2021 한국차세대컴퓨팅학회
춘계학술대회

장　　소 : 김대중컨벤션센터 301호 ~ 303호
일　　시 : 2021. 5. 13(목) 13:00 ~ 5. 14(토) 12:30
주최 · 주관 : 한국차세대컴퓨팅학회
후 원 : 광주관광재단, ㈜트라콤, 아주대학교 MR-IoT 재난대응인공지능연구센터

클라우드 서비스 정보보호 프레임워크에 관한 연구 (보안 요구사항을 중심으로)

A study on the cloud service information security framework (Focused on security requirements)

Chan-Woo Lee
Information Security
Sejong University
Seoul, Korea
jg719411@nate.com

Ki-Woong Park[1]
Information Security
Sejong University
Seoul, Korea
woongbak@sejong.ac.kr

Abstract

최근 클라우드 서비스가 더욱 보편화되면서 경제성과 확장성, 탄력성 등 클라우드의 도입으로 인한 장점뿐만 아니라 클라우드 서비스의 도입으로 인해 발생하는 보안 위험에 대한 우려가 증가하고 있다. 하지만 기존의 전통적인 정보보호 관리체계에서 요구되는 보안 요구사항은 이러한 클라우드 서비스의 보안 위험을 적절히 대응하지 못하고 있는 실정이다. 이에 본 논문은 클라우드 보안 프레임워크의 선행연구와 클라우드 컴퓨팅의 보안 위험을 분석하고 종합하여 클라우드 서비스 정보보호 프레임워크를 수립하기 위해 필요한 보안 요구사항을 제안하였다. 본 논문에서 제안한 보안 요구사항은 기업의 정보보호 관점에서 관리적, 물리적, 기술적인 전체 최적화를 이루는 데 도움을 줄 수 있고, 클라우드 서비스를 안전하게 도입 및 활용하고자 하는 기업에서 수립해야 할 클라우드 서비스 정보보호 프레임워크의 기초를 제공할 것으로 예상한다.

Keywords: 클라우드 서비스, 보안 프레임워크, 보안 위험, 보안 요구사항

1. 서론

클라우드 컴퓨팅은 서로 다른 물리적 위치에 존재하는 컴퓨팅 자원을 가상화 기술로 통합해 서비스를 제공하는 기술로써, IT 자원을 서로 공유하고 유휴 자원을 효율적으로 이용해 궁극적으로는 전체적인 비용절감 효과를 가져온다. 한편, 클라우드 서비스란 클라우드 컴퓨팅 기술을 활용하여 IT 자원을 필요한 만큼 클라우드 공급자로부터 빌려서 원하는 시점에 사용하는 서비스를 의미한다. 최근 이러한 가상화 기술을 기반으로 한 클라우드 서비스가 더욱 보편화되면서 경제성과 확장성, 탄력성 등 클라우드의 도입으로 인한 장점뿐만 아니라 클라우드 서비스의 도입으로 인해 발생하는 보안 위험에 대한 우려가 증가하고 있다. 하지만 기존의 전통적인 정보보호 관리체계에서 요구되는 보안 요구사항은 자원의 통합 및 가상화 기술을 이용하는 클라우드 서비스의 다양한 보안 위험을 적절히 대응하지 못하고 있는 실정이다[1]. 이에 본 논문은 클라우드 보안 프레임워크의 선행연구와 클라우드 컴퓨팅의 보안 위험을 분석하고 종합하여 클라우드 서비스 정보보호 프레임워크를 수립하기 위해 필요한 보안 요구사항을 제안하였다. 기존 연구의 경우 부분적인 클라우드 환경의 보안 요구사항을 정의하였기 때문에 전체 보안 프레임워크 관점에서 국소 최적화의 함정에 빠질 가능성이 존재하나, 본 논문에서 제안하는 보안 요구사항은 기존 연구의 한계

[1] 교신저자

사항을 모두 반영하였으며, 관리적, 물리적, 기술적인 보안 영역에 대한 전역 최적화를 목적으로 하기 때문에 클라우드 서비스를 안전하게 도입 및 활용하고자 하는 기업에서 보안 프레임워크를 구성하고자 할 때 유용하게 활용할 수 있을 것으로 예상한다. 본 논문의 구성은 다음과 같다. 2장에서는 클라우드 서비스 정보보호 프레임워크과 관련한 선행연구를 분석함으로써 전통적인 보안 프레임워크와 클라우드 서비스 보안 위험, 클라우드 서비스 보안 요구사항을 각각 고찰한다. 3장에서는 본 연구에서 제안하고자 하는 클라우드 서비스 정보보호 프레임워크의 보안 요구사항을 설명한다. 마지막으로 4장에서는 본 논문의 결론을 제시하고, 향후 연구 계획을 소개한다.

