# 기업 소셜네트워크 서비스의 모바일 단말 활용을 위한 보안위협 및 대응방안 연구

**최민희***, 김동욱*, 정남준*
한전 전력연구원 S/W센터*

# Study on Security Threats and Countermeasures for Applying Mobile Devices in the Enterprise Social Network Service(SNS)

Min-Hee Choi*, Dong-Wook Kim*, Nam-Jun Jung*
KEPCO Research Institute*

**Abstract** - 소셜네트워크의 등장은 기업 환경에도 많은 변화를 가져오고 있다. 초기의 기업 소셜네트워크서비스(SNS)는 자사 고객들과의 커뮤니케이션 채널로 활용되었지만, 최근의 기업 SNS는 자사내의 조직 강화 수단으로 인식되기 시작하고 있다. 직원들의 수평적인 아이디어 뱅크와 인맥 형성(Human networks)을 위해서 많은 기업들이 SNS 활용을 시도하고 있다. 기업 SNS의 활용도가 높아지기 위해서는 Anywhere, Anytime 접근 환경이 지원되어야 한다. 기존 SNS 활용도를 폭발적으로 증가시킨 스마트폰과 같은 모바일 단말 지원도 기업 SNS에서도 이루어져야 한다. 그러나, 모바일 단말은 PC와 같은 기존 사용자 환경에 비해서 보안적으로 많은 취약점을 갖고 있다. 이 논문에서는 기업 SNS에 모바일 단말 활용 시 대두될 수 있는 보안 취약성을 점검하고, 그에 대한 대응책을 제시한다.

## 1. 서 론

소셜네트워크서비스(Social Network Service, 이하 SNS)란 온라인상에서 이용자들이 인맥을 새롭게 쌓거나 기존 인맥과의 관계를 강화시키는 일을 할 수 있게 해주는 서비스를 의미한다.

SNS등장 초기에는 일반 인터넷 사용자들의 커뮤니케이션 중심적인 활동을 지원하였지만, 지금은 기업들에서도 SNS를 사업 영역으로 인식하기 시작했다[1]. 소셜네트워크는 기업 환경의 변화를 가져오고 있다. 초기에는 고객과의 소통을 목적으로 SNS의 활용에 초점을 맞추어 개발되어 왔다[2]. 그러나 최근 소셜네트워크서비스(SNS)는 기업의 조직 강화 수단으로 진화하고 있다[2,3]. 기업들이 고객 커뮤니티 채널로 사용하던 SNS를 최고경영자와 일반 직원간에 소통하는 수평적인 아이디어 공유 방법으로 활용하고 있다. 이는 기업 위기에 신속히 대처하는 통로로 SNS만큼 효율성이 뛰어난 채널이 없다는 전략적 판단에서다. 특히 신기술을 빠르게 흡수하는 IT업체나 통신업체들은 물론 보수적인 금융권에서 SNS가 임직원간 커뮤니케이션 수단으로 활용돼 주목받고 있다[3].

그러나, SNS의 활성화를 위해서 스마트폰과 같은 모바일 단말의 지원은 기업내 네트워크 환경에 보안 취약성을 불러온다. 이러한 보안 취약성 문제로 인해서 현재 공공기관에서는 모바일 단말의 업무지원 시스템을 구축하지 못하고 있다. 따라서 이 논문에서는 기업 SNS에 모바일 단말 활용 시 대두될 수 있는 보안 취약성을 점검하고, 그에 대한 대응책을 제시하고자 한다.

## 2. 기업 SNS 플랫폼 구축 전략

지금까지 기업들은 임직원 개인들의 가치 있는 정보를 모으고 정리하여 기업의 자산으로 만들기 위해서 노력해왔다. 이를 위해서 기업들은 Knowledge Management System을 구축하고 임직원들에게 적절한 포상과 강제를 통해서 지식을 축적해왔다. 그리고 축적된 방대한 정보에서 필요한 정보를 찾을 수 있는 Information Search System을 구축하여 서비스를 제공하였다. 이 전략(Strategy)은 잘 운영될 수 있다면, 좋은 결과를 낳을 수 있다. 또한 많은 성공 사례들도 있다. 그러나 이 방식은 조직의 규모가 커질수록 운영 효율은 낮아지는 문제점을 가지고 있다.

