情 報 保 護 學 會 誌
第22卷 第6號, 2012. 10

클라우드 보안 인증 스킴과 해결과제

신 종 회*

요 약

클라우드는 IT를 직접 소유하기 보다는 제3자가 제공하는 규격화된 요소들(소프트웨어, 플랫폼, 인프라구조 등)을 필요에 따라 셀프서비스 방식으로 사용하고 그에 따른 경비를 지불하는 모델을 포괄적으로 일컫는 용어이다. 그러나, 클라우드는 데이터를 집중 관리하므로 규모의 경제를 달성하는 데 용이하지만 악의적인 공격자에게는 더 매력적인 공격대상으로 간주되기도 한다. 이러한 모든 특징으로 인해 클라우드는 기존의 IT 환경에 비해 더 높은 수준의 보안 프로세스, 기술 및 의식을 요구하고 있다. 본 논문에서는 클라우드 서비스를 보호하기 위한 각종 보안 인증 스킴을 살펴보고, 아울러 클라우드 솔루션을 평가, 구현, 관리, 유지할 때 필요한 규정준수와 위험관리, 사용자 확인과 액세스 제어, 서비스 무결성, 종단점 무결성, 정보보호 등 핵심 보안 고려사항 5가지를 제안하였다.

Ⅰ. 서 론

최근 '클라우드 컴퓨팅'이 IT 분야의 대표적인 화두로 주목 받고 있다. 클라우드는 자체적으로 IT를 소유하고 관리하던 종래의 환경과는 달리 정보가 공급자의 관리 아래에 있게 되므로 특정 공간이나 지역에 한정되지 않으며, 물리적인 보안 또한 공급자에 의해 관리된다. 클라우드는 데이터를 집중 관리하므로 규모의 경제를 달성하는 데 용이하지만 악의적인 공격자에게는 더 매력적인 공격대상으로 간주되기도 한다. 이러한 모든 특징으로 인해 클라우드는 기존의 IT 환경에 비해 더 높은 수준의 보안 프로세스, 기술 및 의식을 요구하고 있다. 본 논문에서는 FISMA(Federal Information Security Management Act), ISO27001, FedRAMP((Federal Risk and Authorization Management Program), CSA CCM(Cloud Security Alliance-Cloud Controls Matrix) 등 클라우드와 관련된 보안 인증 스킴을 살펴보고 클라우드 서비스를 제공함에 있어 고려되어야 할 핵심 보안 고려사항을 제안하고자 한다.

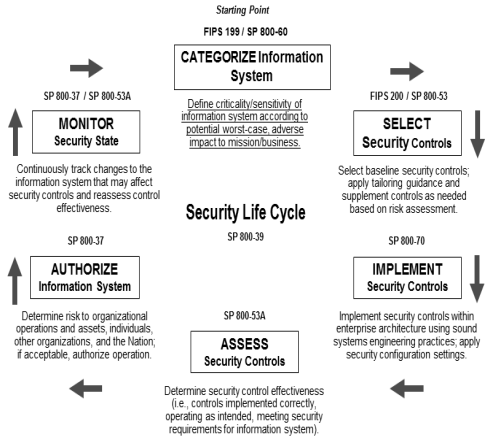
Ⅱ. 클라우드 관련 보안 인증스킴

2.1 FISMA

FISMA는 미국의 연방정보보안관리법으로서연방 정부의 보안 강화를 목적으로 효과적인 정보보안 통제를 위한 프레임워크를 설정하고 네트워크화된 컴퓨팅 환경에서 필요한 정보보안 리 스크를 관리감독하며, 정보와 정보시스템을 보호하기 위한 최소한의 통제 수단을 제공한다. FISMA에 대한 각 연방정부기관의 이해 제고와 수행의 용이성을 위하여 NIST(National Institute of Standards and Technology)는 SP(Special Publications) 800 시리즈 등 FISMA와 연관된 정보보호 표준과 지침들을 개발했다. NIST는 표준과 지침들을 전체적으로 통합하고 설명하기 위하여 위험관리체계(RMF, Risk Management Framework)를 개발했다. 위험관리 체계(RMF)는 위험을 관리하기 위한 활동들을 6단계의 구조 로 분류하여 제시하고 있다. [그림 1]은 RMF의 단계별 특징을 나타내고 있다.

