情 報 保 護 學 會 誌
第22卷 第7號, 2012. 11

Security as a Service 동향

이 종 훈*, 정 승 욱**, 정 수 환**

요 약

본고에서는 최근 클라우드 컴퓨팅이 갖고 있는 보안 기술 동향에 대하여 살펴본다. 특히 클라우드 컴퓨팅이 갖는 보안 위협들을 해결하기 위한 대응책으로 SecaaS(Security as a Service)에 관심이 집중되고 있다. SecaaS는 클라우드 컴퓨팅의 보안 솔루션을 클라우드 컴퓨팅 서비스의 한 형태로 제공하여 안전성과 신뢰성을 보장한다. CSA(Cloud Security Alliance)에서는 클라우드 컴퓨팅 환경의 보안 위협들에 대해 분석하여 클라우드 보안 가이드를 제시했으며, 최근 SecaaS 워킹그룹에서는 10개의 카테고리로 구분하여 보안 솔루션을 구현하기 위한 구체적인 가이드 제시하고 있다. 먼저 전반적인 클라우드 컴퓨팅의 보안 위협에 대해 살펴보고, 이에 대한 해결방안으로 제시되는 SecaaS 기술에 대해 살펴본다.

Ⅰ. 서 론

클라우드 컴퓨팅은 차세대 컴퓨팅 환경으로 주목받고 있는 기술로서 언제 어디서나, 편하게, 구성이 가능한 컴퓨팅 자원(네트워크, 서버, 스토리지, 서비스 등)들이 공유된 풀에 온디멘드 네트워크 접근이 가능한 모델이다. 이 컴퓨팅 자원들은 최소한의 관리 노력 혹은 서비스 제공자와의 상호 작용을 통해 사용자가 원할 때 신속히 제공되고 회수되어야 한다[1]. 네트워크, 서버, 스토리지, 서비스 등과 같은 컴퓨팅 자원들을 필요한 만큼 제공받아 사용하고, 사용한 만큼의 일정 비용을 지불하는 방식으로 관리비용을 절감할 수 있다는 장점을 가진다. 또한 소프트웨어/하드웨어 가상화 기술의 발전으로 다양한 형태의 서비스를 제공하고 있다. 하지만 클라우드 시스템이 갖는 구조적 특징으로 인해 기존 IT 시스템이 갖고 있는 보안 위협과 가상화 기술에 대한 새로운 보안 위협이 더해짐에 따라 이에 대한 대응책 마련이 시급하다. 대부분의 기업들은 클라우드 컴퓨팅이 갖고 있는 보안 위협으로 인해 클라우드 컴퓨팅 서비스의 안전성과 신뢰성에 대한 의문을 제기했다. 따라서 아마존, 구글 같은 글로벌 기업들과 국제 단체들은 클라우드 컴퓨팅이 가지고 있는 보안 위협을 해결위해 노력하고 있다. 특히 CSA (Cloud Security Alliance)에서는 클라우드 컴퓨팅의 보안 위협에 대해 심층적으로 분석하여 클라우드 보안 가이드를 제시했으며, 보안 솔루션 구현을 위한 SecaaS(Security as a Service)란 가이드를 제공하고 있다. SecaaS는 IAM(Indentity and Acess Management), DLP(Data Loss Pre- vention), Web Security, Email Security, Security Assessments, Intrusion Management, SIEM(Security Information and Event Management), Encryption, BCDR(Business Continuity and Dsiaster Recovery), Network Security로 구분하여 구체적인 가이드를 제시한다.

본고에서는 클라우드 환경의 보안 위협에 대해 살펴보고 이를 해결하기 위한 방안으로 관심이 집중되고 있는 SecaaS에 대해 살펴본다.

