석사 학위 논문

제로 트러스트 개념을 활용한 지방행정공통정보시스템 내부 사용자 본인 인증 방법 개선

Improvement of User Authentication Method in the Common Information System of Local Administration by Using the concept of Zero Trust

현 광 남

제주대학교 대학원

융합정보보안학협동과정

2024년 2월

제로 트러스트 개념을 활용한 지방행정공통정보시스템 내부 사용자 본인 인증 방법 개선

이 논문을 융합정보보안학협동과정 석사 학위논문으로 제출함

현 광 남

제주대학교 대학원

융합정보보안학협동과정

지도교수 박 남 제

현광남의 융합정보보안학협동과정 석사 학위논문을 인준함

2024년 2월

심사위원장 최 근 배 인

위 원 박 남 제 인

위 원 주 연 수 인

목 차

표 목차

그림 목차

제로 트러스트 개념을 활용한 지방행정공통정보시스템 내부 사용자 본인 인증 방법 개선

현 광 남

제주대학교 대학원 융합정보보안학협동과정

요 약

4차 산업혁명의 도래와 ICT 기술의 발전으로 컴퓨팅 환경이 급격하게 변화하고 있다. 또한, 코로나바이러스의 확산은 우리 사회의 업무 환경 및 행정서비스 등에 많은 변화를 가지고 왔다.

원격회의와 재택근무가 활성화되고, 워케이션(workation)이 확대됨에 따라 모바일이나 노트북 등을 활용하여 원래 근무지가 아닌 여러 장소에서의 내부 정보 시스템 접근이 증가하고 있다.

이러한 사회적·기술적 변화는 사용자 입장에서는 편리함이 증가하였지만, 보안관리자 입장에서 보면 정보자원 및 정보서비스에 대한 정보보호 차원의 관리 범위가 점점 확대되고, 통제의 어려움이 증가하고 있다. 정보시스템에 대한 해킹 방법이 더욱 다양해지고, 개인정보 유출 등의 정보보안 사고 등이 지속적으로 발생하고 있으며, 사회적인 문제로까지 발전하고 있다.

특히, 행정기관의 정보시스템은 대규모의 데이터를 관리하고 있으며, 주민등록번호 등을 포함한 고유식별번호까지 포함되어 있는 경우가 많아. 정보 유출 시 사회적인 파장이 클 뿐만 아니라, 이와 연계된 각종 범죄가 증가하고 있다.

특히, 공공기관에 대한 보안사고는 외부의 해킹에 의한 사고보다 공공기관 내

부의 근로자 또는 임시 근로자들에 의한 보안 사고가 점점 증가하고 있는 현실이다.

또한, 정부는 전자정부 시대를 지나 디지털플랫폼정부(DPG)를 목표로 인공지능·데이터·클라우드 등 혁신 기술을 활용하여 국가 사회 시스템의 변화를 추구하고 있다. 급변하는 디지털 수요에 대응하기 있기 위해 공공기관 정보 시스템의 고도화 사업 추진하고 있으며, 민간 클라우드 네이티브 컴퓨팅 기술을 도입하기 위한 활동을 지속하고 있다.

그러나 안타깝게도 행정기관의 대표 시스템인 지방행정공통정보시스템은 구축된지 17년이 경과하고 있으나, 관련 혁신 기술을 반영하지 못하고 있고, 향후 2026년이 되어야 새로운 시스템으로 전환·구축할 수 있다.
현재 지방행정공통정보시스템의 현행 방식에 따른 사용자 본인 인증과 사용자 접근 권한 정책으로는 대규모 보안 사고가 발생할 가능성이 아주 높다. 사용자 인증 방식이 단순하고, 시스템 접근 정책이 세밀하지 못하여 업무 담당자별 접근 권한의 체계가 확립되어 있지 않아, 지방행정공통정보시스템의 사용자 인증에 관련된 새로운 보안 정책 개발이 시급하다.

최근 들어, 아무도 신뢰하지 않는다는 제로 트러스트(Zero trust) 개념이 등장하게 되었고, 기존의 사용자 인증 방식과 사용자 접근 정책에 대한 변화를 요구하고 있다. 이에 맞게 지방행정공통정보시스템과 같은 기존 내부 정보시스템에 바로 적용할 수 있는 보안 정책 모델 개발이 필요함에 따라, 이에 대한 연구를 진행하였다.

본 논문은 공공기관의 행정정보시스템의 보급 유형과 변화의 방향을 분석하고, 이에 따른 보안 정책의 변화, 클라우드 컴퓨팅 시스템에서 활용되고 있는

제로 트러스트(Zero trust) 개념에 대한 연구하였다.

지방행정공통정보시스템 접근을 위한 사용자 보안 인증 방법을 다단계 인증(MFA) 방식으로 변경하고, 실시간 인증((Continuous Authentication) 방식의 도입, 사용자 접근 정책을 세분화하는 보안 정책을 설계하고, k-Fold 교차 검증 방식을 통해 보안성과 경제성의 긍정적 효과가 있음을 확인하였다.

공공기관의 행정정보시스템은 광범위하고, 다양하기 때문에 각각의 상황에 맞는 다양한 보안정책 및 시나리오가 필요하나, 본 연구에서 제안한 보안 정책은 모든 행정정보시스템에 적용하지 못하는 한계가 있지만, 공무원 조직의 가장 핵심 시스템인 지방행정공통정보시스템의 업무 환경에서 즉각적으로 실현 가능하면서도 보안성을 강화할 수 있는 보안 정책을 설계하였다는 데 큰 의의가 있다고 할 것이다.

주제어 : 정보 보안, 사용자 인증, 사용자 접근 정책, 행정정보시스템, 제로 트러스트

Ⅰ. 서론

1.1. 연구의 배경

코로나바이러스의 확산에 따라 사회적으로 디지털 전환이 급속하게 이루어졌다. 그로 인해 기존 대면 방식의 업무 스타일에서 비대면 방식의 업무 스타일로 빠르게 전환되었고, 그 현상은 행정・공공기관에도 적용되었다. 재택근무가 활성화되고, 원격회의의 활용 빈도가 많아졌다

이러한 업무 방식의 변화는 보안 정책에도 많은 변화를 가지고 왔다. 기존에는 외부 네트워크와 내부 네트워크와의 차단을 통한 보안 정책에 많은 투자를 했으나, 외부 네트워크에서 내부 네트워크로의 접속이 많아짐에 따라 외부에서 접속하는 내부 사용자들에 대한 체계적인 통제가 필요하게 되었다.

그리고, 디지털 전환에 발맞춰 정부에서도 행정정보시스템을 클라우드 컴퓨팅을 활용한 시스템 전환을 가속화하고 있다. 민원 종류의 확대, 민원 서비스의 다양화 등에 발맞추기 위해 대용량・초고속 시스템이 필요하게 되었고, 민간 기술의 발전과 행정기관의 정보 수준 차이를 극복하기 위해 민간 기술을 적극적으로 도입하고 있다.

그러나 그동안 민간에 비해 폐쇄적이고, 상대적으로 새로운 기술 도입이 늦은 행정기관의 보안 정책은 외부 네트워크에서 내부 네트워크로의 접속을 차단하는데 주력해 왔고, 내부 행정 사용자에 대한 보안 정책 개발에 대해서는 부족한 면이 많았다.

행정기관 업무담당자들의 보안의식 부족과 안일한 태도로 행정기관 내부 사용자들에 의한 개인정보 유출 사건이 지속적으로 발생하고 있다. 하였다. 행정기관 업무 담당자들은 일반 국민들보다 다양하고 대용량의 데이터에 접근할 수 있는 권한이 있으나, 사용자별 접근 권한에 대한 경계가 모호하고, 예전 방식의 사용

자 인증 방식을 사용하고 있다. 이로 인해 자신의 사용자 계정을 다른 사람에게 양도하거나, 다른 사람의 계정을 아무런 죄책감 없이 사용하는 경우가 자주 발생하였고, 사회적 문제로까지 발전하였다.

이에 따라, 행정기관 업무 담당자에 대한 사용자 접근 정책 및 인증 방식을 변경해야 하며, 최근 등장한 제로 트러스트(zero-trust) 개념과 접목한 보안 정책 개발이 시급히 필요한 시점이다.

1.2. 연구의 목적 및 필요성

전자 정부의 출현과 대국민 서비스의 전자화를 통해 공공·행정기관에서 보유하고 있는 데이터의 양은 점점 방대해지고 있다. 특히 사회보장 제도 확대, 복지 시스템 발달, 코로나 19 사태 등으로 공공기관이 보유하게 되는 데이터는 점점 세분화되고, 민감해지고 있다.

그래서 개인정보보호법 등이 제정되고, 관련 제도들을 정비하고 있으나, 행정정보시스템 내부 사용자들에 대한 보안정책은 크게 변화가 없으며, 이에 따라 다양한 보안 취약점이 존재한다.

또한, 코로나 19 바이러스 확산으로 인해 시작된 재택근무를 비롯한 원격 근무의 확대는 공공기관에서도 예외가 되지 않았다. 이러한 원격근무의 증가는 사용자의 입장에서는 편리성이 증가되었지만, 보안적인 측면에서는 바람직하지 상황이 되었다. 내부 정보 시스템이나 데이터에 대한 접근 경로가 다양해지면서, 접근하는 대상에 대한 정확한 인증을 하기 어려워진 현실이 되어 가고 있다.

이에 따라, 아무것도 신뢰하지 않는다는 ‘제로 트러스트’ 개념의 보안 패러다임을 행정에서도 적용해야 될 필요성이 대두되었다. 특히, 행정·공공기관의 업무 처리의 근간이 되고 있는 지방행정공통정보시스템에 대한 사용자 접근 정책과 인증 방법의 한계를 확인하고, 제로 트러스트 개념을 적용할 수 있는 사용자 인증 의 개선 방법을 찾아보고자 한다.

1.3. 연구의 범위와 방법

본 연구의 목표를 달성하기 위해 기존 연구 자료와 공공 기관의 교육 자료, 관련 법령과 지침, 웹 사이트 내에서의 검색 자료를 참조하였다.

본 연구는 빠르게 변화되는 공공기관의 행정정보시스템과 보안 환경의 변화에서 행정정보시스템 운영현황과 새로운 보안 정책의 적용 여부를 반영할 수 있는지에 대한 기술적 방법에 대해 진행하였다. 이를 위해 기존 국가 및 지방정부에서 운영되고 있는 행정정보시스템 운영 상황에 대한 분석을 실시하고, 공공기관에서 도입되고 있는 클라우드 컴퓨팅 시스템과 이에 따른 보안 정책에 대한 사전 분석을 실시하였다.
또한, 지방행정정보시스템 중에서도 행정 업무의 근간이 되고 있는 지방행정공통정보시스템의 사용자 접근 정책과 사용자 인증방식에 대한 사전 연구를 진행하였다.

현재 시점에 적용 가능한 사용자 인증 방식을 통해 새로운 보안 정책 모델을 설계하고, 실질적인 적용 가능 여부를 검증하기 위해 실험 시나리오를 구성하고, k-Fold 교차 검증 방식을 통해 보안성 및 효율성에 대한 검증을 진행하였다.

1.4. 연구의 구성

이 연구는 총 5장으로 구성되며, 각 장은 연구의 전체적인 흐름과 내용을 다룬다. 제 I 장 서론에서는 연구의 배경, 목적 및 필요성, 그리고 구성에 대해 설명한다. 이 장에서는 연구가 다루고자 하는 주요 이슈와 연구방법론, 그리고 연구의 중요성을 강조한다.

제 II 장 이론적 배경에서는 행정정보시스템의 운영 개요와 이에 따라 구축 운영

되고 있는 국가 표준 행정정보시스템과 지방정부 행정정보시스템의 구체적인 사례를 확인하고, 사용자 인증 방식과 관련된 개념 및 선행 연구에 대한 분석을 실시하였다.

제Ⅲ장에서는 지방정부 행정정보시스템의 환경 분석에 대한 세부적인 연구를 진행한다. 클라우드 컴퓨팅 도입과 그에 따른 보안 정책, 새롭게 등장하고 있는 제로 트러스트에 대한 개념, 본 연구에서 다루고자 하는 지방행정공통정보시스템에 대한 권한 체계 및 본인 인증 관리 프로세스에 대해 연구한다.

제Ⅳ장에서는 제로 트러스트 개념에 따른 보안 정책 및 시나리오를 설계하고 이에 따른 이론적 검증을 실시한다.

마지막으로, 제Ⅴ장에서는 본 연구의 결론을 제시하고, 이번 연구의 한계점에 대한 고찰, 연구 결과의 의미와 중요성 강조한다. 또한, 연구 방향에 대한 제안을 통해 연구가 나아가야 할 길을 제시한다.

Ⅱ. 이론적 배경

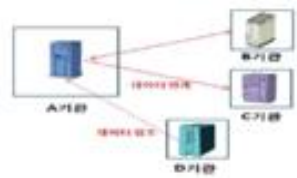
2.1. 행정정보시스템 운영 개요

정부는 정부의 혁신 방법으로 종이문서의 전자화 및 전자 결재화를 시도하며, 행정정보시스템을 구축·운영하고 있다. 행정정보시스템이란 행정기관이 행정정보를 생산·수집·가공·저장·검색·제공·송신·수신하고 활용할 수 있도록 하드웨어·소프트웨어·데이터베이스 등을 통합한 시스템을 말한다. 행정정보시스템을 구조에 따라 분류하면 <표 Ⅱ-1>과 같다.

초기의 행정정보시스템은 각 기관 및 부처에서 개별 시스템을 구축하여 관리하였다. 네트워크의 속도 문제, 데이터 처리를 위한 시스템 성능 문제에 따라 단일 기관 내 단일 시스템을 사용하여 구축하였다. 국가, 안보, 수사 등 기밀 관리를 위한 시스템인 경우도 단일기관 단일 시스템 유형을 사용하였다.

[표 Ⅱ- 1] 행정정보시스템 구조에 따른 구분

구분	개념도	설명(사례)
단일기관 단일 시스템		• 업무 또는 서비스를 위해 단독 시스템으로 구성되어 있으며, 단일기관에서 운영, 관리 •타기관 및 타시스템과 데이터 연계가 없는 단순 구조 •단순한 구조의 유형이며, 관리 주체 등이 명확함 ex) KAIST 전자연구노트시스템
단일기관 통합 시스템		•한 개 기관에서 업무별 다수 시스템이 통합DB를 통해 상호간 데이터를 공유·참조·생성 ex) 특허청 특허넷시스템

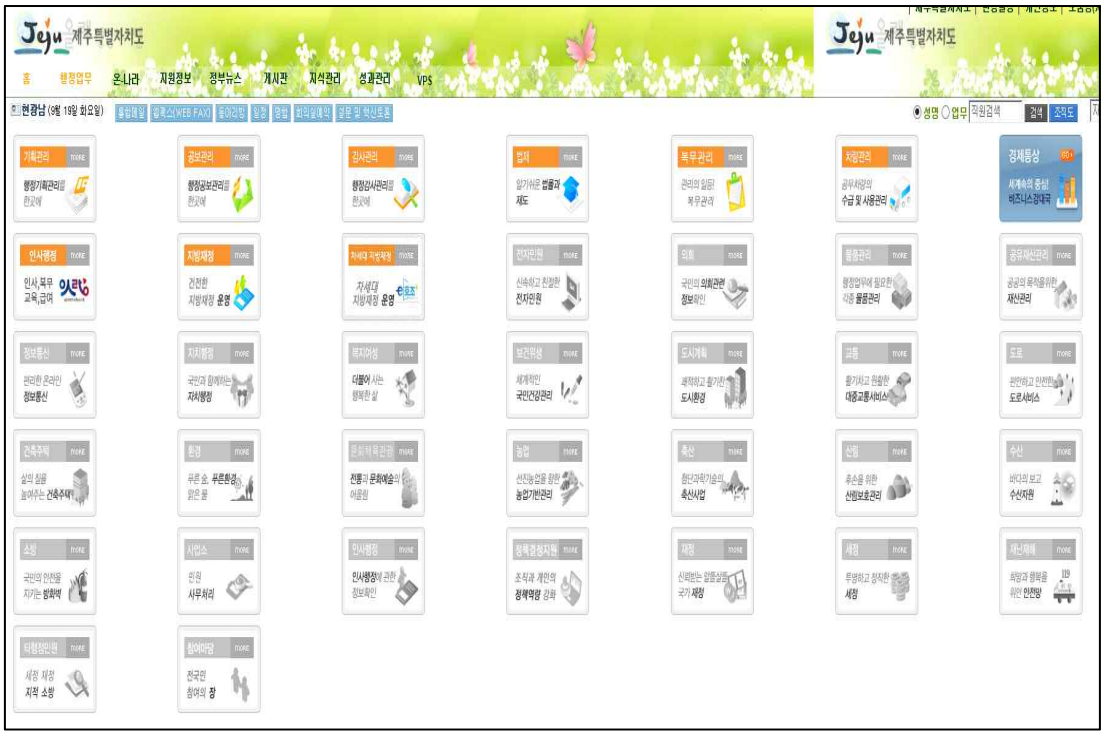
중앙 집중형		•동일 행정기관 내 다수의 기관이 중앙시스템에 접속하여 데이터를 생성·처리 •중앙시스템에 다수 기관에서 생성된 데이터는 업무처리를 위해 각 기관에서 참조 ex) 차세대 지방재정시스템
다기관 연계형		•하나의 기관 시스템에서 생산된 데이터를 다수 기관에서 연계 또는 참조하여 업무 처리하는 유형 ex) 산림청 산림자원통합시스템, 국민신문고시스템
중앙 – 지자체간 연계형		•국가위임사무의 경우 업무처리를 위한 시스템은 각 지자체에서 운영-관리되며, 지자체별 생성된 데이터는 중앙에서 수집하여 통계 분석 등 업무 참조 ex) 국토부 국토정보시스템, 시도.행정시스템

IT 기술의 발달을 통해 시스템 성능이 향상되고, 각 부처 및 기관 데이터 연계의 필요성이 대두됨에 따라 여러 기관 간 정보시스템을 연계하거나 중앙부처에서 개발하고 지방자치단체에서 시스템을 운영하는 중앙-지자체 간 연계형 정보시스템이 보급되기 시작하였다.

대표적인 사례가 지방행정공통정보시스템이다. 전자정부 조기 정착을 위해 중앙기관과 지방자치단체는 정보화사업에 지속적인 투자를 진행해 왔다. 중앙정부기관에서 업무의 일관성과 행정의 효율화 및 국가(지방) 위임사무를 처리하기 위해 위해 중앙-지차체간 연계형인 행정정보시스템들을 개발·구축하고 전국 지방자치단체에 보급하였다. 이런 시스템을 국가표준행정정보시스템이라고 하며, 대표적으로 시도·새올 행정, 지방재정(e-호조), 지방인사(인사랑), 지방세(e-지방세), 건축(세움터), 부동산 거래관리, 세외수입, 도로명 주소 등 다양하다.

이중에서 지방행정공통정보시스템은 전국 17개 시도, 229개 시군구 공무원(약 31만명)이 사용하고 있으며, 일 평균 23만 건의 대민 및 행정서비스를 처리하고

있다.



[그림 Ⅱ- 1] 시도 행정 화면 캡처

행정정보시스템의 정보시스템 유형별로 분류하면 <표 Ⅱ-2>와 같다. 공공부문에서 보유·운영하고 있는 정보자원에 대한 현황 통계를 작성하여 범정부 EA 포털[1]에서 제공하고 있다. 이를 통해 유사 업무가 많은 지방자치단체의 개별 시스템 구축으로 인한 중복투자를 방지하기 위해 공통 업무에 대한 모니터링을 실시하고 있다. 보유 시스템은 소유 기관별로 분류하면 중앙행정기관은 총 개별시스템 1,775개, 공통시스템 146개 등 총 1,921개의 시스템을 운영하고 있다. 또한 광역자치단체는 1,837개 시군구를 포함한 지방자치단체는 7,573개의 시스템 등 총 9,410개의 행정정보시스템을 구축·운영하고 있다. 그 외 입사헌법/독립기관은 148개, 그 외 공공기관은 5,611개 등 총 17,090개의 시스템을 보

1) 범정부 EA 포털 : 범정부적으로 정보자원의 현황 관리 및 정보화를 효율적으로 추진하기 위해 각 기관의 공유 및 공통적으로 관리해야 할 정보항목과 항목 간 연관관계를 정의하고, 각 기관은 정보시스템 대한 정보를 입력하고, 이 정보를 범정부 EA포털에서 제공함. https://www.geap.go.kr/

유하고 있다.

유형별로 분류하면 개별시스템이 총 1만3,307개로 가장 많았고, 표준(공통)시스템은 총 3,670개, 단일(공통)시스템은 총 113개를 가지고 있다.

[표 Ⅱ- 2] 정보시스템 유형별 현황

(단위 : 개, 억원)

구분			개별 시스템[1]	공통시스템[2]		합계	평균[3]
				단일	표준		
중앙행정기관		시스템수	1,775	70	76	**1,921**	**38.42**
		구축비	37,219	7,636	2,987	**47,841**	**24.90**
지방자치단체	광역자치단체	시스템수	1,503	3	331	**1,837**	**108.06**
		구축비	9,719	61	2,442	**12,223**	**6.65**
	기초자치단체	시스템수	4,331	6	3,236	**7,573**	**33.51**
		구축비	11,620	47	6,732	**18,398**	**2.43**
입사헌법/독립기관		시스템수	147	0	1	**148**	**21.14**
		구축비	492	0	0	**492**	**3.32**
공공기관		시스템수	5,551	34	26	**5,611**	**11.09**
		구축비	58,676	1,474	640	**60,790**	**10.83**
합계		**시스템수**	**13,307**	**113**	**3,670**	**17,090**	**21.28**
		구축비	**117,725**	**9,218**	**12,801**	**139,744**	**8.18**

1) 개별시스템 : 기관의 고유 서비스를 지원하는 정보시스템으로 기관별로 구축·운영하는 시스템
2) 공통시스템 : 다수기관의 공통 또는 유사한 업무수행 지원을 위하여 구축한 시스템
3) 평균시스템수 = 총시스템수 / 기관수(정보시스템 등록기관), 평균구축비 = 총구축비 / 시스템수

2.2. 국가 표준 행정정보시스템 구축 및 보급 사례

2.2.1. 차세대 지방재정관리시스템(e-호조)

정부에서 구축하고 지방자치단체에서 업무를 실행하는 국가표준행정정보시스템은 서버(HW)의 배치 장소에 따라 두 가지로 분류될 수 있다. 중앙집중형과 중앙-지자체 간 연계형으로 구분할 수 있다. 일반적인 사례는 중앙에서 시스템을 개발·구축하고 프로그램(SW)은 중앙정부에서 관리하고, 서버(HW)는 각 지방자치단체 전산실에 배치하는 중앙-지자체 간 연계형 구조이다. 전자정부 초기 조기 정착을 위해 행정정보시스템을 구축·보급하였으나, HW의 사양, 네트워크의 성능 저하로 인해 행정정보시스템의 프로그램(SW)은 중앙기관에서 일괄 운영하고, 서버(HW)는 각 지방자치단체 전산실에 배치하는 형태로 구성되었고, 대부분의 시스템이 이러한 방식으로 운영되었다.

