Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.1, Feb. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.1.165

행정업무 능률향상을 위한 통합 계정 및 접근 관리 방안*

박 병 언,[1†] 양 재 수,[2‡] 조 성 제[2]
[1]전라북도, [2]단국대학교

An integrated approach for identity and access management for efficient administrative work*

Byung-eon Park,[1†] Jaesoo Yang,[2‡] Seong-Je Cho[2]
[1]Jeonlabuk-Do, [2]Dankook University

요 약

최근 공공기관 및 대형 포털 사이트에 이르기까지 개인정보관리의 효율적인 관리의 부재로 대량의 고객 정보와 정보 유출 관련 사고들이 연이어 발생하고 있다. 이에 내부 자료의 외부유출을 근원적으로 차단할 수 있는 보안 인프라 구축이 그 어느 때 보다도 중요한 이슈로 등장하고 있다. 이에 사용자의 접근과 권한 관리, 인증, 감사 등을 수행하는 계정 및 권한관리시스템이, 업무의 효율성 향상은 물론, 시스템에 대한 접근과 계정 관리를 위한 안전하고 효과적인 방안으로 대두되고 있다. 본 논문에서는 지방자치 행정업무에서 전산 업무능률 향상과 보안성강화를 위해 어떻게 계정 및 권한관리시스템을 구축해야 하는지 분석하고, 그 방안을 제시하였다.

ABSTRACT

Recently large amounts of customer information has leaked ranging from public institutions to the large-scale of portals, and similar information leakage incidents owing to the absence of personal information management have subsequently occurred. Therefore, the security infrastructure in which leakage of internal data can be blocked fundamentally is emerging as a key issue. An integrated identity and access management architecture which performs user access and its rights management, authentication and audit of the business systems is more important to improve the efficiency of business. In addition, this approach is emerging as a safe and effective ways for identity and access rights management. In this paper, we analyze how an integrated approach for identity and access management to improve the efficiency of the computational work and to strengthen the security in local government administration should be constructed, and proposed the preferred solution.

Keywords: Security infrastructure, Identity and access management, Extranet Access Management, Administrative work

I. 서 론

개인정보관리의 효율적인 관리 부재로 인하여 곳곳에서 대량의 고객 정보에 대해 크고, 작은 정보유출 관련 사고들이 연이어 발생하고 있다. 이를 해결하기 위한 수단으로, 업무시스템 사용자의 접근과 권한 관리, 감사, 인증 등을 수행하는 통합 계정 및 접근관리(IAM, Identity & Access Management) 시스템이 업무의 효율성 향상은 물론, 민감한 데이터 및 시스템에 대한 접근과 계정 관리를 위한 안전하고 효과적인 방안으로 대두되고 있다[1-3].

국가기관이나 기업뿐만 아니라 자치단체에서도 통

접수일(2014년 7월 9일), 수정일(1차: 2014년 9월 22일, 2차: 2014년 12월 26일), 게재확정일(2015년 1월 9일)
* 본 연구는 미래창조과학부 및 IITP의 연구개발사업 [2013-005-016-002,안드로이드 어플리케이션의 소스코드 부정사용 방지 기술 개발] 지원으로 일부 수행하였음.
† 주저자, bupark@korea.kr
‡ 교신저자, js-yang1@daum.net(Corresponding author)

합된 계정 및 접근관리 시스템 도입은 매우 필요한 실정이다. 현재 많은 지자체나 관공서에서는 계정 및 접근관리 시스템이 취약하여, 개별 업무시스템별로 계정관리나 접근제어관리를 수행하고 있으며 이에 따라 문제점이 발생하고 있다. 첫째, 조직변동이나 인사발령시 개별 업무시스템별로 계정이 관리되다보니 업무시스템마다 별도의 수작업으로 조직변동이나 인사이동을 하여 업무능률이 비효율적이다. 둘째, 보안성 강화를 들 수 있는데 각종 업무시스템의 업무권한 이양의 지연으로 인해 권한 없는 자의 업무접근으로 자료 유출 사고가 우려된다. 셋째, 현재 사용자 계정신청은 오프라인 상태에서 수작업으로 진행되고 있어 복잡하다. 이에 본 논문에서는 사용자 계정신청, 변경, 삭제 등을 온라인화하여 간편하게 처리할 수 있는 기법을 제안한다. 넷째, 현재 각 업무시스템별로 사용자 관리가 이루어져 각 업무시스템별로 사용자 정보가 서로 상이한 문제점이 생기고 있다. 따라서 이러한 문제는 모든 업무시스템의 계정통합으로, 계정정보가 하나로 통합되면 계정정보가 동기화되고 정확해짐으로 해결될 수 있다.

