u-City 통합운영센터 관리자 권한관리 체계 분류

Administrator Privilege Management System Classification of u-City Management Center

이완석*, 고 웅**, 원동호*, 여상수***, 곽 진**

Wan-Suck Yi*, Woong Go**, Dong-Ho Won, Sang-Soo Yeo*** and Jin Kwak**

요 약

현재 국내·외에서 유비쿼터스 기술 기반의 혁신도시 개념인 u-City의 추진이 활발히 진행되고 있으며, 이를 위한 통합운영센터에 대한 연구 및 구축도 진행 중에 있다. 하지만 이러한 u-City 통합운영센터에 대한 기술적인 접근은 증가하는 반면, 이를 관리하는 관리자 권한에 대한 연구는 미비한 실정이다. 실제 모든 정보를 관리하게 될 관리자의 권한관리가 이루어지지 않을 경우, 이로 인한 보안 관련 문제점이 발생 할 수 있다. 따라서 본 논문에서는 u-City 통합운영센터의 관리자로 인해 발생할 수 있는 보안 문제점을 분석하고, 이를 효과적이고 체계적으로 해결하기 위한 관리자 권한관리 체계에 대해 제안 한다

Abstract

Recently, a lot of nations are establish and researches the u-City which ubiquitous technology based city, and u-City Management Center(UMC) is also establish and researches. Technical researches of UMC are increasing. However, administrator privilege management researches for UMC is not enough. If we don't manage to administrator privilege who can access and control all of information in UMC, security problems will be occurs. Therefore, in this paper, analyses of administrator privilege management security problems, and proposed administrator privilege management system classification.

Key words : u-City, Administrator Privilege Management System

I. 서 론

현대 사회는 다양한 기술을 통해 필요한 정보의 습득 및 기본적 정보들의 효율적인 제공, 관리를 위한 시스템들의 필요성이 증가하고 있다. 이와 같은 요구로 인해 미래도시는 유비쿼터스 기술이 도입된 첨단 지능형 도시인 u-City가 될 것으로 전망된다.

u-City는 유비쿼터스 기술을 도시 공간과 시민의 생활에 융합하고, 지속적인 발전을 통해 시민의 안전과 삶의 질 향상을 추구할 수 있는 미래형 도시 공간으로 정의될 수 있다. 따라서 주거 공간, 업무용 빌딩, 학교, 공원 등 미래도시 어느 곳에서든지 유비쿼터스

* 성균관대학교 정보보호연구소(Information Security Group., Sungkyunkwan University)
** 순천향대학교 정보보호학과(Dept. of Information Security Engineering., Soonchunhyang University)
*** 목원대학교 컴퓨터공학부(Division of Computer Enginnering., Mokwon University)
· 제1저자 (First Author) : 이완석
· 교신저자 (Corresponding Author) : 곽진
· 투고일자 : 2009년 7월 23일
· 심사(수정)일자 : 2009년 7월 24일 (수정일자 : 2009년 8월 4일)
· 게재일자 : 2009년 8월 30일

기술이 내재된 지능화 사물이 존재하게 되며, 서비스 사용자들은 다양한 기술을 통한 새로운 개념의 서비스를 접할 수 있게 될 것이다. 이와 같은 다양한 서비스가 제공되기 위하여 이를 관리하고 제어하는 기관이 필요하게 되었으며, 이에 따라 u-City의 다양한 서비스를 통합 관리하는 도시통합운영센터(UMC: u-City Management Center) 개념 및 플랫폼이 규정되기 시작하였다 [1].

도시통합운영센터는 u-City 전반에 걸쳐 제공되는 서비스 및 기반 시설들에 대한 제어와 관리를 통해 시민들의 삶의 질 향상을 위한 기능을 수행한다. 이러한 결과로 도시통합운영센터에 대한 중요성이 날로 증가되면서, 기반 시설 관리 및 서비스 제공 등에 대한 다양한 연구가 활발히 진행되고 있다.

도시통합운영센터는 그 특성상 취급되는 정보의 종류가 다양하며, 사용자의 민감한 프라이버시 정보 등 모든 정보가 통합 관리된다. 이에 따라 기존의 개별적 서비스 관리자와 달리 도시통합운영센터의 관리자는 u-City내의 모든 정보를 취급하게 되면서, 이러한 정보를 효율적으로 관리하기 위한 연구가 활발히 진행되고 있다. 그러나 모든 정보를 취급하는 도시통합운영센터의 관리자가 기존 서비스 관리자와 동일한 권한을 소유할 경우, 정보의 오남용, 불법 접근, 불법 마케팅 등의 보안상 문제점을 야기할 수 있다.

이에 따라 본 논문에서는 도시통합운영센터에서 관리자가 취급하게 되는 정보를 ISO 27001의 정보자산 분류 기준을 응용하여 분류하고, 해당 정보를 악의적인 제 3 자가 불법 취득하거나 오남용하는 등의 보안 문제점 발생을 사전에 차단하기 위한 관리자 권한관리 체계에 대하여 제안한다.

본 논문의 구성은 다음과 같다. 2장에서 u-City 통합운영센터에 대해 분석하고, 3장에서 도시통합운영센터의 취급정보 및 권한관리 체계에 따른 문제점을 분석한다. 4장에서 정보의 분류 및 관리자 권한관리 체계에 대해 제안하고, 5장으로 논문의 결론을 맺는다.

Ⅱ. u-City 통합운영센터

2-1 u-City 개요

u-City는 첨단 정보통신 인프라와 유비쿼터스 정보서비스를 도시공간에 융합하여, 도시생활의 편의성 증대와 삶의 질적 향상 및 체계적인 도시 관리 보장 등 도시 핵심 기능의 전반적 향상을 가져오는 첨단 정보통신 도시를 말한다.

이와 같은 첨단 정보통신 도시를 구축하는데 가장 핵심적인 기능을 하는 u-City 통합운영센터는 지난 2006년 5월 정부의 “u-Korea 기본계획”이라는 5대 분야 선진화 과제와 4대 엔진 최적화 과제를 통하여 추진되었다. 이 밖에도 구건설교통부 제4차 국토종합계획, 전자정부법, 구행정자치부의 u지역정보화사업 등을 통해서도 기관 및 지자체내부에서의 정보 공유 등에 관한 통합운영센터 체계 수립에 대하여 정의하고 있다 [2].

u-City에서는 보다 효율적인 서비스를 제공하기 위하여 FTTH, RFID, SoC, IPv6, Embeded S/W 등과 같은 기반기술과 광대역통합망(BcN)을 비롯한 유무선 네트워크 기술, RFID/USN을 비롯한 센서네트워크기술, GIS 등의 응용 연계 기술 등을 적용하고 있다 [3].

그림 1. 기존도시와 u-City 비교
Fig. 1. Compare with Traditional City and u-City

2-2 도시통합운영센터 정의

미래도시인 u-City를 구축하기 위해서는 도시의 정보 융합, 통합, 지능화를 위한 허브 역할을 담당하는 시스템이 필요하게 되는데, 이와 같은 역할을 수행하는 기관을 도시통합운영센터(UMC)라 한다. 도시통합운영센터에서는 통신망, 교통망, 시설물, 통합 단말기 등의 센서기기로부터 도시정보를 수집하고, 이를 통합적으로 분석하는 역할을 수행한다. 이를 통하

여 도시를 효과적으로 운영 및 관리하며, 시민이나 관련 기관에 분석 정보를 제공한다 [1][6].

