특집 03

그린IT 구현을 위한 정보보호

목 차

이응용 · 지순정 · 김성훈 · 이재일
(한국인터넷진흥원)

1. 서 론

에너지 사용의 증가에 따른 자원 고갈 및 탄소 배출량 등 환경문제에 대한 관심이 고조되고 있다. IT 분야는 친환경 산업으로 간주되어 왔으나, 전자제품 사용량 증가에 따른 에너지 소비 증대, 폐기물 증가, 유해물질 배출 증가 등 환경 파괴적인 성격이 부각되면서 IT 산업도 공해를 유발하는 산업으로 인식이 바뀌고 있다. 최근 국제적으로 친환경 IT를 구축하기 위한 노력의 일환으로 그린IT에 대한 정책을 추진하고 있으며, 정부, 민간, 연구소 등 관계기관과의 협력을 통해 적극적인 대처방안을 마련하고 있다.

2008년 Gartner사가 선정한 10대 전략기술에 그린IT가 포함되면서 그린IT에 대한 관심이 더욱 증대되고 있다. 가트너 보고서에 따르면 IT 부문의 탄소배출량은 전 세계 배출량의 2%를 차지하며 이는 전세계 항공기 배출량과 비슷하다고 지적하고 있다. 그린IT의 대표적인 인프라로 스마트 그리드에 대한 관심과 투자가 증대하고 있다. 인터넷을 활용한 스마트 그리드는 최적의 에너지 생산, 유통을 가능케 하면서 에너지 사용을 최적화할 것으로 기대된다. 한편 IT 자원 활용의 최적화를 위한 클라우드 서비스에 연구와 투자가 크게 증가하고 있다. 클라우드 서비스는 IT 자원을 필요한 시점에 필요한 양만큼 사용하게 하여 시스템의 에너지 소모를 크게 감소시킬 것으로 기대된다.

그러나 그린IT의 대표적인 서비스인 스마트 그리드, 클라우드 서비스의 활용에는 정보보호의 확보가 가장 필수적인 요소로 대두되고 있다. 기업 및 기관에서 클라우드 서비스 도입시 가장 우려하는 부분으로 정보보호를 지적하고 있으며, 이에 따라 클라우드 서비스의 신뢰성 확보를 위해 정보보호에 대한 관심과 투자가 증가하는 추세이다. 또한 IT 제품 및 시스템의 일부분인 정보보호 제품도 전력을 소모하기 때문에 전체 IT 제품 및 시스템의 에너지 효율성을 극대화하기 위해 저전력, 고효율 정보보호 제품에 대한 연구도 진행되고 있다.

2. 그린IT 개요 및 동향

그린IT는 컴퓨팅 자원의 에너지 효율성을 극대화하고, 폐기물의 재활용을 통한 환경문제 해

결을 주요 목적으로 한다. 그린IT에 대한 개념적인 출발은 1991년에 환경보호기구인 EPA[1]가 에너지 효율적인 전열사용을 목적으로 'Green Light' 프로그램을 소개하면서 시작되었다[1]. 이후 1992년에는 컴퓨터와 모니터의 에너지 효율적인 기능명세서를 개발하는 에너지 스타(Energy Star) 프로그램이 시작되었다. 그러나 그린IT가 본격적인 관심을 받게 된 것은 10여년 전부터이다. 인터넷 기반의 비즈니스인 클라우드 서비스 활용이 급속히 증가하고 IDC 등 IT 인프라를 운용하는 비용이 증가하면서 그린IT에 대한 관심을 촉발시킨 요인이 되었다. IDC 활용이 증가하면서 IDC 부문의 에너지 사용도 비례하여 증가하고 있다. IDC는 PC 등을 사용하기 위한 전력을 사용할 뿐만 아니라 공기청정기 등 관련 장비 사용에 따른 전력소모가 매우 많기 때문에 국가 전체적으로 IDC의 전력소모는 빠르게 증가하고 있는 상황이다. 미국의 경우 데이터센터의 전력 사용에 따른 비용이 2000년에 비해 2006년에는 2배 증가하고, 9개월만에 전력비용은 2.75배로 증가한 것으로 조사되었다[2]. 이에 따라 AMD, Cisco Systems, Dell, Intel 등 주요 IT 벤더는 저소비 전력 서버 도입이나 자사의 데이터센터의 전력소비 감축을 적극 추진하고 있다. 또한 IBM의 경우, 전력 효율이 높은 데이터센터 구축을 목표로 'Project Big Green' 사업을 추진하고 있다.