Ⅱ. 클라우드 환경의 보안 위협

클라우드 컴퓨팅은 기민한 탄력성, 측정 가능한 서비

본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었습니다.
(NIPA-2012-H301-12-4008)
* 숭실대학교 전자공학과 통신망보안연구실 (ttaz@ssu.ac.kr)
** 숭실대학교 스마트서비스보안연구센터 교수 (seungwookj@ssu.ac.kr)
** 숭실대학교 정보통신전자공학부 교수 (souhwanj@ssu.ac.kr)

〔표 1〕 CSA에서 제시한 클라우드 환경의 보안 이슈

보안 이슈	내 용
가버넌스와 기업 위험 관리	기업 위험을 관리, 측정하는 조직의 능력
법적 및 전자적 증거수집	잠재적인 법적 이슈
컴플라이언스 및 감사	컴플라이언스 유지 및 제공
정보 수명 주기 관리	클라우드에서 데이터를 관리
이식성과 상호 운용성	데이터/서비스의 이전
전통적 보안, 사업 계속성 및 재해 복구	운영 프로세스 절차에 대한 영향
데이터 센터 운영	데이터 센터 아키텍처, 운영 이슈
사고 대응, 고지 및 교정	사건처리와 감식 이슈
애플리케이션 보안	보안 애플리케이션 이슈
암호화 및 키 관리	자원 접근, 데이터 보호 이슈
식별정보 및 접근관리	식별정보 관리, 디렉터리 서비스 이슈
가상화	시스템/하드웨어 가상화 이슈

스, 온디맨드 셀프 서비스, 다양한 네트워크 접근, 가용성 등의 특성을 바탕으로 자원관리의 효율성, 다양한 접근성, 사용자의 편의성, 비용 절감 등 다양한 이점을 강조한다. 하지만 클라우드 컴퓨팅이 갖는 구조적인 특성으로 인해 기존의 보안 위협뿐만 아니라 새로운 형태의 보안 위협이 내제하고 있다. 이 보안 위협에는 하이퍼바이저, 운영체제, 네트워크, 스토리지, 관리자 등에 의한 보안 위협으로 구분할 수 있다. [2]에서는 클라우드 컴퓨팅이 가지고 있는 구조적 관점에서 보안위협을 보여준다. CSA에서는 클라우드 컴퓨팅이 갖고 있는 위협을 바탕으로 표 1에서와 같이 보안 이슈를 제시했고, 각 보안 이슈에 대한 대응 가이드도 제시한다.

한편, 가트너에서는 7가지 보안 위협을 클라우드 컴퓨팅 환경에서 확인해야 한다고 제시했으며 표 2와 같다.

위에서 언급된 클라우드 컴퓨팅에 대한 보안 이슈로 인해 많은 기업들이 클라우드 컴퓨팅 기술을 도입하는 것에 민감한 반응을 보이고 있다. 이에 따라 클라우드 보안 이슈를 해결하려는 노력이 계속 진행되고 있으며, 특히 CSA에서는 보안 이슈 해결을 위한 Security as a Service 워킹 그룹에서 보안 솔루션구현을 위한 구체적인 가이드를 제시하고 있다. 본고에서는 SeccaS 가이드에서 제시하고 있는 보안 기술 에 대해 구체적으로 살펴본다.

〔표 2〕 가트너에서 제시한 클라우드 환경의 보안 이슈

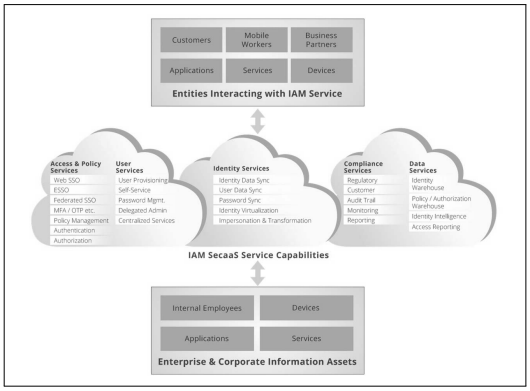
보안 이슈	내 용
특별 사용자 접근 관리	특권 관리자와 일반 사용자에 대한 철저한 관리
규정 준수성	외부 평가 및 감사, 점검 체계
데이터의 입지	데이터의 물리적 입지 (위치, 환경, 법적 이슈 등)
데이터의 격리	데이터의 암호화, 격리
복구 계획	문제 복구와 관련된 제반 활동
조사 가능성	보안사고 및 문제 조사 능력
장기적 경쟁력	안전성, 확장성, 대체 가능성

