J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

미국 정부 TIC 3.0을 적용한 국내 공공·행정기관의 안전한 클라우드 연합 모델 연구☆

A Study on the Secure Cloud Federation Model of Korean Public and Administrative Institutions based on U.S. TIC 3.0

이 수 현[1*] 임 하 늘[1] 배 병 철[2] 강 은 성[3] 김 형 종[3†]
Soo-hyun Lee Ha-neul Lim Byung-chul Bae Eunseong Kang Hyung-Jong Kim

요 약

최근 코로나19로 인해 분야 간의 경계가 무너지면서 모든 데이터를 연결하고 국민, 기업, 정부 모두가 데이터에 접근 가능하도록 하는 정부의 목표가 주목받고 있다. 이러한 목표에는 클라우드 기술이 계속해서 언급되어 오고 있으며 클라우드 사용으로 인한 보안 이슈를 피해갈 수 없어, 이와 관련된 다양한 연구가 진행되고 있다. 본 논문에서는 국내 공공·행정기관에서의 클라우드 사용 사례를 분석하고, 이때 발생할 수 있는 보안 이슈를 완화하기 위해 미국 정부 TIC 3.0 개념을 적용한 모델을 제시하고자 한다. 그리고 이를 토대로 TIC 3.0을 적용한 국내 공공·행정기관의 안전한 클라우드 서비스 모델을 제안하고자 한다.

☞ 주제어 : 클라우드, 클라우드 연합 참조 아키텍처, TIC 3.0, 공공·행정기관

ABSTRACT

Recently, due to the collapse of boundaries between fields caused by COVID-19, the government's goal of connecting all data and making it accessible to people, businesses, and governments has garnered attention. To achieve this goal, cloud technology is consistently mentioned, and since the use of cloud technology inevitably raises security concerns, various studies are being conducted on the topic. This paper analyzes the use of cloud technology in public and administrative institutions in Korea and presents a model that applies the U.S. government's TIC 3.0 concept to mitigate potential security issues. The objective is to provide a secure cloud service utilization model for public and administrative institutions, with reference to TIC 3.0.

☞ keyword : Cloud, CFRA(Cloud Federation Reference Architecture), TIC 3.0, public·administrative institutions

1. 서 론

최근 코로나19로 인해 분야 간의 경계가 허물어지고 예측하기 어려운 위협이 동시다발적으로 발생하면서 클라우드 기술 및 보안이 주목받고 있다. 클라우드는 인터넷 기반 컴퓨팅의 일종으로 인터넷만 연결되어 있다면 언제 어디서든 저장한 데이터를 가져올 수 있다는 장점이 있다. 그러나 디지털 전환이 가속화되면서 사이버 위협이 전 영역으로 확대되고 지능화되어 피해가 급증하고 있으며 이는 클라우드에서 또한 예외는 아니다.

최근 가트너는 클라우드 보안에 대한 재평가를 통해 "고객의 실수로 인한 클라우드 보안 장애가 99%에 달할 것이다."라고 경고한 바 있으며[1], 이를 통해 클라우드 기술의 사용은 점점 증가하고 그에 따라 발생 가능한 보안 이슈도 무시할 수 없음을 예상해 볼 수 있다.

현 정부는 모든 데이터를 연결하고 이를 통해 새로운 가치를 창출하는 것을 목적으로 하는 정책을 논의 한 바 있다. 해당 목적을 위해서는 클라우드 기술 사용이 필요하며 안전하고 신뢰할 수 있는 환경이 보장되어야 한다. 이러한 이유로 우리나라 공공·행정기관은 클라우드 환경에서 서로의 데이터에 직접 접근 가능한 연합 모델이 필요하다. 그러나 공공·행정기관에서의 클라우드 활용과 서로의 접근은 이전보다 보안에 더 많은 신경을 필요로

1 Student, Seoul Women's University, Seoul, 01797, South Korea
2 Principal Researcher, The Affiliated Institute of ETRI, Daejeon, 34129, South Korea
3 Professor, Seoul Women's University, Seoul, 01797, South Korea
* Lead author (altnfsudwo@naver.com)
† Corresponding author (hkim@swu.ac.kr)
[Received 25 September 2023, Reviewed 11 October 2023(R2 23 October 2023), Accepted 25 October 2023]
☆ 이 논문은 ETRI부설연구소의 위탁연구과제[2023-022]로 수행한 연구결과입니다.

한다.

