발 간 등 록 번 호
11-1030000-000020-01

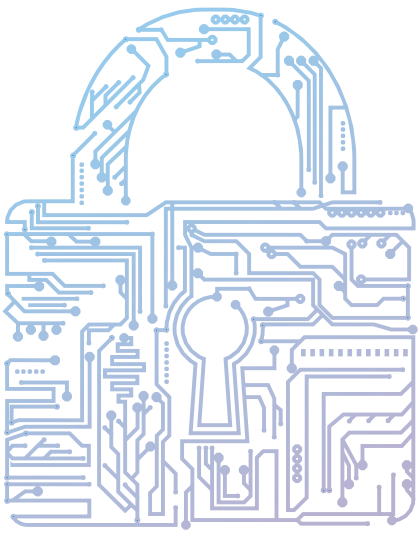
2024

국가 사이버안보 기본계획

2024

관계부처 합동

2024. 9



2024

국가 사이버안보 기본계획

2024

CONTENTS

목 차

Ⅰ 수립 배경

01 사이버안보 환경 변화에 대한 인식 ····· 08

02 「국가 사이버안보 전략」의 이행 ····· 09

Ⅱ 기본 방침

01 수립 체계 ····· 12

02 중점 목표 ····· 12

Ⅲ 윤석열 정부 2년의 성과 및 향후 방향

01 '北 사이버위협' 및 사이버공간상 '허위정보' 대응 ····· 14

02 자유민주주의 수호를 위한 국제사회 사이버안보 협력 강화 ····· 15

03 국가 차원의 사이버위협 대응체계 정립 ····· 16

04 국가 핵심인프라 사이버보안 강화 ····· 18

Ⅳ 전략과제별 세부계획

01 공세적 사이버 방어활동 강화 20

02 글로벌 사이버 공조체계 구축 23

03 국가 핵심인프라 사이버 복원력 강화 25

04 신기술 경쟁우위 확보 28

05 업무 수행기반 강화 30

Ⅴ 이행 방안

I.

수립 배경

01 사이버안보 환경 변화에 대한 인식

02 「국가 사이버안보 전략」의 이행

01 사이버안보 환경 변화에 대한 인식

사이버공간에 대한 위협

- 대한민국의 사이버공간은 다양한 경제·사회·문화 활동이 영위되는 자유민주주의 근간이며, 국가 핵심인프라가 운용되는 안보의 중심
- 최근에는 국제 및 국가배후 해킹조직이 국가기밀 및 첨단기술 절취, 랜섬웨어 협박 등 국가안보·국민안전을 심각하게 위협
- 특히, 북한은 막대한 규모의 해킹조직을 운영하면서 국가기밀을 절취하고 가상자산 탈취 등을 통해 핵·미사일 개발 자금 충당

초연결 사회로 디지털 환경의 급속한 전환

- 사이버공간의 초국경성은 영역·시간의 제약 없이 다양한 이해관계자가 상호 연결되어 편익을 누릴 수 있는 환경을 제공
- 특히, 코로나19로 인한 글로벌 팬데믹은 비대면 디지털 환경으로의 전환을 급속히 촉진해 사이버공간의 중요성이 더욱 증대
- 무한한 가능성의 이면에는 여러 디지털 수단으로부터 비롯된 보안 취약점과 ICT 서비스 장애에 의한 사회혼란 가능성도 존재

글로벌 사이버안보 강화 트렌드

- 전세계 주요국은 사이버안보를 강화하기 위한 국가전략을 수립하고 국제규범과 법·제도 개선 및 국가·국제기구간 협력 심화 중

02 「국가 사이버안보 전략」의 이행

「국가 사이버안보 전략」을 토대로 우리 정부는 **사이버안보** 위협에 **선제적으로 대처**하고 사이버 **역량과 복원력을 강화**하여, **대한민국을 안전하게** 지켜나갈 것입니다. 또한 자유, 인권, 법치의 규범과 가치를 공유하는 우방국들과 **사이버안보 공조를 강화**하면서 **국제사회의 평화와 번영에 기여**해 나갈 것입니다.

– 윤석열 대통령 공표 「국가 사이버안보 전략」 서문 (2024.2.1) –

- 정부는 변화된 안보 환경과 국정 기조를 반영하여 국가 차원의 전략 방향을 제시하는 새로운 「국가 사이버안보 전략」 발표
- 새로운 전략은 △자유민주주의 가치 수호 △글로벌 중추국가 실현 △법치와 규범 기반 질서 수호 등 정부의 외교안보 국정 철학 반영

