情報保護學會論文誌
第 21 卷 第 5 號, 2011. 10

# 스마트 모바일 오피스 보안을 위한 CERT와 ISAC의 역할*

이 근 영,† 박 태 형, 임 종 인‡
고려대학교 정보보호대학원

# A Study on Roles of CERT and ISAC for enhancing the Security of Smart Mobile Office*

Keun-Young Lee,† Tae-Hyoung Park, Jong-In Lim‡
Graduate School of Information Security, Korea University

요 약

모바일 오피스란 PC위주의 사무범위를 벗어나 장소와 단말에 구애를 받지 않고 휴대용 단말을 이용하여 언제 어디서나 네트워크에 접속하여 업무를 수행하게 하는 새로운 근무형태이다. 스마트폰의 보급과 확산, 유비쿼터스시대의 망고도화, 무선인터넷 확대 등 모바일 오피스의 환경을 이루는 요소들의 발달과 국가의 스마트워크 활성화 정책에 반해, 모바일 오피스라는 새로운 환경에서의 보안위협들에 대한 보안 가이드라인과 정책 등이 미흡한 상황이다. 본 논문에서는 안전한 모바일 오피스 구축을 위해 요구되는 보안 대응으로써, 이미 구축된 보안대응시스템인 CERT와 ISAC의 기능을 분석, 활용하여 스마트 모바일 오피스 보안 강화를 위한 CERT와 ISAC의 역할을 제시하고자 한다.

ABSTRACT

Mobile Office is a new type of working method in the workplace that can be used at any time or anywhere by connecting to the network with mobile devices. This allows people to do their jobs without their physical presence in their offices to use computers. The elements in mobile office environment are advancing. They include the widespread distribution of the smart phones, the network enhancing strategy in a ubiquitous environment and expansion of the wireless internet; however, there are not enough security guidelines or policies against these threats on the new environment, the mobile office, although there is the revitalization policy of smart work supported by the government. CERT and ISAC, the known security system as of now, could be used for the secure mobile office. In this paper, suggestions are to be provided for strengthening the security of smart mobile office by analysing the functions of CERT and ISAC.

**Keywords**: Smart Phone, Mobile Office, Mobile Security Threats, CERT, ISAC, Security Policy

## 1. 서 론

스마트폰의 보급과 확산, 스마트폰 금융서비스의 등장, 유비쿼터스시대의 망고도화, 모바일 에코시스템 등 모바일 환경의 변화 등을 배경으로 모바일 오피스가 가능하고 발전할 수 있는 기반이 마련되고 있다. 모바일 환경의 발전은 모바일 오피스의 이동성, 편리

접수일(2011년 3월 23일), 수정일(2011년 5월 16일), 게재확정일(2011년 6월 27일)
* 본 연구는 지식경제부 및 정보통신산업진흥원의 "대학 IT연구센터 육성 · 지원사업(NIPA-2011-C1090-1001-0004)"의 연구결과로 수행되었음.
† 주저자, starnyou@korea.ac.kr
‡ 교신저자, jilim@korea.ac.kr

성 등과 함께 스마트워크 인프라 고도화 및 민간 활성화 기반 조성(안)과 같은 국가의 스마트워크 정책으로 더욱 지원을 받고 있다. 도시철도공사의 현장 실시간 업무지원시스템, 기상청의 FMC/UC/그룹웨어 기반의 모바일 오피스, 삼성SDS의 모바일 데스크, 삼성증권 모토로라 FMC(유무선 통합) 솔루션을 도입, 포스코 그룹의 모바일 오피스 구축 등 기업들이 속속 모바일 오피스를 도입하면서 관련 시장도 급속도로 성장할 전망이다. 하지만 모바일 오피스라는 새로운 환경의 위협들에 대한 보안 대응으로써의 보안 정책이나 가이드라인 등을 제시하지 못하고 있는 국내 상황에서 모바일 오피스를 도입했거나 도입하고자하는 기관 및 기업들은 편리성과 더불어 보안의 문제에도 관심을 가져야 한다. 실제 모바일 오피스에서의 보안 이슈들로는 기존의 RIM 社의 블랙베리 폰을 이용한 모바일 오피스에서 통신 양방의 동의 없이 통신 기록을 수집함에 따라 모바일 오피스 서비스 제공회사인 RIM 社가 빅브라더화 되는 문제와 블랙베리 시스템에서 PIN 메시지가 서버에 축적됨에 따라 개인정보가 침해되는 문제 등을 들 수 있다. 또한 국정원의 스마트폰 보안취약성으로 전자결제 제한, 오바마 대통령의 행정용 스마트폰에 대해 대통령 기록법에 의한 이메일 등 개인적 의사소통 수단 해지의 이슈가 존재한다. 모바일 환경에서의 보안과 관련된 선행연구들은 주로 모바일 오피스를 구성하고 있는 요소들에 대해서 기술적인 측면에서 보안시스템, 보안기술에 대해서 이루어져 왔다. 모바일 오피스의 보안이라는 주제로 관리·통합적 측면이나 정보보안 정책적인 측면으로 접근한 연구는 찾아보기 힘들다. 모바일 오피스에 대한 도입과 활성화를 위해서는 모바일 오피스 보안에 대한 정책적 연구는 필수적으로 요구되며, 본 논문에서는 모바일 오피스 보안 현황을 분석하고 이를 바탕으로 정보보호 정책 관점에서 요구되는 사항을 도출함으로써, 모바일 오피스 보안 강화를 위한 정책 제안을 하도록 한다. 모바일 오피스 보안 문제들을 포함하여 모바일 오피스를 구성하고 있는 요소들을 기술적, 법적, 관리적 측면으로 구분하여 발생 혹은 발생할 수 있는 보안 위협들에 대해 분석하고, 이들 각각에 대한 보안 현황에 대해 검토한 결과 모바일 오피스 보안을 위한 하나의 대응방안으로써 국내 CERT와 ISAC의 역할들을 도출할 수 있었다.

본 논문에서는 스마트폰의 확산 등 새로운 정보통신 환경의 변화와 모바일 오피스의 발달 및 확대에 따라 결부되어 일어나는 모바일 오피스 환경의 보안위협과 대응현황에 대해 살펴보고, 기업의 안전한 모바일 오피스 구축을 위해 요구되는 보안 대응방안으로 이미 구축된 시스템인 CERT와 ISAC을 활용하여 모바일 오피스의 보안대응방법의 하나로써 제안한다.

## II. 이론적 배경

### 2.1 모바일 오피스

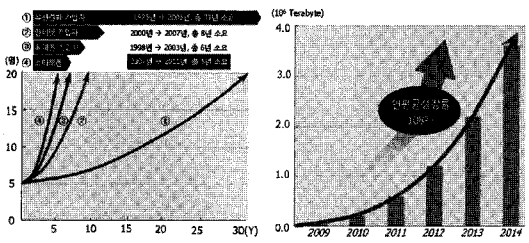
#### 2.1.1 모바일 오피스 개념

모바일 오피스(Mobile Office)란 과거 사내 무선 네트워크와 노트북을 이용하는 수준에서 벗어나 이동통신망과 휴대단말기를 이용한 서비스 환경을 제공하는 B2B 서비스로써, 휴대용 단말기 등 IT기기를 활용해 언제 어디서나 네트워크에 접속할 수 있는 시스템을 의미한다[1]. 새로운 근무형태로 휴대용 컴퓨터 및 휴대폰, PDA 등과 같은 첨단정보통신기술을 이용하여 시간과 장소에 구애 없이 정보를 이용하여 업무를 수행하게 하는 근무환경이라고 정의할 수 있을 것이다.

#### 2.1.2 모바일 오피스 시대의 도래

애플의 아이폰이 폭발적인 반응을 얻는 등 세계적인 스마트폰 열풍으로 휴대폰 제조사들은 고성능 스마트폰을 경쟁적으로 출시하면서 2011년에는 5명 중 1명이 스마트폰을 보유할 것으로 예상되며, 사용자 수 증가속도(100명당 사용자 : 5명 → 20명)에서 스마트폰(5년)이 유선전화(31년), 인터넷(8년), 휴대폰(6년)을 압도하고 있다. [그림 1]과 같이 모바일 트래픽은 연평균 108% 이상 성장해 2014년에는 2009년 수준의 39배인 360만TB(테라바이트)에 이를 전망이다[2].

스마트폰 사용자가 2010년 700만 명을 넘은데 이




[그림 1] 세계 스마트폰 사용과 모바일 트래픽 증가 추이

어 올해는 전체 가입자의 40% 수준인 2,000만 명에 이를 것으로 전망하고 있고[3], 스마트폰의 빠른 보급은 어디서나 온라인 접속의 가능, 트위터 등 소셜네트워크 서비스(SNS, Social Network Service)의 활성화, 사용자 위치기반 서비스(LBS, Location-Based Service)와 모바일에 특화된 서비스 등 사용자의 라이프스타일과 기업의 비즈니스 모델 및 기업환경의 변화를 가져오고 있다. 매일경제신문이 57개 국내 대기업 최고경영자(CEO)를 대상으로 '모바일 오피스 도입 현황' 설문조사를 한 결과 모바일 오피스 도입 기업이 1년 만에 15.8%에서 56.1%로 크게 증가 했으며, 2011년 중 도입할 예정인 기업이 전체 설문 대상 업체 중 87.7%를 차지하여[4], 모바일 오피스에 대한 국내기업의 인식변화를 보여주고 있다. KT경제경영연구소에 의하면 2009년 2조 9000억원 규모였던 국내모바일 오피스 시장이 2014년 5조 9000억원 규모로 확대될 것으로 전망하고 있고[4], 국가정보화전략위원회 주관, 방통위, 행안부 공동의 "스마트워크 인프라 고도화 및 민간 활성화 기반 조성(안)" 또한 국내 모바일 오피스 시장의 확대에 기여할 것으로 예상된다.

### 2.2 침해사고대응시스템(CERT)

"침해사고"란 해킹, 컴퓨터 바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생하는 사태를 말한다(정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조 7항). 사이버 침해란 정보시스템의 취약한 부분을 공격하여 시스템 내부에 침입하거나 시스템을 마비·파괴하는 등의 사고를 유발하는 모든 행위를 말한다. 사이버 침해사고 발생원인은 해킹수법의 진화, 보안패치 미흡, 홈페이지 보안취약점 방치, 취약한 패스워드 설정 등 기본적인 보안관리 사항의 불이행 등 직접적인 원인과 최신 정보보호 제품(웹방화벽, PMS(Patch Management System), VMS(Virus Management System) 등) 구비 미흡, 전문인력 부재, 정보보호에 대한 전반적인 투자부족 등 간접적인 영향이 있다. 최근의 사이버 침해의 추세는 다양한 유형의 정보 갈취형 해킹사고가 빈발하면서 시스템 마비, 실력 과시 등의 단순 목적이 아닌 금전적 이득을 노리는 범죄 수단으로 악용되고 있는 것으로 나타났다[5][6]. 이러한 사이버 침해에 대해 대응하기 위해서 국내·외적으로 국가, 국방, 민간차원에서 사이버대응시스템으로 CERT나 ISAC 등의 조직을 운영하고 있다.

침해사고대응팀(CERT, Computer Emergency Response Team)은 침해사고대응시스템으로써 정보통신망 등의 침해사고에 대응하기 위해 기업이나 기관의 업무 관할 지역 내에서 침해사고의 접수 및 처리 지원을 비롯해 예방, 피해 복구 등의 임무를 수행하는 조직을 말한다[7]. 기업통합 정보보호 관리시스템(ESM, Enterprise Security Management) 등을 통해서 정보보호 솔루션들을 통합하여 모니터링을 수행하지만, 침해사고대응, 공격평가, 조기 예·경보의 기능 등 사이버상에서 좀 더 효율적인 침해대응이 가능한 종합침해사고대응시스템의 필요성이 제기되고 있다[8]. 또한 기업에서 CERT 조직은 정보보호 관련 정비가 잘된 소수의 조직에서나 볼 수 있는 상황이며, 지난 1·25 인터넷 대란은 몇몇 기업 내의 잘 훈련된 CERT만으로는 문제를 해결할 수 없음을 증명하는 사례였다. 정보화의 진전으로 금융·통신 등 주요 정보통신기반시설의 상호 의존도가 높아지면서 사이버테러로 인한 피해 발생 시 효율적인 대응이 필요하였다. 1·25 인터넷 대란의 경우, 금융권에서는 ISAC을 중심으로 각 은행과 증권업계들은 공동대처를 한 본보기로, 국가정보원 산하 국가사이버안전센터를 중심으로 이미 설립, 운영 중인 ISAC을 연결하여 금융권 보안체계를 구성하였다. ISAC의 기능은 기존 CERT의 포괄적인 침해사고대응 업무를 특화된 영역 내에서 종합적인 예방 및 대응체계를 기반으로 업무를 수행한다. 침해사고대응을 위한 독자적인 대응체계 구축을 위한 비용절감효과와 각 분야의 전문적인 정보분석 능력 및 공유의 효율성을 위해 ISAC의 구축이 필요하다고 할 수 있다.

