情報保護學會論文誌
第 22 卷 第 3 號, 2012. 6

국방 클라우드 컴퓨팅 도입에 관한 보안체계 연구

장 월 수,† 최 중 영, 임 종 인‡
고려대학교 정보보호대학원

A Study on adopting cloud computing in the military

Worl-Su Jang,† Jung-Young Choi, Jong-in Lim‡
Graduate School of Information Security, Korea University

요 약

국방부에서는 2012년도에 클라우드 컴퓨팅을 시범적으로 도입하는 것으로 계획하고 추진하고 있는데 군과 같이 고도의 보안이 요구되고 전시 임무 등을 고려할 때 자칫 잘 못 설계될 경우 국가안보와 국가이익에 엄청난 피해가 예상된다. 특히, 남북이 대치되어 있고 평시에도 보안사고가 지속적으로 발생하여 보안취약점이 대군불신을 유발하고 있음에도 불구하고 보안대책 검토 없이 무조건 도입하는 것은 보안관련 법규에 위반될 뿐만 아니라 국내·외적인 여러 부작용을 유발할 수 있다. 따라서, 본 논문에서는 국방업무 중에서 클라우드 컴퓨팅을 적용해도 가능한 업무와 보안기술, 보안관리, 보안사고 처리 방법 및 보안관련 법적 해결 조건 등을 제시하면서 도입조건을 정립하였다.

ABSTRACT

The South Korean Defense Ministry is planning and pushing forward to conduct a cloud computing pilot project in 2012. Taking into consideration the high-level security necessary in the military as well as wartime duties, if not designed properly, this project may anticipate severe damage to national security and interest. In particular, despite the fact that vulnerability due to inter-Korean confrontation and regular security-related incidents have been triggered, unconditionally conducting a cloud computing pilot project without reviewing not only violates security regulations but also causes various security-related side effects in and outside South Korea. Therefore, this thesis found conditions for conduct of this project by suggesting duties that can apply cloud computing as well as security technology, administration, post-accident matters and conditions for legally solving cloud computing in the military.

Keywords: Cloud computing, Security system, Military security, Information protection, Security policy

I. 서 론

국방부에서는 2012년에 클라우드 컴퓨팅을 시범적으로 도입하는 것으로 계획하고 추진하고 있다. 클라우드 컴퓨팅이란 사용자들이 인터넷에 연결된 단말기를 통해 대용량의 컴퓨터 집합에 접속하여 애플리케이션, 스토리지, OS, 보안 등 필요한 IT자원을 원하는 시점에 필요로 하는 만큼 골라서 사용하며, 사용량에 기반하여 대가를 지불하는 컴퓨팅을 말한다[1].

최근에는 네트워크의 고도화와 가상화 같은 소프트웨어 기술이 발전되면서 광범위한 분야의 소프트웨어와 IT자원들이 인터넷을 통해 제공될 수 있는 환경이 조성되어 클라우드 컴퓨팅이 확산되고 있다. 특히, 여러 공간에서 다수의 사용자에 의하여 이루어지는 서비스이므로 보안 체계에 대한 확립 없이는 안전한 서비스를 보장 할 수 없다.

이러한 보안취약점이 있음에도 군과 같이 고도의 보안이 요구되고 전시 임무 등을 수행하는 특수조직에

접수일(2012년 1월 9일), 수정일(1차 : 2012년 3월 9일, 2차: 2012년 4월 9일), 게재확정일(2012년 5월 29일)
† 주저자, jworls@hanmail.net
‡ 교신저자, jilim@korea.ac.kr

서 무분별하게 도입할 때에는 자칫 국가안보와 국가이익에 엄청난 피해가 예상된다. 또한, 평시에도 보안사고가 지속적으로 발생하여 보안취약점이 대군불신을 유발하고 있음에도 불구하고 보안대책 및 보안정책 검토 없이 무조건 도입하는 것은 보안관련 법규에 위반될 뿐만 아니라 국내·외적인 여러 부작용을 유발할 수 있다.

따라서 본 연구에서는 현재까지 국방 분야에 클라우드 컴퓨팅 도입과 관련 보안문제를 연구한 내용이 없는 점 유사한 연구 2건 : 국방 분야에서 클라우드 컴퓨팅 기반 무인무기체계의 임무수행 SW에 관한 연구, 네트워크 중심전(NCW)에서의 클라우드 서비스 상호 운용성 보안기술 연구을 감안하여 국방업무 중에서 클라우드 컴퓨팅을 적용해도 가능한 업무와 보안기술, 보안관리, 보안사고 처리 방법 및 보안관련 법적 해결 조건 등을 제시하면서 신중한 도입조건을 정립하였다.

논문의 구성은 다음과 같다. 2장에서는 클라우드 컴퓨팅 보안동향을 분석하고, 3장에서는 클라우드 컴퓨팅 보안기술 및 정책을 평가해본다. 4장에서는 클라우드 컴퓨팅 실천적 적용 방안을 제안하고, 마지막으로 5장에서는 결론을 맺는다.

II. 국방 클라우드 컴퓨팅 구축 방안

2.1 클라우드 컴퓨팅 도입 필요성

국방정보체계에 클라우드 컴퓨팅을 도입해야 하는 이유는 기존의 데이터 센터에 클라우드를 도입할 경우 물리적 공간의 80%와 에너지 소비를 약 40%를 절약할 수 있다. 또한 군의 통합정보관리소 구축 시 체계 통합률을 향상시켜 체계 구축 및 운영비용을 절감하고, 체계운영 또한 안정성을 향상시킬 뿐만 아니라 DR(재해복구) 체계 구축비용을 절감하면서 운영의 효율화도 기할 수 있기 때문에 필요하다.

