creative commons
COMMONS DEED

저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:

저작자표시. 귀하는 원저작자를 표시하여야 합니다.

비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.

변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 이용허락규약(Legal Code)을 이해하기 쉽게 요약한 것입니다.

Disclaimer

dCollection

[UCI]I804:21031-000002236965

공 학 석 사 학 위 논 문

재난안전 정보시스템의 취약성 분석 및 개선 방안

2016년 2월

부 경 대 학 교 대 학 원

정보시스템협동과정

김 태 연

공 학 석 사 학 위 논 문

재난안전 정보시스템의 취약성 분석 및 개선 방안

지도교수 김 창 수

이 논문을 공학석사 학위논문으로 제출함.

2016년 2월

부 경 대 학 교 대 학 원

정보시스템협동과정

김 태 연

김태연의 공학석사 학위논문을 인준함

2016년 2월 26일

PUKYONG NATIONAL UNIVERSITY
부경대학교

위 원 장 이학박사 박 만 곤 (인)

위 원 공학박사 김 창 수 (인)

위 원 이학박사 이 경 현 (인)

< 차 례 >

< 그림 차례 >

< 표 차례 >

PUKYONG NATIONAL UNIVERSITY 부경대학교

The Vulnerability Analysis and Investigation of Information System for Disaster Safety

Tae Yeon Kim

Interdisciplinary Program of Information System,
Pukyong National University

Abstract

The various types of disasters have being occurred as urban expands rapidly as to the climate change and science technological development. It is a trend that IT technology converges with related fields to prevent the disasters. In particular, the rapid growth technologies such as Internet of Things (IoT), sensors , Global Position Systems (GPS), real time processing, and mobile devices have been utilized as essential techniques in national emergency management systems.

In this thesis, we investigate some methods to provide the useful information for preparing for disasters in the real-time using recent IT technology focused on the disasters. We survey control systems and the related laws and regulations on the disasters in domestic and international areas.

First, we analyze the various emergency response systems to construct disaster safety information systems, and investigate the related vulnerabilities. We discovered that it is difficult to collect the disaster information in urban area and analyzed vulnerabilities to construct the disaster information systems

based on u-IT. Additionally, the vulnerabilities are analyzed in collecting location information of occurred disasters on the real-time with mobile devices.

We suggest an integrated system using vulnerabilities of the disaster safety information systems. The proposed system includes an integrated disaster safety information system based on the u-IoT, and the authentication and verification method for the location information. Finally, the improvement methods are proposed to integrate the information systems related to disasters.

This research provides an essential information in integrating disaster prevention systems of national and local governments into an entire system as the proposed system includes the improvement methods to resolve vulnerabilities of the integrated control systems in the macro perspective view on constructing disaster safety information systems

1. 서론

1.1 연구 배경

국내외적으로 크고 작은 재난은 기후변화의 원인과 과학기술의 발달로 급속하게 팽창하는 도시화에 따라 다양한 유형의 재난이 발생하고 있다. 이러한 재난에는 과거부터 존재해 왔던 자연재해는 물론 토목·건축기술의 발달로 고층화, 대형화되는 거대 도시의 생성에 따른 인적재난도 지속적으로 증가하고 있다. 또한 IT기반의 첨단 융합 기술들이 발전하면서 사람들에게 편리함을 제공하기 위해 개발된 기술들이 다른 용도로 사용되는 사회적 재난도 점점 증가하고 있다. 이러한 문제점들의 원인을 찾아보고, 완전한 예방은 어렵지만 예측 가능한 재난에 대해 경감할 수 있는 방법을 찾는 것은 매우 중요하다.

본 연구는 재난이라는 키워드와 IT라는 최신 기술의 결합으로 사람들에게 재난에 대비한 정보를 보다 빨리 그리고 실시간으로 제공할 수 있는 방법들이 무엇인지, 그리고 어떤 재난 대응시스템을 구축해야 사람들에게 필요한 정보를 제공할 수 있는지 살펴본다.

우리는 재난의 유형이 매우 많음을 잘 알고 있으며, 각 재난 유형에 따라 인명과 경제적 손실의 크고 작은 차이를 잘 알고 있다. 자연재해는 범위가 넓고 사람의 능력으로 예방할 수 없는 재난도 많이 있다. 그런 반면 인적재난은 산업혁명 이후 기술발전이 매우 급속도로 빠르게 진화하면서 도시화의 일환으로 고층 빌딩과 복잡한 도로망은 크고 작은 재난과 인명 및 경제적 손실을 유발하고 있다.

정부는 물론 각 지자체는 기존 아날로그 형태의 도시발전에서 IT기술의 발달로 사람들은 물론 관공서, 기업, 학교 등은 대부분 IT기술을

기존의 업무에 병행하여 사용하고 있다. 이러한 IT기술은 교육 분야는 물론 금융, 건축, 도로, 하수관리 등은 물론 재난과 관련된 분야에서도 매우 중요한 요소로 활용되고 있다. 따라서 정부는 물론 각 지자체는 재난에 대비한 다양한 재난대응시스템을 각 분야에 따라 자체적으로 시스템을 구축하여 운영하여 왔다. 이렇게 자체적으로 구축된 재난대응시스템은 정보의 호환성은 물론 복합적인 재난에 대해서는 재난대응시스템의 역할을 하지 못하고 있다. 최근에는 이러한 문제점을 보완하기 위해 데이터 공유의 방법이라든가 구축된 시스템과의 연계방법에 대해 많은 연구와 개발이 동시에 진행되고 있다.

본 연구는 최근의 연구 방향에 동승하여 기존의 재난대응시스템을 알아보고, 어떤 문제점이 있는지 분석하여 개선 방안을 제시한다.

1.2 연구 목표

재난안전 대응시스템의 구축은 크게 2가지 관점에서 접근할 수 있다. 첫째는 거시적인 관점에서 다양하게 구축된 재난대응시스템들 간의 정보를 공유하기 위해 정보 공유 및 시스템 연계를 통하여 통합적인 재난안전 정보시스템을 구축하는 것이다. 둘째는 미시적 관점에서 특정 재난대응시스템을 구축할 경우 사용하고자 하는 시스템 운영체제, 플랫폼 기술, 현장에서 실시간으로 정보를 수집하기 위한 다양한 재난관련 정보수집 입력장치, 수집된 정보를 가공하여 어떤 방법으로 사람들에게 제공할 것인지에 대한 출력장치, 타 시스템과의 연계를 위한 정보 공유의 데이터베이스 등이 주요 관심의 대상이 된다.

본 연구는 미시적 관점보다는 거시적 관점에서 IT 기술의 발전을 고려한 기존의 재난대응시스템들 간의 연계와 정보공유의 방법들에 대해 알아

본다. 또한 재난은 한 가지 정보만으로 의사결정을 내리는 것은 어렵기 때문에 다양한 정보들을 통합적으로 고려하여 재난대응 의사결정이 이루어져야 한다. 이러한 의사결정에는 제공되는 정보가 변경되지 않아야 되는데, 재난대응 시스템에서 제공하는 정보의 취약성을 알아보고, 그 취약성을 개선할 수 있는 방법을 연구한다.

본 연구는 지자체 혹은 구·군 단위에서 각 재난 유형별 재난대응시스템을 구축할 경우, 각 시스템이 가져야할 정보의 유형과 타 시스템에 운영중인 정보의 내용을 파악하여 어떻게 기존 정보와 새로운 정보를 공유할 것인지에 대한 참고자료 활용가능하다. 또한 최근에는 실시간으로 정보를 제공하고 수신하기 위해 휴대폰을 많이 사용하고 있는데, 이러한 휴대폰의 정보들이 어떤 취약성이 있는지 살펴보고 각 재난대응시스템을 구축할 경우 데이터 및 정보 취약성의 개선 보완에 적용될 수 있다. 따라서 본 연구는 이론적인 재난대응시스템 보다는 실제 현장에서 적용되어 운영될 경우 고려되어야 할 요인들을 살펴보고 예방하는데 도움이 되는 연구이다.

2. 관련연구

본 연구는 거시적 관점에서 다양한 재난유형을 알아보고, 각 재난 유형에 따른 어떤 대응시스템이 구축되어야 하는지 알아본다. 그리고 구축된 대응시스템간의 연계와 내부적으로 발생할 수 있는 취약성에 대해서도 살펴본다. 마지막으로 기존의 재난대응시스템이 가질 수 있는 취약성에 대해 개선방안을 알아보고, 또한 각 재난대응시스템 간의 연계와 정보공유의 방법에 대해 연구한다. 따라서 본 절에서는 본 연구와 관련된 기존의 연구들이 어떤 것이 있는지 살펴보고자 한다.

2.1 재난 및 안전관리 기본법

본 절에서는 본 연구와 관련된 재난 및 안전관리 기본법에 대해 살펴본다. 이는 본 연구에서 기술하고 있는 각 재난대응시스템이 재난 및 안전관리기본법에 따라야 하며, 그리고 기본법은 계속적으로 변경되기 때문에 본 연구와 관련 있는 부분을 중심으로 설명한다.

재난 및 안전관리 기본법의 목적은 약칭으로 재난안전법이라 하며, 이는 각종 재난으로부터 국토를 보존하고 국민의 생명·신체 및 재산을 보호하기 위해 국가와 지방자치단체의 재난 및 안전관리체계를 확립하고, 재난의 예방·대비·대응··복구와 안전 문화 활동, 그 밖의 재난 및 안전관리에 필요한 사항을 규정함을 목적으로 하고 있다. 그리고 기본 이념은 재난을 예방하고 재난이 발생한 경우 그 피해를 최소화하는 것이 국가와 지방자치단체의 기본적 의무이고, 모든 국민과 국가·지방자치단체가 국민의 생명 및 신체의 안전과 재산보호에 관련된 행위를 할 때 안전을 우선적으로 고려하여 국민이 재난으로부터 안전한 사회에서 생활할 수 있도록 규정하고 있다.

재난의 종류에는 크게 자연재난과 사회재난으로 구분하고 있다. 자연재난은 태풍, 홍수, 호우, 강풍, 풍랑, 해일, 대설, 낙뢰, 가뭄, 지진, 황사, 조류 발생, 조수, 화산활동 그 밖에 준하는 자연현상으로 인하여 발생하는 재해로 정의하며, 사회재난은 화재, 붕괴, 폭발, 교통사고(항공 및 해상사고 포함), 화생방사고, 환경오염사고, 에너지·통신·교통·금융·의료·수도 등 국가기반체계의 마비, 감염병, 가축전염병 등이 포함된다. 이 외에도 해외재난으로 대한민국의 영역 밖에서 국민의 생명·신체 및 재산에 피해를 주거나 줄 수 있는 재난으로 정의하고 있다. 그리고 재난정보관리란 재난관리를 위하여 필요한 재난상황정보, 동원가능 자원정보, 시설물정보, 지리정보를 정의한다[1].

재난 및 안전관리 기본법 시행령에는 재난 및 사고유형별 재난관리주관기관이 정의되어 있다(표 1 참조).

[표 1] 재난 및 사고 유형에 따른 재난관리 주관 기관

재난관리 주관기관	재난 및 사고의 유형
교육부	학교 및 학교시설에서 발생한 사고
미래창조과학부	1. 우주전파 재난 2. 정보통신 사고 3. 위성항법장치 전파혼신
외교부	해외에서 발생한 재난
법무부	교정시설에서 발생한 사고
국방부	국방시설에서 발생한 사고
행정자치부	정부주요시설 사고
문화체육관광부	경기장 및 공연장에서 발생한 사고
농림축산식품부	1. 가축 질병 2. 저수지 사고
산업통상자원부	1. 가스 수급 및 누출 사고 2. 원유수급 사고, 3. 원자력안전 사고 4. 전력 사고 5. 전력생산용 댐의 사고

[표 1] 재난 및 사고 유형에 따른 재난 관리주관 기관(계속)

재난관리 주관기관	재난 및 사고의 유형
보건복지부	1. 감염병 재난 2. 보건의료 사고
환경부	1. 수질분야 대규모 환경오염 사고 2. 식용수(지방 상수도 포함) 사고 3. 유해화학물질 유출 사고 4. 조류(藻類) 대발생(녹조에 한정) 5. 황사
고용노동부	사업장에서 발생한 대규모 인적 사고
국토교통부	1. 국토교통부가 관장하는 공동구 재난 2. 고속철도 사고 3. 국토교통부가 관장하는 댐 사고 4. 도로터널 사고 5. 식용수(광역상수도에 한정) 사고 6. 육상화물운송 사고 7. 지하철 사고 8. 항공기 사고 9. 항공운송 마비 및 항행안전시설 장애 10. 다중밀집건축물 붕괴 대형사고
해양수산부	1. 조류 대발생(적조에 한정) 2. 조수(潮水) 3. 해양 분야 환경오염 사고 4. 해양 선박 사고
국민안전처	1. 공동구(共同溝) 재난 2. 화재·위험물 사고, 내륙에서 발생한 유도선 등의 수난 사고 3. 다중 밀집시설 대형화재 4. 풍수해(조수 제외)·지진·화산·낙뢰·가뭄 6. 해양에서 발생한 유도선 등의 수난사고
금융위원회	금융 전산 및 시설 사고
원자력안전위원회	1. 원자력안전 사고 2. 인접국가 방사능 누출 사고
문화재청	문화재 시설 사고
산림청	1. 산불 2. 산사태

재난 및 안전관리 기본법 시행규칙에는 본 연구와 관련된 내용으로는 중앙재난안전대책본부의 운영, 재난상황 보고, 재난안전분야 종사자 교육 종류, 자원관리시스템의 구축·운영, 재난문자방송에 대한 기준·운영 등에 대한 내용이 포함되어 있다[1].

2.2 국가 재난관리 정보시스템

국가 재난관리 정보시스템(National Disaster Management System, 이하 NDMS)은 국가재난관리 전담기관인 소방방재청에서 구축하여 활용중인 것으로, 재난통신시스템, 재난의 체계적인 예방, 대비, 신속한 대응, 복구 업무 지원 및 화재·구조구급 등 119서비스 업무 전 과정을 정보화하여 국민 재난안전 서비스를 제공하기 위해 구축된 시스템이다[2,3].

NDMS는 1차 사업에서 구축된 데이터베이스의 본격적인 활용을 위해 2차 사업을 통해 자치단체별·재해 유형별 현장 대응 체계 구축, 위성통신 등 첨단기술과의 융합에 초점을 두었다. 특히 23개 중앙부처 234개 지방자치단체 등 국가 재난 관리에 관련되는 모든 기관이 동시에 접속·활용하도록 하였다. 그러나 막대한 비용을 투자하여 구축된 시스템이 각 지자체의 해당 부서에서 적극적으로 이 시스템을 활용하지 않는 것이 문제가 되었다. 이후 지속적인 시스템 개선으로 재난관리 전용망, 시스템 내부의 메신저 기능, 수신 경보 기능 등을 개선하여 신속성과 효율성을 높여가고 있다.

[표 2]는 국가 재난관리 정보시스템의 주요 기능을 나타내고 있다. NDMS의 구축과 운영의 취지는 매우 중요하고 정보를 중앙 집중화 한다는 측면에서는 많은 의미가 있다. 그러나 이러한 시스템은 다양한 종류의 재난발생과 IT기술의 발전으로 지속적인 개선과 기술개발이 함께 이루어져야 된다. 그러나 실제 현황은 그렇지 못하고 있다.

