클라우드 기반 보안서비스 기술 동향

정 수 환
숭실대학교

Ⅰ. 서 론

클라우드 컴퓨팅은 인터넷 기술을 활용하여 IT 자원을 서비스로 제공하는 컴퓨팅으로 사용자의 요구에 대해 최소한의 관리를 통해 손쉽게 IT 자원(서버, 데스크탑, SW, 스토리지, 네트워크 등)을 제공한다[1]. 클라우드 컴퓨팅은 컴퓨팅 인프라를 서비스하는 Infrastructure as a Service (IaaS), 플랫폼을 서비스하는 Platform as a Service (PaaS), 애플리케이션 소프트웨어를 서비스하는 Software as a Service (SaaS)의 3가지 형태로 나뉘어 제공되었다. 또한 클라우드 컴퓨팅이 급속하게 확장됨에 따라 컴퓨팅에 대한 패러다임의 변화를 가져왔으며, 더 나아가 다양한 형태의 클라우드 서비스로 변화되고 있으며 Anything as a Service (XaaS)로 정의하고 있다. 이러한 클라우드 컴퓨팅의 확장은 보안에서도 변화를 가져오고 있다. 기존에 Security Appliance 형태로 제공되었던 보안서비스가 클라우드 컴퓨팅과 결합을 통해 하나의 클라우드 보안서비스로 제공되는 Security as a Service (SecaaS)가 등장하고 있다. 가트너에서 조사한 클라우드 기반 보안서비스의 시장은 2016년까지 4.2 억불에 달할 것으로 예상하고 있으며 2013년에는 기존의 보안 시장을 앞설 것으로 보고 있다[2]. 클라우드 컴퓨팅은 보안의 변화를 이끌고 있으며, 전문적이고 체계적인 보안서비스를 요구하고 있다. 최근 3 · 20과 같은 사이버 테러는 이러

클라우드 컴퓨팅이 급속하게 확장됨에 따라 컴퓨팅에 대한 패러다임의 변화를 가져왔으며, 더 나아가 다양한 형태의 클라우드 서비스로 변화되고 있으며 Anything as a Service (XaaS)로 정의하고 있다.

한 요구를 가속화하고 있다.

본고에서는 클라우드 기반 보안서비스인 SecaaS의 기술 동향과 국제 표준화 추세, 그리고 클라우드 보안 서비스 동향에 살펴봄으로써 앞으로 보안서비스에 대한 변화에 대해 소개하고자 한다.

Ⅱ. Security as a Service

1. CSA (Cloud Security Alliance)

CSA는 클라우드 컴퓨팅에서의 보안 이슈를 해결하기 위한 비영리 단체로서 2008년 ISSA(Information Systems Security Association) CISO 포럼을 계기로 하여 설립되었으며, 클라우드 컴퓨팅에서의 9가지의 Top Threats를 정의하였으며, 이에 대한 보안 가이드를 14가지의 도메인으로 나누어 제시하고 있다.

우선 클라우드 컴퓨팅에서의 9가지 위협은 〈표 1〉과 같다[3].

클라우드 컴퓨팅에 대한 위협들은 클라우드 컴퓨팅을 적용하는데 있어서 걸림돌이 되어 왔다. 이와 같은 보안 이슈를 해결하기 위한 노력들이 계속되고 있으며, CSA에서는 클라우드 컴퓨팅에서의 보안 위협들을 고려하여 보안 가이드를 제시하고 있다. CSA에서 제시한 14가지 도메인은 〈표 2〉와 같다[4].

