ICT Expert Interview

김재성 TTA 정보보호기술위원회(TC5) 의장,
한국인터넷진흥원, 한림대학교 겸임교수

01.

1. ICT 환경이 급변함에 따라 전통적인 보안의 개념도 변화하고 있습니다. 거의 모든 분야에서 보안을 고려해야 할 만큼 보안의 개념이 크게 확장됐는데, 이러한 변화를 일으킨 핵심 요인은 무엇이라고 생각하시는지요?

재택근무의 확대, 국가간 기술무역 갈등, 금리변동과 무역 불균형 등 여러 분야에서 국내외적으로 변화가 일어나면서 사회·경제·정치·군사 등 모든 분야에서 정보보호의 중요성이 커졌습니다. ChatGPT와 같은 인공지능 챗봇, 무인 자율주행차, 양자컴퓨팅 등의 등장으로 새로운 보안 개념의 확장도 불가피해졌습니다.

이러한 상황에서 금융분야의 역할이 컸습니다. 금융분야는 마이데이터 도입 이전에도 신용정보집중기관을 중심으로 개인의 다양한 금융거래 정보가 집중되었고, 이러한 정보를 바탕으로 개인의 신용을 평가함으로써 거래 안전을 도모해왔습니다. 특히 정보 전송 인프라가 잘 갖춰져 있었기 때문에 전송요구권에 따라 개인정보가 이동하는 것이 개념적으로나 기술적으로 수용하기 수월했습니다. 금융 관련 정보가 정형화된 정량 정보라 표준화에 필요한 노력이 적었던 것도 특징입니다. 나아가 전송요구권의 수범자들인 금융회사들이 허가를 받아 사업을 수행하고, 상대적으로 강한 산업규제를 받아왔기 때문에 마이데이터라는 법제도에 대한 수용성이 상대적으로 높았다고 생각합니다.

02.

보안의 적용 분야가 다양해지는 만큼 기술이나 제도가 적용되는 영역 및 층위도 다변화되고 있습니다. 최근의 보안 이슈를 간략하게 분류한다면 어떻게 구분할 수 있을까요?

글로벌 환경이 빠르게 변화하면서 정보보호의 중요성이 날로 증대되는 상황에서 다각적인 관점에서 다음과 같이 정보보호기술을 구분해 보고자 합니다. 데이터 생태계 관점에서 데이터 보안·개인정보 보안, 산업 및 유통 생태계 관점에서 공급망 보안·물리 보안, 정보통신망 인프라관점에서 유무선 네트워크 보안·사이버 보안, 정보보호 관점에서 암호기술·사용자 인증기술·접근통제기술·정보관리체계 보안·보안성 평가기술 등 공통기반 보안, 소프트웨어와 하드웨어 인프라 관점에서 AI 보안·로봇 보안·양자정보통신 보안기술·스마트카 보안·디지털 헬스케어 보안·텔레바이오인식기술·모빌리티 보안 등 차세대 융합보안기술로 분류할 수 있습니다.

03.

정보의 원활한 유통과 신뢰성을 보장해서 데이터 인프라가 매끄럽게 작동하게 하는 것이 보안의 역할이라고 생각됩니다. 미래의 보안은 어떤 요건을 갖춰야 할까요?

정보보호의 근간은 데이터 무결성, 기밀성, 가용성을 보장하는데 목적이 있다. 급변하는 미래 환경에 능동적으로 대처하기 위한 보안기술의 요건으로는 무결성 보장 관점에서 데이터 보안·개인정보보호·모바일 비대면 사용자 인증·AI 보안·로봇 보안·스마트카 보안·디지털 헬스케어 보안·텔레바이오인식기술·모빌리티 보안 등을 꼽을 수 있습니다. 기밀성 보장 관점에서는 암호기술·양자암호를 포함한 양자정보통신보안 등을 요구하고, 가용성 보장 측면에서는 물리보안·공급망 보안·유무선 네트워크 보안·사이버 보안·보안성 평가기술 등이 필요할 것으로 보입니다.

04.

데이터 유통이 급증하면서 공급망을 공격하는 '위험의 체인화' 경향이 나타나고 있습니다. 이는 전통적인 서버-클라이언트 보안과는 전혀 다른 보안 환경을 요구한다고 생각되는데요, 이에 따라 어떤 기술적 대응이 필요하다고 생각하시는지요?

모빌리티 이동성 수요 증대, 코로나 이후 비대면 사이버 공간에서의 경제활동 증가, 세계 무역의 다양성 확대 등의 요인으로 인하여 공급망을 공격하는 위험 체인화 현상은 앞으로 날로 증가할 것이 명확합니다. 이에 효과적으로 대응하기 위해서는 보다 종합적이고 체계적인 각국의 정보보호 체계 구축이 무엇보다도 중요합니다. 이를 위해서 ICT제품·정보통신시스템·ICT정보서비스에 대한 무결성 보장을 위한 악성코드 분석, 비대면 사용자 인증, 보안성 평가, 정보보호 관리체계 보안, 개인정보 및 프라이버시 보호 등을 포함하는 데이터 보안 등이 필요합니다. 기밀성 보장 측면에서는 내성암호기술과 양자암호기술이, 가용성 측면에서는 물리보안, 공급망 보안,

보안성 평가 등 범국가 차원의 통합보안관제 관리체계 수립이 필수적입니다.

05.

