chapter 1

클라우드 보안 기술 및 표준 동향

박인상 ‖ 이글루시큐리티 책임연구원
이호형 ‖ 신세계아이앤씨 부장
조수연 ‖ CJ올리브네트웍스 차장

언택트 시대가 도래하면서 클라우드 서비스의 활용이 급속도로 증가되고 있으나 이에 따른 보안 위협도 증가되고 있다. 전통적인 보안에서는 보안 위협에 대응하기 위해 통합보안관제센터(SOC)를 구축하고 사람에 의한 보안관제 및 침해대응을 위해 정보보호와 개인정보보호체계를 구축하였다. 클라우드 서비스에서는 전통적인 보안과 달리 자동화된 보안체계의 구축이 필요하다. 이를 위해 국내외 클라우드 서비스 제공자들은 다양한 보안 서비스 제공을 위해 많은 노력을 기울이고 있다. 본 고에서는 클라우드 보안 기술과 표준 동향에 대해 알아보도록 한다.

I. 서론

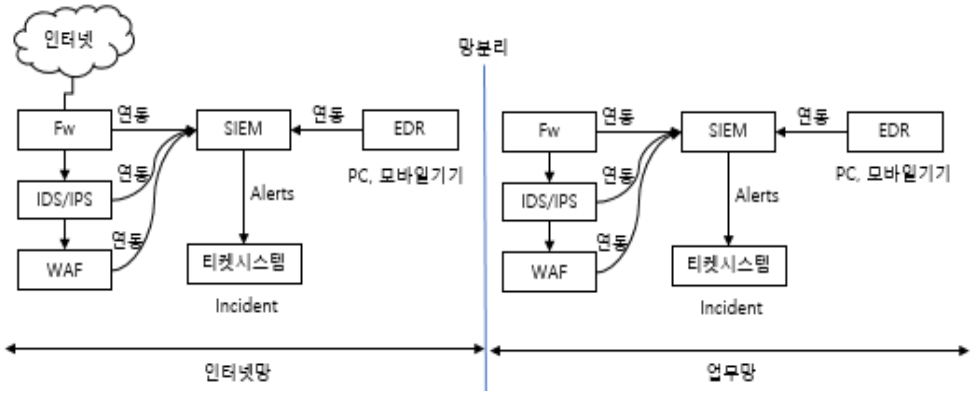
디지털 기술이 발전함에 따라 인프라 운영방식의 근본적인 변화가 필요한 디지털 트랜스포메이션으로 비즈니스 환경이 급변하고 있다. 금융기관, 공공기관 등 많은 기관들이 전통적인 비즈니스 환경인 온-프레미스(On-Premise)에서 클라우드 중심으로 변화하고 있다. 온-프레미스와 퍼블릭 클라우드를 조합한 하이브리드 클라우드로 운영하거나 다수의 퍼블릭 클라우드를 조합한 멀티 클라우드로 운영하는 등 비즈니스에 가장 적합한 서비

* 본 내용은 박인상 책임연구원(☎ 02-3452-8814, insang.park@igloosec.com)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.

스를 이용하는 형태로 복잡하게 변화하고 있다. 이러한 변화는 보안 환경의 변화에도 영향을 끼치고 있다.

전통적인 보안은 네트워크 보안과 엔드포인트 보안으로 구분할 수 있다. 네트워크 보안에서는 망 분리된 네트워크에 방화벽, 침입탐지시스템(Intrusion Detection System: IDS), 침입방지시스템(Intrusion Prevention System: IPS), 웹 애플리케이션 방화벽(Web Application Firewall: WAF) 같은 네트워크 보안시스템을 구축한다. 그리고 네트워크 보안시스템을 통합하여 모니터링 및 관리를 위해 보안시스템에서 발생되는 보안 이벤트와 시스템 정보를 SIEM(Security Information and Event Management)에 연동하여 보안시스템을 모니터링하고, 위협이 탐지되면 Alerts을 발생시키고 티켓시스템을 이용하여 발생된 Alerts을 인시던트(Incident)로 처리한다. 엔드포인트 보안인 EDR(Endpoint Detection and Response)은 사용자 PC, 모바일기기 등에 설치하여 랜섬웨어나 바이러스를 탐지하고 사용자 프로세스를 통제한다. 이러한 네트워크 보안과 엔드포인트 보안은 [그림 1]과 같이 통합보안관제센터인 SOC(Security Operation Center)에서 관리적, 물리적, 기술적인 서비스인 Managed Security Service로 제공된다.