2-3 도시통합운영센터의 기능과 역할

도시통합운영센터의 주요 역할은 다양한 유비쿼터스 기술 기반 서비스의 정보를 수집, 가공 및 배포하기 위한 수단으로, 개별적 콘텐츠 전달의 한계성 및 비경제적인 인프라 구축을 지양하고 한정된 제도 안에서 외부기관과의 유기적인 연계 및 확장을 수행한다. 또한, 기존의 시스템이 가지는 기능 외에도 사람 중심의 정보 제공 및 배포에 큰 비중을 두고 있다.

이와 같은 도시통합운영센터는 다양한 기기를 통해 정보를 수집하고, 수집된 정보의 실시간 감시, 품질 분석 등을 통해 사용자에게 보다 유용한 정보를 제공한다. 그리고 기존 시스템 및 u-City 환경 내의 신규 시스템과의 유연한 연계 및 확장으로 서비스의 질적 향상 및 사용자의 편의 증대를 도모한다 [4].

현재 국내에 새로 개발되는 크고 작은 규모의 u-City에서 통합운영센터(서울), 도시통합정보센터(화성, 동탄지구), 도시통합네트워크센터(파주, 운정지구), 인천경제자유구역, 수원광교(도시통합관제센터), 성남판교(도시정보관제센터), 공공정보상황실(용인, 흥덕지구)등 다양한 명칭으로 도시통합운영센터가 구축되어 있다. 이와 같이 현재 국내에는 표준안이 마련되어 있지 않으며, 관련 협회들을 중심으로 표준안 마련을 위한 연구가 진행 중에 있다.

표 1. 도시통합운영센터의 역할
Table 1. Role of u-City Management Center

항목	내용
정보의 수집	• 기존 기업 및 정부 기관 등 • 신규 u-City 서비스(교통정보, 환경정보 등) • 시민이 사용하는 각종 유무선 장치(통합단말기, 휴대전화 등) • 다양한 센서 정보
운용 관리	• 수집된 정보의 통합 감시 및 실시간 품질 분석 • Device 및 Network등 인프라의 능동적 운영 • 통합관제실 운영 및 고객 불만 처리
정보 배포	• 유무선 Device에 대한 개인화 서비스 제공 • 관련기관 및 연관 시스템에 대한 정보 제공 • Web Portal, IPTV등에 대한 대화형 정보 제공
통합 및 연계	• 기존 시스템 및 신규 시스템과의 유연한 연계 • 개방형 표준에 따른 단계적 확장 • 도시간 가용성 기반의 연동 • u-Service를 위한 핵심 공통 기능 제공(인증, 과금 등)

다음 표 2는 국내 도시통합운영센터의 현황을 정리한 것이다.

화성 동탄의 경우는 완전한 모습의 도시통합운영센터라기 보다는 공공지역방범, 교통정보 제공, 실시간 신호제어 등의 서비스를 제공하고 있어 초기단계의 공공 관제실 및 정보센터 정도의 성격을 가지고 있다.

용인흥덕 지구의 경우 포털, 상 수도정보 제공 등 기본적인 공공서비스만 제공되고 있어 서비스 차별화 측면에서 만족도가 높지 못하다.

대한주택공사가 시행하는 파주 운정의 경우에는

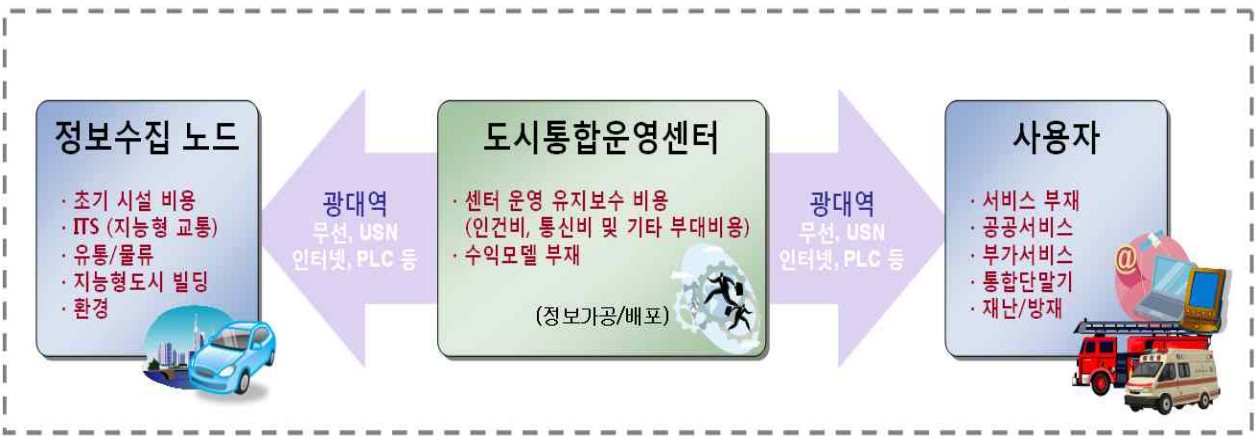

그림 2. 도시통합운영센터 구성도
Fig. 2. u-City Management Center

표 2. 도시통합운영센터 현황
Table 2. The Present State of u-City Management Center

사업지구	면적	인구	서비스 내용	구축비	운영비	현안과제
화성동탄	274만평	12만 명	• 5개 서비스(1차) : 방범CCTV, 교통 정보, 교통신호 실시간제어, 상수도 누수관리, 동탄 포탈 • 7개 서비스(2차) : 미디어보드 외	460억	65억 원	• 운영예산 확보 난이 • 센터 운영주체 • 서비스 차별화 부재
용인흥덕	65만평	2만8천명	• 7개 서비스 : 방범CCTV, 교통정보, 상수도정보화, 포탈 하수도모니터링, 원격검침, 정거장 미디어보드	140억	30억 원	• 서비스 차별화 부재
파주운정	289만평	12만4천명	• 토털 라이프 케어, 스마트 교통, 사회복지, 장애인, 어린이, 노약자 서비스, u환경 등 48개 서비스 제공	900억	68억 원	• 센터 운영주체 • 운영비용 마련 • 기술적 구현가능성 • 제도적 구현가능성
성남판교	281만평	8만7천명	• 13개 서비스 : 기상, 대기•수질, 상수도, 영상감시(CCTV), 교통신호 제어서비스, 교통 약자지원, 재난재해 예방, 원격교육 등	841억	30억	• 기존도시와 신도시 통합운영 • 서비스 차별화 및 통합 서비스 제공
수원광교	341만평	7만7천명	• 7개 서비스 : u-시설물관리, 방범/방재, 환경, 도시관리, 교육, 포털, 민원행정 등	958억	60억	• 행정구역 이분화로 인한 운영조직 문제

공공과 민간의 다양한 서비스 도입을 추진 중에 있으나, 검증되지 않은 서비스로 인하여 기술적이나 법제도 적으로 안정적인 서비스 제공에 대한 우려가 제기되고 있다. 또한 센터 및 시설물 관리 운영 주체와 운영비용 처리 방법에 대해서도 검토를 진행하고 있다.

