NOW

일본 산업리포트

경제안보 시대 일본의 사이버보안 전략: 기업의 지정학 인식, 관련 법제도

KJCF (재)한일산업·기술협력재단
www.kjc.or.kr

경제안보 시대 일본의 사이버보안 전략: 기업의 지정학 인식, 관련 법제도

❑ 지정학적 리스크 등의 증대에 따라 경제안보적 관점의 중요성 증대

○ 미중 갈등, 대만 정세불안, 우크라이나 전쟁, 중동 정세불안, 팬데믹 등의 영향으로 지정학적 리스크가 증대하고 있음.

○ 이러한 지정학적 리스크의 증대는 다음과 같은 다양한 경제안보 이슈를 발생시키고 있음.

- 지정학적 리스크 증대에 따라 반도체 부족 문제(공급망 위기), 중요자원 및 에너지 조달 불안의 확대, 핵심 인프라의 자율성 훼손, 부정 수출(이중용도 재화 등), 기술·정보 유출, 사이버 공격 등 다양한 경제안보 이슈가 부상되고 있음.

- 경제 안보적 관점은 미국, 유럽, 일본 등 주요국의 국가 전략(특히, 대외 전략(외교안보정책, 통상정책 등)이나 성장전략 등)에서 그 중요성이 높아지고 있음.

→ 기존 세계화 시대에는 타국과의 경제협력의 심화에 관해서 긍정적 영향(경제적 이익의 획득)을 중시했다면, 미중전략경쟁의 심화나 사이버 공격의 다발 등에 따라 경제의 '분절화', 세계화의 후퇴가 진행되고 있고, 이로 인해, 각국 기업과 정부는 공급망이나 주요 광물 및 에너지 조달, 인프라 구축을 위해 경제성과 더불어 타국에 의존하는 리스크(특히 지정학적 리스크)를 동시에 고려해야 하는 국면에 접어들었음.

○ 세계화의 후퇴, 경제의 분절화는 기업 차원에서 보면 새로운 위협 요인이 될 수도 있고, 새로운 성장동력으로 활용할 가능성도 혼재되어 있음.

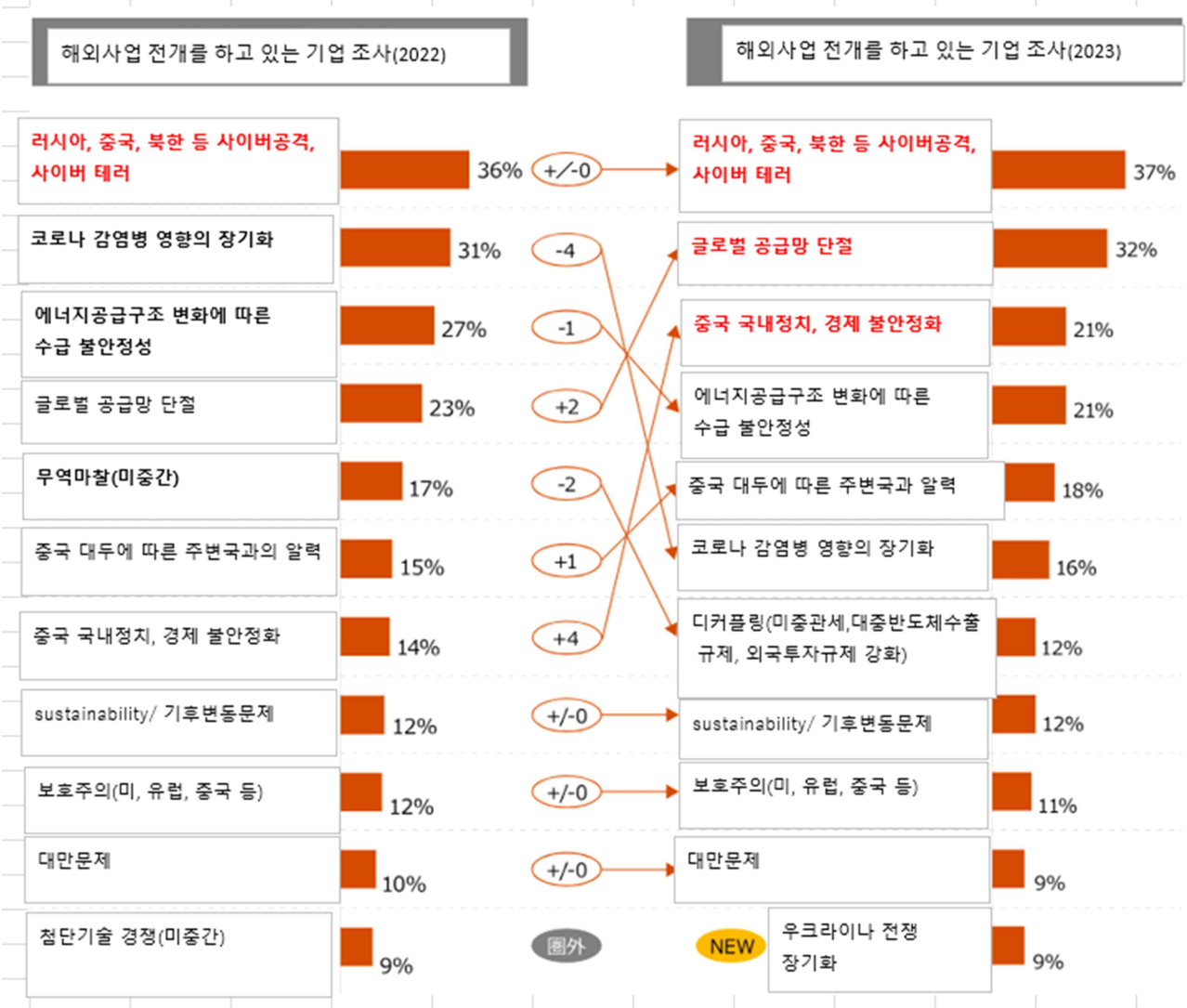
→ 국익 차원에서 추진되는 경제안보 목적은 다양한 업종, 이해관계를 가지고 있는 기업의 목적과 완전히 일치하는 것은 아님. 일반적으로 정부는 국가 전략적 이익을, 기업은 경제적 이익을 우선

