국방 스마트워크 보안 이슈 및 고려사항

송 일 선* 한 영 섭* 임 회 성* 백 진 욱**

목 차

1. 서 론

정보통신 기술의 발전 및 관련 인프라의 확대로 인해 사용자들은 언제 어디서나 다양한 정보를 접할 수 있게 되었다. 그리고 이러한 기술발전을 밑바탕으로 하여 기업 및 정부에서의 업무 효율을 높이기 위한 다양한 방법이 시도되고 있다.

스마트워크는 정보통신 기술을 이용하여 시간과 장소에 얽매이지 않고, 언제 어디서나 편리하게 일할 수 있는 업무 환경을 의미한다[1]. 스마트워크는 원격지에서도 근무지와 비슷한 환경에서 근무 할 수 있는 스마트워크 센터, 이동 중에 모바일 단말을 이용하여 실시간으로 업무 수행이 가능한 모바일 오피스, 자택에서 IT기기를 활용하여 업무를 보는 홈 오피스, 그리고 회사 내 정보 체계 등 업무 환경을 개선하여 보다 효율적인 업무 환경을 구축하는 스마트 오피스 등으로 구분 할 수 있다. 스마트워크를 도입하기 위한 기관 및 기업에서는 스마트워크 유형별 특징 및 각 조직의 현 업무 특성을 고려하여, 이에 적합한 스마트워크 환경을 구축하여야 한다.

스마트워크를 도입하게 되면 업무 효율 상승, 비용 절감, 일과 삶의 조화 등 다양한 효과를 거둘 수 있다. 이러한 여러 가지 장점으로 인해 이미 미국, 일본, 네덜란드 등 선진 국가에서는 각 국가별 특성에 맞는 스마트워크를 도입하여 운영 중에 있으며, 이를 더욱 활성화하기 위한 정책 마련 등 스마트워크에 대한 관심이 집중되고 있다.

이와 같이 효율적인 스마트워크 도입을 위해 기관 및 기업에서 중요하게 고려해야 할 사항 중 하나가 바로 보안 문제이다. 스마트워크 환경에서는 외부에 위치한 사용자가 기업 내 정보 체계에 접속하여 업무를 수행하기 때문에, 여러 가지 보안관련 문제가 발생할 수 있다. 특히 국방환경에서는 보안 문제가 민감한 사안이므로 원활한 스마트워크 도입을 위해서는 보안 요소들을 식별하고, 이를 해결하기 위한 대처방안을 수립하는 연구가 필요하다.

따라서, 본고에서는 2장에서 스마트워크 보안에 관한 연구 동향을 살펴보고, 3장에서는 국방 환경에서 스마트워크 도입 시 생각해 보아야 할 여러 가지 보안 이슈에 대해 알아본다. 4장에서는 국방 스마트워크 도입을 위한 고려사항을 관리적·물리적·기술적 보안 관점으로 구분하여 살펴보고, 5장에서 추후에 진행되어야 할 스마트워크 보안에 관한 연구 방향 제시와 함께 결론을 맺는다.

2. 스마트워크 보안 연구 동향

2.1 스마트워크 정보보호 연구 동향

스마트워크 도입이 활성화 되면서 스마트워크 환경에서 기관 또는 기업의 내부 정보를 보호하기 위한

* 국방기술품질원
** 안산대학교 금융부동산정보과

다양한 연구가 진행되고 있다. 스마트워크 환경에서 정보보호를 위해서는 우선적으로 대표적인 보안 위협에 대한 분석과 함께 보안 요구사항 분석이 필요하다[2]. 이 연구에서는 스마트워크 센터 근무 또는 이동 근무 환경에서 제3자에 의한 보안 위협, 단말기 도난 및 분실에 의한 보안 위협, 내부 정보 시스템으로의 원격 접속기술 사용 시 통신 환경의 취약성 등으로 인한 보안 위협, 그리고 PC나 모바일 단말기에 감염된 악성코드에 의한 보안 위협 등을 제시하고 있다. 그리고 이러한 보안 위협에 대처하기 위한 요구사항으로 방화벽, 백신 및 침입탐지 소프트웨어와 같은 기술적 보안 요구사항, 단말기 보안 요구사항, 그리고 정보자산 구분 및 관리 체제, 교육 등의 기업 준수 정책과 사용자 계정, 통신 경로 및 단말기 관리와 같은 관리자 및 사용자 준수 정책을 제시했다.

