클라우드 네트워크 가상화 서비스의 안전한 제공을 위한 정책 방안 연구

이은지*, 배원일*, 곽진**
*아주대학교 컴퓨터공학과 정보보호응용및보증연구실
**아주대학교 사이버보안학과
e-mail:ejlee.isaa@gmail.com*, wibae.isaa@gmail.com*, security@ajou.ac.kr**

Study on Policy for Secure Provision of Cloud Network Virtualization Service

Eun-Ji Lee*, Won-il Bae*, Jin Kwak**
*ISAA Lab., Department of Computer Engineering, Ajou University
**Department of Cyber Security, Ajou University

요 약

클라우드 컴퓨팅 환경은 가상화 인프라를 제공하며 클라우드 서비스 참여자는 이러한 가상화 자원을 사용하여 서비스를 제공 및 활용한다. 그러나, 클라우드 가상화 환경에서의 보안위협이 지속적으로 증가하고 있는 반면, 안전한 클라우드 가상화를 위한 정책 연구는 미비한 실정이다. 이에 따라, 본 논문은 클라우드 가상화 인프라 중 클라우드 네트워크 가상화의 서비스를 안전하게 제공하기 위한 정책 방안을 제안한다. 제안하는 방안에서 클라우드 네트워크 가상화 환경에서 발생 가능한 보안위협을 도출하고 이에 따른 보안요구사항을 도출한다. 결과적으로, 클라우드 네트워크 가상화 서비스를 안전하게 제공하기 위한 정책 마련 시 클라우드 서비스 제공자가 고려해야할 보안요구사항 도출을 목표로 한다.

1. 서론

클라우드 컴퓨팅 환경은 가상화 기술을 통해 가상화 인프라를 제공한다. 이때, 클라우드 네트워크 가상화는 네트워크 장비를 가상화함으로써 클라우드 환경을 구성하는 물리적인 네트워크 자원을 분리해 여러 사용자에게 서비스를 제공하기 위한 기술이다.

최근까지 국내·외 클라우드 서비스 활성화를 위한 정책연구가 활발히 진행되고 있다. 이에 반해, 안전한 클라우드 가상화를 위한 정책연구는 몇몇의 표준 정책 이외에 연구는 미비한 실정이다. 더불어, 가상화 환경에서 동작하는 악성코드가 클라우드 가상화 환경을 타겟으로 하는 등 클라우드 가상화 환경에서 보안위협 또한 증가하고 있다. 이에 따라, 클라우드 서비스 사용에 앞서 클라우드 가상화 서비스를 안전하게 제공할 필요가 있으며 본 논문은 클라우드 네트워크 가상화 서비스를 안전하게 제공하기 위한 정책 방안을 연구한다[1,2].

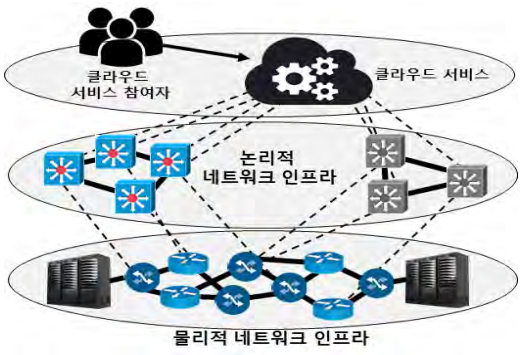
본 논문의 구성은 다음과 같다. 2장에서 클라우드 네트워크 가상화, 기존 클라우드 컴퓨팅의 보안위협 등을 분석하며 3장에서는 클라우드 네트워크 가상화에서 발생 가능한 보안위협과 이에 따른 보안요구사항을 도출한다. 더불어, 클라우드 네트워크 가상화 환경에서 클라우드 서비스 제공자가 고려해야할 정책 방안을 연구한다. 마지막으로, 4장에서 결론을 맺는다.

이 논문은 2016년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.R0126-16-1111, 클라우드 보안을 위한 위험기반 인증·접근제어 프레임워크 및 보안상태 점검기술 개발).