신뢰할 수 있는 안전한 클라우드 환경을 위해서는 보안의 신패러다임인 제로트러스트(Zero Trust)[2], [3]와 TIC(Trust Internet Connection) 3.0 개념 적용이 필요하다. 제로트러스트는 외부에 중점을 두는 기존의 경계 기반 보안에서 발전한 것으로 외부, 내부에 대한 모든 신뢰를 0(Zero)에 두고 최소한의 권한만 부여하며 지속적으로 검증하는 보안 개념이다. NIST에서는 이러한 제로트러스트에 접근할 수 있는 3가지 방법론을[4] CISA에서는 제로트러스트 5대 핵심 기술에 대한 3단계 성숙도 모델을 제시한다[5]. TIC 3.0은 제로트러스트와 함께 언급되는 개념으로 이전의 TIC 2.2 개념을 확장한 것이다. 과거 한 곳에서 정책을 시행했던 것과는 다르게 TIC 3.0은 각 엔티티 사이의 인터넷 연결에서 범용 보안 기능과 PEP(Policy Enforcement Point) 보안 기능을 적절하게 분산 배치하여 경계를 허물고 인터넷 전체에 신뢰할 수 있는 연결을 형성한다.

사례연구로서 2022년까지 코로나19 입원, 격리자 생활지원비 지원을 받기 위해서는 개인이 지원비 신청을 하기 전 국민건강보험 홈페이지 또는 앱을 이용해 직접 본인의 건강보험 본인부담금 이력을 확인해야 했다. 그러나 코로나19 입원, 격리자 생활지원비 지원 결정 여부는 환자·보호자의 신청만으로 끝나는 것이 아니다. 정부는 코로나 생활지원비 지원을 신청한 환자·보호자의 건강보험 본인부담금이 <건강보험료 산정기준>을 만족하는지 국민건강보험공단에 환자·보호자의 건강보험 본인부담금 데이터를 직접 요청한 후 확인해야 한다. 이러한 반복적이고 제한적인 데이터 접근 때문에 코로나19 입원, 격리자 생활지원비 지원 소요기간은 평균 59.7일이라는 긴 시간이 소요된다.

본 논문에서는 클라우드 연합을 구성한 국내 공공·행정기관 간 모델을 제안하고 TIC 3.0을 적용함으로써 보안성과 국민의 편의성을 개선하는 아키텍처를 구성하였다. 1장 서론에 이어, 2장에서 클라우드 기술 기반으로 클라우드 연합 참조 아키텍처와 클라우드 연합 참조 아키텍처 배포 모델 중 하나인 내부 P2P를 설명하고 3장에서는 TIC 3.0을 적용한 공공·행정기관 간의 클라우드 연합 모델 동작 과정에 대해서 다룬다. 마지막, 4장 결론에서는 향후 연구 진행 방향을 설명하고 있다.

2. 클라우드 기술 관련 연구

본 장에서는 클라우드 연합 참조 아키텍처(CFRA), TIC 3.0 아키텍처의 개념을 다루고 이를 활용한 국내외 사례를 살펴봄으로써, 국내 공공·행정기관 간의 통신에서 클라우드 기술 적용 시 어떤 특징을 가지는지 살펴보고자 한다. TIC 3.0을 기반으로 하는 국내 공공·행정기관 클라우드 연합 모델의 경우, 기관 간의 자율적 연합이 가능하고 구현이 단순한 내부 P2P 방식을 채택한다. 이러한 모델은 클라우드 연합 및 TIC 3.0 개념 사용이 필요하기 때문에 우리나라보다 앞서 연구가 진행된 미국의 클라우드 기술 관련 문서들을 중심적으로 살펴본다.

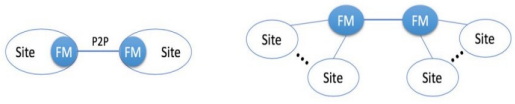
2.1 클라우드 연합 참조 아키텍처(CFRA)

2.1.1 NIST.SP.500-332

본 문서에서는 클라우드 연합에 대해 “둘 이상의 클라우드 공급자(CSP)가 상호작용하여 협력하는 것을 의미한다”고 언급한 바 있다[6]. 이는 공공·행정기관과 민간 기업 간의 연합일 수 있고 공공·행정기관 간 혹은 민간 기업 간의 연합일 수 있다.

클라우드 연합의 핵심은 연합 인증 및 권한 부여로 IdP(Identity Provider), SP(Servide Provider), User 간의 통신이 중요하다. 결과적으로 클라우드 연합은 분산 환경 전반에서 인증 및 권한 부여 관리를 할 수 있으며 때문에, 데이터, 플랫폼 그리고 인프라 연합을 제공하기 위한 리소스의 안전한 공유가 가능하게 된다.

