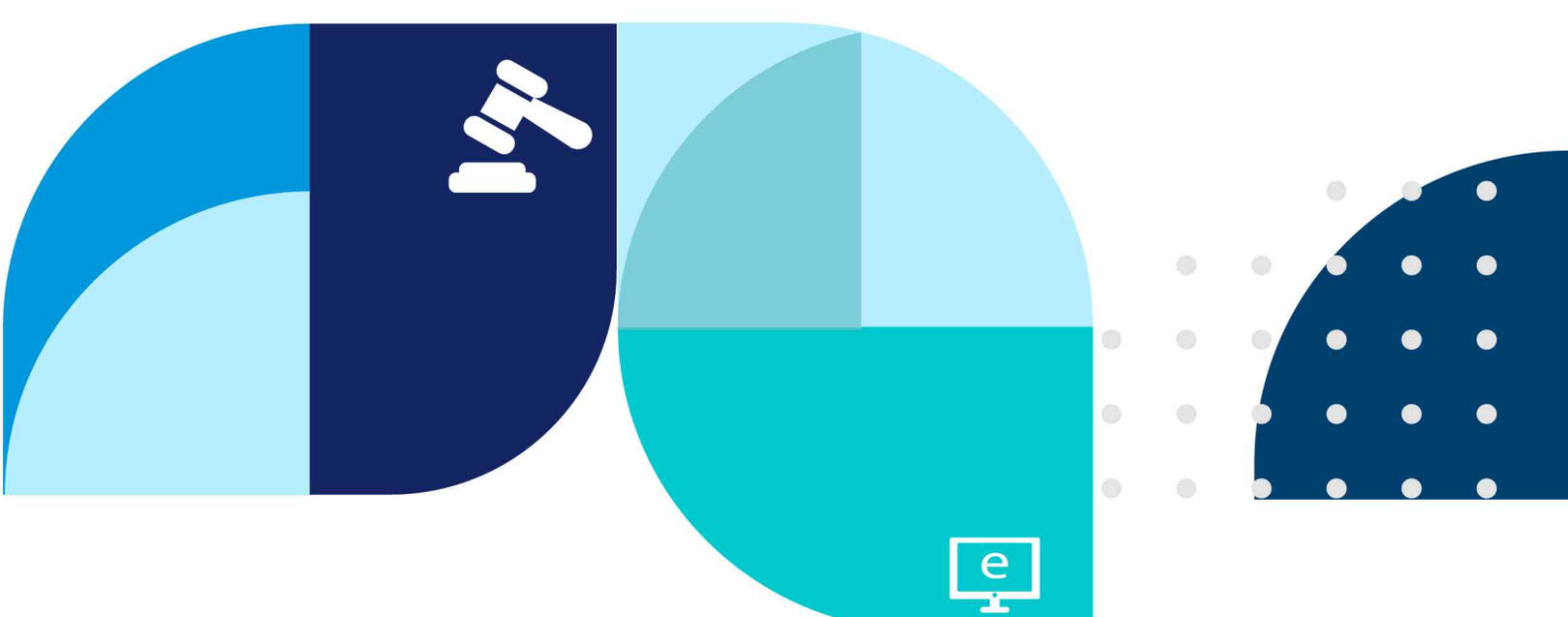
인터넷·정보보호 법제동향

Vol. 206 | November 2024



KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

Vol. 206 | November 2024

Contents

국내 입법 동향

〈발의된 법률안〉

해외 입법 동향

〈EU〉

〈호주〉

〈독일〉

〈영국〉

〈미국〉

국내 입법 동향 요약

■ 발의된 법률안

법령명	발의일	주요내용
「인공지능 발전과 신뢰기반 조성 등에 관한 기본법안」 대안 (과학기술정보방송통신위원회)	2024. 11. 26.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** AI의 건전한 발전을 지원하고 AI 사회의 신뢰 기반 조성에 필요한 기본적인 사항을 규정 • **(주요내용)** – (기본계획) 과기정통부장관은 3년마다 정책방향, 전문인력 양성, 신뢰기반 조성 등을 포함한 AI 기본계획을 수립·시행해야 함 – (안전연구소) 과기정통부장관은 AI 안전을 확보하기 위하여 인공지능안전연구소를 운영할 수 있음 – (고영향 AI) AI 사업자는 고영향 AI 또는 이를 이용한 제품 및 서비스를 제공하는 경우, 안전성 및 신뢰성 확보조치를 이행 – (시정조치 등) 과기정통부장관은 소속 공무원으로 하여금 의무를 위반한 AI 사업자에 대하여 조사, 시정 등의 조치를 명할 수 있음
「인공지능 발전과 산업기반 조성 등에 관한 법률안」 제정법률안 (성일종 의원 등 10인)	2024. 11. 20.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** AI 발전을 지원하고 AI 산업기반을 조성하기 위하여 필요한 기본사항을 규정 • **(주요내용)** – (기본계획) 과기정통부장관은 3년마다 정책방향, 신뢰기반 조성, 산업진흥 등을 포함한 AI 기본계획을 수립·시행해야 함 – (사업지원) 정부는 AI 기술개발 활성화 등을 위하여 국내외 동향 및 제도조사, 인프라 확충 및 접근성 개선사업 등을 지원 – (집적화) AI 산업 진흥을 위한 기반시설, 단지의 기능적·물리적·지역적 집적화를 추진할 수 있도록 함 – (고위험 AI) 고위험 AI 관련 개발사업자와 이용사업자를 구분하여 AI 신뢰성과 안전성을 확보하기 위한 조치를 취하도록 함
「위치정보의 보호 및 이용 등에 관한 법률」 일부개정법률안 (김상욱 의원 등 10인)	2024. 11. 8.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** 일부 위치정보사업자의 경우, 긴급구조 요청 시 개인정보보호를 이유로 개인위치정보를 제공하지 아니하는 등 긴급구조의 사각지대 존재 • **(주요내용)** – (위치정보사업자의 의무) 긴급구조기관 또는 경찰관서로부터 긴급구조를 위한 개인위치정보 제공 요청을 받은 위치정보사업자의 정보제공 의무 규정 – (벌칙 및 과태료) 위치정보사업자가 의무를 위반한 경우, 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하도록 함

