발간등록번호
12-1025000-000003-01

국가 사이버안보 전략

대한민국
청 와 대

국가안보실

서문

대한민국은 세계 최고수준의 정보통신기술과 인프라를 보유하고 있습니다. 국민은 다양하고 편리한 사이버 공간을 통해 삶의 지평을 넓혀왔습니다. 정부의 행정서비스와 국가 주요 기간시설 운영의 핵심 기반 역시 사이버 공간입니다.

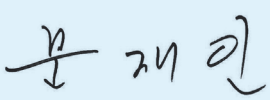
그러나 최근 사이버 범죄와 테러가 급증하면서, 국민의 일상과 기업의 경제활동이 위협받고 있습니다. 조직화된 사이버 공격은 국가안보에 심각한 도전이 되고 있기도 합니다.

이에 정부는 대한민국 최초로 '국가사이버안보전략'을 수립했습니다. 사이버 범죄로부터 국민의 안전과 권익을 지키겠습니다. 조직적 사이버 위협을 신속히 탐지하고 차단하여 국가 주요기능이 안정적으로 운영되게 할 것입니다. 사이버안보 인력 양성과 관련 산업 발전에도 지속적으로 힘을 기울여 나갈 계획입니다.

사이버안보의 중심은 국민입니다. 국민을 위한 사이버안보의 3대 기본원칙도 마련했습니다. 국민의 기본권을 철저히 보장하고, 반드시 법치주의에 기반을 둔 안보활동을 전개하겠습니다. 국민의 참여를 보장해 투명한 사이버 안보를 실현하겠습니다.

사이버공간의 안전은 정부와 기업, 개인 모두 함께 협력할 때 확보될 수 있습니다. 정부는 자유롭고 안전한 사이버 공간을 만들기 위해 최선의 노력을 다하겠습니다. 국민 여러분께서도 대한민국이 세계 최고의 사이버 안보 강국이 될 수 있도록 힘을 모아주시기 바랍니다.

대한민국 대통령 **문 재 인**



NATIONAL CYBER SECURITY STRATEGY

CONTENTS

National
Cybersecurity
Strategy

I

수립 배경

1. 변화와 도전
2. 성과와 반성
3. 새로운 이정표

01 변화와 도전

사이버공간 취약성 증대

우리나라는 세계최고 수준의 정보통신기술과 관련 인프라를 바탕으로 다른 어느 나라보다 편리하고 풍요로운 사이버공간을 건설해 왔다.

이제 사이버공간은 국민의 일상생활은 물론 기업의 경제 활동과 정부의 행정 서비스 등 국가 운영의 핵심기반으로 자리매김하였다.

그러나 다양한 정보통신 기기와 네트워크의 상호 연결은 사이버공간의 복잡도를 급격히 증가시켜 안전한 관리를 점차 어렵게 만들고 있다.

영역 구분이 없는 사이버공간의 특성으로 인해 일부 정보통신 기기의 취약점이 사이버공간 전체의 안전을 위협하는 요인으로 작용하기도 한다.

또한, 가전·의료·공장이나 기반시설 등에 사물인터넷 기반의 융합기술 보급이 본격화됨에 따라 사이버공간의 위협이 현실 공간까지 확산되고 있다.

사이버 위협 심각성

개인이나 해커그룹이 주도하던 사이버 공격이 범죄·테러 단체로 확산되고, 나아가 국가가 개입·지원하는 등 조직화·대규모화 되는 상황이다.

사이버 공격의 양상도 기밀절취·금전취득에서 정치적 목적의 사회혼란 야기, 기반시설을 마비·파괴하는 사이버테러 등으로 다양화하고 있다.

최근에는 사이버공격을 통해 전통적인 무력공격 수준의 피해를 발생시키는 사이버전쟁 발생 가능성도 점차 증대하고 있는 실정이다.

국가간 사이버안보 역량경쟁 심화

국가간 정치·경제·군사적 분쟁이 사이버상에서 충돌로 이어지고 있으며 실제 물리적 공격 전후에 사이버 공격을 감행하는 사례도 발생하고 있다.

각국은 사이버 역량을 국가안보에 중요한 영향을 미치는 비대칭 전력으로 인식하여 오랜 기간 전문 인력을 집중 육성하고 국가 조직을 확대하고 있는 상황이다.

