디지털로 여는 좋은 세상

2023-4호

D.gov 해외동향

Issue

미국, 클라우드 서비스 보안 관련 발간물 발표

호주, 공공서비스 분야 생성형 AI 활용 임시 지침 발표

News

두바이, 7가지 새로운 디지털 전략 발표 등 총 7건

NIA 한국지능정보사회진흥원
NATIONAL INFORMATION SOCIETY AGENCY

CONTENTS

01 Issue

02 News

ISSUE ① 미국, 클라우드 서비스 보안 관련 발간물 발표

Reading Point

- 미국 연방 정부 및 주요기반시설의 사이버보안을 담당하는 CISA가 '보안 클라우드 비즈니스 애플리케이션(SCuBA)' 프로젝트의 일환으로 클라우드 서비스 보안 관련 첫 번째 결과물을 공개[1)]
- 이번 결과물은 기술 참조 아키텍처(TRA)와 확장형 가시성 참조 프레임워크(eVRF)로 구성되었으며, 클라우드 보안 준수 지침 및 모범 사례와 함께 CISA·연방 부처·클라우드 공급업체의 각 역할을 구체적으로 명시

Ⅰ 개요

❍ 미국의 사이버보안 전담 기관(CISA)*이 정부 기관의 클라우드 서비스의 보안 및 복원력 모범 사례를 다룬 발간물을 2023년 6월에 발표

* 미국 국토안보부(DHS) 산하 기관으로 모든 연방 부처 및 산하 기관의 사이버보안 및 인프라 보호를 강화하고, 외부 해커에 대항해 정부의 사이버보안 업무를 담당

- 2022년에 실시한 공공의견 수렴을 바탕으로 '보안 클라우드 비즈니스 애플리케이션(SCuBA)'* 프로젝트의 일환인 보안 지침 자료 최종판 첫 번째 시리즈 발표

* SCuBA는 CISA의 주도 하에 연방 부처의 클라우드 비즈니스 애플리케이션 환경 보호 및 클라우드 환경 속에서 연방 정보를 보호하기 위한 프로젝트

❍ 이번 발간물은 ▲기술 참조 아키텍처(TRA, Technical Reference Architecture)[2)] ▲확장형 가시성 참조 프레임워크(eVRF, The Extensible Visibility Reference Framework) 가이드북[3)]으로 구성

1) CISA(2023.6.27.), CISA Releases Cloud Services Guidance and Resources
2) CISA(2023.6), Secure Cloud Business Applications (SCUBA) – Technical Reference Architecture
3) CISA(2023.6), Secure Cloud Business Applications (SCUBA) – Extensible Visibility Reference Framework

- **(TRA)** 클라우드 배포, 적응형 솔루션, 보안 아키텍처 및 제로 트러스트 프레임워크를 위한 기술 채택 시 참조할 수 있는 보안 가이드 기술 문서
- **(eVRF 가이드북)** 특정 제품 및 서비스의 가시성 데이터 제공 범위에 대한 이해를 돕고 잠재적인 보안 문제 파악을 목적으로 하는 eVRF 프레임워크에 대한 전반적 개요를 설명

❍ CISA는 TRA와 eVRF가 연방 부처를 포함한 모든 조직에 적용할 수 있는 유연하며 시의성 있는 지침으로 제공할 것으로 기대

- 이 문서들을 통해 조직은 사이버보안 및 가시성 격차를 해결하여 사이버 위험을 적절히 이해하고 관리하는 데 기여

❍ 이하에서는 SCuBA 프로젝트의 TRA를 중심으로 미국 연방 정부의 보안 클라우드 채택과 관련된 요구사항, CISA·부처·공급업체의 역할을 살펴보고자 함

Ⅱ SCuBA 프로젝트

1 SCuBA 프로젝트 개요

○ **(목표)** SCuBA는 일관성 있고 효과적인 최신 보안 구성을 통해 클라우드 환경 내에 저장된 연방 행정 기구(FCEB, Federal Civilian Executive Branch)의 정보 자산을 보호

○ **(역할)** CISA 사이버보안 서비스 제공 및 타 기관과의 협력을 촉구하며, 연방 정부의 보안 요구 사항 실행과 국토안보부(DHS)의 사이버보안 임무를 주도하는 CISA를 지원

- 정부 및 주요기반시설 파트너 대상 클라우드 보안 지침의 가용성 확대
- 기존 및 계획된 보안 프로그램에서 사용 가능한 클라우드 보안 관련 데이터의 활용도 제고
- 보안 프로그램 요구사항 및 서비스 개선
- 민간 서비스 제공사의 상용 제품 및 전문 지식 활용
- 연방 엔터프라이즈 전반의 클라우드 비즈니스 애플리케이션 환경 보호

〈 SCuBA 프로젝트 진행 상황 〉

시점	추진 내용
2022년 10월	• CISA는 Microsoft 365 사용과 관련된 보안 기준점(baseline)*을 발표하고 연방 부처가 시범적으로 사용하고 피드백을 제공하도록 권장 * 연방 정부 전체에 걸쳐 클라우드 비즈니스 애플리케이션 환경의 보안을 개선하기 위한 템플릿. 현재 Google Workspace(GWS) 보안 구성 기준점도 개발 중
2023년 3월	• CISA는 하이브리드 ID 솔루션 아키텍처 지침 문서(초안)에 대한 공공의견 수렴 개시 (2023년 4월 19일에 종료)
2023년 6월	• SCuBA 기술 참조 아키텍처(TRA) 및 확장형 가시성 참조 프레임워크(eVRF) 가이드북 확정

2 SCuBA TRA의 목표 및 범위

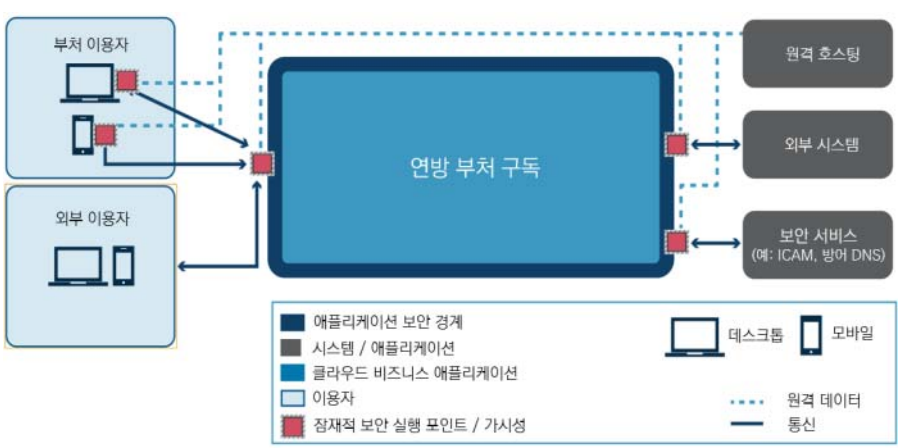
○ **(목표)** SCuBA 기술 참조 아키텍처(TRA)는 기술·활용의 맥락, 표준 및 용어 정의 등을

통해 SCuBA의 하위 프로젝트 간 일관성과 통합성을 유지

- 이번 TRA는 CISA, 미국 디지털 서비스(USDS) 및 연방 클라우드 보안 인증 프로그램(FedRAMP)이 공동 발간한 '클라우드 보안 TRA(Cloud Security TRA)'를 기반으로 작성
- TRA는 제품 및 공급업체에 구애받지 않는 기술 중립성을 지니며, 연방 클라우드 보안 가이던스와의 일관성을 도모
- TRA는 제품별 보안 기준점을 제시하고, 연방 부처의 안전한 클라우드 비즈니스 애플리케이션 채택을 지원하기 위한 위기 기반 지침을 제공하되, 기존 연방정부의 요구사항이나 규정을 대체하지는 않음

❍ **(범위)** 클라우드 기반 애플리케이션을 보호하고 모니터링을 위해 구독제 기반 서비스형 소프트웨어(SaaS) 모델을 기반으로 제공되는 클라우드 비즈니스 애플리케이션을 포괄

〈 SCuBA 시스템 개요 〉



- 상기 그림의 SCuBA 시스템 개요는 연방 부처가 SCuBA를 안전하게 구성하고 보안 요구 사항을 충족하기 위한 관련 로그 및 원격 측정 수집 책임의 범위를 제시
- 클라우드 서비스 제공업체(CSP, Cloud Service Providers)는 기본 인프라를 보호할 책임이 있어 본 SCuBA TRA의 범위에는 해당하지 않음

3 주체별 책임과 역할: CISA, 연방 부처 및 공급업체

❍ **(CISA)** CISA는 연방 행정 기구(FCEB)들과 협력을 통해 기관 클라우드 로그 및 원격 분석을 지속적으로 수집하여 공동 사고 대응 및 위협 추적 활동을 실시

- 클라우드 공급업체와 협의하여 연방정부 기관이 사용하는 클라우드 비즈니스 애플리케이션에 대한 보안 및 지원을 강화하는 솔루션을 개발하고 개선 기회를 파악
- 진화하는 클라우드 위협에 대응하고 효과적인 모니터링, 위협 헌팅 및 사고 대응 활동을 수행하기 위해 이러한 정보를 확보하고 가시성과 역량을 확보해야 함
- 위협 정보를 연방 부처들과 공유하여 부처들의 원격 분석 내용을 수집, 처리, 분석하여 자체 내부 보안 요구사항을 충족하고 가시성을 강화하며 임무 요구사항을 충족할 수 있도록 지원

❍ **(연방 부처)** CISA와의 협력을 통해 관리 예산처(OMB)의 사이버보안 관련 지침을 준수

- OMB의 지침(M-21-31)*에 따라 CISA와 협력하여 TRA의 지침을 기반으로 포괄적인 로깅 및 정보 공유 기능을 구현해야 함

  * OMB(2021.8.27.), M-21-31: 국가 사이버보안 환경을 개선하고 보호하기 위한 연방 부처 요구사항을 기술한 각서(memorandum)

- 클라우드 비즈니스 애플리케이션의 원격 측정과 로그 기록을 CISA와 공유
- OMB 지침(M-22-09)*의 제로 트러스트 원칙 및 요구사항에 따라 클라우드 비즈니스 애플리케이션을 보호하고 모니터링을 실시

  * OMB(2022.1.26.), M-22-09: 사이버보안 위협에 대한 미국의 정부의 방어 역량을 강화하기 위해 2024 회계연도 말까지 연방 부처들 특정 사이버보안 표준 및 목표 달성을 위한 연방 제로 트러스트 아키텍처(ZTA) 전략을 제시한 각서. M-22-09에 따라 각 연방 부처는 2022년 봄까지 OMB에 제로 트러스트 실행을 위한 상세 계획을 제출

- 이와 관련, TRA는 연방 부처가 애플리케이션, 워크로드 및 데이터에 대한 OMB M-22-09에 수록된 요구사항을 충족할 수 있도록 지원

❍ **(클라우드 공급업체)** 부문과 서비스 제공 전반에 걸친 동향과 위협 활동 파악 역량 측면에서 장점을 활용하여 보안 취약점에 적극 대응

- 클라우드 공급업체는 테넌트(tenant)*가 감지 못하는 위협과 취약점에 대응하고, 공격 요인을 완화하기 위해 지속적으로 제품을 개선

* 클라우드 인프라나 서비스를 제공하는 소프트웨어 아키텍처. 싱글 테넌트의 경우 1개 서버에 대해 1개 기업의 데이터와 애플리케이션만 제공하며, 멀티 테넌트는 다른 사용자들과 서버, 스토리지를 공유