성남 판교 신도시의 경우 신도시와 기존 도시의 통합운영 문제를 가지고 있다. 판교의 경우 도시통합운영센터를 판교 외곽 지역에 위치한 성남시청에 두어 성남 구시가지와 분당, 판교 신도시까지 전체적으로 서비스를 하도록 계획하고 있다. 이 경우 판교 신도시 지역은 도시 설계 단계부터 u-City 계획을 반영하여 기반 인프라를 설치하고 서비스를 제공할 수 있지만, 기존 구시가지 영역의 경우 동질의 기반 인프라를 같이 설치할 수 없어 서비스 제공에 문제가 발생할 수 있다. 또한 서비스에 있어서도 기존의 공공서비스 위주로 되어 있어 통합서비스와의 서비스 차별화가 어려운 실정이다 [5][6].

III. 취급 정보 및 권한관리 체계 문제점 분석

3-1 관리자 정보 접근 권한 문제

본 논문에서 정의하는 관리자 권한관리 체계는 특정 서비스를 제공 또는 이용하는데 필요한 정보에 대한 접근 및 사용 권한, 서비스 사용자의 접근 허용/거부 등을 규정하고, 이를 체계적으로 관리하여 사용자에게 보다 효율적이고 안전한 서비스를 제공하기 위한 관리자 권한관리 체계를 의미한다.

u-City 사회에서 첨단 인프라, 융합 서비스 등을 원활히 제공하기 위하여 도시통합운영센터에서 다루게 되는 정보는 기존 도시에 비해 그 양과 다양성이 증가하게 된다. 도시통합운영센터에서 수집되는 정보는 서비스 제공을 위한 시스템 정보뿐만 아니라 사용자의 취향 정보, 서비스 이용 성향 등 사용자의 프라이버시에 밀접한 정보까지 모두 포함된다. 이와 같은 정보에 대해 기존의 각 서비스 업체에서는 사용자의 동의하에 필요한 개인 정보의 수집이 이루어졌으나, u-City 환경에서는 서비스의 효율적인 제공을 위해 다양한 정보가 도시통합운영센터에서 통합적으로 관리 및 저장되어 운용된다.

기존 각 서비스 업체의 개별적 정보 관리 및 저장 환경에서는 관리자가 접근할 수 있는 정보가 한정되었다. 그러나 도시통합운영센터에서는 관리자가 네트워크를 통해 전송되는 모든 정보에 대한 접근이 가능하게 되면서, 관리자 정보 접근 권한에 따라 개인 프라이버시 정보까지 오남용 할 수 있는 등의 문제가 발생할 가능성이 증가하였다. 또한, 관리자 정보 접근 권한에 대한 명확한 규정이 부재할 경우, 관리자 개인적인 결정으로 정보의 변경, 사용, 삭제 등이 가

능하고 모든 정보를 통한 빅브라더와 같은 문제점이 발생할 수 있다.

□ 불법 접근

도시통합운영센터에는 다수의 관리자가 존재하게 되며, 각 관리자는 서비스 영역에 따라 나누어지게 된다. 그리고 사용자들은 도시통합운영센터를 통해 이용할 수 있는 기업의 서비스, 공공기관의 행정업무 등 다양한 영역으로 나누어지게 되면서, 다양한 사용자 정보를 서비스 이용을 위해 제공하게 된다.

이와 같이 네트워크상의 모든 정보가 도시통합운영센터를 통해 관리/제공되면서, 악의적인 공격자가 관리자 권한을 불법적으로 습득할 경우 서비스 및 사용자 정보에 접근이 가능하게 된다. 따라서, 각 영역별 관리자의 정보 접근 권한이 서비스 제공을 위한 최소한의 정보에 국한되지 않고, 민감한 서비스 설정 및 개인 신상 정보에 대한 접근까지 허용되므로, 서비스 운영상의 가용성 및 개인 프라이버시 보호에 대한 문제점이 발생 할 수 있다.

□ 불법 마케팅

서비스를 제공하는 기업 측에서는 사용자들의 이용을 증가시키기 위한 다양한 마케팅 전략을 시도하게 된다. 이러한 마케팅 전략은 시민의 취향, 행동반경 등과 같은 정보를 토대로 수립되고 진행된다. 하지만 이와 같은 정보는 개인의 프라이버시 정보와 밀접한 관계를 가지고 있으므로, 사용자의 동의 없이 해당 정보를 수집 및 활용하는 것은 불법적인 활동이라 할 수 있다.

그러나 도시통합운영센터에서는 이러한 다양한 정보를 통합 수집하고 관리하게 되므로, 해당 정보의 보안 수준에 따라 문제가 발생할 수 있다. 만약 관리자가 해당 정보를 서비스 제공자에게 사용자의 동의 없이 제공할 경우, 이를 활용한 서비스 제공자의 불법 마케팅으로 사용될 수 있으며, 사용자들은 원하지 않는 스팸 문자, 메일 등에 따라 피해를 입을 수 있다. 또한, 개인의 취향, 행동반경 등과 같은 민감한 프라이버시 정보가 제 3 자에게 유출되는 문제도 발생하게 된다.

3-2 도시통합운영센터 신뢰성 문제

도시통합운영센터는 도시 전반에 구축된 다양한 단말을 통하여 정보를 수집하고, 품질 분석, 관리/배포 등의 업무를 수행하게 된다. 따라서 수집된 정보는 무엇보다 중요하고 안전하게 관리되어야 한다.

이와 같은 중요 정보를 다루기 위해서는 사용자가 신뢰할 수 있는 관리자가 필요하다. 신뢰할 수 있는 관리자들로 운영된다는 것은 도시통합운영센터 전체의 신뢰성 보장을 의미한다.

따라서 관리자의 정보 접근 권한 설정을 통해 원천적인 정보 접근 가용성을 규정하고 제한함으로써 사용자의 신뢰성을 높일 필요가 있다.

□ 관리자 관리 문제

도시통합운영센터에서 취급하는 정보를 관리자가 서비스 제공에 이용할 경우, 정당한 목적으로 사용되었는지 등에 대한 관리자 관리가 필요하다.

관리자에 대한 관리는 서비스의 가용성 및 정보의 오남용 사례를 방지하고, 서비스를 이용하는 사용자가 서비스 전반에 걸친 신뢰성 유지에 필수사항이다. 그러나 기존의 서비스를 제공하는 관리자의 권한은 이와 같은 정보 접근에 대한 관리자 관리 요소를 적용하기 힘들며, 정당한 정보 이용이 이루어졌는지에 대한 검증이 어렵다.

따라서 사용자의 정보 및 서비스 정보가 정당한 목적으로 사용되었는지 검증이 불가능하게 되면, 사용자는 서비스에 대한 정보 제공을 기피하게 될 수 있으며, 서비스 전반에 걸친 신뢰도 하락으로 이어지게 된다. 이와 같은 서비스 신뢰도 하락은 도시통합운영센터 전반에 영향을 미치게 된다.

