정 보 보 호 학 회 지
제24권 제6호, 2014. 12

클라우드 컴퓨팅 환경의 식별 및 접근제어

장 은 영*

요 약

클라우드 컴퓨팅 서비스는 자원 공유와 가상화 기술 및 자원의 서비스화 등 기존 컴퓨팅 환경과 다른 특성으로 인해 클라우드 컴퓨팅 환경에 적합한 식별/접근제어 기술 및 보안 통제 사항이 요구된다. 그러므로 기존 컴퓨팅 자원을 클라우드 컴퓨팅 환경으로 변경하는 서비스 제공자나 클라우드 서비스로 이동하는 서비스 사용자는 특정한 보안 요건을 검토해야 한다. Cloud Security Alliance에서 배포한 Cloud Control Matrix와 ISO/IEC 27001을 비교 분석하여, 클라우드 컴퓨팅 환경에서 특별히 요구되는 식별 및 접근제어의 보안 통제 요건을 확인하였다. 또한, 주요 클라우드 컴퓨팅 서비스인 아마존의 AWS, 구글의 Google Cloud Platform과 VMware의 vCloud 서비스의 식별 및 접근제어 기술을 조사하였다. 이를 기반으로 클라우드 컴퓨팅 환경의 식별 및 접근제어 기술에서 필요한 보안 요건을 확인하였다.

Ⅰ. 서 론

클라우드 컴퓨팅은 컴퓨팅, 네트워크, 정보 및 스토리지 자원들을 가상화 기술을 이용하여 통합 및 분리하여 서비스, 애플리케이션, 정보 및 인프라를 사용하는 것을 말한다. 가상화 기술의 활용 및 활성화로 인해 일반적으로 동적 통합, 프로비저닝, 사용량 및 서비스 조절, 이동성 및 확장 등의 기능을 제공한다. 즉, 클라우드 컴퓨팅 환경은 기존 컴퓨팅 방식과 다르므로 기존 컴퓨팅 방식의 컴플라이언스 및 기술을 그대로 적용할 수 없다. 이에 CSA(Cloud Security Alliance)에서는 클라우드 컴퓨팅 영역에 대한 보안 지침(Security Guidance for Critical Areas of Focus in Cloud Computing) 및 CloudCERT, CCM(Cloud Control Matrix)등 다양한 가이드를 제시하고 있으며, 각 클라우드 컴퓨팅 벤더는 클라우드 컴퓨팅 서비스의 보안성을 유지하기 위한 보안 기술 및 거버넌스 등을 적용하고 있다.

본 논문에서는 클라우드 컴퓨팅 환경의 특성 중 자원의 통합, 공유, 서비스의 유연성과 확장성, 이동성을 제어하기 위해 중요한 역할을 하는 식별 및 접근제어 기술에서 기존 컴퓨팅 환경과 다르게 특별히 요구되는 보안 요구사항을 확인하고자 한다. 클라우드 컴퓨팅 환경의 통제 매트릭스인 CCM은 클라우드 컴퓨팅 환경에서 요구되는 통제 항목을 제시하고 있지만, 기존 컴퓨팅 환경과 비교하여 특별히 고려해야 하는 사항을 명시적으로 확인하기는 어렵다.

본 논문에서는 CCM을 ISO/IEC 27001:2005, ISO/IEC 27001:2013과 비교하여 클라우드 컴퓨팅 환경에서 특별히 요구되는 보안 통제 사항을 도출하였다. 또한, 주요 클라우드 컴퓨팅 서비스에 적용된 식별 및 접근제어의 보안 기술을 파악하였다. 이를 기반으로 클라우드 컴퓨팅의 식별 및 접근제어 기술의 보안 요구사항을 검토해 보고자한다.