본 절에서는 NDMS가 가지고 있는 취약성을 분석하여 본 연구의 거시적 관점과 연계하고자 한다. 예를 들면 영상처리 기술을 이용하여 산불화재 조기경보 관리시스템이나, 태풍, 집중호우에 따른 하천범람 등에 적용할 수 있다. 그러나 아직도 CCTV의 기능이 많이 개선되었다고는 하지만 야간이나 안개가 낀 열악한 환경에서는 현재 CCTV 기능으로 정확한 정보를 수집하는 것이 어렵다. 이 외에도 각 지자체의 구·군에서는 다양한 유형의 재난발생에 대해 여러 가지 중요한 정보를 다양한 미디어를 활용하여 NDMS 시스템에 정보를 입력할 수 있어야 하나, 실제 입력은 사고발생의 경위, 장소, 인명 피해 등 중요 요소만 입력할 수 있어, 사후 재난

예방을 위한 재난 발생의 다양한 정보들을 입력할 수 있는 기능들이 개선되어야 한다. 또한 재난발생 시 응급구조를 위한 위치 인식기능도 보완되어야할 요인이다. 즉, 화재 또는 지진으로 인해 건물 내에서 연기 또는 붕괴된 건물의 잔해로 피해자의 위치를 인식하기 힘들기 때문에 건물 내에서의 위치식별과 다양한 통신 기능들이 통합되어 전송될 수 있도록 개선되어야 한다[5].

[표 2] 국가 재난관리 정보시스템의 주요 기능

구분	주요 기능	업무 적용
예방 및 대비관리 시스템	- 시설관리 - 물자관리 - 웹 GIS - 재난시설관리 - 지역관리	- 방재시설물관리와 피해발생시 대피수용시설관리 지원 - 응급복구장비 및 수방자재관리 방역물자관리, 구호기증물자관리 - 지리적 위치를 이용한 자원정보 제공 - 재난발생 위험 및 예방 필요시설·지역을 위험등급 별로 분류 및 관리
대응관리 시스템	- 피해상황관리 - 일일상황관리 - 대응지시관리	- 인명·재산피해상황 보고 및 실시간 집계 - 지역별 피해 및 조치상황 실시간 조회, 대응책 마련 - 교통사고, 화재폭발 등 재난발생 현황 및 조치 결과 실시간 정보공유 연계 지원 - 중앙과 지방간 메신저, SMS, PDA 등을 통해 쌍방간 재난대응 및 조치사항 실시간 전달
복구관리 시스템	- 복구계획관리 - 복구진도관리	- 피해상황관리시스템에서 입력된 시군구별 시도별 공공시설 등의 피해현황 및 복구비 산정 지원 - 복구비 집행여부 및 복구사업진행 정도 모니터링, 관리

2.3 재난관련 관제시스템

본 절에서는 재난관련 관제시스템을 조사하고, 현재 관제시스템이 가지고 있는 취약성 부분도 알아본다. 기본적으로 관제시스템이란 물리적 위협수단인 사람, 자동차, 집중호우, 화재 등으로부터 사람들을 보호하기 위해 CCTV나 보안시스템을 구축하여 모니터링 하는 시스템이다.

2.3.1 CCTV 관제시스템

행정안전부는 2015년까지 전국 지자체 229개 시·군·구에 CCTV 통합관제센터를 설치하여 방범, 어린이 보호, 재난 감시용 등으로 운영되고 있는 CCTV 10만여 대를 통합·연계할 연차적 목표를 제시하였다. 그리고 현재 10여개 부서에서 관리하고 있는 CCTV 업무를 1개 전문부서로 통합하고, 전국에 CCTV 전문 관제요원을 배치하여 10만여 대의 CCTV를 모니터링 함으로써 재난 및 방범에 대비하고자 하였다. 그리고 CCTV 통합·연계에 따른 취약성을 예방하기 위하여 모든 CCTV 영상정보를 암호화하여 전송·보관하고, 외부의 해킹 공격을 방어하기 위해 높은 수준의 보안기능을 추가할 계획을 발표하였다. [표 3]은 행정안전부 CCTV 종합대책에서 제시하고 있는 개선 업무를 나타내고 있다[4,12].

[표 3] 행정안전부 CCTV 종합 개선 방향

업무	현재	개선
재난재해 감시	3.7% CCTV만 단속	모든 CCTV 단속·감시
수배차량 추적	CCTV별 추적	전국 CCTV 동시
증거자료 확보	CCTV별 개별 확인	전국 CCTV 동시 확인

그러나 위이 표에서 보면 재난재해 감시용으로 CCTV를 활용하고 있지만, 모든 CCTV에 재난과 관련된 감시기능을 탑재할 계획으로 되어 있지만 현실적으로는 CCTV의 기술과 야간 및 안개 등의 열악한 환경에서 적용이 아직 어렵기 때문에 실제 사용은 저조하게 운영되고 있다.

CCTV와 관련된 주요 솔루션으로는 지능형 영상보안 기술이 있는데, 이는 특정 이벤트의 영상 데이터를 자동으로 분석하여 실시간으로 파악하는데 있다. 예를 들면 침입탐지 감시, 치매환자 등의 배회 감시, 차량번호, 문자, 안면 인식 등 다양한 영역으로 확대되고 있다. 이러한 기술을 바탕으로 최근에는 사람의 비명, 차량 충돌음, 물건 깨지는 소리 등을 감지하여 감지된 위치에 카메라를 이동시키고 해당 영상을 캡처하여 관제센터로

전송하는 기술들이 개발되고 있다. 이러한 기술들을 기반으로 최근에는 각 지자체가 지능형 CCTV 시스템이란 이름으로 기존의 문제점을 개선하는 방향으로 진행되고 있다[7]. [표 4]는 재난관리 기관별 CCTV 활용 현황 및 개선 사항을 나타내고 있다.

[표 4] 재난관리 기관별 CCTV 활용 현황 및 요구 사항

구분	현행	요구사항
시·군·구	- 재난상황실에서만 모니터링	- 업무담당자도 모니터링 기능 개발 - 시군구 재난 관리 시스템 기능 추가
	- CCTV 도입시점별 장비종류가 달라 호환이 되지 않음	- CCTV 종류에 관계없이 통합관리 - 아날로그 CCTV의 디지털 변환·통합
소방서 (119안전센터)	- CCTV 모니터링체계 없음 -일부는 해당 시군구에 직접 모니터링	- 관할지역 내 CCTV를 통합모니터링 할 수 있는 조회프로그램 개발 제공
시·도 (소방본부)	- 대부분 통합 모니터링 체계 없음	- 관할 시군구에 설치된 CCTV 영상정보를 통합모니터링하고 타 시도와 공동이용 할 수 있는 체계 구축
소방방재청 (재난 상황실)	-행안부에서 연계한 철도, 공항 등 26개 영상을 단순 모니터링 -국토부 교통정보센터와 전용선으로 연계하여 고속도로 및 국도상황을 모니터링	- 지자체 및 유관기관으로부터 수집한 영상정보를 통합 모니터링하고 상호 공동이용 할 수 있는 체계 구축 -CCTV 영상정보와 관측정보 등 현장 상황정보를 연계 및 통합 표출하는 기능 구축

CCTV 관제기술은 CCTV의 기능이 계속하여 발전되기 때문에 특히 재난과 관련하여 CCTV의 역할은 매우 중요하다. 그러나 아직도 CCTV는 보안과 관련하여 취약한 부분이 많기 때문에 이러한 부분에 대한 연구와 개선은 필요하다.

2.3.2 교통관제 시스템

교통관제시스템도 재난과는 밀접한 연관이 있다. 일반적으로 교통관제 시스템은 ITS(ITS: Intelligent Transport Systems, 이하 ITS)란 이름으로 많은 연구들이 진행되고 있다. ITS는 교통정보, 기상정보, 도로상태 정보 등을 수집한 후, 사람 혹은 차량들에 필요한 정보로 가공하여 교통 단말기, 차내 단말기, 교통방송, 인터넷 등의 무선 통신수단을 이용하여 차량 및 운전자에게 전송함으로써 통행의 편의와 교통량의 원활한 소통을 이루는 시스템이다.

1980년대 중반부터 미국, 일본, 유럽 등 선진국은 ITS에 대한 연구·개발이 활발하게 추진되어 왔으며, 국내에서도 1997년 "국가 ITS 기본계획"을 확정하여 기본 틀을 마련하였다. 이후 2000년 "국가 ITS 기본계획 21"로 수정·보완 하여 교통류 관리, 기본 교통정보 제공, 대중교통정보제공 및 관리, 정보 연계 등 다양한 분야의 시스템이 확장되어 운영되고 있다.

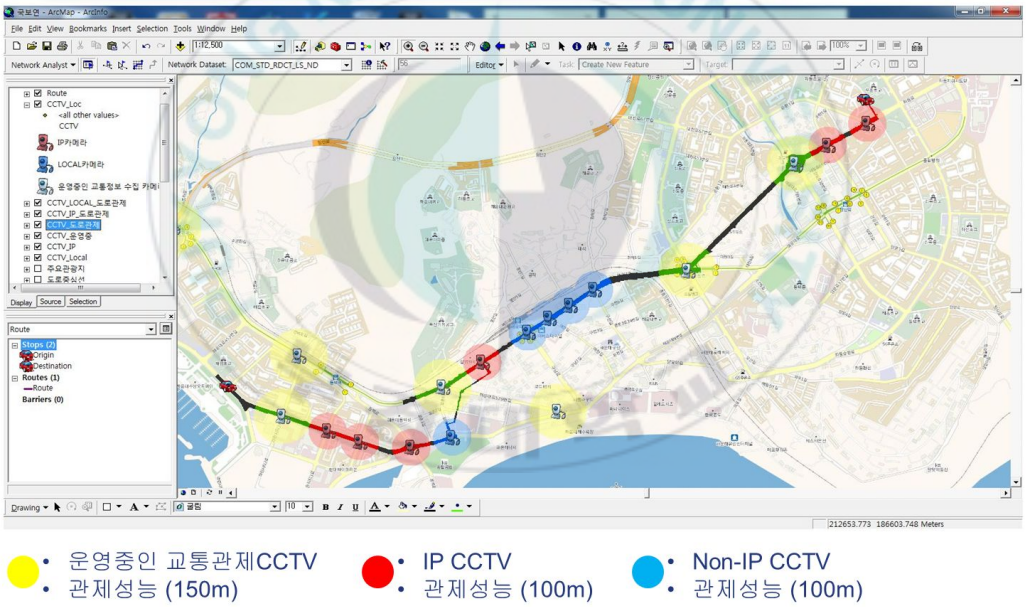
다음은 국내외 ITS 구축현황에 대해 설명한다.

(1) 국내 ITS 구축 현황

ITS 시스템 추진 및 구축현황은 수도권을 비롯하여 첨단모델도시 및 각 지방자치단체에서 추진되어 왔으며, 이는 교통체증감소와 교통사고 저감, 대중교통 서비스 개선 등을 시민에게 실질적인 편의를 제공하는데 목적으로 개발되어 왔으며, 최근에는 방범 및 재해에 대비한 교통관리 분야에도 활용되고 있다. 그러나 방범 및 교통통제의 관제시스템에 적용될 경우 악의적인 사용으로 취약점이 나타나고 있다.

예를 들면 부산시 교통 관제센터에서 운영중인 차량번호 판독용 CCTV 시스템(Vehicle number Identification CCTV Integration Oversee System : VICIOS)에 대해 의도적인 목적으로 CCTV의 방범 관제를 회피하는 시나리오가 가능하다. CCTV 관제 불능 상황은 CCTV에 붙어있는 카메라에 악의적 공격으로 카메라의 관제 시야를

돌린다거나, 영상을 조작하여 관제가 불가능한 카메라로 변경될 수 있다. 이러한 경우 실제 운영중인 교통관제 CCTV가 IP기반으로 연결되어 있을 경우 해킹 혹은 불법 접근으로 정상적인 관제 상황을 진행하지 못하도록 설정할 수 있다. [그림 1]은 가상의 교통관제 상황에서 고의적인 침입으로 붉은색 카메라가 관제 불능 상태에 있을 경우 관제율을 측정하기 위한 연구내용을 나타내고 있다. 이는 특정 CCTV의 카메라가 정상작동을 하지 못할 경우 전체 교통관제시스템에서 관제율을 측정할 수 있는 모델링이 가능하다. 이러한 연구로 국내 ITS 교통관제 시스템에서도 방범과 재난에 대비한 취약성을 개선할 수 있는 연구가 필요하다[3,5].



[그림 2] CCTV 교통관제에서 의도적인 상황변경 모델링

(2) 국외 ITS 구축 현황

미국의 ITS 관제시스템은 1960년대 말 ERGS 그룹과 1988년 말 연구그룹인 'MOBILITY 2000' 등의 활동에 의해 진행되어 오다가, 1991년 '육상교통효율화법' 이 제정됨에 따라 본격화 되었다. 이는 1994년에 'ITS America'로 변경되어 ITS 전문기구로 연방 교통성(FOT)의

정책 및 연구 자문 역할을 수행하고 있다. 그리고 미국은 분야별로 첨단교통체계인 ITS를 구축하고 있는데, 교통관리 도시교통신호제어시스템(TSCS)을 통해서 실시간으로 간선도로 상의 교통상황을 파악할 수 있는 검지기를 여러 도시에서 설치 및 활용하고 있다. 이는 간선도로 교통 정보, 고속도로 관리 시스템(FTMS)을 통해 사고관리, 교통제어, 교통 정보제공, 공공의 안전성 확보를 위해 DMS(Dynamic Message Signs), Har(Highway Advisory Radio), IVS(In-Vehicle Signing)을 통하여 운전자에게 정보를 제공하고 있다.

일본의 ITS 교통관제는 1983년경부터 건설성(MOC), 경찰청(NPA), 통산성(MITI), 운수성(MOT), 우정성(MPT)의 정부 5개 부처가 중심이 되어 추진하고 있다. 1996년 "일본 ITS종합계획(Comprehensive plan for ITE in Japan)"을 발표하여 ITS 사업이 궁극적으로 광역 통합 관제시스템으로 개선될 수 있도록 표준화 등의 계획을 수립하였다.

특히 일본은 첨단자동항법시스템(VICS)이라는 실시간교통정보제공 서비스를 구축하여 통행시간, 교통체증, 사고, 주차정보, 제한속도 등의 정보를 제공하고 있다.

유럽은 1980년대 중반 이후 범 유럽적인 추진조직을 구성하여 첨단교통체계를 위한 프로그램으로 EUREKS에 의한 PROMETHEUS(1986~1995)와 유럽 위원회(European Community)에 의한 DRIVE I(1989~1991), DRIVE II(1992~1994), T-TAP(1995~1998) 등이 ITS 연구의 대표적이다. 유럽의 '도로교통을 위한 Telematics(Road Transport Telematics)' 계획은 교통부문에 정보통신기술을 적용하여 차량, 사람, 하부구조사이에 통합된 환경을 만들어 안전성 향상, 효율성 제고, 환경개선을 궁극적 목표로 하는 첨단교통체계 구축사업을 진행해 오고 있다[5].

(3) 재난관련 ITS 운영 및 개선내용

현재의 ITS 관련 연구들은 운전자에게 교통정보를 실시간으로 제

공하는데 대부분 초점이 맞추어져 있다. 그러나 도로침수, 교통사고 등의 긴급 상황에 대한 대처가 미비하다. 도로침수의 경우 관리자가 직접 해당 지점의 신호를 제어해야 한다. 그러나 교통 혼잡의 상황에서, 신속한 대응이 사실상 불가능하며, 인근 지역의 우회도로를 고려하기 힘들다. 따라서 ITS에서 긴급 상황 지역을 광범위하게 원격 조정 제어 할 수 있는 기능과 긴급 상황 별 신호등의 알고리즘 연구가 필요하다.