❑ 해외사업을 전개하는 기업은 지정학적 리스크를 어떻게 인지하고 있는가?

○ 2023년 8월의 조사에 의하면, 국내사업만 하는 기업군과 해외사업이 있는 기업군을 대상으로 각각 과거 3년간 비즈니스에 관해서 지정학적 리스크에 대한 인식에 대해 질문을 했더니, 전자의 52%, 후자의 72%가 지정학적 리스크가 증대하고 있다고 답변

→ 국내 사업만 기업과 비교하여, 해외사업을 하는 기업이 지정학적 리스크의 증대를 강하게 인지함

<그림 1> 해외사업 전개를 하고 있는 기업의 지정학적 리스크 인식(2022년, 2023년 조사)



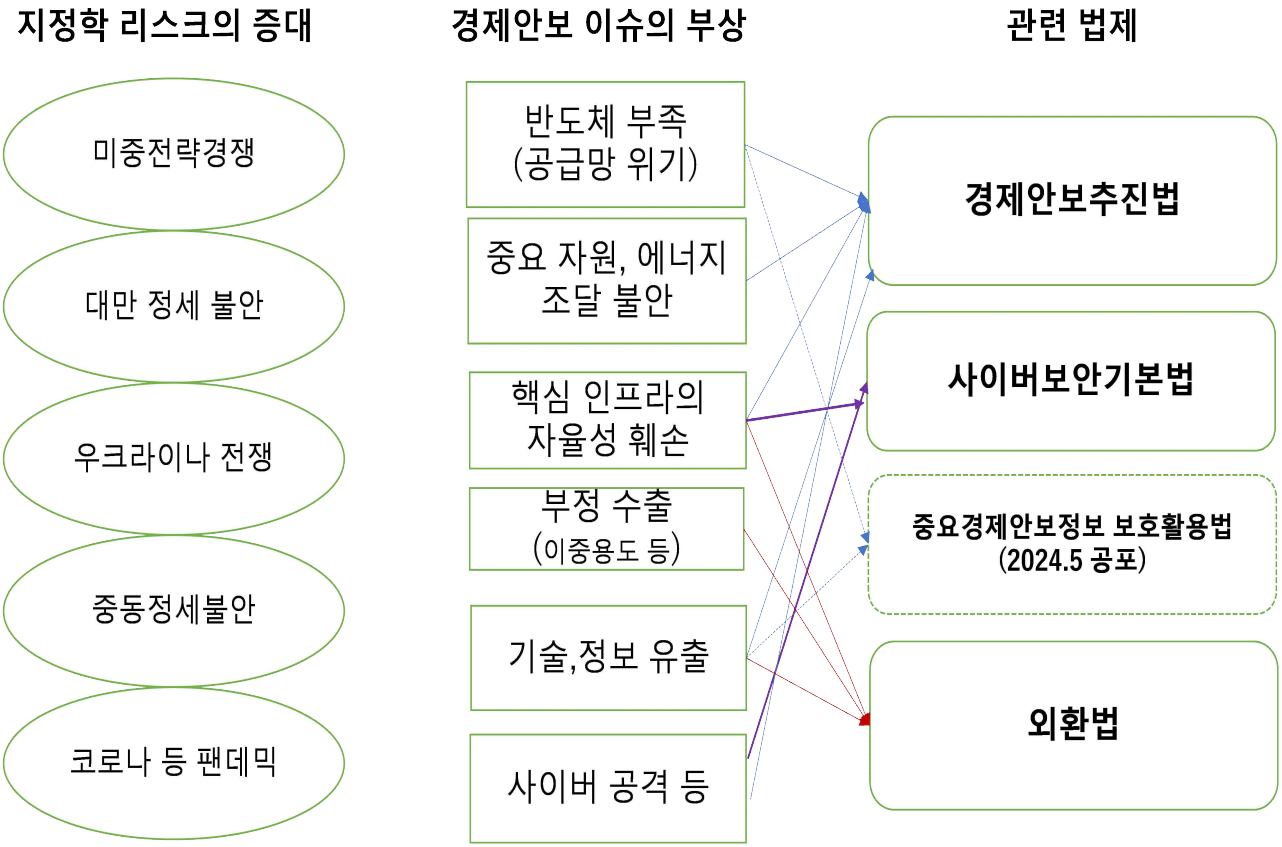
(자료) PwC Japanグループ「企業の地政学リスク対応実態調査2023」2023.8.24.

○ 기업들이 인지하고 있는 지정학적 리스크의 종류에 대해서는

- 2023년 기준으로 러시아, 중국, 북한의 사이버 공격, 사이버테러를 거론하는 기업(37%)이 가장 많음. 다음으로 중국이나 미중갈등 관련 리스크(글로벌 공급망 단절, 중국 국내 정치/경제 불안, 미중 무역마찰, 미중의 보호주의, 대만 문제 등), 에너지 수급 문제, 기후 변동 등 순이었음.

