결과보고서 | 2024년

인터넷·정보보호 법제동향

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

CONTENTS

미국

EU

CONTENTS

유럽 각국

일본

중국

캐나다

호주

싱가포르

기타

서 문

■ 개요

디지털 기술의 급속한 발전과 함께 사이버 공간에서의 위협도 나날이 진화하고 있다. 사이버범죄의 지능화와 대규모화, 국가 인프라를 겨냥한 사이버 공격의 증가, 신기술로 인한 새로운 형태의 위험 등으로 인해 기존 법제도의 한계점이 드러나고 있다. 이에 각국은 사이버보안 관련 법제를 전면적으로 정비하고 있으며, 특히 2024년에는 이러한 움직임이 더욱 가속화되는 양상을 보인다.

주목할 만한 것은 최근의 입법 동향이 단순한 기술적 대응을 넘어 포괄적이고 체계적인 접근을 시도하고 있다는 점이다. ▲사이버범죄 대응, ▲주요 인프라 보호, ▲제품 보안 강화, ▲AI 거버넌스 구축 등 다양한 영역에서 새로운 법적 프레임워크가 등장하고 있으며, 이는 디지털 시대에 걸맞은 새로운 법제 패러다임의 형성을 예고한다.

본 보고서는 **2024년 주요국의 사이버보안 관련 입법 동향을 네 가지 핵심 영역**으로 나누어 분석하고, 이를 통해 향후 법제 발전의 방향성을 전망하고자 한다.

Ⅰ. 사이버범죄 대응 입법: 디지털 불법행위의 법적 대응 강화

최근 사이버범죄 대응을 위한 각국의 입법 동향을 살펴보면, 법제도가 보다 포괄적이고 선제적인 방향으로 진화하고 있음을 확인할 수 있다. 특히 주목할 만한 것은 개별 국가 차원의 대응을 넘어 UN「사이버범죄 방지 협약」과 같은 초국가적 공조체계가 제도화되고 있다는 점이다. 이는 사이버범죄의 초국경적 특성을 고려할 때 필연적인 변화로 보인다.

또한, 최근의 입법 동향은 사후 처벌 중심에서 예방과 역량강화로 무게중심이 이동하고 있음을 보여준다. 특히, UN「사이버범죄 방지 협약」에서는 개발도상국의 사이버보안 대응역량 강화를 강조한다. 이는 글로벌 사이버 안보가 가장 취약한 연결고리부터 강화되어야 한다는 인식을 반영한다.

한편, 독일 연방의회의 딥페이크 활용 범죄 처벌을 위한「형법」개정안 발의에서 볼 수 있듯이, 각국은 신기술 발전으로 인한 새로운 위협들에 대해 선제적으로 대응하려 노력하고 있다. 기존 법체계로는 규율하기 어려운 새로운 유형의 범죄들이 등장함에 따라, 법제도 역시 이에 발맞춰 진화하고 있다. 이 과정에서 단순히 기술적 보안을 넘어 개인의 프라이버시, 인격권, 디지털 권리 등을 포괄적으로 보호하려는 관점이 강화되고 있다는 점도 주목할 만하다.

이러한 입법 동향은 디지털 시대의 법제가 국제 협력을 기반으로 하되, 보다 예방적이고 포괄적인 방향으로 발전해 나가고 있음을 시사한다. 앞으로도 기술 발전 속도와 그로 인한 위협의 다변화를 고려할 때, 이러한 경향은 더욱 강화될 것으로 전망된다.

II. 주요 인프라 보호 및 강화 입법: 국가 운영체계의 사이버 대응력 강화

주요 인프라의 사이버보안에 관한 최근 각국의 입법 동향을 살펴보면, 국가 안보의 핵심 요소로서 더욱 체계적이고 포괄적인 보호체계가 구축되고 있음을 알 수 있다. 특히 주목할 만한 점은 단순한 기술적 방어를 넘어 국가 차원의 전략적 대응으로 법제도가 진화하고 있다는 것이다.

2024년 각국의 입법 동향은 크게 세 가지 방향성을 보인다. 첫째, 분야별 맞춤형 규제체계가 도입되고 있다. 미국의 「의료 사이버보안 법안」, 미국 연방항공청의 「항공기 장비 등의 사이버보안에 관한 잠정규정 예고문」, 독일 연방금융감독청의 「디지털 운영 복원력법에 관한 이행지침」 등은 각 분야의 특수성을 고려한 세분화된 접근을 보여준다. 이는 획일적 규제에서 벗어나 분야별 위험 특성과 운영 환경을 반영한 실효성 있는 보호체계를 구축하려는 노력으로 해석된다.

둘째, 사이버보안 관리체계가 더욱 정교화되고 있다. 미국 CISA의 「주요 기반시설 사이버사고 보고법(CIRCIA) 잠정규정 예고문」이나 싱가포르의 「사이버보안 개정 법안」 개정안에서 볼 수 있듯이, 사고 보고체계의 의무화, 보안 표준 수립, 정기적 취약점 평가 등이 제도화되고 있다. 특히 캐나다의 「사이버보안에 관한 법률」이나 EU의 「NIS2 지침」은 주요 기반시설에 대한 체계적인 보호 프레임워크를 제시하고 있다.

셋째, 국가 간 데이 터 안전 관리가 강화되고 있다. 미국 법무부의 「자국민 민감 개인정보 등에 대한 우려국가의 액세스 방지를 위한 잠정규정예고문(NPRM)」이나 중국의 「네트워크 데이터안전 관리조례」는 자국 데이터의 보호와 통제를 강화하는 추세를 보여준다. 이는 디지털 시대에서 데이터 주권이 국가 안보의 핵심 요소로 부상하고 있음을 시사한다.

이러한 입법 동향은 결과적으로 국가 기반시설의 사이버 복원력을 종합적으로 강화하는 방향으로 수렴되고 있다. 특히 주목할 만한 것은 대부분의 국가들이 사전 예방과 신속한 대응, 그리고 장기적인 관점에서의 회복력 강화라는 다층적 접근을 취하고 있다는 점이다. 앞으로도 기술 발전과 위협의 진화에 따라 이러한 법제 발전은 더욱 가속화될 것으로 전망된다.

III. 제품 사이버보안 강화 입법: 디지털 제품의 보안 표준화

최근 디지털 제품의 사이버보안 관련 입법 동향을 살펴보면, 제품 설계 단계부터 보안을 의무화하는 포괄적인 규제 체계가 확립되고 있음을 알 수 있다. 특히 주목할 만한 점은 제품 보안이 더 이상 제조업체의 자율적 영역이 아닌 법적 강제사항으로 진화하고 있다는 것이다.

최근의 입법 동향은 크게 세 가지 방향성을 보인다. 첫째, 제품 책임 범위가 디지털 영역으로 확대되고 있다. EU의 새로운 「제조물 책임지침」은 AI 시스템과 소프트웨어를 제조물의 범위에 포함시키고, 책임 주체도 제조업체에서 유통업자까지 확장했다. 이는 디지털 제품의 결함에 대한 책임을 명확히 하고, 소비자 보호를 강화하는 새로운 규제 패러다임을 보여준다.

둘째, IoT 제품에 대한 보안 표준화가 강화되고 있다. EU의 「사이버복원력법」은 연결된 디지털 제품의 설계·개발·생산 단계에서 보안성 확보를 의무화하고, CE 인증을 통한 검증 체계를 도입했다. 이는 IoT 제품의 보안을 제품 수명주기 전반에 걸쳐 관리하려는 체계적 접근을 보여준다.

셋째, 디지털 인프라의 보안 강화가 추진되고 있다. 미국 FCC의 「인터넷 라우팅 보안 강화 위한 NPRM」이나 일본의 「스마트폰 소프트웨어 경쟁 촉진법」은 디지털 인프라의 안전성과 공정성을 동시에 확보하려는 시도를 보여준다. 특히 시장 지배적 사업자에 대한 규제를 통해 보안과 경쟁이라는 두 가지 목표를 동시에 달성하려는 접근이 주목된다.

이러한 입법 동향은 결과적으로 디지털 제품의 보안을 소비자 권리 보호와 연계시키는 방향으로 발전하고 있다. 앞으로도 기술 발전과 함께 새로운 형태의 디지털 제품이 등장할 것으로 예상되는 만큼, 이러한 법제 발전은 더욱 가속화될 것으로 전망된다.

IV. 인공지능 거버넌스 입법: 책임있는 AI 발전을 위한 법적 프레임워크

인공지능 거버넌스에 관한 최근 각국의 입법 동향을 살펴보면, AI 기술의 안전하고 책임 있는 발전을 위한 포괄적인 법적 프레임워크가 구축되고 있음을 알 수 있다. 특히 주목할 만한 점은 AI 규제가 단순한 기술적 관리를 넘어 윤리적 가치와 사회적 영향을 포괄하는 방향으로 발전하고 있다는 것이다.

최근의 입법 동향은 크게 네 가지 방향성을 보인다. 첫째, AI 안전성 확보를 위한 제도적 기반이 강화되고 있다. 미국의 AI 보안 위험관리를 강화하기 위한 「안전한 AI 법안」이나 뉴욕주 금융서비스국의 「AI에 따른 사이버보안 위험 대응 등을 위한 지침」은 AI 시스템의 보안과 안전성을 확보하기 위한 구체적인 메커니즘을 제시한다. 특히 취약점 관리, 보안사고 보고체계 구축 등 실질적인 안전 관리 방안을 규정하고 있다.

둘째, 공공부문의 AI 활용에 대한 규제 체계가 확립되고 있다. 미국 백악관의 「연방정부의 안전하고 책임성 있는 AI 사용에 관한 신규 각서」나 예산관리국의 「정부의 책임있는 AI 조달 추진을 위한 각서」는 정부 차원의 AI 활용에 대한 명확한 기준을 제시하고 있다. 특히 AI 책임자 지정, 거버넌스 체계 구축 등을 통해 체계적인 관리를 도모하고 있다.

셋째, AI의 사회적 영향에 대한 관리가 강화되고 있다. FCC의 「정치광고에서의 AI 생성 콘텐츠 공개 및 투명성에 관한 NPRM」이나 「원치 않는 로보콜 및 로보텍스트로부터 소비자를 보호하는 AI 기술의 영향에 관한 NPRM」은 AI 기술이 민주주의와 소비자 권리에 미치는 영향을 고려한 선제적 대응을 보여준다. EU의 「AI와 인권, 민주주의, 법치에 관한 협약」 역시 AI 발전이 기본적 인권과 민주주의 가치에 부합하도록 하는 국제적 합의를 이끌어냈다는 점에서 의미가 있다.

이러한 입법 동향은 결과적으로 AI 기술의 혁신과 안전성을 균형 있게 발전시키는 방향으로 수렴되고 있다. 특히 주목할 만한 것은 대부분의 법제가 투명성, 설명가능성, 공정성, 프라이버시 보호 등 다차원적 가치를 고려하고 있다는 점이다.

■ 결어

지금까지 살펴본 각국의 사이버보안 관련 입법 동향은 몇 가지 주목할 만한 공통점을 보여준다. 첫째, 법제도가 더욱 포괄적이고 체계적으로 발전하고 있다는 점이다. 단편적인 대응에서 벗어나 예방-대응-복구를 아우르는 종합적인 접근이 이루어지고 있으며, 이는 사이버보안을 국가 안보의 핵심 요소로 인식하는 관점의 변화를 반영한다.

둘째, 국제 협력의 제도화가 강화되고 있다. UN의 「사이버범죄 방지 협약」이나 EU의 「AI와 인권, 민주주의, 법치에 관한 협약」과 같이, 초국가적 차원의 공조체계가 법적 구속력을 갖춘 형태로 발전하고 있다. 이는 사이버 위협의 초국경적 특성을 고려할 때 필연적인 변화로 평가된다.

셋째, 기술 발전에 대한 선제적 대응이 이루어지고 있다. AI나 IoT와 같은 신기술이 가져올 수 있는 잠재적 위험을 사전에 식별하고 관리하려는 노력이 법제도에 반영되고 있으며, 이는 앞으로도 더욱 강화될 것으로 예상된다.

이러한 변화는 결과적으로 더욱 안전하고 신뢰할 수 있는 디지털 환경을 구축하는 데 기여할 것으로 기대된다. 다만, 기술 혁신을 저해하지 않으면서도 효과적인 보안을 확보하는 균형점을 찾는 것이 앞으로의 핵심 과제가 될 것이다. 각국의 법제도가 이러한 도전과제를 어떻게 해결해 나갈지 지속적인 관심이 필요한 시점이다.

미 국

해외 입법 동향

미국 상원, 「의료 사이버보안 개선법안」 발의

미국 마크 워너(Mark R. Warner) 상원의원은 사이버 사고 발생 의료기관에 대한 경제적 보호 조치를 주요 내용으로 한 2024년 「의료 사이버보안 개선법안(Health Care Cybersecurity Improvement Act of 2024)」을 발의 (2024. 3. 22.)

■ 개요

○ 의료 사이버보안 개선법안은 의료 서비스 제공자가 최소한의 사이버보안 표준을 충족한다면 사이버 사고 발생 시 연방정부로부터 비용 신속 및 선지급(AAP)[1]을 받을 수 있도록 허용하는 것을 골자로 함

○ 메디케어 파트 A 공급업체(예: 급성 치료 병원, 전문 간호 시설 및 기타 입원 환자 치료 시설 등) 및 메디케어 파트 B 공급업체(예: 의사(physicians), 의료계 종사자(nonphysician practitioners), 내구 의료 장비 공급업체, 외래 환자 서비스 제공업체 등)는 통제 불가능한 특정 상황에서 현금 유동성 문제에 직면할 수 있음

- 이에 1980년대부터 미국의 메디케어 및 메디케이드 서비스 센터(CMS)는 신속 및 선지급 프로그램을 운영하여 해당 프로그램 참여자를 대상으로 일시적인 재정 지원을 제공해 옴

○ 특히 동 법안은 미국 의료업계에 큰 영향을 미친 Change Healthcare 사건 발생을 계기로 발의되었으며, 사이버 사고 발생 시 의료 서비스 제공자가 직면하는 재정적 문제 해결을 목표로 함

- Change Healthcare 사건이란, 2024년 2월 미국 주요 의료 서비스 기술 회사인 Change Healthcare에서 발생한 랜섬웨어 공격이 미국 전역 의료 서비스 제공업체의 처방전 적체 및 수익 누락으로 이어져 환자 치료 및 기관 운영에 타격을 입힌 사건

- 마크 워너 상원의원은 그동안 의료 부문의 사이버보안 취약점에 대해 지속적으로 우려를 제기해 왔으며, 의료 부문의 사이버보안 개선을 위해 공공·민간 부문의 협력, 의료 서비스 제공자의 사이버보안 역량 강화, 강력한 공격 대응 시스템 구축 등을 강조한 바 있음

1 Accelerated and Advanced Payment

■ 주요내용

○ **(개요)** 의료 사이버보안 개선법안은 현행 《메디케어 병원 신속 지급 프로그램》[2]과 《메디케어 파트 B 선지급 프로그램》[3]을 개정

○ **(신속 및 선지급 자격 요건)** 보건복지부 장관이 사이버보안 사고로 인해 병원 중개인의 운영이 중단되거나 해당 병원의 운영상 비정상적인 상황이 발생하여 해당 병원의 현금 유동성에 문제가 발생했다고 판단한 경우, 다음의 기준을 충족한 병원에게만 신속 및 선지급을 허용

- (1) 해당 병원이 장관이 정한 최소한의 사이버보안 기준을 충족하는 경우
- (2) 해당 병원의 중개인이 운영하는 경우, 해당 중개인이 장관이 정한 최소한의 사이버보안 기준을 충족하는 경우

○ **(평가 권한)** 동 법안은 보건복지부 장관에게 사이버사고를 당한 업체에 자금 신속 및 선지급이 필요한지에 관한 결정 권한을 부여함

○ **(시행일)** 동 법안은 입법이 될 경우, 제정일로부터 2년 후 시행에 들어갈 전망

■ 전망 및 시사점

○ 이번 개정 법안은 최근 의료 부문의 사이버 공격이 기하급수적으로 증가하는 상황에서 사이버 공격으로 인한 재정적 위기로 의료기관의 운영상 어려움이 닥쳤을 때 신속하게 대처할 수 있다는 점에서 긍정적으로 평가

- 환자 치료와 안전에 직접적으로 영향을 미치기 때문에 의료기관에서 발생한 사이버 사고에 대한 빠른 대처는 그 어느 분야보다도 중요

○ 의료 서비스 제공자와 그 서비스 공급업체가 최소한의 사이버보안 표준을 충족해야 해당 개정법의 혜택을 받을 수 있도록 함으로써 의료기관이 사이버 사고에 대비할 수 있는 시스템을 갖추게 하는 유인 요인을 마련했다는 점에서 의의가 있음

2 Medicare Hospital Accelerated Payment Program
3 Medicare Part B Advance Payment Program

Reference

- https://www.warner.senate.gov/public/index.cfm/2024/3/responding-to-change-healthcare-warner-introduces-legislation-to-protect-providers-in-the-event-of-future-hacks-requiring-minimum-cybersecurity-standards
- https://www.warner.senate.gov/public/index.cfm/2024/3/statement-of-sen-warner-on-change-healthcare-cyberattack
- https://www.warner.senate.gov/public/index.cfm/2022/11/warner-releases-policy-options-paper-addressing-cybersecurity-in-the-health-care-sector
- https://www.warner.senate.gov/public/_cache/files/9/1/912e96f3-6819-42f2-b6bc-11b4ed794889/A3B1C470B439B26BBC83E6C7FFFFFA34.goe24245.pdf
- https://www.medicare.gov/what-medicare-covers/what-part-b-covers

해외 입법 동향

미국 사이버보안 및 인프라 보안국, 주요기반시설 사이버 사고 보고 규정을 담은 잠정규정 예고문 발표

미국 사이버보안 및 인프라 보안국(CISA)이 주요기반시설 소유자 및 운영자가 사이버보안 사고를 72시간 이내에 보고할 것을 의무화하는 잠정규정 예고문(NPRM)을 발표 (2024. 3. 27.)

■ 개요

○ 미국 사이버보안 및 인프라 보안국(CISA)[1]은 《주요기반시설에 대한 사이버 사고 보고법(CIRCIA)》[2] 시행 잠정규정 예고문(NPRM)[3]을 발표[4]

- 2022년 3월 제정된 CIRCIA는 사이버보안 및 인프라 보안국에게 동 법에서 명시한 사이버 사고 및 몸값(ransom) 지급 통지 요건에 관한 규칙을 마련하도록 요구하고 있음

○ 제안된 규정은 적용 대상 기업이 '중대한' 사이버 사고를 발견한 직후 72시간 이내에 사이버보안 및 인프라 보안국에 이를 통지하도록 의무화

- 또한, 기업은 랜섬웨어 공격에 대응하여 몸값을 지급하는 경우, 24시간 이내에 이를 사이버보안 및 인프라 보안국에 통지해야 함

○ 동 규칙은 미국 중소기업청(SBA)[5]의 중소기업 규모 규정보다 크거나, 동 잠정규정 예고문(NPRM)에서 명시한 부문별 기준을 충족하는 기업에 적용

○ 잠정규정 예고문(NPRM)에 대한 공공의견은 연방 관보(Federal Register)에 잠정규정 예고문(NPRM)이 게재된 이후 60일 동안 접수한 뒤 이를 토대로 사이버보안 및 인프라 보안국이 최종 초안을 작성해 발표할 예정

1 Cybersecurity and Infrastructure Security Agency. 미국 사이버 보안 및 기반시설 보호 전담기관
2 Cyber Incident Reporting for Critical Infrastructure Act
3 Notice of Proposed Rulemaking
4 2024년 4월 4일 CISA는 NPRM을 연방 관보(Federal Register)에 공식 게재
5 Small Business Administration

■ 주요내용

① 적용대상

○ **(개요)** 적용 대상은 《주요기반시설 보안 및 복원력에 관한 대통령 정책 지침》[6]에서 언급한 16개[7] 주요기반시설 부문 중 특정 기준을 충족하는 기업으로 제한

○ **(적용 기준)** 동 잠정규정 예고문(NPRM) 중소기업청(SBA)에서 정한 '소기업(small business)[8]' 기준을 초과하는 모든 주요기반시설 기업을 적용 대상에 포함하거나, 상기 규모 기준을 충족하지 않더라도 각 부문별 기준을 충족하는 법인을 적용 대상에 포함하도록 제안

- CISA는 16개 주요기반시설 부문 중 3개(▲상업 시설 ▲댐 ▲식품 및 농업) 부문에 속한 법인에 대해서는 별도 기준을 제시하지 않고, 나머지 13개 부문에 대해서 다음과 같은 기준을 제시

〈 주요기반시설 부문별 적용 기준 〉

구분	주요 내용
화학	· 화학 시설 테러 방지 기준의 적용을 받는 화학 시설을 소유 또는 운영하는 법인
통신	· 일반인, 기업 또는 정부에 유·무선 통신을 통해 통신서비스를 제공하는 모든 법인
중요 제조	· 네 가지 중요 제조산업(▲1차 금속제조업 ▲기계제조업 ▲전기장비/전기기기 및 부품 제조업 ▲운송장비 제조업) 중 하나 이상에 종사하는 사업체를 소유 또는 운영하는 모든 법인
방위 산업 기지	· DFARS[9] 252.204-7012에 따라 국방부에 사이버 사고를 보고해야 하는 계약자 또는 하청업체
응급 서비스	· 5만 명 이상의 인구에게 응급 서비스/기능 5가지(▲법 집행 ▲소방 및 구조·구난 서비스 ▲긴급 의료 서비스, ▲비상관리 ▲공중보건과 안전에 기여하는 공공서비스) 중 하나 이상을 제공하는 모든 법인
에너지	· NERC[10]의 주요기반시설 신뢰성 표준에 의거해 사이버 보안 사고를 보고하거나 에너지부에 전기 비상 사고 및 장애 보고서 OE-417 양식 또는 후속 양식을 제출해야 하는 모든 법인
금융 서비스	· 국가의 경제 안보에 영향을 미칠 가능성이 있는 다음 세 가지 범주에 해당하는 법인 - 통화감독청, 특정 법령에 따른 연방준비제도, 연방예금보험공사 등이 규제하는 은행 또는 조직 - 연방차원에서 지급보증을 받고 신용협동조합청이 규제하는 신용협동조합 - 상품선물거래위원회가 규제하는 기관
정부 시설	· ▲주, 지방, 부족 및 자치(SLTT) 정부 시설 ▲교육시설[11] ▲선거시설[12] 등의 세 가지 기준 중 하나를 충족하는 법인
의료 및 공중 보건	· 환자 서비스 관련 특정 기준을 충족하는 모든 주체 및 특정 의약품·기기 제조업체

6 Presidential Policy Directive - Critical Infrastructure Security and Resilience
7 ▲화학 ▲상업 시설 ▲통신 ▲중요 제조 ▲댐 ▲방위 산업 기지 ▲응급 서비스 ▲에너지 ▲금융 서비스 ▲식품 및 농업 ▲정부 시설 ▲의료 및 공중 보건 ▲정보 기술 ▲원자로, 재료 및 폐기물 ▲운송 시스템 ▲상하수도 시스템
8 13 CFR part 121에 명시된 미국 중소기업청(SBA)의 소기업 규정에 근거함
9 Defense Federal Acquisition Regulation Supplement. 미국 국방부 조달 규정

구분	주요 내용
정보 기술	· 다음 네 가지 기준 중 하나 이상을 충족하는 기업 – 연방정부에 IT 하드웨어, 소프트웨어, 시스템 또는 서비스를 제공하는 기업 – NIST에서 정의한 '중요 소프트웨어'의 정의를 충족하는 소프트웨어를 개발하여 지속적으로 판매, 라이선스 또는 유지 관리하는 기업 – OT 하드웨어 또는 소프트웨어 구성 요소의 OEM, 공급업체 또는 통합업체 – 도메인 이름 운영 관련 기능을 수행하는 기업
원자로, 재료 및 폐기물	· 상업용 원자로 또는 연료 주기 시설을 소유하거나 운영하는 기업
운송 시스템	· 비해상 운송 관련 기준을 충족하거나 선박, 시설 또는 대륙붕 외곽 시설을 소유 또는 운영하는 기업
상하수도 시스템	· 커뮤니티 상수도 시스템 또는 공공 소유 처리장(POTW)의 특정 소유자 및 운영자

② 통보의무(Cyber Incident Notification Requirement)

○ **(정의)** 잠정규정 예고문(NPRM)에서 '중대한 사이버 사고(substantial cyber incident)'는 사고의 원인보다 결과에 중점을 두고 있으며, 다음 중 하나 이상을 초래하는 사고로 정의

– 기업의 정보시스템 또는 네트워크의 기밀성, 무결성 또는 가용성에 대한 상당한 손실

– 기업의 운영시스템 및 프로세스의 안전성 및 복원력에 심각한 영향

– 기업의 비즈니스·산업 운영, 또는 재화·서비스 제공 능력의 중단

– 클라우드 서비스 제공업체, 관리형 서비스 제공업체, 기타 제3자 데이터 호스팅 제공업체의 침해 또는 공급망 침해를 통해 또는 이로 인해 발생한 대상 기업의 정보 시스템 또는 네트워크 또는 그 안에 포함된 비공개 정보에 대한 무단 액세스

○ **(사례)** 통보 대상인 중대한 사이버 사고의 사례 유형은 다음과 같음

– 장기간 고객의 기업 서비스 사용을 차단시키는 서비스 거부 공격(DoS attack)

– 기업의 핵심 비즈니스 시스템 또는 정보 시스템 중 하나를 암호화하는 사고

– 관리 서비스 제공업체의 손상된 자격 증명을 사용하여 기업 시스템에 무단 접근한 사고

10 North American Electric Reliability Corporation(북미전력신뢰도위원회): 북미지역 대전력계통(bulk power system)의 신뢰도 관리·감독 담당
11 ①지방정부 산하 교육기관(LEA), 교육서비스기관(ESA), 또는 학생 수 1,000명 이상인 주정부 산하 교육기관(SEA), 또는 ②고등교육법 등에 따라 자금 지원을 받는 고등교육기관(IHE)에 해당하는 모든 기관
12 선거시설은 ▲유권자 등록 데이터베이스 ▲투표시스템 ▲선거 결과를 보고/표시/검증 또는 확정하는 데 사용하는 정보통신기술 등을 포함하되 이에 국한되지 않고, 선거 절차를 지원하거나 주, 지방, 부족 및 자치(SLTT) 정부를 대신하여 결과를 보고 및 표시하는 데 특별히 사용되는 정보통신기술을 개발·판매하거나 관리 서비스를 제공하는 모든 법인을 포괄

○ **(보고 기한)** 적용 대상 기업은 사이버 사고가 발생했다는 '합리적인 믿음(reasonable belief)'이 든 시점으로부터 72시간 이내에, 몸값을 제공했다면 24시간 이내에 이를 보고해야 함

- 다만, 사이버보안 및 인프라 보안국(CISA)은 '합리적인 믿음'이라는 기준이 주관적인 점을 고려하여, 사고 발생 즉시 통보를 기대하기보다는 어느 정도 유연성을 두고 있음

- 만약 사이버 사고와 몸값 지급이 모두 발생한 상황에서는 72시간 이내에 공동 통지하도록 허용하고 있음

○ **(보고서 형식 및 내용)** 사이버보안 및 인프라 보안국(CISA)은 기업이 웹 기반 'CIRCIA 사고 보고 양식(CIRCIA Incident Reporting From)'을 활용하여 《주요기반시설에 대한 사이버 사고 보고법(CIRCIA)》에서 명시한 네 가지[13] 유형의 보고서를 제출할 것을 제안

- 기업은 모든 유형의 보고서 작성 시 ▲보고서 유형 ▲적용 대상 기업의 신원 ▲연락처 ▲(제3자가 대신 제출하는 경우) 위임장 등을 공통적으로 포함해야 함

- 특정 사이버 사고 보고서에는 ▲사고에 대한 설명[14] ▲취약점에 대한 설명 ▲유지한 보안 방어 조치 ▲위협 행위자가 사용한 전술, 기술 및 절차(TTP)[15] ▲위협 행위자의 신원 정보 ▲완화 및 대응조치 ▲기타 정보 등을 제공해야 함

- 몸값 지급 보고서의 경우, 상기 특정 사이버 사고 보고서에 명시해야 하는 항목에 추가로 몸값 지불에 관한 정보(예: 금액) 및 몸값 지불 결과를 보고해야 함

- 한편, 사이버보안 및 인프라 보안국(CISA)는 기업이 이전에 보고한 사이버 사고에 대한 추가 정보를 입수한 경우에는 즉시 보충 보고서를 제출하도록 요구하고 있음

③ 집행

○ **(CISA 집행 권한)** 주요기반시설 업체가 중대한 사이버 사고에 대한 통보 의무를 다하지 않은 경우, 사이버보안 및 인프라 보안국(CISA)은 해당 사고에 대한 보고를 강제할 수 있는 권한을 보유

- 집행 메커니즘으로는 ▲추가 정보 요청(RFI) 발행 ▲소환장 발행 ▲민사 소송(civil action)을 위해 법무부 장관에게 사안 회부 ▲영업 정지 및 금지 절차 착수 등을 포함

13 ▲특정 사이버 사고 보고서(Covered Cyber Incident Report) ▲몸값 지급 보고서(Ransom Payment Report) ▲특정 사이버 사고 및 몸값 지급 합동 보고서(Joint Covered Cyber Incident and Ransom Paymenr Report) ▲보충 보고서(Supplemental Report)

14 사고에 대한 설명에는 ▲영향을 받은 정보 시스템, 네트워크 또는 기기 ▲영향을 받은 정보 시스템 또는 네트워크의 기밀성, 무결성 또는 가용성의 상당한 손실 또는 비즈니스 또는 산업 운영의 중단을 초래한 무단 액세스에 대한 설명 ▲사고의 예상 날짜 범위 ▲해당 기업의 운영에 미치는 영향 등을 포함해야 함

15 Tactics, techniques and procedures

■ 전망 및 시사점

○ 이번 잠정규정 예고문(NPRM)은 국방부 《사이버 사고 보고 조항 및 기타 규정》 등 기존의 다른 사이버 사고 보고 요건에 비해 적용 대상 범위를 크게 확장하고 사고 보고 및 몸값 지급에 관한 구체적인 일정을 확정함

○ 동 잠정규정 예고문(NPRM)의 세부 사항은 공공의견에 따라 변경될 가능성이 있으나 미국 사이버보안 및 인프라 보안국(CISA)의 전반적인 규제 방향성을 제시하고 있다는 점에서 의의가 있음

○ 이에 잠재적 적용 대상 기업은 동 규칙의 주요 조항을 숙지하고, 다른 기관의 사이버 사고 보고 의무와 중복되는 사항 여부를 재점검할 필요가 있음

Reference

- https://www.cisa.gov/news-events/news/cisa-marks-important-milestone-addressing-cyber-incidents-seeks-input-circia-notice-proposed
- https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements
- https://crsreports.congress.gov/product/pdf/R/R48025/1
- https://www.jdsupra.com/legalnews/cisa-cyber-incident-reporting-for-7574549/
- https://www.dataprotectionreport.com/2024/04/cisa-issues-proposed-rules-for-cyber-incident-reporting-in-critical-infrastructure

해외 입법 동향

미국 백악관, 연방정부의 안전하고 책임성 있는 인공지능 사용에 관한 신규 각서 발표

미국 백악관이 AI 위험으로부터 공공의 안전을 보호하기 위해 연방정부 부처 및 기관을 대상으로 각서(Memorandom) 및 팩트시트(Fact Sheet)를 발표 (2024. 3. 28.)

■ 개요

○ 미국 관리예산국(Office of Management and Budget)이 발표한 각서 및 설명자료는 지난 2023년 10월 발표된 '안전하고 신뢰할 만한 AI에 관한 대통령 행정명령'[1]에 근거하여 발행된 문서에 해당

- 동 각서는 미국 연방 부처 또는 기관을 대상으로 AI 위험 관리, 투명성, 거버넌스 등에 대한 표준을 설정함으로써, 빠르게 진화하는 AI 산업에 대한 안전장치를 확립함과 동시에 AI 기술의 추가적인 혁신을 장려

- 이를 통해 연방정부가 AI 규제가 미흡한 부분에서 발생할 수 있는 위험으로부터 대중을 보호하고 공공의 이익을 추구할 수 있도록 함

■ 주요내용

○ **(안전성 강화)** 연방기관은 2024년 12월 1일까지 기관이 사용하는 AI 도구가 미국인의 권리 및 안전에 영향을 미칠 것을 대비해 인공지능 사용에 있어 위험관리(Managing risks from the use of AI) 조치를 시행해야 함

- 해당 위험관리 조치에는 대중에 대한 AI의 영향을 안정적으로 평가, 테스트 및 모니터링하는 것을 비롯, 알고리즘 차별에 대한 위험 감소 및 AI 사용 방식에 대한 투명성 제공 등과 같은 다양한 수단 등이 포함

1 Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (2023. 10. 30)

구분	주요 내용
영향 평가	• 연방기관은 정기적으로 영향 평가를 최신화하고 AI의 수명 주기에 걸쳐 이를 활용해야 함 – 이때 연방기관은 최소한 ▲의도한 AI의 목적과 그 기대 이익 ▲AI 사용과 관련한 잠재적 위험 및 위험 최소화를 위한 조치 ▲관련 데이터의 품질과 적절성 여부 등을 문서화해야 함
성능 테스트	• 연방기관은 AI가 실제 상황에서 의도한 대로 작동하는지 여부를 확인하기 위해 적절한 테스트를 수행해야 함
외부기관 평가	• 연방기관은 AI 시스템이 적절하게 의도한 대로 작동하고 있는지, 또한 기대되는 혜택이나 이점이 잠재적인 위험을 능가하는지 여부를 보장하기 위해 독립적인 외부기관을 통해 관련 AI 문서를 검토받아야 함
모니터링	• 연방기관은 AI의 기능 저하를 모니터링하고 권리 및 안전에 미치는 영향의 변화를 감지하기 위해 지속적인 절차를 마련해야 함
정기적 위험 평가 (인적 검토)	• AI 모니터링과 관련해서는 AI 배포 상황, 위험, 이점 및 연방기관의 요구가 반영됐는지 여부를 결정하기 위해 정기적인 인적 검토가 수행되어야 함 – 최소한 연간 단위 또는 AI 사용 요건 및 상황이 크게 변경된 후에는 인적 검토가 이루어져야 하며, 실제 상황에서 AI가 작동하는지 여부를 확인하는 성능 테스트가 새로이 수행되어야 함
위험 완화 조치	• 연방기관이 지속적 모니터링, 정기적 위험 평가 등을 통해 권리 및 안전에 대한 새로운 위험을 식별하게 되는 경우, 연방기관은 해당 위험을 최소화하기 위해 AI를 업데이트하거나 보다 엄격한 인간 개입 요건 등을 설정하는 등의 조치를 취해야 함
훈련 및 평가	• 연방기관은 AI 작동 담당자가 AI의 결과물을 해석하고 이에 따라 조치를 취할 수 있도록 보장하기 위해 충분한 훈련, 평가 및 감독 체계를 구현해야 함
인간 개입	• 연방기관은 권리 또는 안전에 중대한 영향을 미칠 수 있는 AI의 결정 또는 행동과 관련해 추가적인 인간 감독, 개입 및 책임을 제공해야 함
공고 및 일반언어 문서 제공	• 연방기관은 개인정보 보호, 민감한 법 집행 또는 국가 보안 등을 포함하여, AI 활용 사례 목록이 이용자와 일반 대중에게 AI를 공개적으로 고지하는 역할을 할 수 있도록 일반언어로 작성된 문서를 제공해야 함

· 이를 통해 대중들은 ▲공항에서의 AI 안면 인식 활용 거부 ▲연방 의료 시스템 내 의학적 진단 과정에서 사용되는 AI에 대한 인간의 감독 요구 ▲연방정부 서비스 내 사기 탐지 용도로 활용된 AI가 가한 피해에 대한 해결책 요구 등의 이익 또는 혜택을 향유 가능

– 만약 연방기관이 상기 위험관리 조치를 적용할 수 없는 경우 AI 기술 사용이 필요하다는 것을 증명할 수 없는 한 해당 기술 사용을 반드시 중단해야 함

○ **(투명성 확대)** 연방기관은 AI 사용과 관련하여 대중에 대한 투명성을 개선하기 위해 다양한 조치를 시행해야함

투명성 조치
· 대중의 권리나 안전에 영향을 미치는 연방기관의 AI 사용 사례 및 관련 위험 해결 방법 등을 포함한 연방기관의 AI 사용 사례 연간 목록 공개
· 민감도로 인해 공개 목록에서 제외된 연방기관의 AI 사용 사례에 관한 판단 기준 보고
· 관리예산국 정책 준수 의무에서 면제된 모든 AI에 대한 면제 정당성 여부와 그 사유 공개
· 연방정부가 소유한 AI 코드, 모델 및 데이터 공개 (다만, 해당 공개가 공공 또는 정부 운영에 위험을 초래하지 않는 범위 내에 한정)

○ **(혁신 촉진)** 연방기관은 AI 혁신을 가로막는 불필요한 장벽을 제거하여, AI 기술로써 연방기관이 사회의 가장 시급한 문제를 해결할 수 있도록 해야 함

- 관리예산국은 각 연방기관이 업무를 수행하면서 적절한 위험관리 조치를 취함과 동시에 생성형 AI가 과도한 위험을 초래하지 않게끔 사용할 수 있도록 권장하고 있으며, 생성 AI의 발전에 힘입어 사회적 문제 해결의 기회 창출을 장려

기관별 AI 활용 사례

· **(재해 대응)** 연방재난관리청(Federal Emergency Management Agency)은 허리케인 여파에 따른 구조적 피해를 신속하게 검토하고 평가하기 위해 AI 적극 활용
· **(기후위기 극복)** 연방해양대기청(National Oceanic and Atmospheric Administration)은 기상이변, 홍수, 산불 등에 대해 보다 정확한 예측을 위해 AI 개발
· **(공중 보건 증진)** 질병통제예방센터(Centers for Disease Control and Prevention)는 AI를 활용해 질병의 확산을 예측하고 아편성 진통제인 오피오이드의 불법 사용을 감지하며, 메디케어 및 메디케이드 서비스 센터(Center for Medicare and Medicaid Services)는 AI를 통해 폐기물을 줄이고 약품 비용의 이상 징후를 파악
· **(공공 안전 보호)** 연방항공청(Federal Aviation Administration)은 AI를 활용해 대도시 지역의 항공 교통 혼잡도를 완화함으로써 이동시간을 개선하며, 연방철도청(Federal Railroad Administration)은 철도 선로의 안전성 상태를 예측하기 위해 AI를 연구

○ **(인력 확충)** 연방기관은 AI 위험관리, 혁신 및 거버넌스를 발전시키기 위해 적극적으로 AI 인재를 확충 및 강화할 예정

- 연방정부는 신뢰할 수 있고 안전한 AI 사용을 촉진하기 위해 100명의 AI 전문가를 2024년 여름까지 고용할 예정이며, 2024년 4월 18일 연방정부 전역에서 AI 인재를 위한 취업 박람회를 개최

  · 이를 뒷받침하기 위해 인사관리국(Office of Personnel Management)은 AI 인재를 확보하기 위한 목적으로 AI 인재에 대한 급여 및 근무 유연성을 높이는 지침을 발표한 바 있음

  · 연방정부 차원에서도 2025 회계연도 대통령 예산에 연방정부 주도의 AI 교육 프로그램을 확대하기 위해 추가로 500만 달러 규모의 예산을 편성

○ **(AI 거버넌스 강화)** 연방기관은 AI 사용에 대한 책임, 리더십 및 감독을 보장하기 위해 거버넌스와 관련한 여러 조치를 취해야 함

- **(최고 AI 책임자 지정)** 연방기관은 AI 사용을 조정할 책임자로서, 동 각서 발행일로부터 60일 이내에 최고 AI 책임자(Chief AI Officer Council, CAIO)를 지정해야 함

- **(AI 거버넌스 위원회 설치)** 연방기관 중 CFO법 기관(CFO Act agency)[2]에 해당하는 기관은 AI

2 Chief Financial Officers (CFO) Act of 1990을 준수해야 하는 미국 연방 부처 및 기관. CFO법은 연방정부의 재무 관리를 개선하기 위한 미국 연방법으로, 동 법에 따라 미국의 24개 부처(15개 부)와 연방기관(9개 기관)에 CFO 직위가 신설되었으며 이들을 관리예산국이 관리

사용에 대한 장벽을 철폐하고 관련 위험을 관리하는 등 기관의 AI 사용을 관리할 수 있는, 고위 관리로 구성된 AI 거버넌스 위원회를 설치해야 함

· 현재 ▲국방부(Department of Defense) ▲제대군인부(Department of Veterans Affairs) ▲주택도시개발부(Department of Housing and Urban Development) ▲국무부(Department of State)가 위원회 설치를 완료

· 아직 설치하지 못한 CFO법 기관들도 2024년 5월 27일까지 AI 거버넌스 위원회 설치를 마쳐야 함

■ 전망 및 시사점

○ 미국 행정부의 이번 각서 발행은 AI 기술이 초래할 수 있는 위험성에 대비해 정부 차원에서 발 빠른 대처를 보였다는 점에서 긍정적으로 평가

- 질병에 대한 치료법 발견이나 철도 안전 개선 등과 같은 AI 기술의 긍정적 효과 이면에는 소수자가 표적이 될 가능성 및 생물학적 무기 개발에 쉽게 악용될 가능성 등이 상존하는데, 이를 우려한 전문가들의 의견이 시의적절하게 정부 정책에 반영된 결과

○ 미국 정부 또한 이번 각서 발행을 통해 AI에 대한 투명성 제고 등을 바탕으로 공공 서비스를 개선하고 다양한 사회적 과제에 대한 진전을 이룩할 기회가 될 것이라고 기대감을 표명

○ 그러나 일각에서는 행정부 차원에서 동원할 수 있는 수단에는 한계가 뚜렷하므로 AI 산업의 근간을 전체적으로 확립할 수 있는 입법적 방식이 반드시 동반되어야 한다는 비판도 제기

- 다만 EU가 추진하고 있는 세계 최초 AI 규제입법인 인공지능법이 최종 입법단계에 접어든 것과 대조적으로, 미국의 경우 단시일 내에 입법적 성과가 나타나지 않을 가능성이 높다는 전망이 지배적

Reference

▪https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf
▪https://www.whitehouse.gov/briefing-room/statements-releases/2024/03/28/fact-sheet-vice-president-harris-announces-omb-policy-to-advance-governance-innovation-and-risk-management-in-federal-agencies-use-of-artificial-intelligence/
▪https://edition.cnn.com/2024/03/28/tech/vp-kamala-harris-agencies-ai-technology/index.html
▪https://ny1.com/nyc/all-boroughs/politics/2024/03/27/biden-administration-artificial-intelligence-policy-federal-government
▪https://www.wired.com/story/white-house-new-guardrails-government-use-of-ai/

해외 입법 동향

미국 상원, 「미래 AI 혁신 법률(안)」 발의

미국 상원은 AI 표준 확립 및 AI 안전연구소 설립을 골자로 하는 「미래 AI 혁신 법률(안)[1]」을 발의 (2024. 4. 19.)

■ 개요

○ 「미래 AI 혁신 법률(안)」은 미국 AI 안전연구소(AI Safety Institute)를 설립하여 AI 관련 조치를 취할 수 있도록 권한을 부여하는 한편, AI 표준 확립 및 AI 산업 발전을 위한 정책 촉진에 관한 사항을 담고 있음

- 동 법안은 2023년 10월 조 바이든 대통령이 발표한 AI 행정명령[2]의 내용과 일맥상통하며, 「미국 반도체 및 과학법[3]」을 기반으로 민간부문의 주요 AI 혁신을 지원하도록 함

■ 주요내용

○ **(용어 정의)** 「미래 AI 혁신 법률(안)」에서는 법률 용어를 다음과 같이 정의함

구분	주요 내용
인공지능 (AI)	• AI는 2020년 국가 인공지능 이니셔티브법(15 U.S.C. 9401) 제5002항 준용 – 인간이 정의한 특정 목표에 대해 현실 또는 가상 환경에 영향을 미치는 예측, 추천 또는 결정을 내릴 수 있는 기계 기반 시스템을 의미 – 기계 및 인간 기반 입력을 사용하여 실제 및 가상 환경을 인식하고, 자동화된 방식으로 분석을 통해 이러한 인식을 모델로 추상화하며, 모델 추론을 사용하여 정보 또는 행동에 대한 옵션을 공식화함
블루팀 (Blue Team)	• 인공지능 시스템의 네트워크 보안 상태에 대한 독립적인 기술적 검토가 필요한 기관에 운영 네트워크 취약성 평가를 수행하고 완화 기술을 제공하기 위한 노력을 의미
레드팀 (Red Team)	• 시스템의 유해한 출력, 예기치 않거나 바람직하지 않은 시스템 동작, 제한 사항 또는 시스템 오용과 관련된 잠재적 위험 등 인공지능 시스템의 위험, 결함 및 취약성을 식별하기 위한 인공지능 시스템에 대한 구조화된 적대적 테스트 노력을 의미
테스트베드 (Testbed)	• 인공지능 시스템을 포함한 도구 및 기술의 기능, 신뢰성, 유용성 및 성능을 평가하기 위해 엄격하고 투명하며 복제 가능한 테스트를 수행할 수 있는 시설 또는 메커니즘을 의미

1 Future of Artificial Intelligence Innovation Act of 2024 (S.4178)
2 Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence
3 CHIPS and Science Act of 2022 (Public Law No.117-167)

○ **(AI 안전연구소 설립)** 상무부의 표준기술 차관은 동 법안 제정 후 1년 이내에 미국 AI 안전연구소를 설립해야 하며, 해당 연구소는 AI 분야의 혁신을 촉진하기 위한 표준 개발을 담당

- AI 안전연구소는 AI 시스템 및 파운데이션 모델과 관련해 ▲개발 관행 통합을 위한 표준 개발 ▲안전성, 신뢰성, 보안 및 개인정보보호 연구 수행 ▲외부 공격 및 보안 취약성으로부터 보호하기 위한 지침, 방법론 및 모범 사례 마련 ▲사고 추적 도구 개발 등의 업무를 수행할 예정

○ **(AI 테스트베드 프로그램 구축)** 국립 연구소들과 국립표준기술연구소(NIST), 국립과학재단(NSF), 에너지부(DOE) 및 민간 부문의 협력을 통해 AI 시스템의 기능 및 한계 평가를 위한 테스트베드 프로그램 운영 사항을 규정

- 특히, 신소재 개발을 목적으로 양자 하이브리드 컴퓨팅, 로봇 공학 등 신기술과 결합한 AI를 활용한 공공-민간 협력 테스트베드를 승인

테스트베드 프로그램 주요내용

- 인공지능 시스템의 기능과 한계에 대한 평가를 실행
- 실행 가능한 최대 범위까지 기존 솔루션을 사용
- 실행 가능한 범위 내에서 인공지능 시스템에 대한 자동화되고 재현가능한 평가 및 위험평가 개발
- 인공지능 시스템의 평가 및 위험평가를 실행하는 데 필요한 계산 리소스 평가
- 인공지능 시스템의 평가 및 위험평가를 실행하는 데 필요한 컴퓨팅 리소스를 효과적으로 최소화하는 방법 연구
- 고, 중, 저 컴퓨팅 집약도를 위해 설계된 인공지능 시스템에 대한 테스트, 평가 및 위험평가 개발을 고려
- 테스트베드에서 평가한 인공지능 시스템이 보안 위험을 초래하는 방식으로 배치될 수 있는 시나리오를 우선적으로 식별 및 평가해야함
- 필요한 경우 국립연구소에서 ▲자율 공격 사이버 역량 ▲인공지능 소프트웨어 생태계 및 그 밖의 사이버 보안 취약점 ▲화학, 생물학, 방사능, 핵, 주요 기반 시설 및 에너지 보안 위협 또는 위험 ▲차관이 필요하다고 판단하는 기타 역량 관련하여 기밀 테스트베드를 구축하거나 기존의 기밀 테스트베드를 활용하는 것을 우선적으로 고려

○ **(데이터 세트 개방)** 과학기술정책실(OSTP)[4]장은 국립표준기술연구소(NIST)를 통해 AI 시스템 훈련 및 평가를 위한 공개적으로 이용할 수 있는 데이터세트 우선순위 리스트를 생성해야 함

- 우선순위를 정하기 전 민간 업계, 학계, 시민 사회 및 기타 관련 이해관계자로부터 의견을 받기 위한 공개 의견수렴 절차를 구현해야 함

- 의견수렴을 거쳐 정해진 우선순위에 따라 생성된 해당 리스트는 ① 공익을 위해 새로운 AI 시스템을 발전시킬 수 있는 데이터와 ② 연방정부의 자금 지원 없이는 민간 부문에서 독립적으로 충분한 지원을 받지 못할 데이터세트를 우선시해야 함

- 특히, 과학기술정책실(OSTP)장은 ▲농업, 의료, 운송, 제조, 통신, 기상서비스 등의 업계와 미국 중소기업에 긍정적인 효용가치를 제공하는 데이터 ▲데이터세트의 공개가 가져올 수 있는 잠재적 국가 안보 위협 등을 고려하여 우선순위를 선정해야 함

4 Office of Science and Technology Policy

○ **(연방 경연대회 개최)** 양자 컴퓨팅 등 신기술과 고급 AI 기술의 통합을 통한 AI 솔루션 발견에 중점을 두고, 전국의 연구원들을 참여시켜 과제를 진행하는 형태의 그랜드 챌린지를 개최하도록 규정

- 그랜드 챌린지는 아래와 같은 우선순위가 높은 과제에 대한 돌파구를 찾는 것을 목표로 함

우선순위 과제
• 머신러닝 및 양자 등 새로운 기술과의 통합을 통해 컴퓨팅 및 AI의 발전을 위한 마이크로전자공학의 엔지니어링 및 응용 연구의 장벽 극복을 위해 AI 활용 • 컴퓨팅 및 AI 기술의 혁신적 또는 장기적 발전을 촉진 • 미국 첨단 제조업의 장벽을 극복하기 위해 양자 및 머신러닝과 같은 신흥 기술 간의 통합을 포함한 차세대 AI 솔루션 개발 • 해양 선박에서의 AI 사용 확대 등 경제 각 부문에 대한 AI 솔루션 개발 • 펜타닐, 불법 밀수품 및 기타 불법 활동 탐지와 관련된 솔루션을 포함하여 국경 보안을 개선하기 위한 AI 솔루션 개발

○ **(국제협력 구축)** 미국 상무부(DOC)[5] 장관, 국무부(DOS)[6] 장관 및 과학기술정책실(OSTP)장은 국제 AI 표준에 대한 협력과 세계 각국 과학 및 학술 기관 간의 다자간 연구 협력을 위해 미국 동맹국들과의 AI 연맹을 결성해야 함

AI연맹을 통한 국제협력 주요내용
• 인공지능과 인공지능 생태계의 혁신과 발전에 대한 접근 방식 협력 • 상호 운용가능한 국제표준의 개발·사용 또는 인공지능과 관련된 표준의 조화에 대한 조정 • 공통 인공지능 표준의 채택 촉진 • 적절한 경우 정부 간 정보공유를 위한 협정 체결을 포함하여 인공지능 안전 표준의 일관된 글로벌 적용 조정을 촉진하기 위해 필요한 정부 간 인프라를 개발하기 위한 노력 • 파트너 국가의 민간 부문 이해관계자를 참여시켜 연합 파트너에게 인공지능 및 관련 표준 개발의 최근 개발 상황 전파

■ 전망 및 시사점

○ 「미래 AI 혁신 법률(안)」은 정부·민간·학계 간의 협력을 중심으로 AI 표준화, 연구개발, 인재 육성, 신산업 창출을 가속화할 수 있는 기반을 마련함으로써 미국의 AI 경쟁력을 높일 것으로 기대

- 동 법안은 AI 표준 개발을 통해 AI 제품과 서비스의 상호운용성과 호환성을 높이고, 신뢰성과 안전성을 높이며, 개발 및 구현의 효율성을 향상하고, 글로벌 협력과 경쟁력 강화에 이바지함으로써 궁극적으로 AI 혁신과 산업화를 가속화할 수 있다는 점에서 의의가 있음

- 특히 공공 데이터 세트의 개방은 데이터 접근성이 낮은 중소기업에게도 AI 시스템의 새로운 발전에 기여할 수 있는 기회를 제공할 것으로 전망

5 Department of Commerce
6 Department of State

Reference

- https://www.hickenlooper.senate.gov/press_releases/hickenlooper-bipartisan-senators-introduce-ai-bill-to-accelerate-innovation-strengthen-u-s-leadership/
- https://www.cantwell.senate.gov/news/press-releases/cantwell-colleagues-introduce-bipartisan-bill-to-ensure-us-leads-global-ai-innovation
- https://www.hickenlooper.senate.gov/wp-content/uploads/2024/04/Future-of-AI-Innovation-Act-Bill-Text.pdf
- https://www.hickenlooper.senate.gov/press_releases/hickenlooper-proposes-ai-auditing-standards-calls-for-protecting-consumer-data-increasing-transparency/
- https://www.congress.gov/bill/118th-congress/senate-bill/4178/all-info

해외 입법 동향

미국 상원, AI 보안 위험관리 강화를 위한 「안전한 AI 법안」 발의

미국 상원에서 AI 관련 보안·안전 사고 및 위험의 추적·처리를 개선하고, AI 보안센터를 신설하는 것을 골자로 하는 초당적 성격의 「안전한 AI 법안」[1] 발의 (2024. 5. 1.)

■ 개요

○ AI 활용이 확산됨에 따라, 증가하는 AI 관련 보안·안전 위험을 예방·완화하기 위하여 미국 연방정부의 현행 사이버보안 사고 보고 및 취약점 관리체계를 개선·조정하는 내용의 「안전한 AI 법안」 발의

○ 법안에 따르면, 미국 표준기술연구소(NIST)[2], 사이버보안 및 기반시설 보호국(CISA)[3], 국가안보국(NSA)[4] 등 정부기관들은 AI 안전 및 보안 강화를 위해 다음과 같은 활동을 전개해야 함

- AI 보안 사고 및 위험의 추적·처리를 개선하기 위하여 ▲보안 사고 및 취약점 정보 관리체계 업데이트 ▲AI 보안사고와 관련된 취약점 데이터베이스(DB) 구축 ▲AI 모델의 공급망 위험에 대한 모범사례 개발 등을 추진

- AI 보안센터를 신설하여 AI 보안·안전 위험에 대한 연구 활동을 촉진하고, AI 보안 관련 지침을 개발

■ 배경 및 목적

○ **(배경)** AI의 개발 및 활용이 증가하는 가운데 일반 소프트웨어와는 다른 AI 시스템의 특성을 고려한 보안 위험관리 필요성이 대두

- **(사고 보고 및 취약점 정보공유의 중요성)** 보안 사고 보고(report)와 관련 취약점 대한 체계적인 문서화 및 정보공유는 사이버보안 위험을 완화하고 미래에 발생가능한 사고를 예방하는 데에 매우 중요

1 Secure Artificial Intelligence Act of 2024 (S. 4230)
2 National Institute of Standards and Technology. 과학, 산업기술 분야 표준을 연구하는 미국 상무부 기술관리국 산하 국영 연구소
3 Cybersecurity and Infrastructure Security Agency. 미국 사이버 보안 및 기반시설 보호 전담기관
4 National Security Agency. 국방부 산하 해외 통신 및 정보·수집 분석을 담당하는 정보기관

- **(현행 체계)** 미국 연방정부는 보안 사고 및 취약점 정보를 수집·추적·공유하기 위해 NIST의 국가취약점데이터베이스(NVD)[5]와 CISA의 공개적으로 알려진 컴퓨터 보안 취약점 목록(CVE)[6] 프로그램을 운영 중

- 또한 NSA는 사이버보안 협력센터(CCC)[7]를 통하여 신규 또는 기존의 사이버보안 과제들에 대한 지침을 제공

- **(AI 확산으로 인한 과제)** AI 시스템의 취약점은 일반 소프트웨어의 취약점과 다르고 AI 시스템에 대한 공격 방식도 기존의 공격 방식과 상이하나, 현재 연방정부의 정보보안 위험관리 노력에는 AI 관련 위험이 적절히 반영되지 못함

○ **(목적)** 연방정부의 사이버보안 사고 보고 및 취약점 관리체계를 업데이트하여 정부와 민간기업 간 정보공유를 개선하고, AI에 대한 보안 위험을 더욱 효과적으로 관리할 필요

■ 주요내용

① 정의

용어	정의
AI 안전 사고 (AI Safety Indicent)	• AI 시스템의 운용이 ▲신체적·정신적 피해를 초래하거나, 또는 ▲인간의 생명·건강·재산이나 환경을 위험에 빠뜨릴 위험이 커지는 사건
AI 보안 사고 (AI Security Incident)	• ▲제3자가 AI 시스템의 동작이나 특성에 대한 정보를 추출할 수 있는 방식으로 AI 시스템이 작동될 위험이 커지거나, ▲제3자가 AI 시스템이나 관련 시스템의 기밀성, 무결성, 가용성을 파괴할 수 있는 조작 능력이 커지는 것
AI 보안 취약점 (AI Security Vulnerability)	• 제3자가 데이터포이즈닝[8], 회피공격[9], 개인정보 기반 공격[10], 남용 공격[11] 등을 통해 승인 없이 AI 시스템의 기밀성, 무결성, 가용성을 파괴하는 데에 악용할 수 있는 AI 시스템의 취약점
반AI (Counter-AI)	• AI시스템 또는 인접 시스템(adjacent system)[12]의 기밀성, 무결성, 가용성을 파괴하기 위해 AI 시스템의 동작이나 특성에 관한 정보를 추출하거나, AI 시스템을 조작하는 방법을 학습하는 기술(techniques) 또는 절차(procedures)

5 National Vulnerability Database. NIST가 관리하는 공식적인 보안 취약점 데이터베이스
6 Common Vulnerabilities and Exposures. 1999년 비영리 연구개발기관인 MITRE가 이미 알려진 보안 취약점을 식별하는 방식을 표준화하기 위하여 미국 연방정부의 후원으로 소프트웨어와 펌웨어의 취약점을 파악·분류해 개발한 식별 코드를 의미. 보안 관리자는 공통으로 정의된 CVE 식별 코드를 통해 특정 보안 취약점과 관련한 정보를 획득하고 보안 경고에 효과적으로 대응 가능
7 NSA Cybersecurity Collaboration Center. 사이버 방어를 위한 공공-민간 부문 사이버보안 전문가 간 파트너십을 도모하기 위해 설립
8 Data Poisoning. 고의로 오류를 포함한 데이터를 학습 데이터셋에 추가함으로써 AI 모델을 손상시키는 행위
9 Evasion Attack. AI가 잘못된 의사결정을 하도록 머신러닝 모델의 추론 과정에서 데이터(입력 값)를 조작하여 머신러닝을 속이는 공격 유형
10 Privacy-based Attack. AI가 훈련한 데이터 중 민감 정보를 추출하여 이를 오용하는 시도
11 Abuse Attack. 피싱 이메일을 생성하거나 악성코드 작성과 같이 악성 콘텐츠를 생성하기 위해 AI 도구를 무기화하는 공격(사이버 범죄를 지원하는 대규모언어모델(LLM) 등)
12 작업에 데이터를 제공하거나 작업에서 데이터와 관리를 가져오는 것

② 주요 조치

○ **(NVD 및 CVE 프로그램 업데이트)** NIST와 CISA로 하여금 각각 NVD와 CVE 프로그램을 업데이트하거나 AI 보안 취약점에 대한 자발적 보고를 추적할 수 있는 새로운 프로세스를 수립하도록 요구

- NIST와 CISA는 동 법 제정 후 180일 이내에 각각 NVD와 CVE 프로그램에 대한 업데이트 진행

구분	역할
NIST 소장	• NVD 업데이트 작업을 통해 NVD 및 관련 취약점 관리 프로세스에 AI 보안 취약점을 최대한 반영하고, NVD의 활용을 부적절하게 하는 AI 보안 취약점의 특성을 식별하며, 해당 취약점들을 관리하기 위한 프로세스를 개발
CISA 국장	• CVE 업데이트 작업을 통해 CVE 및 관련 프로세스·절차에 최대한 많은 AI 보안 취약점들을 목록화하여 포함시키고, CVE의 활용을 부적절하게 하는 AI 보안 취약점의 특성을 식별하며, 해당 취약점들을 목록화할 수 있는 프로세스를 개발

- NIST는 동 법 제정 후 30일 이내에 기존의 취약점 보고 프로세스 및 표준이 AI 보안 취약점들을 효과적으로 담아낼 수 있는지를 평가하기 위한 '다수 이해관계자간 협력 프로세스(multi-stakeholder process)'[13]를 시작하고, 필요시 기존의 보고 프로세스 및 표준에 대한 업데이트 추진

○ **(AI 보안 사고 취약점 DB 구축)** NIST와 CISA는 AI 보안 사고에 대한 자발적인 보고 내용을 추적할 수 있는 공공 DB를 구축해야 함

- NIST와 CISA는 동법 제정 후 1년 이내에 AI 보안·안전 사고와 취약점을 추적할 수 있는 자발적 보고 DB를 개발 및 구축

- DB는 모든 AI 보안 취약점에 대한 공개 저장소로 ▲민간기업, 공공기관, 시민사회단체, 학계 연구자 등이 자발적으로 보고하는 모든 확인된 또는 의심되는 AI 보안 사고들을 담고 있으면서도, ▲영향받는 당사자들에 대한 기밀성은 유지하고, ▲AI 보안 사고를 적절히 분류하여 정보 접근성을 개선할 수 있는 방식으로 구축

- 특히 주요기반시설, 안전 필수 시스템(safety-critical system)[14], 상업·공공 조직에서 널리 활용되는 AI 모델과 관련된 사고와, 미국 국민이나 국가 경제에 치명적인 영향을 미칠 수 있는 사고들을 중요하게 간주하여 우선적으로 다룸

○ **(AI모델 공급망 위험 관련 모범사례 개발)** AI모델의 훈련·유지와 관련하여 공급망 측면의 위험[15]들을 관리할 수 있는 모범사례를 개발·채택하도록 규정

- CISA는 동법 제정 후 90일 이내에 NSA 및 NIST와 협력하여 관련 모범사례의 개발·채택을 위한 다수 이해관계자간 협력 프로세스를 추진

13 정부기관, 비영리조직, 민간기업 등 다양한 관련 주체들이 공동의 목표를 달성하기 위해 협력하는 프로세스
14 시스템 고장이나 오작동으로 인간의 사망이나 중상, 장비·재산의 손실 또는 심각한 손상, 환경에 중대한 악영향을 초래할 수 있을 만큼 중요성이 큰 컴퓨터·전기·전자시스템 등으로, 인간의 생명과 밀접한 관련이 있는 항공기, 원자력 발전 제어 설비, 의료 설비 등이 대표적인 예
15 학습 데이터의 수집 및 처리 등에서 해외 인력에 대한 높은 의존도, 제한적인 훈련 데이터 등

○ **(AI 보안센터 설립)** 동 법안은 NSA로 하여금 법 제정 후 90일 이내에 AI 보안센터 신설을 명시

- **(AI 보안센터의 역할)** ▲민간 부문 및 학계 연구자들을 위한 AI 보안 연구 테스트베드 제공 ▲'반AI 기술' 등을 방지하거나 완화할 수 있는 지침 개발 ▲국가안보시스템 관리자들의 안전한 AI 채택 관행의 촉진 등

■ 전망 및 시사점

○ 동 법안은 연방정부가 기존의 사이버보안 사고 보고 메커니즘을 기반으로 새롭게 대두하는 AI 관련 위험을 관리할 수 있도록 사고 보고 및 취약점 DB를 현대화하는데 초점

- 자발적 사고 보고 메커니즘에 관여하는 여러 정부기관들에 새로운 임무를 부여하고, 이들 기관이 관련 노력을 조화롭게 추진할 수 있도록 역할을 조정

○ 또한 '반AI 기술' 등 AI 보안 분야에서 핵심적인 연구활동을 촉진하는 데에 기여할 전망

- AI 보안센터의 설립 및 역할에 대한 법적 근거를 확립함으로써 민간·학계의 관련 연구활동과 이에 대한 정부 지원을 활성화할 것으로 기대

- 특히 바이든 대통령의 '안전하고 신뢰할 수 있는 인공지능 개발 및 사용 행정명령'[16]에서 강조하고 있는 AI 분야 연구 장려 방침을 지원할 전망

Reference

▪https://www.warner.senate.gov/public/index.cfm/2024/5/warner-tillis-introduce-legislation-to-advance-security-of-artificial-intelligence-ecosystem
▪https://www.warner.senate.gov/public/_cache/files/5/d/5d8e0506-640c-44b2-bf9e-02f1e05d7517/1086DA0659080D3B088DEF8979CEAE38.secure-ai-full-text.pdf
▪https://www.warner.senate.gov/public/_cache/files/3/c/3c24cbde-e4f5-419c-9e92-6e03dc41b801/C703EAA7ADE81649290CC7518FA1916F.secure-ai-act-one-pager-v2.pdf
▪https://www.medianama.com/2024/05/223-us-senate-proposes-new-bill-to-address-ai-security-concerns/
▪https://www.dataguidance.com/news/usa-senators-introduce-bill-secure-ai-act-2024-congress
▪https://www.theverge.com/2024/5/1/24146566/ai-security-bill-warner-tillis-senate-redteam-safety

16 Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence(EO 14110, 2023.10.30.)

해외 입법 동향

미국 연방통신위원회(FCC), ‘인터넷 라우팅 보안 개선을 위한 보고 요구사항’에 관한 잠정규정 예고문(NPRM) 발표

미국 연방통신위원회(FCC)가 사이버공격으로부터 미국의 통신 네트워크를 보호하기 위하여, ‘인터넷 라우팅 보안 개선을 위한 보고 요구사항’[1]에 대한 잠정규정 예고문(NPRM)을 발표 (2024. 6. 7.)