대다수 기업의 IT 책임자들이 효율적인 비용절감 효과를 위해 그린IT에 관심을 두고 있다. 그러나 그린IT를 통해 친환경 문제 해결 및 비용절감을 촉진할 것으로 기대하고 있지만 아직까지 구체적으로 실현되지는 못하고 있는 상황이다. 최근에는 OECD, APEC 등 국제기구에서도 지구온난화, 환경오염 등 환경문제 해결을 위한 IT 활용방안에 대한 논의가 활발하다.

Forrester 리서치에 따르면, 전세계 그린IT 시장은 경기침체에도 불구하고 지속적으로 증가하여 '08년 5억 달러에서 수준에서 '13년에는 48억 달러로 급성장할 것이라고 전망하고 있다. 이에 따라 EU, 일본 등 선진 각국은 정보차원에서 IT를 성장동력으로 인식하고, 국가의 지속적인 경쟁력을 확보하기 위해 그린IT 전략을 적극 추진하고 있다.

우리나라에서도 녹색성장을 위해 그린IT 정책을 정부차원에서 적극 추진하고 있다. 우리나라는 세계 최고 수준의 정보통신인프라, 높은 교육수준으로 인해 국민들의 IT 활용능력이 우수하여 그린IT를 조기에 실현하기 위한 좋은 인프라를 지니고 있다. 정부가 "저탄소 녹색성장" 비전을 선포하고, 녹색성장위원회의 그린IT 국가 전략 방향에 따라 방송통신위원회, 행정안전부, 지식경제부 등 IT 관련 부서를 중심으로 그린IT 구현을 위한 관련 조직을 신설하고 세부사항을 마련 중이다. 특히 방송통신위원회는 지난 3월에 그린방송통신서비스 종합계획, 지식경제부는 1월에 그린IT 전략, 행안부는 1월에 녹색정보화 계획을 수립하여 추진하고 있다.

2.1 IT 제품 · 시스템의 그린화

그린IT 실현을 위해 IT 제품, 시스템, 서비스 등 전분야에 걸친 그린화 물결이 일고 있다. 저전력 · 고효율 IT 제품 및 시스템의 이용은 소비전력을 크게 감소시킬 수 있다. 또한 PC, 모니터, TV 등에 저전력 고효율 기술을 본격적으로 적용하면 에너지 효율을 높일 수 있다. IT 제품의 제조공정에서 발생하는 탄소 배출량은 25%에 불과한 반면 75%는 실제 사용 중에 발생하기 때문에 IT 제품 이용과 관련된 서비스 단계에서의 그린화에 대한 체계적인 연구가 진행될 필요가 있다.

2.2 녹색성장을 위한 IT 활용

녹색성장을 위해 IT 활용을 극대화하려는 노

1) Environmental Protection Agency

력도 함께 진행되고 있다. IT 산업과 타산업과의 융합을 통해 에너지 효율화, 교통·물류·전력망 등 SOC 지능화, 일하는 방식 선진화, 생활양식 녹색화가 가속화될 수 있다. 전력시스템과 인터넷을 융합한 스마트 그리드의 경우, 전력정보가 쌍방향으로 유통하여 전력 이용효율을 극대화하여 녹색성장 사회로의 전환을 촉진할 수 있다.