스마트워크 보안 위협요소 분석을 기반으로 보안 대책이 마련되어야 한다[3]. 이 연구에서는 물리적, 소프트웨어, 네트워크, 모바일 센터와 같은 스마트워크 보안 위협 요소와 보안 요구사항을 분석하고, 이에 따른 보안 대책을 제시했다. 보안 대책의 경우, 패스워드 및 PKI 인증서 등을 이용한 사용자 및 단말 인증 대책, 코드서명 및 인가된 SW 접속 허용 등을 포함한 앱 보안 대책, MDM(Mobile Device Management)을 이용한 단말 분실/도난 대책, 플랫폼 구조변경 자동 탐지 및 멀티태스킹 기능 제어와 같은 플랫폼 보안 대책, 그리고 TPM(Trusted Platform Module)과 같은 하드웨어 기반 단말 보안 대책을 제시했다.

2.2 국방 정보보호 연구 동향

국방 환경에서도 통신, 네트워크, 단말 등과 관련한 보안기술 연구가 진행되고 있다.

국방환경에 무선 네트워크 도입을 위한 연구[4]에서는 IEEE802.11b/g 기술을 중심으로 무선보안기술을 분석하고, 검토되어야 하는 고려사항을 제안하였다. 기술적 검토분야의 경우, VPN(Virtual Private Network), 스마트카드, PKI(Public Key Infrastructure), 생체인식 등을 이용한 접근 통제, ACL(Access Control List) 기반 MAC(Media Access Control) 주소 관리를 통한 클라이언트 접근 통제, 보안상 취약한 프로토콜 식별 및 제한 등의 프로토콜 관리와 같은 내용을 제시하였다. 정책적 검토분야는 무선 네트워크 프로토콜 통제, 무선네트워크 도입에 따른 위협식별 및 평가 계획, 보안 감사 및 교육 등을 포함한다.

국방 환경에 스마트 모바일 단말 도입을 위한 연구[5]에서는 모바일 단말 도입에 따른 보안 위협 요소 분석과 함께 모바일 단말 보안기술 동향을 소개했다. 이 논문에서는 현재 미군 및 국토안보부와 국방부 등에서 블랙베리(Black Berry) 및 안드로이드(Android) 운영체제 기반 스마트 단말기를 사용하여, 전장을 포함한 다양한 국방 서비스에 활용하는 사례를 설명했다. 스마트 단말의 경우 개방형 플랫폼 사용에 따른 보안 취약성, 다양한 네트워크 경로를 통한 위협요인, 단말기 도난 및 분실로 인한 개인 및 그룹 정보 유출 위협 등을 가지고 있다. 이러한 보안 위협 요소를 해결하기위해 MTM(Mobile Trusted Module) 및 가상화 기반 보안을 포함하는 플랫폼 보안기술, 코드 사이닝(Code Signing)과 같은 앱스토어 보안 기술로서의 서비스 보안기술, 원격보안관리와 단말암호화 기능을 포함하는 데이터 관리기술, 그리고 침해단말 접속제어 및 무선 IPS(Intrusion Prevention System) 기술 등을 포함한 네트워크 보안기술 적용을 제안했다.

국방 전산망에서의 침해사고 대응체계 개선을 위한 연구[6]에서는 통합 로그센터 구축을 제안했다. 본 논문에서 제안한 로그분석 모듈과 리포팅 시스템을 이용하여 이종의 전산 인프라에서 발생하는 다양한 로그정보를 분석 및 통합함으로써 전산망 침해사고로부터 신속한 대응이 가능하도록 하였다.