II. 계정관리시스템 도입필요성 및 계정관련 시스템 비교

계정관련시스템(솔루션)의 도입이 필요한 것은 나날이 증가하는 정보시스템에 누가 어떤 정보시스템의 리소스에 접근하여야 하는지에 대해 지침도 없이 계정요청이 여기저기에서 발생하고 있고 또한 승인도 여러 차례 이루어지고 있다. 이렇게 단순작업처럼 처리하고 있는 계정관련 작업들이 계정요청의 처리 지연이나 수작업에 의한 실수 등이 일반적으로 발생하고 있고 이러한 실수가 발생 했을 때 그로인한 문제를 바로잡기는 대단히 어려운 문제다. 조직변경으로 급격한 부서 및 직원 이동이 대량으로 발생하는 경우 이러한 현상은 더욱 악화될 수 밖에 없다. 또한, 과거 보안의 가장 큰 문제는 외부로 부터의 침입을 어떻게 방어하는지에 있었다. 하지만 현재 내부사용자의 보안의 중요성이 증가하고 있으며, 내부직원 즉 사람을 통제해야 할 필요가 발생하고 있다. IT자원에서 바라본 사람은 곧 ID로 정의되고 그 ID를 통제하고 관리하는 것이 계정관리시스템이며, 내부보안의 출발점이다. 그런데 사용자 계정은 나날이 증가하고 있으며 이에따라 개인업무계정을 본인 스스로 관리하기에는 힘들게 되었으며 이로인해 계정관련 시스템들이 나오게 되었다. 그럼 각 계정관련 시스템(솔루션)들에 대해 살펴보자. 먼저 각 업무시스템들의 사용자 계정을 통합관리하는 계정관리시스템(IM, Identity Management)이 있는데 계정관리시스템(IM)은 계정의 신청·승인 등 계정을 효율적으로 관리하는데 초점이 맞춰있는 솔루션이다. 사용자의 계정신청 및 관리자 승인을 통한 효율적인 사용자들의 개인화 관리가 용이하며 다양한 업무시스템의 계정통합관리가 가능하다. 단일인증 시스템(SSO, Single Sign On)은 업무사용자들이 다양한 업무시스템별로 존재하는 ID와 비밀번호를 모두 외우고 있어야 업무시스템에 접근이 가능한 번잡함을 피하기 위해 단한번의 인증으로 모든 업무시스템에 접근이 가능하도록 지원해 주는 시스템이다. 접근권한관리시스템(EAM, Extranet Access Management)은 인사이동시 자동화된 Role정책에 따라 업무시스템 권한이 부여되며, 사용자의 속성정보를 기준으로 공통된 역할을 분류하여 최소자원만을 접근·관리토록 지원한다. 통합 계정 및 접근관리(IAM,, Identity and Access Management)은 각 업무시스템의 사용자를 식별하고 기 정의된 사용자의 권한에 의해 업무시스템의 리소스에 대한 접근을 제어하기 위한 시스템으로 기 정의된 Role에 의해 접근할 수 있는 업무시스템과 접근가능한 업무권한이 있는 업무에만 접근 할 수 있도록 관리한다. 통상 통합계정 및 접근관리(IAM)은 접근을 제어하기 위한 솔루션들의 집합으로 IM과 EAM, 및 SSO솔루션의 기능을 포괄하고 있다.

III. 업무시스템의 계정 및 접근관리 현황

3.1 업무시스템 현황 분석

본 논문에서는 어느 지자체(JB, JeollaBuk-do)에서 운영 중인 단일인증시스템(SSO, Single Sign- On), 계정관리 및 접근관리 운영의 현황과 운영에 따른 문제점을 다음과 같이 도출하였다[1,2,4].

첫째, 통합 계정 및 접근관리(IAM, Identity and Access Management)에 대한 고찰과 현황을 파악하였다. 특히, 계정관리시스템의 도입 필요성, IAM에 대한 아키텍처, 특징, 계정관리, 인증관리, 계정감사, 통합저장소에 대해 파악하였다.

