情 報 保 護 學 會 誌
第21卷 第3號, 2011. 5

스마트워크 보안위협 및 보안 요구사항 분석

정 명 수*, 이 동 범**, 곽 진***

요 약

최근 발달된 IT 기술을 활용하여 국내에서는 업무와 삶의 균형을 추구하는 스마트워크 기술 개발에 대한 움직임이 활발히 진행되고 있다. 그러나 국내의 많은 기업들이 스마트워크 기술 도입의 악영향으로 보안 관리에 대한 문제를 지적하고 있다. 이러한 보안 관리 문제는 기술만으로 해결하는 것이 아니라, 기업에서의 기술·정책적 관리를 통해 스마트워크 환경에서 발생할 수 있는 보안 사고를 미연에 방지할 수 있다. 이에 본 고에서는 스마트워크 환경에 대한 보안위협과 스마트워크 환경을 구축하기 위해 필요한 보안 요구사항에 대하여 분석하고자 한다.

Ⅰ. 서 론

최근 IT 기술의 급격한 발달로 인하여 생활방식에 많은 변화가 일어나고 있으며, IT 기술을 일상생활에 활용하여 편리하고 친환경적인 기술을 개발하여 적용하는 연구가 활발히 진행되고 있다.

현재, 국내에서는 업무와 삶의 균형을 추구하고 기업의 비용절감 및 업무의 효율성을 향상시키기 위한 스마트워크 기술 개발에 대한 움직임이 활발히 이루어지고 있다. 스마트워크는 기존의 업무 형태를 탈피한 업무 방식으로 사용자가 언제 어디서든지 시간이나 장소의 제약 없이 업무를 처리할 수 있는 업무 환경이다 [2].

스마트워크 기술은 재택근무나 기업에서 구축한 스마트워크 센터, 휴대 가능한 모바일 단말기 등을 활용하여 원격 협업 환경을 구성하고 보다 유연한 근무 환경 기반을 만들 수 있다. 이에 행정안전부에서는 2010년 11월 스마트워크 센터 1호를 개설하여 정부의 각 부처나 자치단체는 물론 공공기관 및 민간기업의 직원도 이용 가능한 공간을 국내 최초로 설치하였다. 또한 2015년까지 스마트워크 센터를 50개까지 증설하고 스마트워크 센터 시설기준 및 운영방법과 스마트워크 확산을 위한 법·제도적 기반을 제정하는 등 공공 및 민간 기업의 스마트워크 센터의 구축 및 운영을 지원하여 국내 스마트워크 환경 구축에 앞장설 계획이다 [3].

하지만, 스마트워크로 제공되는 근무 환경은 기업으로부터 완벽한 보안 통제가 이루어지지 않고 있으며, 다양한 컴퓨팅 기술의 접목으로 인하여 새로운 보안위협들이 존재하고 있다. 이러한 보안위협을 고려하지 않을 경우, 근무자의 개인정보와 더불어 기업의 내부 정보까지 유출될 우려가 있다. 기업의 내부 기밀 정보가 유출될 경우, 한 기업의 정보 유출로 인한 손실은 국가적 손실까지도 이어질 수 있다. 실제로, 기업에서 스마트워크 도입 시 스마트워크 환경에서의 보안 관리 문제로 인하여 많은 노력을 하고 있다 [4].

이에 본 고에서는 스마트워크 환경에서 발생할 수 있는 보안위협들을 분석하고, 안전한 스마트워크 환경을 구축하기 위한 보안 요구사항에 대하여 분석한다.

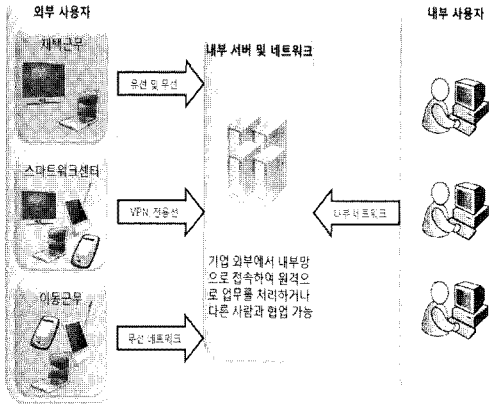
Ⅱ. 스마트워크

2.1 개요

스마트워크는 기존의 업무방식을 탈피한 미래지향적인 업무 환경으로, 다양한 정보통신기술을 이용한 새로운 업무 환경이다. 스마트워크 환경에서는 [그림 1]과 같이 다양한 장소와 이동 환경에 구애받지 않고 언제

이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2011-0007755).
* 순천향대학교 정보보호학과 정보보호응용및보증연구실 (msjeong@sch.ac.kr)
** 순천향대학교 정보보호학과 정보보호응용및보증연구실 (dblee@sch.ac.kr)
*** 순천향대학교 정보보호학과 (jkwak@sch,ac,kr)

어디서나 원하는 업무를 자유롭고 효율적으로 처리할 수 있도록 제공해 준다. 또한 원격 협업을 통해 보다 실시간으로 의사소통이 가능하고, 문제해결을 신속하게 처리할 수 있다[5].