3. 국방 스마트워크 보안 이슈

행정안전부, 방송통신위원회 등 정부 주요부처의 스마트워크 추진에 이어 국방부 및 국방기술품질원 등 국방관련 기관에서도 스마트워크 추진을 위한 연구가 진행되고 있다. 국방 관련 기관의 경우 다른 기관에 비해 보안에 보다 엄격한 기준을 가지고 있으므로, 스마트워크 도입을 위해서는 다각도로 보안위협 분석 노력이 필요하다.

국방 환경에 스마트워크를 도입하기 위해서는 먼저 외부에서의 국방망 내 정보 이용과 관련한 보안 이슈

를 해결해야만 한다. 국방망 내에는 군 관련 자료가 유통되고 있으므로 비인가자에 의한 국방망 침해시 국방관련 자료가 외부에 노출 될 수 있다. 따라서 현 국방 정책상 국방망은 외부접속을 금하는 폐쇄망으로 운영되고 있으며, 외부와의 연계 등 보안 위협이 될 수 있는 부분은 보안심사를 거친 일부자료를 제외하고 그 이용을 엄격히 제한하고 있는 실정이다.

국방 스마트워크 센터에서의 주요 보안 이슈로는 비인가자 출입통제, 공용PC 사용 정책, 국방망/외부망 활용 및 연계 방안 등이 있다. 스마트워크 센터의 경우 국방망 사용을 전제로 하면, 공용PC 사용 시의 보안 이슈 등을 제외하고 기존 근무지에서의 보안 이슈와 크게 다르지 않다. 물론 신규 스마트워크 센터 구축은 국방망에 대한 접근점 증가에 따른 잠재적 보안 위협을 가지고 있으므로 이에 대한 대책이 필요하다.

국방 환경에서 모바일 오피스의 주요 보안 이슈로는 외부 사용자의 국방망 내 정보이용 정책, 단말기 분실·도난 대책, 단말기 보안 관리 및 인증 방안 등이 있다. 먼저 모바일 오피스 활용에 따른 보안 위협을 최소화하기 위한 체계적이고 합리적인 수준에서의 논리적·물리적 망분리 검토가 필요하다. 또한 아직 스마트폰과 같은 모바일 단말기 보급의 활성화가 시작된 지 얼마 안 되는 시점이기에 플랫폼 신뢰성 등 고려해야 할 사항이 많이 남아 있다. 모바일 단말기는 이동성이 주는 편리함과 동시에, 분실 및 도난의 위협이 존재하며, 악성코드와 같은 보안위협에 취약한 특성을 가지고 있다. 이와 함께 모바일 단말의 다양한 통신 및 부가 기능으로 인한 보안 위협이 존재하며, 특히 탈옥(Jailbreak) 및 루팅(Rooting)과 같이 보안에 위배되는 행위에 대한 대처가 필요하다.

국방 환경에서 스마트 오피스 환경 구축을 위한 주요 보안 이슈로는 레거시 시스템과의 연계 보안 및 신규 기술 적용을 위한 보안취약성 분석 이슈 등이 있다. 신뢰성 있는 스마트 오피스 설계를 위해서는 기존 레거시 시스템과의 연계 보안 검토가 필요하며, 각종 보안 위협을 다각적이고 통합적으로 파악할 수 있는 환경 구축이 필요하다. 또한 통합커뮤니케이션, 정보공유, 클라우드와 같은 최신 정보기술 및 개념을 현 정보체계에 적용해야 하며, 각 기술 및 개념이 가진 보안 취약점을 분석하고, 이에 대한 대책을 마련함으로써 국방 환경에 적용을 검토 해 볼 수 있다.