둘째, JB 통합 계정 및 권한관리 적용방안을 도출하기 위하여 JB의 단일인증시스템, 업무시스템의 계정관리 운영현황, 권한관리시스템의 구축현황 등을 분

석하였다.

셋째, 범정부 통합인증체계인 통합인증프레임워크를 분석하고 통합인증게이트웨이의 주요기능인 신뢰수준관리, 통합 인증 및 권한관리에 대해 분석하였으며, 마지막으로 자치단체에서 효율적인 통합계정 및 접근관리시스템 구축방안을 제시하였다.

3.2 행정업무시스템 운영 현황

JB 전직원 대상 사용자계정관리가 필요한 업무시스템은 행정정보시스템, 온나라시스템, 인사행정시스템, 내부메일시스템, 성과관리시스템, 보안USB관리시스템, 대화형업무협의시스템(내부메신저), 세외수입정보시스템(eNIS), 소방통합포탈시스템 등 총 9종이다. 이중 행정정보시스템, 온나라시스템, 인사행정시스템, 내부메일시스템, 대화형업무협의시스템, 세외수입정보시스템, 소방통합포탈시스템 등 8종의 시스템은 단일인증시스템으로 연동되어 있다[4]. 또한 행정정보시스템은 SSO와 더불어 RBAC(역할기반 접근제어) EAM(Extranet Access Management)시스템이 구축되어 있다. 각 업무시스템 중 별도로 계정을 관리하는 업무시스템은 행정정보시스템, 온나라시스템, 대화형업무협의시스템, 내부메일시스템, 소방통합포탈시스템 등 5개 시스템이며, 이중 권한관리시스템 즉, EAM솔루션이 구축되어있는 시스템은 행정정보시스템과 성과관리시스템, 인사행정시스템 등이며 이외의 업무시스템들은 어플리케이션을 이용하여 업무권한관리를 수행하고 있다[4].

3.3 행정업무시스템 운영 문제점

현재 일부 지자체 또는 관공서에서 운영하고 있는 업무시스템들의 운영상 가장 큰 문제점은 각각 단위업무시스템별로 계정관리를 진행하고 있다는 사실이다. 행정정보시스템은 별도의 저장소에 계정관련 자료를 저장해서 운영하고 있고, 다른 업무시스템인 온나라시스템 또한 계정관리를 별도로 운영하고 있어 계정관련 자료를 자체 저장소에 별도로 관리하고 있다. 또 다른 업무시스템인 내부메일시스템 또한 사용자 계정을 별도로 관리하고 있는 실정이다. 따라서 각각의 업무시스템별로 각자의 시스템에 계정관련 DB를 관리하다보니, 조직개편이나 인사발령 시 사용자 계정관련 업무시스템들은 인사발령 변동작업을 매번 업무시스템마다 따로따로 수작업 해주어야만 한다[3-5].

더군다나 이러한 권한관리 업무는 인사이동에 따라 권한이 없는 자의 업무시스템 접근으로 인한 자료유출 사고 위험에도 노출되어있는 상황이다. 따라서 업무시스템에 대한 계정 및 접근관리 업무를 통합하여 체계적으로 관리해야만 업무시스템의 계정관리 업무에 효율성을 높이고 사용자 업무관리에 철저를 기함으로써 내부자에 대한 보안성을 크게 강화시킬 수 있을 것이다.

3.4 안행부 통합인증게이트웨이 구축사례

정부에서도 각 정부부처 및 자치단체별로 상이한 계정관련 자료를 통합해야만 타기관의 정보를 공동활용 할 수 있게 된다.

이렇기 때문에 기관별로 상이한 사용자 인증체계를 통합 할 수 있고, 인증분야에서는 정부표준이 없기 때문에 범정부 인증체계인 통합인증프레임워크를 구축하게 되었다.

통합인증게이트웨이는 보안수준에 따른 차별적인 관리가 가능하고 행정서비스 연계에도 가능하도록 지원해 주는 정보자원의 보안수준에 따라 체계적으로 관리되는 정부표준 인증시스템이다.