〈표 1〉 Cloud Computing Top Threats

위 협	내 용
Data Breaches	가상머신에서의 side channel 공격 등으로 인한 데이터 침해
Data Loss	해킹, 재해 등의 사고로 인한 데이터 손실이나 유출
Accounting Hijacking	피싱, 사기 등 공격으로 인한 계정 강탈
Insecure APIs	CSP의 정책을 우회하는 위협
Denial of Service	DoS나 DDoS 공격으로 인한 클라우드 서비스 방해
Malicious Insider	악의적인 내부자에 대한 위협
Abuse of Cloud Services	클라우드 서비스를 이용한 공격
Insufficient Due Diligence	클라우드 컴퓨팅에 대한 이해부족
Shared Technology Issues	가상화를 통한 리소스 공유 기술에 대한 취약점

〈표 2〉 Security Guidance for Critical Areas of Force in Cloud Computing

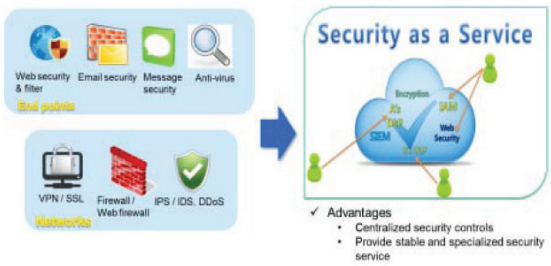
도메인	내 용
Cloud Computing Architectural Framework	클라우드 컴퓨팅의 아키텍처 구조에 대한 이해
Governance and Enterprise Risk Management	기업 위험을 관리, 측정하는 조직의 능력
Legal Issues: Contracts and Electronic Discovery	잠재적인 법적 이슈
Compliance and Audit Management	컴플라이언스 유지 및 제공
Information Management and Data Security	클라우드에서의 데이터 관리
Interoperability and Portability	데이터/서비스의 이전
Traditional Security, Business Continuity, and Disaster Recovery	운영 프로세스 절차에 대한 영향
Data Center Operations	데이터 센터 아키텍처, 운영 이슈
Incident Response	사건처리와 감식 이슈
Application Security	보안 애플리케이션 이슈
Encryption and Key Management	자원 접근, 데이터 보호 이슈
Identity, Entitlement, and Access Management	식별정보 관리, 디렉터리 서비스 이슈
Virtualization	시스템/하드웨어 가상화 이슈
Security as a Service	클라우드 컴퓨팅을 기반으로 한 전문 보안서비스

특히 CSA에서는 SecaaS 워킹그룹을 통해서 클라우드 기반 보안서비스 구현을 위한 가이드를 제시하고 있다. CSA에서는 Identity and Access Management (IAM), Data Loss Prevention (DLP), Web Security, Email Security, Security Assessments, Intrusion Management (IM), Security Information and Event Management (SIEM), Encryption, Business Continuity and Disaster Recovery (BCDR), Network Security의 총 10개 카테고리로 구분하여 클라우드 서비스로 구현 시에 고려 사항과 문제점들에 대해 자세히 설명하고 있다[5].

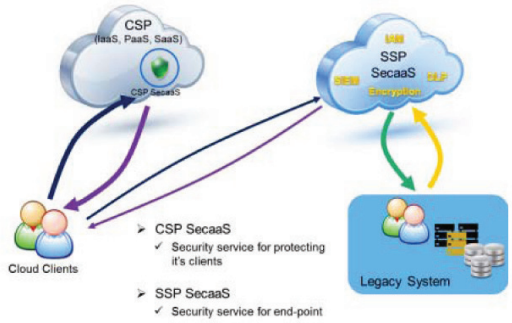
2. 보안 패러다임의 변화

기존의 보안은 Regacy System의 구조를 고려하여 다양한 형태의 제품들을 추가하여 보안 위협으로부터 각종 시스템들을 보호해왔다. 네트워크에서는 VPN/SSL, Firewall, Web Firewall, IPS/IDS, Anti-DDoS 시스템 등이 있으며, 엔드 포인트에서는 Web Security & Filter, Email Security, Message Security, Anti-virus, DB encryption 등 다양한 형태의 보안제품들이 있다. 이러한 보안제품들은 안전한가? 대답은 그렇지 않다. 아직 알려지지 않은 취약점들이 많이 있으며, 이기종 보안 제품들 간의 중복된 기능이 많으며 또한 제품들 간에 충돌되는 문제도 있다. 무엇보다 보안을 일정한 수준으로 관리하고 유지한다는 것은 여간 어려운 일이 아니라는 것이다. 많은 시스템들을 모니터해야 하며 다양한 보안 시스템 사용을 위한 지속적인 교육이 필요하다.