최근 들어 HW 성능과 네트워크 속도의 증가, 기 구축 행정정보시스템의 노후화, 시스템 보안 이슈 다변화 등으로 새로운 시스템 개발·구축이 진행되었고, 차세대 행정정보시스템으로 전환을 시작하였다. 차세대 행정정보시스템은 모든 정보자원(SW, HW)을 중앙 단위에 비치하고(클라우드 방식), 지방자치단체 사용자들은 웹 형태의 접속을 통해 업무를 진행하는 방식이다.

행정안전부는 예산 집행, 계약, 자금, 자산, 부채, 세입세출외 현금 등 지방재정 운영과 보조금 관리를 위한 차세대 지방재정관리시스템(e호조)을 2023년부터 구축·운영하고 있다. 이와 더불어 지방보조금 시스템(보탬e)을 통합하여 운영하였다.

지방재정관리시스템은 전 지방자치단체의 수입·지출을 포함하여 자산 및 부채를 관리·처분하는 재정활동을 관리하는 국가 3대 시스템으로 2008년 구축하여 18년 동안 운영·유지 관리 되어왔다.

지방재정관리시스템을 통한 지출 건수는 일평균 5.9만건, 지출금액 1.7조원이며, 243개 기관 39만명이 상시 이용중이다. 또한 자치단체 67개 시스템과 국고보조금 등 33개 외부시스템과의 연계를 통해 종합적 재정관리체계 프로그램으로 활용되고 있다.

그러나, 지방재정관리시스템 구축 후 12년이 경과함에 따라 기술 구조·재정환경 등의 변화, 지출문서의 전자화에 따른 용량 부족, Active X 등 다양한 보안이슈에 대한 취약점 발견, 재정통계·분석의 한계 등의 문제가 대두됨에 따라 2018년 차세대 지방재정 정보화종합계획(ISP)이 수립되고, 예비타당성 검토를 진행하였다.

[그림 Ⅱ- 2] 차세대 지방재정관리시스템 구성도

차세대 지방재정관리시스템은 지방세, 세외수입, 보조금 등 각종 재원시스템과 지방공공기관 등과의 연계 확대를 통해 통합적인 재정관리체계 뿐만 아니라 지방보조금 운영 전반을 전자화하여 중복·부정 수급을 근절하도록 하였다. 이는 지방재정 전 주기의 관리를 통해 업무 효율성 및 정확성을 강화하고 기관·업무간 긴밀한 연계·통합을 통한 종합적 관리체계가 가능해졌다.

[그림 Ⅱ- 3] 차세대 지방재정관리시스템 업무 화면

연계된 시스템 간의 데이터를 활용한 빅데이터 플랫폼을 제공하여 가용재원, 재정추이, 통합재정수지 등에 대한 범 국가적 재정통계 및 국제 통계 작성이 가능하고, 실시간 재정 상황 분석을 통한 신속한 의사 결정 지원이 가능해졌다.

지방보조금의 철저한 관리를 위해 수기로 관리되던 지방보조사업에 대해 보조금의 공모, 집행, 정산 등의 사업관리와 지방재정(예산편성, 집행) 기능을 연계·통합·활용 기능으로 신청서류 허위 제출, 중복집행, 부정 수급 방지 등이 가능

해졌다.

또한, 주민 생활에 밀접한 개별 예산 사업에 대한 맞춤형 정보 제공 기능이 추가되었다. 주민참여예산 등 온라인 투표 플랫폼의 구현과 세금 계산서, 거래명세서 등 각종 대금 서류의 온라인 서비스를 제공한다.

각 시도단위별로 분산된 정보자원(HW, SW)을 포함한 전산시스템을 클라우드 기반의 중앙 집중형 시스템으로 개발·구축하여 통합 관리를 통한 비용절감, 자원 관리 효율화 및 범정부 프레임워크 전환, 웹표준 환경 등 개방형 표준구조를 도입하고, 보안에 취약한 Active x를 제거하여 보안성을 강화하였다.

2.2.2. 온나라 전자문서 시스템

온나라 전자문서 시스템은 중앙정부 및 지방자치단체 등 거의 모든 행정기관 전자문서의 기안, 결재, 발송, 기록 등의 처리를 담당하는 정부표준업무관리시스템이다. 온나라 시스템은 2003년 전자정부 사업의 일환으로 개발된 ' 이지원 ' 업무관리시스템 기반으로 활용하기 시작하였고, 2005년 '온-나라 업무관리시스템'(On-nara Business Process System), '온-나라 BPS'를 개발하였다.

2008년에는 정부통합지식행정시스템 'GKMC' (Government Knowledge Management Center) 개발(현재 '온나라 지식')하였으며, 2014년 정부통합의사소통 시스템 '나라e음' 개발 (현재 '온나라 이음')하였다. 2015년 온-나라 시스템과 정부통합지식행정시스템(GKMC)을 클라우드 기반으로 재개발하여 전 행정기관에서 사용하기 시작하였고, 2022년 ' 온나라 서비스 '로 명칭을 변경하여 통합 서비스를 제공하고 있다.

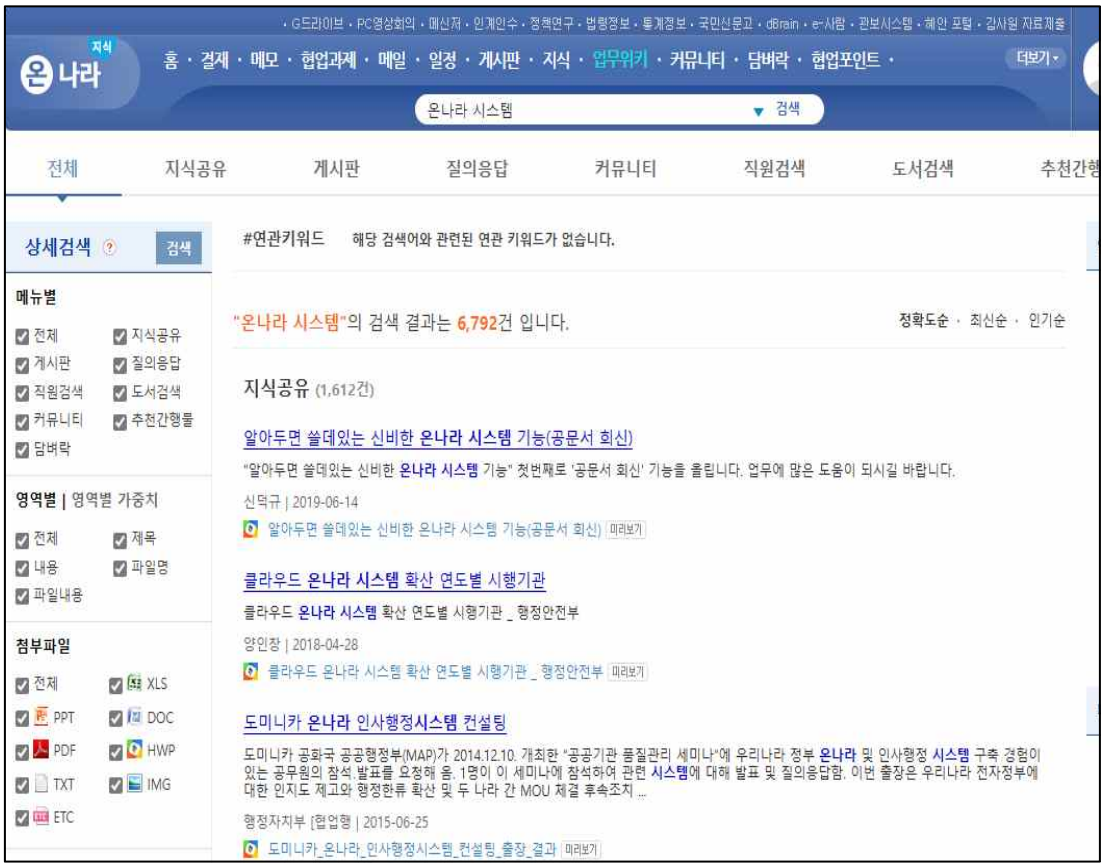
온나라 서비스는 프로그램(SW)은 중앙 단위로 구축하고, 각 서버(SW)는 광역자치단체 전산실에 비치하는 중앙-지자체 연계형 구조로 보급되었으며, 기본 구조는 [그림 II - 4] 와 같다.

[그림 Ⅱ- 4] 온나라 서비스 구성도

1) 온나라 시스템의 주요 기능

온나라 문서 기능은 웹 표준 기안기를 도입하여 기존 hwp 파일 포맷 기준에서 표준 문서 포맷(odt)을 활용하여 별도 프로그램 설치 없이 문서 작성이 가능하며, 다른 기관의 문서를 검색할 수도 있고, 대용량 파일을 첨부할 수도 있다. 하나의 공문서에 둘 이상의 기관이 공동으로 기안하고 결재할 수 있으며, ActiveX 제거 후 HTML5 기준으로 설계하였다. 업무 결재의 간소화를 위한 메모보고 기능도 포함되어 있다.

2016년 행정자치부는 기존 GKMC를 전면 개편하여, 새로운 범정부 지식관리시스템인 '온-나라 지식' 서비스를 시작했다. '온-나라 지식'은 GKMC에 있던 지식공유, 커뮤니티 기능만이 아니라, 주제별 게시판, 일정관리 등 새로운 기능도 추가하였으며, '온-나라 메일' 기능을 추가하여 행정망에서 부처, 지자체 공무원 간 이름이나 부서 검색으로 메일을 주고받을 수 있도록 하였다.



[그림 II - 5] 온나라 지식 화면 구성도

온나라 이음 기능은 온나라 시스템 내 소셜 기능이 가미된 '담벼락'과 '협업포인트' 서비스 내부 직원 메신저인 '온-나라 메신저', ' 온-나라 PC영상회의 ' 등의 기능을 제공한다. 특히, 온-나라 PC영상회의는 코로나 19 이후 비대면 회의 수요가 급속하게 증가하게 됨에 따라 국민과의 소통을 확대하기 위해 외부용 영상회의 기능을 추가하였다.

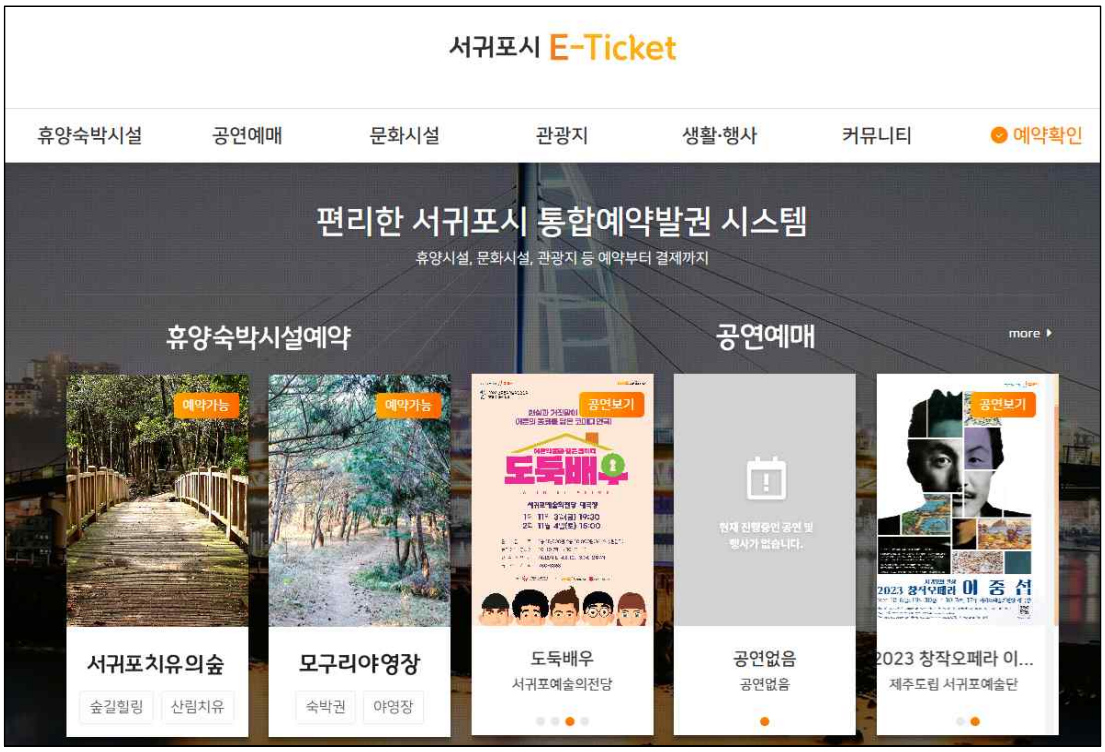
온나라 영상회의는 코로나 19 이후에 사용자가 급속하게 증가되었다. 코로나 19 이후 각종 대면 회의가 비대면 회의로 전환되면서 온나라 PC 영상회의를 주도적으로 사용하였다. 공무원 내부에서만 활용되던 온나라 PC 영상회의는 민간 참여가 요구되어짐에 따라 민간 참여가 가능한 플랫폼으로 전환되었다.

2.3. 지방정부 행정정보시스템 구축 사례

2.3.1. 서귀포시 통합예약발권시스템(e-ticket)

1) 서귀포시 통합예약발권시스템(e-ticket) 개요

지방정부의 원활한 업무 수행을 위해 디지털 서비스를 활용한 사례들이 있다. 스마트폰 보급과 예약 문화의 발달로 각 기관에서는 해당지역의 다양한 공연, 시설에 대한 인터넷 예약 서비스를 제공하고 있다. 서귀포시도 2016년 전자정부의 개방형 OS 환경 개발 및 시범 보급 사업으로 서귀포시 직영 시설(관광, 문화, 휴양, 야영 등)에 대한 매표 및 발권 업무를 온라인으로 처리하기 위한 서귀포시 통합예약발권시스템을 구축하여 서비스를 제공하고 있다.



[그림 Ⅱ- 6] 서귀포시 통합예약발권 시스템 화면

서귀포시 통합예약발권시스템은 휴양숙박시설에 대한 정보 제공, 서귀포시 치유의 숲과 모구리 야영장의 사용 예약 기능을 제공한다. 공연과 문화시설에 대한 예약은 입장권 구입부터 발권의 기능까지 제공한다. 실시간으로 할인 현황을 적용하여 결재를 할 수 있으며, 위치정보, 이용시간 안내 등의 서비스를 제공한다.

2) 서귀포시통합예약발권시스템(e-ticket) 추진 배경

서귀포시는 관광도시 임에도 불구하고, 관광지 입장 발권은 현장에서만 이루어지는 불편함이 있었다. 대규모 관관객인 경우 여행사나 관광대행사를 통해 입장권을 일괄 발권을 하였으나, 올레길의 활성화 등으로 개별 관광객이 증가함에 따라 관광지 이용현황에 대한 정보, 주변 인프라(식당, 카페)에 대한 소개 등이 필요했고, 대기 시간 감소를 위해 인터넷을 통한 예약에 대한 요구가 증대되었다. 2010년은 전후로 제주로 전입되는 귀농·귀촌인이 폭발적으로 증가하였다.

[표 Ⅱ- 3] 제주도 지역별, 시기별 인구변화 추이

지역구분		2000~2009년 인구증감	2010~2013년 인구증감	2000~2013 인구증감
제주시		**39,875**	**22,248**	**67,396**
제주시부 읍면지역	한림읍	-1,461	1,553	290
	애월읍	1,043	1,265	3,686
	구좌읍	-25,189	-502	-2,948
	조천읍	-18	-637	-123
	한경면	-1,675	35	-1,524
	추자면	-453	-242	-689
	우도면	-159	54	-54
서귀포시		**-1,934**	**2,874**	**2,104**
서귀포시부 읍면지역	대정읍	-2,355	456	-1,765
	남원읍	-2,437	-30	-2,259
	성산읍	-1,773	-1	-1,694
	안덕면	-980	307	-711
	표선면	-565	103	-303

제주로 이주해온 사람들은 제주 문화에 다양한 변화를 가지고 왔다. 본업 외에도 제주에서의 각종 위원회나 단체에 가입을 하여 자신들의 목소리를 내기 시작하였고, 자연환경 또는 지역의 문화를 개발하여 상품화하는 데 적극적으로 나서기도 하였다.

이들은 단순한 농업·어업 부문 뿐만 아니라 비농업·비어업 분야에도 중요한 역할을 하게 됨에 따라 각 지자체는 이들을 위한 다양한 정책적 지원을 시작하기 시작하였다. 이주민의 증가로 음식점 및 카페, 게스트하우스 등이 증가하였고, 대면 서비스와 더불어 인터넷 예약을 통한 서비스를 제공하기 시작하였다. 그리고 다른 지역의 귀농·귀촌 사람들과의 연대를 위한 네트워크를 구성하는 데 ICT 등을 적극 활용하였다.

이주민의 증가는 제주 지역의 문화·공연에 대한 수요를 폭발적으로 증가시켰다. 이주민들은 도시 지역에서의 문화 활동을 지속적으로 이어 나갈 방법을 강구하였고, 이를 반영한 다양한 문화 활동이 이루어졌다. 그로 인해 각 지역마다 문화 시설(서귀포 예술의 전당) 등을 신축하게 되는 결과를 가져왔고, 여기서 이루어지는 다양한 공연·전시에 대한 예약 시스템 개발이 요구되었다.

3) 서귀포시 통합예약발권시스템의 주요 기능과 한계

서귀포시 통합예약발권시스템은 서귀포시에서 운영중인 대표적인 관광지와 야영장 등의 대한 예약 가능 현황 및 시설 정보, 위치 정보, 할인 정보 등을 서비스하고 있다. 모든 서비스는 실시간으로 제공하며, 다양한 사람들의 참여를 위해 하루에 1회에 한하여 예약을 할 수 있도록 서비스를 제공한다.

또한, 관광객들의 증가에 따라 차량 이동량이 많아짐에 따라, 서귀포시가 운영하고 있는 공영주차장에 대한 정보를 제공하고, 정기 주차권을 발급할 수 있는 기능을 제공한다

서귀포시 통합예약발권시스템은 구축 후 7년이 지났으며, 사용자가 지속적으로 증가하고 있다. 또한, 서귀포시에서도 문화 시설이 확대됨에 따라 대규모 공연·

행사가 자주 이루어지고 있으나, 통합예약발권시스템의 처리량 부족으로 인한 시스템 과부하로 인해 서비스가 정지되는 경우가 종종 발생하고 있다. 또한 시스템 이용자의 예약·결재 정보를 활용한 통계 정보 제공이 미흡하며, 문화 관광 빅데이터와 연계한 관광 소비 패턴 분석, 관광지 밀집도 정보 제공 등 개인별 맞춤형 정보 제공이 부족한 현실이다.

2.3.2. e-체송함 시스템

1) e-체송함 시스템 개요 및 추진 배경

민원인들이 인허가 신청, 보조금 서류 접수 등 다양한 문서를 행정기관으로 제출·신청 위해서는 공공기관을 직접 방문을 하거나 팩스, 우편 등을 활용해 왔다. 이에 따른 번거로움과 불편함, 그리고 시간적·공간적 낭비 요인이 발생하였고, 제출된 서류의 누락 등으로 인해 다양한 문제점들이 발생하기도 했다.

접수된 공문서를 처리하는 행정기관과 담당 공무원 입장에서도 접수된 서류를 스캔하고, 전자결재 문서시스템에 등록하여 별도로 관리하는 등의 문제가 발생하였다.

지역마을회, 유관기관 등 각종 민간 단체·기관 등은 개발·구축 비용이 높은 전자결재시스템을 자체적으로 운영하기 어려워 수기 문서 체제를 유지하였다. 이로 인해 종이문서의 과다 생산, 기록물 관리의 어려움, 단순 반복 업무의 자동화 부재 등 다양한 문제를 발생시켰다.

2) e-체송함 시스템 개발 및 발전

제주특별자치도는 이러한 문제점을 해결하기 위해 행정기관의 공문서를 자동으로 민간 기관에게 발송하고, 처리할 수 있는 시스템의 도입을 검토하게 되었고, 2009년 전국 처음으로 ’e-체송함 시스템‘을 개발하여 보급하기 시작하였다.

2009년 처음 개발된 ’e-체송함’은 서귀포시와 서귀포시 관내 기관 단체 전자문서 송수신 시 공공기관 전자문서시스템에서 기안, 발송한 문서를 수신 기관의 팩스로 자동으로 수신할 수 있는 시스템으로 구축되었다. 이로 인해 공공기관과 민간 기관간 1:N 구조의 문서 발송이 가능하게 되었다.

공공기관에서의 발송은 편리해졌으나, 수신을 받는 기관 입장에서는 여전히 팩스를 통한 수발신으로 인해 예전과 큰 차이를 느끼지 못했다. 이에 따라 서귀포

시에서는 기능 고도화사업을 통해 인터넷을 활용한 전자문서 송수신이 가능하도록 시스템을 개편하였다. 이로 인해 각 민간 기관·단체에서는 e-체송함 시스템을 통해 문서를 수발신 할 수 있게 되었고, 제주시와 제주특별자치도 전 기관·단체로 확대 사용할 수 있게 되었다.

[표 Ⅱ- 5] e-체송함 연도별 처리 건수 현황

(단위 : 건)

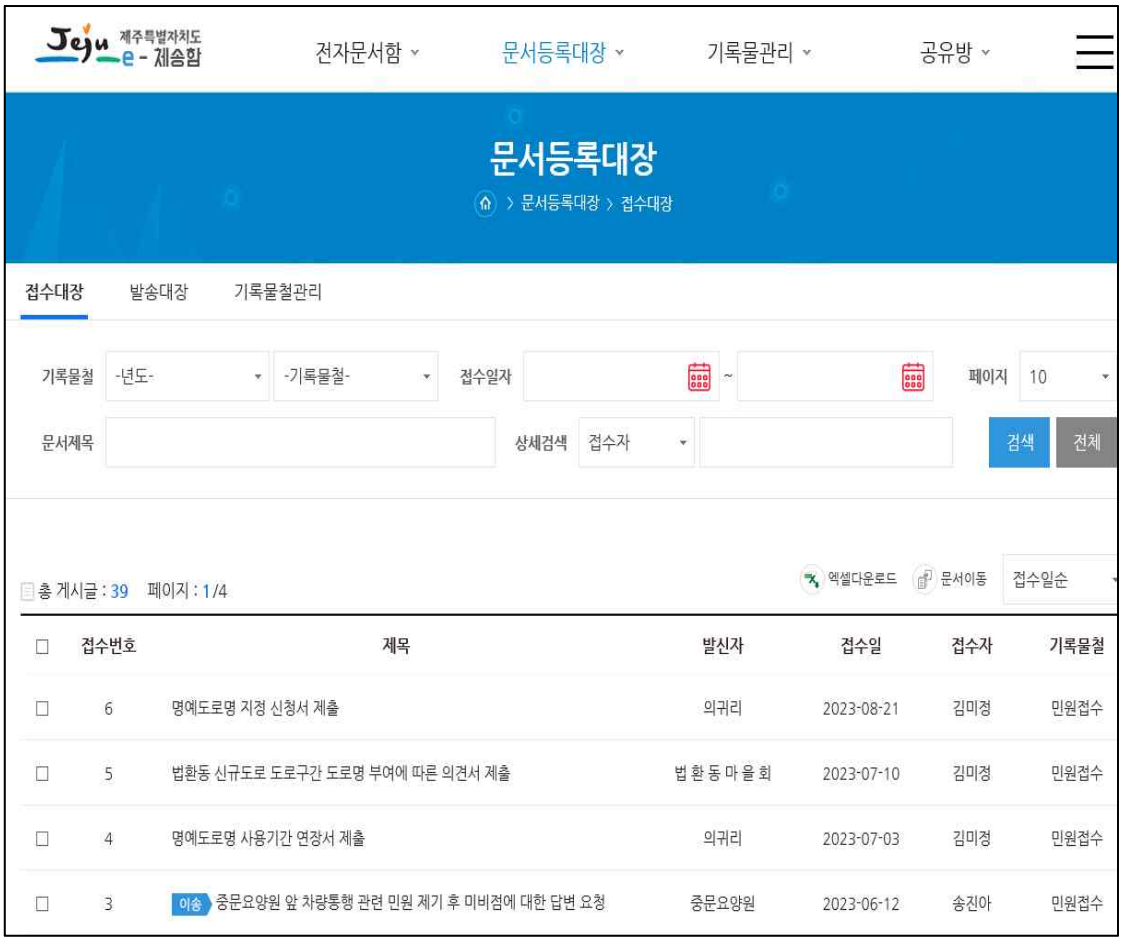
연도별	계	발송	접수	비 고
계	**2,163,709**	**468,310**	**1,695,399**	
2022년	**176,700**	52,627	124,073	
2021년	**171,568**	49,824	121,744	
2020년	**178,484**	47,550	130,934	
2019년	**194,127**	47,621	146,506	
2018년	**172,608**	41,265	131,343	
2017년	**182,764**	43,036	139,728	
2009년~2016년	**1,087,458**	186,387	901,071	

3) e-체송함 주요 기능

e-체송함은 전자문서의 생산, 발송, 송수신 등의 전자결재시스템의 기능을 가지고 있다. 전자문서 등이 효력을 발생하는 시점은 결재권자가 결재를 하는 시점이다.(전자정부법, 제26조). 민간 단체·기관도 이와 비슷한 효력을 지닌다.