다음은 재난과 ITS와 연관된 연구들 및 개선 내용이다.

(a) 재난 상황에 따른 도로 운영 및 대응 방안이 미흡

우리나라의 경우 홍수, 태풍 등 자연재해의 발생이 증가하는 추세에 있고, 그에 따른 도로침수 등의 재난에 대비한 조기감지 및 대응이 신속하게 이루어지는 연구가 필요하다. 이전에도 도로침수로 인한 재난발생의 정보 부족으로 도로 이용자 및 운영자들이 통제 불능의 상태로 빠지게 되어 도로의 극심한 정체는 물론 나아가 인명 및 재산 피해가 발생하기도 하였다. 이러한 도로 정체를 해소하고 이용자의 안전을 확보하기 위해서는 재난 ITS 시스템이 지속적으로 개발되어 운전자 및 도로 관리자에게 실시간으로 정보를 제공하는 교통 방재시스템이 구축이 필요하다.

(b) 차량 통신 네트워크 보안 문제

최근 차량의 자율주행에 대한 연구들이 차세대 먹거리 산업으로 각광받고 있다. 우리나라에서도 지능형 차량의 이름으로 다양한 서비스를 제공하기 위한 통신(V2V, V2I) 기술과 이러한 차량 통신 환경에서의 보안 취약성 개선 문제 등에 대한 연구개발이 진행되고 있지만, 아직은 초보단계이다.

그러나 미국의 경우 IEEE 802.11p/P1609(WAVE)에서 US VSCC (Vehicle Safety Communication Consortium)의 지원을 받아서 차량

통신용 키 관리를 위한 익명성 지원 비대칭 암호 기술을 연구하고 있으며, 유럽의 경우 i2010 Flagship의 intelligent car initiative 프로젝트를 통해서 차량 통신에서 보안 및 프라이버시, 키 관리 문제 등에 대한 연구결과를 산출하고 있다.

(c) 효율적인 교통정보 분석 기술 요구

정확하고 효과적인 교통정보를 제공하려면 교통량, 속도, 밀도 및 이동시간 등 상당히 많은 교통 정보가 필요하다. 이러한 정보들은 운전자, 통행자, 교통통제 관련 기관에게는 매우 중요한 정보이다. 이를 위해 이전에는 교통량, 속도, 이동시간 등 교통 매개변수 정보를 수집하기 위해 감응식 루프 검지기(ILD: Inductive Loop Detector)를 사용하여 왔으나, 일정한 공간에서 개별 차량의 이동에 대한 데이터보다는 집단화된 교통 정보만을 제공하는 문제점이 있다. 이는 교통정보 매개변수의 90~95% 이상의 정확성을 제공하기 어렵다고 판단되어 선진국에서는 감응식 루프 검지기 대신 영상처리 기반의 교통정보 분석 기술을 사용하고 있다.

영상처리 기반의 교통정보 분석 기술은 교통량, 차량, 속도, 차량 경로, 밀도 및 차종 구분 등을 포함한 다수의 교통 매개변수들을 측정하는 데 용이하며, 영상 검지기의 경우 루프 검지기보다 넓은 지역을 검지할 수 있고, 설치 및 운용도 교통 흐름에 영향을 별로 주지 않고 비용도 저렴하다. 그러나 아직은 교통체증을 자체적으로 분석하고 해결하기 위한 기술들은 연구가 더 필요하다. 또한 재난이 발생할 경우 기존의 최적 도로정보 알림에서 재난 장소를 우회하여 빨리 갈 수 있는 연구에 대한 기술이 필요하다.

2.3.3 IoT 관제시스템

IoT(Internet of Things)는 인터넷을 기반으로 모든 사물을 연결하는 사람과 사물, 사물과 사물 간의 정보를 상호 소통하는 지능형 기술 및 서비스를 의미한다. 이는 여러 가지 응용분야에 활용될 수 있지만 재난과 관련된 필요한 정보를 수집하여 서버로 정보를 생성하고 전달하는 역할에

활용된다. 그러나 재난관련 정보를 수집하기 위한 장치들은 대부분 취약한 환경에서 동작하며 무선 환경을 통한 수집된 데이터 전달을 위해서는 개선해야 할 많은 문제들이 있다[9].

다음은 IoT 장치들을 이용한 재난관제시스템의 기술 및 응용에 대한 내용이다.

(1) IoT 기술을 적용한 분산형 재난관리시스템

재난, 재해를 사전에 예방 및 통제하고 환경정보를 수집하기 위해 다수의 사물 센서 노드를 설치하고, 정보 수집을 위한 분산형 제어 시스템 기법을 활용하기 위한 연구가 진행되어 왔다. 응용분야에 따라 차이가 있는 하지만 대부분은 재난관련 센서를 통해 주위 환경 정보를 센싱하여 수집된 데이터를 자체적으로 분석하여 재난이 발생하였는지 여부를 판단한다. 이때 주변의 여러 센서 노드들과 정보를 교류하여 목표하는 의사결정에 도달하기 위한 방법이 분산형 재난관리 시스템이다. 그러나 앞에서도 설명하였듯이 재난과 관련된 정보를 수집하기 위해서는 환경이 열악할 뿐만 아니라 습한 곳에서 오랫동안 자체적으로 전원을 생성하면서 정보를 수집해야 하는데, 이러한 기술은 아직도 개발되어야 할 내용이 많이 있다. 그러나 이러한 연구들은 최근 센싱 기술의 발달과 초소형 및 저전력 센서 기술들이 개발되면서 다양한 위치에서 정보를 수집할 수 있는 환경이 조금씩 제공되고 있다. 이러한 기술 발전과 무선 정보전송 기술의 발전은 IoT 기반의 재난관리시스템 개발이 가능한 환경으로 진행하고 있다.

(2) IoT 기술을 적용한 하천관리시스템

이는 유량·수질측정망을 연계한 IoT 기술과 연계한 홍수·가뭄 및 하천관리에 적용하기 위한 시스템이다. 하천은 기본적으로 상류와 하류까지 넓은 지역을 대상으로 홍수와 가뭄에 의한 범람과 적조 등의 문제가 항상 존재하고 있다. 집중호우에 의한 범람의 경우 상류에서 흘

러들어온 수량의 점검이나 CCTV 등 다양한 정보 수집원을 통해서 특정 위치의 범람을 예측할 수 있는 연구들이 진행되고 있다. 이러한 하천의 범람은 인명피해는 물론 경제적 손실이 매우 크기 때문에 사전에 범람을 예측하는 기술은 매우 중요하다. 그러나 사람들은 실제 범람이 발생한 경우에 판단이 쉽지만, 예측은 시스템 환경에서 자동으로 판단을 하기 위해서 하천 주변에서 올라오는 다양한 정보들을 취합하여 범람에 대한 빠른 의사결정이 이루어져야 사용가능한 하천관리 관제시스템이 될 수 있다.

[그림 2]는 부경대 도시방재연구실에서 연구한 수영강을 대상으로 다양한 침수관련 센싱 정보를 활용하여 특정 지점 혹은 특정 영역의 범람 범위를 예측하기 위한 시뮬레이션 내용을 나타내고 있다. 여기서의 연구는 하천 주변의 다양한 센싱 정보들을 가상으로 설정하여 시뮬레이션 모델링을 수립하였지만, 실제 재난환경에서 사용되기 위해서는 하천 주변에 IoT 장치들의 센싱 정보를 이용하여 현장 중심적 하천관리 관제시스템에 적용되어야 한다.

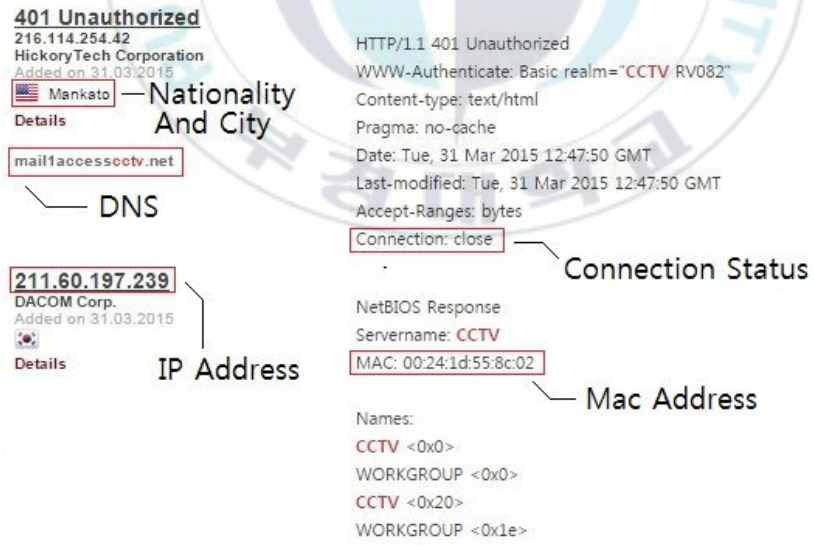
[그림 2] 실시간 침수예측 및 하천관리시스템의 시뮬레이션

2.4 물리보안 관제시스템

현재 운영 중인 재난관제시스템은 대부분 IP기반의 센서 노드를 활용한 재난정보 수집을 이용하여 관제시스템을 운영한다. 따라서 본 절에서는 IP주소 기반 물리보안 관제시스템, 특히 IP기반 CCTV, 각종 인증장비, 교통관제, IoT 관제 등의 물리보안관제 장비들에 대한 보안 취약성을 알아보고, 이들의 문제점을 분석한다[12].

2.4.1 IP기반 IoT 장치의 검색 엔진

쇼단(Shodan) 검색 엔진은 미국에서 만들어진 사물인터넷(IoT) 디바이스의 검색 엔진으로, 방대한 검색 결과와 정확도를 자랑한다. 키워드를 입력하면 웹 기반 사용자 인터페이스 전용 HTTP 헤더를 검색하여 해당 키워드를 포함하고 있는 장치의 IP주소, 접속 가능한 포트, 장치의 국적과 도시, 위도와 경도 등 많은 정보를 보여준다. [그림 3]은 쇼단 검색엔진을 이용하여 수집할 수 있는 정보를 나타내고 있다.



[그림 4] 쇼단 검색엔진을 이용한 수집가능한 정보

이 결과와 더불어 해당 장치의 기본적인 다른 정보를 인터넷으로 검색하여 얻을 수 있는 2차적인 정보들까지 더한다면, 해킹과 크래킹에 아무

런 지식이 없는 사람일지라도 불특정 다수의 기기에 대한 관리자 권한을 획득하는 것이 어렵지 않다. 주로 CCTV나 웹캠이 많이 검색되며, 공유기나 라우터, 와이파이 익스텐더, NAS, 가정용 스마트 홈 컨트롤 디바이스까지 검색 및 접속이 가능하다[11].

다음은 영국의 umbrellium사에서 만든 씽풀(Thingful.net)은 쇼단과는 조금 다른 성격을 가지고 있다. 사물 인터넷 장치에 대한 검색 목적은 동일하지만, 접근을 허용한 공공 기기들에 대한 정보 수집이 주요 목적이다. 주요 카테고리는 건강, 환경, 가정용, 운송, 에너지, 식물과 동물로 나뉘고 공공 목적에 필요한 정보를 공유하는 것이 목적이다. 예를 들면 대기 성분을 분석하는 장치라던가, 현재 항해 중인 배의 정보라던가, 온실의 온도와 습도 등을 나타내는 장치들을 접근하여 정보를 수집할 수 있다. 씽풀은 기본적으로 모든 정보를 GIS에 기반하여 지도에 위치를 표시하고 있기 때문에 위치정보와 센싱 정보를 이용하여 유용한 목적에 사용할 수 있다. 그러나 씽풀도 쇼단의 악의적인 접근 정보를 얻는데 활용될 수 있기 때문에 이러한 문제점을 공유하거나 사용을 불허하는 정책이 필요하다.

2.4.2 국내외 물리보안 관제시스템 피해사례

본 절에서는 국내외 물리보안 관제시스템이 피해사례를 기술하고, 이들의 문제점에 대해 설명한다[6].

(1) 국내 물리보안 관제시스템 피해사례

국내 물리보안 관제시스템의 피해사례는 여러 가지가 있으나, 본 절에서는 본 연구와 관련 있는 부분만 기술한다.

가. CCTV에 백도어 설치

국외 유명 CCTV 제조사 두 곳은 국내에 판매중인 일부 IP기반 CCTV 카메라에서 녹화된 영상정보를 유출할 수 있는 백도어 기능을 몰래 심어져 있는 것으로 조사되었다. 이는 자사가 제조한 IP카메

라의 모든 권한을 가질 수 있는 백도어를 심어놓고, 제조사의 클라우드 서버를 통해서만 접근할 수 있도록 하여 사생활 침해는 물론 국가기반 시설의 정보 유출이나 관제시스템의 사용불능을 유도할 수 있는 문제점이 있다.

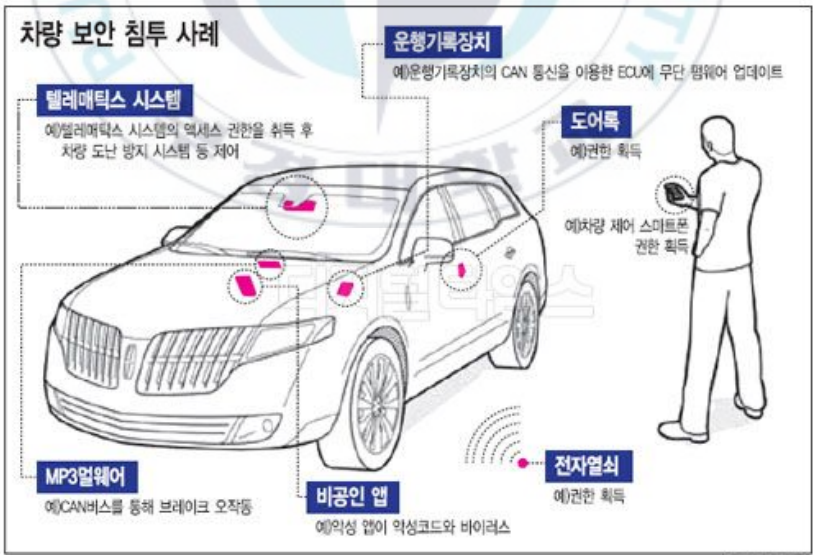
[그림 4]는 국외 CCTV 업체의 백도어 장착 내용을 나타낸 것으로, 해당 IP카메라에 대해 관리자 권한을 획득한 공격자가 임의의 악성코드를 설치해 영상정보를 탈취하는 것은 물론, 이 카메라가 기업이나 국가 주요시설에 네트워크로 연결되어 있을 경우에는 공격자가 내부 네트워크로 접속하여 산업 기밀이나 국가 중요 기밀 등을 훔쳐낼 수 있다.