■ 개요

○ 연방통신위원회는 광대역 인터넷 액세스 서비스 제공업체를 대상으로, 경계 경로 프로토콜(Border Gateway Protocol, BGP) 보안 강화를 위한 잠정규정 예고문을 발표하고 7월 17일까지 의견수렴

- 미국의 모든 광대역 인터넷 액세스 서비스 제공업체들은 BGP의 취약점 완화 관련 향후 계획 보고서를 연 1회 작성 및 업데이트해야 하고, 특히 대규모 업체들은 분기별로 BGP 위험완화 진행상황을 입증하는 구체적인 데이터를 추가로 연방통신위원회에 제출·공개해야 함

■ 배경

○ 연방통신위원회장 제시카 로젠워셀(Jessica Rosenworcel)은 기업 운영, 온라인 뱅킹, 원격의료 및 응급 서비스에 이르기까지 다양한 일상 활동에서 BGP에 대한 의존도가 높다고 언급

〈 경계 경로 프로토콜(BGP)의 역할 〉

경계 경로 프로토콜 (Border Gateway Protocol)	• 인터넷 네트워크 간 데이터 교환과 효율적 경로 선택(라우팅)을 가능하게 해주는 역할을 담당하여, **인터넷을 가능하게 하는 '접착제'**로 비유될 정도로 인터넷의 핵심 구성요소 - 1) 인터넷은 수만 개의 상호 연결된 독립적인 자율 시스템(Autonomous System, AS)으로 구성 - 2) 자율 시스템(AS)은 글로벌 도메인 간 라우팅 프로토콜인 BGP를 통해 상호 연결을 달성·유지 - 3) BGP는 AS 간에 도달가능한 정보(reachability information)들을 교환할 수 있도록 함

○ 그럼에도 BGP는 30년 전 학술 및 연구기관을 대상으로 설계되어, 독립적인 인터넷 네트워크간 트래픽 교환의 안전을 보장할 수 있는 ‘내장된 보안 기능’(intrinsic security features)이 부재

- 라우팅 시스템 공격자가 BGP 보안 취약점을 악용하여 인터넷 트래픽 흐름을 방해할 수 있어, 시민의 일상생활과 국가 주요기반시설 보안에도 악영향을 미칠 가능성이 제기됨

1 FCC, FCC PROPOSES REPORTING REQUIREMENTS TARGETED TO IMPROVING INTERNET ROUTING SECURITY, 2024.06.06.

○ 특히, 연방통신위원회는 국방부와 법무부 자료를 인용하여, 중국 통신회사가 BGP 취약점을 이용해 미국 인터넷 트래픽을 최소 6차례 잘못 라우팅했다고 밝히는 등 BGP 보안이 국가 안보와 관련된 사안임을 시사함

○ 또한 미국 국가사이버보안전략 실행계획(National Cybersecurity Strategy Implementation Plan)에서도 BGP 보안을 위한 주요 이행방안을 제시한 바 있음

- 국가사이버국장실(ONCD)에 BGP 보안 문제해결 기술을 포함, 안전한 인터넷 라우팅 기술 채택을 위한 로드맵 개발을 명시[2]

○ 최근 10년간 연방통신위원회는 BGP 보안취약점 개선을 위해 ▲민간이 포함된 자문위원회 운영, ▲인터넷 라우팅 보안 강화를 위한 질의서(Notice of Inquiry, NOI) 발표 등을 추진하였으며, 이번 잠점규정 예고안도 그러한 과정의 일환임

〈 연방통신위원회의 BGP 보안 개선을 위한 주요 활동 〉

구분	주요 내용
자문 위원회 구성	• 통신 업계의 이해관계자 및 기타 관련 분야의 특별고문으로 구성된 연방자문위원회인 **'통신 보안, 신뢰성 및 상호운용성 위원회(CSRIC)'** 운영 • 제3기, 제6기 위원회는 BGP와 관련된 문제와 리스크에 대해 논의하여, 리스크 완화 권장사항 및 모범사례 표준에 대해 권고 - **(3기 위원회)** 인터넷 네트워크 사업자가 인터넷 라우팅 레지스트리 항목이 정확하고 완전하며 최신 상태인지 확인하고, 네트워크 사업자가 인터넷 자원 및 라우팅 권한의 암호화 보안 데이터베이스를 제공하기 위한 표준 기반 접근법으로 **라우팅 인증(RPKI, Resource Public Key Infrastructure)[3] 사용 권고** - **(6기 위원회)** 3기 위원회 권고안을 기반으로 네트워크 사업자가 MANRS 표준[4](Mutually Agreed Norms for Routing Security) 및 인터넷 엔지니어링 태스크포스(IETF) 공통 모범사례 및 표준 지원을 제안하는 추가 지침 개발
인터넷 라우팅 보안 강화 질의서(NOI)	• BGP 리스크 대응책 후속 조치로 '**보안 인터넷 라우팅 질의서**(Secure Internet Routing NOI)' 발표 - BGP에 내재된 취약점으로부터 국가 통신 네트워크 및 기타 중요 인프라를 보호하고 강화하기 위해 연방통신위원회가 고려해야 할 조치에 대한 의견요청 - 3기, 6기 위원회에서 권장하는 보안조치와 네트워크 사업자가 업계에서 개발한 사용 가능한 BGP 보안 권장사항을 구현한 정도에 대한 의견요청

2 국가사이버보안전략 실행계획(NCSIP) Ver 2.0('24. 5.) 4.1.5. 주요 이해관계자와 협력하여 안전한 인터넷 라우팅 추진(Collaborate with key stakeholders to drive secure Internet routing)

3 라우팅 인증(RPKI)이란 인터넷주소자원 소유기관 및 IP주소, AS번호 등을 PKI(공개키 기반 암호화) 기반으로 전자서명 처리하여 해당 라우팅 정보의 무결성을 인증하는 것, [출처] 한국인터넷정보센터, https://한국인터넷정보센터.한국/jsp/resources/rpki.jsp 참고

4 인터넷 라우팅 기능의 보안 취약점을 개선하기 위해서 인터넷 소사이어티(ISOC)가 인터넷서비스 제공업체(ISP)와 협의하여 만든 표준, [출처] https://terms.tta.or.kr/dictionary/dictionaryView.do?subject=%EC%9D%B8%ED%84%B0%EB%84%B7+%EC%86%8C%EC%82%AC%EC%9D%B4%EC%96%B4%ED%8B%B0 참고

■ 주요내용

연방통신위원회는 BGP 보안 강화를 위한 사항을 ▲BGP 보안 리스크 관리계획 ▲BGP 라우팅 보안 정보(분기별 보고서) ▲BGP 계획 기밀 취급 등으로 구분하여 제시

① BGP 보안 리스크 관리계획

○ 특정 대규모 광대역 인터넷 액세스 서비스 제공업체[5](이하, 서비스 제공업체)가 라우팅 보안 위험관리 계획(BGP 계획)을 준비 및 유지하도록 요구할 것을 제안

- 연방통신위원회가 서비스 제공업체에 ▲라우팅 인증(RPKI)을 도입한 방식, ▲추후 RPKI 도입 계획을 요구하여 표준설정 프로세스에 대한 참여를 촉진할 수 있을 것으로 기대

- 서비스 제공업체가 ▲경로 출발지 유효성(Route Origin Validation, ROV) 필터링을 수행하는 정도와 ▲BGP 보안을 위한 다른 조치 방법을 증명하고, 이러한 계획을 매년 최신화하도록 요구

② BGP 보안 정보

○ **(분기별 보고서)** 연방통신위원회는 대규모 서비스 제공업체가 특정 데이터를 분기별로 제출하도록 요구

- 이를 통해, 연방통신위원회는 서비스 제공업체의 경로 출발지 승인(Route Origin Authorizations, ROA) 등록 및 유지 관리의 진행 상황을 측정하고, 서비스 제공업체의 BGP 계획 합리성을 평가

③ BGP 계획 기밀 취급

○ 연방통신위원회는 BGP 계획에 고도의 기밀 및 경쟁적으로 민감한 영업 정보가 포함될 수 있다고 판단하여, BGP 계획을 기밀로 취급할 것을 제안

- 연방통신위원회가 「정보공개법(FOIA)」[6]에 따른 BGP 계획 정보공개 요청을 받은 경우, 해당 정보공개 요청에 대해 서비스 제공업체가 이의를 제기할 수 있도록 보장

  · 연방통신위원회는 정보공개 이의제기 기한(10일)을 규정하고, 서비스 제공업체가 응답하지 않을 시 공개에 이의가 없는 것으로 간주

5 AT&T, Altice USA, Charter Communications, Comcast, Cox, Lumen Technologies, T-Mobile USA, Telephone & Data Systems(US Cellular 포함), Verizon Communications

6 Freedom of Information Act

■ 전망 및 시사점

○ 이번 잠정규정 예고문은 연방통신위원회에서 만장일치로 통과되었다는 점에서 인터넷 트래픽 라우팅의 핵심 역할을 하는 BGP 보안강화 의지를 보인 것으로 해석 가능

○ 일각에서는 연방통신위원회의 BGP 보안 계획이 실질적 규제보다 보고 요구사항 중심으로 제안되어, 대규모 서비스 제공업체의 부담을 완화할 수 있을 것이라는 평가

Reference

▪https://www.fcc.gov/document/fcc-proposes-internet-routing-security-reporting-requirements-0
▪https://www.telecomstechnews.com/news/2024/jun/07/fcc-moves-strengthen-internet-routing-security/
▪https://cyberscoop.com/fcc-moves-ahead-on-internet-routing-security-rules/

해외 입법 동향

미국 상원, 「AI 대중 인식 및 교육 캠페인 법안」 발의

미국 상원은 대중에 대한 AI 관련 지식 보급 등을 목적으로 하는 초당적 성격[1]의 「AI 대중 인식 및 교육 캠페인 법안」[2]을 발의 (2024. 6. 20.)

■ 개요

○ 동 법안은 상무부(Department of Commerce) 장관으로 하여금 AI 기술이 일상에 미치는 영향에 대한 교육 캠페인을 실시하도록 요구함

○ 해당 법안은 **AI 기술의 책임 있는 활용 촉진** 및 이와 **관련된 위험 최소화**를 주된 목표로 함

- AI 캠페인에 ▲AI 관련 개인의 법적 권리 증진, ▲AI가 생성한 미디어를 감지·구분할 수 있는 다양한 도구 및 수단 지원, ▲개인의 일상생활에 각종 AI 보급 촉진, ▲AI 관련 기술자에 대한 공공부문 취업 기회제공 등을 포함

○ 미국 상원 의회의 초당적 AI 실무그룹[3]이 약 1년간 검토한 'AI 로드맵 정책문서'[4]가 공개된 후, 그 중 일부 내용을 추진하기 위해 동 법안 발의

- 해당 정책문서는 AI 기술의 다면적인 기회 제공과 AI가 초래할 수 있는 위험을 해결하기 위한 포괄적 프레임워크를 제시

〈 AI 로드맵 주요 정책 우선순위 및 내용 〉

정책	주요내용
AI 혁신 촉진 (Promoting AI Innovation)	• 다양한 규모의 기업이 AI 혁신을 위해 경쟁할 수 있도록 자금 지원
연구·개발 투자 (Investment in Research and Development)	• 글로벌 경쟁력을 유지하고 기술 발전을 촉진하기 위해 AI 연구·개발에 자금을 우선 지원

1 공화당 상원의원 토드 영(Todd Young)과 민주당 상원의원 브라이언 샤츠(Brian Schatz)가 법안을 공동발의
2 Artificial Intelligence Public Awareness and Education Campaign Act (S. 4596)
3 법안 발의자인 토드 영(Todd Young) 공화당 상원의원을 비롯하여, 공화당 소속 마이크 라운즈(Mike Rounds) 상원의원, 민주당 소속 척 슈머(Chuck Schumer) 상원의원 및 마틴 하인리히(Martin Heinrich) 상원의원 등으로 구성
4 Driving U.S. Innovation in Artificial Intelligence: A Roadmap for Artificial Intelligence Policy in the United States Senate (2024. 5. 17)

정책	주요내용
인재 개발 (Workforce Development)	• AI 기반 경제에서 성공하는 데 필요한 기술을 근로자에게 제공하는 동시에 일자리 문제를 해결할 수 있는 교육 프로그램 시행
AI 법률, 지침의 개발 및 집행 (Development and Enforcement of AI Laws and Guidelines)	• 개인정보보호, 투명성, 편향성을 고려하는 등 AI 기술의 책임 있는 개발과 보급에 관한 '윤리 지침'을 수립하고 기존 법률의 집행을 보장
지식재산권 (Intellectual Property)	• AI를 통한 개인의 이름, 이미지, 초상권, 음성 등을 무단으로 사용하지 못하도록 별도의 보호 법률이 필요한지 여부 평가
선거/민주주의 - 대중 보호 (Elections/Democracy - Protecting the Public)	• '딥페이크'가 선거 콘텐츠에 악용되는 등 AI 기술이 사적인 영역에 악용되는 문제를 해결하고, AI가 콘텐츠 제작자에게 미치는 영향을 연구
프라이버시 및 책임 (Privacy and Liability)	• AI 시스템에 저장 및 사용되는 개인정보에 관한 보호정책을 모색하고, 이를 위해 「연방 개인정보보호법」[5] 추진에 대한 지지 표명
AI 관련 위험관리 (Managing AI-Related Risks)	• 위험평가, 평가 방법론, 메커니즘 등의 개발 및 표준화 지원
국가안보 및 사이버보안 (National and Cyber Security)	• 새로운 AI 기술을 활용하여 국가안보를 강화

■ 주요내용

○ **(AI 캠페인)** 상무부장관은 동 법의 시행일로부터 180일 이내에 국립표준기술연구소[6] 소장 등을 포함한 연방기관의 장과 협력하여 AI 교육 캠페인을 실시해야 함

- 상무부장관은 대중 인식 고취 및 교육을 위한 해당 캠페인 과정에서 다음 사항을 수행해야 함

구분	주요내용
핵심성과지표 결정 등	• AI 캠페인 효과를 평가하기 위한 핵심성과지표(KPI)[7] 결정 및 AI 캠페인 성공 여부를 측정하는데 있어 필요한 기본 데이터 획득
정보공유 및 접근성 촉진	• AI에 대한 최신 지식을 습득하고 AI 관련 법률에서 인격권을 증진하기 위하여, AI 관련 정보공유 및 접근성 촉진
	- AI와 관련된 새로운 기능 및 서비스에 관한 이해도 향상 - AI 관련 정책에 대한 정보 접근성 강화 - 머신러닝, 자연어 처리 등 최신 기술 발전 양상에 대한 인식 제고 - AI 시스템 작동 원리에 대한 투명성 요구권 및 AI가 초래한 피해에 대한 구제책 보장 - AI 시스템이 야기할 수 있는 차별에 대하여 공정한 처우를 받을 권리 보장
출처정보 감지 지원	• 디지털 미디어 관련 출처정보 감지를 위한 최적의 활동을 식별, 촉진 및 장려하기 위해 다양한 방법 도입
	- AI 캠페인 활동에 인간이 생성하거나 알고리즘이 생성 및 수정을 가한 콘텐츠(예: 딥페이크 및 챗봇 프로그램으로부터 생성된 콘텐츠)와 같은 디지털 미디어 포함 - 상기 미디어 콘텐츠 등을 탐지하거나 구분하기 위한 도구와 그 방법에 대한 자원 및 가이드 제공 - AI를 악용한 사기 행위에 특히 취약한 연령층을 파악하고, 해당 연령층에 AI 관련 사기 활동에 대해 알리고 이를 예방하기 위한 맞춤형 지원활동 수행

5 Federal data privacy law to protect personal information
6 National Institute of Standards and Technology, NIST

구분	주요내용
시민사회 지원	• 미국 시민의 일상생활과 밀접하게 연관된 AI에 대하여, 시민사회를 위한 다음과 같은 지원활동 수행
	- ▲텍스트 음성 변환 기능, ▲실시간 경로 예측, ▲문구 추천 기능과 같은 개인의 생산성을 향상시킬 수 있는 애플리케이션 보급 - 자동화된 의사결정, 사기 탐지, 금융 거래 등을 위한 상업용 애플리케이션 보급 - AI 개발, 배포 및 사용 경험이 있는 기술자 등을 위해 연방정부에서 일할 수 있는 취업 기회 등 제공

○ **(전문가 협의)** 상무부장관은 AI 캠페인 진행 과정에서 산업계, 학계 등 다양한 이해관계자와 협의해야 함

- 기업, 개발자, 배포자, 이용자 및 AI 관련 전문지식을 갖춘 커뮤니티 운영조직 등이 포함

○ **(보고)** 상무부장관은 AI 캠페인을 시작한 날로부터 1년 이내에 AI 캠페인 활동에 대한 보고서를 의회[8]에 제출해야 하며, 이때 보고서에 ▲AI 캠페인 효과를 평가하기 위해 활용된 핵심성과지표, ▲AI 캠페인 성과가 부진한 것으로 파악된 주요 분야에 대한 향후 후속조치를 포함해야 함

■ 전망 및 시사점

○ 동 법안은 상무부의 AI 관련 대중 캠페인을 통해 시민의 AI 도구 활용성을 높이고 해당 도구가 촉발할 수 있는 위험에 대한 대중의 인식을 제고하는 데에 긍정적 역할을 할 것으로 기대

- 공화당 Todd Young 상원의원은 개인이 AI 기술을 명확하게 인식하고, 각자의 일상생활에서 AI 활용을 극대화할 수 있도록 돕는 것이 그 어느 때보다 중요해졌다고 입법 취지를 밝힘

Reference

▪https://www.young.senate.gov/wp-content/uploads/Artificial-Intelligence-Public-Awareness-and-Education-Campaign-Act-.pdf
▪https://www.young.senate.gov/newsroom/press-releases/young-schatz-introduce-bill-to-raise-awareness-boost-public-trust-in-artificial-intelligence/
▪https://www.nextgov.com/artificial-intelligence/2024/06/bill-would-require-commerce-launch-ai-public-awareness-campaign/397553/
▪https://www.meritalk.com/articles/senate-bill-aims-to-boost-ai-awareness-education/
▪https://fedscoop.com/bipartisan-senate-bill-wants-commerce-secretary-to-raise-awareness-of-ai-jobs/
▪https://www.mayerbrown.com/en/insights/publications/2024/05/senate-ai-working-group-releases-roadmap-for-artificial-intelligence-policy

7 이니셔티브가 목표 달성에 효과적이었는지 여부를 측정할 수 있는 정량 지표를 뜻함
8 상원 상업, 과학, 교통위원회(Committee on Commerce, Science and Transportation of the Senate) 및 하원 과학, 우주, 기술위원회(Committee on Science, Space, and Technology of the House of Representatives)를 의미

해외 입법 동향

미국 상원, 「인터넷 애플리케이션 무결성 및 공개에 관한 법안」 발의

미국 상원은 해외 적대국으로부터 미국 내 데이터를 보호하기 위하여, 초당적 성격[1]의 「인터넷 애플리케이션 무결성 및 공개에 관한 법안[2]」을 발의 (2024. 6. 20.)

■ 개요 및 추진배경

○ **(배경)** 「해외 적대국으로부터 미국인 데이터 보호법」(Protecting Americans' Data from Adversaries Act, 이하 PADFA)이 발효되었고(2024. 6. 23.), 미국 상원은 적대국을 대상으로 한 인터넷 서비스 제공자의 의무를 규정한 「인터넷 애플리케이션 무결성 및 공개에 관한 법안」을 발의

- 「PADFA」는 '해외 적대국' 및 '민감 개인정보'의 종류를 규정하고, 데이터 브로커가 미국 국민의 민감 개인정보를 해외 적대국 등에 제공하지 못하도록 규제 강화

  · 또한, 「PADFA」는 바이든 행정부의 '미국인의 대량의 민감한 개인정보 및 미국정부 관련 정보에 대한 우려국가의 접근 방지에 관한 행정명령(EO 14117)'[3]보다 정의규정을 구체화

- 2023년 2월 하원에서 발의된 「인터넷 애플리케이션 무결성 및 공개에 관한 법안」(H.R. 784)은 중국만을 적대국으로 지정하고 있으나, 본 법안의 경우 적대국 범위를 확대(중국, 러시아, 북한, 이란)

〈 행정명령 14117과 「PADFA」 비교 〉

구분	행정명령 14117	「PADFA」
해외 적대국 관련 단체 (금지 적용대상)	• ▲우려 국가의 소유, 통제하에 있거나 관할권 또는 지시에 종속된 법인, ▲그러한 법인의 직원 또는 계약자인 외국인, ▲우려 국가의 직원 또는 계약자인 외국인, ▲우려 국가의 영토 관할권에 주로 거주하는 외국인	• 해외 적대국에 의해 통제받는 개인 또는 법인 – 해외 적대국에 소재하거나, 본사를 두고 있거나, 주요 사업장을 보유하고 있거나, 해외 적대국의 법률에 따라 조직된 법인 – 위 조건을 충족하는 외국 법인이 20% 이상의 지분을 직접 또는 간접적으로 소유하는 법인 – 위 조건을 충족하는 외국 법인의 통제 또는 지시를 받는 법인

1 공화당 소속 Chuch Grassley 상원의원과 민주당 소속 Catherine Cortez Masto 상원의원이 공동으로 법안을 발의
2 Internet Application Integrity and Disclosure Act (S. 4598)
3 Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern (EO 14117)

구분	행정명령 14117	「PADFA」
해외 적대국	• (근거) 행정명령 13873에 따른 잠정규정 예고문 • (표현) 우려 국가(Countries of Concern) • (해당국) 중국, 러시아, 쿠바, 이란, 베네수엘라, 북한	• (근거) Title 10 U.S.C. § 4872 • (표현) 해외 적대국(foreign adversary country) • (해당국) 중국, 북한 러시아, 이란
민감 개인정보	• ▲개인식별정보, ▲지리적 위치정보, ▲생체인식 정보, ▲인간 게놈정보, ▲ 인간 오믹정보, ▲개인 건강정보, ▲개인 금융정보 또는 ▲이 정보들의 모든 조합을 의미 ※ [2024년 3월] 인터넷·정보보호 법제동향 제198호 참고	• 단독으로 또는 다른 데이터와 결합하여 개인 또는 장치를 식별하거나, 연결하거나, 합리적으로 연결할 수 있는 모든 민감정보 • 민감정보(sensitive data) 종류 – 사회보장번호, 여권번호, 운전면허증 번호 등 정부에서 발급한 식별정보 – 개인의 과거, 현재 또는 미래의 신체 건강, 정신 건강, 장애, 진단, 건강상태 또는 치료를 설명하거나 드러내는 모든 정보 – 계좌 번호, 직불 카드 번호, 신용카드 번호 또는 개인의 소득 수준이나 계좌 잔고를 설명하거나 드러내는 정보 – 생체 인식정보 – 유전정보 – 정확한 지리적 위치정보 – 음성 메일, 이메일, 문자, 쪽지, 메일, 음성 통신, 영상 통신 등 개인의 사적인 통신 또는 그러한 통신의 당사자를 식별하거나 통신의 전송과 관련된 정보 – 계정 또는 디바이스 로그인 자격증명 또는 디바이스의 보안 또는 액세스 코드 – 개인의 성행위를 식별하는 정보 – 캘린더 정보, 주소록 정보, 전화 또는 문자 로그, 사진, 오디오 녹음 또는 동영상 – 개인의 알몸 또는 속옷을 입은 사적인 부위를 보여주는 사진, 영화, 비디오 녹화물 또는 기타 유사한 매체 – 개인이 요청하거나 선택한 동영상 콘텐츠가 드러나는 정보 – 만 17세 미만의 개인에 관한 정보 – 개인의 인종, 피부색, 민족 또는 종교 관련 정보 – 웹사이트 또는 온라인 서비스에서 시간 경과에 따른 개인의 온라인 활동을 식별하는 정보 – 군대 구성원으로서 개인의 신분을 드러내는 정보 – 데이터 브로커가 나열된 데이터 유형을 식별할 목적으로 해외 적대국 또는 해외 적대국이 통제하는 단체에 판매, 라이선스, 대여, 거래, 양도, 공개, 액세스 제공 또는 기타 방식으로 제공하는 기타 모든 데이터

■ 주요내용

‘해외 적대국(foreign adversary country)’의 ‘적용대상 서비스(covered service)’ 관련 정보공개 의무화

○ **(목적)** 해외 적대국과 관련된 **웹사이트나 앱을 운영, 판매, 배포하는 자** 또는 이들로부터 **수집한 정보를 해당 국가에 저장하는 자**가 이용자에게 이 사실을 공개하기 위함

○ **(정의)** 동 법은 주요 용어를 다음과 같이 정의함

구분	주요내용
적용대상 서비스 (Coverd Service)	• 다음과 같은 인터넷 웹사이트 또는 모바일 애플리케이션을 의미 - 해외 적대국, 해외 적대국 소유 기업, 또는 해외 적대국에 위치한 비(非) 국영기업이 전체 또는 부분적으로 소유한 경우 - 해당 웹사이트나 앱에서 수집한 정보를 해외 적대국에 저장하고 유지하는 경우
해외 적대국 (Foreign Adversary Country)	• 10 U.S. Code § 4872 제d항제2호[4]에 명시된 국가 - 중국, 러시아, 북한, 이란
개인 (Individual)	• 미국에 거주하는 자연인
해외 적대국에 위치한 비(非) 국영기업 (Non-State-Owned Entity Located In a Foreign Adversary Country)	• 다음과 같은 기업을 의미 - 해외 적대국의 정부 조직에 의해 통제되는 기업 - 해외 적대국의 법률에 따라 조직된 기업

○ **(공개 요구사항)** 이 법 제정 1년 후부터, 대상 서비스를 소유, 관리 또는 배포하는 모든 자는 해당 서비스를 다운로드하거나 사용하는 개인에게 다음 사항을 명확하고 명시적으로 공개해야 함

공개 사항
- 대상 서비스가 해외 적대국, 해외 적대국 소유 기업, 또는 해외 적대국에 위치한 비(非) 국영기업에 의해 전체 또는 부분적으로 소유되었는지 여부 - 대상 서비스에서 수집된 정보가 해외 적대국에 저장되고 유지되는지 여부 - 해외 적대국 또는 해외 적대국 소유기업이 해당 정보에 접근할 수 있는지 여부

○ **(집행)** 동 법의 위반은 「연방거래위원회법[5]」 제18조제a항제1호B목에 따른 ‘불공정하거나 기만적인 행위 또는 관행을 정의하는 규칙’(15 U.S. Code § 57a(a)(1)(B)) 위반으로 간주

- 연방거래위원회는 「연방거래위원회법」의 모든 적용 가능한 조건과 조항이 동 법에 통합되어 일부가 된 것처럼 동일한 방식, 동일한 수단, 그리고 동일한 관할권, 권한, 의무로 동 법을 집행해야 함

- 단, 동 법의 어떠한 내용도 다른 법 조항에 따른 연방거래위원회의 권한을 제한하는 것으로 해석되어서는 안 됨

4 10 U.S. Code § 4872 - Acquisition of sensitive materials from non-allied foreign nations: prohibition
5 Federal Trade Commission Act

■ 전망 및 시사점

○ **(데이터 보호 및 주권 강화)** 「인터넷 애플리케이션 무결성 및 공개에 관한 법안」은 미국 정부의 개인정보보호와 데이터 주권 강화 의지를 표현

- 공화당 Chuck Grassley 상원의원은 국가안보와 개인정보보호를 위해, 적대국 통제하에 있는 웹사이트와 애플리케이션 정보를 공개하도록 하는 법안을 발의한 것이라고 입법취지를 밝힘

- '해외 적대국'으로 지정된 국가들과 해외 적대국의 통제하에 있는 단체들에 대한 규제를 강화하며, 이는 추후 미국의 데이터 주권 강화로 이어질 것으로 예상

○ **(기업의 투명성)** 해당 법안은 특정 국가와 관련된 웹사이트나 앱의 소유권, 데이터 저장 위치 등에 대한 정보공개를 규율하여 외국 기술 기업들에 높은 투명성을 요구

○ **(국제 관계)** 미국과 '해외 적대국' 간의 기술 및 데이터 관련 갈등을 심화시킬 수 있으며, 국제 관계에 영향을 미칠 가능성이 클 것으로 예측

- 국가 간 데이터 관련 갈등 심화는 글로벌 데이터 경제와 국제 데이터 거버넌스 체계에 변화를 가져올 수 있으며, 각국의 데이터 정책에도 영향을 미칠 것으로 예상

Reference

▪https://www.grassley.senate.gov/news/news-releases/grassley-cortez-masto-work-to-protect-americans-data
▪https://www.congress.gov/bill/118th-congress/house-bill/7520/text
▪https://www.grassley.senate.gov/imo/media/doc/internet_application_integrity_and_disclosure_act.pdf
▪https://www.govinfo.gov/app/details/BILLS-118hr784rh/summary
▪https://www.radioiowa.com/2024/06/24/grassley-bill-aims-to-force-adversaries-to-disclose-ownership-of-apps-websites/

해외 입법 동향

미국 상원, 공중보건 분야 사이버보안 개선을 위한 「의료 사이버보안법안」 발의

미국 상원의원 Jacky Rosen(민주당), Todd Young(공화당), Angus King(무소속)은 의료 분야의 사이버보안을 강화할 수 있는 초당적 성격의 「의료 사이버보안법안[1]」을 발의 (2024. 7. 11.)

■ 개요 및 추진배경

○ 동 법은 사이버보안 및 인프라 보안청(Cybersecurity and Infrastructure Security Agency, CISA)이 보건복지부(Department of Health and Human Services, HHS)와 협력하여, 비(非) 연방기관들을 위한 사이버위협 지표 및 적절한 방어 조치에 관한 자원을 개발하도록 규정

- CISA 내에 보건복지부와 소통하는 연락 담당자를 두어, 사이버보안 사고 발생 시 정부 대응을 조율하고 의료 및 공중보건(Healthcare and Public Health, HPH) 부문 기관에 대하여 지원하도록 함

○ 최근 급증하는 의료기관에 대한 사이버 공격에 대응하여 의료 및 공중보건 부문의 사이버보안 강화 조치의 필요성이 대두

- 보건복지부에 보고된 데이터에 따르면, 2018년부터 2022년까지 의료 시설 정보 시스템에 대한 대규모 사이버 침해가 93% 증가

- 또한, 2022년 한 해에만 「건강보험 양도 및 책임에 관한 법률(HIPAA)」[2]에서 정의한 적용대상 기관에서 500명 이상에게 영향을 미친 정보 유출 사례가 626건 발생했으며, 보건복지부 민권국[3]의 데이터에 따르면 그 결과 약 4,200만 명의 건강정보가 유출

1 Healthcare Cybersecurity Act of 2024 (S.4697)
2 Health Insurance Portability and Accountability Act of 1996, Public Law 104-191
3 Office for Civil Rights of the Department(OCR)로, 미국 내에서 의료 서비스 이용 시 공정성을 보장하고, 개인의 민감한 의료 정보를 보호하는 중요한 역할을 수행

〈 법안 구성 및 핵심내용 〉

구분	핵심내용
법안 제정 배경 (제3조)	• 최근 의료 시스템의 사이버공격 사례와 그 결과로 발생하는 잠재적 위험, 비용 증가, 환자 치료에 미치는 부정적인 영향 언급
기관 협력 (제4조)	• CISA와 보건복지부가 협력하여 의료 부문 사이버보안을 강화하는 방안을 수립 - 이를 위해 보건복지부 내에 CISA와의 협력 및 사이버사고 대응을 위한 연락 담당자를 지정
의료자산 소유자 등 교육 (제5조)	• CISA는 의료자산 소유자 및 운영자에게 사이버보안 위험 및 완화 전략에 대한 교육을 제공 - 교육에는 최신 위협정보, 위협대응 및 위험관리 방법 등이 포함
부문별 계획 (제6조)	• CISA와 보건복지부는 사이버보안 계획을 업데이트하여, 특히 농촌 및 중소규모 의료 제공자들이 직면한 특정 도전 과제를 포함하도록 하고, 이 계획은 모범사례와 위험완화 전략을 포함
고위험 자산 식별 (제7조)	• CISA는 높은 사이버보안 위험을 가진 의료자산을 식별하는 기준과 방법론을 개발해야 함 - 고위험 의료자산에 대한 자원 할당의 우선순위를 지정하기 위함
보고서 제출 (제6조)	• CISA는 의료 부문에 제공된 사이버보안 지원 및 활동에 대해 연례 보고서를 의회에 제출 - 보고서에는 제공된 기술적 지원, 교육, 및 개선된 사이버보안 대응 능력 등에 대해 다룸

■ 주요내용

○ **(정의)** 주요 용어를 다음과 같이 정의함(제2조)

구분	주요내용
적용대상 자산 (Covered Asset)	• 기술, 서비스 및 유틸리티(Utility)를 포함한 의료 및 공중보건 부문의 자산을 의미함
사이버안보 조정관 (Cybersecurity State Coordinator)	• 「2002년 국토안보법(Homeland Security Act of 2002)」 제2217조제(a)항*에 따라 임명된 사이버안보 조정관을 의미함 * CISA 청장은 적절한 사이버보안 자격과 전문지식을 갖춘 직원을 각 주에 있는 기관에 임명해야 하며, 이들은 사이버안보 조정관의 역할을 수행함
의료 및 공중보건 부문 (Healthcare and Public Health Sector)	• 대통령 정책지침 21호(2013년 2월 12일, 주요기반시설 보안 및 복원력 관련)에 명시된 의료 및 공공보건 부문을 의미함
정보공유 및 분석조직 (Information Sharing and Analysis Organizations)	• 「2002년 국토안보법(Homeland Security Act of 2002)」 제2200조*에 명시된 정보공유 및 분석조직을 의미함 * 공공 또는 민간부문 조직이 주요기반시설 관련 보안 문제 및 상호 의존성을 더 잘 이해하기 위하여 만들거나 고용한 공식 또는 비공식 단체 등을 의미함

○ **(기관 협력)** CISA는 보건복지부와 협력하여 의료 및 공중보건 분야의 사이버보안을 개선

- CISA 청장은 보건복지부 장관과 협력하여, 사이버보안 자격 및 전문지식을 보유한 전문가를 보건복지부에 연락 담당자로 임명

연락 담당자의 의무
• 적용대상 자산의 소유자 및 운영자에게 사이버보안 개선과 관련된 기술 지원, 정보 및 모범사례 제공
• 사이버보안 문제를 조정하기 위하여, CISA와 보건복지부를 연결하는 주요 담당자 역할 수행
• 사이버보안 계획의 이행 및 집행을 지원하고 사이버보안 계획에 대한 업데이트 개발을 지원
• 사이버보안 위험에 대한 이해와 사이버보안 사고에 대한 상황인식을 개선하기 위해 사이버위협 정보공유 촉진
• 의료 및 공중보건 부문 자산의 소유자 및 운영자를 위한 교육을 진행

연락 담당자의 의무
• 의료 및 공중보건 부문 내 사이버보안 사고 발생 시 CISA와 보건복지부 간의 조정 역할 수행 • 의료 및 공중보건 부문의 사이버보안 개선을 위하여 보건복지부 장관이 필요하다고 판단하는 기타 의무 수행

- 연락 담당자는 CISA 청장 및 보건복지부 장관과 협의하여, CISA와 보건복지부 간 사이버보안 조정 개선 활동에 대한 보고서를 법 제정 후 18개월 이내에 작성하여 의회[4]에 제출

- CISA는 각 기관[5]과 협력하여 의료 및 공중보건 부문 단체의 필요에 맞는 제품(Product) 개발, 그리고 사이버위협 지표 및 적절한 방어조치와 관련된 정보공유 진행

○ **(적용대상 자산 소유자 등을 위한 교육)** CISA의 사이버안보 자문관[6] 및 사이버안보 조정관[7]은 연락 담당자 및 민간부문 의료 전문가와 협력하여, 적용대상 자산 소유자 및 운영자에게 교육을 제공

- ▲의료 및 공중보건 부문의 위험, ▲적용대상 자산에 대한 사이버보안 위험, ▲의료 및 공중보건 부문의 정보 시스템에 대한 위험 완화방법 등에 대한 사이버보안 교육을 의미

○ **(의료 및 공중보건 부문별 계획 수립)** 보건복지부 장관은 CISA 청장과 협력하여 동 법의 시행일로부터 1년 이내에 다음 사항을 포함하는 사이버보안 계획을 수립

사이버보안 계획 수립
• 식별된 사이버보안 위험이 적용대상 자산(농촌 및 중소규모 대상 의료자산에 대한 영향을 포함)에 구체적으로 어떤 영향을 미치는지에 대한 분석
• 적용대상 자산의 소유자와 운영자가 직면한 문제에 대한 평가 – ▲적용대상 자산이 소유, 임대 또는 의존하는 업데이트된 정보 시스템 보안, ▲적용대산 자산이 소유, 임대 또는 의존하는 의료기기 또는 장비에 대한 보안, ▲민감한 환자 건강정보 및 전자 건강기록 보안에 대한 평가 – 사이버보안 프로토콜 구현에 대한 평가 – 환자 치료에 대한 접근성, 환자 치료의 질, 의료 서비스 제공의 적시성 및 건강에 미치는 영향을 포함한 데이터 침해 또는 사이버보안 공격에 대한 대응에 대한 평가
• 데이터 침해 또는 사이버보안 공격 이전, 도중, 이후에 해당 기관에 훈련된 사이버안보 자문관 및 사이버안보 조정관을 배치하기 위한 모범사례 평가
• 농촌 및 중소규모의 적용대상 자산에서 발생하는 의료 및 공중보건 부문 사이버보안 인력부족에 대한 평가
• CISA와 보건복지부가 해당 적용대상 자산의 소유자와 운영자에게 사이버보안 권장사항 및 도구를 전달하고 배포할 수 있는 접근 가능하고 시의적절한 방법에 대한 평가

- 보건복지부 장관은 동 법의 제정일로부터 120일 이내에 CISA 청장과 협의하여 계획 수립에 관한 보고서를 의회에 제공해야 함

4 상원의 보건·교육·노동 및 연금위원회, 재정위원회, 국토안보 및 정부업무 위원회와 하원의 에너지 및 상업위원회, 세입위원회, 국토안보위원회
5 정보공유 및 분석 조직(ISAOs), 정보공유 및 분석센터, 부문 조정 협의회, 국무부가 관리하는 프로그램을 통해 공유되는 정보를 받는 비(非)연방기관을 의미
6 Cyber Security Advisors
7 Cybersecurity State Coordinators

○ **(고위험 자산 식별 및 관리)** CISA 청장은 동 법 시행일로부터 90일 이내에 고위험 적용대상 자산을 지정하기 위한 객관적 기준을 설정하고 위험평가 방법론을 수립해야 함

- 보건복지부 장관은 고위험 적용대상 자산으로 결정된 각 대상자산의 소유자 및 운영자 목록을 작성하고 2년마다 검토 및 업데이트하며, 변경사항을 의회에 통지해야 함

- 식별된 고위험 적용대상 자산 목록은 보건복지부가 사이버 복원력 강화를 위한 자원 할당의 우선순위를 지정하는 데 사용

■ 전망 및 시사점

○ CISA와 보건복지부 간의 협력 증진을 통해, 의료 시스템 보안이 체계적으로 개선되고 사이버위협 대응 능력이 향상될 것으로 예상

- 의료자산 소유자 및 운영자에게 제공되는 사이버보안 교육이 강화되어, 의료 서비스 제공자의 사이버보안 역량이 향상될 것으로 기대

○ 농촌 지역 및 중소규모 의료 서비스 제공자들에게 기술 자문, 재정, 교육 등 지원이 강화됨으로써 사이버보안 취약점을 완화하고, 해당 기관들이 효과적으로 보안 체계를 구축할 수 있도록 함

Reference

▪https://www.rosen.senate.gov/2024/07/11/rosen-young-king-introduce-bipartisan-bill-to-improve-cybersecurity-in-health-care-public-health/
▪https://www.congress.gov/bill/118th-congress/senate-bill/4697/text
▪https://www.hipaajournal.com/healthcare-cybersecurity-act-of-2024/

해외 입법 동향

미국, 「연방 사이버보안 규정 간소화 법안」 상원 상임위원회 통과

사이버보안 규제 체제 간 불일치 및 중복성을 최소화하기 위한 「연방 사이버보안 규정 간소화 법안」[8]이 상원의 국토안보·정무위원회[9]를 통과 (2024. 7. 31.)

■ 개요

○ 2024년 7월 8일, 게리 피터스(Gary Peters) 민주당 상원의원과 제임스 랭크포드(James Lankford) 공화당 상원의원은 사이버보안 규제 체제(regulatory regimes)간 조화를 강조하는 초당적 성격의 동 법안을 공동발의

○ 동 법안은 미국 백악관 **국가사이버국장실**(Office of the National Cyber Director) 산하에 **기관 간 사이버보안 요구사항을 조율하는 규제조화위원회(Harmonization Committee)**를 구성하도록 함

■ 주요내용

○ **(정의)** 동 법안은 주요 용어를 다음과 같이 정의함

구분	주요내용
사이버보안 요구사항 (Cybersecurity Requirement)	• 정보보안, 정보기술, 사이버보안, 사이버위험 또는 복원력과 관련된 규정, 지침, 공지 또는 시험 등을 포함한 **행정적, 기술적 또는 물리적 보호조치, 요구사항 또는 감독 활동**
조화 (Harmonization)	• 규제기관에서 발표한 사이버보안 요구사항을 다음과 같이 구성하도록 조율하는 절차 – 정보보안 또는 사이버보안과 관련된 신규 또는 진화하는 위험을 해결하기 위해 주기적으로 업데이트될 수 있는, 여러 부문에 걸쳐 적용되는 최소한의 공통 요구사항 – 상기 최소한의 요구사항으로 적절히 해결되지 않는 부문별 위험을 해결하는 데 필요한 부문별 요구사항 – 적절한 경우 각 해당 부문 또는 유사 부문의 기타 요구사항과 실질적으로 비슷한 부문별 요구사항
규제기관 (Regulatory Agency)	• ▲의무적인 사이버보안 요구사항을 발행하거나 집행할 법적 권한이 있는 모든 독립 규제기관, ▲사이버보안 요구사항을 발행하거나 집행할 법적 권한이 있는 기타 기관
독립 규제기관 (Independent Regulatory Agency)	• 「미국연방법전」 제44편 제3502조 제5항에 열거된 기관*[10] * 연방준비제도이사회(Board of Governors of the Federal Reserve System), 소비자제품안전위원회(Consumer Product Safety Commission), 연방통신위원회(Federal Communications Commission) 등

8 Streamlining Federal Cybersecurity Regulations Act (S. 4630)
9 Committee on Homeland Security and Governmental Affairs of the Senate
10 주로 연방 행정부 외부에 설립된 기관으로, 이러한 기관은 행정부 내 상위부처에 보고할 의무가 없고 행정부로부터 일정 수준의 독립성이 보장됨

구분	주요내용
관계 위원회 (Appropriate Congressional Committees)	- 상원 국토안보·정무위원회(Committee on Homeland Security and Governmental Affairs of the Senate) - 하원 감독·책임위원회(Committee on Oversight and Accountability of the House of Representatives) - 규제기관의 활동을 담당하는 의회 위원회 - 규제기관이 규제하는 부문에 대하여, 부문별 위험관리 기관(Sector Risk Management Agency)의 활동을 담당하는 의회 위원회
부문별 위험관리 기관 (Sector Risk Management Agency)	• 「미국연방법전」 제6편 제650조의 정의*를 준용 * 법률이나 대통령 지시에 따라 지정된 연방부서 또는 기관으로서 ▲각 부문에 대한 제도적 지식과 전문성을 제공하고, ▲모든 위험 환경에서 주요기반시설 부문의 프로그램 및 관련 활동을 주도, 촉진 또는 지원할 책임이 있으며, ▲연방 부서와 협력하여 해당 부문의 모든 위험 환경을 관리할 책임이 있는 기관

○ **(규제조화위원회 설립)** 국가사이버국장(National Cyber Director)은 미국 내 적용되는 사이버보안 요구사항 간 불일치 및 중복을 해소하고 조율하기 위해 규제조화위원회(Harmonization Committee)를 설립해야 함

- (구성원) 규제조화위원회는 ▲국가사이버국장 (규제조화위원회 의장(Chair)직 수행) ▲각 규제기관장(Head of each regulatory agency) ▲관리예산국 정보 및 규제 사무국 책임자(Head of the Office of Information and Regulatory Affairs of the Office of Management and Budget) ▲규제조화위원회 의장이 결정하는 기타 관계기관의 장으로 구성됨

- (명단 유지 등) 규제조화위원회는 소속된 기관의 명단을 공개된 웹사이트에 유지 및 제공해야 함

○ **(규제조화위원회 역할)** 규제조화위원회는 다음과 같은 역할을 수행

구분	주요내용
헌장(Charter)	• ▲규제조화위원회의 절차 및 규칙 ▲규제조화위원회의 목적 및 범위, 기타 필요 항목 등을 담은 헌장을 작성하여 의회에 제출하고 대중에게 공개해야 함
조정을 위한 규제 프레임워크	• 규제조화위원회는 동 법 제정일로부터 1년 이내에 각 규제기관의 사이버보안 요구사항을 조화롭게 조정하기 위해 규제 프레임워크를 개발해야 함 - 복수의 규제기관으로부터 규제를 받는 조직의 정보보안 또는 사이버보안 관련 최소 요구사항에 대한 상호 규정준수 메커니즘 수립 - 과도하게 부담이 되거나 일관성이 없거나 모순되는 사이버보안 요구사항 식별 - 일관성이 없거나 모순되는 사이버보안 요구사항을 해결하기 위해 규정 등 업데이트 • 규제조화위원회는 규제 프레임워크 개발이 완료되면 연방관보(Federal Register)에 해당 규제 프레임워크를 공표해야 함
파일럿 프로그램 운영	• 규제조화위원회가 선정한 최소 세 곳 이상의 규제기관은 상기 수립된 규제 프레임워크를 구현하기 위해 사이버보안 요구사항에 대한 파일럿 프로그램을 수행해야 함 - (자발적 참여) 규제조화위원회는 프로그램 참여와 관련하여 **규제기관**의 동의를 받아야 하며, **규제대상 조직** 또한 파일럿 프로그램의 참여가 자발적이어야 함 - (사이버보안 요구사항 선정 시 유의점) ▲파일럿 프로그램에서 선정되는 사이버보안 요구사항 중 적어도 두 개 이상은 동일 규제대상 기업에 공통적으로 적용되어야 하며[11], ▲해당 사이버보안 요구사항 간 정보보안 또는 사이버보안 측면에서 서로 매우 유사하거나 관련성이 있어야 함

○ **(보고서 제출)** 규제조화위원회는 의회의 '관계 위원회'에 다음과 같은 보고서 제출 의무를 부담

구분	주요내용
연례보고서	• 동 법 제정일로부터 12개월 이내 및 그 이후 매년 다음을 포함한 보고서를 제출해야 함 - 회원 참여 - 개발된 규제 프레임워크에 따른 사이버보안 요구사항 적용 등
파일럿 프로그램 운영보고서	• 파일럿 프로그램 시작일로부터 12개월 이내에 다음을 포함한 보고서를 제출해야 함 - 해당 프로그램에서 선택된 사이버보안 요구사항(선택된 이유 포함) - 프로그램을 통해 얻은 정보 - 프로그램 운영 중 발생한 애로사항 - 프로그램을 다른 조직 및 사이버보안 요구사항으로 확대하는 가능성에 대한 평가

○ **(사고보고 관련 업데이트)** 사이버보안 및 인프라 보안청(Cybersecurity and infrastructure Security Agency, CISA)장(이하 CISA 청장) 및 국토안보부(Secretary of Homeland Security) 장관은 동 법 제정일로부터 늦어도 180일 이내에 (그 후 최소한 180일마다) ▲합의각서, ▲사이버사고 보고위원회 사항을 의회의 '관계 위원회'에 제공해야 함

구분	주요내용
합의각서 관련	• CISA 청장은 기관 간 합의각서(Memoranda of agreement)의 개발 및 이행에 대한 최신 현황[12]을 관계 위원회에 제공해야 함
사이버사고 보고위원회 관련	• 국토안보부장관은 사이버사고 보고위원회(Cyber Incident Reporting Council)[13]의 성과 등에 대한 최신 현황을 각 관계 위원회에 제공해야 함

■ 전망 및 시사점

○ 미국은 국가사이버보안 전략실행계획(NCSIP, '23.7 발표)의 전략목표 중 하나[14]로 '사이버 규제조화에 대한 이티셔티브 수립[15](1.1.1 Establish an initiative on cyber regulatory harmonization)'을 제시하는 등 국가 안보와 공공의 안전을 위하여 사이버보안 규제조화의 중요성을 강조

○ 동 법안은 그간 업계에서 제기되었던 사이버사고 보고 기한 및 기타 절차의 상호 불일치 및 비효율성에 대한 부담감 등 규제관련 민원사항을 해소하기 위해 노력했다는 점에서 긍정적으로 평가

11 예컨대, 파일럿 프로그램에서 사이버보안 요구사항으로서 A요건, B요건, C요건 등 세 개의 요구사항이 선정되었다고 가정하고 규제조화위원회가 규제기관 선정 시 X기관, Y기관, Z기관 등 세 곳의 기관을 선정했다고 가정한다면, A~C 요건 중 적어도 두 개의 요건이 X기관, Y기관, Z기관 각각에 중첩적으로 적용되도록 하여, 요구사항 중첩 적용 시 요구사항 간의 충돌 여부를 파악해 볼 수 있도록 해야 함

12 「2022년 주요 기반시설 사이버사고 보고법」(Cyber Incident Reporting for Critical Infrastructure Act of 2022) 제104조 제(a)항 제(5)호에서 규정

13 「2002년 국토안보법」(Homeland Security Act of 2002) 제2246조에 따라 설립

14 Strategic Objective 1.1 : Establish Cybersecurity Requirements to Support National Security and Public Safety

15 (이니셔티브 1.1.1) Establish an initiative on cyber regulatory harmonization

○ 동 법안이 법률로 제정될 경우 사이버보안 관련 규제 간 일관성 확보를 통해 보다 관리가 용이한 규제환경이 조성될 것으로 기대

- 동 법안은 7월 31일 상원 상임위원회를 통과함으로써 상원 본회의 의결을 앞두고 있으며, 상원 본회의에서 가결 후 하원으로 회부되어 하원의 법안 심의 절차를 단계별로 밟게 될 예정

Reference

- https://www.congress.gov/bill/118th-congress/senate-bill/4630
- https://www.nextgov.com/cybersecurity/2024/07/senate-panel-advances-cyber-regulatory-harmonization-bill/398478/
- https://solondais.fr/2024/07/11/news202917/the-balance-act-streamlining-federal-cybersecurity-laws/
- https://cyberscoop.com/senate-homeland-security-streamlining-cyber-regulations-bills/
- https://cyberscoop.com/cybersecurity-regulations-harmonization-federal-agencies-senate-bill/
- https://www.centraleyes.com/balancing-act-streamlining-federal-cybersecurity-regulations/

해외 입법 동향

미국 FCC,「정치광고에서의 AI 생성 콘텐츠 공개 및 투명성에 관한 잠정규정 예고문」발표

미국 연방통신위원회(FCC)는 정치광고에서 AI가 생성한 콘텐츠의 공개 및 투명성에 관한 잠정규정 예고문(NPRM)[1]에 대한 의견수렴을 진행 (2024. 8. 5. ~ 9. 19.)

■ 개요 및 추진배경

○ AI 기술 발전에 따라, 해당 기술을 악용하여 생성된 가짜 목소리와 이미지(소위 '딥페이크')가 유권자에게 기만적이거나 오해의 소지가 있는 사기성 정보를 제공할 위험성 대두

- 뉴햄프셔주에서 치러진 민주당 대통령 후보 예비경선에서 수천 명의 유권자가 AI가 생성한 음성메시지[2]를 받았고, 플로리다 주지사 선거에서는 AI 조작 이미지 유포[3] 등의 사례 발생

- 절반 이상의 주[4]에서 AI와 딥페이크 기술 규제법을 제정했으나 일관성이 부족하여 연방 차원의 규정을 통해 통일성과 안정성을 제고할 필요성 증대

■ 주요내용

○ FCC는 선거 후보자가 정치광고에서 AI를 활용할 경우 특정 커뮤니티에 최적화된 광고를 쉽게 만들 수 있는 등 유익한 수단이 될 수 있음을 인정하고, **정치광고에 AI 사용을 허용**

- 단, **TV/라디오 정치광고**에서 **AI가 생성한 콘텐츠를 사용할 경우, 이를 공개**하도록 규율하여 시청자로 하여금 정치광고를 스스로 평가할 수 있게 함

○ **(AI 생성 콘텐츠)** FCC는 'AI 생성 콘텐츠'에 대해 정의하고, 이에 대한 의견을 요청

1 Disclosure and Transparaency of Artificial Intelligence-Generated Content in Political Advertisements
2 AI 기술을 악용하여 바이든 대통령의 목소리를 사칭한 뒤 유권자들에게 투표하지 말 것을 지시
3 론 드산티스(Ron DeSantis) 주지사 선거캠프가 AI로 조작된 트럼프 전 대통령의 가짜 이미지를 유포
4 캘리포니아, 아이다호, 인디애나, 미시간, 미네소타, 뉴멕시코, 오리건, 텍사스, 유타, 워싱턴, 위스콘신 등 11개 주가 정치광고 및 기타 캠페인에서 AI가 생성한 '딥페이크'를 규제하는 법안을 제정하는 등 28개의 주에서 유사한 법안이 검토 중

〈 AI 생성 콘텐츠의 정의 〉

구분	주요내용
AI 생성 콘텐츠	• 컴퓨터 기술 또는 기계 기반 시스템을 사용하여 생성된 이미지, 오디오 또는 비디오 • 개인의 외모, 음성, 행동, 또는 사건, 상황, 환경을 묘사하는 것 • 특히 인간의 목소리처럼 들리는 AI 생성 음성과 인간 배우처럼 보이는 AI 생성 배우를 포함

○ **(적용대상)** TV/라디오 방송국, 케이블 운영자, 직접방송 위성(Direct Broadcast Satellite, DBS) 공급자, 자주방송(自主放送, Origination Programming)[5]에 참여하는 '위성 디지털 오디오 라디오 서비스(Satellite Digital Audio Radio Service, SDARS)' 라이선스 소지자, 「통신법」 제325조제C항[6]에 따라 허가받은 자(permit holders)[7]에게 적용

○ **(AI 콘텐츠 확인)** FCC는 정치광고를 방영하는 방송국으로 하여금, 해당 광고에 AI 생성 콘텐츠가 포함되었는지 여부를 확인하도록 요구함

- **방송국은** 방송시간 구매를 요청하는 개인 또는 단체에게 **AI 생성 콘텐츠 포함 여부를 문의**하고 AI 생성 콘텐츠가 포함된 정치광고에 대해 **방송 중 공개가 필요하다는 사실을 알려야 함**

○ **(AI 콘텐츠 포함여부 공개)** FCC는 방송국에서 AI 생성 콘텐츠가 포함된 정치광고를 방영할 경우, 해당 광고에 AI 생성 콘텐츠가 포함되어 있음을 공지하도록 요구

구분	주요내용
TV	- (구두 안내) 명확하고 적절한 속도의 목소리로, "다음 메시지에는 AI를 통해 전체 또는 부분적으로 생성된 정보가 포함되어 있습니다." 등의 안내 - (문구 안내) 최소한 4초 동안 자막으로, "다음 메시지에는 AI를 통해 전체 또는 부분적으로 생성된 정보가 포함되어 있습니다." 등의 안내
라디오	- (구두 안내) 명확하고 적절한 속도의 목소리로, "다음 메시지에는 AI를 통해 전체 또는 부분적으로 생성된 정보가 포함되어 있습니다." 등의 안내

- FCC는 표준화된 언어를 사용하여 정치광고 직전(直前) 또는 광고 중에 AI 생성 콘텐츠 포함여부를 공개할 수 있도록 제안하고, AI 사용공개의 적절성, 공개 방식, 그리고 AI 사용 여부에 대한 분쟁 발생 시의 대응방안과 관련하여 의견 요청

- 또한, 방송국이 네트워크 또는 신디케이션[8] 회사로부터 방송 시간을 구매한 당사자와 직접 접촉하지 않을 가능성이 높아 방송국에서 방영하는 네트워크 또는 신디케이션 프로그램에 삽입된 정치광고에 공개 요구사항을 어떻게 적용해야 하는지에 대한 의견 요청

5 방송 시스템 중의 하나로, 기존 프로그램을 재송신하는 서비스 외에 자체 스튜디오에서 제작한 영화나 지역 정보를 추가로 방송하는 시스템
6 47 U.S.C. § 325(c) Broadcast to foreign countries for rebroadcast to United States; PERMIT
7 「통신법」 제325조제C항에 따른 허가는 미국에서 프로그램을 제작하지만 미국 라이선스 방송국에서 프로그램을 방송하는 대신 미국 스튜디오에서 미국 외 지역으로 프로그램을 전송하는 경우 필요
8 네트워크를 거치지 않고 프로그램 제작사에서 지역 방송국으로 완성된 프로그램을 직접 공급하는 것

■ 전망 및 시사점

○ FCC는 오랫동안 TV/라디오 정치광고 관련 투명성을 규제해왔고, 연방선거관리위원회(Federal Election Commission, FEC)와 협력하여 AI 규제를 추진할 계획

- FEC는 연방 선거와 관련되지 않은 TV/라디오 광고(예: 주 선거 후보의 광고 또는 독립적인 이슈 캠페인)를 규제할 권한이 없기 때문에, FCC는 FEC가 조치할 수 없는 영역에 집중

○ 동 잠정규정 예고문은 정치광고 내 AI 생성 콘텐츠 공개를 통한 투명성과 신뢰성을 제고하여, 유권자들로 하여금 AI 생성 콘텐츠를 식별하고 부정확한 정보 유포를 막도록 할 수 있음

○ AI 생성 콘텐츠 공개 규제 적용범위가 점차 케이블, 위성 등 다른 플랫폼으로 확대될 것으로 예상되고, 추후 AI 생성 콘텐츠에 대한 종합적인 규제 체계가 마련될 가능성이 있음

- 주 단위에서 AI 생성 콘텐츠 관련 규제가 파편적으로 발의되고 있으나, 이를 통해 연방 차원에서의 일관성 있는 정책 집행이 가능할 것으로 기대

Reference

▪https://docs.fcc.gov/public/attachments/FCC-24-74A1.pdf
▪https://docs.fcc.gov/public/attachments/DOC-404252A1.pdf
▪https://www.federalregister.gov/documents/2024/08/05/2024-16977/disclosure-and-transparency-of-artificial-intelligence-generated-content-in-political-advertisements

해외 입법 동향

미국 FCC,「원치 않는 로보콜 및 로보텍스트로부터 소비자를 보호하는 AI 기술의 영향에 관한 잠정규정 예고문」발표

미국 연방통신위원회(FCC)는 AI가 생성한 로보콜과 로보텍스트로부터 소비자를 보호하는 방안에 관한 잠정규정 예고문(NPRM)[1]에 대한 의견수렴을 진행 (2024. 8. 8. ~ 10. 20.)

■ 개요 및 추진배경

○ 2023년 11월 16일, FCC는 불법적이고 원치 않는 로보콜과 로보텍스트로부터 소비자를 보호하기 위한 지속적 노력의 일환으로 AI 기술을 이해하기 위한 질의서(Notice of Inquiry, NOI)를 발표

NOI 주요내용
• AI 기술이「전화소비자보호법(TCPA)[2]」에 따른 FCC의 법적 책임에 어떻게 부합하는지 • 향후 AI 기술이「TCPA」의 적용을 받게 되는 시점과 상황 • AI가 기존 규제체계와 향후 정책 수립에 미치는 영향 • FCC가 신뢰할 수 있는 출처에서 합법적으로 생성된 AI 음성 또는 텍스트 콘텐츠의 진위를 확인하는 방법을 고려해야 하는지 여부

○ 2024년 2월 8일, FCC가「전화소비자보호법(TCPA)」등에 명시된 '인공 또는 사전 녹음된 음성'에는 "인간의 목소리를 닮았거나 사전 녹음된 음성을 사용하여 통화 콘텐츠를 생성하는 현재 AI 기술을 포함한다"라는 선언적 결정(Declaratory Ruling)[3]을 발표

- AI 기술을 사용하는 통화가「TCPA」등에 해당할 경우, 비상 목적이나 예외규정이 없는 한 수신자의 사전 명시적 동의가 필요하다는 점을 분명히 함

○ 2024년 8월 8일, FCC는 **AI 기술의 오용**으로부터 소비자를 보호하고, **AI 기술의 긍정적 사용**을 제고하기 위하여 동 잠정규정 예고문을 발표

1 Implications of Artificial Intelligence Technologies on Protecting Consumers from Unwanted Robocalls and Robotexts
2 Telephone Consumer Protection Act
3 규정의 유효성, 규정의 적용가능성 또는 관할권 문제에 대한 기관의 결정

■ 주요내용

○ **('AI 생성 통화' 정의)** FCC는 'AI 생성 통화'를 정의하고, 이러한 정의가 AI 기술의 악용 방지와 긍정적 활용 사이의 균형을 유지하는지에 대한 의견 요청

〈 AI 생성 통화의 정의 〉

구분	주요내용
AI 생성 통화 (AI-Generated Call)	• 예측 알고리즘과 대규모 언어 모델(LLMs)을 포함한 컴퓨터 기술이나 기계 학습을 사용하여 인공 음성을 만들거나 자연어를 처리해 음성 또는 텍스트를 생성함으로써, 발신 전화로 수신자와 통신하는 모든 기술이나 도구를 활용한 통화

- 지난 2월 선언적 결정을 통해 「TCPA」에 명시된 "인공 또는 사전 녹음된 음성"에 AI 기술이 포함되었음을 고려할 때, 'AI 생성 통화'를 별도로 정의할 필요성에 대한 의견 요청

○ **('AI 생성 통화' 공개)** 로보콜 및 로보텍스트 발신자에게 AI 기술을 이용해 생성한 인공 음성 또는 사전 녹음된 음성의 사용 여부를 의무적으로 공개하도록 요구

주요내용
• **AI가 생성한 인공 또는 사전 녹음된 음성 메시지**를 사용하여 **전화를 거는 발신자**는 인공 또는 사전 녹음된 전화 수신에 대한 소비자의 동의를 받아야 함 – 소비자의 동의를 받을 경우, 전화에 FCC가 정의한 'AI 생성 통화'가 포함될 수 있음을 명확하게 명시해야 함 • **AI 생성 콘텐츠가 포함된** 자동 다이얼 **문자 메시지를 보내는 발신자**도 AI 생성 콘텐츠 수신에 대한 소비자의 동의를 받아야 하며, 그 사실을 소비자에게 명확하게 공개해야 함 • **AI 생성 음성을 사용하는 발신자**는 통화를 시작할 때, 통화에 AI 생성 기술이 사용되고 있다는 사실을 수신자에게 명확하게 공개해야 함

○ **(장애인의 전화서비스 이용 촉진)** FCC는 언어 또는 청각 장애가 있는 개인이 AI 기술을 포함한 모든 기술을 사용하여 전화 통신망을 활용할 수 있도록, 예외규정 도입[5]

주요내용
• **특정 의료 전화와 관련**하여, AI 생성 음성을 사용하는 **언어 또는 청각 장애인에게** 인공 또는 사전 녹음된 통화 **동의 및 신원확인 요구사항 예외규정** 도입 – 장애인의 통신 서비스 접근 향상을 통해 「미국 장애인법[4]」에 규정된 통신 중계 서비스(Telecommunications Relay Service) 프로그램의 목표를 달성하기 위함 • **장애인**이 인공 또는 사전 녹음된 음성을 활용하여 **주거용 전화선으로 의사소통하는 경우**, AI 및 기타 관련 기술의 사용에 대한 **예외규정** 도입 – 이러한 전화는 비상업적 목적으로서, 원치 않는 광고가 포함되어선 안 됨

4 Americans with Disabilities Act

5 「TCPA」 제227조제b항제2조에 근거하여, FCC는 규칙 또는 명령에 따라 ▲상업적 목적으로 이루어지지 않은 통화 및 ▲원치않는 광고를 포함하지 않고 개인정보보호에 부정적 영향을 미치지 않는 상업적 목적의 통화를 동의 및 신원확인 요구사항 예외규정으로 정할 수 있음

○ **(기술 개발)** FCC는 질의서(NOI)를 통해 장치 또는 네트워크 수준에서 다음과 같은 기능을 수행할 수 있는 기술의 개발과 가용성에 대한 의견을 요청

주요내용
• 음성통화 내용의 실시간 분석을 기반으로 잠재적으로 사기성이 있고 AI로 생성된 수신 통화를 감지하는 기술
• 이러한 음성통화가 사기성이 있고 AI에 의해 생성되었을 가능성이 있음을 소비자에게 경고하는 기술
• 분석을 통해 유사하게 AI로 생성되었거나 사기성이 있는 것으로 식별된 향후 음성 통화를 잠재적으로 차단하는 기술

■ 전망 및 시사점

○ FCC는 2023년 말 바이든 대통령의 AI 행정명령[6]에 따라 AI의 위험을 해결하기 위한 다양한 방법을 적극적으로 모색하고 있고, 동 NPRM도 그러한 조치의 일환으로 진행

- 소비자들이 로보콜 및 로보텍스트 등 AI 생성 콘텐츠를 명확히 인지할 수 있도록 함으로써 궁극적으로 AI 오남용의 위협으로부터 소비자를 보호하기 위함

○ AI 기술의 긍정적 활용 사례 증가와 더불어 AI 기술의 혜택을 극대화하면서도 위험을 최소화하는 균형잡힌 정책접근이 요구되며, 이는 AI 기술의 지속적인 발전과 사회적 수용성 제고에 중요한 역할을 할 것으로 기대

○ AI 사기 탐지, 실시간 분석 및 경고 시스템 등 관련 기술의 발전으로 통신 및 AI 관련 기업들에게도 새로운 비즈니스 기회가 제공될 것으로 기대

Reference

▪https://www.fcc.gov/document/fcc-proposes-first-ai-generated-robocall-robotext-rules-0
▪https://www.fcc.gov/consumer-governmental-affairs/fcc-propose-ai-generated-robocall-rules-protecting-accessibility
▪https://docs.fcc.gov/public/attachments/DOC-397925A1.pdf
▪https://docs.fcc.gov/public/attachments/FCC-24-84A1.pdf

6 Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 2023.10.30.

해외 입법 동향

미국 연방항공청(FAA), 「항공기 장비 등의 사이버보안에 관한 잠정규정 예고문」 발표

미국 연방항공청(FAA)은 「(항공기) 장비, 시스템 및 네트워크 정보보안 보호에 관한 잠정규정 예고문(NPRM)」[1]을 발표 (2024. 8. 21. ~ 10. 21.)

■ 개요 및 추진배경

○ 항공기 설계 추세가 내외부 데이터 네트워크 및 서비스에 대한 연결성을 고려함에 따라, 사이버보안 취약점에 노출될 위험이 증가함[2]

○ 특히, 운송 범주 항공기, 엔진 및 프로펠러 장비, 시스템 및 네트워크를 '**의도적인 무단 전자 상호작용**(Intentional Unauthorized Electronic Interactions, **IUEI**)'으로부터 보호하고자 함

■ 주요내용

○ (요구사항) FAA는 '의도적인 무단 전자 상호작용(IUEI)'으로부터 운송 범주 항공기, 엔진 및 프로펠러의 안전을 보장하고자 요구사항을 제안

- ▲설계 승인 신청자(Design approval applicants)는 시스템, 내외부 인터페이스 등과 관련된 모든 위협조건을 식별하기 위해 사이버보안 위험분석을 수행해야 하고, ▲FAA는 이러한 위험분석을 통해 위협조건의 심각성을 평가해야 함

〈 항공기 사이버보안 관련 주요 요구사항 〉

구분	주요내용
운송 범주 항공기 보호	• 설계 승인 신청자는 안전, 기능 및 지속적인 감항성에 필요한 보안위험을 완화하기 위하여 **두 가지 요구사항**을 충족한다는 것을 **입증**해야 함 ※ 동 요구사항은 실질적으로 FAA가 과거 운송 항공기 인증 프로젝트에서 발행한 ASISP 특별 조건 등의 권장사항을 기반으로 함 - **1)** 항공기 내부 또는 외부의 네트워크 무단 액세스로부터 보호되도록 설계하였음을 입증해야 함 - **2)** 안전한 운항에 필요한 항공기 장비, 시스템 및 네트워크에 대한 악의적인 변경 및 부정적 영향을 방지하도록 설계하였음을 입증해야 함

1 Equipment, Systems, and Network Information Security Protection

2 ▲항공기 유지보수 노트북, ▲공항 또는 항공사 게이트 연결 네트워크, ▲인터넷 등 공용 네트워크 및 셀룰러 네트워크, ▲무선 항공기 센서 및 센서 네트워크, ▲휴대용 전자기기 및 휴대용 전자비행정보장치(Electornic Flight Bag, EFB), ▲GPS 및 위성기반 증강 시스템 디지털 데이터 등에서 사이버보안 취약점이 발생할 가능성이 있음

	• **(IUEI의 정의)** 정보 및 항공기 시스템 인터페이스의 무단 액세스, 사용, 공개, 거부, 중단, 수정 또는 파괴로 인하여 항공기에 영향을 미칠 수 있는 상황 또는 사건 ※ 본 정의는 맬웨어 및 외부 시스템이 항공기 시스템에 미치는 영향을 포함하지만, 물리적 공격이나 전자기 전파 방해 등은 포함하지 않음 - 설계 승인 신청자는 사이버보안 위협이 시스템 간 전파될 수 있다는 점에서 항공기의 장비, 시스템 및 네트워크를 '다른 시스템과 관련하여' 별도로 고려해야 함
	• **(요구사항의 범위)** 항공기의 안전이나 운영에 영향을 미칠 수 있는 사이버보안 위협에만 적용됨 - 예를 들어 ▲승객 신용카드를 처리하는 항공기 장치의 잠재적 취약점 ▲기존 항공기나 장비 ▲물리적 전자 공격에는 해당하지 않음
엔진 및 프로펠러 제어시스템 보호	• 장비 및 네트워크에 설치된 모든 엔진 및 프로펠러 제어 시스템을 IUEI로부터 보호해야함 - 설계 승인 신청자는 IUEI로 인해 발생하는 모든 보안위험을 식별하고 평가한 후, 안전, 기능 및 지속적인 감함성에 필요한 보안위험을 완화해야 함
지속적인 감항성을 위한 지침	• 설계 승인 신청자는 IUEI에 대한 지속적인 사이버보안을 보장하기 위하여 필요한 모든 절차를 운송 범주 항공기, 엔진 또는 프로펠러의 **첫 번째 소유자**에게 제공하고, **후속 운영자가 사용**할 수 있도록 **보안지침을 준비**해야 함

○ (규제조화) FAA는 동 NPRM을 통해 새로운 항공기를 제작하거나 기존 항공기에 대한 변경된 인증의 규제준수 소요시간을 줄이기 위하여, 다른 국가의 항공 규제당국 간 요구사항을 조정하고자 함

- 특히, 유럽항공안전청(European Union Aviation Safety Agency, EASA)의 요구사항과 조화시켜 제조업체에게 규정 준수를 입증해야 하는 단일 요구사항을 제공함으로써 인증 비용과 복잡성을 줄이고 일관된 안전 수준을 성문화함

■ 전망 및 시사점

○ 항공 전문가들은 항공기의 통신 및 연결 구성요소 증가를 고려할 때, 동 NPRM과 같은 명시화된 항공기 사이버보안 요구사항이 오래전부터 필요했음을 강조

- 동 NPRM은 항공기 디지털화에 따른 사이버위협에 대응하기 위한 중요한 단계로 볼 수 있음

○ 동 NPRM은 기존 관행인 FAA의 특별 조건과 EASA의 요구사항의 대부분을 반영하여, 항공기 제조업체 및 FAA 양측에 인증과정의 시간과 비용을 줄이는 데 도움이 될 것으로 평가

Reference

▪https://www.federalregister.gov/documents/2024/08/21/2024-17916/equipment-systems-and-network-information-security-protection

▪https://public-inspection.federalregister.gov/2024-17916.pdf

▪https://therecord.media/faa-new-cybersecurity-rules-airplanes

해외 입법 동향

미국 상무부 산업안보국, 「첨단 AI 모델과 컴퓨팅 클러스터 개발 관련 보고 의무화 규정」 제안

산업안보국(Bureau of Industry and Security, BIS)은 첨단 AI 모델 및 컴퓨팅 클러스터 개발 활동에 대한 상세보고를 의무화하는 규정[1]을 제안하고 대중의 의견을 수렴 (2024. 9. 11. ~ 10. 11.)

