최종연구보고서	KISA-WP-2024-0016

클라우드 분야 개인정보 보호조치 현황 분석

수탁기관 : 포유씨큐리티

2024.04

KISA 한국인터넷진흥원

본 보고서에 수록된 내용은 집필한 연구자의 의견이며,
한국인터넷진흥원의 공식 의견이 아님을 밝힙니다.

제 출 문

한국인터넷진흥원 원장 귀하

본 보고서를 “클라우드 분야 개인정보 보호조치 현황 분석”의 최종연구개발 결과보고서로 제출합니다.

2024년 04월 30일

수탁 기관 : 포유씨큐리티
연구책임자 : 대 표 이 사 옥 은 택 (포유씨큐리티)
참여연구원 : 수석컨설턴트 신 동 훈 (포유씨큐리티)
선임컨설턴트 옥 은 미 (포유씨큐리티)
전임컨설턴트 나 지 원 (포유씨큐리티)

요 약 문

1. 제목

ㅇ 클라우드 분야 개인정보 보호조치 현황 분석

2. 연구개발의 목적 및 중요성

ㅇ 클라우드 서비스 제공사업자(Cloud Service Provider, 약칭 'CSP')의 개인정보 보호조치 현황을 분석하여, 클라우드 분야 민관협력 자율규제 추진 시 활용하고자 함

3. 연구개발의 내용 및 범위

ㅇ 국내·외 클라우드 서비스 제공사업자 현황 조사
ㅇ 클라우드 서비스별 개인정보 보호조치 현황 조사
ㅇ 클라우드 인증 항목과 개인정보 처리 위·수탁 점검항목 비교·분석
ㅇ 클라우드 환경에 적합한 안전성 확보조치 고시 개선방안 마련

4. 연구결과

ㅇ 클라우드 서비스 제공사업자의 일반현황(매출액, 사용자 수 등)을 조사하고 이를 기준으로 조사대상 상위 사업자를 선정함
ㅇ 클라우드 이용사업자가 개인정보의 안전성 확보조치기준 고시를 준수할 수 있도록 클라우드 서비스 제공사업자가 마련한 보호조치기능 현황을 조사·분석함
ㅇ 클라우드 보안 인증항목과 개인정보 처리 위·수탁 점검항목을 비교하여 양자의 대체가능성을 판단함
ㅇ 클라우드 환경에서 현행 개인정보 안전성 확보조치 제도와의 간극을 진단하고 향후 합리적인 법집행 방향성을 제안함

5. 활용에 대한 건의

ㅇ 클라우드 분야 민관협력 자율규제 추진을 위한 기초자료 및 규약 방향성 도출을 위한 보안전문가 의견자료로서 활용 가능

6. 기대효과

ㅇ 국내 기업이 이용하는 주요 클라우드 환경에서 개인정보 안전성 확보 및 합리적인 제도 운영에 기여할 것으로 기대됨

목 차

제 1 장 개 요 ····· 1
제 1 절 연구의 목적 ····· 1
제 2 절 수행 범위 ····· 1
제 3 절 수행 인력 ····· 2

제 2 장 국내·외 클라우드 서비스 제공사업자 현황조사 ····· 3
제 1 절 클라우드 서비스 사업자 일반현황 및 조사대상 선정 ····· 3
제 2 절 클라우드 사업자 주요서비스 흐름분석 ····· 5

제 3 장 클라우드 제공 보호조치기능 현황조사 ····· 14
제 1 절 조사 항목 선정 ····· 14
제 2 절 조사대상 클라우드 서비스의 보호조치기능 제공현황 ····· 21

제 4 장 클라우드 인증항목과 수탁사 점검항목 비교 ····· 26
제 1 절 수탁사 점검항목 도출 ····· 26
제 2 절 수탁사 점검항목과 클라우드 인증항목의 유사도 분석 ····· 31
제 3 절 수탁사 점검범위와 클라우드 인증범위의 중첩도 분석 ····· 40

제 5 장 클라우드 환경에 적합한 안전성 확보조치 제도 집행방안 제언 ··· 42
제 1 절 클라우드 제공사업자의 수탁자 지위 명확화 필요성 ····· 42
제 2 절 클라우드 제공 보호조치기능 관련 제언 ····· 45

[첨부 1] 클라우드 분야 개인정보 보호조치 현황조사 세부 결과 ····· 47

(별첨 1) 대상사업자 일반현황 및 보호조치기능 현황조사 세부 결과

(별첨 1) 수탁사 점검항목과 클라우드 인증항목 비교 세부 결과

제 1 장 개 요

제 1 절 연구의 목적

본 연구는 클라우드 분야 민관협력 자율규제 추진에 앞서 클라우드 서비스 제공사업자(Cloud Service Provider, 약칭 'CSP')의 개인정보 보호조치 현황을 조사·분석하여 시사점을 도출하는 것을 목적으로 한다.

이를 위해 국내·외 주요 클라우드 서비스 제공사업자를 선정하여 서비스 제공 형태, 개인정보 처리·흐름 및 개인정보 보호를 위한 안전성 확보조치 현황을 조사하고자 한다. 정보 보안 및 개인정보 보호 관련 인증체계와 개인정보 보호 법령이 요구하는 보호조치 항목을 비교하며, 클라우드 영역에서 개인정보 보호를 위한 제도적 요구사항을 도출하고자 한다.

제 2 절 수행 범위

구분	수행 과제
국내·외 주요 클라우드 서비스 제공사업자 현황조사	■ 주요 클라우드 서비스 제공사업자 현황조사 - 국내·외 클라우드 서비스 제공사업자 중 사업 규모, 매출액, 서비스 분야, 인지도 및 이용자 수를 고려하여 조사대상 상위 IaaS, SaaS 사업자 선정 - 선정된 IaaS, SaaS 서비스 흐름분석
클라우드 서비스별 보호조치기능 현황조사	■ 클라우드 제공 보호조치기능 현황조사 - 클라우드 이용사업자가 개인정보 안전성 확보조치기준 고시를 준수할 수 있도록 하기 위하여 IaaS, SaaS에서 제공되어야 하는 보호조치기능 항목 도출 - 조사대상 IaaS, SaaS서비스별 보호조치기능 제공여부, 제공방식(필수/선택), 비용부과 여부(유상/무상), 특이사항 등 세부사항 조사

클라우드 인증 항목과 개인정보 처리 위·수탁 점검항목 비교·분석	■ 클라우드 분야 개인정보 처리 위·수탁 점검항목·범위와 보안인증 항목·범위 비교분석 - 개인정보보호법, 안전성 확보조치기준 고시 등을 고려하여 클라우드 환경에 적합한 수탁사 점검항목 도출 - 클라우드 서비스 제공사업자들의 클라우드 보안인증(ISMS-P, CSAP, ISO27002/18) 취득현황 조사 - 수탁사 점검항목과 클라우드 인증항목의 유사도 분석 - 수탁사 점검범위와 클라우드 인증범위의 중첩도 분석
클라우드 환경에 적합한 안전성 확보조치 고시 개선방안 마련	■ 클라우드 서비스 환경에 적합한 개인정보 안전성 확보조치 제도 집행방안 제안 - 클라우드 제공사업자의 수탁자 지위 명확화 필요성 도출 및 이를 전제로 한 클라우드 서비스 제공사업자 개선방안 도출(이용사업자의 개인정보 처리 시 CSP 통지절차 마련, 클라우드 이용사업자측 해킹사고 원인조사 시 CSP 수검의무 부과, 이용종료 시 파기확인서 제공 등) - 클라우드 이용사업자에게 제공되는 보호조치기능 관련 합리적인 법집행 방향성 제시

제 3 절 수행 인력

구분	이름	직급	등급	담당업무
포유씨큐리티	옥은택	대표	특급	사업총괄(PM)
포유씨큐리티	신동훈	수석	특급	보호조치 현황분석, 고시 개선(안)
포유씨큐리티	옥은미	선임	중급	조사분석, 사업지원
포유씨큐리티	나지원	전임	초급	조사분석, 현황조사

제 2 장 국내·외 클라우드 서비스 제공사업자 현황조사

제 1 절 클라우드 서비스 사업자 일반현황 및 조사대상 선정

클라우드 서비스 제공사업자별 매출액은 기업공시 등 공개자료, 언론 보도 자료 등을 통하여 조사하였다. 한편, 클라우드 서비스 제공사업자의 법인 전체 매출액이 공개되어 있을 뿐, 개별 서비스 매출액 자료는 공개되어 있지 않은 관계로 법인 전체 매출액을 기준으로 자료를 조사하였다. 이용자 수는 클라우드 서비스 제공사업자의 홈페이지에 대한 방문자 수를 기준으로 측정하였다. 측정 데이터의 객관성을 확보하기 위해, 월간 방문자 수를 측정하는 글로벌 사이트인 Similarweb (https://www.similarweb.com)의 월간 방문자 수(MAU : Monthly Active Users)를 기준으로 조사하였다.

본 개인정보 보호조치 현황조사를 위한 조사 대상은 일반조사 현황을 기반으로 주요 클라우드 서비스를 선정하여 조사하도록 한다. 서비스 사업자 중 시장 인지도 등을 고려하여 현황조사 대상 후보를 선정하여, 매출액, 클라우드 서비스 포털 방문자 수, 이용자 인지도 등을 고려하여 아래 [표 2-1]과 같이 14개 서비스를 선정하였다.

IaaS 분야의 경우 서비스가 동질적이므로 규모 및 인지도를 기준으로 상위 8개 서비스를 선정하는데 별다른 어려움이 없었다.

한편, SaaS 분야의 경우 오늘날 기업용 솔루션은 사내 서버 설치형(on-premise)이 아니라면 사실상 전부 SaaS 방식으로 출시될 정도로 활용분야가 방대하고 시장이 매우 다변화되어 있어 보편적인 기준에서 상위 서비스를 선정하기가 매우 난해하였다. SaaS가 활용 중인 대표적 분야를 예시하면 사내그룹웨어(협업·HR관리), CRM(고객관계관리), ERP(전사자원관리), ITSM(IT서비스관리), 이커머스(쇼핑몰솔루션), 의료(진단·처방) 등이 있는데, 이 중 서로 다른 분야별에서 각 SaaS 서비스를 선정할 경우 동일선상 비교가 되지 않아 연구의 시사점을 도출하기 어려운 문제가 발생한다. 따라서 본 연구에서는 사내그룹웨어 1개 분야에서 상위 SaaS 사업자를 6개 선정하여 비교·분석을 수행한다.

[표 2-1] 조사 대상 클라우드 서비스 선정

#	유형	구분	사업자	서비스명	홈페이지
1	IaaS	국내	네이버클라우드	네이버 클라우드	www.ncloud.com
2	IaaS	국내	엔에이치엔클라우드	NHN Cloud	www.nhncloud.com
3	IaaS	국내	KT cloud	KT 클라우드	cloud.kt.com
4	IaaS	국내	카카오엔터프라이즈	카카오 클라우드	kakaocloud.com
5	IaaS	국내	가비아	가비아 클라우드	cloud.gabia.com/gcloud
6	IaaS	국외	Amazon	AWS	aws.amazon.com
7	IaaS	국외	Google	GCP	cloud.google.com
8	IaaS	국외	Microsoft	Azure	azure.microsoft.com
-	IaaS	국내	삼성SDS	삼성 클라우드 플랫폼	cloud.samsungsds.com
-	IaaS	국내	스마일서브	koreav 클라우드	www.koreav.kr
-	IaaS	국내	이노그리드	퍼블릭클라우드잇	cloudit.co.kr
9	SaaS	국내	네이버클라우드	네이버웍스	naver.worksmobile.com
10	SaaS	국내	디케이테크인	카카오워크	www.kakaowork.com
11	SaaS	국내	KT클라우드	KT BizOffice	cloud.kt.com/bizstore/bizcon/KTBizOffice.jsp#
12	SaaS	국내	가비아	하이웍스	hiworks.com
13	SaaS	국외	세일즈포스	SLACK	slack.com/intl/ko-kr
14	SaaS	국외	젠데스크	Zendesk	www.zendesk.kr
-	SaaS	국외	그린하우스 소프트웨어	Greenhouse	www.greenhouse.com

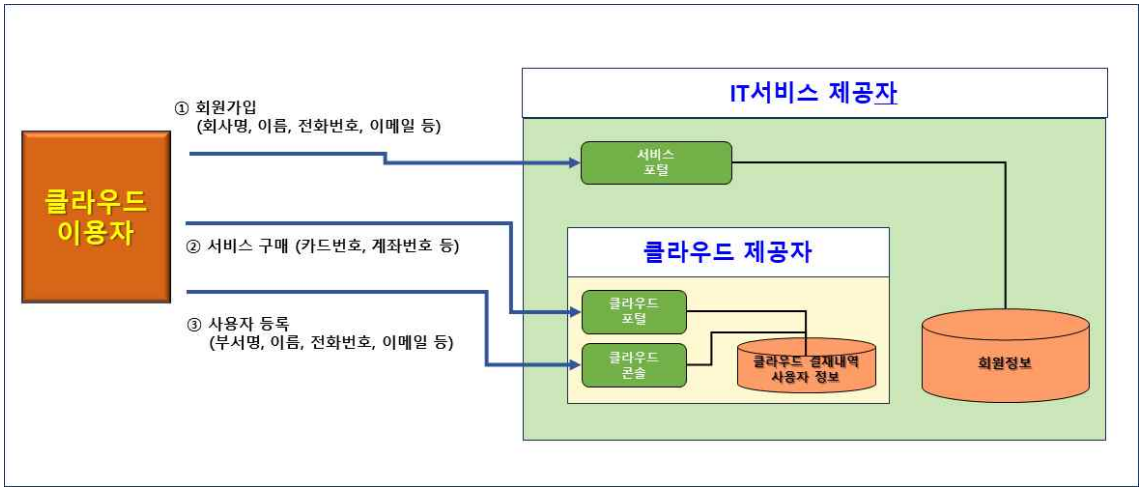
* 법인 매출액 : 공개된 법인 전체 매출액 기준 / ** 이용자 수 : 24년 2월 MAU 기준, 단위 (만명)

제 2 절 클라우드 사업자 주요 서비스 흐름분석

1. IaaS 사업자의 제공서비스 및 흐름분석

조사 대상 IaaS별로 제공되는 주요 서비스와 클라우드 서비스 이용을 위해 접속하는 경로(서비스 가입·신청·설정 흐름)를 분석한 결과는 아래 [그림 2-1]과 같다.