조직이 커지고, 축적된 정보의 양이 방대해지면 검색되어 나오는 결과가 많아지게 되고 그 중 필요한 정보를 찾기 어려워진다. 결국 가장 가치 있는 정보는 내가 원하는 것을 누구에게 얻을 수 있는지 혹은 어떻게 찾아야 하는지 아는 것이 최우선이다. 이때 기업조직내의 SNS 시스템의 힘을 이용하면 문제해결을 쉽게 할 수 있다. 잘 알려져 있듯 트위터의 강력한 정보 전파력은 강력한 무기가 될 수 있다. 또한 관심사항과 전문분야를 기반으로 인맥형성을 도와주는 페이스북 스타일의 SNS 시스템은 조직 내에서 항상 최신의 유용한 정보가 최우선으로 유통될 수 있도록 도와주는 역할을 할 수 있다. 물론 기존의 지식관리 시스템도 활성화 될 수 있는 원동력을 제공해줄 수 있다.

### 2.1 기업 SNS의 특징

사내에 소셜네트워크(SNS) 도입시 기업은 다음과 같은 장점을 취할 수 있다.

- **정확한 정보**: SNS의 인맥을 이용하여 항상 정확하고 빠른 정보 습득이 가능하다. 정보검색 시스템보다 더 정확성 높은 정보 제공이 가능하다.
- **빠른 커뮤니케이션**: PC와 스마트폰과 같은 다양한 환경을 통해서 시간과 장소에 구애 받지 않기 때문에 빠른 커뮤니케이션 지원이 가능하다.
- **쉽고 간단한 의사소통**: 마이크로 블로깅을 지원하기 때문에 자유로운 커뮤니케이션이 가능하다. 기존의 보고서와 같이 무겁거나 형식적인 대화에서 벗어나 모두가 동등한 위치에서 자유로운 의사소통이 가능하도록 도와준다.
- **사내 정보 유지**: 사내 구성원들로만 소셜커뮤니티가 형성되기 때문에 내부 자료와 의견을 안전하게 교환할 수 있으며, 회사의 중요 정보가 외부로 유출되지 않는다.

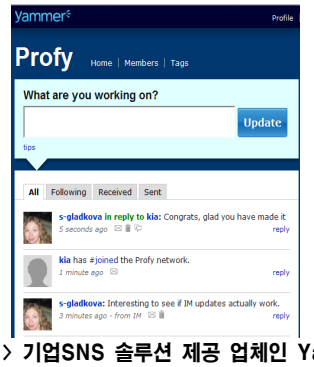
### 2.2 기업 SNS 구축 사례 연구

사내 SNS 서비스를 도입하기 위해서는 다음과 같이 두 가지의 방법을 고려해 볼 수 있다. 첫 번째는 외부 업체의 기업형 SNS 솔루션을 활용하는 방법이고, 두 번째는 기업 자체적으로 SNS 서비스 플랫폼을 개발 및 구축하는 방법이다. 이 두 방법은 비용, 시간, 그리고 활용 측면에서 장단점을 갖고 있다.

#### 2.2.1 외부의 기업형 SNS 서비스 활용

기업형 SNS 서비스 제공 업체에서 제공하는 불특정 다수의 회사들을 위한 기업형 SNS 서비스 활용하는 방법이다. 이 방법은 SNS 서비스를 제공하는 서버가 외부 업체에 있고, 회사는 사용 비용을 지불하고 서비스를 이용하는 방법이다. 몇몇 기업들은 트위터(Twitter)[8], 야머(Yammer)[9]와 같은 기존 SNS 서비스를 기반으로 자사의 SNS 서비스 구축을 시도하고 있다. 예를들어, SK그룹의 경우 최근 오픈한 그룹포털에 트위터에 기반한 SNS 서비스를 포함시켰다. LG전자도 야머를 일부 R&D 조직에서 SNS를 통한 소통의 창구로 사용하고 있으며 LG CNS는 트위터 API를 기반으로 SNS서비스를 사내에 구축한 경험을 갖고 있다.

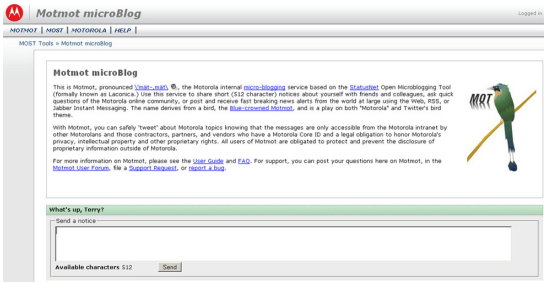
외부의 SNS 서비스를 활용하기 때문에 비용 및 시간적 측면에서 장점이 많다. 그러나 사내 정보가 외부 기관에 존재하기 때문에 데이터 가공을 통한 경영 의사결정에 반영이 어렵고, 회사내 기구축된 시스템과 연동이 어렵기 때문에 다양한 서비스 개발이 어렵다. 외부 회사에서 제공하는 SNS 솔루션이 더 이상 제공되지 않는 경우, 그동안 축적된 정보를 잃어버릴 수 있다.




