트럼프 2기 행정부의 미국 사이버보안 정책방향 전망

이경복 한국국방연구원 군사발전연구센터 AI·정보화연구실 선임연구원 | kblee@kida.re.kr
박태현 한국국방연구원 미래전략실 선임연구원 | tpark@kida.re.kr

그동안의 미국 사이버보안 정책 동향

미국의 국가 사이버보안 정책은 약 30년 전인 빌 클린턴 행정부('93~'01)로부터 시작되었다. 인터넷 초창기인 이 시기에 클린턴 행정부는 인터넷으로 대표되는 사이버공간을 국가안보와 관련된 핵심기반시설로 인식하고, 핵심기반시설보호(Critical infrastructure protection) 관점에서 사이버보안 정책을 마련하였다. 특히 민간과의 협력을 중요시한 결과 사이버보안을 위한 정보공유분석센터(ISAC)를 설립하는 등 국가와 민간 분야의 사이버보안 협력이 시작되었다. 다만, 이러한 클린턴 행정부의 정책은 사이버위협에 대한 인식을 정부 차원에서 공론화한 정도였으며, 국가 정책으로서 본격화된 것은 2000년대 부시 행정부('01~'09)부터이다.

부시 행정부는 2001년 9.11 테러 사건 이후 사이버위협을 테러 대응의 관점으로 접근하여 국가안보의 중요한 부분으로 인식하였고, 미국의 첫 번째 국가 사이버안보 전략인 『National Strategy to Secure Cyberspace』(2003)와 연방정부의 사이버보안 강화에 대한 종합적인 계획인 『Comprehensive National Cybersecurity Initiative』(2008)를 발표하는 등 국가안보적 관점의 사이버보안 정책을 마련하고 이행하였다. 또한, 부시 행정부 시기 미 합동참모본부는 사이버공간의 도메인(영역)에서 미군이 전략적 우위를 달성하는 것을 보장하기 위한 군사전략으로 『The National Military Strategy for Cyberspace Operations』(2006)를 발표하였고, 이를 기점으로 미국은 사이버공간에서의 군사작전을 강조하기 시작하였다.

2010년대의 오바마 행정부('09~'17)는 국가 차원의 전략을 수립하지는 않았지만, 백악관이 국가 사이버보안 정책을 총괄 조정하는 중앙집권적인 거버넌스 구조를 정립하고, 『Cybersecurity National Action Plan』(2016)을 통해 연방정부 차원에서 통합된 접근방법으로 사이버보안을 강화하는 정책을 시행하였다. 또한, 국제협력의 중요성을 강조한 『International Strategy for Cyberspace』(2011)와 같이 미국이 글로벌 사이버보안 규범을 주도하려는 시도도 오바마 행정부에서 시작되었다. 오바마 행정부 시기 국방부는 두 차례에 걸쳐 국방사이버전략[1]을 발표하였다. 이들 전략은 사이버공간을 군사작전 영역으로 인식하는 것을 넘어, 사이버공간의 전략적 중요성을 강조하고 사이버 능력을 군사작전에 통합하는 발전 방향을 제시하였으며, 이를 통해 보다 군사적 차원을 강조하는 사이버보안 정책을 펼쳤다.

이후 트럼프 행정부('17~'21)는 국가 사이버보안을 위한 실무적 역할을 담당하던 국토안보부(DHS)를 중심으로 국방부, 국가안보국(NSA) 등이 사이버보안 정책을 자율적으로 수립하고, 직접적으로 사이버 위협에 대응하는 분권적 구조로 국가 사이버안보 거버넌스를 재편하였다. 그리고 2003년 발표된 부시 행정부의 첫 번째 국가 사이버안보 전략 이후 15년 만에 연방정부 차원의 국가 사이버보안 전략인 『National Cyber Strategy』(2018)를 수립하고, 이를 통해 미국 우선주의 정책 기조에 따라 힘에 의한 미국 중심의 국제 질서를 강조하면서 공세적인 사이버보안 정책을 추진하였다. 국방 분야에서도 이러한 공세적인 정책 기조를 바탕으로 『2018 Department of Defense Cyber Strategy』(2018)를 통해 선제 방어(Defend Forward)로 대표되는 적극적이고 공격적인 정책 기조를 구체적으로 표명하였다.

