The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 23, No. 3, pp.19-26, Jun. 30, 2023. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2023.23.3.19
JIIBC 2023-3-3

하이퍼 스케일 클라우드에 적합한 정보보호 및 개인정보보호 관리체계 인증 통제항목 연구

A Study on ISMS-P Controls for Hyper Scale Cloud

신용녀*

Yong-Nyuo Shin*

요 약 전 세계적으로 에너지, 금융 서비스, 보건, 통신, 교통 분야의 클라우드 전환에 따라 지속적으로 클라우드제공업체에 대한 주요기반시설 지정 움직임이 확산되고 있다. 또한, 우크라이나 사태에서는 국가 주요시설의 클라우드 사용 규제 철폐와 신속한 주요 데이터에 대한 클라우드 전환으로 인해 러시아의 기반시설을 겨냥한 사이버 공격에 효율적으로 대처할 수 있었다. 한국에서는 체계적, 종합적인 정보보호 관리체계를 구현하고, 조직의 정보보호 및 개인정보보호 관리 수준 향상을 위해 ISMS-P가 기업의 정보보호 및 개인정보보호 수준 제고를 위해 운영되고 있다. 클라우드 환경을 고려한 통제항목이 수정, 추가 되어 기업의 심사에 운영되고 있다. 그러나, 클라우드의 국내외 기술적 수준이 상이하고 하이퍼스케일 규모에 대한 국내 인증심사원들의 교육을 위해서는 Microsoft같은 클라우드 공급업체의 결함사항에 대한 정보를 구하기 쉽지 않았다. 이에, 본 논문에서는 하이퍼스케일 클라우드상 에서의 결함사항을 분석하고, 하이퍼스케일 환경과 ISO/IEC 27001 및 SOC 보안 국제 표준과의 정합성을 고려하여 보다 클라우드에 특화된 통제항목 개선방안을 제시하였다.

Abstract Critical information infrastructure designations for cloud service providers continue to spread around the world as energy, financial services, health, telecommunications, and transportation sectors move to the cloud. In addition, in the case of Ukraine, the removal of restrictions on the use of cloud for national critical facilities and the rapid transition of critical data to the cloud enabled the country to effectively respond to cyberattacks targeting Russian infrastructure. In Korea, the ISMS-P is operated to implement a systematic and comprehensive information protection management system and to improve the level of information protection and personal information protection management in organizations. Control items considering the cloud environment have been modified and added to the audit of companies. However, due to the different technical levels of clouds between domestic and global, it is not easy to obtain information on the findings of cloud providers such as Microsoft for the training of domestic certification auditors on hyperscale scale. Therefore, this paper analyzes findings in hyperscale clouds and suggests ways to improve cloud-specific control items by considering the compatibility of hyperscale environments with ISO/IEC 27001 and SOC(System and Organization Control) security international standards.

Key Words : Personal Information & Information Security Management System, Critical Information Infrastructure, Finding, Control

*정회원, 마이크로소프트 최고기술임원(National Technology Officier)
접수일자 2023년 4월 2일, 수정완료 2023년 5월 2일
게재확정일자 2023년 6월 9일

Received: 2 April, 2023 / Revised: 2 May, 2023 / Accepted: 9 June, 2023
*Corresponding Author: yoshin@microsoft.com
Dept. of Public Sector, Microsoft, Korea

I. 서 론

러시아가 우크라이나 전쟁에서 물리적 공습과 병행하여 우크라이나의 주요기반시설(Critical Information Infrastructure)를 겨냥한 '폭스블레이드(Foxblade)[1]' 라는 사이버 무기를 사용하면서, 군사 침공을 방어하려면 대부분의 국가들은 국경 너머 다른 국가로 디지털 운영과 데이터 자산을 분배하고 분산할 수 있는 능력을 갖추어야 하는 필요성이 제기 되었다. 우크라이나 전 이전에는 프라이어시와 데이터 가버넌스 측면을 고려하여 공공기관, 에너지 등을 포함한 주요기반시설에 온-프레미스(on premises) 서버에서 운영되도록 정부가 규제하고 있었다. 그러나, 러시아가 48곳의 국가주요기반시설에 네트워크에 파괴적인 '와이퍼(wiper)' 공격을 감행함으로써, 우크라이나 정부는 유럽 전역의 데이터 센터에서 관리되는 하이퍼 스케일의 퍼블릭 클라우드로 디지털 인프라를 신속하게 분산함으로써 소프트웨어와 데이터를 파괴하도록 설계된 맬웨어를 유포해 네트워크 도메인에 침투하게 하는 공격에 사이버 방위가 가능했다.