2. 선행연구 및 이론적 배경

본 장에서는 정보보호 관리체계, 클라우드 서비스 보안 위험 및 보안 요구사항의 선행연구를 분석함으로써 각각의 이론적 배경을 살펴본다.

2.1. 정보보호 관리체계

정보보호 관리체계를 효율적으로 수립할 수 있도록 표준화된 보안 프레임워크로써 정보보호 국제표준인 ISO/IEC(International Organization for Standardization/International Electrotechnical Commission) 27001이 대표적이다. 기업의 관리적, 물리적, 기술적인 보안통제 항목을 기술하고 있기 때문에 기업의 보안수준을 전사적인 관점에서 최적화시키기 용이하지만, 물리적인 자원 통합과 가상화 기술, 인터넷을 통한 접근, 멀티 테넌시 등 클라우드 서비스의 환경적인 특징을 통제항목에 적절히 반영하지 못하는 한계사항이 존재한다. 한편, ISO/IEC 27001 표준에서는 <Table 1>과 같이 14개의 통제항목(인증기준)을 권고하고 있다[2].

<Table 1> 정보보호 관리체계

통제항목	의미
1. 정보보안정책	정보보안에 대한 경영방향을 설정해야 한다.
2. 정보보안조직	정보보안을 담당하는 내부조직을 구성해야 한다.
3. 인적보안	고용, 퇴직 및 직무변경 시 보안 점검을 수행한다.
4. 자산관리	자산을 분류하고, 관리자를 지정해야 한다.
5. 접근통제	접근통제를 위한 비즈니스 요구사항을 정의하고, 시스템과 애플리케이션의 접근 통제를 수행해야 한다.
6. 암호통제	암호와 키에 대한 보안 관리를 수행해야 한다.
7. 물리적및환경적 보안	보안 구역을 지정하고, 기업에서 보관되고 있는 장비를 안전하게 관리해야 한다.
8. 운영보안	운영절차를 정의하고, 기술적인 취약점을 관리한다.
9. 통신보안	네트워크 보안을 통해 안전하게 정보를 전송한다.
10. 시스템수용, 개발및유지	정보시스템의 보안 요구사항을 정의하고 개발 및 시스템 운영 전반에 반영해야 한다.
11. 공급자관계	공급자와의 관계에서 정보보안을 정의하고, 공급자가 제공하는 서비스를 관리해야 한다.
12. 정보보안사고 관리	정보보안 사고에 대해 모니터링하고 사고 발생 시, 신속하게 조치해야 한다.
13. 업무연속성 관리	재해 복구 대책과 업무 연속성 계획을 수립해서 조직의 비즈니스 연속성을 확보해야 한다.
14. 준수	법규 및 계약의 요구사항의 준수여부를 검토한다.

2.2 클라우드 서비스 보안 위험

클라우드 서비스의 제공 및 도입 시 활용할 수 있는 정보보호 국제표준으로써 2015년, ISO/IEC (International Organization for Standardization International Electrotechnical Commission) 27017이 제정되었다. 클라우드 서비스를 사용함에 따라 발생할 수 있는 다양한 비즈니스 이슈와 법적인 문제, 클라우드 서비스 공급업체에 대한 의존성 등 클라우드 서비스의 특징을 잘 반영하여 보안 위험을 구성하였지만, 클라우드 서비스의 기술적인 보안 요구사항을 세부적으로 표현하지 못하는 한계사항이 존재한다. 한편, ISE/IEC 27017 표준에서는 <Table 2>와 같이 클라우드 서비스의 보안 위험을 15개로 선정하였다[3].

