스마트워크 환경 변화에 따른 보안위협과 대응방안

이경복† · 박태형†† · 임종인†††

요 약

본 연구는 국가 어젠다로 추진되고 있는 스마트워크 환경에서의 정보보호 관련 주요 이슈와 문제점들을 살펴보고 해결방안을 제시하고자 한다. 특히 최근 스마트워크 1.0에서 스마트워크 2.0으로 진화되고 있는 시점에서 보안 문제에 대한 논의는 매우 중요하다. 본 논문에서는 재택근무, 모바일 오피스, 스마트워크센터 등 대표적 스마트워크 1.0 환경에서 발생하는 보안문제와 이에 대한 대응방안을 살펴보며, 또한 협력성의 확대 및 창의성의 증가 등 스마트워크 2.0에서 새로이 부각되는 주요 개념들로부터 파생되는 보안이슈와 대응방안을 고찰한다.

주제어 : 스마트워크, 보안관리, 모바일오피스, 스마트워크센터, 스마트워크 2.0

Security Threats and Countermeasures according to the Environmental Changes of Smart Work

Kyung-bok Lee† · Tae-Hyoung Park†† · Jong-In Lim†††

ABSTRACT

This research suggests the effective countermeasures for the security threats on 'Smart Work 2.0'. It is important to discuss the Smart Work 2.0 security issues and threats at the point of evolving form Smart Work 1.0 into 2.0. In this research, first, the security issues, threats and countermeasures of telecommunication working, mobile office and smart work center are discussed. Second, we explore the security issues derived from co-working or creativity as major concepts of Smart Work 2.0.

Key Words : Smart Work, Security Management, Mobile Office, Smart Work Center, Smart Work 2.0

† 고려대학교 정보보호대학원 정보보호학과 박사과정
†† 고려대학교 정보보호대학원 정보보호연구원 연구교수
††† 고려대학교 정보보호대학원 원장/교수 (교신저자)
논문접수: 2011년 7월 8일, 1차 수정을 거쳐, 심사완료: 2011년 7월 29일

1. 서 설

스마트워크는 언제 어디서나 편리하게 효율적으로 업무에 종사할 수 있도록 하는 미래지향적인 업무 환경으로, 업무속도와 생산성의 향상을 도모할 뿐만 아니라 신속한 의사결정과 빠른 문제해결을 가능하게 한다. 이러한 측면에서 우리나라의 국가정보화전략위원회에서는 스마트워크의 구현을 국가 주요 어젠다로 설정하여 추진하고 있다[8].

이렇게 추진되고 있는 스마트워크의 도입은 주로 비용절감, 편익 등의 긍정적인 기대효과에 근거를 두고 있어 보안문제를 간과하게 될 위험성이 존재한다. 실제로 한국정보화진흥원에서 실시한 설문조사에서는 59.3%의 응답자가 스마트워크의 부정적인 기대효과로 정보보안의 우려를 제기하였으며[12], 삼성경제연구소에서 CEO를 대상으로 한 설문에서도 설문자의 47.9%가 보안문제로 인해 스마트워크 도입에 대해 고민하고 있음을 밝히고 있다[1].

스마트워크 도입을 활발하게 추진하고 공공부문에서 보안 침해사고가 발생한다면 경제적 피해뿐만 아니라 국가 중요정보의 유·노출 등으로 인해 국가위상을 크게 위협할 수 있으며, 민간부문의 경우에도 기업의 산업기밀이나 핵심기술의 유출 등으로 인해 막대한 경제적 피해를 입을 수도 있다. 즉, 스마트워크 도입에 있어 보안은 가장 필수적으로 논의해야하는 핵심 요소로[9], 스마트워크에서의 보안이 해결되지 않는다면 스마트워크의 활성화는 어려울 것이다.

최근에는 스마트워크 1.0의 확산과 함께 스마트워크 2.0으로의 진화에 대해 활발히 논의되고 있다[3]. 따라서 본고에서는 정보보안의 관점에서 스마트워크의 진화에 따른 보안 이슈를 살펴보고 이를 통해 보다 안전하고 신뢰성 있는 스마트워크의 구축을 위한 방향을 논의하고자 한다. 이를 위해 다음에서는 현재 스마트워크 1.0의 보안 이슈와 이에 대한 보안 관리를 견고할 수 있는 대응방안을 논의하고, 이와 함께 향후 확대될 스마트워크 2.0의 보안 이슈를 살펴보도록 하겠다.

2. 스마트워크 1.0에서의 보안

2.1 스마트워크 1.0에서의 보안 이슈

2.1.1 스마트워크에 대한 보안의 우려

스마트워크는 기본적으로 조직 밖의 다양한 장소에서 조직 내에 위치한 업무 서버나 개인의 워크스테이션에 원격 접속하여 실시간으로 업무를 처리할 수 있도록 하는데 초점을 두며, 이를 위해 자택근무나 스마트워크센터, 모바일오피스와 같은 다양한 접근 형태로 구축된다. 스마트워크는 조직 내 네트워크 및 시스템에 대한 외부 접근을 증가시키며, 이는 곧 내부 시스템에 대한 보안위협의 경로 가능성을 증가시킨다. 스마트워크에서의 외부 업무 처리 지원은 관리가 어렵고 회사의 내부 기밀 정보 유출의 위험성을 내재하고 있기 때문이다.

특히 인터넷과 같은 공용 네트워크에는 수많은 악성코드와 백도어 프로그램이 전파·설치되어 다양한 정보가 유출되고 있으며, 금전적인 이득이나 사이버 테러 등의 목적으로 수많은 해킹이 시도되고 있기 때문에, 이러한 보안의 위협이 스마트워크의 환경에서 실제화 된다면 조직은 스마트워크가 가지는 엄청난 보안 리스크를 가지게 된다고 할 수 있다. 최근 발생한 NH농협의 전산망 사고에서 내부 네트워크에서만 사용되어야 하는 노트북이 농협 외부에서 사용, 악성코드에 감염되어, NH농협 내부 네트워크에 대한 악성코드의 감염경로로 작용하여 NH농협의 온라인 관련 서비스가 약 18일간 중단되었던 것과 같이, 조직 외부 네트워크에서의 보안위협이 내부로 전이되는 경우 큰 경제적 피해를 야기할 수 있다.

