차세대 보안 표준 및 시험인증

김재성 TC5(정보보호 기술위원회) 의장, 한국바이오인식협의회(KBID) 회장

1. 국내외 사이버 환경변화

정보보호 또는 정보보안의 정의는 정보의 수집, 저장, 송수신 등 처리과정 중 정보의 위·변조, 훼손, 유출, 사용 방해 등을 방지하기 위한 관리적·기술적 수단과 모든 정보자산의 안전성을 유지하는 일체의 행위를 의미한다. 최근 들어 ICT 환경 급변으로 전통적인 보안의 개념도 변화됨에 따라 [그림 1]에서 보는 바와 같이 정보보호, 물리보안, 융합보안을 포괄적으로 포함하는 차세대 보안을 나타내기 위해 국내외적으로 '사이버보안(Cyber Security)'을 확장된 개념으로 활용하는 추세이다.

[그림 1] 사이버 보안기술 개념도

전통적으로 정보보호(보안)는 <표 1>에서 보는 바와 같이 암호, ID 관리, 데이터 보안, 시스템 및 디바이스 보안, 네트워크 보안, 응용서비스 보안, 시험·평가 등의 일반적인 정보보호, 주요시설·장소·자원 등을 물리적인 위협인 무단 접근, 도난, 파괴, 화재, 범죄(테러) 등으로부터 보호하기 위한 영상 보안, 휴먼/바이오인식 등의 물리 보안, 정보보호와 기타 ICT와 결합되는 인공지능 보안, 제로트러스트 및 공급망 보안, 우주·항공 보안, 선박·해양 보안, 사물인터넷 보안, 스마트시티·의료·산업제어·모빌리티 보안 등의 융합 보안으로 크게 분류할 수 있다.

<표 1> 사이버 보안기술 분류

중분류	소분류	요소기술
정보보호	암호	암호 설계, 암호 분석
	디지털 ID 관리(인증/인가)	범용 인증, 바이오 기반 인증, ID 관리 및 접근제어
	데이터 보안	데이터 비식별화, 디지털저작물 침해/권리 보호
	시스템 및 디바이스 보안	보안취약성 분석, 침해사고 대응, 서버 및 플랫폼 보안, 디지털 포렌식, 디바이스 보안
	네트워크보안	사이버 위협 분석 및 대응, 유선네트워크 보안, 무선 및 이동통신 보안, 클라우드 및 엣지 보안
	응용서비스 보안	웹 보안, 이메일 보안, 전자화폐 보안, 블록체인 보안, 전자거래 보안
	시험·평가	IT제품 보안성 평가, 암호모듈 시험평가
물리보안	휴먼/바이오인식	바이오인식 센서, 바이오인식 알고리즘, 휴먼/바이오인식 응용, 반려동물/바이오인식 응용
	영상 보안	영상 시스템 보호, 지능형 영상 분석, VMS/통합 관제 및 연동, 영상 보안 응용 서비스
융합보안	인공지능 보안	인공지능 서비스 보안, 인공지능 보안 위협 분석 및 대응
	메타버스 보안	메타버스 인증 및 프라이버시 보호, 메타버스 플랫폼 및 디바이스 보안
	제로트러스트 및 공급망 보안	SW/HW 유통 보안, 데이터 유통 보안
	우주·항공보안	무인항공기 시스템 및 통신 보안, UAM 인프라 및 기체 보안, 위성/지상 통신 보안, 위성간 링크(ISL) 보안
	선박·해양 보안	스마트 선박 내부 보안, 선박/항만 통신 보안, 스마트선박 인프라 통신 보안
	사물인터넷	IoT 디바이스 보안, IoT 서비스 보안
	스마트시티 보안	홈·시티 디바이스 보안 및 제어, 홈·시티 데이터 프라이버시
	스마트모빌리티 보안	V2X 통신 및 응용 서비스 보안, 커넥티드카 침입 탐지 및 방지, URLLC를 지원하는 C-V2X 보안
	헬스케어·의료 보안	헬스케어 디바이스·센서 보안, 의료 데이터 보안 및 공유, 스마트헬스 시스템 및 서비스 보안
	산업제어시스템 보안	스마트공장 보안, 기반시설 보안, 스마트 에너지 보안