특히, 군에서는 네트워크戰에 대비하여 TICN(전술정보통신체계)을 도입하기 때문에 클라우드 컴퓨팅의 장점인 유·무선 네트워크를 이용한 이동성을 향상과 데이터센터의 집중적인 보안관리 등을 위해 반드시 도입할 가치가 있다.

2.2 클라우드 컴퓨팅 프레임워크

클라우드 컴퓨팅 도입 프레임워크는 전투체계, 전투근무체계, 연구개발체계 및 서비스체계 등을 고려하여 4가지로 구분하였다. 첫째, C4I체계, 국방 아키텍처 등 국방전력의 핵심이 되는 정보화 부문에서는 클라우드 컴퓨팅보다는 군 주도개발(in-house)개발과 같은 일반적인 정보시스템 구축 방법을 활용한다. 둘째, 온 나라시스템, 국방동원정보체계와 같은 일반 행정시스템은 서비스의 연속성이 중요하지만 경쟁우위와 연결되지는 않으므로 SaaS 서비스로 구축한다. 셋째, 국방 분야에서 필요한 신기술의 적용 가능성을 실험하는 U-defence 협력 사업에선 PaaS이나 IaaS 서비스를 활용한다. 넷째, 전자 기록관시스템 구축과 같은 필요하지만 상대적으로 중요도가 떨어지는 시스템은 SaaS 서비스를 활용하도록 한다.

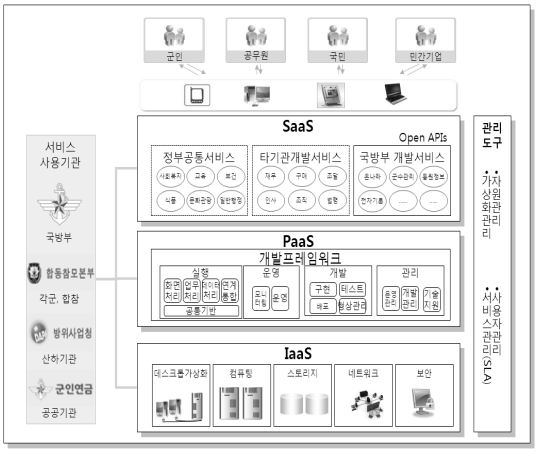
[표 1] 국방 정보화를 위한 클라우드 컴퓨팅 도입 프레임워크

구 분	코어	컨텍스트
미션 크리티컬	① C4I체계, 국방아키텍처	②(SaaS)온나라시스템, RFID군수물자관리체계, 국방동원정보체계, 기관 홈페이지
비-미션 크리티컬	③ (PaaS, IaaS) 과학화훈련장 시뮬레이터 연동, U-defence 협력사업	④(SaaS)전자기록관리시스템

2.3 국방 클라우드(K-Defence Cloud)의 설계

클라우드 컴퓨팅 분류(SaaS, PaaS, IaaS)에 따라 국방부의 클라우드 서비스 모델(K-Defence Cloud)을 구성하면 〈그림 1〉과 같다. SaaS는 국방부에서 자체 개발한 서비스 컴포넌트와 기 개발한 정부공통서비스나 타 부처에서 개발한 서비스를 연계하여 사용한다. 여기에서 사용되는 컴포넌트는 주로 국방 PaaS에서 개발된 것으로 한번 개발되면 공통적으로 사용되기 때문에 중복개발에 따른 혼란과 예산낭비를 줄일 수 있다. 현재 각 기관별로 확산하고 있는 정부업무관리시스템이나 전자기록관 시스템도 SaaS 형태로 개발하면 한 번의 노력으로 여러 기관이 시스템을 도입하는 효과를 거둘 수 있다[2].

또한, PaaS에서는 행정안전부가 개발하여 보급중인 전자정부 개발 표준 프레임워크를 활용하여 국방부에서 필요한 서비스를 개발할 수 있는 도구를 제공한다. 행정안전부를 비롯한 많은 중앙행정기관의 정보시



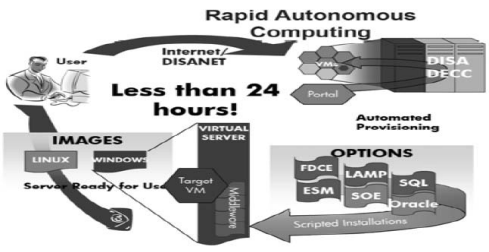
〔그림 1〕 국방 클라우드(K-Defence Cloud)의 구성

스템 개발에 적용 되고 있는 전자정부 개발 표준 프레임워크는 유지보수의 주체가 분명하고 사용 경험이 있는 개발자가 많다는 장점이 있다.

IaaS서비스는 비교적 저렴한 인텔사의 x86계열 CPU를 사용하지만, 가상화(virtualization) 기술을 사용하여 윈도우(Windows) 뿐만 아니라 Unix나 메인프레임 같은 운영체제도 제공할 수 있기 때문에 유지보수 수명연한을 다한 하드웨어를 저렴한 비용에 대체할 수 있다.

2.4 외국의 도입사례

美 국방성 사례를 살펴보면 美 국방성의 정보시스템계획국(DISA)은 '08년에 서버, 웹 애플리케이션 플랫폼 등 필요한 개발 환경을 인터넷을 통해 제공하는 클라우드 서비스 개발 인프라 및 테스트 환경인 RACE(Rapid Access Computing Environment)를 구축하였다. 이를 통해 정보통신기술 인프라 구매 비용 절감, 각 클라이언트의 요청에 따른 자원할당 소요시간 단축을 통해 생산성 증대 및 운영비



〔그림 2〕 美 국방성 DISA의 RACE 시스템

용을 절감하고 있다〔3〕.