바이든 행정부('21~'25)는 트럼프 행정부에서 재편한 국가 사이버보안 거버넌스를 백악관 주도로 복원하고, 국가안전보장회의(NSC)의 사이버보안 정책 조정기능을 강화하였다. 그리고 미국의 국가 사이버안보를 위해 사이버공간 방어에 대한 책임을 민간기업 등에도 부과하고, 장기 투자에 유리하도록 인센티브를 재정비하는 두 가지 근본적인 변화에 초점을 둔 『National Cybersecurity Strategy』(2023)를 발표하여 사이버공간의 회복탄력성 확보를 강조하고, 연방정부 차원의 제로 트러스트(Zero Trust) 추진,

1 『Department of Defense Strategy for Operating in Cyberspace』(2011), 『The Department of Defense Cyber Strategy』(2015)

기업 책임 부여, SW 공급망 보안, 동맹국과의 협력 강화 등을 바탕으로 하는 사이버보안 강화 정책을 추진하였다. 또한 국방부의 국방사이버전략인 『2023 Department of Defense Cyber Strategy』를 통해 사이버작전이 미국과 동맹 군사력의 필수 요소이며 미국이 추구하는 통합억제의 핵심 구성요소를 형성함을 강조하는 등 사이버공간에 대한 군사전략 방향과 실행방안이 발전되어 왔다.

상기와 같이, 미국의 사이버보안 정책은 국가 정책으로 논의가 시작된 부시 행정부부터 바이든 행정부에 이르기까지 일부 변화가 있었지만, 전체적인 정책 방향성은 일관되게 유지 및 발전되었다. 단순 핵심기반시설 보호에 중점을 둔 사이버보안 정책은 점차 국가안보의 핵심적인 정책으로 자리 잡았으며, 특히 사이버 영역의 안보화, 군사화, 국제화가 두드러지면서 공세적인 측면을 강조하는 국가 사이버보안 정책으로 발전되었다.

트럼프 2기 행정부의 정책 기조와 미국의 사이버보안 주요 이슈

트럼프 2기 행정부의 정책 기조: 바이든 행정부 정책 철회 및 트럼프 1기 정책 복원

트럼프 2기 행정부는 트럼프 대통령 취임 시작과 함께 바이든 행정부의 다수 정책을 철회하며, 대내외 안보 정책과 국방, 경제, 사회 정책 전반의 대변혁을 위한 다양한 정책을 급격하게 추진하고 있다. 특히, 1기 행정부 초기 오바마 행정부 정책을 철회했던 국정 운영 기조의 수준을 넘어, 바이든 행정부 정책을 더욱 강력하게 비판함과 동시에 미국 우선주의를 재강조하며 트럼프 1기 행정부의 정책을 복원하고 더 강화하는 수준으로 정책을 추진하고 있다. 트럼프 대통령은 제47대 대통령 취임 직후인 2025년 1월 20일 대통령 행정명령-14148 『Initial Rescissions of Harmful Executive Orders and Actions』에 서명하여 이전 행정부에서 마련된 다수의 행정명령을 철회하였다.

미국 내 사이버보안 주요 이슈

미국은 수많은 사이버공격이 발생하는 주요 국가 중 하나이다. 특히, 중국, 러시아, 이란, 북한은 사이버보안 관점에서 미국의 국가안보를 위협하는 국가로 언급할 만큼, 이들 국가로부터의 사이버공격이 연방정부, 핵심기반시설, 민간 영역을 대상으로 지속적으로 발생하고 있다. 특히, 2023년에 식별된 Volt Typhoon 해킹 공격 사례[2]는 중국 정부의 지원을 받은 것으로 추정되는 해커 그룹(Volt Typhoon)에 의해 수행되었음이 밝혀지면서, 현재 미국은 중국에 의한 사이버위협에 대해 강력한 대응 의지를 밝히고 있다.

2 미국의 통신, 교통, 수자원, 에너지, 국방 분야의 핵심기반시설을 대상으로 정보를 유출하고, 중국-대만 충돌과 같은 사건 발생 시, 미국 내 기반시설을 중단시키기 위해 장기간 은닉하는 형태(Living off the land)의 해킹 공격으로 분석되고 있다.