[그림 2-1] IaaS 서비스 흐름도



예를 들어 구글, MS, 가비아 등은 '서비스 포털'에서 회원 가입을 위해 이용사업자 담당자의 개인정보(기관명, 이름, 전화번호, 이메일 등)를 수집한 후, '클라우드 포털' 또는 '콘솔'을 통해 클라우드 서비스 구매(결재정보), 사용자 계정정보(부서명, 이름, 전화번호, 이메일 등) 등록 및 보안설정(개인정보 안전성 확보조치에 관련된 설정)을 한다.

위 구조는 서비스별로 조금씩 다를 수 있다. AWS, 네이버 클라우드, KT 클라우드 등은 별도의 '서비스 포털' 없이 바로 '클라우드 포털'에 접속하여 회원가입, 클라우드 서비스 구매 등을 수행하고, '콘솔' 등을 통해 클라우드 사용자 정보를 등록하고, 보안설정을 한다. 반면, 카카오 클라우드 등은 '서비스 포털' 및 '클라우드 포털'이 없고 대신에 '콘솔'로 직접 접속하여 회원 가입을 위한 개인정보 수집, 클라우드 서비스 신청 및 구매, 사용자 계정등록 및 보안설정을 수행한다. 사업자별 세부 현황은 아래 [표 2-3]과 같다.

본 과제는 클라우드에서 제공하는 개인정보 보호조치기능 현황을 조사하는 것이 주요 목적이므로, 일반적인 서비스 신청 페이지에 불과한 '서비스 포털'의 경우 특별히 서비스 전체에 영향을 미치는 보안설정 옵션(예: 비밀번호 규칙 설정)이 있는 경우에 한하여 해당 항목만 조사하였고, 클라우드 보안설정(접속 IP 통제, 접속로그 분석, 2차 인증 등) 기능을 제공하는 '클라우드 포털' 또는 '콘솔'의 기능을 위주로

진행하였다.

IaaS 서비스를 활용하여 정보통신서비스 등을 구성하는 작업에는 상당한 전문성이 요구되기 때문에, 이용사업자로서는 이를 직접 수행하기 어려운 경우 별도로 매니지드 서비스 제공자(Managed Service Provider)에게 외주를 주어 구성·운영·설정 작업에 도움을 받을 수 있다. 대부분 IaaS 서비스 사업자별로 사전에 업무협약을 맺은 매니지드 서비스 제공자가 있어, 클라우드 이용자가 쉽게 클라우드 플랫폼을 활용하여 정보통신서비스를 구성할 수 있도록 하고 있다. 클라우드 서비스 제공자별 매니지드 서비스 제공자 현황은 본 보고서의 [별첨1]에 첨부하였다.

IaaS 이용사업자는 클라우드 포털·콘솔을 통해 가상화된 정보시스템에 접속할 수도 있으나, 클라우드 내 가상화된 서버, 네트워크, 보안장비 등에 인터넷 서비스(ssh, ftp, https 등)를 이용하여 직접 접속할 수 있다. 특히, 정보시스템 관리자는 익숙하지 않은 클라우드 포털·콘솔보다는 업계에서 서버 설치형(on-premise) 시절부터 보편적으로 사용해온 서버 접근제어 혹은 DB 접근제어 등 도구를 통해 가상화된 정보시스템에 직접 접속하는 것이 작업 효율성이 높을 수 있다.

참고로 이용사업자가 클라우드 포털·콘솔이 아닌 CLI(Command Line Interface), API(Application Programming Interface) 등을 통해서 클라우드 가상서버 등을 이용하는 경우에는 계정 자격증명을 위해 Access Key를 CSP로부터 발급받아 접속하는 것이 보편적이다. 아래 [표 2-2]는 AWS에서의 Access Key 사용 사유 예시이다.

[표 2-2] AWS에서 Access Key 사용 사유 예시

■ AWS Access Key가 필요한 이유
- AWS 서비스 자동화 : AWS CLI, SDK 또는 애플리케이션을 사용하여 S3 버킷에 파일 업로드, EC2 인스턴스 시작, RDS 데이터베이스 쿼리 등 다양한 AWS 작업을 자동화 가능
- 보안 : AWS Access Key는 사용자에게 부여된 권한에 따라 AWS 리소스에 대한 액세스를 제어하는 데 사용됨
- 편리함 : AWS 콘솔에 로그인하지 않고도 스크립트 및 프로그램에서 AWS 서비스에 액세스할 수 있음

■ AWS Access Key 사용 케이스
- AWS CLI : 명령줄 인터페이스를 사용하여 AWS 서비스를 관리에 사용
- AWS SDK : 다양한 프로그래밍 언어에서 AWS 서비스와 상호 작용하는 데 사용
- 애플리케이션 : 자체 애플리케이션을 개발하여 AWS 서비스와 상호 작용할 수 있음

그런데 클라우드 보안사고 사례를 살펴보면 github 등 인터넷에 공개된 곳에 Access Key를 그대로 올려놓거나, 소스코드 내 암호화되지 않은 Access Key를 하

드 코딩하여 이것이 노출되었던 적이 빈번했다. 이에 대한 대응방안으로 Access Key이외에 2차 인증(Multi-Factor Authentication)를 적용하여 보안을 강화하는 방법이 있다. 아래 예시는 AWS 환경 CLI 환경에서 2차 인증을 설정하는 방법에 대한 예시이다.

[표 2-2] AWS CLI 환경에서 2차 인증 설정방법 - 예시

MFA 는 AWS 관리 콘솔 뿐만 아니라 AWS CLI 에서도 사용이 가능합니다. 관리 콘솔에서는 로그인 과정이 별도로 존재하기 때문에 사용자가 로그인을 하는 과정에서 MFA 를 적용받게 되고 MFA 를 사용하여 인증한 사용자는 MFA 사용을 요구하는 IAM 정책에서 문제없이 권한을 부여받을 수 있었습니다. 하지만 AWS CLI 환경에는 Login 과 같은 절차가 존재하지 않습니다. 따라서, 관리 콘솔과는 약간 다른 방식을 통해 MFA 가 사용되며 MFA 를 사용 여부를 확인하기 위한 IAM 정책을 생성할 때도 AWS CLI 에서의 특성을 고려하여 정책을 생성하여야 합니다. 그럼 먼저, AWS CLI 환경에서 MFA 를 사용하는 방법을 살펴 보도록 하겠습니다.

AWS CLI 환경에서 MFA 사용을 증명하기 위해서는 " `aws sts get-session-token` " 이라는 명령을 이용해서 별도의 Session Token 을 발급받아야 합니다. AWS 관리 콘솔에서는 로그인 후 웹 브라우저를 이용하여 MFA 의 적용 여부가 AWS 서비스를 호출할 때마다 지속적으로 반영이 되지만 AWS CLI 는 Login의 절차가 없으므로 자신이 발급받은 Access Key/Secret Key 으로 " `aws sts get-session-token` " 명령을 실행하여 새로운 Session Token 을 발급받음으로써 MFA 인증 여부를 증명하게 됩니다.

1. AWS CLI 를 사용하기 위해서는 먼저 IAM 관리자로부터 부여받은 AWS Access Key와 Secret key 를 AWS CLI 명령어를 이용하여 등록합니다.

   ```
   aws configure --profile profile-name
   ```

   #AWS CLI 중 `--profile` 로 시작하는 부분은 AWS CLI 에 여러 쌍의 Access Key/Secret Key 를 사용하는 경우 구분하기 위한 용도로 사용됩니다. 한 쌍의 Access Key/Secret Key 만을 사용하는 경우라면 이 부분은 생략해도 됩니다.
   참고. AWS CLI 의 설치 방법 또는 업데이트를 참고하세요.

   부여받은 Access Key 와 Secret Key 를 정상적으로 등록하였다면 아래의 명령어를 입력하여 정상적으로 Access Key/Secret Key 가 입력되어 있는 것을 확인합니다.

   Bash
   ```
   aws sts get-caller-identity --profile profile-name
   ```

2. Access Key/Secret Key 가 CLI Profile 에 등록되었다면 이번에는 관리 콘솔에서 등록하였던 MFA 장치의 serial number 를 준비해야 합니다. 이 부분은 MFA 등록 완료 후 아래와 같은 화면에서 확인할 수 있었던 "할당된 MFA 디바이스" 에 나타난 값을 준비하시면 됩니다.

3. MFA Serial Number 가 준비되었다면 아래와 같은 명령어를 입력하여 Session Token 을 발급받도록 합니다.

   Bash
   ```
   aws sts get-session-token --serial-number arn:aws:iam::account-id:mfa/user-a --token-code token
   ```

   정상적으로 MFA 인증이 완료되었다면 아래와 같은 응답을 받게 됩니다.

   JSON
   ```
   {
     "Credentials": {
       "AccessKeyId": "ASIAEXAMPLEKEYID",
       "SecretAccessKey": "gY+LIyWk24rExamPleSecRetV/+MQY1",
       "SessionToken": "IQoExampleSessionEND/////////wEaDmFwLW5vcnRoZWFzdC0yIkcwRQIhAOe13M5fPZ4q(
       "Expiration": "2022-05-27T19:38:59+00:00"
     }
   }
   ```

참고. AWS CLI 를 이용하여 MFA 인증 후 발급되는 Session Token 에는 위 응답에서와 같이 3가지 값이 포함되어 있습니다.

```
Access Key, Secret Key, Session Token
```

4. 사용자는 이 3가지 값을 이용하여 AWS CLI 를 이용해야만 AWS Service 에서 사용자가 MFA 인증을 완료한 사용자인지를 확인할 수 있습니다.따라서, 이 3가지 값을 AWS CLI 에 반영해주어야 하는데요. 적용하는 방법은 여러가지가 있지만 가장 단순한 방법은 아래의 명령과 같이 3개의 값을 각각 환경변수로 등
록하여 사용하는 것입니다.

Bash

```
export AWS_ACCESS_KEY_ID=ASIAEXAMPLEKEYID
export AWS_SECRET_ACCESS_KEY=gY+LIyWk24rExamPleSecRetV/+MQY1
export AWS_SESSION_TOKEN=IQoExampleSessionEND//////////wEaDmFwLW5vcnRoZWFzdC0yIkcwRQIhAOe13M5fF
```

5. 위와 같은 명령을 이용하여 3가지 값을 환경변수로 등록하였다면 아래의 명령을 실행하여 확인하도록 합니다.

Bash

```
aws sts get-caller-identity --profile profile-name
```

AWS CLI 에서의 MFA 사용과 관련한 자세한 사항은 링크를 참고하시기 바랍니다.

* 출처 : https://aws.amazon.com/ko/blogs/tech/all-for-mfa-in-aws-environment/

참고로 클라우드 보안사고 사례를 살펴보면, 이용사업자가 개발하는 프로그램의 소스코드 내 암호화되지 않은 Access Key를 하드 코딩하거나 또는 이것을 github 등 인터넷상 소스코드 저장소에 올려놓은 것이 노출되었던 사고가 빈번했다. 이에 대비하기 위해서는 소스코드 내 Access Key를 '난독화'하는 등의 노출방지 조치를 취하고, 해당 프로그램 운영서버의 IP 주소에서만 Access Key를 통한 접속이 가능하도록 '네트워크 접근제한' 조치가 필요하다. 다만 '2차 인증'을 적용하는 데에는 다소 한계가 있다. 클라우드에 접속하는 것이 사람이라면 2차 인증값을 별도 확인하여 로그인 화면에 입력하면 되지만, 자동화된 프로그램이 Access Key를 가지고 자동 로그인을 하려면 2차 인증값을 가져오는 부분까지 자동화를 해야 한다. 이 경우 2차 인증 자동화 기능도 소스코드에 탑재되어야 하고, 소스코드(및 이에 포함된 Access Key)에 접근할 수 있는 침입자라면 2차 인증 자동화 코드에도 접근할 수 있으므로, 이를 이용해 2차 인증값을 얻어오는 공격은 시간과 비용이 조금 더 소요될 뿐 원천 차단되는 것은 아니기 때문이다.

