

보도 시점 2026.5.28. (목) 12:00
(2026.5.29. (금) 조간)

배포 2026.5.28. (목) 09:00

“민·관·국민 삼각 공조로 보안구멍 미리 찾아 막는다” 국내 첫 ‘보안취약점 상시 신고조치제’, 시범사업 실시

- 19세 이상 국민 누구나 착한 해커(화이트해커)로 참여 가능,
통신·게임·금융 기술 서비스(핀테크) 등 국민 생활 밀접 기업과
공공 기관의 보안 선제 점검 -

- △ [실전형 검증/투명 공개] 단순 제품 점검의 기존 모의해킹, 신고 포상제 한계를 넘어 실제 운영 망 등에 대해 취약점 실전 탐색, 조치 후 공개
- △ [선도기관 솔선수범] 숨기는 보안에서 열린 보안으로 사후조치에서 사전 예방으로의 패러다임 전환을 위해 15개 민간기업·공공기관 자발적 참여
- △ [철저한 안전장치] 참여 화이트해커 대상 사전 윤리교육, 정보 유출방지 서약, 개인정보 처리위탁 등 부작용 방지를 위한 통제장치 철저 운영
- △ [글로벌 스탠다드化] 시범사업 발판, '27년부터 美·EU와 같이 제도화 추진

국가인공지능전략위원회 (위원장 이재명 대통령, 이하 ‘위원회’), 과학기술정보통신부(부총리 겸 과학기술정보통신부장관 배경훈, 이하 ‘과기정통부’), 국가정보원(이하 ‘국정원’), 한국인터넷진흥원(이하 ‘KISA’)은 5.28일(목), 안전하고 투명한 보안 생태계 구축을 위해 국내 최초로 「보안 취약점 신고·조치·공개(CVD/VDP*) 제도」 (이하 ‘보안취약점 상시 신고조치제’) 시범 사업을 전격 추진한다고 밝혔다.

* 화이트해커가 자사 취약점을 합법적으로 찾고 신고할 수 있도록 하는 ‘취약점 공개 정책’(VDP : Vulnerability Disclosure Policy)과 ‘신고된 취약점을 조치한 이후에 공개하는 정책’(CVD : Coordinated Vulnerability Disclosure)을 의미

보안취약점 상시 신고조치제는 기존 공공기관·민간기업 등에서 일시적 이벤트 형태로 제품·가상 망을 대상으로 운영하는 모의해킹, 취약점 신고 포상제(분기별) 등과 달리, 실제 운영 망 등에 대해 365일/24시간 선의의 정보보호 연구자(‘화이트해커’)가 취약점을 탐색할 수 있도록 하는 정책(VDP)을 공개하고, 이를 준수하는 범위 내에서 화이트해커가 취약점을 발굴·신고하면 피신고 기업/기관이 조치 이후 투명하게 공개하는 정책(CVD)이다. 이 제도는 이미 미국·유럽 등에 널리 운영되고 있었으나 국내에는 운영되지 않고 있다.

※ (美) 공공기관 의무화, 민간기업은 자율이나 공공조달 제품에 해당제도 운영 요건 필수화
(EU) 공공기관 의무화, 민간기업도 에너지·운송·우편 등 국민 생활 필수/중요 분야 의무화

정부는 지난해 연쇄 대형 보안사고를 계기로 상시적이고 선제적, 실전형 대응 체계의 필요성을 인식하고 동 제도를 포함한 「정보보호 종합대책(’25.10월, 국가안보실 주도 범정부 합동)」과 「국내 보안취약점 신고·조치·공개 로드맵(’26.2월, AI전략위원회 보안특위)」을 수립하는 등 해당 제도의 국내 도입을 추진 중이다.

이번 시범 사업은 내년부터 본격 추진될 제도화에 앞서 대국민 인식 제고와 그 실효성을 사전에 검증하기 위한 목적으로 추진된다. 특히 최근 미토스發 AI기반 상시적 해킹 위협이 현실화 됨에 따라, 환경 변화에 발맞춘 실전적/상시적 방어 역량 향상을 위해 참여 화이트해커들의 AI활용 해킹도 시범 사업에서 허용할 방침이다.

1. (참여 기관·기업) 총 15개, 민간기업(7개)/공공기관(8개) 참여

민간의 경우 통신사·게임·금융/핀테크 등 사고발생 시 대규모 피해가 예상되는 분야 기업들이, 공공의 경우 안전·보건·의료·전력·교통 등 대국민 밀접 서비스를 제공하는 기관들이 자발적으로 참여하여 자사 실제 운영 망/제품 등에 대해 화이트해커의 취약점 탐색 활동을 허용한다.

< 투명하고 선제적인 K-보안 생태계 조성 기여, 선도기업·기관 목록 >

민간 (7)	[통신] LG유플러스, [게임] 넥슨, 엔씨, [금융/핀테크] 토스페이먼츠, 삼성생명, [보안] 이스트시큐리티, 잉카인터넷
공공 (8)	[안전] 국민안전24(행안부), [보건의료] 건강보험심사평가원(심평원), 예방접종도우미(질병청), [전력] 한전ON(한국전력), [교통] 국가교통정보센터(국토부), 사이버검사소(한국교통안전공단), [기타 : 경제·채용] 경제통계시스템(한국은행), 공공기관 채용정보시스템(재경부)

2. (정보보호연구자(‘화이트해커’)) 대한민국 국적 보유 19세 이상 누구나 참여 가능

참가 화이트해커는 대한민국 국적 보유 19세 이상 누구나 신청할 수 있으며, 인원 규모는 별도 제한을 두지 않는다. 다만 실제 운영 망에 대한 취약점 발견 과정에서 개인정보 유출, 망 운영저해 등 국민·기업의 피해를 방지하기 위해 △ 기업/기관별 취약점 탐색 허용 정책(대상 사이트, 허용 범위 등) 마련, △ 화이트해커 관련 내용 숙지와 사전 윤리교육 이수, △ 해당 정책 준수 서약 및 개인정보 처리 위탁 체결 등 보완 장치를 마련해 운영해 나갈 계획이다.