4 SCuBA 프로젝트의 보안 구성 요소별 특징

① 구성 요소

❍ TRA는 클라우드 비즈니스 애플리케이션을 보호하고 강화하기 위해 SCuBA의 보안 서비스 및 기능의 필수 구성 요소에 대해 기술

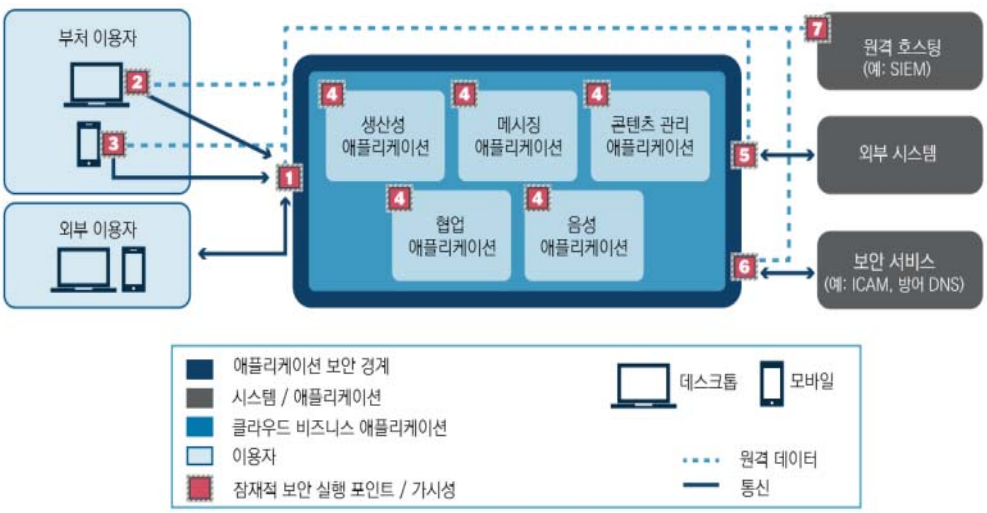
- 보안 서비스 및 기능은 구현, 구성 및 관리 과정에서 클라우드 비즈니스 애플리케이션에 영향을 미치는 취약성 및 위협을 방지하고 완화
- 보안 서비스 및 기능이 일단 구축되면 시스템 성능 역시 개선됨에 따라 클라우드 비즈니스 애플리케이션의 보안과 애플리케이션을 호스팅 하는 플랫폼을 강화

❍ 보안 서비스와 구성 방식은 기존의 업무 기능, 해당 기능에 대한 위협 및 이와 관련된 연방 및 CISA의 방침에 따라 결정

- 보안 서비스와 구성은 연방 부처별 고유의 위험 요인 및 허용 범위에 따라 구현되어야 함
- 이렇게 구축된 보안 서비스 구성은 실시간으로 잠재적인 사이버보안 위협을 식별하고 환경을 보호, 모니터링 및 유지 관리할 수 있도록 하는 선제적 보안 접근 가능

❍ 이하의 그림은 SCuBA 보안 및 가시성 포인트를 개념화한 것으로 각 포인트는 아래 표와 같이 SCuBA TRA의 하나 이상의 관련 섹션과 매핑됨

〈 SCuBA 시스템 개요 〉



〈 보안 실행 포인트/가시성 별 해당 섹션 〉

보안 실행 포인트/가시성	TRA 내 관련 섹션
1	- 신원, 자격증명 및 액세스 관리(ICAM, Identity, Credential, and Access Management) - 모든 위치에서 안전한 클라우드 액세스 - 보호 도메인 이름 시스템(pDNS) - 데이터 공유 및 유출 보호
2	- 신원, 자격증명 및 액세스 관리 - 데스크톱 엔드포인트 보안
3	- 신원, 자격증명 및 액세스 관리 - 모바일 엔드포인트 보안
4	- 애플리케이션 보안 구성
5	- 외부 이메일 보호 - 데이터 공유 및 유출 방지
6	- 신원, 자격증명 및 액세스 관리 - 보호 도메인 네임 시스템
7	- 사이버 가시성 및 eVRF 분석 프레임워크 - 원격 분석 생성 및 처리

② 신원, 자격증명 및 액세스 관리(ICAM)

❍ 신원, 자격증명 및 액세스 관리(ICAM)*는 제로 트러스트의 핵심 원칙이며 사이버보안 위기 관리 시 의사결정을 촉진

* 연방 부처에서 적절한 개인이 적절한 리소스에 적절한 이유로 적시에 액세스하도록 지원하기 위한 일련의 도구, 정책 및 시스템을 의미

- 미국 정부 서비스국(GSA)은 연방 ICAM(FICAM) 아키텍처와 디지털 신원 서비스에 대한 지침을 담은 미국 국립표준기술연구소(NIST)의 발간물인 '디지털 ID 관리'[4]를 통해 ICAM 프로그램 실행과 관련된 세부 지침*을 제시

* 연방 부처를 대상으로 다양한 수준의 신원 증명, 등록, 인증자, 인증 프로토콜 및 연합을 결정하기 위한 지침을 제공

- 연방 부처들은 기존 ICAM 프로그램이 있는 경우가 많아 이를 비즈니스 애플리케이션과 통합(federation)할 수도 있지만 기존 인프라를 재사용함으로써 온-프레미스 사이버보안 인프라를 손상할 수 있어, 클라우드에 위험을 초래
- 대안 방안으로 클라우드 공급업체를 통해 인증을 실행하는 클라우드 기반 IDaaS(Identity as a Service) 방식이 최근 연방 부처들의 주목을 받고 있으며, 이 경우 보안에 대한 책임은 IDaaS 제공업체, 대행사 및 CISA가 공동 부담

❍ ICAM은 클라우드 애플리케이션 보안에 매우 중요한 요소로 액세스 관리 책임은 클라우드 비즈니스 애플리케이션 단위에서뿐만 아니라 전사적인 차원에서의 관리도 필요

- 클라우드 리소스에 대한 최종 사용자의 액세스를 관리하려면 강력한 관리 제어와 최소 권한 원칙이 필수적이며, 보안 클라우드 액세스 및 엔드포인트 보호 기술을 함께 사용해야 함
- CISA는 현재 이러한 요인들을 고려하여 특정 클라우드 네이티브 ID 및 액세스 관리 서비스에 대한 보안 구성 기준점(baseline)을 개발 중

4) NIST(2017.6), Digital Identity Guidelines- SP 800-63-3

③ 어느 곳에서든 안전한 클라우드 액세스

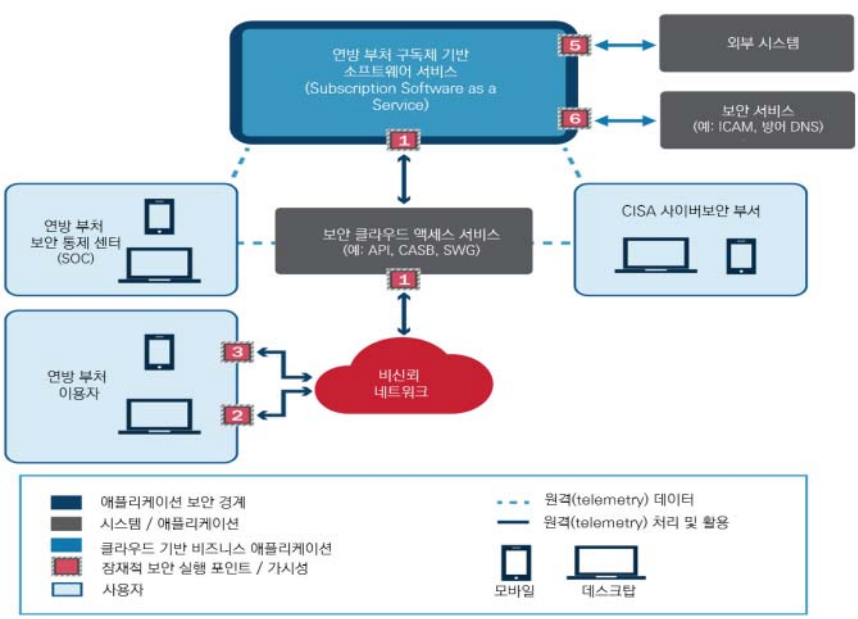
❍ 클라우드 액세스 보안 취약점 해소하기 위해 새로운 모델인 신뢰 인터넷 접속(TIC, Trusted Internet Connection)* 프로그램을 제공

* CISA의 클라우드 보안 지침 중 하나

- SCuBA TRA는 보안 클라우드 액세스(SCA) 제품 및 서비스를 사용하는 비즈니스 애플리케이션에 대한 사용자 액세스를 보호하기 위한 토대로서 TIC 3.0 지침[5]을 적용

❍ SCA 솔루션은 기관의 클라우드 비즈니스 애플리케이션 구축 시 반드시 포함해야 하는 요소

〈 보안 클라우드 액세스(SCA)의 개념 〉



- 현재 클라우드 업계에서는 제로 트러스트 네트워크 액세스, 클라우드 액세스 보안 브로커(CASB), 보안 이메일 게이트웨이(SEG), 보안 액세스 서비스 에지(SASE) 등 다양한 SCA와 관련된 솔루션 및 서비스가 확산
- SCA 솔루션은 사용자가 클라우드 서비스 제공업체(CSP) 내 연방 부처의 비즈니스

5) CISA(203.4.17), Trusted Internet Connections (TIC) 3.0 Core Guidance Documents

애플리케이션에 안전하게 액세스할 수 있도록 지원하며, 비즈니스 애플리케이션 사용자는 엔터프라이즈 네트워크, 분원(branch offices), 원격 디바이스 또는 모바일 디바이스를 통해 액세스가 가능

- SCA 솔루션은 대상 CSP 및 소스 워크스테이션 또는 디바이스에 탑재된 보안 서비스* 등은 TIC 지침을 따라야 함

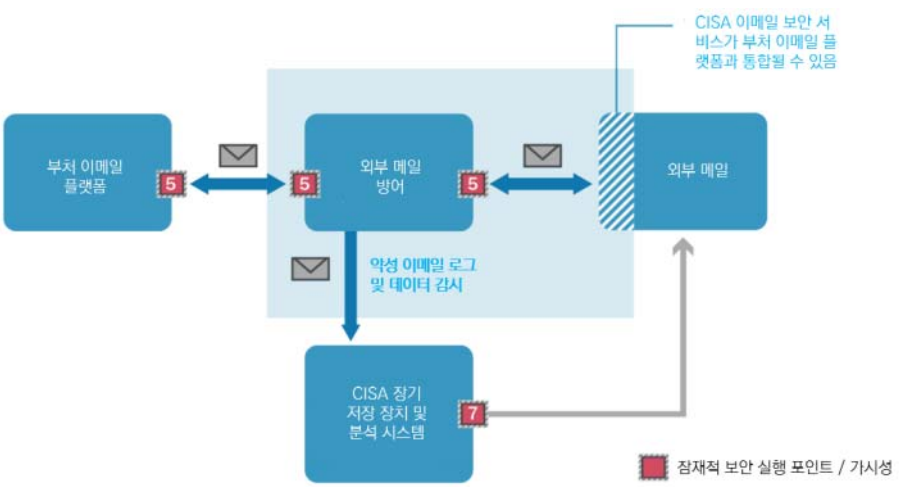
  * 예: 엔드포인트 탐지 및 대응(EDR, Endpoint Detection and Response)

