 위한 제도적 보완책 마련

5 **산업시설(스마트팩토리 등), 국가기반시설 보호**

(기반시설 관리 환경 구축) OT보안 기술 개발, 공급망 보안 체계 구축 등을 통한 산업 안전망 확보

사이버침해에 선도적 대응 필요

① 사이버보안의 사회이슈화

✓ 국가차원의 사이버 보안강화 의지를 담은 **'사이버 범죄와의 전쟁'** 선포 및 강력한 대응 방안 수립·집행

☞ 지능화되어가고 있는 사이버 위협에 대해 국가 전체의 역량을 결집한 대응 필요



2022년 주요 사이버위협 전망
Log4j 취약점 장기화
사물인터넷(IoT) 기기 대상 사이버위협
끊임없는 랜섬웨어 위협
디지털 대전환 핵심 '클라우드' 보안 위협
메타버스·NFT, AI 등 신기술 대상 신종위협
사회적 이슈 활용한 스미싱·해킹 메일 지속

자료:과학기술정보통신부 · 한국인터넷 진흥원

사이버침해에 선도적 대응 필요

② 중소기업을 랜섬웨어로부터 해방

- ✓ 컨설팅을 통해 중소기업 환경에 맞는 맞춤형 솔루션을 지원하고 중요데이터 백업 지원

- ✓ (홍보 강화) 중소기업 스스로 랜섬웨어에 대응하기 위해 TV광고 및 다큐멘터리 제작, 홍보대사 운영 등을 통한 대국민 홍보 필요



사이버침해에 선도적 대응 필요

③ 메타버스 등 웹 3.0 인터넷 전환 대응

✓ 개인 계정을 해킹하여 가상자산, 결제 정보를 활용해 금전적 피해를 입히거나 가상자산 불법 복제가 예상

☞ 표준 보안모델 개발 및 지재권 보호를 위한 **제도적 보완책 마련 필요**

메타버스에서는 사용자의 시선, 뇌파, 행동, 발언 등 기존에 없던 다양한 데이터가 축적

보안사고 발생시 큰 피해로 이어질 가능성이 높음


메타버스 시대 '보안' 없이는 기회도 없다…'인증' 보안 마련 급선무

김가은 기자 | 승인 2022.04.13 17:45

가 가

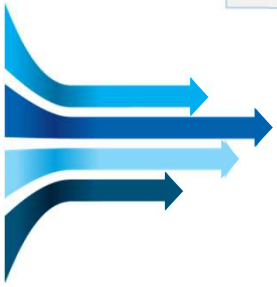
/사진=디미넷 제공

사이버침해에 선도적 대응 필요

④ 산업시설, 국가기반시설 보호

- ✓ 기반시설들을 관리하는 운영기술(OT, operation technology) 환경은 폐쇄망으로 운영되었으나
- ✓ 디지털전환에 따라 수많은 산업용 기기들이 유지보수, 패치를 위해 인터넷에 연결

산업시설 등 대상의 사이버위협 증가



스마트시티, 대규모 플랜트 등 산업시설과 교통, 통신, 에너지 등 **국가주요 기반시설 및 군사안보시설을 안전하게 제어하기 위한 기술개발 및 인프라 구축 필요**

사이버침해에 선도적 대응 필요

⑤ 국가 사이버보안 총괄 컨트롤 타워

사이버보안 특성상* 민·관·군을 총괄하는 체계 필요

고도화, 지능화되고 있는 사이버공격에 선제적 대응을 위해 강력한 국가사이버보안 컨트롤 타워 구축 필요

* 초 단위로 빠르게 퍼지는 사이버위협 및 사고에 의해 막대한 피해를 입을 수 있으며, 국가 단위의 대규모 피해 발생도 가능함

※ 현 사이버보안 대응체계 : 민간(과기정통부,KISA), 공공(국정원), 국방(국방부)로 3分

110대 국정과제 '101. 국가사이버안보 대응역량 강화' 주요 내용

- 대통령 직속 국가사이버안보委 설치 및 운영체계 강화
- 민관 합동 사이버협력체계 강화
- 안전한 디지털 플랫폼 정부 구현
- 기술 고도화 및 국제협력 강화

