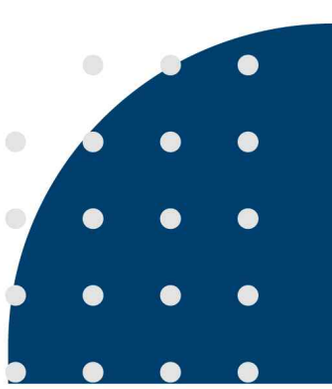
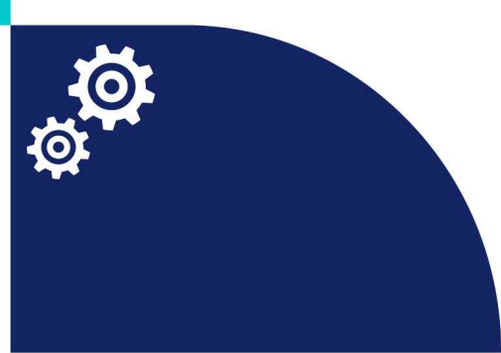
인터넷·정보보호 법제동향

Vol. 192 | September 2023





KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

Contents

국내 입법 동향

〈국회 제출 법률안〉

해외 입법 동향

〈중국〉

〈미국〉

〈해외 단신〉

국내 입법 동향 요약

■ 국회 제출 법률안

법안명	대표발의 (날짜)	주요내용
「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안	이인영의원 (2023. 9. 25.)	- 현행법상 한국인터넷진흥원의 설립 근거 및 업무 수행과 관련하여 최근 방송과 관련된 업무 및 관련 조직이 없다는 문제 제기 - 한국인터넷진흥원 설립 및 업무수행 관련 규정에 방송에 관한 사항을 제외하도록 규정
「방송통신발전 기본법」 일부개정법률안	변재일의원 (2023. 9. 26.)	- 일정 규모 이상의 부가통신사업자에 방송통신발전기금 조성 의무를 부과하여 기금 재원을 안정적으로 확보하는 규정 신설 - 방송통신발전기금 용도에 취약계층을 대상으로 부가통신역무의 요금감면을 지원하도록 하여 이용자를 보호하는 규정 신설
「전기통신사업법」 일부개정법률안	변재일의원 (2023. 9. 26.)	- 일정 기준의 부가통신사업자가 서비스 이용조건 등 기준을 갖춘 서비스 이용약관을 과기정통부장관에게 신고하도록 의무 부과 - 과기정통부장관이 신고된 이용약관에 대한 적정성 여부를 평가하고 필요시 개선사항을 권고할 수 있도록 하는 규정 신설
「지능정보화 기본법」 일부개정법률안	박덕흠의원 (2023. 9. 13.)	- 장애인·고령자 등 디지털 소외계층의 소외현상이 심화되어 정보격차 해소를 위한 교육의 표준이 마련되어야 한다는 문제 제기 - 국가기관·지자체 등의 지능정보서비스 제공 실태 관리·감독에 필요한 시책을 마련하고 정보격차 해소를 위한 교육과정을 개발·보급하여 디지털 소외계층의 접근성을 향상시키는 규정 신설
「국가연구데이터 관리 및 활용촉진에 관한 법률」 제정법률안	정필모의원 (2023. 9. 19.)	- 과기정통부장관이 국가연구데이터의 통합적 관리, 상호 연계 및 활용 촉진을 위한 국가연구데이터센터를 지정·운영할 수 있는 규정 마련 - 보안이 요구되는 국가연구데이터에 대해 보안대책을 수립하고 별도로 분류하여 필요한 보안관리 조치 규정 마련
「의료기기법」 일부개정법률안	강기윤의원 (2023. 9. 8.)	- 의료·건강지원 소프트웨어를 제조 또는 수입하여 판매하려는 자가 식품의약품안전처장에게 신고할 수 있도록 하는 권고 규정 신설 - 식품의약품안전처장이 의료·건강지원 소프트웨어의 안전성과 품질, 성능 확인을 위하여 소프트웨어를 수집하고 검사할 수 있으며, 우려가 인정되는 경우 판매 중지를 명할 수 있는 근거 마련
「저작권법」 일부개정법률안	이인영의원 (2023. 9. 25.)	- 빅데이터 및 인공지능 등 신기술의 발달로 데이터마이닝 과정을 통한 저작물 활용하는 과정에서 저작권 침해 관련 문제 제기 - 복제된 저작물에 대해 복제방지 및 보안 등 필요한 조치를 하여 데이터관련 사업자의 활동 영역 보장과 저작자의 권리 보호 규정 신설

국내 입법 동향

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안

(이인영의원 대표발의, 2023. 9. 25. 제안)

■ 소관 상임위원회 : 과학기술정보방송통신위원회

■ 제안이유 및 주요내용

○ 한국인터넷진흥원은 현행법을 근거로 설립된 법인으로, 정보통신망의 고도화와 안전한 이용 촉진 및 방송통신과 관련한 국제협력 · 국외진출 지원을 효율적으로 추진하기 위하여 정보통신망의 이용 및 보호, 방송통신과 관련한 국제협력 등을 위한 법 · 정책 및 제도의 조사 · 연구 등의 사업을 수행할 수 있음

○ 그런데 한국인터넷진흥원의 5개년 사업계획(2022~2027)에 방송과 관련된 업무가 없고, 현재 해당 법인 내에 방송 관련 업무를 수행하는 조직이 없다는 점에서 한국인터넷진흥원의 설립 및 업무수행에 관한 규정에서 방송에 관한 사항을 제외하여야 한다는 지적이 있음

○ 이에 한국인터넷진흥원의 설립 및 업무수행에 관한 규정에서 방송에 관한 사항을 제외함으로써 해당 법인의 성격을 명확히 하려는 것임(안 제52조)

• Reference

의안정보시스템 (http://likms.assembly.go.kr/bill/main.do)

국내 입법 동향

「방송통신발전 기본법」 일부개정법률안

(변재일의원 대표발의, 2023. 9. 26. 제안)

■ 소관 상임위원회 : 과학기술정보방송통신위원회

■ 제안이유 및 주요내용

○ 현행법에 따르면 과학기술정보통신부장관과 방송통신위원회는 방송통신의 진흥을 지원하기 위하여 방송통신발전기금을 설치, 조성, 운용하고 있음

○ 방송통신발전기금은 방송통신 관련 연구개발, 인력양성, 서비스 활성화 및 기반 조성, 콘텐츠 제작 · 유통 · 부가서비스 개발, 소외계층의 방송통신 접근 지원 등을 위한 용도로 사용되어, 방송통신과 유사한 서비스를 제공하고 있는 OTT 등 온라인플랫폼 사업자들도 기금의 혜택을 받고 있으며 그간 이를 통해 급격히 성장해왔음

○ 그러나 ICT 기술 발전과 서비스에 대한 이용자 행태변화 등으로 기존에 기금을 부담해온 방송사업자들의 수익성이 악화되어 기금 재원 마련의 부담이 커지고 있는 반면, 여전히 온라인플랫폼 사업자들은 기금 부담 없이 혜택만을 향유하고 있어 형평성 문제가 심각한 상황임

○ ICT 환경 변화를 고려하여 일정 규모 이상의 온라인플랫폼인 부가통신사업자에도 기금 조성 의무를 부과함으로써 사회적 기여 수준의 형평성을 제고하고 기금 재원을 안정적으로 확보할 수 있는 근거를 마련하고자 함(안 제25조제5항 신설)

○ 또한 방송통신발전기금의 용도에 장애인 · 저소득층 등 취약계층에 부가통신역무에 대한 요금감면을 지원하도록 하여 변화된 디지털 미디어 환경에서 방송통신 이용자를 더욱 두텁게 보호하고자 함(안 제26조제1항제16호 신설)

• Reference

의안정보시스템 (http://likms.assembly.go.kr/bill/main.do)

국내 입법 동향

「전기통신사업법」 일부개정법률안

(변재일의원 대표발의, 2023. 9. 26. 제안)

■ 소관 상임위원회 : 과학기술정보방송통신위원회

■ 제안이유 및 주요내용

○ 디지털 기술의 발전과 사회 환경 변화에 따라 온라인플랫폼은 소비자와 생산자를 연결하고 상호작용하며 국민 생활에 필수불가결한 역할을 수행하고 있음

○ 그러나 포털, 메신저, 온라인상거래 서비스 등을 제공하는 일부 온라인플랫폼의 영향력이 현저하게 증대되고 온라인플랫폼에 대한 의존도도 높아지면서 경제적 · 사회적 부작용도 함께 커지고 있는 상황임