III. 클라우드 컴퓨팅 보안 기술 및 정책

국방부에서는 2012년에 클라우드 컴퓨팅을 시범 구축할 예정인데 이는 IT 인프라스트럭처의 범위가 외부까지 확대 되면서 보안문제가 큰 과제로 대두되고 있다. 클라우드 컴퓨팅을 통해 데이터가 연동되고 자원을 다양하게 활용하는 것에는 軍事관련 데이터 보호와 자원의 관리 정책, 군사 비밀 관리 그리고 장병들의 프라이버시 측면에서 문제점이 존재한다. 따라서 클라우드 컴퓨팅의 보안적인 위협 및 문제점을 분석하여 클라우드 컴퓨팅 공급자, 군 조직 및 이용자를 위한 보안 기술과 정책들을 연구하였다.

3.1 보안기술

3.1.1 암호화 및 키 관리

클라우드 컴퓨팅 시스템에서 보관하고 있는 자료에 대한 강력한 암호화와 사용자들의 수시 변경에 따른 키 관리가 핵심 메커니즘이다. 특히, 클라우드 컴퓨팅으로 인해 경계선이 급격하게 무너지면서 저장된 데이터와 이동 중인 데이터 사이의 구분이 불명확해지고 있다〔4〕. 따라서 데이터 전송 메커니즘과 데이터 저장 메커니즘을 서로 조화롭게 사용되어야 하고 군과 서비스 제공자는 모두 암호화 및 키 관리만 제공할 수 있는 데이터 무결성 컴퓨터 시스템이 필요하다.

3.1.2 인증 정보 및 접근관리

클라우드 컴퓨팅 서비스 제공자들은 기존 인증 서비스 제공자와 통합할 수 있도록 초기에 연계 표준지원을 문의하고 사용 중인 표준과 일치시킬 수 있는지 확인하는 것이 중요하며 연계를 위한 업계표준을 폭넓게 지원해야 한다. 보통 클라우드 서비스 제공자가 보안 표준 언어 (SAML: Security Assertion Markup Language)와 같은 연계 표준을 사용하여 기업인증 서비스 제공자에게 인증 업무를 위임한다〔5〕. 장기적으로 고객들은 Extensible Access Control Markup Language(XACML)를 내부적으로 구현하지 않는 경우에도 클라우드 서비스 제공자 측에서 XACLM 호환 권한 관리를 더 욱 적극적으로 지원하여야 한다.

3.1.3 애플리케이션 보안

클라우드 플랫폼에 배치할 애플리케이션 설계 및 구현을 위해서는 기존의 애플리케이션 보안 프로그램의 최신화 및 표준화를 재평가하여야 한다. 기업의 최신 애플리케이션 보안 사례와 표준을 변경하기 위해서는 클라우드 플랫폼의 미묘한 차이점을 다루어야 한다. 이러한 차이 중 일부는 클라우드 플랫폼의 다중 애플리케이션 환경과 이 환경에 대한 직접적인 통제 수단의 부족, 그리고 클라우드 플랫폼을 제공하는 기업의 데이터 접근 권한으로 발생한다. 이러한 차이점은 애플리케이션 수준의 일련의 통제 수단을 통하거나, 클라우드 제공기업과의 서비스 계약을 통한 애플리케이션으로 처리되어야 한다.

3.2 보안관리

3.2.1 서비스 제공자 역할

서비스 제공자는 악의적인 직원이나 벤더는 조기에 찾아내어 처리하고, 정보 누설 예방을 위해 직무 및 접근 권한을 분류한다. 접근 권한은 직무수행을 위해 필요한 사람들에게만 부여되며 조직체 내에서의 상태 또는 직위만을 근거로 부여되지 않는다. 모든 채용자와 퇴사자는 접근 권한통제시스템을 정기적으로 검토하는 것이 필요하다. 또한, 재난 복구 관련 내용, 국제법과 국내법, 업계 표준 등의 준수 상태를 확인한다.

3.2.2 서비스 이용자 역할

서비스 이용자는 서비스 제공자에게 데이터의 보안 요구사항과 업무성격을 명확히 알려주고 특히, 유사시 위기관리 내용도 계약상에 포함시켜야 한다. 그리고 서비스 제공업체의 물리적·인적 보안 조치, 재난 복구 및 업무 연속성 계획을 검사하고 중요한 기능의 복구 목표에 대한 구체적인 서약서를 받아 클라우드 서비스 제공자가 보안에 대해 계약상의 책임을 지게 해야 한다.

3.2.3 정보 보안법 준수

서비스 제공 업체에서는 보안 대책을 강구하지 않을 경우 민사 소송과 집단 소송을 당할 수 있으며, 법 집행 기관에 의해 법 집행 조치도 당할 수 있다. 그리고 위탁된 데이터를 안전하게 보호하기 위하여 적절한 기술적, 물리적 및 조직적 조치를 강구해야 한다. 특히, 서비스 제공자와 클라이언트가 각각 해야 할 일을 명확하게 하는 서비스 계약의 구체적인 조항에 반영되어야 한다.

3.2.4 클라우드 서비스 활동 모니터링

클라우드 서비스 제공자의 업무 수행을 모니터링하고 시스템의 취약점을 시험하고 새로운 위협이나 취약점이 발견되면 변경을 요청하는 것은 회사의 법적 책임에 속한다. 이런 목적에서 클라우드 서비스 계약은 이 모니터링과 테스트를 실시할 수 있는 회사의 능력을 규정해야 한다.

3.2.5 기타 고려사항

계약에 일반적인 '감사 권리' 조항을 두는 것 외에, '감사 가능성'과 관련하여 계약 내용에 더 많은 주의가 필요하다. 정부기관이나 공공기관은 보안관련 법에 의거 매년 보안감사를 하고 있어 어떻게 수검을 받을 것인지 등에 대해 정립하고 계약 당사자 간에 마찰 및 부작용이 발생하지 않도록 명시한다.