3. 정보보호산업의 글로벌 수준 육성

사이버보안산업의 세계적 수준 육성을 위한 방안

1

사이버보안 패러다임 전환

(스타트업 활성화) 다양한 인증기준을 통해 창의적인 아이디를 보유한 정보보호 스타트업 활성화 기반마련

2

혁신보안제품 개발 환경 조성

(구독형 서비스 활성화) 일체형 정보보호제품의 도입과 함께 다양한 서비스를 제공할 수 있는 구독형 서비스 활성화

3

정보보호기업의 대형화 유도

(보안투자 활성화) 정보보호 투자활성화를 통한 기초가 튼튼한 정보보호산업 생태계 조성

4

스타트업 육성

(사이버보안 중점 투자펀드 운영) 정보보호 스타트업 성장 지원을 위한 전용 전문투자조합 출자

5

보안지속성서비스비 지급

(정보보호 대가지급 정상화) 정보보호 제품, 서비스에 대한 적정 대가 지급 및 보안 연속성 유지

정보보호 산업의 글로벌 육성

① 사이버보안 패러다임 전환

국외



지난해 *기반시설 목표로
랜섬웨어 공격 진행
대혼란 야기

*송유관회사 →최대 육가공업체
→ 뉴욕시 법무전산시스템 등

국내



랜섬웨어
피해 대폭 증가로
심각한 피해 발생

*기업의 40.27%가 랜섬웨어
피해 경험, 이중 절반
가까이(44.86)는 대응 방안 없음

✓ 기존 방어 기술로 대응하기 어려운 사이버 공격 증가

- 사회 공학적 기술을 통한 중요 정보 탈취
- 공급망 공격으로 광범위한 피해 유도
- AI 등 첨단기술을 활용한 공격으로 실시간 대응/차단 어려움

✓ COVID-19 로 인한 일반 기업의 디지털 전환 가속화

- 보안 역량이 부족한 중소기업 증가로 공격 대상 지점의 증가

디지털 콘텐츠 및 지식재산권
보호 조치 관련
보안 방안 필요

- NFT 위작 보증 시스템
- 브랜드 지재권, 개인정보 보호

IoT 적용 확대에 따라
수많은 산업용 기기 연결
사이버 공격 증가

- 국내 원전 등 중요시설
핵심기술 탈취사이버공격지속
발생

DX 관련 *신기술 분야, 융합
인프라 보강 강화를 위한
기술개발 및 투자 강화

*양자암호,5G,스마트팩토리,메타버스.
IoT, 블록체인 및 융합 보안 등

연구개발, 보안인프라 구축 등
보안정책 수립 및 시행

정보보호 산업의 글로벌 육성

② 혁신보안제품 개발환경 조성

✓ 사이버보안은 신종위협에 대응이 가능한 아이디어의 신속한 제품化와 사업化가 관건

☞ 정보보호제품 인증 제도 개선을 통해 혁신 제품 개발 환경 조성 필요

☞ 인증 제도 개선 → 신기술의 진입장벽 해소 → 혁신기업 시장 진출 확대

[사이버보안 대계 세워라] CC인증 경직성 해소해야

발행일 : 2022-03-16 16:00 지면 : 2022-03-17

인증·조달체계 개선 최우선
신기술 진입장벽 해소 필요
시행령 개정·인프라 확충하고
기업 인증 등 발상 전환 촉구

IoT 기기 정보보호인증 제도 활성화... 사이버보안 확보 기대

승인 2022.01.08 20:28

[보안칼럼]CC인증 개선, 포스트 코로나 시대 '혁신 마중물'로

발행일 : 2021-02-22 16:00 지면 : 2021-02-23

천편일률적인 클라우드·망분리 규제 개선된다

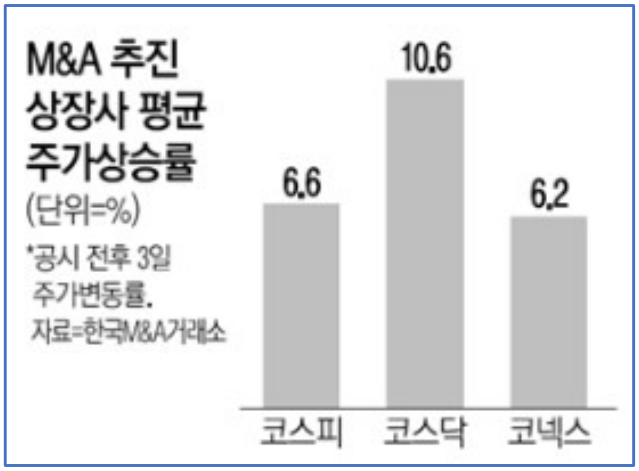
송고 2022.04.14 13:38
수정 2022.04.14 13:39
EBN 신주식 기자 (winean@ebn.co.kr)

클라우드 이용시 업무중요도 평가 구체적 기준 마련하고 CSP 평가 간소화
비중요업무 등은 망분리규제 예외 적용 "논리적 망분리 선택권 부여 검토"

