Ubiquitous City 구축을 위한 U-City전산센터의 보안요구사항 분석 및 기술적 보안관리 대책

홍지범*, 이희조
*고려대학교 디지털정보공학과
e-mail : redziver@korea.ac.kr

An analysis of security requirements and a technical security management plan of U-City computer centre for the construction of Ubiquitous City.

Ji-Boum Hong*, Heejo Lee
*Dept. of Digital Information Engineering, Korea University
e-mail : redziver@korea.ac.kr

요 약

최근 건설되어지는 도시들은 정부의 신도시 정책의 일환인 첨단 도시 건설을 목적으로 하는 Ubiquitous City를 계획하고 있다. Ubiquitous City는 언제 어디서나 유비쿼터스 서비스와 인프라가 제공되는 환경을 가지고 있으므로 노출 위험이 높다. 보안을 고려한 개별 시스템들의 설계는 정부 정책과 함께 활발히 진행되지만 통합 시스템을 관리하는 면에서의 방안은 제시되지 못하고 있다. 보안관리방안이 성립되지 못한다면 침해 유형이 고도화되면서 항상 변화하는 유비쿼터스 시대에 보안은 취약해질 수밖에 없다. 시스템을 총괄 관리 및 관제하는 통합네트워크전산센터인 U-City전산센터의 보안 관리망을 구성하고 취약한 시스템들의 보안을 관리하는 대책이 필요하다. 본 논문에서는 유비쿼터스 보안망의 체계적인 관리 방안을 통합보안관리(ESM)를 중심으로 기술적인 보안관리대책을 제안한다. 제안된 보안관리대책이 Ubiquitous City를 계획하는 모든 신도시들의 플랫폼이 되도록 한다.

1. 서론

IT시대에 유비쿼터스가 주요 관심사가 되면서 홈 네트워크가 구축된 개별 주거 단지의 유비쿼터스 개념을 넘어선 Ubiquitous City(U-City)에 대한 사회적인 관심과 발전이 나타나고 있다. U-City는 유비쿼터스 컴퓨팅 환경이 도입된 도시로 휴대전화와 정보가전, 그리고 도시 공간의 시설물까지 인터넷으로 연결·제어되면서 사람과 인공물, 자연물 등 3자간 커뮤니케이션의 총체가 비즈니스 모델이 되는 유비쿼터스 시대의 도시를 말한다[1].

유비쿼터스 개념이 도입되면서 개인의 정보가 다른 사람에게 알려지는 비밀 없는 세계가 될 수 있고 이외 크래킹에 의한 정보유출, 바이러스 유포, 컴퓨터 범죄, 프라이버시 침해 등 각종 부작용도 일어날 수 있다[2]. 이로 인해 유비쿼터스 보안이란 새로운 이슈가 부각되었고 많은 연구가 진행되고 있으나 관리적인 측면에서 보안 대책은 다뤄지고 있지 않다. 본 논문에서는 통합보안관리망을 중심으로 보안정책을 수립하고 수립된 보안 정책에 따라서 해당하는 보안 시스템을 지원하며, 이를 모니터링하거나 신속하고 효과적인 조치를 취하기 위해서 각종 경보기능을 제공하는 등 일련의 작업들을 일관되게 운영/관리해 주는 기능을 하도록 현재 개발되는 2기 신도시들의 U-City전산센터의 보안관리대책을 제안한다. 본 연구의 결과는 파주운정신도시 U-City 계획에 반영되도록 할 것이다.

본 논문의 구성은 2장에서 U-City 전산센터의 보안 관리 필요성 및 보안요구사항을 언급하고, 홈네트워크 보안요구사항과 비교하였으며, 3장은 U-City 전산센터의 보안관리대책을 기술적인 부문으로 제안한다. 4장은 결론 및 향후과제를 제시한다.

2. U-City전산센터의 보안 필요성 및 보안요구사항

U-City는 유비쿼터스 서비스와 인프라의 효율적 관리 및 모니터링, 정보자원 체계적 관리 및 활용 극대화, 행정서비스 통합 지원하는 통합전산환경이 제공된다. 따라서 U-City전산센터는 개별 주택사업들의 홈네트워크 및 공공 인프라를 손쉽게 연결, 사용할 수 있게 함과 동시에 모든 입주민의 사생활, 개인정보보호 대책도 제공해야 한다.

이러한 U-City의 전산환경의 특성을 통해 U-City 전산센터의 보안 요구사항은 표 1과 같이 정리할 수 있다.