■ 개요 및 추진배경

○ 동 규정(안)은 바이든 행정부의 AI 행정명령(EO 14110)[2]에 따른 후속 조치

- EO 14110에 따르면, '이중용도 파운데이션 모델' 개발 역량을 갖춘 기업은 해당 모델의 세부 정보를 연방정부에 지속적으로 제공해야 함

구분	주요내용
제4.2조제(a)항제(i)호	• 이중용도 파운데이션 모델을 개발하는 회사는 모델의 훈련, 개발, 생산 활동과 관련된 정보 및 이에 대한 물리적, 사이버보안 보호 조치를 연방정부에 제공해야 함 • 해당 회사는 모델 가중치의 소유권 정보와 이를 보호하기 위한 보안 조치, 그리고 AI 레드팀 테스트 결과 및 이에 따른 모델 보안 강화 조치에 대해 보고 • 회사는 생물무기 개발 위험, 소프트웨어 취약점, 자가복제 가능성 등 잠재적 위험 요소의 평가 결과와 이에 대응하기 위한 안전 조치를 국립표준기술원의 지침에 따라 제공
제4.2조제(a)항제(ii)호	• 대규모 컴퓨팅 클러스터를 획득, 개발 또는 보유한 모든 주체는 해당 클러스터의 존재, 위치, 총 컴퓨팅 파워를 포함한 상세 정보를 의무적으로 보고

○ 2024년 1월 26일, 산업안보국은 이중용도 파운데이션 모델을 개발하거나 개발 계획이 확인된 기업을 대상으로 조사(Survey)를 실시해 AI 행정명령에서 요구한 정보를 수집

- 조사를 완료한 기업 및 이중용도 파운데이션 모델 또는 대규모 컴퓨팅 클러스터를 개발하거나 개발 중인 여타 기업은 분기별로 해당 활동에 대한 정보를 제출할 필요

- 조사를 통해 정보 일체를 제출한 기업은 이미 보고한 내용을 제외하고 조사 이후 추가 및 업데이트, 변경된 사항을 보고할 필요

1 Establishment of Reporting Requirements for the Development of Advanced Artificial Intelligence Models and Computing Clusters
2 Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (2023.10.30.)

■ 주요내용

○ **(정의)** 규정(안)은 주요 용어를 다음과 같이 정의

구분	주요내용
AI 레드팀 (AI Red-teaming)	• 통제된 환경에서 AI 개발자와 협력하여 AI 시스템의 결함과 취약점을 찾아내기 위한 체계적인 테스트 노력 • AI의 맥락에서 레드팀 활동은 주로 적대적 방법을 채택하여 AI 시스템의 유해하거나 차별적인 결과물, 예기치 않거나 바람직하지 않은 시스템 동작, 한계 또는 시스템 오용과 관련된 잠재적 위험과 같은 결함과 취약점을 식별
AI 모델 (AI Model)	• AI 기술을 구현하고 연산, 통계 또는 기계학습 기술을 사용하여 주어진 입력 세트에서 출력을 생성하는 정보 시스템의 구성 요소
AI 시스템 (AI System)	• 전체 또는 일부가 AI를 사용하여 작동하는 모든 데이터 시스템, 소프트웨어, 하드웨어, 애플리케이션, 도구 또는 유틸리티
이중용도 파운데이션 모델 (Dual-Use Foundation Model)	• ▲광범위한 데이터로 훈련되고 ▲통상 자체 감독을 사용하며 ▲100억 개 이상의 매개변수를 포함하고 ▲광범위한 맥락에서 적용가능하며 ▲안보, 국가 경제안보, 공중보건과 안전 등에 심각한 위협을 제기하는 과업에서 높은 수준의 성과를 보이거나 보일 수 있도록 쉽게 수정 가능한 경우 - 비전문가가 화학·생물학·핵·방사능(CBRN) 무기를 설계, 합성, 획득 또는 사용할 수 있도록 진입 장벽을 크게 낮추는 경우 - 광범위한 사이버 공격 목표를 겨냥한 자동화된 취약점 발견 및 악용을 통해 강력한 사이버 공격 작전을 가능케 하는 경우 - 기만이나 혼란을 초래하는 방식으로 인간의 통제나 감독을 회피할 수 있게 하는 경우
모델 가중치 (Model Weights)	• 신경망 계층에서 사용되는 수치적 매개변수

○ **(적용대상)** 6개월 이내 다음과 같은 활동에 참여하거나 참여할 계획이 있는 기업은 분기별로 산업안보국에 정보를 보고할 필요

주요내용
• 10^{26} 플롭스(FLOPS)[3]를 초과하는 연산을 사용하여 **AI 모델을 훈련하는 경우** 또는 • 300Gbit/s 이상의 데이터센터 네트워킹으로 연결되고 이론상 최대 10^{20} 플롭스를 처리할 수 있는 연산 능력을 갖춘 **컴퓨팅 클러스터를 획득, 개발 또는 보유하는 경우**

○ **(보고내용)** 적용 대상에 해당하는 기업은 다음의 정보를 제출할 필요

주요내용
• 정교한 위협으로부터 훈련 과정의 무결성을 보장하기 위한 물리적·사이버보안 보호를 포함해 **이중용도 파운데이션 모델의 훈련, 개발, 생산과 관련해 진행 중이거나 계획된 모든 활동**
• 이중용도 모델 가중치의 소유권 및 점유권과 해당 **모델 가중치 보호를 위해 취한 물리적·사이버보안 조치**
• 관련 **AI 레드팀 테스트에서 확인된 이중용도 파운데이션 모델의 성능 결과**(레드팀 테스트 과정에서 성능 개선 및 전반적 모델 보안 강화를 위한 조치 등 안전 목표 달성과 관련된 조치에 대한 설명 포함)
• **이중용도 파운데이션 모델의 안전성과 신뢰성 관련 기타 정보** 또는 미국 국가 안보를 위협하는 활동이나 위험

3 컴퓨터가 1초 동안 수행할 수 있는 부동소수점 연산의 횟수로, 컴퓨터의 성능을 수치로 나타날 때 주로 사용되는 단위

○ **(보고시기)** 적용 대상에 해당하는 기업은 분기별로 관련 활동을 통지해야 하며, 통지 시점으로부터 6개월 동안 계획된 활동을 모두 포함할 필요

○ **(후속 대응 및 질의)** 적용대상에 해당하는 기업은 관련 활동에 대한 보고 이후 산업안보국이 문의하는 질의에 대하여 30일 이내에 응답해야 하며, 보고 및 응답이 불충분한 경우 산업안보국은 불완전 보고를 통지하고 14일 이내에 재응답을 요구

- 산업안보국이 질의에 대한 응답을 받은 이후 추가 질의를 하는 경우, 질의를 받은 기업은 7일 이내에 응답할 필요

○ **(의견수렴 내용)** 산업안보국은 규정(안)에 대하여 특히 다음 사항에 대한 대중의 의견을 요청

구분	주요내용
통지 일정	• AI 모델 및 컴퓨팅 클러스터의 안전과 보안에 대한 정보를 적시에 제공받는 동시에 응답자의 계획 수립을 돕고 부담을 완화하기 위해 산업안보국이 제안한 분기별 통지 일정에 대하여 의견을 요청
정보의 수집 및 보관	• 수집된 정보의 민감성을 고려해 데이터의 안전을 보장할 수 있는 수집과 보관 방법에 대한 의견을 요청
적용 기준	• 현행 적용 기준(10^{26} 플롭스(FLOPS)를 초과하는 연산을 사용하는 AI 모델 및 300Gbit/s 이상의 데이터센터 네트워킹으로 일시 연결되고 이론상 최대 10^{20} 플롭스를 처리할 수 있는 연산 능력을 갖춘 컴퓨팅 클러스터)에 대한 의견을 요청

■ 전망 및 시사점

○ 미국 정부는 AI 모델의 안전성과 신뢰성을 보장하고 사이버 공격을 방어하며 적대국의 오남용에 따른 위험을 제한하기 위해 첨단 AI 모델 개발기업 및 클라우드 사업자를 대상으로 구체적인 보고를 요구하는 이번 규정(안)을 마련

- 동 규정(안)은 미국연방규정집(CFR) 제15편 제702부(산업기반 조사-데이터 수집)[4]을 개정하는 것으로, 보고 의무를 준수하지 않으면 강제집행 및 1만 달러 이하의 벌금 또는 1년 이하의 징역형 등 민형사 처벌을 받을 가능성이 있음

○ 한편, AI 모델은 국가 안보에 필수적인 군용 장비나 신호정보 장치(예: 위성, 카메라, 레이더), 사이버보안 등의 제품과 서비스 역량을 크게 강화할 수 있으므로, 미국 정부는 국제 경쟁력을 유지하기 위해 AI 모델을 국방 산업에 통합하는 것이 필수적

· 미국 정부는 AI 모델을 방위산업에 통합하기 위해 AI 모델이 안전하고 신뢰할 수 있는 방식으로 작동하도록 필요한 조치를 이행하고 사이버보안 취약점을 최소화해야 함

4 Title 15(Commerce and Foreign Trade) Part 702(Industrial Base Surveys-Data Collections)

· 또한, 외국의 적대 세력이 국가안보를 위협하는 활동에 AI 모델을 사용할 가능성에 대비해야 하고 이를 위하여 AI 모델의 안전성 및 신뢰성 관련 정보를 확보할 필요

○ 다만, 상무부 산업안보국에 따르면 규정(안)이 제시한 보고 요구사항은 일반적으로 중소기업들이 접근할 수 없는 방대한 컴퓨팅 자원을 갖춘 소수의 빅테크에만 적용[5]되어 영향이 제한적

- 그러나, 새로운 보고 요구사항을 준수해야 하는 기업들은 장기적으로 규정 준수 인력의 확대와 새로운 보고 체계의 구현, 정기감사 진행 등의 규제 부담이 예상되며, 비용 문제를 넘어 기업의 혁신을 저해할 수 있다는 우려도 제기됨

Reference

▪https://www.federalregister.gov/documents/2024/09/11/2024-20529/establishment-of-reporting-requirements-for-the-development-of-advanced-artificial-intelligence

▪https://www.bis.gov/press-release/commerce-proposes-reporting-requirements-frontier-ai-developers-and-compute-providers

▪https://www.mayerbrown.com/en/insights/publications/2024/09/us-department-of-commerce-issues-proposal-to-require-reporting-development-of-advanced-ai-models-and-computer-clusters

▪https://www.cio.com/article/3513255/us-targets-advanced-ai-and-cloud-firms-with-new-reporting-proposal.html

5 규정(안) 발행 시점에서 보고 요구사항을 적용받는 기업은 0~15개로 평가

해외 입법 동향

미국 예산관리국(OMB), 「정부의 책임있는 AI 조달 추진을 위한 각서」 발표

미국 예산관리국(OMB[1])은 정부기관의 AI 조달 관련 비즈니스 프로세스를 관리하기 위하여, 「정부의 책임있는 AI 조달 추진을 위한 각서(M-24-18)[2]」발표 (2024. 10. 3.)

■ 개요

○ 본 각서는 정부기관이 AI 조달업무를 수행하는 경우 **▲부서 간 또는 정부기관 간 협업을 구축하고, ▲AI 위험 및 성과를 관리하며, ▲혁신적 조달을 통한 경쟁력 있는 AI 시장을 촉진**할 수 있도록 구체적 기준을 제시

- 「미국 AI 진흥법(Advancing American AI Act)」, AI 행정명령(EO 14110)[3] 및 「정부기관의 AI 사용을 위한 거버넌스, 혁신, 위험관리 개선에 관한 각서(M-24-10[4])」에 따라, OMB 국장은 정부기관의 AI시스템 및 서비스 조달 시 일관적 기준을 제시하기 위하여 동 지침을 마련

■ 주요내용

○ **(정의)** 본 각서의 용어는 기존 법령 등에서의 정의 규정을 인용하고 있으며, 이는 연방정부 차원의 일관된 AI 관련 용어 체계 구축을 위한 것임

주요 용어	주요내용
기관 (Agency)	· ▲행정부처, 군사부처 ▲정부법인, 정부통제법인 ▲행정부 기타기관(대통령실 포함) ▲독립규제기관 - 제외 : ▲회계감사원(GAO) ▲연방선거위원회 ▲컬럼비아 특별구 정부 ▲미국 영토/속령 정부 ▲정부소유-계약자운영 시설 *미국연방법전(U.S.C.) 제44편 공개 인쇄 및 문서 제3502조제1항의 정의를 활용
인공지능 (Artificial Intelligence, AI)	· 자율적 시스템: 인간 감독 없이 불확실한 상황에서 작업 수행 ▲데이터 기반 학습/성능 향상 가능 · 인간형 문제해결 시스템: ▲인간형 인지/계획/학습/소통/행동 수행 ▲소프트웨어/하드웨어 형태 구현 · 인간 모사 시스템: ▲인지 아키텍처, 신경망 활용 ▲인간 사고/행동 모방 · 인지 작업 수행 시스템: 기계학습 기반 인지 작업 · 합리적 행동 시스템: ▲목표 달성을 위한 지능형 에이전트/로봇 ▲인지/계획/추론/학습/의사결정 수행 *국방수권법(2019) 제238조제g항 정의 활용

1 Office of Management and Budget
2 Advancing the Responsible Acquisition of Artificial Intelligence in Government memorandum (M-24-18)
3 Executive Order 14110(Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence), 2023.10.30.발표
4 Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence, 2024.3.28.발표

주요 용어	주요내용
AI 모델 (AI Model)	· AI 기술을 구현하고 계산, 통계 또는 기계 학습 기술을 사용하여 주어진 입력 집합에서 출력을 생성하는 정보 시스템의 구성 요소를 의미 *AI 행정명령(EO 14110), 제3조제c항 활용
AI 시스템 (AI System)	· ▲AI 연구/개발/구현 목적 시스템 ▲AI가 통합된 업무/운영 시스템 ▲동적/정적 기계학습 알고리즘 사용 - 제외 : ▲AI 내장된 일반 상용 제품 ▲워드프로세서/지도 등 *미국 AI 발전법(Advancing American AI Act) 제7223조 정의 활용
생성형 AI (Generative AI)	· 입력 데이터의 구조와 특성을 에뮬레이션하여 파생된 합성 콘텐츠를 생성하는 AI 모델 클래스를 의미 (이미지, 비디오, 오디오, 텍스트 및 기타 디지털 콘텐츠가 포함) *AI 행정명령(EO 14110), 제3조제p항 활용
레드팀 활동 (Red-teaming)	· AI 시스템의 결함과 취약성을 식별하기 위한 구조화된 시험을 수행하는 팀을 의미하며 일반적으로 통제된 환경에서 AI 개발자와 협업하여 수행 *AI 행정명령(EO 14110), 제3조제d항 활용
조달 (Acquisition)	· 연방정부용 물품/서비스의 계약적 획득으로서, 구매/임대 모두 포함하며, 수요확인부터 계약관리까지 전 과정을 의미 *연방조달규정(FAR) subpart 2.1 정의

○ **(적용 범위)** 본 각서는 「미국연방법전」 제44편 제3502조제1항(44 U.S.C. § 3502(1))에 정의된 모든 기관[5]이 직접 또는 이를 대신하여 획득한 AI 시스템 또는 서비스에 적용됨

- 단, AI가 포함된 일반 사용제품(예: 워드프로세서, 지도 내비게이션 시스템 등)은 적용되지 않음

본 각서는 ①새로운 AI 책임을 반영하기 위해 **부서 간 또는 정부기관 간 협업 구축** ②**AI 위험 및 성과 관리** ③혁신적 조달을 통한 경쟁력 있는 **AI 시장 촉진을 위한 새로운 요구사항**을 제시함

① **(부서 간 · 정부기관 간 협업 구축)** 조달 과정 전반에 걸쳐 AI에 대한 책임 및 거버넌스를 반영한 조달 정책, 절차, 관행 등 업데이트를 위한 부서/기관 간 협력 강조

- **(부서 간 협력)** AI 위험 및 성과 관리를 위하여 내부 협력을 위한 정책 및 절차를 수립하도록 하는 등 각 부서 기능 간의 협력을 공식화하며, 각 기관의 AI 최고책임자(CAIO)는 AI 조달 조정계획을 OMB에 제출해야 함

- **(기관 간 협력)** AI 최고책임자(CAIO)는 모든 정부기관에 제공될 AI 조달 관련 정보 및 아티팩트(information and artifacts)[6]를 식별해야 하며, AI 조달 과정에서 지속적으로 발생하는 문제를 검토할 실무그룹을 설립하도록 함

② **(AI 위험 및 성과 관리)** AI 시스템 및 서비스의 개발, 교육, 배포 시 조달 정책 및 관행을 조정하기 위하여 개인정보보호, 사이버보안, 데이터 소유권 및 권리 등 구체적인 조치를 포함하고 있으며, AI 사고 발생 시 이를 보고하도록 의무화하고 있음

5 행정부 부처, 군사 부처, 정부 기업, 정부가 통제하는 기업, 행정부의 기타 기관(대통령 집행실 포함), 독립 규제 기관을 의미

6 아티팩트란, AI 조달 과정에서 생성되는 구체적이고 실질적인 문서나 도구들을 지칭하는 것으로, 다른 기관들이 실제로 참고하고 재사용할 수 있는 유형의 산출물을 의미

<table>
<tr><th>구분</th><th>주요내용</th></tr>
<tr><td>AI 조달 식별 및 관리</td><td>· (AI 사용사례 관리) 연간 AI 사용사례 목록 업데이트, 권리/안전 영향 여부 평가
· (벤더 관리 요구사항) AI 시스템 용도의 명확한 커뮤니케이션, 신규 AI 기능 통합 시 사전 통지 의무, AI 사용 현황 정기적 보고</td></tr>
<tr><td>핵심 보호 조치</td><td>· (개인정보보호) SAOP 조기 참여 보장, 전체 수명주기 관리, PII 보호 기술 평가
· (생체인식 시스템 관리) 합법적 데이터 수집 검증, NIST 평가 참여, 품질 기준 준수, 감사 로그 유지
· (차별 방지) 데이터 편향성 검토, 차별적 결과 모니터링, 완화 전략 수립</td></tr>
<tr><td>성과 및 위험 관리 체계</td><td>· (요구사항) 성과 기반 요구사항 및 평가 기준 수립, 계약 체결 전 AI 시스템 성능 평가 및 검증, 지속적인 성능 모니터링 및 사후관리 체계 구축
· (IP 및 데이터 관리) 정부와 계약자 간 IP 권리의 명확한 구분, 기관 데이터의 적절한 처리와 보호를 위한 체계 수립, AI 훈련용 데이터 사용에 대한 명확한 제한 설정
· (사이버보안 및 정부기관의 데이터 보호 승인 조치) ▲트레이닝의 안전성 확보 및 ▲AI모델보안을 위한 소프트웨어 관리, ▲AI모델 설계 및 트레이닝에 사용되는 모든 데이터 평가 등을 위하여 모든 문서 및 액세스 권한을 확보할 수 있도록 계약 요건에 포함할 필요
<table>
<tr><td>트레이닝의 안전성 확보를 위한 소프트웨어 관리</td><td>· 정부에 제공되는 AI 모델에 대한 트레이닝 세션 중에 사용된 데이터 소싱, 입력, 매개변수 등의 증거를 포함하도록 계약업체에 트레이닝 로그 요청 등</td></tr>
<tr><td>AI 모델 보안을 위한 소프트웨어 관리</td><td>· 개인정보보호 및 보안을 위한 소프트웨어 관리 등 데이터 보호를 위한 정부기관의 요구사항을 벤더가 준수하는지 여부를 포함해야 함. 이 때, 벤더는 AI 모델의 출처 및 보안 입증을 위하여 해당 모델에 사용된 트레이닝 절차 관련 상세문서를 제공해야 함</td></tr>
<tr><td>AI 모델 설계 및 트레이닝에 사용되는 모든 데이터 평가</td><td>· 정부기관의 데이터를 사용한 AI 모델 훈련의 경우, 최소한의 기대치를 명시하도록 함
– 데이터 중독, 데이터 유출 등의 추가적인 AI 위험성을 관리하기 위함</td></tr>
</table></td></tr>
<tr><td>특수 AI 관리 체계</td><td>· (생성형 AI 조달 시 계약에 포함되어야 할 사항) AI 생성 콘텐츠에 대한 워터마크 등 식별 메커니즘 구현, 유해/불법 콘텐츠 생성 방지를 위한 기술적 조치, 모델 학습 및 평가 과정의 상세 문서화, 시스템 사용으로 인한 환경 영향 평가 및 완화 방안</td></tr>
<tr><td>모니터링 및 보고</td><td>· (지속적 모니터링 요구사항) AI 시스템의 기능 저하 및 권리/안전 영향 변화 감지, 분기/반기 단위 정기적 성능 및 위험 평가 실시, 실제 운영 환경에서의 테스트 및 결과 검증 등
· (사고보고 체계) 심각한 AI 사고/오작동 발생 시 72시간 이내 보고 의무화, 권리/안전 침해, 중요 인프라 중단, 재산 피해, 시스템 손실, 임무 실패, 인명 피해 등 보고 대상 명확화, 제3자 발견 및 공공 보고 체계 구축</td></tr>
</table>

③ **(혁신적 조달을 통한 경쟁력있는 AI 시장 촉진)** AI 시장에는 광범위한 공급업체(AI 모델 개발자, 인프라 제공업체, AI 서비스 제공업체 등)가 존재함에 따라, 정부기관은 다양하고 진화하고 있는 시장 환경에서의 공급업체가 준수해야하는 사항을 제시

– 벤더는 ▲계약수행 중 최초 생산된 코드/데이터/모델에 대한 적절한 권한을 정부기관에 제공해야하며, ▲투명한 라이선스 조건에 동의하며, 획득한 AI 시스템 또는 서비스를 합리적으로 사용할 수 있도록 인프라 지원, ▲AI 수명주기 전반의 가격 투명성 보장 등을 준수해야 함

■ 전망 및 시사점

○본 각서는 AI 기술의 빠른 발전과 그에 따른 위험을 고려하여, 연방정부의 AI 조달 과정에서 책임성, 투명성, 그리고 효율성을 증진시키는 중요한 역할을 할 것으로 기대됨

- 특히, AI 시스템 및 서비스의 개발, 교육, 배포 시 개인정보보호, 사이버보안 등의 조치를 이행하도록 하는 한편, AI 사고 발생 시 이를 보고하도록 의무화하는 등 AI 위험 및 성과 관리사항을 구체적으로 제시하고 있음

○다만, AI 투자 촉진·산업 진흥을 강조하는 트럼프 2기 행정부의 출범이 확정('25.1월~)됨에 따라, 동 지침을 포함한 바이든 행정부의 AI 규제 관련 기조가 계속 유지될지는 불확실하다는 의견도 있음

Reference

▪https://www.whitehouse.gov/omb/briefing-room/2024/10/03/fact-sheet-omb-issues-guidance-to-advance-the-responsible-acquisition-of-ai-in-government/

▪https://www.whitehouse.gov/wp-content/uploads/2024/10/M-24-18-AI-Acquisition-Memorandum.pdf

▪Proskauer Rose, “Upcoming Changes to AI Regulation in the New Administration”, Lexology, 2024.11.11.

해외 입법 동향

뉴욕주 금융서비스국, 「AI에 따른 사이버보안 위험 대응 등을 위한 지침」 발표

뉴욕주 금융서비스국(Department of Financial Services, DFS)은 해당 규제를 받는 기관들이 AI로 인해 발생하는 사이버보안 위험에 대응하기 위한 전략[1]을 발표 (2024. 10. 16.)

■ 개요

○ 뉴욕주 금융서비스국은 규제 적용대상이 「금융 사이버보안 규정[2]」(23 NYCRR 500)의 의무사항을 준수하는 한편, AI로 인한 새로운 위협으로부터 뉴욕시민 등을 보호하기 위하여 동 지침을 발표

○ 동 지침은 뉴욕주 금융서비스국의 규제 적용대상이 「금융 사이버보안 규정」에 명시된 사이버보안 위험관리 및 완화조치를 AI 위험 대응에 활용하기 위한 기준을 제시하는 등 권고적 성격에 해당

■ 주요내용 (※ 세부내용은 '붙임' 참고)

○ **(AI 위험 구분)** 동 지침은 AI와 관련된 사이버보안 위험을 ①사이버위협 행위자의 AI 사용으로 발생하는 위험과 ②적용대상의 AI 사용 또는 의존으로 발생하는 위험으로 구분

- **(사이버위협 행위자의 AI 사용)** ▲AI를 활용한 사회공학적 공격기법(AI-Enabled Social Engineering) 및 ▲AI로 고도화된 사이버보안 공격에 주목

- **(적용대상의 AI 사용·의존으로 발생하는 위험)** ▲방대한 양의 미공개정보 노출 또는 절도, ▲제3자 서비스제공자 및 기타 공급업체 의존으로 인한 취약점 증가를 우려

○ **(AI 위험완화 조치)** 동 지침은 AI 관련 위험을 완화하기 위한 조치로 「금융 사이버보안 규정」에 따른 ▲위험평가 기반 프로그램 설정, ▲제3자 서비스제공자 및 공급업체 관리, ▲액세스 통제, ▲사이버보안 교육 등을 제시

1 Cybersecurity Risks Arising from Artificial Intelligence and Strategies to Combat Related Risks

2 2017년 3월 뉴욕주는 금융기관을 위한 사이버보안 특화 규정을 시행하여, ▲위험평가 기반 사이버보안 프로그램 수립, ▲미공개정보에 대한 보안고도화, ▲정보보호최고책임자(CISO) 지정, ▲내부위험요소 제거, ▲연간보고의무 등 최소한의 요구사항을 규정하였고, 2023년 9월 11일 뉴욕주 금융서비스국은 동 규정을 개정하여 ▲다중인증(Multi-Factor Authentication) 요구사항을 확대하고 ▲랜섬웨어 보고의무 등을 도입

- **(위험평가 기반 프로그램 등 설정)** 사이버보안 위험평가를 기반으로 ▲방어조치를 결정하고, ▲위험평가를 설계하며, ▲사이버보안 위험요소에 중대한 변경이 발생할 때마다 위험평가를 매년 업데이트해야 함

- **(제3자 서비스제공자 및 공급업체 관리)** 정보시스템 및/또는 미공개정보에 액세스할 제3자 서비스제공자를 사용하기 전에 ▲제3자 서비스제공자에 대한 액세스 제어, ▲암호화, ▲실사 및 ▲계약 보호에 대한 지침 마련 등을 수행해야 함

- **(액세스 통제)** AI로 고도화된 사회공학적 공격기법에 대처하고 위협행위자가 적용대상의 정보시스템 및 미공개정보에 대한 무단 액세스 권한을 얻는 것을 방지하기 위하여, ▲다중인증(MFA) 활용, ▲추가적인 액세스 통제 정책, ▲액세스 권한 업데이트 등을 추진해야 함

- **(사이버보안 교육)** 고위 경영진을 포함한 모든 직원, 사이버보안 담당자, 제3자 서비스제공자에게 특화된 사이버보안 교육을 제공해야 함

- **(모니터링)** 미공개정보가 유지·관리되는 정보시스템에 대한 무단 액세스, 사용 또는 변조를 감지하기 위해, 새로운 보안취약점을 즉시 식별할 수 있는 모니터링 프로세스를 마련해야 함

- **(데이터관리)** 위협행위자가 정보시스템에 액세스할 수 있는 경우 노출 위험이 있는 미공개정보를 제한하고, 합법적인 비즈니스 목적에 필요하지 않은 미공개정보를 폐기하는 등 데이터 최소화 관행을 구현해야 함

■ 전망 및 시사점

○ 동 지침은 「금융 사이버보안 규정」의 적용대상이 사이버보안 프로그램을 개발하고 사이버보안 제어를 구현할 때 AI로 인해 발생할 수 있는 사이버보안 위험을 고려할 것을 강조

○ 뉴욕 금융서비스국은 동 지침을 기반으로 기업의 사이버보안 프로그램을 평가할 것으로 보이며, 동 지침은 다른 규제기관이 AI 사이버보안 위험에 접근하는 방식에 영향을 미칠 것으로 전망됨

Reference

▪https://www.dfs.ny.gov/industry-guidance/industry-letters/il20241016-cyber-risks-ai-and-strategies-combat-related-risks

▪https://www.mayerbrown.com/en/insights/publications/2024/10/new-york-state-department-of-financial-services-issues-industry-letter-on-cybersecurity-risks-arising-from-artificial-intelligence

붙임 뉴욕주 금융서비스국의 「AI에 따른 사이버보안 위험 대응 등을 위한 지침」 세부내용

○ **(정의)** 동 지침은 주요 용어를 「금융 사이버보안 규정」에서 인용함

구분	주요내용
적용대상 (Covered entity)	• 「은행법」, 「보험법」 또는 「금융 서비스법」에 따른 면허, 등록, 헌장, 인증서, 허가, 인증 또는 이와 유사한 승인에 따라 직무를 수행하는 모든 사람
승인된 사용자 (Authorized user)	• 적용대상의 사업 운영에 참여하고 해당 기관의 정보시스템 및 데이터에 액세스하고 사용할 권한이 있는 모든 직원, 계약자, 대리인 또는 기타 사람
사이버보안 이벤트 (Cybersecurity event)	• 정보시스템 또는 해당 정보시스템에 저장된 정보에 대한 무단 액세스, 중단 또는 오용을 얻거나 실패하는 모든 행위 또는 시도
사이버보안 사고 (Cybersecurity incident)	• 해당 기관, 그 계열사 또는 제3자 서비스 제공업체에서 발생한 사이버보안 사고 – 적용대상에 영향을 미치고 해당 주체가 정부 기관, 자율 규제 기관 또는 기타 감독 기관에 통지하도록 요구하는 경우 – 또는 해당 주체의 정상 운영 시 중요부분에 실질적인 해를 끼칠 합리적 가능성이 있는 경우 – 또는 그 결과 해당 주체의 정보시스템의 중요한 부분 내에 랜섬웨어가 배포되는 경우
정보시스템 (Information system)	• 전자 정보의 수집, 처리, 유지 관리, 사용, 공유, 보급 또는 처분을 위해 조직된 개별 전자 정보 리소스 집합 – 산업/프로세스 제어 시스템, 전화 교환 및 민간 지점 교환 시스템, 환경 제어 시스템과 같은 특수 시스템도 포함
미공개정보 (Nonpublic information)	• 공개적으로 사용가능한 정보가 아니며 다음과 같은 모든 전자 정보 – 해당 주체의 사업 관련 정보, 해당 주체의 사업, 운영 또는 보안에 중대한 부정적인 영향을 미칠 수 있는 정보의 변조 또는 무단 공개, 액세스 또는 사용 – 이름, 번호, 개인 표시 또는 기타 식별자로 인해 다음 데이터 요소 중 하나 이상과 함께 해당 개인을 식별하는 데 사용할 수 있는 개인에 관한 모든 정보 · (i) 사회 보장 번호; (ii) 운전 면허증 번호 또는 비운전자 신분증 번호; (iii) 계좌 번호, 신용 카드 또는 직불 카드 번호; (iv) 개인의 금융 계좌에 대한 액세스를 허용하는 보안 코드, 액세스 코드 또는 암호; 또는 (v) 생체 인식 기록 – 연령 또는 성별을 제외하고, 의료 서비스 제공자 또는 개인이 생성하거나 그로부터 파생된 모든 형태 또는 매체의 모든 정보 또는 데이터 · (i) 개인 또는 가족 구성원의 과거, 현재 또는 미래의 신체적, 정신적 또는 행동적 건강 또는 상태; (ii) 개인에 대한 의료 서비스 제공; 또는 (iii) 개인에 대한 의료 서비스 제공에 대한 지불
위험평가 (Risk assessment)	• 조직 운영(임무, 기능, 이미지 및 평판 포함), 조직 자산, 개인, 고객, 소비자, 기타 조직 및 주요기반시설에 대한 사이버보안 위험을 식별, 추정 및 우선순위를 지정하는 프로세스
고위 관리기관 (Senior governing body)	• 이사회(또는 그에 상응하는 위원회) 또는 이에 상응하는 관리기관, 또는 둘 다 존재하지 않는 경우 해당 기관의 사이버 보안 프로그램을 담당하는 해당 기관의 고위 임원 또는 임원
제3자 서비스제공자 (Third-party service provider)	• ▲정부기관이 아니고, ▲적용대상에 대한 서비스 제공을 통해 미공개정보에 대한 액세스를 유지, 처리 또는 기타 방식으로 허용하는 사람

동 지침은 AI와 관련된 사이버보안 위험을 **①사이버위협 행위자의 AI 사용으로 발생하는 위험**과 **②적용대상의 AI 사용 또는 의존으로 발생하는 위험**으로 구분

〈 ① 사이버위협 행위자의 AI 사용 〉	
AI를 활용한 사회공학적 공격기법 (AI-Enabled Social Engineering)	• 금융 서비스 부문에 가장 심각한 위협 중 하나로, **사이버위협 행위자는 AI를 활용해 고도로 설득력 있고 사적이며 정교한 콘텐츠를 생성**할 수 있는 능력을 갖춤 – 위협행위자는 AI를 사용하여, 이메일, 전화, 텍스트, 화상회의 및 온라인 게시물을 통해 특정 개인을 표적으로 삼을 수 있는 사실적 대화형 오디오, 비디오 및 텍스트(딥페이크)를 제작 – 위협행위자는 딥페이크를 통해 미공개정보가 포함된 정보시스템에 액세스하거나 특정 개인의 외모나 목소리를 흉내내어 생체인증 기술을 우회하는데 사용
AI로 고도화된 사이버보안 공격 (AI-Enhanced Cybersecurity Attacks)	• 위협행위자는 AI를 활용하여 **기존 사이버공격의 잠재력, 규모 및 속도를 증폭** – AI는 인간보다 훨씬 신속하게 방대한 양의 정보를 스캔하고 분석하여 보안취약점을 식별하고 악용할 수 있으며, 더 많은 정보시스템에 액세스할 수 있음 · 조직의 정보시스템에 침투한 후 ▲AI를 활용한 악성 소프트웨어 배포, ▲미공개정보 유출, ▲새로운 변종 멀웨어 개발 가속화, ▲보안제어 우회를 통한 탐지회피 가능 – 공개적으로 사용가능한 AI 지원제품 및 서비스 확산이 증가함에 따라, 기술적으로 미숙한 위협행위자가 자체 공격을 시작할 수 있음 · AI 지원배포 속도와 함께 위협행자의 진입장벽이 낮아질 경우 수익성이 있는 금융 서비스 부문에서 사이버 공격의 횟수와 심각성이 증가할 수 있음
〈 ② 적용대상의 AI 사용·의존으로 발생하는 위험 〉	
방대한 양의 미공개정보 노출 또는 절도 (Exposure or Theft of Vast Amounts of Nonpublic Information)	• **미공개정보를 대량으로 유지**하면서 AI를 개발하거나 배포하는 적용대상은 재정적 이익 또는 기타 악의적 목적을 가진 **위협행위자의 표적이 될 가능성**이 높음 – 일부 AI는 생체 인식 데이터를 저장하고 있으며, 위협행위자는 생체 인식 데이터를 훔쳐 권한 있는 사용자를 모방하고 다중인증 체계(MFA)를 우회할 수 있음 – 또한 위협행위자는 생체 인식 데이터를 사용하여 매우 사실적인 딥페이크를 생성할 수 있음
제3자 서비스제공자, 공급업체 및 기타 공급망 의존성으로 취약점 증가 (Increased Vulnerabilities Due to Third-Party, Vendor, and Other Supply Chain Dependencies)	• AI 또는 **AI 통합 제품**을 사용하는 경우 **공급망 취약점 위험증대** – AI 기반 도구 등은 방대한 양의 데이터 수집 및 유지관리에 크게 의존하고, 이러한 데이터 수집 프로세스에는 공급업체 및 제3자 서비스 제공업체와의 협력이 포함되어 있음 – 공급망의 각 연결 지점에는 위협행위자가 악용할 수 있는 잠재적 보안취약점이 존재하고, 결과적으로 사이버보안 사고로 인해 공급망 전체에 광범위한 피해가 발생할 수 있음

동 지침은 **AI 관련 위험을 완화하기 위한 조치**로 「금융 사이버보안 규정」에 따른 ▲위험평가 기반 프로그램 설정, ▲제3자 서비스제공자 및 공급업체 관리, ▲액세스 통제, ▲사이버보안 교육 등을 제시

위험평가 기반 프로그램 설정	
위험평가	• **(방어조치 결정)** 적용대상이 직면한 사이버보안 위험(딥페이크 및 AI가 제기하는 기타 위협 포함)을 고려한 후 방어조치를 결정해야 함
	• **(위험평가 설계)** 적용대상은 다음과 같은 잠재적 취약점 영역에서 AI 관련 위험을 해결해야 함 – 조직 자체의 AI 사용 – 제3자 서비스제공자 및 공급업체가 사용하는 AI 기술 – 정보시스템의 기밀성, 무결성 및 가용성에 위험을 초래할 수 있는 AI 애플리케이션
	• **(업데이트)** 적용대상은 비즈니스 또는 기술의 변경으로 인해 해당 적용대상의 사이버보안 위험 요소에 중대한 변경이 발생할 때마다, 위험평가를 최소 매년 업데이트해야 함
사전예방 조치계획	• 적용대상은 사이버보안 이벤트를 조사 및 완화하고 운영 복원력을 보장하기 위한 사전 예방적 조치가 포함된 계획을 수립, 유지, 관리, 평가해야 함 – 사고 대응, 비즈니스 연속성 및 재해복구 계획을 포함해야 하며, 동 계획에는 AI와 관련된 모든 유형의 사이버보안 이벤트 및 기타 업무중단을 해결하도록 합리적으로 설계해야 함
사이버보안 위험관리	• 고위 관리기관은 사이버보안 문제를 충분한 이해하고, 사이버보안 위험관리 감독을 행사하며, 사이버보안 문제 관리보고서를 정기적으로 수신 및 검토해야 함

제3자 서비스제공자 등 관리정책
• 정보시스템 및/또는 미공개정보에 대한 액세스 권한이 있는 제3자 서비스제공자에 대한 액세스 제어, 암호화, 실사 및 계약 보호에 대한 지침과 관련된 최소 요구사항을 포함해야 함
• 적용대상은 제3자 서비스제공자가 보유한 적용대상의 정보시스템 또는 미공개정보에 직접적인 영향을 미치는 모든 사이버보안 이벤트에 대해 알림을 제공하도록 제3자 서비스제공자에게 요구해야 합
• 또한 제3자 서비스제공자가 AI를 사용하는 경우, 적용대상은 향상된 개인정보보호, 보안 및 기밀 유지 옵션을 활용하기 위한 요구사항을 포함하여 적용대상의 미공개정보에 대한 안전한 사용을 보장해야 함

액세스 통제 정책
• **(다중인증(MFA) 활용)** '다중인증'이란 권한있는 사용자가 세 가지 인증요소 중 두 가지 이상을 사용하여 신원을 인증하도록 요구하는 인증체계로, 무단 액세스 방지에 효과적
• **(추가적인 액세스 통제)** 적용대상은 다중인증 체계로 위협행위자의 무단 액세스를 방지하지 못한 경우 위협행위자의 액세스를 제한하는 추가적인 통제체계를 구축해야 함
• **(액세스 권한 업데이트)** 적용대상은 매년 액세스 권한을 검토하여 각 권한 있는 사용자가 직무기능을 수행하는데 필요한 미공개정보에만 액세스할 수 있는지 확인해야 함

사이버보안 교육	
모든 직원	• 고위 경영진을 포함한 모든 직원에게 ▲AI로 인한 위험, ▲AI와 관련된 위험, ▲AI로 고도화된 사회공학적 기법에 대응하는 방법을 인식하도록 교육을 제공해야 함
사이버보안 담당자	• ▲위협행위자가 사회공학적 공격에서 AI를 사용하는 방법, ▲AI를 사용하여 기존 유형의 사이버공격을 촉진하고 고도화하는 방법, ▲AI를 사용하여 사이버보안을 개선하는 방법을 교육해야 함
제3자 서비스제공자	• ▲AI 시스템을 보호하고 방어하는 방법, ▲AI 시스템을 안전하게 설계·개발하는 방법을 교육해야 함 – 관련 직원이 AI 기반 애플리케이션을 사용할 수 있는 경우, 미공개정보를 공개하지 않도록 쿼리 초안을 작성하는 방법에 대해 교육을 받아야 함

해외 입법 동향

미국 법무부, 「자국민 민감 개인정보 등에 대한 우려국가의 액세스 방지를 위한 잠정규정예고문(NPRM)」 발표

미국 법무부는 「우려국가의 정부 데이터 및 민간 개인정보 액세스 방지에 관한 행정명령 14117호」[1]를 이행하기 위하여 동 「잠정규정예고문[2](NPRM)」을 발표 (2024. 10. 21.)

■ 개요 및 추진배경

○ 바이든 정부는 중국, 북한 등 우려국가의 데이터 수집 및 악용에 대응하기 위한 행정명령 14117호를 발표하였고, 법무부장관은 이를 이행하기 위하여 규제대상 및 범위 등을 구체화한 기준을 제시

- AI 등 첨단 기술을 활용한 대규모 민감 정보분석 및 조작을 통해 스파이 활동, 사이버 작전 등 악의적 활동에 활용될 우려가 증가함에 따라 미국의 국가안보와 외교 정책에 위협이 된다고 판단

〈 바이든 행정부, 적대국의 데이터 수집·거래 위협 등 대응을 위한 규제경과 〉

구분	주요내용
행정명령 13873호[3] ('19.5)	• 미 상무부장관은 외국 적대세력이 설계·개발·제조·공급하는 정보통신 기술 및 서비스(ICTS)의 취득, 수입, 이전, 거래 등 금지
▼	
행정명령 14034호[4] ('21.6)	• 중국 등 외국 적대세력이 소프트웨어 애플리케이션을 통한 기업·개인 등의 방대한 데이터 수집 위협에 대응하기 위하여, 외국 적대세력의 데이터 접근에 대한 추가적인 규제 근거를 마련
▼	
행정명령 14117호 ('24.2)	• 우려국가들의 데이터 수집 및 악용에 대응하기 위한 포괄적 규제 체계 수립을 지시 • 법무부장관에게 구체적인 규제 방안 수립 권한을 위임하고 우려국가 지정 기준을 제시 • 라이선스 제도와 기록 보관 의무 등 세부 규제 수단의 도입 근거를 마련
▼	
법무부 ANPRM[5] 발행 ('24.3)	• 행정명령 14117호의 효과적 이행을 위한 구체적 규제 방안을 제시 • 규제 대상 데이터의 범위와 우려국가 분류 기준을 구체화 • 이해관계자들의 의견수렴을 통해 실효성 있는 규제 방안을 모색

1 Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern(미국인의 대규모 민감 개인정보 및 미국 정부 관련 데이터에 대한 우려 국가들의 접근 방지), 2024.2.28. 발표

2 Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons

3 Securing the Information and Communications Technology and Services Supply Chain

4 Protecting Americans' Sensitive Data from Foreign Adversaries

5 National Security Division; Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern, ANPRM은 잠점규정에 관하여 규정의 필요 여부, 어떤 규정을 개발해야 하는지 등의 의견을 수렴하기 위한 사전통지를 의미

■ 주요내용

○ **(주요 용어)** 동 NPRM에 데이터 거래 행위 금지 등 분류 시 구체적인 기준으로서 사용되는 용어

구분	주요내용
액세스 (Access)	• 데이터 획득, 읽기, 복사, 해독, 편집, 전환, 공개 등 모든 형태의 액세스를 포함한 논리적/물리적 액세스를 포괄하는 광범위한 정의 채택 – 정보시스템, 클라우드, 네트워크 등을 통한 모든 접근 방식을 포괄하며, 전환(divert) 등의 우회적 접근 및 암호화된 데이터에 대한 접근도 규제대상에 포함
민감 개인정보 (Sensitive personal data)	• 미국의 식별 가능한 그룹 또는 개인과 연결될 수 있는 6가지 범주(▲규제대상의 개인 식별자, ▲정확한 지리적 위치 데이터, ▲생체 인식 식별자, ▲인간 게놈 데이터, ▲개인 건강 데이터, ▲개인 금융 데이터) 민감 정보를 정의
대량의 민감 개인정보 (Bulk U.S. sensitive personal data)	• 미국인 관련 민감 정보의 대량 수집/보유에 대한 기준을 설정 – 12개월 동안의 데이터 양을 기준으로 하고, 익명화/암호화된 데이터는 물론 단일 또는 복수의 거래 등을 모두 포함
리스트된 식별자 (Listed identifier)	• 구체적인 8가지 데이터 분류(▲정부 발급 ID 및 계정 번호, ▲금융 계좌 번호 및 PIN, ▲기기/하드웨어 기반 식별자, ▲인구통계/연락처 데이터, ▲광고 식별자, ▲계정 인증 데이터, ▲네트워크 기반 식별자, ▲통화 세부 데이터)를 통해 개인 식별자를 정의
정부 관련 데이터 (Government-related data)	• 정부 시설 위치·현직/전직 정부 직원· 정보군사/정보기관 정보 등 정부 시설 및 인력 데이터를 의미
규제대상 데이터 거래 (Covered data transaction)	• ▲데이터 중개, ▲공급업체 계약, ▲고용 계약, ▲투자 계약의 4가지 유형의 거래가 포함된 정부 관련 데이터나 대량의 민감 개인정보에 대한 접근이 포함된 거래를 뜻함

○ **(우려국가**(Country of concern) **지정)** 법무부장관은 국무부장관과 상무부장관의 동의를 얻어 결정한 바에 따라, 중국, 쿠바, 이란, 북한, 러시아, 베네수엘라 6개국을 지정

– ▲미국의 국가안보 또는 미국인의 안전에 현저히 불리한 행위를 장기간 반복적으로 또는 심각하게 행하고, ▲정부 관련 데이터 또는 대량의 민감 개인정보를 악용하여 미국의 국가안보 또는 미국인의 안전에 해를 가할 위험성이 높은 외국 정부를 뜻함

○ **(규제 대상자)** 우려국가의 소유권, 법적, 물리적 관계 등을 기준으로 규제대상 기업/개인을 정의

– 제3국 거주자나 미국 내 체류자에 대한 예외사항을 명확히하여 규제대상의 범위를 구체화

구분	주요내용
규제대상 기업 (Entity)	• 우려국가나 규제대상자가 직/간접적으로 지분의 50%이상을 소유한 외국기업의 경우, 해외자산관리국(OFAC[6])의 제재 규정을 인용하여 규제대상 기업으로 분류 • 우려국가의 법률에 따라 설립되었거나 주요 사업장을 둔 기업 및 우려국가의 직원/계약자도 규제대상에 포함
규제대상 개인 (Individual)	• 우려국가에 주거주자인 외국인은 규제대상에 해당하나, 제3국에 거주하는 우려국가의 시민은 정부나 규제대상 기업 근무자가 아닌 경우 제외 – 단, 미국 체류자 및 미국의 자회사 근무자는 원칙적으로 제외됨(인종이나 국적이 아닌 우려국가와의 관계를 기준으로 적용)

– **(규제 대상자의 지정 절차)** 법무부장관이 해외자산관리국(OFAC)의 제재대상 지정 절차를 모델로

6 Office of Foreign Assets Control

하여 공개적으로 지정하고, 이를 연방관보 및 웹사이트에 공시

- 이때, 지정은 즉시 효력이 발생하며 연방관보 게재 후에는 이를 인지하였음으로 간주되고, 다른 정부 지정 목록과는 독립적으로 효력을 지님
- 한편, 지정된 대상자는 상황 변화에 따른 재검토나 해제를 요청할 수 있는 행정적 이의제기 절차가 보장

○ **(금지된 거래 및 관련 활동)** 데이터 거래 시 데이터 성격을 위험도에 따라 유형화하고, 규제의 성격을 **'① 전면 거래 금지 〉 ② 제한적 거래행위의 허용 〉 ③ 거래제한조치 예외'**를 단계적으로 분류하고 있음

- **(금지된 데이터 중개 거래)** 국가안보나 미국인에 위협이 될 우려가 있는 데이터의 경우 우려국가나 규제 대상자와의 중개 거래를 전면 금지하는 한편, 데이터 재이전을 방지하기 위한 조치를 명시

구분	주요내용
금지된 데이터 중개 거래	• 우려국가나 규제 대상자와의 직접적인 데이터 중개 거래를 전면 금지하는 한편, 미국인이 우려 대상국 또는 규제 대상자와 데이터 중개 거래 행위를 금지 - 민감 개인정보나 정부 관련 데이터에 대한 접근이 포함된 거래로서, 원 데이터 주체로부터 직접 수집/처리하지 않은 데이터의 거래만 해당(데이터 판매, 접근권한 허가, 데이터 이전 등의 상업적 거래를 포함
기타 금지된 데이터 중개 거래	• 우려국가나 규제 대상자에게 데이터 재이전을 방지하기 위하여, 제3국과의 데이터 중개 거래 시 해당 사항을 계약조항으로 의무화해야 함 - 위반 시 보고의무와 실사 요건을 부과하며, 위반자는 규제 대상자로 지정될 수 있음

- **(제한된 거래행위의 허용) 보안 요건을 준수하는 경우에 한하여** 특정 유형의 거래를 **허용**하는 프레임워크 제시

- 벤더 계약, 고용 계약, 투자 계약의 3가지 거래 유형에 대해 CISA의 보안 요건[7] 및 기타 적용 가능한 요구사항을 준수하는 경우에만 허용되며, 라이선스 없이 다른 위험 완화 조치는 사용 불가

구분	주요내용
벤더 계약	• 고용 계약을 제외한 모든 상품 및 서비스 제공 계약으로서, 클라우드 컴퓨팅 서비스를 포함하여 대가나 기타 보상을 받고 상품이나 서비스를 제공하는 모든 형태의 계약 또는 약정을 의미함 ※ 향후 NIST 정의[8]를 참조한 클라우드 컴퓨팅 관련 세부 지침이 제공될 수 있음
고용 계약	• 독립 계약자를 제외한 모든 형태의 고용 관계로서, 이사회나 위원회 고용, 임원급 약정, 운영 수준의 고용을 포함하여 독립 계약자가 아닌 개인이 대가나 기타 보상을 받고 직접 업무나 직무를 수행하는 모든 계약 또는 약정을 의미
투자 계약	• 미국 내 부동산이나 법인에 대한 소유권 또는 권리 취득 계약으로서, 미국 내 부동산이나 법인에 대한 직간접적 소유권이나 권리를 취득하는 계약을 의미 - 단, 수동적 투자 및 공개 거래 증권, SEC 등록 투자회사 증권, 벤처캐피탈/사모펀드 등에 대한 제한된 파트너로서의 투자, 10% 미만의 의결권/지분 투자, 표준적 소수주주 보호권만을 가지는 투자는 제외

7 CISA 보안요건 주요 구성: 전사적 사이버보안 정책 수립과 위험 관리 체계를 구축, 접근 통제/네트워크 보안/모니터링 체계를 구현, 데이터 최소화/마스킹/암호화 등 기술적 보호 조치를 적용

8 https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

구분	주요내용
법률에 따른 예외대상	• 국제긴급경제권한법(IEEPA)에 따라 법적으로 규제가 면제되는 3가지 기본 거래 유형(▲개인 간 통신, ▲정보 또는 자료, ▲해외 여행 관련 데이터) 등을 정의[9]
미국 정부의 공식 업무	• 정부 직원, 수혜자, 계약자의 공식업무 수행, 정부 기관의 승인된 활동, 정부와의 계약에 따른 거래는 규제 적용대상 예외에 해당
금융 서비스	• 은행, 자본시장, 금융보험 서비스 제공 과정에서 필수적으로 발생하는 데이터 거래 등 금융 서비스 제공에 필수적인 데이터 거래의 경우 예외로 함 (단, 금융 서비스와 직접 관련되지 않은 고용이나 벤더 계약은 제외)
기업그룹 내 거래	• 우려국가에 위치한 자회사나 계열사와의 인사, 급여, 세무 등 일상적 업무 운영을 위한 데이터 거래 등 동일 기업그룹 내 필수적인 운영 시 관련 데이터 거래의 경우 예외대상에 해당
법률/국제협약에 따른 데이터 거래	• 연방법이나 미국이 당사자인 국제협약에 따라 요구되거나 승인된 데이터 거래는 예외로 함 - 단, CBPR[10]이나 EU-US DPF[11]와 같은 일반적인 데이터 전송 관련 협약은 제외
CFIUS[12] 심사 대상 투자 계약	• CFIUS가 거래를 중지시키거나 민감 개인정보 접근과 관련된 위험 완화 조치를 부과한 투자 계약은 중복 규제 방지를 위해 예외로 함
통신 서비스	• 국제 통화, 모바일 음성, 데이터 로밍 등 통신 서비스 제공을 위해 필수적인 데이터 거래는 예외대상에 해당 (단, 고객 데이터의 판매나 접근권 임대는 제외)
의약품/의료기기 인증	• 우려국가에서의 의약품, 생물학적 제제, 의료기기의 시장 승인을 얻거나 유지하는데 필요한 비식별화된 데이터 거래는 예외대상에 해당하나, 이 경우 보고의무가 부과됨
기타 임상시험/시판후 조사	• FDA 규제 대상 임상시험 데이터, 실제 임상 데이터, 시판후 안전성 모니터링 데이터와 관련된 거래는 예외대상이나, 구체적 범위와 조건은 의견수렴을 통해 결정될 예정

○ **(거래제한조치 예외)** 정부의 공식 업무, 법률에 따라 인증·승인되는 경우 등 거래제한조치의 예외로서 분류

○ **(자료제출 및 기록 등 관리조치)** 법무부장관은 데이터 거래 등 엄격한 관리를 위하여 필요 시 자료제출 요구를 수시로 할 수 있으며, 특히 제한된 거래행위의 경우 해당 관련 자료를 상세히 작성 및 보관해야함

- **(자료제출 요구)** 법무부장관은 미국인을 대상으로 금지 또는 제한된 데이터 거래와 관련된 정보를 수시로 요청할 수 있음

- **(기록 및 기록유지 요건)** 제한된 거래행위에 참여하는 미국인은 컴플라이언스 프로그램, 보안 조치 이행 정책, 감사 결과, 실사 문서화 등 거래와 관련된 모든 기록을 정확히 작성해야 함(거래일로부터 10년간 보관해야 함)

- **(연간 보고서 제출)** 클라우드 컴퓨팅 서비스와 관련된 제한된 거래행위에 참여하는 미국인이 우려국가나 규제 대상자가 직/간접적으로 25% 이상의 지분을 보유한 경우, 매년 보고서를 제출해야 함

9 International Emergency Economic Powers Act(국제긴급경제권한법)에서의 개인 간 통신의 자유 (50 U.S.C. 1702(b)(1)) 정보 및 정보 자료의 자유로운 이동 (50 U.S.C. 1702(b)(3)), 여행 관련 거래의 자유 (50 U.S.C. 1702(b)(4))에 따라 정의

10 APEC(아시아•태평양경제협력체) 프라이버시 보호 원칙을 기반으로 기업의 개인정보 보호 체계를 평가하여 인증하는 글로벌 인증제도

11 EU-US Data Privacy Framework. EU에서 DPF에 참여하거나 인증을 받은 미국 내 조직으로 개인 데이터를 전송하기 위한 법적 메커니즘

12 Committee on Foreign Investment in the United States의 약자로 미국 연방정부의 9개 행정부처 장관들을 정규 구성원으로 재무부 장관이 위원장직을 맡고 있는 외국인 투자 위험 평가 조직

- **(금지된 거래 제안 거부 시, 보고의무)** 금지된 거래 제안을 받았으나 이를 거부한 경우, 14영업일 이내에 해당 보고서를 법무부에 제출해야 함

○ **(위반에 대한 처벌)** 허위 진술 및 인증, 데이터 보안 조치 미비, 기록유지 및 보고의무 불이행 등의 경우 처벌대상에 해당하며, 데이터 보안이라는 특수성을 반영한 민사 제재금 부과 절차를 규정 및 기준 제시

- **(제재금 산정)** 2015년 연방 민사처벌 인플레이션 조정법 개선법[13]에 따라 최대 $368,136 또는 위반 거래액의 2배 중 더 큰 금액을 기준으로 부과함

■ 전망 및 시사점

○ 본 규정은 국가안보 관점에서 민감 데이터 보호를 강화하고 우려국가들이 해당 데이터에 접근하는 행위 등을 제한하기 위한 포괄적 규제체계 마련을 목적으로 함

- 현행 데이터 보호 규제는 여러 기관에 분산되어 있어 일관성 있는 관리·감독에 한계가 있으며, 데이터 브로커들의 활동을 효과적으로 규제할 수 있는 포괄적 법적 프레임워크가 부재한 상황

○ 규제 실효성 확보를 위하여, 본 규정에서는 ANPRM 의견수렴 결과를 반영하여 '액세스(access)'의 정의를 명확히 하였음

- ANPRM 의견수렴 과정에서 일부 액세스의 개념 중, '전환(divert)' 용어 삭제 제안이 있었으나, 실제 데이터 접근이 없는 활동도 국가안보에 위험이 될 수 있다는 판단 하에 의도적으로 광범위한 정의를 채택하였음

○ 본 규정은 데이터 브로커, 클라우드 서비스 제공업체 등 관련 기업들의 규제 준수 부담이 증가할 것으로 예상되나, 국가안보 강화라는 정책 목표 달성을 위해 필요한 조치로 평가

Reference

- https://www.justice.gov/opa/pr/justice-department-issues-comprehensive-proposed-rule-addressing-national-security-risks
- https://www.whitehouse.gov/briefing-room/presidential-actions/2024/02/28/executive-order-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern/
- https://www.justice.gov/d9/2024-10/nsd_104_-_data_security_-_1124-aa01_-_notice_of_proposed_rulemaking_0.pdf

13 Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015

해외 입법 동향

미국 교통안전국, 「지표면(Surface)의 사이버위험 관리 강화에 관한 잠정규정예고문」 발표

미국 교통안전국(Transportation Security Administration, 이하 TSA)은 지상교통 및 파이프라인 시스템의 사이버보안 강화를 위하여 동 잠정규정예고문[1](NPRM)을 발표 (2024. 11. 7.)

■ 개요 및 추진배경

○ 중국·러시아·이란 등의 국가 주도 사이버 공격과 랜섬웨어로 인한 주요기반시설 운영 중단 사례가 증가함에 따라, 지상교통 및 파이프라인 시스템에 대한 사이버 위협이 고조되고 있는 상황

- 2021년 5월, 러시아 기반의 사이버범죄 그룹 다크사이드의 랜섬웨어 공격으로 미국 동부 연안 5,500마일의 석유 파이프라인 운영이 일주일간 중단되어 동부 연안 지역에 비상사태 선포

○ 2021년 다크사이드의 공격 이후 TSA는 파이프라인, 화물철도, 여객철도 등 주요기반시설 운영자를 대상으로 ▲사이버보안 코디네이터 지정, ▲사고보고 의무화 등을 포함한 보안지침을 순차적으로 발령

구분	주요내용
2021년 5월	• 파이프라인 사이버보안 지침(SD Pipeline-2021-01)을 발령하여, ▲사이버보안 코디네이터 지정, ▲사이버보안 사고 24시간 내 보고, ▲취약점 평가실시 규정
2021년 7월	• 파이프라인 추가 보안지침(SD Pipeline-2021-02)을 발령하여, ▲랜섬웨어 등 위협대응 조치, ▲사이버보안 사고 대응계획 수립 규정
2021년 12월	• 화물철도 및 여객철도 대상 보안지침 발령(SD 1580-21-01 series, SD 1582-21-01 series) - 본부급 사이버보안 코디네이터를 지정하여, TSA 및 CISA와 24시간 연락체계 구축 - 사이버보안 사고 발생 시 영향받은 시스템, 피해 정도, 대응조치 등을 24시간 이내에 CISA에 보고 - IT/OT 시스템에 대한 사이버보안 사고 대응계획을 수립하고 연 2회 이상의 모의훈련 실시 - 시스템 취약점을 식별하고 개선 조치를 이행하기 위한 사이버보안 취약점 평가 실시
2022년 7월	• 파이프라인 사이버보안 지침을 성과기반 요구사항으로 개정하여 운영자들에게 더 큰 유연성 제공 - 기존의 획일적이고 처방적인 요구사항에서 벗어나 운영자가 자체 운영환경에 맞는 보안조치를 선택 - 새로운 기술과 보안역량을 자유롭게 도입할 수 있게 하면서도 TSA가 요구하는 핵심 보안목표는 유지
2024년 5월	• PTC(Positive Train Control) 시스템을 주요 사이버 시스템으로 포함하도록 철도 보안지침 개정 - PTC는 열차 충돌방지, 과속 탈선방지 등 철도 안전의 핵심 시스템으로, 사이버공격 시 심각한 안전사고로 이어질 수 있음 - 특히 PTC 도입으로 철도 시스템 간 상호연결성이 증가하여 사이버보안 위험도 함께 증가한 상황 반영

○ 국가 사이버보안 전략('23. 3.)에서는 TSA가 파이프라인 및 철도부문에서 자발적인 사이버보안 지침을 수립했음을 언급했지만, 의무요건의 부재로 일관성 없는 결과를 초래하였다는 지적제기

1 Enhancing Surface Cyber Risk Management

- TSA는 기존 보안지침(SD)의 주요 요구사항을 포함하고, 「교통안전법[2]」 및 「9/11위원회권고이행법[3]」에 근거한 동 잠정규정 예고문을 통해 포괄적 규제 프레임워크를 확립

■ 주요내용

(주요 요구사항) 체계적인 위험 관리체계 구축, 투명한 사고 보고체계 확립 등을 통해 지상교통 및 파이프라인 운영자들의 사이버보안 대응역량을 강화하기 위한 포괄적 규제 프레임워크를 제시

○ **(적용대상)** ▲에너지 수송을 위한 파이프라인 소유자 및 운영자, ▲화물·여객철도 등의 소유자 및 운영자, ▲장거리버스(OTRB) 소유자 및 운영자가 규제대상에 해당

○ **(사이버보안 위험관리(CRM[4]) 프로그램)** 조직의 현재 보안수준을 평가하고, 체계적인 이행계획을 수립하여, 지속적으로 모니터링하는 종합적인 위험관리 체계를 구축

구분	주요내용
사이버보안 평가 (Cybersecurity Evaluation)	• 조직의 물리적·논리적 보안 통제현황을 포함한 ▲전반적인 사이버보안 수준을 연간 단위로 평가하고, ▲그 결과를 7일 이내 TSA에 통보하며 ▲TSA의 요청이 있을 경우, 상세 결과를 제출
▼	
사이버보안 운영 이행계획 (Cybersecurity Operational Implementation Plan)	• CRM 프로그램의 거버넌스 구조, 주요 시스템 식별·보호·탐지·모니터링 정책, 사고 대응 절차 등을 포함하여 TSA의 승인을 받고, 취약점 평가 결과에 따른 개선계획을 반영하여 지속적 갱신
▼	
사이버보안 평가계획 (Cybersecurity Assessment Plan)	• 이행계획(COIP) 승인 후 평가계획을 90일 이내에 TSA에 제출 - 2년 주기의 아키텍처 설계 검토와 함께 매년 요구사항의 1/3 이상을 독립적인 평가자가 검토 - 3년 이내 전체 요구사항에 대한 평가를 완료하며 그 결과를 TSA에 보고

○ **(사이버보안 코디네이터 지정)** 사이버보안 위협 대응을 위한 전문성을 갖춘 전담 인력을 지정하여 내·외부 이해관계자와의 효과적인 협력체계를 구축하도록 함

- **(자격요건)** ▲일반적인 사이버보안 지침 및 모범사례, ▲사이버보안 법규, ▲민감 보안정보(Sensitive Security Information, SSI) 등의 취급, ▲해당 조직의 운영 및 시스템에 적용되는 현행 사이버보안 위협에 대한 지식을 보유한 미국 시민권자

- **(주요역할)** ▲TSA와 CISA간의 연중무휴 연락체계 유지, ▲위협정보 공유, ▲국토안보부 보안정보 공유 플랫폼[5](Homeland Security Information Network)을 통한 정보공유, ▲사이버보안 위협 및 사고대응을 위한 법 집행기관간의 협력수행

2 Aviation and Transportation Security Act
3 Implementing Recommendations of the 9/11 Commission Act of 2007
4 Cybersecurity Risk Management
5 미국 국토안보부가 운영하는 보안 정보 공유 플랫폼으로, TSA의 규정에서는 사이버보안 코디네이터가 HSIN 계정을 보유하거나 TSA가 지정한 다른 통신 플랫폼을 활용하여 관련 정보를 공유하도록 요구

○ **(사이버보안 사고 보고)** 사이버보안 사고 발생 시 신속한 상황 전파와 대응을 위해 24시간 이내 상세정보를 CISA에 보고하도록 하는 보고체계를 확립

- **(보고대상)** ▲IT/OT 시스템 무단 액세스, ▲악성 소프트웨어 발견, ▲서비스 거부 공격 등 운영 중단을 초래하거나 그 위험이 있는 모든 사이버보안 사고 포함

- **(보고내용)** ▲보고자 정보 및 연락처, ▲영향받은 시스템·시설 정보, ▲최초 침해 및 탐지 날짜, ▲조치 사항, ▲악성 IP·도메인·멀웨어 등 관련 정보, ▲운영상 실제·잠재적 영향, ▲대응 계획 등을 제출하고 추가정보 확보 시 보완보고

○ **(「주요기반시설 사이버사고보고법(CIRCIA)」과의 조화)** 사이버보안 사고 발생 시 24시간 내 CISA에 보고하여, 위협식별 및 동향분석을 위한 정보통합의 이점을 확보하고 보고체계를 효율화

○ **(사이버보안 교육)** 조직 구성원의 역할과 책임에 따른 맞춤형 교육을 정기적으로 실시하여 전사적 사이버보안 문화 조성

- 사이버보안 운영 이행계획(COIP) 승인 후 60일 내 초기 교육을 실시하고, 신규 직원은 10일 내 교육을 완료하며, 매년 직원의 최초교육 기준 월을 기준으로 재교육을 실시

구분	주요내용
기본 사이버보안 교육	• IT/OT 시스템 액세스 권한이 있는 전 직원을 대상으로 ▲원격 작업 보안, ▲모바일 기기 보안, ▲데이터 관리, ▲정보보안, ▲의심스러운 활동 보고절차 등에 대한 기본적인 보안인식 교육 제공
역할 기반심화 교육	• 일선 직원을 대상으로 ▲사이버보안 운영 이행계획(COIP) 요구사항, ▲계정 및 액세스 관리, ▲서버 및 어플리케이션 관리, ▲위협탐지 및 대응 등 직무 특성에 맞는 전문 교육 제공

(보안통제 요구사항) TSA는 네트워크 분리, 액세스 통제, 공급망 관리 등 핵심적인 보안 통제 요구사항을 제시하여 사이버공격에 대한 예방-탐지-대응-복구의 전 주기적 방어 체계를 구축하고자 함

구분	주요내용
네트워크 분리	• 시스템 간 논리적 분리와 통신 통제를 통해 사이버 공격의 확산을 방지하고 핵심 시스템을 보호하기 위한 심층 방어 체계를 구축
	- IT/OT 시스템을 물리적·논리적으로 분리하여 한쪽 시스템의 침해가 다른 시스템에 영향을 미치지 않도록 차단
	- 업무나 운영에 필수적인 것으로 검증된 통신만을 선별적으로 허용하여 불필요한 시스템 간 접촉을 최소화
	- 영역 간 통신이 필요한 경우 적절한 수준의 암호화 또는 이에 준하는 보안조치를 적용하여 데이터를 보호
	- 허가되지 않은 영역 간의 모든 통신을 기본적으로 차단하여 잠재적 위협 요소를 제거
액세스 통제	• 시스템과 데이터에 대한 액세스를 체계적으로 통제하여 무단 액세스와 권한 남용을 방지하기 위한 종합적인 액세스 관리 체계를 수립
	- 강력한 인증체계와 안전한 패스워드 정책을 수립하여 기본적인 액세스 통제를 강화
	- 중요 시스템에 대해 다중인증을 적용하거나 이에 준하는 보안조치를 통해 인증 체계를 강화
	- 사용자별로 필요 최소한의 권한만을 부여하고 직무 간 권한을 분리하여 관리

구분	주요내용
	- 공유계정의 사용을 필수적인 경우로 제한하고 사용 내역을 지속적으로 모니터링
	- 시스템 간 신뢰 관계를 정기적으로 검토하여 불필요한 액세스 경로를 제거
로깅 정책	• 보안 관련활동을 체계적으로 기록하고 관리하여 보안 사고의 탐지, 분석, 대응을 위한 기반 마련
	- 모든 보안 로그를 보안정보 및 이벤트 관리 도구나 분리된 네트워크의 데이터베이스와 같은 중앙 시스템에 안전하게 저장하고 관리하며, 승인된 인증된 사용자만이 액세스할 수 있도록 통제
	- 승인된 담당자만이 로그에 액세스하고 수정할 수 있도록 액세스를 통제하여 로그의 무결성을 보장하고, 로그 자체가 공격 대상이 되거나 사고 증거가 임의로 삭제되는 것을 방지
	- 보안 사고 조사에 필요한 충분한 기간동안 로그를 보관하여 증거를 확보하고, 위험 분석과 관련 표준 또는 규제 지침에서 요구하는 기간동안 로그를 유지
	- 조직의 위험 분석을 기반으로 규제 요구사항, 저장 공간, 분석 필요성 등을 종합적으로 고려하여 로그의 보관 기간을 합리적으로 설정하고 효율적인 로그 관리 체계를 구축
백업 정책	• 시스템과 데이터의 가용성을 보장하고 사고 발생 시 신속한 복구를 지원하기 위한 체계적인 백업 체계를 구축함
	- 시스템과 데이터의 중요도에 따라 적절한 주기로 백업을 수행하여 중요 데이터의 가용성을 보장
	- 백업 데이터를 원본과 물리적으로 분리하여 보관해 동시 피해를 방지하고 시스템 복구 가능성을 확보
	- 정기적으로 백업 데이터의 무결성을 검증하여 실제 복구 필요 시 사용 가능성을 보장
	- 백업 데이터의 악성코드 감염 여부를 확인한 후 복구를 진행하여 안전한 시스템 복구를 보장
공급망 위험관리	• 제품과 서비스 공급망의 보안 위험을 체계적으로 관리하여 공급망을 통한 보안 위협을 최소화함
	- 공급업체가 사이버보안 사고 발생 시 위험 평가에 필요한 시간 내에 통보하도록 요구
	- 공급업체가 제공하는 제품, 서비스, 기능에 영향을 미치는 보안 취약점이 확인된 경우 위험 평가에 필요한 시간 내에 통보하도록 요구
	- 조달 문서에 사이버보안 요구사항 평가를 포함하여, 비용과 기능이 유사한 경우 더 높은 수준의 사이버보안을 제공하는 제품이나 공급업체를 선호
	- 사이버보안 사고나 취약점 통보 접수 시 주요 사이버 시스템에 대한 위험을 해결하기 위한 완화 조치를 즉시 고려하고 필요한 경우 사이버보안 운영 이행계획(COIP) 개정

■ 전망 및 시사점

○ 이에, TSA는 기존 파이프라인 및 철도 대상 보안지침의 주요 요구사항을 체계화하고, 업계의 의견을 수렴하여 실행가능한 수준의 규제 프레임워크를 제시한 것이 특징

○ 「주요기반시설 사이버사고보고법(CIRCIA)」 제정에 따라 TSA는 중복보고를 방지하기 위하여, CISA 중심의 효율적인 사이버보안 사고보고 및 대응체계 구축

Reference

▪https://www.federalregister.gov/documents/2024/11/07/2024-24704/enhancing-surface-cyber-risk-management

▪https://www.tsa.gov/news/press/releases/2024/11/06/tsa-announces-proposed-rule-would-require-establishment-pipeline-and

해외 입법 동향

미국 연방통신위원회, 「해저케이블 라이센스 관련 잠정규정예고문」 발표

미 연방통신위원회(FCC)는 해저케이블 시스템의 국가 안보 위험에 대응하고 사이버보안 관리를 강화하기 위해 해저케이블 허가 규정 전면 개정안을 담은 규칙제정안(NPRM) 발표 (2024. 10. 31.)