‘e-체송함’ 시스템에서는 전자문서의 작성 뿐만 아니라 결재권자의 ‘결재’ 기능이 포함시켜 공식적인 문서로서의 기능이 가능토록 하였다. 전자문서의 발송을 위한 수신 기관 지정, 발신 기관의 로고 및 발신 명의 지정 등의 기능을 제공한다. 접수대장과 등록대장 기능을 통해 수발신 문서들의 목록을 확인할 수

있다.



[그림 Ⅱ- 7] e-체송함 시스템 화면

행정기관 뿐만 아니라 민간 기관에서도 업무와 관련하여 생산·접수된 문서 및 기록물 등 보존 가치가 인정되는 자료 등을 보관할 필요성이 제기되었다. ‘e-체송함’ 시스템에서는 문서등록대장을 통해 수·발신된 문서를 보관하고 열람할 수 있다. 기록물의 체계적인 분류를 위해 기록물철 기능을 추가하였고, 각 기록물철 별 보존기간 설정을 할 수 있도록 하였다. 보존 기간이 경과된 기록물은 이관 또는 선택적 폐기를 할 수 있는 기능을 제공한다.

e-체송함 시스템의 구축 목표 중 행정기관과 민간 기관과의 전자문서 유통뿐만 아니라 신속한 행정 정보 공유도 있었다. e-체송함은 민간 기관·단체에서 주로 사용하는 행정기관 홈페이지 및 보조금 시스템을 연계하였다. 「공유방」기능을 통해 다른 민간 기관과의 문서 유통 및 정보 공유가 가능하도록 구현하였다.

2009년 PHP 언어 기반으로 구축된 'e-체송함'은 시스템의 노후화에 따른 성능 저하, 개발 언어의 보안 취약성 증가, Active X 기반한 공인인증서를 활용한 단일 인증 로그인 방식으로 많은 불편함을 초래하였다. 그리고 전자정부표준프레임워크 및 HTML5 기반의 웹 표준 기술 적용이 필요했고, 다양한 이용자 환경(OS, 웹브라우저)에서의 접속, 모바일 접속을 위한 시스템이 필요함에 따라, 2018년 시스템을 재구축하였으며, 운영 주체도 서귀포시에서 제주도로 전환되었다.

3) e-체송함 유사 사례

'스마트 이장넷'은 e-체송함 기능을 활용하여 2015년 충북 괴산군에서 구축하였으며, 2015년 행정안전부의 우수정보시스템으로 선정됨에 따라 다른 지자체에서 확대 보급되었다. '스마트 이장넷'의 주용 기능은 공개 가능한 문서를 스마트 기기를 통해 이장에게 전달하는 시스템으로 문서 수·발신, 공지사항 알림, 재난 재해 현장 상황 보고, 회의 일정 및 결과 공유 등을 할 수 있다.

최초의 '문서 24' 시스템은 행정안전부에서 용역, 비영리법인, 영유아보육, 렌터카, 일자리지원, 행정처분 등 6개 분야에 대한 신청서를 행정기관 방문 없이 제출할 수 있도록 구축되었다. 행정과 민간과의 양 방향 송수신은 불가능했으며, 민간에서 행정으로의 서류 제출만 가능했고, 사전에 등록되어 승인된 업무의 서류 제출만 가능하였다.

[그림 Ⅱ- 8] 문서24 시스템 화면

2018년 행정안전부에서는 '문서 24' 시스템의 기능을 확대 구축하면서 국민과 행정기관 간 양방향 문서 수발신이 가능하도록 기능을 개선하였다. 이를 통해 민관 기관에서 발송한 문서가 공공기관 전자문서 시스템인 온나라 전자 결재 시스템으로 바로 연계됨에 따라, 수기로 등록 관리하는 불편함을 개선하였다.

'문서 24'는 'e-체송함'의 기본 기능을 전제로 개발하였기 때문에 전체적인 기능은 'e-체송함'과 유사하며, 다음과 같은 차이점이 있다.

[표 Ⅱ- 6] e-체송함과 문서24 비교

구분	e-체송함	문서24
구축연도	2009	2016
이용 대상	이·통장, 수협·농협, 복지시설 등	대국민, 민간기업
문서 작성	O	O
결재선 지정	O	X
문서 수·발신	O	O
문서 보관	O (폐기 전까지 영구 보관 가능)	O (3개월간 보관 가능)
문서 도달지점	온-나라 등 결재 시스템에 비전자문서로 등록	온-나라 등 결재시스템에서 바로 접수 가능
전달사항 안내 등 공유방	O	X
모바일	O	O

2.4. 사용자 인증

2.4.1. 사용자 인증의 개념

사용자 인증(User Authentication) 기술은 정보시스템에 접근하려는 사용자나 디바이스가 적법한 권한을 가진 자원인지를 증명하는 기술을 말한다. 가장 보편적인 기술은 ID/PW를 활용한 사용자 인증 방식이며, 각각의 금융기관, 행정기관 등에 신뢰할 수 있는 기관에서 발행된 인증서를 통한 인증, 지문이나 홍채 등 생체 정보를 활용한 사용자 인증, 두 개 이상의 사용자 인증 방식을 활용하는 다중 인증 방식(Multi-Factor Authentication)으로 발전해 나아가고 있다.

2.4.2. 사용자 인증 방식의 구분

사용자 인증 방식은 어떤 정보를 활용하느냐에 따라 지식기반 인증, 생체기반 인증, 소유 기반 인증으로 분류한다.

1) 지식 기반 인증 방식

지식기반 인증 방식은 정보시스템에 접근하고자 하는 사용자들의 정보를 사전 등록한 인증 시스템의 정보와 사용자들이 입력한 정보가 일치하는지 검증을 통해 사용자의 신분을 확인하는 방식이다.

대표적인 방식은 ID/PW 방식, 패턴 인식 방식 등 다양하게 존재하며, 각각의 보안 규칙에 따라 보안성을 강화하며, 일반적으로 인증 요소의 길이 및 조합에 따라 보안의 강도가 정해진다.

ID/PW기반 인증 방식은 초창기 정보시스템에서 적용되어 왔다. 사용자들이 직접 ID/PW를 설정할 수 있어 편리성이 높고, 시스템 관리 측면에서도 유지보수 비용이 작고, 시스템 구현이 쉬운 점이 장점이다. 시스템 구현이 간단하기 때문에 다양한 보안 취약점 공격이 존재한다.

패턴 기반 인증은 문자나 숫자의 조합이 아닌 ‘연속적으로 연결되는 선분이나 그림의 선택’을 통해 사용자를 인증하며, 사용자가 설정한 패턴 방식의 길이나 모양에 따라 보안성이 강화된다.

2) 생체기반 인증 기법

생체기반 인증 기법은 각 개인별로 고유한 값을 가지고 있는 지문, 홍채, 정맥, 안면 정보 등 생체 정보를 활용하여 사용자를 식별하는 방식이다.

사전 등록된 생체 정보와 생체 정보를 인식할 수 있는 별도의 기기를 활용하여 제시된 정보의 일치 여부를 통해 사용자를 인식한다. 생체기반 인증 방식은 소유 기반 인증 방식에 비해 복제 또는 탈취가 어렵기 때문에 보안성이 뛰어나다. 다만, 생체 정보를 인지하기 위한 별도의 장비가 반드시 필요하다는 단점이 존재하며, 최근에는 발달된 AI 기술을 활용하여 생체정보를 도용하는 경우도 발생하고 있다.

3) 소유기반 인증

소유기반 인증 방식은 OTP, 인증서, 모바일 등의 인증 토큰을 활용하여 사전 등록된 정보화 비교하여 사용자의 신분을 확인하는 방식이다.

인증서 기반 인증 방식은 신뢰할 수 있는 기관을 통해 발급 받은 개인키 인증서를 통해 인증서버에서 사용자의 공개키 인증서를 통해 검증하는 방식이다.

OTP 기반 인증은 별도의 기기나 프로그램을 이용해 일회성 난수를 생성하고 사용자가 생성된 난수를 입력 하면 인증 서버의 OTP 값과 비교하여 사용자 검증을 하는 방식이다.

4) 다중 인증(MFA : Multi-Factor Authentication)

사용자 인증에 대한 보안 공격이 다양화되고 지능화됨에 따라 기존의 사용자 인증을 복합적으로 활용하여 보안성을 강화하는 방식이다.

2.5. 관련 연구 동향

2.5.1. 기본 패스워드와 회원 가입 정보를 이용한 사용자 인증 시스템

해당 논문에서는 사용자 인증 단계에서 패스워드가 일치하지 않는 경우 회원 가입 시 추가적으로 등록된 개인 정보를 토대로 추가 인증을 통해 로그인 할 수 있는지에 대한 연구를 진행한다.

SNS, 이메일, 유튜브 등 다양한 웹 사이트를 이용하기 위해 사용자 인증을 진행한다. 최근 들어 모바일 인증, SSO 인증, 지문 인증 다양한 방식의 사용자 인증방식이 보급되어 있으나, 기본적으로 ID/PW 방식의 사용자 인증이 사용되고 있다.

패스워드를 영문, 숫자, 특수 문자 등을 활용하여 설정하나, 각 사이트마다 비패스워드 세부 설정 규칙이 다르기 때문에 사용자가 사이트별 패스워드를 기억하기 쉽지 않다. 이런 문제점으로 인해 웹사이트 방문 시 패스워드 오류로 인해 재설정을 해야 되는 경우가 많아지고 있다.

이런 문제점을 해결하기 위해 해당 논문에서는 회원가입 시에 사이트에서 요구되는 추가적인 정보를 바탕으로 사용자 인증을 진행하고, 국내의 대표 포털 사이트에서 평균 접속 시간을 단축 정도를 통해 검증하여 보안성과 편리성을 제공함을 증명하였다.

해당 논문에서의 연구 목적과 방식은 현재 시스템에서 구현된 기능을 활용하여 즉시 적용할 수 있음을 증명함으로써, 본 논문에서 연구하고 증명하고자 하는 새로운 보안 정책 개발에 적용할 수 있음을 확인할 수 있다.

2.5.2. 행정전자서명 암호체계 기술 현황 분석 및 고도화 방향

해당 논문에서는 중앙·지방 정부, 공공기관 등에서 작성자의 신원 및 문서의 변경 여부를 확인할 수 있는 행정전자서명(GPKI) 암호체계에 대한 기술 현황 분석과 고도화 방향에 대해서 연구한다

행정전자서명은 행정 환경에서의 신뢰성 및 안정성을 보장하기 위해 구축되었으며, 행정안전부에서 관리하는 “행정전자서명 프로파일 및 알고리즘 상세서‘에 의해 암호 체계를 정리한다.

행정전자서명은 안전한 암호 사용을 위하여 적용하는 연도별 적정 안정성 수준에 따르면 2020년 이후에는 128비트 암호체계로 전환하는 것을 권고하고 있다. 이를 위해 행정전자서명 암호체계 관련 표준의 현재 상태를 확인하고, 표준의 유효성 확인을 통해 충분한 안정성을 제공하는 새로운 알고리즘의 도입이 필요한지를 분석한다.

행정전자서명 알고리즘은 크게 KCDSA, RSA, ECDSA를 사용하며, 공개키 암호화 방식은 RSA 공개키를 사용한다. 대칭키 암호체계의 블록 암호는 TDEA, SEED, ARIA 등이 사용되었다. 메시지 인증코드(MAC, Message Authentication Code)는 해시 함수를 사용하는 HMAC 알고리즘을 사용한다. 이 밖에도 행정전자서명 암호체계에 적용된 다양한 암호 알고리즘, 인증서 체계, 인증서 저장 및 서비스에 대한 분석을 실시한다.

이를 통해서 행정정보시스템에서 사용되는 행정전자서명(GPKI)의 암호체계 고도화를 위해 적용되어야 다양한 연구 방법을 제시한다.

Ⅲ. 지방정부 행정정보시스템의 환경 변화 분석

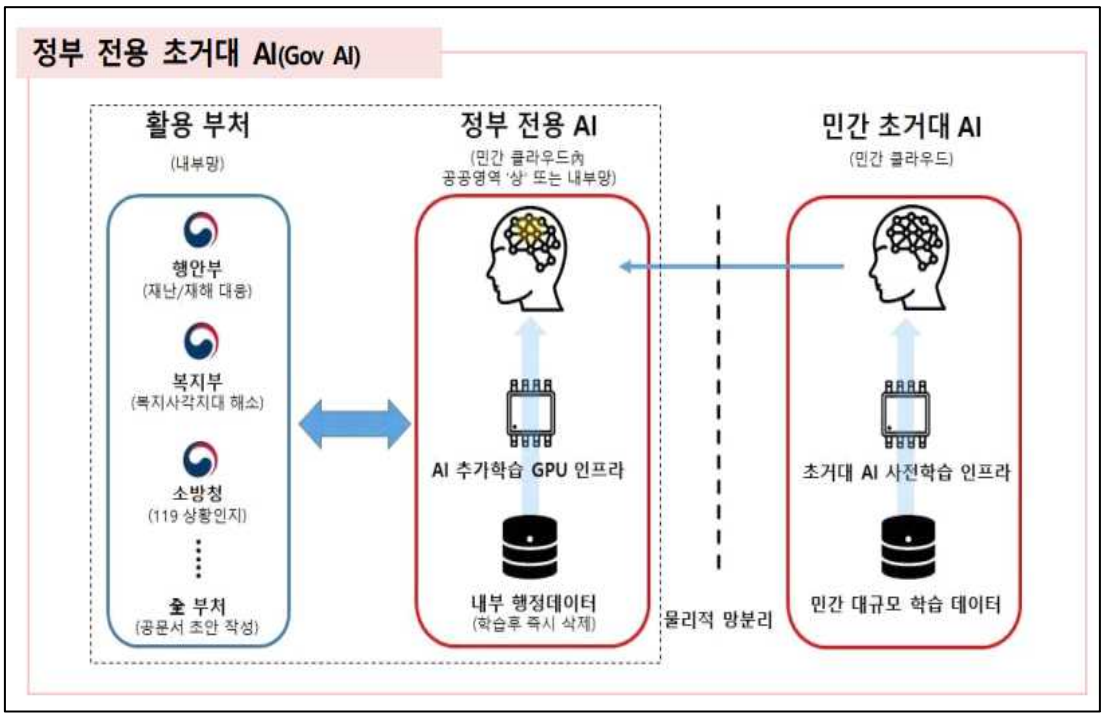
3.1. 클라우드 컴퓨팅 도입

3.1.1. 클라우드 컴퓨팅 도입 정책 개요

정부는 2021년「행정·공공기관 정보자원 클라우드 전환·통합 추진 계획」을 발표하여 코로나19 이후 급격하게 늘어난 디지털 수요를 해결하고자 했다. 정부는 행정기관 및 공공기관 정보자원 통합기준(행안부 고시, 20.6.16)에 따라 행정·공공기관 정보시스템을 공공클라우드 센터와 민간클라우드센터로 이원화 하는 계획을 통해 2025년까지 약 10,000여개의 정보시스템을 클라우드 기반으로 전환한다고 밝혔다.

[그림 Ⅲ- 1] 연도별 클라우드 전환계획(행정안전부)

2022년 윤석열 정부가 들어서면서 추진한 디지털플랫폼정부에서는 기존 행정·공공기관 정보자원 클라우드 전환·통합 추진 계획보다 더 강화된 클라우드 정책 계획이 수립되었다. 디지털플랫폼 정부 혁신 인프라를 구현하기 위해 정부기관 간, 정부와 민간 부분 간 연계·협업과 민간·공공의 데이터와 서비스 기능의 자유롭고 안전한 공유·활용할 수 있도록 클라우드 기반 통합플랫폼(가칭 ‘DPG 허브’)을 마련하기 위한 계획을 발표하였다. 이를 통해 최고 수준의 개인 맞춤형, 대화형 ‘AI 활용 인프라’를 마련하고, 정부 서비스 내 여러 기관이 공동으로 활용하는 ‘범부처 공용서비스 빌딩블록’을 구축을 목표로 하였다.



[그림 Ⅲ- 2] 초거대 인공지능 대화형 민원도우미 구성도

이번 발표된 계획에서는 GovTech 기업 성장을 지원하기 위해 공공부문에 민간 클라우드를 적극적으로 도입하는 공격적인 정책을 지원한다. 노후화 된 시도·시군구 시스템을 클라우드 기반의 지방행정공통정보시스템으로 재구축하여 지방자치단체 내 이원화된 행정시스템을 단일 시스템으로 전환한다.

지방 공공기관별 독자적으로 구축·운영되고 있는 행정정보시스템을 클라우드로 전환하며, 표준시스템을 구축·보급함으로써 시스템 구축 비용 절약, 정보자원(HW, SW)의 유지 관리 비용 절약 등 불필요한 경제적 손실을 절감한다.

인터넷 브라우저를 통해 최종 사용자에게 응용 소프트웨어를 제공할 수 있는 SaaS(서비스형 소프트웨어)의 도입·전환을 통해 글로벌 경제력 강화하고자 한다. 이를 위해 클라우드 서비스에 대해 관련 제도 개선, 디지털 서비스 전문 계약제를 통한 등록·심사 절차 간소화, ISP 제도 개선 등 다양한 정책을 진행한다.

3.1.2. 클라우드 컴퓨팅 정의 및 개요

클라우드 정책의 변화와 그에 따른 다양한 제도적인 정비도 이루어지고 있다. 정확한 정의가 어려운 최신 트렌드에 대한 정의에 대한 기준도 표준화되고 있다. 클라우드 컴퓨팅 시스템에 대한 정의도 비슷하다. 클라우드 보안에 대한 연구에 앞서 클라우드 컴퓨팅에 대한 정의 및 개요에 대해 확인해 보고자 한다.

클라우드 컴퓨팅은 2006년 구글 직원인 크리스토프 비시글리어(christophe Bisciglia)가 유휴 컴퓨팅 자원 대한 활용을 제안하면서 다양한 개념으로 사용되어 왔으며, 초창기 컴퓨팅 모델이 특정 장소에의 물리적 장치(HW)와 논리적 프로그램(SW)으로 이루어졌다면, 클라우드 컴퓨팅은 네트워크의 발달, 인터넷 확산 등으로 다양한 네트워크 컴퓨팅 연결이 가능해지면서 발생된 개념이다.

클라우드 컴퓨팅 개념에 대한 초기 당시의 개념은 [표 Ⅲ-1]과 같다.

[표 Ⅲ- 1] 클라우드 컴퓨팅에 대한 다양한 정의

기 관 명	정 의
NIST	이용자는 IT자원(소프트웨어, 스토리지, 서버, 네트워크)을 필요한 만큼 빌려서 사용하고, 서비스 부하에 따라서 실시간 확장성을 지원받으며, 사용한 만큼 비용을 지불하는 컴퓨팅
Gartner	인터넷 기술을 활용해 많은 고객들에게 수준 높은 확장성을 가진자원들을 서비스로 제공하는 컴퓨팅의 한 형태
Forrestet Research	표준화된 IT 기반 기능들이 IP로 제공되고, 언제나 접근이 허용되며, 수요변화에 따라 가변적이며, 사용량이나 광고를 기반으로 비용을 지불하고 웹 또는 프로그램적인 인터페이스를 제공하는 형태
IBM	웹 기반 응용 소프트웨어를 활용해 대용량 데이터베이스를 인터넷 가상공간에서 분산처리하고, 이 데이터를 컴퓨터나 휴대전화, PDA 등 다양한 단말기에서 불러오거나 가공할 수 있게 하는 환경
TTA	가상화와 분산처리 기술을 기반으로 인터넷을 통해 대규모 IT자원을 임대하고, 사용한 만큼의 요금을 지불하는 컴퓨팅 환경을 의미

각 기관마다 클라우드 컴퓨팅을 정의하는 개념은 조금씩 차이가 있으나, 기본적인 개념은 비슷하다. 네트워크의 발달과 가상화 기술을 활용하여 필요한 자원(서버, 스토리지, sw 등) 을 직접 구축하지 않고, 임대해서 사용할 수 있는 시스템을 말한다고 볼 수 있다. 클라우드 컴퓨팅 환경과 기존 환경과의 차이는 [표 Ⅲ- 2]와 같다.

[표 Ⅲ- 2] 클라우드 컴퓨팅과 기존 컴퓨팅 환경과의 차이

대 상	기존 환경	클라우드 환경	특 징
서버	IT 자원 개별 구축·운영	IT 자원 통합 구축·운용	중앙집중화
	물리적 서버 단위 이용	논리적 서버 단위 이용	신속한 서버자원 추가
	서버별 운용 환경 상이	동일 서버 운용 환경 제공	서버 보안정책 반영 용이
소프트웨어	사무실의 PC 등 고정장소	장소 이동 가능	중앙집중화
	물리적 PC에 설치 후 이용	서비스 단위 이용	신속한 자원 추가
	개인 PC 운용 환경 상이	동일 서비스 환경 제공	정책반영 용이

클라우드 컴퓨팅은 서비스의 형태에 따라 분류하면 인프라제공서비스(IaaS), 플랫폼 제공 서비스(PaaS), 소프트웨어 제공 서비스(SaaS)의 세 가지로 분류되며 최근에는 두 가지 이상 복합하여 서비스를 제공하는 형태도 등장하고 있다.

인프라제공서비스(IaaS) 클라우드 컴퓨팅의 구성 요소 중 서버, PC, 스토리지, 네트워크 등 인프라를 구성하는 자원을 서비스 형태로 활용한다.

