효과적인 ICT보안 위협 대응을 위한 법률·제도적 제언

이근우 법무법인 화우 파트너

1. 머리말

급속한 ICT 발전, 폭발적인 데이터 증가로 인해 사이버 보안 위협이 더욱 복잡해지고 있다. 특히 AI를 활용한 공격이 발생하고, 공급망에 대한 공격이 빈발하면서, 보안의 중요성이 그 어느 때보다 강조되고 있다.

사이버 위협은 그 방법이 다양해지고, 타깃 역시 확대되는 추세다. 이에 대응하기 위해선 역시 보안 방법과 보호 대상을 확대할 필요가 있다. 더욱이 사이버 위협이 민·관을 가리지 않고 있는 이상, 그 대응을 위해 민간과 정부의 협업·협력이 더 긴밀해져야 한다.

더 나아가, 사이버 세계엔 국경의 장벽이라는 것이 무의미하기에, 좀 더 확고하고 적극적으로 국제협력을 확대해야 한다. 민간의 경우, 아무리 보안 실무·담당자가 심각성을 인지하고 전력을 다해도, 소위 C-레벨이라고 하는 경영진의 보안 인식이 낮고 보안 강화에 대한 의지가 없다면, 제대로 된 성과를 거둘 수 없다. 이는 지금까지 여러 통계, 자료, 경험을 통해 널리 알려진 바이며, 그러므로 경영진의 보안 인식과 보안 강화에 대한 의식제고가 무엇보다 중요하다. 이러한 문제의식을 바탕으로 ICT 발전과 데이터 증가에 따른 보안 위협에 효과적으로 대응하기 위한, 법률·제도적 방안을 정리해 본다.

2. 보안 강화AI 시스템에 대한 규제 완화 및 독려를 위한 입법 필요성

디지털 시대의 AI는 다양한 분야에서 활용되고 있는데, 불행하게도 사이버 위협의 큰 축으로도 사용되고 있다. 반대로 말하면, AI가 사이버 보안 분야서 획기적이면서도 폭넓게 사용될 수 있다는 의미다. 예를 들어, AI·머신러닝 기술을 활용한 위협 탐지 시스템을 구축해 실시간으로 네트워크 트래픽을 분석하고, 이상징후를 빠르게 감지하는 방법이 있다. 이러한 시스템은 패턴 인식을 통해, 기존엔 알려지지 않았던 새로운 위협을 탐지할 수 있다.

AI를 활용해 추가 대응체계를 구축하는 것도 중요하다. 즉, AI를 활용한 자동화된 대응 체계를 도입해, 사이버 보안 위협을 감지하면 자동으로 대응 절차가 실행되도록 하는 것이다. 예를 들어, 의심스럽거나 비정상적인 활동이 감지되면 즉시 해당 네트워크를 격리하거나, 공격을 차단하는 등의 조치를 자동으로 취하게 된다.

위와 같은 AI 기반 보안강화 시스템의 경우, 현재의 AI 규제 트렌드와는 그 궤를 달리할 필요가 있다. 즉, 불필요한 규제를 줄여 그 활용을 장려하는 방식의 입법이 필요하다는 것이다.

현재 EU(유럽연합, European Union)에선 인공지능법(AI ACT)이 발효돼 EU 역내 국가들은 관련 법률을 제정해야 한다. 반면, 우리나라에선 AI 시스템을 규율하는 법제도가 아직 정립되지 않았다. 지난 21대에 이어, 22대 국회에서도 다양한 AI 법률안들이 제안된 상태인데, 주로 규제를 중심으로 이용자 보호에 그 초점이 맞춰져 있다. 실제 김성원, 안철수, 정점식, 조인철 의원이 각각 대표발의한 22대 국회 AI 관련 주요 입법안을 살펴보면, 대부분 AI를 '금지 AI, 고위험 AI, 생성형 AI'로 나누고, 그에 따라 규제 정도를 달리하는 내용이다.

하지만 AI 기반 보안강화 시스템은, 어떠한 경우로 보더라도, 그 효과와 목적이 사람의 생명, 신체, 기본권에 위협이 되는 것이 아니라 그러한 위협으로부터 사람의 재산권, 기본권을 지켜주는 것이다. 결국 사이버 위협에 효과적으로 대응하기 위한 사이버 보안의 주요 수단으로서, AI 기반 보안강화 시스템은 널리 사용될 필요가 있다. 특히 그 효과와 목적이 사람의 생명, 신체, 기본권 보호에 맞춰져 있는 이상, 장려를 위해서라도 불필요한 규제를 없애는 방식의 입법이 필요하다고 생각한다.