3. 그린IT의 위험요인

IT활용은 녹색성장에 크게 기여하는 한편, 보안에 대한 충분한 사전적 고려가 없으면, 사회시스템과 연계된 그린IT 서비스에서 사이버위협이 크게 증가하고, 이로 인한 사후적인 경제적인 비용이 크게 증가할 것으로 예상된다. 스마트 그리드의 경우, 해커가 스마트 미터를 통해 웜을 전파하여 스마트 그리드에 대한 통제권을 확보하여 시스템을 중단시키고, 대규모 정전사태를 유발할 수 있다. 또한 해커는 일부지역에서 전력 수요를 급작스럽게 증가 또는 감소시킴으로서 특정 지역의 전력 수급에 심각한 차질을 초래하여 정전상태를 유발할 수 있으며, 특정 지역의 급작스런 전력 수급 불균형은 타지역으로 확산되어 연쇄적으로 대규모의 정전사태를 유발할 수 있다. 서비스제공업체는 다양한 가전제품의 소비 전력을 제어하고, 전력이용 데이터를 수집할 수 있어 개인정보 유출 위험이 있다. 이와 같이 보안에 대한 충분한 고려가 없이 그린IT를 추진하는 경우에 향후 소비자들의 강력한 거부에 직면하여 구축된 시스템이 철거될 가능성도 있다.

클라우드 서비스의 활성화에 있어서도 보안문제 해결이 필수적이다. 클라우드 서비스는 데이터 용량 증가와 기기들의 다양화 등으로 인해 효율적 자원 관리의 중요성이 제기되면서 출현하였다. IDC의 자료에 따르면, 2010년까지 생성·저장될 디지털콘텐츠의 양이 988exa bytes (1zetta = 1000exa = 1012 giga bytes)까지 증가할 것으로 예상된다. 클라우드 서비스는 인프라 집중화를 통한 비용절감, 최대 용량 증가, 시스템 효율성 향상 등 그린IT를 위한 핵심서비스가 될 전망이다. 클라우드 서비스의 이용 증가와 함께 보안 문제가 최대 이슈로 부상하고 있다. 클라우스 서비스 제공 업체가 악의적인 공격을 받거나 장애 발생 시, 서비스가 중단되면 어떠한 작업도 불가능하게 되므로 큰 혼란 발생이 가능하다. 일례로 2008년 6월, 구글 「클라우드 컴퓨팅」의 핵심 기능을 맡고 있는 '구글 맵 엔진'이 장애를 일으켜 서비스기능 정지 상태가 발생하였다. DDoS와 같이 대량의 트래픽을 유발시켜 서버를 다운시키는 공격을 받는 경우 더욱 심각한 피해를 유발할 수도 있다. 지난해 2월, 인증서버 과부하로 인해 아마존의 S3서비스가 3시간이상 중단되어 사용자가 큰 불편을 겪는 사고가 발생하였다.

4. 그린IT 실현을 위한 정보보호

정보보호는 그린IT 실현을 위한 핵심적인 역할을 수행한다. 정보보호는 IT 제품 및 시스템의 그린화 측면에서 중요하다. 침해사고 예방 및 대응을 통해 침해사고로 인한 전력소모를 감소시킬 수 있고, IT 제품에 필수적인 암호 및 보안제품의 저전력, 고효율화를 통해 시스템 전체의 그린화를 향상시킬 수 있다. 또한 정보보호는 그린 IT 서비스의 이용활성화를 통해 그린IT 실현에 기여할 수 있다. 정보보호는 클라우드 서비스, 스마트 그리드 등 그린IT서비스의 안전성 및 신뢰성을 개선시켜 이용자의 보안 우려를 해소하여 서비스를 빠르게 수용하게 한다.