→ 최근 지정학적 리스크에 대한 논의에서 미중전략 경쟁에 주목하는 경향이 강하지만, 2022년 및 2023년 일본 기업 조사에서는 공통적으로 러시아·러시아·북한 등 사이버 공격·테러를 가장 중요한 지정학적 리스크로 간주하고 있음.

<그림 1> 경제안보 이슈의 부상과 일본의 관련 법제



(자료) 저자 작성

경제안보 관련 법제

- 외환법 (1949년 제정)
- 사이버 보안기본법 (2014년 성립)
- 경제안보추진법 (2022년 성립)
- 중요경제안보정보 보호활용법(2024년 5월 성립·공포, 공포 1년 이내로 시행 예정).

경제안보관련 법제 1: 외환법에 의한 수출 관리, 기술 제공 관리

○ 일본 정부는 외환법에 의거하여, 안전보장상 우려가 있는 화물 수출과 기술 제공에 대해서 경제산업대신의 **허가제**로 운용하고 있음.

- 화물 수출의 개념은 비교적 명확하지만, 기술 관리의 대상, 개념은 명확하지 않음.

- 일본에서는 기술관리 시에 국적보다는 거주성을 중시하므로, 외국국적자라 해도, 거주자 요건을 충족하고 있는 경우, 기술관리 대상이 되지 않았음. 이러한 한계를 극복하기 위해 이루어지고 있는 규제가 '간주수출 관리'인데, 거주자가 직접 비거주자에 민감 기술을 제공하는 경우에 한해 허가 신청을 요구했음.

