2023 국가정보보호 백서

National Cybersecurity White Paper

발간기관

국가정보원 NATIONAL INTELLIGENCE SERVICE

과학기술정보통신부 Ministry of Science and ICT

행정안전부 Ministry of the Interior and Safety

개인정보보호위원회 Personal Information Protection Commission

금융위원회 Financial Services Commission

외교부 Ministry of Foreign Affairs

지원기관

KISA 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY

NSR 국가보안기술연구소

금융보안원 FINANCIAL SECURITY INSTITUTE

2023 국가정보보호 백서

National Cybersecurity White Paper

발간기관 국가정보원 NATIONAL INTELLIGENCE SERVICE · 과학기술정보통신부 Ministry of Science and ICT · 행정안전부 Ministry of the Interior and Safety · 개인정보보호위원회 Personal Information Protection Commission · 금융위원회 Financial Services Commission · 외교부 Ministry of Foreign Affairs

지원기관 KISA 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY · NSR 국가보안기술연구소 · 금융보안원 FINANCIAL SECURITY INSTITUTE

일러두기

백서에 수록된 통계와 지표 수치는 반올림되었으므로 세부 항목의 합과 전체 합계가 일치하지 않을 수 있습니다.

2023 국가정보보호백서의 **구성과 특징**

2023 국가정보보호백서는 〈서두〉·〈본문〉·〈부록〉 등으로 구성되어 있다.
먼저 2022년 정보보호와 관련된 주요 내용을 나타내는 '**정보보호 연혁**'과 '**2022년 정보보호 10대 이슈**'를 서두로 하였다. '**정보보호 연혁**'은 최근까지의 중요한 정책, 입법 및 사건을 연도별로 정리하여 역사적 의미를 이해하는 데 도움이 되도록 하였다.

'**2022년 정보보호 10대 이슈**'는 2022년 주요 언론 매체 및 유관 기관에서 발표한 정보보호 관련 이슈를 바탕으로 정보보호 전문가들의 의견 수렴을 통하여 선정한 내용을 소개하였다.

〈본문〉 중 **제1편 '정보보호 환경 변화 및 사이버위협 동향'**에서는 국내외 정보보호 환경의 변화와 그에 따른 사이버공격 및 위협의 변화를 다루었다.

제2편 '정보보호 법·제도 및 기관'에서는 정보보호 담당기관과 법·제도를 다루었다. 정보보호 법·제도는 정보보호 법·제도 발전 과정, 분야별 정보보호 법·제도와 2022년 주요 제·개정 법령을 작성하였으며, 정보보호 담당기관은 국가기관과 전문기관으로 나누어 소개하였다.

제3편 '분야별 정보보호 활동'에서는 국가정보통신망 보호, 디지털정부, 주요정보통신기반시설, 정보통신서비스, 금융서비스 등 주요 분야별로 정보보호 정책과 제도 및 활동 등을 상세하게 다루었다.
제1장 '국가정보통신망 보호'에서는 사이버공격 탐지·차단, 사고조사 및 정보 공유, 보안관리컨설팅 및 관리실태 평가, 보안적합성 검증, 암호모듈 검증, 정보보호제품 평가·인증 등을 소개하였다.
제2장 '디지털정부'에서는 디지털정부 정보보호, 소프트웨어 개발보안, 전자서명 인증 등을 소개하였다.
제3장 '주요정보통신기반시설'에서는 주요정보통신기반시설 보호 추진체계와 주요 활동, 국내외 침해사고 사례 등을 소개하였다.
제4장 '정보통신서비스'에서는 침해사고 대응과 예방 활동, 정보보호 관련 제도, 융합보안 등을 소개하였다.
제5장 '금융서비스'에서는 금융서비스 정보보호, 금융분야 사이버공격 대응 및 정보 공유, 금융 IT 및 전자금융·핀테크의 보안평가·점검 등을 소개하였다.

제4편 '정보보호 기반조성'에서는 정보보호산업 육성, 정보보호 기술 개발, 정보보호 인력 양성 분야, 개인정보보호, 대국민 정보보호, 국제협력 등의 내용을 다루었다.
제1장 '정보보호산업 육성'에서는 정보보호산업 현황과 산업 육성을 위한 다양한 정책과 제도를 소개하였다.
제2장 '정보보호 기술 개발'에서는 원천기술 개발 현황과 상용기술 개발 현황을 소개하였다.
제3장 '정보보호 인력 양성'에서는 정규교육과정 및 전문기관 교육과정에 의한 인력 양성, 정보보호 자격증 제도 등을 소개하였다.
제4장 '개인정보보호'에서는 개인정보보호를 강화하기 위하여 그 동안 추진한 정책 등을 소개하였다.
제5장 '대국민 정보보호'에서는 정보보호 상담과 처리, 인식제고 활동 등을 소개하였다.
제6장 '국제협력'에서는 사이버안보 외교 활동과 사이버보안에 관련한 국제협력 활동에 대한 내용을 소개하였다.

끝으로 〈**부록**〉에서는 우리나라의 정보보호 수준을 정확하게 이해하기 위하여 설문조사를 통하여 획득한 통계자료를 국가·공공부문과 민간부문으로 나누어 구체적으로 제공하였다. 또한 2022년 주요 정보보호 행사, 국내 정보보호 관련 주요 사이트, 정보보호 관련 민간단체, 국내 ISAC 현황 등을 소개하였다.

정보보호 **연혁**

1964 _ 1999

1964
- 「보안업무규정」(대통령령) 및 규정 시행규칙(대통령훈령) 제정

1981
- 국가 통신 보안 업무에 대한 기획·조정 절차와 방법 규정을 위한 「정보 및 보안업무 기획·조정규정」(대통령령) 제정

1986
- 「전산망보급확장과이용촉진에관한 법률」 제정

1989
- 국내 최초 정보보안 학술대회(WISC) 개최

1990
- 한국통신정보보호학회(KIISC) 설립

1994
- 체신부 확대 개편 및 과학기술처·공보처·상공자원부 정보통신 관련 기능을 흡수·통합한 정보통신부 출범

1995
- 제1회 정보통신망 정보보호 콘퍼런스(NetSec-KR) 개최

1996
- 한국정보보호센터(KISA) 설립

1998
- 한국정보보호산업협회(KISIA) 설립
- 최초 국산 블록암호 알고리즘(SEED) 개발
- 정보보호시스템 평가·인증 제도 시행

1999
- 을지연습 시 사이버전 모의훈련 최초 실시
- 「전산망보급 확장과 이용촉진에 관한 법률」을 「정보통신망 이용촉진 등에 관한 법률」로 개정
- 「국가정보통신보안기본지침」 제정
- 「전자서명법」 제정

2000 _ 2010

2000
- 국가보안기술연구소(NSRI) 설립
- 한국전자통신연구원(ETRI) 정보보호연구본부 설립

2001
- 「정보통신기반보호법」 제정
- 「전자정부구현을 위한 행정업무 등의 전자화촉진에 관한 법률」 제정
- 「정보통신망 이용촉진 등에 관한 법률」을 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」로 개정
- 한국사이버테러정보전학회(KIAS) 설립
- 한국정보보호센터(KISA)가 한국정보보호진흥원(KISA)으로 승격
- 정보보호 관리체계 인증제도(ISMS) 도입
- 한국통신정보보호학회(KIISC)가 사단법인 한국정보보호학회로 명칭 변경

2002
- 국가정보보호백서 창간
- 국가정보보안연합회(NISA) 설립
- 정보보호시스템 공통평가기준(CC) 제정

2003
- 1.25 인터넷 대란 발생
- KISA 인터넷침해사고대응지원센터 설립
- 대국민 행정서비스용 블록암호 알고리즘(ARIA) 개발

2004
- 국가사이버안전센터(NCSC) 설립
- 「국가위기관리기본지침」(대통령훈령) 및 국가사이버위기관리 매뉴얼 제정

2005
- 「국가사이버안전관리규정」(대통령훈령) 제정
- 제1회 사이버안전의날 개최

2006
- 국제상호인정협정(CCRA) 인증서 발행국 가입
- 국가 사이버위기대응 통합연습 실시
- 금융보안연구원(FSA) 설립

2007
- 정보보호제품 민간 평가기관 지정
- 「전자정부구현을 위한 행정업무등의 전자화촉진에 관한 법률」을 「전자정부법」으로 개정

2008
- 범국가 차원의 보안관제 체계 구축 및 국방·외교·행정 등 10대 핵심 부문 보안관제센터 설립

2009
- 7.7 디도스(DDoS) 공격 발생
- 국가 사이버위기 종합 대책 수립
- 한국인터넷진흥원(KISA) 출범 (한국정보보호진흥원, 한국인터넷진흥원, 정보통신국제협력진흥원 통합)
- 한국지식정보보안산업협회(KISIA) 재출범

2010
- 사이버사령부 설립
- 전자금융거래 공인인증수단 다양화
- 「전자정부법」 전부 개정

2011 _ 2015

2011
- 「개인정보보호법」 제정 및 개인정보보호 위원회 출범
- 3.4 디도스 공격 발생
- 국가 사이버안보 마스터플랜 수립 및 시행
- 국군사이버사령부(R.O.K. Cyber Command) 출범
- 개인정보보호 관리체계 인증제도(PIMS) 도입
- 금융회사 IT보안 강화 종합 대책 수립 시행

2012
- 정보보호의 날 제정
- 민·관·군 사이버위협 합동대응팀 가동
- 한국사이테러정보전학회(KIAS)가 한국융합보안학회(KCGSA)로 명칭 변경

2013
- 소프트웨어 취약점 신고포상금제 운영
- 3.20 사이버테러, 6.25 사이버공격 발생
- 국가 사이버안보 종합 대책 발표
- 인터넷상 주민등록번호 수집 및 사용 제한 제도 시행
- 정보보호 최고책임자 협의회(CISO) 출범

2014
- 카드사 및 통신사 고객 정보 유출, 정상화 대책 발표
- 한국수력원자력(KHNP) 해킹 사고 발생
- 국가보안기술연구소 사이버안전훈련센터 (CSTEC) 개소

2015
- 「정보보호산업의진흥에관한법률」 제정
- '개인정보 유효기간제' 실시
- 금융보안원(FSEC) 출범
- 국가사이버위협 정보공유시스템 운영
- 국가사이버안보태세 강화 종합 대책 발표
- 한국지식정보보안산업협회(KISIA)가 한국정보보호산업협회로 명칭 변경

2016 _ 2022

2016
- K-ICT 융합보안 발전 전략 발표
- 사이버 시큐리티 인력 양성 종합 계획 발표
- K-ICT 시큐리티 2020[제1차 정보보호산업 진흥계획 (2016 ~ 2020)] 발표
- 정보보호 관리체계 인증 의무 대상 확대(교육·의료 분야)
- 정보보호 공시제도 도입·운영
- 워너크라이 랜섬웨어 공격

2017
- 국내 호스팅업체 랜섬웨어 감염 사고 발생
- 국내 가상화폐거래소 해킹 사고 발생
- 정보보호클러스터 개소
- 범부처 IP카메라 종합 대책 발표
- 민간자율 IoT 보안인증 제도 도입

2018
- 한국인터넷진흥원 사이버보안 빅데이터센터 개소
- 정보보호 및 개인정보보호 관리체계인증(ISMS-P) 통합

2019
- 국가사이버안보 전략 발표
- 국가사이버안보 기본 계획 발표
- 5G+ 전략 발표
- 사이버작전사령부(Cyber Operations Command) 출범

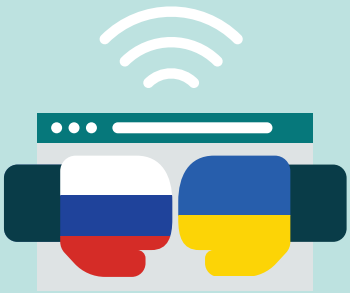
2020
- 「국가정보원법」 개정 및 「사이버안보 업무규정」 제정
- 「전자서명법」 전부 개정으로 인한 공인인증서 폐지
- '데이터 3법(「개인정보 보호법」, 「정보통신망법」, 「신용정보법」)' 개정
- 제2차 정보보호산업 진흥계획 발표

2021
- 디지털뉴딜 종합계획 내 K-사이버방역체계 구축 발표
- 범부처 랜섬웨어 대응 강화방안 발표
- 국가사이버안보센터(NCSC) 출범
- EU GDPR 개인정보보호 적정성 결정 최종 승인
- 「정보보호산업법」시행령 개정에 따른 정보보호 공시 의무화 제도 시행

2022
- 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「정보통신기반보호법」 개정
- NATO 사이버방위센터 가입
- 디지털플랫폼정부 추진 계획 발표
- 대한민국 디지털 전략 발표
- 12대 국가전략기술 발표
- 공공분야 도입·운용 IT보안제품 신보안적합성 검증체계
- 국가사이버안보협력센터(NCCC) 개소
- 대한민국의 영국 개인정보보호 적정성 결정 최종 승인

2022년 정보보호 10대 이슈

2022년 한 해 동안 국내에서 주요한 관심사로 떠오른 정보보호 10대 이슈를 소개한다.
이들 이슈를 통하여 2022년 한 해 동안의 주요 정보보호 동향을 돌아보는 한편, 정보보호에 대한 인식을 제고하고자 한다. 주제 선정을 위하여 백서 발간에 참여한 기관의 담당자와 외부 전문가가 참여하였으며, 다수의 주제 후보를 먼저 선정하고 이 주제 후보 중 유사한 주제를 통합하는 한편, 여러 기관에서 중복하여 제안한 주제를 중심으로 최종 후보를 선정하였다.
이후 편집위원회 및 자문위원회의 협의를 거쳐 최종 후보 중 10개의 주제를 엄선하였다. 2022년 이슈는 국가 정책 및 제도 개선 사항과 신기술에 수반되는 보안 관련 내용 그리고 주요 보안사건 사고로 구성되었다.



01 러시아-우크라이나전 등 현대 전쟁을 통하여 본 사이버공격의 위력

02 북한 등 국가배후 해킹 확산에 따른 사이버안보 위협 고조

03 국내외 관심 이슈 악용 '사회공학적 해킹' 공격 지속 증가

04 외화벌이 목적 등 가상자산 타기팅 사이버공격 전세계 확산

05 '디지털플랫폼정부' 출현에 따른 사이버보안 중요성 증가

06 정부와 기업 간 소통·협력·상생의 '국가사이버안보협력센터' 개소

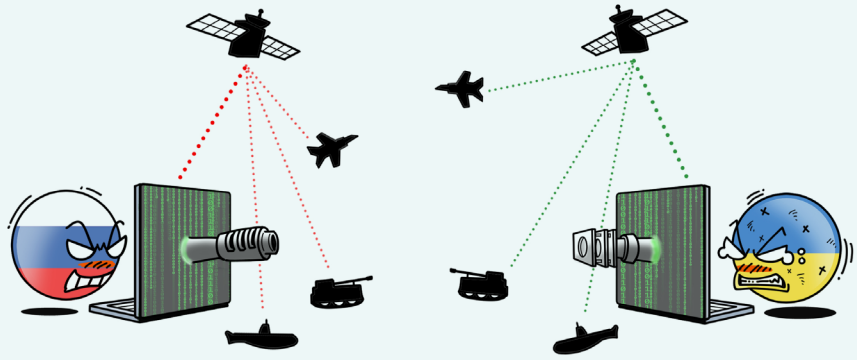
07 아시아 최초 'NATO 사이버방위센터' 정회원 가입, 국제 공조 수준 제고

08 국가정보원, 세계 최초 양자암호통신 안전성 검증체계 수립

09 범정부 차원의 체계적 대응을 위한 사이버안보법 제정 추진

10 공공분야의 안전한 민간 클라우드 도입을 위한 클라우드 보안인증제 개선 추진

01 러시아-우크라이나전 등 현대 전쟁을 통하여 본 사이버공격의 위력



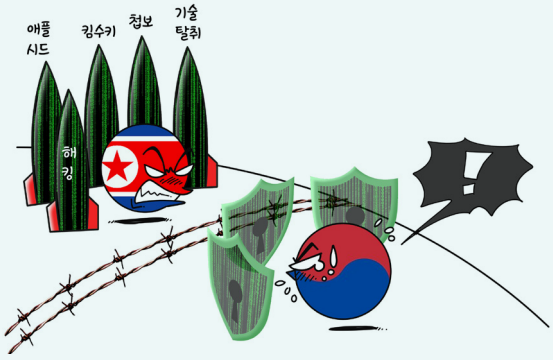
2021년 말 러시아는 우크라이나의 북대서양조약기구(North Atlantic Treaty Organization, NATO) 가입 움직임에 대항하여 우크라이나 접경지역에 군사력을 집중적으로 배치하였다. 러시아·우크라이나·미국·NATO 사이의 외교적 해결 노력이 결국 실패로 돌아가자, 2022년 2월 24일 러시아는 우크라이나를 침공하였고, 현재까지 전쟁이 이어지고 있다.

우크라이나·미국·영국·EU는 2022년 1월 우크라이나 정부 웹사이트와 금융기관 등을 상대로 발생한 웹변조와 디도스 공격이 러시아의 행위라며 공개적으로 배후를 지목한 바 있다. 또한 우크라이나는 2022년 2월 24일 러시아가 침공하기 대략 한 시간 전 미국의 통신회사 비아셋(Viasat)이 운영하는 위성 네트워크를 상대로 사이버공격을 받았다고 발표하였다. 이 공격으로 위성 통신에 상당히 의존하고 있던 우크라이나의 군 통신이 타격을 입었고, EU 회원국 역시 영향을 받게 됨에 따라 EU는 이러한 사이버공격이 '사이버공간에서 지속되는 러시아의 무책임한 행동 패턴의 전형'이라며 비난하였다.

이러한 사이버공격에도 우크라이나는 치명적 피해를 받지 않았다. 이는 우크라이나가 2014년 크림반도 병합 이후 사이버위협에 대비하여 대응 역량을 꾸준히 강화해 왔고, 미국·EU 등과도 파트너십을 맺고 정보를 공유해 왔기 때문으로 보인다. 미국 전략국제연구소(Center for Strategic and International Studies, CSIS) 제임스 루이스(James Lewis) 수석부소장은 러시아-우크라이나 전쟁에서 우크라이나의 사이버공격 대응에 관하여 '사이버공간에서 잘 준비되고 적극적인 방어가 공격보다 이점을 가질 수 있다'고 평가하였다.

우리는 우크라이나의 사이버안보 역량 강화 노력으로부터 교훈을 얻어야 한다. 국제협력을 강화하여 국가 간 정보 공유를 활성화할 필요가 있으며, 민간이 보유한 위협정보의 신속한 공유 등 민간부문의 참여 활성화 방안을 모색할 필요가 있을 것이다.

02 북한 등 국가배후 해킹 확산에 따른 사이버안보 위협 고조

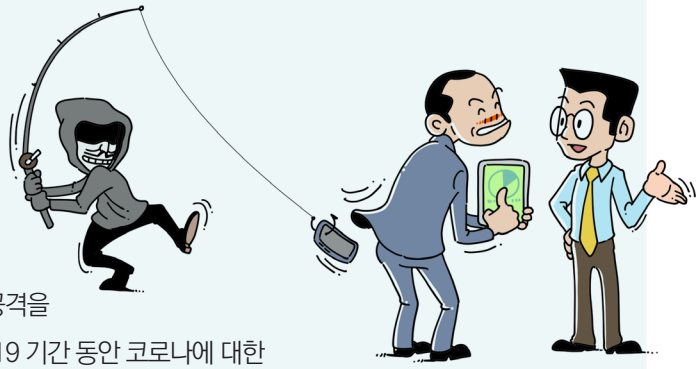


디지털 전환이 가져온 산업 패러다임 변화는 우리 생활 전반과 사이버공간의 융합을 촉진하고 있다. 이는 편의성과 효율성 증진을 꾀하는 한편, 사이버공격에 노출되는 영역도 증대시켰다. 국민의 보편적 일상은 물론 경제·사회의 존속을 위한 기반 전체가 사이버위협의 대상이 되는 것이다. 특히 방위산업·원자력 등과 같은 국가핵심기술에 대한 지식재산 탈취와 주요 기반시설 마비 등을 목표로 하는 사이버공격이 급증하여 국가안보를 직접적으로 위협하고 있다. 고도화된 공격기법과 막대한 자본을 기반으로 한 국가배후 해킹조직이 국가안보를 위해(危害)하는 사이버공격의 주요 위협원으로, 최근 미국·중국, 러시아·우크라이나 등 국가 간 갈등과 분쟁이 격해짐에 따라 이들의 활동 빈도와 범위가 더욱 증가하고 있는 중이다. 우리나라의 경우 사이버 능력을 핵심 비대칭 전력 중 하나로 삼고 있는 북한이 사이버 수단을 활용하여 지속적인 위해 활동을 전개하고 있다.

2021년 한국원자력연구원이 북한 소행으로 추정되는 사이버공격을 받은 데 이어, 2022년에도 국내 원자력 관련 조직과 기업에 대한 공격 시도가 지속되고 있다. 원자력 부문 관계자 대상의 피싱공격이 포착된 것이다. 공격자는 '배치도 고리2호기' 등 원전 관련 문서 형태로 위장한 문건에 백도어 악성코드를 숨겨 개인정보 탈취와 같은 악의적 활동을 꾀하였는데, 이 때 활용된 악성코드는 '애플시드'로 알려졌으며, 이는 북한이 지원하는 해킹조직 '킴수키'가 개발한 것으로 추정된다. 국가안보와 직결된 국방 핵심원천기술에 대한 탈취시도 또한 지속되고 있다. 2018~2022년 방위산업기술 연구·개발·생산과 관련된 국방과학기술연구소와 방위산업청 대상의 해킹시도만 3만 건 이상인 것으로 집계되고 있다. 시스템 무단접속, 악성코드 삽입 등 형태와 방법이 다양한 악성행위들이며, 시도 횟수가 매년 크게 증가하고 있다.

국가사이버안보센터는 국내 원자력·방위산업뿐 아니라 반도체 등 국가 주요기반산업 전반을 대상으로 한 국가배후 해킹조직의 침해시도가 거세질 것으로 전망하였다. 이러한 우려에도 높은 점유율로 광범위하게 활용되는 플랫폼과 소프트웨어, 애플리케이션을 악용하는 사례가 증가하여 공격에 대한 대비도 쉽지 않다. 더욱이 우리나라와 대치 중인 북한은 기술 탈취, 첩보, 자금 조달 등을 위하여 지속적으로 사이버 역량 강화에 힘을 쏟고 있어, 우리나라 사이버안보 리스크를 증대시키고 있다. 국내 민간 및 정부 유관부처 간 협력과 우방국과의 국제협력을 통한 강력한 안보태세 확립이 그 어느 때보다 중요한 시기이다.

03 국내외 관심 이슈 악용 '사회공학적 해킹' 공격 지속 증가



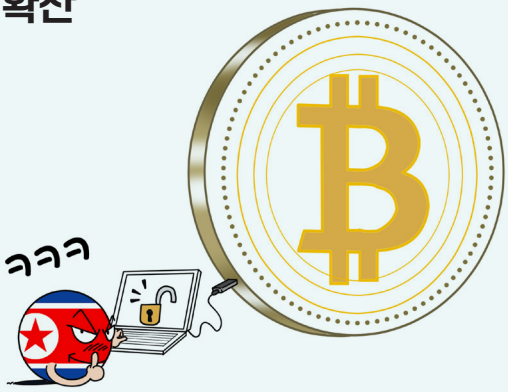
사회공학적 해킹'은 시스템 보안 취약점을 노린 기술적 해킹이 아니라 사람의 사회적·심리적 요인을 악용하여 권한 탈취를 노리는 해킹 기법으로, 그 동안에는 내부자 위협, 표적화 공격, 피싱 공격을 위한 세부 기법 중 하나로 여겨 왔다. 그러나 코로나19 기간 동안 코로나에 대한 두려움을 악용하는 사회공학적 해킹이 급증하면서 관련 공격이 다양화·지능화되어 별도의 위협 형태로 발전하였다.

코로나19를 기점으로 인터넷 암시장으로 불리는 다크웹에서 피싱을 위한 인프라와 서비스를 제공하는 Phishing-as-a-Service(PhaaS), 이른바 피싱 키트 판매가 성행하면서 피해 규모가 양적·질적으로 확대되고 있다. 이 피싱 키트는 피싱에 활용되는 콘텐츠를 합법적인 콘텐츠로 위장할 수 있도록 맞춤법과 문법을 교정하고, 적절한 이미지 사용을 지원함으로써 피싱을 위한 초기 진입장벽을 낮추어 더 많은 위협행위자를 유인하고 있으며, 나아가 피해자로부터 취득한 자격 증명을 피싱 키트를 개발·판매한 범죄집단에도 전달하여 2차 피해를 초래하고 있다.

다양화·고도화된 사회공학적 해킹은 재난과 장애 등 사회적으로 민감하고 관심도가 큰 이슈가 발생할 때마다 기승을 부릴 것으로 전망된다. 지난 한 해 국내에서는 경기도 판교 SK(주) C&C 데이터센터 화재로 '카카오 먹통'이 발생하자 '카카오톡 설치파일(KakaoTalkUpdate.zip 등)'로 위장한 악성코드가 발견되었고, 서울 이태원 사고 이후에는 '서울 용산 이태원 사고 대처상황(06시)'이라는 제목의 공문서 위장 공격이 확인되었다. EU의 사이버보안 전문기관 ENISA(European Network Information Security Agency)도 사이버위협 경향 보고서를 통하여 2022년 8대 사이버위협 중 하나로 사회공학적 공격을 언급하며 다양화·고도화되는 피싱 공격의 위험성을 경고하였다.

사회공학적 해킹은 소프트웨어나 시스템의 취약점이 아닌 사람의 실수나 불안과 같은 사회·심리적 요인을 공격에 이용한다는 점에서 기술적·관리적 예방 및 탐지가 어렵다는 특징이 있다. 더욱이 그 수법이 갈수록 교묘해지고 전문화·분업화되고 있기 때문에 이러한 공격을 완벽히 방어하기는 사실상 불가능에 가깝다고 할 수 있다. 이에 사회공학적 해킹에 대한 개인의 보안의식을 향상하고, 다중인증(Multi Factor Authentication, MFA)과 같은 계정 보안을 강화하는 등 전 국민이 사이버위생(Cyber Hygiene) 향상 노력에 적극 동참하여야 할 것이다.

04 외화벌이 목적 등 가상자산 타기팅 사이버공격 전세계 확산



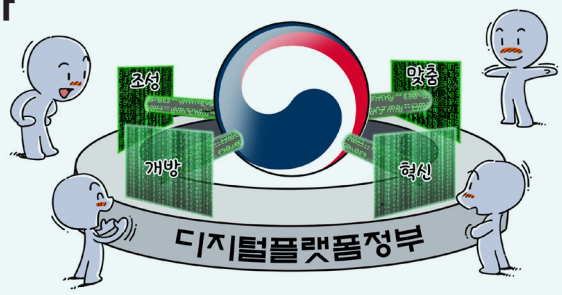
최근 북한이 수행하는 사이버공격의 빈도와 규모가 급증하고 있고 공격의 형태도 다양해지고 있다. 특히 대북제재가 심화됨에 따라 북한은 새로운 외화벌이 영역으로 사이버 금전 탈취에 주력 중이다. 가상자산은 자금 추적이 어렵고, 시스템 침해 및 탈취에 성공한 후 돈세탁 과정 등 자금 활용까지의 과정이 기존 금융체계에 비하여 용이하기 때문이다.

2017~2018년 북한의 초기 해킹 방식은 국외의 가상자산 거래소를 직접 해킹하는 것이었다. 취약점이 노출된 운영 서버를 해킹하여 거래 서버에 직접 접근하거나, 거래소 임직원에게 피싱 메일을 보내 내부망 메인 서버에 접근하는 방식이다. 실제 국내 최대 규모 가상자산거래소 '빗썸(Bithumb)'은 2017~2018년 북한에 의하여 최소 4회 이상 침해되었으며, 총 5,800만 달러 상당의 사이버 금전을 탈취당하였다.

북한의 해킹 방식은 점차 진화하여 2022년 3월에는 베트남 비디오 게임사 '스카이마비스'의 사내 탈중앙화 금융시스템을 해킹하여 가상자산 7,500억 원가량을 탈취하고, 5월에는 미국의 블록체인기업 '하모니'의 '호라이즌 브릿지'를 해킹하여 가상자산 1,300억 원을 탈취하였다. 브릿지는 가상자산을 블록체인에서 다른 블록체인으로 이동해 주는 응용 프로그램으로 해킹에 비교적 취약하다는 지적을 받고 있다. 미국 체이널리시스사에 따르면 2022년 북한의 사이버공격으로 인한 가상자산 피해액은 약 2조 원으로 추정되고 있으며, 이는 전체 가상자산 해킹 피해액의 50%를 웃도는 것으로 파악된다.

국내에서는 특정 금융거래법에 따라 가상자산 거래가 실명제로 바뀌어 보안이 강화되었기 때문에 2022년에 가상자산을 절취당한 사례는 없는 것으로 알려져 있다. 그러나 국내 가상자산 시장 규모는 꾸준히 증가 중이기 때문에 북한의 해킹 위협의 대상이 될 가능성이 여전히 존재한다. 이에 국가정보원은 북한의 해킹 위협에 선제적으로 대응하기 위하여 2022년 11월 경기도 판교에 '국가사이버안보협력센터'를 개소하였다. 민·관·군으로 분리된 우리나라 사이버 대응 역량을 결집하고 국제 공조를 강화하여 공격 정보를 공유·분석하는 등 범국가적 공동 대응 체계를 갖추어 나갈 것으로 보인다.

05 ‘디지털플랫폼정부’ 출현에 따른 사이버보안 중요성 증가



윤석열 정부는 효율적인 국정운영을 약속하면서 2022년 5월 모든 데이터가 연결되는 ‘디지털플랫폼정부’ 추진 계획을 발표하였다. 디지털플랫정부는 국민·기업·정부가 함께사회 문제를 해결할 수 있는 장을 마련하고 이를 통하여 새로운 가치를 창출하는 것을 목표로 한다. 이를 위하여 같은 해 9월 공식 출범한 디지털플랫폼정부위원회는 ▲맞춤형 공공 서비스 제공 ▲양질의 데이터 전면 개방 ▲정부의 일하는 방식 혁신 ▲안전한 이용 환경 조성을 4대 중점 추진과제로 설정하고, 2023년 3월 중 디지털플랫폼정부 로드맵을 발표하였다.

업무환경에 클라우드·인공지능 등 새로운 IT의 접목이 확대됨에 따라 세계적으로 인정받는 전자정부 강국으로서 각 부처·기관에서 운영 중인 시스템 간 효율적이면서도 안전한 연계 환경 마련이 필요한 상황이다. 이에, 정부는 디지털플랫폼정부를 구현하여 범정부 데이터·서비스의 개방·연계·활용이 가능한 인프라를 구축하고, 데이터를 안전하고 신뢰성 있게 사용할 수 있는 체계를 마련하고자 한다. 또한 클라우드 기반으로 서비스를 개발하여 접근성·효율성을 향상하고 인공지능 기술을 도입하여 공공 서비스를 지능화할 계획이다. 디지털플랫폼정부가 구현될 경우 보안성이 담보된 간편한 인증·결제 수단을 통하여 각종 대국민 서비스를 편리하게 이용할 수 있을 것으로 전망된다.

디지털플랫폼정부가 활성화될 경우 공공행정 정보, 국민 개인정보 등을 통합·처리·공유하게 되어 고부가가치 데이터를 노리는 사이버공격의 표적이 될 가능성이 있다. 이에 정부는 디지털플랫폼정부의 설계 과정에서부터 블록체인, 인공지능, 양자암호 통신 등 첨단보안기술의 도입과 함께 제로 트러스트(Zero Trust)* 개념 기반의 보안체계 확립 등 다각적인 보안 전략을 모색하고 있다.

디지털플랫폼정부의 핵심 중 하나는 ‘단일 플랫폼 내 모든 데이터의 통합’이라고 할 수 있다. 기존 사이버보안 정책뿐 아니라 제로 트러스트의 관점에서 모든 사용자·단말기에 최소 권한을 부여하고, 사용자 계정과 업무 연관성에 따라 필요한 접근만을 허가할 수 있는 강력하고 동적인 보안체계를 형성할 필요가 있다는 것이다. 그러나 제로 트러스트 기반의 보안체계는 단순히 보안 솔루션을 도입하는 것만으로는 달성될 수 없으며, 사이버보안 전반에서의 변화가 요구되므로 기존 사이버보안 정책과 융합되어 보안성이 강화될 수 있도록 장기적인 계획 속에서 지속적인 정책 변화가 핵심이 될 것으로 보인다.

---

* 보안 시스템(보안경계)을 통과하여 IT 시스템에 접속한 사용자·단말기라라도 IT 자원(네트워크, 데이터, 시스템, 응용프로그램 등)에 접근을 요청할 때 보안 위반사항이 포함될 수 있다고 가정하고 지속적으로 재확인하는 보안 전략으로, IT 자원에 대한 모든 접근에 최소 권한을 부여하고 포괄적으로 모니터링함으로써 강력하고 동적인 대응을 가능하게 한다.

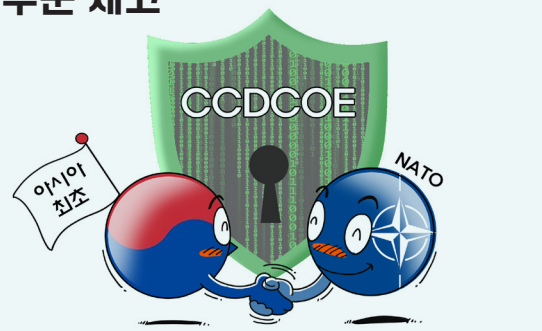
06 정부와 기업 간 소통·협력·상생의 '국가사이버안보협력센터' 개소

2022년 11월 국가정보원은 지능화·고도화하고 있는 사이버 공격에 맞서 정부와 기업이 협력하여 사이버 안보 위협 정보와 기술을 공유하는 한편, 공동 대응할 수 있도록 기존 국가사이버안보센터의 하부조직으로 국가사이버안보협력센터(이하 '협력센터')를 설립하였다. 협력센터는 기획재정부·과학기술정보통신부·국방부·행정안전부·금융보안원 등 유관 정부기관과 민간 IT보안 기업이 함께 참여하여 설립된 조직이다. 사이버안보 위협 동향·기술 분석과 정보 공유가 센터의 설립 목적으로, 유관 정부기관 직원과 민간기업 직원이 함께 센터에 상주하며 협업하게 된다.

미국과 영국도 정부와 기업의 사이버안보 위협 정보 분석·공유를 위하여 우리나라 협력센터와 유사한 조직을 설립·운영 중이다. 미국은 국가안보국 사이버안보협력센터[NSA Cybersecurity Collaboration Center(CCC)]를 운영하여 국외 사이버안보 위협에 대한 분석·공유 업무를 수행하고 있고, 국가정보국(DNI) 산하 정보협력 합동기구로서 사이버위협정보통합센터(CTIIC, Cyber Threat Intelligence Integration Center)를 설립하여 사이버위협 정보 수집 및 해킹 배후를 규명하고 있다. 영국은 국가통신정보본부(GCHQ) 산하 국가사이버안보센터(NCSC)를 통하여 사이버안보 정보 공유 파트너십(CISP, Cybersecurity Information Sharing Partnership)을 운영 중이고, 회원사와 함께 근무하며 사이버안보 위협 정보를 분석·공유하는 조직을 마련하고 있다.

우리나라 협력센터는 현재 5개 기업과 국가정보원을 포함한 18개 국가·공공기관이 참여하고 있으며, 앞으로 더 많은 업체와 기관이 추가로 참여할 예정이다. 또한 국가정보원은 '차세대 국가 사이버위협 정보공유 시스템'을 개발하여 사이버안보 위협 정보 공유 대상을 더욱 확대하고, 향후 가상자산 관련 해킹 공격 수법과 최신 악성코드 등 전문 정보도 공유하는 협력 강화 계획도 발표하였다. 사이버안보 위협에 대한 정보 공유는 사이버 위험을 최소화 및 예방하는 데 매우 중요한 요소로, 협력센터는 국가 사이버안보에서 정부와 기업이 소통·협력·상생하는 창구 역할을 수행할 것이다. 이번 협력센터 개소를 계기로 국내에 사이버위협 정보 공유·협력 문화가 확산될 것으로 기대된다.

07 아시아 최초 'NATO 사이버방위센터' 정회원 가입, 국제 공조 수준 제고



Cooperative Cyber Defence Centre of Excellence

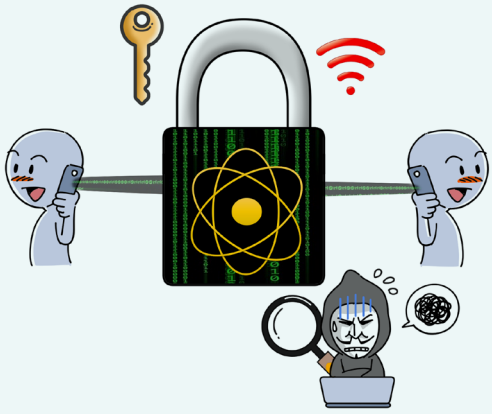
2022년 5월 우리나라는 NATO 사이버방위센터(Cooperative Cyber Defence Centre of Excellence, CCDCOE)에 정식 가입하였다. CCDCOE는 2007년 에스토니아를 대상으로 발생한 대규모 사이버공격이 계기가 되어 에스토니아 주도로 2008년 5월 14일 에스토니아의 수도 탈린에 설립되었으며, NATO 동맹국과 그 외 파트너들과 함께 유사한 입장을 취하는 국가 간 사이버안보 협력을 강화하는 것을 목표로 활동한다. CCDCOE 회원의 지위는 후원국과 기여국으로 나뉘는데, 이번 가입으로 한국은 기여국의 지위를 갖게 되었다. 현재 후원국은 NATO 30개 회원국으로 구성되어 있으며, 기여국은 오스트리아·핀란드·스웨덴·스위스·일본(2022. 11.)·오스트레일리아 등 총 9개국이다.

CCDCOE는 사이버안보 관련 기술·전략·작전·법 영역에서 연구·교육·훈련을 수행한다. 주요 연구성과로는 현존하는 국제법이 사이버공간 이용에 어떻게 적용되는지에 관한 규칙을 담은 탈린매뉴얼이 있으며, 이는 CCDCOE 주도로 진행되어 2013년 최초 발간되었다. 2017년 탈린매뉴얼 개정본이 발간되었으며, 현재 세 번째 탈린매뉴얼 작업이 진행 중이다. 이 밖에도 CCDCOE는 2010년부터 매년 사이버안보 분야 최대 글로벌 콘퍼런스인 '사이버충돌에 관한 국제 콘퍼런스'(International Conference on Cyber Conflict, CyCon)를 개최하고 있다.

한편 CCDCOE는 전략·작전·법·기술 등 사이버공간 내 활동과 관련한 다양한 교육 과정도 함께 진행하고 있다. 훈련의 경우 사이버방어 훈련인 락드실즈(Locked Shields)와 사이버공격 훈련인 크로스드 스워즈(Crossed Swords)를 정기적으로 실시하고 있다. 우리나라는 2021년 라트비아와 연합하여 공동으로 락드실즈에 참여하였으며, 2022년 우리나라 단독으로 국가정보원·국가보안기술연구소·국방부·한국전력공사 등 민·관·군으로 구성된 70여 명이 훈련에 참여하였다. 락드실즈를 통하여 사이버공격 발생 시 국가 간 협력, 국제법에 기반한 대응, 복구 우선순위 등 다양한 의사결정 훈련을 발전시키고 있다.

우리나라는 2019년부터 사이버침해 사고 대응, 주요 기반시설 보호 등과 관련한 사이버안보 주요 전략과 교훈을 습득하고, 유사입장국들과 국제협력을 증진하기 위하여 CCDCOE 가입을 추진하였다. 2021년부터는 락드실즈 참여 등을 통하여 한국의 사이버안보 역량과 국제협력 의지를 보여 줌으로써 CCDCOE 회원 자격을 인정받게 되었다. CCDCOE 가입으로 우리나라의 사이버안보 분야 국제협력 역량이 한층 강화될 것으로 기대된다.

08 국가정보원, 세계 최초 양자암호통신 안전성 검증체계 수립



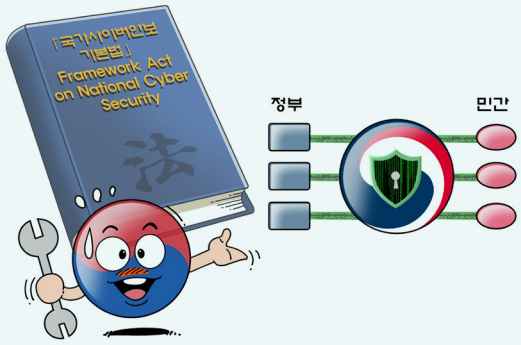
양자암호통신은 수학적 복잡성에 기반하는 공개키 등 기존 암호체계와는 달리 비밀키를 생성하기 위하여 정보를 주고받는 과정을 양자 상태에서 진행하기 때문에 제3자는 비밀키에 대한 정보를 전혀 알 수 없다. 암호키(비밀키)가 전송되는 중간에 해킹당할 경우 발신자와 송신자는 양자 속성상 이 사실을 즉각 알 수 있다.

최근 국가정보원은 세계 최초로 양자암호통신 장비의 보안인증 기준인 '양자암호통신 국가용 보안요구사항'을 확정하여 발표하였다. 양자암호통신 부문에 대한 국가정보원의 안전성 검증 노하우와 산·학·연 전문가와 오랜 논의를 더한 끝에 도출된 검증체계이다. 우리나라 공공기관은 「전자정부법」 제56조와 「국가정보원법」 제4조에 따라 보안적합성 검증을 받은 제품만 사용할 수 있는데, 이에 양자암호통신 국가용 보안요구사항이 반영·활용될 것으로 보인다.

국가정보원에 따르면, 보안요구사항에는 양자키분배장비, 양자키관리장비, 양자통신암호화장비가 반드시 지켜야 하는 필수 요구사항 116개가 포함된다. 예를 들어, 양자키분배장비가 비밀키를 안전하게 저장하는지, 더 이상 사용하지 않는 비밀키를 안전하게 파기하는지 등을 점검하게 된다. 구체적인 보안요구사항 가이드라인이 공개될 예정이며, 검증 실무는 한국전자통신연구원(ETRI)과 한국정보통신기술협회(TTA)가 담당한다.

검증이 마련됨에 따라 정부와 공공기관도 최신 보안제품을 들여올 수 있게 된다. 최신 기술을 보유한 국내 보안기업들의 공공시장 진출 문턱이 낮아지고 국외 진출에도 도움이 될 전망이다. 우리나라의 정보통신기술(ICT) 수준과 군사적 특수성을 감안하면 보안적합성 검증이 갖는 신뢰도가 다른 나라에 비하여 높기 때문이다. 실제로 SK텔레콤 등 통신사들은 양자암호통신 시스템을 수출하기 위하여 각국 정부와 통신사와 협의 중이며, 가시적 성과가 나올 것으로 기대된다.

09 범정부 차원의 체계적 대응을 위한 사이버안보법 제정 추진



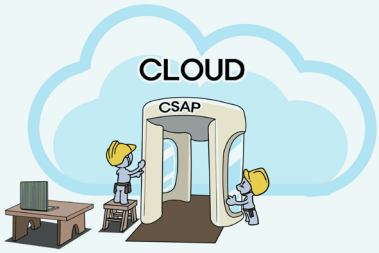
우리나라는 인터넷 속도나 전자정부 수준 등이 OECD 국가 중에서도 손꼽히는 ICT 인프라 강국으로, 최첨단 기술 보유하면서 세계 어느 선진국보다도 뛰어난 ICT 환경을 갖추고 있다. 반면에, 이를 악용하고 절취하려는 국제·국가배후 해킹조직의 위협이 지속적으로 늘어나고 있는 상황이다. 국제·국가배후 해킹조직은 국가안보와 국민의 안전을 위협하고 있고, 금전탈취 목적의 해킹시도가 급증하는 등 국가 전 영역에 대한 동시다발적인 공격을 자행하고 있다. 최근 우리나라는 우주항공·에너지·의료 분야 등 다양한 공공기관이 국가배후의 사이버공격을 받았고, 기업의 첨단기술, 개인의 개인정보까지도 탈취당하는 등 위협 범위가 확장되고 있다.

그럼에도 불구하고 우리나라는 사이버안보 위협 대응을 위한 국가 차원의 통일된 체계를 구축하지 못한 상황으로, 현재 각 정부 부처가 개별 법령에 따라 별도로 소관 분야를 보호하고 있는 실정이다. 국가·공공기관의 경우 사이버보안 조직 구성·예산 확보·절차 등 예방·대응 업무를 비교적 체계적으로 수행하고 있으나, 민간의 경우 소관 부처에서 별개의 정책에 따라 각자 대응 중으로 사이버안보를 위한 개별 법령이 갖추어지지 못한 경우도 있으며, 법령이 있다고 하더라도 민간을 강제할 수 없는 경우가 많아 결국 기업의 자체 노력에 의존하고 있다. 이에 현행 법체계로는 국가 사이버안보 위기가 발생할 경우 각 부처가 역할에 혼선을 빚거나 업무가 중복되어 신속하고 통합적인 대응에 문제가 발생할 우려가 다분하다.

정부는 이에 대한 해결책으로 2022년 11월 국가역량을 결집한 사이버안보 대응 체계 및 활동과 기관의 역할을 규정한 「국가사이버안보 기본법(안)」을 입법예고하였다. 법안의 주요 내용에는 ▲대통령 소속의 국가사이버안보위원회 설치 ▲중앙행정기관 등의 각 소관 분야에 대한 예방·대응 활동 수행 책임 ▲공급망보안 위협 예방 및 공세적 대응조치 방안 마련 ▲사이버안보 위협 정보 공유 ▲국회의 사이버안보 업무 조사·감독권 등이 포함되어 있다.

「사이버안보법」 제정으로 사이버안보 업무의 단일창구가 마련되어 국가안보를 위협하는 국제·국가배후 해킹조직에 대한 범국가적 대응이 가능할 것으로 전망되고, 사이버안보 위협에 대한 억지력 강화에도 이바지할 것으로 예상된다. 이러한 사유로 미국 등 주요 사이버 강국은 이미 몇 년에 걸쳐 국가 차원의 사이버안보 역량을 강화하기 위한 입법을 진행하고 있다. 우리나라도 국가 사이버안보 기반 마련과 발전의 초석이라고 할 수 있는 「국가사이버안보법(안)」 제정을 신속하게 추진하여야 할 것이다.

10 공공분야의 안전한 민간 클라우드 도입을 위한 클라우드 보안인증제 개선 추진



클라우드 컴퓨팅 환경은 서비스 제공자가 이미 마련한 시스템을 네트워크 통하여 임대·활용하는 개념이다. 이에 사용자는 시스템 구축에 필요한 물리적 서버, 운영을 위한 공간과 전력 등 초기 투자비용과 유지보수 비용을 대폭 절감할 수 있다. 또한 활용 목적·환경에 따라 맞춤형 서비스를 제공받을 수 있어, 현재 클라우드 서비스는 새로운 시스템 운영방식으로 각광받고 있다. 글로벌 기업은 물론, 미국 등 주요국은 공공기관에도 클라우드 도입을 추진 중이며, 우리나라도 공공기관의 민간 클라우드 이용과 확산을 위하여 2016년부터 '클라우드 보안인증제(Cloud Service Assurance Program, CSAP)'를 시행하고 있다. 클라우드의 안전성 보장과 공공시장 도입 촉진이 목표인 CASP는 시행 이후에 '전환 대상 시스템의 중요도에 따른 보안기준 차등화 필요성'과 '민간 클라우드 환경에서 공공시스템에 대한 국가정보원 및 이용기관의 보안관제, 사고조사 및 사이버공격 위협에 대한 예방 대응활동 등의 적용방안 부재' 등에 대한 논의가 지속되었다.

정부는 공공기관 민간 클라우드 서비스 공급을 더욱 활성화하기 위하여 2022년부터 CSAP 제도 개선에 착수하였다. 시스템의 운영 목적과 취급 시스템 중요도에 따라 상·중·하 3단계로 구분된 보안인증을 추진하는 것이 골자이다. 클라우드 사업자에 대한 보안인증 평가 기준은 등급별로 차등화하여, 기존 평가항목 기준으로 상등급 평가 기준은 보완·강화하고, 중등급 평가 기준은 현행 수준을 유지하는 한편, 하등급 평가 기준은 합리적으로 완화한다. 하등급은 개인정보를 포함하지 않고 공개된 공공 데이터를 운영하는 시스템, 중등급은 비공개 업무 자료를 포함 또는 운영하는 시스템, 상등급은 민감정보를 포함하거나 행정 내부 업무 운영 시스템으로 분류할 계획이다. 특히 하등급 시스템의 경우 클라우드 시스템의 민간·공공 영역 간 논리적 분리도 허용하되 클라우드 시스템 및 데이터, 관리 주체의 물리적 위치를 국내로 한정한다. 이는 국가안보를 저해하지 않고 공공 클라우드 산업 생태계 전반의 발전을 꾀하려는 정부의 방침으로 해석된다. 상·중등급 시스템의 경우 안전성 확인을 위하여 실증·검증을 거쳐 평가 기준을 보완할 예정이다. 기존 인증제도 대비 중요 시스템은 더 높은 신뢰성을 확보하고, 상대적 중요도가 낮은 시스템은 개방성을 높여 제도 전반의 효율성이 제고될 것으로 보인다.

2022년 5월 출범한 새정부의 디지털플랫폼정부 구현 등 이미 많은 국정 과제가 클라우드 환경 고유의 특성을 요구하고 있다. 미국은 과거 클라우드 도입 확대에 초점을 둔 '클라우드 퍼스트' 정책에서 최근 보안과 국가안보 등의 상황을 종합적으로 고려한 '스마트 클라우드' 정책을 도입하고 있다. 우리나라 역시 국가안보 상황·정책 등을 종합적으로 고려하여 안전성과 보안성이 담보된 높은 품질의 클라우드 컴퓨팅 서비스를 도입할 필요가 있다. 정부의 이번 CASP 개선이 전자정부 강국으로 다시 한번 도약하는 계기가 되기를 기대한다.

CONTENTS

2023 국가정보보호백서의 구성과 특징
정보보호 연혁
2022년 정보보호 10대 이슈

제1편 정보보호 환경 변화 및 사이버위협 동향

제1장 정보보호 환경 변화 ····· 2
제2장 사이버위협 주요 이슈와 전망 ····· 4

제2편 정보보호 법·제도 및 기관

제1장 정보보호 법·제도
제1절 정보보호 법·제도 발전과정 ····· 10
제2절 정보보호 법·제도 현황 ····· 13
제3절 2022년 정보보호 관련 주요 개정 법령 ····· 21

제2장 정보보호 기관 및 단체
제1절 국가기관 ····· 23
제2절 전문기관 ····· 39

제3편 분야별 정보보호 활동

제1장 국가정보통신망 보호
제1절 사이버공격 탐지·차단 ····· 46
제2절 사고조사 ····· 49
제3절 보안관리컨설팅 및 관리실태 평가 ····· 53
제4절 보안적합성 검증 ····· 56
제5절 암호모듈 검증 ····· 64
제6절 정보보호제품 평가·인증 ····· 71

제2장 디지털정부
제1절 디지털정부 정보보호 ····· 81
제2절 소프트웨어 개발보안 ····· 86
제3절 전자서명 인증 ····· 90

제3장 주요정보통신기반시설
제1절 추진 체계 ····· 97
제2절 주요 활동 ····· 101
제3절 국내외 침해사고 사례 ····· 109

제4장 정보통신서비스
제1절 침해사고 대응 ····· 112
제2절 침해사고 예방 ····· 117
제3절 정보보호 및 개인정보보호 관리 체계 인증 ····· 120
제4절 클라우드 보안인증제도 ····· 126
제5절 융합보안 ····· 131

제5장 금융서비스
제1절 금융서비스 정보보호 ····· 135
제2절 금융분야 사이버공격 대응 및 정보공유 ····· 141
제3절 금융IT 및 전자금융·핀테크의 보안평가·점검 ····· 148

제4편
정보보호 기반조성

제1장 정보보호산업 육성
제1절 개요 ····· 154
제2절 정보보호 업체 및 시장 현황 ····· 156
제3절 정보보호산업 관련 제도 ····· 159

제2장 정보보호 기술 개발
제1절 개요 ····· 172
제2절 원천기술 개발 ····· 175
제3절 상용기술 개발 ····· 185

제3장 정보보호 인력 양성
제1절 개요 ····· 189
제2절 정규교육 과정 ····· 190
제3절 전문기관 교육 과정 ····· 196
제4절 각종 대회를 통한 인력 양성 ····· 211
제5절 정보보호 자격증 제도 ····· 217

제4장 개인정보보호
제1절 「개인정보 보호법」 개정 추진 및 행정 체계 ····· 223
제2절 법·제도적 기반 강화 ····· 227

제5장 대국민 정보보호
제1절 정보보호 상담 및 처리 ····· 234
제2절 인식제고 ····· 236

제6장 국제협력
제1절 주요 사이버안보 외교 활동 ····· 241
제2절 사이버보안 국제협력 ····· 245

부록

제1장 통계로 보는 정보보호
가. 국가·공공부문 ····· 250
나. 민간부문 ····· 278

제2장 2022년 주요 정보보호 행사 ····· 288
제3장 국내 정보보호 관련 주요 사이트 ····· 289
제4장 정보보호 민간단체 ····· 290
제5장 국내 ISAC 현황 ····· 291

표 차례

[표 3-1-1-1] 부문보안관제센터 운영 현황(44곳) ····· 47
[표 3-1-3-1] 보안컨설팅 절차와 주요 내용 ····· 54
[표 3-1-4-1] 안전성 검증 없이 자율 도입·운영이 가능한 제품 ····· 57
[표 3-1-4-2] 그룹별 편성 기준 및 대상기관 ····· 58
[표 3-1-4-3] '가'그룹 편성기관의 주요 IT보안제품 사전인증요건 ····· 60
[표 3-1-4-4] '나'그룹 편성기관의 주요 IT보안제품 사전인증요건 ····· 62
[표 3-1-5-1] 암호모듈 검증 절차 세부사항 ····· 68
[표 3-1-5-2] 검증대상 암호알고리즘 ····· 70
[표 3-1-5-3] 검증필 암호모듈 현황 ····· 71
[표 3-1-6-1] 정보보호제품 평가보증등급 ····· 74
[표 3-1-6-2] IT보안인증사무국이 인정한 CC 평가기관 ····· 75
[표 3-1-6-3] 평가보증등급별 인증제품 현황 ····· 77
[표 3-1-6-4] CCRA 회원국 현황 ····· 79
[표 3-2-1-1] 국제정보화 지수별 우리나라 순위 ····· 83
[표 3-2-1-2] 행정안전부 소관 주요정보통신기반시설 지정 현황(2022년 기준) ····· 85
[표 3-2-2-1] 소프트웨어 개발보안 제도 개요 ····· 87
[표 3-2-2-2] 소프트웨어 보안약점 진단 현황 ····· 88
[표 3-2-2-3] 모바일 디지털정부 서비스 앱 보안성 검증 현황 ····· 88
[표 3-2-2-4] 소프트웨어 개발보안 안내서 현황 ····· 89
[표 3-2-2-5] 소프트웨어 개발보안 교육 및 진단원 자격취득 현황 ····· 89
[표 3-2-3-1] 행정전자서명 인증기관 ····· 91
[표 3-2-3-2] 행정전자서명 기관별 주요 역할 ····· 92
[표 3-2-3-3] 평가기관 선정 현황(2022. 12. 기준) ····· 94
[표 3-2-3-4] 증명서 발급 현황(2022. 12. 기준) ····· 95
[표 3-3-1-1] 수행 주체별 주요 기능 ····· 101
[표 3-3-2-1] 주요정보통신기반시설 지정 기준 ····· 102
[표 3-3-2-2] 연도별 주요정보통신기반시설 지정 현황 ····· 104
[표 3-3-3-1] 국내외 정보통신기반시설 침해사고 사례 ····· 109
[표 3-4-1-1] 악성코드 은닉사이트 점검 대상 ····· 113
[표 3-4-1-2] 연도별 악성코드 은닉사이트 탐지·대응 건수 ····· 113

[표 3-4-1-3] 사이버대피소 서비스 현황 114
[표 3-4-1-4] 감염PC 사이버 치료 체계 운영 현황 115
[표 3-4-1-5] 모바일 응급 사이버 치료 체계 운영 현황 117
[표 3-4-3-1] ISMS-P 인증제도 122
[표 3-4-3-2] ISMS-P 인증서 유지 현황 122
[표 3-4-3-3] ISMS 의무 대상자 기준 124
[표 3-4-3-4] ISMS-P 인증심사 기준 126
[표 3-4-4-1] 클라우드 서비스 보안인증 기준 129
[표 3-5-3-1] 보안 취약점 평가 분야별 주요 평가 내용 149

[표 4-1-2-1] 정보보호기업 종사자 규모별 현황(2021. 12. 기준) 156
[표 4-1-2-2] 정보보호산업 매출 현황 157
[표 4-1-2-3] 정보보호산업 매출 추이 158
[표 4-1-2-4] 정보보호산업 수출 현황 158
[표 4-1-2-5] 정보보호산업 수출 추이 159
[표 4-1-3-1] 정보보호 전문서비스 기업 지정 심사 기준 160
[표 4-1-3-2] 정보보호 전문서비스 기업 현황 161
[표 4-1-3-3] 보안관제 전문기업 지정 심사 기준 163
[표 4-1-3-4] 보안관제 업무수행 능력 평가 기준 163
[표 4-1-3-5] 보안관제 전문기업 지정 현황 164
[표 4-2-1-1] 정보보호핵심원천기술개발 사업 추진 세부 과제 174
[표 4-2-2-1] 정보보호 분야 2022년 국가표준 제·개정 현황 183
[표 4-2-3-1] 정보보안 기업 자체기술연구소 및 전담부서 운영 현황 186
[표 4-2-3-2] 정보보안 기업 연도별 기술 개발 투자액 현황 186
[표 4-2-3-3] 정보보안 대분류별 매출 현황 187
[표 4-2-3-4] 정보보안 제품 및 서비스 매출 현황 187
[표 4-2-3-5] 정보보안 대분류별 수출 현황 188
[표 4-2-3-6] 정보보안 제품 및 서비스 수출 현황 188
[표 4-3-1-1] 정보보호산업 인력 현황 189
[표 4-3-1-2] 정보보호산업 매출 규모별 인력 현황(2021. 12. 기준) 190

[표 4-3-1-3] 정보보호산업 채용 규모(2021년 기준) 190
[표 4-3-2-1] 2022년 전문대학 정보보호 관련 학과 현황 191
[표 4-3-2-2] 2022년 대학 정보보호 관련 학과 현황 192
[표 4-3-2-3] 2022년 대학원 정보보호 관련 학과 현황 194
[표 4-3-3-1] 2022년 사이버안전훈련센터 연간 교육 과정 196
[표 4-3-3-2] 2022년 국가공무원 인재개발원 정보보안 교육 과정 197
[표 4-3-3-3] 2022년 민간 교육센터 교육 현황 198
[표 4-3-3-4] 2022년 융합보안 대학원 현황 201
[표 4-3-3-5] 2022년 산업보안 전문인력 양성 과정 운영 현황 203
[표 4-3-3-6] 2022년 대학 정보보호 동아리 현황 204
[표 4-3-3-7] 2022년 융합보안 인력 양성 과정 교육 내용 205
[표 4-3-3-8] 2021년 중앙부처 국가기간·전략산업 직종훈련 과정 207
[표 4-3-3-9] 2022년 사이버교육 과정 207
[표 4-3-3-10] 2022년 주요 집합교육 209
[표 4-3-3-11] 금융보안관리사 배출 현황 210
[표 4-3-4-1] 2022년 수상작 관련 내용 216
[표 4-3-5-1] 정보보호 전문 자격증 현황 217
[표 4-3-5-2] 정보보안 국가기술자격시험 응시자 및 합격자 현황 218
[표 4-3-5-3] 산업보안관리사 자격시험 응시자 및 합격자 현황 219
[표 4-3-5-4] CISSP 자격보유자 현황 220
[표 4-4-1-1] 「개인정보 보호법」 개정안 주요 내용 224
[표 4-5-1-1] 연도별 118상담센터 민원 접수처리 현황 235
[표 4-5-1-2] 118상담센터 분야별 상담 현황 235

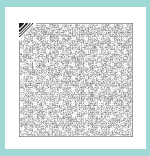


그림 차례

[그림 3-1-2-1] 위협정보 분석·판단 과정 51
[그림 3-1-2-2] 국가사이버위협 정보공유시스템 구축 배경 및 운영근거 53
[그림 3-1-3-2] 정보보안 관리실태 평가 절차 55
[그림 3-1-5-1] 암호모듈 시험·검증 체계 66
[그림 3-1-5-2] 암호모듈 시험·검증 절차 67
[그림 3-1-5-3] 검증효력 만료 도래 시 및 형상 변경 시 조치사항 69
[그림 3-1-5-4] 검증대상 암호알고리즘 70
[그림 3-1-6-1] 정보보호제품 평가·인증 체계 75
[그림 3-1-6-2] 정보보호제품 평가·인증 절차 76
[그림 3-2-1-1] 정부민원포털 '정부24' 서비스 활용 현황 82
[그림 3-2-2-1] 소프트웨어 개발보안 개념 86
[그림 3-2-3-1] 행정전자서명 인증 체계 91
[그림 3-2-3-2] 연도별 행정전자서명 인증서비스 이용 현황 92
[그림 3-2-3-3] 전자서명인증사업자 인정·평가 체계 94
[그림 3-2-3-4] 간편인증을 적용한 대법원 가족관계등록시스템 로그인 화면 96
[그림 3-3-1-1] 주요정보통신기반시설 보호 추진 체계 100
[그림 3-3-2-1] 주요정보통신기반시설 지정 절차 103
[그림 3-3-2-2] 주요정보통신기반시설 지정 권고 절차 104
[그림 3-3-2-3] 주요정보통신기반시설 보호 업무 절차 106
[그림 3-3-2-4] 주요정보통신기반시설 보호대책 이행 여부 확인 절차 107
[그림 3-3-2-5] 주요정보통신기반보호 워크숍 108
[그림 3-3-2-6] 기반보호포럼 108
[그림 3-4-3-1] ISMS-P 인증 개요 121
[그림 3-4-3-2] ISMS-P 인증 추진 체계 123
[그림 3-4-3-3] ISMS-P 인증 절차 125
[그림 3-4-4-1] 클라우드 서비스 보안평가·인증 체계 127
[그림 3-4-4-2] 클라우드 서비스 보안인증 평가 절차 131
[그림 3-4-5-1] 융합서비스 보안모델 132
[그림 3-4-5-2] 5대 융합서비스 보안리빙랩 134
[그림 3-5-1-1] 금융보안 체계 138

[그림 3-5-2-1] 금융부문 보안관제 체계 141
[그림 3-5-2-2] 사이버위협 정보공유 체계 142
[그림 3-5-2-3] 금융보안관제시스템 143
[그림 3-5-2-4] 피싱·파밍 사이트 모니터링 절차 144
[그림 3-5-2-5] 범금융권 보이스피싱 사기 정보공유시스템 145
[그림 3-5-2-6] 이상금융거래 정보공유 체계 146
[그림 3-5-2-7] 디도스 비상대응센터 대응 체계 148

[그림 4-1-3-1] 구매수요정보 제공 절차 165
[그림 4-1-3-2] 2022년 확정 정보보호 구매수요정보 주요 결과 166
[그림 4-1-3-3] 2023년 예정 정보보호 구매수요정보 주요 결과 167
[그림 4-1-3-4] 정보보호 공시제도 개요 169
[그림 4-1-3-5] 정보보호 공시 종합포털 171
[그림 4-2-1-1] 12대 국가전략기술 173
[그림 4-2-2-1] IoT/IIoT 디바이스 안전성 보장을 위한 취약점 보안검증 기술 개념 176
[그림 4-2-2-2] 소프트웨어 공급망 보안을 위한 SBOM 자동생성 및 무결성 검증기술 개념 177
[그림 4-2-2-3] 사이버공격 그룹 식별 및 유형 분석 기술 개념 178
[그림 4-2-2-4] 랜섬웨어 공격 근원지 식별 및 분석 기술 개념 179
[그림 4-2-2-5] 인공지능 기술 활용 디지털 증거 분석 기술 개념 180
[그림 4-2-2-6] SASE 기반 지능형 통합 보안 에지 기술 개념 181
[그림 4-2-2-7] 자가진화형 인공지능 기반 사이버 공방 핵심원천기술 개념 182
[그림 4-3-3-1] 정보보호 특성화대학 지원사업 체계도 200
[그림 4-3-3-2] 2022년 최정예 정보보호 전문인력 양성 정규 과정 운영 현황 202
[그림 4-3-4-1] 우리나라 합동방어팀 훈련 현장(밀리토피아 호텔) 212
[그림 4-3-4-2] 2022 사이버공격방어대회 포스터 213
[그림 4-4-1-1] 개인정보보호 행정 체계 226
[그림 4-4-1-2] 개인정보 침해 신고 및 민원처리 절차 227
[그림 4-5-2-1] 제11회 '정보보호의 날' 기념식 236
[그림 4-5-2-2] 인식 제고 홍보 활동 238
[그림 4-5-2-3] 금융정보보호 콘퍼런스(FISCON 2022) 239

[그림 4-5-2-4] 금융권 버그바운티 240
[그림 4-6-1-1] 제7회 사이버공간 국제 평화 안보체제 구축에 관한 학술회의 242
[그림 4-6-1-2] 제2차 세계신안보포럼 244
[그림 4-6-2-1] CAMP 제7차 연례총회와 지역포럼 246

[그림 부록 1-가-1] 정보보호 전담부서 운영 현황 251
[그림 부록 1-가-2] 정보보호 전담부서 인원 수 현황 251
[그림 부록 1-가-3] 정보화 담당조직 인원 수 대비 정보보호 전담조직 인원 수 252
[그림 부록 1-가-4] 정보보호 전담부서 실제 구성인원과 희망 구성인원 비교 252
[그림 부록 1-가-5] 정보보호 전담부서 최상급자 직급 253
[그림 부록 1-가-6] 조사 대상 범주별 정보보호 최상급자 직급 253
[그림 부록 1-가-7] 정보보호 전담인력의 해당 분야 평균 업무 경력 254
[그림 부록 1-가-8] 정보보호 전담부서의 필요성 255
[그림 부록 1-가-9] 전담조직을 신설하지 않은 이유 255
[그림 부록 1-가-10] 기관장의 정보보호 계획 결정 참여 여부 256
[그림 부록 1-가-11] 직원의 정보보호 정책·규정 준수 및 위반 책임 부담 필요성 256
[그림 부록 1-가-12] 정보보호 관련 학위 및 공인 자격증 소지자 현황 257
[그림 부록 1-가-13] 정보보안 담당자 전문교육 실시 현황 258
[그림 부록 1-가-14] 일반 임직원에 대한 정보보안 직무교육 실시 현황 258
[그림 부록 1-가-15] 교육 운영 형태 259
[그림 부록 1-가-16] 교육 일수 현황 259
[그림 부록 1-가-17] 기관별 정보보호 예산 용도 260
[그림 부록 1-가-18] 정보화 예산 대비 정보보호 예산 비율 변화 261
[그림 부록 1-가-19] 정보화 예산 대비 정보보호 예산 희망 비율 262
[그림 부록 1-가-20] 주요정보시스템 운영·관리 방법 263
[그림 부록 1-가-21] 외부인력 출입관리 방법 263
[그림 부록 1-가-22] 정보시스템 운영·관리 상주 외부인력 수 264
[그림 부록 1-가-23] 상주 외부인력 근무 장소 265
[그림 부록 1-가-24] 상주 외부인력 보안관리 방법 265
[그림 부록 1-가-25] 휴대용 정보통신기기 관리 방법 266

[그림 부록 1-가-26] 연간 사이버공격 피해 발생 횟수 267
[그림 부록 1-가-27] 사고 발생 시 가장 긴급한 활동 267
[그림 부록 1-가-28] 사이버분야 위기대응매뉴얼 제작·보유 현황 268
[그림 부록 1-가-29] 일반 직원의 피해 발생 인지 수준 269
[그림 부록 1-가-30] 보안 사고 발생의 핵심 원인 269
[그림 부록 1-가-31] 정보보호 업무 만족 여부 270
[그림 부록 1-가-32] 정보보호 업무 불만족 사유 271
[그림 부록 1-가-33] 정보보안 담당자의 상대적 부담감 271
[그림 부록 1-가-34] 정보보호 담당자의 업무 부담감 발생 사유 272
[그림 부록 1-가-35] 정보보호 업무수행 애로 사항 273
[그림 부록 1-가-36] 소속기관 정보보호 수준 자체평가 273
[그림 부록 1-가-37] 소속기관이 가장 취약한 정보보호 분야 274
[그림 부록 1-가-38] 기관별 가장 우려되는 정보보호 위협요인 275
[그림 부록 1-가-39] 기관 정보보호 수준 향상을 위한 최우선 요소 275
[그림 부록 1-가-40] 기관별 보완이 필요한 정보보호 인력 전문분야 276
[그림 부록 1-가-41] 국가 전체의 정보보호 우선순위 277
[그림 부록 1-나-1] 정보보호 정책 수립 278
[그림 부록 1-나-2] 개인정보보호 정책 수립 279
[그림 부록 1-나-3] 정보보호 조직 운영 279
[그림 부록 1-나-4] 정보보호 교육 실시 280
[그림 부록 1-나-5] 정보보호 예산 활용 분야 281
[그림 부록 1-나-6-1] 정보보호제품 이용 282
[그림 부록 1-나-6-2] 물리보안제품 이용 282
[그림 부록 1-나-7] 국내외 정보보호제품 및 서비스 선호도 283
[그림 부록 1-나-8] 시스템 및 네트워크 보안점검 실시 283
[그림 부록 1-나-9] 정보보호 위협요인 284
[그림 부록 1-나-10-1] 시스템 로그 백업 285
[그림 부록 1-나-10-2] 데이터 백업 방식 285
[그림 부록 1-나-11] 침해사고 직접 경험 286
[그림 부록 1-나-12] 침해사고 경험 유형(복수 응답)-침해사고 경험 기업체 286

[그림 부록 1-나-13-1] 정보보호 및 개인정보보호 중요성 인식 ····· 287
[그림 부록 1-나-13-2] 정보보호 애로 사항(복수 응답) ····· 287

1

제1편

정보보호 환경 변화 및 사이버위협 동향

제1장 정보보호 환경 변화
제2장 사이버위협 주요 이슈와 전망

제1장

정보보호 환경 변화

코로나19 장기화로 인한 산업 전반의 디지털화, 비대면 경제의 확대, 가상경제 발전 등 전통적인 산업구조는 변화하고 있으며, 경제 전반에 걸쳐 사이버보안 이슈가 부각되고 있다.

우크라이나-러시아 전쟁이 장기화함에 따라 2023년에도 글로벌 해킹 조직의 활동이 꾸준히 증가하고 있으며, 주요 기반시설 또는 글로벌 기업 대상의 대규모 사이버공격 시도가 지속될 것으로 예상된다.

랜섬웨어 공격이 일반화되면서 암호화한 중요 정보의 복호화 대가로 요구하는 몸값, DDoS(분산서비스거부, Distributed Denial of Service) 공격과 함께 기업 고객에 대하여 직접적으로 협박하는 등 다중협박(Multi Extortion) 형태로 진화하고 있다.

또한 해킹 조직의 직접적인 수익 창출을 위하여 가상거래소, 전자지갑, DeFi(탈중앙화 금융, Decentralized Finance) 등을 겨냥한 가상자산 타깃형 공격이 더욱 활발해질 것으로 예상된다.

코로나19, 우크라이나-러시아 전쟁, 경기도 판교 데이터센터 화재 등 재난과 장애로 인한 민감한 사회적 이슈를 악용한 공격 형태가 나타나고 있다. 피싱·스미싱, 해킹메일 유포, APT(지능형 지속 공격, Advanced Persistent Threat)뿐 아니라 첨단기술 기반의 가짜 뉴스를 통한 국가 신뢰도 저해 등 사회공학적 기법을 통하여 악성코드가 지속적으로 유포될 것이며,

이메일뿐 아니라 소셜미디어 등 개인화된 채널을 활용한 공격 또한 증가할 것으로 보인다.

사이버 범죄 조직이 소셜미디어를 통하여 공격행위를 공개하는 등 대담한 활동이 증가할 것으로 예측되면서 해킹 조직 '랩서스'와 같이 비국가적·비조직적 공격자에 의한 침해사고 우려도 주목하여야 할 부분이다.

최근 비대면 원격근무의 확산, 클라우드 전환 등으로 인하여 기업의 업무망이 복잡해지고, 네트워크 경계가 모호해지면서 내부 직원의 계정과 권한을 탈취한 해커를 정상적 이용자로 신뢰하면서 내부망 자료가 유출되는 피해가 증가하고 있다.

이러한 문제를 해결하기 위하여 모든 접속자에 대한 잠재적 위협을 미리 식별하고, 새로운 접근에 대해서는 지속적인 확인 절차를 거쳐 적절한 권한을 부여하는 '제로 트러스트(Zero Trust)' 철학이 주목받고 있다. 기존의 경계 기반 보안에서 제로 트러스트로 전환, 오픈소스 등 소프트웨어 안전성을 확보할 수 있는 공급망 보안 체계의 도입이 시급한 상황이다.

미국 바이든 정부도 국가 사이버보안 개선에 대한 행정 명령(EO14028, 2021. 5.)을 발표하면서 제로 트러스트 구조를 연방정부에서 구현하도록 요구하고, 연방 기관에 소프트웨어 내장 제품을 납품할 경우 SBOM(소프트웨어 구성요소를 식별하기 위한 명세서, Software Bill of Materials) 제출을 의무화하는 등 공급망 보안 강화에 집중하고 있다.

과학기술정보통신부와 한국인터넷진흥원도 제로 트러스트 보안모델과 가이드 마련 필요성을 제시한 바 있으며, 이를 구체화하고 능동적으로 대응하기 위하여 2022년 10월 '제로 트러스트·공급망 보안 포럼'을 발족하였다.

고도화된 방어 체계에도 불구하고, 예측 불가능한 침해사고가 발생할 수 있으며, 방어에만 치중하기보다는 그 피해가 확대되지 않도록 조기에 대응하고 회복하는 대응 체계를 갖추는 것이 중요하다. 사이버 침해를 당하더라도 업무가 중단되지 않도록 백업 체계를 마련하고, 신속한 복구가 이행되도록 복구 훈련을 주기적으로 실시하는 등 사이버 복원력(Cyber Resilience) 대응 체계를 도입할 필요가 있다.

제2장

사이버위협 주요 이슈와 전망

가. 기업정보 탈취 목적의 스피어피싱 공격 위협

이메일은 전세계적으로 가장 보편적으로 사용되는 소통 수단이지만, 다른 수단과는 달리 송신자에 대한 위조가 쉬운 약점이 있다. 공격자는 이러한 약점을 악용하여 이메일을 원하는 공격 대상에게 보내고 필요한 정보를 요청하거나 악성 코드를 전송하여 기업 내 내부 단말을 감염시킨다.

최근 공격자는 기업 내부에 침투하기 위하여 악성 메일의 본문과 첨부파일을 업무와 관련된 내용으로 작성하여 발송하는 등 더욱 정교하게 제작된 스피어피싱(Spear-Phishing) 메일을 활용하고 있다. 공격자는 이메일을 보내기 전에 공격 대상을 연구하여 사전 정보를 수집하고, 이메일 내용에 반영하여 직원들이 이메일을 더 쉽게 믿고 열람하도록 유도할 수 있으며, 공격에 성공한 후 기업정보를 탈취하여 이를 볼모로 금전을 요구한다.

스피어피싱 메일을 통한 사이버위협은 지금 이 순간에도 지속적으로 발생하고 있으며, 앞으로도 다양한 내용과 더욱 정교한 방법으로 진화할 것으로 예상된다. 따라서 기업은 이러한 공격에 대비하여 보안 체계를 강화하고, 직원들에게 보안 교육을 실시함으로써 보안 위협에 대처할 수 있는 능력을 갖추어야 한다.

나. 클라우드 서비스 전환에 따른 보안 위협

많은 기업과 기관은 비용을 절감하고 유연성과 확장성을 향상하기 위하여 클라우드 서비스로의 전환이 가속화되고 있다. 그러나 클라우드 서비스의 보안은 여전히 많은 기업이 걱정하는 문제이다.

클라우드 서비스에서 제공되는 기본적 보안기능을 사용하면 기업 보안에 대한 일부 요구사항을 충족시킬 수 있지만, 해당 기능만으로는 기업 보안 정책과 서로 다를 수 있으며, 충분한 보안 요건을 충족시키기 어려울 수 있다.

그래서 기업 보안담당자는 클라우드 서비스 제공업체와 함께 보안 정책을 구체적으로 수립하고, 기업 환경에 맞추어 보안 시스템을 구축하여야 한다. 특히 IT(정보기술, Information Technology)와 융합되는 OT(운영기술, Operation Technology)에 대한 위협은 클라우드 서비스의 보안 위협 중 하나이며, 기업의 생산 시설 또는 생산 라인과 같은 시스템을 의미한다. 이러한 시스템은 클라우드 서비스를 이용하여 제어 및 모니터링을 수행할 수 있다. 그러나 OT 시스템은 IT와는 달리 물리적 제어 시스템을 포함하기 때문에 보안 위협에 대한 대응도 달라진다. 따라서 IT와 융합되는 OT 시스템을 클라우드 서비스를 통하여 이용하는 기업은 이러한 위협에 대한 구체적인 대응책을 마련하여야 한다.

다. 대화형 인공지능 서비스를 악용한 사이버보안 위협

대규모 언어 모델에 기반한 대화형 인공지능 서비스(Large Language Models Conversational AI)는 최근 인공지능 기술의 발전으로 인하여 빠르게 성장하고 있다. 대화형 인공지능 서비스는 일반 사용자와 상호작용하여 자연스러운 대화를 제공하고, 다양한 작업을 수행할 수 있다. 그러나 인공지능 기술의 발전과 더불어 인공지능을 악용한 사이버보안 위협 역시 중요한 문제로 부각되고 있다.

특히 잠재적으로 악용 가능한 인공지능 모델 중 하나는 GPT-3와 같은 대형 언어 모델이다. 이러한 모델은 자연어 처리와 생성 분야에서 광범위하게 사용되지만, 사이버 범죄와 같은 불법적인 목적으로 사용될 가능성이 있다.

① 스팸 및 사기: GPT-3와 같은 대화형 인공지능 모델은 사람처럼 글을 쓰고 응답할 수 있어 스팸 메시지나 사기 문자 등을 생성하는 데 사용될 수 있다.

② 협박 및 교란: 대화형 인공지능 모델은 텍스트를 분석하고 생성할 수 있어 협박 메시지나 가짜 뉴스 등을 생성하여 사람들을 교란시키는 데 사용될 수 있다.

③ 개인정보 침해: 대화형 인공지능 모델은 텍스트를 분석하여 이름, 전화번호, 이메일 주소 등과 같은 개인정보를 추출·수집하고 악의적인 목적으로 사용될 수 있다.

인공지능 기술의 발전과 사회적 활용에 따라 인공지능 시스템을 악용하려는 시도도 증가할 것이다. 인공지능 시스템의 악의적 활용이나 개인정보 유출과 같은 사이버위협을 방지하기 위해서는 윤리적이고 안전하게 인공지능 기술을 개발하고 활용하는 것이 중요하며, 이를 위한 정책·법률·교육 등의 대책 마련이 필요하다.

국가 차원에서 인공지능 기술의 개발과 적용에 대한 법적 규제와 지침 등을 마련하여야 하며, 개인정보보호와 같은 사용자 보호에 대한 법적 책임과 권리를 강화할 뿐 아니라 교육적 대책도 필요하다. 대화형 인공지능 서비스의 사용자는 이러한 위협에 대하여 인식하고, 언어 모델을 적절하게 사용하는 방법을 배워야 한다.

라. 소프트웨어 취약점을 이용한 타깃형 공급망 공격의 위협

소프트웨어 취약점을 이용한 공격은 사이버위협에서 가장 위협적이고 강력한 공격 방법 중 하나이다. 시스템과 소프트웨어에는 항상 취약점이 존재하며, 해커가 이를 찾아 내어 악용하기 위하여 지속적으로 노력하고 있다. 그뿐 아니라 소프트웨어 개발사를 공격하여 소스코드를 유출하고 나아가 공급망 공격을 수행하는 사례도 발생하고 있다.

최근 국민 대다수가 사용하고 있는 소프트웨어의 취약점을 통하여 타깃형 공격을 수행하는 사례가 증가하고 있다. 소프트웨어 취약점을 이용한 타깃형 공급망 공격은 범용적으로 사용되는 소프트웨어의 취약점을 이용하여 불특정 다수의 사용자 중 공격 대상인 타깃에게만 악성 코드를 유포하는 방식으로 이루어진다. 공격자는 특정 대상에게만 익스플로잇(보안취약점, Exploit) 코드를 전달하고 실행시켜 공격을 수행한다.

해당 공격은 특정 목표에게만 취약점 코드가 전달되기 때문에 보안업체나 기관에게 익스플로잇 코드의 노출을 최소화할 수 있다. 하나의 취약점을 통하여 오랫동안 공격에 악용할 수 있다는 장점이 있다.

이러한 공격은 공급자와 최종 사용자 모두에게 큰 위협이 될 수 있다. 소프트웨어 공급자는 고객의 신뢰를 잃을 뿐 아니라 법적 문제도 발생할 수 있다. 따라서 소프트웨어 개발 기업이나 조직은 보안 전문가와 협력하여 소프트웨어 취약점을 최대한 줄이는 보안 대책을 마련하고, 취약점이 발견될 경우 즉각적으로 대응하여야 한다. 일반 기업이나 조직에서도 보안 대책을 지속적으로 강화하고, 최신 사이버위협 동향과 사례를 파악하고 대비책을 마련하여야 한다.

마. 모바일 장치를 통한 새로운 보안 위험 증대

재택·원격 근무 확대로 BYOD(Bring Your Own Device) 업무 환경이 확산됨에 따라 이와 관련된 보안 위협도 증가하면서 모바일 단말 관리 등 높은 수준의 모바일 보안 기술이 절실하게 요구되고 있다.

모바일 장치 사용의 증가로 인하여 페가수스(Pegasus)와 같은 사이버 스파이 도구가 악용되는 사례가 증가하고 있다. 페가수스는 공식적으로 정부와 법 집행 기관 등에서만 사용할 수 있지만 민간 기업과 정부 관리자 등을 대상으로 한 공격 사례가 나타나고 있다.

FlyTrap·Triada·MasterFred 맬웨어(악성 소프트웨어, Malicious Software)를 포함하여 다양한 모바일 맬웨어가 생겨나고 있으며, 소셜미디어, 취약한 앱 스토어 보안 제어, 유사 기술 등을 이용하여 모바일 단말에 대한 접근 및 필요 권한을 획득한다.

모바일 맬웨어는 이메일이 아닌 모바일 문자 메시지를 통하여 전송하는 스미싱(문자 메시지 피싱, SMS 피싱) 수법을 활용하고 있으며, 별도의 기술력이 없더라도 저렴한 가격($50~100)의 피싱 도구를 활용하여 상대적으로 쉽게 접근할 수 있다.

모바일 단말은 사이버보안 위협의 새로운 통로가 되었으며, 지금이 모바일 보안 환경에 대한 즉각적인 대비책을 마련하여야 하는 시점이다.

바. 화재 등 재난재해에 의한 서비스 중단 위협

2022년 10월 SK C&C 데이터센터 화재로 인하여 많은 국민이 이용하던 서비스인 '카카오톡'을 비롯한 멜론·티스토리·다음 등 카카오의 대다수 서비스뿐 아니라 네이버·SK의 일부 서비스 등의 이용이 불가능하였다. 전기실 내 정전으로 인한 서버 셧다운을 방지하기 위하여 구축된 무정전 전원장치(UPS)에서 시작된 화재로, 화재 시점으로부터 서비스가 완전히

정상화되는 데까지 약 5일이 소요되었다.

대다수 국민이 사용하는 서비스이었기 때문에 금융·결제·교통 등의 서비스 중단으로 인하여 많은 혼란을 일으켰으며, 서비스 중단으로 인한 피해는 고스란히 사용자가 떠안게 되었다.

2022년 8월 미국 아이오와주 구글 데이터센터에서도 전기 관련 폭발 사고가 일어나 작업자 3명이 부상을 입었으며, 약 30분간 구글의 일부 서비스(지메일, 구글드라이브 등)가 중단되어 사용자들이 불편을 겪었다.

데이터센터 화재 사고 이후 카카오는 통신뿐 아니라 금융에서도 중요한 위치를 담당하고 있어 메인센터와 동일하게 DR(재해복구, Disaster Recovery)센터를 구성하여 동시에 서비스를 제공하는 미러 사이트(Mirror Site) 구축 등 다각화 전략을 사용하여야 한다는 의견이 있었으나, 다각화가 복제보다 많은 비용이 소요된다는 문제점이 존재한다.

DR센터는 재난 발생 시에도 서비스가 안정적으로 제공·유지될 수 있는 역할을 하고, 이러한 서비스의 지속성은 기업의 수익, 이미지 등에 많은 영향을 미치기 때문에 많은 기업과 공공기관들은 DR센터를 설치하여 운영하고 있다.

정부는 이에 「방송통신발전기본법」 개정안을 발의하였으며, 개정안에는 데이터센터 사업자가 의무적으로 이중화 조치를 갖추도록 하는 내용이 담겼다. 또한 네이버·카카오 등 부가통신사업자도 기간통신사업자처럼 재난관리 기본 계획을 의무적으로 세우도록 하였다.

「정보통신망 이용촉진 및 정보보호 등에 관한 법」 개정안은 데이터센터를 운영하는 기업뿐 아니라 이를 빌려 쓰는 카카오·네이버 등 기업에게도 보호 조치 의무를 부과한 바 있다. 이는 네이버·카카오 등 외부 데이터센터를 빌려 쓰는 통신사업자가 데이터센터 출입을 통제하거나 필요한 설비를 내부에 설치하여 운영하는 등 데이터센터 공간을 직접 관리하는 경우 대통령령에 따른 보호 조치를 갖추어야 한다는 것이다. 그리고 재난 등으로 서비스가 멈추면 현황과 조치 내용을 과학기술정보통신부 장관에게 의무적으로 보고하게 하는 내용도 포함되었다.

2022년 러시아의 우크라이나 침공 상황을 고려하였을 때 재난·전시 상황에서 민간통신의 중요성이 입증된 만큼 비용 투자의 시급성을 고려하여야 한다. 사이버 복원력 관점에서 재난을 경감하고 유용성을 판단하여 점진적인 시스템 개선이 필요한 시점이다.

2

제2편

정보보호 법·제도 및 기관

제1장 정보보호 법·제도
제2장 정보보호 기관 및 단체

제1장

정보보호 법·제도

제1절 정보보호 법·제도 발전과정

1. 정보사회 초기단계(1980년대~1999년)

1980년대부터 추진해 온 국가 정보화와 함께 이에 따른 역기능이 대두되면서 정보보호 법·제도가 본격적으로 정비되기 시작하였다. 1986년 정보화에 관한 국가 시책과 제도를 규정한 「전산망 보급확장과 이용촉진에 관한 법률」이 제정되었다. 이 법은 전산망을 보호하기 위한 일부 규정을 포함하고 있으나, 정보보호의 중요성에 초점을 맞춘 법률은 아니었다.

1995년 정보화 촉진에 관한 내용과 더불어 정보보호에 관한 기본적인 규정을 담은 「정보화 촉진 기본법」이 제정되었다. 또한 「형법」이 개정되어 전자기록 위작·변작죄 및 전자기록에 대한 비밀침해죄 등이 신설되었다.

한편 인터넷의 본격적 보급에 따라 전자상거래의 이용 증가에 따른 개인 및 기업의 정보 유통과 중요 정보를 보호하기 위하여 1999년 「전자서명법」 제정을 비롯하여 「전산망 보급확장과 이용촉진에 관한 법률」을 「정보통신망 이용촉진 등에 관한 법률」로 전면 개정하는 등 정보화 역기능에 대한 규정 정비가 이루어졌다.

2. 정보사회 고도화단계(2000~2007년)

2000년대에 들어서면서 정보통신 시스템에 대한 국가와 사회의 의존도가 점차 높아짐에 따라 정보보호 법률이 제정되거나 기존 법률이 전면 개정되기 시작하였다.

2001년 에너지·금융·통신 등 국가와 사회의 중요한 정보통신기반시설 보호를 주요 내용으로 하는 「정보통신기반 보호법」이 제정되었으며, 「형법」 개정을 통하여 컴퓨터 등 정보처리장치에 허위정보나 부정한 명령을 입력하여 다른 사람의 재산을 빼앗는 온라인 사기행위 형벌이 규정되었다. 또한 「정보통신망 이용촉진 등에 관한 법률」 명칭을 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」로 변경하면서 정보보호와 관련된 규정을 대폭 강화하였다. 이 법은 2003년 발생한 '1.25 인터넷 대란'을 계기로 침해사고 대응 관련 규정을 크게 보완하였으며, 2004년과 2005년에도 정보보호 관련 규정을 정비하였다.

2005년 국가안보를 위협하는 해킹·바이러스 등 사이버공격으로부터 국가정보통신망을 보호하기 위하여 사이버안전에 관한 조직 및 운영에 대한 사항을 체계적으로 정립한 「국가사이버안전관리규정」이 대통령훈령으로 제정되었다.

2007년 「전자정부 구현을 위한 행정업무 등의 전자화촉진에 관한 법률」을 「전자정부법」으로 전면 개정하는 등 전자정부 구현 관련 법제의 정비가 이루어졌다.

3. 지식정보사회 구현단계(2008~2015년)

2000년대 후반에는 정보자원의 지식화와 정보의 공동이용 활성화를 통하여 국가경쟁력을 제고하고 삶의 질을 향상시키는 이른바 지식정보사회 구현이 정보화 정책의 중요한 방향으로 인식되기 시작하였다.

2009년 「정보화촉진 기본법」을 「국가정보화 기본법」으로 전면 개정하고, 「정보통신산업진흥법」을 제정하여 정보보호산업의 활성화를 촉진하는 제도적 기반을 마련하였다.

2010년 「국방정보화 기반조성 및 국방정보자원관리에 관한 법률」이 제정되고, 「전자정부법」이 전면 개정되어 행정 정보화를 촉진하는 동시에 정보보호를 개선하였다.

2011년 「개인정보 보호법」이 제정되고, 관계 법령의 개인정보보호 규정이 개정되어 개인

정보보호가 대폭 강화되었다. 한편 「지식재산 기본법」 제정에 따라 지식재산권 보호를 강화하기 위한 정보보호의 중요성이 더욱 증대되었다.

2013년 청와대를 중심으로 하는 범국가적 정보보호 추진 체계의 의미 있는 변화를 반영하여 「국가사이버안전관리규정」이 개정되었으며, 전자금융분야에 대한 침해사고 대응을 위하여 「전자금융거래법」이 개정되었다.

2014년 정보통신망 침입 등을 예방하기 위하여 중소기업 대상 기술보호관제 및 보안 시스템을 구축하는 내용이 포함된 「중소기업기술 보호 지원에 관한 법률」이 제정되었다.

2015년 「정보보호산업의 진흥에 관한 법률」이 제정되어 정보보호산업의 발전과 일자리 창출 등의 환경이 조성될 것을 기대할 수 있게 되었다.

4. 지능정보사회 구현단계(2016~현재)

빅데이터와 인공지능 등을 활용하는 지능정보기술의 발달과 4차 산업혁명이라는 변화의 시대를 맞이하면서 정보보호는 모든 산업 활동의 바탕이자 일상생활의 안전을 위한 기반으로 자리매김하였다. 이에 따라 새로운 정보보호 환경에 맞춘 제도적 개선이 이루어지고 있다.

2016년 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」이 개정되어 스마트폰 응용프로그램 개발자나 개발회사의 접근권한으로부터 이용자를 보호할 수 있도록 하고, 정보통신서비스 제공자 등의 개인정보 분실·유출 등에 대한 징벌적 손해배상을 도입하였다.

2017년 「4차산업혁명위원회의 설치 및 운영에 관한 규정」을 제정하여 4차 산업혁명을 본격적으로 준비하고 역기능에 대처하는 체계를 본격적으로 구축하기 시작하였다.

2018년 4차 산업혁명의 발전단계를 맞이하여 관련 산업을 뒷받침하는 다양한 법령의 제·개정이 이루어지는 한편, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」등 각종 법령을 통하여 정보보호를 확보하는 방안을 함께 마련하였다

또한 산업분야별 특성에 맞는 정보보호 역량을 강화하고자 금융분야는 「전자금융감독규정」 개정(2016. 10. 5.), 의료분야는 「의료법」 개정(2019. 8. 27.) 등을 통하여 산업분야별 정보보호 체계를 정비하였다.

2020년 신산업 육성을 위한 데이터 이용 규범을 정립하기 위하여 기존 여러 법령에 분산되어 있던 개인정보보호 관련 법령을 「개인정보 보호법」 중심으로 정비하였고(2020. 8. 5.), 정보통신망연결기기 등의 정보보호에 관한 대책을 보완하기 위하여 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 개정하였다.

아울러 국가 사이버안보 강화를 위하여 「국가정보원법」을 개정하여 국제 및 국가배후 해킹조직 등 사이버안보에 관한 정보의 수집·작성·배포와 중앙행정기관·지방자치단체·공공기관 대상 사이버공격·위협에 대한 예방과 대응을 국가정보원의 직무로 명시하였고, 대통령령 「사이버안보 업무규정」을 제정하여 국가정보원에 국가사이버안보센터(NCSC, National Cyber Security Center)를 두도록 하였다.

2021년에는 「국가정보원법」을 일부 개정하여 정보활동기본지침 개정 시 국회정보위원회에 보고하도록 하고, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 정보보호 최고책임자에 대한 명확한 법 해석상 기준과 총괄 업무 내용 등을 명시하였다.

제2절 정보보호 법·제도 현황

1. 주요 법령

가. 국가정보원법

「국가정보원법」은 국가안전보장에 관련된 정보와 보안 사무를 담당하는 국가정보원의 조직·직무범위 등을 정하는 법률이다. 2020년 하반기에 국회는 국가정보원이 다변화하고 있는 대외 위협으로부터 국가 안보를 수호하고 국제적 경쟁력이 높은 순수정보기관으로 변모하여야 한다는 국민적 요구에 부응하여, 북한·국외정보 및 대테러·방첩·사이버안보 직무 등을 포함하여 「국가정보원법」을 전면 개정하였다(2020. 12. 15.).

이에 따라 2021년 1월 1일자로 시행된 「국가정보원법」은 국가 전체 영역을 포괄하는 사이버안보 정보업무 체계와 공공부문을 대상으로 하는 사이버공격·위협에 대한 예방·대응 체계를 구성하는 근거가 되며, 그 내용은 다음과 같다.

국가정보원장은 국제 및 국가배후 해킹조직 등 사이버안보 관련 정보의 수집·작성·배포 직무를 수행하며, 직무 수행을 위하여 필요한 경우 현장조사·문서열람·시료채취·자료제출 요구 및 진술요청 등의 방식으로 조사할 수 있다. 사이버안보 정보에 관련된 조치로서 국가안보와 국익에 반하는 북한·외국 및 외국인·외국단체·초국가행위자 또는 이와 연계된 내국인의 활동을 확인·견제·차단하고, 국민의 안전을 보호하기 위하여 취하는 대응조치를 수행한다. 또한 국가정보원장은 중앙행정기관(대통령 소속기관과 국무총리 소속기관을 포함한다.) 및 그 소속기관과 국가인권위원회, 고위공직자범죄수사처, 행정기관 소속 위원회, 지방자치단체와 그 소속기관, 그 밖에 대통령령으로 정하는 공공기관 대상 사이버공격·위협에 대한 예방 및 대응 직무를 수행한다.

사이버안보 관련 정보 업무 또는 사이버공격·위협에 대한 예방 및 대응 직무 수행과 관련하여 국가정보원장은 정보 및 보안 업무를 기획·조정하는 한편, 직무 수행과 관련하여 필요한 경우 국가기관이나 그 밖의 관계 기관 또는 단체에 대하여 사실의 조회·확인, 자료 제출 등 필요한 협조 또는 지원을 요청할 수 있다. 이 경우 요청을 받은 국가기관이나 그 밖의 관계 기관 또는 단체의 장은 정당한 사유가 없으면 그 요청에 따라야 한다.

그 밖에 국가정보원장은 다른 법률에 따라 국가정보원의 직무로 규정된 사항을 수행하며, 여기에는 다른 법률에 따라 부여된 사이버안보 관련 사항이 포함된다.

나. 사이버안보 업무규정

국가정보원의 직무 범위에 국제 및 국가배후 해킹조직 등 사이버안보 관련 정보의 수집·작성·배포에 관한 사항을 추가하는 등의 내용으로 「국가정보원법」이 개정(2021. 1. 1. 시행)됨에 따라, 정부는 사이버안보 업무의 수행과 관련하여 법률에서 위임된 사항과 그 시행에 필요한 사항을 정하기 위하여 대통령령으로 「사이버안보 업무규정」을 제정(2021. 1. 1. 시행)하였으며, 주요 내용은 다음과 같다.