4.1 정보보호 제품·시스템의 그린화

4.1.1 인터넷침해대응시스템의 그린화

인터넷에서 발생하는 침해사고로 인한 환경문제 즉, 탄소배출량을 최소화하기 위하여 인터넷

침해대응 시스템 및 장비 등의 그린화 추진이 요구된다. 인터넷 침해사고와 환경문제는 밀접한 관계가 있다. 호스트가 악성코드에 감염되면 CPU, 메모리, HDD 등의 장치에서 전력 소모가 증가한다. 일일 호스트 1대당 일일 평균 약 25% [2]의 전기소모가 증가한다. CPU의 전력을 소모시키는 주요 악성코드로는 Worm.Win32.Sasser, Win-Trojan/Downloader.40960.B, Win-Trojan/ DDoS_Boxed.27206, Trojan.Neokey, Win-Trojan/Kineo. 180224 등 다양하다. 또한 네트워크 트래픽을 유발하는 악성코드로는 Worm.Win32.Conficker, Trojan.Win32. DDos-Agent 등 다양하다. 이러한 악성코드를 제거하면 불필요한 CPU 사용을 최소화하여 에너지 저감 효과를 거둘 수 있다.

분산서비스거부(DDoS) 공격이 발생할 경우, 피해사이트는 대량의 공격 패킷을 처리하기 위하여 메모리, CPU 등의 사용이 증가하게 되어 전력소비 및 탄소배출량을 증가시킨다. 홈페이지에 악성코드가 은닉되어 있는 경우, 접속자는 불필요한 인터넷 접속트래픽을 유발하고, 악성코드에 감염된 PC는 불필요한 자원 사용으로 전력사용이 증가한다. 악성코드 감염 PC의 경우, 평균 25%의 전력사용이 증가하는 것으로 추정된다.

네트워크 침해사고의 신속한 대응을 통해 네트워크의 그린화를 향상시킬 수 있다. 침해사고 발생시 피해사이트 조사, 로그수집, 악성코드 분석, 악성코드 유출 경로 차단, 공격근원지 조사 및 해커조정지 차단 등 일련의 프로세스를 신속히 수행하여 네트워크, 이용자 PC, 서버 등의 부하를 최소화할 수 있다. 웹서버에 숨겨진 악성코드를 이용자들이 접속하기 전에 사전에 탐지하여 조치함으로써 접속트래픽 및 악성코드 감염으로 인한 자원소비 절감 효과를 기대할 수 있다.

4.1.2 위협관리시스템의 그린화(UTM)

정보보호 제품의 그린화와 관련하여 UTM (Unified Threat Management, 통합위협관리) 활용이 부각되고 있다. UTM은 방화벽, IPS/IDS, VPN 기능을 기본적으로 갖추고, 안티바이러스, 안티 스팸 기능이 탑재된 제품을 지칭한다. 통합위협관리시스템은 다양한 위협관리 기능을 통합된 제품으로 구현하여 다차원적인 보안기능을 제공한다. 단일의 UTM 시스템은 5~6개의 보안기능 또는 서버 기능을 대체하여 전력 소모를 크게 감소시킬 수 있다. 또한 다양한 보안제품을 사용할 때 필요한 공기 청정기능 등에 소모되는 전력도 크게 감소시킨다. 가상화 기술을 활용한 통합위협관리시스템은 그린화의 효과를 향상시킬 수 있다. 침해탐지기능, 침해차단기능, 안티스팸기능, 콘텐츠 필터링 등의 보안기능을 통합하여 강력한 보안기능을 제공하면서도 사용자에게는 효율적인 환경을 제공한다. 물리적으로 하나의 시스템으로 동작하지만, 사용자에게는 여러 개의 보안 서버 기능을 제공하여 단일 시스템 운영으로 인한 비용 절감 효과 및 관리 효율을 얻을 수 있다. 향후 하드웨어 플랫폼의 변경없이 기능 개선이나 업그레이드가 가능할 것이며, 통합보안제품의 지속적인 개선을 통해 보안에 사용되는 전력 사용을 감소시킬 것으로 전망된다.