법령명	발의일	주요내용
「위치정보의 보호 및 이용 등에 관한 법률」 일부개정법률안 (윤준병 의원 등 10인)	2024. 11. 26.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** 치매환자의 경우 실종 등 각종 위험에 노출되어 있음에도 보호자가 직접 개인위치정보를 요청할 수 없고 긴급구조를 요청한 경우에 한하여 개인위치정보가 제공되는 실정 • **(주요내용)** – (위치정보 이용대상 확대) 8세 이하의 아동등의 보호를 위한 위치정보 이용의 대상에 「치매관리법」 제2조제2호에 따른 치매환자에 해당하는 자를 추가
「개인정보보호법」 일부개정법률안 (김태호 의원 등 12인)	2024. 11. 18.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** 국내에 주소 또는 영업소가 없는 개인정보처리자의 국내대리인 지정요건에 운영방식에 대한 별도의 규정이 부재 • **(주요내용)** – (국내대리인의 지정) 개인정보처리자가 국내법인을 설립·운영 중인 경우 해당 법인을 국내대리인으로 지정 – (과태료 부과) 국내대리인 지정 요건을 충족하지 아니하거나 개인정보 처리방침에 국내대리인의 전화번호 등을 포함하지 아니한 경우에 과태료 부과
「개인정보보호법」 일부개정법률안 (백혜련 의원 등 10인)	2024. 11. 27.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** 현행법은 완전히 자동화된 결정에 대하여만 정보주체의 거부권 등을 허용하고 있어 실질적으로 AI를 활용하여 처리되는 개인정보 보호에 한계가 있다는 지적 • **(주요내용)** – (자동화된 결정에 대한 정보주체의 권리 등) 완전히 자동화된 시스템이 아닌 어느 정도 사람의 개입이 이뤄지면서 자동화된 결정이 발생하는 경우에도 정보주체가 거부권 등을 행사할 수 있도록 하여, 정보주체의 개인정보자기결정권을 강화

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 게이터 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

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	

주요내용
7. 사이버보안 위험관리 조치의 효과성 평가
• 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 CISO[5]를 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

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
5 정보보호 최고책임자(Chief Information Security Officer)

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

- (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

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

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 고지'를 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

- 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)

○ **(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 지침**을 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

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/

붙 임 컴퓨터 범죄 관련 「형법」 개정안 신구조문 대비표

현행법	개정안
· 제202a조 (데이터 감시 행위)	· 제202a조 (데이터 감시 행위)
- **(제1항)** 보안을 뚫고 자신의 것이 아니거나 부당한 접근으로부터 보호되는 데이터에 권한 없이 접근 또는 3자에 접근권을 제공한 자는 3년 이하의 징역 또는 벌금형에 처함 - **(제2항)** 제1항의 의미에서 데이터는 전자적, 자기적 또는 기타 즉각적으로 인지할 수 없는 방식으로 저장되거나 전송되는 것만을 지칭	좌 동
〈 신 설 〉	- **(제3항)** 다음 행위는 제1항의 권한 없는 행위에 해당하지 않음 1. 정보기술 시스템의 취약점, 기타 보안위험을 식별하려는 의도로 수행된 행위, 그리고 식별된 보안 취약점에 대한 정보를, 취약점을 해소하거나 이를 위탁할 수 있는 위치에 있는 책임기관, 즉 해당 정보기술시스템 책임자, 시스템 운영 서비스 제공자, 해당 IT 애플리케이션 제조업체 또는 연방 정보기술 보안청(BSI)의 책임자 등에 고지하려는 의도를 가진 행위 2. 보안 취약점 식별에 필수불가결한 행위 - **(제4항)** 제1항의 특히 심각한 사건에는 3개월 이상 5년 이하의 징역에 처하며 특히 심각한 사건은 일반적으로 다음 행위를 지칭 1. 대규모 자산 손실을 초래하거나 2. 영리 추구, 상업적 이유로 범행하거나 이러한 행위를 지속적으로 영위하기 위한 범죄단체의 일원으로서 행한 경우 3. 핵심인프라의 가용성, 기능, 무결성, 신뢰성 또는 기밀성을 해치거나 독일 연방 공화국 또는 연방주의 안보를 침해한 경우
· 제202b조 (데이터 탈취 행위)	· 제202b조 (데이터 탈취 행위)
- 승인 없이 기술적 수단(제202a조제2항)을 사용하여 비공식 데이터 전송 또는 데이터 처리 시스템의 전자파 방사로부터 자신의 것이 아닌 데이터를 획득 또는 3자에 전달한 자는 더 무거운 형량을 부과할 기타 조문에 해당하지 않는 한 최대 2년의 징역형 또는 벌금형에 처함	- (제1항) 좌 동 - (제2항) 제202a조 제3항 및 제4항 적용

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 국가안보나 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

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

구분	주요내용
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
	- 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

인터넷·정보보호 법제동향
Vol. 206 (November 2024)

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

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