○ 대형 온라인플랫폼 기업들은 과도한 이용자 정보 수집, 서비스 알고리즘의 불투명한 적용, 약탈적 가격설정, 온라인플랫폼 이용자에 대한 불공정 행위를 통해 영향력을 확대한 후, 이를 기반으로 온라인플랫폼을 이용하는 이용자와 사업자에 대해 일방적으로 요금 및 수수료를 인상하는 등 이용조건을 변경하거나 이용자 보호조치 없이 서비스를 해지 · 중지하는 등 국민 피해를 야기하고 있으나 현행법상 부가통신사업자인 온라인플랫폼의 일방적 요금 · 수수료 인상, 서비스 해지 · 중지, 민원처리 등에 대한 법적 규율은 미비해 이용자 피해가 확산되고 있는 실정임

○ 이에 일정 기준에 해당하는 부가통신사업자는 과학기술정보통신부장관에게 서비스 이용조건 및 대가, 이용조건 변경 시 사유 및 절차, 해지나 서비스 제한의 절차 및 요건, 이용자의 이의제기 및 피해구제의 기준을 갖추어 서비스의 이용약관을 신고하도록 의무를 부여하고자 함(안 제28조의2 신설)

○ 이와 함께 신고된 이용약관에 대해 과학기술정보통신부장관이 약관에 포함해야 할 사항의 적정성 여부 등을 평가하고, 개선이 필요한 경우에는 개선사항을 권고할 수 있도록 하여 이용자의 권익을 보호하고, 공정한 ICT 시장환경의 기반을 조성하려는 것임(안 제28조의3 신설 등)

• Reference

의안정보시스템 (http://likms.assembly.go.kr/bill/main.do)

국내 입법 동향

「지능정보화 기본법」 일부개정법률안

(박덕흠의원 대표발의, 2023. 9. 13. 제안)

■ 소관 상임위원회 : 과학기술정보방송통신위원회

■ 제안이유 및 주요내용

○ 현행법은 국가기관과 지방자치단체에 누구나 정보서비스에 원활하게 접근하고 활용할 수 있도록 정보격차 해소 시책을 마련하도록 하고, 정보격차의 해소를 위하여 필요한 교육(이하 “정보격차해소교육”이라 함)을 시행하도록 규정하고 있음

○ 그런데 장애인 · 고령자 등의 디지털 소외 현상이 심화됨에 따라 국가기관 등이 지능정보서비스 제공 실태에 대한 관리 · 감독을 강화하여야 하며, 정보격차해소교육의 교육과정, 교재 등의 표준이 마련되어야 한다는 지적이 제기됨

○ 이에 국가기관, 지방자치단체 및 공공기관에 지능정보서비스 제공 실태에 대한 관리 · 감독 등에 필요한 시책을 마련하도록 하고, 한국지능정보사회진흥원에 정보격차해소교육의 표준이 되는 교육과정과 교재 등의 사항을 개발 · 보급하도록 하여 장애인 · 고령자 등의 디지털 접근을 향상시키고 이용 편의를 보장하려는 것임(안 제12조 및 제45조)

• Reference

의안정보시스템 (http://likms.assembly.go.kr/bill/main.do)

국내 입법 동향

「국가연구데이터 관리 및 활용촉진에 관한 법률」 제정법률안

(정필모의원 대표발의, 2023. 9. 19. 제안)

■ 소관 상임위원회 : 과학기술정보방송통신위원회

■ 제안이유

○ 연구성과뿐만 아니라 연구 과정을 개방하는 오픈 사이언스 정책이 세계적인 추세임. 천문, 항공, 우주, 유전자 등 첨단 분야에서 실험 장비가 비약적으로 발전함에 따라 연구실험데이터가 급격하게 증가하고 있어 양질의 데이터를 체계적으로 축적하고 이를 공개·공유할 수 있는 데이터플랫폼의 구축 필요성도 강조되고 있음

○ 미국, 영국, EU 등 주요 선진국들은 공적자금을 투입한 연구과제의 경우 연구 과정에서 생성된 연구데이터를 공유하고 활용할 수 있도록 의무를 부과하고 있음

○ 연구데이터를 국가 중요자산으로 인식하기 시작한 우리나라도 2018년 국가연구데이터 공유·활용전략을 수립하고, 2019년 연구데이터관리계획(DMP) 시범 적용, 국가연구데이터플랫폼(DataON) 구축 등 연구데이터 정책을 추진해왔으나 국가연구데이터 관리에 대한 근거가 지침(공동관리규정)으로만 존재하고 있을 뿐 범정부 차원의 통합적인 관리가 어려운 상황임

○ 국가자산이자 과학기술의 원천인 연구데이터가 과학자들의 후속연구에 적극적으로 활용될 수 있도록 환경을 만들어줘야 할 필요가 있으므로 범정부 차원에서 연구데이터를 통합적으로 관리하고 개방형 연구데이터 생태계를 구축하기 위한 제정법 마련이 필요한 것임

○ 특히 우리나라의 경우 앞으로 심화 될 연구인력난을 대비한다는 측면에서 연구 비용과 시간을 절감하고 연구 생산성을 극대화할 수 있는 국가연구데이터 공유활용체계를 조속하게 구축할 필요가 있음

○ 이에 국가연구데이터센터, 전문연구데이터센터를 비롯한 각 연구개발기관에서 국가연구데이터를 효과적으로 관리할 수 있는 정책과 사업을 추진할 수 있도록 하고 정부가 이를 행정적·재정적으로 뒷받침하는 추진체계를 구축하고자 함

○ 더불어 국가연구데이터 공개원칙, 표준화, 품질관리, 보안관리, 활용촉진, 연구자 권리보호, 전문인력 양성 등 원활한 사업 추진에 필요한 규정들을 함께 마련함으로써 수많은 연구데이터들이 체계적으로 관리 · 보존되고 연구자와 연구기관 간 데이터 공유활용이 활성화되도록 이바지하려는 것임

■ 주요내용

○ 국가연구데이터는 연구개발기관이 연구개발과제를 수행한 연구자로부터 그에 대한 권리를 승계하여 소유하는 것을 원칙으로 하며, 연구개발기관은 연구자의 국가연구데이터 성과를 적절히 보호 · 관리하여야 하고, 연구자는 그 데이터를 통해 발생한 가치에 대하여 정당한 보상과 평가를 받을 권리를 갖도록 함(안 제5조)

○ 정부는 3년 단위의 국가연구데이터 관리 및 활용 촉진에 관한 기본계획을 수립하고, 과학기술정보통신부장관은 연차별 국가연구데이터 관리 · 활용 시행계획을 수립하도록 함(안 제6조 및 제7조)

○ 과학기술정보통신부장관이 관계 중앙행정기관이 관리하는 국가연구데이터의 통합적인 관리와 상호 연계 및 활용 촉진을 위하여 국가연구데이터센터를 지정 · 운영할 수 있도록 함(안 제9조)

○ 국가연구데이터센터는 국가연구데이터의 효율적인 등록 · 관리 · 제공 · 연계 및 공동활용 등을 지원하기 위한 국가연구데이터 통합플랫폼을 구축 · 운영하고, 전문연구데이터센터는 소관 분야의 국가연구데이터의 효율적 제공 · 연계 및 공동활용 등을 지원하기 위한 전문연구데이터 플랫폼을 구축 · 운영하도록 함(안 제11조)

○ 국가연구데이터는 국가연구데이터 통합플랫폼 또는 전문연구데이터 플랫폼에 등록하고 이를 일반에 공개해야 하며, 비공개 사유가 있는 경우에는 해당 비공개 기간 동안 국가연구데이터의 등록 및 공개를 유보할 수 있으며, 비공개 기간이 종료된 경우에는 즉시 국가연구데이터를 등록 및 공개하도록 함(안 제13조)

○ 국가연구데이터의 표준화를 추진하고, 그 추진 과정에서 필요한 지원을 할 수 있는 근거를 마련하고, 국가연구데이터의 품질관리를 위한 시책을 마련하도록 함(안 제14조 및 제15조)

○ 보안이 요구되는 국가연구데이터에 대해 보안대책을 수립하고, 별도로 분류하여 필요한 보안관리 조치를 하도록 함(안 제16조)

○ 국가연구데이터의 상호 제공 및 활용을 촉진하기 위해 필요한 시책을 수립하고, 국가연구데이터의 중요성, 권리 보호의 필요성 등에 대한 사회적 인식을 제고하기 위하여 필요한 사업을 실시하도록 함(안 제18조 및 제20조)

○ 국가연구데이터의 관리 및 활용에 필요한 인력수요에 효율적으로 대응하기 위하여 전문인력 양성에 관한 시책을 수립하고, 전문기관에 관련 교육훈련을 시행하도록 하고 그에 필요한 경비를 지원할 수 있도록 함(안 제21조)

• Reference

의안정보시스템 (http://likms.assembly.go.kr/bill/main.do)

국내 입법 동향

「의료기기법」 일부개정법률안

(강기윤의원 대표발의, 2023. 9. 8. 제안)