4.1.3 암호기술 적용 제품의 그린화

SEED, RSA 등 기존 암호기술은 암호 연산과정에서 많은 양의 전력이 소모됨에 따라 탄소배출량을 최소화하기 위해 저전력의 경량 암호기

2) ITA 주간기술동향 1344호 2008. 4. 30 "PC 전력이 새고 있다." : 펜티엄4 기준으로 부하시험 시 소비전력(160W)과 최대소비전력(191W)의 평균값인 175W를 악성코드 소비전력으로 산정, 따라서, 평균소비전력(140W) 기준으로 25%(35W) 전기소모가 증가

술 개발 및 적용이 필요하다. 최근 경량 암호 프로토콜이 설계에 대한 다양한 접근법이 제안되고 있으며, 센서 노드를 위한 저전력의 키관리 프로토콜 등 다양한 암호알고리즘에 대한 연구가 진행되고 있다[3].

암호기술은 대부분의 정보보호 제품 및 서비스에서 활용되고 있으나, 암호기술은 수학적 연산 과정이 많아 전력 소비량이 높다. 특히, 암호기술을 최적화되지 않은 상태로 구현하는 경우 부가적으로 전력 소비가 증가할 수 있다. 그린IT에 대한 접근방법으로 암호기술의 경량화·최적화를 통해 탄소 배출량 감소를 유도할 수 있다. 즉, 기존 암호기술을 대체할 뿐만 아니라 RFID 등 저전력을 요구하는 환경에 적용 가능한 저전력·경량 암호기술을 개발하고, 최적화된 방법으로 구현·적용함으로써 탄소 배출량을 최소화할 수 있다. 암호기술의 경량화·최적화를 통해 그린IT 기반 구축을 최적화할 수 있다. 최근 무선센서네트워크 보안에 대한 관심이 증가하고 있다. 무선네트워크는 내부적인 보안취약성으로 인해 네트워크 공격을 받기 쉬우며, 무선 통신에서 사용되는 전파는 벽, 창문 등을 통과하기 때문에서 무선네트워크의 경계가 모호하고, 이로 인해 유선네트워크에 비해 도청, 데이터 수정 등 보안위협에 취약하다[4]. 무선센서네트워크 등에 적합한 경량 암호기술 적용 시, 기존 암호기술 대비 전력 절감 효과를 기대할 수 있다[4].

저전력의 경량 암호기술은 신규 IT서비스에서의 에너지 절감효과도 기대할 수 있다. 인터넷전화(VoIP)서비스는 멀티미디어 등의 데이터 전송이 가능하여 기존 전화 서비스에 비해 최소 50배 이상의 데이터를 전송할 수 있기 때문에 경량 암호기술의 적용에 따른 효과가 크게 증가할 수 있다. 암호기술은 RFID/USN 관련 다양한 서비스의 통신보안, 보급된 PC의 인증관리, 시스템·네트워크 제품의 기본적인 보안 관리를 위한 활용이 증가하고 있고, 이로 인해 저전력 암호기술의 사용으로 인한 에너지 절감효과가 지속적으로 증가할 것으로 예상된다.

4.2 그린IT 서비스의 이용활성화 기여

4.2.1 스마트 그리드 안전성 제고를 통한 조기 도입 유도

우리 정부는 녹색성장 동력으로 스마트 그리드를 지정하고, 2012년까지 한전 전력망에 IT를 도입하여 양방향 전력시스템을 구축할 계획이다. 한국을 비롯한 세계의 에너지 소비량은 꾸준히 증가할 것으로 예상되며, 스마트 그리드 구축을 통한 에너지의 효율적인 소비가 절실한 상황이다. 스마트 그리드는 전기사용 행태 및 전기요금을 실시간으로 보여주어 소비자의 자발적인 에너지 절약을 유도한다. 지구 온난화 방지를 위한 교토의정서가 발효됨에 따라 CO2 의무감축 대응과 녹색 성장을 위한 대체 에너지 확대 차원의 스마트 그리드 구축이 세계적인 추세이다. 미국 전력연구원은 스마트 그리드의 활용으로 '30년까지 미국 전역 전력 소모량의 4.3%인 2천억 KW/h의 전력량이 감소할 것으로 예상하였다.