클라우드 연합 배포의 모델 종류로는 (외부·내부) 중앙 집중식 FM(Federation Manager) 배포, Pair-wise 배포, 계층적 FM 배포, P2P FM 배포 등이 있으며 이때 P2P FM 배포의 경우 구현이 가장 간단하며 연합을 맺는 기관의 자율도가 높다는 장점이 있다.



(그림 1) Pair-wise, P2P FM 배포
(Figure 1) Pair-wise, P2P FM distribution

이와 관련된 해외 사례로는 The Conflated Dataset Workflow가 있으며 해당 사례는 내부의 Pair-wise P2P FM 배포가 어떻게 작동하는지를 보여준다[6]. 조직 A와 B는

IdP, Site Admin, User 3가지 요소와 FM 간의 통신으로 연합 인증 및 권한 부여를 수행하며 서비스 연합을 구성한다. 이때, 구성된 연합은 특정 조직에서의 변경된 사항이 다른 조직에도 반영되는 P2P FM 배포 모델의 특징을 가진다. 연합 이후, 조직 B의 서비스를 조직 A의 소속인 User A가 이용하고자 하는 경우, 해당 연합의 구성원임이 인증되면 조직 B의 데이터 및 서비스에 접근하는 것이 가능해진다.

결국, 이러한 클라우드 연합 참조 아키텍처의 목적은 클라우드를 사용하는 각 기관이 서로의 데이터에 접근하여 반복적인 작업을 줄이는 데 있다.

2.2 TIC 3.0 참조 아키텍처

2.2.1 CISA TIC 3.0 Reference Architecture

최근 코로나19로 인해 원격, 비대면 서비스가 증가하고, 클라우드 서비스 활용의 보편화로 내부, 외부의 경계 구분이 어려워지고 이용자와 단말을 신뢰할 수 없는 환경이 되었다. 내부자의 권한을 탈취하는 등 내부 네트워크 사용자를 암묵적으로 신뢰하여 발생하는 공격 사례가 증가하고 있다. 이에 제로트러스트와 TIC 3.0이라는 새로운 보안 패러다임이 주목받고 있다.

해당 문서에서는 TIC 3.0 참조 아키텍처를 다루며 신뢰영역 및 수준, 보안기능 등과 같은 핵심 구성 요소를 설명하며 이후 사용 사례에 따른 보안 패턴과 사례마다 사용이 권장되는 보안 기능 등을 다룬다.

이러한 TIC 3.0의 목적은 각 엔티티의 신뢰 영역을 설정하고 신뢰 영역 사이 또는 내부에 PEP를 배치함으로써 기관의 다중 경계환경을 보호하고 인터넷 전체에 신뢰할 수 있는 연결을 형성하는 것에 있다.

3. 국내 공공·행정기관 클라우드 활용 사례와 TIC 3.0의 적용

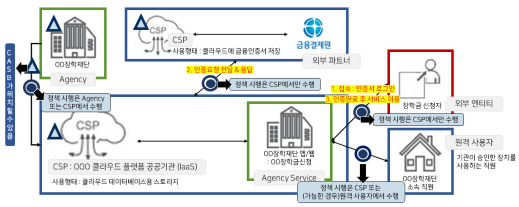
모든 사례의 신뢰 영역 및 수준, 가정과 제약 조건, PEP 배치와 정책 시행 엔티티는 TIC 3.0 Cloud Use Case를 참고하였다[7].

3.1 활용 사례1 - OO재단

OO재단은 국가 장학 기금을 효율적으로 운영하여 맞춤형 학자금 지원 체제를 구축함으로써 경제적 여건에 관계없이 누구나 의지와 능력에 따라 고등교육 기회를 가질 수 있도록 지원하는 교육부 산하 위탁집행형 준정부기관이다.

장학금 신청자들은 장학금신청을 위해 매년 OO재단의 웹과 앱을 이용하며 서비스 이용을 위해 로그인을 필수적으로 수행한다. 본 내용에서는 로그인하는 여러 방법 중 금융인증서를 이용하는 경우를 다루며 이때, OO재단에서는 인증서 클라우드 서비스를 이용한다. 인증서 클라우드 서비스란, 이용자가 보유한 인증서를 금융결제원이 관리하는 클라우드 서버에 보관하여 언제 어디서나 클라우드 연결을 통해 인증서를 이용하는 서비스를 말한다. 또한 OO재단은 데이터베이스용 스토리지 네이버클라우드 플랫폼 공공기관용(IaaS)를 이용하고 있다.