■ 소관 상임위원회 : 보건복지위원회

■ 제안이유

○ 미국의 경우 「21세기 치유법(21st Century Cures Act)」을 통하여 건강한 생활 방식의 유지·향상을 목적으로 하는 소프트웨어를 의료기기에서 명확하게 제외하고, 이와 의료기기와의 관계를 명확하게 하는 등 법적 체계를 마련한 바 있으나 우리나라의 경우 이에 대한 법적 체계가 부재한 상황임

○ 이에 의료기기에 해당하지 않으나 의료의 지원 또는 건강의 유지·향상을 목적으로 사용되는 소프트웨어를 의료기기와 명확하게 구분하고, 이에 대한 자율 신고제도 도입과 유통관리 등을 통하여 국민 건강 증진을 위한 올바른 정보를 제공하는 한편 소비자 보호 체계 등을 마련하려는 것임

■ 주요내용

○ 의료의 지원 또는 건강의 유지·향상을 목적으로 생체신호를 측정, 분석 등 하거나 생활 습관을 기반으로 건강관리 목적에 따라 식이·운동 등 정보를 제공하는 소프트웨어를 의료·건강지원 소프트웨어로 정의하고 의료기기와 명확하게 구분(안 제2조)

○ 의료·건강지원 소프트웨어를 제조 또는 수입하여 판매하려는 자는 식품의약품안전처장에게 자율적으로 신고할 수 있도록 하고, 식품의약품안전처장은 신고 제품을 유형별로 분류하여 관리목록에 등재하는 한편 인터넷 홈페이지 등을 통하여 공개 가능(안 제43조의7)

○ 식품의약품안전처장은 의료·건강지원 소프트웨어의 안전성과 품질, 성능을 확인하기 위하여 유통관리 계획을 수립하고 유통 중인 의료·건강지원 소프트웨어를 수집하여 검사할 수 있으며, 국민 건강에 중대한 위해를 끼치거나 끼칠 우려가 있다고 인정되는 경우 회수·교환·폐기 또는 판매중지를 명할 수 있는 근거 마련(안 제43조의8)

• Reference

의안정보시스템 (http://likms.assembly.go.kr/bill/main.do)

국내 입법 동향

「저작권법」 일부개정법률안

(이인영의원 대표발의, 2023. 9. 25. 제안)

■ 소관 상임위원회 : 문화체육관광위원회

■ 제안이유 및 주요내용

○ 현행법은 저작물의 통상적인 이용 방법과 충돌하지 아니하고 저작자의 정당한 이익을 부당하게 해치지 아니하는 경우에 저작물을 이용할 수 있도록 규정하고 있음

○ 그러나 최근 빅데이터 및 인공지능 등 신기술의 발달로 대량의 정보를 분석하여 유용한 정보를 추출하는 데이터마이닝 과정을 통하여 저작물을 활용하는 경우가 많아지고 있고, 그 분석과정에서 저작물을 허락 없이 이용하는 사례가 늘어나고 있는데, 이 경우 저작권 침해 여부에 대하여 현행법의 규정이 불분명하다는 지적이 있음

○ 또한, 영국, 독일, 일본 등에서 저작권 관련법의 개정을 통하여 정보분석을 위한 복제·전송을 명시적으로 허용하고, EU에서는 「디지털 단일시장 저작권 지침」을 제정하여 데이터마이닝에 관한 통일적 기준을 마련하는 등 데이터 관련 산업의 활성화와 저작물의 공정한 이용을 보장하고 있는 점을 고려할 필요성이 있음

○ 이에 대학·연구기관 등에서 교육·조사·연구 등 비상업적 목적으로 적법하게 접근한 저작물에 대하여 자동화된 정보분석을 하려는 경우 저작물의 복제·전송이 가능하도록 하고, 복제된 저작물에 대해서는 복제방지 및 보안 등 필요한 조치를 하도록 함으로써 데이터 관련 사업자의 활동 영역을 보장하고 저작자의 권리를 보호하려는 것임(안 제35조의5 신설 등)

• Reference

의안정보시스템 (http://likms.assembly.go.kr/bill/main.do)

해외 입법 동향

중국 국가정보보호표준화기술위원회, 중요데이터 처리 기준에 대한 새로운 규칙 초안 발표(2023. 8. 25.)

중국 국가정보보호표준화기술위원회는 정보보호기술 관련 데이터 처리자에게 중요데이터를 처리할 때 보안과 관련된 요구사항을 준수하도록 하는 새로운 규칙 초안을 발표(2023. 8. 25.)

■ 개요

○ 중국 국가정보보호표준화기술위원회는 8월 25일에 데이터 처리자가 중국의 데이터 및 사이버보안 규정의 중요한 개념인 중요데이터를 처리할 때 보안 요구사항을 충족하도록 하는 새로운 규칙 초안을 발표함

■ 주요 내용

① 중요데이터 정의 및 인프라 보안

○ **(정의)** 본 규칙은 중요데이터, 데이터 처리 등 주요 용어를 다음과 같이 정의함

구분	정의
중요데이터	· 특정 분야, 그룹, 지역 또는 정밀도와 규모의 데이터가 유출되거나 변조되면 국가 안보, 경제 운영, 사회 안정, 공중 보건 및 안전을 직접적으로 위태롭게 할 수 있는 데이터
데이터 처리	· 데이터를 수집, 저장, 사용, 처리, 전송, 제공, 공개 및 삭제하는 활동으로 정의하며, "데이터 처리 활동"으로도 부름
데이터 처리자	· 데이터 처리 활동에서 처리 목적과 처리 방식을 자율적으로 결정하는 조직 및 개인

○ **(인프라 보안)** 인프라 보안으로는 시스템 보안과 클라우드컴퓨팅서비스 플랫폼 보안이 있음

- **(시스템 보안)** 중요데이터를 처리하는 모든 정보시스템은 중국의 정보보호 기술 관련 국가표준인 'GB/T 22239-2019'[1]의 네트워크 보안의 등급 Ⅲ 기준[2]을 충족하여야 함

- **(클라우드컴퓨팅서비스 플랫폼 보안)** 클라우드컴퓨팅서비스 제공자는 플랫폼을 사용하여 중요데이터를 처리하기 전에 위험 평가를 수행하여 중요데이터를 분류하고 클라우드컴퓨팅서비스 제공자의 보안, 신뢰성을 중점으로 하는 평가를 정기적으로 실시해야 함

1) Information security technology - Baseline for classified protection of cybersecurity(정보보호 기술 - 사이버보안의 기밀 보호를 위한 기준)
2) Level 3 security requirements, ▲일반적인 보안 요구사항 ▲클라우드 컴퓨팅 보안 요구사항 ▲모바일 인터넷 보안 요구사항 ▲IoT보안 요구사항 ▲산업용 제어시스템 보안 요구사항

② 데이터의 전체 라이프사이클 관련 요구사항 및 조치

○ **(데이터 분류 관련 요구사항)** 동 규칙은 데이터 분류와 관련하여 데이터 처리자에게 데이터 출처, 분류시스템, 등급제도에 대한 요구사항을 다음과 같이 규정하고 있음

구분	데이터 분류 관련 요구사항
데이터 출처	· ▲데이터 형식, 품질 지침 및 평가 방법, 목적, 규모, 방식 등을 명시하는 **데이터 수집 절차를 개발** 해야 함 ▲수집하기 전 데이터의 목적, 보관 기간 등이 법률 및 규정을 준수하는지 **보안 평가를 수행**해야 함 ▲데이터의 진위 여부 및 정확성 검증과 데이터의 품질을 정기적으로 분석 및 모니터링하여 **비정상적인 데이터를 적시에 수정**해야 함
데이터 분류시스템	· ▲국가 및 규제기관의 데이터 분류에 관한 규정 요건을 준수하여 조직의 **데이터 분류시스템을 개발하고 정기적으로 업데이트**해야 함 ▲조직의 특정 상황과 데이터 특성 및 유형 등의 요소를 고려하여, 규정 요건에 위배되지 않는 데이터 분류시스템 규칙을 설정할 수 있음 **▲조직 자체의 데이터 분류시스템을 구현**해야 함
데이터 등급제도	· ▲국가 및 규제기관의 데이터 분류에 관한 규정의 요건을 준수하여 **데이터 등급 관리 시스템을 공식화하고 정기적으로 업데이트**해야 함 ▲조직의 특정 상황, 데이터의 중요성 및 피해 정도를 충분히 고려하여 데이터 등급 관리 시스템에 데이터 등급 지정규칙을 설정할 수 있으며, **등급 지정규칙은 보안 위험 변화에 따라 동적으로 조정하고 최적화되어야 함**

○ **(중요데이터 처리 관련 요구사항)** 동 규칙은 중요데이터 처리와 관련하여 데이터 처리자에게 중요데이터의 식별, 데이터 목록화 등에 대한 요구사항을 다음과 같이 규정하고 있음