3.3 보안사고 관리

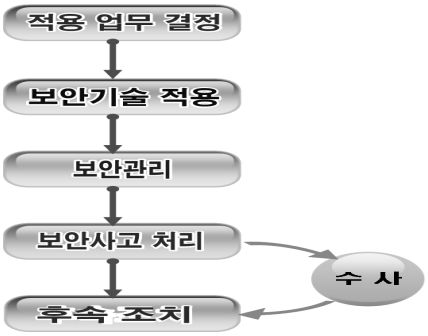
3.3.1 사고 대응, 통보 및 치료

서비스 제공자의 사고 대응 전략은 문제 식별과 통보를 담당해야 하며, 데이터에 대한 범죄자들의 접근을 시정하는 옵션을 강조해야 할 것이다. 아울러, 데이터 관리 및 접근권한은 애플리케이션 사용자가 거주하는 위치(국가)에 따라 의미가 다르고 규제 요건도 달라진다.

사고 대응은 사고에 대해 표면화시킬 수 있는 구체적인 데이터 및 데이터 관리 도구에 연관시켜 그 데이터를 처리 할 수 있는 능력이 있는가에 따라 달라질 것이다. 그리고 발생하는 사고에서는 위반 또는 기타 악의적인 사용이 탐지되면 일반적으로 제일 먼저 취하는 조치가 애플리케이션 실행 중지이며, 문제가 완전히 진단되어야 최종 치료가 완료된다.

3.3.2 보안 위반 처리

클라우드 서비스 제공자와 클라이언트는 모두 상대측이 위반이 존재함을 즉시 공개하는지 확인해야 한



〔그림 3〕 美국방 분야 도입을 위한 보안연구 절차

다. 클라이언트는 위반 발생에 대해 자신의 고객들이나 직원들에게 알려야 할 것이다. 클라우드 서비스 제공자는 위반이 발생했음을 다른 클라이언트들에게 알려야 할 수도 있다. 클라우드 컴퓨팅에서는 많은 자원을 공유하는 환경이 구축되므로 양 계약자들이 모두 서비스 운영에 영향을 주는 보안 위반을 즉시 공개할 책임이 있다. 이런 공개는 클라우드 내부나 외부에서 파문 효과를 일으켜 더 많은 감염이 발생하는 것을 방지하는데 필요하다. 계약자들은 보안 위반을 철저하게 그리고 신속하게 처리하는 보안사고 대응 계획을 마련해야 한다.

3.4 법적문제

클라우드 컴퓨팅을 도입할 경우 우선적으로 서비스 제공자와 이용자들이 법적인 요구사항을 파악해야 한다. 왜냐하면, 데이터를 제3자에게 위탁하면 유출 여부 및 훼손 등을 이유로 분쟁이 발생하고 서비스 제공자의 폐업으로 데이터를 담보로 잡을 수도 있으며 민사 소송과 정부 기관의 조사로 증거를 수집할 수 있기 때문이다.

아울러, 클라우드 서비스를 활용하기를 원하는 글로벌 회사는 자회사, 클라이언트 및 비즈니스 파트너들이 다른 제한 규정이 있는 외국법을 지켜야 하는 사람들이 위험하게 되지 않기를 원한다〔5〕.

또한, 회사는 고용인, 클라이언트 및 기타 사람들의 개인 데이터가 배치 될 위치를 알고 싶어 한다. 외국 데이터 보호법에서 요구하는 구체적인 제한 사항에 대처할 수 있기 때문이다. 클라우드 서비스 제공자가 데이터가 움직이는 위치를 아는 것은 데이터가 국경을 통과하는 것을 제한하는 현지 법률 준수를 보장하는 요구된 조치를 시행하는 것의 전제 조건이다〔6〕.

IV. 클라우드 컴퓨팅 실천적 적용 방안

클라우드 컴퓨팅을 국방분야에 도입하기 위한 보안 체계는 먼저 적용해도 보안상 문제가 크지 않은 업무를 식별하고 기존의 보안 기술 중 국정원 승인된 제품을 적용할 수 있는 지 판단한다. 이어 보안 관리를 클라우드 컴퓨팅 업체와 효율적으로 할 수 있는 보안정책을 수립한다. 아울러, 보안위규 사항에 대해 국내외 제반 보안관련 법에 저촉되지 않도록 하면서 군사기밀에 유출되었다고 판단될 경우 수사를 어떻게 할 것인지를 정립한다. 마지막으로 사후 유사문제 예방차원에서의 후속 조치 방안에 대해 문제가 없도록 방안을 제시하고자 한다.

4.1 국방 적용업무 결정

클라우드 컴퓨팅을 국방분야에 적용하기 위해서는 몇 가지 필요충분조건을 갖추어야 한다. 첫째, 군사비밀이나 군사자료가 포함된 업무가 아니어야 하고 둘째, 클라우드 컴퓨팅을 적용함에 따라 경제적 효과가 있어야 하며 셋째 국방망에 있는 자료를 쉽게 이동하거나 보안취약점이 없어야 함과 아울러, 넷째, 군내 사용하고 있는 시스템과 호환성이 있어 유사시 활용할 수 있어야 한다. 예를 들어 각급부대에서 운영하고 있는 홈페이지, 예비역들에게 제공하는 대민서비스 업무 및 현역과 예비역이 사용하는 복지관련 사이트 등에 활용으로써 군의 경량화는 물론 편리성에 도움이 될 것으로 보인다.

4.2 보안기술

클라우드 컴퓨팅의 보안기술 적용 방안을 제시하기 위해 플랫폼, 저장방식, 네트워크, 단말로 구분하여 정립하였다. 플랫폼에 사용되는 보안기술로는 접근제어와 사용자 인증 기술이 가장 대표적으로 쓰인다. 접근제어는 운영체제상의 한 프로세스가 다른 프로세스의 영역(파일 혹은 메모리)에 근하는 것을 통제하는 기술로 Discretionary Access Control(DAC), Mandatory Access Control(MAC), Role Based Access Control(RBAC) 등이 대표적이다. 사용자 인증을 위해 사용되는 기술은 크게 일반적인 사용자 인증 방식과 네트워크상에서의 인증방식으로 나누어진다〔7〕.

