동남정보보호지원센터

과학기술정보통신부 Ministry of Science and ICT

KISA 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY

부산광역시 BUSAN METROPOLITAN CITY

부산정보산업진흥원 Busan IT Industry Promotion Agency

지역정보보호지원센터 운영목적

지역 중소기업의 정보보호 수준제고 및
침해사고 예방·대응 역량강화를 통한 정보보호 산업 활성화

지역정보보호지원센터 구축현황 (전국 10개소)

ICT 중소기업 정보보호 지원 사업

지역 전략산업 영위기업 및 침해사고 피해기업을 대상으로
맞춤형 정보보호 컨설팅, 보안솔루션 지원을 통해 지역 정보보호 내재화 촉진

정보보호 컨설팅 및 보안솔루션 지원

- 지원내용 :컨설팅(500만원) 보안솔루션 도입비용(최대540만원)
- 지원규모 : 9개사

신청 및 선정 (신청 접수 및 대상 선정) → 컨설팅 지원 (지역 전략산업 분야 정보보호 컨설팅) → 보안솔루션 지원 (컨설팅 기반 보안솔루션 지원) → 사후 관리 (이행점검 및 만족도 조사)

클라우드 기반 보안서비스(SECaaS)지원

- 지원내용 : 보안서비스 도입비용 (최대495만원)
- 지원규모 : 49개사

신청 및 선정 (신청 접수 및 대상 선정) → 보안서비스지원 (보안서비스 도입 지원) → 사후관리 (이행점검 및 만족도 조사)

중소기업 정보보호 서비스 지원

지능형 CCTV 성능 시험인증

제공 서비스

- 한국인터넷진흥원이 구축한 영상DB를 통해 솔루션이 영상 DB내 특정이벤트를 판별할 수 있는지 시험하고 점수를 산출해 주는 서비스
  ※ '지능형 CCTV 성능시험·인증'은 지능형 CCTV 산업 활성화를 위하여 현재 무료로 진행되고 있음

평가 분야

- 일반 분야
  배회, 침입, 유기, 싸움, 방화, 쓰러짐, 마케팅, 낙상, 익수자 탐색, 실종자 수색
- 일반 분야
  교통사고, 화재, 범죄, 생활안전, 자살(추가예정), 감염병(추가예정)

시험 절차

시험 준비 → 시험 신청 → 사전 시험 → 본 시험 → 인증

동남정보보호지원센터

과학기술정보통신부 Ministry of Science and ICT
KISA 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY
부산광역시 BUSAN METROPOLITAN CITY
부산정보산업진흥원 Busan IT Industry Promotion Agency

한국인터넷진흥원 연계 기업 지원

내 서버 들보미

내 서버 들보미란 ?

내 서버 들보미 서비스는 기업에서 운영중인 서버에 대한 보안취약점 원격 점검 서비스입니다.
본 서비스를 통해 귀사 정보자산의 보안위협을 제거하고 사이버보안 면역력을 강화할 수 있습니다.
서비스 이후 자율적으로 서버의 보안취약점을 식별하고 조치할 수 있는 자가진단도구를 제공합니다.

서비스 대상

- 지원 대상: 중소기업기본법 제2조 제1항에 의거한 중소기업
- 모집 기간 및 규모: 상시모집 '영세·중소기업 350개'
- 점검대상: 기업의 주요서버 WEB/WAS, DB 서버 등

서비스 내용

서버 원격보안점검

구 분	Windows 계열	Linux/UNIX 계열
진단 분야	CCE, CVE, 침해사고 흔적 등	
진단 범위	OS, WEB/WAS, DBMS, 오픈소스 SW 등	
진단 항목	10개 영역 104개 항목	10개 영역 93개 항목

현장 방문 점검

현장방문 요청 시 기업의 정보보호 정책, 조직, 자산 보안, 물리 보안, 접근 통제, 운영 보안 등 기업의 정보보호 관리체계 점검 추가 제공 (서버 보안 점검 포함)

- 7개 영역 17개 항목

+

자가진단 도구 제공

기업 자체 서버 보안점검 및 취약점 관리를 위한 자가진단도구 제공
Windows, Unix 서버의 보안점검 도구
서버별 보안점검 결과 통합관리

+

온라인 보안교육(매월)

매월 실무현장 중심의 교육 프로그램 제공
최신 취약점 대응기술 교육(이론, 실무)
최신 정보보호 동향 및 보안트렌드 소개

이행 점검

직접 조치가 어려운 경우 전문 컨설턴트를 통한 취약점 즉시 조치 지원
점검 시 자산의 중요도 및 위협도에 따라 취약점에 대한 조치 계획 수립을 지원하고 조치 계획에 따른 이행여부 점검

서비스 절차

원격보안점검 신청 시
신청/접수 → 신청서 검토 → 사전협의 → 보안점검 → 개선지원

자가진단도구 신청 시
신청/접수 → 신청서 검토 → 신청서 검토

사이버 위기대응 모의훈련

사이버 위기대응 모의훈련이란 ?