2. 관련연구

2.1 클라우드 네트워크 가상화

클라우드 네트워크 가상화는 클라우드 환경에 가상화 기술을 도입하여 하나의 물리적인 네트워크 자원을 분리하여 논리적으로 구성하는 기술이다. 이를 통해, 여러 사용자에게 서비스를 제공할 수 있으며 클라우드 서비스 참여자들은 가상화 인프라의 가상자원을 이용해 클라우드 서비스를 제공 및 사용한다. 이에 따른 클라우드 네트워크 가상화 구성은 (그림 1)과 같다[3].



(그림 1) 클라우드 네트워크 가상화 구성

2.2 클라우드 서비스 참여자별 역할

클라우드 서비스 참여자는 클라우드 서비스 소비자(Cloud Service Customer), 클라우드 서비스 제공자(Cloud Service Provider), 클라우드 서비스 파트너(Cloud Service Partner)로 구분된다.

CSC는 마이그레이션과 같은 네트워크 서비스를 포함한 클라우드 서비스를 사용하는 주체이다. CSP는 해당 서비스를 CSC가 원활이 이용 가능하도록 서비스를 제공하며, CSN은 네트워크 기능 개발 등 CSC 또는 CSP에게 서비스 활동이 가능하도록 지원한다.

즉, CSP는 CSN으로부터 서비스 참여 역할에 따른 서비스 활동을 지원 받아 CSC에게 서비스를 제공한다. 이때, CSC가 안전하게 클라우드 서비스를 사용하기 위해서는 먼저, 해당 서비스를 제공하는 CSP 측면에서 서비스 제공의 안전성이 보장될 필요가있다.

이때, 클라우드 서비스 각 참여자는 사업적, 운영적, 보안적 등의 여러 관점에서 세부 역할이 분류된다. CSP의 경우 세부 역할에 따라 클라우드 서비스 운영 관리자, 클라우드 서비스 관리자 등으로 구분되며 이 중 보안적 관점에서의 역할을 갖는 주체로는 클라우드 서비스 보안 및 위험 관리자가 있다. 클라우드 서비스 보안 및 위험 관리자는 클라우드 서비스의 제공, 활용 및 지원하는 과정에서 발생되는 보안위협 및 위험을 관리한다[4].

2.3 클라우드 컴퓨팅 보안위협

CSA(Cloud Security Alliance), ENISA(European Network and Information Security Agency)에서는 각각 「Cloud Computing Top Threats in 2016」, 「Threat Landscape 2015」, 문서를 통해 클라우드 컴퓨팅 환경에서 발생할 수 있는 보안위협을 정의 및 발표하였다[5,6]. 이에 따라, CSA 및 ENISA에서 제시한 클라우드 컴퓨팅 환경에서의 보안위협은 <표 1>과 같다.

<표 1> CSA 및 ENISA 클라우드 컴퓨팅 보안위협

No	CSA Cloud Computing Top Threats in 2016	ENISA Threat Landscape 2015
1	데이터 유출	악성코드
2	부적절한 신원	웹 기반 공격
3	불안전한 API	웹 응용 프로그램 공격
4	시스템 및 응용 프로그램 취약점	봇넷
5	계정 도용	서비스 거부
6	악의적인 내부자	내부자 위협
7	APT(Advanced Persistent Threats)	데이터 유출
8	데이터 손실	사이버 간첩
9	클라우드 서비스 이해 부족	신분 도용
10	클라우드 서비스 남용	정보 누설
11	서비스 거부	
12	공유된 기술의 취약점	

2.4 클라우드 서비스 참여자별 보안위협

ITU-T(International Telecommunication Union Telecommunication Standardization Sector)의 「Security framework for cloud computing」 문서는 CSA 및 ENISA와는 다르게 클라우드 컴퓨팅 환경에서의 보안위협과 더불어, 해당 보안위협이 클라우드 서비스 참여자별 발생 가능한 경우를 구분한다.