또한, 인공지능(AI)·빅데이터 기반의 첨단 사이버기술 개발과 아울러 사이버 첩보수집, 인터넷망 교란, 주요시설 마비 등을 위한 역량확충에 대규모 예산을 투입하고 있다.

사이버범죄로 인한 국민의 피해 심화

첨단기술과 개인정보 등을 가로채거나 암호화하여 금전을 요구하는 사이버범죄가 증가하여 기업과 국민의 피해가 커지고 일상화되는 양상이 나타나고 있다.

국가·테러단체 등의 개입으로 인해 사이버범죄 피해의 규모와 심각성이 확대되어 국가안보에 대한 위협으로 대두되는 사례도 증가하고 있다.

02 성과와 반성

우리나라가 정보통신기술 강국으로 도약했던 성과 이면에는 우리의 사이버 공간이 다양한 위협에 취약했던 뼈아픈 경험이 공존하고 있다.

정부는 대규모 사고 발생 시마다 관계부처 합동으로 종합대책을 수립·시행함으로써 국가 사이버안보 체계를 발전적으로 보완하였다.

그러나 이러한 노력에도 불구하고 사이버공간의 급속한 발전과 사이버안보 위협의 증가로 인해 적극적인 보완·개선이 지속적으로 필요한 상황이다.

대응 역량

정부는 사이버공격 실시간 탐지·대응체계 구축, 인터넷과 업무용 정보통신망 분리 등을 통해 사이버 방어 역량을 지속적으로 강화해 왔다.

그러나 진화하는 사이버공격에 효율적으로 대응하기 위해서는 국가 핵심 서비스의 생존성 강화 및 능동적인 대응 수단 확보가 더 한층 필요한 시점이다.

인력·예산

정부는 사이버안보 전문 인력을 지속 확충하고 관련 예산을 별도 항목으로 편성·확대하였으며 기업도 인력과 예산 투자를 확대해 왔다.

그러나 아직도 예산 비중이 선진국보다 낮은 수준이며 시장수요의 급증으로 전문 인력의 질적·양적 부족 현상도 심각하게 발생하고 있다.

산업·기술

정부는 관련 법률을 제정하여 보안 산업 경쟁력 강화와 일자리 창출을 견인하고 관련 기술에 대한 연구개발 계획을 지속 수립·시행해 오고 있다.

그러나 보안을 비용으로 인식하여 투자에 소극적이고 기초·차세대 보안기술 등의 연구가 활성화되지 못해 주요 국가와 기술 격차가 좁혀지지 않고 있다.

안보 의식

사이버위협으로 인한 피해의 급증과 정부의 다양한 인식 제고 노력으로 인해 개인과 기업 모두 사이버안보의 중요성에 대한 인식이 향상되었다.

그러나 개인은 기본적인 보안수칙을 실천하지 않고 많은 기업은 정보보호대책을 이행하지 않는 등 인식과 실천 사이에 괴리가 존재하는 것도 사실이다.

국제 협력

정부는 초국가적인 사이버위협에 대응하기 위해 우방국가 및 UN·ITU 등 국제기구와의 협력체계 구축을 추진하고 있다.

그러나 국제협약 가입, 정보·기술 교류 및 사이버안보 국제규범 마련 등 보다 체계적이고 실질적인 국제공조 활동 추진이 필요하다.

03

새로운 이정표

사이버공간의 변화와 도전 그리고 우리의 현실은 국가 사이버안보에 대한 보다 전략적이고 체계적인 접근방식을 요구하고 있다.

사이버위협에 대응하고 국가번영을 이룩하기 위해서는 일관된 전략을 바탕으로 분야별 역량을 강화하고 상호 협력이 절실히 필요하다.

정부는 사이버위협을 안보위협으로 인식하여 모든 역량을 결집·대응할 수 있도록 「국가안보전략」에 따라 「국가사이버안보전략」을 최초로 수립하였다.

전략 수립을 위해 그간의 사이버안보 정책의 성과와 대응체계, 제도, 역량 등에 대한 성찰과 다양한 의견을 수렴하였다.

「국가사이버안보전략」은 대한민국 사이버안보의 미래 비전과 목표를 제시하고 개인·기업·정부가 중점 추진해야 할 전략적 과제를 제시한다.