□ 서비스 가용성

도시통합운영센터가 취급하게 되는 정보는 그 종류가 다양하고 범위 또한 광범위하며, 이 범위에는 개인 사용자의 민감한 프라이버시 정보까지 포함하게 된다. 따라서 해당 정보에 접근할 수 있는 접근 권

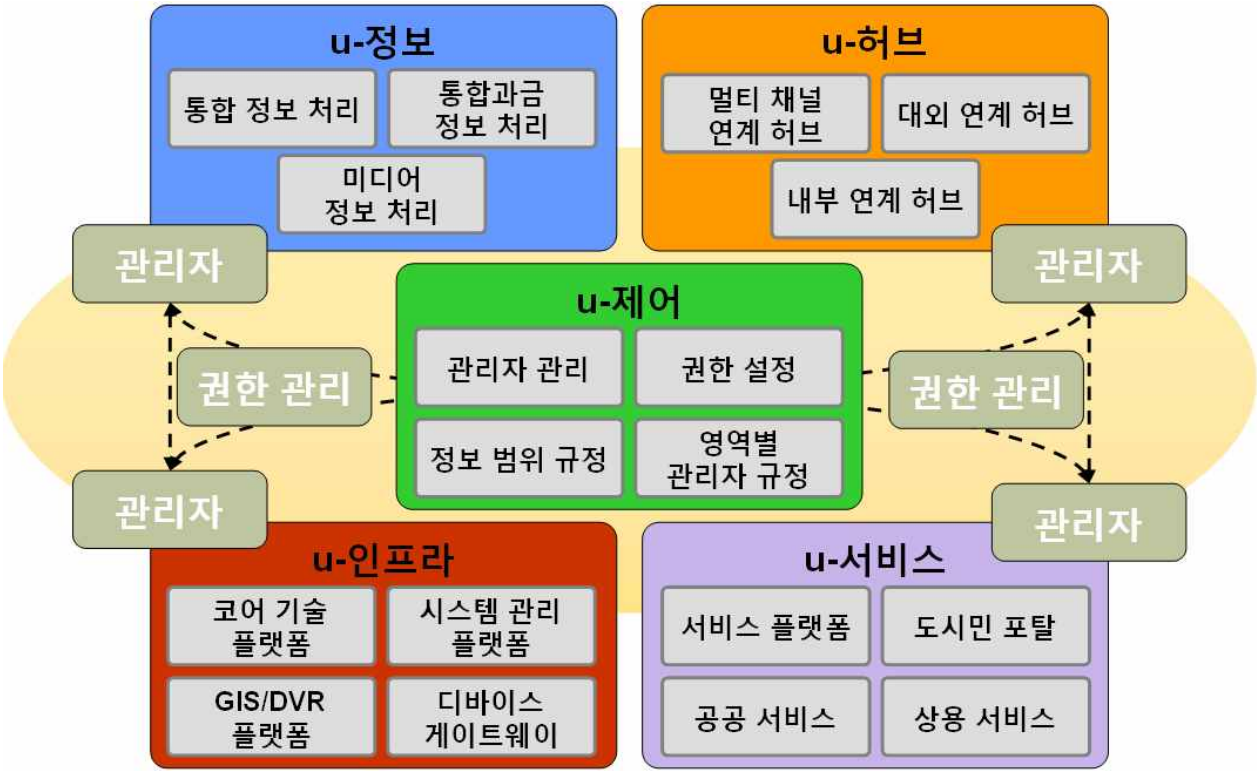

그림 3. 관리자 권한관리 기반 도시통합운영센터
Fig. 3. Administrator Privilege Management Infrastructure Based u-City Management Center

한 및 제어 권한 등에 대한 신뢰성은 도시통합운영센터의 신뢰성까지 연계되어 판단될 것으로 분석된다.

도시통합운영센터에서 취급하는 민감한 정보에 대한 관리자 권한 설정이 명확하게 이루어지지 않을 경우, 한명의 관리자 권한만 취득하면 모든 정보에 불법적인 접근을 할 수 있게 된다.

이와 같은 문제가 발생하면 서비스를 강제 종료하거나, 사용자 정보를 통한 불법 이용 등으로 정당한 사용자가 서비스를 제공받지 못하는 문제가 발생할 수 있다.

따라서 관리자의 권한을 제한하여 이와 같은 문제점을 해결하여야 할 것이다.

Ⅳ. 제안하는 관리자 권한관리 체계 분류

본 논문에서는 도시통합운영센터에서 발생할 수 있는 관리자의 권한 오남용 및 불법 접근에 대한 보안을 위하여 관리자 권한관리 체계를 제안한다.

도시통합운영센터 기반 서비스는 적용되는 다양한 환경에 따라 영역별 관리자가 필요하게 되며, 이들은 서비스 제공에 필요한 정보의 접근 권한을 가지게 된다. 또한, 서비스 제공 대상이나 도시통합운영센터의 내부 프레임워크 분류에 따라 다수의 관리자가 존재하게 되며, 필요한 정보 또한 다양하게 존재한다. 도시통합운영센터는 서비스 제공에 필수적인 정보뿐만 아니라, 네트워크를 통해 전송되는 모든 정보를 저장/관리하므로, 정보의 불법 사용 및 오남용을 막기 위한 정보의 분류 및 관리자 권한 설정에 대한 연구가 필요하다.

본 논문에서는 이를 위하여 도시통합운영센터에서 관리하는 정보를 중요도에 따라 분류하고, 각 정보의 접근 권한을 구분하는 관리자 권한관리 체계에 대하여 제안한다.

4-1 정보의 분류

본 논문에서는 도시통합운영센터를 그림 3과 같이 구성하고 각 서비스 영역에서 관리자가 서비스를 제공하는데 필요한 정보를 분류한다. 정보 분류는 ISO

27001의 정보 자산 분류를 위한 기준 사항 분석을 기반으로 실제 영역에서 사용되는 정보의 사용자 민감성과 정보를 이용함으로써 발생할 수 있는 이익, 효과 등의 가치 정도를 기준으로 구분한다. 각 영역에 따른 권한 설정을 위해 Class 1부터 Class 4까지 4단계로 정보의 중요도를 구분한다 [9].

□ u-정보

u-정보는 통합 정보 처리, 미디어 정보 처리, 통합 과금 정보 처리로 나누고, 통합 정보 처리에 분석/리포팅, 데이터 적재/연계, 통합 데이터베이스, 메타 데이터 관리, 실시간 정보 저장소, 데이터 저장의 세부 항목 등으로 나눈다. 미디어 정보 처리에는 미디어 스트리밍, 미디어 콘텐츠 관리, 미디어 권한 제어로 나누며, 통합과금 정보 처리에서는 과금 관리, 과금 발행/처리, 정산 및 연계 처리 등으로 나눈다. 본 영역에서 필요한 정보는 다음과 같다.

표 3. u-정보 정보 분류
Table 3. Classification Information of u-Information

분류	내용
Class 1	미디어 서비스 제어 정보, 과금 제어 정보, 센싱 데이터 정보(제품), 메타 데이터, 실시간 스트리밍, 과금 정보 등
Class 2	미디어 사용자 요구 사항, 데이터 요금 정보, 요금 정산 정보 등
Class 3	미디어 권한 정보, 데이터 분석 정보, 관리자 권한 정보 등
Class 4	센싱 데이터 정보(개인), 금융 계좌 정보, 개인 신상 정보, 미디어 이용자 정보 등

Class 1에서는 서비스 제공을 위한 정보이며, 미디어 서비스 제어를 위한 설정, 사용자에게 과금되는 정보, 센서 노드들을 통해 전송되어진 제품의 정보, 실시간 스트리밍 서비스 정보 등이 해당된다.

이러한 정보는 서비스가 원활이 제공되는지를 확인하거나, 잘못된 정보의 제공 시 변경이 가능하도록 설정할 수 있는 권한 등의 수준이다.

Class 2는 센서 노드를 통해 들어온 정보의 소유자(사업자), 미디어를 이용하는 사용자의 기본 정보 - 성별, 나이 등과 같이 개인의 프라이버시를 최대한 침해하지 않는 한도 내에서 서비스 제공에 필요한 기본 정보 - 및 데이터 이용에 따라 과금되는 요금 청구 정보 등이 포함된다.

