Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.2, Apr. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.2.411

안전한 클라우드 환경을 위한 클라우드 데이터 관리 시스템에 적용 가능한 보호프로파일에 관한 연구*

위 유 경,[1†] 곽 진[2‡]
[1]순천향대학교 정보보호학과 정보보호응용및보증연구실, [2]순천향대학교 정보보호학과

A Study on Cloud Database Management System Protection Profile for the Secure Cloud Environment*

Yukyeong Wi,[1†] Jin Kwak[2‡]
[1]ISAA Lab, Dept of Information Security Engineering, Soonchunhyang University,
[2]Dept of Information Security Engineering, Soonchunhyang University

요 약

클라우드 컴퓨팅이 활성화됨에 따라 다양한 클라우드 서비스가 대중적으로 보급되고, 그에 따른 클라우드 컴퓨팅 관련 제품들을 IT시장에서 쉽게 접할 수 있게 되었다. 일반적으로 IT제품군에 대해서 보안성 평가를 수행하고, 그 결과값을 통해 소비자에게 객관적인 지침으로 활용될 수 있는 국제 표준인 공통평가기준에서는 보안 제품군에 대한 보안목표명세서인 보호프로파일을 제공하고 있다. 하지만 현재 일반적인 IT제품군에 대한 보호프로파일은 존재하지만 클라우드 관련 제품군에 대해서는 보호프로파일이 존재하지 않아 보안성 평가를 위한 표준화된 방법이 없는 실정이다. 따라서 본 논문에서는 클라우드 데이터 관리 시스템 보호프로파일을 제안하고자 한다.

ABSTRACT

As cloud computing has enabled, a variety of cloud services has come into wide use. Thus, cloud computing products can be easily identified in the IT market. Common Criteria is international standards for security evaluation performed of IT products. In addition, Consumers can be used as a objective guideline for the evaluation results. And, it is a provides for protection profile(security target of security products). For general, IT products are providing the protection profile. However, for cloud-related products of protection profile is not being provided. Thus, about cloud security products, there is no way for evaluation. Therefore, in this paper, we propose protection profile on cloud database management system for the secure cloud environment in common criteria.

Keywords: Protection Profile, Cloud Datacenter, Availability, Access Control, TOE

I. 서 론

모바일 디바이스 시장의 성장과 콘텐츠 시장의 확대로 인해 관련 데이터가 급격하게 증가하게 됨에 따라 사용자가 필요로 하는 서버, 스토리지, 어플리케이션, SW 플랫폼 등의 각종 IT 자원을 구매하여 소유하지 않고 필요할 때마다 네트워크를 통해 서비스 형태로 이용하는 방식인 클라우드 컴퓨팅이 대중적으로

접수일(2013년 12월 17일), 수정일(2014년 2월 5일), 게재확정일(2014년 2월 7일)
* 이 논문은 2013년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2012-010886).
* 이 논문은 순천향대학교의 지원을 받아 수행된 연구임.
† 주저자, ykwi@sch.ac.kr
‡ 교신저자, jkwak@sch.ac.kr(Corresponding author)

보급되게 되었다.

최근의 클라우드 컴퓨팅 서비스는 다양한 디바이스를 통해 하나의 작업을 수행해도 언제 어디서나 원하는 시간과 장소에 구애받지 않고 연속된 작업을 수행하기 위한 연구가 진행되고 있는 추세이다. 이에 따라 원활한 데이터 동기화 서비스를 사용하기 위한 데이터센터를 구축하고 확장하는 등의 관심이 증가하고 있다. 하지만 일반적으로 데이터센터를 구축하기 위해서는 값비싼 하드웨어의 도입, 전력 소비량 등의 비용적인 측면과 노력의 양이 증가하는 문제점이 존재한다. 이와 같은 문제점을 해결하기 위해서 기존의 데이터센터 내에 클라우드 컴퓨팅의 개념을 도입하여 외부의 악의적인 요소로부터 하드웨어 및 스토리지를 보호하기 위한 클라우드 데이터센터의 중요성이 높아지고 있는 추세이다[1]. 그러나 클라우드 데이터센터는 다수의 스토리지가 집약되어 있어 권한이 없는 사용자의 무분별한 내부 스토리지 접근, 악의적인 데이터 무단 업로드 및 무단 삭제, 필터링 되지 않은 악의적인 데이터의 스토리지 저장으로 인한 서비스 가용성의 침해 등의 보안 위협이 존재한다. 따라서 클라우드 환경에서 데이터를 안전하게 관리하기 위해서는 다양한 보안 문제점이 해결되어야한다[2].

국제 공통평가기준 상호인정협정(CCRA)의 정책은 회원국가간 보안 기능성이 있는 IT 제품의 개발, 평가 또는 조달에 대한 지침으로 활용될 수 있는 공통평가기준(CC: Common Criteria)으로 인증된 제품을 동일한 수준으로 상호간에 인정한다는 것을 의미한다[3]. 이러한 공통평가기준에서는 일반적으로 보호프로파일(PP : Protection Profile)이라는 보안제품군에 대한 보안목표명세서(ST : Security Target)를 제공하고 있는데 이는 독립적인 보안성 평가의 결과들을 비교할 수 있도록 하는 국제 표준이다. 보호프로파일은 정보보호 시스템 사용 환경에서 보안 문제를 해결하기 위해 공통평가기준 내에 기술되어 있는 보안기능에서 선택하여 작성한 정보보호 제품군 · 시스템별 보안기능요구사항을 명시하고 있다.[4, 5]. 하지만 현재 공통평가기준에서는 클라우드 제품군에 대한 보호프로파일을 제공하지 않아 국내·외의 국가별로 클라우드 보안 정책 및 가이드라인을 제시하고 그에 따른 보안 통제항목을 설정하여 준수하고 있다. 따라서 각국의 정보보호 평가 및 인증체계의 기준이 서로 상이하여 클라우드 제품군에 대해서 보안성을 평가하기 위한 공통적인 평가 방법이 정립되지 않은 현실이다.

따라서 본 논문에서는 클라우드 환경에서 데이터센터에 데이터를 저장 및 관리할 때 발생하는 보안문제를 정의하고, 이를 기반으로 보안 목적 및 보안기능요구사항을 도출하여 클라우드 데이터 관리 시스템의 보안성 평가 시에 활용 가능한 보호프로파일을 제안하고자 한다. 추가적으로 국내·외의 클라우드 인증제도 및 가이드라인과 비교·분석을 통하여 본 논문에서 제안하는 보호프로파일의 적합성을 검증하고자 한다.

II. 국내·외 클라우드 인증제도 및 가이드라인

다양한 클라우드 제품 및 서비스가 대중적으로 보급되었지만 클라우드 제품군에 대한 평가 및 인증체계가 정립되지 않아 세계 각국의 기준이 상이하여 객관적인 보안성 평가의 기준이 없는 실정이다. 따라서 본 장에서는 국내·외 각국의 클라우드 인증제도 및 가이드라인을 비교를 통해 분석하고자 한다.

2.1 국외 가이드라인

2.1.1가트너 보고서

미국의 IT분야의 리서치 및 자문 회사인 가트너(Gartner, Inc.)는 2008년 6월에 클라우드 컴퓨팅의 보안 위험 평가(Assessing the Security Risks of Cloud Computing)라는 지정 보고서를 발표했다. 해당 보고서는 클라우드 컴퓨팅에 보안 위험이 존재하기 때문에, 사용자와 기업은 클라우드 서비스를 사용하기 전에 다음과 같은 7가지 보안문제에 대해서 유의할 필요가 있다고 지적하고 있다. 즉, 사용자가 클라우드 공급업체를 선택하기 전에 확인해야 하는 사항이다[2, 6, 7, 8].

• 사용자 권한에 따른 접근

아웃소싱된 서비스의 경우에는 "물리적, 논리적, 인력 제어"가 불가능하므로 기업 외부에서 처리되는 중요한 데이터(Sensitive Data)는 위협에 노출될 가능성이 높다. 그러므로 데이터를 관리하는 관리자로부터 정보를 최대한 제공받아야 하며 제공자에게 권한 및 접근 제어에 대한 통제를 요청해야 한다.

• 규정의 준수

서비스 제공자가 안정적인 클라우드 서비스를 제공하여도 고객은 자신의 데이터 보안과 무결성에 대해

최종적인 책임이 있다. 일반적으로 서비스 제공자는 외부 감사 및 보안 인증을 받게 된다. 하지만 해당 외부 감사를 거부하는 클라우드 서비스 제공 업체는 가장 평범한 기능만 이용할 수밖에 없다는 것에 유의해야 한다.

• 데이터의 위치

클라우드 서비스를 사용할 때 대다수의 사용자가 자신의 데이터가 어느 곳에 저장되어 있는지 알지 못한다. 심지어 어느 국가에 있는지도 알지 못 한다. 서비스 제공자의 특정한 사법 관할이 포함되는 범위에서 데이터를 보관 및 처리하고 있는지 여부와 고객의 거점이 있는 특정 관할에 개인정보보호 요구사항을 준수하는 계약상의 의무에 대해 실시할 수 있는 여부를 확인할 필요가 있다.