이에, 전략을 구체화하고 성실히 이행할 수 있도록
세부 추진계획을 담은 「국가 사이버안보 기본계획」을 수립

「국가 사이버안보 전략」(2024.2.1) 주요 내용

비 전

사이버공간에서 **자유·인권·법치**의 가치를 **수호**하며 국제사회에서 역할과 책임을 다하는 **글로벌 중추국가**

3대 목표

공세적 사이버 방어 및 대응	글로벌 리더십 확장	건실한 사이버 복원력 확보

기본원칙

- 국가의 핵심가치와 국민의 경제적 이익을 균형있게 중시
- 정부·산업계·학계 등 모든 이해관계자가 협력하여 사이버 위협에 공동으로 대응
- 규범에 기반하여 정당한 목적과 적법한 수단으로 업무수행

5대 전략과제

01 **공세적 사이버 방어활동 강화**
국가안보·국익을 위협하는 악의적 사이버활동에 대한 억지력을 확보하고, 위협행위자의 사이버공격에 대한 선제적 방어역량 강화

02 **글로벌 사이버 공조체계 구축**
국제사회와의 적극적인 협력을 통해 사이버위협 대응의 실효성을 제고하고, 글로벌 중추국가로서 안전하고 평화로운 사이버공간 구축에 기여

03 **국가 핵심인프라 사이버 복원력 강화**
국가 핵심인프라와 중요 시스템의 사이버 복원력을 강화하여 모든 기업과 국민에게 필수적인 서비스의 안전성 제공

04 **신기술 경쟁우위 확보**
국가 사이버안보 역량의 기반이 되는 핵심기술을 적극적으로 육성하고 안전하게 보호함으로써 국제 경쟁력 및 기술주도권 확보

05 **업무 수행기반 강화**
개인, 기업, 정부의 역할과 책임을 유기적으로 연결하고 조화를 이루도록 제도를 정비하여 범국가 차원의 통합대응 체계 확립

Ⅱ.

기본 방침

01 수립 체계

02 중점 목표

01 수립 체계

- 사이버안보 컨트롤타워인 국가안보실의 감독하에, 사이버안보 주무부처인 국가정보원을 주관기관으로 하여 관계부처 합동으로 수립
  * 국정원은 대통령의 지시·감독을 받아 사이버안보 관련 정보·보안 업무를 기획·조정(「국정원법」 제2조·제4조, 「사이버안보 업무규정」 제3조의2)
- 정부 각 부처는 법령에 따른 소관 분야에서 5대 전략과제 이행에 필요한 실천과제를 발굴하고, 부처간 공동·협업 요소에도 착안
  * 실천과제 중복·연계점을 고려하여 관계부처 협의를 통해 면밀 조율
- 국제전략·법률·IT공학 등 분야별 전문가 시각을 적극 반영하고, 수립된 계획을 국민에게 최대한 알리고 이해를 구함으로써 '정책의 투명성'과 '이행의 당위성'을 지속 확보·유지

02 중점 목표

- 윤석열 정부의 지난 2년간 사이버안보 활동 성과를 평가하여 향후 업무수행 방향을 제시하고 기본계획에 충실히 반영
- 「국가 사이버안보 전략」이 강조하고 있는 △북한의 불법 사이버 활동 차단 △사이버위협에 대한 선제적 식별 및 공세적 대응 △자유민주주의 가치 공유 국가와의 글로벌 협력 △사이버 복원력 제고 △신기술 국제 경쟁력 확보에 중점

「국가 사이버안보 기본계획」의 수립·이행을 통해
사이버안보 역량을 더욱 강화하고 사이버공간에서
안전한 기업 활동과 국민의 생활을 보장하기 위해 노력

Ⅲ.

윤석열 정부 2년의 성과 및 향후 방향

01 '北 사이버위협' 및
사이버공간상 '허위정보' 대응

02 자유민주주의 수호를 위한
국제사회 사이버안보 협력 강화

03 국가 차원의 사이버위협 대응체계 정립

04 국가 핵심인프라 사이버보안 강화

01 '北 사이버위협' 및 사이버공간상 '허위정보' 대응

가 성과

- 전 세계를 위협하는 '북한의 악의적인 사이버활동'에 대응하기 위해 국제협력, 합동발표, 대북제재 공조 등 국제사회內 대응활동 주도
  * 세계 주요국과 합동 보안권고문 발표, 유엔 안보리 등 국제회의 참여를 통해 北 위협 실태 공론화
- 국내외에서 발생한 사이버안보 침해행위를 탐지·대응하고, 국민에게 적절히 알림으로써 북한 등 위해세력에 대한 경각심 제고

나 향후 방향

- 군 및 정보기관은 공세적 사이버 정찰 활동을 통해 북한 등 위협 행위자의 활동을 적극적으로 확인·견제·차단하는 등 선제적 대응 체계로의 전환 필요
- 이와 함께, 국론 분열과 사회혼란을 유발하는 북한 등 해외발 가짜뉴스·허위정보 유포 등에 대응할 수 있는 업무기반 확보 긴요