이를 통해 사회 각 주체별 역할과 책임이 명확해지고 국민적 실천문화가 형성되어 국가 전반의 사이버방어 능력이 제고될 것으로 예상한다.

또한, 사이버위협으로부터 우리의 사이버공간을 보호하여 국민 모두가 사이버공간을 더 안심하고 향유할 수 있게 될 것으로 기대한다.

II

비전 및 목표

비 전

자유롭고 안전한 사이버공간을 구현하여
국가 안보와 경제 발전을 뒷받침하고 국제 평화에 기여

목 표

1. **국가 주요기능의 안정적 수행**: 어떠한 사이버위협에도 지속적 운영이 가능하도록 국가 핵심 인프라의 생존성과 복원력 강화
2. **사이버공격에 빈틈없는 대응**: 사이버위협을 억지하고 조기 탐지·차단하며 신속하고 능동적인 사고대응 역량 확보
3. **튼튼한 사이버안보 기반 구축**: 사이버보안 기술·인력·산업이 경쟁력을 갖출 수 있는 공정하고 자율적인 생태계 조성

기본 원칙

1. **국민 기본권과 사이버안보의 조화**: 프라이버시 등 국민의 기본권 보장과 사이버공간 보호 활동을 균형 있게 추진
2. **법치주의 기반 안보활동 전개**: 정부의 사이버안보 정책과 활동은 관련 국내법과 국제법·규범을 준수하여 투명하게 추진
3. **참여와 협력의 수행체계 구축**: 개인, 기업, 정부가 사이버 안보 활동에 함께 참여하여 협력하며 국제사회와도 긴밀히 공조

National
Cybersecurity
Strategy

III

전략 과제

1. 국가 핵심 인프라 안전성 제고
2. 사이버공격 대응역량 고도화
3. 신뢰와 협력 기반 거버넌스 정립
4. 사이버보안 산업 성장기반 구축
5. 사이버보안 문화 정착
6. 사이버안보 국제협력 선도

01 국가 핵심 인프라 안전성 제고

국가핵심 인프라의 생존성과 복원력을 강화하여 어떠한 사이버 공격에도 국민 생활의 기반이 되는 서비스는 중단 없이 제공

1 국가 정보통신망 보안 강화

1) 국가 정보통신망의 구축, 운영, 폐기에 이르기까지 사이버위협으로부터 안전하게 운영될 수 있도록 단계별 보안조치를 시행한다.

2) 국가 정보통신망과 정보통신 장비의 보안 취약점으로 인해 위험이 발생하지 않도록 상시 점검 및 개선 방안을 마련한다.

3) 다양한 사이버 공격에도 국가 정보통신망 서비스를 지속하기 위한 시스템 성능 고도화, 백업설비 확충 등 생존성 강화 대책을 추진한다.

4) 모바일, 클라우드 등 최신 정보통신기술 기반 업무환경이 사이버위협의 표적이 되지 않도록 보안 기술·시스템을 적시 개발·적용한다.

5) 국가기밀이 유출·훼손되지 않고 안전하게 보호될 수 있도록 암호체계 및 기밀보호 시스템을 고도화한다.

6) 국가 정보통신망 구축시 국내외 기술 표준 준수를 강화하여 취약점 등 보안문제 발생시 신속히 대처하게 한다.

2 주요 기반시설 보안환경 개선

1) 국민 이용이 많고 사이버 공격시 피해가 큰 시설에 대해 국가가 주요 기반시설로 신속히 지정·보호할 수 있도록 관련 제도를 개선한다.

2) 주요 기반시설을 운영하는 기관이 사이버보안 업무 전담조직 및 일정비율 이상 예산을 확보할 수 있도록 지원을 강화한다.

3) 기관이 주요 기반시설을 구축하는 단계에서부터 보안을 고려할 수 있도록 가이드라인을 마련하고 관련 점검체계를 구축한다.

4) 민간분야 기반시설 관리기관이 도입하는 네트워크·정보보호 장비 등에 대해 자율적으로 보안성을 검토할 수 있는 환경을 마련한다.

5) 분야별 맞춤형 보안취약점 점검 기준을 마련하고, 사고발생시 서비스 지속성 확보대책을 시행한다.

