情 報 保 護 學 會 誌
第18卷 第2號, 2008. 4

u-City 서비스 정보보호 위협 및 보호대책

이 익 섭*, 김 호 성*, 이 완 석**

요 약

유비쿼터스 기술의 보급으로 우리 생활에 밀접한 연관이 있는 도시시설 등이 IT기술과 융합되어가고 있다. 이로 인해 개별 네트워크에서 운영되던 각종 IT 서비스들도 u-City 서비스로 융합되고 있다. 하지만, u-City 안에서 새로이 융합되는 신규 IT서비스들이 구축되는 과정에서 보안요소의 고려 및 적용이 미흡할 경우에 u-City 서비스의 안전성 및 신뢰성에 심각한 문제를 야기할 수 있다. 이를 해결하기 위해, 본 논문에서는 u-City 서비스에서 발생 가능한 정보보호 위협을 분석하고 이를 극복하기 위한 정보보호대책 및 정책 과제를 제시하도록 한다.

Ⅰ. 서 론

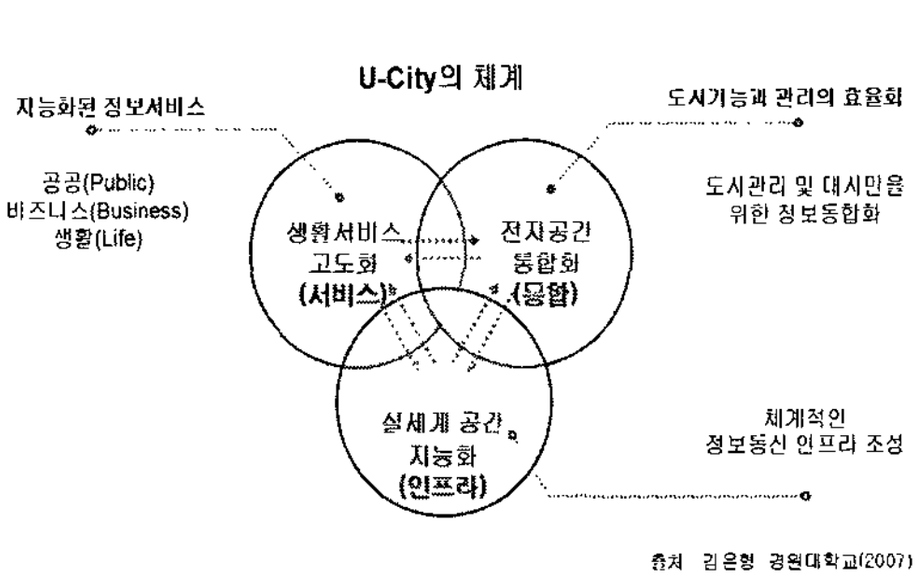
유비쿼터스 기술의 보급으로 우리 생활에 밀접한 연관이 있는 도시시설 등이 IT기술과 융합되어가고 있다. 이로 인해 개별 네트워크에서 운영되던 서비스들도 u-City 서비스로 융합되고 있다. u-city개념이 도입되면서 민원처리, 안전관리 등의 업무가 하나로 통합되어 유기적으로 관리되고 정보를 공유할 수 있는 체계로 발전하고 있다. 유비쿼터스 사회의 도래와 u-City의 구축, 확산의 이면에는 다양한 정보매체를 통한 비윤리적, 반사회적 컨텐츠가 범람하고 개인의 재산과 생명을 위협하는 사이버 범죄 등 정보 보안 위협이 날로 증대되고 있다. u-City 안에서 새로이 융합되는 신규 IT서비스들이 구축되는 과정에서 보안요소의 고려 및 적용이 미흡할 경우에 u-City 서비스의 안전성 및 신뢰성에 심각한 문제를 야기할 수 있다. 이를 해결하기 위해서, 본 논문에서는 u-City 서비스에서 발생 가능한 정보보호 위협을 분석하고 이를 극복하기 위한 보호대책 및 정책과제를 제시하도록 한다.

Ⅱ. u-City 개요 및 국내외 동향

본장에서는 u-City 정의를 포함한 개요와 국내외 구축 현황에 대해 정리하였다.

2.1. u-City 서비스 개요

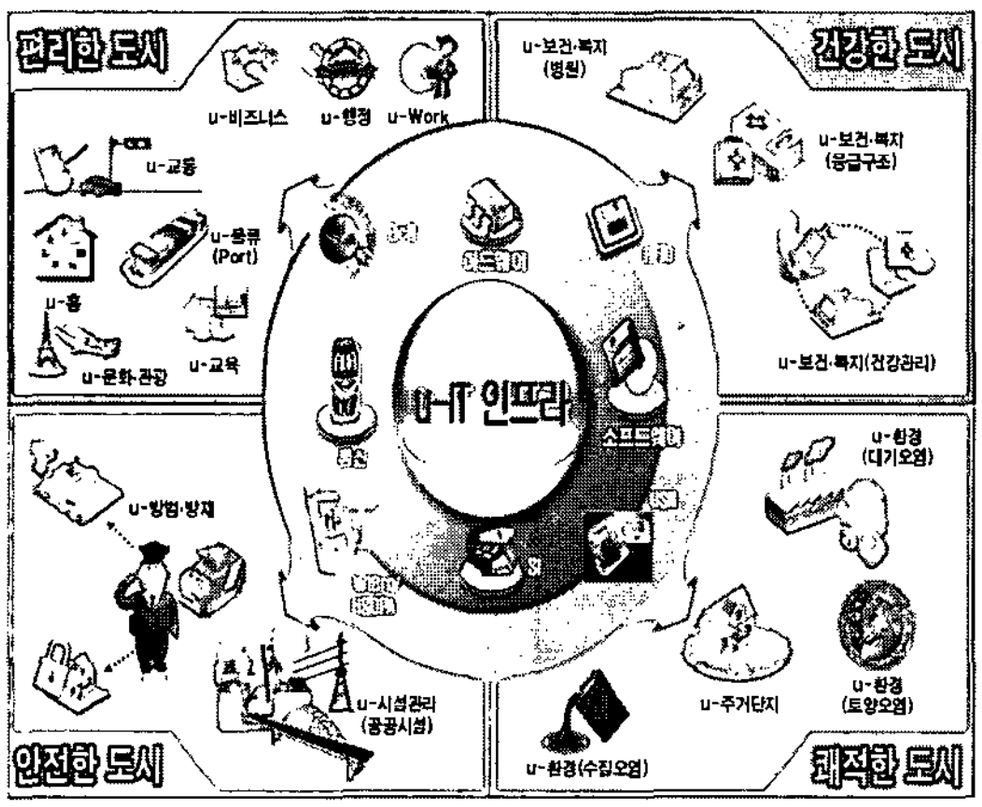
현재 국내에서는 u-City 개념 정립과 관련 기술 분석 및 개발이 동시에 진행되고 있으며, u-City에 대한 정의를 다음과 같이 내릴 수 있다. u-서비스는 실생활에서의 필수 서비스들을 유비쿼터스 기술을 활용하여 사용자 중심적으로 좀 더 편리하게 제공하기 위한 것이며, u-City는 도시 관리, 주민 편의 등 도시를 기반으로 각종 u-서비스를 도시민에게 제공하기 위한 서비스의 유기적인 조합을 통해서 이루어 진다. 이를 개념적으로 정리하면 u-City는 [그림 1]과 같이 실세계 공간의 지능화, 생활서비스의 고도화, 전자 공간의 통합을 통해 도시민에게 안전하고, 쾌적한 생활을 제공하는 신개념의 도시로 정의할 수 있다[1].