2. 국내외 사이버 보안기술의 현황 및 전망

2.1 국내 기술 동향

암호 분야에서는 BIC, 스마트기기, 블록체인 등 신규 ICT 환경 적용 및 양자컴퓨터 위협 대응을 위한 범용 알고리즘과 민감 정보를 포함한 데이터를 안전하게 처리하기 위한 활용성 강화 암호기술(동형암호 등) 등에 대한 연구개발이 활발하다. 디지털 ID 분야에서 스마트폰 환경에서의 바

이오 인증, 분산 신원 관리(DID) 등에 관한 기술은 상용화 수준에 이르렀다. 다만, 메타버스 등 新 플랫폼을 위한 인증기술은 연구 시작 단계이다.

데이터보안 분야에서는 암호화를 통한 데이터 프라이버시 보호를 기반으로 데이터 활용성 강화 및 1인 미디어 활성화와 디지털 콘텐츠에 대한 폭발적인 수요 증가에 따른 콘텐츠 저작권 보호 기술이 개발되고 있다. 시스템 및 디바이스보안 분야에서는 취약점에 대한 버그바운티와 관리 방안의 중요성이 커지고 호스트 기반 침해사고 대응 수요 증가에 맞춰 이에 대한 연구 개발을 추진하는 중이다. 네트워크보안 분야에서는 랜섬웨어 공격 대응, 인공지능 기반 지능형 보안관제 기술 및 근거리 무선 통신망을 포함한 5G 이동통신망과 클라우드 및 엣지의 융합에 필요한 보안을 위한 다양한 기술 개발이 추진되고 있다.

응용보안 분야는 웹 보안, 이메일 보안, 전자화폐 보안, 블록체인 보안, 전자거래 보안 등의 다양한 기술들로 구성되어 있으며, 일상과 밀접한 관계를 갖는 서비스라는 특징에 맞추어 기술 개발이 이뤄지고 있다.

시험평가 분야는 인증기관과 평가기관, 제품 개발업체에서 정보보호시스템과 네트워크 장비의 국가·공공기관 도입에 필요한 평가 기술 및 기준을 공동개발 중이다. 휴먼/바이오인식 분야는 디지털 ID 기술과 결합되어, 비대면 인증, 헬스모니터링 등에 적용되고 있으며, 최근 반려동물 개체식별로도 활용되고 있다. 영상보안 분야에서는 영상정보 오남용 방지를 위한 On-CCTV 자율보호 체계 및 자유로운 기술 적용 확대를 위한 개방형 영상보안플랫폼 등에 대한 기술 개발이 진행 중이다.

2.2 해외 기술 동향

암호 분야는 미국 NIST가 국제 공모사업을 중심으로 새로운 표준 암호기술을 확보하고 있다. 블록체인, 클라우드, 메신저 등 새로운 응용 환경 및 서비스를 대상으로 가용성과 보안성을 강화하기 위한 다양한 암호 원천기술 개발을 확대하고 있다. 디지털 ID 분야에서는 사용자의 디지털 신원과 자산 보호를 위한 새로운 패러다임의 인증 신기술이 도입되어 서비스 중이며, 디지털 지갑 기술의 활용이 증가 추세이다.

데이터보안 분야는 GDPR 등 개인 데이터에 대한 프라이버시 강화 추세에 따라 차등 프라이버시, 신뢰·보안 컴퓨팅 등 암호 및 시스템 기술과 디지털 콘텐츠, 생성형 AI 모델 저작권 보호를 위한 제도적 대응기술 개발을 진행하는 중이다. 시스템 및 디바이스보안 분야에서는 보안취약점의 버그바운티에 대한 다양한 산업이 발전하고 있다. 가상화 관련 취약점 대응 체계와 위협 최소화 연구, 여러 기기의 데이터를 통합하고 연관분석하는 방향으로 디지털 포렌식 연구가 진행 중이다.