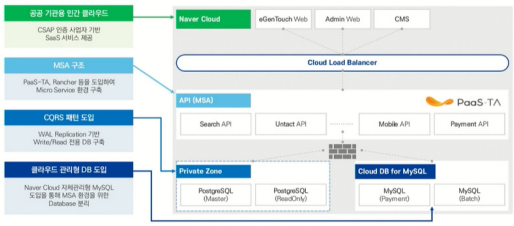
결론적으로 OO재단은 클라우드를 이용해 서비스를 운영하고 있으며 금융결제원이라는 외부 파트너와 상호작용하는 운영 흐름을 가지고 있다. 이러한 한국장학재단의 서비스 흐름에 MGMT (Management Entities)와 PEP를 배치하여 인터넷 전체에 신뢰할 수 있는 연결을 형성하고자 한다[8].



(그림 2) TIC 3.0을 적용한 OO재단
(Figure 2) TIC3.0 based OO Organization

3.2 활용 사례2 - OO시 도서관

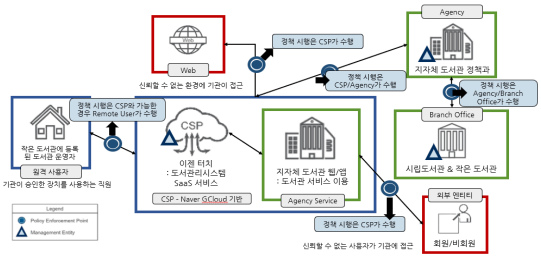
이 사례의 경우, 실제 국내에서 클라우드 서비스를 사용하고 있는 기관을 확인할 수 있는 '행정·공공기관 민간 클라우드(SaaS) 이용사례집'을 참고하였다[9], [10]. OO시 도서관은 네이버 클라우드를 사용하고 CSAP(Cloud Security Assurance Program) 인증 사업자 기반으로 SaaS 서비스를 제공한다.



(그림 3) OO시 도서관의 SaaS 클라우드 사용 예
(Figure 3) The SaaS based OO Library Case

현재 OO시 도서관의 서비스 흐름은 도서관 관리부서, CSP를 이용하는 도서관 관리 서비스 즉, OO시 도서관 앱·웹 그리고 이에 접근하는 원격 사용자 혹은 외부 엔티티로 구성되어 있다.

결론적으로 OO시 도서관은 SaaS 서비스를 제공받아 도서관 관리 서비스를 운영하는 흐름을 가지고 있다. 이러한 OO시 도서관 서비스 흐름에 MGMT와 PEP를 분산되게 배치함으로써 TIC 3.0을 만족시키고 해당 연결에 속해 있는 환경 전체에 신뢰를 형성하고자 한다[8].



(그림 4) TIC 3.0을 적용한 OO시 도서관
(Figure 4) TIC 3.0 based OO Library

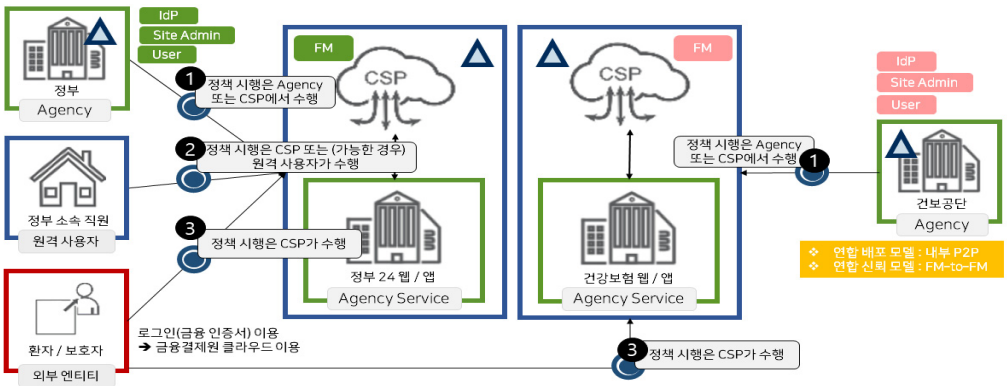
4. TIC 3.0 기반 공공·행정기관의 안전한 클라우드 서비스 활용 모델

코로나19로 인해 모든 공공·행정기관에 이와 관련된 업무 및 서비스가 증가하고 있다. 백신 접종 예약 시스템의 경우, 클라우드가 활용되면서 초기 긴 대기 시간과 시스템 사용 시 발생하는 오류가 줄어들었고 시간당 최대 처리 수준은 약 2백만 명까지로 높아지는 결과를 가져왔다.