02 자유민주주의 수호를 위한 국제사회 사이버안보 협력 강화

가 성과

- 한·미 정상은 '전략적 사이버안보 협력 프레임워크'를 공동 발표하고, 이에 대한 후속 조치로 사이버안보 협력 고위운영그룹(SSG) 발족
- 한·영 '전략적 사이버 파트너십' 협력문서 체결과 함께 민관협력·기술교류·북한대응 등 협력과제 채택

나 향후 방향

- 사이버위협의 초국경성에 대응하기 위해 자유민주주의 가치를 공유하는 여러 국가들과 연대를 구축하고 협력 강화 긴요

  * 외교·정보 당국의 '北 사이버위협' 경각심 제고와 국제공조 대응 활동 등도 강화

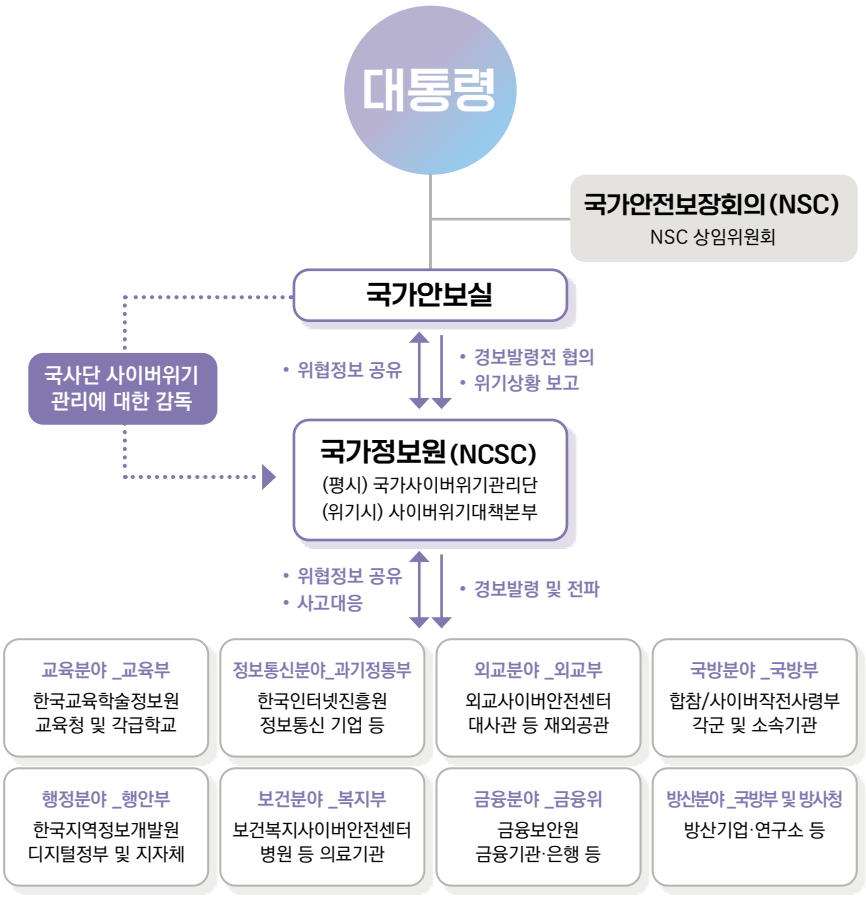
- 또한, 책임있는 글로벌 중추국가로의 도약을 위해 유엔 등 국제사회의 사이버안보 규범 논의에 대한 참여를 확대하고 신뢰구축을 위한 노력 필요

03 국가 차원의 사이버위협 대응체계 정립

가 성과

◆ 국가안보실을 컨트롤타워, 국가정보원을 실무 주관기관으로 정하고 안보실 관리·감독하에 사이버안보 위협으로부터 국민안전 보호를 위한 민관합동 통합대응 조직(국가사이버위기관리단)을 설치

나 국가사이버안보 수행체계



- 안보실은 국가 사이버안보 관련 업무 전반을 조율하고, 중장기 정책방향을 수립·검토하는 최상위 컨트롤타워 역할을 수행

- 국정원은 국제 및 국가배후 해킹조직 등 사이버안보 관련 정보를 수집·작성·배포하고, 북한·외국 등의 안보침해행위에 대한 확인·견제·차단과 국민안전 보호 대응조치를 수행하며, 국가사이버안보센터 내에 국가사이버위기관리단을 설치하여 유관부처, 전문기관·기업 등과 실시간 위협정보 공유 및 사이버위기에 대비·대응

- 각 부처는 개별 법령에 근거하여 각 분야별 보안·보호 활동을 수행

  예) ▲ '국가·공공' 분야는 국정원(「국정원법」등) ▲ '교육' 분야는 교육부(「교육기본법」 등) ▲ '금융' 분야는 금융위(「전자금융거래법」) ▲ '정보통신' 분야는 과기정통부(「정보통신망법」 등) ▲ '보건의료' 분야는 보건복지부(「의료법」) ▲ '교통' 분야는 국토부(「자동차관리법」) ▲ 군 분야는 국방부(「국방정보화법」)가 각 보호활동 수행