3 차세대 보안 인프라 개발

1) 기술융합 및 신기술 등장으로 발생되는 새로운 보안위협에 대응하기 위한 기술적·제도적 방안을 마련한다.

2) 국민 생활과 직결되는 정보통신기술 제품·서비스의 보안이 확보될 수 있도록 개발 단계부터 보안기능을 내재화한다.

3) 사이버위협을 원천 차단할 수 있도록 高신뢰 네트워크를 개발·보급한다.

4) 초연결, 인공지능 환경에서 국민들이 온라인 서비스를 편리하고 안전하게 이용할 수 있도록 차세대 보안인증 인프라를 구축한다.

02 사이버공격 대응역량 고도화

사이버공격을 사전에 효율적으로 억지하고 사고발생시 신속하고 능동적으로 대응할 수 있도록 선제적이고 포괄적인 역량 확충

1 사이버공격 억지력 확보

1) 국가안보와 국익을 침해하는 모든 사이버공격에 대해 국가적 역량을 결집하여 적극 대응한다.

2) 사이버공간의 취약점을 효율적으로 수집·관리·제거할 수 있는 체계 구축을 통해 예방능력을 강화한다.

3) 사이버공격 원인 분석과 공격자 규명을 위한 실질적 역량을 확보한다.

2 대규모 공격 대비태세 강화

1) 대규모 사이버공격으로 인한 사이버위기 상황의 판단과 전파, 유관기관 합동 조사·대응 체계를 종합적으로 점검·보완한다.

2) 사이버공격에 대해 실시간으로 탐지·차단할 수 있도록 공격탐지 범위를 확대하고 인공지능기술 기반의 대응기술을 개발한다.

3) 민·관·군 합동 훈련을 실시하고 을지연습 등 국가 위기관리 훈련과 연계하여 범국가적 사이버위기 대응능력을 제고한다.

4) 사이버위기경보 발령, 위협정보 공유, 합동 조사·수사 등의 민·관·군 협업기반의 임무·기능을 활성화한다.

5) 개인, 기업 및 정부가 사이버위기 대응 조치를 적기 취할 수 있도록 사이버위기 수준 정량화 방안을 마련한다.

3 포괄적·능동적 수단 강구

1) 중대한 사이버안보위협 발생시 국제규범에 따라 취할 수 있는 모든 대응 수단을 검토하고 구체적 방안을 마련한다.

2) 사이버전에서 국가안보와 국익을 보호할 수 있도록 다양한 전략·전술 개발, 전력체계 보강 및 핵심기술을 확보한다.

3) 사이버전의 효율적 수행을 위해 사이버전 수행 인력을 전문화·정예화하고 대응조직을 증강한다.

4 사이버범죄 대응역량 제고

1) 사이버범죄에 악용되는 시설·서비스에 대한 관리를 강화하고 유관기관·기업·단체·국민 등이 참여하는 사이버안전망을 구축한다.

2) 사이버범죄 수사 전문성 및 국내외 유관기관간 협력을 확대하여 사이버범죄 주체에 대한 식별 및 검거·기소 역량을 제고한다.

03 신뢰와 협력 기반 거버넌스 정립

개인, 기업, 정부 간의 상호 신뢰와 협력을 바탕으로
민·관·군 영역을 포괄하는 미래지향적인 사이버안보 수행체계 확립

1 민·관·군 협력 체계 활성화

1) 정부를 비롯한 모든 이해당사자가 사이버안보에 대한 역할과 책임을 분담하고 상호 협력하는 거버넌스 체계를 정립한다.

2) 정부는 개인과 기업이 국가적 비전을 공유하고 자체 역량을 제고하여 각각의 역할과 책임을 다할 수 있도록 지원한다.

3) 사이버안보 전략·정책 및 관련 주요 이슈를 심층 연구하기 위한 국내외 전문가 협력 네트워크를 구축한다.

4) 민간분야 사이버안보 사각지대 해소를 위해 대응체계 개선, 유관기관간 공조체계 강화 및 지원기관의 인력·예산 확충을 추진한다.

5) 공공분야의 자체 보안관리 체계 구축을 위해 전담조직 및 전문인력을 확대하고 민간분야와 협력체계를 활성화한다.