본 장에서는 이러한 긍정적인 효과를 기대하며 정부24와 국민건강보험공단 간의 협력이 필요한 코로나19 생활비 지원비 지원 서비스에 클라우드 연합 아키텍처와 TIC 3.0을 적용한 모델을 새롭게 제안한다.

4.1 공공·행정기관 간의 클라우드 연합 모델

다음 제안모델은 재난지원금 지급 소요기간을 줄이는데 효과적일 수 있는 가상 시나리오이며 TIC 3.0 만족을 위한 PEP와 MGMT 배치를 포함하는 정부와 건강보험공단 간의 (Pair-wise) 내부 P2P 연합이다. [그림 5]는 제안모델의 각 엔티티가 가지는 신뢰 영역과 배치 가능한 PEP, MGMT를 나타낸 것이다. 해당 가상 시나리오는, TIC 3.0 사용 사례를 전체적으로 참고한 것이며 그중 Cloud 사용 사례의 보안 패턴, 신뢰 수준, 가정 및 제약을 따른다[7], [8], [11], [12].



(그림 5) TIC 3.0을 적용한 국내 공공·행정기관의 안전한 클라우드 연합 모델
(Figure 5) TIC 3.0 based Korean Public Organization's Secure Cloud Federation Model

(표 1) 그림 5에서 사용해야 할 PEP 보안 기능
(Table 1) The PEP Capabilities for Fig. 5's model

	PEP Security Capability
①	파일, 네트워킹, 엔터프라이즈, 데이터 보호, 복원력, DNS, 침입탐지
②	파일, 이메일, 엔터프라이즈, 데이터 보호, 복원력, DNS, 침입탐지, 신원, UCC(Unified Communications and Collaboration)
③	파일, 엔터프라이즈, 데이터 보호, 복원력, DNS, 침입탐지, 신원, 서비스

4.2 제안모델의 동작 방법

해당 시나리오의 경우, 총 11단계로 이루어져 있으며 코로나19 입원, 격리자 생활지원비 지원을 위한 정부와 건강보험공단 간의 연합 과정을 보여주고자 한다. 연합이 형성되기 전 각 조직이 독립적으로 서비스하는 모습을 시작으로 연합 형성 후 서로 통신 하는 모습까지를 다룬다. 그리고 해당 모델의 장점과 단점을 표로 정리한다.

Step 1. 연합 형성 전의 조직 A(국민건강보험공단)와 B(정부24)

연합을 형성하기 전 각 조직의 독립적인 모습으로 클라우드 기술을 사용 중인 조직 A와 B이다.

Step 2. COVID-19 대응 서비스를 인스턴스화 하는 조직 A

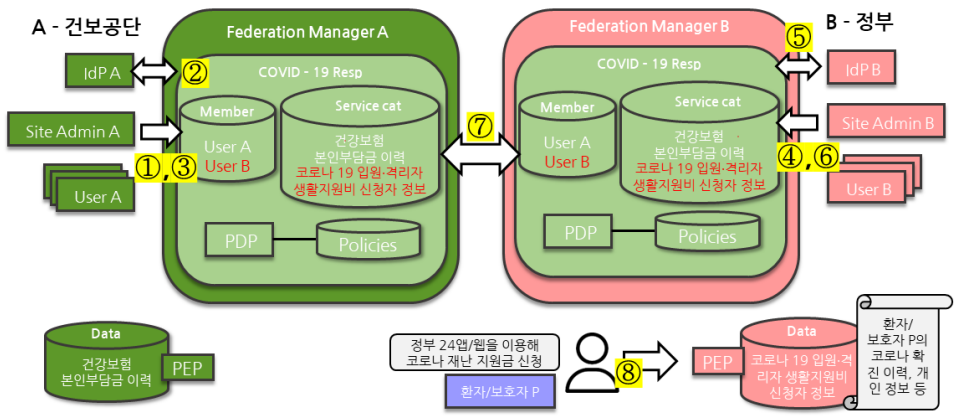
국민건강보험공단의 Site Admin A는 연합하고자 하는 COVID-19 대응 서비스를 FM A에 인스턴스화 한다. 이때 해당 서비스의 멤버, 서비스 카탈로그와 정책 서버는 비어 있는 상태이다.

