미국 정부, 2023정보보호 전략 발표

- 책임의 재분배, 협력강화, 적극적 대응, 투자의 확대 -

최근 미국 바이든 행정부는 새로운 국가사이버보안전략(National Cybersecurity Strategy)을 발표하였습니다. 주요 내용은 개인 중소기업 등이 가지고 있던 사이버보안에 대한 책임을 전문기관이 전담하고, 전략적으로 장기적인 투자를 이끌도록 하는 인센티브 재조정, 동맹국간 협력과 국가 행동 규범을 강화하고 인프라 전반에 걸쳐 효과적인 사이버 보안이 적용될 수 있도록 하는 전략입니다. 미국 행정부의 전략은 국내 정보보호 산업에도 직/간접적으로 영향을 미칠 수 있음으로 주의 깊게 살펴볼 필요가 있습니다.

1. 바이든 행정부의 사이버보안 전략의 비전

美 국가 사이버보안 전략은 사이버 위협을 해결하고 인프라 재건, 청정 에너지 부문 개발, 기술 및 제조 기반 재구축에 대한 투자를 독려하고 동맹국 및 파트너와 함께 디지털 생태계를 만들어 가는 것을 목표로 하면서, 美 행정부는 사이버 보안의 3가지 비전에 대한 키워드를 꼽았습니다.

① **Defensible**, 사이버 위협에 대한 방어가 압도적으로 쉽고, 저렴하고, 효과적이어야 한다.

② **Resilient**, 사이버 사고와 오류가 광범위하거나 지속적인 영향을 거의 미치지 않아야 한다.

③ **Values-aligned**우리가 가장 소중히 여기는 가치가 디지털 세계를 형성하고 이를 통해 강화되어야 한다.

2. 접근 방식

바이든 행정부의 국가 사이버보안 전략은 5가지의 접근 방식을 중심으로 협력관계를 구축 및 강화할 계획입니다.

1) 중요 인프라 보호

위험과 책임을 공평하게 분배하고 디지털 생태계에 기초적인 수준의 보안과 복원력을 제공하는 지속적이고 효과적인 협업 방어 모델을 운영하는 것을 목표로 하여 민간과 협력과 정부에서는 제로 트러스트 아키텍처 전략을 구현하고 IT 및 OT 인프라 현대화로 안전하고 탄력적인 시스템 구축의 성공적 모델을 만드는 것입니다.

전략적 목표	설명
① 국가안보 및 공공안전을 지원하기 위한 사이버보안 요구 사항 수립	각 부문의 위험 프로필에 맞게 조정되고, 중복을 줄이고, 민관 협업을 보완하며, 구현 비용을 인식하는 사이버 보안을 위한 현대적이고 민첩한 규제 프레임워크 필요함.
② 공공-민간 협업을 확장	CISA는 부문별 위험 관리 기관(SRMA)과 협력하여 연방 정부가 미국 전역의 중요 인프라 소유자 및 운영자와의 협력을 확대할 수 있도록 지원
③ 연방 사이버 보안 센터 통합	국토 방위, 법 집행, 정보, 외교, 경제, 군사 임무 전반에 걸쳐 범정부적 역량을 융합하는 협업 노드 역할을 수행하는 연방 사이버 보안 센터로의 통합
④ 연방 사고대응 계획 및 프로세스 업데이트	해킹 사고 발생 시, 어느 기관에 어떻게 신고하고 지원을 요청할 것인지에 대한 지침을 제공하고, 연방정부는 효과적으로 정보를 공유하고 업무를 지원하며, 피해 발생 후 얻은 Insight를 활용할 수 있도록 프로세스 개선
⑤ 연방 방위 고도화	기존 네트워크 경계 안팎에서 위협에 대응해야 한다는 제로 트러스트 원칙에 따라 연방 기업을 방어하고 연방 시스템을 현대화하기 위한 장기적인 노력을 추진

2) 위협 행위자 교란 및 해체 (랜섬웨어 방어 국가적 총력 대응 체계)

모든 국가 권력의 수단을 사용하여 악의적인 사이버 행위자가 미국의 국가 안보 또는 공공 안전을 위협할 수 없도록 만듭니다. 모든 국력을 전략적으로 사용하고, 국제 파트너 또는 민간이 활동에 참여하여 포괄적인 접근 방식을 통해 랜섬웨어 위협에 대처합니다.