구분	중요데이터 처리 관련 요구사항
중요데이터 식별	· ▲관할 산업 규제기관의 관련 규정 요건을 준수하여 **중요데이터 식별을 위한 시스템을 개발하고 정기적으로 업데이트**해야 함 ▲산업 특성 및 비즈니스 유형과 같은 요소를 기반으로 **중요데이터 특성을 파악**해야 함 ▲조직에서 처리하는 데이터를 등급별로 분류하고 **중요데이터를 식별하기 위해 데이터 등급제도 및 중요데이터 식별시스템을 구현**해야 함 ▲식별된 중요데이터는 출처, 목적, 저장 위치 및 기간 등을 목록화하여 기록해야 함
데이터 목록화	· ▲중요데이터 목록 관련 규정 요건을 준수하고 **중요데이터를 목록화하기 위한 기술적 조치를 취하여 목록을 작성하고 정기적으로 업데이트 및 유지**를 해야 함 ▲중요데이터 목록화에 기본 데이터 정보, 데이터 보안 책임자 등을 포함한 책임 당사자의 정보 데이터 처리 상황 등의 정보를 설명해야 함 **▲중요데이터 목록을 정기적으로 검토하고 업데이트하여 유효하고 합법적인지 확인**해야 함
접근 제어	· **▲접근 제어 정책 및 시스템을 구현하고 최소 권한 및 업무 분리 원칙을 준수하며 보안 조치를 구현**해야 함 ▲접근 관리 플랫폼을 구축하고 다단계 인증 등의 기술적 조치를 취하여야 함 **▲중요데이터에 대한 세분화된 접근 제어 메커니즘 제공 및 구현**해야 함 ▲사용자가 접근할 수 있는 데이터 범위를 제한하여 **데이터의 무단 유출 및 손상을 방지**해야 함 ▲중요데이터가 있는 시스템에서 **권한 있는 계정의 설정 및 사용을 엄격하게 제한**해야 함 ▲중요데이터의 사용 목적과 범위를 통제하고 데이터 유출 위험을 줄이기 위한 기술을 채택해야 함
평가 및 승인	· **데이터 사용 또는 처리 전 중요데이터에 대한 보안 평가 체계를 수립**하고 평가의 주요 사항, 평가 프로세스 및 승인 절차를 명시해야 하며 조직의 데이터 보안 책임자가 평가 결과를 승인하고 이에 대한 기록을 3년 이상 보관해야 함
데이터 삭제	· ▲삭제 관련 규범을 수립하여 **이에 따라 중요데이터 삭제 활동을 수행**해야 함 ▲중요데이터 삭제에 대한 평가 및 승인 프로세스를 수립하고 **중요데이터의 범위, 삭제 사유 등을 평가하여 데이터 보안 책임자의 승인을 받은 후 삭제**해야 함 ▲삭제된 데이터를 **상업적 수단으로 복구할 수 없도록 보장**해야 함 ▲데이터 삭제에 대한 효과를 평가하기 위한 메커니즘 수립과 **효과를 정기적으로 확인**해야 함 ▲데이터 삭제 프로세스에 대한 로그를 보관하여 **데이터 삭제의 승인 등 세부 사항을 기록**해야 함 ▲데이터 삭제 후 **중요데이터 목록을 업데이트**해야 함

③ 조직의 보안 의무

○ **(보안 책임자)** 데이터 처리자는 의사결정이 가능한 수준의 구성원 중 데이터 보안 책임자를 임명하여 보안 관리와 보호 계획을 수립하도록 하고 독립적인 직무 수행을 보장하여 데이터 보안 관리 상황을 네트워크 정보 부서 및 관할 당국에 직접 보고할 수 있도록 권리를 부여해야 함

○ **(보안 관리 조직)** 데이터 처리자는 데이터 보안 관리 조직을 설립하여 다음과 같은 업무를 수행하도록 함

구분	수행 업무
보안 관리 조직	· ▲중요데이터 보안에 관한 연구 ▲중요데이터 보안 관리 시스템, 운영 절차 및 데이터 보안 사고의 대응 계획 수립과 시행 ▲중요데이터 보안에 대한 모니터링, 위험 평가, 안전 교육 및 훈련 등의 수행 ▲관련 규정을 준수하여 네트워크 정보 부서 및 관할 당국에 데이터 보안 상황을 보고 ▲특정 유형의 중요데이터가 네트워크 및 정보 부서 또는 관할 기관에서 보유하는 경우 데이터 보안 관리 조직을 독립적으로 설립해야 함

○ **(보안 관리 시스템)** 데이터 처리자는 보안 관리 시스템이 중요데이터 처리의 목적, 범위, 방식 등의 요건을 준수하고 있는지 확인해야 하고 중요데이터의 보안을 위한 위험 평가 시스템을 수립하고 이에 대한 규칙을 명시해야 함

○ **(위험 평가)** 데이터 처리자는 중요데이터의 보안을 위한 위험 평가 시스템 수립과 관련하여 ▲중요데이터의 공유 및 법률의 새로운 요구 사항의 여부 등의 내용을 담은 위험 평가 보고서를 보관해야 함 ▲중요데이터 처리 활동에 대한 연례 평가 실시와 위험 평가 보고서를 네트워크 및 정보 부서 또는 관할 당국에 제출해야 함

■ 전망 및 시사점

○ 본 규칙은 10월 24일까지 의견 의견을 받을 예정이며 최종 확정 시 중요데이터와 관련된 집행을 위한 규제 지침 역할을 할 것으로 예상됨

○ 중요데이터는 네트워크 안전법 등에서 강화된 규정을 준수하도록 하고 있으나, 데이터 처리에 관한 세부 규정은 아직 명확하지 않아 본 규칙을 통해 명확한 기준을 제시하고자 함

- 데이터 처리, 보안 관리 등의 중요성이 강조되고 있는 전 세계적 추세 속에서 중국 내 중요데이터 처리에 대한 기준을 제시한다는 점에서 긍정적으로 평가됨

• Reference

https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20230825215527429474&norm_id=20221102143953&recode_id=52804
https://www.lexology.com/library/detail.aspx?g=cef3045e-a1f4-4534-b10f-af8d6acbde9d

해외 입법 동향

미국 하원,「계약업체 사이버보안 개선법(안)」발의(2023. 8. 29.)

미국 하원은 연방 계약업체의 정보 기술 계약자가 취약성 공개 정책 및 프로그램(VDPs[1])을 준수하도록 하는「계약업체 사이버보안 개선법(안)[2]」발의 (2023. 8. 29.)

■ 개요

○ 미국 하원은 8월 29일에 연방 계약업체의 정보 기술 계약자에게 요구되는 취약성 공개 정책 및 프로그램(VDPs)을 준수하도록 하는 내용의「계약업체 사이버보안 개선법(안)」을 발의함

○ 본 법안은 취약성 공개 정책 및 프로그램(VDPs)을 유지하여 연구자가 소프트웨어의 취약성을 공격자보다 먼저 식별하고 수정하여 공격자의 악용을 막는 것을 목표로 함

■ 주요내용

○ **(정의)** 동 법안은 집행기관, 연구자 등 용어에 대한 정의를 다음과 같이 명시함

구분	정의
집행기관	· ▲연방법 제5편 제101조에 명시된 행정부 ▲연방법 제5편 제102조에 명시된 군부 ▲연방법 제5편 제104조에 명시된 독립 기관 ▲연방법 제31편 제9101조에 명시된 공기업
연구자	· 보안 취약성 보고서를 제출하는 개인을 의미함
정보기술	· 연방법 제40편 제11101조에 명시된 정보기술로써 집행 기관과 관련하여 자동 획득, 저장, 분석, 평가, 조작, 관리, 이동, 제어, 표시, 전환, 교환, 전송 또는 수신에 사용되는 모든 장비 또는 상호 연결된 시스템 또는 장비의 하위 시스템을 의미하고 해당 장비가 집행 기관에 의해 직접 사용되거나 사용이 필요한 집행 기관과의 계약에 따라 계약자가 사용하는 경우, 집행 기관에 의한 데이터 또는 정보의 해당 장비 또는 서비스 수행 등을 의미함

○ **(취약점 공개 정책 및 프로그램 준수)** 동 법안은 취약점 공개 정책 및 프로그램(VDPs)에 해당하는 내용 및 범위를 명시하는 한편, 연방 계약업체의 정보 기술 계약자 및 CISA에 관련 의무를 부과함

1) Vulnerability Disclosure Policies and Programs
2) Improving Contractor Cybersecurity Act (H.R.5310)