• 데이터의 분리여부 파악

클라우드 환경에서의 데이터는 일반적으로 다른 사용자들과 공유되는 환경에 보관된다. 하지만 암호화는 효과적인 방법이지만 최적의 보안 방법은 아니다. 이에 따라 저장된 데이터를 어떤 방식으로 분리하고 있는지를 파악하고 있어야 한다. 또한 클라우드 서비스 제공자는 전문가들에 의해 암호화 체계를 설계하고, 이를 경험이 풍부한 전문가에게 검증을 받고 있다는 확증을 제공하여야 한다.

• 데이터 복구

사용자가 자신의 데이터가 어느 곳에 보관되어 있는지 알 수 없어도 클라우드 공급자는 사용자에게 보안 사고가 발생하는 경우에 데이터와 서비스에 어떤 피해가 있는지 알릴 의무가 있다.

• 위법행위에 대한 조사지원

클라우드 컴퓨팅에서는 부적절한 행위 및 비합법적인 활동을 조사하는 것이 어렵다. 이는 여러 사용자를 위한 기록과 데이터가 호스트와 데이터센터의 설정 변경과 공통된 위치에 있을 가능성이 높기 때문이다. 따라서 특정한 조사에 협력한다고 하는 계약상의 의무를 얻을 수 없는 한 조사 및 복구를 바라는 요구는 실현되지 않을 가능성이 높다.

• 장기적인 실행 가능성

사용자가 클라우드 컴퓨팅 서비스 업체를 선택할 때 파산 또는 대기업에 인수·합병 될 가능성이 적은 업체를 선택하는 것이 이상적이다. 만약에 서비스가 중단되는 사태가 발생하더라도 자사의 데이터를 안정적으로 서비스가 가능하도록 해야 한다. 이 때 사용자는 데이터를 어떻게 반환받고, 연속적인 서비스가 가능한 지의 여부를 확인할 필요가 있다.

2.1.2 CSA(Cloud Security Alliance) 가이드라인

글로벌 IT업계의 정상들의 비영리 단체(NPO)인 클라우드 보안 협회(CSA)는 2012년 12월에 클라우드 컴퓨팅의 중점 분야에 대한 보안 가이드라인(Security Guidance for Critical Areas of Focus in Cloud Computing V2.1)을 발표했다. 해당 가이드라인에서는 클라우드 컴퓨팅의 사용자 기업 및 서비스 공급자에 대해 13가지의 주요 전략 분야 및 문제점을 정리하고 있다. 다음은 CSA에서 발표한 가이드라인을 13개의 항목으로 분류한 세부사항이다 [7, 9, 10, 11].

• 클라우드 컴퓨팅 구조적 프레임워크

클라우드 컴퓨팅의 특성, 서비스 제공 모델, 이익활용과 소비 형태를 분류하여 그에 따른 클라우드 컴퓨팅의 정의를 선언하고 있다. 또한 SaaS, IaaS, PaaS 3개의 서비스 모델의 확장성(개방성)과 보안책임의 이율배반을 명심하는 것이 중요하다고 지적하고 있다.

• 통제 및 전사적 위협 관리

클라우드로 절감되는 비용은 보안 강화에 충당해야 하며, 서비스 제공자는 제 3의 기관으로부터 위험도 평가를 받아 그 결과를 사용자에게 공개해야 한다. 또한 공급 업체의 재정안전성을 파악해야 한다.

• 법적, 전자적 증거수집

서비스 제공자가 준수하는 법률과 사용자를 통제하는 법률 사이에 입장차이가 있다는 것을 명심해야 한다. 이는 법률 정보규제에 대한 공급자의 대응을 파악해 두는 것을 뜻한다. 또한 국내가 아닌 다른 나라에서 서버를 운영함으로 인한 데이터 전송의 가능성을 확인하고 필요에 따라 이를 금지하는 계약이 필요하다. 추가적으로 서비스 제공자와 사용자간의 계약상에서 서면으로 보안 문제의 해결을 도모하는 서비스 수준 계약(SLA) 조항을 포함시키는 것이 중요하다.

• 규정준수 및 감사

규정을 준수하는 요구사항을 확인하기 위하여 데이터 및 시스템을 체계적으로 분류한다. 특히 데이터의 복사본과 데이터의 저장위치 등을 인식하고 있는 것이 중요하다. 또한 개인정보 영향 평가와 같은 외부에서 행하여지는 위험 평가를 이용한다.

• 정보 생명주기 관리

서비스 제공업체의 데이터 프라이버시 규정을 인식하는 것이 중요하다. 데이터 무결성 및 데이터 손상에 대한 공급자의 정책과 그에 따른 처리과정을 인지해야 한다. 또한 정기적인 백업 및 복구 테스트 실시하여 사전에 정보의 생명주기를 관리하는데 그 목적이 있다.

• 이동성 및 상호호환성

SaaS는 정기적인 데이터 추출 및 백업을 실시하고, IaaS는 VM이미지를 추출하여 런타임 환경에서 어플리케이션을 활용하는 방향으로 한다. 또한 PaaS는 주의를 필요로 하는 어플리케이션 개발 기술이 필요하다. 서비스의 시장이 급속하게 발전하고 있으며 그에 따른 개발 환경도 다양해짐에 따라 이동성과 상호운영성에 유의해야 한다.

• 전통적 보안, 업무 연속성 및 재난에 대한 복구

클라우드 환경에서는 데이터가 스토리지에 집중되기 때문에 서비스 제공자의 내부에서 위협이 문제가 될 가능성이 크다. 서비스 제공자는 가장 엄격한 수단의 보안요구사항을 보안 기준으로 적용한다. 또한 업무의 분리를 철저히 하고 업무 이행에 필요한 최소한의 정보만 열람할 수 있도록 한다.

• 데이터센터 운영

사용자는 서비스 제공자가 클라우드 컴퓨팅의 기본 특성을 파악하여 문제없이 실행 가능한지 여부를 파악해야 한다. 또한 기술 아키텍처와 인프라가 어떻게 SLA를 만족하는지 파악해야한다.

• 사고대응, 경고, 개선

데이터 유출 규제로 인한 비공개로 분류되는 데이터는 항상 암호화를 수행하고 사고가 발생할 위험 가능성을 낮춰야 한다. 또한 다수의 사용자를 대상으로 하는 클라우드 서비스 제공자에게 보안 침해 사고가 발생할 시에 적절한 분석 대응 체계를 갖춰야 한다.

• 애플리케이션 보안

어플리케이션의 비밀 키의 관리 및 보호를 철저하게 해야 한다. 또한 위협원에 대한 신뢰된 모델의 업데이트, 클라우드 환경의 평가 도구 업데이트, 어플리케이션 보안 아키텍처 변화를 인프라 개발과 같은 소프트웨어 개발주기(SDLC)의 보안이 중요하다.

• 암호화 및 키 관리

암호화는 데이터의 저장과 서비스를 분리하는 것으로써 클라우드 네트워크 내에서 암호화하지 않는 데이터를 보관하는 것은 데이터의 "유출"로 간주된다. 또한 백업을 관리하지 않는 어플리케이션 공급자가 백업 데이터를 보관할 때 반드시 데이터를 암호화해야 한다. 추가적으로 업계표준과 정부기준을 준수하는 암호화 규정을 사용하는지 확인해야 한다.

• 아이덴티티 및 접근관리

강력한 통합 ID 아키텍처 서비스를 통해 클라우드 환경에서 효율적인 ID 관리가 요구된다. 따라서 SAML, WS-Federation, Liberty ID-FF 등의 연방정부 표준의 이용을 권고하고 있다. 서비스 제공자가 사용자의 회사 정책보다 강도 높은 사용자 인증 및 암호 정책을 보유하고 있는지 확인해야 한다.

• 가상화

가상화 운영체제는 제 3의 보안기술로 강화시켜 계층화된 보안 관리를 수행하여 기존의 플랫폼의 의존도를 줄여야 한다. 가상화는 어플리케이션의 불안정성을 최소화하여 복구를 단순화하는 메모리 영역의 개선하는 등 보안상의 이점이 있다. VM플랫폼에서 가상의 이미지를 생성할 때 보안상의 취약점이 존재하기 때문에 기본적으로 보안 강화가 필요하다. 따라서 관리자의 가상화 운영체제 사용과 관리가 매우 중요하다.

2.1.3 ENISA(European Network and Information Security Agency) 가이드라인

EU의 사이버 보안 담당 기관인 유럽정보보호진흥원(ENISA)에서 2009년 11월에 Cloud Computing : Benefits, Risks and Recommendations for Information Security라는 가이드라인을 발표하였다. 해당 가이드라인에서는 클라우드 서비스의 기술적, 정책적, 법적, 일반적 위협의 4가지 영역으로 분류하고, 세부적으로 35개

항목의 주요한 보안 위협으로 구분하여 클라우드에 대한 모든 보안과 프라이버시 문제에 대해서 독립적이고, 심층적인 분석 및 위험 평가 절차를 제시하고 있다. 또한 ENISA에서는 다음의 12개의 정보보증 요구사항을 제시하여 클라우드에 특화된 취약점 및 자산을 분류하고 있다[2, 12, 13, 14].