Step 3. Member, 서비스 카탈로그, 정책 서버를 채우는 Site Admin A

Site Admin A가 비워져 있던 서비스 카탈로그와 정책을 채우기 시작한다. (1단계) Site Admin A는 국민건강보험공단 소속 직원인 User A에게 COVID-19 대응 서비스 멤버십을 부여한다. (2단계) IdP A는 User A에 대한 자격 증명을 발급한다. 이후, User A는 Member로 채워지게 된다. (3단계) Site Admin A는 국민건강보험공단의 건강보험 본인부담금 이력 데이터를 서비스 카탈로그에 채워 넣는다. 데이터, Member와 관련된 정책 또한 정책 서버에 추가한다.

Step 4. COVID-19 대응 서비스에 가입을 성공한 조직 B

정부에서 국민건강보험공단의 COVID-19 대응 서비스에 가입하려고 하는 경우이다. [그림 6]에서 정부 소속의 Site Admin B는 FM B에게 국민건강보험공단의 COVID-19 대응 서비스에 가입하길 권한다. FM B는 Site Admin B의 요청을 FM A에게 전달하고 Site Admin A는 신뢰관계를 바탕으로 가입 여부를 결정한다. 현재 시나리오에서는 가



(그림 10) Step 1에서 Step 7까지의 과정
(Figure 10) The illustration from Step 1 to Step 7

입이 수락된 형태이므로 정부는 국민건강보험공단 COVID-19 대응 서비스 현재 상태 그대로의 복사본을 받게 된다.

Step 5. COVID-19 대응 서비스를 채워 넣는 조직 B

COVID-19 대응 서비스에 정부가 사용자와 서비스를 추가하는 경우이다. [그림 6]에서 (4단계) Site Admin B는 정부 소속 직원인 User B에게 COVID-19 대응 서비스에 대한 멤버십을 부여한다. (5단계) IdP B는 User B에게 서비스 이용을 위한 자격 증명을 발급한다. (6단계) 이후 User B는 Member로 등록되며 Site Admin B는 코로나 재난지원금 신청자 정보 데이터를 서비스 카탈로그에 채워 넣는다. 데이터, Member와 관련된 정책 또한 정책 서버에 추가한다.

Step 6. 일관성을 달성한 FM A와 FM B

(7단계) P2P 배포 모델의 특징을 보여준다. 해당 시나리오의 경우, 내부 P2P 연합 배포 모델이기 때문에, FM A와 FM B는 COVID-19 대응 서비스에 대한 일관성을 유지해야 한다. 결국 국민건강보험공단과 정부는 COVID-19 대응 서비스에 대한 동일한 Member, 서비스 카탈로그, 정책 서버를 가진다.

Step 7. 코로나 재난지원금을 신청한 환자·보호자 P

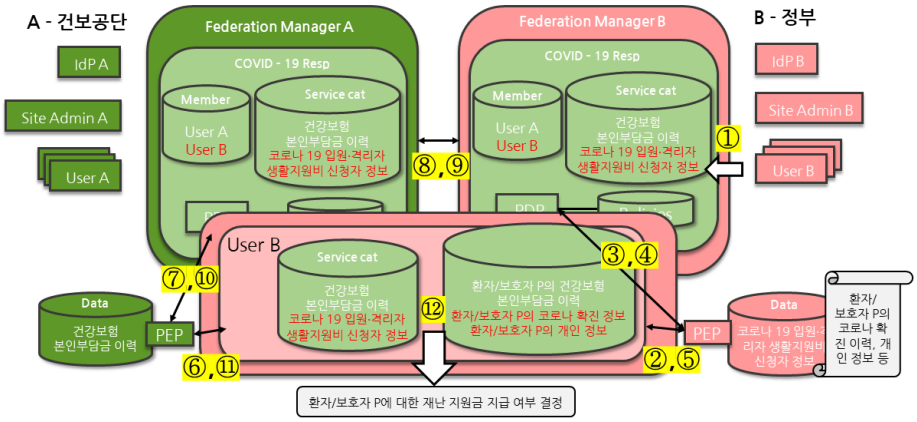
국민건강보험공단과 정부 간의 연합 형성이 완성된 후, 환자·보호자 P가 정부24 앱이나 웹을 통해 코로나 재난지원금 신청을 한 경우이다. (8단계) 신청이 들어오면 신청자의 코로나 확진 이력, 개인 정보가 정부의 코로나 재난지원금 신청자 정보에 올라온다.

Step 8. 환자·보호자 P에 대한 재난지원금 지급 여부 결정을 위한 조직 B 소속 User B의 접근

환자·보호자 P의 신청을 확인하고 재난지원금 지급 여부를 결정하기 위한 정부 직원 User B의 접근을 보여준다. (1단계) User B는 COVID-19 대응 서비스에 접근하기 위해 인증을 시도한다. User B는 Member에 소속되어 있는 사용자이므로 접근 가능한 서비스 카탈로그 일부를 반환받는다. (현재 시나리오에서는 모든 서비스 카탈로그에 접근 가능하다.)