다 향후 방향

- 민관합동 통합대응 조직의 역량 강화를 위해 외교·통일·교육 등 참여기관 확대와 정보보호 기업 등 민간역량 활용 확대방안 강구

- 안보실 중심 현 국가사이버안보 수행체계를 공고화하고, 개별 법령에 따른 각 부처의 역량이 최대한 발휘되도록 협업체계 정비도 필요

04 국가 핵심인프라 사이버보안 강화

가 성과

- 국가·공공기관 및 주요정보통신기반시설 사이버보안 강화를 위한 지속적인 법제도 개선과 예방·점검 활동으로 보안성 향상
- 소관 분야별 보안·보호 활동을 통해 안정적인 업무 수행 기반 유지

나 향후 방향

- AI·양자암호 등 신기술이 유발하는 신종 사이버 위협에 대한 선제적 대응 역량 확보를 위해 연구개발 투자와 인력양성 추진
- 공공분야 기존 망분리 정책의 문제점을 개선하고 ▲제로트러스트·다층보안체계 적용 ▲AI·클라우드 도입 등 신기술 활용 필요

Ⅳ.

전략과제별 세부계획

01 공세적 사이버 방어활동 강화

02 글로벌 사이버 공조체계 구축

03 국가 핵심인프라 사이버 복원력 강화

04 신기술 경쟁우위 확보

05 업무 수행기반 강화

01 공세적 사이버 방어활동 강화

가 국가안보 위해(危害) 활동에 대한 공세적 대응 강화

【 기반 구축 】

- 최신 공격기술, 국내외 첩보를 포괄한 범국가 위협정보DB 구축과 유관기관 합동 평가를 통해 공격주체 판단의 객관성 및 정확성 제고
  * 배후지목을 위한 절차 및 기준 수립 등 국제공조 대응을 위한 기반 구축
- 국제 및 국가배후 해킹조직 등 위협행위자를 식별하고 해킹 거점·인프라 및 활동을 추적하는 기술 개발

【 대응활동 강화 】

- 군 및 정보·수사기관간 ▲사이버공격 수법 ▲위협행위자 신원·거점 ▲해킹 조사·수사 등 사이버위협정보 공유 및 협업을 통해 적극 대응
- 군의 사이버작전 역량을 강화하기 위해 국방사이버 전략·정책을 수립하고, 국가안보에 기여하는 사이버작전을 시행
- 사이버보안 권고문 발표에 따른 위협 억지 효과 극대화를 위해 다수 자유진영 국가 참여하 위협 행위자·실태 폭로 등 국제적 연대 강화

나 위협정보 수집·분석 기반 강화

【 법제도 기반 마련 】

- 국제 및 국가배후 해킹조직의 안보침해 활동 조사에 필요한 국내 소재 디지털정보를 확인할 수 있는 명확한 절차 마련
  * 오남용을 통제하기 위한 사법통제 등 엄격한 법적 장치 동반
- 국제 및 국가배후 해킹조직의 안보침해 활동 확인·견제·차단에 필요한 공격 근원지·거점 추적에 대한 명확한 절차 및 통제장치 마련

【 역량 고도화 】

- 국제 및 국가배후 해킹조직 등 위협행위자의 사이버공격에 대한 선제적 방어를 위해 공격 근원지에 대한 정찰·첩보 활동 및 역량 강화
- AI 등 신기술을 적용하여 국가 전 영역에서 국제 및 국가배후 해킹조직 등의 사이버 안보 위협활동을 탐지·분석하는 체계 구축·운영
- 주요 인터넷서비스 공격 징후를 조기에 포착하고 연관성 분석을 수행하는 AI기반 통합 탐지·대응 시스템 구축·운영

【 국내·외 협업 강화 】

- 해외 정보기관 및 보안기관과 국제 해킹조직 등에 대한 위협정보 교류·합동분석 정례회의 개최를 확대하고 실시간 정보공유 채널 확충
- 금융권 대상 사이버위협을 적시에 탐지·대응하기 위해 위협 모니터링을 강화하고 글로벌 차원의 위협정보 공유 등 국제공조 활성화
- 국내외 최신 사이버범죄에 대한 정보 수집·분석·공유 체계를 확립하고 효과적인 범죄 대응을 위한 유관기관 협력체계 강화
  * AI기반 안보침해 범죄 대응 통합분석 플랫폼을 개발, 효율적인 침해사고 수사 지원

