특집 02

신규 IT 서비스 도입 확산을 위한 정보보호

목 차

유지영 · 이재일
(한국인터넷진흥원)

1. 서 론

최근 들어 IT 자원의 효율적 운용을 통한 경제성 제고 및 일자리 창출 등이 기업과 국가 경쟁력 창출에 있어 핵심동력으로 부상하면서 클라우드 서비스, 스마트 그리드 등 인터넷을 기반으로 한 신규 IT 서비스 산업에 대한 관심이 증대되고 있다.

인터넷을 활용한 스마트 그리드의 경우 최적의 에너지 생산과 유통을 가능케 하면서 에너지 사용을 절감시킬 수 있으며, 클라우드 서비스 또한 IT 자원을 필요한 시점에 필요한 양만큼 사용하게 함으로써 시스템 에너지 소모를 크게 감소시킬 것으로 기대되어 녹색환경 구현을 위한 최적의 IT기술들로 각광 받고 있는 것이다.

그러나 이러한 신규 IT서비스는 안정적인 도입 및 활성화의 필요성과 더불어 추진 동력을 저해하는 요소로서 정보보안에 대한 우려가 제기되고 있다. 해커에 의한 시스템 공격, 기기간 통신 방해, 개인정보 유출 등 서비스 도입 시 예상되는 사이버 위협과 관련 법 · 제도 미비에 따른 사회적 신뢰기반 취약 등이 서비스의 도입을 늦추게 하는 요인으로 작용하고 있는 것이다. 이러한 이유로 기업 및 관계기관에서는 신규 IT 서비스 도입에 대해 우려의 목소리가 높은 것이 현실이다.

보안업체인 트렌드 마이크로(Trend Micro)社는 2010년 예측 보고서를 통해 다양해진 인터넷 연결 방법으로 인한 사이버 범죄 증가, 인터넷 보급 증가로 인한 멀웨어 시장 확대, 신기술 등장에 따른 사이버 위협 문제 대두, 클라우드 컴퓨팅 및 가상화 증가에 따른 보안 문제 등 기술 · 사회 변화에 따른 보안위협에 대한 예측과 함께 이를 해결하기 위한 새로운 기술과 방법이 도입되어야하는 필요성에 대해 강조하고 있다.

인터넷이 사회 전분야에 확산되면서 사이버공간이 글로벌 환경에 있어서 중요한 인프라로 인식되고 있는 요즘, 경제 · 사회적 불안을 초래할 수 있는 사이버 공격의 급증은 정보보호에 대한 국제사회의 관심과 인식을 증대시키는 계기가 되고 있으며, 선진 각국은 정보보호 전략 수립, 전담조직 확충 등 사이버 보안 체계 강화에 적극 노력하고 있다.

본고에서는 클라우드 서비스, 스마트 그리드

등 신규 IT 서비스의 개요와 동향 및 보안 위협 등에 대해 살펴보고 도입 확산을 위한 정보보호 대책 마련에 대한 방안을 제시하고자 한다.