클라우드는 개방적인 네트워크 환경으로 온-프레미스에 SOC를 구축하여 보안체계를 구성하는 전통적인 방식과는 달라진다. 클라우드 환경에서는 방화벽, IDS, IPS, WAF의 전통적인 방식뿐만 아니라 가상머신, 컨테이너, 계정관리 등 클라우드를 위한 보안까지도 요구된다.



〈자료〉 이글루시큐리티 자체 작성

[그림 1] 전통적인 통합보안관제센터(SOC) 구성

[표 1] 미국 CSA(Cloud Security Alliance)의 SECaaS(SECurity as a Service)

카테고리	설명	카테고리	설명
BCDR(Business Continuity and Disaster Recovery)	비즈니스 연속성 및 재해복구	Intrusion Management	침입 시도 탐지 및 방지
Continuous monitoring	지속적인 위험관리	Network Security	네트워크 보안
DLP (Data Loss Prevention)	데이터 암호화, 민감 데이터 관리	Security Assessment	거버넌스 & 리스크 관리, 컴플라이언스 감사
E-Mail Security	악성 첨부파일과 스팸으로부터 조직보호	SIEM(Security Information and Event Management)	실시간 로그, 보안이벤트, 시스템 정보 수집
Encryption	데이터 암호화	Vulnerability Scanning	취약점 검사
IAM(Identity and Access Management)	인증, 신원보증, 권한관리	Web Security	웹 트래픽, 웹 애플리케이션 보안

〈자료〉 이글루시큐리티 자체 작성

클라우드에서는 보안을 서비스의 관점으로 바라보고 있으며 클라우드 보안 서비스 모델로 [표 1]과 같이 미국 CSA(Cloud Security Alliance)의 SECaaS(Security as a Service) 모델의 구현이 요구되고 있다[1]. 다양한 멀티 클라우드를 사용하는 환경에서도 일관된 보안정책이 요구되기도 하며 관련된 솔루션으로 가트너가 제시한 CASB(Cloud Access Security Broker)가 주목을 받고 있다. 클라우드에서는 온-프레미스에 비해 네트워크에 대한 접근(Access)이 자유롭기 때문에 제로 트러스트(Zero Trust) 모델도 요구된다.

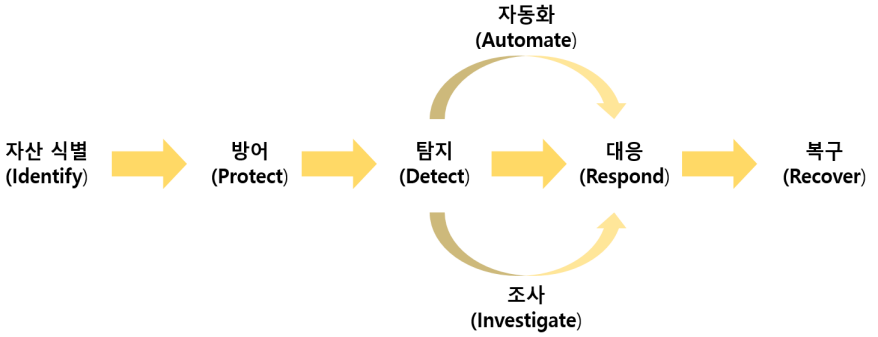
가트너는 2020년 세계 퍼블릭 클라우드 컴퓨팅 시장 규모를 2,579억 달러로 전망하였다[2]. 또한, 최근 COVID-19으로 인해 클라우드의 사용이 급증하면서 보안에 대한 인식이 국내·외적으로 확산되고 있다.

본 고에서는 클라우드 보안 기술 동향과 관련 국제 표준을 설명하고자 한다. 이를 위해, 먼저 II장에서 글로벌 클라우드 서비스인 아마존 AWS(Amazon Web Service), 마이크로소프트 Azure, 구글 GCP(Google Cloud Platform)의 보안 서비스를 살펴보도록 한다. III장에서는 클라우드 관련 국제 표준인 ISO 27000 Family, ISO 27017, ISO 27018에 대해 살펴보고, IV장에서 본 고의 결론을 제시한다.