Step 9. 환자·보호자 P의 코로나19 관련 정보 접근

User B가 코로나 재난지원금 신청자 정보 서비스에 먼저 접근하는 경우이다. (2단계) User B는 서비스 카탈로그를 이용해 코로나 재난지원금 신청자 정보 데이터에 접근 요청을 보낸다. 이 요청은 PEP가 받게 되고 (3단계) PEP는 다시 PDP(Policy Decision Point)에게 요청을 전달한다. (4단계) PDP는 정책 서버에서 해당 요청에 대한 정책을 찾고 결정한 정책을 다시 PEP에게 반환한다. PEP는 PDP가 결정한 정책을 시행하여 데이터 접근에 가능한지 아닌지 판단하여 (5단계) 결과를 User B에게 전달한다. 데이터로



(그림 11) Step 8에서 Step 12까지의 과정
(Figure 11) The illustration from Step 8 to Step 12

의 접근이 허용되었으므로 User B는 환자·보호자 P의 코로나 확진 이력, 개인 정보 등을 알 수 있다.

Step 10, 11. 조직 A 서비스로 접근하는 User B

그러나 환자·보호자 P의 코로나 확진 정보와 개인 정보만으로는 재난지원금을 받을 수 있는 사람인지 판단하기 어렵다. [그림 7]은 판단에 필요한 건강보험 본인부담금을 확인하기 위해 User B가 국민건강보험공단의 서비스에 접근하는 과정이다. (6단계) User B는 서비스 카탈로그를 사용해 조직 A의 서비스에 접근 요청을 보낸다. 이는 PEP가 받게 되고 (7단계) PEP는 다시 PDP에게 해당 연결에 대한 요청을 보낸다. FM A는 이 요청과 연결된 자격 증명이 신뢰할 수 있는 피어인 FM B에 의해 발급되었음을 확인한다. (8, 9단계) FM A는 FM B에게 유효성 검사 및 권한 부여 결정을 내리도록 요청하고 반환받는다. (10, 11단계) 해당 요청이 승인되면 User B는 국민건강보험공단의 데이터에도 접근이 가능해진다.

Step 12. 코로나19 재난지원금 지급 여부를 결정하는 User B

(12단계) User B는 환자·보호자 P의 건강보험 본인부담금 이력과 코로나 확진 정보, 개인 정보를 모두 확인 가능하므로 재난지원금 지급 여부를 결정할 수 있게 된다.

(표 2) 시나리오의 장점 및 단점
(Table 2) Pros and Cons of the Scenario

	설 명
장점	· **자율성:** 기관 간의 자율적 연합을 구성할 수 있고 쉽게 구현 가능. · **유연성:** 현재 코로나19 입원 및 격리자 생활지원비 지원에 국한되어 있지만, 이후 추가적인 서비스로 사용할 경우 긍정적인 효과를 기대 가능. · **보안성:** 모든 접근 데이터가 남기 때문에 이를 로그로 활용하여 보안 모니터링에 활용 가능.
단점	· **불필요한 데이터 축적:** 현시점에서 국민건강보험 공단이 정부와 협력하여 얻는 이득이 없음. · **무조건적 일관성 유지:** P2P 방식을 사용함에 따라 코로나19 대응 서비스가 항상 일관성을 유지해야 함. 이때, 국민건강보험 공단에서 정부 직원의 접근 이력이나 권한을 확인할 가능성이 발생

5. 결 론

국내의 공공·행정기관은 국민에게 빠르고 신뢰할 수 있는 서비스를 제공해야 할 의무가 있다. 이러한 서비스를 위해서는 클라우드 기술 사용이 필수적이다. 그러나 공공·행정기관에서 클라우드를 사용하는 것은 악의적인 의도를 가진 사용자에게 매우 좋은 먹잇감일 수 있다. 이 때문에 외부, 내부 할 것 없이 모든 영역에서 보안 이슈가 발생할 수 있음을 고려해야 한다.

이를 위하여 본 논문에서는 미국의 클라우드 연합 참조 아키텍처 및 TIC 3.0 개념을 정리하였다. 또한, 국내 공공·행정기관 사례에 TIC 3.0 개념을 적용하여 새롭게 제시하였으며 이러한 분석을 바탕으로 TIC 3.0을 기반으로 하는 국내 공공·행정기관 간의 안전한 클라우드 연합 서비스 활용 모델을 제안해 보안 측면 향상에 도움이 되고자 하였다.

