모바일 오피스 유형분석을 통한 정보보호관리체계 (ISMS) 정보보호모형의 개선에 대한 연구

최연호*, 이송희**, 최진영***
*고려대학교 디지털정보미디어공학과
**고려대학교 컴퓨터정보통신연구소
***고려대학교 컴퓨터학과
yono72@korea.ac.kr, {shlee, choi}@formal.korea.ac.kr

A Study on Improvement of Information Security Management System (ISMS) Information Security Model through Analysis of the Type of Mobile Office

Yeonho Choi*, Songhee Lee**, Jinyoung Choi***
*Dept of Digital Information and Media Engineering, Korea University
**Institute of Computer Information and Commnunications, Korea University
***Dept of Computer Science and Engineering, Korea University

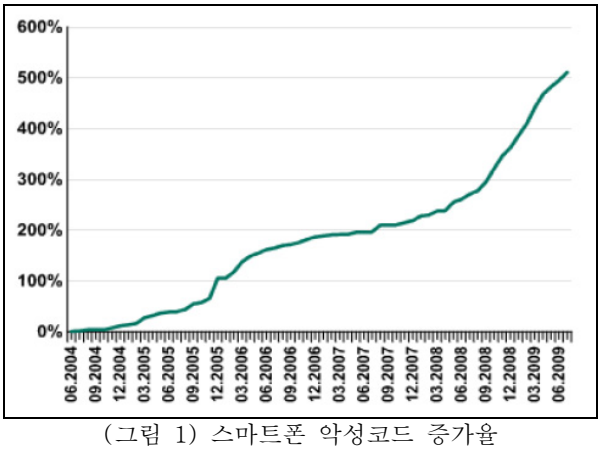
요 약

최근 스마트폰의 발전으로 인하여 기업 및 기관에 모바일 오피스의 도입이 빠르게 확산되고 있다. 모바일 오피스는 업무의 편의성을 제공하지만 반면 무선네트워크의 사용량 증가와 상대적으로 보안이 취약한 스마트폰의 이용의 증가로 인하여 정보유출의 위협이 높아지고 있다. 본 논문에서는 "스마트 모바일 오피스 환경에서의 정보보호관리체계(ISMS)를 확장한 정보보호모형 "[1]에 유형별로 분류한 모바일 오피스를 분석하고 정보보호모형을 발전시켜 모바일 오피스를 도입하려는 기업 및 기관의 보안환경에 적합한 유형을 선택하는 방향을 제시하고자 한다.

1. 서론

세계적으로는 물론 국내에서도 PC 의 기능을 탑재한 휴대폰인 스마트폰이 본격적으로 보급되고 있다. 이에 많은 개인들의 핸드폰이 급속도로 스마트폰으로 교체되고 있으며 기업/기관에서는 모바일 오피스를 도입하거나 준비하고 있다. 하지만 스마트폰이 빠르게 보급되고 무선인터넷의 이용이 늘어남에 따라 스마트폰과 관련한 보안취약점과 사고가 증가하고 있다. (그림 1)에서 볼 수 있듯이 스마트폰이 보급되기 시작하는 2004 년 이후 악성프로그램이 나타나기 시작하였고 2009 년 6 월에는 2006 년을 기준으로 악성코드가 500%가 증가한 걸 알 수 있다[2]. 이는 스마트폰에 PC 와 같은 기능이 내포되어 성능적으로는 우수하지만, 스마트폰에서 발생할 수 있는 다양한 위협들에 대해서는 충분히 고려되지 않은 데에 그 이유가 있다.

이처럼 보안문제가 확대됨에 따라 2010 년 1 월 국정원은 스마트폰으로 내부 전산망에 들어가 전자결재를 하거나 내부 이메일을 열람하는 행위를 제한할 것을 지시한 공문을 공공기관에 송부한바 있고, 2010 년 8 월 독일 정부는 연방정보보안청(BSI) 권고에 따라 공무원들에게 보안 문제를 이유로 블랙베리와 아이폰 사용을 금지했다. 2010 년 8 월프랑스 컴퓨터긴급대응센터(CERTA)는 해커들이 아이폰 등 애플제품에서 사용자 정보의 유출 및 통화 도청이 가능함을 경고했다. 2010 년 8 월 사우디 아라비아 통신당국은 국가보안을 이유로 블랙베리 서비스 중단을 명령하였다[3].