- SCuBA TRA에서는 SCA가 다루는 주제를 중심으로 소개하고 있으며, 다양한 SCA 사용 사례와 관련된 내용은 TIC 3.0 지침 문서를 통해 확인 가능

④ 외부 이메일 보호

❍ 이메일은 피싱 링크와 멀웨어 등을 통해 정부 부처 환경으로의 진입 지점으로 자주 활용

〈 외부 이메일의 흐름도 〉



- 이메일 관련 위험은 일반적으로 클라우드 제공업체의 제품에 내장된 네이티브 보안 기능과 써드파티 제품 간의 결합을 통해 해결이 가능

❍ 이메일 보안 솔루션의 유형은 다음과 같음

- **(필터링 및 태그 지정)** 멀웨어 탐지, 스팸 식별, 부처용 태그 지정 등을 위해 모든

메시지(예: 수신, 발신, 내부)에 대한 이메일을 필터링

- **(로그 가시성)** CISA 및 부처 보안 운영 담당자는 이메일 속성에 대한 가시성을 확보
- **(인증 및 무결성)** 송수신 이메일 서버가 상호 인증되고 전송 중에 메시지가 변조되지 않도록 보장
- **(추가 기능)** 지표 프로비저닝 자동화, 위협 인텔리전스, 첨단 애널리틱스, 보고, 사이버 위협 헌팅(cyber hunt) 지원 및 사고 대응, 샌드박스(sandboxing)*, 디토네이션(detonation)**, 써드파티 보안 서비스 통합 기능 등

* 외부로부터 들어온 프로그램이 보호된 영역에서 동작해 시스템이 부정하게 조작되는 것을 막기 위한 보안 기술

** 적극적인 사이버 방어 기법으로 악성코드 분해나 해체 활동을 의미

❍ CISA는 현재 이메일 보안을 위한 보안 구성 기준치를 제공하기 위한 문서를 개발 중

- 부처들은 외부 이메일 보호 기능을 통합하고 이메일 보안에 영향을 미치는 중요한 클라우드 서비스*에 대한 보안 구성 기준점을 마련해야 함

* 예: Exchange Online, Azure Active Directory, Google Cloud Identity 또는 기타 타사 공급업체

- CISA는 새로운 DNS 기능을 제공하고 이메일 보안을 개선하며 궁극적으로 E3A(EINSTEIN 3 Accelerated) 서비스를 대체할 최신 이메일 보호 서비스(Protective Email Services)를 개발 중

⑤ 방어 DNS(Protective Domain Name System)

❍ SCA 솔루션* 외에도 DNS 조회(lookup)는 인터넷 인프라에서 사이버보안 정책과 가시성을 구현하는 데 널리 사용되는 삽입 지점을 제공

* 엔드포인트와 클라우드 애플리케이션 간의 네트워크 흐름에 정책을 적용하고 원격 분석 결과를 수집

❍ CISA 방어 DNS 솔루션에는 다음의 주요 기능이 포함

- 인터넷 프로토콜(IP) v4 및 v6 소스 주소 확인
- IP, 도메인, 하위 도메인 또는 레코드 유형별로 쿼리를 필터링
- 새로 생성된 도메인, 유사 도메인(homoglyph), 비표준 쿼리 구조 및 알려진 위험

도메인을 자동으로 차단

- 허용 쿼리, 차단(악성) 쿼리 및 비정상적인 오탐(false positives)* 비율을 측정하기 위한 자체 모니터링 휴리스틱(heuristic)**

  * 실제로 오류가 존재하지 않지만, 오류라고 보고하는 경우

  ** 기존의 악성코드를 토대로 패턴을 도출하여 향후 출현하게 될 악성코드의 패턴을 예측하는 것

- 직접 우회: 중요한 DNS 쿼리를 전송하기 위한 활용 사례를 위한 기능
- 위치 추적 차단
- 전송 계층 보안을 통한 DNS(DoT) 및 하이퍼텍스트 전송 프로토콜 보안을 통한 DNS(DoH)
- 연방 부처 및 CISA를 위한 원격 분석 수집(예: 아웃바운드 명령 및 제어 트래픽 탐지)

⑥ 엔드포인트 보안 서비스

❍ 클라우드 비즈니스 애플리케이션을 보호하고 제로 트러스트 접근 방식을 유지하기 위해 모든 엔드포인트(모바일, 서버, 가상 머신, 데스크톱 포함)에 대한 관리 체제 확립은 매우 중요한 요소

※ 모바일 보안은 SCuBA 프로젝트의 범위에 포함되지 않지만, 연방 부처는 모바일 및 데스크톱 기기에서 안전하게 액세스할 수 있도록 클라우드 비즈니스 애플리케이션을 배포하고 구성해야 함

〈 주요 엔드포인트별 연방 보안 관리 체계 지침 〉

엔드포인트 유형	보안 관리 체계 지침
데스크톱 엔드포인트 보안	• 호스트에 대한 상태 평가를 근거로 부처 데이터에 대한 액세스를 제한하도록 클라우드 비즈니스 애플리케이션 액세스 정책을 구성 • 기관 엔드포인트 보안 정책을 준수하는 부처 관리 기기 상에서만 이루어지도록 강제해야 함 • EDR 제품을 활용하여 정책 결정을 내리는 데 필요한 신호를 수집하고 엔드포인트의 핵심적인 보안 요소들의 가시성을 부여하여 사이버보안 대응을 촉진
모바일 엔드포인트 보안	• 모바일 디바이스 및 애플리케이션을 보호하고 관리하기 위해 CDM* 프로그램에서 엔터프라이즈 모빌리티 관리(EMM) 기능을 배포하도록 지원 * 지속적 진단 및 완화(Continuous Diagnostics and Mitigation): 사이버보안 도구, 통합 서비스 및 대시보드를 제공하여 정부 네트워크 및 시스템 사이버보안을 강화하기

	위한 CISA 프로그램 • EMM 솔루션을 통해 부처는 ▲디바이스 구성 및 디바이스 규정 준수 관리 ▲디바이스 모니터링 및 추적 ▲허가 모바일 앱 관리 ▲모바일 위협 방어 및 모바일 애플리케이션 검사를 통한 악성 모바일 앱 탐지 및 해결 ▲네트워크 기반 공격 및 취약한 구성 발견 및 대응 ▲모바일 디바이스에서 프로비저닝 된 자격증명 발급 ▲수명 주기 관리 등을 지원

❍ 한편, CISA는 기업과 소비자의 모바일 디바이스 사이버보안 개선을 위한 역량 강화 가이드[6]와 부처의 제로 트러스트 계획과 로드맵 개발 지원을 위한 백서인 '기업 모빌리티 제로 트러스트 원칙 적용[7]'도 공표한 바 있음

⑦ 애플리케이션 보안 구성

❍ 클라우드 서비스 내의 모든 정보 자산과 클라우드 서비스에 대한 연결을 보호하기 위해 일관되고 효과적이며 관리가 가능한 보안 구성을 보장하는 것이 필수적

❍ 현 시점 SCuBA 프로젝트는 연방 정부 환경 전반에 걸쳐 쉽고 빠르게 채택할 수 있도록 최소한의 보안 기준점(Security Baseline) 지침을 개발, 테스트 중

- 보안 기준점은 어떤 서비스 또는 시스템 환경에서라도 기본적으로 충족해야 하는 일련의 기초적 보안 목표를 정의

  ※ 보안 기준점은 ICAM, 협업, 클라우드 액세스 보안 브로커 기능, 위협 인텔리전스, 탐지, 완화, 클라우드 스토리지, 클라우드 네이티브 이메일 서비스 보안, 클라우드 네이티브 비즈니스 애플리케이션을 포함한 SCuBA 보안 아키텍처의 전체 범위를 다루고 있음

- Microsoft 365나 Google Workspace를 사용하는 부처는 해당 권장 사이버보안 구성을 손쉽게 채택할 수 있음
- CISA는 연방 부처의 의견과 지원을 받아 개발을 추진 중이며, 해당 지침을 유지 관리하고 갱신하는 것은 일관된 보안 태세를 보장하는 데 필수적
- 보안 기준점은 자동화를 염두에 두고 개발되어 애플리케이션의 일관성을 개선하고 배포 시간을 단축

---

6) CISA(2021.11.24.), CISA Releases Capacity Enhancement Guides to Enhance Mobile Device Cybersecurity for Consumers and Organizations

7) CISA(2022.3.8.), Applying Zero Trust Principles to Enterprise Mobility

❍ 부처는 부처 외부의 다른 이해관계자와의 협업(콘텐츠, 캘린더 등을 공유)과 부처 데이터 보호 간의 균형을 유지해야 함

- 부처는 최소한 클라우드 비즈니스 애플리케이션에 탑재된 규칙 시스템을 활용하여 테넌트 간 데이터 공유를 감시해야 함
- 필요 시 부처는 임무 요구사항에 따라 특정 유형의 데이터*에 대한 테넌트 간 공유를 차단해야 할 수도 있음

* 예: 문서가 아닌 사용/미사용 등의 상태 정보 공유

⑧ 사이버 가시성 및 eVRF 분석 프레임워크

❍ 연방 부처는 클라우드 비즈니스 애플리케이션 사용과 관련된 공격 지표(IOA, Indicators of Attack)* 및 침해 지표(IOC, Indicators of Compromise)**를 탐지하기 위해 운영 및 기술***에 대한 사이버 가시성을 확보하고 적용

* 사이버 공격자의 공격 의도를 보여주는 디지털 또는 물리적 증거. IOA 탐지는 공격자가 사용한 특정 도구나 방법보다는 공격자의 동기에 초점을 맞춤

** 시스템 로그 항목이나 파일에서 발견되는 데이터와 같이 시스템이나 네트워크에서 잠재적으로 악의적인 활동을 식별하는 포렌식 데이터 증거

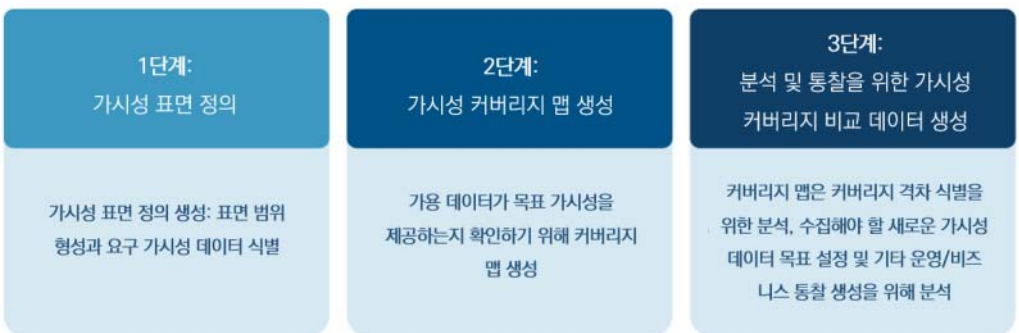
*** 예: 자산, 사용자, 시스템, 데이터, 이벤트, 로그에 대한 인사이트