플랫폼 제공 서비스(PaaS)는 웹 애플리케이션 개발을 위한 플랫폼 자원을 가상 환경에서 이용할 수 있도록 하는 서비스를 말한다.

소프트웨어 제공 서비스(SaaS)는 웹오피스, 화상 회의 등 다양한 소프트웨어를 별도 구매・설치하지 않고 서비스 형태로 제공받는 형태를 말하며, 최근 디지털 플랫폼 정부에서는 공공부분 정보시스템을 SaaS 형태로 확대・구축 운영해 나갈 예정이다.

각각의 서비스를 복합한 클라우드 서비스를 제공하는 사례가 증가하고 있으며, 이를 복합 서비스라고 하며, 주요 사례로는 별도의 PC나 SW를 구매하지 않고, 가상 PC와 소프트웨어를 제공하는 DaaS(Desktop as a Service) 서비스가 있다.

3.1.3. 공공기관 클라우드 컴퓨팅 서비스 도입 절차 및 방법

1) 클라우드 컴퓨팅 도입 규정

디지털플랫폼정부에서는 행정·공공기관의 정보시스템 도입 및 전환 시 관련 법률에 따라 클라우드 컴퓨팅 서비스를 고려해야 하며, 특히 상용 SaaS를 도입할 수 있는지 여부를 검토하도록 규정하고 있다.

이는 민간이 클라우드 서비스를 제공하고 공공은 서비스 이용료를 지불하는 방식으로 민간 클라우드를 활성화하기 위한 방식이며, 이를 뒷받침하기 위해 행정기관에서의 클라우드 도입을 위한 다양한 제도적 정비가 지속적으로 시행되고 있으며 이에 따른 관련 근거는 아래와 같다.

- 「전자정부법」 제54조 및 제54조2(클라우드컴퓨팅서비스의 이용)
- 「클라우드컴퓨터팅 발전 및 이용자보호에 관한 법률(이하 ‘클라우드 컴퓨팅법’」 제12조(국가기관등의 클라우드컴퓨팅 도입 촉진) 및 제20조(국가기관등의 클라우드컴퓨팅서비스 이용 촉진),
- 「클라우드컴퓨팅법 시행령」 제8조의2(디지털서비스의 선정 등)
- 「국가를 당사자로 하는 계약에 관한 법률 시행령」 제26조(수의계약에 의할 수 있는 경우)
- 「정부 입찰·계약 집행기준」 제16장의3 디지털서비스 계약의 집행
- 「행정기관 및 공공기관의 클라우드컴퓨팅서비스 이용기준 및 안전성 확보 등에 관한 고시」
- 「행정기관 및 공공기관 정보자원 통합기준」
- 「행정기관 및 공공기관의 클라우드컴퓨팅서비스 이용기준 및 안전성 확보 등에 관한 고시(이하 ’ 클라우드컴퓨팅서비스 이용기준 ‘)」
- 「사이버안보 업무규정」
- 「국가 클라우드 컴퓨팅 보안 가이드라인」
- 「행정기관 및 공공기관 정보시스템 구축·운영 지침」

2) 클라우드 컴퓨팅 관련 용어

또한, 다양한 제도에 따른 사용자들의 혼란을 최소화하기 위해서 용어에 대한 표준화를 지속해 나가고 있으며, 이에 따른 주요 내요은 표 [Ⅲ-3] 과 같다.

[표 Ⅲ- 3] 클라우드 컴퓨터 용어

<table>
<tr><th colspan="3">용어</th><th>용어정의</th></tr>
<tr><td colspan="3">클라우드컴퓨팅
(Cloud Computing)</td><td>집적·공유된 정보통신기기, 정보통신설비, 소프트웨어 등 정보 통신 자원(이하 "정보통신자원"이라 한다)을 이용자의 요구나 수요 변화에 따라 정보통신망을 통하여 신축적 으로 이용할 수 있도록 하는 정보처리체계</td></tr>
<tr><td colspan="3">클라우드컴퓨팅기술</td><td>클라우드컴퓨팅의 구축 및 이용에 관한 정보통신기술로서 가상화 기술, 분산처 리 기술 등 대통령령으로 정하는 것을</td></tr>
<tr><td colspan="3">클라우드컴퓨팅서비스</td><td>클라우드컴퓨팅을 활용하여 상용(商用)으로 타인에게 정보통신자원을 제공하는 서비스로서 대통령령으로 정하는 것을 말한다.</td></tr>
<tr><td colspan="3">이용자 정보</td><td>클라우드컴퓨팅서비스 이용자(이하 "이용자"라 한다)가 클라우드컴퓨팅서비스를 이용하여 클라우드컴퓨팅서비스를 제공하는 자(이하 "클라우드컴퓨팅서비스 제공자"라 한다)의 정보통신자원에 저장 하는 정보(「지능정보화 기본법」 제2조제1호따른 정보를 말한다)로서 이용자가 소유 또는 관리하는 정보</td></tr>
<tr><td rowspan="3">클라우드컴퓨팅 서비스 도입 방법</td><td colspan="2">신규구축</td><td>기존에 없는 시스템을 새로 구축할 때 클라우드컴퓨팅서비스를 이용하여 구축</td></tr>
<tr><td rowspan="2">교체</td><td>전환</td><td>기존 서비스 환경을 클라우드컴퓨팅서비스 기반으로 전환</td></tr>
<tr><td>재 구축</td><td>클라우드컴퓨팅서비스가 기존 운영체계를 지원하지 않는 등 직접 전환할 수 없는 경우, 시스템을 클라우드컴퓨팅서비스 환경에 맞도록 재설계하는 등의 방법으로 전환</td></tr>
<tr><td colspan="3">응용프로그램(AP)</td><td>운영체제(OS)기반에서 대국민 서비스 또는 내부행정 서비스를 제공하기 위해 개발된 소프트웨어를 말함</td></tr>
<tr><td colspan="3">클라우드컴퓨팅서비스 환경</td><td>클라우드컴퓨팅서비스 제공을 위한 가상의 자원 및 네트워크 보안 등 서비스가 적용된 환경</td></tr>
</table>

용어	용어정의
CSP 사업자 (Cloud Service Provider, 클라우드컴퓨팅서비스 사업자)	「클라우드컴퓨팅법」제2조 제4호에 따라 클라우드컴퓨팅서비스를 제공하는 민간 기업 또는 단체
MSP 사업자(Managed Service Provider)	클라우드컴퓨팅서비스 도입 및 전환에 필요한 컨설팅, 마이그레이션, 운영서비스 등을 지원하는 민간 기업 또는 단체
CSAP(CloudSecurity Assurance Program, 클라우드 보안인증)	과학기술정보통신부장관이 고시한 「클라우드컴퓨팅서비스 정보보호에 관한 기준」제7조에 따라 한국인터넷진흥원의 장이 클라우드컴퓨팅서비스의 보안성에 대하여 실시하는 인증
3rd Party 소프트웨어 (3rd Party S/W)	• 응용프로그램(AP)에서 사용되는 제3자가 공급하는 S/W • 클라우드 교체 시, 환경 변화에 따른 커스터마이징이 필요하거나, 추가 라이선스 구매 등 비용이 발생할 수 있음
디지털서비스 이용지원시스템	클라우드컴퓨팅법 시행령」 제8조의2 제3항에 따라 디지털서비스를 등록 및 관리 하는 시스템

*자료출처: 행정·공공기관 클라우드 컴퓨팅 서비스 이용안내서 재편집

3) 클라우드 컴퓨팅 도입 절차

정부는 ” 행정기관 및 공공기관의 클라우드컴퓨팅서비스 이용기준 및 안전성 확보 등에 관한 고시 “ 제정(이하 ’ 클라우드컴퓨터서비스 이용기준 ‘)을 통해 공공기관의 민간 클라우드 우선 이용 정책을 제도화하였으며, 2022년 공공부문 클라우드 기술선도 프로젝트를 진행하였다. 해당 프로젝트는 정부 및 지자체 등이 민간 클라우드 이용을 우선 검토하고, SaaS 적용가능한지 확인해야 하며, 적정한 SaaS가 부재한 경우, 플랫폼 클라우드 서비스(PaaS) 기반의 클라우드 네이티브 서비스 구현을 하도록 하고 있다. 이에 따른 도입 절차는 [그림 Ⅲ- 4] 와 같다.

[그림 Ⅲ- 4] 클라우드 컴퓨터서비스 이용 단계 및 절차

4) 클라우드 컴퓨터 도입 유형

국가정보원에서는 2023. 1월 시스템 중요도를 재분류하고 클라우드 영역별 보안 기준을 추가한 ’ 국가 클라우드 컴퓨터 보안 가이드라인 ‘를 개정하여, 공행정・공공기관이 클라우드 컴퓨팅 도입하는 유형에 대한 분류를 하였다. 총 6가지로 분류하였으며, 그 유형은 [표 Ⅲ- 4] 와 같다.

① 기관 구축・이용(On-site Private)은 독립된 네트워크를 사용하고, 기관 내부망과 외부망 사이에 정보보호시스템 구축과 암호화 통신 등의 장치가 필요하다

② 기관 구축・커뮤니티 이용(On-site Community) 방식은 공공기관 중 동일 네트워크를 사용하는 기관 간 클라우드의 독자적인 구축・관리가 론란 한 경우를 말하며, 기관 간 접근 통제를 허용하는 방식이다.

③이용 외주(Out-sourced)방식은 클라우드 환경을 자체 구축하는 것이 비효율적이고, 관리가 어려운 경우 사용하며, 공공영역과 민간 영역이 분리되도록 구축한다.

④ 하이브리드(Hybrid) 유형은 보안 수준이 높은 데이터에 대해서는 공공기관에서 운영중인 정보시스템을 유지하고, 그 외의 데이터에 대해서는 민간 클라우드 서비스를 사용하는 방식이다. 이 때는 기관 내부망과 민간 클라우드 사이의 자료 교환・연계 등을 위한 솔루션 및 정보보호 시스템 구축이 요구된다.

⑤ 멀티 클라우드(Multi Cloud) 방식은 다수의 민간 클라우드를 연계하여 활용하는 방식이며 인프라(IaaS)를 연계한 클라우드 서비스(PaaS, SaaS)를 활용할 수 있다.

[표 Ⅲ- 4] 국가·공공기관 클라우드 컴퓨팅 구축 유형

용어	용어정의
① 기관 구축·이용 (On-site Private)	o 기관이 자체 구축하고 직접 관리하며, 독립된 네트워크를 사용 o 기관이 클라우드 자원 통제권 보유 o 다른 기관과의 자원 공유 없음,
② 기관 구축· 커뮤니티 이용 (On-site Community)	o 기관이 자체 구축하고 직접 관리 o 기관이 클라우드 자원 통제권 보유 o 커뮤니티에 속한 기관 간 클라우드 자원 공유 o 커뮤니티 외부 기관과의 자원 공유 없음
③이용 외주 (Out-sourced)	o 다수 기관이 공공 영역을 공동 임차 o 기관이 클라우드 자원 통제권 미보유 o 공용 영역 내 기관들과의 자원 공유
④ 하이브리드 (Hybrid)	o 기관 내부 정보시스템과 기관 외부의 외주 클라우드를 연계하여 활용 o 기관과 클라우드 제공자 간 클라우드 자원통제 공유 o 다른 기관과의 자원 공유 없음
⑤ 멀티 클라우드 (Multi Cloud)	o 기관이 다수의 상용 클라우드를 연계하여 활용 o 기관이 클라우드 자원 통제권 미보유
⑥ 공개 클라우드 (Public Cloud)	o 상용 클라우드 서비스를 활용 o 기관이 클라우드 자원 통제권 미보유 o 모든 기관 또는 사용자와 자원

3.2. 클라우드 컴퓨팅 보안 정책 연구

3.2.1. 보안 정책의 변화

클라우드 컴퓨팅 시스템 도입으로 인해 비용 절감, 물리적 접근 강화, 가상 머신 부하 분산 기능 등 다양한 장점이 있지만 그에 못지 않은 단점도 존재한다. 클라우드 컴퓨팅 환경에서는 데이터의 중앙 집중화에 의해 보안 사고 발생 시 대량 데이터 유출 등의 사고가 발생할 수 있다. 특히, 2021년 발생한 러시아와 우크라이나 전쟁 이후 각 정부 웹사이트와 금융기관, 행정기관을 상대로 다양한 디도스 공격과 웹변조 공격이 이루어지고 있다. 군사력을 동원한 물리적 충돌은 여전하지만, ICT 기술을 활용한 최첨단 무기들과 위성통신을 활용한 위치 정보 활용 등이 증가됨에 따라 사이버공격에 대한 위력이 날로 강화되고 있다.

2021년 한국원자력연구원 자료 해킹과 관련해서 그 배후 세력으로 북한이 지목되고 있으며, 국가 주요기반산업에 대한 국가 배후의 해킹 및 보안 침해는 어느 하나의 시스템에 대한 단순한 피해가 아닌 국가 전체적인 위협으로 다가오고 있다.

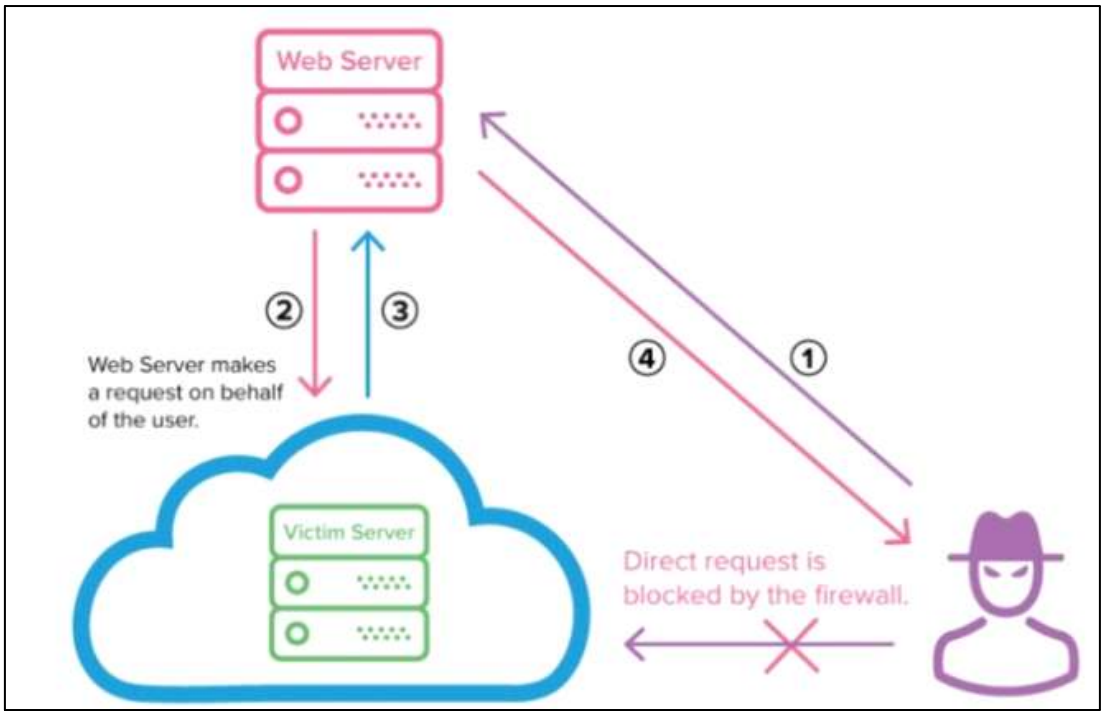
클라우드 컴퓨팅 환경에서는 기존 정보시스템 환경에서 존재하는 다양한 보안 위협과 클라우드 컴퓨팅 환경에서의 보안 위협 등이 복합적으로 나타날 수 있으며, 그 유형은 [표 Ⅲ- 5] 와 같다.

[표 Ⅲ- 5] 클라우드 보안 위협 예시

클라우드 컴퓨팅 환경 구성요소	보안 위협 예시	
가상환경	- 악성코드 감염 - SaaS 애플리케이션 취약점 - 인터페이스 및 API 취약점 - 가상자원 격리 위협 - App 데이터 변조	
클라우드 인프라	설비	- 물리적 위협(화재, 정전 등)
	하드웨어	- QoS - DDos - Flood Attack - 네트워크 장비 설정 오류
	가상화 인프라	- Multi-Tenancy(다중임차) - 공유 위협 - 솔루션 설정 오류
정책	- 규정/법 미준수 - SLA 위반 - 인적 보안 - 용역 관리	
사고 및 장애 대응	- 동일 사고 재발생 - 백업/복원 실패 - 사고 후 운영 실패	
인증 및 권한	- 계정 탈취 - 권한 상승/오용 - 내부자 위협 - 단말 보안	
데이터	- 데이터 유출/파괴 - 데이터 위치(사법관할권) - 데이터 안전정서(백업 및 복원 - 쉐도우 데이터(Shadow data)	

1) 전통적 방식에 의한 해킹

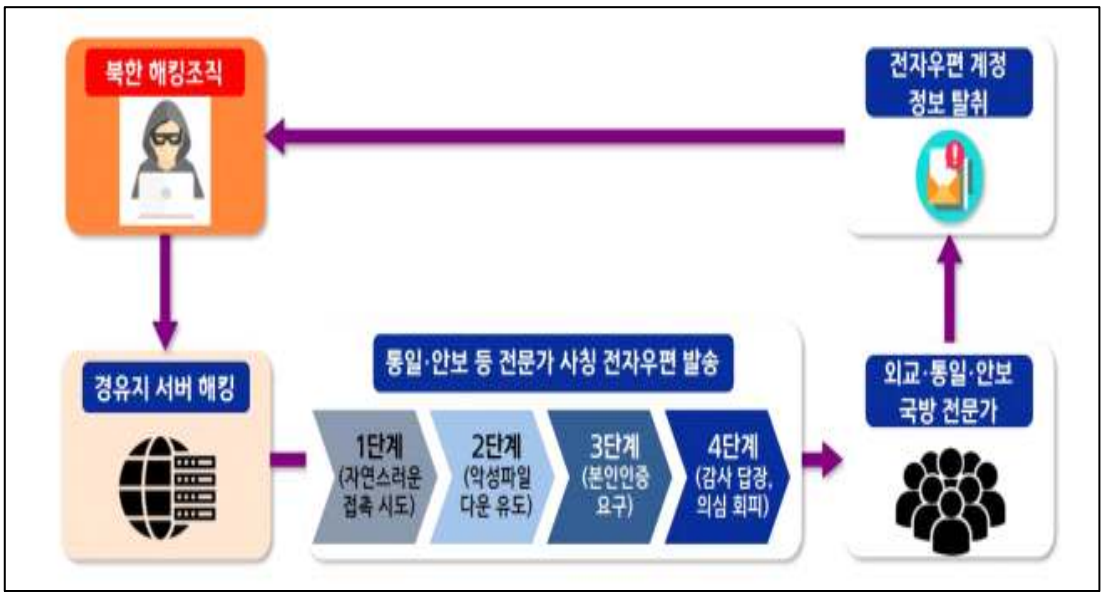
기본 정보시스템에 대한 해킹 방식은 다양하다. 전통적 방식에 의한 해킹 중 첫 번째 방식은 웹 보안 취약점을 악용한 해킹 사례이다. 2019년 7월 미국의 대형은행 ' 캐피털원(capital one) '에서는 해커들에 의해 웹 방화벽 취약점을 뚫고 아마존(Amazon) 클라우드인 AWS에 저장된 신용 카드 고객 정보가 해킹 당하는 사건이 발생했다. 해커들은 캐피털 원이 AWS에 설치하여 사용하고 있는, open-source WAF(Web Application Firewall)의 설정이 잘못된 것을 이용하여, AWS 상에 저장된 캐피털 원의 고객 데이터에 접근하였다, 해커들은 탐지되는 것을 피하기 위하여, Tor(토르) 브라우저를 사용하고, Private VPN 통해 AWS에 접근하였으며, SSRF(Sever Side Request Forgery) 취약점을 통해 정보를 해킹하였다. SSRF(Sever Side Request Forgery) 해킹 방식은 [그림 Ⅲ- 5]과 같다.



[그림 Ⅲ- 5] SSRF(Sever Side Request Forgery) 해킹 방식

*자료출처 : www.netsparker.com 의 blog, 작성자 AEP코리아네트

두 번째로는 이메일을 활용한 피싱 해킹 사례이다. 최근 2023년 공개된 '사이버 안보 분야 한미정부 합동주의소 북한 김수키 조직의 싱크탱크.학계. 미디어 대상 사회공학적 기법을 악용한 해킹 공격' 사례에서 보듯이 해커들은 전문가의 의견을 묻거나, 사회적 이슈에 대한 캠페인으로 위장, 유명 포털 사이트로 위장하는 방식을 사용한다. 메일에 첨부된 대용량 문서 파일을 다운로드하고, 신뢰성을 위해 암호화 조치를 하였다는 위장 메시지를 통해 사용자가 문서 확인을 위한 본인 인증을 위한 피싱 사이트 접속을 유도하여 정보를 탈취하며, 주요 방식은 [그림 Ⅲ- 6]과 같다.



[그림 Ⅲ- 6] 이메일 악용 공격 수법 사례

*자료 출처 :https://www.datanet.co.kr/news/articleView.html?idxno=184937

2) 물리적 위협에 의한 사고

2014년 삼성 SDS 과천 데이터 센터 화재 사고, 2018년 서울 KT 아현지사 화재 등으로 많은 피해가 발생하였다. 삼성 SDS 과천 데이터 화재 사고는 약 1,069억원, 서울 KT 아현지사의 피해액으로 약 80억원으로 추정된다.

물리적 위협(화재)에 의한 클라우드 사고는 물적 피해 뿐만 아니라 사회적 파장도 적지 않다. 그 대표적인 것이 2022년 10월 발생한 카카오 SK 판교데이터센터 화재로 인한 서비스 장애 사고이다. 국민 메신저라고도 불리는 카카오는 카카오 게임, 카카오 택시 등을 포함한 카카오 모빌리티, 카카오엔터테이먼트 등의 서비스에 약 3000만 여명이 가입되어 있으며, 데이터 센터 화재로 인해 신고된 피해 사례만도 약 8만 7,000여건으로 집계되었으며, 이로 인해 피해 보상 규모는 275억원으로 집계되었다.

3) 인적 자원에 의한 보안 사고

전통적 방식에 의한 해킹 사고와 물리적 위협에 의한 사고보다 인적 자원(내부자)에 대한 사고가 지속적으로 증가하고 있다. 국가통계포털(KOSIS)의 ” 우려하는 개인정보 유출요인 “ 에 대한 통계 조사를 살펴보면 외부로부터의 해킹 사례는 점점 감소하고 있으나, 관리 실수로 인한 유출과 내부자에 의한 유출의 비중이 점점 증가하고 있다.