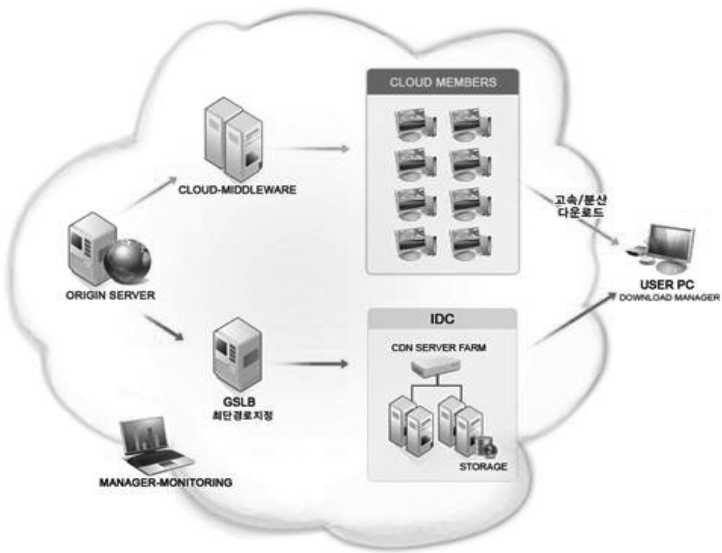
2. 신규 IT 서비스 개요 및 동향

가트너의 '2010년 CIO 아젠다' 및 '2010년 톱 10 전략 기술' 발표에 따르면 클라우드 서비스가 2010년 CIO들이 가장 주목하는 기술 2위, 10대 전략기술 중 1위로 선정되는 등 전 세계적으로 주목을 받고 있다. 우리나라 역시 대용량으로 증가하고 있는 데이터 보관을 위한 시설 증강 및 공간 확보 등으로 인한 IT 비용 절감, 탄소배출량 감소뿐만 아니라 사용의 편리성, 효율성, 투자대비 높은 산업적 파급효과 등을 고려해 클라우드 서비스의 도입이 적극 추진되고 있다.

클라우드 서비스는 모든 실행 프로그램과 하드웨어가 거대한 구름인 클라우드에 네트워크로 연결되어 있고, 사용자는 단순히 네트워크 접속만 가능한 단말기를 통해서 각 프로그램을 불러들이기만 하면 된다. 작업의 내용은 웹에 저장되며 어떤 장소에서 원하는 시점에 자신이 가지고 있는 단말기에서 접속해 볼 수 있다. 이 과정에서 정보를 실행하기 위한 고사양의 개인용 단말기는 필요가 없으며, 네트워크에 접속할 수 있는 최소한의 기능만 있으면 클라우드 안의 컴퓨터들이 대신 기능을 처리하여 사용자의 단말기로 결과를 도출하여 전송한다.

우리나라에서는 삼성SDS, LG CNS, KT, SKT, 네이버, 다음, 클루넷, 이노그리드 등 국내 기업들을 중심으로 활발한 도입 움직임을 보이고 있으며, 방송통신위원회, 지식경제부, 행정안전부 등 3개 부처가 공동으로 '클라우드 컴퓨팅 활성화 종합계획'('09.12.30)을 발표해 공공부문 선제 도입, 민간 클라우드 서비스 기반마련, 핵심 클라우드 기술 개발 및 연구, 클라우드 컴퓨팅 서비스 활성화 여건 조성 등 4개 부문에서 10대 세부과제를 도출하여 범정부 차원의 클라우드 컴퓨팅 서비스 산업 활성화를 지원하고 있다.

해외 글로벌 기업들도 초기단계의 클라우드 서비스 시장을 선점하기 위해 발 빠르게 움직이고 있다. Google의 경우 AppEngine를 통해 어플리케이션 개발을 용이하게 하는 플랫폼 서비스



(그림 1) 클라우드 컴퓨팅 서비스 구성도(출처 : 클루넷 홈페이지)

및 개발을 위한 호스팅 공간을 제공하고 있으며, 구글 Earth, 구글 캘린더 등 각종 어플리케이션 서비스를 제공 중에 있다. MS는 전통적인 OS 소프트웨어 부문에서 윈도우 애저(Azure)를 이용한 클라우드 컴퓨팅 환경 개발을 지원하고 있으며, 아마존(Amazon)은 온라인 도서판매 서비스에서 서버 및 스토리지를 제공하는 인프라 및 플랫폼 서비스로 사업을 확대하고 있다. HP는 고객들이 원하는 솔루션을 웹 기반 하에서 온디맨드 방식의 서비스로 제공하는 'Everything as a Service(EaaS)'를 추진하는 등 다양한 서비스 추진과 함께 IT분야별 협업을 통한 글로벌 경쟁력을 확보해 가고 있다.

스마트 그리드는 발전소와 송·배전 시설, 전력 소비자를 정보통신망으로 연결하고 양방향으로 공유하는 정보를 통하여 전력 시스템 전체가 효율적으로 작동하도록 하는 것으로 공급자와 소비자간 실시간 정보 교환을 통해 에너지 효율화에 최적화한 지능형 전력망이다. 미국 뉴욕 타임스 논설위원인 '토마스 프리드먼(Thomas L. Friedman)'은 그의 저서 '코드그린(Code Green)'에서 이산화탄소 배출문제를 최소화할 수 있는 기술이 미래의 성장 동력이 될 것이라고 하며 그 중 하나가 스마트 그리드 기술이라고 주장한 바 있다.