❍ 사이버 가시성 확보 활동을 수행할 때는 eVRF 분석 프레임워크를 참조해야 함

- eVRF 가이드북은 사이버 가시성을 수집하고 적용하여 위협을 감소하기 위해 CISA, FCEB 기관 및 기타 파트너 업체들이 사용할 수 있는 개념, 요구사항 및 메커니즘을 정의
- SCuBA 맥락에서의 eVRF 개념은 "사이버상에서 관찰 가능한 데이터가 존재하거나 존재해야 하는 디지털 환경"으로 정의되는 가시성 표면(visibility surface)을 의미
- eVRF 디지털 환경에는 악성 및 양성 활동의 증거를 제공하는 모니터링, 감사 및 경고 서비스를 통해 생성된 애플리케이션 로그, 엔드포인트 액세스 로그, 프록시 로그, 서비스 로그, 보고서 및 경고 등이 포함
- 클라우드 비즈니스 애플리케이션 제공업체나 써드파티 업체가 제공하는 위협 탐지 서비스는 탐지된 이상 징후를 전달하고, 위협을 예방하고, 완화 조치를 적용해야 함

❍ eVRF 가이드북에서는 사이버 가시성을 달성하기 위한 3가지 업무 흐름 단계로 ① 가시성 영역 정의 ② 가시성 범위 맵 생성 ③ 분석 및 인사이트를 위한 범위 비교 생성을 순차적으로 제시

〈 eVRF 업무 플로우 〉



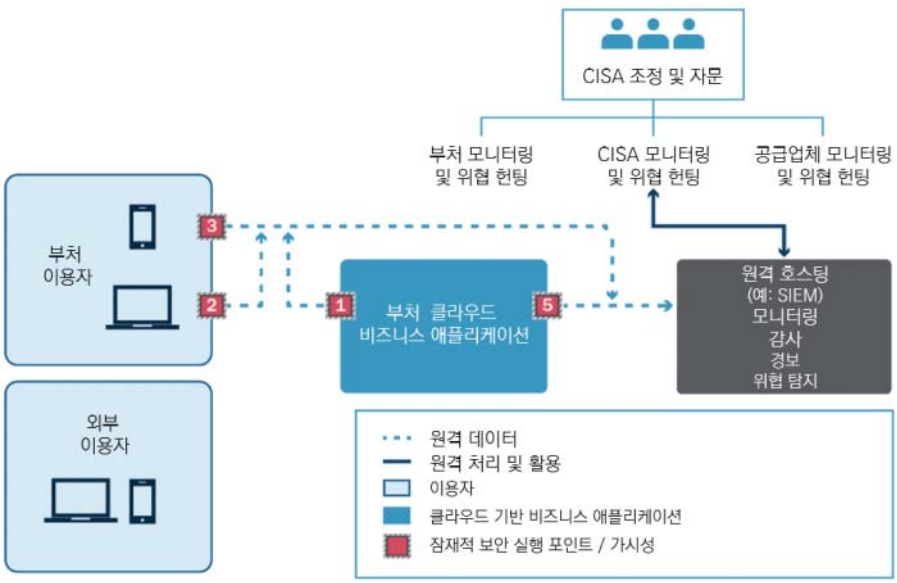
- eVRF 가이드북에 따르면 CISA는 eVRF 가시성 표면 정의 및 요구사항 적용 범위 맵을 개발해야 하며, 벤더/서비스 제공업체는 eVRF를 준수하고 자사 제품의 가시성 격차를 최소화해야 함

⑨ 원격(Telemetry) 생성 및 처리

❍ 사이버 분석에 수반되어야 하는 가시성의 품질과 완전성은 관찰 지점과 원격 분석 생성 시스템의 구성 요소에 따라 상이

- TRA에서는 클라우드 비즈니스 애플리케이션의 효과적인 보안 가시성 및 관리를 보장하기 위해 부처들이 사용하는 ▲로깅 ▲모니터링 ▲감사 ▲경보 ▲위협 탐지 등의 서비스를 설명

〈 SCuBA 원격 정보 및 로그 수집 개념도 〉



〈 원격 생성 및 처리 시 동작별 보안 가시성 및 품질 보장 방안 〉

동작 유형	보안 가시성 및 품질 보장 방안
로깅	• 부처는 가시성 향상, 자산 관리, 사고 대응 등을 위해 종합적이고 독립적인 클라우드 보안 기능을 포함한 클라우드 서비스를 구성해야 함 • AI 엔진을 결합하면 병렬 처리를 활용하여 저렴한 비용으로 효율적으로 모니터링 및 위협 방지가 가능 – SCuBA eVRF 통합 문서(workbook)를 기반으로 다양한 TTP를 탐지하기 위해 어떤 로그 데이터를 수집 및 공유할 것인지 결정 – 적절한 수준의 가시성을 확보하려면 여러 관찰 지점에서 로그를 수집해야 함
모니터링	• 기록 보관 및 규정 준수 목적으로 저장하는 로그도 있으나, 광범위한 원에서 로그에 대한 모니터링 필요 • 클라우드 비즈니스 애플리케이션의 로그를 모니터링 서비스에 통합하여 메트릭스 추적 상태를 업데이트하고, 리소스 매핑을 수행하며, 보안 보고서를 생성하여 감사, 경보 및 위협 탐지를 촉진
감사	• 부처는 보안 감사를 통해 애플리케이션 로그와 보안 보고서를 추가로 분석해야 함 • 이를 통해 관련된 사용자, 프로세스, 서비스 또는 애플리케이션, 수행한 작업, 발생 장소, 발생 시기 및 기간, 발생 방법, 영향 등 잠재적인

	이벤트에 대한 다양한 상황별 정보를 확보 • 모든 로그는 NIST 지침에 규정된 대로 네트워크 시간 프로토콜 표준을 사용해야 함 • 정기 감사 진행과 함께 조직의 가시성(비즈니스 기능, 우선순위, 위험 및 협업 계약 인지)을 검토하면 부처에 다양한 통찰을 제공
경보	• 부처는 모니터링 및 감사 데이터를 기반으로 자동 생성되는 비즈니스 애플리케이션에 대한 경보 체제를 구축해야 함 • 비즈니스 애플리케이션의 다양한 문제를 신속하게 식별하여 검토 및 수정할 수 있어야 함 • 부처는 정기적인 테스트를 수행하고 경보를 검토하여 정확성 및 적시성 지표가 연방 요건을 준수하는지 확인해야 함
위협 탐지	• 서비스 거부, 데이터 유출, 멀웨어, 무단 권한 상승 및 계정 생성 등이 위협의 유형에 포함 • AI나 머신러닝 등 자동화된 수단이나 수동 검색을 통해 위협을 탐지할 수 있음 • 데이터 시각화 도구와 대시보드는 부처 보안 전문가의 클라우드 비즈니스 애플리케이션 내 위협 탐지를 용이하게 할 수 있음 • 부처는 기본 서비스를 검토하여 클라우드 비즈니스 애플리케이션에 대한 위협 탐지 기능에 이상 징후 탐지, 머신러닝, 위협 인텔리전스 등을 통합해야 함 • 서비스 테스트 후생성된 경보의 정확성과 탐지 지연 시간 등을 벤치마킹해야 함 • 또한 부처는 위협 탐지 기능과 선제적 위협 헌팅 활동에서 얻은 교훈을 바탕으로 로깅, 모니터링, 감사, 경보 정책과 절차를 업데이트해야 함

⑩ 책임 공유 모델

❍ SCuBA TRA는 부처, CISA 및 공급업체 간의 공동 책임 모델을 활용

- 각 주체는 강력한 보안 태세를 보장하고 방어 보안 제어와 가시성, 탐지 및 대응과 관련하여 목표 보안 결과 달성에 중요한 역할을 담당

〈 SCuBA 보안 태세 강화를 위한 주체별 역할 〉

구분	방어 보안 통제 및 서비스	가시성, 탐지 및 대응
부처	• 선택 클라우드 비즈니스 애플리케이션 플랫폼을 SCuBA 솔루션 아키텍처 문서에 따라 적절하게 구성 • SCuBA 배포가 다른 보안 서비스의 적절한 기능을 활용하도록 보장	• 경보 분류 및 제한된 범위의 인시던트에 대한 대응 등 일선 보안 운영 담당 • 로그 수집 및 보관과 CISA 가이드라인 준수 • CISA에서 제공하는 공유 서비스를 활용하여 로깅 및 보안 모니터링 운영을 개선 • 원격 측정 구성 및 가시성 범위 맵 생성 적용과 관련하여 공급업체와 협력 • 특정 클라우드 비즈니스 애플리케이션에 eVRF 개념을 적용하여 적절한 로그를 생성하고 SCuBA 보안 기준점에 기반하여 보안 제어가 실시
공급업체	• 비즈니스 애플리케이션의 기반이 되는 SaaS 플랫폼 보호 • 필요 시 독립 소프트웨어 벤더 솔루션과의 통합(예: 이메일 보안 서비스 또는 ID 서비스 제공)을 포함하여 보안 제어를 구현하는 데 필요한 제품 기능을 부처에 제공	• 취약성 및 침해 관련 정보를 CISA 및 부처와 공유 • 서비스 제공 전반의 동향과 위협 활동 파악 • 테넌트가 감지할 수 없는 위협에 대응하기 위해 제품 업데이트 제품 제한 사항 및 기능에 대한 이해를 돕기 위한 교육 및 훈련 기회 제공
CISA	• SCuBA 비전을 실현하는 데 필요한 기본 보안 요구 사항, 아키텍처 및 구성 정의 • TRA의 일부(예: 방어 이메일 서비스(PES))를 구현하기 위한 공유 서비스 개발	• 가시성 요청을 구체화하고, 보안 기준점을 업데이트하며, 대응 지원 실시 • 부처 위협 발견 및 해결 지원 • 클라우드 공급업체와 협력하여 보안 및 가시성 격차를 해소하고 클라우드 비즈니스 애플리케이션 보안 강화

Ⅲ 시사점

❍ 전 세계적으로 필수 보안 이슈로 자리 잡은 주요 기반시설 및 정부 공급망 공격에 대비하기 위해서는 온프레미스와 클라우드 환경 전반에 걸친 엔드포인트 보호와 정부 네트워크의 역량 강화가 필요

❍ SCuBA 프로젝트는 정부 부처가 준수해야 하는 최소한의(baseline) 시스템 사양과 규제 준수 조건을 제시함으로써 민감한 정보를 보호하는 데 초점을 두고 있음

- TRA는 정부 기관의 클라우드 구축과 최근 행정부 차원에서 적극적으로 추진 중인 제로 트러스트 프레임워크 구축 시 개별 부처들이 고려해야 할 다양한 기술 요건을 제안
- 특히 다수의 이해당사자가 관여하고 있는 정부 보안의 책임성을 위해 본 TRA에서는 정부 부처, 공급업체 및 조정 자문 역할을 하는 정부 기구인 CISA 각각의 역할도 구체적으로 제시한 점도 주목할만한 대목
- 이 같은 노력은 최근 연방 클라우드 보안 인증 프로그램(FedRAMP) 제시 준수 사항에 대해 미온적으로 대응 해온 연방 부처들에게도 경각심을 일깨울 수 있을 것으로 예상

※ 미국 회계감사원(Government Accountability Office)이 발표한 보고서('23.5)[8]에 따르면 재무부, 노동부, 국토안보부, 농무부 등 4개 연방 부처가 FedRAMP에 명시된 보안 요건을 미이행하는 것으로 확인