[표 Ⅲ- 6] 우려하는 개인정보 유출 요인 분석

구분	외부로부터 해킹	관리실수로 인한 유출	내부자에 의한 고의 유출	외주(아웃소싱) 업체에 의한 유출
2016	72.2	70.0	32.9	9.1
2017	77.4	73.6	33.4	11.7
2018	81.0	77.9	30.9	7.3
2019	64.1	76.0	42.8	10.8

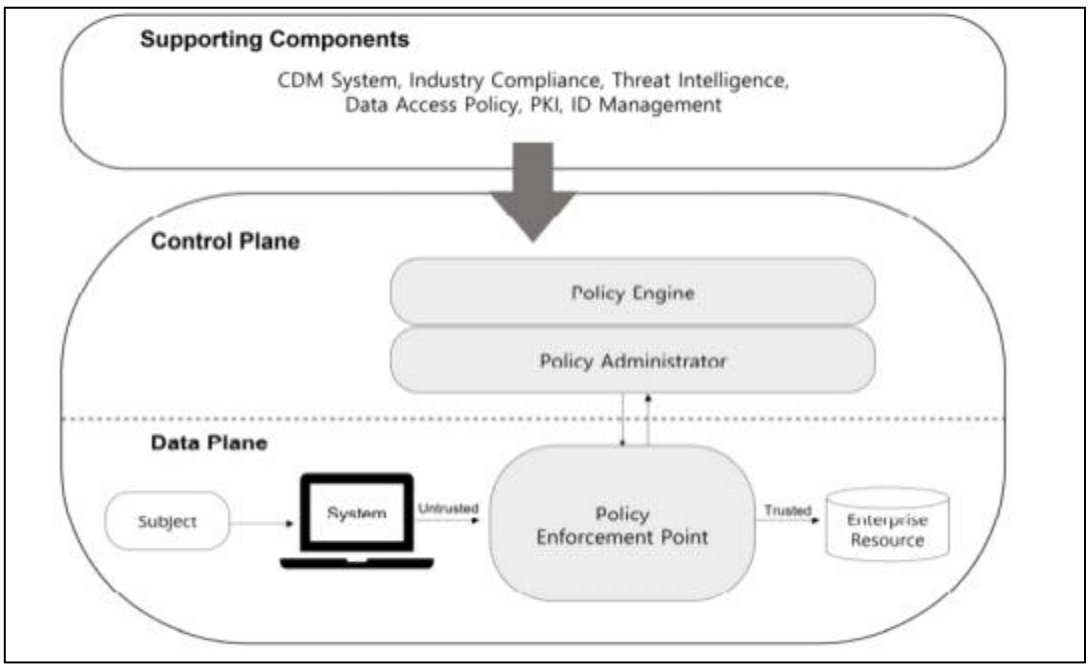
4) 제로 트러스트(Zero-Trust)의 등장

제로 트러스트(Zero-Trust)는 내부 사용자에 대한 보안 사고가 증가함에 따라 네트워크를 통한 접근자에게 최소한의 접근 권한을 부여한다는 개념으로 클라우드 서비스에 접근하는 모든 기기와 사용자에 대해 신뢰하지 않음을 나타낸다.

고전적인 방식에서의 외부 네트워크에서 내부 네트워크로의 접근 통제는 방화벽, 침입 탐지 시스템(IDS, Intrusion Detection System) 침입 방지시스템 (IPS, Intrusion Prevention System,), 가상 사설망(VPN) 등 보안 장비와 프로그램으로 통제한다.

그러나, 클라우드 컴퓨팅 시스템은 다양한 디바이스와 네트워크(장소)에서 접속이 가능하기 때문에 기존 외부에서의 차단과 더불어 내부에서의 보안 정책이 필요한 시점이다.

제로 트러스트 보안 정책은 비인가 사용자에 대한 접근 차단 뿐만 아니라, 인가 받은 사용자 또는 디바이스의 클라우드 시스템 접속에 대한 정확하고 검증 및 최소 권한만을 허용함으로써 허가된 사용자에 대한 집중적이고 지속적인 감시를 수행한다.

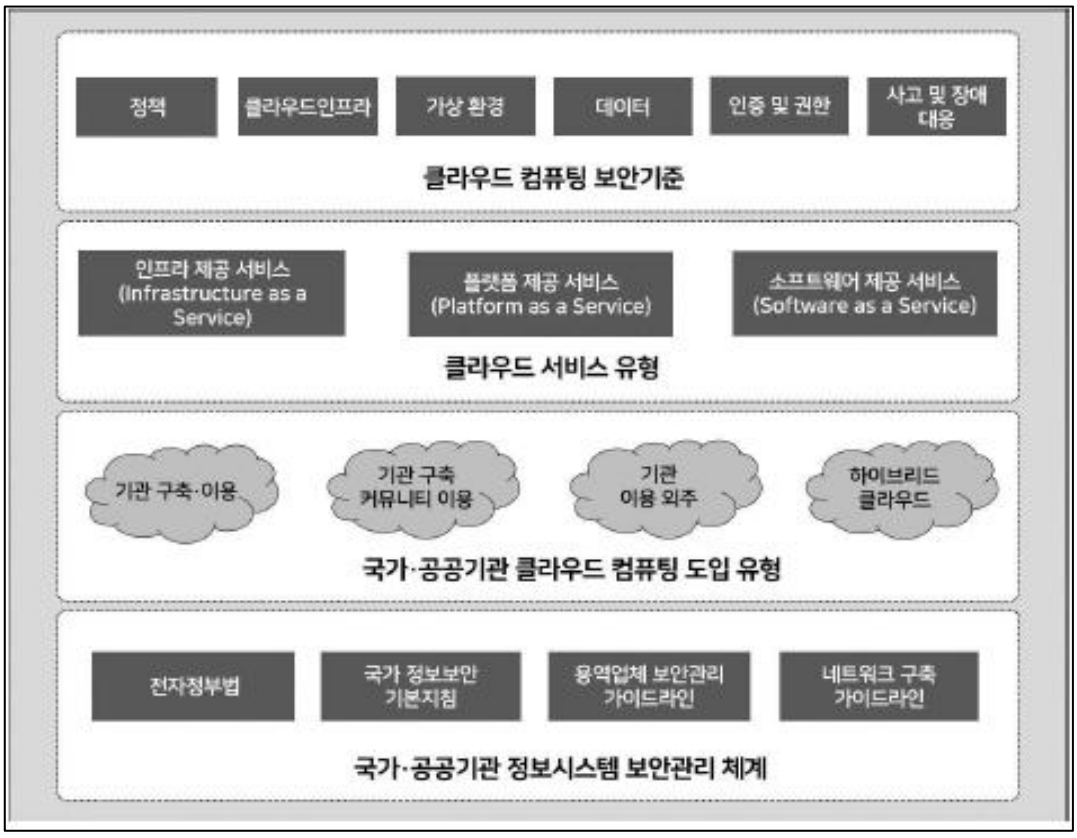


[그림 Ⅲ- 7] 제로 트러스트 개념도

3.2.2. 클라우드 컴퓨팅 도입 시 보안 기준

클라우드를 행정기관에 도입하기 위한 절차는 앞선 선행연구에서 살펴보았다. 클라우드 도입에 따른 제도적 장치와 그에 따른 준수 사항이 광범위하기 때문에 업무 수행에 많은 어려움을 가지고 있는 것도 사실이다.

이에 따라 국가정보원에서는 「국가 클라우드 컴퓨팅 보안 가이드라인(2023. 1)」을 통해 보안 공공기관에서의 클라우드 컴퓨팅 도입 시 보안 기준을 마련하였다. 앞서 살펴본 클라우드 도입 5가지 유형을 크게 기관 자체 클라우드 컴퓨팅 보안 기준과 민간 클라우드 컴퓨팅 서비스 이용 시 준수하여할 보안 기준으로 설정하였으며, 그 개념도는 [그림 Ⅲ- 8]와 같다.



[그림 Ⅲ- 8] 국가・공공기관 클라우드 컴퓨팅 도입 보안체계

1) 기관 자체 클라우드 컴퓨팅 구축 보안 기준

- 정책적 측면에서의 기본원칙

기관 자체 클라우드 컴퓨팅 구축은 기관에서 자체적으로 클라우드 컴퓨팅 시스템을 구축하여 클라우드 자원에 대한 통제권을 가지기 때문에 기존 구축된 정보시스템 시스템에 대한 보안 기준 뿐만 아니라 클라우드 컴퓨터 구축에 따른 보안 기준을 마련하여야 한다.

이를 위해서는 국가·공공기관 활용 클라우드 영역 분류 방법과 시스템 중요 분류 및 기준 및 절차에 따라 클라우드 영역을 분리하고, 도입되는 정보보호시스템에 대한 안정성 확인을 반드시 해야 한다.

클라우드 영역을 통해 내부 업무용 영역과 외부 공개용 클라우드 컴퓨팅 서비스 사용 영역을 분리하여야 하며, 인터넷·업무망의 분리를 통한 영역 간 데이터 교환을 차단하고, SaaS 클라우드 인프라, 개발·운영 환경의 물리적 위치와 데이터의 위치는 국내로 한정해야 한다.

클라우드 인프라 환경에 대한 보안성 확인 및 SaaS 개발·운영 환경은 SaaS 서비스 가용성을 보장해야 한다.

클라우드 컴퓨팅 서비스의 사용자와 관리자를 지정하여 책임과 관리에 관한 보안 책임 영역을 별도로 지정한다. 특히 퇴직 및 직무 변경의 상황에 따른 접근 권한 관리를 통해 비인가자에 대한 클라우드 접속을 차단하고, 각 영역별 정보보호 교육을 주기적으로 진행한다.

로그인 기록(단말 PC IP, 사용자 ID, 시간, 작업내용), 데이터 접근(다운로드, 수정, 작성), 관리자 권한으로 실행한 기능 등의 로그 기록을 1년 이상 보관·보호할 수 있는 시스템을 마련하여야 한다.

- 기술적 측면에서의 원칙

비공개 업무용과 인터넷, 홈페이지, 대민 서비스 등 외부 공개용 클라우드 영역의 분리와 중요자산(가상머신, 스토리지 등)에 대해 이중화를 구성하고, 백업체계를 구축하여야 한다.

관리자 및 이용자의 권한을 다양화하고, 업무 자료에 대한 암호화 조치를 진행한다. 해킹 탐지 및 대응체계 마련을 위한 보안 관제 시스템을 구축하여야 하며, 국가정보원의 클라우드 보안 관제 가이드 라인 기준을 준수하여야 한다.

유지보수 인력에 대한 보안 서약서 집행, 보안 교육, 작업 수행 내용 등을 기록관리하고, 지정된 장소에서의 접속을 진행하도록 해야 한다.

특히, SaaS 애플리케이션 개발 시에는 안전하고 다양한 인증 방안을 마련하고, 접근 권한에 따른 차등된 정책이 적용되도록 한다. SaaS에 대한 감사 기록을 관리·보호하고 주기적인 취약점 점검 및 보안패치를 실행한다.

클라우드 시스템에 대한 이동식 저장매체 등의 접근을 제한하고, 사용자 계정에 대한 관리 지침을 수립한다.

2) 민간 클라우드 컴퓨팅 서비스 이용 보안 기준

민간 클라우드 컴퓨팅 서비스 이용은 민간 사업자가 제공하는 클라우드 컴퓨팅 서비스를 기관이 이용하는 형태로 디지털플랫폼 정부에서의 추진하는 전략이다.

- 정책적 측면에서의 기본 원칙

민간 클라우드 컴퓨팅 서비스를 이용하는 경우에도 관련 법령에 따른 시스템 중요도 등급 분류 및 클라우드 영역 분류를 진행해야 하며, 클라우드 시스템 및 데이터의 물리적 위치는 국내로 한정해야 한다.

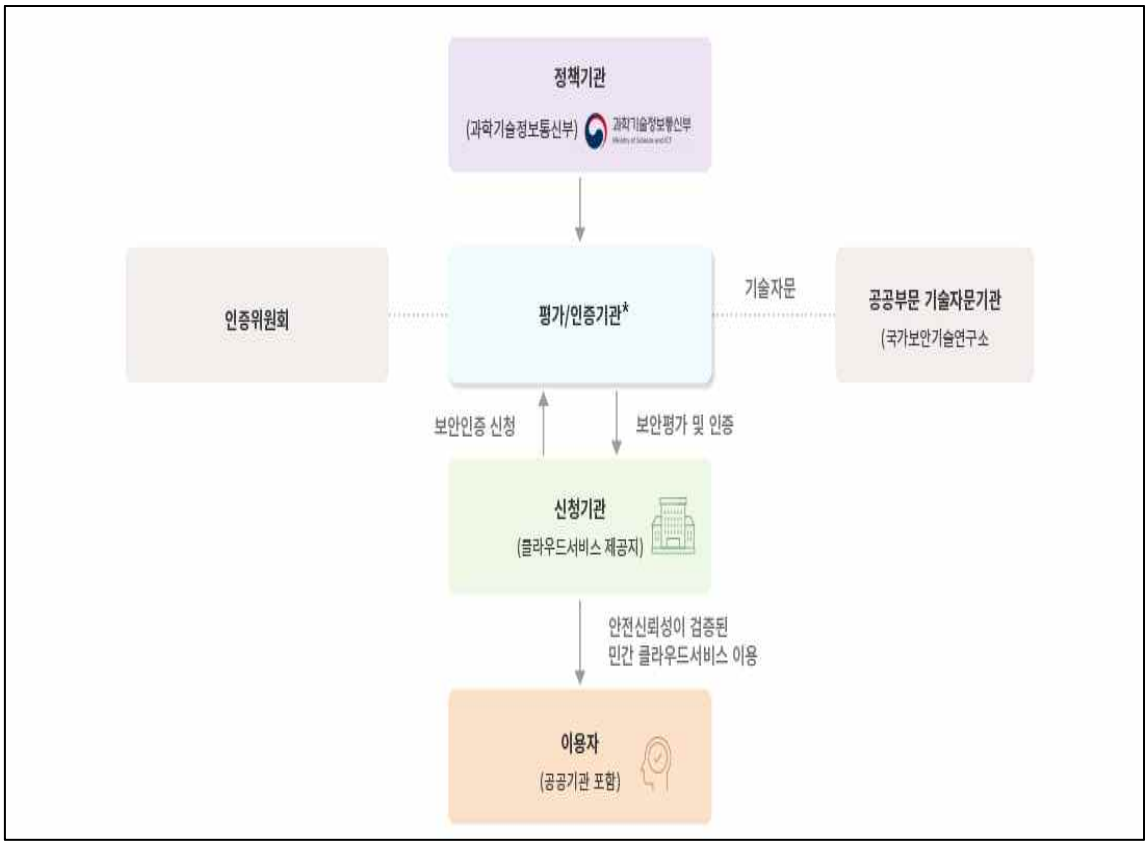
반드시 국가정보원이 보안적합성 검증제도(cc 검증)를 통해 도입 요건을 확인한 민간 클라우드 서비스를 이용하여야 하며, 클라우드 운영·이용에 대한 보안 관리 책임은 이용기관(공공기관)에, 클라우드 서비스 제공자(CSP 사업자, Cloud Service Provider / MSP 사업자(Managed Service Provider)와 기관의 보안 관리체계를 반영하는 보안 서비스 수준 협약(SLA)을 통해 책임의 소재를 명확하게 해야 한다.

- 기술적 측면에서의 기본 원칙

기술적인 측면에서의 원칙은 기관 구축 클라우드 컴퓨팅 서비스와 비슷하다. 업무망·인터넷 망과의 분리, 중요 자산 이중화 및 백업시스템 구축, 관리자 및 이용자에 대한 접근 권한 및 통제 수단 마련 등이 필요하며, 클라우드에 저장되거나 송수신 되는 모든 데이터에 대해서는 암호화·복호화를 할 수 있어야 한다.

3) 클라우드 컴퓨팅 서비스 보안인증 제도(CSAP)

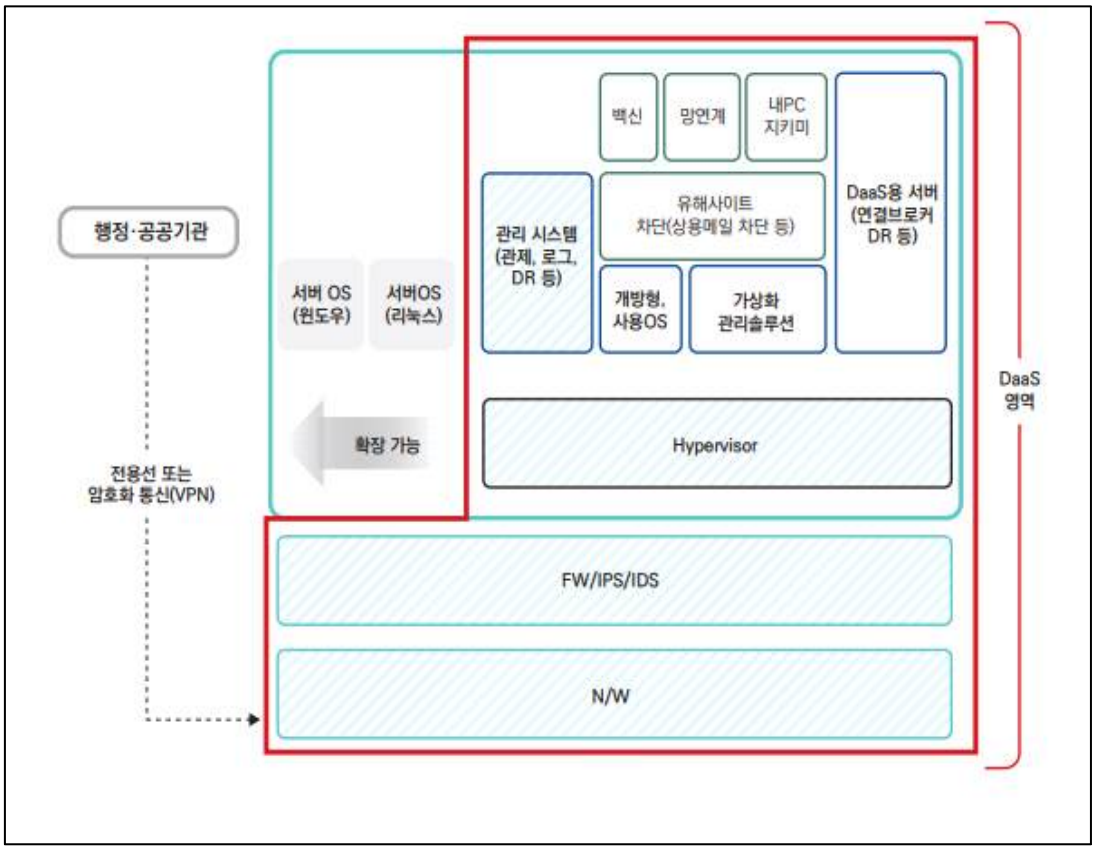
민간 클라우드 컴퓨팅 서비스 이용시 가장 큰 고려사항은 보안성과 신뢰성이다. 대용량 데이터 관리에 따른 기술적·인적 능력 외에도 해당 서비스 제공자가 신뢰성이 있는지에 대한 평가가 반드시 이루어져야 한다. 이를 위해서 과학기술정보통신부에서는 한국인터넷진흥원을 통해 클라우드 컴퓨팅 서비스 사업자자 제공하는 서비스에 대한 정보보호 기준의 준수여부를 평가하고 인증하는 제도(클라우드 컴퓨팅 서비스 보안인증 제도(CSAP, Cloud Security Assurance Program)를 시행하고 있으며, 관련 절차는 [그림 Ⅲ- 9]과 같다.



[그림 Ⅲ- 9] CSAP 인증 체계

*자료 출처: 한국인터넷진흥원

인증대상은 클라우드 컴퓨팅 기술을 이용하여 정보시스템의 인프라(IaaS), 응용프램(SaaS), 개발 환경(PaaS) 중 어느 하나 이상을 제공하는 클라우드 서비스 제공 사업자이며, 클라우드 서비스에 포함되거나 관련 있는 모든 자산(서버, 네트워크, 응용프로그램, 단말기 등), 인적자원, 지원서비스 등이 모두 포함된다.



[그림 Ⅲ- 10] DaaS 보안인증 대상 확인

3.3. 제로 트러스트(Zero-trust)

3.3.1. 제로 트러스트 개요

제로 트러스트(zero-trust)의 개념에 대해서는 앞장에서 간략하게 살펴보았다. 제로 트러스트 보안 개념은 기존의 보안 자원을 통해 물리적·논리적으로 분리된 네트워크 경계를 설정하여 신뢰할 수 있는 영역과 신뢰하지 못하는 영역을 분리하던 방식에서 벗어나 시스템에 접근하는 모든 사용자나 디바이스에 대한 검증을 통해 업무 권한을 부여하는 구조를 말한다. 즉, '신뢰하는 검증' 방식에서 '어떤 것도 신뢰하지 않고 전부·항상 검증' 하는 방식으로의 변화된 형태를 말한다.

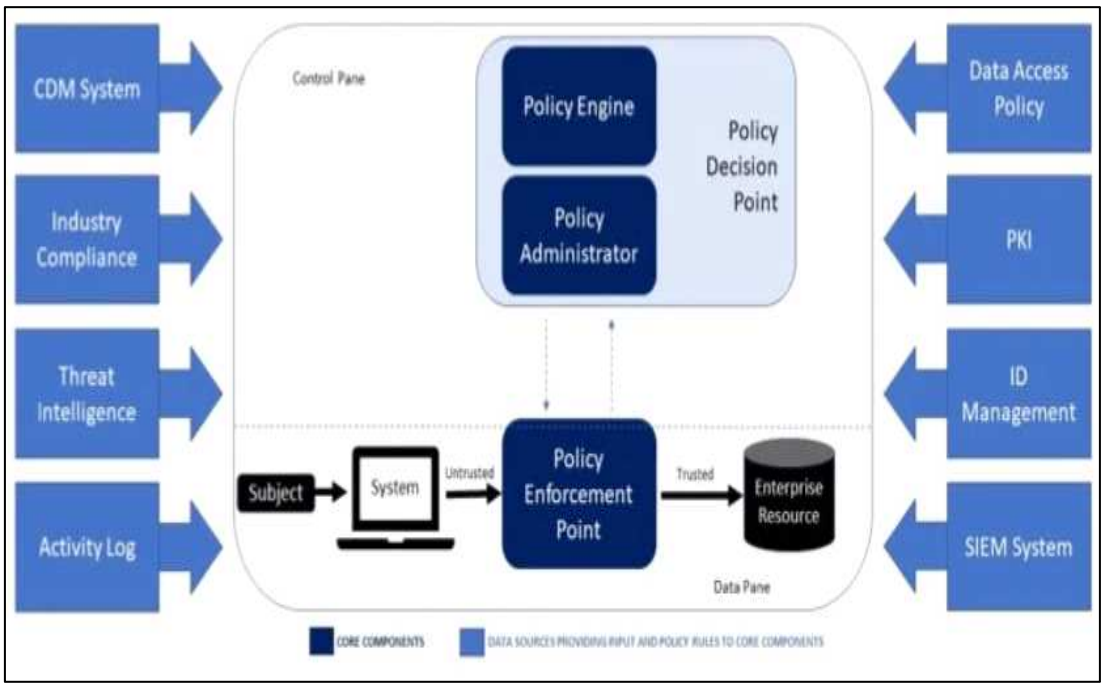
특히, 정보시스템의 클라우드 컴퓨팅 방식으로 전환·신규 구축, 코로나 19 이후에 원격 근무의 증가, 워케이션(workation)의 문화 확산으로 정보시스템의 접근 방식이나 물리적 위치에 변화가 많아졌다.
이에 따라 물리적으로 네트워크 경계 설정이 점점 어려워지고, 내부 사용자 및 디바이스에 대한 관리가 어려워짐에 따라 제로 트러스트에 기반에 새로운 보안 정책이 필요하다.