[그림 4] 국외 CCTV 업체의 백도어 장착 현황

나. 스마트카 서비스 해킹

2013년 해킹 컨퍼런스 데프콘21에서는 도요타, 프리우스, 포드 등의 자동차를 해킹하여 마음대로 조작할 수 있게 만드는 방법을 공개하였다. 포드 이스케이프는 자동차의 대시보드 부분을 열어 일부를 조작해 노트북과 무선통신을 할 수 있도록 하여 주행 중인 자동차의

브레이크를 못쓰게 만들거나 핸들을 마음대로 조작하는 등의 동작을 시연했다. 또한 엔진을 끄거나 라이트를 켜는 등의 행위와 경적을 울리는 동작을 하였으며, 연료가 없는데도 연료가 가득 차있게 보이도록 하는 시연도 하였다. 이러한 해킹의 원리는 자동차에 사용되는 각종 센서들을 직·간접적으로 조작하는 것으로, 최근 관심을 많이 가지고 있는 자율주행 자동차는 GPS, 라이다(LIDAR), 카메라, 밀리미터파 레이더(millimeter wave radar), 디지털 콤파스, 휠 인코더, 관성측정 유닛 등 수많은 센서와 연동하여 주행하게 된다. 그러나 자동차의 IP기반 다양한 센서들을 외부에서 접근이 가능하다면 매우 심각한 재난이 발생할 수 있는 가능성이 존재하게 된다. 따라서 이러한 IP 기반의 센서 노드들이 자동차는 물론 재난관제시스템에 적용될 경우 센서 노드의 보안에 대해서는 아주 세밀한 설계와 분석이 필요하다. [그림 5]는 데프콘 21 컨퍼런스에서 시연한 스마트 카의 해킹 사례를 제시하고 있다.



[그림 5] 스마트카 외부 해킹의 사례

다. 홈 오토메이션 시스템에서의 해킹

최근 가정에서도 다양한 IoT 장비들이 판매되면서 홈 오토메이션 환경이 구축되고 있다. [그림 6]은 홈 오토메이션 시스템의 콘솔 화면을 나타낸 것으로 다양한 장치들을 제어할 수 있는 환경을 제공하고 있다.

[그림 7] 홈 오토메이션 시스템의 콘솔 화면

그러나 홈 오토메이션의 편리함도 있지만, 이도 앞의 스마트 카와 유사하게 다양한 센서들이 연계되어 운영되기 때문에 외부의 해킹은 항상 열려져 있다. 예를 들면 HP 사는 10종의 홈 완제품 보안시스템을 조사한 결과 비밀번호 및 중간자 공격에 취약한 기기들이 많음을 보고하였다. 또한, 코드 보안업체인 베라코드(Veracode) 사는 장치의 디버깅 인터페이스 접속을 방어하지 못해 관련 기기를 쉽게 해킹할 수 있다는 보고를 하였다.

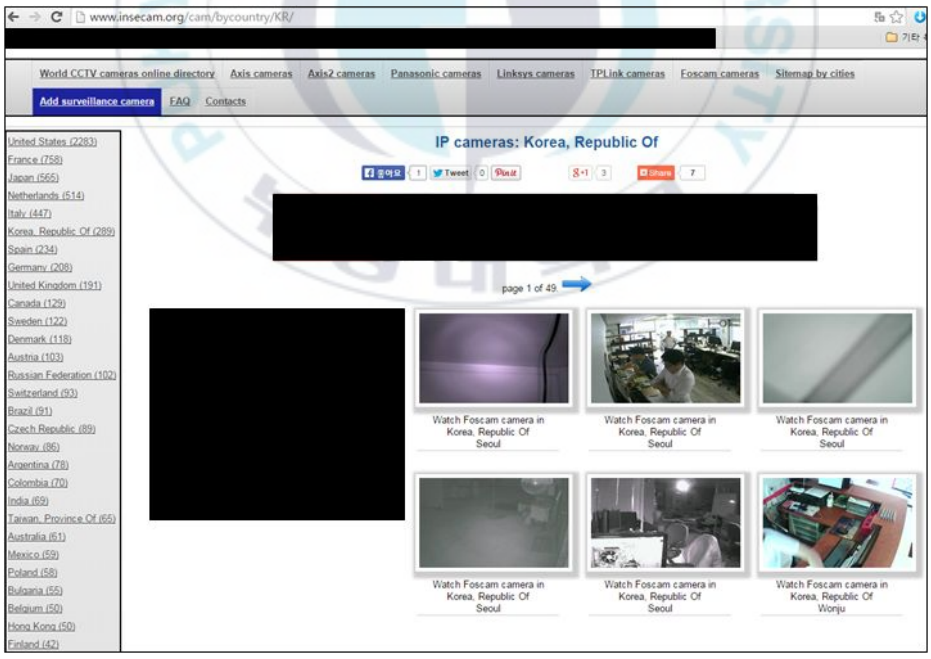
홈 오토메이션도 다양한 센서 노드들이 가정의 편리함을 위해 적용되고 있지만, 이들의 보안 취약성으로 재난의 위험에 직면할 수 있다. 따라서 IP를 기반으로 한 홈 오토메이션 장치들에 대한 보안 강화 정책은 필수적이다[14].

(2) 국외 물리보안 관제시스템 피해사례

앞에서 국내 물리보안 관제시스템의 피해사례는 설명하였고, 본 절에서는 국외 물리보안 관제시스템의 피해 사례를 기술한다.

가. 러시아 인스캠 사이트의 해킹

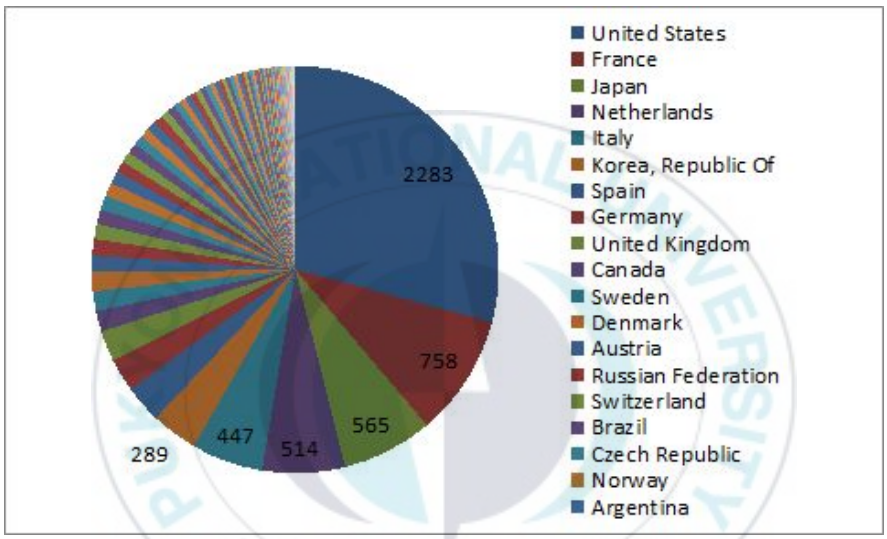
2014년 러시아의 인스캠(Insecam)이라는 사이트에서 IP주소가 노출된 개인용 CCTV 73,000여 개를 해킹하였고, 해킹당한 CCTV의 화면들을 실시간으로 생중계하여 개인 사생활을 침해하였다. 해킹 방법은 먼저 인터넷에 노출되어 있는 수많은 IP주소를 수집하고 그 중 패스워드가 없거나 'admin-1234', 'admin-admin' 등과 같은 기본 패스워드를 가지고 있는 CCTV에 접속하여 권한을 얻은 후 CCTV 화면을 획득하는 방법을 사용하였다(그림 7 참조).



[그림 7] 인스캠 사이트의 CCTV 해킹 화면

[그림 7]에서 좌측 메뉴에는 국가별 CCTV 영상을 구분하고, 해킹당한 CCTV의 개수를 표시하였고, 중앙에는 사이트 접속자가 선택한

CCTV의 화면을 볼 수 있도록 구성하였다. 국내 CCTV도 6,000여 개가 해킹당한 상태를 보여주고 있다. 2015년 6월 인스캠 사이트에서 공개하고 있는 디바이스의 수는 예전에 비해 많이 줄었지만 여전히 7800여개의 장치들이 보안의 허술함으로 인해 해킹되고 있음을 [그림 8]은 보여주고 있다. 아래 그림에서 볼 수 있듯이, 미국의 장치 수가 가장 많고, 그 다음 프랑스, 일본, 네덜란드, 이탈리아, 한국, 스페인, 독일의 순이고 이 외에도 수많은 국가들의 장비가 공개되어있다.



[그림 8] 인스캠에서 공개된 해킹 장치들의 국가별 분류(2015년 6월)

비록 인스캠의 해킹 사례가 CCTV 보안 설정의 중요성을 알리기 위해 발생한 것이라 하더라도, 쉽게 IP주소를 인터넷에서 획득할 수 있다는 점과 기본 패스워드를 바꾸지 않거나 설정 자체를 하지 않는 등 사용자들의 보안에 관심을 가지지 않으면 적게는 개인 사생활 침해로 이어질 수 있으며, 크게 국가의 중요한 재난관제시스템에 대한 공격까지 가능하다.

나. 미국 중앙 교통 관제시스템의 해킹

2009년 미국 인디아나주에서는 해커가 중앙교통통제시스템을 해킹

해 “앞쪽에 공룡이 있으니 주의하세요”라는 메시지를 교통표지판에 남긴 사례가 발생하였다([그림 9] 참조). 이는 어떻게 보면 단순히 전광판의 글자만 바꾼 것으로 간단한 장난으로 생각될 수 있으나, 만일 공사 중인 도로 상태를 정상적인 상태로 문자를 변경하여 알려주면 큰 교통사고를 유발할 수 있다.

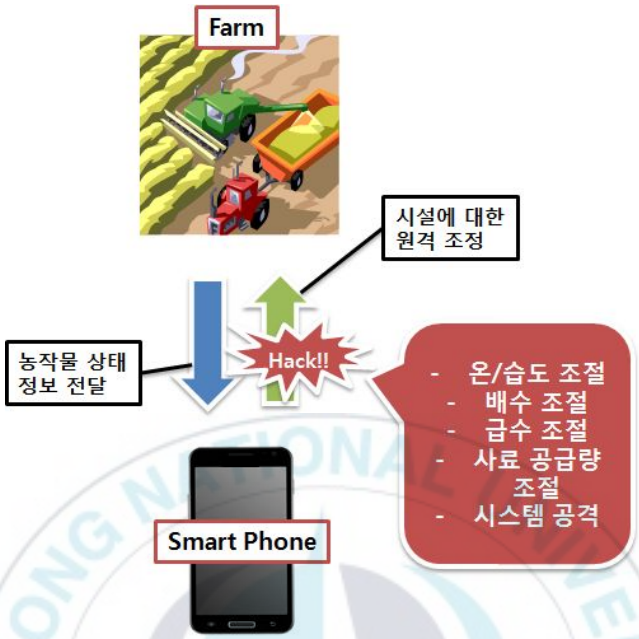
[그림 9] 미국 중앙교통통제시스템 해킹

다. 스마트팜 서버시스템의 해킹

스마트팜은 최근 건강한 생활 환경에 관심이 많은 사람들이 많이 접근하여 활용하는 생활 및 환경 관제시스템으로 볼 수 있다. 사물인터넷을 효과적으로 이용하는 사례 중 하나가 바로 스마트팜(Smart Farm) 서비스로 볼 수 있다. 국내 모 통신사는 스마트폰을 이용하여 농작물의 상태나 비닐하우스의 온도·습도 등의 정보들을 알 수 있는 스마트팜 서비스를 선보였으며, 유럽 등 국외에서도 비닐하우스 내부의 온도·습도 및 급수와 배수, 사료 공급 등을 원격 지원하는 스마트팜 서비스가 도입되었다.

그러나 유럽에서 스마트팜을 악의적으로 해킹하여 원격제어를 통한 온도, 급수, 사료공급 등을 망쳐놓으려는 시도가 있었다. 만약 스

마트팜에 대한 해킹이 성공하였다면 농작물이나 축산물 등의 관리 시스템이 엉망이 되어 막대한 피해를 입게 되었을 수도 있었다.



[그림 11] 스마트팜 서비스 해킹

앞의 여러 가지 IP 기반 IoT 장치들에 대해 해킹이나 불법 접근에 의해 개인적인 피해나 국가적인 피해는 항상 열려져 있음을 볼 수 있었다. 앞으로 IoT 기술들이 발전할수록 다양한 관제시스템은 늘어날 수 밖에 없기 때문에 IoT 장치들의 보안관리는 매우 중요한 요소이다. 본 연구에서도 이러한 문제점을 고려하여 재난관련 관제시스템의 취약성 분석과 개선 방안을 연구하고자 한다[12].

3. 재난안전 정보시스템 취약성 분석

3.1 재난안전 정보시스템 통합 필요성

최근 재난안전은 기존의 재난안전 관련 기술과 IT기술을 융합한 정보시스템을 구축하여 빠른 정보 생성은 물론 재난에 대응하기 위한 연구와 관심이 집중되고 있다. 본 연구는 재난안전 정보시스템을 구축하기 위한 다양한 정보들의 조사하고, 기존의 이러한 정보시스템들이 어떤 취약성이 존재하는지 분석한다.

3.1.1 자연재해 및 인적재난의 대응시스템 분석

모든 나라는 다양한 재난으로부터 국토를 보존하고 국민의 생명과 재산을 보호하기 위한 법률 및 시행령을 제정하여 운영하고 있다. 우리나라는 재난 및 안전관리 기본법에는 크게 자연재해와 사회재난으로 구분하고 있으며, 좀더 포괄적인 의미에서 해외재난이라 하여 대한민국 영역 밖에서 국민의 생명과 재산을 보호하기 위해 법률을 정의하고 있다.

본 연구에서는 정부의 재난 및 안전관리 기본법에서 보다 세분화하여 자연재난, 인적재난, 사회적 재난 중에서도 주요 재난 영역에 대한 방재대상 영역과 피해원인 및 현황, 필요 데이터, 대응시스템에 대해 살펴본다.

자연재해는 태풍, 호우, 홍수, 폭풍, 설해, 가뭄, 지진, 지진해일, 해일, 황사, 적조, 냉해/동해, 우박/서리, 병충해 등으로 분류할 수 있으며, 냉해(cold-weather damage)는 여름철 저온에 의한 농작물 피해의 경우이며, 동해(freezing damage)는 겨울철 심한 추위로 농작물의 피해

가 발생하는 경우이다. 인적재난은 화재(폭발포함), 도로 및 철도, 지하철, 산불(기타 산림재난 포함), 전기/가스/유류, 붕괴사고, 다중이용시설, 시설물 및 위험물, 방사능, 해상, 항공, 통신, 환경오염, 산업단지사고, 유도선(조명이 없는 계단/빌딩의 비상 유도), 문화재 등이 포함된다. 사회적 재난은 노동쟁의, 파업, 조류독감, 쇠고기 파동 등이 포함되며, 이 외에도 해외 재난에 대한 내용들이 포함된다.

본 논문에서는 자연재해와 인적재난을 중심으로 사람들에게 가장 많이 발생할 수 있는 재난발생에 대한 재난 유형에 따른 방재시스템 구축 내용을 정의하고자 한다.

자연재해의 경우 본 논문에서는 홍수(호우 포함), 태풍, 폭풍 및 지진해일, 지진, 폭설, 황사, 가뭄에 대한 방재대상영역, 방재시스템 구축을 위한 정보수집 데이터, 방재 대응시스템에 대한 내용을 간략히 기술하면 [표 5]와 같다[1,2,14].