〔그림 1〕 스마트워크 개념도

이러한 스마트워크 환경에서의 근무 형태는 [표 1]과 같이 근무 환경에 따라 분류할 수 있는데 일반적으로 재택근무, 스마트워크 센터 근무, 이동근무로 분류할 수 있다.

먼저, 재택근무는 직장이 아닌 자택에서 업무를 처리하는 근무 형태로 기업에서 구축한 네트워크로 접속하여 업무를 수행하고, 본사나 다른 근무자들과 원격회의, 협업 등을 통해 업무를 수행하게 되는 근무 형태이다. 재택근무는 별도의 사무 공간이 불필요하고 근무자가 출퇴근에 따른 시간과 교통비를 감소시킬 수 있다.

스마트워크 센터 근무는 기업에서 구축한 원격 업무 시스템을 갖춘 스마트워크 센터 시설로 업무에 필요한 사무공간과 육아시설이나 휴식공간을 제공하는 복합 공간에서 업무를 수행하는 형태이다. 스마트워크 센터에서는 다른 근무 형태와 달리 보안성이 일부 강화되어 실제 기업과 동일한 수준의 환경에서 업무 수행이 가능하고 다른 관계자들과 협업 및 지속적인 업무를 수행을 통해 기업에서도 다른 형태에 비해 근무자의 관리가 용이한 근무 형태이다.

마지막으로 이동근무는 스마트폰이나 태블릿PC를 이용한 모바일 오피스 환경을 구축하거나 휴대 가능한 단말기를 이용하여 기업과 멀리 떨어져 있는 장소나 이동 중에도 업무 처리 및 다른 근무자와 정보를 교환하여 장소에 구애받지 않고 근무할 수 있는 형태이다. 보통 출장, 고객 대면 등으로 업무 시간의 대부분을 기업 외부에서 보내는 영업 직종이나 컨설팅 업무를 하는 근무자에게 제공되는 근무 형태이다[6].

〔표 1〕 스마트워크 근무 형태

형태	내용
재택근무	자택에서 기업 내 네트워크에 접속하여 근무
스마트워크 센터 근무	자택 부근의 ICT 환경이 갖춰진 사무실에서 근무
이동근무	모바일 오피스 환경을 이용한 현장에서 직접 근무하거나 이동하면서 근무

Ⅲ. 보안위협

스마트워크를 이용하여 편리하고 신속한 업무처리와 효율적인 업무환경을 구축할 수 있는 반면에, 스마트워크로 제공되는 업무 형태가 기업으로 하여금 보안 통제가 이루어지는 사내 공간이 아닌, 다양한 공간에서 업무를 수행할 수 있는 환경이 구축되는 것이다. 또한 스마트워크에는 다양한 컴퓨팅 기술들이 사용되면서 기존 컴퓨팅 기술의 보안위협들이 그대로 적용되어 근무형태나 컴퓨팅 환경에 따른 여러 보안위협이 추가적으로 발생할 수 있다. 따라서 본 장에서는 스마트워크 환경에서 예상되는 대표적인 보안위협에 대해서 분석한다.

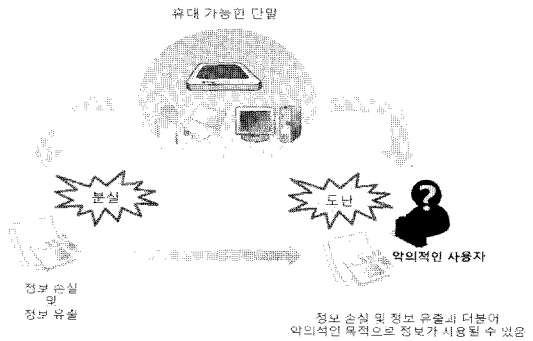
3.1 노출된 공간

기존의 업무에서는 보안이 통제되는 기업 내에서 업무를 처리하게 된다. 하지만 스마트워크 센터 근무나 이동근무 형태에서는 보안이 통제되지 않는 물리적 공간과 제 3자와 함께 시설을 사용하는 등의 노출된 공간에서 업무를 처리하게 된다. 이에 따라, 스마트워크 센터 근무나 이동근무에서는 자신이 처리하는 업무를 제 3자가 볼 수 있는 경우가 발생될 수 있다. 또한 스마트워크 센터에서는, 잠시 자리를 비운 사이에 자신이 사용하는 단말기를 제 3자가 사용할 수 있으며, 공동으로 사용하는 PC의 경우에는 자신이 사용하는 데이터 기록이 해당 PC에 남아있을 수 있다.