Ⅲ. 클라우드 환경의 Security as a Service

클라우드 컴퓨팅에서는 보안 이슈에 대한 해결 솔루션을 클라우드 컴퓨팅의 한 형태의 서비스로 제공하려고 한다. CSA SecaaS에서는 클라우드 컴퓨팅 서비스 사용자로부터 수집된 정보를 통해 10개의 카테고리로 구분하여 구체적인 가이드를 제시하고 있다. 각 카테고리의 의미와 보안 이슈에 대한 해결 기술에 대해 살펴보겠다.

1. Identity and Access Management

클라우드 컴퓨팅은 공유 풀에 있는 자원을 여러 사용자가 나누어 사용하는 멀티 테넌시의 특성을 가지고 있다. 또한 자원은 최소한의 관리를 통해 자동화하여 할당하고 관리한다. 즉 자원 접근에 대해 안전하고 효율적인 관리가 필요하며 관리 부재 시 다양한 보안 위협이 발생한다.



〔그림 1〕 SeccaS IAM의 기본 구조

〔표 3〕 SecaaS IAM의 핵심 기능과 보안 위협

핵심 기능	
√ Provisioning/de-provisioning of accounts	
√ Authentication (multiple forms and factors)	
√ Federated SSO & Web SSO	
√ Authorization	
√ Privileged user management	
√ Role Based Access	
√ Policy & regulatory compliance monitoring and management	
보안 위협	
√ Identity theft	√ Excess privileges / excessive access
√ Unauthorized access	
√ Privilege escalation	√ Delegation of authorizations / entitlements
√ Insider threat	
√ Non-repudiation	√ Fraud

여기서 보안 위협에는 신원 도용, 무단접근, 권한상승, 부인방지 등이 있으며, 해결 방안으로 계정관리, 안전한 인증 및 권한부여, 보안 정책 준수 및 관리, 모니터링 등의 다양한 기술이 적용되고 있다.

SecaaS IAM은 확실한 식별정보와 접근 관리를 제공한다. 사용자, 프로세스, 시스템의 식별정보에 대한 검증을 거쳐 엔터프라이즈 자원에 대한 접근 및 접근 권한을 관리한다. 또한 식별정보 인증의 성공 및 실패, 자원 접근에 대한 로그 감시를 응용 소프트웨어로 제공한다[4]. SecaaS IAM에서는 신원 확인과 인증 관리에 필요한 요소를 분석하고 안정적인 아키텍처를 제시하며 그림 1과 같다. SecaaS IAM의 핵심 기능과 보안 위협은 표 3과 같다.

2. Data Loss Prevention

클라우드 서비스는 여러 사용자의 데이터를 공유 자원 풀에서 안전하게 저장, 관리한다. 즉, 사용자 데이터는 제3의 서비스 제공자가 제공하는 분리된 공간에 저장, 관리됨에 따라 다양한 위협이 존재한다. 위협 요소에는 데이터 손실 및 유출, 무단 접근, 데이터 소유권, 데이터 위변조 등이 있으며, 대응책으로는 데이터 라벨링과 분류, 암호화, 전자서명 등의 기술을 적용하고 있다.

SecaaS DLP 기술은 데이터의 모니터링 및 보호, 보안 검증을 제공한다. 데이터 상태를 in-use(endpoint action), in-motion(network traffic), at-rest(data storage)로 구분하며 각 상태마다 데이터를 안전하게 저장, 관리한다[5]. SecaaS DLP 기술의 핵심 기능과 보안 위협은 표 4와 같다.