[표 2-3] IaaS 서비스 흐름 및 주요 제공 서비스 현황

#	사업자	제공서비스	흐름 분석			주요 특징
			서비스 포털	클라우드 포털	콘솔	
1	네이버 클라우드	Compute, Containers, Storage, Networking, Database, Security, AI Services, Application Services, AI·NAVER API, Big Data & Analytics, Blockchain, Business Applications, Content Delivery, Developer Tools, Dgital Twin, Gaming, Hybrid & Private Cloud, Internet of Things, Management &Governance, Media, Migration	-	O	O	-
2	NHN Cloud	Compute, Container, Network, Storage, Database, Hybrid & Private Cloud, Game, Security, ContentDelivery, Notification, AIService, MachineLearning, ApplicationService, MobileService, Search, Data&Analytics, DevTools,Management, Bill, Dooray!, Dooray!|ERP,Dooray!|Groupware, ContactCenter,IDC,Governance&Audit	-	O	O	-
3	KT cloud	AI Computing, Computing, Container, Network, Storage, Hybrid/Private Cloud, DB, Big Data, Security, Business Service, CDN, AI API, Application, Development Service, Management, Enterprise	-	O	O	-

#	사업자	제공서비스	흐름 분석			주요 특징
			서비스 포털	클라우드 포털	콘솔	
4	카카오 엔터프라이즈	Beyond Compute Service, Beyond Networking Service, Beyond Storage Service, Management, Container Pack, Developer Tools	-	-	O	-
5	가비아	가상 서버, 베어메탈 서버, 스냅샷/이미지, 오토스케일링, 이미지 백업, 서버호스팅, 코로케이션, 커넥터, 블록 스토리지, NAS, 파일 백업, VPC, 로드밸런서, CDN, 방화벽, 웹방화벽, VPN, 웹쉘 탐지, DB 보안, 바이러스백신, 매니지드 서비스, 기술지원, 통합 모니터링, HA 솔루션, 공공기관 전용 클라우드, AWSevent, MS Azure	O	-	O	-

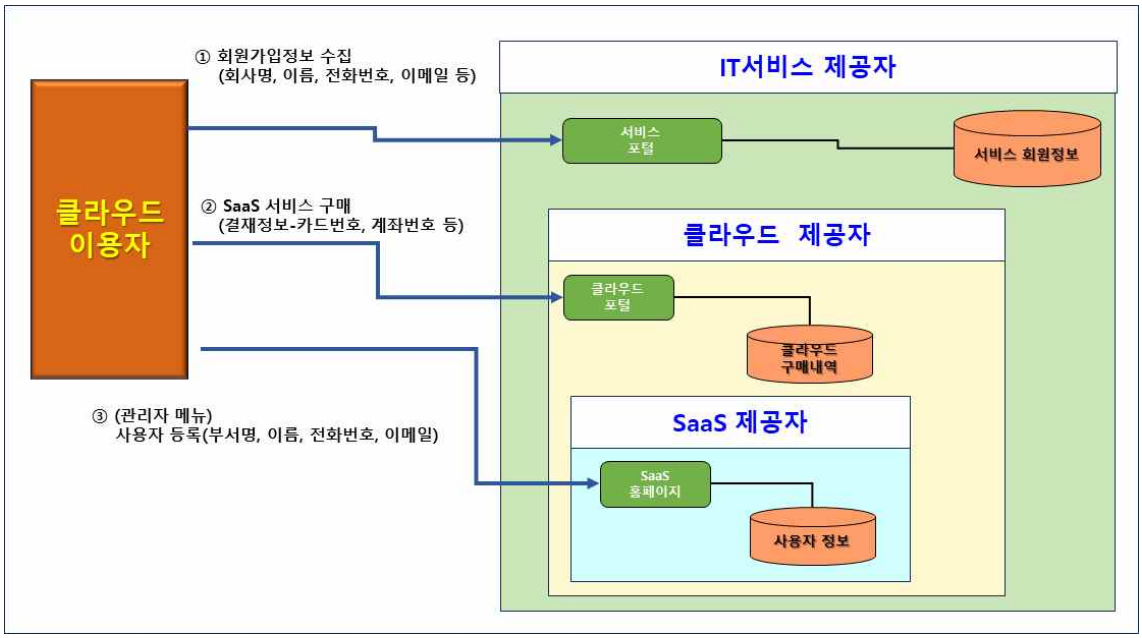
#	사업자	제공서비스	흐름 분석			주요 특징
			서비스 포털	클라우드 포털	콘솔	
6	Amazon	Featured Services, Analytics, Application Integration, Blockchain,Business Applications, Cloud Financial Management, Compute, Contact Center, Containers, Database, Developer Tools, End User Computing, Front-End Web & Mobile, Games, Internet of Things, Machine Learning, Management & Governance, Media Services, Migration & Modernization Networking & ContentDelivery, QuantumTechnologies, Robotics, Satellite, Security, Identity, &Compliance, Serverless, Storage,SupplyChain	-	O	O	-
7	Google	Featured products, AI and Machine Learning, Business Intelligence, Compute, Containers, Data Analytics, Databases, Developer Tools, Distributed Cloud, Hybrid and Multicloud, IndustrySpecific, IntegrationServices, ManagementTools, MapsandGeospatial, MediaServices, Migration, MixedReality, Networking, Operations, Productivity and Collaboration, SecurityandIdentity, Serverless, Storage, Web3	O	-	O	-

#	사업자	제공서비스	흐름 분석			주요 특징
			서비스 포털	클라우드 포털	콘솔	
8	Microsoft	AI + 기계 학습, Analytics, 컴퓨팅, 컨테이너, 데이터베이스, 개발자 도구, DevOps, 하이브리드 + 다중 클라우드, ID, 통합, 사물 인터넷, 관리 및 거버넌스, 미디어, 마이그레이션, 혼합 현실, 모바일, 네트워킹, 보안, 스토리지, 가상 데스크톱 인프라, 웹	O	O	-	-

2. SaaS 사업자의 제공서비스 및 흐름분석

조사 대상 SaaS별로 제공되는 주요 서비스와 클라우드 서비스 이용을 위해 접속하는 경로(서비스 가입·신청·설정 흐름)를 분석한 개요는 아래 [그림 2-2]와 같고, 상세 내용은 아래 [표 2-4]와 같다.

[그림 2-2] SaaS 서비스 개인정보 흐름도



SaaS 또한 이용사업자가 '서비스 포털'에서 회원 가입 후, '클라우드 포털'에서 이용신청·구매·결재 등을 하는 과정은 앞서 IaaS와 유사하였다.

한편, IaaS에서 가상화된 서버 정책설정을 위해 '콘솔' 또는 가상화 서버에 대한 직접접속 수단을 제공하였던 것과 다르게, SaaS의 경우 그러한 '애플리케이션' 단계까지 클라우드 서비스 제공사업자가 미리 마련하여 제공하므로, 이용사업자는 그러한 '애플리케이션'(주로 관리자용 웹페이지)에 접속하여 고객(end-user) 정보를 취급하는 것이 일반적이었다.

참고로 IaaS의 '콘솔'은 주로 보안정책을 설정하는 곳일 뿐 실제 고객정보에 접근하는 기능은 없었던 반면, SaaS의 관리자용 웹페이지의 경우 실제 고객정보를 대량으로 조회·다운로드하거나 다른 하위관리자 계정의 접근권한을 설정하는 등의 기능을 수행하는 곳이 있었다. 그러한 관리자용 웹페이지는 '개인정보처리시스템'에 해당하여 침입탐지, 2차 인증, 자동로그아웃, 망분리 등 조치의무 대상이 됨에 유의하여야 한다.

[표 2-4] SaaS 서비스 흐름 및 주요 제공 서비스 현황

#	서비스명	세부 서비스	흐름분석			주요특징
			서비스 포털	클라우드 포털	SaaS 홈페이지 (관리자)	
1	네이버웍스	메시지, 영상통화, 게시판, 할일, 설문, 메일, 드라이브, BOT			O	-
2	카카오워크	채팅, 워크보드(피드형게시판), 메일, 설문, 캘린더, 화상회의, 웨비나, 할일관리, 알림, 전자결재			O	-
3	KT BizOffice	메일, 전자결재, 근태관리, 사내공지, 일정관리, 게시판, 프로젝트관리, 메신저, 주소록		O	O	-
4	하이웍스	그룹웨어, 경비지출관리, 근무관리(전자결재), 메일	O		O	-
5	Slack	채널, 협업, 채팅, 화상대화, 클립, 파일 공유, 검색, 앱 통합, 워크플로 빌더(작업자동화)			O	-
6	Zendesk	메시지, 음성대화, 봇, 상담사워크스페이스, 통합티켓관리, 헬프 센터			O	-

제 3 장 클라우드 제공 보호조치기능 현황조사

제 1 절 조사 항목 선정

1. IaaS 보호조치기능 조사 항목 선정

개인정보 안전성 확보조치기준 고시 조항별 요구사항을 기준으로, 클라우드측에서 관련 기능을 제공해 주어야만 이용사업자가 이를 준수할 수 있는 사항(이하 '보호조치기능')을 아래 [표 3-1]과 같이 13개 조사 항목으로 선정하였다.

[표 3-1] IaaS 보호조치기능 항목 선정

안전성 확보조치 고시		IaaS 보호조치기능 조사 항목	
제4조	내부 관리계획의 수립·시행	-	
제5조	접근 권한의 관리	1	ㅇ 접근권한 차등부여
		2	ㅇ 접근권한 변경내역 3년 이상 보관
		3	ㅇ 일정 횟수(5회)이상 인증 실패 시 보호대책 적용 (24년 9월까지 유예)
		4	ㅇ 로그인 시 패스워드 설정규칙 적용 여부
제6조	접근통제	5	ㅇ 관리자 ID에 대한 IP 접근제한 적용 여부
		6	ㅇ 외부 인터넷을 통한 접속 시 2차 인증수단 (인증서, 보안토큰, 일회용 비밀번호 등) 적용
		7	ㅇ Idle timeout 적용 여부
		8	ㅇ (망분리) 관리자 계정, IP 제한 가능 여부
제7조	개인정보의 암호화	9	ㅇ 인터넷 접속구간 암호화 적용 여부
제8조	접속기록의 보관 및 점검	10	ㅇ 접속기록 1년이상 보관 여부
		11	ㅇ 접속로그 검토, 확인 기능 제공 여부
		12	ㅇ 접속기록 별도 보관 여부
제9조	악성프로그램 등 방지	-	
제10조	물리적 안전조치	-	
제11조	재해·재난 대비 안전조치	-	
제12조	출력·복사 시 보호조치	-	
제13조	개인정보의 파기	13	ㅇ 이용사업자 이용종료 시 해당 데이터 파기

2. SaaS 보호조치기능 조사 항목 선정

개인정보 안전성 확보조치 고시 조항별 요구사항을 기준으로, SaaS 제공사업자가 기능을 제공해 주어야만 이용사업자가 이를 준수할 수 있는 사항을 아래 [표 3-2]와 같이 16개 조사 항목으로 선정하였다. SaaS 애플리케이션 단계까지 클라우드에서 제공된다는 특성을 고려하여 IaaS 대비 암호화 항목 및 화면출력 시 마스킹 항목을 추가하였다.