<Table 2> 클라우드 서비스 보안 위험

보안 위협	의미
1. 거버넌스 손실	퍼블릭 클라우드의 경우, 고객은 보안 문제에 대한 제어권을 클라우드 공급자에게 넘겨야 한다.
2. 책임의 모호성	클라우드 서비스의 사용과 보안에 대한 책임이 공급업체와 고객에게 분산되며, 책임을 명확하게 정의하지 않는 경우 보호받지 못할 가능성도 있다.
3. 격리의 실패	퍼블릭 클라우드는 리소스 공유와 멀티 테넌시라는 특성으로 인해 정보가 유출될 수 있다.
4. 공급업체 의존성	특정 클라우드 서비스 공급 업체의 서비스에 의존하면 유연한 보안 구성이 힘들어 질 수 있다.
5. 규정 준수 및 법적 위험	클라우드 서비스 공급 업체가 정보보호 통제에 적절히 협조하지 않으면 정보보호 인증에 차질이 생긴다.
6. 보안사고 대응	클라우드 서비스의 침해 사고를 감지하고 후속 조치를 수행하는 역할을 공급 업체에 의존해야 한다.
7. 관리 인터페이스 취약성	클라우드 서비스의 관리자 페이지는 인터넷을 통해 접근하기 때문에 원격 또는 웹 취약점에 노출된다.
8. 데이터 보호	고객 및 공급 업체에 데이터 유출 위험이 존재한다.
9. 공급업체 파산	파산으로 인해 서비스 가용성이 침해될 수 있다.
10. 내부자 위협	내부자에 의해 서비스 권한이 오남용될 수 있다.
11. 데이터센터 장애	클라우드 서비스가 공급되는 데이터 센터의 장애는 클라우드 서비스의 장애로 이어진다.
12. 마이그레이션 및 통합 실패	클라우드 서비스 환경으로의 마이그레이션 및 통합이 실패하면 보안 문제가 야기될 수 있다.
13. 구성요소의 변경	클라우드 서비스의 구성요소가 변경됨으로 인해 새로운 보안취약점이 발생할 수 있다.
14. 관할권 문제	공급자와 고객의 관할권 분쟁이 발생할 수 있다.
15. 불완전한 데이터 삭제	클라우드 서비스 계약 종료 시, 불완전한 데이터 삭제 조치로 인해 정보유출이 발생할 수 있다.

2.3. 클라우드 서비스 보안 요구사항

기존에 연구된 '클라우드 컴퓨팅 보안 기술 표준화를 위한 계층 및 역할별 보안 요구사항 제안' 논문[4]에서 클라우드 컴퓨팅 서비스의 보호를 위해 고려해야 하는 보안 요구사항을 <Table 3>과 같이 6가지로 정의하였다. 클라우드 서비스의 기술적인 보안 요구사항을 세부적으로 구분했지만, 계약 및 법적 문제 등 클라우드 서비스를 사용하면서 발생할 수 있는 관리적, 환경적인 보안 요구사항을 포함하지 않은 한계사항이 존재한다.

<Table 3> 클라우드 서비스 보안 요구사항

보안 요구사항	의미
1. 기밀성 및 데이터 암호화	클라우드 서비스는 일반적으로 다수 사용자들이 공용 환경에서 이용하기 때문에 비인가된 개인, 단체, 프로세스 등으로부터 중요한 정보를 보호해야 한다.
2. 사용자 인증과 접근제어	다수의 사용자의 데이터가 공존하는 클라우드 환경에서 인가된 사용자에 대한 정확한 본인확인을 위한 사용자 인증과 권한 관리를 위한 접근제어 기법이 필요하다.
3. 데이터 무결성	클라우드 환경에서 서비스 이용자의 정보의 저장과 전달 시, 클라우드 서비스는 비인가된 방식으로 정보와 소프트웨어에 접근하고 변경되지 않도록 정확성과 안정성을 확보해야 한다.
4. 가용성 및 복구	클라우드 서비스는 인가된 사용자가 정보나 서비스를 요구할 때, 언제든지 즉시 사용 가능하도록 제공해야 하며, 사고로 인한 서비스 중단이나 데이터 손실을 막기 위해 사고 발생 시 서비스의 지속성을 확보해야 한다.
5. 가상화 보호	클라우드 컴퓨팅 환경에서는 기존의 컴퓨팅 환경과 다른 새로운 보안 취약점이 발생하며, 클라우드 가상화 시스템의 보호를 위한 기능을 제공해야 한다.
6. 네트워크 보안 및 웹 보안	기존의 네트워크와 웹에서 발생 가능한 위협이 클라우드 환경에서도 동일하게 발생할 수 있다.

3. 제안하는 클라우드 서비스 정보보호 프레임워크의 보안 요구사항

본 장에서는 클라우드 서비스 보안 프레임워크와 관련한 선행연구를 분석하고 고찰한 2장의 이론적 배경을 토대로 클라우드 서비스 정보보호 프레임워크를 수립하기 위해 필요한 보안 요구사항을 새롭게 재정립하였으며, <Table 4>와 같이 8개의 카테고리로 구분하여 제안한다. 기존 연구의 경우 일반적인 보안의 관점 또는 비즈니스 및 기술적 관점 등에서 보안 요구사항을 정의하며, 클라우드 환경에서 발생가능한 다양한 이슈를 다루기에 일부 한계사항이 존재했으며 이로 인해 클라우드 서비스를 이용하는 기업의 전체 보안 프레임워크 상의 국소 최적화의 문제가 발생할 수 있다. 그러나, 본 논문에서 제안하는 보안 요구사항은 비즈니스 요구사항과 아키텍처의 최적화 설계를 위한 요구사항, 벤

더와 제품을 포함한 클라우드 서비스의 본질적인 보안 요구사항 등을 포함하며 관리적, 물리적, 기술적인 보안 영역에 대한 전역 최적화를 목적으로 하고 있기 때문에 기존 연구에 비해 균형잡힌 클라우드 서비스 정보보호 프레임워크를 설계할 수 있다.