3. (추진 일정) (5.29일 ~ 6.12일) 화이트해커 참가 접수 → (6월) 사전 윤리 교육, 참가 승인 → (~11월) 취약점 탐색/신고/조치 → (연말) 결과 공개

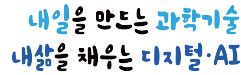
5월 29일부터 6월 12일까지 2주간 홈페이지(<https://www.cvdvdp.kr>)를 통해 대국민 참가 희망 화이트해커 접수가 진행된다. 이후 참가자 교육과 승인 절차를 거쳐 6월 이후 본격적인 취약점 탐색/신고/조치 활동이 약 5개월간 지속된다. 최종 발견된 취약점과 조치 결과 등은 연말 공개될 예정이며 우수 취약점을 발굴한 화이트해커에게는 공공과 민간을 통틀어 총 16점의 상장과 2,000만 원 규모의 상금 수여 등 격려 체계도 운영한다.

배경훈 위원회 부위원장이자 부총리 겸 과학기술정보통신부 장관은 “AI 시대 보안은 국가 경제와 안보를 지탱하는 핵심기반이라며, 미토스 사태가 촉발한 AI기반의 상시 위협에 대응하기 위해서는 실전적이고 선제적인 보안 체계 도입이 불가피 하다”고 강조했다. 아울러 “이번 시범 사업을 마중물 삼아 보안취약점 상시 신고조치제의 성공적인 도입과 안착 등 투명하고 안전한 K-보안 생태계 조성에 적극 기여하겠다”고 밝혔다.

국정원도 “국가 사이버보안 분야에서 중요 파트너인 화이트해커의 전문성을 통해, 국가·공공기관의 잠재적 취약점을 사전에 발굴하고 개선할 수 있기를 기대한다”며, “보안취약점 상시 신고조치체가 조기에 정착할 수 있도록 시범 사업 진행에 만전을 기하겠다”고 강조했다. 끝.

붙임1, 붙임2 : 인포그래픽

담당 부서	국가인공지능전략위원회 AI데이터·규제혁신팀	책임자	팀장	유경태 (02-2224-4131)
		담당자	사무관	강영근 (02-2224-4138)
담당 부서	과학기술정보통신부 사이버침해대응과	책임자	과장	백대현 (044-202-6460)
		담당자	사무관	이재원 (044-202-6467)



CVD/VDP 시범사업 참가 개요

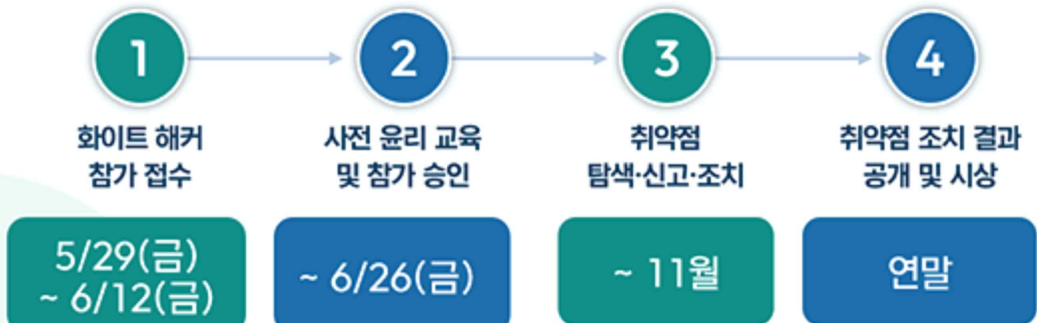
참가신청 홈페이지 
www.cvdvdp.kr

※ 문의 : 02-405-6697, cvd@kisa.or.kr

아래 조건을 모두 충족한 자만 참가 가능

- 1  만 19세 이상의 대한민국 국적자
- 2  참가 신청서 제출
- 3  개인정보 수집·이용 동의서 제출
- 4  취약점 공개 정책(VDP) 준수 및 보안서약서 제출
- 5  개인정보처리 위탁 계약 체결
- 6  시범사업 사전 윤리교육 이수

📅 추진 일정



※ 실제 운영망 등이 대상인 관계로 철저한 사전교육 이수, VDP 준수 서약서 등 관련 서류 제출 필요

보안 취약점 상시 신고조치제 특징

- 기존 모의해킹 / 취약점 신고포상제와 차이 중심 -

구분	모의해킹 / 취약점 신고 포상제	보안취약점 상시 신고조치제
 점검 대상	 가상망 / 제품 위주	 실제 운영망 포함
 기간	 정해진 특정 기간 위주 (모의해킹)	 365일 / 24시간 상시 신고·조치
 취약점 조치	 기업 / 기관 자율 조치	 VDP에 따라 신고 취약점 조치
 취약점 공개	 기업 / 기관 자율 공개	 조치 후 협의하 공개
 법적 보호	 사고 시 면책 없음	 VDP 준수 시 법적 보호