초기에는 미정부가 FISMA를 통해 클라우드 서비스 보안에 대한 인증을 일부 수행하였으나, 현재는 FedRAMP를 통해 클라우드 서비스 보안 평가・인증을 수행하는 스킴을 추진하고 있다.

* 한국마이크로소프트 최고보안임원 이사(joshin@microsoft.com)



〔그림 1〕 NIST의 위험관리체계

2.2 ISO27001

국제 표준 정보 보호 관리 체계(ISMS: Information Security Management System) 인증으로 국제표준화기구(ISO)에서 제정한 국제 정보 보호 관리 체계 국제 규격. 현재 정보 보호 분야에서 가장 권위 있는 국제 인증 규격으로 지난 2005년 10월 영국 표준인 BS7799를 기반으로 만들어진 ISO 17799를 새로운 국제 표준인 ISO 27001로 승격, 위험 관리와 보안 정책 자산 분류 등 11개 분야 133개 항목에 대한 규격을 담고 있다. 통제항목은 정보보호 정책 2개, 조직 11개, 자산관리 5개, 인적자원 보안 9개, 물리적/환경적 보안 13개, 통신 및 운영관리 32개, 접근통제 25개, 정보시스템 도입, 개발, 유지 16개, 보안사고 관리 5개, 사업연속성 관리 5개, 법규준수 10개로 구성된다. 인증은 제3의 심사기관에 의해 수행되며, 문서심사와 본심사로 이뤄진다. 인증서는 통제항목에 대한 중 부적합 사항이 없으면 부여하게 되는데 지적사항이나 경 부적합 사항은 'Corrective Action Plan'을 작성하여 조치를 취하면 된다. 6개월 마다 사후심사와 3년 후 갱신심사를 받아야 한다.

2.3 FedRAMP

FedRAMP는 '11년 12월 국립표준기술연구소(NIST), 조달청(GSA), 국방부(DOD), 국토안보부(DHS), 연방 CIO협의회 등의 공동 작업을 통해 미 연방정부에 도입되는 클라우드 제품 및 서비스에 대한 보안성 평가·인증 및 지속적인 모니터링을 위해 도입된 프로그램으로서 미국은 기존 정부기관별로 수행하던 IT 시스템에 대한 보안성 평가를 클라우드에 한해 FedRAMP로 통합하여 정부 기관에 안전한 클라우드 컴퓨팅의 도입을 가속화시키고 있다.클라우드를 도입하려는 모든 미 정부기관은 반드시 적용해야 하며 다만 정부기관 내에 구축되는 프라이빗 클라우드는 제외된다. 인증 내용을 살펴보면 기존 정부기관 대상의 보안 통제 항목(367개 항목)에 클라우드 특화 항목(46개)을 추가하여 총 413개 항목에 대한 클라우드 서비스 보안 평가·인증을 수행하게 된다. 평가항목들은 접근 제어, 감사·책임, 보안 교육, 보안 평가·인증, 구성 관리(Configuration Management), 위기 대응 계획, 사고 대응 등으로 구성되어 있다. 아울러, 일관성 있는 보안 평가·인증 수행을 위해 전문 평가 대행기관(3PAO, Third Party Assessment Organization)을 선정하였는데 전문 평가 대행기관으로는 연방정부 1곳과 민간 기업 8곳이 선정되었으며, 대행기관을 통해 보안 평가 후, 평가 결과를 토대로 인증위원회에서 잠정인증 여부 결정하게 된다. 보안성 평가, 사후관리 등을 위한 기준 개발은 미 국립표준기술연구소(NIST)에서 담당하게 된다. 인증수준은 기존에 NIST가 정부기관의 정보보호 인증 수준에 따라 상(High), 중(Moderate), 하(Low) 등 3개 등급으로 구분하는 규정을 마련하였는데 여기서 중·하 등급에 해당되는 통제항목으로 수준을 정의하였다.