○ 또한, 외환법에 의거하여, 대내직접투자에 대한 심사(審査)부(付) **사전신고제**(재무대신 및 사업소관대신)를 운용하고 있음.

○ 2019년 10월 외환법 개정(2020년 5월 시행)으로 외국에 대한 대내직접투자 관리가 강화되었음.

- 사전신고대상이 되는 주식취득비율을 10%에서 1%로 강화. 단, 지정업종의 대해서도 포트폴리오 투자 등은 사전신고 면제대상으로 간주

○ 2021년 11월 외환법 개정(2022년 5월 시행)을 통해 간주수출관리가 강화되었음(즉, 기술관리 대상이 확대되었음).

- 국경 안에서 거주자에 의한 거주자에 기술 제공이 이루어지는 경우에도, 외국 정부나 외국 법인 등의 지휘, 명령 하에 있는 경우, 외국 정부의 지배하에 있는 경우에는 규제 대상이 된 것임.

경제안보관련 법제 2: 경제안전보장추진법에 의한 공급망 강화, 인프라 안전성 확보 등

○ 2022년 제정된 경제안전보장추진법의 주요 내용을 살펴보면, 중요물자 등의 안정적인 공급 확보(2장), 기간 인프라의 안전성 확보(3장), 첨단 중요기술의 개발지원(4장), 안전보장상 필요에 의한 특허 비공개(5장) 등을 규정하고 있음.

<표 1> 경제안전보장추진법의 주요 내용

장	내 용	비고
제1장 기본방침 책정	안전보장의 확보의 추진에 관한 기본방침을 책정 규제는 경제활동에 주는 영향을 고려하여, 합리적으로 필요한 한도로 실시	
2장 중요물자 안정적 공급 확보에 관한 제도	중요 물자의 안정적인 공급의 확보를 위해 중요물자 지정, 민간사업자 계획의 인정·지원 조치 등을 규정	<공급망 강화> 반도체 등 국내생산을 지원, 단, 조달처 및 보관 상황 등에 대한 공개에 대한 노력 의무
3장 기간 인프라의 안정적 제공 확보에 관한 제도	기간 인프라의 중요 설비의 도입, 유지관리 등 위탁의 사전 조사, 권고/명령 등을 조치	<인프라 안전성 확보> 안보상 위협이 되는 해외제품이나 시스템 국내 도입을 정부가 심사
4장 첨단 중요기술 개발지원에 관한 제도	첨단 중요기술의 연구개발의 촉진과 적절한 활용을 위해, 자금지원, 관민 협력 지원을 위한 협의회 설치, 조사연구 업무의 위탁(싱크탱크) 등 설치	<관민기술협력>민간에 대한 지원, 단 민간에 비밀유지 의무 부과
5장 특허출원의 비공개에 관한 제도	특허에 관한 공개, 유출을 방지하기 위해 외국특허출원 제한 조치	군사이용할 수 있는 민간특허출원은 비공개

(자료) 허재철 등 (2022)『미중 전략경쟁 시대 지정학적 리스크와 경제안보』대외경제정책연구원; 経済安全保障推進法の概要 https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/doc/gaiyo.pdf

❑ 경제안보관련 법제 3: 사이버보안 기본법에 의한 사이버보안 관련 거버넌스 구축

○ 사이버보안 기본법의 재개정

- 2014년 사이버보안기본법이 통과되어, 기존 정부의 사이버보안 전략을 담당해 온 '정보보안정책회의'를 발전시켜서, 내각에 '사이버보안 전략본부'의 설립을 규정
- 또한, 기존 '정보보안정책회의'의 사무국 역할을 담당하던 '내각관방 정보보안센터(National Information Security Center)'를 '내각 사이버보안센터(National center of Incident readiness and Strategy for Cybersecurity)'로 확대 개편. 단, 영문명칭은 NISC로 변동 없음.
- 기존 NISC는 내각관방의 규칙에 의한 조직에 불과하여, 법적 권한의 제약이나 인재 부족 등으로 범정부의 사이버공격에 대응하는 사령탑의 역할을 충분히 못하고 있다는 의견이 강했음. 2014년 사이버보안 기본법 제정으로, NISC의 역할 등을 명시하여, 범정부차원의 사령탑으로 기능할 수 있게 되었음.
- 2015년 일본연금기구의 개인정보 유출 사고가 발생했지만, 기존 사이버보안 기본법에서는 NISC(내각 사이버보안 센터)의 조사 대상을 중앙성청으로 한정하고 있었으므로, 충분한 조사를 할 수 없었음. 이에, 2016년 사이버보안 기본법 개정으로, NISC의 조사대상이 독립행정법인 등으로 확대되었음.
- 2017년 일본을 포함하는 150개국 이상에서 랜섬웨어 공격이 발생함. 또한, 2018년 한국 동계올림픽 등 개최 당시 사이버테러 등이 다수 발생함. 이에, 2020년 도쿄 올림픽 개최 등을 염두에 두고, 2018년 사이버보안 기본법이 개정되어, 사이버보안 협의회(2019년 4월 발족)가 설치됨. 동 협의회는 행정기관, 지방자치단체, 중요 인프라 사업자, 사이버 관련 사업자, 대학·교육연구기관, 유식자 등으로 구성