(그림 2) 스마트 그리드 개념도

스마트 그리드 구축을 통해 이용자는 가격신호에 반응해 전기사용 시간을 조절하여 소비를 절약하고, 사업자측은 소비자의 자율 수요 조절로 인해 발전원으로서의 수익이 발생하는 등 경제적 이점이 발생한다. 또한 공급자와 소비자간 실시간 전력정보 교환을 통해 전기 사용 패턴 및 전기 요금 확인으로 에너지 효율을 높일 뿐만 아니라 에너지 수요를 감당하기 위한 발전 설비의 지속적인 확대가 불필요해진다.

이로 인해 스마트 그리드에 대한 국제적인 관심과 함께 차세대 성장 동력으로서 투자가 증가하는 추세이다. 유럽은 물론, 미국, 캐나다, 호주 등 주요 선진국에서도 에너지 관련 법 제·개정, 스마트 그리드 관련 연구 지원, 스마트 미터(지능형 계량기) 보급 등 정부차원에서 적극적으로 주도하고 있다. 우리나라도 스마트 그리드 산업 창출 등 업계 간 협력 틀 마련을 위해 한국스마트그리드협회(KSGA)가 공식 출범하였고 한국형 스마트 그리드 기술을 실제 생활에서 시험하고 평가하기 위한 '지능형 전력망 통합실증단지(Test Bed)' 구축을 제주도에 추진 중이다.

3. 신규 IT 서비스에 대한 보안 위협

3.1 클라우드 서비스 보안 위협

클라우드 서비스는 IT 자원 활용에 있어 최적의 조건들을 겸비한 분야이지만 개인정보 유출 및 사이버 위협 등과 같은 보안성 문제에 대한 해결책 또한 시급한 실정이다. 한국정보화진흥원은 2009년 주요 IT 전략 기술에 따른 보안 이슈로 클라우드 서비스 환경의 보편화로 인한 데이터 손실 우려, 개인화된 서비스 가치로의 중심 이동에 따른 정보 보안 문제, 외부 보안 위협자에 가려졌던 내부자 위협(insider threat) 문제 등을 발표한바 있다. 2009년 2월 발표된 UC Berkeley, IDC 및 가트너 보고서, CSA 등에서도 클라우드 서비스 도입시 야기 될 수 있는 보안 이슈에 대해 문제를 제기하고 있다〈표 1〉.

클라우드 서비스는 이용자의 데이터를 집약하여 저장하고 처리한다는 점에 있어 일부 시스템에 대한 침해사고 발생시 이와 연결된 다른 시스

〈표 1〉 클라우드 서비스 도입시 예상 보안 이슈

구분	UC Berkeley : 10가지 기회요소	Gartner Report : 7가지 위험	Cloud Security Allacne : 14가지 보안 도메인
기술 보안 요소	- 서비스 가용성 - 데이터 잠금 - 데이터 기밀과 감시 - 데이터 전송지원 - 성능 예측의 불확실성 - 확장 가능한 스토리지 - 대규모 분산 시스템에서의 에러 - 빠른 확장성	- 권한있는 사용자에 의한 접근 - 규제에 대한 적법성 - 사용자간 데이터의 구분 문제 - 복구의 모호성	- 기존 보안성, 업무 연속성 및 재난복구 - 데이터 센터 운영 - 사고대응, 홍보 및 자료 - 애플리케이션 보안 - 암호화 및 키 관리 - 인증 정보 및 접근 관리 - 스토리지 - 가상화
비즈니스	- 평판 공유의 문제 - 소프트웨어 라이센싱 문제	- 데이터의 물리적 위치 - 조사에 대한 지원 여부 - 장시간 동안의 생존능력	- 거버넌스 및 기업 위험관리 - 법률 - 전자증거수집 - 규제 준수 및 준수 - 정보라이프사이클 관리 - 이식성 및 상호 운용성

템으로까지 문제가 확산되어 개인정보의 유출에 대한 연쇄적 피해가 발생할 가능성이 높다. 특히 서비스마다 독자적 플랫폼 사용으로 인해 이용자가 서비스 사업자를 변경하려고 해도 호환이 불가능해 서비스社 변경이 불편하며, 서비스사간의 이익을 위한 단합으로 이용기업의 중요 정보가 외부 서비스업체에 넘어갈 수 있어 정보에 대한 통제권·접근권 및 프라이버시 침해 등에 대한 규제가 시급하다 하겠다.