3.2 단말기 도난 및 분실

스마트워크의 근무 형태 중에서 스마트워크 센터 근

무나 이동근무의 특징으로는 사용자의 단말기가 휴대 가능한 단말기를 사용할 수 있다는 것이다. 이러한 단말기는 최근 널리 보급되고 있는 스마트폰이나 태블릿PC, 노트북 등 휴대 가능한 단말기로 사용자가 언제 어디서나 휴대할 수 있다는 장점을 지니고 있지만, 단말기에 대한 관리가 부족할 경우 단말기를 도난당하거나 분실할 위험이 존재한다. 아래의 [그림 2]와 같이 단말기를 분실하거나 도난당할 경우, 정보 손실 및 정보 유출이 될 수 있으며, 단말기를 악의적인 사용자가 습득했을 경우에는 개인정보 및 기업 내부 정보가 악의적인 목적으로 사용될 수 있다.

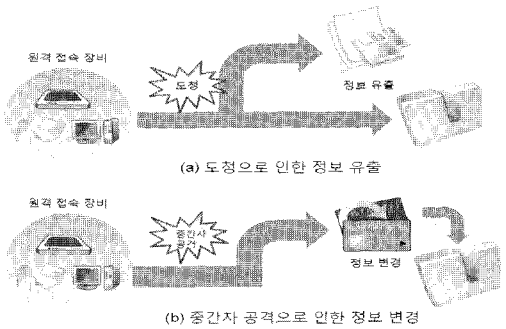


〔그림 2〕 단말기 분실 및 도난

3.3 원격접근

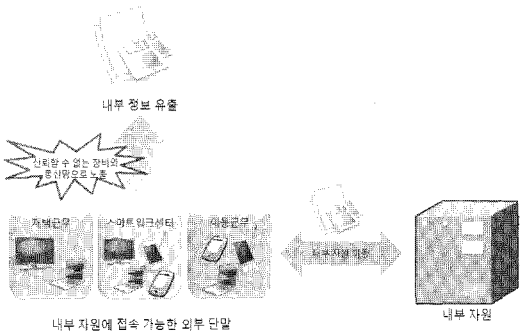
스마트워크에서 핵심 기술로 사용되는 원격 접근기술은 주로 외부에서 업무를 처리할 때 기업 내부 시스템에 접속하여 내부망의 자원을 원격으로 처리하거나 내부망을 통하여 본사 내 다른 근무자들과 협업을 통한 업무를 처리하게 된다. 하지만 외부망이나 외부 전산장비를 통하여 접속하는 것은 내부에서 사용하는 방식보다 많은 위험이 내재되어 있으며 내부 자원들이 원격 접근을 통하여 외부로 노출될 위험이 높다.

대부분의 원격 접근은 인터넷을 통해 이루어지기 때문에 기업에서는 일반적으로 스마트워크 근무자들이 사용하는 외부 통신망들의 보안을 통제할 수 없다. 원격 접근에 사용되는 통신은 [그림 3]과 같이 대부분 도청 및 중간자 공격에 취약하여 원격으로 접속하는 동안 전송되는 내부 중요 데이터들이 유출되거나 통신내용이 변경되어 전송될 수 있다[7].



〔그림 3〕 외부 통신망에 대한 공격

또한 기존의 근무형태에서는 기업 내에 존재하는 내부 자원을 외부에서 접근할 수 없었지만, 스마트워크 환경에서는 이러한 내부 자원을 외부에서 원격 접근을 통해 접근이 가능해진다. 이에 따라 [그림 4]와 같이 외부에서 접근하는 내부 자료들을 신뢰할 수 없는 장비와 통신망으로 노출시켜 중요한 내부 자료가 외부로 유출될 수 있다.

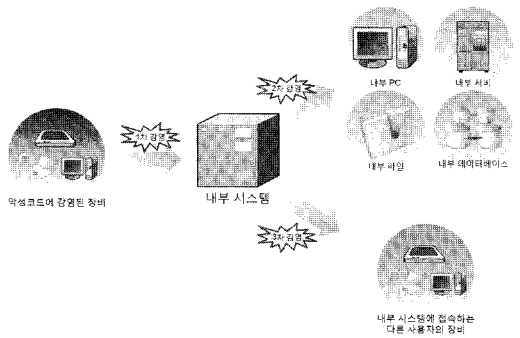


〔그림 4〕 외부 전산장비에 노출된 내부 자원

3.4 악성코드

최근 유행하는 악성코드는 시간이 지나면서 감염 증상이나 유포 방법이 다양해지고 복잡해지면서 지능화되고 있는 추세이다. 이로 인해 스마트워크에서 모바일 단말기를 이용하는 이동근무나 스마트워크 센터, 재택근무에서 사용되고 있는 PC나 모바일 단말기에 악성코드가 감염될 경우에는 사용자의 개인정보나 기업의 중요한 정보가 유출될 수 있다. 또한 사용자가 악성코드의 감염을 인지하지 못한 상태에서, 악성코드에 감염된 단말기를 사용할 경우에는 [그림 5]와 같이 감염된 단말