〔그림 1〕 u-City 정의 및 체계

* 한국정보보호진흥원 IT기반보호단 u-IT서비스보호팀 연구원 ({islee, hoseong}@kisa.or.kr)
** 한국정보보호진흥원 IT기반보호단 u-IT서비스보호팀 팀장 (wsyi@kisa.or.kr)

u-City는 [그림 2]와 같이 도시에 센서, 태그, 단말기 등의 하드웨어, 미들웨어, 플랫폼 등 소프트웨어, BcN, USN, WiBro, 무선메쉬 네트워크 등 통신 인프라를 이용하여, u-교통, 교육, 문화, 행정(편리한 도시), u-방범·방재, 시설관리(안전한 도시), u-토양·대기·수질 관리(쾌적한 도시), u-병원, 응급구조, 건강관리(건강한 도시) 등 다양한 응용서비스의 구현이 가능하다[2].



〔그림 2〕 u-City 인프라 및 서비스

u-서비스는 크게 공공, 비즈니스, 생활의 3가지 형태로 분류 될 수 있으며, 서비스 제공을 위한 인프라 즉, 단말, 통신인프라, 시스템 및 SW로 구성될 수 있다. u-서비스 각각은 특정한 목적을 갖고 다양한 형태로 추진되지만, 각 서비스에서 사용되는 요소기술들은 비교적 제한적이다.

〔표 1〕 u-City 구성요소 및 특징

구 분	특 징
u-City 운영센터	· 도로 등 도시인프라와 공항 등의 도시기반시설 등을 유비쿼터스 환경으로 실시간 관리
서비스 플랫폼	· 누구든지, 어디서나, 언제라도 서비스를 이용하기 위한 공통 플랫폼 필요 · u-City 서비스에 대한 품질 감시 및 서비스, 인프라에 대한 운용 관리 시스템
네트워크	· 도시라는 물리적 공간을 전자적 공간으로 구현하는 기반 · 도시의 모든 사람, 사물, 기기 들을 끊김없이 연결
단말	· 정보를 인식하고 수집하기 위한 센서 · 누구든지, 어디서나, 언제라도 서비스를 이용하기 위한 단말기

2.2. u-City 국내외 구축현황

세계 각국은 [표 2]와 같이 도시의 IT인프라를 광대역화 및 무선화함으로써 언제 어디서나 접속가능한 인터넷 도시의 구현을 중점으로 추진 중이다.

〔표 2〕 국외 u-City 추진현황

지역	명칭	내용
일본 오사카	도시재생 프로그램	GPS탑재 휴대폰을 이용한 최적 경로 검색, RFID, CCTV 부착 자판기를 활용한 유아관리 서비스 등 12개 실증실험 추진 중
홍콩	Cyber Port	광통신망 기반의 100M~1Gbps 인터넷 서비스 제공 및 Intelligent Office 구현을 목표로 추진 중
두바이	Internet City	중동의 IT허브 구현을 목표로 다국적 IT 기업을 위한 VoIP 등 유무선 기반환경 구축
덴마크 코펜하겐	Crossroads	2014년까지 'mCluster' 구현을 목표로 다양한 모바일 기반 서비스 제공 예정
핀란드 헬싱키	Arabianranta	Virtual Village Portal Service를 제공을 위해 2010년까지 1Gbps급 통신환경 구축 중
싱가포르	One North	2020년까지 세계적인 의학·문화·미디어 허브 구현을 목표로 Bandwidth On Demand, VoIP 등 원활한 통신인프라 기반 구축 예정

국내에서는 [표 3]과 같이 현재, 전국 20여개 지자체에서 u-City 추진을 표방하며 USP(Ubiquitous Strategy Plan)를 수립 중이거나 초기 구축단계에 있다[3].

이와 더불어 정부차원에서의 활동도 활발히 진행되고 있다. (구)정보통신부는 "u-City추진 활성화 기본계획"에 u-City 추진을 위한 범정부 추진체계 및 u-City지원센터를 설립, 운영토록 하였으며, 국토해양부의 "유비쿼터스 도시의 건설 등에 관한 법률(안)"에 유비쿼터

〔표 3〕 국내 u-City 추진현황

구 분	도 시 명
기존 도시	서울, 부산, 대전, 광주, 울산, 인천, 전북, 충남 홍성, 충북 오송, 전주, 양산, 포항, 강릉, 제주
신도시	공주·연기군(행정복합도시), IFEZ, 아산 탕정, 화성 동탄, 파주 운정, 판교, 용인 흥덕, 수원 광교

스도시위원회 · 유비쿼터스 도시사업협의회 등의 지원 조직을 둘 수 있도록 하였고, 행정안전부의 "u-Life21 기본계획"에도 범정부 추진체계를 계획하고 있다[4][5][6].

u-City 추진 활성화와 기반조성을 위해 한국정보사회진흥원에 "u-City지원센터"가 설립되어 현재 운영 중이며, 한국정보보호진흥원에 "u-City정보보호 협의회"가 구성되어 "u-City 정보보호 기본계획"을 수립하는데 기여하고 있다. 또한 한국u-City협회의 u-City포럼에 u-City정보보호 워킹그룹이 운영 중이이며, u-City 정보보호의 기반 확산을 위한 활동을 전개하고 있다[7][8].