- 인적보안
- 공급망 보증
- 운영 보안
- 식별 및 접근 관리
- 자산 관리
- 데이터와 서비스 이식성
- 업무 연속성 관리
- 물리적 보안
- 환경 통제
- 법규 요구사항
- 법규 권고사항
- 유럽 위원회의 법규 권고사항

2.2 국내 인증제도 및 안내서

2.2.1 KISA 클라우드 서비스 정보보호 안내서

국내의 인터넷 및 정보보호 정책관련 정부기관인 한국인터넷진흥원(KISA)에서 2011년 10월에 '클라우드 서비스 정보보호 안내서'를 발행하였다. 해당 안내서에서는 클라우드 서비스 모델과 주요 기능들을 소개하고 있다. 또한 향후 예상되는 신규 보안 위협 및 보안 취약점 등을 분석하고 클라우드 서비스 제공자와 이용자를 대상으로 보안 이슈 및 정보보호 고려사항 등을 제시하고 있다[14, 15].

다음은 '클라우드 서비스 정보보호 안내서'에서 제시하고 있는 클라우드 서비스 제공자의 관리적, 기술적 정보보호 고려사항이다.

- 정보보호정책 및 약관 수립

현재 관련 법률 및 규정으로는 침해사고 발생에 따른 보안책임에 대하여 명확하게 판단할 수 있는 근거가 없어 법적논쟁이 우려된다. 따라서 서비스 제공자는 클라우드 서비스와 관련된 이용 주제를 세분화하여 각 주체별 역할, 의무 등을 정보보호정책 및 이용약관 등에 명확히 명시해야 한다.

- 정보보호조직 구성·운영 및 인력 보안

서비스 제공자는 이용 주체별 역할과 보안책임을 분리 및 정의하고 전체 조직의 사업목표와 업무절차 등을 고려한 정보보호전략을 수립하여 정보보호조직을 구성 및 운영해야 한다. 정보보호전약 수립과 이행에는 개인, 기업 이용자의 보안 요구사항을 반영해야 하며, 개인정보 암호화 저장과 같은 법적·정책적 보안조치가 적용될 수 있도록 해야 한다.

- 자산분류 및 통제

서비스 제공자는 이용자가 소유한 IT 자원을 효율적으로 이용할 수 있도록 데이터 유출 및 노출을 방지하기 위해 해당 자산을 정확히 파악해야 한다. 또한 자산의 특성과 중요도에 따라 적절한 통제 방안을 마련하기 위해 식별 및 분류 작업을 정확히 수행해야 한다.

- 비상대응체계 구축

클라우드 서비스에서 정보의 중앙 집중화로 인해 발생한 침해사고는 연계된 모든 서비스에 치명적인 영향을 미칠 수 있다. 따라서 침해사고 대응 및 관리를 신속하게 하기 위해서 내부 보안관제 기준에 의거하여 비상대응체계를 구축해야 한다.

- 서비스 연속성 확보

클라우드 서비스는 구성방법에 따라 지리적으로는 분산된 환경, 업체에서 제공하는 장비에 따라서 다양한 IT 인프라로 구현할 수 있다. 이것은 시스템 관리자가 예측하기 어려운 사고로 이어질 가능성이 높다는 것을 의미한다. 이에 따라 발생할 피해와 손실은 이용자뿐만이 아니라 연계된 모든 서비스에 영향을 미칠 수 있다. 따라서 서비스 제공자는 피해 확산을 방지하고 손실을 최소화하기 위해 시스템 가용성 및 서비스 연속성 확보대책을 마련해야 한다.

- 관련 법률 및 제도의 준수

서비스 제공자는 서비스를 제공하는 영역의 국가 및 기관에서 요구하는 관련 법률 및 제도를 준수하기 위해 변경사항을 인지하고 신속히 정책에 반영해야 하며, 관련 법·제도에 대한 준거성 확보를 위해 대응방안을 마련해야 한다.

- 네트워크 보안

클라우드 서비스에서는 서비스 이용자의 모든 정보와 이용자가 임대한 IT 자원이 인터넷 환경을 통해 제

공되므로 보안이 강화된 네트워크 구축이 요구된다. 특히, 서비스 제공자는 지리적으로 분리된 다수의 데이터 처리 서버의 운영에 따른 안전한 데이터 송·수신을 위한 통신 암호화를 적용하고, 네트워크 서비스거부공격 등에 대한 대응방안을 마련해야 한다.

• 시스템 및 가상화 보안

서비스 제공자는 가상화 기술 안에서 IT 자원을 통합·재배치하여 활용성을 극대화하기 때문에 운영비용 절감 및 공간 절약의 효과를 기대할 수 있다. 따라서 이용자의 데이터가 손실 또는 위·변조되어 서비스 이용에 제한을 받지 않도록 무결성을 보장해야 한다.

• 데이터센터 구축 및 이용 조건

클라우드 서비스는 구성에 따라 지리적으로 분리된 다수의 데이터센터를 통해 데이터를 처리한다. 따라서 서비스 제공자는 데이터센터를 특별한 보호가 필요한 보호대상 시설로 지정하고, 안전하게 관리해야 한다. 안전한 데이터센터를 구축하기 위해 안전한 위치 선정 및 내부 설비 보호를 위한 장비를 마련하고 출입 통제를 철저하게 관리해야 한다.

• 이용자 데이터 저장 및 관리

클라우드 서비스 제공자는 이용자의 안정적인 서비스 접속 및 이용을 보장하기 위해 서비스 이용에 따라 생성된 이용자 데이터를 안전하게 저장 및 관리해야 한다. 이용자 데이터는 데이터의 기밀수준에 따라 암호화하여 안전하게 전송한 후 저장 및 관리해야 하며 주기적으로 백업해야 한다.

• 사용자 인증 및 접근제어

서비스 제공자는 IT 자원에 접근이 허가된 이용자만이 서비스에 접속할 수 있도록 보장해야 한다. 따라서 서비스 이용자의 제한된 영역에 대한 접근 시도와 같은 부적절한 행위에 대한 보안관제 메커니즘을 마련해야 한다.

2.2.2 클라우드 서비스 인증

2012년 2월에 방송통신위원회 산하 한국클라우드서비스협회(KCSA)가 정부의 “클라우드 컴퓨팅 확산 및 경쟁력 강화 전략”의 일환으로 시작된 ‘클라우드 서비스 인증제도’를 시작하게 되었다. 이는 클라우드 업체가 제공하는 서비스를 평가하여 일정수준 이상의 체계 및 절차를 확보하여 인증평가기준에 합격한 서비스에 대하여 인증을 부여한다. 또한 클라우드 인증을 획득한 서비스 중에서 99.5% 이상의 가용성을 이용약관 및 서비스수준협약을 통해 보장하며, 그에 관련하여 글로벌 주요기업 수준의 손해배상액을 제시하고, ‘정보통신망이용촉진및정보보호등에관한법률’ 제47조에 따라 정보보호관리체계 인증을 받는 조건들을 모두 만족하는 서비스에 한해서 ‘클라우드 서비스 우수 SLA 인증’을 부여한다.

클라우드 서비스 인증의 심사항목은 다음과 같이 크게 가용성, 확장성, 성능, 데이터 관리, 보안, 서비스 지속성, 서비스 지원의 7개 항목과 40개의 세부항목으로 구성되어 있다[2, 14].

• 가용성

신청기관은 클라우드 서비스를 약정된 내용에 따라 상시적으로 제공하기 위해 제반 조치를 하여야 한다.

• 확장성

클라우드 서비스 제공자는 클라우드 서비스 수요에 유연하게 자원을 확장하여 제공할 수 있도록 필요한 정책, 인적 물적 자원 등을 갖추어야 한다.

• 성능

클라우드 서비스 제공자는 서비스의 품질(속도)을 보장하기 위해 적절한 성능을 유지하여야 한다. 이를 위해 필요한 정책, 인적 물적 자원 등을 갖추어야 한다.

• 데이터 관리

클라우드 서비스 제공자는 클라우드 서비스 이용자의 데이터를 안전하게 보호/관리하기 위해 필요한 정책 및 인적/물적 자원 등을 갖추어야 한다.

• 보안

조직의 보안을 효과적으로 구현하기 위해 관리체계를 수립하여야 한다. 또한 조직의 물리적 시설 및 설비를 보호하기 위해 물리적 보호 방안이 마련되어야 한다. 또한 다양한 취약성을 분석하고 그에 대한 적절한 대책을 마련하고 적용하여야 한다.

• 서비스 지속성

이용자가 믿고 클라우드 서비스를 이용할 수 있도록 사업자는 인적・물적 기반을 확보하고 이를 관리하여야 한다.

• 서비스 지원

클라우드 서비스 제공자는 이용자의 서비스 만족도를 제고하기 위해 각종 기술지원, 제공방식의 다양성, 수준의 보장 등 지원 체계를 갖추어야 한다.

