ISMS-P 기반 클라우드 보안대책 수립

박광열, 장경준, 김해진

(지도교수 : 장원태)

Cloud Information Security measures from ISMS-P

Gwang-Yeol Park , Gyeong-Jun Jang , Hae-Jin Kim

요약

정보화시대를 넘어 4차 산업시대에 도달하면서 개인이나 기업의 정보는 중요한 자산이 되었고 해킹에 대한 위협도 점점 증가하고 있다. 개인과 기업의 사용하는 정보량이 증가하여 대중적인 정보관리 기술 중 하나인 클라우드 사용량도 증가함에 따라 클라우드를 안전하게 보호할 수 있는 대책이 필요하다.

클라우드의 보안대책을 ISMS-P 국내정보 보호 기반으로 하여 안전한 정보보호 기술을 모색한다. 본 논문에서는 클라우드 서비스 모델 중 IaaS 클라우드 모델의 공유자원 책임 문제와 SaaS 클라우드 모델의 가상화 기술에 따른 보안 취약성 문제에 대한 보안대책을 연구한다.

Abstract

After the information age, the information of individual or business has become an important asset, and the threat of hacking is also increasing. As the amount of information used by individuals and corporations increases, the usage of cloud, which is one of the popular information management technologies, also increases, and measures to protect the cloud are needed.

The security measures of the cloud are based on the ISMS-P information protection system to seek safe information protection technology. In this paper, we study the security measures for the shared resource responsibility problem of the IaaS cloud model and the security vulnerability according to the virtualization technology of the SaaS cloud model

Keyword: 클라우드 보안, ISMS-P

I. 서 론

정보화시대를 넘어 4차 산업시대에 도달하면서 개인이나 기업의 정보는 중요한 자산이 되었고 해킹에 대한 위협도 점점 증가하고 있다. 특히 클라우드는 사용자가 컴퓨팅 자원에 접근하기 쉽고 데이터 처리 및 연산을 할 수 있도록 네트워크, 서버, 디스크 등을 연결하는 컴퓨팅 서비스를 제공하여 효율성과 접근성이 높아 클라우드 시장은 빠르게 성장하였다. 이에 따라 클라우드 취약점을 노린 정보 침해 공격에 대응 및 예방하기 위한 보안대책이 요구되며 클라우드 사용자의 정보보안 중요성에 대한 인식 향상이 필요하다.

본 논문에서는 클라우드 서비스 취약점과 그에 따른 대안을 알아보며 국내 정보보호 관리체계(K-ISMS)와 개인정보보호 관리체계(PIMS) 인증기준에 기반을 둔 IaaS 클라우드 모델의 공유자원 책임 문제와

SaaS 클라우드 모델의 가상화 기술에 따른 보안 취약성 문제에 대한 보안대책을 연구한다.

II. 본론

2.1 국내 정보보호 관리체계 인증제도 개요

국내 정보보호 관리체계는 한국인터넷진흥원(KISA)에서 권고하는 정보보호 및 개인정보 관리체계 인증으로 기업을 대상 주요 정보자산의 기밀성, 무결성, 가용성 실현을 위한 정보관리체계 ISMS(Information Security Management System)와 기관과 기업이 개인정보보호 관리체계를 갖추어 체계적이고 지속해서 수행하는 데 필요한 보호조치가 표준에 맞게 구축되어 있는지 인정을 해주는 인증제도 PIMS(Personal Information Management System)가 있다. 정보보호 중요성이 높아짐에 따라 ISMS와 PIMS를 통합하여 관리체계기반을 점검 및 개선하고 보호 대책 요구사항 64가지와 개인정보 처리단계별 요구사항 22개를 통합 인증하는 ISMS-P를 시행 중이다. 즉 정보보호 관리체계 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 인증하는 제도로 기존의 ISMS 의무대상자는 ISMS, ISMS-P를 선택해서 인증을 취득할 수 있다. ISMS-P는 기존에 시행하던 ISMS와 PIMS의 정책 중 유사하거나 중복된 부분을 통합하고 유지와 관리, 비밀번호 관리, 정보 주체권리 등이 하나로 통합 및 수정되었으며, 최신 기술 동향인 핀테크(Financial Technology), 클라우드 서비스 등을 반영하여 신규 정책을 추가하여 최신 기술과 흐름도 반영되었다.

