석 사 학 위 논 문

軍내 이동전화 통제에 관한 연구

-모바일단말관리 시스템을 중심으로-

2013년

한성대학교 국방과학대학원

안 보 전 략 학 과

군 사 전 략 전 공

서 경 진

석 사 학 위 논 문
지도교수 구형회

軍내 이동전화 통제에 관한 연구

-모바일단말관리 시스템을 중심으로-

Study of control over mobile phones in military

-Focused on mobile device management system-

2012년 12월 일

한성대학교 국방과학대학원

안 보 전 략 학 과

군 사 전 략 전 공

서 경 진

석 사 학 위 논 문
지도교수 구형회

軍내 이동전화 통제에 관한 연구

-모바일단말관리 시스템을 중심으로-

Study of control over mobile phones in military

-Focused on mobile device management system-

위 논문을 안보전략학 석사학위 논문으로 제출함

2012년 12월 일

한성대학교 국방과학대학원

안 보 전 략 학 과

군 사 전 략 전 공

서 경 진

서경진의 안보전략학 석사학위논문을 인준함

2012년 12월 일

심사위원장 _____ 인

심 사 위 원 _____ 인

심 사 위 원 _____ 인

국 문 초 록

軍내 이동전화 통제에 관한 연구
-모바일단말관리 시스템을 중심으로-

한성대학교 국방과학대학원
안보전략학과
군사전략전공
서 경 진

군은 2012년 '상용 우수 IT 신기술 국방적용 시범사업'의 일환으로 모바일 기기 통제체계 구축 사업을 추진하고 있다. 이 사업의 핵심은 모바일단말관리 시스템의 도입으로, 이를 위해 군은 2012년 8월부터 국방부 본관과 합동참모본부 신청사에서 시범사업을 진행 중이다.

2012년 9월말 현재 54,274,905명의 이동전화 사용자 중 스마트폰 사용자가 30,876,600명을 차지하고 있고, 군 이동통신에서도 LTE특수요금제와 같은 스마트폰 요금제의 신설로 인해 영내 스마트폰 반입은 더욱 증가하고 있는 현실이다.

스마트폰은 개방성, 휴대성, 다양한 접속경로를 통한 연결 편리성과 같은 특성을 갖고 있으나 이는 악성코드의 손쉬운 유포, 분실 시 개인정보의 유출가능성, 보안소프트웨어에 대한 실시간 감시가 불가능하다는 한계점으로 작용하게 되는바 PC에 비해 상대적으로 보안의식이 미약한 사용자와 결부하여 보안에 있어 여러 심각한 문제들을 발생시키고 있다.

그 결과 오늘날 국내 스마트폰 OS의 87%를 차지하고 있는 안드로이드 운영체제에 대한 악성코드 발견이 급증하고 있다는 현실은 군사보안적 측면에서 영내 스마트폰 반입의 증가는 필연적으로 보안침해사고가 발생할

가능성을 높인다고 할 수 있겠다.

따라서 이러한 점에서 군의 모바일단말관리 시스템 도입추진은 스마트폰의 영내반입으로 인한 군사보안 침해가능성에 대해 기존 특정구역 출입시 스마트폰을 회수하는 단순한 대책에서 벗어나 군 내 모든 구성원을 일괄적으로 통제할 수 있다는 점에서 유효한 기술적 통제방안이라 할 수 있다.

그러나 최근 LG전자의 모바일단말관리 시스템 도입 간 발생한 개인 사생활 침해논란과 같이 군 내 모바일단말관리 시스템의 전면 도입 간 개인 사생활에 민감한 세대인 초급간부 집단을 중심으로 사생활침해에 대한 반발이 발생할 가능성이 있으며, 모바일단말관리 시스템의 적용을 회피하기 위해 타인명의의 스마트폰을 개통하여 임의 반입하는 사례가 발생할 수 있다.

본 연구는 위와 같이 군내 모바일단말관리 시스템의 도입 간 예상되는 한계점에 대해 기술적 측면에서 이미 민간에서 스마트폰의 NFC기능으로 기존 RFID출입증을 대체하여 운용하고 출입과 동시의 스마트폰의 모바일단말관리 시스템을 작동시킨다는 점에서 착안하여 군의 RFID영문출입통제와 스마트폰간의 연계를 통한 모바일단말관리 시스템의 자연스러운 보급을 제안하고, 이러한 일련의 통제가 기본권 제한의 논란을 발생시킬 수 있다는 점에서 헌법상 명시된 바와 같이 법률에 의한 통제목적·근거·적용대상 및 절차 등을 마련할 필요성을 검토하였다. 그리고 보안사고 중 상당한 수준을 차지하고 있는 상용정보통신장비에 대한 사례위주의 군법교육과 함께 모바일단말관리 시스템의 신속하고 성공적인 보급을 위해 적용대상에 대한 지속적인 추적·관리가 용이한 군 이동통신으로의 유인이 필요하다는 점을 인식하고 이에 경제적 요인에 의한 유인방안과 같은 일련의 대안을 검토 및 제안하고자 한다.

【주요어】 군사보안, 군 이동통신, 모바일단말관리

목 차

제 1 장 서 론 ····· 1

제 1 절 연구의 목적 ····· 1
1. 안보환경의 변화 및 시사점 ····· 1
2. 연구의 목적 ····· 3

제 2 절 연구의 범위 및 방법 ····· 4

제 2 장 모바일단말관리 시스템의 도입에 관한 일반적 고찰 ····· 7

제 1 절 스마트폰의 개념과 특징 ····· 7
1. 스마트폰의 개념 ····· 7
2. 스마트폰의 특징 ····· 7

제 2 절 모바일단말관리 시스템의 개념과 주요 기능 ····· 9
1. 개념 및 등장배경 ····· 9
2. 주요기능 및 활용형태 ····· 10

제 3절 軍 RFID영문출입통제 사업 ····· 14
1. RFID의 개념・특성 ····· 14
2. RFID기술의 군사적 활용 ····· 16

제 4 절 NFC의 개념과 특징 ····· 19
1. 개념 ····· 19
2. 특징 및 활용전망 ····· 19

제 5 절 선행연구 ····· 22

제 3 장 스마트폰이 군사보안에 미치는 영향 ····· 24

제 1 절 스마트폰의 사용 확산과 보안취약점 요소 ····· 24
1. 스마트폰의 사용 확산 ····· 24
2. 스마트폰의 특성과 보안위협 ····· 26
3. 스마트폰의 악성코드 피해사례 및 유형 ····· 34

제 2 절 스마트폰이 군사보안에 미치는 영향 ····· 40
1. 군 이동통신의 특성 ····· 40
2. 기능별 군사보안침해 가상시나리오 ····· 41
3. 소결론 ····· 43

제 4 장 軍내 모바일단말관리 시스템의 도입 간 예상 한계점 ····· 46

제 1 절 모바일단말관리 시스템의 도입현황 ····· 46
1. 민간분야 ····· 46
2. 군사분야 ····· 47
3. 검토 ····· 48

제 2 절 도입 간 예상되는 한계점 ····· 48
1. 개인프라이버시 침해우려로 인한 사용자의 거부감 ····· 48
2. 타인명의의 스마트폰 사용에 대한 통제 불가 우려 ····· 51
3. 소결론 ····· 52

제 5 장 軍내 모바일단말관리 시스템의 도입 간 예상 한계점의 해결방안 54

제 1 절 전제조건 ····· 54

제 2 절 기술적 해결방안 ····· 54

1. 스마트폰의 NFC 기능과 RFID출입통제 시스템의 연계 ····· 54

제 3 절 제도적 해결방안 ····· 57

1. 법적 근거의 마련 ····· 57

2. 군 이동통신으로의 유인 ····· 58

3. 내부 컴플라이언스 ····· 60

제 6 장 결 론 ····· 66

【참고문헌】 ····· 68

【 표 목 차 】

[표 2-1] PC, 피쳐폰 및 스마트폰의 특징 비교 ····· 8
[표 2-2] 매체별 인식능력 비교 ····· 14
[표 2-3] 군 RFID출입통제시스템의 구축방안 ····· 17
[표 2-4] NFC 기반 주요 응용서비스 ····· 21
[표 2-5] 군용 RFID의 주파수와 NFC 주파수간 비교 ····· 22
[표 3-1] 국내 스마트폰이용자 비율 변화 ····· 25
[표 3-2] 모바일단말의 특성과 보안위협 ····· 27
[표 3-3] 스마트 시대의 정보 보안 위협 10가지 ····· 29
[표 3-4] 주요 위협요인에 대한 대응방안 ····· 30
[표 3-5] 안드로이드 운영체제 상위 11대 악성코드의 진단명 및 특징 ····· 37
[표 3-6] 악성코드 제작자 측면에서 본 안드로이드의 매력 ····· 38
[표 3-7] 스마트폰의 주요기능과 배치되는 군사보안규정 ····· 45
[표 4-1] 민간분야의 모바일오피스 도입사례 ····· 46
[표 5-1] 군 RFID영문출입통제시범사업의 성과지표 ····· 55
[표 5-2] 금융회사의 통제방안 구분 ····· 62
[표 5-3] 금융회사의 모바일단말 모범규준 ····· 63

【 그 림 목 차 】

<그림 2-1> 모바일단말관리 서비스의 주요 기능 ····· 11
<그림 2-2> RFID시스템의 구성 ····· 15
<그림 2-3> 스마트폰 NFC 기능을 활용한 결제 ····· 20
<그림 3-1> 우리나라의 휴대폰과 데스크톱간 점유율 변화 ····· 24
<그림 3-2> 우리나라의 모바일 운용체제(OS) 이용현황 비교 ····· 26
<그림 3-3> 리패키징 기법 ····· 33
<그림 3-4> 안드로이드 악성코드 샘플 접수량 ····· 34
<그림 3-5> 애플리케이션의 설치 간 악성코드에 감염된 경우와 비교 ····· 39

제 1 장 서 론

제 1 절 연구의 목적

1. 안보환경의 변화 및 시사점

국가안보란 본래 외부의 직접적 위협으로부터 국가의 안전을 확보하는 것을 의미한다. 이는 국가 간 자국의 이익달성을 그 목적으로 하는 것으로서 전통적으로는 전쟁이 국가위협이었다.[1)]

그러나 최근 변화된 안보환경은 정치, 사회, 군사 등 다양한 국가 간 갈등요소에 있어 전통적인 무력충돌인 전쟁만을 유일한 해결책으로 보지 않고 새로운 기술의 발견을 통한 다양한 공격 수단을 마련하고 있는 특징이 있다. 이런 새로운 기술의 대표적인 예는 이란의 우라늄농축시설에 대한 '스턱스넷'[2)] 공격을 들 수 있다.

이러한 사실이 주는 시사점은 국가이익의 증진 및 보호역할을 수행하고 있는 군이 국가안보의 핵심적인 기능을 수행한다고 할 때, 국가안보의 보장을 위해서는 지속적이고 성공적인 군사보안의 유지가 요구되고 이는 각종 기술의 발달에 대응할 수 있는 다양한 수단의 마련을 통해 달성할 수 있다고 할 수 있다는 것이다.

통상적으로 보안에 있어 기밀보호확률은 각개 구성원의 기밀보호확률을 서로 곱한 값으로 본다고[3)] 할 때, 이는 취급당사자 중 어느 한 사람이라

---

1) 조영갑(2006), 『국가안보학』, 서울 : 선학사, pp.206-207.

2) 스턱스넷(Stuxnet)은 2010년 6월에 발견된 웜 바이러스로 마이크로소프트 윈도를 통해 감염되어, 지멘스 산업의 SCADA 시스템만을 감염시켜 장비를 제어하고 감시하는 특수한 코드를 내부에 담고 있다. 이러한 스턱스넷의 여러 변종이 이란에 있는 5개 시설에서 발견되었으며, 지멘스는 이 웜이 자사의 고객에게 어떤 피해도 끼치지 않았으나, UN 안보리 결의안 1737호에 의해 사용 금지된 지멘스 제품을 비밀리에 입수하여 사용중인 이란 핵시설만이 피해를 입었다고 발표했다는 점에서 웜의 공격목표는 이란의 우라늄 농축 시설로 보인다. 이 공격에는 이스라엘과 미국이 참여한 것으로 추정된다.

3) 박해종(2012), "군 RFID출입통제시스템을 이용한 이상징후 탐지방법", 수원 : 아주대학교 석사학위논문, p.38. : 통상 기밀 인지자의 기밀 보호 확률은 "갑", "을", "병"3인이 기밀을 알고 있다고 할 때 기밀을 누설하지 않을 확률이 "갑"은 0.9, "을"은 0.8, "병"은 0.7이라고 가정

도 기밀을 누설하는 경우 다른 사람의 누설여부와 관계없이 누설된 것이란 점[4]을 고려하여 기밀보호를 위해 기밀보호확률을 향상시킬 수 있는 방법을 강구해야 하는데 가장 손쉬운 것은 기밀을 인지할 수 있는 인원을 최소화하는 것이다.

그러나 많은 수의 인원들이 다양한 군사보안 객체를 취급하는 군사보안의 특성상 취급인원의 최소화는 실현이 불가능하다는 점에서 보안 취급자 개인의 보안침해요소를 줄이려는 노력 및 기술적 방안의 마련이 차선책이 될 것이다.

개인의 보안침해요소를 줄이려는 기술적 방안 마련의 일환으로 항시 휴대하는 휴대폰에 대하여 살펴본다면 다음과 같다. 예전에 국가정보원장이 CDMA의 도·감청이 가능하다고 인정[5]한 바와 같이 도·감청이 휴대폰에 있어 주요 군사보안 이슈였다면 최근에는 일반 PC와 비슷한 사양을 갖춘 스마트폰의 등장으로 인하여 뒤에서 살펴볼 내용과 같이 차원이 다른 이슈를 가져올 수 있기에 원천적 수준에서 군의 휴대폰에 대한 보안대책이 재검토되어야 한다.

특히 이러한 대책마련은 2009년 iPhone이 국내에 출시된 이후 방송통신위원회에 따르면 2012년 9월 현재 54,274,905명의 이동전화 사용자 중 스마트폰 사용자가 30,876,600명에 이르렀고, 군 이동통신에서도 LTE특수요금제와 같은 스마트폰 관련 요금제가 신설되면서 영내 반입되는 휴대폰 중 스마트폰의 비중이 점차 증가하고 있다는 점에서 최우선 과제가 되어야 할 것이다.

이에 최초로 등장한 대응책은 스마트폰을 영내 혹은 주요보안구역에 반입하지 않는 반입통제로 퀵윈(quick win)전략이라 한다. 이는 즉시 적용가능하지만, 단순한 반입통제에 불과하다는 점에서 보안측면의 실효성은 상당히 낮은 수준이라 하겠다.

그렇다면, 군사보안측면에서 실효성 있는 방안을 살펴보기에 앞서 군이

한다면 “갑”, “을”, “병”3인에 의한 기밀 보호확률은 0.9×0.8×0.7= 0.054로 “갑”, “을”, “병”이 기밀을 보호할 확률은 50.4%가 된다.

4) 박해종(2012), 전게논문, p.38. : 이 경우 기밀보호확률이 가장 높은 갑이 누설할 경우(기밀보호확률이 0이 되는 경우이다) 기밀보호확률은 0×0.8×0.7=0 으로 기밀이 누설된다.

5) 조선일보, 2003년 4월 11일, A2면

스마트폰의 반입[6]에 대해 암묵적으로 허용하고 있다는 점과, 저격수용 탄도계산어플리케이션과 같은 스마트폰과 군사용 앱을 접목시켜 활용방안을 모색하는 미국 의 사례와 우리나라도 최근 군사용 앱을 개발하고 이를 활용할 군 전용 스마트폰 시범 사업을 추진하는 가운데[7] 군사보안을 강화하기 위해 반입되는 스마트폰에 대해 모바일단말관리 시스템의 도입을 추진하는 점[8]등을 종합해보면 스마트폰의 전면적 반입통제 및 사용제한이 아닌 스마트폰의 활용을 전제로 일정한 수준의 제한적 통제방안으로 접근해야 한다는 점을 인식할 수 있을 것이다.

그러나 이러한 대응책(모바일단말관리)의 시행에 있어 영내에 반입되는 모든 스마트폰에 대해[9] 강제적으로 통제방안을 적용할 수 있는 법적근거는 마련되어 있는지, 강제적인 분위기나 제제가 예상되는 이러한 추진과정은 2012년 초 종북애플리케이션 삭제 지침에서와 같은 개인의 프라이버시 침해 논란 등이 발생하게 될 경우 대응방안 및 논리와 기술적 차단(통제) 혹은 정책적인 유인책은 마련되어 있는지가 의문이다.

2. 연구의 목적

본 연구는 군(軍)내 스마트폰 반입에 있어 스마트폰의 특성인 보안 취약점과 이를 이용한 각종 악성코드의 출현이 군사보안에 영향을 미칠 가능성에 주목하여 이에 대응하기 위해 군이 최근 도입을 추진하고 있는 모바일단말관리(MDM : Mobile Device Management)시스템의 도입과정에서 예상되는 한계점과 그 해결방안을 살펴봄으로서 이의 성공적인 도입을 통한 군사보안 및 국가안보에 기여하기 위함이다.

---

6) 본 연구에서는 영내 스마트폰의 반입이 간부에 의해 발생한다고 가정하였으며, 본 연구에서 등장하는 '사용자'는 별도언급이 없는 경우 스마트폰을 사용·반입하는 간부를 지칭하는 것이다.

7) 국방일보, 2012년 7월 16일, 2면

8) 국방일보, 2012년 4월 23일, 2면

9) 영내에 반입되는 스마트폰을 군 이동통신에 가입된 사용자 명의의 스마트폰, 군 이동통신에 가입하지 않은 사용자명의의 스마트폰, 그리고 타인명의의 스마트폰으로 구분한다면, 이러한 군의 스마트폰에 대한 통제는 영내에 반입되는 '모든'스마트폰에 대하여 일괄적으로 적용되어야 그 실효성을 확보 할 수 있을 것이다.

따라서 본 논문에서는 스마트폰의 통제방안 구축 시 예측가능한 수준의 문제점에 대하여 민간의 사례 등을 통해 살펴보고, 그 해결방안을 기술적·제도적 측면으로 구분하여 도출 및 제안함으로서 군내 이동전화 통제의 실효성 증대측면에 기여하고자 한다.

제 2 절 연구의 범위 및 방법

스마트폰은 우수한 성능을 갖춘 기기이고 그 성능을 기반으로 한 다양한 앱을 통해 사용자는 활용도를 극대화 할 수 있다. 그러나 다양한 앱의 제작을 위해 상당부분이 공개되어 있는 OS 와 접근성이 갖는 근본적 한계와 검증되지 않은 앱, 그리고 24시간 연결되어 있는 네트워크로부터 유입 가능한 악성코드는 스마트폰의 보안을 취약하게 하는 주요요인으로 작용한다.

물론 스마트폰의 보안취약성이 곧바로 군사보안 침해라는 결과를 가져온다고는 할 수 없다. 그러나 최근 영내 스마트폰의 반입이 기하급수적으로 증가하고 있다는 점과 앞으로 살펴볼 내용과 같이 군 이동통신이 갖는 다양한 특성들은 적성세력에 의해 군 이동통신 사용자를 직접 목표로 하여, 사용자가 스마트폰을 영내에 반입하는 경우 이를 군사보안 침해의 도구로 활용할 수 있다는 점과, 적성세력에 의해 포섭된 예비역 중사[10]와 자발적으로 북한공작원과 접촉하여 공작교육을 받고 동해안 경계철책 감시카메라의 기밀을 넘기는 등 간첩행위에 동조한자[11]의 사례가 다시 발생할 경우 이러한 자들이 스마트폰을 직접적인 군사보안 침해의 수단으로도 활용할 수 있다는 점[12]에서 스마트폰으로 인한 군사보안 침해가능성은 다양한 측면으로 고려해야 할 사안이라 하겠다.

따라서 본 연구에 있어서는 스마트폰이 갖는 근원적인 보안취약성과 이

10) 북한 女공작원의 회유로 인해 자진 월북하여 정보기관 관계자에게 현역 복무 간 알게 된 군사기밀을 넘기고 같이 근무했던 현역군인들에게 월북을 권유한 예비역 부사관의 사례
11) 중앙일보, 2012년 9월 5일, 19면
12) 현역 군인과의 접촉, 영내 출입 시 스마트폰의 무단 반입 등을 통한 군사보안의 침해우려 등

를 대상으로 한 악성코드의 출현이 영내 스마트폰 반입의 증가란 현실과 맞물려 필연적으로 군사보안 침해 가능성을 증대시킬 것이라고 전제 하였다.