또한 최근 스마트폰의 확산에 따라 스마트워크가 더욱 가속화되고 있다고 볼 수 있는데, 이러한 스마트워크를 위해 사용되는 스마트폰이나 스마트 패드와 같은 새로운 유형의 단말기는 스마트워크에 대한 보안을 걱정하게 하는 요소 중 하나이다. 이러한 단말기의 개방성과 휴대성은 스마트워크의 효율성을 보장하는 핵심 요소이지만, 분실 및 도난이 쉽게 발생할 수 있기 때문에 보안위협을 내재하고 있다[14]. 만약 스마트워크에 사용된 스마트폰이 악의적인 목적을 가진 산업스파이나 해커 등에 의해 훔쳐진 경우 스마트

폰에서 열람한 기밀 정보가 유출될 위험이 존재하며, 더 나아가서 공격자가 스마트폰 내 메모리의 분석을 통하여 저장된 내부망의 접속 IP나 공인인증서 등을 추출하여 스마트워크의 내부망을 해킹할 수도 있다.

2011년 5월 보안업체인 Symantec에서 기업 내 스마트폰 사용자를 대상으로 실시한 설문조사에서는 업무에서의 스마트폰 사용이 일상화 되었지만 스마트폰의 보안에 대한 기업의 강화 노력이 부족함을 밝히고 있다. 설문에서 전체 설문자의 63%가 기업에서 업무를 위해 스마트폰 사용을 허용하고 있으나 이중 51%가 스마트폰 보안 정책이나 정보보호방안에 대한 교육을 받은 적이 없다고 밝혀, 기업에서 업무에 사용되는 스마트폰에 대한 보안 관리가 제대로 이루어지고 있지 않음을 확인할 수 있다. 또한 설문의 응답자 가운데 75%가 스마트폰의 사용이 기업 네트워크 및 정보보안에 아무런 영향을 미치지 않거나(23%) 미미하게 영향을 미친다고(52%) 답하고 있고, '스마트폰, 노트북, 지갑, 자동차 키' 중 분실 시 가장 걱정이 되는 물건을 선택하라는 질문에서 13%만이 스마트폰을 선택하고 있어, 스마트폰의 중요성에 비해 사용자의 보안 인식이 미흡한 상황임을 분석하고 있다[15][16].

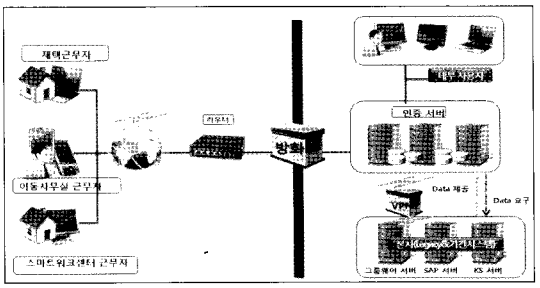
실제로 조직에서 스마트워크 도입에 있어 가장 큰 고민은 스마트워크의 도입으로 목적한 효율성을 달성할 수 있는 것인가가 아닌, 과연 스마트워크가 신뢰할 만큼 안전한가이다. 2010년부터 현대중공업이나 포스코 등의 기업에서 모바일 오피스 기반의 스마트워크를 추진하고 있으나 내부 도면이나 시설 구조, 장비현황 등과 같은 기밀 정보가 스마트워크를 통해 유출되는 경우 기업 경쟁력을 상실할 수 있기 때문에, 보안에 가장 중점을 두고 신중히 스마트워크를 도입하고 있다. 즉, 보안의 위협은 조직이 스마트워크를 도입하는데 있어 가장 걸림돌로 해결해야만 하는 최우선의 문제 중 하나이다.

하지만 스마트워크에 대한 보안의 강화로 인해 조직 내부 구성원들에 대한 더 많은 사생활의 침해가 가능하다는 우려도 제기되고 있다[5][13]. 스마트워크에서는 IT 컴플라이언스 준수를 통한 보안 강화를 위해 이메일이나 메신저, 전자문서의 송수신 및 열람 등의 모든 업무가 감시되고 로그가 기록되는데, 이러한 사용자 행위의 기록 보존은 직장 내 감시의 일종으로 사생활 침해의 문제가 발생할 수 있다. 스마트워크에서의 프라이버시 침해 문제는 프라이버시가 가지는 인권적 가치와 조직이 가지는 이해 가치 사이에서 균형점을 모색함으로써 해결할 수 있기 때문에, 조직에서는 스마트워크에서의 합리적이고 명확한 모니터링 및 로깅 범위 등을 규정하고 근로자가 이를 이해하고 동의할 수 있도록 조율해야한다.

2.1.2 스마트워크에 대한 보안위협

스마트워크 환경에서 보안위협은 조직 내 내부 정보 및 내부 시스템과 외부에서 사용하는 단말기에 대해 발생한다. 스마트워크 환경에서는 기존의 보안위협이 그대로 발생하기도 하지만, 조직의 보안 정책을 우회하는 모바일 악성코드 등의 새로운 보안위협이 등장하고 있기 때문에, 어떠한 보안위협이 발생할 수 있는지를 예측하고 이에 대한 대응책을 수립하는 것이 매우 중요하다[7].

[그림 1]에서와 같이 스마트워크는 기본적으로 스마트워크센터나 재택근무지와 같은 조직 외부의 특정 장소나 스마트폰이나 스마트패드, 노트북 등의 단말기에서 다양한 통신 방법을 통하여 조직 내 시스템에 접근하는 구조로 구축되고 있다[2]. 따라서 스마트워크에서는 기본적으로 내부의 시스템 및 정보가 보호해야할 자산이 되며, 외부에 위치하는 모든 단말기는 모두 내부 시스템에 대한 보안위협을 발생시킬 수 있는 위협원으로 조직 내부의 자산에 미치는 보안위협 여부를 식별해야만 한다. 즉, 스마트워크 환경에서는 기본적으로 조직 내 설치된 방화벽을 기준으로 보안위협의 목표와 대상이 각각 위치한다고 볼 수 있다.



[그림 1] 스마트워크의 기본 시스템 구조 [2]

스마트워크 환경에서 발생하는 보안위협으로 가장 먼저 스마트폰 등의 단말기에 대한 보안위협을 생각할 수 있다. 스마트워크 환경에서 단말기는 시스템

구조 상 외부의 제일 마지막 단에 위치하며 다양한 통신 네트워크와 연결되어 있기 때문에 바이러스나 악성코드가 감염될 수 있으며, 외부인이 단말기 자체에 대한 물리적으로 접근하여 불법 사용할 수도 있다. 단말기에 대한 외부의 보안위협은 기기 내부에 저장된 정보를 유출시킬 수 있는데, 이러한 정보의 유출은 다양한 보안위협을 발생시킨다. 단말기에 저장된 사용자의 개인정보는 해커가 사용자 계정을 도용하여 내부 네트워크로 위장 접근하는데 사용될 수 있으며, 이와 유사하게 IMEI(International Mobile Equipment Identity)이나 MAC(Media Access Control)과 같은 기기 자체의 정보는 해커가 내부 네트워크로 침입하기 위한 접근 연결성을 확보하기 위해 사용할 수 있다. 또한 단말기에서 업무 처리를 위해 사용한 민감한 기밀 정보는 금전적인 목적을 가진 해커의 공격 대상이 될 수 있다. 단말기에 대한 외부의 보안위협은 스마트워크에서 대한 가용성의 측면에서 기기 자체를 사용하지 못하게 함으로써 스마트워크를 마비시킬 수 있으며, 해커가 악성코드를 통하여 내부 시스템에 접근하여 조직 내 전산시스템을 마비시킬 수도 있다.