"Fig.1."은 통합인증게이트웨이의 전체 시스템 개념도를 나타낸다. 정부에서 통합인증게이트웨이 추진

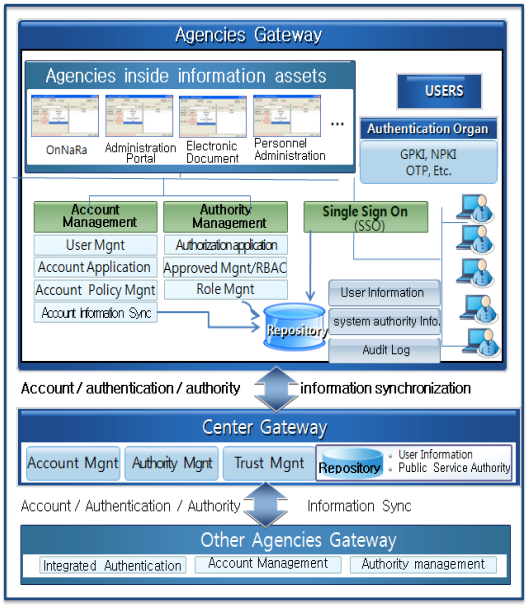

Fig.1. System overview of unified authentication gateway

한 이유는 첫째, 규제개혁 등으로 인하여 민원인에게 각종 인허가 과정에서 발생하는 민원서류 제출을 최소화하여, 행정기관에서 구축된 행정자료를 공동 이용하는데 있다. 둘째, 이렇게 각 기관에서 구축된 행정자료를 기관 자체내에서만 활용하지 않고, 공동 이용 체계를 지원하기 위해, 또한 이를 위해 고도의 지능화되는 해킹으로부터 중요 내부 행정자료의 정보유출을 차단하기 위한 대비책으로 개발하였다. 안전행정부에서는 통합인증게이트웨이의 구축효과로 크게 보안성강화와 업무편의성 증가 및 예산절감을 들었는데 통합인증게이트웨이 구축 시 보안성 강화는 크게 좋아질 것으로 판단된다.

그러나 예산절감 효과에 대해서는 현재 대부분의 기관에서 통합인증시스템이나 권한관리시스템(EAM 및 PMI) 또는 계정관리시스템들을 부분적으로 구축하여 사용하고 있기 때문에 기존에 사용하는 시스템들을 통합인증프레임워크에 맞추기 위해서 다시 새로이 구입하여 사용한다는데 대해서는 예산 절감효과에 어려움이 예상된다[4].

IV. 통합 계정 및 접근관리시스템 구축 방안

4.1 통합 계정 시스템 구축 방안

자치단체에서 운영중인 모든 업무시스템의 계정을 통합한다는 것은 자치단체에서 운영중인 모든 정보시스템의 계정을 통합하는 것이며 결국 계정관리시스템을 통해서 보호해야할 자산은 자치단체에서 구축되어 있는 모든 정보시스템에 보관되어 있는 DB자료이다. 따라서 모든 업무시스템을 총괄관리하는 계정관리시스템의 구축은 자치단체 전체 IT자산을 보호하는 첫 걸음이다. 그러나 현재 시도에서 운영 중인 업무시스템들은 통합된 인사정보시스템과 연계된 계정관리시스템이 구축되어 있지 않아서 계정정보를 각 업무시스템별로 별도로 운영되고 있다. 이렇게 개별시스템별로 계정관리가 운영되다 보니 여러 문제점들이 나타나고 있다[4].

- 첫째, 사용자 임용/퇴직/전입/전출과는 별개로 계정 변경 절차가 수동으로 이루어지고 있음.
- 둘째, 각 개별 시스템별로 상이한 패스워드 정책으로 로그인시에 불편함.
- 셋째, 인사시스템과 별개로 각 업무 시스템별로 사용자등록이 이루지고 있어 조직개편 시 각 개별 업무시스템마다 계정변경처리가 필요함.
- 넷째, DBMS 및 OS에 대한 통합적인 계정관리가 이루어지고 있지 않음.
- 다섯째, 어플리케이션 또는 WAS에서 DBMS에 대한 계정을 하드 코딩하여 사용하고 있음.

따라서 위와 같이 개별 계정관리의 문제점 들을 해결하기 위해서는 각 업무시스템별로 관리하는 계정관련 DB를 통합 관리하여야 하며 이를 위해서는 통합계정관리시스템(IM, Identity Management) 구축이 필요하다.

