한국전자정부의 Smart Office 구현

박용석

세종사이버대학교

정보보호대학원 주임교수

Smart Office Implementation for Korea m-Government

Yongsuk Park

Graduate School of Information Security, Sejong Cyber University

E-mail : yongspark@sjcu.ac.kr

요 약

세계적인 전자 정부의 발전에 맞추어, 한국의 전자정부는 지난 몇 해 동안 그 발전을 거듭해왔다. 국제 연합 (United Nations) 에 의하면 전에는 한국 전자 정부는 세계 10위권 밖 이었으나, 몇 해 전부터는 세계 1위에 이르게 되었다. 지속적으로 여러 국가 기관들, 즉 안전행전부와 미래 창조과학부 등이 다양한 전자 정부 활성화 전략(전자 정부 3.0 등)을 제시 하고 추진 중에 있다. 하지만 세계 경제 포럼의 국가 네트워크 준비 지수를 보면, 한국은 무선통신이 그 취약점이며, 이는 한국 공공기관의 유무선 통신 활성화와 최근 추세인 BYOD (Bring Your Own Device) 와 Smart office 구현에 부합하는 데 취약하다. 본고는 선진국 사례 및 정책 등을 분석하고 한국 정부에 적합한 BYOD 서비스 구현 및 그 보안을 알아본다.

ABSTRACT

Korean e-goverment has shown its development phase upgrade following the world' e-government evolution. By United Nations, Korea was ranked number one in e-government yet it was not even in top ten for past years. Even now, a number of Korean government organizations such as Ministry of Security and Public Administration and Ministry of Science, ICT and Future Planning have presented and executed various directions and strategies (for example, e-gov 3.0). On the other hand, World Economic Forum put Korea out of top 10 in Networked Readiness Index and hence wireless mobile communication of Korea is a weak point making difficulties for smart office and Bring Your Own Device (BYOD) implementation. This paper details the analysis of leading countries' strategies and policies on m-Government and provides some suggestions for Korean m-government.

키워드

전자정부, 보안, SE-Linux, 정책

Ⅰ. 서 론

세계적인 전자정부의 발전에 맞추어, 한국의 전자 정부는 지난 몇 해 동안 그 발전을 거듭해왔다. 국제 연합 (United Nations) 에 의하면 전에는 한국 전자 정부는 세계 10위권 밖 이었으나, 몇 해 전부터는 세계 1위에 이르게 되었다. 2010년도 기준으로 UN 전자정부 발전 순위 1위, 온라인 참여지수 1위, ITU ICT 발전 지수 1위이다 [1].

여러 국가 기관, 즉 안전행전부와 미래 창조과학부 등이 지속적으로 다양한 (전자 정부 3.0 등)

전자 정부 활성화 전략을 제시 하고 추진 중에 있다. 하지만 세계경제포럼 (WEF) 네트워크 준비 지수(networked readiness index) 순위는 세계 10 위권에 들지 못하며, 이는 한국은 무선통신이 그 취약점으로, 한국 공공기관의 유무선 통신의 활성화와 최근 추세인 Smart Office 와 BYOD (Bring Your Own Device) 에 부합하는 데 취약하다. 본고에서는 BYOD 에 강한 선진국 사례 및 정책 등을 알아보고 대한민국 정부에 적합한 BYOD 서비스 구현 및 그 보안을 알아본다. 본론에서는 선진국들의 구체적 사례들을 분석하고 한국의 제도 및 현황을 비교하고 결론에서는 비교 분석을 통한 보안의 방향성을 도출한다.

II. 본론

미국 정부는 오바마 정부가 시작되면서 투명한 정부와 IT 인프라 비용 삭감을 위해 연방 정부기관내의 클라우드 서비스 (Cloud First) 를 추진하였으며, 이와 연계되어 강한 보안을 추구하는 SE (Security Enhanced) Linux를 기반으로 한 SE Android 프로젝트[2]와 무선 단말기가 군 목적 등의 최고 수준의 보안이 아니어도 어느 정도의 민감한 보안을 규정하는 미 표준을 국가 공공기관인 NIST (National Institute of Standards and Technology) 의 FIPS (Federal Information Processing Standards) 인증을 통하여 정하고 있다.

영국 정부는 국민과 기업에게 보다 나은 서비를 제공할 수 있는 “보다 나은 정부” 건설을 이라는 목표 달성을 위하여 “정부 현대화 백서” 를 추진하고 정보보안에 관하여 정보보호분야국가기술국인 CESG (Communications-Electronics Security Group)가 정책부서와 사업부서로 나뉘어 공공정보기술 및 통신 시스템의 안전을 위한 정보보호 관련 제품 및 서비스책임 보안 정책 지침서 및 표준발간 정보보호정책 개발 및 자문을 맡고 있다.

독일 정부는 Federal Office for Information Security (BSI) 가 암호 장비 개발 및 IT 제품 및 서비스에 대한 인증과 정부 네트워크에 대한 IT 보안을 담당하며 추가적으로 국내 및 국제 표준에도 참여하고 있다.