❍ 또한, 이번 문서들은 정부 기관의 클라우드 이전 및 통합 과정에서 빈번하게 발생하고 있는 해커들의 공격 표면(Attack Surface) 확보 활동을 저지하는 데에도 주안을 두고 있음

- TRA와 함께 시스템 전반에 대한 보안 가시성 확보를 위해 마련된 eVRF 관련 통합 문서는 미국 연방 정부의 공격 표면 관리(ATM) 대응력 강화에 일조할 것으로 기대

8) GAO(2023.5.18.), Cloud Security: Selected Agencies Need to Fully Implement Key Practices

ISSUE ②

호주, 공공서비스 분야 생성형 AI 활용 임시 지침 발표

Reading Point

- 호주 디지털혁신처(DTA), 생성형 AI 활용과 관련하여 공공서비스 직원이 활용할 수 있는 임시 지침 발표[9]
- 공공서비스에서의 생성형 AI 활용을 위한 윤리적 사용 원칙, 주요 사용 사례 등을 가이드라인으로 제시

Ⅰ 개요

❍ 호주 디지털혁신처(DTA)와 산업과학자원부(DISR)는 공공서비스 직원*의 생성형 AI** 사용에 대한 임시 지침을 발표

* 지침 내 Australian Public Service(APS) staff로 명시

** 생성형 AI(generative AI) : 텍스트, 오디오, 이미지 등의 기존 콘텐츠를 활용하여 유사한 콘텐츠를 새로 만들어내는 인공지능 기술

❍ DTA의 생성형 AI에 대한 임시 지침은 ▲책임 있고 안전한 기술 사용 및 발생 가능한 피해를 최소화하고 ▲신뢰할 수 있으며 ▲공정한 결과를 창출하는 것을 목표로 함

- ChatGPT, Bard AI, Bing AI와 같은 공개 생성형 AI가 정부 업무에 사용될 때, 잠재적 위험과 이점을 평가해야 함
- 평가 시 지침의 원칙(Principles)과 전술적 지침(Tactical Guidance)을 활용해야 함

9) Global government Forum(2023.7.11.), Australia issues guidance on how public servants can use AI in government

Ⅱ AI 활용 관련 원칙

1 생성형 AI 활용 윤리 원칙

○ 호주 정부는 생성형 AI의 윤리적 사용을 위해 4가지 원칙을 제시하였으며, 해당 원칙은 호주 공공서비스 직원의 책임감 있고 안전한 생성형 AI 활용을 보장하기 위해 설계됨

- **(위험 가능성 고려)** 공개적으로 생성형 AI 활용 시 위험성이 낮은 경우에만 사용해야 함*
  * ▲대량의 정부 자료나 기밀정보, 민감정보를 입력하는 경우 ▲의사결정이 내려지는 경우 ▲정부 시스템 내에서 코딩 결과가 사용되는 경우 등을 허용할 수 없는 위험 사례로 제시
- **(신뢰성)** 데이터 출처와 생성형 AI의 특성에 대한 이해를 바탕으로 생성형 AI가 제공하는 결과물에 대한 신뢰성을 비판적으로 검토할 필요가 있음
- **(원칙 준수 및 개인정보 보호)** 생성형 AI에 정보를 입력할 때 정보 및 데이터와 관련된 법률 및 정책을 준수해야 하며, 기밀정보 또는 민감정보를 유추할 수 있는 정보를 입력해서도 안 됨
- **(책임감 있는 의사결정)** 책임감(accountability)은 공공서비스 활동에서의 핵심 원칙이라 할 수 있으며, 생성형 AI는 조언은 할 수 있지만 최종 의사결정은 사람이 검토해야 함

2 전술적 지침

○ 생성형 AI 활용 시 4가지 윤리 원칙을 구현하기 위해 전술적 지침(Tactical Guidance)을 제시

- 업무 수행 시 생성형 AI를 활용할 때 공무원은 기업 자격 증명*을 이용하여 가입 또는 로그인해야 함
  * 업무 이메일을 사용자 ID로 사용하고 새로운 고유 암호를 만들어야 하는 것을 뜻함
- 신뢰할 수 있는 출처의 링크만 클릭해야 하며, 악성코드 포함 가능성에 따라 생성형 AI에서 생성된 모든 파일을 주의하여 처리해야 함
- 호주 정부의 AI 윤리 원칙과 아키텍처(AI 가이드라인)에 부합해야 함

3 호주의 AI 윤리 원칙

❍ 호주의 AI 윤리 원칙은 AI를 안전하고 신뢰할 수 있도록 설계함

- 호주 국민에게 안전하고 신뢰성 있는 결과를 제공하고, AI 적용에 따른 부정적 영향에 대한 위험을 감소
- 기업 및 정부에서 AI 설계·개발·구현 시 수준 높은 윤리적 기준을 작용할 수 있음

❍ **(개인·사회 및 환경 복지 기여)** AI 시스템은 수명주기(lifecycle) 전반에 걸쳐 개인, 사회 및 환경에 도움이 되어야 함

- 전 세계적인 문제를 해결하는 데 도움이 되는 AI 시스템은 장려해야 하며, AI 시스템은 미래 세대를 포함하여 모든 사람에게 이익이 되도록 사용되어야 함

❍ **(민주적 사회에 기여)** AI 시스템은 인권, 다양성, 개인의 자율성을 존중해야 함

- AI 시스템은 인권 존중 및 보호, 다양성 존립, 자율성 존중, 환경 보호 등을 통해 평등하고 민주적인 사회가 작동할 수 있도록 도움이 되어야 함

❍ **(형평성 준수)** AI 시스템은 포괄적이고 접근용이 해야 하며, 개인, 지역사회에 대한 부당한 차별을 수반하거나 초래해서는 안 됨

- AI 시스템은 사용자 중심이어야 하며, 상호작용하는 모든 사람이 관련 제품 또는 서비스에 접근할 수 있는 방식으로 설계되어야 함
- 이는 연령, 장애, 인종, 성 등과 관련하여 취약한 그룹에 AI가 영향을 미칠 수 있다는 점이 있어 특히 중요한 원칙임

❍ **(개인정보 보호 및 보안)** AI 시스템은 개인정보 및 데이터 보호를 존중하고 보안을 보장해야 함

- AI 시스템에서 모든 데이터에 대한 적절한 데이터 거버넌스와 관리뿐만 아니라 잠재적 보안 취약성 식별 및 적대적 공격에 대한 회복력을 보장하는 것을 의미

❍ **(신뢰성과 안전성)** AI 시스템은 의도된 목적에 따라 안정적으로 작동해야 함

- AI 시스템은 신뢰할 수 있고 재현가능한(reproducible) 속성을 보장해야 함을 뜻하며,

의도된 목적을 충족하는지 확인하기 위해 지속적으로 모니터링 및 테스트해야 함

❍ **(투명성 있는 공시)** 사람들이 AI에 의해 상당한 영향을 받고 있음을 인지하고 AI 시스템과 인간이 어떠한 관계를 형성하고 있는지에 대해 투명성과 책임 있는 공시가 필요

❍ **(이의 제기 프로세스 존재)** AI 시스템이 사람, 지역사회, 환경 등에 중대한 영향을 미칠 때, 사람들이 AI 시스템의 사용 또는 결과에 이의를 제기할 수 있는 프로세스가 존재해야 함

- AI 시스템에 이의를 제기할 수 있는 효율적이고 접근 가능한 메커니즘을 비롯하여, 사람의 판단을 적절하게 활용할 수 있는 효과적인 감독 시스템이 필요

❍ **(결과에 대한 책임감)** 책임자들은 AI 시스템의 결과에 대해 식별 가능하고 책임을 질 수 있어야 하고, 감독이 가능해야 함

- 이는 설계, 개발, 배치 및 운영하는 AI 시스템의 결과에 책임을 인정하는 것을 목표로 함

Ⅲ 공공부문의 AI 지침

1 공공 부문 및 호주 APS의 AI 사용

○ 2030년까지 AI와 관련된 기술이 세계 경제에 20조 달러 이상을 기여할 것으로 추정

- AI 기술은 정부 및 정부 서비스 사용자에게 자원 관리, 효율성 개선, 공공 서비스 강화 등의 이점을 가져다 줄 것으로 기대
- AI 시스템은 작업을 개선하고 효율성을 향상시킬 수 있음에도 불구하고, 규제 또는 공공 서비스에 해당 기술을 적용하는 것이 개인과 기업에 영향을 미칠 수 있는 부정적 효과도 고려해야 함

○ AI 기능은 호주 연방 기관의 서비스 관리 관련 챗봇 및 가상 비서, 부정 탐지 등 호주 여러 정부 기관의 솔루션에 사용되고 있음

- AI 관련 프로그램은 정부 기관, 개인, 기업 등 다양한 주체에 영향을 미칠 수 있으므로 AI 시스템을 사용하려는 호주 연방 기관은 AI 시스템 채택·적용 관련 거버넌스, 위험, 윤리적·법적 측면에서 주의를 기울여야 함

2 AI 활성화를 위한 호주 정부의 노력

○ AI의 중요한 특성 및 정부에서의 AI 활용에 따른 잠재적 이점으로 인해 호주 정부에서 AI와 관련하여 다양한 이니셔티브(initiative)와 조사가 시작됨

- 의사결정을 위한 AI 이니셔티브, 자동화 의사결정 및 AI 규제 백서, 자동 부채 환수 시스템(Robodebt)에 대한 호주 특별조사위원회(royal commission)의 조사 등이 이러한 이니셔티브 및 조사 활동에 해당

○ 공공부문의 AI 지침을 통해 정부는 기존 AI 원칙을 실천하기 위한 현실적인 상황과 지침의 격차를 좁히려 한다는 목표를 명시

- AI 기술의 적절한 설계, 구축 및 사용에 대한 명확성을 제공함에 따라 호주 정부 기관에서

AI를 활용하는 데 신뢰를 제고하고자 함

- 이러한 목표를 달성하기 위해 공공 부문에서는 AI 활용에 따른 위험*을 인식하는 것이 중요

  * AI 알고리즘에 내장된 데이터 비효율성과 편향성이 해결 또는 완화되지 않을 시 의도하지 않은 대규모 피해가 발생할 수 있음

○ 공공부문 AI 지침의 주요 대상은 ▲AI 기술의 산출물에 관여하고 ▲AI 기술에 의해 지원되는 비즈니스 프로세스 또는 정책 결과에 책임이 있으며 ▲기관 내 AI 기술 사용과 관련된 결정에 책임이 있거나 ▲AI 기술을 직간접적으로 운영하는 호주 공공 서비스 구성원임

3 공공부문의 AI 채택

○ **(거버넌스)** 거버넌스는 조직의 시스템과 책임을 져야 하는 메커니즘을 포괄하며 적절한 거버넌스 구조는 공공부문에서 AI의 윤리적이고 책임 있는 사용을 실현하는 데 중요

○ **(AI 도입 전 고려 사항)** AI를 비즈니스 프로세스 및 기관에 도입하기 전 다양한 사항을 고려해야 함

- ▲비즈니스 결과를 제공하는 기존 접근 방식을 어떻게 개선할 것인지 ▲非 AI 및 기존 시스템과 프로세스를 고려할 수 있는지 등을 고민해야 하는 사항으로 제시

