u-City 통합운영센터의 시스템 보안 관리 대책에 대한 연구

김영수*, 박석천*
*경원대학교 소프트웨어학부

Strategies of System Security Control in u-City Management Center

Kim, Young Soo*, Park, Seok-Cheon*
Division of software Kyungwon University
E-mail : zestys@gmail.com, scpark@kyungwon.ac.kr

요 약

유비쿼터스 사회가 도래함에 따라 유비쿼터스 기술을 도시에 적용한 u-City가 개발되고 있다. u-City는 다양한 정보화 기기들이 존재하며 정보화 기기 사이를 연결하는 다양한 네트워크 기술이 상존한다. u-City의 핵심 요소인 u-City 통합운영센터는 u-City 내의 모든 서비스를 처리하도록 설계되었으며, 도시를 통제·관리하는 중요한 업무를 수행한다. 이 중에서 보안관리 업무는 시스템에서 수집, 가공, 산출하는 데이터 및 정보의 보안유지를 위해 중요한 부분이다. 따라서 본 논문에서는 u-City 통합운영센터의 보안유지를 위한 기술적, 물리적, 관리적인 측면에서 보안관리 대책을 제시하였다.

1. 서론

유비쿼터스 사회가 도래함에 따라 유비쿼터스 기술을 도시에 적용한 u-City가 국내·외적으로 활발히 개발되고 있다.

u-City는 도시 생활 서비스의 지능화를 통한 도시민의 생활의 편익과 지역 산업의 지능화 및 특화를 통한 도시 경쟁력 강화를 추구하고 있으며 유비쿼터스 IT 기술을 이용하여 교통, 환경, 시설물 관리, 도시안전관리, 문화 등의 다양한 도시 활동을 정보화하고자 한다. 또한 도시 특화 산업의 육성을 위해 지역도시의 경제 활성화를 위한 특화 산업을 포함하고 있으며, 유·무선통신, RFID, USN 등을 적용하여 도로, 건물, 시설물 등의 도시 인프라를 지능화하고자 한다.

이를 위해 u-City 통합운영센터가 등장하게 되었다. u-City 통합운영센터에서는 기존에 분리되어 운영되었던 각 서비스별 센터를 u-City 전체를 대상으로 통합 운영할 수 있도록 통합 GIS를 기반으로 안전/교통/생활/행정 전반에 걸쳐 총괄 운영하는 기능을 수행한다[1].

u-City 통합운영센터의 관리 업무는 센터 시스템에 대한 관리계획, 운영상태관리, 변경관리, 보안관리, 백업관리, 유지보수, 성능관리 등이 있다.

특히, 보안관리 업무는 시스템에서 수집, 가공, 산출하는 데이터 및 정보의 보안유지를 위한 중요한 부분이다.

본 논문에서는 u-City 통합운영센터의 보안유지를 위해서 기술적, 물리적, 관리적인 측면에서의 보안관리 대책에 대해서 제안한다.

* 일반대학원 전자계산학과 석사과정
** IT대학 정교수(교신저자)

2. 관련연구

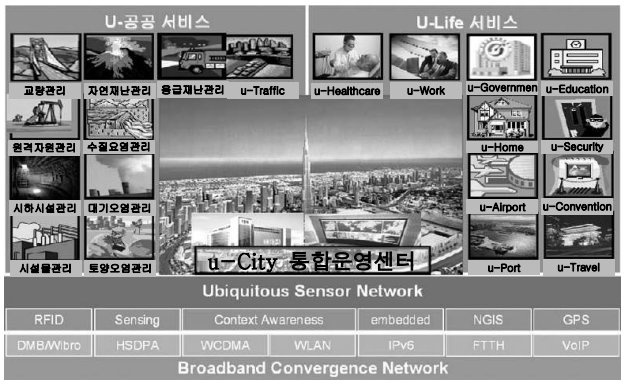
2.1 u-City

u-City는 'Ubiquitous City'의 준말로서 유비쿼터스 기반기술과 첨단 IT인프라에 의하여 정보통신, 행정, 건설 등 도시기능이 이루어지는 신 개념의 도시를 말하는 것이다[2][3]. 즉, 첨단 정보통신 인프라와 유비쿼터스 정보기술을 도시공간에 융합하여 도시생활의 편의증대와 삶의 질을 향상시키고, 체계적인 도시 관리에 의한 시민안전보장, 복지향상, 신산업창출 등 도시의 제반기능을 혁신시킬 수 있는 유비쿼터스 기반의 신도시를 말한다.