3.3.2. 제로 트러스트 주요 보안 기술

제로 트러스트의 모델은 2020년 5월 NIST(미국표준기술연구소)가 발표한 제로 트러스트 아키텍처 기술서(800-207)에 의해 주요 개념이 정리되었으며, 주요 구성요소는 다음과 같다.

- 정책 엔진(Policy Engine): 접근 정책 및 허용 여부를 최종 결정을 책임지는 역할로 사용자, 디지털기기 또한 어플리케이션 사용자에게 액세스 권한을 부여

- 정책 관리자(Policy Administrator) : 사용자와 접근 시스템 간의 통신 경로를 설정하거나 종료할 책임을 가지며, 정책 시행 지점(PEP)이 인증정보, 키 또는 토큰을 통해 세션 시작을 명령함.
- 정책 시행시점(Policy Enforcement Point) : 리소스에 대한 접근을 제어하고 보호하는 게이트웨이 역할을 수행하며, 사람, 시스템, 어플리케이션과 대상 엔터프라이즈 리소스 간에 세션 활성화, 모니터링 시작 및 종료하는 역할

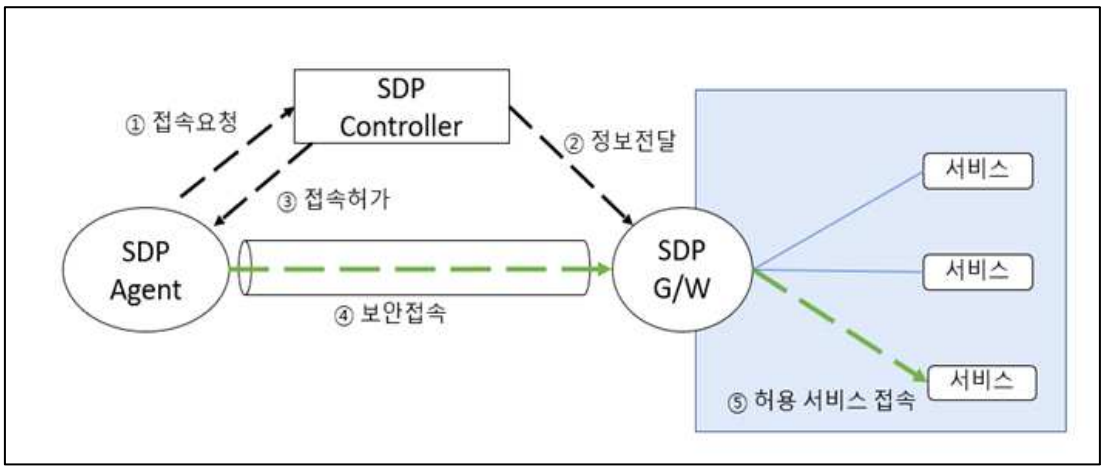


[그림 Ⅲ- 11] NIST SP 800-207 Zero Trust Architecture

1) 소프트웨어 정의 경계(SDP, software Defined Perimeter)

어플리케이션의 연결을 허용하기 이전에 사용자 상태 및 ID를 확인하고, 단말기의 인증을 통해 네트워크를 접속할 수 있도록 하는 클라우드 환경의 접근제어 프레임 워크를 말한다.

일반적으로 외부망에서 내부망으로 접근은 VPN 등 보안 네트워크를 활용하여 연결 후 인증을 하는 방식이라면 SDP 방식은 선 인증 및 후 연결 하는 방식이다.



[그림 Ⅲ- 12] SDP 개념도

*자료 출처: https://blog.naver.com/palanmanzang/222970842103, 2023.10.10.

SDP 방식은 인증 절차와 보안 접속 방식으로 구분되며

① 접속 요청 : oAuth 등 인증 기술을 활용한 접속 요청

② 정보 전달 : SPA(Single Packet Authorization) 기반 사용자 인증

③ 접속 허가 : 제로트러스트 기반 보안 접근 정책 및 통제

④ 보안 접속 및 허용 서비스 접속 : 인증된 사용자에게 서비스 제공 순으로 작동된다.

2) 다중요소 인증(MFA, Multi-Factor Authentication)

다중 요소 인증(MFA, Multi-Factor Authentication)은 두 가지 이상의 인증 요소들을 활용하여 본인 인증을 하는 방법으로써, 기존의 단일 인증 방식의 보안 취약점을 보완하는 방식으로 대두되었다.

- 지식기반 인증: ID/PASSSWORD 등 사용자가 알고 있는 정보를 활용하는 전통적인 방식
- 소유기반 인증 : 모바일 인증번호나 인증 코드를 통한 일회용 인증키를 활용하는 방식
- 속성 기반 인증 : 얼굴 인식, 홍체 인식, 행동 인식 등 사람의 고유한 특징을 활용한 인증 방식
- 위치 기반 인증 : GPS 기기를 활용하여 사용자의 위·경도 값을 기준으로 인증하는 방식

3.4. 지방행정공통정보시스템 현황 분석

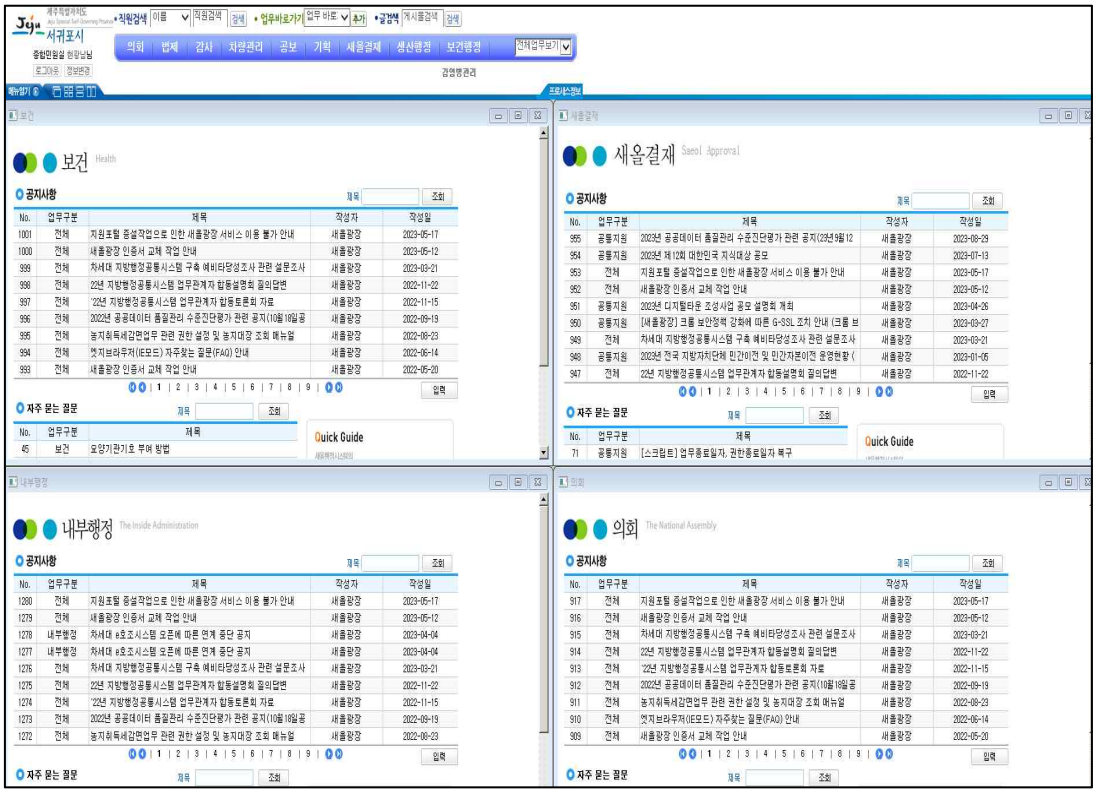
3.4.1. 지방행정공통정보시스템 개요

지방행정공통정보시스템은 국가 사무와 지방 사무를 지원하며 전국 17개 시도 228개 시군구에서 거의 모든 지방자치단체 공무원이 사용하며 연간 8천만건의 민원처리(전체 민원사무의 50%)하며, 290개 기관 9,000개의 정보가 연계되어 있는 행정정보시스템이다. 지금 현재 HW는 공통기반시스템으로 각 지자체 전산실에 배치되어 있으며, 응용 프로그램은 시도·시군구(새올)로 구분되어 한국지역정보개발원에 위탁관리 운영하고 있다.

[그림 Ⅲ- 13] 지방행정공통정보시스템 구성도

지방행정공통정보시스템은 1988년 ‘지방자치법’의 전면 개정을 통해 지방자치 정부의 토대가 마련됨에 따라 지방자치단체에서 독자적으로 운영되고 있던 시스템의 표준화 및 단일화를 목표로 시작하였다.

지방의 정보화 사업은 지방정부의 재정자립도에 따라 지역 간 정보화 불균형이 심화되었고, 동일 기능 시스템을 각 지방자치단체에서 개별적으로 구축함에 따라 개발비용의 이중 투입, 유지보수 인력의 부족으로 인한 보안 체계 미흡 등의 문제가 발생하였다.



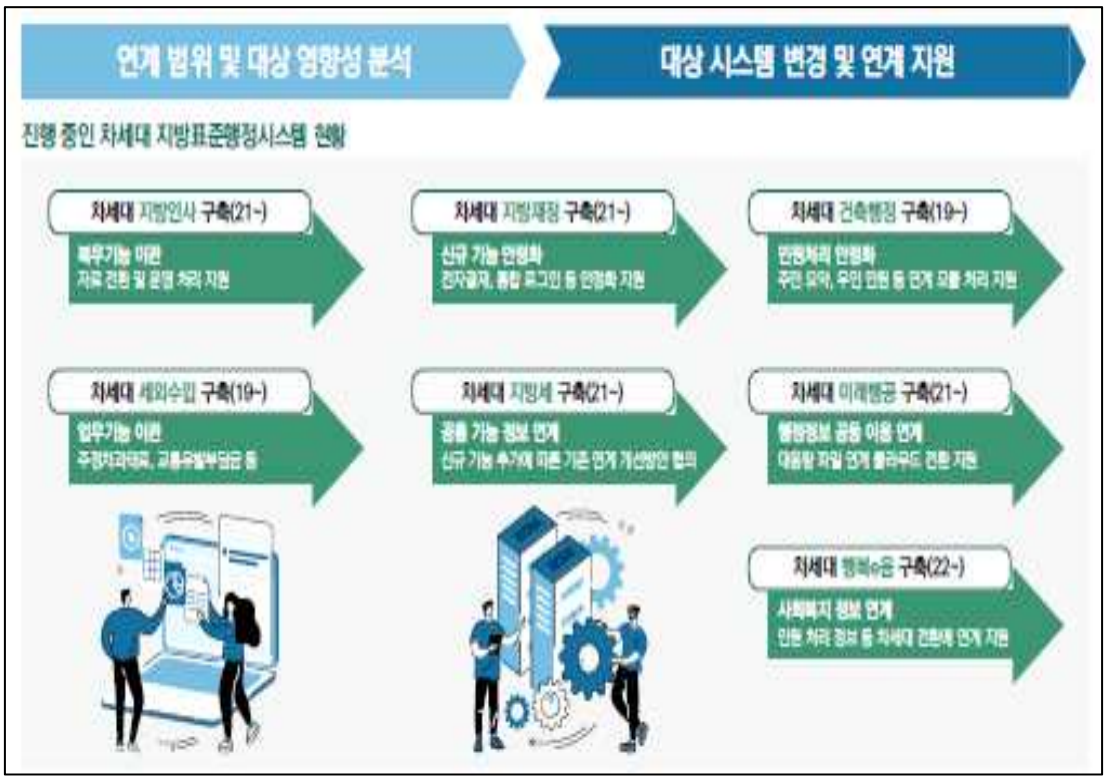
[그림 Ⅲ- 14] 시군구(새올) 화면 캡처

이에 따라, 업무 효율 및 대국민 편의성 향상을 위해 국가표준행정시스템을 보급하기 위한 ‘시군구 행정정보시스템 1단계’ 사업이 1998년 시작되었다. 시스템 연계 및 민원 서비스의 전자화를 위해 ‘시군구 행정정보시스템 2단계’ 사업이 2002년부터 시행되었으며, 두 개의 사업을 단일화하여 ‘공통기반 Ⅰ’ 시스템을 구축하였다. 지방행정정보화 사업은 자치단체별로 상이하게 이루어지고 있는 서비스를 동일화하였으며, 수기로 처리되던 업무를 전자적으로 처리하고, 유관 부서·기관 간 정보 연계를 통해 행정 업무 프로세스를 개선시키는 성과를 가지고 왔다.

이후 행정안전부의 ‘시군구 행정정보 고도화사업(2004년)에 따라 전국 시군구 공통 업무(위생, 여성, 내부행정, 감사, 법제, 의회)에 대한 프로세스 통합과 8개 기본 시스템을 통합 운영 관리하도록 고도화하여 ’ 시군구 공통기반 Ⅱ 시스템 ‘을 구축하여 사용하고 있다.

공통기반시스템이 구축되고 17년이 지나면서 시스템의 노후화, 행정 서비스의 다양화, 민원 업무의 디지털화가 가속화 되었으나, 국가행정표준시스템인 공통기반시스템에 대한 차세대시스템으로 전환은 이루어지지 않았다. 그 사이 공통기반시스템에 탑재되어 있던 개별 시스템(인사, 지방재정, 지방세, 도로명주소 등)은 클라우드 기반의 차세대 시스템으로 전환・구축하였다.

이에 따라 공통기반시스템도 차세대로 전환하기 위한 사업에 착수하였고, 그 명칭도 ’ 지방행정공통정보시스템 ‘으로 변경하여 예비 타당성 조사를 진행하였다.



[그림 Ⅲ- 15] 지방표준행정시스템의 차세대 구축 지원 현황

1) 지방행정공통정보시스템 대표 서비스 사례

지방행정공통정보시스템 구축으로 지방자치단체, 광역자치단체 뿐만 아니라 각 국가 기관과의 시스템 연계를 통해 업무 효율성의 증가, 대국민 서비스 질 향상과 편의성이 확대되었으며, 대표적인 서비스 사례를 확인해 보고자 한다.

- 생애주기 원스톱 서비스

지방행정공통정보시스템은 기관 간 시스템 연계를 통해 민원 처리 절차를 간소화하는 ’ 원스톱 서비스 ‘를 운영한다. 대표적인 사례로는 사망자의 재산을 한번에 조회할 수 있는 ’ 사망자 재산 조회 통합 처리 서비스 ‘이다. 지금까지 사망자의 유산을 확인하기 위해서는 상속인 금융기관에서 재산 내역, 공공기관의 세금 납부 내역, 국민연금관리공단의 수급 내역, 그 밖에 재산 소유 내역을 각 기관별 방문을 통해 확인하여야 하는 불편함이 있었다. 이에 따라 재산 상속에 따른 절차를 이행하지 못하는 경우도 발생하였다. 이를 개선하기 위해서 2015년부터 사망자의 재산을 일괄로 조회할 수 있는 서비스를 제고하여 2022년까지 약 111만명의 이용하였다.

[그림 Ⅲ- 16] 지방표준행정시스템 원스톱 서비스 운영 현황

- 무인민원발급기 서비스 및 정부 24 온라인 서비스

각종 제증명을 위한 서류 발급을 위해 행정기관을 방문하는 데는 많은 시간적·거리적 제한이 있다. 이러한 불편한 점을 개선하고 행정기관 업무 시간 외에도 서류를 발급받거나 온라인을 통한 열람·발급하기 위한 서비스를 확대하였다. 이에 따른 대표적인 서비스가 무인민원발급기를 활용한 오프라인 발급과 ' 정부 24 '를 활용한 온라인 발급 서비스이다.

무인민원발급기는 행정기관에 대한 접근성이 부족한 지역에 설치되기 시작하였으며, 2023년 기준 전국에 5,488대가 설치되어 민원인들의 접근성을 확대하였다. 각종 시스템과의 연계를 통해 주민등록등초본, 토지대장 등 행정기관의 각종 서류뿐만 아니라, 국민연금공단 등과 같은 타 국가 기관의 발급 서비스와 연계하는 등 119종의 증명서를 발급받을 수 있도록 하였다.

또한, 디지털 기술의 발달과 코로나19에 따른 비대면 서비스에 대한 수요 증가에 의해 ' 정부24 '를 활용한 온라인 민원 발급 서비스가 점점 확대 되어가고 있다. 정부 24 포털에서는 93,988종의 서비스를 실시간으로 제공받을 수 있다.

정부 24 서비스는 기존의 ' 민원 G4C'의 기능과 정보공개 청구, 법원에서 발급하는 가족관계증명서 등 거의 모든 국가 기관의 서류를 발급받을 수 있고, 한 번의 인증으로 모든 시스템을 접속할 수 있는 기능을 제공하고 있다.

3.4.2. 지방행정공통정보시스템 접근 권한 및 사용자 인증 체계

1) 지방행정공통정보시스템 개념 및 사용자 분류

지방행정공통정보시스템은 보안을 위해 내부망(행정망)에서만 접속되고, 외부망에서는 접속이 불가하다. 접속을 위해서는 본인 확인 및 접근 권한을 부여받아야 한다. 이와 관련된 지방행정공통정보시스템 용어 정의는 아래와 같다.

1. “이용자“란 다음 각 목의 사람을 말한다.
   가. 업무담당자: 정보시스템 또는 행정정보를 이용하여 행정업무를 수행하는 사람
   나. 시스템 관리자: 행정업무의 원활한 수행을 위하여 정보시스템을 운영·관리하는 사람

2. “본인확인“이란 이용자가 가지고 있거나 알고 있는 정보를 이용하여 본인임을 확인하는 것을 말한다.

3. “접근권한“이란 정보시스템에 접속하여 정보자원을 활용할 수 있는 권한과 행정정보를 생성·변경·열람·삭제 등을 할 수 있는 권한을 말한다.

4. “정보보유기관“이란 행정기관으로서 행정정보를 직무상 작성·취득하여 유지·관리하는 기관을 말한다.

5. “정보시스템“이란 정보의 수집, 가공, 저장, 검색, 송신·수신 및 그 활용과 관련되는 기기와 소프트웨어의 조직화된 체계를 말한다.

6. “행정정보“란 행정기관이 직무상 작성 또는 취득하여 관리하고 있는 자료

로서 전자적 방식으로 처리되어 부호 · 문자 · 음성 · 음향 · 영상 등으로 표현된 것을 말한다.

7. “모바일 공무원증“이란 「국가공무원 복무규칙」 제62조의2제1항 또는 자치법규에 따라 발급하는 전자적 방식의 공무원 신분증을 말한다.

또한, 지방행정공통정보시스템을 직접적으로 사용하는 공공기관의 업무 담당자를 접근 권한별로 구분하면 크게 4가지 유형으로 분류할 수 있다.

- 공무원: 관련 법령(국가・지방공무원법 등)에 의해 채용된 사람, 각 부서 및 업무별 권한을 부여

- 공무직 근로자: 상시적 · 지속적으로 업무에 종사하며 근로 기간의 정함이 없이 근로계약을 체결한 사람으로서 공무원이 아닌 자, 기본 권한 및 각 업무별 권한 부여

- 기간제 근로자: 기간의 정함이 있는 근로계약을 체결한 사람으로서 공무원이 아닌 자, 필요한 경우에만 권한 부여

- 외주 직원: 공무를 위탁받거나 유지관리하기 위해 외부 기관에 채용된 사람, 담당 공무원이 승인한 경우에만 권한 부여

지방행정공통정보시스템 업무담당자는 시스템 관리자에게 본인 확인 및 접근 권한 부여를 요청한다. 시스템 관리자는 업무담당자의 업무 영역에 따라 업무 권한을 부여하고, 본인 확인을 위한 방법을 기본적인 방법을 부여한다.

시스템 관라자에 의해 지방행정공통정보시스템에 등록된 대상자는 ID/PW를 부여받게 된다. ID/PW 방식으로 본인 인증 및 시스템 접근을 하는 업무담당자는

지방행정공통정보시스템의 기본 권한을 부여받게 된다.

업무 담당자 중 공무원과 공무직은 필요에 따라 행정전자서명 인증관리센터를 통해 행정전자서명(GPKI)를 발급받을 수 있으며, 이를 통해 지방행정공통정보시스템 접속을 위한 사용자 인증 권한을 부여받게 된다.

2) 접근 권한 통제 정책

지방행정공통정보시스템의 접근 권한 정책은 행정포털의 기본권한과 부서 및 사용자의 업무 권한에 따라 차등으로 부여되며, 기본 프로세스은 [표 Ⅲ- 7] 와 같다.

정보시스템은 행정기관에서 사용되고 있는 시스템 전체를 말하며, 본 논문에서는 지방행정공통정보시스템으로 제한한다.

[표 Ⅲ- 7] 지방행정공통정보시스템 접근 관리 프로세스

구분	권한 관리	업무처리자
개인별 신규 등록	권한 부여	시스템 관리자
부서별 권한	권한 등록·변경	시스템 관리자
전출, 퇴사	접근 회수	시스템 관리자
부서 이동 및 업무 변경	접근권한 회수 및 변경	시스템 관리자, 부서관리자
주기적인 접근권한 관리	접근 권한 점검, 관리	시스템 관리자

지방행정공통정보시스템의 접근 권한 제한은 업무를 위해 수집된 개인정보에 대한 보안 관리 및 관리의 효율성에 대응하기 위해 필수적으로 이루어진다.

접근 권한을 부여받고자 하는 이용자는 정보시스템 이용 또는 활용 목적 및 근거, 행정 정보의 사용 범위 등을 명시하고, 반드시 부서장의 결재를 받아 권한관

리책임자에게 접근권한을 신청한다.

접근 권한 관리 책임자는 법령 또는 업무 규정 등에 따라 업무 담당자에게 접근 권한을 부여하며, 업무수행에 필요한 최소한의 범위로, 차등적으로 부여한다.

접근 권한 정책은 각 기관별 접근 계획을 수립하도록 되어 있고, 제주특별자치도 지방행정공통정보스템은 접근 권한 통제 정책은 [표 Ⅲ- 8] 과 같다.

[표 Ⅲ- 8] 이용자별 권한 부여 현황 예시

권한의 종류	설 명	접근 허가
시스템관리자 (2인)	- 시스템 총괄 관리(시스템관리자 & 대직자) - 도 전체 사용자와 소속기관에 대하여 모든 권한 부여 가능	- 사전등록된 사용자 및 IP 확인 후 사용
행정시 시스템관리자 (각 행정시 2인)	- 행정시 시스템 운영 총괄관리 - 각 행정시 소속 사용자 총괄 권한부여 가능	- 사전등록된 사용자 및 IP 확인 후 사용
부서관리자 (일반부서 2인, 소방부서 3인)	- 부서 내 사용자관리(사용자 정보수정, 사용자 이동 등) 및 부서관리 가능 - 인사이동시 인수인계 메뉴를 이용하여 권한 인수.인계 - 전임자 휴직, 동일부서 업무변경 등 직접 인수.	- 시스템 관리자의 권한 부여 후 접속 가능 - 본인 인증 후 접속 가능
업무관리자	접근권한관리책임자로부터 소관 업무관리자 권한을 부여받고 소관 업무에 대한 권한관리를 처리 - 물품관리(물품총괄부서), 차량관리(차량총괄부서), 공유재산관리(공유재산총괄부서) 성과관리(성과관리총괄부서)	- 시스템 관리자의 권한 부여 후 접속 가능 - 본인 인증 후 접속 가능
일반사용자	시도.시군구 행정포털의 기본권한 사용(자동부여) 행정업무권한은 담당자간 인수.인계	- 행정망 내부 접근 가능

3) 사용자 인증

사용자 인증은 행정정보시스템에 접근 시 사전 확인된 사람이 접근할 수 있도록 한다.