[표 3-2] SaaS 보호조치기능 항목 선정

안전성 확보조치 고시		SaaS 보호조치기능 조사 항목	
제4조	내부 관리계획의 수립·시행	-	
제5조	접근 권한의 관리	1	ㅇ 접근권한 차등부여
		2	ㅇ 접근권한 변경내역 3년 이상 보관
		3	ㅇ 일정 횟수(5회)이상 인증 실패 시 보호대책 적용 (24년 9월까지 유예)
		4	ㅇ 관리자 페이지 로그인 시 패스워드 설정규칙 적용 여부
제6조	접근통제	5	ㅇ 관리자 ID에 대한 IP 접근제한 적용 여부
		6	ㅇ 외부 인터넷을 통한 접속 시 2차 인증수단 (인증서, 보안토큰, 일회용 비밀번호 등) 적용
		7	ㅇ Idle timeout 적용 여부
		8	ㅇ (망분리) 관리자 계정, IP 제한 가능 여부
제7조	개인정보의 암호화	9	ㅇ 인터넷 접속구간 암호화 적용 여부
		10	**ㅇ 주요정보 저장 시 암호화 적용 여부**
		11	**ㅇ 암호키 설정, 관리절차 제공 여부**
제8조	접속기록의 보관 및 점검	12	ㅇ 접속기록 1년 이상 보관 여부
		13	ㅇ 접속로그 검토, 확인 기능 제공 여부
		14	ㅇ 접속기록 별도 보관 여부
제9조	악성프로그램 등 방지	-	
제10조	물리적 안전조치	-	
제11조	재해·재난 대비 안전조치	-	
제12조	출력·복사 시 보호조치	**15**	**ㅇ 개인정보의 화면 출력 시 항목 최소화 또는 마스킹 기능 제공 여부**
제13조	개인정보의 파기	16	ㅇ 이용사업자 이용종료 시 해당 데이터 파기

3. 안전성 확보조치 고시, IaaS/SaaS 각 보호조치 기능 항목 비교

[표 3-3] IaaS/SaaS 보호조치 기능 조사 항목 비교

안전성확보 조치 고시				IaaS 보호조치기능		SaaS 보호조치기능	
구분		#	내용	#	내용	#	내용
제4조	내부 관리계획의 수립·시행	1	○ 내부관리계획의 수립				
		2	○ 내부관리계획 이행실태 점검 연1회 이상				
제5조	접근 권한의 관리	1	○ 취급자별 최소 범위로 권한 차등부여 및 변경·말소	1	○ 접근권한 차등부여	1	○ 접근권한 차등부여
		2	○ 접근권한 부여, 변경, 말소 기능 제공내역 3년 이상 보관 * 접근권한에 관한 기록 : ① 계정신청정보(ID, 사용자), ② 신청일시, ③ 권한 상태 (권한 및 생성/변경/말소), ④ 승인자 및 발급자 정보, ⑤ 신청 및 발급 사유 등	2	○ 접근권한 변경내역 3년 이상 보관	2	○ 접근권한 변경내역 3년 이상 보관
		3	○ 1인 1계정 발급 및 공유 금지				
		4	○ 개인정보취급자 또는 정보주체가 일정 횟수 이상 인증 실패 시 접근 제한 (24년 9월까지 유예)	3	○ 일정 횟수(5회) 이상 인증 실패 시 보호대책 적용 (24년 9월까지 유예)	3	○ 일정 횟수(5회) 이상 인증 실패 시 보호대책 적용 (24년 9월까지 유예)
		5	○ 인증수단 안전하게 관리 - 비밀번호, 생체인식 등 안전한 정책 마련 및 적용	4	○ 로그인 시 패스워드 설정규칙 적용 여부	4	○ 관리자 페이지 로그인 시 패스워드 설정규칙 적용 여부

안전성확보 조치 고시				IaaS 보호조치기능		SaaS 보호조치기능	
구분		#	내용	#	내용	#	내용
제6조	접근통제	1	ㅇ 인가받지 않은 접근제한 - 접속 권한별 인터넷 프로토콜(IP) 주소 등으로 제한 적용 - 접속한 인터넷 프로토콜(IP) 주소 등을 분석	5	ㅇ 관리자 ID에 대한 IP 접근제한 적용 여부	5	ㅇ 관리자 ID에 대한 IP 접근제한 적용 여부
		2	ㅇ 외부에서 접속하려는 경우 안전한 인증수단(인증서, 보안토큰, 일회용 비밀번호 등) 적용 ㅇ 이용자 외 개인정보처리 시 가상사설망등 안전한 접속수단 또는 안전한 인증수단 적용	6	ㅇ 외부 인터넷을 통한 접속 시 2차 인증수단(인증서, 보안토큰, 일회용 비밀번호 등) 적용	6	ㅇ 외부 인터넷을 통한 접속 시 2차 인증수단(인증서, 보안토큰, 일회용 비밀번호 등) 적용
		3	ㅇ 인터넷 홈페이지, P2P, 공유설정 등을 통하여 권한 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기 조치				
		4	ㅇ Idle Time out - 일정시간이상 업무처리를 하지 않는 경우 자동으로 접속 차단	7	ㅇ Idle timeout 적용여부	7	ㅇ Idle timeout 적용여부
		5	ㅇ 업무용 모바일 기기 비밀번호 설정 등의 보호조치				

안전성확보 조치 고시				IaaS 보호조치기능		SaaS 보호조치기능	
구분		#	내용	#	내용	#	내용
		6	ㅇ 망분리 - 클라우드 컴퓨팅 서비스를 이용하여 개인정보처리시스템을 구성·운영하는 경우에는 해당 서비스에 대한 접속 외에는 인터넷을 차단하는 조치	8	ㅇ (망분리) 관리자 계정, IP 제한 가능 여부	8	ㅇ (망분리) 관리자 계정, IP 제한 가능 여부
제7조	개인정보의 암호화	1	ㅇ 안전한 암호 알고리즘으로 저장 시 암호화 - 비밀번호: 일방향 암호화 - 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호, 신용카드번호, 계좌번호, 생체인식정보 - 정보주체 고유식별정보: 인터넷망 구간 및 DMZ 저장 시 암호화, 내부망 저장 시 암호화			9	ㅇ 주요정보 저장 시 암호화 적용 여부
		2	ㅇ 인터넷망 구간으로 송·수신 시 암호화	9	ㅇ 인터넷 접속구간 암호화 적용 여부	10	ㅇ 인터넷망 구간으로 송·수신 시 암호화
		3	ㅇ 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장 시 안전한 암호알고리즘을 사용하여 암호화				

안전성확보 조치 고시				IaaS 보호조치기능		SaaS 보호조치기능	
구분		#	내용	#	내용	#	내용
		4	○ 암호키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립 · 시행			11	○ 암호키 설정, 관리절차 제공 여부
제8조	접속기록의 보관 및 점검	1	○ 접속기록 1년 이상 보관 * 접속기록 내역 - 식별자, 접속일시, 접속지(IP 주소 등), 정보주체 정보, 수행업무, ○ 보유기간 - 모든 개인정보처리시스템 : 1년 이상 - 유출 시 피해 가능성이 높은 개인정보 (5만명 이상 개인정보, 고유식별정보 또는 민감정보) : 최소 2년 이상 - 기간통신사업자 : 최소 2년 이상	10	○ 접속기록 1년이상 보관 여부	12	○ 접속기록 1년이상 보관 여부
		2	○ 접속기록 월 1회 이상 점검, 다운로드 사유 확인	11	○ 접속로그 검토, 확인 기능 제공 여부	13	○ 접속로그 검토, 확인 기능 제공 여부
		3	○ 접속기록이 위·변조 및 도난, 분실되지 않도록 안전한 보관	12	○ 접속기록 별도 보관 여부	14	○ 접속기록 별도 보관 여부
제9조	악성프로그램 등 방지	1	○ 악성프로그램 등을 방지 · 치료할 수 있는 보안 프로그램을 설치 · 운영				

안전성확보 조치 고시				IaaS 보호조치기능		SaaS 보호조치기능	
구분		#	내용	#	내용	#	내용
제10조	물리적 안전조치	1	ㅇ 출입통제 절차를 수립 · 운영				
		2	ㅇ 잠금장치가 있는 안전한 장소에 보관				
		3	ㅇ 보조저장매체의 반출 · 입 통제				
제11조	재해·재난 대비 안전조치	1	ㅇ 위기대응 매뉴얼 등 대응절차를 마련하고 정기적 점검				
		2	ㅇ 백업 및 복구를 위한 계획				
제12조	출력·복사 시 보호조치	1	ㅇ 개인정보의 출력 시(인쇄, 화면표시, 파일생성 등) 용도를 특정, 용도에 따라 출력 항목 최소화			15	ㅇ 개인정보의 화면출력 시 항목 최소화 또는 마스킹 기능 제공 여부
		2	ㅇ 종이 인쇄물, 외부 저장매체 등 출력 · 복사물 안전조치				
제13조	개인정보의 파기	1	ㅇ 개인정보 파기 : 전체파기, 일부파기, 파기에 준하는 조치	13	ㅇ 이용사업자 이용종료 시 해당 데이터 파기	16	ㅇ 이용사업자 이용종료 시 해당 데이터 파기

제 2 절 조사대상 클라우드 서비스의 보호조치 기능 제공현황

1. IaaS 제공사업자의 보호조치기능 제공현황

본 연구 대상으로 선정된 IaaS 제공사업자는 앞서 도출한 13개 보호조치 기능을 대체로 제공하고 있는 것으로 조사되었다.

다만 일부 IaaS의 경우 이용사업자가 개인정보취급자를 관리감독하기 위해 필요한 접근권한 차등부여, 접근권한 변경이력 3년간 보관 기능 제공, IP 기반 접속제한, 접속기록의 보관·검토 기능이 다소 미흡하다고 보인다. 이 경우 해당 IaaS의 이용사업자가 개인정보 보호법상 안전조치의무를 과연 준수할 수 있을지, 준수할 수 있다면 이를 위해 이용사업자가 투입해야 하는 추가적인 비용·노력이 어느 정도일지에 관한 추가적인 검토가 필요하다.

파기의 경우 조사 대상인 IaaS 제공사업자 모두 이용사업자의 서비스 탈퇴 또는 이용종료 시 해당 이용사업자의 가상시스템상 데이터를 삭제하고 있다고 약관 등을 통해 밝히고 있으나, 건별로 파기 확인서 등 문서는 발급해주지 않고 있다. 따라서 일반적인 약관 등을 가지고 건별 파기 확인서 발급을 갈음할 수 있을지 논의가 필요하다.

또한 고시에서는 idle timeout을 일률적으로 요구하고 있으나, 일부 IaaS의 경우 신뢰할 수 있는 단말기(trusted device)나 자동 로그인을 설정할 수 있는 기기 등에 대해서 자동 로그아웃이 안 되도록 idle timeout 면제 설정을 제공하고 있었다. 또한 로그인 인증오류 횟수 초과 시 조치의 경우, 고시 해설서에서는 '계정잠금 및 재인증'을 일률적으로 요구하고 있으나, 다수 IaaS의 경우 비밀번호 오류 시 재시도 시간 제한(수초 sleep)이나 캡차(capcha) 입력 정도만을 요구함으로써 비밀번호 무작위 대입공격(brute force attack)에 대비하고 있었다. 이러한 현장의 상황과 비교해보면 현행 고시의 일부 획일적 조치의무를 여과 없이 적용할 경우 자칫 고시 위반으로 판단되는 이용사업자를 대량으로 양산할 우려가 발생하므로, 그러한 고시상 조치의무가 과연 고시 제1조의 취지에 맞는 '안전성 확보에 필요한 최소한의 기준'에 해당하는지에 관한 논의가 필요해 보인다.

2. SaaS 제공사업자의 보호조치기능 제공현황

SaaS의 경우 클라우드에서 애플리케이션을 제공한다는 점에서 애플리케이션 단계의 보호조치기능 또한 SaaS 사업자가 제공해 주어야만 한다. 이용사업자의 경우 클라우드에 마련된 애플리케이션을 그대로 사용하는 경우가 대부분이고 해당 애플리케이션의 코드를 수정할 수 없으며 부가기능(plug-in) 추가도 제한적이라는 점을 고려할 때, 일정한 보호조치기능의 경우 SaaS 사업자가 제공해주지 않으면 이용사업자 관점에서 해당 보호조치의무를 준수하는 것은 원시적 불능에 빠지고 만다.

예를 들어 SaaS 자체에 개인정보취급자 접근권한 부여 내역을 3년간 보관하는 기능이 없다면, 이를 이용하는 이용사업자는 애플리케이션을 수정할 방법이 현실적으로 없으므로 해당 보호조치의무 고시를 사실상 준수할 수 없다. 2차 인증의 경우에도 SaaS 로그인 페이지에 이 기능이 없거나 별도 2차 인증 plug-in을 붙일 수 있는 계정관리 환경이 마련되어 있지 않다면 이용사업자가 이를 준수하기가 곤란하다. 화면출력 시 마스킹 또한 SaaS의 고객정보 조회 등 페이지에 마스킹 기능이 들어가 있지 않다면, 이용사업자가 해당 페이지를 별도 구현하는 사례는 드물 것이므로 의무위반 상태에 빠질 소지가 크다.

한편, 암호화 저장의 경우, SaaS 내부에 보관되는 데이터가 실제 암호화 되어있는지 여부를 이용사업자 관점에서 알 방법이 없는 경우가 많았고, 또한 대부분의 SaaS는 이용자에게 별도의 암호키를 설정할 수 있는 기능을 제공하지 않고 있었다. 이 경우 개인정보 암호화 저장이 미흡하여 사고가 터지면 이용사업자가 아닌 SaaS 서비스 제공사업자가 전적으로 법적 책임을 부담해야 할 것이다.