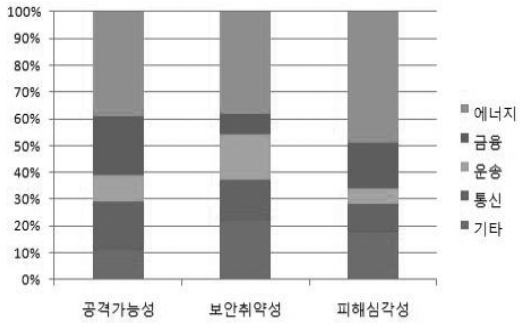
또한 클라우드 서비스는 기존의 SaaS나 유틸리티 컴퓨팅과 달리 B2B 뿐만 아니라 B2C 서비스를 포함하고 있다는 점에서 대량의 개인정보를 취급하게 되므로 개인정보보호에 대하여 외부해킹, 접근통제 미비 등에 의한 대량 유·노출 위협, 서비스 공급자의 폐업으로 인한 데이터의 대량 유실, 국가기관 등에서 범죄수사 등의 목적으로 클라우드 서비스 업체에 정보제공 요청, 데이터의 법적 관할권 문제와 국가간 정보·공유 이전 문제 등 다양한 이슈 제기가 가능하나 이에 대한 구체적인 법적 제도가 미비한게 현실이다.

3.2 스마트그리드 보안 위협

세계 주요 국가에서 많은 관심을 가지고 추진중인 스마트 그리드는 에너지 효율화에 기여할 수 있는 장점이 있는 반면, 수용가와 전력사업자간 IT기반의 양방향 통신기술을 이용함에 따라 불법적인 데이터 위·변조 공격, 해커 등의 고의적 악성 바이러스 유포로 인한 시스템 통제권 상실 및 통제권 상실로 인한 시스템 중단, 대규모 정전사태, 지역 간 전력 수요 불균형 등에 대한 사이버 보안 위협 등의 문제가 존재하고 있다.

보안전문회사인 Secure Computing가 '08년 9월 Annual Cyber Security 컨퍼런스 참석자들을 대상으로 실시한 에너지, 금융 등 5개 산업별 공격가능성, 보안취약성, 피해의 심각성 등에 관한 설문조사 결과에 따르면 에너지산업(전력, 석유, 가스)의 보안이슈가 가장 큰 비중을 차지하고 있어 스마트 그리드에 대한 보안대책 마련이 요구되고 있음을 알 수 있다.

최근 미국 CIA는 스마트 그리드 기술을 적용시킨 시스템이 해커들에 노출될 경우 노출된 시스템과 연결된 다른 시스템으로까지 그 영향이 확산되어 대규모 정전사태가 발생한 사례를 지적하였으며, 전력 제어시스템이 인터넷과 연동될 경우 외부에서 인터넷의 취약성을 이용하여 제어시스템으로 침투할 가능성이 존재한다고 발



(그림 3) 산업별 공격가능성, 보안취약성, 피해심각성 설문조사 〈출처 : Secure Computing, 2008〉

표하였다. 또한 미국의 보안회사 Industrial Defender는 과거 7년 동안 전력 인프라를 중심으로 100번 이상의 위협요소를 평가 한 결과 34,000개의 취약점을 발견했음을 보도하였고, 실제로 '08년 RSA Conference(미국정보보안기술박람회)에서 한 보안전문가는 전력업체 직원이 흔히 사용하는 이메일 서비스를 이용하여 멜웨어(Malware)를 자신의 컴퓨터에 다운로드 하고, 이를 기반으로 발전소 전체를 마비시키는 과정을 상세히 시연하기도 하였다.

이러한 전력 및 통신 기반시설 관련된 보안위협과 함께 소비자들의 상세한 전력 사용 내역이 자동 전송됨에 따라 개인 정보의 유출 가능성도 제기되면서 최근 보안에 대한 우려가 더욱 높아지고 있다. 관련하여 지난 '06년 유럽의회는 회원국에 소비자의 전기요금 통제와 에너지 절약 유도를 목적으로 스마트미터의 도입을 권고하는 지침을 발행하였고, 네덜란드에서는 스마트그리드 설치 의무화를 추진했었으나, 소비자단체에 의해 제기 된 스마트미터(Smart Energy Meter)의 프라이버시 문제에 따라 강제설치 추진을 철회한 사례('09.4)가 있다. 또한 Tilburg 대학 연구원들은 스마트 계량기에 심각한 프라이버시 문제가 있다는 내용의 보고서를 발표하기도 했다.