[표 5] 자연재해 유형별 방재 정보시스템 데이터 및 대응시스템

자연재해 유형	방재대상영역	필요데이터	대응시스템
홍수 (집중호우 포함)	하천, 도로, 산사태, 붕괴, 교통/통신 두절 등	도로/지형도/지질도, 과거이력, 피난정보, 주민정보, GIS, 각종 통신정보, 조수간만	-홍수예측 및 대응시스템(주민대피 포함)
태풍	붕괴, 해일, 낙석, 산사태, 농작물, 비닐하우스 등	위의 홍수 필요데이터, 기상청정보, 바람피해 이력정보 등	-태풍정보시스템
폭설	기온/강수/풍속, 도로통행, 농/축산물, 산행 등	도로/지형도/지질도, 폭설이력 및 피난정보, 농축산물정보 등	-폭설 예측 및 대응시스템
해일(태풍/지진)	도로, 선박, 해안침수 등	도로/해안지형도, 해일이력정보 등	-해일정보시스템

[표 5] 자연재해 유형별 방재 정보시스템 데이터 및 대응시스템 (계속)

자연재해 유형	방재대상영역	필요데이터	대응시스템
지진	항구, 선박. 원자력 발전소,	홍수 필요 데이터 외 지형/지반/지질도, 지진예측정보	-지진대응시스템
황사	항공기, 호흡기 질환, 청소비용	홍수 필요데이터 외 기상청, 풍향/풍속/습동,	-황사예측시스템
가뭄	농작물, 주민 급수, 농업 및 공업용수	홍수 필요데이터 외 가뭄이력, 저수량/용수량	-가뭄예측 및 대응시스템

다음은 인적재난에 대한 내용으로 본 연구에서는 화재, 교통사고, 폭발, 붕괴, 화생방, 환경오염에 대한 정보시스템 구축을 위한 방재대상영역 및 필요한 데이터에 대해서 살펴본다([표 6] 참조).

[표 6] 인적재난 유형별 방재 정보시스템 데이터 및 대응시스템

인적재난 유형	방재대상영역	필요데이터	대응시스템
화재	지하공간, 고층빌딩, 터널, 선박, 항공, 화학공장 등	화재이력, 지하공간/도로/터널/공장 등 화재취약정보,	-화재대응 및 대피시스템
교통사고	도로, 교량, 어린이, 교차로, 야간, 교통체증, 2차사고, 태풍/폭설/호우 등	도로, 교통량, 위험지역, 대풍/호우/폭설, CCTV 등 IT정보	-교통체증 및 사고대응시스템
폭발	대형트럭, 화학공장, 지하철, 방화, 도시가스, 위험물질 등	가스/인화물질/방화, 안전교육 등	-폭발대응시스템
붕괴	건축물, 다리, 사면 등	홍수/폭설, 노후건물정보, 다리/사면/ 등	-붕괴대응시스템

[표 6] 인적재난 유형별 방재 정보시스템 데이터 및 대응시스템(계속)

인적재난 유형	방재대상영역	필요데이터	대응시스템
화생방	화학적원인, 생물학적원인, 방사능	생물/독소, 해독제, 공중위생, 방사능, 화생방교육, 국제대응 등	-화생방 대응시스템
환경오염	대기오염, 수질오염, 토양오염 등	대기(도시, 공장), 하천수질, 연안해양, 공장, 도시개발토양	-환경오염 대응시스템

인적재난의 유형은 자연재해의 경우보다 더 많지만, 본 연구에서는 자연재해와 같이 우리 주변에서 많이 발생할 수 있는 재난을 대상으로 현재 구축되어 있는 정보시스템이나 향후 구축할 정보시스템을 대상으로 시스템 구축에 따른 최신 IoT 장비들을 대상으로 취약성 분석을 진행하고자 한다.

3.1.2 재난 대응시스템의 연계성 분석

IT기술의 급속한 발전과 도시의 거대화 및 사람들의 도시 집중화는 고층빌딩은 물론 거미줄 네트워크를 형성하고 있는 도로, 그리고 거대한 지하철 및 지하상가 등의 구축은 사람들에게 편리함을 제공해 주지만, 상대적으로 위험성은 매우 높아지고 있다.

IT기술은 우리가 살고 있는 사회를 여러 가지로 변화시키고 있다. 2000년대 초부터 유비쿼터스라는 용어가 학계에서 사용되기 시작하면서 IT기술을 활용한 여러 가지의 실험적인 테스트와 실제 적용을 위한 계획을 국가, 지자체, 대학 그리고 기업들이 많은 관심을 가지고 시도를 해왔다. 이러한 유비쿼터스 환경을 구현하기 위한 다양한 접근방향에서 u-라는 알

파벳 단어를 앞에 붙여서 실험적인 연구들이 진행되었는데, 그 중에서 국가와 지자체는 물론 기업들도 많은 관심을 가진 u-City라는 단어의 사용이다. u-City의 기본 개념은 USN(Ubiquitous Sensor Network)기반의 IT 기술을 적용하여 사람들에게 편리함을 제공하는 것은 물론 지자체는 도시관리, 기업은 경제적인 성과를 창출할 수 있는 기회로 생각하고 대부분의 지자체들은 다양한 이름의 u-City라는 사업으로 도시의 첨단화를 이끌어 왔다.

이와 같이 도시의 거대화와 IT기술의 발달로 사람들에게 편리함을 제공하지만, 이면에는 안전과 재난에 따른 문제점 해결 방안에 대한 방법들이 고려되어야 한다. 본 절에서는 재난안전 정보시스템 관점에서 u-IT의 연계 방안에 대해 설명한다[8,10].

1) 재난안전과 u-IT의 연계

각 지자체는 도시의 경쟁력을 향상시키기 위해 지자체의 특성을 고려한 u-City 사업을 적극적으로 추진하여 왔으며, 대부분의 지자체는 방재 또는 안전이라는 이름으로 u-City 사업의 중요한 부분 중의 하나로 재난에 대비한 예방 사업을 적극 추진하여 진행하였다. 이러한 테스트베드 사업은 IT 기술을 접목한 방재영역이 반드시 고려되고 있으며, 지자체가 가지고 있는 기존의 인프라를 최대한 연계된 통합방재시스템 구축을 목표로 하고 있다. 기존의 도시 방재에서 유비쿼터스 방재 기술은 USN을 기반으로 한 실시간 및 정량화된 데이터 수집을 가능하게 하며, UIS(Urban Information System)정보와 연계하여 시민들에게 필요한 정보를 지도와 함께 신속하게 전달할 수 있다.

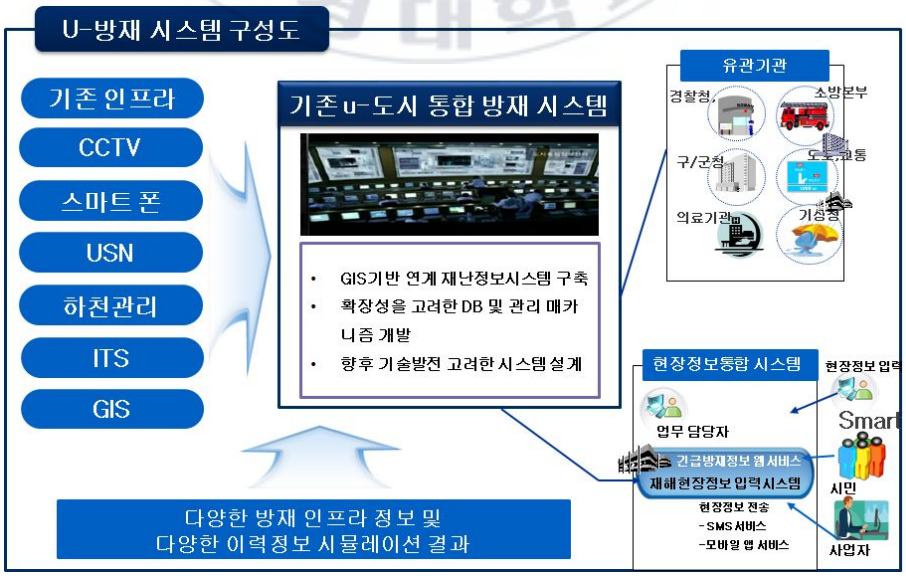
도시방재와 IT 연계 기술의 접목 방향은 u-City를 위해 구축한 다양한 IT 인프라를 활용하여 통합 표준플랫폼에서 시민 및 사업자, 정부

및 지자체 유관기관에 필요한 정보를 제공하는 과정이 필요하다. 도시의 대형 건축물과 복잡한 도로망은 재난안전과 관련된 정보를 다양한 방법으로 정보를 수집하기 위해서는 지자체, 국가 또는 기업에서 제공하는 인프라와 연계가 되어야 한다. 이러한 인프라와 센싱 장치들에서 올라오는 정보들을 통합운영센터는 다양한 자료와 인프라 정보들을 종합적으로 분석할 수 있는 기능과 분석된 결과를 관리자 혹은 시민들에게 빠른 정보를 전송하기 위한 모니터링 및 정보전송 방법의 시스템들이 필요하다. 그러나 기존의 통합 플랫폼들은 각 지자체가 자체적으로 통합시스템 내에 안전관련 기능들을 추가하여 관리하고 있기 때문에 전체적으로 보면 각 지자체는 자체의 플랫폼 기반 재난관리 모듈들을 가지고 운영하고 있다. 이는 특히 자연재해의 경우 재난영역이 광범위하기 때문에 각 지자체가 가지고 있는 플랫폼들이 연계되고 정보를 교환할 수 있는 기능들이 포함되어야 하나 그렇지 못한 상태이다. 따라서 재난안전과 u-IT기술들을 연계한 정보들을 수집하고 분석하여 필요한 기관이나 시민들에게 종합적인 정보를 제공할 수 있는 통합 플랫폼 구축이 필요하다.

2) 도시안전의 통합 정보시스템 구축방안

u-도시방재 통합 정보시스템 구축 방안은 통합 플랫폼 인프라를 기반으로 재해·재난을 위해 필요한 정보들을 관리하는 기능이 필요하다. 도시안전 통합 정보시스템 구성은 크게 3가지로 구성할 수 있다. 하나는 현장정보를 수집하는 시스템 구축과 다른 하나는 현장에서 올라오는 정보들을 다양한 미디어들로 분류하고 이들을 분석 및 필요한 정보들로 가공하는 재해·재난 통합정보시스템 구축 내용이며, 다른 한 구성은 이러한 정보들을 어떤 기관 혹은 사람들에게 정보를 제공할 것인가에 대한 상세한 구축 방안에 대한 내용들이 필요하다. 첫 번째

를 위한 정보수집 방법은 현장에서 가장 직접적이고 실시간적으로 정보를 수집할 수 있는 휴대폰 등의 모바일 기능과 CCTV 등의 동적 아날로그 정보를 수집하는 것이다. 이 외에도 시와 구/군 방재관련 정보, 동네 예보, 소방본부, 사회단체 등 재난정보를 수집할 수 있는 시스템 구축이 필요하다. 둘째는 현장 및 시/군/구 등에서 수집한 정보를 다양한 미디어별로 분류와 연계를 할 수 있는 데이터베이스 및 모니터링 시스템 구성에 대한 방안이 필요하다. 그리고 향후의 IT기술의 발전을 고려한 클라우드 기반의 데이터 관리 및 분산에 대한 구성도 고려되어야 하며, USN 기술을 사용하기 위한 IoT 장치들에 대한 정보수집 및 분석 방법, 특히 자연재해는 관련된 데이터가 방대하기 때문에 빅데이터 분석을 위한 추가 기능을 위한 시스템 구성에 대한 방안도 고려되어야 한다. [그림 11]은 u-도시안전 통합 정보시스템 구축을 위한 전체적인 내용 및 개발 방향에 대한 내용을 제시하고 있다. 그러나 아직은 [그림 11]과 같이 통합된 형태의 도시안전 통합시스템 구성은 초보적인 단계에 있다[3,5,6].



[그림 11] u-도시안전 통합시스템 구축 방안

3.2 재난안전 정보수집 및 정보시스템 구축의 취약성

재난안전과 관련된 정보 수집은 재난의 종류에 따라 수집해야할 내용은 완전히 다르다. 본 연구는 자연재해를 중심으로 시스템 설계를 제안하고 있기 때문에 인적재난보다는 자연재해 중심의 정보수집 및 시스템 구축 방법에 대해 연구한다. 앞에서 기술한 자연재해는 여러 가지 원인들이 있겠지만, 태풍, 호우, 홍수에 대한 재해가 인명은 물론 경제적인 피해를 가장 많이 발생하고 있다. 이러한 관점에서 본 논문에서는 태풍이나 호우에 의해 도시지역의 침수가 발생할 경우 빠른 대피와 경제적인 손실을 최대한 경감하는 것이 필요하다. 과거의 재해·재난은 대응과 복구 중심에서 최근에는 예방과 대응의 관점으로 변화하고 있다. 이와 같이 예방을 위해서는 과거의 정보와 IT기술을 최대한 연계하여 사람들에게 예측된 정보를 가능한 빨리 정보를 제공하는 것이 필요하다. 이를 위해 본 연구에서는 태풍이나 집중 호우에 따른 IT기술을 기반으로 정보수집에 따른 취약성을 알아본다.

3.2.1 도시 지역의 재해정보 수집의 취약성

도시지역의 재해관련 정보 수집은 각 도시가 가지고 있는 환경과 지정학적 요소에 따라 수집해야할 정보들은 많은 차이점을 가지고 있다. 앞의 3장에서 기술한 자연재해 및 인적재난의 대응시스템에서 수집해야할 방재대상영역 및 데이터에 따른 대응시스템 구축은 각 도시별로 차이점이 있다. 그러나 재해정보의 수집은 사용 목적에 따라 달라진다. 그 이유는 수집된 정보를 어떻게 활용할 것인가에 있다. 수집된 정보를 기준으로 장기적인 관점에서 도시계획과 대응시스템을 구축할 경우에는 다양한 정보들을 종합적으로 판단할 필요가 있지만, 시민들의 안전과 경제적 손실을 예방하기 위한 대응시스템을 구축할 경우 수집되는 데이터는 완전히 다르다.

이러한 관점에서 [표 7]은 재해정보 수집에 따른 사용목적의 차이점을 나타내고 있다. 장기적인 관점에서는 자연재해든 인적재난이든 필요한 정보들은 대부분 비슷하거나 지자체의 특성에 따라 조금씩 차이가 날 수 있다. 그러나 단기적인 관점에서 실시간 및 현장 정보의 데이터 수집은 정보를 어떻게 가공해서 제공할 것인지와 누구에게 줄 것인지에 따라 매우 다를 수 있다. 예를 들면 실시간 및 현장 정보의 경우 최근에는 현장에 있는 사람들의 휴대폰을 이용한 SNS 정보를 이용하거나 주변에 있는 CCTV 및 관련 센싱 장치들의 정보들을 수집하여 시스템에서 초기 단계의 의사결정과정이 포함된 재난 실시간 대응시스템을 개발하여 시민들에게 제공하고 있다. 그러나 재해의 경우 날씨가 좋지 않거나 인적이 드문 지역에서 재해가 발생할 경우 주변에 사람들이 없거나 정보를 수집할 센싱 장치들이 설치되어 있지 않을 경우 훌륭한 실시간 대응시스템이 구축되어 있다 할지라도 수집되는 데이터의 부족으로 필요한 정보를 생성할 수 없다. 이러한 문제를 해결하기 위해서는 다양한 정보원을 발굴하여 언제 어디서든지 재해에 따른 필요한 정보를 생성할 수 있는 방법을 찾아야 한다.

대부분의 지자체들은 도시의 특성에 따라 필요한 방재서비스를 제공하기 위해 시스템을 구축하여 시민들에게 정보를 제공하고 있다. [그림 12]는 대부분의 지자체들이 최근의 IT기술을 접목한 재해와 재난에 대비한 방재서비스를 제공하기 위해 수집하고자 하는 정보들의 영역을 나타내고 있다. 크게는 대부분의 도시들이 편리하고 안전하고 미래지향적 도시를 구축하기 위해 u-IT 기술을 최대한 연계한 통합 방재시스템을 구축하여 제공하고 있다[6,10].