기업에게 있어서 보안은 어려운 문제로 인식되고 있으며 법적 책임이 강화되면서 꼭 해결해야 하는 문제이기도 하다. 최근 ESG Research에서 실시한 설문조사에 따르면 기업의 56%가 보안을 서비스로 제공받고 싶어 하며, 39%는 전문 보안서비스 제공자가 수행하는 것이 더 안전하다고 생각한다. 또한 기업의 29%는 전문 보안 인력을 확보하기 어렵다고 하며, 새로운 보안 위협에 대응하기 위해 외부 전문가에 의존하고 있다고 한다[6]. 설문조사에서도 알 수 있듯이 전문 보안서비스에 대한 요구가 높아지면서 보안에 대한 패러다임이 변화되고 있다. 〈그림 1〉에서와 같이 기존의 Security Appliance 기반에서 클라우드 기반의 보안서비스로 변화되고 있다.



〈그림 1〉 보안 패러다임의 변화



〈그림 2〉 SecaaS Architecture

보안 패러다임의 변화에 따라 CSA에서 제시한 보안 가이드에서 Security as a Service가 추가되었다. 또한 클라우드의 보안도 클라우드 컴퓨팅의 자체 보안을 위한 보안 플랫폼과 보안서비스로 구분된다. 보안 플랫폼은 클라우드 컴퓨팅 모델의 구조를 있어서의 취약점을 고려하고 있으며, 보안서비스는 체계적이고 일정한 보안 수준으로 관리하는 전문 보안서비스이다.

3. Security as a Service

SecaaS는 SaaS의 한 종류로써 소프트웨어 형태의 보안서비스이다. 클라우드 컴퓨팅의 Remote Access, Low Cost, Centralized Management, Reduce Vulnerability와 같은 장점을 바탕으로 클라우드 기반의 보안서비스로 발전되고 있다. SecaaS는 〈그림 2〉와 같이 크게 CSP에 의한 SecaaS와 Security Service Provider(SSP)에 의한 SecaaS로 구분되어 진다. CSP SecaaS는 클라우드 서비스 제공자가 자신의 클라우드 시스템을 이용하는 사용자들을 보호하기 위해 제공되는 서비스이고, SSP SecaaS는 전문 보안서비스 제공자가 제3자에게 제공되는 서비스이다.

Ⅲ. 국제 표준화 동향

CSA에서는 클라우드 보안, 클라우드 기반 보안서비스 등 보안 이슈에 관련하여 국제 표준화를 추진하고 있다. 국제 표준화 단체인 ISO/IEC, ITU-T에서 진행되고 있는 표준들은 〈표 3〉과 같다[7-8].

먼저 ISO/IEC JTC 1/SC 27 그룹에서는 IT 보안

〈표 3〉 International Standards for Cloud Security

ISO/IEC의 JTC 1/SC 27	
27017	ISO/IEC 27002을 기반으로 클라우드 컴퓨팅 서비스를 위한 정보보안통제의 실천지침
27018	퍼블릭 클라우드 컴퓨팅 서비스에서 개인 식별 정보를 보호하기 위한 실천지침
27036-X	클라우드 컴퓨팅 공급자와의 관계에 대한 정보보안
ITU-T의 FG Cloud	
X.ccsec	클라우드 컴퓨팅에 대한 높은 수준의 보안 프레임워크
X.sfcse	SaaS 애플리케이션 환경에 대한 보안기능 요구사항
X.idmcc	클라우드 컴퓨팅에서의 식별자 관리를 위한 요구사항

기술에 대한 표준화를 다루고 있으며, 클라우드 컴퓨팅에 대한 보안 관련해서는 아래와 같다.