II. 클라우드 보안 기술 동향

1. 아마존 AWS

아마존 AWS는 클라우드 보안 위협 탐지 및 대응에 대한 접근 전략으로서 자동화 기반 사용자 격리 및 지능화 기반 보안 위협 탐지를 위한 보안 서비스들을 제공한다. 자동화 기반의 사용자 격리를 위해 람다(Lambda), SNS(Simple Notification Service), Cloud Formation 등의 서비스가 있고, 지능화 기반 보안 위협 탐지를 위해 AWS Config Rules, Amazon Inspector, Amazon GuardDuty 등의 서비스가 있다.



〈자료〉 아마존 AWS

[그림 2] AWS 보안 서비스 워크플로우

미국 국립표준기술연구소인 NIST의 사이버 보안 프레임워크를 기반으로 [그림 2]와 같이 아마존 AWS의 보안 서비스를 식별, 방어, 탐지, 대응, 복구의 각 단계별 서비스로 구분할 수가 있으며[3], 이 중에서 [표 2]와 같이 식별, 탐지, 대응 단계의 아마존 서비스를 살펴보도록 한다.

식별 단계의 서비스로서 AWS Config는 AWS 리소스의 변경사항을 추적하고 감사하는 서비스이다. 보안 규정을 위반하는 리소스나 규정 위반 건수 등의 모니터링을 제공하는 통합 Account Dashboard를 제공한다. 또한, AWS Config Rules 서비스를 통해 기준 정책의 위배 시에 람다를 이용하여 자동화된 차단 및 통지가 가능하다.

탐지 단계의 서비스로는 Amazon GuardDuty, Amazon Inspector, Amazon Macie, AWS Security Hub 등이 있다[4]. Amazon GuardDuty는 관리형 위협 탐지 및 통지

[표 2] 아마존 AWS 보안 서비스

단계	보안 서비스	설명
식별	AWS Config	변경 리소스를 Config Rules로 대응 규칙 실행
탐지	Amazon GuardDuty	관리형 위협 탐지 및 통지 서비스
	Amazon Inspector	Amazon EC2 instances의 자동화된 보안 수준 점검
	Amazon Macie	기계학습 기반 민감한 중요 데이터의 발견 및 분류
	AWS Security Hub	AWS 환경에 대한 보안과 규정 준수 현황 확인 서비스
대응	AWS CloudTrail	AWS API 요청의 처리내역을 로깅하는 서비스
	Amazon CloudWatch	AWS 리소스와 AWS기반 애플리케이션에 대한 모니터링
	Amazon Detective	보안사고 원인을 분석, 조사, 규명하는 서비스

〈자료〉 이글루시큐리티 자체 작성

서비스이다. 가상 네트워크인 VPC(Virtual Private Cloud)의 플로우(Flow) 로그, DNS 로그, AWS CloudTrail 로그에 대해 에이전트 없이 머신러닝을 기반으로 이상행동 탐지가 가능하다. 트리거인 람다(Lambda)와 연계하여 가상머신에 대한 네트워크 격리, 블록 스토리지인 EBS(Elastic Block Store)의 스냅샷 생성 등의 자동화된 대응 조치를 취할 수 있다. Amazon Inspector는 에이전트 기반의 보안 취약점 점검 서비스이다. 리눅스, 윈도즈 서버 등의 탐지 자동화를 위해 람다를 이용하여 점검 대상 EC2(Elastic Compute Cloud) 인스턴스에 조치를 실행할 수 있으며 보안 진단 결과와 취약점에 대한 대응 가이드를 제공한다. Amazon Macie는 기업의 민감한 중요 데이터에 대한 식별과 유출 차단을 위한 서비스이다. 기계학습을 기반으로 PII(Personally Identifiable Information)와 같은 민감 데이터에 대한 식별이 이루어지며 주기적인 탐색이 가능하다. 발견된 항목을 Amazon CloudWatch에 Events로 전송하여 통합 대응이 가능하다. AWS Security Hub는 AWS 계정 전반에 걸쳐 우선순위가 높은 보안 경고 및 규정 준수 상태를 종합적으로 확인할 수 있는 서비스이다. 자동으로 로그에 대한 수집과 파싱, 연관 분석이 가능하고 SIEM, Ticketing, SOAR(Security Orchestration Automation and Response)와 연계 가능하다. 또한, CIS Foundation과 PCI DSS 등의 보안 표준 기준에 대한 점검과 대응 가이드를 제공한다.