구분	내용 및 범위
취약점 공개 정책 및 프로그램	· 해당 범위 내 있는 시스템에 대한 설명 ▲허용된 각 시스템에 대한 정보 기술 테스트 유형 ▲민감정보가 포함된 시스템에 대한 접근, 저장, 사용 등의 제한 여부[3] ▲개인이 취약성 보고서를 제출하는 방법에 대한 설명[4] ▲집행기관이 취약성 공개 정책에 대한 선의의 위반 시 계약자의 소송 금지 약속 ▲취약성 공개 정책에 따라 행동하는 개인이 제3자에 의해 고소를 당한 경우, 계약자가 정책을 준수하고 있었음을 법원에 알리겠다는 약속 ▲보고서를 제출하려는 개인에게 보고서의 수령 통지를 받게되는 기간과 계약자가 취할 조치에 대한 설명 ▲연구자의 활동에 대한 허용과 비허용을 규정하는 지침 마련

- **(정보 기술 계약자의 의무)** 정보 기술 계약자는 ▲정부 또는 업계의 다른 당사자에게 영향을 미칠 가능성이 있는 상용 소프트웨어 또는 서비스를 사용하는 시스템에 알려지지 않은 공개 취약점이 있는 경우 ▲계약자가 CISA[5]의 참여가 도움이 되거나 필요하다고 판단하는 경우에 취약성 보고서가 접수되어 정책이 게시된 날로부터 7일 이내에 CISA에 보고해야 함

- **(CISA의 취약점 제출)** CISA는 필요에 따라 MITRE사[6]의 공개적으로 알려진 컴퓨터 보안 결함 목록(CVE[7]) 또는 국가표준기술연구소(NIST[8])의 국가 취약성 데이터베이스에 취약점 사항을 전달 및 제출해야 함

■ 전망 및 시사점

○ 본 법안은 지난 2021년에 발의되었지만, 미 하원 감독위원회에서 통과되지 못하였고 2023년 8월 29일에 재도입되었으며, 동 법안을 통하여 연방 계약업체를 대상으로 공개 정책 및 프로그램(VDPs)을 준수하도록 하는 최초의 법적 기준을 마련하고자 함

- 본 법안과 유사한 내용의 연방 계약자들에게 취약점 공개 정책 및 프로그램(VDPs)의 이행을 준수하도록 하는 「연방 사이버보안 취약성 감소법(안)[9]」과 비슷한 시기에 발의되었으며, 양 법안 모두 통과될 경우 상호 보완을 통한 시너지 효과를 낼 것으로 기대됨

• Reference

https://www.congress.gov/bill/118th-congress/house-bill/5310
https://www.meritalk.com/articles/rep-lieu-calls-for-vdps-for-federal-it-contractors/

3) ▲민감한 정보를 저장, 전송 또는 기타 방식의 접근을 금지함 ▲민감한 정보는 취약성 식별에 필요 최소한의 범위내에서만 확인하고 보관을 금지함 ▲연구자가 탐색하거나 상호작용을 통해 얻은 시스템 또는 서비스 관련 정보의 사용을 취약성 보고와 직접 관련된 활동으로 제한함
4) ▲웹 양식이나 이메일 주소 등 보고서를 전송할 위치 ▲취약성 재현에 필요한 기술 정보 등 취약성을 발견하고 분석하는데 필요한 정보 유형(취약성에 대한 설명, 위치 및 잠재적 영향, 취약성 재현에 필요한 기술 정보 및 개념 증명 등)에 대한 설명 ▲익명의 취약성 보고서 제출물을 평가하는 방법 등의 명확한 진술
5) Cybersecurity and Infrastructure Security Agency
6) MITRE Corporation은 미국의 비영리 조직으로써 항공, 국방, 의료, 국토 안보 및 사이버보안 분야에서 다양한 미국 정부 기관을 지원하는 연방 자금 지원 연구개발 센터를 관리함
7) Common Vulnerabilities Exposures database, CVE프로그램은 CISA의 재정 지원을 받고 MITRE사에서 감독함
8) National Institute of Standards and Technology
9) [2023년 8월] 인터넷·정보보호 법제동향 191호 참고

해외 입법 동향

미국 하원, 「2023 국가 위험 관리법(안)」 발의(2023. 9. 13.)

미국 하원은 국토안보부 장관으로 하여금 국가위험관리 프로세스를 수립하도록 하는 「2023 국가 위험 관리법(안)[1]」을 발의함 (2023. 9. 13.)

■ 개요

○ 미국 하원은 「국토안보법[2]」을 개정하여 국토안보부 장관[3]으로 하여금 국가위험관리 프로세스를 수립하도록 하는 「2023 국가 위험 관리법(안)」을 발의

■ 주요내용

○ **(국가 위험 관리 프로세스)** 「국토안보법」 제22장[4] A절[5]을 개정하여 국가위험관리 프로세스 조항을 신설함(제2220F조 신설)

- **('국가 주요 기능' 정의)** 미국의 정부 및 민간 부문의 매우 중요한 기능으로써, 혼란, 부패 또는 기능 장애가 발생할 경우 국가 안보, 공중 보건·안전 등에 악영향을 미칠 수 있는 것을 의미함

- **(위험 식별 및 평가)** 국토안보부 장관은 사이버보안 위협과 물리적 위협, 위협 가능성 및 위협에 영향을 받기 쉬운 시스템 내의 취약성을 고려하여 주요 인프라에 대한 위험을 식별하고 평가하기 위한 반복적인 프로세스를 수립해야 함

  · 국토안보부 장관은 '위험 식별 및 평가'에 따라 요구되는 프로세스를 수립함에 있어서 ▲부문별 위험 관리 기관 ▲주요 인프라 소유자 및 운영자 ▲대통령 국가안보보좌관[6] ▲대통령 국토안보보좌관[7] ▲국가 사이버 국장[8]과 협의해야 함

1) National Risk Management Act of 2023 (H.R.5439)
2) Homeland Security Act of 2002
3) Secretary of Homeland Security
4) CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY
5) Cybersecurity and Infrastructure Security
6) Assistant to the President for National Security Affairs
7) Assistant to the President for Homeland Security

· **(프로세스 요소)** 국가 위험 관리 프로세스는 다음의 요소를 포함해야 함

(i) 위험관리기관(SRMA)[9]으로부터 제2218조에 따라 수집된 위협, 취약성 관련 정보 및 위험관리기관들의 특정 부문과 연관된 결과를 수집함
(ii) 주요 인프라 소유자 및 운영자가 관련 정보를 장관에게 제출하여 허용함
(iii) 장관이 다른 연방 부서 및 기관으로부터 어떻게 의견을 구할 것인지 개략적으로 설명함

· **(보고서 제출)** 국토안보부 장관은 위험 식별 및 평가 프로세스에 따라 확인된 사이버보안 위협 및 물리적 위협의 위험에 대한 보고서를 대통령, 의회의 관계위원회[10]에 제출해야 함

- **(국가 주요 인프라 복원력 전략[11])** 대통령은 국토안보부 장관이 보고서를 제출한 날로부터 1년 이내에 식별된 위험을 해결하기 위한 국가 주요 인프라 복원력 전략을 의회[12]에 송부하여야 함

전략 수립 시 고려요소
(i) 국가 안보, 경제 안보 또는 공중 보건 및 안전에 영향을 미치는 국가 주요 기능을 손상시키거나 방해할 수 있는 주요 인프라에 대한 위험영역을 우선적으로 고려해야 함
(ii) 해당되는 경우 이전의 국가 주요 인프라 복원력 전략의 시행을 평가해야 함
(iii) 식별된 위험 해결을 위해 취해야 할 리소스 요구사항을 포함하여 현재 및 제안된 국가차원의 조치, 프로그램 및 노력을 파악하고 개요를 설명해야 함
(iv) 각 국가 수준의 행동, 프로그램 또는 노력을 주도하는 책임이 있는 연방 부서 또는 기관과 각 부서에 관련된 주요 인프라 부문을 식별해야 함
(v) 전략 성공 실행에 있어 필요한 추가 기관을 요청해야 함

■ 전망 및 시사점

○ 본 법안은 초당적 성격의 법안으로써, 국토안보부 장관이 국가 위험 관리 사이클을 개발 및 수립하도록 요구함으로써 주요 인프라 부문의 대응 능력을 강화하기 위한 것임

- 본 법안을 대표발의한 공화당 하원의원은 국가 위험 관리 프로세스 도입은 기본적인 사이버-하이진(Hygiene) 조치로써, 궁극적으로 사회 기반시설의 복원력 강화를 통한 잠재적인 사이버 공격에 대한 대응능력을 강화하기 위한 방편이라고 설명함

• Reference

https://www.congress.gov/bill/118th-congress/house-bill/5439/text?s=2&r=116
https://www.meritalk.com/articles/house-cyber-bill-calls-for-a-national-risk-management-cycle/
https://gallagher.house.gov/media/press-releases/gallagher-spanberger-introduce-bipartisan-bill-strengthen-defenses-against

8) National Cyber Director
9) Sector Risk Management Agency, PPD-21에 따라 식별된 분야별 위험 관리 기관으로써 CISA홈페이지를 통해 확인할 수 있음
10) Committee on Homeland Security and Governmental Affairs of the Senate, Committee on Homeland Security of the House of Representative
11) NATIONAL CRITICAL INFRASTRUCTURE RESILIENCE STRATEGY
12) 상원의 다수당·소수당 원내대표(the majority and minority leaders of the Senate) 및 하원의장 및 소수당 원내대표(the Speaker and minority leader of the House of Representatives), 상원의 국토안보·정무업무위원회(the Committee on Homeland Security and Governmental Affairs of the Senate) 및 하원의 국토안보위원회(the Committee on Homeland Security of the House of Representatives)

해외 입법 동향

미국 하원, 외국의 스파이웨어 제재 조치 등 국가 안보 대응 강화를 위한 법안 발의

미국 하원은 스파이웨어 대응 강화를 위한 「외국의 상업용 스파이웨어로부터 미국인 보호법(안)[1]」(2023. 9. 13.) 및 「외국의 감시 스파이웨어 제재법(안)[2]」(2023. 9. 18.)을 발의함

■ 개요

○ **(「외국의 상업용 스파이웨어로부터 미국인 보호법(안)」)** 미국 하원은 「대외원조법[3]」을 개정하여 미국인을 대상으로 하는 외국의 상업용 스파이웨어 사용에 관여하는 해외 정부에 대한 원조 및 기타 목적을 금지하는 법안 발의(2023.9.13.)