이와 같은 정보는 서비스를 제공하는데 있어서 자동화된 어플리케이션에 의한 해당 정보 처리에 문제가 생겼을 경우, 이에 대한 검증 및 오류 수정을 위한 권한의 범위이다. 따라서 본 정보들은 기본적인 프라이버시 정보가 포함되며, 실제 과금되는 요금 정보 등 관리자가 임의로 수정할 경우, 사용자에게 실제 피해를 줄 수 있는 정보들이 포함된다.

Class 3은 u-정보 분야의 관리를 담당하는 관리자의 권한 정보 및 통합 정보 처리에서 들어오는 센서 정보들의 통합 분석/리포팅 정보들이 해당된다. 통합 정보 처리 섹션에서 들어오는 정보는 그 중요성이 낮은 것에서부터 높은 것까지 모두 포함되므로, 이에 대한 분석 정보를 임의로 열람하는 것은 빅브라더와 같은 문제를 발생시킬 수 있다. 본 권한에서는 통합 관리센터의 모든 관리자 권한 정보를 변경 가능하며, 제공되고 있는 미디어 소유권 등에 관한 민감한 정보들의 변경 등의 일을 수행할 수 있다.

Class 4는 가장 높은 수준의 권한이 필요한 정보들을 포함하고 있으며, 이에 포함되는 정보로는 개인 프라이버시 정보, 과금 계좌 정보, 미디어 서비스 이용자의 세부 정보, 센서 노드를 통해 들어온 개인 정보 등이 해당되며, 이와 같은 정보들은 개인에게 직접적인 피해를 줄 수 있는 정보이다. 따라서 이와 같은 정보의 오남용 시 도시통합운영센터의 보안성 저하와 신뢰도 하락으로 이어질 수 있다.

□ u-허브

u-허브는 내부연계허브, 멀티 채널 연계 허브, 대외 연계 허브로 나누어진다. 또한, 세부적으로 파서(Parser), 라우터(Router), 트랜스포머(Transformer), 빌더(Builder) 등으로 나누어진다. 허브는 내・외부적으로 데이터의 이동을 담당하게 되며, 해당 패킷의 정확한 경로 설정 및 수신/정송 등의 역할을 수행한다. 본 영역에서 필요한 정보는 다음과 같다.

표 4. u-허브 정보 분류
Table 4. Classification Information of u-Hub

분류	내용
Class 1	라우터, 파서 등 정보 설정, 멀티 채널 허브 정보 설정, 외부 서비스 연결 허브 설정 등
Class 2	-
Class 3	라우터 권한 설정, 전류 및 전압 설정, 라우터 테이블 수정 등
Class 4	허브 시스템 교체, 연계 허브 변경 등

Class 1에서는 라우터, 파서 등에 대한 기본 정보 및 라우터 연결 설정 등에 해당하는 기본 네트워크 설정과 내・외부를 연결하는 허브의 정보 및 설정을 위한 사항들을 포함한다.

본 정보는 패킷의 원활한 흐름과 통제를 위해 도시통합운영센터 내외로 이어진 허브의 기본 설정을 확인 수정하는 정도의 수준을 가진다. 허브는 특성상 기기 장치를 직접 설정하는 경우도 있으나, 이는 본 논문에서 논의하는 디지털 정보의 범위를 벗어나므로, 이를 포함시키지는 않았다. 이에 Class 2에 해당하는 정보는 분류되지 않았다.

Class 3은 라우터 테이블, 라우터 및 허브 제어권 설정 등을 통해 라우터를 지나가는 패킷에 영향을 줄 수 있는 세부적인 설정 등을 포함한다. 이와 같은 정보는 다양한 정보의 접근이 가능한 특성상 패킷의 도청이 쉽고, 정보의 열람이 쉽다는 단점으로 인해 해당 패킷을 우회하여 도청하는 등의 불법 접근을 막는 수준으로 설정되었다.

Class 4는 도시통합운영센터 내부에 기설치 된 장비에 대한 교체를 위해 정보 백업 등과 같은 업무 전반에 영향을 줄 수 있는 수준의 정보들을 포함한다.

□ u-인프라

u-인프라는 코어 기술 플랫폼, 시스템 관리 플랫폼, GIS/DVR 플랫폼, 그리고 디바이스 게이트웨이 플랫폼 등으로 나뉜다. 세부적으로 암호화 기술, 인증 기술, 연계 기술, 성능 및 장애 관리, 데이터베이스 및 보안관리, 3D 모델링 엔진 등 다양한 중요 기술과 관리 플랫폼을 포함한다. 각 종 코어 기술 및 시스템 관리 플랫폼은 서비스를 제공하기 위한 기반 기술로 이용되며, 보다 효율적인 서비스 제공을 위한 역할을 수행한다. 본 영역에서 필요한 정보는 다음과 같다.

표 5. u-인프라 정보 분류
Table 5. Classification Information of u-Infra

분류	내용
Class 1	코어 기술 접근 권한, 성능/장애/구성 관리, 영상정보 분류, 3D 엔진 설정 등
Class 2	보안 관리, 백업 관리, 플랫폼 구성 설정, 데이터베이스 권한관리 등
Class 3	플랫폼 관리자 권한 설정, 코어 기술 변경, 게이트웨이 설정, 외부 인프라 접근 설정, 코어 기술 서비스 매치 설정 등
Class 4	-

Class 1은 도시통합운영센터가 u-City의 서비스들을 관리하기 위한 핵심 인프라 도시통합정보 관리 및 기본 서비스 설정 등 도해당하는 코어 기술 접근 권한, 성능/장애/구성 관리 등을 포함하고 있다.

본 정보는 u-City의 서비스가 원활히 제공될 수 있는 기본 핵심 기술들의 대한 정보를 포함하며, 해당 정보를 통한 기본적인 성능/장애/구성 관리를 수행하여 서비스 이용자에게 보다 유용한 기술을 제공하는 정도의 수준을 가지고 있다.

Class 2에서는 서비스를 제공하기 위한 인프라에 대한 보안 관리, 백업 관리 등 보안 설정과, 플랫폼을 구성하는 형태 설정, 데이터베이스 관리 등이 포함된다.

본 정보는 서비스의 질적 향상을 위한 보안성 증가를 위한 설정을 포함하여, 유사시에 발생할 수 있는 문제점을 예방하는 역할을 수행할 수 있다. 보안성과 연관되어 있으므로. 관리자가 임의로 제 3 자의 보안 설정 등을 변경하거나, 백업 데이터의 변경 등을 통해 서비스 인프라에 영향을 줄 수 있는 권한 등에 대한 제어가 가능하다.

Class 3은 다양한 인프라를 분류해 구성하는 플랫폼에 대한 총괄적인 설정에 관한 권한, 서비스 인프

라 코어 기술 변경 및 수정, 게이트웨이 구성 설정 등을 포함하고 있다. 본 정보는 서비스가 실제 운영되는데 직접적인 영향을 주게 되는 플랫폼의 변경 등과 같은 그 영향 범위가 넓은 권한에 대해 변경하거나 수정할 수 있는 정보이다. 따라서 관리자 개인이 임의적으로 변경 불가능하도록 Class 3의 수준을 가지도록 규정한다. 이를 통해 플랫폼에 연계된 다양한 서비스의 가용성을 증가시킬 수 있다.

u-인프라에서는 사용자의 개인 프라이버시 정보와 같은 민감한 정보보다 핵심 기술에 대한 설정 정보 등을 다루게 되므로 Class 4를 분류하지 않는다.