일반적인 사용자 인증 방식으로 Single-Sign On

(SSO) 형태의 인증 기술, ID와 Password 인증, Public Key Infrastructure(PKI) 공개키 암호기법, Multi-factor 인증(지문, 홍채 등과 같은 생체인식, 인증서, OTP 등), i-PIN 등이 있고 네트워크 상에서의 사용자 인증은 Microsoft .Net Passport(LiveID), ID 연계 기반 인증 방식, User-centric 이용 방식 및 URL 기반 인증 방식 등을 적용할 수 있다[8].

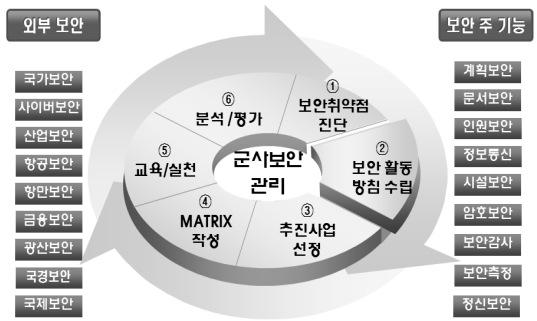
저장방식에 대한 대표적인 보안 기술로 '검색 가능 암호시스템'과 'Privacy Preserving Data Mining(PPDM)' 기술을 들 수 있다. 검색 가능 암호 시스템은 기존의 암호 기술과 같이 암호화된 정보에 대한 기밀성을 보장하면서 동시에 특정 키워드를 포함하는 정보를 검색할 수 있도록 고안된 암호 기술이고 PPDM은 일반적으로 실용적인 프라이버시 보존형 데이터 마이닝과 데이터 마이닝에 Secure Multiparity Computation(SMC) 기술이 적용된다.

네트워크 보안 기술은 인터넷의 발전과 함께 해왔다. 클라우드 컴퓨팅 기술이 새로운 기술이 아니라 실제 네트워크 기술을 발전 시켜 변화했기 때문에 보안 내용 또한 새로운 보안 기술이 필요한 것이 아니라 네크워크 보안 기술 중 클라우드 컴퓨팅 환경에 맞는 기술들이 필요하게 되었다. 클라우드 컴퓨팅에서 필요한 대표적인 기술로 통신상의 기밀성을 보장하는 SSL과 IPsec 기술, 그리고 네트워크를 통한 공격을 차단하는 application firewall과 DDoS 방지 기술을 들 수 있다. 단말은 클라우드 컴퓨팅 환경에서 빼놓을 수 없는 요소이다. 대표적인 단말 보안 기술들은 대부분 암호학적 이론에 근거한 알고리즘 및 프로토콜 기반으로 동작되기 때문에 단말 인식 및 인증 기법, 암호학적 프리미티브에 대한 안전성 보장 기법 등이 있다. 이중에서 하드웨어를 이용하여 암호학적 프리미티브를 물리적으로 보호하는 기술들은 현재까지 가장 안전한 기술로 여겨지고 있다.

4.3 보안관리

군사보안의 보안관리는 군의 임무, 기능, 보유장비 및 특수한 신분 등으로 인해 〈그림 4〉와 같이 외부적인 보안과 연계가 되고 군 내부의 보안 주요기능도 다양할 뿐만 아니라 복잡하게 이루어져 있다. 특히, 정보체계를 도입하거나 훈련 및 각종 임무를 수행할 때에는 6단계의 보안절차를 걸쳐 진행된다.

이러한 복잡한 보안관리를 클라우드 컴퓨팅 체계라



〔그림 4〕 군사보안 관리 절차 및 주요 기능

〔표 2〕 국방 정보화를 위한 클라우드 컴퓨팅 도입 프레임워크

보안환경 4단계	조 치 내 용
전투 상황	- 복구후 사용이 불가하도록 완전 파기하고 사전 군 요구 시 협조 조치
국지전(局地戰)	- 국지전 발생 지역에서 적에게 피탈되거나 해킹 등 침해사고 차단 조치
비상 상황	- 군 비상상황에 부합되도록 모든 이용자 통제 및 비상인력 투입 유지
평시 상황	- 서비스 제공자 입장에서 기술보안 및 관리보안 임무 수행

는 하나의 사업을 도입하는 차원에서 보안 주요 기능에 대해 세부적으로 방안을 제시하고자 한다.

4.3.1 계획보안

계획보안이란 기관·사업별로 보안 주요 업무를 어떻게 수행할 것인지를 계획, 관리, 분석하는 핵심 보안업무이다. 클라우드 컴퓨팅을 도입하기 위해서는 문서보안, 인원보안, 정보통신보안, 시설보안, 암호보안, 보안감사, 보안측정 및 정신보안 업무를 어떻게 하겠다는 종합적인 보안정책 보안정책에는 개요, 중점, 추진업무, 일정, 참고사항 및 예산 등을 포함하여 기술한다.

이 포함되어야 하고 반드시 보안 계약서의 특수조건이 포함되어야 한다. 특히, 군의 보안환경 변화에 따라 클라우드 서비스 제공자와 이용자의 보안관리도 〔표 2〕 와 같이 신속한 조치가 이루어져야 한다.

4.3.2 문서보안

문서보안 분야는 클라우드 서비스 이용자와 제공자 간에 문서상으로 계약을 체결한다. 계약서에는 목적,

보안책임, 군사보안 관련 법규, 군사자료(비밀, 개인정보) 관리, 출입통제, 보안조치, 보안점검, 사고협조, 보안감사 및 자료반납 등 갑·을 갑은 국방부를 비롯하여 군부대이고, 을은 클라우드 서비스 제공업체이며, 병도 있을 수 있는데 이는 최대한 제한하는 것이 복잡하지 않을 것이다.