[표 7] 재해정보 데이터의 수집의 다양성

재해의 종류	장기적 관점		단기적 관점	
	도시계획	사람중심 방재	현장정보	실시간 대응
자연재해	-기상재난정보 -풍수해중심 -지진·해일 재난정보 등 -도시계획시설	-방재대책수립 -풍수해 예측 -지진해일 예측시스템 등	-재난구조/구급 -구/군·지자체 단위 대응 -CCTV, GIS 정보 제공 등 -뉴스, 웹 정보 제공 등	-실시간 위치 정보제공 -신속한 시민대피 -모바일 기반 실시간 정보 제공 시스템 구축 등
인적재난	-화재, 교통 등 -소방, 지하철 -화생방, 환경오염 등	-인적재난별 예측 및 대응시스템 개발 -공공성, 편리성		

[그림 12] 지자체 방재서비스를 위한 정보수집 영역

3.2.2 u-IT 기반의 재해 정보시스템 구축의 취약성

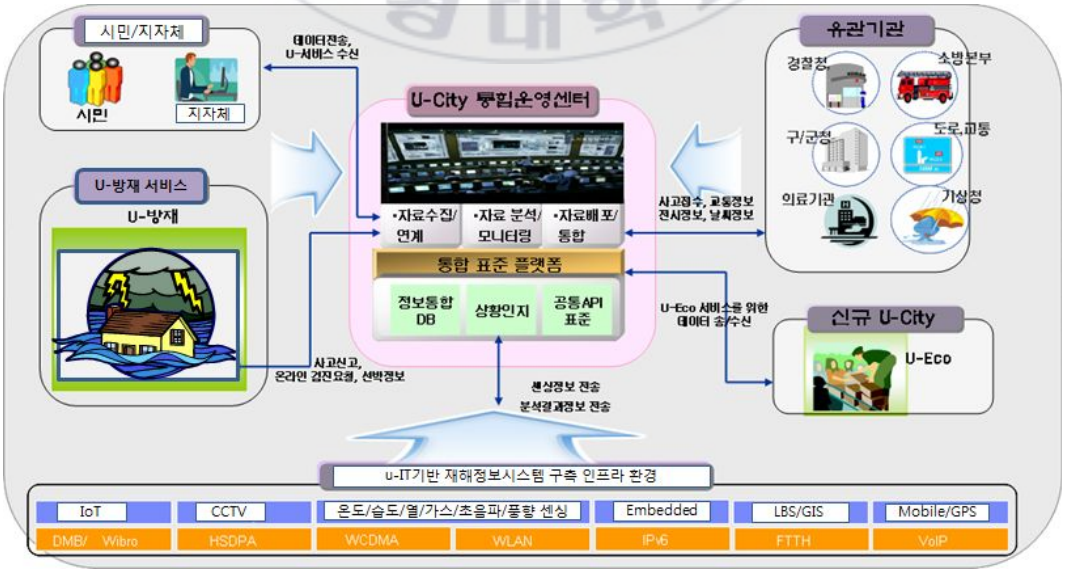
u-IT 기반의 재해 정보시스템 구축은 재해와 관련된 모든 정보를 IT를 이용한 정보시스템을 구축하는 것이다. 여기에 최근의 유비쿼터스 기술을 접목하는 것은 용어의 차이는 있지만, 클라우드 컴퓨팅, 빅데이터, IoT를 종합적으로 연계하는 것은 물론 기존의 IT 인프라를 모두 활용한 미래 지향적 재해 정보시스템을 구축하고자 하는 것이다. 이러한 연구들은 국내는 물론 국외에서도 많은 연구들이 진행되고 있고, 국내에서는 국가기관은 물론 연구소, 대학, 기업들이 최신의 IT기술을 활용한 대용량의 재해정보를 활용한 실시간 방재시스템을 구축하는데 목표를 두고 있다.

그러나 아직은 IoT 장치들이 인터넷에 연결된 것은 1% 정도만 연결되어 있기 때문에 현장 설치는 미비한 수준에 그치고 있으며, 방재의 영역은 재해의 종류에 따라 다르지만 좁은 영역에서 국가 혹은 세계적인 범위까지 방재 서비스의 범위가 매우 다양하게 요구되기 때문에 데이터의 양도 엄청날 수 있다. 범위가 넓을수록 필요로 하는 재해정보와 관련된 기존의 데이터는 엄청난 범위로 늘어나기 때문에 재해와 관련된 IT 인프라 구성도 매우 다양한 시스템들의 연계와 통합이 필요하다. 이러한 관점에서 u-IT기반의 재해정보시스템 구축은 어떤 정보와 연계되어서 활용될 것인가에 대한 정의와 범위가 설정되지 않고는 시스템을 구성하는 것이 불가능하다.

[그림 13]은 본 연구에서 제안하는 u-IT기반 재해정보시스템 구축 및 서비스 방향을 제시한 것으로 미래지향적인 방향보다는 현실적인 상황을 고려한 구축 및 서비스 방향을 제시하고 있다. IT인프라 부분은 최근 많은 발전으로 데이터 전송 및 다양한 디바이스들 간의 연계는 많은 문제점을 해결하고 있으나, 아직 IoT관련 장치들의 현장 설치와 재해와 관련된 다양한 데이터의 연계 및 통합은 아직 해결해야할 문제들이 많이 있다.

그리고 제안된 u-IT기반 방재정보시스템 구축은 지자체 혹은 적용되는 분야에 따라 많은 차이점이 있기 때문에 현장의 상황을 고려한 시스템 설계가 필요하다. 이러한 관점에서 방재정보시스템 구축은 목표하는 방향은 설정할 수 있지만 이들을 연계하고 통합하는 하드웨어와 소프트웨어를 통합한 IT기반의 재해정보시스템 구축은 현실적으로 해결해야할 많은 문제점을 가지고 있다. 최근의 연구들은 현재 나타나고 있는 문제점들을 하드웨어적인 문제와 소프트웨어적인 문제점으로 나누어 해결 방법을 연구하고 있으며, 조금씩 접근 방법을 찾아내고 있다.

앞 절에서도 기술하였듯이 재해정보시스템은 장기적 관점과 단기적 관점에서 정보시스템을 구축하는 데이터의 구성이 많은 차이가 있기 때문에 이들을 통합적으로 고려한 재해정보시스템 구축 방향을 설계하는 것이 매우 중요하다. 아직은 기술적인 문제점과 다양한 방재영역을 통합하고 필요한 영역을 연계하는 과정에 대한 연구들이 필요하며, 체계적인 접근 방법에 대한 연구가 필요하다. 본 연구에서는 이러한 문제점을 제시하고 향후 고려되어야할 취약점에 대해 부분적으로 살펴보는 측면에서 연구를 제안하고 있다.



[그림 13] u-IT기반 재해 정보시스템 구축 및 서비스 방향

3.3 재난대응을 위한 실시간 정보시스템 취약성 분석

재난안전 정보시스템을 구축하기 위해서는 재난 현장에서 일어나는 정보들을 신속하게 수신하고, 다양하게 들어오는 정보들을 통합·연계된 재해정보시스템을 구축하는 것이 매우 중요하다. 앞에서도 기술하였듯이 재난·재해가 발생하면 이들의 종류에 따라 다르겠지만, 어떤 재해던 빠른 대응이 필요한 것이 대부분이다. 이러한 경우 가장 중요한 것이 실시간과 현장의 정확한 정보를 수집하는 것이 필요하다.

앞에서 u-IT기반 재해정보시스템 구축을 위한 전반적인 내용을 기술하였다면, 여기서는 재해의 경우 빠른 대응 능력과 정확한 현장 정보를 수집하는 것이 매우 중요하기 때문에 이들의 정보 수집에 있어서 취약성 혹은 변조의 가능성에 대한 대비가 필요하다고 판단하여 재해 정보수집의 취약성 부분을 다루고자 한다.

3.3.1 재난현장 위치정보 수집의 취약성 분석

재난은 언제 어디든 다양한 공간에서 발생할 수 있다. 이러한 재난은 사람들이 많이 모이는 공간에서 일어날 수도 있고, 그렇지 않을 수도 있다. 그러나 사람들이 없는 공간이라면 재난이 발생하더라고 인명 피해와 경제적 손실도 거의 없기 때문에 중요성이 떨어진다. 그러나 사람들이 많이 모이고 집중된 도시의 경우는 대부분의 사람들이 휴대폰이나 모바일 기기를 가지고 움직이기 때문에 모바일 기기는 재난 정보를 실시간 및 정확한 정보를 제공할 수 있는 장점이 있다. 그러나 이러한 정보들이 사용자의 오류나 적극적인 침입으로 위치 및 영상정보를 변경될 경우 잘못된 위치와 영상정보를 전송할 경우 재난을 관리하는 정보시스템의 자동 탐지 서버는 정확한 의사 결정을 내리지 못하는 문제점이 발생한다. 이러한 문

제점은 관리자의 경험으로 어느 정도 수정이 가능하지만 매우 많은 정보들을 통합하여 의사결정을 내릴 때는 취약하고 혼란스러운 정보가 될 수 있다.

이러한 관점에서 본 절에는 스마트폰에서 위치정보의 취약성에 대해 알아본다. 스마트폰의 영상정보는 기본적으로 이미지(비정형) 데이터를 생성하고, GPSInfo의 속성파일에 첨부시켜서 데이터를 전송한다. 최근 대부분의 스마트폰이 사용하는 데이터 포맷은 JPEG 이미지 기반의 EXIF(EXchangable Image File format)을 사용하고 있다. 이는 이미지 및 위치(GPS)정보, 시간, 환경정보 등을 포함하여 전송할 수 있다. 그런데, 이러한 메타데이터 중 GPS 정보의 속성파일을 변경할 경우 정보를 수신한 서버는 변조된 위치정보를 가지고 재해 위치정보를 제공하거나 통합된 의사결정시스템에 활용될 수 있다.

이러한 문제점을 분석하기 위해서 스마트폰에서 사용하는 EXIF 포맷에서 위치정보를 가지고 있는 GPSInfo 태그에 대해 살펴본다([표 8] 참조). GPSInfo는 실제 30개의 필드를 가지고 있으나, 본 절에서는 본 연구와 관련된 내용만을 추출하여 표시한 것으로, 이 중에서도 ID 02/04가 위도/경도를 나타내는 변수명으로 위치정보를 제공한다. 그러나 이러한 정보는 메터데이터 형태이기 때문에 다양한 방법으로 정보를 수정할 수 있다.

먼저 스마트폰의 경우 카메라 어플레케이션 기능을 통하여 GPS 수신 허용을 설정하면 이미지의 EXIF 포맷에 위치정보를 삽입하여 정보를 전송할 수 있다. [그림 14]는 스마트폰에서 사진의 EXIF 포맷에서 위치정보가 포함되어 수신된 내용을 보여주고 있다.

그리고 EXIF 포맷에서 위치 정보 등은 윈도우즈 환경에서도 확인이 가능하며 다른 방법으로도 확인이 가능하다. 그러나 이러한 이미지 정보는 “Stripper”라는 유틸리티 혹은 “Exif Pilot Pro"등을 사용하면 EXIF에 포

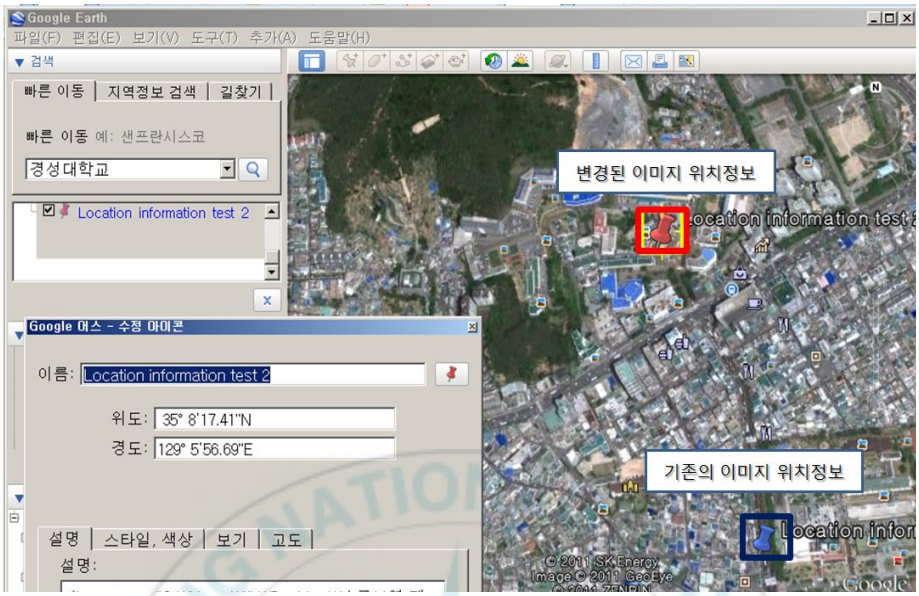
함된 정보를 삭제하거나 수정하는 것이 가능하기 때문에 고의적으로 위치 정보를 변경하여 상대방에게 정보를 전송할 수 있다[13,17].

[표 8] GPSInfo 태그

ID	변수명	변수타입	크기	설명
01	GPSLatitudeRef	ASCII	2	N, S
02	GPSLatitude	RATIONAL	3	위도
03	GPSLongitudeRef	ASCII	2	E, W
04	GPSLongitude	RATIONAL	3	경도
05	GPSAltitudeRef	ASCII	1	고도와 해수면의 관계
06	GPSAltitude	ASCII	1	고도
11	GPSImgDirection	RATIONAL	1	피사체의 방향

[그림 14] EXIF 파일 포맷에서 위치정보 포함된 정보 전송

[그림 15]는 EXIF 태그 내의 정보와 실제 위치정보를 변경한 경우를 나타내고 있다.



[그림 16] 기존위치정보와 변경된 위치정보

이와 같이 재난현장의 위치정보는 매우 중요한 역할을 하지만, 때로는 고의적으로 위치정보를 변경하거나 삭제할 경우 재난대응시스템의 정보를 구축하는데 문제점이 될 수 있다. 따라서 정확하고 신속한 의사결정이 필요한 대응시스템에서는 이러한 문제점의 개선 방안에 대한 연구가 필요하다.

3.3.2 재난현장 영상정보 수집의 취약성 분석

재난현장의 영상정보는 재난 의사결정시스템을 구성하는데 매우 중요한 역할을 한다. 그 중에서 CCTV는 다양한 재난안전 관제시스템에 있어 중요한 요소를 차지하고 있다. 국가 및 지자체는 경제성이나 관리측면에서 매우 편리하기 때문에 CCTV를 이용한 관제의 적용 범위는 확대되고 있으며, 설치 규모가 커지면서 CCTV에 대한 보안성도 설치자 및 관리자의

소홀로 취약성을 가지고 있다. 취약성이 커지고 있는 원인 중에는 현재의 CCTV는 IP기반으로 관제 및 방범 등의 목적으로 사용되기 때문에 인터넷에 연결되어 있을 경우 취약성은 높을 수밖에 없다.

본 절에서는 재난관련 관제 시스템에 있어 CCTV가 매우 중요한 역할을 하지만, 보안기능의 부족과 사용자의 부주의에 의해 종종 해킹 대상이 될 수 있음을 언론이나 연구 발표에서 문제점으로 지적되고 있다. 이러한 취약점을 알아보기 위해 CCTV에서 발생 가능한 시나리오를 고려할 경우 크게 다음 3가지로 구분할 수 있다[7.20].

① 아날로그 CCTV에서 동축케이블 접근에 의한 해킹 위협

② 네트워크 기반의 CCTV에서 발생하는 해킹 위협

③ ARP Spoofing 공격에 의한 해킹 위협

위의 방법 중에서 본 연구와 관련 있는 IP기반의 CCTV 시스템에서 발생 가능한 보안 위협에 대해서 살펴본다.