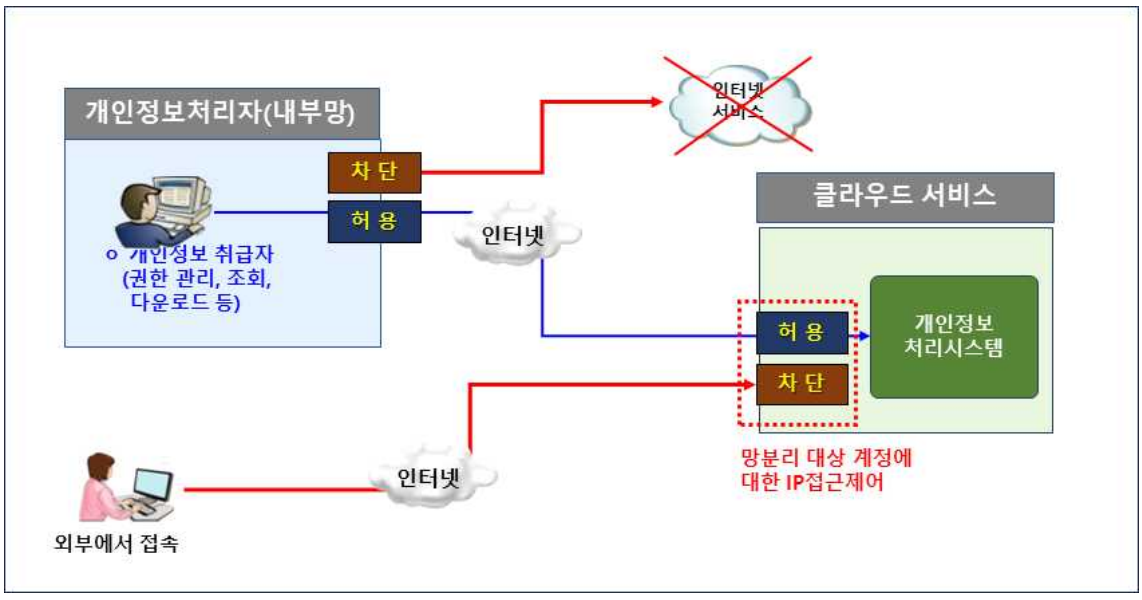
3. 참고 - 클라우드 서비스 이용사업자의 인터넷망 차단조치 구현형태

개인정보의 안전성 확보조치 기준 고시 제6조 제6항은 클라우드 서비스를 활용하여 개인정보처리시스템을 구성·운영하는 경우에는 해당 서비스에 대한 접속 외에는 인터넷 접속을 차단하도록 규정하고 있다. 예컨대 어느 기업이 클라우드가 아니라 자체 서버로써 개인정보처리시스템을 구축하고 있다면, 해당 사내 서버에 접속하는 개인정보취급자의 관리용 단말기·PC 등이 외부 인터넷에 연결되지 않도록 물리적 또는 논리적으로 분리하는 조치가 고시상 인터넷망 차단조치의 전형적인 모습이다. 한편, 클라우드를 개인정보처리시스템으로 쓰는 이용사업자라면, 해당 클라우드 콘솔(취급자 계정 접근권한 설정이 가능한 곳) 및 고객정보 조회·업데이트·파기 명령(쿼리)을 실행할 수 있는 관리자페이지 등(이하 '인터넷망 차단조치 대상 클라우드 시스템')에 대해 다음 조치를 함으로써 고시상 인터넷망 차단조치를 구현할 수 있으며, 실제 이렇게 구현하는 사례도 있다.

① 인터넷망 차단조치 대상 클라우드 시스템에 대해 개인정보취급자의 접속이 허용된 IP 주소 대역(이른바 '사내망')에서만 접속이 되고 다른 외부 IP 주소에서는 접속되지 않도록 차단 설정할 것

② 개인정보취급자의 관리용 단말기·PC 등(위 허용된 IP 주소 대역 안에 있는 것)에서 인터넷망 차단조치 대상 클라우드 시스템에 접속하는 동안에는 다른 외부 인터넷이 접속하지 못하도록 사내망 방화벽 등을 설정할 것

[그림 3-1] 클라우드 서비스 이용사업자의 인터넷망 차단조치 구현형태 개념도



이 중 ①을 IaaS/SaaS 제공사업자가 클라우드 기능으로써 제공한다면, 이용사업자로 하여금 인터넷망 차단조치를 구현할 수 있는 기반을 제공해준 것으로 평가할 수 있다. 한편, ②는 클라우드 바깥에서 이루어지는 것이므로 이용사업자가 자체 방화벽 등을 구축·설정함으로써 별도 구현해야 한다.

제 4 장 클라우드 인증항목과 수탁사 점검항목 비교

제 1 절 수탁사 점검항목 도출

2023년 한국인터넷진흥원에서 발주하여 한국CPO포럼에서 수행한 선행 연구용역[1]에 따르면, SaaS는 물론 IaaS 또한 클라우드 서비스 제공사업자를 개인정보 보호법상 수탁자로 볼 수 있다는 것이 최근 전문가들의 대체적인 견해라고 한다. 이에 따를 때 클라우드 서비스 제공사업자가 수탁자의 지위에서 위탁자인 이용사업자로부터 위·수탁 점검을 받아야할 만한 항목을 도출하면 아래 [표 4-1]과 같다. 각 점검항목의 내용은 개인정보보호법 및 안전성 확보조치기준 고시 등이 요구하는 수탁사 관리·감독 사항을 바탕으로 정리하였다.

[표 4-1] 클라우드 서비스 개인정보 수탁사 점검 항목

#	Category	Area	Domain	Control	근거		Questionnaire
					법	고시	
1	정보보호 및 개인정보 관리적 보호조치	정보보호 및 개인정보보호 정책	정책 승인 및 공표	정책 수립	제29조 (안전조치 의무) ※ 이하 '-' 표기	제4조 ①항	(개인)정보보호정책 및 정책의 시행을 위하여 필요한 세부적인 방법, 절차, 주기 등을 규정한 정보보호 지침, 절차, 매뉴얼 등을 수립하고 있는가?
2			내부관리계획수립 및 시행	정책 수립	-	제4조 ①항	개인정보의 안전한 취급을 위하여 "내부관리계획"을 마련하고 있는가? - 내부관리계획에 대한 최고경영자의 승인 - 내부관리계획공표(전파)
3			침해사고 대응절차 수립	정책 수립	-	제4조 ①항	개인정보 유·노출 등 침해사고 발생 시 대응절차 및 방법을 보유하고 있는가?
4		정보보호 및 개인정보보호 조직	개인정보 보호책임자 지정	책임자 지정	-	제4조 ①항	개인정보 보호책임자(CPO)를 지정하고 있는가?
5			개인정보 취급자 관리	취급자 관리	-	제4조 ①항	개인정보 취급자를 최소한으로 제한하고, 개인정보취급자 목록을 관리하고 있는가?

1) 한국씨피오포럼, 클라우드 개인정보 처리기준 마련 연구, 한국인터넷진흥원(최종연구보고서 KISA-WP-2023-0041), 2023

#	Category	Area	Domain	Control	근거		Questionnaire
					법	고시	
6				보안서약서 징구	제28조 ①항	-	수탁사 내 개인정보취급자에게 개인정보취급에 대한 보안서약서를 받고 있는가?
7				퇴직 및 직무 변경 관리	-	제5조②항	개인정보취급자의 퇴직 및 직무변경 시 자산반납, 계정 및 권한 회수·조정, 결과 확인 등의 개인정보취급자 인사관리 절차를 수립하고 이행하고 있는가?
8				개인정보 보호 교육 시행	-	제4조②항	개인정보보호교육 계획을 수립하고, 개인정보 보호교육을 정기적으로 시행하고 있는가?
9		개인정보 이용·제공	외부 (재)위탁시 개인정보 보호	위탁 계약 체결	제26조①항	-	개인정보의 처리 업무를 위탁 및 재위탁하는 경우, 필수 법적요건을 모두 만족하는 문서에 의해 계약이 체결되고 있는가?
10				재위탁 관리	제26조⑥항	-	개인정보의 처리 업무를 위탁 및 재위탁하는 경우 위탁사에게 동의를 받고 있는가?
11				수탁자 감독	제26조④항	-	수탁자 또는 재수탁자가 위탁받은 정보주체의 개인정보를 분실·도난·유출·변조 또는 훼손되지 아니하고, 개인정보를 안전하게 처리하는지를 지속적으로 감독하고 있는가?
12	정보보호 및 개인정보 기술적 보호 조치	개인정보 처리 시스템 관리	사용자 계정 및 권한 관리	고유 계정 사용	-	제5조④항	개인정보처리시스템에 접속할 수 있는 사용자 계정을 발급하는 경우, 개인정보취급자 별로 한 개의 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 하고 있는가?
13				안전한 비밀번호 사용	-	제5조⑤항	개인정보취급자가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하고 있는가?

#	Category	Area	Domain	Control	근거		Questionnaire
					법	고시	
14				최소 접근 권한 부여	-	제5조①항	개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하고 있는가?
15				접근 권한 변경 관리	-	제5조②항	전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하고 있는가?
16				접근 권한 변경 이력 보관	-	제5조③항	개인정보처리시스템에 대한 '권한 부여', '변경' 또는 '말소'에 대한 내역 기록을 최소 3년간 보관하고 있는가?
17			접속 기록 관리	접속 기록 보관	-	제8조①항	개인정보취급자가 개인정보처리시스템에 접속한 기록을 최소 1년 이상 (고시에서 정한 경우 2년 이상) 보관·관리하고 있는가?
18				접속 기록 정기 검토	-	제8조②항	개인정보처리자는 개인정보의 유출·변조·훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월1회 이상 점검하고 있는가? (다운로드가 있는 경우 다운로드 사유를 확인해야 한다.)
19				접속 기록 위·변조 방지 및 백업	-	제8조③항	개인정보취급자의 접속기록이 위·변조되지 않도록 별도의 물리적인 저장 장치에 보관하여, 정기적으로 백업을 수행하고 있는가?
20			개인 정보 저장 · 전송시 암호화	개인 정보 및 비밀 번호 암호화	-	제7조①항	비밀번호, 고유식별정보, 생체인식정보, 주민등록번호, 신용카드번호 및 계좌번호에 대하여 안전한 암호화 알고리즘을 적용하여 저장하고 있는가?
21				개인 정보 전송시 암호화	-	제7조	개인정보를 정보통신망을 통하여 송·수신하거나 보조저장매체 등을 통하여 전달하는 경우, 개인정보를 암호화조치를 취하고 있는가?
22			개인 정보 파기 관리 (개인 정보	수집 목적 달성시 지체없이 파기	제21조①항	제13조	해당 개인정보의 수집목적이 달성되었을 경우 개인정보처리시스템에서 지체없이 파기하고 있는가? (단,다른법령에따라해당개인정보를 추가로보존하여야하는경우예외로함)

#	Category	Area	Domain	Control	근거		Questionnaire
					법	고시	
23			처리 시스템)	개인정보 파기 방법	제21조②항	-	개인정보를 파기하는 경우 복구 또는 재생 할 수 없는 방법으로 파기하고 있는가?
24				개인정보 보존 시 분리 저장·관리	제21조③항	-	개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 해당 개인정보를 다른 개인정보와 분리하여 저장·관리하고 있는가?
25		PC 보안 관리	개인정보 저장시 암호화	PC 내 개인정보 암호화	-	제7조⑤항	이용자의 개인정보를 개인용 컴퓨터에 저장 시 암호화하여 저장하고 있는가?
26			출력·복사 관리	개인정보 출력·복사 기록 관리	-	제12조①항	개인정보가 포함된 종이 인쇄물, 개인정보가 복사된 외부 저장매체 등 개인정보의 출력·복사물을 안전하게 관리하기 위해 출력·복사 기록 등 필요한 보호조치를 갖추고 있는가?
27			개인정보 파기관리 (PC)	수집 목적 달성 시 지체 없이 파기	-	제13조	해당 개인정보의 처리목적이 달성되었을 경우 개인정보취급자의 단말기(PC)에서 지체없이 파기하고 있는가?
28				개인정보 파기 방법	-	제13조	개인정보를 파기하는 경우 복구 또는 재생 할 수 없는 방법으로 파기하고 있는가?
29			계정 암호정책	패스워드 복잡도	-	제5조⑤항	패스워드는 영문자, 숫자, 특수문자 중 3가지 종류 조합 시 최소 8자리 이상, 2가지 종류 조합 시 최소 10자리 이상인가?
30				패스워드 최대 사용기간 설정	-	제5조⑤항	개인정보취급자 PC의 비밀번호를 분기별 1회 이상 변경하고 있는가?
31			기본 보안 설정 관리	공유 폴더 사용 제한	-	제6조③항	개인정보취급자 PC의 공유 폴더 사용을 제한하고 있는가?
32				보안프로그램 설치 및 실행	-	제9조①항	개인정보취급자의 PC에 백신 소프트웨어 등의 보안 프로그램을 설치하고, 실시간 감시를 적용하고 있는가?

#	Category	Area	Domain	Control	근거		Questionnaire
					법	고시	
33				운영체제 패치 적용	-	제9조②항	개인정보취급자 PC의 운영체제에 대해 최신 보안 패치를 설치하고 있는가?
34				매체 제어	-	-	보조저장매체에 대해 쓰기 금지 정책이 적용되어 있는가?
35			네트워크 접근통제(PC)	유해 사이트 및 프로그램 통제	-	제6조③항	취급중인 개인정보가 인터넷 홈페이지, P2P 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터 및 모바일기기 등에 별도의 조치를 취하고 있는가?
36		접근 통제	네트워크 영역 통제	네트워크 영역 분리	-	제6조⑥항	서비스, 사용자 그룹, 정보자산의 중요도, 법적 요구사항에 따라 네트워크 영역을 물리적 또는 논리적으로 분리하고 있는가?
37			시스템 접근통제	개인정보처리시스템 접근 통제	-	제6조②항	개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 안전한 인증수단을 적용하고 있는가?
38				정보 시스템 접근 통제	-	제6조①항	정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 정보시스템(서버, 응용프로그램, DB 등)의 접근을 제한하고 있는가?
39		운영 통제	백업 및 복구	백업 및 복구절차 수립·이행	-	제11조	백업 대상, 주기, 방법, 절차 등이 포함된 백업 및 복구절차를 수립·이행하고 있는가?
40			취약점 점검	정보 시스템 주기적 취약점 점검	-	제4조①항	정보시스템 취약점 점검 절차를 수립하여 정기적으로 점검을 수행하고 있는가?
41	정보보호 및 개인정보 물리적 보호조치	보호구역 통제	개인정보의 보관 및 출입통제 절차	서류, 저장매체 보관	-	제10조②항	개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하고 있는가?
42				보호구역 통제	-	제10조①항	전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하고 있는가?