국가정보원장은 사이버안보 업무를 효율적으로 수행하기 위하여 국가사이버안보센터를 둘 수 있으며, 이의 운영을 위하여 필요한 경우 중앙행정기관 등의 장에게 소속 공무원 또는 임직원 파견 등 협조를 요청할 수 있다.

국가정보원장은 사이버안보 관련 정보업무의 수행을 위하여 필요한 경우 중앙행정기관 등

및 외국 정보·보안기관과 정보협력 체계를 구축하고, 관련 정보를 중앙행정기관 등에 배포·공유하기 위하여 정보공유시스템을 구축·운영할 수 있다.

국가정보원장은 중앙행정기관 등에 대한 사이버공격·위협 예방·대응 업무를 효율적·체계적으로 수행하기 위하여 사이버안보 기본대책을 수립·시행하고, 중앙행정기관 등의 장은 사이버안보 기본대책에 따라 해당 기관을 대상으로 한 세부 대책을 수립·시행한다.

국가정보원장은 중앙행정기관 등을 대상으로 한 사이버공격·위협에 대한 예방 및 대응의 일환으로 보안성검토와 정보보호시스템 등 도입·운영 관련 검증 및 보안관리컨설팅을 실시하며, 이와 관련된 교육·훈련과 실태평가를 실시할 수 있다. 또한 정부보안관제 체계를 구축하여 중앙행정기관 등 대상 사이버공격·위협을 즉시 탐지·대응하는 보안관제를 실시하고 경보를 발령한다. 또한 사이버공격으로 인한 사고 발생 시 공격주체의 규명과 원인 분석 및 피해내역 확인 등을 위한 조사를 실시한다.

중앙행정기관 등의 장은 해당 기관에 대한 훈련과 진단·점검을 실시하여 취약요소를 시정하여야 하며, 해당 기관의 보안관제를 위하여 정부보안관제 체계와 연계된 보안관제 체계를 설치·운영하거나 다른 기관이 운영하는 보안관제센터를 활용할 수 있다.

국가정보원장은 사이버안보 업무 수행에 필요한 전략·정책 및 기술을 연구·개발할 수 있으며, 이를 위하여 과학기술 분야 정부출연연구기관 등을 전문기관으로 지정할 수 있다.

다. 정보통신망 이용촉진 및 정보보호 등에 관한 법률

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」은 민간부문의 정보보호 추진 체계를 구성하며, 그 내용은 다음과 같다.

정보통신서비스 제공자는 정보보호 최고책임자를 지정할 수 있으며, 종업원 수, 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 정보보호 최고책임자를 지정하고 과학기술정보통신부장관에게 신고하여야 한다. 정보통신서비스 제공자는 정보통신서비스 제공에 사용되는 정보통신망의 안전성 및 정보의 신뢰성을 확보하기 위한 보호조치를 하여야 한다.

또한 다른 사람의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는

사업자는 정보통신시설을 안정적으로 운영하기 위한 보호조치를 하여야 한다.

과학기술정보통신부장관은 정보보호지침을 고시하고, 정보보호 사전점검기준에 따른 보호조치를 권고할 수 있으며, 정보보호 관리등급 부여, 정보보호 관리 체계를 운영하는 자에 대한 인증을 할 수 있다.

주요 정보통신서비스 제공자 및 집적정보통신시설 사업자는 침해사고 관련 정보를 과학기술정보통신부장관 또는 한국인터넷진흥원장에 제공하여야 한다. 과학기술정보통신부장관은 침해사고 관련 정보의 수집·전파, 침해사고의 예보·경보, 침해사고에 대한 긴급조치를 수행하며, 필요한 경우 한국인터넷진흥원이 수행하도록 할 수 있다.

주요 정보통신서비스 제공자 및 집적정보통신시설 사업자는 침해사고가 발생할 경우에는 즉시 그 사실을 과학기술정보통신부장관 또는 한국인터넷진흥원장에게 신고하여야 한다. 과학기술정보통신부는 정보통신서비스 제공자의 정보통신망에 중대한 침해사고가 발생한 때에는 민·관 합동조사단을 구성하여 원인분석을 할 수 있다.

과학기술정보통신부장관은 정보통신망 연결기기 등과 관련된 침해사고가 발생하여 국민의 생명·신체 또는 재산에 위험을 초래할 가능성이 있는 경우 관계 중앙행정기관의 장에게 피해 확산 방지조치 등을 하도록 요청할 수 있으며, 정보통신망 연결기기 등이 인증기준에 적합한 경우 정보보호 인증을 할 수 있다.

라. 정보통신기반 보호법

「정보통신기반 보호법」은 주요정보통신기반시설에 대한 정보보호 추진 체계를 구성하며, 그 내용은 다음과 같다.

정보통신기반보호위원회는 주요정보통신기반시설의 보호에 관한 사항을 심의한다. 위원장은 국무조정실장이며, 위원은 대통령령이 정하는 중앙행정기관의 차관급 공무원 및 위원장이 위촉하는 자이다.

중앙행정기관은 전자적 침해행위로부터 보호가 필요하다고 인정되는 정보통신기반시설을 정보통신기반보호위원회의 심의를 거쳐 주요정보통신기반시설로 지정한다. 과학기술정보통신부장관과 국가정보원장 등은 필요하다고 판단되는 시설에 대하여 중앙행정기관에

주요정보통신기반시설 지정을 권고할 수 있다. 분야별 정보통신기반시설을 보호하기 위하여 취약점 및 침해요인과 대응방안에 관한 정보 제공, 침해사고 발생시 실시간 경보·분석 체계 운영을 하고자 하는 자는 정보공유·분석센터를 구축·운영할 수 있다.

주요정보통신기반시설을 관리하는 기관(이하 '관리기관')은 정기적으로 또는 중앙행정기관의 장의 명령에 따라 소관 주요정보통신기반시설의 취약점을 분석·평가하며, 국가보안기술연구소, 한국인터넷진흥원, 정보공유·분석센터, 정보보호 전문서비스 기업에 취약점 분석·평가를 위탁할 수 있다. 관리기관은 취약점 분석·평가 결과에 따라 주요정보통신기반시설 보호대책을 수립·시행하고, 관계 중앙행정기관의 장에게 제출한다. 관계 중앙행정기관은 소관분야의 주요정보통신기반시설 보호계획을 수립·시행하고, 주요정보통신기반시설 보호지침을 제정하며, 관리기관에 보호조치를 명령 또는 권고할 수 있다.

과학기술정보통신부장관과 국가정보원장은 주요정보통신기반시설 보호대책 및 주요정보통신기반시설 보호계획의 수립지침을 관계 중앙행정기관의 장에게 통보할 수 있으며, 주요정보통신기반시설 보호대책의 이행 여부를 확인할 수 있다. 과학기술정보통신부, 국가정보원, 국가보안기술연구소, 한국인터넷진흥원, 정보공유·분석센터, 지식정보보안 컨설팅 전문업체는 주요정보통신기반시설 보호대책 수립, 침해사고 예방 및 복구, 보호조치 명령·권고 이행에 대한 기술적 지원을 수행한다.

관리기관은 침해사고 발생 시 관계 행정기관 등에 그 사실을 통지하고, 복구 및 보호조치에 필요한 지원을 요청할 수 있다. 정보통신기반보호위원회는 주요정보통신기반시설에 대하여 광범위한 침해사고 발생 시 정보통신기반 침해사고 대책본부를 둘 수 있다.

마. 정보보호산업의 진흥에 관한 법률

「정보보호산업의 진흥에 관한 법률」은 정보보호산업의 진흥에 필요한 사항을 정함으로써 정보보호산업의 기반을 조성하고 그 경쟁력을 강화하여 안전한 정보통신 이용환경을 조성하고자 하는 법률이며, 그 내용은 다음과 같다.

국가 및 지방자치단체는 정보보호산업의 진흥에 필요한 정책을 수립하여 시행하고 이에 필요한 재원확보 방안을 마련한다. 과학기술정보통신부장관은 정보보호산업의 진흥에 관한 정책목표와 방향을 설정하기 위하여 정보보호산업 진흥계획을 수립·시행한다.

과학기술정보통신부장관은 행정기관 또는 공공기관의 정보보호기술 구매수요정보를 정보보호기업에 제공할 수 있다. 행정기관 또는 공공기관은 정보보호제품 및 정보보호서비스의 대가를 적정한 수준으로 지급하도록 노력한다. 또한 정보보호 준비도 평가, 정보보호 공시 등의 제도를 시행한다.

정보보호산업 진흥의 기반조성을 위하여 과학기술정보통신부장관은 기술개발 및 표준화 추진, 전문인력 양성, 국제협력, 정보보호제품에 관한 성능평가, 우수 정보보호기술 및 우수 정보보호기업 지정·지원, 정보보호기업 자금융자, 수출지원, 세제지원, 정보보호 전문서비스 기업 지정 등을 할 수 있다. 정보보호산업에 관련된 사업을 경영하는 자는 과학기술정보통신부장관의 인가를 받아 한국정보보호산업협회를 설립할 수 있다.

정보보호제품 및 정보보호서비스의 개발·이용 등에 관한 분쟁을 조정하기 위하여 정보보호산업 분쟁조정위원회를 둔다. 과학기술정보통신부장관은 정보보호기업이 자율적으로 준수할 수 있는 이용자보호지침을 정할 수 있다. 정보보호기업은 과오납금의 환불, 정보보호제품 및 정보보호서비스 이용계약의 해제·해지의 권리, 제품결함 등으로 발생하는 이용자의 피해보상 등의 내용이 포함된 약관을 마련하여야 하며, 과학기술정보통신부장관은 정보보호산업 거래에 관한 표준약관을 마련할 수 있다.

바. 전자정부법

「전자정부법」은 행정업무의 전자적 처리를 위한 기본원칙과 절차 및 추진방법 등을 규정하며, 그 중에서 정보보호에 관한 내용은 다음과 같다.

국회사무처·법원행정처·헌법재판소사무처·중앙선거관리위원회사무처·행정안전부 등 중앙사무관장기관의 장은 행정정보 공동이용의 안전성 확보에 관한 사항을 포함한 전자정부 기본계획을 수립한다. 행정안전부장관은 국가정보원장과 사전 협의를 거쳐 전자적 대민서비스와 관련된 보안대책을 마련하고, 그러한 보안대책에 따라 중앙행정기관과 그 소속기관 및 지방자치단체의 장은 해당 기관의 보안대책을 수립·시행한다.

행정기관 등의 장은 정보자원 관리를 위하여 클라우드 컴퓨팅 서비스를 이용할 수 있고, 행정안전부장관은 행정기관 등의 장이 클라우드 컴퓨팅 서비스를 안전하게 이용할 수 있도록 필요한 시책을 수립하고, 행정기관 등의 장에게 필요한 지원을 할 수 있다. 행정안전부장관은

클라우드 컴퓨팅 서비스의 이용 기준 및 안전성 확보 등에 필요한 사항을 정하여 고시할 수 있고, 이 경우 보안 관련 사항은 국가정보원장과 협의하여 정한다.

국회·법원·헌법재판소·중앙선거관리위원회·행정안전부는 전자정부의 구현에 필요한 정보통신망과 행정정보 등의 안전성 및 신뢰성 확보를 위한 보안대책을 마련하고, 그러한 보안대책에 따라 행정기관의 장은 소관 정보통신망 및 행정정보 등의 보안대책을 수립·시행한다. 그리고 행정기관의 장은 해당 기관 및 그 소속기관의 정보시스템 장애 예방 및 대응을 위한 방안을 마련한다.

행정기관의 장은 정보통신망을 이용하여 전자문서를 보관·유통할 때 위·변조·훼손 또는 유출을 방지하기 위하여 국가정보원장이 안전성을 확인한 보안조치를 하여야 하고, 국가정보원장은 그 이행 여부를 확인할 수 있다. 그러한 안전성 확인은 국회·법원·헌법재판소·중앙선거관리위원회의 행정사무를 처리하는 기관의 경우에는 해당 기관의 장이 필요하다고 인정하는 경우에만 적용하며, 필요하지 않다고 인정하는 경우에는 안전성을 확인한 보안조치에 준하는 보안조치를 한다.

행정기관 및 공공기관의 장은 정보시스템의 특성 및 사업 규모 등이 대통령령으로 정하는 기준에 해당하는 정보시스템에 대하여 감리법인으로 하여금 정보시스템 감리를 하게 하여야 한다. 행정안전부장관은 정보시스템 감리의 업무범위, 절차 및 준수사항 등 감리하기 위하여 필요한 기준을 정하여 고시한다. 정보시스템 감리를 하려는 자는 정보시스템 감리에 필요한 사항을 갖추어 행정안전부장관에게 법인으로 등록하고, 등록사항을 변경할 때에는 변경사항을 미리 행정안전부장관에게 신고한다. 행정안전부장관은 일정 사유에 해당하는 감리법인 등록을 취소하거나 업무의 정지를 명할 수 있다.

사. 전자금융거래법

「전자금융거래법」은 전자금융거래의 법률관계를 명확히 하는 법률이며, 그 중에서 정보보호에 관한 내용은 다음과 같다.

전자금융거래를 위한 접근매체를 양도·양수, 대가 수수·요구 등을 수반하거나 범죄에 이용할 목적인 대여 또는 보관·전달·유통 등과 그러한 행위의 알선 및 광고는 다른 법률에 특별한 규정이 없는 한 금지된다. 금융회사 또는 전자금융업자는 이용자로부터 접근매체의

분실이나 도난 등의 통지를 받은 때에는 제3자의 해당 접근매체 사용으로 인한 이용자의 손해를 배상할 책임을 진다. 금융회사·전자금융업자·전자금융보조업자는 전자금융거래의 안전성을 확보하고 정보보호최고책임자를 지정한다. 금융회사 및 전자금융업자는 전자금융기반시설에 대하여 취약점을 분석·평가하고 금융위원회에 보고한다.

전자금융기반시설에 대한 전자적 침해행위는 금지된다. 금융회사·전자금융업자는 전자적 침해행위로 인하여 전자금융기반시설이 교란·마비되는 등의 침해사고를 금융위원회에 지체 없이 알리고 원인 분석과 피해 확산 방지조치를 한다. 금융위원회는 침해사고에 관한 정보의 수집·전파, 침해사고의 예보·경보, 침해사고에 대한 긴급조치 등 침해사고에 대응하기 위한 업무를 수행하고 「전자금융감독규정」에 따라 금융보안원 등을 침해사고대응기관으로 지정하여 금융권 통합보안관제센터를 운영하고 침해사고조사단을 구성할 수 있다.

아. 중소기업기술 보호 지원에 관한 법률

「중소기업기술 보호 지원에 관한 법률」은 중소기업의 기술보호 역량을 강화하기 위한 법률이며, 그 중에서 정보보호에 관한 내용은 다음과 같다.

중소벤처기업부장관은 중소기업이 보유한 기술의 유출방지와 정보통신망을 통한 외부의 침입 등을 예방하기 위하여 중소기업을 대상으로 한 기술보호관제서비스를 제공할 수 있다. 기술보호관제서비스는 기술보호 수준 및 보안취약점 등의 사전진단, 네트워크 및 시스템 장애 등에 대한 점검 및 관련 정보의 공유, 정보통신망을 통한 기술유출 또는 침해 발생 시 그 원인 분석 및 대응 지원 사항을 포함한다. 또한 중소벤처기업부장관은 중소기업의 보안환경에 대한 정밀진단을 통하여 적합한 보안시스템의 설계와 구축을 지원할 수 있다.

중소벤처기업부장관은 기술보호관제서비스와 보안시스템 구축 지원업무를 관련 기관 또는 단체에 위탁할 수 있고, 필요 경비의 전부 또는 일부를 지원할 수 있다.

자. 의료법

「의료법」은 국민의료에 필요한 사항을 규정한 법률이며, 그 중에서 정보보호에 관한 내용은 다음과 같다.

의료인 또는 의료기관 개설자는 전자의무기록에 대한 전자적 침해행위로 진료정보가

유출되거나 의료기관의 업무가 교란·마비되는 등 진료정보 침해사고가 발생한 때에는 보건복지부장관에게 즉시 그 사실을 통보하여야 하며, 보건복지부장관은 진료정보 침해사고의 통지를 받거나 사고 발생 사실을 알게 되면 이를 관계 행정기관에 통보하여야 한다.

보건복지부장관은 진료정보 침해사고의 예방·대응하기 위하여 진료정보 침해사고에 관한 정보의 수집·전파, 예보·경보, 긴급조치, 전자적 침해행위의 탐지·분석 등을 수행하며, 업무의 전부 또는 일부를 전문기관(사회보장정보원)에 위탁할 수 있다.

제3절 2022년 정보보호 관련 주요 개정 법령

1. 정보통신망 이용촉진 및 정보보호 등에 관한 법률(법률 제18871호, 2022. 6. 10. 일부개정, 시행 2022. 12. 11.)

침해사고를 예방하기 위하여 정보보호 취약점 신고자에 대한 포상금 지급 근거를 마련하였다. 또한 침해사고의 원인분석 및 대책 마련을 위한 후속 대응 체계를 강화하기 위하여 정보통신서비스 제공자가 다른 법률에 따라 침해사고 통지 또는 신고를 한 경우 이 법에 따라 침해 신고를 한 것으로 보고, 관계기관의 장은 관련 정보를 지체 없이 공유하도록 의무화하였다. 나아가 침해사고가 발생한 경우 과학기술정보통신부장관은 그 원인을 분석하고 대책을 마련하여 해당 사업자에게 필요한 조치를 하도록 권고할 수 있고, 필요 시 관련 자료의 보전 또는 자료 제출을 요구할 수 있도록 법률을 개정하였다.

2. 정보통신기반 보호법(법률 제18870호, 2022. 6. 10. 일부개정, 시행 2022. 9. 11.)

주요정보통신기반시설을 관리하는 기관의 장이 정기적인 취약점 분석·평가 의무를 이행하지 않거나 관계 중앙행정기관의 장의 분석·평가 명령에 불응하는 경우에 대한 사후조치가 마련되어 있지 않고, 관계 중앙행정기관의 장의 보호조치 명령을 이행하지 않은 경우 과태료를 부과하고 있으나, 그 금액이 적어 실효성을 담보하기 어려운 문제를 해결하기 위하여 보호조치 명령을 위반한 자에 대한 과태료 금액을 상향하고, 정기적으로 취약점을

분석·평가하지 않거나 취약점 분석·평가 명령에 따르지 않은 자에 대하여 과태료 부과하도록 법률을 개정하였다.

제2장

정보보호 기관 및 단체

제1절 국가기관

1. 국가안보실

국가안전보장에 관한 대통령의 직무를 보좌하는 국가안보실은 2015년 4월 사이버안보 수행 체계를 일원화하여 사이버안보에 관한 대통령의 직무를 효율적으로 보좌하기 위하여 사이버안보비서관을 신설하였다.

2017년 7월 '국정운영 5개년 계획'을 발표하여 사이버위협에 대응하기 위한 국가차원의 사이버안보 대응 역량 강화를 과제목표로 제시하였고, 국가안보실 중심의 사이버안보 컨트롤타워 강화, 체계적인 사이버안보 수행 체계 정립·발전, 사이버공간의 안전한 보호 및 사이버전 수행 능력 확보 등 국가 사이버안보 수행 체계를 강화하여 선진국 수준의 사이버안보 대응 역량 강화를 추진하고 있다.

2018년 8월 정보융합비서관과 사이버안보비서관을 통합하여 사이버정보비서관으로 개편하였고, 2021년 12월 사이버정보비서관과 안보전략비서관을 통합하여 신기술·사이버안보비서관을 신설하였다.

국가안보실은 2019년 4월 3일 사이버안보에 대한 중·장기 정책방향을 제시하는 '국가

사이버안보전략'을 발표하였으며, 그 후속으로 범부처 차원에서 이행할 구체적인 실행계획을 위하여 과학기술정보통신부·국가정보원·국방부 등 9개 기관 관계부처 합동으로 '국가사이버안보 기본계획'을 마련하여 2019년 9월 3일 국무회의에 보고·확정하였으며, 기관별 실행계획을 18개 중점과제, 100개 세부과제로 종합하고 단계적으로 추진하는 등 사이버안보 기관의 컨트롤타워 역할을 수행함으로써 사이버안보 역량을 강화하는 데 주력하고 있다.

2. 국가정보원

국가안전보장에 관련된 정보·보안 사무를 담당하기 위하여 대통령 직속으로 설치된 국가정보원은 「국가정보원법」과 「사이버안보 업무규정」등 개별 법령에 따라 국가 전체 영역을 포괄하는 사이버안보 관련 정보 업무와 공공부문을 대상으로 하는 사이버공격·위협의 예방·대응업무를 수행하고 있으며, 구체적인 역할은 다음과 같다.

첫째, 「국가정보원법」과 「사이버안보 업무규정」에 따라 국가정보기관으로서 수행하는 국가정보 업무이다.

국가정보원은 국제 및 국가배후 해킹조직 등 사이버안보 관련 정보의 수집·작성·배포 직무를 수행하며, 직무 수행을 위하여 필요한 경우 현장조사·문서열람·시료채취·자료제출 요구 및 진술요청 등의 방식으로 조사할 수 있다. 이와 관련하여 「전기통신사업법」에 따른 통신자료 제공요청, 「통신비밀보호법」에 따른 국가안보목적 통신제한조치 및 통신사실 확인자료 제공요청 등의 법적 수단을 활용할 수 있다.

이와 관련하여 국가안전보장과 관련된 정보 분석을 목적으로 국가정보원이 수집 또는 제공요청하는 개인정보에 대하여는 「개인정보 보호법」 제58조제1항제2호에 따라 「개인정보 보호법」 제3장부터 제7장까지 적용되지 않는다.

사이버안보 관련 정보 업무를 위하여 필요한 경우 중앙행정기관 등 외국의 정보·보안기관과 정보협력 체계를 구축하고, 관련 정보를 중앙행정기관 등에 배포·공유하기 위하여 정보공유 시스템을 구축·운영할 수 있다.

이와 관련하여 국가정보원은 2016년부터 '국가사이버위협 정보공유시스템(NCTI, National Cyber Threat Intelligence)'을 구축하여 운영하고 있으며, 2020년 10월부터

방산업체·국가핵심기술보유기업 등 국익 및 국가안보와 직결되는 민간 산업분야와 정보공유 협약을 체결하고 인터넷 기반의 정보공유시스템(KCTI, Korea Cyber Threat Intelligence)을 구축하여 정보서비스를 진행하고 있는 등 사이버안보 정보의 허브 역할을 수행하고 있다. 2023년 1월 1일 기준 국가·공공기관 326개 및 방산업체를 비롯한 153개 민간기업이 정보공유시스템을 이용 중이며, 범국가 차원의 사이버위협 대응 체계를 갖추는 것을 목표로 한다.

국가정보원은 「국가안전보장회의법」 제10조에 따라 사이버안보 등 국가안전보장에 관련된 국내외 정보를 수집·평가하여 국가안전보장회의(NSC)에 보고함으로써 심의에 협조하고 있다.

아울러 사이버안보 관련 정보에 관한 조치로 국가안보와 국익에 반하는 북한·외국 및 외국인·외국단체·초국가행위자 또는 이와 연계된 내국인의 활동을 확인·견제·차단하고, 국민의 안전을 보호하기 위하여 대응조치를 취할 수 있다.

둘째, 「국가정보원법」 과 「사이버안보 업무규정」·「보안업무규정」에 따라 국가보안기관으로서 수행하는 공공부문 사이버공격·위협에 대한 예방·대응 업무이다.

국가정보원은 중앙행정기관(대통령 소속기관과 국무총리 소속기관을 포함한다.) 및 그 소속기관과 국가인권위원회, 고위공직자범죄수사처, 행정기관 소속 위원회, 지방자치단체와 그 소속기관, 「공공기관 운영법」에 따른 공공기관, 지방공사·공단, 한국은행 등 주요 특수법인, 국립·공립학교, 정부출연연구기관 대상 사이버공격·위협에 대한 예방·대응 직무를 수행하며, 그 일환으로 ▲사이버안보 기본대책 수립·시행 ▲보안성검토 ▲정보보호시스템 등 도입·운영 관련 검증 및 보안대책 수립 ▲보안관리컨설팅 ▲교육·훈련 ▲실태평가 ▲정부보안관제 체계 구축 및 중앙행정기관 등 대상 보안관제와 경보 발령 ▲사이버공격으로 인한 사고 발생 시 공격 주체 규명, 원인 분석 및 피해내역 확인 등을 위한 조사를 실시한다.

국가정보원은 「보안업무규정」에 따라 전자적 방법에 의한 비밀 보호기술을 개발·보급하고, 암호자재를 제작하여 공급하며, 각급기관이 이를 적절하게 수행하는지를 확인한다. 또한 각급기관의 정보통신보안규정 위반사항을 적발한 때에는 해당 정보통신 운영기관의 장에게 통보하여 조치하도록 하고 있다.

셋째, 그 밖에 다른 법률에 따라 국가정보원의 직무로 규정된 사항 중에서 공공부문

사이버보안에 관련된 업무이다.

국가정보원은 「전자정부법」에 따라 행정기관의 장이 정보통신망을 이용하여 전자문서를 보관·유통할 경우 보안대책을 지원하고 그 이행여부를 확인할 수 있다. 아울러 「공공기록물 관리에 관한 법률 시행령」에 따라 공공기관 및 기록물관리기관의 장이 전자기록물의 생산·이관·보존·폐기 등 기록물관리 과정에서 전자기록물을 안전하게 관리할 수 있도록 보안대책을 지원하고 그 이행 여부를 확인할 수 있다.

국가정보원은 「정보통신기반보호법」에 따라 주요정보통신기반시설 보호에 관하여 심의하기 위하여 설치된 국무총리 소속 정보통신기반보호위원회의 실무기구인 '공공분야 정보통신기반보호실무위원회'를 운영하고 공공분야 주요정보통신기반시설 보호대책 이행 여부를 확인하는 등 공공분야 정보통신기반시설 보호업무를 총괄하고 있다. 또한 공공·민간분야를 막론하고 국가안전보장에 중대한 영향을 미치는 주요 교통시설, 에너지·수자원 시설, 방송중계·국가지도통신망 시설, 원자력·국방과학·첨단 방위산업 관련 정부출연연구기관 연구시설의 경우 국가안보에 현저하고 급박한 위험이 있고 관리기관의 장이 요청할 때까지 기다릴 경우 그 피해를 회복할 수 없을 때에는 관계 중앙행정기관의 장과 협의하여 그 지원을 할 수 있다.

국가정보원은 「국가정보원법」·「사이버안보 업무규정」·「보안업무규정」·「정보 및 보안업무 기획·조정규정」·「전자정부법」·「공공기록물 관리에 관한 법률 시행령」·「정보통신기반보호법」에 따라 각 국가·공공기관이 수행하여야 할 사이버보안과 관련한 기본업무를 집대성한 「국가 정보보안 기본지침」(국가정보원 지침)을 대외 시행하고 있다.

이상 살펴본 바와 같이 국가정보원은 사이버안보 관련 정보 및 사이버공격·위협에 대한 예방·대응 업무를 수행하며, 이와 관련하여 정보 및 보안업무를 기획·조정하는 한편, 직무수행과 관련하여 필요한 경우 국가기관이나 그 밖의 관계기관 또는 단체에 대하여 사실의 조회·확인, 자료 제출 등 필요한 협조 또는 지원을 요청할 수 있다. 이 경우 요청을 받은 국가기관이나 그 밖의 관계기관 또는 단체의 장은 정당한 사유가 없으면 그 요청에 따라야 한다.

국가정보원은 2003년 발생한 1.25 인터넷 대란을 계기로 사이버공격에 대한 종합적이고 체계적인 예방·대응을 위하여 2004년 2월 국가사이버안전센터(NCSC)를 설립하였으며,

「국가정보원법」 개정과 「사이버안보 업무규정」 제정에 따라 2021년 1월 1일자로 국가사이버안보센터(NCSC)로 명칭을 변경하였다. 국가정보원장은 국가사이버안보센터 운영을 위하여 필요한 경우 중앙행정기관 등의 장에게 소속 공무원 또는 임직원 파견 등 협조를 요청할 수 있다.

국가정보원은 사이버안보 업무 수행에 필요한 전략·정책·기술을 연구·개발할 수 있고, 이를 위하여 과학기술분야 정부출연연구기관 등을 전문기관으로 지정할 수 있으며, 현재 한국전자통신연구원 부설 국가보안기술연구소를 전문기관으로 지정하여 활용하고 있다.

3. 과학기술정보통신부

과학기술정보통신부는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」·「정보통신기반보호법」·「국가정보화기본법」·「전자서명법」·「정보보호산업의 진흥에 관한 법률」 등 관계 법령에 근거하여 민간분야 침해사고 예방·대응 체계의 구축·운영, 민간분야 주요정보통신기반시설의 지정 권고 및 취약점 분석·평가, 전자인증, 정보보호산업 및 정보보호 인력 관련 주요 정책 수립·추진 등 민간분야 정보보호에 관한 업무를 수행하고 있다.

2013년 3월 행정안전부·지식경제부·방송통신위원회에 나뉘어 있던 정보보호에 관한 업무가 미래창조과학부로 이관되었으며, 2017년 정부조직개편에 따라 미래창조과학부에서 과학기술정보통신부로 명칭이 바뀌었다.

과학기술정보통신부는 사이버보안 강화를 통한 국민 불안 해소를 국정과제로 하여 안전한 사이버환경을 조성하기 위한 정책을 추진하고 있다. 국내 인터넷의 이상징후를 365일 24시간 상시 모니터링하고, 340만여 개 홈페이지의 악성코드 감염을 탐지하고 있다. PC가 악성코드에 감염될 경우 해당 사실을 개인에게 통지함으로써 사이버공격 발생 시 신속하게 대응하여 피해를 최소화할 수 있도록 하고 있다.

특히 2017년 전세계에 동시다발적으로 전파되어 150여 개국에서 30만 대 이상의 시스템을 감염시킨 워너크라이(WannaCry) 랜섬웨어를 초기에 분석하고 대책을 마련하여 국내 피해를 최소화(피해신고 21건)하는 성과를 거두었다. 아울러 지능형 지속공격(APT, Advanced Persistent Threat) 등 날로 고도화·지능화하고 있는 사이버공격을 예방·대응하기 위하여

범국가적 정보보호시스템을 확충하고 악성코드·악성앱 차단율을 높이기 위하여 노력하고 있다.

한편 더욱 고도화하는 사이버위협에 선제적으로 대응하기 위하여 사이버위협 정보공유기관을 2018년 230개사에서 2019년 260개사로 확대하였으며, 최근 산업·사회 전 분야로 확대되고 있는 사이버공격의 대응과 예방을 위하여 정보보호 협력채널 및 1만 9,000여 개 기업의 보안담당자와 유기적 연대를 이루기 위한 'K-사이버보안 대연합'을 출범(2021. 11.)하였다.

또한 사이버위협 정보 분석·공유 시스템(C-TAS: Cyber Threat Analysis & Sharing)을 개방형으로 전환(2022. 1.)하여 기업 누구나 활용할 수 있도록 지원하고 위협상황을 신속히 전파할 수 있는 체계를 구축하였다.

과학기술정보통신부는 정보통신·금융·교통 등 민간분야의 중요 시설에 대하여 주요정보통신기반시설로 지정되도록 관계기관에 권고하여 국민 생활 인프라에 대한 사이버안전망 확충에 이바지하고 있다. 또한 정보보호 관리 체계(ISMS)와 개인정보보호 관리 체계(PIMS, Personal Information Management System)를 통합한 정보보호 및 개인정보보호 관리 체계(ISMS-P) 인증 제도를 시행하고, 정보보호 최고책임자 지정·신고 제도를 운영하는 등 기업이 침해사고 발생을 예방하고 정보보호 대응능력을 제고할 수 있도록 유도하고 있다.

정보보호산업 생태계의 새로운 거점을 마련하기 위하여 2017년 9월 경기도 판교 제2테크노밸리에 정보보호 클러스터를 조성하였다. 정보보호 클러스터에서는 정보보호 관련 기업·대학·연구기관 등 다양한 이해관계자들이 인적 교류를 통하여 정보와 지식을 공유하고, 우수 정보보호제품·서비스 개발 지원, 예비창업자 및 스타트업을 육성하기 위한 환경을 제공하고 있다. 2022년 기준 정보보호 클러스터에 17개 기업이 입주할 수 있는 사무공간이 있으며, 정보보호 테스트베드·제품전시관·교육훈련장 등을 조성하여 국내 정보보호 산업이 활성화할 수 있도록 지원하고 있다.

또한 다양하고 편리한 신기술 전자서명 확산과 공인·사설인증서 간 차별을 폐지하기 위하여 「전자서명법」 전부개정을 추진하였다. 과학기술정보통신부는 전자서명의 안전성·신뢰성·보안성 등을 확인해 주는 평가·인정 제도를 도입하여 운영하고 있다. 이 제도는 국민이 전자서명 수단을 선택하는 데 도움을 주기 위하여 전자서명인증의 안전성·신뢰성·보안성 등을 확인해

주는 제도이다. 전자서명인증사업자는 평가기관으로부터 전자서명의 운영기준 준수 여부를 평가받고 인정기관(한국인터넷진흥원)의 승인을 받아 '전자서명인증업무 운영기준 준수사실 인정 증명서'를 발급받을 수 있다. 2022년 기준 19개 전자서명인증사업자가 전자서명인증업무 운영기준 준수사실 증명서를 발급받아 전자서명인증 서비스를 제공하고 있다.

과학기술정보통신부는 4차 산업혁명과 디지털경제 발전을 뒷받침하고, 글로벌 보안 수요 증대를 기회로 국내 보안기업의 혁신성장을 지원하기 위하여 2019년 '민간부문 정보보호 종합계획'을 수립하였다. 이를 통하여 ▲사이버안전망 확대 ▲정보보호산업 경쟁력 강화 ▲정보보호 기반 강화 등을 추진 중이다.

또한 4차 산업혁명의 지속 가능성을 뒷받침하기 위하여 급변하는 사이버위협에 효과적으로 대응하고, 관련 산업 기술경쟁력 강화를 위하여 추진해야 할 '민간부문 정보보호 R&D 중장기 전략'을 제시하였다. 이 전략을 통하여 콘텐츠·플랫폼·네트워크·디바이스 등 ICT 전 영역에 걸쳐 보안수준을 높이기 위한 핵심기술개발을 추진하고, '사이버보안 그랜드 챌린지'와 같은 혁신적 R&D를 추진하고 있다.

과학기술정보통신부는 정보보호제품을 평가하고 인증하기 위하여 ▲CC인증 ▲성능평가 ▲신속확인제를 운영하고 있다. CC인증 제도는 정보보호제품의 신뢰성 향상과 보안수준 제고를 위하여 2002년 도입되었으며, 2014년부터 과학기술정보통신부가 운영하고 있다. CC인증을 받을 경우 공공조달 시 수의계약이 가능하여 현재 시장에서의 영향도가 가장 높다. 성능평가는 성능이 우수한 정보보호제품의 도입을 활성화하기 위하여 정보보호제품의 처리성능을 종합적으로 시험·평가하는 제도이다. 다른 제도와 달리 제품의 성능 평가에 중점을 두고 있는 것이 특징이다. 신속확인제는 평가기준이 없어 기존 인증제도에서 평가할 수 없었던 신기술 및 융·복합제품을 보안성 점검과 기능시험이 완료되면 공공시장에 신속히 진출할 수 있도록 규제를 개선하여 2022년 10월부터 운영하고 있다. 과학기술정보통신부는 신속확인제가 시장에 안착할 수 있도록 공공 수요처와 공급기업을 대상으로 제도 홍보, 기업 지원 체계 마련 등 지속적인 노력을 기울이고 있다.

과학기술정보통신부는 국내 기업의 정보보호 투자 확대를 유도하고, 이용자의 안전한 인터넷 이용을 꾀하기 위하여 2016년부터 정보보호 공시제도를 운영하고 있다. 2021년까지는 기업의 선택에 따라 자율적으로 운영되었지만, 디지털 대전환 시대에 대비하여 모든 산업

분야에 정보보호 투자 선순환 구조가 정착될 수 있도록 2021년 12월 「정보보호산업법」을 개정·시행하여 2022년부터 일정규모 이상 기업의 경우 정보보호 공시를 의무화하였다. 또한 공시내용의 정확성·신뢰성 등을 검증하기 위하여 허위·불성실 공시에 대한 제재 방안을 마련하는 등 정보보호 공시제도의 실효성을 지속적으로 확보할 예정이다.

또한 정보보호 인력 수급 문제를 해소하기 위하여 2025년까지 정보보호 인력 3만 명을 양성할 계획이며, 이를 위하여 해마다 실전형 사이버훈련장(Security-Gym), 차세대보안리더(BoB) 양성과정 등을 운영 중이다. 2019년 3개, 2020년 5개 총 8개의 융합보안대학원을 신설하여 스마트시티·스마트공장 등 융합산업 분야 보안인재를 양성하고 있다.

한편 코로나19 확산으로 인하여 정보보호 교육을 받지 못하는 경우를 방지하고, 지역에 거주하는 국민도 언제든지 교육받을 수 있도록 온라인 실전형 사이버훈련장(Online-Security-Gym)을 신설하였다. 앞으로도 정보보호 전문인력 양성 교육은 시대 변화를 반영하여 지속적으로 개편할 예정이다.

코로나19에 따른 전 산업의 디지털 전환으로 비대면 서비스 확산에 필수적인 정보보호 수요를 차세대 핵심산업으로 육성하기 위하여 2020년 6월 '제2차 정보보호산업 진흥계획(2021~2025)'을 발표하였다.

또한 2020년 6월 정보보호인증의 법적 근거 마련 등 ICT 융합보안 강화를 위한 「정보통신망 이용촉진 및 정보보호에 관한 법률」이 개정되었고, 하위법령도 12월에 개정되어 시행하고 있다.

2021년 2월 디지털경제 시대를 선제적으로 대비하고 디지털안심 국가를 실현하기 위한 'K-사이버방역 추진전략'을 발표하였다. 2023년까지 총 6,700억 원을 투자하여 디지털안심 국가 기반 구축, 보안 패러다임 변화 대응 강화, 정보보호산업 육성 기반 확충 등 3대 중점전략을 추진할 계획이다.

디지털 대전환에 따른 데이터 활용이 확산되면서 안전한 데이터 활용을 위한 데이터 보호기술에 대한 수요가 급증하고 있다. 이에 2021년 데이터 이용을 활성화하고 안전한 데이터 경제로의 전환을 뒷받침하기 위한 '데이터 보호 핵심기술 개발전략'을 마련하여 발표하였다.

최근 프로그래머가 랜섬웨어를 제작하여 범죄조직에 공급하고 수익을 공유하는 '서비스형 랜섬웨어(RaaS, Ransomware as a Service)'가 활성화함에 따라 범죄형태 또한 분업화·조직화하고 있다. 이에 따라 2021년 8월 관계부처와 합동으로 '랜섬웨어 대응 강화방안'을 수립하여 '24시간 랜섬웨어 대응지원반'을 운영하고, 주요정보통신기반시설 긴급점검을 실시하였다.

전통산업과 ICT의 융합이 가속화하면서 스마트공장·스마트카 등의 보안 내재화를 위한 융합보안 시장의 성장이 전망되며, 이에 대응하기 위하여 2022년 2월 과학기술정보통신부는 '정보보호산업의 전략적 육성 방안'을 발표하였다. 정보보호산업의 성장 동력 확보를 위하여 ▲정보보호 신시장 창출 ▲글로벌 일류 정보보호기업 육성 ▲정보보호산업 기반 강화를 위한 생태계 확충 ▲차세대 정보보호 기술경쟁력 확보 등 4개 전략을 중심으로 실행 과제를 마련하여 정보보호산업의 차세대 전략산업으로의 도약을 추진할 계획이다.

4. 행정안전부

행정안전부는 「전자정부법」·「정보통신기반 보호법」 등 관계 법령에 따라 소관 정보보호 업무를 수행하고 있으며, 디지털정부의 사이버침해 대응 역량을 강화하기 위하여 국가정보자원관리원과 한국지역정보개발원 및 광역자치단체 17곳에 사이버침해대응센터를 구축하여 각종 사이버공격에 공동 대응하고 있다. 또한 2009년 7.7 디도스 공격 이후 국가적 사이버 위기에 대응하기 위하여 유관기관과 합동으로 범정부 공조 체제를 가동하고 있다. 특히 국가정보통신망 내 정보시스템에 대한 디도스 공격 대응 역량을 강화하기 위하여 실시간 패킷 분석, 디도스 공격 차단, 사이버대피소 등 빅데이터 분석 및 선제적 정보보호 관리 체계(nAEGIS)를 구축하였다.

지능화·고도화하는 사이버공격에 대하여 보안 인력만으로는 효과적으로 대응하기 어려운 한계를 극복하기 위하여 국가정보자원관리원에서는 국가·공공기관 최초로 인공지능 기반 보안 체계를 구축하여 2021년부터 실제 운영환경에 적용하여 사이버공격 대응 범위를 확대하였고, 한국지역정보개발원에서는 지방자치단체를 대상으로 인공지능 기반 통합보안 관제분석시스템을 확대 구축하고 있다.

지방자치단체 정보통신기반시설의 보안관리를 강화하기 위하여 주요정보통신기반시설

101개(2022년 12월 기준)을 지정하여 정보시스템 보안취약점을 점검·조치하고, 방화벽·일방향 전송장비 등 필수 보안장비를 설치·보급하고 있으며, 사이버공격에 대비한 실전훈련을 실시하여 국민이 안심하고 기반시설을 이용할 수 있도록 관리하고 있다.

행정·공공기관이 디지털정부 정보시스템을 개발할 때는 정보시스템 설계단계부터 시큐어 코딩을 적용하여 소프트웨어의 보안취약점을 원천적으로 방지하도록 소프트웨어 개발보안 정책을 시행하고 있으며, 적용 여부를 확인하기 위하여 자료 요청 및 현장 방문을 실시할 수 있도록 지침에 규정하고 있다. 소프트웨어 보안약점 진단 전문가 양성을 위하여 일정 기간 소프트웨어 보안약점 진단·분석 업무를 수행한 사람을 대상으로 개발보안 진단원 양성교육과 자격시험을 실시하여 진단원 자격을 부여하고 있다.

또한 정보시스템을 데이터와 서비스의 중요도 등에 따라 5등급으로 분류하고, 등급에 따라 보안관리를 차등 적용하는 정보시스템 등급제를 마련하여 일부 중앙부처와 광역자치단체에 시범 적용하였으며, 전체 기관으로 확산을 추진하고 있다. 정보시스템 등급제에 따른 보안관리 기준 안내 등 인식 확산을 위하여 권역별로 설명회를 개최하였다.

중앙부처, 지방자치단체, 공공기관의 정보보호 관련 조직·인력 등 인적 역량을 강화하고 있다. 정보보호 업무의 전문성과 책임성을 높이기 위하여 각 기관에 정보보호 전담조직을 설치하고 적정인력이 배치될 수 있도록 각 기관과 공동으로 협업하고 있으며, 정보보호 담당자의 직무별·수준별 역량을 강화하기 위하여 국가직무능력표준에 기반한 정보보호 교육과정을 편성하여 운영하고 있다.

행정안전부는 관계부처 합동으로 2019년 10월 '디지털 정부혁신 추진계획'과 2020년 6월 '디지털 정부혁신 발전계획'을 발표하였으며, 편의성을 향상하고 안전성을 강화한 인증 체계 마련을 추진하였다. 2021년 1월부터 모바일 공무원증을 발급하여 모바일 신분증 시대를 열었다. 스마트폰으로 정부청사·스마트워크센터를 출입하고, 행정전자서명 인증서(GPKI) 없이도 출장·재택근무 시 업무시스템 등에 로그인할 수 있다. 2022년 1월 일반 국민 대상의 첫 모바일 신분증으로 모바일 운전면허증을 서울서부·대전 지역에서 시범 발급하였으며, 7월에는 전국으로 발급을 시작하였다. 모바일 운전면허증은 공공·금융기관, 렌터카·차량공유 업체, 공항, 편의점 등 실물 운전면허증이 사용되는 모든 곳에서 동일하게 사용할 수 있으며, 온·오프라인 통합 신분증으로서 온라인 환경에서도 사용할 수 있다.

2020년 12월 「전자서명법」 개정·시행으로 공인인증서 제도가 폐지되어 다양한 민간 전자서명에도 공동인증서(예전의 공인인증서)와 동일한 법적 효력이 부여되었다. 행정안전부는 디지털정부 서비스 인증 수단을 다양화하고 국민이 조기에 체감할 수 있도록 공공웹사이트에 다양한 민간 전자서명 도입을 선제적으로 추진하였다. 2021년 1월 홈택스 '연말정산 간소화서비스', 정부24 '연말정산용 주민등록증 발급 서비스', 국민 신문고 '민원·제안 신청 서비스'에 카카오·패스 등 민간 전자서명을 전자서명 공통기반을 통하여 시범 적용하였다. 이후에도 국민이 다양한 민간 전자서명을 선택하여 이용할 수 있도록 위택스, 예방접종 사전예약 시스템 등 공공웹사이트에 확대 적용하고 있다. 더불어 하나의 계정과 패턴·지문·안면인식 등 다양한 인증 수단으로 디지털정부 서비스를 편리하게 이용할 수 있는 디지털 원패스도 지속적으로 확대하고 있다.

5. 금융위원회

금융위원회는 「전자금융거래법」 등 관계 법령에 근거하여 전자금융 거래 이용자 보호와 전자금융 분야의 정보보안정책 수립 및 제도개선 업무를 수행하고 있다.

금융위원회는 2011년 농협 전산망 마비 사고 발생 이후 금융회사 등으로 하여금 정보보호 최고책임자(CISO)를 지정하여 조직 내 정보보호를 상시 관리하도록 하였으며, 2013년에 발생한 '3.20 사이버테러' 이후 전자금융기반시설에 대한 취약점 분석·평가 의무화와 전자적 침해행위 금지 및 침해사고 발생 시 금융위원회·금융회사의 대응 조치 등에 관한 내용을 「전자금융거래법」에 추가하였다.

2014년 1월 카드사의 개인정보 유출 사고 발생을 계기로 금융위원회는 금융감독원·금융협회·유관기관 등과 함께 '금융 분야 개인정보 유출 재발 방지 종합대책'을 마련하였다. 이를 통하여 개인정보 파기 관련 가이드라인 마련, 개인정보 입수 서식 및 제3자 제공 동의서 개선, 주민등록번호 과다노출 관행 개선, 신용조회 중지 요청 시스템 구축, 카드 가맹점 단말기의 IC 전환 등을 추진하고, 금융회사와 유관기관의 고객정보 보호 실태 및 수준을 점검하고 취약점을 조치하도록 하였다. 또한 「전자금융감독규정」을 개정하여 내부 및 외주업체 통제를 강화하고, '정보보안 점검의날'을 지정·운영하는 등 금융권의 개인정보보호를 더욱 강화하였다.

2015년 민간의 다양한 보안·인증기술을 활용할 수 있도록 전자금융 거래 시 공인인증서 사용 의무와 관련한 규제를 폐지하였다. 이에 따라 금융회사는 거래 인증 수단을 채택할 때 안전성과 이용 편의성 등을 고려하여 자율적으로 인증 수단을 적용할 수 있게 되었다. 규제 폐지 이후 생체인증·휴대폰SMS·QR코드를 이용한 본인인증 등 공인인증서를 대체할 수 있는 다양한 인증 수단의 활용이 증가하고 있으며, 블록체인 등 신기술 기반의 인증 수단이 더욱 활성화할 수 있도록 제도와 관행을 지속적으로 개선하고 있다.

2016년 금융권에서도 클라우드를 활용할 수 있도록 관련 규제를 개선하였고, 2018년 '금융권 클라우드 이용 확대 방안'을 발표하여 클라우드 활용 정보의 범위를 개인신용정보 및 고유식별정보까지 확대하였다. 이를 통하여 핀테크 기업이 특별한 제약 없이 클라우드를 활용하고, 금융회사가 클라우드 플랫폼을 이용하여 빅데이터·인공지능 기술을 자유롭게 테스트할 수 있도록 함으로써 혁신적인 서비스를 출시할 수 있는 여건을 마련하였다. 이와 함께 금융권 클라우드 서비스 이용·제공 기준을 마련하여 안전성 관리를 강화하였다.

한편 금융위원회는 보이스피싱 피해 규모가 지속적으로 증가함에 따라 과학기술정보통신부·외교부·법무부·방송통신위원회·방송통신심의위원회·경찰청·금융감독원과 함께 '전기통신금융사기 방지대책 협의회'를 운영하면서 2018년 12월 보이스피싱 현황을 점검하고 '전자금융사기(보이스피싱) 방지 종합대책'을 발표하였다. 이를 통하여 보이스피싱 수단별 대응을 강화하고 대포통장 사전 방지 및 사후 제재를 강화하는 한편, 국민의 인식을 제고하기 위하여 피해 예방 홍보 및 교육을 추진하였다. 2020년에는 전화 가로채기 악성 앱 등 기술적으로 고도화하고 있는 보이스피싱 수법에 대응하여 디지털 경제의 신뢰 기반조성을 위한 '보이스피싱 척결 종합방안'(2020. 6.)을 발표하는 등 보이스피싱 피해 예방·대응 활동을 강화하였다.

금융위원회는 데이터 활용을 활성화하면서도 정보 주체의 권리를 내실 있게 보호함으로써 국민의 신뢰를 제고하기 위하여 '금융 분야 데이터 활용 및 정보보호 종합방안'(2018. 3.)과 이 방안의 후속 조치로 '금융 분야 개인정보보호 내실화 방안'(2018. 5.)을 발표하였고, 「신용정보의 이용 및 보호에 관한 법률」을 개정(2020. 2.)하여 '금융권 정보보호 상시평가제' 및 '정보활용 동의 등급제'를 도입하고 개인신용정보를 안전하고 신뢰할 수 있는 방식으로 처리할 수 있도록 하였다.

또한 핀테크 산업 활성화에 따라 민간 중심의 자율적 보안 체계가 확립될 수 있도록 기반을 조성하고 있다. 사전 보안성 심의제 폐지(2015. 6.), 전자자금이체 시 일회용 비밀번호(OTP, One-Time Password) 사용 의무 폐지(2016. 6.) 등 금융보안 규제를 정비하였다. 더불어 혁신적 금융서비스의 실험 및 시장 안착을 지원하기 위한 금융규제 테스트베드 도입 방안을 발표(2017. 3.)하고, 블록체인 공동인증 서비스 상용화를 지원하는 등 새로운 보안 기술을 활용한 보안 수준 향상 및 이용 편의성 개선을 적극적으로 지원하고 있다.

금융위원회는 금융회사의 자율보안 체계 확립을 지원하는 한편, 사후 제재는 강화하였는데, 「전자금융거래법」을 개정하여 과태료 부과 한도를 인상하고 보안 관련 법규를 위반하였을 때 과징금 규모를 2~3배 확대함으로써 금전적 제재의 실효성을 제고하였다.

또한 '금융결제 인프라 혁신 방안'(2019. 2.)을 통하여 핀테크 기업이 오픈뱅킹 서비스를 구축하면 핀테크 보안점검 및 취약점 점검을 통과한 이후에 서비스를 제공할 수 하도록 하여 핀테크 기업이 보안 위협에 선제적으로 대비할 수 있도록 지원하였다.

2020년 '디지털금융 종합혁신방안'(2020. 7.)을 발표하여 새로운 디지털 리스크의 관리·감독을 선진화하고, 민간의 금융보안 관련 거버넌스 강화와 금융 분야 사이버안보 관리 체계 정립 등 디지털금융의 안전성 강화를 추진하고 있다.

2022년에는 '망분리 및 클라우드 규제 혁신방안'(2022. 4.)을 발표하여 금융보안 규제로 인하여 금융분야에 디지털 신기술 도입이 저해되는 상황을 해소하고, 금융회사의 혁신 및 글로벌 성장을 지원하고 있다.

한편 금융부문에서 클라우드·빅데이터·AI 등 다양한 디지털 신기술 활용이 확대됨에 따라 사이버위협의 범위와 유형이 변화하고 있다. 이에 금융위원회는 '금융보안규제 선진화 방안'(2022. 12.)을 발표하고 '금융보안 규율 체계 정비 T/F'(2023. 2.)를 구성하여 보안 거버넌스 개선, 목표·원칙·사후책임 중심의 보안규제 정비, 관리·감독 선진화를 추진하고 있다.

6. 개인정보보호위원회

개인정보보호위원회는 2020년 8월 5일 데이터3법(「개인정보 보호법」·「정보통신망법」·「신용정보법」) 시행에 따라 종전 행정안전부와 방송통신위원회 등에 흩어져 있던 개인정보 보호 기능을 이관받아 중앙행정기관으로 출범하였다.

개인정보보호위원회는 데이터 경제 시대에 부합하는 개인정보 관련 정책을 총괄·조정하며, 유관기관과 협력을 통하여 개인정보 침해·유출 사고 예방 및 대응에도 힘쓰고 있다. 아울러 안전한 데이터 활용 기반을 조성하여 데이터 경제 활성화 지원에도 노력하고 있다.

개인정보보호위원회는 출범 후 코로나19 방역과 관련하여 수기명부 개선, 전자출입명부 동의절차 간소화 등 효율적 방역 체계는 유지하면서 국민의 개인정보 최소수집 원칙은 철저히 준수하도록 보호조치를 강화하였다. 또한 페이스북 등 보호의무 위반 사업자에 대한 엄정한 처분으로 안전한 보호 여건을 조성하고 있다.

개인정보보호와 안전한 활용의 균형을 달성하기 위하여 개인정보보호 기본계획(2021~2023)을 마련하였으며, 개인정보보호 정책협의회, 가명정보 결합 체계 협의회 등의 구성·운영을 통하여 유관 부처와의 협력을 강화하고 정책의 일관성·효과성을 제고하고 있다. 또한 신기술 환경에서 개인정보의 안전한 보호를 위한 개인정보 보호·활용기술 R&D 로드맵을 마련하여 연구개발을 통한 안전 활용기반을 조성하였다.

이 밖에도 가명정보 결합 등에 관한 구체적 기준을 제시하여 가명정보 활용에 대한 불확실성을 제거하고, 공익적 목적 등 파급효과가 큰 분야를 중심으로 데이터 결합을 위한 선도 우수사례 발굴 및 가명정보 결합지원센터를 설치하여 가명정보 활용기반을 공고화하고 있다.

또한 산업현장과 전문가 등의 의견을 반영하여 가명정보 처리 과정에서 발생할 수 있는 불확실성을 해소하고 이를 통하여 정보보유기관의 적극적인 가명정보 활용을 유도하기 위하여 2022년 가명정보처리 가이드라인을 개정하였다.

2021년 5월 31일 인공지능 기술·서비스의 개발·운영 시 활용할 수 있는 개인정보보호 자율점검표(안내서)를 발표하였다.

2021년 6월 APPA 포럼을 개최하는 등 글로벌 거버넌스에 주요국으로 적극적으로 참여하고

있다. 국외 개인정보 유출 사고에 효과적으로 대응하기 위하여 APEC 프라이버시 법집행 협정(CPEA)*에 가입하였으며, 2021년 12월 EU GDPR 개인정보보호 적정성 결정 최종 승인을 받아 글로벌 수준의 개인정보보호 법제를 마련하였다.

*Cross Border Privacy Enforcement Arrangement : 회원국 간 정보공유 및 공동조사 등을 위한 집행 협정

2022년 11월 한·영 개인정보 적정성 결정이 최종 채택되었다. 이로써 EU와 영국을 포함한 유럽 전반에 자유로운 데이터 이전 혜택을 누릴 수 있게 되었다.

또한 현재 금융·공공분야 등에 도입된 마이데이터 서비스를 전 분야에 확산하기 위한 노력을 계속하고 있다. 2021년 9월 '마이데이터 데이터 표준화 방안'을 발표하고, 11월 '마이데이터 표준화 협의회' 1차 회의를 시작으로 2022년 12월까지 총 5회에 거쳐 관계부처와 함께 국가 차원의 전 분야 마이데이터 도입을 위한 논의를 지속하고 있다.

데이터 경제 견인, 국민 개인정보 신뢰 사회 구현, 국제 기준에 부합하는 개인정보 규범 선도 등을 위하여 필요한 내용을 담은 「개인정보 보호법」개정안을 마련하여 2021년 9월 국회에 제출하였다. 이번 개정안은 '개인정보 전송요구권'의 일반법적 근거와 이동형 영상정보처리기기의 기준을 마련하는 등 디지털 대전환 추세에 부합하도록 필요한 내용을 담았다. 「개인정보 보호법」은 2023년 2월 27일 국회를 통과하여 3월 14일에 공포, 2023년 9월부터 시행될 예정이다.

7. 외교부

사이버공간의 특성인 개방성과 초국경성으로 인하여 사이버위협은 시간적·장소적 제약 없이 여러 국가에 피해를 일으키므로 사이버안보는 개별 국가의 노력을 넘어 국제 공조가 필수적이다. 이러한 문제 의식에 따라 외교부는 사이버안보 분야 국제협력을 적극적으로 추진하고 있다.

외교부는 2012년 한·미 양자 사이버정책협의회를 시작으로 미국·영국·네덜란드·오스트레일리아·태국 등 다양한 국가 및 국제기구와 사이버정책협의회를 개최하고 있으며, 이러한 협의회를 통하여 양 국가(기관)의 사이버위협 동향을 평가하고, 국제무대에서의 건설적인 협력방안을 모색하고 있다.

또한 외교부는 유엔을 중심으로 이루어지는 사이버안보 국제규범 정립 논의에 적극 참여하고 있다. 2019년부터 유엔총회 1위원회 산하 정보안보 개방형 워킹그룹(OEWG, Open-ended Working Group)에 참여하여 사이버공간에서의 국가행동 규범, 국제법 적용 원칙, 역량 강화 및 신뢰구축 증진 논의에 이바지하고 있다. 아울러 합의된 규범의 구체적인 이행과 개도국의 이행 역량 강화를 위하여 사이버공간의 책임 있는 국가행동 증진을 위한 행동계획(PoA, Programme of Action for Responsible State Behaviours) 공동제안국으로 참여하는 등 개방되고 안전하고 평화로운 사이버공간을 만들려는 국제사회의 노력에 동참하고 있다.

아울러 외교부는 역내 ICT 분야 안보 제고를 위한 신뢰구축조치(CBM, Confidence Building Measure) 이행 방향 논의를 위하여 2017년 신설된 아세안지역안보포럼(ARF, ASEAN Regional Forum) ICT 안보 회기간 회의(ISM, Inter-Sessional Meeting)의 2021-2023 공동의장국을 수임하고, 유럽안보협력기구(OSCE, Organization for Security and Co-operation in Europe)와 공동으로 사이버 신뢰 구축 협력 증진을 위하여 사이버안보 콘퍼런스를 정기적으로 개최하는 등 지역협의체 중심으로 진행되는 사이버안보 신뢰구축조치 논의에 참여하고 있다. 또한 개발도상국을 대상으로 사이버공간에서의 국제법 적용 관련 세미나를 개최하고 한국국제협력단(KOICA, Korea International Cooperation Agency)의 공적개발원조(ODA, Official Development Assistance) 사업을 통하여 사이버보안 전문인력을 양성하고, 사이버 범죄 대응 환경 구축을 위하여 노력하고 있다.

이와 함께 외교부는 사이버안보 위협을 포함한 새로운 안보 위협에 대응하기 위한 우리 정부의 연대와 협력의 국제질서 선도 의지를 실현하기 위하여 세계신안보포럼을 창설하였으며, 기존 국제협력의 성과를 바탕으로 효과적인 국제협력의 발전 방향을 제시하고 진영과 이해관계를 아우르는 논의를 통하여 공통의 이해관계에 기반한 국제협력 방안을 모색하는 국제협력의 장을 마련하였다.

제2절 전문기관

1. 한국인터넷진흥원

한국인터넷진흥원(KISA, Korea Internet and Security Agency)은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 근거, 디지털 미래사회의 안전한 기반조성을 위하여 민간분야 사이버침해 사고 예방 및 대응, 개인정보보호 및 피해 대응, 정보보호산업 및 인력 양성, 정보보호 대국민서비스, 국가도메인(.kr/.한국) 서비스, 불법스팸 관련 고충처리, 블록체인과 같은 ICT 신산업 진흥 등의 업무를 수행하고 있다.

사이버침해 사고 대응을 위하여 인터넷침해대응센터(KISC, Korea Internet Security Center)를 운영하여 인터넷트래픽의 이상징후를 365일 24시간 상시 모니터링하고 주요 취약점에 대한 보안권고문을 배포하고 있다. 이와 함께 국가를 대표하는 인터넷침해사고대응팀(CERTCC)으로서 국내외 관계기관과 글로벌 공조 체계를 구축하고 사이버위협에 선제적으로 대응하고 있다.

또한 사이버보안빅데이터센터 및 민·관 협력 플랫폼인 'K-사이버보안 대연합'을 운영하여 사이버위협 정보를 민간과 신속하게 공유함으로써 사이버안전에 이바지하고 있다. 중소·영세 사업자를 위해서는 맞춤형 전용백신과 웹 취약점 점검 도구 등을 무료로 배포하고 있으며, 사이버대피소를 구축·운영하여 디도스 공격으로부터 서비스를 안정적으로 제공할 수 있도록 지원하고 있다.

전국 10개 거점지역에서 운영 중인 지역정보보호지원센터는 지역 중소기업을 대상으로 맞춤형 정보보호 서비스를 지원하며, 지역 사이버안전망 구축 및 정보보호 사각지대 해소를 위하여 노력하고 있다.

안전하고 경쟁력 있는 5G+ 융합서비스 환경을 조성하기 위하여 자율주행차·스마트공장 등 5G+ 핵심 서비스의 보안 내재화를 지원하는 '보안 리빙랩'을 운영하고 있다. 기업이 높은 보안수준의 제품을 생산하고 이용자는 안전한 제품을 선택할 수 있도록 사물인터넷(IoT) 보안인증서비스를 제공하고 있으며, 정보보호 및 개인정보보호 관리 체계 인증(ISMS-P), 클라우드 보안인증 등 안전하고 신뢰할 수 있는 정보보호 인증 체계 운영에 힘쓰고 있다.

아울러 국가 글로벌 경쟁력을 선도하는 정보보호 인재를 양성하고 보안교육 생태계를 조성하여 국가 발전에 이바지하고자 사이버보안인재센터를 운영하고 있다. 이와 함께 융합적 보안지식을 활용할 수 있는 실무인력 양성을 목표로 실전형 사이버훈련장(Security Gym)과 최정예 사이버보안 인력(K-Shield) 양성 사업을 운영하여 해마다 약 1,500여 명의 우수 인력을 양성하고 있다.

개인정보보호 관련 대내외 이슈 대응에도 다방면으로 힘쓰고 있다. EU 개인정보보호 협력센터 등을 통하여 국외 개인정보 규제 대응 및 국제협력을 강화하고 있으며, 국내 법·제도 개선 및 사업자 지원에 앞장서며 개인정보보호 정책 선진화를 추진하고 있다.

결합키 관리기관의 역할을 수행하기 위하여 가명정보 결합 종합지원시스템을 구축·운영하고 있으며, 가명정보 처리 가이드라인 및 결합전문기관 결합·반출 매뉴얼을 마련하는 등 안전한 데이터 활용 기반을 조성하고 있다. 또한 개인정보 가명·익명처리 기술 경진대회를 2018년부터 해마다 개최하고 있으며, 가명처리 전문인력 양성교육 및 맞춤형 컨설팅 제공, 지역 가명정보 활용지원센터 운영 등 저변 확대를 위한 다각적 지원을 아끼지 않고 있다.

디지털·비대면 시대에 국민이 겪는 다양한 사이버 고충 해결에도 앞장서고 있다. '118 사이버도우미'는 365일 24시간 전국 어디에서나 국번 없이 118로 연결되는 전화를 통하여 개인정보 침해·불법스팸·피싱·스미싱 등 인터넷에서 발생하는 각종 문제에 대한 상담 서비스를 무료로 제공하고 있다. '내PC 돌보미' 또한 서비스를 신청한 이용자에게 PC 원격 보안 점검을 무료로 지원하고 있다. 더불어 ICT분쟁조정지원센터는 전자거래, 인터넷주소, 정보보호산업, 온라인 광고 등 스마트 시대에 발생할 수 있는 다양한 분쟁을 상담과 조정을 통하여 해결하고 있다.

디지털 전환 따른 정보보호 패러다임 변화를 정책적 측면에서 대응하기 위한 연구, 블록체인 등 새로운 서비스를 지속적으로 발굴하고 사업화를 지원하며, 국민생활과 밀접한 분야의 전자문서 이용 확산을 추진하는 등 국민이 체감할 수 있는 혁신을 선도하고 있다. 아울러 우리나라 인터넷 서비스의 핵심 인프라인 국가 DNS의 고도화를 추진하는 등 안전하고 신뢰할 수 있는 인터넷 이용환경을 조성하기 위하여 노력하고 있다.

2. 국가보안기술연구소

국가보안기술연구소(NSR, National Security Research Institute)는 「과학기술 분야 정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」에 근거하여 2000년 설립된 정보보호 전문연구기관이다. 국가 암호기술, 해킹 대응 등 국가 사이버안보 확보를 위한 연구·개발을 수행하고, 사이버 부문 교육·훈련 관련 기반 구축과 각종 지원 활동을 수행 중이다. 인공지능 보안기술, 스마트시티 보안, 무인 이동체 위협분석, 클라우드 신뢰성 강화 등 기술 발전에 대응하여 보안 기술 연구·개발 범위를 꾸준히 넓혀 가고 있다. 또한 국가 사이버안보를 위한 정책연구를 수행하여 관계기관에 제공하고, 국외 유관 정부부처·연구기관 등과 협력을 통하여 국제사회에 이바지함은 물론 교류를 주도하고 있다.

국가보안기술연구소는 사이버보안 관련 학술대회, 교육·훈련, 국제회의 등을 주관하여 기술의 보급·공유와 협력관계 구축에 이바지하고 있다. 한국정보보호학회와 공동으로 '정보보호와 암호에 관한 국제학술대회(ICISC, Annual International Conference on Information Security and Cryptology)'를 주최하여 국제적인 학술교류를 활발히 추진하고 있다. 그리고 국내 최초로 실시간 사이버공격·방어 형식을 도입한 '사이버공격방어대회(CCE, Cyber Conflict Exercise & Contest)'를 일종의 훈련으로 운영하고 있다. 국내 기관 전산망 모사를 통하여 실제 위협상황과 유사하게 운영하여 사이버보안 종사자의 실질적 대응능력 강화를 꾀하는 프로그램이다.

해마다 '사이버공간 국제 평화안보 구축 학술회의(GCPR, International Conference on Building Global Cyberspace Peace Regime)'를 개최하여 사이버안보 확보를 위한 전략 및 정책의 국제교류 플랫폼을 제공하고 있다. 이 학술회의는 국가정보원·국가보안기술연구소가 공동 운영하며, 국내외 전문가와 함께 사이버안보 위협에 대한 국제법과 국제규범적 차원의 협력적 대응 방안을 모색한다.

국가보안기술연구소는 국가 사이버안보 강화를 위한 인재양성의 중요성을 인식하고 이를 실현하기 위하여 국가차원의 사이버위기 대응능력 향상을 목적으로 2014년부터 사이버안전훈련센터(CSTEC, Cyber Security Training and Exercise Center)를 운영하고 있다. 이 센터에서는 사이버위기 예방, 안전성 확인·평가, 사이버위협 탐지·대응, 사고분석 및 조치, 실전훈련 등의 교과 과정을 진행한다. 또한 기존 훈련뿐 아니라 스마트카·로봇 등 미래

기술 대상의 사이버공격 대응을 위한 새로운 훈련 콘텐츠를 개발하고 있다. 선진 각국의 유관기관 등이 참여하는 국제 사이버 합동훈련을 실시하고자 이를 위한 훈련장 및 온라인 훈련기술 확보를 목표로 연구개발을 수행 중이다.

국가보안기술연구소는 국제상호인정협정(CCRA, Common Criteria Recognition Arrangement)에서 정한 요건에 따라 국제표준인 공통평가기준(CC, Common Criteria)에 기반을 두고 IT보안성 인증을 수행하는 IT보안인증사무국(ITSCC, IT Security Certification Center)을 운영하고 있다. 우리나라는 2006년 국제상호인정협정에 인증서발행국으로 가입한 후 5년마다 정기심사를 통하여 국제 수준에 부합하는 평가·인증제도를 유지하고 있다. IT보안인증사무국은 국가보안기술연구소가 축적한 시험평가 및 취약성 분석기술을 기반으로 안전성과 신뢰성이 검증된 정보보호제품을 보급하기 위하여 정보보호제품 인증업무를 수행하고 있다. IT보안인증사무국은 국내 정보보호제품 평가자 자격부여 및 평가기관 승인을 통하여 정보보호 인프라 확충에 이바지하고 있다. 또한 국내 정보보호제품의 안전성과 품질 향상을 위하여 정보보호 업체와 평가기관에 대한 체계적인 기술지원과 함께 국제상호인정협정 활동을 수행하고 있다.

3. 금융보안원

금융보안원(FSI, Financial Security Institute)은 금융보안연구원과 금융결제원·코스콤의 금융정보공유·분석센터(ISAC, Information Sharing and Analysis Center) 기능을 통합하여 2015년 4월 출범하였다.

금융보안원은 「정보통신기반보호법」에 따른 금융 분야 정보공유·분석센터(금융ISAC)로, 금융 분야 정보통신기반시설의 취약점과 침해요인에 관한 정보를 공유·전파하고, 침해사고 실시간 경보·분석 체계 운영, 주요정보통신기반시설에 대한 취약점 분석·평가, 보호 대책 수립 지원을 수행하고 있다. 2022년에는 한·미·일 금융권 사이버보안 공조를 위하여 미국 FS(Financial Sector)-ISAC와 일본 F(Financials)-ISAC 등 미·일 금융보안 전문기관과 업무협약(MOU)을 체결하여 글로벌 사이버 위협에 공동으로 대응하고 있다. 또한 차세대 금융보안관제시스템을 구축하여 인공지능·빅데이터·클라우드 기반의 금융권 맞춤형 보안관제 서비스를 지원하고 있다.

금융보안원은 「전자금융감독규정」에 따른 침해사고 대응 기관으로, 침해사고 정보공유 체계 구축·운영, 침해사고의 예보·경보 발령, 금융권 통합보안관제센터 운영, 침해사고 조사·분석, 고위험군 악성코드 수집·분석, 디도스 공격 비상대응센터 구축·운영, 침해사고 비상 대응훈련 실시 등 침해사고 대응 업무를 수행하고 있다.

또한 취약점 분석·평가 전문기관으로, 전자금융기반시설에 대한 취약점 분석·평가, 금융회사의 자체 취약점 점검 지원 및 전자금융보조업자 취약점 점검 지원 업무를 수행하고 있다. 2019년부터 금융회사가 이용하고자 하는 클라우드 컴퓨팅 서비스 제공자(CSP, Cloud Service Provider)에 대한 안전성 평가를 지원하고 있으며, 금융권 버그바운티를 최초로 실시하여 전자금융거래를 위협하는 신규 취약점을 조기 발견하고, 금융권에 대한 사이버위협 인텔리전스 보고서를 발간·공유하여 사이버침해 예방 및 피해확산 방지를 지원하고 있다. 2022년에는 모의해킹 전담인력 운영 체계를 구축하여 금융회사 취약점 분석·평가를 강화하였다.

금융보안원은 금융회사에서 발생한 이상금융거래정보를 다른 금융회사와 실시간으로 공유하는 이상금융거래정보공유 체계(FISS, Fraud Information Sharing System)를 구축·운영하고 있으며, 악성파일 실시간 탐지 체계를 구축하여 악성파일 공격을 조기에 탐지·차단하고 있다. 또한 '보이스피싱 척결 종합방안'(2020. 6.)에 따라 시중은행과 대형 전자금융업자 등을 중심으로 보이스피싱 예방·대응을 위한 기술적 방안을 마련하였으며, 2021년 금융·통신·보안분야 유관 전문기관과 협력하여'범금융권 보이스피싱 사기정보 공유시스템'을 구축하였다.

2019년부터 금융보안 레그테크 포털(regtech.fsec.or.kr)을 운영하여 금융보안 컴플라이언스 자동화, 인텔리전스 검색·알림, 보고서 자동 생성, 금융보안 자문 서비스 등 금융보안 레그테크 서비스를 제공함으로써 금융회사의 규제준수 지원과 규제 대응 역량 강화를 지원하고, 금융보안 관련 가이드 개발·배포, 금융보안표준화협의회 운영을 통한 금융보안 표준화 추진 등 금융회사의 자율보안 역량 강화를 지원하고 있다.

2020년 금융데이터 유통 플랫폼인 금융데이터거래소(FinDX)를 개소하여 금융분야 데이터 유통 시장을 조성하고 데이터 기반 혁신 금융비즈니스 활성화를 촉진하였으며, 금융분야 데이터전문기관으로 지정되어 데이터(정보집합물) 결합, 개인정보 익명 처리 적정성 평가 등을

수행하고 있다. 2022년 데이터전문기관 최초로 원스톱(One-stop) 샘플링 결합 서비스를 개설하여 국내 데이터 결합 시장 활성화를 지원하고 있다.

금융보안원은 2017년부터 금융권 개인(신용)정보 처리 수탁자 공동점검을 실시하여 금융회사의 규제 비용을 절감하면서도 정보 주체의 개인(신용)정보를 안전하게 보호할 수 있도록 지원하는 한편, 「신용정보의 이용 및 보호에 관한 법률」 개정(2020. 2.)에 따라 2021년부터 금융권 개인신용정보 보호실태를 상시·체계적으로 점검하는 「금융권 정보보호 상시평가제」를 지원하여 금융권 개인신용정보 처리의 보안수준을 높이고 있다.

한편 금융보안원은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」과 「개인정보 보호법」에 따른 ISMS-P 인증기관으로, 금융회사·전자금융업자 등 금융권 ISMS-P 인증심사 및 인증을 수행하여 금융권의 자율보안 강화 노력을 지원하고 있다.

또한 핀테크 산업 활성화를 위하여 핀테크 지원센터 및 금융회사와 연계하여 핀테크 기술·서비스에 대한 보안 상담과 보안 컨설팅을 제공하고, 혁신금융사업자, 오픈뱅킹 이용기관 및 금융규제 샌드박스 참여 핀테크 기업에 대한 보안점검과 핀테크 서비스 취약점 점검을 수행하고 있다. 중소 핀테크 기업의 보안 점검을 지원하는 정부의 핀테크 보안 지원 사업 수행기관으로서 2022년부터 오픈뱅킹·P2P(Peer to Peer)뿐 아니라 금융 데이터 보호를 위하여 마이데이터 서비스 보안 점검을 추가로 지원하고 있다.

금융보안원은 「전자서명법」에 따라 과학기술정보통신부로부터 다양한 민간 인증수단의 안전성을 검증하는 전자서명인증 평가기관으로 선정(2020. 12.)되어 2021년부터 전자서명 인증 사업자를 대상으로 「전자서명법」상 운영기준 준수 여부를 평가하고 있다.

금융보안교육센터에서는 금융보안 관련 실무지식, 신기술 및 법·제도 동향 등에 관한 사이버교육과 집합교육을 제공하고, 정보보호 경영진 대상 금융보안 최고위 교육과정과 특화된 금융보안 전문가 양성을 위한 금융보안관리사 자격제도를 운영하고 있다.

이 밖에도 금융보안 통계 및 모범사례 조사·공유, 디지털금융 및 사이버보안 이슈 전망 발표, 금융정보보호협의회·금융보안포럼사무국 운영, 금융정보보호콘퍼런스(FISCON) 및 금융보안 공모전 개최, 금융회사 최고경영자 초청 세미나 개최, 계간지 '전자금융과 금융보안' 발간 등을 통하여 정보보호 인식제고를 지원하고 있다.

3

제3편

분야별 정보보호 활동

제1장 국가정보통신망 보호
제2장 디지털정부
제3장 주요정보통신기반시설
제4장 정보통신서비스
제5장 금융서비스

제1장

국가정보통신망 보호

제1절 사이버공격 탐지·차단

국가정보원장은 「사이버안보 업무규정」 제14조제1항 및 제3항에 따라 정부 차원에서 사이버공격·위협을 즉시 탐지·대응하기 위하여 보안관제 체계를 구축·운영하며, 이를 활용하여 중앙행정기관 등에 대한 보안관제를 실시하고 있다.

중앙행정기관·지방자치단체·공공기관의 장은 「사이버안보 업무규정」 제14조제2항에 따라 사이버공격을 실시간으로 탐지·분석하여 즉시 대응조치를 수행할 수 있도록 보안관제센터를 구축·운영하고 있다.

국가·공공기관의 보안관제는 단위보안관제(각급기관) → 부문보안관제(중앙행정기관) → 국가보안관제(국가사이버안보센터)로 구성된 3단계 사이버공격 탐지·차단 체계로 이루어져 있다. 국가사이버안보센터는 국가보안관제센터로서 부문·단위보안관제센터에 사이버공격을 탐지할 수 있는 기술을 배포하고, 국가안보를 위협하는 사이버공격을 탐지·대응하는 역할을 수행하고 있다.

현재 중앙행정기관은 44곳의 부문보안관제센터를 운영하고 있으며, 해당 기관 및 소속·산하기관 정보통신망을 대상으로 24시간 365일 무중단 보안관제를 실시하고 있다. 부문보안관제센터는 해당 국가·공공기관에서 운영 중인 정보시스템과 정보통신망 및 보유 정보에 대한

사이버공격을 탐지·차단하고 피해 확산을 방지하고 있다.

2022년에는 2021년 개소한 부처 합동 사이버안전센터에 2개 기관(질병관리청·새만금개발청)이 추가되어 총 6개 기관으로 공동 운영기관이 확대되면서 기관 간 보안관제 우수 협업사례로 평가되며 운영비 절감 등 성과를 나타내고 있다. 한편 보안관제 업무를 수행하기 위해서는 전문인력과 시설을 갖추어야 하는데, 필요한 경우 과학기술정보통신부장관이 지정하는 보안관제 전문기업의 기술·인력을 지원받아 보안관제 업무를 수행할 수 있다.

또한 '보안관제센터 구축·운영 가이드라인'을 발간하여 국가·공공기관의 보안관제 체계 표준화를 통한 사이버안보 대응 역량 강화를 위한 기반도 마련하였다. '신규 구축'과 '실무 운영'의 용도별로 구분된 가이드라인은 기관 상황에 따라 참조할 수 있도록 국가사이버위협정보공유시스템(NCTI, National Cyber Threat Intelligence)에 등재되었다.

보안관제를 통하여 사이버공격을 실시간으로 탐지하고 있으며, 공격에 의한 피해를 최소화하기 위하여 관계기관과 신속한 정보공유 체계를 유지하고 있다. 이에 따라 보안관제센터는 수집된 사이버공격 정보가 다른 보안관제센터의 업무와 연관될 경우 탐지·분석한 공격정보를 해당 보안관제센터에 실시간으로 공유함으로써 국가 차원의 사이버위협에 종합적이고 체계적으로 대응하고 있다.

표 3-1-1-1 부문보안관제센터 운영 현황(44곳)

분야	담당 기관	수행 조직
국무	국무조정실	국조실 사이버안전센터
감사	감사원	감사원 사이버보안센터
금융	금융위원회	금융보안원
국민권익	국민권익위원회	권익위 사이버안전센터
공정거래	공정거래위원회	공정위 사이버안전센터
재정	기획재정부	재정경제 사이버안전센터
교육	교육부	교육부 사이버안전센터
통신·과학	과학기술정보통신부	과학기술정보통신 사이버안전센터
		KISA 침해사고대응센터
		과학기술 사이버안전센터
외교	외교부	외교 사이버안전센터
통일	통일부	통일 사이버안전센터

분야	담당 기관	수행 조직
법무	법무부	법무 사이버안전센터
국방	국방부	사이버작전사령부
행정	행정안전부	국가정보자원관리원(대전)
		국가정보자원관리원(광주)
		사이버침해대응지원센터(G-CERT)
		행안부 보안관제센터
문화	문화체육관광부	문체부 사이버안전센터
	문화재청	문화재청 사이버안전센터
농식품	농림축산식품부	농식품부 사이버안전센터
에너지	산업통상자원부	산업통상자원 사이버안전센터
보건의료	보건복지부	보건복지 사이버안전센터
환경	환경부	환경부 사이버안전센터
노동	고용노동부	고용노동 사이버안전센터
국토교통	국토교통부	국토교통 사이버안전센터
해양	해양수산부	해양수산 사이버안전센터
	해양경찰청	해양경찰청 사이버안전센터
중소기업	중소벤처기업부	중소벤처기업부 사이버안전센터
국세	국세청	국세청 사이버안전센터
관세	관세청	관세청 보안관제센터
조달	조달청	조달청 사이버안전센터
통계	통계청	통계청 사이버보안관제센터
검찰	검찰청	대검 사이버안전센터
병무	병무청	병무청 사이버안전센터
방위산업	방위사업청	방위사업 관제센터
치안	경찰청	경찰전산보호센터
소방	소방청	소방청 사이버안전센터
농촌진흥	농촌진흥청	농진청 사이버안전센터
산림	산림청	산림청 사이버안전센터
특허	특허청	특허청 보안관제센터
기상	기상청	기상청 사이버안전센터
식품의약	식품의약품안전처	식약처 사이버안전센터
기관 합동	국가보훈처, 인사혁신처, 법제처, 행정중심 복합도시건설청, 질병관리청·새만금개발청	부처 합동 사이버안전센터

국가정보원 국가사이버안보센터는 보안관제 실무자 간 교류·협력 증진을 위하여 해마다 워크숍을 개최하고 있다. 2022년에는 코로나19 이후 3년 만에 대면 워크숍을 최대 규모로 개최하여 최신 보안관제 정책·기술 공유 등은 물론 기관 간 결속력을 높였다.

국가정보원 국가사이버안보센터는 각 보안관제센터와 정보공유·상황전파 등 신속한 대응 체계를 유지하는 한편, 새로운 사이버위협에 대응하기 위하여 각 보안관제센터와 함께 관제 체계를 지속적으로 고도화하고 보급을 확대하기 위하여 노력하고 있다. 특히 인공지능·빅데이터 기술을 활용한 탐지기술 개발과 일선기관 적용에 주력하고 있으며, 국가·공공기관 정보자원의 클라우드 전환·통합 계획에 발맞추어 클라우드 보안관제에 대한 연구도 병행하면서 고도화한 사이버공격 방어역량을 강화하고 있다. 또한 사이버위협 패킷이 암호화되는 추세에 적절히 대응하기 위하여 각급기관에 암호화 패킷 관제를 위한 가시화장비 설치를 독려하는 등 변화하는 공격 양상에 따라 탐지역량을 최적화하고 있다.

제2절 사고조사

국가정보원 국가사이버안보센터의 조사·분석업무는 「국가정보원법」 제5조제2항을 근거로 국제 및 국가배후 해킹 조직의 행적을 확인하거나, 「국가정보원법」 제4조제1항제4호마목 및 「사이버안보 업무규정」 제16조에 의거, 국가·공공기관 등을 대상으로 일어나는 사이버공격·위협에 대한 공격주체를 규명하고 피해 원인과 범위를 신속히 파악하여 적절한 대응이 이루어질 수 있도록 하는 데 목표를 두고 있다.

국가·공공기관 등 대상 사이버공격·위협에 해당하는 사고의 대부분은 취약한 민간 홈페이지나 국외 사이트·IP를 해킹 경유지로 악용하고 있어서 국내외 유관기관과 공조 체계를 상시 유지하고 있고, 외국의 정보기관이나 그에 협력하는 보안기업과 최신 해킹 사례나 사고조사 기법을 공유하는 등 정보협력에도 힘쓰고 있다.

2022년에 발생한 주요 해킹 사고로는 ① IT유지보수 용역업체를 통한 기술자료 절취 ② 문서보안 프로그램 제작업체 해킹 ③ 방산업체로 위장하여 해킹 메일을 유포한 사례가 있다.

첫 번째는 IT유지보수 용역업체를 공략하여 국가·공공기관 전산망에서 중요자료를 절취한 사례이다. 2022년 11월 북한의 해킹 조직이 국가·공공기관의 정보시스템 유지보수를 담당하는 용역업체 서버를 해킹하여 국책연구기관 가상사설망(VPN) 접속 계정 정보를 획득한 후 해당 기관 전산망에 침투하여 다량의 기술자료를 절취하였다. 국가정보원은 피해 기관의 신고 등으로 관련 사항을 인지한 즉시 유관기관과 합동 조사를 펼쳐 공격주체와 피해 내역 등을 파악하였으며, 피해 요인에 대한 보안패치를 신속히 실시하고 NCTI 보안권고문을 통하여 각급기관 IT유지보수 용역업체에 대한 예방점검 등을 추진함으로써 피해 확산을 차단하였다.

두 번째는 기관·업체 등 다수 이용자가 사용하는 문서보안 프로그램 제작업체가 해킹된 정황을 확인하고 대응한 사례이다. 2022년 8월 유관기관의 제보를 바탕으로 해당 업체 해킹 피해 사실을 확인한 후 신속히 한국인터넷진흥원과 합동 조사를 펼쳤다. 북한의 해킹 조직이 해당 업체 내 취약한 전산장비들을 순차적으로 해킹하여 암호화키 및 소스코드 등 다량의 중요자료 절취 사실을 확인하였다. 해당 프로그램을 사용하는 시스템 대상 보안점검 등 국가·안보기관 및 민간기업에 미칠 영향을 면밀히 파악하고, 해킹 경유지 차단 등 신속 대응으로 이어질 수 있는 추가 피해를 원천 차단하였다.

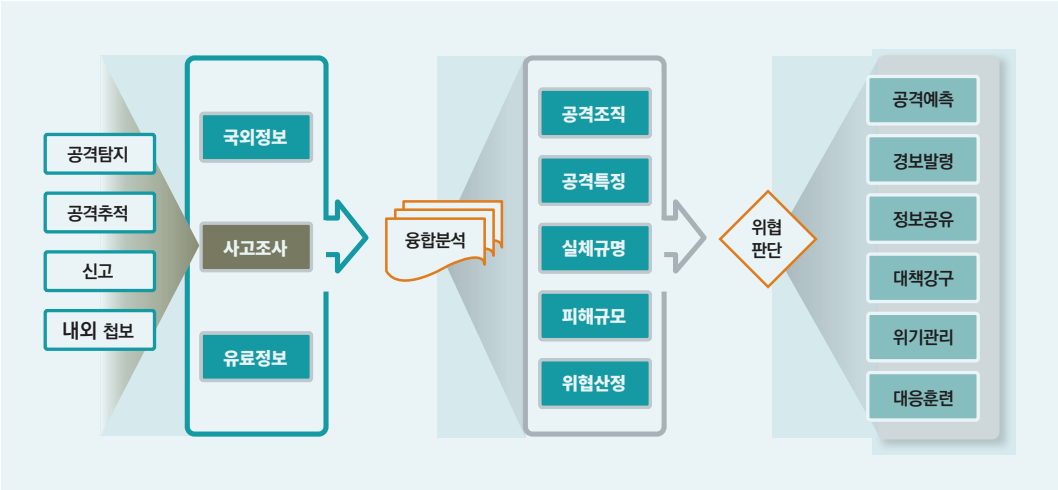
세 번째는 방산업체 직원 이메일을 탈취·악용하여 유포한 해킹 메일 대응 사례이다. 2022년 1월 확실하지 않은 해커가 방산업체 직원 이메일 계정을 탈취하여 국가기관과 민간업체에 해킹 메일을 유포한 정황이 포착되었다. 이에 유관기관과 합동 조사를 실시한 결과 메일서버 자체가 점거된 피해 사실을 확인하여 보안조치하였으며, 해킹 메일 수신자 대상 악성코드 감염 등 피해 유무를 신속히 파악하여 피해 확산을 차단하였다. 유사한 형태의 이메일주소 사용을 넘어 신뢰 관계에 있는 업무유관자 이메일 계정을 탈취하여 해킹 메일을 유포하는 등 수법이 더욱 치밀해짐에 따라 메일 열람 시 특이한 첨부파일이 포함되어 있지는 않은지 등 이상 유무를 꼼꼼히 확인해야 할 필요성을 느끼게 해 주는 사례이기도 하다.

분석업무는 조사과정에서 채증하거나 신고 또는 외국 정보기관, 국내외 보안업체로부터 입수한 악성코드 등 위협정보를 분석하여 공격기법, 취약점, 해킹 목적, 공격주체 등을 파악하는 역할을 한다. 또한 유사한 사이버침해사고의 탐지·예방 등을 위하여 악성코드의 통신 패턴을 파악하여 보안관제 탐지규칙에 반영하고, 악성코드 및 침해지표를 보안업체와 NCTI에 공유한다. 한편 공격주체를 파악하기 위해서는 다양한 해킹 조직의 기존 공격 프로파일인

데이터베이스가 필요한데, 단일 기관의 자료로는 정확한 판단이 불가하여 국내 조사·수사 기관, 국내외 정보보안업체와 합동으로 해킹 조직을 분류·판별하기도 한다.

또한 보안관제 정보, 조사 결과 등 각종 정보를 종합하여 공격실체, 특징, 피해 규모 등을 판단하고 앞으로의 공격을 예측하여 사전 대비하는 등 위기 관리를 수행하며, 범국가 차원의 위기상황으로 발전할 경우 위기평가회의를 개최하여 위기징후를 판단하고 위협수준에 따라 사이버위기 경보를 발령하고 있다.

그림 3-1-2-1 위협정보 분석·판단 과정



정부는 2014년 12월 한국수력원자력 해킹 사건을 계기로 2015년 4월 '국가 사이버안보 태세 강화 종합대책'을 수립하고, 대규모 사이버공격 시 민·관·군 간 정보공유로 신속한 상황 파악·공동대응을 통한 피해 확산 방지를 위하여 NCTI 구축을 과제로 선정하였다.

이에 국가안보실·국가정보원·과학기술정보통신부·국방부·금융위원회 등 사이버보안 관련 주요 10개 기관이 참여하여 2015년 12월 국가정보원에 정보공유시스템 구축을 완료하고, 민·관·군·금융 등 분야별 사이버위협 판단·전망 및 사이버공격 피해 사고·대응 현황과 보안관제 탐지 현황 등에 대한 정보를 본격 공유하였다.

공공분야에서 발생한 사이버공격 상황 파악 및 국가·공공기관의 사이버위기 대응 역량 강화를 위하여 2016년 6월 모든 중앙행정기관에 이 시스템을 연동하였으며, 2017년 7월부터

공공기관으로 확대하였다. 또한 2018년 2월 서울·경기도·강원도 3개 광역자치단체를 시작으로 지방자치단체 대상 정보공유시스템 연동을 착수하였다.

이와 더불어 사이버위협정보 공유의 실질적 내실화를 위하여 2017년 10월 국가안보실·국가정보원 등 주요 10개 기관이 참여하는 '정보공유 활성화 T/F'를 발족하여 민·관·군·금융 분야의 정보공유 활성화를 견인하고 있다.

정보공유시스템은 각급기관 간 사이버위협 정보를 안정적으로 공유하기 위하여 국가정보원을 중심으로 한 네트워크 체계를 갖추고 있으며, 지방 혁신도시 소재 공공기관의 정보공유시스템 연동을 위한 접근성 강화를 위하여 2019년 5월 광역자치단체와 공조하여 권역허브망을 구축하고 전국적인 네트워크 관리 체계 구성을 완료하였다.

이러한 네트워크 환경을 기반으로 국가정보원은 국가·공공기관 간 신속한 정보공유와 위협대응 역량을 강화하기 위하여 새로운 NCTI 구축에 착수, 2020년 2월 위협대응·예방보안·최신동향·통계 등의 다양한 정보를 지원하는 사이버정보 종합포털로 발돋움하였으며, 2022년 1월 침해지표 정보검색 서비스가 강화된 신NCTI를 공개하였다.

정보공유시스템은 2023년 1월 기준 326개 국가·공공기관·지방자치단체가 연동되어 있다. 2021년 약 10만 건, 2022년 약 11만 건의 사이버위협 정보를 공유하는 등 하루 평균 300건의 정보를 공유함으로써 국가 최대 정보공유 플랫폼의 역할을 수행하고 있다. 2023년은 기초지방자치단체를 대폭 확대하여 200개 이상 지방자치단체를 연동할 계획이다.

또한 국가정보원은 국가·공공기관과 실질적인 협력관계를 강화하고 정보공유시스템 사용자 의견 수렴 등 운영을 내실화하기 위하여 모든 이용기관 대상 간담회·워크숍을 해마다 개최하고, 강의·컨설팅 지원으로 정보공유 활성화에 박차를 가하고 있다.

한편 국가정보원은 방산업체·국가핵심기술 보유기업 등 국가안보 및 국익과 직결되는 산업분야의 사이버보안 강화를 위하여 인터넷 기반의 국가사이버위협 정보공유시스템(KCTI, Korea Cyber Threat Intelligence)을 구축하고, 2020년 10월부터 민간기업 대상 사이버위협정보공유 서비스를 시작하였다. 첫 대상으로 13개 주요 방산업체와 정보공유 협약을 체결하고 정보서비스를 진행하였고, 2022년 12월 기준으로 방위산업·핵심기술·제약바이오·에너지 등 153개 기업이 회원사로 가입되어 있다.

그림 3-1-2-2 국가사이버위협 정보공유시스템 구축 배경 및 운영근거

제3절 보안관리컨설팅 및 관리실태 평가

국가정보원은 「국가정보원법」 제4조 및 「사이버안보 업무규정」 제9조, 「전자정부법」 제56조 및 시행령 제70조, 「공공기록물 관리법 시행령」 제5조, 「국가정보보안기본지침」 제97조 등에 따라 국가·공공기관 정보통신망을 대상으로 보안관리컨설팅(이하 '보안컨설팅')을 실시하여 보안 취약요인을 발굴하고 각 기관이 보안대책을 수립할 수 있도록 컨설팅을 실시하고 있다. 또한 중앙행정기관 등은 「사이버안보 업무규정」 제12조에 따라 해당 기관에 대한 사이버공격·위협에 대한 예방 및 대응에 필요한 진단·점검을 연 1회 이상 실시하여야 한다.

국가정보원이 실시하는 보안컨설팅은 현장 점검과 원격 점검의 융합 방식으로 진행된다. 현장 점검은 전문요원이 대상 기관을 직접 방문하여 기관이 운영하는 정보통신망 및 보안장비 등 전반적인 시스템의 구성·운영현황을 파악하고 데이터 보호·시스템 접근통제 등 보안체계를 확인한다. 또한 인터넷 등 외부 접점을 통한 내부망으로의 침투 가능성, 비인가자에 의한 시스템 무단 접속 및 주요 데이터 유출 위험성 등을 중점 점검한다.

원격 점검은 기관의 대표 홈페이지 등 인터넷을 통하여 접근 가능한 시스템에 대하여 원격지에서 컨설팅을 실시한다. 실제 공격자가 관리자 권한 탈취·데이터 절취 등 시스템에 침투하는 방법과 동일한 방식으로 모의 공격을 실시하여 취약요인을 확인한다.

현장 점검 및 원격 점검을 실시한 후에는 시스템에 내재된 취약점을 파악하여 해당 기관이 보안대책을 수립하고 조치할 수 있도록 맞춤형 컨설팅을 실시하고 있다.

보안컨설팅은 각 기관으로부터 희망 의사를 파악한 후 대상 기관을 선정하고 상호 협의하여 컨설팅 대상 및 일정 등을 확정한다. 컨설팅 절차는 현황 분석, 취약점 진단, 결과 분석 및 보안대책 수립·권고 등 4단계로 이루어진다.

표 3-1-3-1 보안컨설팅 절차와 주요 내용

단 계	주요 내용
현황 분석	컨설팅 대상 정보통신망 구성·운영현황 등 파악 및 보안 체계 분석
취약점 진단	모의 공격으로 인터넷을 통한 내부망 침투 가능성, 비인가자의 시스템 무단 접속 및 데이터 유출 위험성 등 취약요소 중점 점검
결과 분석	진단 결과 확인된 취약요인 분석 및 위험도 평가
보안대책 수립·권고	취약요인별 보안대책 수립 권고 등 컨설팅 결과 통보

2022년에도 대국민 서비스를 제공하는 국가·공공기관 시스템과 외교·안보기관, 국가핵심기술 보유기관 중심으로 보안컨설팅을 실시하였다. 확인된 주요 보안 취약점으로는 여전히 망분리(업무망·인터넷망 등) 기관에서 시스템 정책설정 및 네트워크 구성 오류 등으로 발생한 망간 접점이었으며, 이로 인하여 업무망으로의 해킹 가능성이 우려되었다. 신속한 조치가 필요한 사항은 현장 기술지원으로 취약점을 제거하였으며, 보안장비 설치 등 시스템에 대한 개선·보완이 필요한 사항은 조속히 보안대책을 마련하여 이행하도록 권고하였다.

국가정보원은 중앙행정기관·광역자치단체·공공기관 대상 사이버공격·위협에 대한 예방·대응을 위하여 체계적인 정보보안 업무 수행 여부 등 '정보보안 관리실태'를 평가하고 있다. 「국가정보원법」 제4조 및 「사이버안보 업무규정」 제13조, 「전자정부법」 제56조, 「공공기록물 관리법 시행령」 제5조, 「국가정보보안기본지침」 제98~101조 등을 업무수행 근거로 하고 있다. 2006년 중앙행정기관을 시작으로 2007년 광역자치단체, 2009년 공공기관으로 평가 대상을 확대하였으며, 2022년에는 중앙행정기관(46개), 광역자치단체(17개), 공공기관(130개) 총 193개 기관을 평가하였다.