○ **(「외국의 감시 스파이웨어 제재법(안)」)** 미국 하원은 외국의 상업용 스파이웨어 확산 또는 사용에 관여하는 특정인 등에 제재를 가하기 위한 법안 발의(2023.9.18.)

■ 외국 상업용 스파이웨어로부터 미국인 보호법(안)

○ **('외국의 상업용 스파이웨어' 정의)** 구매자가 인터넷에 연결된 전자 장치에 저장되거나 전자 장치를 통해 전송되는 정보에 대한 원격 액세스를 할 수 있도록 제공하는 외국 스파이웨어 회사가 개발 또는 소유한 다음과 같은 엔드투엔드(end-to-end) 시스템으로 판매, 임대 또는 기타 제공되는 툴을 의미함

〈 스파이웨어의 엔드투엔드(end-to-end) 시스템 기능 〉

- 악성 행위자가 무선 인터넷 및 셀룰러 데이터 연결을 통해 모바일, 인터넷 연결 기기에 악성코드를 감염시킬 수 있도록 하는 경우(기기 사용자의 별도 요건 불요)
- 전화 및 기타 오디오 녹음 등이 가능함
- 장치의 위치 추적이 가능함
- 문자 메시지, 파일, 전자 메일, 녹취록, 연락처, 사진 및 검색 기록을 포함한 장치의 정보에 접근 및 검색이 가능함

1) Protecting Americans from Foreign Commercial Spyware Act (H.R.5440)
2) Combatting Foreign Surveillance Spyware Sanctions Act (H.R.5522)
3) Foreign Assistance Act of 1961

○ **(미국인을 대상으로 한 외국의 상업용 스파이웨어 사용에 관여하는 해외 정부에 대한 지원 제재 조치)** 대통령이 신뢰할 수 있는 정보를 바탕으로 결정한 국가의 중앙 정부 및 다음사항을 고려하여 미국인을 대상으로 한 외국의 상업용 스파이웨어를 사용하는 행위에 관여하는 국가에 대하여는 본 법에 따른 원조 제공행위를 금지함(「대외원조법」 제620N조 신설)

〈 고려사항 〉

· 외국의 상업용 스파이웨어를 획득한 기록
· 자국민, 특히 언론인, 정치적 반대자 또는 활동가를 대상으로 외국의 상업용 스파이웨어를 사용한 경우
· 비민주적인 방식으로 외국의 상업용 스파이웨어의 사용 방지를 위한 지속적인 노력 수행에 실패한 경우
· 단, 군사적 지원행위는 예외적 사항에 해당함

- **(제재 조치 종료)** 다만, 국가의 중앙 정부에 대한 원조제공 금지 규정과 관련하여 대통령이 해당 정부가 더 이상 미국인을 표적으로 하는 외국의 상업용 스파이웨어 사용에 관여하지 않는다는 결정을 내린 1년 후에 종료함

- **(면책 사항)** 대통령이 보증하는 예외적 상황 또는 국가 안보상 우선사항에 해당한다고 의회 관계위원회에 서면으로 증명하는 경우, 미국은 해당 정부에 원조 제공을 할 수 있음

■ 외국의 감시 스파이웨어 제재법(안)

○ **(주요 용어)** 본 법에서의 '외국의 상업용 스파이웨어', '외국 기업', '스파이웨어', '대상 기업(COVERED ENTITY)'의 용어는 「국가보안법」 제1102A조[4]를 준용함

○ **(외국의 상업용 스파이웨어의 확산 또는 사용에 대한 제재)** 정책 수립, 제한조치, 처벌 등의 규정 마련

〈 정책 목표 〉

(1) 미국의 국가 안보 또는 외교 정책 이익에 반하는 행동을 하는 사용자에게 외국의 상업용 스파이웨어를 판매하는 회사의 서비스 제공 능력을 저하시킴으로써 방첩 위협에 단호하게 대처함
(2) 외국의 상업용 스파이웨어를 판매하는 기관을 이끌고 미국의 국가 안보 또는 외교 정책 이익에 반하는 활동에 관여하는 개인에 대해 단호하게 조치함
(3) ▲인지된 상대를 타겟으로 삼고 위협함 ▲반대 의견 제한 ▲표현, 평화로운 집회 또는 결사의 자유 제한 ▲기타 인권침해 또는 시민의 자유 억압 ▲미국인을 추적하거나 타겟으로 삼는 것과 같은 부적절한 목적의 외국의 상업용 스파이웨어 사용을 억제(deter)함

- **(임의적 제재)** 대통령은 위 정책 목표를 진전시키기 위해 다음의 대상에 대하여 임의적 제재조치를 취할 수 있음 (단, 새로운 제재를 부과할 수 있는 권한은 본 법 제정일로부터 7년이 지난날 종료한다는 일몰 규정임)

4) Section 1102A of the National Security Act of 1947 (50 U.S.C. 3231 et seq.).

〈 제재 대상 〉

(1) 미국의 주정부 관료 또는 정보기관 직원을 표적으로 삼을 수 있는 스파이웨어를 고의로 개발, 유지, 소유, 운영, 중개, 마케팅, 판매, 임대, 라이센스하거나 기타 방법으로 제공하는, 미국의 국가 안보에 위험을 초래한다고 대통령이 결정한 해당 주체

(2) (A) 위 제1항에 기술된 기업의 현재 또는 전 고위 임원인 경우 및 (B) 미국 정부 공무원 또는 정보 커뮤니티의 직원을 표적으로 할 수 있는 외국의 상업용 스파이웨어 판매에 고의로 관여한 경우의 모든 외국인

(3) (A) 외국 정부의 공무원이거나 해당 공무원을 대리하거나 대리하는 자 (B) 외국의 상업용 스파이웨어를 사용하여 미국 정부 관리 또는 정보 커뮤니티의 직원을 표적으로 하는 행위에 고의로 관여한 경우의 모든 외국인

· **(제재 조치)** 자산 동결, ▲비자, 입국 또는 가석방의 부적격 ▲현재 비자 취소 등 미국 입국 불가 및 비자 또는 기타 문서 취소 조치를 할 수 있음

제재조치	내용
자산 동결 (BLOCKING OF PROPERTY)	· 대통령은 국제긴급경제권한법[5]에 따라 대통령에게 부여된 모든 권한을 행사할 수 있으며, 해당 자산 및 자산에 대한 이해관계가 미국에 있거나, 미국 내에 있거나, 미국인의 소유 또는 통제권 내에 있는 경우에는 대통령에 의해 임의적 제재의 대상이 된다고 결정된 개인의 자산과 자산에 대한 모든 거래를 필요한 범위 내에서 차단하고 금지할 수 있음 – 단, 본 법(50 U.S.C. 1701)의 제202조의 요건이 적용되는 경우는 제외함
미국 입국 불가 및 비자 또는 기타 문서 취소	· **(비자, 입국 또는 가석방의 부적격)** (i) 미국에 허용되지 않는 (ii) 미국 입국을 위한 비자 또는 기타 서류를 받을 수 없는 경우 (iii) 미국에 입국 또는 가석방되거나 이민 및 국적법[6](8 U.S.C. 1101 et seq.)에 따라 다른 혜택을 받을 수 없는 경우의 외국인 · **(현재 비자 취소)** 대통령이 임의적 제재조치 적용 대상으로 결정한 외국인이 개인인 경우, 해당 비자 또는 기타 입국 서류가 언제 또는 발급되었는지에 관계없이 해당 개인의 비자 또는 기타 입국 서류는 취소되어야 함. 즉시 취소효력이 발생하며, 해당 개인이 소유하고 있는 기타 유효한 비자 또는 입국 서류를 자동으로 취소해야 함 · **(예외)** 1947년 11월 21일 발효된 유엔 본부에 관한 협정[7] 또는 기타 해당되는 국제 의무를 준수하기 위해 미국에 입국을 인정하거나 가석방할 필요가 있는 경우는 제외함