이 준수해야할 사항을 명확히 정립하여 포함한다. 아울러, 합법적인 수사를 제외하고 자료, 데이터 로그 및 제반 체계내용 등을 제3자에게 공개·제공·열람이 불가하도록 보안대책을 강구한다.

또한, 서비스 이용자는 어떤 개인의 정보보호 및 공개 요구사항이 존재하는지 판단하고, 서비스 제공자가 그런 요구사항을 지원할 수 있는지 확인하는 조치를 취해야 한다[9].

4.3.3 인원관리

군 시스템 전담 보안담당관 및 장비담당관(정·부)과 관련자는 신원조사를 실시한 후에 적격자에 한하여 이용자에게 임명을 의뢰하고 데이터가 종합되어 비밀이거나 대외비가 될 경우 비밀취급인가를 승인해 준다[10]. 군 시스템 전담 소속 全직원은 군사기밀보호법, 국가보안법 및 군사보안업무훈령 등 보안관련 법규를 준수하겠다는 보안준수 서약서에 서명한다. 특히, 외국인 및 외국 업체에 위탁할 때에는 종합적인 보안대책을 강구하고 시행 전에 서비스 이용자에게 승인을 득해야 하며 현행 보안관련 법규로는 불가하기 때문에 주의해야 한다. 또한 인원이 변경되었을 때에는 신규 전담인원 임명과 동일하게 신원조사 및 승인을 득하고 투입한다.

투입 인원에 대한 보안교육은 월 1회 2시간 이상을 교육해야 하며 군과 관련 사항이 외부로 유출되지 않도록 포괄적인 사항을 교육한다. 필요시 군사보안 전문가를 초빙하여 교육할 수 있으며 서비스 제공자 측에서 교육하고자 할 때에는 보안담당자 전원이 참석해야 한다.

4.3.4 정보통신보안

정보통신보안은 클라우드 컴퓨팅 서버 접근관리, 데이터관리, 저장매체·장비·개인 핸드폰 반출입관리 및 암호장비 등을 체계적으로 조정·통제하는 보안업무이다. 먼저, 서비스 이용자는 데이터에 대한 누가, 언제 어떤 조건에서 데이터에 접근해야 하는지 결정하는 일을 담당한다. 제공자는 데이터 접근 권한을 직원 및 다른 고객들에게는 주지 않는다는 것을 보장하는 계약내용을 명시해야 한다. 또한, 물리적 스토리지 위치에 대한 접근 권한이 있는 모든 클라우드 서비스 제공자 직원들은 계약 및 보증이 되어야 한다.

둘째, 서비스 제공자는 데이터의 백업 기능을 제공하고 서비스 이용자는 종종 지속적인 논리적 데이터 구분을 검증하는 테스트를 수행해야 하며 데이터 보유 및 파기 스케줄은 서비스 이용자의 책임이다. 클라우드의 자원을 공유하는 것은 서비스 이용자가 항상 그 데이터에 대해 사용된 매체를 삭제된 데이터의 모든 흔적이 사라지기 전에 다른 용도로 재사용했는지 확인해야 한다.

셋째, 서버실 반·출입 장비는 반입단계에서 장비대장에 등록하고 하드디스크에 악성코드나 바이러스가 저장되어 있는지 확인해야 한다. 반출단계에서는 반드시 완전 포맷 조치하고 그 근거를 대장에 기록하며 이를 장비 담당관 '정'이 직접 수행해야 한다. 마지막으로, 암호장비는 군전용 국가용 비공개 알고리즘을 사용하기 때문에 별도 대장을 유지하고 필히 서비스 이용기관의 보안담당관이 접근할 수 있도록 조치한다.

4.3.5 시설보안

클라우드 컴퓨팅 서버실은 통제구역으로 설정하고 군사보안업무훈령에 의거 출입문에 '군사 통제구역' 경고 문구를 부착하거나 부착 시 오히려 노출 우려가 있을 경우 출입자 제한 조치만 철저히 한다. 그리고, 출입인원은 승인권자 승인 이후 출입하도록 시스템을 구축하고 출입대장을 유지한다[11].

또한, 첨단 보안시스템은 출입문에 생체인식 시스템을 2단계 인증으로 출입하도록 하고, CC폐쇄회로)TV는 사각지점이 최소화되도록 설비함과 아울러, 화재예방을 위해 열 센서를 구축하여 24시간 중앙통제실에서 모니터링 한다. 서버실의 시설강도는 1000LB 이상 중요 시설물 강도는 2000년 이전에 500LB 이상으로 규정했으나 이후에 각종 무기들의 효과가 높아짐에 다라 1000LB이상의 강도로 설계하고 있다.

적의 폭격에도 안전하고 직격탄 및 지근탄으로부터 보호가 될 수 있도록 설계함은 물론., 충격 완화를 위해 주 서버 장비 하단에 스프링으로 지지한다.

4.3.6 보안감사

보안감사는 보안업무를 보안관련 각종 규정에 따라 시행 했는지 등을 전반적으로 점검하고 보안 취약점을

발국하여 사고예방 대책을 강구하도록 지원하는 정기 감사와 수시 감사가 있다. 정기 보안감사는 서비스 이용자 측에서 연 1회 정기 감사와 수시 감사를 실시할 수 있으며 감사관은 서비스 이용자 측이 정식으로 통보·승인한 인원만이 출입시키고 감사준비는 갑과 을이 협의 하에 사전 정리하여 감사 간 문제가 없도록 한다. 감사 후 수정·보완은 계약조건, 예산, 취약점 발생원인 제공자, 타 기관과의 형평성 및 군의 특수 보안환경 등을 분석하여 신속히 조치한다[12].