이때, CSP는 CSC와 비즈니스 관계를 갖기 때문에 CSP 뿐만 아니라 CSC의 보안위협 또한 고려하여 안전하게 서비스를 제공할 필요가 있다. 이에 따라, CSC 및 CSP에게 발생 가능한 보안위협은 <표 2>와 같다[7].

<표 2> CSC 및 CSP의 보안위협

No	ITU-T보안위협	CSC	CSP
1	데이터 손실과 유출	✓	
2	불안전한 서비스 접근	✓	
3	내부자 위협	✓	✓
4	비인가된 관리자 접근		✓
5	책임의 모호성	✓	✓
6	신뢰의 손실	✓	
7	기밀성 손실	✓	
8	프라이버시 손실	✓	
9	서비스 비가용성	✓	
10	클라우드 서비스 제공자 종속	✓	
11	지적재산권 남용	✓	
12	소프트웨어 무결성 손실	✓	
13	공유된 환경		✓
14	보호 매커니즘 충돌		✓
15	관할 충돌		✓
16	점진적 위험		✓
17	잘못된 마이그레이션 및 통합		✓
18	비즈니스 불연속성		✓
19	클라우드 서비스 파트너 종속		✓
20	공급 체인의 취약점		✓
21	소프트웨어 종속성		✓

3. 제안방안

3.1 클라우드 네트워크 가상화 보안위협

2.3 및 2.4절에서 분석한 내용을 바탕으로 CSC 및 CSP가 클라우드 네트워크 가상화 서비스 활용 시 발생 가능한 직접 및 간접적 보안위협을 도출한 결과는 <표 3>과 같으며, 각 보안위협에 대한 설명은 아래와 같다. 이때, 직접적인 보안위협은 클라우드 네트워크 자원을 활용하는 참여자의 실질적인 자산을 해치는 위협이다. 또한, 간접적 보안위협은 클라우드 네트워크 가상화 서비스 운영 과정에서 발생하는 문제로, 이는 직접적 위협을 야기할 수 있다[7].

• T1. 데이터 유출

가상화된 네트워크상에서 전송되는 데이터가 공격자에 의해 탈취되어 유출 및 손실될 수 있다. 이는 프라이버시와 같은 중요 정보의 누설 등 간접적 위협을 야기한다.

<표 3> CSC 및 CSP가 클라우드 네트워크 가상화 서비스 활용 시 발생 가능한 보안위협

No	보안위협	위협 구분	관련 보안위협		
			CSA	ENISA	ITU-T
T1	데이터 유출	직접	데이터 유출 데이터 손실	데이터 유출 정보 누설	데이터 손실과 유출
T2	서비스 비가용성	직접	서비스 거부	서비스 거부	서비스 비가용성 비즈니스 불연속성
T3	악성코드	직접	APT 클라우드 서비스 남용	악성코드 웹기반 공격 봇넷	-
T4	비인가된 접근	간접	부적절한 신원 공유된 기술의 취약점	웹 응용 프로그램 공격 신분 도용	불안전한 서비스 접근 비인가된 관리자 접근 보호 매커니즘 충돌 공유된 환경
T5	소프트웨어적 취약점	간접	불안전한 API	-	소프트웨어 무결성 손실 점진적 위험 공급 체인의 취약점 소프트웨어 종속성
T6	부적절한 마이그레이션	간접	-	-	잘못된 마이그레이션 및 통합

• T2. 서비스 비가용성

DDoS 공격 등의 네트워크 공격을 통해 클라우드 서비스의 가용성이 침해 될 수 있다. 이때, 사용자는 서비스를 사용할 수 없게 되며 이는 비즈니스의 불연속을 야기한다.

• T3. 악성코드

악성코드 자체는 데이터 유출, 서비스 비가용성 등을 발생시키는 직접적 보안위협이 될 수 있다. 악성코드를 이용한 공격으로 웹 기반 악성코드, 봇넷, APT 등이 포함된다. 또한, 클라우드 서비스의 저조한 보안 등의 서비스 남용은 클라우드 컴퓨팅 모델을 악성코드 공격에 노출시킨다.