〔표 1〕 통제항목 비교

영향 수준	NIST 통제 항목	FedRAMP 추가 항목	총 통제 항목
하급	115	1	116
중급	252	45	297
소계	367	46	413

2.4 CSA-CCM

CSA-CCM은 비영리조직인 클라우드보안연합체가 클라우드 컴퓨팅에서 보안인증을 제공하고 베스트 프랙티스를 촉진시키기 위하여 BSI(British Standards Institution)와의 파트너쉽을 통해 개발한 통제항목으로 현재 v.1.2가 '11년 8월에 발표되었다. CSA의 개방형 인증프레임워크를 살펴보면 3단계의 인증수준을 가지고 있는데, 1단계 : 클라우드 서비스 제공자의 자기평

가, 2단계 : 제3기관에 의한 평가 (CCM 사용), 3단계 : 지속적인 모니터링 기반의 평가로 구성된다. CCM 항목은 컴플라이언스 6개, 데이터 거버넌스 8개, 보안설비 8개, 인적관리 3개, 정보보안 34개, 법규준수 2개, 운영관리 4개, 위험관리 5개, 공표관리5개, 사고복구 8개, 보안아키텍처 15개로 총 98개 항목으로 구성되어 있다. 인증은 제3자에 의한 독립적인 인증 프로세스를 거치게 되며 CCM 통제항목 기준에 의거하여 PDCA(Plan-Do-Check-Act) 접근방법을 사용하게 된다.

Ⅲ. 클라우드 보안 해결과제

클라우드 보안과 관련된 여러 가지 인증스킴들이 존재하지만 클라우드와 관련된 여러 보안 우려에 대해서는 아직 충분히 경험하거나 이해되지 못한 점들도 많다. 따라서, 클라우드 컴퓨팅의 이점이 제대로 실현되려면 특히 보안과 관련된 이점과 위험이 처음부터 충분히 강조되어야 할 것이다. 본 절에서는 클라우드 솔루션을 평가, 구현, 관리, 유지할 때 필요한 규정준수와 위험관리, 사용자 확인과 액세스 제어, 서비스 무결성, 종단점 무결성, 정보보호 등 5가지의 핵심 고려사항을 제안하고자 한다.

3.1 규정준수와 위험관리

클라우드를 사용할 때 관련된 여러 규정을 준수하는 것은 궁극적으로 사용자에게도 큰 책임이 있다. 규정 준수를 클라우드 서비스 공급자의 책임으로만 오해하는 경우를 종종 볼 수 있는데 이는 사실과 크게 다르다. 비유적으로 말하자면 도로교통에서 보행자와 시설물을 안전하게 보호하기 위해 자동차를 안전하게 운전해야 하는 책임은 운전자에게 있다. 물론 운전자의 의지에 따라 도로교통법을 준수할 수 있게 자동차를 설계, 제조할 책임은 제조사에 있지만 모든 안전운전을 제조사의 책임하에 둘 수는 없는 일이다. 여러 공급자가 제공하는 클라우드 서비스를 혼합하여 사용하는 경우 공급자의 투명성이 절대적으로 요구된다. 클라우드 공급자 입장에서는 서비스 경쟁력을 유지, 확대하기 위해 공개하기 힘든 요소들도 있게 마련이다. 그러나 사용자가 규정준수를 위해 올바른 판단을 내리기에 충분할 정도로 하드웨어 자산에 대한 물리적 보안, 적용하고 있는 보안 프로세스 등의 정보를 투명하게 공개할 필요가 있다. 사용자는 이러한 정보를 기반으로 위험도를 분석하여 자체적인 규정준수 프레임워크와 결합할 수 있다. 이 과정에서 필요에 따라 추가 정보를 위해 공급자와 협상하기도 해야 한다. 이를 위해서 사용자는 스스로 숙련된 위험관리팀을 조직, 운영하여야 한다. 만약에 발생할 수도 있는 정보유출 및 내부자 부정행위에 대응하여 디지털포렌식 정보감사를 고려하는 것도 필요하다. 디지털포렌식 검증 도구 활용을 통해서 클라우드 서비스의 보안상의 취약점을 분석하고 서비스를 제공하는 조직 내 정보보호의 관리체계를 강화함으로서 사용자들이 보다 안심하고 서비스를 활용할 수 있는 계기가 될 수 있을 것이다.