이렇듯 스마트미터에 의해 체크되는 기록 즉 소비자들의 상세한 전력 사용 내역이 전송되는 시스템 원리로 인해 외출 및 귀가 시간 등과 같은 소비자의 습관에 대한 정보 유출 가능성과 개인의 에너지 사용에 대한 정보가 경찰이나 보험회사 등 제3자에게 유출될 수 있는 위험성 등 국민들의 개인정보보호에 대한 위협 또한 절대 간과할 수 없다.

4. 신규 IT 서비스 도입 확산을 위한 정책 제언

4.1 클라우드 서비스 이용 활성화를 위한 신뢰 기반 조성

보안 대응체계 마련을 전제로 클라우드 서비스의 이용 활성화를 위해서는 서비스 제공자 및 이용자 상호간의 신뢰기반 조성이 우선적으로 요구되며, 이를 위해서는 다음과 같은 대응체계 마련 및 정책추진이 필요하다.

먼저 본격적인 클라우드 서비스 시장의 활성화에 대비하여 예상되는 보안 이슈에 대한 사전 대응체계 연구 및 개발이 요구된다. IDC, 초고속 인터넷 등의 기존 IT서비스의 보안성 심사체계(정보보호 사전진단, 정보보호 제품 인증 등)에 대한 심층 분석 후 클라우드 서비스 특성을 감안하고 기존 IT서비스와 차별화된 보안요소 평가 기준의 정의·수립을 통해 클라우드 서비스 도입에 따른 사전영향평가 체계 수립이 필요하다 하겠다. 또한 클라우드 아키텍쳐 레이어별 보안 취약점 분석을 통한 보안 대응방안 수립이 필요하며, 이를 위해 기존 침해사례 중 클라우드 서비스에 영향을 주는 요소 분석, 클라우드 서비스 모델별(SaaS, PaaS, IaaS 등) 침해사례 조사 및 침해 패턴 분석 등을 통해 클라우드 서비스 아키텍쳐 표준 레이어의 정의를 선행해야 한다. 더불어 각 레이어별 기술적·관리적 측면의 보안 요구기능 도출 및 상세 보안 항목 정의 등을 통해 레이어별 취약점 실증 분석 및 대응방안 수립에 대한 연구가 필요하다. 또한 클라우드 서비스 도입 및 구축시 참조할 수 있는 보안 가이드라인

마련을 통하여 클라우드 서비스 산업의 혁신적인 성장과 기술개발을 효과적으로 지원할 수 있어야 한다.

두번째로는 클라우드 서비스의 사회적 신뢰기반 조성을 위한 사업자의 사회적 책임 강화와 이용자 권익향상을 위한 법·제도 개선 추진이 요구된다. 클라우드 서비스업체에 대한 개인정보 제공 또는 위탁에 대한 통일된 법적근거, 클라우드 서비스 표준 이용약관, 개인정보 유출·유실시 배상방안 등에 대한 법·제도 개선을 통하여 신뢰환경을 조성하되, 규제위주의 시각보다는 적절한 이해관계의 균형을 이루기 위한 규제가 필요하다. 특히 불완전한 서비스 발생시 고객 피해를 최소화하기 위한 사전 조치가 필요하며, 표준서비스수준계약(SLA)의 마련을 통한 고객의 위험과 서비스 업체의 이익 조화가 필요할 것이다. 나아가서는 클라우드 서비스의 개발·제공·이용을 활성화하고 관련 산업을 체계적으로 발전시키기 위한 "클라우드 서비스 육성 기본법"제정 또한 고려해봐야 할 것이다.

마지막으로 컴퓨팅의 발전과 더불어 무단 액세스, 피싱, 멀웨어 및 지적 재산권 도난 행위 등의 '다크 클라우드(Dark Cloud)'가 급속도로 확산되고 있어 기업 및 일반 사용자는 클라우드 서비스 도입을 꺼리게 되며, 이를 해결하기 위해 기업은 인증기능 및 사기 방지 기능을 더욱 강화해하여 이러한 문제점들을 해결하여야 한다. 이를 위해서는 클라우드 서비스의 성능평가기준 등을 포괄하는 종합적인 클라우드 서비스 품질 인증제도 및 사후관리·지원체계 수립과 다양한 클라우드 서비스 환경에서의 호환성 인증제도 마련을 통하여 기업의 서비스 품질 경쟁을 촉진하고 이용자의 서비스 선택권을 강화할 수 있도록 해야 할 것이다.