□ u-서비스

u-서비스는 서비스 관련 일반 프레임워크, 도시민 포털 서비스, 공공 서비스 등으로 분류되며, 세부적으로 일반 프레임워크에 실시간 이벤트 어댑터, 미디어 서비스 어댑터, 과금/권한 제어 어댑터, 서비스 플러그인 프레임워크 등으로 나뉜다. 그리고 도시민 포탈은, 도시 통합 정보/콘텐츠 제공 서비스, 모바일 통합 정보/콘텐츠 제공 서비스 등으로 나뉘고, 공공 서비스에서는 교통, 환경, 시설, 안전, 행정 등의 서비스로 나뉘게 된다. 이를 통해 도시민들의 실제 서비스 이용에 필요한 기본 프레임워크를 제공하게 된다. 본 영역에서 필요한 정보는 다음과 같다.

표 6. u-서비스 정보 분류
Table 6. Classification Information of u-Service

분류	내용
Class 1	실시간 서비스 처리, 과금 처리, 미디어 서비스 제공 관리, 공공 서비스 현황 제어, 센서 제어, 콘텐츠 제공 관리 등
Class 2	서비스 접근 권한관리, 미디어 콘텐츠 변경 및 수정 관리, 연계 서비스 변경 등
Class 3	서비스 및 콘텐츠 제공자 정보 검색/수정/변경, 공공(교통, 환경, 시설, 안전, 행정) 서비스 연계 설정 변경/수정 등
Class 4	서비스 이용 사용자 정보, 콘텐츠 과금 정보, GIS/위치 정보, 공공 서비스 이용 정보 등

Class 1에서는 시민들이 이용할 수 있는 서비스 및 콘텐츠 정보 제공 및 과금 처리 등을 관리 할 수 있으며, 공공 서비스 및 기타 서비스와의 상호 연계를 위한 설정 등에 대한 권한을 포함한다.

본 정보는 시민들에게 직접적으로 서비스가 이루어지는 최종 단말을 통해 수집/제공되는 정보이며, 가장 밀접하게 서비스의 품질을 느낄 수 있는 영역이다. 따라서 해당 정보가 시민들에게 효율적으로 제공될 수 있도록 제어 할 수 있는 권한이 설정된다.

Class 2는 u-City에서 제공되는 서비스가 다양함에 따라 이를 이용할 수 있는 시민도 분류되므로, 이에 대한 서비스 접근 권한(성별, 나이 등에 따라)을 설정할 수 있는 권한을 가진다. 또한, 제공되는 서비스 및 콘텐츠 역시 이와 동일한 등급을 나뉘게 된다, 이러한 등급의 설정을 관리자 독단으로 수행할 경우, 서비스를 제공받는 사용자의 요구사항 등을 잘못 설정함으로 유해한 서비스 및 콘텐츠가 제공되는 등의 문제가 발생할 수 있다.

Class 3은 공공서비스 및 콘텐츠 제공자 및 관리자에 대한 관리 권한을 포함한다. 시민이 이용하게 되는 다양한 공공 서비스는 국가 차원에서 다루어지므로 이에 대한 정보는 관리자 개인이 수정/변경이 불가능해야 하며, 서비스를 제공하는 제공자의 정보 또한 관리자가 개별적으로 검색하거나 수정/변경할 수 없어야 한다. 또한, 공공서비스의 경우 해당 정보 중 서비스를 이용하는데 필요한 기본 정보에 대해서만 접근이 가능하다.

Class 4에서는 실제 서비스를 이용하면서 수집되는 시민들의 개인 정보 및 서비스 이용 정보에 따른 개별적 취향 정보 등과 같은 민감한 프라이버시 정보에 대한 접근 권한을 포함한다. 또한, 서비스 이용자의 위치 정보(센서 또는 GIS를 통해)에 대한 접근 권한과 서비스 이용에 따른 개인의 과금 정보에 대한 접근을 포함한다. 본 정보는 실제 서비스되는 최종 단말에서 직접적인 시민의 민감한 프라이버시 정보가 수집/전송되므로, 가장 높은 단계의 보안 수준이 요구된다.

4-2 관리자 권한 및 안전성/효율성 분류

앞서 도시통합운영센터의 각 영역에 해당하는 정보를 Class별로 나누어 분류하였다. 본 Class별 정보

표 7. 관리자 권한 및 안전성/효율성 분류
Table 7. Classification of Administrator Privilege and Security/Efficiency

관리자 등급	정보 Class 및 정의	영역	내용
개별 관리자	Class 1 서비스 제공을 위한 기본 설정	u-정보	미디어 서비스 및 과금 체계에 관한 기본적인 제공을 위한 설정 정보
		u-허브	라우터, 파서 등 허브를 통한 데이터 전송을 위한 기본 설정 정보
		u-인프라	u-City에서 제공되는 서비스의 핵심 코어 기술 및 관련 플랫폼 기본 설정 정보
		u-서비스	실제 서비스 되는 단말과의 연계 및 정보 전송에 관한 기본 설정 정보
2등급 관리자	Class 2 사용자의 과금 및 서비스 이용 설정	u-정보	미디어 서비스 제공 시 필요한 요구 사항 규정 및 서비스 과금 정보
		u-허브	-
		u-인프라	코어 기술 보안, 플랫폼 및 시스템 백업, 데이터베이스 접근 설정 정보
		u-서비스	서비스 접근 권한관리, 연계 서비스 변경 설정 정보
3등급 관리자	Class 3 관리자 설정 및 서비스 전반에 영향을 미치는 설정	u-정보	서비스되는 미디어에 대한 저작권 권한 정보 및 관리자 권한 설정 정보
		u-허브	라우터 변경 권한 설정 및 물리적 디바이스 설정 정보
		u-인프라	서비스 코어 기술 변경 및 매치 설정, 엔진 플랫폼 구성 설정 정보
		u-서비스	서비스 및 콘텐츠 제공자 및 관리자 권한 검색/수정/변경, 공공서비스 설정 정보
최상위 관리자	Class 4 개인 프라이버시 정보 및 H/W, S/W 변경 설정	u-정보	개인 프라이버시(신상정보, 금융정보, 센싱정보 등) 및 서비스 이용자 정보
		u-허브	허브, 라우터, 파서 등의 시스템 변경 및 교체/설정 정보
		u-인프라	-
		u-서비스	단말을 통해 전송되는 사용자 및 과금, 위치정보, 공공서비스 이용 정보