■ 개요

○ FCC는 해저케이블 시스템의 효과적인 사이버보안 관리를 위해 위험 관리 계획 수립, 공급망 보안 관리, 기본 보안 통제 구현 등에 대한 세부 지침을 제시하고, 각 조직의 특성과 환경을 고려한 유연한 적용이 가능하도록 함

○ 신청자 및 면허권자는 NIST CSF 등 검증된 프레임워크를 활용하여 조직의 사이버보안 위험을 식별·평가하고, CIA(기밀성·무결성·가용성) 보장을 위한 구체적 통제방안을 수립해야 하며, 고위 경영진의 직접적인 책임과 감독하에 이를 지속적으로 이행·개선해야 함

■ 주요내용

○ **(사이버보안 위험 관리 계획)** 해저케이블 시스템의 효과적인 보안 관리를 위해 위험 관리 계획은 포괄적이고 체계적인 내용을 담아야 하되, 각 조직의 특성과 환경을 고려한 유연한 적용이 가능하도록 함으로써 실효성 있는 보안 체계 구축을 도모

- (계획 수립의무) 모든 신청자는 조직의 사이버보안 관리를 위한 포괄적인 계획을 마련해야 함

  • (핵심 구성요소) 조직이 직면한 사이버 위험의 식별 및 평가, 위험 완화를 위한 통제방안 수립, 통제의 효과적 적용을 위한 실행계획 등을 포함

  • (이행의무) 계획의 수립뿐 아니라 실제 이행과 정기적 업데이트를 통한 지속적 개선이 요구됨

- (계획 필수 포함사항) 위험 관리 계획은 조직의 전반적인 보안 관리를 위한 핵심 요소들을 포함해야 하며, 이는 체계적이고 포괄적인 접근 방식을 통해 구현되어야 함

  • (위험식별 및 대응) 조직이 직면한 사이버 위험의 식별 및 평가 방법론을 시작으로, 식별된 위험에 대한 구체적 통제 방안과 완화 전략을 제시하고, 이러한 통제의 효과적 적용을 위한 실행 계획과 모니터링 체계를 마련해야 함

• (보안 운영체계) 시스템과 서비스의 CIA(기밀성·무결성·가용성) 보장을 위한 조직 자원과 프로세스 활용 방안을 상세히 기술하고, 보안 통제의 효과성을 주기적으로 평가하고 개선하기 위한 방법론을 포함

- (유연성 보장) 조직별 특성을 고려한 효과적인 보안 체계 구축을 위해 계획 수립의 유연성을 보장하되, 기본적인 보안 요구사항은 반드시 충족되어야 함

• (기본 원칙) NIST 사이버보안 프레임워크(CSF)[1]와 같은 검증된 위험 관리 체계를 활용하되, 자사의 규모와 특성에 맞는 맞춤형 계획을 수립할 수 있음

• (이행 요건) 위험 분석과 보안태세 개선을 위한 실질적 조치를 반드시 입증해야 하며, 계획의 정기적 검토와 업데이트를 통한 지속적 개선이 이루어져야 함. 이러한 유연한 접근방식은 대기업부터 소기업까지 모든 규모의 기업이 적용가능한 방식으로 설계됨

- (고위 경영진 인증) 계획의 실효성 확보를 위해 고위 경영진의 직접적인 책임과 감독이 요구되고 CEO, CFO, CTO 또는 이에 준하는 조직의 보안 거버넌스 책임자의 서명이 필수

• (배경) 사이버안전검토위원회(Cyber Safety Review Board)[2]의 Microsoft 사례 조사 결과를 반영, 경영진 차원의 엄격한 위험 관리와 보안 중심 의사결정 강화 필요성이 강조됨

○ **(공급망 사이버보안 위험 관리)** 해저케이블 시스템의 안전한 운영을 위해서는 공급망 전반에 걸친 체계적인 사이버보안 위험 관리가 필수적이며, 이를 위한 구체적인 계획 수립과 실행이 요구됨

- (계획 수립범위) 해저케이블 시스템과 관련된 전체 공급망에서 발생할 수 있는 사이버보안 위험에 대한 포괄적인 관리계획 수립 필요

• (위험평가) 공급망 내 주요 구성요소별 사이버보안 위험을 체계적으로 식별하고 평가하는 프로세스 구축

• (완화전략) 식별된 위험에 대한 구체적인 완화 방안과 대응 절차를 수립하고 이의 효과성을 정기적으로 검증

• (모니터링) 공급망 전반에 걸친 지속적인 위험 모니터링 체계 구축 및 운영

- (모범사례 적용) NIST에서 제시하는 공급망 위험 관리 모범사례를 기반으로 한 체계적인 접근 필요

• (프레임워크 활용) NIST의 'Key Practices in Cyber Supply Chain Risk Management[3]' 및 'Cybersecurity Supply Chain Risk Management Practices[4]' 지침 참조

1 NIST가 개발한 조직의 사이버보안 위험을 관리하기 위한 자발적 지침으로, 주요 기능은 식별(Identify), 보호(Protect), 탐지(Detect), 대응(Respond), 복구(Recover)로 구성

2 미국 국토안보부 산하 위원회로, 주요 사이버사고를 조사하고 분석하여 교훈과 권고사항을 도출하는 역할 수행

3 NISTIR 8276. 산업계 관찰을 통해 도출된 공급망 사이버보안 위험 관리의 핵심 실무지침으로, 공급업체 평가 및 선정 프로세스 구축, 공급업체와의 계약 시 보안 요구사항 명시, 공급망 전반의 지속적인 모니터링 및 평가, 취약점 관리 및 인시던트 대응 계획 수립, 공급망 투명성 확보를 위한 정보공유 등이 주요 내용

4 NIST SP 800-161. 조직의 공급망 사이버보안 위험 관리를 위한 상세 프레임워크로, ▲기본 프레임워크: 식별(Identify), 보호(Protect),

- (산업 표준) 통신 산업 특성을 고려한 공급망 보안 표준 및 모범 사례의 적극적 도입
- (검증 체계) 공급망 참여자들의 보안 수준을 주기적으로 평가하고 검증하는 체계 구축

– (독립 계획 수립) Enhanced A-CAM[5] 및 5G Fund 프로그램[6]의 사례를 참고하여 별도의 공급망 위험 관리 계획 수립 검토

- (계획 독립성) 일반적인 사이버보안 위험 관리 계획과는 별도로 공급망에 특화된 독립적인 위험 관리 계획 수립
- (세부 요구사항) 공급망 참여자 평가, 보안 요구사항 정의, 지속적인 모니터링 방안 등 구체적 실행 방안 포함
- (이행 검증) 계획의 실효성 있는 이행을 위한 구체적인 검증 체계와 평가 지표 마련

○ **(보안 통제구현 요건)** 해저케이블 시스템의 안전한 운영을 위해서는 CIA(기밀성·무결성·가용성)를 보장하기 위한 구체적인 보안 통제가 필수적이며, 이를 위한 체계적인 구현 방안과 검증된 모범 사례의 도입이 요구됨

– (기본 보안 통제) 시스템과 서비스의 CIA 보장을 위한 필수적인 보안 통제 구현이 요구됨

- (기밀성 보장) 민감 정보에 대한 접근 통제, 암호화, 보안 정책 수립 등 구현
- (무결성 확보) 데이터 변조 방지, 로그 관리, 감사 체계 구축 등 이행
- (가용성 유지) 시스템 이중화, 장애 복구 계획, 성능 모니터링 등 실현

– (모범 사례 활용) 검증된 보안 프레임워크 및 모범 사례의 적극적 도입 권장

- (CISA CPG 활용) Cross-Sector Cybersecurity Performance Goals[7]의 산업 공통 보안 목표 적용, 주요 통제 영역별 구체적 성과 지표 설정 및 정기적인 성과 평가 및 개선 체계 운영
- (CIS Controls[8] 적용) Center for Internet Security의 핵심 보안 통제 기준 도입으로 조직 규모별 맞춤형 통제 수준 설정 및 단계적 이행 계획 수립 및 실행

탐지(Detect), 대응(Respond), 복구(Recover) ▲위험 관리 생명주기: 프레임워크, 구현, 모니터링 ▲통제 카탈로그: 17개 통제 패밀리에 걸친 상세 보안 통제 항목 등으로 구성

5 NIST CSF 기반의 사이버보안 위험 관리 계획 의무화, 별도의 공급망 위험 관리 계획(Supply Chain Risk Management Plan) 요구, 정기적인 계획 업데이트 및 이행 현황 보고 필수

6 NIST CSF 기반 사이버보안 계획 수립 의무, 독립된 공급망 보안 관리 체계 구축 필요, 정기적인 보안 평가 및 보고 체계 운영

7 CISA에서 개발한 산업 분야 공통의 사이버보안 성과 목표로, 모든 중요 기반시설 분야에 적용 가능한 기본적인 사이버보안 통제 항목과 성과 지표를 제시

8 사이버보안 모범 사례 모음. 조직의 규모와 특성에 따라 단계별로 적용할 수 있는 실용적인 보안 통제 항목들을 제공

- (6대 필수 통제) 기본적인 보안 수준 확보를 위한 핵심 통제의 의무적 구현

  • (계정 보안) 사용자 계정의 안전한 관리를 위해 기본 패스워드의 즉각적인 변경과 다중 인증 등 강화된 인증 체계의 도입 추진

  • (시스템 보안) 시스템의 안정적인 운영과 보안 강화를 위한 정기적인 보안 업데이트 적용 및 방화벽 설정의 체계적 관리 수행

  • (네트워크 보안) 안전한 네트워크 환경 구축을 위한 네트워크 영역 분리와 접근 제어 정책의 수립 및 시행

  • (기타 통제) 노후 장비의 체계적인 교체 계획 수립과 민감 정보의 안전한 폐기를 포함한 전반적인 보안 관리 체계의 확립

○ **(무료/저비용 보안 리소스 활용)** 해저케이블 시스템의 보안 강화를 위해 활용 가능한 다양한 무료/저비용 리소스가 존재하며, 이를 통해 외부 전문가 고용 없이도 보안 통제 구현이 가능함

- (NIST 보안 지침) 조직의 보안 통제 수준 측정 및 개선을 위한 종합적 지침 제공

  • 랜섬웨어, 멀웨어, 악성코드, 스파이웨어 등 최신 위협에 대한 동향 분석과 예방-탐지-대응-복구 단계별 가이드라인, 실제 사례 기반의 대응 절차, 조직 규모별 맞춤형 보안 통제 방안을 포함하는 포괄적 사이버 위협 대응 지침을 제공함

  • DDoS 공격과 피싱 대응, 네트워크 트래픽 모니터링, 접근 통제, 권한 관리, 모바일 기기 보안 등 네트워크 및 시스템 전반의 보안 관리를 위한 기술적 프레임워크와 정책 수립 지침을 제시함

  • 보안 성숙도 평가 모델, 위험 평가/관리 프레임워크, KPI 기반 측정 체계, 단계적 개선 로드맵 등을 통해 조직의 보안 수준을 객관적으로 진단하고 지속적으로 개선할 수 있는 방법론을 제공함

- (CISA 무료 서비스) 주요 기반시설 사업자 대상 보안 서비스 제공

  • 정기적인 네트워크/시스템/애플리케이션 취약점 점검, 상세 분석 보고서 제공, 위험도 기반 조치 권고, 이행 지원 등을 포함하는 종합적인 무료 취약점 진단 및 관리 서비스를 제공함

  • CPG 기반의 평가 교육, 산업별 특화 위험 평가, 실무 중심의 보안 통제 구현 가이드, 전문가 멘토링, 지역 커뮤니티 구축 등을 통해 체계적인 사이버보안 역량 강화를 지원함

- (추가 공공 리소스) 기존 직원과 기술 계약업체가 활용 가능한 다양한 공개 리소스 존재

  • 상세 구현 가이드, 아키텍처 설계 템플릿, 정책/절차 샘플, 오픈소스 보안 도구, 로그 분석/모니터링 솔루션 등 실무에 즉시 활용 가능한 기술 문서와 도구를 제공함

- 위험 평가 매트릭스, 사고 대응 계획, 업무 연속성/재해 복구 계획, 위기 커뮤니케이션 체계 등 조직의 전반적인 위험 관리와 사고 대응을 위한 프레임워크를 제시함

- 일반 직원의 보안 인식부터 관리자의 보안 리더십, 실무자의 기술 역량에 이르는 다양한 수준의 교육 콘텐츠와 모의훈련 시나리오, 온라인 학습 플랫폼 활용 방안을 포함하는 종합적인 보안 교육 체계를 제공함

○ **(위험관리 계획 제출 및 데이터 보존 체계)** 해저케이블 시스템의 위험관리를 위한 계획 제출 의무와 관련 데이터의 체계적 보존에 관한 요구사항을 규정하여 시스템 보안의 지속성과 투명성을 보장함

– (계획 제출 의무) 위험관리 계획의 체계적 검토를 위한 제출 체계 수립

- 위원회가 요청할 경우 신청자 및 면허권자는 해당 시스템의 보안 위험 분석, 완화 조치, 구현 방법이 상세히 기술된 위험관리 계획을 즉시 제출해야 함

- OIA[9]는 PSHSB[10]와의 협력을 통해 특정 계획의 검토 필요성을 판단하고 계획의 적절성을 평가할 수 있는 재량권을 보유하며, 필요시 계획의 수정이나 보완을 요구할 수 있음

- 제출된 계획은 위원회의 규정 및 보안 요구사항 준수 여부를 확인하기 위한 종합적 검토의 대상이 되며, 미흡사항 발견시 시정 조치가 요구됨

– (데이터 보존 요건) 위험관리 계획 관련 데이터의 체계적 보존 체계 구축(para. 117)

- 신청자 및 면허권자는 위험관리 계획 인증 제출일로부터 최소 2년간 모든 관련 데이터와 기록을 체계적으로 보존해야 하며, 요청시 즉시 제출이 가능하도록 관리해야 함

- 보존 대상에는 위험 평가 결과, 보안 조치 이행 증빙, 모니터링 기록 등 계획의 수립과 구현 과정을 입증할 수 있는 모든 문서와 데이터가 포함되어야 함

- 체계적인 데이터 관리 시스템을 구축하여 계획의 지속적 이행 현황과 보안 조치의 효과성을 상시 검증할 수 있어야 하며, 주기적인 평가와 개선이 이루어져야 함

○ **(제3자 계약업체 관리 체계)** 해저케이블 시스템의 제3자 계약업체가 제공하는 시스템 및 서비스에 대한 보안 관리와 책임 소재에 관한 요구사항을 규정함

– (계획 포함의무) 제3자 계약업체의 시스템 및 서비스에 대한 위험관리 계획을 포함하고 신청자가 제3자 계약업체를 통해 시스템이나 서비스를 제공받는 경우, 해당 업체의 보안 관리 체계와 위험 요소를 상세히 분석하여 위험관리 계획에 반드시 포함해야 함

9 Office of International Affairs. FCC의 국제 업무를 담당하는 부서로, 국제 통신 정책과 규제 관련 업무를 수행
10 Public Safety and Homeland Security Bureau. FCC의 공공안전 및 국토안보국. 통신 기반시설의 보안과 복원력 강화를 위한 정책을 담당

- 제3자가 제공하는 모든 시스템과 서비스에 대한 구체적인 보안 요구사항, 모니터링 방안, 보안사고 대응 절차 등이 계획에 명확히 명시되어야 함

- 제3자의 시스템과 서비스에 대한 접근 통제, 취약점 관리, 보안 감사 등 포괄적인 보안 통제 체계를 수립하고 지속적으로 운영해야 함

– (책임소재) 제3자 계약업체 관련 보안 문제에 대한 책임 규정

- 제3자 계약업체의 고의 또는 과실로 인한 모든 보안 사고와 위반 사항에 대해 신청자가 최종적인 법적, 행정적 책임을 지며, 이는 계약상의 면책 조항과 관계없이 적용됨

- 신청자는 제3자의 비합리적 행위나 실수로 인한 시스템/서비스의 보안 훼손 발생시, 즉각적인 조치와 복구를 수행해야 하며 관련된 모든 피해에 대해 책임져야 함

- 제3자 관리에 대한 신청자의 포괄적 책임 원칙을 명확히 하여, 계약업체 선정부터 관리, 감독에 이르는 전 과정에서 충분한 주의의무를 다하도록 함

■ 전망 및 시사점

○ FCC의 해저케이블 시스템 관련 규제 개편은 사이버보안 위험 관리를 더욱 강화하는 방향으로 진행될 전망이며, 특히 SLTE 소유·운영자, IRU 보유자 등으로 허가 대상을 확대하고 허가 기간을 단축하는 등 관리·감독이 강화될 것으로 예상됨

○ 사이버보안 위험 관리 계획은 각 조직의 특성과 환경에 맞게 유연하게 수립·이행할 수 있도록 하되, NIST CSF 등 검증된 프레임워크 활용을 의무화하고 고위 경영진의 책임을 강화함으로써 보안 거버넌스의 실효성을 제고하고자 함

○ 2024년 대선 이후 FCC 리더십 변화에 따라 규제 개편의 우선순위와 세부 이행 방안이 조정될 가능성이 있으나, 해저케이블 보안이 초당적 이슈라는 점을 고려할 때 사이버보안 위험 관리 강화라는 큰 방향성은 유지될 것으로 전망됨

Reference

▪https://docs.fcc.gov/public/attachments/FCC-24-119A1.pdf
▪https://www.gtlaw.com/en/insights/2024/11/fcc-aims-to-overhaul-subsea-cable-regulations

EU

해외 입법 동향

EU 집행위원회, 「NIS2 지침」 이행규정 초안에 대한 의견수렴

EU 집행위원회는 「NIS2 지침[11]」에 열거된 다양한 디지털 서비스 제공자에 대한 사이버보안 위험관리 조치의 기술 및 방법론적 요구사항을 규정하고, 규정 초안[12]에 대한 의견수렴 (2024. 6. 27.)

■ 개요 및 추진배경

○ **(배경)** EU 집행위원회는 회원국의 사이버보안 수준을 향상하기 위한 「NIS2 지침」을 채택한 이후, 동 지침을 구체화하고 실질적으로 이행할 수 있도록 이행규정(Implementing Regulation[13])을 마련

- **(「NIS2 지침」)** 필수·중요조직이 효과적인 사이버보안 위험관리 시스템을 운영하고, 중대한 사이버사고가 발생한 경우 관련 당국에 보고하도록 요구

  · **(적용대상)** 공공 전자통신 서비스 제공자, 디지털 서비스, 폐수 및 폐기물 관리, 필수제품 제조, 우편 및 택배 서비스, 공공 행정 등 경제와 사회 전반에서 중요한 기능을 수행하는 중대형 기업

○ EU 집행위원회는 **「NIS2 지침」의 위임에 따라 동 이행규정을 마련**하였고, 디지털 기반시설, 디지털 서비스 공급업체, ICT 서비스 관리(기업 간) 부문에 대한 사이버보안 위험관리 조치의 기술 및 방법론적 요구사항을 구체적으로 정비

○ 동 규정안은 '중대한 사고(Significant Incidents)'의 정의를 명확히 하고, **각 디지털 서비스 유형별로 구체적인 중대한 사고의 기준을 제시**하는 것을 주요 내용으로 함

- 중대한 사고의 기준에는 ▲재정적 손실 ▲평판 손상 ▲데이터 유출 ▲인명 피해 등이 포함

11 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

12 COMMISSION IMPLEMENTING REGULATION (EU) …/... of XXX laying down rules for the application of Directive (EU) 2022/2555

13 회원국들이 유럽 법률을 일괄적으로 이행하는 것을 보장하기 위하여, 추가 조치가 요구되는 경우에만 이행규정이 발행될 수 있음. 따라서 이행규정의 내용은 일괄적인 이행을 보장하기 위한 내용으로 제한되어 추가, 보완, 인접 규칙을 새로이 설정할 수 없음. 이행규정은 매우 구체적인 정책을 다루거나 종종 매우 기술적인 세부사항을 다룸. [출처] https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vkh7cggewpvt

■ 주요내용

다양한 디지털 서비스 제공자들이 사이버보안 사고를 정의하고, 대응하기 위한 명확한 기준 제시

○ **(중대한 사고(Significant Incidents)** ▲재정적 손실, ▲평판 손상, ▲데이터 유출, ▲인명 피해 등 여러 기준을 제시

중대한 사고 유형
• 관련 기관에 **10만 유로 또는 연간 매출의 5% 중 더 적은 금액**을 초과하는 **재정적 손실**이 발생했거나 발생할 수 있는 경우
• 관련 기관에 **평판 손상**이 발생했거나 발생할 수 있는 경우
• (EU)2016/943[14]의 제2조제1항제1호에 정의된 **영업 비밀이 유출**되었거나 유출될 수 있는 경우
• **자연인의 사망**이 발생했거나 발생할 수 있는 경우
• **자연인의 건강**에 상당한 손상이 발생했거나 발생할 수 있는 경우
• 네트워크 및 정보 **시스템**에 대한 **악의적**이고 **무단**으로 의심되는 **액세스**가 성공적으로 발생한 경우
• **반복 사고** 기준에 해당하는 경우
• 디지털 서비스 **유형별 중대한 사고 기준**을 충족하는 경우

○ **(평판 손상)** 관련 조직이 평판 손상을 판단함에 있어 ▲언론보도, ▲불만사항 발생, ▲요구사항 불이행, ▲고객 이탈 가능성 등 네 가지 기준을 고려하도록 함

평판 손상의 기준
• 사고가 **언론에 보도**된 경우
• 사고로 인하여, **다른 사용자 또는 중요한 비즈니스 관계로부터 불만사항이 발생**한 경우
• 관련 조직이 사고로 인하여, **규제 요구사항을 충족할 수 없거나 충족할 수 없을 가능성**이 있는 경우
• 관련 조직이 사고로 인하여, **비즈니스에 중대한 영향을 받아 고객을 잃을 가능성**이 있는 경우

○ **(반복 사고(Recurring Incidents)** ▲6개월 이내에 최소 2회 발생하고, ▲명백하고 근본적인 원인에서 동일하게 기인한 사고들을 집합하여 중대한 사고로 간주

○ **(서비스별 중대한 사고)** 각 디지털 서비스 유형별로 구체적인 중대한 사고 기준을 제시

구분	주요내용
도메인 네임 시스템 (DNS) 서비스	• 재귀적(Recursive)이거나 신뢰할 수 있는(Authoritative) 도메인 네임 분석(Domain name resolution)[15] 서비스에 대하여, 10분을 초과하여 완전히 사용할 수 없는 경우
	• DNS 요청에 대한 재귀적이거나 신뢰할 수 있는 도메인 네임 분석 서비스 평균 응답시간이 10분을 초과하는 경우가 1시간을 초과할 때
	• 저장, 전송 또는 처리된 데이터의 무결성, 기밀성, 진본성이 훼손된 경우 ※ DNS 서비스 제공자가 관리하는 1,000개 미만의 도메인 네임 데이터가 DNS 서비스 제공자가 관리하는 도메인 네임의 1% 미만인 경우 제외
최상위 도메인(TLD) 네임 등록 서비스	• 신뢰할 수 있는 도메인 네임 분석(Domain name resolution) 서비스를 완전히 사용할 수 없는 경우
	• DNS 요청에 대한 신뢰할 수 있는 도메인 네임 분석 서비스 평균 응답시간이 10초를 초과하는 경우가 1시간을 초과할 때
	• 저장, 전송 또는 처리된 데이터의 무결성, 기밀성, 진본성이 훼손된 경우

14 미공개 노하우 및 기업정보(영업비밀)의 불법 취득, 사용 및 공개로부터의 보호에 관한 유럽연합(EU) 지침

구분	주요내용
클라우드 컴퓨팅 서비스	• 제공된 서비스 중 하나 이상이 10분을 초과하여 완전히 사용할 수 없는 경우 • 연합 내 서비스 사용자의 5% 또는 100만 명 초과 중 더 적은 수의 SLA(Service Level Agreement)[16]가 충족되지 않은 경우가 1시간을 초과할 때 • 연합 내 서비스 사용자의 5% 또는 100만 명 초과 중 더 적은 수에 대하여, SLA(Service Level Agreemnet)가 체결되지 않은 서비스의 가용성이 제한되는 경우가 1시간을 초과할 때 • 저장, 전송 또는 처리된 데이터의 무결성, 기밀성 또는 진본성이 악의적인 것으로 의심되는 행동의 결과로 손상된 경우 • 저장, 전송 또는 처리되는 데이터의 무결성, 기밀성 또는 진본성이 손상되어 연합 내 서비스 사용자의 5%를 초과한 인원에 영향을 미치는 경우
데이터센터 서비스	• 제공된 서비스 중 하나 이상을 완전히 사용할 수 없는 경우 • SLA(Service Level Agreement)가 충족되지 않은 경우가 1시간을 초과할 때 • SLA(Service Level Agreement)가 악의적인 것으로 의심되는 행동의 결과로 충족되지 않은 경우 • 저장, 전송 또는 처리된 데이터의 무결성, 기밀성 또는 진본성이 악의적인 것으로 의심되는 행동의 결과로 손상된 경우 • 데이터센터에 대한 물리적 액세스가 손상된 경우
콘텐츠 전송 네트워크 서비스, 관리형 (보안) 서비스	• 제공된 서비스 중 하나 이상을 10분을 초과하여 완전히 사용할 수 없는 경우 • 연합 내 서비스 사용자의 5% 또는 100만 명 초과 중 더 적은 수의 SLA(Service Level Agreement)가 충족되지 않은 경우가 1시간을 초과할 때 • SLA(Service Level Agreement)가 체결되지 않은 서비스의 가용성이 사고의 영향을 받는 경우 • 저장, 전송 또는 처리된 데이터의 무결성, 기밀성 또는 진본성이 악의적인 것으로 의심되는 행동의 결과로 손상된 경우 • 저장, 전송 또는 처리되는 데이터의 무결성, 기밀성 또는 진본성이 손상되어 연합 내 서비스 사용자의 5%를 초과한 인원에 영향을 미치는 경우
신뢰 서비스[17]	• 서비스 또는 그 기능의 일부에 대하여, 10분을 초과하여 완전히 사용할 수 없는 경우 • 서비스 또는 그 기능의 일부를 사용자가 일주일 단위로 1시간을 초과하여 사용할 수 없는 경우 • 연합 내 사용자의 1%를 초과한 인원이 서비스 응답시간 지연에 크게 영향을 받는 경우 • 네트워크 및 정보 시스템의 물리적 접근 또는 물리적 접근 보호가 손상되는 경우 • 저장, 전송 또는 처리되는 데이터의 무결성, 기밀성 또는 진본성이 손상되어 연합 내 서비스 사용자의 1%를 초과한 인원에 영향을 미치는 경우
온라인 마켓 서비스, 온라인 검색엔진 서비스, SNS 플랫폼 서비스	• 연합 내 사용자의 5% 또는 100만 명 초과 중 더 적은 수가 서비스 또는 그 기능의 일부를 완전히 사용할 수 없는 경우 • 연합 내 사용자 5% 또는 100만 명 초과 중 더 적은 수가 대규모 지연의 영향을 받는 경우 • 저장, 전송 또는 처리된 데이터의 무결성, 기밀성 또는 진본성이 악의적인 것으로 의심되는 행동의 결과로 손상된 경우 • 저장, 전송 또는 처리되는 데이터의 무결성, 기밀성 또는 진본성이 손상되어 연합 내 서비스 사용자의 5%를 초과한 인원에 영향을 미치는 경우

15 기호명(Symbolic Name)을 숫자 주소로 변화하는 작업. TCP/IP 네트워크에서는 도메인 네임 시스템(DNS)으로 네트워크나 주 컴퓨터에 기호명을 기계가 사용하는 숫자 주소인 IP 주소로 변화해 줌. 이러한 변환 역할 컴퓨터를 도메인 네임 서버(DNS)라고 함
[출처] https://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=049884-1 참고

16 '서비스 수준 계약', 고객이 공급업체에게 기대하는 서비스 수준을 기술한 문서로, 제공될 서비스, 기대되는 성능 수준, 성능 측정 및 승인 방법, 성능 수준이 충족되지 않을 경우의 조치 등을 설명함
[출처] https://www.ibm.com/kr-ko/topics/service-level-agreement

17 공개키를 등록하는 것 또는 키 검증 위치를 포함하여, 키 정보 서비스를 제공할 수 있는 서비스
[출처] https://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=094252-1 참고

○ **(시행)** 관보에 게재된 날로부터 20일째 되는 날에 시행하고, 2024년 10월 18일부터 적용 예정

○ **(의견수렴)** EU 집행위원회는 규정 초안에 대하여, 2024년 6월 27일부터 7월 25일까지 4주간 의견수렴 진행

■ 전망 및 시사점

○ 본 이행규정은 구체적으로 중대한 사고의 기준을 제시하여, 디지털 서비스 제공자들의 사이버보안 투자와 관심이 증가하고 디지털 서비스의 안정성 및 신뢰성이 향상될 것으로 기대

- 중대한 사고의 기준에는 사용자에게 미치는 영향이 포함되어 디지털 서비스 제공자들이 사용자 보호에 더 많은 주의를 기울일 것으로 전망됨에 따라, 개인정보보호와 서비스 안정성 측면에서 사용자에게 긍정적 영향을 미칠 것으로 예상

○ 이행규정을 준수하기 위해 기업들은 추가적인 보안 시스템 구축과 인력 확보가 필요할 것으로 예상되어 단기적으로 비용 부담이 가중될 우려가 있음

- 그러나, 규정 준수를 위한 기업들의 투자 증가로 사이버보안 관련 산업이 성장할 것으로 예상되며, 이는 새로운 일자리 창출과 기술 혁신으로 이어질 것으로 보임

Reference

▪https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14241-Cybersecurity-risk-management-reporting-obligations-for-digital-infrastructure-providers-and-ICT-service-managers_en

▪https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14241-Rules-specifying-the-obligations-laid-down-in-Articles-21-5-and-23-11-of-the-NIS-2-Directive_en

▪https://digital-strategy.ec.europa.eu/en/news/commission-seeks-feedback-draft-implementing-act-under-nis2-directive

해외 단신

EU 집행위원회, 「연합 전체의 높은 공통 수준의 사이버보안 조치에 관한 지침 (NIS2 지침)」 이행규정 채택

○ **(개요)** EU 집행위원회는 「NIS2 지침」을 구체화하고 실질적으로 적용하기 위한 이행규정(Implementing Regulation) 초안을 발표하고 ('24. 06. 27.) 4주간의 의견수렴을 거쳐 채택 ('24. 10. 17.)

- 채택된 이행규정은 별도의 제정 절차 없이 관보에 게재된 날로부터 20일 후 발효됨

○ **(주요내용)** 채택안은 초안에 제시된 '중대한 사고(Significant Incidents)'의 기준 중 **평판손상을 삭제**하고, 각 디지털 서비스 **유형별 중대한 사고의 기준을 수정**

〈 **중대한 사고(Significant Incidents)의 기준** 〉

[초안] 중대한 사고 유형 ※ 자세한 내용은 인터넷·정보보호 법제동향 제202호('24.7.) 참고	[채택안] 중대한 사고 유형
• **10만 유로 또는 연간 매출의 5% 중 낮은 금액**을 초과하는 **재정적 손실**이 발생했거나 발생할 수 있는 경우 • 관련 기관에 **평판 손상**이 발생했거나 발생할 수 있는 경우 • (EU)2016/943[1]의 제2조제1항제1호에 정의된 **영업 비밀이 유출**되었거나 유출될 수 있는 경우 • **자연인의 사망**을 초래했거나 초래할 수 있는 경우 • **자연인의 건강**에 상당한 손상을 초래했거나 초래할 수 있는 경우 • 네트워크 및 정보 **시스템**에 대한 **악의적**이고 **무단**으로 의심되는 **액세스**가 성공적으로 발생한 경우 • **반복 사고** 기준에 해당하는 경우 • 디지털 서비스 **유형별 중대한 사고 기준**을 충족하는 경우	• **50만 유로 또는 연간 매출의 5% 중 낮은 금액**을 초과하는 **재정적 손실**이 발생했거나 발생할 수 있는 경우 • **〈삭 제〉** • (EU)2016/943의 제2조제1항제1호에 정의된 **영업 비밀이 유출**되었거나 유출될 수 있는 경우 • **자연인의 사망**을 초래했거나 초래할 수 있는 경우 • **자연인의 건강**에 상당한 손상을 초래했거나 초래할 수 있는 경우 • 네트워크 및 정보 **시스템**에 대한 **악의적 무단 액세스가 의심되고 심각한 운영상 방해를 초래할 수 있는 경우** • **반복 사고** 기준에 해당하고, **사고로 인한 재정적 손실이 첫 번째 기준을 충족하는 경우** • 디지털 서비스 **유형별 중대한 사고 기준**을 충족하는 경우

- **(서비스별 중대한 사고)** 각 디지털 서비스 유형별로 구체적인 중대한 사고 기준을 수정

구분	주요내용
도메인 네임 시스템 (DNS) 서비스	• 재귀적(Recursive)이거나 신뢰할 수 있는(Authoritative) 도메인 네임 분석(Domain name resolution) 서비스에 대하여, **30분** 이상 초과하여 완전히 사용할 수 없는 경우
	• 1시간을 초과하여, DNS 요청에 대한 재귀적이거나 신뢰할 수 있는 도메인 네임 분석 서비스 평균 응답시간이 **10초**를 초과하는 경우
	• 저장, 전송 또는 처리된 데이터의 무결성, 기밀성, 진본성이 훼손된 경우 ※ DNS 서비스 제공자가 관리하는 1,000개 미만의 도메인 네임 데이터가 DNS 서비스 제공자가 관리하는 도메인 네임의 1% 이하인 경우 제외
최상위 도메인(TLD) 네임 등록 서비스	• 신뢰할 수 있는 도메인 네임 분석(Domain name resolution) 서비스를 완전히 사용할 수 없는 경우
	• 1시간을 초과하여, DNS 요청에 대한 신뢰할 수 있는 도메인 네임 분석 서비스 평균 응답시간이 10초 이상 초과하는 경우
	• 저장, 전송 또는 처리된 데이터의 무결성, 기밀성, 진본성이 훼손된 경우

1 미공개 노하우 및 기업정보(영업비밀)의 불법 취득, 사용 및 공개로부터의 보호에 관한 유럽연합(EU) 지침

구분	주요내용
클라우드 컴퓨팅 서비스	• 제공된 서비스 중 하나 이상이 **30분** 이상 초과하여 완전히 사용할 수 없는 경우
	• 연합 내 서비스 사용자의 5% 또는 100만 명 초과 중 더 적은 수에 대하여, SLA(Service Level Agreemnet)가 체결되지 않은 서비스의 가용성이 제한되는 경우가 1시간을 초과할 때
	• 저장, 전송 또는 처리된 데이터의 무결성, 기밀성 또는 진본성이 악의적인 것으로 의심되는 행동의 결과로 손상된 경우
	• 저장, 전송 또는 처리되는 데이터의 무결성, 기밀성 또는 진본성이 손상되어 연합 내 서비스 사용자의 5% 또는 **100만명 초과 중 더 적은 수에 대하여 영향을 미치는 경우**
데이터센터 서비스	• 제공된 서비스 중 하나 이상을 완전히 사용할 수 없는 경우
	• SLA(Service Level Agreement)가 충족되지 않은 경우가 1시간을 초과할 때
	• SLA(Service Level Agreement)가 악의적인 것으로 의심되는 행동의 결과로 충족되지 않은 경우
	• 저장, 전송 또는 처리된 데이터의 무결성, 기밀성 또는 진본성이 악의적인 것으로 의심되는 행동의 결과로 손상된 경우
	• 데이터센터에 대한 물리적 액세스가 손상된 경우
콘텐츠 전송 네트워크 서비스, 관리형 (보안) 서비스	• 제공된 서비스 중 하나 이상을 10분을 초과하여 완전히 사용할 수 없는 경우
	• 연합 내 서비스 사용자의 5% 또는 100만 명 초과 중 더 적은 수의 SLA(Service Level Agreement)가 충족되지 않은 경우가 1시간을 초과할 때
	• 저장, 전송 또는 처리된 데이터의 무결성, 기밀성 또는 진본성이 악의적인 것으로 의심되는 행동의 결과로 손상된 경우
	• 저장, 전송 또는 처리되는 데이터의 무결성, 기밀성 또는 진본성이 손상되어 연합 내 서비스 사용자의 5% 또는 **100만명 초과 중 더 적은 수에 대하여 영향을 미치는 경우**
신뢰 서비스	• 서비스 또는 그 기능의 일부에 대하여, **30분** 이상 초과하여 완전히 사용할 수 없는 경우
	• 서비스 또는 그 기능의 일부를 사용자가 일주일 단위로 1시간을 초과하여 사용할 수 없는 경우
	• 연합 내 사용자의 1% 또는 **20만명 초과 중 더 적은** 수의 인원이 서비스 **가용성 제한의 영향을 받는 경우**
	• 네트워크 및 정보 시스템의 물리적 접근 또는 물리적 접근 보호가 손상되는 경우
	• 저장, 전송 또는 처리되는 데이터의 무결성, 기밀성 또는 진본성이 손상되어 연합 내 서비스 사용자의 **0.1% 또는 100명 초과 중 더 적은 수를 초과한** 인원에 영향을 미치는 경우
온라인 마켓 서비스, 온라인 검색엔진 서비스, SNS 플랫폼 서비스	• 연합 내 사용자의 5% 또는 100만 명 초과 중 더 적은 수가 서비스 또는 그 기능의 일부를 완전히 사용할 수 없는 경우
	• 연합 내 사용자 5% 또는 100만 명 초과 중 더 적은 수가 서비스 **가용성 제한의 영향을 받는** 경우
	• 저장, 전송 또는 처리된 데이터의 무결성, 기밀성 또는 진본성이 악의적인 것으로 의심되는 행동의 결과로 손상된 경우
	• 저장, 전송 또는 처리되는 데이터의 무결성, 기밀성 또는 진본성이 손상되어 연합 내 서비스 사용자의 5% 또는 **100만명 초과 중 더 적은 수에 대하여 영향을 미치는 경우**

Reference

■ https://digital-strategy.ec.europa.eu/en/library/nis2-commission-implementing-regulation-critical-entities-and-networks

해외 입법 동향

EU 집행위원회, 「AI와 인권, 민주주의, 법치에 관한 협약」 서명

EU 집행위원회(European Commission)는 인권 및 민주주의 등에 영향을 미치는 AI 위험을 완화하기 위하여, 유럽평의회(Council of Europe)가 주도한 AI 협약에 서명함 (2024. 9. 5.)

■ 개요 및 추진배경

○ **(배경)** AI 시스템의 수명주기 내 특정 활동이 인간의 존엄성, 개인의 자율성, 인권, 민주주의 및 법치를 훼손할 수 있다는 우려가 제기됨

- 특히, AI 시스템에 내포된 차별의 위험, 디지털 영역에서 여성이 경험하는 불평등을 포함하여 경제·정치·사회·문화적 불평등을 생산하는 AI 시스템 오용에 대한 우려 증대

○ 동 조약은 유럽평의회[1](Council of Europe, CoE)가 주도하여 초안을 마련하였고, 유럽연합 회원국, 영국, 미국 외 7개국이 동 협약에 서명

○ 「AI와 인권, 민주주의, 법치에 관한 협약[2]」은 최초의 법적 구속력이 있는 AI 관련 국제 조약으로, AI 시스템의 생명주기 내 활동이 인권, 민주주의, 법치와 양립할 수 있도록 법적 프레임워크를 제공

〈 「AI와 인권, 민주주의, 법치에 관한 협약」 구성 〉

조항	주요내용
제1장 총칙	· 대상과 목적(제1조), AI 시스템의 정의(제2조), 적용범위(제3조)
제2장 일반적 의무	· 인권의 보호(제4조), 민주적 절차의 완전성 및 법치에 대한 존중(제5조)
제3장 AI 시스템 수명주기 내 활동 관련 원칙	· 일반적 접근법(제6조), 인간의 존엄성과 개인의 자율성(제7조), 투명성 및 감독(제8조), 책임과 의무(제9조), 평등 및 차별금지(제10조), 프라이버시 및 개인정보보호(제11조) 등
제4장 구제수단	· 구제수단(제14조), 절차적 보호조치(제15조)
제5장 위험 및 부정적 영향 평가 및 완화	· 위험 및 영향 관리 프레임워크(제16조)
제6장 협약의 이행	· 차별금지(제17조), 장애인 및 아동의 권리(제18조), 공개협의(제19조), 디지털 리터러시 및 기술(제20조), 현존하는 인권에 대한 보호(제21조), 포괄적 보호(제22조)
제7장 후속조치와 협력	· 당사국 협의체(제23조), 보고의무(제24조), 국제협력(제25조), 효과적 감독기구(제26조)
제8장 최종규정	· 협약의 효력(제27조), 개정(제28조), 분쟁해결(제29조), 서명 및 발효(제30조), 가입(제31조) 등

1 1949년 민주주의 증진, 인권·법치주의 보호를 목표로 설립된 유럽 인권기구로서 유럽연합(EU) 27개 회원국을 포함한 46개 국가가 가입함 [출처] https://www.yna.co.kr/view/AKR20240627160500088

2 Framework Convention on artificial intelligence and human rights, democracy, and the rule of law (CETS No. 225)

■ 주요내용

○ **(목적)** AI 시스템의 수명주기 내 활동이 인권, 민주주의 및 법치에 부합하도록 보장하는 것을 목표로 하며, 이를 위해 당사국은 적절한 입법·행정적 조치 또는 기타 조치를 채택하거나 유지해야 함

○ **(정의)** 동 협약은 'AI 시스템'을 다음과 같이 정의

구분	주요내용
AI 시스템	• 명시적 또는 묵시적 목적을 위해 수신된 입력으로부터 물리적 또는 가상 환경에 영향을 미칠 수 있는 예측, 콘텐츠, 권장사항 또는 결정 등의 출력 생성방법을 추론하는 기계기반 시스템

○ **(적용범위)** ▲당사국은 **공공기관** 및 **당사국을 대신하여 활동하는 민간부문**의 **AI 시스템 활동**에 동 협약을 적용하고, 당사국은 ▲의무 이행에 있어 입법, 행정적 조치 또는 기타 조치를 채택하거나 유지할 수 있음

- 단, 당사국은 국가안보를 보호하기 위한 AI 시스템 수명주기 내 활동에 대해 동 협약을 적용하지 아니할 수 있음

○ **(기본원칙)** AI 시스템의 수명주기 내 활동과 관련하여, 인감의 존엄성 및 자율성, 투명성, 평등 등을 보장하기 위한 일반적인 공통원칙을 규정

구분	주요내용
인간의 존엄성과 개인의 자율성 (Human dignity and individual autonomy)	• 각 당사국은 인간의 존엄성과 개인의 자율성을 보호하기 위한 조치를 채택하거나 유지해야 함
투명성 및 감독 (Transparency and oversight)	• 각 당사국은 AI 시스템에 의해 생성된 콘텐츠의 식별과 관련하여, 특정 상황 및 위험에 맞춤화된 적절한 투명성 및 감독 요구사항이 마련되어 있는지 확인하기 위한 조치를 채택하거나 유지해야 함
책임과 의무 (Accountability and responsibility)	• 각 당사국은 인권, 민주주의, 법치와 관련된 AI 시스템의 부정적 영향에 대한 책임과 의무를 보장하기 위한 조치를 채택하거나 유지해야 함
평등 및 차별금지 (Equality and non-discrimination)	• 각 당사국은 관련 국제법 및 국내법에 규정된 바에 따라 성평등 및 차별금지를 보장하기 위한 조치를 채택하거나 유지해야 함
프라이버시 및 개인정보보호 (Privacy and personal data protection)	• 각 당사국은 프라이버시 및 개인정보보호 권리가 국제법 및 국내법 등을 통해 보호되기 위한 조치를 채택하거나 유지해야 함
신뢰성 (Reliability)	• 각 당사국은 AI 시스템의 적절한 보안 요구사항 등 AI 시스템의 신뢰성과 그 결과물에 대한 신뢰를 증진하기 위한 적절한 조치를 이행해야 함
안전한 혁신 (Safe innovation)	• 각 당사국은 관할 당국의 감독하에 AI 시스템을 개발, 실험 및 테스트하기 위한 통제된 환경을 적절하게 구축할 수 있도록 노력해야 함

○ **(위험관리)** 각 당사국은 인권, 민주주의, 법치에 대한 실질적이고 잠재적인 영향을 고려함으로써 AI 시스템에 의해 제기되는 위험의 식별, 평가, 예방 및 완화를 위한 조치를 채택하거나 유지해야 함

위험 및 영향관리 프레임워크
• 인권, 민주주의 및 법치에 대한 위험과 관련하여 AI 시스템의 맥락과 의도된 사용을 충분히 고려해야 함
• AI 시스템으로 인한 잠재적 영향의 심각성과 가능성을 충분히 고려해야 함
• 이해관계자, 특히 권리에 영향을 받을 수 있는 사람들의 관점을 고려해야 함
• AI 시스템의 수명주기 내 활동 전반에 걸쳐 반복적으로 적용해야 함
• 인권, 민주주의 및 법치에 대한 위험과 부정적 영향에 대한 모니터링을 포함해야 함
• 위험, 실제 및 잠재적 영향, 위험관리 접근방식에 대한 문서를 포함해야 함
• AI 시스템을 처음 사용하기 전, AI 시스템을 대폭 수정할 경우 AI 시스템을 테스트해야 함

○ **(협약의 이행원칙)** 동 협약은 이행과 관련하여 일반적 공통원칙을 규정

구분	주요내용
차별금지 (Non-discrimination)	• 각 당사국의 협약 이행은 국제적 인권 의무에 따라 어떠한 이유에서도 차별없이 보장되어야 함
장애인 및 아동의 권리 (Rights of persons with disabilities and of children)	• 각 당사국은 국내법 및 국제법에 따라 장애인 및 아동의 권리 존중과 관련하여 특정 취약성을 적절히 고려해야 함
공개협의 (Public Consultation)	• 각 당사국은 공개적 토론과 이해관계자 협의를 통해 AI 시스템과 관련하여 제기되는 중요한 문제들이 사회, 경제, 법률, 윤리, 환경 및 기타 관련 함의에 비추어 적절하게 고려되도록 노력해야 함
디지털 리터러시 및 기술 (Digital literacy and skills)	• 각 당사국은 AI 시스템에 의해 제기되는 위험의 식별, 평가, 예방 및 완화를 담당하는 사람들을 위한 특정 전문 기술을 포함하여, 적절한 디지털 리터러시 및 기술을 장려하고 촉진해야 함
인권 보호 (Safeguard for existing human rights)	• 동 협약의 어떠한 규정도 국내법 혹은 국제협약에 따라 보장될 수 있는 인권 또는 기타 관련 법적 권리 및 의무를 제한하거나 비하하거나 영향을 미치는 것으로 해석되지 아니함
포괄적 보호 (Wider protection)	• 동 협약의 어떠한 규정도 동 협약에 규정된 것보다 더 넓은 보호를 부여할 수 있는 가능성을 제한하거나 영향을 미치는 것으로 해석되지 아니함

○ **(당사국 협의체)** 협약 당사국의 대표로 구성된 당사국 협의체는 다음과 같은 역할을 수행함

당사국 협의체의 역할
• 동 협약의 효과적인 적용과 이행을 촉진하기 위하여 정기적으로 협의해야 함
• 동 협약의 보충 또는 개정 가능성을 고려해야 함
• 동 협약의 해석 및 적용에 관한 사항을 고려하고 구체적으로 권고해야 함
• 동 협약의 이행을 위해 관련성이 있는 중요한 법적, 정책적, 또는 기술적 발전에 관한 정보공유를 촉진해야 함
• 동 협약의 적용과 관련된 분쟁의 우호적 해결을 촉진해야 함
• 동 협약 이행에 있어, 공청회를 포함하여 관련 이해관계자와의 협력을 촉진해야 함

- 유럽평의회 사무총장[3](the Secretary General of the Council of Europe)이 필요할 때마다 당사국 협의체를 소집할 수 있고, 당사국 과반수가 소집을 요청할 때는 어떠한 경우라도 반드시 협의체를 소집해야 함

3 '24. 6. 25. 전 스위스 대통령 알랭 베르세가 유럽평의회 사무총장으로 선출됨 [출처] https://www.yna.co.kr/view/AKR20240627160500088

○ **(보고의무)** 각 당사국은 당사국이 된 후 첫 2년 이내에 당사국 협의체에 보고서를 제출해야 하며, 당사국 협의체는 보고의 형식과 절차를 결정함

○ **(국제협력 및 정보공유)** 당사국은 이 협약의 목적을 실현하기 위하여, 인권, 민주주의 및 법치 준수에 중대한 영향을 미칠 수 있는 AI 시스템 관련 정보를 상호공유해야 함

○ **(분쟁해결)** 동 협약의 해석 또는 적용에 관하여 당사국 간 분쟁이 발생하는 경우, 협상 또는 당사국 협의체, 기타 평화적 수단을 통하여 분쟁의 해결을 모색해야 함

○ **(발효)** 최소 3개 유럽평의회 회원국을 포함한 5개 서명국이 비준한 날로부터 3개월 후 발효

■ 전망 및 시사점

○ 글로벌 AI 거버넌스의 기틀을 마련하며 기술적 위험을 공통된 가치에 맞춰 관리하기 위한 국제 표준으로 기능할 것으로 기대됨

○ AI 시스템의 개발과 사용에 있어 인권, 민주주의, 법치주의 가치를 보호하면서도 혁신을 촉진하는 균형 잡힌 접근을 추구하지만, 국가안보 목적 AI 시스템에 대한 면제조항과 공공부문 대비 민간기업에 대한 제한적 감시 등이 한계로 지적됨

○ 일부 전문가들은 협약이 광범위한 원칙들의 집합으로 구성되어 규범적 성격이 약화되었음을 지적하고, 원칙과 의무 사항의 모호한 표현으로 인한 법적 불확실성 및 실효성 있는 집행이 가능한지에 대해 우려 제기

○ 협약의 실제 이행과 효과성은 각 서명국의 구체적인 적용 방식에 따라 달라질 수 있어, 향후 이행 과정을 주목할 필요가 있음

Reference

- https://www.eeas.europa.eu/delegations/council-europe/european-commission-signs-historic-council-europe-framework-convention-artificial-intelligence-and_en
- https://www.coe.int/en/web/portal/-/council-of-europe-opens-first-ever-global-treaty-on-ai-for-signature
- https://digital-strategy.ec.europa.eu/en/news/commission-signed-council-europe-framework-convention-artificial-intelligence-and-human-rights
- https://www.gov.uk/government/news/uk-signs-first-international-treaty-addressing-risks-of-artificial-intelligence

해외 단신

EU, 「AI법」 발효 및 'AI 협약' 초안 발표

○ **(「AI법」 발효)** 「AI법」이 EU 관보에 게재되었고(2024. 7. 12.), 공식 발효됨(2024. 8. 1.)

- 「AI법」은 일부 예외*를 제외하고 2년 후에 완전히 적용됨(2026. 8. 2.)

  * 「AI법」이 관보에 게재된 날로부터, 금지조항은 6개월 후, 거버넌스 규칙 및 범용 AI 모델에 대한 의무조항은 12개월 후, 규제 제품에 내장된 AI 시스템에 대한 조항은 36개월 후 적용됨

- **(「AI법」 주요내용)** 인공지능을 위험성에 따라 ▲금지된 수준의 위험, ▲고위험, ▲제한된 위험, ▲최소 위험으로 구분하고 각기 다른 정도로 규제

  ※ [인터넷·정보보호 법제동향 참고] (「AI법」 추진현황」) 제189호('23.3.), 제195호('23.12.), 제200호('24.5.)

○ **('AI 협약' 초안)** EU 집행위원회는 관련 조직이 「AI법」의 요구사항을 선제적으로 이행할 수 있도록 'AI 협약' 초안을 발표(2024. 7. 22.)

- EU 집행위원회는 「AI법」의 발효일(2024. 8. 1.)과 적용일(2026. 8. 2.) 사이 과도기에 관련 조직이 자발적으로 요구사항을 이행하도록 참여자를 모집하였고, 550개 기관이 참여의사를 표명

- 'AI 협약'은 두 가지 핵심 축(Pillar)으로 구성

AI 협약 (「AI 법」 이행을 대비하기 위한 프레임워크)	
제1축 (Pillar I)	**제2축 (Pillar II)**
• AI 협약 네트워크 구성 및 정보공유	• 관련 조직의 「AI 법」 의무준수 촉진 및 홍보
- AI 사무국이 주최하는 워크숍을 통한 정보공유 - 모범사례 교환을 위한 전용 온라인 공간 구축 및 관리	- 「AI 법」 조기 구현을 촉진하기 위한 프레임워크 제공 - 조직의 참여선언 서약을 통한 점진적 목표 구축

- **('AI 협약' 주요내용)** 협약에 참여하는 모든 조직이 「AI법」이 적용되는 시점까지 다음과 같은 핵심요건을 이행할 것을 강조

  · 조직 내 **AI 활용을 촉진**하고, 향후 「AI법」 준수를 위한 **AI 거버넌스 전략을 채택**

  · 「AI법」에 따라 **고위험으로 간주되는 영역**에서 개발되거나 사용되는 **AI 시스템을 식별**

  · AI 시스템을 **개발**하는 조직의 경우, 수명주기 전반에 걸쳐 AI 시스템의 사용으로 인해 발생할 수 있는 **건강, 안전 및 기본권에 관한 위험을 식별하기 위한 프로세스** 등을 마련해야 함

  · AI 시스템을 **배포**하는 조직의 경우, 관련 AI 시스템의 사용을 통해 **영향을 받을 수 있는 개인 및 그룹의 기본권리에 대한 위험** 등을 **식별**해야 함

Reference

■ https://digital-strategy.ec.europa.eu/en/policies/ai-pact

해외 입법 동향

EU 집행위원회, 「사이버감시 품목 수출에 관한 권고안」 발표

EU 집행위원회는 사이버감시 기술의 오용 위험을 줄이고 수출업체가 인권에 미치는 영향을 평가할 수 있는 실질적인 툴을 제공하기 위하여, 「사이버감시 품목 수출에 관한 권고안[1]」을 발표 (2024. 10. 16.)

■ 개요

○ EU 집행위원회는 「이중용도 품목의 수출 등 통제에 관한 규정[2]((EU)2021/821)」(이하 「이중용도 품목규정」) 제26조에 따라, 수출업체가 동 규정에 명시되지 않은 별도의 사이버감시 품목을 심사하는데 도움을 줄 수 있도록 권고안을 마련

○ 동 권고안은 「이중용도 품목규정」 제5조제2항에 따라, 수출업체가 규정에 명시되지 않은 사이버감시 품목을 통제하는 것을 목표로 하며 해당 품목의 수출과 관련된 위험을 평가하는 실사조치를 포함

〈 「이중용도 품목규정」 제5조제2항에 명시된 요구사항 〉

수출업체가 **규정에 명시되지 않은** 사이버감시 품목을 수출할 경우, → 해당 품목이 내부탄압 등에 악용될 의도를 **실사(Due Diligence)**하고 → 실사결과, 악용될 의도를 알게되면 **관할당국에 통지해야 함**

※ 「이중용도 품목규정」에 명시된 사이버감시 품목의 경우, 수출 허가를 받아야 함

■ 주요내용 (※ 세부내용은 '붙임' 참고)

○ **(정의)** 동 권고안은 주요 용어를 다음과 같이 정의함

구분	주요내용
사이버감시 품목 (Cyber-surveillance items)	• **정보통신시스템**으로부터 데이터를 **모니터링, 추출, 수집 또는 분석**함으로써 **자연인**을 **은밀하게 감시**할 수 있도록 **특수 설계**된 이중용도 품목 (「이중용도 품목규정」 제2조제20항)
내부탄압 (Internal repression)	• 세계인권선언, 시민·정치적 권리에 관한 국제규약 등 관련 국제인권조약에 명시된 인권 및 기본적 자유에 대한 기타 주요 침해가 포함
국제인도법을 심각하게 위반한 행위 (Commission of serious vidation of international humanitarian law)	• 국제인도법은 무력충돌 시 적대행위에 참여하지 않거나 더 이상 적대행위에 참여하지 않은 사람들을 보호하기 위한 제네바협약 등을 통해 발전해왔음 - 사이버감시 품목은 무력 충돌의 맥락에서 전쟁수단 및 방법으로 사용될 때 국제인도법을 준수해야 함

1 COMMISSION RECOMMENDATION (EU) 2024/2659 of 11 October 2024 on guidelines on the export of cyber-surveillance items under Article 5 of Regulation (EU) 2021/821 of the European Parliament and of the Council

2 REGULATION (EU) 2021/821 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items(recast)

○ **(잠재적 위험성이 있는 사이버감시 품목[3])** ▲안면 및 감정인식 기술(Facial and emotion recognition technology), ▲위치추적장치(Location tracking devices), ▲비디오 감시시스템(Video-surveillance systems)은 일상생활에 다양한 용례로 사용되어 「이중용도 품목규정」에 명시되지 않았으나 잠재적 위험성이 있어 수출업체는 사이버감시 품목의 가능성이 있는 경우 주의해야 함

○ **(실사조치)** 수출업체는 「이중용도 품목규정」에 명시되지 않은 사이버감시 품목 분류 및 거래위험 평가에 관한 '거래 심사조치(transaction-screening measures)'를 통해 실사를 수행해야 함

〈 거래 심사조치 단계별 검토사항 〉

① 사이버감시 품목 검토	▶	② 오용가능성 검토	▶	③ 이해관계자 검토	▶	④ 예방계획 수립
규정에 명시되지 않은 품목을 수출할 경우, 사이버감시 품목의 정의에 비추어 품목의 기술적 특성에 대한 검토		해당 품목의 기능을 검토하여, 내부탄압 및 국제인도법에 대한 심각한 위반행위의 가능성을 판단		관할당국의 지원을 받아 거래와 관련된 이해관계자(최종 사용자 및 유통업체, 리셀러 등)를 검토		실사결과에 따라 인권과 관련된 부정적 영향을 유발하거나 기여하는 활동을 중단하고 시정조치 계획을 수립·시행해야 함

■ 전망 및 시사점

○ 동 권고안은 EU 내 수출업체가 단계별 접근방식을 통해 실사를 수행하는 방법을 포함하여 사이버감시 품목과 관련된 수출통제를 탐색하는 데 도움이 되도록 기준을 제시

○ 또한 수출업체들은 동 권고안을 통해 특정 사이버감시 품목의 수출이 수입국의 내부탄압이나 인권 및 국제인도법에 관한 심각한 위반을 초래할 수 있는지 여부를 평가하는 데 도움이 될 것으로 기대

○ 사이버감시 도구의 확산과 오용을 해결하는 문제는 단일 정책수단으로 달성할 수 없는 복잡한 과제인만큼, EU는 지속적으로 보다 포괄적인 정책 대응을 추진할 것으로 전망

Reference

▪https://policy.trade.ec.europa.eu/news/commission-publishes-guidelines-cyber-surveillance-exporters-2024-10-16_en
▪https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202402659
▪https://www.sipri.org/commentary/topical-backgrounder/2024/making-most-eu-catch-all-control-cyber-surveillance-exports

3 Potential non-listed cyber-surveillance items

붙임 EU 집행위원회의 「사이버감시 수출업체를 위한 권고안」 세부내용

○ **(정의)** 동 권고안은 '사이버감시 품목'의 정의 규정을 세부적으로 검토

구분	주요내용
사이버감시 품목 (cyber-surveillance items)	• **정보통신시스템**으로부터 데이터를 **모니터링, 추출, 수집 또는 분석**함으로써 **자연인**을 **은밀하게 감시**할 수 있도록 **특수 설계**된 이중용도 품목 (「이중용도 품목규정」 제2조제20항)
정보통신시스템 (information and telecommunication systems)	• 소프트웨어·웹·컴퓨터·저장 기술 등을 포함한 프로그래밍/코딩, PC 시스템(하드웨어) 운영 및 기타 정보관리와 같은 정보를 전자적으로 처리하는 시스템 및 원거리에 걸쳐 정보를 전달하는 일부 시스템을 의미함
데이터 모니터링, 추출, 수집, 분석 (Monitoring, extracting, collecting, analysing data)	• **(모니터링)** 정보통신시스템의 데이터를 모니터링하는데 사용되는 항목(해당 시스템에서 전송되는 데이터의 파일 크기 또는 패키지 트래픽)을 위한 기술기능을 갖추고 있어야 함 • **(추출)** 침입 및 추출을 수행하여 정보통신시스템에서 데이터를 추출하는 항목(침입 소프트웨어)을 위한 기술기능을 갖추고 있어야 함 • **(분석)** 정보통신시스템에서 추출한 데이터를 분석할 수 있는 항목으로, 해당 시스템에 저장된 카메라 이미지를 처리할 수 있는 항목(안면 인식 시스템의 일부로 사용되는 특정 유형의 데이터 분석기술)을 갖추고 있어야 함
자연인 (Natural persons)	• 법인 또는 단체와 구별되는 살아있는 인간을 의미함
은밀한 감시 (Covert surveillance)	• 자연인이 객관적으로 감시받고 있는 것을 인지할 수 없는 경우, 은밀한 감시로 간주될 수 있음 - 사이버감시 물품의 존재를 인식하지 못하여 해당 감시에서 자신을 제외하거나 최소한 그에 따라 행동을 조정할 기회가 없는 경우 - 공공장소에 설치되거나 운영되는 물품을 통해 감시가 진행되더라도 데이터 수집이 다른 목적으로 전환, 평가 또는 처리되는 경우
특수 설계된 (Specially designed)	• 자연인에 대한 은밀한 감시가 제품 개발 및 설계의 주요 목적이었을 경우

○ **(사이버감시 품목의 특성 검토)** 동 권고안은 부록을 통해, 「이중용도 품목규정」에 명시되어 수출통제되는 사이버감시 품목 중 예외로 인정되는 품목의 기술적 특성을 설명

- 예를 들어, 전자장치에 대한 원격 액세스 권한을 은밀하게 획득할 수 있는 침입 소프트웨어는 「이중용도 품목규정」(부록I 4A005)에 의해 통제되지만, 제품 취약점을 보완하기 위해 침입 소프트웨어와 관련된 정보를 공유하는 사이버보안 연구원의 활동은 통제되지 않음

구분	주요내용
통신감청시스템 (Telecommunication interception systems)	• 통신 콘텐츠(음성 또는 데이터)를 추출하도록 설계된 장비, 무선통신을 통해 무선으로 전송되는 가입자 식별 또는 기타 메타데이터 및 무선 주파수 모니터링 장비에 적용됨 - **다만, 이동통신 방해장비(Mobile telecommunications jamming equipment)는 데이터를 수집하지 않기 때문에 사이버감시 품목에 해당하지 않음**
인터넷 감시시스템 (Internet surveillance systems)	• 메타데이터 콘텐츠(음성, 비디오, 메시지 등)의 분석, 추출 및 인덱싱을 수행하고 사람들의 관계형 네트워크를 매핑하기 위해 캐리어급[4] IP 네트워크에서 작동하는 인터넷제어시스템 - **다만, 사용자 또는 구독자의 작업 또는 상호작용이 존재하는 시스템 (예 : 소셜 네트워크 및 상업용 검색 엔진 등)은 해당하지 않음**
침입 소프트웨어 (Intrusion software)	• 침입 소프트웨어의 생성, 명령 및 제어 또는 전달을 위해 특수 설계 또는 수정된 소프트웨어뿐 아니라 시스템, 장비, 구성요소 및 관련 기술이 포함됨

구분	주요내용
	- 다만, 제품에 대한 취약점이 공개되기 전에 수정사항을 개발하기 위해 침입 소프트웨어와 관련된 정보를 공유하는 사이버보안 연구원 등의 활동은 해당하지 않음
통신 모니터링 소프트웨어 (Communication monitoring software)	• 통신 서비스 제공업체에서 요청한 감청조치를 통해 수집된 데이터를 권한있는 법 집행기관에서 모니터링 및 분석하도록 설계된 소프트웨어 **- 다만, 청구, 네트워크 서비스 품질, 체감 품질, 모바일 결제 또는 은행 이용과 같은 순수한 상업적 목적을 위해 특수 설계되거나 수정된 소프트웨어는 해당하지 않음**
포렌식/조사 도구 (Forensic/investigative tools)	• 컴퓨팅 또는 통신장치에서 원 데이터를 추출하여 데이터가 변조되거나 손상되지 않고 범죄 수사 또는 법원에서 사법 목적으로 사용될 수 있도록 설계된 품목 **- 다만, 은밀한 감시를 위해 특수 설계되지 않은 포렌식/조사 도구(사용자 데이터만 추출하거나 장치에서 데이터가 보호되지 않는 포렌식/조사 도구는 해당하지 않음**

○ **(오용가능성 검토)** 수출업체는 해당 품목이 내부탄압 및 국제인도법에 대한 심각한 위반행위의 가능성이 있는지 여부를 다음과 같은 위험신호를 통해 평가해야 함

품목의 오용가능성 위험신호
• 품목이 은밀한 감시를 위한 잠재적 사용과 관련된 정보와 함께 판매되는 경우
• 유사한 품목[5]이 내부탄압 및/또는 국제인도법에 대한 심각한 위반행위와 관련하여 요용되었음을 나타내는 정보
• 해당 품목이 회원국에 대한 감시 활동 또는 EU 시민에 대한 불법감시와 관련하여 불법적으로 사용되었음을 나타내는 정보
• 내부탄압 및/또는 국제인도법의 심각한 위반행위와 관련하여 오용되는 것으로 알려진 시스템을 설정, 사용자 지정 또는 구성하는 데 사용할 수 있는 품목이 거래에 포함되어 있음을 나타내는 정보

○ **(이해관계자 검토)** 수출업체는 관할당국을 지원하기 위해, 거래와 관련된 이해관계자를 검토해야 함

거래와 관련된 이해관계자 검토사항
• 거래 전이거나 진행 도중에 수취인 및/또는 최종사용자가 최종 사용명세서를 기반으로 제품·서비스를 어떻게 사용하려는지 검토
• 품목이 도달하는 목적지의 인권에 대한 일반적 상황을 숙지
• 다음과 같은 위험신호를 통해 제품·서비스가 승인되지 않은 다른 최종사용자에게 전달될 수 있는 위험을 검토
- 최종사용자가 내부탄압 또는 인권 등에 대한 심각한 위반을 자행한 이력이 있는 외국정부와 명백한 관계를 맺고 있는 경우
- 최종사용자가 구조적으로 군대 또는 내부탄압 조치 및/또는 과거에 인권 및 국제인도법에 대한 심각한 위반과 관련된 무력 충돌에 연루된 다른 그룹의 일부인 경우
- 최종사용자가 과거에 사이버감시 품목의 사용으로 인해 내부탄압 조치 및/또는 국제인도법에 대한 심각한 위반이 발생한 국가에 사이버감시 품목을 수출한 적이 있는 경우

○ **(예방계획 수립)** 수출업체는 실사결과를 통해, 인권과 관련된 부정적인 영향을 예방하고 완화하기 위한 계획을 수립·시행해야 함

주요내용
• 기업의 정책을 업데이트하여, 향후 부정적 영향을 피하고 해결하는 방법에 대한 권고안을 제공하고 구현해야 함
• 위험평가 결과를 바탕으로 관리 시스템을 개선하여 부정적 영향이 발생하기 전에 정보를 더 잘 추적하고 위험을 표시해야 함
• 인권과 관련된 부정적 영향의 위험을 이해하기 위한 정보를 수집해야 함
• 회원국의 관할 당국에 실사결과를 통지하여, 특정 항목, 최종사용자 및 목적지와 관련된 정보공유를 촉진해야 함

4 통신 분야에서 높은 수준의 일관된 품질, 신뢰성, 가용성을 갖춘 성능을 제공하는 제품등급

5 「이중용도 품목의 수출 등 통제에 관한 규정((EU)2021/821)」의 제5조제6항에 따라 유럽연합 공식관보의 C 시리즈에 게재됨

해외 입법 동향

유럽사이버보안청(ENISA), NIS2 지침 이행규정 관련 가이던스 발표

유럽사이버보안청(ENISA)은 NIS2 지침에 따른 사이버보안 조치를 효과적으로 구현하고, 디지털 서비스 제공자 등 NIS2 지침 이행규정의 적용대상을 지원하기 위한 가이던스[1] 초안을 발표 (2024. 11. 7.)