따라서, 통합계정관리시스템은 각 기관에서 운영중인 개별 업무시스템에 대한 계정을 통합적으로 관리하여 직원의 임용/퇴직/전입/전출/인사변경시 일원화된 정책에 따라 계정의 생성/폐기가 이루어짐으로써 업무효율성과 보안성을 극대화 시켜주는 기능을 제공해야한다.

계정관리시스템의 단위기능으로는 계정통합관리(인사정보동기화), 프로비저닝, 워크플로우, 셀프서비스, 패스워드 관리, 관리기능으로 단위 기능 등을 제공하여야 한다. 일반사용자는 셀프서비스 기능을 통해 자신의 계정관리 기능을 제공받는다[1-3,5].

4.2 통합 접근관리 시스템 구축 방안

현재 시도에서 운영 중인 업무시스템들은 접근권한관리시스템(EAM, Extranet Access Management)이 존재하나, 사용자 계정관리시스템(IM, Identity Management)이 없으며, 운영되고 있는 EAM도 모든 시스템에 적용되는 통합된 통합계정 및 권한관리시스템(IAM, Identity Access Management System)이 없어 각 업무시스템별로 업무권한 관리를 처리하고 있다고 볼 수 있다. 이에 따라 나타나는 문제점은 다음과 같다. 첫째, 업무위임을 위해 인증정보가 공유되고 있다는 점이다. 출장, 교육 등 부재 시 업무위임을 위해 인증정보(ID/PW, 인증서 등)를 공유하고 있으며, 인증정보 공유로 인해 비인가자의 업무시스템 및 정보에 접근이 가능하여 내부자료 정보유출 위험이 존재한다. 둘째, 수동처리로 인한 업무권한 위임에 지연 발생으로 업무공백이 발생한다. 사용자등록 신청서 작성 후 공문 등을 통한 권한신청 및 권한반영을 위한 작업이 수작업으로 이루어지다 보니 즉시 처리되지 못하고 권한반영까지 업무공백이 발생된다. 셋째, 권한부여 기준이나 역할이 세분화되어 있지 않아서 과도한 권한이 부여 되고 있다는 점이다. 넷째, 권

한관리시스템인 EAM시스템이 일부시스템에만 구축되어 있고 대부분의 업무시스템들은 자체 응용프로그램의 권한관리를 활용하여 사용하고 있다는 점이다. 이에 따라 대부분의 업무시스템에서는 권한관리 업무가 제대로 이루어지지 않고 있다. 따라서 위와 같은 문제점을 해결하기 위해서는 업무관리시스템에 권한관리 업무를 담당할 통합권한관리시스템 도입이 필요하다.

접근관리시스템 도입으로 사용자 역할(Role)관리, 권한 신청 및 승인(워크플로우), 권한 할당 등의 업무가 강화될 수 있다. "Fig.2."는 접근관리시스템과 계정관리시스템의 연동절차를 보여 준다. 그동안 시도업무시스템별로 인증정보, 소스코드 프로그래밍, EAM, PMI 등 다양한 형태로 수행되던 접근관리를, 역할기반 접근제어로 일원화할 필요가 있다. 역할기반 접근관리 방식에서는 사용자 제출한 인증정보를 이용하여 역할정보를 도출하고 역할에 정의되어 있는 자원에만 접근할 수 있도록 한다[6-9].

종전에는 각 사용자마다 일일이 접근 권한을 부여하던 것이 역할로 변경됨에 따라 권한 관리의 업무가 감소하게 된다. 사용자의 직무 및 역할이 바뀌어도 변경된 정보에 따라 각 정보자원의 접근권한을 설정하지 않아도 되며, 사용자가 소속된 역할만 변경함으로써 역할에 부여된 모든 자원에 접근 권한을 갖게 되므로 권한변경이 용이하고 권한관리 비용이 감소하게 된다.

접근계정관리(SSO/EAM)시스템은 사용자 정보 동기화를 위해서는 반드시 계정관리(IM)시스템과 연계를 해야 하는데 이때 연동절차는 다음과 같다.