다 사이버공간상 영향력 공작 대응

- 심각한 사회혼란을 유발할 수 있는 허위조작정보 근절을 위해 범부처 합동 대응방안을 마련·실행하고 포털·플랫폼사업자 자율규제를 강화
- 해외에서 유발된 허위조작정보 및 영향력공작에 효과적으로 대응하기 위해 미비한 관련 법제 정비
  * ▲외국을 위한 간첩행위 처벌 ▲외국 대리인 등록 의무 등
- 우리나라에 대한 영향력 공작을 목표로 해외에서 생산되어 국내에 유포되는 가짜뉴스 등 허위정보를 탐지·대응하는 체계적 수단 확보
- 다양한 방식과 수단으로 진화 중인 북한의 사이버상 선전·선동에 대응하기 위해 불법정보 차단 업무 역량 제고 및 유관기관 협력 강화

라 사이버범죄에 대한 예방·대응역량 제고

- 가상자산 사기·탈취 등에 대한 사이버범죄 수사 기법을 개발·연구하는 한편, 신종 사이버범죄 분야 발굴 및 추적 기술·역량 확보
  * 랜섬웨어·보이스피싱·디도스 등 공격 근원지·행위자 프로파일링 시스템 개발
- 사이버수사 전문인력 양성을 위한 교육 훈련 및 사이버범죄 수사 전담조직을 보강하고, 국내외 유관기관 및 전문가와의 협력을 강화
  * 디지털포렌식 전문자격을 갖춘 경찰 시도청 현장 지원팀 신설 등
- 사이버사기·도박·성폭력 등 민생침해 사이버범죄 및 신종범죄에 대한 집중 수사 체계를 확립
- ▲사이버 드보크 ▲스테가노그라피 등 고도화·첨단화된 범죄수법에 대응하기 위해 디지털증거 수집·분석 역량 고도화

02 글로벌 사이버 공조체계 구축

가 미국을 비롯한 다양한 국가와의 사이버안보 협력 공고화

【 전략적 공조 】

- 한·미 '전략적 사이버안보 협력 프레임워크' 이행을 위한 고위운영그룹(SSG) 활동 강화와 함께 위협정보·기술·인력·정책 교류 및 민간협력 확대
- 한·영 '전략적 사이버 파트너십' 후속조치로 사이버위협 예방·대응을 위한 정보공유 및 정책·기술 협력 추진
- 미·영 이외 자유민주주의 가치를 공유하는 국가들과도 협력·공조를 강화하고, 양자·다자 공동대응 및 협력 체계 구축
- 북한의 핵·미사일 개발 자금 조달 수단인 불법적인 사이버활동에 대해 국제사회 경각심을 제고하고 이를 차단·억지하는 국제활동 주도
  * 한·미·일 합동 보안권고문 발표, 실무회의 운영 등 협력·공조 강화
- 한·미 국방분야간 사이버 정책·작전·인력 교류 및 사이버훈련 강화

【 형사사법 공조 】

- 해외 법집행기관과 협력 강화 모델 수립 및 교류를 다변화하고, 공조국 검사·수사관 역량구축 지원 등 협력 강화
- 해외 법집행기관 상시연락 네트워크 구축 및 다자간 사이버범죄협약 접촉창구(POC) 개설 등 국제공조 확대
- 사이버 범죄대응 분야 ▲선도국 법집행기관과 협력협정 체결 ▲유로폴 수사협력관 파견 ▲사이버범죄대응 국제행사 등을 통해 국제 공조망 확충

- ‘사이버수사 국제공조포털시스템’ 고도화를 추진, 국제공조 요청에 대한 원스톱지원 체계를 구축하는 등 국제 공조수사 효율성 제고

나 국제 사이버규범 논의 및 신뢰구축조치 이행 활동에 적극 참여

【 국제규범 참여 】

- 부다페스트협약 가입에 필요한 국내 이행입법 및 협력창구 지정 등 부처간 협의를 완료하고 가입을 조속히 추진
- ▲유엔 안보리 이사국 활동(2024~25) ▲유엔 정보안보 개방형 실무그룹(OEWG) 실질회의 등을 통한 유엔 차원의 사이버안보 논의 지속 참여
- 아세안지역안보포럼(ARF), 유럽안보협력기구(OSCE) 등 다양한 국제기구에서 사이버 규범이행, 신뢰구축, 역량강화 논의 참여
  * 랜섬웨어 대응 이니셔티브(CRI), 상업적 스파이웨어 확산 및 오용 대응 노력에 대한 공동성명 등 사이버위협 대응을 위한 활동논의에도 동참

【 신뢰관계 증진 】

- 정부간 사이버안보 정책협의회를 우리의 국격과 위상에 걸맞게 다양한 국가로 확대하여 상호간 이해와 신뢰 증진
- 우리나라가 개최하는 ‘사이버 서밋 코리아(CSK)’ 등 사이버안보 국제행사에 참여하는 해외기관 및 국제기구와의 협력 관계를 강화

다 민간·국제기구들과 협력 및 글로벌 역량강화 지원 확대

- 아세안 등 개도국 대상 사이버안보·범죄 분야 역량 배양 사업 확대, 국가 간 격차 해소에 적극 기여하고 우리나라 위상과 리더십 제고
- 아태지역 침해사고대응 역량 강화를 위해 각국 침해사고대응팀(CERT) 대상 교육·훈련을 지원하고 공동 대응 기반을 마련