보안은 산업적 측면에서도 중요하지만 안보 차원에서도 매우 중요합니다. 이를 두 가지로 나누면 공격 탐지 역량과 대응 역량으로 구분할 수 있을 텐데요, 각 분야에서 한국의 역량은 어느 정도 수준인가요?

최근에 국제 갈등과 사이버전의 위험이 커지면서 안보 차원에서의 정보보안의 중요성이 부각되는 추세입니다. 특히 사이버 공간은 민간·국가보안을 구분할 수 없으며, 보안이 취약한 국가를 통하여 우회하여 강대국의 정보통신 기반 시설을 공격할 수 있습니다. 이러한 위협은 날로 지능화·조직화·상업화·군사화되어 가고 있는 실정입니다. 한편 무역·경제·사회·정치적으로 세계가 블록화되는 경향을 보이는데, 국가보안 측면에서의 공격탐지 및 대응 역량은 각 진영의 강대국인 미국, 나토 소속 유럽국가, 중국, 러시아 등이 우세합니다. 한국의 경우 대통령실 국가안보보장회의(NSC) 산하위원회(국정원, 행안부 등 정무위원) 주재 하에 국가정보원 중심의 정부·공공기관 공격보안 대응체계가 구축되어 있으며, 과기정통부·한국인터넷진흥원 중심의 민간 분야 공격보안 대응역량도 잘 갖추어 있다고 생각합니다. 하지만 지능화되어 가는 악성코드·해킹 등 사이버 공격의 능동적인 탐지를 위해서는 주요 우방인 미국, 유럽 등과 긴밀한 사이버보안 대응체계를 체계적으로 발전시킬 필요가 있다고 판단됩니다. 이를 위하여 2023년 초반 우리나라 국정원은 나토의 사이버보안 협력국으로 가입한 바 있습니다.

06.

딥페이크 등 명백한 공격으로 보기 어려운 보안 위협 요소도 빠르게 늘어나고 있습니다. 이러한 위협 요소는 새로운 기술에 따른 것이라 관련 제도나 대응체계가 따라잡기 어려운 면이 있는데요, 이와 관련하여 보안 분야에서는 어떤 논의가 이루어지고 있는지요?

딥페이크, AI 보안, 사이버공간에서의 아바타 인증 위협, 무인 자율주행차에서의 보안 위협 등 미래 첨단 기술과 관련된 알려지지 않은 보안위협에 대응하는 기술에 대한 연구는 과기정통부 지원 하에 한국인터넷진흥원 중심으로 ETRI·국가보안기술연구소·보안업체 등이 공동으로 진행하고 있습니다. 민간 차원에서 연구개발 및 표준화가 이루어지고 있습니다. 다만 국가안보 차원에서 일부 제한적으로 제로 트러스트·공급망 보안포럼, 사이버보안정책포럼 등과 같은 산학연관 전문가그룹 형태로 차세대 보안기술에 대한 대응을 추진하고 있는 상황입니다.

07.

새로운 공격을 효과적으로 예방하려면 대응 기술의 핵심 요소를 최대한 노출시키지 말아야 할 수도 있을 텐데요, 그러한 관점에서라면 보안 기술의 표준화에 일정한 한계가 있지 않을까 합니다. 이에 대해서는 어떻게 생각하시는지요?

국가안보 차원과 기업 고유의 노하우 보호 차원에서 일부 보안 대응 기술의 핵심 요소에 대한 철저한 보호조치가 필요합니다. 이를 위해 국가 차원에서는 정보보호 제품 및 시스템 조달정책을 시행하고 민간 기업은 특허를 출원합니다. 이에 따라 표준화 측면에서는 기술 자체보다 관련 기술에 대한 개발 프로세스, 시험인증절차 및 체계, 정보보호 관리체계, 제품의 호환성 보장을 위한 표준적합성 시험인증 방법론 등에 대한 표준화에 초점을 두어 진행할 수 있다고 판단됩니다. 또한 사이버 위협에는 국경이 무의미한 만큼 미국·유럽·일본 등과 정기적이고 유기적인 국가 차원의 국제 협력을 이어가고, 민관 공동연구 체계를 구축하는 것이 무엇보다 중요합니다.

08.

마지막으로 산업 인프라 고도화와 안보 확보를 염두에 둘 때, 미래에 한국이 선점해야 할 보안 관련 기술적, 제도적 요소를 설명해주셨으면 합니다. 또한 이러한 요소가 반영된 보안 환경에 대한 청사진도 궁금합니다.

데이터 보호 측면에서 개인 프라이버시 보호를 위한 법제도 정비는 지속적으로 이어가되, 디지털 헬스케어·모빌리티·자율주행차·AI·원활하고 안전한 공급망 보급 등에 필요한 정보보호 산업 활성화를 위한 정보보호 관련 법제도 개선 노력이 병행되어야 합니다. 첨단기술 연구개발 차원에서 샌드박스 기술검증 시범사업 활성화를 통하여 제도적 보완책을 강구할 필요가 있습니다. 또한 이를 체계적으로 뒷받침할 환경을 조성하려면 무엇보다 대통령실 사이버보안 비서관실이 범부처 콘트롤타워 역할을 잘 수행할 수 있어야 합니다. 산학연관 연구개발 및 국가안보 대응 협력 체계 구축이 선제적으로 이뤄져 국가안보와 민간 산업 활성화라는 두 마리 토끼를 잡을 수 있게 하는 지혜와 노력이 무엇보다도 시급한 상황입니다.