1) 사용자 정보변경 발생시 계정관리시스템에서 인사변동자료 처리
   ① 인사시스템에 의한 사용자 인사변동 발생시 인사시스템과 동기화로 계정관리시스템에서 배치작업 처리
   ② 사용자 본인이 주소, 전화번호 등 기본정보 변경시 계정관리시스템의 셀프서비스를 이용하여 직접 수정
2) 계정관리시스템에서 사용자 계정정보 프로비저닝 처리후 접근관리시스템에 전달
3) 사용자 계정정보 변경내용을 접근관리시스템 권한 Role에 적용함으로써 사용자 업무접근 및 업무시스템 자원 접근 허용 또는 통제정책 적용.

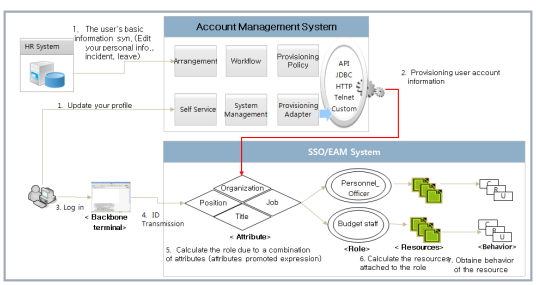

Fig. 2. Interaction of identity and access management systems

4.3 효율적인 통합계정 및 접근관리시스템 구축 방안

본 논문에서는 제시하는 통합계정 및 접근관리시스템(IAM)구축방안은 현재 광역자치단체에서 운영중인 업무시스템의 현황 분석아래 타기관의 정보시스템과의 정보연계 등 호환성을 유지하고 정부 공통표준을 준수 하면서도 가장 저렴한 비용에 보안성을 확보하면서도 효율적인 구축방안이 무엇인지를 고려하여 구축방안을 제시하고자 노력하였다. 우선 각 시도에서 통합계정 및 권한관리시스템(IAM)을 신규로 구축할 때 우선 검토해야 할 사항을 정리해보면, 먼저 시도에서 활용하는 모든 정보시스템에 공통으로 적용될 수 있는 사용자 계정관리시스템(IM이 필요하다는 점이다. 둘째, 통합된 계정관리를 바탕으로 한 역할기반 접근제어(RBAC) 권한관리시스템(EAM) 구축이 되어야 한다는 점이다. 셋째, 이렇게 구축된 시도의 통합계정 및 접근관리시스템을 활용하여 안행부에서 기구축 완료한 센터 통합인증게이트웨이와 우리기관 인증정보를 공유하여 타기관의 내부정보를 공동활용 할 수 있도록 편리성과 보안성을 고려하여 구축하여야 한다는 점이다. 한 개의 기관에서 A라는 사용자가 최초 접속시 기관내부의 인증시스템의 인증정보가 그 사용자의 허가받은 업무의 신뢰수준에 따라 타기관 공동 정보이용시에도 타기관의 추가인증 절차없이 공동활용 할 수 있도록 구축해야만 한다. 따라서 이러한 통합계정 및 접근관리의 효율적인 구축방법으로 본 논문에서는 두가지 방안을 제안해 보았다.

1안은 통합계정 및 권한관리를 위해 통합인증게이트웨이 구축시 사용된 솔루션을 통째로 신규 도입하는 방안이다.

2안은 별도의 통합 계정 및 권한관리 시스템을 구축하는 방안이다.

통합인증게이트웨이를 각 시도에서 신규 도입하는 방안의 장점은 개발이 완료되어 있고, 서울시나 안행

부 운영사례가 있다는 점이다.

또한 정부 표준 프레임워크를 준수했기 때문에 향후 타 기관 정보시스템 이용시 호환성이 좋다는 점이다.

단점으로는 첫째, 구축시 비용이 많이 소요된다.

둘째, 기존 행정정보시스템에 SSO로 연동되어 있는 시스템들과 통합인증게이트웨이와 연동에 문제가 있다는 점이다.

왜냐하면 기존시스템과 인증정보만 연동되지 계정정보나 권한정보는 연동되지 않기 때문이다.