지방행정공통정보시스템의 사용자 인증 방식은 ID/PASSWORD 본인확인 방식과 행정전자서명(GPKI) 방식으로 이루어진다. 이론적으로는 모바일 공무원증을 통한 본인 확인이 가능하나, 지금 버전의 지방행정공통정보시스템은 적용이 불가하다.

- ID/PASSWORD 사용자 인증

업무 담당자가 시스템관리자에게 지방행정공통정보시스템 접근 권한을 부여받음과 동시에 기본적으로 ID/PW를 부여받게 된다. ID/PW 사용자 인증 방식은 가장 전통적인 인증 수단이며, 가장 보편화된 방식이다.

ID는 업무담당자 1인당 1개만 부여되고, 영어와 숫자 조합을 통해 생성한다. PASSWORD는 대문자, 소문자, 숫자, 특수 문자를 포함한 9자 이상의 조합으로 이루어지면 3개월에 한번씩 변경하도록 설정되어 있으며, 설정된 PASSWORD는 DB에 암호화 된다.

ID/PASSWORD 사용자 인증 방식은 가장 보편적이고 간단하지만, 그에 따라 보안에 취약하고, 관련 보안 이슈들이 많다. 이에 대한 주요 공격에 [표 Ⅲ- 9]와 같다.

[표 Ⅲ- 9] ID/PASSWORD 사용자 인증 공격 방법

공격 명칭	공격 방식
APT (Advanced Persistent Threat; 지능형 지속 위협)	- 장기간에 걸쳐 단일 사용자의 패스워드를 표적으로 하여 다양한 수단으로 해킹을 시도하는 공격 방식 - 해킹 표적에 대한 Social Engineering Attack, Phishing 등을 통해 표적 디바이스를 감염

공격 명칭	공격 방식
Offline Dictionary Attack (오프라인 사전 공격)	- Password File을 강탈한 공격자가 흔히 사용되는 패스워드의 해시값과 Password File의 해시값을 비교하여 사용자의 패스워드를 알아내는 공격 방식이다.
Macro Attack (매크로 공격)	- Password Retry에 따른 Account Blocking Time이 상대적으로 짧을 경우, 공격자는 Macro Program을 통해 패스워드를 알아낼 때까지 시도하기가 쉬워진다.
DoS Attack (Denial of Service Attack; 서비스 거부 공격)	- Password Retry에 따른 Account Blocking Time이 상대적으로 긴 경우, 공격자는 이를 이용하여 특정 사용자의 계정을 의도적으로 Block 시키는 DoS 공격을 수행할 수 있다.
Use Default Password (기본 패스워드의 사용)	- Router, Set-Top Box와 같은 통신장치에 기본으로 부여된 패스워드를 지속하여 사용할 경우 공격자의 표적이 되기 쉽다.
Credential Stuffing (크리덴셜 스터핑)	- 공격자가 사용자의 계정 정보를 탈취해 다른 서비스에 무작위로 대입하여 무단 로그인을 시도하는 공격 방식이다.
Cached Password in Modern WEB Browser (최신 웹 브라우저들의 비밀번호 저장)	- 최신 웹 브라우저들은 사용자 편의를 위해 비밀번호를 저장(캐싱)해놓는 경우가 많은데, 이는 패스워드 암호 체계를 취약하게 만든다.
Specific Account Attack (특정 계정 공격)	특정 계정의 비밀번호를 알아낼 때까지 추측하여 입력하는 공격 방식이다.
Popular Password Attack (잘 알려진 패스워드 공격)	- 사용자가 기억하기 쉬운 패스워드를 사용하는 경우 공격의 난이도가 쉬워진다.
Password Guessing Against Single User (단일 사용자의 패스워드 추측)	- 공격자가 사용자의 계정 정보와 시스템 비밀 번호 정책을 통해 비밀번호를 추측할 수 있다.
Workstation Hijacking (단말기 강탈)	- 공격자가 사용자의 Device를 직접 이용하게 될 경우이다. - 일정 시간 작동이 없으면 로그아웃하게 하거나 사용자의 행동 변화를 감지하면 로그아웃하게 하는 방법으로 예방할 수 있다.

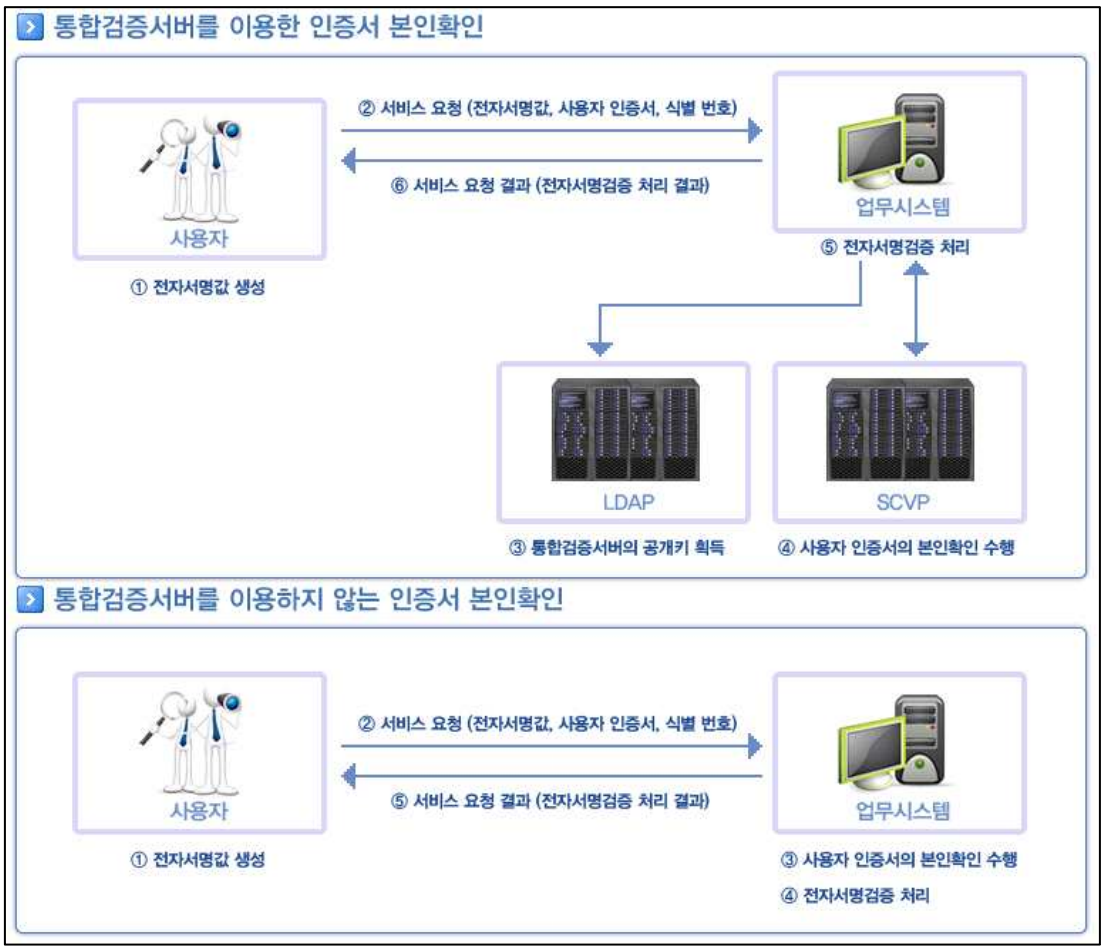
공격 명칭	공격 방식
Exploiting User Mistakes (사용자의 실수를 이용)	- 사용자가 패스워드를 잊지 않기 위해 패스워드를 메모해놓는 등의 보안상 실수이다. Social Engineering Attack과 같은 인간의 상호 작용을 기반으로 한 비기술적 공격이다.
Exploiting Multiple Password Use (하나의 패스워드를 다중으로 사용)	- 사용자가 여러 네트워크에서 단일 패스워드를 사용할 경우, 공격자의 공격에 지워지는 Burden이 작아져 공격이 쉬워지는 경우이다.
Electronic Monitoring (컴퓨터 모니터링)	- 패스워드가 네트워크상에서 원격으로 전달될 경우, Eavesdropping(도청)에 취약할 수 있다.

*자료 출처 : https://dad-rock.tistory.com/830,2023,10.9. 자료 재편집

- 행정전자서명(GPKI) 사용자 인증

공공부문에서 가장 널리 사용되고 있는 행정전자사명(GPKI. Government Public-Key Infrastructure) 사용자 인증 방식은 공공기관에서 유통되는 전자 공문서의 위·변조를 방지하고, 공무원의 신원 확인, 전자 민원 처리 시 민원인의 신원 확인을 위해 2000년 정부 차원의 정보보호책으로 시작되었다.

인증서를 활용하여 인증서를 검증, 공개 키 암호문 제공, 디지털 서명, 본인확인, 전자문서 진본 확인 등을 역할을 수행하여, 특히 행정정보시스템에서 본인인증을 위한 수단으로 널리 사용되고 있다.



[그림 Ⅲ- 17] 행정전자서명(GPKI)를 활용한 본인 검증 방법

*자료 출처: 행정전자서명 인증관리센터(https://www.gpki.go.kr/)

인증서는 수행 업무 및 발급 대상에 따라 그 종류가 달라진다. 우선 기관의 역할에 따른 분류를 살펴보면 행저전자서명 인증 업무 수행 등에 활용하는 최상위 인증기관을 위한 ' 최상위인증기관 인증서 ', 행정안전부 장관이 지정·고시하는 정부 인증기관을 대상으로 인증 업무를 수행하는 ' 인증기관용 인증서 ', 등록기관 등록 업무 수행 등에 활용하도록 하는 ' 등록기관용 인증서' 등으로 구분되어진다.

행정전자서명(GPKI)은 업무 용도에 따라 기관용과 개인용으로 구분되어지며, 그 구분은 [표 Ⅲ-10]와 같다 .

[표 Ⅲ- 10] 행정전사서명(GPKI) 종류

기관	전자관인용	사무관리규정에 따라 관인을 가질수 있는 행정기관, 보조기관, 보좌기관등의 과단위까지의 1개의 기관 인증서를 발급
	특수목적용	사무관리규정에 따라 관인을 가질수 있는 행정기관, 보조기관, 보좌기관등의 과단위까지의 1개의 기관 인증서를 발급
	서버용	행정기관에서 관리해야할 책임이 있는 정보통신 장비가 일정 규칙에 의해 정보통신 장비가 지속적으로 행정업무를 처리하고자 하는 경우에 서버 단위로 인증서를 발급
	G-SSL용	웹상에서 사용자 PC와 웹 사이트 사이에 송수신되는 정보를 암호화 전송하여 개인정보 유출 방지 하는 보안서버 구축을 위한 발급하는 인증서를 발급
개인	행정기관 소속 공무원이 사용자인증 및 전자결재, 보안메일 등의 행정업무에 활용하도록 하기 위해 부처별 개인단위로 인증서 발급	

*자료 출처: 행정전자서명 인증관리센터(https://www.gpki.go.kr/) 재편집

3.4.3. 접근 권한 및 본인 인증 관리 프로세스 문제점

1) 업무 담당자 구분에 따른 문제점

지방행정공통정보시스템의 접근 권한은 업무 담당자별로 차등으로 부여하고, 관리한다. 공공기관에서 업무 담당자 중에는 공무원과 공무직 등은 상시 근로자로서 법적인 권한과 책임이 따른다.

공공기관 근무자 중 필요한 경우 기간제 근로자와 외주 인력(이하 '일시적 업무 이용자'에 대한 접근 권한을 부여한다. 이 경우 보안서약서를 징구하고, 최소한의 개인정보보호교육 이수를 통해 지방행정공통정보시스템의 기본 권환과 업무 권한을 부여하는 데, 이 때 주어지는 기본 권한의 범위가 광범위하다.

일시적인 업무 이용자인 경우 시스템 접근 권한 관리는 각 부서의 장에게 위임 되어 있다. 일시적 업무 이용자가 지방행정공통정보시스템에 접속하는 경우 접속 기록은 관리되고 있으나, 어떤 업무를 수행했는지에 대한 로그 기록은 시스템 관리자만이 관리할 수 있어 각 부서의 장은 접근 권한에 대한 관리·감독이 어렵다.

2) 부서 관리자에 의한 PASSWORD 초기화 기능

지방행정공통정보시스템 접근 권한을 관리함에 있어 접근권한 관리자의 일부 권한을 부서의 장에게 위임하고 있다. 이를 부서 관리자라고 하며, 부서 관리자에게는 업무별 권한 부여 및 업무 담당자의 PASSWORD 초기화 기능을 부여하고 있다.

이는 비밀번호 분실 또는 5회 이상 불일치로 인한 초기화 발생 시 부서 관리자의 확인을 통해 비밀번호를 초기화 할 수 있도록 하는 기능이다. 그러나 이런 기능의 취약점을 활용한 문제점이 발생하고 있다.

- 지방행정공통정보시스템 비밀번호 초기화 기능을 악용한 사례

제주특별자치도에 근무하는 회계 담당자 A씨가 2억여원의 공금을 횡령한 사실이 확인되어 구속되었다. A씨는 회계 담당자 및 지방행정공통정보시스템 부서 관리자로서 주말에 출근하여 자신의 문서를 기안하고, 상급자(팀장, 과장)의 지방행정공통정보시스템 및 지방재정관리시스템 비밀번호를 자신이 초기화하고, 변경하여 문서를 결재하고 지출 서류를 조작하여 공금을 횡령하였다.

3) 부서별 업무에 따른 접근 권한 부여

지방행정공통정보시스템의 접근 및 업무 권한은 업무사용자별 등급에 따라 부여되고 있으나, 개인별 접근 권한은 부서 관리자가 부여하도록 되어 있어, 형식적인 관리만 이루어지고 있다. 이에 따라 각 부서 소속 업무 이용자는 자신의 업무 영역 이외의 업무 영역 접근이 가능하다.

4) 행정전자서명의 다중 접속 가능

행정전자서명(GPKI)은 사용자 본인 인증 수단으로 개인별 1개의 인증서만 발급 받을 수 있다. 행정전서명의 인증은 PC 내 특정 경로에 지정된 개인 인증서 값(개인 키)에 의해 본인을 확인하고, 인증하는 방법이다.

일반적으로 1개의 인증서에 대해서 1개의 PC에서만 사용되어져야 하나, 인증서를 복사하여 다른 장소(PC)에 저장되는 경우에도 사용자 인증이 되는 문제점이 발생하고 있다.

특히, 인사 발령으로 단말기(PC)가 변경되는 경우나, 공무원의 업무를 다른 사람에게 일시적으로 부탁하는 경우 행정전자서명의 취약점을 활용한 보안 문제가 발생하고 있다.

- 행정전자서명을 양도하여 발생된 사례

텔레그램 ‘박사방’ 운영자에게 피해자의 개인정보를 넘긴 협의로 사회복무요원이 실형을 선고받았다. 사회복무요원은 주민센터에 근무하면서 주민등록시스템 담당 공무원이 공유한 접근 권한(ID, 행정전자서명)을 이용하여 피해자의 개인정보를 불법적으로 조회하고, 범죄자들에게 전달하여 피해를 키웠다.

5) 접근 권한의 수동 관리

접근 권한이 부여되었다가 전출, 전보, 퇴직 등의 인사 발령이 나면 사용자의 접근 권한을 회수 처리 하여야 하는데 다수의 접근 권한을 일괄로 처리하다 보면 잘못된 권한 부여, 권한 회수 누락 등의 문제가 발생한다.

그리고 일정기간 사용이 없는 계정에 대한 접근 권한 검토를 다시 해야 되나, 모든 작업이 수작업에 따라 이루어지기 때문에 시스템 담당자가 업무처리를 누락 하는 경우가 발생하고 있다.

Ⅳ. 제로 트러스트 보안 정책 설계

4.1. 제로 트러스트 보안 정책 설계

앞장에서 살펴본 지방행정보시스템 현황, 보안 사고 유형의 변화 및 지방행정공통정보시스템의 '기술적 취약성' 등으로 인해 현재의 지방행정정보시스템의 사용보안 체계는 너무나 취약하다. 특히, 외부 경계설정에 대한 보안 관리는 물리적 장치를 통해 최소한의 범위에서 이루어지고 있으나, 내부자(업무 담당자)에 대한 사용자 인증 및 접근 권한 관리가 디지털 전환의 속도를 따라가지 못하고 있는 실정이다.

디지털플랫폼 정부의 클라우드 네이티브 우선 정책으로 기존의 정보시스템이 클라우드 컴퓨팅 기반으로 전환되고 있으며, 관련 보안 정책이 적용되고 있으나, 국가직·지방직 공무원들이 대표적으로 사용하고 있는 지방행정공통정보시스템의 인증 방식은 구시대의 것이고, 이를 사용하는 일반 사용자들의 보안 의식도 현실과 많이 떨어지는 상황이다.

또한, 코로나 19 이후에 확산된 재택 근무는 공직사회에서도 일반화되고 있다. 이로 인해 다양한 장소에서 내부행정정보시스템에 접근하는 경우가 많으나, 공무원 내부의 관행적인 ID/PW 공유, 사용자 접근 권한과 실제 근무자의 사용자 권한 차이로 인해 행정전자서명을 복사 등을 통한 공동 사용이 만연하게 이루어지고 있다.

이를 위해 지금 현재 구현되어 있는 기능을 활용한 제로 트러스트 개념을 실현할 수 있는 방법을 찾아보고자 한다.

그럼에도 불구하고 현 정부에서는 지방행정공통정보시스템의 구축 및 서비스 시행 시기를 빠르면 2026년이 될 것으로 예상하고 있다. 이에 따라 새로운 보안 시스템을 도입함에 있어 예산적인 측면이나, 시기적인 측면에서 보면 적당하지 않은 시점인 듯 한다.

따라서, 본 눈문에서는 기존 지방행정공통정보시스템에서 구현되어져 있는 인증 문제를 보완하고 좀 더 효율적인 방법으로 운영할 수 있는 방법으로 지금 현재 시점에서 지방행정공통정보시스템에 바로 적용할 수 있는 인증 보안 방법을 연구하고 적용해 보고자 한다.

새로운 접근 권한 정책을 수립하기 위해서는 공공기관 내의 공감대가 필요하며, 자산 현황(PC 정보, IP 정보, 권한 정보)에 대한 정확한 데이터가 필요하며, 새로운 접근 권한 정책을 수용할 수 있는지 여부에 대해서도 확인을 하여야 한다.

이를 위한 보안 정책을 마련하기 위해서는 제로 트러스트 환경에 필요한 요소들에 대한 개념을 이해하고, 실현 가능한 방법을 제안하고자 한다.

[표 Ⅳ- 1] 제로 트러스트 적용 환경에 필요한 6가지 component

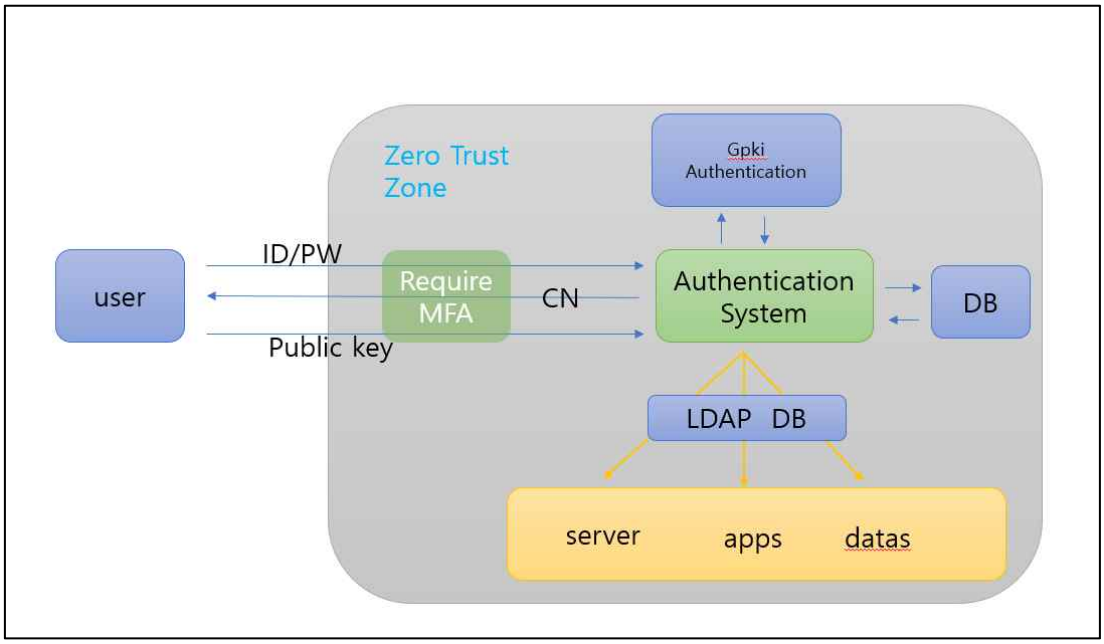
Pilllars	content
사용자 (Identity)	사용자에 대한 신원 확인 및 접근 권한 제어, SSO, 생체인증, 다중요소 접근 제어(MFAC)형태로 접근제어
디바이스 (Endpoint)	기업 내 자산에 접근하는 모든 디바이스에 대한 검증과 모니터링 진행
네트워크 (Network)	소프트웨어 정의 경계(SDP: Software Defined Perimeter) 기술을 활용하여 작은 조각으로 세그먼트(Segment)를 각각 별도 분리하여 네트워크 단위로 접근제어

인프라 (Infra)	서버 운영체제, 오브젝트 스토리지 소프트웨어, CDN 등 형상 관리(Configuration Management) 및 소프트웨어 업데이트
애플리케이션 (Workload	On-premise 로컬 애플리케이션 , 클라우드 기반 애플리케이션 서비스 등에 대한 라이프사이클 관리
데이터 (Data)	데이터에 대해 접근 권한별로 분류하고 이에 대한 접근 정책 적용

4.1.1. 지식 기반 인증 강화

본 논문에서는 제로 트러스트 모델에서 지식 기반 인증 방식을 2단계로 강화한 방법과 모마일 공무원증을 활용한 소유기반 인증을 통해 '사용자(identity)' 환경 요소를 강화하여, 보안성을 증대하는 정책안을 마련하고, 지방행정공통정보시스템에 대한 인증 및 권한 여부를 결정하는 방안을 제시하자 한다. 또한, 더 나아가 인증된 정보를 통해 개별적인 업무 권한을 부여할 수 있는 방안을 제안하여 제한된 접근 및 허용이 가능하도록 구현하고자 한다.

제로 트러스트 기반의 지식 기반 인증 방법은 기존의 ID/PW 방식으로 1차 인증을 하고, 인증 서버에서 회신된 행정전자서명(GPKI)의 인증서 값에 대한 비밀번호를 입력하는 방식으로 인해 보안성을 강화하는 방식을 구현한다.