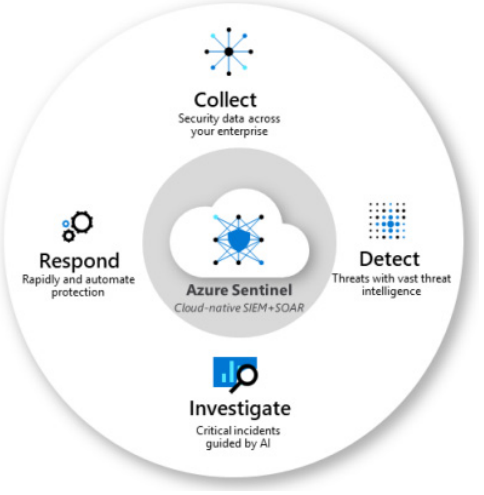
대응 단계에서 침해에 대한 조사(investigate)를 위한 서비스로는 AWS CloudTrail, Amazon CloudWatch, Amazon Detective 등이 있다. AWS CloudTrail은 AWS API

요청의 처리내역을 로깅(logging)하는 서비스이다. AWS에서 발생하는 모든 API 호출을 로깅하며 기계학습을 통해 갑작스런 가상머신 생성의 급증, 비정상적인 계정 활동 등의 비정상적인 API 호출에 대한 모니터링이 가능하다. Amazon CloudWatch는 AWS 리소스와 AWS 기반 애플리케이션에 대한 모니터링 서비스이다. 메트릭 데이터인 CPU, Memory, Disk I/O, Network 모니터링 데이터와 애플리케이션 로그를 수집·모니터링하고 Alerts를 설정한다. 그래프 및 통계 수치기능을 제공하며 대시보드를 활용하여 시각화도 할 수 있다. Amazon Detective는 신속하게 보안 사고의 원인을 분석, 조사 규명을 위한 서비스이다. 기계학습과 연계하여 잠재적인 보안 문제나 보안 침해가 의심되는 활동에 대한 원인 분석 및 조사가 가능하다.

2. 마이크로소프트 Azure

마이크로소프트 Azure의 주요 보안 서비스로는 [표 3]과 같이 Azure Monitor, Azure Sentinel, Azure Active Directory, Azure Security Center가 있다[5].

Azure Monitor는 애플리케이션, 인프라, 네트워크 등의 모니터링이 가능한 서비스이다. Azure Monitor는 가상머신의 모니터링을 위해 가상머신 로그와 메트릭 정보를 수집한다. 수집된 가상머신의 로그 분석을 통해 리눅스 및 윈도 VM의 성능과 상태를 분석하며 대규모 Azure VM을 모니터링하기도 한다. 또한, 컨테이너 모니터링을 위해 Log Analytics 에이전트를 이용하여 컨테이너 로그와 메트릭을 수집하며 Kubernetes 클러스터에서 모니터링을 하기도 한다. 관리형 Kubernetes 서비스인 AKS(Azure Kubernetes Service)는 배포된 컨테이너 워크로드의 성능 모니터링도 가능하다. 메트릭 API를 통해 Kubernetes에서 사용할 수 있는 컨트롤러, 노드 및 컨테이너의 메모리 및 프로세서 메트릭을 수집하여 성능을 시각적으로 표시한다. 모니터링 데이터 시각화를 위해 대시보드를 활용할 수 있



〈자료〉 MS Azure

[그림 3] Azure Sentinel

다. Azure Monitor의 Alerts는 메트릭 기반으로 실시간에 가까운 경고를 제공한다.

[그림 3]의 Azure Sentinel은 Cloud Native SIEM을 제공하는 SaaS 형태의 서비스이다. 클라우드에 방화벽, IDS, IPS, WAF 등 가상화된 보안시스템을 구축 후 로그를 수집(Collect)한다. 실시간 분석을 위해 보안 규칙의 설정이 가능하며 규칙에 의해 위협을 탐지(Detect)한다. 탐지된 위협정보를 조사(Investigate)하기 위해 티켓시스템을 통해 인시던트로 생성하며 위협 사냥(Threat hunting) 기능과 인공지능 분석이 가능하다. 플레이북(Playbook)을 활용하여 자동화된 대응(Respond) 구현이 가능하며 SOAR를 구현할 수도 있다.