Table 1. Analysis of domestic and foreign cloud certification system and guideline

	Gartner	CSA	ENISA	KISA	KCSA
Availability	○	○	○	○	○
Auditing/ Monitoring	○	○	○	○	○
Data security	○	○	○	○	○
Security policy	○	○	○	○	
Authentication/ access control	○	○	○	○	
Intrusion response	○	○	○	○	○
System Security		○	○	○	○
Physical Security			○	○	○
Virtualization environment		○		○	
etc.					

III. 클라우드 데이터 관리 시스템 보호프로파일

현재 '네트워크 침입방지시스템', '가상사설망', '통합 보안관리시스템' 등의 일반적인 IT제품군에 대한 보호프로파일은 존재하고 있으나, 클라우드 제품군에 대한 보호프로파일이 존재하지 않아 클라우드 컴퓨팅 관련 제품군의 보안성의 척도를 평가하기 위해 기존의 보호프로파일을 적용하기에는 다소 무리가 있다. 따라서 본 장에서는 클라우드 데이터 관리 시스템에 적용 가능한 보호프로파일을 제안한다.

최근 클라우드 컴퓨팅은 사용자가 다양한 디바이스로 하나의 작업을 수행해도 언제 어디서나 해당 작업의 연속성을 높일 수 있는 서비스가 제공되고 있다. 따라서 자원을 빌려서 사용하는 기존의 가상화 기술 중심에서 데이터 관리 및 공유 중심의 서비스로 이동하고 있다. 이에 따라 클라우드 데이터센터에 대한 중요성이 증가하게 되었다. 따라서 본 논문에서 다양한 클라우드 제품군 중에서도 클라우드 데이터센터의 스토리지 중심으로 TOE(Target of Evaluation)의 범위를 설정하여 서술한다.

클라우드 데이터 관리 시스템 보호프로파일의 제안 절차는 정보보호 시스템 공통평가기준에서 보호프로파일 개발 시 보안 요구사항을 도출하는 방법론을 준용하며, 일부 약어 및 명확한 의미 전달을 위해 사용된 표기법, 형태, 작성규칙은 공통평가기준을 따른다[14, 16].

3.1 TOE 개요

본 논문에서 제안한 보호프로파일은 클라우드 환경에서 외부 네트워크의 침해공격 및 데이터센터 내부의 데이터 유출 등의 공격으로부터 데이터센터의 스토리지를 보호하기 위한 수단으로서 사용되는 클라우드 데이터 관리 시스템의 보안기능요구사항을 정의한다.

TOE는 클라우드 데이터센터에서 데이터를 안전하고 효율적으로 관리 및 공유하기 위한 데이터 관리 시스템을 의미한다.

3.1.1 TOE 운영환경

클라우드 데이터센터는 안정적인 인터넷 연결 회선 및 전력공급, 외부 재해 요소로부터 컴퓨터 및 스토리지 등을 보호하기 위해 설립 및 운영되는 데이터센터 내에 클라우드 컴퓨팅의 개념을 도입하여 기존 데이터센터의 IT자원으로 퍼블릭 클라우드, 데스크톱 가상화 등의 클라우드 방식을 서비스할 때 기반이 되는 데이터센터를 말한다. 즉, 클라우드 환경은 데이터와 IT 인프라가 기업 내부에 존재하지 않고, 외부 클라우드 데이터센터에 저장하게 된다. 최근 들어 다수의 클라우드 서비스 공급자들은 외부 데이터센터를 설립하여 운용하고 있는 추세이다.

다음의 Fig.1.은 클라우드 환경에서 TOE가 설치 및 운영되는 환경을 나타낸다. TOE는 물리적으로 독립적인 클라우드 데이터센터와 데이터센터를 운영하기 위한 서버로 구성된다.

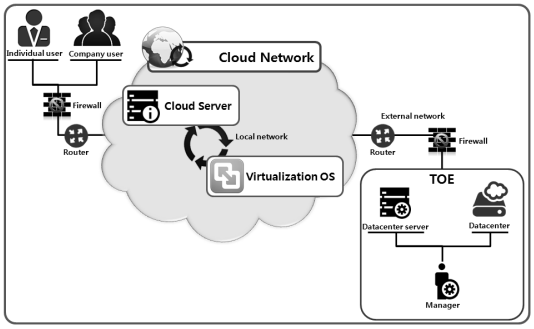

Fig.1. TOE operational environment

TOE는 인가받은 다수의 사용자가 접근하여 데이터를 업로드 및 사용자간에 서로 공유할 수 있도록 하는 시스템이다.

TOE와 TOE를 운영하는 서버 사이에 송수신되는 메시지는 보호되어야 하며, 송수신되는 메시지는 사용자의 데이터 또는 TSF(TOE Security Function)가 될 수 있다.

TOE를 사용하는 사용자는 TOE의 보안정책을 관리하는 인가된 관리자와 TOE내부의 관리되고 공유되는 데이터를 사용하는 일반적인 사용자로 구분된다.

TOE는 운영환경에 따라 클라우드 환경에 맞게 가상화 서버에 의해 운영될 수 있다.

TOE가 보호하고자하는 주요 자산은 조직이 관리하고 있는 사용자의 데이터를 의미한다. 또한, TOE 자체와 인증 데이터, 보안속성, 프로세스 등의 TSF 데이터 역시 보호해야 하는 부가적인 자산이다.

따라서 클라우드 환경은 TOE의 안전한 운영을 위해 신뢰된 관리자와 원활한 서비스 운영이 제공되어야 하며, 관리자와 TOE 서버 사이, 사용자와 TOE 사이에 송수신 되는 데이터를 보호하기 위해 보안 기능 유지와 안전한 채널이 제공되어야 한다. 또한 TOE에서 실시간으로 발생하는 감사데이터의 유효성 검사를 위해 타임스탬프 기능을 제공되어야 한다.

3.1.1 TOE 범위

다음 Fig.2.는 TOE의 구조를 나타낸다. TOE의 구조는 TOE 및 TOE 서버로 구성되어 있으며 상호간에 메시지 및 데이터를 송수신 한다.

Fig.1.과 같이 TOE는 데이터센터가 물리적으로 외부에 위치하여 데이터센터 서버로부터 원격으로 운영되는 경우와 데이터센터 서버가 데이터센터와 같은 시스템에 설치되는 경우로 구성될 수 있다.

다음은 TOE의 구성을 나타낸다.

- 스토리지 : 클라우드 네트워크를 통해 전송된 데이터를 저장한다.
- 인덱스 DB : 별도의 데이터베이스를 구축하여 전송받은 사용자 데이터에서 메타데이터를 추출하여 저장한다.
- 암호화 모듈 : TOE 서버와 TOE 간의 데이터 송수신시에 해당 값이 노출되지 않도록 보호한다.
- 데이터센터 서버 : 사용자로부터 인증정책, 접근정책, 정보의 흐름 통제 등 데이터센터의 각종 정책을 설정하여 통제할 수 있다.
- 관리자 : 지역 또는 원격으로 TOE 및 TOE 서버의 보안 설정 및 통제를 할 수 있다.

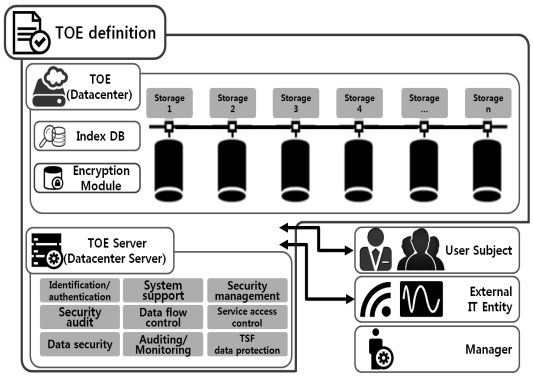

Fig.2. TOE definition

다음은 TOE가 기본적으로 제공해야 하는 보안기능을 나타낸다.

- 식별 및 인증/서비스 접근제어

TOE는 사용자의 신원을 식별 및 인증하고, 인가된 사용자에게만 TOE에 접근할 수 있도록 보장할 수 있어야 한다.

- 데이터 보안

TOE가 수행하는 데이터 보안 기능은 저장된 데이터, TOE에 업로드 또는 TOE에서 다운로드 중인 전송상태의 데이터, 인증 및 식별을 위한 메시지 등으로 구분된다.

- 저장된 데이터의 기밀성 유지를 위해 정당한 사용자만이 확인 가능해야 하며, 사용자가 TOE에 접근하기 위한 인증정보의 발신지 및 수신지, 통

신횟수, 길이, 통신상의 트래픽 특성에 대하여 공격자가 알 수 없어야 하며, 암호화 기능으로 저장된 데이터를 안전하게 보관할 수 있어야 한다.
- 전송상태의 데이터 무결성 보장을 위해 전자서명 또는 해쉬함수 연산 등을 이용하여 TOE와 사용자 사이에 전송되는 데이터의 위조 및 변조를 감지할 수 있어야 한다.
- 인증 및 식별을 위한 통신상의 송수신되는 메시지 보안을 위해 TOE에 접근하여 서비스 이용을 원하는 사용자가 전송한 메시지 및 데이터의 출처가 정확히 확인되고, 그 실체의 신분이 거짓이 아닌 정당한 사용자라는 것을 검증할 수 있어야 한다.