스마트워크를 운영하는 서버나 데이터베이스 등의 스마트워크를 구성하는 기반시설에서도 다양한 보안위협이 존재하는데, 기본적으로 물리적 접근과 관련된 보안위협이 발생할 수 있다. 만약 직원이 아닌 사람이 스마트워크센터의 중앙 관제실과 같은 곳에 들어갈 수 있다면, 아무리 스마트워크센터 내 업무용 컴퓨터에 보안 기술을 사용하더라도 모든 정보가 유출될 수밖에 없다. 그리고 네트워크 측면에서도 기존의 업무환경을 지원하는 시스템과 스마트워크를 지원하는 시스템 간 연동되는 부분에서 보안성 및 가용성이 침해될 수 있는 보안위협이 존재한다. 또한 스마트워크를 구성하는 무선 네트워크의 경우에는 외부에 노출될 수 있기 때문에, 도청 및 감청의 보안위협을 내재하고 있다. 그리고 분산서비스거부(DDoS) 공격과 같이 악성코드나 유해트래픽으로 기반시설이 마비되어 스마트워크를 중단시킬 수 있는 보안위협도 존재한다.

그리고 스마트워크 시스템을 사용하는 사람의 부주의나 고의로 보안사고가 발생하는, 인적 부분에 대한 보안위협이 존재한다. 앞서 언급한 농협 사고에서도 NH농협의 전산망에 악성코드를 감염시킨 노트북은 소유자가 농협의 내부 전산망에서만 사용해야하는 보안 규정을 무시하고 외부로 반출, 인터넷을 연결, 사용함으로써 사고를 발생시켰다. 조직 내부 인원이 가지고 있는 내부 시스템의 사용과 정보의 열람 등 업무 권한은 조직 내 자산의 보안과 밀접한 관계를 가지고 있기 때문에 인적 보안위협을 중요시해야할 필요가 있다.

1) 재택근무에서의 보안위협

스마트워크에 대한 논의가 있기 전부터 근무의 한 형태로 활용되어온 재택근무는 단어 그대로 직원의 가정에 조직의 업무환경과 동일한 환경을 구성하여 업무를 처리하는 스마트워크의 형태 중 하나이다.

재택근무는 조직 내의 업무환경이 회사 외부(집안)에 위치한다는 점에서부터 보안위협이 발생할 수 있다. 가정에 설치되는 업무용 컴퓨터는 업무 외로 개인적으로 사용되거나 근무자 외의 사람에 의해 사용될 가능성이 회사 내에서 보다 클 수밖에 없는 것이 현실이고, 이러한 업무 외적인 사용은 악성코드나 해킹과 같은 외부의 보안위협으로부터 컴퓨터를 취약하게 한다. 또한 안티바이러스 프로그램의 설치, OS 보안 패치의 관리, 주기적인 보안성 검사 등과 같은 단말기에 대한 보안 관리·유지 절차가 제대로 이루어지지 않을 수 있다. 이와 같은 단말기에 대한 물리적·관리적 통제의 어려움은 곧 보안위협의 발생 원인이 된다.

가정 내 단말기에서 악성코드와 같은 보안위협의 침해가 발생한 경우 악성코드를 통해 컴퓨터 내부에 저장된 기밀 정보가 유출될 수 있고, 사용자 정보나 컴퓨터의 정보가 유출되어 다른 보안위협을 발생시킬 수 있다. 또한 재택근무 환경은 해커가 내부 시스템에 대한 원격 접속의 통신 데이터를 가로채 통신 내용을 도청·감청 할 수 있는 보안위협도 가지고 있다.

2) 모바일 오피스에서의 보안위협

스마트워크의 여러 형태 가운데 이동성이 강조되는 모바일 오피스의 경우 노트북 중심에서 최근에는 스마트폰에 초점을 두고 스마트워크가 구축되고 있다. 스마트폰은 일반적인 악성코드나 바이러스에 감염되지 않아 보안에 있어 노트북과 같은 컴퓨터보다

강한 보안을 가진다고 할 수 있지만, 최근 스마트폰을 대상으로 하는 모바일 악성코드가 등장하고 있고 무선인터넷 사용에 대한 해킹이 가능해지고 있어 보안취약성이 증가하고 있는 실정이다. 또한 스마트폰이 아직까지는 전력 및 성능적인 제약으로 인하여 모바일 백신과 같은 보안 프로그램을 원활하게 사용할 수 없기 때문에 스마트폰 자체가 스마트워크에서의 보안위협을 야기하는 원인 중 하나라고 할 수 있다.

모바일 오피스에 대한 보안위협의 요소로 큰 비중을 차지하는 스마트폰에서는 주로 업무정보나 개인정보의 유출이나 전력 소모 및 서비스거부(DoS) 공격과 같은 스마트폰의 오작동, 콘텐츠 복제와 같은 과금 회피 등의 목적으로 하는 보안위협이 존재하며, 이러한 보안위협은 스마트폰 플랫폼이나 애플리케이션, 네트워크에서 주로 발생한다.

스마트폰 플랫폼에서는 모바일 악성코드나 웜 등이 플랫폼 단에 감염되거나 시스템 내부 파일에 접근하기 위해 시스템을 언락하여 스마트폰 내 주요정보를 침해하거나 스마트폰을 원격 제어할 수 있는 보안위협이 존재하며, 사용자가 검증되지 않은 애플리케이션을 설치하여 스마트폰 내 SMS나 이메일, 연락처 등의 정보를 사용자 몰래 유출할 수 있는 보안위협이 존재한다.

특히 모바일 악성코드의 경우, 2010년 한 해 동안 2009년 대비 250%가 증가하였으며 구글 안드로이드 OS에 대한 악성코드의 경우 2010년 상반기에 400%가 증가하는 등 엄청난 속도로 증가하고 있어 스마트폰에 대한 보안위협을 더욱 급격하게 확대시키고 있다[17].