Azure Active Directory는 기업ID 서비스를 제공하며 Single Sign-On 및 다단계 인증을 제공한다. 사용자 계정을 생성하고 조직에 맞게 디렉토리를 생성하여 권한을 사용자에게 할당해 줄 수 있다. ID 거버넌스를 사용하여 ID 수명주기 거버넌스, 액세스 수명주기 거버넌스, 관리를 위한 권한 있는 액세스 보호기능을 조직에 맞게 제공해 줄 수 있다.

Azure Security Center를 이용하여 보안 정책 및 자동화를 사용하여 대규모 환경에서 신속하게 위협을 식별하고 대응이 가능하며 조직 보안 정책 및 준수 관리도 가능하다. 또한, 관리 그룹, 전체 구독 및 전체 테넌트에 대해 정책을 설정할 수 있다.

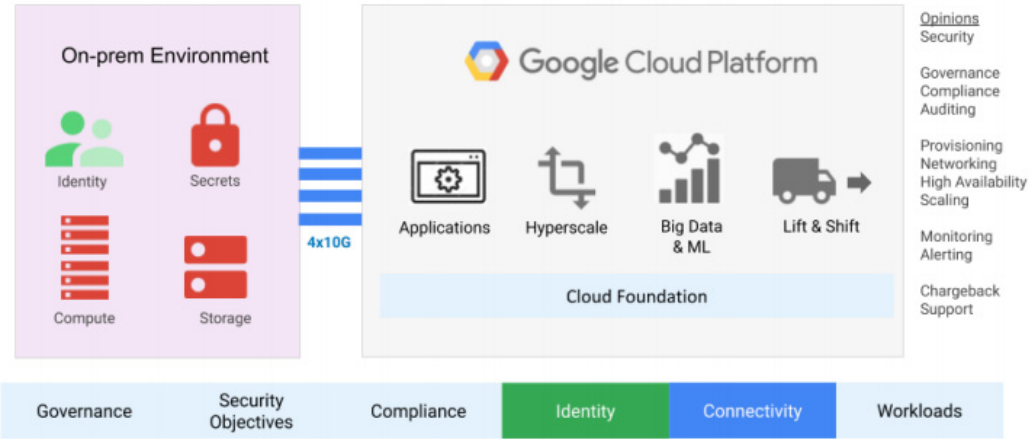
[표 3] 마이크로소프트 Azure 주요 보안 서비스

서비스	기능	설명
Azure Monitor	애플리케이션 모니터링	DevOps 프로세스 및 도구 모니터링
	인프라 모니터링	가상머신, 컨테이너, Azure Storage 인프라 모니터링
	네트워크 모니터링	패킷 캡처 트리거, 네트워크 흐름 로그 모니터링
Azure Sentinel	Cloud Native SIEM	가상화된 보안 시스템 연동 및 인시던트 처리
Azure Active Directory	리소스에 대한 액세스 보호	사용자의 앱 및 데이터에 대한 액세스를 제어
Azure Security Center	지능형 위협 방지 기능	클라우드 전체 통합된 인프라 보안 관리 시스템

〈자료〉 이글루시큐리티 자체 작성

3. 구글 GCP

GCP(Google Cloud Platform)는 [그림 4]와 같이 On-Premise 환경과 연계된 보안 모델을 제공하며, [표 4]와 같이 IAM(Identity and Access Management), 키 관리, 클



〈자료〉 구글 GCP

[그림 4] GCP 보안 모델

라우드 모니터링, Security Command Center를 통해 지능적인 보안 서비스를 제공한다[6]. GCP 보안 모델은 정책과 아키텍처로 구성된 예방통제(Preventative Controls)와 탐지통제(Detective Controls)를 제공한다.

Cloud Identity and Access Management는 조직 전체에 적용되는 보안 정책에 관한 통합 뷰를 제공하고 규정 준수를 위한 감사 기능을 제공한다. 사내 직무를 그룹 및 역할로 매핑하여 접근 권한을 제어하며 머신러닝인 추천자 기능을 사용한다[7].