03 국가 핵심인프라 사이버 복원력 강화

가 주요 정보시스템 보안 강화

【 기반시설·제어시스템 】

- 신규 정보통신 기반시설을 발굴하고 제도권에 편입·보호하기 위해 분야별 정보통신 기반시설 지정 평가절차·기준 등 개선
- 기반시설의 취약점 식별, 조치, 관리 등 점검 항목과 평가 기준을 보완하는 등 기반시설 정보보호 종합수준 평가 기준 개선
- 제어시스템이 가동 이후에는 중단·보완이 어려운 점을 고려, 기반시설 관리기관이 제어시스템 도입전 검토·적용할 보안 요구사항을 마련

【 행정 정보시스템 】

- 개방·공유를 지향하는 디지털플랫폼정부 구현을 위해 국가정보자원관리원 보안관리 체계를 新 보안체계로 전환
- 지방자치단체 전산망의 보안관제 이행여부 조사 및 주기적인 취약점 점검·조치를 통해 보안관리 사각지대 해소

【 신기술 적용 시스템 】

- AI·인공위성 등 신기술 분야 보안위협 선제적 대응을 위해 ▲신기술 위협·정책 선행연구 ▲해외 주요국 대응 사례 분석 ▲민관 전문가 의견수렴 등을 반영하여 관련 지침·매뉴얼 제개정 추진

  * AI·스마트그리드·인공위성 보안가이드라인 제정 및 국가정보보안 기본지침 보완

나 디지털플랫폼정부 구현에 대비한 보안관리체계 재정립

【 보안정책 개선 】

- AI시대 안보환경에 부응하는 사이버안보 패러다임 구축을 위해 한국형 제로트러스트 기술 적용 모델을 연구, 각급기관에 적용 추진
  * 민간기업 대상 제로트러스트 도입을 지원하고 국내 기업 업무환경 보안성 강화
- 보안성을 유지하면서 외부망·인터넷 데이터를 자유롭게 이용할 수 있도록 국가·공공기관 망 분리정책 개선
  * 업무망내 AI·클라우드 등 신기술 활용으로 업무 생산성 제고 기대
- 클라우드 보안인증제도 운영을 통해 공공 분야 민간클라우드 이용을 활성화하고 국내 클라우드 산업 경쟁력도 강화
- IT제품·네트워크 장비 등 정보보호제품 보안적합성 제도 개선 및 국가·공공기관 도입요건 간소화를 통해 신속한 도입 기반 마련

【 보안 체질 강화 】

- 월패드·디지털도어락 등 국민생활과 밀접한 사물인터넷(IoT) 기기에 대한 보안내재화 촉진 및 국내 IoT 보안인증 제품의 해외진출 지원
- 중앙행정기관·광역지자체·공공기관에 대해 실시중인 '사이버보안 실태평가' 저조 기관 대상 보안컨설팅 실시 등 보안강화 지원

다 범국가적 차원의 ICT 공급망 보안정책 및 대응체계 확립

- SW 개발·공급 단계의 취약점 내재 위험성에 대응하고, 국내 SW 기업의 해외 무역장벽 극복을 위해 미국·유럽 등 주요국과 유사한 SW 구성요소 명세서(SBOM, SW Bill of Material) 도입을 지원
  * 국정원·과기정통부·디플정 합동으로 SW 공급망 보안 가이드라인 마련·보급

- 국가·공공기관에 도입되는 SW의 공급망 보안 관리체계를 강화하기 위해 범정부 합동으로 SW 공급망 보안 관련 제도·지침 정비

  * 국가·공공기관에 도입되는 SW 구성정보 항목을 표준화하고 행정지원 디지털서비스의 설계·구현 단계 개발보안 적용 지원 강화

- SW 공급망 보안관리 중요성에 대한 인식 제고를 위해 국가·공공기관 대상 공급망 보안 관리체계 교육 및 기술지원 확대

04 신기술 경쟁우위 확보

가 기반 기술의 전략산업화

【 사이버보안 R&D 확대 】

- 디지털 전환 가속화 및 사이버위협 증가에 따라 고성장 산업인 글로벌 보안시장 주도권 확보를 위해 사이버보안 R&D 지원을 확대
  * 글로벌 사이버보안 시장: ('22년)1,735억$ → ('27년)2,662억$ (연평균8.9% 성장)
- 데이터·AI보안, 양자 컴퓨팅, 디지털 공급망 분석대응, 네트워크·클라우드 보안, 미래산업·융합보안 등 중점 분야에 대한 R&D 확대 및 기술경쟁력 강화 추진