6) 국방분야 정보통신망에 대한 사이버위협에 능동적으로 대응하기 위하여 국방 사이버안보 수행체계를 개선한다.

7) 민·관·군 협력체계를 강화하고 국가차원에서 사이버안보 정책을 발굴·추진하기 위해 국가안보실이 컨트롤타워 역할을 수행한다.

2 범국가 정보공유체계 구축 및 활성화

1) 사이버위협 정보를 신속하게 공유할 수 있도록 민간·공공·국방 영역을 포괄하는 국가차원의 정보공유체계를 구축한다.

2) 민·관·군 사이버위협 정보를 최대한 공유할 수 있는 방안을 지속적으로 발굴하고 시스템 기능을 개선·보완한다.

3) 공유되는 정보의 비밀 유지, 정보공유 과정에서 프라이버시 침해 및 목적 외 사용 방지 등을 보장할 수 있도록 법적 장치를 마련 한다.

4) 초국가적 사이버위협 대응을 위해 해외 전문기관과의 정보 공유를 적극 추진하고 관련 정보를 국내 유관기관과 공유한다.

3 사이버안보 법적기반 강화

1) 민·관·군 부문별 사이버안보 역량을 극대화하고 국가 역량을 결집하여 사이버안보 위협에 체계적으로 대응하기 위한 방향으로 법·제도를 개선한다.

2) 민·관·군 영역 간 사이버위협 정보를 체계적으로 공유하고 분석·활용할 수 있도록 법적 장치를 강구한다.

3) 인공지능기술 발전으로 인한 새로운 취약요인 출현 등 변화하는 사이버안보 환경에 적극 대응하기 위한 법적 근거를 강화한다.

04 사이버보안 산업 성장기반 구축

국가 사이버안보의 기반역량이 되는 기술·인력·산업의 경쟁력 확보를 위해 제도 개선, 지원 확대 등 보안산업 혁신 생태계 조성

1 사이버보안 투자 확대

1) 사이버보안 산업계가 국가 사이버안보 수준 향상에 중추적 역할을 할 수 있도록 규제 개혁 및 지원을 확대한다.

2) 정부의 정보보호 예산을 지속 확대하고 대규모 사이버공격 대응 등 유사시 활용할 수 있는 재원조달 방안을 마련한다.

3) 민간분야 투자 촉진을 위해 정보보호 공시제도를 활성화하고 보안시스템 및 연구개발 투자에 대한 세제지원을 확대한다.

2 보안 인력·기술 경쟁력 강화

1) 고도화되는 사이버안보 위협에 대응할 수 있도록 세계 최고 수준의 전문성과 경쟁력을 갖춘 사이버보안 인재를 집중 육성한다.

2) 기업, 정부, 군 등 국가사회 전반에 다양한 역량을 갖춘 인력이 공급될 수 있도록 생애주기별 맞춤형 인력양성 프로그램을 강화한다.

3) 사이버보안 업무 전문성을 향상시키고 우수 인재를 유치하기 위한 사기 진작방안을 마련한다.

4) 선진국과 기술격차를 해소하고 글로벌 시장을 선도할 혁신적 원천기술 확보를 위해 사이버보안 연구개발 예산을 대폭 확대한다.

3 보안기업 성장환경 조성

1) 혁신적인 기술 및 아이디어가 사업화될 수 있도록 정보보호 클러스터 구축 등 산·학·연 협업기반 창업환경을 마련한다.

2) 사이버보안 스타트업·중소기업들이 경쟁력 있는 기업으로 성장할 수 있도록 정부지원 강화 및 관련제도를 지속 개선한다.

3) 글로벌 기업과의 전략적 제휴 유도, 해외진출 지원을 위한 해외거점 확대 등을 통해 국내 보안 산업의 글로벌 경쟁력을 강화한다.

4 공정경쟁 원칙 확립

1) 사이버보안 제품·서비스의 조달체계 등을 '가격' 위주에서 '성능' 위주로 개선하여 기술경쟁 시장으로 체질을 강화한다.

2) 사이버보안 서비스에 대해 정당한 대가를 지불하기 위한 방안을 강구하고 불법 하도급 등을 철저히 조사·시정한다.