ISMS-P의 인증 대상자는 자율신청자와 의무신청자가 존재하며 내용은 다음과 같다.

구분	의무대상자 기준
ISP	전기통신사업법 제6조 제1항에 따른 허가를 받은 자로서 서울특별시 및 모든 광역시에서 정보통신망 서비스를 제공하는 자
IDC	정보통신망법 제46에 따른 집적정보통신시설 사업자
하나라도 해당하는 경우	연간 매출액 또는 세입이 1,500억 원 이상인 자 중에서 다음에 해당하는 경우 - 의료법 제3조의4에 따른 상급 종합병원 - 직전 연도 12월 31일 기준으로 재학생 수가 1만 명 이상인 고등교육법 제2조에 따른 학교
	정보통신서비스 부문 전년도(법인 경우 전 사업연도) 매출액이 100억 원 이상인 경우
	전년도 직전 정보통신서비스 이용자 수가 3개월 일일 평균 100만 명 이상인 경우

[표 2-1] ISMS-P 인증 의무대상자

자율신청자는 표[2-1]에 해당하는 의무대상자에 속하지 않으나 자율적으로 정보보호 관리체계를 구축하여 운영하는 기업, 기관을 의미한다.

2.1.1 정보보호 관리체계(ISMS-P) 기준 및 과정

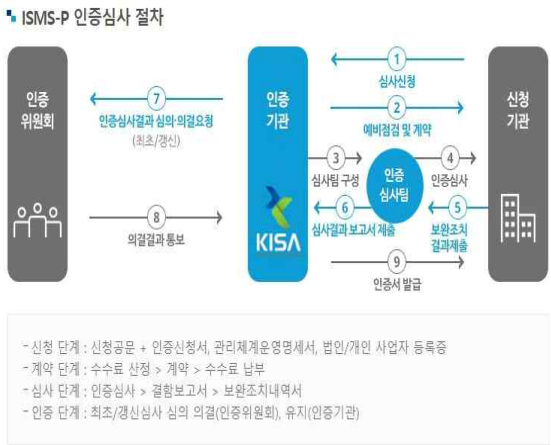
[그림 2-1] ISMS-P 인증기준

최초 정보보호를 위해 ISMS가 존재했다. 하지만 뒤늦게 개인정보보호에 대한 인식이 커지면서 PIMS를 신설했으나, 두 가지 기준을 만족하게 하기 위해서는 인증을 두 번 받아야 하는 번거로움이 있었다. 그래서 기존 정보보호 항목이 들어간 ISMS와 개인정보 보호 항목이 들어간 PIMS를 합쳐서 ISMS-P를 신설했다. 기존 ISMS 항목 중 관리체계 수립 및 운영 관련 16개, 보호 대책 요구사항 64개를 비롯해 개인정보 처리단계별 요구사항 22개가 포함되어 있다.

기존 ISMS, PIMS와 같이 KISA에서 진행되며 절차는 [그림2-2]와 같다. 심사종류는 아래 [표 2-2]와 같다.

종류	설명
최초심사	처음으로 인증을 취득할 때 진행하는 심사. 인증 내용에 중요한 변경이 있을 경우 다시 인증을 신청하여 실시하는 심사도 포함. 인증 취득 시 3년의 유효기간 부여
사후심사	인증 취득한 후, 정보보호 관리체계가 지속적으로 유지 및 관리되고 있는지 심사하는 것으로 인증 유효기간 중 매년 1회 이상 시행하는 심사.
갱신심사	ISMS-P 인증 유효기간을 연장하는 것이 목적인 심사.

[표 2-2] ISMS-P 심사종류



[그림 2-2] ISMS-P 인증심사 절차

ISMS-P는 정보보호를 목적으로 한 ISMS와 달리 개인정보보호까지 인증하므로 인증범위 역시 차이가 있다.

구분	설명
ISMS-P	정보서비스를 운영하거나 보호하는 데 필요한 정보자산, 물리적 위치, 조직. 개인정보 처리를 위한 수집, 보유, 이용, 제공, 파기에 관여하는 개인정보 처리 시스템, 취급자 포함.
ISMS	정보서비스의 운영 및 보호에 필요한 조직, 물리적 위치, 정보자산.