정보보호 산업의 글로벌 육성

③ 정보보호기업의 대형화 유도

✓ 글로벌 경쟁력 강화를 위해 기존 정보보호기업, 스타트업 등의 M&A를 통한 대형化·전문化 촉진



이제는 보안기업?…거침없는 MS의 인수합병(M&A) 배경

Home > 전체기사

사이버 보안 분야에 M&A가 끊임없이 일어나는 이유

보안 / 비즈니스|경제

올해도 뜨겁다, 2022년 사이버보안 M&A 10건

사이버보안 M&A·IPO 기지개…韓 보안업계 몸값상승 기대감↑

✓ **해외 사이버 보안 기업들의 핵심 성장 전략으로 활용됨**

- 활발한 전략적 M&A로 대형화, 전문화 추진 중
- 스타트업, 유니콘 기업은 물론 일반 IT대기업 역시 M&A 확대
- 다양한 기술 및 인력의 확보는 물론, 기업 경쟁력 확대 가능

✓ **국내 기업들을 위한 제도적 뒷받침 필요**

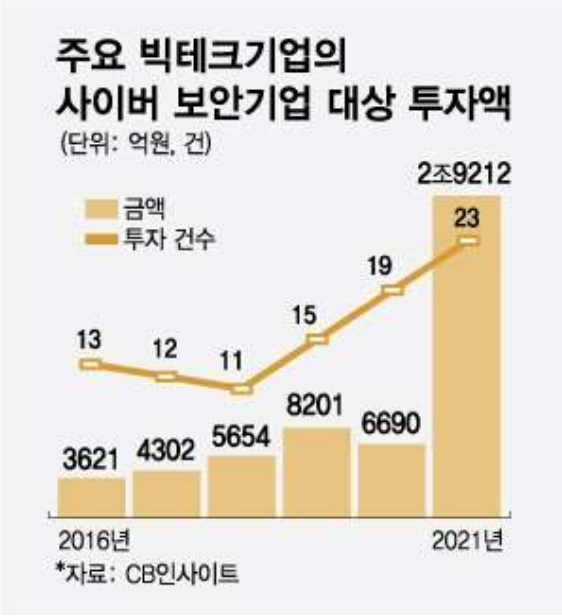
- M&A를 위한 금융 지원 강화(전문투자조합, 모태펀드 등)
- M&A를 위한 통합 컨설팅 지원 강화
- M&A에 대한 부정적 인식 개선을 위한 홍보, 교육 강화

정보보호 산업의 글로벌 육성

④ 스타트업 육성

- ✓ 글로벌 정보보호 기업 육성과 유망 보안 스타트업 성장지원을 위해 사이버보안 중점 투자펀드 조성 및 운영 필요 ☞전문투자조합(子펀드) 출자를 통한 母胎펀드형태 운영
- ✓ 정보보호 스타트업 제품/서비스에 대한 정부 · 공공기관의 강력한 예산집행 및 도입 의무화
  - ☞ 국내 공공 서비스 등의 납품 레퍼런스가 해외 수출 시 큰 지렛대 역할 수행

〈빅테크 기업의 사이버보안 투자액 2조9,212억원〉



〈이스라엘의 사이버 보안 기업 육성 사례〉



- ✓ 젊은 인재들의 '군(軍)' → '학(學)' → '산(産)' 선순환
- ✓ 정부의 활발한 투자와 M&A를 통한 자본금 지원
- ✓ 자유로운 네트워크를 통한 기술 협력, 투자, 채용

정보보호 산업의 글로벌 육성

⑤ 보안성지속서비스비 지급 정상화 필요



- ✓ 신규 취약점은 지속적으로 발생

  ※ 하루평균 악성코드 탐지 약 2만 3000건 (KISA)

- ✓ 신규 취약점에 대비하기 위해 정보보호기업은 제품도입 즉시 보안성 지속 서비스를 통해 제품의 보안성을 유지하고 있음

- ✓ 보안성지속서비스에 따른 대가 지급을 통해 **기업의 성장 동력 확보 및 고객 서비스 향상**

※ 유지관리 : 제품 수정 및 보완, 기능향상, 장애처리지원, 고객 맞춤지원(커스터마이징), 교육 등

※ 보안성 지속 서비스 : 보안업데이트, 보안정책관리, 보안기술 자문, 위협/사고분석

4. 정책 제안

민·관 협력 원스톱 서비스 지원 제도

랜섬웨어 위협 대응 정책 제안 – 대응 현황 분석

✓ 정보보호 관련 기관 및 보안 서비스 제공 기업의 유기적인 연결성 부족으로 일회성에 그침

과기정통부

랜섬웨어 종합 대책

개별 지원 정책이
상호 유기적으로 연결될 필요가 있음

KISA

랜섬웨어 신고 센터

신고, 원인분석에 이어 데이터 복구
및 향후 대응 서비스 보완 필요

기업(KISIA)