### 2.3 정보공유분석센터(ISAC)

ISAC은 미국 대통령 지시명령(Presidential Decision Directive, PDD-63, 1998.5.22, Bill Clinton)에서 시작되어 금융을 비롯한 통신·국방·교통 등 8개 분야에 걸쳐 특화된 ISAC이 조직되었으며, 우리나라는 2001년 1월 26일 관련 법률인 『정보통신기반보호법』 제 16조 (정보공유·분석센터, 2001년 7월 1일 시행)에 의거하여 금융ISAC을 시발로 각종 침해사고나 보안정보 공유를 위해 설립되었다. ISAC의 주 업무는 사이버테러 취약점과 요인, 대응방안에 관한 정보를 제공하고 침해사고가

발생하면 실시간 경보와 분석업무를 수행한다. 분야별 여건을 고려하여 침해사고 대응체계 구성 및 운영, 정보통신 기반시설 보호시스템 시험 등 정보보호 관련 교육과 훈련 서비스 등을 제공하여 관련기관이 침해사고 발생의 주요정보사항을 공유, 공동대응하고 있다. ISAC의 역할은 국가의 중요 정보통신기반시설에 대한 보호를 위해 주기적인 취약점 분석, 평가, 보호대책 및 보호계획을 수립함으로써 공동대응체계를 구축하는 것이다. 정보공유 및 분석업무지원, 제공되는 정보들의 신뢰성 보증, 관리주체로서 영역 내의 주요기반 시설에 대한 보안 구조 이해, 대외적인 상호의존적 영역에서도 신뢰성 확보, 해당 영역에서 발생 가능한 영향과 관련성을 분석 및 평가하고 결정, 특화된 영역 내의 모든 위협들에 대한 신속하고 정확하게 위협 분석, 회원사들의 만족도와 신뢰성 최대화하는 것이다[9].

## III. 모바일 오피스 환경에서 CERT 및 ISAC

### 3.1 모바일 오피스의 보안위협과 대응현황

모바일 오피스 시대의 도래라고 불릴 만큼 모바일 오피스를 이루는 환경요소들의 확대 및 빠른 성장과 동시에 반드시 해결해야 할 문제는 바로 모바일 오피스의 보안문제일 것이다. 2010년 5월 방송통신위원회와 한국인터넷진흥원과 공동으로 실시한 '스마트폰 이용 실태조사 자료보고서'에 따르면 스마트폰 이용자의 47.2%가 스마트폰 보안문제(바이러스 및 악성코드 감염, 개인정보 유출 등)에 대해 걱정하고 있는 것으로 나타났으며 주로 '이메일 및 문자메세지 첨부파일 다운로드(67.7%)' 또는 '무선랜(WiFi), 블루투스 등 무선 네트워크 접속(64.8%)'을 통해 보안 문제가 발생할 가능성이 높을 것이라고 인식하고 있었으며, 이외에도 '모바일앱 등 응용프로그램 다운로드(50.3%)', '웹사이트 접속(41.9%)' 등을 걱정하는 것으로 조사되었다. 하지만 스마트폰 이용자의 69.9%가 스마트폰 보안문제에 대응하기 위해 '발신인이 불명확하거나 의심스러운 메시지 및 메일 삭제'하는 방법을 이용하고, '다운로드 파일은 스마트폰에서 바이러스 유무를 검사한 후 사용(51.9%)', '비밀번호 설정 기능 이용 및 정기적 변경(49.1%)'하는 적극적인 대응방안은 낮은 비율을 차지했다. 빠르게 성장하고 있는 모바일 오피스 시장에서 모바일 오피스를 구성하고 있는 여러 환경요소들의 보안 위협들은 산업기밀이나 민감한 개인정보와 결부되어 모바일 오피스 보안의 위협요소로 나타날 수 있으며, 이러한 위협요소들에 대한 보안대응은 중요한 이슈로 대두되고 있다.

#### 3.1.1 모바일 오피스의 기술적 보안위협과 대응현황

모바일 오피스 환경을 이루는 요소는 스마트폰 단말, 애플리케이션 및 플랫폼, 서버 및 네트워크로 구분할 수 있다. 이들 각각의 요소의 보안위협은 곧 모바일 오피스의 보안위협요소이며, 기존의 보안위협과 결부된 위협들, 모바일 오피스를 위한 환경요소들 중 새롭게 나타난 위협들이 존재하며, 보안대응현황 또한 기존의 정보보호관련 시스템으로 대응할 수 있는 형태의 것과 모바일 오피스를 위한 새로운 환경과 관련된 보안대응형태가 존재한다.

##### 3.1.1.1 스마트폰 단말 보안위협과 대응현황

모바일 오피스 시대의 도래라고 불릴 만큼 손안의 PC라 불리우는 모바일 오피스의 단말기(노트북, PDA, 스마폰 등 휴대 단말)는 이동성·휴대성이라는 특성으로 인해, 사용자의 부주의로 인한 분실 혹은 제3자에 의한 도난이라는 위험이 존재한다. 실제 스마트폰의 분실·도난 사고는 월평균 20만대에 이르고 있으며[10], 분실·도난 된 단말기는 도청, 단말복제, 악성코드 삽입 등의 악용과 단말기에 저장된 개인정보 데이터 노출의 위협에 노출되어 있다. 특히, 모바일 오피스에 사용되는 단말기의 경우 산업기밀 및 기업정보 유출이라는 심각한 문제가 될 수 있다. 모바일 오피스에서 스마트폰은 개인의 사용자 비밀번호 설정, 분실 사고 시 고객센터에서 서비스 정지 등의 방법만으로는 단말보안의 문제를 해결하는데 미흡한 실정이다. 분실·도난 된 스마트폰에 대해 MDM(Mobile Device Manager)를 통한 원격 잠금, 원격파일 삭제 기능의 기술이 존재하지만, 개인적 용도로도 사용이 가능한 모바일 오피스용 스마트폰은 위치정보보호법 이슈 등으로 이러한 기술의 도입과 반영에는 어려움이 존재한다. 또한, 스마트폰 단말 보안 관련해서 사용자 10대 안전수칙이 제시된 것에 불가하며, 모바일 오피스에서 기업용 스마트폰 사용의 개인적 사용범위 제한수준은 부재한 상황이다.

##### 3.1.1.2 모바일 악성코드 보안위협과 대응현황

모바일 악성코드 위협은 모바일 오피스의 기술적 보안 위협 중 여러 유형의 위협으로 발전할 수 있는

요소를 지니고 있다. 전 세계적으로 알려진 모바일 악성코드의 수는 2004년 15건, 2005년 131건, 2006년 353건, 2007년 381건, 2008년 429건, 2009년 상반기까지 524건으로 매년 증가하는 추세이다(2009년 6월에는 2006년 기준으로 스마트폰 기반 악성코드가 500% 증가)[11][12]. 모바일 악성코드는 주요 활동별 특성으로 단말장애 유발형, 배터리 소모형, 과금유발형, 정보유출형, 크로스 플랫폼형 악성코드로 구분되며, 초기에 단순히 전파를 목적으로 하거나 단말의 기능적 동작을 마비시키는 형태에서 개인정보의 유출 및 금전적 이득을 목적으로 하는 형태로 변화하고 있다[13]. 모바일 악성코드는 애플리케이션, 네트워크 등 다양한 감염경로를 통해서 피해가 발생할 수 있어 감염경로에 대한 주의가 요구된다. 실제 스마트폰 사용자 20%가 SMS/MMS 및 메일을 통해 피싱 메시지를 수신하였고[14], 모바일 오피스용 스마트폰에서는 SMS/MMS를 통한 악성코드 감염 시, 부정과금 유발, 휴대전화 소액결재, 유료전화서비스 악용 등의 문제로 기업정보보호에 위협을 가할 수 있다. 스마트폰 기반의 악성 프로그램의 전파 방식이 매우 다양하여 악성코드 수집 단계에서부터 문제가 발생하고 있고, 안드로이드나 iOS, 심비안, 블랙베리 등 다양한 종류의 운영체제를 운영함으로써 수집된 악성프로그램의 분석에도 어려움이 있다[11]. 이에 스마트폰 기반의 악성코드를 수집·분석·테스트를 위한 망, 시스템 구축이 요구되고 있다. 백신업체들은 빠르게 증가하는 악성코드에 대해 스마트폰의 여러 OS의 특성에 맞는 보안 솔루션을 강구하고 있다. 하지만 대표적인 안티바이러스 제품들의 경우, 악성코드의 시그니처 수집을 통해 시그니처 값을 비교하여 악성코드를 탐지하는 시그니처 기반의 탐지방법을 사용 중이다. 이러한 시그니처 기반 탐지방법은 알려지지 않은 새로운 악성코드나 기존의 악성코드에 약간의 수정을 가한 변종 악성코드의 경우 탐지가 불가능하다는 문제점이 존재한다. 알려지지 않은 악성코드의 탐지와 이에 대한 백신개발을 위해 외국의 엔진이 아닌 국내의 지속적인 기술 확보 및 관련 연구가 필요하나 이에 대한 어려움이 많다. 국제전화를 거는 과금 유발형 스마트폰 악성코드인 테러리스트 다이얼(진단명:WinCE/TerDial)이 2010년 4월 19일 국내서 첫 발생시, 방송통신위원회가 스마트폰 정보보호 민관합동대응반을 구성하여 조사결과 다행히 직접적인 피해는 발생하지 않았다고 설명했다. 하지만 모바일 오피스 환경에서도 악성코드를 이용하여, 과금 유발뿐만 아니라 대규모 사이버공격상황이 일어날 가능성은 매우 높다. 모바일 악성코드에 대비하여 선언적 의미가 아니라 원활한 정보공유를 위한 지속적인 선 대응체제가 이루어지지 않는다면, 7·7 DDoS사건의 문제점으로 지적되었던 악성코드 수집·분석·장비·전문 인력의 부족 등이 모바일 오피스에서도 재현될 가능성이 높다.

3.1.1.3 서버 및 네트워크 보안위협과 대응현황

서버 및 네트워크 보안 위협요소들은 특히 모바일 오피스 네트워크 환경의 다양화에 기인한다. Wi-Fi 망 확대, 블루투스, 3G망을 통한 데이터 서비스, 테더링 서비스 등 다양한 무선환경을 통해 스마트폰을 경유하여 사내 인트라넷 서버에 접속하는 모바일 오피스에서는 패킷스니핑, 스마트폰 전화도청, 서버감염, 악성코드 설치, 기업정보유출 등의 위협들이 존재한다. 또한, 모바일 오피스용으로 사용하는 스마트폰의 DDoS와 같은 트래픽 점유 악성코드 감염 시 기업내부 서버의 가용성을 저해할 수 있으며, 스마트폰 사용자의 23%만이 보안프로그램을 사용 중인 것으로 조사되어[14], 이러한 위협에 대해 모바일 오피스용 스마트폰의 보안지침이나 PC와 동일 수준의 트래픽 모니터링이 필요하다. PC기반의 봇넷이 스팸메일을 보내는 유형과 비슷하게 스마트폰을 좀비로 만들어 자동으로 광고메시지를 전파할 수 있게 하는 악성코드가 중국에서 사용자 점유율이 높은 심비안 OS에서 2010년 10월 중국에서 발견되었다. 스마트폰을 좀비폰으로 만들어 단말이용 불능 및 특정 사이트 트래픽 유발, 모바일 분산서비스 거부(DDoS)공격을 일으킬 수 있는 악성코드인 것이다. 이는 스마트폰이 DoS공격을 실행할 수 있는 도구가 되는 잠재적 위협성을 의미한다[11]. 현재 모바일 오피스의 FMC기반 네트워크로써 Wi-Fi 및 WiBro의 보안대응은 인증과 암호화, 이에 대한 표준화 준수 등이 있으며, 기업의 VPN 등 보안장비 사용과 망분리를 통한 통신 및 서버 보호대책이 시행되고 있지만, 모바일 오피스 환경에서 적절한 무선랜 보안운영방침과 관리 및 가이드라인의 부재가 문제가 되고 있다.