• 침해사고 식별·대응 및 감사·모니터링

TOE에 접근한 경로 및 메시지가 정당한 요청인지 식별할 수 있어야 한다. 만약 요청된 값이 정당한 값이 아닌 악의적인 요청일 경우에 침해사고로 이어질 수 있다. 이때 침해사고로부터 TOE의 데이터를 안전하게 보호할 수 있는 대응체계가 보장되어야 한다. 또한 TOE는 보안과 관련된 행동에 대한 책임을 추적하기 위해 보안 관련 사건들의 감사 레코드를 생성, 기록, 검토한다. 또한, 감사된 사건에 대한 잠재적인 보안 위반을 탐지하고 대응행동을 수행할 수 있어야 한다.

• 데이터 흐름통제

TOE는 데이터의 흐름을 중재하기 위해서 관련된 보안정책이 수행되고 있음을 보장해야 한다. TOE는 클라우드 망에서 TOE로 유입되는 유해한 트래픽(허가되지 않은 서비스에 대한 접근, 정상적인 패킷 구조를 가지고 있지 않는 네트워크 패킷, 웜·바이러스를 포함하는 패킷, 서비스 거부 공격을 수행하는 패킷 등)을 사전에 탐지한 후 차단하여 TOE의 정보자산 및 자원을 안전하게 보호할 수 있어야 한다.

• 기타 TSF 보호

TOE가 장애로 인해 서비스가 중단이 되었을 때 안전한 상태를 유지하고, TSF 데이터 및 TSF의 무결성을 검증하기 위한 자체적인 시험을 수행할 수 있어야 한다. 또한 TOE는 인가된 관리자 및 서비스 사용자에게 서비스 장애로 인한 사용중지 기간 이후에 대한 세션관리 기능을 제공할 수 있어야 한다.

본 논문에서 TOE는 클라우드 네트워크 외부에 독립적으로 운용될 수 있기 때문에 원활한 운영을 위해 부가적인 하드웨어, 소프트웨어 또는 펌웨어를 필요로 할 수 있다.

3.1 보안문제정의

보안문제정의는 TOE 및 TOE 운영환경이 다루도록 의도된 위협, 조직의 보안정책 및 가정사항을 정의한다.

3.1.1 위협

위협원은 일반적으로 외부에서 TOE 및 클라우드 환경에 불법적인 접근 시도를 하거나 또는 비정상적으로 TOE의 자산에 위협을 가해 데이터의 위변·조 및 유출을 일으키는 IT 실체 및 사용자이다. 위협원은 기본 수준의 전문지식, 자원, 동기를 가진다[16, 17, 18, 19, 20, 21].

• T.위장(T.Impersonation)

위협원은 TOE에 접근하기 위해 인가받은 사용자의 권한을 획득하여 위장할 수 있다.

• T.서비스 거부 공격(T.DoS attack)

위협원은 TOE 운영환경에 있는 데이터센터 서버에 비정상적으로 초과 접속하여 정상적인 인증과정을 수행한 사용자들의 TOE 사용을 방해할 수 있다[22, 23].

• T.저장데이터 훼손(T.Stored data problem)

위협원은 TOE에 저장된 사용자 데이터 또는 TSF 데이터를 인가받지 않은 불법적인 행위로 노출, 위조, 변조, 삭제할 수 있다[24, 25, 26, 27].

• T.전송데이터 훼손(T.Transport data problem)

위협원은 클라우드 네트워크를 통해 TOE로 송수신되는 데이터, TOE와 TOE 서버간의 TSF 데이터를 인가받지 않은 불법적인 행위로 노출, 위조, 변조할 수 있다[24, 25, 26, 27].

• T.불법적인 서비스 접근(T.Illegal service access)

위협원은 데이터센터에 허가되지 않은 서비스에 접근하여, TOE의 정상적인 서비스 제공을 방해할 수

있다[27, 28, 29, 30].

• T.악의적인 내부자(T.Malicious insider)
위협원은 인가받은 신뢰된 관리자로 위장하여 TOE에 불법적으로 접근할 수 있다[31].

• T.메시지 도·감청(T.Message eavesdropping)
위협원은 클라우드 네트워크상에서 TOE와 TOE 서버 사이에서 인증 및 식별을 위한 통신상의 송수신되는 TSF 데이터의 패킷을 불법으로 수집하여 도청 및 감청할 수 있다[22, 23].

• T.개인정보 노출(T.Privacy spill)
위협원은 피싱, 사기 등을 이용하여 클라우드 서비스 사용자의 고객정보를 유출할 수 있다[28, 30].

• T.데이터 저장 실패(T.Data storage failure)
위협원은 TOE의 저장용량을 모두 소진시켜서 송수신되는 데이터가 저장되지 않도록 할 수 있다[27].

• T.디바이스의 다양성(T.Device variety)
위협원은 TOE에 접근하는 사용자의 PC, 스마트폰, 태블릿PC, 스마트TV 등 다양한 형태의 디바이스에 따라서 그에 따른 각각의 디바이스가 지니는 고유의 보안위협을 발생시킬 수 있다[32].

• T.가상화 환경 문제
(T.Virtualization environment threat)
위협원은 클라우드 네트워크상에서 물리적인 시스템에 비해 상대적으로 보안관리가 미흡한 가상화 환경의 특성을 이용한 가상화 시스템의 내부 경로를 통해 신규 악성코드를 감염 및 새로운 유형의 해킹공격을 수행할 수 있다[26, 29, 32].

• T.분산된 데이터의 정보유지(T.Information maintenance of distributed data)
대용량의 데이터가 분산파일시스템을 통해 다수의 서버들에 분산 저장 및 관리되므로 위협원은 관리시스템 노출을 통해 악의적인 해킹, 사용자 데이터의 손실 및 유출시킬 수 있다[32].

3.1.2 조직의 보안정책

다음의 조직의 보안정책은 본 논문에서 제안하는 보호프로파일을 수용하는 TOE에서 준수되어야 한다[16, 17, 18, 19, 20, 21].

• P.감사(P.Audit)
TOE 및 TSF데이터의 보안과 관련된 모든 행동에 대한 책임을 추적하기 위해 보안관련 사건을 정확하게 기록하고 유지해야 하며, 기록된 감사데이터는 검토할 수 있어야 한다[33].

• P.안전한 관리(P.Secure management)
TOE는 인가된 관리자가 안전한 방식으로 TOE 및 TSF데이터를 관리할 수 있도록 관리 수단을 제공해야 한다[34].

• P.신속한 침해사고 대응(P.Expeditious intrusion incident response)
주기적인 보안 취약점 진단 및 최신패치 적용으로 침해사고가 발생했을 때 신속하게 대응할 수 있는 수단과 클라우드 인프라 자체에 대한 관제 모니터링이 제공되어야 한다[33, 34].

• P.확장성 있는 스토리지(P.Extendability storage)
클라우드 인프라의 특성상 데이터 스토리지 용량이 한계에 도달할 가능성이 크다. 따라서 TOE는 스토리지 시스템을 개선하는 작업이 매우 중요하며, 확장성을 위한 자원 관리, 고 가용성의 기준치를 만족 시킬 수 있는 확장성 있는 스토리지가 제공되어야 한다.

• P.서비스 장애 복구(P.Service failure recovery)
TOE는 침해사고 및 서비스 거부 공격 등 TOE를 운영함에 있어 장애가 발생했을 때 서비스 장애 복구를 위해서 인가된 관리자에게 TOE 관리 방안 및 복구 대응을 할 수 있는 가이드라인과 그에 맞는 역할이 부여되어야 한다[33].

3.1.3 가정사항

다음의 조건들이 본 논문에서 제안하는 보호프로파일을 수용하는 TOE 운영환경에 존재한다고 가정한다[16, 17, 18, 19, 20, 21].

• A.물리적 보안(A.Physical Security)
TOE가 운영되는 환경은 물리적으로 안전한 환경에 위치하며, 인가되지 않은 물리적 접근으로부터 보호된다.

• A.신뢰된 관리자(A.Trust manager)
TOE의 인가된 관리자는 악의가 없으며, TOE 관리 기능에 대하여 적절히 교육받고, 관리자 지침에 따라 정확하게 의무를 수행한다.

• A.안전한 채널(A.Trusted channels)
TOE와 클라우드 네트워크 사이에 전송되는 TSF 데이터는 인가되지 않은 방식으로부터 보호된다.

• A.법적·제도적 보강
(A.Institutional supplementation)
외국에서 TOE를 운영하는 경우에 재판 관할권에 따른 법규가 국내와 상이하여 데이터의 위치에 따른 법적 책임 문제로부터 TOE에 저장되는 사용자의 데이터가 보호된다[14, 26, 34].

• A.알려지지 않은 위협에 대한 보안유지
(A.Security maintain for unknown threat)
TOE는 기본적으로 현재까지 알려지지 않은 새로운 보안 위협에 대해서 보안유지가 되어 안전한 환경을 제공한다[35].