Ⅱ. 관련 연구

2.1 클라우드 컴퓨팅 위협 및 보안

클라우드 컴퓨팅 서비스 모델은 비공개형(Private Cloud), 공개형(Public Cloud), 공동체형(Community Cloud)와 두 모델이 혼합된 하이브리드(Hybrid Cloud)의 형태로 제공된다. 클라우드 서비스가 제공되는 방식은 대부분 자산, 자원, 서비스 소유자의 관리나 보안 경계선의 위치를 기준으로 설명된다. 클라우드 서비스는 연결성, 정보 교환의 불규칙성, 동적인 특성 및 서비스 운영의 이동성의 특성을 가지고 있다. 이러한 특성은 기

* ㈜안랩 보안정책팀(eunyoung.jang@ahnlab.com, elishajev@gmail.com)

존의 정적인 보안 컨트롤로 대처하기 어렵기 때문에 서비스에 대한 경계선 재설정이나 서비스 영역에 대한 신뢰 약화되는 문제가 증가할 것이다. 그러므로 클라우드 서비스는 물리적 위치를 고려해야 하며, 그 서비스 사용자, 거버넌스, 보안성 및 정책/표준 준수 등을 고려해야 한다. 또한 애플리케이션, 정보, 서비스의 유형과 관리자 및 관리 방식, 규제에 대해 고려하는 것이 중요하다[1].

2.2 클라우드 컴퓨팅 통제 매트릭스

CSA(Cloud Security Alliance)에서는 클라우드 컴퓨팅의 보안 가이드인 CCM(Cloud Control Matrix)을 제공하였다. 벤더에게 기본적인 보안 원칙을 가이드하고 사용자가 클라우드 서비스 제공자의 보안 위험을 평가를 지원하기 위한 가이드이다. CCM v3.0.1은 ISO/IEC 27001:2005, 2013, ACIPA, BITS, COBIT, COPPA, HIPAA, ITAR, NIST SP 800-53, PCI DSS등 과 매핑되는 6개의 통제 영역과 133개의 통제로 구성되어 있다. CCM은 시스템의 구성과 클라우드 서비스 모델 등에 따라 통제항목을 적용 할 수 있다[2,3].

ISO/IEC 27001은 조직이 보안사고로부터의 사업연속성을 보장하기 위한 관리체계이며 전 세계 유일한 국제인증이다. 위험분석 접근법을 기반으로 정보관리체계(Information Security Management Model)를 수립, 이행, 운영, 감시, 검토, 유지 및 향상을 위한 전체적인 관리 시스템이다. ISO/IEC 27001:2005는 11개의 도메인과 133개 통제항목으로 구성되어 있으며, ISO/IEC 27001:2013은 14개의 도메인, 114개 통제 항목으로 구성되어 있다. ISO/IEC 27001:2013은 2005버전과 비교하여 아웃소싱에 대한 새로운 섹션, 써드 파티에 의존하는 조직들에 대한 사실 반영 및 조직의 ISMS 수행을 어떻게 잘 평가할 것인가를 강조하고 있다[4,5].

2.3 클라우드 컴퓨팅 환경의 접근제어

클라우드 컴퓨팅 환경은 IT 자원이 통합된 시스템 환경에서 유연성과 확장성을 보장하는 서비스를 제공한다. 그러나 클라우드 서비스 변경으로 인한 자원 이동 및 사용자 관리는 많은 절차가 요구된다. 이는 사업자가 제공하는 서비스가 표준화되지 않았기 때문이다.

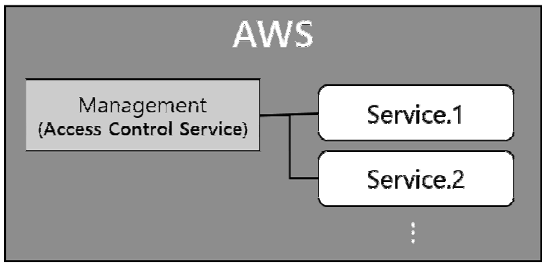
규칙기반의 CloudRBAC(Cloud Role-Based Access Control)은 클라우드 사업자가 제공하는 클라우드 서비스를 역할로 정의하고 모델링하여 서비스 변동에 따른 불필요한 관리 및 절차를 감소시킨다. 이와 같은 서비스 접근제어 기술은 서비스의 세부적인 속성 및 상세 값이 명시된 역할을 사용자에게 부여하고 그 역할에 따라 관리하며, 서비스 확장 요구에 따른 역할 변경이 자동으로 가능하다[6].

이 모델은 역할을 클라우드 서비스 역할, 사용자 역할과 관리자 역할로 구분한다. 역할마다 정책 설정 및 접근 권한 부여 방법이 달라 역할 충돌 및 의무 영역을 분리하여 효율적이고 보안적인 관리가 가능하다. 또한 규칙을 기반으로 역할 변동이 이루어지기 때문에 유동적인 클라우드 서비스를 보안을 보장하며 효율성 있게 할당 및 관리가 가능하다.