05 사이버보안 문화 정착

국민 모두가 사이버보안의 중요성을 인식하고 실천하며
정부는 정책 수행 과정에서 기본권을 존중하고 국민 참여를 활성화

1 사이버보안 인식 제고 및 실천 강화

1) 국민들이 사이버보안의 중요성을 인식하고 일상생활 속에서 쉽게 실천할 수 있도록 사이버보안 기본수칙을 개발·보급한다.

2) 학생, 공무원, 군인 및 기업인 등 사회분야별 맞춤형 사이버윤리 및 보안 교육프로그램을 개발·실시한다.

3) 기업이 소관 사이버공간을 보호하고 제품과 서비스에 적절한 수준의 보안을 유지할 수 있도록 사회적 책임을 강화한다.

2 기본권과 사이버안보의 균형

1) 정부는 자유롭고 개방적인 사이버공간에서 기본권을 존중하며 이를 불법·부당하게 간섭하거나 침해하지 않을 의무를 실천한다.

2) 국민 의견을 수렴하는 다양한 수단을 강구하여 국가 사이버안보 정책 과정에 국민 참여와 신뢰를 강화한다.

3) 정부는 사이버안보 상황에 대한 정보를 국익이 손상되지 않는 범위에서 국민에게 적극적이고 투명하게 공개한다.

06 사이버안보 국제협력 선도

국제적인 파트너십을 강화하고 국제규범 형성을 주도하는 등 사이버안보 선도국가로서의 리더십 확보를 통해 국가안보와 국익 수호

1 양·다자간 협력체계 내실화

1) 사이버정책협의회 개최, 국제기구 파트너십 강화, 국제협약 가입 등을 통해 양·다자간 실질적인 협력방안을 모색하고 공조체계를 구축한다.

2) 전쟁·테러·범죄 등 다양한 사이버안보 위협에 대응하기 위해 국방·정보·수사 등 분야별 협력 및 민간 교류를 촉진한다.

3) 국제협력 과정에서 유관부처가 정부의 정책 방향을 제시하고 수집한 정보를 상호 공유할 수 있도록 제도적 장치를 마련한다.

2 국제협력 리더십 확보

1) 사이버안보 관련 보편타당한 국제규범 정립 과정에 참여를 확대하고 국제규범 및 모범사례 확산을 선도한다.

2) 사이버공간에서의 오해와 오인으로 인한 국가간 긴장 고조를 예방하기 위해 신뢰구축 관련 논의에 적극 참여한다.

3) 상호 호혜적 관점에서 개발도상국 대상 사이버안보 기술과 제도를 제공하는 등 해외 사이버안보 역량강화 지원 사업을 확대한다.

Ⅳ

이행 방안

정부는 국민과 기업은 물론 국제 사회와 협력하여 「국가사이버안보전략」의 비전과 목표를 달성할 수 있도록 책임을 다하며 리더십을 발휘한다.

정부는 전략을 구체화하고 성실히 실행하기 위해 「국가 사이버안보 기본계획」과 「국가 사이버안보 시행계획」을 수립하여 추진한다.

각 부처는 사이버안보 관련 법규와 제도, 정책 등을 추진함에 있어 이 전략에 명시된 목표를 지향하고 기본원칙을 준수하며 전략 과제를 실천해야한다.

국가안보실은 이 전략의 이행 여부와 개인·기업·정부 등 각 주체별 사이버안보 수준의 향상 정도를 정기적으로 점검한다.

또한, 전략 이행에 필요한 예산, 인력, 조직 등 사이버안보 기반환경의 적절성을 평가하고 개선하기 위해 노력한다.

아울러 안보환경 변화에 따른 사이버안보 수행체계 및 추진전략의 효율성을 점검하여 미비점을 개선하고 필요시 이를 전략에 반영한다.

사이버안보는 정부뿐 아니라 개인, 기업 모두의 참여가 필수적인바 이를 위해 정부는 협력과 개방을 강화하고 정책 투명성을 높여 국민 신뢰 기반의 사이버안보 정책을 지속적으로 추진하겠습니다.

국가사이버안보전략

발 행 일 2019년 4월
발 행 처 국가안보실
문 의 02-770-7393
jykim0110@president.go.kr

발간등록번호 12-1025000-000003-01