전력과 통신이 융합된 스마트 그리드는 여러 가지 효율성과 함께 새로운 보안위협이 존재한다. 그러나 스마트 그리드의 성공적인 구축을 위해 정보보호가 선결조건이다. 스마트 미터의 보안이 완전하지 않다면, 전기의 공급을 방해하는 해킹을 당할 수 있고, 스마트 그리드 전체 시스템이 불안전할 수 있다. 전문가들은 보안취약성이 해결되기 전에 스마트 그리드가 확산될 경우, 종국에는 대량교체 사태가 발생할 수 있다고 경고하고 있다. 미국 국제전략연구소(CSIS)의 국장 제임스 루이스는 사이버보안의 개선이 선행되어야만, 스마트 그리드 관련 정부계획이 순조롭게 진행될 수 있음을 피력하였다.

이미 지속적으로 제기되어 온 전력인프라 보안 기술의 허점과 수많은 스마트 그리드 관련 침해사고 사례들이 발생하고 있으며, 사이버보안 전문가들은 몇몇 계량기들을 비롯하여 스마트

그리드 통신 시스템의 해킹 가능성을 경고하고 있다. 지난 3월, 미국 보안컨설팅업체 IOActive의 실험 결과 해커들이 간단한 해킹 기술로 네트워크에 접속하여 전기 공급을 중단할 수 있음이 증명되었다. 전기와 소프트웨어에 관한 약간의 지식과 500달러짜리 장비만 있으면 스마트 그리드 시스템에 침입이 가능하며, 한 개의 장비를 해킹하면 다른 시스템 전체의 조종이 가능하였다. 또한 Black Hat 2009에서 스마트 미터의 취약점을 이용한 웜 감염 및 전파 시연 결과, 웜에 감염된 스마트 미터의 모든 기능을 해커가 통제할 수 있었으며 대규모 정전 등을 통한 사이버 무기화 가능성이 확인되었다. 스마트 그리드는 고객의 프라이버시 침해를 유발할 수 있으며[5], 스마트 미터에 저장된 에너지 사용 정보는 고객의 습관과 행위에 대한 정보를 노출시킬 수 있다. 텔레비전 시청과 같은 특정한 행위는 전력소비에 대한 행위 분석에 활용될 수 있고, 이러한 스마트 그리드 관련 개인의 이력정보가 타인에게 오남용 될 경우 개인의 프라이버시가 크게 침해될 수 있다[6].

주요국에서는 스마트 그리드의 보안 기술 및 정책 개발을 핵심 요소로 인식하고, 이에 대한 기술과 정책 개발에 힘쓰고 있다. 미국은 전력에 대한 보안 위협 대처 방안으로 연방에너지규제위원회(FERC)에 전력인프라에서의 사이버보안이 긴급히 요구될 경우 긴급 규칙·명령 권한, 국토안전부(DHS)에 연방의 주요 전력 인프라에 대한 외부의 침입 여부의 조사 권한을 부여하는 "주요전력시설보호법(Critical Electric Infrastructure Protection Act)' 초안을 제정하였다. EU 역시 "European Technology Platform Smart Grids'를 설립하여 스마트 그리드의 비전과 연구개발 전략을 수립, 총 5개 부문의 19개 세부과제를 선정하고, 스마트 그리드의 장애 및 외부 공격 대응방안, 송배전 시스템의 사이버 보안 및 복구 능력 향상을 위한 방법론 등을 연구하였다. 한국은 제주 스마트 그리드 실증단지에 해킹 방지 솔루션을 채택, 전력망의 제어용과 실증용 통신망간 분리 운용, 모의 사이버 대응 훈련 등 보안강화 대책을 함께 마련할 계획이다.