■ 개요

○ 동 가이던스는 NIS2 지침에 따른 사이버보안 위험관리 조치별 고려사항, 추가 설명, 의무 준수여부를 평가할 수 있는 방안 등을 제시하고 **법적 구속력 없는 권고적 성격**을 지님

○ 유럽사이버보안청, 유럽 집행위원회 등은 기술 발전과 환경 변화를 정기적으로 검토하고, 조직의 규모, 업종, 사이버위협 노출 정도 등을 종합적으로 고려하여 적절한 수준의 보안조치를 제시하는 등 동 가이던스를 지속적으로 갱신되는 '살아있는 기록(living document)'으로써 관리

■ 주요내용 (※ NIS2 지침 이행규정의 세부내용은 인터넷·정보보호 법제동향 제205호('24.10) 참고)

○ **(적용대상)** NIS2 지침 이행규정의 의무를 적용받는 디지털 인프라, 디지털 서비스 제공자 및 ICT 서비스 관리 부문의 조직을 대상으로 함

구분	주요내용
도메인 네임 시스템 서비스 제공자	• 인터넷 도메인 이름을 IP 주소로 변환하는 서비스 제공
최상위 도메인 네임 등록기관	• '.com', '.org' 등 최상위 도메인 관리
클라우드 컴퓨팅 서비스 제공자	• 컴퓨팅 자원의 온디맨드 접근을 제공
데이터센터 서비스 제공자	• 데이터 저장, 처리, 전송을 위한 시설 운영
콘텐츠 전송 네트워크 제공자	• 웹 콘텐츠 전송 최적화 서비스 제공
관리형 보안 서비스 제공자	• IT 시스템 관리 및 보안관리 서비스 제공
온라인 마켓플레이스 제공자	• 온라인 상거래 플랫폼 운영
신뢰 서비스 제공자	• 전자서명 등 신뢰성 보장 서비스 제공
온라인 검색엔진 제공자	• 디지털 검색 서비스 제공
소셜 네트워킹 서비스 플랫폼 제공자	• 소셜 미디어 플랫폼 운영

○ **(일반원칙)** 네트워크 및 정보시스템 보안 정책, 위험관리, 사고처리 등 NIS2 지침에 명시된 사이버보안 조치 요구사항을 기반으로, 일반원칙을 제공

1 IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures

주요내용	
1. 네트워크 및 정보시스템 보안 정책	
• 조직의 보안관리를 위한 최상위 문서를 작성하고, 전반적인 보안 접근방식과 사업 전략 및 목표와의 연계성을 규정 • ▲보안 목표설정, ▲지속적 개선을 위한 자원할당, ▲이해관계자와의 의사소통 방안, ▲역할과 책임 등을 정의 • 문서 보관기간, 세부정책 목록, 모니터링 지표 등을 명시하고 관리 기구의 공식 승인을 받도록 함	
2. 위험관리 정책	
• 네트워크 및 정보시스템의 위험을 식별, 분석, 평가하고 처리하기 위한 프레임워크를 구축 • 위험평가 결과에 따른 처리 계획을 수립하고 이행상태를 지속적으로 모니터링 • 규정 준수여부를 모니터링하고 독립적인 검토를 통해 접근방식의 적절성을 평가	
위험관리 프로세스	• **(위험평가 및 처리)** 조직의 자산과 서비스에 대한 위험을 평가하고 문서화하여 경영진의 승인을 받은 후, 위험 경감을 위한 구체적인 처리 계획을 수립하고 이행 상태를 지속적으로 모니터링 • **(체계적 관리 절차)** 위험관리 방법론과 허용 수준을 설정하고, 이를 바탕으로 제3자 위험을 포함한 모든 보안 위험을 식별·분석·평가하여 적절한 처리 방안을 마련하고 실행 • **(주기적 검토)** 모든 위험 평가 결과와 처리 계획은 최소 연 1회 정기적으로 검토하고, 중대한 사고나 환경 변화 발생 시 즉시 재검토하여 필요한 개선사항을 반영
3. 사고처리	
• 사고의 탐지, 분석, 대응, 복구를 위한 정책과 절차를 수립하고 문서화 • 네트워크와 정보시스템에 대한 지속적인 모니터링과 로깅을 수행하며, 의심스러운 이벤트에 대한 보고체계를 구축 • 사고의 성격과 심각성을 판단하기 위한 평가·분류 기준을 수립하고, 사고 후 검토 프로세스를 실시	
사고대응	• **(사고 처리 정책)** 사고의 분류 체계, 커뮤니케이션 계획, 담당자 역할과 책임, 필요 문서 등을 포함한 종합적인 사고 처리 정책을 수립하고 이를 업무 연속성 계획과 연계하여 관리 • **(탐지 및 보고체계)** 네트워크와 시스템 활동에 대한 자동화된 모니터링과 로깅을 수행하고, 의심스러운 이벤트를 즉시 보고할 수 있는 체계를 구축하며, 로그의 무결성과 시간 동기화를 통해 사고의 상관관계를 분석할 수 있어야 함 • **(대응 및 복구 활동)** 사고 발생 시 확산 방지를 위한 봉쇄, 재발 방지를 위한 근절, 정상 운영으로의 복구 등 단계별 대응 절차를 수립하고, 사후 검토를 통해 도출된 교훈을 정책과 절차 개선에 반영
4. 비즈니스 연속성 및 위기관리	
• 사고 발생 시를 대비한 비즈니스 연속성 및 재해복구 계획을 수립 및 유지 • 데이터와 시스템의 백업 사본을 유지하고 적절한 수준의 중복성을 보장하기 위한 자원을 제공 • 위기 상황에서의 의사소통 계획을 수립하고, CSIRT 또는 관할 당국과의 협력 체계를 구축함	
비즈니스 연속성 및 복구 계획	• **(계획 수립 및 구현)** 목적과 범위, 역할과 책임, 의사소통 채널, 계획 활성화 조건, 복구 순서와 목표, 필요 자원 등을 포함한 종합적인 연속성 및 복구 계획을 수립하고, 이를 실제 운영에 적용할 수 있도록 구체화해야 함 • **(영향 분석 및 요구사항)** 운영 중단이 비즈니스에 미치는 잠재적 영향을 분석하고, 이를 바탕으로 복구 시간 목표(RTO)[2], 복구 시점 목표(RPO)[3], 서비스 제공 목표(SDO)[4] 등 구체적인 복구 요구사항을 수립해야 함 • **(정기적 검증 및 개선)** 수립된 계획은 정기적인 테스트를 통해 실효성을 검증하고, 중대한 사고나 환경 변화 발생 시 즉시 검토하여 개선사항을 반영함으로써 계획의 실행력을 지속적으로 강화
5. 공급망 보안	
• 직접 공급자 및 서비스 제공자와의 관계를 관리하는 보안 정책을 수립하고, 공급망 내 조직의 역할을 명확히 함 • 공급자 선정 시 ▲사이버보안 관행, ▲보안 사양 충족 능력, ▲ICT 제품·서비스의 품질과 복원력을 평가 • 공급자 및 서비스 제공자의 최신 디렉터리를 유지·관리	
6. 시스템 획득·개발·유지관리 보안	
• ICT 서비스, 시스템, 제품 획득 시의 보안 요구사항을 정의하고 위험을 관리 • 보안 테스트 정책을 수립하고 실행하며, 보안 패치의 적시 적용을 보장 • 네트워크 세분화를 구현하고, 취약점의 식별·분석·처리를 위한 절차를 수립	
7. 사이버보안 위험관리 조치의 효과성 평가	

주요내용
• 조직이 이행한 사이버보안 위험관리 조치가 효과적으로 구현되는지 평가하는 정책과 절차를 수립
• 모니터링과 측정방법, 시기, 책임자를 명확히 정의
• 모니터링 및 측정 결과를 분석하고 평가하는 체계를 구축
8. 기본 사이버 위생 및 보안 교육
• 모든 직원이 위험을 인식하고 기본적인 사이버 위생 수칙을 적용하도록 보장
• 보안 관련 역할을 수행하는 직원을 식별하고 정기적인 교육을 제공
• 교육 프로그램의 효과성을 테스트하고 위협 환경 변화에 따라 주기적으로 업데이트
9. 암호화
• 데이터의 기밀성, 진정성, 무결성 보호를 위한 암호화 정책과 절차를 수립
• 자산 분류 및 위험평가 결과에 따라 적절한 암호화 조치의 유형, 강도, 품질을 결정
• 키 관리 접근방식을 정의하고 암호화 정책을 주기적으로 검토·업데이트
10. 인적자원 보안
• 직원들이 보안 책임을 이해하고 이행하도록 적절한 절차를 수립
• 역할에 따라 필요한 경우 직원의 배경을 검증하는 절차를 마련
• 고용 종료 또는 변경 시 보안 책임과 의무를 명확히 하고 이행을 보장
11. 액세스 통제
• 비즈니스 및 보안 요구사항에 기반한 논리적·물리적 접근 통제 정책을 수립
• 접근권한의 제공, 수정, 삭제 절차를 문서화하고 접근권한 등록부를 유지
• 특권 계정과 시스템 관리 계정에 대한 강화된 통제를 구현
12. 자산관리
• 네트워크 및 정보시스템 범위 내 모든 자산에 대한 분류 수준을 설정
• 자산의 전체 수명주기에 걸친 취급 정책을 수립하고 관련자에게 전달
• 완전하고 정확한 자산 목록을 개발하고 변경사항을 추적 가능한 방식으로 기록
13. 환경 및 물리적 보안
• 지원 유틸리티의 장애나 중단으로 인한 시스템 운영 중단을 예방
• 자연재해 등 물리적·환경적 위협으로부터 시설과 시스템을 보호하기 위한 조치를 구현
• 보안 경계를 설정하고 물리적 출입 통제를 통해 비인가 접근을 예방·모니터링

○ **(접근방식)** 조직의 규모와 특성을 고려하여 유연한 구현을 허용하고 위험평가를 기반으로 한 핵심 보안원칙 준수를 요구

- (조직 특성에 따른 차등적 접근) 대규모 조직은 전담 정보보안 조직을 운영하고 CISO를 지정하는 반면, 소규모 조직은 기존 역할에 보안 업무를 추가하거나 간소화된 프로세스를 적용할 수 있음

- (위험기반 요구사항 이행) 자산의 분류 수준과 위험평가 결과에 따라 보안조치의 강도를 차등 적용하되, 중요 데이터 처리 시스템 등과 같은 고위험 영역에 대해서 강화된 보안 통제를 적용

- (핵심 보안원칙 준수) 최소 권한 부여, 중요 업무의 분장, 다층적 보안 통제 구현, 업무 효율성을 고려한 현실적 보안 조치 적용 등의 기본원칙을 준수하면서 보안 체계를 구축

○ **(예외 관리)** 일반원칙의 엄격한 적용이 어려운 상황에 대하여 예외를 허용하되, 이에 대한 지속적인 모니터링과 관리를 요구

2 Recovery time objectives (RTOs): 재해 발생 후 비즈니스 자원과 기능(ICT 시스템과 프로세스)의 복구를 위해 허용되는 최대 시간
3 Recovery point objectives (RPOs): 중단으로 인해 특정 ICT 활동이나 애플리케이션에서 손실될 수 있는 데이터의 양
4 Service delivery objectives (SDOs): 대체 처리 모드 동안 비즈니스 기능이 도달해야 하는 최소 성능 수준

- (예외 승인 절차) 일반원칙 적용예외의 필요성, 범위, 기간, 위험영향 분석을 포함한 예외 신청서를 제출하고 보안 책임자 또는 위험관리 위원회의 검토와 승인을 거쳐 예외 등록부에 기록·관리

- (주요 예외상황 및 대응) 소프트웨어 업데이트 지연, 다중 인증 미적용, 레거시 시스템의 암호화 미적용 등의 상황에서 대체 보안통제 조치를 이행하여 보안 위험을 완화

- (예외 관리 및 통제) 모든 예외에 대해 분기별 재검토, 대체 통제의 효과성 평가, 위험 모니터링을 실시하고 예외 상황 해소를 위한 중장기 개선 계획을 수립하여 관리

○ **(평가 및 감독)** 일반원칙 준수 여부에 대한 평가 및 감독 관련 사항을 규정

- (감독 체계의 유연성) 각 회원국은 자국의 법·제도적 환경을 고려하여 독자적인 감독 체계를 구축할 수 있으며, 기존의 감독 체계를 활용할 수 있음

- (평가기관의 다양성) 국가가 지정한 적합성 평가기관뿐만 아니라 승인된 독립 감사자(Independent auditors)를 통한 평가도 인정하여 조직의 선택권을 보장

- (기존 프레임워크 활용) 국가별 사이버보안 프레임워크나 업종별 보안 기준이 본 규정과 동등한 수준의 보안을 보장하는 경우, 해당 프레임워크를 통한 준수 입증을 허용

○ **(일반원칙 준수여부 입증방안)** 일반원칙의 준수여부를 입증하기 위한 구체적인 증거 유형을 제시

구분	주요내용
정책 및 절차 문서화	• 조직의 네트워크 및 정보시스템 보안관리를 위한 최신 정책과 절차, 계획, 가이던스 등이 문서화되어 있고 정기적으로 검토·갱신되고 있음을 보여주는 증거 - 정보보안 정책문서, 위험관리계획서, 사고대응절차서, 업무연속성계획서, 공급자관리 정책, 정책 검토 의견서 및 변경이력관리대장 등
운영기록	• 보안 통제 설정, 모니터링 로그, 접근 제어, 사고 대응 등 일상적인 보안 운영 활동이 정책과 절차에 따라 수행되고 있음을 입증하는 기록 - 보안시스템 구성설정파일, 시스템·네트워크 모니터링 로그, 사용자 접근권한 관리대장, 보안사고 대응 활동일지, 백업 및 복구작업 기록 등
평가 및 검토 결과	• 내부/외부 감사, 취약점 평가, 보안 테스트, 독립적 검토 등을 통해 보안 조치의 적절성과 효과성을 주기적으로 평가하고 있음을 보여주는 결과물 - 보안감사보고서, 취약점 진단결과보고서, 모의해킹 결과보고서, 공급자 보안평가서, 독립적 보안검토 결과보고서 등
인적자원 관련 기록	• 직원들의 보안 교육 이수, 인식제고 활동 참여, 보안 책임 이행 동의 등 인적 보안 관리가 적절히 이루어지고 있음을 입증하는 문서 - 보안교육 이수증, 인식제고 활동 참석부, 직원 신원조회 결과서, 비밀유지서약서, 보안 위반 징계조치 기록 등
관리활동 증거	• 경영진의 보안 활동 검토, 리스크 승인, 자원 할당 등 조직 차원의 보안 관리와 지원이 이루어지고 있음을 보여주는 증빙자료 - 정보보안 경영검토 회의록, 위험수용 승인서, 보안예산 할당 문서, 보안활동 성과측정 보고서 등

■ 전망 및 시사점

○ 동 가이던스는 소프트웨어 업데이트 지연, 다중인증 미적용 등에 대한 예외를 허용하되 위험 영향 분석과 대체 통제수단 마련을 강조하는 등 현실적인 보안 이행 체계를 제시하여 조직의 규모와 특성에 따른 유연한 접근방식을 제시

- 일각에서는 도메인 네임 시스템 서비스 제공업체 등 의무 적용대상이 실용적인 접근방식을 통하여, NIS2 지침의 엄격한 기대치를 충족하는 사이버보안 관행을 구축할 수 있을 것으로 기대

Reference

▪https://www.enisa.europa.eu/news/asking-for-your-feedback-enisa-technical-guidance-for-the-cybersecurity-measures-of-the-nis2-implementing-act
▪https://www.enisa.europa.eu/publications/implementation-guidance-on-nis-2-security-measures/@@download/fullReport

해외 입법 동향

EU,「사이버복원력법」제정

EU 이사회는 디지털 요소가 있는 제품의 사이버보안 강화와 통합된 취약점 관리를 목적으로 하는「사이버복원력법[1]」을 제정하여, 포괄적인 사이버보안 규제체계를 구축 (2024. 11. 20.)

■ 개요

○ EU 내 디지털 요소가 있는 제품의 보안성 향상과 사이버위협 대응을 위하여, EU 집행위원회는 제품의 전체 생애주기 걸친 사이버보안 규제 프레임워크를 마련

- 「사이버복원력법」은 EU 공식관보에 게재되고 20일 후에 발효되며(12. 10), 그로부터 36개월이 경과한 시점부터 본격 시행될 예정

○ 디지털 요소가 있는 제품의 생산, 유통 등에 관여하는 모든 경제사업자들의 책임과 의무를 명확히 규정하고 디지털 요소가 있는 제품의 선택·사용 시 사용자가 사이버보안을 고려할 수 있는 조건 형성

〈 EU「사이버복원력법」의 주요구성 〉

구분	주요내용
제1장 일반조항	• 제1조 목적, 제2조 적용범위, 제3조 정의, 제4조 자유로운 이동, 제5조 디지털 요소 포함 제품의 조달 및 사용, 제6조 디지털 요소 포함 제품 요구사항, 제7조 중요 디지털 요소 포함 제품 등
제2장 경제 사업자의 의무 및 자유 등	• 제13조 제조업자의 의무, 제14조 제조업자의 보고의무, 제15조 자발적 보고, 제16조 단일 보고 플랫폼 구축, 제18조 공인대리인, 제19조 수입업자의 의무, 제20조 유통업자의 의무 등
제3장 디지털 요소가 있는 제품의 적합성	• 제27조 적합성 추정, 제28조 EU 적합성 선언, 제29조 CE 마크 일반원칙, 제30조 CE 마크 부착규칙 및 조건, 제31조 기술문서, 제32조 적합성 평가절차 등
제4장 적합성 평가기관의 통지	• 제35조 통지, 제36조 통지기관, 제37조 통지기관 관련 요구사항, 제39조 인증기관 관련 요구사항, 제40조 인증기관의 적합성 추정, 제42조 통지 신청, 제43조 통지 절차 등
제5장 시장감시 및 집행	• 제52조 EU 시장의 디지털 요소 포함 제품 시장감시 및 통제, 제53조 데이터 및 문서 접근, 제54조 중대한 사이버보안 위험 제품에 대한 국가 절차 등
제6장 위임권한 및 위원회 절차	• 제61조 위임의 행사, 제62조 위원회 절차
제7장 기밀유지 및 처벌	• 제63조 기밀유지, 제64조 처벌, 제65조 대표소송
제8장 경과 및 최종 규정	• 제66조 시장 감시를 강화하기 위한 규정(EU) 2019/1020 개정, 제67조 지침(EU) 2020/1828 개정, 제69조 경과 규정, 제70조 평가 및 검토, 제71조 발효 및 적용

1 REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)

■ 주요내용

① **(일반조항)** 디지털 요소가 있는 제품의 시장 출시를 위한 사이버보안 요구사항과 적용범위를 설정하고, 주요 용어를 정의하여 규정의 기본 프레임워크를 수립

○ **(적용범위)** 기기·네트워크에 대한 직·간접적인 또는 논리적·물리적 데이터 연결을 의도로 하거나 합리적으로 예측가능한 사용범위에 포함된 디지털 요소가 있는 제품

- **(중요제품)** 디지털 요소 포함 제품 중 다른 제품의 사이버보안에 중요한 기능을 수행하거나 다수의 제품이나 사용자에게 영향을 미칠 수 있는 중요기능을 수행하는 제품

- **(핵심제품)** 디지털 요소 포함 제품 중 필수 조직의 의존성이 높고 사고가 발생하거나 취약점이 노출되었을 경우 시장 공급망에 심각한 혼란을 초래할 가능성이 있는 제품

〈 중요제품 및 핵심제품 〉

구분	주요내용
중요(Important) 제품 (부속서 III에 규정)	〈 클래스 I 제품 〉 • 신원 관리 시스템 소프트웨어 및 특별권한 접속 관리 소프트웨어 • 독립형 또는 내장형 브라우저 • 패스워드 관리자 • 악성 소프트웨어를 검색, 제거 또는 격리하는 소프트웨어 • 가상사설망(VPN) 기능을 갖춘 디지털 요소가 포함된 제품 • 네트워크 관리 시스템 • 보안정보 및 이벤트 관리(SIEM) 시스템 • 부팅 관리자 • 공개키 인프라 및 디지털 인증서 발급자 • 물리적 및 가상 네트워크 인터페이스 • 운영체제 • 라우터, 인터넷 연결을 위한 모뎀 및 산업용 스위치 • 보안관련 기능을 갖춘 마이크로프로세서 • 보안관련 기능을 갖춘 마이크로컨트롤러 • 보안관련 기능을 갖춘 애플리케이션 특정 집적회로(ASIC) 및 필드 프로그래밍 가능 게이트 어레이(FPGA) • 스마트홈 범용 가상비서 • 스마트 도어록, 보안 카메라, 유아 모니터링 시스템 등 보안 기능을 갖춘 스마트 홈 제품 • 소셜 상호작용 기능이 있거나 위치 추적기능이 있는 인터넷 연결 장난감 • 건강 모니터링 목적이 있고 인체에 착용하거나 부착하는 개인용 웨어러블 제품 또는 어린이가 사용하거나 어린이를 위한 개인용 웨어러블 제품 〈 클래스 II 제품 〉 • 운영체제 및 유사환경의 가상화된 실행을 지원하는 하이퍼바이저 및 컨테이너 런타임시스템 • 방화벽, 침입탐지 및 방지 시스템 • 변조방지 마이크로프로세서 • 변조방지 마이크로컨트롤러
핵심(Critical) 제품 (부속서 IV에 규정)	• 보안박스가 있는 하드웨어 기기 • 스마트미터링 시스템 내의 스마트미터 게이트웨어 및 암호화 처리 등 고급보안 목적의 기타 장치 • 보안요소를 포함한 스마트카드 또는 이와 유사한 장치

○ **(정의)** 동 법은 주요 용어를 다음과 같이 정의

구분	주요내용
디지털 요소가 있는 제품 (Product with digital elements)	• 소프트웨어나 하드웨어 제품 및 그 원격 데이터 처리 솔루션 ※ 별도로 시장에 출시되는 소프트웨어나 하드웨어 구성요소 포함
원격 데이터 처리 (Remote data processing)	• 제조업체 또는 그 책임 하에 소프트웨어가 설계·개발된 곳에서 떨어져서 이루어지는 데이터 처리로, 데이터 처리가 없으면 제품의 기능 수행을 방해할 수 있는 것
경제사업자 (Economic operator)	• 제조업자, 공인대리인, 수입업자, 유통업자 또는 본 규정에 따라 디지털 요소 포함 제품의 제조나 시장 출시와 관련된 의무를 지는 기타 자연인/법인
제조업자 (Manufacturer)	• 디지털 요소 포함 제품을 개발/제조하거나 설계/개발/제조하도록 하여 자신의 이름이나 상표로 유료/무료로 시장에 출시하는 자연인/법인
오픈소스 소프트웨어 관리자 (Open-source software steward)	• 제조업자가 아닌 법인으로서, 상업적 활동을 위한 자유·오픈소스 소프트웨어인 특정 디지털 요소 포함 제품의 개발을 지속적으로 지원하고 해당 제품의 생존성을 보장하는 자
공인대리인 (Authorised representative)	• EU 내에 설립된 자연인/법인으로서 제조업자로부터 특정 업무수행을 위한 서면위임을 받은 자
수입업자 (Importer)	• EU 내에 설립된 자연인/법인으로서 EU 외 설립된 자연인/법인의 이름이나 상표가 부착된 디지털 요소 포함 제품을 시장에 출시하는 자
유통업자 (Distributor)	• 제조업자나 수입업자가 아닌 공급망 내 자연인/법인으로서 제품의 특성에 영향을 주지 않고 EU 시장에서 디지털 요소 포함 제품을 유통하는 자
통지기관 (Notifying authority)	• 적합성 평가기관의 평가, 지정, 통보를 위한 필요 절차 수립/수행 및 모니터링을 담당하는 국가기관
적합성 평가 (Conformity assessment)	• 부속서 I의 필수 사이버보안 요구사항 충족 여부를 확인하는 과정
적합성 평가기관 (Conformity assessment body)	• 인증 및 시장감시 관련 규정(EC) 765/2008 제2조(13)에 정의된 적합성 평가기관
인증기관 (Notified body)	• 제43조와 기타 관련 EU 조화법령에 따라 지정된 적합성 평가기관
실질적 수정 (Substantial modification)	• 시장 출시 후 제품의 변경으로서, 부속서 I 제I부의 필수 사이버보안 요구사항 준수에 영향을 미치거나 평가된 의도된 목적을 수정하는 경우
CE 마킹 (CE marking)	• 제조업자가 제품과 프로세스가 부속서 I의 필수 사이버보안 요구사항 및 기타 관련 EU 조화법령을 준수함을 나타내는 표시
중대한 사이버보안 위험 (Significant cybersecurity risk)	• 기술적 특성상 상당한 물질적/비물질적 손실이나 중단을 초래할 수 있는 사고의 발생 가능성이 높다고 가정할 수 있는 사이버보안 위험
악용 가능한 취약점 (Exploitable vulnerability)	• 실제 운영 조건에서 적대자가 효과적으로 사용할 수 있는 잠재성이 있는 취약점
적극적으로 악용되는 취약점 (Actively exploited vulnerability)	• 악의적 행위자가 시스템 소유자의 허가 없이 시스템에서 악용했다는 신뢰할 만한 증거가 있는 취약점

② **(사이버보안 의무사항)** 디지털 요소가 있는 제품의 필수 사이버보안 요구사항과 경제사업자인 제조업체, 수입업체, 유통업체 등의 사이버보안 의무사항을 규정

○ **(제품 사이버보안 요구사항)** 디지털 요소가 있는 제품은 필수 사이버보안 요구사항과 제조업자의 취약점 처리 요구사항을 모두 충족할 때 시장 출시가 가능

구분	주요내용
필수 사이버보안 요구사항	• 적절한 수준의 사이버보안을 보장하는 방식으로 **제품 설계·개발·생산** • 악용가능한 취약점이 없는 상태로 제품 납품 • 제품을 원래 상태로 재설정할 수 있는 기능 • 자동 보안 업데이트, 명확하고 사용하기 쉬운 옵트아웃 메커니즘 등을 통한 취약점 해결 • 인증, 신원확인, 접속 관리 시스템 등 **무단 접속으로부터 보호** • 저장, 전송 또는 처리된 **데이터의 기밀성 보호** • 승인되지 않은 조작, 수정으로부터 데이터, 프로그램, 구성의 무결성 보호 • 데이터 활용과 관련해 적절하고 관련성이 있는 것으로 제한하여 처리 • 서비스 공격 거부에 대한 탄력성, 완화 등 필수 기능 보호 • 다른 장치나 네트워크가 제공하는 부정적인 영향 최소화 • 외부 인터페이스를 포함한 공격 표면을 제한하도록 **설계·개발·생산** • 악용 완화 매커니즘·기술을 활용해 사고의 영향을 줄이는 **설계·개발·생산** • 데이터, 서비스, 기능에 대한 접근 또는 수정을 포함하여 관련 내부 활동을 기록·모니터링하여 보안 관련 정보 제공 • 사용자가 모든 데이터와 설정을 영구적으로 안전하고 쉽게 삭제할 수 있는 기능 제공
제조업자의 취약점 처리 요구사항	• 제품의 최상위 종속성을 포함하여 기계로 읽을 수 있는 형식의 **소프트웨어자재명세서(SBoM)* 작성** 등 제품에 포함된 취약성 및 구성요소 식별, 문서화 • 보안 업데이트를 제공하는 등 지체없이 취약점을 해결 및 수정 • 제품의 보안에 대한 효과적이고 **정기적인 시험과 검토** • 보안 업데이트 시 취약점 설명, 영향 받는 제품 정보, 취약점의 영향, 심각도, 취약점 개선에 도움이 되는 정보를 포함해 고정된 취약점에 대한 정보 공개 • 조정된 취약점 공개에 대한 정책 수립 및 시행 • 제품 취약점을 디지털 요소로 보고하기 위한 연락처 제공 등 제품의 잠재적 취약점에 대한 정보를 제3자 구성요소와 쉽게 공유할 수 있도록 조치 • 공격 가능한 취약점이 적시에 수정, 완화되도록 보장하기 위해 제품에 대한 **업데이트를 안전하게 배포하는 매커니즘 제공** • 보안 문제 해결을 위해 보안 업데이트를 하는 경우, 사용자가 취할 수 있는 조치 등 관련 정보를 제공하는 메시지와 지체 없이 무료 배포되도록 보장

- (고위험 AI 시스템) 고위험 AI 시스템 역시 상기 사이버보안 요구사항을 모두 충족해야 하며, 본 규정에 따라 발행된 EU 적합성 선언을 통하여 보안수준을 입증해야 함

○ **(경제사업자의 의무)** 제조업체, 수입업자, 유통업자 등 경제사업자별로 제품의 설계부터 유통까지 전 과정에서의 사이버보안 의무사항 등을 명확히 규정

구분	주요내용
제조업체	• **(위험관리 등)** 사이버보안 위험평가를 수행하고, 평가결과를 반영한 설계를 하며, 취약점 최소화 조치를 실시해야 함 • **(문서화)** 기술문서를 작성 및 보관하고, 적합성 선언을 작성하며, 제품 식별정보를 제공해야 함 • **(지원)** 최소 5년의 지원기간을 보장하고, 보안 업데이트를 10년간 유지해야 함 • **(보고)** ▲취약점은 24시간 내 초기통지, 72시간 내 상세보고, 14일 내 최종보고 해야하고, ▲심각한 사고는 24시간 내 조기경보, 72시간 내 사고통지, 1개월 내 최종보고를 완료해야 함 – (보고내용) 사고 및 취약점 상세정보를 포함하고, 영향 평가 및 범위를 분석하며, 대응 조치 계획을 수립해야 함

구분	주요내용
공인대리인	• **(보관)** EU 적합성 선언과 기술문서를 시장 출시 후 10년 또는 지원기간 중 더 긴 기간 동안 시장감시당국이 이용할 수 있도록 보관 • **(정보제공)** 시장감시당국의 합리적 요청 시 제품의 적합성 입증에 필요한 모든 정보와 문서 제공 • **(협력)** 위임받은 제품의 위험 제거를 위한 조치에 대해 시장감시당국과 협력
수입업자	• 시장 출시 전, 적합성 평가 확인, 필수 문서 구비 검증, 제조업체 정보확인을 실시햐야 함 • 부적합 제품을 시정하고, 당국과 협력하며 정보를 제공하고, 문서를 10년 이상 보관해야 함
유통업자	• CE 마킹을 확인하고, 문서의 완전성을 검증하며, 제조업체/수입업자 정보를 확인 • 취약점을 제조업체에 즉시 통보하고, 시정 조치를 이행하며, 당국과 협력할 의무가 있음
오픈소스 소프트웨어 관리자	• 오픈소스 소프트웨어 관리자는 안전한 제품 개발과 취약점의 효과적 처리를 위한 사이버보안 정책을 수립·문서화하고, 자발적 취약점 보고와 오픈소스 커뮤니티 내 정보 공유를 촉진해야 함

③ **(적합성 평가)** 제품의 사이버보안 요구사항 충족 여부를 검증하기 위한 표준화된 적합성 평가 절차와 CE 마킹 규정을 제시

○ **(적합성 선언)** 제조업체는 제품의 필수 사이버보안 요구사항 충족을 입증하기 위해 부속서에서 정한 형식과 절차에 따라 일반 또는 간소화된 EU 적합성 선언을 작성해야 함

구분	주요내용
일반 적합성 선언서	• ▲제품식별 정보, ▲책임자 정보(제조업체나 공인대리인의 상세 연락처), ▲법적 책임, ▲제품 설명, ▲규정준수, ▲기술참조(적용된 표준, 규격, 인증정보), ▲평가정보(인증기관 및 평가 절차 세부사항), ▲인증서명(책임자 서명, 날짜, 장소)을 포함해야 함
간소화된 적합성 선언서	• "[제조업체명]은 [제품명/모델명]이 EU 규정을 준수함을 선언합니다"와 같은 핵심정보를 포함하고, 전체 적합성 선언문을 확인할 수 있는 웹사이트 주소 제공 • 소비자 친화적 형태로, 제품 패키지나 퀵가이드 등에 포함 가능

○ **(적합성 평가)** 제조업체는 디지털 요소 포함 제품의 필수 사이버보안 요구사항 충족을 입증하기 위해, 제품의 중요도(일반/중요/핵심)와 적용가능한 표준 및 인증체계에 따라 내부통제, EU 유형검사, 품질보증 등 적절한 적합성 평가 절차를 수행해야 함

구분	주요내용
디지털 요소가 있는 제품	• 제조업체는 다음 절차 중 하나를 사용하여 필수 사이버보안 요구사항의 적합성을 입증 - 부속서 VIII에 명시된 내부통제 절차**(모듈 A 기준)** - 부속서 VIII에 명시된 EU형 심사절차**(모듈 B 기준)**와 부록 VIII에 명시된 내부 생산통제에 기반한 EU형 적합성 평가**(모듈 C기준)** - 부속서 VIII에 명시된 전체품질 보증에 기반한 적합성 평가**(모듈 H 기준)**
클래스 I 제품	• 클래스 I 제품은 제조업체가 EU 조화표준, 공통규격, 유럽 사이버보안인증을 신청하지 않았거나 일부만 적용한 경우 다음 절차 중 하나를 이용해 평가 - 부속서 VIII에 명시된 EU형 심사절차**(모듈 B 기준)**와 부속서 VIII에 명시된 내부 생산관리 **(모듈 C 기준)**을 기반으로 한 EU형 적합성 평가 - 부속서 VII에 명시된 전체품질 보증에 기반한 적합성 평가**(모듈 H 기준)**
클래스 II 제품	• 클래스 II 제품은 다음 중 하나를 이용해 평가 - 부속서 VIII에 명시된 EU형 심사절차**(모듈 B 기준)**와 부속서 VIII에 명시된 내부 생산통제에 기반한 EU형 적합성**(모듈 C 기준)** - 부속서 VIII에 명시된 전체품질 보증에 기반한 적합성 평가**(모듈 H 기준)**

○ **(CE 마크)** 시장 출시 전 제품의 적합성에 대한 규정 요구사항을 준수하였다는 표시로 CE 마크를 부착해야 함

- (CE 마크의 일반원칙)[2] CE마크는 인증 및 시장감시에 대한 요구사항 관련 규정에 따른 일반원칙에 따라, 가시성과 영구성을 확보하고 제품 및 포장에 표시

- (CE 마크의 부착기준) 시장 출시 전, 눈에 띄게 읽기 쉽고 지워지지 않게 제품에 부착해야 함

○ **(통지기관)** 회원국은 적합성 평가기관의 평가·지정 및 모니터링을 위해 독립적인 단일 통지 당국을 지정하고, 이의 효율적 운영을 위한 조직 구성과 권한 위임 체계를 구축해야 함

- (기본체계) 회원국은 적합성 평가기관의 관리를 위해 독립적 운영 구조, 전문 인력, 내부 감사 체계를 갖춘 단일 통지 당국을 지정하고 운영해야 하고, 통지 당국은 적합성 평가기관의 평가·지정, 인증기관 모니터링, 성과 평가 및 국제 협력 등의 핵심 책임을 수행

- (권한위임) 통지 당국은 평가·모니터링, 행정 지원, 기술 검증, 문서 관리 등의 업무를 적격한 기관에 위임할 수 있고, 권한을 위임받는 기관은 법인격과 독립성을 보유하고, 전문성 증명 및 책임 보험 가입 등의 조건을 충족해야 함

④ **(시장감시 및 집행)** 회원국의 시장 감시 활동, 위험 제품 처리 절차, EU 차원의 보호조치 등 규정의 효과적 집행을 위한 체계를 수립

○ **(시장감시)** 회원국은 디지털 요소 포함 제품의 시장 안전성을 확보하기 위해 독립적인 감시 당국을 지정하고 정기감시와 특별조사를 수행하며, 관련 기관과의 협력 네트워크를 구축·운영해야 함

- (기본체계) 회원국은 독립적 의사결정 구조와 전문인력을 갖춘 전담 감시당국을 지정하고 충분한 자원과 권한을 부여해야 하며, CSIRT, ENISA, 타 회원국 등과의 협력 네트워크를 구축·운영해야 함

- (감시활동) 위험기반 점검과 샘플 테스트를 포함한 정기적 시장 모니터링을 실시하고 결과를 분석·보고하고, 신고/제보 처리, 긴급 상황 대응, 심층 조사 및 증거 수집 등 특별조사 수행

○ **(국가 차원의 검토 및 중단)** 회원국은 중대한 사이버보안 위험이 확인된 제품에 대해 종합적인 위험평가를 실시하고, 평가 결과에 따라 시장출시 중단, 리콜 등 필요한 시정 조치를 취해야 함

- (위험평가) 기술적·비기술적 요소와 공급망 위험, 사용자 영향을 포함한 종합적 위험평가를 수행하고, 초기 스크리닝, 상세 분석, 전문가 자문 및 이해관계자 의견 수렴 절차를 진행

2 Regulation (EC) No 765/2008 제30조 적용

- (시정조치) 시장 출시 중단, 리콜, 사용자 통지, 보안 패치 배포 등 필요한 조치를 실시하고, 조치의 이행을 모니터링하고 효과성을 평가하며 필요시 추가 조치 검토

○ **(EU 차원의 조치)** 집행위원회는 회원국의 조치만으로는 충분하지 않거나 광범위한 영향이 예상되는 경우, ENISA 및 회원국과 협의하여 EU 차원의 긴급 조치나 시장제한 조치를 취할 수 있음

- (집행위원회 개입) 즉각 개입이 필요하거나 회원국 조치가 미흡한 경우, 광범위한 영향이나 시스템적 위험이 있을 때 개입하고, ENISA 분석요청, 회원국 협의주도, 긴급조치 명령 등을 수행할 수 있음

- (이행 체계) 이해관계자 협의와 비례성 원칙 준수를 바탕으로 적절한 조치를 결정하고, 이행 상황을 점검하고 효과성을 평가하며 필요시 조치를 조정

⑤ **(벌칙 등 기타조항)** 규정위반에 대한 처벌기준 및 발효 등과 관련된 최종규정 마련

○ **(기밀성)** 본 규정에 따라 취득한 정보의 기밀성을 보장하기 위해 지식재산권, 영업비밀, 보안 관련 정보를 체계적으로 보호하고, 정보공유 시 엄격한 조건과 보안 요구사항을 준수해야 함

○ **(처벌)** 본 규정 위반에 대해 위반의 성격과 영향을 고려한 체계적인 처벌 체계를 수립하고, 중소기업 등 특수한 상황을 고려한 처벌 절차를 운영

- (처벌체계) 필수 요구사항 위반 시 최대 1,500만 유로나 매출의 2.5%, 보고/문서화 위반 시 1,000만 유로나 매출의 2%를 부과하며, 위반의 고의성, 피해 규모, 시정 노력 등을 종합적으로 고려하여 처벌수준을 결정

- (특별 규정) 중소기업에 대한 비례적 처벌과 공공기관에 대한 회원국별 특별 규정을 적용하고, 체계적인 조사와 의견 청취를 거쳐 처벌을 결정하며 이의제기 및 사법적 구제 절차를 보장

○ **(전환 및 최종규정)** 법 시행의 단계적 적용과 기존 인증의 유효성 인정 등 원활한 제도 이행을 위한 전환 규정을 마련

- (전환규정) 기존 인증의 유효성을 유지하면서 실질적 수정이 있는 경우를 구분하여 단계적으로 새로운 규정을 적용하고, 신규 제품에 대해서는 36개월 이후 전면 적용

- (평가 및 검토) 본 규정의 효과성, 기술적 적절성, 국제 경쟁력을 정기적으로 평가하고, 보고 플랫폼의 성능과 정보공유 체계를 지속적으로 모니터링

- (발효 및 적용) 공식관보 게재 후 20일 후 발효되며, 일반 규정 36개월, 보고 의무 21개월, 인증기관 18개월 등 분야별로 차등 적용

■ 전망 및 시사점

○ EU 시장에 공급되는 디지털 요소가 포함된 제품의 생애주기 전반에서 보안 관리를 강화하고, 소비자가 제품을 선택하고 사용할 때 보안을 고려할 수 있도록 입법화

- 보안내재화(security by design), 공급망 보안(SBoM), 안전한 보안업데이트 매커니즘 제공, 취약점 개선 등 제조업자의 보안 관리를 의무화하고, 시장 출시 전 적합성 평가 수행 및 CE마크를 부착하도록 규정

○ 특히, EU 시장에 공급되는 ICT 제품·서비스에 대한 사이버보안 인증체계가 확립되고 제품 제조·수입업자, 서비스 제공자에 대한 보안의무가 강화될 경우, EU시장과 거래하는 외국기업도 영향을 받을 수 있음

○ 한편, 제조업체 등 경제사업자가 동 법에서 요구하는 엄격한 의무사항을 준수하는데 부담이 예상되어 규정의 실효성에 대한 의문이 제기

Reference

▪https://www.consilium.europa.eu/en/press/press-releases/2024/10/10/cyber-resilience-act-council-adopts-new-law-on-security-requirements-for-digital-products/

▪https://www.european-cyber-resilience-act.com/

▪https://data.consilium.europa.eu/doc/document/PE-100-2023-INIT/en/pdf

해외 입법 동향

EU,「제조물 책임지침」개정

디지털 시대가 도래함에 따라 소프트웨어 등 새로운 '제조물'의 개념을 도입하기 위하여, EU 집행위원회는 약 40년 전에 채택된 기존「제조물 책임지침[1]」(Product Liablility Directive, PLD)을 전면 개정 (2024. 11. 18.)

■ 개요

○ 디지털 시대에 맞춰 EU의 제품책임 체계를 현대화하고, 결함 제품으로 발생할 수 있는 소비자 피해에 대한 구제수단 마련

- 기존「제조물 책임지침」(이하 PLD)이 도입한 무과실책임 원칙에 따라, 피해자는 제품의 결함과 피해 발생 간의 인과관계만 입증하면 보상이 가능

〈 주요 논의경과 〉

구분	주요내용
2022년 9월	• EU 집행위원회는 ▲AI, 소프트웨어 등 디지털 제품을 포함하고 ▲온라인 마켓플레이스의 책임규정을 신설하며, ▲입증부담 완화 등 소비자 보호 강화방안 등을 제시한 포괄적 개정안 발표
2023년 12월	• EU 이사회, 의회, 집행위원회 간 삼자협의(Trilogue)를 통하여 잠정 합의안을 도출하고 주요 쟁점 사항(▲AI 시스템의 책임범위, ▲입증책임 완화기준, ▲온라인 마켓플레이스의 책임조건, ▲개발위험 항변(development risk defence)의 적용범위 등)에 대한 절충안을 마련
2024년 3월	• EU 의회 본회의에서 전체회의 투표를 통해 최종법안(회원국 이행을 위한 구체적 지침 포함) 승인
2024년 11월	• EU 공식관보 게재

■ 주요내용

○ **(목적)** 결함 제품으로 인한 피해에 대하여 경제사업자의 무과실책임 원칙을 확립하고 피해자 보상 체계를 규정함으로써 EU 내부 시장의 기능 향상과 소비자 보호를 도모

○ **(적용범위)** 본 지침은 발효일로부터 24개월 후 시장에 출시되거나 서비스가 개시되는 제품에 적용되는 한편, 상업적 활동 외에서 개발·제공되는 무료 오픈소스 소프트웨어 등은 제외됨

※ 무료 오픈소스 소프트웨어 : 오픈소스 소프트웨어가 상업적 활동 외에서 개발·제공되는 경우, 비영리 조직이 무료로 제공하거나 오픈 저장소를 통해 공유하는 것은 시장 출시로 간주되지 않음

1 DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on liability for defective products and repealing Council Directive 85/374/EEC

○ **(정의)** 동 규정은 주요 용어를 다음과 같이 정의하고 특히 제품의 영역을 전기, 디지털 제조파일, 소프트웨어 등으로 확대하여 새로운 제조물 개념을 도입

구분	주요내용
제품 (Prodcut)	• ▲모든 동산, ▲다른 동산이나 부동산에 통합/연결된 경우도 포함, **▲전기, 디지털 제조 파일, 원자재, 소프트웨어 포함**
디지털 제조 파일 (Digital manufacturing file)	• ▲유형물 생산에 필요한 기능적 정보를 포함한 디지털 버전/템플릿, ▲기계나 도구(드릴, 선반, 밀링머신, 3D 프린터 등)의 자동제어를 가능하게 하는 파일
제조업체의 통제 (Manufacturer's control)	• 제조업체가 다음을 수행하거나 제3자의 행위에 대해 승인/동의하는 경우 – 구성요소(소프트웨어 업데이트/업그레이드 포함)의 통합, 연결, 공급 – 제품의 수정(실질적 수정 포함) • 제조업체가 직접 또는 제3자를 통해 소프트웨어 업데이트/업그레이드를 제공할 수 있는 능력 보유
제조업체 (Manufacturer)	• ▲제품을 개발, 제조, 생산하는 자연인/법인, ▲제품 설계/제조를 의뢰하는 자, ▲자신의 이름, 상표, 식별표시를 제품에 부착하여 제조업체로 표시하는 자,▲자가 사용을 위해 제품을 개발, 제조, 생산하는 자
공인대리인 (Authorised representative)	• ▲EU 내 설립된 자연인/법인, ▲제조업체로부터 특정 업무수행을 서면 위임받은 자
수입업체 (Importer)	• 제3국의 제품을 EU 시장에 출시하는 자연인/법인
유통업체 (Distributor)	• 제조업체나 수입업체가 아닌 공급망 내 제품 공급자
실질적 수정 (Substantial Modification)	• 제품 안전 관련 EU/국가 규정상 실질적 수정으로 간주되는 경우 • 관련 규정이 없는 경우 다음 조건 충족 시 – 제품의 원래 성능, 목적, 유형의 변경(제조업체의 최초 위험평가에서 예상치 못한 변경) – 위험의 성격 변경/새로운 위험 창출/위험 수준 증가

○ **(보상범위의 확대)** 결함 제품으로 인한 피해에 대하여 제조업체 등의 무과실책임을 원칙으로 하되, 피해자의 입증부담을 완화하고 책임주체와 보상범위를 디지털 시대에 맞게 확대

– (손해배상의 범위) 결함 제품으로 인한 배상 가능한 손해의 유형과 범위를 규정하고, 특히 데이터의 파괴나 손상에 대하여 복구 및 복원비용 등을 보상받을 수 있도록 규정

구분	주요내용
인적 손해	• 사망이나 신체적 상해, 의학적으로 인정된 정신적 건강 손상에 대한 보상이 이루어져야 함
재산적 손해	• 결함 제품 자체를 제외한 재산상 손해는 배상 대상이 되나, 제조업체 통제하의 결함 구성요소가 통합된 제품이나 전문적 목적으로만 사용되는 재산의 손해는 제외
데이터 손해	• 전문적 목적이 아닌 데이터의 파괴나 손상에 대해 복구 및 복원 비용을 포함한 보상이 가능

○ **(경제사업자의 책임)** 결함 제품에 대한 책임은 제조업체와 결함 구성요소 제조업체가 1차적으로 부담하되, EU 역외 제조업체의 경우 수입업체, 공인대리인 등이 순차적으로 책임을 지며, 이들을 확인할 수 없는 경우 유통업체가 보충적 책임을 부담

1차 책임		EU 역외 제조업체 관련 책임		유통업체 책임
• 결함 제품의 제조업체와 제조업체 통제하에 통합/연결된 결함구성요소의 제조업체가 1차 책임 부담	▶	• EU 역외 제조업체의 경우 수입업자, 공인대리인, 그리고 이들이 없는 경우 풀필먼트 서비스 제공자가 순차적으로 책임을 부담	▶	• 책임있는 경제사업자를 1개월 이내에 확인하지 못하는 경우 유통업체가 보충적 책임을 부담

○ **(입증책임의 면책사유) ▲제조업체/수입업체/유통업체가** 해당 제품을 시장에 출시/공급하지 않은 경우, ▲시장출시 시점에 결함이 없었거나, 법적 요구사항 준수로 결함이 발생했거나, 당시 과학기술 수준으로 결함을 발견할 수 없었던 경우, **▲결함 구성요소 제조업체는** 완제품을 설계하는 제조업체의 지시에 따라 결함이 발생한 경우에 입증책임이 면책됨

- 다만, ▲제조업체의 통제 범위 내에서 관련 서비스나 소프트웨어로 인한 결함이 발생한 경우, ▲안전 유지에 필요한 소프트웨어 업데이트 미제공이나 실질적 수정으로 인한 결함의 경우 면책을 제한

○ **(최종규정)** 회원국의 이행의무, 발효 등 실효적 적용을 위한 절차적 사항을 규정

- **(국내법 전환)** 회원국은 본 지침 시행일로부터 24개월 이내에 법률, 규정, 행정조치 등 관련 법규를 정비하고 본 지침을 참조하는 표시를 의무화해야 함

- **(발효)** 본 지침은 EU 관보에 게재된 날로부터 20일 후에 발효되며, 모든 공식 언어본이 동등한 효력을 가지고 회원국에 즉시 통보

■ 전망 및 시사점

○ 개정된 PLD는 기존의 EU 디지털 규제(AI법, 디지털서비스법, 사이버복원력법 등)와 연계되어 디지털 제품 안전과 소비자 보호를 강화할 것으로 전망

- 이번 개정으로 제품책임 보험시장이 확대되고 기업들의 제품 안전 관리가 강화될 것으로 예상되며, EU의 새로운 제조물 책임기준이 국제교역 환경에도 큰 영향을 미칠 것으로 전망

○ 전문가들은 입증책임 완화와 보상 범위 확대로 소비자의 실질적 권리구제가 용이해질 것으로 예상하는 한편, 기업들의 책임 범위가 확대됨에 따라 기업 부담이 증가할 수 있어 제품 안전관리 체계 고도화와 보험가입 등 선제적 대응이 필요할 것으로 전망

Reference

▪https://data.consilium.europa.eu/doc/document/PE-7-2024-INIT/en/pdf
▪https://www.consilium.europa.eu/en/press/press-releases/2024/10/10/eu-brings-product-liability-rules-in-line-with-digital-age-and-circular-economy/
▪https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739341/EPRS_BRI(2023)739341_EN.pdf
▪https://www.europarl.europa.eu/legislative-train/carriage/new-product-liability-directive/report?sid=8501

해외 입법 동향

EU, 「사이버보안법」 개정안 및 「사이버연대법」 채택

EU 이사회는 사이버보안 입법 패키지의 일환으로 사이버 연대와 능력 강화를 위한 「사이버보안법」 개정안과 「사이버연대법」을 채택 (2024. 12. 2)

■ 개요

○ EU 이사회는 사이버 위협에 대한 탐지·대비·대응을 위한 EU의 연대와 능력을 강화하기 위해 「사이버보안법(Cyber Security Act)」 개정안과 「사이버 연대법(Cyber Solidarity Act)」을 각각 채택함

○ 동 법안은 사이버공격의 규모, 빈도 및 영향이 EU와 글로벌 수준에서 증가하고 있는 점을 고려하여, 네트워크 및 정보시스템의 기능에 대한 심각한 위협에 대응하기 위해 마련됨

- 특히 우크라이나에 대한 러시아의 전쟁 이후 지정학적 긴장 상태에서 다양한 행위자들이 관련된 위협이 지속될 것으로 예상되어 EU의 사이버보안 프레임워크 강화 요구

○ 이에 따라 EU는 디지털 경제 전반에 걸쳐 산업과 서비스의 경쟁력을 강화하고, 디지털 전환을 지원하기 위해 디지털 단일시장의 사이버보안 수준을 강화하는 것이 필요하다고 판단

- 시민, 기업(마이크로기업, 중소기업 및 스타트업 포함), 핵심 인프라 운영 기관의 사이버 위협에 대한 회복력 증대가 필요

○ EU는 이미 핵심 인프라와 기관의 취약성을 줄이고 위험에 대한 복원력을 높이기 위한 여러 조치를 취해왔으나, 진화하는 위협 환경에 대응하기 위해 보다 포괄적이고 체계적인 접근이 필요한 상황임

■ 「사이버연대법」 주요내용

○ **(목적)** EU의 디지털 경제 전반에서 산업과 서비스의 경쟁력을 강화하고, 사이버보안 분야에서 EU의 기술 주권과 전략적 자율성에 기여하기 위함

- (구체적 목적) EU의 사이버 위협·사고 감지 능력과 상황 인식을 강화하고, 핵심분야 운영 기관의 대비태세를 강화하며 대규모 사이버보안 사고 대응을 위한 연대를 강화하고, 중대한 사이버보안 사고나 대규모 사이버보안 사고에 대한 검토·평가를 통해 EU의 복원력을 제고함

- (시행 범위) 회원국의 권한을 존중하면서 CSIRTs 네트워크[2], EU-CyCLONe[3], NIS 협력그룹의 활동을 보완함

○ **(시행체계)** Digital Europe Programme (DEP)[4]을 통한 시행

- (기본 원칙) 본 규정에 따른 조치들은 DEP를 통해 자금을 지원받으며, Regulation (EU) 2021/694의 Specific Objective 3[5]에 따라 시행됨

- (시행 주체) European Cybersecurity Alert System[6]과 기타 조치들은 주로 ECCC[7]를 통해 시행되나, EU Cybersecurity Reserve[8]는 EU 집행위원회와 ENISA가 시행함

- (예산 운영) 사이버보안 긴급대응체계 및 상호 지원 조치에 대해서는 사용하지 않은 예산의 이월이 허용되며, 다음 회계연도 12월 31일까지 집행 가능

○ **(사이버보안 경보체계)** 사이버 위협 탐지 및 정보공유를 위한 범유럽 인프라 구축 (제3조 내지 제9조)

- (참여 및 구성) 각 회원국은 자발적으로 참여하여 국가 차원의 위협 탐지 활동을 조정하는 단일 국가 사이버허브를 지정하고, 3개 이상 회원국이 참여하는 국경간 사이버허브를 구성하여 위협 탐지와 정보 공유 플랫폼으로 활용

- (자금 지원) ECCC는 국가 사이버허브 및 국경간 사이버허브의 도구, 인프라, 서비스 공동 조달을 지원하며, 국가 사이버허브는 EU 기여금으로 최대 50%, 국경간 사이버허브는 최대 75%까지 지원받음. 2년 내 Cross-Border Cyber Hub에 참여하지 않는 경우 추가 지원 제한

- (협력체계) CSIRTs 네트워크와 절차적 협력 방안 합의, 대규모 사이버보안 사고 발생 가능성이 있는 경우 EU-CyCLONe에 관련 정보와 조기 경보를 제공, ENISA는 법 시행 후 12개월 내에 발행하는 상호운용성 가이드라인(정보공유 형식 및 프로토콜 포함)에 따라 사이버허브 간 협력협정 체결

- (보안 요건) 참여 회원국은 높은 수준의 사이버보안, 기밀성, 데이터 보안을 보장하며, EU·국가 데이터보호법과 경쟁법을 준수해야 함

---

2 'Computer Security Incident Response Teams Network'의 약자로, EU 회원국의 CSIRT들과 CERT-EU로 구성된 네트워크. NIS 지침(Directive (EU) 2022/2555)에 따라 설립되었으며, 회원국 간의 신속하고 효과적인 운영 협력을 촉진하기 위한 조직

3 EU Cyber Crisis Liaison Organisation Network의 약자. 대규모 사이버보안 사고와 위기 상황에 대한 조정된 관리를 지원하기 위한 네트워크로, 회원국과 EU 기관들 간의 정기적인 정보 교환을 보장하며, 대규모 사이버 사고나 위기 상황에 대한 공동 상황 인식을 개발하는 역할을 담당

4 EU의 디지털 기술 개발 및 보급을 지원하는 자금 지원 프로그램으로, Regulation (EU) 2021/694를 통해 2021-2027 기간 동안 운영

5 DEP의 다섯 가지 특정 목표 중 하나로 "사이버보안 및 신뢰" 분야를 다루고, EU의 사이버보안 역량과 인프라 강화를 목표로 함

6 사이버 위협 탐지 및 정보 공유를 위한 범유럽 인프라를 의미. 국가 사이버허브와 국경간 사이버허브로 구성

7 European Cybersecurity Industrial, Technology and Research Competence Centre. EU의 사이버보안 산업, 기술, 연구 역량 센터로, 사이버보안 관련 자금과 프로젝트를 관리하는 중심 기관

8 신뢰할 수 있는 관리형 보안서비스 제공자들의 서비스로 구성된 예비대로, 중대하거나 대규모 사이버보안 사고 대응 지원

○ **(사이버보안 긴급대응체계)** 사이버 사고 대응을 위한 EU 차원의 지원체계 구축

- (목적 및 범위) 회원국의 노력을 보완하여 중대한 사이버보안 사고나 대규모 사이버보안 사고에 대한 대비, 대응, 복구를 지원하고, UCPM[9], IPCR[10] 등 기존 EU 위기대응 체계와 조정하여 운영

- (예비대 구성) EU 사이버보안 예비대는 신뢰할 수 있는 관리형 보안서비스 제공자들의 서비스로 구성되며, 사전 확보된 서비스를 포함함. 집행위원회가 전반적인 구현 책임을 지고 NIS 협력그룹과 협의하여 우선순위를 결정

- (지원 절차) 회원국 사이버 위기관리기관, CSIRTs, CERT-EU를 통해 지원을 요청할 수 있으며, 계약당국은 48시간 이내에 응답. 요청 시 영향받는 기관 정보, 잠재적 영향, 요청 서비스 등의 정보 포함 필요

- (우선순위) 동시 요청 시 사고의 규모와 심각성, 영향받는 기관의 유형, 잠재적 영향, 국경 간 확산 위험, 기존 대응 조치를 고려하여 결정. 동등 평가 시 회원국 요청 우선

○ **(DEP 연계국 지원)** DEP 연계 국가에 대한 EU 사이버보안 예비대 지원

- (지원 요건) DEP 연계 협정에 EU 사이버보안 예비대 참여가 명시된 국가로서, 지원 신청 전 3개월 내 자국의 사이버 복원력 및 위험관리 능력 정보를 제출하고, 3가지 기준(협정 준수, 사고 대비 적절성, EU 정책과의 일관성)을 모두 충족해야 하며, 집행위원회는 High Representative[11]와 협의하여 공동 외교안보정책과의 정합성을 평가함

- (승인 절차) 집행위원회가 평가 및 High Representative와 협의 후 이사회에 제안하면, 이사회가 implementing acts[12]로 승인하고, 특별한 경우 이사회는 자체 발의로 승인 내용 수정 또는 철회 가능

- (지원 조건) 지원은 최대 1년간 제공되며 갱신 가능하고, 집행위원회는 implementing acts에서 단일 요청에 대한 지원을 최소 75일 이상으로 제한할 수 있음

○ **(사고 분석체계)** 중대한 사이버보안 사고에 대한 분석 및 평가체계 마련

- (분석 수행) 집행위원회나 EU-CyCLONe의 요청에 따라 ENISA가 CSIRTs 네트워크의 지원과 관련 회원국의 승인을 받아 중대한 사이버보안 사고나 대규모 사이버보안 사고에 대한 검토·평가를 수행

- (보고서 작성) ENISA는 회원국, EU 기관, 민간부문 대표 등과 협력하여 사고 검토 보고서를 작성. 보고서는 사고의 원인, 영향, 완화조치를 평가하고 필요시 EU의 사이버보안 태세 개선을 위한 권고사항 포함

9 Union Civil Protection Mechanism. EU 시민보호 메커니즘의 약자로, 자연재해나 인공재해에 대한 EU 차원의 협력 체계
10 EU Integrated Political Crisis Response. EU 통합 정치적 위기 대응 체계로, 주요 위기 상황에 대한 EU 차원의 조정된 대응을 위한 체계
11 EU 외교안보정책 고위대표로, EU의 공동 외교안보정책을 대표하고 조정하는 역할
12 EU 법률의 시행을 위한 집행 법률. 집행위원회가 채택하는 구체적인 이행 조치

- (정보보호) 보고서는 EU나 국가법에 따른 민감·기밀정보 보호 요건을 준수하며, 요청 시 정보를 익명화함. 현재 악용 중인 미패치 취약점의 세부사항은 포함하지 않음

○ **(시행)** 동 법안은 EU 관보 게재 후 20일째 되는 날부터 시행

■ 「사이버보안법」 개정안 주요내용

○ **(개정 목적)** ICT 제품 등에 대한 기존 사이버보안 인증체계를 관리형보안서비스로 확대

- (체계 보완) 기존 ICT 제품, 서비스, 프로세스에 대한 인증체계를 관리형보안서비스까지 확대하여 EU 내 적절한 사이버보안 수준을 보장하고, 인증체계의 분절화를 방지함

- (시장 강화) 내부 시장 기능을 향상시키고 역내 서비스의 신뢰성에 대한 보증을 제공하며, 이를 통해 EU의 사이버공격 대응 복원력을 강화함

○ **(인증 대상)** 관리형보안서비스에 대한 인증체계 적용 범위 규정

- (서비스 범위) 사이버보안 위험 관리 활동의 수행 또는 지원과 관련된 서비스로, 사고 처리, 침투 테스트, 보안 감사, 기술지원 관련 컨설팅 등을 포함함

- (보안 요건) 서비스 제공 인력은 해당 분야의 충분한 기술 지식, 역량, 경험을 갖추고 최고 수준의 직업적 청렴성을 유지해야 하며, 서비스는 지속적인 품질 보장을 위한 적절한 내부 절차를 구비해야 함

○ **(인증체계 평가)** 사이버보안 인증체계의 정기적 평가 및 검토

- (평가주기) 채택된 유럽 사이버보안 인증체계의 효율성과 활용도를 정기적으로 평가하며, 첫 평가는 2023년 12월 31일까지, 이후 최소 2년마다 실시

- (평가내용) 특정 인증체계의 의무화 필요성 평가 및 대상 ICT 제품, 서비스, 프로세스, 관리형보안서비스 식별

○ **(보증 수준)** 위험도에 따른 3단계 보증 수준 적용

- (기본 수준) 기본적인 사이버보안 위험을 최소화하기 위한 평가를 실시하는데, 평가 활동은 최소한 기술문서 검토를 포함해야 하며, 이러한 검토가 적절하지 않은 경우 동등한 효과를 가진 대체 평가 활동을 수행함

- (중급수준) 제한된 기술과 자원을 가진 행위자에 의한 사이버공격의 위험을 최소화하기 위한 평가를 실시하고, 공개적으로 알려진 취약점이 없음을 입증하기 위한 검토와 필요한 보안 기능이 올바르게 구현되었음을 입증하기 위한 테스트를 포함함

- (고급수준) 최첨단 사이버공격에 의한 위험을 최소화하기 위한 평가를 실시하고, 공개적으로 알려진 취약점 부재 검토, 최신 기술 수준의 필요 보안 기능 구현 검증, 침투 테스트를 통한 숙련된 공격자에 대한 저항성 평가를 포함함

○ **(평가체계)** 인증체계의 평가·모니터링 및 평가기관 요건 (제53조, 제54조, 부칙)

- (적합성 평가) 저위험 서비스에 한해 제조사나 제공자의 자체 적합성 평가를 허용하며, 이 경우 EU 적합성 선언문 발행과 요구사항 충족에 대한 책임을 짐

- (평가기관) 평가기관은 평가 대상으로부터 독립성을 유지해야 하며, 평가기관과 그 인력은 평가 대상의 설계, 제조, 공급, 설치, 구매, 소유, 사용, 유지보수와 관련된 활동 수행 불가, 평가기관과 시험소는 Regulation(EC) No 765/2008의 관련 harmonised standard 요구사항[13]을 충족해야 함

○ **(감독체계)** 인증요구사항 준수 여부에 대한 관리·감독 (제58조)

- (감독 활동) 국가 사이버보안 인증기관은 해당 영토 내에서 발행된 유럽 사이버보안 인증서의 규정 준수 여부를 감독하고 집행하며, 이는 관련 시장 감시 당국과의 협력을 통해 수행함

- (자체평가 감독) 자국 내 설립된 제조사나 제공자의 자체 적합성 평가 의무사항, 특히 EU 적합성 선언문 발행 관련 의무사항의 준수 여부를 모니터링하고 집행함

- (협력체계) 다른 국가 사이버보안 인증기관 및 공공기관과 협력하여 규정이나 특정 유럽 사이버보안 인증체계의 요구사항 미준수 가능성에 대한 정보를 공유함

■ 전망 및 시사점

○ EU의 「사이버 연대법」과 「사이버보안법」 개정은 사이버보안 위협에 대한 EU 차원의 공동 대응 능력을 강화하고, 회원국간 협력을 증진하는 계기가 될 것으로 전망됨

- 특히 사이버보안 경보체계는 국가간 정보공유를 통해 사이버 위협에 대한 선제적 대응을 가능하게 할 것으로 기대

○ 관리형보안서비스에 대한 인증체계 도입은 EU 역내 사이버보안 서비스의 품질을 제고하고 시장 단일화를 촉진할 것으로 예상되나, 중소기업의 인증 부담 등에 대한 고려가 필요함

○ 향후 EU는 동 법안을 통해 구축되는 체계를 바탕으로 회원국간 사이버보안 협력을 더욱 강화하고, 역내 사이버보안 서비스 시장의 경쟁력을 제고할 것으로 전망됨

13 EU의 제품 인증 및 시장 감시에 관한 규정으로, 평가기관이 따라야 하는 통일된 표준 요구사항을 규정

Reference

- https://www.consilium.europa.eu/en/press/press-releases/2024/12/02/cybersecurity-package-council-adopts-new-laws-to-strengthen-cybersecurity-capacities-in-the-eu/
- https://data.consilium.europa.eu/doc/document/PE-94-2024-INIT/en/pdf
- https://data.consilium.europa.eu/doc/document/PE-93-2024-INIT/en/pdf

유럽 각국

해외 단신

영국, 「제품보안 및 통신인프라(PSTI) 법 및 규정」 시행

○ **(개요)** 「2022 제품보안 및 통신인프라(PSTI) 법[1]」과 「2023 제품보안 및 통신인프라 규정[2]」이 시행될 예정('24.4.29)

- 「2022 PSTI 법」은 1부(제품보안)와 2부(통신인프라)로 구성되었으며, 「2023 PSTI 규정」은 제조업체를 위한 제품보안 요구사항 등을 규정함

○ **(연결가능제품)** 인터넷 연결가능제품 및 네트워크 연결가능제품을 의미하며, 이중규제를 피하기 위하여 국무장관이 규제범위에서 제외할 수 있는 예외제품을 규정함

○ **(대상자)** ①제조업체, ②수입업체, ③유통업체는 제품보안 관련 의무를 준수해야 함

- **(보안 요구사항 준수의무)** 대상자가 제품이 영국 소비자 연결가능제품이 될 것임을 알았거나 제품이 사용될 수 있도록 한 시점에 알았던 경우, 보안 요구사항 준수의무가 발생함

- **(제조업체를 위한 보안 요구사항)** ①범용 디폴트 비밀번호(Default Password) 금지, ②문제 보고를 위한 제조업체 연락처 정보게시, ③제품보안 업데이트 지원기간 공개를 준수하도록 의무화함

  ※ 연결가능제품의 ①하드웨어, ②제품이 사용될 수 있게 한 시점에 사전 설치된 소프트웨어, ③설치 가능한 소프트웨어에 보안 요구사항이 적용됨

- **(보안 요구사항 간주조건)** 유럽통신표준(ETSI EN 303 645)의 소비자 IoT를 위한 사이버보안 조항의 일부를 충족할 경우, 보안 요구사항을 준수한 것으로 간주함

○ **(집행)** 국무장관은 제품보안 관련 규정을 집행할 책임이 있음

  ※ 국무장관은 규정 미준수가 있다고 판단하는 경우, 대상자에게 리콜 통지나 1,000만 파운드 또는 연간 글로벌 매출의 4% 중 더 큰 금액을 과징금(Civil Penalty)으로 통지할 수 있음

Reference

■https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime

1 「Product Security and Telecommunications Infrastructrue Act 2022」('22. 12. 6.)
2 「The Product Security and Telecommunications Infrastructure(Security Requirements for Relevent Connectable Products) Regulations 2023」('23. 9. 14.)