[표 2-3] ISMS-P와 ISMS의 인증범위

2.1.2 정보보호 관리체계(ISMS-P)의 필요성

2002년 첫 시행 된 ISMS는 국내 정보보호 산업에 있어 빠질 수 없는 제도 중 하나이다. 정보통신기술의 발달과 함께 정보의 중요성이 증가함에 따라 정보보호 진단 대상과 그 범위에 따라 민간기업 대상인 ISMS, 공공기관 대상인 G-ISMS, 금융기관에 적용되는 F-ISMS, 개인정보 걸음마다 관리체계인 PIMS, 개인정보보호 인증제(PIPL) 등 수 많은 제도가 도입되고 운영되었다. 하지만, 동일 유사항목에 대한 인증제도가 여러 개 운영됨에 따라 통합된 관리의 필요성이 대두되었다. 기존에 있던 ISMS의 인증범위는 서비스 운영 중심이었고, PIMS는 개인정보를 중심으로 개인정보 처리를 위한 정책 중심으로 운영되었다. 이러한 문제점을 해결하기 위해 2018년 ISMS-P는 유사하거나 중복되는 항목을 통합 및 재배치하고 핀테크, 클라우드 서비스 등의 최신 기술 및 흐름을 반영함으로써 더욱 발전된 형태를 갖추었다.

현재 ISMS-P는 기업이 정보 및 개인정보보호를 위해 최소한 기준 이상의 업무 환경과 프로세스를 갖추었는지 그리고 유지하는지 검증하는 것이다. ISMS-P의 인증이 어떠한 침해 공격에도 안전하다는 것이 아니라 자사의 시스템 보안성을 향상해 주는 디딤돌이다.

2.1.3 국내 표준 클라우드 보안과 국제 표준 클라우드 보안 비교

지난 2015년 3월에 “클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률”(이하 클라우드 발전법)이 제정, 시행됨에 따라 클라우드 정보보호 대책은 1. 클라우드 사업자의 정보보호 수준 향상 및 공격 대응체계 구축, 2. 클라우드 이용자 정보보호 기반 구축, 3. 클라우드 정보보호 기업 육성 등의 과제로 단계적 추진 중이다. ICT 활용 패러다임이 기존의 소프트웨어 솔루션 등을 자체적으로 보유하여 직접 서버에 설치해 운영하는 방식인 On-Premise(온프레미스) 방식을 사용하였다면 최근 이용자의 요구에 맞춰 네트워크를 통해 원하는 자원을 제공하는 On-Demand(온디맨드) 방식으로 전환되는 추세로 주요 클라우드 사용 국가에서는 공공의 클라우드 우선정책(Cloud First)을 통해 민간 클라우드 서비스 확산을 추진하고 있다. 먼저, 국외의 클라우드 보안 정책을 살펴보면 다음과 같다.

1. 미국: 미 연방정부가 사용하는 클라우드 보안인증을 위한 FED RAMP 프로그램 수립, 운용
   인증 명: FedRAMP
   심사기준: NIST SP 800-53
2. 영국: 정부 인가제도 운용하여 클라우드 서비스의 보안 수준을 측정
   인증 명: UK G Cloud
   심사기준: ISO/IEC 27001 + 자체규정
3. 일본: 클라우드의 안전성, 신뢰성 검증을 위한 인증제도운영
   인증 명: ASP 인증
   심사기준: 클라우드 서비스의 안정, 신뢰

성에 관한 정보 공개 지침

다음으로 국내의 경우 앞서 설명한 “클라우드 발전법” 시행에 따른 후속 조치로 국내 클라우드 민간 사업자들에게 공공부문 서비스 제공 권한을 부여하는 보안인증 기준인 “클라우드 보안인증제”를 제정하고 시행 중이다.