국가정보원은 정보보안 환경 변화, 최신 사이버위협 등을 반영하여 해마다 평가 지표를 수정·보완하고 있으며, 평가 시행을 위한 항목·절차·시기 등을 해당기관에 미리 통보한다.

그림 3-1-3-2 정보보안 관리실태 평가 절차

평가 절차는 5단계로 이루어져 있는데, 우선 평가 대상으로 선정된 기관은 평가 지표를 참조하여 정해진 기간 동안 평가 항목별로 자체 평가를 실시한다. 국가정보원은 기관 자체 평가에 대한 객관성·적절성을 확인하기 위하여 해당 기관을 방문하여 자체 평가 결과를 검증한다. 이 때 검증에 대한 공정성과 객관성을 담보하기 위하여 현장 실사에 학·연 전문가를 함께 참여시킬 수 있으며, 해당 기관의 장에게 자체 평가에 대한 증빙자료 제출, 담당자 면담 등 협조를 요청할 수 있다. 현장실사 종료 후 각 기관은 추가 증빙자료를 통하여 이의신청을 할 수 있으며, 국가정보원은 합동 검증에서 이의신청 내용에 대한 평가 반영 여부를 검토한다.

이후 학·연 전문가로 구성된 '정보보안 관리실태 평가위원회'를 개최하여 평가 결과에 대한 적정성을 검토·확인하고 최종 평가결과를 대상 기관에 통보하며, 해당 기관은 평가 결과를 자체 정보보안 정책 수립 시 반영하고 미흡한 점을 개선·보완한다. 또한 평가 결과는 국가·공공기관 정부업무평가에 반영하도록 행정안전부와 기획재정부에 통보하고 국무조정실을 통하여 국무회의에 보고한다. 국가정보원은 평가 결과 공통적으로 드러난 보안 취약요인을 개선할 수 있도록 정보보안 정책 수립 시 반영하는 한편, 다음해 정보보안 관리실태 평가 시 개선 여부를 집중 점검한다.

제4절 보안적합성 검증

1. 개요

국가정보원은 국가·공공기관 정보통신망의 보안수준을 제고하고 외부로부터의 사이버 위협에 대응하기 위하여 「국가정보원법」 제4조 및 「사이버안보 업무규정」 제9조, 「전자정부법」 제56조 및 동법 시행령 제69조, 「국가정보보안기본지침」 제21조·제32조·제34~36조에 따라 국가·공공기관이 도입하는 정보보호시스템 등 IT제품의 보안기능에 대한 안전성을 검증하고 있다.

2001년 4월 K(K1~K7)등급 대상 이외 정보보호제품에 대하여 보안성 기능 검토를 시작하였으며, 2005년 1월 공통평가기준(CC, Common Criteria) 인증 획득 제품에 대하여 CC인증범위 이외 보안 및 암호 기능에 대한 보안성 검토를 실시하였다.

2006년 1월 정보보호제품에 대한 '보안성 검토'를 '보안적합성 검증'으로 명칭을 변경하였다. 2006년 8월 공공분야 도입 정보보호제품의 사전인증요건을 CC인증으로 지정하였으며, 2008년 도입 전 검증하던 CC인증제품의 검증 절차를 '도입 후 검증'으로 변경하였다. 2010년 7월 국내용 CC인증제품에 대하여 도입 후 검증을 생략하였으며, 2014년 10월 보안적합성 검증대상에 네트워크 장비를 추가하였다. 2016년 7월 도입 후 검증에 필요한 절차를 간소화하기 위하여 공인 시험기관이 '국가용 보안요구사항' 만족 여부를 시험하여 안전성을 확인하여 주는 '보안기능 시험결과서 발급' 제도를 실시하였다. 2019년 4월부터 네트워크 장비에 대한 안전성을 제고하기 위하여 발급기준과 필수 검증항목을 강화하고 보안위해 요소가 있는 하드웨어 검증을 추가하였다.

2020년 1월 '보안기능 시험결과서 발급'을 '보안기능 시험'제도로 명칭 변경하는 한편, 전산망 보안강화를 위하여 악성코드 유입·내부자료 유출방지에 중요 역할을 담당하는 제품에 대하여 '선검증 후도입'으로 전환을 공표하였다. 2020년에는 각급기관이 네트워크 장비·보안USB·가상화 관리 제품 3종, 2021년에는 네트워크 자료유출 방지제품·호스트 자료유출 방지제품, 2022년에는 망간자료 전송제품 순으로 전환되었다. 또한 각급기관이 정보보호제품을 용이하게 도입·운용할 수 있도록 정보공유시스템에'안전성 검증필 제품목록'을 게시함으로써 목록에 등재된 제품 도입 후 검증 절차를 거치지 않고 간소화하도록 제도를 개선하였다.

2020년 7월에는 보안기능이 미약한 제품(7종)에 대하여 검증 대상에서 제외됨을 공표하여 각급기관에서 이들 제품을 자유롭게 도입·운용할 수 있도록 하였다.

표 3-1-4-1 안전성 검증 없이 자율 도입·운영이 가능한 제품

순번	제품 유형	주요 기능
1	네트워크 기반 개인정보보호 제품	네트워크 기반 개인정보 검출
2	호스트 기반 개인정보보호 제품	호스트 기반 개인정보 검출
3	네트워크 취약점 점검 도구	네트워크 취약점 분석 및 보고
4	호스트 취약점 점검 도구	호스트 취약점 분석 및 보고
5	유해사이트 차단시스템	유해사이트 접속 차단
6	웹셸 탐지 제품	웹서버 내 웹셸 탐지 및 격리

또한 2020년 9월 GS인증 제도가 안전성 확인에 미흡한 부분이 있고, GS인증 신청 건수도 적어 2022년 1월부터 GS인증을 정보보호시스템 유형별 도입요건에서 제외됨을 공표하였다. 2020년 10월 다수 정보보호제품에서 더 이상 관리되지 않는 낮은 버전(2.X)의 리눅스 커널을 수정하여 탑재하고 있어 2023년부터 낮은 버전의 커널을 탑재한 제품의 신규 도입을 제한하기로 하였다.

2020년 1월 ▲국내용 CC인증제품 ▲국가용 보호프로파일(Protection Profile, PP)을 준수한 국제용 CC인증제품 ▲보안기능 확인서 발급 제품 ▲국가용 보안요구사항을 준수하여 성능평가 결과 확인서를 받은 제품 ▲국가용 보안요구사항을 준수하여 GS인증을 받은 제품을 수록한 '검증필 제품목록'을 정보공유시스템에 등재하였으며, 2021년 12월 국가사이버안보센터 홈페이지 개설과 함께 공개하였다.

2021년 6월 정부의 클라우드 보급촉진 기조에 맞추어 클라우드에서 운용되는 정보보호 제품에 대하여 2024년까지 검증을 유예하였으며, 2012년 12월 CC인증으로 일원화된 공공분야 도입 정보보호제품 24종의 사전인증요건을 'CC인증 또는 보안기능 확인서'로 확대하여 2022년 1월부터 적용하였다.

2022년 3월에는 국가·공공기관에서 운영 중인 IT보안제품의 보안 취약점이 확인된 경우 보안위협 확산을 방지하기 위하여 'IT보안제품 취약성 대응 체계'를 마련하여 공개하였다. IT보안제품에서 발견되는 취약점에 따라 4단계 절차로 구분하였으며, 취약점이 경미한

1·2단계는 도입기관과 공급업체에서 자율 보완하도록 하였고, 중대한 취약점이 발견된 3·4단계는 즉시 보완 또는 연동 배제하도록 하였다.

2022년 11월 보안적합성 검증정책의 효율성 제고와 규제 완화 차원에서 제도를 개선하였다. 3만여 개에 이르는 검증 대상기관을 중요도에 따라 가·나·다 그룹으로 편성하고, 그룹별로 도입기준을 차등 적용함으로써 주요 기관에 대한 보안수준을 유지하면서 그 밖의 기관에 대해서는 IT보안제품 도입에 최대한 자율성을 보장하였다.

아울러 국가 공급망 보안강화를 위하여 「국가정보원법」 제5조제1항에 의거, 모든 국가·공공기관에서는 국제사회의 제재를 받는 IT기업이 개발한 제품이 도입되지 않도록 유의할 것을 요청하였다.

표 3-1-4-2 그룹별 편성 기준 및 대상기관

그룹 명칭	편성 대상
가	▲중앙행정기관 ▲국방부 소속·산하기관[1] ▲경찰청·해양경찰청 산하 경찰청·경찰서 ▲검찰청 및 지방검찰청 ▲각 교육청 ▲주요 공공기관[2] ▲주요정보통신기반시설관리기관 ▲광역지방자체단체 ▲국가보안시설[3]의 감독기관 ▲기타 관계 중앙행정기관이 편성을 요청한 소속·산하기관 등
나	▲중앙행정기관의 소속·산하기관(예: 각 지역의 인권사무소·고용노동청·세무서·국립과학관·119구조대·연구소(원)·우체국 등) ▲각 지구대 또는 파출소 ▲기타 공공기관[4] ▲각 교육지원청 ▲지방자체단체 소속기관 중 상·하수도 운영 기관 ▲각급 대학교
다	▲중앙행정기관 산하 위원회 ▲기초지방자치단체 ▲기초지방자치단체의 산하기관·지방공기업[5] ▲각급학교(국·공립 초·중·고등학교) 등

1) 「국군조직법」(법률 제10821호, 2011. 7. 14.)과 「국군조직법」 제9조제3항에 따른 전투를 주 임무로 하는 각 군의 작전부대 등에 관한 규정(대통령령 제32560호, 2020. 4. 1.)에 의하여 설치된 각 군 및 각 부대 등은 제외

2) '주요 공공기관'이란 「공공기관의 운영에 관한 법률」(법률 제18795호, 2022. 2. 3.) 제48조에 의하여 기획재정부장관이 경영실적을 평가하는 공공기관(공기업·준정부기관)

3) '국가보안시설'이란 「보안업무규정」(대통령령 제31354호, 2020. 12. 31.) 제32조에 의하여 국가정보원장이 지정한 시설

4) '기타 공공기관'이란 '가'그룹에 속하지 않는 나머지 공공기관

5) '지방공기업'이란 「지방공기업법」(법률 제18747호, 2022. 1. 11.) 제2조에 따라 지방자치단체가 직접 설치·경영하는 지방직영기업·지방공사·지방공단

2. 도입 후 검증 절차

정보보호시스템 및 네트워크 장비 등 보안기능이 있는 정보통신기기를 도입하는 국가·공공기관은 도입 대상제품이 CC인증, 보안기능 확인서 등 사전 도입 요건을 만족하였는지를 확인한 후 검증이 필요한 제품에 대하여 국가정보원에 보안적합성 검증을 신청한다. 국가정보원은 국가보안기술연구소를 통하여 보안기능을 검증하고, 그 결과를 신청기관에 통보한다. 신청기관은 검증과정에서 발견된 취약점에 대한 개선 및 보안대책을 적용하고 미비점을 보완한 후 제품을 운용한다. 국가사이버안보센터 홈페이지에 등재된 검증필 제품목록에 수록된 제품은 도입 후 보안적합성 검증 신청을 생략하고 운용 점검사항과 도입확인서, 인증서 사본 등을 제출하여 운용할 수 있다.

3. 그룹별 IT보안제품 도입기준

가. '가'그룹에 편성된 기관의 도입기준 제품

'가'그룹에 편성된 기관은 보안적합성 검증 체계 개편 이전과 동일한 정책이 적용된다.

IT보안제품 중 침입차단시스템·침입방지시스템 등 16종은 보안기능 확인서 또는 국내외 CC인증을 획득한 제품을 도입하여야 하며, 가상사설망·통합인증제품(SSO) 등 4종은 사전인증요건에 더하여 국가정보원장이 검증한 '검증필 암호모듈'이 탑재되어야 한다.

검증필 제품목록에 등재된 제품은 보안적합성 검증 신청 절차를 생략하여 도입하고 운용할 수 있다. 디지털 복합기를 제외하고 CC인증을 받았지만, 검증필 제품목록에 등재되지 않은 제품은 도입 후 보안적합성 검증 신청을 하여야 한다.

표 3-1-4-3 '가'그룹 편성기관의 주요 IT보안제품 사전인증요건

범례 ❶ 보안기능 시험제도(보안기능 확인서) ❷ CC인증제도(CC인증서) ❸ 성능평가제 ❹ 암호모듈검증제도

연번	제품군	제품 유형	사전인증요건
1	침입차단 제품군	침입차단시스템(FW)	❶·❷ 중 어느 하나
2		침입차단시스템(FW+VPN)	❶·❷ 중 어느 하나, 그리고 ❹
3		웹 방화벽	❶·❷ 중 어느 하나
4		DDoS 대응장비	❶·❷·❸ 중 어느 하나
5		인터넷 전화 보안제품	❶·❷ 중 어느 하나
6		침입차단제품군 기타	❶·❷ 중 어느 하나 (미발급제품은 도입 후 검증신청)
7	침입방지 제품군	침입방지시스템(IPS)	❶·❷ 중 어느 하나
8		침입방지시스템(IPS+VPN)	❶·❷중 어느 하나, 그리고 ❹
9		무선침입방지제품	❶·❷ 중 어느 하나
10		침입방지제품군 기타	❶·❷ 중 어느 하나 (미발급제품은 도입 후 검증신청)
11	구간보안 제품군	가상사설망(VPN)	❶·❷ 중 어느 하나, 그리고 ❹
12		네트워크 접근통제	❶·❷ 중 어느 하나
13		망간자료전송제품	❶
14		무선랜 인증제품	❶·❷ 중 어느 하나
15		구간암호화제품	❹(❶+❹ 권고)
16		구간보안제품군 기타	❶·❷ 중 어느 하나 (미발급제품은 도입 후 검증신청)
17	전송자료보안 제품군	스팸메일 차단시스템	❶·❷중 어느 하나
18		네트워크자료유출방지제품	❶
		소프트웨어 보안USB제품	❶ 그리고 ❹
19		호스트자료유출방지제품	❶
20		메일암호화제품	❹(❶+❹ 권고)
21		전송자료보안제품군 기타	❶·❷ 중 어느 하나 (미발급제품은 도입 후 검증신청)

연번	제품군	제품 유형	사전인증요건
22	보안관리 제품군	스마트카드	❶·❷ 중 어느 하나
23		통합보안 관리제품	❶·❷ 중 어느 하나
24		소스코드 보안약점 분석도구	❶·❷·❸ 중 어느 하나
25		패치관리시스템	❶·❷ 중 어느 하나
26		데이터베이스 접근통제제품	❶·❷ 중 어느 하나
27		통합인증제품	❶·❷ 중 어느 하나, 그리고 ❹
28		보안관리제품군 기타	❶·❷ 중 어느 하나 (미발급제품은 도입 후 검증신청)
29	가상화제품군	가상화관리제품	❶
30		가상화제품군 기타	❶·❷ 중 어느 하나 (미발급제품은 도입 후 검증신청)
31	엔트포인트 보안제품군	디지털복합기	❷(별도 검증신청 불요)
32		안티바이러스제품(Windows)	❶·❷·❸ 중 어느 하나
33		안티바이러스제품(Linux·Mobile)	❸
34		스마트폰 보안관리제품	❶·❷ 중 어느 하나
35		운영체제(서버) 접근통제제품	❶·❷ 중 어느 하나
36		문서암호화제품(DRM)	❶·❷ 중 어느 하나, 그리고 ❹
37		DB암호화제품	❶·❷ 중 어느 하나, 그리고 ❹
38		엔드포인트보안제품군 기타	❶·❷중 어느 하나 (미발급제품은 도입 후 검증신청)
39	네트워크 장비	L3·L4·L7 스위치	❶
40		라우터	❶
41		SDN 컨트롤러	❶
42		SDN 스위치	❶
43		L2 보안시스템	❶
44		네트워크 장비 기타	❶

나. '나'그룹에 편성된 기관의 도입기준 제품

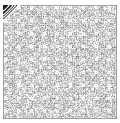
'가'그룹의 요건인 ▲보안기능 확인서 ▲CC인증서뿐 아니라 성능평가의 인정범위가 모든 제품유형으로 확대되며, '신속확인서'가 ▲신기술·신종제품의 사전인증요건으로 추가된다. '나'그룹에 편성된 기관의 사전인증요건은 [표 3-1-4-4]와 같으나 완화가 가능하다. 예를 들어 국내 시험(평가)기관에서 시험·CC평가·신속확인이 진행 중(계약체결)인 제품을 도입하거나 국내외 암호모듈 검증기준을 준수한 암호모듈을 탑재한 경우를 의미한다.

또한 '나' 그룹에 편성된 기관이 도입하려는 ▲보안기능 확인서 ▲CC인증서 ▲성능평가 ▲신속확인서 중 어느 하나만 획득하더라도 보안적합성 검증을 생략하고 곧바로 운용할 수 있다.

표 3-1-4-4 '나'그룹 편성기관의 주요 IT보안제품 사전인증요건

범례 ❶ 보안기능 시험제도(보안기능 확인서) ❷ CC인증제도(CC인증서) ❸ 성능평가제 ❹ 암호모듈검증제도 ❺ 신속확인제도

연번	제품군	제품 유형	사전인증요건
1	침입차단 제품군	침입차단시스템(FW)	❶·❷·❸ 중 어느 하나
2		침입차단시스템(FW+VPN)	❶·❷·❸ 중 어느 하나, 그리고 ❹
3		웹 방화벽	❶·❷·❸ 중 어느 하나
4		DDoS 대응장비	❶·❷·❸ 중 어느 하나
5		인터넷 전화 보안제품	❶·❷ 중 어느 하나
6		침입차단제품군 기타	❶·❷·❺ 중 어느 하나 (미발급제품은 도입 후 검증신청)
7	침입방지 제품군	침입방지시스템(IPS)	❶·❷·❸ 중 어느 하나
8		침입방지시스템(IPS+VPN)	❶·❷·❸ 중 어느 하나, 그리고 ❹
9		무선침입방지제품	❶·❷ 중 어느 하나
10		침입방지제품군 기타	❶·❷·❺ 중 어느 하나 (미발급제품은 도입 후 검증신청)
11	구간보안 제품군	가상사설망(VPN)	❶·❷·❸ 중 어느 하나, 그리고 ❹
12		네트워크 접근통제	❶·❷ 중 어느 하나
13		망간자료전송제품	❶·❷ 중 어느 하나
14		무선랜 인증제품	❶·❷ 중 어느 하나
15		구간암호화제품	❹(❶+❹ 권고)
16		구간보안제품군 기타	❶·❷·❺ 중 어느 하나 (미발급제품은 도입 후 검증신청)



연번	제품군	제품 유형	사전인증요건
17	전송자료보안 제품군	스팸메일 차단시스템	❶·❷ 중 어느 하나
18		네트워크자료유출방지제품	❶·❷ 중 어느 하나
		소프트웨어 보안USB제품	❶·❷ 중 어느 하나, 그리고 ❹
19		호스트자료유출방지제품	❶·❷ 중 어느 하나, 그리고 ❹
20		메일암호화제품	❹(❶+❹ 권고)
21		전송자료보안제품군 기타	❶·❷·❺ 중 어느 하나 (미발급제품은 도입 후 검증신청)
22	보안관리 제품군	스마트카드	❶·❷ 중 어느 하나
23		통합보안 관리제품	❶·❷ 중 어느 하나
24		소스코드 보안약점 분석도구	❶·❷·❸ 중 어느 하나
25		패치관리시스템	❶·❷ 중 어느 하나
26		데이터베이스 접근통제제품	❶·❷ 중 어느 하나
27		통합인증제품	❶·❷ 중 어느 하나, 그리고 ❹
28		보안관리제품군 기타	❶·❷·❺ 중 어느 하나 (미발급제품은 도입 후 검증신청)
29	가상화제품군	가상화관리제품	❶·❷ 중 어느 하나
30		가상화제품군 기타	❶·❷·❺ 중 어느 하나 (미발급제품은 도입 후 검증신청)
31	엔트포인트 보안제품군	디지털복합기	❷(별도 검증신청 불요)
32		안티바이러스제품(Windows)	❶·❷·❸ 중 어느 하나
33		안티바이러스제품(Linux·Mobile)	❶·❷·❸ 중 어느 하나
34		스마트폰 보안관리제품	❶·❷ 중 어느 하나
35		운영체제(서버) 접근통제제품	❶·❷ 중 어느 하나
36		문서암호화제품(DRM)	❶·❷ 중 어느 하나, 그리고 ❹
37		DB암호화제품	❶·❷ 중 어느 하나, 그리고 ❹
38		엔드포인트보안제품군 기타	❶·❷·❺ 중 어느 하나 (미발급제품은 도입 후 검증신청)
39	네트워크 장비	L3·L4·L7 스위치	❶·❷ 중 어느 하나
40		라우터	❶·❷ 중 어느 하나
41		SDN 컨트롤러	❶·❷ 중 어느 하나
42		SDN 스위치	❶·❷ 중 어느 하나
43		L2 보안시스템	❶·❷ 중 어느 하나
44		네트워크 장비 기타	❶·❷ 중 어느 하나

* 성능평가로 도입가능한 제품은 KISA의 성능평가제도 운영정책에 따라 확대 또는 축소될 수 있음.

다. '다' 그룹에 편성된 기관의 도입기준 제품

'다'그룹 편성기관은 제품유형을 불문하고 자체 판단, 상위 그룹의 도입기준뿐 아니라 GS인증 등 사전인증요건을 자율지정, 도입할 수 있다. 또한 자체 판단에 따라 보안적합성 검증을 생략할 수 있다.

라. 공공기관 도입 영상보안장비 보안 준수

국가·공공기관에서는 2018년부터 영상정보 처리기기(시설보안 및 관리를 위한 IP기반 CCTV, NVR 등) 도입 시 보안기능에 대한 안전성을 확인하기 위하여 '공공기관용 보안 성능 품질 TTA Verified Ver. 1' 인증을 획득한 제품을 사용하여야 한다. 또한 국가정보원이 공개한 '국가·공공기관 영상정보 처리기기 도입·운영 가이드라인(2019년)'에 따라 보안위협을 확인하고 적절한 보안대책을 준수하도록 하였다.

제5절 암호모듈 검증

1. 개 요

국가정보원은 「사이버안보 업무규정」 제9조제2항·제3항, 「전자정부법」제56조 및 동법 시행령 제69조, 「암호모듈 시험 및 검증지침」에 따라 국가정보통신망에서 소통·저장되는 비밀이 업무자료 보호를 위하여 사용하도록 암호모듈의 안전성과 구현 적합성을 검증하고 있다.

검증대상 암호모듈은 검증대상 암호알고리즘을 포함하여 소프트웨어·펌웨어·하드웨어 또는 이들을 조합한 형태로 구현한 것으로, 암호모듈 보안요구사항(KS X ISO/IEC 19790:2015)을 준수하여야 한다. 한편 암호모듈 보안요구사항 적합 여부는 암호모듈 시험요구사항(KS X ISO/IEC 24759:2015)을 이용하여 시험한다.

암호모듈 검증은 2005년부터 시행하였으며, 2015년 암호모듈 보안요구사항과 시험요구사항을 개정하고 2016년 6월부터 개정된 표준을 적용하여 암호모듈 검증을 수행하고 있다. 2018년 한국인터넷진흥원이 암호모듈 시험기관으로 추가 지정되어 현재 국가보안기술연구소와

한국인터넷진흥원, 2개 기관이 암호모듈 시험업무를 수행하고 있다.

국가정보원은 사이버안보센터 '암호모듈 검증' 홈페이지를 신규 개설하여 ▲제도 소개 ▲암호모듈 시험·검증절차 상세 설명 ▲자주 묻는 질문 메뉴를 신설하여 제도 운영의 투명성과 소통을 강화하였다. 또한 난수발생기 신규 시험방법론을 개발하고, TTAK.KO-12.0235(운영체제별 잡음원 수집 및 응용지침) 및 TTAK.KO-12.0341(소프트웨어 암호모듈에 사용되는 잡음원 시험평가 지침) 시험 방법론에 대한 표준을 개선하였다. 이에 난수발생기 신규 시험기술을 2022년 6월 1일자로 의무 적용하도록 하여 업체의 암호모듈 구현 용이성과 암호모듈의 안전성을 제고하였다. 또한 2023년 3월 9일자로 '암호모듈 시험 및 검증지침'을 개정하여 기존 공공 중심의 암호모듈 시험 체계를 민간으로 단계적 전환하기 위한 기반을 마련하였다. 개정된 지침에는 민간시험기관의 지정 요건, 선정 절차와 관리 체계 등 민간 시험 체계와 관련된 내용이 포함되어 있다.

한편 한국인터넷진흥원과 협조하여 암호관련 업계와 대학원(생)을 대상으로 암호모듈 전문교육 교육과정을 운영 중이다. 2022년에는 기초 암호수학, 암호알고리즘, 암호모듈 검증기준 해설 및 가이드라인 소개 등을 교육하였다. 암호모듈 전문교육에는 약 200여 명이 온라인으로 수강하였으며, 이와 더불어 5개 영세·중소업체를 대상으로 컨설팅 지원사업으로 암호모듈 검증기준 해석 교육 및 제출물 검토 등으로 업체에서 암호모듈 시험신청 시 제출 문서(기본 및 상세설계서, 시험절차 및 결과서, 형상관리문서)를 작성·보완할 수 있도록 지원하였다.

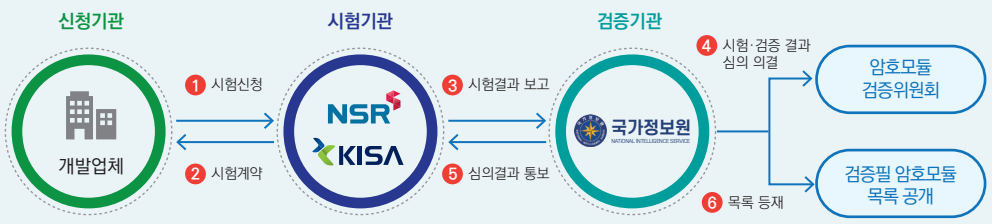
또한 국가정보원은 암호모듈 검증에 대한 진입장벽을 낮추기 위하여 3개의 가이드라인을 공개하였다. 3월에 공개한 '암호모듈 운용가이드'에는 실제 암호모듈을 사용하는 국가·공공기관 정보보안 담당자를 대상으로 암호모듈을 도입하고 운용할 때 필요한 정보가 체크리스트 형태로 수록되었다. 5월에 공개한 '암호모듈 구현가이드'는 암호모듈을 개발하는 개발자를 위한 가이드라인으로 암호모듈을 안전하게 구현하기 위한 방법 등이 수록되어 있다. 8월에 공개한 '암호모듈 제출물 작성 안내서'는 암호모듈 응시자를 대상으로 신청 제출 서류와 작성 방법 등을 자세히 명시하였으며, 이 안내서에 따라 신청하면 시험 기간이 단축될 것으로 기대된다.

2. 검증 체계 및 절차

가. 암호모듈 검증 체계

암호모듈 검증 체계는 역할과 책임에 따라 검증기관과 시험기관으로 구분된다. 국가정보원은 검증기관으로서 암호모듈 검증정책 수립 및 시행, 검증기준 개발 및 시험기술 승인, 시험기관의 지정·관리·감독 및 시험결과 검증, 암호모듈 검증위원회 개최, 검증필 암호모듈 목록 관리 등을 수행하고 있다. 국가보안기술연구소와 한국인터넷진흥원은 시험기관으로서 암호모듈 시험계약 체결 및 시험, 암호모듈 시험 관련 기준·기술 연구개발, 교육·컨설팅 등과 더불어 민간시험 체계와 관련하여 검증기관의 일부 업무를 지원하고 있다.

그림 3-1-5-1 암호모듈 시험·검증 체계



❶ 신청기관은 암호모듈의 적절한 보안수준을 결정한 후 시험기관에 시험 신청
❷ 시험기관은 신청서와 제출물을 검토한 후 신청기관과 시험계약을 체결하고, 암호모듈 검증 기준에 따라 시험 수행
❸ 시험기관은 시험을 완료한 후 검증기관에 시험결과 보고
❹ 검증기관은 암호모듈 시험결과를 검토하여 검증기준에 부합하는지를 확인하고 암호모듈 검증위원회에서 시험·검증결과의 타당성과 공정성 심의
※ 검증위원회는 관·학·연 전문가로 구성
❺ 검증기관은 암호모듈 심의결과를 시험기관에 통보
❻ 검증기관은 심의가 완료된 암호모듈을 검증필 암호모듈 목록에 등재

나. 암호모듈 검증 절차

그림 3-1-5-2 암호모듈 시험·검증 절차

❶ 시험기관은 검증기준에 따라 검증대상 암호모듈을 시험하며, 제출물의 수정사항 발견 시 신청기관에 보완 요청

❷ 신청기관은 시험기관의 보완 요청에 따라 제출물을 보완하여 시험기관에 제출

❸ 시험기관은 시험을 완료한 후 검증기관에 시험결과를 보고하며, 검증기관은 시험결과가 검증기준에 부합하는지 검토

❹ 검증기관은 관·학·연 전문가로 구성된 암호모듈 검증위원회에서 시험·검증결과의 타당성·공정성에 대한 심의·의결을 수행하고 시험기관에 심의 결과 통보

❺ 검증기관은 심의가 완료된 암호모듈에 검증번호를 부여하고 검증필 암호모듈 목록에 등재

※ 시험기관은 원활한 시험 수행과 제출물의 이해를 위하여 신청기관에게 시험환경 지원과 설명회 개최 요청 가능

※ 시험기관은 신청기관이 특별한 사유 없이 제출물 보완을 지연하는 등 시험을 계속 진행할 수 없다고 판단하는 경우 시험계약 중지 가능

※ 시험기관은 신청기관의 암호모듈 개발 환경 보안관리 실태를 점검하는 권한 보유

암호모듈 검증 절차인 예비검토 단계, 사전검토 단계, 암호모듈 시험 단계, 암호모듈 검증 단계에 대한 세부사항 및 행정 절차는 [표 3-1-5-1]과 같다.

표 3-1-5-1 암호모듈 검증절차 세부사항

단계	진행 과정
시험문의	• 신청기관은 시험기관에 암호모듈 시험신청 방법, 소요기간, 제출물 작성 방법 등을 유선 또는 이메일로 문의 • 시험기관은 유선이나 이메일로 답변하며, 필요 시 오프라인 설명 요청 가능
↓	
❶ 예비검토	• 신청기관은 아래의 제출물을 준비하여 시험기관에 예비검토 요청 ※ 제출물 : 기본 및 상세설계서, 형상관리문서, 시험서(자체 시험결과서) 등 • 시험기관은 제출물을 검토하고 예비검토 설명회 요청 • 시험기관은 제출물의 완성도가 높은 경우 예비검토 완료
↓	
공문접수	• 신청기관은 예비검토 완료 후 공문 및 시험신청서와 제출물을 준비하여 시험기관에 시험 신청 ※ 제출물 : 암호모듈 구현물 일체, 암호모듈 소스코드, 기본 및 상세설계서, 형상관리문서, 시험서(자체 시험결과서), 테스트 프로그램 등
↓	
❷ 사전검토	• 시험기관은 암호알고리즘 구현 적합성 → 엔트로피 → 취약점 점검 등의 자동화 시험 진행 • 시험기관은 자동화 시험 완료 후 순차적으로 시험자 배정 • 시험기관은 제출물의 완성도가 높은 경우 사전검토 완료
↓	
시험계약	• 시험기관은 제출물의 타당성과 일관성을 검토한 후 시험 종료 가능 여부를 판단하고 신청기관과 시험계약 체결
↓	
❸ 시험	• 시험기관은 검증기준 만족 여부를 시험하며, 필요 시 신청기관에 제출물과 소스코드 수정 요청 ※ 제출물: 수정된 문서, 소스코드, 동작시험을 위한 시험환경 등 • 시험기관은 신청기관 개발환경 보안점검 수행 • 시험기관은 암호모듈 시험결과보고서 작성
↓	
❹ 검증	• 검증기관은 시험결과가 검증기준에 부합한지 검토한 후 암호모듈 검증위원회에서 시험 결과의 타당성·공정성에 대한 심의·의결 • 검증기관은 심의가 완료된 암호모듈을 검증필 목록에 등재

다. 검증효력 만료 도래 시 및 형상 변경 시 조치사항

그림 3-1-5-3 검증효력 만료 도래 시 및 형상 변경 시 조치사항

❶ 검증필 암호모듈의 검증효력 만료일이 도래하거나 암호모듈의 형상이 변경될 경우 신청기관은 재검증신청서와 제출물을 준비하여 시험기관에 재검증 신청

❷ 시험기관은 검증기준에 따라 검증대상 암호모듈을 시험하며, 제출물의 수정사항 발견 시 신청기관에 보완 요청

❸ 신청기관은 시험기관의 보완 요청에 따라 제출물을 보완하여 시험기관에 제출

❹ 시험기관은 시험을 완료한 후 검증기관에 시험결과를 보고하며, 검증기관은 시험결과가 검증기준에 부합하는지 검토

❺ 검증기관은 시험 · 검증결과의 타당성 · 공정성에 대한 심의를 수행하고, 시험기관에 심의 결과 통보

❻ 검증기관은 재검증 심의가 완료된 암호모듈의 검증번호를 갱신(또는 유지)하고 검증필 암호모듈 목록 갱신

※ 시험기관은 원활한 시험 수행과 제출물의 이해를 위하여 신청기관에 시험환경 지원과 설명회 개최 요청 가능

※ 시험기관은 재검증 신청기관의 암호모듈 개발 환경 보안관리 실태 점검 가능

※ 시험기관은 재검증 신청기관이 특별한 사유 없이 제출물 보완을 지연하는 등 시험을 계속 진행할 수 없다고 판단하는 경우 시험계약 중지 권한 보유

※ 신청기관은 암호모듈 검증효력을 연장하기 위하여 재검증을 신청할 경우 검증효력 만료 6개월 이전에 신청

※ 검증필 암호모듈에 심각한 취약성이 발견된 경우 시험기관의 요청에 의하여 재검증이 수행될 수 있으며, 이 때 신청기관은 해당 취약점을 도입기관에 즉시 고지하여야 하고, 취약점이 보완될 때까지 암호모듈 검증효력 중지 가능

※ 시험기관은 암호모듈 형상 변경이 일정 범위를 벗어나거나 운영환경 등 그 밖의 상황에 따라 재검증 시험으로는 안전성 제공이 어렵다고 판단될 경우 신규 시험으로 처리 가능

※ 암호모듈 형상 변경 범위에 따라 검증효력 유효기간 연장 여부가 결정되며, 그 밖의 자세한 사항은 '암호모듈 시험 및 검증지침(2023. 3. 9.)' 참고 권장

※ 시험기관은 재검증 과정에서 암호알고리즘 구현 적합성 점검을 위한 자동화 시험 결과를 신청기관에 요청 가능

3. 검증대상 암호알고리즘

검증기관은 안전성(보안강도), 효율성, 표준화 동향, 국내외 암호사용 정책, 상호 호환성 및 지식재산권 등을 고려하여 검증대상 암호알고리즘을 선정하고 있다. 검증대상 암호알고리즘은 블록암호, 해시함수, 메시지인증코드, 난수발생기, 키 설정방식, 공개키 암호, 전자서명, 키 유도 등 8종 23개로 분류되며, 112비트 이상의 보안강도를 만족하여야 한다.

그림 3-1-5-4 검증대상 암호알고리즘

표 3-1-5-2 검증대상 암호알고리즘

분류		암호알고리즘
블록암호 및 운영모드		ARIA, SEED, LEA, HIGHT(키 길이 112비트 이상)
		ECB, CBC, OFB, CFB, CTR, CCM, GCM
해시함수		SHA-2(SHA-224/256/384/512), SHA-3(SHA3-224/256/384/512), LSH(LSH-224/256/384/512/512-224/512-256)
메시지 인증코드	해시함수 기반	HMAC
	블록암호 기반	GMAC, CMAC
난수 발생기	해시·HMAC 기반	Hash_DRBG, HMAC_DRBG
	블록암호 기반	CTR_DRBG
공개키암호		RSAES(공개키 길이 : 2048/3072, 해시함수 : SHA-224/256)
전자서명		RSA-PSS(공개키 길이 : 2048/3072, 해시함수 : SHA-224/256) KCDSA(공개키 길이 : 2048, 개인키 길이 : 224/256, 해시함수 : SHA-224/256) EC-KCDSA(P-224, P-256, B-233, B-283, K-233, K-283, 해시함수 : SHA-224/256) ECDSA(P-224, P-256, B-233, B-283, K-233, K-283, 해시함수 : SHA-224/256)
키 설정		DH(공개키 길이 : 2048/3072, 개인키 길이 : 224/256) ECDH(P-224, P-256, B-233, B-283, K-233, K-283)
키 유도		KBKDF(HMAC, CMAC) PBKDF(HMAC)

4. 검증필 암호모듈 현황

검증필 암호모듈 목록은 국가사이버안보센터 홈페이지(https://www.ncsc.go.kr:4018/PageLink.do)에서 확인할 수 있으며, 목록에는 암호모듈의 명칭, 모듈 형태, 검증일, 효력 만료일, 보안수준, 보안정책 문서 및 형상 데이터 정보 등이 포함되어 있다. 2005년부터 2022년 12월까지 총 333개 암호모듈을 검증 완료하였고, 국가·공공기관은 검증필 암호모듈 목록에 등재된 암호모듈 중 효력이 유효한 소프트웨어 68개, 펌웨어 13개, 하이브리드 펌웨어 1개, 하드웨어 8개 등 총 90개 암호모듈을 도입할 수 있다.

표 3-1-5-3 검증필 암호모듈 현황

(단위: 건)

구 분		2016	2017	2018	2019	2020	2021	2022	합계
합 계		23	19	22	25	27	29	24	169
시험 유형	신 규	7	5	9	9	13	14	15	72
	재검증	16	14	13	16	14	15	9	97

제6절 정보보호제품 평가·인증

1. 개요

정보보호제품 평가·인증제도는 「지능정보화기본법」 제58조 및 동법 시행령 제51조, 「정보보호 시스템 평가·인증 등에 관한 고시」(과학기술정보통신부 고시)에 근거하여 과학기술정보통신부장관이 고시한 기준의 부합 여부를 확인하는 제도이다.

1998년 국가안전기획부(현재의 국가정보원)가 국내 실정에 적합한 평가기준(K 기준)을 개발·고시함으로써 본격적인 평가·인증제도를 시작하였으며, 1998년 침입차단시스템, 2000년 침입탐지시스템, 2002년 가상사설망, 2003년 운영체제보안시스템·지문인식 시스템·스마트카드로 평가·인증 대상을 확대하였다. 2005년 평가기준을 CC로 일원화하고 평가·인증 대상을 모든 정보보호제품으로 확대함으로써 제품의 다기능화 및 통합화 추세에 대응하였고, 2006년 K제도를 폐지하였다.

2007년 국제용으로 운영하던 CC 기반의 평가·인증제도를 국제용과 국내용으로 이원화함으로써 평가기간을 단축하여 중소 정보보호업체의 경제적 부담을 대폭 완화하고 정보보호제품을 적시에 공급할 수 있는 체계를 구축하였다. 2010년 국내용 평가·인증제도를 정비하여 평가를 간소화함으로써 중소업체의 부담을 더욱 경감하였다.

2011년 평가·인증대상을 26종으로 선정하였고, 2012년 2월부터 평가·인증제품의 품질을 더욱 향상시키기 위하여 국내용 정보보호제품 보안요구사항을 발간하였으며, 인증제품의 보안성을 향상하기 위하여 인증서 유효기간제(3년)를 신설하였다. 2012년 11월 국가사이버안전센터 산하 IT보안인증사무국을 국가보안기술연구소로 이관하였다. 2013년 스마트폰 보안관리제품과 소스코드 보안약점 분석도구의 보안요구사항을 개발하여 국가·공공기관용 평가·인증대상을 28종으로 확대하였다.

2014년 10월 당시 미래창조과학부는 국가정보원으로부터 CC인증 정책업무를 이관받았다. 국가정보원, 미래창조과학부, 국가보안기술연구소 IT보안인증사무국은 2016년 1월 평가·인증대상을 정비하여 24종으로 개편하였다.

미래창조과학부는 2017년 7월 과학기술정보통신부로 명칭을 변경하였으며, 과학기술정보통신부와 IT보안인증사무국은 최신 CCRA 협정서 및 정책 등을 반영하여 「정보보호제품 평가·인증 수행규정」을 개정하였다. 2017년 4월 CCRA는 CC를 개정하였으며, IT보안인증사무국은 개정 시 에디터 역할을 수행하여 CC의 지적재산권을 가진 기관으로 국가보안기술연구소를 등록하였다. 2017년에는 침입방지시스템, 호스트 자료유출방지, 네트워크 자료유출방지, 무선침입방지시스템, 데이터베이스 암호화, 문서 암호화, 통합 인증 등 7개 제품 유형의 국가용 보호프로파일을 추가 인증함으로써 더욱 다양한 제품 유형에 대한 국제 수준의 평가·인증이 가능하도록 지원하였다. 2020년 1월 보안USB 등이 보안기능 확인서로 국가공공기관으로 도입 가능해짐에 따라 국가공공기관 도입 시 CC인증이 필요하였던 정보보호시스템 유형이 침입차단시스템 등 22종 제품으로 소폭 감소하였다.

IT보안인증사무국은 디지털 복합기 제품의 국가·공공기관 도입정책을 지원하기 위하여 2018년 복합기 cPP 개발이 필요함을 발의하여 CCDB(CC개발위원회, Common Criteria Development Board) 복합기 워킹그룹의 주도국 역할을 수행하고 있으며, 우리나라 국가·공공기관 요구사항이 포함된 필수 보안요구사항을 개발하였다. 또한 우리나라에서

개발한 국제표준 암호알고리즘 4종(SEED, HIGHT, KCDSA, EC-KCDSA)이 포함된 정보보호제품을 CC에 기반한 평가·인증 시 보안요구사항을 정의하는 방법에 대한 CCRA 공통의 기술문서를 제안하였다.

2018년 최신 기술동향과 보안위협을 고려하여 통합보안 관리제품, 호스트 자료유출 방지제품, 소프트웨어기반 보안USB 제품 등 3종의 국가용 정보보호제품 보안요구사항을 개정하였으며, 국가·공공기관 도입 시 CC인증이 필요한 제품 유형인 스마트폰 보안관리 및 데이터베이스 접근통제 등 2개 제품 유형의 국가용 보호프로파일을 추가 인증하였다.

IT보안인증사무국은 2015년부터 평가·인증이 필요한 국가용 보호프로파일을 개발하였으며, 2022년까지 네트워크 접근통제 제품 등 17개 제품 유형의 국가용 보호프로파일을 개발하고 인증함으로써 국제 수준의 평가·인증 규격을 마련하였다.

또한 2019년 「국가를 당사자로 하는 계약에 관한 법률」 시행령 제26조에 국가용 보안요구사항을 만족하는 CC인증제품도 수의계약 가능하도록 개정하고 같은 해 12월 시행하였다.

2. 평가·인증 체계 및 절차

정보보호제품 평가·인증은 국제표준인 정보보호시스템 공통평가기준(CC, Common Criteria, ISO/IEC 15408)을 기준으로 정보보호시스템 공통평가방법론(CEM, Common Evaluation Methodology, ISO/IEC 18045)에 기반을 두어 수행하고 있다. 평가보증등급은 제품의 보안기능이 보안목적에 부합하도록 정확하게 구현되었는지에 대한 신뢰도 수준으로서 EAL(평가보증등급, Evaluation Assurance Level)로 구분한다. 등급별 평가 수준은 [표 3-1-6-1]과 같다.

표 3-1-6-1 정보보호제품 평가보증등급

보증등급	보증 수준 및 설명
EAL1	개발자 도움 없이 제품 설명서에 기반한 사용자 수준의 기능 시험
	일반인 수준의 공격자에 의한 공개된 취약성 시험
EAL2	외부 인터페이스에 기반을 둔 개발자 수준의 기능 시험, 평가자의 독립적인 시험
	일반인 수준의 공격자에 의한 공개된 취약성 시험, 독립적인 취약성 분석
EAL3	EAL2 수준의 시험 외에 내부 인터페이스 시험, 개발환경 및 제품 형상변경 체계 검증
	일반인 수준의 공격자에 의한 공개된 취약성 시험, 독립적인 취약성 분석
EAL4	EAL3 수준의 시험 외에 소스코드 수준의 설계검증 및 개발 도구에 대한 검증 수행
	숙련자 수준의 공격자가 설계 정보 등을 활용한 취약성 시험
EAL5~7	하위 수준보다 엄격하고 상세한 설계서 검증, 제품 형상변경 체계 검증 강화
	전문가 이상의 공격자가 전문 장비 및 전문 지식을 활용한 취약성 시험

정보보호제품 평가·인증 체계는 역할과 책임에 따라 정책기관, 인증기관, 평가기관, 인정기관으로 구분한다.

정책기관인 과학기술정보통신부는 정보보호제품 인증에 관한 국가정책 결정, 평가인증 수행규정 및 기준 수립, 인증기관 관리, 평가·인증 지침 수립 및 고시 등을 수행한다.

인증기관인 IT보안인증사무국은 평가기관이 제출한 평가결과의 적정성과 타당성을 확인한 후 인증보고서와 인증서를 발급하고 평가자 자격 부여 및 평가기관 지정 등 평가기관 관리 업무를 수행하며, CCRA위원회 활동 및 가입국 심사 등 국제협력 업무를 담당하고 있다.

관련 법에 따라 평가기관으로 지정된 한국인터넷진흥원과 인증기관이 승인한 6개 평가기관(KoSyAs, KSEL, TTA, KOIST, KTC, KTR)은 정보보호제품 평가 등을 수행한다.

인정기관인 국가기술표준원(KATS)은 인증기관에 의하여 정보보호제품 평가기관으로 승인받고자 하는 시험기관을 국제표준에 따른 공인시험기관으로 인정하는 역할을 수행한다.

정보보호제품 평가·인증절차는 준비 단계, 평가·인증 단계 및 종료 단계로 구분된다. 준비 단계에서 평가 신청업체의 평가신청과 제출물 검토 등이 이루어진다. 평가·인증 단계에서는

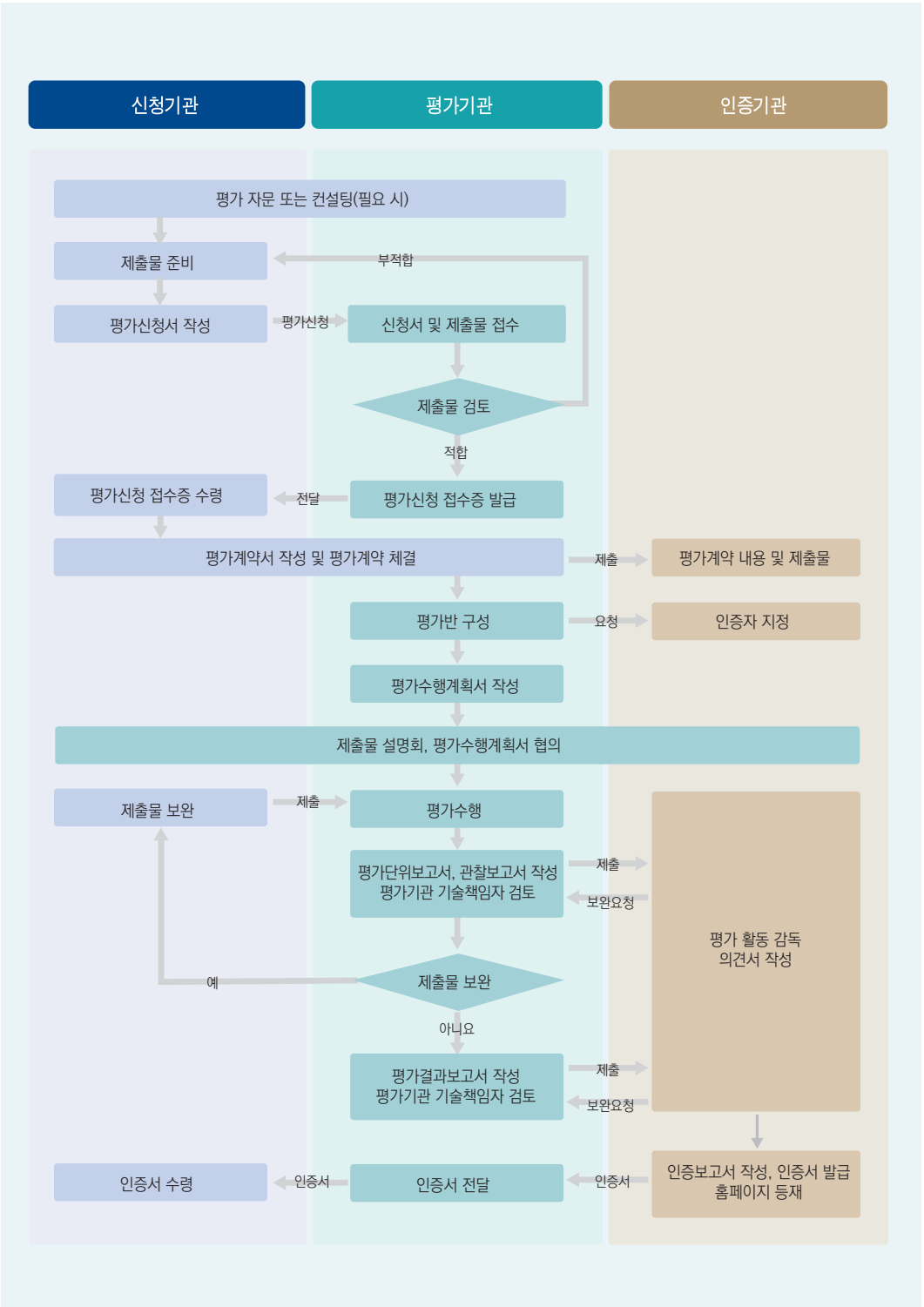
그림 3-1-6-1 정보보호제품 평가·인증 체계

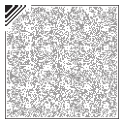
표 3-1-6-2 IT보안인증사무국이 인정한 CC 평가기관

명칭	설립 연월	홈페이지
한국인터넷진흥원	1998. 2.	http://www.kisa.or.kr
한국시스템보증㈜	2007. 8.	http://www.kosyas.com
㈜한국아이티평가원	2009. 8.	http://www.ksel.co.kr
한국정보통신기술협회	2009. 10.	http://www.tta.or.kr
(재)한국화학융합연구원	2010. 10.	http://www.ktr.or.kr
㈜한국정보보안기술원	2014. 4.	http://www.koist.kr
(재)한국기계전기전자시험연구원	2014. 12.	http://www.ktc.re.kr

평가계약을 체결하고 평가기관이 정보보호제품의 안전성과 신뢰성을 검증하기 위하여 설계오류 검증과 같은 제출물 평가, 보안기능 시험 및 취약성 검증 등 평가를 수행한다. 인증기관은 평가기관이 수행한 평가결과에 대하여 검토·심의한다. 종료 단계에서 인증기관이 인증보고서를 작성하고, 평가 신청업체에게 인증서를 교부한다.

그림 3-1-6-2 정보보호제품 평가·인증 절차





3. 평가·인증 현황

2022년 12월 31일 기준 CC인증을 받은 정보보호제품 수는 보안 취약점 등으로 인하여 인증 취소된 제품 및 인증서 유효기간이 경과하여 효력이 만료된 제품을 포함하여 국내용 1,016건, 국제용 164건 등 총 1,180건이다. 국내용 CC인증제품의 경우 침입차단시스템, 침입방지시스템, 접근통제시스템 등 네트워크 보안장비유형이 전체의 절반 이상을 차지한다.

표 3-1-6-3 평가보증등급별 인증제품 현황

(단위: 건)

보증등급		2003~2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	합계
EAL1	국제용							2	3	1	1	1	1	1	10
	국내용														0
EAL1+	국제용							5	7	2	5			2	21
	국내용														0
EAL2	국제용				1		2		2		1			2	8
	국내용	48	36	28	14	43	42	33	36	24	23	32	29	10	398
EAL2+	국제용					1	5	2	1			1			10
	국내용	3	1												4
EAL3	국제용	8	1												9
	국내용	31	14	15	20	16	15	19	14	12	18	12	10	13	209
EAL3+	국제용	9		4		2									15
	국내용	67			2		1								70
EAL4	국제용	20	1	1	1										23
	국내용	68	9	23	8	26	40	22	18	16	17	30	24	33	334
EAL4+	국제용	11		3		1	1				1		1		18
	국내용		1												1
EAL5+	국제용	2	1		3	3	3		3		1	1	2		19
	국내용														0
PP 준수	국제용								1	3	12	7	5	3	31
	국내용														0
국제용 합계		50	3	8	5	7	11	9	17	6	21	10	9	8	164
국내용 합계		217	61	66	44	85	98	74	68	52	58	74	63	56	1,016
합계		267	64	74	49	92	109	83	85	58	79	84	72	64	1,180

국제용 CC인증제품에서는 전자여권, 스마트카드 운영체제 등 스마트카드 관련 제품과 디지털 복합기 제품이 전체의 절반 이상을 차지하며, 2016~2017년에는 스마트TV 보안 소프트웨어 등 신규 기술유형의 국제용 CC인증을 완료하였다. 2018년 이후에는 국가용 보호프로파일을 기반으로 한 암호제품 3종(문서 암호화, 데이터베이스 암호화, 통합인증)에 대한 인증이 이루어졌다. 2020년부터 2022년까지의 경우 국내용 CC인증 및 국제용 CC인증 건수는 감소하였다.

4. CCRA 활동

2006년 CCRA에 가입한 후 인증서발행국으로서의 위상을 제고하기 위한 국제협력에 노력하고 있다. 이를 위하여 CCMB(기술위원회, Common Criteria Maintenance Board)·CCDB(CC개발위원회, Common Criteria Development Board)·CCES(집행위원회, Common Criteria Executive Subcommittee)·CCMC(관리위원회, Common Criteria Management Committee)로 구성된 CCRA(국제상호인정협정, Common Criteria Recognition Arrangement) 국제회의에 참석하여 국내 정보보호제품 평가·인증현황을 발표하고 국제 평가기술과 평가정책 동향 등을 분석하였다.

CCRA와 더불어 아시아 CCRA 가입국의 평가·인증관련 정책 및 기술 공유를 꾀하고 아시아 국가의 CCRA 인증서발행국 가입 지원 등의 국제협력을 강화하기 위하여 2009년 AISEC (Asian IT Security Evaluation and Certification) 포럼을 발족하였다.

CCRA는 2012년 공동의 보안규격인 cPP 개발을 주요 내용으로 하는 비전 선언문을 발표하였다. 이에 따라 보안기술 분야별로 개발업체·평가기관·인증기관·국가기관 등이 참여하는 국제 기술커뮤니티를 구성하여 cPP 개발에 주력하고 있다. CCRA는 2014년 7월 cPP 기반 인증제품 상호 인정을 주요 내용으로 하는 협정서 개정안에 합의하였으며, 같은 해 9월 전체 26개 CCRA 회원국이 개정 협정서에 서명하였다. 우리나라는 국가정보원과 국가보안기술연구소가 개정 협정서에 공동 서명하였다. 2017년 에티오피아, 2018년 폴란드, 2019년 인도네시아와 슬로바키아가 인증서수용국으로 CCRA에 가입하여 CCRA회원국은 31개국이며, 우리나라에서 발급한 국제용 CC인증서를 31개국에서 상호 인정하고 있다.

개정된 CCRA 협정서는 cPP 기반 인증제품 상호 인정을 원칙으로 하되 cPP가 사용되지 않은 인증제품은 최대 EAL2까지 상호 인정할 수 있도록 규정하고 있다. cPP는 최대 EAL4까지 포함할 수 있으나 EAL2 이하를 포함하도록 권고하고 있다. 2022년 기준 CCRA는 8개의 국제 기술커뮤니티를 승인하여 보안USB, 네트워크 장비, 디스크 암호화, 응용 소프트웨어 보안, 전용 보안모듈, 데이터베이스, 바이오인증 제품유형에 대한 cPP 개발을 진행하고 있으며, 디지털 복합기 의 경우 2022년 10월 대한민국 주도로 한·미·일 인증기관이 참여하여 디지털 복합기 cPP 개발을 완료하였다.

IT보안인증사무국은 CCRA위원회, CCUF(CC 사용자 포럼, CC Users Forum) 및 국제 기술 커뮤니티 활동을 통하여 cPP 제정에 참여하고 있으며, 2012년 이후 CCRA에서 CC 제·개정 실무를 담당하는 상설위원회인 CCMB(기술위원회, Common Criteria Maintenance Board) 의장국으로 독일과 공동으로 선임되어 역할을 수행하고 있어 CCRA 내에서 발언권 등을 더욱 강화하였다.

또한 IT보안인증사무국은 개정 CCRA 협정서의 인증서발행국 인증기관으로, CCRA 가입국 정기심사 등에 심사국으로 참여하고 있다. 2014년 튀르키예 인증기관 정기심사 심사장, 2015년 일본 인증기관 정기심사 심사장, 2016년 오스트레일리아 인증기관 정기심사 부심사장 역할을 각각 수행하였다.

표 3-1-6-4 CCRA 회원국 현황

국가		인증기관 홈페이지
인증서발행국 (16개국)	오스트리아	https://www.cyber.gov.au/acsc/view-all-content/programs/australasian-information-security-evaluation-program
	캐나다	https://www.cyber.gc.ca
	프랑스	http://www.ssi.gouv.fr/
	독일	http://www.bsi.bund.de/
	인도	http://www.commoncriteria-india.gov.in/
	이탈리아	http://www.ocsi.isticom.it/
	일본	https://www.ipa.go.jp/security/jisec/jisec_e/
	말레이시아	http://www.cybersecurity.my/mycc

국가		인증기관 홈페이지
인증서발행국 (16개국)	네덜란드	https://www.tuv-nederland.nl/common-criteria/
	노르웨이	http://www.sertit.no/
	대한민국	http://itscc.kr
	싱가포르	https://www.csa.gov.sg/programmes/csa-common-criteria
	스페인	https://oc.ccn.cni.es
	스웨덴	https://www.fmv.se/verksamhet/ovrig-verksamhet/csec/
	튀르키예	https://en.tse.org.tr/KurumsalSablon?ID=666&ParentID=2312
	미국	https://www.niap-ccevs.org/
인증서수용국 (15개국)	오스트리아	http://www.digitales.oesterreich.gv.at/
	체코	https://www.nukib.cz/en/
	덴마크	https://www.cfcs.dk
	에티오피아	http://www.insa.gov.et
	핀란드	https://www.ncsc.fi/
	그리스	http://www.nis.gr/
	헝가리	http://www.kormany.hu/en/ministry-of-national-development
	인도네시아	https://www.bssn.go.id/idcc
	이스라엘	http://www.sii.org.il/
	파키스탄	http://www.commoncriteria.org.pk/
	폴란드	https://www.gov.pl/web/cyfryzacja/cyberbezpieczenstwo
	카타르	http://www.motc.gov.qa/
	슬로바키아	https://www.nbu.gov.sk/en/index.html
	영국	http://www.ncsc.gov.uk/
	뉴질랜드	https://www.cyber.gov.au/programs/australasian-information-security-evaluation-program

[출처: CCRA 홈페이지]

제2장

디지털정부

제1절 디지털정부 정보보호

1. 개요

정보기술의 급격한 발전과 인터넷 이용 확산으로 우리나라는 2002년 11월 전자민원 단일 창구(G4C)를 개통하여 본격적인 전자정부 시대를 열었다. 2010년 '민원24'를 시작으로 2017년 개통한 정부민원포털 '정부24'는 국민이 관공서를 방문하지 않고 인터넷으로 간편하게 약 3,600여 종의 행정서비스를 PC·태블릿·모바일 등 다양한 기기를 통하여 이용할 수 있도록 제공하고 있다.

전자정부 서비스의 이용 추이를 살펴보면 정부민원포털 '정부24'의 경우 서비스 신청 건수가 2014년 6,300만여 건에서 2022년에는 1억 5,800만여 건을 신청할 정도로 손쉽게 전자정부 서비스를 이용하고 있으며, 정부는 민원처리를 인터넷으로 빠르고 편리하게 이용할 수 있도록 제공하고 있다.

그림 3-2-1-1 정부민원포털 '정부24' 서비스 활용 현황

[출처: 행정안전부(정부민원포털 '정부24')]

정부는 2002년 「전자정부법」 시행과 함께 전자정부 구축을 본격 추진한 결과, 유엔 전자정부 발전지수에서 2010·2012·2014년 3회 연속 1위를 기록하였고, 2010·2012·2014·2018·2020년 온라인 참여지수에서 1위, 2009년부터 2017년까지 9년 동안 ICT 발전지수 평가에서 1·2위를 유지하는 등 국제사회에서 인정받고 있다.

2022년에는 유엔 전자정부 발전지수 및 온라인 참여지수 3위, 네트워크 준비지수 9위를 차지하는 등 민원·세정·조달 등 각 분야에서 다양하고 편리한 전자정부 서비스를 제공하고 있다.

표 3-2-1-1 국제정보화 지수별 우리나라 순위

(단위: 위/개국)

[작성기관] 지수명	지수 설명	우리나라 순위 (조사 대상 국가 수)														
		2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
[ITU] ICT 발전 지수	국가별 ICT에 대한 접근성, 이용도, 활용 역량 종합 평가	-	2 (159)	1 (159)	1 (152)	1 (155)	1 (157)	2 (166)	1 (167)	1 (175)	2 (176)	-	-	-	-	-
[UN] 전자정부 발전지수	국가별 ICT 주도의 발전을 위하여 전자정부를 이용하는 역량과 의지	6 (192)	-	1 (192)	-	1 (193)	-	1 (193)	-	3 (193)	-	3 (193)	-	2 (193)	-	3 (193)
[UN] 온라인 참여 지수	국가별 온라인을 통한 시민의 공공 정책 의사결정에 참여할 수 있는 수준	2 (192)	-	1 (192)	-	1 (193)	-	1 (193)	-	4 (193)	-	1 (193)	-	1 (193)	-	3 (193)
[PI] 네트워크 준비지수	국가별 경제발전과 경쟁력 제고를 위하여 ICT를 활용하는 정도 측정	9 (127)	11 (134)	15 (133)	10 (138)	12 (142)	11 (144)	10 (148)	12 (143)	13 (139)	-	-	17 (121)	14 (134)	12 (130)	9 (131)
[ITU] 글로벌 사이버 보안 지수	국가별 사이버 보안 수준 5가지 영역에 대한 종합 평가	-	-	-	-	-	-	-	5 (193)	-	13 (193)	-	15 (194)	-	4 (194)	-

※ ICT 발전지수 : ITU, Measuring the information Society(2018),(ICT Developement Index(IDI) 평가 기준 개정 관련 회원국과 협의 중으로 2018년부터 발표하지 않음.)
※ 전자정부 발전지수/온라인참여지수(격년제 발표) : UN, United Nations E-Government Survey(2022).
※ 네트워크 준비지수 : Portulans Institute, The Network Readiness Index(2022).
※ 글로벌사이버보안지수(격년제 발표) : ITU, Global Cybersecurity Index(2021).

지금까지 이루어 낸 전자정부의 성과와 함께 더불어 정부는 디지털정부 구현을 위한 국민 편의와 행정효율에 힘쓰고자 '디지털정부 혁신 추진계획(2019년)', '포스트코로나 시대의 디지털정부 혁신 발전계획(2020년)', '한국판 뉴딜 종합계획(2020년)'에 이어 2021년 6월 '제2차 전자정부 기본계획' 5개년을 발표하여 ▲지능형 서비스 혁신 ▲데이터 행정강화 ▲디지털 기반 확충이라는 3가지 과제를 중심으로 디지털정부 혁신을 가속화를 위하여 노력하고 있다.

국민이 디지털정부 서비스를 편리하면서도 안전하게 이용할 수 있도록 추진하는 것이 어느 때보다 중요한 과제가 되었으며, 이에 정부는 정부기관 사이버안전 대응 체계 강화, 사이버보안 기술 수준 제고, 정보보호 인력 전문성 강화 등을 추진하고 있다.

2. 주요 내용

행정안전부는 2001년 제정된 「전자정부법」에 각종 정보화 사업의 정보보호 추진 체계 및 기반 구축을 강화하는 근거 규정을 발표하였고, 이에 필요한 각종 세부지침을 수립·시행하여 정보보호에 대한 지침을 제시하였다. 같은 해 12월 중앙행정기관·지방자치단체가 이용하고 있는 정부고속망과 지방행정정보망을 주요정보통신기반시설로 지정하였으며, 2002년 4월부터 이에 대한 취약점 분석·평가를 실시하여 관리적·물리적·기술적 보호대책을 수립하였다.

디지털정부 대민서비스의 보안성을 강화하기 위하여 중앙행정기관 성과관리·자체평가 행정관리역량 부문 계획에 따라 '디지털정부 대민서비스 정보보호 수준' 평가지표를 운영하고 있다. 중앙행정기관은 세부지표에 따른 자체평가 결과를 행정안전부에 제출하고, 행정안전부는 결과를 검증하여 각 기관에 통보하고, 증빙자료 보완, 결과 이의제기 등을 거쳐 평가 결과를 확정한다.

행정안전부는 중앙행정기관·지방자치단체의 주요 정보시스템과 디지털정부의 핵심 기반시설인 국가정보통신망을 사이버위협으로부터 안전하게 보호하는 것을 목표로 국가정보자원관리원, 한국지역정보개발원 및 광역자치단체 사이버침해대응센터를 통하여 각종 사이버공격에 공동으로 대응하고 있다.

국가정보자원관리원은 디도스 공격 등 공격 유형별 관제 및 대응 활동으로 입주한 중앙행정기관 정보시스템에 대한 공격을 차단하고 있다. 한국지역정보개발원은 사이버침해대응지원센터를 운영하여 기초 및 광역자치단체 정보시스템에 대한 보안관제 및 사고대응·분석 등 기술지원을 하고 있다. 광역자치단체도 해당 기초자치단체와 산하기관 정보시스템에 대한 보안관제를 위하여 사이버침해대응센터를 운영하고 있다.

특히 국가정보자원관리원은 국가정보통신망 내 정보시스템에 대한 디도스 공격 대응 역량을 강화하기 위하여 실시간 패킷 분석, 디도스 공격 차단, 사이버대피소 등 다단계 방어 체계를 구축하였다. 보안 기반시설이 상대적으로 취약한 국가정보자원관리원 미입주기관의 정보시스템을 보호하기 위하여 2012년 중앙행정기관 소속기관 등 기관 300여 곳을 대상으로 디도스 공격 방어 체계를 확대 구축하고 2013년부터 방어 서비스를 제공하고 있다. 또한 주요

정보시스템 및 정보통신망에 대한 보안취약점 점검을 연 2회 이상 실시하고 부처별 방문으로 현장에서 발견된 보안취약점을 개선하는 등 보안을 지속 강화하고 있으며, 정기 점검 외에도 각 기관이 별도 요청 시 보안진단을 실시하여 사이버침해 시도로부터 보안성을 강화하고 있다. 정기적으로 관계기관과 공동으로 사이버침해대응훈련을 실시하여 대규모 디도스 공격 등 주요 사이버공격에도 대비하고 있다.

정부는 「정보통신기반 보호법」에 따라 국가안보와 경제사회에 미치는 영향 등을 고려하여 각 부처 소관의 중요시스템에 대하여 주요정보통신기반시설로 지정(2022년 12월 기준 426개) 관리하고 있고, 정보통신서비스에 대한 의존도가 심화하면서 이란의 석유시설 공격(2012), 3.20 사이버 테러(2013) 등 주요정보통신기반시설을 겨냥한 표적 공격이 현실화하고 있는 상황이다.

행정안전부는 소관 분야 중요 시스템에 대하여 주요정보통신기반시설로 지정하여 제어시스템 51개, 정보시스템 50개 등 총 101개(2022년 12월 기준)를 관리하고 있고, 사이버위협으로부터 주요정보통신기반시설을 보호하기 위하여 보안취약점 분석·평가, 보호대책 수립 및 보호조치 이행 등의 지원과 기술 지침 배포 등 관리감독을 수행하고 있다.

표 3-2-1-2 행정안전부 소관 주요정보통신기반시설 지정 현황(2022년 기준)

(단위: 개)

합계	제어시스템(51)						정보시스템(50)		
101	철도운영	교통신호	상수도	지역난방	스마트 도시	물 재생	긴급구조	시·도 행정	행안부
	13	12	16	2	5	3	19	17	14

이와 함께 행정안전부는 2013년 2월부터 한국지역정보개발원에 지방자치단체 정보공유·분석센터(ISAC)를 구축하여 운영하고 있으며, 각 광역자치단체의 인터넷, 업무시스템, 교통신호 제어시스템, 철도운영종합관제시스템, 정수제어시스템 등에 대한 보안취약점 분석·평가를 실시하여 보호대책 수립 등을 지원하였다.

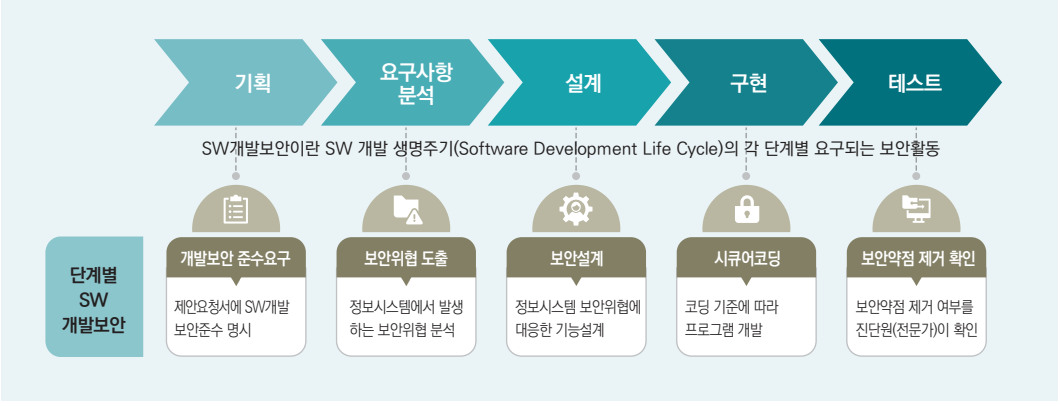
제2절 소프트웨어 개발보안

1. 개요

최근 제로데이 공격, 웹사이트 해킹 등 보안패치가 발표되기 이전에 소프트웨어에 내재된 보안취약점을 악용하는 사이버공격이 지속적으로 증가하고 있다. 특히 이러한 사이버공격의 75% 이상이 응용프로그램의 보안취약점을 악용한다는 점에서 소프트웨어 개발 단계부터 보안취약점의 원인이 되는 보안약점을 진단·제거하는 보안 활동의 필요성 및 중요성이 강조되고 있다.

소프트웨어 개발과정에서 개발자의 실수, 논리적 오류 등으로 소프트웨어에 내포될 수 있는 보안취약점의 원인, 즉 보안약점을 최소화하여 고조되는 사이버위협에 대응할 수 있는 안전한 소프트웨어를 개발하기 위한 일련의 보안 활동을 '소프트웨어 개발보안'이라고 한다.

그림 3-2-2-1 소프트웨어 개발보안 개념



행정안전부는 2012년 「행정기관 및 공공기관 정보시스템 구축·운영 지침」(행정안전부 고시)을 개정하여 소프트웨어 개발보안 기준 및 절차 등을 규정하고 행정기관과 공공기관이 이를 준수하도록 제도화하였고, 정보화사업 규모에 따라 2013년 40억 원 이상, 2014년 20억 원 이상, 2015년 감리 대상 전체로 소프트웨어 개발보안 적용 의무 대상을 점차 확대하였다.

2016년에는 정보시스템 추진 시 소프트웨어 개발보안 적용범위를 구현단계에서 설계단계까지 확대하여 정보시스템의 보안성을 강화하였고, 2018년에는 소프트웨어 개발보안 적용을

위한 비용을 산정하기 위하여 '소프트웨어 사업 대가 산정 가이드'를 개정하여 개발보안 비용 산정 근거를 마련하였다.

소프트웨어 보안약점 기준은 설계단계 보안약점 기준 20개와 구현단계 보안약점 제거 기준 49개가 있다. 2012년 구현단계 보안약점 제거 기준 43개를 신설하여 2013년 47개로 확대하였으며, 2020년 최신 보안위협에 대응하기 위하여 49개로 추가 확대하였다. 2016년 소프트웨어 설계단계부터 개발보안 적용을 위하여 설계단계 보안설계 기준 20개를 신설하였고, 개발보안 적용 범위를 설계 산출물부터 시작하도록 제도화하였다.

모바일 디지털정부 서비스 활용도가 높아지면서 모바일 서비스에 대한 개발보안의 필요성이 높아졌다. 행정안전부는 2014년 「모바일 전자정부 서비스 관리 지침」(행정안전부 예규)을 개정하여 모바일 디지털정부 서비스에 대하여 보안약점을 진단·제거하도록 하였고, 모바일 디지털정부 서비스에 특화된 보안약점 점검 기준 26개를 수립하였다.

표 3-2-2-1 소프트웨어 개발보안 제도 개요

구분	내용	비고
근거	• 행정기관 및 공공기관 정보시스템 구축·운영 지침 제50~54조 • 모바일 전자정부 서비스 관리 지침 제26조	전자정부법
대상	• 정보시스템 감리 대상 정보화사업 ※ 40억 원 이상(2013. 1.) → 20억 원 이상(2014. 1.) → 감리대상 전체(2015. 1.) • 모바일 전자정부 서비스(2014.9, 모바일 전자정부 서비스 전체) ※ 모바일 웹, 모바일 앱, 하이브리드 앱 등	단계적 확대
범위	• 설계단계 산출물 및 소스코드 전체(신규 개발 전체, 유지보수로 변경된 부분)	상용 소프트웨어 제외
기준	• 소프트웨어 설계단계 보안설계 기준 (지침 별표3, DBMS 조회 및 결과 검증 등 20개 항목)	소프트웨어 보안약점 (설계단계)
	• 소프트웨어 구현단계 보안약점 제거 기준 (지침 별표3, SQL 삽입 등 49개 항목)	소프트웨어 보안약점 (구현단계)
	• 모바일 앱 보안약점 점검기준 (지침 별표3, SQL 삽입 등 26개 항목)	모바일 보안약점
	• 모바일 서비스 앱 대상 보안취약점 점검기준 (지침 별표1, 반복설치 시 오류발생 등 20개 항목)	모바일 보안취약점

2. 기반조성 활동

소프트웨어 개발보안 제도 정착과 저변 확대를 위하여 2009년부터 디지털정부 소프트웨어에 대한 보안약점 진단과 모바일 디지털정부 서비스에 대한 보안성 검증을 실시하고 있다. 또한 개발보안 안내서 배포, 교육 제공, 자격제도 운영, 경진대회 개최 등 개발보안 인식 제고를 위한 다양한 활동을 수행하고 있다.

가. 디지털정부 소프트웨어 보안약점 진단

한국인터넷진흥원은 2009년부터 행정기관과 공공기관이 신규로 개발하는 정보시스템을 대상으로 소스코드 보안약점 진단 및 개선 조치를 지원하였다. 2013년부터는 운용 중인 시스템으로 진단 대상 범위를 확대하여 지원하고 있으며, 2022년에는 소프트웨어 보안약점 진단을 125건 지원하였다.

표 3-2-2-2 소프트웨어 보안약점 진단 현황

(단위: 건)

연도	합계	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
대상	964	2	10	23	33	161	31	35	60	87	91	99	127	80	125

나. 모바일 디지털정부 서비스 앱 보안성 검증

모바일 디지털정부 서비스의 보안성과 신뢰성을 제고하기 위하여 2011년 한국인터넷진흥원에 '모바일 전자정부 서비스 앱 보안성 검증센터'를 개소하여 2014년까지 850여 개 모바일 앱에 대한 보안성 검증을 수행하였고, 이후 '전자정부 SW 보안센터'를 통하여 모바일 앱 보안성 검증을 지원하고 있다. 2022년에는 모바일 디지털정부 서비스 앱 보안성 검증을 251건 지원하였다.

표 3-2-2-3 모바일 디지털정부 서비스 앱 보안성 검증 현황

(단위: 건)

연도	합계	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
대상	2,752	30	240	286	292	345	218	366	158	171	187	208	251

다. 안내서 개발 및 배포

행정안전부는 소프트웨어를 개발할 때 보안약점이 제거된 안전한 개발 방법을 제시하기 위하여 소프트웨어 개발보안 안내서를 개발하여 배포하였다. 소프트웨어 개발보안 안내서 3종과 모바일 관련 안내서 2종 등 총 5종을 배포 중이며, 소프트웨어 개발보안 제도, 보안약점 기준 등의 변경에 따라 지속적으로 개정하고 있다. 2021년에는 '소프트웨어 개발보안 가이드'·'모바일 앱 소스코드 검증 가이드라인'·'소프트웨어 보안약점 진단 가이드' 등 3종을 개정하였다.

표 3-2-2-4 소프트웨어 개발보안 안내서 현황

가이드명	제정연월	현재	내용
소프트웨어 개발보안 가이드	2011. 6.	2021. 11.	소프트웨어 개발보안 적용 절차 및 방법 설명
모바일 앱 소스코드 검증 가이드라인	2011. 8.	2021. 10.	모바일 전자정부 서비스 앱 보안성 검증 신청 방법 설명
소프트웨어 보안약점 진단 가이드	2012. 5.	2021. 11.	소프트웨어 보안약점의 진단방법 및 조치방법 설명
모바일 대민서비스 보안취약점 점검 가이드	2014. 10.	2015. 12.	모바일 앱 취약점 기준(20개)에 대한 점검절차, 방법 등 제공
공개 소프트웨어를 활용한 소프트웨어 개발보안 점검 가이드	2016. 2.	2019. 6.	공개 소프트웨어 진단도구를 활용한 개발보안 점검방법 등 소개

라. 인식제고 활동

소프트웨어 개발보안 인식을 제고하기 위하여 2009년부터 공무원·개발자·감리원 등을 대상으로 안전한 소프트웨어 개발방법론과 개발 단계에서의 보안약점 진단·제거 방법 등에 대한 교육을 실시하고 있다. 2012년에는 소프트웨어 보안약점 진단 전문가 양성을 위하여 진단원 양성과정을 개설하여 2022년까지 진단원 658명을 배출하였다.

표 3-2-2-5 소프트웨어 개발보안 교육 및 진단원 자격취득 현황

(단위: 명)

구분	합계	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
개발보안 교육	21,865	109	266	1,019	2,262	2,544	2,100	1,432	1,568	1,866	2,335	1,590	1,313	1,740	1,806
진단원 자격취득	658	-	-	-	82	143	120	111	41	25	28	17	23	32	36

또한 2011년부터 소프트웨어 개발보안 제도의 성과를 공유하고 발전 방향을 논의하기 위하여 공무원·개발자·감리원·진단원 등을 대상으로 소프트웨어 개발보안 콘퍼런스를 해마다 개최하고 있으며, 2014년부터 미래 개발자인 대학생 등을 대상으로 소프트웨어 개발보안을 홍보하고 관심을 유도하기 위한 경진대회를 개최하고 있다.

제3절 전자서명 인증

1. 행정전자서명 인증

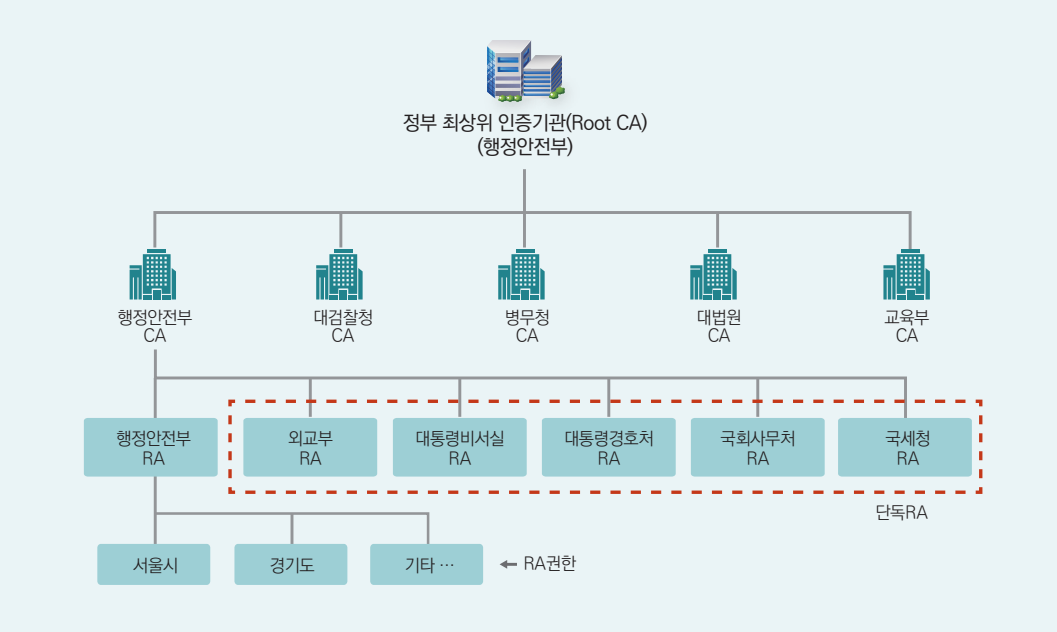
가. 개요

디지털정부의 행정 환경이 종이문서 기반에서 전자문서 기반으로 전환되면서 동시에 해킹 등에 의한 주요 정보의 노출·변조·훼손 등 피해 가능성이 높아져 행정기관 간 전자문서 유통의 연속성과 안전한 복구를 보장할 수 있는 방안이 모색되었다. 이에 정부는 전자문서 송·수신에 대한 행정기관 및 공무원 신원확인, 전자문서 위·변조 방지 등을 보장하고 행정전자문서의 안정적인 유통을 위하여 행정전자서명 인증 체계(GPKI, Government Public Key Infrastructure)를 구축·운영하게 되었다.

행정전자서명 인증 체계는 「전자정부법」 제29조 및 동법 시행령 제28조에 따라 운영되며, 2002년 12월 민·관 전자서명 상호연계 및 인증 체계를 구축하여 명실상부한 디지털정부 인증시스템으로서의 면모를 갖추었다. 2006년 2월 암호키 위탁·복구 관리시스템이 구축되어 행정업무의 연속성과 보안성이 보장되었고, 공공·금융기관 확대 보급을 위하여 2006년 공공·금융용 인증시스템을 구축하였으며, 행정전자서명 인증서의 보안성·신뢰성을 보장하기 위하여 2011년 전자서명 키길이 상향(2,048비트) 및 해시 알고리즘(hash algorithm) 교체 등 행정전자서명 암호 체계 고도화를 추진하였다.

2012년 다양한 웹브라우저에서도 인증서 발급·이용이 가능하도록 관련 소프트웨어를 개선하였고, 2014년 안정적인 서비스를 위하여 노후장비 교체를 완료하였으며, 2015년 국내 인증기관 최초로 인증기관(CA, Certificate Authority) 및 SSL(Secure Sockets Layer) 분야의 국제 신뢰성 마크(웹트러스트 인증)를 동시에 취득하였다.

그림 3-2-3-1 행정전자서명 인증 체계



행정전자서명 인증기관은 최상위 인증기관(행정안전부, Root CA)과 행정안전부장관이 지정·고시하는 인증기관(CA) 5곳, 인증기관이 지정 운영하는 등록기관(RA, Registration Authority) 974곳으로 구성되어 있다. 또한 공인전자서명 인증 체계(NPKI, National Public Key Infrastructure)와 상호 연동하여 사용자 인증 서비스를 제공하고 있다.

표 3-2-3-1 행정전자서명 인증기관

(단위: 곳)

기관	기관 수	대상 기관
최상위 인증기관	1	• 행정안전부
인증기관	5	• 행정안전부, 교육부, 대검찰청, 병무청, 대법원(법원행정처)
등록기관 (하위기관 포함)	974	• 중앙행정기관 : 대통령비서실 등 기관 64 • 지방자치단체 : 서울특별시 등 기관 17 • 각 기관의 산하 및 소속기관

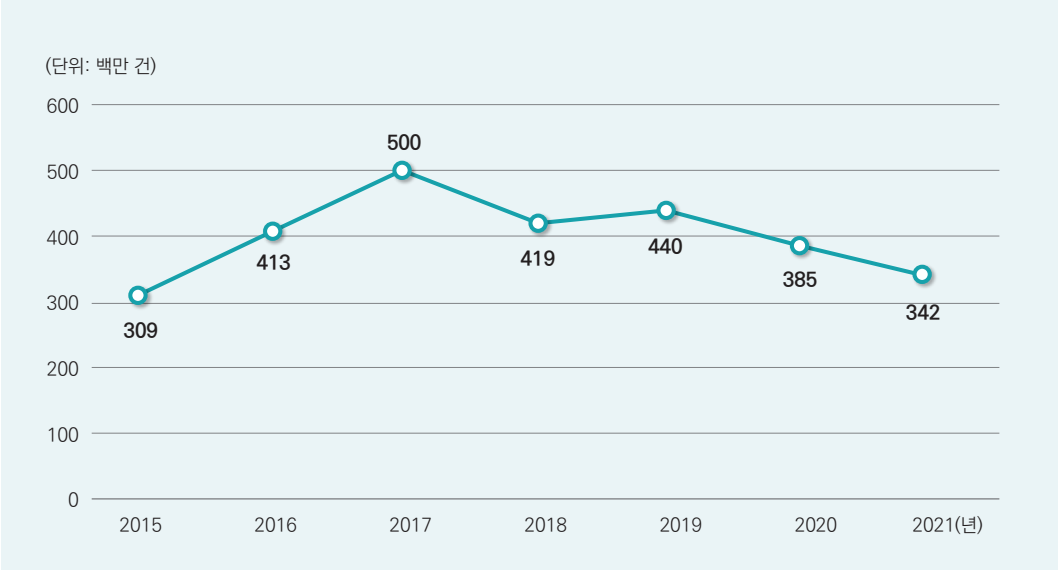
표 3-2-3-2 행정전자서명 기관별 주요 역할

기관	주요 역할
최상위 인증기관	• 인증기관 지정·고시 및 인증기관 인증서 발급·관리 등 인증업무 • 행정전자서명 기술표준 및 GPKI↔NPKI 상호연계방안 마련 • 인증기관 시설 및 장비 기준 제정과 운영실태 조사 • 인증기관의 인증서와 인증서 폐지목록 게시 등
인증기관	• 행정전자서명 인증기관 구성요건, 상호연동 기술표준을 준수하여 인증시스템 구축 등 인증업무 수행 • 등록기관 지정·관리, 서버용 인증서 신청자(기관)의 신원확인
등록기관	• 인증서 신청 접수, 사용자의 신원확인 및 등록·관리 • 원격 등록기관 지정·관리

나. 인증서 발급 및 이용 현황

행정전자서명 인증서는 2021년 12월 기준 721만 건이 발급되어 공무원 신원확인, 전자문서 위·변조 방지 등을 위하여 기관 1,493곳, 행정서비스 11,067개에서 활용하고 있으며, 개인정보보호를 위하여 행정기관 홈페이지에 디지털정부 웹서비스(G-SSL) 인증서를 도입하여 보안서버를 구축할 수 있도록 지원하고 있다.

그림 3-2-3-2 연도별 행정전자서명 인증서비스 이용 현황



다. 인증서비스 기반 확대

해킹 기술 발전에 따른 외부 위협으로부터 디지털정부 서비스의 보안성을 강화하기 위하여 정부 일회용 패스워드(OTP, One Time Password), 2채널 복합인증, 전자문서 진본 확인 등 다양한 인증 서비스를 제공하고 있다.

2015년 모바일·클라우드 등 기술 변화와 웹브라우저 운영사의 정책 변경 등에 따른 개별적 협의로는 신뢰성을 인정받는 데 한계에 이르러 행정전자서명에 대한 관리적·기술적 신뢰성 확보를 위하여 국제인증을 추진하였다. 2015년 10월 국내 인증기관 최초로 'WebTrust for CA'와 'WebTrust for SSL' 분야에서 웹트러스트 인증을 동시에 취득하였고, 국제표준화 작업에 참여하기 위하여 CA/브라우저 국제기술포럼에도 가입하였다.

2. 민간 전자서명 인증

가. 개요

1999년 2월 정부는 전자문서의 안전성과 신뢰성을 확보하고 이용을 활성화하기 위하여 전자서명에 관한 기본적인 사항을 정한 「전자서명법」을 제정하였다.

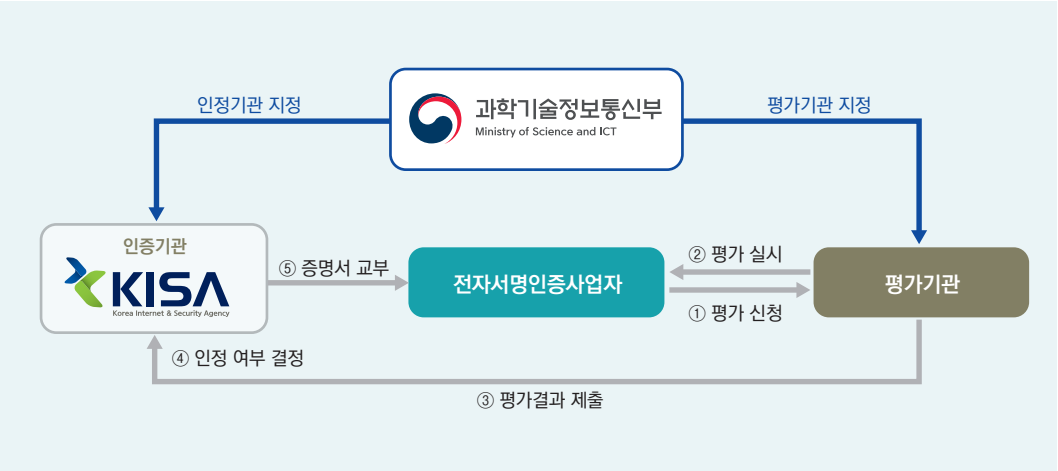
공인인증서는 우리나라의 전자서명제도 도입 초기에 광범위하게 활용되면서 전자상거래 활성화 등 국가정보화에 크게 이바지하였으나, 공인인증서가 시장독점을 초래하고, 전자서명 기술의 발전과 서비스 혁신을 저해하며, 다양하고 편리한 전자서명에 대한 국민의 선택권을 제한한다는 등의 문제점이 제기되었다.

이러한 문제점을 개선하기 위하여 공인인증서 제도를 폐지함으로써 다양한 전자서명이 기술 및 서비스를 기반으로 차별 없이 경쟁할 수 있는 여건을 조성하고, 전자서명의 신뢰성을 제고하면서 국민의 전자서명인증서비스 선택권 제공을 위하여 전자서명인증사업자 인정·평가 제도를 신규 도입한 개정 「전자서명법」이 2020년 12월 시행되었다.

나. 전자서명인증사업자 인정·평가 제도

전자서명인증업무의 안정성과 신뢰성을 확보하고, 국민의 다양하고 편리한 전자서명 선택권을 보장하기 위하여 민간 평가기관이 전자서명인증업무 운영기준 준수사실 여부를 평가하여 해당 결과의 적정성을 검토하고, 인정기관에서 인정 여부를 결정하는 제도이다.

그림 3-2-3-3 전자서명인증사업자 인정·평가 체계



과학기술정보통신부는 전자서명의 안전성·신뢰성 및 다양성 제고 등을 위한 정책을 수립하고, 한국인터넷진흥원은 전자서명인증업무 운영기준 준수사실 인정 여부 결정 및 인정 취소 등 업무를 수행하며, 평가기관은 평가를 신청한 전자서명인증사업자의 운영기준 준수 여부에 대한 평가 업무를 수행한다.

표 3-2-3-3 평가기관 선정 현황(2022. 12. 기준)

연번	평가기관	선정일
1	한국정보통신기술협회	2020. 12. 22.
2	금융보안원	2020. 12. 22.
3	딜로이트(안진회계법인)	2020. 12. 22.
4	KPMG(삼정회계법인)	2022. 4. 18.

다. 증명서 발급 현황

개정 「전자서명법」 시행 이후 19개 전자서명인증사업자가 한국인터넷진흥원으로부터 전자서명인증업무 운영기준 준수사실 증명서를 발급받았다.

표 3-2-3-4 증명서 발급 현황(2022. 12. 기준)

인정번호	업체명	인정범위
제2021-001호	엔에치엔페이코㈜	PAYCO 인증서비스
제2021-002호	㈜신한은행	신한Sign 서비스
제2021-003호	네이버㈜	모바일 앱 기반 네이버 인증서 서비스
제2021-004호	㈜국민은행	KB국민인증서 서비스
제2021-005호	금융결제원	YesKey 인증서 서비스(공동인증서 및 금융인증서)
제2021-006호	㈜한국정보인증	공동인증서비스
제2021-007호	㈜비바리퍼블리카	토스인증서
제2021-008호	㈜뱅크샐러드	뱅크샐러드 인증서
제2021-009호	㈜카카오	카카오 인증서
제2021-010호	㈜코스콤	코스콤 SignKorea 인증서비스
제2021-011호	한국전자인증㈜	CrossCert 전자인증서비스(공동인증서)
제2021-012호	㈜한국무역정보통신	TradeSign 인증서비스(공동인증서)
제2021-013호	㈜하나은행	하나OneSign 인증서 서비스
제2021-014호	에스케이텔레콤㈜	SK텔레콤 PASS 인증서 서비스
제2021-015호	㈜케이티	KT PASS 인증서
제2021-016호	㈜한국정보인증	S-PASS 인증서비스
제2022-001호	㈜드림시큐리티	드림인증 전자서명 서비스
제2022-002호	NH농협컨소시엄	NH모바일 인증서
제2022-003호	주식회사 카카오뱅크	카카오뱅크 인증서 서비스

라. 민간 전자서명 이용 현황

과학기술정보통신부와 한국인터넷진흥원은 다양한 전자서명수단 도입을 희망하는 이용기관을 대상으로 '간편인증 통합모듈 지원 시범사업'을 추진하였다. '간편인증 통합모듈'은 다양한 간편인증 서비스를 통합 중계하기 위하여 전자서명 이용기관에 설치되는 프로그램으로, 국민이 희망하는 간편인증 서비스를 편리하게 이용할 수 있도록 지원하는 기능을 수행한다.

행정안전부는 「전자서명법」 개정에 따라 국민이 쉽고 편리하게 디지털정부 서비스를 이용할

수 있도록 정부24·홈택스 등 주요 공공웹사이트에 민간 전자서명, 일명 '간편인증'을 공공웹사이트에 적용하였다. 간편인증 서비스는 2021년 55개 공공웹사이트에 적용되었으며, 2022년에는 경찰청 교통민원24와 대법원 가족관계등록시스템 등 공공웹사이트 110곳에 연계 적용을 완료하였다. 이와 더불어 적용 가능한 민간인증서도 5종에서 12종으로 다양화하여 이용 편의를 제고하였다. 행정안전부는 2023년까지 70개의 공공웹사이트에 간편인증 방식을 추가 도입하여 총 180개 사이트에서 간편인증을 사용할 수 있도록 할 계획이다.

그림 3-2-3-4 간편인증을 적용한 대법원 가족관계등록시스템 로그인 화면

한편 과학기술정보통신부는 2023년부터 전자서명 이용기관의 전자서명수단 도입 편의 증대와 국민의 이용 편의성을 확대하기 위하여 디지털인증확산센터를 신규 구축하여 운영할 계획이다. 한국인터넷진흥원은 디지털인증확산센터 구축을 위하여 한국전자서명포럼과 함께 다양한 전자서명 기술 간 상호연계가 가능하도록 메시지 규격, 인증수단 유효성 검증 방법 등에 대한 표준화 작업을 2022년 11월부터 진행하고 있다.

제3장

주요정보통신기반시설

제1절 추진 체계

1. 개요

2000년대 들어 정보통신 인프라 발전으로 행정·방송통신·금융·에너지 등 국가 기반시설의 정보통신기술에 대한 의존도가 심화되면서 해킹, 악성코드 유포, 디도스 공격 등 전자적 침해행위가 새로운 위협요소로 대두되었다. 주요정보통신기반시설의 교란 또는 마비가 막대한 경제적 손실과 사회적 혼란을 일으킬 수 있음에도 불구하고 전자적 침해행위 사전 예방 및 사후 대응 체계를 규정하는 법령은 미비하였다. 이에 따라 해킹·악성코드 등 전자적 침해행위로부터 주요기반시설의 정보통신시스템을 보호하는 범정부적 대응 체계를 구축하기 위하여 2001년 「정보통신기반 보호법」을 제정하였다.

2007년 ICT 환경 변화와 현행 제도의 운영과정에서 나타나는 미비점을 반영, 정보통신기반보호위원회 아래 실무위원회를 공공분야와 민간분야로 나누어 그 역할을 구체화하였다. 또한 국가정보원장과 과학기술정보통신부장관 등 대통령령이 정하는 국가기관의 장이 중앙행정기관에 주요정보통신기반시설의 지정을 권고하고 주요정보통신기반시설 보호대책 이행 여부를 확인할 수 있는 권한을 부여하였다.

2009년 실효성 있는 정보통신산업 진흥 정책을 추진할 수 있도록 「정보통신산업 진흥법」이 제정되었다. 이에 따라 「정보통신기반 보호법」의 정보보호 컨설팅 전문업체 조항이 이관되어 「정보통신산업 진흥법」상에 지식정보보안 컨설팅 전문업체로 변경되었고, 2015년 「정보보호산업의 진흥에 관한 법률 시행규칙」이 공포되어 정보보호 전문서비스 기업으로 변경되었다.