전략적 목표	설명
① 연방 파괴 활동을 통합	미국의 이익을 보호하는 동시에 민간, 법 집행 기관 및 정보 파트너와의 작전 통합 및 조정을 지속적으로 강화하여 대규모 악의적 활동을 방해
② 공공-민간 운영 협력 강화를 통한 공격자 교란	민간 부문 파트너 들과 가상 협업 플랫폼을 사용하여 양방향으로 정보를 공유하고 신속하게 협력하여 적을 교란할 수 있도록 연방 정부가 규제 완화등 정책적 지원
③ 인텔리전스 공유 및 피해자 알림의 속도와 규모 확대	연방정부는 사이버 위협 인텔리전스 공유의 속도와 규모를 늘려 조직이 적극적으로 표적이 되고 있거나 이미 침해당했을 가능성이 있다는 정보가 있을 때 사이버 방어자에게 사전에 경고하고 피해자에게 알릴 것
④ 미국 기반 인프라의 남용 방지	클라우드 및 기타 인터넷 인프라 제공업체와 협력하여 미국 기반 인프라의 악의적인 사용을 신속하게 식별하고, 남용에 대해 쉽게 신고할 수 있도록 하여 악의적인 행위자가 미국의 인프라 사용을 더 어렵게 만들 것
⑤ 사이버 랜섬웨어 퇴치	모든 국가적 역량을 동원하여 다음 네 가지 노력에 따라 위협에 대응 (1) 국제 협력을 활용하여 랜섬웨어 생태계를 교란하고 범죄자들에게 안전한 피난처를 제공하는 국가들을 고립 (2) 랜섬웨어 범죄를 조사하고 법 집행 기관 및 기타 당국을 사용하여 랜섬웨어 인프라와 행위자를 방해 (3) 랜섬웨어 공격을 견딜 수 있도록 중요 인프라 복원력을 강화 (4) 몸값을 세탁하기 위한 가상 화폐의 남용을 해결

3) 정보보호 및 회복력을 촉진하기 위한 시장의 힘을 형성(피해책임 법률 재구성)

민간 시장에 혁신과 경쟁을 유지하면서 디지털 생태계의 정보보호 및 복원력 강화를 장려하는 현대 디지털 경제 구축을 목표로 하여 데이터 관리자에게 개인 데이터 보호에 대한 책임을 강화하고, 보다 안전한 통신 기기 개발을 촉진하며, 사이버 보안 오류, 소프트웨어 취약성, 소프트웨어 및 디지털 기술로 인해 발생하는 기타 위험으로 인한 데이터 손실 및 피해에 대한 책임을 규율하는 법률을 재구성합니다. 美 연방정부의 구매력과 보조금을 활용하여 보안에 대한 인센티브를 제공하고, 사이버 보험시장을 활성화/안정화하여 더 나은 사이버 보안 환경을 제공할 수 있는 방안을 마련합니다.

전략적 목표	설명
① 데이터 관리자에게 책임 부여	개인 데이터의 수집, 사용, 전송 및 유지 기능에 강력하고 명확한 제한을 부과하고 지리적 위치 및 건강 정보와 같은 민감한 데이터에 대한 강력한 보호를 제공하기 위한 입법
② 보안 IOT 장치 개발을 추진	2020년 IoT 사이버보안 개선법에 명시된 대로 연방 연구 개발(R&D) 등 IoT 사이버보안을 지속적으로 개선
③ 안전하지 않은 소프트웨어 제품 및 서비스에 대한 책임을 전가	행정부는 의회 및 민간 부문과 협력하여 소프트웨어 제품 및 서비스에 대한 책임을 규정하는 법안을 개발할 것
④ 연방 보조금 및 기타 인센티브를 사용하여 보안을 강화	미국 연방 정부는 중요 인프라의 사이버 보안과 복원력을 강화하기 위해 보조금 프로그램을 통해 투자하고, SLTT 기관, 민간 부문 등 파트너와 협력하여 중요 제품과 서비스에 대한 보안과 복원력이 강화된 투자를 촉진하며, 사이버 보안 연구 및 개발을 지원
⑤ 연방 조달을 활용하여 책임을 개선	연방 정부의 공급업체에 대한 사이버 보안 계약 요건을 강화하고, 이를 위반한 경우 민사소송을 제기하는 민간 사이버 사기 이니셔티브(CCFI)를 활용하여 사이버 보안 제품 및 서비스를 안전하게 운영하도록 책임을 조정
⑥ 연방 사이버 보험 Backstop 탐색	사이버 사고가 발생하면 연방 정부는 경제 안정화와 복구를 지원해야 함으로, 행정부는 재난이 발생하기 전에 대응방안을 수립하고 연방 보험 대응 방안을 평가하며, 기존의 사이버 보험 시장을 지원

4) 회복력 있는 미래에 투자

차세대 통신과 IoT부터 분산형 에너지 자원에 이르기까지 차세대 디지털 인프라를 구축하고 인공지능과 양자 컴퓨팅이 가져올 기술 환경의 혁신적인 변화에 대비하면서 이러한 투자 격차를 해소해야 할 필요성이 증대되고 있고, 사이버 보안을 위해 중요하고 새로운 기술이 개발되고 배포될 때 이를 최적화하기 위한 집중적이고 조율된 조치를 통해 다른 국가를 능가하는 혁신을 위한 우리의 노력을 보완해야 합니다. 개인정보를 보호하고, 공평한 디지털 생태계를 구축하기 위하여 전략적 투자와 다양한 국가/조직과 수행방안을 조율하고 협력합니다.