(그림 1) 스마트폰 악성코드 증가율

본 논문에서는 "스마트 모바일 오피스 환경에서의 정보보호관리체계(ISMS)를 확장한 정보보호모형 "[1]을 이용하여 모바일 오피스의 유형별로 보안 난이도를 점검한다. 이후 본 논문은 보안 난이도와 스마트폰의 보안 위협을 통해 ISMS 인증심사 기준을 점검하

여 정보보호모형의 발전모델을 제시하고자 한다.

2. 모바일 오피스 현황과 스마트폰 보안 취약점

2.1 모바일 오피스의 개념

모바일 오피스(mobile office, 이동 사무실)란 언제 어디서나 모바일 단말기(이동통신기기)를 통해 외부에서 회사 업무를 처리할 수 있는 업무시스템이다.

주요 서비스로는 <표 1>과 같이 메일, 전자결재 등의 그룹웨어로 많이 활용되며, 특화현장업무나 기업/기관 내의 음성통화서비스가 있다[3].

<표 1 모바일 오피스 서비스>

서비스	주요 내용
그룹웨어	메일, 전자결재, 회계처리 등
특화업무	현장단속, 시설물관리, 보험상담 업무 등
음성통화	기업, 기관 내에서는 스마트폰을 내부통화 무료, 외부통화는 인터넷전화로 제공

2.2 모바일 오피스의 유형별 분류

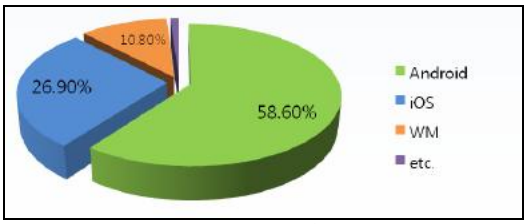
<표 2 모바일 오피스 유형분류>

분류 방식	유형	보안점검 사항
모바일 플랫폼	구축형	활용형의 경우 기업정보가 타 서버에 저장되고, 보안위협에 능동적으로 대처하기 어려움
	활용형	
개발 방식	App 방식	App 방식의 경우 운영체제가 제한적이지만 Web 방식에 비해 보안 우수
	Web 방식	
운영 체제	iOS	운영체제에 따라 보안위협도 달라질 수 있음
	Android	

모바일 오피스는 <표 2>와 같이 모바일 플랫폼, 개발방식, 운영체제에 따라 분류될 수 있으며, 모바일 플랫폼은 기업·기관이 직접 구축하는 방안(구축형)과 사업자의 시설을 활용하는 방안(활용형)으로 구분된다. 특히 활용형의 경우 상대적으로 보안위협에 능동적으로 대처하기 어려우므로 보안체계의 점검이 필요하다.

개발 방식으로는 앱방식과 웹방식으로 나뉘어지는데 앱방식은 속도가 빠르고 보안성이 우수하며 실시간 서비스인 푸시서비스가 가능하다는 장점이 있지만 모바일단말기의 운영체제의 제한이 있다는 점과 상대적으로 비용이 많이 드는 단점이 있다. 그에 반해 웹방식은 하드웨어에 상관없고 어디서나 사용할 수 있지만, 속도 면이나 보안적인 면에서 떨어진다[5].

마지막으로 모바일 오피스의 단말기의 운영체제로 분류될 수 있다. 2011 년 2 월 7 일 모바일 광고 플랫폼업체 라이브포인트에 따르면 (그림 2)와 같이 국내 스마트폰 OS 점유율은 안드로이드가 58.6%로 과반수를 넘은 것으로 나타났고 iOS 26.9%, WM(윈도우모바일)은 10.8% 순이었다[5]. 보안회사인 트렌드마이크로에 의하면 안드로이드는 오픈소스이어서 상대적으로 보안에 취약하다고 한다[9].