- 27017 : ISO/IEC 27002를 기반으로 하여 클라우드 컴퓨팅에 대한 정보보안통제 지침으로 클라우드 서비스 사용자/소비자/고객과 클라우드 서비스 제공자 모두에 대한 정보보안 지침을 제공한다.
- 27018 : 퍼블릭 클라우드 컴퓨팅 서비스에 대한 개인정보보호 요소에 대한 지침을 제공하며 개인 데이터 보안의 맥락에서의 해석을 의미한다.
- 27036-X : 클라우드 공급 체인과 관련된 부분을 포함하여 공급자의 관계 관리를 위한 정보보안 지침으로 IT 아웃소싱, 클라우드 서비스 매입사와 공급자에 대한 가이드를 제공한다.

다음으로 ITU-T의 FG Cloud는 클라우드 컴퓨팅에 관한 국제 표준을 추진하고 있으며 클라우드 컴퓨팅의 보안 이슈에 관한 표준은 아래와 같다.

- X.ccsec : 클라우드 보안 위협, 보안 요구사항과 보안 영역에 대한 분석을 바탕으로 클라우드 컴퓨팅에 대한 높은 수준의 보안 프레임워크로 클라우드 컴퓨팅 구조의 각 기능블록 별로 필요한 보안 기능을 식별하기 위한 방법을 제공한다.
- X.sfcse : 네트워크 유형, 운영체제, 미들웨어 등 SaaS 애플리케이션의 환경을 고려한 보안서비스의 일반적 기능을 제공한다. 또한 안전하고 관리 가능한 서비스를 정의, 설계, 구현하기 위한 구조적 접근방식에 대해 설명하고 있다.
- X.idmcc : 클라우드 컴퓨팅 환경에서 통신 서비스들의 조화에 초점을 맞추고 있다. 사용사례와 요구사항 분석을 시작으로 공통 식별자 관리 인프라를 기반으로 통신 서비스들과 인터넷 서비스들 간의 조화를 위한 기준을 제시한다.

CSA에서는 클라우드 보안, 클라우드 기반 보안서비스 등 보안 이슈에 관련하여 국제 표준화를 추진하고 있다.

지금까지 클라우드 컴퓨팅을 도입하는데 있어 보안이슈는 큰 걸림돌이 되어 왔다. 이에 따라 국제 표준단체에서는 클라우드 컴퓨팅에서의 보안위협을 줄이기 위한 표준들이 진행하고 있으며 그 결과 클라우드 컴퓨팅에 대한 인식이 변화됨에 따라 확산이 가속화되고 있다.

Ⅳ. 클라우드 기반 보안서비스 동향

앞에서 언급했듯이 SecaaS는 크게 CSP SecaaS와

〈그림 3〉 클라우드 컴퓨팅 서비스 현황

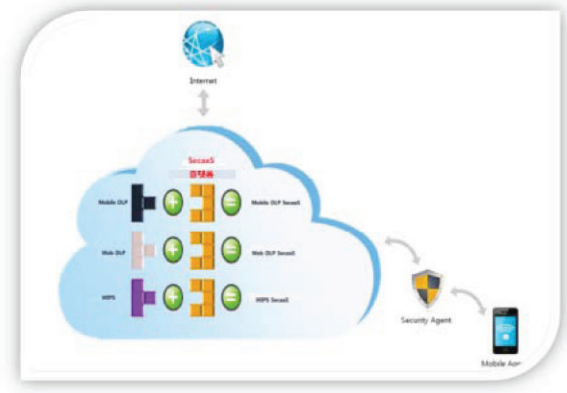
SSP SecaaS로 구분되고 있으며 이에 대한 보안서비스 동향에 대해 알아보고자 한다.