【 국내 정보보호 산업 활성화 】

- 기업의 정보보호 현황을 공개·관리하는 정보보호 공시제도의 이행률 제고를 위한 교육실시 및 신뢰성 확보를 위해 사후검증 제도 운영
- 사이버보안 기술을 보유한 혁신 유니콘 기업을 육성하고, 민간투자 확산 및 사업 영역·규모 확대 M&A 활성화
- 인증 기준이 없어 적기 도입이 어려운 신기술 및 융·복합 보안제품의 시장 진입을 위해 정보보호제품 신속확인제도 활성화 추진
  * 기업 대상 점검가이드 마련, 수수료 지원(중소기업 80%), 수요처 홍보 등 추진('23~)
- 국내 유망 정보보호 스타트업 육성·지원을 위한 정보보호 클러스터(판교·동남) 운영 및 지역 거점 확대 사업 추진
  * 입주공간 지원, 테스트베드·사이버훈련장 운영, 광역공동협의체 운영 등

【 정보보호산업 해외진출 지원 】

- 민간 기업이 주도하고 정부가 지원하는 'K-시큐리티 얼라이언스' 구성, 분야간 협업 문화를 확산하고 우수 통합보안 모델 시범개발 추진
- 우리나라 사이버보안 정책 홍보 및 국내 기업의 국제시장 진출 지원을 위해 개도국 대상 '글로벌 사이버보안 협력 네트워크(CAMP)' 확대
  * 회원국 대상 역량 강화 지원 활동을 통해 정보보호산업 영향력을 확대
- 국내 정보보호기업의 해외인증제도 획득 및 사업타당성·시장 조사·진출전략·마케팅 등 지원 활동을 통한 해외진출 활성화

나 신기술에 대한 사이버위험 관리체계 확립

- 자율주행·도심항공 등 신기술에 대한 사이버보안 정책 및 기술연구를 위한 민관 협의체 구성·운영
- 국가 미래산업을 대상으로 기업이 제품·서비스를 기획하는 단계부터 보안내재화를 고려할 수 있도록 취약점 점검·보안컨설팅 지원 확대
  * 스마트공장·헬스케어·자율주행·우주·로봇·스마트선박 등 미래산업
- 보안 투자 여력이 부족한 영세·중소기업 대상으로 사이버 침해사고 대응·피해복구 및 정보보호 역량 강화 지원
  * 해킹진단도구 보급과 함께 침해사고 피해기업 대상 보안조치 이행 점검 등 지원
- 대규모·고성능 양자컴퓨터 출현시 현 암호체계 무력화 가능성에 대비, 국가 전반의 암호체계 고도화 방안·일정 등 범정부 종합 대책 마련·시행

05 업무 수행기반 강화

가 국가 사이버위협 대응체계 정립

【 법제도 기반 마련 】

- 「사이버안보법」을 제정하여 국가 차원 대응체계를 정립 및 실질적 구체적인 사이버안보 활동의 제도적 기반 마련
- '국가위기관리기본지침'에 따라 작성된 '국가사이버위기관리 표준 매뉴얼'에 입각하여 각 부처의 소관 분야별 실무매뉴얼을 정비

【 국가차원 통합대응 및 정보협력체계 강화 】

- 사이버안보 위협으로부터 국민안전 보호를 위하여 설치된 민관 합동 통합대응 조직(국가사이버위기관리단)의 역량 강화를 위해 외교·통일·교육 등 참여기관 확대 및 민간 전문업체와 협업·정보 공유 강화 추진
- 국가 사이버안보 위협정보 공유플랫폼(NCTI·KCTI) 고도화 및 사이버안보 관련 정보 교류·협력의 장으로 도약

  * NCTI(National Cyber Threat Intelligence): 국정원이 운영하는 국가·공공기관간 사이버위협정보 전파·공유 시스템, KCTI는 민간기업 전용 정보공유 시스템