러시아와의 연계성을 가진 2020년 식별된 SolarWinds 공급망 공격 사례[3]와 2021년 발생한 Colonial Pipeline 랜섬웨어 공격 사례[4]도 미국에 대한 심각한 위협으로 분석되어, 바이든 행정부는 이 사건들을 계기로 미국의 사이버보안 강화를 위한 행정명령(Executive Order 14028)에 서명하였다.

선거에 대한 사이버위협 역시 미국에서 부상하는 주요한 사이버보안 이슈 중 하나이다. 트럼프가 제45대 대통령으로 당선되었던 2016년 대선 과정에서 러시아로 추정되는 사이버공격과 정보 작전이 발생함[5]에 따라, 선거에 대한 사이버위협은 미국 국가안보의 주요한 위협으로 현실화되었고, 이로 인해 오바마 행정부 말기인 2017년 1월 국토안보부는 미국의 국가 선거시스템을 핵심기반시설로 지정했다. 2020년 대선 과정에서도 중국 및 러시아에 의한 선거 개입과 허위정보 유포(영향력 행사) 등 사이버위협이 지속적으로 부상함에 따라, 사이버보안·인프라보안국(CISA)은 'Rumor Control'이라는 웹사이트를 신설하여 2020년 대선 관련 허위정보 대응체계를 구축하기도 했다.

미국이 우려하는 외국의 영향력 행사 등의 사이버위협은 중국 IT 플랫폼에서의 프라이버시 침해와 데이터보안 위협과 연관된다. 트럼프 1기 행정부는 미국 내 TikTok의 사용 증가에 따른 개인정보 유출 및

3 러시아 지원 해킹그룹으로 추정되는 공격자에 의한 SW 공급망(Supply Chain)에 대한 공격 사례이다. 공격자는 SolarWinds의 SW 개발 및 업데이트 프로세스와 서버에 침투한 후, 악성코드(SUNSPOT)를 이용하여 SW 업데이트에 정보 탈취를 위한 악성코드(SUNBURST)를 삽입 및 전파하고, 이를 통해 배포된 악성코드(SUNBURST)가 여러 기관에서 사용하는 SolarWinds의 네트워크관리시스템 Orion에 은닉되어 정보를 탈취하였다. Orion은 미국 내 약 3만 개 이상의 지방, 주, 연방기관에서 IT 자원 관리에 사용되어, 심각한 사이버위협으로 분석되었다.

4 러시아 내 위치한 사이버범죄 해킹그룹 DarkSide가 미국 동부 석유 공급량의 45%를 담당하는 석유 공급업체인 Colonial Pipeline을 대상으로 수행한 랜섬웨어 공격이다. 해당 랜섬웨어 공격은 Colonial Pipeline 내부 IT시스템을 암호화하였고, DarkSide는 암호화 해제로 75비트코인(당시 약 500만 달러)을 요구하였으며, Colonial Pipeline은 이를 지불하고 복구키와 프로그램을 받아 시스템을 복구하였다. 이 과정에서 Colonial Pipeline은 제어시스템으로 랜섬웨어 확산을 방지하기 위해 내부 네트워크를 선제적으로 임시 차단하였고 이에 따라 송유관이 중단되어 미 동부지역에 석유 부족 사태가 발생함에 따라 바이든 행정부는 국가비상사태를 선포하였다.

5 러시아 군사정보국(GRU)은 민주당 전국위원회(DNC)의 네트워크에 침투하여 수천 개의 문서를 탈취했으며, 이를 WikiLeaks를 통해 전략적으로 공개했다. 동시에 인터넷 연구소(IRA)는 가짜 온라인 페르소나를 생성하고 소셜 미디어를 통한 영향력 작전을 수행하여 수백만 명의 미국 유권자들에게 영향을 미쳤다.

국가안보 위협에 대응하여 TikTok을 서비스하는 모회사인 ByteDance의 미국 사업을 제한하는 행정명령을 발표한 바 있으며, 바이든 행정부도 유사하게 연방정부 및 기관 내 TikTok 사용을 전면 금지하는 법(No Tiktok on Government Devices Act)을 2022년 제정하였다. 나아가 이를 확대하여 미국 내 TikTok 사용을 제재하는 법(Protection Americans from Adversary Controlled Applications Act)을 2024년 제정하였다.