3. CISO의 실질적 지위·역할 보장을 위한 이사회보고 정례화

3.1 CISO의 현행법상 역할

정보통신망이용촉진 및 정보보호 등에 관한 법률(정보통신망법), 전자금융거래법 등 우리나라 현행법은 기업에 CISO(정보보호최고책임자, Chief Information Security Officer)를 임명하도록 하고 있다. 이 중 정보통신망법에선, 동법 제45조의3을 통해 '정보통신서비스 제공자에게 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위해 일정한 기준에 해당하는 임직원을 CISO로 지정하고 과학기술정보통신부 장관에게 신고'하도록 명시하고 있다. 이에 더해, 일정규모 이상에 해당하는 정보통신서비스 제공자의 경우, CISO 업무를 겸직할 수 없다.

CISO의 업무는 정보보호 계획의 수립·시행 및 개선, 정보보호 실태와 관행의 정기적인 감사 및 개선, 정보보호 위험의 식별 평가 및 정보보호 대책 마련, 정보보호 교육과 모의 훈련 계획의 수립 및 시행을 총괄하는 것이다. 그리고 CISO는 정보보호산업의 진흥에 관한 법률 제13조에 따른 정보보호 공시에 관한 업무, 정보통신기반 보호법 제5조 제5항에 따른 정보보호책임자의 업무, 전자금융거래법 제21조의2제4항에 따른 정보보호최고책임자의 업무, 개인정보보호법 제31조 제2항에 따른 개인정보보호책임자의 업무도 같이 수행할 수 있다.

정보통신서비스 제공자는 침해사고에 대한 공동예방 및 대응, 필요한 정보의 교류, 그 밖에 대통령령으로 정하는 공동의 사업을 수행하기 위해 CISO를 구성원으로 하는 협의회를 구성·운영할 수 있다. 그리고 정부는 CISO 협의회의 활동에 필요한 경비의 전부 또는 일부를 지원할 수 있다.

3.2 CISO의 실질적 지위·역할 보장을 위한 이사회 보고 정례화 입법 필요성

이처럼 여러 법률에서 CISO의 역할, 활동, 자격을 규정하고 있다. 그럼에도 불구하고, 기업의 최고 경영진 레벨, 소위 C-레벨이 낮은 보안 인식 수준을 갖거나 보안 필요성을 느끼지 못한다면, 성과를 제대로 거두지 못하는 경우가 빈번하다. 결국 기업 보안 문제에선, 다른 무엇보다 최고 경영진 레벨의 보안 인식 전환과 실천 의지가 중요하다. 결정적으로 기업 정보보호 거버넌스의

최종 책임자는 이사회이지 CISO가 아니다.
그러한 점에서, CISO를 임명한 것으로 정보보안 거버넌스의 책임자인 이사회의 업무가 마무리되는 것은 아니다. CISO의 업무인, 정보보호 계획 수립·시행·개선, 정보보호 실태와 관행의 정기적인 감사 및 개선, 정보보호 위험의 식별 평가 및 정보보호 대책 마련, 정보보호 교육과 모의훈련 계획 수립·시행이 요식적인 행위로 진행될 수 있기 때문이다. 단순히 법률요구 사항을 충족한 것으로는 충분하지 않다.
결국 기업은 CISO 임명에 그치지 않고, 최소한 법에서 CISO에게 명한 업무를 제대로 수행할 수 있도록 CISO의 지위와 업무를 보장해야 한다. 특히 최고 경영진의 보안 의지가 중요하다는 점에서, CISO가 경영진 및 이사회를 대상으로 정기적인 보안 교육과 훈련을 실시해, 경영진 인식을 제고하는 한편 보안 대응능력을 강화하는 것이 중요하다.
이러한 CISO 지위·업무 보장을 위해선, 현행법처럼 단순히 CISO 자격을 법률로 규정하고, 특정 규모 이상 기업에서 그 겸직을 금지하는 것만으론 충분치 않다. 더 나아가 CISO 업무가 정기적으로 이사회에 보고될 수 있도록, 제도적인 보완이 필요하다. 이를 통해 CISO는 비로소, 이사회로 대변되는 경영진에게 '보안 투자 및 전략적 결정'과 관련해 적절한 조언과 역할을 할 수 있게 될 것이다.

4. 민관 협력 강화

4.1 사이버 위협 정보 공유 플랫폼 구축

사이버 보안은 정부와 민간의 경계를 가리지 않는다. 그러한 점에서 사이버 위협에 효과적으로 대응하기 위해선 정부와 민간 기업의 원활한 협업이 필요하다. 이러한 협업 방법 중 하나가, 사이버 위협 정보를 정부와 민간 기업이 실시간으로 공유하는 플랫폼 구축이다. 참고로 현재 민간의 경우, 여러 산업에 걸쳐 광범위하게 발생하고 있는 침해사고에 대응하기 위해, C-TAS라는 플랫폼을 2014년부터 운영하고 있다. 현재 보안, 금융, 전자상거래, 호스팅 등 다양한 분야기업이 참여해 위협정보를 공유하고 있다.
보안에 있어서도, 정부와 민간 기업 간 이러한 플랫폼이 마련된다면 큰 도움이 될 것으로 예상된다. 이를 통해 다양한 사이버 위협 정보가 신속하게 공유되고, 중요 사이버 위협이나 사이버 보안 이슈에 대해선 민관이 효과적으로 공동 대응할 수 있다.