3.1.1.4 애플리케이션 및 플랫폼 보안위협과 대응현황

국내 이동통신사업자들이 운영하는 앱스토어에 대해서는 각사가 보안검증체계를 구축하고는 있으나, 해외 개방형 애플리케이션 마켓에 대해서는 플랫폼별 앱스토어의 검증기술, 절차의 부재 및 미비로 애플리케

이션 보안관리는 허술한 상황이다. 검증과정을 위해 단말사, 콘텐츠 제공사, 이동통신사, 모바일오피스 도입 기업들의 공조체계를 통한 적극적 협업관계 또한 미흡한 실정이다. 스마트폰 애플리케이션의 보안검증 문제를 해결하기 위해 개발자, 이용자, 스마트폰 애플리케이션 마켓, 스마트폰 애플리케이션 보안성 검증 센서를 주체로 한 스마트폰 애플리케이션 보안성 검증 절차 및 모델들이 제시는 되고 있다. 그 중 WAC(Wholesale App. Community, 도매 애플리케이션 연합체)는 국제표준 단말 플랫폼을 기반으로 이와 호환되는 다양한 국가의 개발자들이 만든 애플리케이션을 확보해 통합 앱스토어를 만든다는 목적을 가지고 있다. WAC가 역할을 수행하기 위해서는 서버 Platform구축을 위한 태스크포스 구축, 관리운영조직구현, 관리비용, 오퍼레이션 전반에 대한 룰과 가이드라인을 필요로 한다. 하지만 사업자의 참여도, WAC 컨셉트의 현실화의 어려움 등으로 WAC 성공에는 부정적인 전망이 존재한다[16]. 모바일 단말의 기반이 되는 운영체제를 비롯한 소프트웨어 체계를 일컫는 모바일 플랫폼은 사용자 환경변경, 성능향상 등을 목적으로 변조되었을 때 여러 가지 보안문제가 발생할 수 있다. 변조된 스마트폰 플랫폼에서 기업용 애플리케이션을 이용하는 경우, 다른 애플리케이션과의 충돌, 주요 정보유출 및 악성코드 감염 등 또 다른 보안문제를 야기할 가능성을 내재하고 있다. 모바일 플랫폼은 점차 데스크톱 수준으로 발전하고 있고 애플리케이션과 서비스가 다양화되고 있다. 특히, 오픈플랫폼 트렌드 속에서 개별 애플리케이션의 신뢰성을 확보하기가 점차 어려워져 응용 계층의 보안 기술만이 아니라 운영체제 계층에서도 보안 해결책이 필요한 실정이다[15]. 현재, 스마트폰 플랫폼의 보안취약점 연구 및 업데이트, 앱의 검증기술, 실행인증, 검증방식에 대한 다양한 연구들이 진행되고는 있지만, 총괄적인 검증기능의 강화를 위한 협업체제나 표준화에 있어서는 문제점이 존재한다.

### 3.1.2 모바일 오피스의 법적 보안위협과 대응현황

모바일 오피스의 보안위협 중 법적 부문과 관련된 분야는 프라이버시, 저작권, 산업기밀보호가 존재한다. 피비스틸러(PbStealer), 플렉시스파이(Flexi-Spy), 콤워리어(Commwarrior), 스미싱(SMS+phishing), 인포잭(InfoJack)과 같은 개인정보 유출 악성코드로 인한 개인정보보호의 위협요소가 존재

〔표 1〕 스마트폰 사용자의 모바일 사용용도

| 순위 | 사용용도 |
|---|---|
| 1 | 장치의 85%가 비즈니스 다이어리로 사용 |
| 2 | 장치의 80%가 비즈니스 대상 이름/주소 저장에 사용 |
| 3 | 장치의 79%가 개인 이름과 주소를 저장하는데 사용 |
| 4 | 장치의 75%가 개인 다이어리에 사용 |
| 5 | 장치의 48%가 오락(게임/음악)에 사용 |
| 6 | 장치의 35%가 문서에 사용 |
| 7 | 장치의 33%가 패스워드/PIN 번호 저장에 사용 |
| 8 | 장치의 32%가 이메일 수신하는데 사용 |
| 9 | 장치의 25%가 은행계좌 관련 사항 저장에 사용 |
| 10 | 장치의 25%가 기업정보를 저장하는데 사용 |

하며, 기업의 입장에서 기술부문의 취약성과 더불어 스마트폰의 개인사용과 결부된 각종 산업기밀유출 위협요소가 존재한다. 〔표 1〕처럼 Pointsec Mobile Technologies에 의해 수행된 모바일 사용에 대한 조사에 따르면, 사용자의 85%가 비즈니스 다이어리, 80%가 비즈니스 대상 이름과 주소 입력 등에 활용한다고 한다[17]. 즉, 모바일 오피스용 디바이스로 사용하지 않더라도, 개인의 모바일 디바이스를 비즈니스용으로 사용함이 높은 %를 나타내고 있음은, 모바일 오피스에서 스마트폰의 분실, 도난, 악성코드 감염 등과 결부될 때 심각한 기업정보 및 고객정보 노출 위협으로까지 이어질 수 있다. 하지만 모바일 오피스를 사용하는 기업에서 업무용 이외에 개인적 용도로도 사용이 가능한 스마트폰의 위치추적이나 LBS기능을 포함한 기업의 애플리케이션을 사용하는 경우, 위치정보보호법을 적용 반영 하는 데는 어려움이 있다.

### 3.1.3 모바일 오피스의 관리적 보안위협과 대응현황

모바일 오피스를 도입한 기업입장에서는 기술적인 보안 위협과 더불어 관리적 보안위협에 대한 대응 또한 소홀히 할 수 없다. 개인이나 기업을 포함한 유기적이며 통합적인 대응책들의 선택과 활용, 그리고 조직의 현실을 가장 잘 반영할 수 있는 정보보호관리 체계의 수립을 언급하고 있는 정보보호관리체계(ISMS, Information Security Management System)는 아직까지 스마트 모바일 오피스 환경에서 정형화된 정보보호관리체계를 적용하지 못하고 있다[18]. 기업에서 이미 적용하고 있는 정보보호 정책 및 관리요소들에 모바일 오피스의 보안 위협 요소와 대응방안들을 구체적으로 적용하되 그 수준과 시기가 충분히 고려되

어 제시된 바는 없다.

〔표 2〕는 스마트폰 기반 모바일 오피스의 보안 위협과 대응현황에 대하여 정리하였다. 모바일 오피스의 보안 위협요소들을 기술적, 법적, 관리적 측면에서 구분하여 기술하고, 이러한 위협에 대응하는 보안 솔루션이나 시스템 또는 관련 제도에 대해서 정리하였다. 특히, 보안 대응 및 현황에서는 모바일 오피스 환경에서만 필요한 새로운 형태의 보안 대응들 이외에 기존

〔표 2〕 스마트폰 기반 모바일 오피스의 보안위협과 대응현황

| 구분 | | 보안 위협 | 보안 대응 및 현황 |
|---|---|---|---|
| 기술부문 | 스마트폰 단말 | • 분실, 도난, 재사용<br>• VM뱅킹, 모바일 안심출금서비스, USIM을 통한 ATM 연동에서 부정사용<br>• 카메라 촬영, 녹음 기능<br>• 스마트폰을 USB와 같은 이동형 저장장치로 활용 | • 스마트폰 분실, 도난 시 MDM(Mobile Device Manager)을 통한 원격 잠금, 파일삭제, 기기사용 중지<br>• USB 보안 솔루션<br>• 모바일 Device 관리 시스템에 구성 가이드〔19〕 |
| | 모바일 악성코드 | • 단말장애 유발형, 배터리 소모형, 과금유발형, 정보유출형, 크로스 플랫폼형 악성코드 유형들과 매년 악성코드 증가(2009년 상반기까지 524건)<br>• 악성코드에 감염된 스마트폰에서 SMS/MMS, E-Mail등 경로로 개인정보 및 기업정보 유출위협 | • 안철수 연구소, NSHC, 하우리, 소프트 씨큐리티 등 업체에서 모바일 백신 서비스 제공<br>• 허니팟 기반 Honeyspot과 Smartpot, 웜뱃프로젝트 기반의 Paranoid Adroid과 Bluebat 등 국내 산·학계에서 연구되고 있는 악성코드 수집 시스템〔11〕 |
| | 애플리케이션 및 플랫폼 | • 누구나 제작, 배포, 설치가 가능한 오픈마켓의 특성에 의한 악의적 소프트웨어 등록 등 애플리케이션의 부정사용<br>• 탈옥, 검증받지 않은 애플리케이션을 통한 플랫폼 위·변조로 스마트폰 기능 장애<br>• 플랫폼별 앱스토어의 검증기술, 절차의 미비<br>• 펌웨어 취약점을 이용한 서비스 거부<br>• 플랫폼과 펌웨어의 충돌 및 변조가능성<br>• Web2.0 AJAX관련 취약점(동일 근원지 정책우회, 크로스사이트 스크립트, 크로스 사이트 요청변조, Open API에 의한 Mash-up취약점)〔20〕 | • 폐쇄적 형태인 Apple의 앱스토어 앱 검증절차<br>• 아이폰의 애플, 안드로이드폰의 구글, 윈도우모바일의 MS는 애플리케이션 검증방식의 개발가이드 제공<br>• 애플리케이션 코드 난독화 기술<br>• Code Signing 기술 등 모바일 애플리케이션 유통 인증기술<br>• 애플리케이션 실행인증 기술<br>• 사용자 인증 기술<br>• 애플리케이션들에 대한 검증과정을 위해 단말사, 콘텐츠 제공사, 통신사, 모바일오피스 도입 기업들의 협업관계 부재 |
| | 서버 및 네트워크 | • Wi-Fi 증대, 블루투스, 3G망을 통한 데이터 서비스, 테더링 서비스 등 다양한 무선인터페이스 지원에 따른 비인가 접속의 위협<br>• SMS/MMS 대량 발송으로 트래픽 점유로 인한 스마트폰 사용망의 가용성 침해<br>• 무선 데이터 수집 등 패킷 스니핑<br>• 전화도청으로 인한 기업정보 도청위험<br>• 취약한 인증·전송 정보노출<br>• 스마트폰을 경유하여 내부망 접속에 의한 서버·DB 감염 및 해킹경로로 이용<br>• 기업서버에 산업정보유출 악의적 프로그램 설치 | • AES 등이 적용된 암호화 기능 및 VPN기술<br>• Wi-Fi 무선구간 보안을 위한 WPA2(Wi-Fi Protected Access v2)표준<br>• Wibro환경에서 인증과 암호화를 위한 보안부계층(Security Sublayer)〔21〕<br>• DMZ구성 및 망 분리, 이동통신망 접속 제한 기술<br>• WIPS(Wireless intrusion prevention system) 등 Rogue AP 차단 솔루션<br>• 무선 AP자체의 보안설정으로 접근제어<br>• 서버망 보호를 위한 유해트래픽 탐지시스템<br>• ESM등 네트워크 자원제어 모니터링 솔루션 |
| 법적부문 | 프라이버시 저작권 산업기밀 보호 | • 스마트폰 위치기반서비스, 소셜 네트워크 서비스 등으로 인한 개인정보 침해위협요소 존재<br>• 앱스토어의 컨텐츠 제작 및 2차적 저작물에 대한 저작권 침해 및 적용여부<br>• 국외 애플리케이션을 모방한 국내 애플리케이션의 저작권 문제<br>• 기술부문의 취약성 및 스마트폰의 개인사용에 있어서 각종 산업기밀유출 위협요소 존재 | • 위치정보보호 및 개인정보보호법<br>• 공공기관의 개인정보보호에 관한 법률시행규칙 제6조 - 단말기의 설치·관리<br>• 불법복제 및 유통 어플리케이션의 실행을 제한하는 개발자의 저작권보호를 위한 T스토어(SKT)의 ARM(Application Right Management) 정책〔16〕<br>• 스마트폰이라는 새로운 디바이스에서 일어날 수 있는 위협에 대한 산업기술유출방지 기술 미비 |
| 관리부문 | 정책 및 관리 | • 모바일 오피스 보안을 위한 정책 및 관리의 미비<br>• 모바일 오피스 보안을 위한 모니터링, 감사 미비<br>• 모바일 오피스 구축 보안 가이드라인 부재 | • ESM(Enterprise Security Management) 등 네트워크 자원제어 모니터링 솔루션<br>• 스마트폰 사용자 10대 안전수칙 |
| | 사고대응 | • 모바일 오피스 관련 보안사고 대응계획체계 부재<br>• 모바일 오피스 관련 CERT 등 대응 및 복구 체제 부재 | • 스마트폰 정보보호 민·관 합동대응반 긴급 구성하여, 스마트폰 정보보호 주체별 역할 정립추진, 모바일 악성코드 공동대응 모의훈련 실시〔22〕 |

의 정보보호관련 시스템으로 대응하고 있는 형태의 것들에 대해서도 기술하였다.