Ⅲ. 클라우드 서비스의 식별 및 접근제어 기술

클라우드 서비스에 적용된 식별 및 접근제어 기술을 파악하기 위해 주요 클라우드 서비스인 아마존의 AWS와 구글의 Google Cloud Platform 서비스, VMware의 vCloud를 조사하였다. 이와 같은 클라우드 서비스는 자원 사용의 효율성과 보안성을 위해 계정기반 접근제어, 네트워크 접근제어, 속성기반 접근제어, 데이터기반 접근제어 등을 적용하고 있다.

3.1 AWS의 IAM



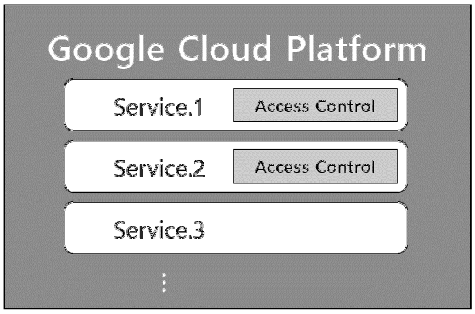
〔그림 1〕 클라우드 서비스와 IAM 서비스

Amazon의 AWS(Amazon Web Service)는 컴퓨팅, 스토리지, 데이터베이스, 분석, 애플리케이션 및 배포서비스의 클라우드 컴퓨팅 서비스를 제공한다. 아AWS 계정을 기반으로 사용자의 접근을 제어하기 위해 IAM(Identity and Access Management) 웹 서비스를

제공하고 있다. IAM은 Amazon에서 제공하는 모든 서비스와 무료로 연동이 가능하며, 서비스 특성에 따라 일부 기능이 제한된다.

IAM은 AWS 계정을 기반으로 사용자와 그룹을 생성하고 사용자 별 특정 보안 자격 할당 및 권한 제어를 할 수 있게 한다. 데이터 기반으로 사용자 접근과 보안 자격을 중앙 제어하며, 직무 및 역할 기반의 접근 제어와 IP, 포트, 프로토콜 기반의 네트워크 접근 제어를 제공한다. 또한, 자원 공유 및 중앙제어로 데이터 연속성 유지하고 자원 생성 영역 통제한다.

3.2. Google Cloud Platform의 접근제어 기술



〔그림 2〕 Google Cloud Platform 의 접근제어 기술

Google은 IaaS, PaaS 형태의 엔진, SaaS 형태의 저장소, 빅 데이터 서비스와 이외 다양한 서비스를 제공하고 있다. 각 서비스의 특성에 따라서 적절한 접근 제어 기술을 포함하고 있다.

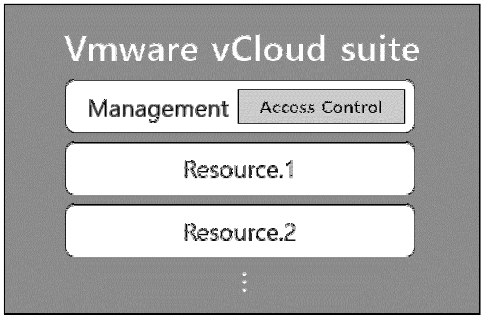
Google Compute Engine은 IaaS 서비스로 구글 인프라를 실행하는 가상 머신을 제공하여 대규모 컴퓨팅 클러스터를 쉽게 실행 할 수 있게 한다. Instance 단위로 접근 설정을 하는데, 파라미터가 인스턴스와 프로젝트, 쿼리 그리고 네트워킹 인터페이스이며 접근 설정 값을 요청한다. 자원 타입, 자원 아이디, 자원 명, 영역, 타겟 아이디, 상태, 시간, 위치 등의 값으로 응답하게 된다. 인스턴트는 요청/응답에 따라 쓰기-읽기 권한, 읽기 권한을 갖게 된다.

Google Cloud Storage는 구글 클라우드에 데이터를 제한 없이 저장할 수 있는 인터넷 서비스이다. 접근 제어를 위해 ACLs(Access Control Lists)와 Singed URLs(Query String Authentication)을 제공한다. 2가지 방법의 접근제어는 동시에 사용 가능하다.