이와 함께, 최근 중국의 첨단 AI 모델로 각광받는 DeepSeek 앱에서 ByteDance의 데이터 수집 구성요소가 발견되고, 웹 로그인 페이지에서 미국 내 운영이 금지된 차이나모바일[6]과의 연결이 확인됨에 따라, 중국 IT 플랫폼의 광범위한 데이터 수집 관행과 중국 기반 직원들의 미국 사용자 데이터의 접근 가능성은 지속적인 국가안보 우려를 야기하고 있다.

마지막으로 트럼프 2기 행정부에서 신설된 대통령 자문기구 성격의 정보효율성부(Department of Government Efficiency, DOGE)로 인한 개인정보 노출 및 오용의 우려와 정부 기밀의 유출 및 남용, 연방정부의 보안 규제 및 준수 무력화 등이 사이버보안 이슈로 떠오르고 있다. 트럼프 대통령은 미 연방정부의 낭비, 사기, 남용을 근절하고 연방규제를 삭감하기 위한 목적으로 DOGE에 연방정부의 모든 데이터에 제한 없이 접근할 수 있는 최고기밀 등급의 보안인가를 임시로 부여하였다. 이로 인해 많은 연방 데이터가 AI 분석을 위해 DOGE 내 서버에 저장되고 있는데, 이와 관련하여 기존의 개인정보보호 및 보안인증 절차와 규제가 대부분 우회되고 있으며, 서버 자체도 인가 여부가 확인되지 않는 것으로 논란이 되었다. 또한, DOGE의 일부 인원이 정보 유출 전력이 있는 것으로 밝혀지면서 미국의 사이버보안에 대한 많은 우려와 논란이 제기되고 있다.

트럼프 2기 행정부의 미국 사이버보안 정책방향 전망

트럼프 1기 행정부 전후의 사이버보안 정책 기조 변화

트럼프 2기 행정부는 아직 사이버보안과 관련된 정책 기조를 명확히 표명하지 않았다. 그러나, 이전 트럼프 1기 행정부 초기에 오바마 행정부의 정책 지우기와 유사하게 현재 바이든 행정부의 정책 철회 움직임을 고려하면 유사한 상황이 발생할 것으로 전망된다. 따라서, 트럼프 1기 행정부에서 이전과 다르게 추진된 사이버보안 정책의 특징을 분석하고, 같은 맥락에서 바이든 행정부에서 변화된 부분도 함께 살펴보도록 한다.

6 차이나모바일은 2019년 미 연방통신위원회(FCC)가 '중대한' 국가안보 우려를 이유로 미국 내 운영 권한을 거부했고, 2021년에는 중국 군대와의 연관성이 확인되어 미국의 투자가 제한되었다.

표 1 - 미국 행정부별 사이버보안 정책의 특징 비교

	오바마 행정부('09~'17)	트럼프 행정부('17~'21)	바이든 행정부('21~'25)
거버넌스	백악관 중심 중앙집권적 구조	국토안보부 중심 분권적 구조	백악관 중심 중앙집권적 구조
정책 중점	방어 중심	선제 방어 / 공세적	선제 방어 / 공세적
국제협력	국제협력 강조	국방부 역할 강화	동맹국과 협력 강화
민간 규제	자율적 규제 (Cybersecurity Framework)	규제 최소화 / 기업 자율적 보안	규제 강화(Zero Trust) / 기업 법적 책임 강화
선거보안 관련	• 러시아 해킹 시도 대응 국토안보부 주도 사이버보안 지원 강화 • 선거시스템을 국가핵심기반시설로 지정 • 국토안보부와 주/지방 정부, 민간 협력	• 선거보안 규제에 대한 민간 자율성 강조 • 국토안보부/CISA 역할 강화 및 FBI와의 협력 • 법 제도적 규제 강화보다 정보공유 및 위협 탐지 강조	• 선거보안을 국가안보 우선순위로 지정 • 선거시스템 보안을 위한 법적 프레임워크 마련 및 강화
대중 정책방향	• 미·중 사이버협정('15)을 통한 사이버공격 자제 협상 • 중국 해커에 대한 경제적 제재	• 미·중 무역전쟁/기술 전쟁 이슈에 따른 중국기업(화웨이 등)에 대한 강력한 경제적 제재 • 사이버공격에 대한 경제적 제재 및 법적조치 • 군사적 대응 강조	• 중국을 주요 위협 국가로 설정 • 사이버공격에 대한 국제협력 등을 통한 강력한 외교적 대응 • 5G 등 기술 경쟁에 따른 경제적 제재