II. 주요기반시설 지정 개념

각국 정부는 국가 경제와 사회 기능에 가장 중요한 시스템의 복원력을 파악하고 보장하기 위한 국가 프로그램을 수립해왔다. 1997년부터 미국이 이를 선도해 왔지만, 수십 개의 다른 국가에서도 유사한 프로그램을 추진하고 있다[2]. 특히 에너지, 금융 서비스, 보건, 통신, 교통 분야의 클라우드 전환에 따라 더 자동화되고 상호 의존성이 커지고 있다는 인식에 따라 지속적으로 클라우드제공업체(Cloud Service Provider) 자체에 대한 주요기반시설 지정 움직임이 확산되고 있다[3]. 2008년 금융 위기 이후 일부 주요기반시설 기능이나 경제 시스템이 단일 기업에 너무 의존적이어서 해당 기업의 실패가 전체 산업 또는 경제의 붕괴를 유발할 수 있으며, 따라서 "시스템적 위험"을 초래할 수 있다는 인식도 점차 높아지고 있다. 디지털 트랜스포메이션 전환이 가속화됨에 따라 무엇이 중요하고 시스템적 위험이 어디에 존재할 수 있는지에 대한 새로운 사고를 유도하고 있다. 정부 부처는 점점 더 중요한 워크로드에 클라우드 기술을 활용하거나 평가하고 있으며, 전통적으로 중요하다고 여겨지던 분야에서도 사이버 위협을 추적하고 예측하는데 AI(Artificial Intelligence)에 기반한 광범위한 데이터 분석을 위해 클라우드 서비스를 전환이 가속화 되고 있다. 특히 인프라 및 플랫폼 수준 서비스의 경우 소수의 공급업체가 시장을 장악하고 있으며, 특히 AWS, Azure, Alibaba, Google Cloud Platform이 시장의 84%를 점유하고 있다[4].

금융, 정부 기관들의 주요 국가 기반시설의 하이퍼 스케일 도입에 따라, 여러 정부 정책 입안자와 규제 당국은 클라우드 서비스를 주요기반시설로 지정할지 또는 클라우드제공업체(CSP)를 시스템 리스크를 입증하는 주체로 지정할지 여부와 그 방법을 표 1과 같이 모색하고 있다.

표 1. 각국의 CSP 기반시설 지정 현황
Table 1. CSP desigantions as a CII in each country

국가	핵심 기반 시설 지정	시스템적 리스크 감지	참고
미국	외국인 투자 위원회를 통해 시사되어 미국 국토안보부에서 고려 중	2017년 연간 행정명령 13636 9항 평가의 일환으로 고려됨	위반사례 및 공급망 교차점으로 인해 해당 작업이 가속화될 수 있음
유럽 연합	2016년 완료된 네트워크 및 정보 보안 부서 (NIS)의 지침사항 버전 1 개발 중에 고려됨	2019년 보고서에서 강조된 바와 같이, 유럽 은행 감독 기관에 의해 평가 중	2021년에 NIS 지침사항이 업데이트/개정 될 경우 재평가 될 예정
독일	물리적 클라우드 시설 (즉, 데이터 센터)이 핵심 기반 시설"로 고려됨	해당없음	물리적 시설 이외의로 지정 범위를 확대 할 수도 있음
중국	현재 두개의 정부기관에서 동시에 검토 중	해당없음	내외부적 정치적 요인이 중대한 영향을 미칠 수 있음
싱가포르	핵심 인프라 보호법 개발 하던시기인 2017년에 고려되었으며, 2018년에 확정됨 (대신, IT 벤더의 위험은 간접적으로 관리)	해당없음	금융감독기관들은 시스템적 리스크에 대해 유럽 모델을 따를 수 있음
대한민국	핵심 정보 인프라로 간주	해당없음	2022년 지정

1. 클라우드 기반 시설의 기술적 이점

기반 시설 운영자가 클라우드에 대한 위험 기반 평가(risk-based assessment)를 수행하기 위해서는 클라우드의 특성을 이해하고 잠재적으로 발생할 수 있는 위험에 대한 평가를 수행해야 한다. 클라우드 기반 기술 솔루션을 사용할 때 얻게 되는 잠재적 이점은 첫째, 보안에 관한 높은 인지도 제공이 가능하다. 많은 조직들이 아직도 레거시 IT 및 관련 운영 기술(OT)에 의존하고 있는