ACLs는 구글 계정을 사용하여 접근 기간을 제한하지 않는다. 오브젝트와 버킷의 접근을 관리하는 메커니즘으로 다른 사용자와 오브젝트를 공유하고 버킷과 오브젝트에 접근하는 다른 사용자를 허가한다. ACLs는 범위 내의 권한을 할당하는 하나 이상의 엔트리를 포함한다. 권한은 오브젝트 나 버킷에서 수행 가능한 행동으로 읽기, 쓰기 등을 말하며, 범위는 권한을 할당받는 그룹이나 사용자를 말한다.

Signed URLs는 구글 계정을 사용하지 않고 제한된 기간 내에 사용 가능한 “valet-key”타입의 접근을 제공한다. 응용프로그램 별로 특정 로직을 사용하는 접근 제어로 자원을 읽고, 쓰고, 삭제하는 권한을 할당할 수 있다.

3.3. VMware vCloud Suite의 접근제어 기술



〔그림 3〕 VMware vCloud Suite의 접근제어 기술

VMware는 클라우드 데이터 센터, 인프라, 애플리케이션 가상화, 데스크톱 가상화 등의 서비스를 제공한다. VMware vCloud Suite은 소프트웨어 정의 데이터 센터 아키텍처를 기반으로 프라이빗 클라우드를 구축하고 관리하는 제품이다. 이 중 vCloud Director는 소프트웨어 정의 방식으로 가상화된 컴퓨팅, 네트워킹, 저장소 등의 가상 인프라 리소스를 가상 데이터 센터에 가상 데이터 센터에 풀링하고 이러한 리소스를 자동화된 카탈로그 기반 서비스로 사용자에게 노출하여 보안 다중 테넌트 클라우드를 구축할 수 있게 해 주는 소프트웨어이다.

vCloud Director는 RBAC 모델을 지원하여 유연한 사용자 권한 부여 기능을 제공한다. 예를 들어, 사용자의 서비스 제약사항 (디스크 쿼드, 서비스 사용기간, 임대 정책 등 서비스 수준에 따른 다양한 조건 등)을 기준

으로 다양한 권한을 설정하고 사용자의 역할과 조합한 정책을 바탕으로 접근 통제를 수행한다.

Ⅳ. 클라우드 컴퓨팅의 식별 및 접근제어 통제

클라우드 컴퓨팅 환경에서 특히 준수해야 하는 식별 및 접근제어 통제 사항을 확인하기 위해 CCM 중 IAM(Identify & Access Management)의 통제 항목을 ISO/IEC 270001 통제 항목의 비교 및 분석하였다. 기존 컴퓨팅 환경에서 지속적으로 요구되던 통제 사항을 삭제하고, 클라우드 컴퓨팅 환경에서 추가로 요구되는 통제 사항을 구분하였다.

〔표 1〕 CCM V3.0 IAM의 ISO/IEC 27001 매핑 항목

CCM V3.0	ISO/IEC 27001-2005	ISO/IEC 27001-2013
IAM-01	A.15.3.2	-
IAM-02	A.11.1.1 A.11.2.1, 4 A.11.4.1 A.11.5.2 A.11.6.1	A.9.1.1, 2 A.9.2,1, 2, 5 A.9.4.1
IAM-03	A.10.6.1 A.11.1.1 A.11.4.4 A.11.5.4	A.13.1.1 A.9.1.1 A.9.4.4
IAM-04	-	A.9.2
IAM-05	A.10.1.3	A.6.1.2
IAM-06	A.12.4.3 A.15.1.3	A.9.4.5 A.18.1.3
IAM-07	A.6.2.1 A.8.3.3 A.11.1.1 A.11.2.1, 4	A.9.1.1 A.9.2.1, 2, 5, 6
IAM-08	-	A.9.2 A.9.3.1 A.9.4.1~3, 5
IAM-09	A.11.2.1, 2 A.11.4.1, 2 A.11.6.1	A.9.1.2 A.9.2.1, 3 A.9.4.1
IAM-10	A.11.2.4	A.9.2.5
IAM-11	A.8.3.3 A.11.1.1 A.11.2.1, 2	A.9.1.1 A.9.2.1, 2, 3, 6
IAM-12	A.8.3.3 A.11.1.1 A.11.2.1, 3, 4 A.11.5.5	A.9.1.1 A.9.2.1, 2, 4, 5, 6 A.9.4.2
IAM-13	A.11.4.1, 4 A.11.5.4	A.9.2.1 A.9.4.4

- IAM01: Audit Tools Access

기존 시스템은 감사 툴의 접근이 남용 및 오용에 대한 보호가 요구되지만, 클라우드 환경에서는 상호작용하는 시스템의 감사 툴 간 로그 데이터에 대해 남용 및 오용이 방지되고 있는지 확인해야 한다.