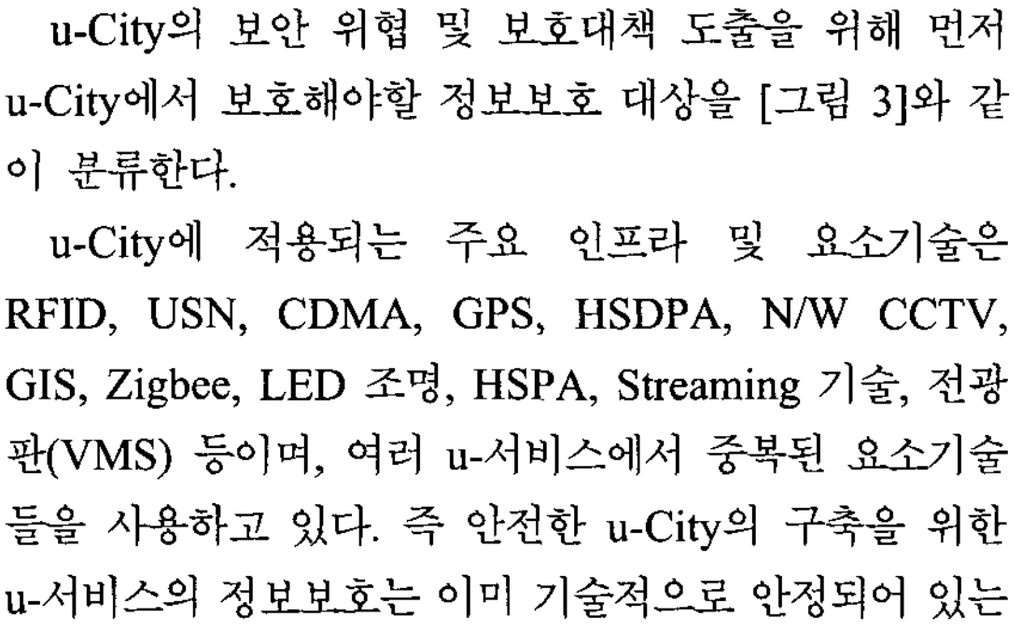
Ⅲ. u-City 서비스의 위협

본장에서는 u-City 서비스의 발생가능한 보안 위협에 대해 분석하였다.

3.1. u-City 서비스의 보호대상

u-City의 보안 위협 및 보호대책 도출을 위해 먼저 u-City에서 보호해야할 정보보호 대상을 [그림 3]와 같이 분류한다.

u-City에 적용되는 주요 인프라 및 요소기술은 RFID, USN, CDMA, GPS, HSDPA, N/W CCTV, GIS, Zigbee, LED 조명, HSPA, Streaming 기술, 전광판(VMS) 등이며, 여러 u-서비스에서 중복된 요소기술들을 사용하고 있다. 즉 안전한 u-City의 구축을 위한 u-서비스의 정보보호는 이미 기술적으로 안정되어 있는 요소기술들에 대한 적절한 보안 대책 마련이 그 선행 과제임을 알 수 있다. u-City 서비스를 구성하는 요소를 크게 인프라 계층, 인프라를 기반으로 직접 사용자에게 제공되는 서비스 계층 및 다양하게 제공되는 서비스의 결합에 의한 전자공간 통합계층으로 분류하였다.



〔그림 3〕 u-City 보호대상

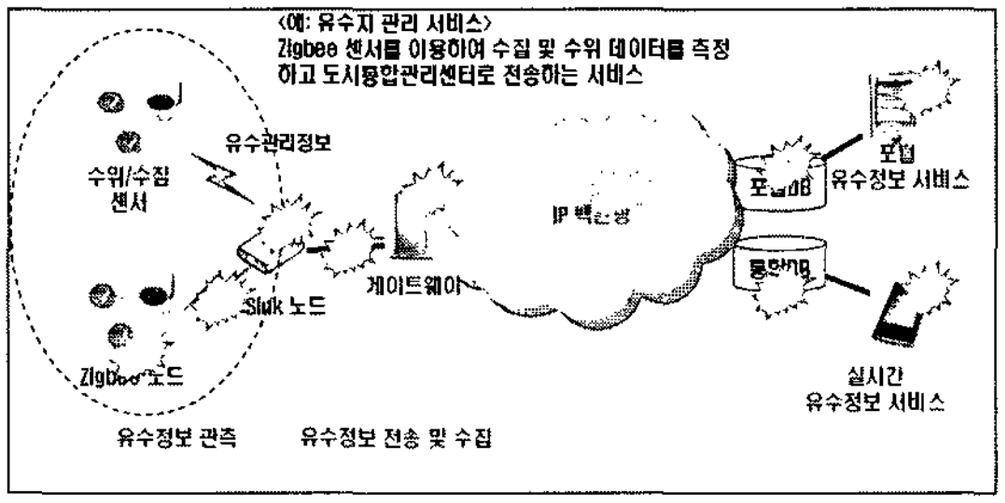
3.2. u-City 서비스의 정보보호 위협

u-City 서비스에 대한 정보보호 위협 분석은 앞서 분류한 정보보호 대상에 대해 현재 고려되고 있는 서비스 모델의 예를 활용하여 위협 분석을 실시하고 가능한 위협시나리오에 대해 제시하였다.

3.2.1 서비스 위협

가. u-City 공공서비스

공공서비스의 대표적인 서비스로 [그림 4]의 u-수질/수위 관리 서비스를 보면, Zigbee 센서를 이용하여 수질관련 데이터를 도시통합관리센터로 전송하는 수질관리 서비스와 초음파 수위센서를 통해 수위 데이터를 측정하고 도시통합관리센터로 전송하는 수위관리 서비스로 구성된다.



〔그림 4〕 공공서비스(u-수질/수위관리)의 위협

〔표 4〕 u-수질/수위 관리 서비스 위협

① 센서 복제 및 위치 변조로 인한 상황인지 정보의 무결성 훼손
② ZigBee 노드와 Sink노드간 데이터의 암호화 미비에 따른 도청으로 정보 노출
③ Sink노드의 접근통제 미비로 센서 정보 위변조 및 Sink 노드와 ZigBee노드의 상호인증 미비에 따른 Sink 노드의 기능 마비
④ Sink노드와 게이트웨이간 데이터 암호화 미비에 따른 도청으로 데이터 유출
⑤ 게이트웨이의 접근통제 미비에 따른 비인가자의 정보의 위변조
⑥ 게이트웨이와 통합서버의 DB간 데이터 암호화 미비로 데이터 유출
⑦ DB의 접근통제 및 암호화 미비에 따른 DB 저장 데이터의 노출 및 위변조
⑧ 포털서비스 단말 및 관리자 휴대단말 등 접근통제 미비로 단말 데이터 노출

u-수질/수위 관리 서비스에 대한 취약점은 수질수위 센서 복제 및 위치 변조로 인한 상황인지 정보의 무결성 훼손의 가능성 있으며, 전체 도출된 위협은 [표 4]와 같다.

u-수질/수위 관리 서비스 이외에 시설물관리서비스의 도시가스관 위치정보 위변조로 인한 굴착공사 오류로 도시가스 폭발 등이 발생하면, 도시기능 마비 및 도시민 안전에 위협이 발생할 수 있다. 교통정보 서비스는 중앙서버에 전달된 교통트래픽 상황정보, 차량사고지역 정보 등을 이용하여 교통제어를 하여야 하나, 게이트웨이에서의 기능마비 공격시 제어 오류로 교통대란이 발생될 수 있다. 재난방지를 위해 강물의 수위정보를 수집하는 센서 정보의 전송과정에서 악의적인 해커가 전송정보를 위변조하면, 홍수 등 재해에 의한 도시기능 마비의 우려가 존재한다.

나. u-City 비즈니스 서비스 위협

비즈니스 서비스 중 전시물 설비 관리 서비스는 [그림 5]과 같이 전시장의 고가 전시장비에 능동형 RFID 태그를 부착하여 전시물 정보를 제공하는 서비스이다.

전시물 설비 관리 서비스에 대한 취약점은 RFID 태그발행기 비인가접근을 통한 태그정보의 위변조의 가능성 있으며, 전체 도출된 위협은 [표 5]와같다.