4. 국방 스마트워크 보안 고려사항

앞서 살펴본 보안 이슈를 바탕으로 국방 스마트워크 도입 시 검토해야 할 보안 고려사항을 관리적·물리적·기술적 관점으로 나누어 살펴보고자 한다. 관리적 보안은 스마트워크를 도입하기 위해 조직 내부의 정보보호 체계를 정립하고, 정보체계의 이용 및 관리 절차를 수립하고, 비상사태에 대비하기 위한 대책을 마련하는 등 보안 관리의 전반적인 정책 및 절차와 관련된 관점을 나타낸다. 물리적 보안은 비인가자 접근 통제, 주요 시설물 설계 등 각종 스마트워크 설비 및 시설에 관련된 물리적 대책을 포함하며, 기술적 보안은 정보자산 및 시스템에 기술적으로 적용 가능한 네트워크·시스템·어플리케이션과 같은 관점에서의 보안을 의미한다.

4.1 스마트워크 센터

국방 환경에서 스마트워크 센터 구축을 위해서는 입지 선정에서부터 많은 이슈를 가지고 있다. 아직까지 외부에서 원격으로 국방망에 접속하는 것을 엄격하게 금지하고 있기 때문에, 국방망 사용을 위해서는 그 위치가 제한적일 수밖에 없다. 하지만 보다 유연한 스마트워크 센터 구축을 위해서는, 외부에서도 일부 업무를 볼 수 있는 환경 구축이 필요하다. 현재 보안심사를 거친 일부 자료를 이용 할 수 있도록 국방망 데이터를 망 전환장치를 통해 외부망에 제공하고 있지만 극히 제한된 업무범위 내에서만 이를 허용하고 있어, 사실상 외부에서의 업무 활용도가 높지 않다. 따라서 우선적으로 업무분석과 정보자산 분류 등을 통해 현 국방망 및 외부망 구성체계에서의 업무 활용 가능성 재검토가 필요하다. 그리고 이렇게 검토된 내용을 바탕으로 외부망에서의 정보체계를 재구성하고, 이를 복합인증 및 가상사설망(VPN)과 같은 보안기술을 이용하여 제한적으로 접속을 허용한다면, 국방망 기반 스마트워크 센터가 아닌 외부 스마트워크 센터를 활용한 업무수행도 일부 가능할 것으로 보인다.

스마트워크 센터 구축 시 공용PC 사용에 따른 보안 위협 분석과 이에 대한 대책 마련도 필요하다. 스마트워크 센터 내 공용PC를 이용할 경우, 업무수행에 따른 각종 자료가 PC에 남아있을 수 있으며, 각 자료에 이용권한이 없는 사용자가 이를 악용할 경우 문제가 생길 수 있다. 따라서, 스마트워크 센터 이용을 마쳤을 경우 PC 내 자료 삭제를 위한 정책 및 솔루션 도입이 필요하다. 이 외에도, 국방환경에서 스마트워크 센터 도입을 위해 검토가 필요한 관리적·물리적·기술적 요소들이 있으며 이를 (표 1)에 기술하였다.

(표 1) 국방 스마트워크 센터 보안 고려사항

구분	고려사항
관리적 보안	○ 보안 체계 수립 • 관리적·물리적·기술적 보안 체계 마련 • 정보보호 거버넌스 연계 검토 ○ 보안 정책/지침/절차 제정 • 침해사고 대응절차 마련(정보유출 및 위변조, 분실신고, 정보유출 방지 보호조치 수립 등) • 이용환경 제한 지침 마련(보안 검토 SW 설치 준수, 이동 저장매체 사용제한, 지정 통신수단 사용 등) ○ 보안 담당자 및 조직 구성 ○ 주요 자산 식별 • 접근 통제 정책 수립 포함 ○ 이용자 관리 • 사용자 인증 및 권한 관리 • 사용자 계정 및 패스워드 관리 등 ○ 이용자 보안 교육 및 안내 ○ 보안 감사 • 보안체계 수립 내용, 정책, 지침 등 충족 여부 점검 • 보안 문제점 파악 및 보완적용 ○ 이용자 모니터링
물리적 보안	○ 출입 통제 • 센터 출입인원 통제 • 센터 내 특정지역 접근 통제 • 출입권한 승인 및 변경 관리 • CCTV 설치 및 운영 등 ○ 장비 보안 • 공용PC 보안 • 네트워크 장비 보안
기술적 보안	○ 운용 서버 및 시스템 보안 • 시스템 구성 및 설정 관리, 침입 차단, 보안 운영체제 적용 등 ○ 네트워크 보안 • 암호통신, 침입차단, 유해트래픽 차단, 네트워크 취약점 분석, 로그관리 및 모니터링 등 ○ 운용 어플리케이션 보안 • 사용자 인증, 개발 보안관리 등 ○ DB 및 데이터 보안 • 데이터 접근 제어, DB 로그관리 및 모니터링, 암호화 등