[그림 Ⅳ- 1] 제로 트러스트 제안 모델 구조

지방행정공통정보시스템에 등록된 ID/PW 값을 통해 1차 인증을 실시한다. ID/PW를 통해서는 중복 사용자 인증이 되지 않는다. ID/PW를 통해 사용자 인증이 이루어지면 해당 ID와 일치하는 행정전자서명(GPKI)의 개인 인증서 값을 사용자에게 회신한다. 이렇게 되면 사용자는 행정전자서명의 개인키 값을 입력하도록 하여 두 번째 인증을 진행한다.

사용자 인증 후에는 인사랑 시스템에서 부여하는 개인식별키와 비교한다. 개인식별키의 값에 따라 일반 공무원과 임시직 사용자 구분을 하고, 이에 따른 시스템 서버 및 각 애플리케이션의 접속을 승인한다. 이를 위한 수행 단계는 아래와 같다.

① 업무 담당자가 지방행정공통정보시스템에 ID/PW 인증을 실시한다.

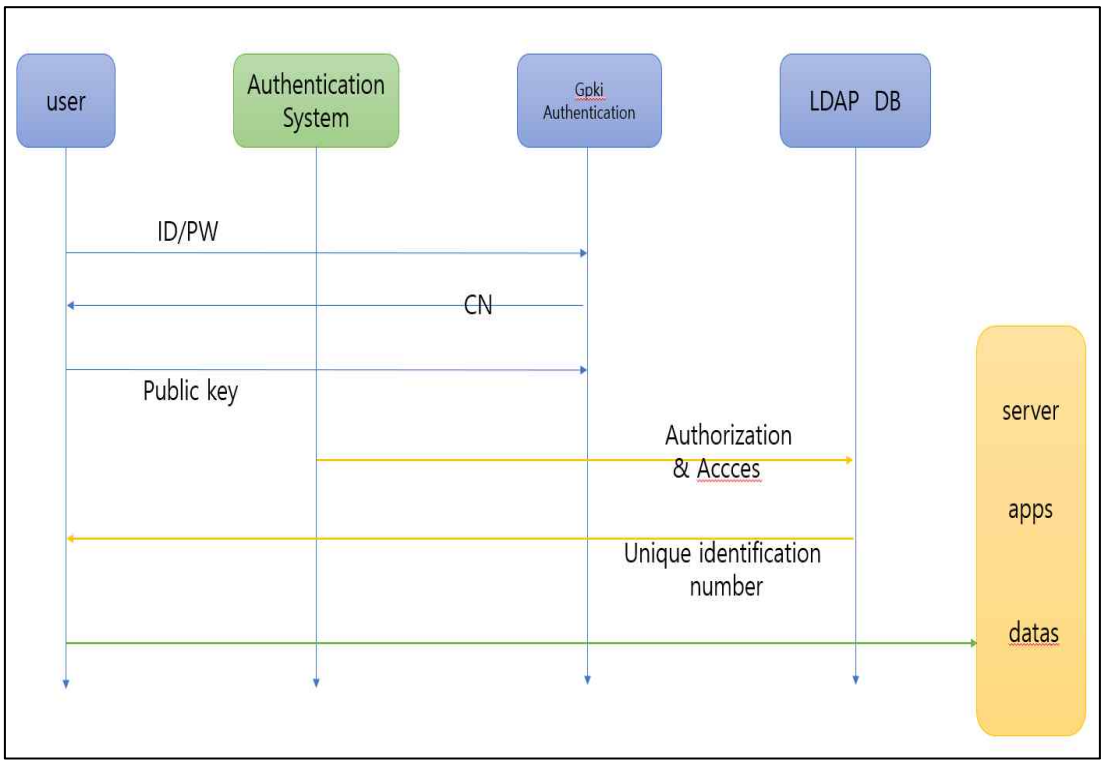
② 인증 서버(Authentication System)에서 ID/PW를 확인하고 행정전자서명 인증센터에서 이와 일치하는 사용자를 찾고, 사용자의 인증서(CN) 값을 사용

자에게 전달한다.

③ 업무 담당자는 행정전자서명 개인키(Public key) 값을 통해 2차 인증을 진행한다.

④ 지방행정공통정보시스템 접속에 따른 사용자 인증을 처리하고, 인사랑 시스템 내 고유식별번호(Unique identification number의 헤더 값을 추출한다.

⑤ 고유식별번호 값의 헤더 값의 분류에 따라 서버 및 지방행정공통정보시스템의 사용자 접근 정책에 따라 각 고유 업무에 접속한다.



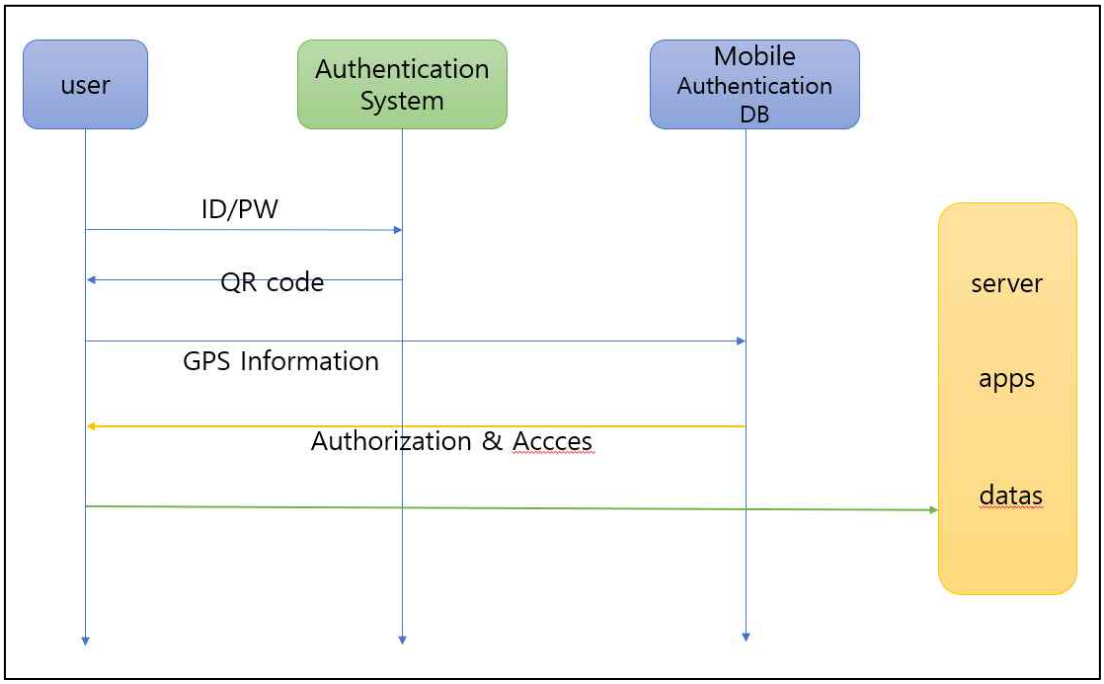
[그림 Ⅳ- 2] 지식 기반 제로 트러스트 접속 단계

4.1.2. 소유 기반 & 위치 기반 인증 강화

두 번째로 모바일 공무원증을 활용한 지방행정공통정보시스템의 사용자 인증을 진행하는 방식이다. 모바일공무원증 DID(Decentralized Identifie) 기술이 적용된 자지 주권 신원 증명(Self Sovereign Identity)의 모바일 신분증으로서, 개인별 1개씩 발급되고 있다.

모바일 공무원증을 통해 내부 네트워크 접속을 위한 사용자 인증을 실시하고, 2단계로 모바일 공무원증을 소지한 사람의 스마트폰 GPS 위치와 사전에 지방행정공통정보시스템이 접속 가능한 지역의 위치값을 비교하여, 사용자 인증 및 접근 권한을 부여하는 방식이다. 이를 수행하는 단계는 아래와 같다.

① 업무 담당자가 ID/PW를 통해 지방행정공통정보시스템의 사용자 인증을 진행한다
② 인증 서버를 통해 사용자 일치 여부를 확인 후 QR 코드를 발급한다.
③ 모바일 공무원증을 통해 QR코드르 스캔하고, 사용자 인증을 진행한다.
④ 이 때, QR 코드 인증 시 업무 담당자의 GPS 위치 값을 인증 서버로 전달한다.
⑤ 인증 서버의 저장된 위치값과 QR 코드의 위치값을 비교하여 신뢰할 수 있는 지역 여부를 판단하여 사용자 인증 및 접근 권한을 부여한다.



[그림 Ⅳ- 3] 소유 기반 & 위치 기반 제로 트러스트 접속 단계

업무담당자의 모바일 공무원증을 통한 1차 인증과 스마트 폰 위치 정보의 적정설 및 정확성의 오차 범위를 비교하여 해당 범위 내에서의 접속을 허용하는 사용자 인증 방식을 구현한다.

4.2. 검증 및 분석

이번 장에서는 앞장에서 제안한 두 가지의 제로 트러스트 보안 정책을 기존 보안 정책과의 비교를 통해서 보안성(security)과 적합성(suitability), 유용성(usability), 경제성(economy) 등을 증명하고자 한다.

4.2.1. 실험 설정 및 적용

제안된 제로 트러스트 보안 정책과 기존의 보안 정책을 비교하기 위해서 디바이스, 네트워크 등 기타 다른 사용자 요소들은 동일하다는 전제 조건이 성립되어야 한다.

또한, 편의상 기존의 보안 정책을 E.A, 지식 기반 인증 보안 정책을 K,B, 모바일 공무원증을 활용한 보안 정책을 M.B로 정의한다.

4.2.2. 실험 시나리오

세 가지의 보안 정책에 대해서 k-Fold 교차 검증 방식으로 진행하고자 한다. k-fold 교차 방식은 전체 데이터 집합을 부분별로 구분하여 각각을 학습용 데이터와 테스트용 데이터로 나눈 후 비교 검증을 하는 방식으로 데이터 개수가 적은 경우 데이터 검증의 정확도를 높일 수 있는 방식이다.

또한, K.B 보안 정책의 검증은 기존 E.A의 단계적 확대이기 때문에 별도의 검증을 진행하지 않고, 모바일 공무원증을 활용한 보안정책(M.B)에 대해서 집중적인 검증을 실시한다. 위치 정보를 확인하는 방법은 안드로이폰을 기준으로 하며, 스마트폰의 위치 정보 서비스 또는 구글 계정을 통해 위치 정보를 수집할 수 있다. 각각의 요소에 대해서 Low, Mid, High 세 단계로 구분하여 검증한다.

업무 담당자의 모바일 공무원증을 통해 지방행정공통정보시스템에서 생성된 QR 코드를 스캔하여 1차 사용자 인증을 진행한다. 이 때 QR 코드에 스마트 폰

의 위치 정보(위. 경도)가 사용자 인증 서버로 전달된다.

사용자 인증 서버에서는 사전에 등록된 위치 정보 DB에 입력된 신뢰 영역(trust zone) 데이터와 비교하게 된다.

[표 Ⅳ- 2] 각 건물 위치별 위치정보 DB

건물명	부서명(사용자명, ID)	위도	경도
서귀포시청 1청사	종합민원실, 총무과 (현길동, 이지은....)	33.254071 33.253565 33.253724 33.254214	126.558953 126.559075 126.560027 126.559927
서귀포시청 2청사	주민복지과, 상하수도 (송새벽, 하인철...)	33.254242 33.254086 33.254182 33.254306	126.560015 126.560054 126.560514 126.560529
서홍동 주민센터	서홍동 주민센터 (이장미. 강서홍..)	33.256070 33.255881 33.255913 33.256092	126.559896 126.559921 126.560514 126.560483

[표 Ⅳ- 3] 사용자 위치 기반 인증 정보

예시	사용자 ID	사용자명	부서명	위도	경도	접근 허용
1	a600115	현길동	총무과	33.253931	126.559630	허용
2	a600115	현길동	총무과	33.253849	126.560797	거부(위치 정보 불일치)
3	p600223	송새벽	상하수도과	33.254243	126.560442	허용
4	p600223	송새벽	상하수도과	33.256021	126.560110	거부(위치 정보 불일치)

행정기관 특성 상 다양한 위치 정보가 있다. 각 지역에 대해 위치정보를 DB화 하고, 각 업무 담당자의 부서 정보와 사용자 ID정보를 포함한다.

첫 번째 예시에서, 모바일 공무원증을 통해 1차 인증을 통과한 '현길동, a600115'의 위치정보와 건물 위치별 DB 정보를 비교한 결과, 서귀포시청 1청사의 신뢰 영역(trust zone) 내에 위치하는 것으로 판단되어 사용자 인증이 허용되었다.

반면, 두 번째 예시에서 1차 사용자 인증을 확인한 '현길동, a600115'의 위치정보가 서귀포시청 1청사의 신뢰 영역(trust zone)을 벗어나서 사용자 인증 및 접근 권한이 거부 되었음을 알 수 있다.

3번째 예시인 '송새벽, p600223'는 1차 인증과 2차 인증이 확인되어 접근 권한이 부여되었고, 4번째 예시인 경우 '송새벽, p600223'을 통해 1차 인증이 되었지만, 위치 정보도 서귀포시청이 아닌 서홍동주민센터의 신뢰 영역(trust zone)에 포함되므로 접근이 거부되었다.

4.2.3. 실험 결과

이번 연구를 통해 지방행정공통정보시스템의 사용자 인증 및 접근 권한을 기존의 보안 정책과 제로 트러스트 기반 보안 정책을 비교하여 기존의 방식에 비해 보안성과 효율성 등이 증가됨을 알 수 있었다.

[표 Ⅳ- 4] 보안 정책 비교

구분	E.A	K.B	M.B
MFA(다단계 인증)	X	O	O
실시간 인증(Continuous Authentication)	X	O	O
최소 권한 부여 (Least Privilege Principle)	X	O	O
SECURITY(보안성)	L	M	H
economy (경제성)	H	M	H
suitability(적합성)	L	M	H
usability(유용성)	M	H	H

특히, 지식 기반 인증 보안 정책과 모바일 공무원증을 활용한 제로 트러스트 활용 보안 정책인 경우 업무사용자 또는 디바이스가 지방행정공통정보시스템에 접속할 때마다 실시간 다중 인증(Continuous Authentication)을 통해 사용자 권한 감시를 실시간으로 진행하며, 각 사용자의 고유식별번호를 활용하여 각 업무 사용자에 대해 최소한의 권한만을 부여함으로써 보안성(security)을 강화하고 있다.

그리고 기존의 개발・운영되고 있는 인증 수단(행정전자서명, 모바일 공무원증)을 활용함으로써 경제성(economy)을 증대하고, 기존 사용자에 대해서 거부감을 최소화 할 수 있을 것으로 예상된다.

Ⅴ. 결론 및 향후 연구 과제

5.1. 결 론

본 논문에서는 공공기관 행정정보시스템에 대한 분석 및 시대적인 흐름에 따른 행정정보시스템의 환경 변화 및 이에 따른 근무 환경의 변화에 대해 알아보았다. 행정기관의 정보시스템은 대규모의 데이터를 관리하고 있으며, 주민등록번호 등을 포함한 개인정보들까지 포함되어 있는 경우가 많다. 또한, 다양한 사회적 가치를 추구하는 공공기관은 공무원뿐만 아니라 공무직, 임시 근로자 등 각계 각층의 사람들이 근무하는 공간이기도 하다.

이러한 특수한 성격을 가지고 있는 공공기관의 행정정보시스템의 사용을 위한 사용자 인증과 접근 권한은 다른 시스템보다 더욱 강화되고 체계적으로 운영되어져야 한다.

지금까지 공공기관의 보안 체계는 경계 기반의 보안 체계를 통해 외부에서 내부로의 접근을 보안 시스템을 통해 통제해 왔다. 그러나 클라우드 컴퓨팅의 확산으로 인한 정보시스템 민간 클라우드 네이티브 시스템으로의 전환, ICT 기술의 발전과 원격 근무의 확산, 공공기관 근로자의 관행적 업무 처리 방식으로 인한 보안 사고의 증가 등은 새로운 보안 정책을 요구하게 되었다.

이를 통해 아무도 신뢰하지 않는다는 제로 트러스트(Zero trust) 개념이 등장하게 되었고, 기존의 사용자 인증 방식과 사용자 접근 정책에 대한 변화가 필요하게 되었다. 그러나 대규모 예산이 투입되는 지방행정공통정보시스템의 개발・구축이 늦어짐에 따라, 기존 시스템 내에서 적용할 수 있는 보안 정책 모델 개발이 필요하게 되었고, 본 논문을 통해 연구를 진행하였고, 그 결과를 정리하면 다음과 같다.

첫째, 업무 담당자의 지방행정공통정보시스템 접근을 위한 사용자 보안 인증 방법을 다단계 인증(MFA) 방식으로 변경하고, 실시간 인증((Continuous Authentication) 방식을 통해 보안성을 강화하였다.

둘째, 지방행정공통정보시스템 사용자 인증 방식과 사용자 접근 정책을 접목하여 행정기관 업무 권한 및 담당자별 차등적으로 시스템 접근이 가능토록 하여 효율성과 경제성을 확대하였다.

5.2. 연구의 한계 및 향후 연구과제

이 연구는 제로 트러스트 모델을 활용하여 기존 시스템에서 운영되고 있는 기능을 활용하여 새로운 보안 정책을 설계하여, 보안성이 강화됨을 확인하였다. 그러나, 행정의 연속성 등으로 인해 새로운 보안정책 모델을 직접적으로 지방행정공통정보시스템에 적용하지 못하고, 이론적 검증에 지나지 않는다는 한계가 있었다.

또한, 공공기관의 행정정보시스템은 광범위하고, 다양하기 때문에 각각의 상황에 맞는 다양한 보안 정책 및 시나리오가 필요하나, 본 연구에서 제안한 보안 정책 모델은은 모든 행정정보시스템에 적용하지 못하는 한계가 있다.

이에 따라, 향후 연구 과제로는 행정정보시스템이 민간 클라우드 네이티브 시스템으로 전환 속도가 빨라짐에 따라, 이에 따른 보안 정책 개발과 다양한 행정정보시스템에 공통적으로 적용될 수 있는 보안 정책의 개발과 내부자에 대한 보안 의식 강화를 위한 교육 방법에 대한 연구가 필요하다.

참고 문헌

주효진, 최희용, 최윤희. (2022). 디지털플랫폼정부와 정부혁신:정부 역할 및 기능 재정립을 중심으로. 지방정부연구 26(3), 307-327.

디지털플랫폼정부위원회. (2023). 디지털플랫폼정부 실현계획.

송효준. (2008). 정보화정책의 역사적 성찰과 향후 과제. 한국지역정보화학회지, 11(1), 1~15.

이주용. (2021). 지방정부의 디지털화 필요성에 관한 연구. 석사학위 논문, 경희대학교.

김수영. (2022). 행정정보시스템 분류 방식을 적용한 행정정보 데이터세트 기록관리의 실제적 실행연구. 기록과 정보・문화 연구 (14), 55~88.

행정안전부. (2023). 2023년도 공공부문 정보자원 현황 통계 보고서(22.12.31. 기준).

행정안전부. (2022). 지방재정관리시스템 공무원 교육자료.

행정안전부. (2022). 통합 온나라 서비스 교육자료.

부혜진. (2015). 귀농・귀촌 인구 증가에 따른 제주도 촌락지역의 변화. 한국지역지리학회지, 21(2), 226-241.

행정안전부. (2021). 행정・공공기관 정보자원 클라우드 전환・통합 추진 계획.

김태진, 김도형, 황성수, 서승현. (2014). 지방전자정부 클라우드 추진 타당성 연구.

국가정보원. (2023). 국가 클라우드 컴퓨팅 보안 가이드라인.

행정안전부. (2022). 행정・공공기관 클라우드 컴퓨팅 서비스 이용안내서.

한국지능정보사회진흥원. (2021). 2022년도 공공부문 클라우드 기술선도 프로젝트 수용조사.

국가통계포털(KOSIS). (2019). 우려하는 개인정보 유출 요인 분석.

나인혜, 강혁, 이근호. (2023). 블로체인과 제로 트러스트 기반 클라우드 보안 기법. 사물인터넷융복합논문지, 9(2) 55-60.

국가정보원. 국가 클라우드 컴퓨팅 보안 가이드라인.

한국문화정보원. (2022). 제로 트러스트 보안기술 동향과 적용방안. 문화정보 이

슈리포트, (6).

한국지역정보개발원. (2022). 지역정보화백서.

행정안전부. (2021). 행정기관 정보시스템 접근권한 관리 규정[국무총리훈령 제795호].

행정안전부. (2023). 행정전자서명 인증관리센터(https://www.gpki.go.kr/).

임형석. (2022). 제로 트러스트 보안 프레임워크 설계에 관한 연구.

Improvement of User Authentication Method in the Common Information System of Local Administration by Using the concept of Zero Trust

HYEON KWANG NAM

Department of Convergence Information Security Course
The Graduate School
Jeju National University

Abstract

With the advent of the 4th Industrial Revolution and the development of IOT technology, the computing environment is rapidly changing. In addition, the spread of coronavirus has brought many changes to our society's work environment and administrative services.

As teleconferencing and telecommuting are activated, and work is expanding, access to internal information systems is increasing at various places other than the original workplace by utilizing mobile or laptop computers.

These social and technological changes have increased

convenience for users, but from the security manager's point of view, the scope of information protection management of information resources and information services is gradually expanding, and control difficulties are increasing. Hacking methods for information systems are becoming more diverse, information security accidents such as personal information leakage continue to occur, and social problems are also developing.

In particular, the administrative agency's information system manages large-scale data and often includes unique identification numbers, including resident registration numbers. Not only is the social impact of information leakage large, but it is also increasing in various crimes related to it. In particular, security accidents against public institutions are more and more caused by workers inside public institutions or temporary workers than by external hacking.

In addition, the government is pursuing changes in the national social system by utilizing innovative technologies such as artificial intelligence, data, and cloud with the goal of digital platform government (DPG) after the e-government era. In order to respond to rapidly changing digital demand, the government is pursuing the advancement of information systems in public institutions, and continues its activities to introduce private cloud native computing technology.

Unfortunately, however, the local administrative common system, which is the representative system of administrative agencies, has been established for 17 years, does not reflect related innovative technologies, and cannot be converted and built into a new system until 2026.

Currently, there is a very high possibility of a large-scale security accident with user self-authentication and user access rights policies according to the current method of the local administrative common system. Since the user authentication method is simple and the system access policy is not detailed, a system of access rights for each person in charge is not established, it is urgent to develop a new security policy related to user authentication of a common local administrative system.

Recently, the concept of zero trust that no one trusts has emerged, and changes to existing user authentication methods and user access policies have been required. In accordance with this, research was conducted on the need to develop a security policy model that can be directly applied to existing internal information systems such as local administrative common systems.

This paper analyzes the types of dissemination and changes in the administrative information systems of public institutions, and studies the concept of zero trust used in cloud computing systems, changes in security policies, and changes in the direction of changes.

It was confirmed that the security authentication method for access to the local administrative common system was changed to a multi-level authentication (MFA) method, the introduction of a real-time authentication method, a security policy that subdivides user access policies, and the k-Fold cross verification method had a positive effect on security and economic feasibility.

Since public institutions' administrative information systems are broad and diverse, various security policies and scenarios are needed for each situation, but the security policy proposed in this study has limitations in that it cannot be applied to all administrative information systems, but it is significant that it has designed a security policy that can be immediately realized and strengthened security in the work environment of the local administrative common system, the core system of public officials.

keyword: information security, user authentication, user access policy, administrative information system, zero trust