기로 기업의 내부 시스템에 접속하거나 다른 사람과 정보를 주고받는 과정에서, 악성코드가 기업 내부의 다른 단말기 및 서버 등과 스마트워크 센터의 단말기나 다른 사용자의 단말기에 전이될 우려가 있다. 이와 같이 전이된 악성코드는 또 다른 사용자에게 감염시키면서 빠른 속도로 악성코드가 확산될 수 있다.



〔그림 5〕 악성코드의 확산

이러한 악성코드는 사용자의 부주의로 악성코드를 유포하는 웹페이지에 접속하거나 P2P 서비스 사용, 불법 복제 프로그램을 사용할 때 감염되거나 내부자나 외부 공격자가 악성코드를 직접 설치 및 스팸 메일에 포함시키는 등 다양한 경로를 통해 악성코드에 감염될 수 있다.

Ⅳ. 보안 요구사항

위에서 살펴본 것처럼 스마트워크 환경에서는 다양한 보안위협이 존재하고 있다. 이러한 보안위협은 전혀 막을 수 없는 위협들이 아니라 사용자나 기업의 측면에서 기술·정책적으로 관리한다면, 위와 같은 위협들로부터 보다 안전한 스마트워크 환경을 사용할 수 있다. 본 장에서는 스마트워크 환경을 안전하게 구축하기 위해서 필요한 보안 요구사항에 대해서 분석한다.

4.1 기술 요구사항

스마트워크 기술은 주로 외부 사용자에게 내부 자원에 대한 접근을 제공하기 위해 VPN 게이트웨이와 포털 서버와 같은 원격 접근 서버를 사용하기 때문에 보안이 특히 중요하다. 일반적으로, VPN 게이트웨이와 포털 서버를 보안하기 위한 방법으로는 방화벽, 백신 및 침입 탐지 소프트웨어와 같은 보안 기술을 사용할 수 있다. 원격 접근이 가능한 서버에서 위와 같은 보안 방법에 대한 모든 패치를 주기적으로 적용해야 하며 기업에서 정한 보안 환경설정 기준을 사용하여 운영하고 별도의 시스템 관리자를 선정하여 호스트를 관리 및 운영해야 한다[8].

그리고 내부 서버에 저장되는 데이터에 대한 보안 설정은 원격 접근 서버 보안을 위한 매우 중요한 사항이다. 사용자가 업무 처리 도중에 데이터를 저장하는 방법에는 먼저, 사용자 단말기에 저장하는 방법이 있지만, 휴대 가능한 단말기에는 많은 위협들이 있기 때문에 우선적으로, 사용자들이 업무를 처리하는 내부 서버에 데이터를 저장할 수 있는 서버가 제공되어야 한다. 이러한 내부 서버에는 데이터 저장 시 암호화 등을 거쳐 내부 서버 내 데이터에 대한 보안을 철저히 해야 한다. 내부 서버에서는 사용되지 않거나 필요하지 않은 데이터를 삭제하여 서버에 위협을 미칠 수 있는 잠재적인 요소를 없애야 한다. 이러한 데이터는 스마트워크를 운영하는 기업이나 기관에서 데이터에 따른 위험 평가 제도를 마련하여, 평가 제도를 통하여 불필요한 데이터를 선별하여 제거해야 한다.

또한 스마트워크를 제공하는 기업은 원격 접근을 통한 안전한 접근을 보장하기 위해서 보다 확실한 인증 체계를 사용하여 사용자들이 필요한 자원에만 접근이 가능하도록 하여 원격 접근 서버 및 내부 서버를 보호해야 한다. 그리고 기업의 중요 업무를 수행하는 직책이나 서버 내에 주요 기밀 자료에 접근을 해야 하는 경우에는 별도의 보안 인증 절차를 마련해야 한다. 사용자가 원격 접근에 대한 인증을 거친 상태라 하더라도 일정시간 이후나 유효시간이 지난 후에는 재인증을 통한 사용자 확인을 해야 한다. 또한 사용자가 사용하는 단말기가 비활성 된 시간으로부터 일정시간이 지난 다음에 재인증을 요구하는 기능이 수행되어야 한다.