4.2 모바일 오피스

스마트워크 센터 구축 시 보안 이슈와 마찬가지로, 모바일 오피스 역시 외부에서 모바일 단말기를 이용하여 내부 정보 이용이 필요하며, 이때 비인가자 접속 및 해킹, 악성코드 배포 등 다양한 보안위협 및 이슈가 발생할 수 있다. 이러한 보안위협으로부터 벗어나기 위해서는 우선적으로 국방망과 분리된 외부망을 구성하고, 모바일 오피스 사용이 가능한 업무분석을 통해 보안 위협이 크지 않은 업무부터 단계적으로 모바일 오피스 환경에 적용이 필요하다. 또한 모바일 환경에서 가장 빈번하게 일어날 수 있는 단말기 분실 및 도난 등에 대처하기 위해 단말기 원격제어 기술을 활용한 대비책을 마련해야하며, 사용자가 이를 인식하였을 경우 즉시 관련 조직 또는 기관으로 연락이 취해질 수 있도록 교육이 필요하다. 또한 악성코드 등 보안 위협에 대비하기 위해 바이러스 백신, 주기적 보안패치 및 펌웨어 업데이트가 가능한 플랫폼을 적용하고, 통신시에는 모바일 VPN 등 보안이 갖추어진 환경에서 이용해야 한다. 그리고, 모바일 오피스 이용을 위한 인증을 위해 사용자 및 단말의 복합 인증과 같은 대책과 함께 네트워크에 접속하는 모든 기기의 보안상태를 검사해 안전이 확인된 기기만 접속시키는 NAC(Network Access Control) 등의 솔루션 적용 검토가 필요하다.

아직 국방 환경에서는 모바일 단말기의 사용을 제한하고 있으며, 특히 플랫폼이 오픈되어 있지 않은 애플의 iOS기반 단말기는 국내 행정안전부에서도 보안성 검토 등의 이유로 모바일 전자정부 시스템에서 제외하고 추진되고 있다. 하지만 앞서 제시한 모바일 오피스 보안 적용 방안 및 아래의 모바일 오피스 보안 고려사항 등을 면밀히 검토하고 적용한다면, 국방 환경에서도 안전하고 신뢰성 있는 모바일 오피스 환경을 구축할 수 있을 것이다.