〔표 4〕 SecaaS DLP의 핵심 기능과 보안 위협

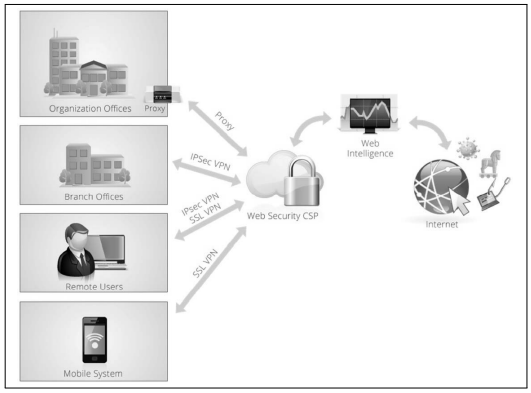
핵심 기능
√ Data labeling and classification
√ Identification of Sensitive Data
√ Structured Data Matching (data-at-rest)
√ Traffic Spanning (data-in-motion) detection
√ Signing of Data
√ Cryptographic data protection & access control
보안 위협
√ Data loss/leakage
√ Unauthorized access
√ Malicious compromises of data integrity
√ Data sovereignty issues
√ Regulatory sanctions and fines

3. Web Security

클라우드 서비스는 기본적으로 사용자의 쉬운 사용과 접근성을 제공하기 위해 웹 서비스를 사용한다. 웹 환경에서의 보안 위협에는 키로거, 멀웨어, 스파이웨어, 피싱, 바이러스, 스팸 등이 있으며 대응책으로는 웹 필터링, 피싱 사이트 블락, 멀웨어 및 스파이웨어 블락 등의 기술들이 있다. SecaaS Web Security은 실시간으로 웹 트래픽을 보호하는 솔루션으로 클라우드의 가상화 특성을 고려하여 가이드를 제공한다. 그림 2는 SecaaS Web Security의 기본 구조를 보여주며, 핵심 기능과 보안 위협은 표 5와 같다.

〔표 5〕 SecaaS Web Security의 핵심 기능과 보안 위협

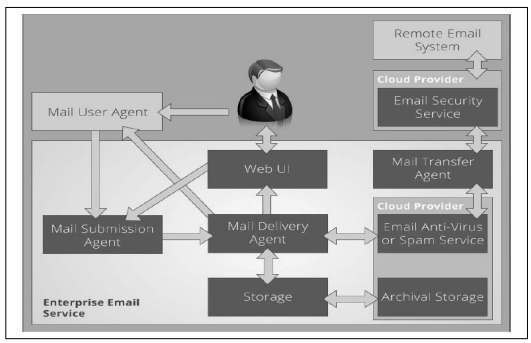
핵심 기능	
√ Web Filtering	
√ Phishing site blocker & Email Security	
√ SSL (decryption / hand off)	
√ Data Loss Prevention	
√ Cryptographic data protection & access control	
√ Web Access Control	
√ Fraud Prevention	
√ Instant Messaging Scanning	
보안 위협	
√ Keyloggers	√ Domain Content
√ Malware & spyware	√ Bandwidth consumption
√ Bot Network	√ Data Loss Prevention
√ Phishing	√ Spam
√ Virus	



〔그림 2〕 SecaaS Web Security의 기본 구조

4. Email Security

SecaaS Email Security는 수신, 발신하는 이메일에 대해 피싱, 악성 첨부파일, 스팸 등과 같은 보안 위협으로부터 보호하고 관리하는 솔루션으로 그림 3의 기본 구조에서 보듯이 이메일 보안 모듈을 제공한다. SecaaS Email Security의 핵심 기능과 보안 위협은 표 6과 같다.