### 3.2 모바일 오피스 보안을 위한 대응체계로써 CERT와 ISAC

정보 시스템 및 정보유통 체계의 발달로 수많은 정보가 인터넷을 통하여 유통되고 또 노출되어 있다. 이 과정에서 정보시스템과 정보를 겨냥한 보안사고가 등장하고 있으며, 특히 최근에는 금전적 이익을 취득하기 위한 목적으로 다양한 공격 기법들이 등장해 기승을 부리고 있다. 사이버 침해사고에 대하여 조직적인 대응체계를 구축함으로써 기술적인 사이버 침해사고 대응이 다루어져왔으며, 현재는 다양한 보안위협에 대응하기 위하여 기존의 기술적인 측면뿐만 아니라 관리적인 측면과 물리적인 측면에 대한 관심도 높아지고 있다. CERT의 역할은 기술적 부분에 한정하여 다루어서는 안 되며, 해당 조직 전체를 보호할 수 있도록 조직체계와 역할을 정의하여야 한다. 또한 정부와 민간, 산업별, 국가 간, 멤버 및 파트너간의 정보를 공유하며, CERT의 성공적인 활동을 위해서는 CERT의 역할 및 범위와 정보보호 활동 계획 등이 정의되어 유기적인 연관관계를 가져야 한다[23]. ISAC의 주 역할은 사이버테러 취약점과 침해요인, 대응방안에 관한 정보를 제공하고 침해사고가 발생하면 실시간 경보와 분석업무를 수행하며, 아울러 분야별 여건을 고려, 침해사고 대응체계(CERT) 구성 및 운영, 정보통신 기반시설 보호시스템 시험 등 정보보호 관련 교육과 훈련 서비스 등을 제공하여 관련 기관이 침해사고 발생의 주요 정보사항을 공유, 공동 대응하는 데 있다[24][25]. 음성 인터넷 프로토콜(VOIP, Voice Over IP)처럼 새롭게 등장하거나 새로운 부분에 대해서 CERT와 ISAC이 위협 대응체계를 별도로 갖추었듯이, 모바일 오피스 환경이라는 새로운 환경에 대해서도 위와 같은 CERT와 ISAC의 기능은 새로운 환경에 대한 보안대응과 지속적 모니터링, 선제적 사고대응협력 및 공조체제, 정보공유 및 분석의 기능을 수행해야 한다.

### 3.3 국내 CERT와 ISAC의 현황 및 문제점

국내의 침해사고 대응체계는 국가정보원의 국가사이버안전센터(NCSC, National Cyber Security Center), 국방부의 국방정보전대응센터, 공공기관은 시·도 자체 사이버침해대응지원센터, 민간분야는 한국정보보호진흥원의 인터넷침해사고대응지원센터(KISC, Korea Internet Security Center)로 구성되어 있다. 국내의 보안정보공유를 위한 정보보호기관들의 주요 활동 및 업무는 아래와 같다[26].

국가사이버안전센터(NCSC)에서는 국가 사이버 안전 정책을 총괄하며, 사이버 안전 예방 활동, 사이버위협정보 수집·분석·전파, 침해사고 대응, 국내외 사이버위협 정보 공유 체계 운영 등의 종합보안서비스를 제공하고 있다. 정부 보안정보공유분석센터(GISAC)는 주요 정보시스템과 전자정부 통합망 사이버 공격 대응, 국가사이버안전센터에 로그정보 제공, 전자정부 통합망의 정부기관들의 보안관련 정보를 공유하고 있다. 국방정보전 대응센터는 국방 주요 정보체계 취약성 진단·탐지·분석 임무와 국방전산망에 대한 침해사고 예방 및 사고조사·수사 임무, 국내외 정보전 관련 정보분석, 사이버전 대응훈련, 국가사이버안전센터와 연동하여 군 인터넷 환경을 대상으로 보안관제 업무를 지원하고 있다. 방송통신위원회의 인터넷침해사고대응지원센터(KISC)에서는 취약점, 웜·바이러스 등 모니터링·탐지·분석·예방 역할을 수행하며, 국내 정보통신서비스제공자(ISP), 백신업체, 보안관제업체 등과 정보공유, 공동대응체계 구축, 해외 유관기관과의 공조체계 활동을 하고 있다. 국내에서는 취약점 관리 및 연계체제에 있어서 별다른 연계체제 없이 서로 다른 기관이 정보보호 업무를 담당하고 있으며, 취약점에 대한 체계적 관리와 공유 또는 통합된 DB가 존재하지 않는다[20].

모바일 오피스를 구성하는 요소들에 대해 기술적, 법적, 관리적 측면으로 구분하여 발생 혹은 발생할 수 있는 보안 위협들에 대해 분석하고, 이들 각각에 대한 현재 보안 현황 실태를 검토한 결과 현재 모바일 오피스 보안을 위한 국내 CERT와 ISAC에 대해 다음과 같은 문제점을 도출할 수 있었다.

첫째, 모바일 오피스는 이전의 오피스 환경과는 다른 새로운 환경요소를 가지고 있으며, 추가된 특수한 범위에서 나타날 수 있는 보안위협들에 대해 기존의 보안대응으로 해결할 수 없는 부분이 존재한다. 이러한 새로운 영역에 대한 보안 대응이 필요하다. 다양한 무선 인터넷 환경, 스마트폰과 태블릿PC, Web 2.0, 앱스토어의 애플리케이션 등은 이전의 오피스 환경과는 다른 요소이며, 이에 대한 새로운 위협 요소들이 존재하고 있다. 테더링(Tethering) 서비스와 같은 경우, 컴퓨터가 스마트폰을 통해 인터넷을 접속할 수

있게 해주는 방법으로 컴퓨터는 모바일폰과 케이블, 블루투스 연결 또는 다른 다양한 방법으로 연결된다. 스마트폰이 무선공유기(AP)와 같은 역할을 수행하므로 모바일 오피스에서 내부 인프라 서버접속방법의 새로운 방식을 제공하지만, 테더링 서비스가 악용될 경우, 모바일 오피스 구축사들에게는 기업정보 유출 등 무선랜 보안위협 요소로 작용할 수 있다. 이미 기업에 구축된 네트워크 보안 인프라 요소들인 방화벽(Firewall), 침입탐지시스템(IDS), 침입차단시스템(IPS), 가상사설망(VPN), DMZ(demilitarized zone)구성 등 만으로는 테더링 서비스의 악용과 같은 비 인가된 무선접속 환경에 대해 대응하기 어려운 부분이 존재한다. 세계 모바일 보안시장의 경우, 6년간('09~'15년) 2.2배 증가하여 '15년에 약 2,864백만달러(약 3조원)가 될 것으로 전망(IDC, '10.5월)하고 있다. '10년 국내 정보보안 시장규모는 9,179억원(예측치)이며, 그 중 모바일 보안시장은 약 57억원(0.6%)차지하며, 연평균 206%성장 예상으로 '15년 약 2,078억원(12.9%)에 이를 전망이다[27]. 이러한 모바일 보안시장의 활성화에 비해 WIPS, Mobile VPN 등 모바일 오피스 환경에 맞는 보안기술, 솔루션을 적용하고자 할 때 구체적인 활용방법과 규제가 미흡하다. 또한 모바일 오피스 활성화와 보안위협 대응간의 최적 보안투자 수준의 적정성을 위한 허용 정책기준과 나아가 모바일 응용의 확장에 대한 부분을 고려하여, 보안설정 및 솔루션 도입 고려사항 등 CERT의 역할도 고려하여야 한다.

둘째, 모바일 오피스는 모바일 오피스를 구성하기 위한 새로운 요소들에 의한 위협과 기존의 보안위협과 결부되어 다양한 형태들로의 위협 및 가능성을 가지고 있다. 이에 대해 포괄적이고 총괄적인 보안 대응 및 관리가 필요하다. [표 2]의 모바일 오피스의 보안 위협과 대응현황에서 각 부분별로 기술적 대응은 존재하지만, 통합적으로 이를 관리하는 관리부분에 대한 대응이 부재하다는 것을 알 수 있으며, 향후 기업 전체의 보안에 모바일 오피스 보안을 포함할 수 있는 기존 시스템을 활용할 수 있는 방법이나 시스템이 요구된다. 특히, 스마트폰은 모바일 오피스에서 기존의 업무 PC를 대신하는 단말기이지만, 인터넷 환경과 함께 PC환경에서 나타날 수 있는 보안 위협들이 스마트폰을 대상으로 변화된 환경에 맞추어 나타나고 있고, 앞서 살펴본 모바일 오피스의 보안위협 중 기술 부분의 스마트폰 단말 영역에서의 위협뿐 아니라 다른 영역과 다양한 형태로의 위협으로 연계되어 나타나고 있다. 스마트폰의 다양한 통신 인터페이스 제공을 악용한 Cross-Service 공격의 경우, 무선인터넷을 통해 회사 내부 서버에 접속하는 사용자를 대상으로 공격자는 무선네트워크를 모니터링하여 엑세스 포인트에 엮인 장치를 스캔하여 취약한 서비스를 통해 스마트폰에 대한 출입권한을 얻은 후 과금 청구 등을 일으킨다[28]. 즉, 특정 네트워크 서비스로 들어온 프로세스가 다른 서비스와 관련된 자원을 접근하며, 기존의 무선 환경에서 존재하던 공격과는 달리 과금과 배터리 소모를 야기 시킨다는 면에서 더 위협적이다. 이는 스마트폰이 다양한 무선접속환경의 개방성, 휴대성, 저성능의 특성[10]으로 기존 PC환경의 보안위협과 더불어 새로운 보안 위협에 노출되어 있다는 것이며, 기존 PC와 같은 형태로 보안기술이나 정책을 적용했을 경우, 예측할 수 없는 새로운 형태의 또 다른 위협을 야기할 가능성이 크다는 것이다.

셋째, 앞서 지적한 새로운 환경에 대한 보안 대응을 위해 자체적인 정보력 등이 부재하다면, 모바일 오피스 환경 보안을 위한 CERT의 본연의 기능인 선제적 사고대응협력 및 공조체제를 통한 보완이 필요하며, 현재 이에 대한 부분이 미흡하다. 2005년 6월부터 민간기업·기관에 소속된 침해사고 대응팀(CERT)이 참여하는 협의체 조직인 CONCERT(Consortium of CERT)가 운영되고 있지만, 7·7 DDoS와 같은 비상상황에서 악성코드 수집·제거 및 시스템 복구 등 실질적인 대응 미흡 등 민관협력공조체제의 한계라는 문제점[29]이 지적된바 있다. 스마트폰 기반 악성코드들 중에서 대량 SMS메시지 전송을 이용한 DDoS 공격이 행해진다면, 그 피해는 7·7 DDoS 사태를 능가하는 결과를 초래할 가능성도 충분하다. 2010년 1월 방송통신위원회가 스마트폰의 보안위협에 대한 대응을 위해 '스마트폰 정보보호 민·관 합동대응반'을 구성하였지만, 7·7 DDoS 공격 대응의 문제점을 따르지 않기 위해 선언적 의미가 아닌 국제 공조, 선제적 대응협력체제 구축 등 지속적인 전개가 요구된다.

