제로트러스트 관점으로 본 디지털플랫폼정부 고려 사항

목정현[1], 이석준[2]
[1]가천대학교 컴퓨터공학과 학부생
[2]가천대학교 컴퓨터공학부 교수
johnmok@gachon.ac.kr, junny@gachon.ac.kr

Consideration of Digital Platform Government with Zero Trust

Jung-Hyun Mok[1], Sokjoon Lee[2]
[1]Dept. of Computer Engineering, Gachon University
[2]Dept. of Smart Security, Gachon University

요 약

인공지능·데이터·클라우드 등 혁신적인 기술로 새로운 사회 구조를 만드는 시대가 도래하면서 현 정부 핵심 국정과제 중 하나로 디지털플랫폼정부(DPG) 구현이 언급되었다. DPG는 수많은 공공 데이터를 관리하고 있으며, 중요·민감 데이터의 안전성을 유지하기 위한 신보안체계로서 '제로트러스트'를 고려하고 있다. 하지만 DPG에 제로트러스트 보안 개념을 적용하고자 할 경우 기업이나 정부 기관 대상의 제로트러스트와 달리 DPG는 참여 주체(정부, 민간 기업, 일반 국민 등)가 다양하고 민간 클라우드 활용을 지향하는 만큼, 이러한 특징을 고려하여 아키텍처를 설계해야 한다. 따라서, 본 논문에서는 DPG에 제로트러스트 보안 아키텍처를 도입할 경우, 고려해야 할 점을 제시한다.

1. 서론

디지털 전환과 클라우드 시대가 도래하면서 정부는 국민에게 빠른 처리 속도와 편리함을 바탕으로 다양한 양질의 정부 서비스를 제공하기 위해 '디지털플랫폼정부(Digital Platform Government, 이하 DPG)라는 개념을 앞세웠다. 국정과제에서 DPG를 "모든 데이터가 연결되는 디지털플랫폼에서 국민·기업·정부가 함께 사회문제를 해결하고, 새로운 가치를 창출하는 정부"라고 정의했다[1].

DPG에는 공공재 성격의 다양한 중요 데이터를 이용·저장할 수 있어야 하므로, 보안 아키텍처를 신중하게 설계해야 한다. DPG 실현을 위해 설립된 대통령 직속 디지털플랫폼정부위원회(이하 DPG위원회)에서 새로운 보안 체계로 제로트러스트를 도입한다고 언급했다[2]. 제로트러스트란, 네트워크가 침해되었다는 가정하에 정보 시스템 및 서비스가 각각의 요청에 대한 접근 권한을 정확하고 최소한으로 판단함으로써 불확실성을 최소화하려는 개념이다[3]. 이미 미국, 영국 등 글로벌 국가들은 제로트러스트를 정부 시스템에 적용하겠다고 선언했으며, 국가 기관의 보안 체계를 위해 제로트러스트는 중요하게 다루어지고 있다. 따라서, 본 논문에서는 DPG에 제로트러스트 도입할 경우 고려할 점을 제시하고자 한다.

2. 디지털플랫폼정부 목표

DPG위원회에서 발표한 DPG 목표는 ①기존 기관 간의 데이터 칸막이를 해소하고 디지털을 기본으로 행정체계를 전반적으로 혁신 ②한 곳(플랫폼)에서, 인공지능·데이터 기반의 과학적 행정 일상화 ③민관이 함께 사회문제를 발굴·해결하는 협업플랫폼 구축 ④개인정보 등 정보 주체에 대해 안전을 보장하는 보안 체계 구축 등 크게 4가지로 구성된다.

이와 같은 목표를 가지고 DPG에서는 'DPG 허브'라는 클라우드 기반 통합플랫폼 구성도를 발표했다. (그림 1)은 DPG 허브의 개념도이다.

(그림 1) DPG 허브 개념도[2]

3. DPG에 제로트러스트 도입 시 고려할 점

3.1 5가지 핵심 요소별 고려 사항

미국 사이버보안 및 인프라보안국(CISA)에서 2021

년 6월에 '제로트러스트 성숙도 모델'을 발표하고, 5가지 핵심 요소에 대한 제로트러스트 관점의 성숙도 모델을 제안했다[3]. 다음은 위에서 언급한 5가지 핵심 요소를 기준으로 DPG에 제로트러스트 도입 시 고려할 점에 대하여 정리했다.