수시 감사는 서비스 이용기관에서 판단했을 때에 보안취약점이 표출되었거나 보안사고가 발생하였을 때에 서비스 제공자와 이용자가 함께할 수도 있고 서비스 이용자와 보안 전문기관이 할 수 있다.

4.3.7 계약종료 보장

클라우드 서비스 계약은 계약 기간이 끝나면 갱신되지 않을 수 있고 계약자들 중 한 사람의 계약 불이행이나 중대한 위반, 또는 재정적인 어려움과 파산 절차로 인해 계약 관계가 종료될 수도 있다. 이럴 때에 을은 데이터 보호법 등에 의거 위탁된 데이터를 계속 책임지며, 갑에게 데이터 필요 유무를 확인하여 제공해야 한다. 역으로 갑의 잘 못으로 을이 데이터를 보관하는 경우도 있는데 공간 절약이나 기술적인 이유로 갑의 데이터가 다른 클라이언트의 데이터와 섞일 수 있으며, 다른 구성요소들과 분리할 수 없을 수 있다. 따라서 서비스 계약을 체결할 때도 이런 문제를 예상하고 계약 종료 시의 적절한 절차를 정의하고 분쟁을 해결하는 타개책을 명시해야 한다.

4.4 보안사고 처리

서비스 제공자는 보안사고 및 안전사고 군사기밀 유출, 개인정보 공개, 제3자로 하여금 위험 수준 평가, 서비스 중단·확장·이관· 시설변경, 민원발생, 재난복구, 천재지변 등이다.

등 서비스 이용자 측이 알고 조치해야할 사항이 있을 때에는 신속히 2중 통신망으로 연락한다. 또한, 서비스 작업 중지서, 소환장, 정보수집 요구사항 및 기타 강제된 공개에 어쩔 수 없이 정보를 공개해야 하는 경우, 훼손된 부분이 없어야 한다. 서비스 이용자는 모든 데이터가 손상되지 않고 적절하게 공개되었음을 확인해야 할 뿐만 아니라, 다른 데이터도 전혀 영향을 받지 않았음을 확인해야 한다. 데이터를 공개할 수밖에 없을 경우 반드시 서비스 이용자에게 알려야 한다.

아울러, 국가의 보안업무 체계상 군사보안사고에 대해서는 군사보안업무훈령을 적용받은 직원만 해당되므로 계약을 체결한 서비스 업체(을 측)는 조사할 수 없고 외국기업은 더욱더 불가능하기 때문에 계약서상에 보안사고 조사에 대해 적극 협조함은 물론, 필요시 조사에 적극 응할 수 있도록 해야 한다.

또한, 보안사고의 범위, 절차, 을 측의 의무, 포렌식 조사 시 공개 범위 및 로그 다운로드 시 절차 등을 세부적으로 명시해야 한다. 기타 보안관련 법을 적용받지 않은 범죄행위에 대해서도 클라우드 컴퓨팅을 도입한다면 보안사고 조사 절차와 동일한 내용을 명시해야 한다[13].

4.5 수사

군사기밀이 외부로 유출되었을 경우, 〈표 3〉와 같이 신분과 관계없이 관련법에 의거 수사기관에서 수사를 할 수 있으나 클라우드 컴퓨팅 보안환경에서는 군기법의 형식성, 실질성, 비공개성을 입증하는데 어려움이 있기 때문에 서비스 이용자들이 보다 자료관리에 관심을 가져야 한다[14]. 그러나 클라우드 컴퓨팅 사용이 확산되고 점점 복잡해지면서 관할구역이 어디냐에 따라 복잡한 문제가 발생한다. 예를 들어 한국에서 생산된 비밀이 미국의 서버에 저장되어 있을 수 있고 사고가 발생하면 공조가 이루어져야 하며 시간이 장시간 소요될 수 있다. 미국 회사에서 중국에 아시아 지역 서버를 위치시킬 경우 중국의 법을 따라야 하는 문제가 발생한다는 것을 인식하고 회사 선정 및 사고발생 시 대처 방법을 미리 계약서에 포함해야 한다.

량 출입증은 RFID(Passive 900MHz)와 번호인식시스템을 혼합한 全軍 동일 체계 개념으로 구축하여 각급부대에서 시스템으로 자동 통제되고 근무자는 승차 인원 확인 및 검문검색에 집중할 수 있도록 구축해야 한다.

4.6 보안취약점 조치

각 클라우드 컴퓨팅을 운영하면서 발생할 수 있는 보안취약점은 크게 3가지로 유형으로 구분할 수 있다. 먼저 보안감사 및 보안순찰 등을 통해 보안취약점이 나타날 수 있고 두 번째는 서비스 제공자, 서비스 이용자 및 제3의 해커가 보안사고를 유발시킬 수 있으며 세 번째는 서비스 사용자에 의한 부주의로 군사기밀을

유출시키거나 서비스 제공자에 의해 개인정보 등 데이터를 유출할 수 있다.

이러한 유형에 따른 조치 방안으로 경미한 사항은 서비스 제공업체에서 우선적으로 조치하고 서비스 사용자에게 통보하며 예산과 장시간 소요되는 조치사항은 상호협의 하에 세부 조치방안을 수립하여 시행한다. 아울러, 예산이 소요되더라도 우선 조치가 필요한 사항은 계약서상에 명시하여 先 조치 後 정산 개념으로 보안을 우선 시 해야 한다. 대형 보안사고는 책임한계를 명확히 하여 선의의 피해가 없도록 계약서에 명시하고 이로 인한 유무형의 피해에 대해서도 보험가입 등을 통해 해결 방안을 준비해야 한다.