사이버 공격 예방 및 피해 최소화를 위해 기업의 보안수준 강화와 임직원 인식을 제고하고자 실전형 모의훈련을 실시하고 있습니다.
다양한 분야의 많은 민간 기업에 기회를 제공하기 위하여 모의훈련 참가기업을 공개모집하고 있습니다.

서비스 대상

- 지원 대상: 민간기업 전체 (대기업, 비영리 등 참여대상 제한 無)
- 훈련기간: 신청기간 및 훈련기간 추후 별도공고
- 훈련대상: 해킹메일, 디도스공격 모의 침투, 취약점 탐지대응

※ 단, 훈련 수행 예산 및 인력의 한정으로 인해 참여에 제한이 있을 수 있음

서비스 내용

해킹메일

임직원 대상으로 최신 유행하는 사회공학적 해킹메일을 발송·훈련

디도스 공격

홈페이지 대상 디도스 공격 (최대 20Gbps)수행

모의침투

국제 해킹대회 입상자를 활용한 홈페이지 실전 모의침투 수행·조치 안내

취약점 탐지 대응

외부에 공개된, 대외 서비스(홈페이지, 메일 등)를 제공하는 서버 대상 보안 취약점, 보안 약점, 알려진 포트(well known) 등을 점검
보안 장비가 없어도 신청 가능

서비스 절차

1. 서비스 모집
   - 참여기업 공개 모집: 보호나라, C-TAS웹사 등
   - 훈련방법 안내: 사전설명회, 전화, 메일 등
2. 훈련
   - 실전: 해킹메일, 디도스공격, 모의침투, 취약점 탐지대응
3. 결과
   - 훈련결과 모범사례 최신동향 공유 우수기업 시상

동남정보보호클러스터

Information Security Cluster

과학기술정보통신부 Ministry of Science and ICT
KISA 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY
부산광역시 BUSAN METROPOLITAN CITY
경상남도 GYEONGNAM

주관기관 부산정보산업진흥원 Busan IT Industry Promotion Agency

참여기관 경남테크노파크 Gyeongnam Technopark
울산정보산업진흥원 UIPA
부산대학교 PUSAN NATIONAL UNIVERSITY
KR 케이알
WINETECHNET

지역 거점 정보보호 클러스터 구축 사업 목적

배경	동남권은 국가 기간산업 집적지로 사이버 위협에 노출되어 있어 막대한 피해가 예상됨에 따라 지역 전략산업의 안전한 디지털 전환 견인과 지역 정보보호 사각지대 해소 필요
목적	지역 전략산업과 연계한 지역 거점 정보보호 클러스터 구축을 통해 지역 내에서 성장하는 정보보호 산업 생태계 조성
3대 특화산업	스마트오션, 스마트시티, 스마트공장
위치	부산광역시 해운대구 센텀중앙로55, 동서대학교 센텀캠퍼스 7층~8층
면적	약 400평 (전용면적 : 1,306.32㎡)
개소일	2023년 12월 21일

정보보호 기업 발굴 및 육성

시큐리티 캠퍼스
대학동아리 발굴 및 프로그램 운영을 통한 창업촉진 및 정보보호 분야 스타트업 육성

지역특화산업(스마트오션) 분야 정보보호 제품 및 서비스 개발 지원을 위한 신규 비즈니스 모델 도출

지역특화기반 정보보호 비즈니스 모델 발굴

정보보호 서비스 개발 및 사업화 지원
지역특화산업(스마트오션·스마트시티·스마트공장)과 정보보호를 융합한 서비스 개발 및 사업화를 통하여 지역 정보보호 산업의 고부가가치 창출

지역특화 분야 맞춤형 해외 마케팅을 통한 신시장 발굴 및 판로 개척 확대

맞춤형 국내외 마케팅 지원

입주지원 시설 운영
정보보호 분야 기업 발굴 및 육성을 위한 입주공간 제공

정보보호 네트워크 활성화

사이버 시큐리티 위크
사이버공방전(핵시움)을 통해 지역 정보보호 우수인재를 발굴하고 정보보호산업에 대한 인식향상 기대

정보보호 세미나
- 동남권 정보보호 지산학 네트워킹 구축을 통한 기업의 애로사항 등 의견 수렴
- 정보보호산업 발전방안에 대한 특강 개최를 통한 네트워킹 구축의 장 마련

지역·광역 공동협의체 운영
- 동남권 지역 전문가 구성 및 운영을 통한 지역 특화산업과 보안 접목 기술 발굴
- 도출된 기술을 향후 정책수립 및 동남권 클러스터 내 활용하여 기대효과 창출

정보보안 통합 플랫폼 운영
- 보안 취약점에 대한 온라인 접수창구 역할을 통해 지역 산업의 보안위협을 탐지·예방하고 사업홍보 및 대관, 교육에 대한 정책수요자의 접근성 향상