○ **(의사결정에 대한 책임감)** 비즈니스 책임자 및 의사 결정자는 AI를 활용한 의사결정에 책임이 있으며, AI 프로세스 내 기술 적용과 산출물에 대한 이해가 필요

- AI 기술 개발 및 유지보수에 대한 감독은 특정 ICT 거버넌스 협정에 국한하지 않고 기존 의사결정 및 책무 체계에 통합되어야 함
- AI 기술 관련 거버넌스 기구는 AI 사용 및 의사결정 지원 방식을 검토하고 수용할 수 있는 보고 통로가 존재해야 하며, AI 기술 작동 방식에 대한 충분한 이해가 필요함

○ **(위험 관리)** 위험 감수 수준(risk tolerance)은 AI 기술에 대한 각각의 사용 사례에 의해 결정되어야 하며, 각 정부 기관 내 기존 위험 관리 프레임워크와 일치해야 함

○ **(위험 관리 프레임워크 활용)** 기존 위험 관리 접근 방식에 맞추어 조정된 위험 관리

프레임워크*를 활용하여 AI 시스템의 위험을 평가하고 관리해야 함

* 뉴사우스웨일즈 AI 인증 프레임워크(NSW AI Assurance Framework), 아오테아로아 뉴질랜드 알고리즘 헌장(Algorithmic Charter for Aotearoa New Zealand), 캐나다 재무부의 자동화된 의사결정에 대한 지침(Directive on Automated Decision Making) 등을 참고할 수 있는 예시로 언급

Ⅳ 시사점

❍ 생성형 AI는 정부에 새롭고 혁신적인 기회를 제공하지만, 빠른 속도로 진화함에 따라 생성형 AI의 사용에 관련된 위험을 고려 및 평가할 필요성이 증대

- 호주 DTA의 최고 경영자 Chris Fechner는 AI 공공서비스 직원들이 기술 사용과 관련된 위험 평가 시 참고할 수 있는 지침에 대한 요구가 증가하고 있다고 설명

❍ 호주뿐만 아니라 전 세계 정부에서 공공부문의 AI 활용 규칙을 만드는 데 고려하고 있으며, 이 중 몇몇 국가는 공공부문의 AI 활용에 대한 지침을 발표하거나 실태 조사를 진행

❍ 2023년 6월 영국 내각부(UK Cabinet Office) 또한 생성형 AI 사용에 대한 공식 지침[10]을 발표한 바 있음

- 공공서비스 직원이 생성형 AI를 활용할 수 있는 적절한 사례 및 부적절한 사례를 제시
- 예를 들어, 생성형 AI를 통해 기존 정책 방향의 변화에 대한 보고서를 작성하는 것은 기술적으로는 가능하지만, 공개적으로 사용할 수 있는 생성형 AI에 민감한 자료를 입력해야 할 가능성이 높아 생성형 AI 사용을 금지하는 것을 사례로 제시

❍ 글로벌정부포럼(Global Government Forum, GGF)의 조사에 따르면 캐나다 공무원들은 이미 업무에 AI를 활용 중인 것으로 나타남

- 캐나다 전역의 1,320명의 공공 서비스 제공 직원 중 10% 이상이 업무에 ChatGPT와 같은 AI 플랫폼을 사용했다고 응답했으며, 많은 양의 데이터 처리 및 공공 서비스 제공 관련 실시간 분석 및 모니터링 등에서 AI 활용의 긍정적인 부분으로 나타남
- 그러나 조사 대상 공무원 중 절반(48%)에 달하는 응답자가 AI 기반 의사결정 및 행동에 대한 책임에 대해 매우 우려한다고 응답하는 등 부정적인 의견도 존재

10) Guidance to civil servants on use of generative AI(2023.6.29.)

NEWS 1 두바이, 7가지 새로운 디지털 전략 발표[11)]

❍ 두바이 정부는 새로운 디지털 전략 7가지* 핵심 분야를 발표('23.6.23.)

* 디지털 도시, 디지털 경제, 데이터 및 통계, 디지털 인재, 디지털 인프라, 사이버 보안, 디지털 경쟁력

〈두바이의 새로운 디지털 전략 7가지〉[12)]

❍ 지속적인 디지털 경험을 위한 통합된 도시를 목표로 하는 '디지털 도시 경험 계획(Digital City Experiences initiative)'을 수립

- 시민, 기업이 효율적인 디지털 경험을 즐길 수 있도록 통합된 디지털 채널 제공 예정

❍ 사용자들이 모든 부문에서 데이터베이스와 디지털 서비스에 접근할 수 있는 새로운 버전의 공식 웹사이트 'Dubai.ae' 공개

- 도시 서비스, 정책 향상을 위해 지역사회와 정부가 상호작용을 할 수 있는 e-참여 섹션 제공
- 주민들의 삶의 질 향상을 위한 아이디어를 공유하거나 토의 및 제안을 할 수 있는 공간을 제공

❍ 관련 부처가 다양한 채널을 통해 모니터링을 할 수 있고 정부의 업무수행능력을 실시간으로

---

11) Gulf Business(2023.6.22.), Dubai: Sheikh Hamdan launches Digital Strategy, new digital projects

12) 사이버 복원력; 사이버물리시스템에서 임무를 실패 후 얼마나 빨리 복구되는가를 표시함 (TTA 정보통신용어사전)

평가할 수 있는 '두바이 처리 지표(Dubai Transaction Index)'를 검토

- 사용자는 'DubaiNow' 앱을 통해 그들이 요청한 서비스의 진행현황을 추적 가능

❍ 생성 AI 개발을 목표로 '혁신적인 디지털 어시스턴트 계획(Innovative Digital Assistant Initiative)' 발표

- 생성 AI의 개발은 'Smart Employee' 앱에 통합하여 정부 내 직원들이 빠르고 쉽게 접근할 수 있도록 제공

❍ 신뢰성 높은 데이터를 활용한 '두바이 리더십 대시보드(Dubai Leadership Dashboard)'*를 검토 중

* 대시보드에는 인구지표, 행복지수, 사업 라이선스, 관광, 해외 무역 거래량, 부동산 거래 등이 포함

❍ 정부 서비스 보안 향상을 위한 사이버 보안 사전 예방 시스템으로서 'Maha Project'를 소개

- 이는 온라인 정부 서비스를 보호하기 위한 진보화된 시스템으로 서비스의 취약한 부분을 모니터링

❍ 정부 시설 등에서 AI 기술을 활용한 'Happiness Meter and Environmental Quality IOTs' 검토

- 표정 인식 기술을 활용하여 특정 장소와 시각에 대중의 행복도에 대한 일반적 지표를 제공

NEWS 2 영국, 클라우드 우선(Cloud First) 정책 갱신[13)]

❍ 영국 중앙디지털데이터청(Central Digital and Data Office, CDDO)은 공공 부문에 퍼블릭 클라우드* 사용 촉구를 위한 클라우드 우선 정책을 갱신

* 클라우드 서비스 제공자가 제어하는 자원을 누구나 사용할 수 있도록 제공하는 클라우드 배포 모델

- 클라우드 우선(Cloud First) 정책에 따라 영국의 공공 부문은 신규 또는 기존 서비스 조달 시 퍼블릭 클라우드를 기본적으로 채택해야 함
- 이러한 정책은 중앙 정부에 필수적으로 도입되고 있으며, 이번 갱신을 통해 더욱 넓은 범위의 공공 부문에 강력히 권장

❍ 클라우드 우선 정책에 대한 지침이 갱신됨에 따라, 공공 부문에서 클라우드 공급업체 선택 시 준수해야 하는 9가지 원칙이 추가됨

- 제시된 9가지 원칙은 제한된 비용과 리소스 내에서 기술의 신속한 제공과 위험 감소 사이의 균형을 맞추는 것이 목표임

13) GOV.UK(2023.6.19.), Government Cloud First policy Tech Monitor(2023.6.22.), Government's 'cloud first' policy update urges more departments to use public cloud

〈 클라우드 공급업체 선택 시 준수해야 할 9가지 원칙 〉

구분	주요 내용
비즈니스 가치 제공	• 보다 높은 수준의 클라우드 서비스를 사용하여 성능, 탄력성, 보안 및 복구 가능한 서비스를 통해 비즈니스 가치를 신속하게 제공
코드 기반 인프라 구축	• 퍼블릭 클라우드 또는 SaaS*가 우선이나, 그렇지 않은 경우 프라이빗 클라우드** PaaS*** 및 IaaS**** 오퍼링을 사용하여 코드 기반 인프라를 구축 * 서비스형 소프트웨어(Software as a Service, SaaS)는 클라우드 서비스 제공자가 필요로 하는 애플리케이션을 가상화된 서비스로 제공하는 클라우드 서비스 (출처: TTA 정보통신용어사전) ** 프라이빗 클라우드(private cloud)는 특정 사용자(기업이나 조직)가 원하는 자원을 독점 사용하고 관리, 제어할 수 있도록 제공하는 클라우드 배포 모델 (출처: TTA 정보통신용어사전) *** 서비스형 플랫폼(Platform as a Service, PaaS)은 클라우드 서비스 제공자가 프로그래밍 언어와 개발 환경을 포함한 플랫폼 기능을 제공하여 사용자가 애플리케이션을 배포, 관리, 실행할 수 있는 클라우드 서비스 (출처: TTA정보통신용어사전) **** 서비스형 인프라스트럭처(Infrastructure as a Service, IaaS)는 클라우드 서비스 제공자가 하드웨어, 가상 머신, 저장장치, 네트워크 등의 인프라스트럭처(Infrastructure) 자원을 가상화된 서비스로 사용자에게 제공하는 클라우드 서비스 (출처: Crown Commercial Service)
보안 고려	• 퍼블릭 클라우드가 아닌 프라이빅 클라우드를 사용해야 하는 경우, 5가지 기본 클라우드 요소*를 제공해야 하며, 우수한 클라우드 서비스를 채택함으로써 보안상 이점을 얻을 수 있는지 고려해야 함 * ▲온디맨드(on-demand) ▲광범위한 네트워크 접근 ▲리소스 풀링(pooling) ▲신속한 탄력성 ▲서비스 측정
크라운 호스팅 활용	• 온프레미스 방식을 선택할 수밖에 없는 경우, 최상의 옵션인 크라운 호스팅*을 사용하여 신속하게 계약하고 위험을 줄여야 함 * 영국 내각 정부기관과 민간 기업 Ark Data Centres 간 합작 법인인 Crown Hosting Data Centres가 정부 데이터를 호스팅하는 서비스 (출처: Crown Commercial Service)
세계 공용 클라우드 서비스 사용	• 해외 또는 전 세계에서 제공되는 클라우드 서비스를 사용할 수 있도록 지원
재사용 코드 지원	• 공공 부문 전반에 걸쳐 클라우드 구성, 아키텍처 등을 조정하여 클라우드에서 재사용할 수 있는 코드를 지원
NCSC 클라우드 보안 원칙 준수	• NCSC*의 클라우드 보안 원칙에 따라 항상 합의된 표준으로 시스템과 서비스를 보호하도록 설계 * 영국 국가사이버보안센터(National Cyber Security Center)
최상의 상업 관행 활용	• 영국 조달청이 형성한 공급업체 관계를 바탕으로 한 단일 정부 집단 구매력(one-government collective buying power)을 통해 최상의 상업 관행을 활용
공급업체 지원	• 새로운 서비스나 기능을 구축할 때마다 모든 클라우드 공급업체를 고려함으로써, 클라우드 공급업체 간 경쟁과 제품 개선에 대한 투자를 장려