3.2 사용자 확인(AuthN)과 액세스 제어(AuthZ)

클라우드 기반의 서비스는 종종 여러 도메인을 넘나드는 협업을 필요로 한다. 소중한 자산에 접근할 가능성이 있는 서비스를 위한 사용자 확인 및 액세스 제어 시스템은 직접 확인 혹은 이에 준하는 수준의 강력한 프로세스와 견고하게 암호화된 신원정보를 사용하는 사용자정보 프레임워크에 기반하여야 한다. 클라우드가 확산되기 이전부터 AuthN과 AuthZ를 위한 여러 기술들이 개발되어 왔으며 사용자명/암호, X.509, Kerberos, SAML 등이 널리 사용되고 있다. 그러나 이들을 그대로 클라우드에 적용하기에는 몇 가지 문제점이 있다. 먼저 각각의 기술은 특정 시나리오에는 잘 적용되지만 다른 시나리오에는 적용하기 어려운 문제가 있다. 그 결과 채택된 기술에 따라 그 기술을 사용하는 서비스에도 제한사항이 그대로 반영되는 경우가 많다. 그러므로 서로 다른 요구사항을 가진 여러 도메인을 넘나드는 클라우드 서비스를 위한 AuthN/AuthZ 시스템은 특정 기술에 종속되지 않고 여러 기술의 상호운용이 가능한 체제를 기반으로 해야 한다. 또 다른 문제점은 프라이버시의 문제이다. 보안을 강화하기 위해서 사용자에게 필요 이상으로 많은 정보를 요구하다 보면 프라이버시를 침해할 수 있으며, 이는 규정준수를 어렵게 하기도 한다. 그러므로 정확히 필요한 정보만 사용하는 체제가 요구된다. 클레임-기반 ID(claims-based Identity)는 이러한 문제점들에 대한 근원적인 해결책을 제시한다. 이는 서비스와 ID를 효과적으로 분리하여 시나리오에 구애 받지 않는 보편적인 솔루션을 가능하게 하고, 기존의 여러 ID 기술을 수용할 수 있어서 서로 다른 기술의 상호운용을 가능하게 하며, 필요 이상의 정보 노출을 방지할 수 있

는 최신 기술과도 결합될 수 있는 등 여러 측면에서 클라우드 서비스에 적용하기에 용이하다. 클레임-기반 ID는 ID제공자, ID사용자, 서비스 사용자의 3자 사이의 정보 흐름을 기반으로 하고 있는데 이 가운데 ID제공자의 무결성이 절대적으로 중요하다. 그러므로 가능하다면 ID제공자 승인과 등급지정도 고려해볼 만 하다. 클레임-기반 ID는 클라우드 뿐만 아니라 기존의 자체보유 IT 환경에도 적용될 수 있으며 이는 IT 환경 전반에 걸쳐 보안과 데이터 무결성을 획기적으로 개선할 수 있을 것으로 기대된다.

3.3 서비스 무결성 (integrity)

서비스 무결성은 클라우드 공급자가 서비스의 개발 전 과정에서 보안을 반영하도록 하는 방법과, 개발된 서비스가 사용자가 원하는 정도의 신뢰성과 지원 수준을 만족하도록 운영하는 방법을 포함한다.