해외 단신

영국, 「사이버보안 및 복원력 법안」 제정 추진 발표

○ **(개요)** 영국 정부는 「사이버보안 및 복원력 법안[1]」을 의회에 제출할 예정(2024. 7. 17.)

- 사이버 위협이 고도화됨에 따라, 영국 전역의 주요기반시설을 보호하고 디지털 서비스 보안을 개선하기 위하여 동 법안을 제안할 예정

※ 최근 영국 국민 보건 서비스(UK National Health Service)가 랜섬웨어 공격을 받아, 런던의 주요 병원에서 수천 건의 예약이 취소되고 운영이 중단[2]되는 사태 발생

○ **(주요내용)** 영국의 공공 및 민간 조직에 대한 사이버 위협을 완화하기 위하여, 주요기반시설을 보호하고 규제기관의 권한 등을 확대할 계획

- (주요기반시설 보호) 영국 「NIS 규정(NIS Regulations 2018)」의 적용대상을 확대하여, 디지털 서비스와 공급망 등 보다 광범위한 주요기반시설을 보호

※ 주요기반시설 운영자에게 취약점 평가 등 보다 엄격한 보안 요구사항을 적용

- (규제기관 권한확대) 규제기관이 잠재적인 사이버보안 취약점을 사전 조사할 수 있도록 추가 권한을 부여

- (공급망 사이버보안) 공급업체와 파트너가 일정 수준의 사이버보안 표준을 유지하도록, 관련 조직이 공급망 전반의 사이버보안을 모니터링

- (사이버사고 보고) 사이버 위협의 출처를 이해하기 위한 기반을 제공하고 잠재적 위협을 예측할 수 있도록, 주요기반시설 운영자의 사이버사고 보고의무를 강화

Reference

■ https://assets.publishing.service.gov.uk/media/6697f5c10808eaf43b50d18e/The_King_s_Speech_2024_background_briefing_notes.pdf

1 Cyber Security and Resilience Bill
2 2024. 6. 3. 러시아 사이버 범죄 그룹이 랜섬웨어 공격을 통해 NHS가 관리하는 환자 데이터(이름, 생년월일, NHS 번호, 혈액 검사 설명 등)를 훔치고 몸값으로 가상화폐를 요구 [출처] https://www.bbc.com/news/articles/c9777v4m8zdo 참고

해외 입법 동향

영국 상원, 「데이터 사용 및 액세스 법안」 발의

영국 상원은 데이터의 효과적 활용을 통해 경제성장을 도모하고 공공서비스를 개선하기 위하여, 「데이터 사용 및 액세스 법안(Data Use and Access Bill)」을 발의 (2024. 10. 23.)

■ 개요 및 추진배경

○ 동 법안은 영국 총리가 제시한 '영국 재건을 위한 5대 과제[1]' 중 3가지 과제(▲경제성장 촉진, ▲치안 확보, ▲영국 국민보건서비스(NHS)의 미래지향적 혁신) 달성을 위한 핵심 법안

○ 동 법안은 데이터 보안과 활용 간의 균형을 확보하고, 공익을 위한 안전하고 효과적인 데이터 활용을 보장하며, 불필요한 행정부담을 최소화하여 데이터 기반 혁신을 촉진하기 위함

〈 데이터 사용 및 액세스 법안 주요구성 〉

구분	주요내용
제1장 고객 및 비즈니스 데이터 액세스	· 고객 데이터 관련 규정 제정 권한(제2조), 비즈네스 데이터 관련 규정 제정 권한(제4조), 의사결정권자(제6조), 규정 시행(제8조), 금전적 패널티(제10조) 등
제2장 디지털 인증 서비스	· 디지털 인증 서비스(DVS) 신뢰 프레임워크(제28조), 디지털 인증 서비스 등록부(제32조) 등
제3장 국가 지하자산 등록부	· 국가 지하자산 등록부: 잉글랜드 및 웨일즈(제56조) 등
제4장 출생 및 사망 등록부	· 출생 및 사망기록이 보관되는 형식(제61조), 등록 요구사항(제63조) 등
제5장 데이터 보호 및 프라이버시	· 처리의 적법성(제70조), 목적 제한(제71조), 연구 등 목적으로 처리하는 경우의 안전장치(제85조) 등
제6장 정보위원회	· 정보 커미셔너 직책폐지(제116조), 정보위원회로의 기능 이관(제117조) 등
제7장 데이터 사용 및 액세스 관련 기타조항	· 영국 의료 및 사회복지 정보 표준(제119조), 스마트미터 통신 면허 부여(제120조), 공공 서비스 제공 개선을 위한 정보공개(제121조) 등
제8장 최종조항	· 결과적 수정권한(제133조), 규정(제134조), 범위(제135조), 시행(제136조) 등

1 영국의 스타머(Keir Starmer) 총리가 제시한 5가지 정책 과제로, ▲경제성장 촉진(Kickstarting economic growth), ▲에너지 강국 발전(Making Britain a clean energy superpower), ▲치안확보(Taking back our streets), ▲기회균등(Breaking down barriers to opportunity), ▲영국 국민보건서비스(NHS)의 미래지향적 혁신(Building an NHS fit for the future)이 있음

■ 주요내용

① **(비즈니스 및 고객 데이터 액세스)** 비즈니스 및 고객 데이터에 대한 접근성을 높이기 위하여 데이터 보유자의 의무와 권한, 데이터 공유의 기준과 절차를 규정

○ **(정의)** 주요 용어를 다음과 같이 정의함

구분	주요내용
비즈니스 데이터 (Business data)	• 거래자가 공급하거나 제공한 **상품, 서비스 및 디지털 콘텐츠**에 대한 정보 • 거래자의 상품, 서비스 및 디지털 콘텐츠의 **공급 또는 제공**과 관련된 정보 • 상품, 서비스 및 디지털 콘텐츠(또는 그 공급 또는 제공)에 대한 **피드백**과 관련된 정보 • 상기 세 가지 정보를 데이터 규정에 따라 **개인에게 제공하는 것**과 관련된 정보
고객 데이터 (Customer data)	• 거래자가 고객의 요청에 따라 **고객 또는 다른 사람에게** 제공한 정보 • 또는 제공하는 **상품, 서비스 및 디지털 콘텐츠**와 관련된 정보 • 상기 정보 또는 고객 관련 기타 정보를 데이터 규정에 따라 **개인에게 제공하는 것**과 관련된 정보
데이터 보유자 (Data holder)	• 비즈니스 및 고객 데이터와 관련하여, 거래자(trader) 또는 비즈니스 과정에서 데이터를 처리하는 자
데이터 규정 (Data regulations)	• 제2조(고객 데이터를 제공할 수 있는 권한) 및 제4조(비즈니스 데이터를 제공할 수 있는 권한)
거래자 (Trader)	• 개인적으로 또는 대리인을 통해 비즈니스 과정에서 상품, 서비스 또는 디지털 콘텐츠를 제공하는 사람

○ **(데이터 액세스 관련 규정 제정권한)** 국무장관(The Secretary of State) 또는 재무부장관(the Treasury)은 데이터 보유자가 고객 등에게 비즈니스 데이터 및 고객 데이터를 제공하도록 하는 규정을 마련할 수 있음

구분	주요내용
비즈니스 데이터 액세스	• **국무장관 또는 재무부장관은 데이터 보유자가** ▲비즈니스 데이터를 **공개**하거나 ▲비즈니스 데이터와 관련된 거래자의 **고객 등에게 제공하도록** 하는 **규정을 마련**할 수 있으며, 다음 조항이 포함될 수 있음
	- 고객, 제3자 수신자 또는 다른 사람의 요청에 대한 조항
	- 데이터 보유자가 요청에 대한 조치를 거부할 수 있거나 거부해야 하는 상황에 대한 조항
	- 비즈니스 데이터를 수신할 수 있는 사람을 특정 요구사항을 준수한 사람으로 제한하는 조항
	- 개인이 상기 권한과 관련된 요구사항을 충족하는지 여부를 판단할 의사결정자와 관련된 조항
고객 데이터 액세스	• **국무장관 또는 재무부장관은 데이터 보유자가** 고객 데이터를 ▲**고객** 또는 ▲고객이 데이터를 수신하도록 **승인한 특정인에게** 제공하도록 하는 **규정을 마련**할 수 있으며, 다음 조항이 포함될 수 있음
	- 고객이 개인에게 고객 데이터를 수신하거나 기타 작업을 수행할 수 있는 권한을 부여하는 절차에 대한 조항
	- 특정 요구사항을 준수하는 사람에게만 상기 권한을 부여할 수 있도록 제한하는 조항
	- 개인이 상기 권한과 관련된 요구사항을 충족하는지 여부를 판단할 의사결정자와 관련된 조항

② **(디지털 인증(Verification) 서비스 체계)** 인터넷 기반 인증 서비스의 신뢰성과 안전성을 확보하기 위한 제도적 기반을 구축하고, 서비스 제공자에 대한 등록 · 감독 체계를 확립

○ **(디지털 인증 서비스(Digital Verification Services, DVS))** 국무장관은 DVS 제공에 관한 기본규정을 명시한 문서인 'DVS 신뢰 프레임워크'를 수립하고, 이를 보충하는 규정(supplementary code)을 제정한 후 최소 12개월마다 기본규정과 보충규정을 검토·개정해야 함

○ **(DVS 등록부)** 국무장관은 적합성 평가기관의 인증을 받은 서비스 제공자를 등록 · 관리하고 국가 안보나 프레임워크 미준수 등의 사유가 있는 경우 등록을 거부하거나 취소할 수 있음

○ **(신뢰마크)** 국무장관은 디지털 인증 서비스용 신뢰마크를 지정하여, 등록된 서비스 제공자만이 신뢰마크를 사용할 수 있도록 하고 위반 시 민사상 금지명령(Civil injunction) 처분가능

③ **(데이터 보호 및 프라이버시)** 디지털 시대의 개인정보보호를 강화하면서도, 연구 · 법집행 · 공익 목적의 정당한 데이터 활용을 보장하기 위한 세부 규칙과 보호장치를 제시

○ **(개인정보처리 목적제한 원칙 변경)** 수집 목적 외 처리를 원칙적으로 금지하고 이러한 목적과 양립할 수 없는 방식으로 처리될 수 없다고 규정한 「영국 일반 데이터 보호규정(UK GDPR)」의 제5조(개인정보처리에 관한 원칙)를 개정하여, 양립가능한 추가처리 조건을 명시

- ▲과학적 또는 역사적 연구, ▲공익을 위한 보관, ▲통계 목적으로만 사용되고 이러한 데이터 처리에 관하여 정보주체의 새로운 동의를 받은 경우, 원래 목적과 호환되는 방식으로 처리

○ **(연구, 보관 또는 통계 목적의 처리를 위한 안전장치)** 「UK GDPR」에 제8장의A(연구, 보관 또는 통계 목적의 처리를 위한 안전장치)를 신설하여, 정보주체의 신원을 확인할 수 없도록 가명처리 등 데이터보호 조치를 의무화하고 처리 목적과 무관한 조치를 금지

○ **(개인정보 유출사고 통지 등)** 「2003년 프라이버시 및 전자통신 규정(PECR)」을 개정하여, 개인정보 유출사고 발생 시 서비스 제공자가 사고를 인지한 후 72시간 이내에 정보위원회에 통지하도록 함

④ **(정보위원회(Information Commission))** 효과적인 데이터 보호감독을 위해 「2018년 데이터보호법」을 개정하여 기존의 커미셔너(Commissioner) 체제를 정보위원회로 전환

○ **(정보위원회 신설)** 기존 커미셔너 체제의 모든 권한과 기능이 신설된 정보위원회로 이전되며, 정보위원회는 확대된 권한을 바탕으로 독립적인 감독기구로서의 역할을 수행

- (구성) 의장은 임기는 최대 7년으로 연임할 수 있고 3~14명의 상임 및 비상임위원으로 구성되며, 국무장관은 비상임위원이 상임위원보다 많도록 보장해야 함

※ 법안이 제정될 경우, 현 정보 커미셔너가 임기가 만료될 때까지 정보위원회의 첫 번째 의장으로 추대되어 국무장관이 임명하고, 비상임위원은 의장과의 협의를 거쳐 국무장관이 임명

- 국무장관은 재산, 권리, 의무의 포괄적 승계를 위한 계획을 수립할 수 있고, 동 계획에는 다음 사항이 포함될 수 있음

정보위원회 포괄적 승계 계획 주요내용
• 기존의 정보 커미셔너 체제에서 수행한 작업의 효과를 보장하기 위한 조항 마련 • 기존의 정보 커미셔너 체제에 의해 수행된 작업(법적 절차를 포함)의 연속성을 보장하기 위한 조항 마련 • 모든 문서에서 정보 커미셔너에 대한 언급이 정보위원회로 취급되도록 보장하는 조항 마련 • 사업양도(고용보호) 규정(S.I. 2006/246)과 동일하거나 유사한 조항 마련 • 기타 결과적, 보충적, 부수적 또는 과도기적 조항 마련

⑤ **(데이터 사용 또는 액세스에 관한 기타 규정)** 영국의 의료·사회 복지, 스마트 미터링, 공공서비스 등 다양한 분야에서의 데이터 활용을 촉진하고 규제하기 위한 세부 규정을 제시

○ **(보건 및 성인 사회복지 정보표준)** 「보건 · 사회복지법(Health and Social Care Act)」 제9장에 따라 정보표준을 수립하여, 의료서비스 제공자들이 일관된 방식으로 정보를 수집 · 저장 · 공유하도록 함

○ **(스마트미터 통신서비스 면허)** 스마트미터 통신 서비스 제공을 위한 면허 발급 체계를 구축하고, 에너지 소비 데이터의 수집 · 전송 · 활용에 관한 표준을 수립하여 효율적 에너지관리 시스템을 구현

○ **(공공서비스 개선을 위한 정보공개)** 「디지털경제법」(Digital Economy Act) 제35조(공공서비스 전달 개선을 위한 정보공개)를 개정하여 기업 대상 공공서비스 개선을 위한 정보공개 범위를 확대

⑥ **(최종규정)** 동 법 시행과 관련된 최종적인 행정적 · 절차적 사항들을 규정하며, 법안의 효과적인 이행을 위한 세부 권한과 지역별 적용 범위를 명확히 함

○ **(결과적 개정권한)** 국무장관은 법 시행에 따른 결과적 개정(Consequential Amendments)이 필요한 사항(법령의 개정 · 폐지 · 수정 및 과도기적 조치나 경과규정 포함)에 대하여 제정권한을 부여받음

- 국무장관이 규정을 제정할 시, 주요사항(Primary legislation)에 대한 개정은 의회의 승인이 필요한 적극적 절차(Affirmative procedure)[2]를 따름

○ **(시행)** ▲규정 제정권한 등 행정적 준비가 필요한 조항은 동 법이 시행되는 날부터 즉시 시행되고, ▲국무장관이 제정한 규정은 장관이 지정하는 날부터 시행됨

2 적극적 절차(affirmative procedure)는 초안형태로 의회에 제출된 위임 법안이 발효(법률)되기 전에 의회의 승인을 거쳐야 하는 절차

■ 전망 및 시사점

○ 동 법안은 데이터 경제 활성화와 공공서비스 혁신을 동시에 추구하는 포괄적 접근방식을 채택하고 있어, 향후 영국의 디지털 전환을 가속화할 것으로 전망

○ 영국 국민보건서비스(NHS)와 경찰업무 효율화를 통해 공공서비스의 질적 향상이 기대되고, 이는 타 국가의 공공부문 디지털화에도 영향을 미칠 것으로 예상

Reference

▪https://bills.parliament.uk/bills/3825

▪https://www.gov.uk/government/news/new-data-laws-unveiled-to-improve-public-services-and-boost-uk-economy-by-10-billion

▪https://bills.parliament.uk/publications/56527/documents/5211

해외 입법 동향

독일 연방 내무부, 「NIS2 지침 이행법(안)」 공식 초안 발표

독일 연방 내무부(BMI)[1]는 「EU 사이버보안 지침(이하 NIS2 지침)」에 따라 기존 사이버보안 요건을 강화하고 보안사고 통지 요건을 확대하는 「NIS2 지침의 이행 및 연방 행정부의 정보보안 관리의 필수 원칙 규제에 관한 법률안(이하 NIS2 지침 이행법(안))[2]」 공식 초안을 발표 (2024. 5. 7.)

■ 개요

○ 독일 연방 내무부(BMI)는 「NIS2 지침」[3]의 국내법 적용을 위해 2024년 5월 발의한 「NIS2 지침 이행법(안)」의 공식 초안[4]을 공개

- 「NIS2 지침 이행법(안)」은 「연방정보기술보안청법(BISG)」, 「전기통신법」, 「전자정부법」, 「원자력법」, 「에너지산업법」, 「IT 보안법 2.0」, 「사회법」, 「에너지 안보법」 등을 개정함

  · 특히, 현행 「IT 보안법 2.0」를 개정하여 적용대상에 디지털서비스제공업체, 전기통신사업자, 의료서비스 및 제약업체 등을 포함함으로써 「NIS2 지침」의 범위를 확대

- 「NIS2 지침」의 '필수조직'과 '중요조직'은 「NIS2 지침 이행법(안)」에서 '특별히 중요한 조직'과 '중요조직'으로 구분되어 적용

- 독일의 주요기반시설을 일컫는 KRITIS[5]의 적용범위는 「NIS2 지침 이행법(안)」에서도 동일하며, 이때 KRITIS 운영자는 '특별히 중요한 조직' 사업자로 분류

- 적용 기업들은 독일 연방정보기술보안청(BSI)[6]의 감독을 받게 될 전망

1 Bundesministerium des Innern und für Heimat
2 Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS2UmsuCG)
3 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)
4 동 법안의 비공식 초안은 2023년 4월부터 공개
5 「연방정보기술보안청법(BSI-Gesetz)」에 따른 「연방정보기술보안청 주요기반시설 규정(BSI Kritis Regulation)」에 의하여, KRITIS의 부문, 주요 서비스, 임계값(threshold) 등을 명확히 규정함
6 Bundesamt für Sicherheit in der Informationstechnik

■ 주요내용

① 적용 범위 및 대상

○동 법안의 적용대상인 기업의 유형은 크게 ▲특별히 중요한 조직(Besonders wichtigen)(제28조제1항) ▲중요조직(Wichtige Einrichtungen)(제28조제2항) ▲주요기반시설 운영자(기존 KRITIS 운영자)(제28조제6항)로 분류

- **(특별히 중요한 조직 / 중요조직)** NIS 2 지침 부속서(Annex) I, II에서 열거한 부문(sector)에 해당하는 대기업, 중견기업 및 규모와 무관하게 적용되는 일부 기업 등을 포함하며, 직원수(FTE), 연간 매출액 및 자산 총액 규모 등을 기준으로 구분

※ 동 법안에서의 KRITIS 운영자는 '주요기반시설 운영자'로서, ▲에너지, ▲운송, ▲금융/보험, ▲건강, ▲식수, ▲식품, ▲IT 및 통신, ▲우주, ▲지자체 폐기물 등을 포함 (제28조제7항)하며, '특별히 중요한 조직'으로 분류

〈「NIS2 지침 이행법(안)」 의무 적용대상〉

구분	부문(Sector)	기업 규모
특별히 중요한 조직	· 에너지, 운송 및 교통, 금융 및 보험, 의료, 식수, 폐수, 정보 기술 및 통신, ICT 서비스 관리, 우주	· 대기업(「NIS 2 지침」 부속서 I) – 250 FTE 이상, 또는 – 연간 매출액(revenue) 5,000만 유로 초과 및 자산 총액(balance) 4,300만 유로 초과
	· 공용 통신 네트워크 및 통신 서비스 제공업체	· 중견기업
	· QTSP(Qualified trust services), TLD(Top-Level Domain) 레지스트리, DNS(Domain Name System) 서비스	· 기업 규모 무관한 특수 사례
	· 주요기반시설 운영자(KRITIS 운영자) – 임계값을 초과하는 주요기반시설로서, 일반적으로 공급 인원이 50만 명 이상인 경우	
중요조직	· 우편/택배, 도시 폐기물, 화학, 식품, 제조, 디지털 서비스, 리서치	· 대기업(「NIS 2 지침」 부속서 II)
	· 에너지, 운송 및 교통, 금융 및 보험, 의료, 식수, 폐수, 정보 기술 및 통신, ICT 서비스 관리, 우주	· 중견기업(「NIS 2 지침」 부속서 I) – 50 FTE 이상, 또는 – 연간 매출액 1,000만 유로 초과 및 자산 총액 1,000만 유로 초과
	· 신탁 서비스 제공자	· 기업 규모 무관한 특수 사례

② 보안 및 위험관리 의무사항

○특별히 중요한 조직/중요조직은 사이버 침해를 방지하고 서비스 제공에 영향을 미치는 사고 피해를 최소화하기 위해 적절하고 비례적이며 효과적인 기술적·조직적 조치를 취해야 함 (제30조제1항)

- 위험 노출도, 규모, 보안 사고 발생 가능성 및 심각성, 사회 및 경제적 영향 등을 고려해야 하며, 위험관리 조치의무 준수 사항은 문서화할 의무가 있음

○ **(보안 조치)** 기술적·조직적 위험관리 조치는 유럽 및 국제표준과 이행비용을 고려하여 최신 기술 준수 및 기존 위험에 적합한 정보 기술 시스템, 구성요소, 프로세스의 보안 수준을 보장하는 한편, 다음의 사항을 다루어야 함 (제30조제2항)

〈보안 조치 고려 사항〉
· 정보 시스템의 위험분석 및 보안과 관련한 개념
· 사고 대응 및 관리
· 유지보수 및 복구, 백업관리, 위기관리
· 공급망 보안, 기업 간 보안, 서비스 제공업체 보안
· 개발, 조달, 유지보수 보안
· 정보 시스템, 구성요소 및 프로세스 획득·개발·유지·보수를 위한 보안조치(취약점 관리 및 공개 포함)
· 사이버보안 및 위험관리 효과성 평가
· 기본적인 사이버보안 위생(cyber hygiene) 절차 및 사이버보안 교육
· 암호화(cryptography 및 encryption)
· 인력 보안, 액세스 제어 및 시설 관리
· 다단계 인증(MFA) 및 지속적 인증(continuous authentication)에 대한 개념과 절차
· 안전한 비상통신
· 안전한 커뮤니케이션 방식(음성, 영상 및 문자)

○ **(주요기반시설 운영자)** 주요기반시설(KRITIS) 운영자의 경우, 제30조에서 규정한 보안 조치 및 적정성 평가와 관련하여 보다 높은 기준과 추가 요건을 비례적으로 적용해야 함 (제31조)

- 주요기반시설 운영자는 공격 탐지 시스템(OH SzA)을 사용해야 하며, 해당 시스템은 적절한 매개변수와 특성을 지속적·자동적으로 기록하고 분석할 수 있어야 함

- 또한, 주요기반시설 운영자는 지속적으로 위협을 식별·예방해야 하며, 발생한 결함에 대해 적절한 수정 조치 제공 의무가 있음

③ 보안사고 발생 시 보고·정보제공·고지의무

○ **(감독기관에 대한 보고의무)** 특별히 중요한 조직/중요조직은 보안사고 발생 시 24시간 내 연방정보기술보안청(BSI)에 통지*해야하며, 점진적(incrementally)으로 업데이트 한 후속 보고를 해야 함 (제32조제1항)

최초 보고 (제32조제1항제1호)	**후속 보고** (제32조제1항제2호)	**중간 보고** (제32조제1항제3호)	**최종 보고** (제32조제1항제4호)
· 중대한 보안사고(significant security incident)에 대한 초기 보고서는 **보안 사고를 인지한 즉시, 늦어도 24시간 이내에 제출해야 함**	· 최초보고에 대한 후속보고는 사고 심각도, 영향 및 피해에 대한 평가를 포함해야 하며, **보안 사고 인지 시점으로부터 72시간 이내에 제출**	· **BSI의 요청이 있을 경우**, 진행 현황을 최신화한 중간 보고서를 제출해야 함	· 최종 보고서 또는 진행 상황 보고는 **제32조제1항제2호에 언급된 후속보고를 제출한 후 1개월 이내**에 이뤄져야 함 – 해당 보안사고에 대한 자세한 설명(심각도, 영향 포함), 원인, 조직이 취했거나 진행 중인 시정 조치, (해당할 경우) 해외에 미친 영향 등을 포함해야 함

○ **(주요기반시설 운영자의 정보제공 의무)** 주요기반시설 운영자는 중대한 보안사고가 주요기반시설에 영향을 미쳤거나 미칠 가능성이 있는 경우, ▲영향을 입은 시설 및 주요 서비스(critical service)의 유형, ▲보안 사고가 해당 서비스에 미치는 영향에 대한 정보를 제공해야 함 (제32조제3항)

○ **(서비스 수신자 고지의무)** 연방정보기술보안청(BSI)은 중대한 보안사고 발생 시, 특별히 중요한 조직/중요조직이 고객('서비스 수신자')에게 해당 사실을 알리도록 지시할 수 있음 (제35조제1항)

- ▲금융 및 보험 ▲정보기술 및 통신 ▲ICT 서비스 ▲디지털 서비스 부문에 종사하는 조직은 중대한 사이버 위협(significant cyber threat)에 따라 잠재적 영향을 받을 가능성 있는 서비스 수신자에게 해당 사실을 즉시 통지해야 하며, 이때 서비스 수신자가 취할 수 있는 조치를 함께 안내해야 함 (제35조제2항)

- 연방정보기술보안청(BSI)이 중대한 보안 사고의 예방 또는 대처를 위해 ▲대중의 인식을 제고할 필요가 있거나 ▲공익을 위해 필요하다 판단할 경우, 연방정보기술보안청(BSI)는 중대한 보안 사고를 대중에게 직접 알리거나 조직에 이를 요청할 수 있음 (제36조제2항)

④ 연방행정기관의 정보보안 관련 의무사항

○ **(정보보안 관리)** 시설 경영진(facility management)은 IT 운영의 요구사항을 고려하여 정보보안 보장 여건을 조성해야 하며, 정기 교육과정 참여를 통해 정보보안 분야의 위험 및 관리 관행과 시설에서 제공하는 서비스에 대한 영향을 식별·평가할 수 있는 충분한 지식 및 기술을 습득해야 함 (제43조제1항, 제2항)

- 민간 기관이 연방 정보기술에 대한 서비스 제공을 위탁받는 경우, 계약상으로 정보보안 요건 준수사항을 보장해야 함 (제43조제3항)

- 연방행정기관이 동 법안 제32조에서 규정한 통지의무 외에 업무 수행 또는 연방 통신기술의 보안에 중요한 정보를 인지하게 된 경우, 다른 기관이 관여하지 않는 한, 즉시 이를 연방사무국(Federal Office)에 통지해야 함 (제43조제5항)

○ **(주요 디지털화 프로젝트 및 연방정부 통신 인프라)** 주요 디지털화 프로젝트 및 연방 통신 인프라의 계획과 실행을 위해서는 동 법안 제45조(연방행정기관의 정보보안책임자)에 따라 별도의 정보보안책임자를 임명해야 함 (제47조)

- 특히 연방 디지털화 프로젝트 또는 통신 인프라는 연방 통신 기술이 여러 부서에 걸쳐 운영되거나 부서 간 통신 또는 부서 간 데이터 교환에 사용되는 경우 필수적인 것으로 간주

- 합리적인 기간 내에 부서 간 디지털화 프로젝트 또는 통신 인프라와 관련해 여러 참여 부처 및 기타 연방 최고 기관의 기관 지정에 대한 합의에 도달할 수 없는 경우, 정보보안 코디네이터는 어느 기관이 지정할 것인지 결정해야 함

■ 전망 및 시사점

○ 2024년 5월 공개된 초안에 의하면, 「NIS 2 지침 이행법(안)」은 2024년 10월 시행될 전망이며, 각 조직에 대한 의무 적용은 별도 전환기간(transition period)을 거치지 않고 바로 진행될 예정

○ 「NIS 2 지침 이행법(안)」이 법률로 제정될 경우, 독일의 약 30,000개 기업(특별히 중요한 조직 8,250개(이 중, 주요기반시설 운영자 5,000개), 중요조직 21,600개)이 영향을 받을 것으로 추정

- 다만 이 중 현재 17%만이 법률을 준수하기 위한 충분한 조치를 취하고 있는 것으로 파악됨에 따라, 기존 사업자를 제외하면 20,000개 이상의 기업들이 동 법안을 준수하기 위한 조치를 취해야 할 것으로 전망

- 새로운 사이버 보안 요건과 프로세스 적응을 위해 필요한 기업 비용은 ▲일회성 비용 약 21억 유로 ▲연간 비용 21억 유로 정도가 요구될 것으로 예상

○ 한편, 독일은 「NIS 2 지침 이행법(안)」과 별개로 주요기반시설의 복원력 및 물리적 보안을 포괄적으로 규제하기 위한 「KRITIS 포괄법KRITIS-Dachgesetz)」 제정을 추진 중

Reference

▪https://www.bvmw.de/de/recht/gesetze-unter-der-lupe/nis-2-umsetzungs-und-cybersicherheitsstaerkungsgesetz-nis2umsucg
▪https://www.dataguidance.com/news/germany-bsi-publishes-draft-law-implementing-nis-2
▪https://www.nis-2-directive.com/
▪https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html
▪https://www.taylorwessing.com/en/insights-and-events/insights/2023/08/nis-2-umsetzungs--und-cybersicherheitsstaerkungsgesetz
▪https://www.twobirds.com/en/insights/2023/germany/nis2-directive-first-insights-into-germanys-implementation-of-the-eu-cybersecurity-act

해외 입법 동향

독일 연방의회, 딥페이크 처벌을 위한 「형법」 개정안 발의

독일 연방의회는 디지털 위변조를 통한 인격권(Persönlichkeitsrecht) 침해와 관련하여, 딥페이크 처벌을 규정하는 새로운 「형법」 개정안[1]을 발의 (2024. 7. 5.)

■ 개요 및 추진배경

○ 연방의회는 AI로 생성되는 사실적인 미디어 콘텐츠로부터 인격권(Persönlichkeitsrecht)을 보호하기 위하여, 「형법(Strafgesetzbuch, 일명 StGB)」 제201b항을 신설하여 딥페이크 관련 범죄를 규제

○ **(배경)** AI를 통해 생성되거나 변형되어 사실적으로 보이는 미디어 콘텐츠(소위 '딥페이크')가 수년 동안 증가 추세에 있고, 딥페이크와 관련된 기술 조작은 개인의 재산과 인격권은 물론 민주적 의사결정 과정에 심각한 위험을 초래

- 딥페이크는 인공지능 시대의 역동적인 기술 발전, 높은 수준의 현실성 등으로 인해 국가와 시민을 위협하는 정보조작의 한 형태로 자리잡음

- 허위 정보 유포와 불법 이득을 목적으로 하는 딥페이크 사용 범죄가 증가하고, 딥페이크는 인격권 보호에 위협이 되는 실정

딥페이크 악용 사례
• 얼굴이나 기타 신체 부위를 교체하고 몸짓, 표정 및 목소리를 모방하는 이미지 및 동영상 조작을 통해, 여성이 원치 않는 성적 맥락에 놓이는 경우(소위 딥누드)[2]
• 정치적 경쟁 관계에서 상대방의 신용을 악의적으로 깎아내리고 부정적인 여론을 형성하기 위해 딥페이크를 사용
• AI가 생성한 가족의 목소리를 범죄에 활용하는 쇼크콜(Schockanrufe)[3]

1 Entwurf eines Gesetzes zum strafrechtlichen Schutz von Persönlichkeitsrechten vor Deepfakes
2 딥누드(Deepnude)는 악의적인 딥페이크가 가장 일반적으로 적용되는 분야로 인터넷에 배포되는 딥페이크의 90%는 음란물에 해당. [출처] https://posteo.de/news/bundesrat-fordert-strafen-f%C3%BCr-b%C3%B6sartige-deepfakes
3 '충격 전화' 또는 '공포 전화'라는 의미로, 주로 사기꾼들이 피해자에게 극도의 스트레스나 공포를 유발하는 거짓 정보를 전달하는 전화

- 현행 「형법」 상 딥페이크 관련 범죄는 ‘사진 촬영을 통한 사생활과 인격권 침해’ 조항[4](제201a조)을 적용하여 처벌하고 있음

  · 그러나 해당 조항은 딥페이크 관련 범죄의 본질적 특성을 포괄하지 못하고 있어, 딥페이크 범죄를 특정하여 처벌할 수 있는 새 법률의 필요성이 대두

○ **(목적)** 딥페이크와 같은 기술적 정보조작으로부터 인격권을 보호하기 위한 법적 근거 마련

- 타인의 외모, 행동 또는 언어 표현을 사실적인 영상이나 녹음처럼 보이게 하는 컴퓨터 기술을 사용하여, 생성 또는 변형된 미디어 콘텐츠를 제3자에게 제공하는 자는 디지털 위변조에 의한 인격권 침해 혐의로 처벌

■ 주요내용

▲컴퓨터 기술을 이용해 조작된 미디어 콘텐츠(소위 ‘딥페이크’)를 제3자에게 제공함으로써 타인의 인격권을 침해한 경우, 최대 2년의 징역 또는 벌금형에 처하고 ▲이러한 조작 콘텐츠를 대중적으로 공개하는 경우, 최대 5년의 징역 또는 벌금형에 처하도록 하는 조항을 기존 「형법」에 추가

○ **(디지털 위변조를 통한 인격권 침해)** 디지털 기술 발전에 따른 인격권 침해 문제에 대응하기 위한 법적 장치 마련 (제201b조 신설)

- 컴퓨터 기술을 이용해 타인의 외모, 행동, 또는 언어 표현을 사실적으로 보이게 만든 미디어 콘텐츠를 제3자에게 제공하여 타인(사망한 사람 포함)의 인격권을 침해하는 행위를 금지하고, 이러한 행위를 한 자는 2년 이하의 징역이나 벌금형에 처해질 수 있음 (제1항)

- 이러한 위변조된 미디어 콘텐츠를 대중에게 공개하거나, 특히 개인의 내밀한 사생활을 대상으로 한 콘텐츠를 공개하는 경우에는 그 처벌이 더욱 엄중해져 5년 이하의 징역 또는 벌금형에 처해질 수 있음 (제2항)

- 다만, 이 법은 표현의 자유와 공익을 고려한 예외 조항을 두어 예술, 과학, 연구, 교육, 시사 보도, 역사적 사건에 대한 보도 등 정당한 이익을 위한 행위에는 적용되지 않음 (제3항)

- 추가적인 범죄 예방과 증거 보전을 위한 조치로 범죄에 사용된 영상촬영, 녹음기기, 기타 기술적 수단은 몰수(eingezogen werden)할 수 있음 (제4항)

4 § 201a Verletzung des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten durch Bildaufnahmen

■ 전망 및 시사점

○ 동 개정안은 딥페이크와 같은 첨단 기술을 이용한 범죄에 대한 법적 대응이 본격화됨을 의미하고, 향후 이와 관련된 판례가 축적되면서 법 적용의 구체성과 정확성이 높아질 것으로 예상

- 다만 동시에 인격권 보호와 표현의 자유 사이의 균형을 유지하는 것이 중요한 과제로 다뤄질 것이며, 이를 위해 사회적 논의와 합의 과정이 전개될 것으로 보임

Reference

▪Budesrat, Entwurf eines Gesetzes zum strafrechtlichen Schutz von Persönlichkeitsrechten vor Deepfakes

▪https://posteo.de/news/bundesrat-fordert-strafen-f%C3%BCr-b%C3%B6sartige-deepfakes

▪https://www.heise.de/news/Bis-zu-5-Jahre-Haft-Bundesrat-will-Deepfakes-eindeutig-strafbar-machen-9791798.html

해외 입법 동향

독일 연방금융감독청, 「디지털 운영 복원력법」에 관한 이행지침 발표

독일 연방금융감독청은 「디지털 운영 복원력법[1]」의 적용[2]에 대비해 금융사의 법률 준수를 지원하기 위한 이행지침[3]을 발표 (2024. 7. 8.)

■ 개요

○ 독일 연방금융감독청(Bundesanstalt fur Finanzdienstleistungsaufsicht, 이하 BaFin)은 「디지털 운영 복원력법」(Digital Operational Resilience Act, 이하 DORA)의 IT 관련 요건에 대한 금융사의 이해 증진을 위하여, 구속력 없는 이행지침을 발행

○ 동 이행지침은 '기존 금융부문에 대한 IT 감독요건 체제'(은행(BAIT[4])·보험사(VAIT[5])·자본관리자(KAIT[6])·전자화폐기관(ZAIT[7]))와 비교한 「DORA」의 주요 특징을 설명

- ▲거버넌스 및 조직 ▲정보위험 및 정보보안 관리 ▲IT 운영 ▲ICT 사업 연속성 관리 ▲IT 프로젝트 관리 및 애플리케이션 개발 ▲ICT 제3자 위험관리 ▲운영 정보보안 ▲신원 및 권한 관리 등 8가지 항목별로 금융사가 수행해야 할 사항을 나열

○ 「DORA」는 전반적으로 '기존 금융부문에 대한 IT 감독요건'의 주요내용을 포함하고 있지만, 디지털 복원력에 중점을 두고 있어 기존 IT 감독요건보다 포괄적인 요구사항을 규정

■ 주요내용 (※ '기존 금융부문에 대한 IT 감독요건'과 비교한 「DORA」의 특징을 규제 수준별로 재구성)

○ 「DORA」는 ▲거버넌스 및 조직, ▲정보 위험 및 정보보안 관리, ▲ICT 사업 연속성 관리 사항에서 '기존 금융부문에 대한 IT 감독요건'과 비교하여 보다 **포괄적인 요구사항**을 규정

1 REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011
2 디지털 운영 복원력법은 2023년 1월 16일 발효되었고, 2025년 1월 17일부터 적용될 예정
3 Hinweise zur Umsetzung von DORA im IKT-Risikomanagement und IKT-Drittparteienrisikomanagement
4 IT 관련 은행 감독요건, Bankaufsichtlichen Anforderungen an die IT
5 IT 관련 보험사 감독요건, Versicherungsaufsichtlichen Anforderungen an die IT
6 IT 관련 자본관리자 감독요건, Kapitalaufsichtlichen Anforderungen an die IT
7 IT 관련 전자화폐기관 감독요건, Zahlungsdiensteaufsichtlichen Anforderungen an die IT von Zahlungs- und E-Geld-Instituten

구분	주요내용
거버넌스 및 조직	• 「DORA」는 **내부 ICT 거버넌스 및 복원력 강화** 등에 초점을 맞춤
	- **(거버넌스)** 금융사는 전반적인 위험관리의 일부로서 ICT 위험관리 프레임워크를 갖추어야 하며, ▲위험관리 기능, ▲통제 기능, ▲내부감사 기능 등 다양한 기능이 적절하게 분리되어 독립성을 갖춰야 함
	- **(조직)** 금융사 경영기구(Management Body)의 구성원은 관리해야 할 ICT 위험에 대한 충분한 지식과 기술을 보유하고 있어야 하며, 이를 최신 상태로 유지해야 함
정보위험 및 정보보안 관리	• '기존 금융부문에 대한 IT 감독요건'은 정보보안 조치를 우선시했으나, 「DORA」는 **ICT 위험관리**에 보다 중점을 둠
	- **(ICT 통제기능)** '기존 금융부문에 대한 IT 관련 감독요건'의 정보보안 책임자와 동등한 수준의 ICT 통제 기능을 요구하지만, 「DORA」는 정보보안과 관련한 모든 책임을 맡기지 않고, 'ICT 위험관리 및 모니터링 책임'만을 부과
	- **(감사 및 보고)** 「DORA」는 금융사로 하여금 기존 ICT 시스템, 사고 등에 대한 광범위한 감사와 분석을 하도록 규정하고, ICT 부서의 고위직원이 매년 자사 경영기구에 사이버 공격 및 사고 등을 보고하도록 의무화
	- **(교육)** 금융사는 직원과 경영진을 위한 ICT 보안인식 프로그램과 디지털 운영 복원력 교육을 개발하는 등 직원과 고위 관리자의 교육 의무를 수행해야 함
ICT 사업 연속성 관리	• 「DORA」는 '기존 금융부문에 대한 IT 관련 감독요건'에서 구체적으로 다루지 않았던 **ICT 사업 연속성 관리**에 대하여 **포괄적인 요건**을 설정
	- **(정책 문서화)** 금융사는 ▲ICT 관련 사고에 대한 신속하고 적절한 대응, 피해 최소화, 활동 재개 및 복구 조치, ▲ICT 관련 사고 발생 시 격리 조치, 과정 및 기술 구현 및 추가 피해 방지계획 활성화, ▲영향, 피해, 손실 추산 등 ICT 사업 연속성을 위한 일련의 문서화된 준비, 계획, 절차, 메커니즘 등을 구현해야 함
	- **(복구 계획 시 신규 고려사항)** 금융사는 ICT 대응 및 복구계획을 준비할 때, 「DORA」에 규정된 의무 검토사항과 별도로 ▲기후변화 및 관련 환경 악화, 자연재해, 전염병, ▲강도 및 테러 공격을 포함한 물리적 공격, ▲내부자 공격, 국가의 정치적 및 사회적 불안정, ▲대규모 정전 등 보다 광범위한 사항을 고려하는 것이 필요
	- **(정기 검토)** 금융사는 최소 1년에 한 번 ICT 사업 연속성 계획을 정기적으로 검토해야 함

○ 「DORA」는 ▲IT 프로젝트 관리 및 애플리케이션 개발, ▲신원 및 권한 관리 사항에서 '기존 금융부문에 대한 IT 감독요건'과 **유사한 수준의 요구사항**을 규정

구분	주요내용
IT 프로젝트 관리	• 금융사의 IT 프로젝트 관리 및 애플리케이션 개발과 관련하여, **'ICT 위험관리 프레임워크에 대한 규제기술 표준**[8](Regulatory Technical Standard, 이하 RTS)'에서 상세히 설명
	- **(IT 프로젝트 관리)** 금융사는 '기존 금융부문에 대한 IT 관련 감독요건'과 유사하게 IT 프로젝트 관리를 수행하되, ICT 프로젝트 위험평가에 따라 금융사의 중요·핵심 기능에 영향을 미치는 프로젝트의 수립 및 진행과 관련된 위험을 자사 경영기구에 보고해야 함
	- **(애플리케이션 개발)** 금융사는 애플리케이션 개발과 관련해 '기존 금융부문에 대한 IT 관련 감독요건' 대비 ▲안전한 애플리케이션 구현 ▲구현에 필요한 요건 식별에 더욱 중점을 둬야 함

구분	주요내용
신원 및 권한관리	• 금융사는 '기존 금융부문에 대한 IT 관련 감독요건'과 유사한 수준의 신원 및 권한 관리를 「DORA」 체제에서 유지하는 것으로도 충분
	- **(권한 부여)** 금융사는 자사의 정보 자산 및 ICT 자산에 접근하는 각 직원(제3자 ICT 서비스 제공사 직원 포함)에게 고유 ID를 할당하고, 조직 개편 시 및 계약 관계가 만료된 후에도 유지하며, ID 및 계정에 대한 수명 주기 관리 프로세스를 도입하는 것이 이상적
	- **(재인증)** 금융사는 모든 ICT 시스템의 접근 권한에 대해 최소 연 1회, 중요·핵심 기능을 지원하는 ICT 시스템의 경우 **최소한 6개월에 한 번씩 접근권한을 업데이트**해야 함

○ 「DORA」는 ▲IT 운영, ▲ICT 제3자 위험관리, ▲운영 정보보안에서 '기존 금융부문에 대한 IT 감독요건'보다 **엄격한 수준의 요구사항**을 규정

구분	주요내용
IT 운영	• 「DORA」는 '기존 금융부문에 대한 IT 관련 감독요건'에 비해 엄격한 **운영 안전성 요구사항**을 규정
	- **(시스템 최신 유지 등)** 금융사는 ICT 시스템을 항상 최신 상태로 유지하도록 하고, 이때 최신 상태의 ICT 시스템은 ▲각 금융사의 업무 규모에 적합하고 ▲신뢰할 수 있으며 ▲업무 처리를 위한 여유 있는 용량을 갖추고 ▲기술적으로도 복원력이 뛰어나야 함
	- **(리소스 관리)** 금융사가 리소스 최적화 조치와 함께 리소스 병목 현상[9]이 발생하지 않도록 관리하고, 비즈니스 요구사항을 충족할 수 있는 적절한 자원, 용량, 기능 등을 갖추도록 규정
	- **(변경사항 관리)** 금융사는 ICT 시스템에 대한 모든 변경사항을 관리해야 하며, 그 과정에서 기록, 테스트, 평가, 승인, 구현 및 검토 활동 등이 수반될 수 있음
	- **(데이터 백업 및 복구)** 금융사는 데이터 백업 및 복구를 수행할 때 시스템 보안과 데이터 가용성, 신뢰성, 무결성, 기밀성이 위협받지 않도록 해야 하며, 데이터를 복원할 때는 기존 시스템과는 물리적 및 논리적으로 분리된 ICT 시스템을 사용해야 함
ICT 제3자 위험관리	• 「DORA」는 **제3자 서비스 제공사의 ICT 서비스 이용과 관련한 사항**을 구체적으로 규정
	- **(계약)** 금융사-ICT 제3자 서비스 제공사의 계약상의 권리와 의무는 명확하게 서면으로 명시되어야 하고, 여기에는 ▲문서의 형식 및 표현을 포함한 형식적 요건 ▲중요하거나 중요한 기능을 지원하기 위한 계약의 최소 내용 ▲하도급이 허용되는지 여부 및 허용되는 경우 하도급에 적용되는 요건 ▲해지권(Kündigungsrechte) 등이 포함되어야 함
	- **(하도급 규제)** 금융사는 중요·핵심 기능에 대한 ICT 제3자 서비스 제공사의 하도급에 있어, ▲ICT 제3자 서비스 제공사가 하청업체를 적절하게 선정하고 모니터링할 수 있는지 여부를 평가하고 ▲하청업체와 관련된 계약 내용 및 하도급 공급망을 문서화·모니터링하며 ▲중대한 변경 사항 발생 시 관련 절차 수행 및 해지권(Kündigungsrechte) 등을 적절히 보장해야 함
	- **(출구전략)** 금융사는 제3자 ICT 서비스 제공사와의 계약 종료 시 대고객 서비스의 중단이나 위험 없이 원활한 비즈니스 운영을 보장할 수 있도록 출구전략(Ausstiegsstrategien)을 마련해야 함
	- **(경영기구 관여 확대)** 「DORA」는 ▲ICT 제3자 위험 검토 ▲핵심 또는 중요 기능을 지원하는 ICT 서비스 사용에 대해 자사의 제3자 서비스 사용 정책 승인 ▲ICT 서비스 사용에 대한 보고 채널 구축 등 금융사 경영기구의 관여를 강화

8 Commission Delegated Regulation (EU) 2024/1774 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework

구분	주요내용
운영 정보보안	• 「DORA」는 '기존 금융부문에 대한 IT 관련 감독요건' 대비 **운영 정보보안 분야의 요건**을 엄격하게 설정하였으며, 또한 **제3자 ICT 서비스 제공사가 운영하는 ICT 시스템**에는 보다 **엄격한 요건**이 적용
	- **(네트워크 보안)** 금융사는 침입(Intrusion)[10] 및 데이터 오용으로부터 네트워크 보안을 보장하기 위해, 보호 조치의 일환으로 ▲네트워크 세분화 및 분리 ▲네트워크 접근 제어 ▲타사 디바이스 감지 등을 포함한 정책, 절차, 프로토콜 등을 개발해야 함 - **(취약점 보고)** 제3자 ICT 서비스 제공사는 금융사의 ICT 시스템에 영향을 미치는 취약점을 해결하고 중요 취약점 등은 적시에 금융사에 보고하며, 적절한 경우 대중에게도 책임감 있고 적절하게 전달해야 함 - **(취약점 처리)** 금융사는 ▲취약점의 중요도 ▲자산의 분류 및 위험 프로필을 고려하여 자체적 우선순위에 따라 해결해야 하며, 취약점 패치의 경우 자동화 도구를 사용하여 소프트웨어 및 하드웨어 패치와 업데이트를 식별하고 평가하는 등 취약점 패치를 다른 조치보다 우선 처리해야 함

■ 전망 및 시사점

○ 동 이행지침은 2023년 산업계, 독일 연방은행, 독일 연방금융감독청장으로 구성된 실무그룹의 협력을 바탕으로 약 1년 만에 도출된 결과물임

- 실무그룹은 30회 이상의 회의를 통해 「DORA」의 요건을 '기존 금융부문에 대한 IT 관련 감독요건'과 비교하여 주요 차이점을 발견하고 조치의 필요성을 확인

○ 한편, 독일 연방금융감독청은 2025년 1월에 적용되는 「DORA」를 고려하여 '기존 금융부문에 대한 IT 감독요건(은행(BAIT)·보험사(VAIT)·자본관리자(KAIT)·전자화폐기관(ZAIT))'을 폐지하는 등 중복 규제를 방지할 계획

Reference

▪https://www.bafin.de/SharedDocs/Downloads/DE/Anlage/Aufsichtsmitteilung/dl_2024_07_08_Aufsichtsmitteilung_Umsetzungshinweise_DORA.pdf?__blob=publicationFile&v=1

▪https://www.finbridge.de/aktuelles/2024/07/16/bafin-dora-bait-vait-umsetzungshinweise

9 시스템의 성능 등이 특정 부문의 과부하로 인해 전체적으로 제한이 가해지는 현상으로, 컴퓨터의 CPU에 과부하가 걸리는 경우 컴퓨터의 전체적 처리 속도 저하 현상이 발생하는 경우를 예로 들 수 있음

10 악의적 의도를 가진 해킹 및 자동화된 도구를 이용한 공격 등으로부터 비롯되는 시스템 및 네트워크에 대한 원치 않은 조작을 의미

해외 단신

독일, 「NIS2 지침 이행법(안)」의 정부 초안(Regierungsentwurf) 채택

○ **(개요)** 독일 연방정부는 「NIS2 지침 이행법안[1]」의 내무부 초안(Referentenentwurf)에 대한 연방 주, 협회, 기관 등의 의견을 수렴한 후 정부 초안(Regierungsentwurf)을 채택(2024. 7. 24.)

- 추후 정부 초안은 연방의회에서 3차 독회를 거쳐, 본회의 최종 표결이 진행될 예정

※ EU 회원국은 2024년 10월 18일까지 EU 「NIS2 지침」을 국내 이행입법으로 마련해야 함

○ **(주요내용)** 공공 또는 민간 조직의 사이버보안 강화를 위하여 적용대상의 범위를 중요도에 따라 구분하고 중대한 사고가 발생한 경우, 관련 조직의 보고의무 등을 강화

- 적용대상의 범위를 '특별히 중요한 조직(Besonders wichtigen)', '중요조직(Wichtige Einrichtungen)'으로 구분하여 사이버 위협을 방지하기 위한 기술적·조직적 조치의무를 규정

- 주요기반시설(KRITIS) 운영자의 경우, 지속적으로 위협을 식별·예방해야 하고 발생한 결함에 대해 적절한 수정조치를 제공해야 하는 등 보다 엄격한 보안 조치의무를 규정

- 중대한 사이버사고가 발생한 경우, '특별히 중요한 조직' 및 '중요조직'은 감독기관*에 ▲24시간 이내로 **최초보고**, ▲72시간 이내로 **후속보고**, ▲후속보고 이후 1개월 이내로 **최종보고**를 진행해야 함

* 독일 연방정부와 연방국민보호재난지원청이 공동 설립한 신고센터

- 연방정보기술보안청(BSI)의 사이버보안 사고 감독권한을 확대하고, 독일 연방정부의 정보보안 관리 개선을 위하여 정보보안책임자 임명 등 관련 의무사항을 규정

※ [2024년 5월] 인터넷·정보보호 법제동향 제200호 참고

Reference

- https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/nis2umsucg.html
- https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/CI1/nis2-regierungsentwurf.pdf?__blob=publicationFile&v=1

1 Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)

해외 입법 동향

독일 연방 법무부, 컴퓨터 범죄 관련「형법」개정안 발표

독일 연방 법무부(BMJ)[1]는 IT 보안 연구자의 특정 행위에 대하여 범죄성립의 예외를 규정하는 한편, 특정 유형의 데이터 감시(Ausspähen) 및 탈취(Abfangen) 행위에 관한 처벌강화를 골자로 한「형법」개정 초안(Referentenentwurf)을 발표 (2024. 11. 4.)

■ 개요 및 추진배경

○ **(배경)** IT 보안 연구자나 서비스업체가 IT 보안연구 수행을 위하여 취약점을 탐지하고 침투테스트(Penetrationstest)를 실행하는 등 타사 시스템 및 데이터에 접근해야 하는 경우가 있으나, 형사상 책임을 부담 우려가 있음

- IT 보안연구의 형사상 책임 부담은 사회적으로 바람직한 행동에도 제약을 가하기 때문에 역효과가 발생할 가능성이 존재하고, 대규모 자산 손실을 초래하거나 주요기반시설(kritische Infrastrukturen)에 심각한 피해를 주는 데이터 감시 및 탈취 행위에 대해서 보다 강력한 처벌이 필요한 상황

○ **(개요)** 독일 연방 법무부는 IT 보안 연구자 및 보안 서비스 제공업체의 활동을 제약한다고 평가받는 컴퓨터 범죄 관련 형법 조항을 개선하기 위하여「형법」개정 초안[2]을 마련

- 개정안은 IT 보안 연구자의 선의의 목적으로 보안 취약점 탐지행위를 하는 경우에는「형법」상 범죄성립의 예외로서 규정하고, 주요기반시설(kritische Infrastrukturen)에 피해를 발생시키는 등의 심각한 데이터 감시 및 탈취 행위에 대한 처벌을 강화

■ 주요내용

(목적) ▲보안 취약점의 탐지와 해소를 의도하는 행위를 보호하고, ▲심각한 피해를 주는 데이터 범죄행위에 대한 제재를 강화하는 컴퓨터 관련 형법의 현대화

○ **(IT 보안연구 행위 처벌예외)** 새로 추가된 형법 제202a조제3항은 아래 조건을 모두 충족하는 경우의 행위는 '권한없는(unbefugt)' 행위가 아니므로 처벌할 수 없다고 규정

1 Bundesministerium der Justiz (BMJ)
2 Referentenentwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Modernisierung des Computerstrafrechts

- **(알리기 위한 목적)** IT 시스템의 보안 취약점 또는 기타 보안위험을 식별하여 해당 IT 시스템 책임자, 시스템 운영 서비스 제공자, 해당 IT 애플리케이션 제조업체 또는 연방정보보안청(BSI)의 책임자 등에게 알리기 위한 의도를 가진 행위

  ※ 다만, 법은 고지 형식을 규정하지 않고 있으며, 공인된 표준화된 절차는 아직 부재한 실정

- **(식별의도)** IT 시스템의 취약점 또는 기타 보안위험을 식별하려는 의도로 수행된 행위

- **(필수불가결성)** 보안 취약점 식별에 필수불가결한(erforderlich) 행위

  ※ 형사책임 배제는 보안 취약점을 확인하기 위해 해당 조치가 필수적인 경우에만 적용되어야 하며, 보안 취약점을 식별하는 데 필요 이상의 데이터에 접근하는 자는 계속 처벌

○ **(심각한 데이터 감시 및 탈취 행위 처벌강화)** 새로 추가된 형법 제202a조제4항은 심각한 데이터 감시 및 탈취 행위에 대한 처벌을 강화함으로써 기존 형법 조문을 보완

- 데이터 감시 및 탈취에 해당하는 사례는 현행(감시의 경우 최대 3년, 탈취의 경우 최대 2년)보다 엄격하게 처벌되어야 하며, 이에 형량을 징역 3개월~최대 5년으로 강화

심각한 데이터 감시 및 탈취 행위의 유형
• 범죄자가 대규모 자산손실을 초래하는 경우
• 영리추구, 상업적 이유로 범행하거나 이러한 행위를 지속적으로 영위하기 위한 범죄단체의 일원으로서 행한 경우
• 주요기반시설의 가용성, 기능, 무결성, 신뢰성 또는 기밀성을 해치거나 독일연방 공화국 또는 주(州)의 안보를 침해한 경우

○ **(현행 제202c조 유지)** 데이터 감시 및 탈취 예비(Vorbereiten) 행위에 대한 처벌규정인 현행 형법 제202c조는 변경이 불필요하다고 판단

- 본 조항은 데이터 감시(제202a조) 또는 데이터 탈취(제202b조) 범죄 실행 목적의 컴퓨터 프로그램을 대상으로 하고있으나, 범죄 준비 행위를 전제하므로 보안연구와 관련된 컴퓨터 프로그램은 범죄성립 요건과는 무관하기 때문이라 설명

- '범죄목적은 범죄자가 추구한 의도를 의미할 뿐 컴퓨터 프로그램의 객관적 범죄 적합성을 가리키지는 않는다'는 연방 헌법재판소 판결(BverfG BvR 2233/07)[3]을 통해, 해킹 도구라 할지라도 IT 보안 연구에 필요하다면 별도의 처벌없이 사용가능함을 시사

3 데이터의 감시 및 탈취(컴퓨터 프로그램, 이중사용도구, 해킹 도구, 범죄를 저지를 의도로 개발 또는 수정, 보안점검 목적의 조달 또는 공개, 고의성 판단) 예비행위에 대한 형사책임 등에 관한 헌법소원의 가능성 여부

■ 전망 및 시사점

○ 독일 법무부는 형법 제202a조 및 제202b조를 일부 변경하는 컴퓨터 범죄 관련 형법의 현대화를 통해 형법이 보안 연구자의 보안 취약점 식별과 같이 사회적 이익에 부합하는 바람직한 행위를 제약하는 일이 발생하지 않을 것으로 기대

- 일각에서는 IT 보안 연구자들이 자신의 행위가 범죄가 아닌 의도에서 수행되었음을 법적으로 문서화하는데 어려움이 예상되므로 개선이 필요하다고 평가

○ 형법 제202c조(컴퓨터 프로그램이나 데이터 접근을 위한 비밀번호 또는 보안코드를 생산, 조달, 판매, 양도, 배포하여 범죄를 준비하는 행위를 처벌)는 해킹 도구의 소지를 범죄로 규정할 여지가 있음에도 조문 변경이 불필요하다는 법무부의 설명에 대하여 많은 반발이 있을 것으로 예상

Reference

- https://www.bmj.de/SharedDocs/Downloads/DE/Gesetzgebung/RefE/RefE_ComputerStrafR.pdf?__blob=publicationFile&v=3
- https://www.bmj.de/SharedDocs/Downloads/DE/Gesetzgebung/Synopse/Synopse_ComputerStrafR_RefE.pdf?__blob=publicationFile&v=2
- https://www.bmj.de/SharedDocs/Downloads/DE/Gesetzgebung/Dokumente/Infopapier_ComputerStrafR.pdf?__blob=publicationFile&v=4
- https://www.heise.de/hintergrund/Neues-Computerstrafrecht-Mehr-Schutz-fuer-Sicherheitsforscher-10032287.html
- https://www.heise.de/news/CCC-Gesetzentwurf-zum-Entschaerfen-der-Hackerparagrafen-ist-stumpf-9995004.html
- https://netzpolitik.org/2024/hacker-paragrafen-wir-veroeffentlichen-den-gesetzentwurf-zum-computerstrafrecht/

해외 입법 동향

스위스, 사이버보안에 관한 법률명령(안) 의견수렴

스위스는 「정보보안법[1]」 개정에 따라 도입된 주요기반시설 사이버공격 보고의무를 구체화하는 사이버보안 법률명령(안)[2]을 마련(2024. 5. 22.)하였고, 올해 9월 13일까지 의견수렴 예정

■ 개요 및 추진배경

○ 스위스는 2023.9.29. 「정보보안법」[3]을 개정하여 ①연방사이버보안청[4]의 역할을 정립하고, ②주요기반시설 운영자 등 적용대상[5]에게 사이버공격 보고의무를 도입함

- 이에 연방사이버보안청의 업무 및 주요기반시설 사이버공격에 대한 보고 요구사항을 구체화하는 시행령(안)을 마련하여 의견수렴 추진

〈 정보보안법의 주요 개정내용 〉

연방사이버보안청의 역할	• 기술 분석을 통해, **사이버사고 및 사이버 위협을 예방**하고 **취약점**을 **식별 및 제거**함 (제73a조) • 사이버사고 및 사이버위협 보고를 접수하고, **내용을 분석하여 제조업체에 취약점 보완을 요구** (제73b조) • **사이버사고 관련 정보를 공개**할 수 있으며 **보고된 내용을 연방 당국 및 조직과 공유** (제73c조 및 제73d조)
사이버공격 보고의무	• 주요기반시설 운영자 등 **적용대상은 사이버공격 발생 시 연방사이버보안청에 그 사실을 보고**해야 하고, 연방사이버보안청은 사고처리를 지원할 수 있음 (제74a조) • 사이버공격으로 인한 시스템 오작동이 **경제 기능 또는 공공복리에 경미한 영향을 미치는 경우**, 해당 조직은 **보고의무 적용대상에서 제외**됨 (제74c조) • ▲주요기반시설의 기능을 위태롭게 하거나, ▲정보 조작 또는 유출을 초래하는 등의 경우에는 연방 사이버보안청에 반드시 보고해야 함 (제74d조) • 사이버공격 발견 후 **24시간 내 연방사이버보안청에 보고**해야 하며, ▲보고의무가 있는 조직, ▲사이버 공격의 성격과 그 영향, ▲이행조치 및 추가 조치 등에 대한 정보를 포함해야 함 (제74e조) • **보고의무 위반 시**, 연방사이버보안청은 **최대 10만 스위스 프랑의 벌금**을 부과 (제74h조)

1 Federal Act on Information Security at the Confederation(Information Security Act, ISA)
2 Ordonnance sur la cybersécurité(OCyS), 스위스 연방 일반법(Le droit ordinaire fédéral)은 연방법(Les lois fédérales)과 법률명령(Les Ordonnances)으로 구분, [출처] https://world.moleg.go.kr/web/wli/nationReadPage.do?ISO_NTNL_CD=CH 참고
3 https://www.fedlex.admin.ch/eli/fga/2023/2296/de 참고
4 l'Office fédéral de la cybersécurité를 말하며, 2024.1.1일부터 기존 재무부 산하 국가사이버보안센터(NCSC)를 국방·시민보호 및 스포츠부(DDPS) 산하 연방기관으로 전환
5 ▲대학, ▲연방조직 및 군사조직, ▲안전 및 구조, 식수 공급, 폐수 처리, 폐기물 처리 부문 공공조직, ▲에너지 부문 조직, ▲은행 등 금융조직, ▲의료 시설, ▲의료 실험실, ▲스위스 라디오 텔레비전 등 언론기관, ▲우편 서비스, ▲대중교통, ▲민간 항공, ▲필수적인 일상용품 공급조직, ▲통신 서비스, 정치적 권리행사 서비스, 디지털 서비스 제공업체, ▲하드웨어 및 소프트웨어 제조업체 등이 포함 (「정보보안법」 제74b조)

■ 주요내용

○ **(국가사이버전략)** 스위스 연방정부는 ▲사이버보안 사고·위협 예방, ▲사이버위협 조기 탐지, ▲사고 발생 시 대응 및 복원력 확보를 위하여 전략적 프레임워크 형성

- 스위스 연방정부는 국가사이버전략운영위원회(La Cyberstratégie nationale)를 설립하고, 연방사이버보안청이 국가사이버전략운영위원회 사무국을 운영함

- 국가사이버전략운영위원회는 ▲최소 5년마다 전략을 검토, ▲이해관계자들과 협의하여 전략의 우선순위를 정하고 추진일정 제안서를 작성하며, ▲정기적으로 전략 이행을 평가하여 연방정부와 주정부에 결과를 통보하고, ▲필요한 경우 추가 조치에 대한 제안서를 연방정부에 제출해야 함

○ **(연방사이버보안청)** 사이버사고 및 사이버위협에 대해 기술 분석을 진행하고, 이러한 분석을 위하여 연방 IT시스템과 독립적으로 운영되는 인프라를 갖춰야 함

연방사이버보안청의 역할

- 신고 접수받은 취약점을 국제적으로 인정된 표준에 따라 조정하여 공개
- 관련 하드웨어 또는 소프트웨어 제조업체가 취약점을 제거할 수 있도록 90일의 기한을 설정
- 다음과 같은 경우 90일의 기한을 단축할 수 있음
  - 주요기반시설의 기능을 위태롭게 하는 경우
  - 사이버공격에 매우 쉽게 악용될 수 있는 경우
  - 광범위한 시스템에 영향을 미치는 경우
- 취약점 해결이 특히 복잡한 경우 기한을 연장할 수 있음

※ 연방통신청(l'Office fédéral de la communication, OFCOM)이 통신 장비에 관한 법률명령 제36조[6]에 따른 모니터링 과정에서 발견한 취약점에는 해당하지 않고, 연방사이버보안청은 「통신법」 제3조제d항[7]에 따라 통신 장비에서 발견한 취약점을 즉시 연방통신청에 통보해야 함

- 사이버공격 발생 시 자문 및 지원에 대한 수요가 연방사이버보안청의 수용 능력을 초과할 경우, 공공안전과 질서, 경제 기능 또는 공공복리를 고려하여 우선순위를 결정할 수 있음

- 연방사이버보안청은 사이버보안 표준 및 규정의 개발·구현·검토에 있어, 연방 및 주 당국을 지원함

○ **(정보공유)** 사이버보안청은 사이버위협 및 사이버사고 정보를 공유할 수 있는 통신시스템과 정보시스템을 제공해야 하고, 이러한 시스템의 보안을 보장해야 함

- 통신시스템을 사용하려는 당국 및 조직은 ▲당국 또는 조직의 명칭·주소, ▲등록한 사람의 연락처 정보를 포함해야 등록해야 하며, 정보가 변경될 경우 연방사이버보안청에 지체없이 보고해야 함

- 정보공유에 참여하고자 하는 주요기반시설 운영자는 연방사이버보안청에 ▲회사명 또는 ▲자신의 이름과 연락처 정보를 표시하여 통지해야 함

6 art. 36 ss de l'ordonnance du 25 novembre 2015 sur les Ordonnance sur la cybersécurité installations de télécommunication
7 l'art. 3, let. d, de la loi du 30 avril 1997 sur les télécommunications

- 연방사이버보안청은 사이버위협·공격에 관한 정보의 공개 여부와 시기를 결정할 권한이 있음

○ **(보고의무)** 보고의무가 있는 모든 당국 및 조직은 사이버공격 발생 시 ▲공격 발생 날짜 및 시간, 공격 유형, 공격 방법, 공격자 관련 정보, ▲사이버공격 결과에 대한 정보, ▲당국 및 조직의 기능에 미치는 영향을 포함하여, 24시간 이내에 연방사이버보안청에 알려야 함

- 24시간 이내에 필요한 모든 정보가 제공되지 않을 경우, 연방사이버보안청은 보고의무가 있는 당국 및 조직에 14일 이내에 보고서를 작성하도록 함

보고의무 면제조직
• 경제기능이나 공공복리에 직접적인 영향을 미치지 않는 사이버공격을 받은 조직
• 에너지 공급, 운송 등 일부 부문에서 보고의무 면제를 정의하기 위해 설정된 임계값 미만인 모든 조직
• 직원 수가 50명 미만이고 연간 매출 또는 대차대조표 총액이 1,000만 스위스 프랑 미만인 조직
• 주민 1,000명 미만을 책임지는 당국

○ **(시행일)** 동 시행령은 2025년 1월 1일부터 시행

■ 전망 및 시사점

○ 스위스 정부는 정보보안법 개정과 사이버보안 법률명령(안) 입법 추진을 통해, 국가사이버보안전략의 수립 등 국가 차원의 체계적인 사이버보안 관리체계를 구축하고, 주요기반시설 보호 및 사이버 위협에 효과적으로 대응하기 위한 법제도적 기반을 마련하고 있음

- 특히, 주요기반시설 사이버사고 보고의무의 방법, 적용대상, 보고해야 하는 사고의 범위, 보고의무의 면제 범위 등을 구체화하여, 적용대상 기관등에 실질적인 기준을 제시할 것으로 보임

Reference

▪https://www.ncsc.admin.ch/ncsc/en/home/dokumentation/medienmitteilungen/newslist.msg-id-101088.html
▪https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/dl/proj/2024/35/cons_1/doc_1/fr/pdf-a/fedlex-data-admin-ch-eli-dl-proj-2024-35-cons_1-doc_1-fr-pdf-a.pdf
▪https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/dl/proj/2024/35/cons_1/doc_2/de/pdf-a/fedlex-data-admin-ch-eli-dl-proj-2024-35-cons_1-doc_2-de-pdf-a.pdf
▪https://www.mme.ch/en/magazine/articles/the-new-information-security-act
▪https://www.fedlex.admin.ch/eli/fga/2023/2296/de

일 본

해외 입법 동향

일본 정부, 「중요 경제안보 정보보호·활용법」 제정

일본 정부는 경제안보상 비밀 정보 관리를 강화하기 위해 경제 안전보장 분야의 중요 정보를 취급하는 담당자를 정부가 인정하는 '적격성 평가(Security Clearance)' 제도 신설을 골자로 한 「중요 경제안보 정보보호·활용법[1]」을 제정 (2024. 5. 10.)