군은 이러한 군사보안 침해에 대응하기 위해 2014년까지 사단급 이상 부대로 단계적인 보급완료를 목표로 모바일단말관리 시스템을 시범사업으로 추진하고 있는 중이나, 아직 이와 관련된 문제점 및 개선방안에 대하여 도출된 연구결과는 없다.

따라서 이에 대해 민간의 사례 등을 통해 발생이 예측가능한 문제점들을 살펴보고, 그 해결방안을 도출하기 위해 본 연구의 대상을 다음과 같이 구분하였다.

첫째, 스마트폰이 갖는 보안취약성 요소는 무엇인가? 둘째, 스마트폰의 보안취약성과 군 이동송신의 특성에 의해 군사보안은 어떻게 침해받을 수 있는가? 셋째, 군에서 도입이 진행 중인 모바일단말관리 시스템은 어떠한 특성을 갖고 있으며 예상되는 한계점은 무엇이고 이를 해결하기 위해 어떤 수단을 강구해야하는가?

이에 대한 결론을 도출하기 위해 앞서 제1장에서 살펴본 바와 같이 본 논문의 연구 목적은 군 내 스마트폰 반입으로 인한 군사보안상의 위험성을 살펴보고, 이에 대응방법으로 시범사업이 진행 중인 모바일단말관리 서비스에 대하여 발생가능한 문제점을 미리 도출하고 기술적·정책적 대응방안을 제안함으로서 모바일단말관리 서비스 사업의 성공적인 도입과 이를 통하여 군사보안 대비태세 완비, 나아가 국가안보에 기여하고자 함이다.

이를 위해 모바일단말관리 서비스의 시행예정시기까지 사용(예정)가능한 기술들을 중심으로 연구하였고, 본 연구와 연관된 개념인 RFID·NFC·모바일단말관리 시스템 등에 관하여 제2장을 통해 소개해두었다. 그리고 제3장을 통해, 스마트폰으로 인한 군사보안 침해우려에 대하여 2009년 이후 기하급수적으로 증가하는 스마트폰 이용자와 더불어 영내 스마트폰 반입의 허용으로 인한 스마트폰 반입확산현황을 인식하고, 스마트폰이 갖는 근본적인 보안취약성과 이를 악용한 각종 악성코드가 제작되는 현실에서 적성

세력이 군 이동통신의 특성상 군 이동통신 사용자를 직접 목표로 스마트폰의 특정기능을 제어할 수 있을 정도로 높은 수준의 보안 침해가 가능할 것이라 가정하여 현재 혹은 가까운 장래에 스마트폰으로 인한 군사보안 침해가 가능하다고 판단하였으며 이에 대해 크게 스마트폰의 반입 금지와 기술적 통제의 대안이 있으나, 반입통제정책은 무의미한 수준의 대안이라 할 수 있어 민간분야에서의 모바일단말관리 서비스와 같은 기술적 통제방안을 군 이동통신에 도입하기 위한 필요성이 있다고 보았다.

그러나 제4장 및 제5장의 내용과 같이 모바일단말관리 서비스의 도입 간 발생이 가능한 개인 프라이버시 침해에 따른 반감을 극복하고 타인명의 스마트폰의 반입과 같은 경우에도 전면적으로 적용할 수 있어야 군사보안이란 목표를 달성할 수 있을 것인바, 이를 위하여 우선 모바일단말관리 서비스를 적용할 수 있는 근거와 그 한계를 법적으로 명확히 명시하여야 하며, 기술적으로는 영문출입통제 시스템과의 연계, 정책적으로는 군 이동통신으로의 유인책을 통하여 보다 원활한 사용자 관리 및 악성코드 유포 등에 대한 효율적 대처를 하여야 한다고 보았다.

마지막으로 제6장에서는 본 연구를 통하여 제시된 대안들을 종합하여 결론을 도출하였다.

제 2 장 모바일단말관리 시스템의 도입에 관한 일반적 고찰

제 1 절 스마트폰의 개념과 특징

1. 스마트폰의 개념

스마트폰의 사전적 정의를 살펴보면 다음과 같다[13].

스마트폰은 휴대폰과 개인휴대단말기(PDA : Personal Digital Assistant)의 장점을 결합한 것으로, 휴대폰 기능에 일정관리, 팩스 송·수신 및 인터넷 접속 등의 데이터 통신기능을 통합시킨 것이다. 가장 큰 특징은 완제품으로 출시되어 주어진 기능만 사용하던 기존의 휴대폰과는 달리 수백여 종의 다양한 애플리케이션(응용프로그램)을 사용자가 원하는 대로 설치하고 추가 또는 삭제할 수 있다는 점이다.

무선인터넷을 이용하여 인터넷에 직접 접속할 수 있을 뿐 아니라 여러 가지 브라우징 프로그램을 이용하여 다양한 방법으로 접속할 수 있는 점, 사용자가 원하는 애플리케이션을 직접 제작할 수도 있는 점, 다양한 애플리케이션을 통하여 자신에게 알맞은 인터페이스를 구현할 수 있는 점 그리고 같은 운영체제(OS)를 가진 스마트폰 간에 애플리케이션을 공유할 수 있는 점 등도 기존 휴대폰이 갖지 못한 장점으로 꼽힌다.

2. 스마트폰의 특징

스마트폰은 최근 LTE망의 보급과 WiFi망의 확대로 고속 무선인터넷이 가능해지고, 기기자체의 성능이 비약적으로 발전함에 따라 모바일오피스와 같은 새로운 업무형태의 등장과 각종 어플리케이션의 등장으로 인해 삶에

13) 두산백과사전의 스마트폰의 정의, 네이버 지식백과(http://terms.naver.com/entry.nhn?cid=2000000000&docId=1199937&mobile&categoryId=200000749)

효율성을 더하고 있다.

이러한 스마트폰의 특징을 살펴봄에 있어 스마트폰이 PC에 버금가는 성능을 갖고 있지만 그 근간이 휴대폰(피쳐폰)이라는 점에서 아래의 [표 2-1]을 통해 PC, 피쳐폰과 구별되는 특징을 찾아보도록 하자.

[표 2-1] PC, 피쳐폰 및 스마트폰의 특징 비교

구 분	PC(노트북)	피쳐폰	스마트폰
OS	· 개방형 플랫폼 · MS Windows가 90%이상 차지 사실상 독점	· 폐쇄형 플랫폼 · 전용 OS · 제조사별 개별 탑재	· 개방형 플랫폼 · 범용 OS · 다수의 범용 OS가 존재
써드파티 (3rd party) 애플리케이션	· 다양한 애플리케이션 다운로드 및 설치 가능 · 누구나 제작, 배포, 설치 가능 · 커스터마이징 가능	· 단말 벤더에 종속된 애플리케이션만 설치 가능 · 모바일 플랫폼 표준규격(위피 : WIPI) 기반에서 해당 통신사만 탑재 가능 · 커스터마이징 불가	· SDK(소프트웨어 개발 키트) 공개에 따른 써드파티 개발자의 애플리케이션 개발 및 공유 가능 · 누구나 제작, 배포, 설치 가능 · 커스터마이징 가능
인터넷 접속환경	· 유무선 네트워크	· 2G, 3G 네트워크 · CDMA, WCDMA, HSPA	· 3G, 4G, LTE · WCDMA, HSPA, WiFi, Bluetooth, PC Sync
사용시간	· 인터넷 또는 문서작업 등의 필요한 시간에만 사용 후 전원 끔 · 전원 켠 상태에서 사용자의 시선을 벗어나는 시간이 짧음	· 항상 전원 켜진 상태로 이용 · 전원 켠 사애에서 사용자의 시선을 장시간 벗어나는 것이 가능	· 항상 전원 켜진 상태로 이용 · 전원 켠 상태에서 사용자의 시선을 장시간 벗어나는 것이 가능
주요 H/W	· 프로세스 : 2.4GHz · 저장용량 : ~500GB · 디스플레이 : ~ 18.4인치(노트북 기준)	· 프로세스 : 1.5GHz · 저장용량 : ~32GB · 디스플레이 : ~ 4인치	· 프로세스 : 1GHz · 저장용량 : ~500GB · 디스플레이 : ~ 18.4인치

출처 : 유길상(2011), 고려대학교 석사학위논문, pp.7-8.

이러한 비교를 통해 살펴볼 때 스마트폰은 피쳐폰과 달리 커스터마이징[14]이 가능하다는 점(다양한 네트워크의 선택적 지원 및 다양한 애플리

케이션의 개발을 통한 활용가능성)에서 개방성과 PC와 달리 항시 휴대 가능하고 연속사용시간 및 장기간 대기가 가능하다는 점에서 높은 휴대성 및 이동가능성을 가지지만 PC와 피쳐폰의 중간에 위치하는 수준의 성능이란 점에서 저성능이란 한계를 갖는다는 점을 살펴볼 수 있다.

제 2 절 모바일단말관리 시스템의 개념과 주요 기능

1. 개념 및 등장배경

모바일단말관리 시스템은 일반인에게는 다소 생소한 개념으로 이는 기업들이 스마트폰 확산추세에 발맞춰 모바일오피스를 도입하는 가운데 이를 관리하기 위해 도입한 것[15]으로서 휴대폰에 대한 관리와 업무시간 중 사용에 대한 통제로부터 비롯되었다고 할 수 있다.

1) 휴대폰에 대한 관리[16]

기업은 모바일오피스를 도입하기 위해 스마트폰을 구입하는 단계에서부터 '관리'에 대하여 고려하고 대안을 찾을 필요가 발생하였다. 이러한 '관리'는 업무용 스마트폰을 구입하여 폐기할 때까지 애플리케이션을 배포. 업그레이드하고 불필요한 애플리케이션을 삭제할 수 있어야 하며 안정적인 서비스를 제공하기 위하여 품질을 모니터링 하는 등의 업무를 의미한다. 기업의 경우 모바일오피스의 도입·운영 간 관리해야 할 스마트폰의 대수가 적게는 수백 대에서 1,000대 이상이기 때문에 전문적인 솔루션의 필요성이 대두되었고, 이를 위해 모바일단말관리 시스템이 등장하게 되었다.

---

14) 생산업체나 수공업자들이 고객의 요구에 따라 제품을 만들어주는 일종의 맞춤제작 서비스를 말하는 것으로, '주문 제작하다'라는 뜻의 customize에서 나온 말이다. 최근에는 IT산업의 발전으로 개발된 솔루션이나 기타 서비스를 소비자의 요구에 따라 원하는 형태로 재구성•재설계하여 판매하는 것으로 그 의미가 확장되었다.

15) 임팩트(2012), 『스마트워크 모바일오피스 실태와 전망』, 서울 : 임팩트, p.41. 참고하여 재정리

16) 유길상(2011), "금융시장 건전성을 해치는 모바일단말 위협에 대한 대응방안", 서울 : 고려대학교, 석사학위논문, pp.58-59. 참고하여 재정리

이러한 통상적인 '관리' 측면에 있어 모바일단말관리 시스템이 요구되는 가장 큰 이유는 분실가능성이다. 이는 휴대폰이 갖는 이동성에 기인한 것으로 도난당하거나 분실할 경우 휴대폰에 저장된 정보가 유출될 위협 및 분실한 기기를 이용하여 그룹웨어 등 내부 시스템에 침입하여 정보를 삭제하거나 정보를 유출할 위협이 매우 높기 때문이다.

또한 이러한 경우 외에도 악성코드에 기반을 둔 해킹이 발생한 경우 그룹웨어에 대한 직접적 공격이 발생할 수 있다는 점과 통상적으로 휴대폰이 PC보다 보안에 취약하다는 점은 이러한 사고를 예방하기 위하여 회사 차원에서 휴대폰에 대한 '관리'를 강화해야 할 필요성을 갖게 하였고 이에 따라 기업은 모바일단말관리 시스템의 도입을 통한 보안강화 시도를 하게 되었다.

2) 업무시간에의 통제필요성

이는 금융회사의 경우[17]를 통해 살펴볼 수 있다. 금융회사의 경우 임직원이 업무시간에도 휴대폰을 통해 E-mail, 메신저, 카카오톡 및 페이스북과 같은 SNS서비스 등을 사용하여 외부에 있는 사람들과 통신할 수 있으며, MTS(Mobile Trading System)를 이용하여 시간과 장소에 제약받지 않고 증권거래를 하는 등 다양한 모바일 애플리케이션을 사용할 수 있고, 이러한 점은 금융기관의 내부 투자정보 등이 외부로 유출되거나 임직원들에 의해 악용될 소지가 있다는 점에서 이를 통제하기 위해 업무시간ㄴ에 모바일단말관리 서비스를 통한 통제방안을 마련하는 배경이 되었다.

2. 주요기능 및 활용형태

1) 주요기능

17) 유길상, 전게논문, p.5.

<그림 2-1> 모바일단말관리 서비스의 주요 기능

출처 : 삼성SDS계열 Mobiledesk사의 MDM 플랫폼 소개 중 주요기능 (http://mobiledesk.co.kr)

<그림 2-1>에서 살펴본 모바일단말관리 시스템의 기능 중 일부를 소개하면 아래와 같다[18].

① 스마트폰 관리 기능 (IT Control Center) - 스마트폰의 관리 업무를 담당하는 관리자에게 가장 필요한 기능으로서 수많은 스마트폰에 업무용 소프트웨어와 파일을 배포하여 관리하는 기능, 원격에서 스마트폰을 제어할 수 있는 기능, 그리고 회사의 보안 정책에 맞도록 스마트폰을 사용할 수 있도록 하는 기능으로 스마트폰 관리 기능에는 원격 지원 기능이 포함된다. 기업 내에는 스마트폰 사용에 익숙하지 않은 직원들도 많이 있으며 이러한 직원들을 원격에서 스마트폰 환경을 공유하면서 가이드 해줄 수 있는 기능이 원격 지원 기능이다. 또한 스마트폰의 분실을 대비하여 원격 잠금, 파일삭제, 초기화 등의 기능을 제공한다.

② 스마트폰 사용 현황 관리(Mobile Activity Intelligence) - 스마트폰 사용 현황 관리 기능은 스마트폰 사용에 대한 통계 및 실시간 리포팅을 제공하는 기능으로 Dashboard를 통해 전체 사용자의 사용 현황을 종합적으로 모니터링 할 뿐만 아니라 개별 스마트폰에 대한 상세 정보, 사용자 정보를 관리 할 수 있다. 또한 사용 통화량에 대한 조회를 통하여 전체적인 요금 관리가 가능하며, 통신망의 품질 정보를 조회할 수 있어 스마트폰의 안정적인 서비스 제공에 활용할 수 있다.

③ 스마트폰 사용자 포탈 - 사용자를 위한 기능으로 사용자가 스마트폰을 사용하는데 있어 필요한 관리 기능을 웹사이트의 포탈 형태로 제공하는 것이다. 사용자는 포탈 접속을 통하여 자신의 데이터를 백업하고 사용 현황을 조회하고 필요시 원격 잠금 등의 설정을 할 수 있다 이러한 기능은 관리자의 관리 업무의 일부를 사용자가 직접 수행할 수 있는 창구를 마련해 줌으로써 관리 업무의 부담을 그만큼 줄여 줄 수 있다.

④ 스마트폰 보안성의 확보 - 모바일 오피스 구현으로 향상되는 업무 효율성은 보안성을 갖출 때에 진정한 의미가 있다. 스마트폰 분실 시의 데이터 보호뿐만 아니라 스마트포의 카메라, 외장 메모리 등의 사용을 제어

18) 김영철(2011), “스마트폰 활성화 전망에 따른 군사보안 대응방안 연구”, 서울: 숭실대학교, 석사학위논문, pp.51-53.

하여 기업의 중요 정보가 외부로 유출되는 것을 방지할 수 있으며 관리적인 차원의 보안성 확보를 넘어 스마트폰에 대한 Data-aware Architecture를 구현한다. 이러한 구조는 스마트폰에서 사용하는 데이터 가운데 기업 입장에서 보호하여야 하는 데이터를 정의하고 해당 데이터의 사용과 접근에 대해서는 완벽한 보안을 적용하게 하고 개인의 프라이버시에 해당하는 음악, 사진등과 같은 사용자 데이터에 대해서는 자유로운 사용을 침해하지 않는다.

⑤ 구성 - 통상 서버용 Software와 개별 단말기용 Agent Software로 구성된다. 개별 단말기의 Agent Software는 서버 Software와 네트워크를 통해 통신을 하면서 각종 관리 기능을 처리하게 된다.

개별 단말기의 Agent Software 설치는 OTA(Over The Air) 방식으로 각 스마트폰에 설치가 되며 Agent Software 설치 이외에 사용자가 설정할 부분은 전혀 없다. 이러한 단순한 구조와 간단한 적용은 MDM 도입 자체에 요구되는 노력을 크게 줄여준다

2) 최근의 활용형태

최근에는 위와 같은 기본적 관리기능에 더하여 회사 건물에 출입함과 동시[19]에 카메라·WiFi·USB저장소 등의 기능을 차단(자동적으로 직접제어)함으로 보안 사고를 미연에 방지할 수 있는 수준까지 발전하고 있다.

또한 휴대폰의 반입을 원천적으로 방지하는 부서·장소에 출입하는 경우 휴대폰을 회수함과 동시에 휴대폰에 걸려오는 전화를 개인 책상의 유선전화로 자동 착신전환이 되도록 구현하는 경우도 있다.

그러나 회사 및 통제장소를 벗어날 경우 이러한 통제가 자동적으로 해제됨으로서 규정된 업무시간 및 통제장소에서만 제한을 가한다는 점에서 점차 정교한·개별화된 통제로 까지 이루어지고 있다는 점을 살펴볼 수 있다.

19) 모바일단말관리 시스템은 사내 출입시스템과 연동하여 보안정책을 자동 적용하거나 위치정보 기반(GPS, AP, 3G, 4G)으로 단말기 위치를 파악하여 보안정책을 적용하는 방식으로 작동한다.

제 3절 軍 RFID영문출입통제 사업

1. RFID의 개념・특성

RFID(Radio Frequency Identification)란 일정 주파수(RF)대역을 이용, 무선으로 사물에 부착된 전자태그를 식별하여 사물의 정보를 획득/처리하는 기술을 말하며, 사물 등에 RFID태그를 부착하고 전파를 사용하여 해당 사물 등의 식별정보 및 주변 환경정보를 인식하여 각 사물 등의 수집, 저장, 가공 및 활용하는 기술을 말한다.

RFID는 기존의 광학기술 기반의 식별방식인 바코드 시스템과 마그네틱 시스템 등을 기반으로 한 정보인식시스템의 단점 해소 요구의 증가에 따라 개발되어 다양한 분야에 응용이 활성화되고 있다. RFID는 기술은 [표 2-2]에서와 같이 기존의 바코드에 비해 ① 인식속도가 0.01~0.1초로 빠르고 ② 수십 m의 원거리에서도 인식이 가능하며 ③ 99.9% 이상의 높은 인식률을 갖고 ④ 대용량 정보저장이 가능하고 재기록이 용이함은 물론 ④ 패스워드 보안기술 적용이 가능한 장점이 있다.[20]

[표 2-2] 매체별 인식능력 비교

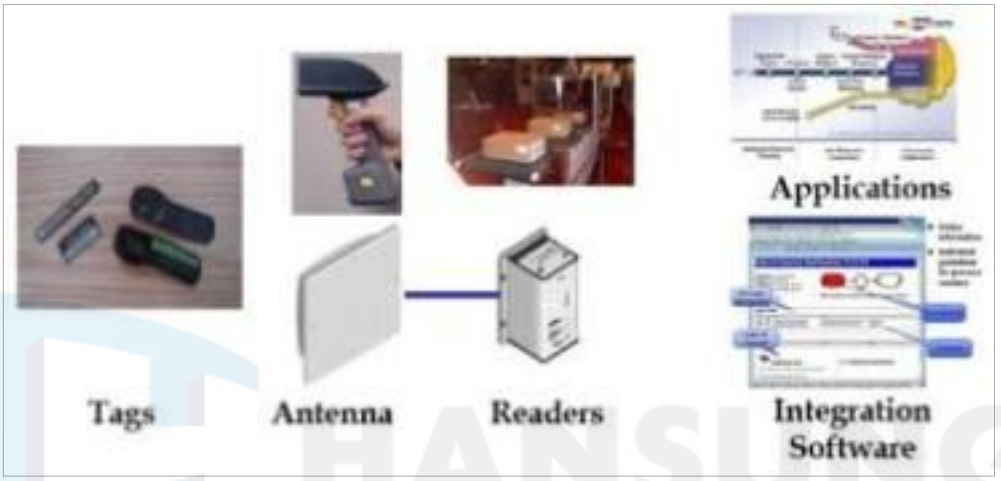
구 분	바코드	자기카드	IC카드	RFID
인식방법	비접촉식	접촉식		비접촉식
인식거리	0~5cm	리더기에 삽입		0~수m
인식속도	4초	4초	1초	0.01~0.1초
인식률	95% 이하	99.9%이상		
투과력	불가능			가능
사용기간		1만번 이내 (4년)	1만번 이내 (5년)	10만번 이내 (60년)
데이터저장	1~100byte		16~64Kbyte	64kbyte
쓰기기능	불가능	가능		
손상율	매우 잦음	잦음		거의 없음
태그비용	가장 저렴	저렴	높음	다양
보안능력	거의 없음		높음	높음
재활용	불가능	가능		

출처 : 박해종(2012), 아주대학교 석사학위논문, p.3.