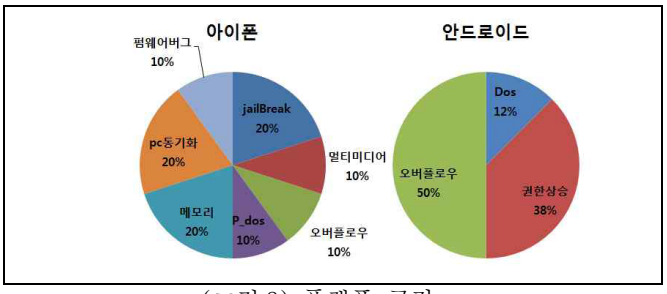


(그림 2) 국내 스마트폰 OS 점유율(출처: 라이브포인트)

2.3 스마트폰의 보안 취약점 분류[4]

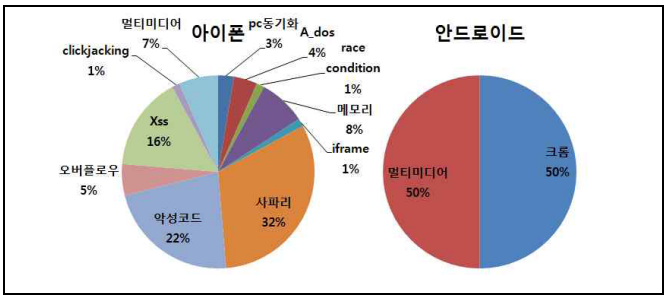
스마트폰 보안 위협 요소는 크게 플랫폼 관련 취약점, 애플리케이션 관련 취약점, 네트워크 관련 취약점으로 나눌 수 있다.

플랫폼 공격은 운영체제의 보안취약점을 이용하거나 자의적 해킹에 의한 것을 말하며 세부 공격으로는 바이러스/웜, 키보드해킹, 시스템 Unlock 등이 있다. (그림 3)와 같이 스마트폰 출시 시에 탑재되어 있는 제조사 펌웨어 S/W 를 변조하여 사용자 등이 조작한 새로운 펌웨어로 교체하는 Jailbreak(아이폰), Rooting(안드로이드) 등은 스마트폰 보안에 가장 큰 영향을 미치는 공격이다.



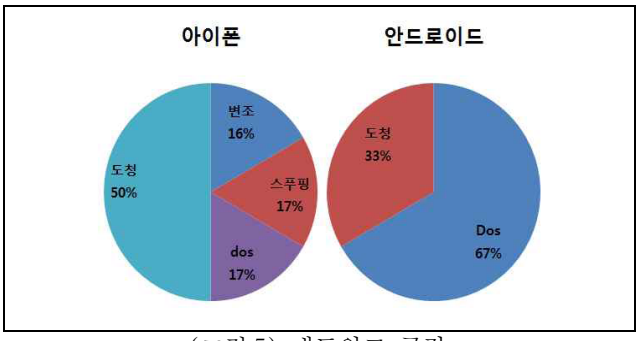
(그림 3) 플랫폼 공격

애플리케이션 공격은 웹이나 마켓에 있는 애플리케이션이 취약점을 이용한 공격으로 금융기관 등의 애플리케이션으로 위장한 피싱 애플리케이션 공격, 겉으론 정상적으로 보이지만 내부에 의도적으로 악의적인 코드를 내장한 악성 애플리케이션 공격 등이 있다. (그림 4)의 결과를 보면 브라우저에 대한 취약점 공격이 많은 것을 알 수 있다.



(그림 4) 애플리케이션 공격

네트워크 관련 취약점은 블루투스, 와이파이 등 접속경로 등과 연관이 있으며 바이러스 감염 및 공격대상이 되는 것으로 와이파이 도청/변조와 DoS 공격 등이 있다. (그림 5)를 보면 도청과 DoS 가 많이 차지하는 것을 알 수 있다.



(그림 5) 네트워크 공격

3. 모바일 오피스 환경에서의 ISMS 를 확장한 정보보호 모형을 통한 점검[1]

이 장에서는 "정보보호관리체계(ISMS)를 확장한 정보보호모형"을 앞에서 살펴본 모바일 오피스 유형별 보안점검사항과 스마트폰의 보안위협을 이용하여 정보보호모형의 개선방향을 찾아보고자 한다.

<표 3>에서는 정보보호모형에 모바일 오피스의 유형에 따라 통제사항의 점검사항의 정도가 아주 중요한 경우 '◎' 표시를, 중요인 경우 '○'를 표시하였다. 그리고 공통적인 점검사항에는 '-'표시를 하였다.