그리고 사용자에게 사용 권한을 부여하기 위한 절차인 인증에서 사용되는 암호와 타임스탬프 값은 기업에서 사용되는 모든 프로세스들이 동일한 타임스탬프 값을 가질 수 있도록 해야 한다.

4.2 단말 요구사항

기업의 내부 서버로 접근 가능한 사용자의 단말기가

제대로 보안이 이루어지지 않는다면, 이 단말기로 내부 서버에 접근할 경우에는 사용자가 접근한 정보나 기업의 내부 시스템 및 다른 사용자에게 추가적인 위협을 초래할 수 있다.

먼저, 사용자가 사용하는 모든 단말기에는 개인 방화벽을 필수적으로 설치해야 한다. 개인 방화벽을 이용하여 다양한 환경에서 사용되는 사용자 단말기에 대한 위협을 사전에 방지해야 한다. 방화벽은 기업의 네트워크 환경이나 외부 환경에 맞게 구성되어야 하며, 여러 정책 지원이 가능해야 한다[9].

그리고 사용자 단말기에 저장되는 데이터를 암호화하는 기술을 마련해야 한다. 데이터 암호화를 통해 사용자가 기업의 스토리지가 아닌 단말기에 데이터를 저장하는 경우, 단말기 도난 및 분실이나 무단 접근에 의한 정보 유출을 방지할 수 있다. 또한 기업에서는 기업 외부에서 업무를 수행하는 사용자들을 위하여 외부에서 사용할 수 있는 보안 스토리지를 마련하여 외부 사용자가 수시로 데이터를 암호화하여 백업 및 저장할 수 있어야 한다.

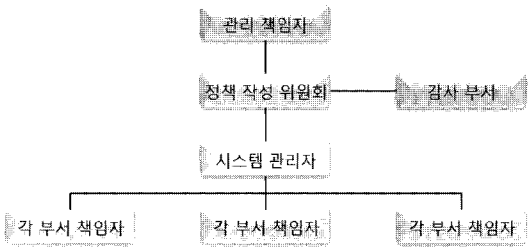
4.3 정책 요구사항

기업에서 안전한 스마트워크 환경을 구축하기 위해서는 우선적으로 기업 내에 스마트워크에 대한 보안 정책이 제대로 마련되어야 한다. 보안 정책이 마련되더라도 이 정책이 현재 기업에 적용이 가능한지 혹은 정책이 제대로 준수되고 있는지를 주기적으로 검토하여 정책을 관리하고 유지해야 한다.

4.3.1 기업 준수 정책

기업에서는 우선적으로 스마트워크에 대한 관리 체제와 책임 소재 및 기업에서 보호해야 할 정보자산의 구분을 명확히 정해야 한다.

정보자산에 대해서 하드웨어 및 소프트웨어, 정보 등으로 구분하여 이에 대해 보관이나 관리 및 사용자 범위 등을 고려하여 정보자산에 대한 우선순위를 명확히 정의해야 한다. 정보자산에 따른 평가를 거친 정보자산에 따른 등급을 설정하고, 기업은 [그림 6]과 같이 정보자산에 따른 관리 책임자, 부서 책임자, 시스템 관리자 등 관리 체제를 마련하고 이에 대한 책임자들에게 권한을 부여해야 한다. 각 권한에 따른 역할은 [표 2]와 같이 구성해야 한다. 그리고 이러한 책임자들을 감사하는 인원들을 구성하여 관리 체제가 책임자들로 하여금 제대로 이루어지는지 확인해야 한다[1].



〔그림 6〕 기업의 정보보안 관리 체계

〔표 2〕 스마트워크 근무 형태

구분	역할
관리 책임자	스마트워크를 사용하는 기업의 최고 직위를 포함하는 책임자로 스마트워크의 정보보안 정책을 총괄하여 관리한다.
정책 작성 위원회	스마트워크에 대한 시스템, 관리, 현장 부분 등에 대한 정보보안 정책을 작성한다.
감사 부서	스마트워크를 사용하는 기업 내에 정보보안의 준수 여부를 확인하기 위한 부서로 정보보안 관리 체제의 여러 부서를 감사한다.
각 부서 책임자	각 부서의 스마트워크 사용자들을 1차적으로 관리하며, 스마트워크 관련 요구 및 문제점을 받아 보고하여 개선될 수 있도록 한다.

기업에서는 정보보안 관리 체제를 통해 위급 상황이나 사고 발생 시 신속한 초기 대응 및 연락망을 통해 각 담당 관리자에게 연락할 수 있는 체제를 마련하고, 이를 문서화하여 사용자들에게 배포해야 한다.