<표 1> 모바일 악성코드의 유형 [10]

유 형	설 명
장해 유발형	스마트폰의 사용을 불가능하게 만들거나 장애를 유발하는 공격 유형
배터리 소모형	스마트폰의 전력을 지속적으로 소모시켜 배터리를 고갈시키는 공격 유형
과금 유발형	스마트폰의 메시징 서비스 나 전화 시도를 지속적으로 시도하여 과금을 발생시키는 공격 유형
정보 유출형	감염된 스마트폰의 정보나 사용자 정보를 외부로 유출하는 공격 유형
크로스 플랫폼형	스마트폰을 통해 컴퓨터를 감염시키는 공격 유형

모바일 악성코드는 스마트폰에 악성코드가 포함된 애플리케이션이 설치되어 스마트폰에서 기밀 정보를 유출하거나 통신을 도청하거나 악성코드를 유포하거나 조직 내 스마트워크 시스템을 해킹하기 위하여 스마트폰을 원격 제어하는 보안위협이 발생할 수 있다. 초기의 모바일 악성코드는 단순히 악성코드를 유포하거나 단말기의 기능을 중단시켜 가용성을 저하시키는 형태였으나 최근에는 기기에 저장된 정보를 유출하고 금전적인 목적으로 결제 기능을 수행하는 등 특정 이익을 위한 형태로 진화되고 있다. 현재까지 등장한 모바일 악성코드는 <표 1>과 같이 장애 유발형, 배터리 소모형, 과금 유발형, 정보 유출형, 크로스 플랫폼형의 5가지로 분류 할 수 있다[10].

또한 모바일 오피스에서는 이동성을 보장하기 위해서 3G, WiFi, Bluetooth 등과 같은 무선 통신 기술이 사용되어 조직 내 내부 시스템으로의 접근 경로가 다양화되고 있기 때문에 모바일 악성코드가 전파되거나 해킹의 경로로 이용될 수 있는 보안위협이 존재한다. 그리고 기존에 조직 내에서 사용되어온 전사적 자원 관리 시스템(ERP: Enterprise Resource Planning System)이나 고객 관계 관리 시스템(CRM: Customer Relationship Management System), 공급사슬 관리 시스템(SCM: Supply Chain Management System) 등의 레거시 시스템이 업무의 중요한 비중을 차지하고 있어 모바일 오피스 지원 플랫폼과 상호 호환성의 문제가 존재할 수 있으며, 두 시스템의 연동 시 이를 이용한 보안위협이 발생할 수 있다.

마지막으로 스마트폰의 휴대성 때문에 발생할 수 있는 스마트폰의 분실 및 도난으로 인하여 기업 정보가 유출될 수 있는 보안위협이 존재하며, 이와 유사하게 타인이 스마트폰을 소유자 몰래 사용하여 내부에 저장된 기밀을 열람·유출하거나 악의적인 목적으로 정보를 변조 또는 삭제할 수 있는 보안위협도 존재한다.

3) 스마트워크센터에서의 보안위협

스마트워크의 여러 형태 가운데 스마트워크센터를 통하여 업무가 이루어지는 경우 스마트워크센터를 구성하는 공용 IT 인프라 환경의 취약성으로 인하여 보안위협이 발생할 수 있다.

이를 세분화하면 스마트워크센터에서 공용으로 사

용하는 컴퓨터의 경우 계정 분리 등과 같은 다양한 방법으로 사용자의 정보를 분리·보호하도록 하지만, 메모리나 HDD 등의 저장 매체가 포함되어 있기 때문에 사용 정보가 공유되어 유출될 수 있는 보안위협이 존재하며, 이러한 위협들은 결국 조직의 내부 네트워크에 대한 해킹 또는 비인가 접근 등의 보안위협으로 연계된다.

네트워크의 측면에서는 스마트워크센터의 네트워크가 각 조직의 내부망과 연결되어 있는 점을 이용하여 스마트워크센터에 해킹이나 피기배킹(piggyback-ing)을 통하여 침입 후 각 조직의 내부망으로 해킹을 시도할 수 있는, 즉 공격의 우회경로로써 사용될 수 있는 보안위협이 존재한다.

2.2 스마트워크 1.0의 보안을 위한 정책적 고려사항

2.2.1 안전한 스마트워크 환경의 구축을 위한 고려사항 : 방송통신위원회의 권고사항을 중심으로

2011년 1월 방송통신위원회는 '삶과 일의 균형을 통한 글로벌 스마트 강국 구현'을 비전으로 2015년까지 근로자 30%의 스마트워크 실시를 목표로 하는 「스마트워크 활성화 추진계획」을 수립·발표하면서 「스마트워크 활성화를 위한 정보보호 권고」를 제정·보급하였다[6]. 이 권고 사항은 정부차원에서 안전한 스마트워크 환경에 대한 첫 번째 정보보호 권고라는 점에서 중요한 의미를 가진다고 할 수 있다.

따라서 본 절에서는 방송통신위원회의 「스마트워크 활성화를 위한 정보보호 권고」를 중심으로 일반적인 스마트워크 환경의 보안문제 해결방안을 먼저 살펴보고, 다음으로 재택근무·스마트워크센터·모바일 오피스 등 스마트워크의 유형에 따른 보안문제 해결방안을 살펴보도록 한다.

1) 스마트워크 서비스 제공자의 고려사항

스마트워크 서비스 제공에 있어서 보안요소를 고려해야 하는 중요 포인트는 스마트워크 인프라와 스마트워크센터 내 공용 컴퓨터 등이다.

첫째, 스마트워크 환경의 인프라를 안전성과 신뢰성을 유지하기 위해서는 CCTV나 스마트카드 등 물리적 보안통제를 이용한 접근통제를 제공해야 한다. 또한 유·무선 네트워크의 연동구간에 대한 보안성과 가용성을 확보하고, 단말기 인증 및 암호화 통신 등의 보안기능을 제공해야 한다. 그리고 악성코드나 유해트래픽 차단 등 악의적인 공격을 사전에 탐지할 수 있는 해킹대응 기술을 마련하고, 장애발생 시 신속한 대응 및 복구를 통해 지속적인 스마트워크 서비스의 가용성을 확보해야 한다.

둘째, 스마트워크 내의 공용 컴퓨터에 대해서는 업무 관련 중요정보가 컴퓨터에 저장되지 않도록 하고, 내부 규정에 따라 이동식 저장매체와 소프트웨어의 설치를 통제하도록 해야 한다. 또한 컴퓨터의 접속 네트워크는 지정한 통신 수단만을 이용하도록 통제해야 한다.