일반적 보안요구사항	추가적 보안요구사항
■ 사용자 및 기기 인증 ■ 데이터의 기밀성과 무결성 ■ 일반적 접근 제어 ■ 물리적, 관리적, 기술적 보안관리대책	■ 정보보호 관리 체계의 수립 ■ 접근 차단 및 탐지 ■ 유동적인 보안 서비스 ■ 계층화된 보안 ■ 추가적 접근제어 ■ 사용자 인식 재고 ■ 대응 팀

<표 1> U-City전산센터의 보안요구사항

추가적 보안 요구사항은 설명하면 다음과 같다.

- 정보보호 관리 체계의 수립 : U-City전산센터는 정보보호 관리체계의 수립으로 내부 보안성 향상 및 위험 관리 능력을 도모해야한다.
- 접근 차단 및 탐지 : U-City전산센터의 접근 차단 및 모니터링을 통한 침입탐지가 가능하고 웜/바이러스, 유해트래픽, 외부 침입으로부터의 네트워크가 보호기능을 수행해야 한다.
- 유동적인 보안 서비스 : 시스템별 중요도 및 정보보호 특성에 맞는 보안 통제 시스템을 적용하고 네트워크, 시스템, 응용시스템, 데이터, PC의 각 단계별로 영역에 맞는 접근제어 및 서비스가 보장해야 한다.
- 계층화된 보안 : U-City전산센터 한 영역에 대한 보안만이 이루어진다면, 그 부분에의 공격이 실제 U-City전산센터 전체에 영향을 미치게 된다. 따라서 특정부분에 대한 공격이 전체 네트워크의 안전성에 영향을 미치지 않도록 해야만 한다[3].
- 추가적 접근제어 : 서비스에 접근할 수 있는 권한 허용의 여부를 말하며, 주로 가능한 모든 것을 차단하고 업무에 꼭 필요한 부분에만 접근을 허용하는 POLP(Policy of Least Privilege)를 적용한다. 또한 사용자의 역할에 근거 할당하는 것이 좋다.
- 사용자 인식 재고 : 사용자에게 정보보호 마인드를 가지게 하고, 정보보호 정책을 따르도록 한다.
- 대응 팀 : 사전에 시스템 공격에 대비한 대응책을 세워두는 것이 필요하다. 최적의 경우는 미리 대응팀을 구성하고 실제 행동 요령에 대한 대응 지침을 작성하고 이에 따른 훈련을 해두는 것이다.

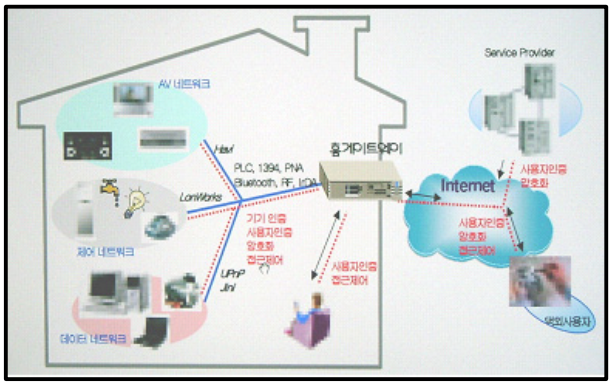
이러한 보안요구사항을 만족하기 위해서는 통합보안관리망을 중심으로 보안 정책을 수립하고 수립된 보안정책에 따라서 해당하는 보안 시스템을 지원하며, 이를 모니터링하거나 신속하고 효과적인 조치를 취하기 위해서 각종 경보기능을 제공하는 등 일련의 작업들을 일관되게 운영/관리해 주는 기능을 하도록 U-City전산센터의 보안관리대책이 선행되어야만 한다.

따라서 보안 장비의 자원 실시간 관리, 보안관리를 위한 작업자 관리 기능, 공격자 추적기능, 알려지지 않은 웜에 대한 감지 및 경고 기능, 내부 및 외부 네트워크 등 다양한 공격 지점에 웜 센서 설치 가능, 계층적 구조로 최대의 확장성/가용성 확보, 이기종 보안시스템 및 각종 장비들의 통합 로그 모니터링 및 관리, 방화벽 로그 분석·IDS 로그 분석·취약점 분석·라우터 로그 분석 등의 지식 정보 제공, 신규 취약점 정보 및 해결 방안 주기적 업데이트, 보안상황 발생시의 상황분석·역추적 방안·관련 정보 제공 등이 필요하다. 이상의 일반적, 추가적 보안요구사항들은 네트워크와 맞물려있는 U-City전산센터에 대한 보안관리대책을 설계할 때 염두에 두어야 할 원칙들이 될 수 있다.