[표 4] 구글 GCP 주요 보안 서비스

단계	서비스	설명
예방 (Policy and architecture)	Cloud Identity and Access Management	ID, 접근 권한 관리, 작업 그룹 기준 사용자 접근 권한 제어
	Cloud Key Management Service	암호화된 키 관리, 중앙 집중식 키 관리, H/W 보안모듈 제공 및 외부 키 관리
탐지 (Detection)	Cloud Asset Inventory	클라우드 모니터링, 대시보드, 알람
	Security Command Center	취약점 스캔, 구성 오류 탐지, Security Health Analytics, Web Security Scanner 서비스로 취약점 탐지
		Event/Container Threat Detection(베타) 서비스로 이벤트 및 컨테이너 위협 탐지 (멀웨어, 암호화폐 채굴, DDoS)

〈자료〉 이글루시큐리티 자체 작성

Cloud Key Management Service는 Google Cloud에서 암호화 키를 관리하는 서비스이다. 중앙에서 암호화 키 관리를 제공하고 민감한 정보는 하드웨어 보안 모듈(HSM)을 사용할 수 있으며 EKM(External Key Manager)을 통해 외부 키 관리도 지원하고 있다[8].

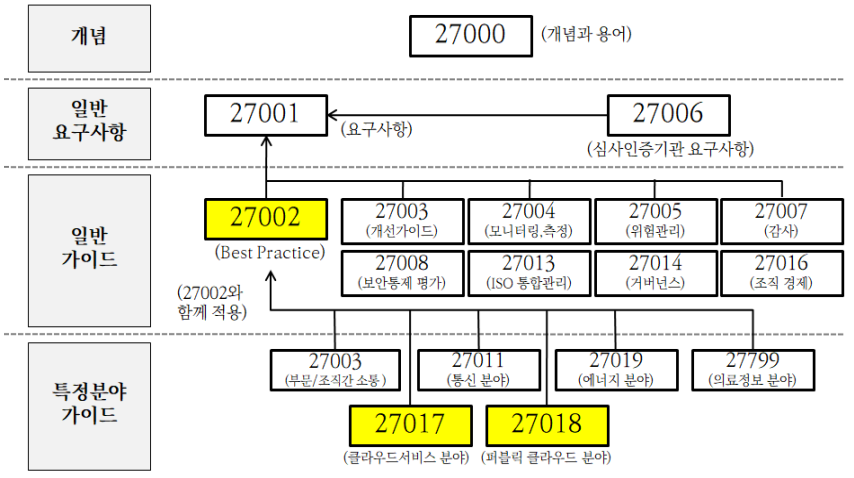
Cloud Asset Inventory는 서비스 중인 모든 자원을 가시화하여 모니터링 및 분석하는 기능을 제공한다. GCP 서비스, 쿠버네티스 리소스 및 RBAC 정책과 Anthos 배포 모니터링을 지원한다. Cloud Pub/Sub을 통해 구성 변경에 대한 실시간 알람을 제공하고 BigQuery로 보안 위협에 대한 분석기능이 가능하다[9].

Security Command Center는 Google Cloud의 표준 보안 및 위험 데이터베이스로 조직 전체에서 Google Cloud 보안 및 데이터 위험을 탐지하고 대응하기 위한 지능적인 대시보드 및 분석 시스템이다.

III. 클라우드 보안 표준 동향

1. ISO/IEC 27000 계열 표준

ISO/IEC 27000은 [그림 5]와 같이 ISO/IEC 27000계열의 표준 전반에 대한 원칙과



〈자료〉 이글루시큐리티 자체 작성

[그림 5] ISO 27000 계열 표준

용어이다. ISO/IEC 27001은 요구사항, ISO/IEC 27002는 일반적인 지침이다.

ISO/IEC 27002를 기반으로 특정 분야에 대한 표준이 제공되고 있으며, ISO/IEC 27017과 ISO/IEC 27018은 클라우드 서비스에 대한 정보보안 가이드를 제공하고 있다[10].