<표 3>" 정보보호관리체계(ISMS)를 확장한 정보보호모형" 을 이용한 모바일 오피스 유형별 점검

통제 분야	통제목적	통제사항	통제내용 요약	모바일 플랫폼		구현방식		운영체제		개선 분야
				구축형	활용형	App	Web	iPhone	Android	
정보보호 정책	정책의 승인 및 공표	정책의 공표	정보보호 정책은 모든 모바일 오피스 이용자가 확실히 인지 할 수 있도록 함	-	-	-	-	-	-	
	정책의 체계	정책문서의 유형	정보보호 정책서와 각 영역별 지침서 수립	-	-	-	-	-	-	
	정책의 유지관리	주기적 검토	변화가 빠른 스마트 모바일 오피스 환경에서 주기적인 갱신과 타당성의 검토	○	◎	-	-	-	-	외부자 보안
물리적 보안	물리적 보안 대책	물리적 접근 통제	위치정보를 연계한 관제 시스템 적용	-	-	-	-	-	-	
	장비보호	주요시스템 보호	중요정보를 담고 있는 저장 매체의 도난을 방지하며 도난 시 원격파기	-	-	○	○	○	○	운영 관리
		장비의 배치	모바일을 통한 카메라 촬영, 녹음기능을 사용 금지함	-	-	-	-	-	-	
시스템 개발보안	분석 및 설계 보안관리	인증 및 암호	모바일 컨텐츠의 암호화 (DRM, 워터마크)	○	◎	○	◎	-	-	
암호통제	암호정책		정기적으로 비밀번호 변경	-	-	○	○	○	○	접근통제, 전자거래보안
	암호사용		영문/문자 등을 조합하여 8 자리 이상으로 설정	-	-	○	○	○	○	
	키 관리		주민등록 번호의 대체 수단(공인인증서, 아이핀, OTP, 보안토크, 생체인식) 사용	-	-	○	○	○	○	
접근통제	접근통제 정책	정책의 내용	외부 접속 시 권한을 제한	○	◎	-	-	-	-	모니터링
	접근통제 영역	네트워크 접근	신뢰할 수 있는 사이트를 방문하고 연결을 통제함	-	-	-	-	○	○	
운영관리	시스템 운영	시스템도입	문서보안/결재보안 솔루션 의 필요	○	◎	○	◎	-	-	운영 관리
	네트워크 운영	네트워크 운영대책	무선 네트워크의 암호화 선택/보안장비 설치	○	◎	○	◎	-	-	
		원격운영 관리	사내 망에 안전한 접속을 위한 IPsec 기반 모바일 VPN 적 용	○	◎	○	◎	-	-	
	악성 소프트웨어 통제		모바일 단말기의 백신설치/업데이트	-	-	-	-	○	◎	
보안사고 관리	대응계획 및 체계	대응계획 수립	모바일 악성코드의 피해를 최소화하도록 침해 대응체계 수립 및 이행	○	◎	-	-	-	-	외부자 보안
	대응 및 복구	보안사고 보고	정보가 유출된 경우 기업에 보고	○	◎	-	-	-	-	
	사후관리	보안사고 분석 및 정보 공유	사고의 정보와 취약점을 공유하고 디지털 포렌식 적용	○	◎	-	-	-	-	
검토, 모니터링 및 감사	법적 요구사항 준수검토	요구사항 명시	업무용 모바일 의 경우 이메일, 메시지 등이 수집되는 사실에 대한 공지 필요	-	-	-	-	-	-	
		준수검토	정보를 제공할 때 정보취급 방침 및 약관을 검토	-	-	-	-	-	-	

<표 3> 의 점검 결과에 따르면 활용형에 비해 구축형, 웹 방식에 비해 앱 방식, Android 에 비해 iOS 가 보안난이도가 상대적으로 낮다는 결과를 알 수 있다. 활용형에 경우 플랫폼의 능동적인 대처를 할 수 없는 것이 가장 큰 문제점이며, 웹 방식의 경우 패킷이 유출될 수 있다. Android 의 경우 구조와 소스코드가 알려져 있어 상대적으로 보안에 취약하다는 것을 알 수 있다.