20) 박해종, 전게논문, p.3.

RFID시스템은 <그림 2-2>과 같이 정보를 저장하거나 처리하는 태그와 전파를 이용하여 태그 정보를 송수신하는 안테나 및 리더기, 그리고 리더기로부터 정보를 받아 태그 정보를 관리하는 서버 및 네트워크 등으로 구성된다.

<그림 2-2> RFID시스템의 구성



출처 : 출입통제 시스템, RFID에 대해 알아볼까요?
(http://blog.naver.com/yes_id?Redirect=Log&logNo=90042006975)

태그는 안테나로부터 RF신호가 들어오면 진폭 또는 위상 변조하여 태그에 저장된 데이터를 특정 캐리어 주파수 신호로 리더기에 되돌려 주고, 태그로부터 신호를 되돌려 받은 리더기는 변조신호를 복조 및 복호화로 태그의 정보를 해독하는 것이 기본원리다[21].

태그는 내부에 전지가 포함되었는지의 유무에 따라, 전지 없이 리더의 신호로부터 에너지를 공급받아 동작하는 수동형 태그와 자체에 전원을 갖고 있으면서 송신과 수신이 가능한 능동형 태그로 나눌 수 있다. 능동형은 인식거리를 멀리할 수 있는 장점이 있으나 전원의 수명에 따라 작동시간에 제한이 있으며, 크고 무거우며, 고가라는 단점이 있다. 반면 수동형은 가볍고 반영구적이며 가격도 저렴한 장점에 비해 인식거리는 짧다는 단점이 있다[22].

21) 박해종, 전게논문, p.8.

RFID의 경우 사용 주파수에 따라 태그의 크기 및 가격, 주파수 인식거리가 달라지고 이에 따라 쓰이는 응용분야가 달라진다. 주파수가 고주파일수록 RFID의 인식속도가 빨라지고 주변 환경으로부터의 영향에 민감하며 태그의 크기는 줄일 수 있고, 수 미터에서 수십 미터의 중장거리의 인식에 용이하다[23].

그리고 고유 정보기록 방식에 따라서 Read-Only 형과 Read-Write형으로 구분이 가능한데, 현재의 바코드 및 전자 품목관리를 대체하는 물류관리 분야에서는 저가의 Read-Only형이 더 유리하다. 한편 Read-Write형의 경우에는 정보가 수정 가능하여 데이터베이스 관리에 의한 보다 복잡한 RFID시스템 구현이 가능하다는 장점이 있다.

2. RFID기술의 군사적 활용

현재 RFID기술의 군사적 활용은 국방탄약 관리 시스템, 공군 F-15K 부품 관리 시스템 등에서 활용이 이루어지고 있으며, 본 연구에서는 00-Army 실험사업[24]간 수행되었던 RFID영문출입통제시범사업[25]에 대해 살펴보고자 한다.

1) 현행 위병소 출입통제 시스템의 한계[26]

현제 군 출입 통제는 수작업 위주로 통제되어지고 있으며 전산화 되어진 체계는 위병소 출입통제 시스템으로서 여단급 이상 제대에서 사용하고

22) 권혁제(2011), "RFID/USN 기술기반 軍 실험사업 체계구축 개선 방안 연구", 수원 : 아주대학교, 석사학위논문, p.8.
23) 상게논문, p.7.
24) 상게논문, p.32. : 이는 국방부・정보통신부 협력 사업으로 육군본부에서 위임받아 IT 新기술을 적용한 네트워크기반의 첨단 정보화 육군 건설 목표를 위해 2007년 00사단을 실험부대로 선정 후 실험체계를 구축하여 추진된 사업이다. USN(Ubiquitous Sensor Network) 기술을 적용한 무인감시 체계, 생체인식 기반의 출입관리체계, 국방 물류・자산관리 통합체계, 국방원격 진료체계, 인터넷을 이용한 음성・데이터 통신체계 와 체계통합운용 등 총 6개 분야로 나눠 추진된 실험사업이다.
25) 이는 00-Army 실험사업간 생체인식 기반의 출입관리체계사업간 일부를 구성하였다
26) 이훈(2006), "RFID기술을 적용한 군 출입통제 시스템 구축방안", 춘천 : 강원대학교, 석사학위논문, p.8.

있다. 이 시스템은 민간인이 부대를 출입하기 위한 신청과 승인, 부대 내 장병의 출입시간을 기록하는 시스템으로서 단순한 수작업의 절차를 PC를 이용하여 기록하는 수준의 시스템으로 운용되고 있다.

따라서 군 출입통재 체계는 수작업 위주로 각 시설별 출입대장을 별도로 작성하고 있으나 기록의 정확성 보장과 이력관리가 불가한 실정이다. 따라서 군사자료 유출시 봉제구역 출입대장을 통한 추적이 불가하며 사건해결을 위한 많은 시간과 인력이 소요되며 출입대장의 수기 작성 및 열람 그리고 간부들의 시간외 근무수당 계산을 위한 자료 산출시 많은 시간과 인력이 소요되는 한계가 있다.

2) RFID영문출입통제시스템의 구축

군은 2006년부터 RFID출입통제시스템을 구축하고 있으며 기 구축된 부대들을 살펴보면 기본적으로 인원 및 차량의 출입증과 외부인원의 방문출입증에 RFID태그를 부착하여 부대출입을 통제하고 있다. 부대 출입에 대한 모든 사항은 자동으로 기록을 하고 있으며 각종 보안시스템(인증시스템, CCTV, 경계병 등)과 병행하여 출입자에 대한 보안을 강화하고 있다. 주요 내용은 [표 2-3]과 같다.[27]

[표 2-3] 군 RFID출입통제시스템의 구축방안

인 원	차 량	주요건물
전 장병·군무원 출입증RFID 태그 부착, 고정·휴대용 리더기 설치	개인 및 부대 등록차량 RFID 태그, 태그 리더기, 차량 차단기	태그 리더기 설치와 병행하여 생체인식, 전자 시건장치, 감시용 실내외 카메라 설치

출처 : 박해종(2012), p.26.

군 RFID출입통제시스템이 구축된 부대들의 주요 운용개념을 살펴보면 먼저 인원에 대해서는 위병소 등 주요 건물에 설치된 출입증 리더기에 확인절차를 거친 후 부대 및 사무실을 출입할 수 있으며, 차량은 위병소에

27) 박해종, 전게논문, p.26.

설치된 리더기가 차량에 부착된 RFID태그를 확인 후 차량 차단기가 자동 작동되도록 되어 있다. 주요건물에도 리더기가 설치되어 태그를 식별하여 출입을 할 수 있으며 이와 병행하여 특수구역에는 출입대상자에 한해 생체인식시스템(지문 또는 생체맥)을 사전 등록하고 등록여부를 확인 후 출입할 수 있고 건물 내의 CCTV 카메라에 출입 영상이 자동 녹화된다. 또한 비인가 인원 및 차량이 진입을 시도할 때는 경광등이 작동하고 보안관리자에게 통보가 되며 CCTV 카메라가출입하는 인원 및 차량을 자동적으로 녹화가 된다.

시범사업간 RFID태그는 900MHz의 수동형[28] 및 전자식별코드가 적용되었는데, 이는 국방 수동형 RFID기술(국방 수동형 RFID구현 가이드북상 860-960KMz을 사용)이 적용된 것이다. 이 이유는 이 주파수 대역은 전원이 필요 없다는 가운데 비용에 비해 비교적 긴 인식거리를 갖기 때문에 군 유통물류, 출입통제 등에 다양하게 활용될 수 있기 때문이다[29].

이렇게 RFID출입통제 시스템의 예상되는 도입효과는 다음과 같다[30].

첫 번째는 출입 통제를 위한 다양한 서류의 전산화이다. 인원 및 차량의 출입 내역이 네트워크를 통해 출입통제 서버에 전송되며 서버는 그 내역을 DB화 관리하게 되어 기존 수작업 체계의 각종 대장을 전산화 할 수 있다.

두 번째는 출입에 관한 업무의 효율성과 시간 절감이다. 실시간으로 출입자 현황을 파악가능하고 시간외 근무수당 계산을 위한 당직근무자 확인 서명, 위병소 출입일지와의 대조, 수작업에 의한 시간 산출 및 계산 등을 자동화 처리함으로서 수작업에 의한 오류와 시간절감이 가능하다.

세 번째는 출입에 관련된 업무의 신뢰성 및 투명성 보장이다. 기존의 출입 내역 기록은 기록하는 인원의 능력에 따른 오류가 존재할 수 있으며

---

28) 이훈(2006), 전게논문, p.10. : 수동형은 리더기로부터 안테나를 매개로 전송되는 송신출력을 받아 사용하기 때문에, 보통 태그와 판독기의 거리가 2-3M내인 단거리에서 사용하는 것이 일반적이다. 이밖에도 태그의 안테나를 크게 하고 판독기의 송신출력을 크게 만든 장거리 형이나 위치확인용 RFID제품도 있다. 현재, 능동형에 비해 수동형의 가격이 저렴하고 수명이 반영구적이므로 많이 사용되고 있다.

29) 박해종, 전게논문, p.29.

30) 이훈(2006), 전게논문, pp.39-40. 요약

기록된 내역의 정확성에 대해 100% 신뢰가 불가능 하였다,

제 4 절 NFC의 개념과 특징

1. 개념[31)]

NFC는 13.56MHz[32)] 대역의 통신 주파수에서 106Kbps에서 424Kbps의 통신 속도를 제공하는 통신범위 약 10cm 이내의 근접거리 무선 통신 기술이다.

NFC는 네트워크 설정에 필요한 시간이 약 0.1초 수준으로, 기존의 Bluetooth 등과 차별화된 즉시 응답성이 필요한 형태의 응용에 매우 적합하다. NFC는 두 단말의 안테나를 통하여 유도기전력을 기반으로 통신하는 기술로 각 단말의 전자기장의 생성 여부에 따라 수동 통신모드[33)]와 능동 통신[34)]모드로 동작한다.

2. 특징 및 활용전망

NFC기술은 최근 근접통신의 응용기술에 대한 요구의 급증에 따라 기존 RFID기술을 대체할 것으로 보이며 스마트폰에 있어 실제 활용한 사례는 2011년 초 출시된 Google과 삼성의 Nexus S가 NFC 기술을 채용하여 Google Wallet 등의 서비스를 출시한 것이고, 그 후 삼성의 Galaxy S Ⅱ·Ⅲ, RIM의 BlackBerry Bold 등 최근 출시되는 많은 스마트기기에서 NFC

31) 이민구 외(2012), "NFC를 활용한 능동형 인증 방법", 『한국통신학회논문지 제 37권 제2호』, 서울: 한국통신학회, p.141.

32) 이훈(2006), 전게논문, p.27. : 13.56MHz RFID시스템은 최근 활용도가 급증하고 있는 시스템으로 주로 교통카드, 신분증, 출입카드, 보안 분야에 널리 활용되고 있다. 이 시스템은 데이터 전송속도 측면에서 133MHz보다 우수하고 판독기 안테나도 유리하므로 최근에 현재까지 활용사례가 가장 광범위하며 주로 보안시스템, 단순인식 카드 분야에 작은 사이즈 안테나의 RFID시스템이 활용되고 있다.

33) passive communication, 단말이 스스로의 전자기장을 생성하지 않고, 능동 통신 모드의 단말이 생성한 전자기장으로부터 유도되는 전력을 이용하여 통신을 수행하는 것

34) active communication, 단말이 캐리어 주파수에 전자기장을 생성하여 다른 단말에 유도기전력을 공급하여 통신을 수행

기술을 채택하고 있다[35]는 점을 통해 살펴볼 수 있다.

이러한 NFC모듈 보급의 확대는 이동통신사와 신용카드사의 제휴 등[36][37]을 통해 모바일 결제시장의 급성장을 가져올 것으로 전망된다. 이는 기존 여러 장의 신용카드를 하나의 휴대전화유심(USIM)칩에 통합할 수 있으며, <그림 2-3>과 같이 지갑 역할을 휴대폰이 수행하고, 결제・멤버십・쿠폰・포인트 등 독립적으로 수행하던 서비스를 휴대폰으로 통합해서 제공할 수 있기 때문이다.

<그림 2-3> 스마트폰 NFC 기능을 활용한 결제

출처 : 아시아투데이, 2012년 5월 11일

그 외 NFC 기반 응용서비스는 아래 [표 2-4]와 같다

35) 이민구 외(2012), 전게논문, p.141.
36) 휴대폰의 USIM에 발급가능한 신용카드는 BC모바일카드, 하나SK카드 등이 있다
37) 유길상(2011), 전게논문, pp.15-16.

[표 2-4] NFC 기반 주요 응용서비스

구 분		서 비 스 형 태
모바일단말간 접촉 응용서비스	결제	대금 지불
	계좌이체	온라인 계좌 연계를 통한 계좌이체 등
	명함 교환	연락처, 이메일 등의 명함 정보 교환
	페어링	단말간 자료 교환을 위한 무선통신 접속
개인정보관리 응용서비스	개인 인증	인증을 통한 출입문 개폐(도어락)
	액세스 컨트롤	건물, 차량 등에 대한 리모트 컨트롤
정보 제공 및 맞춤형 광고 관련 응용서비스	관광안내	박물관, 관광 정보 제공(음성/문자) 및 위치안내
	의료	진료기록관리
	주차	주차위치 확인
	예약	포스터 접촉을 통한 공연 티켓팅 대중교통 티케팅 등
	광고/쿠폰	위치 기반 광고 및 쿠폰 제공 등
	제품 정보	제품 정보 열람, 진품 판정, 이력 추적, 매뉴얼 제공 및 A/S 정보 제공 등
	콘텐츠 구매	e-book, 음악 등의 콘텐츠 다운로드
	소셜 네트워크	태그로부터 읽어 들인 정보를 네트워크로 바로 전송

출처 : 이민구 외(2012), p.141.

이렇게 주목받고 있는 NFC의 주요 응용 분야에서 요구되는 핵심 기반 기술은 사용자에 대한 인증으로, 기존의 RFID태그의 주요 응용 분야인 출입통제나, 교통카드 등을 NFC로 대체하여 NFC 스마트기기를 이용하여 서비스 인증을 수행하고, 인증이 완료된 경우 사용자에게 서비스를 제공하는 응용분야에서 RFID를 대체하고 있다[38].

일례로 KT텔레캅은 기존 RFID의 주요 응용 분야인 출입통제 시스템을 NFC 스마트기기로 대체하여 개발하여 자사 직원에게 적용[39]하였는데, 이

38) 이민구 외(2012), 전게논문, p.141.
39) 한국경제, 2011년 5월 24일, 24면

를 통해 RFID태그가 내장된 사원증이 아닌 휴대폰의 NFC기능을 이용하여 출입게이트를 통과하며 출입과 동시에 모바일단말관리 시스템이 작동하는 등의 기능을 수행하게 된다.

앞서 제3절에서 국방 RFID표준규격의 주파수인 900Mhz와 NFC의 주파수 대역이 갖는 특징을 비교·정리하면 아래 [표 2-5]와 같다.

[표 2-5] 군용 RFID의 주파수와 NFC 주파수간 비교

주파수	고주파(HF)	극초단파(UHF)	
	13.56KHz	433.92MHz	860~960MHz
인식거리	60Cm	50~100m	3.5~10m(수동형)
일반특성	· 저주파보다 고가 · 짧은인식거리와 다중태그 인식이 필요한 응용분야에 적합	· 긴 인식거리 · 실시간 추적 및 컨테이너 내부습도, 충격 등 환경 센싱	· 가장저가 · 다중태그 인식거리와 성능이 가장 뛰어남
동작방식	수동형	능동형	능동/수동형
적용분야	· 수화물관리 · 대여물품 관리 · 교통카드 · 출입통제/보안	· 컨테이너관리 · 실시간 위치 추적	· 공급망 관리 · 자동통행료 징수

출처 : 이훈(2006), p.21.의 표를 요약 및 재정리

제 5 절 선행연구

최초 연구주제를 탐색함에 있어 『국가안보』[40]를 통해 새로운 시각에서 안보문제를 다룰 수 있는 본 주제를 발견하였고, 연구 진행 간 실제 세부적인 내용을 확정함에 있어 현 근무지가 RFID영문출입통제시스템을 적용하고 있다는 점이 많은 시사점을 주었다.

40) 김열수(2011), 『국가안보 : 위협과 취약성의 딜레마』, 파주 : 법문사

그러나 본 연구의 주된 내용인 모바일단말관리 시스템은 매우 최신의 개념으로 민간분야에서도 대기업·연구소를 중심으로 보급이 이루어지는 단계로 본 연구주제에 직접 부합하는 선행연구를 찾을 수는 없었다.

다만 스마트폰 활성화 전망에 따른 군사보안 대응방안에 관한 김영철의 연구를 기반으로 스마트폰의 특성을 군사보안 측면에서 이해할 수 있었고, 금융시장 건전성을 해치는 모바일단말 위협에 대한 대응방안에 관한 유길상의 연구를 통하여 군 내 모바일단말관리 시스템의 도입 필요성에 동감하며 군의 일련의 도입이 적절한 것이었음을 판단하게 되었다.

그리고 LG전자의 사례 등을 통해 모바일단말관리서비스 도입 간 예상되는 한계점을 검토하였으며 군 RFID영문출입통제에 관한 이훈과 권혁제의 연구는 NFC기술을 출입통제에 활용한 KT텔레캅 등으로부터의 시사점과 함께 본 연구에서의 기술적 대안으로 제시될 수 있었다.

제 3 장 스마트폰이 군사보안에 미치는 영향

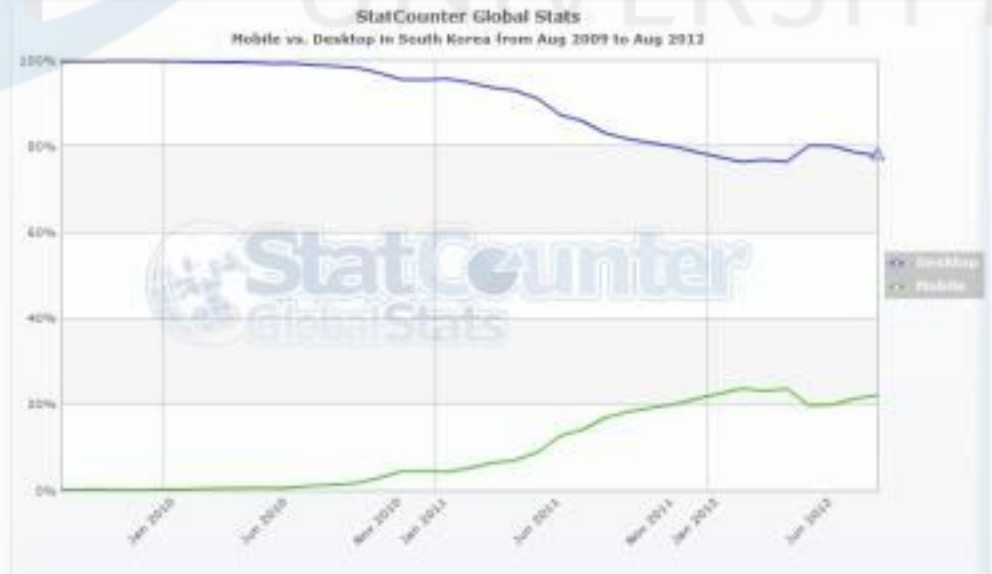
제 1 절 스마트폰의 사용 확산과 보안취약점 요소

1. 스마트폰의 사용 확산

앞서 제1장 및 제2장 제1절에서 살펴본 바와 같이 스마트폰은 단순통화 기능만 있는 피쳐폰에서 발전한 형태로 오늘 날 PC와 거의 동일한 수준의 업무를 수행할 수 있는 능력을 갖춰가고 있다.