네트워크보안 분야는 랜섬웨어 공격 및 사이버위협 등에 대응을 위해 ML/AI 기술을 적용한 네트워크 보안 제품 개발과 근거리 무선 통신망을 포함한 5G 이동통신망과 클라우드 및 엣지의 융합에 필요한 보안기술이 연구되고 있다. 응용보안 분야는 미래 사이버공간의 서비스 보안과 밀접한 관계를 갖는 분야로, 최근 국외 선진국은 Web 3.0 등에 대한 기술 개발을 추진하는 중이다.

시험평가 분야에서는 보안성 평가 및 암호모듈 시험평가 관련 국제표준을 JTC1 SC27이 개발 중이다. 휴먼/바이오인식 분야에서는 미국·유럽 등 주요 선진국이 바이오인식 센서부품·위변조 탐지 및 성능시험 기술 등의 원천기술을 개발, 생체신호 인증기술을 의료·국방 분야에 활용하고 있다.

영상보안 분야에서는 기존의 단순 위험감지 수준을 벗어나 영상에서 발생하는 전반적인 상황을 이해·묘사하고 징후를 감지하는 기술 연구와 고화질 CCTV 급증에 따른 AI 서버 부담 경감을 위한 고성능 SoC 내장제품 개발이 증가하는 추세이다.

2.3 국내 표준화 현황 및 전망

2.3.1 국내 표준화 현황

사이버보안 기술 주요 분야에 대한 국내 표준화 현황은 <표 2>에서 확인할 수 있다.

<표 2> 사이버보안 관련 국내 표준화 현황

구분	표준화 기구	주요 내용
단체(TTA)	지능형 CCTV PG (PG427)	• 지능형 CCTV 시스템/데이터 보호를 위한 보안 프레임워크 및 비식별화 기술 규격, 분석된 메타정보 저장, 전송, 협업을 위한 포맷/인터페이스 규격, 이종/다중 영상시스템 간 표준 연동을 위한 규격 등을 정의
	응용보안/평가인증 PG (PG504)	• 정보보호관리체계(ISMS), 공통평가기준(CC), 암호모듈검증(KCMVP) 등 보안성 인증 및 평가 기술에 대한 표준화 진행
	바이오인식 PG (PG505)	• 모바일 바이오인식 전자금융서비스, 바이오정보 보호기술, 바이오인식시스템 성능 및 표준적합성 시험규격, 생체신호기반의 텔레바이오인식 응용서비스, 바이오인식기반의 반려동물 개체식별기술, 바이오인식기반의 지능형 CCTV 보안기술 등의 단체표준 개발, JTC1 SC27/SC37 및 ITU-T SG17 국제표준화 대응 활동 지원
	정보보호기반 PG (PG501)	• 양자내성 암호를 포함한 범용 암호 알고리즘 규격 및 운용 기술 표준화 추진 개인정보보호/ID관리, 블록체인
	보안 PG (PG502)	• ID 관리(객체 식별, 본인확인, 인증, 접근제어) 기술, 블록체인 보안 기술, 디지털 거래 보안 기술, 개인정보보호 기술에 대한 국내표준 개발 및 국제표준 개발을 협력하고 있으며, 용어정의, 처리과정, 비식별 프레임워크 및 검증자 확인을 위한 상호인증 분산ID 프레임워크 표준화 추진
	사이버보안PG (PG503)	• 클라우드 컴퓨팅, 미래인터넷 등 네트워크 보안기술, 사이버 보안기술(해킹대응, 악성코드, 스팸대응 등), 사이버 범죄 대응기술(역추적, 디지털 포렌식 등)에 관한 국내 표준기술 개발
	메타데이터PG (PG606)	• 유통·활용 데이터 점검 방법, 학술자료 이미지 저작권 검증을 위한 메타데이터 및 DOI 등록 및 관리를 위한 메타데이터 등의 국내 표준화 추진
	블록체인기반기술 프로젝트그룹 (PG1006)	• 블록체인 데이터 분석 프레임워크 인터페이스 요구사항, 검증가능한 크리덴셜 기반 사용자 신원확인을 위한 프로파일 및 분산 식별자 기반 모바일 운전면허증 규격 등의 국내 표준화 추진
포럼	한국바이오인식협의회 (KBID)	• 민간분야 휴먼대상의 바이오인식시스템 성능시험 및 응용서비스, 민간/공공분야 반려동물 대상의 바이오 인식기반 개체식별기술 및 성능시험인증 서비스 표준화 추진
	분산원장기술 표준 포럼	• 분산원장기술 분야의 국내외 표준 개발 및 확산을 목적으로 하는 포럼으로, 분산원장 기반 자기주권적 ID기술에 대한 국내외 표준 개발 중