4.2 안전한 스마트 그리드 이용 신뢰기반 조성

스마트그리드의 안전한 신뢰기반 조성을 위해서 스마트그리드의 활성화 분야와 보안을 동시에 고려해야 하지만 어느 한쪽으로 치우침이 있어서는 안 될 것이다. 따라서 이와 같은 요소를 고려함에 있어 조금 더 신중한 접근이 요구되며 아래와 같은 3가지 우선 항목을 도출하여 정책적으로 제안하고자 한다.

첫째, 스마트그리드는 전력과 통신의 인프라가 서로 다른 영역에서 발전하여 하나로 융합되어 서비스가 제공되는 특징에 따라 현존하는 법·제도 정비의 필요성을 고려해 볼 수 있다. 지식경제부에서 발표한 스마트그리드 로드맵('10.1.25)에 따르면 올해 "지능형전력망 구축 및 지원에 관한 특별법"이 제정되고 더불어 "전기사업법", "정보통신망의 이용촉진 및 정보보호에 관한 법"등의 일부 개정이 필요할 것으로 보인다. 이러한 법의 제·개정에는 보안요소가 필수적으로 고려되어 포함되어야 할 것이다. 특히 스마트미터 등을 통해 개인정보의 수집이 일어날 수밖에 없는 서비스의 특성상 소비자 보호를 위한 조항이 반드시 포함되어 개인정보의 유출 등과 관련된 내용을 명확히 할 필요가 있다. 또한 스마트그리드의 초기 정착 및 활성화를 위해서는 스마트그리드 관련 사업자를 위한 지침 및 가이드라인 등의 개발을 통해 투자대비 효율이 떨어진다는 보안이 가지고 있는 일반적인 인식을 개선하고 스마트그리드가 초기에 정착될 수 있도록 관련 사업자들의 역할을 독려해야 할 것이다.

둘째, 우리나라에서의 스마트그리드는 이제 막 시작하는 초기단계이므로 전문 인력의 양성이 필요하다. 기본적으로 스마트그리드 보급 및 확산 초기인 경우에는 스마트그리드를 전력과 인터넷, 그리고 보안이라는 다양한 측면에서 이해하고 대책을 수립할 수 있는 전문가가 상당기간 부족할 수밖에 없다. 따라서 정부에서는 이러한 특화된 분야의 인력 수급에 대한 정확한 수요조사를 통해 사회에서 필요로 하는 전문 인력을

배출할 수 있도록 시스템화 시키는 것이 필요하다. 대학의 관련학과나 전공개설 지원을 통해 고급인력을 양성하는 한편, 이미 사회에 배출되어 있는 인력에 대해서는 관련 기술 등의 재교육을 통해 스마트그리드 관련 전문 인력을 양성 추진해야 하겠다.

그리고 마지막으로 안전한 스마트그리드의 이용환경 조성을 위해 대국민 인식제고 노력이 필요할 것이다. 스마트그리드를 완벽하게 구현하기 위해서는 사업자 및 공급자뿐만 아니라 소비자 측면에서도 보안에 대한 적절한 인식 및 조치를 취할 수 있는 적극적인 자세가 필요하다. 소비자로서의 일반 국민뿐만 아니라, 관련 분야 종사인력들에게 각종 위협 및 이로 인한 피해를 최소화 할 수 있도록 세미나 혹은 TV, 신문 등 대중매체를 활용한 정부의 적극적인 홍보가 필요할 것이다. 아울러 전력 시스템과 인터넷이 결합됨에 따라 국경을 초월한 데이터의 이동이 가능하므로 스마트 그리드 보안에 대한 국제적 정보교류, 협력 체계 강화 또한 정부 차원의 지원이 뒷받침되어야 할 것이다.

5. 결 론

클라우드 서비스, 스마트 그리드 이외에도 신성장 동력으로서, 그리고 그린 IT 실현을 위해 앞으로도 지속적으로 새로운 IT 서비스 산업 모델들이 발굴될 것이다. 그러나 이처럼 인터넷을 기반으로 기기와 서비스간 융합이 진행되면서 새롭게 창출되는 신규 IT융합서비스 분야에 있어 보안의 중요성은 지속적으로 증대될 것이다.