넷째, 모바일 오피스 환경의 지속적인 모니터링 및 관련기관과의 협력체제가 미비하여 총체적인 정보수집과 관리에 대한 부분이 부재한 상황이다. PC환경의 경우 악성코드를 분석하기 위한 정형화된 기법과 도구들이 많이 알려져 있으며, 대부분 윈도우즈 플랫폼 기반의 악성코드이기 때문에 분석 기법 및 도구의 활용이 용이하다. 반면, 스마트폰 상에서 동작하는 모바일 악성코드의 경우에는 분석 가능한 전용도구들이 부재할 뿐 아니라, 스마트폰 자체가 수십 종의 플랫폼 상

에서 구현되며 다양한 운영체제를 탑재하고 있기 때문에 체계적으로 악성코드를 분석하는데 어려움이 있다[30]. 악성코드를 분석하기 위해서는 악성코드 수집하는 기술이 선행되어야하며, 수집시스템은 여러 프로젝트에서 허니팟 시스템 기술을 적용하여 악성코드를 분석하고 수집하고 있다. 그러나 허니팟(HoneyPot)은 오탐률(False Positive)과 미탐지율(False Negative)을 감소시킬 수 있지만 탐지영역의 한계가 존재한다[11]. 모바일 악성코드를 분석하기 위해서는 감염된 단말기로부터 실제 악성코드를 수집하는 것도 중요하지만, 단말기 사용자로부터 악성코드 감염에 따른 단말기 증상에 관한 정보를 추가적으로 얻는 것이 중요하며, 이는 단말기 내에 저장된 악성코드를 식별하고 관련 프로세스에 의한 악성행위를 분석하는 데 소요되는 시간을 단축시킬 수 있다[30]. 이와 같이 스마트폰 기반 악성코드 수집방법에 한계가 존재하며, 모바일 악성코드에 대한 분석 및 대응 준비가 부족한 것이 국내 현실이다. 모바일오피스 사용기업의 모니터링 시스템이나 관리체계를 통한 데이터 및 정보들은 악성코드 수집 및 분석에 활용하는 방안으로 고려될 수 있으며, 스마트폰 모바일 관련 악성코드 수집, 분석기술의 개발을 위한 정보공유의 장이나 체제가 요구된다.

## IV. 주요국의 CERT 및 ISAC

### 4.1 미국의 CERT 및 ISAC

미국의 사이버위기 대응체제는 국토안보부(DHS, Department of Homeland Security)를 중심으로 효율적인 대응체계를 마련하였고, 사이버보안 정책 추진을 위해 국립표준기술연구소(NIST, National Institute of Standard and Technology), 전미과학재단(NSF, National Science Foundation), 에너지부(DoE, Department of Energy) 등 타부처와 유관기관들이 협조하고 있다. 정부기관과 민간에서 CERT와 ISAC을 운영하고, 국방부는 CERT를 운영하여 민·관·군이 상호 공조하는 CERT와 ISAC위주로 정보보안 정책을 추진하고 있다[31]. 보안정보공유체계로써 미국은 사이버보안정보공유프로젝트(CSISP, Cyber Security Information Sharing Project)와 사이버경보정보망(CWIN, Cyber Warning Information Network)를 추진하여 정부와 민간부분의 정보공유모델을 연구 및 공유하고 있으며, 총 17개의 중요정보통신기반구조별 CERT 또는 ISAC이 연계되어 운영 중에 있다. 보안정보공유를 위해 국토안보부 책임하 국가차원의 취약점DB인 NVD(National Vulnerability Database)를 구축하고, 보안전문가 소프트웨어벤더, 침해사고대응팀 등 관련기관과 협력체계를 이루어 운영하여 관리하고 있다. 국토안보부의 국가사이버보안부(NCSC)와 SRI International, Symantec, Computer Associates가 참여하는 '사이버보안 모니터링 프로젝트'에서 비영리용 데이터 수집 시스템의 개발을 수행하고 협조체제를 구축하고 있다. 이러한 공조체계를 뒷받침하는 취약점 관리 체계로써 CVE(Common Vulnerabilities and Exposures), CWE(Common Weakness Enumeration), OSVDB(Open Source Vulnerability DB) 등의 데이터베이스를 통해 보안위협정보제공, 정보공유, DB 작업비용 감소의 역할을 하고 있다[32].

미국은 스마트폰 OS 취약점에 대해서도 정보제공 및 관리를 하고 있으며, 별도의 항목으로 구성하여 보안취약점 정보를 제공하고 있다. CVE와 NVD에서는 스마트폰 중 아이폰과 안드로이드폰에 대한 보안 취약점들이 보고되고 있고 US-CERT의 National Cyber Alert System에서도 해당 보안취약점들이 포함되어 정보가 제공되고 있다[33][34][35]. SANS와 CWE에서는 '2010 CWE/SANS Top25 Most Dangerous Software Errors'는 심각한 소프트웨어 취약점을 야기 시킬 수 있는 가장 위험한 프로그래밍 에러에 대해 발표[36]하고 있어 스마트폰 애플리케이션 개발에 보안사항으로 참고할 수 있다. OWASP(The Open Web Application Security Project)은 애플리케이션 소프트웨어 보안강화를 위해 2004년 미국에서 설립된 국제 조직으로, 빠른 모바일 컴퓨팅의 성장에 맞추어 안전한 모바일 개발을 위한 요구를 반영하여 '모바일 보안 프로젝트(Mobile Security Project)'를 실시하고 있다. 이 프로젝트에서는 아이폰OS·안드로이드·웹OS·윈도우 모바일 OS·블랙베리 플랫폼으로 구분하여 모바일 어플리케이션에 나타나는 위험 정보제공·방지를 위해 Security Testing(일반적인 모바일 애플리케이션 평가방법론)도 제공하고 있다[37]. Aspect Security 회사와 MITRE-CVE 이외에 여러 기업들이 'OWASP Top 10 2010'도 발표하고 있으며, 여기에는 스마트폰 환경의 기반인 Web 2.0의 보안 취약점을 포함하고 있다.

### 4.2 유럽의 CERT 및 ISAC

유럽의 정보보호 추진체계는 유럽집행위원회(European Commission)의 정보사회미디어총국(INFSO)과 유럽네트워크정보보호청(ENISA, European Network and Information Security Agency)에서 역할을 수행하고 있으며, 유럽연합의 ENISA에서는 유럽조기경보시스템(EWIS, European Warning and Information System)을 구축하여 각 회원국가의 국가정보보호조직, 통신사업자, 개인 이용자 등을 연결하는 작업을 수행하였다. 조기경보체제에서 분야별 대표 CERT 또는 ISAC을 구축 및 육성하여 사이버테러에 대응하고 있으며, 미국 NIST 등과 연계하여 미국 NVD 및 CVE 등의 취약점 정보들을 공유하고 있다. 또한 유럽국가들의 CERT그룹인 EGC(European Government CERTs Group)에서 CRIRTUK(영국), CERT-Bund(독일), CERTA(프랑스) 등 각 유럽국가의 멤버 CERT들이 취약점 및 침해사고에 효율적으로 대응하기 위한 기관을 두고 있다[32].

### 4.3 일본의 CERT 및 ISAC

일본은 정보보호정책회의(ISPC)와 정보보호센터(NISC)에서 정보보호를 담당하고, 사이버침해사고 대응체계는 국가긴급대응팀(NIRT)이 있다. 보안정보공유시스템으로써 2007년부터 3단계 IRISS프로젝트를 추진하여 전세계 다중센서들을 통해 보안정보를 수집, 연관성분석, 사이버공격 관련 보안정보를 기관·기업 등의 회원사들에게 제공하는 WorldMap View 프로젝트가 있다. IPA(Information-technology Promotion Agency)와 JPCERT/CC가 각각 취약점 정보수집·분석, 대외협력기관역할을 하며, 국가취약점 DB인 JVN(Japan Vulnerabilities Notes)과 JVN iPedia가 있다. 미국 및 영국과 공조체제를 구축하여 보안취약점 대외협력체계를 구축하는 동시에 국내외 취약점을 별도로 관리하고 있다[32].

일본은 미국처럼 별도의 Mobile Security 관리시스템은 없지만 JVN iPedia DB에서 구글 안드로이드·Web Toolkit·안드로이드 SDK·Chrome OS, 애플 iOS·아이폰 등 Vendor의 product별 취약점 정보를 제공하고 있다[33].

### 4.4 모바일 오피스 환경에서 국내 CERT와 ISAC의 비교·분석 및 시사점

미국과 일본의 경우, 모바일 보안 분야가 CERT, ISAC, 취약점 DB에 포함되는 등 모바일 오피스라는 새로운 환경의 위협에 대해서도 대응할 수 있는 효율적이고 안정화된 시스템을 가지고 있으며, 이러한 해외 사례를 통해 CERT의 기능 중 대응시스템과 ISAC의 역할 중 보안 취약점 관리체계 및 국제협력관계에 있어서 시사점을 도출할 수 있다.

첫째, 미국과 유럽의 경우 분야별 CERT와 ISAC을 운영하며 동시에 이들을 서로 유기적으로 연계시켜, 실시간 모니터링을 통한 효율적 정보수집·제공의 기능과 더불어 빠른 사이버침해조기대응시스템을 갖추고 있음을 알 수 있다. 미국의 경우, 사이버보안정보공유프로젝트(CSISP)와 같은 국가와 민간 전문가들의 정보공유를 통해 사이버경보정보망(CWIN)과 같은 조기경보체제를 구축하고 있으며, 유럽의 경우 자체 취약점 DB는 없지만 대외협력체계구축을 통해 유럽조기경보시스템(EWIS)과 같은 조기경보 및 대응시스템을 갖추고 있다. 이렇듯 CERT와 ISAC의 유기적 연계 및 협력관계를 통해, 신뢰할 수 있는 취약점 정보공유체계와 신속한 조기경보시스템은 급속한 증가추이를 보이고 있는 스마트폰 악성코드에 대한 위협대응체계로써 고려될 수 있다.

둘째, 취약점 DB구축 및 관리체계에 있어서 미국과 일본의 경우 대외협력조직체계, 취약점 통합관리체계, 취약점정보 활용체계 등을 잘 구성하고 있으며, 취약점 관리체계과 협조체제는 예방의 기능과 관련되어 있다. 미국의 취약점 DB인 NVD는 보안전문가 소프트웨어벤더, 침해사고 대응팀 등 관련기관과 협력체계를 이루어 운영하여 통합 관리되며, 일본 국가 취약점 DB인 JVN(iPedia)은 미국 및 영국과 공조체제를 구축하여 보안취약점의 대외협력체계구축 및 국내외 취약점은 별도 관리되고 있다. 국가차원에서 취약점 DB가 잘 구축·관리 된다면 취약점 대응 및 보안사고 예방의 역할 뿐 아니라, 스마트폰과 같은 새롭게 등장하는 환경에 대해서도 기존의 취약점 DB나 통합관리체계 및 정보시스템 활용체계에 적용하는 것은 어렵지 않다. 또한 새로운 모바일 오피스라는 환경에 대한 위협도 기존 시스템을 활용하거나 통합적 관점에서 취약점 관리가 가능하다.

