情 報 保 護 學 會 誌
第23卷 第2號, 2013. 4

기업의 무선 환경 도입에 따른 정보보호정책 변화 방안

박 종 일*

요 약

기업의 스마트워크나 유연근무제 도입이 활발해 지면서 무선 환경 도입에 대한 직원들의 요구는 증가하고 있으나 Mobility 지원을 위한 기업 내부의 정보보호정책은 현재 유선 인트라넷 기반의 정책을 기반으로 하여, 업무 환경 변화를 적시에 반영하지 못하고 있는 실정이다. 지속적인 스마트워크 환경 도입이라는 거대한 조류 확산에 따라 본 논문은 기존 기업의 유선 중심의 정보보호정책을 분석한 후 무선 환경 도입에 맞게 새로운 통합 유무선 정보보호정책에 대한 방안을 제안한다.

Ⅰ. 연구 배경 및 목적

최근 기업 내 스마트폰, 스마트패드를 활용한 모바일 업무 환경의 급속한 확대로 인해 기존의 유선, 인트라넷 중심의 정보보호기반 환경에서 벗어나 무선, 이동 환경에서도 유연하게 근무할 수 있는 정보보호 방안에 대한 기업의 요구가 점차 증대되고 있다.

이에 따라 기업 정보보호 담당자 입장에서는 스마트 단말기의 기업 내부 정보 접근 및 유출에 대한 문제 발생 가능성도 점차 증가 할 수 있다.

본 논문은 모바일 환경에서 정보보호 담당자 관점의 기업 정보 유출에 대한 기술적, 정책적 방지 방안과 직원 입장의 업무 유연성 확보를 위한 정보보안 정책 변경 요청을 절충 할 수 있는 기업의 정보보안변화 방안에 대해 정책적 측면의 고려사항과 변화 방향에 대한 현장 기반의 연구를 수행 하는데 목적이 있다.

Ⅱ. 관련 연구

2.1. 기업의 정보보호정책

기존 기업의 유선 기반 정보보호정책 문서의 경우 대부분 ISO 12207, 27001을 기반으로 정보시스템 감리 점검 프레임워크이나 정보보안 관리시스템 구동 환경에서의 정보보호방침에 대한 요건을 명시하였으며 아래와 같은 요소를 포함한다.[1]

(1) 보안 요건 및 목적을 적절하고 명확하게 나타냄
(2) 보안 위험은 비용 효율적인 방법으로 관리됨
(3) 법률 및 규정 준수
(4) 조직의 보안 목적을 보장하기 위한 통제의 도입 및 관리에 대한 적절한 구성의 충족
(5) 조직의 정책 , 지침 및 기준 준수
(6) 고객을 위한 정보 보안

대부분의 기업의 정보보호정책 정책서는 위에서 제시한 점검 항목을 수용하여 각 기업의 특수한 환경에 맞는 방안을 문서화하고 이를 통제 시스템으로 구축하는 방식으로 관리되고 있다.

2.2. 기업의 정보보호 관련 용어정의

‘정보’란 관찰이나 측정을 통하여 수집한 자료를 실제 문제에 도움이 될 수 있도록 정리한 지식 또는 그 자료를 의미하고 유출이란 귀중한 물품이나 정보가 불법적으로 국가나 조직의 밖으로 나가버림을 의미한다.

‘정보유출’이란 종이나 전자적으로 된 문서의 정보를 취득하여 불법적으로 국가나 조직 밖으로 나가는 것을 의미하며, 기업에서 정의되는 내부 정보는 ‘부정경쟁방지 및 영업 비밀 보호에 관한 법률’에서 영업 비밀 부분에 해당한다.

‘정보보호정책서’는 정보보안에 관한 CEO의 경영적

* 엠트리소프트 대표 (pji@mtreesoft.co.kr)

의지, 주요 보안 목표 및 지침 정의, 정보보안 준수 및 지침 준수, 책임 등을 명시하는 정보보안관리체계의 최상위 문서를 의미한다.