2) 스마트워크 관리자의 고려사항

스마트워크 환경에서 관리자의 정보보호 고려사항은 단말기·서비스·콘텐츠 보안, 인적자산 관리, 침해사고 대응절차 마련 등이다.

첫째, 단말기를 통한 스마트워크 서비스 이용에서 중요정보를 취급하는 경우 반드시 단말기 잠금 및 암호기능을 제공해야 하며, 웜·바이러스 등의 악성코드 감염에 대응하기 위해서 모바일 전용 백신 설치, 보안패치 적용, 펌웨어 업데이트 등을 주기적으로 수행해야 한다. 또한 원격지에서 단말기에 대한 보안정책 설정 및 변경이 이루어질 수 있도록 원격제어 기능을 제공해야 한다. 무엇보다 단말기의 분실 및 도난위험이 높기 때문에 조직의 중요정보 또는 개인정보 유출에 대비하여 원격백업 및 삭제·복원 등의 보호대책을 마련해야 한다.

둘째, 스마트워크 환경에서 제공되는 서비스를 통해 중요정보를 취급하는 경우 서비스 유형에 적합한 보안대책이 필요하다. 모바일 오피스의 경우에는 비인가자의 불법적 취득 및 접근이 상대적으로 용이하기 때문에, 단말기에 대한 복합인증을 제공하고 중요정보 등에 대해서는 암호화 저장, VPN 사용, 데이터 암호화 통신 등의 보호대책을 마련해야 한다. 클라우드 서비스의 경우에는 이용자에 대한 통합 식별·인증 방식을 도입·관리해야 하고 클라우드 내에 분산된 중

요정보에 대해 안전한 암호화 및 키 관리 등의 보호 대책을 제공해야 한다. 이메일, 그룹웨어, 메신저 등 통합 커뮤니케이션의 사용 시에는 공유되는 비밀정보나 멀티미디어에 대해 비인가자의 수집 및 이용을 방지할 수 있도록 조치를 취해야 한다.

셋째, 스마트워크 업무와 관련된 중요정보 등의 콘텐츠 보호를 위해 암호화나 정보자산의 분류 등의 보안대책을 적용해야 한다. 중요정보의 암호화를 위해서는 이기종 단말기 간의 호환성을 고려하여 DRM 및 암호화 조치를 취해야 하고, 정보의 중요도에 따른 자산분류를 통해 정보자산을 등급별로 보호하는 조치도 병행해야 한다.

넷째, 안전한 스마트워크 서비스의 이용을 위해 인적자산에 대하여 적절한 관리적 보호대책을 마련해야 한다. 스마트워크와 관련한 정보보호 교육·훈련을 정기적으로 실시하고, 내부규정에 따라 업무현황에 대한 모니터링을 실시할 수 있으며, 또한 스마트워크를 적용하고 있는 조직의 경우 정보보안을 위한 관리조직을 별도로 구성할 수도 있다.

다섯째, 사후적 보안대책으로서 침해사고 대응절차는 스마트워크 서비스의 가용성에 있어서 매우 중요하다. 스마트워크 관리자의 입장에서 보안 침해사고는 주로 스마트워크에 활용되는 컴퓨터 및 휴대 단말기의 분실 및 도난 시 발생하는데, 이러한 사고 발생 시 비인가자의 데이터접근을 제한하고, 도난 또는 분실된 단말기의 용도에 따라 비인가자가 우회하거나 인증정보를 알아내더라도 원천적으로 중요정보에 접근이 불가능하도록 하는 대응절차의 마련이 요구된다. 또한 정보의 유출 및 위·변조 사고의 발생 시에는 원인분석방법, 대응방법 등 신속한 초기대응을 위한 절차를 내부규정으로 마련해야 한다.

3) 스마트워크 이용자의 고려사항

스마트워크 이용자가 고려해야 하는 정보보호 준수사항은 이용자가 자발적으로 정보보호 노력을 기울여야 한다는 전제가 성립되어야 한다. 이용자 스스로 비밀번호를 주기적으로 변경한다든지, 운영체제나 백신프로그램을 최신 버전으로 업데이트하여 관리한다는 등의 사항은 스마트워크 이용자의 보안인식 수준에서 비롯된다고 할 수 있다.

<표 2> 스마트워크 정보보호 고려사항

준수사항		세 부 내 용
서비스제공자	인프라 보안	안전한 스마트워크 인프라 환경을 위한 해킹대응, 유·무선 네트워크 보안, 물리적 보안 등 기술적 보호대책
	공용컴퓨터 보안	센터 내 공용 컴퓨터의 기업저장장치, 이동식 저장매체 등에 대한 기술적 보호대책
관리자	단말기·서비스 콘텐츠 보안	악성코드, 분실·도난 등으로부터 단말기, 서비스, 콘텐츠 보호를 위한 관리적 보호대책
	인적자산 관리	이용자의 안전한 스마트워크 서비스 이용을 위한 교육·훈련, 모니터링 등의 관리적 보호대책
	침해사고 대응절차	스마트워크 환경에서 발생 가능한 다양한 보안 침해사고에 대한 대응절차
이용자	정보자산 취급·관리	정보자산의 적절한 보호를 위해 이용자가 점검 및 수행할 수 있는 수칙 제공
	인식제고	이용자의 지속적인 정보보호 인식제고를 위한 정보보호 주의사항, 대응절차 등의 교육 및 학습 활동 수행
	침해사고 대응	스마트워크 환경에서의 보안 침해사고 발생 시 이용자가 신속하게 대처해야 할 사항 안내

2.2.2 스마트워크 유형에 따른 보안문제 해결방안

1) 재택(원격)근무 환경

재택근무 형태의 스마트워크에서 발생하게 되는 정보보안 침해사고의 영역은 크게 세 부분으로 나눌 수 있다. 먼저 스마트워크 업무 공간은 댁내에 조직의 업무시스템과 연결되어 있는 개인 컴퓨터가 설치되는데, 이에 대한 비인가자의 접근을 통제하는 것이 가장 중요하다. 이를 위해서는 정보보호 권고에 따라 CCTV나 바이오인증 등을 사용하여 물리적 보안을 수행할 수 있는데, CCTV의 경우 댁내 개인의 프라이버시 침해 이슈가 존재할 수 있어 적합하지 않을 수 있다.

두 번째는 유·무선 네트워크의 구축 구간으로, 이 영역에서는 기밀성과 가용성이 중요한 보안요소이다.

기밀성 측면에서 비인가자가 악의적인 목적으로 중요정보를 탈취하는 것을 막기 위해 가상사설망(VPN)의 설치나 데이터를 암호화하여 송·수신해야 하며, 가용성 측면에서는 네트워크 인프라가 손괴 또는 파괴되지 않도록 물리적 보안을 철저히 해야 한다.