기존의 도시의 경우 도시가 개발이 된 상태에서 정보통신인프라를 구축하고, 특정부문과 영역에 한정되어 유비쿼터스 컴퓨팅 서비스가 제공되는 것이었다면, u-City는 도시개발의 계획단계에서부터 네트워크시스템의 구축을 통해 상시적인 유비쿼터스 컴퓨팅기술의 일상적 실현이 이루어지는 도시라는 점에서 차이가 있다.

2.2 u-City 통합운영센터

u-City 통합운영센터는 도시의 지능형 교통, 물류, 건물, 시설물 등 첨단화된 기반시설을 도시 전체적으로 관리하고 체계적으로 통제할 수 있는 기능을 수행한다.



[그림 2.1] u-City 통합운영센터의 개요

u-City 통합운영센터는 그림 2.1과 같이 u-City 내 통신망, 교통망, 시설물 등의 각종 센서로부터 도시정보를 수신하고 이를 통합적으로 분석하여 도시를 효과적으로 운영, 관리하고, 거주민이나 관련 기관에 분석된 도시정보를 실시간으로 배포·제공한다. u-City 통합운영센터를 통해 가정, 지역, 도시에 대한 서비스 발굴 및 통합으로 도시전체를 하나로 연결시켜줄 뿐 아니라, 단위 서비스 간의 통합에서부터, 도시를 구성하는 조직 사이의 수직적 통합과 각각의 계층에 놓인 서비스 사이의 수평적 통합을 구현한다. 이와 같은 u-City 통합운영센터는 통합운영플랫폼을 기반으로 도시통합운영센터, 고객 센터 및 전산실 등의 부대시설과 공공서비스(시설물관리, 환경, 교통, 안전, 방재, 종합행정) 관리 기능 등으로 구성된다[4].

2.3 u-City 통합운영센터의 시스템 관리 업무

u-City 통합운영센터는 u-City에서 운영될 다양한 u-Service의 정보매체로의 유익한 정보를 수집-가공-배포하기 위한 수단으로, 개별적 콘텐츠 전달의 한계성 및 비경제적인 인프라 구축, 서비스의 중복 개발 등을 지양하고, 외부기관과의 유기적인 연계 및 확장을 위해 반드시 필요한 u-City의 핵심부분으로, u-City 통합운영센터의 전반적인 시스템을 관리하는 업무는 다음 표 2.1과 같다[5].

<표 2.1> u-City 통합운영센터의 시스템 관리 업무

시스템 관리계획	- 시스템 관리(운영상태관리, 변경관리, 보안관리, 유지보수(장애관리), 성능관리 등)의 업무 수행 전반에 관한 안전관리계획 수립 등의 업무를 포함
운영상태 관리	- 시스템 구성요소에 대한 모니터링을 통하여 이상 징후를 발견, 기록, 분류, 통지하여 해당 업무 담당자들이 조치를 수행하도록 하는 업무
변경관리	- 시스템 구성요소에 대한 변경사항 발생시의 변경 신청과 검토 및 승인 업무
보안관리	- 시스템에서 수집, 가공, 산출하는 데이터 및 정보의 보안유지를 위한 업무
유지보수	- 현장시설 유지관리, 센터 시스템 장애관리, 문서 기록관리 업무
성능관리	- 시스템 성능관리, 시스템 성능개선, (성능 관리·개선) 문서 기록관리 등의 업무

u-City 통합운영센터의 여러 가지 시스템 관리 업무 중에서 특히 보안에 관련된 업무는 매우 중요한 부분으로, 각종 수집된 정보와 이를 가공하여 만들어진 새로운 정보들이 일반인에게 노출 되었을 때에는 개인적·사회적으로 심각한 파장을 불러일으킬 수 있고, 국가 전체가 공황상태에 빠질 수 있다.

3. u-City 통합운영센터의 보안 대상 및 적용 범위

u-City 통합운영센터의 보안관리는 시스템에서 수집, 가공, 산출하는 데이터 및 정보의 보안유지를 위한 업무로, 이에 대한 보안 대상 및 적용 범위는 다음의 표 3.1과 같다.