2.3.2 국내 표준화 발전 전망

사이버보안 관련 국내 주요 표준화 동향은 다음과 같이 정리할 수 있다. 우선, 국내에서도 자체적인 양자내성 암호 공모 등을 통해 표준화 가능 핵심 원천기술을 확보하고, 이후 알고리즘 및 암호 프로토콜 적용 기술의 표준화를 추진할 것으로 전망된다. 분산 신원확인 등 넓은 범위의

메타버스 인증 기술에 대한 표준화도 진행되고 있다. 메타버스 환경에서 활용 가능한 새로운 인증 서비스를 구축하기 위한 기술 개발 및 표준화가 추진될 것으로 보인다.
또한 정부 차원에서 데이터 산업 진흥 정책을 시행하고 있어, 이에 필요한 신뢰성 있고 안전한 데이터가 활발히 유통되도록 하기 위하여 데이터 가공 과정을 검증하는 방법에 대한 표준화가 추진될 것으로 예상된다.
국내 기업의 해외 진출을 지원하고 보안 위협에 효과적으로 대응하기 위해 국내외 표준의 조화가 더욱 강화되고, 새롭게 생겨나는 보안 위협에 대응하기 위한 새로운 보안 표준이 개발될 것으로 예상된다.
사이버보안을 효율화하기 위하여 능동적 네트워크 방어, 보안 오케스트레이션 등 보안 위협 인텔리전스 관리기능에 대한 표준화도 추진될 전망이다. 금융권을 중심으로 Open API 기술이 적용되면서 핀테크 서비스 발전을 촉진하고 있는 가운데, 마이데이터 등에 대한 후속 서비스와 규제도 정비되면서 이 분야가 계속 발전하고 있어 이에 대응한 보안 기술 개발도 주목받고 있다. Web 3.0 등 분산화/탈중앙화에 대한 표준 개발도 속도가 붙을 전망이다.
한편, TTA 응용보안/평가인증(PG504) 분야에서는 암호모듈 및 하드웨어 시험 관련 표준화를 논의할 예정이다. 클라우드 서비스에서는 보안인증제도(CSAP, Cloud Security Assurance Program)를 시작하였으나, 아직 환경을 충분히 고려하지는 않고 있는 현실이다.
반려동물 관련 보안 기술 표준도 진행되고 있다. 펫보험 사기예방 및 유기·유실동물 예방을 위하여 비문 인식 기반의 반려동물 개체식별용 데이터베이스 구축지침이 개발된 상태이다. 바이오인식 기반의 반려동물 개체인증 알고리즘 성능시험 지침도 개발이 진행 중이다.
최근 영상보안 제품 기술이 확산함에 따라 영상분석을 기반으로 한 다양한 기술이 개발되고 있으며, 이같은 추세에 대응하여 개인정보 비식별 및 이기종 기기 간 연동을 위한 표준화 기술이 필요한 상황이다.

2.4 해외 표준화 현황 및 전망

2.4.1 국제 표준화 현황

사이버보안 기술에 관련한 국제 표준화 동향은 <표 3>에서 확인할 수 있다.