미국의 정부는 GSA (General Services Administration) 가 FSSI (Federal Strategic Sourcing Initiative) Wireless Program을 통하여 통신업체 (AT&T, Verizon 등), 단말기 업체, 보안기관 등과 공조하여 보안, 낮은 가격, 안정성, 관리 등을 이루고 있다. 구체적으로 GSA의 FSSI Wireless Program 은 각 통신사와 서비스 수준 (Service Level Agreement) 을 여러 단계로 계약을 맺고 공공 기관에게는 활용 가이드라인을 제공하게 된다. 또한 보안 스펙 개발 및 인증기관 (예, NIST 의 FIPS 140-2, NSA 의 Security Enhancement) 과 협력하여 유무선 서비스의 보안 수준을 인증을 한다. 추가적으로 공공 기관의 구성원의 서비스 현황을 관리 할 수 있는 웹 포털 제공하고 공공 기관의 성공 사례를 교류하고 향상책을 관리하게 된다. 추후 공공 기관은 각 기관이 필요한 서비스 수준과 보안 수준을 선택하여 진행하게 된다[3].

SiMKO [4] 는 독일 정부에서 공공기관에 사용하기로 한 무선 단말기를 위한 보안 기술이다. 기본적으로 미국의 NSA SE 와 유사하여 한 단말기에 다른 프로파일을 활성화하여 2개의 OS를 사용한다. 이에 따라 하드웨어와 소프트웨어에 견고한 보안 환경을 제공한다. SiMKO 보안 기술의 주요 특징을 보면, 첫째, 개인과 공공기관의 mobile OS를 독자적 운영이 가능하고 둘째, 보안에 민감한 camera, WLAN, VoIP를 보안 지원 한다. 셋째, e-mail, calendar, contacts 등 Data Application을 지원한다. 넷째, VoIP (Voice Over IP)를 highly secure encryption method 로 지원하고 다섯째, 가정에서 업무를 볼 수 있도록 tablets 과 notebook을 지원하는 등 여러 가지 안전하고 효과적인 업무 환경을 지원한다.

한국에서는 안전행정부가 전자정부의 주관 기관이며 총괄 기획 및 조정을 하고 국가정보통신인프라기관협의회, 한국정보화진흥원(제도운영 및 기술지원), 회선서비스그룹(통신사업자), IP응용서비스그룹(통신사업자)가 협조하여 국가정보통신서비스 즉 GSN (Government Network Service) 을 구성 및 운영한다[5]. 즉 이용제도 마련은 안행부와 한국정보화진흥원 (NIA) 가 인프라의 구성은 국가 정보 통신 사업자가 그리고 그 서비스를 이용 기관이 (국가 공공기관 및 지자체) 가 활용하게 된다. 이를 통하여 보안성, 생존성 및 통신 품질을 보장 및 관리하고 있다. 하지만 아직 무선 단말기에 대한 구체적 제도는 없는 상태이다.

이에 따라, 우리는 몇 가지 문제점을 제시 해본다. 첫째 중복 투자이다. 여러 기관이 기존에 가지고 있는 인프라에 대해여 중복 투자를 하고 있으며, 높은 통신비 구조를 가지고 있고 가이드라인이 부족하며, 중앙 관리 기관 기능을 하는 역할을 하는 기관이 없다. 둘째, 활성화의 부족으로 서비스 품질, 단말기, 보안상의 문제를 들 수 있다. 셋째, 보안 결여 및 적절한 보안 정책이 없다. 즉 미국 NSA SE 시스템과 GSA FIPS 와 같은 명확한 가이드라인 제공과 공공기관에서 인증을 받고 사용할 만한 규제가 없다. 넷째, BYOD 도입을 위해서는 시중보다 저렴한 가격과 기관 별 각기 다른 가입 혜택 계약 조건 등 고려해야할 사항 등이 있다. 다섯째, 서비스 품질이다. 즉, WiFi, 펨토셀, 기지국, 서버 등의 적절한 설치 및 관리가 필요하다.

Ⅲ. 결 론

해외 사례를 비추어 볼 때, 미국 GSA에서 추진하는 FSSI Wireless Program 은 통합적으로 관리하지 못하고 중복 투자, 및 안정성확보를 못하고 있는 한국 전자 정부의 제도의 향상 방향성을 보여 준다. 미국의 NIST FIPS 나 NSA SE 보안 인증은 보안 수준에 따른 다른 검증된 인증을 원활하게 할 수 있는 방향성을 한국 전자정부에 보여 주고 있다. 또한 영국과 독일에서의 사례에처럼, 단말기 제조사로부터 보안 API를 받아 자체적으로 보안 수준을 setting 할 수 있는 보안의 유연성을 확보하는 데 도움이 될 수 있다.

참고문헌

[1] “국가정보화백서,” 한국정보화진흥원, 2010.
[2] “Securing Android-Powered Mobile Devices Using SELinux,” A. Shabtai, Y. Fledel, Y. Elovici, IEEE Security & Privacy, Vol. 8 , Issue 3, 2010 , page 36 - 44.
[3] "GSA Managed Mobility Program," Jon M. Johnson, www.gsa.gov, 2014
[4] "Security for mobility- Think Bigger," A. Alkassar, A. Stett, RSA conference 2009
[5] 국가정보통신서비스 이용지침서, 안전행정부, http://www.egovnet.go.kr/, 2013