보안기업의 보안수준 향상을 위한 지원(제도, 인증)사업

□ 한국인터넷진흥원에서는 기업의 보안 수준 제고를 다음과 같은 사업을 추진하고 있습니다.

지원(제도, 인증)사업명	지원(제도, 인증) 주요내용	지원(신청)대상	지원(신청)방법	지원사업 신청 링크
정보보호 공시제도	· 이용자의 안전한 인터넷 이용 및 정보보호 투자 활성화를 위하여 기업의 정보보호 현황(정보보호 투자, 인력, 인증, 활동 등)을 공개	· 사업분야*, 연 매출액 3천 억 원 이상, 이용자 수 100만 명 이상 * 기간통신사업자, 집적정보통신시설 사업자, 상급종합병원, 클라우드사업자	홈페이지 신청	www.isds.kisa.or.kr
중소기업 정보보호 지원사업	· 중소기업 보안수준 강화를 위한 정보보호 컨설팅 및 보안솔루션, SECaaS* 지원 * (Security as a Service) 클라우드 환경을 통해 소프트웨어 형태로 제공되는 보안 서비스	· 지역 전략산업 內 중소기업 * 지역 보안기업도 가능	홈페이지 신청	risc.kisa.or.kr
사이버 위기대응 모의훈련	· 해킹메일 훈련, 디도스 대응 훈련, 모의침투, 탐지대응 훈련 등 민간분야 사이버 위기대응 모의훈련 지원(정기 및 상시)	· (정기훈련) 대상 제한 없음, 연 2회 · (상시훈련) 중소기업 한정	홈페이지 신청	www.boho.or.kr
중소기업 원격보안점검 (내서버돌보미)	· 기업에서 운영 중인 서버에 대한 원격 보안점검 및 기업 스스로 보안관리를 위한 자가진단 도구 제공	· 영세·중소기업	홈페이지 신청	www.boho.or.kr
중소기업 보안취약점 점검	· 기업의 보안 취약점 발견 및 조치를 위한 시스템·서비스 모의해킹/취약점 점검 지원	· (모의해킹) 중견 및 중소기업 · (취약점점검) 중소기업	(모의해킹) 대상 섭외 (점검) 홈페이지 신청	www.boho.or.kr
중소기업 침해사고 피해지원	· 침해사고 피해기업 대상 사고 원인분석 결과 및 조치 대응방안 안내	· 중소기업기본법 제2조에 해당하는 중소기업	홈페이지 신청	www.boho.or.kr

지원(제도, 인증)사업명	지원(제도, 인증) 주요내용	지원(신청)대상	지원(신청)방법	지원사업 신청 링크
해킹진단도구 보급	· 기업 스스로 해킹피해 여부를 점검할 수 있도록 시스템 정보를 수집하여 해킹피해 사실여부를 분석해 주는 해킹 진단도구 보급	· 대기업, 비영리 기업, 중소기업 등 제한 없이 민간기업 전체	홈페이지 신청	www.boho.or.kr
사이버 위협정보 공유체계	· 기업·기관의 사이버 위협 적시 대응을 위한 실시간 상황전파 및 사이버 위협정보 공유체계(C-TAS) 운영 * (운영 근거)「정보통신망법」 제48조의2 제1항제1호	· 국내 모든 기업, 기관 * (회원사 수) 4,488개社(25.2월)	홈페이지 신청	ctas.krcert.or.kr
보안 취약점 신고포상제	· 국내 보안 취약점 발굴·조치 활성화를 위해 소프트웨어 신규 취약점을 발굴·신고한 자에 포상금을 지급하는 제도 * 취약점의 위험도, 파급도, 발굴 난이도이 따라 최대 1,000만원/건 포상금 지급	· 대상 제한 없음	홈페이지 신청 (취약점 신고 접수 메뉴)	knvd.kcert.or.kr
ISMS 인증	· 정보자산 유출 및 피해 예방을 위해 기업 또는 기관이 스스로 구축·운영 중인 정보보호 체계가 적합한지 인증하는 제도	· 정보통신망 서비스 제공자(ISP), 집적통신시설 사업자(IDC), 상급종합병원, 대학 등	공문 접수 (심사 수행기관에 제출)	isms.kisa.or.kr
클라우드 보안인증 (CSAP)	· 클라우드서비스의 보안인증기준 적합여부를 평가하는 보안인증 제도	· 클라우드 컴퓨팅 서비스 기업	이메일 접수	cloud@kisa.or.kr