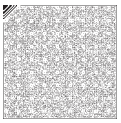
2012년 개정된 시행령은 2007년 12월 「정보통신기반 보호법」 개정에 따라 위임받은 사항을 반영하여 실무위원회의 변화에 걸맞은 구체적인 구성·운영방식을 명시하였다. 그리고 국가정보원장 등의 보호대책 이행 여부 결과 보고에 관한 사항, 주요정보통신기반시설 지정 권고방식 등에 관한 사항을 수록하였다. 또한 취약점 분석·평가 주기를 2년에서 1년으로 단축하는 등 운영상 나타난 일부 미비점을 개선·보완하였으며, 주요정보통신기반시설 보호 지원기관의 범위를 넓히는 등 제도 개선이 이루어졌다.

2015년 동종 산업분야별 기반시설 관리기관 간 사이버위협을 공동으로 분석하고 정보공유를 활성화하기 위하여 정보공유·분석센터(ISAC, Information Sharing & Analysis Center)를 설립·운영할 경우 정부가 기술적인 부분뿐 아니라 재정적 지원을 할 수 있도록 근거를 마련하였다. 또한 ISAC 설립 시 통지 의무를 삭제하는 등 절차를 간소화함으로써 신규 설립을 장려하는 바탕을 마련하였다.

2018년 정보통신기반보호위원회 실무위원회 심의 사항에 주요정보통신기반시설의 지정 및 지정 취소에 관한 사항을 명시적으로 규정함으로써 주요정보통신기반시설을 효과적으로 보호하기 위하여 도입된 지정 권고 제도의 실효성을 확보하였다.

2019년 새로운 형태의 전자적 침해행위로부터 주요정보통신기반시설을 보호하기 위하여 필요한 경우나 주요정보통신기반시설에 중대한 변화가 발생하여 별도의 취약점 분석·평가가 필요하다고 판단되는 경우에 중앙행정기관의 장이 해당 관리기관의 장에게 주요정보통신기반시설의 취약점 분석·평가하도록 명령할 수 있는 법적 근거를 마련하는 등 현행 제도의 운영상 나타난 일부 미비점을 개선·보완하였다.

2021년 ICT 환경 변화에 따른 신규 취약점 분석·평가항목을 과학기술정보통신부·국가정보원 합동으로 정비(2019~2021년)하여 2021년 3월에 고시, 주요정보통신기반시설의 사이버공격에 대한 대응능력을 한층 강화하였다. 그리고 주요정보통신기반시설의 효율적 관리를 위하여 「정보통신기반 보호법 시행령」을 개정하여, 지정 여부 결정 이후 지정 여부



결과에 대한 통보기한(30일 이내) 및 취약점 분석·평가 명령에 따른 이행 기한(6개월 이내)의 법적 근거를 마련하였다.

2. 추진 체계

정부는 주요정보통신기반시설의 안정적 관리·운영을 위하여 정보통신기반보호위원회를 운영, 정보통신기반 보호정책 수립과 시행을 총괄·조정함으로써 관계 중앙행정기관 간 침해사고 예방 및 대응 업무가 상호 협력 및 보완될 수 있도록 하고 있다.

정보통신기반보호위원회는 국무조정실장을 위원장으로, 중앙행정기관의 차관급 공무원을 위원으로 구성하고 있다. 정보통신기반보호위원회는 주요정보통신기반시설 보호정책의 조정, 주요정보통신기반시설 보호계획의 종합·조정, 주요정보통신기반시설 보호와 관련된 제도 개선, 기반시설의 신규 지정 및 지정 취소 등 주요 정책사항을 심의한다.

또한 정보통신기반보호위원회를 효율적으로 운영하고 지원하기 위하여 정보통신기반보호 실무위원회를 두고 있다. 실무위원회는 정보통신기반보호위원회에 제출된 안건과 정보통신기반보호위원회로부터 위임받거나 정보통신기반보호위원회의 위원장으로부터 지시받은 사항을 검토·심의한다.

실무위원회는 공공분야 실무위원회(위원장: 국가정보원 차장)와 민간분야 실무위원회(위원장: 과학기술정보통신부 차관)를 각각 운영하고 있으며, 보호대책 및 보호계획 수립 지침을 배포하고 주요정보통신기반시설의 신규 지정 권고 등 역할을 수행한다.

한편 중앙행정기관은 주요정보통신기반시설을 지정하고 관리기관이 제출한 주요정보통신기반시설 보호대책을 검토한 후 보호계획을 수립·시행한다. 관리기관은 주요정보통신기반시설에 대한 침해사고를 예방하고 대응하기 위하여 해당 시설에 대한 취약점 분석·평가를 실시하고 보호대책을 마련한다. 또한 사고가 발생할 경우 관계 중앙행정기관·수사기관 등에 사고 내용을 통지하고 신속히 복구 작업을 실시한다.

특히 주요정보통신기반시설에 대하여 중대한 침해사고가 광범위하게 발생한 경우에는 정보통신기반보호위원회 산하에 정보통신기반침해사고 대책본부를 한시적으로 운영하여 응급대책, 기술 지원 및 피해 복구 등을 수행한다.

주요정보통신기반시설 보호를 위한 지원기관으로는 한국인터넷진흥원, 국가보안기술연구소, 정보공유·분석센터, 정보보호 전문서비스 기업이 있다. 이들 지원기관은 주요정보통신기반시설 보호대책의 수립 및 침해사고 예방·복구 등에 대한 기술적 지원을 수행한다.

그림 3-3-1-1 주요정보통신기반시설 보호 추진 체계

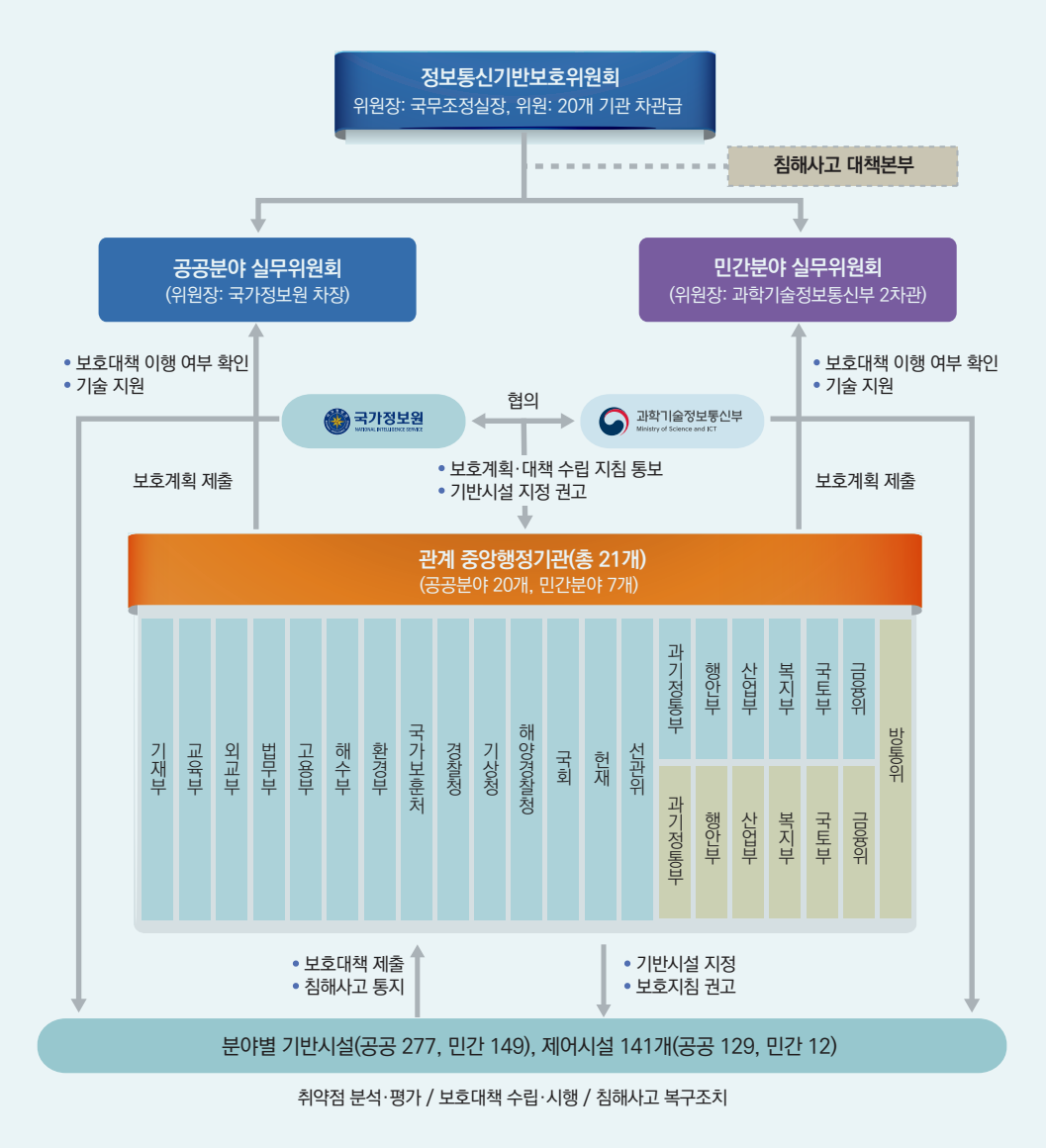


표 3-3-1-1 수행 주체별 주요 기능

수행 주체	주요 기능
정보통신기반보호위원회 (국무조정실)	• 기반시설 보호정책 및 제도개선 심의 • 침해사고 대책본부 운영
중앙행정기관	• 소관 분야 보호계획 수립 및 보호지침 제·개정 • 관리기관 대상 보호조치 명령·권고 • 기반시설 신규 지정 및 지정 취소
관리기관	• 소관 시설 보호대책 수립 및 취약점 분석·평가 • 기반시설 신규 지정 및 지정 취소 여부 자체평가 • 침해사고 통지 및 복구 조치
국가정보원/ 과학기술정보통신부	• 보호대책 및 보호계획 수립지침 작성·배포 • 관리기관 보호대책 이행 여부 확인 및 기술 지원 • 취약점 분석·평가 기준 재·개정
한국인터넷진흥원/국가보안기술연구소/ 정보공유·분석센터/정보보호 전문서비스 기업	• 취약점 분석·평가 • 침해사고 예방 및 복구 지원 • 보호대책 이행 여부 확인 지원

제2절 주요 활동

1. 주요정보통신기반시설 지정 및 지정 취소

주요정보통신기반시설 지정 및 지정 취소는 각 중앙행정기관의 장이 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 지정하며, 해당 시설의 폐기·통합·업무 이관 등으로 인하여 더 이상 지정을 유지할 수 없다고 판단한 때에는 지정 취소할 수 있다. 또한 지정 및 지정 취소를 하고자 하는 경우에는 정보통신기반보호위원회의 심의를 받아야 하며, 그 결과에 대하여 고시하여야 한다.

표 3-3-2-1 주요정보통신기반시설 지정 기준

1 해당 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가적·사회적 중요성
2 1호에 따른 기관이 수행하는 업무의 정보통신기반시설에 대한 의존도
3 다른 정보통신기반시설과의 상호 연계성
4 침해사고가 발생할 경우 국가안전보장과 경제사회에 미치는 피해 규모 및 범위
5 침해사고의 발생 가능성 또는 그 복구의 용이성

주요정보통신기반시설의 지정 대상은 국가·공공기관뿐 아니라 민간이 운영·관리하는 정보통신기반시설을 포함한다. 또한 전자적 침해 행위가 발생할 경우 국가안보, 국민의 기본생활과 경제 안정에 중대한 영향을 미칠 수 있는 국가안전보장, 행정, 국방, 치안, 금융, 방송통신, 운송, 에너지 등의 업무와 관련된 전자적 제어·운영시스템과 정보통신망이 해당된다.

또한 과학기술정보통신부와 국가정보원은 각 중앙행정기관에 주요정보통신기반시설의 지정을 권고할 수 있다. 소관 기반 시설이 주요정보통신기반시설로 지정할 필요가 있다는 권고를 받은 중앙행정기관의 장은 「정보통신기반 보호법」에 따라 해당 시설의 지정 여부 결정에 대한 정보통신기반위원회의 심의를 거친 후 개정된 「정보통신기반 보호법 시행령」(2021. 3.)에 따라 30일 이내에 그 결과를 과학기술정보통신부장관과 국가정보원장에게 통보하여야 한다.

2022년 12월 기준 공공분야 140개 관리기관 277개 시설, 민간분야 92개 관리기관 149개 시설 등 총 426개 주요정보통신기반시설을 지정·관리 중이다.

그림 3-3-2-1 주요정보통신기반시설 지정 절차

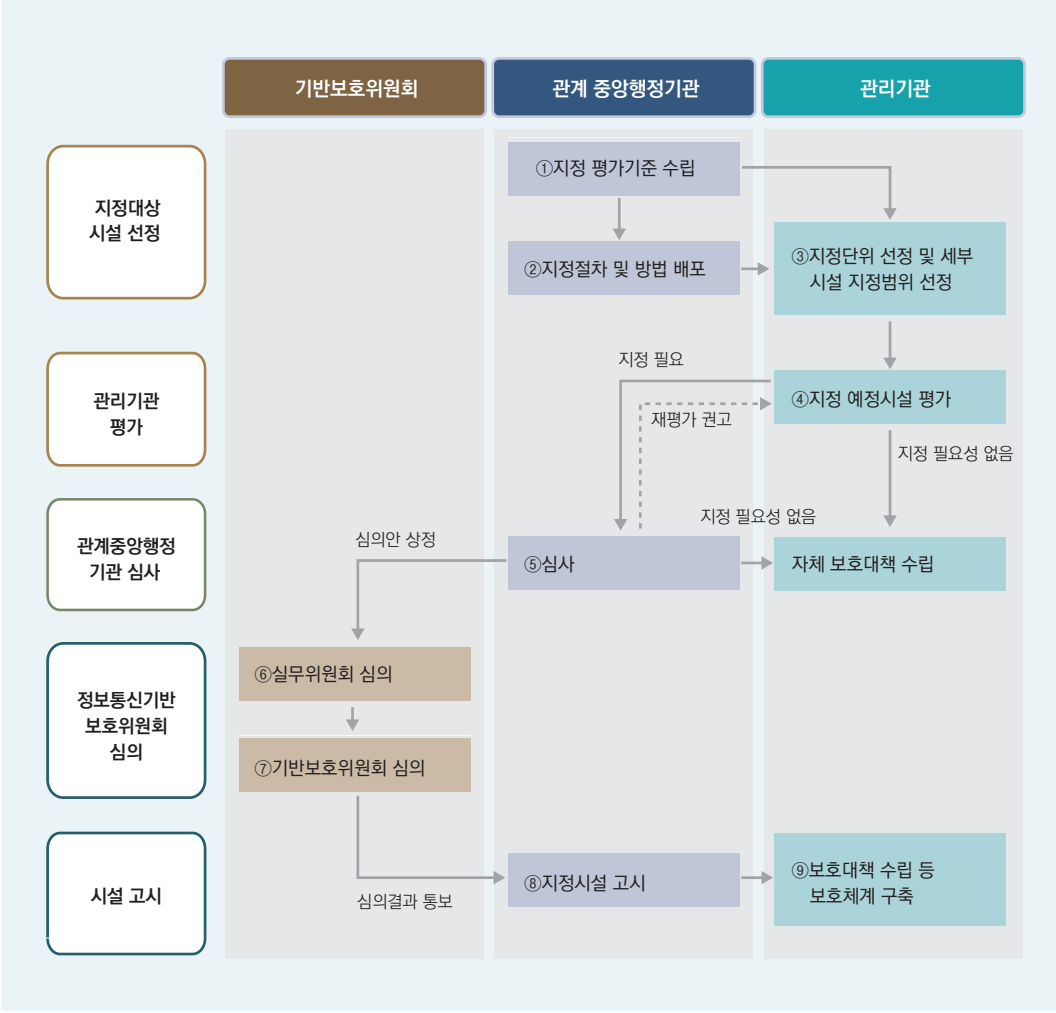


그림 3-3-2-2 주요정보통신기반시설 지정 권고 절차

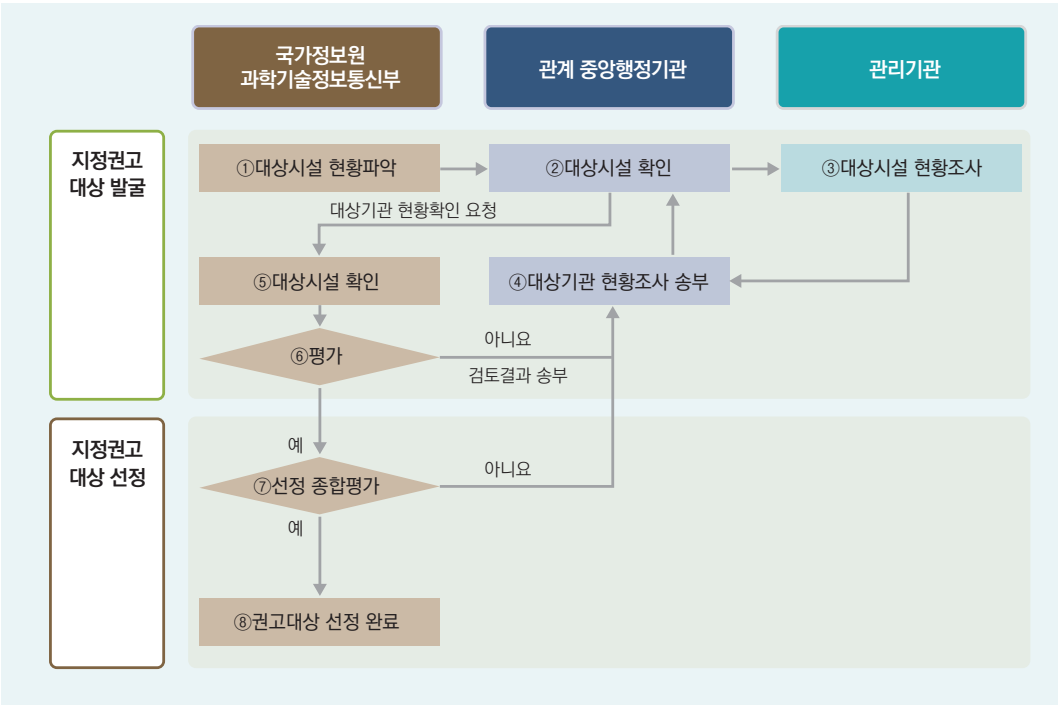


표 3-3-2-2 연도별 주요정보통신기반시설 지정 현황

(단위: 개)

구분	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
공 공	135	193	227	243	252	262	265	274	277	277
민 간	74	99	127	142	141	149	149	148	147	149
합 계	209	292	354	385	393	411	414	422	424	426

관계중앙행정기관의 장은 관리기관이 해당 업무를 폐지·정지 또는 변경하는 경우에는 직권 또는 해당 관리기관의 신청에 의하여 주요정보통신기반시설의 지정을 취소할 수 있다. 지방자치단체의 장이 관리·감독하는 기관의 주요정보통신기반시설은 행정안전부장관이 지방자치단체의 장과 협의하여 지정을 취소할 수 있다. 한편 중앙행정기관의 장이 주요정보통신기반시설의 지정을 취소하고자 하는 경우에는 정보통신기반보호위원회의 심의를 받아야 한다.

2. 취약점 분석·평가

관리기관의 장은 해마다 주요정보통신기반시설에 대한 보호대책을 수립하여야 한다. 이를 통하여 단기적으로는 신규 취약점을 발견하여 제거하고, 장기적으로는 침해사고 발생 시 파급효과 등을 분석하여 실효성 있는 관리 체계를 수립한다.

또한 관리기관의 장은 「정보통신기반 보호법 시행령」(2021. 3.)에 따라 주요정보통신기반시설이 신규 지정될 경우 6개월 이내에 취약점 분석·평가를 실시하여야 한다. 다만 소관 주요정보통신기반시설 지정 후 6개월 이내에 이 시설에 대한 취약점 분석·평가를 시행하지 못할 특별한 사유가 있는 경우에는 관할 중앙행정기관의 승인을 받아 지정 후 9개월 이내에 실시하여야 한다.

취약점 분석·평가는 기존에는 2년 주기로 실시되었으나, 새로운 사이버위협이 해마다 증가하는 상황을 고려하여 단축 필요성이 제기되었다. 이에 따라 2012년 「정보통신기반 보호법 시행령」 개정을 통하여 연 1회 실시로 단축하고, 소관 주요정보통신기반시설에 중대한 변화가 발생하였거나 관리기관이 취약점 분석·평가가 필요하다고 판단하는 경우에는 1년이 되지 않은 때에도 취약점의 분석·평가를 실시할 수 있다.

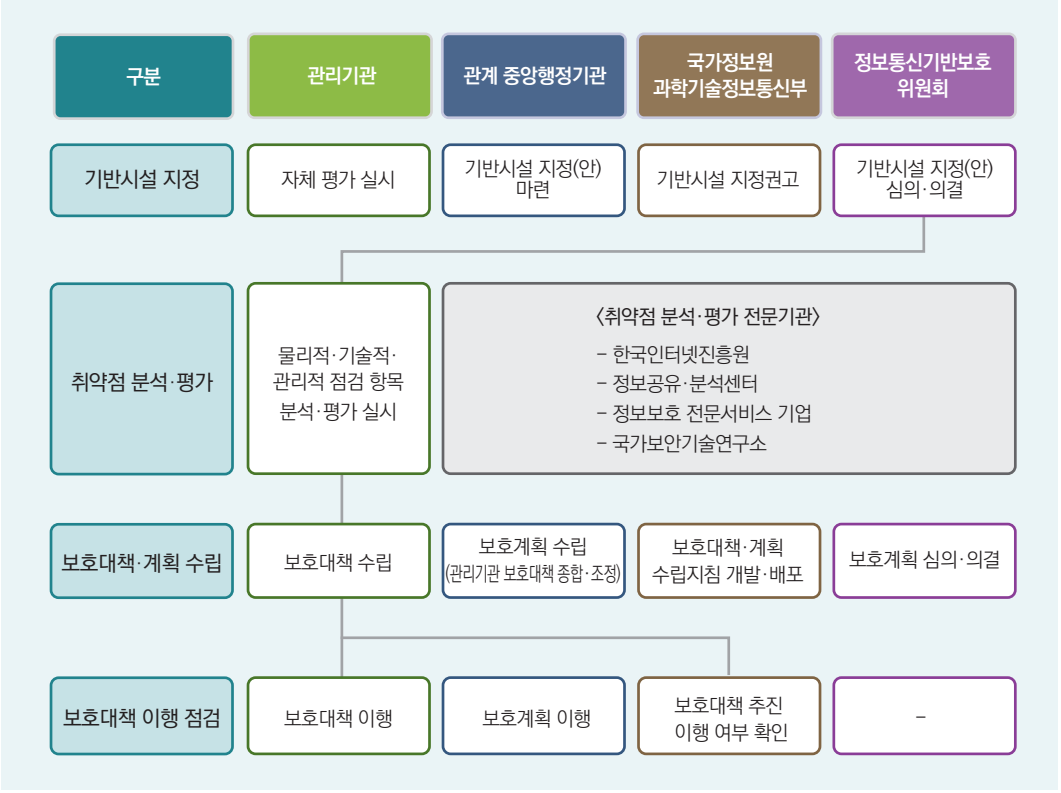
관리기관의 장은 「정보통신기반 보호법」 제9조에 따라 취약점 분석·평가를 위하여 내부 전담반을 구성하여 소관 시설에 대한 취약점 분석·평가를 수행하거나 한국인터넷진흥원, 국가보안기술연구소, ISAC, 정보보호 전문서비스 기업에 위탁할 수 있다.

과학기술정보통신부와 국가정보원은 최근 변화하는 사이버위협에 대비할 수 있도록 「주요정보통신기반시설 취약점 분석·평가기준」(과학기술정보통신부 고시 제2021-28호)을 개정하여 클라우드 시스템의 계정관리 등 보안관리를 위한 항목을 신설하고 기존 항목 중 유사하거나 중복되는 항목을 삭제하였다. 또한 개선이 불가능하여 별도 관리가 필요한 조치불가 취약점의 정의를 신설하고, 관리기관에 조치불가 취약점에 대한 보완대책을 요구하고 있다. 이에 대하여 과학기술정보통신부에서는 관리기관을 지원하기 위하여 주요정보통신기반시설 기술적 취약점 분석·평가 방법 상세가이드(2021. 3.)를 제작하여 한국인터넷진흥원 보호나라 홈페이지(www.boho.or.kr)를 통하여 배포하고 있다.

3. 보호계획 및 대책의 수립·시행과 이행 여부 확인

주요정보통신기반시설을 관할하는 관계 중앙행정기관의 장은 해마다 소관 분야 주요정보통신기반시설에 관한 보호계획을 수립·시행하여야 한다. 보호계획은 관리기관에서 제출한 보호대책을 종합·조정하여 작성한다. 그리고 관계 중앙행정기관의 장은 다음 연도의 보호계획과 정보통신기반시설의 신규 지정 안건 등을 정보통신기반보호위원회에 제출하여 심의를 받는다. 위원회에 제출된 보호계획은 심의과정을 통하여 종합·조정하도록 하고 있다.

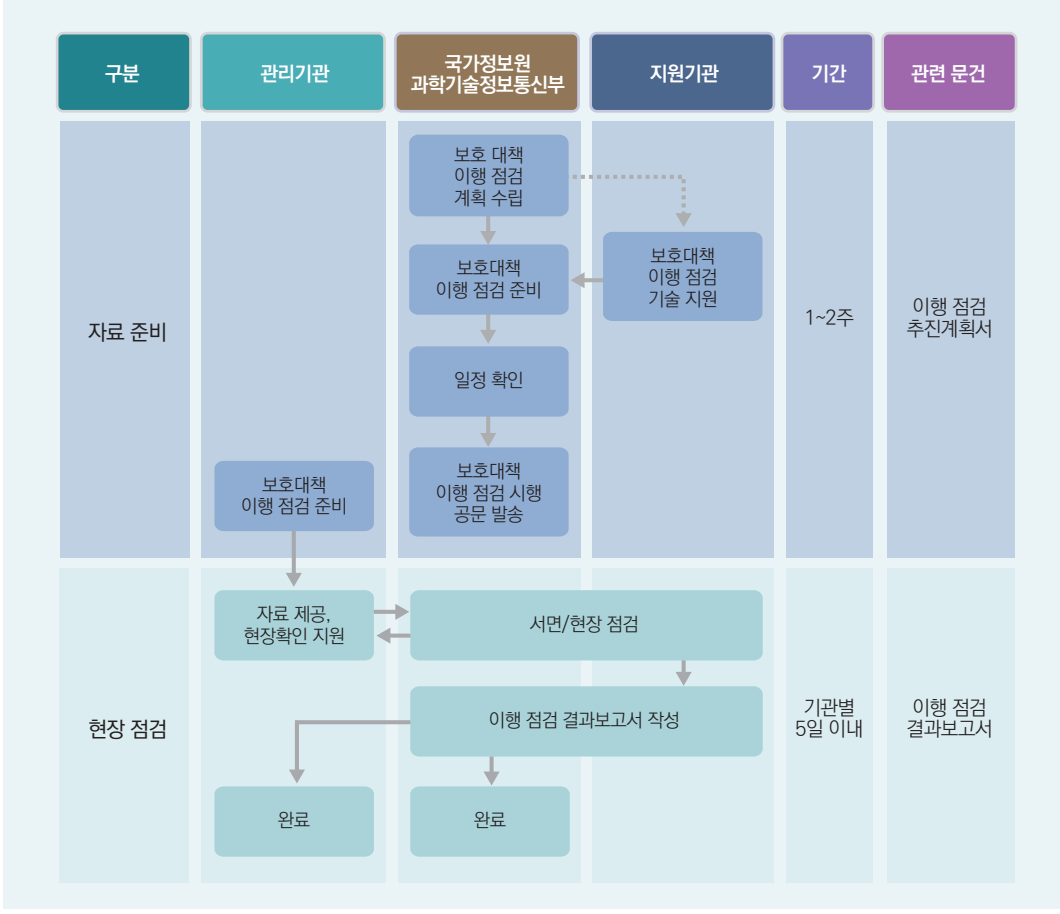
그림 3-3-2-3 주요정보통신기반시설 보호 업무 절차



국가정보원장과 과학기술정보통신부장관 등 대통령령으로 정하는 국가기관의 장은 관리기관에 대하여 주요정보통신기반시설 보호대책의 이행 여부를 확인할 수 있으며, 이행 여부 확인에 필요한 자료의 제출 및 보호조치의 세부적인 내용을 확인·점검할 수 있다. 보호대책 이행 여부는 서면 점검과 현장 점검으로 이루어지며, 점검 평가는 관리기관에서 제출한 보호대책 이행 평가와 보호대책 이행 여부 확인 항목에 기반한 이행 평가로 이루어진다. 또한 국가정보원장과

과학기술정보통신부장관은 주요정보통신기반시설 보호대책의 이행 여부 확인 결과를 정보통신기반보호위원회에 보고하여야 하며, 보완이 필요하다고 판단되는 관리기관에 대해서는 개선을 권고할 수 있도록 하고 있다.

그림 3-3-2-4 주요정보통신기반시설 보호대책 이행 여부 확인 절차



4. 인식제고

가. 주요정보통신기반보호 워크숍

2004년부터 국가정보원과 과학기술정보통신부는 주요정보통신기반시설 담당자의 정보보호 인식 제고 및 역량 강화를 위하여 주요정보통신기반보호 워크숍(WIPRO)을 해마다 개최하고 있다.

2022년에는 사회적 거리두기로 완화로 인하여 오프라인으로 진행하였으며, 122개 기관 216명의 기반시설 담당자가 참여하여 자율협력주행 등 신기술 발전으로 인한 기반보호 환경 변화에 따른 신규 보안정책 추진 현황을 공유하고 유공자 포상을 통하여 우수 인원을 격려하는 등 관계자 간 소통을 강화하였다.

그림 3-3-2-5 주요정보통신기반보호 워크숍

과학기술정보통신부 개회사

시상식

나. 기반보호포럼

2012년부터 공공분야 주요정보통신기반시설 관리기관 간 협력 강화 및 정보교류 확대를 위하여 기반보호포럼을 운영하고 있다.

2022년에는 공공분야 기반시설 담당자 130여 명이 참석하여 1박2일간 기술·사회 변화에 따른 기반보호 정책 추진 방향에 대하여 논의하여 발전방안을 수립하고 관련 정보공유를 통하여 주요 현안에 대한 기관 간 공감대를 형성하였다.

그림 3-3-2-6 기반보호포럼

참석자 기념촬영

주요현안 토의

다. 사이버공격 대응훈련

2022년 7월 기반시설 58개 관리기관의 130개 제어시스템을 대상으로 러시아-우크라이나 전쟁에서 발견한 디스크 파괴형 악성코드 감염 상황을 가정하여 사이버공격 대응 실전훈련을 실시하였다. 훈련 결과설명회를 개최하여 실제 사고 발생 시 훈련사항을 활용하도록 주요 우수사례를 공유하고 각 기관의 미진사항을 개선하도록 지원하였다.

제3절 국내외 침해사고 사례

과거에는 정보통신기반시설이 폐쇄망으로 운영되어 물리적 공격이나 조작 실수로 인한 피해 사례가 대부분이었다. 그러나 정보통신기반시설에 정보통신서비스가 도입되면서 해킹, 악성메일 및 랜섬웨어 유포 등 사이버공격으로 인한 피해가 자주 발생하고 있다. 침해사고는 전력·수자원·교통·금융 등 다양한 분야에 걸쳐 발생하고 있으며, 인명 및 경제적 손실을 포함하여 대규모의 피해를 일으키기도 한다.

표 3-3-3-1 국내외 정보통신기반시설 침해사고 사례

시기	발생국	사고 내용	비고
2003. 1.	미국	오하이오주 DAVIE-BESSE 원자력발전소의 사설 컴퓨터 네트워크에 슬래머웜이 침투하여 안전감시시스템이 5시간 동안 운행 정지	원자력
2007. 3.	미국	국토안보부(DHS) 주관 발전소 제어시스템 모의해킹에서 발전기 가동 사이클을 변경하여 발전기 파괴	전력
2007. 8.	미국	전직 직원이 캘리포니아주 TCCA 운하 제어시스템에 악성프로그램을 설치하여 운하 운영 마비, 5,000만 달러 이상 손실 발생	수자원
2008. 1.	폴란드	14세 소년이 TV 리모컨을 개조하여 트램 교차로를 불법 조작함으로써 4대의 트램 탈선 및 12명 부상	교통
2008. 5.	미국	회계감사원(GAO) 주관 미국 최대 국립전력회사 TVA사 제어시스템 모의해킹에서 인터넷 발전소 제어시스템 침투에 성공	전력
2008. 8.	튀르키예	석유송유관 카메라 통신 소프트웨어 취약점을 이용한 네트워크 침투로 알람 관리 네트워크 장애 발생 및 석유 압력 변조로 폭발 사고 유도	에너지
2009. 8.	러시아	수력발전댐의 터빈 제어시스템 장애로 인한 발전기 터빈 폭발로 75명 사망	수자원

시기	발생국	사고 내용	비고
2010. 7.	이란	원자력발전소 제어시스템에 스턱스넷 바이러스가 침입하여 나탄즈 원자력 원심분리기의 일부 기능 마비	원자력
2011. 11.	미국	일리노이주 상수도시설 시스템 침투로 펌프 작동 시스템이 파괴	수자원
2012. 5.	이란·수단·시리아 등	중동국가의 컴퓨터가 해킹되어 중요 데이터 유출·파괴	국가주요시설
2012. 10.	미국	전력시설 터빈 제어시스템이 악성코드에 감염되어 3주간 운영 중단	전력
2013. 3.	한국	방송 및 금융 등 다수 기업 전산망에 악성코드로 인한 시스템 파괴 등 장애가 발생하여 PC 및 시스템 4만 8천여 대 피해 발생	방송 금융
2014. 1.	일본	후쿠이현 몬주 핵발전소 내 관리자 PC가 바이러스에 감염되어 교육·훈련보고서, 조직 변경 홍보 메일 등 사내 데이터 유출	원자력
2014. 12.	독일	철강회사의 용광로 제어시스템에 장애 발생	철강
2015. 12.	우크라이나	전력발전소에 악성코드 침투로 제어시스템 서비스가 중단되어 8만여 가구에 정전 발생	전력
2016. 10.	미국	호스팅업체 DYN사의 DNS 서비스가 디도스 공격으로 웹사이트 접속 장애 발생	통신
2017. 6.	일본	혼다모터스 사야마 공장에 워너크라이 랜섬웨어가 유포되어 48시간 동안 생산 중단	일본
2018. 1.	일본	가상화폐거래소 코인체크사가 해킹되어 580억 엔 피해 발생	금융
2018. 5.	멕시코	은행 5곳이 해킹되어 1,540만 달러가 가짜계좌로 인출되는 사고 발생	금융
2018. 11.	미국	HSBC은행 미국 지점에서 신원 미상의 해커가 고객의 온라인 계정에 불법 접근하여 일부 정보 유출	금융
2019. 1.	미국	오클라호마 보안부에서 RSYNC 서비스를 통하여 FBI 수사자료 등 유출	행정
2019. 3.	미국	태양광·풍력 에너지 공급기업 에스파워가 시스코 방화벽 취약점으로 디도스 공격을 받아 발전설비 및 12개 회사와 연결 중단	에너지
2019. 5.	미국	볼티모어에서 랜섬웨어 공격을 받아 파일이 암호화되는 피해 발생	행정
2019. 7.	남아공	요하네스버그 전력공급사 시티파워를 대상으로 랜섬웨어 공격이 발생, 대부분 지역에서 정전사태가 발생하고 전기료 납세 행정처리 마비	전력
2020. 7.	남아공	요하네스버그 전력공급사 시티파워를 대상으로 랜섬웨어 공격이 발생, 대부분 지역에서 정전사태가 발생하고 전기료 납세 행정처리 마비	전력

시기	발생국	사고 내용	비고
2020. 9.	독일	신원 미상의 해커가 뒤셀도르프 대학병원 망에 랜섬웨어를 감염시켜 서비스 중단 및 중증환자 1명을 다른 병원으로 후송 도중 사망 사고 발생	병원
2020. 10.	인도	뭄바이시가 사이버공격으로 송전 시스템, 교통 시스템, 열차 운행이 마비되었으며, 도시 운영에 꼭 필요한 시스템을 복구하는 데 2시간, 나머지 영역을 복구하는 데 12시간 이상 소요	전력
2020. 12.	영국	스코틀랜드 지역 전력공급 업체 피플에너지사가 해킹 공격을 받아 27만 명의 개인정보 유출	전력
2021. 2.	미국	플로리다주 상수도 공급 시설이 해커 공격에 노출되어 화학물질 농도가 급격히 높여졌으나 직원이 마우스 움직임을 감지한 후 차단	수자원
2021. 5.	미국	송유관 업체 콜로니얼 파이프라인사가 랜섬웨어에 감염되어 며칠 동안 송유관 가동 중단	에너지
2021. 5.	한국	한국원자력연구원을 대상으로 사이버공격 발생, 연구로 핵연료부를 포함한 직원 이메일, RODS, 휴대전화 번호, 계정정보 등이 도난됨.	원자력
2021. 6.	오스트레일리아	세계 최대 육가공 업체 JBS푸드사가 랜섬웨어 공격을 받아 육류 가공 생산 차질	육가공
2022. 2.	독일, 벨기에, 네덜란드	독일(오일탱킹)·벨기에(씨인베스트·네덜란드(이보스) 등 유럽 내 정유회사가 사이버공격을 받아 시스템 가동이 중단되어 석유를 저장·운송하는 시설에 피해 발생, 석유 공급에 차질	에너지
2022. 5.	잠비아	중앙은행이 랜섬웨어 공격을 받아 모니터링 시스템 및 웹사이트 등 손상	금융

제4장

정보통신서비스

제1절 침해사고 대응

1. 종합상황실 운영

과학기술정보통신부와 한국인터넷진흥원은 민간분야의 인터넷 침해사고 사전예방 및 사고 발생 시 신속한 대응과 피해확산방지를 위하여 인터넷침해대응센터를 운영하고 있으며, 국내 인터넷상 이상징후 모니터링 및 침해사고 발생 시 대응, 국내외 유관기관과 협력 및 공동대응 등 다양한 활동을 수행하고 있다.

인터넷침해대응센터 종합상황실은 국내 인터넷망의 트래픽 소통 현황과 주요 DNS (Domain Name System) 서비스 상태, 국내 주요기관(정부·공공·금융 등)의 웹서버 접속 상태 등을 365일 24시간 상시 모니터링하고, 디도스 공격이나 피싱·스미싱 사고, 홈페이지 변조 등에 대한 신고접수·탐지 및 초동 대응을 수행하는 한편, 신규 악성코드와 보안 취약점에 대한 국내 위험도를 평가하여 수준별 대응·조치를 실시하고 있다.

대통령 선거, 2022 월드컵 등 사회적 이슈를 노린 사이버공격 발생에 대비하여 비상대응 체계(이상징후 모니터링 강화, 유관기관 핫라인 운영을 통한 협력 강화, 침해사고 원인 분석 및 기술지원 등)를 운영하였다. 또한 러시아-우크라이나 전쟁, 카카오서비스 장애 등 이례적 사고

발생 시에도 비상대응 체계(백신사와 협력, 이슈 관련 스미싱 문자 및 중앙재난안전대책본부 사칭 악성코드 실시간 탐지 및 긴급차단 등)를 운영하여 사이버공격에 선제적으로 대응하였다. 이 밖에도 주요 정보통신서비스제공 사업자(ISP, IDC, 이동통신사, MSO 등), 보안업체·유관기관 등과 정보보호 주요 현안에 대한 정보 공유 및 비상시 긴급대응을 위한 침해대응 협력 체계를 긴밀히 유지하였다.

2. 홈페이지 은닉 악성코드 탐지 및 대응

홈페이지를 통하여 악성코드를 유포하는 사례가 발생하면서 2006년부터 악성코드 은닉사이트 탐지 및 대응 활동을 지속하고 있다. 또한 웹하드 사이트의 전용프로그램 및 국내 무료 배포 소프트웨어(약 200여 개) 위·변조 점검 등을 통하여 악성코드 탐지 및 대응을 강화하고 있다.

악성코드 은닉사이트 탐지 시스템은 2006년부터 7만 7천 개 홈페이지를 점검 대상으로 시작하여 점검 도메인을 지속적으로 확대하였다. 2022년에는 430만 개 홈페이지를 대상으로 점검을 실시하였다.

표 3-4-1-1 악성코드 은닉사이트 점검 대상

(단위: 만 개)

연도	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
점검 대상	7.7	10	12	20	100	180	200	230	250	280	340	370	340	380	400	410	430

※ 국내 도메인 430만 개 : ccTLD(.kr, 한국) 340만 개, gTLD(.com, .net, .name 등) 90만 개

악성코드 은닉사이트 탐지 건수는 2021년 대비 93%(2021년 7,043건 → 2022년 13,661건) 증가하였다.

표 3-4-1-2 연도별 악성코드 은닉사이트 탐지·대응 건수

(단위: 건)

연도	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
유포지	993	1,619	1,324	1,731	1,434	1,433	3,270	4,472	2,583	3,295	1,370	1,197	856	566	738	2,584	4,354
경유지	5,624	3,932	7,654	5,621	5,240	10,372	9,748	13,278	45,120	43,555	9,674	12,150	13,898	7,733	5,296	4,459	9,307
합계	6,617	5,551	8,978	7,352	6,674	11,805	13,018	17,750	47,703	46,850	11,044	13,347	14,754	8,299	6,034	7,043	13,661

※ 유포지 : 악성코드 유포 홈페이지
※ 경유지 : 인터넷 이용자를 유포지로 유도하는 홈페이지

홈페이지를 통하여 유포된 악성코드 유형은 주로 계정 정보 유출형 및 기기 정보 유출형(74%)이 가장 높았으며, 이 밖에도 추가 악성코드를 설치하는 다운로더(12%), 원격제어(5%), 가상통화 채굴(4%) 등의 순으로 나타났다.

국외 유포지의 경우에는 국내 주요 인터넷서비스 제공자(ISP, Internet Service Provider)와 공조를 차단함으로써 국내 이용자의 접속이 불가능하도록 조치하였다. 또한 경유지의 경우에는 해당 홈페이지 운영자에게 전화·메일·공문을 통하여 악성코드 유포에 이용되고 있음을 알려 주고 악성코드 삭제 등 보안조치를 하도록 권고하였다.

3. 디도스 공격 대응

디도스 공격은 홈페이지 등 서비스를 제공하는 시스템이나 네트워크에 과부하를 일으켜 정상적인 서비스를 제공하지 못하도록 하는 공격 유형으로 접속장애 등 직접적인 피해를 일으킨다. 디도스 공격은 해커의 조종을 받는 감염PC로부터 공격이 시작되기 때문에 피해를 최소화하기 위해서는 공격트래픽 차단과 함께 감염PC에 대한 조치가 이루어져야 한다.

한국인터넷진흥원은 공격 대상 웹사이트로 향하는 공격트래픽을 우회시켜 일반 사용자가 웹사이트를 정상적으로 이용할 수 있도록 지원하는 디도스 사이버대피소를 운영하고 있다.

2009년 3.4 디도스 공격 발생 이후 사이버대피소 서비스의 필요성을 인식하고, 2010년 시스템을 구축하였다. 서비스를 개시한 이후 2022년까지 사이버대피소 서비스 총 33,874건을 제공하였으며, 총 1,458건의 디도스 공격을 방어하였다.

표 3-4-1-3 사이버대피소 서비스 현황

(단위: 건)

연도	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	합계
서비스 이용 업체	52	101	175	260	413	593	1,012	1,640	2,854	3,839	4,590	7,271	11,074	33,874
디도스 공격 방어	25	60	138	116	110	83	96	87	126	167	235	108	107	1,458

또한 한국인터넷진흥원은 침해사고에 악용되어 공격을 유발하는 PC 사용자에게 감염사실을 직접 통보하고, 맞춤형 전용백신을 제공하여 보다 체계적으로 감염PC를 치료하는 서비스를

제공하고 있다. 감염PC 사용자가 감염사실을 인지할 수 있도록 웹브라우저를 사용하여 인터넷 접속 시 팝업창을 띄워 감염사실을 통보하며, 해당 PC를 감염시킨 악성코드를 치료할 수 있는 맞춤형 전용백신을 동시에 제공하여 치료를 유도하고 있다.

2022년 총 856회의 치료 안내를 하였으며, 207,766건 감염PC 대상 감염 알림을 하였고, 총 177종의 전용백신을 제작·배포하였다.

표 3-4-1-4 감염PC 사이버 치료 체계 운영 현황

(단위: 건, 종)

연도	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	합계
감염 알림	9,404,759	61,347	64,206	248,281	110,413	47,776	124,310	106,525	267,456	381,492	135,747	207,766	11,160,078
전용 백신 제작	54	51	57	67	74	82	92	103	113	127	144	177	1,141

4. 전자금융사기(피싱, 파밍, 스미싱) 대응

가. 피싱 대응

피싱(phishing)은 개인정보(private data)와 낚시(fishing)의 합성어로, 금융기관 또는 공공기관 등을 사칭하여 전화나 이메일로 피싱 사이트 접속을 유도하여 개인정보(ID/PW) 또는 금융정보(보안카드, 공인인증서 정보) 등을 입력하도록 요구하여 사용자의 중요한 정보를 몰래 빼가는 수법이다.

한국인터넷진흥원은 사이버 사기 대응 체계를 통하여 정상 사이트를 사칭하여 이용자를 속이고 개인정보 및 금융정보를 탈취하는 피싱 사이트를 지속적으로 탐지하고 있다.

한국인터넷진흥원은 신고·접수된 피싱 사이트 도메인 중 다수가 .com과 .net을 사용하는 점에 착안하여 .com, .net 도메인 등록업체인 베리사인(VeriSign)과 협력하여 신규 등록 도메인을 대상으로 피싱 여부를 탐지·차단할 수 있는 시스템을 구축하였다. 2014년에는 신규 등록되는 .kr 도메인도 조사하여 피싱 사이트를 사전에 탐지할 수 있도록 시스템을 고도화하였다.

나. 스미싱 대응

2012년부터 등장하기 시작한 스미싱(smishing)은 SMS와 피싱의 합성어로, 신뢰할 수 있는 사람·기업·공공기관 등이 보낸 것처럼 가장한 휴대전화 문자에 악성앱의 링크(URL)를 포함시켜 사용자의 스마트폰에 악성앱을 설치하도록 유도하는 수법이다. 스마트폰 보급이 증가함에 따라 스미싱 악성앱의 악성행위는 진화되고 있으며, 이용자의 안전한 모바일 이용을 위협하고 있다. 이러한 스미싱으로 인한 국민 피해를 최소화하기 위하여 2014년부터 스미싱 대응 체계를 구축·운영하고 있다.

한국인터넷진흥원은 스미싱 피해를 최소화하기 위하여 기술적·정책적 대응활동을 수행하고 있다. 기술적 대응으로는 스미싱 대응시스템과 사이버트랩시스템을 구축·운영하고 있다. 스미싱 대응시스템은 다양한 신고 채널에서 스미싱 의심 문자를 수집하고, 악성앱 다운로드 여부를 분석한다. 사이버트랩시스템은 신고 채널에 의존하는 스미싱 대응시스템의 한계를 극복하기 위하여 가상의 허니팟용 개인정보를 생성·노출하여 전자금융사기 의심 정보를 선제적으로 수집한다. 대응시스템에서 수집·분석된 악성앱 유포지나 정보 유출지는 스미싱 피해 방지를 위하여 차단하고 있다.

정책적 대응으로는 '후후', '알약M2.0' 업체와 협력하여 이용자가 문자메시지에 악성으로 의심되는 정보가 있어 신고할 경우 이를 분석하여 스미싱 여부를 답변해 주는 서비스를 제공 중이다. 또한 스미싱 판정 정보를 이동통신사 등에 제공하여 스미싱 탐지에 활용할 수 있도록 데이터 개방을 추진하였다.

5. 모바일 악성코드 대응

2012년 하반기부터 모바일 악성코드(악성앱)가 본격적으로 유포되기 시작하고 2013년부터 급증함에 따라 2014년 모바일 악성앱에 감염된 좀비 스마트폰을 대상으로 감염알림 및 치료제공이 가능한 '모바일 응급 사이버 치료 체계'를 시범 구축하였으며, 2015년부터 이동통신3사(SKT, KT, LGU+)를 대상으로 악성앱 감염 스마트폰 치료서비스를 제공하였다.

모바일 응급 사이버 치료 체계는 이동통신사와 협조를 통하여 이동통신 가입자를 대상으로 제공되며, 탐지한 악성앱의 유포지, 정보유출지, C&C정보를 바탕으로 이동통신사가 감염의심

스마트폰을 식별하여 감염사실을 알리고 악성앱에 대한 치료서비스를 제공한다. 감염알림은 스마트폰에 기본 탑재되는 보안앱 또는 문자메시지를 통하여 전송되며, 사용자의 스마트폰에 설치된 악성앱을 삭제하여 치료서비스를 제공한다. 2022년에는 좀비 스마트폰 5,187건을 찾아 내어 감염사실을 안내하였다.

표 3-4-1-5 모바일 응급 사이버 치료 체계 운영 현황

(단위: 건)

연도	2015	2016	2017	2018	2019	2020	2021	2022	합계
통보 건수 (단말기 기준)	24,517	27,608	47,152	20,277	29,752	54,533	43,797	5,187	252,823

* 악성앱 유포 트렌드가 기존 문자 내 다운로드 유도 방식에서 카톡 등 SNS 메신저를 통한 유포 방식으로 변경되는 추세로, 2022년 통보 건수가 2021년에 비하여 감소

제2절 침해사고 예방

1. 국내 활동

한국인터넷진흥원은 주요 정보통신서비스제공 사업자(ISP, IDC, 이동통신, MSO 등 기간통신사업자), 보안 관련 업체 및 유관기관 등과 사이버위협 공동 대응, 소통을 통한 현장 중심 침해대응 정책 수립, 정보공유 강화를 통한 사이버 방어 체계 구축 등 침해대응 협력 체계를 긴밀히 유지하고 있다.

가. 사이버위협 인텔리전스 네트워크 운영

2014년 12월부터 사이버위협에 공동 대응하기 위한 민·관 인텔리전스 구축의 필요성에 따라 한국인터넷진흥원은 국내 보안업체(안랩, 이스트시큐리티, 하우리, 잉카인터넷, NSHC, 빛스캔)와 함께 '사이버위협 인텔리전스 네트워크'를 구성·운영하였다. 2023년 사이버공격을 전망하고 '22 사이버위협 분석 및 23년 전망분석 보고서'를 공동 발표하였다.

나. 사이버위협 정보 분석·공유 시스템 운영

한국인터넷진흥원은 사이버공격에 효과적으로 대응하기 위하여 2014년 8월부터 사이버위협

정보 분석·공유(C-TAS, Cyber Threat Analysis & Sharing) 시스템을 운영하고 있다. 2022년 12월 말 기준 정보통신·제조·금융업 등 총 2,161개 기업이 참여하고 있으며, 4억 2천 5백만여 건의 사이버위협 정보를 공유하고 있다.

C-TAS에 참여하는 회원사는 공유된 악성코드 및 사이버위협 정보를 분석하고 특징을 추출하여 보안제품 업데이트 등에 사용하고 있으며, 악성URL 및 IP정보는 자사 보안정책에 적용하여 유해 트래픽 차단에 활용하고 있다.

C-TAS는 더 많은 기업이 사이버위협 대응에 참고할 수 있도록 2021년 12월, 개방형 체계로 전환하면서 보안실무자와 관리자 등 직급과 업무 특성에 따른 다양한 형태의 맞춤형 정보를 제공하고 있다. 또한 문자(SMS)나 알림톡(SNS)를 통하여 긴급 대응이 필요한 정보 제공 등 긴급 상황 전파 체계 서비스도 제공하고 있다.

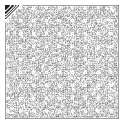
다. 사이버보안빅데이터센터 운영

한국인터넷진흥원은 고도화된 보안위협에 인공지능·빅데이터 등 지능정보기술을 활용하여 사이버위협을 선제적으로 예방·탐지하고 대응할 수 있도록 2018년 12월 사이버보안빅데이터센터를 개소하였다.

사이버보안빅데이터센터는 기존 C-TAS에서 수집하는 위협정보를 포함하여 국내외 공공분야 및 상용·오픈 인텔리전스 서비스 등 다양한 채널의 위협정보를 수집하고 있다.

2021년부터 민간분야 지능정보기술 적용 촉진 및 사이버 침해사고 대응 업무 지능화를 위하여 악성코드, 침해사고 분야 AI데이터셋 2종 구축에 이어 2022년에도 산·학·연 수요조사, 전문가 자문을 통하여 애플리케이션 보안, 능동형 보안관제, 위협 프로파일링 3종 AI데이터셋을 구축하여 개방을 앞두고 있다. 단순히 위협정보를 수집할 뿐 아니라, 인공지능 데이터셋 구축의 모든 주기(수집 → 가공 → 라벨링)에 대한 과업을 수행하여 보안분야 외 공공·통신 등 희망 기업 대상으로 데이터셋을 개방하여 민·관 협업 기반 보안성 강화를 지원하고 있다.

또한 기업·학교·연구소 등 보안에 관심 있는 누구나 사이버보안빅데이터센터에서 위협정보를 분석할 수 있도록 기존 플랫폼을 개선한 '사이버보안 인공지능·빅데이터 활용



플랫폼'을 제공한다. 지능형 보안기술 연구개발에 필수적인 ▲양질의 데이터셋 ▲인공지능·빅데이터 분석도구 ▲GPU 자원 등 인공지능 분석 환경을 온·오프라인으로 제공하여 사이버보안 인공지능·빅데이터 활용 촉진을 위하여 노력하고 있다.

사이버보안빅데이터센터에서는 국민 참여를 바탕으로 인공지능·빅데이터 활용 역량을 강화하기 위하여 사이버보안 인공지능·빅데이터 활용 경진대회를 개최하고 있다. 집단 지성을 이용한 인공지능·빅데이터 분석·활용, 신모델 발굴 및 성과공유를 통하여 보안 분야 빅데이터 활용에 대한 저변 확대를 지속적으로 추진하고 있다.

라. 지역정보보호센터 운영

한국인터넷진흥원은 지역의 열악한 정보보호 환경을 개선하고자 2014년부터 지방자치단체와 연계하여 현재 전국 10곳*에 정보보호지원센터를 운영하고 있다.

* 인천, 대구, 호남, 중부, 동남, 경기, 울산, 강원, 경북, 충남

정보보호지원센터에서는 중소기업의 정보보호 수준을 제고하기 위하여 정보보호 의지가 있으나 예산·인력 부족으로 자발적인 정보보호 활동이 어려운 ICT중소기업을 대상으로 정보보호 컨설팅 및 컨설팅 결과조치를 위한 보안솔루션 도입비용을 지원하고 있으며, 소규모의 ICT인프라 자산으로 컨설팅조차 어려운 영세한 기업을 대상으로 클라우드 기반의 보안서비스도 지원하고 있다.

또한 지역 중소기업 재직자와 정보보호 관련학과 대학생에게 정보보호 전문교육을 무료로 지원하고 있으며, 초급과 중급 수준으로 분류하여 참여 인원 수준에 맞는 맞춤형 교육을 제공하고 있다.

제3절 정보보호 및 개인정보보호 관리 체계 인증

1. 개요

블록체인·클라우드·5G·사물인터넷 등 4차 산업혁명 시대에 신기술 발전은 우리 생활의 모든 영역에 영향을 미치고 있다. 새로운 기술이 실생활에 밀접해지면서 중요도가 높아짐에 따라 카드사 개인정보 대규모 유출, 가상자산거래소 해킹, 클라우드 장애에 의한 서비스 마비 등 다양한 위협이 증가하였다. 사이버공격은 기업의 기밀이나 개인정보 등의 특정 정보를 목표로 지능화·고도화하고 있으며, 이에 따른 피해는 기업의 첨단 기술과 개인정보의 유출, 기업의 신뢰도 하락과 고객 이탈, 주가 하락뿐 아니라 집단소송과 대규모 피해보상 등 사회적·경제적 측면에서 큰 문제를 일으키고 있다. 이러한 문제를 해소하기 위하여 기술적 대책, 일회성 관리, 부분적 보완에 그치지 않는 근본적인 해결방안이 필요하게 되었다.

정보보호 및 개인정보보호 관리 체계(ISMS-P, Personal Information & Information Security Management System) 인증은 기업 또는 기관이 사이버공격 및 개인정보 유출을 예방하기 위하여 수립하는 관리 체계에 대한 표준 모델과 인증기준을 제시한다. 인증을 희망하는 기업 또는 기관은 독립적이고 객관적인 입장에 있는 제3의 인증·심사기관을 통하여 정보보호 및 개인정보보호 관리 체계가 지속적으로 운영하기에 적합한지, ISMS-P 인증기준을 준수하고 있는지에 대하여 심사받고 인증을 획득하게 된다. 인증제도의 공정성과 객관성을 확보하기 위하여 한국인터넷진흥원이 법정인증기관으로 그 역할을 수행하고 있으며, 과학기술정보통신부장관이 지정한 금융보안원도 인증기관의 업무를 수행하고 있다. 심사기관으로는 한국정보통신진흥협회·한국정보통신기술협회·개인정보보호협회·차세대정보보안인증원이 지정되었다. 지속적인 인증 대상 및 분야 증가에 따라 인증기관과 심사기관을 점차 확대할 계획으로, 2021년부터는 심사기관을 희망하는 기관의 신청을 통하여 상시 지정하는 절차를 운영하고 있다.

2001년 ISMS 인증제도가 도입된 후 2002년 최초 인증서가 발급되었다. 2013년 일정 규모 이상의 주요정보통신서비스 제공자 등이 ISMS 인증 의무 대상자로 지정되었다. 2016년에는 매출액 또는 세입 1,500억 원 이상인 상급종합병원과 재학생 수 1만 명 이상의 대학교 등 비영리 분야로 의무 대상자가 확대되었다.

정보보호와 개인정보보호의 연계 필요성이 제기되어 2018년 정보보호 관리 체계(ISMS)와 별도로 운영되던 개인정보보호 관리 체계(PIMS, Personal Information Management System)를 통합하여 ISMS-P 인증 등에 관한 고시를 개정하고 통합인증제도를 시행하였고, 가상자산·클라우드 인프라 등 새로운 기술의 등장에 효과적으로 대응하기 위하여 고시를 개정하였다.

2021년 「특정금융정보법」이 개정됨에 따라 가상자산사업자에게도 ISMS 인증 신고 의무를 이행할 수 있도록 예비인증 특례(ISMS-P 인증고시 제18조의2 신설, 2022. 7. 21. 시행)를 도입하였다.

이에 따라 신규 가상자산사업자의 시장진입의 교두보를 마련하고, 이용자가 가상자산 서비스를 안전하게 이용할 수 있도록 하였다.

그림 3-4-3-1 ISMS-P 인증 개요

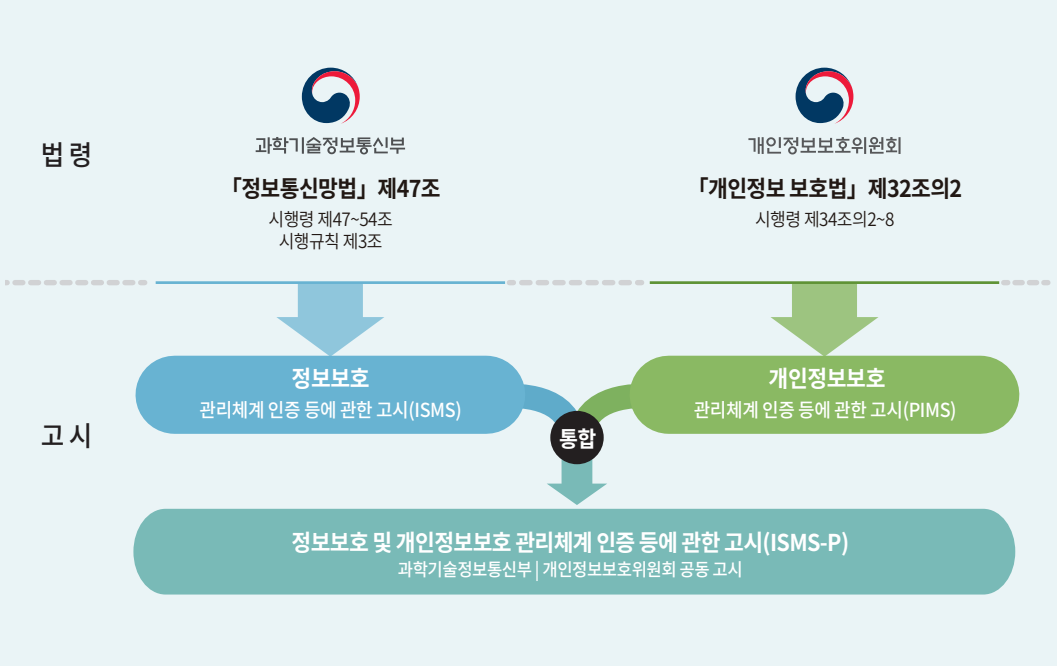


표 3-4-3-1 ISMS-P 인증제도

연도	내용
2001	• ISMS 인증제도 도입(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조)
2002	• 인증심사 기준 고시(정보통신부고시 제2002-22호) • 최초 인증서 발급
2004	• 정보보호 안전진단제도 도입(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제46조의3)
2011	• ISMS 인증기준 개정(기존 : 137개 통제항목 → 개정 : 104개 통제항목) • PIMS 인증제도 도입
2013	• 정보보호 안전진단제도를 ISMS 인증제도로 일원화 • 주요정보통신서비스 제공자 등을 의무 대상자로 지정 • ISMS 인증제도와 G-ISMS 인증제도의 일원화 • PIMS 시행(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조의3)
2014	• ISMS 심사기관 지정 ※ 한국정보통신진흥협회(2014. 5.), 한국정보통신기술협회(2015. 2.)
2015	• ISMS 인증기관 추가 지정 ※ 금융보안원(2015. 7.)
2016	• 의료·교육분야로 ISMS 인증 의무 대상 확대 ※「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조 및 시행령 제49조
2018	• ISMS와 PIMS 인증제도 통합 ※「정보보호 및 개인정보보호 관리 체계 인증 등에 관한 고시」(과학기술정보통신부 고시 제2018-80호) 개정(2018. 11.)
2019	• ISMS-P 인증기관, 심사기관 지정 ※ 인증기관(금융보안원), 심사기관(한국정보통신기술협회, 한국정보통신진흥협회)(2019. 7.)
2020	• ISMS-P 심사기관 지정 ※ 개인정보보호협회(2020. 2.)
2021	• ISMS-P 심사기관 상시지정, 사후관리, 재난재해 발생 시 예외조항 신설 등 제도개선 ※「정보보호 및 개인정보보호 관리 체계 인증 등에 관한 고시」(과학기술정보통신부 고시 제2021-27호) 개정(2021. 3.)
2022	• 정보보호 관리 체계 예비인증 특례 도입 등 제도개선 ※「정보보호 및 개인정보보호 관리 체계 인증 등에 관한 고시」(과학기술정보통신부 고시 제2022-46호) 개정(2022. 7.)

표 3-4-3-2 ISMS-P 인증서 유지 현황

(단위: 건)

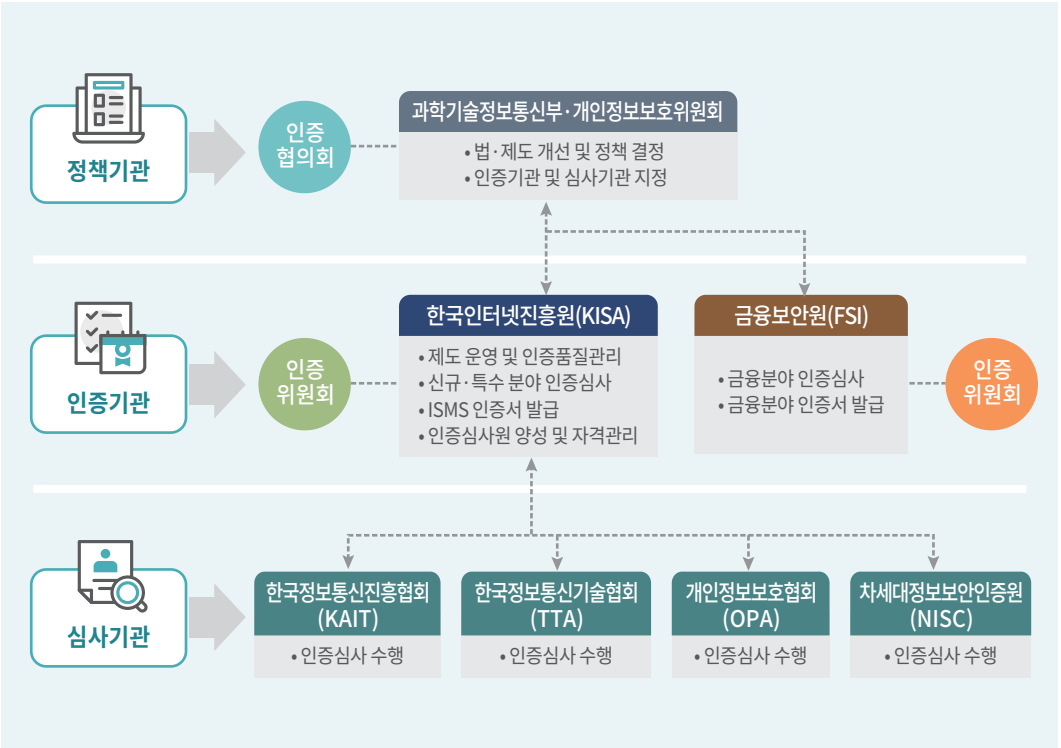
연도	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
(구) PIMS	28	27	41	63	71	76	35	22	137	-
(구) ISMS	272	377	415	470	517	601	584	349	10	-
ISMS-P	-	-	-	-	-	-	136	464	789	953
합계	300	404	456	533	588	677	755	835	936	953

2. 추진 체계

ISMS-P 인증 추진 체계는 정책기관(협의회), 인증·심사기관, 인증위원회 및 인증심사원으로 구성된다. 과학기술정보통신부와 개인정보보호위원회는 정책기관으로서 법·제도 개선 및 정책 결정, 인증·심사기관의 지정 및 감독 등의 역할을 수행하고 있으며, 한국인터넷진흥원은 법정인증기관으로서 인증심사, 인증위원회 운영, 인증서 발급·관리, 인증제도 및 기준 개선 등의 역할을 수행하고 있다.

인증위원회는 인증심사 결과의 심의·의결, 인증 취소의 타당성 등에 대하여 심의하며, 정보보호전문가·정보시스템감리사 등 정보보호 분야에 학식과 경험이 있는 35명 이내의 위원으로 구성된다. 인증심사원은 인증기관이 심사원 자격을 취득한 분야별 전문가 중에서 선정한다.

그림 3-4-3-2 ISMS-P 인증 추진 체계



3. 인증 대상과 절차

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제2항에 따라 의무 대상자는 ISMS 인증을 받아야 하며, ISMS-P 인증을 받은 경우에도 인증의무를 이행한 것으로 본다. 의무 대상자가 인증을 취득하지 않은 사실이 확인되는 경우 과태료가 부과된다.

표 3-4-3-3 ISMS 의무 대상자 기준

구분	의무 대상자 기준
ISP	「전기통신사업법」 제6조제1항에 따른 등록을 한 자로서 서울특별시 및 모든 광역시에서 정보통신망서비스를 제공하는 자
IDC	「정보통신망법」 제46조에 따른 집적정보통신시설 사업자
매출액 또는 이용자 수 요건에 따른 대상자	정보통신서비스 부문 전년도 매출액이 100억 원 이상인 자
	전년도 직전 3개월간 정보통신서비스 일일 평균 이용자 수가 100만 명 이상인 자
	연간 매출액 또는 세입이 1,500억 원 이상인 자 중에서 다음에 해당되는 경우 - 「의료법」 제3조의4에 따른 상급종합병원 - 직전연도 12월 31일 기준 재학생 수가 1만 명 이상인 「고등교육법」 제2조에 따른 학교

인증을 획득하고자 하는 사업자 및 기관은 개인정보의 흐름과 정보보호 영역을 모두 인증하는 경우 ISMS-P 인증, 정보보호 중심으로 인증하는 경우 ISMS 인증을 자율 판단하여 선택하고, 인증 대상 서비스 범위의 적절성을 한국인터넷진흥원 등 인증기관 또는 심사기관과 협의한다. 이후 구축하고 있는 ISMS의 적절성에 대하여 인증심사팀이 방문하여 서면·현장심사를 수행한다. 인증심사팀이 지적한 결함사항 등 심사 결과에 대하여 신청기관은 보완조치를 이행하고, 인증위원회에서 이를 심의하여 인증서를 발급한다.

그림 3-4-3-3 ISMS-P 인증 절차

4. 인증 기준

ISMS 인증은 관리 체계 수립 및 운영(16개)과 보호대책 요구사항(64개)으로 구성되어 있다. ISMS-P 인증기준은 ISMS 인증 기준(80개)과 개인정보 처리 단계별 요구사항(22개)으로 구성되어 있다.

표 3-4-3-4 ISMS-P 인증심사 기준

인증		구분	인증기준 분야별 개수	
ISMS-P (102)	ISMS (80)	1. 관리체계 수립 및 운영 (16)	1.1 관리체계 기반 마련(6)	1.2 위험관리(4)
			1.3 관리체계 운영(3)	1.4 관리체계 점검 및 개선
		2. 보호대책 요구사항 (64)	2.1 정책, 조직, 자산 관리(3)	2.2 인적보안(6)
			2.3 외부자 보안(4)	2.4 물리보안(7)
			2.5 인증 및 권한 관리(6)	2.6 접근통제(7)
			2.7 암호화 적용(2)	2.8 정보시스템 도입 및 개발 보안(6)
			2.9 시스템 및 서비스 운영관리(7)	2.10 시스템 및 서비스 보안관리(9)
			2.11 사고 예방 및 대응(5)	2.12 재해복구(2)
	–	3.개인정보 처리단계별 요구사항 (22)	3.1 개인정보 수집 시 보호조치(7)	3.2 개인정보 보유 및 이용 시 보호조치(5)
			3.3 개인정보 제공 시 보호조치(3)	3.4 개인정보 파기 시 보호조치(4)
			3.5 정보주체 권리보호(3)	

제4절 클라우드 보안인증제도

1. 개요

팬데믹 이후 오프라인에 있던 많은 부분이 온라인 서비스로 전환되면서 그 플랫폼으로 클라우드를 적극 활용하고 있다. 급속도로 증가하는 데이터 관리가 쉽고 서비스 구축비용을 절감할 수 있다는 장점으로 온라인 서비스 사업자의 클라우드 활용이 늘어나고 있는 만큼 클라우드 환경에서의 보안사고도 늘어나고 있는 추세이다. 이에 클라우드 보안인증을 통하여 클라우드 서비스 제공자의 보안수준을 제고하고 안전한 클라우드 서비스 제공을 위한 보안기준을 제시하고자 하였다.

클라우드 서비스 제공자는 「클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률」(이하 '클라우드컴퓨팅법') 제23조의2에 따라 클라우드 보안인증을 받을 수 있다. 클라우드컴퓨팅법 시행령 및 관련 고시에 따른 평가기관에서 클라우드 서비스의 정보보호 기준 적합 여부를 평가하고 인증기관을 통하여 인증서를 발급받을 수 있다. 특히 행정·공공기관 정보시스템의 클라우드 전환 등 클라우드 활성화 정책 방향에 맞추어 공공에서 활용될 민간 클라우드

서비스의 안전성과 신뢰성을 검증하기 위하여 활용되고 있으며, 궁극적으로는 객관적이고 공정한 클라우드 서비스 보안인증제도를 통하여 이용자의 보안 우려를 해소하고 국내 클라우드 서비스의 경쟁력을 확보하는 데 그 목적이 있다.

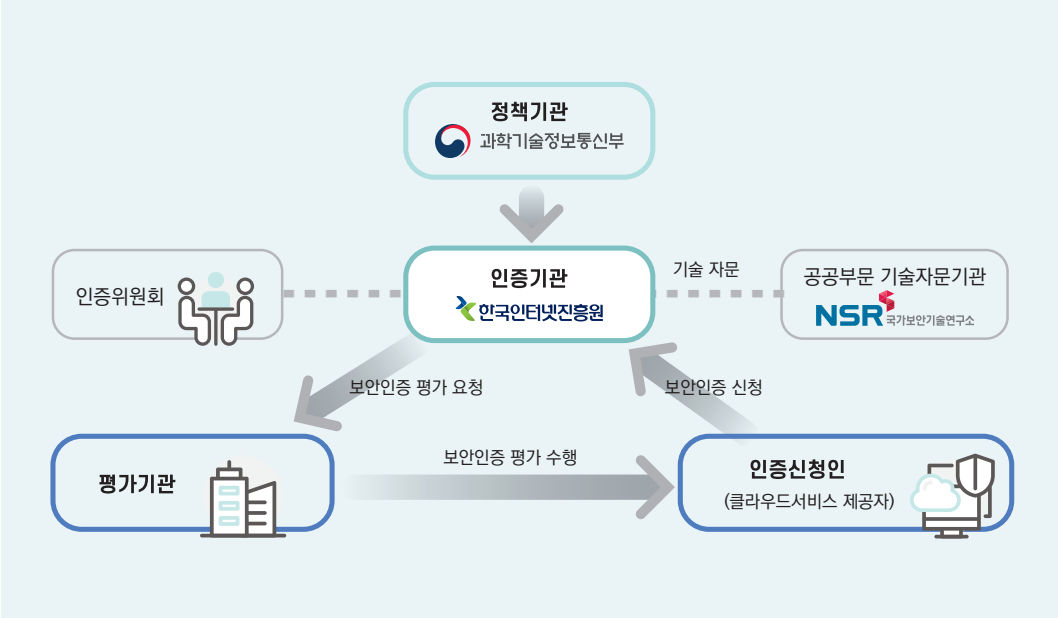
클라우드 보안인증제도는 2016년부터 시행되어 현재 총 82개의 서비스가 인증을 유지하고 있다.(2023년 2월 기준)

2. 보안평가·인증 체계

클라우드 서비스 보안평가·인증 체계는 역할과 책임에 따라 정책기관, 인증기관, 인증위원회, 기술자문기관, 평가기관, 신청기관, 이용자로 구분한다.

정책기관은 과학기술정보통신부로 법·제도 개선 및 정책 수립, 평가·인증기관 지정 등의 역할을 수행하며, 평가·인증기관은 한국인터넷진흥원 외 관련 고시에 따라 지정된 기관으로 인증평가, 인증서 발급 및 인증기준·지침 개발 등의 업무를 수행한다. 클라우드 관련 전문가 15인 이내로 구성한 인증위원회에서 평가결과를 심의·의결하며, 평가기준 개발·개정을 위하여 국가보안기술연구소의 자문을 받고 있다.

그림 3-4-4-1 클라우드 서비스 보안평가·인증 체계



3. 인증유형과 인증기준

클라우드 보안인증의 대상은 클라우드 컴퓨팅 기술을 이용하여 정보시스템의 인프라(IaaS)·개발환경(PaaS)·응용프로그램(SaaS) 중 어느 하나 이상을 제공하는 클라우드 서비스로, 클라우드 서비스 정보보호 수준에 따라 인증 유형 및 인증 등급을 선택하여 보안인증을 신청할 수 있다.

가. IaaS 보안인증

클라우드 서비스를 운영하기 위해서는 서버, 스토리지, 네트워크, 데이터베이스 등 여러 가지 인프라가 필요하다. 인프라스트럭처 서비스(IaaS, Infrastructure as a Service)는 이러한 것을 가상 환경에서 쉽고 편하게 이용할 수 있게 서비스 형태로 제공한다.

IaaS 인증은 이와 같은 환경에서 SaaS·DaaS 등의 사업자가 안심하고 사용할 수 있도록 관리적·물리적·기술적 보호조치 및 공공기관용 추가 보호조치 중심 총 116개로 이루어진 통제항목을 기준으로 평가한다.

나. SaaS 보안인증

클라우드 환경에서 동작하는 응용프로그램을 서비스 형태로 제공하는 것을 소프트웨어 서비스(SaaS, Software as a Service)라고 한다. 이를 활용하여 홈페이지, 화상회의 시스템, 전자결재 시스템 등 다양한 서비스 제공이 가능하다.

SaaS는 다양한 서비스 제공이 가능한 만큼 중요 데이터 기준으로 간편등급과 표준등급 2가지 형태로 인증제도를 운영하고 있다. 표준등급은 중요자료를 다루는 전자결재, 회계관리, 인적자원관리, 보안서비스, 플랫폼 서비스(PaaS, Platform as a Service) 5개 항목 중 1개 이상 포함하면 표준등급으로 인증을 받아야 한다. 그 밖의 서비스는 모두 간편등급으로 인증을 받을 수 있으며, 인증별로 표준등급 79개, 간편등급 31개의 통제항목이 있다.

다. DaaS 보안인증

데스크톱 서비스(DaaS, Desktop-as-a-Service)는 가상 PC환경을 원격으로 제공하는 클라우드 서비스이다. 네트워크를 통하여 개인 PC환경에 접속이 가능해지면서 개인 업무 환경을 언제 어디서나 다양한 기기에서 접속 가능한 것이 장점이다.

코로나로 인하여 재택근무가 활성화되면서 DaaS를 활용하여 회사 업무망에 접속하는 사례가 증가하고 있다. 회사에서 사용하는 망을 외부에서 접근이 가능한 만큼 회사 내부 자료가 외부로 유출될 가능성도 적지 않다. 이러한 환경에서 보안성을 확보하기 위하여 통제항목 110개 기준으로 보안인증을 시행하고 있다.

라. 클라우드 보안인증 등급제 도입

민간 클라우드 이용 활성화 등을 지원하기 위하여 그 동안 획일적으로 운영되던 보안인증 체계를 개선하여 2023년 상·중·하 등급제를 도입하였다. 하등급은 개인정보를 포함하지 않고 공개된 공공 데이터를 운영하는 클라우드 서비스로 상반기부터 평가·인증을 시행하며, 비공개 업무자료, 민감정보 등을 포함하는 상·중등급의 클라우드 서비스는 실증과 검증을 통하여 2023년 내 시행할 예정이다.

표 3-4-4-1 클라우드 서비스 보안인증 기준

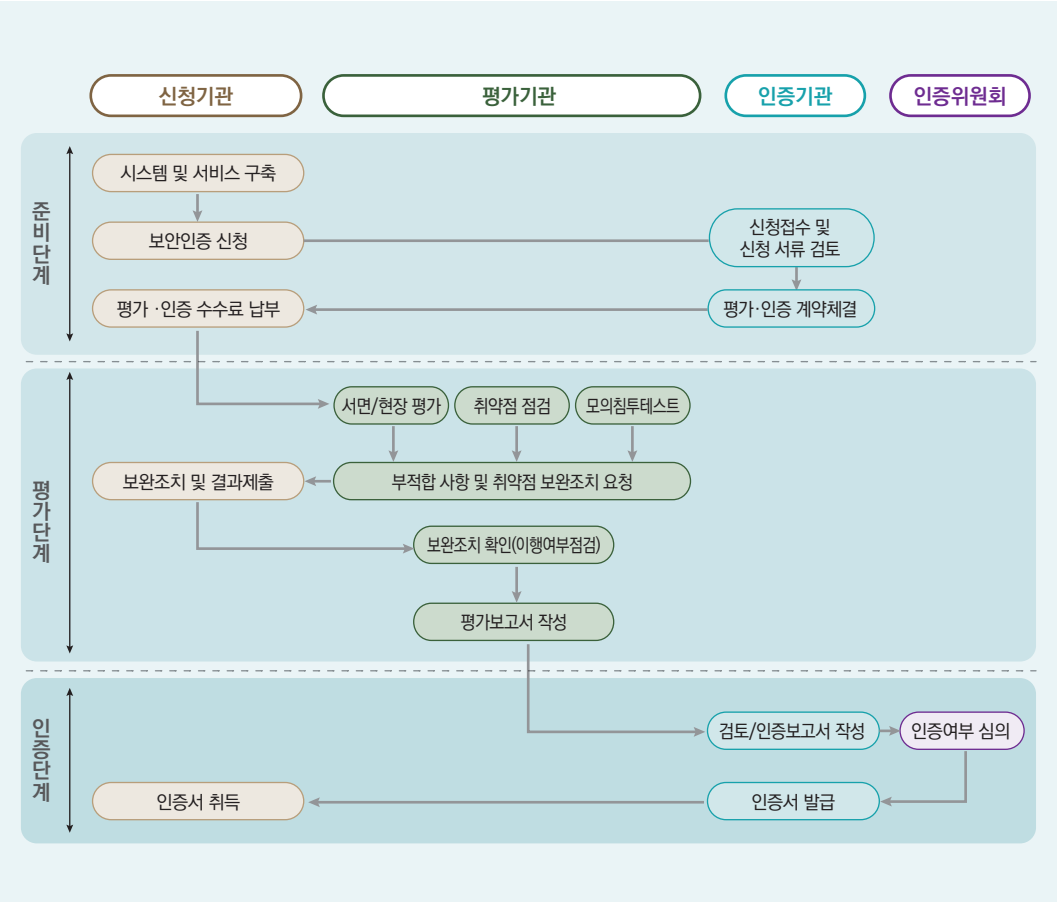
통제 분야	통제 항목	통제항목 수
1. 정보보호 정책 및 조직	1.1 정보보호 정책	3
	1.2 정보보호 조직	2
2. 인적보안	2.1 내부인력 보안	5
	2.2 외부인력 보안	3
	2.3 정보보호 교육	3
3. 자산관리	3.1 자산 식별 및 분류	3
	3.2 자산 변경관리	3
	3.3 위험관리	4
4. 서비스 공급망 관리	4.1 공급망 관리정책	2
	4.2 공급망 변경관리	2
5. 침해사고관리	5.1 침해사고 절차 및 체계	3
	5.2 침해사고 대응	2
	5.3 사후관리	2
6. 서비스 연속성 관리	6.1 장애대응	4
	6.2 서비스 가용성	3

통제 분야	통제 항목	통제항목 수
7. 준거성	7.1 법 및 정책 준수	2
	7.2 보안 감사	2
8. 물리적 보안	8.1 물리적 보호구역	5
	8.2 정보처리 시설 및 장비보호	6
9. 가상화 보안	9.1 가상화 인프라	6
	9.2 가상 환경	4
10. 접근통제	10.1 접근통제 정책	2
	10.2 접근권한 관리	3
	10.3 사용자 식별 및 인증	4
11. 네트워크 보안	11.1 네트워크 보안	6
12. 데이터 보호 및 암호화	12.1 데이터 보호	6
	12.2 매체 보안	2
	12.3 암호화	2
13. 시스템 개발 및 도입 보안	13.1 시스템 분석 및 설계	5
	13.2 구현 및 시험	4
	13.3 외주 개발 보안	1
	13.4 시스템 도입 보안	2
14. 공공기관 추가보안 요구사항	14.1 관리적 보호조치	4
	14.2 물리적 보호조치	2
	14.3 기술적 보호조치	4
총 계		116

4. 평가 절차

클라우드 서비스 보안인증은 준비단계·평가단계·인증단계 등 세 단계로 구분할 수 있다. 평가기관은 신청기관에 방문하여 서면·현장평가, 취약점 점검 등을 수행한 후 부적합 사항을 도출하면 신청기관은 30일 이내(연장 시 최대 90일)에 부적합 항목을 모두 보완하여야 한다. 모든 항목에 대하여 보완이 완료되면 인증위원회 심의를 통하여 인증서 발급 여부를 결정한다.

그림 3-4-4-2 클라우드 서비스 보안인증 평가 절차



제5절 융합보안

기존 산업의 생산성·효율성을 높이기 위하여 ICT를 접목한 스마트공장·스마트시티·자율주행차 등 ICT 융합은 더욱 가속화할 전망이다. ICT 융합서비스 가속화는 사이버보안 위협이 전통산업의 위협으로 전이·증대되어 국민의 생명·안전 및 경제 전반에 직접적 피해 초래가 가능하다. 이미 세계적으로 스마트공장·스마트시티 분야에서 실제 사이버침해 사고가 발생하고 있으며, 자율주행차 등 다양한 융합서비스에서 보안취약점이 발견되고 있다. 이에 정부는 ICT 융합 기기·제품·서비스의 개발·구축 단계부터 보안위협을 예방하기 위하여

'5G+ 핵심서비스 융합보안 강화 방안'을 마련(2019. 10.)하고 그 정책과제의 일환으로 5대 융합서비스* 보안모델 개발 및 보안리빙랩을 구축·운영 중에 있다.

* 5대 융합서비스: 스마트공장, 자율주행차, 스마트시티, 디지털헬스케어, 실감콘텐츠로 5G+ 전략(2019. 4.)에서 시장성, 경쟁력, 정책지원 필요성 등을 고려하여 도출한 5G+ 핵심서비스

1. 융합서비스 보안모델 개발

ICT 융합의 확산은 사이버보안 위협이 핵심서비스 분야로 확대될 수 있으며, 국민 생명·안전 및 경제 전반에 직접적 피해를 초래할 수 있는 위험성을 내포하고 있다. 이에 과학기술정보통신부는 5대 융합서비스 분야에서 제품·서비스 개발 단계부터 보안 강화를 위하여 융합서비스 기업이 안전한 제품 개발 및 서비스를 운영할 수 있도록 취약점 점검, 보안성 시험 등 보안위협을 진단하여 보안 개선방안을 제시하고 분야별 적용이 가능한 보안모델을 개발하였다. 이러한 보안모델은 융합서비스 분야별로 도출된 보안위협에 대응하기 위하여 보안요구사항, 보안기술·솔루션 등 보안대책을 제시하고 있다. 융합서비스 산업현장에 보안모델을 시범 적용하기 위하여 2020년 12월 보안모델 1차 버전을 개발하였으며, 2021년 12월에는 융합서비스 보호 대상 범위를 확대하여 보안대책을 제시한 보안모델 2차 버전을 마련하였고, 2022년 12월에는 개발된 보안모델을 바탕으로 보안모델 실증 사례집과 해설집을 개발하여 산업현장에 활용되도록 배포하고 있다.

그림 3-4-5-1 융합서비스 보안모델

2. 5대 융합서비스 보안리빙랩 구축

보안리빙랩은 융합보안 수요자와 기업이 필요한 보안기술을 검증하고 융합서비스 기기·플랫폼의 보안성을 테스트할 수 있는 공간으로, 융합산업 현장의 많은 기업이 사용할 수 있도록 융합산업 주무 부처 및 유관기관과 협력하여 5대 융합서비스 분야별로 융합산업 특화지역 5곳에 구축하였다.

스마트공장은 경기도 안산에 위치한 스마트제조혁신센터의 데모공장과 연계하여 구축하였다. 실제 스마트공장 해킹 사고 시나리오를 기반으로 공정 로봇 오작동, 생산 수치 오류 유발 보안위협을 체험할 수 있으며, PLC·HMI를 비롯한 산업용 유·무선 스마트공장 설비와 솔루션의 보안성 테스트를 진행할 수 있다.

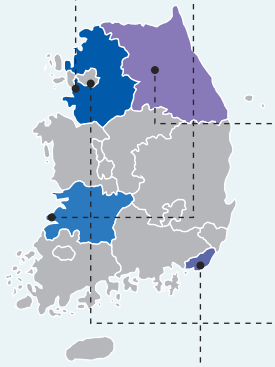
자율주행차는 전라북도 군산의 자동차융합기술원에 위치한 새만금 자율주행테스트베드와 연계하여 구축하였다. 실제 자동차 기반의 시험환경을 구축하여 자동차 전자식제어장치(ECU), 인포테인먼트(IVI) 등 핵심기기의 주요 취약점 점검 지원과 함께 자율주행 센서, V2X 통신 대상의 보안성 시험을 위하여 이동식 보안 시험환경을 조성하였다.

디지털헬스케어는 강원도 원주의 원주의료기기테크노밸리의 의료기기종합지원센터 내에 구축하였다. 병원시스템 데이터변조 시연 등 7개의 보안위협 시연이 가능하며, 디지털헬스케어 관련 의료기기 및 서비스, 의료정보시스템 간 연동을 통한 보안성 시험을 지원하고 있다.

실감콘텐츠는 경기도 판교 제2테크노벨리 기업지원허브 내에 구축하였다. 해킹 공격으로 VR서비스에서 변조된 영상 송출 시연과 메타버스 서비스에서 채팅 스니핑 등의 위협 시연이 가능하고 제작설비, 이용 기기, 메타버스·디지털 트윈 서비스·기기 등의 보안성 테스트가 가능하다.

스마트시티는 동남정보보호지원센터 내 스마트시티 국가 시범도시와 연계를 위하여 부산에 구축하였다. 로봇 서비스 보안위협과 통합플랫폼 연계 보안위협에 대한 모의해킹 시나리오를 볼 수 있으며, 통합플랫폼 연계, 로봇서비스, 안전서비스, 스마트시티 IoT 디바이스 등의 보안성 테스트를 할 수 있다.

그림 3-4-5-2 5대 융합서비스 보안리빙랩



스마트공장
(스마트제조혁신센터 내 데모공장 연계)

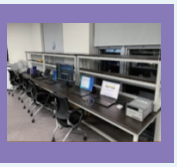
- 공정 로봇 오작동 시연
- PLC, HMI, 솔루션 테스트


자율주행차
(자동차융합기술원 내 새만금 자율주행 테스트베드 연계)

- 차량 모사환경, 핵심 센서시험
- ECU, ADAS 등 핵심기기 테스트


디지털헬스케어
(원주의료기기 테크노밸리 내 의료기기종합지원센터 연계)

- 병원시스템 데이터 변조 시연
- 의료기기, 서비스 보안성 테스트

실감콘텐츠
(판교 제2테크노밸리 기업지원허브 내 IoT 보안 테스트베드 연계)

- 해킹 공격으로 변조영상 송출 시연
- 제작설비, 이용 기기 테스트


스마트시티
(부산 EDC 내 스마트시티 국가 시범도시 연계)

- 로봇, 도시통합 플랫폼 위협 시연
- 도시통합플랫폼 디바이스테스트


제5장

금융서비스

제1절 금융서비스 정보보호

1. 정책의 시대적 변화

가. 인프라 구축 시기(2000~2010년)

인터넷뱅킹 서비스 개시를 계기로 전자금융 사고 예방을 위한 정책 및 기술 분야의 보안 인프라를 정부 주도로 구축하여 금융보안의 기반을 확립한 시기이다. 2002년 세계 최초로 전자금융거래에 공인인증서를 적용하였고, 금융 정보공유·분석센터(ISAC, Information Sharing and Analysis Center)를 설립하였다.

2005년 '전자거래 안전성 강화 종합대책'을 발표하여 전 금융권에 보안프로그램 사용 등 대책을 적용하였으며, 2006년 금융보안의 기본 법규에 해당하는 「전자금융거래법」을 제정하였다.

나. 고도화 시기(2011~2014년 상반기)

금융위원회는 2011년 '금융회사 IT보안 강화 종합대책'을 발표하여 정보보호최고책임자(CISO) 지정 의무화 등 금융회사의 주의·감독 의무를 강화하였다. 또한 금융보안을 총괄하는

전담과를 신설하고, 2013년 3.20 사이버테러 후속 대책으로 금융전산 망분리 및 이상금융거래 탐지시스템(FDS, Fraud Detection System) 구축 등 금융회사의 보안관리 체계 강화에 중점을 둔 '금융전산 보안강화 종합대책'을 발표하였다.

2014년 신용카드사 고객정보 유출 사고가 발생하자, 관계부처 합동으로 '금융분야 개인정보 유출 재발방지 종합대책'을 마련하여 금융소비자의 고객정보 자기결정권을 보장하고 정보유출 시 제재를 대폭 상향함으로써 금융회사의 과도한 고객정보 수집·사용 관행을 개선하였다.

다. 자율보안 체계 정착 시기(2014년 하반기~2017년)

핀테크 산업 활성화 등을 계기로 금융보안의 패러다임이 자율보안 체계로 전환됨에 따라 금융위원회는 2015년 'IT·금융융합 지원방안'(2015. 1.)을 발표하고 사전규제 최소화, 기술중립성 원칙 반영, 전자금융 사고 책임부담 명확화 등 금융보안 규제를 정비하였다. 또한 '금융IT부문 자율보안 체계 확립방안'(2015. 6.)을 통하여 금융회사의 자율점검 강화, 이상금융거래 정보공유 체계 구축 등 자율보안 세부 이행과제를 제시하는 한편, 금융보안원이 금융회사 자체 보안성 심의를 위한 기술 지원, 보안 가이드 마련 등 자율보안을 지원하는 금융보안 전문기관으로서 역할을 수행하도록 하였다.

라. 디지털금융 혁신 시기(2018년~현재)

2018년 전세계적으로 4차 산업혁명으로 인한 산업구조의 변화가 시작되면서 금융위원회는 '핀테크 혁신 활성화 방안'(2018. 3.)을 발표하고 혁신성장 8대 선도사업인 핀테크 활성화를 추진하는 한편, 혁신기술에 대한 단계별 보안진단 및 보안컨설팅 지원, 침해대응을 위한 금융보안원-금융회사 간 정보공유시스템 고도화, 레그테크 활용 분야 확대 등 핀테크 혁신의 잠재적 위험에 대응하기 위한 금융권 보안 지원 체계 및 안전성 강화를 추진하였다.

또한 '금융권 클라우드 이용 확대 방안'(2018. 3.)을 발표하고, 금융권 클라우드 이용 범위를 중요정보 처리시스템 등으로 확대하는 한편, 안전성 평가 등 클라우드 서비스 이용·제공 기준 마련, 클라우드 서비스 감독·검사 강화 등 클라우드 이용 확대에 따른 안전성 강화를 추진하고 있다.

2020년 신기술 도입의 확산과 코로나19 등의 영향으로 디지털 리스크 대응 체계 강화

필요성이 지속적으로 증가함에 따라 금융위원회는 '디지털금융 종합혁신방안'(2020. 7.)을 발표하고 디지털 금융보안에 대한 관리·감독 체계 확립, 민간·공공을 아우르는 사이버 리스크 통제 체계 정립 등 디지털금융에 대한 안정성 강화를 추진하고 있다.

코로나19의 영향으로 비대면 금융서비스의 확산이 가속됨에 따라 금융이용자가 비대면 온라인 금융서비스의 신원확인 등에 이용할 수 있도록 안전한 비대면 인증 신원기준을 마련하고 있으며, 인공지능 등을 활용한 디지털 혁신을 뒷받침할 금융 인프라 구축을 추진하고, 다양한 아이디어가 금융서비스로 이어지도록 디지털 샌드박스를 도입하여 핀테크 산업육성을 위한 체계적인 지원방안을 마련하고 있다.

2. 정책 내용

가. 추진 체계

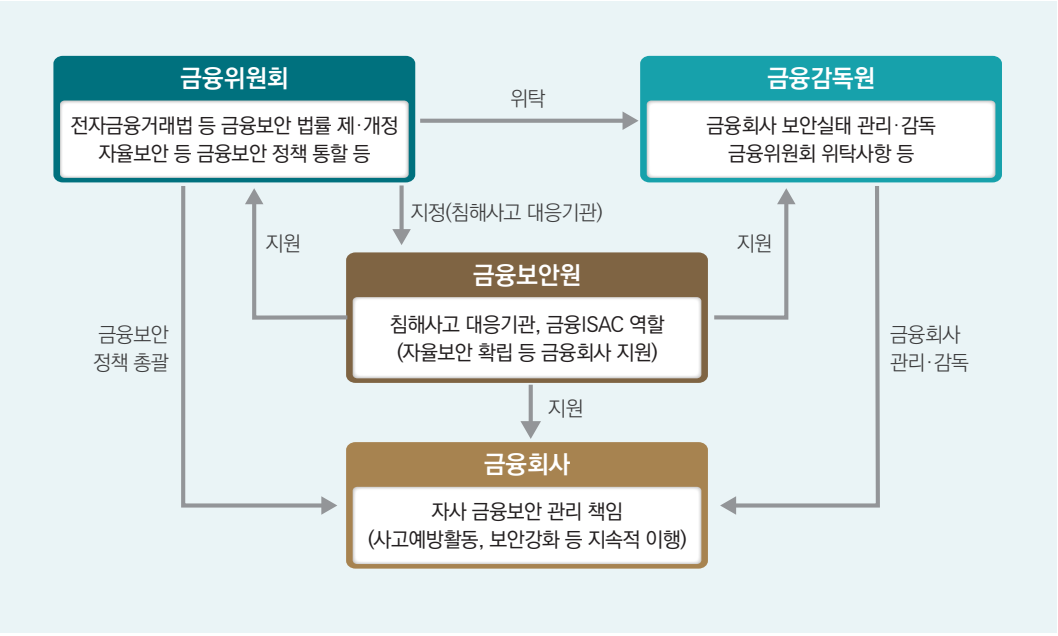
금융위원회는 「전자금융거래법」·「신용정보의 이용 및 보호에 관한 법률」 등에 따라 금융보안 정책 및 제도에 관한 사항과 금융회사 감독·검사·제재에 관한 사항 등을 총괄·관리하고 있다. 또한 금융권의 침해사고 대응을 총괄·관리하는 침해사고 대책본부의 운영, 침해사고에 관한 정보의 수집·전파, 예보·경보 및 긴급대응 조치 등의 업무도 통할하고 있다.