2.4.2 국제 표준화 발전 전망

최근 주요 국가의 미래 전략 기술로 주목받는 양자기술 관련 보안 위협을 극복하기 위한 표준 기술 개발이 활발해질 전망이다. 양자내성 암호 활용을 위한 알고리즘 및 프로토콜 적용 기술이 우선 표준화될 것으로 보이며, 이와 함께 동형 암호 등 보안 위험을 낮추면서도 주요 데이터의 활용성을 강화하는 암호기술의 표준화가 추진될 전망이다.
메타버스 표준 개발은 현재 개념 정립 단계이나, 사용자-아바타의 식별·인증이나 프라이버시 보호 등을 위한 요구사항, 상호연동 등을 위한 표준화가 우선 추진될 것으로 예상된다.
또 비식별 처리 기술과 처리 절차, 개인정보가 노출되지 않도록 비식별 처리된 데이터의 처리 수준에 대한 요구사항에 맞춰 실제 데이터 수준을 측정하는 방법에 대한 표준화가 요구되는 상황이다.

<표 3> 사이버보안 관련 해외 표준화 현황

구분	표준화 기구		주요 내용
공식	ITU-T	SG17	(Security) ITU-T SG17은 ITU-T의 모든 스터디 그룹에서 추진하는 보안 관련 작업에 대해 전반적인 조종하며, 타 표준개발기구 협력을 통한 보안 관련 표준화를 추진하고, 사이버 보안, 보안 관리, 보안 아키텍처 및 프레임워크, 스팸 방지, ID 관리, 개인 식별 정보 보호, 데이터 보호의 운영 측면, 개방형 ID 신뢰 프레임워크, 양자 기반 보안 관련 표준화 추진, 또한 사물 인터넷(IoT), 스마트 그리드, 스마트폰, 소프트웨어 정의 네트워킹, 웹 서비스, 빅 데이터 분석, 소셜 네트워크, 클라우드 컴퓨팅, 모바일 금융 시스템, IPTV, 분산 원장 기술을 위한 애플리케이션 및 서비스의 보안 관련 표준화 추진 중
		SG9	(Broadband cable and TV) 초고화질 및 3D TV와 같은 고급 기능을 지원하는 TV 및 사운드 프로그램 배포에서의 통신 시스템 및 인터넷 액세스를 포함하여 대화형 음성, 비디오 및 데이터 서비스를 제공하기 위한 통합 광대역 네트워크로서 주로 텔레비전 및 사운드 프로그램을 가정으로 배포하기 위해 설계된 케이블 및 하이브리드 네트워크 관련 표준화 추진
	JTC 1	SC27	(Information security, cybersecurity and privacy protection) 보안 요구 사항 캡처 방법론, 정보 보안 관리 시스템, 보안 프로세스, 보안 통제/서비스, 신원 관리, 생체 인식/프라이버시, 정보보안 관리 시스템 분야의 적합성 평가, 인증/감사 요구사항 및 암호 원천기술(동형 암호, 양자내성 암호, 경량 인증 암호화, 다자간 계산등) 등에 관한 표준화 추진
		SC37	(Biometrics) 응용 프로그램과 시스템 간의 상호 운용성 및 데이터 교환을 지원하기 위한 생체인식 관련 용어/인터페이스/데이터 호환규격/표준적합성 시험/응용서비스/시스템 성능 시험기술 및 프라이버시 보호정책 등에 대한 표준화 추진
		TC307	(Blockchain and distributed ledger technologies TC) 분산원장에서의 프라이버시 및 PII 보호 고려사항에 대한 기술보고서가 2020년 완료되었으며, 분산원장기술(DLT) 기반 분산 ID와 식별자 등에 대한 표준 개발 중
	ISO	TC171	(Document management applications) 캡쳐/인덱싱/스토리지/검색/분포/표현 등 문서 관리 어플리케이션 기술 및 프로세스와 관련된 표준화
사실	ABC		(EXCO 집행위원회 그룹) 아시아 8개국 지역의 지문·홍채 등 바이오인식제품에 대한 성능시험 및 표준적합성 상호인정 시험기술 사실표준을 개발하여 제품 호환성 검증을 진행 중임
	IETF		(Security Area) TLS, IPsec, MLS 등 주요 암호 프로토콜 규격 및 암호 알고리즘 적용 방법에 대한 표준화 추진 중
	IRTF		(CFRG/Crypto Forum) 암호 프로토콜에서 사용할 수 있는 공통 기반 암호기술 및 운용 가이드라인에 대한 표준화 추진 중
	3GPP		신규·진화된 서비스, 특징, 수용성 및 식별성을 고려한 전반적인 서비스(SA1) 및 3GPP 시스템의 요구사항 정의, 그리고 보안과 프라이버시를 위한 구조와 프로토콜 명세 등의 표준화 추진
	EUDI ARF		EU 신원지갑의 정의 및 목적과 생태계를 정의하고 PID 및 (Q)EAA 발급 요구사항과 아키텍처와 참조 레퍼런스 개발 추진
	W3C		웹 애플리케이션(자바스크립트)을 통해 생체인식, 보안토큰 등 다양한 인증 수단을 활용하기 위한 웹 인증(Web Authentication), 분산 ID의 핵심 아키텍처 및 데이터 모델 등, 검증 가능 크리덴셜 데이터 모델 등의 표준화 추진
	FIDO Alliance		패스워드를 대체하여 다양한 인증 수단을 수용할 수 있는 개방형 표준을 개발하는 조직으로, 인증 제품의 표준 적합성, 보안성, 생체인식 성능 등을 평가하기 위한 표준화 추진
	NIST		NIST는 암호모듈 시험기관으로 사이버 보안 개선, 사이버보안 및 위협관리 프레임워크, IoT 사이버보안 등의 표준화를 추진하고 있으며, 최근 CNSA 2.0이 발표됨에 따라 신규 암호 알고리즘에 대한 시험 방법을 개발하는 중
	CCRA/CCUF		보안성 평가를 위한 공통평가기준(CC)와 평가방법론(CEM)에 대한 표준 개발, 개정, 배포하고 있으며, ICT 환경의 변화에 따른 새로운 기술의 제품 평가를 위한 보호프로파일와 보조문서를 지속적으로 개발 추진 중
	OSSA		안드로이드 기반 영상보안시스템의 보안 프레임워크 및 영상분석 앱과의 데이터 표준 교환을 위한 API 정의 등의 표준화 추진