현재 세계적 화두인 저탄소 녹색성장을 위한 대표 기술인 스마트 그리드 도시 구축 시 IT에 대한 도입, 설계, 구축, 운영 단계별 보안체계 구축은 선택이 아닌 필수이다. 스마트 그리드 구축과 관련된 모든 기술, 연구, 정책들에 사이버 보안에 대한 구체적 방안들이 제시되어야 함은 물론 민관 모두에게 끊임없는 기술·제도적 대책 강화가 필요하다. 스마트 그리드의 보안을 위해서는 암호화, 접근제어와 같은 다양한 보안 서비스가 제공되어야 할 것이다. 전력 계통을 구성하는 발전, 송전, 배전, 시장 영역별 보안 제어 방안을 마련하고, 보안 및 관련 표준의 개발이 요구된다. 국제적으로 통용될 수 있는 스마트 그리드 보안 표준을 마련하고, 전력망에 대한 단계별 보안위협 대처방안을 마련하여 스마트 그리드의 안전한 이용을 확산할 필요가 있다. 새로운 보안문제들이 등장할 가능성도 있게 때문에, 기존 보안기술을 고도화하고, 스마트 그리드에 적합한 보안 기술의 연구·개발이 지속적으로 필요하다.

4.2.2 클라우드 서비스 신뢰성 향상을 통한 이용 활성화

최근 데이터 용량의 증가와 기기의 다양화 등으로 효율적인 IT 자원 관리의 중요성이 제기되면서 클라우드 서비스가 신 IT 트렌드로 대두되고 있다. IT자산의 양적인 증대로 인해 데이터와 소프트웨어 등의 효율적 관리가 필요하게 되었으며, 상호연동 가능한 디바이스의 증가와 이를 활용할 수 있는 다양한 서비스의 등장에 따라 자원 관리의 중요성이 증가되고 있다.

효율적 IT 자원관리, 비용 감소 등 다양한 장점이 부각되면서 클라우드 서비스 시장은 지속

적으로 증가하는 추세이다. IDC는 '12년에 전세계 클라우드 서비스 규모가 42조 달러에 도달할 것으로 예상하였으며, 클라우드 서비스는 27%의 높은 성장률을 기록할 것으로 전망하였다. 가상화 기술을 도입한 클라우드 서비스는 서버 효율을 증대시켜서 에너지 절감 및 서버 도입·관리비용을 절감할 수 있다.

녹색 성장 구현에 기여하는 클라우드 서비스의 활성화를 위해서는 보안성 확보, 기존시스템과의 통합, 가용성 확보, 성능개선 등이 필요하며, 특히 보안이슈 해결이 선제적으로 필요하다. 2008년 8월, 미국 CIO Research가 IT및 비즈니스 분야 리더 173명을 대상으로 클라우드 서비스에 관한 설문조사를 실시한 결과, 자사에 클라우드 서비스를 도입할 때 가장 우려가 되는 부분에 대한 질문에 45%의 응답자가 보안문제라고 대답하였다. 데이터 통제권에 상실에 관한 우려 또한 26%로 매우 높게 나타났다.

클라우드 서비스의 신뢰성 향상을 통해 이용자의 우려를 불식시키고 보안사고 피해를 최소화하기 위한 서비스 전단계의 보안대책을 강화가 필수적이다. 클라우드 서비스의 전단계의 보안대책 강화를 통해 이용자의 우려를 불식시켜야 한다. 정보 소유자는 본인 이외의 타인이 해당 정보 접근을 제한할 필요가 있다. 또한 정보통제권 및 보안책임이 사용자에서 서비스 제공업체로 이관됨에 따른 다차원적인 안전장치가 구축되어야 한다. 아울러 클라우드 서비스는 그간의 IT 환경에 새로운 패러다임을 제시하는 신기술로 그간의 개인정보보호법 혹은 정보통신 관련 법률의 개정 및 보완이 필요하다. 각종 규제와 정책의 수립과 함께 사용자, 공급자의 적극적 협조를 유도하여 안전한 이용 환경을 조성해야 할 것이다.

5. 결 론

정부, 기업 등에서 그린IT의 실현을 위해 기술 및 서비스 개발, 제도 정비, 인식제고 등을 추진하면서 그린IT 서비스의 보안 및 프라이버시에 대한 국민의 우려를 불식시키고, 서비스의 수용도를 제고하기 위해서는 그린IT 관련 정보보호에 대한 사전적 고려가 필수적으로 요구된다.