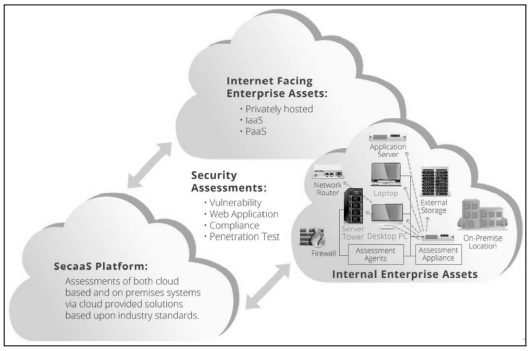
〔그림 3〕 SecaaS Email Security의 기본 구조

〔표 6〕 SecaaS Email Security의 핵심 기능과 보안 위협

핵심 기능	
√ Accurate filtering to block spam and phishing √ Deep protection against viruses and spyware √ Deep content scanning to enforce policies √ Option to encrypt some / all emails based on policy √ Integration with various email server solutions	
보안 위협	
√ Phishing √ Intrusion √ Malware	√ Spam √ Address spoofing

5. Security Assessments

SecaaS Security Assessments는 제 3기관이 클라우드 서비스나 기업 사내 네트워크에 대해 감사, 평가하는 것을 의미한다 [8]. 보안평가는 기존 평가 툴을 SaaS의 형태로 제공하고 또한 클라우드 서비스의 형태(SaaS, PaaS, IaaS) 특성에 적합한 플랫폼으로 설계함으로써 효적인 보안 평가 서비스를 제공하고자 한다. 그림 4는 SecaaS Security Assessments의 기본 구조를 보여주며, 표 7은 핵심 기능과 보안 위협을 보여준다.



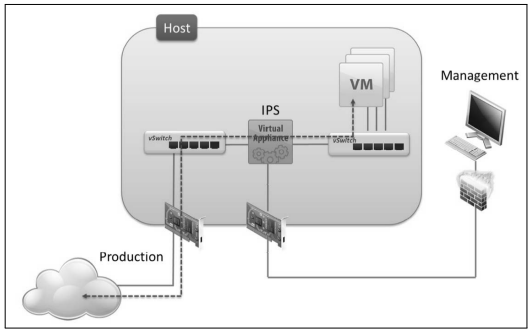
〔그림 4〕 SecaaS Security Assessments의 기본 구조

〔표 7〕 SecaaS Security Assessments의 핵심 기능과 보안 위협

핵심 기능
√ Governance & Risk Management √ Compliance & Technical Compliance Audits √ Application Security Assessments √ Vulnerability Assessments √ Penetration Testing √ Security / risk rating
보안 위협
√ Inaccurate inventory √ Lack of continuous monitoring √ Lack of correlation information √ Lack of complete auditing √ Failure to meet/prove adherence to Regulatory /Standards Compliance √ Insecure / vulnerable configurations √ Insecure architectures √ Insecure processes / processes not being followed

6. Intrusion Management

SecaaS Intrusion Management는 패턴 인식 기법을



〔그림 5〕 SecaaS Intrusion Management의 가상화 IPS

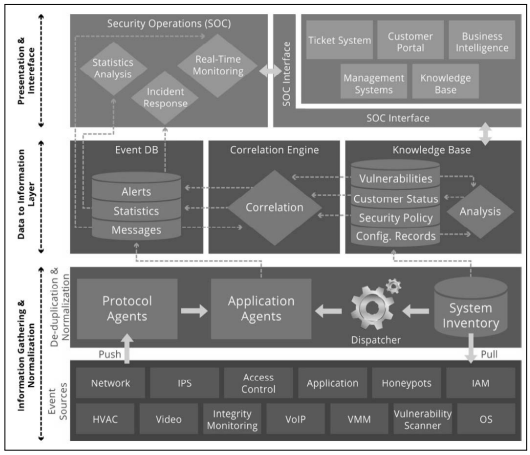
〔표 8〕 SecaaS Intrusion Management의 핵심 기능과 보안 위협

핵심 기능	
√ Identification of intrusions and policy violations √ Automatic or manual remediation actions √ Updates to address new vulnerabilities, exploits and policies √ Deep Packet Inspection √ System Call Monitoring √ System/Application Log Inspection √ Integrity Monitoring OS √ Integrity Monitoring VMM/Hypervisor √ VM Image Repository Monitoring	
보안 위협	
√ Intrusion	√ Malware

통해 침입을 탐지하고 통계적인 분석을 통해 이상 이벤트에 대응하는 것을 의미한다 [9]. 클라우드의 가상화, 멀티 테넌시와 같은 특성으로 인해 발생되는 새로운 침입 방법에 대한 대응에 중점을 두고 있다. 가상 머신과 하이퍼바이저의 시스템 콜, 로그 등의 모니터링을 통해 침입 탐지, 차단하는 방법에 대한 가이드를 제시한다. 그림 5는 가상화의 특성을 활용한 가상화 IPS에 대해 소개하며, SecaaS Intrusion Management의 핵심 기능과 보안 위협은 표 8과 같다.