– **(이행 조치)** 대통령은 국제긴급경제권한법(50 U.S.C. 1702 및 1704) 제203조 및 제205조에 따라 제공된 모든 권한을 행사할 수 있으며, 본 조항을 수행하는 데 필요한 규정, 라이센스 및 명령을 발행해야 함

· **(처벌 규정)** 국제긴급경제권법(50 U.S.C. 1705) 제206조의 (b)항 및 (c)항에 따라 규정된 이행 위반, 위반 시도, 위반 공모 또는 위반을 유발하는 자는 해당 조문(a)항에 기술된 불법 행위를 저지른 자와 동일한 범위 내에서 동법 제206조의 (b)항 및 (c)항에 규정된 처벌규정 준용

5) International Emergency Economic Powers Act
6) Immigration and Nationality Act
7) 1947년 6월 26일 Lake Success에서 체결된 유엔 본부에 관한 협정

· **(처벌 예외 규정)** ▲국가보안법 제5장[8]에 따라 '보고 조치'를 준수하는 모든 활동 ▲ 미국의 모든 공인된 정보 또는 법 집행 활동에 따른 정보 및 법 집행 활동

■ 전망 및 시사점

○ 스파이웨어 제재 성격의 본 법안들은 국가 안보에 위험을 초래하는 외국의 상업용 스파이웨어에 대한 확산을 방지하고 예방하기 위한 적극적 제재조치의 성격을 담고 있음

- 올해 3월 바이든 행정부는 '국가 안보에 위험을 초래하는 상업용 스파이웨어에 대한 미국 정부의 사용금지에 관한 행정명령[9]'을 발표하였는 바, 본 법안이 통과될 경우 상업용 스파이웨어 제재 조치에 대한 상호보완적 효과가 기대됨

• Reference

https://www.congress.gov/bill/118th-congress/house-bill/5440/text?s=2&r=115
https://www.congress.gov/bill/118th-congress/house-bill/5522/text?s=1&r=33
https://www.whitehouse.gov/briefing-room/presidential-actions/2023/03/27/executive-order-on-prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to-national-security/

8) TitleV of the National Security Act of 1947 (50 U.S.C. 3091 et seq.)
9) Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security(2023.3.27.)

해외 입법 동향

미국 상원, 「중소기업 사이버 복원력법(안)」 발의(2023. 9. 7.)

미국 상원은 사이버위협으로부터 중소기업이 효과적으로 예방 및 대응할 수 있도록 지원하는 「중소기업 사이버복원력법(안)[1]」 발의함 (2023. 9. 7.)

■ 개요

○ 미국 상원은 중소기업청[2]에 중앙 중소기업사이버보안부를 설치하여 연방정부의 중소기업 대상 사이버보안 관련 사항을 총괄하도록 하는 등 중소기업 사이버보안 위협 문제를 해결하고 중소기업의 역량 강화를 위한 「중소기업 사이버 복원력법(안)」 발의

■ 주요내용

○ **(주요 용어)** 본 법안에서의 사이버보안 위험, 사이버 위협 지표, 방어 조치, 사고 관련 등 주요 용어는 「국토안보법 2002[4]」 제2200조의 정의 규정을 준용함

주요 용어	내용
사이버보안 위험 (Cybersecurity risk)	· 정보 또는 정보시스템에 대한 위협 및 취약점, 그러한 정보 또는 정보시스템의 무단 접근, 사용, 공개, 중단, 수정 또는 파괴로 인해 발생하거나 그로 인해 발생하는 모든 관련 결과를 의미(테러 행위로 인해 발생하는 관련 결과도 포함) - 단, 소비자 서비스 약관 또는 소비자 라이센스 계약 위반 사항만을 포함하는 조치는 제외
사이버 위협 지표 (Cyber threat indicator)	· "사이버위협지표"란 다음 각 호의 사항을 기술하거나 식별하기 위하여 필요한 정보를 의미 - 사이버보안 위협 또는 보안 취약성과 관련된 기술 정보 수집을 목적으로 전송되는 것으로써 변칙적인 통신 패턴을 포함한 악의적인 정찰 행위 - 보안통제를 무력화하거나 보안 취약점을 악용하는 방법 - 정보시스템에 정당하게 접근한 이용자 또는 무의식적으로 정보시스템에 저장·처리·전송된 정보에 대한 보안통제를 무력화하거나 보안 취약점을 악용하도록 하는 방법 - 악의적인 사이버 명령 및 통제 - 특정 사이버보안 위협의 결과로 유출된 정보에 대한 설명을 포함하여 사고로 인해 야기된 실제 또는 잠재적 피해 - 사이버보안 위협의 다른 속성, 해당 속성의 공개가 법에 의해 금지되지 않은 경우 등

1) Small Business Cyber Resiliency Act(s.2740)
2) Small Business Administration

주요 용어	내용
방어적 조치 (Defensive measure)	· 정보시스템 또는 정보시스템에 적용되는 행위, 장치, 절차, 서명, 기법, 그 밖의 조치로써 사이버보안의 위협 또는 보안상 취약성이 알려져 있거나 의심되는 것을 탐지, 예방 또는 완화하는 정보시스템에 저장, 처리 또는 전송하는 것을 의미 - (예외) 다음의 정보시스템 또는 정보시스템에 저장되어 있는 정보를 파괴, 사용할 수 없게 하거나, 무단으로 접근하게 하거나, 상당한 해를 끼치는 조치는 제외함 (i) 본 장(제6장 국내의 안보[3])의 제1501조에 정의된 바와 같이 해당 조치를 운영하는 민간 주체 (ii) 동의를 제공할 권한이 있고 해당 민간단체에 해당 조치 운영에 대한 동의를 제공한 다른 단체 또는 연방 단체
사고 (Incident)	· 정보시스템에 관한 정보의 무결성, 비밀 유지 또는 가용성을 법적 권한 없이 사실상 또는 즉시 위태롭게 하는 사고를 의미

○ **(기관 간 협정)** 중소기업청[5]은 CISA와 관계부처 간 협정을 통해 중소기업의 사이버보안 리소스 및 대응력을 향상하기 위해 행정기관과 협력하고 정보공유를 확대해야 함

○ **(리소스 파트너[6]를 통한 지원)** 국토안보부 및 기타 연방정부 기관은 리소스 파트너를 통해 사이버보안 툴(사이버보안 평가 툴, 사이버 복원력 리뷰)을 사용하여 중소기업 문제를 지원하는 한편, ▲사이버보안 인프라를 개발·강화하는 과정에서의 중소기업의 우려사항, ▲사이버 위협 지표에 대한 인식 개선, ▲사이버보안 사고 대응 계획, ▲직원 역량 강화를 위한 사이버 교육 프로그램 지원을 위하여 사이버보안 위험 및 기타 국토안보 문제와 관련된 정보를 배포함

- **(연간 간행물)** 본 법 제정일로부터 1년 이내(이후 매년) 관리자는 리소스 파트너가 지원한 중소기업 문제사항의 갯수를 중소기업청 홈페이지에 게시해야 함

○ **(중앙 중소기업 사이버보안 지원부서[7] 설립)** 중소기업청장은 상무부 장관[8], 국토안보부 장관 및 법무장관[9]과 협의하여 행정관 내에 중앙 중소기업 사이버보안 지원부서를 설립해야 함

- 중앙 중소기업 사이버보안 지원부서는 국토안보부가 개발한 것과 같은 연방 정부 전반의 중소기업 관심사에 대한 사이버 보안 자원의 중앙 정보센터 역할을 할 것임

〈 중앙 중소기업 사이버보안 지원부서 역할 〉

구분	직무 내용
중소기업 사이버보안 업무 총괄	· 자원, 행정낭비 등 중복업무를 줄이기 위해 중소기업청 내 내부적 사이버보안 업무 조정

3) 6 U.S.C. - DOMESTIC SECURITY
4) Homeland Security Act of 2002(6 U.S.C. 650)
5) Small Business Administration
6) 중소기업 개발 센터; 제29조에 기재된 여성 비즈니스 센터 ; 제8조(a)(1)(A)에 기술된 퇴직 간부 서비스 부대의 장.
7) Central Small Business Cybersecurity Assistance Unit
8) Secretary of Commerce
9) Attorney General