전시물 설비 관리 서비스 이외에도 비즈니스 서비스의 식품이력 추적서비스에서 인증미비로 식품 RFID 태그의 유통기한 또는 원산지 정보를 위변조 하여 소비자 건강에 직접적인 위해와 유통질서의 혼란이 초래될 수

〔표 5〕 u-설비관리 서비스 위협

① RFID 태그발행기 비인가접근을 통한 태그정보의 위변조
② 태그에 비인가 리더의 과다 정보요청으로 태그전력 소모 및 서비스 방해
③ RFID 리더의 태그인식 방해를 위한 비인가 전파발생기 사용 및 리더의 절취
④ RFID 리더와 AP간 상호인증 및 전송 데이터 암호화 미비로 비인가 AP가 정보 유출하거나 도청
⑤ RFID 미들웨어에 대한 접근통제 미비로 비인가자에 의한 태그정보의 위변조
⑥ 응용서버 접근통제 미비로 비인가자에 의한 서비스 및 사용자 정보 위변조
⑦ 응용서버, 관리실간 데이터 암호화 미비로 도청을 통해 장비위치 추적 및 절취
⑧ 관리실 단말 및 UMPC에 대한 접근통제미비로 비인가자에 장비위치 노출

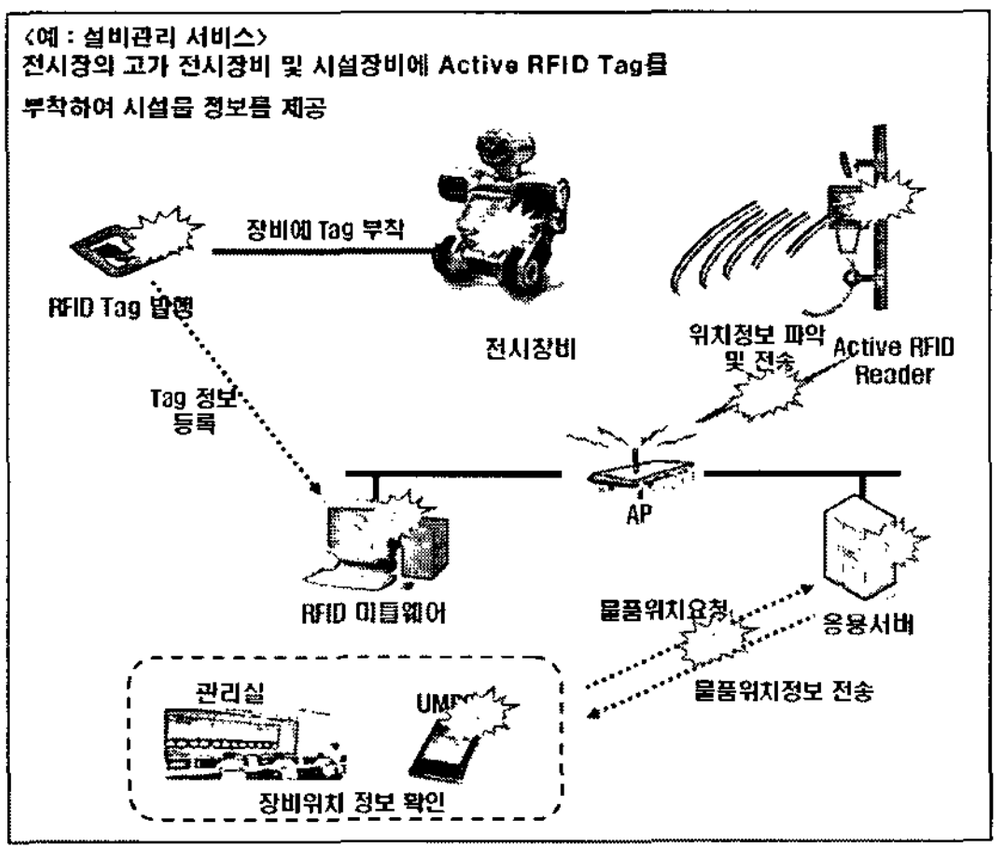
있다. 물류, 유통관리 서비스에서 인증미비로 출고 및 입고물품 수량정보 위변조와 함께 출고물품 대량 도난에 대한 인지 불가로 사후조치가 어려워 경제적 손실이 발생 가능하다. 전시물품 도난 관리 서비스에서 전시 물품에 부착된 RFID 태그의 전력소모 등의 공격을 통해 태그 기능을 정지시킴으로써 전시물품 도난의 위험 발생이 가능하다.

다. u-City 생활서비스 위협

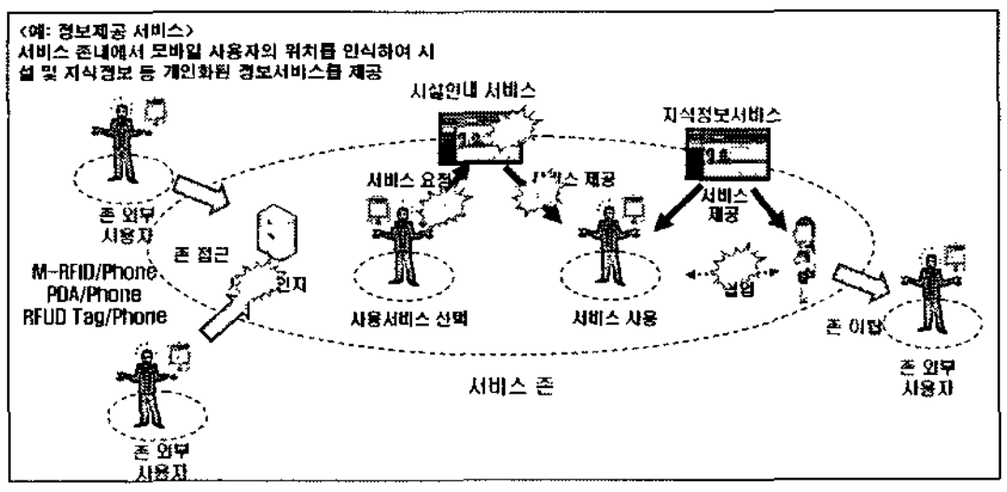
생활서비스 중 정보제공 서비스는 [그림 6]과 같이 서비스 존내에서 모바일 사용자의 위치 등을 인식하여 시설 안내 및 지식정보 등 개인화된 정보서비스를 제공하는 서비스이다.