1) IP 기반의 CCTV 취약점을 이용한 보안 위협

IP 기반 CCTV는 인터넷 혹은 전용선 등을 이용하여 영상정보를 관제서버로 전송할 경우 공인 IP나 유동 IP를 이용한다. 공인 IP를 사용하는 경우 CCTV 시스템 설치 시, 오랜 기간 동안 사용하게 되어 IP주소의 노출에 대한 우려가 있다. 취약성이 있는 CCTV의 영상정보는 다양한 해킹 소프트웨어를 통해 사용자 ID와 패스워드를 검색하여 영상 정보를 보거나 탈취할 수 있다. 그리고 공인 IP의 경우 비용 부담 등이 있기 때문에 유동 IP 회선을 많이 이용한다. 이러한 경우 IP 주소가 자주 변경되기 때문에 지정된 호스트 도메인에 자동 매핑 되는 DDNS(Dynamic Domain Name Service) 기술을 이용하여, 예측 가능한 명칭입력으로 CCTV의 접

근이 가능한 기술들이 개발되고 있다. 따라서 오랫동안 사용하게 되면 다양한 경로와 관리 부실로 노출이 가능할 수 있으며, 한번 노출되면 CCTV 시스템 관리자의 ID와 패스워드는 바로 탐지되어 접근이 가능하게 된다.

2) 검색엔진을 이용한 CCTV 및 IoT 장치의 접근

구글 검색 엔진은 매우 강력한 기능을 가지고 있어. 어떤 주기로 전세계 10억여 개의 웹 사이트 및 서버를 검색하여 갱신된 정보를 구글 서버에 저장하고 검색 엔진으로 제공하고 있다. 이는 인터넷에 한번 올린 정보는 실제로 삭제하더라도 복사된 정보가 구글 서버에 남아 있어 악용될 소지가 가능하다. [표 9]는 구글 검색 엔진을 이용한 CCTV 종류에 따른 해킹에 사용되는 검색어의 예를 나타낸 것으로, 일부만 제시한 것이다. 표에서 제시한 검색어로 구글 검색을 통해 검색할 경우, CCTV의 IP 주소를 포함한 URL이 검색되는데 이것을 이용하면 CCTV에서 사용자 웹 뷰어로 전송되는 영상을 획득 및 컨트롤할 수 있다[11,12].

이 외에도 쇼단(Shodan) 검색엔진은 CCTV를 포함한 IoT장치들의 검색 엔진으로 방대한 양의 검색결과를 제공하고 있다. 이는 키워드를 입력하면 웹 기반 사용자 인터페이스 전용 HTTP 헤더를 검색하여 해당 키워드를 포함하고 있는 장치의 IP주소, 접속가능한 포트, 장치의 국적과 도시, 위도와 경도 등의 많은 정보를 취득할 수 있다. 쇼단 검색엔진에서 제공가능한 장치들은 CCTV, 웹캠을 비롯하여 공유기, 라우터, 와이파이 인덱스, 가정용 홈 디바이스까지 다양한 종류의 IP기반 장치들에 접근할 수 있다.

[표 9] 구글 검색엔진에 의한 CCTV 접근 및 취약성

CCTV 종류	검색어	컨트롤범위
Axxx Camera	/view/view.shtml	좌/우/확대
	"Live view - / - Axxx"	
Cxxx Camera	sample/LvAppl/	
FxWx Camera	/app/idxas.html "Saving & Retrieving Mode"	좌/우 /확대/축소
Pxxx camera	/ViewerFrame?Mode=Motion	
Sxxx camera	/home/homeJ.html	좌/우 /확대/축소
Webcam XX	inurl: /view.shtml intitle: liveapplet	상/하/좌/우
Exx WebCam	intitle: liveapplet inurl: LvAppl	좌/우/확대·축소

이 외에도 악의적인 용도보다는 사용이 허락된 공공기관의 IoT장치들에 대해 정보수집이 가능한 씽풀(Thingful.net) 등의 검색엔진이 제공되고 있다. 이는 악의적인 용도로 사용되지 않기 때문에 취약성이라기보다는 긍정적인 IoT 장치들의 접근 방법을 제공하지만, 이도 수집된 정보를 다른 검색엔진과 연계하여 사용할 수 있기 때문에 악의적인 사용으로 가능하다.

4. 재난안전 정보시스템 개선 방안

4.1 재난안전 정보시스템 구축 방안

본 연구의 기본 방향은 3장에서 설명한 재난안전 정보시스템의 취약성에 대한 개선 방안을 제시한다. 3장에서는 도시지역의 재해정보 수집의 취약성에 대한 내용을 기술하고 있는데, 이는 도시지역이 많은 사람들이 거주하고 건물이나 복잡한 도로 그리고 하천을 기반으로 대부분의 도시들이 구성되어 있기 때문에 풍수해나 화재 등에 취약한 구조를 가지고 있다. 또 다른 관점은 u-IT기반의 재해정보 수집에 대한 취약성을 기술하고 있는데, 이는 최근의 IT기술들이 발달되었기는 하지만, 아직도 임베디드 시스템 혹은 IoT 디바이스들에 대한 현장 설치 및 운영에 있어서는 많은 문제점을 가지고 있다.

본 절에서는 도시지역을 대상으로 최신의 IT기술을 접목한 사람중심의 재난안전 정보시스템 구축에 대한 개선 방안을 제시한다. 개선 방안의 접근 방법은 각 도시의 특성과 현재의 IoT 디바이스들의 특성을 분석하여 개선방향을 찾아가는 미세적인 부분의 접근이 가능할 수 있는데, 본 연구에서는 거시적인 관점에서 재난안전 정보시스템의 구축방향을 제시하고, 이러한 목표에 기반한 정보수집의 방향을 제시할 수 있다고 판단하여 다음과 같은 개선안을 제시한다.

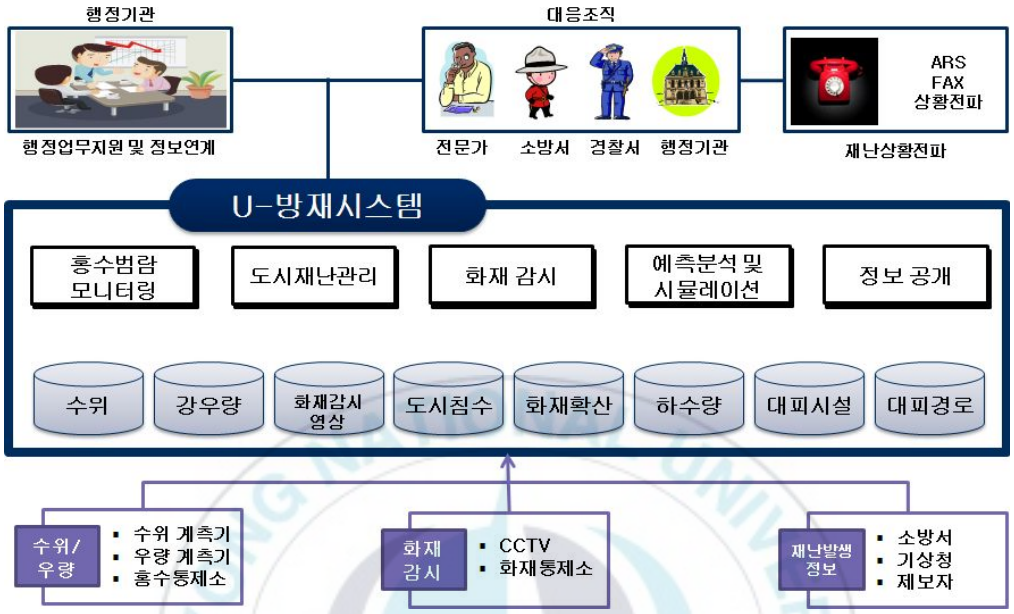
방재시스템의 기본 목적은 사람들에게 필요한 정보를 빠르고 편리하게 제공하는데 목적이 있다. 이를 위해서는 어떤 서비스를 제공해야할지 목표가 필요하며, 서비스 유형에 따라 필요한 데이터가 요구된다. 그리고 필요한 데이터는 현장에서 올라오는 다양한 정보들이 포함되는데, 기본적으로 CCTV 정보를 포함하여 IoT 디바이스, 모바일 장치 등의 현장 및 실시간 정보가 수집되어야 한다.

본 절에서는 재난안전 정보시스템이 제공해야하는 서비스에 따른 어떤 데이터들이 필요한지 살펴보고, 이러한 데이터들의 연계 및 검색에 대한 기능들이 포함되어야 한다. [그림 16]은 재난안전 정보시스템의 서비스 내용을 기술하고, 그에 따른 필요한 데이터의 구성이 어떤 것인지를 나타내고 있다. 본 연구가 모든 재난관련 서비스를 나타낼 수 없고, 또한 그 서비스에 따른 필요한 데이터를 모두 나타낼 수 없기 때문에 그림과 같이 필요한 서비스에 따른 데이터의 구성 요소를 제시하여 재난안전 방재시스템 구축의 개선방안을 제시한다[14,18].

[그림 16] 통합 DB와 서비스가 연계된 정보시스템 구축 방안

[그림 16]에서 제시된 사람중심의 방재서비스가 구축될 경우 이를 어떤 방법으로 전달하고 대응할 것인지에 대한 연구가 필요하다. [그림 17]은 통합방재시스템이 구축될 경우 대응조직과 서비스에 따른 대응절차를 나타낸 것이다. 대응절차 방안에 대한 연구는 다시 세부적으로 기술되어야

하나, 본 연구의 목적은 취약성에 대한 개선 방안만을 고려하기 때문에 재난에 따른 세부적인 대응 절차에 대해서는 기술하지 않는다.



[그림 17] 통합 방재시스템의 대응 절차 방안

4.2 재난정보 수집의 취약성 개선 방안

본 절에서는 3장의 재난현장 위치정보 수집과 영상정보 수집의 취약성에 대한 개선 방안을 제시한다. 앞에서도 기술하였듯이 재난은 현장의 영상정보와 위치정보는 매우 중요하기 때문에 이들의 보안 혹은 물리적인 취약성에 대한 연구는 지속되어야 한다. 본 연구에서는 기술적인 취약성 개선방안 보다는 실제 현장에서 적용될 경우 취약성에 대해 고려해야할 기능들에 대해 설명한다.

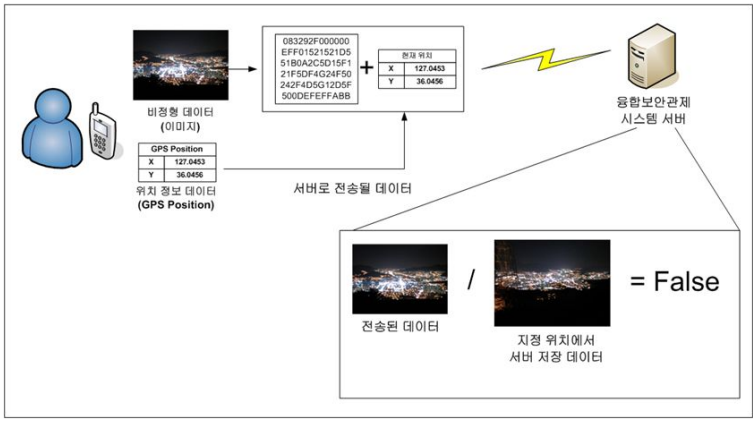
1) 재난현장의 위치정보 취약성 개선 방안

재난현장의 영상정보를 빠르게 수신하기 위해서는 최근 재난현장 주

변에 있는 사람들의 스마트폰으로부터 정보를 수신하는 방법을 많이 고려하고 있다. 본 연구에서도 재난현장의 정보를 수신하는 방법에서 가장 많이 사용하는 스마트폰의 경우 위치정보를 변경하거나 삭제하는 취약성에 대한 개선 방안을 제시한다. 앞에서도 설명하였듯이 스마트폰은 기본적으로 비정형 데이터(이미지)를 생성할 때 GPS 정보 속성파일에 첨부시켜서 파일을 만드는데, 속성파일을 훼손할 경우 변조된 데이터를 받은 서버 또는 사용자는 왜곡된 정보를 가지고 사용하게 된다.

이러한 문제점을 개선하기 위해 기본적인 인증, 무결성, 기밀성, 부인방지 등의 정보보호 서비스 기능을 사용하거나, 이미지 워터마킹 기법 등을 사용하여 위치정보의 변조를 보호하는 기법들이 적용될 수 있다. 본 연구에서는 기본적으로 스마트폰을 이용한 EXIF 태그 내 변조된 위치정보를 확인할 수 있는 방법을 제시한다.

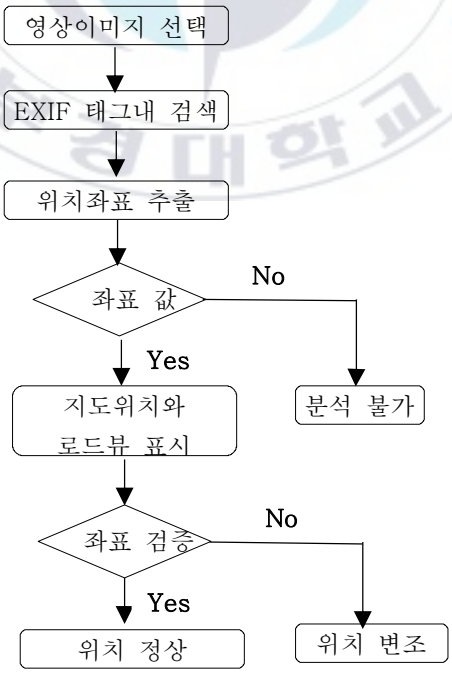
[그림 18]은 스마트 폰에서 전송하는 위치정보에 대해 변조가 가능한 취약성을 나타낸 그림이며, 스마트폰 내의 EXIF 포맷에서 가지고 있는 위치정보를 변조하여 서버로 보낼 경우 잘못된 위치정보의 판정을 위한 과정이 필요하다[5].



[그림 18] 스마트폰 위치정보 변조 및 오류생성

본 연구에서는 변조된 전송 데이터의 경우 서버 시스템에서 이상 정보를 찾아내는 방법을 제안한다. 스마트폰에서 전송하는 위치정보의 검증 문제를 개선하기 위해 EXIF 태그 내 좌표위치 확인 소프트웨어를 활용하여 검증하는 것이다. 예를 들면 CVS(Coordinate in the image file Verification Software) 기능을 가지는 소프트웨어를 작성하여 GPS 좌표가 포함된 이미지 파일을 불러들이고, 이미지 내의 EXIF태그를 읽어 좌표를 추출하게 하고, 기존의 영상과 전송된 영상이 위치를 비교하는 기능을 가지는 방법을 적용할 수 있다.

[그림 19]는 스마트폰의 이미지 파일의 위치정보를 비교할 수 있는 알고리즘을 제시한 것이다. 제시된 알고리즘에 의해 전송된 이미지를 선택하고, EXIF 태그 내에 있는 좌표를 추출하여 구글의 로드뷰 기능을 연계하여 위치정보를 검증할 수 있다.



[그림 19] 스마트폰 위치확인 검정 알고리즘

2) 재난현장의 영상정보 취약성 개선 방안

3장에서 재난현장의 영상정보, 특히 CCTV 보안장비의 취약성에 대해서 여러 가지가 있지만, IP기반의 CCTV 취약점과 검색엔진을 이용한 보안 취약점에 대해 기술하였다. 본 절에서는 앞의 취약점에 대해 개선 방안을 설명한다.