시스템 및 디바이스 보안은 넓은 범위의 기술, 프로세스, 방법을 다루기 때문에 암호화, 신원 인증, 접근제어 등 다양한 측면을 포괄하는 통합적인 보안 표준형태로 개발이 진행될 것으로 예상된다. AI 기술의 발전에 대응, 사이버공간에서 발생하는 침해사고 및 취약점 등에 대한 AI 기반의 자동 대응과 정보공유, 보안 오케스트레이션 등에 대한 표준화 작업 역시 활발해질 전망이다. Open API 기반의 안전한 핀테크 서비스 활용을 위한 표준개발을 시작으로 오픈소스 공급망과 같은 표준이 개발될 것으로 보이며, 이 과정에서 분산화를 지향하는 Web 3.0과의 융합이 활발하게 일어날 것이다.

암호모듈 탬퍼에 대한 ISO 국제표준은 아직 개념 정립 단계이다. 하지만 탈취, 분실 등의 문제를 막기 위해 필수적인 요소이므로 관련 기술 개발 및 표준이 반드시 필요한 분야이다. 클라우드 제품에 대한 기본적인 평가 프레임워크를 제공하기 위해 CCUF의 클라우드 기술작업반(CCitC)과 협력 하에 가이드라인이 개발 작업도 시작되었다.