4. 정보보호모형의 발전모델

이 장에서는 <표 3>에서 살펴본 모바일 오피스의 유형별 보안난이도 결과에 따른 개선분야와 2.3 에서 살펴본 스마트폰의 보안취약점에서 살펴본 내용(운영체제의 변조, 브라우저 이용, 와이파이 위협 등 주요 취약점 관리방안)을 기준으로 정보보호관리체계 인증심사 기준[8]을 재점검하여 6 개 통제분야를 추가하고 4 개 통제분야를 개선한 발전모델을 <표 4> 와 같이 제시한다.

<표 4 정보보호모형(개선)>

통제 분야	통제목적	통제사항	통제내용 요약	비고
외부자 보안	계약 및 서비스 수준 협약 보안 관리	외부위탁 계약 시 보안요구 사항	모바일 오피스 구축 시 보안 요구사항이 계약서 상에 분명히 명시	추가
정보보호 교육 및 훈련	교육 및 훈련 프로그램 수립	훈련계획 교육 및 훈련내용	모바일 오피스에 대한 보안교육 필요	추가
인적 보안	책임할당 및 규정화	인사규정	스마트폰의 탈옥이나 루팅을 통한 보안무력화 대비하여 보안규정 명시	추가
시스템 개발 보안	구현 및 이행 보안관리	구현 및 시험	모바일 오피스의 안전한 구현을 위한 코딩 규약 및 표준	추가
접근통제	사용자 접근 관리	사용자 패스워드관리	패스워드는 저장하지 못하도록 하고 주기적으로 변경하도록 한다.	개선
운영관리	매체 및 문서관리	매체의 폐기	단말기가 폐기되거나 재사용 시 데이타의 삭제 점검	개선
	원격컴퓨터 및 원격작업	이동컴퓨팅	정책수립, 분실 시 정보유출 방지 대책, 보안교육, 공공망 이용 대책	개선
전자거래 보안	전자우편		모바일 단말기로 전자우편 서비스에 대한 가용성 대책수립	추가
	이용자 공지사항		모바일 오피스 이용 시 이용자에게 해킹위험 및 패스워드 관리, 접속관리 등 공지	추가
검토, 모니터링 및 감사	모니터링	접근 및 사용 모니터링	사용자가 시스템 및 네트워크 사용 및 접근이 허용된 범위에 있는지 모니터링하고 정기적으로 점검	개선

5. 결론

모바일 오피스는 기업의 효율성과 빠른 의사결정을 위하여 대기업에서 중소기업으로 급속히 확대될 가능성이 높다. 이는 정보의 유출가능성의 확대 이어질 수 있으며, 보안에 대한 준비 없이는 본디 얻으려 했던 이익보다 정보유출로 인하여 해를 입는 결과를 초래할 수 있다.

본 논문에서 개선된 모바일 오피스 정보보호모형은 이미 모바일 오피스를 도입한 기관/기업에서는 정보보호 점검을 하기 위한 도구로, 도입하려는 곳에서는 해당 기관/기업의 환경에 적합한 모바일 오피스의 유형을 선택할 수 있는 검토자료로 활용 될 수 있다고 생각된다.

향후에는 정보보호모형의 정립을 위하여 설문조사를 통한 검증이 필요할 것으로 본다.

참고문헌

[1] 추연철, “스마트 모바일 오피스 환경에서의 정보보호관리체계(ISMS)를 확장한 정보보호모형 연구”, 2010
[2] KISA, “스마트폰 기반의 악성코드 수집 분석 플랫폼 개발을 위한 연구”, 2010
[3] 한국정보화진흥원 “스마트폰과 모바일 오피스의 보안 이슈 및 대응 전략” 2010.10
[4] 김기연 “스마트폰 보안 취약점 동향”, 2010
[5] http://www.zdnet.co.kr 홈페이지 “모바일 오피스 논쟁…… 앱이냐 웹이냐”, 2010
[6] http://www.edaily.co.kr 홈페이지 “안드로이드 vs 애플 국내에선 누가 승자?”, 2011
[7] 방송통신위원회, 행정안전부, 지식경제부 “2010 국가정보보호 백서”, 2010
[8] KISA “정보보호관리체계 인증심사 기준표”
[9] http://inews24.com 홈페이지 “안드로이드 OS, 아이폰보다 보안 취약”, 2011