상기 [표 1]에서 비교한 바와 같이, 트럼프 1기 행정부와 전후 행정부와 비교했을 때, 사이버보안 정책의 변화된 요소는 거버넌스, 민간 규제, 그리고 선거보안에 대한 인식 차이이다. 민주당 기반의 오바마와 바이든 행정부는 백악관 중심의 강력한 중앙집권적 거버넌스 구조를 통해 국가 사이버보안 정책을 주도했다. 반면, 공화당 기반의 트럼프 행정부는 국토안보부가 실무적 역할을 담당하되, 국방부를 비롯한 각 부처가 각자의 역할을 자율적으로 수행하는 분권적 거버넌스 구조를 채택하였다. 그리고 이러한 거버넌스 변화에 따라 기존 정책을 철회하거나 새로운 부처가 신설되는 등의 변화가 진행되었다. 또한, 오바마 행정부가 민간을 대상으로 사이버보안의 자율적 규제를 위해 발표한 Cybersecurity Framework나, 바이든 행정부가 마련한 제로 트러스트 정책 및 기업의 법적 책임 강화에 대비해, 트럼프 행정부는 민간에는 상대적으로 규제를 완화하거나 자율성을 강조하는 방향으로 사이버보안 정책을 추진하였다. 국제협력 측면에서도 오바마와 바이든 행정부는 사이버보안을 위한 국제협력을 강조한 반면, 트럼프 행정부는 미국 우선주의에 입각하여 국제협력보다 국방부의 역할을 더욱 강화하는 방향으로 사이버보안 정책을 추진하였다.

대통령 행정명령 중심의 변화 요소

미국 대통령이 연방 기관에 내리는 명령인 대통령 행정명령(Executive Order)은 의회 승인 없이 백악관 내 법무검토 등 간소한 절차를 통해 입법과 같은 효력을 갖는다는 점에서 대통령 주도의 정책을 빠르게 펼치기 위한 주요한 수단이다. 사이버보안 분야 역시 다양한 대통령 행정명령을 통해 정책이 추진되어 왔기

때문에, 이전 정부인 바이든 행정부의 사이버보안 관련 주요 행정명령을 살펴보고, 이를 중심으로 기존 정책과 무엇이 다르고, 향후 어떻게 변화될지에 대해 간략히 살펴보도록 한다.

바이든 행정부는 연방정부의 사이버보안을 강화하는 두 가지 행정명령을 마련하였다. 첫 번째는 행정부 초기에 발표된 대통령 행정명령-14028로, 기존의 연방정부 사이버보안을 위해 규제를 보완하기 위해 NIST 사이버보안 프레임워크를 도입하는 등의 내용을 담고 있다. 두 번째는 이전의 행정명령(14028)을 더욱 강화한 대통령 행정명령-14144로, SW 공급망 보안, 클라우드 보안 기준, 연방 계약업체 보안요건을 강화하는 내용을 담고 있으며, 바이든 행정부 말기에 발표되었다. 한편으로 대중국 정책의 일환으로 발표한 TikTok 규제와 관련된 대통령 행정명령-14034도 바이든 행정부가 발표한 주요한 사이버보안 행정명령 중 하나이다. 이 행정명령은 트럼프 1기 행정부가 TikTok 등 중국 앱의 직접적인 사용 금지한 행정명령(13942, 13943, 13971)[7]을 폐지하고, 외국의 적대세력과 연관된 앱들의 위험성에 대해 엄격하고 증거 기반의 분석으로 접근할 것을 권고함으로써 중국 앱에 대한 위협 인식은 유지하되 보다 완화된 접근을 시도하고 있다. 또한, AI 안전성을 위한 대통령 행정명령-14110은 AI 시대의 새로운 보안 위협에 대응하기 위해 민간 AI 개발에 대한 안전을 규제하는 프레임워크를 마련했다는 점에서 사이버보안과 관련성이 있다.