2.1 홈네트워크 보안 요구사항과의 비교

U-City전산센터는 U-City 전체 네트워크에 내재하고 있는 잠재적 공격과 위협들에 대응하기 위해서 수많은 보안관련 이론과 기술적 도구들이 존재한다. 본 절에서는 U-City전산센터의 보안요구사항을 중심으로 [4]에서 제시하는 홈네트워크의 보안요구사항을 비교한다.

홈네트워크에서 공격의 대상이 다양한 정보가전기기들이지만 U-City는 개별 홈네트워크를 연결하는 전체 네트워크를 대상으로 대규모의 홈네트워크가 구성됨으로 공격 대상이 홈네트워크를 포함한 전체 네트워크가 된다.



(그림 1) 홈네트워크의 보안 프레임워크[4]

그림 1처럼 홈게이트웨이 중심인 홈네트워크 보안요구사항과 U-City전산센터의 필수적인 보안요구사항을 비교하면 표2와 같다.

홈네트워크 보안요구사항	U-City전산센터 보안요구사항
■ 상호간 디바이스 인증 ■ 사용자 인증 ■ 기기간 인증 ■ 접근제어 ■ 미들웨어 보안 기능	■ 계층화된 보안 ■ 접근제어 ■ 역할기반 정보보호 ■ 모니터링 ■ 시스템 패치 ■ 관리적 측면의 대응팀 구성 및 사용자 인식 재고

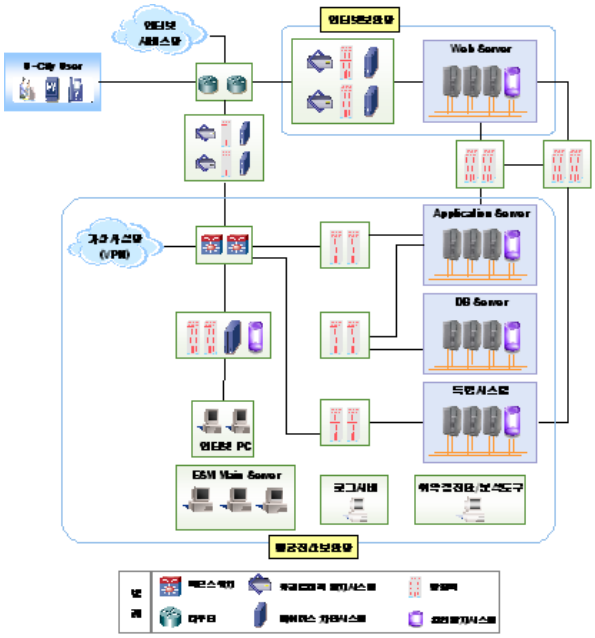
<표 2> 홈네트워크와 U-City전산센터 보안요구사항 비교

3. U-City 전산센터의 기술적 보안관리대책

본 장에서는 2장에서 정리한 U-City 전산센터의 보안요구사항을 만족하기 위한 기술적 보안관리대책을 방화벽, 유해트래픽 탐지시스템, 바이러스 차단시스템, 취약점진단/분석도구 등을 중심으로 제안한다.

U-City전산센터의 기술적 보안관리대책은 네트워크 보안과 인증관리체계를 기반 이루어진다. ESM 또는 보안 대상별 별도의 관리 시스템을 통해 U-City 보안을 위한 전체 보안 시스템에 대한 장애 발생 여부를 감시하고, 보안 상황을 감시해 침해사고에 대비한다. 로그시스템을 별도로 운영하여 정상적으로 감시됐는지 기록을 남기며, 보안 시스템 관리를 위한 각종 정보를 제공한다[5]. 이를 통해서 모니터링 및 침입 탐지의 보안요구사항을 만족할 수 있게 된다.

또한 보안 관리 영역은 U-City전산센터의 기본적인 보안 모델인 Web Server 영역, Application Server 영역, DB Server 영역과 고도의 보안이 필요한 독립시스템 영역으로 분류된다. Web Server 영역은 인터넷 구간에서 별도의 제공하는 영역으로 논리적으로 U-City에서 제공하는 서비스와 완벽하게 분리한다. U-City전산센터의 보안 관리망은 인터넷보안망과 통합전산보안망으로 구성된다(그림 2).



(그림 2) U-City전산센터의 보안 관리망 구성도

U-City의 내부 통합전산망에서 외부 인터넷 서비스를 이용하는 것은 원천적으로 허용하지 않고 Web Server 구간에 위치한 시스템으로의 직접적인 인터넷 접속만 허용한다. U-City전산센터 내부 업무용 PC의 인터넷 접속은 어떠한 경우에도 허용하지 않는다. 단, 별도의 인터넷 PC를 설치하고 방화벽을 통해서 불법적인 침입 및 사용의 오용을 차단하고 통제한다.