정보제공 서비스에 대한 취약점은 서비스 존내 사용자 및 기기의 인증 미수행시, 비인가자의 정보 무단 이용의 가능성 있으며, 전체 도출된 위협은 [표 6]과 같다.

u-서비스 존 서비스에서 서비스 존 내에서 저장 및 관리되는 개인의 정보 이용행태, 취미 등의 민감한 정보



〔그림 5〕 비즈니스 서비스(u-설비관리 서비스)의 위협



〔그림 6〕 생활 서비스(u-정보제공 서비스)의 위협

〔표 6〕 u-정보제공 서비스 위협

① 서비스 존내 사용자 및 기기의 인증 미수행시, 비인가자의 정보 무단 이용
② 서비스 존내 사용자와 서비스 제공서버간의 전송 데이터가 암호화 미비시, 사용자의 위치정보 및 서비스 이용내역 노출에 따른 프라이버시 침해
③ 서비스 제공서버의 접근제어 미구현시, 위치정보 및 서비스 이용내역 노출에 따른 프라이버시 침해
④ 서비스 존내 사용자간 인증 기능 미구현시, 협업을 통한 비인가자에 대한 사용자 및 서비스 정보의 노출
⑤ 사용자의 서비스 존 이탈시, 사용자의 서비스 이용로그에 대한 안전한 저장과 관리가 이루어지지 않으면 사용자 프라이버시 침해

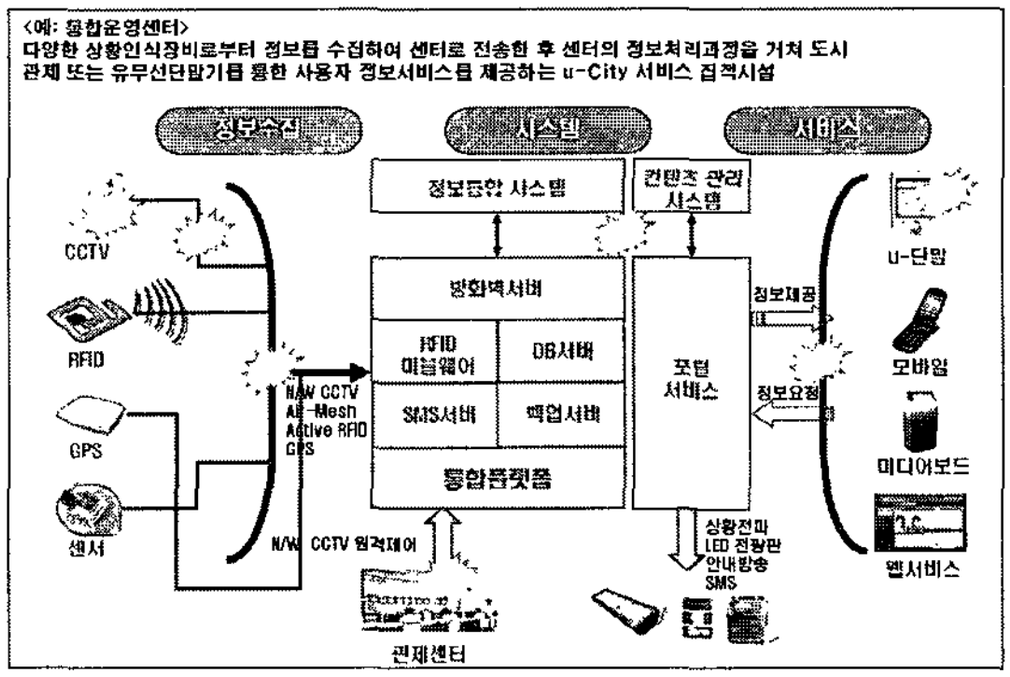
가 불법 수집, 가공 및 노출될 경우 개인 프라이버시 침해 발생 가능하며, 마케팅 수단으로 악용될 우려가 있다. 위치기반 서비스를 위해 수집되는 사용자 위치정보가 비인가자에게 노출될 경우, 사용자 프라이버시 침해 발생 및 신변 안전에 위협을 준다. 원격검침, 통합과금 서비스의 검침량 데이터 위변조로 인해, 사용자 요금 과다 부과로 인한 사용자 피해 및 서비스 업체 신뢰성 저하, 요금 누락으로 인한 업체의 피해발생이 가능하다. 응급환자 처치를 위하여 이송 중 병·의원 등 의료기관에 제공하는 개인정보 및 병력정보가 노출되어 프라이버시 침해의 우려가 있다.

3.2.2. u-City 통합계층 정보보호 위협

u-City 서비스를 통합 관리하는 도시통합운영센터는 [그림 7]과 같이 도시내 다양한 정보의 수집, 처리 과정을 거쳐 도시관제 또는 유무선 단말기를 통한 사용자 정보서비스를 제공하는 u-City 서비스 집적시설이다.

도시통합운영센터에 대한 취약점은 다양한 상황인식장비의 보안기능 미비시, 비인가장비의 기기 및 데이터 위변조 의 가능성 있으며, 전체 도출된 위협은 [표 7]과 같다.

u-City 통합계층에서 도시 전체의 관제, 관리 기능을 가지는 도시통합운영센터의 장애 발생시 서비스 중단 또는 오작동으로 도시기능 마비 및 도시민 안전에 중대한 위협을 초래될 수 있다. 각종 센서를 이용한 실시간 교통, 하천 수위, 긴급화재 등 상황정보와 시민 개개인의 정보 등 주요정보들이 집적되어 있어 해킹이 이루어질 경우 대량 정보유출로 사회문제화 될 수 있다. 또한



〔그림 7〕 통합계층 위협

〔표 7〕 도시통합운영센터의 위협

① 다양한 상황인식장비의 보안기능 미비시, 비인가장비의 기기 및 데이터 위변조
② 정보수집장치, 통합센터간 전송데이터 암호화 미비시, 주요 정보의 노출 및 위변조
③ 통합운영센터를 통한 서비스 결합 및 연동으로 서비스별 정보보호 보증수준 저하
④ 통합운영센터의 정보시스템 통합에 따른 데이터 결합/추론에 의한 기밀정보 노출
⑤ 관제센터와 통합운영센터간 전송 데이터의 암호화 미비시, 시설 및 설비에 대한 제어정보 위변조
⑥ 포털서비스시스템과 정보이용 단말간 데이터의 암호화 미비시 사용자 개인정보 및 서비스 이용내역 노출로 비즈니스 영업 기밀 및 프라이버시 침해
⑦ u-서비스 단말의 접근제어 미비시, 비인가자에 의한 정보 유출

u-City 서비스간 연동시 상이한 암호화 또는 인증 정책으로 인하여 주요 기밀정보의 외부 유출 가능성이 존재한다.