셋째, 미국의 경우 안드로이드, 아이폰 등 모바일 오피스의 가장 핵심적인 요소인 스마트폰의 OS별 악

〔표 3〕 국내외 사이버 침해사고 대응체계와 보안정보공유체계, 취약점관리체계 및 국제협력관계, 모바일 오피스 보안 관련 체계

| | 사이버 침해사고 대응체계 | 보안정보공유체계 | 보안취약점 관리체계 및 국제협력 | 모바일 오피스 관련 취약점DB·활용체계 |
|---|---|---|---|---|
| 미국 | • 국토안보부(DHS) : 국토안전 및 사이버보안 주무처<br>• 국가사이버보안센터(NCSC) :국토안보부내 정보보호업무 담당<br>• 사이버보안 정책 추진시, 국토안보부 주체로 국립표준기술연구소(NIST), 국가과학재단(NSF), 에너지부(DOE) 등 타 부처 및 유관기관과 협조<br>• 컴퓨터 긴급대응팀(US -CERT) : 국토안보부(DHS)산하 국가보호프로그램<br>• 대통령직속 주요기반보호위원회(PCIPB) : 사이버공간 보안 국가전략(National Strategy to Security Cyber space)를 수립<br>• 총 17개의 중요 정보통신기반 구조별 CERT 또는 ISAC<br>• 사이버경보정보망(CWIN): 조기경보체제로 인터넷과 분리한 독립 사설망 | • 사이버보안정보공유프로젝트 (CS-ISP): 정부·민간의 정보공유<br>• 사이버경보정보망(CWIN): NIPC, CIAO, 민간 ISAC, 기타 정부 보안관련기관 참여로 정부·민간 전문가들의 정보공유<br>• 사이버보안 모니터링프로젝트 : 국가사이버보안부(NCSD)와 SRI International, Symantec, Computer Associates 참여, 비영리용 데이터수집 시스템, 협조체계 구축<br>• MITRE : 미국연방정부가 설립, 미국방부, 연방, 항공국, 국세청 등의 보안관련 정보 연구, 개발<br>• CVE : Microsoft, IBM, Computer Associates, Novell 등 200여개 회사, 단체들의 보안위협정보 정리 제공<br>• CWE : 소프트웨어 취약성의 정식 목록작성 및 보안정보공유<br>• OSVDB : 보안전문가 그룹의 S/W 보안결함정보공유 무료DB | • 사이버보안정보공유프로젝트 (CS-ISP), 사이버경보정보망 (CWIN) : 보안취약점 관리 및 대외협력조직체계<br>• NVD: 국가 취약점 DB, 보안전문가, 소프트웨어 벤더, 침해사고 대응팀 등 협력체계<br>• Secunia DB : 기업에서 전세계 공공·금융·교육기관과 CVE· NVD 연계, 권고용 취약점 DB<br>• OSVDB : 데프콘컨퍼런스에서 설립한 공개형 취약점DB<br>• CVE, CWE, OVAL, CPE 등은 미국정부의 정보보안 위협기술 자동화·표준화 구성요소<br>• OVAL(Open Vulnerability and Assessment Language) : NVD 정보를 이용, 컴퓨터 시스템의 보안설정상태 검사 위한 언어<br>• CPE(Common Platform Enumeration) : H/W, S/W, OS, Application 취약점 정보를 식별하기위한 공통플랫폼 목록 | • CVE, NVD DB : 스마트폰 OS취약점에 대한 정보제공 및 관리<br>• US-CERT : 아이폰, 안드로이드폰의 취약점이 National Cyber Alert System 내용에 포함<br>• OWASP : Mobile Security Project<br>• OWASP Top10 : AspectSecurity社, MITRE-CVE, 기업들의 웹애플리케이션 보안위험기술<br>• CWE/SANS Top 25 Most Dangerous Software Errors |
| 유럽 | • 정보사회미디어총국(INFSO)과 유럽네트워크정보보호청 (ENISA)에서 정보보호 수행<br>• 분야별, 중요정보통신기반별 대표 CERT/ISAC 구축·운영<br>• 유럽조기경보시스템(EWIS): ENSIA에서 회원국의 국가정보보호조직, 침해사고대응팀, 정보공유 및 분석센터, 기업의 정보보호 조직, 통신사업자, 개인 이용자를 연결<br>• EGC : 유럽 멤버 CERT들의 취약점관리,침해사고대응 | • 유럽네트워크정보보호청 : ECU회원국의 IT정보보호 전담기구역할 수행 및 정보보호 관련 정보공유<br>• 분야별, 중요정보통신기반구조별 ISAC을 육성하여 정보공유 | • EU산하기관인 유럽네트워크정보보안청(ENISA)과 유럽국가들의 CERT그룹인 EGC에서 취약점 체계 주도적 관리<br>• ENISA: 유럽 정보보호의 전반적 조율, 네트워크 및 정보보호 문제, 대외협력조직체계 담당<br>• 유럽조기경보시스템(EWIS): ENSIA에서 회원국의 취약점 관리 위한 국제협력담당<br>• 미국 NIST와 연계, NVD, CVE 등 취약점 정보공유 | • 모바일 오피스 관련 자체적인 취약점 DB 및 활용체계 없음 |
| 일본 | • 정보보호정책회의(ISPC)와 정보보호센터(NISC)에서 정보보호 담당<br>• 경찰청 사이버포스팀(Cyber Force) : 사이버테러 확산방지, 모니터링, 긴급대응<br>• 지역별 정보통신부서에 사이버범죄기술부(HTCTD)설립<br>• 국가긴급대응팀(NIRT): 내각관방 소속 일본정보 침해사고대응센터 | • WorldMap View 프로젝트 : 2007년부터 3단계 IRISS프로젝트 추진하여 전세계 설치된 다중센서들을 통해 보안정보 수집, 연관성 분석하여 사이버 공격에 대한 대규모 보안정보를 기관·기업 등의 회원사들에게 제공 | • IPA와 JPCERT/CC :취약점 정보수집·분석·공개,대외협력기관<br>• 정보보안 조기경보 파트너십 (Information Security Early Warning Partnership) : IPA와 JPCERT/CC중심의 취약점 관리<br>• JVN, JVN iPedia : 국가취약점 DB<br>• 보안취약점 대외협력체계: 미국 및 영국과 공조체제 구축, 국내외 취약점 별도관리 | • 별도의 Mobile Security메뉴없음<br>• RSS, OpenAPI로 신규취약점 서비스 제공<br>• JVN iPedia DB :구글 안드로이드, 애플 iOS·아이폰 등 Vendor의 product 별 취약점정보 제공 |
| 한국 | • 국가정보원의 국가사이버안전센터(NCSC)<br>• 국방부 국방정보전대응센터<br>• 공공기관의 시·도자체 사이버침해대응지원센터<br>• 민간부분의 인터넷 침해사고대응지원센터(KISC) | • 국가사이버안전센터(NCSC): 정보공유 및 공유체계운영<br>• 국방정보전대응센터: 정부 기관들의 보안관련 정보 공유<br>• 인터넷침해사고대응지원센터(KISC) : ISP, 백신업체, 보안관제업체 등과 정보공유 | • 취약점 관리 및 연계체제 부재<br>• 취약점에 대한 체계적 관리와 공유부재<br>• 통합된 DB부재 | • 모바일 오피스 관련 자체적인 취약점 DB 및 활용체계 없음 |

성코드에 대해서 취약점 DB를 보유, 관리하고 있었다. 즉, 새롭고 특화된 환경에 대한 취약점 DB에 대해서 별도의 관리 및 정보제공의 기능을 하고 있다. 물론 모바일 오피스의 환경을 이루고 있는 여러 다른 요소인 WiFi, 무선네트워크 등은 이미 기존의 오피스 환경 요소로써 취약점 DB가 존재하기 때문에 여기서는 논외로 한다. 국내의 경우는 취약점이 발견되면 개인이 벤더나 기관에 해당 사항을 신고하고 보안패치가 나올 때까지 기다리는 상황이지만, 국가 주도적이거나 협력체계에 의해 잘 구축된 DB가 존재할 경우, 관련 업체들은 예방차원에서 해당 취약점을 선적용하여 제품을 개발하거나 서비스를 할 수 있다. 'CWE/SANS 25대 위험한 프로그래밍 에러(Top25 Most Dangerous Software Errors)'와 'OWASP 10대 취약점(Top 10 Application Security Risks)'을 활용하는 방법이 그 예이다.

넷째, 유럽의 경우 국제 협력체제를 통해서 DB를 공유하고 받아들여서 조기경보시스템 등과 연계시켜 활용하고 있다. 국내에서도 2000년대 초반 미국의 NVD나 CVE를 벤치마킹한 KCVE(Korea-CVE)의 구축을 계획했지만 현재진행상황에 대해서는 알 수 없으며, 외부로 공개되지 않는 취약점 DB가 존재[20]하는 등 취약점 통합관리체계나 통합된 DB가 미비한 실정이다. 미국의 경우, CSISP, CWIN에서 대외협력관련 조직체계를 갖추고 있고, 유럽은 ENSIA 중심으로 각국의 CERT 연계체계를 가지고 있으며, 일본의 경우 미국 및 영국과 공조체계 구축하여 대외협력체계를 구축하고 있다. 그러나 국내의 경우 정보보호 관련 기관마다 다른 체계 및 정책을 가지고 있어 국제협력 등을 통한 관리체계 등이 갖추어지지 않는다면 잘 구축된 취약점 DB나 관리체계가 없는 상황에서 모바일 오피스에서 일어날 수 있는 보안취약점과 침해사고 시 해당 정보에 대한 신속한 대응이 불가능하다.

## V. 안전한 모바일 오피스 구축을 위한 CERT 및 ISAC 개선방향

### 5.1 모바일 오피스 환경의 새롭고 특수한 범위에 대한 보안대응 마련

모바일 오피스를 구성하고 있는 환경 요소들에 대한 보안위협과 현황을 분석한 결과 기존의 기업의 보안인프라로는 해결할 수 없는 부분들도 존재함을 알 수 있었다. 앞서 지적한 기 구축된 보안장비 시스템이나 보안 인프라만으로는 커버할 수 있는 영역에 대한 한계가 존재하므로, 새롭고 특수한 범위에 대해서 나타날 수 있는 위협에 대해 예측하고 이에 대한 보안대응 방안을 강구하는 것이 필요하다. [표 4]는 Web 2.0에서 발생 가능한 취약점들이다.

[표 4] Web 2.0에서 발생 가능한 취약점

| 구분 | 취약점 |
|---|---|
| AJAX 관련 취약점 | 동일 근원지 정책 우회 |
| | 크로스 사이트 스크립트 |
| | 크로스 사이트 요청 변조 |
| | Open API에 의한 Mash-up취약점 |
| SNS 관련 취약점 | 개인정보 유출 가능 |
| | 인증관리 취약점 |
| | 업무 관련 정보 유출 가능 |
| | 신뢰성 관련 취약점 |
| | 피싱 |
| 기타 | XML Injection |
| | Xpath Injection |
| | JavaScript Injection |

예를 들어 모바일 오피스의 특징적인 구성요소로써 스마트폰 환경의 기반인 Web 2.0에서는 기존의 Web 1.0에서와 같은 보안문제점이 그대로 존재하기도 하지만, 새로운 취약점들 또한 나타나고 있다. 사용자 참여 등 개방성에 따른 보안 이슈와 Web 2.0에서 XML 데이터를 주고 받으며 사용자측의 많은 취약성을 갖는 자바스크립트가 주된 기술인 AJAX 등이 주로 사용되었기 때문에 기존의 Web 1.0보다 보안취약점에 대응하기 위하여 더 많은 노력을 기울여야 한다[20]. 해마다 증가하고 있는 새로운 모바일 악성코드를 분석하기 위해서 악성코드를 수집하는 기술이 선행되어야 하겠지만, 스마트폰 악성코드에 대한 대응준비가 부족한 국내 상황에서 정부나 연구기관의 경우는 허니팟 기반의 수집시스템, 웜뱃 프로젝트에 참여하고 있는 수집 시스템, 산·학계에서 연구되고 있는 수집시스템, 여러 제안기법 등을 이용해야할 것 있다. 취약점 통합관리체계나 모바일 오피스 관련 취약점 DB가 없는 국내의 상황을 고려한다면, 유럽이나 일본의 경우처럼 CERT와 ISAC을 통한 국제협력체제를 통해 신속한 모바일 오피스 보안취약점 정보를 공유하는 방안도 고려될 수 있다. 또한, 일반 사용자들의 모든 스마트폰의 데이터를 수집하기 보다는, 모바일 오피스에서 특히, 기업에 이미 존재하는 ESM 시스템 등 보안 모니터링 시스템을 활용하거나 무선 데이터 수집 및 활용방안은 모바일 오피스를 사용하고 있는 기업의 CERT를 활용함으로써 악성코드의 샘플 수집

및 분석, 채집기술에 대해 기여할 수 있다. 물론 모바일 오피스에서 사용하는 스마트폰은 개인적 용도로의 사용은 어느 정도 제한하되, 업무용으로 사용에 있어서 모바일 악성코드 수집에 대한 협조부분은 개인정보 법률상의 제약조건을 제외하면 다소 제한적이지만 기여를 할 수 있다고 판단된다.

### 5.2 유기적·통합적 보안관점에서 모바일 오피스 보안 대응을 위한 CERT와 ISAC

기업의 모바일 오피스 보안은 단순히 스마트폰이라는 디바이스 보안이 아니라 네트워크, 서버, 정책 등 각 영역별로 유기적으로 연계되어 있다. 모바일 오피스 보안 대응은 기술뿐 아니라 관련 법·제도, 기술표준화, 정책, 물리적·관리적 대응 등 각 영역에서 필요한 정보보호 요구사항들의 통합적 보안을 의미한다.