표 2 - 바이든 행정부의 사이버보안 관련 대통령 행정명령의 주요 내용

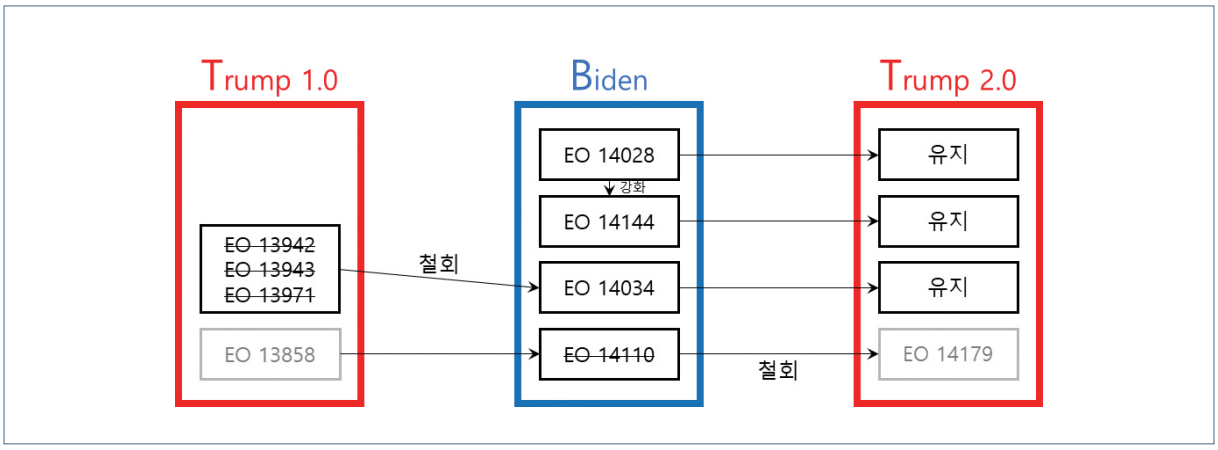
대통령 행정명령 #	발표 시기	주요 내용
14028 "Improving the Nation's Cybersecurity"	2021년 5월	• 연방정부 사이버보안 현대화 • NIST 사이버보안 프레임워크 도입 • 제로 트러스트 아키텍처 의무화
14144 "Strengthening the Nation's Cybersecurity through Software Supply Chain Security"	2025년 1월 17일	• SW 공급망 보안 강화 • 연방 계약업체 보안 요건 강화 • AI 기반 위협 탐지 시스템 의무화 • 클라우드 보안 기준 강화
14034 "Protecting Americans' Sensitive Data From Foreign Adversaries"	2021년 6월	• 외국 앱의 데이터 수집 및 사용에 대한 위험 평가 • 미국인의 데이터 보호를 위한 추가 조치 권고
14110 "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence"	2023년 10월	• AI 시스템 보안 평가 • 강력한 AI 모델 보고 의무화 • 합성 콘텐츠 탐지/인증 표준화

7 ① 대통령 행정명령-13942 "Addressing the Threat Posed by TikTok, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain"
② 대통령 행정명령-13943 "Addressing the Threat Posed by WeChat, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain"
③ 대통령 행정명령-13971 "Addressing the Threat Posed by Applications and Other Software Developed or Controlled by Chinese Companies"

트럼프 2기 행정부가 시작된 2025년 2월 초를 기준으로 대통령 행정명령-14148을 통해 철회된 대통령 행정명령 가운데 사이버보안과 관련된 직접적인 대통령 행정명령은 포함되어 있지 않지만, AI 안전 규제에 대한 대통령 행정명령-14110이 포함되어 있다. 트럼프 대통령은 1기 행정부 시기에 미국 우선주의를 바탕으로 AI 혁신을 방해하는 규제 장벽 제거를 강조하는 대통령 행정명령-13858 "Maintaining American Leadership in Artificial Intelligence"에 서명한 바 있다. 이러한 기조를 바탕으로 트럼프 대통령은 2025년 1월, AI 규제를 강조하는 바이든 행정부의 대통령 행정명령-14110을 철회하고, 미국의 AI 리더십을 가로막는 장벽 제거를 명시적 목표로 제시하는 대통령 행정명령-14179 "Removing Barriers to American Leadership in Artificial Intelligence"에 서명하였다.