금융감독원은 「전자금융거래법」에 따라 금융위원회로부터 위탁받은 금융회사의 보안관리 실태 관리·감독업무를 수행하고 있다. 감독 결과 법규 위반사항이 확인되면 시정명령이나 주의 또는 경고·문책 등을 금융위원회에 건의할 수 있으며, 금융위원회는 이를 검토하여 조치한다. 또한 금융위원회의 위탁을 받아 전자금융업의 인허가 검토, IT 부문계획서와 취약점 분석·평가 결과의 접수 등 다른 전자금융 및 보안 관련 업무도 수행하고 있다.

금융보안원은 「전자금융감독규정」에 따른 침해사고 대응기관 및 「정보통신기반 보호법」에 따른 금융 정보공유·분석센터로서 금융권 통합보안관제센터 구축·운영, 침해위협 및 이상금융거래 정보공유, 전자금융기반시설 취약점 분석·평가 등 금융권 침해 예방 및 대응 업무를 수행하고 있다. 또한 금융위원회의 금융보안 정책 수립 지원이나 금융감독원의 검사 지원은 물론, 금융회사의 자체 보안성 심의 지원 및 적합성 시험, 금융보안 레그테크 포털 운영, 금융보안 가이드 개발, 금융보안 전문인력 양성 등 금융권의 자율보안 체계 정착을

지원하는 역할도 수행하고 있다.

그림 3-5-1-1 금융보안 체계



최근에는 범금융권 보이스피싱 사기 정보공유 체계 구축, 다크웹 위협정보 수집·대응 등 금융권의 사이버방어 대응 역량 강화와 함께 혁신금융서비스 보안성 검토 지원, 비대면 실명확인 보안성 검증 지원 및 금융권 인공지능 활용 활성화 관련 정책·기술 지원 등 금융 신기술 도입은 물론 디지털금융 혁신 관련 보안 지원에도 노력을 기울이고 있다.

금융회사는 자사 금융서비스 보안에 대한 책임의 주체로서 최고경영자의 책임 아래 금융보안 사고 예방 활동을 이행하며, 금융보안 인력 및 예산 확보 등 자체 보안역량 강화를 위한 활동을 수행하고 있다. 최근에는 금융의 디지털 전환(Digital Transformation) 등에 따른 비대면 금융서비스 확산에 따라 디지털금융 리스크 대응 체계를 확립·이행하기 위하여 노력하고 있다.

나. 정책 주요 내용

금융위원회는 핀테크 산업 활성화와 금융권 자율보안 체계의 정착을 위하여 전자금융보안 규제를 지속적으로 정비하고 있다. 금융회사 스스로 정보보안 및 내부통제를 강화하고 핀테크 시대에 부응하는 민간 중심의 자율보안 체계를 확립할 수 있도록 사전규제를 사후규제로 전환하여 핀테크 산업 진입의 장애요인이 될 수 있는 기본적 보안규제를 정비하였다. 그리고 인증방법 평가위원회 및 국가인증 정보보호제품 사용의무 폐지, 사전 보안성 심의 제도 폐지 등과 같은 절차적 보안규제도 철폐하였다.

보안규제 정비와 함께 금융회사의 자율보안 체계 확립을 위한 지원을 더욱 확대하였다. IT감사 역량이 부족한 중소형 금융회사를 지원하고, IT부문 금융회사 내부감사 협의제도를 내실화하는 등 금융회사 자율점검을 강화하였다. 금융회사의 클라우드 서비스 이용 활성화를 위하여 이용 범위를 확대하고 가이드라인과 제공 기준을 마련하는 한편, 클라우드 서비스에 대한 감독·검사를 함께 강화하였다. 또한 금융보안 관련 가이드를 정비하여 금융회사가 적기에 사용할 수 있도록 하였으며, 금융회사가 금융 신기술에 대한 보안 전문성을 갖춘 자체 보안성 심의 체계를 운영할 수 있도록 금융보안원에 보안성 검토를 의뢰할 수 있는 프로세스도 구축하였다.

금융위원회는 「신용정보법」 개정(2020. 2.)에 따라 2021년부터 '금융권 정보보호 상시평가제'를 시행하고 있다. 이를 위하여 금융보안원은 금융회사가 개인신용정보 관리·보호 실태에 대한 자체평가를 해마다 수행할 수 있도록 상시평가 기준을 수립하고 자체평가 안내서 및 온라인 상시평가지원시스템을 개발하여 제공하고 있다. 또한 금융보안원은 금융회사가 제출한 자체평가에 대한 서면점검을 수행하고 이를 점수 또는 등급으로 표시한 결과를 금융위원회에 해마다 보고하고 있다.

정부의 핀테크 혁신 활성화와 공인인증서 의무사용 폐지 등 규제개선 정책 등에 힘입어 간편인증 수단을 활용한 간편결제 및 간편송금 서비스가 지속적으로 증가하여 2022년 상반기 기준 일평균 간편결제 이용금액은 7,232억 원, 일평균 간편송금 이용금액은 6,024억 원으로 이용규모가 해마다 증가하고 있다. 또한 자산관리, 국외 송금, 금융 크라우드 펀딩(Crowd funding), 로보어드바이저, P2P(Peer to Peer) 대출, 인슈어테크(InsureTech) 등 새로운 핀테크 서비스도 지속적으로 출시되고 있으며, 2019년 4월 금융규제 샌드박스 제도를 도입한 이래

2022년 말까지 총 237건의 혁신금융서비스가 지정되었다.

금융혁신 촉진을 위한 오픈뱅킹이 전면시행(2019년) 된 후 2021년 순가입자 3천만 명, 순등록계좌 수가 1억 개로 국내 경제활동인구(2,853만 명, 2021년 10월 기준) 대비 약 105%가 오픈뱅킹을 사용하고 있으며, 플랫폼을 통한 온라인 대출상품 비교, 안면인식 결제, NFC 결제 서비스 등 다양한 규제 특례를 통하여 신기술과 금융의 융합을 이루어 가고 있다.

전화 가로채기 악성앱 등 보이스피싱 수법이 기술적으로 고도화함에 따라 관계부처 합동으로 디지털 경제의 신뢰 기반조성을 위한 '보이스피싱 척결 종합방안'(2020. 6.)을 발표하고, 선불폰 등 통신수단의 부정 사용을 예방하기 위한 종합적인 대응 체계 구축, 공공기관·금융회사 등을 사칭하는 전화번호 거짓 표시(변작) 차단 체계 구축, 보이스피싱 이용 전화번호의 중지 절차 개선, 빅데이터·인공지능 등을 이용한 보이스피싱 방지 신기술 개발, 금융회사의 FDS 고도화를 위한 금융권 공동 컨소시엄 구축, 보이스피싱 방지 홍보 강화 등 민생침해 범죄인 보이스피싱 피해 예방·대응 활동을 강화하고 있으며, 이와 관련하여 「전기통신금융 사기 피해 방지 및 피해금 환급에 관한 특별법」을 개정하여 시행(2020.11. 20.)하고 있다.

「신용정보법」 개정으로 2022년 1월부터 마이데이터 사업자가 전송요구를 통하여 정보주체 개인의 금융정보(개인신용정보)를 통합 관리해 주는 것이 가능해졌다.

인공지능 기술이 금융서비스에 사용됨에 따라 관련 서비스의 신뢰를 제고하고 활성화하기 위하여 모범규준 '금융분야 AI가이드라인'을 마련하였으며, 가상자산의 거래 투명성을 제고하고 이용자를 보호하기 위하여 「특정금융정보법」을 개정하여 가상자산거래를 제한하는 기준을 마련하고 시행하였다.

클라우드·빅데이터·인공지능 등 디지털 신기술에 대한 금융권 수요가 늘어남에 대응하여 클라우드 이용 절차를 합리화하고 망분리 규제를 개선하기 위하여 '클라우드 및 망분리 규제 개선방안'을 마련하였으며, 제도 개선방안이 금융현장에 원활하게 안착할 수 있도록 「전자금융 감독규정」을 일부 개정하였다.

제2절 금융분야 사이버공격 대응 및 정보공유

1. 금융보안관제센터

금융보안원은 「정보통신기반 보호법」에 따른 금융 정보공유·분석센터 및 「전자금융감독규정」에 따른 침해사고 대응기관의 역할을 수행하고 있다.

금융보안원은 금융권 전체를 대상으로 금융보안관제센터를 운영하여 금융부문 보안관제를 수행하고 있으며, 국가보안관제(국가사이버안보센터) 및 개별 금융회사가 수행하는 자체 보안관제와 함께 3선 보안관제 체계를 구축하여 금융권 전체의 보안 수준을 높이고 있다.

그림 3-5-2-1 금융부문 보안관제 체계

금융보안관제센터는 침해행위 탐지·분석, 최신 탐지기법 개발·적용, 사이버위협 정보공유 등을 수행하고 있다.

침해행위 탐지·분석은 금융회사 대상의 전자적 침해 시도에 대하여 금융보안관제시스템을 이용하여 365일 24시간 실시간으로 탐지하고 이를 분석하는 업무로, 2022년 약 548만 건의 침해행위를 탐지·분석하였다. 사이버공격으로 판단되는 침해 시도는 금융회사에 즉시 통보하여 공격 시도를 차단하거나 소관 시스템의 취약점을 보완하는 등 대책을 마련하고 있다. 또한 2022년 은행 등을 대상으로 하는 랜섬 디도스 공격, Log4j 취약점을 표적으로 하는 제로데이 공격 등에 대하여 신속히 탐지·전파하여 금융회사의 대응을 지원하였다.

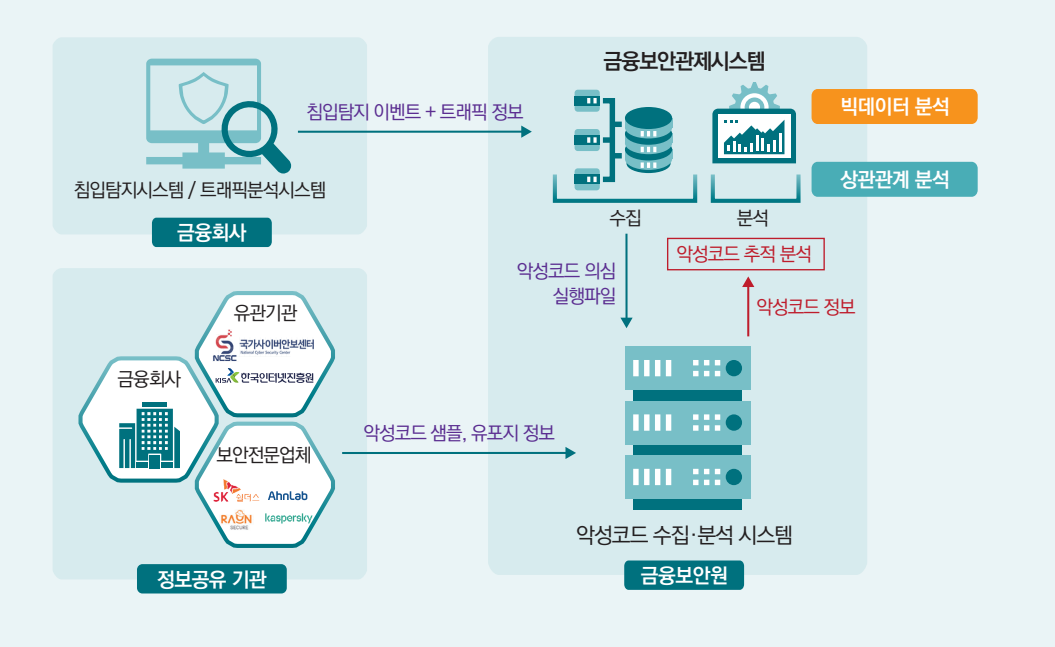
2021년부터 금융보안원은 금융분야 통합보안관제센터에 인공지능·빅데이터·클라우드 등 최신 보안기술을 적용한 차세대 관제시스템을 구축하였다. 이와 함께 금융 사이버위협 정보공유 시스템을 연계하여 갈수록 고도화되는 사이버위협에 신속하고 효과적으로 대응하고 있다.

금융보안원은 금융 사이버위협에 능동적으로 대응하기 위하여 국가사이버안보센터 등 국가기관과의 공조를 강화하는 동시에 한국인터넷진흥원과 미·일 금융ISAC(정보공유·분석센터, Information Sharing Analysis Center) 등 국외 금융보안 전문기관과 협력을 통하여 침해행위 관련 정보를 수집하여 대응하고 있다.

사이버위협 정보공유는 금융보안원이 금융회사·유관기관·보안전문업체 등과 상호 정보교환을 통하여 개별 금융회사에서 탐지된 침해정보 중 긴급 대응이 필요한 정보를 전 금융권 및 대외기관에 신속히 공유하는 것으로, 2022년 약 183만 건의 위협정보를 공유하였다. 또한 국가 차원의 보안 강화에 이바지하기 위하여 금융위원회와 금융감독원 등 금융분야 유관기관은 물론, 국가사이버안보센터·검찰청·경찰청·한국인터넷진흥원 등과도 긴밀한 공조 체계를 유지하고 있다.

그림 3-5-2-2 사이버위협 정보공유 체계

그림 3-5-2-3 금융보안관제시스템

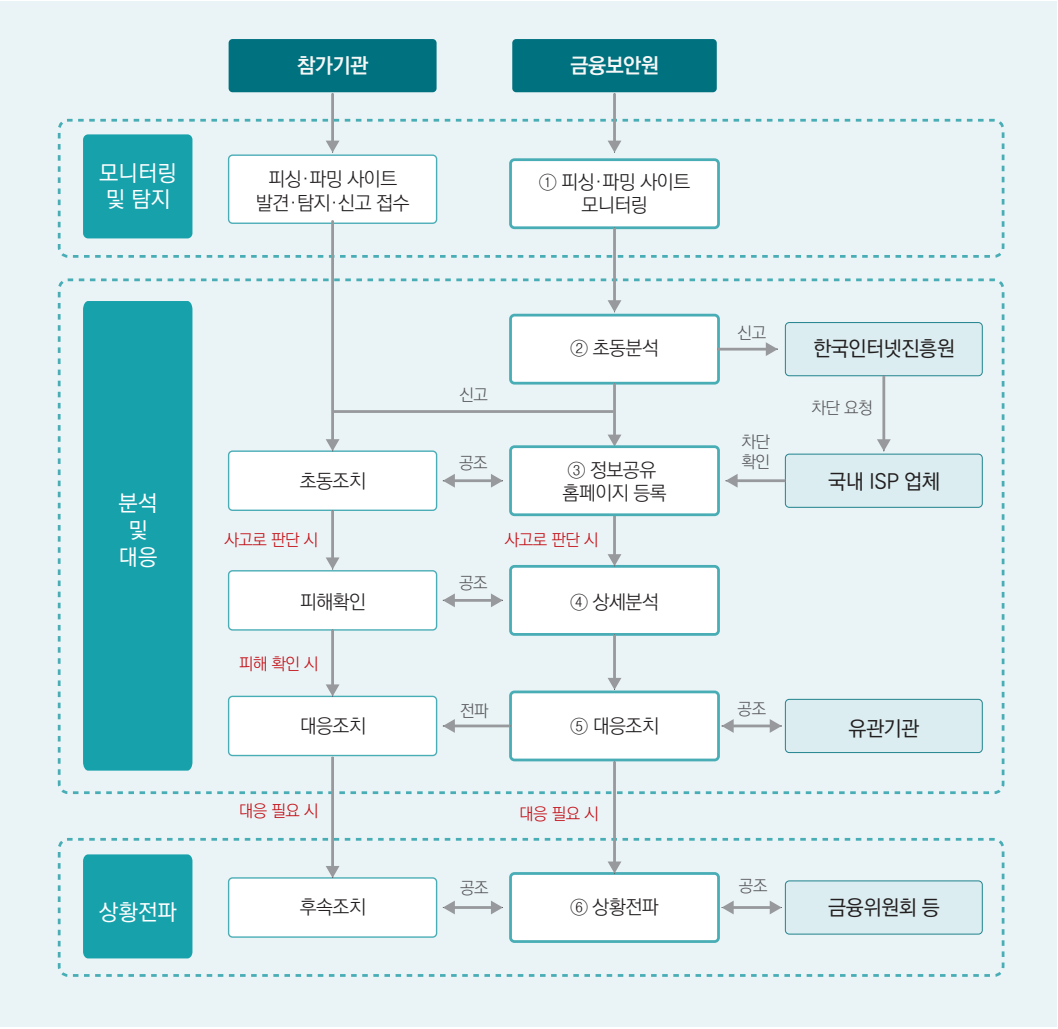


2. 피싱·파밍 사이트 모니터링

금융보안원은 자체 개발한 피싱탐지시스템을 활용하여 금융회사 홈페이지를 사칭한 피싱·파밍 사이트를 탐지·분석하고 차단함으로써 금융소비자 대상 사기 피해의 확산을 방지하고 있다.

금융보안원은 피싱탐지시스템을 통하여 피싱·파밍 의심 사이트를 탐지·분석하여 개인정보를 수집하는 등의 악성 행위가 발견되면 해당 사이트를 한국인터넷진흥원에 신고하여 인터넷서비스 제공업체(ISP, Internet Service Provider)를 통하여 차단하도록 한다. 또한 해당 정보는 정보공유 홈페이지에 등록하여 금융회사가 고객을 대상으로 피해방지 안내문을 게시하는 등 조치를 취할 수 있도록 하고 있다.

그림 3-5-2-4 피싱·파밍 사이트 모니터링 절차



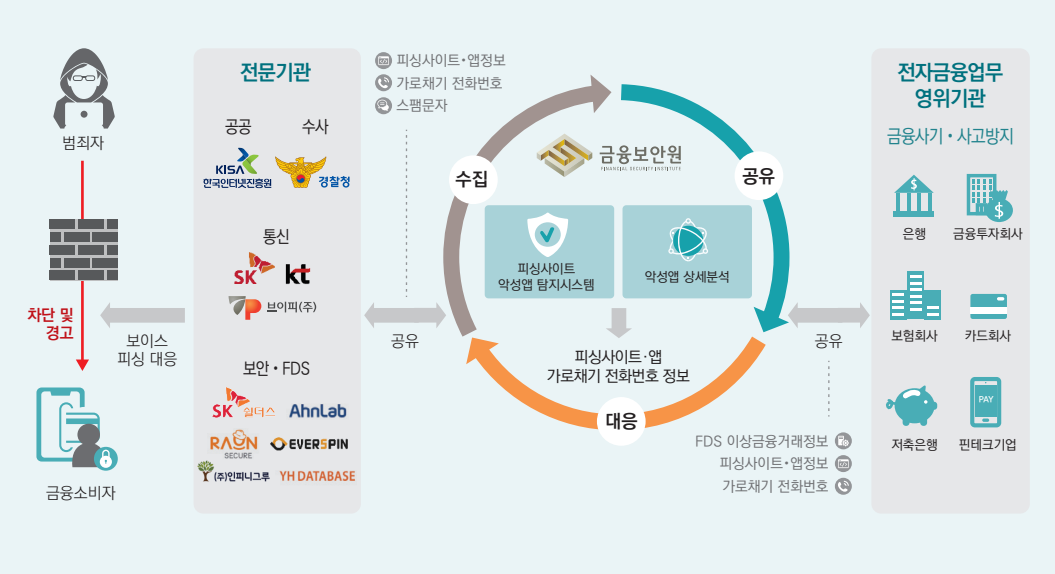
2022년 금융보안원은 약 2만 7천여 건의 피싱·파밍 시도를 탐지하였으며, 2020년 '경찰통계연보'(2021년 12월 발간)에 명시된 피싱·파밍 사이트 건당 평균 피해 금액인 약 650만 원을 기준으로 약 1,755억 원의 금융소비자 피해를 예방하였다. 한편 2019년부터는 금융보안원이 자체 개발한 보이스피싱 악성앱 유포지 탐지 기능을 피싱탐지시스템에 적용함으로써 피싱·파밍과 더불어 보이스피싱의 모바일 영역까지 선제적 대응에 나서고 있다.

3. 보이스피싱 예방·대응

2022년 금융보안원은 시중은행과 대형 전자금융업자 등과 함께 최신 보이스피싱 동향 및 사례 분석, 신종 보이스피싱 기법 차단기술 연구 등 금융권 전반에 적용 가능한 보이스피싱 예방·대응의 기술적 방안을 마련하였다.

금융보안원은 2021년 1월 금융·공공·통신·보안 등 범금융권 차원에서 보이스피싱 사기 정보의 수집-공유-대응의 유기적 협력 체계 운영을 목적으로 '범금융권 보이스피싱 사기 정보 공유시스템' 구축을 완료하였다. 이를 본격적으로 가동하여 2022년에는 보이스피싱 사기 정보 2만 8천여 건에 대한 공유 및 대응을 지원하였다.

그림 3-5-2-5 범금융권 보이스피싱 사기 정보공유시스템



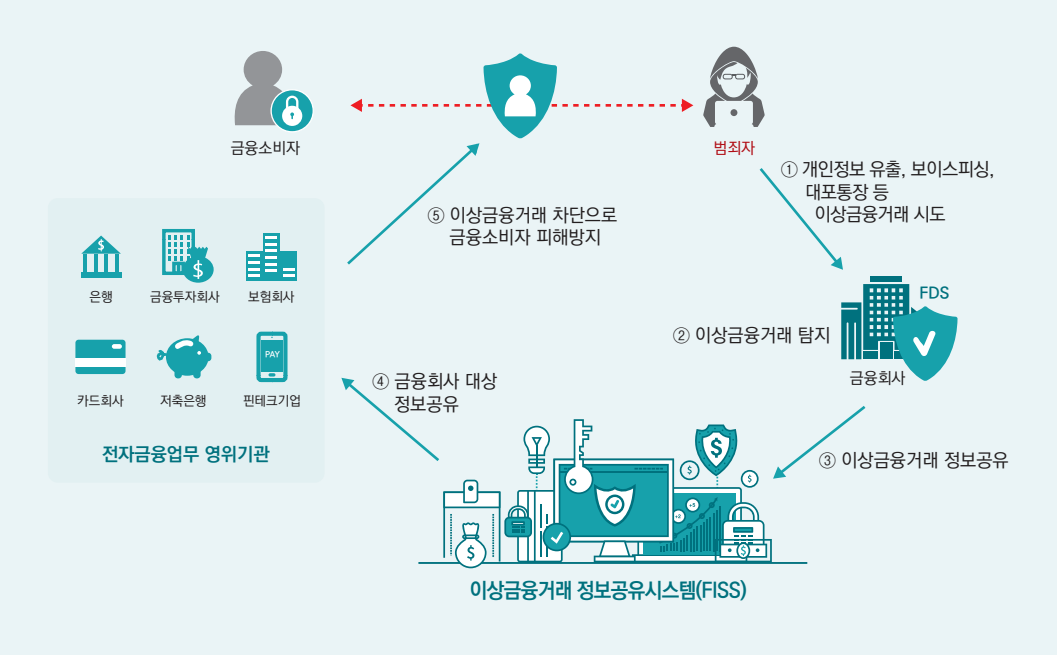
4. 이상금융거래 정보공유

사회공학 기법을 악용한 보이스피싱, 전자금융 사기 등 금융소비자 대상의 공격이 날로 고도화·지능화함에 따라 각 금융회사는 금융소비자의 재산을 보호하기 위하여 FDS를 구축·운영하고 있으며, 금융보안원은 금융권이 금융 사기에 공동 대응하기 위하여 2016년 2월부터 각 금융회사의 FDS가 탐지한 이상금융거래정보를 공유하는 이상금융거래 정보공유시스템

(FISS, Fraud Information Sharing System)을 운영하고 있다.

2022년 97개 금융회사와 전자금융업자가 이상금융거래 정보공유 업무에 참여하고 있으며, 184건의 이상금융거래 정보를 공유하여 약 104억 4천여만 원의 금융소비자 피해를 예방하였다.

그림 3-5-2-6 이상금융거래 정보공유 체계



5. 악성코드 수집·분석 및 대응

금융보안원은 금융권에 영향을 미칠 수 있는 악성코드를 다양한 채널을 통하여 수집하고, 악성코드 분석시스템을 운영하며 랜섬웨어, APT(Advanced Persistent Threat) 공격 등 지능화하고 있는 악성코드를 분석·프로파일링(연관성 및 유형 그룹화)하고 있다. 악성코드 분석 후 위협그룹 식별 및 패턴에 대한 추적·관찰 정보를 금융회사와 유관기관에 제공하고 있으며, 금융회사 시스템에 대한 감염 시도, 금전적 목적으로 유포되는 악성코드 및 유포사이트 등의 정보도 금융회사·유관기관과 공유하고 있다.

2022년 악성코드 수집·분석 건수는 약 2,564만 건으로, 이 중 실제 악성코드로 판별된 약 73만 건의 정보를 금융회사·유관기관과 공유하였다.

또한 국내를 표적으로 하는 위협그룹 프로파일링 등 사이버위협 인텔리전스를 연구하고 있으며, 2022년 'Masscan 랜섬웨어 위협 분석'(11. 1.),과 '디도스 공격 트렌드 및 주요 봇넷 분석' 보고서(12. 7.)를 발간하였다.

6. 침해사고 대응·복구 훈련 실시

금융회사와 전자금융업자는 다양한 공격유형의 전자적 침해사고에 대한 대응 및 복구능력을 강화하기 위하여 「전자금융감독규정」에 따라 연 1회 이상 침해사고 대응 및 복구 훈련을 실시하고 있다.

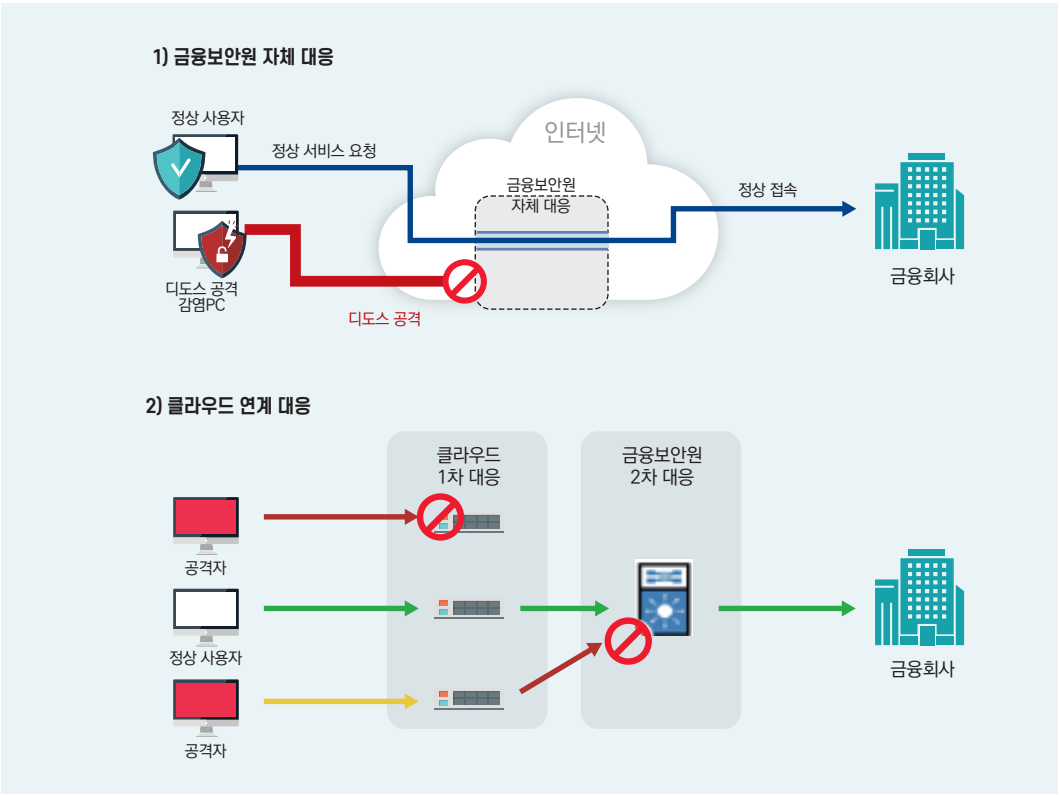
금융보안원은 자체 개발한 훈련 콘텐츠를 활용한 디도스 공격, 서버해킹 공격, APT 공격 등 금융회사의 침해사고 대응훈련을 지원하고 있으며, 2022년 총 541회의 침해사고 대응훈련을 수행하였다.

7. 디도스 공격 대응

금융회사는 「전자금융감독규정」 제15조에 따라 전자적 침해사고를 방지하기 위하여 자체적으로 정보보호시스템을 구축하여 디도스 공격에 대응하고 있다. 금융회사의 대응능력을 초과하는 디도스 공격이 발생할 경우를 대비하여 금융보안원은 디도스 공격 비상대응센터를 운영하고 있으며, 이와 함께 대용량 클라우드와의 연계를 통해서도 디도스 공격을 차단하고 있다.

또한 금융보안원은 국가사이버안보센터·한국인터넷진흥원·경찰청·회선사업자·보안업체·국외 유관기관과 긴밀한 정보공유 체계를 구축하여 디도스 공격에 유기적으로 대응하고 있다.

그림 3-5-2-7 디도스 비상대응센터 대응 체계



제3절 금융IT 및 전자금융·핀테크의 보안 평가·점검

1. 보안 취약점 평가

금융보안원은 「전자금융감독규정」에 따른 침해사고 대응기관 및 「정보통신기반 보호법」에 따른 금융분야 정보공유·분석센터로서 전자금융기반시설 및 금융분야 주요정보통신기반시설 등에 대한 보안 취약점 평가를 수행하고 있다.

금융보안원은 최신 점검항목과 점검기술을 사용하여 전자금융거래에 이용되는 정보처리 시스템과 정보통신망을 대상으로 정보보호 관리 체계, 모의해킹 등 총 10개 분야의 보안 취약점 평가를 수행한다.

점검항목은 금융보안원의 「전자금융기반시설 보안 취약점 평가 기준」과 과학기술정보통신부의 「주요정보통신기반시설 취약점 분석·평가 기준」을 기반으로 한다.

2022년 오픈소스 기반 시스템과 마이데이터 서비스를 위한 평가 기준을 새롭게 마련하였으며, 금융업권별 오픈뱅킹 모바일 애플리케이션을 대상으로 테마점검*을 수행하였다. 또한 모의해킹 전문인력을 구성하여 차별화되고 전문화된 점검 서비스를 제공하였다.

* 금융권의 최신 보안 위협 및 전자적 침해사고가 우려되는 분야에 대한 이슈를 선정하고, 사원기관을 대상으로 해마다 취약점 점검 서비스를 제공한다.

표 3-5-3-1 보안 취약점 평가 분야별 주요 평가 내용

평가 분야		주요 내용	방법
인프라 영역	정보보호 관리 체계	• 「전자금융거래법」·「전자금융감독규정」 등을 중심으로 금융회사 내부규정 및 절차의 적정성 평가	체크리스트 기반 점검, 자동화 도구 점검, 수작업 점검, 담당자 인터뷰, 현장실사 등
	서버	• 정보처리시스템 운영 시 불필요한 서비스 활성화 등 운영체제 보안 설정에 관한 적정성을 기술 중심으로 평가	
	데이터베이스	• DBA 계정 권한, 비밀번호 등에 관한 보안설정의 적정성을 기술 중심으로 평가	
	네트워크 인프라	• 네트워크 망분리, 네트워크 접근통제 등 네트워크 구성 및 가용성 확보에 관한 적정성을 관리 중심으로 평가	
	네트워크 장비	• 네트워크 운영 장비에 관한 보안설정 등에 관한 적정성을 기술 중심으로 평가	
	정보보호시스템 장비	• 보안정책 및 정보보호시스템의 보안설정 등에 관한 적정성을 기술 중심으로 평가	
서비스 영역	웹	• 인터넷뱅킹 등 웹 기반 전자금융거래 서비스에 대한 침해 가능성을 기술 중심으로 평가	
	모바일	• 모바일뱅킹 등 모바일 기반 전자금융거래 서비스에 대한 보안 침해 가능성을 기술 중심으로 평가	
	HTS	• 증권회사에서 제공하는 HTS 애플리케이션에 대한 침해 가능성을 기술 중심으로 평가	
공통	모의해킹	• 다양한 취약점을 이용한 내부 침투 가능성 및 개인신용정보 등 중요 정보 유출 위험 평가	시나리오 기반 점검

2. 전자금융보조업자 합동점검

금융회사는 정보기술부문과 연계된 전자금융보조업자의 정보처리시스템을 대상으로 보안점검을 실시하여야 하며, 금융보안원은 이를 지원하기 위하여 금융회사와 합동점검반을 구성하여 보안점검을 실시하고 있다.

2021년 '전자금융보조업자 보안 취약점 점검 안내서'(4. 12.)를 발간하여 전자금융보조업자 보안점검 시 이용하고 있으며, 2022년에는 64개 금융회사와 합동으로 CD VAN, 카드 VAN, CMS 사업자 등 전자금융보조업자 39개사에 대한 보안 취약점 점검을 실시하였다.

또한 금융회사와 합동으로 보안 취약점을 점검할 수 있는 기능과 점검 결과 관리 및 계약 관계 등을 통합관리할 수 있는 '전자금융보조업자 보안 통합지원시스템'을 운영하는 등 제3자 리스크에 선제적으로 대응하고 있다.

3. 개인(신용)정보 수탁자 합동점검

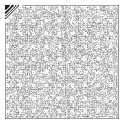
금융회사(위탁자)는 개인정보처리업무 수탁자가 개인(신용)정보를 안전하게 처리하는지를 주기적으로 관리·감독하여야 하며, 금융보안원은 합동점검 방식을 통하여 수탁자가 개인(신용)정보를 처리할 때 안전성 확보에 필요한 기술적·관리적 보호 조치의 적정성을 연 1회 점검하고 있다.

2022년 수탁자의 자체점검 및 실질적인 개인(신용)정보 안전성 확보 조치에 참고할 수 있는 가이드를 제공하였으며, 71개 사원기관의 신청에 따라 총 104개 수탁자를 대상으로 점검을 실시하였다.

한편 금융권 수탁자 점검을 효율적으로 수행하기 위한 '개인(신용)정보 수탁자점검 지원 시스템'을 구축하여 운영 중이다.

4. 클라우드 컴퓨팅 서비스 제공자 안전성 평가

금융회사 또는 전자금융업자는 상용 클라우드 컴퓨팅 서비스를 이용할 때 클라우드 컴퓨팅 서비스 제공자(CSP)에 대한 안전성 평가를 수행하여야 하며, 금융보안원은 침해사고 대응기관



으로서 2019년부터 금융회사의 CSP 안전성 평가를 지원하고 있다. 2021년에는 합동평가 방식을 도입하여 동일 CSP 사업자의 클라우드 서비스에 대한 금융회사의 중복평가를 방지하여 CSP 안전성 평가 부담을 완화하였다.

CSP가 준수하여야 할 일반적 보안 기준인 '기본 보호 조치'와 금융분야 특화 기준인 '금융부문 추가 보호 조치'로 구분하여 평가하고 있으며, 2022년에는 9개 CSP 사업자에 대하여 CSP 안정성 평가를 수행하고, 평가결과를 금융회사에 공유(223건)하였다.

또한 금융회사에게 CSP 안전성 평가 관련 정보, 평가 결과서 등을 공유할 수 있는 'CSP 안전성 평가 통합지원시스템'을 구축하는 등 금융권 클라우드 이용 생태계 조성 지원과 보안성 제고에 이바지하고 있다.

2023년부터 개정된 54개 평가항목으로 금융보안원이 금융회사를 대표하여 CSP 안전성 평가를 수행(대표평가)하고 평가 결과를 금융회사에 공유할 계획이며, 클라우드 서비스에 잠재된 보안 취약점을 실증하는 기술점검을 도입할 예정이다.

5. 핀테크 보안점검

금융보안원은 안전한 오픈뱅킹 환경을 조성하고 혁신적인 핀테크 서비스가 신뢰성을 확보할 수 있도록 지원하고자 오픈뱅킹 및 금융 테스트베드(혁신금융서비스 등)에 참여하는 핀테크 기업과 온라인투자연계금융업자에 대한 보안점검을 수행하고 있다.

핀테크 보안점검은 총 2종으로, 핀테크 기업이 기본적인 보안관리 체계를 확보하는 데 필요한 관리적·물리적·기술적 항목을 점검하는 '핀테크 기업 보안점검'과 핀테크 서비스(앱/웹)에 대하여 중요정보 보호, 거래정보 위·변조, 클라이언트 보안, 서버 보안, 인증 항목을 점검하는 '핀테크 서비스 취약점 점검'으로 구성된다.

2022년 금융보안원은 핀테크 기업을 대상으로 총 298건(전년 대비 22% 증가)의 보안점검을 수행하였다.

제4편

정보보호 기반조성

제1장 정보보호산업 육성
제2장 정보보호 기술 개발
제3장 정보보호 인력 양성
제4장 개인정보보호
제5장 대국민 정보보호
제6장 국제협력

제1장

정보보호산업 육성

제1절 개요

정부는 2015년 'K-ICT 시큐리티 발전전략' 수립 및 「정보보호산업 진흥에 관한 법률」(이하 '정보보호산업법')을 제정하고, 2016년 '제1차 정보보호산업 진흥계획'을 발표하였다. 기본계획에 따라 범정부 차원에서 ▲정보보호 창업 활성화 ▲정보보호 투자 확대 및 신시장 창출 ▲글로벌 진출로 시장 확대 ▲ICT융합산업의 지속적인 성장 생태계 조성 등 4대 전략 과제를 추진하였다.

「정보보호산업법」 제정에 따라 수요 측면에서는 정보보호시장 창출 등 산업 선순환 생태계를 강화하는 계기를 마련하고, 공급 측면에서는 체계적인 정보보호산업 진흥 기반조성을 위한 규정을 마련하여 사이버공격 대응 체계의 핵심 구성요소로서 국내 정보보호산업을 육성·강화하는 기반을 마련하였다.

「정보보호산업법」에 이어 2017년에는 정보보호 공시제도를 시장에 안착시키고 성능평가 제도의 기반을 마련하였으며, 융합보안 관련 인력 양성 및 보안가이드를 마련하였다. 이어 정보보호 관련 제도 설명회, 기업 자율 공시, 정보보호제품 성능평가 운영지침 제정·시행 등 정보보호산업 기반 마련과 기업 경쟁력 강화를 위하여 노력하였다.

2019년 4월 청와대 국가안보실에서 발표한 '국가사이버안보전략'은 '사이버보안 산업

성장기반 구축'을 6대 전략과제 중 하나로 삼고 정보보호산업 성장을 지원하고 있다. 본격적인 과제 실행을 위하여 관계부처인 과학기술정보통신부·국가정보원·행정안전부·외교부·교육부 합동으로 2019년 9월 '국가 사이버안보 기본계획'을 수립하였다.

2020년 코로나19로 인한 비대면 서비스 확산으로 디지털 전환이 가속화되고, 민간 사이버 복원력 확보를 위하여 정보보호산업 생태계 강화에 대한 사회적 요구에 따라 과학기술정보통신부는 2020년 6월 '제2차 정보보호산업 진흥계획(2021~2025)'을 발표하여 안전한 디지털 신뢰사회를 구현하고자 하였다.

2025년까지 정보보호산업은 전체 매출액 20조 원, 300억 이상 기업 100개, 16만 5,000명의 인력 양성을 목표로 설정하고, 이를 달성하기 위해 중소기업의 자발적인 정보보호 역량 강화, 정보보호 기업 간 기술 제휴 및 차세대 기술 개발을 위한 상생 협력 체계 강화, 정보보호 인력 양성 전주기 관리체계 구축을 추진하고, ▲디지털 전환에 따른 정보보호 신시장 창출 ▲민간 주도의 사이버 복원력 확보를 위한 투자 확대 ▲지속성장 가능한 정보보호 생태계 조성을 중점 세부과제로 설정하였다.

2021년은 포스트 코로나19로 인하여 재택·원격근무, 온라인 수업 등 비대면 환경이 빠르게 확산됨에 따라 비대면 서비스 보안의 중요성이 부각되었다. 정보보호산업의 범위도 가전, 모바일기기, 산업기계 등 유·무선 네트워크 연결에 따른 ICT보안으로 더욱 확장되어 정보보호의 중요성이 그 어느 때보다 강조되었다. 특히 정부는 코로나19의 영향으로 안전한 비대면 서비스가 신속히 제공될 수 있도록 원격 교육·재택근무, 비대면 진료 등 서비스에 보안기술을 적용한 안전한 비대면 서비스 상용화를 지원하였다. 또한 재난·재해 및 생체정보 기반의 인공지능 학습데이터 등도 제공하여 국내 정보보호 신시장이 창출될 수 있는 기반을 마련하였다.

2022년 5월, 정부는 110대 국정과제를 발표함으로써 사이버보안을 과학기술 5대 강국으로 도약하기 위한 전략기술에 포함시켰으며, 보안 산업의 역량 강화를 위한 전략산업화를 추진하였다.

같은 해 9월, 과학기술정보통신부는 '대한민국 디지털 전략'을 수립하고, 사이버보안 산업의 전략산업화를 위한 세부 추진계획을 발표하여 인재 양성에서 기술개발·연구(R&D) 및 시장 확산까지 전 방위적 지원을 강화하고자 하였다.

이번 계획을 기반으로 ▲민·관·군 협력 사이버보안 10만 인재 양성 ▲기업성장 지원 강화 ▲융합보안 거점 구축을 통한 융합산업 보안강화 ▲정보보호 클러스터 구축 확산을 추진하여 국내 사이버보안 매출액을 2027년까지 20조 원으로 확대할 계획이다.

제2절 정보보호 업체 및 시장 현황

국내 정보보호 업체 및 시장 현황자료는 국내 소재 정보보호 기업 총 1,517개(정보보안 669개, 물리보안 848개)를 대상으로 한국정보보호산업협회에서 조사하여 작성한 '2022년 정보보호산업 실태조사'를 활용하였다.

1. 기업 현황

정보보호 관련 기업의 종업원 규모별 현황을 살펴보면 20인 미만 기업이 779개(51.4%), 20인 이상 100인 미만 기업이 506개(33.3%), 100인 이상 200인 미만 기업이 103개(6.8%), 200인 이상 기업이 129개(8.5%)인 것으로 조사되었다. 종업원 수가 100인 미만인 기업은 정보보안 79.1%, 물리보안 91.9%로 전체의 89.2%를 차지하고 있음을 알 수 있다.

표 4-1-2-1 정보보호기업 종사자 규모별 현황(2021. 12. 기준)

(단위: 개, %)

구분	정보보안		물리보안		합계	
	기업 수	비율	기업 수	비율	기업 수	비율
20인 미만	267	39.9	512	60.4	779	51.4
20~100인 미만	262	39.2	244	28.8	506	33.3
100~200인 미만	61	9.1	42	4.9	103	6.8
200인 이상	79	11.8	50	5.9	129	8.5
합계	669	100.0	848	100.0	1,517	100.0

2. 시장 현황

2021년 전체 정보보호산업 매출액은 총 13,861,180백만 원으로 2020년 대비 13.4% 증가한 것으로 조사되었다. 정보보안 매출액은 2020년 3,921,387백만 원에서 2021년 4,549,734백만 원으로 16% 증가하였으며, 물리보안 매출액은 2020년 8,302,865백만 원에서 2021년 9,311,446백만 원으로 12.1% 증가하였다.

표 4-1-2-2 정보보호산업 매출 현황

(단위: 백만 원, %)

구분	정보보안		물리보안		합계	
	2020	2021	2020	2021	2020	2021
매출액	3,921,387	4,549,734	8,302,865	9,311,446	12,224,252	13,861,180
성장률	16.0		12.1		13.4	

2021년 정보보호산업 매출액은 13,861,180백만 원으로 2020년 12,224,252백만 원 대비 13.4% 증가한 것으로 조사되었다. 이 중에서 정보보안 매출액은 2014년 1,735,865백만 원에서 연평균 14.5%씩 성장하고 있으며, 물리보안 매출액은 2014년 5,519,452백만 원에서 연평균 5.8%씩 성장하였다.

코로나19 이후 비대면·비접촉 관련 보안수요가 급증함에 따라 전년 대비 매출액이 대폭 성장하였으며, 정부의 정보보호 제도개선 정책, 중소기업 대상 지원사업 등을 통하여 보안수요가 지속적으로 창출될 수 있도록 하였다,

특히 보안에 취약한 중소기업을 대상으로 정부가 정보보호 컨설팅 및 보안제품 도입을 지원함에 따라 중소기업의 보안수요도 지속적으로 증가하고 있는 것으로 분석되었다.

정보보호산업 매출액이 지속하고 있는 것은 정부의 법·제도 정비, 최근 보안사고 증가로 인한 경각심 고조, 정부와 기업의 보안 투자 강화, 국외 진출 노력 등이 주요 원인인 것으로 분석된다.

표 4-1-2-3 정보보호산업 매출 추이

(단위: 백만 원, %)

연도	정보보안	물리보안	합계
2015	2,108,659	6,110,086	8,218,745
2016	2,454,024	6,588,787	9,042,811
2017	2,744,940	6,840,822	9,585,762
2018	3,082,926	7,034,918	10,117,844
2019	3,618,773	7,561,734	11,180,507
2020	3,921,387	8,302,865	12,224,252
2021	4,549,734	9,311,446	13,861,180
CAGR(2015~2021)	13.7	7.3	9.1

3. 수출 현황

정보보호산업 수출액은 2020년 1,913,523백만 원에서 2021년에는 8.5% 증가한 2,076,780백만 원이 될 것으로 예상된다. 정보보안 수출액은 2020년 145,592백만 원에서 2021년 152,604백만 원으로 4.8% 증가하였으며, 물리보안 수출액은 2020년 1,767,931백만 원에서 2021년 1,914,176백만 원으로 8.8% 증가하였다.

표 4-1-2-4 정보보호산업 수출 현황

(단위: 백만 원, %)

구분	정보보안		물리보안		합계	
	2020	2021	2020	2021	2020	2021
수출액	145,592	152,604	1,767,931	1,924,176	1,913,523	2,076,780
증감률	4.8		8.8		8.5	

정보보호산업 수출액은 2015년 1,623,673백만 원에서 연평균 4.2%씩 성장하고 있다. 이 중에서 정보보안 수출액은 2015년 78,133백만 원에서 연평균 11.8%씩 성장하고 있으며, 물리보안 수출액은 2015년 1,454,540백만 원에서 연평균 3.7%씩 성장하고 있다.

표 4-1-2-5 정보보호산업 수출 추이

(단위: 백만 원, %)

연도	정보보안	물리보안	합계
2015	78,133	1,545,540	1,623,673
2016	88,978	1,400,102	1,489,080
2017	94,398	1,475,755	1,570,153
2018	82,363	1,473,769	1,556,132
2019	122,766	1,657,080	1,779,846
2020	145,592	1,767,931	1,913,523
2021	152,604	1,924,176	2,076,780
CAGR(2015~2021)	11.8	3.7	4.2

제3절 정보보호산업 관련 제도

1. 정보보호 전문서비스 기업 지정

가. 개요

정보보호 전문서비스 기업 제도는 「정보보호산업의 진흥에 관한 법률」(이하 '「정보보호산업법」') 에 따른 정보보안 컨설팅 전문기업 지정제도를 말한다. 이 제도는 주요정보통신기반시설에 대한 취약점 분석 및 보호대책 수립 업무를 지원하기 위하여 정보보호컨설팅 분야에서 전문능력과 신뢰성을 갖춘 민간기업을 지정하여 양질의 정보보호서비스를 제공하기 위한 것으로 2001년부터 시행하였다. 「정보통신기반보호법」과 「정보보호산업법」에 근거하여 시행되고 있으며, 관련 고시에서 지정 기준, 절차, 방법 등에 관한 세부 사항을 정하고 있다.

지능형 사이버위협이 증가하면서 주요정보통신기반시설이 확대되고 그 취약점 분석 주기가 2년에서 매년 수행으로 단축되었다. 이에 따라 늘어나는 신규 컨설팅 수요에 대응하기 위하여 정보보호 전문서비스 기업의 확대 필요성이 계속 제기되어 왔다. 이러한 추세를 반영하여 2013년 미래창조과학부(현재의 과학기술정보통신부)는 정보보호 전문서비스 기업의 지정제도 개선과 확대를 통한 서비스 품질 제고 및 시장 활성화 계획을 수립하고 관계법령의 개정을 완료하였다.

「정보통신산업진흥법」 시행규칙 일부개정안을 마련하여 2012년 9월 지식정보보안 컨설팅 전문업체 지정제도 개선을 위한 공청회를 개최하였고, 11월 입법예고 등의 의견수렴 절차를 거쳐 2013년 2월 「정보통신산업진흥법」 시행규칙 개정안이 공포되었으며, 개정된 시행규칙은 2013년 5월부터 시행되었다. 현재 이와 같은 법령 내용은 「정보보호산업법」에 이관되어 있다. 또한 2013년 11월 「지식정보보안 컨설팅 전문업체 지정 등에 관한 고시」(현재의 「정보보호 전문서비스 기업 지정 등에 관한 고시」, 이하 '고시')가 개정되어 시장 활성화 방안으로 정보보호 전문서비스 기업 지정요건이 완화되었으며, 정보보호 전문서비스 기업으로 지정받고자 하는 신규기업의 진입 장벽이 낮아졌다. 이후 고시는 '정보보호 전문서비스 기업'으로 제도 명칭과 부처명이 변경되었고, 사후관리 규정 정비 등의 내용을 반영하여 2017년 10월부터 개정·시행 중이다.

과학기술정보통신부는 2017년 10월부터 준비된 기업이면 언제든지 신청할 수 있도록 연중 상시 접수제를 시행하고 있다.

정보보호 전문서비스 기업은 사이버침해 행위가 발생하였을 때 국가안보와 국민의 기본생활 및 경제안정에 중대한 영향을 미치게 되는 주요정보통신기반시설을 점검하게 되므로 엄격한

표 4-1-3-1 정보보호 전문서비스 기업 지정 심사 기준

심사 기준	개정 전	개정 후 (2013. 5. 20.부터 시행)
인력요건	기술인력 15명 이상 (고급 5명 이상 포함)	기술인력 10명 이상 (고급 또는 특급 3명 이상 포함)
자본요건	납입자본금 20억 원 이상	자본총계 10억 원 이상
설비요건	컨설팅 업무를 수행하거나 지원하기 위한 설비, 도구 보유 여부	현행과 같음
보안요건	정보보호 관리규정 보유 및 준수 여부	현행과 같음
수행요건	업무수행 능력심사 평가 기준 70점 이상 계량평가: 경험, 전문화, 신뢰도, 기술 개발 실적 (70점) 비계량평가: 종합심사(30점)	업무수행 능력심사 평가 기준 70점 이상 계량평가: 경험, 전문화, 신뢰도, 기술 개발 실적 (85점) 비계량평가: 종합심사(15점)

[출처: 「정보보호산업의 진흥에 관한 법률」 시행규칙 제8조, 과학기술정보통신부 고시 제2017-24호(별표 2)]

심사와 관리가 절대적으로 요구된다. 이에 과학기술정보통신부는 지정 당시 법령상 지정 요건과 의무를 준수하고 있는지에 대하여 해마다 사후 관리를 실시하고 있다.

또한 허위 등 부정한 방법으로 지정받거나, 지정 기준에 미달하거나, 업무수행 중 알게 된 정보를 오용 또는 남용하여 주요정보통신기반시설의 운영 장애 등을 일으킨 경우에는 「정보보호산업법」 제23조제6항에 따라 지정을 취소하거나 3개월 이내의 기간을 정하여 그 업무의 전부 또는 일부의 정지를 명할 수 있다.

한편 정보보호 전문서비스 기업은 지정된 후 법인의 대표자 및 임원, 납입자본금, 기술인력, 정보보호 전문서비스 관리규정 등의 중요사항에 변동이 있을 경우 1개월 이내에 과학기술정보통신부에 관련 서류를 제출하여 신고하여야 한다.

나. 기업 현황

정보보호 전문서비스 기업은 2001년(9개)과 2002년(4개) 총 두 차례에 걸쳐 13개 기업을 지정하였으나, 컨설팅 사업 폐지, 재지정 탈락 등으로 6개 기업이 인수·합병 또는 지정 취소되었다. 이후 2014년에 11개 기업을 신규 지정하였으며, 2017년 10월 이후 상시 지정을 시작하여 2022년 12월 기준 28개 전문기업이 활동하고 있다.

표 4-1-3-2 정보보호 전문서비스 기업 현황

	업체명	지정일
1	시큐아이㈜	2001. 11. 29.
2	㈜안랩	2001. 11. 29.
3	㈜에이쓰리시큐리티	2001. 11. 29.
4	㈜싸이버원	2001. 11. 29.
5	에스케이쉴더스㈜	2002. 10. 8.
6	㈜소만사	2014. 3. 28.
7	㈜씨에이에스	2014. 3. 28.
8	㈜에스에스알	2014. 3. 28.
9	㈜윈스	2014. 3. 28.
10	㈜이글루시큐리티	2014. 3. 28.

	업체명	지정일
11	㈜시큐어원	2014. 3. 28.
12	한전KDN㈜	2014. 3. 28.
13	㈜파수	2016. 6. 2.
14	엔시큐어㈜	2017. 12. 26.
15	롯데정보통신㈜	2018. 4. 24.
16	㈜파이오링크	2018. 4. 24.
17	㈜신한DS	2018. 4. 24.
18	한국통신인터넷기술㈜	2018. 4. 24.
19	㈜에프원시큐리티	2019. 5. 16.
20	㈜케이씨에이	2019. 7. 22.
21	㈜한국정보기술단	2020. 2. 24.
22	㈜씨드젠	2020. 7. 29.
23	㈜라온화이트햇	2020. 7. 29.
24	한시큐리티㈜	2020. 10. 6.
25	㈜보안그룹모비딕	2020. 11. 10.
26	㈜시큐리티허브	2020. 12. 29.
27	㈜엘앤제이테크	2020. 12. 29.
28	㈜핀시큐리티	2021. 6. 14.

2. 보안관제 전문기업 지정

가. 개요

정부는 디도스 공격 등 신종·변종 해킹 공격으로부터 국가 주요 정보시스템을 보호하기 위하여 2010년 4월 「국가사이버안전관리규정」에 국가·공공기관의 보안관제센터 구축 의무화 조항을 포함하였다. 그 후속 조치로 2010년 12월 보안관제센터를 실질적으로 운영할 전문업체를 지정하기 위하여 보안관제업계의 의견을 폭넓게 수렴하고 '보안관제 전문업체 지정 등에 관한 공고'를 발표하였다.

2013년 5월 「국가사이버안전관리규정」을 재·개정하여 보안관제 전문기업의 지정·관리

등에 필요한 사항은 과학기술정보통신부장관과 국가정보원장이 협의하여 정하도록 하였고, 2016년 11월 '보안관제 전문기업'으로 명칭 변경 및 2017년 10월 부처명 변경을 반영하여 '보안관제 전문기업 지정 등에 관한 공고'를 개정하였다. 또한 2019년 8월 보안관제 전문기업의 양도·합병에 관한 조항을 신설하여 '보안관제 전문기업 지정 등에 관한 공고'를 일부 개정하였다.

보안관제 전문기업 지정기준은 기술인력 15명 이상, 자기자본 20억 원 이상, 업무수행 능력 평가를 기준 점수 이상 통과하여야 한다.

표 4-1-3-3 보안관제 전문기업 지정 심사 기준

심사 기준	심사 내용	판정 기준
인력요건	기술인력 15명 이상(고급 3명 이상, 중급 6명 이상)	적합 여부
자본요건	자기자본 20억 원 이상	적합 여부
수행요건	보안관제 업무수행 능력 평가 통과	70점 이상

[출처: 보안관제 전문기업 지정 등에 관한 공고(과학기술정보통신부 공고 제2019-441호)]

표 4-1-3-4 보안관제 업무수행 능력 평가 기준

평가 기준	평가 내용
경험(45점)	최근 1년간 보안관제 수행실적(자사인력 비중이 높고 파견관제 시 우대)
전문성(40점)	고급 기술인력 수, 보안관제 방법론, 자체 보안관제센터 운용 적절성 등
신뢰도(15점)	기업신용평가등급, 정보보호 인증기업 여부 등
기타(가감)	벤처기업 우대, 공공기관 입찰 참여제한 경력 등 감점

[출처: 보안관제 전문기업 지정 등에 관한 공고(과학기술정보통신부 공고 제2019-441호)]

보안관제 전문기업의 경우 지정요건을 최소한으로 정하여, 요건에 충족하면 언제든지 취득이 가능하기 때문에 시장 진입장벽이 없다. 이는 경쟁 촉진을 통한 양질의 보안관제 서비스 제공을 유도하기 위한 것이다. 다만 공공부문은 민간부문에 비하여 침해사고가 발생하였을 때 피해규모가 크고 광범위함을 고려하여 사후관리를 강화하고 있다. 보안관제 전문기업은 연 1회 사후관리 심사를 받아야 하며, 지정기준에 미달할 경우에는 지정이 취소된다.

나. 지정 현황

2011년 7월부터 보안관제 전문기업 지정제도가 시행되어 같은 해 10월 12개 기업이 지정되었다. 이후 2018년 16개 기업, 2019년 17개 기업, 2020년 17개 기업이 지정되었으며, 2021년 2개 기업, 2022년 1개 기업이 신규 지정되어 2022년 12월 기준 20개 기업이 활동하고 있다.

과학기술정보통신부는 신규지정 신청 접수 및 제도 관련 자문 등을 상시 실시하고 있으며, 업계 애로사항을 해결하기 위하여 노력하고 있다.

표 4-1-3-5 보안관제 전문기업 지정 현황

	업체명	지정일
1	㈜싸이버원	2011. 10. 31.
2	㈜안랩	2011. 10. 31.
3	㈜윈스	2011. 10. 31.
4	㈜이글루시큐리티	2011. 10. 31.
5	에스케이쉴더스㈜	2011. 10. 31.
6	㈜한국통신인터넷기술	2011. 10. 31.
7	한전KDN㈜	2011. 10. 31.
8	㈜시큐어원	2012. 4. 27.
9	㈜케이티디에스	2016. 1. 12.
10	삼성에스디에스㈜	2016. 8. 5.
11	㈜파이오링크	2017. 10. 18.
12	㈜가비아	2017. 10. 18.
13	㈜에이쓰리시큐리티	2018. 4. 25.
14	롯데정보통신㈜	2018. 7. 13.
15	㈜엘지씨엔에스	2018. 7. 13.
16	㈜시큐아이	2019. 3. 19.
17	씨엠티정보통신㈜	2020. 11. 10.
18	㈜피디정보통신	2021. 6. 14.
19	㈜신한DS	2021. 10. 18.
20	㈜엔아이티서비스	2022. 4. 8.

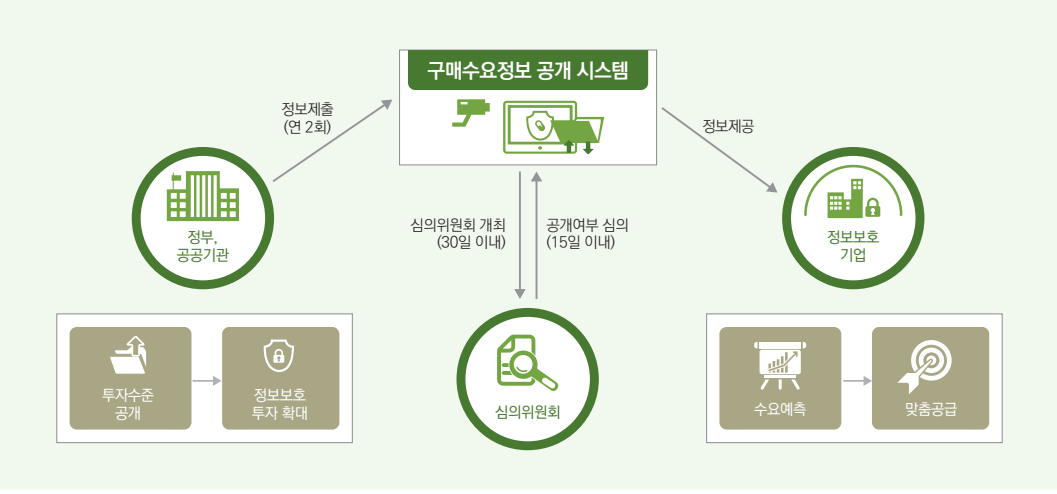
3. 정보보호 구매수요정보 조사

가. 개요

정부는 국내 공공부문의 정보보호제품 및 서비스 시장 수요 예측과 공급자의 맞춤형 정보보호기술 개발 촉진을 위하여 2015년에 시행한 「정보보호산업의 진흥에 관한 법률」 제6조(구매수요정보의 제공)에 따라 연 2회 당해 연도 확정 구매수요(상반기) 및 차년도 예정 구매수요(하반기) 조사를 수행하고 있다.

정보보호 구매수요정보 조사 절차를 살펴보면, 먼저 정부는 「정보보호산업의 진흥에 관한 법률 시행령」 제4조(구매수요정보의 제출 등)에 따라 정보보호 구매수요정보 제공 의무가 있는 공공부문으로부터 정보보호제품(하드웨어·소프트웨어) 및 서비스 구매수요정보를 수집한다. 이후 수집된 정보를 대상으로 구매수요정보 심의위원회를 통하여 국가안전 및 공공의 이익에 중대한 영향을 미치지 않는 정보를 최종 검토, 정보보호산업진흥포털(www.ksecurity.or.kr)에 게시함으로써 기업에 제공한다.

그림 4-1-3-1 구매수요정보 제공 절차



나. 2022년 확정 정보보호 구매수요정보 조사 결과

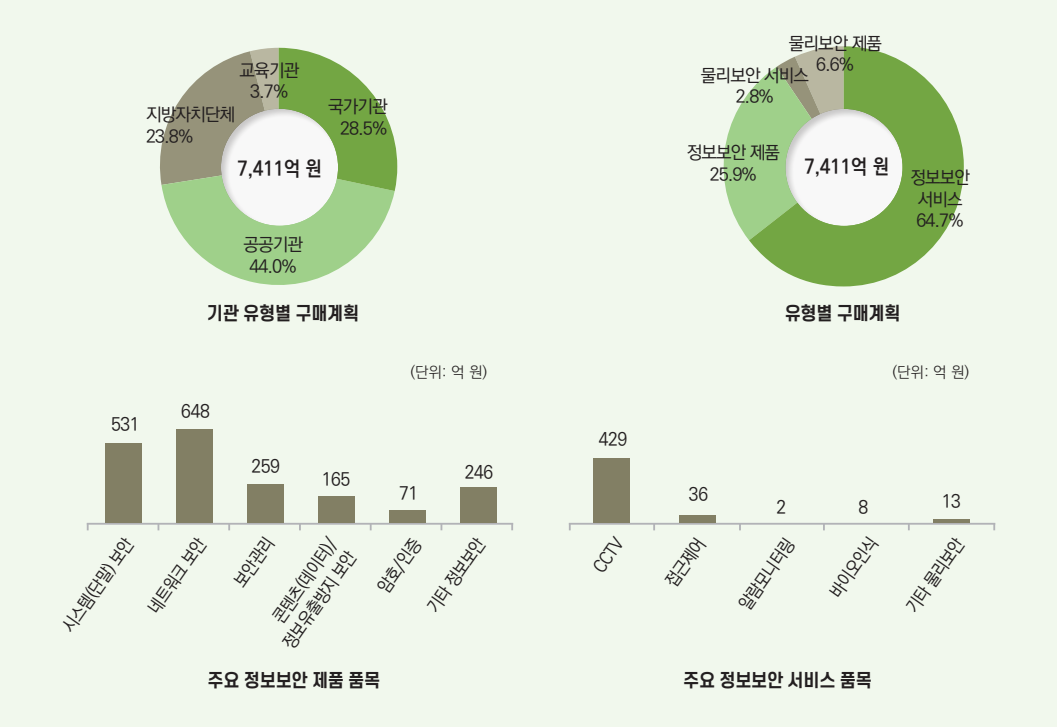
정부는 2022년 1~2월 국가기관, 공공기관, 지방자치단체, 교육기관 등 공공분야 2,583개 기관을 대상으로 정보보호 구매수요정보 조사를 수행하였다.

2022년 확정 정보보호 구매수요 예산은 총 7,411억 원이며, 기관 유형별로 살펴보면 국가기관 예산이 2,117억 원으로 전체 예산의 28.5%를 차지하였으며, 공공기관이 3,260억 원으로 44.0%, 지방자치단체가 1,763억 원으로 23.8%, 교육기관이 272억 원으로 3.7%를 차지하였다. 유형별로는 서비스 구매예산이 5,002억 원(67.5%), 하드웨어 1,533억 원(20.7%), 소프트웨어 876억 원(11.8%) 순으로 조사되었다.

정보보안 제품·서비스, 물리보안 제품·서비스 등 총 4가지 분야 중에서 정보보안 서비스 구매예산이 4,792억 원으로 전체 예산의 64.7%로 가장 높은 비중을 차지하였으며, 정보보안 제품이 1,920억 원으로 25.9%, 물리보안 제품이 488억원으로 6.6%, 물리보안 서비스가 211억 원으로 2.8%로 조사되었다.

주요 정보보안 제품 구매 품목으로는 네트워크 보안(648억 원), 시스템(단말) 보안(531억 원), 보안관리(259억 원) 순이었으며, 물리보안 제품 구매 품목으로는 CCTV(429억 원), 접근제어(36억 원) 순으로 나타났다.

그림 4-1-3-2 2022년 확정 정보보호 구매수요정보 주요 결과

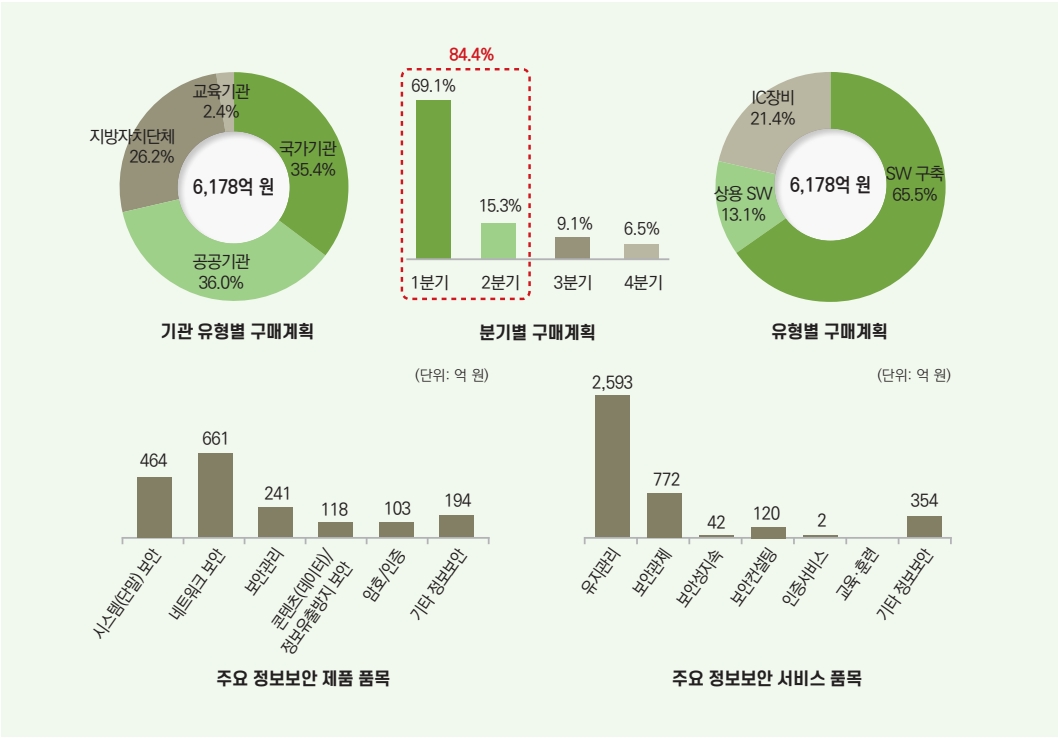


[출처: 한국인터넷진흥원]

다. 2023년 예정 정보보호 구매수요정보 조사 결과

정부는 2022년 10~11월 국가기관, 공공기관, 지방자치단체, 교육기관 등 공공분야 2,593개 기관을 대상으로 정보보호 구매수요정보 조사를 수행하였다.

그림 4-1-3-3 2023년 예정 정보보호 구매수요정보 주요 결과



2023년 예정 정보보호 구매수요 예산은 총 6,178억 원이다. 기관 유형별로 살펴보면 공공기관 예산이 2,223억 원(36.0%)으로 가장 높았으며, 국가기관이 2,190억 원으로 35.4%, 지방자치단체가 1,616억 원으로 26.2%를 차지하였다. 발주 시기별로 살펴보면, 1분기 정보보호 구매예산이 4,266억 원으로 가장 큰 비중(69.1%)을 차지하였으며, 2분기(947억 원, 15.3%)까지 합친 정보보호 구매예산 비중은 총 84.4%로 상반기에 집중될 것으로 조사되었다.

유형별로 살펴보면 소프트웨어 구축 예산이 4,048억 원(65.5%), ICT 장비 예산 1,321억 원(21.4%), 상용 소프트웨어 예산 809억 원(13.1%) 순으로 나타났다. 정보보안 제품·서비스, 물리보안 제품·서비스 등 총 4가지 분야 중에서 정보보안 서비스 구매예산이 3,883억 원

으로 전체 예산의 62.8%로 가장 높은 비중을 차지하였으며, 정보보안 제품이 1,779억 원으로 28.8%, 물리보안 제품이 351억 원으로 5.7%, 물리보안 서비스가 165억 원으로 2.7%로 조사되었다.

주요 정보보안 제품 구매 품목으로는 네트워크 보안(661억 원), 시스템(단말) 보안(464억 원), 보안관리(241억 원) 등으로 조사되었고, 정보보안 서비스 구매 품목으로는 유지관리(2,593억 원), 보안관제(772억 원), 기타 정보보안(354억 원) 등으로 나타났다.

4. 정보보호 공시

가. 개요

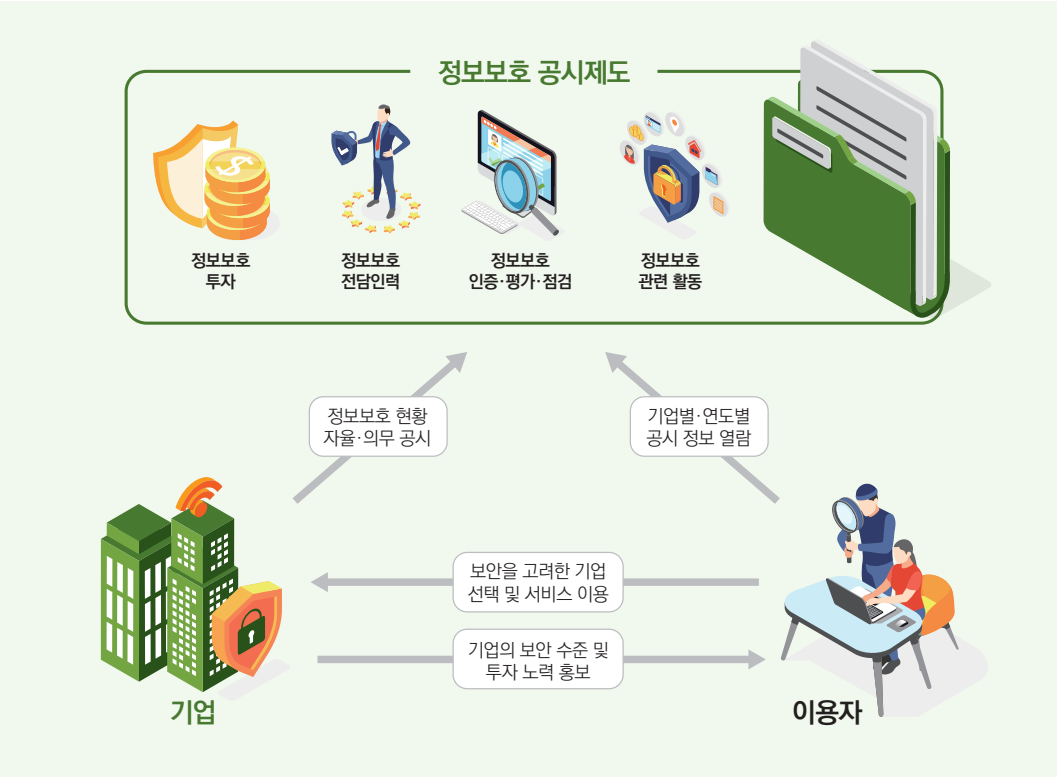
디지털 전환이 가속화되면서 사이버침해 사고 발생 시 파급효과가 특정 기업이나 개인 차원을 넘어 국가 차원의 경제적 손실로 이어지게 되면서 정보보호의 중요성이 강조되고 있다.

나날이 증가하는 사이버위협에 효과적으로 대응하기 위하여 기업은 정보보호에 대한 투자를 늘리고, 관련 정보의 공개를 통하여 기업과 주주·이용자·국민 등 이해관계자 사이의 정보 비대칭성을 최소화할 필요성이 높아졌다.

그럼에도 불구하고 그 동안 경영주체들은 정보보호를 단순 비용으로 취급하고, 기업의 정보보호 현황과 관련된 정보는 관리·감독을 하는 특정 집단만이 보유하고 있었다. 따라서 주주·이용자·국민 등 이해관계자들은 이와 관련한 충분한 정보를 제공받지 못한 채로 의사결정을 하는 문제가 존재하였다.

이에 따라 기업이 정보보호 투자 및 인력 현황, 정보보호 관련 인증 등 정보보호 현황을 공개하도록 하는 정보보호 공시제도가 도입되었다. 이 제도는 이용자에 대해서는 객관적인 기업 선택 기준을 제시하는 한편, 기업에 대해서는 정보보호 수준을 객관적으로 파악함으로써 경영 의사를 결정할 때 정보보호를 중요 요소로 참고할 수 있도록 하였다.

그림 4-1-3-4 정보보호 공시제도 개요



[출처: 정보보호 공시 가이드라인]

나. 공시제도의 근거

「정보보호산업의 진흥에 관한 법률」 제13조에 근거한 정보보호 공시제도는 정보통신망을 통하여 정보를 제공하거나 정보의 제공을 매개하는 자가 '정보보호 투자 및 인력 현황, 정보보호 관련 인증 등 정보보호 현황'을 재량에 따라 공개할 수 있는 임의사항으로 정하였다.

원활한 공시 이행을 위하여 과학기술정보통신부에서 정보보호 공시 작성 기준과 방법 등 상세내용을 기재한 '정보보호 공시 가이드라인'을 배포하고, 「정보보호 공시에 관한 고시」를 제정하였음에도 불구하고, 52개 기업만이 정보보호 현황을 공시하는 등 제도 도입 후 5년 경과 시점에도 낮았다.

이에 2021년 정보통신서비스 이용자의 안전한 인터넷 이용 및 기업의 정보보호 투자 촉진을 위하여 일정 규모 이상의 기업에 대하여 정보보호 공시를 의무화하도록 「정보보호산업의

진흥에 관한 법률」을 개정하였다.

2022년부터 정보보호 의무공시제도가 본격 시행됨으로써 대·중견 이상의 상장회사를 비롯하여 주요 정보통신 설비를 갖춘 통신사 및 클라우드 서비스 제공자, 이용자 수가 많아 정보보호 필요성이 큰 온라인 쇼핑, 배달 서비스 운영사 등이 정보보호 공시 의무자에 포함되어 기업의 정보보호 현황을 공시하였다.

다. 공시제도 주요 내용

정보통신망을 통하여 정보를 제공하거나 정보의 제공을 매개하는 자라면 누구나 정보보호 현황을 자율적으로 공시할 수 있다. 다만 사업분야·매출액·이용자 수 등을 고려하여 「정보보호 산업의 진흥에 관한 법률 시행령」 제8조의 기준에 해당하는 자는 반드시 정보보호 현황을 공시하여야 한다.

정보보호 현황을 공시하려는 경우 ▲정보기술부문 투자 현황 대비 정보보호부문 투자 현황 ▲정보기술부문 인력 대비 정보보호부문 전담인력 현황 ▲정보보호 관련 인증·평가·점검 등에 관한 사항 ▲그 밖에 정보통신서비스를 이용하는 자의 정보보호를 위한 활동 현황 등의 내용을 포함하여야 한다.

정보보호 공시를 하는 경우 공시 주체의 정보보호 최고책임자가 주관하여 공시하여야 하는데, 작성한 정보보호 현황(공시내용)에 대하여 최고경영자의 확인을 거친 후 매년 6월 30일 이전까지 전년도 정보보호 현황을 공시 기관에 제출한다. 공시 기관은 그 내용을 과학기술정보통신부 전자공시시스템에 게시한다.

의무공시 대상이 아니지만 자율적으로 정보보호 공시를 이행한 주체는 정보보호 관리 체계 인증(ISMS), 정보보호 및 개인정보보호 관리 체계 인증(ISMS-P)을 신청할 때 인증 수수료(최초, 사후, 갱신 모두 포함)의 30%를 할인받을 수 있다.

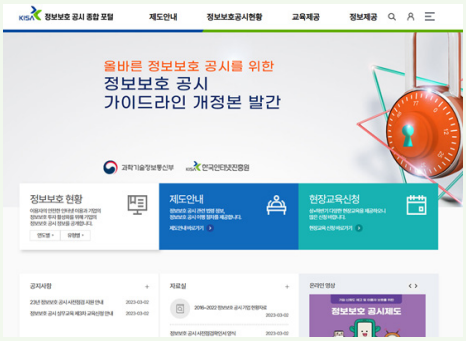
라. 정보보호 공시 현황

2016년 2개 기업, 2017년 10개 기업, 2018년 20개 기업, 2019년 30개 기업, 2020년 45개 기업, 2021년 64개, 2022년 658개 기업이 정보보호 공시제도에 참여하였다.

2022년에는 의무공시 시행으로 정보통신업과 도소매업을 비롯하여 제조업·건설업·보건업 등 다양한 업종 및 규모의 기업·기관이 정보보호 공시제도에 참여하였다. 2022년 12월 기준 테크빌교육·SK텔레콤·NHN 등 49개 기업이 2년 이상 연속으로 정보보호 현황을 공시하였다.

정보보호 공시 현황은 정보보호 공시 종합포털(isds.kisa.or.kr)의 정보보호 공시 현황 페이지에서 확인할 수 있다.

그림 4-1-3-5 정보보호 공시 종합포털



제2장

정보보호 기술 개발

제1절 개요

2020년부터 시작된 코로나19로 인하여 일상 생활뿐 아니라 사이버 환경도 많은 변화가 발생하였다. 특히 비대면·무인화, 재택근무, 화상회의 등이 일상화하면서 사이버 환경에 접근하기 위한 다양한 기기 활용이 증가하였고, 인공지능 등 초지능 기술의 발전으로 어느 때보다 그 활용도가 늘어나고 있다.

2022년 말 정부에서는 12대 국가전략기술과 분야별 목표를 발표하고 미래사회의 기술 주도권을 갖기 위한 노력을 시작하였다. 12대 국가전략기술은 반도체·우주항공 등 미래사회를 주도할 핵심 기술이 포함되었으며, 이에 맞추어 사이버보안도 핵심 전략기술로 포함되었다.

이와 같은 비대면 환경과 사이버 환경의 접점이 늘어나면서 사이버공격 및 범죄 경로가 증가하는 것과 비례하므로 온·오프라인의 경계가 없는 현재 상황에서 정보보호의 이슈 대두는 필연적이다.

그림 4-2-1-1 12대 국가전략기술

[출처: 과학기술정보통신부]

사이버 환경에 접근하는 IoT 등의 기기, 비대면 금융거래 등을 표적으로 하는 해킹 공격, 디도스·랜섬웨어 등 대규모 국민·기업·기관 대상 공격 등 환경 변화에 맞추어 사이버공격 및 범죄 행위가 지속적으로 증가하고 있다.

이에 과학기술정보통신부는 정보보호 분야의 핵심 보안 기술 개발을 위하여 정보통신기획평가원을 통하여 '정보보호핵심원천기술개발' 사업을 추진하고 있으며, 2022년에도 핵심적인 영역의 보안을 위한 기술 개발을 추진하고 있다.

'2022년도 제1차 정보통신·방송 기술개발사업 및 표준개발지원사업 신규지원 대상과제 공고'에는 정보보호 분야뿐 아니라 ICT 융합, 통신·네트워크, 인공지능·데이터 등 다양한 ICT 환경에 필요한 기술 개발 내용이 포함되어 있으며, '정보보호핵심원천기술개발'사업은 3개 내역 사업에 따라 과제를 공고하였다.

표 4-2-1-1 정보보호핵심원천기술개발 사업 추진 세부 과제

번호	내역 사업명	과제명	총 수행 기간	2022년 (총) 출연금	과제 특징
1	ICT인프라·서비스 보호 강화	IoT/IIoT 디바이스 안전성 보장을 위한 취약점 보안검증 기술 개발	4년	10 (46)	• 혁신도약형(선도형) • 디지털 뉴딜R&D • 기술패권경쟁(첨단기술) • 산업체 참여 필수
2		소프트웨어 공급망 보안을 위한 SBOM 자동생성 및 무결성 검증 기술 개발	4년	10 (46)	• 디지털 뉴딜R&D • 기술패권경쟁(첨단기술)
3	융합산업 및 공공기술 역량 강화	다크웹 은닉서비스 식별 및 근원지 추적 기술 개발	4년	10 (46)	• 혁신도약형(선도형) • 디지털 뉴딜R&D • 기술패권경쟁(첨단기술) • 산업체 참여 필수
4		사이버공격 대응을 위한 라이프사이클 기반 공격그룹 식별 및 유형 분석 기술 개발	4년	8 (38)	• 혁신도약형(선도형) • 디지털 뉴딜R&D • 기술패권경쟁(첨단기술) • 산업체 참여 필수
5		랜섬웨어 공격 근원지 식별 및 분석 기술 개발	3년	8 (28)	• 혁신도약형(선도형) • 디지털 뉴딜R&D • 기술패권경쟁(첨단기술)
6		인공지능 기술 활용 디지털 증거 분석 기법 개발	4년	10 (46)	• 디지털 뉴딜R&D • 기술패권경쟁(첨단기술) • 다부처 협력(경찰청)
7		이벤트 기반 실험시스템 구축을 통한 자동차 내·외부 아티팩트 수집 및 통합 분석 기술 개발	3년	11 (35)	• 혁신도약형(선도형) • 디지털 뉴딜R&D • 기술패권경쟁(첨단기술) • 다부처 협력(대검찰청)

번호	내역 사업명	과제명	총 수행 기간	2022년 (총) 출연금	과제 특징
8	유망 신기술 및 글로벌 선도기술 확보	내용 기반 중요문서 분류 및 등급별 보안서비스 개발	6년 (3+3)	7 (52)	• 혁신도약형(전문연구실) • 디지털 뉴딜R&D • 기술패권경쟁(첨단기술)
9		다양한 사용자 환경 및 기업망 보호를 위한 SASE 기반 지능형 통합 보안 엣지 기술 개발	3년	10 (36)	• 디지털 뉴딜R&D • 기술패권경쟁(첨단기술) • 산업체 참여 필수
10		엣지 인공지능 보안지능의 지속적 최적화 및 엣지 보안단말의 연계 협업을 지원하는 무선 엣지 영상보안시스템 기술 개발	4년	7.5 (37.5)	• 사회문제해결형 • 디지털 뉴딜R&D • 기술패권경쟁(첨단기술) • 산업체 참여 필수
11		자가진화형 인공지능 기반 사이버 공방 핵심원천기술 개발	6년 (3+3)	7 (52)	• 혁신도약형(전문연구실) • 디지털 뉴딜R&D • 기술패권경쟁(첨단기술)

[출처: 과학기술정보통신부]

이처럼 사이버위협이 증가하는 환경에서 사용자의 사이버 접점에 있는 기기의 보안, 사이버 공격 및 범죄 피해 방지, 인공지능 기반의 보안 기술 등 사이버보안 핵심원천기술의 개발 사항에 대하여 살펴본다.

제2절 원천기술 개발

1. ICT 인프라·서비스 보호 강화 기술

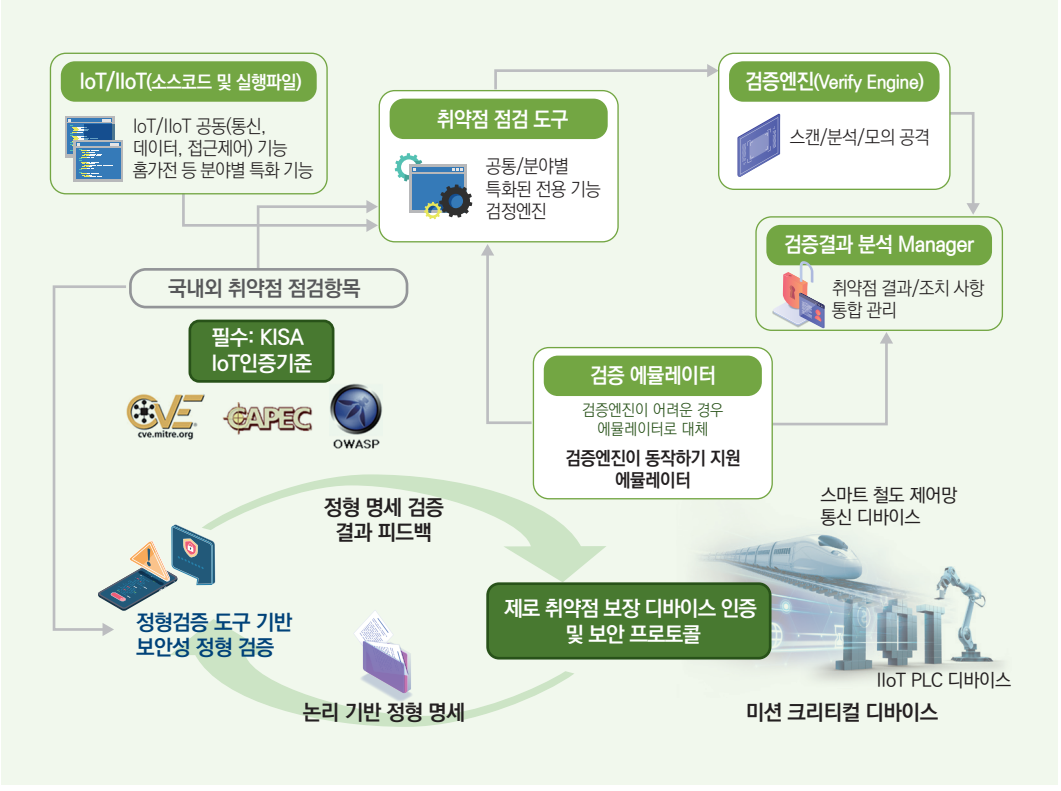
가. IoT/IIoT 디바이스 안전성 보장을 위한 취약점 보안검증 기술

IoT(Internet of Things)/IIoT(Industrial Internet of Things) 시장이 급격하게 성장함과 동시에 디바이스로부터 발생할 수 있는 지능화된 사이버보안 위협이 계속 증가하고 있다. 이와 관련하여 일상 생활과 밀접하게 관련되고, 높은 수준의 보안성을 요구하는 미션 크리티컬 IoT/IIoT 디바이스를 안전하게 보호하여야 할 필요가 있으며, IoT/IIoT 디바이스에 대한 보안

취약점을 미리 점검함으로써 외부 공격에 대응할 수 있는 기술을 제공하여야 한다.

이에 '일반 생활에 밀접한 주택·가전 위주의 IoT/IIoT 디바이스뿐 아니라 고도의 사이버 공격에 대응하기 위하여 높은 수준의 보안성을 보증하는 정형 검증 기반 디바이스 보안검증 기술 개발'이 추진되고 있다.

그림 4-2-2-1 IoT/IIoT 디바이스 안전성 보장을 위한 취약점 보안검증 기술 개념



[출처: 정보통신기획평가원]

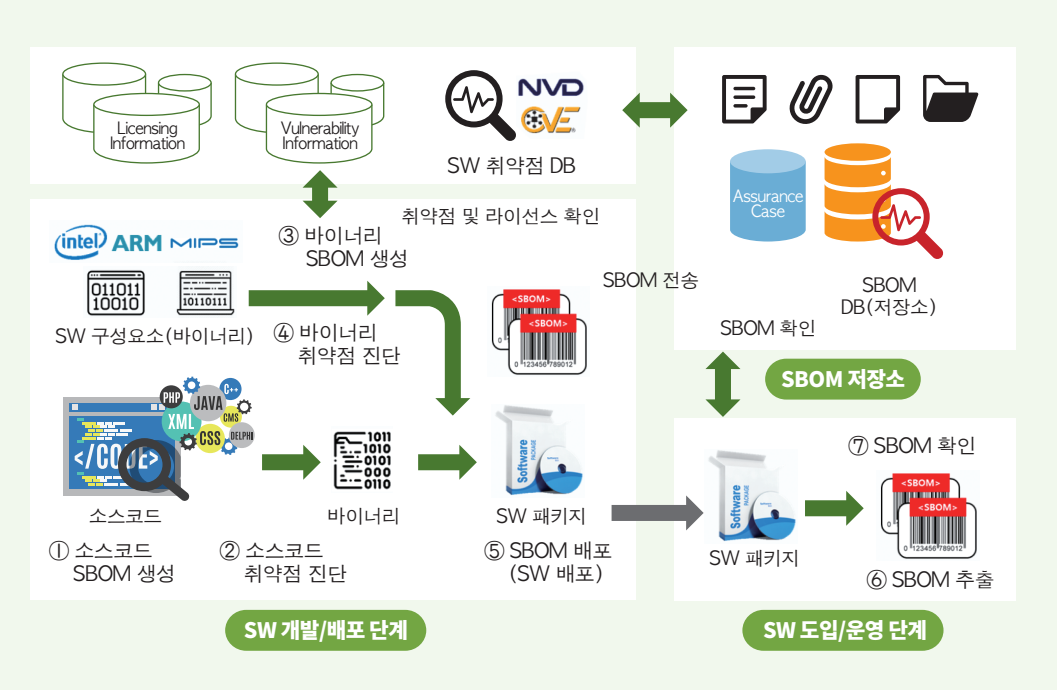
나. 소프트웨어 공급망 보안을 위한 SBOM 자동생성 및 무결성 검증기술

소프트웨어 제조·유통과정에서 악성 소프트웨어를 설치하는 등 소프트웨어 공급망 전주기에 걸친 보안 위협이 계속 발생하고 있으며, 복잡한 공급망 구조로 인하여 취약점 패치 등 신속하게 사고 대응을 할 수 없어 소프트웨어 공급망 신뢰성 확보에 어려움을 겪고 있다. 투명한 소프트웨어 공공조달 제도의 정착 등 안전한 소프트웨어 배포를 위해서는 소프트웨어 구성요소 자동 분석 및 SBOM(Software Bill of Materials) 생성을 통하여 소프트웨어

무결성을 검증할 수 있는 보안 기술을 제공하여야 한다.

이에 '소스코드나 바이너리 형태의 소프트웨어 구성요소를 자동 분석하여 보안취약점과 연계한 SBOM을 생성하고, 무결성 기반 생성 배포기술을 가진 SBOM 저장소와 연계하여 보안취약점 및 위·변조를 탐지할 수 기술 개발'이 추진되고 있으며, 이는 인공지능 기술을 활용한 정적·동적 기반의 바이너리, 소스코드 취약점 탐지 기술 등을 제공할 수 있다.

그림 4-2-2-2 소프트웨어 공급망 보안을 위한 SBOM 자동생성 및 무결성 검증기술 개념



[출처: 정보통신기획평가원]

2. 융합산업 및 공공기술 역량 강화

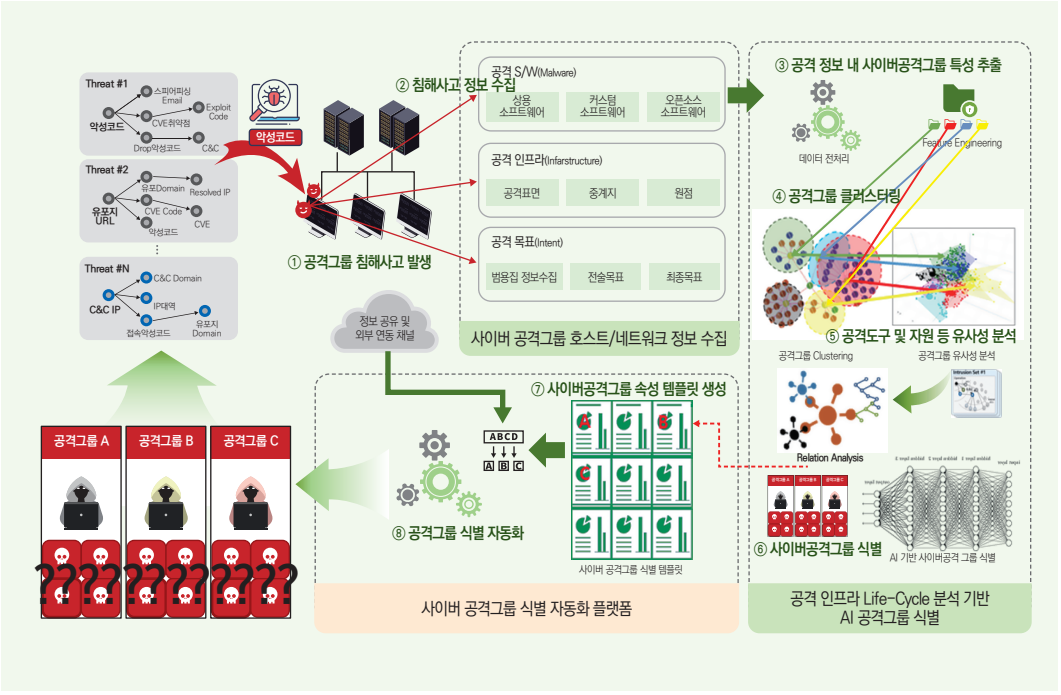
가. 사이버공격 대응을 위한 공격그룹 식별 및 유형 분석 기술

최근 사이버공격은 기존의 무차별적 공격에서 정교하게 타깃화된 공격으로 진행하고 있으며, 기술이 고도화되고 구조적으로 조직화되면서 공격그룹의 활동이 크게 증가하고 있다. 특히 정부 차원의 지원을 받는 공격이 증가하고 단계별 역할을 구분한 조직적 공격이 발생하고 있다.

그러나 현재의 사이버공격 및 공격그룹에 대한 분석 기술은 악성코드 기반의 도구 분석이 대부분이어서 공격과 공격그룹의 연관성을 식별하기에는 제한적이다. 이는 공격그룹에 대한 원천적 대응이 어렵다는 것을 의미한다.

따라서 기존 사이버공격 분석 및 공격그룹 식별제한의 한계점을 극복하기 위하여 공격 원점에서 최종 피해 발생지까지의 공격행위 전반에 대한 분석 및 공격그룹 식별을 통한 추적·대응 기술 개발이 필요하다. 이에 사이버공격 그룹을 빠르게 식별하고 추적·대응하기 위하여 공격 인프라의 라이프사이클 분석을 통한 인공지능 기반 공격그룹 식별과 지속적으로 발생하는 새로운 공격의 자동 식별 및 정보공유 플랫폼 기술 개발이 진행되고 있다.

그림 4-2-2-3 사이버공격 그룹 식별 및 유형 분석 기술 개념



[출처: 정보통신기획평가원, 한국인터넷진흥원]

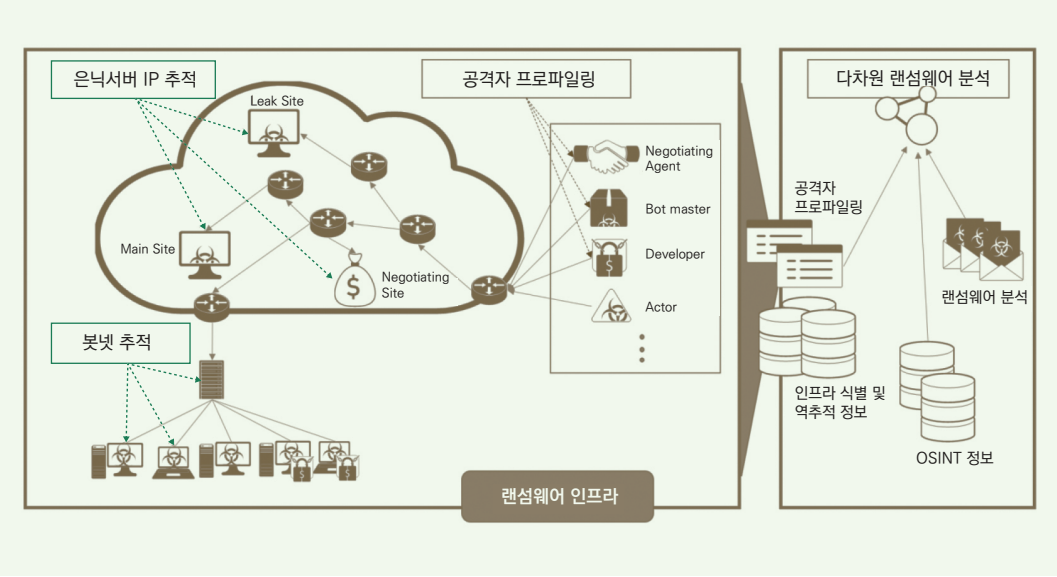
나. 랜섬웨어 공격 근원지 식별 및 분석 기술

랜섬웨어를 통한 사이버 범죄로 인하여 개인·기업·기관 등의 금전적 피해뿐 아니라 개인정보 유출 등 2차 피해가 지속적으로 발생하고 있다. 국가 차원에서는 핵심기술 유출이나 주요 지적재산권의 피해 등이 유발되고 있는 상황이다. 이러한 범죄는 자신을 감추기 위하여 다크웹을

주활동 영역으로 움직이고 있고, 외부에 잘 드러나지 않는 시스템의 특성상 실제 수사의 한계 및 피해 방지에 어려움을 겪고 있다.