- Identity: DPG에서 기관·기업·국민은 데이터 인프라에 있는 데이터를 자유롭게 조회·이용이 가능하지만 모든 데이터에 대한 접근 권한을 가지는 것은 아니다. 예시로, 일반 사용자는 원하는 공개데이터를 조회할 수 있지만, 기관·기업은 공개데이터뿐만 아니라 민감도가 높은 데이터(다수의 공공·개인정보를 활용)도 이용 가능할 것이다. 또한 서비스 접속 과정에서 사용되는 다양한 인증 체계(공동·금융인증서, 민간 SSO, KISA의 DID)가 이용되고 있어, 각 체계에 따르는 인증시 신뢰도를 적절하게 추론할 수 있는 시스템을 만들어야 한다.
- Devices: DPG 허브에 접속하는 모든 단말은 내부 공격의 시작점이 될 수 있으므로, 단말의 안전성을 위해 EDR(Endpoint Detection Response) 솔루션과 같은 지속적인 단말 상태 수집·모니터링으로 사이버 공격에 대비해야 한다.
- Networks: DPG 허브에 접속하려면 DPG에서 지정한 안전하고 암호화된 DNS서버를 통해 접속하는 것이 바람직하다. 또한, 네트워크가 공격당했어도 조직 내 다른 환경은 공격당하지 않도록 Micro Segmentation, SDP와 같은 기술들이 활용되어야 한다[4].
- Application&Workload: DPG 허브는 수많은 응용 프로그램을 포함하거나 접속을 허용할 것이나 모든 안전성을 사전에 평가하기 어려울 수 있다. 이를 위해 보안 테스팅을 위한 업체를 선정하고 버그 보상금과 같은 취약점 공개 프로그램을 활성화하는 것이 바람직할 것으로 보인다.
- Data: 데이터 관리 및 보안 가이드 개발이 필요하고 국내에서 민간 클라우드 기업 이용 시 CSAP의 보안 인증을 통과한 기업의 클라우드를 이용하는 것을 권장한다.

3.2 신원인증 체계에 따르는 신뢰도 평가 방안

DPG에서 여러 기관·기업이 참여하는 만큼 신원인증 수단이 필요하다. 신원 인증 수단으로 가장 일반적인 형태인 ID/PW, DID, 공동인증서 등이 가능하며, 미 연방정부의 경우 NIST의 NPIVP[5] 등의 사례도 존재한다. 하지만 현재 DPG에서는 각각의 인증 수단에 대한 신뢰도 및 위험을 어떻게 평가해야 할지에 대한 구체적인 방안이 없다. 따라서, 제로트러스트 관점에서 DPG 인증 체계 및 일관된 신뢰도 평가 방안에 대한 고려가 필요할 것으로 보인다.

3.3 CSAP 인증제 발전 가능성

국내에서 사용하는 클라우드 보안 인증제도로 CSAP(Cloud Security Assurance Program)가 있다. 클라우드컴퓨팅법 제20조에 따라 DPG가 클라우드 서비스를 이용하려고 할 때 CSAP 인증을 받은 클라우드 서비스를 이용할 가능성이 크다. 비슷한 사례로 미연방 정부에서 FedRAMP라는 연방 정부를 위한 클라우드 보안 인증제를 시행 중이다.

FedRAMP의 경우 2011년, CSAP는 2015년에 연구가 시작되어 상대적으로 CSAP의 연구 기간이 비교적 짧다. FedRAMP는 보안 등급을 3단계(High·Moderate·Low Impact Level)로 나누고 있으나, CSAP는 2023년 1월에 본격적으로 등급을 3단계로 나누었고 현재는 하등급만 인증하고 있다. 이는 앞으로 상·중등급에 대해서 구체적으로 통제항목을 정하여 관리할 필요성이 있음을 보여준다. 따라서 FedRAMP와 CSAP의 세부적인 통제항목의 내용을 비교하여 상·중 등급을 개선·보완하는 과정이 필요할 것으로 보인다.

4. 결론

DPG의 목표 및 DPG 허브의 개념에 대해 간단히 소개하고 제로트러스트 도입 시 핵심 5요소(Identity, Device, Network, Application&Workload, Data)를 가지고 어떤 점을 고려해야 하는지, 어떤 개선점이 있을지 살펴보았다. 신원인증체계에 따르는 신뢰도 평가 방안 및 CSAP 인증제의 발전 가능성에 대해 차후 구체적인 해결방안을 모색할 계획이다.

5. Acknowledgement

이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.RS-2023-00225201, 국방 무인이동체 역이용 방지 제어권 보호기술 개발)

참고문헌

[1] 백인수, 디지털 플랫폼 정부의 개념과 특징, 한국지능정보사회진흥원(NIA), 2022

[2] 디지털플랫폼정부위원회, 디지털플랫폼정부 '실현계획', 2023

[3] CISA, Zero Trust Maturity Model, 2021

[4] Scott Rose et al., Zero Trust Architecture, NIST, NIST SP800-207, 2021

[5] "해외보안인증제도 연구조사", 한국인터넷진흥원, 2020