<표 3.1> 보안 대상 및 적용 범위

보안대상		적용범위
서버 및 OS	- 정보시스템 운영의 기본이 되는 것으로 이의 손상 및 침해시 전 업무의 마비가 초래될 수 있는 중요한 보호 대상임	- 사용자 계정관리 - 패스워드 관리 - 시스템 권한 제한 및 분리 - 서버 운영체제의 취약점 관리
DB	- 각종 DB 등 운영 업무에 관한 제반 정보들을 무단 변경이나 파괴로부터 보호	- 데이터베이스 사용자 분류 및 역할 구분 - 사용자 권한 관리
네트워크	- LAN, 인터넷, 전용선 등을 통한 신뢰성 있는 정보 전송 확보	- 외부에서 내부로의 네트워크 상의 접근에 대한 접근통제 및 감시, 인증 - IP address 관리 및 보호 - 외부 기관과의 네트워크 연계에 대한 보안 - 네트워크 logging 관리
응용프로그램	- 정보 처리 및 서비스 제공을 위한 프로그램의 취약점 보안 및 비인가자의 응용프로그램 무단 접속을 방지	- 응용프로그램별 접근 통제 - 단위 업무별 접근통제 - 응용 프로그램 사용상태 관리
클라이언트	- 시스템 자원 및 응용프로그램을 사용하기 위해 쓰이는 PC에 대한 보호	- 개인 PC 에 대한 패스워드 관리 - 개인 PC의 자원(파일 및 디렉토리)에 대한 관리

4. u-City 통합운영센터의 보안관리 대책

4.1 기술적 보안관리 대책

u-City 통합운영센터의 기술적 보안은 DB, 하드웨어, 소프트웨어, 네트워크 등에 대한 접근통제, 변경관리 등의 보안유지 업무를 말한다.

이에 대한 주요 보안대책은 다음의 표 4.1과 같다.

<표 4.1> 기술적 보안관리 대책

구 분	주요 보안대책
사용자 식별 및 인증	- 각 개인에게 고유의 사용자 ID를 부여하여 권한이 허용된 시스템만을 사용하도록 함 - 비밀번호의 주기적 변경, 입력 횟수 등을 시스템 측면에서 강제적으로 통제하도록 함 - 사용자의 식별과 인증을 일원화하여 통합적으로 관리함
시스템 자원의 접근통제	- 데이터베이스의 접근권한을 사용자 별로 분류함 - 임의의 사용자/그룹에 대한 접근 모드를 설정함
감사 및 관리	- 시스템 이용에 관한 기록(Login시 실패한 사용자의 ID 식별/인증 처리, 관리자의 특별권한 사용 등)을 수집하여 감사함 - 불법 사용에 대한 처벌 등을 홍보하여 시스템의 부정 사용을 억제함
데이터 복원	- 사용자의 운영 오류, 하드웨어 결함, 의도적 데이터 파괴, 천재지변 등의 재해로부터 데이터를 보호하고 무중단 운영을 위한 백업 대책을 마련함
네트워크 보안	- 상대방 인증, 메시지인증, 네트워크 패킷에 대한 접근 통제 등 네트워크 상의 데이터 보안대책을 마련함

4.2 물리적 보안관리 대책

u-City 통합운영센터의 물리적 보안은 센터 시설에 대한 출입통제 및 우발적 사고, 화재 발생 시의 대응 업무를 말한다.

데이터 및 정보보호체계에서 근간을 이루는 기본 통제선 항목의 일부로서 센터 시스템에 가해질 수 있는 물리적인 구성요소에 대한 피해를 최소화하기 위한 것으로 접근통제와 시스템의 파손 대비를 목적으로 한다.

이에 대한 주요 보안대책은 다음의 표 4.2와 같다.

<표 4.2> 물리적 보안관리 대책

구 분	주요 보안대책
출입 통제	- 센터 내 출입인원 통제 - 출입권한의 승인, 변경 관리 - CCTV 설치 및 운영 - 건물 내 핵심지역의 접근 통제
장비 보안	- 서버, 네트워크 장비를 보안이 통제되는 장소에서 운영 및 보관 - 장비의 위치, 네트워크 구성요소와 접속장치, 하드웨어, 소프트웨어의 등록 사항을 기록 및 관리
화재 예방 및 감시 시스템	- 화재 초기 진압을 위한 장비 설치 및 방화구역 설치 - 화재 안전시설의 운용 실태와 인화성 물질의 사용 여부 등을 확인 - 전기장치 및 난방 시설의 정비 상태 등을 수시 확인 - 화재감시 시스템은 독립적으로 설치 - 소화전을 설치하고 소방훈련, 화재대비 훈련을 주기적으로 연습
각종 설비의 보호 및 안전	- 무정전 전원설비, 항온항습, 공기정화 설비의 유지관리 - 고층일수록 진동의 영향을 크게 받을 수 있으므로 심한 진동을 일으키는 기기에 대한 적절한 위치 선정 - 부식성 가스, 증기, 염분 등의 환경으로부터 안전한 곳에 설치 - 센터 내외의 환경을 청결히 함 - 동물 침투 예상 지역에 보호 철망 설치 - 정기적 점검 - 장애시 처리절차의 수립
감사	- 주기적 시설물 및 장비에 대한 점검, 감사 - 사전 예고 없이 각종 시설물 및 장비에 대한 점검, 감사