■ 개요

○ 일본은 「중요 경제안보 정보보호·활용법」 제정[2]을 통해 안보에 영향을 줄 수 있는 정보를 '중요 경제안보정보'로 지정하고 이를 보호·활용하도록 규정

- 본 제정법은 ▲중요 경제안보 정보 지정 ▲국가안보 확보에 기여 활동을 하는 사업자에 대한 중요 경제안보 정보 제공 ▲중요 경제안보 정보취급자 제한 등 정보 누설을 방지하고, 국가와 국민 안전 확보를 목표로 함

■ 주요내용

○ **(정의)** 동 법은 '중요 경제기반'과 '중요 경제기반 보호정보' 등을 정의함 (제2조)

구분	정의
중요 경제기반	• ▲일본의 국민생활 또는 경제활동의 기반이 되는 공공 업무 제공에 지장이 있는 경우에 일본 및 국민의 안전을 해치는 사태가 발생할 우려가 있는 주요기반시설, ▲국민의 생존에 반드시 필요하거나, 일본의 국민생활 또는 경제활동에 널리 필요할 것으로 예상되는 중요한 물자의 공급망
중요 경제기반 보호정보	• ▲외부 행위로부터 중요 경제기반을 보호하기 위한 조치 또는 이에 관한 계획이나 연구, ▲중요 경제기반의 취약점, 중요 경제기반 관련 혁신적 기술, 기타 중요 경제기반에 관한 중요한 정보로서 안전보장에 관한 것, ▲중요 경제기반 보호조치에 관하여 수집한 외국의 정부 또는 국제기관으로부터의 정보 등

1 重要経済安保情報の保護および活用に関する法律

2 ▲특정비밀은 누출 시 안전보장에 '현저한 지장'을 주는 정보로 「특정비밀보호법」에서 대응 (예) 방위, 외교, 간첩활동 방지, 테러 방지 등 4개 분야(향후 경제 분야로도 확대 예정) ▲중요 경제안보정보는 누출 시 안전보장에 '지장'을 주는 정보로 「중요 경제안보정보 보호·활용법」에서 대응 (예) 사이버 위협 및 대책에 관한 정보, 공급망상 취약점 관련 정보 등(KPMG, セキュリティ・クリアランス制度, 2024.4.22.)

○ **(행정기관 지정 권한)** 행정기관의 장은 '중요 경제안보 정보'를 지정하고 관련 정보를 제공할 수 있음

권한	내용
중요 경제안보 정보 지정	• 행정기관의 장[3]은 '중요 경제기반(중요 기반시설, 물자의 공급망) 보호 정보' 중, 유출되었을 시 일본의 안전보장에 지장을 줄 우려로 인해 특히 은닉할 필요성이 있는 공개되지 않은 정보를 '중요 경제안보 정보'로 지정 (제3조 ~ 제5조) - 행정기관의 장은 중요 경제안보 정보 취급 업무를 수행하는 담당자의 범위를 정하는 등 해당 정보 보호에 필요한 조치를 강구해야 함 · 이때, 지정일로부터 5년을 넘지 않는 범위 내에서 유효기간을 설정(유효기간 연장은 원칙적으로 30년을 초과할 수 없음)하되, 지정요건을 결여한 경우에는 신속히 해제
중요 경제안보 정보 제공	• 행정기관의 장은 ▲다른 행정기관 등에 대한 중요 경제안보 정보, ▲적합 사업자에 대한 중요 경제안보 정보를 제공할 수 있음 (제6조 ~ 제10조) - ▲다른 행정기관, 외국 정부, 국제기구 등이 이용할 필요가 있다고 인정할 때, 또는 ▲일본의 안전보장에 현저한 지장을 미칠 우려가 없다고 인정할 때에는 국회, 수사기관, 법원 등에 중요 경제안보 정보를 제공할 수 있음 - 적합 사업자(시행령으로 정하는 보전 기준에 적합한 사업자)와의 계약에 따라 중요 경제기반에 대한 취약점 해소 등 일본의 안전보장 확보에 이바지하는 활동 촉진을 위해 필요하다고 인정할 때에는 중요 경제안보 정보를 제공할 수 있음[4]

○ **(중요 경제안보 정보취급자 제한)** 중요 경제안보 정보의 취급 업무는 적격성 평가에서 중요 경제안보 정보를 누설할 우려가 없다고 인정된 자로 제한 (제11조)

- 「특정비밀보호법」에 따른 적격성 평가에서 특정비밀 취급 업무를 수행한 경우, 이를 누설할 우려가 없다고 인정된 자는 5년 동안 중요 경제안보 정보를 취급하는 업무를 할 수 있음

○ **(적격성 평가)** 행정기관의 장은 본인의 동의를 얻은 후, 내각총리대신의 조사 결과에 따라 적격성 평가를 실시(적격성 평가의 유효기간은 10년) (제12조~제17조)

- (행정기관의 장이 적격성 평가를 실시할 때) 내각총리대신에게 필요한 자료를 첨부하여 적격성 평가에 필요한 조사를 실시하도록 요구하고, 이에 내각총리대신은 조사를 실시하고 의견을 붙여 조사 결과를 행정기관의 장에게 회신

조사 내용
• ▲중요 경제기반 훼손 활동[5]과의 관계(평가 대상자의 가족 및 동거인의 성명, 생년월일, 국적, 주소를 포함) ▲범죄 및 징계 경력 ▲정보 취급과 관련된 위법행위 경력 ▲약물의 남용 및 영향 ▲정신 질환 ▲음주 ▲신용상태 등 경제적 상황에 관한 사항

- (행정기관 외의 기관장이 적격성 평가를 실시할 때) 평가 대상자가 가장 최근에 실시한 적격성 평가(10년을 경과하지 않은 것에 한함)에서 중요 경제안보 정보를 누설할 우려가 없다고 인정받은 경우 재조사하지 않고 적격성 평가를 할 수 있음

3 행정사무를 분담 관리하는 각 부처 대신

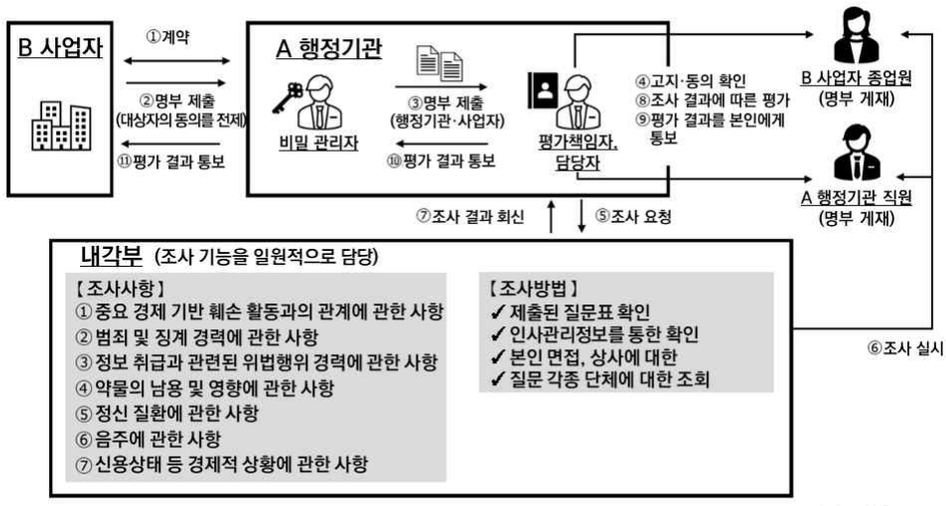
4 계약을 통해 규정하는 사항은 ▲중요 경제안보정보 취급을 수행할 권한이 있는 자의 범위 ▲중요 경제안보정보 보호 업무의 관리자 선임에 관한 사항 ▲중요 경제안보정보 보호에 필요한 시설 및 장비 설치에 관한 사항 ▲임직원에 대한 중요 경제안보정보 보호 교육에 관한 사항 ▲행정기관의 장이 요구한 경우에는 중요 경제안보정보를 행정기관의 장에게 제공해야 한다는 사항 ▲해당 적합 사업자가 중요 경제안보정보를 보호하기 위해 필요하다고 판단한 것으로서 시행령에서 정하는 사항(1년 내 시행 예정)

5 중요 경제기반에 관한 공개되지 않은 정보 중 그 누설이 일본의 안전보장에 지장을 줄 우려가 있는 것을 취득하기 위한 활동을 하거나, 중요 경제기반에 대해 일본 및 국민의 안전을 현저하게 해칠 우려가 있는 활동

- 중요 경제안보 정보를 취급하는 적합 사업자에 소속된 종업원(민간인)도 같은 조사·평가를 실시

- 행정기관의 장은 적격성 평가를 실시한 경우, 그 결과를 평가 대상자 및 내각총리대신에게 통보, 인정되지 않은 경우에는 적격성 평가의 원활한 실시 확보를 방해하지 않는 범위 내에서 평가 대상자에게 사유를 함께 통보

적격성 평가 업무 흐름도[6]



○ **(벌칙)** 중요 경제안보 정보 누설 시 5년 이하의 구금형이나 500만 엔 이하의 벌금 또는 이것을 병행 부과하는 벌칙 등을 규정 (제22조~제27조)

■ 전망 및 시사점

○ 일본은 「중요 경제안보 정보보호·활용법」 제정을 통해 국가안보에 지장을 줄 가능성이 있는 정보를 '중요 경제안보 정보'로 지정·관리함으로써 안보의 범위를 경제분야로 확대

○ 또한, 일본의 안보 확보를 위한 중요 경제기반 정보, 특히 비밀유지가 필요한 정보에 대해 국제기준의 비밀보호제도를 마련하여 보호·활용하는 체제 확립

- 일본은 2013년에 제정된 「특정비밀보호법」으로 외교·방위 등 분야에서 비밀정보를 보호해왔으나, 주요 7개국(G7) 중 유일하게 경제안보 분야 관련 명확한 규정이 부재하였음

- 동 법 제정을 통해 외국과 동등한 제도를 마련함으로써 국내 기업은 일본 정부를 통해 타국의 기밀 정보를 제공받을 수 있게 되고, 국제 공동 개발과 타국 정부의 조달 참가 기회가 확대됨

- 또한, 동 법은 경제안보 상의 정보 누설 리스크를 줄이는 중요한 포석이며, 같은 제도를 구비하고 있는 유럽과 미국과의 정보 공유나 민간기업의 경쟁력 강화에 이바지할 것으로 평가

6 내각부 「중요 경제안보 정보보호·활용법」 개요 https://www.cas.go.jp/jp/houdou/pdf/20240227_siryou.pdf 참고

○ 반면, 중요 경제안보 정보취급에 대한 적격성 평가 과정에서 민간인 조사를 통한 개인정보 침해 우려가 커졌으며, 최근 일련의 비밀보호법제 강화로 국민의 알 권리는 더욱 제약될 전망

- 국가가 적격성을 인정한 사람만이 정보를 취급하는 '적격성 평가' 제도를 도입해 경제안보상 비밀정보를 취급하는 민간인들도 조사 대상에 포함시켜, 개인정보보호 침해나 자의적인 정보 지정으로 국민의 알 권리가 제한된다는 우려 증대

- 조사 대상자는 정치사상, 범죄 전력, 약물 이용, 정신 질환 등 치료 이력, 가족 국적, 해외여행 이력 등에 이르기 때문에 사생활 침해 우려가 커지고 있음

- 향후 기밀성이 높다고 판단한 '중요 경제안보 정보'는 누설 시, 벌칙이 과중한 「특정비밀보호법」의 적용대상으로써 특정비밀보호법 운용기준도 개정할 계획이라고 밝힘

Reference

▪https://www.cas.go.jp/jp/houdou/pdf/20240227_siryou.pdf
▪https://www.cas.go.jp/jp/houan/240227/siryou1.pdf
▪https://www.sangiin.go.jp/japanese/ugoki/r6/240510.html
▪https://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/honbun/houan/g21309024.htm
▪https://www.tokyo-np.co.jp/article/326405
▪https://www.sankei.com/article/20240510-5XZT5UTGVVPNRASWGVBIIRAPDE/
▪https://www.sankei.com/article/20240512-Z6GCXW77FVPRTLFTKYK5CLEME4/
▪https://www.jcp.or.jp/akahata/aik24/2024-05-11/2024051104_04_0.html

해외 입법 동향

일본,「스마트폰 소프트웨어 경쟁 촉진법」제정

일본은 스마트폰의 특정 소프트웨어 보안을 확보하고 경쟁을 통한 혁신을 활성화하여, 소비자가 다양한 서비스를 선택할 수 있도록「스마트폰 소프트웨어 경쟁 촉진법[1]」을 제정 (2024. 6. 12.)

■ 추진배경

○ 2023년 2월 일본 공정거래위원회는 구글, 애플의 시장 지배력을 제한하기 위하여 사전규제를 도입해야 한다는 취지의「모바일 OS 및 앱 배포 시장에 대한 연구보고서[2]」를 발표하였고, 같은 해 6월 총리 직속의 디지털시장경쟁본부가「모바일 생태계 경쟁 평가 최종보고서[3]」를 발표

○ 스마트폰 소프트웨어 시장에서 공정하고 자유로운 경쟁이 저해되고, 기존「독점금지법[4]」에 따른 개별 안건 대응으로는 입증에 상당한 시간이 소모된다는 지적

■ 주요내용

○ **(정의)** 주요 용어를 다음과 같이 정의함(제2조)

구분	주요 내용
스마트폰	• ▲항상 휴대하고 사용할 수 있을 만큼 충분히 커야 하고, ▲소프트웨어(프로그램)가 설치되어 있어야 하며, ▲전화와 인터넷을 사용할 수 있어야 함
기본 운영 소프트웨어 (OS)	• 스마트폰의 중앙처리장치에서 계산을 제어하고 다른 스마트폰의 동작을 제어하기 위해 정보처리를 수행하도록 구성된 스마트폰 내장 소프트웨어를 의미함
개별 소프트웨어	• 스마트폰에 내장되어 기본 운영 소프트웨어를 통해 이메일 송수신, 지도 표시 등 스마트폰 사용자의 개별 사용을 위해 구성된 소프트웨어
특정 소프트웨어	• 기본 운영 소프트웨어, 앱 스토어, 브라우저 및 검색 엔진 등을 총칭
앱스토어	• 유료 또는 무료로 제공되는 개별 소프트웨어를 스마트폰에 내장할 목적으로 사용되는 개별 소프트웨어

○ **(지정 사업자)** 공정거래위원회는 특정 소프트웨어를 제공하는 사업자 중, 특정 소프트웨어의 종류별로 시행령에서 정하는 일정 규모 이상의 사업자를 규제 대상으로 지정(제3조)

1 スマートフォンにおいて利用される特定ソフトウェアに係る競争の促進に関する法律
2 2023 年2月 公正取引委員会,「モバイルＯＳ等に関する実態調査報告書」
3 2023年６月16日 内閣官房デジタル市場競争本部事務局,「モバイル・エコシステムに関する競争評価 最終報告 概要」
4 私的独占の禁止及び公正取引の確保に関する法律

○ **(금지행위 및 조치의무 규정)** 특정 소프트웨어 관련 경쟁 과제에 대응하기 위해, **지정 사업자**에게 ▲앱 사업자에 대한 차별대우, 앱스토어 간 경쟁제한 등 특정 행위의 **금지**(제5조~제9조)와 ▲데이터 취득의 조건 공개, 지정 사업자 서비스의 기본 설정 등 **조치의무**를 규정(제10조~제13조)

구분		주요 내용
(1) **금지** 행위	취득한 데이터의 부정 이용 금지(제5조)	• 지정 사업자가 취득한 개별 소프트웨어 사용 및 운영 상황, 판매, 사양 관련 데이터를 다른 앱 사업자와 경쟁하는 제품·서비스를 제공하기 위한 목적으로 활용하는 것을 금지함
	앱 사업자에 대한 부당한 대우 금지(제6조)	• 지정 사업자가 다른 앱 사업자의 기본 운영 소프트웨어, 앱스토어 사용조건, 이러한 조건에 기반한 거래에 대하여 부당하게 차별하고 불공정하게 취급하는 것을 금지함
	앱스토어 간 경쟁 제한 금지(제7조제1호)	• 지정 사업자가 ▲다른 업체의 앱스토어 제공을 방해하거나, ▲스마트폰 사용자로 하여금 다른 사업자가 제공한 앱스토어 사용을 막는 행위를 금지함 ※ 사이버보안기본법 제2조에 규정된 **사이버보안[5] 확보**, 스마트폰 이용에 따라 취득되는 성명, 성별 등 **이용자 관련 정보 보호**, 스마트폰 이용 관련 **청소년 보호** 등의 **목적을 달성하기 어려운 경우에는 그러하지 아니함**
	기본 운영 소프트웨어로 제어되는 기능에 대한 다른 사업자의 접근 제한 금지(제7조제2호)	• 기본 운영 소프트웨어로 제어되는 기능과 관련하여, 지정 사업자가 사용하는 스마트폰 조작 기능을 다른 사업자가 사용하지 못하도록 제한하는 행위를 금지함 ※ 정당한 사유가 있는 경우 그러하지 아니함
	지정 사업자 이외의 과금 시스템 이용 제한 금지(제8조제1호)	• 지정 사업자가 직접 제공하는 결제 관리 서비스 이외에 타사의 결제 수단을 이용하지 못하도록 방해하는 행위를 금지함 ※ 정당한 사유가 있는 경우 그러하지 아니함
	앱 내 사용자에 대한 정보제공 제한 금지(제8조제2호)	• 지정 사업자가 앱에서 웹페이지 등을 통해 제공되는 제품·서비스의 가격 표시, 웹페이지로 유도하는 링크 표시를 제한하는 행위를 금지함 • 지정 사업자가 스마트폰 사용자에게 웹페이지를 통해 제품·서비스를 제공하는 것을 금지함 ※ 정당한 사유가 있는 경우 그러하지 아니함
	지정 사업자 이외의 브라우저 엔진 이용 방해 금지(제8조제3호)	• 지정 사업자가 자사의 브라우저 엔진 이용을 조건으로 하는 등 타사의 브라우저 엔진을 이용하지 못하도록 방해하는 행위를 금지함 ※ 정당한 사유가 있는 경우 그러하지 아니함
	검색에 대한 자사 서비스 우선 표시 금지(제9조)	• 지정 사업자가 검색 결과 표시에서 자사 서비스를 정당한 이유 없이 경쟁 관계에 있는 타사의 서비스보다 우선적으로 표시하는 행위를 금지함
(2) **조치** 의무	데이터 취득의 조건 공개에 관한 조치(제10조)	• 지정 사업자는 개별 소프트웨어 사용 및 운영 상황, 판매, 사양 관련 데이터의 취득 또는 이용조건을 다른 개별 소프트웨어 운영자에게 공개해야 함
	취득한 데이터의 전송에 관한 조치(제11조)	• 지정 사업자는 스마트폰 사용자의 요청에 따라 공정거래위원회 규칙에 따라 사용자 또는 사용자가 지정한 사람에게 특정 소프트웨어 데이터를 이전할 수 있도록 조치해야 함
	지정 사업자 서비스의 기본 설정(제12조 제1호, 제2호)	• 기본 설정(Default Setting)에 대해서 일반 스마트폰 이용자가 간단한 조작으로 변경할 수 있도록 해야 함 • 브라우저, 검색 등에 대해 다른 사업자가 제공하는 동종의 서비스 선택사항을 나타내는 선택 화면(Choice Screen)을 제공해야 함
	특정 소프트웨어의 사양 변경 등에 관한 조치(제13조)	• 지정 사업자는 특정 소프트웨어의 사양 설정 및 변경, 사용조건 설정 및 변경을 거부할 수 있고, 거절할 경우 다음 사업자가 필요한 시스템을 구축하는 등 원활하게 대응할 수 있도록 필요한 조치를 해야 함

5 ▲기록, 전송, 송수신한 정보의 누설, 멸실 또는 훼손을 방지하기 위하여 필요한 조치, ▲기타 정보의 안전한 관리를 위하여 필요한 조치, ▲정보통신망의 안전성 및 신뢰성을 확보하기 위하여 필요한 조치, ▲전자 컴퓨터의 무단 행위로 인한 피해를 방지하기 위해 필요한 조치가 포함됨

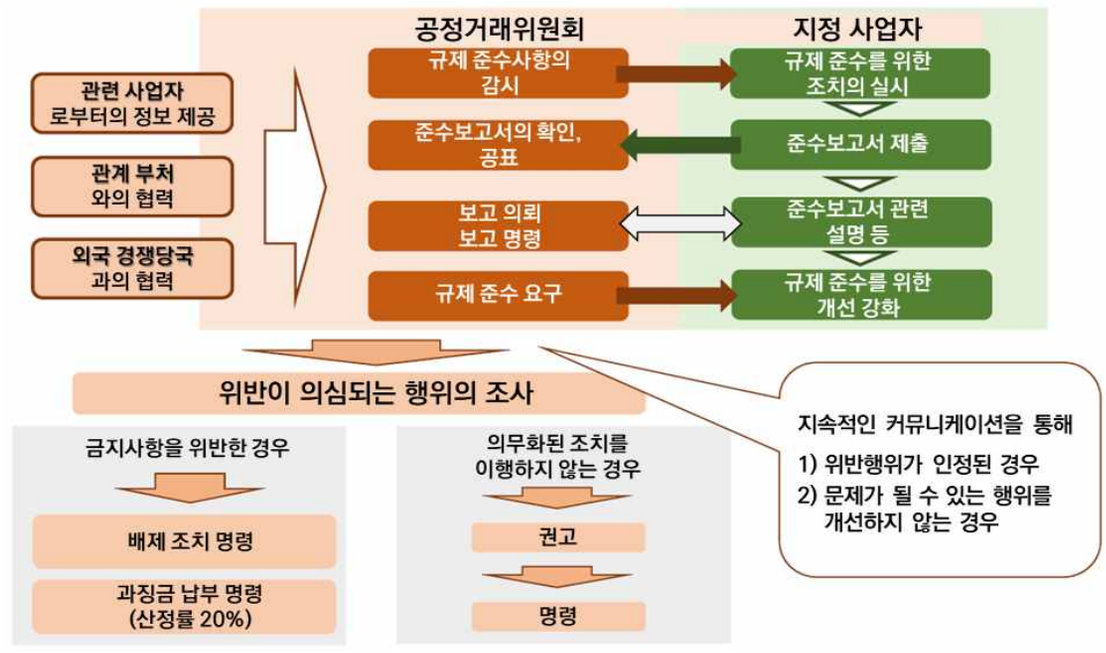
○ **(지정 사업자의 보고의무)** 지정 사업자는 ▲업무 개요, ▲금지행위 및 조치의무, ▲규정 준수상태를 확인하기 위해 필요한 사항 등을 포함한 보고서를 매 회계연도마다 공정거래위원회에 제출

○ **(공정거래위원회의 조치)** ▲위반 행위 등의 신고 및 조사(제15조) ▲규정 위반 시정명령(제16조~제18조) ▲과징금 납부 명령(제19조~제20조) 등의 조치를 할 수 있음

구분	주요 내용
위반행위 신고 및 조사	• 공정거래위원회는 위반행위 신고가 접수된 경우, 해당 신고에 대하여 조사하고 적절한 조치를 이행하거나 이행하지 않기로 결정한 경우 신고자에게 지체없이 그 사실을 통보해야 함
시정명령	• 지정 사업자가 규정을 위반한 경우, 공정거래위원회는 해당 행위의 중지, 사업의 일부 양도 또는 규정을 위반한 행위의 제거를 위하여 필요한 조치를 이행할 수 있음
과징금 납부 명령	• 지정 사업자가 규정을 위반한 경우, 공정거래위원회는 지정 사업자의 제품 및 서비스 판매액의 20%를 납부할 것을 명할 수 있음

- 기존 독점금지법 집행(공정위가 개별 안건별로 대응)과는 달리 지정 사업자, 앱 사업자 등 이해관계자와 지속적으로 대화하면서 비즈니스 모델 개선을 요구하는 새로운 규제의 틀 마련

규제 실효성 확보 조치 흐름도[6]



○ **(시행일)** 공포일로부터 1년 6개월 이내로 시행령에서 정한 날(단, 일부 규정 제외)

6 公正取引委員会, スマートフォンにおいて利用される特定ソフトウェアに係る競争の促進に関する法律案の概要, 2024.4.26

■ 전망 및 시사점

○ 스마트폰 생태계를 지배하는 사업자의 경쟁제한 행위를 금지하고. 대안적인 앱스토어 및 결제수단을 허용하도록 하는 일본판 디지털 시장법(Digital Market Act, DMA)이 제정되었다는 점에서 의의

- 일본 공정거래위원회는 추후 동 법률의 구체적인 해석을 담은 지침을 발표할 것으로 예상

Reference

▪https://www.jftc.go.jp/houdou/pressrelease/2024/apr/240426_digitaloffice.html
▪https://www.jftc.go.jp/houdou/pressrelease/2024/apr/240426_0102gaiyou.pdf
▪https://www.jftc.go.jp/houdou/pressrelease/2024/apr/240426_0101gaiyou.pdf
▪https://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/honbun/houan/g21309062.htm
▪https://www.nli-research.co.jp/report/detail/id=78607?pno=1&site=nli
▪https://www.itmedia.co.jp/mobile/articles/2404/27/news055.html
▪https://www.jiji.com/jc/article?k=2024052300158&g=eco
▪https://www.lawtimes.co.kr/LawFirm-NewsLetter/198588
▪https://www.yna.co.kr/view/AKR20240531130800017?input=1195m

중 국

해외 입법 동향

중국 국무원, 「네트워크 데이터안전 관리조례」 발표

중국 국무원은 「개인정보보호법」, 「네트워크안전법」, 「데이터안전법」의 원칙적인 규정을 구체적으로 보완하고 3법 간의 관계를 조율하기 위하여, 「네트워크 데이터안전 관리조례[1]」를 발표 (2024. 9. 24.)

■ 추진배경 및 개요

○ 중국 공산당 중앙위원회는 제20기 제3차 전체회의(2024. 7. 15. ~ 18.)에서 실물경제와 디지털 경제의 통합을 촉진하기 위하여, ▲플랫폼 경제의 혁신발전 촉진, ▲데이터 보안 거버넌스 및 감독기능 개선, ▲데이터의 국경 간 이동 메커니즘 구축 등을 추진하기로 결정[2]

○ 상기 결정에 부응하여 ▲데이터 국외이전 보안관리, ▲네트워크 데이터 처리자의 의무, ▲네트워크 플랫폼 서비스 제공자의 의무 등을 규정한 동 관리조례는 2025년 1월 1일부터 시행될 예정

■ 주요내용

○ **(목적 및 법적근거)** ▲네트워크 데이터 처리활동의 규제 ▲네트워크 데이터의 보안 강화 ▲네트워크 데이터의 합리적이고 효과적인 사용 촉진 등을 위하여, 「네트워크안전법(网络安全法)」,「개인정보보호법(个人信息保护法)」, 「데이터안전법(数据安全法)」에 의거해 규정을 마련

○ **(적용범위)** 중국 영토 내 네트워크 데이터 처리 활동과 관련된 보안 감독 관리에 적용되며, 중국 국민의 개인정보를 처리하는 국외 활동에도 적용

○ **(정의)** 동 규정은 주요 용어를 다음과 같이 정의

구분	주요내용
네트워크 데이터 (网络数据)	· 네트워크를 통해 가공, 생성된 각종 전자 데이터
네트워크 데이터 처리 활동 (网络数据处理活动)	· 네트워크 데이터의 수집, 저장, 사용, 처리, 전송, 제공, 공개, 삭제 및 기타 활동
네트워크 데이터 처리자 (网络数据处理者)	· 네트워크 데이터 처리 활동에서 처리 목적과 방법을 독립적으로 결정하는 개인과 조직

1 网络数据安全管理条例
2 [출처] KIEP 오늘의 세계경제(2024년 9월 20일 Vol.24 No.12) 「중국의 제20기 3중전회 주요 내용 및 향후 경제정책 방향」, 대외경제정책연구원

구분	주요내용
중요 데이터 (重要数据)	· 특정 분야, 집단, 지역에 관한 데이터 또는 일정한 정확도와 규모를 갖는 데이터로서, – 변조, 손상, 유출 또는 불법 접근 또는 불법 활용 시 국가안보, 경제 운영, 사회 안정, 공중 보건 및 안전에 직접적인 위협이 될 수 있는 데이터
대규모 네트워크 플랫폼 (大型网络平台)	· 등록 사용자 수 5천만 명 이상 또는 월간 활성 사용자 수 1천만 명 이상의 네트워크 플랫폼으로서, – 사업 유형이 복잡하고 네트워크 데이터 처리 활동이 국가안보, 경제 운영, 국민 경제 및 민생에 중대한 영향을 미치는 네트워크 데이터 처리 활동을 하는 플랫폼

○ **(네트워크 데이터 보안관리)** 네트워크 데이터 처리자는 네트워크 데이터 보안을 위해 다음과 같은 조치를 이행해야 함

구분	주요내용
취약점 보고	· 네트워크 제품 또는 서비스에 보안 결함, 취약점 등이 있는 것으로 발견되면 즉시 시정조치를 취해야 하며 사용자에게 즉시 알리고 관할 부서에 보고해야 함 – 국가안보 또는 공공이익을 위태롭게 하는 경우, 네트워크 데이터 처리자는 24시간 이내에 관련 규제부서에도 보고해야 함
보안사고 비상대응 계획	· 네트워크 데이터 보안 사고에 대한 비상대응 계획을 수립하고 완료해야 함 – 네트워크 데이터 보안 사고가 발생하면 즉시 비상대응 계획을 시작하고, 피해 확대를 방지하기 위한 조치를 취하며 규정에 따라 관련 규제부서에 보고해야 함
개인정보 및 중요 데이터 처리 위탁	· 개인정보 및 중요 데이터의 처리를 다른 네트워크 데이터 처리자에게 제공하거나 위탁하는 경우, – 계약 등을 통해 목적, 방법, 범위, 보안 보호 의무 등에 대해 네트워크 데이터 수신자와 합의하고 네트워크 데이터 수신자의 의무 이행에 대한 감독을 수행해야 함 – 다른 네트워크 데이터 취급자에게 제공 또는 위탁받은 개인정보 및 중요 데이터의 처리 기록은 최소 3년 동안 보관해야 함
주요정보기반시설 등 관련 의무	· 국가기관 또는 주요정보기반시설 운영자에게 서비스를 제공하거나 기타 공공 인프라 또는 공공 서비스 시스템의 구축, 운영 또는 유지 보수에 참여하는 경우, – 법률 및 규정 및 계약 계약에 따라 네트워크 데이터 보안 보호의무를 수행하고 안전하고 안정적이며 지속적인 서비스를 제공해야 함

○ **(개인정보보호 방안 구체화)** 개인정보를 처리하는 네트워크 데이터 처리자는 다음 조치를 이행해야 함

구분	주요내용
개인정보 처리규칙 수립	· 개인정보를 처리하기 전에 다음 내용을 포함하여, 구체적이며 명확하게 이해할 수 있는 내용으로 개인정보 처리규칙을 마련해야 함 – 개인정보 처리자의 명칭과 연락처 정보 – 개인정보 처리 목적·방법·유형·민감한 개인정보 처리의 필요성·개인의 권익에 미치는 영향 – 개인정보 보유기간을 확정하기 어려운 경우 보유기간을 정하는 방법 – 개인정보를 검토, 복사, 전송, 수정, 보완, 삭제 또는 제한하는 방법 및 채널, 계정 해지 및 동의 철회의 방법
개인의 동의 획득	· 개인의 동의를 받아 개인정보 처리할 경우 다음 사항을 준수해야 함 – 필요 범위를 초과한 개인정보 수집 금지 및 오해, 사기, 강요를 통한 동의 획득 금지 – 민감한 개인정보 처리 시 별도 동의 획득 – 14세 미만 미성년자 개인정보 처리 시 보호자 동의 획득 – 개인정보 처리 목적, 방법, 종류 변경 시 재차 동의 획득
개인의 권리 행사 지원	· 개인이 자신의 개인정보에 대한 접근, 복사, 수정, 보완, 삭제, 처리 제한을 요청하거나 계정 탈퇴 또는 동의 철회 시 적시에 이를 수락

○ **(중요 데이터 보안 시스템 개선)** 국가 데이터 보안 당국은 관련 부서 간 협의를 통해 중요 데이터 목록을 작성하고 네트워크 데이터 처리자에게 이를 전달해야 하며, 데이터 처리자는 다음을 이행해야 함

구분	주요내용
중요 데이터 보안 책임	· 중요 데이터 처리자는 네트워크 보안 책임자 및 네트워크 데이터 보안관리 기관을 명확히 지정해야 하며, 네트워크 데이터 보안관리 기관은 네트워크 데이터 보안 보호를 위해 다음과 같은 책임을 수행해야 함 - 보안 사고에 대한 네트워크 데이터 보안 관리 시스템 운영 절차 및 비상대응 계획 수립 - 네트워크 데이터 보안 위험 모니터링, 위험평가, 비상 훈련, 홍보, 교육 및 훈련과 같은 활동을 정기적으로 수행하고 네트워크 데이터 보안 위험 및 사고를 신속하게 처리 - 네트워크 데이터 보안 불만 사항 및 보고서를 수락하고 처리
중요 데이터 제공, 위탁, 공동 처리 시 위험평가	· 데이터의 처리자는 중요한 데이터 제공, 취급을 위탁 또는 공동으로 처리하기 전에 (법률상 규정된 의무 또는 의무이행인 경우를 제외하고) 다음 사항을 고려하여 위험평가를 실시해야 함 - 데이터의 제공, 위탁 처리, 공동 처리 및 수탁자의 처리 목적, 방법, 범위가 적법하며 필요한지 - 데이터의 변조, 파괴, 유출, 불법 획득과 사용, 국가안보와 공익, 개인과 조직이 합법적 권익에 미칠 위험 - 수탁자의 무결성과 법률 준수 상태 - 수탁자와 체결하거나 초안을 작성한 관련 계약의 네트워크 데이터 보안에 대한 요구사항이 수탁자의 네트워크 데이터 보안 보호 의무 이행을 효과적으로 구속할 수 있는지 여부 - 채택되거나 채택될 것을 제안하는 기술적 및 관리적 조치가 네트워크 데이터의 변경, 파괴 또는 유출, 불법 취득 또는 불법 사용과 같은 위험을 효과적으로 방지할 수 있는지 여부
위험평가 보고서 작성	· 중요 데이터 처리자는 매년 네트워크 데이터 처리 활동에 대한 위험평가를 시행하고 정부 당국에 보고서를 제출해야 하며, 다음과 같은 사항이 포함되어야 함 - 네트워크 데이터 처리자의 기본 정보, 네트워크 데이터 보안 관리기관에 대한 정보, 네트워크 데이터 보안 책임자의 이름 및 연락처 등 - 중요 데이터 처리 목적, 유형, 수량, 방법, 범위, 저장기간, 저장위치 - 데이터 보안 관리 시스템 및 암호화, 백업, 접근제어 등의 기술적 조치와 그 효과 - 발견된 보안 위험과 발생한 보안 사고 및 처리 - 중요 데이터 제공, 위탁 처리, 공동처리에 대한 위험평가 등의 내용을 포함

○ **(네트워크 데이터의 국외이전 보안 관리)** 네트워크 데이터 처리자는 다음 조건 중 하나가 충족되는 경우, 개인정보를 해외에 제공할 수 있음

구분	주요내용
네트워크 데이터(개인정보)의 국외이전 조건	· 네트워크 안전·정보화 당국의 데이터 국외이전 보안 평가 통과 · 네트워크 안전·정보화 당국의 규정에 따라 전문기관으로부터 개인정보보호 인증 취득 · 네트워크 안전·정보화 당국이 제정한 개인정보 국외이전에 관한 표준 계약 규정 준수 · 개인을 당사자로 하는 계약의 체결과 이행을 위해 개인정보의 해외 제공이 불가피한 경우 · 법률에 따라 제정된 노동 규정 및 단체 계약에 따라 국경 간 해외 인적 자원 관리를 위해 직원 개인정보의 해외 제공이 불가피한 경우 · 법적 의무 이행을 위해 개인정보의 해외 제공이 불가피한 경우 · 긴급 상황에서 자연인의 생명, 건강, 재산의 안전을 위해 개인정보의 해외 제공이 불가피한 경우 · 법률, 행정 법규, 국가 네트워크 당국에서 규정한 기타 조건

- 네트워크 데이터 처리자가 수집 및 생성한 중요 데이터를 해외에 제공할 경우, 당국이 주관하는 데이터 수출 보안 평가를 통과해야 함

○ **(네트워크 플랫폼 서비스 제공자의 의무)** 동 규정은 네트워크 데이터 보안을 위해 플랫폼 서비스 제공자에게 다음과 같은 의무를 부과

구분	주요내용
제3자 제품 및 서비스 제공자 관리	· 플랫폼 규칙이나 계약을 통해 플랫폼과 연결된 제3자 제품 및 서비스 제공자의 네트워크 데이터 보안 의무를 명확히 하고 네트워크 데이터 보안 관리 강화를 촉구
애플리케이션 검증	· 애플리케이션 배포 서비스를 제공할 경우, - 애플리케이션 검증 규칙을 제정하고 네트워크 데이터 보안 관련 검증을 실시 - 법률 또는 표준의 강제 요구사항에 부합하지 않으면 경고, 배포 금지나 중지, 종료 등의 조치를 시행
금지 활동	· 대규모 네트워크 플랫폼 서비스 제공자는 네트워크 데이터, 알고리즘, 플랫폼 규칙 등을 사용하여 다음과 같은 활동 금지 - 오해, 사기, 강압 등을 통해 플랫폼에서 사용자가 생성한 네트워크 데이터 처리 - 정당한 이유 없이 플랫폼에서 생성된 네트워크 데이터에 대한 사용자 접근 제한 - 사용자에 대한 불합리한 차별대우 및 사용자의 정당한 권익 훼손

■ 전망 및 시사점

○ 2021년 11월 처음 초안이 공개되어 2년 반 만에 제정된 「네트워크 데이터안전 관리조례」는 네트워크 데이터와 중요 데이터 등 주요 개념을 정의하고 네트워크 데이터 처리자와 네트워크 플랫폼 서비스 제공자의 법적 의무를 명확히 규정

○ 현지 언론들은 「네트워크 데이터안전 관리조례」의 통과로 사회 각계에서 데이터 보안의 중요성이 커지면서 관련 지출이 증가해 사이버보안 산업이 크게 성장할 것으로 예상

○ 이번 규정은 기존 데이터3법(「네트워크 안전법」, 「데이터안전법」, 「개인정보보호법」)을 보완하여 네트워크 데이터 보안 책임을 한층 명확히 규정한 만큼, 중국 기업들은 규정 준수를 위해 더욱 엄격한 보안 관행 수립에 나설 전망

Reference

▪https://www.gov.cn/zhengce/content/202409/content_6977766.htm
▪https://www.china-briefing.com/news/china-cybersecurity-regulations-what-do-the-new-regulations-say/
▪https://www.lexology.com/library/detail.aspx?g=4e1599ca-c4d3-4bef-96c0-025bbb5d5a18

해외 입법 동향

홍콩, 「주요기반시설(컴퓨터시스템) 보호법안」 제정 추진

홍콩 정부는 핵심기반시설의 컴퓨터 시스템 보안을 강화하기 위한 「주요기반시설(컴퓨터시스템) 보호법안」을 입법회에 제출하여 법제사법위원회의 검토 진행 중 (2024. 12. 11.)

■ 개요

○ 홍콩 정부는 핵심기반시설의 컴퓨터 시스템 보안을 강화하기 위한 「주요기반시설(컴퓨터시스템) 보호법안」을 입법회에 제출하여 법제사법위원회의 검토를 진행 중이며, 이는 현재 홍콩의 핵심기반시설 컴퓨터 시스템 보호를 위한 전담 법률이 부재한 상황에서 제안됨

○ 동 법안은 핵심기반시설 운영이 인터넷, 컴퓨터 시스템, 통신 인프라, 스마트 기기 등에 크게 의존하면서 증가하는 사이버 공격 취약성에 대응하기 위해, 핵심기반시설 운영자에게 컴퓨터 시스템 보호 의무를 부과하고 보안 위협·사고에 대한 조사·대응 체계를 구축하는 것을 주요 내용으로 함

■ 도입배경

○ 현재 홍콩의 핵심기반시설 컴퓨터 시스템 보호를 위한 전담 법률 부재

○ 보안국이 입법회에 제출한 법안설명자료(LegCo Brief[3]) 제2항에 따르면, 현대 핵심기반시설의 운영이 인터넷, 컴퓨터 시스템, 통신 인프라, 스마트 기기 등에 크게 의존하면서 사이버보안 위험 증가

○ 핵심기반시설에 대한 사이버 공격 발생 시 전체 사회에 심각한 결과를 초래할 수 있어 체계적인 보호체계 마련 시급

■ 주요내용

○ **(목적)** 홍콩 정부는 핵심기반시설의 컴퓨터 시스템에 대한 체계적인 보안 관리와 보호를 위해 포괄적인 법적 기반을 마련하고자 함

- (보안 기반 구축) 에너지, 정보기술, 금융, 교통, 의료, 통신 등 주요 8개 분야 핵심기반시설의 컴퓨터 시스템에 대한 보안을 강화하고 시설 운영에 필수적인 컴퓨터 시스템의 보안성을 확보하기 위한 법적 기반을 마련

3 Legislative Council Brief의 약자로, 홍콩 입법회(Legislative Council)에 제출되는 법안 설명자료를 의미

- (규제 대상) 핵심기반시설의 필수 서비스 제공과 관련된 모든 컴퓨터 시스템
- (보호 범위) 시스템 보안, 데이터 보호, 운영 연속성 등 포함

– (운영자 규제체계) 핵심기반시설 운영자에 대한 지정·관리 체계를 구축하고 보안관리계획 수립, 위험평가, 보안감사 등의 의무를 부과하며 사고 발생 시 신속한 보고 및 대응이 이루어질 수 있도록 규제체계를 확립

- (주요 의무) 보안관리계획 수립, 정기적 위험평가 및 감사 실시, 사고 발생 시 신속 보고
- (관리 체계) 컴퓨터 시스템 보안관리부서 설치 및 전문인력 확보 의무화

– (조사·대응체계) 감독관에게 보안 위협 및 사고에 대한 조사 권한을 부여하고 신속한 조사·대응을 위한 법적 근거를 마련하며 관련 정보의 체계적 수집·분석이 가능하도록 제도적 기반을 구축

- (감독 권한) 보안 위협 및 사고에 대한 조사, 시정 조치 명령 등
- (정보 관리) 보안 위협 및 사고 관련 정보의 체계적 수집·분석·공유

– (법적 제재 체계) 운영자의 법적 의무 위반에 대한 처벌 근거를 마련하고 위반 행위의 경중과 지속성에 따른 차등적 제재가 가능하도록 벌칙 체계를 도입

- (제재 범위) 의무 불이행, 허위보고, 조사 방해 등에 대한 처벌
- (제재 방식) 위반 행위의 성격과 지속성을 고려한 차등적 제재

○ **(규제당국 체계)** 핵심기반시설의 컴퓨터 시스템 보안을 위해 감독관을 중심으로 하고 분야별 지정 당국이 보완하는 규제체계를 구축함

– (감독관 지정) 행정장관은 핵심기반시설(컴퓨터 시스템 보안) 감독관(Commissioner)을 임명하여 전반적인 규제·감독 업무를 수행하도록 함

- (권한 범위) 핵심기반시설(Critical Infrastructure, 이하 CI)[4] 식별, 핵심기반시설 운영자(Critical Infrastructure Operator, 이하 CIO)[5] 지정, 주요 컴퓨터 시스템(Critical Computer System, 이하 CCS)[6] 지정, 실무지침 발행 등의 권한 보유

4 Type 1: Schedule 1에 명시된 8개 분야(에너지, 정보기술, 금융·은행 서비스, 항공 운송, 육상 운송, 해상 운송, 의료 서비스, 통신·방송 서비스)에서 필수 서비스의 지속적 제공에 필수적인 인프라
Type 2: 손상, 기능 상실 또는 데이터 유출이 홍콩의 중요한 사회적·경제적 활동의 유지를 저해할 수 있는 인프라

5 CI를 운영하는 조직으로서 감독관이 서면으로 지정한 운영자로, 하나의 CI에 복수의 CIO 지정 가능하고, 하나의 조직이 복수의 CI에 대한 CIO로 지정 가능

6 CI의 핵심기능에 필수적이며 운영자가 홍콩 내외에서 접근 가능한 컴퓨터 시스템으로, 규제당국이 CI 운영자에게 서면으로 지정

- (지정 당국) Schedule 2에 따라 홍콩 금융관리국(Hong Kong Monetary Authority, HKMA)과 통신관리국을 각 분야의 지정 당국으로 규정

  • (소관 분야) 금융관리국은 은행·금융 서비스 분야, 통신관리국은 통신·방송 분야 담당

- (주요 기능) 규제당국은 다음의 핵심 기능을 수행

  • (규제 권한) CI 식별, CIO 지정, CCS 지정

  • (지침 발행) 법령 이행을 위한 실무지침(Code of Practice) 발행

○ **(핵심기반시설 식별 및 운영자 지정)** 법안의 제3장은 사이버보안 보호 대상인 핵심기반시설과 그 운영자 지정에 관한 세부 기준을 규정함

- (핵심기반시설 범위) 규제당국은 다음과 같이 CI 여부를 판단

  • (Type 1 CI) Schedule 1에 명시된 에너지, 정보기술, 금융·은행 서비스, 항공·육상·해상 운송, 의료 서비스, 통신·방송 서비스 등 8개 필수 분야에서 해당 서비스의 지속적 제공에 필수적인 인프라를 지정

  • (Type 2 CI) 인프라의 손상, 기능 상실 또는 데이터 유출이 홍콩의 중요한 사회적·경제적 활동의 유지를 저해하거나 실질적으로 영향을 미칠 수 있는 인프라를 지정

  • (판단 기준) 인프라가 제공하는 서비스의 성격 및 해당 인프라 손상 시 발생할 수 있는 파급효과를 종합적으로 고려하여 결정

- (핵심기반시설 운영자 지정) 감독관은 다음 기준을 고려하여 CI 운영 조직을 CIO로 지정

  • (지정 기준) CI의 핵심기능이 컴퓨터 시스템에 의존하는 정도, 조직이 관리하는 디지털 데이터의 민감도, 조직의 인프라 운영·관리에 대한 통제 범위를 고려하여 지정

  • (지정 방식) 서면 통지로 지정하며, 하나의 CI에 복수의 CIO 지정 가능하고 하나의 조직이 복수의 CI에 대한 CIO로 지정될 수 있음

- (주요 컴퓨터 시스템 지정) 규제당국은 다음 기준에 따라 CCS를 지정

  • (지정 요건) 운영자가 홍콩 내외에서 접근 가능하고 CI의 핵심기능에 필수적인 시스템을 대상으로 함

  • (고려사항) 시스템의 CI 핵심기능 관련 역할, 시스템 중단 시 핵심기능에 대한 영향, 타 컴퓨터 시스템과의 연관성을 종합적으로 검토

- (정보제공 의무) 규제당국의 다음 업무 수행을 위한 정보제공 의무 규정

  • (요구 범위) CI 식별(제14조), CIO 지정(제15조), CCS 지정(제16조), CI의 컴퓨터 시스템 이해(제17조)를 위해 규제당국이 합리적으로 필요하다고 판단하는 정보

  • (위반 제재) 정보제공 의무 위반 시(제18조) 약식재판에서 최대 HK$300만(비운영자 HK$30민) 및 위반 지속 시 일 HK$6민(비운영자 HK$3만), 기소재판에서 최대 HK$500만(비운영자 HK$50만) 및 위반 지속 시 일 HK$10만(비운영자 HK$50만)의 벌금 부과

○ **(핵심기반시설 운영자의 의무)** CI의 컴퓨터 시스템 보안을 위해 운영자가 준수해야 할 의무사항을 3개 범주로 구분하여 규정함

- (조직 관련 의무) CIO는 컴퓨터 시스템 보안을 위한 조직 체계를 다음과 같이 구축·운영해야 함

  • (보안 조직) 전문지식을 갖춘 직원을 감독자로 하는 컴퓨터 시스템 보안관리부서를 설치하고, 이를 통해 조직의 사이버보안 업무를 총괄

  • (변경 관리) 조직 변경으로 인한 보안 공백 방지를 위해 인프라 운영 조직 변경 시 규제당국에 통지

- (보안 예방 의무) CIO는 컴퓨터 시스템의 보안 위협 예방을 위해 다음 의무를 이행해야 함

  • (시스템 변경관리) CI의 핵심기능에 필수적인 컴퓨터 시스템 변경 시 보안 영향을 검토하여 1개월 내 통지

  • (보안 체계 구축) CIO 지정 후 3개월 내 Schedule 3에 따른 컴퓨터 시스템 보안관리계획 수립

  • (주기적 점검) Schedule 4에 따라 12개월마다 보안위험평가, Schedule 5에 따라 24개월마다 보안감사 실시

- (사고 대응 의무) CIO는 컴퓨터 시스템 보안사고 발생에 대비하여 다음 사항을 이행해야 함

  • (대응 태세) 감독관 주관 보안 훈련 참여 및 Schedule 3 Part 2에 따른 비상대응계획 수립

  • (사고 보고) Schedule 6에 따라 보안사고 발생 시 신속 통지(중대사고 12시간 내/경미사고 24시간 내) 및 14일 내 상세 보고서 제출

○ **(보안 조사 권한)** 컴퓨터 시스템 보안 위협 및 사고에 대한 조사 권한을 규정함

- (조사 체계) 감독관은 다음과 같이 보안 위협·사고에 대한 조사를 수행함

  • (조사 개시) CI의 주요 컴퓨터 시스템에 대한 보안 위협이나 사고가 의심되는 경우 사전 통지 없이 선제적 조사 가능

- (조사 범위) 사고의 원인 규명, 보안 위협의 식별 및 대응 조치 등 포함

– (조사 권한) 조사관은 다음의 권한을 행사할 수 있음

- (자료 확보) 컴퓨터 시스템 보안 관련 문서 제출 요구 및 설명 요청
- (현장 접근) 영장을 통해 시설 출입, 전자기기 접근·조사 가능
- (긴급 조치) 보안 위협 해소를 위해 필요시 시스템 사용중지 명령 등 가능

○ **(이의신청)** 컴퓨터 시스템 보안 관련 규제당국의 결정에 대한 이의신청 절차를 규정함

– (이의신청 체계) 규제당국의 결정에 대한 불복 절차를 다음과 같이 규정

- (신청 대상) 핵심기반시설, 운영자 지정, 보안 조치 명령 등 규제당국의 결정에 불복하는 조직의 이의신청 허용
- (결정 효력) 이의신청위원회의 결정으로 최종 확정되며, 결정 내용의 확인·변경·취소 가능
- (세부 절차) Schedule 7에서 이의신청 방법, 처리 기한 등 구체적 절차 규정

○ **(기타 사항)** 컴퓨터 시스템 보안 규제의 효율적 운영을 위한 보충 규정을 둠

– (행정 조치) 규제의 탄력적 운영을 위한 다음의 권한 부여

- (의무 면제) 감독관은 서면통지로 CIO의 보안 관련 의무 면제 가능(입법회 심사 불요)
- (제보자 보호) 컴퓨터 시스템 보안 위협·사고 관련 조사를 위한 정보 제공자 보호

– (법령 정비) 장관에게 다음의 권한 부여

- (규칙 제정) 컴퓨터 시스템 보안 관련 하위 규칙 제정 가능
- (제도 개선) Schedule 개정을 통한 세부 규정 정비 가능
- (입법 통제) 상기 권한 행사 시 입법회 거부절차 적용

■ 전망 및 시사점

○ 홍콩의 「주요기반시설(컴퓨터시스템) 보호법안」은 에너지, 금융, 교통, 의료 등 주요 8개 분야의 핵심기반시설에 대한 체계적인 사이버보안 규제를 도입하는 것으로, 감독관과 분야별 지정 당국을 통한 이원화된 규제체계 구축과 함께 운영자에 대한 구체적 의무 부과를 통해 규제의 실효성을 확보하고자 함

○ 법안은 핵심기반시설 운영자에게 보안관리부서 설치, 정기적 위험평가 및 감사 실시, 사고 발생 시 신속 보고 등 포괄적인 의무를 부과하면서도, "적절한 전문지식" 등 주요 용어의 구체적 기준이 미비하고 제3자 서비스 제공자의 책임 범위가 불명확한 점은 시행 전 보완이 필요한 과제로 지적됨

○ 2024년 말 입법회에 제출된 본 법안은 2026년 초 시행이 예상되며, 그전까지 실무지침 마련, 불명확한 기준의 구체화, 전문인력 확보 방안 등이 해결과제로 남아있으나, 핵심기반시설의 사이버보안 보호가 시급한 과제라는 점에서 법안의 기본 방향성은 유지될 것으로 전망됨

Reference

▪https://www.info.gov.hk/gia/general/202412/04/P2024120400297.htm
▪https://www.gld.gov.hk/egazette/english/gazette/file.php?year=2024&vol=28&no=49&extra=0&type=3&number=30

캐나다

해외 입법 동향

캐나다 하원, 통신시스템 및 주요기반시설 보안을 위한 「사이버보안에 관한 법률(안)」 본회의 회부

캐나다 하원 공공안전 및 국가안보 상임위원회[1]는 통신시스템 및 국가 주요 산업 부문의 사이버보안 체계 강화를 위한 「사이버보안에 관한 법률(안)[2]」을 의결하고, 법안을 하원 본회의로 회부 (2024. 4. 19.)

■ 개요

○ 「사이버보안에 관한 법률(안)」은 2022년 6월 연방정부가 제출한 법안으로, ① 통신시스템 보안 강화를 위한 「통신법[3]」 개정안, ② 주요기반시설 운영기업에게 사이버보안 의무를 부과하는 「주요 사이버 시스템 보호법[4]」 제정안으로 구성됨[5]

■ 주요내용 (※ 최초 정부 제출안 대비 상임위원회 심의 과정에서 추가되거나 수정된 항목은 밑줄 표기[6])

① 「통신법」 개정법률안

○ **(개요)** 캐나다의 통신시스템 보안을 강화하기 위한 연방정부의 명령권 등 규제 권한을 확대하는 한편, 무분별한 권한 행사를 방지하기 위해 구체적인 요건 마련

- 총독(Governor in Council) 및 산업부 장관(Minister of Industry)은 일정 요건을 충족한 경우 합리적인 범위 내에서 통신서비스제공자에게 통신 네트워크 및 통신 시설 관련 제품·서비스의 사용 금지·제거 명령을 내릴 수 있으며, 불이행 시 행정벌금 부과 및 형사처벌 가능

○ **(명령 권한)** 총독과 산업부장관은 간섭(interference), 조작(manipulation), 중단(disruption) 또는 성능 저하(degradation) 등을 포함한 모든 위협으로부터 캐나다의 통신시스템을 안전하게 보호하기 위해 합리적인 근거(reasonable grounds)에 따라 명령을 할 수 있음(제15.1조, 제15.2조 신설)

1 House of Commons Standing Committee on Public Safety and National Security
2 An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts (BILL C-26)
3 Telecommunications Act (1993, c. 38)
4 Critical Cyber Systems Protection Act
5 캐나다 입법은 하원에서 3차 독회, 상원에서 3차 독회를 모두 거쳐야 완료되는데, 「사이버보안에 관한 법률(안)」의 경우 하원 2차 독회까지 이루어진 상황이며 향후 하원 본회의 통과 및 상원 절차가 남음
6 최초 정부 제출안에 관한 자세한 사항은 [2022년 6월] 인터넷·정보보호 법제동향 제177호 참고

- 통신서비스제공자를 대상으로 특정인이 제공하는 모든 제품에 대해 통신 네트워크·시설 또는 해당 네트워크 또는 시설의 일부에서 제거하도록 지시 등 조치 명령 가능

〈총독 및 산업부 장관의 조치 명령〉

구분		명령	주요 내용
총독 (Governor in Council)		금지	· 통신서비스제공자가 특정인이 제공하는 통신 네트워크 및 시설 관련 제품 및 서비스 사용을 금지하도록 명령할 수 있음
		제거	· 통신서비스제공자가 특정인이 제공하는 통신 네트워크 및 시설 관련 제품 및 서비스를 제거하도록 명령할 수 있음
산업부 장관 (Minister of Industry)	공공안전 비상대비부 장관 협의	금지	· 통신서비스제공자가 특정인에게 통신 네트워크 및 시설 관련 서비스 제공을 금지하도록 명령할 수 있음
		중단	· 통신서비스제공자가 특정인에게 통신 네트워크 및 시설 관련 서비스 제공을 일정 기간 중단하도록 명령할 수 있음
	단독	기타	· 통신 네트워크 및 시설 관련 제품 및 서비스 사용금지·제거 명령 · 통신 네트워크 및 시설 관련 제품 및 서비스 사용·제공에 조건 부과 명령 · 통신 네트워크 및 시설 관련 제품 및 서비스 계약금지·해지 명령 · 통신 네트워크 및 시설 관련 보안 계획 개발·평가 관련 명령

○ **(명령 부과의 요건)** 총독 또는 산업부장관은 명령 전, ▲영향을 받게 되는 통신서비스제공자의 운영 및 재정적 파급력 ▲캐나다의 전기통신서비스에 미치는 효과 ▲기타 산업부 장관이 관련이 있다고 판단하는 요소 등을 반드시 고려해야 함

- 또한 명령의 범위와 내용은 간섭, 조작, 중단 또는 성능 저하와 같은 위협의 심각성에 비추어 반드시 합리적이어야 함

○ **(산업부장관의 보고의무)** 산업부장관은 명령권을 행사하는 경우, 관련내용에 대해 의회에 보고하거나 유관기관에 통보해야 함

- (의회 보고) 산업부장관은 매 회계연도 종료 후 3개월 이내에 상·하원에 상기 명령에 대한 보고서 제출

  · (의회 보고서의 내용) ▲명령 건수 및 성격, ▲명령의 영향을 받은 통신서비스제공자의 수, ▲해당 명령을 전체 또는 일부 준수한 통신사업자의 준수사항과 관련한 설명, ▲명령의 필요성, 비례성, 합리성 및 유용성에 대한 설명 등 (제15.21조 신설)

○ **(제재)** 통신서비스제공자가 총독과 산업부장관의 명령(제15.1조, 제15.2조)을 위반할 경우, 매일 최대 1,000만 캐나다 달러(약 100억 원) 부과 (제72.131조 신설)

- 동일 위반이 재차 발생한 경우 매일 최대 1,500만 캐나다 달러(약 150억 원)의 행정벌금을 부과할 수 있으며, 위반이 계속될 경우에는 날짜별로 별도의 위반이 발생한 것으로 간주

- 총독과 산업부장관의 명령(제15.1조, 제15.2조) 위반 시 약식기소(Summary Conviction)에 따라 처벌받을 수 있는 범죄로 취급하여, 개인(individual)의 경우 2년 이하의 징역 또는/및 법원(corporation)의 재량에 따른 벌금, 법인의 경우 법원의 재량에 따른 벌금이 부과됨 (제73조제3.1항 신설)

②「주요 사이버 시스템 보호법」 제정법률안

○ **(개요)** 금융, 통신, 에너지 및 운송 분야 등 주요기반시설을 운영하는 기업의 주요 사이버 시스템을 보호하기 위한 사이버보안 의무를 부과

- 주요 사이버시스템과 연관된 사이버보안 위험을 식별·관리함으로써 필수 서비스 등의 보안을 강화하고, 사이버보안 사고를 감지하여 주요 사이버시스템의 손상을 방지하는 것을 목적으로 함

○ **(주요 용어)** 동 법안은 주요 용어를 다음과 같이 정의 (제2조)

구분	주요 내용
지정 운영자 (Designated operator)	• 총독이 추후 권한 행사를 통해 동법의 적용대상으로 지정하는 모든 유형의 개인, 파트너십, 비법인단체
주요 사이버 시스템 (Critical cyber system)	• 기밀성, 무결성 또는 가용성이 손상될 경우 필수 서비스 또는 시스템의 연속성 또는 보안에 영향을 미칠 수 있는 사이버 시스템
사이버 시스템 (Cyber system)	• 정보의 수신, 전송, 처리 또는 저장을 위한 기반을 형성하는 상호 의존적 디지털 서비스, 기술, 자산 또는 시설 등의 시스템
사이버보안 사고 (Cyber security incident)	• 필수 서비스 또는 시스템의 연속성 또는 보안, 주요 사이버 시스템의 기밀성, 무결성 또는 가용성 등을 방해하거나 방해할 가능성이 있는 작위, 부작위, 정황 등을 포함한 사고
규제기관 (Regulator)	• ▲산업부 (Ministry of Industry) ▲교통부(Ministry of Transport) ▲금융감독청 (Office of the Superintendent of Financial Institutions) ▲중앙은행(Bank of Canada) ▲ 에너지 규제청 (Canada Energy Regulator) ▲원자력 안전위원회(Canadian Nuclear Safety Commission)

○ **(적용대상)** 동 법안은 ▲통신 서비스 ▲지역 간 또는 국제 파이프라인 및 전력선 시스템 ▲원자력 시스템 ▲연방 교통 시스템 ▲은행 및 금융 시스템 등 필수 서비스 및 필수 시스템 (Vital Services and Vital Systems) 부문에서 비즈니스를 수행하는 운영자를 대상으로 함 (제6조 및 제7조, 별표1 및 별표2)

- 각 필수 서비스 및 시스템 부문에 대한 규제기관은 다음과 같음

구분	규제기관
통신 서비스	• 산업부 (Ministry of Industry)
지역 간 또는 국제 파이프라인 및 전력선 시스템	• 캐나다 에너지 규제청 (Canada Energy Regulator, CER)
원자력 시스템	• 캐나다 원자력 안전위원회 (Canadian Nuclear Safety Commission, CNSC)
연방 교통 시스템	• 교통부 (Ministry of Transport)
은행 시스템	• 캐나다 금융감독청 (Office of the Superintendent of Financial Institutions, OSFI)
청산 및 결제 시스템	• 캐나다 중앙은행 (Bank of Canada, BOC)

- 총독은 추후 국가안보 또는 공공안전을 위한 필수 시스템·서비스 및 관련 운영자를 신규 추가, 수정 또는 삭제함으로써 동법의 적용 대상을 조정할 수 있음

○ **(사이버보안 프로그램)** 지정 운영자는 지정된 날로부터 90일 이내에 ▲사이버보안 위험 파악 및 관리 ▲주요 사이버 시스템의 손상 방지 ▲사이버보안 사고 탐지 및 사고로 인한 영향 최소화 등의 내용을 담은 사이버보안 프로그램을 수립하고, 해당 프로그램을 구현 및 유지해야 함 (제9조 및 제12조)

○ **(사이버보안 사고 보고)** 지정 운영자는 주요 사이버 시스템과 관련된 사이버보안 사고를 하위규정에서 정한 기간 내에(다만, 이는 72시간을 초과할 수 없음) 통신보안국[7](Communications Security Establishment, CSE)에 보고해야 하며, 사고 보고 직후 해당 보고 사실을 자신의 적절한 규제당국에 알려야 함 (제17조 및 제18조)

○ **(보호조치 지시명령)** 총독은 명령을 내리는 것이 필요하다고 합리적인 이유로 믿는 경우 지정 운영자에게 주요 사이버시스템을 보호할 목적의 모든 조치를 따르도록 지시 명령할 수 있음 (제20조, 제21조)

· 지시 명령에는 ▲지정 운영자 또는 운영자 집단의 이름 ▲운영자가 취해야 할 조치, ▲조치가 이루어져야 하는 기간 등이 명시되어야 함

· 총독은 지시 명령 전, ▲영향을 받게 되는 통신서비스제공자의 운영 및 재정적 파급력 ▲캐나다의 통신 서비스에 미치는 효과 ▲기타 총독이 관련 있다고 판단하는 요소 등에 대해 반드시 고려해야 함

· 또한, 공공안전비상대비부 장관은 총독이 명령을 내린 후 90일 이내에 국가안보정보위원회와 국가안전정보심사국에 해당 사실을 통보해야 함

· 명령을 받는 모든 운영자는 총독의 명령을 준수하고 해당 명령을 받은 사실 및 그 내용에 관해 기밀을 유지해야 함 (제24조)