셋째, 기존 단일인증시스템(SSO)와 EAM과의 연동문제 때문에 통합인증게이트웨이를 사용하게 되면 기존 SSO나 EAM은 사용 할 수 없고, 새로이 구축을 해야 한다. 그래서 별도의 통합계정 및 권한관리시스템 구축 방안을 생각해 보면, 현재 시·도에서는 사용중인 기존의 단일인증시스템과 권한관리시스템을 그대로 활용하면서 통합계정시스템을 추가로 구축하며, 업무관리시스템에 접근관리 업무를 담당할 통합접근관리시스템을 구축하는 방안을 고려할 수 있다. 이 경우 기존 시스템을 활용하면서 필요한 추가 시스템만을 신규로 구축하면 되기 때문에 예산을 최대한 절감할 수 있다. 또한 행정정보시스템에 구축되어있는 접근관리시스템을 대부분 그대로 활용할 수 있어 행정정보시스템에 대해 추가로 RBAC 기반의 접근제어를 위한 업무분석이 필요하지 않다. 기존의 행정정보시스템 외에 접근관리시스템이 구축되어 있지 않고, 업무시스템의 어플리케이션으로 접근권한을 관리하는 온나라시스템 등 다른 업무시스템들은 통합접근관리시스템을 구축하고, 기존에 구축되어 있지 않은 IM은 신규로 구축하는 방법을 고려해 볼 수도 있다[4,9].

기존의 단일인증시스템 접근관리시스템들을 그대로 활용하고 통합인증게이트웨이와의 호환성을 확보하기 위해서, 안전행정부에서는 각 기관이 기 구축되어 있는 단일인증시스템을 통합인증게이트웨이와 자료 유통이 가능한 표준규격의 프레임워크를 다시 만드는 것을 고려해야 한다. 그래야 각 기관에서 사용 중인 단일인증시스템을 그대로 활용할 수 있다. 만약 그게 어렵다면 시도에서 활용중인 단일인증시스템을 모두 SAML(Security Assertion Markup Language) 기반으로 바꾸어야만 통합인증게이트웨이와 호환성을 확보할 수 있을 것이다.

현재 시·도에서 업무관리시스템의 업무효율성을 높이고 특히 내부자의 자료유출방지 및 권한없는 자의 자료접근 방지를 위해서 계정 및 접근관리 통합이 매우 필요하다. 따라서 통합인증게이트웨이를 도입하지 않더라도 계정 및 접근관리시스템은 반드시 필요하다. 계정관리시스템이 도입되어있지 않은 시도에서는 업무관리시스템들의 계정을 통합하여 계정관리시스템(IM)을 신규로 도입하고, 접근관리시스템(EAM)은 기존에 행정정보시스템에만 구축되어 있기 때문에 다른 업무시스템에도 적용할 수 있는 통합접근관리시스템(IAM) 구축이 필요하다. 그리고 타기관 정보시스템 공동활용을 위해서는 센터게이트웨이에서 기인증받지 않은 미인가 사용자의 불법접속을 센터게이트웨이와 기관게이트웨이간의 자료공유로 근본적으로 차단하기 위해서 각 시도에서도 자체 기관 게이트웨이를 구축해야 할 것이다. 그래야만 타기관 내부정보를 공동 활용할 때 이중삼중의 기관별로 상이한 인증체계를 모두 통과해야하는 번잡함과 단한번의 인증으로도 공통으로 인증할 수 있는 정보표준체계 인증을 받아야만이 권한없는자들이 우리기관 정보시스템의 접근을 원천 차단하는 보안문제를 근본적으로 해결할 수 있다.

본 논문에서 주장하는 바는 시·도나 관공서가 기존에 사용 중인 시스템들을 모두 새로 바꾸어야하는 통합인증게이트웨이 구축을 서두르기 보다는 우선 해당 기관에 기 구축되어 있는 부분은 센터 게이트웨이와 호환성을 갖추기 위한 작업을 진행하면서, 시·도에서 비효율적으로 운영되고 있는 사용자 계정 및 접근관리 시스템은 조속히 통합 구축하여야 한다는 것이다. 이를 위해, 안행부에서도 기존 시도에서 사용중인 단일인증시스템과 센터게이트웨이와의 호환 방법을 마련해야 한다. 따라서 기존의 시스템을 활용할 수 있는 부분은 최대한 활용하고 필요한 부분만 추가로 구축해야만 예산이 절감 되고, 신규개발에 따른 업무분석 등의 노력을 최소화 할 수 있을 것이다.