대통령 행정명령-14110이 트럼프 본인의 대통령 행정명령-13858을 유지 및 발전시켰음에도 불구하고 해당 명령을 철회하고 새로운 행정명령에 서명한 점을 고려하면, 사이버보안에 대한 행정명령(14028, 14144, 14034) 역시 현재는 행정부 초기이기 때문에 유지되고 있을 뿐 향후 변화가 예상된다. 특히, 앞서 살펴본 바와 같이 사이버보안 규제에 대한 트럼프 1기 행정부의 정책 기조가 규제 완화와 자율적 규제였기 때문에, 바이든 행정부의 임기 종료 직전 서명된 대통령 행정명령-14144에 대한 트럼프 행정부의 정책 이행 여부는 미국 사이버보안에 대한 새로운 행정부의 입장을 가늠할 수 있는 중요한 지표가 될 것이다.

그림 1 - 바이든 행정부와 트럼프 행정부(1·2기)의 사이버 관련 대통령 행정명령들 간의 관계



앞으로의 전망

앞서 살펴본 바와 같이, 트럼프 2기 행정부는 1기 때와 유사하게 이전 민주당 행정부에서 마련된 미국의 국가 사이버 정책 방향을 다시 되돌릴 것으로 전망된다. 첫째, 거버넌스와 조직 관점의 변화이다. 트럼프 2기 행정부의 정책 방향을 제시한 것으로 평가받은 Heritage Foundation의 <Project 2025> 보고서는 이에 대한 변화를 이미 제시한 바 있다. 트럼프 2기 행정부는 중앙집권적 사이버보안 거버넌스를 다시

분권적 거버넌스로 되돌리면서, 바이든 행정부에서 신설된 백악관 산하의 국가사이버국장실(ONCD)을 폐지하거나, 직제를 국가안전보장회의(NCS) 산하로 변경할 가능성이 존재한다.

또한, 미국 국가 사이버보안의 실무적 역할을 담당하는 국토안보부 산하의 CISA의 해체 또는 임무 축소 등이 예상된다. 특히, 트럼프 1기 행정부 시기에 신설된 CISA의 임무가 선거보안 관련 허위정보 대응으로 확장된 것과 관련하여 트럼프 대통령은 1기 행정부 때 이를 언론 검열과 선거 영향을 위한 정치적 임무로 비판하며 축소할 것을 강조한 바 있고, 2020년 대선의 부정 선거를 주장할 당시 선거가 조작으로부터 안전함을 강조한 CISA 국장 크리스토퍼 크렙스(Christopher Krebs)를 해고한 전례가 있다. 따라서, CISA에 대한 변화는 필연적일 것으로 예상된다.

한편, 바이든 행정부에서 제정된 핵심기반시설 사고에 대한 보고 의무 등을 규정한 법(Critical Infrastructure Cyber Incident Reporting Act)에 따라 민간 보안기업과 핵심기반시설 운영자는 CISA에게 의무적으로 정보를 공유하고 사고를 보고해야 하는데, 이와 관련하여 트럼프 대통령이 추구하는 규제 완화 측면에서 CISA의 역할과 임무가 변할 가능성도 주목할 필요가 있다[8].

두 번째 변화는 규제 완화이다. 바이든 행정부는 사이버보안과 관련하여 민간 기업의 법적 책임을 국가 사이버안보 전략에서 강조할 만큼 사이버보안에 대한 민간 기업의 의무와 책임 등 규제에 대한 강화를 추진하였다. 하지만 트럼프 행정부는 규제 완화를 이미 추진한 바 있고 기업을 통한 혁신을 더 중요시하고 있어, 사이버보안의 규제 완화 정책이 추진될 것으로 전망된다.