제 2 절 수탁사 점검항목과 클라우드 인증항목의 유사도 분석

주요 IaaS 및 SaaS 제공사업자는 ISMS-P, CSAP, ISO-270001,27002,27018 등의 인증을 취득한 사례가 많다. 해당 인증을 취득하기 위해 인증심사원으로부터 점검받아야 하는 항목 및 앞 절에서 도출한 위·수탁 점검항목을 비교하면 아래 [표 4-2]와 같으며, 위·수탁 점검 항목의 대부분은 인증심사 항목에 포함됨을 확인할 수 있었다. 이에 따를 때, 클라우드 서비스 제공사업자가 이용사업자로부터 고객 개인정보 처리를 위탁받는 서비스와 동일 범위에 대해서 위 클라우드 인증을 받았다고 전제하면(이 전제의 구비 여부에 관하여는 다음 절에서 별도 검토한다), 이용사업자로부터 받아야 할 위·수탁 점검을 인증으로 대체할 수 있음을 시사한다.

[표 4-2] 수탁사 점검항목과 클라우드 인증항목 내용 중첩도 분석

클라우드 서비스 수탁사 점검 항목(안)						CSAP	ISMS-P	ISO 27001	ISO 27002	ISO 27018
#	Category	Area	Domain	Control	Questionnaire	세부인증 항목	세부인증 항목	세부인증 항목	세부인증 항목	세부인증 항목
1	정보보호 및 개인정보 관리적 보호조치	정보보호 및 개인정보 보호정책	정책 승인 및 공표	정책 수립	(개인)정보보호정책 및 정책의 시행을 위하여 필요한 세부적인 방법, 절차, 주기 등을 규정한 정보보호 지침, 절차, 매뉴얼 등을 수립하고 있는가?	1.1.1 정보보호 정책 수립	1.1.5 정책 수립	5.1 정보보안 정책	5.1 정보보안 정책	5.1.1 정보 보안 정책
2			내부관리 계획수립 및 시행	정책 수립	개인정보의 안전한 취급을 위하여 “내부관리계획”을 마련하고 있는가? -내부관리 계획에 대한 최고 경영자의 승인 -내부관리 계획 공표(전파)	1.1.1 정보보호 정책 수립	1.1.5 정책 수립	5.34 개인정보 및 개인 식별 정보(PII) 보호	5.1 정보보안 정책	5.1. 정보 보안 관리 방향
3			침해사고 대응절차 수립	정책 수립	개인정보 유·노출 등 침해사고 발생 시 대응절차 및 방법을 보유하고 있는가?	5.1.1 침해사고 대응 절차 수립	2.11.1 사고 예방 및 대응체계 구축	5.24 정보보안 사고 관리 계획 수립 및 준비	5.24 정보보안 사건 관리 계획수립 및 준비	A 10.1 PII와 관련된 데이터 침해 통지

클라우드 서비스 수탁사 점검 항목(안)						CSAP	ISMS-P	ISO 27001	ISO 27002	ISO 27018
#	Category	Area	Domain	Control	Questionnaire	세부인증 항목	세부인증 항목	세부인증 항목	세부인증 항목	세부인증 항목
4		정보보호 및 개인정보 보호조직	개인정보 보호책임자 지정	책임자 지정	개인정보 보호책임자(CPO)를 지정하고 있는가?	1.2.2 역할 및 책임 부여	1.1.2 최고책임자의 지정	5.2 정보 보안 역할 및 책임	5.34 프라이버시 및 PII의 보호	6.1.1 정보 보안 역할 및 책임
5			개인정보 취급자 관리	취급자 관리	개인정보 취급자를 최소한으로 제한하고, 개인정보취급자 목록을 관리하고 있는가?	2.1.2 주요 직무자 지정 및 감독	2.2.1 주요 직무자 지정 및 관리	5.18 접근 권한	5.18 접근 권한	9.2.2 사용자 접근 권한 설정
6				보안서약서 징구	수탁사 내 개인정보취급자에게 개인정보취급에 대한 보안서약서를 받고 있는가?	2.1.4 비밀유지 서약서	2.2.3 보안 서약	6.6 기밀 유지 협약	6.6 기밀/비밀 유지 협약	A.11.1 기밀유지 협약
7				퇴직 및 직무변경 관리	개인정보취급자의 퇴직 및 직무변경 시 자산반납, 계정 및 권한 회수·조정, 결과 확인 등의 개인정보취급자 인사 관리 절차를 수립하고 이행하고 있는가?	2.1.5 퇴직 및 직무변경	2.2.5 퇴직 및 직무변경 관리	6.5 고용종료, 직무변경 후의 책임	6.5 고용종료, 직무변경 후의 책임	7.3 고용 종료 및 직무 변경
8				개인정보 보호교육 시행	개인정보 보호교육 계획을 수립하고, 정기적으로 시행하고 있는가?	2.3.2 교육 시행	2.2.4 인식제고 및 교육훈련	6.3 정보 보안 인식, 교육 및 훈련	6.3 정보보안 인식, 교육 및 훈련	7.2.2 정보 보안 인식, 교육 및 훈련
9		개인정보 이용·제공		위탁 시 문건에 법적요건 반영	개인정보의 처리 업무를 위탁 및 재위탁하는 경우, 필수 법적 요건을 모두 만족하는 문서에 의해 계약이 체결되고 있는가?	2.2.1 외부인력 계약	2.3.2 외부자 계약 시 보안	5.20 공급자 계약과 관련된 정보 보안 문제 취급	5.20 공급자 협약에서 정보보안 명시	18.1 법적 요건 및 계약 요건 준수

클라우드 서비스 수탁사 점검 항목(안)						CSAP	ISMS-P	ISO 27001	ISO 27002	ISO 27018
#	Category	Area	Domain	Control	Questionnaire	세부인증 항목	세부인증 항목	세부인증 항목	세부인증 항목	세부인증 항목
10			외부 (재)위탁 시 개인정보 보호	재위탁 관리	개인정보의 처리 업무를 위탁 및 재위탁하는 경우 위탁사에게 동의를 받고 있는가?	-	2.3.3 외부자 보안 이행 관리	5.19 공급자 관계에서의 정보 보안	5.19 공급자 관계에서 정보보안	A.8.1 하도급 처리된 PII 공개
11				수탁자 감독	수탁자 또는 재수탁자가 위탁받은 정보주체의 개인정보를 분실·도난·유출·변조 또는 훼손되지 아니하고, 개인정보를 안전하게 처리하는지를 지속적으로 감독하고 있는가?	-	2.3.3 외부자 보안 이행 관리	5.22 공급자 서비스 모니터링, 검토 및 변경 관리	5.22 공급자 서비스 모니터링, 검토 및 변경 관리	-
12	정보보호 및 개인정보 기술적 보호조치	개인정보 처리시스템 관리	사용자 계정 및 권한관리	고유 계정 사용	개인정보처리시스템에 접속할 수 있는 사용자 계정을 발급하는 경우, 개인정보취급자 별로 한 개의 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 하고 있는가?	10.2.2 관리자 및 특수 권한관리	2.5.2 사용자 식별	5.16 ID 관리	5.16 신원 관리	A.11.8 고유한 사용자 ID 보유

클라우드 서비스 수탁사 점검 항목(안)						CSAP	ISMS-P	ISO 27001	ISO 27002	ISO 27018
#	Category	Area	Domain	Control	Questionnaire	세부인증 항목	세부인증 항목	세부인증 항목	세부인증 항목	세부인증 항목
13				안전한 비밀 번호 사용	개인정보취급자가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하고 있는가?	10.3.4 패스워드 관리	2.5.4 비밀번호 관리	5.17 인증 정보	5.17 인증 정보	9.2.4 사용자 비밀 인증 정보 관리
14				최소 접근 권한 부여	개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하고 있는가?	10.2.1 사용자 등록 및 권한부여	2.5.1 사용자 계정 관리	5.18 접근 권한	5.18 접근 권한	9.2.2 사용자 접근 권한 설정
15				접근 권한 변경 관리	전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하고 있는가?	10.2.3 접근권한 검토	2.2.5 퇴직 및 직무변경 관리	5.18 접근 권한	5.18 접근 권한	9.2.2 사용자 접근 권한 설정
16				접근 권한 변경 이력 보관	개인정보처리시스템에 대한 '권한 부여', '변경' 또는 '말소'에 대한 내역을 기록을 최소 3년간 보관하고 있는가?	7.2.2 감사기록 및 모니터링	2.5.6 접근권한 검토	8.15 로깅	8.15 로그 기록	12.4 로그기록 및 모니터링
17			접속기록 관리	접속 기록 보관	개인정보취급자가 개인정보처리시스템에 접속한 기록을 최소 1년 이상(고시에서 정한 경우 2년 이상) 보관·관리하고 있는가?	7.2.2 감사기록 및 모니터링	2.9.4 로그 및 접속기록 관리	8.15 로깅	8.15 로그 기록	12.4.2 로그 정보 보호

클라우드 서비스 수탁사 점검 항목(안)						CSAP	ISMS-P	ISO 27001	ISO 27002	ISO 27018
#	Category	Area	Domain	Control	Questionnaire	세부인증 항목	세부인증 항목	세부인증 항목	세부인증 항목	세부인증 항목
18				접속 기록 정기 검토	개인정보처리자는 개인정보의 유출·변조·훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월1회 이상 점검하고 있는가? (다운로드가 있는 경우 다운로드 사유를 확인해야 한다.)	7.2.2 감사기록 및 모니터링	2.9.5 로그 및 접속기록 점검	8.15 로깅	8.15 로그 기록	12.4 로그기록 및 모니터링
19				'접속 기록 위·변조 방지 및 백업	개인정보취급자의 접속기록이 위·변조되지 않도록 별도의 물리적인 저장 장치에 보관하여, 정기적으로 백업을 수행하고 있는가?	7.2.2 감사기록 및 모니터링	2.9.4 로그 및 접속기록 관리	8.13 정보 백업	8.13 정보 백업	12.3.1 정보 백업
20			개인정보 저장·전송 시 암호화	개인정보 및 비밀번호 암호화	비밀번호, 고유식별정보, 생체인식정보, 주민등록번호, 신용카드번호 및 계좌번호에 대하여 안전한 암호화 알고리즘을 적용하여 저장하고 있는가?	12.3.1 암호 정책 수립	2.7.1 암호정책 적용	8.24 암호화 사용	8.24 암호 사용	10.1 암호 통제
21				개인정보 전송 시 암호화	개인정보를 정보통신망을 통하여 송·수신하거나 보조저장매체 등을 통하여 전달하는 경우, 개인정보를 암호화 조치를 취하고 있는가?	12.3.1 암호 정책 수립	2.7.1 암호정책 적용	8.24 암호화 사용	8.24 암호 사용	10.1 암호 통제

클라우드 서비스 수탁사 점검 항목(안)						CSAP	ISMS-P	ISO 27001	ISO 27002	ISO 27018
#	Category	Area	Domain	Control	Questionnaire	세부인증 항목	세부인증 항목	세부인증 항목	세부인증 항목	세부인증 항목
22			개인정보 파기관리 (개인정보 처리시스템)	수집 목적 달성 시 지체 없이 파기	해당 개인정보의 수집목적이 달성되었을 경우 개인정보처리시스템에서 지체 없이 파기하고 있는가? (단, 다른 법령에 따라 해당 개인정보를 추가로 보존하여야 하는 경우 예외로 함)	12.1.6 데이터 폐기	3.4.1 개인정보 파기	8.10 정보 삭제	8.10 정보 삭제	A.10.3. PII 반환, 전송 및 폐기
23				개인 정보 파기 방법	개인정보를 파기하는 경우 복구 또는 재생 할 수 없는 방법으로 파기하고 있는가?	12.1.6 데이터 폐기	3.4.1 개인정보 파기	8.10 정보 삭제	8.10 정보 삭제	A.10.3. PII 반환, 전송 및 폐기
24				개인 정보 보존 시 분리 저장·관리	개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 해당 개인정보를 다른 개인정보와 분리하여 저장·관리하고 있는가?	-	3.4.2 처리목적 달성 후 보유 시 조치	-	-	-
25		PC 보안 관리	개인정보 저장시 암호화	PC 내 개인 정보 암호화	이용자의 개인정보를 개인용 컴퓨터에(PC)에 저장 시 암호화하여 저장하고 있는가?	12.3.1 암호 정책 수립	2.7.1 암호정책 적용	8.1 사용자 엔드포인트 장치	8.1 사용자 엔드포인트 장치	10.1.1 암호 통제 사용 정책
26			출력·복사 관리	개인 정보 출력·복사 기록 관리	개인정보가 포함된 종이 인쇄물, 개인정보가 복사된 외부 저장매체 등 개인정보의 출력·복사물을 안전하게 관리하기 위해 출력·복사 기록 등 필요한 보호조치를 갖추고 있는가?	12.2.2 이동매체 관리	2.4.7 업무환경 보안	-	-	A11.2 하드카피 자료 작성 제한