정보보호 공시제도

[정보보호산업본부]

○ **(개요)** 이용자의 안전한 인터넷 이용 및 정보보호 투자 활성화를 위하여 정보보호 현황을 공개하는 자율 · 의무공시 제도

※ (법적근거)「정보보호산업의 진흥에 관한 법률」제13조, 동법 시행령 제8조, 동법 시행규칙 제3조의2, 정보보호 공시에 관한 고시

○ **(목적)** 기업의 정보보호 현황을 공개하고 관리함으로써 이용자의 안전한 인터넷 이용과 기업의 정보보호 투자 확대 도모

- 이용자에게 객관적인 기업 선택의 기준을 제시하고, 기업은 정보보호를 기업 활동의 중요 요소로 인식하도록 하여 보안 수준을 제고

○ **(공시내용)** 매년 6월 말까지 공시대상연도의 정보보호 투자액, 전담인력, 인증·평가·점검, 정보보호 활동 등 4개 항목 현황 공개

공시 항목	주요내용
정보보호 투자 현황	▸ 정보기술부문 투자 대비 정보보호부문 투자 현황 등
정보보호 인력 현황	▸ 정보기술부문 인력 대비 정보보호부문 전담인력 현황 등
정보보호 관련 인증·평가·점검	▸ ISMS, CSAP 등 정보보호 관련 인증·평가·점검 현황 등
정보보호를 위한 활동 현황	▸ 정보보호 투자 활성화 실적, 정보보호 인식 제고 교육 등 기업의 정보보호를 위한 대내외 활동 현황 등

○ 공시대상

- **(자율공시 대상)** 정보통신망을 통하여 정보를 제공하거나 정보의 제공을 매개하는 자 ※ 정보보호관리체계(ISMS) 인증 수수료 30%할인

- **(의무공시 대상)** 사업분야, 매출액 및 서비스 이용자 수를 고려하여 일정 규모 이상* 기준에 해당하는 자

* ① 기간통신사업자, 집적정보통신시설사업자, 상급종합병원, 클라우드사업자
② CISO 지정·신고 상장법인 중 연 매출액 3,000억 원 이상
③ 일 평균 이용자 수 100만 명 이상

한국인터넷진흥원

중소기업 정보보호 컨설팅 및 보안솔루션 도입 지원

[정보보호산업본부]

○ **(개요)** 자체 ICT 인프라를 구축/운영중인 중소기업에 지능화 및 고도화 되고 있는 사이버보안 위협 대응/예방을 위한 컨설팅 및 보안솔루션 지원

○ **(지원대상)** 중소기업기본법 제2조에 따른 중소기업

○ **(지원내용)** 정보보호 컨설팅 및 보안솔루션(보안장비 및 SECaaS*)

* Security as a Service : 클라우드 환경을 통해 소프트웨어 형태로 제공되는 보안서비스

- 정보보호 정책수립 현황, PC 및 서버 등 기업 보유 인프라 자산 취약점 진단, 웹 취약점 점검 등 기업의 보안현황에 맞는 맞춤형 정보보호 컨설팅 지원
- 정보보호 컨설팅 결과 기반 보안솔루션 도입 비용 지원

○ **신청방법 및 프로세스**

신청접수
risc.kisa.or.kr
▶
적격심사
(지원대상 여부 검토)
▶
정보보호 컨설팅 및 보안솔루션 지원

※ 매년 6~11월(예산 소진시 조기마감되며, 세부사항은 홈페이지(risc.kisa.or.kr) 참조)