3.3.1 서비스 개발의 무결성

제품에 보안과 프라이버시가 반영되도록 하는 것은 어느 소프트웨어에나 필수적인 요구이며 클라우드도 예외가 아니다. 클라우드 공급자는 분명 높은 수준의 보안 전문지식을 보유하고 있겠지만 개발 및 유지보수의 각 단계마다 보안과 프라이버시를 결합하는 것 또한 매우 중요하다. 마이크로소프트는 보안 개발 주기(Security Development Lifecycle)를 사용하여 클라우드 컴퓨팅 환경 개발 전 과정, 즉 요구분석, 설계, 구현, 검증, 발매, 대응에 이르는 각 단계에 보안을 빈틈없이 결합하여 관리하고 있다.

클라우드 서비스 공급자를 평가할 때 공급자의 보안 개발 프로세스에 대한 구체적인 사항에 대해 질의할 필요가 있다. 또한 위협 모델(threat model)은 얼마나 자주 갱신되는지, 보안 대응팀이 얼마나 잘 작동하고 있는지, 보안 업데이트에 대해 사용자들이 제대로 공지를 받는지 등에 관한 지속적인 보안 노력에 대해서도 확인하여야 한다.

3.3.2 서비스 전달의 무결성

클라우드 공급자는 서비스 수준에 관한 정보를 제공할 때 보안에 관한 정보도 충실하게 제공하고, 사용자는 이를 근거로 제공받기를 원하는 서비스가 보안에 관한 요구사항을 만족하는가를 판단할 수 있어야 한다. 서비스 수준에 포함될 수 있는 대표적인 사항으로는 성능 관리, 필요에 따른 네트워크 및 이미지 포렌식 수행 등을 위한 구체적인 계획이 포함되어야 하며, 서비스 공급이 중단될 때를 대비한 고객 대응 연락처와 복구 프로세스 등도 포함되어야 한다. 서비스 수준 협약은 어떤 보안 모니터링과 감사 기능이 제공되는지, 이에 따르는 비용이 얼마인지 등에 관해 정의하여야 한다.

3.3.3 종단점 (endpoint) 무결성

클라우드 보안에 관해 논의할 때 공급자의 보안 품질과 관행 및 서비스 자체로 한정하는 경우가 종종 있다. 그러나 클라우드 서비스는 조직 내부에서, 혹은 PC나 휴대기기에서 시작(요청)되고 종료되므로 클라우드 외부 요소를 포함하는 전체 서비스 사슬을 고려하여야만 한다. 클라우드 서비스의 전반적인 신뢰도를 높이기 위해 온라인 ID 도용, 웹사이트 교차 스크립트 공격, 피싱 공격, 악의적인 소프트웨어 다운로드 등을 포함하는 위협으로부터 사용자를 보호할 수 있도록 전체 스펙트럼을 아우르는 보안 활동이 요구된다. 특히 여러 공급자로부터의 서비스를 혼용하여 사용하는 환경에서는 전체 기관에 걸쳐 서비스가 전달되고 소비되는 방법 및 이와 관련된 여러 종단점을 함께 고려하는 것이 중요하다.

3.3.4 정보보호

민감한 정보를 공격자로부터 보호하는 것은 클라우드 보안의 핵심 중 핵심이다. 공급자가 서비스를 관리하는 경우트랜잭션 전 과정을 통해 규정 준수를 보장하기 위해 액세스 제어를 활용할 수 있다. 그러나 이에 선행되어야 할 것은 민감성이나 기밀성을 기준으로 데이터를 분류하는 것이다. 분류 결과에 따라 어느 데이터를 어떤 클라우드에 배치하는 것이 더 안심이 되는지 판단할 필요가 있다. 공용 클라우드와 사설 클라우드는 근본 개념에 있어서는 유사하지만 데이터 배치 관점에서의 심리적 저항 수준은 매우 다르다. 기밀성이 중요한 민감한 데이터를 사설 클라우드에 배치함으로써 이러한 심리적 저항을 극복할 수 있다. 정보보호는 암호화와 권한 관리 등의 영구적인 보호와, 트랜잭션 처리 과정에서 이동 중인 데이터의 보호도 고려해야 한다. 정보보호는 기