V. 결 론

본 논문에서는 JB의 업무시스템의 계정 및 접근관리가 비효율적으로 운영되고 있어, 이에 대한 개선점을 찾아보았다. 현재 지자체에서 운영중인 각종 업무시스템의 계정관리 및 접근관리 운영 실태를 파악하여 현황을 진단하였다. 본 논문에서는 어떻게 하면 현재 지자체에서 운영되고 있는 업무시스템들의 계정관리의 비효율성을 개선하고 업무능률을 향상시킬 수 있는 방안을 제안하였다.

또한 업무시스템의 접근관리가 제대로 이루어지지 않아 권한없는 자의 자료 접근허용 등으로 내부자료 정보유출에 무방비 상태로 노출되어 있으며 인사 변동

시 제때에 업무권한 이관이 되지 않아 업무공백 발생이 발생하는 등의 현황을 분석하고 개선 방안을 제안하였다. 한 방안으로 통합계정 및 접근관리시스템을 새롭게 구축하고 단일인증시스템은 기존의 사용하고 있는 시스템에 대한 활용방안을 제시하였다.

통합계정관리시스템 도입 시 계정정보의 중복 관리 대상의 통합화 및 역할 기반 자동 현행화를 통해 여러 시스템에 대한 계정관리 업무는 물론이고 계정의 생성, 수정, 삭제에 대한 승인 업무 프로세스의 자동화로 업무 효율성이 증가할 수 있다. 사용자가 자신의 계정을 관리자 또는 헬프데스크 개입 없이 혼자서 직접 관리함으로써 사용자 편의성이 증대될 수 있다. 계정에 대한 보안 정책 및 실행을 중앙 집중적으로 일관성 있게 적용함으로써 보안성이 강화될 것이다. 정량적 기대효과로는 계정등록 관리를 위한 업무시간 단축 효과와 패스워드 관리를 위한 운영비용 절감효과가 클 것으로 기대된다.

하지만 본 연구에서는 현재 시·도에서 사용 중인 단일인증시스템이 범정부 표준인증체계인 통합인증프레임워크를 준수하지 않아 서로간의 호환이 되지 않고 예산과 인력의 절감을 위해서 이에 대한 개선이 필요하지만, 이를 위한 구체적인 방법을 제시하지는 않았다. 이에 대한 구체적인 방법은 통합인증프레임워크를 개발한 쪽에서 향후 연구과제로 계속 진행되어야 할 것으로 사료된다.

References

[1] IAM in serials, OnTheNet, June ~ Sept. 2008

[2] Networks Times, IAM Series, Nov. 2008 ~ Feb. 2009

[3] William Stallings, Lawrie Brown, Computer Security Principles and Practice, Pearson, 2012

[4] The 28th Annual Research Report, Administration Information, Ministry of Security and Public Administration, Oct. 2009

[5] Jae-Hyung Yoo, "Recent Developments of Integrated Identity Management Technologies to realize Multi-Domain Single Sign On," KT, Aug. 2007

[6] Si-Do Administration Information System SSO Operation Manual, Ministry of Security and Public Administration, Feb. 2007

[7] ISP(Information Strategic Planning) Result of the next generation of integrated authentication system, LG-Nsys consortium, May 2009

[8] Briefing presentation, Organization Gateway Applications, Seoul City, July 2010

[9] Completion Report on Building, "the next generation of integrated authentication system," Ministry of Security and Public Administration, 2008

〈저자소개〉

박 병 언 (Byung-eon Park) 정회원
1987년 2월: 전북대학교 학사
1990년 3월~현재: 전라북도청
2005년 8월: 전북대 컴퓨터정보 석사

양 재 수 (Jaesoo Yang) 정회원
1988년 8월~1993년 1월: 미NJIT공학박사
1981년 3월~1981년 12월: MIC 사무관
1982년 1월~2006년 1월: KT
2006년 3월~2011년 10월: 광운대 교수
2007년 2월~2011년 10월: 경기도 정보화특별보좌관
2011년 11월~현재: 단국대학교 부교수

조 성 제 (Seong-Je Cho) 종신회원
1996년: 서울대학교 컴퓨터공학과 공학박사
2001년: 미국 University of California, Irvine 객원연구원
2009년: 미국 University of Cincinnati 객원연구원
1997년 3월~현재: 단국대학교 교수