분류	비교 대상	기존 관리자 권한관리 서비스	관리자 권한관리 체계 적용 서비스
안전성	불법 접근	- 접근 제어를 통한 보안 가능 - 개별적인 서비스 별로 보안 기능을 설정해야 하는 문제점 - 모든 정보를 한명의 관리자가 관리	- 접근 제어를 통한 보안 가능 - 통합 보안 기능 설정 가능 - 한명의 관리자가 서비스를 위해 필요한 정보 이외의 정보 접근 불가능
	불법 마케팅	- 관리자가 사용자 정보를 통해 자신이 원하는 마케팅 수행 가능 - 사용자 정보를 마케팅 업체 등에 불법적으로 전송 가능 - 사용자의 개인 취향까지 분석 가능	- 민감한 사용자 프라이버시 정보 접근 불가능으로 개인적인 마케팅 불가능 - Class4에 해당하는 프라이버시 정보는 4명이상의 관리자의 동의가 필요 - 임의로 사용자 정보를 마케팅 업체 등에 전송 불가능 - 관리자는 사용자의 기본정보 이외의 특성 분석 불가능
효율성	관리자 관리	- 관리자의 권한 관리 불가능 - 관리자 개인의 양심에 전적으로 의존 - 주기적인 관리자 관리 체계 부재 - 관리자 불법 행위 즉각 탐지 불가 - 빅브라더 문제 발생 가능 - 관리자에 대한 신뢰도 감소	- 관리자의 관리 체계 구축 - 관리자 불법 행위 즉각 탐지 가능 - 실시간 관리자 관리 체계 구축 가능 - 빅브라더 문제 발생 불가능 - 관리자에 대한 신뢰도 향상
	서비스 가용성	- 악의적인 공격자가 관리자 권한을 통해 전체적인 서비스 통제 가능 - 관리자가 이익을 위한 사용자 정보 남용 가능 - 서비스에 대한 신뢰도 감소	- 한명의 관리자 권한만으로는 전체적인 서비스 통제 불가능 - 관리자가 이익을 위한 사용자 정보 남용 불가능 - 서비스 가용성과 관련된 정보에 개별적인 접근 불가능 - 서비스에 대한 신뢰도 향상

는 관리자가 서비스를 제공하거나 사용자의 개인 프라이버시 정보 관리, 시스템 전반에 걸친 제어 환경 설정 등에 필요한 정보들의 분류이며, 관리자의 접근 권한 등급에 따라 접근 가능한 정보의 Class가 나누어지게 된다.

다음은 관리자 등급에 따라 이용 가능한 정보와 이를 통해 얻을 수 있는 안전성 및 효율성 측면에 대해 나타낸 표이다.

□ 개별 관리자

개별 관리자는 각 영역에 해당하는 기본적인 설정 및 사용자의 편의성을 도와줄 수 있는 Class 1에 해당되는 정보에 대한 접근만 가능하다.

□ 2등급 관리자

Class 2에 해당하는 정보에 대한 접근을 요할 때 필요한 관리자 등급이며, 사용자 과금 정보 및 서비스 이용 설정 등이 포함된 정보에 대한 접근이 가능하다. Class 2는 Class 1의 정보를 포함한다.

□ 3등급 관리자

Class 3에 해당하는 각 영역의 정보를 접근하는데 필요한 관리자 등급이며, 영역별 관리자 설정 및 서비스 전반에 영향을 미칠 수 있는 핵심 코어 기술, 기반 인프라 등에 대한 설정 정보에 접근이 가능하다. Class 3은 Class 1과 Class 2의 정보를 포함한다.

□ 최상위 관리자

도시통합운영센터에서 최고 수준의 보안을 요구하는 정보에 대한 접근을 뜻하며, 해당 정보는 개인 사용자의 민감한 프라이버시 정보나 H/W, S/W 변경 등 도시통합운영센터 전체의 운영에 대한 물리적, 환경적 변화에 대한 설정 정보 접근 권한을 포함한다. 본 정보는 Class 4로 구분되고, 이는 하위 Class가 가지는 모든 정보를 포함하여 접근 가능하다.

□ 안전성 및 효율성 분석

앞서 정의한 정보의 분류 및 관리자 분류를 통해

표 8. 관리자 권한 범위
Table 8. Range of Administrator Privilege

가용 정보	기존 서비스 관리자	관리자 권한 체계 분류			
		개별 관리자	2등급 관리자	3등급 관리자	최상위 관리자
서비스 기본 정보 접근	O	O	O	O	O
서비스 환경 설정	O	O	O	O	O
서비스 제어 설정	O	X	X	O	O
핵심 기술 변경 및 설정	O	X	X	O	O
소프트웨어 변경 및 설정	O	X	X	O	O
사용자 프라이버시 정보	O	X	X	X	O
과금 정보	O	X	O	O	O
사용자 정보 변경	O	X	X	X	O
사용자 성향 분석	O	X	O	O	O
사용자 정보 활용	O	X	X	X	O
관리자 기본 정보 설정	O	O	O	O	O
관리자 권한 설정	O	X	X	O	O
관리자 관리 기능	X	O	O	O	O
총괄 시스템 변경 정보	O	X	X	X	O

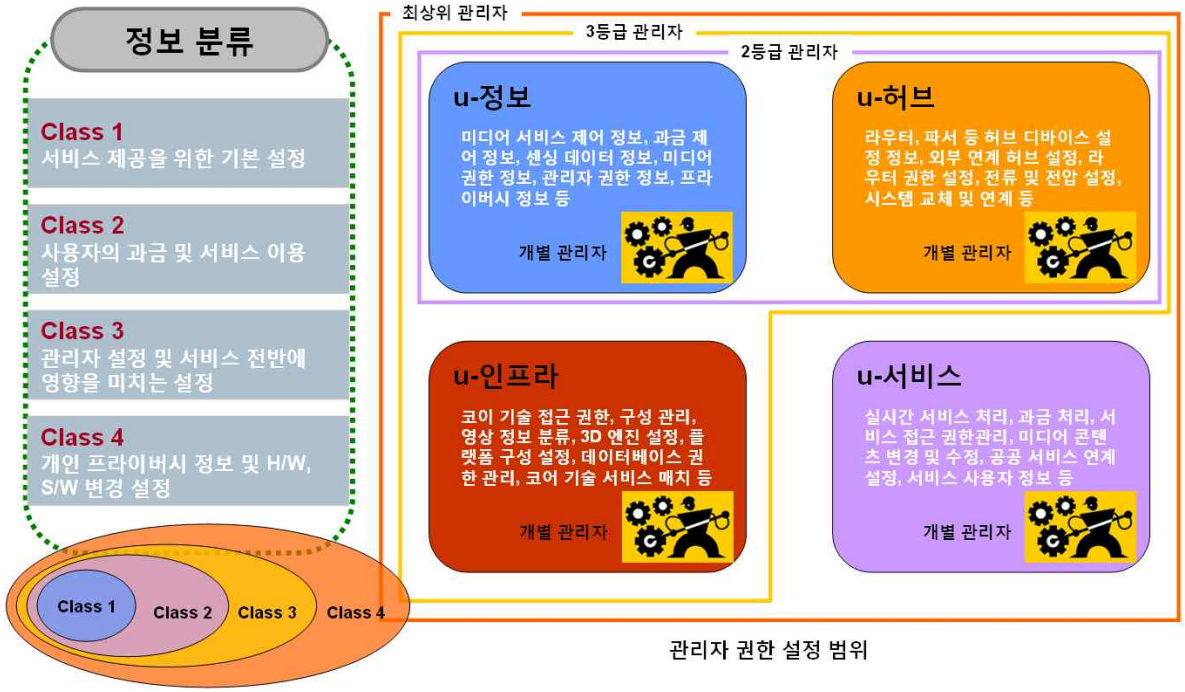

그림 4. 관리자 권한 관리 체계 분류
Fig. 4. Administrator Privilege Management System Classification

관리자 권한관리 분류 체계를 통한 관리자 권한 범위를 표 8에서 분석하였다.

