대통령직속 국가인공지능전략위원회 | 보도자료 | 과학기술정보통신부 | 국가정보원 NATIONAL INTELLIGENCE SERVICE

보도 시점 2026.11.23.(월) 12:00 (2026.11.24.(화) 조간) 배포 2026.11.23.(월) 09:00

“민·관·국민이 함께 찾은 보안구멍, 미리 막았다” 국내 첫 ‘보안취약점 상시 신고조치제’ 시범사업 성과공유회 개최

- 화이트해커 698명 참여, 유효 취약점 202건 전수 조치로 선제적 보안체계 실효성 확인 -

△ **[취약점 사전 차단]** 실제 운영 서비스 대상 **취약점 1,343건 신고**, **유효 취약점 202건 전수 조치**

△ **[민·관·국민 협력] 민간기업(7개)·공공기관(8개)**과 **화이트해커 698명이 참여**한 국내 첫 실전형 시범사업

△ **[안전한 운영] 사전 윤리교육·보안서약** 등 안전장치를 통해 **시범사업 기간 중 서비스 장애 0건**

△ **[제도화 본격 추진]** 시범사업 성과와 현장 의견을 토대로 **’27년부터 美·EU와 같이 제도화** 추진

국가인공지능전략위원회(위원장 대통령, 이하 ‘위원회’), 과학기술정보통신부(부총리 겸 과학기술정보통신부장관 배경훈, 이하 ‘과기정통부’), 국가정보원(이하 ‘국정원’), 한국인터넷진흥원(이하 ‘KISA’)은 11.23.(월) 서울 엘리에나 호텔에서 **국내 최초**로 추진한 **「보안 취약점 신고·조치·공개(CVD/VDP*) 제도」**(이하 ‘보안취약점 상시 신고조치제’) **시범사업 성과공유회 및 시상식을 개최했**다고 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

정부는 **지난해 연쇄**적으로 발생한 **대형 보안사고**를 계기로 기존의 사후 대응 중심 보안체계를 상시적·선제적 예방체계로 전환하기 위해 **「정보보호**

종합대책('25.10월, 국가안보실 주도 범정부 합동)」과 **「국내 보안취약점 신고·조치·공개 로드맵**('26.2월, AI전략위원회 보안특위)」을 수립한 바 있다.

이에 따라 지난 5월 **국내 최초**로 **보안취약점 상시 신고조치제 시범사업**에 착수했으며, 이번 **성과공유회**에서는 **약 5개월간**의 **사업 추진 경과**와 **주요 성과를 공유**하고 **우수 화이트해커**에 대한 **시상을 진행**했다.

특히 이번 시범사업은 기존의 일회성 모의해킹이나 제품 중심 취약점 점검에서 벗어나, **실제 운영 중인 서비스**에 대해 **화이트해커**가 사전에 허용된 범위 내에서 **취약점을 탐색·신고**하고, 기업·기관이 이를 검증·조치하는 **실전형 보안체계**를 **국내 최초로 검증**했다는 데 의의가 있다.

이를 통해 '사후조치에서 **사전예방**으로, 숨기는 보안에서 **열린 보안**으로'의 **보안 패러다임 전환 가능성**을 **확인**했다.

1. (추진 경과) 민간기업(7개)/공공기관(8개) 참여, 화이트해커 698명 참여

이번 시범사업에는 **통신·게임·금융·보안 분야 민간기업 7개사**와 **안전·보건·의료·전력·교통 등 국민 생활과 밀접한 공공서비스**를 제공하는 **8개 기관**이 자발적으로 참여했다.

지난 5월 29일부터 6월 12일까지 진행된 참가자 모집에는 **총 698명의 화이트해커가 참여**했으며, **사전 윤리교육과 보안서약** 등 필요한 절차를 거쳐 취약점 탐색·신고 활동을 수행했다.

특히 **실제 운영 서비스를 대상**으로 하는 만큼 기관별 취약점 탐색 허용 범위와 준수사항을 사전에 명확히 하고, **개인정보 유출과 서비스 장애 등**을 **방지**하기 위한 **안전장치를 마련**했다.

< 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), **[복지의료]** 건강보험심사평가원(심평원), 예방접종도우미(질병청), **[에너지]** 한전ON(한국전력), **[교통]** 국가교통정보센터(국토부), 사이버검사소(한국교통안전공단), **[경제]** 경제통계시스템(한국은행), 공공기관 채용정보시스템(재경부)

2. (주요 성과) 유효 취약점 202건 발굴·전수 조치, 서비스 장애 0건

참여 화이트해커들은 각 기업·기관이 사전에 공개한 취약점 공개 정책(VDP)에 따라 지난 **6월 29일부터 7월 24일까지 약 4주간 실제 운영 서비스**의 **취약점**을 **탐색·신고**했다.

그 결과 **총 1,343건의 취약점 신고가 접수**됐으며, 유효성 검증을 통해 최종 **202건의 유효 취약점**을 **확인**했다. **참여 기업·기관**은 발견된 **유효 취약점**에 대한 **패치·보완 등을 모두 완료**했다.

또한 사전 윤리교육과 기관별 취약점 탐색 허용 범위 설정 등 안전장치를 운영한 결과, 시범사업 기간 중 취약점 탐색 활동에 따른 **서비스 장애는 발생하지 않았다.**

이는 화이트해커의 전문성과 기업·기관의 자발적 참여를 결합해 실제 운영 환경에서도 서비스 장애를 유발하지 않고 잠재적 보안 위협을 사전에 발견·개선할 수 있음을 보여준 성과다.