'정보자산' 정보보안 활동에 의해 안전성과 신뢰성이 유지되어 보호해야 할 가치가 있는 대상으로 지식재산권, 연구개발 정보, 기술상 정보, 경영상 정보 등의 유·무형의 정보 데이터와 정보 데이터를 저장/전송/처리하는 문서 등 매체/소프트웨어, 장비 등 전산시스템/시설/인원 등[2]

Ⅲ. 무선 환경의 보안 위협

3.1. 무선 환경의 개념

무선 환경이라 함은 포괄적으로 모바일 인터넷(Wireless Internet) 환경이라고 해석할 수 있다. 유선에 반대되는 의미로 무선(Wireless)의 종류는 현재 LTE(4G), WCDMA(3G), Wi-Fi, WiBro, Bluetooth 네트워크를 통한 양방향 데이터 통신 방식을 통해 인터넷(인트라넷)에 접속하여 데이터 통신을 이용하는 것으로 정의 할 수 있다. 본 논문에서 무선 환경은 LTE, WCDMA, Wi-Fi를 통해 스마트폰, 태블릿 노트북등 이동성 및 휴대가 가능한 단말기를 활용하여 기업 업무를 처리할 수 있는 환경이라고 정의한다.

3.2. 스마트 디바이스의 업무 활용

다양한 스마트 디바이스의 보급 확대와 기업의 비용 절감, 업무 효율화 실현을 위해 개인이 자율적으로 구입하여 소유한 스마트 디바이스를 직장에서 업무용으로 사용하는 경우를 BYOD(Bring Your Own Device)라 정의한다.

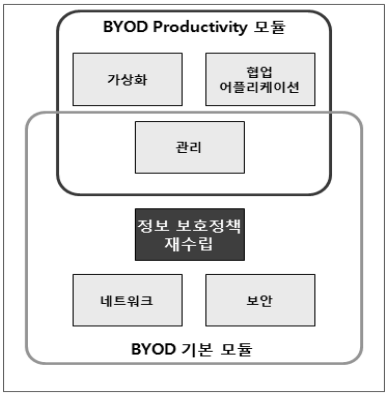
BYOD는 기업의 입장에서 다양한 장점이 있는 동시에 보안이 담보되지 않을 경우 보안 측면에서 기업의 주요 불안 요인이 될 수 있다는 단점도 있다. 많은 기업이 보안상의 문제로 회사 내외부에서 개인 디바이스로 업무 처리를 금지하고 있으나. 최근 직원들의 언제 어디서나 기업 데이터에 접근하여 이동 중 업무를 처리하고자 하는 요구사항은 점차 증가하고 있다. IDC에 따르면 직원들이 개인 소유의 디바이스로 기업 정보에 접근하도록 허용하는 IT 관리자는 40%에 불과한 반면, 이와 같은 방법으로 기업 데이터에 접근하고자 하는 직원은 이미 70%에 이르고 있다.

또한 그림1의 기업 IT 관리자의 스마트워크 도입에 따른 기대 수준을 보면 생산성 향상(58%)과 보안성 향상(55%)이 비슷한 수준으로, 보안에 대한 인식도 생산성 만큼 중요한 항목으로 인식하고 있다.

〔그림 1〕 스마트워크 도입에 따른 개선 기대 수준

이러한 조사 결과를 무시하더라도 현 시점에서 BYOD 트렌드를 부정하는 것은 의미가 없다. BYOD는 이미 빠르게 현장에서 확산되고 있으며, IT 관리자가 갖고 있던 대부분의 보안적 우려는 현실이 되었다. 승인되지 않은 디바이스로 인한 보안 위협 가능성이 증가하고 있으며, 업무 데이터 손실 및 규정 위반, 그리고 인프라 통제력 상실과 같은 리스크들이 현재 기업의 정보보안 환경을 위협하고 있기 때문이다.

그럼 과연 현재 상황에서 정보 보안 담당자로서의 임



〔그림 2〕 BYOD 고려사항

무는 무엇일까? 최선의 방법은 BYOD를 받아들이고 다양한 디바이스 플랫폼에서 기업이 제공하는 정책과 솔루션을 기반으로 직원들이 안심하고 업무를 수행할 수 있도록 기업의 전반적인 모빌리티 보안 인프라 및 정보보호정책을 빨리 재수립함으로써, BYOD가 안정적, 효율적으로 업무에 활용될 수 있도록 하는 것이다.

또한 발생할 수 있는 리스크(단말 분실) 및 보안 위험 요소(해킹)들에 대해 방어적 절차와 대응 방안을 수립하여야 한다.