세 번째는 스마트워크 서비스 운영과 관련된 데이터베이스나 서버 등의 물리적 설치 공간에 대한 접근통제이다. 이 영역에 대해서는 반드시 출입문에 대한 인증시스템을 설치하고 출입기록 문서를 작성·보관해야 한다. 또한 CCTV를 설치하여 출입자에 대한 모니터링을 실시해야 한다. 그러나 재택근무의 경우에는 무엇보다 업무담당자의 보안인식제고와 자발적이고 능동적인 보안관리가 중요하다.

2) 모바일 오피스 환경

모바일 오피스 환경에서는 모바일 단말기의 분실 및 도난에 대비하는 것이 가장 중요하며, 사용자의 부주의 등으로 인해 분실 및 도난사고가 발생한 경우에는 신속한 보고를 통해 원격제어 방식으로 기기 내의 중요정보를 삭제할 수 있어야 한다.

또한 모바일 미들웨어 플랫폼을 대상으로 하는 바이러스 및 웜, 시스템 언락, 키보드 해킹 등의 악의적 공격들에 대해서는 시스템 언락을 탐지·차단하는 기능을 구현해야 하고, 단말기 내에 모바일 전용 백신을 설치하여 최신버전의 상태를 유지해야 한다. 모바일 오피스에 활용되는 애플리케이션들은 앱 스토어 기반의 시스템을 통해 배포·설치하도록 하되, 배포 전 애플리케이션의 보안성 검증을 철저히 해야 한다. 미국의 보안업체인 Lookout에서 50만개 이상의 애플리케이션 분석을 통하여, 침해위험성 및 악성 여부를 식별하는 App Genome Project를 추진하고 있다.

<표 3>은 모바일 오피스 환경에서 주로 이용되는 단말기인 스마트폰에 대한 위협을 중심으로 대응방안을 정리한 것이다[10].

모바일 오피스 환경에서 스마트폰 등의 단말기로 중요정보를 송·수신하는 경우에는 3G나 WiFi 접속을 이용하는데, 이 때 송·수신되는 데이터의 암호화는 모바일 오피스 환경의 기밀성을 보장한다. 따라서 원격 네트워크 접속에서 인증과 송·수신 데이터의 암호화 기능을 갖춘 시스템을 구축·사용하는 것이 중요하며 이를 위해 원격접속 VPN 기술을 적용할 수 있다.

<표 3> 스마트폰 보안 대응방안 [10]

위험분류		세부공격	대응방안
공격대상	플랫폼 공격	• 바이러스/웜 • 시스템 언락 • 키보드 해킹	• 시스템 언락 탐지 • 스마트폰 백신 • 취약점의 빠른 보완
	애플리케이션 공격	• Malicious 앱 • Fishing 앱	• 앱스토어 기반 설치 권장 • 앱스토어 App 검증 강화 • 자원 제어 모니터링
	네트워크 공격	• WiFi 도청/변조 • 서비스거부 공격	• WiFi 통신 암호화/인증 • 자원 제어 모니터링
공격목표	정보 유출	• 개인정보 유출 • 업무정보 유출 • 위치정보 노출	• 앱스토어 기반 설치 권장 • 앱스토어 App 검증 강화 • 자원 제어 모니터링 • WiFi 통신 및 내장정보 암호화/인증
	오작동	• 디바이스 전력 소모 • SMS/MMS 과금 • 서비스거부 공격	• 자원제어 모니터링
	과금 회피	• 콘텐츠 무단복제	• 시스템 언락 탐지

3) 스마트워크센터 환경

스마트워크센터의 경우에는 센터 출입통제와 센터 내의 정보자산에 대한 보안관리가 가장 중요하다. 스마트워크센터 출입통제를 위해서는 CCTV, 스마트카드, 생체인증기술 등을 적용하여 물리적 보안통제를 수행해야 한다.

센터 내의 정보자산에는 주로 공용 컴퓨터나 저장매체에 대한 보안대책이 요구된다. 이 때에는 재택근무의 경우보다 로컬 스토리지를 사용하지 않아야 하며, 업무 관련 중요정보는 서버기반의 스토리지에만 저장하도록 한다. 로컬 스토리지를 사용하는 경우에는 컴퓨터 재부팅이나 사용자 변경 시 내부 저장 정보를 자동 삭제 또는 초기화하는 기능을 구현하는 것이 좋다. 그리고 공용 컴퓨터에는 바이러스·악성코드에 대한 백신이나 키보드 해킹보안 프로그램 등을 설치하고 보안패치를 주기적으로 업데이트 하여 최신의 보안 상태를 유지하도록 해야 한다. 그리고 가급적 USB나 외장형 스토리지 같은 이동식 저장매체는 사용하지 않는 것을 원칙으로 하되, 불가피하게 이동식 저장매체를 사용해야 하는 경우 저장되는 중요정보를 반드시 암호화하여 저장하도록 해야 한다.

또한 스마트워크센터에서 문서를 출력 시에도 문서의 등급분류에 따라 높은 등급의 중요정보는 문서

출력을 제한하고 디지털콘텐츠권리관리(DRM)를 적용하는 등의 보안대책을 시행해야 한다. 스마트워크 센터의 사무공간이 개방된 형태를 가지고 있다면, 담당자 외에 주변 사람이 민감한 자료를 엿볼 수 없도록 하는 보안모니터나 보안필터를 활용하는 것도 가능하다.

3. 스마트워크 2.0에서의 보안 이슈

지금까지 '언제(시간적 자율) 어디서나(공간적 자유)' 업무 생산성 향상과 효율성 증대에 초점을 둔 스마트워크 1.0을 중심으로 정보보안 관리에 대한 이슈와 위협 그리고 해결방안에 대해 살펴보았다. 그러나 최근에는 시간적 자율과 공간적 자유에 추가로 집단지성을 강조하는 스마트워크 2.0가 활발히 논의되고 있다. 스마트워크 2.0 개념의 핵심은 스마트워크 1.0에 집단지성의 변수를 결합시켜 창의적 가치를 창출하는 것으로 협력성과 창의성이 큰 비중을 차지한다[4].

정보보안의 관점에서는 새로운 환경이 확산되기 전에 해당 환경에서의 보안 관리의 문제를 살펴보고 대비하는 것이 올바른 대응이라 하겠다. 따라서 다음에서는 협력성과 창의성이라는 측면에서 스마트워크 2.0의 보안 이슈에 대하여 살펴보도록 한다.