그리고 스마트워크를 사용하는 기업에서는 외부 근무에 필요한 단말기를 기업에서 제공할 수 있도록 해야 한다. 이러한 단말기는 기업이 직접 관리 및 유지해야 제대로 된 정보보안 정책을 수행할 수 있다.

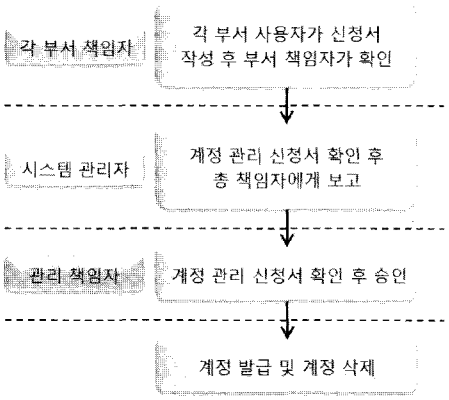
또한 기업에서는 스마트워크를 이용할 인원을 선별하는데 있어 스마트워크 사용자와 내부 정보의 기밀 유지 및 스마트워크를 사용하는데 요구되는 최소 정보보안 요구사항에 대해 준수할 것을 약속해야 한다. 기업 내부의 기밀 정보는 사용자의 작은 실수로 인해 그 영향이 크게 확산될 수 있으므로 기업에서 스마트워크를 사용하는 근무자, 스마트워크 시스템 관리자에게 지속적으로 스마트워크 환경에 대한 정보보안 교육을 주기

적으로 수행해야 한다. 주기적인 정보보안 교육을 통해, 사용자들에게 정보보안에 대한 의식을 권고시키고, 정보보안에 대한 책임 및 규칙 위반 시 처벌 규정이나 손해 배상에 대한 규정을 포함한 정보보안의 중요성을 교육해야 한다[10].

4.3.2 관리자 및 사용자 준수 정책

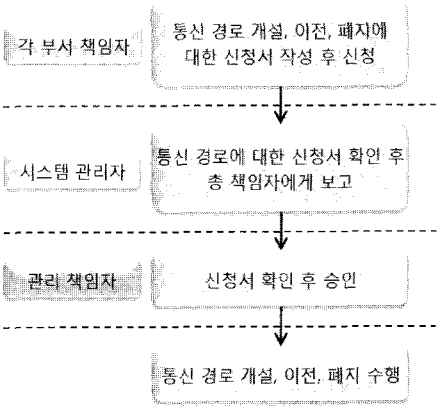
기업에서 선정한 시스템 관리자는 먼저, 스마트워크 환경의 모든 시스템에 대해 관리 및 유지하며 사고 발생에 대해 조기대응을 신속히 할 수 있도록 대비해야 한다. 시스템 관리자가 관리해야 할 기본적인 사항은 다음과 같다.

- □ 사용자 계정 및 패스워드 관리
- □ 내부 환경에 접속 가능한 통신 경로 관리
- □ 단말기 관리



〔그림 7〕 계정 발급 및 삭제 절차

첫 번째로, 기업에서 사용되는 계정에 대해서는 [그림 7]과 같이 계정 발급 및 삭제 절차를 제정하여 계정을 발급 받을 시에는 계정의 사용 목적이 명확한지 확인하고 계정에 따른 사용 기간 및 권한에 대해 설정해야 한다. 그리고 계정에 대한 정보를 변경하거나 삭제할 때에는 정해진 절차에 따라 관리자의 승인을 거쳐 확인해야 하며 삭제하는 계정에 대해서는 계정에 대한 정보를 완전히 삭제해야 한다. 또한 기업에서 운영하는 계정에 대해서는 계정 점검표 등을 마련하여 오래 동안 사용되지 않거나 사용 기간이 지난 계정에 대해서는 계정 관리 절차에 따라 삭제해야 한다. 또한 계정에 대한 접근 권한 설정이 올바르게 설정되었는지 주기적으로 점검할 필요가 있다.



〔그림 8〕 통신 경로에 대한 관리 절차

두 번째로, 기업 내부로 접속하는 통신 경로에 대해서는 [그림 8]과 같이 통신 경로를 관리하는 절차를 제정하여 통신 선로를 신청, 이전, 폐지를 할 경우에 신청자는 각 부서 책임자를 통하여 시스템 관리자와 관리 책임자의 승인을 얻도록 해야 한다.

그리고 통신 경로를 사용함에 있어서는 승인 받은 통신 경로 이외에는 사용하지 못하도록 하여 내부 정보에 대해 외부의 무단 접근을 막아야 한다. 또한, 사용 중인 통신 경로를 주기적으로 점검하여, 경로만 개설 된 상태로 오랜 시간 사용되지 않는 통신 경로나 문제가 있는 통신 경로에 대해서는 이에 대한 사항을 보고 후 통신 경로를 폐지하거나 조치를 취하여 복구할 수 있도록 해야 한다.