또한 스마트폰의 사용자는 고속의 인터넷 접속이 가능한 상황(3G, LTE, WiFi)에서 웹서핑·이메일 송수신·SNS서비스 등의 일상생활과 기업의 모바일오피스 사용의 확산으로 업무영역에까지 활용이 가능하다. 따라서 스마트폰의 확산으로 인하여 2009년 8월부터 2012년 8월 간 우리나라의 데스크톱과 휴대폰의 비중은 아래 <그림 3-1>과 같이 변화하였다.

<그림 3-1> 우리나라의 휴대폰과 데스크톱간 점유율 변화



출처 : http://statcounter.com

이러한 현상은 데스크톱의 경우 고정형으로 휴대성이 제한되고 사무용인 경우 여러 사용자가 겸용으로 사용할 수 있고 윈도우 95의 출시이후 충분한 보급이 이루어져 교체수요 외 신규수요의 증가가 한계가 있는 반면 스마트폰의 경우 휴대형이고 용도에 따라 개인별로 1대 혹은 그 이상을 보유하는 경우도 있으며 보급이 현재진행형인 추세에 있다고 할 수 있다.

이러한 양자 간 격차가 감소하는 추세는 스마트폰의 성능의 발달과 고속 무선인터넷망의 보급에 따라 더욱 가속화 될 것으로 예상된다.

통상 우리나라의 경우 스마트폰 보급 확산의 기점을 2008년 12월 위피(WIPI : Wireless Internet Platform for Interoperability, 한국형 무선인터넷 표준 플랫폼)의 의무탑재 폐지 등에 의한 규제 완화와 2009년 11월 iPhone3의 출시로 보고 있고[41], 이에 따른 스마트폰 보급의 결과는 아래 [표 3-1]를 통해 알 수 있을 것이다.

[표 3-1] 국내 스마트폰이용자 비율 변화

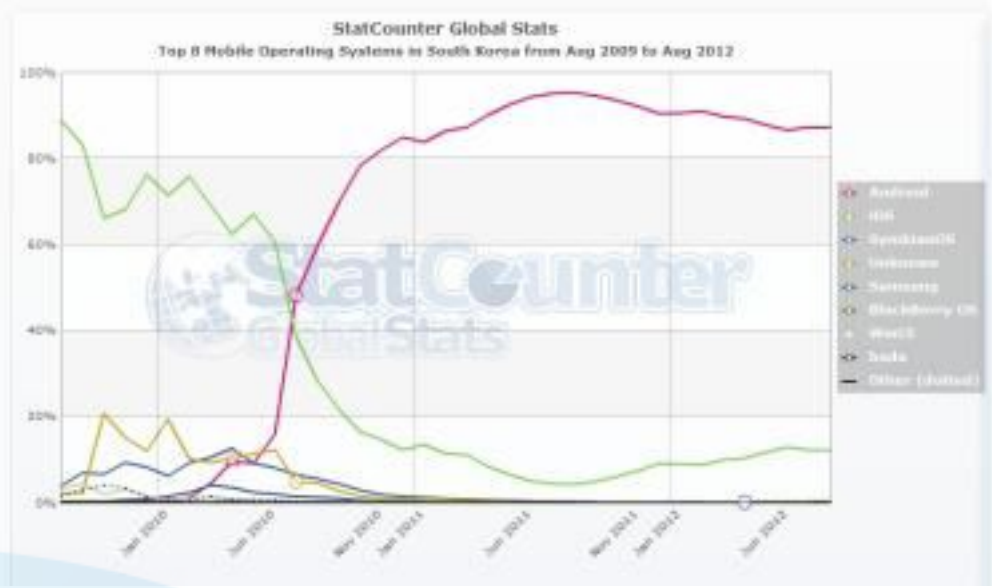
기 간	총 이동전화 이용자 수(A, 명)	스마트폰 이용자 수(B, 명)	비율(B/A*100, %)
2011년 12월	52,373,557	21,346,707	40.758559
2012년 9월	54,274,905	30,876,600	56.889275

출처 : 2011년 12월 및 2012년 9월 유·무선 가입자 현황, 방송통신위원회

약 9개월의 시차를 갖는 자료로 유의미하다고 보기는 어렵지만 해당기간동안 국내 이동전화 사용자 수는 약 3.6%정도 증가한 수준이나 스마트폰 이용자의 비중은 16%에 이를 정도로 큰 폭으로 증가한 점을 알 수 있다. 이로부터 포화상태에 이르렀다고 볼 수 있는 이동전화 시장에서 점차 그 중심은 스마트폰으로 이동하고 있다는 점, 즉 교체수요가 스마트폰으로 이동하고 있다는 점을 알 수 있다.

41) 임상규 외(2011), “스마트 시대의 보안 위협 : EU5의 대응과 시사점”, 『한국위기관리논집 제7권 제4호』, 충북 : 위기관리 이론과 실천, p.138.

<그림 3-2> 우리나라의 모바일 운영체제(OS) 이용현황 비교



출처 : http://statcounter.com

<그림 3-2>를 살펴보면 스마트폰 보급 초기단계인 2010년까지 다양한 운영체제가 있었으나 2010년 중순부터 안드로이드와 아이폰의 OS인 iOS 만이 유효한 수준을(2012년 8월 기준 안드로이드 87.2%, iOS 12.13%) 보여주고 있다.

따라서 이러한 점에서 본 장에서는 국내에 가장 많이 보급된 스마트폰 OS인 안드로이드를 위주로 보안취약점 요소 등을 파악하고자 한다.

2. 스마트폰의 특성과 보안위협

스마트폰은 앞서 제2장 제1절에서 그 특성으로 살펴보았던 개방성·휴대성·저성능은 급증하는 사용자수와 WiFi·Bluetooth 등 다양한 접속경로를 통한 연결의 편리성 등과 결부되어 오히려 보안에 있어 취약점으로 작용하기도 하는데 이는 아래 [표 3-2] 및 이에 대한 세부내용[42]을 통해 살펴보고자 한다.

42) 김영철, 전게논문, pp.12-14.

[표 3-2] 모바일단말의 특성과 보안위협

특 성	특성의 내용	보안 위협
개방성	· 무선인터넷 및 외부 인터페이스를 개발하여 제공 · 애플리케이션 개발 시 시스템자원의 사용을 위해 SDK(소프트웨어 개발 키트)를 이용하여 API(애플리케이션 프로그래밍 인터페이스)를 제공	· 다양한 외부 인터페이스 제공은 악성코드 전파 경로의 다양성을 제공하고, 내부 인터페이스는 악의적인 개발자에 의해 악성코드가 은닉된 애플리케이션 제작을 용이하게 하는 취약점이 존재
휴대성	· 휴대편의성	· 분실 또는 도난 사고 · 모바일단말에 저장된 개인정보유출 · 모바일오피스를 통한 사내 정보의 유출
저성능	· PC에 비해 저 전력, 저성능 · 최근 성능이 향상되고 있지만 아직 컴퓨터에 비해서 저조	· PC환경에서 제공하는 보안소프트웨어를 모바일단말에 적용하기는 무리 · 백신을 비롯하여 보안 소프트웨어의 적용이 어려움

출처 : 유길상(2011), p.40.

① 개방성 : 스마트폰은 피쳐폰보다 월등히 뛰어난 성능을 가지고 있으며 멀티미디어 처리도 우수하다. 스마트폰과 피쳐폰을 구별 짓는 가장 큰 특성은 개방성이라 할 수 있다. 스마트폰은 피쳐폰과는 다르게 무선인터넷 및 외부 인터페이스를 개방하여 제공하고 있다. 또한, 애플리케이션 개발 시 시스템 자원의 사용을 위해 SDK(Software Development Kit)를 이용하여 API(Application Programming Interface)를 제공하고 있다. 스마트폰의 다양한 외부 인터페이스는 사용자에게 다양한 네트워크 서비스를 지원하고, 내부 API 인터페이스 제공은 개발자에게 편리한 개발환경을 제공한다. 하지만 이를 보안적 측면에서 해석하면 다양한 위부 인터페이스 제공은 악성코드 전파 경로의 다양성을 제공하고, 내부 인터페이스는 악의적인 개발자에 의해 악성코드가 은닉된 모바일 애플리케이션 제작을 용이하게

만드는 취약점을 가지고 있다.

② 휴대성 : 스마트폰으로 인해 발생할 수 있는 보안 문제 중에서 먼저 말할 수 있는 것은 스마트폰의 분실 위협이다. 스마트폰은 개인용 PC나 노트북 보다 상대적으로 크기가 작다고 할 수 있다. 작은 크기이기 때문에 휴대하기 편리하지만 작은 크기로 인하여 쉽게 잃어버릴 수 있는 위험성이 존재한다. 샌 모이 리서치인모션 이사에 따르면 스마트폰은 PC에 비해 분실 및 도난의 위험이 15배 이상 높고 스마트폰 이용이 확산되면서 스마트폰 절도 사건이 가파르게 증가할 것이라고 한다.

스마트폰의 제품 자체가 기존의 휴대폰보다 높은 가격이기 때문에 도난이 일어나는 사고가 많아지고 있는 것이다. 스마트폰에 우수한 기능을 집약시키는 노력을 실시함에 따라서 스마트폰을 높은 가격의 부품으로 구성하였다. 높은 가격의 부품으로 구성된 스마트폰은 당연히 제품의 가격이 높을 수밖에 없다. 따라서 스마트폰을 절도하여 직접적인 판매를 통한 수익을 얻으려는 자가 증가하는 것이다.

그러나 더 큰 문제는 스마트폰 안에 저장되어 있는 정보와 자료를 이용하여 개인에게 심각한 피해를 발생시킬 수 있다는 것이다. 스마트폰은 PC와 같은 많은 용량을 가지고 있기 때문에 자료와 정보의 보관에 용이하다. 스마트폰에 회사의 기밀정보나 중요한 자료가 저장되어 있을 경우 이를 분실하게 되면 자료가 외부에 노출되게 됨으로서 심각한 어려움을 겪을 수 있다.

개인의 경우 스마트폰을 이용하는 시간이 많고 스마트폰에 대한 삶의 많은 부분을 의지함에 따라서 스마트폰에 개인의 인적사항이나 정보가 저장되어 있는 경우가 많다 . 이러한 경우에 개인적인 중요한 정보가 외부에 넘어감으로서 개인에게 피해가 발생하는 것이다. 평소 전자거래에서 스마트폰의 활용이 많은 경우 도난당한 스마트폰을 활용하여 그들의 계좌에 접근하여 금전적인 피해를 발생시킬 가능성이 있다. 편리하게 전자거래를 할 수 있다는 스마트폰의 장점이 오히려 단점으로 작용하는 것이다. 이러한 위협이 증가함에 따라 스마트폰에 저장된 정보를 암호화하거나 분실/도난 시 저장된 정보를 원격으로 소거하는 기술들이 등장하고 있다.

③ 저성능 : 스마트폰은 PC에 비해 저 전력, 저성능 기기이다. 따라서 PC환경에서 제공하는 보안 소프트웨어를 스마트폰에 적용하기에는 무리가 있다. PC환경에서는 다양한 보안 위협에 대응하기 위해서 지속적인 모니터링을 통해 악성코드들 탐지해야 하지만 스마트폰은 전력 및 성능적 제약으로 인해 백신을 비롯한 보안 소프트웨어의 적용에 어려움이 있다.

이러한 특성에 기초하여 EU에서는 스마트폰에 대한 정보보안 위협요인 10가지에 대해 아래 [표 3-3]과 같이 보고 있다.

[표 3-3] 스마트 시대의 정보 보안 위협 10가지

구분	위 협	세 부 내 용
R1	Data leakage	스마트 폰의 도난 & 분실로 인한 정보의 보안 문제
R2	Improper decommissioning	폰에 내장된 민감한 정보를 보호하지 않거나 방치한 채로 다른 사람이 폰을 사용 하거나 습득함으로 인한 공격 피해
R3	Unintentional data disclosure	대부분의 앱은 개인 프라이버시 기능을 가지는데, 많은 사용자들이 인식하지 못하고 데이터가 전달되거나 정보의 존재를 인식하게 되는 경우
R4	Pissing	공격자가 사용자의 개인정보(패스워드. 신용카드 번호 등)를 사용하거나 위조하는 것
R5	Spyware	Spyware를 활용한 개인 데이터의 파괴와 악용
R6	Network Spoofing attacks	공격자가 나쁜 네트워크를 만들어 사용자가 접근하게 하여 위험을 초래함
R7	Surveillance	공격 목표가 된 스마트 폰 사용자를 속이면서 스파이 행위를 하는 것
R8	Diallerware	공격자가 서비스나 폰 번호를 알아내어 사용자의 돈을 탈취하는 것
R9	Financial malware	악의적인 소프트웨어(malware)를 통해 신용카드번호와 인터넷 뱅킹의 정보를 훔치는 것
R10	Network congestion	네트워크의 자료가 한계를 벗어나므로 인해 스마트 폰 사용을 못하게 하는 경우

출처 : 임상규 외(2011), pp.144-145.

이러한 보안 위협에 대한 대응방안으로는[43] 먼저 R1에 대한 대응은 자동 잠금 설정을 들 수 있으며 기본적으로 스마트 폰에 많은 개인정보를

보관하는 만큼 높은 수준의 승인요구 등의 보호설정을 명심해야한다. 그리고 R3과 같은 경우는 핸드폰을 교체할 경우를 예로 들 수 있는데 저장되어있는 개인정보를 백업 받은 후에는 다른 이들이 핸드폰을 습득하더라도 남아 있는 개인정보를 활용하지 못하게 삭제나 초기화를 해야 한다.

마지막으로 R6·7, 10의 공인되고 안전한 시스템 이용 및 함께 공유할 수밖에 없는 기지국을 사용하기 때문에 항시 R4의 위험에 대한 인식을 해야 하며 안티바이러스 프로그램과 같은 보안·암호화 관련소프트웨어를 구입하여 철저한 대비를 해야 할 것이며 이를 정리하자면 [표 3-4]와 같다.

[표 3-4] 주요 위험요인에 대한 대응방안

구분	대 응 방 안
R1	- Automatic Iocking (자동 잠금장치) - Regular backups (정기적인 백업) - Note IMEI number (IMEI 번호의 기록) - User-to-smartphone authentication (스마트폰 사용자 인증) - Certification of smartphone (FIPS140-2 등)
R2	- Scrutinize permission requests (면밀한 승인 요구) - Review default privacy settings (개인정보 기본 설정)
R3	- Reset and wipe(before disposing or recycling the phone, wipe all the data and setting) (초기화 & 모든 데이터 삭제) - Decommissioning (해체)
R4	- Be skeptical (다른 이의 사용을 막음) - IT officers should create awareness of this risk (위험의 인식)
R5, R8, R9	- Check reputation(before installing or using new smartphone apps or services, check their reputation using app-store reputation mechanisms (안전하고 공인된 것인지를 확인) - Check resource usage and phone bill - Resource controI(monitor resource usage of smartphones for anomalies(모니터링)
R6	- Cautious use of hotspots(use public WiFi hotspots with caution and configure the smartphone so that it does not connect automatically (공인된 무선랜 기지국 이용) - Communications confidentiality(using VPN or SSL) (통신 비밀의 보장) - Pre-installing server certificates (사용전 서버 인증) - Encryption software (암호화 소프트웨어의 구비

출처 : 임상규 외(2011), pp.144-145.

43) 임상규 외(2011), 전게논문, pp.145-146.

즉 정리하면[44] 스마트 시대가 가져다주는 다양하고 편리한 서비스의 이용을 위해서는 취약한 보안 위험에 대응이 필요하다는 것이다.

먼저 스마트 폰을 비롯한 스마트 정보통신 기기들을 사용하는 사용자의 대응을 필요로 한다. 스마트폰과 PDA같은 기기의 악성 코드 사고에 대한 책임은 전적으로 시스템에만 존재할 수 없는 것이고 사용자들에게도 일정 부분 책임이 있다. 특히, 피쳐폰에서 스마트 폰으로 급속한 전환이 일어나는 시점에서 사용자들은 스마트 폰 보안에 대한 이해가 부족한 실정인데 각종 보안 사안별 위험에 대한 보안의식을 가질 수 있도록 해야 한다. 앞서 살펴본 것 중 R1, R5, R8 그리고 R9의 대응방안이 이 부분에 해당한다고 볼 수 있겠다.

둘째, 기술적인 대응 방안인데, 백신 소프트웨어의 한계이다 PC환경에서 악성코드 검출 및 제거방법으로 백신 프로그램의 설치를 최우선적으로 고려해왔던 것이 사실이다. 반면, 스마트 폰은 일반 폰과 다르게 PC의 기능을 가지고 있기 때문에 기존 PC에서와 동일한 접근방법이 스마트 폰 환경에서도 그대로 적용할 수 있을지에 대한 검토와 함께 스마트 폰에 가장 적합한 환경을 만들어 주어야 한다. 더불어, 스마트 폰에 장착되거나 사용 가능한 소프트웨어 등록 및 검증이 필요하다. iPhone의 경우 앱 스토어에서 개발자가 프로그램 등록 시 이에 대한 보안성 검증 및 테스트가 이루어지는데, 검증과정이 폐쇄적으로 진행되어 어떤 검증과 테스트가 이루어지는지 알 수 없지만 이를 투명성 있게 검증하고 그 결과를 사용자들에게 알려주어야 한다. R5, R8, R9의 위협에 대한 대응 방안으로써 앱이나 프로그램을 설치하기 전에 안전 신뢰도를 알아보고 사용한다면 위협을 줄일 수 있다.

2) 안드로이드의 특성과 보안상 취약점[45]

앞서 제1절에서 살펴본 바와 같이 스마트폰 OS는 안드로이드 운영체제가 압도적인 비중을 차지하고 있는 가운데, 본 항목에서는 안드로이드의

---

44) 임상규 외(2011), 전게논문, p.147.

45) 안철수 연구소, "[Tech Report] 앱보다 많은 모바일 악성코드의 '위협'", (http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=19123)

특성과 보안상 취약점에 주목하여 살펴보고자 한다.

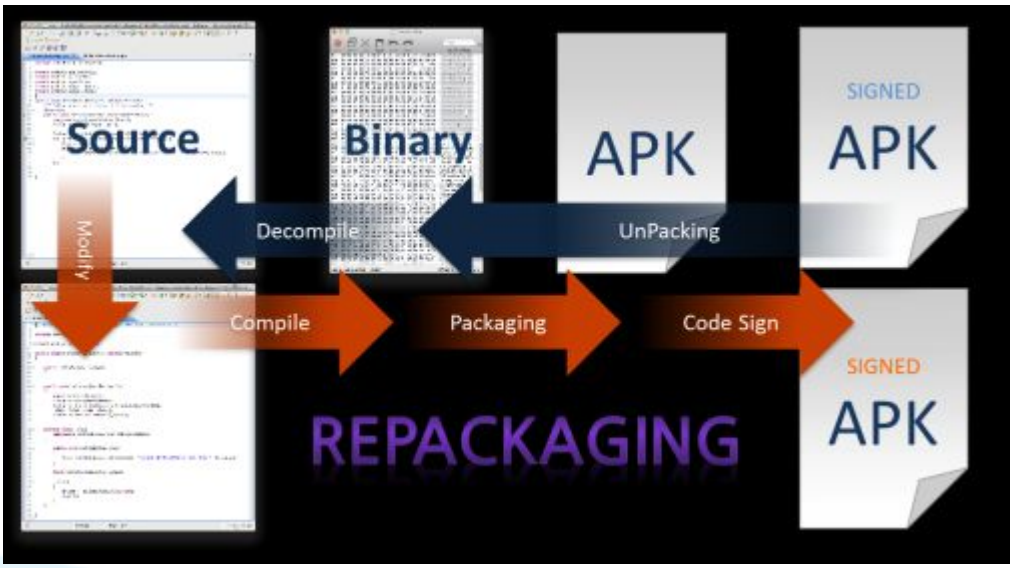
안드로이드는 리눅스 OS 위에서 동작하며 주요 소스들이 공개 배포되고 있다. 개발 언어도 자바나 C(++) 등의 익숙한 언어로 되어 있어 개발자의 진입이 쉽다. 공식 마켓 이외의 마켓을 지원하고 있는 점도 안드로이드 시장 활성화에 영향을 주었을 것이다. 하지만 이런 개방적인 특성은 보안 측면에서는 좋지 않은 영향을 끼친다.