3.1 협력성 증가로 인한 보안 이슈

스마트워크 2.0에서 요구되는 협력성은 '조직 내·외부의 이해관계자와 함께 문제를 해결할 수 있는 신뢰를 기반으로 하는 장을 통한 문제 해결'로 정의된다[11]. 즉, 스마트워크 2.0의 협력성을 확보하기 위해서는 시간적·공간적 제약을 탈피하면서 영상회의와 같은 스마트워크 1.0의 모습보다 협력적인 해결 공간을 고려해야 하며 이러한 공간은 신뢰성을 갖추어야 한다.

이러한 의미에서 최근 활성화 되고 있는 클라우드 컴퓨팅 서비스 등은 스마트워크 2.0의 협력성을 위한 기술이라 할 수 있다. 클라우드 컴퓨팅 서비스는 개인의 데이터나 SW 등을 중앙에 집중시켜 언제든 공유할 수 있게 함으로써 유휴 컴퓨팅 자원의 낭비를 막고 서버자원의 효율도 증가시키면서 업무의 생산성을 향상시킬 수 있도록 한다.

또한 MS에서 Office 프로그램의 차기 버전으로 내세우는 MS Office Live Workspace나 Google Docs 등에서 제공하는 협업적 도구들은 스마트워크 2.0의 협력성에 부합된다고 할 수 있다. 업무담당자는 이들 서비스에서 제공하는 도구와 자택의 개인 컴퓨터나 모바일 단말기 등을 통해 언제 어디서나 자료를 업·다운로드하고 업무를 진행할 수 있으며 거의 실시간으로 다수의 업무관계자가 참여하여 업무를 진행할 수도 있다.

이러한 새로운 환경의 보안 이슈를 생각해 보면, 가장 먼저 데이터의 무결성 관리를 어떻게 보장할 것인가를 고민할 수 있다. 클라우드 시스템이나 협업편집시스템 등과 같이 비대면에 의한 협력 환경에서는 누군가 업로드한 데이터에 오류가 없을 것이라는 신뢰를 바탕으로 업무가 진행된다. 따라서 데이터에 대한 악의적인 훼손 등의 무결성 침해 요인을 제거하는 문제가 매우 중요하다고 하겠다.

다음으로 인증관리의 문제를 생각해 볼 수 있다. 승인받지 않은 제3자의 접근은 중요정보의 유·노출뿐 아니라 정보의 무결성에도 직접적인 침해를 가할 수 있다. 즉, 비인가자에 대한 접근통제가 실패한다면 신뢰를 기반으로 하는 협업 시스템의 협력성이라는 스마트워크 2.0의 가치를 달성하지 못하게 된다.

또한 데이터 무결성 유지와 관련하여 데이터 변경의 추적성 문제를 고려해야 한다. 비인가자의 악의의한 데이터 변경·훼손과 인가받은 업무 담당자의 실수에 의한 오류 등에 대해서 그 당사자가 누구인지 확인할 수 없다면 비대면 상대방과의 협업을 유지할 수 없게 된다.

3.2 창의성 증가로 인한 보안 이슈

협력성과 같이 스마트워크 2.0의 특징으로써 식별되는 창의성은 '소셜 매체에 암묵적으로 유통되는 지능과 지식을 여과하고 종합하여 업무를 창의적으로 수행함'으로 정의된다[11]. 스마트워크 2.0에서 창의성 확보를 위해서는 소셜 매체와 같은 새로운 유형의 미디어, 통신수단 등의 효과적인 활용이 요구되며, 소셜 네트워크 서비스(SNS)가 제공하는 사이버공간이나 웹 2.0에서 등장한 지식공유 서비스 등이 스마트워크

2.0의 창의성을 위한 기술로써 사용된다고 볼 수 있다.

Facebook이나 Twitter로 대표되는 SNS는 특정 서비스마다 약간의 차이가 있긴 하지만 기본적으로 웹 기반 서비스로 친구나 동일 관심사를 가진 사람들을 네트워크를 통해 연결하여 상호간 의사소통이나 중요한 메시지 전달, 정보 또는 자료의 공유를 가능하도록 한다. 웹 2.0의 지식공유 서비스는 WikiMedia 재단에서 운영하는 WikiPedia 백과사전, Google의 Knol 서비스, NHN의 지식In 서비스 등이 존재하며, 이러한 서비스들은 특정 주제의 지식 구축에 있어 사용자의 참여를 통하여 사용자들이 가지고 있는 지식을 모으는 것을 핵심으로 한다.

새로운 미디어나 통신 공간을 통하여 창의적인 업무를 수행하는 스마트워크 2.0에서는 기본적으로 이들 미디어와 공간이 제공하는 정보가 업무에서 사용될 수 있을 만큼 신뢰할 수 있는지를 고려해야 하는데, SNS와 지식공유 서비스들은 개인에 의해 정보가 공유되기 때문에 정보의 옳고 그름을 검증하기 어려울 수 있으며, 또한 의도적인 정보 조작이 가능하기 때문에 업무 사용을 위한 신뢰성이 보장되는지 판단하기 어려운 보안 이슈가 존재한다. 만약 조직의 업무계획이나 R&D 전략 수립 등과 같은 중요한 의사결정에 있어 잘못된 정보가 사용되는 경우 잘못된 정보의 리스크는 무시할 수 없을 만큼 클 것이다.

또한 이러한 정보들이 조직 업무에 사용되는 경우 개인정보나 저작권의 침해 등이 발생하지 않는지 검토해야한다. 지식공유 서비스의 경우에는 정보 공유에 초점을 두기 때문에 이러한 문제가 발생하지 않을 수도 있지만, SNS 등에서의 정보는 주로 사적인 정보 전달을 목적으로 하기 때문에 조직의 이익 추구의 목적으로 SNS 상의 정보를 수집·분석하는 경우 개인정보나 저작권의 침해 등이 발생할 가능성이 존재한다.

또한 SNS 서비스의 이용 주체가 SNS 상의 계정을 사용함에 있어서도 조직과 개인의 구분을 명확하게 하지 않아 조직의 기밀정보나 유출되지 않아야 할 민감한 정보가 유출될 수 있다. 대부분의 SNS는 개인 이메일이나 메신저 등 정보와 개인의 성향, 소속 등의 정보 분석을 통하여 소셜 네트워크 연결성 구축에 있어 사용자의 '사회성'에 초점을 두고 소셜 네트워크를 추가·확장하는데, 이러한 SNS의 '사회성' 특성으로 인해 개인적인 관계로 구축되어 있는 소셜 네트워크를 통해 조직의 업무를 수행하는 경우 조직과 전혀 상관없는 타인이 민감한 조직의 정보를 볼 수 있으며, 또한 사용자의 인지 없이 정보가 유출될 수 있다. 따라서 이들 서비스 등을 통한 업무 수행에 있어 조직의 영업정보나 산업기밀정보, 개인정보와 같은 중요한 정보가 유출되지 않도록 해야 한다.