1. CSP SecaaS 동향

클라우드 컴퓨팅이 확산됨에 따라 다양한 서비스들이 〈그림 3〉과 같이 제공되고 있다[4]. CSP SecaaS는 클라우드 서비스 제공자들이 자신들이 제공하는 서비스를 안전하게 보호하기 위해 제공되는 서비스들이다. 기존에는 자연재해, 관리자 실수 그리고 시스템 에러에 의한 서비스 중단 사고들이 주로 발생되었으며 이로 인해 지속적인 서비스 보장과 재해복구를 위한 BCDR, SIEM과 같은 서비스에 관심이 많았다. 최근 Apple, Dropbox, Evernote의 클라우드 서비스들이 해킹에 의해 데이터 유출 및 손실이 발생되었으며, 후지쯔의 경우 DoS 공격에 의해 서비스가 중단되는 사고가 발생하

〈표 4〉 SSP SecaaS 서비스 현황

구 분	서비스 종류
IAM	Pendo systems (CA Arcot Webfort) McAfee(Cyber Ark Software Privileged Identity Manager) NetIQ(Nevell Cloud Security Services)
Web Security	BlueCoat(Cloud Service), RSA(Silver Tail), TrendMicro(Titanium), Websense(Triton), zScaler(NanoLog)
DLP	Symantec(Data Loss Prevention) Websense(Data Seucriyt Suite) Zenprise(XenMobile MDM) zScaler(Data Protection)
Email Security	Gmail, TrendMicro, Zscaler(NanoLog), McAfee, Microsoft(Cloud Services)
Security Assessments	Agiliance(Risk Vision), Qualys(Qualys Guard), Core Security(Impact), Modulo(Risk Manager), Veracode, WhiteHat(SucessFactors)
IM	Cymtec Scout(SNORT), Sourcefire(Agile Security), StoneGate(Hyperglance), Symantec, TrendMicro(Titanium)
Encryption	Credant, Cypher Cloud, enStratus, Novaho, Perpecsys
BCDR	EMC(Atmos), Decco, Digital Prallels, Rackspace
Network Security	CloudFlare, Imperva(MX Management), Rackspace, Symantec(7100 Series), Stonesoft (NGTIV)



〈그림 4〉 SecaaS Platform Architecture

면서 IAM, DLP, IM, 암호화, 네트워크 보안 등에 대한 서비스들이 제공되고 있다.

2. SSP SecaaS 동향

SSP SecaaS는 기존 클라우드 컴퓨팅 서비스, 레거시 시스템 등 모든 시스템을 대상으로 제공되는 전문 보안서비스이다. SSP SecaaS 형태의 서비스를 제공하는 제공자와 서비스 현황은 〈표 4〉와 같다[5].

SSP SecaaS 제공자들은 기존의 Security Appliance 솔루션을 제공하는 업체들로서 최근에는 클라우드 컴퓨팅을 도입하여 기존 Security Appliance에서 클라우드 보안서비스를 제공하기 시작하였다. 전문적으로 관리되는 보안서비스에 대한 요구가 증가됨에 따라 기존 보안 업체들도 빠르게 클라우드 컴퓨팅을 도입하고 있다. 가트너에서의 보안 시장 조사에서와 같이 클라우드 기반 보안서비스들이 계속해서 성장해 나갈 것으로 예상된다.

또한 SecaaS 플랫폼에 대한 서비스로 확장되어 나갈 것이다. 지금까지는 각 카테고리별로 독자적인 보안서비스를 제공하고 있다. 하지만 많은 기업들은 시스템 전반에 걸쳐 체계적인 보안서비스를 원하고 있다. 따라서 〈그림 4〉와 같이 SecaaS 플랫폼을 통해 SecaaS 형태의 다양한 보안서비스를 고객이 원하는 대로 패키지하여 제공 되어질 것이다. SecaaS 플랫폼 서비스는 통합 보안서비스로 기업들의 보안에 대한 고민을 해결할 솔루션으로 예상된다.