첫째, 검증되지 않은 프로그램의 무분별한 배포 때문에 사용자들의 안전이 보장되지 않는다. 안드로이드 마켓에는 보안상 문제가 있는 애플리케이션이 올라와 있거나, 광고나 수익을 목적으로 하는 애드웨어가 무료 사용을 미끼로 사용자들을 유혹하고 있다. 또한, 공식 마켓에는 애플리케이션에 문제가 있으면 사용자 기기에서 강제로 제거해주는 사후 처리 기능이 있지만, 서드 파티 마켓(Third-party Market)은 사후 검증 및 사후 처리가 되지 않는다.

둘째, 리버싱과 리패키징으로 인해 애플리케이션 제작자나 사용자들에게 피해가 갈 수 있다. 안드로이드에서 배포하는 APK[46] 파일은 DEX와 Manifest 및 다수의 리소스 파일 등으로 이루어져 있는데, 시중에는 이러한 파일을 원본 소스와 근접할 정도로 복구해주는 다양한 프로그램이 있다. 악성코드 제작자는 아래<그림 3-3의> 리패키징[47]기법을 통해 정상적인 애플리케이션으로 위장한 악성코드를 배포한다. 이 경우 비공식 마켓을 이용하는 사용자들이 보안 위협에 노출될 수 있다.

46) Application PacKage의 약자로 안드로이드 애플리케이션의 확장자 명이다.
47) 리패키징은 앱을 제작하는 일련의 과정을 거꾸로 변환해 최초 형태(소스코드)로 만든 뒤, 이를 수정하거나 다른 코드를 삽입해 앱을 재 제작하는 과정을 통칭하는 단어다.

<그림 3-3> 리패키징 기법

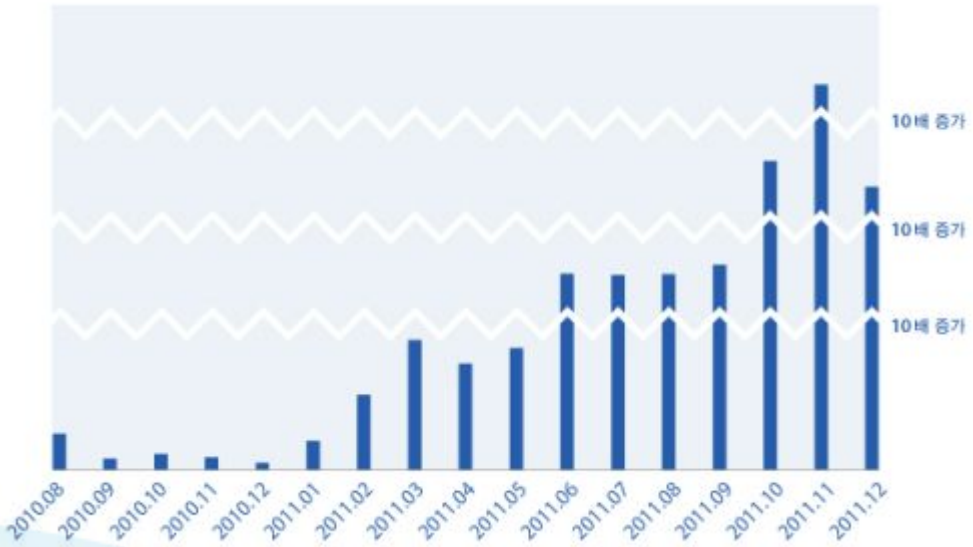


출처 : 안철수 연구소, “스마트폰에 은밀히 숨어든 ‘도둑들’”, (http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?curPage=1&menu_dist=2&seq=19986&dir_group_dist=0)

마지막으로, 취약점이 다수에게 노출되기 쉬워 이를 이용한 악성코드가 더욱 기승을 부릴 수 있다. 실제로 취약점을 이용한 루팅 기술은 인터넷에서 쉽게 찾아볼 수 있고, 그 중 일부를 이용한 exploid, asroot, rageagainstthecage와 같은 루팅 라이브러리는 공공연하게 이용되고 있다. 루팅을 할 경우 해당 애플리케이션은 안드로이드 기기에 대한 모든 제어 권한을 갖게 되어 사용자 몰래 정보를 빼가거나 특정 애플리케이션에 대한 설치·삭제, 녹음, 스크린 샷, 문자 발송 등의 여러 작업이 가능하다.

이와 같은 보안 문제들은 실제 통계를 통해서 확인할 수 있는데 <그림 3-4>은 2010년 하반기 이후의 안드로이드 악성코드 샘플 접수 량이다. 2010년엔 극히 미미하게 접수되던 악성코드가 2011년에 접어들면서 기하급수적으로 증가한 것을 볼 수 있다. 2010년과 2011년 동일 기간(8월～12월)에 접수된 샘플의 수를 비교하면 200배 가까이 증가했다. 이를 통해 악성코드의 증가 추세가 앞서 살펴본 <그림 3-2>에서의 안드로이드 이용자 변동 추세와 상당부분 유사하다는 것을 알 수 있다. 즉, 이용자가 많은 안드로이드를 대상으로 악성코드가 제작되고 있는 것이다.

<그림 3-4> 안드로이드 악성코드 샘플 접수량



출처 : 안철수 연구소, (http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=19123)

3. 스마트폰의 악성코드 피해사례 및 유형

스마트폰의 악성코드로 인한 침해사고는 다양한 감염경로를 통해 발생한다[48].

첫째는 사회 공학적 기법을 이용하는 것으로 무료 지하철 프로그램, 동영상 플레이어, 인터넷 뱅킹 프로그램 등 유용한 소프트웨어로 위장하여 온라인 마켓(구글 Play스토어, 애플 앱스토어 등) 또는 이메일 및 문자메시지의 첨부파일 형태로 감염된다. 그 외 WiFi나 이동통신망을 통한 인터넷 접속, USB, Bluetooth를 통한 통신기능을 이용하여 감염될 수도 있으며, 그리고 스마트폰의 취약점을 이용하는 방법으로 스마트폰 운영체제 및 웹 브라우저의 취약점을 공격하여 악성코드 감염을 시도, 또는 네트워크 취약점(블루투스, 무선랜, 이동통신망)을 통해 특수하게 조작한 패킷을 전송함으로서 스마트폰을 감염시키기도 한다.

48) 김영철(2011), 전게논문, p.19.

이 중 현실에서 발생가능성이 가장 높은 것은 유료프로그램을 불법적인 경로를 통해 공짜로 설치하려다 악성코드로 변조된 애플리케이션을 통한 악성코드의 유입과 USB와 컴퓨터의 연결을 통해 바이러스 및 악성코드가 전파될 가능성이 크다고 생각한다.

1) 스마트폰 악성코드 발견 및 피해 사례[49)]

안철수 연구소는 2010년 4월 22일 국내 윈도모바일 스마트폰에서 악성코드 피해가 발생했다고 발표했다. '트레드다이얼'이라는 이름의 악성코드는 무단으로 국제전화를 걸어 비싼 요금을 내게 하는 것으로 윈도모바일 기반 스마트폰에서 발생했으며 2010년 4월 13일 최초 발견된 후 19일 변종이 추가 발견됐다. 이 악성코드는 삼성전자 옴니아를 포함해 윈도모바일 운영체제(OS)를 탑재한 스마트폰에서 작동한다. 모바일 게임인 '3D 안티테러리스트 액션'과 '코드팩'에 포함돼 배포됐으며 50초바다 국제전화 번호로 전화를 건다. 발표 시점 확인된 번호는 총 6개로 음성 및 데이터 서비스, 퀴즈쇼, 투표 등에 사용되는 번호로 분 단위 과금을 하는 것 들이다.

스마트폰 백신 개발 업체인 쉬프트웍스는 2010년 3월 28일 안드로이드 스마트폰에서 휴대폰 정보 수집 악성코드 수십 건이 발견되었다고 발표했다. 쉬프투웍스에는 지난 3월 18일 국가 최초로 미래에셋 모바일 트레이딩 서비스(MTS)에 상용화된 안드로이드 백신 사용자 신고가 매일 50건 이상 접수되고 있으며, 이를 기반으로 패턴파일을 분석한 결과 20여 건 의 휴대폰 정보수집 악성코드를 발견했다. 이들 악성코드는 수집한 휴대폰 번호를 이용해 스팸이나 광고에 사용하고 있는 것으로 분석 됐으며, 휴대폰 복제나 도청을 가능하게 하는 IMEI(International Mobile Equipment Identity, 단말기 식별정보)정보 수집 악성코드도 발견했다. 이들 악성코드는 휴대폰 정보를 수집하는 악성 애플리케이션으로 실행과 동시에 지정된 서버로 휴대폰 내용을 탈취하는 종류가 가장 많고, 사용자 인증을 하는 것처럼 휴대폰 정보를 빼가는 경우도 있었다.

미국에서는 안드로이드 운영체제를 탑재한 스마트폰에서 배경화면을 바

49) 김영철(2011), 전게논문, pp.20-22.

꿔주는 한 무료 애플리케이션이 이용자 400만 명의 개인정보를 유출한 것으로 밝혀졌다. '재키 월페이퍼'라는 이름의 이 무료 앱은 스마트폰 이용자들의 인터넷 브라우저 기록과 전화번호, 문자 메시지, 음성메일함 비밀번호 등을 수집하여 중국에 있는 서버로 전송한 것으로 알려졌다.

그 외 크로스 플랫폼 형으로 불리는 형태도 발견된 바 있다[50]. 이는 모바일 단말을 통해 PC를 감염시키는 공격 유형으로. 2005년에 발생된 Cardtrap.A가 최초의 크로스 플랫폼형 악성코드로써 폰의 메모리 카드에 윈도 웜을 복사하여, 감염된 폰 메모리 카드를 PC에 장착했을 때 autorun을 통해 PC를 자동으로 감염시켜 데이터를 삭제하거나 성능을 저하시킨다. 모바일 기기간의 확산이 아닌 모바일 기기에서 PC를 감염시킨다는 점에서 새로운 형태의 공격 유형이라 할 수 있다.

2012년 7월에는 'i want to add your birthday to my calender! www.mycalenderbook.com/fb/mobile/accept.php?m=357025&s=42'와 유사한 URL 링크가 담긴 SMS를 수신 후 연결 시, 해당 어플이 자동 설치 되어 자동 실행 후 지인에게 문자 발송 여부에 대한 영문 안내가 나오나 이를 꼼꼼히 읽지 않고, 바로 동의를 선택한 경우 휴대폰에 저장된 모든 전화번호부 전체를 대상으로 문자가 발송되어 발송자의 문자요금 피해 및 연쇄적인 피해가 발생한 경우[51] 있어 이동통신사가 이와 같은 문자의 전송을 차단한 경우가 있었다.

2) 스마트폰 악성코드의 유형

안철수 연구소가[52] 안드로이드 운영체제에 대한 상위 11대 악성코드를 분석한 아래 [표 3-5]에 따르면 악성코드들은 주로 위장된 애플리케이션의 형태로 설치를 시도하는 것을 알 수 있다.

---

50) 김영철(2011), 전게논문, p.19.
51) SKTelecom Tworld 공지사항
52) 안철수 연구소, "[Tech Report] 앱보다 많은 모바일 악성코드의 '위협'", (http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=19123)

[표 3-5] 안드로이드 운영체제 상위 11대 악성코드의 진단명 및 특징

진 단 명	특 징
Android-Trojan / SmsSend	사용자를 속이거나 사용자 몰래 문자를 전송하는 프로그램을 말한다.
Android-Trojan / FakeInst	임의의 애플리케이션 설치 프로그램으로 위장하여 문자 전송 등으로 수익을 도모하거나 실제 악성코드를 설치하는 프로그램들을 말한다.
Android-Spyware / Geimini	정상 애플리케이션의 리패키징을 통해 사용자를 속여서 설치되고, 백그라운드 서비스로 개인정보를 탈취해가는 스파이웨어 악성코드 종류를 말한다.
Android-Exploit / Rootor	이 진단명은 애플리케이션 실행 시 취약점을 이용하여 시스템 권한을 취득하는(루팅) 악성코드 종류를 말한다.
Android-Trojan / LightDD	성인 애플리케이션으로 위장하여 백그라운드에서 사용자 스마트폰 정보를 유출하는 악성코드를 말한다.
Android-Dropper / Anserver	이 진단명은 정상 애플리케이션을 리패키징하여 다른 악성코드(Android-Trojan/Anserver)를 설치하는 형태의 악성코드를 말한다. 이 애플리케이션이 설치되면 사용자의 스마트폰 정보를 유출하거나 다른 악성코드의 다운로드 및 설치 등의 악성 행위를 수행한다.
Android-Trojan / Gdream	게임, 만화(화보)를 리패키징하여 악성코드를 추가한 형태의 악성코드 종류이다. 휴대전화 정보, 위치 정보, 문자/전화 송수신 정보 등을 유출하는 등의 악의적인 행위를 한다. 그리고 네트워크에 접속하여 새로운 명령(다른 악성코드 다운로드, 문자 발송)을 받아 실행한다.
Android-Spyware / BgService	정상 애플리케이션을 리패키징해서 악성코드를 삽입한 형태의 악성코드 종류를 말한다. 백도어 설치, 문자 모니터링, 유료 문자 전송, 웹 사이트 방문 기록 및 북마크 수집, 스마트폰 정보 수집 등의 악의적인 행위를 한다.
Android-Trojan / Boxer	임의의 애플리케이션 설치 프로그램으로 위장하고 실제로는 유료 문자를 발송하는 악성 애플리케이션을 말한다
Android-Spyware / Adrd	정상적인 유틸리티를 리패키징하여 다양한 악의적인 기능을 수행하는 애플리케이션을 말한다. 주요 기능으로는 스마트폰 정보 유출, 북마크 유출, 문자/전화 정보 유출, 유료 문자 발송, 다른 악성코드 설치 등이 있다. 다양한 형태의 변종이 있기 때문에 사용자가 악성코드를 알아보기 쉽지 않다. 중국에서 제작되었으며 비공식 마켓을 이용하여 전파된다.
Android-Spyware / Kmin	월 페이퍼 변경 애플리케이션으로 위장하여 백그라운드로 다양한 악성 기능을 수행하는 애플리케이션을 말한다. 애플리케이션 이름은 KMHome이며 주요 기능으로는 문자/전화 감시, 유료 문자 발송, 스마트폰 정보 유출, 주소록 유출 등이 있다.

출처 : 안철수 연구소, “[Tech Report] 앱보다 많은 모바일 악성코드의 '위협'”, (http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=19123)

3) 소결론

이렇게 악성코드가 증가하는 원인으로는 아래 [표 3-6]과 같이 악성코드 제작자에게 스마트폰이 주는 매력이 있기 때문이라 여겨진다.

[표 3-6] 악성코드 제작자 측면에서 본 안드로이드의 매력

매 력	설 명
수익성	스마트폰 자체의 SMS, Call 기능으로 돈을 벌기가 쉽다.
개인정보	고급 개인정보가 가득 담겨 있다.
연속성	하루 24시간 켜져 있다
네트워크	언제나 네트워크(3G, 4G, Wi-Fi)에 연결되어 있다.
편리한 전파 방법	다양한 마켓을 이용하여 악성코드를 배포할 수 있다.
우수한 하드웨어	악성 행위에 필요한 충분한 성능의 하드웨어
안드로이드의 짧은 역사	잘 알려지지 않은 다양한 형태의 보안 위협이 존재하다
넓은 사용자 층	남녀노소, IT초보자・전문가 누구나 사용한다
사용자의 보안 의식	아직 스마트폰에 대한 의식수준이 낮다.

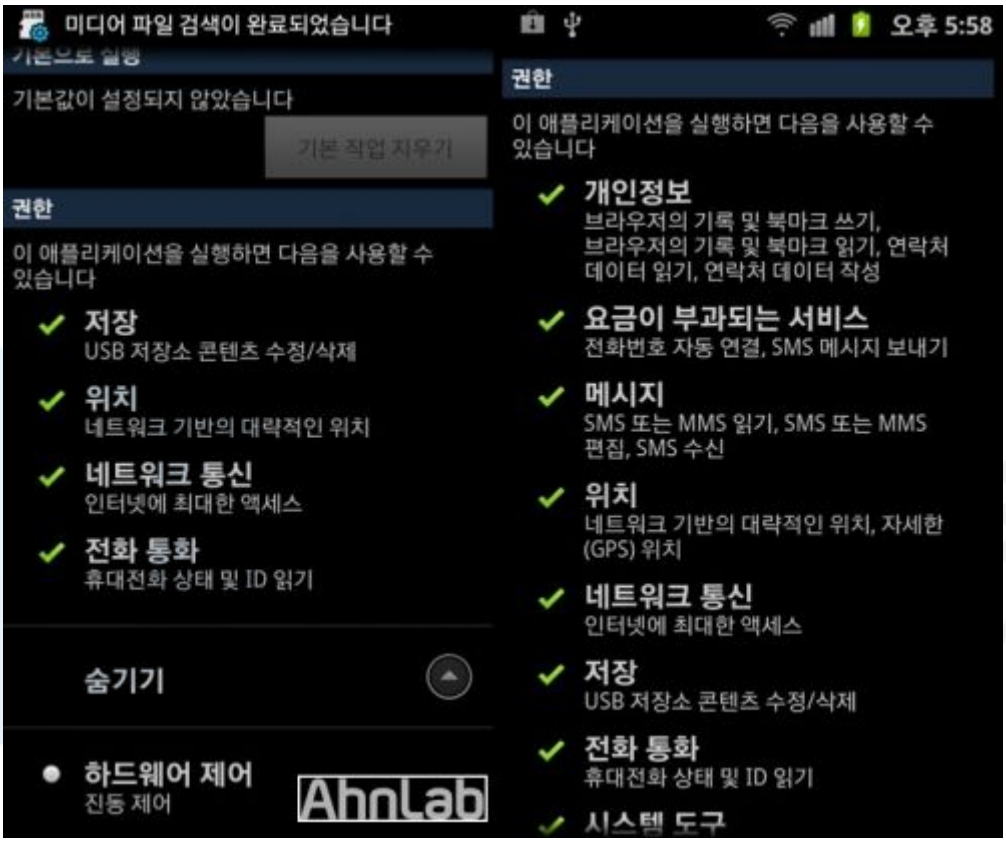
출처 : 안철수 연구소, “[Tech Report] 앱보다 많은 모바일 악성코드의 '위협'”, (http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=19123)

특히 24시간 항시 가동되며 사용자의 인지여부에 관계없이 네트워크에 접속되어 있다는 점, 사용자의 무관심에 가까운 보안의식은 주요한 원인이 될 수 있고 특히 스마트폰 사용자가 루팅[53]을 통하여 더 최적화된 환경의 구축, 기본 안드로이드 기능의 확장을 의도하지만, 이러한 루팅이 악성코드에 의해 악용될 경우 상당한 보안 위협이 될 수 있다. 예를 들어 사용자

53) 루팅은 PC 환경에서의 해킹 기법으로 해커가 특정 시스템에서의 루트 권한을 획득하기 위해 취약점 또는 프로그램 버그를 이용하던 데에서 유래됐다. 통상적으로 스마트폰에 있어 루팅은 루터 권한을 획득하여 불필요하다고 여겨지는 이동통신사에서 설치한 애플리케이션을 삭제하거나 제한된 기능을 활성화 시켜 성능의 향상 혹은 타 사용자가 제작한 Custom Rom을 설치하고자 함에서 시도되는 경향이 크다.

의 적절한 동의나 인지 없이 특정 프로그램을 설치하거나, 카메라 영상·통화·문자 메시지에 접근 혹은 유료 통화·문자 메시지를 전송하는 등의 행위를 할 수 있기 때문이다.

<그림 3-5> 애플리케이션의 설치 간 악성코드에 감염된 경우와 비교



출처 : 안철수 연구소, “[Tech Report] 앱보다 많은 모바일 악성코드의 '위협'”, (http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=19123)

<그림 3-5>의 경우 좌·우는 동일한 애플리케이션의 설치 시 요구되는 권한에 대한 안내문이다. 다만 우측의 경우 악성코드를 삽입하여 과도한 권한을 요구하도록 수정된 상태로서 애플리케이션이 요금이 부과되는 서비스 및 위치, 시스템 도구 등의 권한을 활성화 시켜 실제로 악용할 수 있다.