나 소관부처별 역할과 책임 정립

【 외교·국방·행정 분야 】

- 외교분야 주요 기반시설의 보안을 강화하고, 시스템 장애 대비 시스템 운영·유지보수 및 복구 체계를 구축

- ‘국방 사이버보안 위험관리 제도(K-RMF)’ 조기 정착을 추진, 군 무기·정보 체계의 전 수명주기 동안의 사이버보안 위험 관리 강화

- 행정안전분야 주요정보통신기반시설 대상 ▲취약점 점검 ▲정보보호 진단·컨설팅 ▲보안장비 확충 등을 통한 보호수준 향상

  * 철도운영·교통신호·상수도·지역난방·긴급구조 등 관련 정보통신기반시설

【 산업·경제 분야 】

- 산업·무역·에너지 분야 사이버위협 선제 대응을 위한 보안관제시스템 개선 및 대국민 서비스 상시 모니터링 체계 가동

- 금융분야 주요 정보시스템 침해사고·장애 방지 및 신속대응 체계 마련

- 해사분야 디지털화로 선박·항만 대상 사이버 공격·위협이 증가함에 따라 해사 사이버 안전 종합대책 수립 및 법제도 마련

  * 항만보안을 위협하는 드론 등에 대한 차단시스템 도입과 합동훈련도 추진

- 국가 사이버위기관리 체계에 맞춰 '정보통신분야 사이버위기대응 실무매뉴얼' 개정 추진

【 사회 분야 】

- 교육·교육행정기관 주요정보통신기반시설 보호를 강화하고 교육분야 사이버위협 대응 역량 강화 및 정보보호 수준 제고

  * 교육기관에 ▲AI기반 보안관제 시스템 및 차세대 위협탐지 장비 도입 ▲보안취약점 점검 체계 구축·운영 ▲정보보호 수준 평가·관리 등

다 범국가적 사이버위기 대응을 위한 민간역량 활용 확대

【 전문가 자문 】

- 사이버안보에 관한 민간 전문가의 전문지식 활용 및 의견수렴을 위해 국가사이버안보센터에 사이버안보자문단 설치·운영

【 사이버위협 실데이터 소통 】

- 사이버안보 정보 공유 범위 확대 등 민간기업·단체와의 사이버 안보정보 협력을 강화하여 범국가적 사이버안보 역량 강화
- 정부와 기업간 침해지표 등 공유를 통해 국제 및 국가배후 해킹 조직의 사이버위협에 대한 대응 역량 강화

【 기업들의 자발적 협력 환경 견인 】

- 국내외 정보보호 기업과 긴밀한 정보공유·합동분석을 위한 협의체 및 플랫폼을 구축하고 합동근무 형태의 사이버위협분석센터 개소
- 국내외 정보통신·정보보호 기업과 '정보통신망 침해사고 정보 분석 협업 네트워크' 구축·운영, 침해사고의 신속한 공유 및 공동대응 강화
- 다양한 산업 분야의 기업·기관이 정보통신망 침해사고에 적시 대응할 수 있도록 위협정보 분석·공유 체계 'C-TAS' 회원사 확대 등 활성화 추진

  * C-TAS(Cyber Threat Analysis&Sharing) : 과기정통부 운영 위협정보 공유시스템

라 전문인력 양성 및 유지

【 인력 양성 및 교육 프로그램 】

- 고도화되는 신기술 사이버위협에 대응할 수 있도록 맞춤형 교육·훈련을 통한 분야별 전문인력 양성·유지 체계 구축
- 민간 화이트해커의 신규 취약점 발굴과 신고를 장려하고 참여를 유도하기 위해 취약점 신고에 대한 보상을 강화
- 군 사이버전문인력 양성 및 전문성 제고를 위해 유관부처간 협력을 확대하고, 사이버전문사관 양성·교육 등 프로그램 강화

- 교육분야 정보보호 업무 담당자 전문성 강화를 위한 정보보호교육센터 교육 콘텐츠 품질 개선, 실습 강화 등 운영 내실화

【 실전 훈련 】

- 민간기업이 참여하는 사이버 위기대응 모의훈련을 내실화하고 민·관 협조체계를 지속 점검하여 사이버 위기상황 발생시 신속하게 대응
- 범국가 사이버방어 합동훈련을 통해 국가 전 영역을 위협하는 국제 및 국가배후 해킹조직의 사이버공격을 방어할 수 있는 역량 확보
- 글로벌 사이버안보 위협에 대한 합동대응 역량을 제고하기 위하여 세계적 수준의 최첨단 국제 사이버훈련센터를 구축·운영

마 대국민 인식 제고 및 실천 강화

- SNS·영상물 등을 활용한 국민 참여형 정보보호 인식 제고 캠페인 추진, 일상 속 정보보호 실천을 장려하고 국민 경각심 고취
- 금융이용자 침해사고 피해 예방을 위한 대국민 보안인식 제고 활동 추진
- 정보보호의 날·달 행사를 통해 정보보호 및 사이버안보에 기여한 유공자를 발굴·포상하고, 범국민 정보보호 인식제고 기회로 활용
- 사이버안보 국제행사 '사이버 서밋 코리아(CSK)' 정례화를 통해 글로벌 사이버안보 선도국가로서 책임을 다하는 대한민국의 노력을 대외 공표

V.

이행 방안

V

이행 방안

- 정부는 국민, 기업, 국제사회와 협력하여 동 기본계획을 추진함으로써 전략의 비전과 목표를 달성할 수 있도록 노력 경주
- 각 부처는 과제 이행에 필요한 예산, 인력, 조직 등을 검토·개선하고, 입법조치를 추진하며 각 부처별 중장기 업무계획에도 반영
- 국가안보실은 과제의 이행여부 및 그에 따른 사이버안보 수준의 향상 정도를 정기적으로 점검하며, 국가정보원은 각 부처의 이행 진도 등을 종합하여 국가안보실을 지원

2024

국가 사이버안보 기본계획

2024

관계부처 합동