3.2.3. u-City 인프라 계층의 위협

u-City 서비스의 기반이 되는 인프라 계층에 대한 위협을 [표 8]과 같이 통신 인프라, 시스템 및 소프트웨어, 단말 별로 분석하였다

3.3. u-City 정보보호 진단 및 보호대책

한국정보보호진흥원에서는 07년도 하반기에 실제 u-City 구축 과정에 대한 정보보호 진단을 실시하였다. 진단은, 시범구축 중인 3개 테스트베드 6개 서비스를 대상

〔표 8〕 u-City 인프라 계층의 위협

취약점	위협의 종류
통신인프라	- USN 등 가입자망 및 유무선통신망으로 구성 - USN Sink노드와 게이트웨이간 데이터 위변조 및 서비스 방해 - RFID리더 주변에 비인가 전파발생기를 통한 통신 방해 - 사용자 휴대단말과 서버간 도청으로 사용자 위치정보 노출
시스템 및 소프트웨어	- 해커의 주요 DB 시스템에 대한 비인가접근으로 DB 위변조 - 서버에 저장 중인 로그에 불법접근하여 사용자의 서비스 이용정보 불법 획득 - RFID 미들웨어 해킹으로 전송을 위해 저장중인 태그정보 위변조
단말	- 상황인식센서, 영상표출장치, 개인휴대단말 등으로 구성 - 센서 위치 변조로 인한 상황인지 정보의 오류 발생 - 태그에 대한 과다 정보요청으로 태그전력 고갈 - CCTV 영상위변조, GPS 위치정보 노출 등 데이터 위변조

〔표 9〕 u-City 정보보호 진단 대상서비스

서비스명	서비스 개요
u-Safe	지능형 CCTV를 이용하여 도시, 주민의 안전을 지원
u-폐기물 관리	건축폐기물 운반차량의 위치를 실시간 모니터링하여 폐기물관리의 효율성을 향상하기 위한 서비스 제공
u-방문객	외부 VIP 방문시 이동단말, 로봇, 고정단말 등의 연계를 통해 다양한 정보 제공
u-커뮤니티	RFID 리더기로 직원의 RFID 태그를 인식하여 화장실 및 복도에서 동아리 활동, 영어 컨텐츠 등 개인 맞춤형 서비스 제공
u-회의실	웹기반 회의실 예약, 회의 문서자료 공유, 회의실 제반 기기 무선제어 등 편리한 지능형 회의환경 제공
u-수질수위 관리	센서를 이용하여 청계천의 수질, 수위를 측정하고 USN, 무선 메쉬 네트워크 등을 통해 통합모니터링 센터로 전송 및 관리

으로, 2007년 10월부터 11월까지 KISA의 정보보호 사전진단 방법론에 따라 진행되었다.

진단 대상 서비스는 [표 9]와 같다.

〔표 10〕 u-City 정보보호 진단 결과

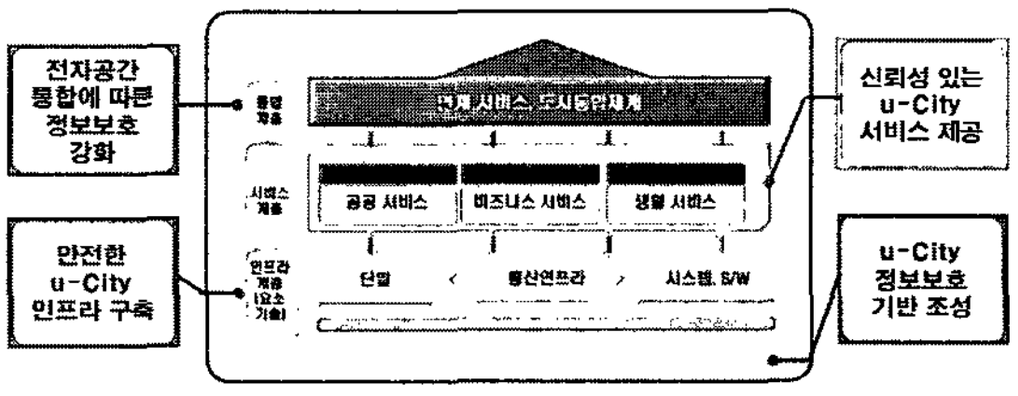
서비스명	주요위협	보호대책
u-Safe	CCTV 네트워크를 이용한 영상정보 위변조, 운영자를 통한 개인영상정보 유출 등	CCTV 와 서버간 인증, 미사용 포트의 비활성화, 운영 보안규정 수립 등
u-폐기물 관리	센서와 MDT단말간 차량무게정보 위변조 등	센서내 무게정보 로깅, 단말 연결부위 고정 등
u-방문객	스마트폰을 통한 비인가 접속, 무선 AP를 통한 서버 접근 등	스마트폰의 접근제어 기능 추가, 무선 AP 인증기능 강화 등
u-커뮤니티	직원 RFID 태그복제, 화장실 단말을 통한 비인가 서버 접속, 개인 위치정보 노출 등	태그복제방지기술 적용, 화장실단말의 상시 모니터링, 서버검색 제한 등
u-회의실	무선 AP를 통한 비인가접속, 회의실서버의 자료 유출 등	무선 AP출력 조정 및 회의실 차폐, 서버 업로드 취약점 보완 등
u-수질수위 관리	Bogus 센서 삽입, ZigBee 도청, 무선노드 암호화키 노출 등	센서의 인증 기능 추가, ZigBee 전송 암호화, 디지털인증서를 사용한 암호키 분배 등

정보보호 진단 결과 N/W CCTV 영상정보 노출 등 74건 위협 도출 되었으며, 이에 대한 보호대책을 권고하였다. 주요 위협 및 보호대책은 [표 10]과 같다.

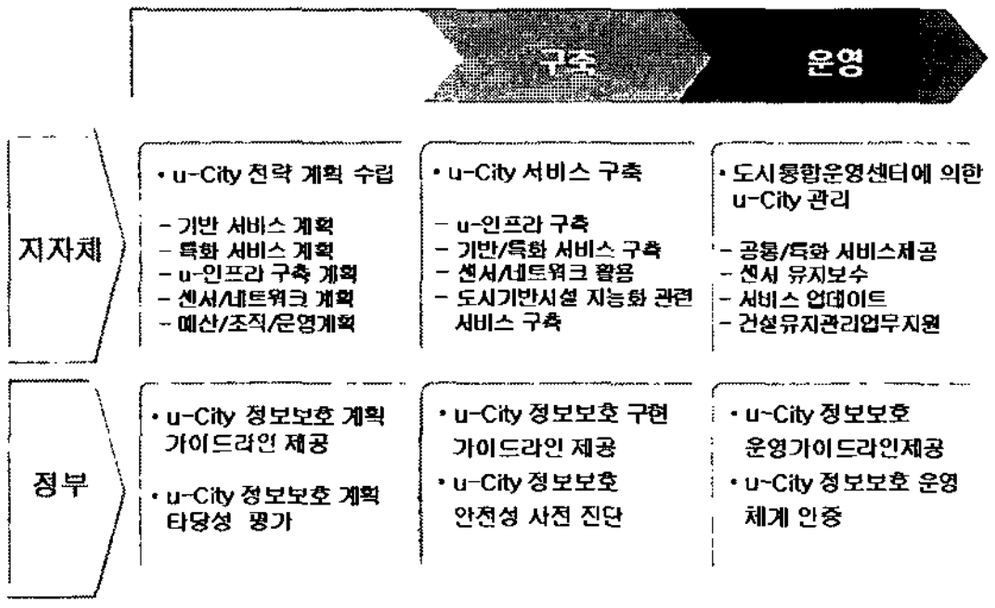
Ⅳ. u-City 서비스 정보보호 대책

4.1. u-City 서비스 정보보호 추진방향

u-City 전반의 체계적이고, 종합적인 정보보호를 위해서는 u-City 구성 체계 및 구축 단계별 보호대책에 따른 추진방향의 정의가 필요하다. u-City 서비스의 위협분석 결과, [그림 8]와 같이 보호대책은 서비스, 인프라, 통합계층 및 기반조성 측면으로 구분이 가능하다.