<Table 4> 제안하는 보안 요구사항

구분	보안 요구사항
1. 비즈니스분석	클라우드 서비스를 도입하는 범위와 목적을 분석하고, 제공되는 계약사항에 대하여 법적 준수 의무와 정보보호 측면에서 검토한다.
2. 데이터보호	클라우드 서비스 상에서 데이터를 수집, 저장, 전송, 처리, 파기 시 법적 의무를 준수하고, 개인정보에 대한 안전성 확보조치를 수행한다.
3. 아키텍처 설계	클라우드 서비스와 내부 시스템을 연동할 경우, 전체적인 시스템 구성의 영향도를 분석하고 위험평가를 실시해서 아키텍처 상 보안결함이 발생하지 않도록 최적화한다.
4. 서비스평가	클라우드 서비스를 제공하는 공급 업체에 대한 평가와 공급업체의 서비스(제품)에 대한 평가를 구별하여 진행한다.
5. 접근통제	클라우드 서비스에서 제공되는 계정과 권한을 파악하고, 역할에 기반하여 접근통제가 구현될 수 있도록 설계한다.
6. 보안시스템 적용	기존의 보안 시스템을 적용하여 클라우드 서비스의 보안 최적화를 검토하고, 미흡할 시 추가적인 대응방안을 마련한다.
7. 모니터링	클라우드 서비스의 보안 상태와 이슈를 모니터링 하고 대응하기 위해서 필요한 로그를 정의하고, 로그를 수집 및 분석할 수 있는 체계를 설계한다.
8. 이해관계자 관리	클라우드 서비스의 도입을 위한 다양한 이해관계자를 식별하고, 책임과 역할을 정의해서 상시 협업의 기반을 마련한다.

4. 결론 및 향후계획

본 논문에서는 클라우드 서비스 보안과 관련한 선행연구를 분석하여 클라우드 서비스 정보보호 프레임워크를 수립하기 위한 보안 요구사항을 새롭게 재정립하여 제안하였다. 본 논문에서 제안한 클라우드 서비스 보안 요구사항은 기업의 정보보호 관점에서 관리적, 물리적, 기술적인 전체 최적화를 이루는 데 도움을 줄 수 있고, 기업에서 클라우드 서비스 정보보호 프레임워크를 수립할 때 기초정보로 활용할 수 있다. 향후 본 논문에서 제안한 클라우드 서비스 보안 요구사항을 토대로 IaaS(Infrastructure as a Service), PaaS(Platform as a Service), SaaS(Software as a Service) 등 다양한 클라우드 서비스의 보안 요구사항을 각각 정의하고, 기업에서 활용할 수 있는 클라우드 서비스 정보보호 프레임워크를 개발할 계획이다.

Acknowledgement

본 연구는 2019년도 과학기술정보통신부의 재원으로 정보통신기획평가원의 지원(No.2019-0-00426) 및 한국연구재단 연구과제(NRF-2020R1A2C4002737)의 지원을 받아 수행된 연구임

References

[1] 정순기, 정만현, 조재익, 손태식, 문종섭, “클라우드 컴퓨팅 가상화 보안을 위한 아키텍처 구성 및 기능 분석 연구”, 보안공학연구논문지, 제8권 제5호, pp.627-644, 2011. 10.

[2] ISO/IEC, 2013, “INFORMATION SECURITY MANAGEMENT”, https://www.iso.org/isoiec-27001-information-security.html

[3] 김정덕, 이성일, “클라우드 컴퓨팅 정보보호 프레임워크에 관한 연구”, 정보보호학회논문지, 제23권 제6호, pp.1,277-1,286, 2013. 12.

[4] 이찬우, 김상곤, 여영민, 문종섭, “클라우드 컴퓨팅 보안 기술 표준화를 위한 계층 및 역할별 보안 요구사항 제안”, 보안공학연구논문지, 제10권 제4호, pp.473-488, 2013. 8.