정보보호는 에너지 및 자원 소모, 환경부하 측면에서 녹색성장에 중추적인 역할을 수행할 수 있다. 직접적 효과로는 악성봇 제거, 저전력 암호이용 등은 CPU, 메모리, 스토리지 자원의 불필요한 전력소모를 최소화하고, 저전력·초소형 암호기술 활용은 IT제품의 에너지 사용 및 탄소배출량을 저감시킬 수 있다. 또한 다양한 기능을 수행하는 통합보안관리(UTM) 제품의 활성화를 통해 정보자원의 전력소모를 최소화할 수 있다. DDoS 등 공격 등 인터넷 전반을 마비시킬 수 있는 사이버공격을 탐지하여 사전 예방하고, 위험 수준에 따라 기업·기관 정보를 백업하여 사이버공격 및 재난으로부터 대규모 자원 손실을 방지할 수 있다.

간접적 효과로는 클라우드 서비스, 스마트 그리드 등 녹색성장의 핵심적인 그린IT 서비스의 이용 활성화에 크게 기여할 수 있다. 클라우드 서비스에서는 고객정보를 보호하고, 자산의 안전성을 확보할 수 있고, 스마트 그리드에서는 자동화된 위험 탐지 및 대응, 탄력적인 공격 및 재해 대응 등 스마트 그리드의 안전성 확보에 기여하여 서비스의 활성화에 기여할 수 있다. 녹색성장에 기여하는 원격화상회의, u-Work 등 다양한 IT서비스의 이용 활성화를 위해서도 정보보호는 사전에 해결해야 할 중요한 과제이다.

참고문헌

[1] Robert R. Harmon1, Nora Auseklis2,Sustainable IT Services: Assessing the Impact of Green Computing Practices, PICMET, 2009

[2] David Wang, Meeting Green Computing Challenges, HDP, 2007

[3] Nachiketh R. Potlapally, Srivaths Ravi, Anand Raghunathan, Niraj K. Jha, Analyzing the Energy Consumption of Security Protocols, ACM, 2003

[4] Phongsak Kiratiwintakorn, ENERGY EFFICIENT SECURITY FRAMEWORK FOR WIRELESS LOCAL,University of Pittsburgh, 2005

[5] Arvinderpal S. Wander, Nils Gura, Hans Eberle, Vipul Gupta, Sheueling Chang Shantz, Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks, IEEE, 2005

[6] Patrick McDaniel, Nils Gura, Sean W. Smith, Security and Privacy Challenges in the Smart Grid, IEEE, 2009

저자약력

이 응 용

1996년 KAIST 전산학과 학사
2003년 KAIST 경영정보학(MIS-MBA) 석사
현재 한국인터넷진흥원(KISA) 정책기획단 정책연구팀 수석연구원
관심분야 : 유비쿼터스, 인터넷 및 정보보호
이 메 일 : eylee@kisa.or.kr

지 순 정

2005년 숙명여대 경제학과 학사
2008년 숙명여대 경제학과 석사
현재 한국인터넷진흥원(KISA) 정책기획단 정책연구팀 연구원
관심분야 : 인터넷 및 정보보호 정책, 스마트 그리드
이 메 일 : sjji@kisa.or.kr

김 성 훈

1990년 연세대학교 컴퓨터과학과 학사
1992년 연세대학교 컴퓨터과학과 석사
2008년 중앙대학교 컴퓨터공학과 박사
현재 한국인터넷진흥원(KISA) 정책연구팀장
관심분야 : 컴퓨터통신, 센서네트워크, 정보보호
이 메 일 : kimsh@kisa.or.kr

이 재 일

1986년 서울대학교 계산통계학과 (이학학사)
1988년 서울대학교 계산통계학과 석사 (전공 : 전산학)
2006년 연세대학교 컴퓨터공학과 박사 (전공 : 정보보호)
현재 한국인터넷진흥원(KISA) 정책기획단장
관심분야 : 인터넷, 정보보호
이 메 일 : jilee@kisa.or.kr