3.2 보안목적

본 논문에서 제안하는 보호프로파일에서는 보안목적을 TOE에 대한 보안목적 및 운영환경에 대한 보안목적으로 분류하여 정의한다. TOE에 대한 보안목적은 TOE에 의해서 직접적으로 다루어지는 보안목적이고, 운영환경에 대한 보안목적은 TOE가 보안기능성을 정확히 제공할 수 있도록 운영환경에서 지원하는 기술적/절차적 수단에 의해 다루어야하는 보안목적이다[16, 17, 18, 19, 20, 21].

3.2.1 TOE 보안목적

다음은 TOE에 의해 직접적으로 다루어져야 하는 보안목적이다.

• O.식별 및 인증
TOE는 TOE의 데이터 흐름통제를 받는 모든 외부 실체와 TOE에 접근하고자 하는 사용자를 식별해야 하며, 사용자의 신원을 인증해야 한다. 또한 관리자를 유일하게 식별하게 하며, TOE의 관리 및 관리 대상 시스템에 대한 접근을 허용하기 전에 관리자의 신원을 인증해야 한다.

• O.감사
TOE는 보안과 관련된 모든 행동의 책임추적이 가능하도록 보안관련 사건을 정확하게 기록하고 안전하게 유지해야 하며, 기록된 감사데이터를 검토할 수 있는 수단을 제공해야 한다.

• O.서비스 거부 공격 차단
TOE의 운영환경에 있는 클라우드 데이터센터 서버가 정상적인 사용자들이 사용할 수 있도록 하기 위하여, 공격자들이 비정상적으로 컴퓨터의 서비스 자원을 사용할 경우에 이를 차단해야 한다.

• O.저장 데이터 보호
TOE는 TOE에 저장된 사용자 데이터 또는 TSF 데이터를 인가되지 않은 불법적인 노출, 위조, 변조, 삭제로부터 보호해야 한다[25].

• O.TSF 데이터 보호
TOE로 송수신 되는 TSF 데이터를 인가받지 않은 노출, 변경, 삭제, 도청, 감청으로부터 보호해야 한다[25].

• O.전송 데이터 보호
TOE는 클라우드 네트워크를 통해 TOE로 송수신되는 데이터, TOE와 TOE 서버간의 TSF 데이터를 인가받지 않은 노출, 위조, 변조 등의 불법적인 행위로부터 보호해야 한다[25].

• O.침해사고 식별·대응
TOE 및 TSF에서 발생하는 침해사고 발생 시에 이벤트 관리, 침해사고의 유형 식별 및 대응을 위해 모니터링 기능을 제공해야 한다.

• O.관리
TOE는 TOE의 인가된 관리자가 TOE를 효율적으로 관리할 수 있는 관리 수단을 안전한 방법으로 제

공해야 한다[29].

• O.데이터 흐름통제
TOE는 보안정책에 따라 클라우드 망에서 데이터 센터 내부로 인가되지 않은 데이터의 흐름을 통제해야 한다.

• O.서비스 접근제어
TOE는 인증 받은 사용자만 TOE에 접근하여 서비스를 받을 수 있도록 해야 한다. 또한 인증 받은 사용자가 TOE에 접근하더라도 사용자의 권한에 따라 요청 가능한 서비스의 수준을 제어해야 한다.

• O.안전한 상태 유지
TOE 및 TSF의 침해사고 및 서비스 거부 공격 등 TOE를 운영함에 있어 장애가 발생한 경우 안전한 상태를 유지해야 하며, 장애에 의한 TSF 및 TSF 데이터의 손실을 탐지하기 위해서 자체적인 시험을 수행해야 한다. 또한 안전한 상태 유지를 위한 정책을 보유해야 한다.

3.1.2 운영환경에 대한 보안목적

다음은 TOE가 보안기능성을 정확히 제공할 수 있도록 운영환경에서 지원하는 기술적/절차적 수단에 의해 다루어져야 하는 보안목적이다.

• OE.신뢰된 관리자
TOE의 인가된 관리자는 악의가 없으며, TOE 관리 기능에 대하여 적절히 교육받고, 정해진 관리자 지침에 따라 정확하게 의무를 수행해야 한다.

• OE.원활한 서비스 운영
TOE는 원활하고 안정적인 서비스 운영 및 관리를 위해 가용성과 성능, 확장성을 보장해야 한다.

• OE.타임스탬프
TOE에 TOE의 운영환경에서 제공하는 신뢰할 수 있는 타임스탬프를 사용하여 보안 및 침해관련 사건을 정확하게 기록해야 한다.

• OE.암호화 및 키 관리
TOE는 TOE에 저장된 데이터 및 TSF 데이터의 안전한 저장 및 전송을 위해 암호화 기능을 제공해야 한다[36].

• OE.물리적 보안
TOE는 물리적으로 안전한 환경에 위치해야 하며, 인가되지 않은 물리적 접근으로부터 보호되어야 한다.

• OE.안전한 채널
TOE와 클라우드 네트워크 사이에 전송되는 TSF 데이터는 인가되지 않은 방식으로부터 보호되어야 한다.

• OE.보안유지
TOE의 운영정책 및 구성 변경, 서비스 수준에 따른 통신망의 증감 등으로 클라우드 네트워크 환경에 변화가 생겼을 때 변화된 환경과 보안정책을 즉시 TOE 운영정책에 반영하여 동일한 수준의 보안을 유지해야 한다.

3.1.3 보안목적의 이론적 근거

보안목적의 이론적 근거는 명세한 보안목적이 적합하고, 보안 문제를 다루기에 충분하며, 과도하지 않고 반드시 필요한 것임을 입증한다. 또한 보안목적의 이론적 근거는 다음을 입증한다.

- 각 위협, 조직의 보안정책, 가정사항이 최소한 하나의 보안목적에 의해서 다루어진다.
- 각 보안목적은 최소한 하나의 위협, 조직의 보안정책, 가정사항을 다룬다.

다음의 Table 2는 보안문제정의와 보안목적간의 대응관계를 나타낸다.

Table 2. Security problem definition - Security objectives counter

Security objectives / Security problem definition	Security objectives for the TOE											Security objectives for the operational environment						
	O. Identification / authentication	O. Audit	O. DDoS firewall	O. Stored data protection	O. TSF data protection	O. Transport data protection	O. Intrusion incident identification / response	O. Management	O. data flow control	O. Service access control	O. Security state information maintenance	OE. Trust manager	OE. Service operation	OE. Timestamp	OE. Encryption / key management	OE. Physical Security	OE. Trusted channels	OE. Security maintain
T. Impersonation	X	X								X								
T. DoS attack	X	X	X										X					
T. Stored data problem	X			X	X		X								X			
T. Transport data problem					X	X	X											
T. Illegal service access								X	X									
T. Malicious insider								X				X						
T. Message eavesdropping							X			X								
T. Privacy spill							X								X			
T. Data storage failure							X						X					
T. Device variety								X										
T. Virtualization environment threat											X							
T. Information maintenance of distributed data				X							X							
P. Audit		X												X				
P. Secure management								X				X						
P. Expeditious intrusion incident response							X						X					X
P. Extendability storage													X					
P. Service failure recovery											X		X					
A. Physical Security																X		
A. Trust manager												X						
A. Trusted channels																	X	
A. Institutional supplementation																X		
A. Security maintain for unknown threat																		X