표 8을 보면 기존 서비스 관리자가 가지고 있는 권한 범위는 가용한 모든 정보를 포함하며, 모든 정보에 대한 정보 접근, 수정, 변경 및 삭제 등이 자유롭다. 이와 같은 관리자의 권한이 분산되지 않고 집결될 경우, 이를 악용할 수 있는 가능성이 높아져 사용자 정보에 대한 안전성에 위협을 받게 된다.

본 논문에서 제안한 도시통합운영센터의 관리자 권한관리 분류 체계는 서비스 정보 및 사용자의 개인 프라이버시 정보의 안전성과 효율성을 보장하고 있으며, 이는 도시통합운영센터가 다루는 정보의 분류와 관리자 체계의 분류를 통해 이루어진다.

위 표는 표 7의 내용을 바탕으로 분석하였으며, 각 요소들을 통해 기존 서비스가 관리자 권한관리 체계의 부재로 인해 관리자가 모든 정보를 제어 할 수 있는 빅브라더와 같은 안전성의 문제를 가지고 있다는 것이 분석된다. 또한, 서비스에 대한 모든 설정 권한을 통해 서비스가 변질될 경우, 서비스의 효율성에 대한 문제도 발생할 수 있다. 이러한 문제점은 최종적으로 해당 서비스에 대한 신뢰도 하락으로 이어지게 된다.

그러나 본 제안 방안의 관리자 권한관리 체계 분류는 관리자의 권한을 분산하여 관리하고, 사용자의 민감한 정보에 대해서는 최고 수준의 관리자 권한을 요구 하는 등, 도시통합운영센터가 다루는 정보에 대한 안전성을 보장하고 있다. 또한, 관리자의 권한을 분류하고 상호 감시체계를 통해 해당 정보에 대한 악의적인 접근을 차단하여 서비스의 효율성 및 가용성을 보장한다.

서비스 및 사용자의 정보와 시스템 전반에 걸친 제어 정보 등의 권한관리 체계를 통해 서비스가 안전하게 제공되면, 이는 결국 도시통합운영센터의 신뢰도 향상과 직결되게 된다.

V. 결론

다양한 서비스가 제공되는 미래 도시인 u-City에서 다양한 정보를 관리하고 서비스를 제공하기 위한 도시통합운영센터는 필수적인 요소로 부각되고 있다. 이를 위하여 현재 다양한 정보의 관리 및 서비스의 효율적인 제공을 위한 연구가 진행되고 있다.

도시통합연구센터의 중요성이 부각되는 커다란

이유 중 하나는 바로 도시 전체가 하나의 네트워크를 통한 정보의 전송과 이를 통한 서비스 제공을 위한 부분이다. 그러나 도시통합운영센터의 정보 관리 및 서비스 제공에 대한 연구가 활발한데 반하여, 이러한 정보를 관리하고 서비스를 보다 안전하게 제공하기 위한 관리자의 권한에 대한 연구는 미비한 실정이다.

이에 따라 본 논문에서는 이에 대한 관리자 권한 관리를 위한 체제 분류에 관하여 연구하였으며, 이를 위하여 도시통합운영센터가 다루게 될 정보의 분류 및 관리자가 관리할 수 있는 정보를 Class별로 분류하였다. 또한, 이를 통한 안전성 및 효율성에 대해 분석하였다.

본 논문의 연구 내용이 u-City내에서 주요한 기관으로 발전할 도시통합운영센터의 관리자 권한관리 체계 개선에 활용될 수 있을 것으로 기대된다.

참 고 문 헌

[1] u-City 협회, “도시통합운영센터 플랫폼 표준화 방안 연구”, 2007. 5.

[2] 김은형, “효율적인 u-City 서비스 구현을 위한 도시정보통합연계 방안”, *u-City 도시통합운영센터 워크샵*, 2007. 4

[3] KT u-City 본부, “KT u-City 추진사례 및 전략”, 2005.

[4] 한국정보사회진흥원, “u-City IT 인프라 구축 가이드라인”, 2008.

[5] 이계원, “도시통합운영센터 현안과제 및 개선방안”, *정보화정책*, 제15권, 제4호, pp. 69-86, 2008.

[6] 한국정보보호진흥원, “u-City 통합운영센터 정보보호참조모델 연구”, 2008. 12.

[7] 윤심, “전국 지자체 u-City 추진현황 분석”, *제9회 전자정부 컨퍼런스* 2007, 2007. 5.

[8] 이익섭, 김호성, 이완석, “u-City 서비스 정보보호 위협 및 보호대책”, *정보보호학회지*, 제18권, 제2호, pp. 67-75, 2008. 4.

[9] ISO, "ISO/IEC 27001:2005 Information technology --Security Techniques -- Specification for an Information Security Management System", 2008. 10.

이 완 석 (李玩錫)

1991년 5월 : Va. Tech. 전산과학과 학사 졸업

2001년 2월 : 동국대학교 정보보호학과 석사 졸업

2004년 9월～현재 : 성균관대학교 전자공학과 박사과정

1994년 7월 ～ 96년 6월 : 현대정보기술 사원

1996년 7월～현재 : 한국정보보호진흥원 u-IT서비스보호팀장

관심분야 : 정보보증, 정보보호 제품 평가, 정보통신기반보호, 신규 IT서비스 보호 등

고 웅 (高雄)

2008년 2월 : 순천향대학교 정보보호학과(공학사)

2008년 3월~현재 : 순천향대학교 정보보호학과 석사과정

관심분야 : 정보보호, 보안성 평가, 개인정보보호, 유비쿼터스 어플리케이션 보안, ID관리 등

원 동 호 (元東豪)

1976년~1988년 : 성균관대학교 전자공학과 (공학사, 공학석사, 공학박사)

1978년~1980년 : 한국전자통신연구원 전임연구원

1985년~1986년 : 일본 동경공업대 객원연구원

1988년~2003년 : 성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장.

1996년~1998년 : 국무총리실 정보화추진위원회 자문위원

2002년~2003년 : 한국정보보호학회장

현재 : 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, 정보통신부지정 정보보호인증기술연구센터 센터장, IT보안성평가연구회 위원장

관심분야 : 암호이론, 정보이론, 정보보호 등

여 상 수 (呂相壽)

1997년~2005년 : 중앙대학교 컴퓨터공학과 (공학사, 공학석사, 공학박사)
2006년 3월~2007년 2월 : 단국대학교 강의전임강사
2007년 2월~2008년 1월 : 큐슈대학교 정보공학부 방문연구원
2008년 2월~2009년 2월 : (주)비티웍스 연구개발본부 부장
2009년 3월~현재 : 목원대학교 컴퓨터공학부 교수
관심분야 : 정보보호 기술 및 정책, 멀티미디어 시스템, 임베디드 시스템, 유비쿼터스 보안 등

곽 진 (郭鎭)

1994년~2006년 : 성균관대학교 전자공학과 (공학사, 공학석사, 공학박사)
2006년 4월~2006년 11월 : 일본 큐슈대학교 시스템정보공학부 방문연구원
2006년 8월~2006년 11월 : 일본 큐슈시스템정보기술연구소 특별연구원
2006년~2007년 2월 : 정보통신부 정보보호기획단 개인정보보호팀 통신사무관
2007년 2월~현재 : 순천향대학교 정보보호학과 교수
관심분야 : 암호프로토콜, RFID 시스템 응용 보안, 개인정보보호, 정보보호제품 평가, u-City 정보보호 기술 등