7. Security Information and Event Management

SecaaS SIEM은 로그, 이벤트 정보를 분석하여 실시간으로 레포트를 하고 이상 사고나 이벤트에 대해 경고하는 것을 의미한다 [10]. SecaaS SIEM은 네트워크, IPS, 가상 머신, 운영체제, 어플리케이션 등 다양한 소스로부터 로그, 이벤트 정보를 수집하고, 수집된 정보를 체계적으로 DB화하여 분석한다. 이렇게 분석된 정보는



〔그림 6〕 SecaaS SIEM의 기본 구조

〔표 9〕 SecaaS SIEM의 핵심 기능과 보안 위협

핵심 기능
√ Real time log /event collection, de-duplication, normalization, aggregation and visualization √ Log normalization √ Real-time event correlation √ Forensics support √ Compliance reporting & support √ IR support √ Email anomaly detection √ Reporting
보안 위협
√ Abuse and Nefarious Use √ Insecure Interfaces and APIs √ Malicious Insiders √ Shared Technology Issues √ Data Loss and Leakage √ Account or Service Hijacking √ Unknown Risk Profile √ Fraud

사용자에게 레포트하고, 이상증후 탐지 시 경고한다. 또한 사고 대응 시스템, 감사 시스템, 유지보수 시스템 등과 같은 다른 시스템에서도 활용될 수 있다. 그림 6은 SecaaS SIEM의 기본 구조를 보여주며, 핵심 기능과 보안 위협은 표 9와 같다.

8. Encryption

클라우드 서비스의 가장 큰 단점 중 하나는 사용자의 데이터가 제 3자에 의해 관리됨에 따라 발생되는 신뢰성 문제이다. SecaaS Encryption은 암호 알고리즘을 사

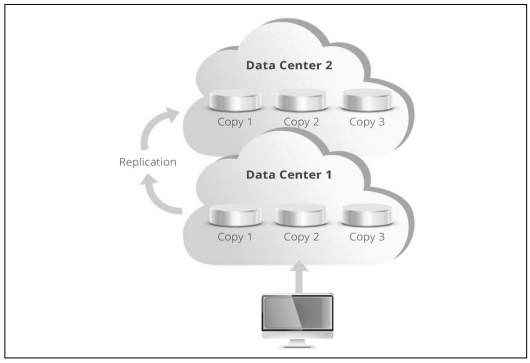
〔표 10〕 SecaaS Encryption의 핵심 기능과 보안 위협

핵심 기능
√ Data protection (at rest and in motion) √ Data validation √ Message Authentication √ Message/data integrity √ Data Time-stamping (digital notary) √ Identity validation √ Code Signing √ Forgery detection √ Identity validation (digital signatures) √ Digital Fingerprinting √ Forensic protection √ Pseudorandom number generation √ Data Destruction √ Key/certificate generation and management
보안 위협
√ Failure to meet Regulatory Compliance requirements √ Mitigating insider and external threats to data √ Intercepted clear text network traffic √ Clear text data on stolen / disposed of hardware √ Reducing the risk or and potentially enabling cross-border business opportunities √ Reducing perceived risks and thus enabling Cloud's Adoption by government

용하여 데이터의 기밀성, 무결성을 보장함으로써 신뢰성 문제를 해결하고자 한다. 데이터의 상태는 Data at rest, Data in transit, Data in use로 나누어 구분되고, SecaaS Encryption은 데이터의 상태 정보에 따라 안전하게 보호하는 방법을 제시한다. 또한 안전한 키 관리 방법에 대해서도 가이드를 제시한다. SecaaS Encryption의 핵심 기능과 보안 위협은 표 10과 같다.