4.2 보안 법률 및 규제의 합목적적 접근 방식

AI, 클라우드, 사물인터넷(IoT)과 같은 다양한 환경은 디지털 보안에 대한 두 가지 견해를 불러온다. 국가 중심의 규제 위주가 우선이냐, 기업 자율성을 강조하는 방향이 우선이냐는 것이다. 어느 방향으로 가야 할 것인지에 대해, 현재 명확한 컨센서스가 존재한다고 보긴 힘들다. 다만 국내 디지털 보안의 경우, 특정 영역에선 국가 중심 규제·인증이 이미 표준으로 자리잡은 동시에, 다른 특정 영역에선 기업 자율성을 강조하는 방향으로 나아가는 경향성을 보이고 있다.
전자의 예로, CSAP(클라우드 서비스 보안인증, Cloud Security Assurance Program)를 들 수 있다. CSAP는 '클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률' 제23조의2에 따라, 정보보호 수

준 향상 및 보장을 위해 클라우드 컴퓨팅 서비스에 대한 보안인증을 수행하는 제도다. CSAP의 목적은 국가·공공기관에 안전성 및 신뢰성이 검증된 민간 클라우드 서비스를 공급하는 동시에, 객관성·공정성을 바탕으로 이용자의 보안 우려를 해소하는 것이다. 이를 통해 클라우드 서비스 경쟁력을 확보하는 것도 중요한 목표다.

후자의 예로는, 금융보안규제 선진화를 들 수 있다. 현재 금융당국은 디지털 금융혁신을 뒷받침하면서 리스크에 효과적으로 대응할 수 있는 금융보안규제 선진화 방안을 마련하고 있다. 이를 구체화하기 위해, 우선 금융회사 등이 전사적 차원에서 금융보안을 준수하고, 자율보안체계를 구축할 수 있도록 규율체계를 개선해 나가고 있다. 이를 바탕으로 금융회사 등은 보안리스크를 스스로 분석·평가하고, 그에 비례해 보안방안을 수립할 수 있는 리스크 기반 '자율보안체계'로의 전환을 추진하고 있는 것이다.

최근 이를 위해 제시된 것이 전자금융감독규정 개정안이다. 이는 금융회사가 스스로 새로운 리스크에 대응할 수 있도록, 293개에 달하는 세세한 행위규칙(Rule)을 166개로 획기적으로 줄인 것이다. 더불어, 규정 형식도 원칙과 목적을 제시하고 나머지 세세한 부분은 금융회사가 스스로 결정하는 방식을 취하고 있다.

다만 정부가 규제의 틀과 기준을 세우고, 기업이 이를 준수한다는 일반적인 모습엔 변함이 없다. 원칙론적으로 정부가 적응력을 바탕으로 디지털 시대에 맞는 보안 관련 법률·규제의 기준을 세우고, 기업이 그에 따라 보안 기준을 준수해야 한다는 점은 부인할 수 없다. 예를 들어, 정부는 중요한 인프라를 운영하는 기업에 정기적인 보안 점검과 침투 테스트를 상황에 맞게 수행하도록 법적 의무 내지 기준을 세우고, 기업이 이를 제대로 준수할 수 있도록 독려하는 것이다. 물론 그 과정에서 과도한 규제가 되지 않도록 정부가 해당 기업 내지 업계 의견을 제대로 수렴해야 한다. 다양한 사이버 위협이 빈발하고, 일률적인 규제로 이에 탄력적으로 대응하는 것은 어렵다. 이 때문에 우리는 해당 산업 분야의 중요성, 기업의 전반적인 보안 수준, 기술발전 속도, 트렌드 등을 종합적으로 고려해야 한다. 이를 바탕으로, 특정 분야의 경우 정부가 더욱 주도적으로, 다른 특정 분야의 경우 기업이 자율성을 더 발휘할 수 있도록, 합목적적이면서 현실 적응성을 가지고 규제에 접근하는 것이 필요하다.