- IAM02: Credential Lifecycle/Provision Management

직무 기반의 최소 권한 할당 규칙에 따라 사용자 계정 권한을 설정하고 권한 설정 절차 및 역할과 책임을 지원해야 한다. 또한, 제3자에 의한 멀티 테넌트 구조의 세션과 데이터 접근 세분화, 서비스 대 서비스 애플리케이션, 데이터와 세션 접근을 위한 인증, 정보처리 상호운용이 관리되어야 한다. 권한 철회 등을 통해 계정 자격증명 라이프 사이클이 관리되어야 하며, 클라우드 컴퓨팅의 법, 규칙 및 규정을 준수해야 한다.

- IAM03: Diagnostic/Configuration Ports Access

클라우드 컴퓨팅 환경에서는 네트워크와 애플리케이션의 접근을 제어해야 하며 이러한 요구사항에 대한 접근 제어 정책을 수립해야 한다. 즉, 클라우드 컴퓨팅 환경에서는 권한이 부여된 개인과 애플리케이션의 접근을 제한할 것을 요구한다.

- IAM04: Policies and Procedures

모든 사용자에 대한 식별 정보를 관리 및 저장하고 접근제어 레벨을 결정하는 정책 및 절차가 수립되어야 한다. 사용자 식별을 기반으로 네트워크 자원에 대한 접근제어 정책도 개발되어야 한다.

- IAM05: Segregation of Duties

기존 시스템은 비인가된 사용 오용 및 남용을 감소시키기 위해 책임과 의무 영역을 분리하지만, 클라우드 컴퓨팅 시스템은 사용자 역할의 충돌로 인한 비즈니스 위험을 고려하여 의무를 분리해야 한다. 이러한 정의를 통해 사용자 접근을 제한하고, 사용자 접근 정책과 절차 수립 및 기술 조치를 지원해야 한다.

- IAM06: Source Code Access Restriction

프로그램 소스코드의 접근 제한에서 애플리케이션,

프로그램과 오브젝트의 소스코드의 접근 제한으로 추가 통제한다. 또한, 기존 시스템은 기록이 손실 및 훼손 등에서 보호되어야 하지만, 클라우드 컴퓨팅 환경에서는 부여된 접근, 소스코드의 접근과 버전에 대한 기록을 유지해야 한다고 명시하고 있다.

• IAM07: Third Party Access

클라우드 컴퓨팅 환경에서는 써드 파티의 부적절한 접근의 영향을 검토, 모니터링 및 측정하기 위해 비즈니스 프로세스 내 위험 평가와 우선순위 정의해야 한다. 또한, 접근 권한 설정 전에 위험 분석에 의한 보완 통제가 수행되어야 한다.

• IAM08: Trusted Sources

비즈니스 요구에 의해 정의된 사용자를 대상으로 최소 권한 및 복제 제한 규칙에 기반하여 인가된 식별자에게 접근 권한을 부여하는 정책/절차 수립해야 한다.

• IAM09: User Access Authorization

데이터, 애플리케이션, 네트워크 서비스 등에 대한 권한 관리를 위해 사용자 등록 절차와 적절한 인증방법, 접근 제어 정책이 요구된다. 클라우드 컴퓨팅 시스템은 수립된 정책 및 절차 보다 조직의 관리가 우선시되어 사용자 접근 권한을 인가해야 한다. 제공자는 사용자 접근에 대해 고객에게 통지해야 하며, 고객 데이터가 서비스의 한 부분으로 사용되거나 고객이 공유 책임이 있을 때 사용자 접근에 대해 반드시 통지해야 한다.