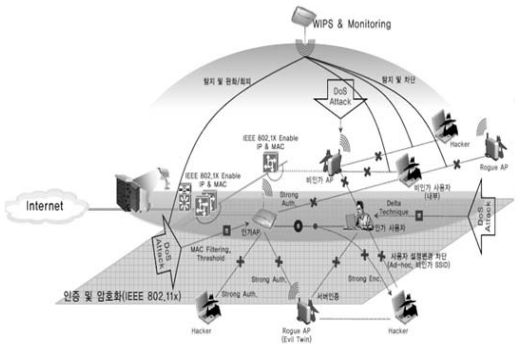
3.3. 무선 환경의 보안 위험 요소

이동통신망(LTE, WCDMA)에 비해 속도 및 가격 면에서 이점을 가진 무선랜(Wi-Fi)을 통한 기업 데이터 접속 요구가 많아지고 사설, 공공 통신망 회사에 의한 무선랜 설치는 해당 주파수에 혼선이 될 정도로 증가하였다. 하지만 무선랜 접속의 편리성 이면에는 무선 전파 수신 범위 내에서 아래와 같은 네트워크 및 단말에 대한 여러 보안 위험 요소를 통해 정보 누출의 위험성도 증가하고 있다.

(1) 도청 및 무선 스캐닝
(2) 서비스 거부 공격
(3) WEP 및 WPA 키 크래킹 공격
(4) 불법 AP 및 단말에 의한 공격
(5) 스마트 디바이스 플랫폼의 장애 악성코드
(6) 스마트 디바이스 내 정보유출형 악성코드
(7) 크로스 플랫폼 형 악성코드

무선랜 환경에서의 무선 데이터 보안 접속 방법은 Ad-hoc Mode와 Infrastructure Mode로 구분 가능하며, 내부의 Rogue AP 또는 보안 취약 AP를 통한 침투가 보안에 가장 위험하다.[3]

위와 같은 무선 환경에서의 보안 위협을 해결하기 위해 기밀성 및 무결성 제공과 인증, 접근제어 및 키관리 기술 등과 같은 무선보안 기술과 침해방지 기술을 통해 기업 내부망의 불법적 데이터 유출 가능성을 방지할 수 있다. 또한 정보보호정책서에도 무선 보안 위협에 대해 보안 구역 내 무선 환경에 대한 '물리적 보안 지침' 및 '네트워크 보안 지침'에 불법적인 AP 접속과 멀웨어(malware) 이식의 가능성, 위장 AP 또는 모바일 핫스팟을 통한 문제에 대해 무선 보안 위협요소와 관리방안을 명시해야 한다.



〔그림 3〕 무선 침해 방지 기술

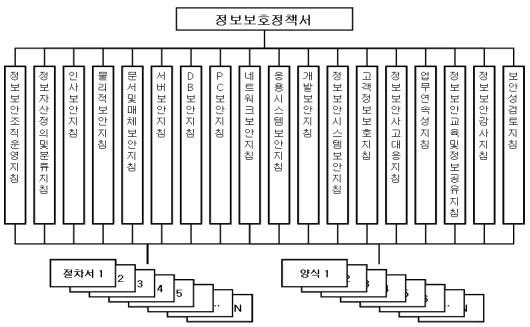
Ⅳ. 기업의 정보보호정책서 변화 방안

이 장에서는 위의 무선 환경의 보안 위험에 대해 기업의 정보보호정책에 대한 변경 범위와 변경 요소에 대해 정의하고, 안전한 기업 내 무선 환경을 보장하고 향후 발생 가능한 보안 위협에 대해 정보보호 담당자가 무선 환경에 대한 보호 조치와 함께 정보보호정책서를 개정할 수 있는 방안을 제시한다.

4.1. 기업의 정보보호정책서

그림4 는 일반적인 기업의 정보보호정책서 체계로 기존 PC기반의 유선 중심의 정보보안 기본 원칙 하에서 지침, 절차, 양식 등 문서와 문서의 구성 체계 형태로 수립되어 있으며, 정책적으로는 직원들의 정보자산 접근에 대해 비밀성, 무결성, 가용성을 보장하는 방안으로 수립되어 있다.

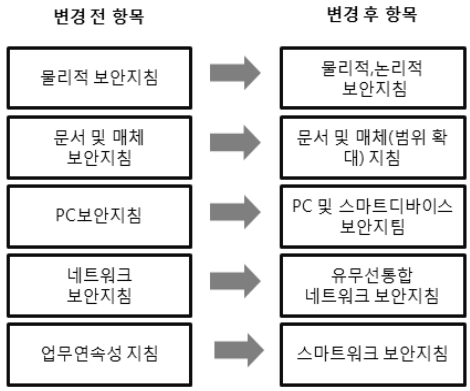
또한 정보보안 관리체계는 기본적으로 효율성, 효과성, 안전성, 신뢰성 확보를 목적으로 수립되고 변경 유



〔그림 4〕 기업의 정보보호관리체계- 예시

지되고 있다.