<그림 1> 기업SNS 솔루션 제공 업체인 Yammer

### 2.2.2 사내 SNS 서비스 플랫폼 구축

특정 기업에서 자사의 환경을 고려하여 사내에 SNS 서비스 플랫폼을 구축하는 방법이다. 사내에 SNS 서비스를 제공하는 서버가 있다는 특징을 갖고 있다. 대표적인 IT기업인 Motorola는 오픈소스 Statusnet를 기반으로 자사 SNS 서비스 플랫폼인 MotMot를 구축하여 사내 시스템과 연동하였다[4]. 이 방법은 자체적으로 SNS 서비스를 개발하기 때문에 많은 시간과 비용이 요구되는 단점을 갖고 있다. 그러나 회사내에 정보가 축적되기 때문에 다양한 정보 활용에 의해서 경영 의사결정에 반영이 용이하고, 정보의 사외 유출 가능성이 낮기 때문에 보안 측면에서 장점이 있다. 또한 자사 SNS 서비스 플랫폼을 갖기 때문에 손쉽게 회사내에 기구축된 시스템들과 연동이 가능하기 때문에 SNS 서비스 활용도를 높일 수 장점이 있다.




〈그림 2〉 오픈소스 기반으로 개발된 Motolora의 MotMot

## 3. 모바일 단말의 보안 취약성

SNS 도입을 고려중인 기업들은 SNS 서비스 도입으로 얻게 되는 문제도 함께 고려를 해야 한다. 가장 먼저 불법 침입, 내부자의 불법적 사용을 방지하는 보안 문제이다.

- **모발 단말의 분실**: 사내 SNS 서비스를 도입하게 되면, 스마트폰과 같은 모바일 단말 이용이 활발해지므로, 개인 모바일 단말의 보안 대책도 함께 요구된다. 만일 모바일 단말을 분실하는 경우, 회사의 정보가 유출될 수도 있고, 스마트폰 어플을 이용하여 사내 시스템내에 불법 접근도 이루어질 수 있다.
- **불법 침입**: SNS 서비스의 활용을 높이기 위해서는 스마트폰과 같은 모바일 단말 활용을 권장해야 한다. 그러나 모바일 단말은 외부에서 사내 서비스 접근을 요구하기 때문에 외부로부터 사내 침투 경로로 활용될 수 있다.
- **내부 공격**: 불법 공격자는 외부에 노출된 SNS 플랫폼에 불법 침입하여 사내의 다른 시스템들의 공격 사이트로 활용할 수 있다. 이것은 내부 네트워크 내에 있는 시스템들간의 보안의 취약성 때문에 커다란 손실을 불러일으킨다.
- **정보 탈취**: SNS 서비스 접근 과정에서 피싱 사이트 또는 악성코드 유포 사이트로 유도될 수 있다. 또한 SNS 서비스내에서 공유되는 정보가 위조 또는 변조될 가능성이 있다. 즉, 메시지 등록시 악의적인 웹 사이트 주소가 삽입되어 악성코드 유포 사이트로 유도할 수도 있다.
- **내부자의 불법 사용**: 회사 임직원들의 불법적인 정보 유출을 위해서 SNS 플랫폼 사용이 가능하다. 다양한 접근 매체의 증가로 이를 막는 것은 어려운 일이 되어 가고 있다.
- **바이러스**: SNS의 대중적 인기는 외부 공격자들에게 가장 이상적인 공격 대상을 제공하고 있다. 공격자의 입장에서는 연동 서비스 또는 웹사이트에 바이러스를 내장시켜서 손쉽게 기업 내 수많은 컴퓨터를 일시에 바이러스에 감염시킬 수 있다.

## 4. SNS활용 모바일 단말의 보안 대응방안

SNS에는 예상치 못한 위험이 내재되어 있으며, 이는 강력한 보안 대책 및 사례를 참조하여 보안 취약성을 최소화 시킬 수 있다.