〔그림 8〕 u-City 정보보호 추진방향



〔그림 9〕 u-City 추진 단계별 정보보호 활동

u-City 계획 수립으로부터 운영까지 전 과정의 정보보호 추진을 위해 [그림 9]과 같이 지자체 및 정부차원의 정보보호 활동 및 지원이 필요하리라 예측된다.

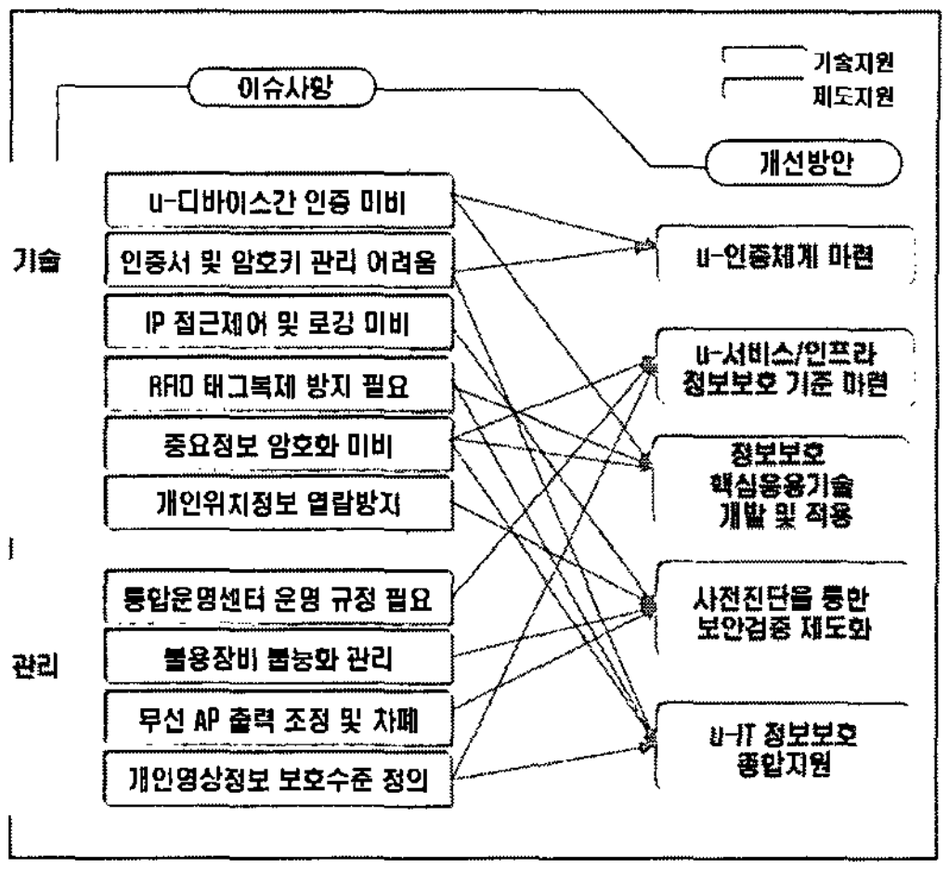
u-City는 도시기능 효율화 및 도시민 편의를 위한 다양한 정보서비스를 제공하나 정보기술에 대한 의존도 증가로 서비스 신뢰성이 우선적으로 확보되어야 한다. 유비쿼터스 서비스 제공을 위해 유무선 네트워크 및 RFID/USN 등 신규 IT기술을 활용하기 때문에 이러한 신규 IT기술에 대한 안전성 보증체계를 수립하고, 동일 공간 내 다수 서비스가 공존 및 상호 연동됨으로써 통합된 데이터의 보호 및 서비스별 상이한 정보보호 수준의 확보 등을 위한 서비스 연동모델의 개발이 필요하다. 또한 u-City 추진주체가 상이하고, 다양한 서비스가 존재하기 때문에 정보보호 정보공유 및 침해사고 시 지원 등을 체계적으로 추진하기 위한 통합지원센터의 수립 등 범정부 차원의 정보보호 기반조성이 필수적이다.

4.2. u-City 정보보호 과제 도출

u-City 정보보호 진단시 도출된 보호대책 및 이슈사항들을 고려한 u-City 정보보호 과제를 도출한 결과, [그림 10]과 같이 u-인증체계 마련, u-서비스/인프라 정보보호 기준 마련, 정보보호 핵심응용기술 적용 등 기술지원과 정보보호 진단의 제도화, u-IT 정보보호 종합지원 등 제도지원 등 세부적인 정보보호 과제를 도출 하였다.

4.2.1 u-인증체계 마련

유비쿼터스 환경에서 고려할 사람, 사물 등 모든 주체와 객체 간 신뢰할 인증 개념이 미흡하며, 현재의 인증 체계는 서비스 사용자를 위주로 구축 및 적용되고 있는 상황이다. 새로운 서비스 개념의 도입으로 인한 사물이나 기기 및 소프트에어 등에 대한 인증 모델은 확립되지 않고 있다. 또한 안전하고 신뢰성 있는 u-City 서비스 제공을 위해 서비스에 사용되는 모든 사물과 사람에 대한 인증 체계, 즉 서비스 구축 및 개시 이전에 u-City에 적용되는 모든 주체와 객체에 통합하여 적용할 수 있는 통합 인증 체계를 구축하여 적용하는 것이 중요하다. 통합 인증 체계를 구축하기 위해 추진해야할 세부 과제는 [표 11]과 같다.



〔그림 10〕 u-City 정보보호 과제도출

〔표 11〕 u-인증체계 세부과제

정보보호 과제
- u-City 서비스 이용권한별 인증 요구수준을 정의한 인증 프레임워크 개발 - 다양한 인증수단과 수준을 수용할 수 있는 확장된 인증 기술 개발 - u-City 개발자의 요청에 따라 인증 요구사항별로 다양한 인증수단을 활용 및 검증할 수 있는 통합인증 서비스체계의 운영

4.2.2 u-서비스 정보보호 기준마련

u-City의 u-서비스는 서비스 사용자에게 서비스를 제공하기 위해 노출되어 있으며, 서비스 사용자 중 악의적 사용자에 의해서 공격을 받을 수 있는 위협이 존재한다. 특히 예측 가능한 위협은 모든 경우에 대해서 보호대책을 제시하여, u-City 구성에 참고 자료로 활용되어야 한

〔표 12〕 u-서비스 정보보호 기준 마련 세부과제

정보보호 과제
- u-City 구성요소의 위협, 보호대책 현황 파악 및 DB 구축 - ·u-서비스별 보안기준 및 정보보호 참조표준 개발 - ·u-서비스별 정보보호 가이드라인 개발 - ·u-서비스별 정보보호 참조표준 보급·활성화

다. 또한 정보보호 참조 표준과 함께 정보보호 가이드라인이 제공되어야 서비스 제공자와 사용자 사이의 안전한 서비스 환경이 구축될 수 있다. u-서비스 정보보호 기준 마련을 위해 추진해야할 세부 과제는 [표 12]와 같다.