2. ISO/IEC 27017:2015

ISO/IEC 27017:2015는 클라우드 서비스를 제공 및 사용할 때 적용되는 정보 보안 통제에 대한 가이드라인으로 [표 5]와 같이 구성된다[11]. 이 표준은 37가지 ISO/IEC 27002 통제에 대한 클라우드 기반 가이드라인을 제공하며 7가지의 새로운 클라우드 통제 가이드를 제공한다. 7가지는 클라우드 서비스 공급자와 클라우드 고객 간의 사안별 소재,

[표 5] ISO/IEC 27017:2015 구성

No.	Section	설명
1	범위	ISO/IEC 27017 표준 구성 범위
2	표준 참조	표준 구성을 위한 참조 정보
3	정의 및 약어	표준 용어 및 약어 정의
4	클라우드 부문별 개념	클라우드 부문별 개념 상세 설명
5	정보 보호 정책	정보 및 기타 자산에 대한 보안 위협 수준과 일치
6	정보 보호 조직	내부 조직 역할과 책임, 모바일 장치와 원격 접근 정책
7	인적 자원 보안	표준과 절차, 보안 위협 관리 방법, 법적 규제사항 교육
8	자산 관리	자산의 책임, 정보 분리, 미디어 제어
9	접근 통제	접근 관리, 사용자 통제, 시스템/소프트웨어 접근 통제
10	암호화	공급자의 암호 기능 사용 정책, 서비스 사용자 키 관리
11	물리적 보안	사무실, 시설 등 보안 영역, 케이블, 시스템 등 보안 장비
12	서비스 운영 보안	문서 운영 절차, 변경 관리, 용량 관리, 백업, 로그 모니터링
13	통신 보안	네트워크 보안 관리, ACL, 정보 전송 정책
14	시스템 개발 및 유지보수	보안 요구사항 적용, 개발 지원 절차, 테스트 데이터
15	공급 업체 관계	공급 업체 정보보호, 공급 서비스 보안 감사, 공급자 신원 확인
16	정보 보안 사고 관리	보안 사고 책임과 절차, 정보보호 이벤트 보고, 포렌식
17	BCM[1]의 정보 보안 측면	ISO 22301 기반 정보보호 지속성 확보, 보안 가용성 확보
18	법률 및 규정	관할 지역 법률 준수, 라이선스 규정 준수 및 문서화

1) BCM: 비즈니스 연속성 관리(Business Continuity Management)
〈자료〉 ISO/IEC 27017 Standards

계약 종료 시 자산 제거 및 반납, 고객의 가상 환경 보호 및 분리, 가상 머신 구성, 클라우드 환경과 관련된 관리 작업 및 절차, 고객의 클라우드 내 활동 모니터링, 가상 및 클라우드 네트워크 환경의 정렬이다. 이 표준은 개인정보보호 외에도 클라우드 컴퓨팅의 광범위한 정보 보안을 커버하기 위해 ISO/IEC 27018:2019와 함께 제공된다.

3. The ISO/IEC 27018:2019

ISO/IEC 27018:2019는 퍼블릭 클라우드에서 개인식별정보(Personally Identifiable Information: PII)를 보호하기 위한 최초의 국제 표준 가이드이다[12]. 조직에서 애플리케이션을 클라우드로 전환할 때 가장 중요하게 고려하는 사항은 클라우드 컴퓨팅의 데이터 보안 및 개인정보보호이다. 퍼블릭 클라우드 서비스 제공업체가 처리하는 개인식별정보(PII) 보호와 관련하여 일반적으로 수용되는 제어 목표, 제어 및 지침을 제시한다. ISO/IEC 27018:2019는 ISO/IEC 27002에서 규정한 제어장치에 대한 11가지 구현 지침을 보완한 가이드를 제공한다. 11가지 통제 항목은 ISO/IEC 27017과 동일하게 구성된다. 개인식별정보 프로세서는 클라우드를 통해 서비스를 제공하는 민간, 공공 부문의 모든