구분	직무 내용
정보센터 웹사이트 구축	· ▲사이버 하이진(hygiene) 모범 사례 관련 안내 자료를 찾는 방법 ▲사이버보안 위반 또는 사고 보고 장소 ▲사이버보안 위반 또는 사고 대응 방법 ▲ 중소기업청의 사이버보안 이행 노력 ▲주요 사이버 범죄에 대한 표준 사고 대응 절차 등의 정보를 포함하여 중소기업 문제에 관하여 공개적으로 이용할 수 있는 사이버보안 정보의 정보센터(clearinghouse)인 웹사이트 구축 및 관리
사이버보안 지원 업무	· 자격조건을 갖춘 직원들과 협력하여 중소기업 문제에 대한 사이버보안 지원 업무 제공
관계 기관과의 협력 등	· 중소기업청장은 접근 가능하고 조치할 수 있는 형태의 사이버보안 정보와 리소스를 중소기업에 식별하고 배포하는 것이 적절하다고 결정하는 경우 국토안보부 및 기타 연방 정부기관과 협력해야 함 · 사이버 위협 지표 및 방어적 조치를 보고하는 등의 중소기업 사이버보안 문의사항을 관계 연방기관에 리다이렉트(redirect)함 · 국립표준기술연구소(NIST)와 협력하여 중소기업 사이버보안 태세(posture) 개선에 적용할 수 있는 NIST의 사이버보안 프레임워크 요소를 구현하는 가장 비용 효율적인 방법에 대한 정보를 식별하고 중소기업에 전파함 · 국방부(DoD[10])와 협력하여 국방)의 사이버보안 성숙도 모델 인증 또는 국방부가 정한 기타 후속 사이버보안 요구사항을 충족하기 위한 정보를 식별하고 중소기업에 전파함
기타	· 중소기업 문제의 사이버보안 태세 개선과 상충되는 연방정부의 모든 부서, 기관 등에서 채택한 정책 또는 절차를 식별하기 위해 행정부 옹호실[11]의 의견을 구함

- **(중소기업을 위한 강화된 사이버보안 보호)** 다른 법률 규정에도 불구하고, 중소기업 문제에 대해 「2015년 사이버 보안 정보 공유법[12]」에 따라 승인된 모든 활동 또는 이에 따라 공유되거나 수신된 사이버위협 지표, 방어조치 등과 관련된 경우 해당 소송은 즉시 기각되어야 함

○ **(의회 보고)** 본 법이 시행된 날부터 1년 이내(이후 매년) 관련 정보를 수집하거나 공유하는 각 연방기관의 장과 중소기업청장은 ▲개인/기업 식별 정보, ▲민감한 금융 정보 및 ▲해당 연방 기관이 수신한 사이버보안 정보를 수집하거나 공유하는 경우, 관련 조치에 대한 공동 보고서를 상원의 중소기업 위원회[13]와 하원의 중소기업 위원회[14]에 제출해야 함

○ **(중소기업의 사이버 위험에 대한 연구 및 보고)** 본 법의 제정일로부터 1년 이내에 행정부 옹호실 수석 고문[16]과 미국 감사원장은 다음과 같은 사항을 수행해야 함

〈 주요 수행 내용 〉
· 중소기업 사이버보안 문제와 관련, 코로나19에 따른 사업장 폐쇄로 인해 온라인 시장으로 전환하는 영향 평가에 대한 공동 연구 수행 · 의회의 해당 위원회[15]에 제출하고 다음에 관한 보고서를 공개적으로 공개해야 함 – 확인된 사이버보안 위험이 2020년 2월 1일부터 2021년 12월 31일까지 온라인상 존재하는 중소기업 문제사항(▲업데이트된 정보시스템 확보 ▲사이버보안 프로토콜 구현 ▲데이터 침해 또는 사이버 공격 대응)에 구체적으로 미치는 영향

10) Department of Defense
11) Office of Advocacy of the Administration, 의회법에 따라 설립된 독립 연방정부기관인 미국 중소기업청 옹호실은 의회, 백악관, 연방기관, 연방 법원 및 주 정책 입안자들에게 중소기업의 견해를 대변함
12) Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.)
13) Committee on Small Business and Entrepreneurship of the Senate
14) House Committee on Small Business
15) 상원 중소기업위원회(Committee on Small Business and Entrepreneurship of the Senate), 상원 국토안보및정무위원회(Committee on Homeland Security and Governmental Affairs of the Senate), 하원 소기업회(Committee on Small Business of the House of

■ 전망 및 시사점

○ 본 법안은 중소기업의 사이버보안 관리 강화를 위하여 중소기업청에 관련 역할 및 권한을 명시적으로 부여함으로써 중앙 집중적 관리 시스템을 구축하는 것으로 평가됨

- 이를 통해 중소기업이 직면한 사이버보안 위협 사항에 대해 직접적인 피드백을 제공하고 지원함으로써 보다 효과적이고 효율적으로 문제를 해결할 수 있을 것으로 사료됨

• Reference

https://www.congress.gov/bill/118th-congress/senate-bill/2740/text?s=9&r=2&q=%7B%22search%22%3A%5B%22cyber%22%5D%7D
https://www.risch.senate.gov/public/index.cfm/pressreleases?ID=A39F60D7-657C-4B05-B707-D8FA31A05128

Representatives) 및 하원 국토안보위원회(Committee on Homeland Security of the House of Representatives)
16) Chief Counsel for Advocacy of the Administration

해외 단신

EU집행위, 디지털시장법(DMA)에 따라 6개의 게이트키퍼 지정(2023. 9. 6.)

○ 2023년 9월 6일, EU집행위원회는 디지털시장법[1](DMA)에 따라 6개의 회사(Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft)를 게이트키퍼로 지정함

〈게이트키퍼 지정 기준〉

(1) EU 내 일정 연간 매출액을 달성하고 EU 회원국 3개 이상에서 핵심 플랫폼 서비스를 제공하는 경우
(2) EU에 설립되거나 위치한 4,500만 명 이상의 월간 활성 최종 사용자와 EU에 설립된 연간 10,000명 이상의 활성 비즈니스 사용자에게 핵심 플랫폼 서비스를 제공하는 경우 (회사가 최근 3년 동안 해당 기준을 충족한 경우 포함)

○ EU집행위원회는 6개의 게이트키퍼 회사에 대해 핵심 플랫폼 서비스를 지정하였으며 이에 따라 게이트키퍼로 지정된 회사는 다음의 이행사항 및 금지사항을 준수해야 함

- 게이트키퍼는 ▲온라인 중개 서비스 ▲온라인 검색 엔진 ▲소셜 네트워킹 서비스 ▲특정 메시징 서비스 ▲동영상 공유 플랫폼 서비스 ▲가상 비서 ▲웹 브라우저 ▲클라우드 컴퓨팅 서비스 ▲운영체제 ▲온라인 광고 서비스에 해당하는 10가지 핵심 플랫폼 서비스 중 하나 이상을 제공하는 것으로, 이 중 Tiktok, Google Play, Amazon, Safari, Whatsapp, LinkedIn 등 22개를 지정함

구분	주요내용
이행사항	▲특정 상황에서 제3자가 게이트키퍼 자체 서비스와 상호 운용할 수 있도록 허용해야 함 ▲게이트키퍼 플랫폼 사용을 통해 생성된 데이터에 비즈니스 사용자의 접근을 허용해야 함 ▲광고주 및 게시자가 독자적으로 게이트키퍼 주최의 광고 검증을 수행할 때 필요한 툴(tools)과 정보를 플랫폼에 광고하는 회사에 제공하도록 함
금지사항	▲게이트키퍼 플랫폼에서 제3자가 제공하는 유사한 서비스 또는 제품보다 게이트키퍼 자체 제공 서비스 및 제품에 대해 유리하도록 순위를 매기는 행위 금지, ▲유효한 동의 없이 타겟 광고를 목적으로 게이트키퍼의 핵심 플랫폼 서비스 외에서 최종 사용자(end users)를 추적하는 행위 금지, ▲사용자가 원하는 경우 사전 설치된 소프트웨어 또는 앱을 제거하지 못하도록 함

- 게이트키퍼는 DMA 규정사항을 어떻게 준수할 것인지 세부적으로 설명하는 보고서를 6개월 이내에 EU집행위원회에 제출해야 하며, EU집행위원회는 이행여부를 모니터링할 예정

▲ **(준수의무 불이행시)** EU집행위원회는 해당 회사의 전 세계 연간 총 매출액 최대 10%까지 벌금을 부과할 수 있으며, 반복적으로 위반하는 경우 최대 20%까지 부과할 수 있음

※ [2021년 12월] 인터넷·정보보호 법제동향 제171호 참고

• Reference

https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328

1) European Parliament, 2020/0374(COD)- Digital Markets Act, 2021.11.23.

인터넷·정보보호 법제동향
Vol. 192 (September 2023)

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

ㅣ 발 행 처 ㅣ 한국인터넷진흥원
(58324) 전라남도 나주시 진흥길 9 한국인터넷진흥원
Tel. 1433-25
ㅣ 기획 · 편집 ㅣ 법제연구팀
ㅣ 발간 · 배포 ㅣ www.kisa.or.kr