인터넷 PC 영역에는 전용 침입탐지시스템을 설치하여 불법적인 침입 및 사용의 오용을 감시한다. 만약 외부방문자가 사용할 경우 방문자는 여부 필요성에 따라 사전에 인증을 받아야 접근이 가능하다. 이러한 기술의 적용은 침입 차단 및 사용자 역할에 따른 접근 제어의 요구사항을 만족시킬 수 있다.

외부로부터의 침입차단과 네트워크 각 영역에서의 논리적인 보호를 위하여 침입차단시스템(방화벽)을 구성해야 한다. 방화벽은 K4등급[6] 또는 CC기반 EAL3+등급[7] 이상 인증 획득, 이중화(HA), 최소권한의 원칙에 입각한 Deny All 접근 기본 정책 [8]을 Inbound/ Outbound에서 동일하게 적용하여야 한다. 안전성에 있어서 충분한 기능의 인증을 받은 시스템을 통해 네트워크 각 영역에 대한 유동적인 보안 서비스 및 계층화된 보안을 제공할 수 있다.

이들 기법 이외에 U-City 전산환경의 가장 중요한 요소인 접근 제어, 차단, 탐지를 위해서 다음의 기술들을 고려할 수 있다.

방화벽을 우회한 침투, 정상적 경로를 통한 침해사고 탐지를 위해서 침입탐지시스템(IDS)을 설치하여야 한다. IDS는 방화벽과 동일한 인증 획득, 침입탐지시스템평가기준 이상 제품을 사용하며 각 영역별로 설치하여야 한다[9]. IDS는 스텔스모드로 동작, 모니터링 포트에 대한 접근은 콘솔 또는 ESM 서버로 제한한다.

공공 기관에서 U-City전산센터로 접근하고자 하는 경우는 가상사설망(VPN)을 통한 사용자 인증과 터널링을 통한 전송 데이터의 노출을 보호한다. 인터넷 보안망을 통한 VPN의 접근은 허용하지 않으며 접속하고자 하는 공공 기관은 Client 방식의 Access VPN을 통하여 U-City전산센터의 해당 시스템에 접근한다.

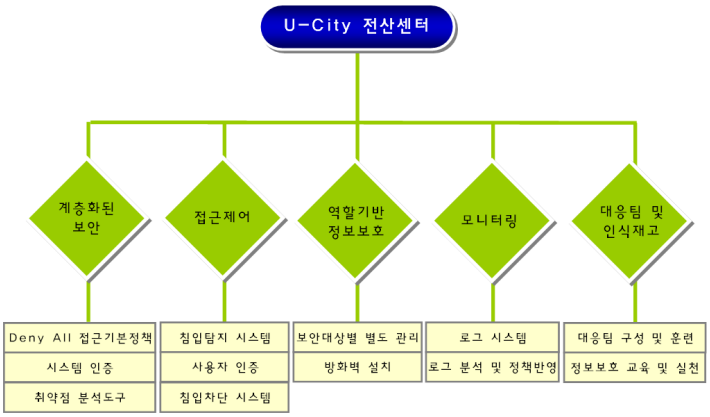
유해트래픽 탐지시스템은 방화벽, IDS가 방어할 수 없었던 유해트래픽을 지능적으로 탐지/차단하여 네트워크를 보호한다. 유해트래픽 탐지시스템은 패킷 모니터링, 트래픽 유형기반 차단, 키워드 필터링, Traffic Shaping, Session Limitation의 기능을 하며 이중화(HA) 및 다단계 방어(Multi Deep Defense)를 하고 U-City전산센터의 인터넷 보안망 구간의 전단에 위치하여 내부 네트워크를 보호한다.

악성코드가 U-City전산센터의 내부 네트워크에 진입하기 전에 발견하고 제거하기 위하여 바이러스 차단시스템을 설치한다. 바이러스를 실시간으로 차단하며 정책에 따라 다양한 툴 설정, Load Balancing(부하의 분산을 위한 툴 설정 지원), 라이브 업데이트, 통합로깅 등의 기능이 있으며 다양한 프로토콜에 대한 검색을 지원한다. U-City 입주민 서비스를 위한 인터넷 보안망 구간의 전단, 공공기

관들의 인터넷 접속 경로, U-City전산센터의 인터넷 PC 전용 구간의 전단에 바이러스 차단시스템을 설치한다.