[표 6] ISO 27018:2019 별첨(Annex): PII 보호를 위한 퍼블릭 클라우드 PII 프로세스 확장 제어

No.	Section	설명
1	일반	ISO/IEC 27018:2019 부속서 일반 개요
2	동의와 선택	데이터 액세스, 수정, 제거 요구 준수를 위한 도구 제공
3	합법성 및 사용목적	고유 목적 외 고객 데이터 사용 금지, 고객의 명시적 동의 필요
4	수집 제한	개인정보 수집 목적 명확화, 목적 외 수집 제한
5	데이터 최소화	지정된 기간 내 파기 및 임시 파일 삭제
6	사용 및 공개 제한	법적 의무 시 사전에 고객에 대한 내용, 대상, 시간 고지의 의무
7	정확성과 품질	개인정보 수집/통제 정확성, 사용 품질 확보
8	개방성, 투명성	서비스 계약 체결 전 업체의 신원 및 PII 처리 위치 공개
9	개인 참여와 접근	개인 자신의 데이터 액세스 권한 주장 시 액세스 권한 제공 등 규정 준수
10	책임	PII 무단 액세스, 손실, 초래 시 관련 고객에게 즉시 고지
11	정보 보호	기밀 유지 의무, 하드 카피 작성 제한, 암호화를 포함한 접근 제한
12	개인정보 보호규정	PII의 반품, 양도 또는 삭제 정책 보유, 고객에 정책 정보 제공

〈자료〉 ISO/IEC 27018 Standards

조직 유형과 규모에 맞게 설계되었다. ISO/IEC 27018:2019의 별첨(Annex)은 [표 6]과 같으며 PII 프로세서로 활동하는 퍼블릭 클라우드 서비스 제공자에게 적용되는 PII 보호 요건을 충족하기 위해 11개 부문의 확장된 지침을 제공한다. 이 지침은 ISO/IEC 29100:2011의 11가지 개인정보보호 원칙에 따라 분류되며, “정보 기술 - 보안 기술 - 개인정보 보호 프레임워크”로 알려져 있다.

IV. 결론

클라우드 보안은 전통적인 온-프레미스(On-Premise) 방식의 보안 방식과는 달라진다. 온-프레미스에서는 사람 중심 보안이였지만 클라우드에서는 인공지능 중심 보안으로 변화하고 있다. 사람이 판단하고 대응하던 수동적인 대응체계가 인공지능이 판단하고 자동화 처리되는 대응체계로 변화되고 있다.

ISO/IEC 27017은 클라우드의 정보보안 가이드를 제공하며 ISO/IEC 27018은 클라우드의 개인정보보호에 대한 가이드를 제공하고 있다. 아마존 AWS, 마이크로소프트 Azure, 구글 GCP는 모두 ISO/IEC 27017, ISO/IEC 27018 인증을 받았다.

많은 기관들이 디지털 트랜스포메이션을 위해 온-프레미스에서 클라우드로 마이그레이션하고 있다. 클라우드 보안은 클라우드 컴퓨팅 서비스 채택의 주요 저해 요소로 남아 있다. 기업이 클라우드를 도입하기 위해서는 정보보안 및 개인 정보 보호 문제에 큰 관심을 갖고 있으므로 보안 서비스들의 활용과 표준 준수를 통해 보안 이슈가 반드시 해결되어야 할 것이다.

[참고문헌]

[1] “Defining Categories of Security as a service:Continuous monitoring,” CSA, 2016
[2] TECHWORLD, “[마켓리포트] 퍼블릭 클라우드 컴퓨팅 서비스시장 규모”, 2020. 9. 4.
[3] 신은수, “AWS환경에서의 위협 탐지 및 사냥”, AWS, 2020.
[4] 임기성, “AWS상의 보안 위협 탐지 및 대응”, AWS, 2019.
[5] “Azure 보안 소개”, 마이크로소프트, 2019.
[6] “Google Cloud security foundations guide,” Google Cloud, 2020.
[7] 발리아파 락쉬마난, 조던 티가니, “구글 빅쿼리 완벽 가이드”, 책만, 2020.
[8] 박정운, “구글 클라우드 플랫폼 뽀개기”, 비제이퍼블릭, 2019.

[9] 조대협 공저, “빠르게 훑어보는 구글 클라우드 플랫폼”, 한빛미디어, 2016.
[10] “An Overview of ISO/IEC 27000 family,” OGCIO, 2020.
[11] “ISO/IEC 27017:2015 Information technology- Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services,” ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection, 1 Edition, 2015.
[12] “ISO/IEC 27018:2019 Information technology - Security techniques - Code of practice for protection of personally identifiable information(PII) in public clouds acting as PII processors,” ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection, 2 Edition, 2019.