○ **(문의처) 지역별 정보보호 지원센터**

센터명	연락처	관할지역
인천정보보호 지원센터	032-710-7840	서울, 인천
대구정보보호 지원센터	053-939-4344	대구
호남정보보호 지원센터	062-655-9907	광주, 전남, 전북, 제주
중부정보보호 지원센터	043-210-0870	대전, 세종, 충북
동남정보보호 지원센터	051-746-4793	부산, 경남
경기정보보호 지원센터	031-698-4705	경기
울산정보보호 지원센터	052-210-0253	울산
강원정보보호 지원센터	033-248-5680	강원
경북정보보호 지원센터	054-223-2297	경북
충남정보보호 지원센터	041-589-0743	충남

한국인터넷진흥원

민간분야 사이버 위기대응 모의훈련

[정보보호산업본부]

○ **(개요)** 사이버위협이 증가하고 있어 민간기업의 사이버위협 대응력 제고를 위해 **실제 해킹과 동일한 방식(해킹메일, 모의침투 등)**으로 모의훈련 추진

○ **(지원대상)** 정기훈련(참여제한 없음), 상시훈련(중소기업 한정)

○ **(지원내용)** 사이버 위기대응 모의훈련(정기훈련) 및 훈련 플랫폼(상시훈련) 제공

- **(정기훈련)** 국가 사이버 위기상황 발생 시 **신속한 대응 및 협조체계 점검**을 위한 민간분야 사이버 위기대응 모의훈련 실시(상·하반기, 연 2회)

- **(상시훈련)** 기업에서 자율적으로 모의훈련이 가능한 플랫폼 제공(상시)
  - 해킹메일, 디도스, 웹 취약점 훈련, 대응가이드 및 평가지표 제공

종류	주기	지원 대상	훈련 내용
상시훈련	상시 운영	영세·중소기업 한정	o 임직원 대상 악성메일 발신 o 디도스 공격 대응 훈련 o 기업 홈페이지 모의침투 o 서버 취약점 탐지·대응 훈련
정기훈련	연 2회 (상·하반기 각 1회)	대기업·비영리 등 참여 제한 없음	

○ **신청방법 및 프로세스**

신청접수
(정기 및 상시훈련)
www.boho.or.kr
▶
적격심사
(지원대상 여부 검토)
▶
정기 및 상시훈련
진행

○ **(문의처) 모의훈련 운영센터**

- **Mail : info@cybersecuritydrill.kr, Tel : 1600-0461**

한국인터넷진흥원

중소기업 원격보안점검 서비스(내서버돌보미)

[정보보호산업본부]

○ **(개요)** 자체 보안점검이 어려운 중소기업 대상 서버 원격보안점검을 제공하여 보안 수준 및 침해사고(랜섬웨어, 정보유출 등) 예방력 강화 지원(22년~)

※ 추진 근거 : 「랜섬웨어 대응 강화방안(관계부처합동, 21.8월)」 - '중소기업 보안역량 지원 강화'

○ **(지원대상)** 중소기업기본법 제2조에 따른 중소기업

○ **(지원내용)** 중소기업 서버 원격보안점검 및 가이드, 자가진단도구 보급 등

○ **신청방법 및 프로세스**

신청접수
www.boho.or.kr

▶

신청서 검토 및 사전협의
(지원대상 여부 검토 등)

▶

서버 원격보안점검 및 가이드, 자가진단도구 제공

○ **(문의처) 내서버돌보미 헬프데스크**

- **Tel : 02-6715-2332, 2333**

한국인터넷진흥원

중소기업 보안 취약점 점검

[디지털위협대응본부]

○ **(개요)** 기업의 시스템·서비스 등에서 정보유출, 시스템 파괴 등 해킹 공격 피해의 원인이 되는 보안취약점을 찾아 조치될 수 있도록 기술지원