<표 2> 사이버보안기본법 개요(2022년 6월 시행 기준, 2024년 8월 유효법률)

장	내 용	비고
1조 (목적)	- 사이버 보안에 대한 위협의 심각화 등을 고려하여, 정보의 자유로운 유통을 확보하면서도, 사이버보안 시책에 대한 기본이념을 규정하고, 정부 및 지자체의 책무를 규정 - **사이버보안전략본부의 설치** 등을 통해 사이버보안에 관한 시책을 종합적으로 추진하고, 이를 통해 경제사회의 활력 향상, 안전보장 기여를 목적으로 함	

2조 (정의)	- **사이버보안이란,** 전자적 방식, 자기적 방식 그 밖에 타인의 인식에 의하여 인식할 수 없는 방식(이하 이 조에서 "전자적 방식"이라 한다)에 의하여 기록되거나 송-수신되는 정보의 유출, 멸실 또는 훼손의 방지 그 밖에 해당 정보의 안전관리를 위하여 필요한 조치(정보통신네트워크 또는 전자적 방식으로 만들어진 기록에 관계되는 기록매체를 통한 전자계산기에 대한 부정한 활동으로 인한 피해 방지를 위하여 필요한 조치를 포함)가 이루어지고 그 상태가 적절하게 유지 관리되고 있는 것을 말함
2장 사이버보안 전략 제12조	- 정부는 사이버 보안에 관한 시책을 종합적이고 효과적으로 추진하기 위하여 사이버 보안에 관한 기본계획(이하 '**사이버 보안 전략**'이라 한다)을 수립하여야 함
제17조 (사이버보안협의회)	- 사이버안보전략본부장 및 그 위임을 받은 국무대신은 사이버 보안에 관한 시책의 추진에 관하여 필요한 협의를 하기 위하여 사이버보안협의회를 조직함.
제4장(25조~30조)	- 사이버보안 관련 시책을 종합적이고 효과적으로 추진하기 위해 내각에 사이버보안전략본부(이하 '본부'라 한다)를 설치함(25조). - 본부는 **사이버보안 전략안 작성** 및 실행 추진에 관한 사항, 국가 행정기관, 독립행정법인 또는 지정법인에서 발생한 **사이버보안 관련 중대사고에 대한 대책 평가**(원인 규명을 위한 조사 포함)에 관한 사항 등을 담당함(26조). - 전략본부장은 내각관방장관(28조)으로 하고, 전략부본부장은 해당 사무를 담당하는 국무대신을 임명함.(29조) - 본부원은 국가공안위원회위원장, 디지털대신, 총무대신, 외무대신, 경제산업대신, 방위대신 등으로 구성함(30조)

(자료) https://laws.e-gov.go.jp/law/426AC1000000104

❑ 사이버보안 정책의 거버넌스

○ 사이버보안 정책 거버넌스에서 중추적 역할을 담당하는 기구로서는 사이버보안 전략본부(본부장)가 설치되어 있음. 동 본부는 NSC(국가안전보장회의, 일본의 경제안보전략을 포함하는 안보정책에 관한 중요사항을 심의하는 기관으로 의장은 수상) 및 디지털청(디지털 사회형성의 사령탑, 주임대신은 수상)과 긴밀하게 연계하여, 사이버보안 정책을 추진하고 있음.