랜섬웨어 대응 서비스 및 제품

개별 기업의 제품 홍보 한계
SMB에 기술과 서비스가 도달 못함

민·관 협력 원스톱 서비스 지원 제도

랜섬웨어 위협 대응 정책 제안 – 원스톱 Cycle

- ✓ 정부의 **정책 주관(예산 지원)** → 전문 기관의 **분석, 복구** → 보안 기업의 **후속 서비스 제공**
- ✓ 랜섬웨어 피해 이후 기업의 업무 정상화와 대응 역량 강화 및 자체적 보안 역량 유지 유도

STEP 1. 피해 신고
신고 창구 개선을 통해
기업 피해 신고 창구 일원화
피해 유형별 신고 절차 정비

STEP 6. 홍보 및 결과분석
랜섬웨어 차단, 대응 효과
분석, 지속적인 정책 지원
유도

STEP 5. 바우처 지원
바우처 사업을 통한
보안 서비스 이용 지원
기업 비용 부담 경감



STEP 2. 피해 분석
피해 분석 서비스 제공
복구 가능 여부, 피해 원인
분석 등의 진단 수행

STEP 3. 복구 지원
데이터 복구 및 업무 정상화
정부의 비용 지원 지양
(복구 비용 기업 자부담)

STEP 4. 재감염 방지
KISIA 기업 채널을 통해
보안 서비스 이용 기회 제공
(체험판, 단기 서비스 등)

5. 결 론

정보보호 산업의 글로벌 육성

유연한 성장 동력을 통한 전략적 산업 육성 필요

사이버 침해 및 국내 사이버 보안 산업에 대한 면밀한 데이터 확보

(국내외 시장에 대한 정보 분석) 국내 사이버 보안 시장의 역량 및 문제점에 대한 지속적인 분석 필요

사이버 침해에 대한 선도적 대응으로 국가 안전망 확보

(선도적 대응) 사이버 범죄와의 전쟁 선포, 보안에 대한 국민 인식 개선, 신규 시장에 대한 선제적 연구 등의 수행

혁신적인 제도 개선과 지속적인 성장동력 공급으로 기업·시장 경쟁력 확보

(정보보호산업 육성) 기업 대형화 유도, 스타트업 기업 육성, 보안성 지속서비스비 지급 정상화 등 당면 과제 해결

- ✓ 민·관·학이 협력하여 정보보호에 함께 대응하고
- ✓ 활발한 투자와 M&A를 통해 글로벌 정보보호 기업이 탄생할 수 있는
- ✓ 혁신적이고 기초가 튼튼한 정보보호 생태계 조성



사이버보안산업 육성 위한 신정부 정책방향

㈜센스톤 최 동 근

Profile



최동근(崔 東根)

㈜센스톤 사장

前.한국CISO협회 회장

dkchoi1@daum.net

◎ 학력:
- 경북대학교 통계학과 졸업
- 고려대 정보보호대학원 정보보호전공 석사
- 롯데그룹 e-MBA / S-EMBA과정 수료
- 건국대 최고경영자과정(AMP) 수료
- 금융보안원 금융보안최고책임자(CISO)과정 수료

◎ 경력:
- 1987 LGCNS (舊.STM) 보안팀 입사
- 1998 LG그룹 IT보안감사팀장
- 2000 ㈜시큐어소프트/이니텍 보안컨설팅사업본부 상무
- 2008 롯데정보통신 통합전산센터 부문장, 상무
- 2008~2014.2 롯데그룹 정보보호위원회 간사
- 2014.3~2019 롯데카드 정보보호부문장 CISO, CPO
- 2020.1~2021 롯데카드㈜ 자문
- 2020.10~ ㈜센스톤 사장

◎ 저서: 개인정보관리사 수험서 Privacy Dictionary (2012)공저

◎ 수상:
- 2011 대한민국 사이버안전대상 국무총리 표창
- 2016 (ISC)² Announces Asia-Pacific ISLA 상 수상
  - senior information security professional 분야
- 2017 올해의 CISO상 수상 (한국정보산업연합회, 전자신문)
- 롯데카드 2017 정보보호대상 대상기업 수상 (과학기술정보통신부)