클라우드 서비스 수탁사 점검 항목(안)						CSAP	ISMS-P	ISO 27001	ISO 27002	ISO 27018
#	Category	Area	Domain	Control	Questionnaire	세부인증 항목	세부인증 항목	세부인증 항목	세부인증 항목	세부인증 항목
27			개인정보 파기관리 (PC)	수집 목적 달성 시 지체 없이 파기	해당 개인정보의 처리목적이 달성되었을 경우 개인정보취급자의 단말기(PC)에서 지체 없이 파기하고 있는가?	12.1.6 데이터 폐기	3.4.1 개인정보 파기	8.10 정보 삭제	8.10 정보 삭제	A.10.3. PII 반환, 전송 및 폐기
28				개인정보 파기 방법	개인정보를 파기하는 경우 복구 또는 재생 할 수 없는 방법으로 파기하고 있는가?	12.1.6 데이터 폐기	3.4.1 개인정보 파기	8.10 정보 삭제	8.10 정보 삭제	A.10.3. PII 반환, 전송 및 폐기
29			계정 암호정책	패스워드 복잡도	패스워드는 영문자, 숫자, 특수문자 중 3가지 종류 조합 시 최소 8자리 이상, 2가지 종류 조합 시 최소 10자리 이상인가?	10.3.4 패스워드 관리	2.5.4 비밀번호 관리	5.17 인증 정보	5.17 인증 정보	9.4.2 안전한 로그인 절차
30				패스워드 최대 사용기간 설정	개인정보취급자 PC의 비밀번호를 분기별 1회 이상 변경하고 있는가?	-	2.10.6 업무용 단말기기 보안	5.17 인증 정보	5.17 인증 정보	9.4.2 안전한 로그인 절차
31			기본 보안설정 관리	공유 폴더 사용 제한	개인정보취급자 PC의 공유 폴더 사용을 제한하고 있는가?	-	2.10.6 업무용 단말기기 보안	8.1 사용자 엔드포인트 장치	8.1 사용자 엔드포인트 장치	-
32				보안 프로그램 설치 및 실행	개인정보취급자의 PC에 백신 소프트웨어 등의 보안 프로그램을 설치하고, 실시간 감시를 적용하고 있는가?	9.2.1 악성코드 통제	2.10.9 악성코드 통제	8.7 악성코드 방지	8.7 악성코드에 대한 보호	12.2 악성코드 방지

클라우드 서비스 수탁사 점검 항목(안)						CSAP	ISMS-P	ISO 27001	ISO 27002	ISO 27018
#	Category	Area	Domain	Control	Questionnaire	세부인증 항목	세부인증 항목	세부인증 항목	세부인증 항목	세부인증 항목
33				운영 체제 패치 적용	개인정보취급자 PC의 운영체제에 대해 최신 보안 패치를 설치하고 있는가?	-	2.10.8 패치관리	8.19 운영 체제에 소프트웨어 설치	8.19 운영 체제에 소프트웨어 설치	12.5 운영 소프트웨어 통제
34				매체 제어	보조저장매체에 대해 쓰기 금지 정책이 적용되어 있는가?	12.2.2 이동매체 관리	2.10.7 보조저장 매체 관리	8.12 데이터 유출 방지	8.12 데이터 유출 예방	A.11.4 외부 반출 저장매체의 데이터 보호
35			네트워크 접근통제 (PC)	유해 사이트 및 프로그램 통제	취급중인 개인정보가 인터넷 홈페이지, P2P 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터 및 모바일기기 등에 별도의 조치를 취하고 있는가?	10.1.1 접근통제 정책 수립	2.6.7 인터넷 접속 통제	8.23 웹 필터링	8.23 웹 필터링	9.1 접근 통제 업무 요건
36		접근통제	네트워크 영역 통제	네트워크 영역 분리	서비스, 사용자 그룹, 정보자산의 중요도, 법적 요구사항에 따라 네트워크 영역을 물리적 또는 논리적으로 분리하고 있는가?	11.1.5 네트워크 분리	2.6.1 네트워크 접근	8.22 네트워크 분리	8.22 네트워크 분리	13.1 네트워크 보안 관리

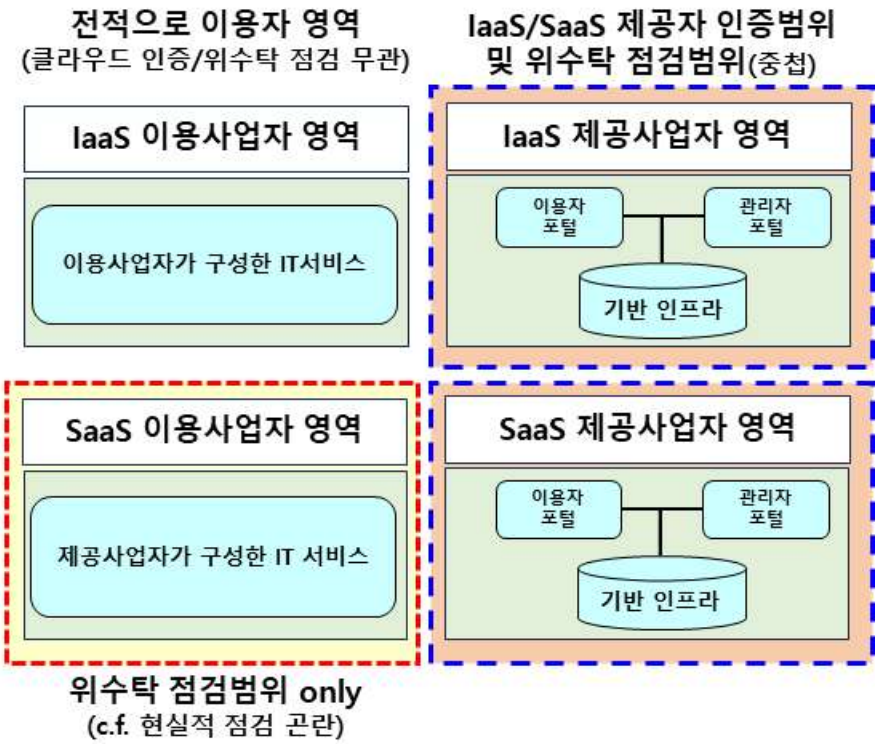
클라우드 서비스 수탁사 점검 항목(안)						CSAP	ISMS-P	ISO 27001	ISO 27002	ISO 27018
#	Category	Area	Domain	Control	Questionnaire	세부인증 항목	세부인증 항목	세부인증 항목	세부인증 항목	세부인증 항목
37			시스템 접근통제	개인정보처리시스템 접근 통제	개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 안전한 인증수단을 적용하고 있는가?	10.3.3 강화된 인증 수단 제공	2.5.3 사용자 인증	8.5 보안 인증	8.5 안전한 인증	9.3.1 기밀 인증정보 사용
38				정보시스템 접근 통제	정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 정보시스템(서버, 응용프로그램, DB 등)의 접근을 제한하고 있는가?	11.1.1 네트워크 보안정책 수립	2.6.2 정보시스템 접근	5.15 접근 통제	5.15 접근 통제	9.4 시스템 및 애플리케이션 접근 통제
39		운영 통제	백업 및 복구	백업 및 복구절차 수립·이행	백업 대상, 주기, 방법, 절차 등이 포함된 백업 및 복구절차를 수립·이행하고 있는가?	14.2.2 중요 장비 이중화 및 백업체계 구축	2.9.3 백업 및 복구관리	8.13 정보 백업	8.13 정보 백업	12.3 백업
40			취약점 점검	정보시스템 주기적 취약점 점검	정보시스템 취약점 점검 절차를 수립하여 정기적으로 점검을 수행하고 있는가?	3.3.2 취약점 점검	2.11.2 취약점 점검 및 조치	8.8 기술적 취약점 관리	8.8 기술적 취약성 관리	12.6 기술적 취약점 관리
41	정보보호 및 개인정보	보호 구역 통제	개인정보 보관 및 출입통제	서류, 저장 매체 보관	개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하고 있는가?	12.2.2 이동매체 관리	2.10.7 보조 저장매체 관리	7.3 사무실, 룸, 시설 보안	7.3 사무 공간 및 시설 보안	11.2.9 책상 정리 및 화면 보호 정책

클라우드 서비스 수탁사 점검 항목(안)						CSAP	ISMS-P	ISO 27001	ISO 27002	ISO 27018
#	Category	Area	Domain	Control	Questionnaire	세부인증 항목	세부인증 항목	세부인증 항목	세부인증 항목	세부인증 항목
42	물리적 보호조치		절차	보호 구역 통제	전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하고 있는가?	8.1.1 물리적 보호구역 지정	2.4.2 출입통제	7.7 책상 정리 및 화면 보호	7.7 책상 정리 및 화면 보호	11.1 보안 구역

제 3 절 수탁사 점검범위와 클라우드 인증범위의 중첩도 분석

앞서 본 클라우드 인증 범위와 위·수탁 점검 범위를 비교하면 아래와 같다.

[그림 4-1] 클라우드 인증범위 및 위수탁 점검범위 비교



IaaS의 경우 가상화 서버와 OS, DB 등 기반 인프라를 IaaS 제공사업자가 제공하고(그림 중 'IaaS 제공사업자 영역'), 그 위에서 작동하는 고객(end-user)용 애플리케이션을 IaaS 이용사업자가 직접 개발·운영하는 구조이다(그림 중 'IaaS 이용사업자 영역'). 이 경우 고객정보는 IaaS 이용사업자 영역의 애플리케이션에서 이용사업자가 프로그래밍 한 대로 처리되고, 이것이 저장·보관되는 기반 인프라가 IaaS 제공사업자 영역일 뿐이다. 즉, 위·수탁 범위는 '기반 인프라 운영'에 한정되므로, IaaS 이용사업자는 제공사업자가 기반 인프라를 안전하게 운영하고 있는지에 대해서만 위·수탁 점검을 하면 된다. 이때 기반 인프라의 안전성에 대하여는 IaaS 제공사업자가 ISMS-P 등 인증을 획득하는 과정에서 이미 심사가 완료되어 있다. 그렇다면 수많은 IaaS 이용사업자가 일일이 기반 인프라의 안전성을 점검하지 않더라도 ISMS-P 등 인증심사원들이 대신 점검을 해준 것으로 볼 수 있고 통상 인증심사원들이 전문성이 훨씬 더 높으므로, 위·수탁 점검을 인증으로 갈음하여도 현실적 문제는 없다고 보인다.

한편, SaaS의 경우 위·수탁 점검범위 중 인증범위와 중첩되는 곳과 그렇지 않은 곳으로 구분된다. SaaS 제공사업자는 기반 인프라(그림 중 'SaaS 제공사업자 영역')

뿐만 아니라 고객용 애플리케이션까지 미리 구성하여 판매하며, 이를 통째로 구독하는 SaaS 이용사업자는 템플릿화된 애플리케이션을 운영하며 고객에게 서비스를 제공한다(그림 중 'SaaS 이용사업자 영역').

전자의 'SaaS 제공사업자 영역'에 대해서는 IaaS와 마찬가지로 이용사업자가 제공사업자에게 기반 인프라 운영을 위탁한 것이고, 제공사업자가 인증을 받았다면 이 부분에 대해 위·수탁 점검이 이루어진 것으로 갈음하여도 문제가 없을 것이다.

이와 달리 후자의 'SaaS 이용사업자 영역'(그림 중 붉은색 점선)의 경우, 대고객 책임주체인 이용사업자(위탁자)가 애플리케이션상에서 이루어는 정보처리를 제공사업자(수탁자)에게 위탁한 구도이므로 현행법대로라면 위탁자는 수탁자가 제공하는 애플리케이션의 안전성 등을 점검해야 하는데, 이는 이용사업자별 맞춤형 소프트웨어가 아니라 제공사업자가 미리 마련해둔 완제품이어서 현실적으로 이용사업자에게 통제권이 없고 이용사업자의 수 또한 워낙 많으므로 일일이 위·수탁 점검을 한다는 것은 사실상 불가능하다. 그런데 이 영역의 애플리케이션은 제공사업자의 클라우드 인증 범위에도 포함되지 않는다. ISMS-P를 비롯한 대부분의 개인정보보호 인증은 인증신청기관이 고객(end-user)으로부터 직접 수집하여 처리하는 부분을 대상으로 하며, 수탁자의 지위에서 처리위탁을 받은 부분의 경우 관행적으로 인증 대상에서 제외하여 왔다. 수탁 부분을 인증 범위에서 제외해온 이유는, 처리되는 개인정보가 수탁자(인증신청기관)측 고객 데이터가 아니라 위탁자 측 고객 데이터인 점, 위탁자의 대고객 책임 영역이므로 위탁자의 인증신청 시 심사해야 할 뿐이지 수탁자의 인증심사 범위로 보기 어렵다는 점 등이다. 즉, SaaS 이용사업자 영역에 탑재된 애플리케이션의 경우 실질적 통제권은 제공사업자에게 있지만, 여기에서 처리되는 데이터가 제공사업자의 것이 아니라는 이유로 클라우드 인증을 통해서 심사를 해주지 않는다. 이에 SaaS 이용사업자 영역은 위·수탁 점검도, 인증에 의한 심사도 이루어지지 않는 사각지대가 될 우려가 크다고 보인다. 다만, 이 문제는 단기적 해결은 어려워 보인다.