[그림 2-3] 클라우드 보안인증제 조직

출처: KISA

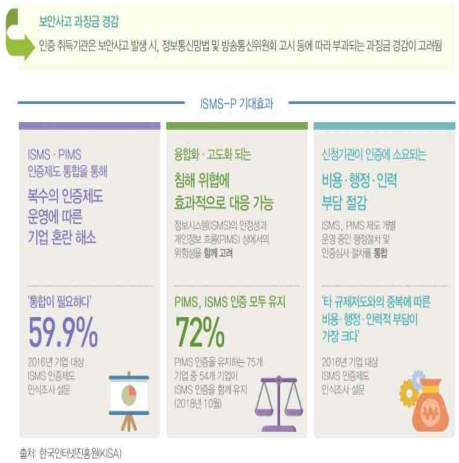
클라우드 보안 인증제도는 인증받는 클라우드 시스템의 상황과 종류에 따라 IaaS/SaaS 표준등급과 SaaS 간편 등급으로 나뉜다. (그림 2-4 참조). 최초평가는 처음으로 보안인증을 취득할 때 진행하는 평가로, 인증 기간 중 중요한 변경사항이 있으면 변경사항에 대한 상시평가가 이루어질 수 있다. 최초평가 통과 시 5년의 유효기간, SaaS 간편 등급은 3년의 유효기간을 부여하며 사후평가는 인증을 취득한 이후에 클라우드 서비스 보안 평가 및 인증기준을 준수하고 있는지 확인하는 평가이다. 인증 유효기간인 3년~5년 안에 매년 시행해야 한다. 갱신평가는 인증 유효기간이 만료되기 전에 클라우드 서비스에 대한 인증기간 연장을 원할 때 실시한다. 갱신평가 통과 시 3~5년의 유효기간을 다시 부여한다.

[그림 2-4] 국내 평가·인증 종류

출처 : KISA

평가·인증범위 기준은 클라우드 서비스에 포함되고 관련 있는 자산(시스템, 설비 등), 지원서비스 등을 포함하여 설정한다. (온·오프라인 자산 및 지원서비스로 서비스 운영 및 관리하여 안전성 및 신뢰성을 확보한다.)

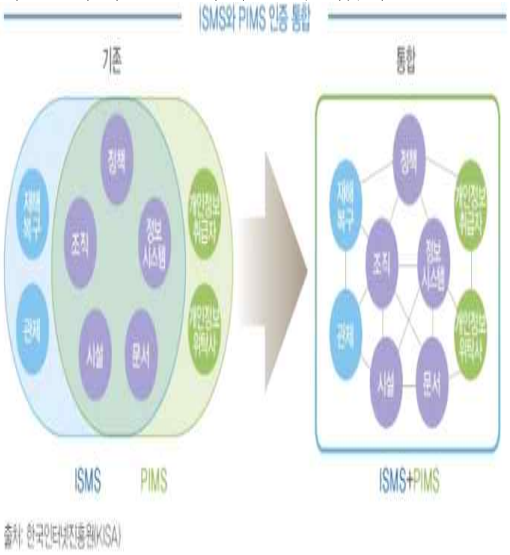
2.1.4 정보보호 관리체계(ISMS-P)의 기대효과



[그림 2-5] ISMS-P 기대효과

ISMS-P 시행 전 ISMS, PIMS를 각각 시행했을 때 중복되는 요구사항의 존재와 추가로 드는 인증비용 때문에 ISMS와 PIMS를 하나로 통합하여 기업 혼란 해소가 필요하다는 의견이 60%에 육박했다.

통합 후 각각 따로 운영되는 분야를 한 곳에 묶어 관리가 더 쉽고 비용이 절감되는 효과를 보였다. 또한, 정보보호와 개인정보 보호를 함께 고려하는 시스템이 구축되기 때문에 기존 인증제도보다 침해 위협에 더욱 효과적으로 대처할 수 있다.



[그림 2-6] ISMS-P 통합 전후

2.2 클라우드 컴퓨팅 개요

클라우드 컴퓨팅이란 컴퓨터 작업에 필요한 요소들을 인터넷을 통해 제공하는 서비스를 의미한다. 필요로 하는 SW를 개인 단말장치에 설치할 필요 없이 클라우드 네트워크를 통해 사용할 수 있고 장소, 시간에 구애받지 않고 필요한 자료를 사용, 공유가 가능하다. 데이터 파일, 소프트웨어, OS, 메모리, CPU 등의 모든 요소를 자신의 단말장치에 설치하지 않고 인터넷상의 어딘가에 두어 스마트폰이나 컴퓨터, TV로 접근하여 이용하면, 구매해서 이용하지 않아도 언제 어디서든 작업을 할 수 있다. 클라우드 컴퓨팅은 인터넷을 통해 사용자가 원하는 요소를 유료나 무료로 제공하며, 사용자가 몇 명이건 사용할 수 있어야 한다. 또한 클라우드가 몇 대의 컴퓨터로 구성되건 사용자는 자신만의 컴퓨터 한 대를 사용하는 것처럼 쓸 수 있어야 한다. 특히 사용자는 클라우드의 서비스가 어떻게 구현되는지 알 필요가 없으며 관리하지 않아도 되므로 비용을 아끼고 효율을 높일 수 있다.