3.2 보안기능요구사항 도출

Table 3. Security functional components - Security objectives counter

Class	Security functional components		Security objectives for the TOE										
			O. [illegible] authentication	O. Audit	O. DDoS firewall	O. Stored data protection	O. TSF data protection	O. [illegible] data protection	O. [illegible] identification/response	O. Management	O. data flow control	O. Service access control	O. [illegible] information maintenance
Security audit	FAU_ARP.1	Security alarms		X					X				
	FAU_GEN.1	Audit data generation		X									
	FAU_GEN.2	User identity association		X									
	FAU_SAA.1	Potential violation analysis		X					X				
	FAU_SAR.1	Audit review		X					X				
	FAU_SAR.2	Restricted audit review		X						X			
	FAU_SEL.1	Selective audit		X					X				
	FAU_STG.1	Protected audit trail storage		X					X				
	FAU_STG.2	Guarantees of audit data availability		X					X				
	FAU_STG.3	Action in case of possible audit data loss		X					X				
	FAU_STG.4	Prevention of audit data loss		X					X				
Crypto support	FCS_COP.1	Cryptographic operation				X							
User data protection	FDP_ACC.1	Subset access control				X						X	
	FDP_ACF.1	Security attribute based access control				X						X	
	FDP_DAU.1	Basic data authentication				X							
	FDP_DAU.2	Data authentication with identity of guarantor	X										
	FDP_IFC.1	Subset information flow control									X		
	FDP_IFF.3	Limited illicit information flows									X		
	FDP_IFF.4	Partial elimination of illicit information flows									X		
	FDP_ITT.1	Basic internal transfer protection				X							
	FDP_ITT.2	Transmission separation by attribute				X							
	FDP_SDI.1	Stored data integrity monitoring				X							
	FDP_UCT.1	Basic data exchange confidentiality					X	X					
	FDP_UIT.1	Data exchange integrity						X					
Identification and authentication	FIA_ATD.1	User attribute definition	X		X						X		
	FIA_UAU.1	Timing of authentication	X									X	
	FIA_UAU.2	User authentication before any action	X									X	
	FIA_UAU.3	Unforgeable authentication	X										
	FIA_UID.1	Timing of identification										X	
	FIA_UID.2	User identification before any action	X		X						X	X	
Security management	FMT_MOF.1	Management of security functions behaviour								X			
	FMT_MSA.1	Management of security attributes								X			
	FMT_MSA.2	Secure security attributes								X			
	FMT_MTD.1	Management of TSF data								X			
	FMT_SMF.1	Specification of management functions								X			
	FMT_SMR.1	Security roles								X			
Protection of the TSF	FPT_FLS.1	Failure with preservation of secure state											X
	FPT_ITC.1	Inter-TSF confidentiality during transmission					X						
	FPT_ITT.1	Basic internal TSF data transfer protection					X						
	FPT_RCV.1	Manual recovery											X
	FPT_RCV.4	Function recovery											X
	FPT_RPL.1	Replay detection							X				
	FPT_TDC.1	Inter-TSF basic TSF data consistency					X						
	FPT_TST.1	TSF testing											X
Resource utilisation	FRU_FLT.1	Degraded fault tolerance											X
	FRU_RSA.1	Maximum quotas			X								
TOE access	FTA_MCS.1	Basic limitation on multiple concurrent sessions			X								
	FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions			X								
	FTA_SSL.3	TSF-initiated termination			X				X				
	FTA_TAB.1	Default TOE access banners							X			X	
	FTA_TAH.1	TOE access history										X	
	FTA_TSE.1	TOE session establishment							X			X	
Trusted path/channels	FTP_ITC.1	Inter-TSF trusted channel						X					
	FTP_TRP.1	Trusted path						X					

보안기능요구사항은 본 논문에서 제안하는 보호프로파일을 수용하는 TOE에서 만족해야 하는 보안기능을 나타낸다.

본 논문에서 제안하는 보호프로파일에서 정의된 보안기능요구사항은 앞에서 식별한 보안목적을 만족시키기 위하여 공통평가기준 2부로부터 관련된 보안기능 컴포넌트를 선정하여 나타내었다. 다음의 Table 2는 본 논문에서 제안하는 보호프로파일에서 사용하는 보안기능컴포넌트를 요약하여 나타낸다[18].

또한 본 논문에서 제안하는 보호프로파일의 보안기능요구사항의 이론적 근거는 다음을 입증한다.

- 각 TOE에 대한 보안목적은 적어도 하나의 보안기능요구사항에 의해서 다루어진다.
- 각 보안기능요구사항은 적어도 하나의 TOE에 대한 보안목적을 다룬다.

IV. 비교 분석

앞선 2장에서 분석한 국내·외의 클라우드 인증제도 및 가이드라인을 비교 분석하여 각 제도간의 관련항목간 매핑을 통해 본 논문에서 제안하는 클라우드 데이터 관리 시스템 보호프로파일의 적합성을 판단하고자 한다. 각 제도간의 유사한 항목들을 통해서 가용성 보장, 감사 및 모니터링, 데이터 보안, 보안 정책 제도, 인증 및 접근제어, 침해대응, 시스템 보안, 물리적 보안, 가상화 환경 보안, 기타 등 총 10가지의 대분류로 나누어 관련항목간의 매핑을 통해 분석을 진행하였다.

이에 따라 제안하는 데이터 관리 시스템 보호프로파일은 10가지의 대분류에 전부 매핑되는 것을 확인할 수 있으며, 특히 KISA의 클라우드 서비스 정보보호 안내서에서 제시하고 있는 클라우드 서비스 제공자

Table 4. Conformance verification on the security of proposed protection profile in comparison by domestic/foreign cloud certification system and guideline.

	Gartner	CSA	ENISA	KISA	KCSA	Proposed protection profile	
						Security problem	Security objectives
Availability	7. Long-term viability	1. Cloud computing architectural framework	2. Supply-chain assurance	5. Secure a continuity of service	1. Availability	5. T.Illegal service access	O.Management
						14. P.Secure management	
					2. Extendability	12. T.Info. maintenance of distributed data	O.Security stateful
						17. P.Service failure recovery	
			5. Asset management		3. Performance	2. T.DoS attack	OE. Service operation
						9. T.Data storage failure	
						15. P.Expeditious intrusion incident response	
					6. Continuity of service	16. P.Extendability storage	
			7. Business continuity management			17. P.Service failure recovery	
					7. Support of service	15. P.Expeditious intrusion incident response	OE. Security maintain
						22. A.Security maintain for unknown threat	
Auditing/ Monitoring	2. Regulatory compliance	4. Compliance and audit	2. Supply-chain assurance	3. Asset classification/control	5. Security	1. T.Impersonation	O.Audit
						2. T.DoS attack	
				7. Network security		13. P.Audit	
						5. T.Illegal service access	O.Data flow control
Data security	4. Data separation	5. Information lifecycle Management	6. Data /services portability	9. Datacenter organization/condition of utilization	2. Extendability	3. T.Stored data problem	O. Stored data protection
						12. T.Info. maintenance of distributed data	
		6. Portability and interoperability				3. T.Stored data problem	O. TSF data protection
						4. T.Transport data problem	
	5. Recovery	8. Data Center operations		10. User data store management	4. Data management	4. T.Transport data problem	O.Transport data protection
						5. T.Illegal service access	O.Data flow control
		11. Encryption and key management				3. T.Stored data problem	OE. Encryption/ key management
Security policy	3. Data location	3. Legal and electronic discovery	10. Legal requirements	1. Policy of info. security/ provisions establish	-	21. A. Institutional supplementation	OE. Physical Security
			11. Legal recommendations	2. Info. security organization, manage/ personnel security			
			12. Legal recommendations to the EU	6. Obey the related laws/system			

	Gartner	CSA	ENISA	KISA	KCSA	Proposed protection profile	
						Security problem	Security objectives
Authentication/ access control	1° Privileged user access	12. Identity and Access Management	1. Personnel security	2. Info. security organization, manage/ personnel security	-	1. T. Impersonation	O. Identification/ authentication
						2. T. DoS attack	
						3. T. Stored data problem	
						5. T. Illegal service access	O. Data flow control
			4. Identity and access management	11. User authentication/access control		1. T. Impersonation	O. Service access control
						5. T. Illegal service access	
						7. T. Message eavesdropping	
						8. T. Privacy spill	OE. Encryption/ key management
Intrusion response	6° Investigative Support	2. Governance and Enterprise Risk Management	3. Operational security	4. Emergency response organization	5° Security	2. T. DoS attack	O. DDoS firewall
		7. Traditional Security, Business Continuity/Disaster Recovery				3. T. Stored data problem	O. Intrusion incident identification/ response
						4. T. Transport data problem	
						7. T. Message eavesdropping	
		9. Incident Response, Notification/ Remediation		7. Network security		8. T. Privacy spill	
						9. T. Data storage failure	
						15. P. Expeditious intrusion incident response	
System Security	-	10. Application Security	3. Operational security	8. System/ virtualization security	5° Security	5. T. Illegal service access	O. Management
			9. Environmental controls			6. T. Malicious insider	
						10. T. Device variety	
						14. P. Secure management	
						13. P. Audit	OE. Timestamp
Physical Security	-	-	8. Physical security	9. Datacenter organization/condition of utilization	5° Security	6. T. Malicious insider	OE. Trust manager
						14. P. Secure management	
						19. A. Trust manager	
						18. A. Physical security	OE. Physical Security
Virtualization environment	-	13. Virtualization	-	8. System/ virtualization security	-	11. T. Virtualization environment threat	O. Security stateful
						12. T. Info. maintenance of distributed data	
etc.	-	-	-	-	-	20. A. Trusted channels	OE. Trusted channels

의 정보보호 고려사항을 모두 만족하고 있으므로 본 논문에서 제안하는 보호프로파일이 클라우드 관련 제품군의 보안성평가를 위해 적용하기에 무리가 없을 것으로 기대할 수 있다[15]. 또한, 추가적으로 기존의 다른 인증제도 및 가이드라인으로부터 다루지 않고 있는 분야의 보안 문제점에 대해서도 커버되는 것을 확인할 수 있다.

V. 결 론

현재 보안 기능성이 있는 IT 제품의 개발, 평가 또는 조달에 대한 지침으로 활용 가능한 공통평가기준에서는 클라우드 제품군에 대한 보호프로파일을 제공하고 있지 않다. 또한, 국내·외의 국가별로 서로 다른 클라우드 보안 정책 및 가이드라인을 제시하고 그에 따른 보안 통제항목을 설정하여 준수하고 있다. 따라서 각국의 정보보호 평가 및 인증체계의 기준이 서로 상이하여 클라우드 제품군에 대해서 보안성을 평가하기 위한 공통적인 평가 방법이 정립되지 않은 것이 현실이다. 따라서 본 논문에서는 클라우드 환경에서 데이터센터에 데이터를 관리 및 저장하는 시스템의 보호프로파일을 제안하였다. 이를 위해 22개의 보안문제, 18개의 보안목적과 그에 따른 54개의 보안기능요구사항을 도출하였다. 또한 도출한 보안문제, 보안목적, 보안기능요구사항의 적합성 판단을 위해 국내·외의 클라우드 인증제도 및 가이드라인을 통해 검증하였다.