이에 다크웹에서 활동하는 랜섬웨어 범죄뿐 아니라 이와 협업하는 다수의 범죄활동 조직의 정보를 획득·분석하는 기술과 이를 통한 랜섬웨어 운영자·핵심 범죄자를 추적하는 기술 등에 대한 연구개발이 추진되고 있다.

그림 4-2-2-4 랜섬웨어 공격 근원지 식별 및 분석 기술 개념



[출처: 정보통신기획평가원]

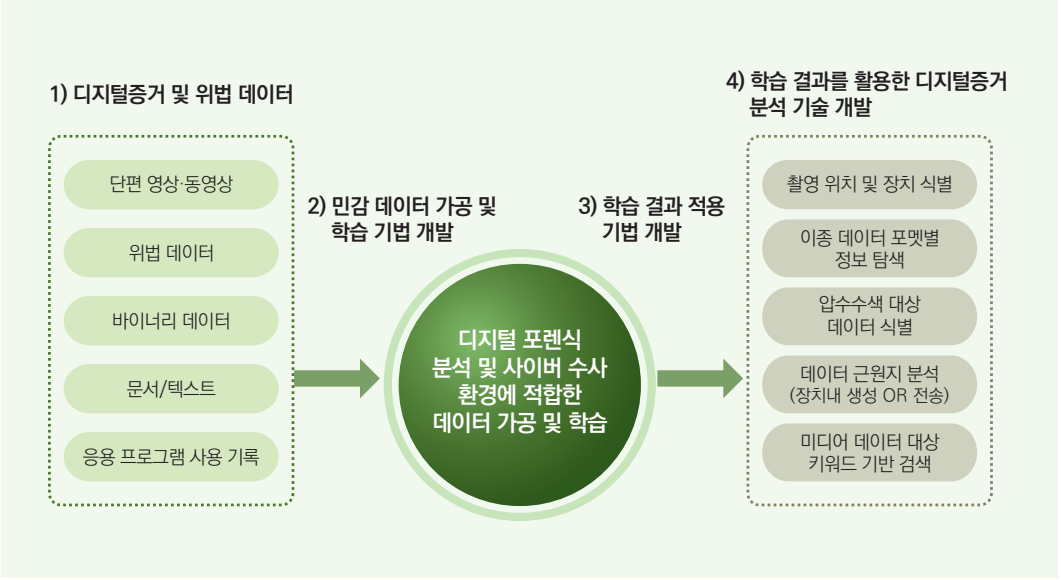
다. 인공지능 기술 활용 디지털 증거 분석 기술

다양한 수사에서 디지털 정보를 증거로 활용하고 있으나, 이를 분석하여 실제 수사에 활용될 수 있는 법적 증거를 확보하는 분석관은 여전히 부족한 상황이다. 디지털 증거 분석 수요 증가로 인하여 분석관을 지속적으로 증원하고 있으나, 기존의 전통적인 분석만으로는 기술의 발전과 디지털 매체의 다양화로 인한 대량 발생 디지털 정보의 증거화 및 분석 대응이 한계에 이르고 있다. 또한 다수의 데이터 내 위법 데이터를 분석·식별하고, 서로 다른 데이터의 유형을 모두 고려하여 분석하는 것에 다수의 시간이 소모되어 효율성에도 어려움이 있는 상황이다.

빠른 수사 대응을 통하여 공공 안전을 확보하기 위해서는 범죄 수사력 및 디지털 포렌식 분석 역량 강화를 위한 디지털 증거의 효과적 선별 및 분석 기술이 필요하다. 이에 국내 환경에

맞는 데이터를 구축하여 인공지능 기반의 디지털 증거 분석 도구를 개발하고, 위법 데이터 식별 및 이종 데이터의 유사도 분석, 확보된 디지털 증거에 숨겨진 아티팩트 선별 등의 기술 개발이 진행 중이다.

그림 4-2-2-5 인공지능 기술 활용 디지털 증거 분석 기술 개념



[출처: 정보통신기획평가원]

3. 유망 신기술 및 글로벌 선도 기술 확보

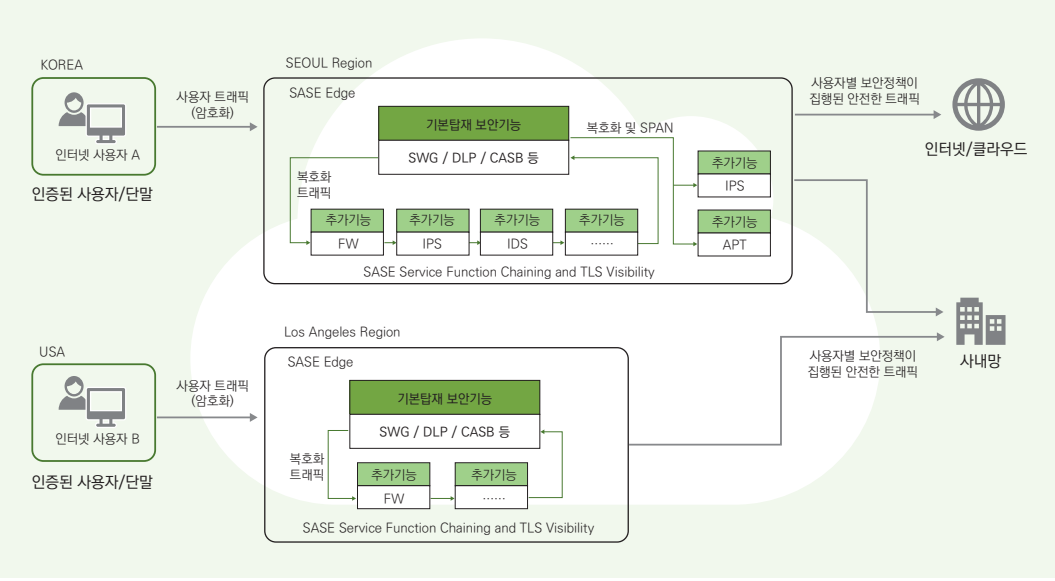
가. 다양한 사용자 환경 및 기업망 보호를 위한 SASE 기반 지능형 통합 보안 엣지 기술

비대면 시대의 확산으로 재택·원격근무, 화상회의 등 기업 근무 환경이 변화함에 따라 기존 온프레미스 환경에서 제공하고 있는 보안 기능으로는 클라우드 기반의 중요 데이터 보호, 단말에 대한 신뢰성 확보 등에 한계가 존재한다. 이를 위하여 다양한 네트워크 환경 및 기업망을 보호하기 위한 안전한 사용자 인증 기술 등 여러 보안 기능을 하나의 클라우드 보안 서비스로 제공할 수 있는 SASE(Secure Access Service Edge) 기반의 지능형 엣지 기술이 요구되고 있다.

이에 '신뢰된 사용자 및 기기 인증을 통하여 가장 가까운 위치에서 다양한 클라우드 기반 보안 서비스를 단일 플랫폼으로 제공 가능한 SASE 기반 지능형 보안 엣지 기술 개발'을

추진하고 있으며, 이는 SWG·DLP·CASB·NGFW 등이 통합된 지능형 클라우드 네트워크 보안 엣지 기술 등을 제공할 수 있다.

그림 4-2-2-6 SASE 기반 지능형 통합 보안 엣지 기술 개념



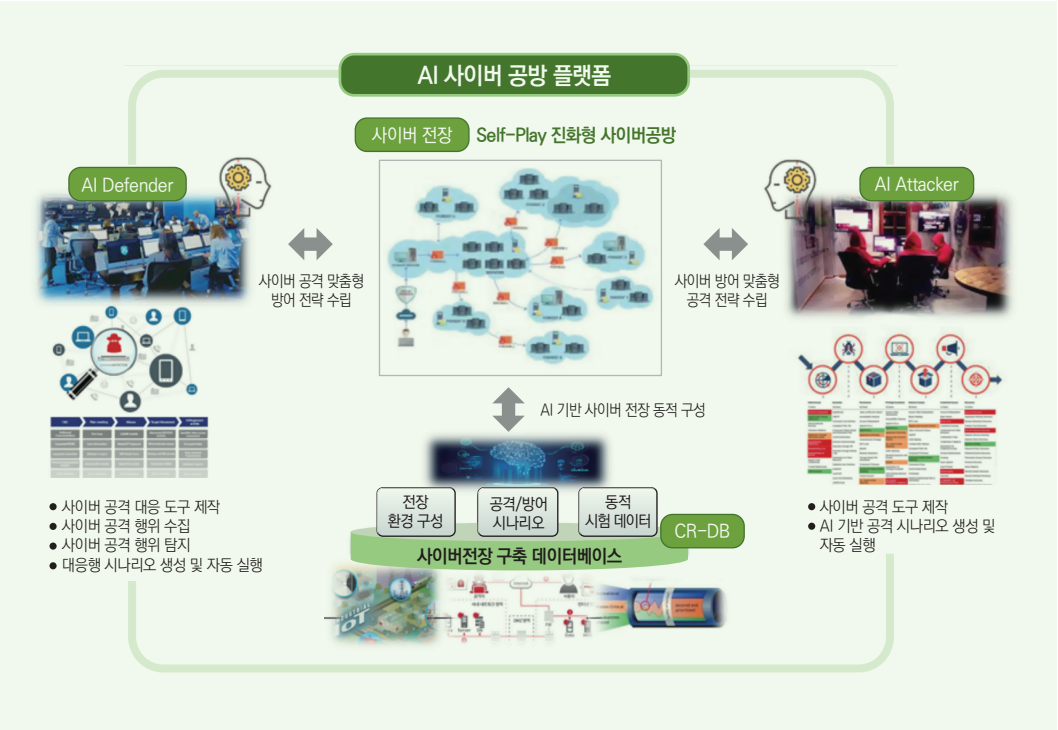
[출처: 정보통신기획평가원]

나. 자가진화형 인공지능 기반 사이버 공방 핵심원천기술 개발

현재 사이버전 대응 훈련 도구는 일부 제한된 전문가에 의하여 수동으로 진행되고 있기 때문에 민·군 등 다양한 운영 환경에서 체계적으로 훈련을 수행하기에는 한계가 존재한다. 더욱이 최신 인공지능 기술을 활용한 자가진화형 사이버 공방 시뮬레이션에 관한 연구가 미흡하고, 국가 차원에서의 능동적인 사이버전 대응 훈련 도구가 부재함으로, 대규모 사이버전장 ICT 인프라 데이터를 수집·학습하여 최적의 공격·대응 전략을 생성 및 실행하는 인공지능 공격자와 방어자 간 사이버전을 수행할 수 있는 사이버 공방 핵심원천기술 개발이 필요하다.

이에 '사이버 공격 시나리오를 자동으로 생성·실행하는 AI Attacker(레드팀)와 최적의 방어전략을 수립·실행하는 AI Defender(블루팀)가 사이버전(Self-Play)을 수행하며 스스로 학습·진화하는 인공지능 기반 진화형 사이버 공방 핵심기술 및 인공지능 기반 사이버 훈련장 수요처 실증'을 추진하고 있다.

그림 4-2-2-7 자가진화형 인공지능 기반 사이버 공방 핵심원천기술 개념



[출처: 정보통신기획평가원]

4. 글로벌 정보보호 표준 주도권 확보 및 정보보호산업 경쟁력 강화

가. 정보보호 분야 국가표준 개발

디지털 대전환에 따른 사이버보안 강화 및 관련 산업 육성을 위하여 국가 정책 방향에 발맞추어 다양한 정보보호 분야의 국가표준을 선제적으로 개발하고 있다. 정보보호 분야 국가표준은 정보보호 관리 체계, 개인정보보호, 암호 알고리즘, 사이버보안 위협 대응 등 폭넓은 분야의 산·학·연 전문가들이 다년간 국제표준화 활동을 적극적으로 수행하여 제정한 국제표준을 기반으로 관련 산업계에서 널리 활용 가능하도록 한글로 부합화하여 개발하고 있다.

2022년 정보보호 분야 국가표준은 개인정보보호, 정보보호 관리 체계, 암호 알고리즘, 네트워크 보안 등의 분야에서 총 15건 제·개정되었다.

표 4-2-2-1 정보보호 분야 2022년 국가표준 제·개정 현황

구분	표준번호	표준명	제·개정일
개정	KS X ISOIEC10118-1	정보 기술 - 보안 기술 - 해시 함수 - 제1부 : 일반	2022. 12. 28.
개정	KS X ISOIEC18028-1	정보 기술 - 보안 기술 - IT네크워크 보안 - 제1부 : 네트워크 보안 관리	
개정	KS X ISOIEC18033-2	정보 기술 - 보안 기술 - 암호 알고리즘 - 제2부: 비대칭형 암호	
개정	KS X ISOIEC27033-3	정보 기술 - 보안 기술 - 네트워크 보안 - 제3부: 참조 네트워킹 시나리오 — 위협, 디자인 기술과 통제 이슈	
개정	KS X ISOIEC10118-1	정보 기술 - 보안 기술 - 해시 함수 - 제1부 : 일반	
개정	KS X ISOIEC11770-4	정보 기술 - 정보보안 - 키 관리 - 제4부 : 취약한 비밀 기반한 메커니즘	
개정	KS X ISOIEC18028-1	정보 기술 - 보안 기술 - IT네크워크 보안 - 제1부 : 네트워크 보안 관리	
개정	KS X ISOIEC18028-3	정보 기술 - 정보보안 - IT네트워크 보안 - 제3부 : 보안 게이트웨이를 이용한 네트워크 간 안전한 통신	
개정	KS X ISOIEC18032	정보 기술 - 정보보안 - 소수생성기	
개정	KS X ISOIEC18033-2	정보 기술 - 보안 기술 - 암호 알고리즘 - 제2부: 비대칭형 암호	
개정	KS X ISOIEC18043	정보 기술 - 정보보안 - 침입탐지시스템의 선택, 배치, 운용	
개정	KS X ISOIEC27031	정보 기술 - 보안기법 - 업무연속성을 위한 정보통신기술 준비도 가이드라인	
개정	KS X ISOIEC27033-3	정보 기술 - 보안 기술 - 네트워크 보안 - 제3부: 참조 네트워킹 시나리오 — 위협, 디자인 기술과 통제 이슈	
개정	KS X ISO/IEC27000:2018	정보 기술 — 보안 기술 — 정보보호 관리 체계 — 개요와 용어	2022. 2. 25.
제정	KS X ISO/IEC27701	보안 기술 — 개인정보보호 관리를 위한 KS X ISO/IEC 27001과 KS X ISO/IEC 27002의 확장 — 요구사항과 지침	
합계	제정 1건, 개정 14건		

국가표준 제·개정 현황을 세부적으로 살펴보면, 정보보호 정책에서 개인식별정보 보호 관련 법률을 구체화하고 준수 및 보안 사고의 책임과 절차, 개인식별정보 유출 사고를 방지하기 위한 기술적·조직적 조치 수립을 위한 인증제도(KS X ISO/IEC27701), 네트워크 시나리오와 관련된 위협에 대한 상세 지침 및 위험을 완화하는 데 필요한 설계기법(KS X ISOIEC27033-3) 등이 2022년 국가표준으로 고시되었다.

나. 정보보호 분야 단체표준 개발

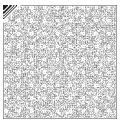
정보보호 분야 단체표준화는 디지털 뉴딜 및 K-사이버방역 등 정부 정책 방향에 부합하는 안전한 데이터 생태계 구축 및 디지털 안심국가 실현을 위하여 양자 컴퓨팅 및 초연결 네트워크 환경을 고려하여 다양한 응용 분야에 적용 가능한 차세대 보안 기술에 대한 표준화를 추진하고 있다. 국내 정보보호 분야 단체표준은 한국정보통신기술협회(TTA)에서 운영하는 정보통신표준화위원회 산하 정보보호기술위원회를 중심으로 개발 중이며, 특히 정보보호 기반, 개인정보보호/ID 관리 및 블록체인 보안, 사이버보안, 응용보안 및 평가인증, 바이오인식 기술 등에 대한 표준을 중점적으로 제정하고 있다.

2022년 정보보호 분야에서는 총 22건의 단체표준과 4건의 기술보고서를 제·개정하였다. 코로나19 확산 및 지속에 따른 개인 프라이버시 보호 및 안전한 개인인증을 위한 표준등이 시의적절하게 개발되었다. 구체적으로는 의료 사물인터넷(IoMT) 플랫폼 사이버보안 점검지침, 스마트시티 플랫폼 소프트웨어 보안요구사항, 스마트공장에서의 5G MEC 보안 요구사항, 분산식별자 구현 지침 등에 대한 표준 등이 주로 제정되었다.

다. 글로벌 정보보호 표준 경쟁력 강화

사이버보안 위협이 날로 지능화·고도화함에 따라 전세계적으로 합의된 정보보호 표준을 기반으로 한 보안 기술을 적용하고, 글로벌 공동 보안 위협 대응 체계를 구축하고 하는 것이 요구되고 있다. 이에 따라 정보보호 분야 산·학·연 전문가 및 유관 조직들은 사이버보안 위협에 효과적·체계적으로 대응하고 나아가 표준을 기반으로 한 정보보호산업 경쟁력을 강화하고자 국내 원천기술을 개발하고 이를 국제전기통신연합(ITU, International Telecommunication Union), ISO/IEC JTC 1(International Organization for Standardization /International Electrotechnical Commission Joint Technical Committee, ISO/IEC 공동기술위원회) 등에 국제표준으로 제안함으로써 적극적인 표준개발 활동을 지속하고 있다.

ITU-T SG17(Study Group 17, 정보보호)은 ITU 산하의 정보통신 관점에서 정보보호 응용서비스 기술에 대한 국제표준을 개발하는 조직이다. 세부적으로 SG17에서는 5G 등을 포함한 네트워크 보안, 정보보호 관리 체계 기술, 사이버보안 및 스팸 대응, 응용 서비스 보안, 신원 관리 및 텔레바이오 인식 기술, 공개키 기반구조 등 보안 응용을 지원하는 일반 기술,



차량통신 보안, 분산원장기술 보안, 양자기반 보안 등에 대한 국제표준을 개발하고 있으며, 순천향대학교 염흥열 교수가 SG17 국제 의장을 수임하는 등 다수의 국내 의장단 및 에디터들이 활발하게 표준을 개발하고 있다.

ISO/IEC JTC 1/SC 27(Sub Committee 27, 정보보안, 사이버보안, 프라이버시 보호)은 ISO/IEC JTC 1 산하의 정보 기술 보안을 위한 일반적 방법과 기술에 대한 국제표준을 개발하는 조직이다. 세부적으로 SC 27에서는 정보보호 관리 체계, 암호화 알고리즘 및 보안 메커니즘, 보안성 평가 기준, 보안 통제 및 서비스, 개인정보보호 및 신원 관리 등에 대한 국제표준을 개발하고 있으며, 국내 고유기술로 개발한 암호 알고리즘, 개인정보보호 기술 등을 국제표준에 적극적으로 반영하고 있다.

이러한 왕성한 국제표준화 활동을 앞으로도 정부와 산·학·연을 중심으로 지속적으로 수행하여, 글로벌 정보보호 표준 주도권 확보 및 정보보호산업의 경쟁력 강화를 꾀할 예정이다.

제3절 상용기술 개발

상용기술 개발자료는 국내 소재 정보보호 기업 총 1,517개(정보보안 669개, 물리보안 848개)를 대상으로 한국정보보호산업협회에서 조사하여 작성한 '2022 정보보호산업실태조사' 결과를 활용하였다.

1. 정보보안 기업의 연구소 및 연구개발 전담부서 운영 현황

정보보안 기업의 기술 개발 관련 자체기술연구소 및 전담부서 운영 현황을 조사한 결과, 기업부설연구소를 운영하는 기업은 479개(71.6%), 연구개발 전담부서를 운영하는 기업은 70개(10.5%)로 조사되었다. 기업부설연구소와 연구개발 전담부서를 모두 운영하지 않는 기업은 120개(17.9%)로 나타나 80%가 넘는 정보보안 기업이 자체적인 기술 개발 및 연구에 힘쓰고 있음을 알 수 있다.

기업부설연구소를 운영하는 479개 기업 중 20인 이상 100인 미만의 기업이 283개였으며, 20인 미만 기업은 161개로 나타났다.

표 4-2-3-1 정보보안 기업 자체기술연구소 및 전담부서 운영 현황

(단위: 개, %)

구분	종사자 기준				운영 현황	
	20인 미만	20인 이상 100인 미만	100인 이상 200인 미만	200인 이상	합계	비율
기업부설연구소 운영	161	283	23	12	479	71.6
연구개발 전담부서 운영	47	12	2	9	70	10.5
없음	73	35	5	7	120	17.9
합계	281	330	30	28	669	100.0

2. 기술 개발 투자 현황

정보보안 기업의 연도별 기술 개발 투자액 현황 및 전망을 조사한 결과 2022년 전체 투자액이 있는 기업은 235개 평균 753백만 원, 연구개발 투자액 규모는 235개 기업 평균 733백만 원을 투자한 것으로 나타났다.

기업당 기술 개발에 투자하는 평균 금액은 해마다 증가하고 있으며, 이를 매출액 대비 비중으로 환산해 보면 2021년 14.2%, 2022년 14.1%로 확인할 수 있다.

표 4-2-3-2 정보보안 기업 연도별 기술 개발 투자액 현황

(단위: 개, 백만 원, %)

구분	2021		2022	
	기업 수	투자액 평균	기업 수	투자액 평균
전체 투자액 (연구개발/건물/기계/설비 등)	235	754	235	753
연구개발 투자액		737		733
매출 대비 투자 비율	14.2		14.1	

3. 매출 현황

2021년 정보보안 산업 전체의 매출은 4조 5,497억 원이며, 이 중 정보보안 제품(솔루션)은 약 3조 1,230억 원, 정보보안 관련 서비스는 약 1조 4,266억 원으로 나타났다.

표 4-2-3-3 정보보안 대분류별 매출 현황

(단위: 백만 원, %)

구분	2021	비중
정보보안 제품(솔루션)	3,123,055	68.6
정보보안 관련 서비스	1,426,679	31.4
합계	4,549,734	100.0

정보보안 관련 주요 매출 분야는 정보보안 제품(솔루션)이 정보보안 관련 서비스보다 약 2배 이상 비중이 높으며, 분야별 세부 매출 현황은 [표 4-2-3-4]와 같이 조사되었다.

표 4-2-3-4 정보보안 제품 및 서비스 매출 현황

(단위: 백만 원)

구분		2021
정보보안 제품(솔루션)	네트워크 보안 솔루션	943,201
	앤드포인트 보안 솔루션	614,592
	플랫폼 보안·보안관리 솔루션	197,830
	클라우드 보안 솔루션	78,623
	콘텐츠·데이터 보안 솔루션	612,153
	공통 인프라 보안 솔루션	676,657
정보보안 관련 서비스	보안컨설팅 서비스	501,012
	보안시스템 유지관리, 보안성 지속 서비스	416,134
	보안관제 서비스	400,206
	보안인증 서비스	5,645
	보안교육 및 훈련 서비스	103,682
합계		4,549,734

4. 수출 현황

정보보안 산업 2021년 수출액은 1,526억 원으로 조사되었다. 2021년 수출 비중을 살펴보면 정보보안 제품(솔루션)의 수출이 전체 수출의 81.7%로 정보보안 관련 서비스(18.3%)보다 높게 나타났다.

표 4-2-3-5 정보보안 대분류별 수출 현황

(단위: 백만 원, %)

구분	2021	비중
정보보안 제품(솔루션)	124,640	81.7
정보보안 관련 서비스	27,964	18.3
합계	152,604	100.0

분야별로 살펴보면 정보보안 제품(솔루션)에서는 네트워크 보안 솔루션 제품이 수출 시장에서 차지하는 규모가 2021년 554억 원으로 가장 크며, 다음으로 콘텐츠·데이터 보안 솔루션 제품이 350억 원으로 나타났다.

정보보안 관련 서비스에서는 보안컨설팅 서비스의 2021년 수출액이 111억 원으로 가장 크게 나타났다.

표 4-2-3-6 정보보안 제품 및 서비스 수출 현황

(단위: 백만 원)

구분		2021
정보보안 제품 (솔루션)	네트워크 보안 솔루션	55,440
	앤드포인트 보안 솔루션	12,560
	플랫폼 보안·보안관리 솔루션	-
	클라우드 보안 솔루션	14,715
	콘텐츠·데이터 보안 솔루션	35,011
	공통 인프라 보안 솔루션	6,914
정보보안 관련 서비스	보안컨설팅 서비스	11,100
	보안시스템 유지관리, 보안성 지속 서비스	7,769
	보안관제 서비스	9,095
	보안교육 및 훈련 서비스	-
	보안인증 서비스	-
합계		152,604

제3장

정보보호 인력 양성

제1절 개요

'2022년 정보보호산업실태조사'에 따르면 국내 소재 정보보호 기업 1,517개(정보보안 669개, 물리보안 848개)를 대상으로 조사한 결과 정보보호산업 인력 수는 총 63,562명(2021년 12월 기준)으로, 이 중 정보보안 인력은 17,699명(27.8%), 물리보안 인력은 45,863명(72.2%)인 것으로 조사되었다.

직급별로는 15년 이상 기술자가 7,618명(12.0%), 11년 이상 15년 미만 기술자가 9,406명(14.8%), 7년 이상 11년 미만 기술자가 12,885명(20.3%), 4년 이상 7년 미만 기술자가 16,439명(25.9%), 4년 미만 기술자가 17,214명(27.1%)으로 조사되었다.

표 4-3-1-1 정보보호산업 인력 현황

(단위: 명, %)

구분	정보보안	물리보안	합계					
			4년 미만	4년 이상 7년 미만	7년 이상 11년 미만	11년 이상 15년 미만	15년 이상	합계
인원 수	17,699	45,863	17,214	16,439	12,885	9,406	7,618	63,562
비중	27.8	72.2	27.1	25.9	20.3	14.8	12.0	100.0

정보보호산업 매출액 규모별 인력 현황을 살펴보면 100억 이상 기업체가 전체 63,562명 중 48,239명을 보유하고 있으며, 10억 미만 기업체가 2,251명, 10억 이상 50억 미만 기업체가 7,591명, 50억 이상 100억 미만 기업체가 5,481명의 인력을 보유하고 있는 것으로 조사되었다.

표 4-3-1-2 정보보호산업 매출 규모별 인력 현황(2021. 12. 기준)

(단위: 명)

매출액 규모	4년 미만	4년 이상 7년 미만	7년 이상 11년 미만	11년 이상 15년 미만	15년 이상	합계
10억 미만	333	927	423	261	307	2,251
10~50억 미만	1,723	1,711	1,614	1,316	1,227	7,591
50~100억 미만	1,232	1,146	1,200	927	976	5,481
100억 이상	13,926	12,655	9,648	6,902	5,108	48,239
합계	17,214	16,439	12,885	9,406	7,618	63,562

2022년 정보보호 기업체의 신규 채용 현황은 총 6,407명이며, 이 중에서 신입은 2,962명(46.2%), 경력은 3,445명(53.8%)으로 경력 채용이 더 많은 것으로 조사되었다.

표 4-3-1-3 정보보호산업 채용 규모(2021년 기준)

(단위: 명, %)

구분	정보보안			물리보안			합계		
	신입	경력	소계	신입	경력	소계	신입	경력	합계
인원 수	1,351	1,230	2,581	1,611	2,215	3,826	2,962	3,445	6,407
비중	52.3	47.7	100	42.1	57.9	100	46.2	53.8	100

제2절 정규교육 과정

2022년 대학·대학원의 정보보호 관련 학과 현황 조사 결과에 따르면 전문대학 7개, 일반대학 45개, 대학원 58개로 총 110개 학과가 운영되고 있다. 2022년 전문대학 이상 정규교육기관의 재적학생 수는 8,245명으로 나타났다.

1. 전문대학

전문대학의 정보보호 관련 학과에서는 주로 컴퓨터(사이버) 정보보안 등을 교육하고 있으며, 2022년 기준 재적학생 수는 419명으로 나타났다.

표 4-3-2-1 2022년 전문대학 정보보호 관련 학과 현황

(단위: 명)

대학교명	학과명	재적학생 수
ICT폴리텍대학	정보보안학과	32
경복대학교	소프트웨어융합과 사이버보안전공	22
명지전문대학	인터넷보안공학과	105
부천대학교	컴퓨터정보보안과	11
신구대학교	정보통신보안과	123
영남이공대학교	사이버보안스쿨	52
조선이공대학교	컴퓨터보안과	74
계	7개	419

[출처: 대학알리미, www.academyinfo.go.kr]

2. 일반대학

정규교육 과정을 통한 체계적인 인력 양성을 위하여 대학·대학원 등에서 정보보호 학과를 신설하거나 기존 학과를 정보보호 관련 학과로 변경하는 등 전반적으로 정보보호 관련 학과에 대한 지속적인 관심을 보이고 있으며, 2022년 일반대학의 정보보호 관련 학과 재적인원은 6,282명으로 나타났다.

최근 들어 사이버침해 사고가 급증하고 국민의 생명·안전·재산을 위협하면서 정보보호의 중요성에 대한 국민적 관심 또한 높아지고 있다. 이러한 사회적 관심과 중요성이 반영되면서 정보보호 인력 양성의 중요성과 필요성 또한 커지고 있다. 또한 ICT 환경 변화와 함께 다양한 ICT 융합 제품·서비스 등으로 보안위협이 확산되면서 융합보안 등과 관련된 학과도 등장할 것으로 보인다.

표 4-3-2-2 2022년 대학 정보보호 관련 학과 현황

(단위: 명)

대학교명	학과명	재적학생 수
가천대학교	컴퓨터공학부(스마트보안전공)	50
건양대학교	사이버보안학과	41
경남대학교	컴퓨터보안전공	74
경희사이버대학교	AI사이버보안전공	77
고려대학교	사이버국방학과	114
	스마트보안학부	56
고려대학교(세종)	인공지능사이버보안학과	130
광주대학교	사이버보안경찰학과	53
국민대학교	정보보안암호수학과	175
단국대학교	산업보안학과	67
대구가톨릭대학교	사이버보안전공	120
대구대학교	컴퓨터정보공학부(정보보호전공)	61
대전대학교	정보보안학과	167
덕성여자대학교	사이버보안전공	59
동국대학교	융합보안학과	165
동명대학교	정보보호학과	132
동서대학교	정보보안학과	116
동신대학교	정보보안학과	126
목포대학교	정보보호학과	139
	컴퓨터·정보보호학부	22
배재대학교	정보보안학전공	89
상명대학교	정보보안공학과	163
서울디지털대학교	정보보안전공	51
서울사이버대학교	빅데이터·정보보호학과	451
서울여자대학교	정보보호학과	366
성신여자대학교	융합보안공학과	328
세종대학교	정보보호학과	140

대학교명	학과명	재적학생 수
세종사이버대학교	정보보호학과	292
수원대학교	정보보호전공	171
순천향대학교	정보보호학과	249
아주대학교	사이버보안학과	187
영산대학교	사이버보안학과	37
우석대학교	정보보안학과	134
우송대학교	IT융합학부 컴퓨터정보·보안전공	223
위덕대학교	경찰정보보안학과	95
유원대학교	정보통신보안학과	117
이화여자대학교	사이버보안전공	139
제주국제대학교	정보보안공학과	13
조선대학교	정보통신공학부(정보보안전공)	93
중부대학교	정보보호학전공	202
중앙대학교	산업보안학과	183
청주대학교	디지털보안전공	120
한국해양대학교	해사인공지능·보안학부	61
한세대학교	산업보안학과	109
한양사이버대학교	해킹보안학과	325
계	45개	6,282

[출처: 대학알리미, www.academyinfo.go.kr]

3. 대학원

최근 산업과 ICT 간 융합이 확산됨에 따라 융합보안 관련 학과 및 전공이 꾸준히 신설되고 있다. 2022년 대학원의 정보보호 관련 학과는 총 58개이며, 재적학생 수는 1,544명으로 나타났다.

표 4-3-2-3 2022년 대학원 정보보호 관련 학과 현황

(단위: 명)

대학원명		학과명	재적학생 수
가천대학교 일반대학원		정보보호학과	8
강원대학교	일반대학원	융합보안학과	20
	정보과학·행정대학원	정보보안전공	3
건국대학교	일반대학원	IT융합정보보호학과	1
	정보통신대학원	정보보안학과	66
경북대학교 일반대학원		정보보호학학과간협동과정	4
경일대학교 일반대학원		사이버보안학과	1
고려대학교	대학원	정보보안학과	78
고려대학교	정보보호대학원	금융보안학과 금융보안정책전공	17
		디지털포렌식학과	21
		사이버보안학과	41
		융합보안학과	16
		융합보안학과 Samsung Advanced Security전공	8
		정보보호학과	190
고려대학교 컴퓨터정보통신대학원		소프트웨어보안학과	31
고려대학교(세종) 일반대학원		사이버보안학과	2
국민대학교	대학원	금융정보보안학과협동과정	39
		보안스마트에어모빌리티학과	3
	법무대학원	보안법무전공	7
극동대학교	글로벌대학원	인공지능보안학과	6
	일반대학원	인공지능보안학과	13
남서울대학교	특수대학원	빅데이터산업보안학과	4
단국대학교	행정법무대학원	융합보안학과	29
대전대학교	일반대학원	정보보안학과	4
동국대학교	국제정보보호대학원	사이버포렌식학과	63
		정보보호학과	88
동서대학교 일반대학원		디지털포렌식학과	3
동의대학교 국가안전정책대학원		보안학과	4
명지대학교	대학원	보안경영공학학과간협동과정	41
	산업대학원	융합보안안보학과	18

대학원명		학과명	재적학생 수
목포대학교	대학원	정보보호기술학협동과정	2
	산업기술대학원	정보보호전공	2
배재대학교 대학원		사이버보안학과	35
부경대학교 대학원		정보보호학과	6
부산가톨릭대학교 대학원		에너지융합보안학과	5
부산외국어대학교 대학원		스마트융합보안학과	12
서강대학교 정보통신대학원		정보보호전공	28
성균관대학교 정보통신대학원		정보보호학과	54
세종대학교 일반대학원		정보보호학과	28
세종사이버대학교 정보보호대학원		정보보호학과	143
순천향대학교 대학원		모빌리티융합보안학과	14
		정보보호학과	6
숭실대학교 정보과학대학원		정보보안학과	46
아주대학교 대학원		사이버보안학과	10
용인대학교 일반대학원		경찰보안정보학과	14
위덕대학교 대학원		경찰보안학과	3
인제대학교 일반대학원		산업융합보안학	23
인하대학교 대학원		산업보안거버넌스전공	19
전남대학교 대학원		정보보안협동과정	59
제주대학교 대학원		융합정보보안학협동과정	5
중부대학교 휴먼텍대학원		정보보안학과	3
중앙대학교	대학원	융합보안학과	41
	보안대학원	산업융합보안학과	60
충북대학교 대학원		융합보안학과간협동과정	7
한국과학기술원 일반대학원		정보보호대학원	74
한세대학교 공학대학원		산업보안안전학과	1
한양대학교 대학원		정보보안학과	5
호서대학교 대학원		정보보호학과	10
계		58개	1,544

[출처: 대학알리미, www.academyinfo.go.kr]

제3절 전문기관 교육 과정

정보보호인력 양성 사업은 교육 대상과 목적에 따라 공공·민간 부문 및 정부지원 사업 등으로 구분된다. 공공 부문은 행정기관과 그 소속·산하기관의 정보보호 담당자 등을 대상으로 사이버안보 교육을 제공 중이다. 민간 부문은 일반인을 대상으로 자격증 취득 과정 및 기업 수요 반영 단기교육 등 산업 맞춤형 장·단기 과정 등이 운영되고 있다. 정부도 한국인터넷진흥원 등 전문기관과 연계하여 정보보호 인력 양성 사업을 추진하고 있다.

1. 공공 부문

국가보안기술연구소 사이버안전훈련센터는 공공기관 및 기반시설 전산·보안 담당자 등을 대상으로 정보보안 맞춤형 실무·현장 교육 및 실전 사이버위기 대응 훈련을 제공한다. 국가·공공 부문 사이버보안을 강화하기 위하여 2014년 10월 개소하였다. 교육 과정은 '정책'·'도입'·'예방'·'탐지'·'조사'로 구분된다.

표 4-3-3-1 2022년 사이버안전훈련센터 연간 교육 과정

분야	교육 과정명	교육 대상자
정책(3)	정보보안 업무 이해	국가·공공기관 정보보안 관련 업무 종사자
	사이버안보 정책	중앙행정기관 과장급 및 산하기관 (본)부장급
	기반시설 보안 정책	중앙행정기관 과장급 및 주요정보통신기반시설 유관기관 (본)부장급
도입(5)	정보시스템 구축·운영 실무	국가·공공기관 정보보안 관련 업무 종사자
	정보화사업 보안성 검토	국가·공공기관 정보보안 관련 업무 종사자
	보안적합성 검증	정보보호제품 및 네트워크 장비 보안적합성 도입·검증·운용 실무 담당자
	상용 암호모듈 활용	국가·공공기관 정보보안 관련 업무 종사자
	안전한 소프트웨어 개발	국가·공공기관 정보보안 관련 업무 종사자
예방(5)	국가·공공기관 보안 위협 사례	국가·공공기관 정보보안 관련 업무 종사자
	업무 PC 보안 강화	국가·공공기관 정보보안 관련 업무 종사자
	기반시설 제어시스템 보안	국가·공공기관 기반시설 제어시스템 운영 담당자
	전자파 보안	주요정보통신기반시설 및 국가·공공기관 정보보안 관련 업무 종사자
	정보보안 관리 실태평가	국가·공공기관 정보보안 관리실태 평가 담당자

분야	교육 과정명	교육 대상자
탐지(5)	사이버위기 대응 도상훈련	국가·공공기관 정보보안 관련 업무 종사자
	악성코드 분석	국가·공공기관 정보보안 관련 업무 종사자
	악성코드 행위 분석	국가·공공기관 정보보안 관련 업무 종사자
	보안관제 및 사고 대응	국가 부문 보안관제센터 운영 및 관련 종사자
	기반시설 사이버공격 대응	주요정보통신기반시설 및 국가·공공기관 정보보안 관련 업무 종사자
조사(4)	업무 PC 침해사고 분석 과정	국가·공공기관 정보보안 관련 업무 종사자
	웹서버 침해사고 분석 과정	국가·공공기관 정보보안 관련 업무 종사자
	디지털포렌식 과정	국가·공공기관 정보보안 관련 업무 종사자
	윈도우포렌식 과정	국가·공공기관 정보보안 관련 업무 종사자

[출처: 사이버안전훈련센터, portal.cstec.kr]

국가공무원 인재개발원은 교육·훈련, 연구·개발 및 평가, 교류·협력 등에 관한 사무를 관장하는 인사혁신처 소속기관으로, 2016년 1월 1일 개원(충청북도 진천군 소재)하였다. 공무원의 직무역량 강화를 위한 다양한 교육 과정(기본교육, 국정철학, 공직자세, 공직리더십 교육, 글로벌 교육, 직무교육, 이러닝 등)을 운영하고 있으며, 정보보호 관련 교육은 직무교육인 정보화 교육 안에서 시행하고 있다.

표 4-3-3-2 2022년 국가공무원 인재개발원 정보보안 교육 과정

분야		교육 과정명	교육 대상자
정보보안	입문	정보보호와 친해지기	국가·지방 공무원
	일반	생활 속의 IoT 보안	
		PC와 스마트폰 정보 지키기	
		개인정보보호 실무	
		정보보안 정책 실무	
		TCP/IP 네트워크 이해	
	전문	네트워크 해킹 및 보안	
		시스템 해킹 및 보안	
		정보보호시스템 운영 및 보안	

[출처: 국가공무원인재개발원, www.nhi.go.kr]

2. 민간 부문

민간 부문의 정보보호 관련 교육은 ICT 융합 등 환경 변화에 따라 보안 이슈가 전 산업으로 확산되면서 기존 자격증 취득 중심의 교육에서 산업 맞춤형 교육까지 다양한 형태의 장·단기 교육 과정이 개설되어 있다.

자격증 취득 관련 교육은 공인정보시스템감사자(CISA, Certified Information Systems Auditor)·공인정보시스템보안전문가(CISSP, Certified Information System Security Professional)·정보보안관리자(CISM, Certified Information Security Manager) 등이 있으며, 「개인정보보호법」 시행 이후 개인정보관리사(CPPG, Certified Privacy Protection General) 자격증에 대한 관심이 높아지면서 관련 자격 취득 과정 또한 다수 교육기관에서 개설되어 운영 중이다.

산업맞춤형 교육 과정으로는 정보보호 컨설턴트, 보안관제, 모의해킹 등 직무 맞춤형 교육이 운영되고 있다.

표 4-3-3-3 2022년 민간 교육센터 교육 현황

기관명	교육 과정	홈페이지
한국정보 기술연구원	침해 대응, 모의해킹, 보안개발자 과정 등 재직자 및 구직자를 위한 양성 과정 등	www.kitri.re.kr
와이즈로드	CISSP, CISM, CPPG, 정보보안(산업)기사 자격증 과정 등	wiseroad.co.kr
라이지움	CISSP, CISA, CISM, CPPG, 정보보안(산업)기사 자격증 과정 등	www.lyzeum.com
멀티캠퍼스	정보보호일반, CISSP, CISA, 정보보안(산업)기사 자격증 과정 등	www.multicampus.com
솔테스크	기업보안전문가 과정, 모의해킹 과정 등	soldesk.com
KG 아이티뱅크	네트워크/시스템 해킹, 포렌식(침해 대응), 악성코드 분석 과정 등	kgitbank.co.kr
인섹시큐리티	디지털 & 모바일포렌식, 침해사고 분석, 취약점 진단, APT 공격 차단 네트워크 보안 등	www.insec.co.kr
패스트레인	네트워크/모바일/시스템 보안 과정, CISSP, CISA 자격증 과정 등	www.flane.co.kr
한국정보보호 교육센터(KISEC)	모의해킹, 진단, 포렌식(침해사고), 보안 일반 과정 등	www.kisec.com

[출처: 기관별 홈페이지]

3. 정부지원 정보보호 인력 양성

정부가 지원하는 대표적인 정보보호 전문인력 양성 사업으로는 과학기술정보통신부의 정보보호 특성화대학, 융합보안 핵심인재 양성 사업(융합보안 대학원), 대학 정보보호 동아리 연합회(KUCIS, Korea University Clubs Information Security), 차세대 보안리더(BoB, Best of the Best) 양성 프로그램 및 사이버보안 실무인재 양성(K-Shield 주니어) 사업 등이 있다. 이 밖에도 고용노동부가 지원하는 최정예 정보보호 전문인력(K-Shield) 및 산업보안 전문인력 양성 사업 등이 있다.

가. 한국인터넷진흥원 추진 사업

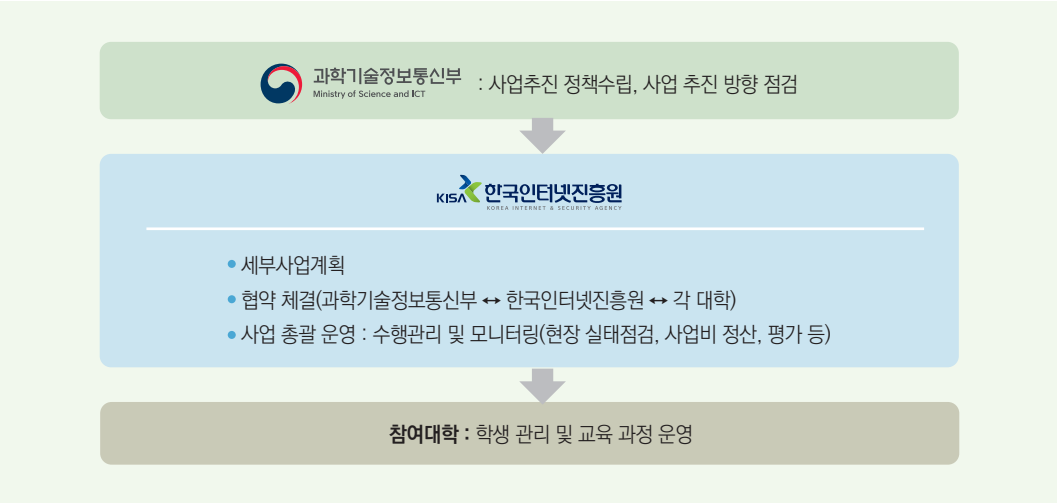
한국인터넷진흥원(사이버보안인재센터)은 글로벌 경쟁력을 선도하는 정보보호 인력 양성 및 교육 생태계 조성을 위하여 정보보호 인력 양성 사업을 운영하고 있다. 우선 최정예 정보보호 전문인력(K-Shield) 및 산업보안 전문인력 양성 사업 등을 통하여 정보보호 담당자의 역량을 강화 중이다. 또한 정보보호 특성화대학, 융합보안 핵심인재 양성 사업 및 대학 정보보호 동아리 연합회 등을 통하여 예비인력을 육성하는 등 생애주기별 맞춤형 교육으로 2022년에는 약 8,000여 명의 우수인력을 양성하였다.

1) 정보보호 특성화대학

과학기술정보통신부는 한국인터넷진흥원과 함께 정보보호 관련 특성화 교육 체계를 갖춘 학과(또는 전공)를 대상으로 2015년부터 정보보호 특성화대학 지원 사업을 추진하였다. 이 사업을 통하여 대학은 정보보호학과 또는 전공 단위로 산업계 수요를 반영한 정보보호 교육과정을 개설하고 정보보호 직무에 특화된 집중 교육을 실시하고 있다.

2015년 고려대학교·아주대학교·서울여자대학교가 최초로 선정된 이후 현재 3개[고려대학교(세종)·성신여자대학교·세종대학교]의 정보보호 특성화대학을 운영하고 있다.

그림 4-3-3-1 정보보호 특성화대학 지원사업 체계도



이 사업은 참여기관(대학)과 국내외 정보보호 관련기업 및 국외대학 등으로 구성된 컨소시엄을 중심으로 운영되며, 컨소시엄 참여기업과의 산학협력 프로젝트 수행, 산학협력 중점교수 활용 등이 필수로 포함되어 있어 산업 현장의 실무형 우수인재 발굴·육성 사업으로 평가되고 있다.

2) 융합보안 핵심인재 양성(융합보안 대학원)

과학기술정보통신부는 융합보안 핵심인재 양성 사업을 통하여 융합보안 대학원을 선정, 운영하고 있다.

이 사업을 통하여 대학은 지역 전략산업 관련 기업·기관과 컨소시엄을 구성, 융합보안 대학원을 개설하는 한편, 지역 전략산업 분야 ICT 융합 제품·서비스의 보안성 제고를 위한 문제해결형 프로젝트를 교육 과정에 반영하는 등 현장과 연계한 교육으로 융합보안 컨설턴트 및 개발자를 양성하고, 지역 전략산업의 융·복합화를 지원할 것으로 기대된다.

2019년 스마트공장 분야 고려대학교, 에너지 신산업 분야 전남대학교, 스마트시티 분야 한국과학기술원을 선정하였으며, 2020년 5G+ 핵심서비스 분야를 중심으로 성균관대학교·강원대학교·순천향대학교·부산대학교·충남대학교 등 5개 대학교를 추가로 선정하여 현재 전국적으로 8개의 융합보안 대학원이 운영 중이다.

표 4-3-3-4 2022년 융합보안 대학원 현황

대학교명	특화 분야	선정연도	대학교명	특화 분야	선정연도
고려대학교	스마트공장	2019	순천향대학교	자율주행차	2020
한국과학기술원	스마트시티		부산대학교	핀테크	
전남대학교	에너지 신산업		강원대학교	디지털 헬스케어	
성균관대학교	디지털 헬스케어	2020	충남대학교	스마트시티	

3) 실전형 사이버훈련

경기도 판교 정보보호 클러스터에 구축된 실전형 사이버훈련장(Security-Gym)은 침해사고 사례를 가상 환경으로 재현한 팀 단위 일방향 침해사고 대응, 사이버공격 및 방어를 진행하는 양방향 실전 공방, 상용 정보보호제품군 보안기능 및 우회공격에 대한 대처방안을 실습하는 정보보호제품군 실습 훈련 등 총 3가지 훈련 과정을 운영 중이다.

2017년에는 군·경찰 등 공공 부문 보안담당자 대상 시범훈련을 통하여 수료생 250명을 배출하였다. 2018년부터 통신사·금융권 등 민간 부문으로 훈련 대상을 확대하여 357명의 수료생을 배출하였고, 수준별 훈련을 위하여 강의식 일방향 침해사고 대응 과정 및 정보보호제품군 실습 과정을 추가 개설하여 2019년 382명의 수료생을 배출하였다.

2022년에는 온라인 실전형 사이버훈련장의 훈련 과정(스피어피싱 대응 심화 과정, 정보보호제품군 실습훈련)을 확대·운영하여 1,087명의 수료생을 배출하였다.

4) 사이버보안 실무인력 양성

과학기술정보통신부는 2018년 청년 일자리 대책의 일환으로 산업계 반응이 좋은 재직자 교육 과정 'K-Shield'를 벤치마킹하여 정보보호 분야 구직자를 실무인력으로 양성하는 'K-Shield 주니어' 교육 과정을 신설하고, 2018년 제1기 204명을 시작으로 2022년까지 총 1,721명의 실무인력을 배출하였다.

이 과정은 정보보호산업 현장에 즉시 투입될 수 있는 실무형 우수인재를 양성하기 위하여 국가직무능력표준(NCS, National Competency Standards)에 정의된 정보보호 분야 33개 능력단위 및 학습모듈을 바탕으로 200시간 이상의 직무별 커리큘럼을 개발하고 전용 실습장을 구축하였다. 교육 종료 후 수료생을 대상으로 한국인터넷진흥원이 실시하는 최종평가를

통하여 최우수 인재에게 과학기술정보통신부장관 명의의 K-Shield 주니어 인증서를 발급한다.

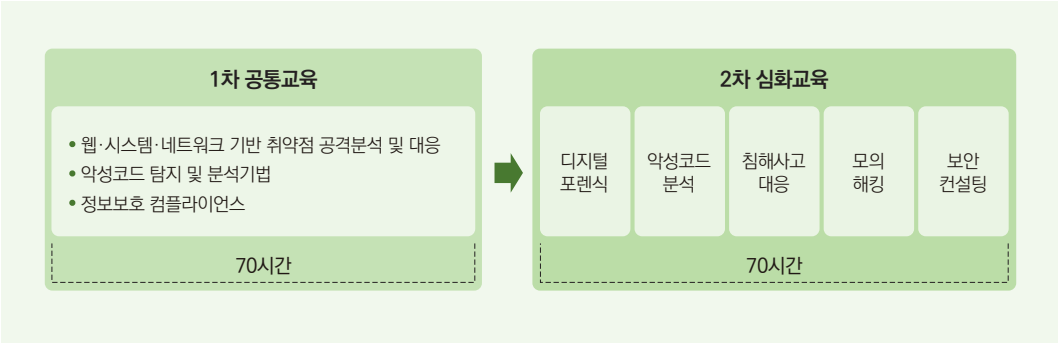
또한 한국인터넷진흥원은 우수 인력 양성 및 수료생에 대한 취업지원을 위하여 2019년부터 정보보호 관련 기업-교육생 간 채용정보 교류의 장인 Meet-up day를 개최하고 있다. 2020년부터 정보보호인력 수요기업과 업무협약을 체결하여 2022년 말 기준 총 82개 기업과 협약하였으며, 협약기업은 교육 과정에 개발·운영에 참여하고 수료생에 대한 특별채용, 채용우대 등의 혜택을 제공한다. 또한 2022년부터 교육생의 실무 프로세스 경험, 보안 직무 이해 등을 위한 정보보호 기업 탐방 프로그램을 기획·운영하며, 교육생과 수료생을 위한 사후지원을 강화하였다.

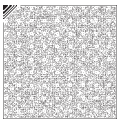
5) 최정예 정보보호 전문인력 양성

한국인터넷진흥원은 2013년부터 3.20 사이버테러와 같은 국가 사이버위기 상황에 신속하게 대응할 최정예 정보보호 전문인력(K-Shield) 양성 사업을 운영 중이다. 이 사업은 취약점 및 악성코드 분석, 모의침투 등 침해사고 대응 기술력 강화를 위한 실무중심의 교육을 실시하였으며, 2018년부터 교육 분야를 정보보호 전반으로 확대하여 다각적인 사이버공격에 대응할 수 있는 최정예 정보보호 전문인력을 양성하고 있다.

교육생은 민간기업 및 공공기관 보안담당자를 대상으로 사전평가를 통하여 선발하고, 선발된 인력은 공통 커리큘럼으로 실시되는 1차 공통교육을 이수한 후 침해사고 대응, 악성코드 분석 등 5개 과정 중 1개 과정을 선택하여 2차 심화교육을 수강하였다.

그림 4-3-3-2 2022년 최정예 정보보호 전문인력 양성 정규 과정 운영 현황





2022년에는 정규 과정 외에 8개 단기 과정을 운영하여 수료생 386명을 배출하였고, 정규 과정을 모두 수료한 82명 중 단계별 이수 결과에 따라 55명에게 K-Shield 양성 과정 인증서를 수여하였다.

6) 산업보안 전문인력 양성

한국인터넷진흥원은 현장 중심의 실무인재 양성 및 산업계 인력의 질적 수급차 문제를 개선하기 위하여 산업체 직무별 요구역량 등을 반영하고 실습이 강화된 디지털포렌식, 지식정보보안 컨설턴트, RFID·USN 보안, 바이오인식 등 4개 교육 과정을 개설하여 2009년 수료생 260명을 배출하였다.

2011년 산업계 수요에 따라 보안관제, 지식정보보안 스킬업 과정 등을 추가 개설하였고, 2012년 부처별 인력 양성 사업 통합 과정에서 고용노동부의 국가인적자원개발 컨소시엄 사업으로 통합되었다.

2022년에는 산·학 전문가와 실무자의 의견을 수렴하여 교육 계획을 수립, '침해사고 분석 대응 전문가'와 '해킹방어를 위한 시큐어코딩' 등 총 10종의 교육 과정을 운영하여 수료생 505명을 배출하였다.

표 4-3-3-5 2022년 산업보안 전문인력 양성 과정 운영 현황

(단위: 회, 시간)

과 정 명	개설횟수	교육시간
침해사고 분석 대응 전문가	3	28
해킹방어를 위한 시큐어코딩	3	21
네트워크 보안 이론과 실무	3	28
포렌식을 활용한 기업 보안사고 대응	2	21
웹 공격 및 대응 기법	3	21
보안컨설팅 이론과 실무	3	21
제어시스템 보안	2	21
데브옵스 환경의 컨테이너 보안	3	21
클라우드 보안구축 실습	4	21
IT/OT 프로토콜 취약점 분석 및 증거수집 기법	2	28

7) 대학 정보보호 동아리 연합회

정보보호 및 유관 전공자가 윤리의식과 보안 역량을 갖추고 사회에 진출할 수 있도록 2006년부터 대학 정보보호 동아리 연합회(KUCIS)를 구성하고, 정보보호 교육, 세미나 및 연구 활동 등을 지원하고 있다.

2022년 국내 전문대학·대학교·대학원 등에 소속된 20개 동아리를 지원하였으며, 서울·경기·강원, 영남, 충청, 호남 등 4개 권역별 운영진을 중심으로 회원 간 정보교류 및 네트워킹을 위한 정보보호 세미나 개최, 취업·창업 캠프 개최 및 연구활동 등을 지원하였다.

표 4-3-3-6 2022년 대학 정보보호 동아리 현황

대학교명	동아리명	권역
가천대학교	Pay1oad	서울 경기 강원
경기대학교	C-Lab	서울 경기 강원
국민대학교	FaS	서울 경기 강원
국민대학교	PEPSI	서울 경기 강원
단국대학교	Aegis	서울 경기 강원
서울여자대학교	SWING	서울 경기 강원
서울여자대학교	SWLUG	서울 경기 강원
세종대학교	Security Factorial	서울 경기 강원
아주대학교	Whois	서울 경기 강원
경일대학교	K-Hackers	영남
영남대학교	@Xpert	영남
극동대학교	POS	충청
대전대학교	HACTOR	충청
백석대학교	HUB	충청
충남대학교	ARGOS	충청
호서대학교	HAIS	충청
목포대학교	SecuMaster	호남
우석대학교	APS	호남
전남대학교	정보보호119	호남
호원대학교	SEED	호남

8) 차세대 보안리더 양성 프로그램

한국정보기술연구원(KITRI, Korea Information Technology Research Institute)이 운영하는 차세대 보안리더(BoB, Best of the Best) 양성 프로그램은 창의적 문제해결 능력을 보유한 차세대 보안리더를 양성하기 위하여 정보보안에 재능 있는 고등학생·대학(원)생 등 청년층 인재를 발굴·육성하는 대표적인 정보보안 인재 육성 프로그램이다.

2019년 제8기를 맞이하여 모집 정원을 200명으로 확대한 BoB는 국내외 최고의 보안 전문가에 의한 단계별 멘토링, 실무연계형 프로젝트, 우수 인재에 대한 평가·인증 및 수료생의 사회진출 지원 등으로 명성을 떨치고 있다. 제1기 60명으로 시작한 BoB는 제11기(2022년)

까지 총 1,690명을 선발하여 교육하였고, 기수별 3단계 교육 과정을 거쳐 선발된 최우수 10명에게는 과학기술정보통신부장관 명의의 BEST 10 인증서 등을 수여한다.

9) 융합보안 인력 양성

ICT 환경 변화 및 융합에 따라 다양한 분야로 확산되는 보안위협에 대응하기 위하여 2016년부터 ICT 융합 제품·서비스 관련 개발자를 대상으로 융합보안 교육 과정을 운영 중이다.

2016년 IoT 보안 코디네이터 과정, 2017년 IoT 디바이스 보안 과정을 운영하였으며, 2018년부터 스마트 에너지, 스마트 의료, 스마트 홈·가전 등 ICT 융합 산업 분야별 교육 과정으로 개편되었다. 2019년 스마트 자동차, 2020년 스마트 제조 분야 과정을 추가하였고, 2022년에는 스마트 자동차, 제조, 홈·가전, 의료, 블록체인, 메타버스 등 총 6개 교육 과정을 운영하였다.

표 4-3-3-7 2022년 융합보안 인력 양성 과정 교육 내용

교과 분야	교육 내용
스마트 에너지	발전시설 해킹 사고 분석과 가상의 발전설비 환경을 활용한 취약점 분석 및 대응 방안(Openplc, ScadaBR 활용)
스마트 제조	스마트공장 해킹 사고 분석과 가상의 생산시설 환경을 활용한 취약점 분석 및 대응 방안(Openplc, ScadaBR 활용)
스마트 의료	종합병원 해킹 사고 분석과 의료기기 중심의 취약점 분석 및 대응 방안(아두이노 및 무선랜 활용)
스마트 홈·가전	홈·가전 기기(AI 스피커)를 활용한 서비스 측면의 취약점 분석 및 대응 방안(AI Makers Kit 활용)
스마트 자동차	스마트카 해킹 사고 분석과 가상의 스마트카 환경을 활용한 취약점 분석 및 대응 방안(아두이노, 차량 데이터셋 활용)

10) 인공지능 보안기술 개발 인력 양성

과학기술정보통신부와 한국인터넷진흥원은 정보보호 자동화·지능화 기술혁신을 지원하기 위하여 2020년부터 인공지능 기술을 활용한 지능형 보안기술 개발 역량을 갖춘 전문인력을 양성 과정을 운영하고 있다. 2020년 제1회 인공지능 보안기술 개발 교육에서는 수료생 50명을 배출하였고, 우수 교육생 5명을 선발하여 한국인터넷진흥원 원장 명의의 인증서를 수여하였다.

또한 미취업 교육생을 대상으로 직무상담, 취업컨설팅, 채용정보 제공 등 취업지원을 추진하여 교육생에게는 채용의 기회를 제공하고, 산업계에는 전문인력 수요를 충족할 수 있도록 지원한다.

인공지능 보안기술 개발 교육은 이론중심의 선수과목으로 구성된 공통교육을 이수한 후 각 산업분야에 인공지능 기술을 적용하는 실습중심의 전문 교육을 이수하도록 구성되어 있다. 2021년에는 인공지능을 활용한 공격과 방어 및 사용자인증, 보안로그 분석 및 이상징후 탐지·분석, 데이터 분석을 통한 침입탐지의 3개 부문으로 구성하여 전문(실습)교육을 진행하였다. 전문교육 수강 후에는 인공지능 보안 신기술을 개발하는 멘토링 중심의 프로젝트를 진행하여 교육성과를 확인하고 공유하는 시간을 가졌다.

나. 대학 ICT연구센터(정보보호 분야)

과학기술정보통신부와 정보통신기획평가원이 2000년부터 첨단 연구역량을 갖춘 석·박사급 전문 연구 인력 양성을 목적으로 지원하고 있는 대학 ICT연구센터(ITRC, Information Technology Research Center)는 2000년부터 2020년까지 인재 양성 15,841명, 특허등록 5,359건, 기술이전 수입 약 481억 원 및 SCI급 논문 12,602건 등 성과를 도출하며 신성장 동력 및 신산업 창출에 이바지하였다.

2020년에는 총 51개의 연구센터가 지원을 받았으며, 그 중 정보보호 분야 ITRC는 숭실대학교 AI보안연구센터가 운영 중이다.

다. 국가기간·전략산업 직종훈련(정보보호 전문가 양성)

과학기술정보통신부와 고용노동부가 주관하고 한국정보기술연구원에서 운영하는 '중앙부처 국가기간·전략산업 직종훈련 사업'은 정보보안 산업계로 진출을 희망하는 미취업자 대상 장기(5개월 이상) 전문기술교육을 통하여 정보보안 산업계의 신입인력 배출을 목표로 운영되고 있다.

이 프로그램은 고용노동부에서 운영하는 직업능력개발 계좌 신청·발급을 통하여 참여할 수 있으며, 참여자는 교육비 전액 지원과 식대·교통비 등을 추가로 지원받을 수 있다.

표 4-3-3-8 2021년 중앙부처 국가기간·전략산업 직종훈련 과정

대상	과정명	정원(명)
구직자	침해 대응 전문가 양성 과정	270
	모의해킹 전문가 양성 과정	
	기업채용 연계 과정	
	보안개발자 양성 과정	
재직자	정보보호 최고책임자 양성 과정	-

라. 금융보안원 추진 교육 과정

1) 사이버교육

금융보안원은 금융보안교육센터(edu.fsec.or.kr)를 통하여 금융회사 임직원의 디지털 금융IT·보안 역량 강화와 보안 인식제고 함양을 위하여 자신의 직무 및 수준을 고려하여 자기주도 학습을 할 수 있도록 계층별 맞춤형 사이버교육을 제공하고 있다. 2022년에는 디지털 전환과 데이터 혁신에 부합하는 인공지능·클라우드·마이데이터 등 최신 이슈와 기술 트렌드를 반영한 교육 과정을 신설하여 제공하였다.

표 4-3-3-9 2022년 사이버교육 과정

구 분	과 정 명
기본소양 (16개)	일상에서 지켜야 할 스마트폰 보안수칙
	정보보호 인식제고(한글/영문)
	금융IT 내부감사활동의 이해
	금융보안 거버넌스의 이해
	신입직원을 위한 금융보안 개론
	비대면 업무 환경에서 이것만은 지키자
	금융권 마이데이터의 이해
	데이터 3법 개정과 금융권 적용 시 유의 사항
	디지털 금융보안 이슈(한글/영문)
	금융보안 법·제도의 이해
	4차 산업혁명의 영향과 보안위협 및 대응
	금융 환경 변화에 따른 전자금융서비스 분석
	금융권 보안 위협 전망
	최근 금융분야 사이버공격 유형 및 대응 방안
	IT아웃소싱 업체 보안 A부터 Z까지
	금융권 클라우드 시스템 도입 시 고려사항

구 분	과 정 명
직무기본 (12개)	웹 애플리케이션 보안
	금융보안 데이터 크롤링을 위한 파이썬 기본 문법
	금융권 APT 공격과 대응 방안
	네트워크의 이해
	블록체인 속의 금융 환경 및 이슈
	안전한 금융보안을 위한 암호기술
	전자금융 보안인증기술의 이해
	정보보안 컴플라이언스 및 시스템관리 기초
	상담원을 위한 금융보안
	IT아웃소싱과 금융보안
	금융회사 임직원이 준수해야 하는 금융IT 내부통제(국/영문)
	내부정보 유출방지를 위한 자가수준진단 및 준수사항
직무강화 (12개)	가명·익명 처리 취급자를 위한 정보보호
	개인신용 정보보호 실무
	금융권 IT 보안 위반 사례
	다크웹과 OSINT(Open Source Intelligence)
	AI를 이용한 금융 데이터 분석 실습
	금융권 클라우드 도입과 보안
	정보보호 관리 체계 구축 및 활용(한글/영문)
	안전한 소프트웨어를 위한 시큐어코딩의 이해
	윈도우 시스템 보안의 이해
	개인정보 책임자를 위한 금융권 개인정보보호
	개인정보 수탁자를 위한 금융권 개인정보보호
	개인정보 취급자를 위한 금융권 개인정보보호

2) 집합교육

전문역량을 함양할 수 있는 교육을 제공하기 위하여 금융회사 임직원 대상으로 계층별·수준별 맞춤형 특화 교육 과정을 운영하고 있다. 비대면 교육 채널을 활용하여 디지털 금융 법·제도, 디지털 금융IT·보안 등 최신 보안 동향과 신기술 등의 주제를 적시에 제공하였으며, 집합교육의 효과를 증대하기 위하여 플립러닝 과정(2021년 2개 → 2022년 3개 과정)을 확대 운영하였다.

* 플립러닝(Flipped Learning) : 사전에 온라인으로 개인학습을 진행한 후 오프라인에서 실습·토론을 진행하는 혼합형 학습

표 4-3-3-10 2022년 주요 집합교육

과 정 명	운영형태	교육 대상
금융 정보보호 및 개인정보보호 관리 체계	이론	관리자·실무자
금융권 IT 컴플라이언스		
정보보호 전략 수립		
금융 IT 감사 실무		
금융 정보보호 법·제도의 이해		
금융보안 거버넌스 구축과 내부통제 강화 방안	이론 (비대면)	
제로 트러스트 개념 및 금융권 도입 전략		
금융권 개인정보보호 실무	이론	실무자
금융분야 개인정보보호 위수탁 업무 기본		
금융권 개인신용정보 보호		
전자금융 보안의 이해		
금융IT 인프라 보안의 이해		
ISMS-P 인증심사 실무		
금융분야 클라우드 컴퓨팅 서비스 제공자 안정성 평가 및 평가 방법		
신용카드 정보를 노리는 사이버공격 위협 분석	이론 (비대면)	
보이스피싱 악성 앱 유포조직 프로파일링		
금융권 수탁업무 관련 개인(신용)정보보호 실무		
'23년도 전자금융기반시설 보안 취약점 평가기준 및 디지털포렌식 주요 아티팩트 수집·분석		
금융권 오픈소스 도입에 따른 보안 리스크 관리		
금융 IT 클라우드 운영 실무	실습	
클라우드 보안 서비스 운영실습		
금융권 데이터 분석 활용		
금융데이터 가명, 익명 처리 및 활용		
금융권 취약점 점검 방법론의 이해		
금융 앱 보안 실무		
금융 APT 공격과 대응		
정보보호시스템 운영관리 실무		
윈도우 시스템 악성코드 분석 및 대응		
금융 IT 보안 입문		
AI를 이용한 금융보안 데이터 분석(기본, 심화)		
디지털포렌식 기본		
이더리움을 이용한 블록체인 플랫폼 구축 실습		

과 정 명	운영형태	교육 대상
OSINT를 활용한 딥웹, 다크웹상의 사이버 위협 분석	실습	실무자
윈도우 시스템 해킹으로 배우는 소프트웨어 취약점 공격 기법		
CTF 문제풀이로 정보보호전문가 따라하기		
클라우드 도입, 설계, 구축 및 보안 관리		
금융권 실시간 침해사고 대응 훈련	실습 (플립러닝)	
금융·보안 정보 수집을 위한 파이썬 웹 크롤링		
'엘라스틱 스택을 이용한 대용량 데이터 분석 및 시각화 실습		
제6기 금융보안 최고위 과정		CISO 등
금융IT CISO 보안리더 교육		CISO

3) 금융보안 자격제도

금융보안원은 금융권에 필요한 검증된 보안 전문인력을 양성하기 위하여 2018년부터 금융정보보호 관련 법·제도, 관리 체계, 금융IT 보안 등의 전문교육 과정과 연계한 금융보안관리사 자격제도를 실시하고 있다. 보다 많은 실무형 금융보안 전문가를 양성하기 위하여 2021년부터 전문교육 과정을 온라인 교육으로 제공하고 있으며, 연 2회 자격 검정시험을 운영하여 금융보안 전문가 양성에 힘쓰고 있다.

금융보안관리사 자격제도는 금융위원회 소관 등록 민간자격으로 전문교육 과정과 자격 검정시험으로 구성되는데, 2018년부터 2022년까지 7회 검정시험을 실시하여 총 205명의 금융보안관리사를 배출하였다.

표 4-3-3-11 금융보안관리사 배출 현황

(단위: 명)

구 분	2018	2019	2020	2021	2022
금융보안관리사	29	33	29	59	55

4) 금융보안캠프 운영

금융보안원은 미래 금융보안 인력 양성을 지원하기 위하여 금융정보보호협의회 및 금융보안포럼과 공동으로 전국의 대학(원)생이 참여하는 금융보안캠프를 개최하고 있다. 2022년에는 코로나19 상황에 따라 참가자의 안전을 고려하여 온·오프라인 혼합형태로 개최하였으며, 31개 대학교 대학(원)생 85명이 참여하였다.

제4절 각종 대회를 통한 인력 양성

인터넷 이용 환경의 변화로 정보보호 대상이 크게 확대되면서 인터넷 침해사고가 크게 증가하고 있고, 이에 따른 정보보호 필요성이 커지면서 전문인력 양성이 새로운 이슈로 부각되고 있다. 이러한 가운데 정부와 주요 기관은 정보보안 전문인력 발굴·육성과 정보보호 인식제고를 위한 노력의 일환으로 다양한 해킹방어대회를 개최하고 있는데, 2022년 국내에서 개최된 주요 대회는 다음과 같다.

1. NATO 주관 락드실즈 훈련

2012년부터 개최 중인 '락드실즈(Locked Shields, LS)'는 미국·EU 등 NATO 사이버방위센터 회원국 38개 간 사이버방어 협력체제 마련과 종합적인 사이버 위기상황을 해결하기 위하여 매년 4월 실시하는 훈련으로, 공격 및 방어 전문가 2천여 명 이상이 참가한다. 락드실즈는 기술훈련과 전략훈련으로 구성되어 있으며, 기술훈련에서는 각 참가팀(블루팀)이 가상의 전력·항공 등 국가 주요 기간전산망을 관리하면서 NATO 공격팀(레드팀)의 사이버공격을 방어하는 역할을 맡는다. 방어에 실패하여 시스템이 다운되면 포인트를 잃고 방어에 성공하면 포인트를 얻는 방식으로 평가가 이루어진다. 특이점은 적의 공격에 대한 기술적 방어 역량만을 평가하는 다른 사이버공격 방어대회와는 달리 락드실즈의 전략훈련은 사이버방어와 연계된 국가 차원의 상황별 사이버·법률·미디어 전략 등 다양한 정책적 요소에 대한 대응 과정도 종합 평가한다는 점이다.

우리나라는 NATO 사이버방위센터의 사이버공격·방어 기술 및 사이버안보 전략·정책 노하우 등을 공유하기 위하여 국가정보원 주도로 2019년 아시아 최초로 회원국에 가입하여 훈련 참가 자격을 확보하였고, 2021년부터 실시간 훈련에 직접 참여하였다(2020년 훈련은

'코로나19'로 취소). 2021년 한국전력공사·한전KDN·국가보안기술연구소와 함께 30여 명 규모의 팀을 구성하여 라트비아와 연합하여 20여 개 회원국 연합팀과 경합하였으며, 2022년에는 국방부 등 민·관·군 8개 기관과 최초의 국가 단일팀을 구성하여 NATO 사이버방위센터 30여 개 회원국과 경합하였다.

그림 4-3-4-1 우리나라 합동방어팀 훈련 현장(밀리토피아 호텔)

2. 공공분야 사이버공격 대응 훈련

국가·공공기관의 사이버위기 단계별 대응 태세를 점검함으로써 실제 위기상황 발생 시 유기적으로 대응하고 피해가 확산되는 것을 사전에 차단하기 위하여 2006년부터 매년 7~9월 중 국가정보원 주관으로 '사이버공격 대응 훈련(Cyber Guard)'을 실시하고 있다. 훈련 대상은 중앙행정기관·광역자치단체·공공기관 등 190여 개 기관이며, 실제 업무 환경을 모사한 훈련 시스템에 접속하여 실시간 기반의 사이버공격을 대응하는 방식으로 훈련이 진행된다.

2022년에는 위장 해킹메일을 발송하여 해킹메일 열람·신고 여부를 점검하는 등 평시 사이버위협 대비태세와, 위기경보 단계(관심→주의→경계→심각)에 맞춘 다양한 형태의 사건 메시지를 통하여 각급기관의 대응 태세를 점검하였고, 참여기관 모두 전반적으로 양호한 것으로 평가되었다. 2023년에는 을지훈련 기간 중 상황 메시지·해킹메일 대응 훈련(8월)을 실시하고, 실시간 모의 대응 훈련은 9월 중 실시 예정이다.

3. 사이버공격방어대회

국가정보원과 국가보안기술연구소는 국가·공공기관·민간 정보보안 종사자의 사이버안보 대응 역량을 강화하고, 대국민 사이버보안 인식을 제고하는 한편, 국가 사이버안보 인재 양성과 차세대 영재를 발굴하기 위하여 2017년부터 '사이버공격방어대회(CCE, Cyber Conflict Exercise)'를 개최하고 있다. 2022년 제6회 대회는 9~10월간 '디지털 플랫폼 시대의 사이버안보'를 주제로 개최하였는데, 공공팀(국가·공공기관)과 일반팀(대학생·직장인)으로 구분하여 참가 신청을 받던 것을 중·고등학생이 참가하는 학생 부문을 신설함으로써 보다 다양한 인원이 참여할 수 있도록 하였다. 실제 기관의 인터넷·업무망을 모사한 환경을 구성하여 실시간 공격에 대한 방어능력을 종합 평가하는 방식으로 진행되며, 예선과 본선을 통하여 결정되는 종합우승팀에게는 국가정보원장상과 상금 3천만 원, 각 부문 준우승팀 등에게는 국가보안기술연구소장상과 상금이 주어진다. 2022년에는 온·오프라인 콘퍼런스와 정보보호제품 전시회도 병행하여 개최되는 등 국내 최대 규모의 대회로 자리매김하고 있다.

그림 4-3-4-2 2022 사이버공격방어대회 포스터

4. 코드게이트

2008년부터 시작된 코드게이트(CODEGATE)는 국내 최초의 국제 해킹방어대회로, 코드게이트 보안포럼에서 운영하고 있다. IT를 중심으로 한 4차 산업혁명시대의 흐름에 발맞추어 새로운 정보보안 기술을 탐구하고 기술 트렌드에 대한 영감을 공유하는 글로벌 정보보안 행사로서 연 1회 개최하고 있다.

2022년 대회에는 일반부 48개국 2,647개 팀, 대학생부 국내 225개 팀, 주니어부 27개국 196명이 각각 참여하였다. 일반부에서는 우리나라 'The Duck' 팀이 우승을 차지하였고, 러시아 'More Smoked Leet Chicken' 팀이 2위에 올랐다. 대학생부에서는 한국과학기술원(KAIST) 'GoN' 팀, 주니어부(만 19세 이하)에서는 한국디지털미디어고등학교 허승환 군이 우승하였다.

5. 사이버안보(보안) 논문 공모전

사이버안보(보안) 논문 공모전은 국가정보원이 주최하고 한국정보보호학회와 정보세계정치학회가 주관하며, 미래인재 양성을 목적으로 하는 공모전이다.

'2022 사이버안보(보안) 논문 공모전'은 기술 및 정책 전 분야를 대상으로 한 공모전이다. 기술분야(시스템·네트워크 보안, 산업보안 등)와 정책분야(국가전략, 국제분쟁, 국제협력 등)로 대상 분야가 광범위하며, 응모자는 대학(원)생으로 제한된다. 총상금 3,100만 원 규모로, 대상·최우수상 등 총 20편을 시상하며, 우수 논문은 본인이 희망할 경우 한국정보보호학회와 정보세계정치학회 논문지에 추천한다.

6. 국가암호 공모전

국가암호 공모전은 국내 암호기술 발전을 위하여 한국인터넷진흥원과 국가보안기술연구소가 주최하고 한국암호포럼과 한국정보보호학회가 주관하며 국가정보원에서 후원하는 공모전이다. '2022 국가암호 공모전'에는 암호 이론과 암호 응용 분야에서 총 66개 팀이 66편의 논문을 제출하였다. 학계 전문가로 이루어진 심사위원회는 1차 서면심사, 2차 심층 인터뷰를 거쳐 이론 분야 15개 팀, 응용 분야 13개 팀 등 총 28개 팀을 최종 수상팀으로 선정하였다. 대상은 기존

연산방식과 다르게 새로운 증명기법을 제시한 한양대학교 팀, 최우수상은 한국과학기술원, 서울대학교, 서울대학교·크립토랩, 한성대학교, 부산대학교, 고려대학교 팀이 받았다.

7. 사이버안보 아카데미

국가정보원·국가보안기술연구소·국제사이버법연구회가 주최하고 고려대학교 사이버법센터가 주관하는 '2022 대학(원)생을 위한 사이버안보 아카데미'가 8월에 실시되었다. 이 행사는 사이버안보 인식제고 차원의 교육프로그램으로, 2014년 국가보안기술연구소와 고려대학교 법학전문대학원 주최 '대학(원)생을 위한 사이버시큐리티 아카데미'로 시작하였다.

2022년 교육은 국가사이버안보센터의 실무자와 산·학·연 전문가로 구성된 강사진이 우리나라 사이버안보 환경을 비롯하여 사이버공격 유형과 기법, 국내외 사이버안보 법제, 사이버공간의 국제법과 규범, 범죄 및 테러 대응, 국제관계에서의 사이버 문제 등을 강의하였다. 2022년 수강생 150명에게는 주최기관장 공동명의의 수료증이 발급되었다.

8. FIESTA

금융보안원은 금융권에 특화된 사이버침해 위협분석 대응 역량을 강화하기 위하여 2018년부터 FIESTA(사이버침해 위협분석 대회)*를 개최하고 있다.

* FIESTA는 Financial Institutes' Event on Security Threat Analysis의 머리글자로, 에스파냐어로 축제를 뜻하며, 대회를 축제처럼 즐기자는 의미이다.

2022년에는 랜섬웨어, 공급망 공격(Supply Chain Attack), 지능형 지속 공격(APT, Advanced Persistent Threat), 악성 앱 분석 시나리오 문제와 침해 대응 기본 문제로 구성하여 다양한 침해사고 사례를 경험하고 위협분석 역량을 향상할 수 있는 문제가 출제되었다.

총 195개팀[금융회사 46팀, 대학(원) 122팀, 내부직원 27팀] 372명이 참여하였으며, 대회 결과 금융회사 부문 5팀, 대학(원) 부문 4팀, 총 9팀을 시상하였다.

9. FSI Data Challenge 2022

금융보안원은 금융권 내 데이터 활용 활성화 및 데이터 전문인력을 양성하기 위하여 대학(원)생 등을 대상으로 2021년부터 데이터 경진대회를 개최하고 있다. 2022년 제2회 대회에는 총 138개 팀이 참여하였고, 7개 팀을 금융위원장상, 금융보안원장상, 금융회사 기관장상 등의 수상자로 선정하였다.

표 4-3-4-1 2022년 수상작 관련 내용

구분	수상	주제
1위	금융위원장상	1인 가구를 위한 소비성향 기반 친구 추천 서비스
2위	금융보안원장상	나의 투자 길잡이, 월렛 버핏
은행	신한은행장상	씬파일러 고객 집단 분류 및 특성 분석을 통한 서비스 및 정책 제언
금융 투자	한국투자증권 대표이사상	클러스터링을 이용한 개인 맞춤형 투자상품 제안
카드	GranData 신한카드 대표이사상	자동차 산업에서의 잠재고객 세그먼트 및 비즈니스 인사이트 도출
	KB국민카드 대표이사상	네이버 검색어 트렌드와 가맹점 매출 데이터를 이용한 고객 연령별 소비 패턴 분석 및 예측
	비씨카드 대표이사상	머신러닝을 활용한 편의점 판매량 예측 모델 및 모델을 활용한 서비스 기획

10. 금융보안원 논문 공모전

금융보안원은 디지털 금융혁신과 금융보안 분야의 우수한 논문을 발굴하기 위하여 금융분야 종사자, 대학(원)생 및 일반인 등을 대상으로 2017년부터 해마다 논문 공모전을 개최하고 있다.

2022년 제6회 논문 공모전에서 대상(금융위원장상)과 최우수상(금융감독원장상) 등 총 8편을 시상하였다.

제5절 정보보호 자격증 제도

정보보호의 중요성이 부각되고 전문인력의 수요가 증가하면서 정보보호 이론과 실무능력을 평가하는 정보보호 자격증에 대한 관심이 커지고 있다.

표 4-3-5-1 정보보호 전문 자격증 현황

구분	명칭	분류	주관기관
국내	정보보안기사, 산업기사	기사·산업기사	과학기술정보통신부, 한국방송통신전파진흥원
	정보보호전문가(SIS)	1급, 2급 ※자격유지	한국인터넷진흥원
	개인정보관리사(CPPG)	-	한국CPO포럼
	개인정보취급사(CPPF)	-	한국CPO포럼
	디지털포렌식전문가	1급, 2급	한국포렌식학회, 한국인터넷진흥원
	산업보안관리사	-	산업통상자원부, 한국산업기술보호협회
	사이버포렌식전문가(CCFP)	-	사이버포렌식전문가협회
국외	정보시스템보안전문가(CISSP)	-	ISC2
	정보보호관리자(CISM)	-	국제정보시스템감사통제협회(ISACA)

1. 국내 정보보호 전문 자격증

가. 정보보안기사·산업기사

국내 정보보호 분야 국가기술자격으로 2012년 정보보안기사·산업기사 2종목이 신설되어, 2013년부터 한국인터넷진흥원이 위탁받아 시행하고 있다.

과거 국가공인 민간자격이었던 정보보호전문가(SIS, Specialist for Information Security) 자격을 벤치마킹하여 국가기술자격으로 정보보안기사·산업기사 제도를 시작하였다.

※ 정보보호전문가의 경우 신규 자격시험은 폐지되었으나, 기존 정보보호전문가 합격자의 자격은 계속 유효하다.

이 자격은 필기시험과 실기시험으로 구성되어 있다. 필기시험은 객관식으로, 산업기사는 시스템 보안, 네트워크 보안, 애플리케이션 보안, 정보보안 일반 등 4개 과목을, 기사는 정보보안 관리 및 법규 과목을 추가한 5개 과목을 치른다. 실기시험은 단답형·서술형·실무형

등 3가지 유형의 필답형 시험으로, 실무에 적합한 지식과 기술력을 검증하는 정보보안 실무 단일과목으로 구성되어 있다.

2022년 정보보안기사·산업기사 시험은 필기·실기 각 3회씩 실시하여 총 9,529명이 응시하였으며, 기사 560명과 산업기사 130명이 배출되었다.

정보보안기사·산업기사 자격제도는 2022년부터 한국방송통신전파진흥원에서 주관하고 있다.

표 4-3-5-2 정보보안 국가기술자격시험 응시자 및 합격자 현황

(단위: 명, %)

연도	정보보안기사			정보보안산업기사		
	실기 응시자	합격자	최종 합격률	실기 응시자	합격자	최종 합격률
2013	3,187	210	6.6	436	149	34.2
2014	2,558	315	12.3	556	87	15.7
2015	3,853	488	12.7	670	252	37.6
2016	4,144	306	7.4	1,292	247	19.1
2017	5,122	631	12.3	1,456	500	34.3
2018	4,650	805	17.3	1,225	288	23.5
2019	4,336	461	10.6	982	254	25.9
2020	4,372	348	8.0	886	331	37.4
2021	3,956	76	2.0	923	294	31.8
2022	4,131	560	13.6	898	130	14.5
합계	40,309	4,200	10.3	9,324	2,532	27.4

나. 디지털포렌식전문가

2016년부터 시행된 디지털포렌식전문가 1급 시험은 디스크분석, 데이터베이스분석, 네트워크분석, 모바일분석, 침해사고 대응 포렌식 등의 기법을 활용한 문제해결 능력을 평가한다. 2급 시험은 컴퓨터 구조와 디지털 저장매체, 파일시스템과 운영체제, 응용프로그램과 네트워크 이해, 데이터베이스, 디지털포렌식 개론 5개 과목으로 구성된 필기시험과 디지털포렌식 실무형 문제로 구성된 실기시험을 실시하고 있다.

다. 산업보안관리사

산업보안관리사는 2016년 산업통상자원부장관의 승인을 받아 2017년부터 국가공인 민간자격으로 시행하고 있다. 이 자격의 목표는 현장에서의 보호가치 대상, 산업기술 관련 인력·관리, 설비·구역, 정보·문서 등이 내외부의 위험요소로부터 침해받지 않도록 예방·관리 및 대응하는 인력 양성이다.

필기시험은 산업보안 관련 분야별 이론 및 기본지식, 응용능력을 바탕으로 산업 현장의 기술보호를 위한 보안정책 수립 및 실행, 평가 등 종합적인 보안 실무업무 능력을 평가한다. 관리적보안, 물리적보안, 기술적보안, 보안 사고 대응, 보안지식경영 등 총 5개 과목으로 구성된다.

국가공인 민간자격으로 승격된 이후 2017년부터 2022년까지 총 12회 시행되었고, 총 1,778명의 합격자를 배출하였다.

표 4-3-5-3 산업보안관리사 자격시험 응시자 및 합격자 현황

(단위: 명, %)

연도	응시자	합격자	최종 합격률
2017	1,114	537	48.2
2018	869	306	35.2
2019	752	224	29.8
2020	492	165	33.5
2021	734	315	42.9
2022	671	231	34.3
합계	4,632	1,778	37.2

[출처: 한국산업기술보호협회, 2022. 12.]

2. 국외 정보보호 전문 자격증

가. CISSP

CISSP(정보시스템보안전문가, Certified Information Systems Security Professional)는 ISC2(International Information Systems Security Certification Consortium, Inc.)에서 주관하는 자격증이다. ANSI/ISO/IEC 17024의 엄격한 요건을 충족한 정보보안 업계 최초의

국제자격증이다. 전세계적으로 15만 명 이상의 합격자를 배출하였고, 우리나라에는 2,144명의 합격자가 활동하고 있다. ISC2는 CISSP 외에도 CCSP(클라우드 보안 전문가, Certified Cloud Security Professional)·SSCP(시스템 보안전문가, Systems Security Certified Practitioner)·CSSLP(보안 소프트웨어 라이프사이클 전문가, Certified Secure Software Lifecycle Professional)·HCISPP(헬스케어 정보보안 및 프라이버시 전문가, HealthCare Information Security and Privacy Practitioner) 등의 자격증을 주관하고 있다. 2022년 ISC)2는 사이버보안 업계에 입문하는 초보 보안자를 위한 사이버보안 전문가(Certified in Cybersecurity-CC) 자격증을 출시하여 주관하고 있다.

표 4-3-5-4 CISSP 자격보유자 현황

(단위: 명)

구분	전세계	한국	미국	일본	중국	홍콩	싱가포르	호주
보유자	156,054	2,144	95,243	3,699	4,136	1,968	2,963	3,305

[출처: ISC2, 2022. 12.]

CISSP 자격증 시험은 보안 및 위기관리(Security and Risk Management), 보안 아키텍처 및 엔지니어링(Security Architecture and Engineering), 커뮤니케이션 및 네트워크 보안(Communication and Network Security) 등 8개 영역(domain)을 평가하는데, 시험 대상 8개 영역에서 5년 이상의 근무경력을 보유한 경우에만 응시 자격을 준다. 다만 학사 이상의 학위 소지나 인정된 별도 전문 자격증 취득 등 특정 조건을 만족할 경우 4년 이하의 근무경력만으로도 취득 가능하다. 경력 조건을 만족하지 못하는 경우 시험 합격 후 요구되는 경력을 채워 정식으로 자격증을 받을 수 있다(Associate 프로그램).

나. CCFP

CCFP(사이버포렌식전문가, Certified Cyber Forensic Professional)는 법정에서 인정받을 수 있는 디지털 증거를 확보하기 위하여 포렌식 기법과 절차, 실행기준, 합법적·윤리적 원칙에 관련한 전문성을 검정한다.

2003년부터 국내 자격으로 운영되었으나, 2013년 9월 ISC2(미국)로 CCFP 자격이 이관되면서 국제 공인 자격으로 승격되었다. 그러나 2017년 ISC2 임원진과 인증서 정책 위원회의 합의에 따라 CCFP 자격 폐지를 알렸고, 해당 자격은 2020년까지만 국제 공인 자격

등급이 유지되었다.

2021년부터는 CCFP는 국내 민간자격으로 등록되어 운영하고 있으며, 사이버포렌식전문가협회(KCFPA)가 소관하여 증거와 특징, 증거의 연계보관, 시행절차, 전문가 증언의 역할, 윤리강령의 과목을 필기 또는 실기의 방법으로 평가하고 있다.

다. CISM

CISM(정보보호관리자, Certified Information Security Manager) 취득을 위해서는 최소 5년의 정보보호 분야의 근무 경력이 요구되는데, 이 중 3년 이상은 정보보호 관리 업무 경험이어야 한다. 평가영역은 정보보안 거버넌스, 정보 위험성 관리 및 준수, 정보 보안프로그램 개발 및 관리, 정보 보안 사고 관리 등 4개이다. 전세계적으로 47,654명의 자격자가 배출되었고, 우리나라에서는 2022년 12월 기준 56명이 활동 중이다. CISM 자격시험은 한국정보시스템감사통제협회(http://isaca.or.kr)가 주관하고 있다.

3. 국내외 정보보호 유관 자격증

정보시스템감리사와 정보시스템감사사는 자격 취득을 위하여 보안지식도 요구한다는 점에서 정보보호 유관 자격증으로 분류하였다.

가. 정보시스템감리사

정보시스템감리사는 정보통신 감리분야의 국가공인 자격증으로, 정보시스템 감리를 수행할 전문인력 확보 목적으로 한국지능정보사회진흥원(NIA)이 해마다 자격시험을 실시하고 있다. 기술사나 기사 취득 후 7년 이상의 실무경력 또는 석사 취득 후 6년 이상의 실무경력을 갖춘 고급기술자가 대상이다. 감리 및 사업관리, 소프트웨어공학, 데이터베이스, 시스템구조, 보안 등 5개 과목으로 구성된 필기시험과 면접전형을 거쳐 합격 여부를 결정한 후 2주간의 이론교육과 1주간의 감리 실무교육을 실시한다.

나. 정보시스템감사사

정보시스템감사사(CISA, Certified Information System Auditor)는 1969년부터

ISACA(정보시스템감사통제협회, Information Systems Audit and Control Association)가 관리하고 있다. 현재 전세계적으로 90,767명이 자격을 취득하였고, 우리나라에서는 2022년 12월 기준 2,236명이 활동 중이다. CISA 자격시험은 정보시스템 감사 프로세스, IT 거버넌스 및 관리, 정보시스템 취득·개발 및 구현, 정보시스템 운영·유지보수 및 지원, 정보자산의 보호 등 5개 영역에 걸쳐 출제된다.

제4장

개인정보보호

제1절 「개인정보 보호법」 개정 추진 및 행정 체계

1. 「개인정보 보호법」의 개정 추진

개인정보 관련 공공분야를 규율하는 「공공기관의 개인정보보호에 관한 법률」을 민간 분야까지 확대 적용하기 위하여 2011년 3월 「개인정보 보호법」을 제정하였다. 현행 「개인정보 보호법」은 개별법의 개인정보보호 관련 규정을 통합하는 등 2020년 2월 4일 개정되어 같은 해 8월 5일 시행되었다. 종전에는 개인정보보호 감독기능이 행정안전부·방송통신위원회·개인정보보호위원회(이하 '개인정보위') 등으로, 개인정보보호 관련 법령은 「개인정보 보호법」과 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '「정보통신망법」') 등으로 각각 분산되어 있어 데이터 이용 활성화 및 정보주체의 권리 보호에 한계가 있었다. 이에 개정 법률은 가명정보를 이용할 수 있는 근거를 마련하고, 개인정보처리자의 책임성 강화 등 개인정보를 안전하게 보호하기 위한 제도를 보완하도록 하였다. 또한 분산되어 있었던 개인정보보호 관련 감독기능은 개인정보위로, 「정보통신망법」과의 유사·중복 규정은 「개인정보 보호법」으로 일원화하여 개인정보보호 관련 법령을 체계적으로 정비하였다.

현행 「개인정보 보호법」은 「정보통신망법」의 규정을 정비하여 하나의 법률로 통합하였으나, 정보통신서비스 제공자 등의 개인정보 처리 등에 관해서는 개인정보처리자와는 별도로 특례를

규정하는 형식을 취하고 있다. 이에 대하여 온·오프라인 이중 규제, 수범자의 혼란 가중 등 문제가 지적되었다. 또한 2020년 2월 「개인정보 보호법」을 포함한 데이터 3법(「개인정보 보호법」·「정보통신망법」·「신용정보법) 개정 논의 시 인공지능·빅데이터 등 변화하는 정보 환경에서 약화될 우려가 있는 국민의 정보주권 강화, 데이터 경제 활성화의 장애 요소로 작용할 수 있는 불합리한 규제 개선 등이 차기 입법과제로 제기되었고, 이 사항들을 「개인정보 보호법」에 반영할 필요가 있었다.

이러한 문제점을 개선하기 위하여 개인정보위는 출범(2020. 8. 5.) 이후 「개인정보 보호법」 개정 태스크포스(TF)를 운영하는 등 추가 개정 논의를 시작, 2021년 1월 「개인정보 보호법」 개정안을 마련하여 입법예고하였다. 그 후 각계(산업계·시민단체·관계부처)의 의견수렴과 전문가의 검토를 거쳐 2021년 9월 법률 개정안을 국회에 제출하였다.

표 4-4-1-1 「개인정보 보호법」 개정안 주요 내용

유형	주요 내용
디지털 시대에 적합한 국민의 권리 강화	• 개인정보 전송요구권(이동권)의 일반법적 근거 마련 ※ 현재 금융과 공공분야에만 시범 도입 → 전 분야, 전 사업 간 자유로운 데이터 이동 • 인공지능 기반의 자동화된 결정이 채용, 복지 대상자 선정 등 국민의 권리·의무에 중대한 영향을 미치는 경우 거부 및 설명 요구 등 적극적 대응권 신설 • 복잡하고 형식적인 '동의'를 국민이 알고 하는 동의제도로 실질화 ※ 계약 체결·이행 시 필수동의 개선, 개인정보 처리방침 평가제 도입 등
디지털 중심 법·체계 정비	• 드론·자율주행차 등 이동형 영상정보 처리기기의 안전한 활용을 위한 운영기준 마련 • 정보통신서비스 제공자 특례를 일반 규정으로 전환하고, 불합리한 규제를 정비하여 '동일행위 – 동일규제' 원칙 적용
글로벌 규제와 정합성 확보	• 과도한 형벌 규정을 경제벌 중심으로 전환(산업계 건의) ※ 개인정보 수집·이용(5년), 유출(2년)에 대한 형벌 삭제 → 과징금으로 전환 • 국제수준에 맞추어 과징금 상한을 '관련 매출액'에서 '전체 매출액'으로 전환 ※ EU: 전세계 매출액의 4%, 중국: 전년도 매출액 5%, 캐나다: 전세계 매출액 5% 예정 • 국경 간 데이터 이동에 대한 국외 이전 요건을 다양화하고, 안전한 데이터 이동을 위하여 국외 이전 중지명령권 신설

개인정보위가 발의한 개정안 외에 국회에 계류 중인 20건의 개정안을 통합한 정무위원회 위원장 대안이 정무위원회에서 의결되었으며(2022. 12. 5.), 2023년 3월 14일 개정되어 같은 해 9월 15일 시행(일부 규정은 2024년 3월 이후 시행)될 예정이다.

「개인정보 보호법」 개정사항은 '디지털 시대에 적합한 국민의 정보주권 강화, 디지털 중심의 법 체계 정비, 글로벌 규제와의 정합성 확보'등 으로 유형화할 수 있으며, 주요 내용은 [표 4-4-1-1]과 같다.