• IAM10: User Access Reviews

수립된 사용자 접근 정책 및 절차에 따라 사용자 접근 권한 부여의 적합성을 검토해야 한다. 특히, 비즈니스 리더십이나 비즈니스 역할/기능에 따라 최소 권한의 적합성이 증명되어야 한다.

• IAM11: User Access Revocation

사용자 접근을 철회하는 서비스 대상이 데이터, 조직이 소유하거나 관리하는 물리적 가상 애플리케이션, 인프라 시스템, 네트워크 컴포넌트로 좀 더 세분화하여 명시되어 있다. 특히 고객 데이터가 서비스의 일부분으로 사용되거나 책임을 공유할 경우, 요청에 따라 제공자는 고객에게 변경 사항을 알려야 한다.

• IAM12: User ID Credentials

신원 신뢰 검증 및 서비스 대 서비스 애플리케이션과 정보처리의 상호운용 식별해야 한다. 철회를 통한 인스턴스화로 계정 자격증명 라이프 사이클을 관리해야 하며, 자격 증명 및 식별 저장(identity store) 최소화하거나 재사용해야 한다. 또한, 산업에 적절하고 규제력 있는 인증, 권한 부여 및 계정 규칙 준수해야 한다.

• IAM13: Utility Programs Access

유틸리티 프로그램 접근제어는 시스템 유틸리티 사용 제어 항목과 유사하나 네트워크 서비스의 사용 및 접근에 대한 제어와 논리적 접근 진단과 환경제어가 요구되는 가상머신 및 오브젝트를 통제해야 한다. 또한, 중요한 시스템에서 잠재적 중요한 시스템으로 통제 영역을 넓혔다.

Ⅴ. 결 론

클라우드 서비스의 식별 및 접근제어 기술은 기능을 나열 및 설명하는 수준으로 정보를 제공하고 있다. 또한, 기존 컴퓨팅 환경에서 클라우드 컴퓨팅 환경으로 변경하는 서비스 보안 관리자나 기존 서비스를 클라우드 서비스로 이동하려는 사용자가 특별히 고려해야하는 식별 및 접근제어의 보안 요건이 무엇인지 명시적으로 확인하는데 어려움이 있다.

본 논문에서는 클라우드 서비스의 식별 및 접근제어 기술을 조사하고, CCM과 ISO/IEC 27001의 비교 및 분석하여 클라우드 컴퓨팅 환경의 특정한 보안 요건을 확인하였다. 이를 통해 클라우드 서비스 사용자는 '클라우드 컴퓨팅 환경의 식별 및 접근제어 통제 사항'을 기준으로 식별 및 접근제어 기술을 위한 정책 및 절차, 관리 등이 제공되고 있는지 서비스 및 계약 사항을 확인할 수 있을 것이다. 또한, 보안성을 이미 만족한 기존 컴퓨팅 환경을 클라우드 컴퓨팅 환경으로 변경 했을 경우, 보안 관리자는 '클라우드 컴퓨팅 환경의 식별 및 접근제어 통제 사항'을 통해 추가 보안성을 점검 할 수 있을 것이다.

참 고 문 헌

[1] “Security Guidance for Critical Areas of Focus in Cloud Computing V3.0, Cloud Security Alliance, 2009 12

[2] “Cloud Control Matrix v3.0.1n ”, Cloud Security Alliance, 2014 7

[3] “Cloud Controls Matrix V1.0”, Cloud Security Alliance, 2010 4

[4] “ISO/IEC 27001:2005(E)(Information technology-Security techniques-A Information security management systems-Requirements)”, British Standards, 2005 10

[5] “ISO/IEC 27001:2013(E)(Information technology-Security techniques-A Information security management systems-Requirements)”, British Standards, 2013 10

[6] “Rule-based Cloud RBAC Model for Flexible Resource Allocation in Cloud Computing Service”, Eun-Young Jang, Hyung-Jong Kim, Information-An International Interdisciplinary Journal, Vol.13, No.5, 2010 9

〈저 자 소 개〉

장 은 영 (Jang Eun Young)
2008년 8월 : 서울여자대학교 공학사
2011년 8월 : 서울여자대학교 이학석사
2011년 6월~현재 : ㈜안랩 재직
관심분야 : 클라우드 컴퓨팅 보안, 개인정보보호. Common Criteria, 시뮬레이션