향후에는 공공·행정기관이 특정 CSP를 채택한다는 가정하에 해당 CSP의 어떤 서비스를 이용해야 하는지, 그리고 제로트러스트 개념을 추가 적용하여 TIC 3.0과 어떤 식으로 조화를 이룰 수 있는지에 대한 방법을 연구하고자 한다.

참고문헌(Reference)

[1] Gartner, Kasey Panetta, Is the Cloud Secure?, Oct 10 2019, https://www.gartner.com/smarterwithgartner/is-the-cloud-secure.

[2] Min-Hyuck Ko, Daesung Lee, “Zero Trust-Based Security System Building Proces,” Journal of the Korea Institute of Information and Communication Engineering, Vol.25, No.12, pp.1898-1903, 2021. http://doi.org/10.6109/jkiice.2021.25.12.1898

[3] Mi Yeon Kim, DaeGyeom Kim, Jong-Min Jang, Sang-Jun Park, Souhwan Jung, Jungsoo Park, “A Study on Zero Trust Technology Trends,” Smart Media Journal, Vol.12, No.2, pp.15-26, 2023. http://doi.org/10.30693/SMJ.2023.12.2.15

[4] Scott Rose, Oliver Borchert, Stu Mitchell, Sean Connelly, “Zero Trust Architecture”, NIST Special Publication 800-207, 2020.

[5] CISA, “Applying Zero Trust Principles to Enterprise Mobility For Public Comment”, 2022.

[6] Craig A. Lee, Robert B. Bohn, Martial Michel, “The NIST Cloud Federation Reference Architecture”, NIST Special Publication 500-332, 2020.
[7] CISA, “TIC 3.0 Cloud Use Case Draft_1”, 2022.
[8] CISA, “TIC 3.0 Security Capabilities Catalog v2.0_0”, 2020.
[9] 행정안전부(디지털자원정책과), “행정·공공기관 민간 클라우드(SaaS) 이용사례집”, pp.77-85, 2022.
[10] 성기화. “행정공공기관 K-클라우드 이용 활성화를 위한 성과 분석 연구” 국내석사학위논문 전남대학교, 2023.
[11] CISA, “TIC 3.0 Remote User Use Case”, 2021.
[12] CISA, “TIC 3.0 Branch Office Use Case”, 2021.

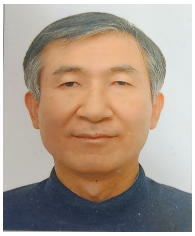
◐ 저 자 소 개 ◑

이 수 현 (Soo-hyun Lee)
2020년~현재 서울여자대학교 정보보호학과
관심분야: 클라우드 보안

임 하 늘 (Ha-neul Lim)
2020년~현재 서울여자대학교 정보보호학과
관심분야: 클라우드 보안

배 병 철 (Byung-chul Bae)
1996년 2월 홍익대학교 일반대학원 전자계산학과 석사
2007년 2월 충남대학교 대학원 컴퓨터공학과 박사 수료
1996년 1월~1999년 1월 국방정보체계연구소 연구원
1999년 1월~2000년 1월 국방과학연구소 연구원
2000년 2월~현재 ETRI부설연구소 책임연구원
관심분야: 클라우드 보안, 개방형 운영체계, 분산컴퓨팅 및 네트워크 보안

◐ 저 자 소 개 ◑



강 은 성(Eunseong Kang)
1986년 서울대학교 전자계산기공학과 공학사
2017년 연세대학교 정보시스템학석사
2003년~2008년 안랩 연구소장
2008년~2013년 SK커뮤니케이션즈 CSO
2014년~2017년 CISO Lab 대표
2017년~2019년 블록체인오에스 CISO
2023년~~현재 서울여자대학교 정보보호학과 조교수
관심분야: 개인정보보호, 위험관리, 공급망보안

김 형 종 (Hyung-Jong Kim)
1996년 성균관대학교 정보공학과 공학사
1998년 성균관대학교 정보공학과 공학석사
2001년 성균관대학교 전기전자 및 컴퓨터공학과 공학박사
2001년~2007년 한국정보보호진흥원 수석연구원
2004년~2006년 미국 Carnegie Mellon University, CyLab 국제공동연구원
2013년~2014년 미국 Carnegie Mellon University, ECE, Visiting Professor
2007년~현재 서울여자대학교 정보보호학과 정교수
관심분야: 개인정보보호, 블록체인 서비스 성능평가, 클라우드 서비스 보안 모델