전략적 목표	설명
① 인터넷의 기술적 기반 보호	연방 정부는 안전한 인터넷 환경을 위하여 여러 보안 조치를 구현하도록 하는 한편, 이해관계자들과 협력하여 솔루션개발, 도입촉진, 연구지원을 통해 보호 기술 선도

② 사이버 보안을 위한 연방 연구 개발 활성화	미래 10년간 미국의 지도력에 결정적인 역할을 할 세 가지 기술 분야, 컴퓨팅 관련 기술, 바이오 기술 그리고 청정 에너지 기술을 보호하는 데 초점을 맞추고, 투자 및 규제 완화로 신뢰성 있는 제품 및 서비스 시장 창출
③ 양자화 이후의 미래를 준비	취약한 공공 네트워크와 시스템을 양자 내성 암호화 기반 환경으로 전환하는 데 우선순위를 두고, 미래의 알려지지 않은 위험에 대비해 암호화 민첩성을 제공하기 위한 보완적인 완화 전략을 개발
④ 청정 에너지의 미래를 보장	미래의 청정 에너지 그리드 시스템을 보호하고 다른 중요 인프라 보호를 위한 보안 모범 사례를 창출
④ 디지털 ID 생태계 개발을 지원	보안, 접근성 및 상호 운용성, 금융 및 사회적 포용, 소비자 개인정보 보호, 경제 성장을 촉진하는 강력하고 검증 가능한 디지털 신원 솔루션에 대한 투자장려 및 활성화
④ 사이버 인력을 강화하기 위한 국가 전략 개발	국가 사이버 인력을 확대하고, 다양성을 개선하며, 사이버 교육 및 훈련 경로에 대한 접근성을 높이기 위한 포괄적이고 조율된 접근 방식을 통해 국가 사이버 인력 및 교육 전략의 개발을 주도하고 수행을 감독

5) 공동 목표 추구를 위한 국제 파트너십 구축

개방적이고 자유로우며 글로벌하고 상호 운용 가능하며 신뢰할 수 있고 안전한 인터넷을 유지하기 위해 노력하는 광범위한 국가연합을 구축하는 동시에 공통의 문제에 대해 우리의 큰 의제에 반대하는 국가들과도 계속 협력합니다. 이를 위해 평시와 위기 상황 모두에서 사이버 위협으로부터 스스로를 방어할 수 있는 파트너의 역량을 강화하고 동맹국 및 파트너와 협력하여 정보 통신 기술 및 운영 기술 제품 및 서비스를 위한 안전하고 신뢰할 수 있으며 신뢰할 수 있는 글로벌 정보보호 공급망을 구축합니다.

전략적 목표	설명
① 디지털 에코시스템에 대한 위협에 대응하기 위한 연합을 구축	파트너십을 통해 미국과 해외 국가들은 △사이버 위협 정보공유 △정보보호 모범사례 교환 △분야별 전문 지식 비교 △설계별 보안 원칙 추진 △정책 및 사고 대응 활동을 조율함으로써 공동의 사이버 보안 이익을 증진
② 국제 파트너 역량을 강화	전 세계 같은 생각을 가진 국가들의 역량을 강화하기 위해 미국은 기관, 공공/민간 부문, 선진 지역 파트너간 전문 지식을 모아 조율, 효과적 국제 사이버 역량 구축 및 운영 협력 노력
③ 미국 동맹국 및 파트너 지원 능력 확대	피해를 입은 동맹국 또는 파트너와의 긴밀한 협력은 적대적 활동에 맞서 연대를 보여주고 반규범적 국가 행동을 폭로하고 처벌을 부과해야 하며, 이를 위해 적절한 정책을 수립 및 보완하여 기존의 재정적 및 절차적 장벽을 신속하게 제거하기 위해 노력
④ 책임 있는 국가 행동의 글로벌 규범을 강화하기 위한 연합을 구축	UN의 모든 회원국은 국제법상 의무에 반하여 중요 인프라를 의도적으로 손상시키는 사이버 작전을 자제하는 것을 포함하여 사이버 공간에서 책임 있는 국가 행동의 평시 규범을 지지하기로 정치적 약속함에 따라 미국에서는 적극적으로 약속을 지키니 않는 국가에 책임을 물을 것
⑤ 정보, 통신, 운영 기술 제품 및 서비스를 위한 글로벌 공급망 보호	CHIPS 및 과학법, 인플레이션 감소법을 통해 새로운 산업 및 혁신 전략 도구를 도입하여 미국과 가까운 파트너의 중요 상품 생산을 회복하는 동시에 우리의 정보 기술과 첨단 제조 공급망을 보호