〔표 5〕 2004년, 2007년, 2010년 OWASP TOP10의 변화

| 순위 | 2004년 OWASP Top10 | 2007년 OWASP Top10 | | 2010년 OWASP Top10 | |
|---|---|---|---|---|---|
| 1 | 입력값 검증부재 | 크로스 사이트 스크립팅(XSS) | | 인젝션 (Injection) | |
| 2 | 취약한 접근통제 | 인젝션 취약점 | | 크로스 사이트 스크립팅(XSS) | |
| 3 | 취약한 인증 및 세션관리 | 악성파일 실행 | 신규 | 취약한 인증과 세션 관리 | |
| 4 | 크로스사이트 스크립팅 (XSS) | 안전하지 않은 직접 객체 참조 | | 안전하지 않은 직접 객체 참조 | |
| 5 | 버퍼 오버플로우 | 크로스 사이트 리퀘스트 변조 (CSRF) | 신규 | 크로스 사이트 요청 변조(CSRF) | |
| 6 | 삽입취약점 | 정보유출 및 부적절한 오류처리 | | 보안상 잘못된 구성 | 신규 |
| 7 | 부적절한 에러처리 | 취약한 인증 및 세션 | | 안전하지 않은 암호 저장 | |
| 8 | 취약한 정보 저장방식 | 안전하지 않은 암호화 저장 | | URL 접근제한 실패 | |
| 9 | 서비스 방해공격 | 불안전한 통신 | 신규 | 불충분한 전송계층 보호 | |
| 10 | 부적절한 환경 설정 | URL 접속 제한 실패 | | 검증되지 않은 리다이렉트와 포워드 | 신규 |
| 비교 | | 2004년 OWASP의 1,5,9,10삭제 | | 2007년 OWASP의 3,6번 삭제 | |

모바일 오피스 환경의 특징적 구성요소인 Web 2.0의 핵심은 디자인 패턴과 비즈니스 모델이며, 여전히 기존 Web 1.0에서와 같은 기술적인 보안 문제점이 존재한다. 〔표 5〕와 같이 2004, 2007, 2010년 발표된 'OWASP Top10'의 변화에서 보면 Web 1.0의 취약점이 계속해서 높은 순위에 올라있는 것을 확인할 수 있다. 실제로 Web 2.0에서 주로 사용하는 JavaScript와 관련한 취약점이 추가된 것을 제외하면, 기존 Web 1.0의 취약점이 Web 2.0에도 역시 그대로 적용되었으며 기존기술의 취약점들이 신기술의 공격에도 사용되고 있다[20]. 이는 신규취약점에 대한 대응이 기존 보안대응시스템선상에서 보안대책을 강구함과 동시에 특수성 및 유기적 연관성까지 함께 고려되어야 함을 의미한다고 볼 수 있다.

미국의 NIST에서 발표한 『Guide to Enterprise Telework and Remote Access Security』에서 재택근무와 원격접속에 대한 통합적 보안 가이드라인과 같이, 현재 모바일 오피스를 사용하거나 도입하고자 하는 기업들을 위한 모바일 오피스 보안 방법에 대해 아직까지 일반적이고 통합적 관점에서 대응책이나 보안 가이드라인이 제시되고 있지는 않다. 마이크로소프트사에서 발표한 『Architecture Guide for System Center Mobile Device Manager 2008』에서는 모바일과 이동 디바이스의 통합을 위한 표준을 제시하였다. 여기서 디바이스 사용 등록 및 추적관리, 모바일VPN, 그룹정책 어플리케이션, 소프트웨어 배포, 어플리케이션 인증 등의 디바이스 관리를 통해 중앙관리 콘솔에서 모니터링 및 통제를 할 수 있는 기능은 제시하고 있으나, 현재 모바일 오피스 보안 현황에서 MDM(Mobile Device Manager)이나 OMA (Open Mobile Alliance)와 같은 표준을 도입, 활용하는 가이드라인은 부재하며, 기존 시스템을 활용하여 모바일 오피스용 디바이스 통제 및 모니터링 시스템까지 서로 연계된 디바이스 보안에 대한 통합적 보안 맥락에서 제시된 바는 없다.

모바일 오피스를 사용하는 기업들의 보안 수준이나 최소한의 요건에 대한 필요성이 제기되며, 통합적 보안관점에서 모바일 오피스 보안은 CERT의 역할 중 침해사고 예방점검 기능을 활용한 보안 사항들에서 찾아볼 수 있을 것이다. 한국인터넷진흥원에서는 인터넷 전화(VoIP)와 같이 새로운 통신기술이 출현하고 발전하였을 때 보안 대응을 위한 예방 점검의 가이드라인으로써 'VoIP 침해사고 대응 안내서'를 내놓았다.

이러한 예방점검 리스트를 참고하고 앞서 분석한 모바일 오피스 환경의 보안위협과 대응을 기반으로 하여, 안전한 모바일 오피스 구축을 위한 '모바일 오피스 침해사고 예방 점검 리스트'로 내용을 구성해야할 것이다. 모바일 오피스 구축 보안가이드라인이 없는 실정에서 CERT라는 검증된 보안 시스템을 이용하여 모바일 오피스 침해사고 예방 점검 리스트를 적용한 모바일 오피스의 기술적, 관리적, 물리적 보호조치에 대한 예방 활동은 침해사고가 발생 가능한 요인을 파악하고 사전에 점검하여 발생 자체를 예방 및 대응을 신속하게 진행할 수 있는 기대효과를 가져올 수 있을 것이다. 또한 이는 모바일 오피스 구축을 위한 보안 가이드라인의 역할도 수행할 수 있을 것이다. 대부분의 기업들이 정보보호를 위해 각종 보안 솔루션을 도입함으로써 기본적 통제는 수행하고 있지만, 모바일 오피스와 같이 새로운 형태의 기술과 점점 더 복잡해지고 다양해지는 서비스들에 대해서는 기존의 네트워크 장비·DB·PC 보안의 기술적 보안뿐 아니라 이에 대한 관리를 포함하여 총체적인 입장에서 보안을 고려해야한다. 모바일 오피스 보안을 위한 예방활동측면에서 예방점검사항들을 체크해보고, 체크리스트는 최초 모바일 구축 시 한 번의 점검에 그치는 것이 아니라, 주기적으로 체크하고 그 결과를 보완하며 새로운 위협에 대한 보안대응방안도 업데이트하여 반영되는 과정이 필요하다.

### 5.3 모바일 오피스 보안을 위한 국제 협조체제의 역할로써 CERT와 ISAC

국내의 경우 정보보호 관련 기관마다 다른 체계 및 정책을 가지고 있어 국제 협력 등을 통한 관리체계 등이 갖추어지지 않는다면 국내에 모바일 오피스 관련 환경인 스마트폰이나 모바일 악성코드에 대한 취약점 DB가 없는 상황에서 침해사고 시 신속한 정보를 얻고 대응을 하기에는 어렵다. 국내에 모바일 오피스 취약점DB가 존재하지 않는다고 하더라도 기존의 CERT와 ISAC의 역할 및 기능 중 정보공유의 기능과 국제협력체계 역할 등의 시스템을 활용하거나 보완한다면, 모바일 오피스 위협에 대한 신속한 대응방안으로 이용할 수 있을 것이다. 그 예로 유럽의 경우, 자체 취약점 DB가 존재하지 않더라도 ENSIA중심으로 각국의 CERT연계체제를 통해 DB를 공유하고 받아들여 조기경보시스템 등과 연계시켜 활용하고 있다. 미국의 경우, CSISP, CWIN에서 대외협력관련 조직체계를 갖추고 있고, 유럽은 ENSIA 중심으로 각국의 CERT 연계체계를 가지고 있으며, 일본의 경우 미국 및 영국과 공조체계를 구축하여 대외협력체계를 구축하고 있다. 즉, 연계체계를 통해서 각 국가의 DB이든 조기경보체계든 정보공유를 통한 활용을 효과적으로 하기 위해서 별도의 기관이나 기구를 둔 셈이다. 이러한 맥락에서 국내의 CERT와 ISAC들은 국내 기관들 간의 연계와 협조 뿐만 아니라 국제적인 활동도 염두해 두어 모바일 오피스 관련 부족한 취약점 정보 등에 대해서 정보공유나 DB구축을 위해 시스템이나 정보체계를 구축해야 한다.

국내에서 조직된 '스마트폰 정보보호 민·관 합동대응반'은 스마트폰 애플리케이션 악성행위에 대한 판단기준을 마련 및 배포, 상호간 정보 공유 등을 통해 스마트폰 전용백신 개발 등에 활용, 모바일 악성코드 피해사례 및 대응 노하우 등을 공유, 민관 합동대응반이 참여하는 모바일 악성코드 대응 모의 훈련 등의 역할을 수행했다. 하지만 이러한 역할들은 일시적인 장애대응이 아니라 지속적으로 그 취지와 역할을 유지하면서 국제 공조와 국제 정보공유의 역할이 필요하며, 이러한 기능과 역할들은 모바일 오피스 관련하여 CERT와 ISAC에서 행해져야 한다. 모바일 오피스 관련 환경 요소들에 대한 보안부분을 추가하여 CERT와 ISAC에서 국제협조를 통해 효과적인 대응체계나 정보공유 활용체계를 수행해야 한다. 네트워크가 발달한 현대 사회에서 해외 사이버 공격은 국내에도 즉시 영향을 미치게 되므로 이러한 공격에 대한 조기대응을 위해서는 국가간 상시 정보공유가 필요하다. 국내의 부족한 모바일 보안에 대해, 정보공유와 대응체계 및 국제협력체제를 통해, CERT와 ISAC은 모바일 오피스 보안에 관련하여 예방의 기능인 선제적 사고대응협력체제와 국제 공조체계로써의 역할을 해야 할 것이다.

### 5.4 모바일 오피스 보안을 위한 주체별 협력체제의 공간을 열어주는 중심으로써 CERT와 ISAC

조나단 지트레인의 『The Generative Internet』에서는 컴퓨터에 end-to-end 네트워크가 더해지면서 혁신적인 "생성적" 플랫폼이 형성되고 우리는 이 플랫폼이 만들어낸 유익한 산물들을 누리고 있지만 유해한 것들에 대해 충분한 주의를 기울이지 않고 있다[39]고 지적한다. 2003년 오픈 프락시(open proxy)서버를 통한 대량 스팸메일 발송, 2004년 새

서(Sasser) 웜이 3일 만에 50만대의 컴퓨터 감염, 2003년 슬래머(Slammer) 웜이 특정제품의 MS 서버 90%를 15분 만에 감염시킨 사건 등은 점차 성장하는 패턴의 일부이고, U.S. CERT가 산출한 바와 같이 특정 시점을 기준으로 폭발적으로 확산되고 있다. 지트레인의 목적은 실제 변화에 대비하게 하는 것이며, 아직 모바일 오피스가 7·7 DDoS 사이버대란과 같은 폭발적인 변화를 일으킨 상황은 아니지만 그 가능성과 위협요인들에 대해서 앞서 충분히 살펴보았고 예측할 수 있으며 이에 대한 보안 대응방안을 강구해야한다.

모바일 오피스를 도입했거나 도입하고자 하는 기업들은 모바일 오피스 환경요소들이 빠르게 성장함에 따라 발생하는 위협들에 대해 대처하기 위한 보안 대응은 늦어지고 있고, 현재 국내의 CERT와 ISAC의 여건과 상황으로써는 급변하는 모바일 인터넷 환경에서 모바일 오피스라는 신규 보안위협에 사전 대비하고 안전하게 이용할 수 있는 보안대책을 마련하기는 어려운 실정이다. 보안대응시스템으로써 이미 검증된 CERT와 ISAC은 모바일 오피스 보안을 위한 협력체계를 구축하기 위한 장의 역할을 수행해야한다. 정부 및 연구기관, 모바일 오피스 기업, 백신개발업체 및 보안전문기업, 스마트폰 환경 관련 기업(단말제조사, 콘텐츠·앱 개발업체, 이동통신사, 스마트폰 제조사), 해외유관기관 등 주체별 역할 관계 속에서 이들 간의 협조체제를 구축하고 강화할 수 있는 시스템이나 장을 CERT와 ISAC이 수행해야 한다. CERT와 ISAC의 본연의 취지인 침해사고 대응과 정보공유 및 분석의 장으로써, CERT와 ISAC이 그 핵심적인 위치에서 그 공간과 시스템을 열어주어 모바일 오피스 기업 및 사용자들의 보안인식 제고와 더불어 지속적으로 대응능력을 강화해 나가야 할 것이다. 이러한 협력체계를 구축할 수 있는 CERT와 ISAC은 국가·공공기관이든 민관기관, 기업들의 비영리 협조체제이든 간에 상관없을 것이며, 각 주체별 안전한 모바일 오피스 구축을 위한 정보공유와 침해사고대응을 위한 적극적 참여와 지속적 지원협조로 이루어져야 한다. 'OWASP Top10'이나 'CWE/SANS Top25 Most Dangerous Software Errors'들이 협조체계의 중심에 있는 CERT와 ISAC에서 먼저 공개된다면 애플리케이션 개발업체에서는 보안성을 강화한 앱 개발, 모바일 오피스 기업의 특화된 프로그램 개발업체에서는 해당 보안성 고려, 플랫폼 제조에 있어서도 취약성 고려 등 각 주체들이 역할에 맞게 보안 대응방안이 선제적으로 강구될 수 있다. 또한, 스마트폰의 악성코드 수집의 어려운 점과 이를 분석할 수 있는 기술의 부족, 나날이 발전하는 스마트폰의 악성코드 취약점에 대해 자체적인 데이터를 축적하고 DB시스템을 갖추기에는 기업별로 한계가 있을뿐더러 국내의 CERT나 ISAC에서도 또한 한계를 가지고 있다. 모바일 오피스를 사용하는 기업들은 국내의 CERT와 ISAC에 협조와 참여할 수 있는 부분을 지원한다면 기업 입장에서는 모바일 오피스 악성코드와 침해사고 발생 시 협력체계와 빠른 정보를 이용하여 좀 더 신속한 대응이나 예방책을 받을 수 있을 것이고, 국내의 CERT와 ISAC은 모바일 오피스 보안과 관련하여 신속하고 질 높은 취약성 정보와 대응책을 제공해줄 수 있을 것이다.