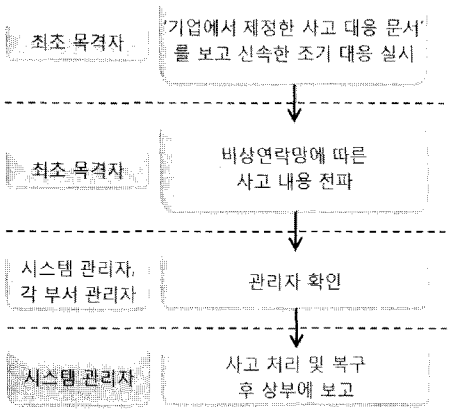
세 번째로, 관리자는 기업에서 제공하는 단말기에 대한 사용 현황을 관리해야 한다. 사용 현황에 해당하는 부분은 사용자, 담당 업무, 사용 기한, 연락처, 단말기에 적용되는 보안 시스템 등이다. 사용 현황 이외에 단말기를 제공하거나 사용한 단말기를 반납 받았을 때는 다음과 같은 사항에 대해 확인해야 한다.

- □ 백신의 설정 및 작동 여부
- □ 이전 사용자에 대한 데이터 존재 여부
- □ 악성코드 감염 여부
- □ 최신 패치 여부(OS, 백신, 기타 애플리케이션)
- □ 개인 방화벽 설정 여부

시스템 관리자는 위와 같은 사항과 단말기 사용 현황을 '단말기 관리 대장'에 작성하여 단말기를 제공하거나 반납 받을 때, '단말기 관리 대장'에 기록하고 반납 받은 단말기에 대해서는 위의 5가지 사항에 대해 검토 및 기록해야 한다. 단말기의 지속적인 점검을 통해 다른 사용자에게 다시 제공할 수 있도록 관리 및 유지해야 한다.

스마트워크를 사용하는 사용자는 먼저, 기업의 스마트워크 보안 정책이나 단말기 사용 정책, 사고 대응 방법을 습득하고, 이를 준수해야 한다. 그리고 사고 발생 시 사용자는 [그림 9]와 같이 신속한 조기 대응을 실시해야 한다. 사용자는 기업에서 제정한 사고 대응 방법에 관한 문서를 보고 사고 발생 유형에 따라 조기 대응을 실시한 후, 비상 연락망을 통해 사고 내용을 관리자 및 관계자에게 전파해야 한다. 신속한 상황 전파를 통해 사고를 조기에 대응하고 사고의 피해를 최소화하고 사고 이후 대응을 신속히 처리해야 한다.

또한 사용자는 스마트워크 환경에서 사용할 단말기를 사용 방법에 준수하여 사용자 스스로 단말기의 분실이나 도난, 단말기 관리 부주의로 인해 발생할 수 있는 사고를 미연에 방지할 수 있도록 노력해야 한다.



〔그림 9〕 사고 발생 시 초기 대응

4.3.3 관리 및 유지 정책

기업의 스마트워크에 사용되는 모든 소프트웨어를 업데이트를 하기 전에는, 기업 및 시스템 관리자가 업데이트에 대한 내용을 확인하고 사용 방법을 습득해야 한다. 그리고 해당하는 업데이트를 기업의 스마트워크 환경에 사용할 경우에 따른 이상 유무를 확인하여 책임자의 승인을 받은 뒤 스마트워크 환경에 업데이트를 수행해야 한다.

또한 기업에서 수립한 스마트워크에 대한 정보보안 정책을 지속적으로 수행하기 위해서는 감사 부서와 기업에서 스마트워크에 대한 정보보안 정책을 주기적으로 평가하여 올바른 업무가 수행되는지 확인해야 한다. 이러한 평가에 대한 올바른 방향과 지침을 제공하기 위해 기업에서는 정보보안 평가 정책을 개발할 필요가 있다. 평가에 따라 정책에 대한 부족한 사항은 검토하여 수정 및 보완해야 한다. 수정 및 보완되는 정책에 대해서는, 수정 된 내용이 일관성을 유지하는지 확인하고 본래의 정책 목적에서 벗어나지 않도록 주의해야 한다. 기업에서는 수정되는 보안 정책을 지속적으로 문서화하여 보관하고, 변동된 사항을 관리자 및 사용자에게 전파 및 교육해야 한다[11].