4.3 관리적 보안관리 대책

u-City 통합운영센터의 관리적 보안은 보안 메뉴얼 작성, 보안교육 감사 등의 업무를 말하며, 사용자의 보안상의 책임한계를 명확히 하고, 사용절차 등의 보안 환경을 사용자 교육을 통하여 보안

의식을 가지도록 하여야 한다.

이에 대한 주요 보안대책은 다음의 표 4.3과 같다.

<표 4.3> 관리적 보안관리 대책

구 분	주요 보안대책
보안 매뉴얼 작성	- 보안 S/W 운영 절차서, 방화벽 운영절차서, 시스템 변경 절차서, ID 및 패스워드 관리 절차서 등 시스템 보안관리 지침 및 절차를 메뉴얼로 작성하여 보급함
보안 교육/훈련	- 철저한 보안 교육을 통하여 사용자들의 보안상의 실수를 예방하고 외부 침입 시도 시, 보고체계를 갖추도록 교육을 실시함 - 다양한 상황을 가상한 현장모의훈련(FTX)을 실시함
감사	- 시스템 보안 체계 수립 시, 당시의 목표와 보안 메뉴얼(지침)에서 규정한 내용들이 충분히 이루어지는지를 점검하고, 파악된 문제점을 검증하여 보안 시스템에 반영함으로서 정보보안 체계가 적정선을 유지할 수 있도록 함

이상과 같이 u-City 통합운영센터에서의 보안관리 대책에 대하여 기술적·물리적·관리적 측면에서 제시하였다.

5. 결론

도시는 농업혁명 이후 형성된 고대도시로부터 시작되어, 산업혁명에 기반 한 근·현대 도시를 거쳐서 정보통신 인프라와 정보서비스를 도시의 다양한 구성요소에 접목시키는 노력이 진행되면서 도시 내 주요기능에 u-서비스가 적용된 u-City가 등장하였다.

u-City란 IT 인프라, 기술 및 서비스를 주거, 경제, 교통, 시설 등 도시의 다양한 구성요소에 적용한 미래형 첨단도시이다. u-City 구축을 통하여 u-교통이나 u-문화·관광 등 편리한 도시, u-방범·방재, u-시설관리 등 안전한 도시, u-환경 등 쾌적한 도시, u-보건복지 등 건강한 도시를 구현하여 도시민의 삶의 질을 제고할 수 있다.

이러한 u-City의 효율적인 운영을 위해 안전/교통/생활/행정 전반에 걸쳐 총괄 운영하는 기능을 수행하는 u-City 통합운영센터가 등장하게 되었다.

이렇게 중요한 기능을 수행하는 u-City 통합운영센터가 여러 가지 보안상의 문제로 제 기능을 하지 못하면 도시 전체가 마비되고, 도시민들은 공황상태에 빠질 수 있다. 이를 방지하기 위해 u-City 통합운영센터의 보안대상 및 적용 범위를 분석하고, u-City 통합운영센터의 보안 유지를 위한 보안관리 대책을 기술적, 물리적, 관리적 측면에서 제시하였다.

이러한 u-City 통합운영센터의 보안관리 대책이 효과적으로 이루어지기 위해서는 무엇보다도 u-City 통합운영센터의 시스템 유지 및 장애관리가 매우 중요하다.

본 논문에서 제시된 u-City 통합운영센터의 보안관리 대책은 현재 구축 혹은 운영 중 인 u-City 통합운영센터의 보안 관련 업무에 활용될 수 있을 것이다.

[참고문헌]

[1] 김성훈 외, "u-City 프라이버시 보호방안 연구", 한국정보보호진흥원, 2006. 12

[2] 유남철, "u-City 핵심성공요인 및 e-Seoul 서비스모델소개", 전자부품연구원 전자정보센터 보고서 2006. 9.

[3] 전영옥, "u-City의 성공적인 개발 모델과 시사점", 삼성경제연구소, 2006. 6.

[4] 임규관, 김지선, "u-City 인프라로서의 u-City 운영센터 및 플랫폼" TTA 저널 No.112, 2007. 7

[5] 이재근 외, "u-City IT인프라 구축 가이드라인 및 인증방안 연구", 한국정보사회진흥원, 2007. 12