3. 시사점

바이든 행정부에서는 향후 10년간의 미국 정부의 사이버보안을 위한 전략을 수립하였습니다. 바이든 행정부에서는 일상생활의 디지털 기술의 사이버 보안이 중요성을 다시한번 부각시킴과 동시에 미국을 보호하고 사이버 위협에 대응할 수 있는 능력을 향상시키고자 하였습니다. 미국 국가 사이버보안 전략에서는 ▲첫째, 책임의 재 분배입니다. 개인 또는 작은 기업에게는 책임을 줄이고, 소프트웨어 개발사들에게 사이버 보안 제품 및 서비스를 안전하게 운영하도록 책임을 강화합니다. ▲둘째, 적극적인 사이버 위협 대응입니다. 악의적인 행위자가 미국의 국가 안보 또는 공공 안전을 위협할 수 없도록 국제적으로 금융제제 및 부당하게 취득한 자산을 환수하는 대응을 수행합니다. ▲셋째, 정보보호를 위해 국가의 재정을 투입합니다. 중요 인프라의 사이버 보안 및 복원력 강화를 목표로 하는 사이버 보안 연구, 개발 및 시연(RD&D) 프로그램에 자금을 지원합니다. ▲네번째로, 협력 강화입니다. 민,관의 전문기관과 신뢰할 수 있는 국가와의 협력을 강화하여 사이버 공격자들의 정보를 신속히 주고 받아 악의적인 행위를 신속히 차단하여 신뢰할 수 있으며 안전한 인터넷이라는 공유 비전을 공유 합니다.

미국이 글로벌 사이버보안 산업을 정부주도로 정책을 설정하고, 특히 금융사 등 국가주요기반시설 보호체계에 대한 강화는 현재 시행중인 한국의 국가기반시설보호법 및 동시행령과 사이버보안 전략적 지향점이 동일합니다. 이는 국내 금융보안정책의 전략수립에도 매우 깊게 참고할만한 사안입니다. 또한 KAIST 정보보호대학원 이주영 책임교수님 연구실에서 연구중인 양자컴퓨팅 기술은 기존의 국가암호체계와 정보보호 생태계를 새로운 시즌으로 돌입하게 해주는 신기술이기 때문에, 이에 대한 디지털금융산업에서의 선제적 대응도 필요합니다.

특히, 본 전략계획에서는 사이버해킹공격으로 발생하는 피해대응과 공격자 처벌에 대하여 미국 등 우방국들과의 범세계적 공동대응체계를 강조하고 있으며, 22년하반기에 국가정보원에서 개소한 '국가사이버안보협력센터'를 통해 국내적으로는 민관합동대응, 국제적으로는 글로벌 협력창구의 역할을 수행하고 있으며 정부에서는 '한미 합동 사이버 보안 권고문' 발표 등 사이버 보안을 위한 협력은 더욱 강화될 것으로 예상됩니다. 이러한 미정부의 사이버보안 및 정보보호 전략은 결국에는 디지털금융 및 주요기업과 정부기관의 정보보호 분야 투자 확대가 이루어질 때 가능한 투자수요를 창출할것이 예상되는바 비즈니스 기반의 국내 정보보호시장 확대가 기대됩니다.

화우 정보보호센터는 오랜 경험과 축적된 노하우를 기반으로 기업 고객을 위한 최적의 솔루션을 안내해 드리고 있습니다. 정보보호 관련 법령의 해석 및 그 대응과 정보보호 기술적 자문(해킹 진단, 보안취약점) 등 포괄적인 올인원(All-in-One) 서비스를 제공하고 있습니다. 관련하여 문의사항이 있으신 경우 언제든지 화우에 연락하여 주시기 바랍니다.

Contacts

이근우 파트너변호사 — T. (+82) 2 6003 7558, E. klee@yoonyang.com

석제범 고문 — T. (+82) 2 6182 8147, E.jbseok@yoonyang.com

이광욱 파트너변호사 — T. (+82) 2 6003 7535, E. kwlee@yoonyang.com

이수경 파트너변호사 — T. (+82) 2 6182 8132, E. sgyi@yoonyang.com

백재환 전문위원 — T. (+82) 2 6182 8366, E. jhb@yoonyang.com

지재원 연구위원 — T. (+82) 2 6003 7568, E. jwji@yoonyang.com