2.2.1 클라우드 컴퓨팅 서비스 분류

클라우드 서비스는 일반적으로 SaaS, PaaS, IaaS 3종류로 구분할 수 있다.

구분	모델	
서비스모델	IaaS	클라우드 서비스가 가능하기 위해 필요한 인프라(Infrastructure)에 관한 서비스
	PaaS	플랫폼 제공형태의 서비스
	SaaS	클라우드의 인프라와 플랫폼에서 구동하는 응용 소프트웨어와 데이터베이스 등을 온디맨드 형태로 제공하는 서비스

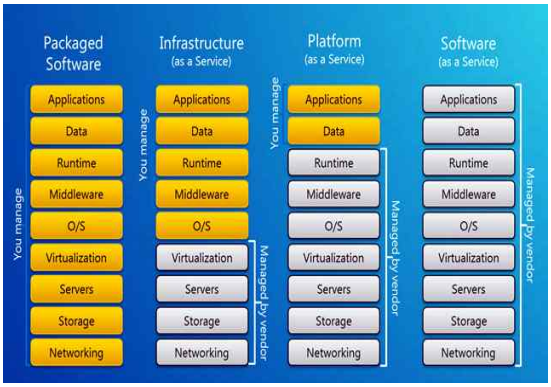
[표 2-4] 클라우드 서비스모델 구분

SaaS(Software as a Service)는 클라우드, 인터넷 등에서 네트워크를 통해 접속하여 애플리케이션의 기능을 제공하는 서비스다. 기존의 설치형 SW를 대체할 수 있는 수단으로 떠오르며 애플리케이션을 조직이나 개인에게 쉽게 제공되는 방식을 의미한다. 서비스 제공의 관점에서 볼 때 소비를 목적으로 해서 사용자는 개발 및 데이터에 대한 추가적인 부담이 없다. 대표적인 SaaS로는 구글 닥스(Google docs)가 있다. 자신의 PC에는 추가적인 설치 없이 PC나 스마트폰 웹을 통해 스프레드시트나 pdf, 프레젠테이션, 워드 프로세서 등으로 사용

할 수 있다.

PaaS(Platform as a Service)는 앱 개발과 관련된 인프라를 직접 만들고 유지 보수할 필요 없이, 간편하게 사용자가 애플리케이션을 개발, 실행, 유지보수 할 수 있도록 플랫폼 형태로 제공한다. 서비스를 개발할 수 있는 플랫폼과 그 플랫폼을 이용하는 프로그램을 개발할 수 있는 API까지 제공한다. 개발자와 개발사에 인프라 또는 OS, 플랫폼 관리에 대한 부담을 줄여주고, 플랫폼 제공업체의 기술력을 통해 원하는 시스템을 개발할 수 있으므로 개발자들을 위한 서비스에 가깝다. 대표적인 PaaS로는 Microsoft, IBM, Redhat이 있다.

IaaS(Infrastructure as a service)는 서버 운영에 필요한 네트워크, 하드웨어, 서버, 디스크 등의 요소를 제공하는 클라우드 서비스이다. 클라우드에서 이를 구현하므로 IaaS는 가상 데이터 기술을 기반으로 이루어진다. 제공업체는 서비스를 이용하기 위한 환경만 제공하며, 애플리케이션, 데이터, OS 등 개발환경을 모두 개발자가 구성한다. 이때, 다양하고 복잡한 다수의 장치를 특정 기술요소가 아닌 광범위한 기술요소를 종합하여 클라우드 컴퓨팅을 구현, 제공하기 위하여 확장성 있는 한 대의 장치처럼 캡슐화하여 제공한다. 대표적인 IaaS로는 아마존(Amazon)이 있다.