3. (우수자 시상) 우수 화이트해커 16명에 상장·상금 총 2,000만 원 수여

이날 성과공유회에서는 시범사업에 적극적으로 참여하고 우수 취약점을 발굴한 **화이트해커 16명**에게 **상장**과 **총 2,000만 원의 상금**을 **수여**했다.

민간부문 우수 화이트해커에게는 과기정통부장관상 8점과 상금 총 1,000만 원을, 공공부문 우수 화이트해커에게는 국정원장상 8점과 상금 총 1,000만 원을 각각 수여했다.

정부는 이번 시상을 통해 취약점 발굴과 책임 있는 신고·조치에 기여한 화이트해커들의 성과를 격려하고, **민·관·국민**이 **함께 참여**하는 **보안문화 확산의 계기**를 **마련**했다.

4. (현장 의견) 상시 취약점 점검 필요성 공감, 법적 보호·전문기관 지원 과제 확인

시범사업에 참여한 화이트해커 52명과 민간기업 7개사를 대상으로 설문조사를 실시한 결과, **화이트해커의 81%**가 **개별적인 사전 동의 없이도** 정해진 기준에 따라 **상시적**으로 **취약점을 점검**할 수 있는 **제도의 필요성에 공감**한 것으로 나타났다. 참여 기업에서도 이에 대한 반대 의견은 제시되지 않았다.

다만 **화이트해커**들은 취약점 탐색·신고 과정에서 발생할 수 있는 **법적 처벌 위험**을, **참여 기업**들은 **서비스 장애 우려**와 **신고된 취약점의 분석·검증 부담**을 주요 개선 과제로 제시했다.

특히 **참여 민간기업 7개사** 모두 신고된 취약점의 검증과 원활한 보안 조치를 위한 **전문기관의 지원**이 **필요**하다는 의견을 제시했다.

5. (향후 계획) '27년부터 보안취약점 상시 신고조치제 제도화 본격 추진

정부는 이번 시범사업에서 확인된 성과와 현장 의견을 토대로 보안취약점 **상시 신고조치제**의 **제도화**를 본격 추진할 계획이다.

특히 미국·EU 등 해외 주요국의 운영 사례를 참고하여 화이트해커가 명확한 기준과 법적 보호 아래 안심하고 취약점을 신고하고, 기업·기관은 예측 가능한 절차에 따라 취약점을 검증·조치할 수 있는 제도적 기반을 마련할 방침이다.

아울러 신고된 취약점에 대한 전문적인 검증·분석 지원과 조치 이후의 책임 있는 공개 절차 등 시범사업 과정에서 확인된 개선 과제를 관계기관과 함께 검토해 나갈 예정이다.

이를 통해 보안취약점을 숨기거나 사고 발생 이후에 대응하는 방식에서 벗어나, 민·관·국민이 함께 위험을 사전에 발견하고 개선하는 투명하고 선제적인 K-보안 생태계를 조성해 나갈 계획이다.

하정우 국가인공지능전략위원회 상근부위원장은 "AI 기술의 발전으로 **사이버 위협**이 더욱 **지능화·고도화**되는 상황에서, 이번 시범사업은 **민·관·국민**이 함께 **보안취약점**을 사전에 발굴·조치함으로써 **선제적 보안체계**의 **가능성**을 **확인**했다는 점에서 의미가 크다"며, "앞으로 **보안취약점 상시 신고조치제**의 **법·제도적 기반**을 **마련**하는 한편, **11월 12일 출범**한 **'국가 사이버 복원력 강화 TF'**를 **중심**으로 **사전 예방**부터 **사고 대응·복구**까지 아우르는 **사이버복원력 중심**의 **보안체계**를 **고도화**하고, 관련 **정책의제**를 **선제적**으로 **발굴**해 나가겠다"고 밝혔다.

배경훈 부총리 겸 과기정통부 장관은 “이번 시범사업은 **화이트해커**와 **기업·기관**이 **함께** 실제 운영 서비스의 **보안취약점을 사전에 찾아내고 개선**할 수 있음을 확인한 뜻깊은 성과”라며, “적극적으로 참여해 준 화이트해커와 선도 기업·기관에 감사드린다”고 밝혔다.

이어 “AI 기반의 사이버 위협이 갈수록 고도화·상시화되는 상황에서 **민간의 전문성과 자발적인 참여**를 활용한 **선제적 보안체계가 중요**하다”며, “시범사업 성과를 바탕으로 기업들이 안심하고 취약점을 신고받고 신속하게 조치할 수 있는 환경을 조성해 나가겠다”고 강조했다.

국정원은 “이번 시범사업을 통해 **화이트해커**와의 **협력**이 **잠재적 보안취약점**을 **선제적**으로 **발굴**하는 효과적인 예방 수단이 될 수 있음을 확인했다”며, “앞으로도 공공부문에서 보안취약점 상시 신고조치제가 안정적으로 정착할 수 있도록 제도 정비 등에 만전을 기하겠다”고 밝혔다.

담당 부서	국가인공지능전략위원회 지원단 AI데이터・규제혁신팀	책임자	팀 장	유경태 (02-2224-4131)
		담당자	사무관	강영근 (02-2224-4138)
담당 부서	과학기술정보통신부 사이버침해대응과	책임자	과 장	김단호 (044-202-6460)
		담당자	사무관	이재원 (044-202-6467)

대체불가 대한민국 내일을 만드는 과학기술 내삶을 채우는 디지털·AI 대한민국 정책브리핑 OPEN 출처표시 공공누리 공공저작물 자유이용허락