4.3 국제협력 강화

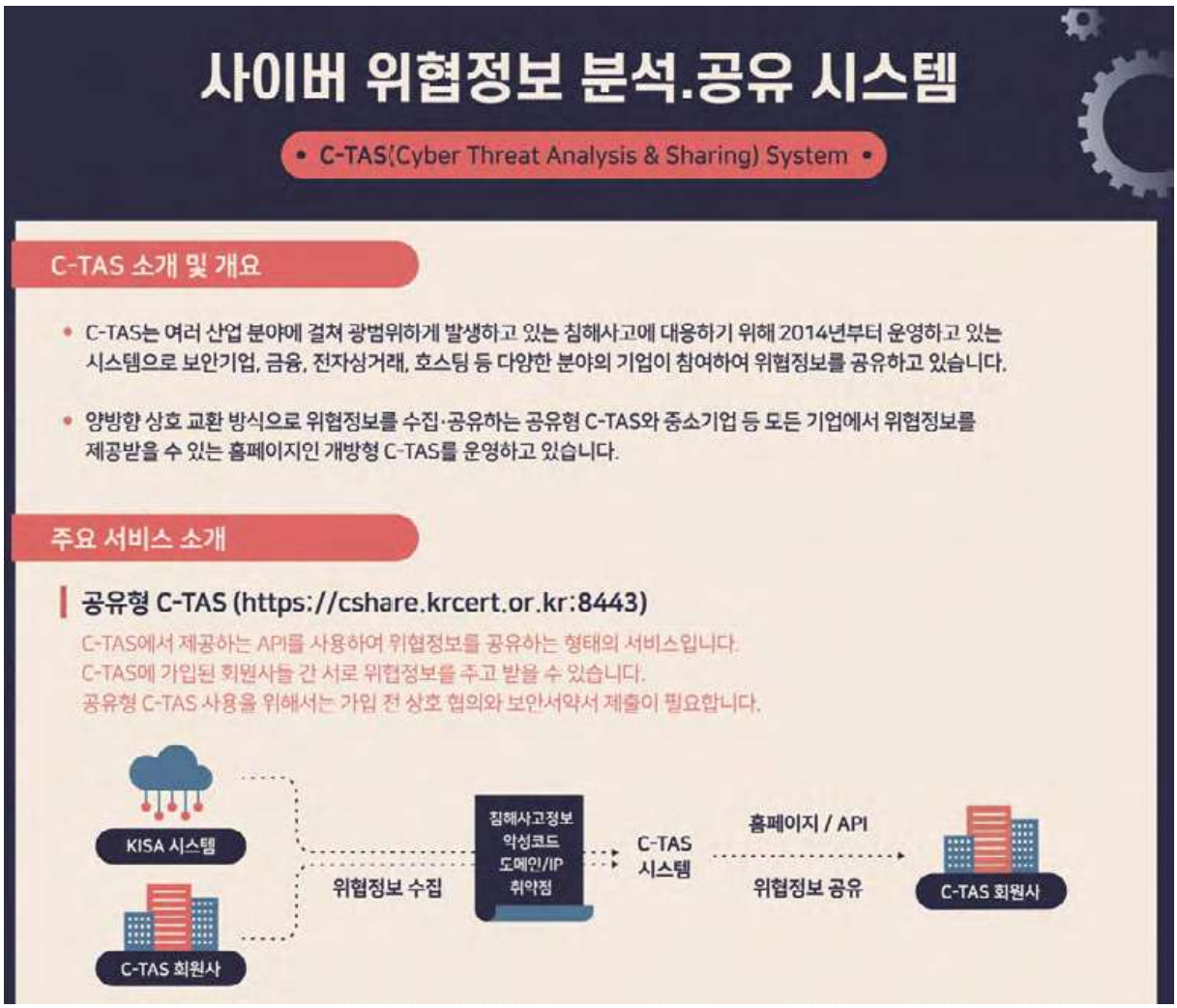
사이버 보안은 국가 간 경계가 없다. 그리고 중요한 사이버 보안 이슈가 외국에서뿐만 아니라 우리나라에서도 동일하게 문제가 되는 경우를 많이 볼 수 있다. 그러한 점에서 사이버 보안을 위해서는 국제적인 협력이 중요하다. 민간의 경우, 자신의 이해관계나 계약상의 지위 등에 따라, 공급망 관점에서 국적을 떠나 상호 협력하는 경우가 많다. 결국 국제협력은 정부가 국제적인 보안 협의체에 적극 참여해, 글로벌 보안 위협에 공동으로 대응하는 체계를 마련하는 것이 중요하다.

5. 맺음말

ICT 발전, 데이터 활용의 혁신적인 증가에 따른 보안 위협은 기업과 정부 모두가 함께 해결해야 할 중요한 과제다. 우리는 AI를 활용한 보안 강화, 이사회와 경영진의 역할 강화, 민·관 협력을

통한 법률·규제 강화 등을 통해 좀 더 안전한 디지털 환경을 구축할 수 있다. 이를 통해 급변하는 사이버 보안 위협에 효과적으로 대응할 수 있을 것이다.

※ 출처: TTA 저널 제214호



[그림 1] C-TAS 소개자료