[그림 2-7] 각 클라우드 서비스의 제공범위

2.2.2 IaaS, SaaS 클라우드 컴퓨팅 취약점

클라우드 컴퓨팅은 설치할 칠요 없이 원하는 서비스를 이용하라 수 있고 데이터가 온라인상에 있기에 여러 기기와 연동이 잘 된다는 장점이 있다. 반면에 저장 공간이 많이 있더라도 애플리케이션의 설치나 서비스 지원이 불가능할 수 있고, 클라우드 컴퓨팅의 핵심 원천인 서버가 공격받을 때 개인정보의 유출이 우려된다는 단점이 있다. 그 때문에 정보의 유출과 같은 개인정보 보안 문제는 클라우드 서비스의 보안 문제 중 1순위 문제로 대두되고 있다.

IaaS, Saas 클라우드 컴퓨팅의 보안은 크게 두 가지로 기술적 보안과 운영적 보안으로 분류한다. 기술적인 보안 구성에는 서비스 제공자와 관련된 인프라, 데이터, 네트워크 통신 부분과 애플리케이션과 관련되어 있고. 운영적 보안의 구성에는 조직의 운영방안, 서비스 정책 수립, 사고 관리, 자사 통제 같은 요소들로 구성되어 있으며 서비스의 제공자와 이용자 모두와 관련된 보안이다.

클라우드 서비스에서 발생한 보안사고를

분석해보면 데이터보안의 책임자가 변화하였을 때 보안사고에 미치는 영향을 알 수 있다. 2018년까지 클라우드 컴퓨팅의 보안사고 유형으로는 작업으로 인한 장애, S3 서버 관리자의 실수, DNS 서버 설정 오류, 관리자의 실수로 인한 데이터 및 백업 파일 삭제 및 유출 등 보안사고의 95% 정도가 관리 부주의로 발생한 것이다. 최근 2019년까지 꾸준히 제기되던 클라우드 사용자와 업체에 의한 데이터 손실과 취약점, 공유기술의 취약점, 서비스 거부 공격(DDoS) 등이 제외되고 클라우드를 구성하는 기술 자체에 대한 문제가 제시되면서 기존 서버 시스템을 클라우드 서버로 옮겨오는 클라우드 마이그레이션 및 서비스 활용사례를 참고하여 더욱 효과적인 클라우드 사용법을 도출할 수 있는 클라우드 우선 적용(Cloud First)을 위한 단계로 발전하고 있다.

또한, 클라우드의 주요 보안 허점인 공유자원 문제와 가상화 기술 문제가 있다. 먼저 공유자원 문제는 데이터 파일의 정확한 저장 위피를 알 수 없고, 데이터가 흩어져 있다는 점이 보안 우려의 주요 요인이다. 가상화 문제는 가상화 기술 환경에 의해 발생할 수 있는 보안 문제로 가상화로 인해 기존 보안 문제의 방어가 어려워지거나 이에 따른 영향이 커지는 문제다.

클라우드 컴퓨팅의 보안 문제에 관련하여 CSA(Cloud Service Alliance)에서는 클라우드 컴퓨팅 위협 7가지를 발표했다. (표 2-5 참조).

위협	문제점
남용 및 불손한 사용	악의적인 의도를 가지고 클라우드 서비스를 도입한다면 기존의 봇넷보다 더 위험한 위협이 될 수 있다.
안전하지 않은 API	애플리케이션 구축 시 안전하지 않은 코드 재사용 및 합성 사용 시 보안 위험성이 높아진다.
내부 스파이	도덕적으로 적합하지 않은 사람을 고용할 시 문제가 발생할 수 있다.
데이터 손실 및 유출	가상머신을 적절히 관리하지 않으면, 서비스 전체가 위협받을 수 있다.
공유기술 취약점	
서비스 및 트래픽 하이재킹	클라우드 컴퓨팅 특성 상 하이재킹 기법에 매우 취약하다.
공개되지 않은 위협	시스템의 구성과 소프트웨어 패치 실행의 문제점 증가.

[표 2-5] CSA 클라우드 7대 위협

2.3 IaaS, SaaS 클라우드 보안대책

앞선 [표 2-5]에서의 CSA 보안 위협 대책은 다음의 [표 2-6]이다.