○ 사이버보안 전략본부(본부장: 관방장관)의 사무국으로 **NISC(내각사이버보안센터)**가 설치되어 있음. NISC는 **사이버보안 전략본부의 사무국**의 역할과 함께, **사이버보안 정책의 사령탑의 역할을 동시에 담당**

○ 중요 인프라를 담당하는 주무부처(금융청, 총무성, 후생노동성, 경제산업성, 국토교통성)는 해당 중요 인프라 관련 사이버보안을 확보해야 함.

○ 각료 본부원 6성청(경찰, 디지털청, 총무성, 외무성, 경제산업성, 방위성)은 각자 디지털 보완과 관련된 업무를 분담하여 담당하고 있음.

○ 사이버보안 협의회는 관민 등 다양한 주체 간의 정보연계 등을 목적으로 설치되었음.

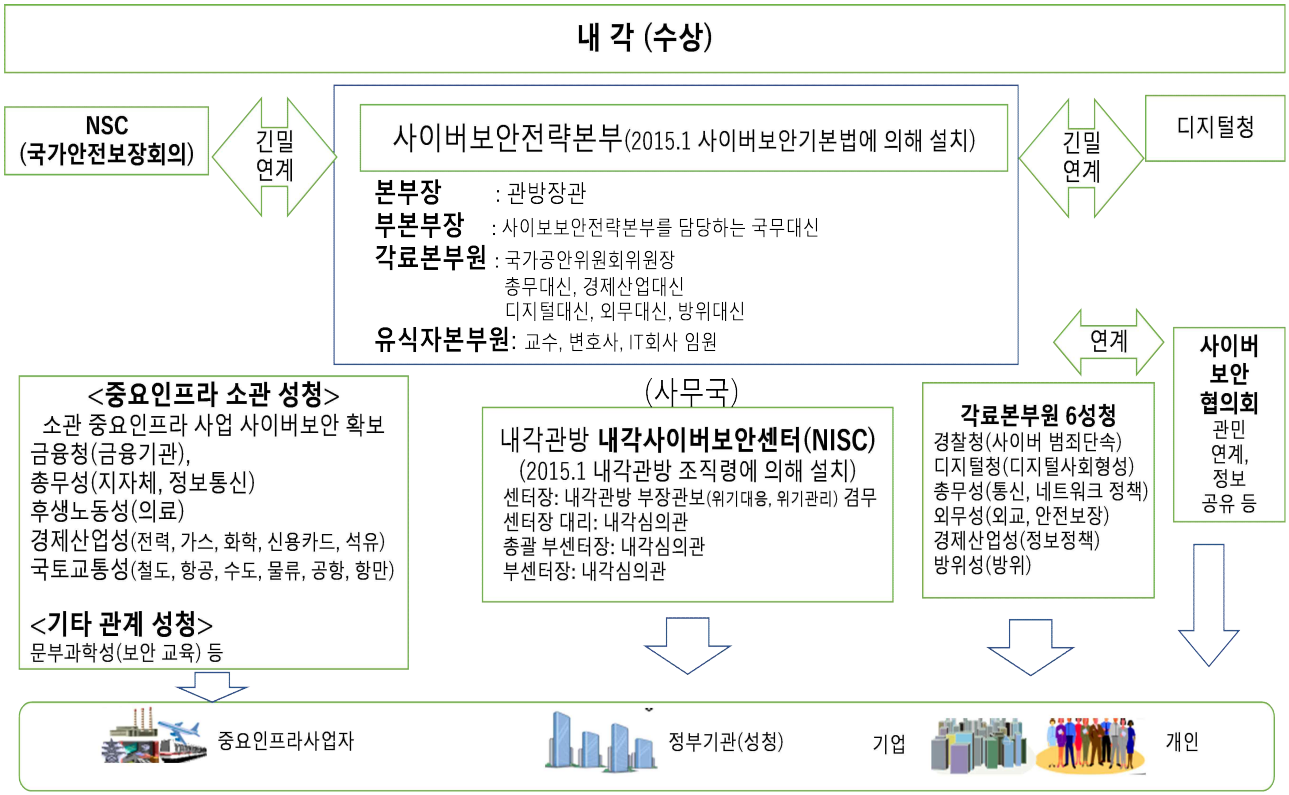
○ 사이버보안 전략본부(본부장: 관방장관)의 사무국 역할을 담당하는 내각 사이버보안 센터(NISC)는 국가안전보장회의(NSC)(의장: 수상)의 사무국 역할을 담당하는 국가안전보장국(NSS)와 긴밀한 협력관계를 구축하고 있음

- 현재 (2023. 5 임명) 스즈키 아츠오(전 방위성 사무차관) 내각관방부장관보(차관급)는 NISC 센터장 및 국가안전보장국 차장을 겸직하고 있음.