이에 원활한 신규 서비스 창출, 시장 조성 및 활성화 등을 위해 사전에 보안문제에 대한 검증이 전제되어야하며, 예상되는 보안 이슈 및 기술에 대한 선제적 대응 체계 마련을 위한 사전 연구와 함께 보안 기술 보호조치 및 기준을 마련해야 할 것이다.

또한 서비스 제공자 및 사업자의 소비자 권익 보호를 위한 지침 또는 안내 해설서 등의 제정과 함께 기존 법률과의 관계정립을 통해 기존 법률의 정비·개선과 신규 법 제정 등 정보 통신망에서 발생하는 각종 사이버 위협에 대한 정보보호를 규율하고 있는 "정보통신망의 이용촉진 및 정보보호에 관한 법률"과의 조화도 고려하여야 할 것이다. 아울러 국경을 초월한 데이터 이동에 따른 국제관계 관련 법제적 정비가 필요하며 국제간 협력 체계 강화 방안 마련 또한 필요할 것이다. 또한 기존 제도에 대한 정비 및 강화를 통해 정보보호에 대한 적절한 인식 및 조치가 가능하도록 적극적인 대처가 요구되어진다.

그러나 이모든 대안들을 아우르는 동시에 지속적인 균형 발전과 에너지 이용의 효율성 향상을 위해서는 무엇보다 국가 차원의 정책·제도 수립, 법제 정비 및 산·학·연·관의 참여와 협력 기반 마련 등 적극적인 지원이 뒷받침 되어야 할 것이다.

참고문헌

[1] 그린 IT 국가 전략(안), '09.5, 녹색성장위원회

[2] 저탄소 녹색성장, 그린 IT의 비전과 전략, 국정감사 정책보고서, '09.10, 국회의원 진성호

[3] 가상화 기술의 현황과 전망, 인터넷이슈리포트 '09. 6호(한국인터넷진흥원)

[4] 스마트 그리드 추진 현황 및 이슈 분석, 인터넷&시큐리티 이슈 '09. 11월호(한국인터넷진흥원)

[5] 국가 스마트 그리드 연계 클라우드, 범정부 클라우드 서비스 활성화 종합계획 中, '09.12

[6] 클라우드 컴퓨팅 보안의 방향성, 월간 PC라인 '09.6월호

[7] 클라우드 컴퓨팅 서비스의 현 위치와 성장

환경 조성을 위한 정책방향, 인터넷이슈리포트 '09. 2호(한국인터넷진흥원)
[8] 국내외 클라우드 컴퓨팅 동향 및 전망, 정보처리학회지 제16권 제2호
[9] 'EMC RSA 클라우드 환경을 위한 보안지침 발표', 디지털데일리 '09.11.16
[10] '클라우드 규제나선 FTC, 국내는?', 디지털데일리 '10.1.7
[11] 'MS, 클라우드컴퓨팅 법안 필요 주장', 전자신문 '10.1.22
[12] Ministry of Internal Affairs and Communications, Digital Japan Creation Project, http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Topics/pdf/090406_1.pdf, 2009. 3.
[13] ENISA, "tCloud computing Risk Assessment: Benefits, risks and recommendations for information security", http://www.enisa.europa.eu/, 2009. 11.
[14] 글로벌 IT 네트워크 - 2009 년 주요 IT 전략 기술에 따른 보안 이슈 및 해결 방안, 한국정보사회진흥원, IT Issues Weekly 제 197호, 2009. 1. 29.
[15] Michael Armbrust, etc, Above the Clouds: A Berkeley View of Cloud Computing,http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html, 2009. 2.
[16] IDC, IDC Enterprise Panel, 2008.8. n=244
[17] J.Heiser and M. Nicolett, Assessing the Security Risks of Cloud Computing, Gartner, 2008. 6.
[18] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing, Apr. 2009.
[19] P.Mell and T. Grance, The NIST Definition of Cloud Computing, 2009. 10.

저자약력

유 지 영

2003년 한국외국어대학교 체코어과(학사)
현재 한국인터넷진흥원(KISA) 인터넷융합단 미래인터넷팀 주임연구원
이 메 일 : yoojy@kisa.or.kr

이 재 일

1986년 서울대학교 계산통계학과(이학학사)
1988년 서울대학교 계산통계학과 석사(전산학)
2006년 연세대학교 컴퓨터과학과 박사
현재 한국인터넷진흥원(KISA) 인터넷융합단장
이 메 일 : jilee@kisa.or.kr