2. 개인정보보호 행정 체계

개인정보위는 「개인정보 보호법」에서 국무총리 소속 중앙행정기관이라고 규정하고 있다. 다만 「개인정보 보호법」은 개인정보위의 독립성을 보장하기 위하여 소관 사무 중 정보주체의 권리침해에 대한 조사 및 이에 따른 처분(시정조치, 과태료·과징금 부과 등)에 관한 사항, 개인정보 처리와 관련한 고충처리·권리구제 및 개인정보에 관한 분쟁 조정, 개인정보 침해요인 평가에 관한 사항에 대해서는 「정부조직법」에 따른 국무총리의 행정감독권의 적용을 배제하고 있다. 그 밖에 개인정보위는 개인정보보호와 관련한 법령 개선, 정책·제도 수립 및 집행, 국제기구 및 외국의 개인정보보호기구와 교류·협력, 개인정보보호에 관한 법령·정책·제도·실태 등의 조사 및 연구, 개인정보보호에 관한 교육·홍보, 개인정보보호에 관한 기술개발의 지원·보급 및 전문인력의 양성 등의 사무를 수행한다. 또한 개인정보위는 중앙행정기관·지방자치단체·국회·법원·헌법재판소·중앙선거관리위원회가 이 법을 위반하였을 때에는 해당 기관의 장에게 시정조치를 하도록 권고할 수 있으며, 개인정보보호와 정보주체의 권익 보장을 위하여 3년마다 개인정보보호 기본계획을 수립한다.

중앙행정기관은 개인정보보호 기본계획에 따라 개인정보보호를 위한 시행계획을 해마다 작성하여 개인정보위에 제출하고, 개인정보위의 심의·의결을 거쳐 시행하여야 한다. 공공기관은 일정 규모 이상의 개인정보 파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우 그 위험요인의 분석과 개선 사항 도출을 위한 평가를 하고 그 결과를 개인정보위에 제출하여야 한다.

개인정보 주체인 국민은 자신의 개인정보에 대한 열람·정정·삭제·처리정지 등의 권리를 요구할 수 있으며, 정보주체가 이러한 권리를 요구할 때 개인정보 처리자는 그 처리 결과를 정보주체에게 통지하여야 한다. 또한 개인정보 처리자는 개인정보보호를 위하여 안전성 확보 조치 및 정보주체의 권리 보호 등을 위한 절차를 마련하거나 조치를 취하여야 한다.

그림 4-4-1-1 개인정보보호 행정 체계

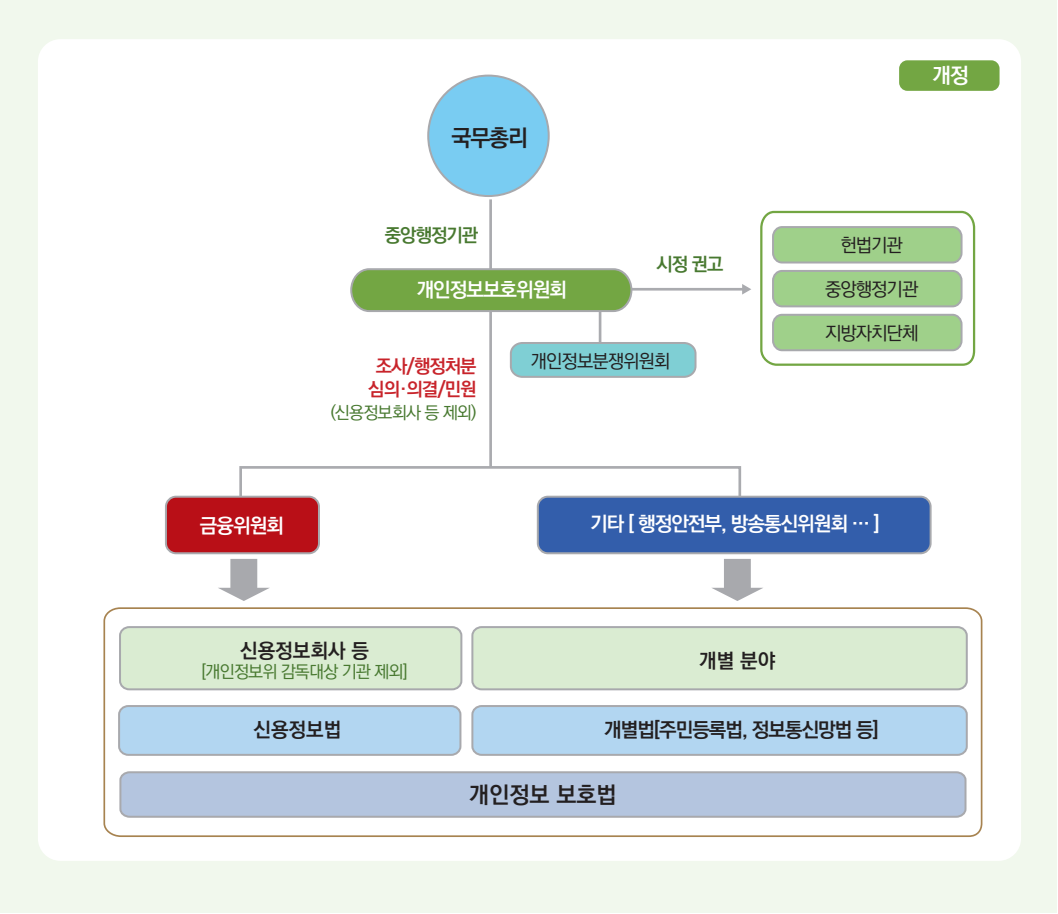
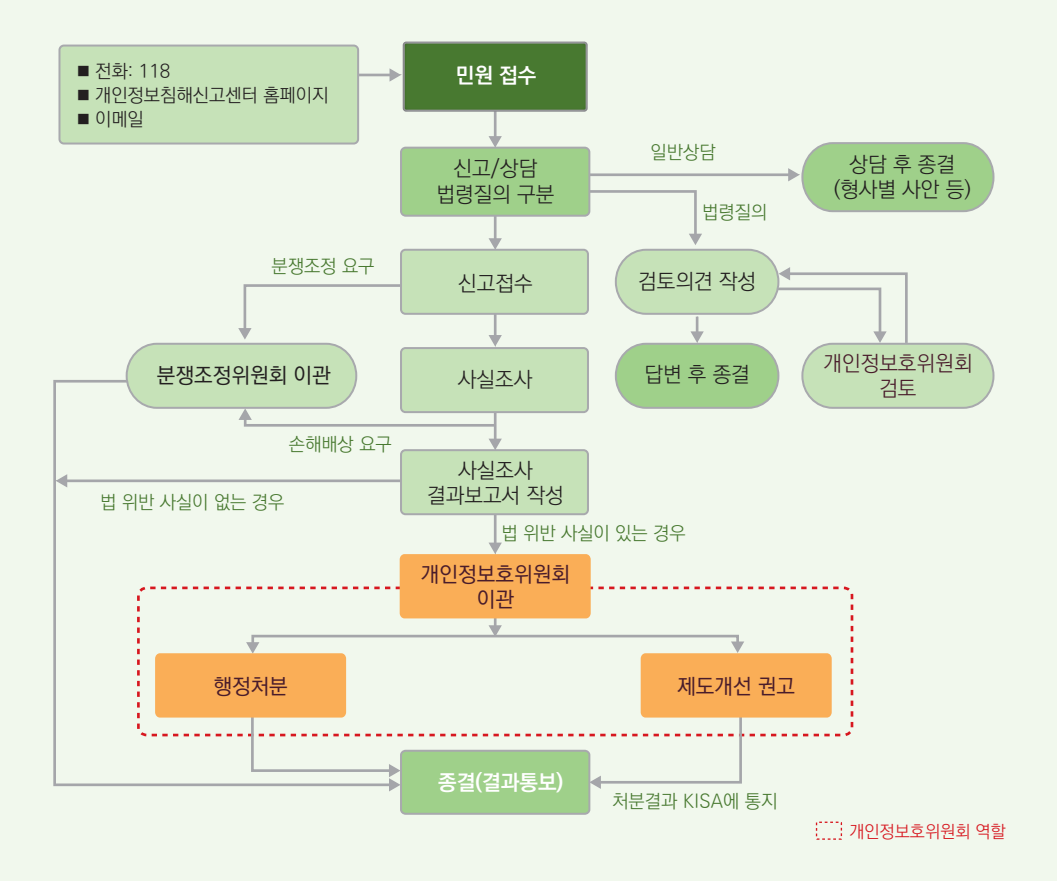


그림 4-4-1-2 개인정보 침해 신고 및 민원처리 절차



제2절 법·제도적 기반 강화

1. 공공 및 일반 부문

개인정보 유출 등 개인정보 침해 사고는 지속적으로 발생하였다. 특히 2014년 1월 카드사 개인정보 유출 사고로 8,868만 건의 대규모 개인정보가 유출되었고, 2014년 3월 통신사 고객정보 유출 사고로 1,170만 건의 개인정보가 유출되었다. 이에 행정안전부·방송통신위원회·개인정보보호위원회·금융위원회·과학기술정보통신부 등 관계부처가 합동으로 개인정보를 보호하고 재발을 방지하는 제도개선 방안을 마련하기 위하여 2014년 7월 '개인정보보호 정상화 대책'을 발표하였다. '개인정보보호 정상화 대책'은 징벌적 손해배상과

법정손해배상 등 새로운 손해배상제도의 도입, 개인정보 범죄에 대한 처벌 강화 등 7대 핵심 과제를 담고 있으며, 이에 따라 개인정보보호 관련 법률 개정 등 개인정보보호 강화 정책이 추진되었다.

「개인정보 보호법」은 제정 이후 개인정보보호 관리수준을 강화하는 방향으로 지속적으로 개정되었다. 2016년에는 정보주체 이외의 자로부터 개인정보를 수집하여 처리하는 경우 정보주체에게 수집 출처·처리 목적 등을 고지하도록 하였고, 민감정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 안전성 확보 조치를 하도록 법률에 의무화 하였으며, 주민등록번호를 수집할 수 있는 법령의 범위를 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙·감사원규칙으로 한정함으로써 주민등록번호 처리기준을 강화하였다. 또한 행정안전부·방송통신위원회·과학기술정보통신부·금융위원회 등 관계부처는 개인정보의 무분별한 수집을 방지하면서도 개인정보 활용이 증가하는 빅데이터 시대 사회 트렌드를 반영하여 관계부처 합동으로 2016년 6월 '개인정보 비식별 조치 가이드라인'을 마련, 금융·의료·공공 등 분야별 전문기관을 통하여 사업자의 비식별 조치를 지원하였다. 그러나 이 가이드라인은 법적 근거가 미흡하여 비식별 조치를 통한 개인정보 이용 활성화의 어려움 등 문제가 지속적으로 제기되면서 '가명정보 처리 가이드라인'으로 대체되었다.

2017년에는 정보주체가 열람, 정정·삭제, 처리정지 요구 등 자신의 권리를 쉽게 행사할 수 있도록 전화·전자우편·인터넷 등을 활용할 수 있는 방법을 제공하도록 하여 정보주체의 권리를 강화하였다. 또한 개인정보처리자가 서면 등으로 정보주체의 동의를 받을 때에는 수집·이용하려는 개인정보의 항목 중 민감정보 등 중요한 내용을 알아보기 쉽게 표시하도록 하고, 글씨 크기 등 표기 방법에 관한 기준을 수립하여 정보주체가 동의할 사항을 쉽게 알아볼 수 있도록 하였다.

2018년에는 개인정보 처리 위탁 시 위탁자와 수탁자가 지켜야 할 의무사항과 조치사항을 제시하여 개인정보 처리 현장의 혼란을 최소화하고, 국외에 개인정보 처리를 위탁할 때 감독 의무의 이행 등 사업자 문의가 많은 부분에 대한 해설을 제공하고자 '개인정보 처리 위·수탁 안내서'를 발간하는 등 환경 변화에 대응하여 개인정보보호 규제 합리화에 노력하였다.

2020년에는 「개인정보 보호법」을 개정하여 '가명처리' 및 '가명정보'의 개념을 도입, 통계 작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수

있도록 하였다. 또한 가명정보 처리와 관련한 구체적인 안내를 위하여 '가명정보 처리 가이드라인'을 발간하였다. 그리고 「개인정보 보호 법령 및 지침·고시 해설」 개정을 통하여 「개인정보 보호법」 전반에 대한 해설을 보완하고 법 개정사항에 대한 해설을 추가하는 등 개인정보의 보호와 활용의 균형을 위한 정책을 추진하였다.

2021년에는 정보주체의 권리 강화, 글로벌 규제와 정합성 확보, 디지털 중심의 법 체계 정비를 주요 내용으로 하는 「개인정보 보호법」 개정안을 마련하여 국회에 제출하였다. 그리고 인공지능·생체정보 등 ICT 신기술 기반의 서비스에서 개인정보의 안전한 활용을 위하여 인공지능 서비스 개발자와 운영자가 개인정보 처리 단계별로 상시 점검하여야 하는 점검항목(16개)과 확인사항(54개)을 알기 쉽게 제시한 '인공지능 개인정보보호 자율점검표'를 발간하였다. 또한 생체정보처리자 등이 개인정보 처리 단계별로 안전한 생체정보 활용을 위하여 준수하여야 할 사항을 현장 실무자가 이해하기 쉽게 구성한 '생체정보 보호 가이드라인'을 발간하였다. 아울러 긴급 상황에 개인정보 처리방법을 4가지 긴급 상황별로 분류하여 관계기관 등의 개인정보 처리 방법을 수집·이용과 제공 단계로 구분하여 설명하는 '긴급상황 개인정보 처리 및 보호수칙'을 마련하였고, 어린이집 아동학대 의심 시 보호자가 CCTV를 신속하게 확인할 수 있도록 제도를 개선하여 CCTV 열람 절차 관련 보호자의 불편을 해소하였다.

2022년에는 동의의 내용이 복잡하고 다양해지는 디지털 환경의 변화, 데이터 처리 확산 등을 고려하여 정보주체가 알아야 할 사항을 충분히 인지하고 동의를 할 수 있도록 '알기 쉬운 개인정보 처리 동의 안내서'를 발간하였다. 이 안내서를 발간함에 따라 기존에 발간한 '개인정보 수집 최소화 가이드라인'(2020. 12.)과 '온라인 개인정보처리 가이드라인'(2020. 12.)」은 폐지되었다. 기존에 공개되어 있는 개인정보 처리방침이 대부분 획일적·형식적으로 작성되어 있어 정보주체가 쉽게 확인하기 어려운 문제가 있었다. 이를 개선하기 위하여 일반 외 보건의료·교육·여행업·공공기관 등 업종별 특성을 구분한 작성지침을 마련하고, 핵심사항은 정보주체가 쉽게 인지할 수 있는 픽토그램(기호) 형태로 구성하였다. 또한 아동·청소년을 개인정보의 주체로 인식, 이들의 권리 실질화 및 역량을 강화하기 위한 '아동·청소년 개인정보 보호 기본계획'을 수립하고, 이에 대한 후속 조치로 '아동·청소년 개인정보보호 가이드라인'을 제정하였다.

2. 정보통신 부문

2014년 7월 개인정보 침해에 대한 국민의 불안감을 해소하고 종합적이고 근본적인 개인정보보호 대책을 마련하기 위하여 방송통신위원회 등 관계부처는 합동으로 '개인정보보호 정상화 대책'을 발표하였다. 2015년 5월 사업자의 자율적 준수를 유도하여 개인정보보호 수준을 제고하고, ICT 환경 변화를 반영하기 위하여 「개인정보의 기술적·관리적 보호조치 기준」을 개정하였다. 기술적·관리적 보호조치란 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영, 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술 등을 이용한 보안조치, 백신 소프트웨어의 설치·운영 등 컴퓨터바이러스에 의한 침해 방지조치 등을 말한다.

2016년에는 「정보통신망법」을 개정하였으며, 주요 내용은 다음과 같다.

첫째, 스마트폰 응용프로그램 개발자나 개발회사가 이용자 스마트폰에 대한 접근권한이 필요한 경우 프로그램 본래 기능 수행에 반드시 필요한 권한과 그렇지 않은 선택적 권한을 구분하여 각각 세부 항목과 이유를 이용자가 명확히 인지하도록 알리고 이용자로부터 동의를 받도록 하였다.

둘째, 스마트폰 응용프로그램 개발자나 개발회사가 프로그램 본래 기능 수행에 반드시 필요하지 않은 선택적 접근권한에 이용자가 동의하지 않는다는 이유로 이용자가 프로그램 자체를 이용할 수 없도록 하는 것을 금지하였다.

셋째, 개인정보 취급업무를 위탁하는 경우에 위탁자에게 수탁자에 대한 교육 의무를 부여하였다.

넷째, 개인정보 취급업무를 위탁하는 경우에 문서에 의하도록 하고, 수탁자는 위탁자의 동의를 받은 경우에 한하여 위탁받은 업무를 제3자에게 재위탁할 수 있도록 하였다.

다섯째, 개인정보보호 책임자는 개인정보보호와 관련하여 이 법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하고, 필요한 때에는 사업주 등에게 보고하도록 하였다.

여섯째, 정보통신서비스 제공자 등의 개인정보 분실·도난·유출·위·변조 또는 훼손 행위에 대한 징벌적 손해배상 및 개인정보 관련 범죄로 인한 이익을 환수하기 위한 몰수·추징 규정을

도입하였다.

또한 유출 사고 발생 직후 사업자의 신속한 조치를 위하여 2016년 8월 '개인정보 유출 대응 매뉴얼'을 마련하였다. 이 매뉴얼은 추가 유출문제 발생을 방지하여 유출로 발생하는 피해를 최소화하기 위한 조치들을 설명하고 있다.

이 밖에도 방송통신위원회는 2017년 2월 인터넷 이용자의 행태정보를 무분별하게 수집하여 광고함으로써 발생할 수 있는 개인정보 침해를 최소화하기 위하여 '온라인 맞춤형 광고 개인정보보호 가이드라인'을 마련하였다.

2017년 3월 관계 사업자의 법령에 대한 이해를 높이고 법규 준수율을 제고하기 위하여 '스마트폰 앱 개인정보보호 안내서'를 발간하였고, 2017년 12월 바이오정보의 보호와 안전한 활용을 위한 '바이오정보보호 가이드라인'을 마련하였다.

또한 사업자가 개인정보를 안전하게 보관·관리하기 위하여 지켜야 할 '개인정보의 기술적·관리적 보호조치 기준 해설서'를 개정하였다. 개정된 해설서는 내부관리계획 수립·시행 등 관리적 분야, 접근통제, 접속기록의 위·변조 방지, 개인정보의 암호화, 악성 프로그램 방지 조치 등 기술적 분야를 포함하여 총 10개 조항에 대하여 보완하고, 2015년 5월 고시 개정을 통하여 반영된 보호조치 기준의 목적, 최대 접속시간 제한조치, 암호화 대상 등 바뀐 제도를 추가하였다.

2018년은 우리나라를 비롯하여 여러 국가에서 개인정보보호 강화를 요구하는 목소리와 4차 산업혁명의 핵심 자원인 개인정보를 활용하고자 하는 목소리가 동시에 부각된 한 해였다. 그 어느 때보다 두 가지 요구의 조화가 강조되는 시기로 방송통신위원회 역시 개인정보보호와 4차 산업혁명 지원 정책의 조화를 이루기 위하여 여러 정책을 추진하였다.

국내에 주소 또는 영업소가 없는 정보통신서비스 제공자 중 일정한 기준을 충족하는 자는 국내에 대리인을 지정하도록 하고 국내대리인은 개인정보보호 책임자의 업무, 개인정보 유출 등의 통지·신고 및 조사에 필요한 자료제출 등의 업무를 수행하도록 하여 우리 국민이 글로벌 사업자에게도 국내 사업자에 대하여 행사하는 것과 마찬가지로 본인의 개인정보에 대하여 수집·이용·제공 등의 동의 철회, 열람청구, 정정요구 등 자기결정권을 실질적으로 행사할 수 있도록 하고, 방송통신위원회가 글로벌 사업자의 개인정보 침해 여부를 판단하기 위하여

자료를 요청할 경우 필요한 자료를 신속하게 제출할 수 있도록 하였다.

그리고 이미 국외로 이전된 개인정보를 제3국으로 재이전하는 경우 국외 이전과 동일하게 원칙적으로 동의를 받도록 하였는데, 특히 우리나라보다 개인정보보호 수준이 낮은 나라로의 이전에 대해서는 국제규범상 동등하게 보호하는 등 우리 국민의 개인정보가 국외에서도 안전하게 유통될 수 있는 방안을 마련하였다. 또한 이용자의 개인정보 수집·이용 동의 획득 방법을 전자우편·전화 등으로 한정적으로 열거하고 있던 현행 「정보통신망법 시행령」을 개정, 문자메시지·모바일 앱·SNS 등 동의 획득 방법을 확대하여 이용자와 사업자의 편익을 향상시켰다. 그리고 이용자 권리가 실질적으로 보장될 수 있도록 개인정보 열람·제공 요구, 이용내역 통지 등 사업자의 구체적인 이용자 권리 운영 기준을 담은 '온라인 개인정보 처리 가이드라인'을 개정하였다.

2019년에는 「정보통신망법」 개정을 통하여 ① 정보통신서비스 제공자로 하여금 만 14세 미만 아동에게 개인정보 처리와 관련된 사항을 알리거나 고지 등을 하는 때에는 이해하기 쉬운 양식과 명확하고 알기 쉬운 언어를 사용하도록 하여 아동의 권리를 강화하고, ② 방송통신위원회로 하여금 정보통신서비스 제공자 등의 자율적인 개인정보보호 활동을 촉진·지원하기 위한 시책을 마련, 정부가 정보통신서비스 제공자 등의 자율적인 규제 활동을 지원하여 그 책임성을 높일 수 있도록 하였다. 또한 ③ 일정 규모 이상의 정보통신서비스 제공자 등에 대해서는 개인정보 침해 사고 시 이용자의 피해구제를 보장할 수 있도록 손해배상책임의 이행을 위하여 보험 또는 공제에 가입하거나 준비금을 준비하는 등 필요한 조치를 하도록 하였다.

또한 개인위치정보가 실질적으로 보호되면서도 안전하게 활용될 수 있도록 「위치정보법」을 개정하여 사물위치정보사업자에 대하여 방송통신위원회의 허가를 받도록 하던 것을 신고하도록 하여 진입규제를 완화하고, 1인 창조기업 또는 소상공인의 경우 신고 절차를 간소화하여 위치기반서비스사업을 할 수 있도록 하였으며, 사물위치정보에 대해서는 소유자의 사전 동의 없이도 위치정보가 처리될 수 있도록 하였다.

이와 같이 방송통신위원회는 개인·위치정보의 철저한 보호를 기본으로 하되, 4차 산업혁명에 대응하여 데이터 기반 신산업 활성화를 지원하기 위한 정책의 조화를 이루기 위한 노력을 지속하고 있다.

2020년에는 「정보통신망법」과 「개인정보 보호법」 개정을 통하여 정보통신 분야의 개인정보 보호 업무를 관장하던 방송통신위원회 업무가 개인정보위로 이관되는 등 큰 변화가 있었다. 「정보통신망법」 개정을 통하여 개인정보 관련 조항(제4장)을 삭제하고, 정보통신서비스 제공자에게 특수하다고 인정되는 규정은 개정된 「개인정보 보호법」(2020. 8. 5. 시행)에 '정보통신서비스 제공자 등의 개인정보 처리 등 특례'(제6장) 규정을 두어 이에 편입하였다. 이러한 특례 규정에는 정보통신서비스 제공자 등에만 적용되는 유출통지·신고 의무(24시간 이내 통지), 손해배상책임 이행을 위한 보험 또는 공제 가입, 1년 이상 서비스 미이용자의 개인정보 파기, 이용내역의 통지, 국내대리인의 지정 등의 내용을 포함하고 있다.

2021년에는 정보통신서비스 제공자 등에 대한 개인정보 처리에 관한 특례 규정을 일반 규정으로 통합하기 위한 「개인정보 보호법」 개정안을 마련(2021. 7.)하였는데, 이 개정안은 정부 입법 심사를 거쳐 2021년 9월 28일 국회에 발의하였다.

개인정보위가 발의한 개정안과 국회에 계류 중인 20건의 의원 발의 개정안을 통합한 정무위원회 위원장 대안이 정무위원회에서 의결(2022. 12. 5.) 되었고, 2023년 3월 14일 개정되어 같은 해 9월 15일에 시행(일부 규정은 2024년 3월 이후 시행)될 예정이다. 해당 개정 법률이 시행되면 정보통신 분야에 대한 별도의 규정이 일반 규정에 통·폐합되어 온·오프라인 구별 없이 모든 개인정보처리자에 대하여 동일한 규제가 시행될 예정이다.

제5장

대국민 정보보호

제1절 정보보호 상담 및 처리

1. 개요

한국인터넷진흥원은 2010년 1월 18일 사이버 고충 민원을 상담·처리하는 118상담 서비스를 시작하였다. 이전에는 해킹·바이러스, 개인정보 침해, 불법스팸 등에 대하여 별도의 상담창구를 운영해 왔으나, 사이버상에서의 피해 형태가 다양해지고 이로 인한 국민의 불편을 최소화하기 위한 통합적인 상담 체계가 필요하다는 목소리를 반영하여 '118상담센터'를 출범시켰다.

'118상담센터'는 언제 어디서나 원하는 시간에 (국번 없이) 118을 누르면 전문상담인력과 연결되어 무료 상담을 받을 수 있으며, 해킹·바이러스, 개인정보 침해, 불법스팸 등 사이버상에서 발생할 수 있는 역기능 문제 외에도 인터넷상의 본인확인, 인터넷 주소 관련 문의 등 인터넷 이용 중에 느끼는 불편이나 궁금증을 전화 한 통화로 해결할 수 있도록 도움을 주고 있다.

2. 118 상담 현황

가. 연도별 상담 현황

118상담센터는 2010년부터 2022년까지 13년 동안 총 5,710,291건을 상담하였다. 2022년 한 해 동안의 전화 및 온라인 상담건수는 30만 861건으로 2021년 대비 25.9% 감소하였다.

표 4-5-1-1 연도별 118상담센터 민원 접수처리 현황

(단위: 건)

연도	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
상담건수	349,185	462,073	477,392	612,496	633,760	553,664	384,311	336,407	378,178	389,611	426,382	405,971	300,861

나. 분야별 상담 현황

2022년 118 상담건수를 분야별로 보면 개인정보(49.8%), 해킹·바이러스(20.8%), 스팸(9.2%) 순으로 많았다.

개인정보 분야의 경우 2021년 대비 약 26.2% 감소한 14만 9,680건이 접수되었는데, 이는 기관 및 지인 등을 사칭한 보이스피싱·메신저피싱 등 금융사기 관련 상담이 감소하였기 때문인 것으로 분석된다.

해킹·바이러스 분야의 경우 2021년 대비 약 13.1% 감소한 6만 2,471건이 접수되었는데, 이는 택배, 교통법규 위반, 건강검진 문자 등으로 피해자를 속여 돈을 가로채는 스미싱 관련 상담이 전년 대비 감소한 것에 따른 영향인 것으로 분석된다.

스팸 분야의 경우 2021년 대비 약 30.0% 감소한 2만 7,721건이 접수되었는데, 이는 금융기관 사칭 불법대출 문자 스팸 사전 차단 등 국민 피해 예방 활동 강화로 불법대출 스팸이 대폭 감소함에 따라 관련 상담 또한 감소한 것으로 분석된다.

표 4-5-1-2 118상담센터 분야별 상담 현황

(단위: 건)

연도	2018	2019	2020	2021	2022
개인정보	163,172	158,214	175,366	202,923	149,680
스팸	45,960	37,272	35,286	39,612	27,721
해킹·바이러스	58,333	66,398	78,284	71,915	62,471
기타*	110,713	127,727	136,446	91,521	60,989
합계	378,178	389,611	426,382	405,971	300,861

* '기타'는 온라인 광고, 전자거래 분쟁 조정, 인터넷 주소 등 한국인터넷진흥원의 사업 관련 문의에 대한 안내 등

제2절 인식 제고

1. '정보보호의 날' 기념식 개최

2022년 제11회 '정보보호의 날'을 맞이하여 과학기술정보통신부·국가정보원·국방부·행정안전부·경찰청이 공동으로 주최하는 기념식이 7월 13일 경기도 판교 제2테크노밸리 기업지원허브에서 개최되었다. 정부는 사회 안전의 기본인 정보보호의 중요성을 강조하고, 증가하는 새로운 사이버위협에 대한 범부처 대응 역량의 결집과 국민적 관심을 촉구하기 위하여 7월을 '정보보호의 달', 7월 둘째 수요일을 법정 기념일인 '정보보호의 날'로 지정·운영하고 있다.

2022년 기념식은 '튼튼한 사이버 안보, 안전한 디지털 강국'을 주제로 사이버위협에 대응하는 디지털 안심 국가 실현이 강조되었다. 윤석열 대통령은 역대 대통령으로서는 처음으로 기념식에 참석하여 정보보호 종사자의 자긍심을 높이고, 사이버안보 기술을 전략산업으로 육성하기 위한 정부의 정책 방향을 밝혔다.

포스트 코로나19 시대에 맞추어 온·오프라인으로 동시 개최된 2022년 행사에서는 기념식과 콘퍼런스에 약 950명이 현장 참석하고, 2천여 명이 온라인으로 참여하여 정부 및 산·학·연 관계자와 국민이 함께 소통하는 장을 마련하였다.

그림 4-5-2-1 제11회 '정보보호의 날' 기념식

정보보호 유공자 시상식에서는 우리나라 정보보호 발전에 이바지한 4명에 대하여 녹조근정훈장, 산업포장, 국민포장, 대통령 표창을 수여하였다. 더불어 정보보호의 비전과 정부의 의지를 담아 사이버안보를 강조하는 세리머니 퍼포먼스를 진행함으로써 10만 사이버 인재 양성, 안심할 수 있는 디지털 환경 구축 등 국정과제 핵심 메시지를 국민과 다시 한번 공유하는

자리를 가졌다.

기념식 행사는 국제 정보보호 콘퍼런스, 정보보호제품 전시회 등의 부대행사와 연계하여 정보보호 기술 동향 및 신규 사이버위협 대응을 위한 국내외 이슈를 공유함과 동시에 국내 보안 기업 제품 홍보 등의 시너지를 창출하였다.

국제 정보보호 콘퍼런스에서는 미래 융합 보안, 디지털 플랫폼 시대의 데이터 보안, 공공분야 사이버보안, 정부 보안 정책, 사이버보안 위협 동향, 개인정보보호 등 3개 트랙 6개 세션으로 구성, 기조연설을 포함하여 총 20개 강연이 온·오프라인으로 진행되었다. 정보보호 제품 전시회에는 17개 기업이 참여하여 보안 솔루션을 소개하고 홍보하는 기회를 가졌다.

2. 범국민 정보보호 인식 제고 활동

국민이 보편적으로 이용하는 월패드 등 홈네트워크 설비 관련 개인정보 유출 등의 정보보안 문제가 2022년 대두되었다. 이에 따라 홈네트워크 설비 관리자와 이용자에게 보안 수칙을 알리고 범국민적 관심과 자율적 정보보호 실천 문화를 확산하기 위한 인식 제고 활동이 실시되었다.

'스마트홈 구성요소에 대한 취약점 발굴 및 보안기술 연구'를 주제로 '2022 사이버보안 챌린지 대회'를 개최하여 보안 관련 기업·대학 등 23개 팀이 참가하여 스마트홈 제품군 6종에 대한 취약점을 발굴하였다. 보안 취약점 신고포상제와 연계하여 69건의 취약점 중 신규 취약점으로 인정된 44건은 별도의 포상금 지원과 장비제조사와 협의하여 보안패치도 마련할 계획이다.

'정보보호의 달'과도 연계하여 월패드 등 홈네트워크로 인한 피해 예방을 주제로 해킹 예방을 위한 보안수칙 포스터, 카드 뉴스, 영상 등을 제작하고 다양한 매체(버스 승차장, 아파트 엘리베이터 내 TV 등)에 송출하여 국민 경각심 고취와 정보보호 인식 제고 효과를 증대시켰다. 또한 SNS를 이용하여 진행된 시민 참여형 정보보호 실천 캠페인은 국민이 흥미를 느끼고 스스로 참여할 수 있는 기회를 제공하여 소통형 홍보 활동이 이루어졌다.

이와 함께 초·중·고교생을 대상으로 찾아가는 정보보호 진로 교육을 진행하여 학생들에게 정보보호에 대한 중요성을 알렸으며, 정보보안 전문가 직무 소개 영상을 제작·배포하여 학생

맞춤형 직무 소개 및 정보보호 인식 제고에 이바지하였다.

그림 4-5-2-2 인식 제고 홍보 활동

3. 금융 정보보호 인식 제고 활동

가. 금융보안 최고위 과정 운영 및 금융회사 최고경영자 초청 세미나 개최

금융보안원은 2017년부터 금융권 금융보안최고책임자(CISO) 등이 참여하는 금융보안 최고위 과정(FSP, Advanced Financial Security Management Program)을 운영하여 CISO의 전문역량을 강화하고 금융보안 공통 관심사에 대한 소통과 논의의 장을 제공하고 있다. 2022년에는 금융권 및 정보보호 산업계 디지털·정보보호 담당 경영진 29명을 대상으로 '제6기 금융보안 최고위 과정'을 운영하였다. 이를 통하여 경영진이 금융의 디지털 전환 및 데이터 혁신을 선도할 수 있도록 포스트코로나 시대의 넥스트 노멀을 준비하는 데 필요한 맞춤형 교육 과정을 제공하였다.

나. 금융정보보호 콘퍼런스 개최

'금융정보보호 콘퍼런스(FISCON, Financial Information Security Conference)'는 금융보안원이 금융보안포럼·금융정보보호협의회와 공동 주최하고, 금융위원회와 금융감독원이

후원하는 금융권 최대의 정보보호 행사이다.

2022년 FISCON은 '디지털화·빅블러 시대 금융보안 전략과 대응'을 주제로 오프라인 행사를 개최, 디지털화·빅블러 시대 및 새로운 디지털 위험에 대응하고자 디지털 건전성 확보 측면에서 금융보안 전략·기술·대응 총 21개 주제의 강연을 제공하였다.

그림 4-5-2-3 금융정보보호 콘퍼런스(FISCON 2022)

다. 금융권 버그바운티

금융보안원은 사이버보안 취약점을 선제적으로 발굴·제거하여 금융소비자 보호와 금융서비스 안전성을 강화하기 위한 금융권 버그바운티(Bug Bounty)를 실시하고 있다.

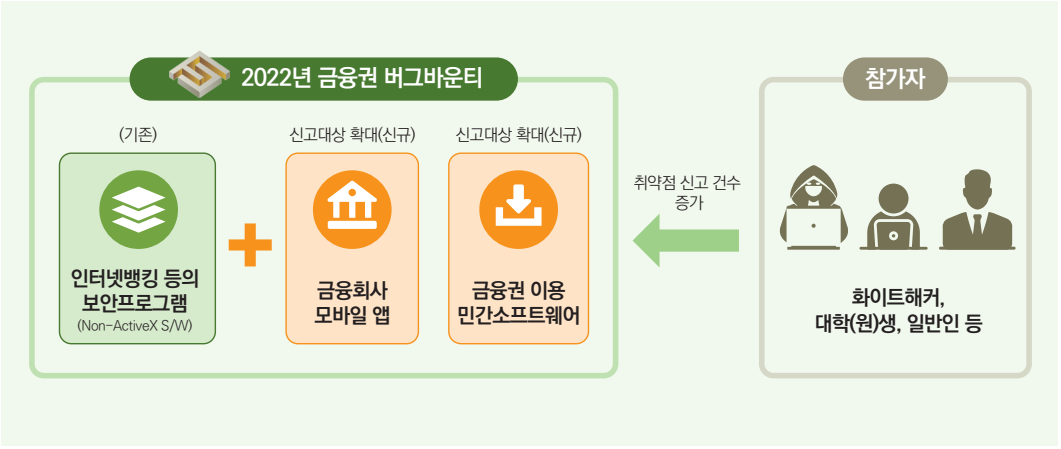
* 버그바운티(Bug Bounty): 취약점 신고 포상제로, 서비스와 제품의 신규 취약점을 신고받아 이를 평가하여 포상금을 지급하는 제도

금융권 버그바운티는 기존 신고 대상인 인터넷 뱅킹 등의 보안프로그램(Non-ActiveX)에서 나아가, 2022년부터 신고 대상을 금융회사 모바일 앱, 금융권 이용 민간 소프트웨어 등으로

대폭 확대하여 실시하였다.

2022년 신고·접수된 취약점은 61건(전년 대비 9배 증가)이었으며, 영향도, 공격난이도, 발굴난이도 등의 기준에 따라 내·외부 평가위원의 평가를 거쳐 25건의 우수 취약점을 선정하였다. 우수 취약점 신고자에게는 금융보안원장 명의의 감사장을 수여하여 금융보안 취약점 사전·식별과 제거의 중요성에 대한 인식을 제고하였다.

그림 4-5-2-4 금융권 버그바운티



제6장

국제협력

제1절 주요 사이버안보 외교 활동

1. 사이버공간 국제 평화 안보체제 구축에 관한 학술회의

국가보안기술연구소와 국가정보원은 2022년 9월 20~21일 '민주주의적 가치에 부합하는 새로운 사이버안보 전략의 발전'을 주제로 '사이버공간 국제 평화 안보체제 구축에 관한 학술회의(GCPR, International Conference on Building Global Cyberspace Peace Regime)'를 개최하였다. 2014년 시작하여 7회째를 맞이한 이 회의에서 각국 사이버안보 전문가가 한자리에 모여 정책 과제의 연구 결과를 검증·비교하고, 사이버공간의 국제 평화 안보체제 발전과 관련한 정책 방향을 모색하였다.

이 회의에서는 민주적 가치를 공유하는 국가 간 사이버안보 인식과 정부 정책 기조를 공유하고 앞으로 추진하여야 할 국가적 노력에 대하여 논의하였다. 국내외 전문가 40여 명과 청중 150여 명이 참석하여 ▲사이버위협의 동향과 한국의 과제 ▲위협 대응과 사이버공간의 국제질서 ▲사이버위협에 대한 적극적 대응 강화 ▲국가 차원의 효과적 대응을 위한 국가 전체적 역량의 강화를 핵심 의제로 논의를 진행하였다.

그림 4-6-1-1 제7회 사이버공간 국제 평화 안보체제 구축에 관한 학술회의

2. 유엔 사이버안보 국제규범 정립 논의

국제사회는 국가안보의 중대한 도전으로 떠오른 초국경적 사이버위협에 대응하기 위하여 유엔 내에서 관련 국제규범을 마련하기 위한 노력을 지속해 왔다.

우리 정부는 2019년부터 유엔총회 1위원회 산하 협의체인 정보안보 개방형 워킹그룹(OEWG, Open-Ended Working Group)에 참여하였다. 2021년부터는 2021~2025년 임기 제2차 OEWG 회의에 참여하였고, 2022년 제2차 실질회의(3. 28.~4. 1.), 제3차 실질회의(7. 25.~29.), 회기간 회의(12. 5.~9.)에도 참석하여 사이버공간에서의 위협, 국제규범 이행, 국제법 적용, 글로벌 연락망 설립 등 신뢰구축조치와 역량 강화 등 우리 정부 입장을 개진하였으며, 제77차 유엔총회에서 채택된 OEWG 연례 경과 보고서 채택에도 이바지하였다.

우리 정부는 합의된 규범의 구체적인 이행과 개발도상국의 이행 역량을 강화하기 위하여 사이버공간의 책임 있는 국가행동 증진을 위한 행동계획(PoA, Programme of Action for Responsible State Behaviours) 설립을 위한 공동제안국으로 참여하여 제77차 유엔총회에서 PoA 결의안이 채택되는 데 이바지하였으며, 앞으로 유엔 내 항구적·포용적 행동기반의 협의체로서 PoA가 성공적으로 정착할 수 있도록 다수의 유엔 회원국과 적극 협력하고 있다.

3. 역내 다자 사이버안보 국제협력 참여

우리 정부는 2017년 아세안지역안보포럼(ARF, ASEAN Regional Forum) 외교장관회의를 계기로 사이버안보 신뢰구축조치(CBM, Confidence Building Measures) 방안을 논의하기 위하여 설립된 ICT 안보 회기간 회의(ISM, Inter-Sessional Meeting)에 적극 참여하고 있다. 또한 2021년 4월 개최된 제3차 ICT 안보 회기간 회의에서 인도네시아·오스트레일리아·러시아와 함께 공동의장국을 수임하여 2023년까지 역내 사이버보안 역량 강화 및 신뢰구축 조치 발전에 이바지할 예정이다. 2022년에는 공동의장국으로서 제4차 ICT안보 회기간 회의를 주재(5. 13.)하여 사이버안보 관련 다자 논의 동향을 공유하고, 역내 사이버 신뢰구축 활동을 점검하였다.

우리 정부는 유럽안보협력기구(OSCE, Organization for Security and Co-operation in Europe)와 공동으로 사이버 신뢰구축 협력 증진을 위하여 사이버안보 콘퍼런스를 정기적으로 개최하고 있다. 2021년 6월에는 '아시아-유럽 지역의 사이버안보 협력'을 주제로 제3차 한-OSCE 사이버안보 콘퍼런스를 개최하여 아시아-유럽지역 정부·국제기구 관계자 및 관련 학계·업계 인사 등 300여 명이 사이버안보와 관련한 다양한 의견과 모범 사례를 공유하고, 지역 간 사이버안보 협력 방안을 심도 있게 논의하였다.

또한 우리 정부는 2022년 10월 미국 국가안보회의(NSC, National Security Council) 주관으로 개최된 '랜섬웨어 대응 이니셔티브'에 참여하여 최근 가장 중요한 사이버위협으로 떠오른 랜섬웨어 대응 방안 모색을 위한 주요국과 협의하였다. 이 회의에는 영국·독일·캐나다·뉴질랜드·싱가포르·일본·도미니카공화국·케냐 등 36개국이 참여하여 네트워크 안보와 회복력, 불법금융 대응, 랜섬웨어 네트워크 차단, 외교적 대응 등 구체적인 랜섬웨어 대응 공조 방안을 논의하였다.

4. 양자 사이버안보 협력을 위한 사이버정책협의회 개최

우리 정부는 2012년 한·미 사이버정책협의회 개최 이래 미국·영국·오스트레일리아·태국 등 13개 국가 및 EU·NATO와 고위급 사이버정책협의회를 개최하고 있다. 이러한 사이버정책협의회는 각국이 사이버안보 관련 전략·정책 및 위협 정보 등을 공유하고 사이버안보 관련

협력을 강화하는 유용한 계기가 되고 있다.

2022년 12월 개최된 제6차 한·미 사이버정책협의회에서는 양국 정부의 사이버안보 관련 정책을 공유하였다. 특히 핵심기반시설을 대상으로 한 사이버위협 탐지 기술 등에 대한 연구·개발 협력을 확대하기로 하고, 인적 교류와 연합 훈련도 추진하기로 하였다.

2023년 2월 개최한 제3차 한·영 사이버정책협의회에서는 양국 수교 140주년을 맞이하여 사이버안보 분야 협력을 양국 관계 발전의 중요한 축으로 더욱 발전시키기로 협의하였다. 양국은 사이버공격에 대한 선제적 억제 전략, 사이버안보 관련 민간분야와의 협력, 유엔 등 다자 무대에서 협력 강화 방안 등에 대하여 논의하였다.

5. 신안보 협력 논의 주도를 위한 세계신안보포럼 개최

우리 정부는 코로나19 확산, 사이버위협 증가 및 다변화, 인간의 통제를 벗어난 신기술 개발 및 오·남용 우려 등 새로운 안보 위협에 대응하고, 우리 정부의 연대와 협력의 국제질서 선도 의지를 구현하고자 2021년 세계신안보포럼을 창설하였다.

2021년 11월 16~17일 서울에서 개최된 제1차 세계신안보포럼에는 주요국 정부 고위인사뿐 아니라 국제기구·학계·기업 전문가들이 연사로 참석하여 보건안보, 사이버안보, 신기술안보 등 최근 국제사회의 신안보 위협 대응 관련 인식 제고 및 협력 강화 방안을 모색하였다. 2022년 6월 21~22일에는 '신흥안보 위협의 과거와 현재, 그리고 미래-신뢰에 기반한 국제협력으로의 길'을 주제로 제2차 세계신안보포럼을 개최하였다.

그림 4-6-1-2 제2차 세계신안보포럼

6. 개발도상국 역량 강화 지원

사이버위협은 사이버보안 역량이 부족한 국가에서 시작되거나 그러한 국가를 경유하는 경우가 많기 때문에 개발도상국의 사이버안보 역량 강화 노력이 중요하다.

우리 정부는 공적개발원조(ODA, Official Development Assistance)를 통하여 개발도상국의 사이버보안을 다방면으로 지원하고 있다. 무상원조 전문기관인 한국국제협력단(KOICA, Korea International Cooperation Agency)은 인도네시아·방글라데시·네팔·알제리·키르기즈공화국·우즈베키스탄·아제르바이잔 등에서 사이버안전 확보를 위한 개발협력 사업을 하고 있다. 한 예로, 경찰청과 국립과학수사연구원 등 관계부처와 협력하여 2018년부터 2024년까지 인도네시아의 사이버 범죄 수사 역량 강화(510만 달러 규모) 사업을 추진하고 있으며, 개발도상국 사이버보안 전문 인력 양성을 위한 위한 초청 연수 사업도 진행하고 있다.

우리 정부는 2021년 8월 네덜란드와 공동으로 '사이버공간에서의 국제법 적용에 관한 세미나'를 개최하여 아세안을 비롯한 14개 아시아 국가의 사이버안보 분야 관계자 50여 명과 사이버공간의 국제법 적용 관련 의견을 교환하고 모범사례를 공유하였다. 아울러 2021-24 회기 ARF ICT안보 회기간 회의 공동의장국 수임을 계기로 신뢰구축조치의 일환으로 '사이버안보 분야 보안 인력 양성' 워크숍 개최를 제안하였고(2022. 5.), 2023년 베트남과 함께 이 워크숍을 개최할 예정이다.

제2절 사이버보안 국제협력

1. 글로벌 사이버보안 협력 네트워크 운영

한국인터넷진흥원은 양자간 공조 체계 강화와 증가하는 다자간 협력 수요에 대응하기 위하여 2016년 7월 국외 침해사고대응팀 등 유관기관이 참여하는 글로벌 사이버보안 협력 네트워크(CAMP, Cybersecurity Alliance for Mutual Progress)를 발족하였다. CAMP는 2022년 말 기준 총 48개국 64개 기관의 회원으로 구성된 글로벌 협의체로, 안전한 사이버

세상과 신뢰 구축을 위한 네트워킹 플랫폼이다. 회원 간 사이버보안 분야 현황을 공유하기 위하여 뉴스레터를 정기적으로 발간하고 있으며, 2022년에는 대면 방식의 연례총회와 지역포럼을 개최하여 회원 기관의 활동 현황과 문제 대응 전략, 회원국의 사이버보안 현황 및 전망을 상호 공유하였다.

2022년 10월 코로나19 확산세 감소에 따라 2019년 이래 3년 만에 대면 방식으로 개최된 연례총회에는 18개국 19개 기관이 참여하였다. 디지털 대전환에 따른 사이버보안 동향 공유와 더불어 코로나19로 국외 홍보 활동이 위축된 기업들의 국외 진출 지원과 국내 우수 정보보호 기업의 기술력과 제품 홍보를 위한 쇼케이스 및 국내 기업-CAMP 회원 간 비즈니스 미팅을 운영하였다.

총회 기간 동안 아시아 권역의 CAMP 회원 간 네트워킹을 위하여 네팔의 사이버보안연구혁신센터, 스리랑카·카자흐스탄의 침해사고대응팀과 함께 지역포럼을 개최하였다. 이 포럼을 통하여 역내 사이버보안 최신 동향 및 쟁점 사항을 공유하고, CAMP 협의체와 아시아 권역 간 협력 강화 방안을 논의하였다.

이 밖에도 CAMP 운영상 이슈를 회원 중심으로 논의하고 이끌어가기 위하여 운영위원회를 구성, 정기적으로 회의를 개최하고 있다. 한국인터넷진흥원은 CAMP 발족 이후 의장과 사무국으로 선출되었으며, 2022년에 재연임되어 2025년까지 활동할 예정이며, 2023년 현재 운영위원으로도 활동하고 있다.

그림 4-6-2-1 CAMP 제7차 연례총회와 지역포럼

2. 국외 사이버보안 지원 활동

과학기술정보통신부와 한국인터넷진흥원은 개발도상국의 사이버보안 역량 강화를 통한 세계 사이버보안 환경을 증진하기 위하여 글로벌정보보호센터(GCCD, Global Cybersecurity Center for Development)를 운영하고 있다.

GCCD에서는 개발도상국을 대상으로 한국의 사이버보안 발전 경험과 노하우를 공유하는 역량 강화 프로그램을 운영 중이며, 2022년에는 사이버보안 수요 및 선호도에 기반한 주제로 사이버보안 온라인 세미나와 가상화 환경 기반 비대면 기술 실습을 제공하였다. 이러한 온라인 프로그램 운영을 통하여 총 29개국 453명이 교육에 참여하였다.

특히 한국인터넷진흥원은 세계은행 한국사무소와 협력하여 2022년부터 2024년까지 개발도상국 디지털개발을 위한 공동 협력 프로젝트(KoDi)를 수행하고 있다. 2022년에는 개발도상국 주요정보통신기반시설 보호를 위한 정책 제언 리포트를 작성하였고, 이 리포트를 기반으로 8개국 31명을 우리나라로 초청하여 주요기반시설 사이버보안 및 복원력 확보를 위한 역량 강화 세미나를 개최하였다.

중미경제통합은행(CABEI)과 코스타리카 과학기술정보통신부(MICITT)와 협력하여 코스타리카 사이버보안 담당자를 대상으로 '한국의 사이버보안 체계'와 '정보보호 및 개인정보보호 관리 체계 인증제도(ISMS-P)'를 전수하는 현지 세미나를 개최함으로써 상호 협력 의지를 확인하고, CABEI와 공동 프로젝트 추진 가능성을 타진할 수 있는 기회를 만들었다.

한국인터넷진흥원은 양자·다자간 협력 활동을 통하여 우리나라의 글로벌 위상을 제고할 뿐 아니라 국내 정보보호 기업 관계자들을 민간 전문가로 활용하여 우리 기업들의 글로벌 레퍼런스를 확보하는 등 앞으로도 글로벌 진출 기반 마련을 위하여 노력할 것이다.

부록

제1장 통계로 보는 정보보호
제2장 2022년 주요 정보보호 행사
제3장 국내 정보보호 관련 주요 사이트
제4장 정보보호 민간단체
제5장 국내 ISAC 현황

제1장

통계로 보는 정보보호

이 장에서는 국가 정보보안 정책의 수립과 개선을 위한 참고자료로 활용하고자 정보보안 실태에 관한 설문조사를 실시하고 그 결과를 분석한다. 국가·공공부문은 국가정보원이 중앙행정기관을 비롯한 99개 기관 정보보호 담당자를 대상으로 하였다.

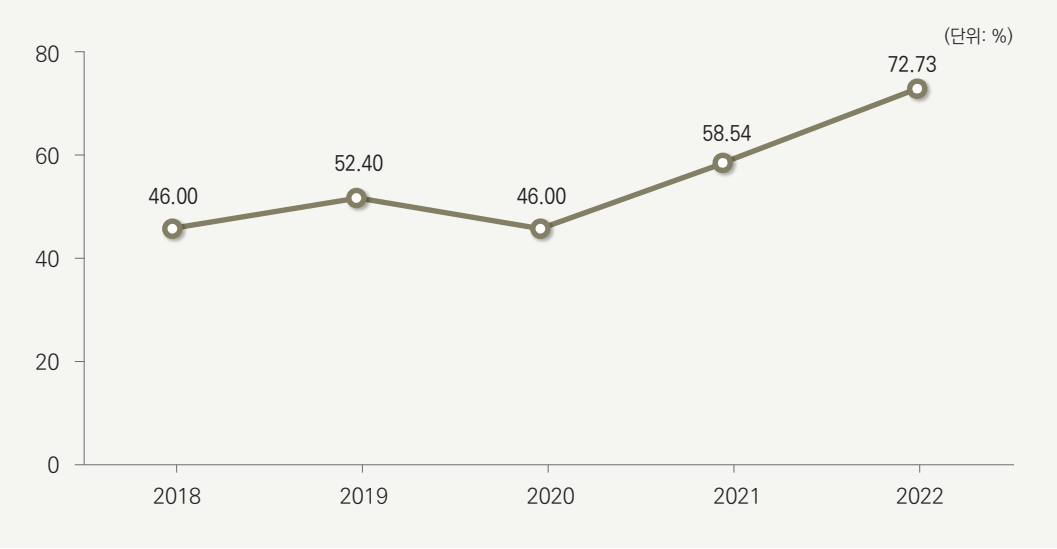
가 국가·공공부문

국가·공공부문 대상의 설문은 2023년 2월 수행하였으며, 총 99개 기관의 응답 결과를 활용하였다. 중앙행정기관 35곳, 지방자치단체 38곳, 공공기관 26곳이 설문에 응답하였다.

1. 정보보호 조직

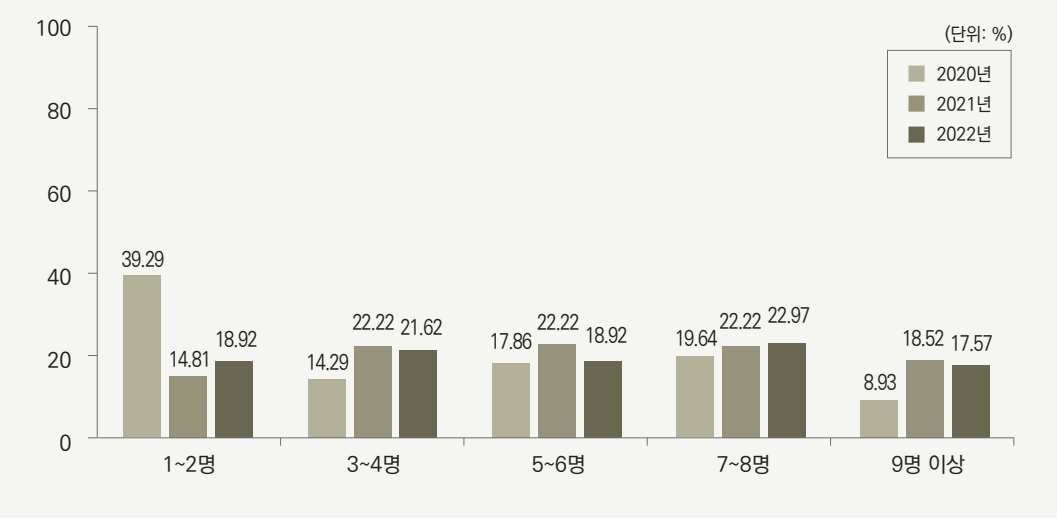
조사 기관 중 정보보호 전담부서를 운영하는 기관은 72.73%로 전년도 58.54%에 비하여 상승한 것으로 나타났다. 전담부서를 운영하지 않는 기관은 63.89%가 예산과 인력 부족, 22.22%는 기관장의 인식 부족을 사유로 꼽았다. 중앙행정기관은 약 50%가 정보보호 전담부서를 운영하지 않는 반면, 지방자치단체와 공공기관은 대부분이 전담부서를 운영 중이었다.

그림 부록 1-가-1 정보보호 전담부서 운영 현황



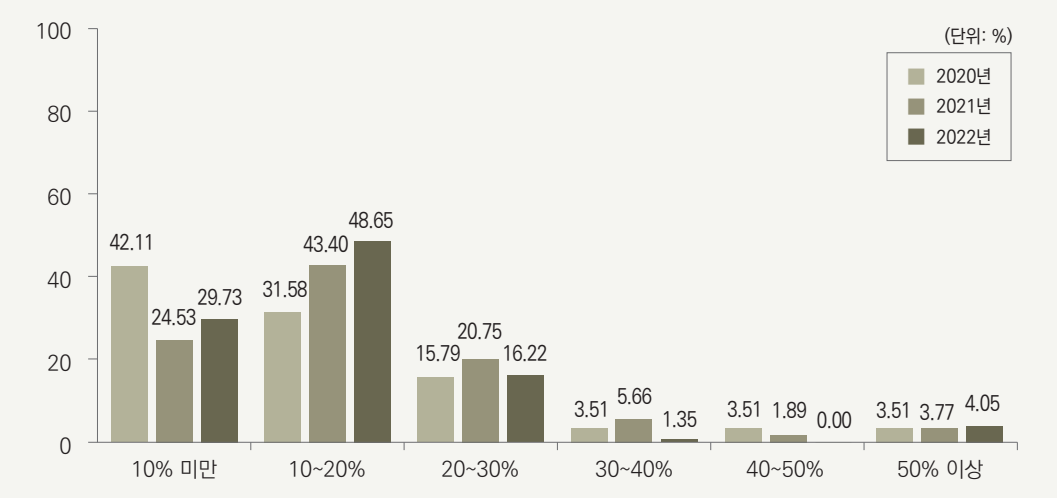
정보보호 전담부서가 있는 경우 해당 부서 인원이 2명 이하인 기관은 18.92%로 전년도에 비하여 다소 증가하였고, 5~6명이라고 답변한 기관은 18.92%로 소폭 감소하였으나, 전반적으로 볼 때 전담부서 인원 배정 현황은 전년도와 비슷한 분포를 보였다.

그림 부록 1-가-2 정보보호 전담부서 인원 수 현황



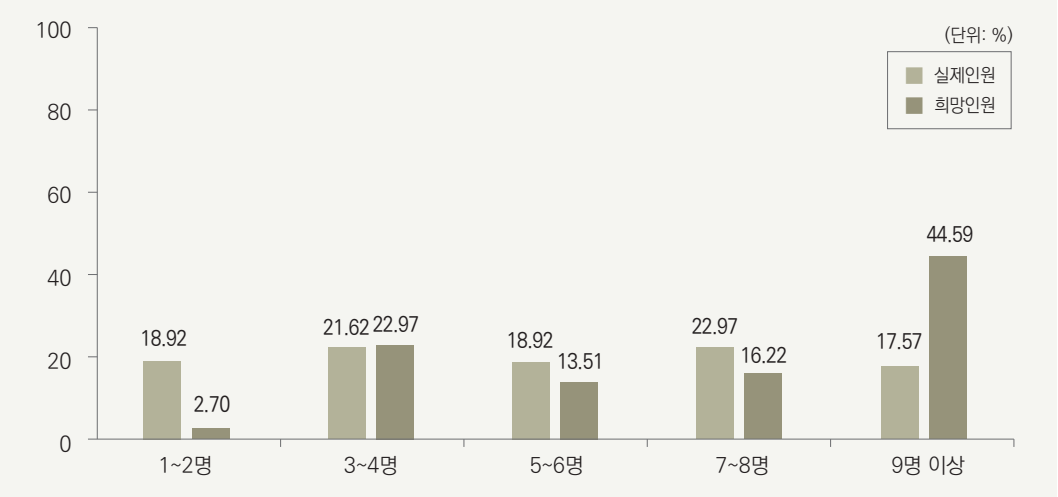
정보보호 전담조직의 절대적 구성원 수는 각 조직의 규모와 업무 특성에 따라 다를 수 있으나, 정보화 담당조직 인원 수에 비해서는 여전히 낮은 비율을 유지하고 있다. 전년도와 같이 정보화 담당조직 대비 정보보호 전담조직 인원 수는 30% 이하가 94.59%에 육박하고 있다.

그림 부록 1-가-3 정보화 담당조직 인원 수 대비 정보보호 전담조직 인원 수



정보보호 전담조직을 운영하는 기관이 희망하는 정보보호 전담인력 규모는 9명 이상이 44.59%로 전년도에 이어 가장 높게 나타났다. 이는 실제 운영 인력과 큰 차이를 보이는 것으로 여전히 현실과 큰 괴리가 있음을 드러냈다.

그림 부록 1-가-4 정보보호 전담부서 실제 구성인원과 희망 구성인원 비교



정보보호 전담부서 최상급자의 직급은 전년도와 마찬가지로 실무자급(공무원의 경우 5~6급)이 39.19%로 가장 높은 비율을 나타내었고, 관리자급(공무원의 경우 1~2급)도 22.97%로 전년도와 유사하게 조사되었다. 조사기관 범주별 최상급자 직급을 살펴보면 지방자치단체는 관리자급(공무원의 경우 1~2급)의 최상급자가 없으며, 실무자급(공무원의 경우 5~6급)의 비율이 가장 높았다. 공공기관은 가장 높은 비율(61.54%)로 관리자급(공무원의 경우 1~2급)을 정보보호 최상급자로 운영하고 있었다.

그림 부록 1-가-5 정보보호 전담부서 최상급자 직급

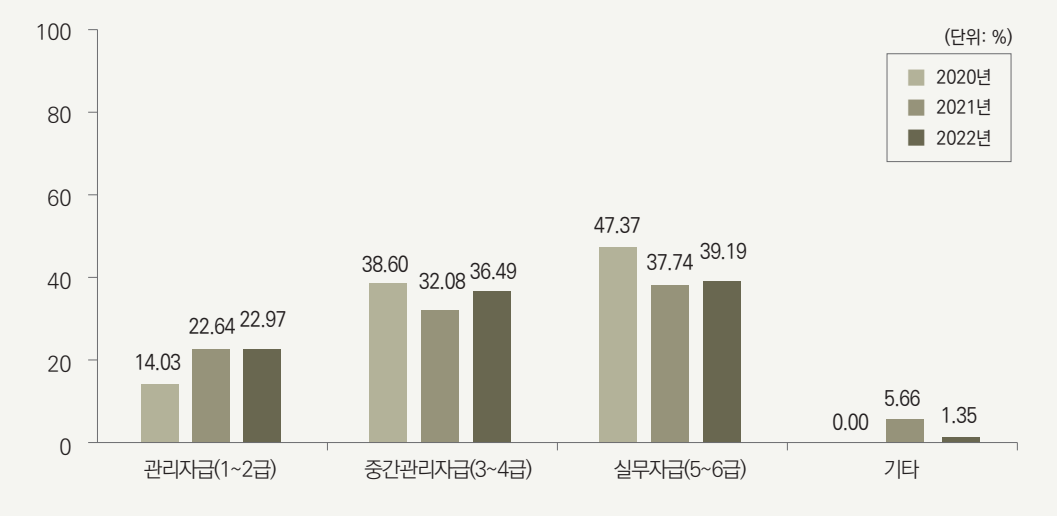
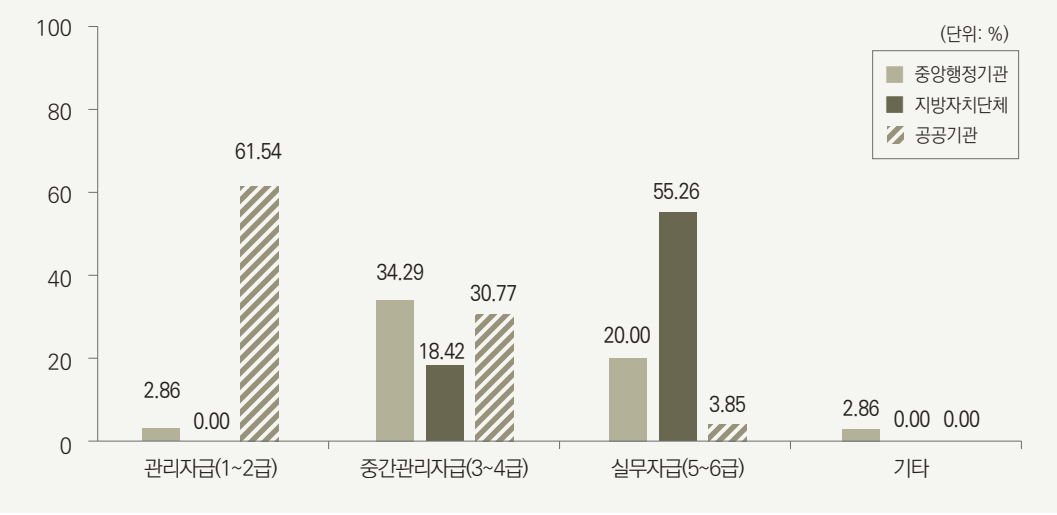
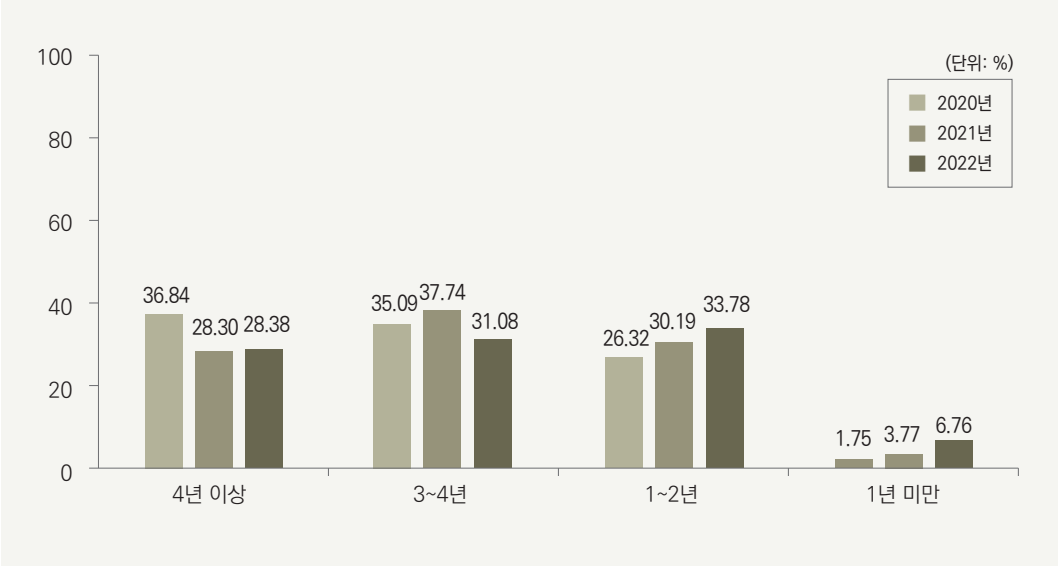


그림 부록 1-가-6 조사 대상 범주별 정보보호 최상급자 직급



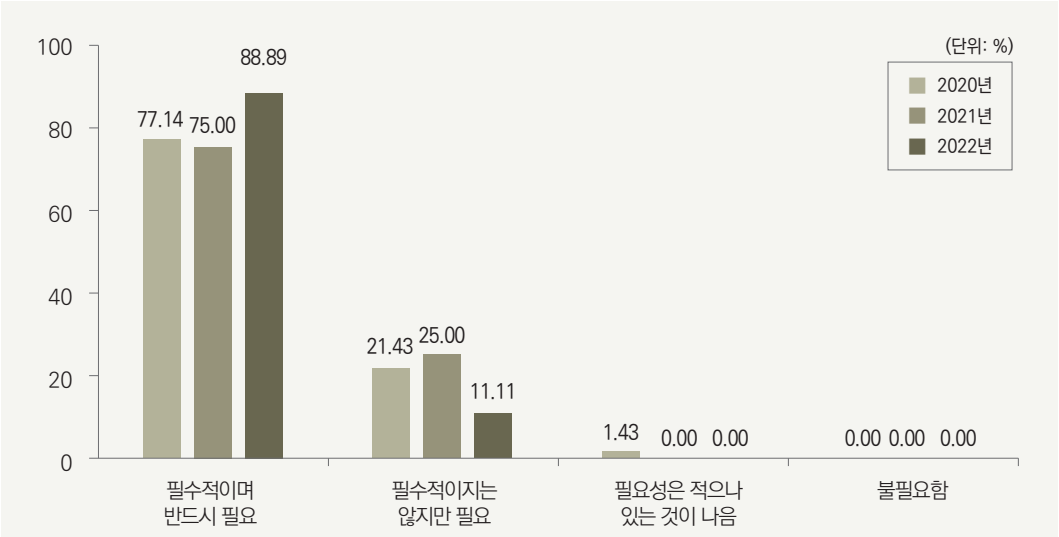
정보보호 전담인력의 해당 분야 평균 업무 경력은 1~2년인 경우가 33.78%로 가장 많은 것으로 조사되었고, 3~4년인 경우(31.08%)와 4년 이상(28.38%)이라는 답변도 유사한 비율로 조사되었다. 전년도에 비하여 1년 미만인 경우는 다소 증가한 수치인 6.76%에 이르는 것으로 조사되었는데, 이는 응답기관 중 중앙행정기관의 비율은 줄고 지방자치단체와 공공기관의 응답 비율은 높았기 때문인 것으로 보인다.

그림 부록 1-가-7 정보보호 전담인력의 해당 분야 평균 업무 경력



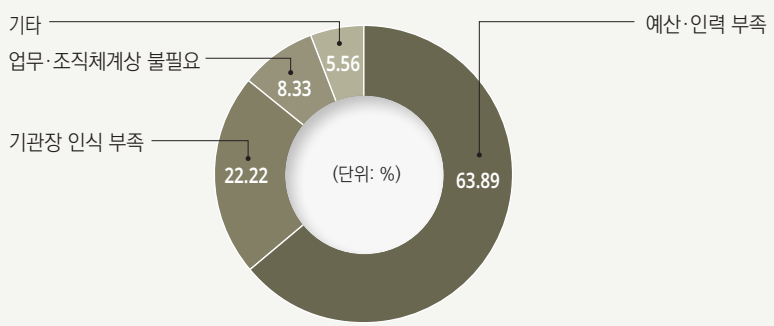
정보보호 전담조직이 없는 경우 전담조직의 필요성에 대해서는 응답기관 전부가 긍정적인 견해로, 88.89%는 조직 발전을 위하여 정보보호 전담부서가 반드시 필요하다는 견해였다.

그림 부록 1-가-8 정보보호 전담부서의 필요성



정보보호 전담조직이 신설되지 않는 이유로 63.89%는 예산·인력 부족, 22.22%는 기관장의 인식 부족을 꼽았다. 중앙행정기관의 경우 예산·인력 부족의 사유가 68.75%, 기관장 인식 부족이 18.75%를 나타낸 반면, 지방자치단체의 경우 기관장 인식 부족이 40%로 상대적으로 높은 비율을 차지하였다.

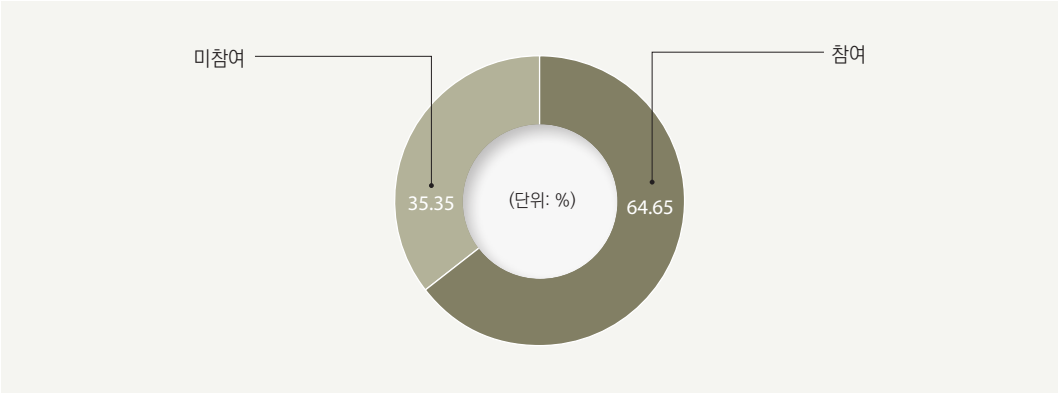
그림 부록 1-가-9 전담조직을 신설하지 않은 이유



2. 정보보안 책임 의식

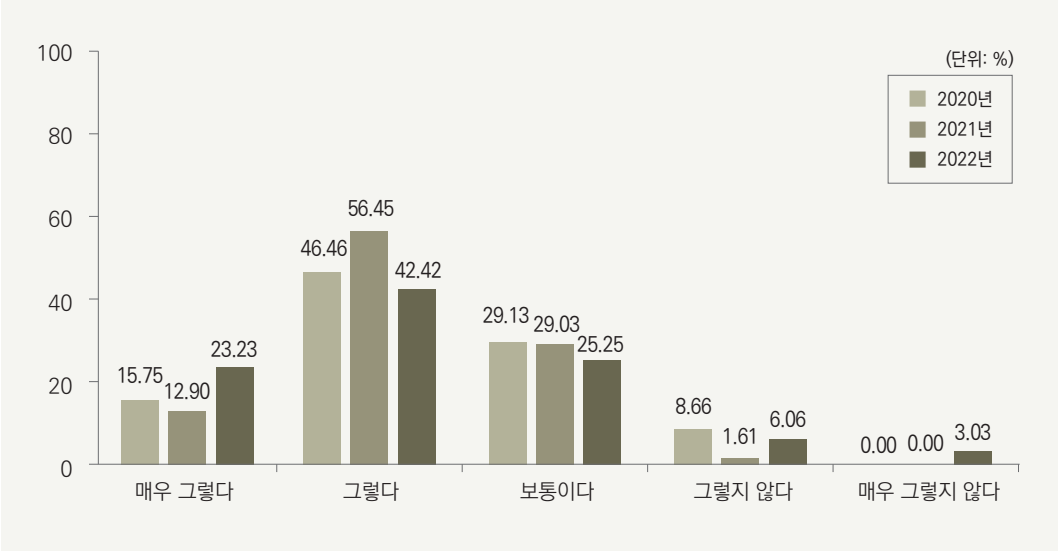
응답기관 중 64.65%의 기관에서 기관장이 정보보호 추진계획에 관심을 갖고 의사결정 과정에 직접적으로 참여한다고 답변하였는데, 공공기관은 84.62%에 이르는 것으로 조사되었다.

그림 부록 1-가-10 기관장의 정보보호 계획 결정 참여 여부



직원이 공지된 정보보호 정책과 규정을 준수하고, 위반할 경우 반드시 책임을 져야 하는지에 대해서는 매우 그렇다는 응답이 23.23%, 그렇다는 응답이 42.42%로, 65.65%가 위반 책임 부담의 필요성을 인식하는 것으로 나타났다.

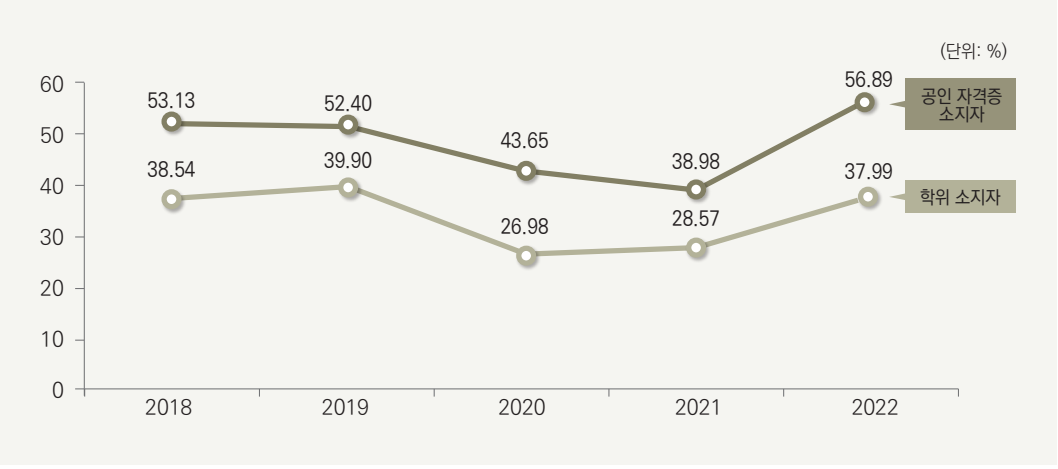
그림 부록 1-가-11 직원의 정보보호 정책·규정 준수 및 위반 책임 부담 필요성



3. 정보보호 인력 역량

정보보호 업무를 수행하는 인원의 전문성을 파악하기 위하여 관련 전공의 석사 학위 이상 소지자 또는 정보보안기사·CISSP·CISA 등 정보보호 관련 공인 자격증 소지자의 비율을 조사하였다. 석사 이상의 정보보호 관련 학위 소지자가 있는 기관은 37.99%였으며, 정보보호 관련 공인 자격증 소지자가 있는 기관은 56.89%로 조사되었다. 이는 전년도에 비하여 증가한 수치였고, 관련 학위 및 자격증을 모두 소지한 인력이 있는 기관도 34.34%로 조사되어 전년도 18.9%에 비하여 상승한 수치를 보였다.

그림 부록 1-가-12 정보보호 관련 학위 및 공인 자격증 소지자 현황



4. 정보보호 교육 현황

정보보안 담당자에 대한 전문교육과 일반 임직원에 대한 정보보호 직무교육 실시 여부와 형태를 조사하였다.

대다수(약 99%)의 기관이 정보보안 담당자 및 일반 임직원 모두를 대상으로 관련 교육을 실시하고 있었으며, 이 중 과반 이상인 70.71%가 이수 시간 또는 성적을 인사고과 등 평가에 반영하는 것으로 조사되었다.

다만 정보보안 담당자 대상 전문교육의 의무 실시 비율(70.71%)이 일반 임직원 대상 직무교육의 의무 실시 비율(77.78%)에 비하여 다소 낮은 상태를 유지하고 있다.

그림 부록 1-가-13 정보보안 담당자 전문교육 실시 현황

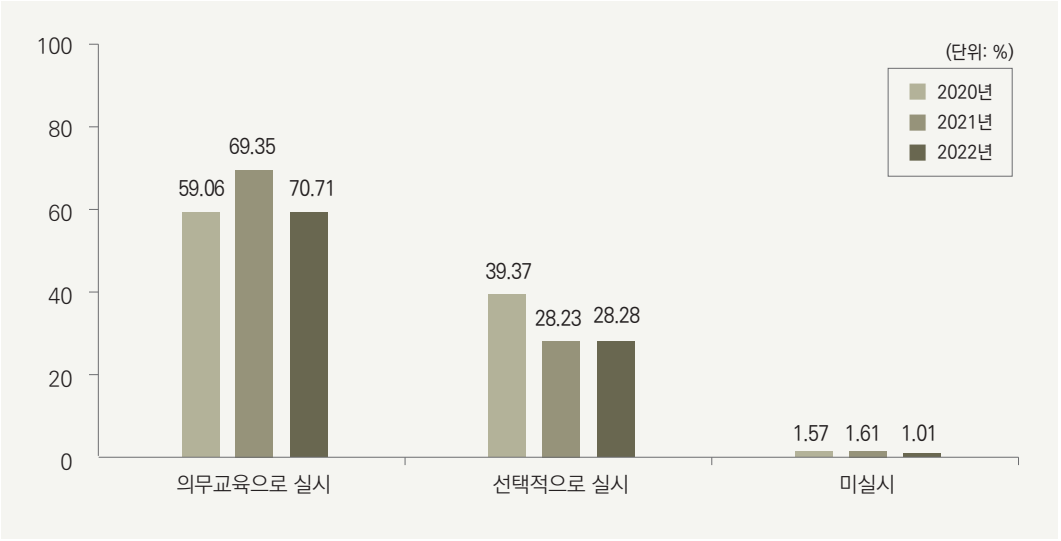
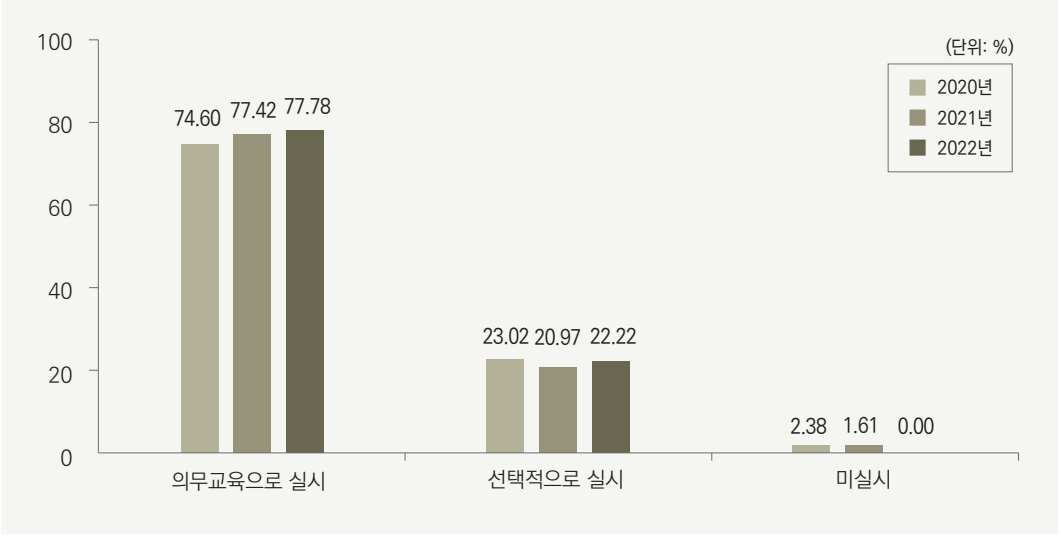
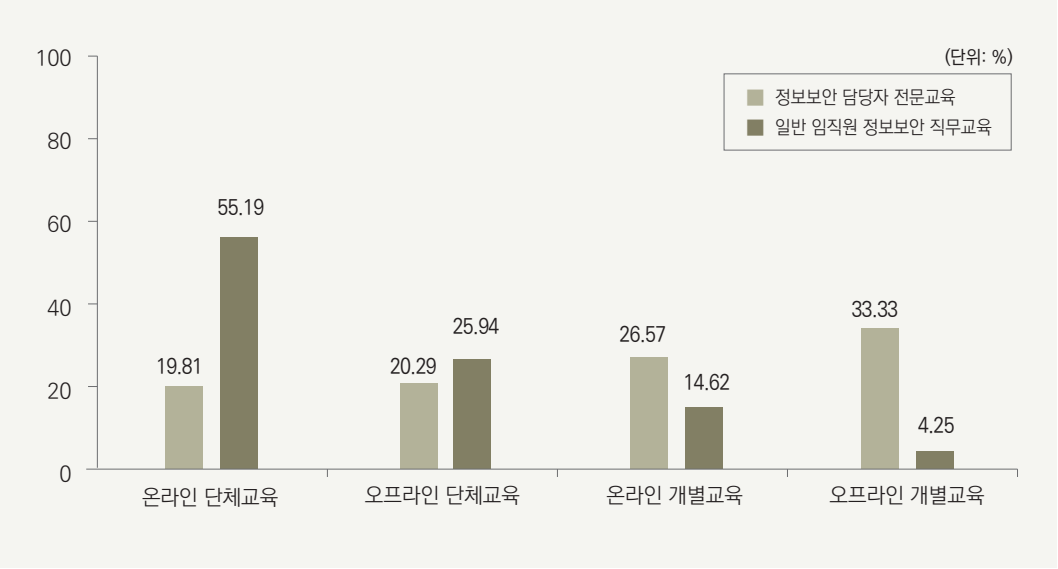


그림 부록 1-가-14 일반 임직원에 대한 정보보안 직무교육 실시 현황



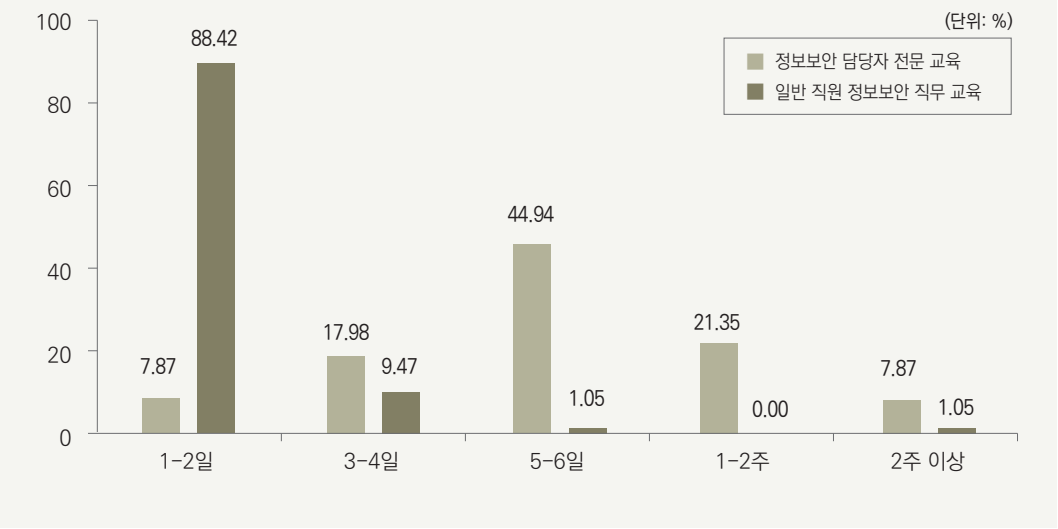
일반 임직원 대상의 정보보안 직무교육은 온라인 69.81%, 오프라인 30.19%로, 이 중 개별교육(18.87%)보다는 단체교육(81.13%) 형태가 높은 비율을 나타냈다. 반면, 정보보안 담당자 전문교육은 온·오프라인 개별교육 형태가 과반 이상(59.9%)의 비율로 운영되고 있었다.

그림 부록 1-가-15 교육 운영 형태



연간 교육일수는 일반 직무교육의 경우 연간 2일 이하로 이루어지는 비율이 88.42%로 대다수를 차지하였다. 반면, 정보보안 담당자에 대한 1주 이상의 전문 교육은 29.22%, 5~6일은 44.94%로 일반 임직원을 대상으로 하는 교육보다 기간이 긴 것으로 조사되었다.

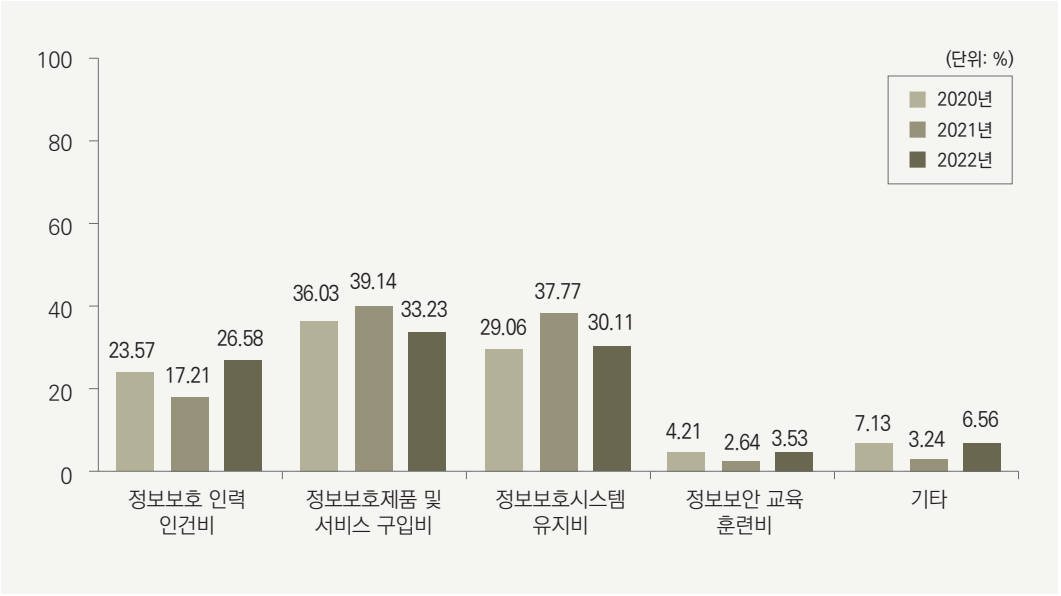
그림 부록 1-가-16 교육 일수 현황



5. 정보보호 예산

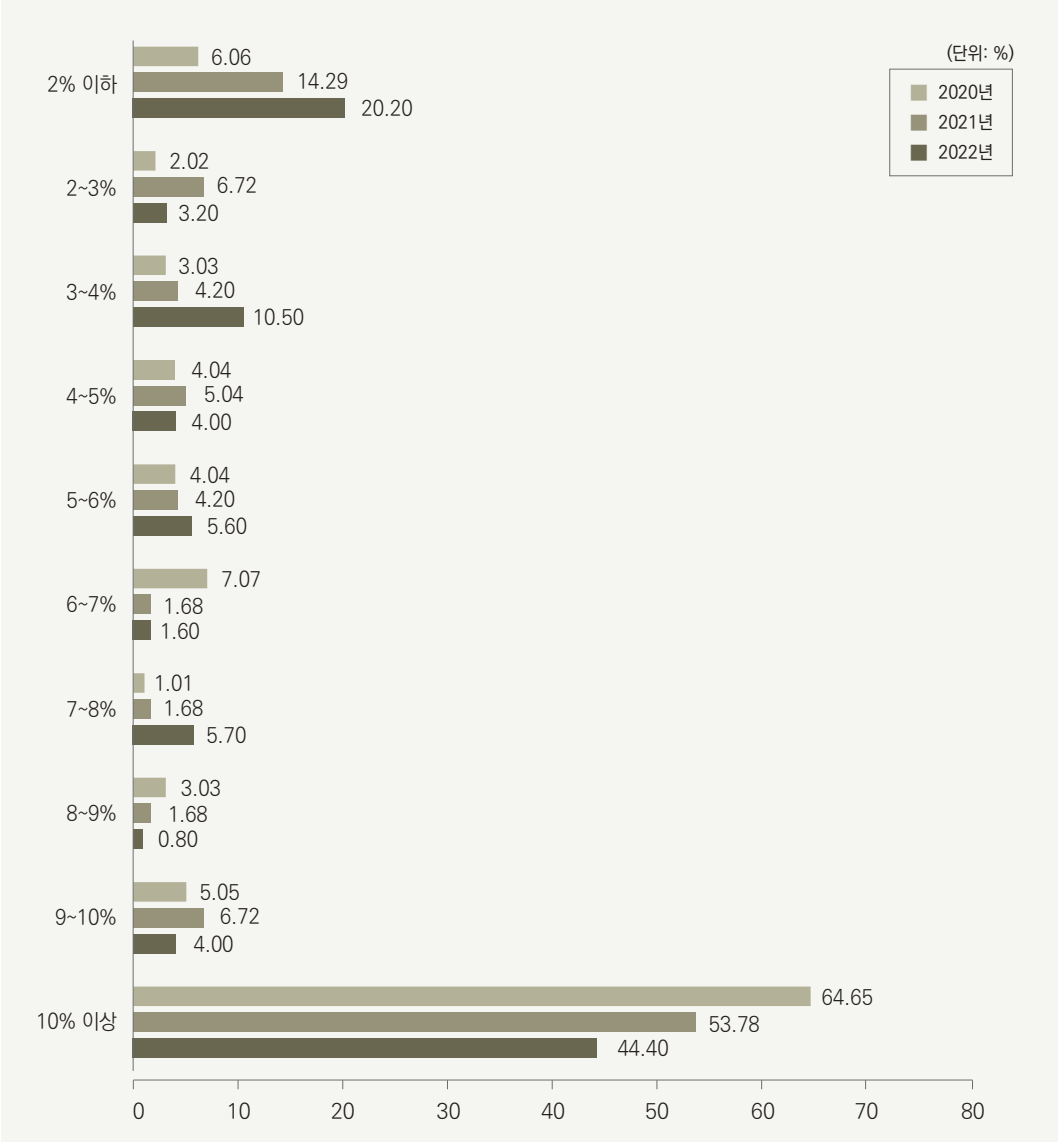
정보보호 예산이 가장 많이 사용되는 분야로는 정보보호제품 및 서비스 구입이 33.23%로 전년도와 같이 가장 높은 비율을 차지하였다. 이어 정보보호시스템 유지비가 30.11%, 정보보호 인력 인건비가 26.58%로, 전년도에 비하여 인건비에 투입된 예산 비율이 높게 조사되었다.

그림 부록 1-가-17 기관별 정보보호 예산 용도



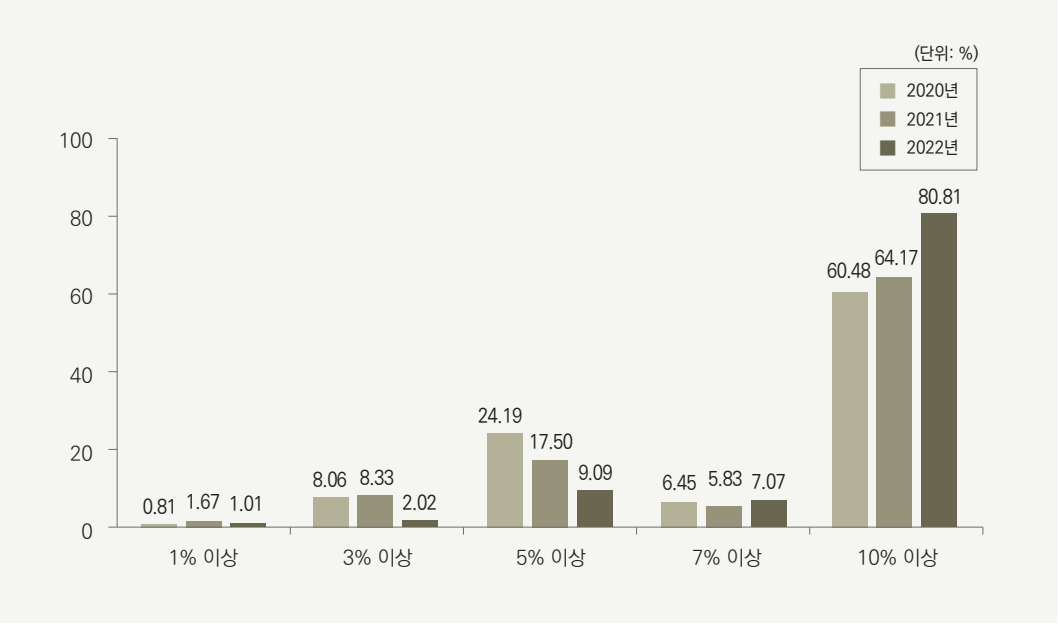
정보화 예산 대비 정보보호 예산 비율은 10% 이상인 기관이 64.65%로 가장 많았고, 전년도에 비하여 10.87% 증가하였다. 또한 2% 이하로 편성한 기관의 수가 전년도에 비하여 8.23% 감소한 6.06%로 나타나 투입 예산 비율이 증가한 것으로 확인되었다.

그림 부록 1-가-18 정보화 예산 대비 정보보호 예산 비율 변화



희망하는 정보화 예산 대비 정보보호 예산 비율을 조사한 결과, 전년도보다 16.64% 증가한 80.81%의 기관이 10% 이상이 적정하다고 응답하였다. 이어서 5% 이상이 9.09%, 7% 이상이라는 응답은 7.07%로 나타났다.

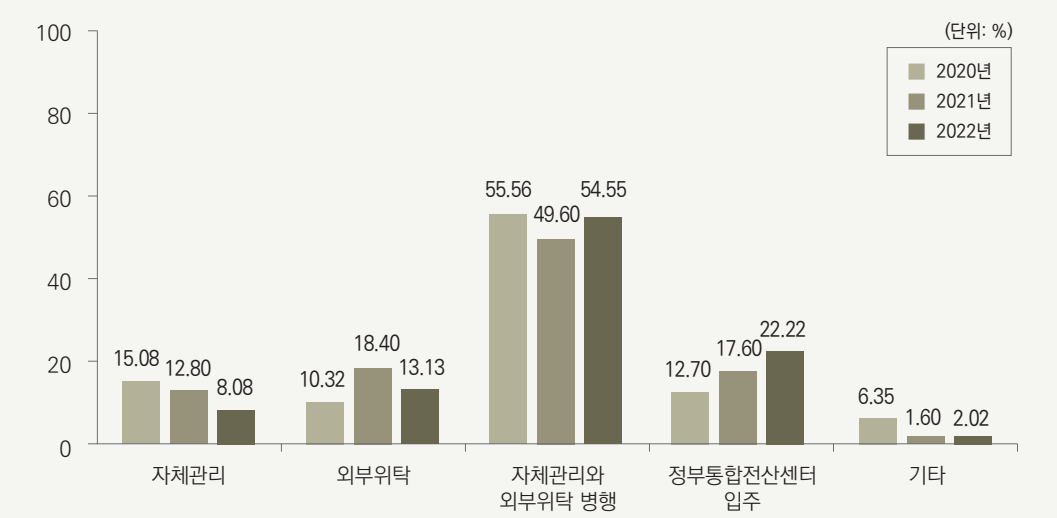
그림 부록 1-가-19 정보화 예산 대비 정보보호 예산 희망 비율



6. 정보시스템 운영·관리 형태 및 외부인력 보안

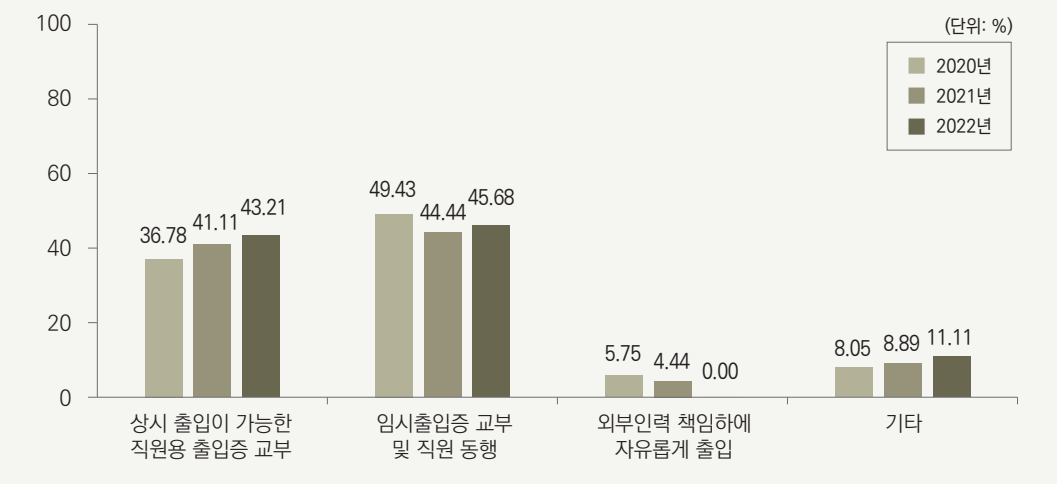
각 기관의 홈페이지·서버 등 주요 정보시스템 운영·관리 방법을 조사한 결과, '자체관리와 외부위탁 병행'이 54.55%를 차지하여 가장 많은 것으로 나타났다. 전적으로 외부업체에 위탁하는 경우는 13.13%로 전년도에 비하여 감소하였으며, 자체관리 비율도 8.08%로 약간 감소하였다. 중앙행정기관의 경우 지방자치단체나 공공기관과는 달리 과반 이상(60%)이 정부통합전산센터에 입주하여 있고, 자체적으로 관리하고 있다고 답변한 기관은 없었다.