존의 IT 환경에 비해 새로운 많은 이슈를 발생시키는데 대표적으로 데이터 주권(data sovereignty) 문제를 들 수 있다. 이는 클라우드에 보관된 데이터를 검열하거나 조회할 권리에 관한 문제인데 흔히 데이터센터의 위치한 지역적 관할(대표적으로는 국가 및 국경)과 연관되어 있다. 새로이 개발되는 일부 서비스들은 이러한 문제를 고려하여 데이터가 실제 저장될 물리적 위치를 명시할 수 있도록 시도하고 있다. 정보의 관리 및 제어 권한이 공급자에게 이양된 경우 정보에 접근하기 위한 ID와 인증체제를 누가 관리하는지, 백업 데이터는 어디에 보관되는지, 데이터 암호화는 지원되는지, 암호화로 인한 손실은 무엇인지 (특정 기능 사용 불가 등), 서비스 가입을 취소할 때 사용자 데이터는 안전하게 폐기되는지 등에 관해 충분히 이해하는 것이 중요하다.

Ⅳ. 결 론

본 논문에서는 클라우드 보안 인증 스킴을 살펴보고, 클라우드 솔루션을 평가, 구현, 관리, 유지할 때 필요한 규정준수와 위험관리, 사용자 확인과 액세스 제어, 서비스 무결성, 종단점 무결성, 정보보호 등 5가지의 핵심 고려사항을 제시하였다. 그러나 기본적으로 전제되어야 할 것은 클라우드 공급자들이 기존 IT 환경에 비해 현저히 높은 수준의 프로세스와 기술을 도입하고 월등히 많은 노력을 기울여 보안에 신경 쓰고 있다는 것이다. 그러므로 보안을 이유로 클라우드의 도입을 주저하기보다는 클라우드 시대에 어울리는 사고의 전환이 요구된다. 클라우드가 보다 높은 수준의 보안을 제공하고 있다고는 하지만 모든 클라우드 공급자가 동일한 수준의 보안을 제공하는 것은 아니다. 그러므로 클라우드 공급자는 서비스 개발, 운영 등을 위한 기술과 프로세스에 있어서 어떤 표준과 관행을 실현하고 있는지 명시적으로 투명하게 공개하고 이를 기반으로 사용자는 적합한 수준의 보안을 제공하는 공급자와 서비스를 선택하는 것이 중요하다. 또한 모든 데이터가 동일한 수준으로 민감한 기밀 데이터인 것은 아니므로 데이터 분류를 기초로 하여 적절한 제어 및 배치 모델을 선택하는 것도 클라우드 도입의 전략이 될 수 있을 것으로 보인다.

참고문헌

[1] NIST SP 800-30, Risk Management Guide for IT Systems, 2002. 7.

[2] NIST SP 800-37, Guide for the Security Certification and Accreditation of FIS, 2004. 5.

[3] NIST SP 800-53A, Guide for Assessing the Security Controls in FIS (second public draft, 2006. 5).

[4] NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, 2004. 6.

[5] NIST FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, 2004. 2.

[6] NIST FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, 2006. 2.

[7] GSA, “Ensuring secure cloud computing for the Federal Government”, 2012. 6.

[8] GCN, “FedRAMP aims to authorize 3 cloud providers by year's end”, 2012. 6.

[9] ISO/IEC 27001:2005 - Information technology - Security techniques - Information security management systems

[10] Cloud Security Alliance, Cloud Controls Matrix v1.2, 2011. 8.

〈著者紹介〉

신 종 회 (Jongwhoi Shin)
종신회원

1990년: 강원대학교, 전자공학 공학사
2002년: 고려대학교, 컴퓨터 공학 석사
2007년: 고려대학교, 컴퓨터 이학 박사
1994년~2001년: 한국전산원, 선임연구원
2002년~2012년: 한국인터넷진흥원, 개인정보안전관리팀장
2012년~현재: 한국마이크로소프트, 최고보안임원 이사
<관심분야> 클라우드 컴퓨팅 보안, 디지털 포렌식, 정보보호관리 및 거버넌스