○ **(지원대상)** 국민생활 밀접 서비스 제공 중소기업
(중소기업기본법 제2조에 따른 중소기업)

○ **(점검대상)** 모바일앱(IOS/Android), 웹(홈페이지), 개발·운영 환경

○ **(지원내용)**

- 기업 대외서비스(홈페이지, 모바일앱) 보안취약점 점검
- 기업 내부 주요 시스템 및 네트워크 보안 취약점 점검

점검분야	주요내용
모바일앱	▸ 앱 변조 및 유포, 중요정보 노출 등 취약점 점검
홈페이지	▸ 중요정보 유출, 악성코드 삽입 등 취약점 점검
개발·운영 환경	▸ 시스템, 네트워크 등 기업 인프라 보안 취약점 점검

○ **신청방법 및 프로세스**

신청접수
www.boho.or.kr
▶
적격심사
▶
점검 추진
· 점검대상 협의
· 취약점 점검 실시
▶
기술지원
· 취약점 조치 요청
· 기술지원

※ 신청 후 적격유무 판단 및 서비스 신청 수요에 따라 1개 이상 분야 취약점 점거 지원

○ **(문의처)** 국번없이 118

한국인터넷진흥원

해킹진단도구 보급

[디지털위협대응본부]

○ **(개요)** 일반기업도 쉽고 간단하게 기업에서 운영하는 시스템의 해킹피해 여부를 자가점검할 수 있는 해킹진단도구를 배포

○ **(지원대상)** 민간기업 전체 ※ 대기업, 비영리 기업도 제한 없음

○ **(점검대상)** 해킹사고 의심 서버 PC

○ **(지원내용)** 기업에서 운영하는 윈도우·리눅스 서버 내 다양한 증거 데이터를 수집·분석하여 해킹피해 여부 탐지 결과 제공

주요 기능	주요내용
수집 기능	▸ 기업 운영 시스템 내 다양한 증거 데이터*를 손쉽게 수집 * 시스템 및 네트워크 현황, 원격접속기록, 프로그램 설치 및 실행, 계정 생성, 시작 프로그램 등록, 로그 삭제, 백신탐지기록, 어플리케이션 로그 등
분석 기능	▸ 수집된 로그 등에 대해 해킹여부 탐지룰을 기반으로 분석·진단 ※ 사용자가 시스템의 해킹여부를 직관적으로 판단할 수 있도록 3단계 결과 제공 (●심각, ●주의, ●정상)

○ **신청방법 및 프로세스**

신청접수
www.boho.or.kr
▶
신청서 검토
▶
해킹진단도구 및 매뉴얼 배포

○ **(문의처)** 국번없이 118

한국인터넷진흥원

중소기업 침해사고 피해지원

[디지털위협대응본부]

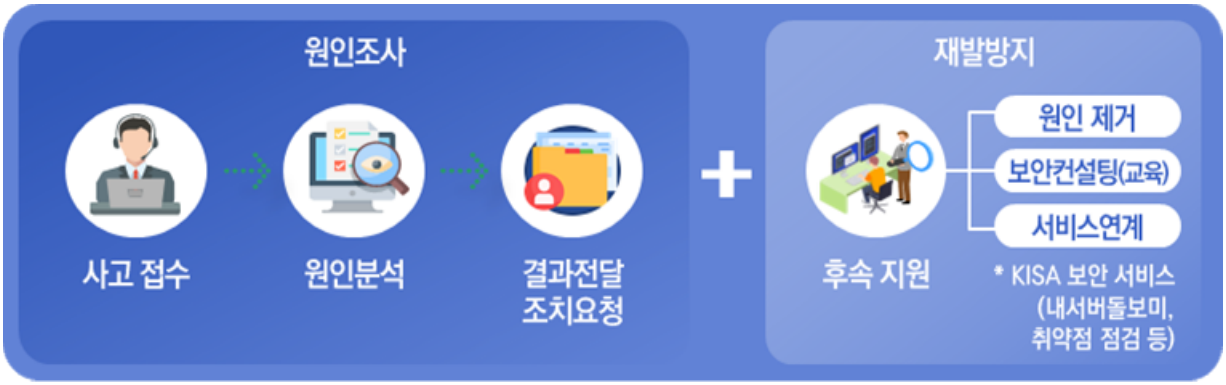
○ **(개요)** 침해사고 피해기업 대상 사고 원인조사 및 재발 방지 조치지원