(표 2)는 국방환경에서 모바일 오피스 도입 시 검

(표 2) 국방 모바일 오피스 보안 고려사항

구분	고려사항
관리적 보안	○ 보안 체계 수립 • 관리적·물리적·기술적 보안 체계 마련 • 정보보호 거버넌스 연계 검토 ○ 보안 정책/지침/절차 제정 • 단말기 보안 정책, 통신 및 네트워크 보안 정책, 소프트웨어 보안정책, 사용 보안 정책 • 모바일 기기 사용자 지침, 컨텐츠 개발 지침, 앱(App) 검증 지침 등 • 침해사고 대응절차 마련(단말기 분실/도난 정보유출 및 데이터 위변조에 따른 행동요령, 보안조치, 원격제어 방안 등) • 이용 환경 제한(메모리슬롯, WPAN, 외부기기 자동 접속 제한, 저장 데이터 제한 등) ○ 적합 업무 및 서비스 분석 ○ 모바일 단말기 정보관리 ○ 보안의식 제고 및 사용자 교육 ○ 보안 감사 및 관리
물리적 보안	○ 모바일 단말관리 및 원격제어 • 단말 분실시 원격잠금 및 원격파일 삭제
기술적 보안	○ 모바일 단말기, 사용자 인증 및 접근 제어 기술 ○ 어플리케이션 취약점 분석/관리 ○ 악성코드 및 스팸 관리 ○ 네트워크 장비인증, 침입 및 유해 트래픽 차단 ○ 모바일 VPN 등 암호화 통신 ○ 네트워크 로그 분석 ○ 단말기 보안 플랫폼 적용 • 바이러스 백신, 보안패치, 펌웨어 업데이트 등 ○ 모바일 단말관리 및 원격제어

토가 필요한 보안 고려사항을 나타낸다.

4.3 스마트 오피스

스마트워크라고 하면 보통 스마트워크 센터 또는 모바일 오피스를 떠올리지만, 사실 스마트워크의 핵심은 조직 내부의 정보체계를 개선하여 보다 효율적이고 지능적인 정보체계를 구성함에 있다. 이러한 스마트 오피스 환경 구축을 위해 국방환경에 통합 커뮤니케이션(UC: Unified Communication)과 정보공유와 같은 스마트 오피스 체계를 적용함으로써 업무 효율 및 편의를 증대시킬 수 있다.

(표 3) 국방 스마트 오피스 보안 고려사항

구분	고려사항
관리적 보안	○ 보안 체계 수립 • 관리적·물리적·기술적 보안 체계 마련 • 정보보호 거버넌스 연계 검토 ○ 스마트 오피스 보안 정책/지침/절차 제정 • 통합 커뮤니케이션 운용 지침, 보안 관리 절차 개인정보보호방안 등 • 정보 공유 시스템 권한 관리, 검색 운용 지침 등 • 데스크탑 가상화 및 각 클라이언트 별 보안 정책 마련 ○ Security as a Service(SecaaS) 적용 방안 수립 ○ 사용자, 프로세스, 시스템의 리소스접근 방안 마련 ○ 모바일 오피스 연계 보안 검토
물리적 보안	○ 구내교환망(PBX) 등 통합커뮤니케이션 장비 보안 관리
기술적 보안	○ 레거시 시스템 연계 보안 ○ 스토리지 암호화 ○ 사용자 권한 및 인증 ○ 공동거주(Co-residence) 탐지 및 하이퍼바이저 취약점 검토 ○ 악성코드 및 스팸 관리 ○ 네트워크 장비인증, 침입 및 유해 트래픽 차단 ○ 통합 로그 분석 ○ 기술적 취약점 분석 • OWASP Top 10 검토 등

(표 3)은 국방환경 내 스마트 오피스에서 검토가 필요한 보안 고려사항을 나타낸다.

4.3.1 통합 커뮤니케이션

통합 커뮤니케이션은 메신저, 이메일, 전화, 영상회의 등 모든 의사소통 수단을 하나의 시스템으로 통합한 환경을 말한다. 의사소통을 위한 기술이 발전하면서 보다 다양한 방법으로 커뮤니케이션 할 수 있게 되었으나, 각 시스템들이 통합되지 않고 산재되어 있어 이를 활용하기 어렵거나 불편한 점이 있었다. 통합 커뮤니케이션을 도입하면, 사용자가 이용할 모든 의사소통 수단을 통합하여 제공함으로써 사용자는 언제 어디서나 사무실과 같은 환경에서 서비스를 제공 받을 수 있다. 또한 통합 커뮤니케이션을 모바일 오피스와 연계하면 스마트워크가 추구하는 업무 환경에 한 걸음 더 가까워진다. 하지만 이러한 장점에도 불구하

고, 여러 가지 보안 위협들로 인하여 국방 환경 내 도입이 미루어지고 있으며, 특히 VoIP나 모바일 오피스와의 연계 등은 아직 적용이 어려울 것으로 보인다. 따라서, 우선 외부 전화망과 연동되는 부분은 음성전용회선을 이용한 망분리를 통해 기본적인 통합 커뮤니케이션 환경을 구축하고, 모바일 오피스와의 연계 보안 검토 등을 통해 단계별로 그 기능을 확장해 나가야 할 것이다.