스마트카를 위한 보안 대책 논의도 활발하다. 스마트카 보안 위협 및 보안 대책에 관한 표준화에서 바이오인식 기술을 이용한 자율주행차의 바이오 트윈 관련 표준화로 진화·발전될 전망이다. 또한 반려견 및 반려묘에 대한 개체식별 인증서비스에 대한 국제표준도 개발 중이다. 마필(말)의 종자 관리 및 개체식별 기술에 대한 국제표준화가 추진될 예정이다. 이와 함께 미국, 유럽 등 선진국 중심으로 이기종 기기 간 연계·협업을 위한 사실 표준, 기술 및 스마트시티 모델 표준화를 진행하고 확대 적용하기 위한 노력이 이뤄지고 있다.

3. 2024년도 사이버 보안 전망

2024년에는 핵티비즘을 내세운 해킹 캠페인과 보안 측면에서의 클라우드 보안의 중요성이 커질 전망이다. 또 사이버 범죄자들이 랜섬웨어를 사용하여 주요 정보통신 인프라를 표적으로 삼고, 생성형 AI와 같은 신기술을 악용할 우려가 높아지는 실정이다. 이에 따라 공공·민간분야에서 정보보호 조직이 사이버 공격자들보다 앞서 나가려면 보안 트렌드를 예측하는 것이 중요하고, 거시 경제적 요인, 신흥 기술, 클라우드 위험 등을 고려한 총체적 접근 방식을 취해야 할 것이다. 글로벌 사이버 보안기업 팔로알토 네트웍스의 관련 보고서는 "2024년에도 강한 동기를 가진 사이버 범죄 조직, 국가 차원의 공격, 핵티비스트들이 계속해서 늘어날 전망이지만 이를 늦추기 위해 우리가 할 수 있는 일은 많지 않다"라며 "하지만 AI를 통해 보안 기능의 복잡성을 해결하여 좀 더 효과적이고 효율적인 비용으로 만들 수 있어야 한다"라고 강조했다. 팔로알토 네트웍스가 공개한 2024년 주목해야 할 사이버 보안 트렌드는 다음과 같다.

① 핵티비즘으로 구현하는 현대판 집단행동

2023년 환경 운동가들이 방송 프로그램에 난입하는 사례가 발생한 데 이어 올해는 이러한 시위가 사이버 중심 캠페인의 형태로 나타날 가능성이 엿보인다. 올림픽, 유로컵, 각국 총선 등 세계 곳곳에서 중요한 이벤트가 열리는 가운데 '핵티비스트(해커 활동가)들은 수백만 명의 공중에게 자신들의 대의를 알릴 방법을 모색하고 있다. 이전에는 높은 수준의 기술 전문 지식이 필요했지만, 서비스형 사이버 범죄 모델 덕분에 문턱이 낮아져 이제 충분한 자금과 의욕이 넘치는 활동가만으로도 이러한 캠페인이 가능해졌다. 핵티비스트들은 또한 격변하는 지정학적 환경을 이용

해 소속 단체의 인지도를 높이고 대의에 대한 공감을 얻고자 시도하고 있다. 대부분의 핵티비스트 활동은 분산 서비스 거부(DDoS) 공격을 통해 이루어지는데, 실제로 2023년 인도에서 열린 G20 정상회의 기간 동안 주변 국가의 30개 이상의 핵티비스트 그룹이 600개 이상의 정부·민간 기관의 웹사이트를 디도스 공격·훼손·데이터 유출 등으로 공격한 바 있다.

② 사이버 보안에서 AI는 좋은 쪽으로도, 나쁜 쪽으로도 진화할 것

2022년 10월 챗GPT가 출시된 이후, 세계적으로 사이버 범죄를 민주화할 가능성에 대한 우려가 제기됐다. 악성 애플리케이션을 방지하는 가드레일이 있음에도 불구하고, 다양한 창의적인 프롬프트를 통해 챗GPT는 '이상한 사람'인 듯 보이는 거의 완벽한 피싱 이메일을 엄청난 규모로 생성할 수 있기 때문이다. 딥페이크와 음성 기술 등 새로운 방식으로 생성형 AI를 사용해 은행에서 수백만 달러를 탈취하는 시도도 발견됐다. 생성형 AI를 도입하는 기업은 모델 오염시키기(poisoning), 데이터 유출, 프롬프트 인젝션 공격 등의 취약성에 주의해야 한다. 공격자들은 합법적인 사용 사례에 생성형 AI를 활용해 혁신의 틈새를 계속해서 악용할 전망이다.