※ 내각관방부장관보(차관급)는 내각관방에 3인(내정, 외정, 위기관리)이 있으며, 내각의 중요정책 등 기획입안 및 종합조정을 담당함.

※ 국가안전보장국장 및 내각위기관리감(内閣危機管理監)은 대신정무관급에 해당함.

<그림 2> 사이버보안 정책의 거버넌스(추진체계)



(자료) NISC "サイバーセキュリティ政策の推進体制"

사이버위협의 현황(공안조사청, 사이버 공간의 위협현황 2021)

ㅇ 사이버위협의 현황

- 방위산업 등을 대상으로 하는 사이버 공격
- 코로나 팬데믹 이후 의료분야에 대한 사이버 공격이 증가
- 랜섬웨어 공격의 증가

ㅇ 사이버 공간의 부정한 활동

- 정부, 기업 등의 정보시스템, PC, 스마트폰 등에 침입하여, 정보 탈취, 비밀 감시 증가
- DDoS 공격 등을 통해 정보시스템의 정지, 오작동을 초래, 특히 원전, 핵시설 등 중요 인프라 시설의 피해를 초래할 가능성 증대.
- 은행이나 가상자산 거래소 정보시스템 침입을 통해 예금, 가상자산 등을 부정 획득
- 정보의 조작 등에 의한 심리전(예: 2016년 미국 대선에 대한 러시아의 간섭)

❑ 사이버 위협의 주체(공안조사청, 사이버 공간의 위협현황 2021)

○ 미국, 영국 등의 자료에 의하면, 사이버 위협의 주체로서는 중국, 러시아, 북한의 국가적 관여가 의심되고 있음.

- 특징으로서는 군, 정보기관의 작전으로 실행, 비용을 무시한 집요한 공격, 범죄자나 해커 등을 외부의 협력자, 대리인으로 활용

❑ 사이버보안 기본법과 경제안보추진법의 중요 인프라 관련 규제

○ 사이버보안 기본법과 경제안보 추진법은 공통적으로 중요 인프라를 지정하여, 국민 생활에 필수적인 인프라의 전략적 자율성 확보를 도모하고 있음.

- 사이버보안 기본법과 경제안보추진법에서 제시하는 중요 인프라 사업자의 범위는 기본적으로 거의 비슷함. 정보통신(방송 포함), 금융, 항공, 철도, 철도, 전력, 가스, 수도, 물류는 2개 법률에 공통적으로 중요 인프라로 간주하고 있음. 단, 사이보보안 기본법에서는 정부-행정 서비스(지자체 포함), 의료, 화학을 중요 인프라로 간주하며, 한편, 경제안보추진법에서는 우편을 중요 인프라로 간주함.

<표 3> 사이버보안기본법과 국가안전보장추진법의 중요 인프라 관련 규제

비교 항목	사이버보안기본법	국가안전보장추진법
소관	NISC(내각사이버보안센터)	NSS(국가안전보장국)
법률내 호칭	중요사회기반사업자	특정사회기반사업자
통상적인 명칭	중요인프라사업자	기간인프라사업자
정의	국민생활 및 경제활동의 기반으로서 그 기능이 정지되거나 저하될 경우 국민생활 또는 경제활동에 중대한 영향을 미칠 우려가 있는 것에 관한 사업을 하는 자	국민생활 및 경제활동의 기반이 되는 서비스로서 그 안정적 제공에 지장이 발생할 경우 국가 및 국민의 안전을 저해할 우려가 있는 서비스

규정되어 있는 업종	정보통신(방송 포함), 금융, 항공, 철도, 철도, 전력, 가스, 정부-행정서비스(지자체 포함), 의료, 수도, 물류, 화학, 신용카드 및 석유 등 13개 분야 (정보보안정책회의, 2014, "중요 인프라 정보보안 대책에 관한 제3차 행동계획")	전기, 가스, 석유, 수도, 철도, 화물 자동차운송, 해양운송, 항공운송, 공항, 전기통신사업, 방송, 우편, 금융, 신용카드

(자료) "経済安全保障推進法をサイバーセキュリティ視点でとらえる~企業が備えるべきポイントを解説~"

○ 중요인프라사업자에 대해서는 사이버 보안 상 관리를 강화하고 있음.