• T4. 비인가된 접근

클라우드 환경은 네트워크 자원을 포함한 인프라 자원을 여러 사용자가 공유하기 때문에 다른 환경에 비해 자원에 대한 무단 접근이 발생하기 쉽다. 이는 직접적 보안위협 유발을 목적으로 계정 도용 등을 통해 부적절한 신원을 갖는 사용자가 접근권한을 갖는 경우 발생 가능하다.

• T5. 소프트웨어적 취약점

네트워크 가상화는 소프트웨어를 기반으로 네트워크 기능이 구현되기 때문에 불안전한 API 등으로 인해 데이터 유출, 비인가된 접근 등 직접 및 간접적 보안위협 모두 발생할 수 있다.

• T6. 부적절한 마이그레이션

클라우드 환경에서의 마이그레이션은 네트워크 자원의 변경을 필요로 한다. 따라서, 부적절한 마이그레이션 과정에서 데이터 유출 등의 보안위협이 발생할 수 있다.

3.2 클라우드 네트워크 가상화 보안요구사항

3.1절에서의 보안위협을 바탕으로 안전한 클라우드 네트워크 가상화 서비스를 위해 도출한 보안요구사항은 <표 4>와 같고 각 보안요구사항에 대한 설명은 아래와 같다.

<표 4> 클라우드 네트워크 가상화 보안요구사항

No	보안요구사항	관련 보안위협					
		T1	T2	T3	T4	T5	T6
R1	접근제한	✓	✓	✓	✓		
R2	악성코드 차단	✓	✓	✓	✓		
R3	소프트웨어 API 모니터링	✓	✓	✓	✓	✓	✓
R4	사고 모니터링	✓	✓	✓	✓		✓
R5	서비스 거부 방지		✓				✓

• R1. 접근제한

데이터 유출, 부적절한 마이그레이션 등을 방지하기 위해 비인가된 사용자에 대한 네트워크 가상화 시스템 및 이를 통해 전송되는 데이터에 대한 접근제한이 필요하다.

• R2. 악성코드 차단

클라우드 서비스 제공, 마이그레이션 등의 과정에서 악성코드 차단을 통해 악성코드 공격으로부터 발생할 수 있는 데이터 유출, 서비스 가용성 침해 등을 방지할 수 있다.

• R3. 소프트웨어 API 모니터링

소프트웨어 기능에 대한 모니터링을 통해 소프트웨어적인 취약성에 의해 발생 가능한 다양한 보안위협으로부터 네트워크 가상화 자원을 보호할 수 있다.

<표 5> 클라우드 네트워크 가상화 서비스의 안전한 제공을 위해 CPS 관점에서 보안요구사항을 만족시키는 정책방안

No	보안요구사항	설 명
R1	접근제한	- 접근제한을 통해 CSC가 사용하는 클라우드 네트워크 가상화 시스템 및 데이터에 대한 비인가된 접근 차단 - 데이터 유출, 서비스 비가용성, 악성코드 공격 등의 추가적인 직접적 보안 위협을 방지
R2	악성코드 차단	- CSC 및 CSP에 대한 악성코드 공격 차단 - 악성코드 공격으로 발생 가능한 데이터 유출, 서비스 비가용성, 비인가된 접근을 방지
R3	소프트웨어 API 모니터링	- 접근제한, 마이그레이션, 패킷 스위칭 등 클라우드 네트워크 가상화 서비스 기능을 구현하는 소프트웨어 API를 모니터링 - 소프트웨어 취약점의 보안위협으로부터 발생 가능한 직접 및 간접적 보안위협 방지
R4	사고 모니터링	- 데이터 유출, 서비스 비가용성, 부적절한 마이그레이션 등의 직접 또는 간접적 보안위협에 따른 보안사고 발생 사항을 모니터링 - 보안사고 발생 시 즉각적 대응 필요
R5	서비스 거부 방지	- CSC는 공유된 클라우드 네트워크 가상화 자원을 사용 - 서비스 거부 공격에 따른 위험도가 비교적 높기 때문에 별도의 서비스 거부 방지 기술이 요구됨

• R4. 사고 모니터링

악성코드 공격, 데이터 유출, 부적절한 마이그레이션 등 직접 및 간접적 보안위협으로 인해 클라우드 네트워크 가상화 환경에서 보안사고가 일어났을 경우 사고 모니터링을 통해 신속히 대응할 수 있다.