9. Business Continuity and Disaster Recovery

SecaaS BCDR은 장애 이벤트에 대한 적절한 대응을 통해 사용자의 서비스 지속성을 보장하고, 또한 자연재해나 인위적인 재해가 발생 시 안전하고 효율적으로 복구를 지원한다[12]. SecaaS에서는 기존 IT 시스템의 BCDR 뿐만 아니라 클라우드 환경에 적합한 가이드를 제시한다. 그림 7은 여러 복구 방법 중 클라우드 데이터를 서로 다른 데이터 센터에 백업함으로써 안전하게 복구하는 모델을 보여준다. SecaaS BCDR에서는 클라우드 서비스 형태(SaaS, PaaS, IaaS)마다 적합한 백업 방법과 복구 방법에 대한 모델들을 제시하고 있으며, SecaaS



〔그림 7〕 SecaaS Cloud to Cloud Disaster Recovery

〔표 11〕 SecaaS BCDR의 핵심 기능과 보안 위협

핵심 기능	
√ Flexible infrastructure √ Secure backup √ Monitored operations √ Third party service connectivity √ Replicated infrastructure components √ Replicated data (core / critical systems) √ Data and/or application recovery √ Alternate sites of operation √ Tested and measured processes and operations to ensure √ Geographically distributed data centers/infrastructure √ Network survivability	
보안 위협	
√ Natural disaster √ Fire √ Power outage √ Terrorism/sabotage	√ Data corruption √ Data deletion √ Pandemic/biohazard

BCDR의 핵심 기능과 보안 위협은 표 11과 같다.

10. Network Security

SecaaS Network Security에서는 기존 네트워크에서의 위협과 클라우드 환경에서 가상화 네트워크의 특성으로 인해 발생되는 새로운 경로를 통한 위협을 효과적으로 대응하는 가이드를 제시한다. 네트워크 보안에서는 안전하게 네트워크 접근을 관리하는 방법으로 방화벽, IDS /IPS, 라우팅 관리, DDoS 공격 차단 그리고 안전한 접근을 위한 VPN 등이 있다. 클라우드 서비스 사용자의 시스템은 기존 IT 시스템과 달리 가상화를 통한 가상 머신으로 구성되어 있다. SecaaS의 네트워크 보안은 이와 같은 클라우드의 구조적 특성을 고려하여 효율

〔표 12〕 SecaaS Network Security의 핵심 기능과 보안 위협

핵심 기능
√ Data Threats
√ Access Control Threats
√ Access and Authentication controls
√ Security Gateways
√ Security Products
√ Security Monitoring and IR
√ DoS protection/mitigation
√ Secure "base services", Management network segmentation and security
√ Traffic / netflow monitoring
√ Integration with Hypervisor layer
보안 위협
√ Data Threats
√ Access Control Threats
√ Application Vulnerabilities
√ Cloud Platform Threats
√ Regulatory, Compliance & Law Enforcement

적인 모델을 제시하고 있으며, 핵심 기능과 보안 위협은 표 5와 같다.