V. 결 론

본 고에서는 스마트워크 환경에서 발생할 수 있는 보안위협들을 분석하고, 다양한 보안위협으로부터 안전한 스마트워크 환경을 위한 보안 요구사항에 대해 분석하였다. 아직까지 국내에 많은 기업들이 스마트워크 도입에 대한 부정적인 영향으로 스마트워크 환경에서의 보안관리 문제를 지적하고 있다.

국내 기업의 스마트워크 도입을 촉진하고, 스마트워크 환경 구축을 활발하게 하기 위해 스마트워크에 대한 보안 요구사항을 준비하고 관련 정책 제정을 준비해야 한다. 이와 같은 기술·정책적 관리를 마련하여 스마트워크 환경에서 발생할 수 있는 보안 사고를 최소화하고 미연에 방지할 수 있도록 준비해야 한다.

참고문헌

[1] 總務省, "*テレワークセキュリティガイドライン解說書*", 2004
[2] 김성태, "*일하는 방식의 대혁명적 변화 '스마트워크'*, 한국정보화진흥원", 2010
[3] 행정안전부, "*스마트워크 추진 계획*", 2010
[4] 김성태, "*녹색생활 실천전략 IT기반 원격근무*", 한국정보화진흥원, 2009
[5] 방송통신위원회, 한국정보화진흥원, "*기업을 위한*

스마트워크 도입·운영 가이드북", 2011

[6] 이재성, 김홍식, "스마트워크 현황과 활성화 방안 연구", *한국지역정보화학회지*, 13(4), pp.78-80, 2010

[7] Lisa J. Carnahan, and Barbara Guttman, "Security Issues for Telecommuting", *National Institute of Standards and Technology*, pp. 2-6, 1996

[8] Karen Scarfone, Paul Hoffman, and Murugiah Souppaya, "*Guide to Enterprise Telework and Remote Access Security*", NIST SP 800-46 Rev 1, 2009

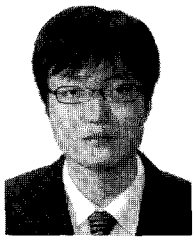
[9] Karen Scarfone, and Murugiah Souppaya, "*User's Guide to Securing External Devices for Telework and Remote Access Security*", NIST SP 800-114, 2007

[10] Office of Information Security, "*Telework and Remote Access Security Standard*", 2010

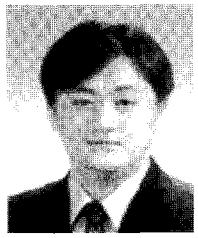
[11] Elizabeth Chew, Marianne Swanson, Kevin Stine, Nadya Bartol, Anthony Brown, and Will Robinson, "*Performance Measurement Guide for Information Security*", NIST SP 800-55 Rev 1, 2008

〈著者紹介〉

정 명 수 (Myeongsoo Jeong)
학생회원
2006년 3월~현재 : 순천향대학교 정보보호학과
<관심분야> 정보보호, 스마트워크 등



이 동 범 (Dongbum Lee)
학생회원
2008년 2월 : 순천향대학교 정보보호학과 학사 졸업
2008년 3월~2010년 2월 : 순천향대학교 정보보호학과 석사 졸업
2010년 3월~현재 : 순천향대학교 정보보호학과 박사과정
<관심분야> 정보보호, 보안성 평가, 전자여권 보안 등



곽 진 (Jin Kwak)
종신회원
1994~2006년 : 성균관대학교 전자공학과(공학사 공학석사, 공학박사)
2006~2006 : 일본 큐슈대학교 방문연구원
2006~2006 : 일본 큐슈시스템 정보기술연구소 특별연구원
2006~2007 : 정보통신부 개인정보보호기획단 개인정보보호팀 통신사무관
2007~2009 : 정보통신연구진흥원 집필위원
2009~2009 : 순천향대학교 공과대학 교학부장
현재 : 순천향대학교 정보보호학과 교수, 정보통신산업진흥원 기술평가위원, 디지털아이디관리포럼 기술평가위원, 한국정보통신기술협회 JTC/SC27 분과 기술위원, 한국정보통신기술협회 표준화 로드맵 기술표준기획 전담반 기술위원, 순천향BIT 창업보육센터 소장, 사) 국제정보능력평가원 쇼핑몰 플래너 자격 검정 출제 및 채점위원, 한국인터넷진흥원 미래융합IT서비스 보안연구회 스마트그리드 보안 분과 기술위원, 교육과학기술부 국가기술 수준 평가 전문위원, 한국과학기술정보연구원 충남 과학기술정보협의회 전문위원, 지식경제부 지식경제기술혁신평가단 평가위원, 순천향대학교 중소기업산학협력센터 소장
<관심분야> 암호프로토콜, RFID 시스템 응용보안, 개인정보보호, 정보보호제품평가, 클라우드 컴퓨팅 보안 등