V. 향후 연구 동향

클라우드 기반 보안서비스에 대해 개념에 대해 살펴봤으며, 클라우드 컴퓨팅으로 인한 보안 패러다임의 변화는 클라우드 기반 보안서비스에 대한 요구를 증대시키고 있다. 이러한 클라우드 기반 보안서비스는 크게 두 가지 형태로 구분되며, CSP SecaaS는 기존 클라우드 서비스 제공자가 자신의 안전한 서비스 제공을 위한 보안서비스이며, SSP SecaaS는 모든 시스템들에 대해 전문적인 보안서비스를 제공하기 위한 서비스이다. 하지만 지금까지 클라우드 컴퓨팅에 대한 보안 이슈는 클라우드 컴퓨팅을 도입하는데 있어 커다란 걸림돌이 되어 왔으나 국제 표준단체에서의 클라우드 컴퓨팅에서에 대한 보안 위협을 줄이기 위한 표준들을 추진함으로써 클라우드 컴퓨팅이 빠르게 확산되고 있다. 전문 보안업체들도 클라우드 컴퓨팅을 도입함에 따라 기존 Security Appliance 기반에서 클라우드 기반 보안서비스로 확장하고 있다. 지금까지 클라우드 기반 보안서비스는 각 카테고리별로 각각의 전문 서비스로 제공되고 있다. 즉, SaaS와 같은 애플리케이션 서비스로 제공되고 있다. 하지만 다양한 전문 보안서비스를 제공하기 위한 플랫폼 개발로 확장될 것으로 예상된다. 시스템 전체에 대해 전문적으로 관리할 수 있는 보안서비스를 고객이 원하는 대로 패키지하여 제공할 수 있는 SecaaS 플랫폼으로 발전될 것이다. 하지만 여러 보안서비스를 패키지 시에 보안서비스 간에 안정적인 조화에 대해 반드시 고려해야 할 것이다.

시스템전체에 대해 전문적으로 관리할 수 있는 보안서비스를 고객이 원하는 대로 패키지하여 제공할 수 있는 SecaaS 플랫폼으로 발전될 것이다.

클라우드 기반 보안서비스는 앞으로의 보안서비스 시장을 바꾸고 있으며, 체계적이고 전문적인 보안서비스를 통해 더 안전하고 견고한 보안서비스를 제공함으로써 보안 패러다임의 변화를 이끌어 나갈 것으로 예상된다.

참 고 문 헌

[1] Peter Mell and Timothy Grance, The NIST Definition of Cloud Computing, Sep. 2011.

[2] Ruggero Contu and Kelly M. Kavanagh, Market Trends: Cloud-based Security Services Market, Worldwide, 2012, Sep. 2012

[3] Top Threats WG, The Notorious Nine Cloud Computing Top Threats, CSA, Feb. 2013.

[4] Chris Hoff and others, Security Guidance for Critical Areas of Focus in Cloud Computing, CSA, Jul. 2011.

[5] SecaaS WG, Defined Categories of Service, CSA, Oct. 2011.

[6] Jon Oltsik, Why is Cisco Getting into Security Services?, ESG Research, Sep. 2013.

[7] ISO 27001 Security, http://www.iso27001security.com/index.html

[8] ITU-T, http://www.itu.int/en/Pages/default.aspx

정 수 환

1985년 2월 서울대학교 전자공학과 졸업
1987년 2월 서울대학교 전자공학과 석사
1996년 6월 University of Washington 박사
1988년 3월~1991년 7월 한국통신 전임연구원
1996년 6월~1997년 2월
Stellar One Corp. Senior Engineer
2006년 1월~2007년 12월
한국연구재단 Program Manager
2009년 3월~2011년 2월
지식경제부 Program Director
1997년 3월~현재 숭실대학교 정보통신전자공학부 교수

〈관심분야〉
이동 및 무선 네트워크 보안, VoIP 보안, SNS 보안, 클라우드 보안