○ **(기록 보관의무)** 각 지정 운영자는 ▲사이버보안 프로그램 구현을 위한 조치 ▲사이버사고 보고 사실 ▲ 공급망 또는 제3자가 제공하는 제품 및 서비스의 위험을 최소화하기 위한 조치 ▲총독의 사이버보안 지시 명령 사항을 이행하기 위한 조치 등에 관한 기록을 보관해야 함 (제30조)

○ **(정부의 기밀 취급 및 제한사항)** 지정 운영자에 대한 사이버보안 명령의 발행, 수정 또는 취소와 관련해 공공안전비상대비부 장관, 관련 규제기관, 통신보안국, 안보정보청(Canadian Security Intelligence Service) 등은 상호 간 기밀 정보를 수집·공유할 수 있으며, 수집·공유되는 모든 정보는 기밀로 취급되어야 함 (제23조)

- 수집·공유되는 정보의 보유 기간은 명령의 발행, 수정 또는 취소, 명령의 이행 여부 확인 또는 불이행 방지를 위해 필요한 범위 내로 제한되어야 하며, 해당 운영자에게는 정보 보유 기간을 반드시 통지해야 함

7 캐나다 국방부 산하의 정보기관으로, ▲캐나다 정부의 네트워크 방어 ▲주요 기반시설 운영자에 대한 조언 및 지원 ▲캐나다 국민의 온라인 보안을 대상으로 한 조언 제공 ▲해외 정보 수집 ▲사이버 작전 수행 ▲연방 기관 지원 등의 역할을 수행

○ **(제재)** 지정 운영자는 위반 사항에 따라 행정벌금 혹은 형사처벌을 받을 수 있음

구분	개인		법인	비고
행정벌금 (Administrative Monetary Penalty)	· 매일 최대 100만 캐나다 달러		· 매일 최대 1,500만 캐나다 달러	사이버보안 프로그램 수립 및 구현 의무, 사이버보안 사고보고 의무, 기록보관 의무, 사이버보안 지시명령 의무 위반 시
약식기소 (Summary Conviction)	· 2년 이하의 징역 · 법원 재량에 따른 벌금	병과 가능	· 법원 재량에 따른 벌금	
정식기소 (Conviction)	· 5년 이하의 징역 · 법원 재량에 따른 벌금	병과 가능	· 법원 재량에 따른 벌금	사이버보안 프로그램 수립 및 구현 의무, 지시명령 위반 시

■ 전망 및 시사점

○ 「사이버보안에 관한 법률(안)」은 하원 상임위원회를 통과하면서 당초 정부가 제출한 원안 대비 연방정부의 광범위한 권한 행사를 통제할 수 있는 여러 요건이 추가된 것이 특징적임

- 본 법안은 캐나다 정부가 2022년 6월 하원 의회에 제출한 후 약 2년 만에 하원 상임위원회를 통과하였으며, 이후 하원 본회의를 거쳐 상원 의회로 회부될 예정

○ 한편, 「주요 사이버 시스템 보호법」 제정법률안의 경우 특정 조항을 원안대비 보다 명확히 규정함으로써 향후 야기될 수 있는 법적 모호성을 최소화하고자 함

- 수정안은 사이버사고 보고 시점을 '즉시(immediately)'에서 '최대 72시간'으로 특정하는 한편 하위규정을 통해 사이버보안 사고의 시급성에 따라 보고 시한을 변경할 수 있도록 함

○ 다만, 수정안은 고위험 공급업체 등을 구체적으로 명시하지 않아 정부가 규제 권한을 행사할 수 있는 범위를 과도하게 확대할 여지가 있음

- 이와 관련, 정부가 특정 국가에서 제조된 장비 또는 서비스에 대해 강력한 통제력을 행사할 가능성이 있다는 비판적 의견 존재

Reference

▪https://www.parl.ca/DocumentViewer/en/44-1/bill/C-26/second-reading
▪https://voi.id/kr/technology/179160
▪https://www.itworldcanada.com/sponsored/the-bill-c-26-regulation-and-its-implications-for-the-critical-infrastructures-cybersecurity-in-canada
▪https://gowlingwlg.com/en/insights-resources/articles/2022/bill-c-26-rights-groups-oppose-infrastructure-law/

호 주

해외 입법 동향

호주, ‘사이버보안 입법패키지’ 최종 승인

호주는 공공 및 민간부문 전반에 걸쳐 사이버보안을 강화하기 위하여 「사이버보안법 2024」 제정 및 기존 「주요기반시설보호법 2018」, 「정보서비스법 2001」 등을 개정하는 ‘사이버보안 입법패키지’를 최종 승인 (2024. 11. 29)[1]

■ 개요

○ 호주 정부는 ‘2023-2030 호주 사이버보안 전략’[2]의 일환으로서, 국제 모범사례에 부합하는 법적 체계의 구축 및 사이버보안 분야 글로벌 리더십 강화를 위하여 사이버보안 분야 입법체계 개선을 강조

- 이에, 지능화·고도화되고 있는 디지털 변화에 따라 주요 사이버 공격에 대한 정부의 대응력 향상 및 보안사고 예방 및 대응 시스템을 구축하기 위하여 「사이버보안법 2024」을 제정하고, 기존 「주요기반시설보호법 2018」, 「정보서비스법 2001」 등을 개정하는 ‘사이버보안 입법패키지’를 마련

〈 (참고) 2023-2030 호주 사이버보안 전략 〉

전략 목표	액션 플랜
강력한 기업과 시민 (Strong businesses and citizens)	• 중소기업의 사이버보안 강화 지원 • 호주인들이 사이버 위협으로부터 스스로를 방어할 수 있도록 지원 • 사이버 위협 행위자가 호주를 공격하는 것을 차단 및 억제 • 랜섬웨어 비즈니스 모델을 파괴하기 위해 업계와 협력 • 기업을 위한 명확한 사이버 지침 제공 • 사이버사고 발생 시 호주 기업이 컨설팅 등 용이하게 이용할 수 있도록 지원 • 신원을 보호하고 신원 도용 피해자에게 보다 효과적인 지원을 제공
안전한 기술 (Safe technology)	• 호주인들이 디지털 제품과 소프트웨어를 신뢰할 수 있도록 보장 • 가장 중요한 데이터셋 보호 • 신흥 기술의 안전한 사용 촉진
세계적 수준의 위협 공유 및 차단 (World-class threat sharing and blocking)	• 경제 전반의 위협 인텔리전스 네트워크 구축 • 사이버 공격 차단을 위한 위협 차단 기능의 확장

1 호주 정부는 ‘사이버보안 입법패키지’를 연방의회에 제출(2024. 10. 9)하였고, 입법 최종단계인 왕실 재가(Royal Assent)를 통해서 최종 승인(2024. 11. 29) 되었음

2 2023-2030 Australian Cyber Security Strategy, 2023.11.22. 발표 (https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy)

전략 목표	액션 플랜
주요기반시설 보호 (Protected critical infrastructure)	• 주요기반시설 규정의 범위 명확화 • 주요기반시설에 대한 사이버보안 의무 및 규정 준수 강화 • 연방 정부의 사이버보안 강화 • 취약점 식별을 위하여 주요기반시설에 대한 압력 테스트(Pressure-test)
주도권 역량 강화 (Sovereign capabilities)	• 국가 사이버 인력의 성장 및 전문화 • 현지(local) 사이버 산업, 연구 및 혁신 가속화
지역 및 글로벌 리더십 회복 (Resilient region and global leadership)	• 사이버 회복력 있는 지역을 파트너로서 선택 및 지원 • 국제 사이버 규칙, 규범 및 표준을 형성, 유지 및 방어

■ 주요내용

① 「사이버보안법 2024」 제정

▲인터넷에 직·간접적으로 연결 가능한 **'스마트 기기**(관련연결가능제품, Relevant connectable product)'**에 대한 보안 표준 준수, ▲랜섬웨어 대금 지급 보고 의무화, ▲국가사이버보안조정관 중심**의 중대한 사이버보안 사고 대응 체계 구축, ▲특정 사이버보안 사고에 대한 검토를 통해 향후 유사한 성격의 사고를 예방·탐지·대응하고 사고 영향을 최소화하기 위한 독립적인 **사이버사고검토위원회 설립, ▲기업 정보의 사용 및 공개 제한** 등을 규정

○ **(정의)** 본 법은 주요용어를 다음과 같이 정의함

용어	정의
호주 신호정보국(ASD) (Australian Signals Directorate)	• 호주의 사이버보안과 정보 수집을 담당하는 정보기관
연방기관 (Commonwealth body)	• 연방정부의 장관 및 부처 • 연방법에 따라 공공목적으로 설립/유지되는 기관(법인 여부 무관)으로 왕실 당국이 아닌 기관
연방 집행기관 (Commonwealth enforcement body)	• 연방경찰(AFP), 금융감독원(APRA), 증권투자위원회(ASIC), 국가반부패위원회 감찰관, 검찰청, 국가반부패위원장, 스포츠청렴위원회, 형사 처벌 관련 법률 집행 권한이 있는 기타 연방기관
사이버보안 사고 (Cyber security incident)	• (제9조) 「주요기반시설보안법 2018」에서 정의하는 사이버보안 사고나 컴퓨터와의 전자통신 무단 침입을 포함하는 사건을 의미하나, 본 법상 사이버보안 사고는 ▲주요기반시설 자산이 포함되거나 ▲헌법 제51조에 적용되는 기업상 단체 활동의 포함, 또는 ▲텔레그래픽, 전화, 헌법 제51조(v)의 범위 내 기타 서비스 수단에 영향을 받거나 컴퓨터의 연결 기능 등이 손상 또는 방해받는 경우, ▲호주와 국민의 사회·경제적 안정성, 국방, 국가안보 등에 심각한 손상을 야기하는 경우 등의 사고를 의미
허가된 사이버보안 목적 (Permitted cyber security purpose)	• (제10조) ▲연방/주 기관, 국가사이버보안조정관이 사이버보안 사고를 대응/완화/해결하는 기능 수행, ▲연방 장관들에게 사이버보안 사고에 관한 정보를 제공하고 자문, ▲호주와 국민의 사회·경제적 안정성, 국방, 국가안보에 대한 심각한 위협을 예방 및 완화, ▲주요기반시설자산에 대한 중대한 위험 예방 및 완화, ▲정보기관과 연방집행기관이 각자의 기능을 수행하는 경우를 뜻함
정보기관 (Intelligence agency)	• 호주범죄정보위원회. 호주지리공간정보기구. 호주비밀정보국, 호주보안정보기구, 호주 신호정보국(ASD), 국방정보기구, 국가정보국

용어	정의
국가사이버보안조정관 (National Cyber Security Coordinator)	• 부처의 국가사이버보안조정관 • 해당 관의 기능/권한 수행 관련 지원하는 공무원/연방기관 직원
관련연결가능제품 (Relevant connectable product)	• (제13조제2항) 인터넷연결가능제품 또는 네트워크연결가능제품
인터넷연결가능제품 (Internet-connectable product)	• (제13조제4항) 인터넷 프로토콜 스위트의 일부인 통신 프로토콜을 사용하여 인터넷을 통해 데이터를 송수신할 수 있는 제품
네트워크연결가능제품 (Network-connectable product)	• (제13조제5항) ▲전기적/전자기적 에너지로 데이터 송수신이 가능하며, ▲인터넷 연결가능제품이 아니며, ▲ 인터넷연결가능 제품과 직접 연결 가능하거나, 동시에 2개 이상 제품과 연결 가능하고 인터넷 연결 가능 제품과도 직접 연결이 가능한 것으로 이 중 하나를 충족하는 것
랜섬웨어 지불 (Ransomware payment)	• (제26조제1항) 사이버보안 사고가 발생/진행/임박하여 보고 대상 사업체에 직간접적 영향이 있고, 갈취 주체의 요구에 따른 랜섬웨어 지불이 이루어지거나 이를 인지한 경우
보고대상 사업체 (Reporting business entity)	• (제26조제2항) 랜섬웨어 지불 당시 연간 매출이 기준치를 초과하는 호주 내 사업체(연방/주 기관, 주요기반시설 책임 실체 제외)이거나, 주요기반시설보안법 2018 Part 2B가 적용되는 주요기반시설의 책임 실체를 의미
랜섬웨어 지불 보고서 (Ransomware payment report)	• (제27조제1항) 보고 대상 사업체가 랜섬웨어를 지불하거나 지불 사실을 인지한 시점으로부터 72시간 이내에 지정된 연방기관에 랜섬웨어 지불 보고서를 제출
중대한 사이버보안 사고 (Significant cyber security incident)	• (제34조) 호주의 사회·경제적 안정/국방/국가안보에 중대한 위험을 초래하거나 호주 국민에게 심각한 우려가 되는 사이버보안 사고를 의미
단체 (Entity)	• 개인, 법인, 파트너십, 의사결정 기구가 있는 비법인 단체, 신탁, 주요기반시설 자산의 책임 실체
사이버사고검토위원회 (Cyber Incident Review Board)	• 제60조에 따라 설립된 위원회로서, 사이버보안 사고를 검토하고 평가하는 독립 기구

○ **(스마트 기기 보안 표준)** 특정 상황에서 호주가 획득한(acquried) 인터넷에 직간접적으로 연결 가능한 스마트 기기('관련연결가능제품')에 대해 보안 표준을 수립해야 함

- 이에, 제조업체 및 공급업체는 보안 표준을 준수한 관련연결가능제품을 제조 및 공급해야함

· 해당 제조업체는 보안 표준의 제품과 관련된 기타 의무(예: 제품에 대한 정보 게시 의무)를 준수할 필요가 있으며, 해당 공급업체는 컴플라이언스 설명서와 함께 호주에서 제품을 공급해야 함

구분	주요내용
관련연결제품의 보안 표준 준수	▪ (제조업체) 관련연결가능제품이 해당 보안 표준을 준수하도록 해야 하고, 위반 시 민사 처벌 대상이 될 수 있음 ▪ (공급업체) 보안 표준을 준수하는 제품만 공급해야 하고, 위반 시 민사 처벌 대상이 될 수 있음
컴플라이언스 설명서가 있는 제품의 제공 및 공급 의무	▪ (제조업체) 호주 내 제품 공급을 위하여 ▲제품이 해당 클라스에 포함되거나 ▲기업이 호주에서 해당 제품이 인수될 것임을 합리적으로 예상가능한 경우 보안 표준을 준수해야 하며, 공급하는 제품에 대한 컴플라이언스 설명서를 제공해야 함 ▪ (공급업체) 컴플라이언스 설명서와 함께 제품을 공급해야 함 ※ 제조업체와 공급업체 모두 컴플라이언스 설명서 보관 의무 존재

- 한편, 장관(Secretary)은 관련연결제품 보안 표준 준수 대상자 또는 컴플라이언스 설명서가 있는 제품을 제공 및 공급해야 하는 자가 해당 사항을 준수하지 않을 경우 '규정 준수 고지(Compliance notice) → 중지(Stop) 고지 → 리콜 고지 → 공개 고시' 등 단계적 조치를 취할 수 있음

- 다만, 장관이 해당 고지를 통해 시정요청을 했음에도 불구하고 이를 이행하지 않는 경우, 서면 통지를 통해 제품 제공 및 공급을 취소할 수 있음 (취소 시 다음 단계의 고지 이행은 불필요)

① 규정 준수 고지 (Compliance notice)	② 중지 고지 (Stop notice)	③ 리콜 고지 (Recall notice)	④ 리콜 고지 미준수 시 공개 고시
·스마트기기 보안표준 준수 대상자 등이 해당 의무를 미준수하거나 가능성이 있는 경우, 이를 준수하도록 '기업명, 미준수 사항, 구체적인 해결 조치 등'의 규정 준수를 고지함 ▶	·규정 준수를 고시받은 대상자가 이를 미이행하거나 시정조치가 불충분한 경우 1회에 한하여 중지 고지 실시 ▶	·중지 고지를 받았음에도, 이를 미이행하거나 시정조치가 불충분한 경우 1회에 한하여 '규정위반 사항, 호주에서 해당 제품을 공급할 수 없도록 하는 등의 조치를 고지 ▶	장관은 '리콜 고지를 받았음에도 해당 기업이 이를 미준수한 경우 ▲부처 웹사이트 등에 정보 (해당 기업의 신원, 제품 상세 정보, 의무 위반 사항 등) 공개 가능

※ (중지/리콜 고지 前) 장관은 대상 기업에 해당 고지를 할 의사가 있음을 알리고, 최소10일간 기업이 이를 해명할 수 있도록 함

○ **(랜섬웨어 보고 의무)** 통신 서비스 공격, 컴퓨터 연결 저해, 국가안보을 위협하는 사이버보안 사고로 인한 랜섬웨어 대금을 직접 지불했거나 특정 단체(보고 대상 사업체)*가 인지한 경우에는 랜섬웨어 대금 지불 또는 인지 시점으로부터 72시간 이내에 지정된 연방기관에 보고서 제출해야 함

* '보고 대상 사업체(Reporting business entity)'는 ▲당해연도 기준 이전 회계연도의 매출액을 초과한 호주 내 사업체(연방/주 기관, 주요기반시설 자산에 대한 책임 주체는 제외), ▲주요기반시설(「주요기반시설보안법 2018」 파트2B의 적용 기관)

- (랜섬웨어 대금 지불 보고서) ▲보고 기관이나 대금 지불 기관의 연락처 및 사업 정보, ▲사이버보안 사고의 내용과 영향, ▲협박 주체의 요구사항, ▲랜섬웨어 대금 지불 내역 ▲협박 주체와의 커뮤니케이션 내용 등 포함

- 랜섬웨어 보고의무를 위반한 경우 60벌점(60 penalty units)[3]의 처벌 부과

○ **(랜섬웨어 대금 지불 정보의 2차적 사용 및 공개 제한)** 랜섬웨어 대금 지불 보고서의 정보를 타 단체 또는 기관이 취득한 경우, 해당 정보의 사용과 공개를 사이버보안 사고 대응 등 특정 목적으로 제한함

랜섬웨어 대금 지불 정보의 사용 및 공개 허용 기준

· 사이버보안 사고 대응 지원, 관련 법적 기능 수행, 형사절차, 정보제공/자문 등 명시된 목적[4]으로만 사용 및 공개 가능 (일반적 법률 위반 조사/집행 목적 등으로는 사용 불가하며 개인정보보호법 준수 필요)

- (예외) 합법적으로 대중에 제공된 정보, 정보주체의 개인정보, 보고 대상 사업체 동의 하에 제공된 자체 정보, 주(州)의 헌법상 기능 수행 관련 정보는 제한적 공개기준 예외에 해당

○ **(국가사이버보안조정관의 역할)** 국가사이버보안조정관은 중대한 사이버보안 사고에 대한 정부의 전반적인 대응 및 분류 조정을 주도하는 한편, 이와 관련하여 장관과 정부에 정보 제공 및 자문을 수행함

3 벌금형을 표준화하기 위한 금전적 가치의 측정 단위. 민형사 소송에서 법원에 의해 부과되며 1페널티 단위의 가치에 범죄횟수 또는 위반횟수를 곱하여 계산됨. 2023년 7월 1일 이후 1패널티 단위의 가치는 313호주 달러.

4 보고 대상 사업체의 사이버보안 사고 대응/완화/해결 지원, 본법 파트 3, 6에 따른 기능 수행, 허위정보 제공 및 공무집행방해 관련, 형사절차, 연방기관의 사고 대응/완화/해결 기능, 주 기관의 사고 대응/완화/해결 기능, 국가사이버보안조정관의 제4장 관련 기능, 장관들에 대한 사고 관련 정보제공/자문, 정보기관의 기능 수행

〈 국가사이버보안조정관의 정보 사용 및 공개 〉

구분	주요내용
중대한 사이버보안 사고 관련 제공받은 정보	▪ 국가사이버보안조정관은 제공받은 정보를 영향범위 내 단체의 사고 대응/완화/해결을 지원하기 위하여 또는 허가된 사이버보안 목적에 한하여 기록/사용/공개할 수 있음 - 단, 일반적 법률 위반 조사/집행 목적으로는 사용할 수 없으며, 개인정보보호법상 금지/제한 사항을 준수해야 함
기타 사고 관련 정보	▪ 국가사이버보안조정관은 중대한 사이버보안 사고가 아닌 경우, 단체가 제공한 정보를 다른 지원 서비스 안내, 정부 차원의 대응 조정, 자문 수행 목적으로만 사용할 수 있음

- 중대한 사이버보안 사고로 영향을 받는 호주 내 사업체나 주요기반시설 책임 단체는 국가사이버보안조정관에게 해당 사고가 중대한 사이버보안 사고이거나 그러할 것으로 예상되는 경우, 단체(Entity)는 직접 또는 대리를 통해 사고 대응 과정에서 언제든지 자발적 또는 조정관의 요청에 따라 관련 정보 제공 가능

- 한편, 사이버보안 사고의 성격이 중대성을 가리는 것이 불분명한 상황에서 정보를 제공하는 경우, 국가사이버보안조정관이 이를 판단하기 위한 목적으로 해당 정보를 수집하고 사용할 수 있음

○ **(사이버사고검토위원회 설립)** 사이버보안 사고를 체계적으로 검토하여, 향후 유사한 성격의 사이버보안 사고를 예방·탐지·대응하는 등 개선사항을 도출하기 위하여 의장과 최대 6명의 상임위원으로 구성된 독립적인 검토위원회를 설립

- **(위원회 구성)** 위원회는 위원장과 2-6명의 상임위원으로 구성되고, 「공공거버넌스법[5]」 상 부처 기관으로 지정되어 위원회 구성원들이 해당 부처의 공무원(officials of the Department)으로서의 지위를 갖게 됨

- **(위원회 기능 및 독립성)** 호주의 사회·경제적 안정성, 국방, 국가안보에 심각한 위해가 있거나, 주목할만한 새로운 수법·기술이 포함되는 경우 등의 사이버보안 사고를 검토하고, 예방 및 대응 사항을 제시하기 위하여 기능 수행의 완전한 재량권 보유

- **(검토 보고서)** 위원회는 사이버보안 사고 검토 결과를 초안 보고서와 최종 보고서로 구분하여 작성하고, 민감 정보의 처리 방식을 준수해야 함

구분	주요내용
초안 검토보고서	• 위원회는 검토 패널이 수행한 검토에 대해 예비 검토 결과, 관련 근거 자료, 제안된 권고사항과 그 사유를 포함한 초안 보고서를 작성하여 장관에게 제출하고, 필요한 경우 다른 연방 또는 주 기관에 의견 수렴을 위해 공유할 수 있으며, 이때 합리적인 의견제시 기간을 부여해야 함
최종 검토보고서	• 위원회는 초안 보고서에 대해 접수된 의견들을 고려하여 최종 검토 결과와 권고사항을 담은 최종 보고서를 작성해야 하며, 이때 사이버보안 사고에 대한 책임 귀속이나 개인 신원 공개를 피하고 부정적 추론을 방지하면서 민감 정보를 제외한 내용을 공개 발간해야 함

5 Public Governance, Performance and Accountability Act 2013

구분	주요내용
민감 정보 처리	• 최종 보고서에서는 국가 안보나 국방, 국제관계를 저해할 수 있는 정보, 연방-주 정부 관계에 영향을 미치는 정보, 범죄 수사 정보원 식별 가능 정보, 개인의 생명이나 안전을 위협하는 정보, 공정한 재판을 저해하는 정보, 법적 공개가 제한된 정보, 기밀이나 상업적 민감 정보, 동의 없는 개인정보 등은 반드시 삭제되어야 함
보호 검토보고서	• 최종 보고서에서 삭제된 민감 정보는 삭제 사유와 함께 별도의 보호 검토보고서에 포함하여 총리와 장관에게 제출되어야 하며, 장관은 사이버보안 사고 대응, 정보기관 업무 수행 등 특정 목적을 위해 필요한 경우 다른 연방 기관이나 주 기관과 공유할 수 있음

- **(수집된 정보의 사용 및 공개 제한)** 위원회와 관련 기관은 수집된 정보를 사이버보안 사고 대응, 범죄 수사, 정보기관 업무 등 법정 목적으로만 사용해야 하며, 민사상 조치나 규제 집행 조사 목적으로는 사용이 금지되나, 이미 공개된 정보는 제한 없이 사용할 수 있음

②「주요기반시설보안법 2018」 및 통신 관련법 개정 - 주요기반시설 및 통신 관련-

▲기업 핵심 데이터를 보관하는 데이터 저장 시스템 규정 신설, ▲주요 기반시설 위험 관리 프로그램 관리 강화, ▲통신보안 관련 사항을「주요기반시설보안법」에 통합 등

○ **('데이터 저장 시스템' 규정)** 기업의 핵심 데이터를 저장하거나 처리하는 '데이터 스토리지 시스템'의 요건을 명확히 규정하고, 해당 요건을 모두 충족한 경우 주요기반시설 자산(국가적으로 중요한 시스템 포함)으로 간주

용어	정의
데이터 저장 시스템 (Data storage systems)	· 주요기반시설 자산(assets)인 경우, 다음의 요건을 모두 충족할 시 데이터 저장 시스템에 해당 - 주요기반시설 자산의 책임 주체가 소유하고 있는 경우 또는 데이터 저장 시스템 운영하는 경우 - 데이터 저장 시스템이 주요기반시설 자산과 연결되어 사용되거나 사용될 예정인 경우 - 비즈니스 핵심(critical)데이터가 데이터 저장 시스템에 의해 저장, 처리되는 경우 - 데이터 저장 시스템에 영향을 미칠 수 있는 위험 발생이 중대한 위험으로 이어질 수 있는 경우 - 주요기반시설 자산에 관련 영향을 줄 수 있는 위험 발생이 중대한 위험이 이어질 수 있는 경우

○ **(주요기반시설 자산에 대한 사고 영향 관리)** 주요기반시설 자산과 하나 이상의 관련 영향을 미쳤거나, 미치고 있거나, 미칠 가능성이 있는 심각한(serious) 사고에 대응하기 위한 연방 체제(regime)를 설정

- 총리(Minister)는 사고 대응을 위하여 장관(Secretary)에게 ▲자산 관련 기관이 자산 관련 정보 수집할 수 있도록 지시 권한, ▲자산 관련 기관에 이행지침을 내릴 수 있는 권한, ▲사이버보안 사고의 경우 장관에게 권한 있는 기관에 개입 요청을 할 수 있도록 권한 부여

○ **(주요기반시설 자산 공개 등 제한)** 주요기반시설 자산 관련 단체 또는 기업은 필요성이 인정되는 경우에 한하여 보호대상 정보를 사용, 공개 또는 기록할 수 있음

용어	정의
보호대상 정보 (Protected information)	· ▲국가 안보 또는 국방 침해가 예상될 때 공개될 수 있거나, ▲국가 또는 국민의 사회·경제적 안정성을 침해할 것으로 합리적으로 예상되는 경우, ▲상업적 기밀 정보 등 기밀 정보에 해당하는 경우, ▲가용성, 무결성, 신뢰성 또는 주요기반시설 자산의 보안공개가 합리적으로 예상되는 경우 '보호대상 정보'를 의미

- 한편, 주요기반시설 자산 관련 단체는 주요기반시설 자산의 지속적인 운영과 관련되거나 기업의 비즈니스, 전문성, 상업 등 업무를 위하여 승인된 경우에 한하여 보호대상 정보를 사용 및 공개할 수 있음

〈 승인된(Authorised) 사용 및 공개 〉

구분	주요내용
가용성, 무결성, 신뢰성 또는 주요기반시설 자산 보안	· 주요기반시설 자산 관련 단체는 ▲주요기반시설 자산의 지속적인 운영과 관련되거나, ▲가용성, 무결성, 신뢰성에 대한 위험 완화를 위하여 보호대상 정보를 사용, 공개하거나 기록할 수 있음
관련 단체의 비즈니스, 전문성, 상업적(commercial) 또는 재무적(financial) 업무	· 주요기반시설 자산 관련 단체는 ▲본 법을 준수하기 위한 목적으로 기업에 의해 획득, 생성, 채택된 보호대상 정보 또는 ▲기업의 비즈니스, 전문성, 상업 또는 재무 업무를 위한 정보를 기록하거나, 사용 또는 공개하는 경우 보호대상 정보를 사용, 공개하거나 기록할 수 있음

○ **(주요기반시설 위험 관리 프로그램 관리 강화)** 관련 공무원은 주요기반시설 위험 관리 프로그램에 심각한 결함(국가 안보, 국방, 사회·경제 안전성)이 하나 이상 있는 경우, 해당 단체가 주요기반시설 위험 관리 프로그램을 다변화(vary)하도록 주요기반시설 자산에 책임있는 기업에 문서화된 지침을 주어야 함

○ **(주요통신 자산 보호를 위한 보안 규정 강화)** 주요통신 자산의 책임주체는 합리적으로 실행가능한 범위 내에서 해당 자산을 보호할 의무가 있으며, 특히 자산에 영향을 미칠 수 있는 중대한(material) 위험이 있는 경우 자산을 보호해야 함

- 주요통신 자산의 책임주체는 통신 서비스 또는 통신 시스템에 대한 특정 변경 또는 변경 제안이 자산 책임자의 역량에 중대한 악영향을 미칠 가능성이 있는 경우, 장관에게 해당 서비스/시스템 변경 등의 제안을 통지해야 함

- 한편, 장관은 주요통신 자산의 사용 또는 공급이 보안에 해가 되거나 해가 될 수 있다고 판단하는 경우, 해당 통신 자산의 책임자에게 운송 서비스를 사용 또는 공급하지 않거나 사용 또는 공급을 중단하도록 지시할 수 있음

③ 「정보서비스법 2001」 등 개정

○ **(연방기능 수행을 위한 '제한된 사이버보안 정보' 커뮤니케이션 및 사용)** 연방기관은 ASD 기능 수행, 사이버보안 사고(또는 잠재적 발생 가능성이 있는 사이버보안 사고) 설명, 국가 사이버기관 기능 수행 등 허가된 사이버보안 목적에 한하여 제한적으로 사이버보안 정보를 커뮤니케이션 및 사용할 수 있음

용어	정의
제한된 사이버보안 정보 (Limited cyber security information)	· 해당 정보가 ▲사이버보안 사고가 발생했거나 발생 중인 경우 · 잠재적으로 발생할 수 있는 사이버보안 사고와 관련된 정보 · ▲ASD에 의해 자발적으로 제공되거나, 사이버보안 사고를 합리적으로 예상할 수 있는 경우 또는 직간접적으로 영향을 받은 경우 또는 ▲잠재적으로 발생할 수 있는 사이버보안 사고에 의해 영향을 받을 것으로 합리적으로 예상되는 등 ASD가 정보를 획득하거나 준비한 경우 · ▲사이버보안 사고와 관련하여 해당 정보가 (i) 「사이버보안법 2024」 제35(2)항에 따라 국가사이버보안조정관이 취득한 정보 등

■ 전망 및 시사점

○ 호주 정부는 최근 증가하고 있는 사이버 범죄를 막기 위해 대규모 예산(약 5,000억 원)을 투입하는 등 심각해진 지정학적, 사이버 위협 환경에 적극적으로 대응하기 위하여 국가 사이버 방어체계 및 사회·경제 전반에 걸친 사이버복원력 강화를 강조

- 사이버사고 피해 확산 방지 및 재발 방지를 위하여 독립적 지위의 사이버사고검토위원회를 설립하는 한편, 주요기반시설 자산에 대한 사고 영향 관리를 효과적으로 관리하기 위하여 정부 지원 프레임워크를 확장하는 등 전반적인 관리 체계를 강화

○ 한편, 랜섬웨어 대금 지불 보고 의무와 정보 공유에 대한 법적 보호 장치는 기업들의 적극적인 보고(reporting) 참여를 유도할 것으로 보이며, 이를 통해 수집된 데이터는 공격 패턴 분석과 예방 대책 수립에 활용되어 국가의 사이버보안 대응 능력을 크게 향상시킬 것으로 기대

○ 또한, 스마트 기기에 대한 보안 표준 도입으로 호주 시장의 IoT 기기 보안 수준이 전반적으로 향상될 것으로 예상되는 등 글로벌 시장에서 호주의 사이버보안 영향력이 점차 강화될 것으로 보임

Reference

▪https://www.homeaffairs.gov.au/news-media/archive/article?itemId=1247
▪https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r7250_first-reps/toc_pdf/24116b01.pdf;fileType=application%2Fpdf

싱가포르

해외 입법 동향

싱가포르 정부, 국가 사이버보안 체계 강화를 위한 「사이버보안법」 개정안 국회 제출

싱가포르 정부는 국가의 디지털화 확대 및 사이버보안 사고 증가에 대응하기 위해 국가 전반의 사이버보안 시스템을 강화하는 「사이버보안법 개정법률안[1]」을 국회에 제출 (2024. 4. 3.)

■ 개요

○ 싱가포르 사이버보안청(Cyber Security Agency of Singapore)은 2018년 제정된 「사이버보안법」(Cybersecurity Act 2018)을 현재 사이버보안 환경에 맞게 최신화한 일부개정법률안을 국회에 제출

- 동 법안은 기존 「사이버보안법」의 일부 미비점을 극복하고 사이버보안청의 감독 범위 확대를 통해 국가 사이버보안 회복력을 강화하기 위함

- 구체적으로, ▲신기술 발전 및 활용 등을 법률에 반영하기 위한 '제3자 소유 주요 정보기반시설(third-party-owned critical information infrastructure)' 개념 도입 및 관련 의무 설정 ▲사이버보안 사고(cybersecurity incident) 보고 대상 확장 ▲규제 대상 범주 신설을 바탕으로 한 사이버보안청의 감독 및 규제 권한 확대 등을 핵심으로 함

○ 이번 법안이 제출되기에 앞서 사이버보안청은 동 법률안에 대한 각계의 다양한 의견 수렴 과정을 거친 바 있음

- 사이버보안청은 2022년부터 이해관계자 협의를 수행하는 한편 2023년 12월~1월 기간 온라인을 통해 공공 의견을 청취 및 수렴했으며, 이후 제안된 의견 등을 이번 개정법률안에 반영

■ 주요내용

○ **(주요 용어)** 동 법안은 아래와 같이 주요 용어를 추가적으로 정의(제2조 개정)

1 Cybersecurity (Amendment) Bill

구분	주요 내용
컴퓨터 및 컴퓨터 시스템	• 컴퓨터 및 컴퓨터 시스템은 가상 컴퓨터 및 가상 컴퓨터 시스템을 포함 – 가상 컴퓨터란 논리, 산술 또는 저장 기능을 수행하면서 소프트웨어와 하드웨어의 시뮬레이션으로 만들어진 컴퓨터의 순수한 디지털 아날로그를 의미 – 가상 컴퓨터 시스템이란 하나 이상의 특정 기능을 수행하도록 설계된 것으로서 상호 연결된 컴퓨터의 배열을 시뮬레이션하여 만든 컴퓨터 시스템의 순수한 디지털 아날로그를 의미
디지털 서비스	• 일방 당사자가 상대방의 개별 요청에 따라 전자적 수단을 통해 상호 간 물리적 대면 없이 상대방에게 제공하는 서비스로서, 통상적으로 보수를 목적으로 제공되는 모든 서비스
기본 디지털 기반시설 서비스	• 디지털 서비스의 가용성, 대기 시간, 처리량 또는 보안을 뒷받침하는 모든 서비스

○ **(주요 정보 기반시설 소유자 개념 세분화)** 개정안은 필수 서비스를 제공하는 제공업체가 항상 주요 정보 기반시설의 소유자가 아니라는 점을 감안[2]하여 소유자 관련 내용을 보다 구체화

– 동 법안은 ▲직접 소유(provider-owned) 주요 정보 기반시설 ▲제3자 소유 주요 정보 기반시설 등으로 소유자 개념을 세분화(제2조 개정)

구분	주요 내용
직접 소유 주요 정보 기반시설	• 사이버보안청장(Commissioner of Cybersecurity)이 싱가포르 필수 서비스의 지속적 제공 등을 위해 필요하다고 판단하여 지정한 컴퓨터 또는 컴퓨터 시스템 중 필수 서비스 제공업체가 직접적으로 통제하는 컴퓨터 또는 컴퓨터 시스템
제3자 소유 주요 정보 기반시설	• 사이버보안청장이 싱가포르 필수 서비스의 지속적 제공 등을 위해 필요하다고 판단한 컴퓨터 또는 컴퓨터 시스템 중 필수 서비스 제공업체가 타인이 통제하는 컴퓨터 또는 컴퓨터 시스템에 대해 제3A부에 따른 사이버보안 담당자로 지정되는 경우, 해당 제3자 통제 하의 컴퓨터 또는 컴퓨터 시스템

· 필수 서비스를 제공하는 '제3자 소유 주요 정보 기반시설' 활용 업체는 일정 요건을 만족할 경우 사이버보안청장으로부터 사이버보안 담당자로 지정됨으로써 해당 타인 소유의 기반시설에 대한 일정한 사이버보안 책임을 부여받음

○ **(사이버보안 사고 보고 대상 확대)** 개정안은 주요 정보 기반시설 직접 소유자에 대해 기존 사이버보안 사고 보고 의무 이외에도 공급망 등 보다 광범위한 범위에서 일어나는 사이버보안 사고에 관해서도 보고 의무를 부과

– 주요 기반시설 직접 소유자는 자신의 통제 아래 또는 자신의 공급업체 통제 아래에 있는 기타 모든 컴퓨터 또는 컴퓨터 시스템과 관련하여 규정된 사이버보안 사고에 대해 사이버보안청장에게 보고할 의무가 있음(제14조 개정)

2 정보통신기술의 발달로 인해 필수 서비스 제공업체가 클라우드 컴퓨팅 서비스를 직접 소유 또는 운영하는 대신, 아마존과 같은 글로벌 기업의 클라우드 컴퓨팅 서비스를 활용하는 사례가 대폭 확대

○ **(제3자 소유 주요 정보 기반시설 관련 의무 부과)** 개정안은 사이버보안청장으로 하여금 제3자 소유 주요 정보 기반시설을 활용하는 필수 서비스 제공업체 중 특정 요건을 충족하는 업체에 대해, 서면 통지를 통하여 해당 기반시설에 대한 일련의 사이버보안 의무를 부담시킬 수 있는 권한을 부여

- 사이버보안청장은 ▲제3자 소유의 컴퓨터 또는 컴퓨터 시스템이 싱가포르의 필수 서비스의 지속적인 제공을 위해 필요하고 ▲해당 시스템의 손실 또는 손상으로 인해 싱가포르 내 필수 서비스가 약화될 가능성이 있는 경우, 제3자 소유 주요 정보 기반시설을 활용하는 필수 서비스 제공업체를 동 기반시설의 사이버보안 담당자로 지정할 수 있음(제17조 및 제18조 삭제, 제3A부 대체 신설)

  · 사이버보안 담당자로 지정된 필수 서비스 제공업체는 해당 기반시설 소유자로부터 법적 구속력이 있는 확약(Legally binding commitment)을 얻음으로써 자신이 동법상의 의무를 이행하고 사이버보안 표준을 유지할 수 있도록 해야 함

  · 확약의 내용에는 ▲해당 기반시설을 대상으로 발생하는 사이버보안 사고에 대한 보고 의무 부과 ▲정기적 사이버보안 감사(cybersecurity audits) 및 사이버보안 위험평가(cybersecurity risk assessment) 수행 등이 포함

○ **(감독 범위 확대)** 개정안은 동법의 적용대상이 되는 신규 범주를 신설하여 사이버보안청의 감독 및 규제 범위를 확대하고자 함

구분	주요 내용
임시 사이버보안 우려 시스템 (system of temporary cybersecurity concern)[3] (제3B부 신설)	• **(요건)** 사이버보안청장은 아래의 요건을 모두 갖춘 컴퓨터 또는 컴퓨터 시스템 소유자를 서면 통지로써 일정 기간에 한정하여 임시 사이버보안 우려 시스템으로 지정할 수 있음 – 특정 기간 동안 컴퓨터 또는 컴퓨터 시스템에 사이버보안상 위험을 초래하거나 사이버보안 사고가 감행될 위험이 높은 경우 – 해당 컴퓨터 또는 컴퓨터 시스템의 손상 등이 국가 안보, 국방, 외교, 경제, 공중 보건, 공공 안전, 공공 질서 등에 심각한 해를 끼칠 수 있다고 판단되는 경우 • **(기간)** 최대 1년 범위 내에서 기간을 정하여 지정하며, 이후 기간 연장 가능 • **(의무)** 해당 시스템의 소유자는 사이버보안청장에 대해 ▲시스템 설계, 구성, 보안 등에 관한 정보 제공 ▲시스템, 이와 연결된 기타 컴퓨터 또는 컴퓨터 시스템과 관련한 사이버보안 사고에 대한 보고 등의 의무 수행
특별 사이버보안 이해관계 법인 (entity of special cybersecurity interest) (제3C부 신설)	• **(요건)** 사이버보안청장은 아래의 요건을 모두 갖춘 법인을 서면 통지로써 특별 사이버보안 이해관계 법인으로 지정할 수 있음 – 법인의 통제 하에 있는 컴퓨터 또는 컴퓨터 시스템에 민감한 정보를 저장하는 경우 – 컴퓨터 또는 컴퓨터 시스템 중단 시 싱가포르의 국방, 외교, 경제, 공중 보건, 공공 안전 또는 공공 질서 등에 심각한 해를 끼칠 수 있는 기능을 수행하는 법인인 경우 • **(기간)** 지정으로부터 5년 동안 유효하며, 이후 기간 연장 가능 • **(의무)** 법인은 사이버보안청장에 대해 ▲시스템 설계, 구성, 보안 등에 관한 정보 제공 ▲법인이 보유한 데이터의 가용성, 기밀성, 무결성이 침해되는 결과를 초래하거나 법인의 사업 운영에 중대한 영향을 미치는 사이버보안 사고에 대한 보고 등의 의무 수행
기본 디지털 기반시설 서비스	• **(요건)** 사이버보안청장은 아래의 요건 중 하나 이상을 갖춘 사업체를 서면 통지로써 기본 디지털 기반시설 서비스 제공업체로 지정할 수 있음

구분	주요 내용
제공업체 (foundational digital infrastructure service provider)[4] (제3D부 신설)	- 싱가포르 내부 또는 외부에서 싱가포르에 있는 사람을 대상으로 하는 디지털 기반시설 서비스로서, 해당 기본 디지털 인프라 서비스 제공의 손실 또는 손상으로 인해 싱가포르에 있는 다수의 기업 또는 조직의 운영이 중단되거나 저하될 가능성이 있는 경우 - 서비스 전부 또는 일부가 싱가포르로부터 제공되며, 해당 기본 디지털 인프라 서비스 제공의 손실 또는 손상으로 인해 이에 의존하는 다수의 기업 또는 조직의 운영이 중단되거나 저하될 가능성이 있는 경우 • **(기간)** 지정으로부터 5년 동안 유효하며, 이후 기간 연장 가능 • **(의무)** 서비스 제공업체는 사이버보안청장에 대해 ▲기본 디지털 기반시설의 사이버보안을 위해 마련한 조치 등에 관한 정보 제공 ▲자신이 통제하는 컴퓨터 또는 컴퓨터 시스템과 관련한 사고로서 싱가포르에서 기본 디지털 기반시설 서비스의 지속적인 제공이 중단되거나 저하되는 사이버보안 사고에 대한 보고 등의 의무 수행

○ **(처벌)** 개정안은 기존 형사 처벌 규정[5]에 더하여 특정 조항 위반과 관련해 민사 벌금 제도를 신설(제37A조 및 제37B조 신설)

- 사이버보안청장은 제3A부~제3D부에 명시된 의무를 위반한 자를 상대로 법원에 소를 제기함으로써 위반사항에 대해 민사 처벌을 구할 수 있음

- 법원은 이에 대해 ▲싱가포르 내 연간 매출액의 10% ▲50만 싱가포르 달러(약 5억 원) 중 더 높은 금액을 상한으로 하는 민사 벌금 처벌을 명령할 수 있음

- 다만, 해당 소송은 제3A부~제3D부의 각 조항을 위반한 날로부터 6년이 경과한 후에는 제기될 수 없음

■ 전망 및 시사점

○ 「사이버보안법 개정법률안」은 기존 「사이버보안법」에서 발생한 법적 공백을 일부 해결하고 있다는 점에서 긍정적으로 평가

- 필수 서비스 제공업체가 해외 아웃소싱을 사용함으로써 자신의 사이버보안 의무를 벗어나려는 것을 방지하기 위해 기반시설 소유자 개념을 세분화함으로써 의무 회피 가능성을 최소화

- 최근 사이버공격이 주요 정보 기반시설 뿐만 아니라 기타 시스템 등으로 대상 범위를 확대하여, 주요 정보 기반시설을 타격하지 않고도 한 국가에 심각한 영향을 미칠 수 있다는 현실을 반영

○ 또한 동 개정법률안은 최근 들어 전 세계적으로 발생한 사이버공격 등을 분석하고 법적 취약점을 파악하여 이를 법률에 충실히 반영하려고 노력

3 대표적인 예로 코로나19 대유행 기간 백신 배포를 위해 사용되던 컴퓨터 시스템, 정상회담 등 중요 국제행사 등에 활용되는 시스템 등이 포함
4 클라우드 컴퓨팅 서비스 또는 데이터 센터 등이 대표적
5 10만 싱가포르 달러(약 1억 원) 이하의 벌금 및/또는 2년 이하의 징역 (제10조제2항)

구분	주요 내용
사이버보안 사고 보고 확대	• **(사례)** 2021년 미국 최대의 연료 파이프라인 운영사를 대상으로 한 사이버공격에서 공격자가 주요 기능이 아닌 기업 결제 서비스를 장악함으로써 심각한 피해 초래 – **(개정안)** 핵심 서비스를 마비시키기 위해 상대적으로 장벽이 낮은 주변 시스템을 공격 대상으로 삼은 사이버공격 발생 사례 극복 시도
제3자 소유 주요 정보 기반시설 관련 의무 부과	• **(사례)** 2021년 마이크로소프트사의 클라우드 컴퓨팅 플랫폼에서 해커가 민감한 데이터베이스로의 접근 통로를 열어둔 심각한 취약점 발견 – **(개정안)** 필수 서비스 제공업체가 제3가 소유 클라우드 서비스를 활용할 때 사이버보안 관련 의무의 회피 위험성 완화
사이버보안청 감독 범위 확대	• **(사례)** 2020년 코로나19 백신 배포를 지원하던 각종 조직이 전 세계적으로 사이버공격의 표적이 되었으며, 공격자들은 네트워크 로그인 자격 증명을 탈취함으로써 백신 배포 방해 – **(개정안)** 주요 정보 기반시설은 아니더라도 특수한 상황에서는 기타 조직 등에 사이버보안 관련 의무를 부과하는 등 국방, 외교, 경제, 공중 보건, 공공 안전 또는 공공 질서에 부정적 영향을 최소화하기 위해 기타 조직을 대상으로 사이버보안청의 감독 및 규제 범위 확대

○ 이번 개정안이 통과될 경우 필수 서비스 제공업체를 비롯, 다수의 조직, 법인 등은 사이버보안 관련 의무의 추가로 인해 운영에 막대한 영향을 받게 될 가능성이 높음

– 따라서 각 조직 등은 관련 의무를 준수하기 위해 사이버보안청과 긴밀한 연락망 및 협의 체계를 구축하고 의무 수행을 위한 대응책을 마련하는 것이 중요

○ 이와 관련, 일각에서는 동 개정안이 사이버보안청에 기타 조직 등에 대한 감독 범위 확대에 있어 지나친 재량권을 부여하고 있다고 우려

– 특히 특별 사이버보안 이해관계 법인 지정 및 기본 디지털 기반시설 서비스 제공업체 지정에 있어서는 사이버보안청이 기업을 어떻게 평가할 것인지에 대한 명확한 기준을 인식할 수 없어 각 법인 및 사업체가 느끼는 불분명성은 상당할 것으로 예상

Reference

▪https://www.parliament.gov.sg/docs/default-source/bills-introduced/cybersecurity-(amendment)-bill-15-2024.pdf?sfvrsn=1bb05508_1
▪https://www.csa.gov.sg/News-Events/Press-Releases/csa-first-reading-of-the-cybersecurity-(amendment)-bill
▪https://www.lexology.com/library/detail.aspx?g=88ea9faf-40f8-4b1d-a513-85d406ca7c87
▪https://www.channelnewsasia.com/singapore/cybersecurity-critical-information-infrastructure-csa-parliament-4238971
▪https://www.straitstimes.com/singapore/politics/proposed-changes-to-cybersecurity-act-of-s-pore-and-what-triggered-them
▪https://www.crowell.com/en/insights/client-alerts/landmark-amendments-to-singapores-cybersecurity-bill-re-interpreting-cii-to-bolster-national-cyber-resilience

기 타

해외 입법 동향

UN, 사이버범죄 예방 및 대응 강화를 위한 「UN 사이버범죄 방지 협약(안)」 타결

사이버범죄 예방 및 대응 강화를 위하여, UN 임시위원회는 「UN 사이버범죄 방지 협약(안)」[1]을 만장일치로 타결 (2024. 8. 8.)

■ 개요 및 추진배경

○ 2024년 8월 8일, UN 산하의 '범죄 목적을 위한 정보통신기술 사용에 대항하는 포괄적 국제협약을 수립하기 위한 임시위원회'(이하 임시위원회)[2]는 UN 최초의 사이버범죄에 관한 포괄적 협약(안)을 타결

- 동 임시위원회는 사이버범죄에 관한 신규 협약을 협의하기 위해 UN 총회에서 설립한 위원회로 3년간의 노력 끝에 협약 최종안에 합의

〈 UN 사이버범죄 방지 협약(안) 추진 경과 〉

구분	주요내용
2017년 10월 11일	• 러시아, 사이버범죄 퇴치협력에 관한 유엔협약 초안[3] 제출
2019년 12월 27일	• UN, 범죄 목적의 정보통신기술 사용에 대한 대응(결의안 74/247)[4] - 범죄 목적의 ICT 사용에 대응하기 위한 포괄적 국제협약을 개발하는 임시위원회 조직
2022년 2월 ~	• 비엔나 3회, 뉴욕 3회 등 총 6회의 협상회의 진행
2024년 8월 8일	• 회원국, 사이버범죄 방지 협약(안) 만장일치 타결 - 추후 2024년 말에 진행되는 UN 총회에 제출되어 공식 채택될 예정

○ 동 협약(안)은 협약 당사국의 사이버범죄 완화를 위한 협력 방안을 설정한 것으로, ▲사이버범죄에 관한 형사범죄 확립 및 국제협력 ▲법 집행 및 형사절차와 관련한 상호 공조 ▲예방조치 ▲기술지원 및 역량강화 등을 주요내용으로 함

1 Draft United Nations convention against cybercrime
2 Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes
3 Letter dated 11 October 2017 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General
4 74/247. Countering the use of information and communications technologies for criminal purposes

〈 UN 사이버범죄 협약 주요 구성 〉

구분	주요내용
제1장 총칙	· 목적(제1조), 정의(제2조), 적용범위(제3조) 등
제2장 범죄화	· 불법 접근(제7조), 불법 감청(제8조), 전자 데이터 침해(제9조), 정보통신기술시스템 방해(제10조), 기기 오용(제11조), 정보통신기술시스템 관련 위조(제12조), 정보통신기술시스템 관련 절도 또는 기망(제13조), 범죄 수익 세탁(제17조), 법인의 책임(제18조), 공소시효(제20조), 기소, 판결 및 제재(제21조) 등
제3장 관할권	· 관할권(제22조)
제4장 절차규정과 법집행	· 절차규정의 적용범위(제23조), 조건 및 안전조치(제24조), 저장된 전자 데이터의 신속한 보존(제25조), 트래픽 데이터의 신속한 보존 및 부분공개(제26조), 제출명령(제27조), 저장된 전자자료의 압수수색(제28조), 트래픽 데이터의 실시간 수집(제29조), 콘텐츠 데이터 감청(제30조), 범죄 수익의 동결, 압류 및 몰수(제31조) 등
제5장 국제협력	· 국제협력의 일반원칙(제35조), 개인정보보호(제36조), 연중무휴 통신망(제41조) 등
제6장 예방조치	· 예방조치(제53조)
제7장 기술지원 및 정보공유	· 기술지원 및 역량강화(제54조), 정보공유(제55조) 등
제8장 이행 메커니즘	· 협약 당사국 회의(제57조), 사무국(제58조)
제9장 최종규정	· 협약의 이행(제59조), 협약의 효과(제60조), 발효(제65조) 등

■ 주요내용

○ **(목적)** ▲사이버범죄를 보다 효율적이고 효과적으로 예방하고 퇴치하기 위한 조치의 촉진·강화 ▲사이버범죄 예방 및 퇴치를 위한 국제협력 촉진·강화 ▲개발도상국의 이익을 위해 사이버범죄를 예방하고 퇴치하기 위한 기술 및 역량구축 지원

○ **(정의)** 동 협약(안)은 주요 용어를 다음과 같이 정의 (제2조)

구분	주요내용
정보통신기술 시스템 (Information and Communications Technology System)	• 프로그램에 따라 **전자 데이터를 수집, 저장 및 자동 처리**하는 **하나 이상의 상호 연결되거나 관련된 장치**, 혹은 **장치 그룹**
전자 데이터 (Electronic Data)	• 정보통신기술 **시스템에서 처리하기에 적합한 형태로 표현된 사실, 정보 또는 개념**을 의미하며, 정보통신기술 시스템이 기능을 수행하도록 하는 데 적합한 프로그램을 포함
트래픽 데이터 (Traffic Data)	• **통신의 출발지, 목적지, 경로, 시간, 날짜, 크기, 기간 또는 기본 서비스의 유형**을 나타내는, 정보통신기술 시스템에 의해 생성된 **통신 관련 모든 전자 데이터**
콘텐츠 데이터 (Content Data)	• **이미지, 문자 메시지, 음성 메시지, 음성 녹음 및 비디오 녹음 등** 정보통신기술 시스템에 의해 전송되는 **데이터의 실질과 관련된 모든 전자 데이터**
개인정보 (Personal Data)	• 식별되거나 식별가능한 자연인과 관련된 모든 정보
중범죄 (Serious Crime)	• 최소 4년 이상의 자유 박탈[5] 또는 그 이상의 중한 형벌에 처해질 수 있는 범죄에 해당하는 행위
재산 (Property)	• 유형 또는 무형, 동산 또는 부동산, 가상 자산을 포함한 모든 종류의 자산과 그러한 자산에 대한 소유권(title) 또는 이권(interest)을 증명하는 법적 문서 또는 증서
범죄 수익 (Proceeds of Crime)	• 범죄행위로 인하여 직·간접적으로 취득한 재산
동결 또는 압류 (Freezing or Seizure)	• 법원이나 그 밖의 권한있는 기관이 내린 명령에 근거하여 재산의 양도, 전환, 처분 또는 이동을 일시적으로 금지하거나 재산의 보관 또는 통제권을 일시적으로 인수하는 것
몰수 (Confiscation)	• 법원이나 그 밖의 권한있는 기관의 명령에 의한 재산의 영구적 박탈

○ **(범죄화)** 각 당사국은 다음 행위를 국내법에 따라 범죄로 구성하는 데 필요한 입법 및 기타 조치를 이행해야 함

구분	주요내용
불법 접근 (제7조) (Illegal Access)	• 고의로 권한없이 정보통신기술 시스템의 전체 또는 일부에 접근하는 행위
불법 감청 (제8조) (Illegal Interception)	• 고의로 권한없이 정보통신기술 시스템 간 이동하거나 또는 내부에서 이뤄지는 전자 데이터의 비공개 전송을 기술적 수단으로 가로채는 행위
전자 데이터 침해 (제9조) (Interference With Electronic Data)	• 고의로 권한없이 전자 데이터의 손상, 삭제, 악화, 변경 또는 억제를 저지르는 행위
정보통신기술 시스템 방해 (제10조) (Interference With An Information And Communications Technology System)	• 고의로 권한없이 전자 데이터의 입력, 전송, 손상, 삭제, 악화, 변경 또는 억제를 통한 정보통신기술 시스템 기능의 심각한 저해를 행하는 것
기기 오용 (제11조) (Misuse Of Devices)	• 고의로 권한없이 동 협약(안) 제7조~제10조에 따라 규정된 범죄, 즉 불법 접근, 불법 감청, 전자 데이터 및 정보통신기술 시스템 간섭 등을 저지를 목적으로 주로 설계 또는 개조된 프로그램을 포함한 기기를 취득, 생산, 판매, 사용, 수입, 유통 또는 기타 방법으로 제공하는 등의 행위 • 고의로 권한없이 본 협약(안) 제7조~제10조에 따라 규정된 범죄, 즉 불법 접근, 불법 감청, 전자 데이터 및 정보통신기술 시스템 간섭 등을 범할 목적으로 상기 언급된 물품을 소지하는 행위
정보통신기술 시스템 관련 위조 (제12조) (Information And Communications Technology System-related Forgery)	• 데이터를 직접적으로 읽을 수 있고 이해할 수 있는지 여부에 관계없이, 법적목적을 위해 진본인 것처럼 조치될 의도로, 고의로 권한없이 전자 데이터를 입력, 변경, 삭제 또는 억제하여 진본이 아닌 데이터를 만드는 행위
정보통신기술 시스템 관련 절도 또는 기망 (제13조) (Information And Communications Technology System-related Theft Or Fraud)	• 고의로 권한없이 다음의 수단으로 타인에게 재산상의 손실을 야기하는 행위 – 전자 데이터의 입력, 변경, 삭제 또는 억제 – 정보통신기술 시스템의 기능에 대한 모든 형태의 방해 – 정보통신기술 시스템을 통해 이루어진 사실적 상황에 대해, 타인이 하지 않았거나 했어야 하는 행위를 하게 하거나 하지 않게 하는 기망행위
온라인 아동 성적 학대 또는 아동 성 착취물 관련 범죄 (제14조) (Offences Related To Online Child Sexual Abuse Or Child Sexual Exploitation Material)	• 고의로 권한없이 정보통신기술 시스템을 통해 아동 성적학대 또는 성 착취물을 제작, 제공, 판매, 배포, 전송, 방송, 전시, 게시 또는 기타 방법으로 제공하는 행위 • 고의로 권한없이 정보통신기술 시스템을 통해 아동 성적학대 또는 성 착취물을 요청, 조달 또는 이에 접근하는 행위 • 정보통신기술 시스템 또는 기타 저장 매체에 아동 성적학대 또는 성착취물을 소지하거나 이를 제어하는 행위 • 상기 위반행위에 자금을 지원하는 행위
아동 성범죄 목적의 권유 또는 그루밍 (제15조) (Solicitation Or Grooming For The Purpose Of Committing A Sexual Offence Against A Child)	• 아동에 대한 성범죄를 범할 목적으로 정보통신기술 시스템을 통해 고의로 통신, 권유, 유인 또는 알선하는 행위
사적 이미지의 무단 유포 (제16조) (Non-consensual Dissemination Of Intimate Images)	• 고의로 권한없이 정보통신기술 시스템을 통해 개인의 동의없는 사적인 이미지를 판매, 배포, 전송, 게시 또는 기타 방식으로 제공하는 행위

5 UN에서 정의하는 자유박탈이란, 모든 형태의 구금, 수감 또는 사법적 및 행정적 기타 권한 있는 기관의 명령에 따라 자유의지로 떠날 수 없는 공공 민간의 구금적 환경에 배치되는 것을 의미

구분	주요내용
범죄 수익 세탁 (제17조) (Laundering Of Proceeds Of Crime)	• 불법적인 재산출처를 은폐 또는 위장하거나, 선행 범죄의 범행에 관여한 자가 자신의 행위로 인한 법적 결과를 회피할 목적으로 그러한 재산이 범죄 수익임을 알면서 재산을 전환 또는 양도하는 행위 • 그러한 재산이 범죄 수익임을 알면서 재산의 진정한 성격, 출처, 위치, 처분, 이동 또는 소유권을 은폐 또는 위장하는 행위 • 수령 당시 해당 재산이 범죄 수익이라는 것을 알면서 재산을 취득, 소유 또는 사용하는 행위 • 동 조에 규정된 범죄에 가담, 관여 또는 범죄를 모의하거나, 동 조의 범죄를 시도하거나, 이를 교사, 방조, 촉진 및 조언하는 행위

○ **(관할권)** 각 당사국은 위반행위가 ▲당사국의 영토에서 행해지거나 ▲해당 당사국의 국기를 달고 있는 선박 또는 법률에 따라 해당 당사국에 등록된 항공기 내에서 행해지는 경우에 대비하여, 동 협약(안)에 따라 확립된 범죄의 관할권을 정하는 데에 필요한 조치를 이행해야 함 (제22조)

○ **(절차규정의 적용범위)** 각 당사국은 특정 범죄수사 또는 절차의 목적을 위해 필요한 입법 및 기타 조치를 이행해야 함 (제23조)

- 각 당사국은 ▲인권보호를 위한 조건 및 안전조치 (제24조), ▲저장된 전자 데이터의 신속한 보존 (제25조), ▲트래픽 데이터의 신속한 보존 및 기관에 대한 부분 공개 (제26조), ▲전자 데이터 및 정보 제출명령 (제27조), 등을 위하여 필요한 입법 및 기타 조치를 이행해야 함

○ **(국제협력의 일반 원칙)** 당사국은 동 협약(안) 규정 및 기타 적용가능한 범죄문제 관련 국제협약 등에 근거하여 상호 협력해야 함 (제35조)

- 구체적으로, 동 협약(안)에 따라 확립된 ▲형사범죄에 대한 수사와 기소 및 사법절차(범죄 수익 동결, 압류, 몰수 및 반환 포함), ▲범죄의 전자적 형태의 증거 수집, 획득, 보존 및 공유, ▲동 협약(안) 채택 당시 시행 중인 다른 UN 협약 및 의정서에 따라 확립된 중범죄를 포함하여 중범죄에 관한 전자적 형태의 증거 수집, 획득, 보존 및 공유 등을 포함

○ **(개인정보보호)** 동 협약(안)에 따라 개인정보를 전송하는 당사국은 국내법 및 해당 국제법에 따라 당사국이 부담하는 모든 의무를 수행해야 함 (제36조)

- 개인정보를 전송하는 당사국은 개인정보보호에 관한 법률에 따라 개인정보를 제공할 수 없는 경우, 동 협약에 따른 개인정보 전송을 수행할 필요가 없음[6]

○ **(형사절차에 관한 상호 공조)** 당사국들은 형사절차의 일관성 및 효율성 등을 위해 아래와 같이 상호 공조를 수행

6 다만, 당사국 간 양자 혹은 다자간 협정을 맺도록 권장함으로써 당사국 간 개인정보를 용이하게 전송하도록 하고 있음

구분	주요내용
범죄인 인도 (제37조)	• 일방 당사국이 징역형 또는 기타 구금형의 최종 선고를 수행할 목적으로 범죄인 인도를 청구하는 경우, 청구를 받은 당사국은 국내법에 따라 인도를 허가할 수 있음
형을 선고받은 자의 이송 (제38조)	• 당사국은 형을 선고받은 자의 권리를 고려하여 동 협약(안)에 따라 확립된 범죄로 인해 징역형 또는 기타 형태의 자유 박탈형을 선고받은 자를 자국 영토로 이송하여 형기를 마칠 수 있도록 양자 또는 다자간 협정을 체결하는 것을 고려할 수 있음
형사소송절차의 이송 (제39조)	• 당사국은 기소집중 등의 목적으로, 여러 관할권이 연관된 사안의 경우 동 협약(안)에 따라 확립된 범죄의 기소를 위해 상호 간 형사소송절차로 이송할 가능성을 고려해야 함

○ **(사법 공조의 일반원칙)** 당사국은 동 협약(안)에 따라 확립된 범죄와 관련하여, 동 협약(안)에 따라 확립된 범죄 및 중범죄에 대한 전자적 형태의 증거 수집을 목적으로, 수사, 기소 및 사법절차에서 가장 광범위한 상호 법적 공조를 서로에게 제공하여야 함 (제40조)

- 이를 위해 당사국은 ▲저장된 전자 데이터의 신속한 보존을 위한 국제협력 (제42조) ▲보존된 트래픽 데이터의 신속한 공개를 위한 국제협력 (제43조) ▲법 집행 협력 (제47조) ▲공동 수사 (제48조) ▲몰수에 관한 메커니즘 구축 및 국제협력 (제49조 및 제50조 등) 등을 수행해야 함

○ **(예방조치)** 각 당사국은 법제도의 기본원칙에 따라 적절한 입법·행정 또는 기타 조치를 통하여 현재 또는 미래의 사이버범죄 가능성을 감소시키기 위한 효과적이고 조정된 정책 및 모범사례를 개발·시행 또는 유지하기 위해 노력해야 함 (제53조)

○ **(기술지원 및 역량강화)** 당사국은 개발도상국의 이익과 필요를 고려하여, 교육 및 기타 형태의 지원, 관련 경험과 전문 지식의 상호 교환, 상호 합의된 조건에 따른 기술 이전 등을 포함한 가장 광범위한 기술지원 및 역량 강화 조치를 능력에 따라 서로 제공할 수 있도록 고려해야 함 (제54조)

○ **(협약 당사국 회의체)** 동 협약(안)에 규정된 목적을 달성하기 위한 당사국 간의 역량과 협력을 증진하고 그 이행을 촉진·검토하기 위하여 협약 당사국 회의체(Conference of the States Parties to the Convention)를 설립함 (제57조)

- (사무국 지원) UN사무총장은 협약 당사국 회의체에 필요한 사무국 서비스를 제공함 (제58조)

〈 사무국의 역할 〉

기능	주요내용
활동 지원	• 당사국총회가 이 협약에 규정된 활동을 수행함에 있어서 보조하고, 이 협약과 관련된 총회의 회기를 위하여 필요한 서비스를 준비하고 제공
정보 제공	• 요청이 있을 경우, 이 협약에서 상정하는 바에 따라 당사국이 당사국총회에 정보를 제공하는 것을 지원
조율	• 관련 국제기구 및 지역기구의 사무국과 필요한 조율을 보장

○ **(발효)** 동 협약은 40번째 비준, 수락, 승인 또는 가입증서가 기탁된 날로부터 90일째 되는 날에 발효 (제65조)

■ 전망 및 시사점

○ 「UN 사이버범죄 방지 협약(안)」은 공식 채택을 위해 UN 총회에 제출될 예정으로, 임시위원회 소속의 당사국이 투표하게 됨에 따라 총회 통과가 가능할 것으로 예상됨

○ 동 협약(안)은 사상 최초로 글로벌 수준의 사이버범죄와 데이터 접근을 방지하기 위한 법적 프레임워크가 확립되었다는 데에 데 의의가 있음

- 사이버범죄에 관한 기존의 국제협약은 2004년 발효된 '사이버범죄에 관한 부다페스트 협약'(The Budapest Convention on Cybercrime)으로, 이는 근본적으로 유럽 중심의 협약에 가까웠음

○ 동 협약(안)은 인권존중(제6조) 및 범죄화(제2장) 등과 관련하여, 협약 당사국 간 첨예한 논쟁이 있었지만 극적으로 합의함

- 중동 등 일부지역 당사국은 인권에 대한 명시적 언급을 원하지 않았지만, 임시위원회는 동 협약(안)이 인권에 미칠 수 있는 영향을 고려하고 다양한 주체의 의견을 수렴하여 인권 조항을 명시함

- 러시아 등 일부 당사국은 테러관련 범죄 등 보다 광범위한 범죄 형태를 규정하고자 했지만, 합의 과정에서 정보통신기술 시스템의 불법 접근 등 사이버상의 범죄유형을 11가지로 규정함

○ 동 협약(안)과 관련하여 다수의 인권단체 및 빅테크 기업은 우려의 입장을 표명함

- 디지털 비영리 단체, 액세스 나우(Access Now)의 아시아 태평양 정책 책임자(Raman Jit Singh Chima)는 '이번 협약(안)이 개인에 대한 국경없는 감시를 가능케 하는 동시에, 과도한 데이터 접근을 가능하게 할 수 있다'고 언급

- 마이크로소프트(Microsoft) 등 150개 이상의 글로벌 기술기업이 속한 연합체, 사이버보안 테크 어코드(Cybersecurity Tech Accord)의 대표들은 인터넷 서비스 제공사 등이 관할권 간 데이터 공유를 강요당할 가능성을 제기하며 우려의 목소리를 표명

Reference

▪https://documents.un.org/doc/undoc/gen/v24/055/06/pdf/v2405506.pdf
▪https://unis.unvienna.org/unis/pressrels/2024/uniscp1180.html
▪https://therecord.media/un-cybercrime-treaty-passes-unanimous
▪https://www.scientificamerican.com/article/0724--un-cybercrime/
▪https://www.euronews.com/next/2024/08/09/un-approves-first-cybercrime-treaty-despite-widespread-opposition
▪https://cyberpeaceinstitute.org/news/cybercrime-convention-adopted/