- **모발 단말 원격 제어**: 모바일 단말 분실 시 사내 정보 유출 및 사내 시스템에 불법 접근을 차단하기 위해서 모바일 단말내 자료의 원격 삭제 및 초기화 기능을 내장하여야 한다. 단말의 분실 신고시, 관리 본부는 이 기능을 이용하여 해당 단말을 초기화 하여 불법 활용을 차단할 수 있다.
- **불법 침입 차단**: 외부에서 사내 SNS 서비스 접근이 이루어지기 때문에 외부로부터 사내 침투 경로로 활용될 수 있다. 따라서 DMZ 내에 SNS 서버를 구축하여 사내 시스템과 격리시켜서 SNS 서버가 외부의 공격 경로로 활용되는 것을 방지해야 한다.
- **접근 제어**: 만일 외부의 불법 침입에 방화벽이 뚫린다하여도 사내의 다른 시스템은 보호되어야 한다. 이와같은 공격에 대응하기 위해서 selinux와 같은 보안 운영체제 기반으로 SNS 시스템이 구축되고, 이를 통해 접근 통제 및 사용자 행위 감시가 이루어져야 한다.
- **통신 보호**: 외부 인터넷망과 사내 SNS 서버 연결 시 정보의 불법적인 변경 및 취득을 방지하기 위해서 모든 통신 채널을 암호화하여야 한다.
- **네트워크 모니터링**: 회사 임직원들의 부적절한 정보 유출 방지를 위해서 네트워크 모니터링 시스템을 구축해야한다. 그러나 이 방법은 개인 프라이버시 침해 논란이 있기 때문에 현명한 방법이 강구되어야 한다.
- **강력한 패스워드 정책**: 공격자들은 개인들의 정보를 이용하여 사용자들의 패스워드를 유추한다. 가령, 생년월일, 전화번호, 또는 사번들은 패스워드를 유추하기에 좋은 정보들이다. 따라서 이러한 패스워드 유추를 막기 위해서 엄격한 패스워드 정책을 수립해야 한다.
- **사용자 계정 관리**: 사내 SNS 시스템을 도입한 후, 활용이 되지 않는 사용자의 계정에 대해서 관리를 해야 한다. 이러한 계정들은 외부의 공격자에 의해서 불법 활용이 되더라도, 개인 사용자가 쉽게 공격 여부를 확인할 수 없기 때문에, 공격자들의 주요 대상이 된다. 따라서 오랫동안 사용되지 않던 계정이 로그인 시도 되거나, 일정 이상의 빈도로 로그인 시도 실패가 발생하면, 개인 확인 작업을 추가로 시행하도록 해야 한다.
- **의심스런 사외 서비스 회피**: 사외 서비스 연동시에 보안 안전성 여부를 신중하게 고려해야한다. 신뢰하는 벤더사에서 제공하는 서비스를 선택하고, SNS의 기능 확장을 위해서 의심스러운 서비스 연동을 자제해야한다. 불가피하게 의심스런 서비스와 연동시킨다면, 공유되는 정보의 수준을 최소한으로 제한해야 하며, 지속적인 감시 시스템을 구축해야 한다.

또한, SNS 플랫폼 관리자는 주기적인 바이러스 백신 검사를 수행해야 하며, 백신과 웹서버 업데이트를 정기적으로 수행해야 한다. 이러한 노력에도 불구하고, SNS 사용자들에 의해서 개인 정보가 유출될 수 있다. 따라서 SNS 사용자에게 위험성을 인식 시키고, 보안 교육을 지속적으로 강화시켜야 한다.

## 5. 결　　론

최근 SNS가 기업의 조직 강화 수단으로 진화하고 있다. 많은 기업들이 고객 커뮤니티 채널로 사용하던 SNS를 최고 경영자와 일반 직원들간에 소통하는 수평적인 아이디어 공유방법으로 활용하기 시작 했다.

그러나 스마트폰과 같은 모바일 단말의 지원은 기업 내 네트워크 환경에 보안 취약성을 불러오기 때문에 SNS 보급의 장애가 되고 있는게 현실이다. 이 논문에서는 모바일 단말의 지원으로 야기될 수 있는 보안 취약성에 대한 대응방안을 제시하였으나, 궁극적으로 내부 사용자들의 보안에 대한 인식 전환이 가장 중요하다.

## [참 고 문 헌]

[1] Nimetz, Jody, “Jody Nimetz on Emerging Trends in B2B Social Networking”, Marketing Jive, November 18, 2007.
[2] Tynan, Dan, “As Applications Blossom, Facebook Is Open for Business”, July 30, 2007.
[3] 강희종, “SNS 기업조직강화 창구 진화”, Digitaltime, 2011.2.27,http://www.dt.co.kr/contents.html?article_no=2011022802010151780001
[4] Jon Phillips, “statusnet revolutionizes Motorola’s Internal communications”, http://status.net/2010/07/08/statusnet-revolutionizes-motorolas-internal-communications
[5] Mindi McDowell, Damon Morda, “Socializing Securely: using social networking services”, 2011 Carnegie Mellon University. Produced for US-CERT ,http://www.us-cert.gov/reading_room/safe_social_networking.pdf
[6] Staff writer, “Hacker Exposes Private Twitter Documents”, July 15, 2009. http://bits.blogs.nytimes.com/2009/07/15/hacker-exposes-private-twitter-documents/?hpw
[7] StatusNet’s main web page, http://status.net/wiki/Main_Page
[8] Twitter’s main web page, http://twitter.com/
[9] Yammer’s about web page, https://www.yammer.com/about/product