4. 결 론

스마트워크 도입현황이나 전망을 볼 때 스마트워크는 분명 지금보다 확대될 것이며, 스마트워크가 공공 및 민간 기업에서 지금보다 활성화되면 그 반대급부로서 정보보안 침해사고도 증가할 것으로 판단된다.

재택근무, 모바일 오피스, 스마트워크센터 등으로 대표되는 스마트워크 1.0에서는 정보보안 침해 관련 사고들이 간헐적이지만 비중 있게 보고되고 있으며, 이러한 침해사고 사례는 스마트워크 2.0을 대비하는 우리에게 안전하고 신뢰성 있는 스마트워크 환경을 구축하는 데 밑거름이 될 것이다.

<표 4>는 스마트워크 1.0과 2.0의 차이와 이에 따른 정보보호 고려사항의 비교로, 스마트워크의 진화에 따라 정보보호의 대상이나 고려사항은 보다 정보보안의 관점에서 더 심화됨을 확인할 수 있으며, 이러한 심화는 정보보호 분야에서 이미 진행되어온 정보보호의 패러다임과 유사하다.

<표 4> 스마트워크 진화에 따른 정보보호 고려사항

구분	스마트워크 1.0	스마트워크 2.0
정보보호의 대상	스마트워크를 구성하는 단말기 및 시스템	스마트워크 내의 정보(데이터) 및 사람
정보보호의 고려사항	가용성과 기밀성에 초점을 둠	무결성과 기밀성에 초점을 둠

새로운 환경이 구축되고 새로운 침해기술이 등장하더라도 그것에 대응하는 보안기술 체계는 기존의 대응기술을 얼마나 적절하고 유기적으로 구성하고 적용하였느냐에 그 성패가 달렸다고 할 수 있다. 따라서 스마트워크 2.0의 새로운 가치의 등장으로 인한 보안위협을 완화하고 방지하기 위해서는 앞서 논의한

스마트워크 1.0에서의 보안문제 해결방안을 새로운 환경에 맞도록 보완하는 것이 중요하다 하겠다.

참 고 문 헌

[1] 김정언 (2010). 스마트워크 추진 현황과 활성화 방안, KISDI Premium Report 10-08, 정보통신정책연구원.

[2] 나성욱 · 이윤희 · 지순정 (2010). 스마트폰과 모바일 오피스의 보안이슈 및 대응전략, CIO Report Volume 26. pp.1-23.

[3] 남양섭 (2011). 소셜 네트워크를 활용한 스마트워크의 발전적 시도, CIO BIZ 스페셜리포트 - 분석과 전망, 2011년 4월 6일.

[4] 노규성 · 유승엽 · 송경석 · 김은희 (2010). 스마트워크 산업 경쟁력분석 및 육성방안, 한국산업기술진흥원.

[5] 박은규 (2011). 스마트 환경 하의 노무관리상 문제점과 고려사항, 월간인사관리 제258호, 한국인사관리협회.

[6] 방송통신위원회 (2011). 스마트워크 활성화를 위한 정보보호 권고.

[7] 벤처기업협회 (2009). 그린 SW 기술 및 시장 동향 보고서 - Virtual Office 분야.

[8] 이각범 (2011). 국가정보화의 당면과제와 미래과제, 한국IT리더스포럼 3월 정기조찬회 발표자료.

[9] 이준호 (2010). 스마트 모바일의 발전과 정보보안, 방송통신정책 제22권 13호 통권 489호, pp. 17-33, 정보통신정책연구원.

[10] 임종인 · 백승조 (2010). 신IT기술 응용 확산과 디지털재난 유형 예측 연구, 경제 · 인문사회연구회 협동연구총서 10-12-16, 정보통신정책연구원.

[11] 최성 (2011). 보다 똑똑한 세상을 열기 위한 스마트워크 정의와 전망, 정보처리학회지 제18권 제2호, pp.6-17.

[12] 한국정보화진흥원 (2009). 녹색생활 실천전략 IT기반 원격근무 - 원격근무 대국민수요조사, IT&Future Strategy 보고서 제11호.

[13] 홍효진 (2011). 스마트워크의 성공적 정착을 위한 제언, IT정책연구시리즈 제5호, 한국정보화진흥원.

[14] Sean Ryan & Charles J. Kolodgy & Stephen D. Drake (2010). World wide Mobile Security 2010 - 2014 Forecast and Analysis, IDC DOC #222348.

[15] Spencer Parkinson (2011). Survey Results: The Consumerization of IT from the End User's Perspective, Symantec's Endpoint Management Community Blog, 17 May 2011.

[16] Spencer Parkinson (2011). What Does the Consumerization of IT Mean to You?(An End-User Survey on Personal and Business Smartphone Trends), Symantec's Endpoint Management Community Blog, 20 April 2011.

[17] Juniper Networks (2011). Malicious Mobile Threats Report 2010/2011 - An Objective Briefing on the Current Mobile Threat Landscape Based on Juniper Networks Global Threat Center Research.

이 경 복

2008 고려대학교 산업시스템 정보공학과(학사)
2010 고려대학교 정보경영공학 전문대학원 정보경영공학과 정보보호전공(공학석사)
2010~현재 고려대학교 정보보호대학원 정보보호학과 박사과정
관심분야: 정보보호정책, 프라이버시 보호, 디지털포렌식정책, 융합기술보안 등
E-Mail: isnare@korea.ac.kr

박 태 형

2002 고려대학교 서양사학과(학사)
2004 고려대학교 행정학과(행정학석사)
2011 고려대학교 정보경영공학전문대학원 정보경영공학과 정보보호전공(공학박사)
2011~현재 고려대학교 정보보호대학원 정보보호연구원 연구교수
관심분야: 정보보호정책, 전자정부, 성과관리
E-Mail: mosto2004@korea.ac.kr

임 종 인

1980 고려대학교 수학과(학사)
1982 고려대학교 수학과(이학석사)
1986 고려대학교 수학과(이학박사)
1986~2001 고려대학교 자연과학대학 정교수
2001~현재 고려대학교 정보보호대학원 원장/교수, 대검찰청 디지털수사자문위원회 위원장, 금융보안연구원 보안전문기술위원회 위원장 등
관심분야: 정보법학, 사이버전, 디지털포렌식, 개인정보보호, 융합기술보안 등
E-Mail: jilim@korea.ac.kr