위협	위협 방지 대책
남용 및 불손한 사용	사용자 신원 검증을 강화하고 프로세스에서 자체적으로 네트워크 보안을 위한 블랙리스트 모니터링 시행.
안전하지 않은 API	익명 사용자가 서비스 접근 시 보안을 강화하는 보호 기능 설계 필요
내부 스파이	명확한 인사 관리 요건 규정하고 직원들에게 정보보안에 관한 문제점과 관리 운영 방식에 대한 책임감 및 투명성에 관련된 규정 준수 요구
데이터 손실 및 유출	무단 변경이나 활동 발생 시 실시간 환경 모니터링, 강력한 인증 시행 및 액세스를 제어하며 주기적인 기술 취약성 검사와 구성 감시 시행
공유기술 취약점	
서비스 및 트래픽 하이재킹	계정 공유 금지하고 단일인증이 아닌 이중 인증 기술 권장, 무단 접근을 방지하기 위한 모니터링 필요
공개되지 않은 위협	해당 로그 및 데이터 공개 인프라 정보 공개

[표 2-6] CSA 클라우드 7대 위협 보안대책

클라우드 서비스 제공자는 클라우드 사용자의 서비스 업무 영역별 적용되는 법적 요구사항을 수립하여 클라우드 컴퓨팅법, 신용정보법, 개인정보 보호법 등의 컴플라이언스를 준수해야한다. 또한 사용자가 클라우드 서비스를 이용 시 안전성, 가용성, 무결성이 확보되도록 클라우드 서비스 보안인증제(CSAP), ISMS-P, ISO/IEC 27001 등의 보안기준 준수와 이를 서비스 사용자와의 서비스 표준계약서(SLA)를 통해 반영할 수 있도록 노력해야 한다.

클라우드 서비스 사용자 또한 클라우드 서비스에 대한 전반적인 아키텍처를 이해하고 IT 자원과 체계를 파악해 필요한 업무형태나 목표에 맞춰 클라우드 마이그레이션 결정 및 수행이 필요하다. 그리고 클라우드 서비스 업무 이전 후에는 운영관리, 구성관리, 보안관리, 성능 및 가용성 관리 등 안정적인 서비스 운영을 위하여 운영체계와 프로세스의 수립이 필요하다.

클라우드에서 사용할 수 있는 보안 솔루션은 여러 종류가 있지만 크게

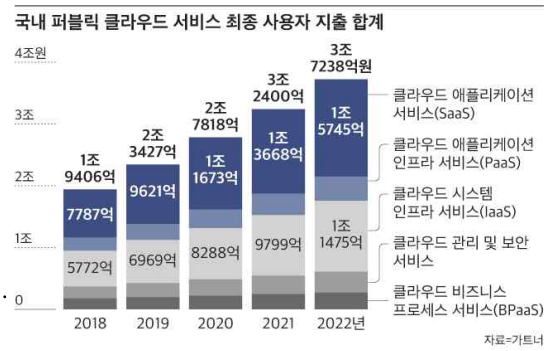
1. 클라우드 가시성 및 데이터 보호.
2. 클라우드 보안 접근 중개 (CASB).
3. 상향식 접근방식을 이용하여 워크로드의 침해시도를 탐지하고 방어하는 클라우드 워크로드 플랫폼(CWPP).
4. 클라우드 보안 형상 관리(CSPM)를 수행하여 클라우드 서비스 구성의 위험평가로 요약된다. 클라우드 보안 솔루션 대응 범위가 넓어지면서 네트워크 기반의 공격에 대한 솔루션과 APT 공격이나 애플리케이션 공격 솔루션까지 포함되어 안정성 있게 운영할 수 있다.

물론 클라우드 보안 솔루션 도입으로 클라우드 보안의 모든 문제 해결되는 것은 아니다. 보안 솔루션 도입과 동시에 클라우드의 서비스 사용 목적과 수준을 기반으로 솔루션의 적용대상과 범위산정이 필요하다. 클라우드 서비스는 서비스 형태에 따라 가시성이 확보되지 않는 경우가 발생하기 때문에 서비스 운영 같은 우선순위가

높은 요소는 서비스 연속성과 장애발생시 대응 및 복구가 가능하도록 프로세스 수립(BCP)과 공격사고가 발생하였을 때의 업무 프로세스를 세우는 것이 필요하다. 이는 클라우드 마이그레이션을 반영하여 클라우드 서비스의 적합성과 효율성에 대해 참고해야 하는 항목이다. 클라우드 보안 아키텍처 수립 시 현재 체계나 프로세스에 알맞게 운영되고 있는지 권한관리, 암호화/복호화 키 관리, 데이터베이스 관리, 계정관리 등 인프라 취약점을 주기적으로 관리해야 하며 모니터링에 대한 대책이 필요하다.