따라서 실행하려는 애플리케이션의 기능과 실제로 요청하는 권한을 잘

살펴보아 과도가거나 위험한 권한을 요청하는 애플리케이션은 가급적 설치하지 않는 것이 좋다. 그리고 안드로이드 스마트폰 악성코드에 현명하게 대처하기 위해서는 사용자 스스로 철저한 보안 의식을 가지고 스마트폰을 사용하는 것이 가장 중요하다. 악성코드들이 대부분 그럴듯한 게임, 유틸리티로 위장하고 있기 때문에 설치 전 반드시 애플리케이션의 허용 권한, 출처, 제조업체, 사용자 리뷰 등을 꼼꼼하게 확인하고 가급적 구글 Play스토어와 같은 공식 배포처를 통해 애플리케이션의 다운로드를 하며 정기적인 스마트폰 전용 백신을 활용하여 악성코드 검사를 해야 할 것이다.

제 2 절 스마트폰이 군사보안에 미치는 영향

1. 군 이동통신의 특성

1) 집단적으로 동일 기지국 사용

평시 주둔지 내에서 대부분의 업무시간을 보내게 되는 군 이동통신 사용자들은 집단적으로 동일한 기지국에 접속해 있게 된다.

이는 제3장 제1절의 표 3-3에서 살펴본 R6의 위험요소에 해당할 가능성이 있다. 특히 이 경우 집단적으로 비인가 WiFi망에 접속 혹은 기지국을 통한 의도된 조작패킷의 배포를 통해 악성코드의 대량 유포가 발생할 가능성이 있다.

2) 동일 국번 사용

군 이동통신 사용자들은 관리의 편의를 위하여 군 이동통신에 가입시 일정한 국번을 부여받아 사용하고 군 이동통신을 해지할 경우 다른 번호로 부여받게 된다.

따라서 특정국번이면 군 이동통신 사용자로 특정할 수 있어 사회공학적 기법[54]을 통한 공격을 시도할 수 있을 것이다.

54) 이는 인간 상호작용의 신뢰를 바탕으로 정상 보안절차를 무력화시켜 원하는 정보를 얻는 공격기법의 통칭이다. 이러한 예로는 전화사기, 이메일 피싱, 보이스 피싱 등이 있으며 개인

3) 임관(최초 개통)후 번호변경 빈도 낮음

군 이동통신 사용자들은 통상 임관시 군 이동통신에 가입을 하고 전역을 통해 군 이동통신을 해지하게 된다. 이 기간 동안 지속적으로 한 번호를 사용하게 되는데 이 점은 간부들의 명함사용, 지휘서신 발송 등으로 인하여 주요직위자의 전화번호가 외부로 유출될 가능성과 함께 4번 항목의 경우와 같이 일상생활을 통해 유출된 전화번호로 인하여 악성코드의 직접적인 표적이 될 수 있는 문제가 발생할 가능성이 있다.

4) 업무 및 일상생활에 공용 사용

군 이동통신 사용자들은 업무용으로 군 전용 스마트폰을 제공받지 않는 이상 통상 1대의 단말기를 업무 및 일상생활에 공용으로 사용하게 된다.

이는 위에서 살펴본 바와 같이 번호변경의 빈도가 낮은 점과 중학교 동창회 연락망 등에 공개된 전화번호를 통해 국정원장의 전화번호가 유출된 것[55]과 같이 동기회 수첩 및 인명록 등을 통해 주요직위자의 개인전화번호가 유출될 수 있는 가능성이 있다.

2. 기능별 군사보안침해 가상시나리오

1) 카메라

최근 스마트폰은 500만 화소 이상의 고화질 카메라 모듈을 장착되어 출시되고 있다. 피쳐폰부터 카메라 촬영 시 촬영음이 발생하도록 기본설정이 되어 있으나, 스마트폰의 경우 무음카메라 앱 등을 제작하여 카메라 촬영음이 발생하지 않게 하여 여성들의 특정 신체부위 등을 촬영하는데 악용되고 있다.

따라서 군사보안을 적극적(소극적)으로 침해할 의도를 갖는 자가 이러한 무음카매라앱을 사용할 경우 군사보안구역이나 장비, 문서 등을 촬영하여 저장・전송을 통한 유포 가능성이 있다

정보의 수집이 용이해지면서 노출된 유명 인사를 목표로 하는 경향이 있다.

55) 조선일보, 2008년 1월 16일, A4면

2) 음성녹음

스마트폰은 내장된 마이크를 통하여 수GB의 저장용량을 다 채우거나 배터리가 모두 소진될 때까지 음성녹음기능을 작동시킬 수 있다. 또한 이 경우 스마트폰이 가슴주머니나 바지주머니 속에 넣고 사용자와 함께 이동하거나 회의시간에 책상 위에 올려둔다는 점에서 사전에 악성코드를 통하여 음성녹음 기능의 작동권한 등을 획득한 경우 무작위로 녹음 및 전송할 경우에 문제가 될 것이다. 예를 들어 무작위의 군 이동통신 사용자에게 악성코드를 유포하고 아침상황회의 시간과 같은 특정시간대를 지정하여 임의로 녹음하고 특정 서버로 전송하게 하는 경우를 들 수 있겠다.

3) GPS

이미 스마트폰 이용자를 대상으로 다수의 무료어플리케이션이 위치정보를 기반으로 한 광고를 제공하거나, 주변검색과 같은 기능을 제공하고 있는데 이는 스마트폰의 GPS기능을 활용하여 사용자의 위치 및 이동정보를 파악하고 있다는 점에서 비롯된 것이다. 이러한 위치정보의 활용은 기업입장에서 대상자를 특정할 수 있는 광고를 제공하고, 스마트폰 사용자의 활용성을 높여준다는 점에서 그 역할을 인정받고 있다.

그러나 이러한 위치정보는 개인의 프라이버시의 영역에 속한다 할 수 있어 임의적으로 활용할 경우 큰 문제가 발생할 가능성이 있다. 사례로 구글과 애플이 사용자의 동의 없이 위치기반정보를 누적 및 임의로 저장하였던 사실이 밝혀져 큰 파장을 일으킨 점을 들 수 있다[56].

만약 군 이동통신 사용자의 스마트폰에 자동으로 GPS 기능을 활성화하고 위치기반정보를 로깅한 후 전송하는 악성코드가 유포된 경우 일정기간 누적된 GPS로그의 분석을 통해 주둔지(가장 많이 누적되어있는 장소), 훈련장(훈련기간 중 이동한 경로 분석), 부대이동경로 등을 파악할 수 있을 것이다.

이러한 점은 적성세력이 주둔지, 부대 전개경로 및 주요직위자의 동선과 같은 자료를 그동안 수집한 수준에 비해 보다 정밀한 위성좌표를 획득할

56) 조선일보, 2011년 4월 26일, A10면

수 있게 된다는 점에서 문제가 된다.

4) USB 저장소 기능

최근 휴대폰들은 16GB 또는 32GB이상의 기본 저장영역을 갖추고 출시되며, 이외에 추가로 외장형 메모리를 사용할 수 있도록 확장 슬롯(slot)을 제공하고 있다. 이러한 저장영역은 USB저장소 기능을 활용하여 컴퓨터와 연결을 통해 USB메모리와 같이 작용하게 되는데, 사용자들은 이를 이용해 음악·동영상을 휴대폰에 전송하여 감상한다.

이 경우 금융회사의 USB통제프로그램이 스마트폰의 USB저장소기능을 완벽히 차단하지 못한 사례가 있는 바, 군의 USB통제프로그램 역시 USB메모리 외 다양한 종류의 스마트폰 OS에 대해 USB저장소기능을 완벽히 차단할 수 있을지는 미지수이다.

만약 완벽히 차단하지 못하게 된다면 내부 전산장비에 있는 정보를 휴대폰에 저장할 수 있고 쉽게 유출할 수 있기 때문에 손쉬운 군사정보 유출의 통로로 작동하게 될 것이다.

5) USB 테더링 기능

테더링(Tethering)은 휴대폰을 통하여 인터넷에 접속할 수 있게 모뎀으로 활용할 수 있는 기능이다. 이 기능을 이용하면 USB 또는 Bluetooth·WiFi 등을 통하여 휴대폰과 군용 노트북, 또는 데스트탑 PC를 연결하여 인터넷을 사용할 수 있게 된다. 즉, 군 인트라넷에 접속된 컴퓨터를 휴대폰의 통신을 이용하여 외부 인터넷에 직접 접속함으로써 내부 보안정책 및 방화벽을 우회할 수 있게 된다.

이러한 테더링 기능은 특히 군용 노트북에 무선랜 기능이나 Bluetooth 기능이 기본적으로 탑재되어 있는 경우 이와 결부하여 군사보안상 위협요소가 될 가능성이 있으므로 군용 노트북의 경우 이러한 기능을 제거하거나 통제프로그램을 설치하여야 할 것이다.

3. 소결론

1) 군 특수성에 따른 스마트폰 보안위협 요소[57)]

군부대의 특징은 폐쇄성이다. 외부인의 출입이 엄격히 제한되어 인가된 인원만이 출입이 가능하다. 내부에서도 보호등급을 구분하여 특별한 시설에는 별도의 인가자만이 출입할 수 있다. 이런 특징인 인원에만 해당하는 것이 아니다. 인가된 물자만이 나가거나 들어올 수 있고 반입되는 자료는 보안상 유해하지 않은지 보안성 검토를 받아야 하며 부대외부로 반출되는 자료에 대해서는 더 엄격한 검토를 받아야만 한다.

네트워크 체계에서도 예외는 아니다. 업무용 전산망은 폐쇄적으로 구성되어 인가된 사용자만이 접속할 수 있다. 인가된 사용자도 비밀번호 변공, 백신 최신화 등 보안정책을 지키지 않으면 접근이 차단된다. 인터넷 사용은 더욱 엄격하다. 인터넷 설치를 위해서는 사전에 장관급 지휘관의 승인을 받아야 하며, 사용전 단말기와 회선에 대한 보안측정을 받아야 하고, 사용 시에는 별도의 계정을 발급받아서 사용하며 인터넷 단말기에는 일체의 군사자료를 저장할 수 없다. 인터넷 사용내역은 서버에 기록되며 외부로 자료를 전송하기 위해서는 보안성 검토를 받아야 하고 이메일 송신내역은 보안부서에서 별도 점검이 실시된다.

이러한 환경에서 스마트폰의 등장은 커다란 위협요소가 되고 있다. 스마트폰의 가장 큰 장점이 언제 어디서든 접속되는 인터넷은 군사보안의 최대 위협요소이다. 일반기업체에서도 정보유출을 방지하고자 스마트폰에 대한 보안을 강화하고 있는 추세이며 이에 대한 솔루션이 출시되어 있지만 이와 다른 군의 가장 큰 차이점은 인터넷이 허용되지 않는다는 것이다. 스마트폰의 첨단 기능과 군사보안 규정의 배치되는 대표적인 사항은 아래 [표 3-7]과 같다.

57) 김영철(2011), 전게논문, pp.58-59.

[표 3-7] 스마트폰의 주요기능과 배치되는 군사보안규정

스마트폰 기능	군사보안 규정
인터넷 검색	승인된 PC에서 인가된 사용자만 사용 가능
이메일 전송	보안성 검토 후 전송, 보안부서 추가점검
사진/동영상 촬영	승인 후 가능, 촬영 후 결과 점검
멀티미디어 기능	MP3, PMP 등 사무실 사용금지
전자서전 기능	전자수첩 사무실 사용금지

출처 : 김영철(2011), p.63.

2) 군사보안위협에 대한 대응책 마련의 필요성

2009년 공군 보안사고 분석 자료에 따르면 정보통신분야의 비중이 42%를 차지하고 있으며 이중 보안사고의 심각성을 인식하지 못하고 사용한 비중이 59%를, 규정된 절차를 이행하지 않아 발생한 사고가 29%를 차지했다[58].

이는 스마트폰이 군 이동통신 사용자에 의해 영내에 반입되는 순간 자의에 따른 군사보안 침해에의 수단이 되거나 자신도 인지하지 못하는 사이에 군사보안 침해의 도구가 될 수 있는 특성을 갖는다는 점에서 스마트폰 사용 확산 추세에 더불어 보안사고 중 정보통신분야의 비중은 점차 증가할 것이다.

이러한 점에서 모바일단말관리 시스템의 도입을 통한 기술적 통제방안의 마련과 스마트폰의 반입과 사용이 군사보안 침해의 가능성이 있다는 점에 대한 지속적인 교육이 필요하다 하겠다.

58) 김영철(2011), 전게논문, p.63.

제 4 장 軍내 모바일단말관리 시스템의 도입 간 예상한계점

제 1 절 모바일단말관리 시스템의 도입현황

1. 민간분야

모바일단말관리 시스템은 앞서 제2장에서 살펴본 바와 같이 스마트폰의 보급의 확산에 힘입어 사내 그룹웨어를 모바일의 영역으로 확장하여 모바일오피스를 구축하려는 가운데 관리측면의 필요성에 의해 등장한 것이다.

따라서 아래 [표 4-1]를 통해 주요 기업의 모바일오피스 도입사례를 보면 이를 통해 어떤 기능들을 활용하고 있는지와, 이미 민간분야에서 상당한 수준으로 이용되고 있다는 점을 볼 수 있다.

[표 4-1] 민간분야의 모바일오피스 도입사례

기 업 명	주 요 기 능
삼성그룹	메일, 결재, 일정, 임직원조회, 연락처 등 그룹웨어 서비스
제일기획	사내트위터, 실시간 게시판, 메일, 결재, 일정, 연락처 등
제일모직	메일, 경엉정보, 영업정보, 물동정보
㈜ 코오롱	전자결재, 메일, 결재, 일정, 임직원조회, 연락처 등
중앙일보	실시간 기사 등록/ 조회, 전자결재, 메일, 결재, 일정, 임직원조회, 연락처 등

출처 : 삼성SDS계열 Mobiledesk의 도입사례 (http://www.mobiledesk.co.kr)

그 외 CJ 제일제당, 하이트 진로, 빙그레, 대우증권, IBK기업은행, 녹십자, 국민건강보험 등 이 모바일오피스를 도입하였으며, 민간분야에서 이의 도입을 통하여 추구하고자 하는 바는 신속한 업무처리 및 의사결정을 통해 외근 및 출장과 같은 물리적 제약을 극복하여 비즈니스 기회 손실을

차단하려는데 가장 큰 목적이 있다고 할 것이다. 그 외 사내 공지사항 및 개별 그룹별 게시판을 통한 임직원 간 커뮤니케이션 및 협업 활성화 , 고객 대응 속도 향상을 도입목적으로 하고 있다.

이외에 눈여겨 볼 사항은 삼성그룹의 경우 삼성그룹의 경우 80여개의 개열사의 10만 여명이 동일한 모바일오피스(그룹웨어)를 사용한다는 점이고 중앙일보의 경우 자체 결재 프로세스와 연동되어 있다는 점인데 이를 통해 민간분야는 대규모 모바일오피스 구축 및 관리능력을 갖추었고 이를 뒷받침할 모바일단말관리 시스템은 상당한 수준으로 발전해 있음을 살펴볼 수 있다.

2. 군사분야

우리 군은 'u-실험사업'의 일환으로 군 전용 스마트폰의 보급과 함께 군사용앱의 개발을 추진하고 있다[59]. 이는 저격수 탄도계산, 무인정찰기 통제 와 비화통화용 앱을 개발하여 사용하고 있는 미국 등의 사례에 힘입어 개발에 착수한 것 이다. 이러한 군사용앱은 인증된 스마트폰에 설치한 후 '국가공공기관 업무 시 스마트폰 보안규격'규정에 따라 외부 망과 분리되어 보안체계가 완비된 군부대내 전용서버를 통해 정보를 전송·공유하는 방식을 채택한 것으로 보인다.

그러나 스마트폰에 대해 이런 군사용앱 외 다른 사용계획은 보이지 않는다 할 것인바, 이는 민간기업의 경우와 달리 군이 모바일오피스를 도입할 경우 군 인트라넷 망과 외부 인터넷망을 직접 연결하게 되고, 스마트폰을 분실할 경우 보안사고의 우려가 있기 때문인 것으로 보인다.

그렇다면 현재 국방부가 '국방 모바일기기 통제체계 구축사업'을 합동참모본부 신청사에서 시범적으로 추진하고 있는 점[60]은 군이 사용자가 개별적으로 반입하는 스마트폰에 대해서는 별도의 활용계획 없이 통제만을 계획하고 있다고 할 수 있겠다.

---

59) 국방일보, 2012년 7월 16일, 2면
60) 국방일보, 2012년 4월 23일, 2면

3. 검토

즉, 군이 '국방 모바일기기 통제체계 구축사업'을 통해 모바일오피스와 연동 없는 모바일단말관리 시스템을 도입하는 것은 위에서 살펴본 바와 같이 군 인트라넷 망과 인터넷 망의 물리적 연동으로 인한 군사보안의 침해우려가 가장 큰 원인이라 할 수 있겠다.

그렇다면 군의 경우 모바일단말관리 시스템의 최초 도입 시 관리서버에 스마트폰을 반입한 사용자와 그들이 사용하고 있는 스마트폰을 등록해야 한다는 점에서 이러한 등록 작업을 영내 반입된 모든 스마트폰을 대상으로 실시할 수 있을지가 의문이다.

제 2 절 도입간 예상되는 한계점

1. 개인프라이버시 침해우려로 인한 사용자의 거부감

모바일단말관리 시스템 도입간 예상되는 군 이동통신 사용자의 거부감은 이를 이미 도입한 금융회사와 최근 불거진 LG전자의 사례를 통해 예상해 볼 수 있을 것이다.

먼저 금융회사의 경우[61] 스마트폰 통제에 있어 아래와 같은 논란이 있었다.

직장에서 임직원 프라이버시는 일부 제한될 수 있다는 것이 일반적인 논리이며 그 동안의 판례였고, 회사는 일을 하는 공간으로 공을 사보다 우선하는 것이 일반적인 입장이었다. 그러나 개인의 스마트폰에까지 금융회사에서 로깅을 하는 등의 통제를 하는 것은 관례를 벗어난 수준의 프라이버시 침해에 해당된다 할 것이다.

따라서 금융회사는 스마트폰에 대한 적극적인 통제의 대상을 어디까지 해야 할 것인지를 결정해야 했다. 스마트폰의 소유권이 임직원 명의이며 고지서가 임직원에게 청구된다면 그 스마트폰은 임직원 개인의 것으로 봐

61) 유길상(2011), 전게논문, pp.45-46. 참고하여 재정리

야 한다. 따라서 임직원의 스마트폰에 대하여 전화 내용을 녹취하거나 보안 프로그램을 통해 이용을 제한하거나 사용기록을 로깅 하는 등의 통제는 할 수 없을 것이다. 다만 개인소유의 스마트폰에 대하여는 업무용으로 이용하지 않도록 조치하고, 금융회사의 전산시스템 및 네트워크에 접속을 허용하지 않도록 해야 할 것이다.

물론 업무용으로 회사에서 지급한 스마트폰의 경우에도 특성상 업무용과 개인 사생활 용도로 함께 혼용되기 때문에 업무용 스마트폰일지라도 통화내용을 녹취하거나 정보의 송·수신내용을 로깅을 하는 방법으로 내부통제수단을 적용한다면 업무시간에 한정하여 적용해야 할 것이고 이에 대한 임직원 개인의 동의를 받아야 하며 녹취 및 로깅 자료에 대한 열람 등에 대하여도 개별적으로 사전 동의를 받도록 하는 등 열람 및 대외제공의 경우에도 준법감시인의 건별 승인을 받도록 하는 절차 및 방법을 구체적으로 제정·명시해야한다는 논란이 있었다.

한편 LG전자의 경우[62] 모든 직원을 대상으로 휴대전화에 '모바일 온'라는 애플리케이션을 설치한 경우에 한하여 회사 출입 시 휴대폰을 반입하는데 필요한 홀로그램 스티커를 부착해주겠다고 하였다. 홀로그램 스티커를 부착하지 않은 휴대전화는 사업장에 반입이 금지되기 때문에 이 조치는 애플리케이션을 설치하지 않는 직원들의 출입을 사실상 금지하는 것이었다.

LG전자는 이 어플리케이션의 설치를 통해 모바일오피스를 구축하여 모든 직원들이 이메일은 물론 전자결제, 주소록, 일정을 확인할 수 있다고 하였으나 그러나 사내 안팎에서는 이번 조치가 임직원들의 개인정보를 감시할 수 있다며 우려를 제기하는 목소리가 있었다.