정보보호 전문인재 양성

취업연계
- 미취업 청년층
- 보안 컨설팅, 보안관제, 보안장비 기술 엔지니어링 양성

대학연계
- 지역 재학생 (석박사)
- 지능형사물인터넷 보안, 지역특화 산업별 고급인재 양성

최종목표
최정에 화이트해커, 지도자급 정보보안 인재양성

기업연계
- 지역(수요)기업 재직자
- 지역특화(스마트오션·시티·공장) 보안 실무자 양성

컨설턴트 양성
- 관련분야 재직자 등
- 지역기업 보안취약점 개선방안 도출 지역산업 보안 컨설턴트 양성

동남정보보호클러스터

Information Security Cluster

과학기술정보통신부 Ministry of Science and ICT
KISA 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY
부산광역시 BUSAN METROPOLITAN CITY
경상남도 GYEONGNAM

주관기관 부산정보산업진흥원 Busan IT Industry Promotion Agency
참여기관 경남테크노파크 Gyeongnam Technopark
울산정보산업진흥원
부산대학교 PUSAN NATIONAL UNIVERSITY
KR
WIN-TECHNET

정보보호 산업기반조성

정주여건 우수성	120여개에 달하는 지역 디지털 인프라 집적
클러스터 집적단지	정보보호클러스터를 통해 역외 우수 기업 유치 거점
접근 편의성	부·울·경 권역 1시간 생활권 중심지

동남정보보호 클러스터 시설현황

소재지
동서대학교 센텀캠퍼스 7~8F

총면적
1,306.4㎡ (약400평)

보안테스트베드 운영

동남권 특화산업(*스마트오션, 스마트시티, 스마트공장)에 대한 보안취약점 분석 환경 제공을 통한 지역 정보보호 수준 제고 및 정보보호 대응 역량 강화 기반 마련

*스마트오션 : 해운, 항만, 조선

지원내용

- 지원대상 : 스마트시티·선박·공장 분야 수요·공급 기업, 연구기관 및 대학 등
- 주요대상 : 스마트선박·공장 테스트베드 구축 및 보안 위협에 따른 대응 방안 지원 등

구분	내용
스마트시티 (부산)	- 지능형 CCTV 솔루션의 사용 확산 및 신뢰도 향상 - 스마트시티 IoT 디바이스 보안시험 환경 및 점검도구 제공
스마트선박 (부산)	- 스마트선박 보안테스트베드 확장 (자율항해시스템, 통신시스템 등) - 스마트선박 보안취약점 분석 및 훈련 시나리오 개발 - 해사사이버보안 훈련 시범 운영
스마트공장 (경남)	- 스마트공장 Wall 제작과 OT 데이터 수집 및 분석 - 스마트공장 보안 점검 자동화 환경 구축 - 산업제어시스템 시각화 구축 및 운영 / 유지보수 방안 마련

입주지원시설 운영

정보보호 분야 관련 기업 발굴 및 육성함으로써
지역 내 정보보호 산업 생태계를 조성하기 위한 입주 공간 운영

지원내용

구분	내용
지원대상	- 정보보호 분야 아이디어 및 기술을 보유한 예비창업자, 사업자, 기업부설연구소 - 정보보호 분야로 입주 전환을 희망하는 사업자 - 정보보호 분야 관련 활동 및 성과를 보유한 협회 등
지원내용	[공간지원] 동남정보보호클러스터 내 사무공간 및 공용공간 제공 [비용지원] 전기료 수도광열비, 네트워크망(인터넷) 비용지원 ※ 예비창업자 대상 보증금, 임대료(리퍼 등 무상지원 [네트워킹] 입주기업 대상 네트워킹 및 역량강화 프로그램 지원 [사업지원] 동남정보보호클러스터 및 동남정보보호지원센터 사업 연계지원

정보보호 대학동아리 지원

동남권 정보보호 대학동아리 발굴·육성을 통한 정보보호 인력육성
동아리 운영을 통한 네트워킹 형성 및 확대

지원내용

- 지원대상 : 동남권 특화산업과 연계한 정보보호 동아리 대상
- 주요대상

구분	내용
스터디모임	정보보호 스터디 모임 운영(동아리별 5회 내외) - 동아리별 프로젝트 계획서 기반 역량 강화를 위한 스터디 모임 진행 - 정보보호 전문가 섭외를 통한 동아리별 스터디 모임 매칭
전문교육	정보보호 전문교육 운영(2회 이상) - 정보보호 단기 교육 진행(1주 교육) - 교육 회차별 실습 중심 커리큘럼 구성을 통한 교육 운영
기관·업 필드투어링	정보보호 기관·업 필드투어링 개최(1회) - 수도권 정보보호 기업 현장방문을 통한 체험 기회 마련
동아리 활동비 지원	정보보호 대학 동아리 활동비 지원 등 - 대학 동아리별 활동비 지원(정보보호 관련 활동 기반)