○ **(지원대상)** 중소기업기본법 제2조에 해당하는 중소기업

○ **(지원내용)** 원인분석 및 재발방지 기술지원

- 침해사고 발생 원인 및 침투경로 분석
- 재발방지를 위한 사고원인 제거 및 맞춤형 보안 컨설팅·교육 지원

< 중소기업 침해사고 피해지원 서비스 흐름도 >



○ **신청방법 및 프로세스**

신청접수	▶	침해사고 분석데이터 수집	▶	사고원인 분석 및 결과보고서 제공
www.boho.or.kr ※ 침해사고 발생 시 한국인터넷진흥원에 신고 및 기술지원에 동의한 기업의 경우 서비스 이용		※ 현장출동 또는 원격지원		

○ **(문의처)** 국번없이 118

한국인터넷진흥원

사이버 위협정보 공유활용을 위한 데이터 개방(C-TAS)

[디지털위협대응본부]

○ **(개요)** 모든 기업이 참여가능한 개방형 홈페이지를 통해 사이버 위협정보, 주요동향 및 실시간 긴급상황 알림서비스 등을 제공

○ **(지원대상)** 중소기업 등 모든기업, 기업 정보보호 최고책임자(CISO) 또는 보안 실무자

○ **(지원내용)**

- 모든 기업이 개방형 홈페이지를 통해 사이버 위협정보 이용 지원
- 사이버 위기상황 또는 침해사고 발생 시 긴급상황전파 체계를 통해 문자 안내 지원
- 위협정보와 더불어 보안뉴스, 보안 가이드라인, 분야별 정보공유방 등 사이버 보안 콘텐츠 제공

○ **신청방법 및 프로세스**

신청접수 https://ctas.krcert.or.kr	▶	회원가입 신청 및 승인	▶	사이버위협정보 공유 실시간 긴급상황전파(문자)

○ **(문의처)** 국번없이 118

한국인터넷진흥원

보안 취약점 신고포상제(버그바운티) 공동운영 제도

[디지털위협대응본부]

○ **(개요)** 취약점 발굴 및 조치를 위한 버그바운티 운영이 어려운 기업을 대상으로 KISA의 신고 포상제 운영경험을 기반한 취약점 버그바운티를 공동으로 운영하는 제도

<버그바운티> 소프트웨어 신규 취약점을 발굴하여 신고한 사람에게 포상금을 지급하는 제도

· (목적) 국내 민간 보안 전문가의 취약점 발굴 활성화, 국내 보안 취약점 발굴·조치 선도적 역할 수행을 통한 해킹사고 악용 예방

· (신고대상) 최신 버전의 소프트웨어에 영향을 줄 수 있는 신규 취약점

· (신고방법) 사이버보안 취약점 정보포털(knvd.krcert.or.kr)의 취약점 신고접수 메뉴를 통해 취약점 신고

· (평가·포상) 취약점의 위험도, 파급도, 발굴 난이도를 평가하며, 평가 점수에 따라 포상금 지급(분기별, 최대 1,000만원/건)

○ **(지원대상)** IT서비스를 제공하는 국내 모든 기업

○ **(지원내용)**

- 보안 취약점 신고·접수 및 분석·평가 지원
- 버그바운티 독립 운영을 위해 운영체계 구축 지원

○ **공동운영사 신청방법 및 프로세스**

신청접수
khs83@kisa.or.kr

▶

KISA-공동운영사 간 업무협약 검토

▶

취약점 신고포상제 공동운영사 참여 발표

※ 사이버 보안 취약점 정보 포털(kvnd.krcert.or.kr) 홈페이지내 신고포상제->공동 운영 제도 설명 참조

○ **(문의처)** 국번없이 118

ISMS 인증 제도

[디지털안전지원본부]