❍ 클라우드 우선 정책 지침 갱신와 관련하여 업계 전문가들은 혁신적이라고 평가

- 사이버 보안 기업 Forescout Technologies의 이사 Fabricio Brasileiro는 클라우드 구성을 표준화하고 설계에 따른 보안 측정을 채택함으로써 시스템과 서비스의 상호 운용성과 보호를 보장할 수 있다고 설명
- 이를 통해 정부 기관 간 원활한 협업이 가능해져 공공 서비스 제공의 효과성 및 효율성 향상 가능

❍ 반면 일각에서는 오픈 소스와 지속가능성(sustainability) 측면을 간과하고 있다고 우려

- 오픈 소스[14] 기술 옹호 단체인 OpenUK의 CEO Amanda Brock은 데이터 센터 환경에서 오픈 소스 사용 시 필요 하드웨어 및 정부 부처의 탄소 발자국을 크게 감축할 수 있다고 주장
- 반면 갱신된 클라우드 우선 정책은 오픈 소스를 인정하지 않는다고 지적하며, 향후 클라우드에 대한 의사 결정 시 오픈 소스의 중요성을 명확하게 이해할 필요가 있다고 부연

14) 오픈 소스(Open source)는 소프트웨어의 설계도에 해당하는 소스 코드를 인터넷 등을 통하여 무상으로 공개하여 누구나 그 소프트웨어를 개량하고, 이것을 재배포할 수 있도록 하는 소프트웨어 (출처: TTA정보통신용어사전)

NEWS 3 영국, 통합 로그인 서비스(GOV.UK One Login) 개선[15]

❍ 영국 정부 통합 로그인 서비스(GOV.UK One Login)* 프로그램 강화 및 확대 시행 계획 발표

* 이용자가 하나의 이메일 주소 및 패스워드를 통해 본인의 신분을 인증하여 모든 정부 공공 서비스에 접근할 수 있도록 하는 운영체계를 의미

- 영국 내각실의 발표에 따르면 기존의 영국 정부 포털사이트(GOV.UK)에 접근하기 위해 이용자가 계정을 설정할 수 있는 방법은 191개, 포털을 통해 로그인 할 수 있는 방법은 무려 44개에 달해 이용자들의 접근성 및 효율성은 다소 떨어지는 상황이었음
- 이번 정부가 발표한 "통합 로그인 서비스" 프로그램 확대를 통해 향후 3년간 약 7억 파운드의 경제적인 비용 절감 효과가 발생할 것으로 예상

❍ 통합 로그인 서비스(GOV.UK One Login)는 기존 영국 정부의 디지털 신원 확인 시스템인 "Verify"*를 개선하기 위해 도입되었음

* 영국 정부 디지털 서비스(Goverment Digital Service, GDS)에 의해 개발된 신원 확인 시스템으로 이용자는 온라인 공공 서비스를 사용하기 위해 정부가 인증한 특정기업들(Verizon, Experian 등)을 통해 신분을 인증받는 형태이며 2016년 5월 본격 도입

- 2016년 도입되었던 기존 영국의 디지털 신원 확인 시스템인 Verify는 예상 대비 낮은 이용자 수, 높은 개발비용, 이용자 등록 문제 등으로 인해 정부 당국으로부터 운영종료를 권고받은 바 있으며, 2023년 3월 공식적으로 종료되었음
- 영국 정부 디지털 서비스(Government Digital Service, GDS)의 발표에 따르면 통합 로그인 서비스(GOV.UK One Login)는 이용자 편의성 등 기존의 Verify를 대폭 개선하였다고 밝힘

❍ 통합 로그인 서비스(GOV.UK One Login)는 도입 이후 현재까지 약 150만명의 이용자 수를 기록했으며, 8개의 영국 정부 기관이 서비스를 도입 및 운영 중

---

15) TECHMONITOR(2023.6.25.), GOV.UK One Login digital identity platform rolled out to eight services and 1.5m users

- 영국 정부는 약 150만 명의 이용자들이 해당 서비스를 통해 신원을 증명하였으며, 어플리케이션 다운로드 횟수는 약 200만 건 이상 기록하였다고 발표
- 현재 영국 공개제외원, 산업통상부, 운전면허국 등 8개 정부 기관이 통합 로그인 서비스(GOV.UK One Login) 시스템을 도입하여 운영 중

〈 통합 로그인(GOV.UK One Login) 지원 정부 부처 및 서비스 목록 〉

정부 부처명	주요 서비스 내용
Disclosure and Barring Service(DBS) (영국 공개제외원)	• 범죄 기록 확인 및 증명서 발급 등
Department for Business and Trade (영국 산업통상부)	• 국제 무역 및 기업 활동을 위한 허가 취득 등
Driver and Vehicle Standards Agency(DVSA) (영국 운전면허국)	• 차량 운전자 면허증 신청 등
Social Work England (영국 교육부 산하 사회복지 관련 기구)	• 사회복지사 등록 등
HM Land Registry (영국 토지등기국)	• 부동산 담보 증서, 관계서류 서명 등
Ofqual (영국 시험감독청)	• 자문가, 어드바이저 등록 등
Modern Slavery Unit (영국 노동착취 및 인신매매 전담반)	• 노동착취, 인신매매 관련 진술 등록 등
HM Revenue and Customs (영국 국세청)	• 법인세, 부가세 등 세금 관련 업무 등

❍ 영국 정부는 2025년까지 통합 로그인 서비스(GOV.UK One Login) 사용 정부 부처 확대 뿐만 아니라 신분 인증 방식 추가 등에도 노력
- 영국 정부는 전담 콜센터 개설을 하여 2025년까지 환경식품농무부, 노동연금부를 비롯한 약 100개의 정부 부처에 통합 로그인 서비스를 확대할 계획
- 또한, 현재는 이용자 최초 신분 인증을 위해 생체인식 거주허가증, 운전면허증, 여권만이 인정되나, 향후 다른 유형의 신분증을 추가로 허용할 계획이라고 밝힘

NEWS 4 스코틀랜드, 디지털 ID 서비스 개선 계획 수립[16)]

❍ 스코틀랜드 정부는 디지털 ID 서비스를 향상하고자 다양한 인증 방법에 대한 계획을 수립

- 스코틀랜드 정부는 2023년 2월부터 'ScotAccount' 시범 사업을 비공개 베타*로 운영
  * 온라인 게임 분야에서 제한된 인원을 대상으로 진행되는 테스트. 비공개 테스트(CBT) 이후 일반인 모두를 대상으로 공개 테스트(OBT)를 거쳐 완성작을 만듦
- 'ScotAccount'는 Disclosure Act 2020*를 바탕으로 사용자에게 세부 정보 제공
  * Disclosure Act 2020은 공개 시스템 환경에서 위험에 노출될 수 있는 대상을 보호하기 위한 입법 프레임워크
- PVG 과정[17)]을 거친 후 이메일 주소, 비밀번호, 그리고 2단계 인증단계를 통해 'ScotAccount'를 생성
- 사용자는 여권, 운전면허증, BRP(Biometric Residence Permit)[18)] 카드와 같은 공식 문서를 통해 신원 증명 가능

❍ 공공부문에서의 디지털 ID 활용은 대규모 사업 추진에 기여할 수 있을 것으로 예상

- Juniper Research는 디지털 ID 앱이 2027년까지 170억 달러 이상의 수익을 창출할 것으로 예상
- 전문가들은 정부가 디지털 ID 시스템을 향상시키고 정교화하는 데에 집중함으로써 성장세를 이끌 수 있다고 주장
- EU의 eIDAS 규정* 활성화에 따라 스코틀랜드에서도 디지털 ID 프로젝트에 투자를 장려할 것으로 예측
  * eIDAS 규제에 따라 모든 EU 회원국은 2024년까지 이용희망자 모두에게 '디지털 ID 월렛'을 제공해야 하며, Visa, Idemia, Thales와 같은 세계적 기술을 보유한 기업들과 디지털 ID 월렛 관련 프로젝트 협업 중

---

16) Biometric News(2023.6.27.), Scotland plans improvements to digital identity service based on pilot

17) 취약 그룹 보호 체계 (참고자료 : https://www.mygov.scot/pvg-scheme)

18) 합법적으로 영국에 거주함을 증명하는 허가증 (참고자료 : https://www.gov.uk/biometric-residence-permits)

NEWS 5 EU, 디지털 전환을 위한 핵심 성과 지표 선정 및 가이드라인 발표[19]

❍ EU집행위원회(European Commission)는 "2030 Digital Decade"* 목표 이행 상황을 모니터링하기 위한 핵심 성과 지표(KPI)를 선정

* 2030년 유럽의 디지털 전환을 위해 향후 10년간 추진하는 정책 프로그램으로 EU 회원국 간의 공동 목표 수립, 목표 달성을 위한 모니터링 체계 및 협력 메커니즘 구축 등이 포함됨

- 이번 선정된 핵심 성과 지표(KPI)는 디지털 인프라, 디지털 기술, 비즈니스 및 공공서비스 영역 등에서 각 회원국의 성과를 측정하기 위한 용도로 활용될 예정
- EU집행위원회는 해당 핵심 성과 지표(KPI)를 바탕으로 "2030 Digital Decade" 진행 상황에 대한 첫 번째 평가보고서를 2023년 하반기 내에 발표할 계획

❍ 또한, EU집행위원회는 성공적인 디지털 전환 목표 달성을 위해 국가 로드맵 수립 방법에 대한 구체적인 가이드라인을 발표

- 가이드라인 세부 내용[20]으로는 디지털 전환 관련 현황 분석, 국가별 목표 설정, 디지털 전환 목표 달성을 위한 정부 정책 및 세부 조치방안 수립 등이 포함
- EU 회원국은 2023년 10월까지 "2030 Digital Decade" 목표 이행을 위한 국가 로드맵을 수립 및 제출해야 하며, 추후 발표 예정인 평가보고서를 바탕으로 5개월 이내에 기존 로드맵에 대한 수정 및 보완을 시행해야 함

---

19) EU(2023.6.30.), 2030 Digital Decade: Commission adopts indicators to monitor Europe's digital transformation and issues guidance to Member States

20) EU(2023.6.28.), Guidance to Member States on the preparation of the national Digital Decade Strategic roadmaps