◎ 활동:
- 現 한국CISO협회 고문 (2010~)
- 現 한국정보보호학회 부회장 (2011~)
- 現 한국CPO포럼 운영위원 (2009~)
- 現 KITRI 차세대 보안리더 양성 BoB 2기 자문위원(2021 ~ 현재)
- 現 고려대학교 정보보호대학원 교우회 회장(2022)
- 前 한국CISO협회 회장(2019)
- 前 금융보안포럼 운영위원 (금융보안원, 2010~2019)
- 前 침해사고대응팀협의회 (ConCERT) 운영위원
- 前 스마트정부 오픈포럼 위원 (한국정보화진흥원)
- 前 국가인적자원개발 컨소시움 컨설팅분과 위원장 (KISA)
- 前 한국정보처리학회 이사

LG CNS
securesoft
INITECH
롯데정보통신
LOTTE CARD
SSenStone



※ CISO: Chief Information Security Officer, CPO: Chief Privacy Officer
ISLA: Information Security Leadership Achievements, 아시아태평양 정보보안 리더십 공로상

사이버보안 산업육성을 위한 제언(1/4)

1) 특정 기업이나 개인 또는 불특정 다수를 노리는 사이버 피해를 방어하기 위한 국가적인 체계마련이 필요하다.

- 어디로 신고해야 하는지 전국민이 알도록 홍보하고 운용되도록 하여야 한다.
- 신속한 피해 신고 접수 (피해 데이터의 확보, 분석을 통해 피해확산을 빠르게 방어할 수 있음)
- 사고이력의 정보축적, 유사사례 공유, 동일 산업군 전파를 통해 피해확산 방어
- 피해 신고자(기업, 개인)에 대한 신원을 확실하게 보장할 수 있는 환경이 마련
- 접수된 정보가 노출되지 않아야 하며, 어떠한 반대급부 - 언론 및 외부노출 - 를 받지 않도록 법적으로 보장되도록 하여야 한다. (분석이후 중과실이 드러날 경우 법적판단을 따르게 할 수 있으나, 피해자 또는 피해기업이 악의적으로 하지 않는 한 피해를 인정하여야 한다)
- 피해 신고자(기업, 개인)에 대한 보상체계도 신속하게 마련되어야 한다. (선지원 후분석이후 과실에 따른 구상권 청구)

사이버보안 산업육성을 위한 제언(2/4)

2) 산업시설의 사이버 운용에 따른 OT보안에 투자확대 및 체계를 마련

- 공장 자동화 등 전반에 걸친 네트워크 연결에 따른 침해 대응 필요
- 공급망에 대한 보안위협을 분석하고 대응
- 반도체, 화학, 에너지, 방산기업들의 제조라인에서의 OT보안을 반드시 마련하도록 해야 한다.

3) 보안전문 인력의 양성도 중요하지만, 양성된 인력이 활동할 수 있는 터전마련도 중요하다.

- 하이-레벨 해커를 양성한 후 이들의 기술을 발전시키고 활용할 수 있는 터전
- 보안전문 인력의 초등에서부터 군, 직업선정에 이르기까지 보안기술 커리어 패스를 제공하여야 한다.

사이버보안 산업육성을 위한 제언(3/4)

현재의 사이버 상황을 비춰볼 때, 민관군 연합의 통합적 사이버 대응을 위한 컨트롤 타워가 구축되여야 한다.

4) 유,무선 통신기반 대응을 하는 상황에서는, 과거와는 달리 통신 3사들의 국가보안을 위한 전략적 투자가 선행되도록 유도하여야 한다.

- 통신이 중단될 경우를 염두에 둔 체계마련
- 비상 상황시 IT자산을 활용할 수 있는 방안도 강구되어야 한다. (지진이나 재난, 전쟁 등의 불가항력적인 상황에서도 IT자산을 최소한으로 활용할 수 있는 환경 마련)

사이버보안 산업육성을 위한 제언(4/4)

5) 영세한 보안기업 문제

- 영역별로 그룹화하여 M&A 환경을 마련하고, 시장개척을 지원하는 시스템 마련
- 신기술 투자를 공동으로 하고 함께 시장개척을 하도록 지원한다.

6) 혁신 보안 신기술 기업 지원

- 신기술에 대한 평가 (산학연 중심으로 기술평가가 이루어 질 수 있는 공학원 같은 버츄얼 조직)
- 평가를 통해 R&D 투자 전폭 지원
- 연구소 및 기관에서의 기술이전 활성화
- 적용을 위한 관련법(시행형, 규칙)개정을 함께 추진한다.
- 글로벌 시장개척 판로지원
- 특허 등 지재권을 위한 투자지원 및 핵심기술의 보호



SSenStone

Simple & Sensible Stone

THANK YOU



세종사이버안보포럼

Sejong Cybersecurity Forum

Cybersecurity Center

SEJONG Institute