③ 손쉽게 접근 가능한 OT 환경을 노리는 공격 증가

운영 기술은 모든 산업 조직의 핵심이다. 주요 수익창출원으로서의 운영기술(OT) 시스템은 높은 수준의 사이버 성숙도를 갖춰야 한다. 많은 조직에서 여전히 OT 환경이 에어 갭을 통해 보호되고 있다고 믿고 있지만, IT·OT 융합으로 인해 OT는 그 어느 때보다 IT와 더 많이 연결되어 있으며, 클라우드와도 연결되어 있다. 이로 인해 공격 표면이 확대되고 OT 네트워크에 대한 위험이 크게 증가했으나 사이버 제어에 대한 투자는 늘지 않은 상황이다. 사이버 보안이 확보되어야 안전하고 신뢰할 수 있는 OT 환경을 구축할 수 있으며, 제로 트러스트 아키텍처는 가장 중요한 OT 시스템을 위협으로부터 보호하는 동시에 조직이 디지털 혁신에 집중할 수 있도록 지원한다. 2024년에는 조직이 가장 중요한 비즈니스 시스템을 보호하고 증가하는 위험을 수용 가능한 수준으로 관리하기 위해 OT 사이버 보안 성숙도에 대한 투자가 늘어날 예정이다.

④ 사이버 보안의 새로운 지평을 여는 통합 접근법

위협 대응이 부진하고, 사일로화된 솔루션을 사용하는 조직은 신속한 디지털 혁신 이니셔티브를 보호하는 데 어려움을 겪는다. 거시 경제의 역풍과 인력 문제에 대응하고, 공급업체 복잡성을 줄이기 위해 통합 접근법을 찾는 조직이 늘어나고 있다. 위기가 닥쳤을 때 단일 창구인 경우 사이버 보안 스택을 관리하기가 훨씬 수월하기 때문이다. 장기적으로는 비용을 절감하고 더 나은 결과를 얻을 수 있다. 더 많은 조직이 통합의 이점을 깨닫고 있으며, 2024년에는 복잡성을 줄이고 통합 사이버 보안 스택으로 전환하는 사례가 증가할 전망이다.

⑤ 멀티·하이브리드 클라우드 보안의 중요성 높아져

클라우드 얼리 어답터는 일반적으로 단일 하이퍼 스케일러로 시작하며, 단일 클라우드 모델은 선택한 클라우드 서비스 공급업체(CSP)의 기본 보안 툴을 채택하게 된다. 그러나 시간이 지남에 따라 멀티 클라우드 또는 하이브리드 클라우드 전략을 채택해야만 해결할 수 있는 문제 및 운영

중단을 경험하게 된다. 이러한 멀티클라우드 여정에서는 네이티브 CSP 보안 툴이 다른 CSP에 원활하게 적용되지 않기 때문에 기존 클라우드 보안 패러다임에 대한 검토가 필요하다. 2024년에는 멀티 클라우드 또는 하이브리드 클라우드 프로젝트를 진행해야 하는 조직에서 둘 이상의 클라우드 공급업체와 거래할 때 보안에 대한 좀 더 통합된 접근 방식을 구축하는 방향으로 나아갈 전망이다.

[참고문헌]
[1] TTA, 사이버 보안의 현재와 미래, TTA 저널, 2023.03.
[2] TTA, 미래의 바이오인식기술, TTA 저널, 2023.03.
[3] TTA, ICT 표준화 로드맵(ver.2024)-차세대 보안, 2023.12.
[4] 보안뉴스, 2024년에 주목해야 할 5가지 사이버 보안 트렌드, 2024.1월

※ 출처: TTA 저널 제211호