○ **(목적)** 정보자산 유출 및 피해 예방을 위해 기업 또는 기관이 스스로 구축·운영 중인 정보보호 체계가 적합한지 인증하는 제도(ISMS*)

* 정보보호 관리체계(Information Security Management System)

※ 「정보통신망법」 제47조(정보보호 관리체계 인증) 근거

○ **(점검항목)** 총 80개(관리체계 수립 및 운영 16개, 보호대책 요구사항 64개)

※ ISMS의 총 80개 점검항목을 기본으로 개인정보 처리단계별 요구사항 21개를 추가한 '정보보호 및 개인정보보호 관리체계'(ISMS-P) 존재

○ **(인증절차)** 서면 및 현장심사의 방법으로 인증심사를 실시하고, 인증위원회의 심의·의결을 거쳐 인증서 부여

- 인증 유효기간은 3년(최초 심사 후 매년 사후심사, 3년 주기 갱신심사)

○ **(인증 수수료)** 1건당 평균 800~1,400만원 내외

○ **(인증 의무대상 「정보통신망법」 제47조)**

구분	상세내용	기업
정보통신망 서비스 제공자(ISP)	■「전기통신사업법」 제6조제1항에 따른 전기통신사업자(기간통신사업자)로서 서울특별시 및 모든 광역시에서 정보통신망서비스를 제공하는 자	13
집적통신시설 사업자(IDC)	■타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는 자	39
전기통신역무를 이용하는 정보 제공자 / 정보의 제공을 매개하는 자	① 연간 매출액 또는 세입 등이 1,500억원 이상이며,	-
	- 「의료법」 제3조의4에 따른 상급종합병원	43
	- 직전연도 12월 31일 기준 재학생 수 1만명 이상인 「고등교육법」 제2조에 따른 학교	29
	② 정보통신서비스 부문 전년도 매출액이 100억원 이상인 자	399
	③ 전년도 말 기준 직전 3개월간의 일일평균 이용자 수가 100만명 이상인 자	2

한국인터넷진흥원

클라우드 보안인증제도(CSAP) 설명자료

[디지털안전지원본부]

○ **(개요)** 국가기관 등이 안전하게 **민간 클라우드 서비스를 이용할 수 있도록 보안성을 검증**하는 제도('16년~)

※ 클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제23조의2 및 「클라우드컴퓨팅 서비스 보안인증에 관한 고시」

○ **(인증대상)** 국가기관 등의 업무를 위해 제공하는 **민간 클라우드 서비스**

○ **(인증유형)** IaaS, SaaS(표준, 간편), DaaS, 하등급(IaaS, SaaS, DaaS)

< 인증유형 > * 괄호 : 인증 평가항목 개수

서비스 유형	기존인증제	등급제(하등급 우선시행)
IaaS	IaaS(116개)	下(64개)
SaaS	SaaS 표준(79개)	-
	SaaS 간편(31개)	下(30개)
DaaS	DaaS(110개)	下(64개)

※ 상·중등급(고시개정 이후) 시행 전까지 기존 인증제에 따라 인증 신청 가능

○ **(인증절차)** 보안인증 신청 시 **예비점검 및 수수료 청구**를 거쳐 **인증평가**를 진행하며 **인증위원회**의 심의 결과에 따라 **인증서 발급**(평균 2.5~5개월 소요)

신청접수	▶	예비점검	▶	수수료 청구	▶	인증평가	▶	인증위원회
서류제출		신청서류 검토		수수료* 납부		본점검(1개월) → 보완조치(1~3개월) → 이행점검(1개월)		심의 및 인증서 발급(0.5개월)

- 서비스 유형별로 자산규모(서버, PC 등 자산 수)를 고려하여 수수료 산정