또한 현재 데이터베이스 제품군에 대한 국내·외의 보호프로파일 현황은 암호화된 저장장치 또는 데이터베이스 내의 데이터를 암·복호화해주는 DB 암호화 제품 등에 대한 보호프로파일이 전부이다. 따라서 본 논문에서 제안하는 보호프로파일은 가상화 운영환경, 데이터센터 등 클라우드 환경에 적용 가능하다. 이에 따라 본 논문에서 제안한 보호프로파일은 향후 클라우드 환경에서 데이터 관리 시스템 관련 제품군의 보안성 평가를 위한 기준이 되는 자료가 될 수 있다. 추가적으로 본 논문에서 제안한 보호프로파일을 통해서 클라

우드 제품군에 대한 보호프로파일 작성 시 수용 가능한 자료로 사용 될 수 있을 것으로 기대된다.

References

〔1〕 ENISA, "Good Practice Guide for securely deploying Governmental Clouds," 2013.

〔2〕 Yukyeong Wi, Jin Kwak, "Analysis of Domestic and Foreign Information Security Evaluation/Certification for Secure Cloud Service," Korea Institute of Information Security and Cryptology CISC-W, Vol23 No.2, pp.280-284, 2013.

〔3〕 Ki-Seok Bang, Il-Gon Kim, Ji-Yeon Lee, Jun-Seok Lee, Jin-Young Choi, "Classification Criteria and Application Methodology for Evaluating IT Security Products," KKITS journal, Vol6 No.5, pp.105-112, 2011.

〔4〕 KISA, "IT Security Evaluation & Certification Guide with Common Criteria," KISA guideline Vol.2010-18, 2010.

〔5〕 KISA, "Information Security System Evaluation & Certification Guide," 2004.

〔6〕 Jon Brodkin, "Gartner:Seven Cloudcomputing security risks," Network world, Jul 2008.

〔7〕 Hyungkeun Park, "Companies to consider using public cloud computing security risks and countermeasures for 小考," Review of KIISC, Vol22 No.7, pp.46-53, 2012.

〔8〕 Park Jae Geol, Jeong Dong Woog, Lee Dong Yeoup, "A Study of Security Management on Cloud Computing in Defense," Conference of The Korean Institute of Communications and Information Sciences, pp.368-369, 2012.

〔9〕 株式會社アイ·ビー·ティ, "クラウド·コンピューティング時代のDependa-bility の考え方などに關する米國の動向調査," 2010.

〔10〕 Hyun-Jung Lee, Dong-Ho Won, "An Analysis of Cloud System Security Functional Requirement," Journal of Security Engineering, Vol9 No.6, pp.495-502, 2012.

〔11〕 CSA(cloud security alliance), "Security guidance for critical areas of focus in cloud computing v3.0," 2011.

〔12〕 ENISA, "Cloud Computing Benefits, risks and recommendations for information security," 2009.

〔13〕 KISA, Internet & Security Issue, Vol.2010-10, pp.56-59, 2010.

〔14〕 Kichul Kim, Ok Heo, Seungjoo Kim, "A Security Evaluation Criteria for Korean Cloud Computing Service," Journal of the Korea Institute of Information Security and Cryptology, Vol.23 No.2, pp.251-265, 2013.

〔15〕 KISA, "Information Security Guide for Cloud Services," KISA guideline Vol.2011-8, 2011.

〔16〕 CCRA, "Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model," CCMB-2012-09-001, Version 3.1r4, 2012.

〔17〕 CCRA, "Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components," CCMB-2012-09-003, Version 3.1r4, 2012.

〔18〕 CCRA, "Common Criteria for Information Technology Security Evaluation Part 2: Security functional components," CCMB-2012-09-002, Version 3.1r4, 2012.

〔19〕 IT Security Certification Center, "Enterprise Security Management System Protection Profile V2.0," 2008.

〔20〕 IT Security Certification Center, "Role Based Access Control System Protection Profile V2.0," 2008.

〔21〕 IT Security Certification Center, "Network Intrusion Prevention System Protection Profile V2.1," 2010.

〔22〕 KISA, "Vulnerability analysis and response technology cloud computing security," 2010.

[23] Eun-Young Jang, Hyung-Jong Kim, Choon-Sik Park, Joo-Young Kim, Jae-il Lee, "The study on a threat counter-measure of mobile cloud services," Journal of the Korea Institute of Information Security and Cryptology, Vol.21 No.1, pp.177-186, 2011.
[24] Jonghoon Lee, Seungwook Jung, Souhwan Jung, "Trends in Security as a Service," Vol.22 No.7, pp.54-61, 2012.
[25] Taehyoung Kim, Inhyuk Kim, Changwoo Min, Young Ik Eom, "Cloud computing security technology trends," Review of KIISE, Vol.30 No.1, pp.30-38, 2012.
[26] Kyoung-a Shin, Sang-jin Lee, "Information Security Management System on Cloud Computing Service," Journal of the Korea Institute of Information Security and Cryptology, Vol.22 No.1, pp.155-167, 2012.
[27] Young-Gi Min, Kab-Seung Kou, "A Designed of Virtual Machine Security Vulnerability Detection Tool in a Cloud Computing Environment," Journal of Security Engineering, Vol.9 No.6, pp.519-530, 2012.
[28] Rak-Cheol Kim, Jeong-Hyun Gong, Geon Kim, Hyung-Hyo Lee, "Security Requirements for Cloud Services," Conference of The Korean Institute of Information Technology, pp.430-434, 2012.
[29] Yukyeong Wi, Jin Kwak, "A study on Security Functional Requirement (SFR) of Applicable to the Cloud Environment in Common Criteria," The 38th conference of the KIPS, Vol20 No.2, pp.731-734, 2013.
[30] Yukyeong Wi, Jin Kwak, "Data Store Scheme for the Secure Cloud Data Center," Korea Institute of Information Security and Cryptology CISC-S, Vol23 No.1, pp.297-300, 2013.
[31] Kim DongWoo, "Smart Media Development and Cloud Security," Review of KIISC, Vol21 No.8, pp.46-54, 2011.
[32] Taeshik Shon, Jongbin Ko, "Cloud Computing in the IoT (Internet of Things) Security Trends," Review of KIISC, Vol22 No.1, pp.20-30, 2012.
[33] Yang Hwan Seok, Lee Byoung Cheon, Yoo Seung Jea, "Study on Intrusion Detection System under Cloud Computing Environment," Jouranl of Information and Security, Vol12 No.3, pp.59-65, 2012.
[34] Lee Hyang Jin, Son Kyoung Ho, Lee Jae Il, "Cloud-based enterprise information security services to Strengthen," Review of KIISC, Vol23 No.4, pp.59-64, 2013.
[35] Eui-nam Huh, "Personal Cloud Security Technology and Privacy," TTA Journal, Vol.139, pp.65-69, 2012.
[36] Jin Hee Kang, Ji Yeon Kim, Choon Sik Park, Hyung Jong Kim, "Privacy IaaS services company considering the characteristics of technical analysis and how to apply research skills," Review of KIISC, Vol22 No.8, pp.61-73, 2012.

〈저자소개〉

위 유 경 (Yukyeong Wi) 학생회원
2012년 2월: 순천향대학교 정보보호학과(공학사)
2012년 2월~현재 : 순천향대학교 정보보호학과 석사과정
〈관심분야〉 정보보호제품평가, 클라우드 컴퓨팅 보안, 제어시스템 보안, 콘텐츠 보안

곽 진 (Jin Kwak) 종신회원
성균관대학교 학사, 석사, 박사
2006년 4월~2006년 11월 : 일본 큐슈대학교 방문연구원
2006년 4월~2006년 11월 : 일본 큐슈시스템정보기술연구소 특별연구원
2006년~2007년 2월 : 정보통신부 정보보호기획단 개인정보보호팀 통신사무관
2007년 3월~현재 : 순천향대학교 정보보호학과 교수
2008년 1월~현재 : 한국정보보호학회 이사
2008년 12월~현재 : 정보통신산업진흥원 기술평가위원
2010년 3월~현재 : 조달청 기술평가위원
2010년 5월~2010년 7월 : 교육과학기술부 국가기술수준평가 위원
2011년 1월~현재 : 한국정보기술융합학회 이사
2011년 1월~현재 : 한국정보처리학회 이사
2011년 1월~현재 : 지식경제부 지식경제기술혁신평가단 위원
2012년 ~현재 : 한국방송통신전파진흥원 평가위원
2013년 ~현재 : 교육부 정책자문위원
2013년 ~현재 : 금융보안연구원 보안기술 자문위원
2013년 ~현재 : 금융감독원 인증방법평가위원
〈관심분야〉 암호프로토콜, 응용시스템보안, 개인정보보호, 정보보호제품평가, 클라우드 컴퓨팅 보안 등