• R5. 서비스 거부 방지

인프라 자원이 공유된 클라우드 환경에서의 가용성 침해가 발생할 경우 다른 환경에 비해 피해 규모가 크기 때문에 별도의 서비스 거부 방지 기술이 필요하다.

3.3 정책 방안

2.2절에서 분석한 내용에 따라 CSP는 서비스를 제공하는 세부 역할에 따라 세부 주체로 구분되며, 제공되는 서비스에 대해 보안적 측면에서 관리 및 운영하는 주체로는 서비스 보안 및 위험 관리자가 있다. 서비스 보안 및 위험 관리자는 CSP의 다른 세부 주체들이 서비스를 제공하는 과정에서 발생 가능한 보안 위협들을 관리해야한다. 클라우드 네트워크 가상화 서비스 제공 측면에서 관리해야할 해당 보안위협은 3.1절에서 도출한 CSC 및 CSP 관점에서의 보안위협으로 정의할 수 있다.

이에 따라, CSP가 클라우드 네트워크 가상화 서비스를 제공하는 과정에서 서비스 보안 및 위험 관리자는 적절한 보안요구사항을 고려해야할 필요가 있다. 해당 보안요구사항은 3.1절에서 도출한 보안위협을 바탕으로 3.2절에서 재도출한 클라우드 네트워크 가상화 보안요구사항으로 정의할 수 있다. 결과적으로, 클라우드 네트워크 가상화 서비스을 안전하게 제공하기 위해 CSP가 보안요구사항을 만족시키는 정책방안은 <표 5>와 같다.

4. 결론

본 논문은 CSC에게 클라우드 네트워크 가상화 서비스를 안전하게 제공하기 위해 CSP 측면에서의 정책방안을 연구하였다. 이를 위해, 기존의 클라우드 컴퓨팅 환경에서의 보안위협과 ITU-T에서 제시한 사항 중 CSC와 CSP의 역할에 따른 보안위협을 바탕으로 클라우드 네트워크 가상화 환경에서 발생 가능한 보안위협을 도출하였다. 더불어, 이를 통해 CSP가 클라우드 네트워크 가상화 서비스 제공시 만족해야 할 보안요구사항을 도출하였다. 결과적으로, 클라우드 네트워크 가상화 서비스의 안전한 제공에 있어 정책 마련 시, CSP는 발생 가능한 각 보안위협에 따라 해당 보안요구사항들을 고려해야한다.

최근 클라우드 가상화 환경에서의 보안위협이 증가하고 있기 때문에 이를 위한 정책 마련이 필요하다. 이에 따라, 본 논문이 추후 안전한 클라우드 가상화를 위한 정책 마련에 적극 활용 될 것으로 기대한다. 향후 연구로는 안전한 클라우드 가상화를 위한 각 참여자별 측면과 클라우드의 다른 가상화 인프라 측면에서의 정책 연구를 진행할 예정이다.

참고문헌

[1] 이강찬, 이승윤, 양희동, “Standardization Trends and Strategies on Cloud Computing”, 2012.09.19.

[2] Yeong-hun Oh 4et.al, “Trends in Domestic and International Standardization of Cloud Computing”, 2014.08.

[3] 정상진, 신명기, 김형준, “미래인터넷을 위한 네트워크 가상화 표준기술 개발 동향”, 한국통신학회지 제27권 제10호, 2010.09.

[4] ISO/IEC 17789:2014, “Information Technology Cloud Computing Reference Architecture(CCRA)”, 2014.

[5] ENISA, “Threat Landscape 2015”, 2016.01.

[6] CSA, “Cloud Computing Top Threats in 2016”, 2016.02.

[7] ITU-T X.1601, “Security framework for cloud computing”, 2015.10.