협조 및 공조 체계의 핵심에 있는 CERT와 ISAC은 Knowledge Database, 사이버재난대응, 연구 및 개발DB, 기술력, 네트워크효과 등을 가져올 수 있으며 지속적 환경 조성과 운영이 활발히 이루어질 때 모바일 오피스 시장이 더욱 확대 되었을 때에는 모바일 오피스 보안시장의 확대 및 투자를 가져올 수 있을 것이며, 이러한 공조체계의 선제적인 역할은 모바일 응용의 확장으로 비용절감의 선순환을 유도하는데 의의가 있다.

## VI. 결 론

모바일 오피스라는 새로운 환경의 등장과 확산으로 인해 신규 취약점들이 나타나면서 이들 취약점을 이용한 사이버 침해, 기업정보 유출 등 보안위협이 발생하거나 발생할 가능성이 증대되고 있다. 그러나 국내에서는 모바일 오피스라는 편리성에 비해 보안 대응에 있어서 체계적 관리체계나 대응시스템을 제시하고 있지 못하고 있다.

본 논문에서는 모바일 오피스 환경을 이루고 있는 구성요소들에서 일어나거나 일어날 수 있는 위협들에 대해 분류하고 현 보안 대응현황을 분석한 후, 안전한 모바일 오피스 구축을 위한 효과적인 하나의 보안대응방안으로써 CERT와 ISAC의 역할을 중심으로 제안하였다.

국외의 사이버 침해사고 대응체계, 보안정보공유시스템, 취약점 관리체계 및 국제협력관계를 분석하여, 모바일 오피스 보안에 있어서 CERT와 ISAC의 기능을 활용하여 적용할 수 있는 효율적이고 안정화된 시스템을 가지고 있음을 도출하였다. 미국의 경우 모바일 보안이라는 분야가 CERT, ISAC, 취약점DB 시

스템에 포함되어 특수하고 새로운 범위에 대한 보안대응을 마련하고 있다는 점과 새로운 기술이 생겨날 때마다 별도의 DB나 관리체계가 아니어도 CERT와 ISAC의 공조체계나 국제협력관계를 통해서 이를 보완하고 선제적 대응체계를 마련할 수 있다는 시사점을 얻을 수 있었다.

모바일 오피스 보안이라는 것은 새로운 환경이지만 특수한 환경에 대한 보안위협대응방안 뿐만 아니라 기존 시스템과 인프라와의 연계성을 함께 고려해야 한다. 그리하여 통합적 맥락에서 예방적 차원의 보안대응 방안으로써 CERT에서는 '모바일 오피스 침해사고 예방점검 리스트'를 구성할 수 있을 것이다. 또한 모바일 오피스라는 새로운 환경에 대한 정형화된 보안틀을 제시하지 못하는 국내 상황에서 ISAC의 정보공유체제의 기능을 살려, 정부 및 연구기관, 모바일 오피스 기업, 백신개발업체 및 보안전문기업, 스마트폰 환경 관련 기업(단말제조사, 콘텐츠·앱 개발업체, 이동통신사, 스마트폰 제조사), 해외유관기관 등 주체별 역할분담과 협력 체제를 위한 정보공유의 장은 CERT와 ISAC에서 그 공간과 시스템을 열어주어야 한다. 그리고 이 공간과 시스템을 바탕으로 모바일 오피스 기업 및 사용자들의 보안인식 제고와 더불어 지속적으로 대응능력을 강화해 나가야 할 것이다.

본 논문에서 제시한 모바일 오피스 보안 강화를 위한 CERT와 ISAC의 역할들을 기반으로 향후에는 모바일 오피스 보안 강화를 위한 구체적인 정책마련, 세부적 도입방안 등에 대해서 연구될 필요가 있다. 또한, 모바일 오피스 보안 영역을 적용하고 있는 국외 CERT와 ISAC의 시스템 구축이나 정책의 구체적인 구현방법, 국제적인 공조체제의 실질절인 사례를 통해 모바일 오피스 보안 강화의 효율성 측정에 대한 연구가 필요할 것으로 보인다.

본 논문은 현재 국내에서 모바일 오피스라는 새로운 환경에 대한 정책적 통제나 규제 및 보안 틀을 제시하지 못하고 있는 상황에서 CERT와 ISAC이라는 기존의 보안 시스템의 침해사고대응과 정보공유라는 기능을 활용하여 기업의 안전한 모바일 오피스 구축을 위해 요구되는 요구사항을 반영하여 제시한 것에 의의가 있다고 할 수 있다.

## 참고문헌


[1] 노현영, 모바일 오피스 서비스 시장 현황 및 전망, SKY Venture VETA Report, 2010년 8월.

[2] 강민형, 김진성, 이준환, 정태수, 이준기, 모바일 빅뱅과 기업경영의 미래, 삼성경제연구소 CEO Information, 제760호, 2010년 6월.

[3] 인터넷한국일보, [사설]가계 짓누르는 통신료 빨리 인하를, 2011년 2월.

[4] 매일경제, 모바일 오피스 도입 기업 1년 새 16%→56% 껑충, 2010년 8월.

[5] 강영길, 윤종현, 이수원, 박인성, "전문가 의견 기반 사이버 침해 예측 방법론 연구," 한국정보과학회 가을학술발표논문집, 34(2D), pp. 112-117, 2007년 10월.

[6] 국가사이버안전센터, 2006년도 사이버 침해사고 사례집, 2007년 4월.

[7] 한국인터넷진흥원, CONCERT, 침해사고대응팀(CERT)구축/운영 안내서, 2010년 1월.

[8] 박광철, "'종합침해사고대응시스템'에서의 블랙리스트 추출방법과 관리방안에 관한 연구," 석사학위논문, 고려대학교, 2004년 12월.

[9] 통신정보공유분석협회, 통신 ISAC 역할정립 및 조직안정화를 위한 컨설팅 연구보고서, 2008년 8월.

[10] 강동호, 한진희, 이윤경, 조영섭, 한승완, 김정녀, 조현숙, "스마트폰 보안위협 및 대응기술," 전자통신동향분석, 25(3), pp. 72-80, 2010년 6월.

[11] 한국인터넷진흥원, 스마트폰 기반의 악성코드 수집/분석 플랫폼 개발을 위한 연구, 2010년 11월.

[12] 국회입법조사처, 모바일 악성코드 현황 및 개선방안, 이슈와 논점, 제 22호, 2010년 2월.

[13] 김기영, 강동호, "개방형 모바일 환경에서 스마트폰 보안기술," 정보보호학회지, 19(5), pp. 21-28, 2009년 10월.

[14] 한국정보화진흥원, 스마트폰과 모바일 오피스의 보안 이슈 및 대응 전략, CIO REPORT, 2010년 10월.

[15] 배근태, 김기영, "모바일 단말 보안 운영체제 기술 동향," 전자통신동향분석, 23(4), pp. 39-47, 2008년 8월.

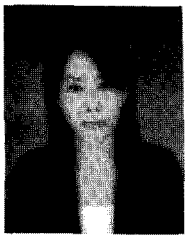
[16] 한국인터넷진흥원, 스마트폰 어플리케이션 마켓중심의 정보보호 대응방안 연구, 2010년 9월.

[17] 최은영, 김미주, 정현철, "스마트폰 보안강화를 위한 방안 연구," 한국인터넷정보학회 학술발표대회 논문집, 37(2B), pp. 781-785, 2010년 6월.

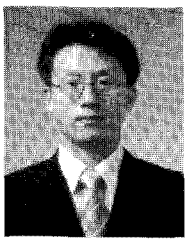
[18] 추연철, 최진영, "스마트 모바일 오피스 환경에서의 정보보호관리체계(ISMS)를 확장한 정보보호 모

형 연구," 한국정보과학회 학술발표논문집, 37(2B), pp. 95-99, 2010년 11월.
[19] Microsoft Corporation, Architecture Guide for System Center Mobile Device Manager, Oct 2008.
[20] 한국인터넷진흥원, 정보신기술 취약점 관리체계 구축(안), 2010년 8월.
[21] 김지연, 김진형, 김형종, 양종한, 이재근, "정보보호를 고려한 행정기관 FMC 도입 및 활성화 방안 연구," Internet and Information Security, 1(1), pp. 126-145, 2010년 5월.
[22] 방송통신위원회 보도자료, 스마트폰 보안위협, 민·관이 공동 대응한다, 2010년 1월.
[23] 김창주, "정보공유분석센터(ISAC)의 운영 현황과 향후 발전 방향 연구," 석사학위논문, 고려대학교, 2007년 6월.
[24] http://www.us-cert.gov/aboutus.html
[25] http://www.egc-group.org/index.html
[26] 국가정보원, 2009국가정보보호백서, 2009년 4월.
[27] 방송통신위원회 보도자료, Smart Korea 강국 도약을 위한 모바일 시큐리티 종합계획, 2010년 12월.
[28] Collin Mulliner, Giovanni Vigna, David Dagon, and Wenke Lee, "Using Labeling to Prevent Cross-Service Attacks Against Smart Phones," SIG SIDAR Conference on DIMVA(Detection of Intrusions and Malware & Vulnerability Assessment) 2006, LNCS 4064, pp. 91-108, Jul. 2006.
[29] 국회입법조사처, '7·7 DDoS사고' 대응의 문제점과 재발방지 방안, NARS현안보고서 제48호, 2009년 12월.
[30] 김익수, 정진혁, 이형찬, 이정현, "모바일 악성코드 분석 방법과 대응방안," 한국통신학회 논문지, 35(4), pp. 599-609, 2010년 4월.
[31] 김도승, "사이버위기 대응을 위한 법적과제 -미국의 사이버위기 대응체계 현황과 시사점을 중심으로," 방송통신정책, 21(17), 통권 470호, pp. 21-56, 2009년 9월.
[32] 김동진, 조성제, "국가DB기반의 국내외 보안취약점 관리체계 분석," Internet and Information Security, 1(2), pp. 130-137, 2010년 11월.
[33] http://cve.mitre.org/compatible/vulnerability_management.html
[34] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-4214
[35] http://www.us-cert.gov/cas/bulletins/pdf/SB09-152.pdf
[36] http://cwe.mitre.org/top25/archive/2010/2010_cwe_sans_top25.pdf
[37] http://www.owasp.org/index.php/Mobile#tab=Main
[38] http://jvndb.jvn.jp
[39] Jonathan L. Zittrain, The Generative Internet, 119 Harvard Law Review 1974, pp. 2009-2012, May 2006.

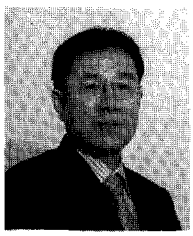
## 〈著者紹介〉



이 근 영 (Keun-Young Lee) 일반회원
1999년 2월: 숭실대학교 사학과 학사
2000년 5월~2001년 11월: 해커스랩 인텔리전스사업부 연구원
2002년 7월~2009년 2월: 어울림정보기술 보안기술부 선임연구원
2009년 4월~2009년 7월: 한국인터넷진흥원 정책개발단 연구원
2011년 8월: 고려대학교 정보보호대학원 석사
현재: 씨큐아이닷컴 재직 중
〈관심분야〉 정보보호정책, 정보법학, 스마트 보안, 융합기술보안, 네트워크 보안 등



박 태 형 (Tae-Hyoung Park) 일반회원
2002년 2월: 고려대학교 서양사학과 학사
2004년 2월: 고려대학교 행정학과 석사
2004년 4월~2008년 4월: 한국행정연구원 연구원
2011년 2월: 고려대학교 정보보호대학원 박사
현재: 고려대학교 정보보호대학원 정보보호연구원 연구교수
〈관심분야〉 정보보호정책, 전자정부, 정보화, 성과관리, 성과평가



임 종 인 (Jong-In Lim) 종신회원
1980년 2월: 고려대학교 수학과 졸업
1982년 2월: 고려대학교 수학과 석사
1986년 2월: 고려대학교 수학과 박사
현재: 고려대학교 정보보호대학원 원장
〈관심분야〉 정보법학, 디지털포렌식, 개인정보보호, 사이버전, 융합기술보안 등