Ⅲ. 결 론

2019년, IT 리서치 기업인 “가트너”의 분석에 따르면 세계 공공 클라우드 서비스 시장 규모가 약 2143억 달러(약 243조 원)에 달할 것이라는 분석 결과가 나왔다. 한국의 퍼블릭 클라우드 서비스 시장 규모는 2조3428억 원에 이르렀다. 2018년 국내 퍼블릭 클라우드 서비스 시장의 매출액은 1조 9407억 원으로 2018년에 비해 21% 증가한 수치다. 국내의 클라우드 시장은 SaaS가 가장 큰 비중을 차지한다. 국내 SaaS 사용자 지출액은 2018년 약 7787억 원으로 지속적으로 증가해 2022년에는 약 1조5745억 원에 도달할 것으로 예상한다. 또한, IaaS의 지출액도 높은 증가율을 보인다. 가트너는 “국내 IaaS의 최종 사용자 지출액 규모는 2018년 5773억 원에서 지속적으로 성장해 2022년에는 1조1475억 원에 달할 것”이라고 예상했다.



[그림 3-1] 국내 퍼블릭 클라우드 매출액

또한, 라이선스 기반 비용을 지불하는 소프트웨어의 소비는 감소하는 반면 사용량에 따른 일정 기간마다 비용을 내 사용하는 SaaS 같은 구독형 클라우드 기반 소프트웨어 소비는 계속 증가하여 2022년까지 클라우드 서비스 시장 규모는 3배 이상의 성장세를 이룰 것이라고 예상한다.

하지만, 이런 가파른 성장세에도 불구하고 국내 클라우드 관리 기업 중 ISMS-P 인증을 받은 기업은 단 한 곳뿐이다.

국내 최대 클라우드 관리기업인 메가존 클라우드가 국내 업계 최초로 정보보호 통합 인증(ISMS-P)을 2020년 5월 13일 획득했다. 위 업체는 ISMS 인증, 정보보안(ISO/IEC 27001)·클라우드 보안(ISO/IEC 27017)·클라우드 개인 정보보안(ISO/IEC 27018) 등 ISO/IEC 국제인증 3개 부문 인증을 획득한 바 있다. 이처럼 개인정보 문제가 대두되면서 기존 클라우드 인증을 받

았음에도 불구하고 ISMS-P가 새로운 보안대책으로 떠오르고 있다.

앞서 2.1.2에서 언급했듯이 ISMS-P는 기업의 안정적인 보안을 위한 첫 발걸음이다. ISMS-P의 요구사항을 만족하여 인증을 받게 된다면 신뢰성 있는 클라우드 컴퓨팅 서비스를 제공할 수 있으므로 ISMS-P의 필수 인증 대상자가 아닌 자율 인증 대상자일지라도 ISMS-P 인증을 받는 것이 권장되는 바이다.

***

References:

[1] igloosec.co.kr

[2] softcamp official blog

[3] SPRi , “Key Issues and Countermeasures in Cloud Security”, vol. 17-006, 2017.

[4] 홍성욱 저, “Effective Management of Information Security Management System(ISMS) and Personal Information Management System(PIMS) Authentication system“, pp 1-7, 2017.12

“ISMS와 PIMS 인증제도의 효과적인 운영방안”, 2017.12

[5] Hee-Kyung Kong, “Research Tends in Economic Effects of Information Security Certification: Focused on the ISMS”, pp 2-3, 2016

[6]https://biz.chosun.com/site/data/html_dir/2019/04/03/2019040302058.html

[7] https://wnsgml972.github.io/network/2018/08/14/network_cloud-computing/

[8] 한국 인터넷 진흥원, KISA

[9] 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시(2018. 11. 7, 제2018-80호)

[10] 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 (2019. 6. 13, 통령령(제29852호))

[11] 클라우드 컴퓨팅서비스 다수공급자계약 특수조건(2019. 2. 1 조달청공고(제2019

-23호))