CCTV 영상정보의 보안위협 요소들을 제거하기 위해서는 다음과 같은 방법을 제시할 수 있다. 첫째는 공격자가 추측하기 어려운 ID와 패스워드를 사용하는 것이고, 둘째는 관리 서버에 대한 접근제어(access control) 기법을 적용하는 것이다. 그리고 IP 주소 필터링 기법을 사용하거나, IEEE 802.1x의 인증 기법 사용과 Secure HTTP 보안 기법들을 적용하거나 VPN 기법을 적용하여 정보를 전송하는 것이다.

CCTV 등 영상정보를 악의적인 목적에 이용되지 않도록 하기 위해서는 보안 취약성 요소들을 찾아내어, 각 요소별 취약성 개선 방안을 가지는 것이다. 기본적으로 CCTV나 IoT 장치들은 IP기반의 운영 장치들로서 IP와 관련된 정보를 노출하지 않고 잘 관리하는 것이 매우 중요하다. IP기반의 장치들에 대해 보안 취약성 레벨의 요소는 다음과 같이 고려할 수 있다.

첫째는 IP 노출에 대한 것으로 구글 검색엔진이나 쇼단 등에 의해 대부분의 IP기반 장치들은 노출되지 않아야 할 정보들이 오픈되고 있다. 이를 위해서는 프록시 서버나 VPN 기법을 적용하여 IP 노출에 대비하는 것이 필요하다.

둘째는 장치 정보의 노출로 각 장치들의 ID와 패스워드 그리고 장치들이 가지고 있는 다양한 정보들 특히 포트에 대한 정보가 노출되어 있는데, 이러한 정보들에 대해서도 앞에서 설명한 것과 보안 취약성을 강화하는 것이 필요하다.

셋째는 위의 이러한 보안 취약성 요소들에 대해 각 설치되어 있는 장치들이 보안 취약성 등급을 설정하여 등급에 따른 관리 방안을 가지고 대응하는 과정이 필요하다.

4.3 재난안전 정보시스템의 통합 개선방안

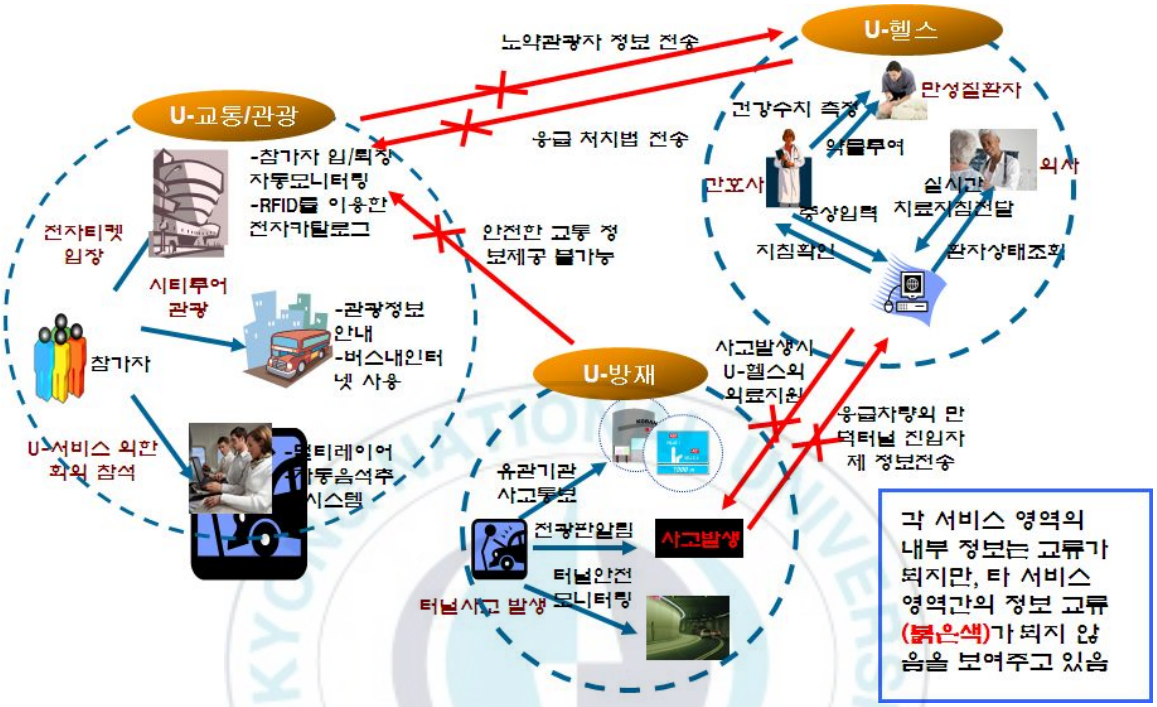
재해·재난의 발생은 다양한 환경 및 복합적으로 발생되는 경우가 많다. 일반적으로 대형 자연재해와 인적재난은 하나의 원인으로 발생하는 것이 아니라 여러 가지 원인에 의해 발생되곤 한다.

본 절에서는 도시에서 대형 재난이 발생할 경우 지자체 혹은 구/군에서 자체적으로 구축된 재난안전시스템이 상호 연계되지 않고 독립적으로 운영되는 문제점을 살펴본다. [그림 20]은 크게 3가지 영역으로 관제 서비스를 제공하는 시스템이 있을 경우 내부적으로는 정보 공유가 일반적으로 원활하게 서비스가 되고 있지만, 외부적으로는 각 시스템이 독립적으로 운영되기 때문에 정보 공유가 되지 않고 있음을 보여주고 있다. 이를테면 어떤 재해가 발생할 경우 방재시스템과 의료관제 서비스가 연계되지 않으면 환자 관리에 문제가 발생할 수 있으며, 그리고 방재와 교통관제 시스템이 연계되지 않을 경우 환자 수송의 문제점이 발생할 수 있다. 이러한 문제점을 사전 혹은 어느 정도 예방하기 위해서는 각 기관이나 서비스 영역별로 관제시스템을 구축할 경우 다른 관제시스템과 연계를 위한 데이터 공유, 서비스 공유, 확장성 공유 등을 고려하여 구축되어야 한다[12,19].

이를 위해 본 연구에서는 [그림 20]과 같이 도시안전을 위한 방재서비스의 정보 흐름을 분석하여 필요한 정보가 공유되지 않을 경우 해당 서비스가 가능하도록 다음과 같은 기능이 포함되도록 제안한다.

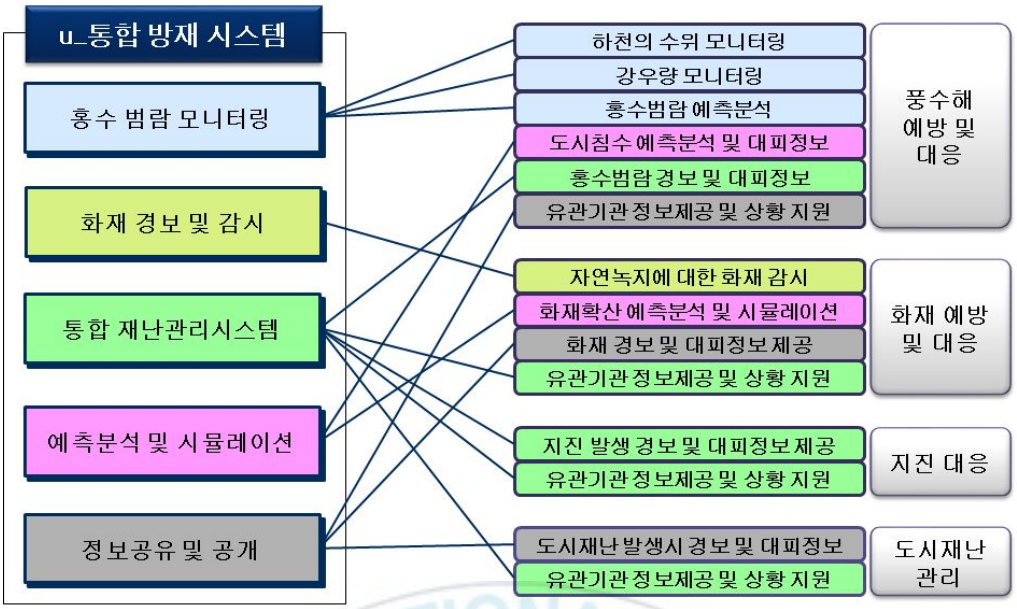
- 기존 방재시스템에 활용할 수 있는 IT융합 부품기술 연계
- 도시안전과 관련된 안전 교육 시스템 연계

- 통합방재센터 구축을 위한 정부/지자체 간의 서비스 연계
- 표준화를 위한 도시안전 통합시스템 구축



[그림 20] 도시안전 정보교환의 방재서비스 문제점

[그림 21]은 위의 여러 가지 관제시스템 간의 정보교환의 문제점을 극복하기 위해 각 방재시스템 서비스가 가지는 세부적인 내용을 제시하고, 이와 연관성이 있는 기능들은 향후 시스템을 구축할 때 데이터 유형, 정보 공유 방법, 서비스 공유 등의 상세한 연계 내용을 공유하기 위한 방안을 제시하고 있다. 본 절에서 제시한 내용은 도시 통합 방재시스템이 가지고 있는 여러 가지 기능들 중에서 자연재해와 인적재난의 일부 내용을 연계시키기 위한 과정과 일부 기능들 중에는 방제 예측을 위한 분석 및 모델링 기능을 연계한 내용을 나타내고 있다.



[그림 21] 도시 통합방재 서비스를 위한 정보 공유 방안

PUKYONG NATIONAL UNIVERSITY 부경대학교

5. 결론

최근 인적재난에 해당하는 세월호 사고는 물론 집중호우에 따른 인명 및 경제적 손실은 매년 증가하고 있다. 자연재해나 인적재난은 완전히 방지할 수는 없지만, 기존에 구축된 재난관련 정보시스템을 최대한 연계하고 통합하는 과정에서 발생할 수 있는 재난을 예방하거나 경감할 수 있다.

본 연구에서는 최근의 IT기술을 기반으로 구축된 재난안전 정보시스템의 주요 내용을 살펴보고, 이들에 대한 취약성 분석을 통해서 개선내용을 제시하고 있다. 재난안전 정보시스템 통합을 위해 자연재해 및 인적재난에 대한 기존의 대응시스템을 분석하였으며, 특히 대응시스템 분석에 따른 연계성 분석 내용을 제시하였다. 그리고 재난안전 정보시스템을 구축할 경우 재해정보데이터 수집의 취약성과 u-IT기반 재해 정보시스템 구축의 취약성에 대해 알아보았다. 마지막으로 재난은 대부분 빠른 대응 능력을 가질 수 있도록 시스템이 구성되어야 하기 때문에 현장성과 실시간성은 매우 중요한 요소이다. 이를 위해 재난현장 위치정보 수집의 취약성 분석과 재난현장 영상정보 수집의 취약성 분석을 살펴보았다.

위의 이러한 취약성 분석에 대해 본 연구에서는 재난안전 정보시스템의 개선 방안을 제시하였다. 첫째는 재난안전 정보시스템 구축에 대한 개선 방안을 제시하였으며, 둘째는 재난 정보 수집의 취약성에 대한 개선 방안을 기술하였다. 마지막으로 앞의 여러 가지 취약성에 대해 종합적인 재난안전 통합시스템의 개선 방안을 제시하였다.

본 연구는 전체적으로 재난안전 정보시스템에 대해 최근 대부분의 연구들이 기존의 재해·재난 예방 기법에서 최신 IT기술을 접목한 현장 중심과 실시간성을 고려한 방재시스템을 구축할 경우 기술적인 문제와 사람 중심의 서비스에서 시스템이 가질 수 있는 취약성과 연계성의 개선 방안에 대

해 연구하였다. 본 연구의 내용은 재난안전 정보시스템의 완전성을 목표로 하는 것이 아니라 다양한 재난에 대비한 서비스 시스템이 구축될 경우 데이터 수집의 취약성과 연계 및 통합성을 고려한 개발이 진행되어야 함을 기술하고 있다.

PUKYONG NATIONAL UNIVERSITY
부경대학교

< 참 고 문 헌 >

[1] 재난 및 안전관리 기본법(법률 제12934호)), 재난 및 안전관리 기본법 시행령(대통령령 제26373호), 재난 및 안전관리 기본법 시행규칙(총리령 제1188호), 법제처 국가법령정보센터

[2] 김창수, “u-City와 도시정보”, 한국지리정보학회지, 2009. 1.

[3] 부경대학교 산학협력단 보고서, “보안관제 융합에 관한 연구”, 2010. 10.

[4] 행정안전부, CCTV 종합대책 발표, 2011. 05.

[5] 부경대학교 산학협력단 보고서, “공간정보기반 융합보안관제”, 2011, 10.

[6] LG CNS와 함께하는 보안 컨설팅 A to Z, "물리보안과 정보보안이 만나 융합보안으로 진화하다(http://blog.lgcns.com/856)“, 2015. 07.

[7] 주용완, 이승재, “지능형 CCTV 동향 및 성능 향상 방안”, 정보통신산업진흥원, 2013.

[8] 강희조, “재난안전통신망에 관한 연구”, 한국항행학회논문지, 18권 1호, pp. 95~100, 2014. 02.

[9] 장명, “IoT 기반의 재난 안전 도시 모델 설계에 관한 연구”, 부경대학교 박사학위논문, 2015. 2.

[10] 유병태, 고재욱, “대규모 인명피해 발생에 따른 재난관리체계 개선방안,” J. of the KOSOS, Vol. 30, No. 2, 2015. 4.

[11] 박광혁, 김국보, 김창수, “글로벌 IoT 장비의 취약성 분석에 관한 연구” 2015년 한국멀티미디어학회 춘계학술발표대회, 18권 1호, pp.260~261, 2015. 05.

[12] 부경대학교 산학협력단 보고서, “물리보안관제의 사이버보안 취약성에 관한연구, 2015. 11.

[13] T. W. Seo, S. R. Lee. B. C. Bae, E. J. Yoon, C. S. Kim, "An Analysis of Vulnerabilities and Performance on the CCTV Security Monitoring and Control", *Journal of Korea Multimedia Society,* Vol. 15, No. 1, pp. 93-100, 2012.

[14]D. H. Kim, S. W. Yoon, Y. P. Lee, "Security for IoT Services", *Korea Communications Society(Information and Communication)*, Vol. 30, No. 8, pp. 53-59, 2013.

[15] KISA, "Survey for Information Security Industry in Korea : Year 2013", KISIA & KDCA, 2013.

[16] Y. W. Joo, S. J. Lee, "Intelligent CCTV Trends and Performance Improvement", *National IT Industry Promotion Agency,* 2013.

[17] KAIST, "Security threat report of Foreign-made CCTV, IP-Camera", SysSec lab, 2015.

[18] S. H. Park, "Intelligent CCTV System technology issues and industry trends", *Korea Electronics Technology Institute,* 2013

[19] R. Bodenheim, J. Butts, S. Dunlap, B. Mullins, "Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices", *International Journal of Critical Infrastructure Protection*, Vol. 7, No. 2, pp. 114-123, 2014

[20] H. J. Shin, Y. K. Jeong, "Device Alive Check Algorithm using TCP Session under CCTV Network based on NAT", *Journal of Korea Multimedia Society,* Vol. 18, No. 5, pp. 631-640, 2015.

[21] Physical Security in Wikipedia(2015), https://ko.wikipedia.org/wiki/%EB%AC%BC%EB%A6%AC%EB%B3%B4%EC%95%88(accessed Aug. 25. 2015).