4.3.2 정보 공유

협력, 집단 지성 등 구성원들 간의 정보 공유와 참여의 개념이 확산되면서, 조직 내 업무 수행 시 팀원 및 동료의 업무 수행 관련 정보가 활용될 수 있도록 많은 연구가 진행되고 있다. 조직 내 정보 공유 시스템이 적용되면, 불필요한 업무 수행을 줄이고, 집단 지성 등 다수의 업무 노하우를 활용 할 수 있으며, 이러한 결과로 업무 수행 효율 및 산출물의 품질을 높일 수 있다. 이러한 정보공유 환경은 클라우드 서비스와 같이 개인의 데이터와 자료 등을 중앙에 집중시켜 권한에 따라 언제든지 공유 및 활용이 가능하게 하고, 개인 업무용 PC에 조직 관련 자료를 남기지 않게 함으로써 조직 내부 자료의 통합관리를 통한 정보보호와 같은 부수적인 장점을 가지고 있다. 하지만, 이와 같은 비대면 협업 환경에서는 업로드된 자료에 오류가 없을 것이라는 신뢰를 바탕으로 협업이 이루어지며, 만약 데이터에 대한 악의적인 훼손 등 무결성을 침해하는 요인이 발생하게 된다면 그 결과는 이를 참조하는 모든 업무에 영향을 미치게 될 것이다. 또한 국방환경에서는 사용자 권한에 따른 문서 및 자료 열람 행위가 엄격히 제한되어 있으며, 이에 따라 정보공유 및 통합검색 환경에 있어 사용자 인증 및 권한 관리 등 보안 요구사항에 대한 면밀한 검토가 필요하다.

4.3.3 클라우드 서비스

클라우드는 언제 어디서나 확장성과 유연성 있는 IT 서비스를 제공하고자 하는 패러다임이다. 네트워크 고도화 및 가상화 기술 등의 발전으로 인해, On-demand 형태로 IT 자원 및 서비스를 이용할 수 있게 되었으며, 스마트워크의 시공간 제약 없이 업무 수행이 가능한 환경 구축을 위해 적용이 필요한 핵심 기술 중 하나이다. 클라우드 서비스는 가상화 기술을 기반으로 하고 있으므로, 사용자의 접근 제어를 위한 보안 정책 및 하이퍼바이저 취약점 분석[7], Co-residence 탐지[8]와 같은 위협 분석을 통해 보안 솔루션 도입 등 대처 방안 마련이 필요하다. 이와 함께 국방환경 내에서 안전한 클라우드 환경을 제공하기 위해서는 클라우드 환경에 대한 공격 모델 및 시뮬레이션 기술 적용, 보안 정책 관리 및 비용분석, SecaaS 적용 분석 등의 노력이 필요하다.

5. 결 론

본 논문에서는 기존 스마트워크 보안 관련 연구 및 국방 환경에서의 정보보호 이슈 등을 종합하여 국내 국방환경에서 스마트워크 도입 시 고려해야 할 사항을 정리하고 적용방안을 모색 해 보았다.

스마트워크 도입 시 발생 할 수 있는 여러 가지 보안 이슈들로 인해 아직까지 국방부 등 국내 국방 환경에서는 스마트워크 도입을 검토 중에 있다. 하지만, 현재 미국방부 정보시스템 계획국(DISA) 등 해외의 국방 관련 기관에서는 텔레워크(Telework)라는 이름으로 원격 근무를 허용하고 있으며[9], 오히려 이를 활성화하기 위한 많은 대책을 마련하고 이를 추진 중에 있다. 이러한 선진 국가에서의 도입 실태를 파악하고, 보안 위협 대책 등 방안을 마련한다면 국내 국방환경에서도 스마트워크를 도입 할 수 있을 것이다.