그 이유로는 모바일오피스를 설치한 스마트폰은 사내에서 카메라는 물론 블루투스, 테더링, 음성녹음을 제한하는 것 외에도 단말기를 분실했을 때 원격에서 기능을 정지시킬 수 있는데 이를 위해서 스마트폰의 유심(USIM)에 접근할 수 있는 권한에 접근할 수 있기 때문이었다.

문제가 된 점은 유심에 휴대전화 가입자 정보와 네트워크 접속 정보, 텍

62)조선비즈, "사생활까지 회사에? LG전자 보안 어플 논란", (http://biz.chosun.com/site/data/html_dir/2012/08/20/2012082001461.html), 재구성

스트메시지, 이메일, 폰북 기록 등 개인부가 서비스 정보가 저장된다는 점이다. 사실상 위치 추적을 비롯해 주요 통화 기록과 메신저 등 개인 정보를 고스란히 담고 있기 때문에 유심을 열람하게 되면 사실상 사생활 기록이 그대로 노출된다는 점이 논란이 된 것이다.

이에 대해 일부 직원들은 스마트폰이 아닌 피쳐폰 모바일오피스가 작동하지 않는 구형 스마트폰으로의 변경을 고민하는 등 사측의 유심 열람 가능성에 대해 반발하였고, 이러한 사항이 언론에 보도되어 논란이 일자 2012년 9월 현재 LG전자의 모바일오피스 구축사업은 보류된 상태이다.

이러한 사례에서 살펴볼 수 있는 점은 모바일오피스에 필수적으로 부가되는 모바일단말관리 시스템은 그 사용여부에 따라 회사 측의 직원에 대한 감시수단이 될 수 있고 이는 개인 프라이버시침해의 우려가 상존한다는 점이다.

군의 모바일단말관리 시스템의 도입에 앞서 고려해야 할 점은 영내 반입되는 스마트폰이 軍의 소유가 아닌 개인의 소유물이라는 점이고, 이 스마트폰에 대해 '군사보안'상의 이유를 들어 일정부분 통제를 하려는 것이 모바일단말관리 시스템의 도입목적이라는 점이다.

그러나 앞서 제2장 제2절에서 살펴본 바와 같이 모바일단말관리 시스템의 기능 상 스마트폰에 설치된 애플리케이션의 목록 및 저장된 파일 등을 열람할 가능성이 있다는 점은 사용자의 개인정보에 관한 접근 권한 및 가능성에 대하여 명확한 기준이 마련되지 않는 한 사용자로 하여금 앱의 목록은 물론 사생활과 관련된 자료의 상시 열람가능성이 있음을 인식하게 되어 개인프라이버시에 대한 침해가능성 및 모바일단말관리 시스템에 대한 거부감을 제기할 수 있다고 본다. 즉, 군사보안과 개인프라이버시의 충돌이 발생할 가능성이 있게 되는 것이다. 특히 이러한 점은 개인 사생활에 민감한 세대인 초급간부 집단을 중심으로 반발이 발생할 가능성이 높아 보인다.

이러한 충돌을 해결하기 위해 군사보안의 목적 달성과 지나친 개인의 프라이버시 침해 방지라는 균형을 이루어야 하고, 어떤 형식이든 프라이버시에 대한 일부 침해가 발생할 수 있다는 점에서 기본권의 침해 논란이

발생할 수 있는바 단순한 훈령이 아닌 법률로 이를 규정해야하며 업무시간에 한하여 혹은 군사보호구역내에서 활동하는 경우에 한하여 통제를 하여야 할 것 이다.

만약 법률로 이를 규정한다면 그 내용은 대략 다음과 같이 규정할 수 있다고 본다. 모바일단말관리 시스템의 운영목적 및 설치대상 및 시스템의 기능을 명시하고, 그 기능을 활용하는 경우 등에 대해 규정해야 한다고 본다. 특히 그 기능을 활용하여 원격으로 감시하는 경우, 예를 들어 개인 스마트폰에 설치된 애플리케이션의 목록을 열람하는 경우는 사전 동의를 받도록 한다, 그 외 사생활 자료(사진, SMS등)의 열람은 군사보안침해 혐의가 있는 경우와 같은 때에 한하여 가능하며 이를 위해서는 영장과 같은 처분을 요한다(단, 본인의 동의가 있거나 범죄혐의의 중대성과 증거인멸의 우려에 의해 긴급성이 요구되는 경우는 사후영장청구)라는 절차 등을 법률로 명문화 하여야 할 것이다.

2. 타인명의의 스마트폰 사용에 대한 통제 불가 우려

앞서 서론에서 살펴본 바와 같이 영내에 반입되는 스마트폰을 군 이동통신망에 등록된 스마트폰, 군 이동통신망에 등록되지는 않았으나 사용자 명의로 된 스마트폰, 그리고 타인명의의 스마트폰 이렇게 3가지로 구분할 수 있을 것이다.

만약, 모바일단말관리 시스템의 적용 대상을 '복무중인 사용자 명의로 된 모든 스마트폰'으로 정의한다면 최초 Agent Software의 설치 및 관리를 위해 각 이동통신 업체로부터 스마트폰을 사용하는 군 간부 및 군무원 등의 명단을 확보해야 할 것이나 이는 현실적으로 불가능에 가까워 보인다.

그렇다면 차선책으로는 '군 이동통신에 가입된 스마트폰'으로 정의를 하여 명단을 확보, 모바일단말관리 시스템을 적용한다고 하더라도 군 이동통신이 아닌 사용자명의의 스마트폰이나 타인명의로 개통한 스마트폰이 단 한대라도 반입되는 한 기밀보호확률은 0이 될 것이고, 모바일단말관리 시

스템이 적용되는 군 이동통신 사용자들의 상대적인 불편 및 사생활침해의 우려만을 초래하여 관리대상이 아닌 타인명의로의 이탈 혹은 업무용으로 피쳐폰을 등록하고 개인용으로는 배우자명의 등 타인명의로 개통한 스마트폰을 몰래 반입하는 등의 현상이 발생 하게 될 것이다.

따라서 모바일단말관리 시스템을 통한 군사보안이란 통제목적의 달성을 위해 적용대상을 영내에 반입되는 모든 스마트폰이라 할 때 본인 명의로 개통하였으나 군 이동통신으로 개통하지 않고 일반으로 개통한 스마트폰의 경우 파악할 수 있을지, 그리고 타인명의로 개통하여 영내에 반입할 스마트폰을 어떻게 파악하여 이를 적용할 수 있을지가 최대의 관건이 될 것이며 최종적으로는 군 이동통신으로의 유인을 통한 획일적인 관리방안이 요구된다 하겠다.

3. 소결론

그렇다면 아직 모바일단말관리 시스템을 적용하지 않은 상황에서 사용자들이 군 이동통신을 사용하지 않는 이유는 무엇일까? 이와 같은 현상이 발생하는 원인으로는 우선 단말기 가격에 있어 보조금이 적용됨이 없다는 점과 군 이동통신의 경우 요금제별 차등적인 망내 무료통화(동일 이동통신사업자에 가입한 군 이동통신 사용자에게) 제공 및 가입비 면제 혜택 외 추가 할인혜택이나 최신 스마트폰에 대한 보험가입 제한, 주요 거점지역에 1개소 정도 위치한 군 이동통신 지점 및 협력업체로 인하여 요금제 변경 및 자동이체 변경과 같은 단순한 업무조차 신분증을 팩스 혹은 Email로 군 이동통신 업체에 발송해서 처리해야 하는 불편함이 있다는 점이다.

즉 정리하자면 경제적인 이유와 각종 불편한 업무절차가 군 이동통신 외 타인명의 개통분에 대한 요인이 된다고 할 수 있다.

그러나 모바일단말관리 시스템의 도입에 있어 최초 Agent Software 설치와 사용자 등록 및 사후 관리에 있어 군은 사기업과 달리 주둔지의 수와 인원의 규모가 비교할 수 없을 정도로 방대하므로 모바일단말관리 시

스템의 설치를 위해 반입통제 및 전수조사를 하는 것은 불가능하다고 생각하며, 이를 위해 다른 요인과 결합을 통한 군 이동통신으로의 유인책 마련이 필요해 보인다.

제 5 장 軍내 모바일단말관리 시스템의 도입 간 예상한계점의 해결방안

제 1 절 전제조건

앞서 제 4장에서 도출한 예상한계점인 타인명의로의 스마트폰 개통 및 개인프라이버시의 해결방안을 모색함에 앞서 다음과 같은 사항을 전제조건으로 본다.

우선 영내 반입되는 스마트폰의 분류(군 이동통신에 가입되고 사용자 명의의 스마트폰, 군 이동통신에 가입되지는 않았으나 사용자 명의의 스마트폰, 타인 명의의 스마트폰) 중 군 이동통신에 가입되고 사용자 명의의 스마트폰에 대하여는 별다른 어려움 없이 모바일단말관리 시스템의 Agent Software를 설치 및 최초 등록을 하고 지속적인 추적·관리가 용이하다는 것이다.

그리고 실제 모바일단말관리 시스템이 정식시행 될 2014년 이후에는 스마트폰 외 피쳐폰이 출시되지 않는 다는 것이며 향후 출시되는 스마트폰은 NFC기능이 기본 탑재되어 있다는 점이다

제 2 절 기술적 해결방안

1. 스마트폰의 NFC 기능과 RFID출입통제 시스템의 연계

1) RFID영문출입통제시범사업간 도출된 문제점

앞서 제2장 제3절에서 살펴본 군 RFID영문출입통제시범사업은 아래 [표 5-1]과 같은 성과를 나타내었으며, 이런 저조한 성과의 원인은 업체의 유지보수 이행수준, 관리자 만족도가 기대치를 만족시키지 못하였기 때문으로 판단된다.

[표 5-1] 군 RFID영문출입통제시범사업의 성과지표

관 점		성 과 지 표	측정결과 (5점 만점)
사용자 관점	출입절차 편리성	위병소출입 이용만족도	3.6점
		통제구역 출입 만족도	3.1점
임무수행 관점	시설보안 강화	출입관리 이력 관리율	정문위병소 87% 아파트 94%
		관리자 만족도	2.0점
		보안의식 향상율	3.4점
기술 및 지원관점	장비운용율 향상	유지보수서비스 수준 이행정도	2.1점
		예비 장비 확보율	0%

출처 : 권혁제(2011), p.39.

사업 추진 간 발생한 문제점 중 본 연구와 연결할 수 있는 부분은 RFID리더기 구축 시스템측면[63]으로 이는 다음과 같다.

사업간 발생한 RFID리더기 고장과 인식률 저조는 68% 수준으로 System의 신뢰도 저하로 위병소의 경우 사람에 의한 정문출입통제를 수기로 중복해서 운용되고 있어 최초 출입통제 자동화 목표는 유명무실해졌다. 또한 DSL구간의 네트워크 불안요소로 망 단절현상이 빈번해 위병소, 제한구역, 통제구역의 수집 자료가 통제서버로 전송이 실패하는 등 체계운용의 제한사항으로 식별되었으며, 예비 장비 미확보로 고장 및 장애발생 시 조치가 불가능하여 장기간 System 서버관리를 방치하는 사례가 발생하였다.

이렇게 직접 발생한 문제점 외에도 RFID경우는 비가시권 통신의 특성상 악의적인 공격의도를 가진 자에 의한 존재가 드러나지 않는 임의의 리더기를 통한 스캔으로 태그에 기록된 정보를 제3자가 손쉽고 은밀하게 판독할 수 있고 장기적으로 태그 정보와 연동된 데이터베이스를 축적 및 이용할 수 있다는 점이 있다[64]. 이 경우 또한 태그정보와 개인정보가 연계될

63) 권혁제(2011), 전게논문, pp.47-48.

경우 개인의 위치, 성향 추적이 가능하다. 따라서 이미 자동차 스마트키 복제와 같은 RFID의 취약 사례가 있는 이상 군 신분증에 RFID태그를 부착할 경우 이러한 공격과 같은 경우를 대비하여 태그에 기록할 정보의 수준에 대한 고려가 필요하다 할 것이다.

2) NFC와 연계한 해결방안제안

본 연구에서 NFC를 RFID출입통제시범사업과 연계하려고 하는 이유는 다음과 같다.

우선 앞서 제2장 제4절에서 살펴본 바와 같이 NFC는 장차 RFID의 영역을 일부 대체하는 수단이 될 것이다. 그리고 NFC의 주파수 대역인 13.56Mhz 대역은 교통카드로 주로 사용되었던 것으로 리더기 등에 대해 오랜기간 안정적인 운영이 이루여 져서 군 RFID시범사업간 논란이 되었던 장비에 대한 신뢰도 해결할 수 있고, 최근 NFC유심을 활용한 모바일 신용카드의 발급 및 안정적인 운용이 이루어지는 점으로 미루어 볼 때 고정형·이동형 리더기와 같은 장비에 있어 상당한 수준의 신뢰도가 확보되었다는 점과 장기간의 운용실적이 있다는 점, 보안성에 대해 입증이 되었다는 점이다.

또한 NFC기능을 영문출입시스템과 연계할 경우 스마트폰의 모바일단말관리 시스템이 작동하게 한 다면 현재 군이 모바일단말관리 시스템의 구성 간 채택한 AP방식[65]의 커버리지보다 넓은 영역인 주둔지 전체를 보호할 수 있고 공유기 실치 및 관리비용 등의 유지·보수에 대한 부담이 적다는 장점이 있으며, 출·퇴근 시각을 가장 확실히 체크가 가능하여 획득한 데이터의 신뢰도도 높다 할 것이어서 이로 인한 시간외 근무수당의 산출 및 비상소집시 전파시간 및 출입시간 확인, 그리고 독립 주둔지 간부들에 대한 근무태도 점검 등의 부수적인 효과를 달성할 수 있을 것이다.

민간에서는 KT텔레캅이 2011년 5월부터 이미 스마트폰의 NFC기능을 활용하여 사원출입증(RFID)을 대체, 출·퇴근 인증 및 사무용기기 개인인

64) 박해종(2012), 전게논문, p.14.

65) 이는 인터넷 접속기능이 배제된 무선 공유기를 활용하여 무선공유기의 전파 반경내 위치시 모바일단말관리 시스템이 작동하도록 하는 방식이다.

증, 그리고 모바일단말관리 시스템의 작동에 활용하고 있기에[66] 군에서도 빠른 시간 내 이와 유사한 출입인증체계를 구출할 수 있다고 판단되며 기존에 기 구축된 RFID영문출입시스템의 활용에 대하여는 차량과 인원으로 구분하여 차량의 경우 RFID출입시스템을 적용하고 인원의 경우는 NFC 출입인증이 필요하다고 생각한다. 그 외 임시방문자의 경우는 휴대폰을 위병소에 회수하는 퀵윈전략 등을 병행하여야 할 것이며, 앞서 RFID영문출입통제시스템 시범사업 간 발생하였던 대대급 예하 부대의 국방전산망 과부하 및 네트워크 품질 불량문제는 출입기록 데이터의 전송을 실시간 전송이 아닌 5~10분간 누적 후 순차 전송하거나 점심시간이나 일과 후 시간 등 망부하가 적은 시간에 전송하도록 조정하여 해결할 수 있다고 본다.

제 3 절 제도적 해결방안

1. 법적 근거의 마련

법적 근거의 마련은 크게 두 가지 측면에서 접근할 수 있다.

법률에 영내 스마트폰의 반입자체를 금지하는 규정이 아닌 '모바일단말관리 시스템'과 같은 통제 프로그램을 설치하지 않은 스마트폰의 반입이 보안규정 위반으로 처벌대상이 된다는 점을 명확히 규정하고, 스마트폰으로 인한 군사보안 침해시의 처벌규정을 명문화해야 한다고 본다.

둘째로는 모바일단말관리 시스템에 관한 규정을 마련해야 할 것이다. 앞서 제4장에서 살펴본바와 같이 모바일단말관리 시스템은 보안유지라는 측면과 동시에 내부통제의 기능을 수행할 수 있다는 점, 그리고 사용자가 반입하는 스마트폰은 업무용과 일상용으로 혼용되어 사용된다는 점에서 군사보호구역 밖 혹은 일과(업무)시간외에는 모바일단말관리 서비스가 작동하지 않음(시간적 공간적 작용한계)을 명확히 규정하고, 설치된 앱 목록 등과 같은 개인의 프라이버시 영역에 관하여는 열람권한자 및 열람사유를 명확히 하고 대상자에게 사전(범죄수사와 같은 긴급을 요하는 부득이한

66) 한국경제, 2011년 5월 24일, 24면

경우는 사후)에 통보함과 최초 설치 시 사전 동의를 받음을 법률로 명확히 규정해야 할 것이다.

이렇게 단순한 훈령이 아닌 법률로 근거를 마련해야 할 필요성은, 앞서 살펴본 바와 같이 개인이 소유한 휴대폰에 대하여 군사보안의 목적상 일정한 통제를 가한다는 점에서 군과 사용자간 특별행정법적 관계에 의해 '법률'에 의한 통제가 필요하기 때문이다. 또한 프라이버시, 즉 개인의 사생활이란 기본권을 일부 제한할 가능성이 있기 때문에 군의 열람가능 한 경우 및 범위 그리고 한계 등을 법률로 규정해야 한다고 본다.

2. 군 이동통신으로의 유인

앞서 제1절에서 전제한 바와 같이 최초 Agent Software의 설치 및 사용자 등록을 통한 모바일단말관리 시스템의 보급과 지속적이고 용이한 관리를 위해서는 영내 휴대폰 사용자인 부 및 군무원을 군 이동통신으로 끌어들여 관리하는 것이 필요하다고 하자.

그렇다면 이를 위해서 경제적 측면과 사용의 편리성이 전제되어야 할 것이다.

1) 경제적 측면의 유인책

현재 군 이동통신의 혜택은 가입비가 무료라는 점, 군 전용요금제별 차등적으로 주어지는 군 이동통신 사용자간(동일 이동통신사업자에 등록된 경우로 제한) 망내무료통화가 사실상 전부이다.

게다가 15만 명에 가까운 넘는 사용자 및 잠재적 사용자가 있는 군 이동통신임에도 불구하고 특정 대리점에 의해 독점적으로 운영되는 구조로 일반 매장이나 인터넷에서 휴대폰을 구입할 때 받을 수 있는 단말기 보조금과 같은 혜택은 조차 없어 통상 동일한 기종의 경우에 10~20만 원 정도를 더 부담하고 구입하고 있는 실정이다.

이러한 현실에서 군 이동통신에 대해 경제적인 혜택을 제공한다면 그 내용은 일정기간마다 공동구매(기기변경 등)의 기회제공 및 단말기 가격의

전부 혹은 일부 부담(단말기 할부금에 대한 일정부분을 국가에서 지원하고 나머지 부분은 개인별 복지자금으로 해결 등), 사용요금의 부가세 면제, 직업의 특성상 고위험 군으로 분류된 탓에 가입이 제한된 단말기 파손·분실보험 등에 대한 단체가입 등이 될 것이다.

이러한 혜택제공은 모바일단말관리 시스템이란 통제에 대한 일정한 대가의 성격과 군 간부에 대한 복지라는 측면에서 고려되어야[67] 할 것이며, 이는 사용자들에 있어 군 이동통신으로의 유인이 되어 모바일단말관리 시스템의 안정적 보급 및 관리에 큰 기여를 할 것이라 생각된다.

혜택의 제공에 필요한 제원은 15만에 이르는 가입자·가입예정자 규모와 장기간 해지나 번호이동 가능성이 낮은 양질의 고객층이라는 점을 이용하여 이동통신 사업자와 구매력을 통한 협상으로 마련할 수 있다고 생각한다.

2) 사용의 편리성

그리고 사용의 편리성 측면에서는 현재 군 이동통신 업무를 직접 처리할 수 있는 대리점이 거점지역별로 1개소밖에 없을 정도로 희귀하다는 점에서 최초 가입은 임관 시 군 이동통신 대리점을 통하더라도 해지를 제외한 요금제 변경권한 및 분실·파손 시 임대폰대여와 같은 업무를 일반 대리점 또는 114 고객센터를 통해 처리할 수 있게만 해도 상당한 편리성을 제공할 수 있다고 생각한다.

이외에 군 인트라넷 망에서 요금제 변경 및 기기변경 각종 신청 등의 업무를 별도의 신분증 제시 없이 인증서를 통한 본인인증을 통해 처리할 수 있다면 편리성이 더해질 것으로 보이나 이는 군 인트라넷 망과 인터넷의 연동이 필수적으로 필요하게 될 것이므로 현실적으로 어렵다고 생각된다.