- 사이버보안기본법 제14조에서는 중요 인프라 사업자에 대한 사이버보안 확보의 촉진을 규정하고 있음.
- 중요 인프라에 대해서 기능보장의 관점에서 사이버 공격이나 자연재해 등에 기인하여 중요 인프라 서비스 장애의 발생을 최소화하고, 문제 발생 시에는 신속한 복구가 가능하도록 경영층의 적극적인 관여 하에 정보보안 대책을 추진해야 함(중요 인프라 정보보안 대책에 관한 제4차 행동계획, 2017년)

○ 중요 인프라사업자에 대해서는 경제안보추진법에 의한 관리가 강화되었음.

- 경제안보추진법에서는 중요 인프라사업자가 해외제품이나 시스템을 국내에 도입하는 경우, 소관 성청의 심사를 받아야 함.

❑ 중요경제안보정보 보호 및 활용에 관한 법

○ 동법은 2024년 5월 성립/공표, 공포 후 1년 이내 시행 예정

○ 주요 내용

- 중요경제안보의 정의를 제시하고, 동 정보를 취급하는 직원의 범위를 지정하고 있음.
- 중요경제안보 정보를 타 행정기관, 의회, 적합사업자 등에 제공하는 기준을 제시
- 중요경제안보정보 취급자의 제한 및 벌칙을 규정

<표> 중요 경제안보 정보보호 및 활용법 개요

개요	내용
중요경제안보정보 지정	- 중요경제안보 정보란 중요 경제기반(중요 인프라 및 물자 공급망)에 관한 일정한 정보 중 공개되지 않은 정보 중 유출 시 국가 안보에 지장을 초래할 우려가 있어 특별히 비밀로 할 필요가 있는 정보(구체적 예: 사이버 위협 및 대책 관련 정보, 공급망 상의 취약성 관련 정보, 공급망의 취약점 관련 정보) - 중요경제안보정보의 취급 업무를 수행하게 하는 직원의 범위를 정하는 등 해당 정보의 보호에 관하여 필요한 조치를 취함. - 지정 유효기간은 5년 이내. 연장 가능하나 원칙적으로 30년을 초과할 수 없음.
중요경제안보정보 제공	- 행정기관의 장은 다른 행정기관이 이용할 필요가 있다고 인정하는 경우, 중요 경제안보정보를 제공할 수 있음. - 안전보장에 현저한 지장을 초래할 우려가 없다고 인정하는 경우 등에는 국회나 법원 등에 중요경제안보정보를 제공할 수 있음. - 중요 경제기반의 취약성 해소 등 일본의 안전보장 확보에 기여하는 활동을 촉진하기 위해 필요하다고 인정하는 경우, 적합사업자(정령으로 정하는 보전기준에 적합한 사업자)와의 계약에 따라 중요경제안보정보를 제공할 수 있음.
중요경제안보정보 취급자 제한	- 중요경제안보정보 취급 업무는 적격성 평가에서 중요경제안보정보를 누설할 우려가 없다고 인정된 자로 제한.
적성 평가	- 행정기관의 장은 본인의 동의를 얻은 후 내각총리대신에 의한 조사 결과에 따라 유출의 우려가 없는지에 대한 평가(적격성 평가)를 실시(적격성 평가의 유효기간은 10년)함. - 중요경제안보정보를 취급하는 적합업종 종사자에 대해서도 동일한 조사·평가를 실시함.
벌칙	- 중요경제안보정보 유출 시 5년 이하의 징역 또는 5억원 이하의 벌금 또는 이를 병과하는 벌칙 등 정비

(자료) 内閣府. 2024.“重要経済安保情報の保護及び活用に関する法律の概要”'의 개정판을 발표하고 있음. 최근에는 23.3월에 2022년 판을 발표

끝