4.2.3 정보보호 핵심응용 기술 개발

u-City를 구현하는 인프라는 아직 국내외 표준으로 정리되어 있지 않지만, 적용가능한 인프라/기술에 대한 보호 대책 수립 및 기술개발이 필요하다. 정보보호 핵심응용 기술 개발을 위해 추진해야할 세부 과제는 [표 13]과 같다.

〔표 13〕 정보보호 핵심응용기술 개발 세부과제

구분	정보보호 과제
USN	- USN용 경량 키 관리 기술 및 암호화 인증기술 개발 - 안전한 USN 라우팅 기술, DDoS 방지 기술 개발 - USN 보안미들웨어 및 보안OS 개발
RFID	- RFID 개인프라이버시 보호 및 위치추적 방지 기술 개발 - RFID 기밀성, 복제방지, 인증, 키관리 기술 개발 등
m-RFID	- mRFID 단말 보안키 설정 및 관리 기능 - 모바일 RFID 서비스 단말 , 미들웨어 보안 기술 개발 - mRFID 단말 리더 실행 인가 기술 개발
IP-USN	- IP-USN OS 플랫폼 보안 기술 개발 - IP-USN용 ID 기반 저전력/초경량 보안 기술 개발 - IP-USN의 All IP 네트워크 인프라 연동을 위한 보안 기술 개발

4.2.4 정보보호 사전진단 등 보안검증 제도 도입

u-City 서비스의 신뢰성 및 사용자의 안전을 보장하고, 침해 사고를 효과적으로 예방하기 위하여, 개별 디바이스 및 시스템별 정보보호에서 컨버전스로 확대된

〔표 14〕 보안검증 제도 세부과제

정보보호 과제
- u-City 서비스에 대한 정보보호 사전진단 실시 및 제도화를 통한 활성화 기반 마련 - u-City 서비스 운영시 객관적 검증제도로써 정보보호관리체계 인증 활성화

타 영역까지 포함하여 종합적으로 정보보호 침해를 점검할 수 있는 체계,.서비스 활용과정에서 발생하는 침해요소를 제거하기 위한 사후방재체계와 함께 사전에 침해를 예방할 수 있는 사전진단체계 구축을 위한 제도 도입이 필요하다. u-City에 대한 보안검증을 위한 제도 도입을 위해 추진해야할 세부 과제는 [표 14]과 같다.

4.2.5 u-City 정보보호 종합지원

다양한 수준의 u-City 운영센터의 정보보호 연계 및 지원 등 체계적인 정보보호 지원을 위한 u-City 정보보호 종합센터의 수립이 필요하다. u-City 정보보호 종합지원을 위해 추진해야할 세부 과제는 [표 15]와 같다.

〔표 15〕 u-City 정보보호 종합지원 세부과제

정보보호 과제
- u-City 정보보호 종합지원센터의 수립 및 u-City 정보보호 지원 - u-City 정보보호 종합센터와 u-City 운영센터간 효율적인 정보공유 및 외부 전문기관, 전문가와의 협조체계 구축을 위한 협의체 구성

Ⅳ. 결론

유비쿼터스 사회의 도래와 u-City의 구축, 확산의 이면에는 다양한 정보매체를 통한 비윤리적, 반사회적 컨텐츠가 범람하고 개인의 재산과 생명을 위협하는 사이버 범죄 등 정보 보안 위협이 날로 증대되고 있다. u-City 안에서 새로이 융합되는 신규 IT서비스들이 구축되는 과정에서 보안요소의 고려 및 적용이 미흡할 경우에 u-City 서비스의 안전성 및 신뢰성에 심각한 문제를 야기할 수 있다.

이에 본 논문에서는 u-City 서비스의 정보보호 문제점을 해결하기 위해서, u-City 서비스에서 일어날 수 있는 위협을 분석하고 이를 극복하기 위한 보호대책 및

정책과제를 제시하였다. 민간에서는 위협에 대응하는 보호대책을 수립, 적용 하여 안전한 u-City 서비스를 구축 제공하여야 하며, 정부 차원에서는 중장기적인 관점에서 u-City 정보보호 종합 대책을 마련하여 정책 수립 및 예산 지원 등 체계적인 대응 및 아낌없는 지원을 필요로 한다.

u-City에서의 정보보호 침해사고는 도시민의 실생활에 치명적인 영향을 미칠수 있다는 경각심을 가지고 u-City 도입 단계부터 정보보호에 대한 완벽한 준비를 통해 안전한 u-City 구축 및 서비스 제공에 민관이 함께 노력하여야 할 것이다.

참고문헌

[1] "u-City 인프라 · 기술 · 서비스의 표준화 방안" 한국정보사회진흥원, 2006.9

[2] 정재훈, "u-City 정책방향 및 향후계획", u-City 구현을 위한 실천전략 세미나, 2007.2

[3] "지자체별 u-City 추진현황", 한국 u-City 협회, 2007.2

[4] "u-City 추진 활성화 기본계획" 정보통신부, 2006.

[5] "유비쿼터스 도시의 건설 등에 관한 법률(안)", 건설교통부, 2007.10

[6] "u-Life 21 기본계획", 행정자치부, 2007.10

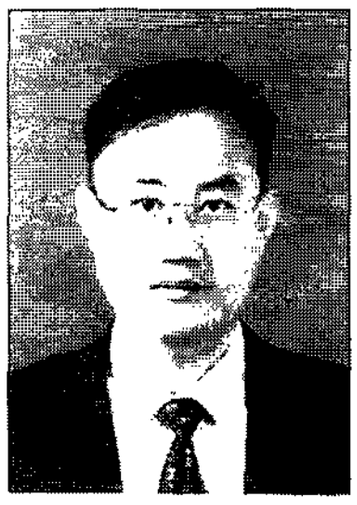
[7] 정부만, "u-City 지원센터 운영방안", 제1차 u-City 지원센터 회의 및 총괄사업추진협의회, 2007.7

[8] www.ubicity.org, u-City 포럼

〈著者紹介〉

이 익 섭 (Ik-Seob, Lee)
2000년 2월 : 부경대학교 정보통신공학과 졸업
2002년 8월 : 부경대학교 정보통신공학과 석사
2002년 7월~현재 : 한국정보보호진흥원 u-IT서비스보호팀 주임연구원
<관심분야> u-City 보안, 정보보호 사전진단

김 호 성 (Ho Seong, Kim)
1994년 2월 : 한양대학교 졸업
2001년 2월 : 포항공과대학교 정보통신학과 석사
2001년 1월~현재 : 한국정보보호진흥원 u-IT서비스보호팀 선임연구원
<관심분야> u-City 보안, BcN 정보보호



이 완 석 (Wan S, Yi)
정회원
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, 주요정보통신 기반시설보호