---

67) 국방부(2011), 『군인복지 기본계획』, 서울 : 국방부, p.28. : 국방부는 군인복지 기본계획에서 간접적 보상을 통한 부가급여형 복지라는 전략을 천명하였고 여기에는 문화·교통·오락시설의 할인제도의 확대가 포함되어있다. 그렇다면 군 이동통신에 대한 할인혜택제공도 이에 포함된다고 할 수 있을 것이다.

3. 내부 컴플라이언스

컴플라이언스(compliance)는 법·명령 등을 준수한다는 사전적 의미를 갖는다. 회사와 같은 조직에서의 컴플라이언스란 통상 내부통제기구 역할을 담당하는 준법감시인과 같은 내부감사기구를 의미하는 것이다.

이러한 컴플라이언스에 대해 금융회사의 내부 컴플라이언스 제도를 살펴보고, 이로부터 군의 모바일단말관리 시스템을 보완할 수 있는 방안을 모색해보고자 한다.

1) 컴플라이언스의 필요성[68]

어느 설문조사에서 직장 동료가 보안규정을 준수하지 않은 사실을 발견한 경우 당신은 어떻게 하시겠습니까? 라는 질문을 하였다고 한다.

이에 미국이나 캐나다 국민은 '신고한다.'라는 비중이 가장 높은 반면 우리나라의 경우에는 '무시하고 그냥 지나친다.'고 대답한 비율이 가장 높았다고 한다. 그 이유에 대한 해석은 분분하지만 우리나라의 온정주의 때문일 것이라는 의견이 많다.

'온정'이란 원칙을 누그러뜨려 따뜻한 마음으로 상대방을 대한다는 뜻이다. 해킹이나 보안 및 내부통제는 모두 사람이 문제이므로 우리나라의 온정주의는 보안 및 내부통제 측면에서는 방해요인이 될 수 있다 직장동료가 규정화된 내부통제 및 보안정책을 지키지 않을 경우 잘못된 것이니 고치라고 알려주거나 내부통제 또는 보안 책임자에게 해당 사실을 알려야 하는데 그렇지 못하기 때문이다.

그런 이유로 내부통제 및 보안을 효율적으로 강제하기 위해서는 내부통제 전산시스템을 개발하여 기술적인 수단을 적용한 컴플라이언스를 갖출 필요가 있다. 단순히 임직원의 윤리의식에 의존하는 선언적 내부통제기준은 사문화되기 쉽기 때문이다.

기술적 측면의 내부통제활동은 임직원의 인식을 전환시켜 다소 불편하더라도 내부통제기준을 반드시 지켜야 하는 직장 문화로 정착 시킬 수 있

68) 유길상, 전게논문, pp.48-50.

는 장점이 있다. 다만, 시스템 구축비용이 소요되므로 위험이 큰 부서부터 적용하는 방법 등으로 선택과 집중이 필요하며, 컴플라이언스 구현을 위하여 다양한 부처 간 협의를 통해 세부기술 및 업무 프로세스 등을 표준화할 필요가 있다.

이와 더불어 내부통제 및 보안의 중심은 사람이므로 임직원을 대상으로 하는 윤리교육과 보안교육을 기술적 내부통제와 병합하여 내실 있게 실시하도록 한다. 내부정보 유출행위는 임직원의 윤리의식의 부족으로부터 시작하기 때문이다. 이와 같은 허위정보 유포, 선행매매 또는 정보유출행위는 임직원 개인의 처벌뿐만 아니라 회사의 평판을 떨어뜨리게 되는 불법행위임을 강조한다. 사실 구성원들은 이런 부당행위에 대한 컴플라이언스 활동에 협조적이지 않기 때문에 이해와 협조를 구할 필요가 있다.

또한 휴대폰은 보안사고 예방관점에서 사용자의 주의와 관리가 절실히 요구되므로 IT조직과 협력하여 올바른 사용방법에 대한 교육을 실시한다. 또한 휴대폰에 대한 보안 가이드북 등 최신 보안자료를 임직원에게 수시로 제공하여 휴대폰을 안전하게 사용할 수 있도록 한다.

2) 금융회사의 내부통제 방안

본래 내부통제란 외부감사의 효율성을 높이기 위해 회사 내부에 적절한 통제기구가 필요하다는데서 비롯된 내부감사인의 활동으로 시작된 것이다. 이는 회사가 관련법규 및 내부정책 절차의 준수, 정확하고 신뢰성 있는 재무보고 체계의 유지 및 효율적인 업무운영 등과 같은 목표를 달성하는데 합리적인 확신(reasonable assurance)을 주기 위하여 회사 내부에서 자체적으로 마련하여 이사회, 경영진 및 직원 등 회사의 모든 구성원이 지속적으로 실행·준수하도록 하는 일련의 통제과정을 말한다.

금융회사의 경우 회사 내 금융거래 등 직무관련 미공개정보를 취급하는 부서의 불건전 영업행위와 불공정거래는 금융시장의 규칙을 위반하는 행위로서 금융시장의 공정성과 건전성을 실추시키게 되므로 각 금융회사 간 내부통제제도를 마련하게 되었다.

전반적으로 컴플라이언스점검의 형태는[69] 아래 [표 5-2]와 같이 내부점

검과 외부점검으로 구분할 수 있으며 내부통제는 내부점검과 관련된다. 최근 금융회사의 내부통제체계의 취약성과 이로 인한 문제점들이 지속적으로 드러나고 있어 내부통제기능을 개선하는 방안을 통해 컴플라이언스 활동을 강화하고 있는 추세이다.

[표 5-2] 금융회사의 통제방안 구분

구 분		내 용
내부점검(내부통제)	컴플라이언스	준법감시인이 조직·구성원 모두가 제반법규를 철저하게 준수하도록 사전적·상시적으로 통제·감독
	내부 감사	내부감사인 이 내부통제조직을 평가하고 각 단위업무에 대한 효율성을 측정하는 등 경영에 관한 사항을 자체감사
외부점검(외부감사)	규제기관에 의한 점검	금융감독원, 감사원과 같은 감독기관에 의한 검사
	외부전문기관에 의한 점검	회사로부터 독립된 외부 감사인 이 행하는 회계감사 및 외부전문기관의 컨설팅 등

출처: 유길상(2011), p.43.

이러한 내부통제 제도 중 오늘날에는 금융회사 임직원이 직무를 수행하면서 법·규정대로 적절하게 수행하고 있는지 감시하고 모니터링 하는 준법감시활동을 보다 효율적으로 수행하기 위해 IT인프라로 구현하는 IT컴플라이언스가 강조되고 있다. 이는 금융거래 등 금융관련 업무 대부분이 IT를 활용하고 금융회사가 고객들의 방대한 개인정보를 취급·보관하고 있다는 점에서 준법감시활동도 IT를 통하여 철저히 대비하기 위함이다. 하지만 IT컴플라이언스의 경우 유선전화나 유선망의 전산장비 및 정보통신수단에 대하여는 내부통제를 실시하고 있음에도 새롭게 등장한 스마

69) 유길상(2011), 전게논문, p.22.

트폰에 대하여는 [표 5-3]과 같은 수준으로의 모바일단말 모범규준의 제정이 논의되고 있는 정도이며, 따라서 내부통제장치 및 보안대책이 없거나 미흡하여 기존 내부통제시스템 및 정보보안의 홀(hole)이 되고 있다는 한계가 있다.

[표 5-3] 금융회사의 모바일단말 모범규준

구 분	전산장비 모범규준	모바일단말 모범규준
적용방법	· 금융회사 소유의 전산장비에 대하여 적극적인 통제 · 개인 소유의 전산장비에 대하여 회사 네트워크에 접속하지 못하도록 접근 통제	· 금융회사 소유의 모바일단말에 대하여는 모바일단말관리, 로깅 등 방법으로 적극적인 통제 · 개인 소유의 모바일단말은 회사에서 사용을 제한(수신으로 한정 등)
임직원의 동의 및 대안 등	· 사생활침해에 대한 반대의견 일부 존재 · 로깅자료에 대한 열람은 개별적으로 사전 동의를 받도록 하는 등 구체적 절차를 마련	· 개인 소유의 모바일단말까지 녹취 또는 로깅 하는 것은 법적으로 불가능하거나 심각한 반대 직면 · 금융회사 소유의 업무용 단말이더라도 녹취 또는 로깅은 주요부서 및 업무시간으로 제한할 필요 ·모바일 오피스 구축을 위해 금융회사 소유의 모바일 단말을 지급할 필요

출처 : 유길상(2011), p.43.

3) 시사점

이렇게 상대적으로 엄격하고 기술의 변화에 신속히 대응하고 있는 금융회사의 경우에도 휴대폰에 대한 내부통제 기준이 마련 중이라는 점에서 군에서 스마트폰 반입에 대한 컴플라이언스를 도입하려는 것은 시기상조라는 지적도 있을 수 있다.

그러나 컴플라이언스란 개념이 조직 및 각개구성원이 제반법규를 준수

하도록 통제·감독하는 것이라 할 때 현행 인트라넷 망 중심의 기술적 통제방안이 상당한 수준으로 발전해 있는 군은 모바일단말관리 시스템의 도입에 발 맞춰 제반법규의 준수를 위한 사전적·상시적 통제 및 감독중심의 체제를 보완해야 한다고 본다. 이의 근간은 모바일단말관리 시스템을 설치하지 않은 스마트폰은 잠재적인 군사보안의 침해요소가 될 수 있다는 점을 인식시키는 것이고 앞서 컴플라이언스의 필요성에서 살펴본 바와 같이 군법교육의 강화로 군사보안침해자에 대한 내부 신고를 이뤄냄으로서 이를 통해 모바일단말관리 시스템으로의 포섭을 이룰 수 있을 것이다.

이에 대한 대안으로 군법교육의 강화와 보안교육의 강화 및 인식의 전환을 유도하여 지위고하를 막론하고 내부적으로 군사보안침해자를 고발하는 방안을 제시하고자 한다.

이를 위하여 지속적인 군법교육이 필요하나 군에서 준법감시인이라 할 수 있는 법무참모가 각 주둔지를 방문하여 군법 교육을 실시하는 것은 물리적인 한계가 있다. 따라서 최초 임관 시 및 각종 교육 과정 간 수료 전 1일(8시간)이상을 군법교육의 날로 의무편성 할 것을 제안한다.

여기서 다룰 군법교육의 내용으로는 공통과정으로 상용정보통신장비에 관한 내용(영내 반입, 사용, SNS를 통한 군 관련사항의 게시[70] 및 계급·과정에 따른 개별과정으로 대민관련 민원 처리 절차, 생활법률(상속, 보증 등) 등으로 현실에 가까운 내용으로 편성하며 국방부 차원에서 표준 교안을 마련하여 일률적인 내용의 교육이 이루어 져야 할 것이다.

또한, 보안위배사항에 대한 사안별 처벌기준을 마련하고 사례를 교육함으로서 보안위배자는 끝까지 추적하여 엄중 처벌한다는 의지를 보여야 할 것이다. 이러한 사례는 국민은행이 행원들에게 업무 마감후 컴퓨터의 마감버튼을 누르면 영업점에서 취급하는 상품에 대해 5문제의 퀴즈를 풀게 함으로서 상품에 대한 이해를 높인다는 점에서 착안[71]하여 매주 수요일 보안의 날 행사간 최초 국방전자결제에 로그인시 O·X형태의 보안 사례 문

70) 2012년 8월 2일자 KBS 뉴스에 따르면 전방사단에 근무하는 부사관이 인접부대 훈련병의 사망으로 인해 행군이 취소되었다며 기뻐하는 내용의 글을 본인의 SNS에 올려서 문제가 된 사실이 있다

71) 조선일보, 2012년 7월 10일, B3면

제(최근 처벌 사례 등) 3~5문제 가량을 풀도록 함으로서 최신 보안침해사례 에 대한 교육을 하는 방안을 제시하고자 한다.

제 6 장 결 론

본 연구는 국내 스마트폰 사용자의 급속한 증가와 이로 인한 영내 스마트폰반입 증가에 따른 군사보안상 위험성 요소를 검토하고, 이에 대비하기 위해 군 당국이 추진 중인 모바일단말관리(MDM) 시스템의 도입필요성과 도입 간 발생할 수 있는 문제점과 이에 대한 대응방향을 제시하고자 하였다.

먼저 스마트폰이 갖는 위험성 요소와 이로 인한 군사보안의 위험성을 요약하면 다음과 같다.

스마트폰은 다양한 응용 애플리케이션의 개발을 위한 개방성, 작은 크기와 가벼움에 의해 높은 휴대성을 갖고 있으나 그만큼 분실의 우려가 높고 배터리로 작동한다는 점에서 PC에 비해 상대적으로 저성능이란 한계를 갖는다. 이는 안드로이드 운영체제 등의 취약성과 맞물려 다양한 형태의 악성코드 개발이 이루어지고 있고, 상대적으로 PC에 비해 낮은 스마트폰 사용자의 보안의식과 결합하여 다양한 유형의 피해가 발생할 것이 예상된다.

스마트폰의 위험성 요소는 군 이동통신 사용자들이 집단적으로 동일한 기지국에 접속한다는 점, 업무 와 일상생활에 공용으로 사용한다는 점과 맞물려 적성세력이나 이에 동조하는 세력이 이 점을 악용할 수 있고, 사용상 부주의로 인해 의도하지 않은 군사보안 침해가 발생할 수 있다.

군은 이런 문제점을 인식하고 그 동안 영내 반입 스마트폰에 대하여 주요 통제구역에 대해 반입통제 전략을 사용하였으나, 15만에 이르는 군 이동통신 사용자와 전국 각지에 주둔하여 직접적인 통제가 어렵다는 한계를 인식하고 현재 민간에서도 최신의 기술인 모바일오피스에 부수된 모바일 단말관리 시스템을 합동참모본부 신청사에 대한 시범사업을 거쳐 2014년까지 사단급 이상 각 제대에 보급을 추진하고 있으며, 이러한 점은 일괄적으로 통제를 적용할 수 있는 기술적 방안이라는 점에서 효과적이라 본다.

그러나 민간의 사례에서 볼 때 사업 추진 간 적용대상자들의 프라이버

시 침해 우려에 기인한 거부감, 이러한 통제를 회피하기 위한 타인 명의의 스마트폰 개통 및 반입 등이 우려되는 바 본 연구에서는 아래와 같은 대안을 제시하였다.

우선 기술적으로는 현재 도입이 상당한 수준으로 진행되고 있는 군 RFID영문출입통제 시스템을 스마트폰의 NFC 기능과 연계하여 출·퇴근 시 위병소에서의 태그를 통해 모바일단말관리 시스템의 작동 및 출·퇴근 시간관리, 시간외 수당 관리 등의 효과를 달성할 수 있을 것이며, 그 외 정책적으로 프라이버시 침해 우려를 최소화하기 위해 법률에 스마트폰 반입에 대한 군사보안 침해가능성에 대응하기 위한 통제 목적, 통제 방안, 통제 수준 및 군사보안 유출 등의 혐의가 있는 경우 원격으로 스마트폰을 통제 및 열람 할 수 있다는 등의 내용을 명문으로 담아야 할 것이다. 그리고 군 복지의 일환으로 군 이동통신에 접근하여 현재 상대적으로 높은 단말기 가격 및 각종 업무처리의 불편 등에 대해 금전 및 편리함을 제공하여 군 이동통신으로 유인을 통한 모바일단말관리 적용대상의 선정과 지속적 관리를 하여야 할 것이며, 보안규정 위반자에 대한 엄중한 처벌방침을 근간으로 스마트폰과 같은 상용정보통신장비의 반입 및 활용에 관한 보안사고 사례 및 군법에 대한 지속적인 교육을 통해 기술적 통제와 부합하는 컴플라이언스(내부통제)를 제안하였다.

본 연구는 모바일단말관리 시스템 도입 간 예상되는 문제점에 대해 대응방향을 제시하였으나, 향후에는 대응방향에 대한 기술적·정책적인 측면에서의 세부적인 검토와 추가적인 연구가 필요할 것으로 생각된다. 기술적 측면에서는 타인명의 스마트폰의 반입에 있어 모바일단말관리 시스템을 탑재하지 않은 스마트폰에 대해 데이터 패킷을 차단하는 등의 방안이 검토될 필요가 있다고 여겨지며, 정책적 측면에서는 모바일단말관리 시스템과 관련된 법률을 마련할 경우 군사보안을 엄격히 요하는 군의 특수성상 구성원에 대한 기본권제한이 어디까지 허용될 것인가의 문제와 맞물려 지속적인 논의가 이루어져야 할 것이다,

【참고문헌】

1. 국내문헌

국방부(2009), 『군인복지 기본계획』, 서울 : 국방부.

권혁제(2011), “RFID/USN 기술기반 軍 실험사업 체계구축 개선 방안 연구”, 아주대학교 석사학위논문

김열수(2011), 『국가안보 : 위협과 취약성의 딜레마』, 파주 : 법문사.

김영철(2011), “스마트폰 활성화 전망에 따른 군사보안 대응방안 연구”, 숭실대학교 석사학위논문

박해종(2012), “군 RFID출입통제시스템을 이용한 이상징후 탐지방법”, 아주대학교 석사학위논문

유길상(2011), “금융시장 건전성을 해치는 모바일단말 위협에 대한 대응방안”, 고려대학교 석사학위논문

이민구 외(2012), “NFC를 활용한 능동형 인증 방법”, 『한국통신학회논문지 제37권 제2호』, 서울 : 한국통신학회, pp.140-156.

이훈(2006), “RFID기술을 적용한 군 출입통제 시스템 구축방안”, 강원대학교 석사학위논문

임상규 외(2011), “스마트 시대의 보안 위협 : EU5의 대응과 시사점”, 『한국위기관리논집 제7권 제4호』, 충북 : 위기관리 이론과 실천, pp.135-150.

임팩트(2012), 『스마트워크 모바일오피스 실태와 전망』, 서울 : 임팩트.

조영갑(2006), 『국가안보학』, 서울 : 선학사

ABSTRACT

Study of control over mobile phones in military

-Focused on mobile device management system-

Seo, Kyong Jin
Major in Military Strategy
Dept. of National Security and Strategy
Graduate School of National Defense Science
Hansung University

The military authorities are proceeding with the project of constructing mobile device control system as a part of 'Demonstration project of applying new excellent common IT technology to defense' in 2012. The core of this project is the adoption of mobile device management system and the authorities are proceeding with demonstration project at the main building of Ministry of National Defense and the new building of Joint Chiefs of Staff for that from August, 2012.

As of September, 2012, smart phone users took 30,876,600 among 54,274,905 mobile phone users and it is reality that the cases of carrying smart phone into the territory increase more due to establishment of smart phone billing system like special billing system for LTE in military mobile communication as well.

Smart phone has the characteristics like openness, portability and serviceability for connection through various access routes, but it causes

various serious problems with regards to security matter concerning the users whose security consciousness is relatively weaker than those who use personal computers as it has the limit that there is a possibility of leaking personal information and impossibleness to apply real-time monitor when malicious code is distributed or the phone is lost.

As its results, the increase of carrying smart phone into the territory can be regarded as that raises the possibility of intrusion into security inevitably in the reality that detection of malicious code rapidly increases in Android operation system that take 87% of domestic smart phone OS today.

So, the adoption of mobile device management system by military authorities can be regarded as the effective technical controlling measure regarding that it can control all members in the military inclusively beyond the simple measure that withdraws smart phones when they access the existing specific areas concerning the possibility of intrusion into military security by carrying smart phone into the territory.

But, like recent issue of privacy invasion that happened during the adoption of mobile device management systems of LG Electronics, there is a possibility of occurrence of opposition to invasion of privacy led by the group of junior officers who is the generation that is sensitive to privacy and there is a possibility of occurrence of cases that carry smart phone of other's name the territory to avoid the application of mobile device management system.

This study suggested the natural distribution of mobile device management system through linkage between RFID access control at main gate of military and smart phone by inventing from the fact the private society operates it replacing the existing RFID pass with NFC function of smart phone and activates mobile device management system of smart phone at the same time of access in technical aspect against the limit that is expected by the adoption of mobile device management system in the

military and reviewed the necessity of preparing for purpose, ground, applicable object and procedure of controlling according to the law as specified in the Constitution regarding that such series of control can cause the dispute of restricting basic human rights.
And it recognized that the inducement to military mobile communication that is capable of continuous easy tracking and management on applicable objects for prompt and successful distribution of mobile device management system together with education of military law based on the cases related with common information and tele-communication equipment that takes the large portion among the security accidents and it is willing to review and suggest a series of alternative plan like inducement method by economic factor accordingly.

【Keyword】 Military security, military mobile communication, mobile device management