제 5 장 클라우드 환경에 적합한 안전성 확보조치 제도 집행방안 제언

제 1 절 클라우드 제공사업자의 수탁자 지위 명확화 필요성

그간 클라우드 서비스 제공사업자가 수탁자 지위에 있는지 여부가 쟁점이 되어 왔고, 특히 IaaS 제공사업자의 경우 개인정보처리 수탁자 지위에 있지 않다는 견해가 현장에 팽배하였다. 그 핵심적인 이유 중 하나는 IaaS의 가상 서버·OS·DB 등 기반 인프라 위에서는 개인정보가 처리될 수도 있고 개인정보가 아닌 다른 데이터가 처리될 수도 있어, IaaS 제공사업자로서는 자신의 인프라 위에서 개인정보 처리가 일어나는지 알 수 없고 이는 오로지 이용사업자가 통제하는 영역이므로, IaaS 제공사업자가 개인정보 처리에 관한 책임을 부담하기 곤란하다는 것이었다.

그러나 2023년 한국인터넷진흥원에서 발주하여 한국CPO포럼에서 수행한 선행 연구용역에서는 SaaS는 물론 IaaS 또한 클라우드 서비스 제공사업자를 개인정보 보호법상 ‘수탁자’로 볼 수 있다는 시사점을 도출하였다. “금융분야 클라우드컴퓨팅서비스 이용 가이드(2023.02, 금융보안원)” 또한 클라우드 서비스 제공사업자를 수탁자로 판단하고 있다. 그렇게 보아야만 사고원인 조사 및 법적 책임 부과에 있어 법집행 공백이 초래되지 않기 때문이다.

■ 금융분야 클라우드컴퓨팅서비스 이용 가이드(2023.02)(3페이지 발췌)

전자금융업무와 관련한 정보처리시스템을 해당 금융회사를 위하여 운영하는 사업자는 전자금융보조업자에 해당하므로, 전자금융업무 관련 정보처리에 클라우드서비스를 이용하는 경우 클라우드서비스 제공자 또한 전자금융보조업자에 해당함.

정보처리의 위탁이라 함은 금융회사가 자신의 정보처리(전산설비를 활용하여 정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기 및 기타 유사한 행위를 하는 것) 업무를 제3자로 하여금 계속적으로 처리하도록 하는 행위를 말하므로, 금융회사가 클라우드서비스 제공자와 계약을 체결하고 클라우드서비스를 이용하는 행위는 정보처리위탁규정 제2조제6항에 따라 정보처리의 위탁에 해당함

전자금융거래법 제11조에 따라 전자금융거래와 관련하여 클라우드서비스 제공자의 고의나 과실은 금융회사의 고의나 과실로 봄

전자금융사고 발생 시 클라우드서비스 이용을 이유로 금융회사의 책임이 면제되지 않으며, 금융회사는 클라우드서비스 제공자가 관계 법령을 준수하도록 관리·감독 하여야 함

사고원인 조사 측면을 보면, 예컨대 클라우드가 아닌 자체 서버 환경에서 안전성 확보조치 미흡으로 유출 등 사고가 발생하는 경우, 개인정보 보호위원회는 해당 개인정보처리자의 서버 내 로그 등을 제출 받아 사고 원인분석을 하고 이를 행정처분 근거자료로 삼는다. 한편, 클라우드 환경에서 유출 등 사고가 터진 경우, 로그 등이 이용사업자 영역이 아니라 클라우드 제공사업자 영역에 보관된 사례가 많다. 이에 개인정보 보호위원회로서는 클라우드측 로그 등을 제출 받을 수 있어야만 사고조사를 제대로 할 수 있고, 사고조사 시 드러난 귀책에 따라서 합리적인 법적 책임을 부과할 수 있다.

그나마 SaaS 제공사업자의 경우 수탁자 지위에 있어 개인정보 보호위원회의 조사 및 자료요구에 응해야 할 법적 의무(이하 '수검의무')가 있다는 인식이 심어져 있는 편이다. 반면에 IaaS 제공사업자의 경우 그러한 인식이 없어 특히 해외사업자의 경우 클라우드측 로그 제출을 요청 받고도 이에 응하지 않는 등으로 인해 사고조사 및 법집행의 난관이 되어 왔다.

이 문제를 해결하려면, 우선 클라우드 서비스 제공사업자가 개인정보보호법상 수탁자 지위에 있다는 해석을 명확히 할 필요가 있다. 물론 수탁의 범위는 클라우드 서비스 내용에 따라 달라지는데, IaaS라면 기반 인프라 제공·관리 부분만 수탁범위일 것이고, SaaS라면 클라우드측에서 마련한 애플리케이션에서 이루어지는 정보처리까지 수탁범위로 보아야 할 것이다. 개인정보 보호법 제63조에 따른 수검업무의 대상자에는 '수탁자'도 포함되므로, 클라우드 서비스 제공사업자의 수탁자로서의 지위를 명확하게 인정하는 해석이 뒷받침되어야 한다.

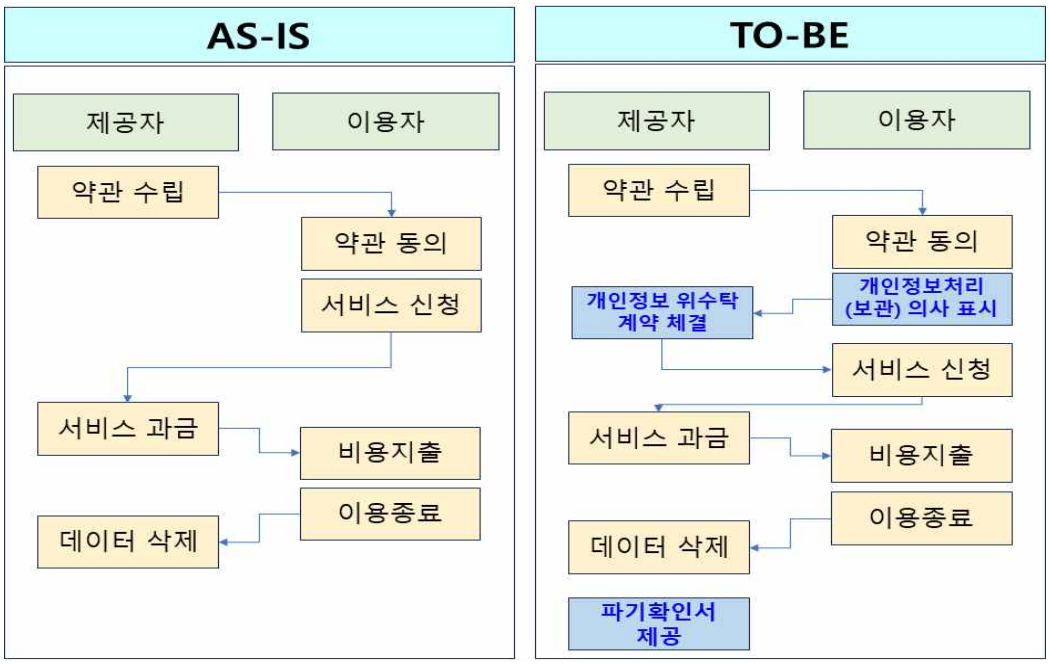
[표 5-1] 개인정보 유출·침해사고 발생시 조사 근거규정

규정	내용
개인정보 보호법	제63조(자료제출 요구 및 검사) ① 보호위원회는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보처리자에게 관계 물품·서류 등 자료를 제출하게 할 수 있다. 1. 이 법을 위반하는 사항을 발견하거나 혐의가 있음을 알게 된 경우 2. 이 법 위반에 대한 신고를 받거나 민원이 접수된 경우 3. 그 밖에 정보주체의 개인정보 보호를 위하여 필요한 경우로서 대통령령으로 정하는 경우 ② 보호위원회는 개인정보처리자가 제1항에 따른 자료를 제출하지 아니하거나 이 법을 위반한 사실이 있다고 인정되면 소속 공무원으로 하여금 개인정보처리자 및 해당 법 위반사실과 관련한 관계인의 사무소나 사업장에 출입하여 업무 상황, 장부 또는 서류 등을 검사하게 할 수 있다. 이 경우 검사를 하는 공무원은 그 권한을 나타내는 증표를 지니고 이를 관계인에게 내보여야 한다. ⑤ 제1항 및 제2항에 따른 자료제출 요구, 검사 절차 및 방법 등에 관하여 필요한 사항은 보호위원회가 정하여 고시할 수 있다. 제73조(벌칙) ① 다음 각 호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다. 4. 제63조제1항(제26조제8항에 따라 준용되는 경우를 포함한다)에 따른 자료제출 요구에 대하여 법 위반사항을 은폐 또는 축소할 목적으로 자료제출

	을 거부하거나 거짓의 자료를 제출한 자 5. 제63조제2항(제26조제8항에 따라 준용되는 경우를 포함한다)에 따른 출입·검사 시 자료의 은닉·폐기, 접근 거부 또는 위조·변조 등을 통하여 조사를 거부·방해 또는 기피한 자
개인정보보호법 시행령	제60조(자료제출 요구 및 검사) ① 법 제63조제1항제3호에서 "대통령령으로 정하는 경우"란 개인정보 유출 등 정보주체의 개인정보에 관한 권리 또는 이익을 침해하는 사건·사고 등이 발생하였거나 발생할 가능성이 상당히 있는 경우를 말한다.
개인정보보호위원회의 조사 및 처분에 관한 규정	제2조(정의) 이 규정에서 사용하는 용어의 정의는 다음 각 호와 같다. 3. "조사대상자"란 개인정보 보호 법령 및 이 규정에 따라 보호위원회의 조사등을 받는 법 제2조제5호에 따른 개인정보처리자(법 제26조제2항에 따른 수탁자를 포함한다. 이하 같다) 및 신용정보법 제45조의3제1항에 따른 상거래기업 및 법인(같은 법 제17조제2항에 따른 수탁자를 포함한다. 이하 같다)을 말한다.

특히 IaaS 제공사업자의 수탁자 지위를 명확히 하려면, 해당 IaaS상에서 개인정보 처리가 일어나는지 여부를 이용사업자로부터 '고지' 받는 절차가 마련되는 것이 바람직하다. 그래야만 IaaS 제공사업자가 자신의 법적 지위를 인식하고 필요한 조치를 취할 수 있기 때문이다. 여기서 '필요한 조치'란, ① 클라우드 서비스 이용개시 시 개인정보 처리에 관한 위·수탁계약을 체결하고(법상 요구되는 위수탁 계약사항이 클라우드 이용약관에 포함되면 될 것이다), ② 이용기간 중 위·수탁 점검에 응하거나 또는 이를 앞서 본 클라우드 인증으로써 갈음하도록 하며, 이용사업자 서비스에서 해킹 사고 발생 시에는 원인조사를 위해 필요한 경우 IaaS측 로그가 제출될 수 있도록 조치하고, ③ 이용종료 시 당해 이용사업자측의 데이터를 파기하는 것이다(파기 증적으로서 파기확인서가 제공되면 가장 바람직하고, 최소한 이용약관에 파기 약정이 있어야 한다).

[그림 5-1] 클라우드 서비스 이용절차 개선방안



제 2 절 클라우드 제공 보호조치기능 관련 제언

제3장에서 살펴보았듯 일부 IaaS/SaaS 제공사업자의 경우 이용사업자가 개인정보 안전성 확보조치기준 고시를 준수하기 위해 필요로 하는 보호조치기능을 일부 미흡하게 제공한 것으로 보였고, 부수적으로 SaaS의 경우 예컨대 애플리케이션 내 마스킹이 미흡하거나 고객정보의 암호화 저장여부를 확인할 수 없는 사례가 있었다. 이러한 경우 과연 이용사업자가 고시를 준수할 수 있을지 검토가 필요하며, 만약 준수할 다른 방법이 있다고 해도 이를 위해 이용사업자가 투입해야 하는 추가적인 비용·노력이 과다하다면 클라우드 서비스 제공사업자 측에서 해당 보호조치기능을 필수 제공하도록 개선·권고하는 방안도 고려해봄직하다.

한편, 고시상 보호조치의무 중 일부는 현재의 기술 트렌드와 어울리지 않거나 또는 현장 상황 대비 지나치게 경직된 기준을 요구하는 것이 있었다. 예외(예: 신뢰할 수 있는 단말기)를 인정하지 않는 idle timeout, 로그인 인증오류 횟수 초과 시 계정 잠금 의무화 등이 그러한 예로 보인다. 이들 고시 조항은 실질적 보안성 제고에 기여하는 정도가 미미한데 비해 수범자들의 규제 준수비용을 과다하게 요구하여 그 존치 필요성에 대한 재검토를 요한다.

클라우드 분야 개인정보 보호조치 현황분석 결과보고서

인 쇄 : 2024 년 05 월
발 행 : 2024 년 05 월

발행인 : 이 상 중
발행처 : 한국인터넷진흥원(KISA, Korea Internet&Security Agency)
전라남도 나주시 진흥길 9
Tel: 1544-5118

<비매품>