〈 EU 디지털 전환을 위한 주요 핵심 성과 지표(KPI) 〉

구분	주요 지표 설명
기본 디지털 역량 (Basic digital skills)	• 5가지 영역(정보, 의사소통, 문제해결, 디지털 콘텐츠 제작, 보안)에서 "기본(basic)"* 이상의 디지털 기술을 보유한 시민의 비율 (16세~74세 사이 전체 시민 대비 백분율) * 정보, 의사소통, 디지털 콘텐츠 제작 등 지난 3개월간 사용자가 수행한 디지털 활동을 기반으로 측정
ICT 전문가 (ICT specialists)	• ICT 시스템 개발, 운영, 유지보수 등 정보통신 전문가로 고용된 사람의 수 및 남녀 성비 융합의 정도 (15세~74세 사이)
기가비트 연결성 (Gigabit connectivity)	• 기가비트급 인터넷 연결이 가능한 가구의 비율
5G 커버리지 (5G coverage)	• 5G 네트워크 연결이 가능한 인구 밀집 지역의 비율
반도체 (Semiconductors)	• EU 내 반도체 밸류체인(Value Chain)의 모든 단계에서 생성된 부가가치
엣지노드 (Edge nodes)	• 20ms* 미만의 레이턴시**를 제공하는 컴퓨팅 노드의 수 * millisecond, 0.001초 ** 하나의 데이터패킷이 한 지점에서 다른 지점으로 이동하는 데 소요되는 시간
양자컴퓨팅 (Quantum Computing)	• 현재 운영 중인 양자 컴퓨터, 양자 시뮬레이터의 수
클라우드 컴퓨팅 (Cloud Computing)	• ERP*, CRM**, 보안 분야 중 하나 이상의 클라우드 컴퓨팅 서비스를 사용하는 기업의 비율 * Enterprise Resource Planning, 재고, 회계, 인사 등 기업의 다양한 업무를 통합하여 관리하는 시스템 ** Customer Relationship Management, 고객 및 잠재고객과 관련된 정보를 추적, 저장, 관리하는 시스템
빅데이터 (Big data)	• 내부 또는 외부의 모든 데이터 소스를 분석하는 기업의 비율
인공지능 (Artificial Intelligence)	• 적어도 1개 이상의 인공지능 기술을 사용하는 기업의 비율
디지털 중소기업 (SMEs)	• 최소 기본 수준의 디지털 집약도를 보유한 중소기업의 비율

구분	주요 지표 설명
유니콘 (Unicorns)	• 유니콘 기업의 수* * 기업가치가 10억 달러(약 1조 원) 이상이고 창업한 지 10년 이하인 비상장 스타트업
시민을 위한 공공서비스 (Key public services for citizens)	• 시민을 위한 주요 공공서비스의 온라인 제공 비율
기업을 위한 공공서비스 (Key public services for businesses)	• 창업, 기업 활동을 위한 공공서비스의 온라인 제공 비율
전자 건강 기록 (E-health records)	• 시민들의 건강, 질병 기록에 대한 온라인 서비스 제공 여부 및 해당 서비스에 접근가능한 시민의 비율
디지털 신분증 (eID)	• EU 규정에 따라 적어도 1개 이상의 국가 디지털 신분증(eID) 제도를 통지한 회원국 수 • EU 규정에 따라 EU Digital Identity Wallet*을 통해 개인 정보보안 강화 eID 서비스를 제공한 회원국 수 * 운전면허증, 의료보험카드 외 각종 공문서까지 저장이 가능한 스마트폰 어플리케이션 형태의 EU 디지털 신분증으로 EU 회원국 내에서 활용이 가능하며, '23년 4월부터 시범 운영이 개시되었음

NEWS 6 캐나다 공무원 11%, 업무 용도 AI 활용 경험 보유[21]

❍ 글로벌정부포럼(GGF)*이 캐나다 공무원 1,320명을 대상으로 한 조사에 따르면, 약 10% 이상이 대량의 데이터 처리, 실시간 분석 및 공공 서비스 모니터링 등에 AI를 활용

* Global Government Forum. 전 세계 국가 공공 분야의 최근 소식을 공유하고 연수 프로그램, 네트워킹, 웨비나 및 포럼 등을 제공하는 기관

- (사용 경험) 업무 목적으로 ChatGPT 및 Bard 등의 AI 도구를 사용해 본 적이 있느냐는 질문에 캐나다 공무원 11%(자주 3%, 가끔 8%)가 경험이 있다고 응답
- (기대 분야) 대량의 데이터 처리, 교통 흐름 분석, 의료 서비스 개선 등 공공 서비스 제공에 대한 실시간 분석 및 모니터링에 AI를 활용하는 것에 긍정적인 평가

❍ 공공 서비스에서의 AI 활용 시, 비합리적 의사결정 및 사용 방법 미숙 등에 대해 우려

- 절반에 가까운 공무원(48%)이 정부에서 'AI 기반 결정과 조치에 대한 책임과 의무'에 대해 매우 우려한다고 응답
- 공무원의 40% 이상은 AI에 대한 과도한 의존으로 인해 공공 서비스의 자율성과 의사결정 능력이 약화될 가능성(44%)과 공무원의 AI에 대한 이해와 친숙도 부족으로 인해 AI 활용이 저해될 가능성(41%)에 대해서도 우려를 표시

※ 최근 글로벌정부포럼(GGF)이 개최한 공공 서비스 AI 활용과 관련된 웨비나*에서 데이터 분석 시스템의 결과가 어떻게 생성되었는지에 대한 근거가 명확하지 않은 경우, 일선 직원들은 데이터 분석 시스템의 결과를 신뢰하지 않을 것이라는 우려가 제기

* 화상 토론회. 컴퓨터와 모바일 기기를 통해 장소에 구애받지 않고 언제, 어디서든지 개최해 참가할 수 있는 양방향 온라인 세미나. 웹(web)과 세미나(seminar)의 합성어로 주로 웨비나라고 부름

❍ 한편, GGF는 향후 수 주 내에 이번 설문조사 결과에 대한 전체 보고서를 발표할 예정

---

21) Global Government Forum(2023.7.5), One in ten Canadian public servants already using AI for work purposes

NEWS 7 맥킨지, 미국 정부 서비스 고객 경험 현황 및 개선방안 발표[22)]

❍ 맥킨지 앤 컴퍼니(Mckinsey&Company)*는 최근 자체 설문조사 결과를 바탕으로 미국 정부 서비스 관련 고객 경험 현황과 향후 개선방안을 발표

* 1926년 제임스 맥킨지에 의해 설립된 이후 현재 약 130개국에서 전략컨설팅 서비스 등을 제공하고 있는 글로벌 컨설팅 회사

- 맥킨지는 2023년 2월과 3월에 약 30,000명의 시민을 대상으로 실시한 설문조사를 통해 40개 이상의 영향력이 큰 공공서비스 제공 기관(High-impact Service Providers, HISPs)*과 5개의 주요 생애주기별 공공서비스**에 대한 고객 경험을 평가하였음

* 시민이 가장 많이 활용하거나, 시민의 일상생활에 있어 중요한 공공서비스를 제공하는 연방기관을 의미하며, 미국 대통령실 소속기관인 예산관리처가 지정함

** 2021년 미국 행정명령에 의해 우선순위가 지정된 주요 생애주기 별 공공서비스는 ▲은퇴 ▲재해 복구 ▲군 복무 후 민간인 생활로의 전환 ▲자녀의 출산 및 유아기 지원 ▲재정적 어려움 직면과 같이 총 5개임

- 이번 설문조사는 사용자의 서비스 접근 편의성, 소요 시간, 공공서비스의 신뢰성 등을 중점에 두고 실시되었으며, 이후 고급 통계 모델링을 통해 분석 결과를 도출하였음

❍ **(고객 경험 현황)** 현재 대부분의 정부 공공서비스는 사용자 만족도 측면에서 민간 부문 서비스에 비해 크게 뒤떨어져 있음

- 사용자들은 불명확한 의사소통 과정, 정보탐색의 어려움이 공공서비스 만족도 저하의 가장 큰 원인이라고 밝힘
- 또한, 사용자들이 서비스 및 혜택을 받기까지 한 달 이상의 긴 시간이 소요되는 경우 해당 공공서비스에 대한 만족도가 급격히 감소하는 것으로 분석되었음
- 최근 민간 부문 서비스의 혁신과 높은 편의성으로 인해 사용자의 눈높이는 더 높아져 있어, 향후 사용자의 기대를 충족시키기 위해서는 지속적인 서비스 개선이 필요할 것으로 전망

22) McKinsey&Company(2023.6.9.), How US government leaders can deliver a better customer experience

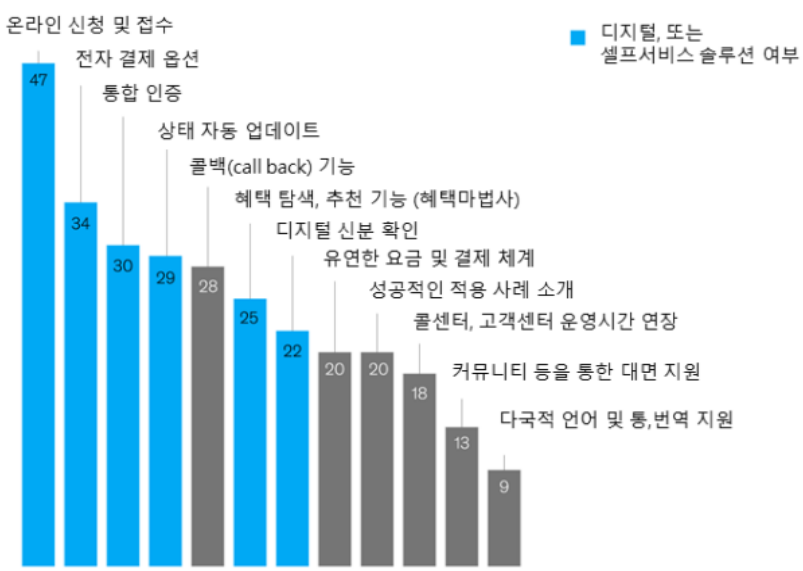
❍ **(고객 경험 개선방안)** 사용자의 공공서비스 만족도 향상을 위해서는 서비스 과정 간소화 등을 통한 사용자 부담 경감 및 디지털 셀프서비스 솔루션* 도입 확대가 필요하다고 주장

* 직원의 도움 없이 고객 스스로가 문제를 해결할 수 있도록 관련 온라인 서비스를 지원

- 서비스 이용을 위한 불필요한 정보탐색, 업무 완료까지 장시간 소요, 중복되는 양식 등은 사용자 만족도 저하뿐만 아니라 정부 서비스 신뢰 하락에도 영향을 끼치므로 서비스 과정 간소화, 명확하고 이해하기 쉬운 언어 사용 등이 필요하다고 강조
- 또한, 사용자들은 빠르고 편리하게 업무를 할 수 있는 디지털 셀프서비스 솔루션을 선호* 하는 경향이 있으므로, 콜센터 운영 확대, 신규 직원 채용 등 오프라인 채널에 대한 투자보다 디지털 솔루션 확대가 고객 만족도 향상에 효율적인 방법이라고 주장

* 시민들은 해당 설문조사에서 연방 정부 서비스의 고객 경험 향상과 관련하여 가장 선호하는 솔루션으로 ①온라인 신청 및 접수(Online applications) ②전자결제 옵션(Electronic-payment options) ③통합인증(Single sign-on) ④상태 자동 업데이트(Automated status updates) ⑤ 디지털 신분 확인(Digital ID verification) 등을 선택

〈 연방 정부 공공서비스 고객 경험 향상을 위한 솔루션 설문조사 결과(%)[23] 〉



※ 29,989명을 대상으로 한 설문조사 결과이며, 각 막대의 수치는 고객 경험 향상을 위해 가장 중요하다고 생각하는 3개의 솔루션 중 해당 솔루션을 포함한 설문 응답자의 비율임

예) 29,989명 중 47%는 "온라인 신청 및 접수"를 고객 경험 향상을 위해 가장 필요한 3개 솔루션 중 하나로 선택

23) 원출처: McKinsey&Company(2023.6.9.), How US government leaders can deliver a better customer experience