Ⅳ. 결 론

본고에서는 클라우드 컴퓨팅이 갖고 있는 특성과 보안 위협에 대해 살펴봤다. 클라우드 컴퓨팅은 기존 시스템이 가지고 있는 보안 위협뿐만 아니라 하드웨어/소프트웨어 가상화, 멀티 테넌시 등의 특성으로 인한 새로운 보안 위협도 있다. 클라우드 서비스 제공하는 기업들과 글로벌 단체에서는 보안 위협에 대해 분석하고 대응하고 있으며, 특히 CSA의 SecaaS 워킹 그룹에서는 클라우드 컴퓨팅 환경에서 보안 솔루션을 구현하기 위한 가이드를 구체적으로 제시하고 있다. 아마존, 구글 등 글로벌 기업들과 CSA와 같은 글로벌 단체들의 노력이 클라우드 컴퓨팅에 대한 안전성을 보장하고 있다. 더 나아가 많은 기업과 사용자가 가지고 있는 클라우드 컴퓨팅의 보안 문제에 대한 인식을 전환시키고 있다. 국내에서도 클라우드 컴퓨팅에 대한 관심이 집중되고 있으며 일부 기업에서는 클라우드 서비스를 상용화하고 있다. 하지만 보안에 대한 대비는 아직 미흡한 실정이다. 국내에서도 클라우드 보안 위협에 대한 대응책을 마련하고, 시스템에 대한 신뢰성을 구축하는데 노력함으로써 국제 경쟁력을 향상시켜야 할 것이다.

참고문헌

[1] 김양우 등, "Cloud Computing Use Cases", TTAK.OT-10.0290, Dec. 2010.

[2] 김태형, 김인혁, 민창우, 엄영익, "클라우드 컴퓨팅 보안 기술 동향", *정보과학회지* (C), 30(1), pp. 30-38, Jan. 2012.

[3] "Security Guidance for Critical Areas of Focus in Cloud Computing", Cloud Security Alliance, Nov. 2011.

[4] Security as a Service Working Group, "Defined Categories of Service", Cloud Security Alliance, Oct. 2011.

[4] Security as a Service Working Group, "Identity and Access Management", Cloud Security Alliance, Sep. 2012.

[5] Security as a Service Working Group, "Data Loss Prevention", Cloud Security Alliance, Sep. 2012.

[6] Security as a Service Working Group, "Web Security", Cloud Security Alliance, Sep. 2012.

[7] Security as a Service Working Group, "Email Security", Cloud Security Alliance, Sep. 2012.

[8] Security as a Service Working Group, "Security Assessments", Cloud Security Alliance, Sep. 2012.

[9] Security as a Service Working Group, "Intrusion Management", Cloud Security Alliance, Sep. 2012.

[10] Security as a Service Working Group, "Security Information and Event Management", Cloud Security Alliance, Sep. 2012.

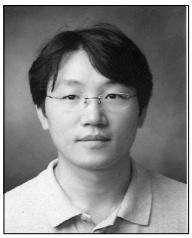
[11] Security as a Service Working Group, "Encryption", Cloud Security Alliance, Sep. 2012.

[12] Security as a Service Working Group, "Business Continuity and Disaster Recovery", Cloud Security Alliance, Sep. 2012.

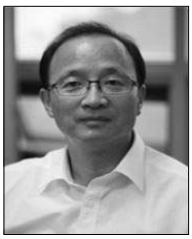
[13] Security as a Service Working Group, "Network Security", Cloud Security Alliance, Sep. 2012.

〈著者紹介〉

이 종 훈 (Jonghoon Lee)
2005년 2월 : 숭실대학교 정보통신전자공학부 학사
2012년 3월~현재 : 숭실대학교 전자공학과 석사과정
<관심분야> 클라우드 보안, 무선 네트워크 보안



정 승 욱 (Seungwook Jung)
정회원
1998년 2월 : 숭실대학교 전자공학과 졸업
2000년 2월 : 숭실대학교 전자공학과 석사
2006년 2월 : University of Seigen 박사
2006년 12월~2012년 8월 : 한국인터넷진흥원
2012년 9월~현재 : 숭실대학교 S4-URC 교수
<관심분야> 암호 응용, 클라우드 보안, 개인정보보호



정 수 환 (Souhwan Jung)
정회원
1985년 2월 : 서울대학교 전자공학과 학사
1987년 2월 : 서울대학교 전자공학과 석사
1988년~1991년 : 한국통신 전임연구원
1996년 6월 : University of Washington 박사
1997년 : Stellar One Corp. Senior Engineer
1997년~현재 : 숭실대학교 정보통신전자공학부 교수
<관심분야> 이동 네트워크 보안, VoIP 보안, SNS 보안, 클라우드 보안