V. 결 론

군에서는 국방자원의 효율성과 활용성을 제고하고 침해사고 즉각 대응 및 생존성을 강화할 목적으로 클라우드 컴퓨팅 도입하는 것으로 추진하고 있기 때문에 이는 아주 고무적인 일이라고 판단된다. 그러나 명확한 보안정책 없이 또는 실질적인 보안관계관 승인을 받지 않은 상태에서 강력히 추진한다는 것은 몇 가지 이익과 편리성을 위해서 국가의 안보를 너무 쉽게 버리는 격이 되고, 이로 인해 피해는 예측이 불가할 수 있다.

따라서 국방부에서는 美 국방성과 유사하게 시범사업이라도 보안정책을 우선적으로 수립하고 문제가 없다고 판단 될 경우 부분적으로 구축해야 한다. 특히 보안과 관련 없는 장병복지 및 대민업무분야 등에 대해서는 적극 권장하고 군사비밀 및 군사자료가 저장·가공·유통되는 8대 자원관리체계와 5대 전장체계는 보안상 취약점이 해결되었을 때에 점진적으로 도입해야 한다.

본 논문에서는 클라우드 컴퓨팅을 군에 도입할 때에 표출될 수 있는 문제점을 사전 예견하고 현재 진행되고 있는 군사보안업무 중 반드시 지켜야할 내용을 정립하여 제시했다는 측면에서 관련 인원들에게 도움이 될 것으로 판단된다. 하지만, 데이터 암호화와 네트워크 간 암호화는 기존 국방에서 사용하고 있는 장비들과 호환이 될수 있는지와 국가 전쟁 수행 단계별로 세부적인 보안취약점과 대책을 어떻게 안정적으로 할 것인지 등에 대해서는 지속적인 연구가 필요하다.

마지막으로, 군사보안의 특수성과 보안문제 때문에 보다 구체적인 보안 취약점 등을 기술하지 못 하였고 참고 문헌 또한 군사보안업무훈령이 미공개 자료인 관계로 연구에 다소 제한이 있었다.

참고문헌

〔1〕 노윤재, 클라우드 컴퓨팅을 이용한 개인정보보호 기술에 관한 연구, 고려대학교, pp.10, 2009.12

〔2〕 김성현, 권혁진, 국방정보화를 위한 클라우드 컴퓨팅 구축 방안, 주간국방논단, 제1378호, pp.6-8, 2011.9.19

〔3〕 김성태, 클라우드 컴퓨팅의 동향과 군 도입 시 고려사항(2), 주간국방논단, 제1402호(12-11), pp.4, 2012.3.2

〔4〕 http//blog.naver.com/soldesks/cloud computing과 가상화, 새로운 IT패러다임. 2010.5

〔5〕 Gerald R. Ferrera, Cyber Law Second Edition, THOMSON, pp.16-17, 2007.7

〔6〕 이태훈, 사이버범죄 방지를 위한 국제공조 방안, 한국형사정책연구원, pp.71. 2004.12

〔7〕 황유동, 박동규, 장종수, 홈네트워크를 위한 디바이스 기반 접근제어, 한국정보기술학회논문지 제3권 제6호. pp.51-52. 2005.6

〔8〕 장월수, 보안총론, KIDA PRESS, pp.207-216. 2011. 1

〔9〕 행정안전부, 개인정보 보호법 제10465호, 제26조 업무위탁에 따른 개인정보의 처리 제한, pp.9. 2011.9

〔10〕 국정원, 보안업무규정 대통령령 제21214호, 제3장 신원조사, 2008.12.31

〔11〕 국방부, 군사보안업무훈령 제1275호, 제84조 군사보호구역의 설정대상, pp.68. 2010.9.27
국정원, 보안업무규정 대통령령 제21214호, 제30조 보호구역, 2008.12.31

〔12〕 국방부, 군사보안업무훈령 제1275호, 제182조 감사기관 및 대상, pp.131-132. 2010.9.27
국정원, 보안업무규정 대통령령 제21214호, 제39조 보안감사, 2008.12.31

〔13〕 국방부, 군사보안업무훈령 제1275호, 제3절 보안사고조사, pp.134-136. 2010.9.27
국정원, 보안업무규정 대통령령 제21214호, 제38조 전말조사, 2008.12.31

〔14〕 국방부, 군사기밀보호법 제7613호, 제22조 검사의 수사 지휘 등, pp.3. 2005.7

〈著者紹介〉

장 월 수 (Worl-Su Jang) 정회원
1990년 2월: 3사관학교 졸업
2002년 2월: 연세대학교 건축공학 석사
2006년 8월: 국방대학교 정보관리 석사
2010년 2월: 고려대학교 정보보호대학원 박사수료
現 한국국방연구원 보안과장, 세종시 보안자문위원 등
〈관심분야〉 국가보안, 군사보안, 비밀관리, 통합보안, 정보보호, 클라우드 등

최 중 영 (Jung-Young Choi) 정회원
2005년 2월: 중앙대학교 산업정보학과 졸업
2011년 8월: 고려대학교 정보보호대학원 석사
現 한국국방연구원 국방정보체계관리단 선임연구원
〈관심분야〉 국방정보체계, 정보보호정책, 개인정보보호, 통합보안, 디지털포렌식 등

임 종 인 (Jong-in Lim) 종신회원
1980년 2월: 고려대학교 수학과 졸업
1982년 2월: 고려대학교 수학과 석사
1986년 2월: 고려대학교 수학과 박사
現 고려대학교 정보보호대학원 원장 (고려대학교 정보보호연구원 원장 겸임), 대검찰청 디지털수사자문위원회 위원장, 금융보안연구원 보안전문기술위원회 위원장, 행정안전부 정책자문위원회 위원, 한국저작권위원회 위원 등
〈관심분야〉 정보법학, 디지털포렌식, 개인정보보호, 전자정부보안, 융합기술보안 등