그림 부록 1-가-20 주요정보시스템 운영·관리 방법



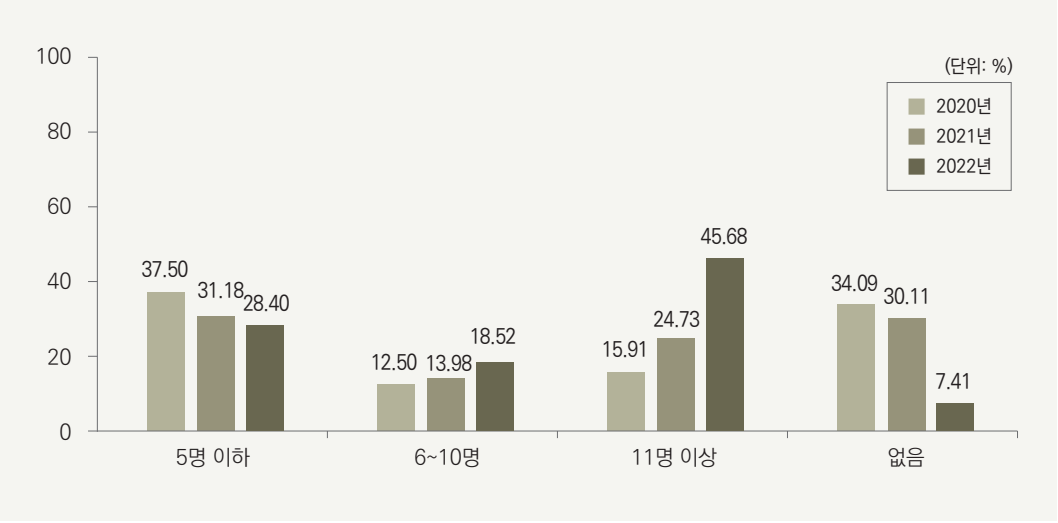
정보시스템 운영·관리에 외부업체를 이용하는 경우 45.68%의 기관이 임시출입증을 교부하고 직원이 동행하는 것으로 조사되었다. 특히 지방자치단체의 60%와 공공기관의 57.69%가 해당 출입관리 방식을 채택하고 있었다. 이어서 상시 출입이 가능하도록 직원용 출입증을 교부하는 경우가 43.21%로 전년도에 비하여 소폭 증가하였는데, 중앙행정기관의 경우 90%가 해당 방식으로 운영하고 있었다. 보안에 취약한 방식인 외부인력 책임하에 자유로운 출입을 허가하고 있다고 답변한 기관은 없는 것으로 조사되었다.

그림 부록 1-가-21 외부인력 출입관리 방법



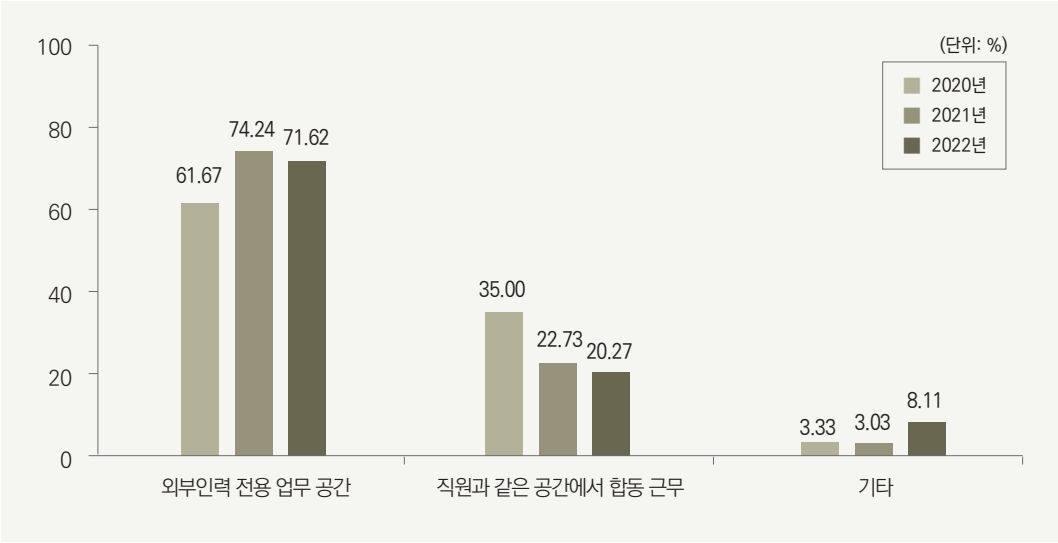
상주하는 외부인력의 수는 11명 이상인 기관이 45.68%로 가장 많았고, 5명 이하는 28.4%, 6~10명은 18.52%로 조사되었다. 전년도와 비교하면 11명 이상인 기관의 증가 폭이 컸고, 상주인원이 없다고 응답한 기관은 7.41%로 대폭 감소하였다.

그림 부록 1-가-22 정보시스템 운영·관리 상주 외부인력 수



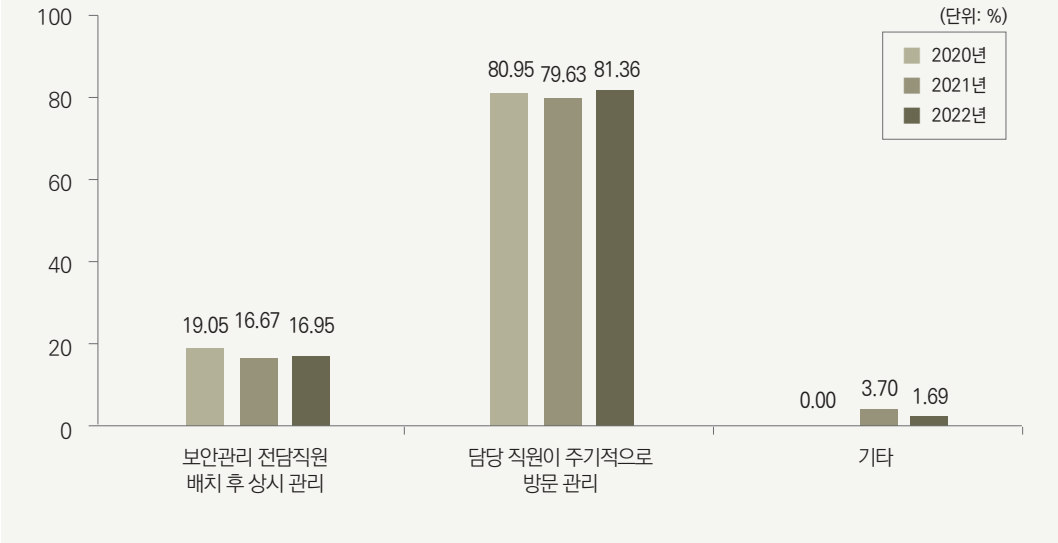
상주하는 외부인력이 있는 경우 해당 인력의 근무 장소가 외부인력 전용 업무 공간이라고 답변한 비율은 71.62%로 전년도와 마찬가지로 가장 많았고, 직원과 같은 공간에서 합동 근무를 한다는 응답은 20.27%로 조사되었다. 기타(8.11%) 외부인력 전용은 아니나 별도 사무실을 운영한다는 의견이 있었음을 감안할 때 80%에 가까운 기관이 보안을 위한 별도 공간을 활용하고 있는 것으로 나타났다.

그림 부록 1-가-23 상주 외부인력 근무 장소



상주하는 외부인력이 전용 사무실에서 근무하는 경우 담당직원이 주기적으로 방문 관리하는 경우가 81.36%로 가장 많았고, 보안관리 전담직원 배치 후 상시 관리를 수행한다는 기관의 비율은 16.95%로 전체적으로 전년도와 비슷한 분포를 보였다.

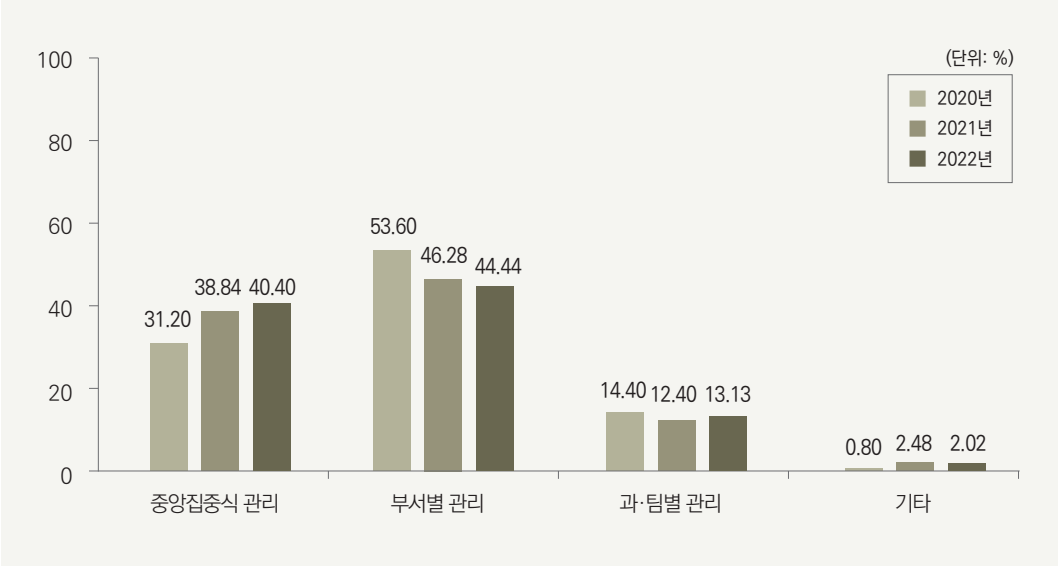
그림 부록 1-가-24 상주 외부인력 보안관리 방법



7. 휴대용 정보통신기기 관리

노트북 등 휴대용 정보통신기기 관리 방법은 부서별 관리가 44.44%로 가장 많은 비율을 차지하였으며, 이는 전년도 대비 소폭 하락한 수치이다. 반면, 정보보안 담당자 또는 정보화 담당자의 중앙집중식 관리 방식을 취하는 기관은 40.4%로 전년도에 비하여 소폭 상승하였다.

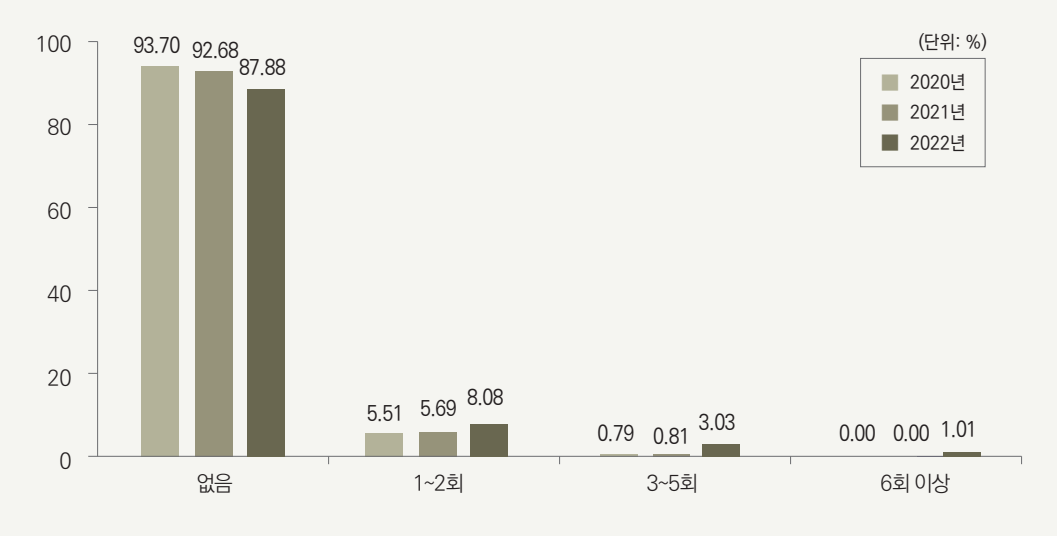
그림 부록 1-가-25 휴대용 정보통신기기 관리 방법



8. 사이버공격 대응 준비

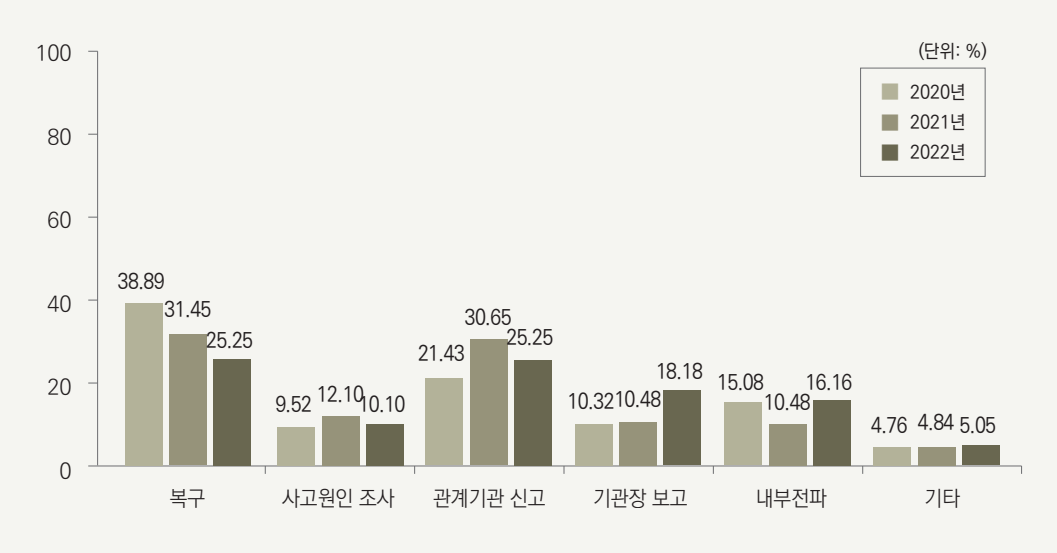
설문에 참여한 대부분의 기관(87.88%)이 2022년 사이버공격으로 인한 피해가 없었던 것으로 응답하였다. 1~2회(8.08%)와 3~5회(3.03%) 등 피해를 받은 기관의 비율도 낮게 조사되었지만, 최근 3년간 추이를 보면 피해를 입는 기관이 소폭 증가 추세에 있음을 알 수 있다.

그림 부록 1-가-26 연간 사이버공격 피해 발생 횟수



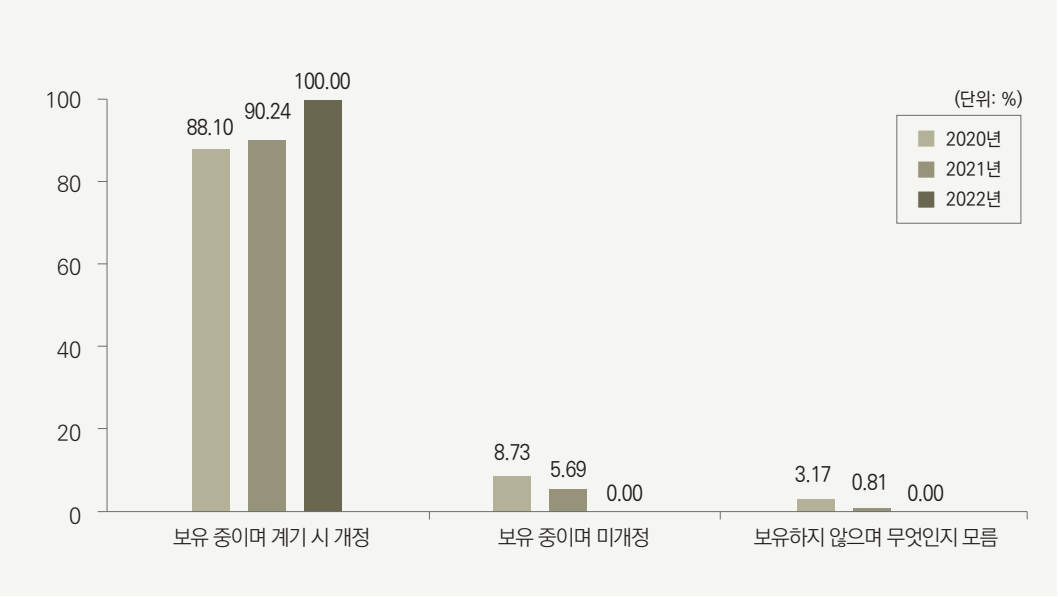
사고 발생 시 가장 긴급한 활동 우선순위는 복구(25.25%) = 관계기관 신고(25.25%) > 기관장 보고(18.18%) > 내부전파(16.16%) > 사고 원인 조사(10.1%) 순으로 나타났다. 이 밖에 피해확산을 방지하기 위한 초동조치(네트워크 분리 등)가 긴요하다는 의견도 5.05% 가량 있었다.

그림 부록 1-가-27 사고 발생 시 가장 긴급한 활동



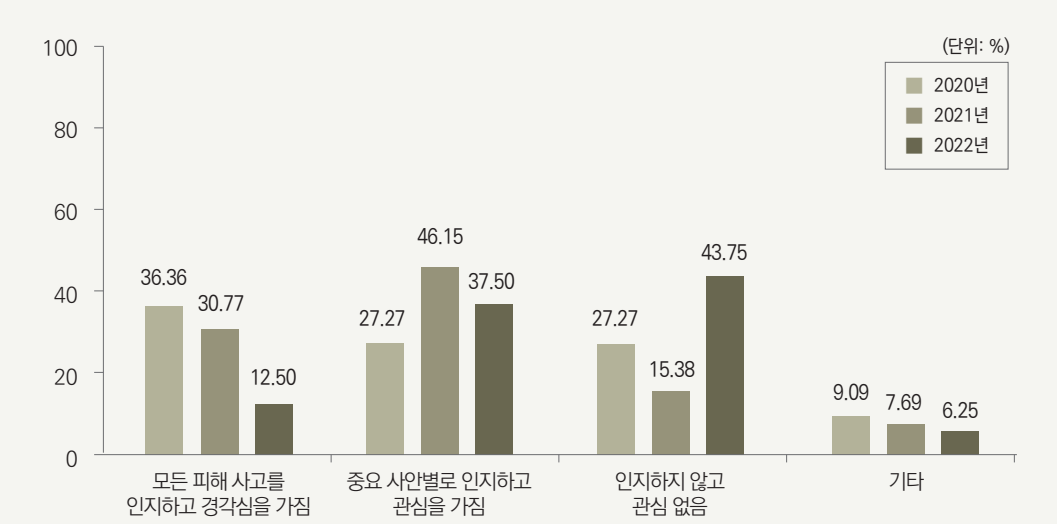
사이버 분야의 각종 지침·규정을 참조한 위기대응매뉴얼 제작·보유 현황에 대한 조사에서는 모든 기관이 이를 보유 중이며, 계기 때마다 개정하고 있다고 응답하였다.

그림 부록 1-가-28 사이버분야 위기대응매뉴얼 제작·보유 현황



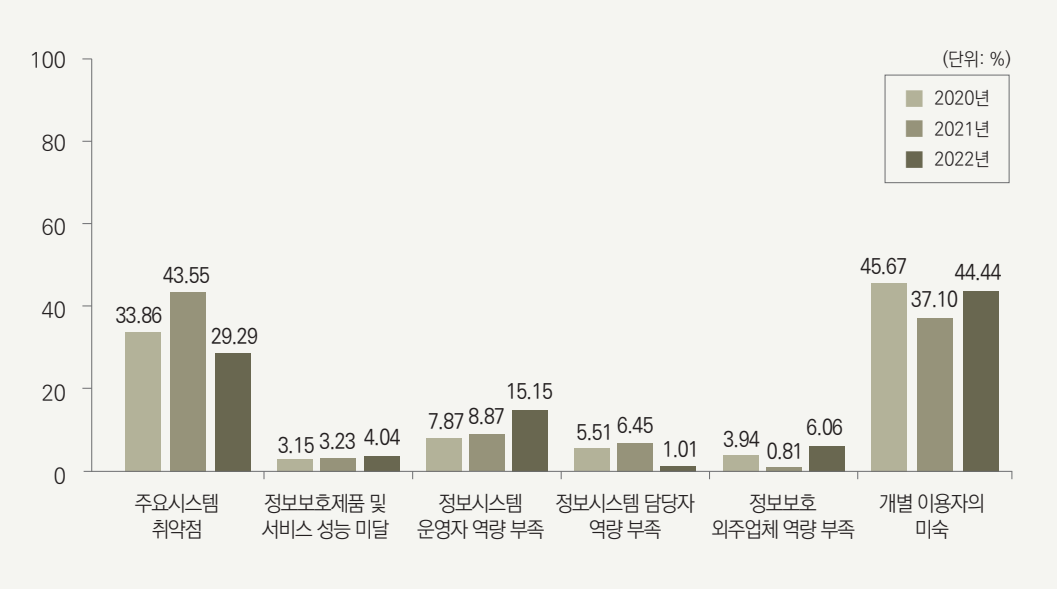
사이버공격으로 피해가 발생한 사례가 있는 기관의 경우 50%의 기관에서 일반 직원이 이를 인지하고 있는 것으로 답변하였는데, 이는 전년도보다 낮은 수치로, 일반 직원이 잘 모르고 있거나 관심도 없다고 답변한 비율도 28.37% 증가한 43.75%에 이르렀다.

그림 부록 1-가-29 일반 직원의 피해 발생 인지 수준



보안 사고 발생의 핵심 원인으로 44.44%의 기관이 개별 이용자의 미숙을 꼽아, 인적보안의 중요성을 인식하고 있는 것으로 조사되었다. 주요시스템 취약점은 29.29%, 정보시스템 운영자의 역량 부족은 15.15%의 기관에서 핵심 원인이라고 답변하였다.

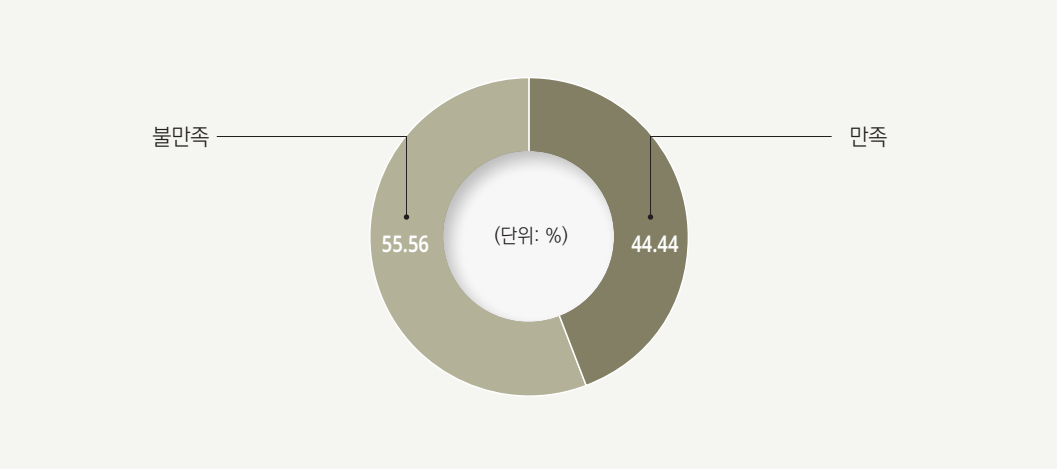
그림 부록 1-가-30 보안 사고 발생의 핵심 원인



9. 정보보호 업무수행 환경

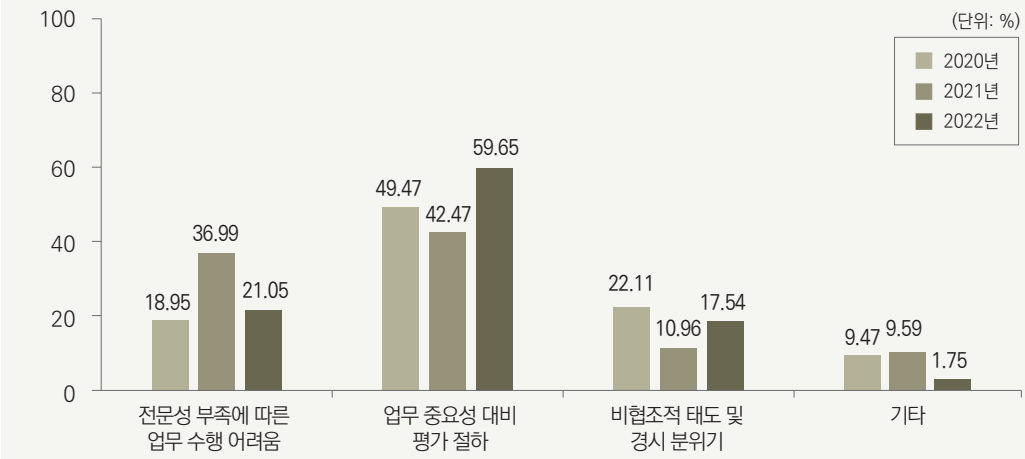
정보보안 담당자 중 55.56%가 업무에 만족하지 않고 있는 것으로 나타났다. 이는 전년도 대비 2.98% 감소한 수치이다.

그림 부록 1-가-31 정보보호 업무 만족 여부



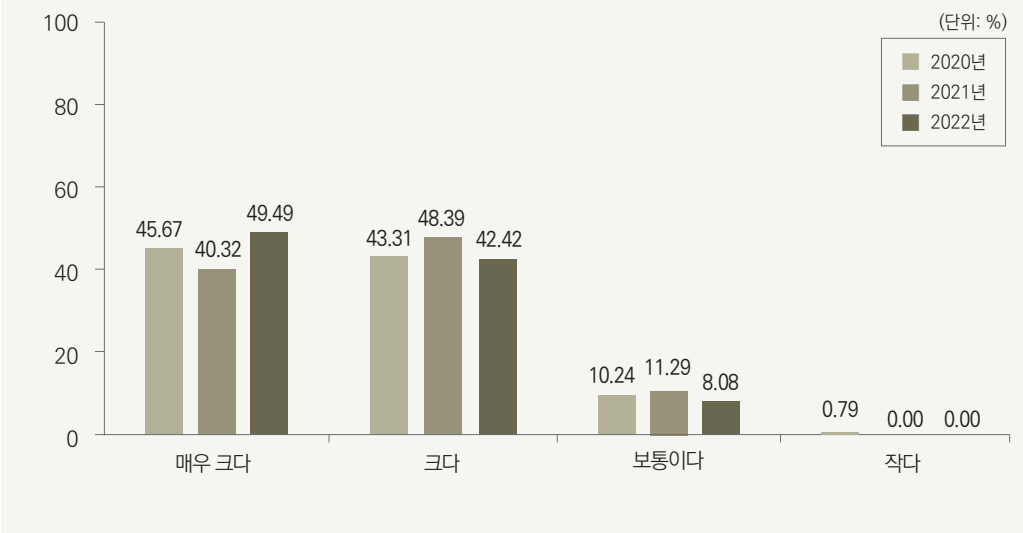
정보보안 담당자가 업무에 만족하지 못하는 이유 중 업무 중요성 대비 평가절하가 59.65%로 가장 높은 비율을 차지하였다. 이어 전문성 부족에 따른 업무수행 어려움이 21.05%, 비협조적 태도와 경시 분위기가 17.54%로 나타났다. 개인의 전문성 부족에 따른 불만족은 감소한 반면, 정보보안 업무수행 환경과 관련한 불만족은 53.43%에서 77.19%로 증가한 것으로 조사되어 개선이 필요한 상황임을 시사하고 있다.

그림 부록 1-가-32 정보보호 업무 불만족 사유



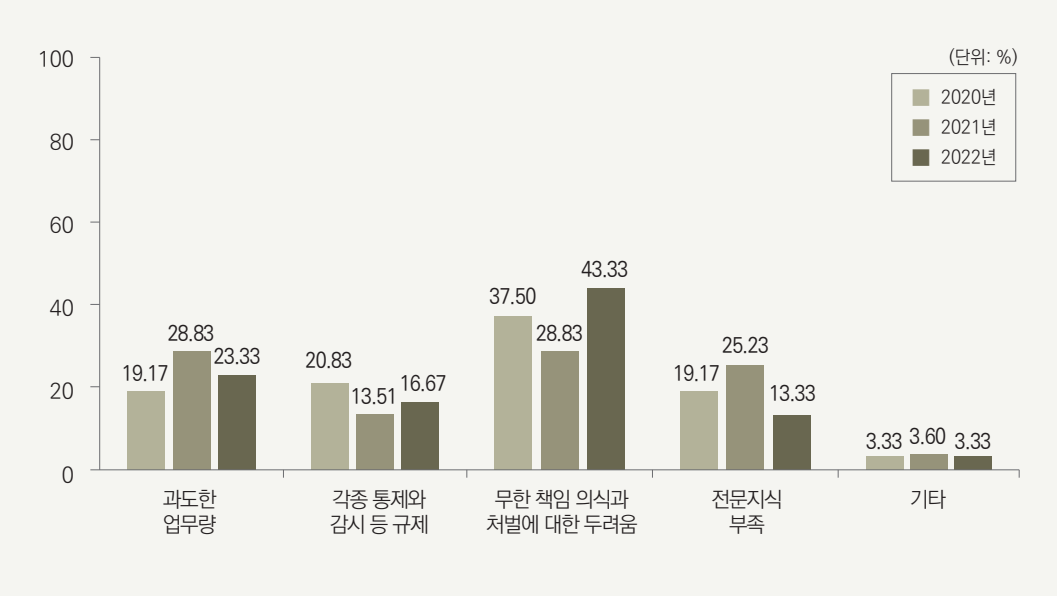
일반적인 다른 업무에 비하여 정보보호 담당자로서 업무 부담이 더 크다고 답변한 기관의 비율은 91.91%로, 전년도에 이어 압도적인 수치를 보여 준다. 다른 업무에 비하여 부담감이 작다는 응답은 없었다.

그림 부록 1-가-33 정보보안 담당자의 상대적 부담감



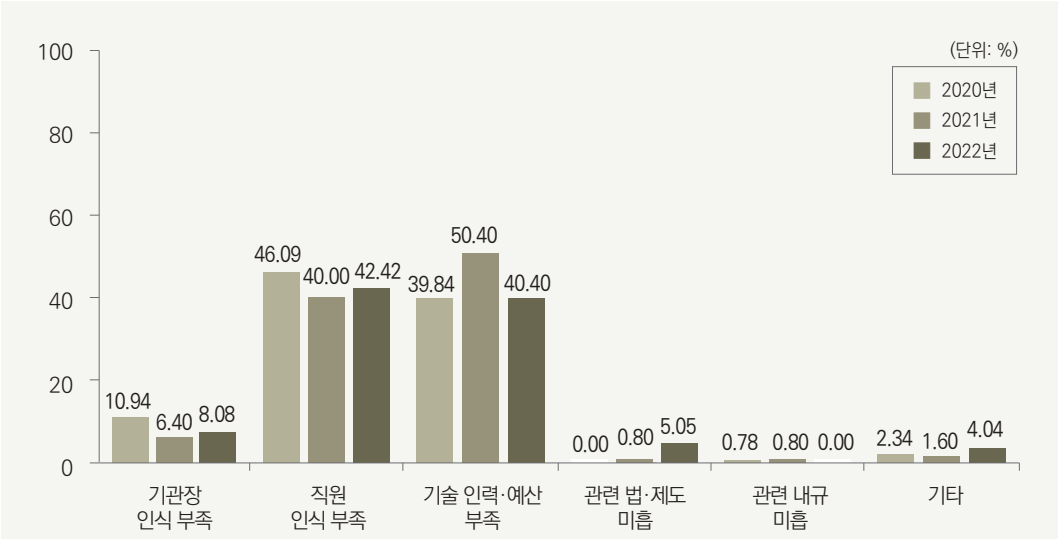
정보보호 담당 업무의 상대적 부담감이 더 크다고 답변한 경우 업무에 대한 무한 책임 의식과 처벌에 대한 두려움을 43.33%의 기관에서 주요 원인으로 꼽았다. 이는 해마다 지속적으로 가장 높은 순위를 차지하는 원인인데, 2022년에는 특히 많은 기관에서 원인으로 응답하였다. 반면, 전문지식 부재를 원인으로 꼽은 기관은 13.33%로 전년도에 비하여 대폭 감소하였다.

그림 부록 1-가-34 정보보호 담당자의 업무 부담감 발생 사유



정보보호 업무수행 중 애로 사항으로는 직원들의 인식 부족과 기술 인력·예산 부족이 각각 42.42%와 40.4%로 큰 비중을 차지하였다. 특이점은 이전 조사에서는 관련 법·제도가 미흡하다는 의견의 거의 없었으나, 이번에는 5.05%의 기관에서 관련 법·제도가 미흡하여 업무수행 시 어려움이 있다고 답변하였다.

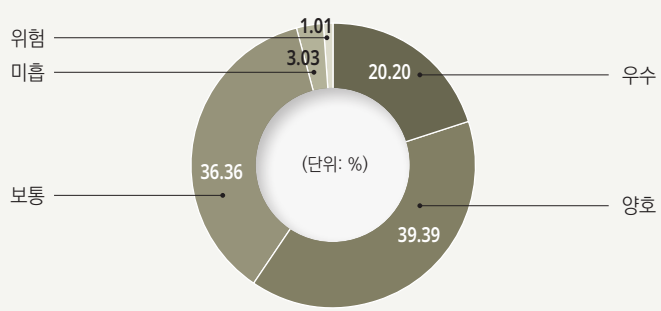
그림 부록 1-가-35 정보보호 업무수행 애로 사항



10. 정보보호 수준 및 취약점

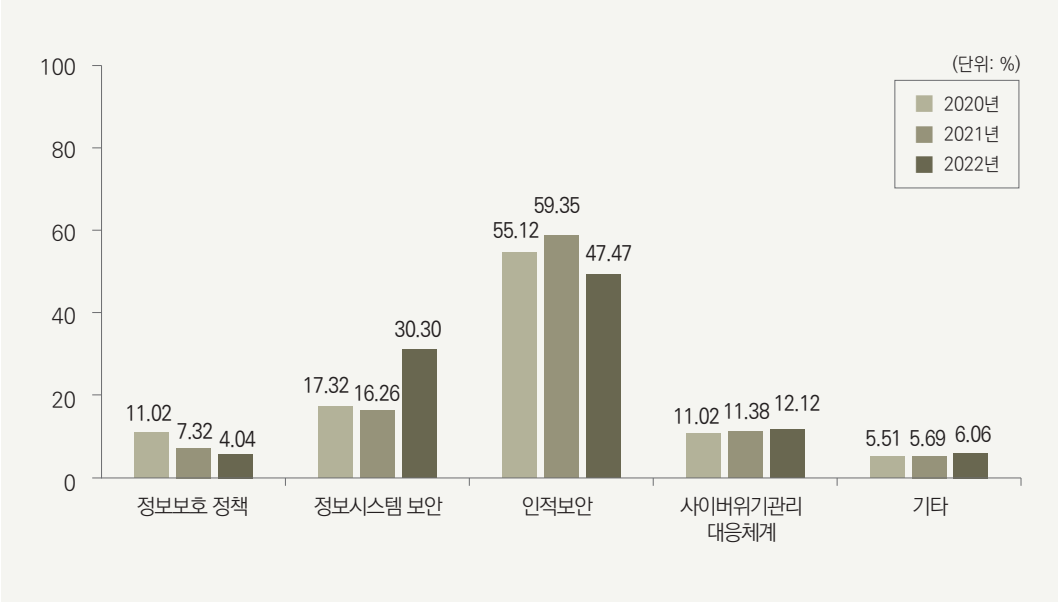
소속기관의 정보보호 수준을 자체 평가한 결과, 양호하다는 응답이 39.39%로 가장 높은 비율을 차지하였다. 이어 보통이라는 응답이 36.36%, 우수라는 응답이 20.2%로 조사되어 전년도와 비슷한 분포를 보였다.

그림 부록 1-가-36 소속기관 정보보호 수준 자체평가



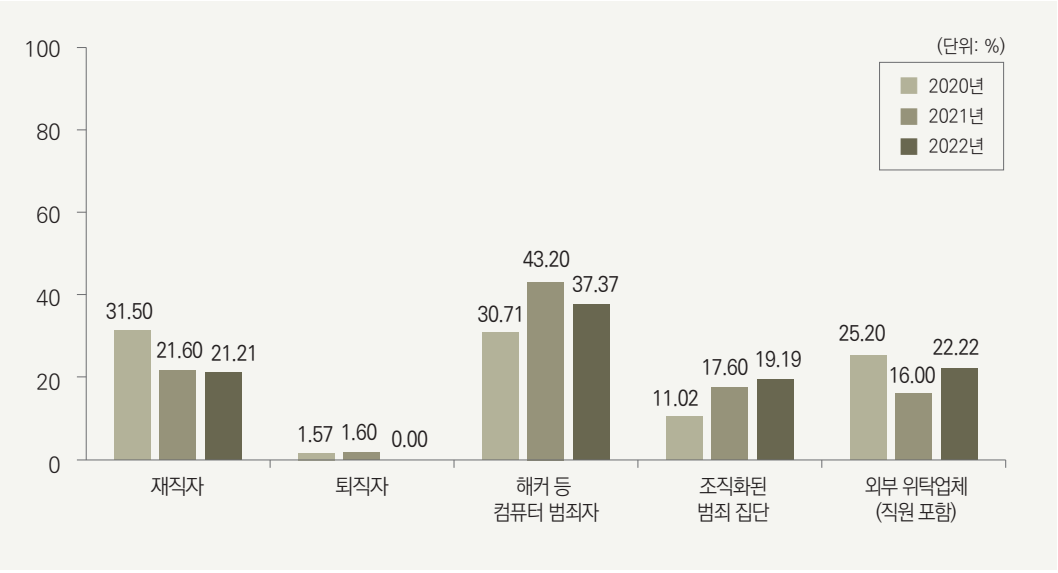
각 기관이 가장 취약하다고 생각하는 정보보호 분야로는 47.47%가 내·외부 인원 관리 등 인적보안이라고 응답하였다. 이어서 정보시스템 보안 30.3%, 사이버위기 관리 대응 체계 12.12%, 정보보호 정책 4.04% 등이 뒤를 이었다. 전년도에 비하여 정보시스템 보안이 취약하다고 답변한 비율은 증가하였고, 인적보안을 문제로 본 기관은 감소하였다. 기타 의견으로 복수의 기관에서 정보보호 전담인력 부족, 전담부서 부재 등을 꼽았다.

그림 부록 1-가-37 소속기관이 가장 취약한 정보보호 분야



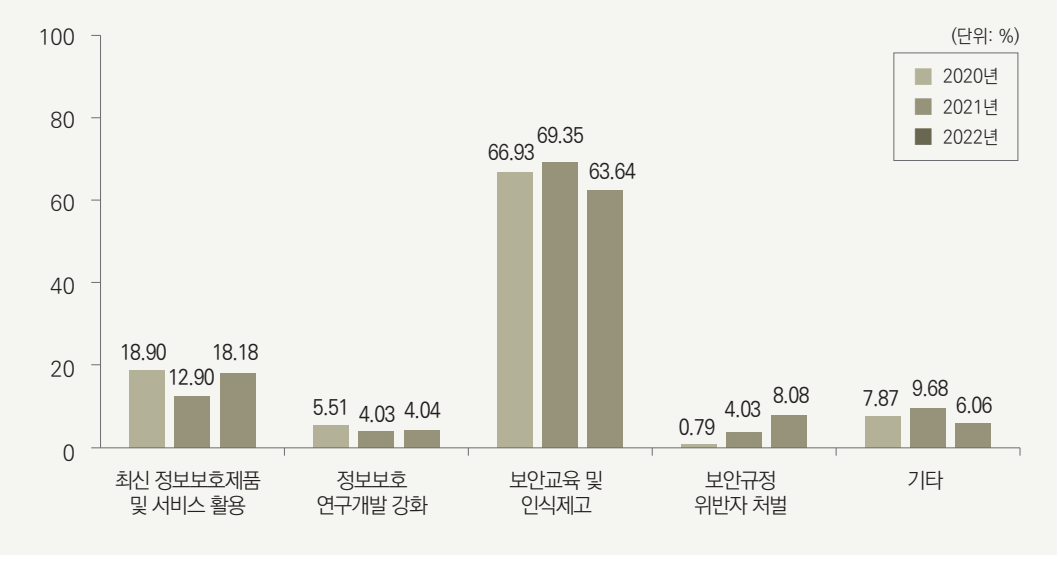
각 기관이 우려하는 정보보호 위협요인에 대한 응답은 해커 등 컴퓨터 범죄자가 37.37%로 전년도에 이어 가장 높은 비율을 차지하였다. 외부 위탁업체 22.22%, 조직화된 범죄집단이라고 응답한 기관도 19.19%에 이르러 내부자로부터의 위협보다 외부 해킹에 대한 관심도가 높은 것으로 조사되었다.

그림 부록 1-가-38 기관별 가장 우려되는 정보보호 위협요인



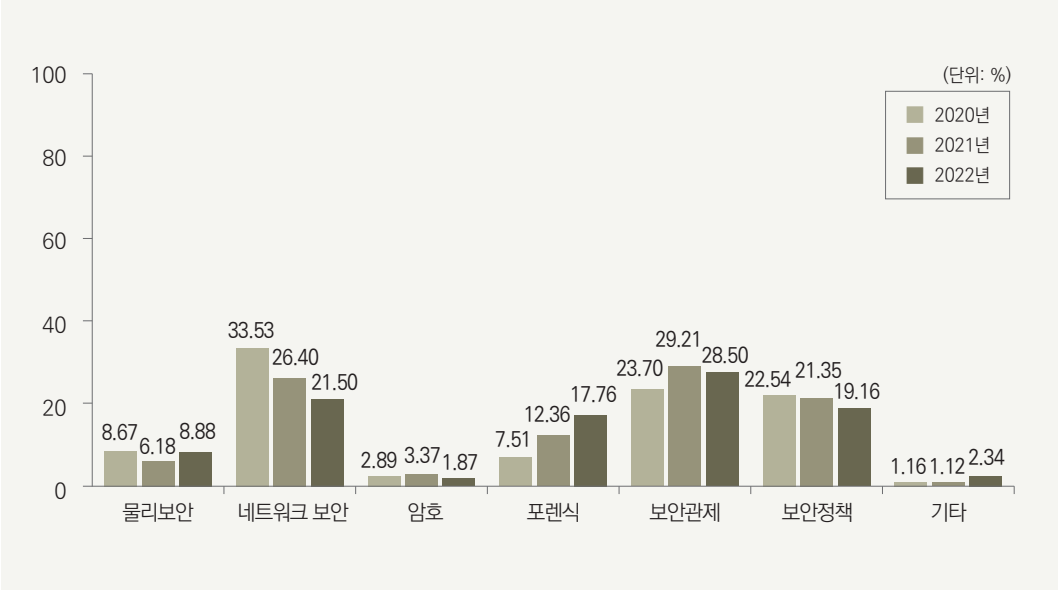
각 기관이 정보보호 수준 향상을 위하여 가장 중요하다고 생각하는 요소로는 보안교육 및 인식 제고가 63.64%로, 전년도에 이어 가장 많은 기관이 최우선 요소라고 답변하였다. 이에 이어 18.18%의 기관이 최신 정보보호제품 및 서비스 활용을 주요 요인으로 꼽았고, 기타 의견으로 전문인력 확보, 전담조직 마련, 예산 배정 등이 있었다.

그림 부록 1-가-39 기관 정보보호 수준 향상을 위한 최우선 요소



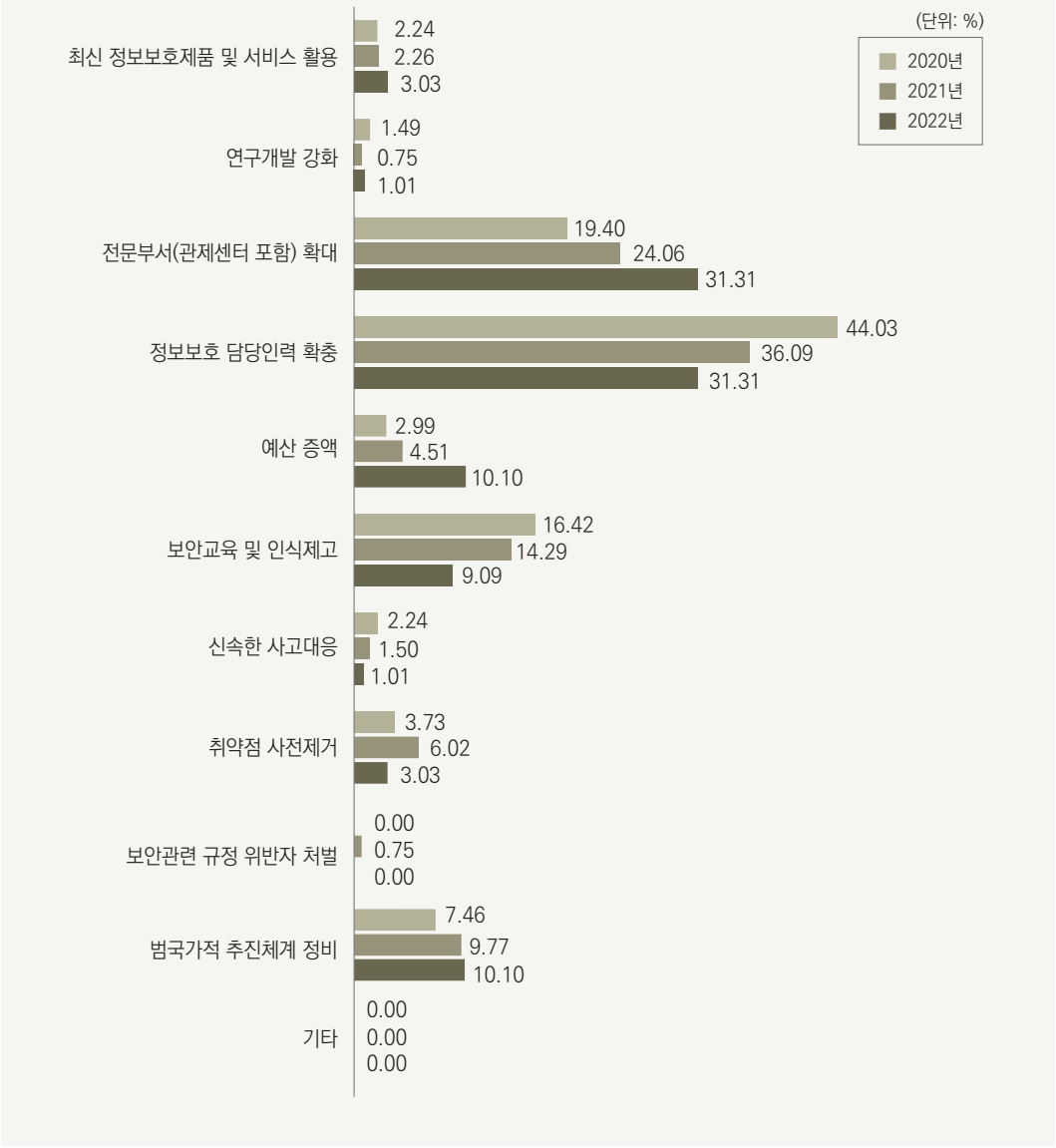
각 기관에서 보완되기를 희망하는 정보보호 인력의 전문분야는 보안관제가 28.5%로 가장 높았다. 이어 네트워크 보안 21.5%, 보안 정책 19.16%라는 응답이 뒤를 이었다. 눈에 띄는 점은 포렌식 관련 정보보호 인력이 보완되기를 바라는 기관이 증가 추세에 있다는 점이다.

그림 부록 1-가-40 기관별 보완이 필요한 정보보호 인력 전문분야



마지막으로, 국가 전체적인 정보보호 우선순위에 대하여는 최근 3년간 가장 높은 비율로 조사되었던 '정보보호 담당인력 확충'과 함께 '전문부서 확대'가 필요하다는 응답도 31.31%로 가장 높게 조사되었다. 또한 전년도에 비하여 '예산 증액'이 필요하다고 응답한 비율이 2배 이상 증가하였다. 이어 범국가적 추진 체계 정비가 10.1%, 보안교육 및 인식 제고가 9.09%를 기록하였다. 국가·공공부문 설문은 전반에 걸쳐 정보보호 인력 확충과 보안 인식 제고, 예산 확보 및 전담조직 신설 등을 긴요한 개선 요소로 꼽고 있는 것을 확인할 수 있었다.

그림 부록 1-가-41 국가 전체의 정보보호 우선순위



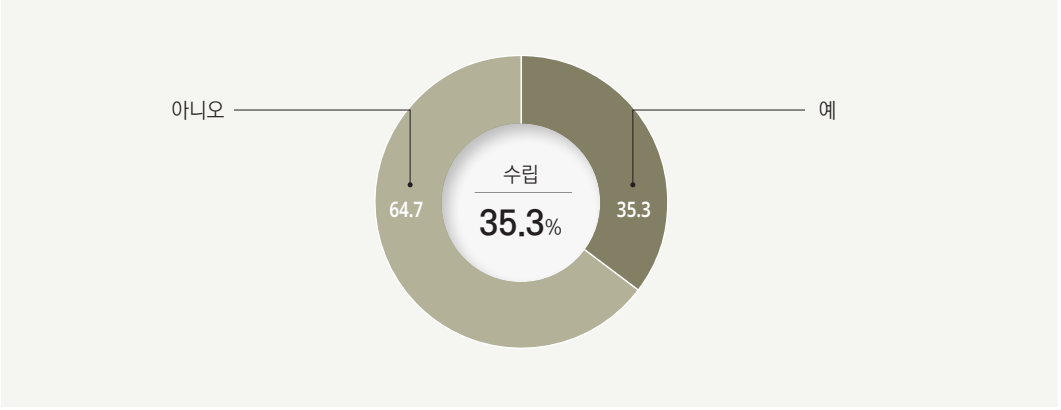
나 민간부문

민간부문 통계는 전국 6,500여 개 종사자 수 10인 이상의 국내 기업체 중 네트워크에 연결된 컴퓨터를 1대 이상 보유하고 있는 기업체를 대상으로 2022년 9월부터 11월까지 실시한 '정보보호 실태조사' 결과를 활용하였다.

1. 정보보호 정책 수립

기업체의 35.3%가 정보보호 정책을 보유하고 있는 것으로 나타났다.

그림 부록 1-나-1 정보보호 정책 수립

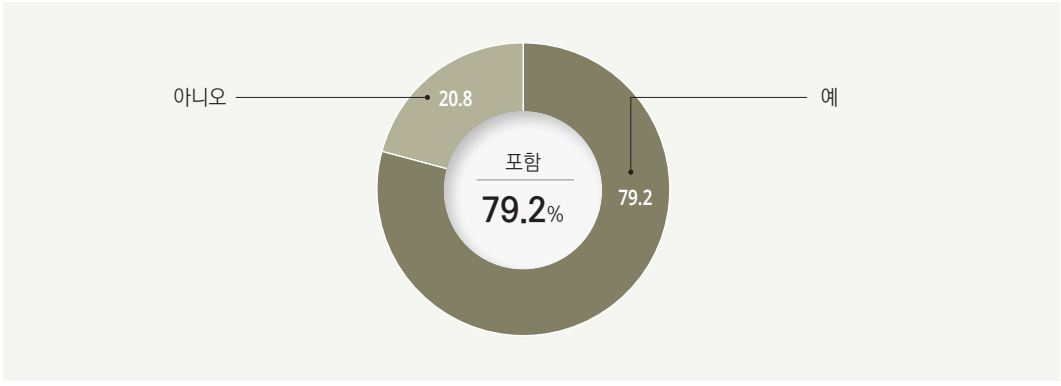


업종별로는 금융 및 보험업이 77.4%로 가장 높게 나타났으며, 종사자 수가 많을수록 정보보호 정책 수립률이 높은 것으로 나타났다.

2. 개인정보보호 정책 수립

기업체 중 79.2%가 정보보호 정책 내 개인정보보호 규정을 포함한 것으로 나타났다.

그림 부록 1-나-2 개인정보보호 정책 수립

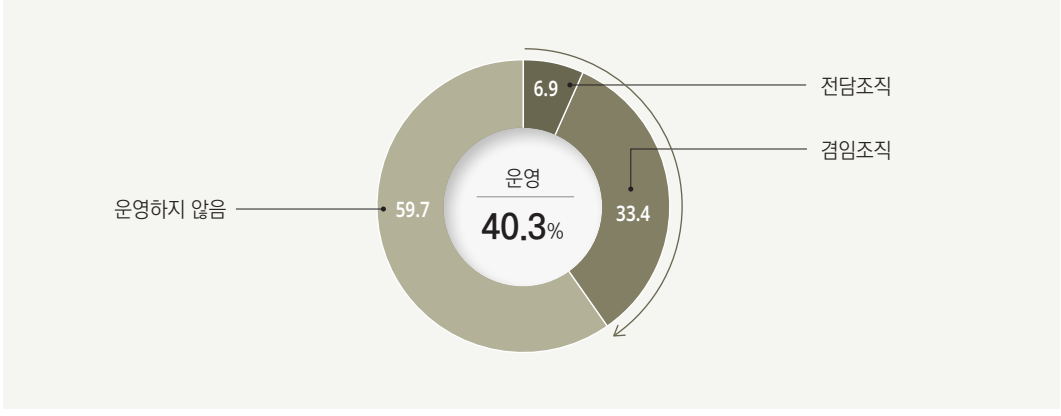


업종별로는 교육 서비스업이 99.4%로 가장 높게 나타났으며, 종사자 수가 많을수록 정보보호 정책 내 개인정보보호 규정이 포함되어 있는 비율이 높은 것으로 나타났다.

3. 정보보호 조직 운영

공식적인 정보보호 조직을 보유한 기업체의 비율은 40.3%로, 이 중 전담조직을 운영하는 경우는 6.9%, 겸임조직을 운영하는 경우는 33.4%로 조사되었다.

그림 부록 1-나-3 정보보호 조직 운영

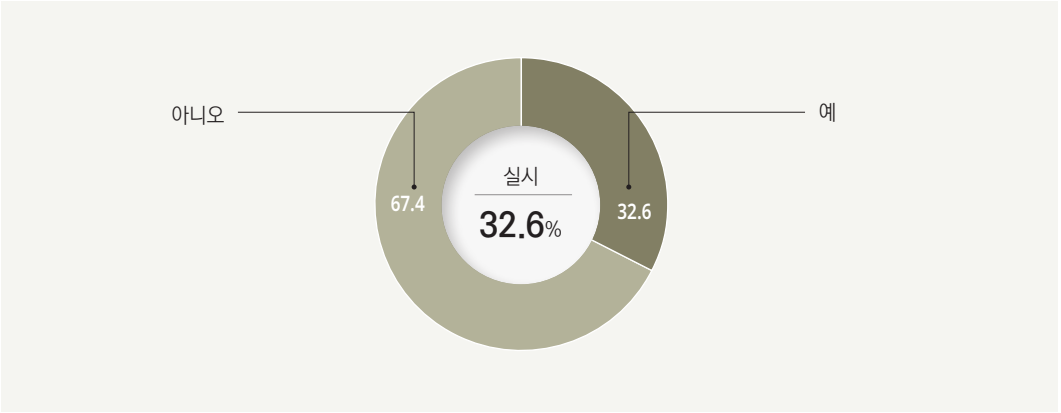


업종별로 금융 및 보험업이 18.9%로 다른 업종에 비하여 정보보호(개인정보보호) 조직을 운영하는 기업체가 많았으며, 규모별로는 250명 이상 대규모 기업체의 정보보호 전담조직 운영 비율이 23.3%로 나타났다.

4. 정보보호 교육 실시

기업체의 32.6%가 1년간 임직원을 대상으로 정보보호 교육을 실시한 것으로 조사되었다.

그림 부록 1-나-4 정보보호 교육 실시

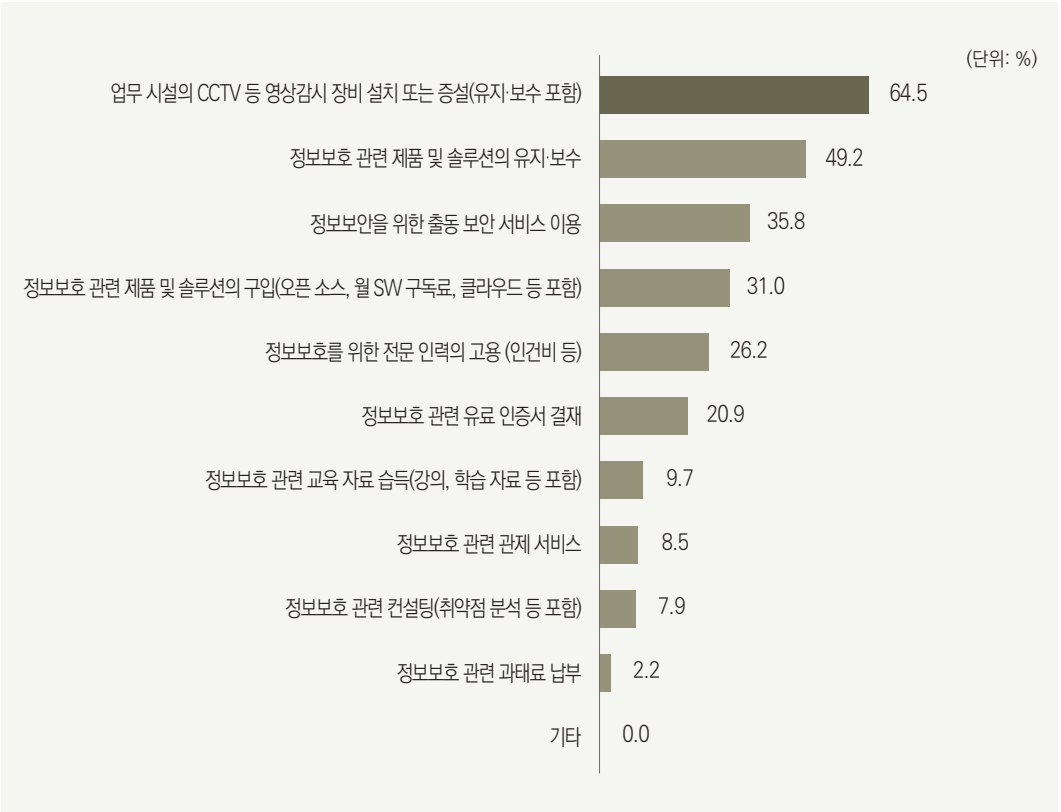


업종별로 금융 및 보험업의 교육 실시율이 60.7%로 가장 높게 나타났고, 다음으로 농림수산업(광업 포함)(49.4%)이 뒤를 이었다.

5. 정보보호 예산

기업체 중 67.9%는 최근 1년간 정보보호 예산을 사용한 경험이 있는 것으로 조사되었다.

그림 부록 1-나-5 정보보호 예산 활용 분야



정보보호 예산 활용 분야는 주로 '업무 시설의 CCTV 등 영상감지장비 설치 또는 증설(유지·보수 포함)'(64.5%)에 편성한 것으로 조사되었다. 다음으로 '정보보호 관련 제품 및 솔루션의 유지·보수'(49.2%), '정보보안을 위한 출동 보안 서비스 이용'(35.8%) 순으로 편성한 것으로 나타났다.

6. 정보보호제품 이용

기업체 중 80.7%가 정보보호 침해사고 예방을 위한 제품 및 솔루션을 이용한 경험이 있는 것으로 나타났다. 정보보안 제품 및 솔루션 중에서는 '시스템(엔드포인트) 보안장비'(73.6%)를 주로 이용하고 있었으며, 물리보안 제품 및 솔루션 중에서는 '출입통제 관리 시스템(출입통제 게이트, 디지털 도어락)'(77.7%)을 주로 이용하고 있는 것으로 나타났다.

그림 부록 1-나-6-1 정보보호제품 이용

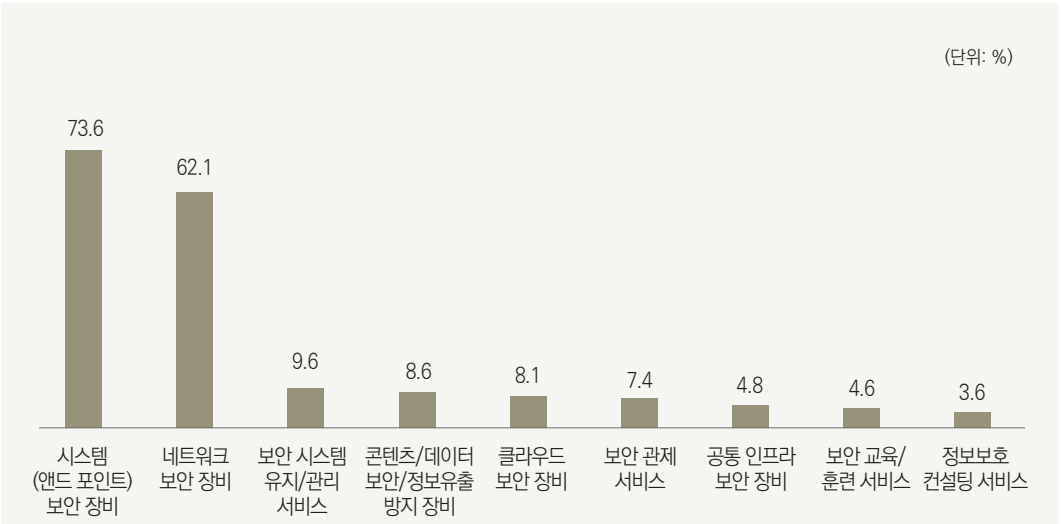
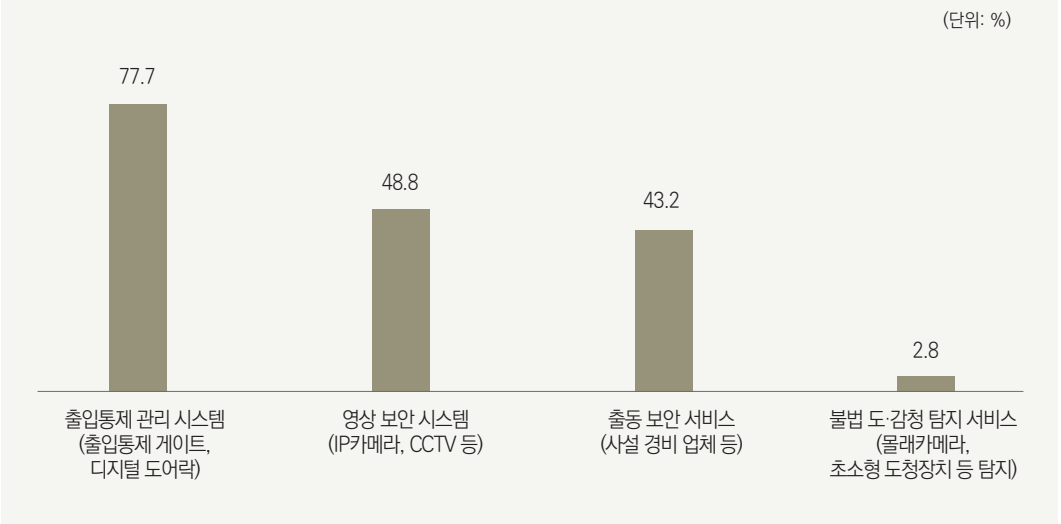


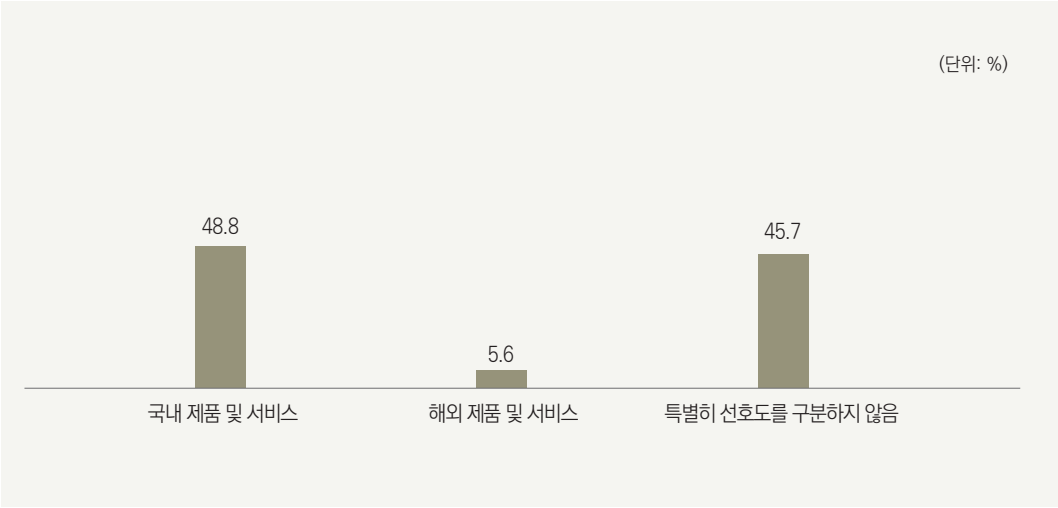
그림 부록 1-나-6-2 물리보안제품 이용



7. 정보보호서비스 이용

기업체 중 국산·외산 제품 및 서비스 선호도는 국산이 48.8%, 외산이 5.6%로 조사되었으며, 기업체의 45.7%는 특별히 선호도를 구분하지 않는 것으로 나타났다.

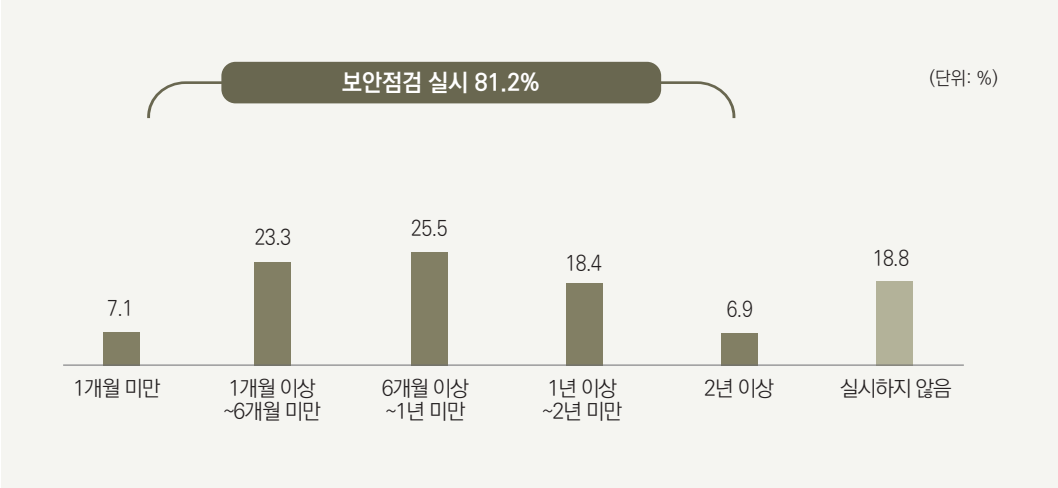
그림 부록 1-나-7 국내외 정보보호제품 및 서비스 선호도



8. 보안점검 및 취약점 점검

시스템 및 네트워크에 대한 보안점검(취약점 점검 등)을 실시하는 기업체는 81.2%였다. 최근 점검 실시 시점은 '6개월 이상~1년 미만'이 25.5%로 가장 높았고, 다음으로 '1개월 이상~6개월 미만(23.3%)' 순으로 조사되었다.

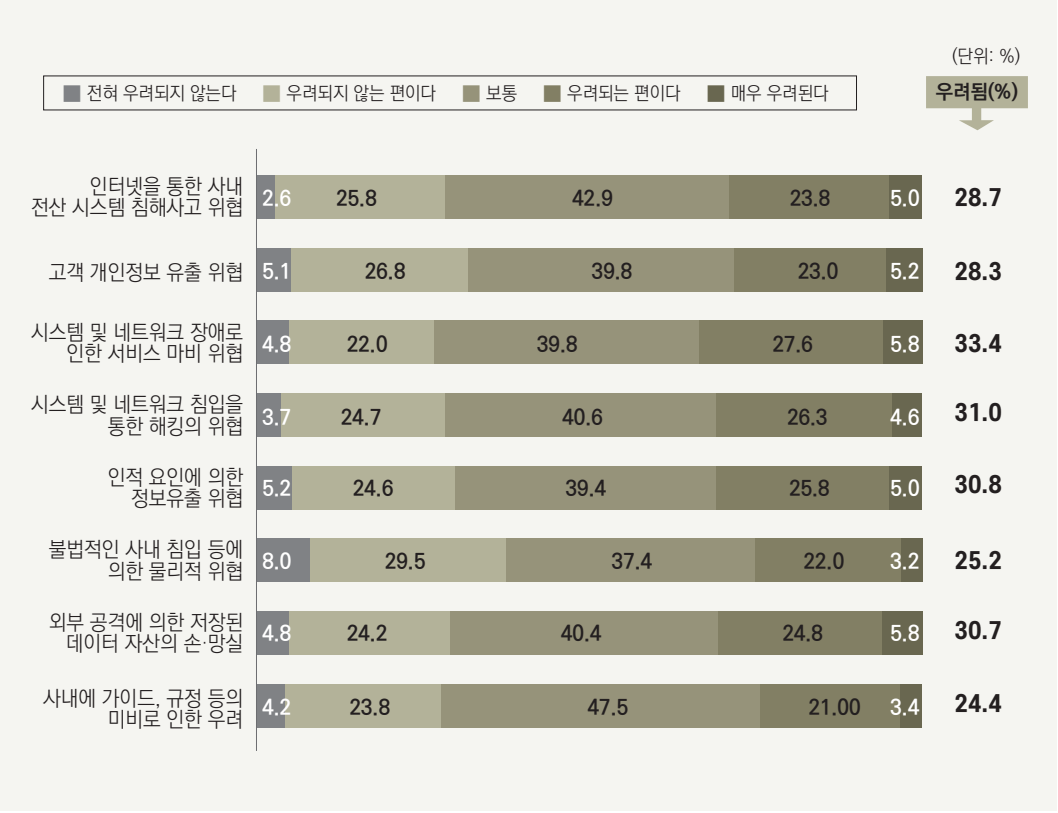
그림 부록 1-나-8 시스템 및 네트워크 보안점검 실시



9. 정보보호 위협요인

기업체가 우려하는 정보보호 위협요인으로는 '시스템 및 네트워크 장애로 인한 서비스 마비 위협'(33.4%)로 높게 나타났으며, 다음으로 '시스템 및 네트워크 침입을 통한 해킹의 위협'(31.0%)으로 나타났다.

그림 부록 1-나-9 정보보호 위협요인



10. 백업 실시

기업체의 89.1%가 데이터 백업을 실시하고 있으며, 백업 실시 유형으로는 '중요 데이터'(80.0%)로 가장 높고, 다음으로 '서버데이터(59.0%)로 나타났다.

그림 부록 1-나-10-1 시스템 로그 백업

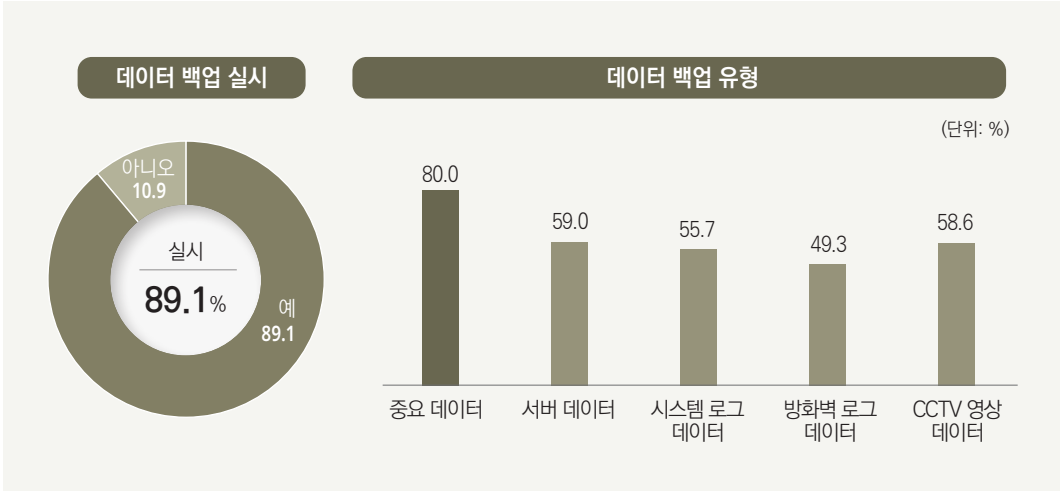
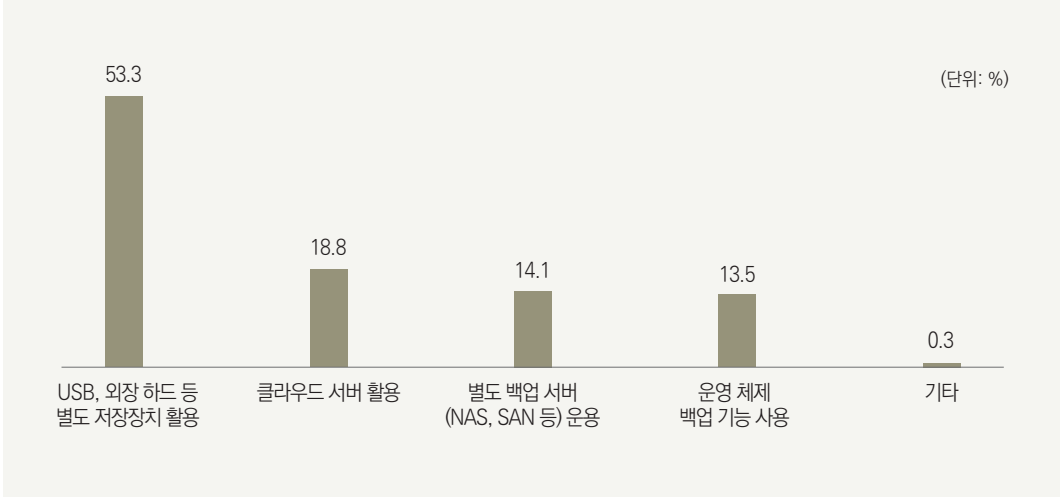


그림 부록 1-나-10-2 데이터 백업 방식

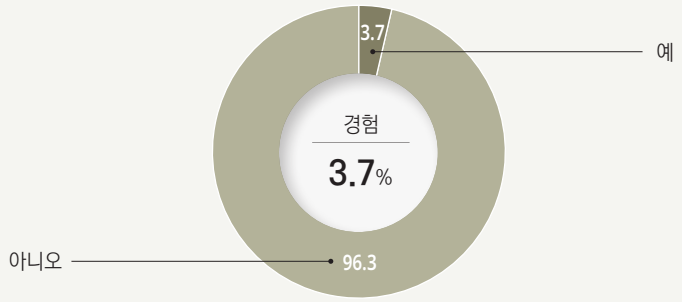


시스템 로그 또는 중요 데이터를 백업하는 방식은 'USB메모리, 외장 하드디스크 등 별도 저장장치 활용'이 53.3%으로 가장 높게 나타났다.

11. 침해사고 경험률

기업체의 3.7%가 침해사고를 직접 경험한 것으로 나타났다.

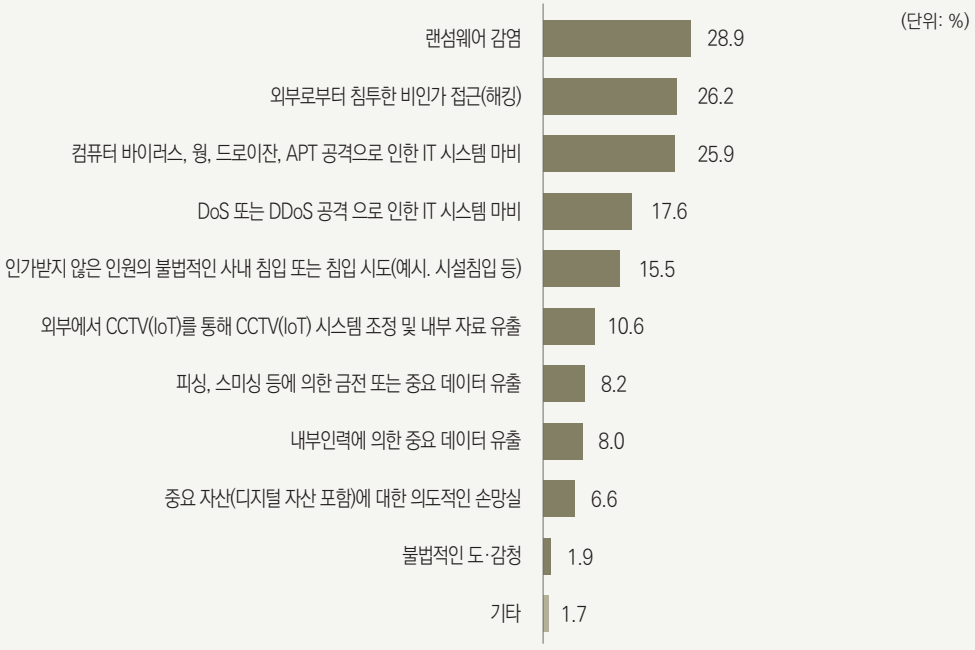
그림 부록 1-나-11 침해사고 직접 경험

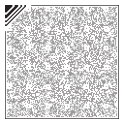


12. 침해사고 피해 유형

침해사고 경험 유형별로는 '랜섬웨어'의 경험률이 28.9%로 가장 높게 나타났고, 다음으로 '외부로부터 침투한 비인가 접근(해킹)'이 26.2%로 조사되었다.

그림 부록 1-나-12 침해사고 경험 유형(복수 응답)-침해사고 경험 기업체

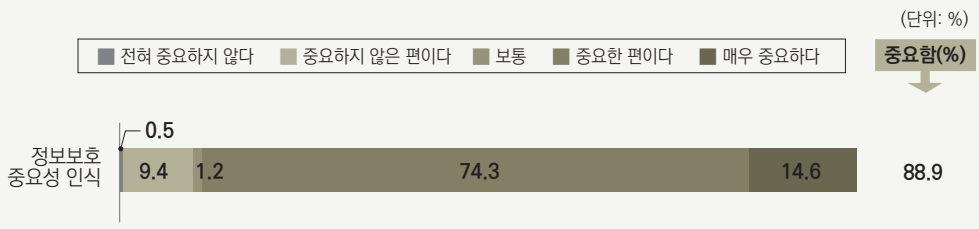




13. 정보보호 인식 및 애로 사항

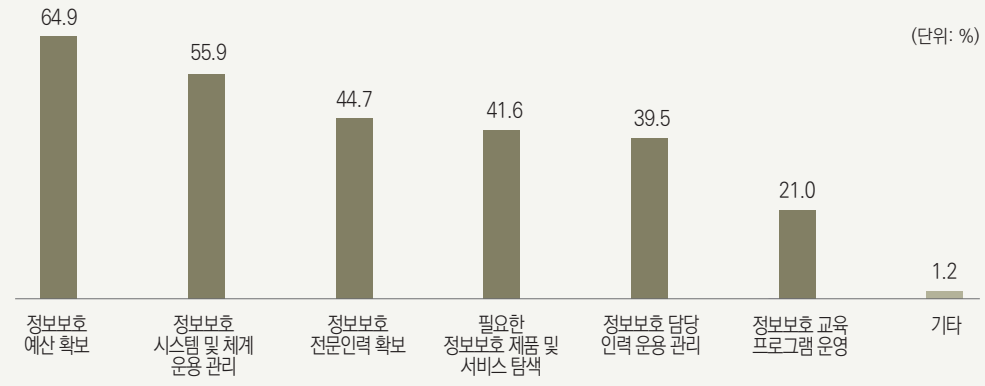
기업체 중 88.9%는 정보보호가 중요하다('중요한 편이다'~'매우 중요하다')고 응답하였다.

그림 부록 1-나-13-1 정보보호 및 개인정보보호 중요성 인식



정보보호에 대한 어려움을 느끼는 사항으로는 '정보보호 예산 확보'가 64.9%로 가장 높게 나타났고, 다음으로 '정보보호 시스템 및 체계 운용 관리(55.9%)', '정보보호 전문인력 확보'(44.7%) 등의 순이었다.

그림 부록 1-나-13-2 정보보호 애로 사항(복수 응답)



제2장

2022년 주요 정보보호 행사

행사명	기간	장소	주요 내용
2022 대한민국 개인정보보호 & 정보보안 콘퍼런스(G-privacy 2022)	3. 29.	서울 더케이호텔	공공부문의 개인정보보호 관련 발표 및 전문가 실무 강연
국제사이버공격방어훈련 (Locked Shields 2022)	4. 19.~ 4. 22.	온라인	사이버방어 협력 체제 구축 및 종합적인 사이버위기 상황 해결을 위한 훈련
제28회 정보통신망 정보보호 콘퍼런스(NetSec-KR)	4. 21.~ 4. 22.	온라인	방송 통신 환경에서의 기술적·정책적 이슈 및 최근 기술 동향과 연구 성과, 정보보호 기술 및 대안 수립을 위한 토론
2022 양자정보주간	6. 27.~ 7. 1.	온라인 & 서울 더케이호텔	양자 기술에 대한 국내외 성과 및 동향 공유와 저변 확대
2022 정보보호의 날 기념식 및 국제 정보보호 콘퍼런스	7. 13.	서울 더케이호텔	정보보호 문화와 관행을 사회 전반에 정착하고자 '정보보호의 날' 지정(매년 7월 둘째 주 수요일)하여 기념. 국제 정보보호 동향 파악을 위한 국제 정보보호 전문가가 참여하는 콘퍼런스도 함께 개최
아시아정보보안 공동회의 (ASIA JCIS 2022)	8. 15~ 8. 16.	온라인	정보보호 관련 최신 논문 발표 및 보안전문가 초빙 기술 강연
국제 정보보호 응용 워크숍 (WISA 2022)	8. 24.~ 8. 26.	제주 종글래드호텔	정보보호 기술 관련 최신 논문 발표 및 미국 육·해·공 보안 전문가 관련 논의
2022 사이버공간 국제평화 안보체제구축 학술회의(GCPR 2022)	9.20. ~ 9.21.	온라인 & 서울 더플라자호텔	사이버 국제 법규범 및 국가 사이버안보 전략 관련 국제 사이버안보 정책 콘퍼런스
개인정보보호&정보보안 콘퍼런스 (PASCON 2022)	9. 28.	서울 더케이호텔	공공기관과 기업 보안 실무자에게 현실적 대응 방안을 제시하는 강연 및 최신 보안 솔루션 전시회
제15회 국제 개인정보보호 심포지엄 (Privacy Global Edge 2022 & Asia Privacy Bridge Forum)	10. 13.	온라인	국내외 개인정보보호 책임자 및 전문가 초청, 개인정보보호 현안 논의
제16회 국제 사이버 시큐리티 콘퍼런스(ISEC 2022)	10. 18.~ 10. 19.	서울 코엑스	아시아 최대 규모의 국제 사이버 시큐리티 콘퍼런스로, 최신 보안 기술 동향 파악을 위한 전시회 및 워크숍
사이버공격·방어대회 2022 (CCE 2022)	10. 27.~ 10. 28.	온라인	사이버공격·방어 대회, 최신 사이버안보 기술·정책 세미나 및 우수 논문 공모전
제12회 소프트웨어 개발 보안 콘퍼런스	11. 4.	온라인 & 서울 코엑스	소프트웨어 중심 4차 산업혁명시대의 소프트웨어 개발 보안을 주제로 다양한 사례 및 최신 동향 공유
금융정보보호 콘퍼런스 (FISCON 2022)	11. 15.	온라인	금융·ICT 융합에 따른 금융보안 전략 수립을 위하여 해킹 시연, 초청 강연 및 주제 발표
제25회 국제 정보보호 및 암호학회 (ICISC 2022)	11. 30.~ 12. 2.	온라인	국내외 정보보안 및 암호학 관련 최신 정보 공유

제3장

국내 정보보호 관련 주요 사이트

	기관명	주소
국가기관	국가정보원	www.nis.go.kr
	과학기술정보통신부	www.msit.go.kr
	방송통신위원회	www.kcc.go.kr
	행정안전부	www.mois.go.kr
	금융위원회	www.fsc.go.kr
	개인정보보호위원회	www.pipc.go.kr
	외교부	www.mofa.go.kr
전문기관	한국인터넷진흥원	www.kisa.or.kr
	금융보안원	www.fsec.or.kr
	한국지역정보개발원	www.klid.or.kr
	한국전자통신연구원	www.etri.re.kr
민간단체	한국정보보호산업협회	www.kisia.or.kr
	한국침해사고대응팀협의회	www.concert.or.kr
	한국CISO협회	www.cisokorea.org
	개인정보보호협회	www.opa.or.kr
	한국정보보호학회	www.kiisc.or.kr
	한국융합보안학회	www.kcgsa.org
	한국사이버안보법정책학회	www.kcsa2012.or.kr
	한국산업보안연구학회	www.kais.or.kr
	한국CPO포럼	www.cpoforum.or.kr
	한국암호포험	www.kcryptoforum.or.kr
	개인정보보호법학회	www.pipla.kr
	개인정보전문가협회	www.ikapp.org
	국가보안학회	www.kaahs.or.kr

제4장

정보보호 민간단체

구분	명칭	설립 연도	주요 활동 분야
협회	한국정보통신진흥협회	1987	방송통신 발전과 공공복리 증진, ICT 분야 이슈 대응, 정보통신 자격검정, 취약점 컨설팅, 민간분야 주요정보통신기반시설보호 지원
	한국정보통신기술협회	1988	국내 유일의 정보통신 단체표준 제정기관이며, 표준화 활동 및 표준 제품의 시험인증 진행
	한국침해사고대응팀협의회	1996	민간 기업·기관의 정보보호 부서 또는 침해사고대응팀(CERT)이 자발적으로 참여
	한국정보보호산업협회	1997	네트워크 보안, 백신·PC 보안, 콘텐츠 보안, 정보보호 컨설팅, 물리보안 등의 정보보안 관련 기업이 회원사로 참여하여 정보보안 산업의 육성 및 발전 추구
	한국CISO협의회	2009	기업·기관의 자발적 참여를 바탕으로 국내 정보보호 최고책임자 간 협력 체계를 구성, 회원 간 협업과 소통을 통한 기업의 정보보호 수준 제고
	개인정보보호협회	2011	개인정보·위치정보 보호와 안전한 이용을 위한 민간 자율 구제 활동을 촉진하고 인증마크제도 운영 및 교육·홍보 등을 통하여 사회 전반의 개인정보보호 인식 제고
학회	한국정보보호학회	1990	정보보호 분야의 학술 활동 및 정보보호 관련 기술의 진흥과 발전에 기여
	한국융합보안학회	2001	회원 간 전문 지식을 배양하고 융합보안 전문인력을 양성하여 국방융합보안 체계 발전에 기여
	한국산업보안연구학회	2008	산업기술정보 및 임직원·시설·장비 등 유무형의 모든 산업 자산을 각종 침해 행위로부터 보호하고 손실을 방지하기 위한 다양한 연구 활동 지원
	한국사이버안보법정책학회	2012	사이버안보 법학 및 관련 학문의 연구·발표와 그 응용 활동을 지원함으로써 사이버안보 법학 발전과 법치주의 진작에 기여
	국가보안학회	2016	국가안보에 중요한 국가비밀과 중요시설의 유지·관리를 연구하는 학자들과 관련 기관에 종사하는 실무자들과의 교류 장려 및 실질적 지원
포럼	한국CPO포럼	2007	사업가·학계·유관 기관 등 사회 각 분야의 주요 인사들이 참여하여 개인정보 관련 현안에 대한 정보 공유, 개인정보보호 관련 법안 및 정책 수립을 위한 민간 분야의 의견을 수렴하고 전달

제5장

국내 ISAC 현황

구분	운영 주체 및 홈페이지	설립 연월	회원사	주요 업무
정보통신 ISAC	한국정보통신진흥협회 (www.kait.or.kr)	2002. 3.	9개 기간통신 사업자	회원사 간 정례 모임, 취약점 컨설팅, 민간분야 주요정보통신 기반시설보호 지원
금융 ISAC	금융보안원 (www.fsec.or.kr)	2012. 12.	19개 국내은행, 37개 증권기관, 42개 보험사 등 총 202개사	회원사(은행·증권 등) 보안관제, 취약점 분석평가, 컨설팅 등
행정 ISAC	한국지역정보개발원 (www.klid.or.kr)	2013. 2.	17개 시·도· 지방자치단체	17개 시·도·지방자치단체 보안관제, 취약점 분석평가, 컨설팅 등
의료 ISAC	사회보장정보원 (www.ssis.or.kr)	2018. 11.	43개 진료정보 문서저장소 및 민간 의료기관	상시 보안관제, 정보공유, 침해 대응, 보안교육 및 훈련

집필진

세부 분류		담당기관	담당자
도입부	2023 국가정보보호백서의 구성과 특징	한국인터넷진흥원	최지훈 선임
	정보보호 연혁	한국인터넷진흥원	최지훈 선임
	2022년 정보보호 10대 이슈	국가정보원 국가보안기술연구소	
제1편 정보보호 환경 변화 및 사이버위협 동향	제1장 정보보호 환경 변화	한국인터넷진흥원	김병재 책임
	제2장 사이버위협 주요 이슈와 전망		
제2편 정보보호 법·제도 및 기관	제1장 정보보호 법·제도		
	제1절 정보보호 법·제도 발전과정	각 기관	
	제2절 정보보호 법·제도 현황	각 기관	
	제3절 2022년 정보보호 관련 주요 개정 법령	각 기관	
	제2장 정보보호 기관 및 단체		
	제1절 국가기관	각 기관	
	제2절 전문기관	각 기관	
제3편 분야별 정보보호 활동	제1장 국가정보통신망 보호		
	제1절 사이버공격 탐지·차단	국가정보원	
	제2절 사고조사	국가정보원	
	제3절 보안관리컨설팅 및 관리실태 평가	국가정보원	
	제4절 보안적합성 검증	국가정보원	
	제5절 암호모듈 검증	국가정보원	
	제6절 정보보호제품 평가·인증	국가정보원	
	제2장 디지털정부		
	제1절 디지털정부 정보보호	한국인터넷진흥원	이유진 책임
	제2절 소프트웨어 개발보안	한국인터넷진흥원	이유진 책임
	제3절 전자서명 인증	한국인터넷진흥원	이은정 책임
	제3장 주요정보통신기반시설		
	제1절 추진 체계	한국인터넷진흥원	김남호 주임
	제2절 주요 활동	한국인터넷진흥원	김남호 주임
	제3절 국내외 침해사고 사례	국가정보원	

세부 분류			담당기관	담당자
제3편 분야별 정보보호 활동	제4장 정보통신서비스			
		제1절 침해사고 대응	한국인터넷진흥원	노경래 선임
		제2절 침해사고 예방	한국인터넷진흥원	김홍기 선임 이재성 선임 복재준 주임
		제3절 정보보호 및 개인정보보호 관리체계 인증	한국인터넷진흥원	한문희 선임
		제4절 클라우드 보안인증제도	한국인터넷진흥원	정유경 책임
		제5절 융합보안	한국인터넷진흥원	김지명 책임
	제5장 금융서비스			
		제1절 금융서비스 정보보호	금융보안원	곽승준 책임
		제2절 금융분야 사이버공격 대응 및 정보공유	금융보안원	곽승준 책임
		제3절 금융IT 및 전자금융·핀테크의 보안 평가·점검	금융보안원	곽승준 책임
제4편 정보보호 기반조성	제1장 정보보호산업 육성			
		제1절 개요	한국인터넷진흥원	배주은 선임
		제2절 정보보호 업체 및 시장 현황	한국인터넷진흥원	배주은 선임
		제3절 정보보호산업 관련 제도	한국인터넷진흥원	이이삭 선임
	제2장 정보보호 기술 개발			
		제1절 개요	한국인터넷진흥원	고 웅 책임
		제2절 원천기술 개발	한국인터넷진흥원	고 웅 책임
		제3절 상용기술 개발	한국인터넷진흥원	고 웅 책임
	제3장 정보보호 인력 양성			
		제1절 개요	한국인터넷진흥원	박유리 수석
		제2절 정규교육 과정	한국인터넷진흥원	박유리 수석
		제3절 전문기관 교육 과정	한국인터넷진흥원 금융보안원	이민경 주임 곽승준 책임
		제4절 각종 대회를 통한 인력 양성	한국인터넷진흥원 국가정보원 금융보안원	이민경 주임 곽승준 책임
		제5절 정보보호 자격증 제도	한국인터넷진흥원	박유리 수석
	제4장 개인정보보호			
		제1절 「개인정보 보호법」 개정 추진 및 행정 체계	한국인터넷진흥원	박지용 책임
		제2절 법·제도적 기반 강화	한국인터넷진흥원	박지용 책임

세부 분류			담당기관	담당자
제4편 정보보호 기반조성	제5장 대국민 정보보호			
		제1절 정보보호 상담 및 처리	한국인터넷진흥원	설원 연구위원
		제2절 인식제고	한국인터넷진흥원 금융보안원	홍 빛 선임 곽승준 책임
	제6장 국제협력			
		제1절 주요 사이버안보 외교 활동	국가정보원 외교부	
		제2절 사이버보안 국제협력	한국인터넷진흥원	허소선 선임
부록	제1장 통계로보는 정보보호			
		가. 국가·공공부문	국가정보원	
		나. 민간부문	한국인터넷진흥원	최지훈 선임
	제2장 2022년 주요 정보보호 행사		한국인터넷진흥원	최지훈 선임
	제3장 국내 정보보호 관련 주요 사이트		한국인터넷진흥원	최지훈 선임
	제4장 정보보호 민간단체		한국인터넷진흥원	최지훈 선임
	제5장 국내 ISAC 현황		한국인터넷진흥원	최지훈 선임

자문위원

소속	자문위원	소속	자문위원
충남대학교	원유재 교수	상명대학교	유지연 교수
순천향대학교	염흥열 교수	서울대학교	이석윤 교수
충남대학교	류재철 교수	부산대학교	김현수 교수

편집진

소속	직위	편집자
한국인터넷진흥원	실장	김정희
	팀장	최영준
	선임	최지훈
국가보안기술연구소	실장	김동희
	연구원	유영인
금융보안원	팀장	김성웅
	책임	곽승준

2023 **국가정보보호백서**

발 간 일: 2023년 5월

발간기관: 국가정보원·과학기술정보통신부·행정안전부·개인정보보호위원회·금융위원회·외교부

지원기관: 한국인터넷진흥원·국가보안기술연구소·금융보안원

세부 분류			담당기관	담당자
제4편 정보보호 기반조성	제5장 대국민 정보보호			
		제1절 정보보호 상담 및 처리	한국인터넷진흥원	설원 연구위원
		제2절 인식제고	한국인터넷진흥원 금융보안원	홍 빛 선임 곽승준 책임
	제6장 국제협력			
		제1절 주요 사이버안보 외교 활동	국가정보원 외교부	
		제2절 사이버보안 국제협력	한국인터넷진흥원	허소선 선임
부록	제1장 통계로보는 정보보호			
		가. 국가·공공부문	국가정보원	
		나. 민간부문	한국인터넷진흥원	최지훈 선임
	제2장 2022년 주요 정보보호 행사		한국인터넷진흥원	최지훈 선임
	제3장 국내 정보보호 관련 주요 사이트		한국인터넷진흥원	최지훈 선임
	제4장 정보보호 민간단체		한국인터넷진흥원	최지훈 선임
	제5장 국내 ISAC 현황		한국인터넷진흥원	최지훈 선임

자문위원

소속	자문위원	소속	자문위원
충남대학교	원유재 교수	상명대학교	유지연 교수
순천향대학교	염흥열 교수	서울대학교	이석윤 교수
충남대학교	류재철 교수	부산대학교	김현수 교수

편집진

소속	직위	편집자
한국인터넷진흥원	실장	김정희
	팀장	최영준
	선임	최지훈
국가보안기술연구소	실장	김동희
	연구원	유영인
금융보안원	팀장	김성웅
	책임	곽승준

2023 **국가정보보호백서**

발 간 일: 2023년 5월

발간기관: 국가정보원·과학기술정보통신부·행정안전부·개인정보보호위원회·금융위원회·외교부

지원기관: 한국인터넷진흥원·국가보안기술연구소·금융보안원

제　　작: 호정씨앤피(Tel. 02-2277-4718)

2023
국가정보보호백서

발간 기관

국가정보원 NATIONAL INTELLIGENCE SERVICE

과학기술정보통신부 Ministry of Science and ICT

행정안전부 Ministry of the Interior and Safety

개인정보보호위원회 Personal Information Protection Commission

금융위원회 Financial Services Commission

외교부 Ministry of Foreign Affairs

지원 기관

KISA 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY

NSR 국가보안기술연구소

금융보안원 FINANCIAL SECURITY INSTITUTE