새로운 공격방법이 계속해서 발견되기 때문에 취약점 진단/분석 도구는 U-City 전산센터에 중요한 역할을 한다. 이는 공격에 취약한 점을 발견하고 보안 정책에 반영한다. 전체 네트워크에 대하여 주기적으로 상호 취약점 진단을 시행하며 지속적인 공격에 대하여 시스템 취약점에 대한 대처와 네트워크 장비, 시스템, 사용자 PC에 대하여 보안 취약성을 주기적으로 진단, 조치함으로써 정보보호 마인드를 향상한다. 관리자 및 일반사용자의 취약점을 별도 진단/분석함으로 취약점 분석시 발생할 수 있는 사용자별 충돌을 막을 수 있다. 또한 공격에 취약한 대상 시스템 분석시 타시스템의 침입시도를 동시에 진단/분석하여 네트워크 전체의 보안 관리 체계를 유지할 수 있다. 이 동성을 보장하며 취약점 DB의 실시간 업그레이드와 보안 취약점의 자동 점검 및 레포팅을 한다. 취약성에 대한 원인, 중요도, 영향 범위, 조치 방법, 관련 사이트 등의 DB도 제공한다. 진단/분석 결과를 중요도별로 분류하고 침입 및 권한탈취 시도의 결과, 보안 취약점, 결함을 교정하고 ESM Main Server에 전송하여 보안 관리 정책에 반영한다.

이상의 기술적 보안대책은 정보보호 관리 체계 하에서 수행되며, 이를 통해 U-City 일반적 보안요구사항인 기밀성, 무결성, 가용성, 인증 이외에 유비쿼터스 환경을 위한 접근 차단 및 탐지, 유동적인 보안 서비스, 계층화된 보안, 접근제어를 만족할 수 있다. 본장에서 다룬 주요 사항은 그림3과 같이 요약할 수 있다. U-City 전산센터만의 보안 요구사항과 이를 실현하기 위한 기술을 연결하였다.



(그림 3) U-City 전산센터의 기술적 보안관리대책

이외의 추가적 보안 요구사항은 교육을 통한 사용자 인식 재고 및 대응팀의 운영 및 관리를 통해서 만족할 수 있다.

4. 결론 및 향후 과제

정부 정책의 일환인 첨단 도시 건설은 U-City 구축으로 달성될 것이다. 하지만 보안 기술의 발전만으로 변화하는 유비쿼터스 시대를 따라 갈 수 없다. 이는 U-City를 관리 및 관제하는 통합네트워크전산센터인 U-City전산센터를 기술적인 보안관리대책을 정립함으로 보완할 수 있다.

본 논문에서는 U-City전산센터의 기술적 보안관리대책을 제안한다. U-City전산센터는 인터넷 서비스를 연결하는 보안 관리망과 통합보안관리 시스템을 연결하는 보안 관리망으로 구성한다. 보안요구사항을 분석하여 계층화된 보안, 접근제어, 역할기반 정보보호, 사용자 인식 재고, 모니터링, 시스템 패치, 대응 팀의 보안 요구 사항에 맞게 U-City전산센터의 보안관리대책을 제안한다.

앞으로 보안 관리 방안을 기술적인 관점에서의 대책뿐만 아니라 관리적, 물리적 대책과 침해사고 대응체계를 제시한다면 보안관리대책의 일관성이 유지될 것이다. 또한 U-City전산센터에 적용되는 정보보호 아키텍처를 관리적, 기술적, 물리적 관점으로 제안한다면 보다 더 체계적인 보안관리대책이 수립될 것이다. 향후 이러한 보안관리대책을 기반으로 관련 법규 및 지침을 만들어 U-City뿐만 아니라 사이버 아파트를 건설하는 첨단주택건설사업자들에게 제공한다면 디지털 라이프 실현을 위한 유비쿼터스 시대에 한걸음 더 나아갈 것이다.

참고문헌

[1] 이홍주 외, “당신의 라이프스타일과 비즈니스 환경을 바꾼다-유비쿼터스 혁명”, 2004.09

[2] 리처드 헌터, “유비쿼터스(공유와 감시의 두 얼굴”, 21세기북스, 2003.03.

[3] 정태명 외, “통합전산환경의 추진방향”, 2004.11

[4] 한종욱 외, “안전한 홈네트워크 구축을 위한 보안요구사항”, 2004.05

[5] 곽희선, “[보안시스템관리방안⑥]보안서비스”, 2004.07

[6] 정보통신부, "정보통신망침입차단시스템평가기준", 2000.02

[7] 최상수 외, “CC 기반에서 보증수준 및 제품유형을 동시에 고려한 평가업무량 모델”, 2004.02

[8] 윤승노, “정보보호뉴스 2004년 11월호”, 발한국정보보호진흥원

[9] 정보통신부, "정보통신망침입탐지시스템평가기준", 2000.07