기업의 업무 환경을 스마트 디바이스 기반의 유무선 통합 업무 환경으로 전환될 경우 보안담당자는 정보보호정책서에서 직접적으로 '물리적 보안지침', '문서 및 매체보안지침', 'PC보안지침', 네트워크보안지침', '업무연속성지침'에 대해 무선 환경에서 발생할 수 있는 다양한 보안 요구사항과 다양한 디바이스 플랫폼에 걸쳐 이를 적용할 수 있도록 하는 모바일 디바이스 관리 시스템(MDM)에 대해 정책서 내에 관련 내용을 수정 보완하여 변화 관리하여야 한다.



〔그림 5〕 정보보호관리정책 변경 예시

그리고 업무 연속성 지침을 기반으로 하는 보안관리 활동에 있어서도 스마트 디바이스와 무선 환경 도입에 따른 효율성과 효과성을 확보할 수 있는 스마트워크 보안 지침으로의 세부 항목에 대한 보안 활동 명세를 수정 보완하여야 한다.

이를 위해 스마트 모바일 기기에 의한 보안위협에 대응하기 위한 보안 인프라(예를 들면 MDM 서버, 인증서버, 테더링 감시 프로그램, WIPS, 구간 데이터 암복호화, VDI,)에 대한 도입 방안과 활용 절차에 대한 정의도 필요하다.

인적 보안 지침과 관련하여서는 업무 직군 및 업무 환경(외부 이동 환경을 구체적으로 명시)에 따라 내부망과 외부망 접근 방식 및 관리 체계에 대한 업무 재정의를 통해 무선 환경에서 직원들이 정확한 업무 가능 영역을 인지할 수 있도록 해야 하며, 해킹, 무선 스캐닝과 같은 외부 침입 위협에도 사전 보안 교육을 통해 인지하고 대응할 수 있어야 한다.

Ⅴ. 결 론

지금까지 기업의 무선환경 도입에 따른 보안 위험성 및 이에 대비한 정보보호 관리정책, 체계 변화를 통해 스마트워크 환경에서도 안전한 기업 업무 수행을 보장하고 향후 발생 가능한 보안 위협에 대해 선제적 방어 체계를 구축하기 위한 유무선 위험 관리 솔루션의 필요성도 확인하였다. 다만 이러한 무선 및 스마트 디바이스 도입을 단순히 사업 환경 변화에 대한 대응이라는 측면에서 소극적으로 접근하기 보다 스마트워크와 같은 업무의 유연성 확보와 전사 차원의 일하는 문화, 조직 체계 변화 입장의 보안 정책 변화 방안으로써 고민하고 지속적으로 직원들의 행태를 분석하여 보안정책에 대해 변화 관리하는 방안을 염두에 두고 "어떻게스마트워크 환경에서 보안 문제를 해결 할 것인가" 라는 공격적 생각으로의 전환을 통해 현재 상황을 극복하는 방식을 생각해 볼 필요가 있다.

참고문헌

[1] 방송통신위원회, "스마트워크 활성화를 위한 정보보호 권고 해설서", pp. 80-86, 2011.12

[2] 김현신 "모바일 인터넷 환경에서 정보유출방지를 위한 보안감리 점검항목", 석사논문, pp. 24-25, 2011.

[3] 김신효, '차세대 무선랜 보안 기술 동향', pp. 2-4, 2013

약어정리

AP	Access Point
BYOD	Bring Your Own Device
LTE	Long Term Evolution
MDM	Mobile Device Management
WPA	Wi-Fi Protected Access
WEP	Wired Equivalent Privacy
WIPS	Wireless Intrusion Prevention System
VDI	Virtual Desktop Infrastructure

〈著者紹介〉

박 종 일 (PARKJONGILL)
2010년 8월 숭실대학교
산업공학/지식경영 석사
현재 : 엠트리소프트 대표, 정보화 전략기획 컨설팅, 모바일 솔루션 개발
<관심분야> HTML5, 모바일 플랫폼, 스마트워크, 정보보호정책