국내 국방 환경 특성상 빠르게 발전하는 기술 트렌드에 맞게 스마트워크를 신속하게 도입하는 것이 어려울 수 있지만, 체계적인 보안기술 적용 및 연구, 그리고 관련 정책의 재점검 등 다양한 노력과 관심이 필요하다. 또한 앞으로의 국방 스마트워크 도입에 대한 연구는 현 국방 정책에서의 보안 관련 제한에 갇혀있지 말고, 보다 체계적인 보안 대책 및 기술개발을 통한 그 가능성을 제시함으로써 스마트워크의 편리함과 보안의 안전함을 모두 취할 수 있도록 진행되어야 할 것이다.

참 고 문 헌

[1] 이재성, 김홍식, “스마트워크 현황과 활성화 방안 연구”, 한국지역정보화학회지 제13권 제4호, 2010, pp.75-96.

[2] 정명수, 이동범, 곽진, “스마트워크 보안위협 및 보안 요구사항 분석”, 정보보호학회지 제21권 제3호, 2011, pp.55-63.

[3] 이형찬, 이정현, 손기욱, “스마트워크 보안 위협과 대책”, 정보보호학회지 제21권 제3호, 2011, pp.12-21.

[4] 안정철, 권혁진, “국방분야 무선Network 도입을 위한 보안기술 측면의 고려사항”, 정보과학회지 제26권 제11호, 2008, pp.98-103.

[5] 손익재, 김일호, 양종휴, 이남용, “사이버 국방을 위한 스마트 단말 보안기술”. 한국통신학회논문지 제37권 제10호(융합기술), 2012, pp.986-992.

[6] 전승민, 이을석, “국방 전산망의 침해사고 대응체계 개선을 위한 통합 로그센터 구축 연구”, 정보과학회지 제26권 제11호, 2008, pp.92-97.

[7] 김지연, 김형종, 박춘식, 김명주, “클라우드 컴퓨팅 환경의 가상화 기술 취약점 분석연구”, 정보보호학회 논문지 제19권 제4호, 2009, pp.72-77.

[8] Y. Zhang., A. Juels., A. Oprea and M. Reiter., “HomeAlone: Co-Residency Detection in the Cloud via Side Channel Analysis”, Security and Privacy IEEE Symposium, 2011

[9] Overmyer. S. P., “Implementing Telework: Lessons Learned from Four Federal Agencies”, Transforming the Workforce Series, 2011.

◐ 저 자 소 개 ◑

송 일 선

2007년 한국기술교육대학교 디지털시스템공학 학사
2010년 한국과학기술원 전산학 석사
2010년~2012년 경북대학교 임베디드 소프트웨어 연구센터 연구원
2012년~현재 국방기술품질원 연구원
관심분야 : 지능형 시스템

한 영 섭

1995년 광운대학교 전자계산학과 학사
2001년 전남대학교 컴퓨터공학전공 석사
2008년~현재 고려대학교 컴퓨터·전파통신공학과 박사과정
1995년~현재 국방기술품질원 선임연구원
관심분야 : 소프트웨어공학, 요구공학, 테스팅

◐ 저 자 소 개 ◑

임 회 성

1984년 인하대학교 항공공학과 학사
2012년 한성대학교 국방M&S학 석사
1990년~현재 국방기술품질원 선임연구원
관심분야 : 국방M&S

백 진 욱

1988년 경북대학교 통계학 학사
1997년 한국과학기술원 전산학 석사
2006년 서울대학교 컴퓨터공학 박사
1990년~1998년 국방기술품질원 연구원
1998년~현재 안산대학교 금융부동산정보과 교수
관심분야 : 금융정보, 에이전트, 알고리즘