세 번째는 미국 주도의 국제협력 축소이다. 트럼프 행정부는 미국 우선주의, 보호무역주의, 이익중심의 외교 등을 강조하고 있어, 사이버보안 강화를 위한 동맹과 국제협력을 축소하고 1기 행정부 때와 같이 미국의 사이버보안 강화를 위해 국방부 등의 부처 능력을 강조하는 다양한 사이버보안 정책을 더 공세적으로 펼칠 가능성이 크다. 트럼프 대통령의 국가안보보좌관으로 임명된 마이클 왈츠(Michael George Glen Waltz)는 임명 전부터 그동안 미국이 사이버보안에 있어 우선시한 방어가 효과적이지 않으며, 공격자들에게 더 많은 비용과 결과를 부과할 수 있도록 강력한 입장을 취해야 한다고 강조한 바 있다. 유사하게 CIA 국장으로 임명된 존 랫클리프(John Ratcliffe)도 미국이 공격자에게 보복할 수 있는 사이버 도구를 개발하도록 CIA를 이끌 것이라는 발언을 하는 등 공세적인 입장을 지속적으로 표명하고 있다.

그리고 이러한 공세적인 사이버보안 정책의 대상이 그동안 미국이 국가 사이버위협으로 지목해온 중국, 러시아, 이란, 북한에서 변화될 것인가에 대해서도 주목할 필요가 있다. 트럼프 대통령이 주도하는 러시아-우크라이나 종전협상으로 인해 러시아와 미국의 관계가 변화하면서, 트럼프 행정부는 러시아를 사이버위협 대상에서 잠정적으로 제외하는 것으로 보여지기 때문이다. 실제로 상기 마이클 왈츠 국가안보보좌관은

8 <Project 2025>에서는 사이버보안·인프라보안국(CISA)을 교통부 산하로 이동할 것을 제안하고 있다.

사이버 억제력을 강조하면서 중국과 이란만을 언급한 바 있고, 최근 국방부장관으로 임명된 피트 헤그세스(Pete Hegseth)가 러시아를 대상으로 하는 사이버공격 등 모든 사이버작전을 중단하라는 지시를 내렸다는 기사가 보도되는 등[9], 미국이 인식하는 공세적인 사이버보안 정책의 대상이 변화할 가능성도 상당히 높다.

다만, 상기 변화 전망과 별개로 미국의 사이버보안 정책의 큰 기조는 이전까지 추진했던 것처럼 국가안보의 핵심으로 공세적 강화를 유지될 것으로 판단된다. 그럼에도 불구하고 트럼프 2기 행정부 시기가 과거와 다르게 AI, 반도체와 같은 첨단기술 분야에서 미·중 간 기술 패권 경쟁이 더욱 치열하게 전개되는 시점이고, 더욱 복잡해진 국제 안보 위험이 기술 등 복합적으로 연계된 상황이기 때문에, 앞으로 미국의 사이버보안 정책이 세부적으로 어떻게 전개될지에 관한 지속적인 추적과 전망이 필요하다. 특히 그동안 미국의 사이버보안 정책이 글로벌 사이버보안 정책 흐름을 주도하였기 때문에 더욱 관심을 가져야 할 필요가 있다.

참고문헌

- 강태욱, 윤주호, 강정희(2025. 1. 20.), “트럼프 2기 행정부 AI 규제 방향”, 법률신문
- 이경복(2023. 8. 1.), “바이든 행정부의 국가 사이버안보 전략: 주요 내용과 시사점”, 한국국방연구원 국방 지능정보화 동향 제4호
- Anastasia Obis(2025. 2. 5.), “DOGE’s ‘unimpeded’ access to classified data poses national, econmic security risks”, Federal News Network
- Brandon Vigliarolo(2024. 12. 16.), “Trump administration wants to go on cyber offensive against China”, The Register
- Ellen Nakashima & Joseph Menn. (2025.3.3.) “As Trump warms to Putin, U.S. halts offensive cyber operations against Moscow”, The Washington Post.
- Heritage Foundation(2025), *Mandate for Leadership: The Conservative Promise*. <Project 2025> - Presidential Transition Project
- Jason Leopold, Margi Murphy, Sophie Alexander, Jake Bleiberg and Anthony Cormier(2025. 2. 8.), “Musk’s DOGE Teen was Fired By Cybersecurity Firm for Leaking Company Secrets”, Bloomberg
- Tim Starks(2025. 1. 15.), “CIA nominee tells Senate he, too, want to go on cyber offense”, CYBERSCOOP

9 다만, 미 국방부는 해당 보도의 내용에 대해 공식적으로 부인하였다.