데, 그들은 사이버 위험 노출에 대한 인식이 부족하다. 데이터를 클라우드 환경으로 이전하면 모든 자원에대한 가시성(Visibility) 제공이 가능하기 때문에 데이터 거버넌스가 강화된다. 이를 통해, 데이터가 어떻게 관리되고 있는지 조직 구성원들의 인식이 높아질 수 있다. 또한, 융합 환경에서 복잡하게 발생하는 사이버 보안 위험도 줄일 수 있다. 둘째, 비즈니스 핵심으로서의 보안성 담보가 가능하다. 비즈니스 모델에서 가장 근본적인 부분은 결국 신뢰이다. 보안은 신뢰와 직결되기 때문에, 클라우드 사업자들에게 보안은 자신들을 차별화하는 핵심 가치이다. 셋째, 복원력 및 복구 가능성 기반의 설계가 가능하다. 하이퍼스케일 클라우드 사업자(Hyperscale cloud provider)는 다양한 상황과 변수에 대응하기 위해서 복원력을 갖춘 시스템을 운영한다. 악성 프로그램 감염, 시스템 장애, 환경 재앙이 발생할 수 있다는 가정에서 출발하고, 데이터 센터 복제, 데이터 미러링, 페일오버(failover) 및 복구 기능은 하이퍼스케일 클라우드 사업자가 서비스를 운영하는 기본적인 방식이다. 넷째, 빠르고 탄력적인 대응이 가능하다. 고객들은 클라우드 복원력을 통해 비상사태에 대응하고 디도스(DDoS) 공격을 더 효과적으로 차단할 수 있다. 클라우드는 빠르고 탄력적이며 스마트한 확장력을 바탕으로 외부의 악의적인 공격이나 갑자기 늘어난 수요에 재빠르게 대응이 가능하다. 다섯째, 보안 유지 보수 및 기능 아웃소싱이 가능하다. 책임 공유 모델에 따라 클라우드 사업자는 데이터 센터 보안뿐 아니라 네트워크 제어, 패치 적용, ID 및 액세스 제어에 관해서도 책임을 질 수 있습니다. 클라우드 사업자는 처리 중인 데이터의 암호화와 같은 고급 보안 기능도 관리할 수 있다.

2. 정부의 기반시설 지정을 위한 고려사항

정부는 기반시설 정책을 보완함에 있어 '국가 안보'와 '경제적 탄력성' 양 측면 모두 세심하게 고려하고자 한다. 정부의 이같은 노력은 기반시설에 대한 사이버공격이 날이 갈수록 점점 더 정교해지고 파괴적이며 많은 손해를 끼친다는 사실과 맞물려 있기 때문이다. 현행 수칙이나 기준, 규제를 기술 변화에 따라 어떻게 통합하고 조정해야 하느냐 하는 문제는 디지털경제 시대에 정부가 풀어야 할 쉽지 않은 과제이기 때문에, 정부가 기반시설에 대한 규제감독을 강화할 때는 주요 핵심 분야에만 한정하고, 리스크 기반(risk-based)으로 접근할 필요가 있다. 세계 각국이 참고하고 있는 국제 모범 사례(international best practice) 도 모두 이 범주에 속한다.

이를 이행하기 위해서는 우선 데이터나 시스템, 그리고 서비스를 각각의 기밀 수준에 맞춰 분류해야 한다. 그런 다음 전체적인 리스크 관리를 위한 전략을 짜야 한다. 데이터, 시스템 및 서비스에 대한 위협과 취약성 분석은 물론이고, 이용하려는 클라우드가 안전성과 복원력(resilience) 을 충족하고 있는지 살피는 일도 중요하다. 지나치게 광범위하고 다루기 어려운 방식을 채택하면 오히려 리스크를 더 키우는 결과를 초래할 수 있다.

정부가 리스크의 우선 순위를 매겨 필요한 곳을 집중 관리한다면 지속적인 디지털 전환과 시장 혁신이 가능하다. 현재 국내는 정보통신기반보호법(제8조의2)에 근거하여 주요정보통신기반시설로지정이되면법적보호조치를 이행해야 하고 매년 점검을 받아야 한다. 또한, 가이드라인에 근거하여 기반시설이 클라우드 이용 시 데이터 및 데이터를 처리하는 시스템은 국내에 위치하여 한다고 규정하고 있다. 이 같은 데이터 현지화는 기반시설 사업자로 하여금 '규모의 경제'를 실현할 수 없도록 하고, 클라우드를 이용함으로써 얻을 수 있는 여러 편익을 저해한다. 뿐만 아니라 하이퍼스케일 의 퍼블릭 클라우드 환경에서의 데이터 보안은 데이터가 어디에 저장되느냐 하는 문제와 거의 관련이 없다. 오히려 데이터 현지화 규정은 다양한 신규 서비스의 출현으로 서버나 데이터 위치의 유연한 선택을 가로막음으로써 보안을 더 취약하게 할 수도 있다. 또한, 기반시설을 겨냥한 사이버 공격에 더 쉽게 노출되는 결과를 초래할 수 있다는 것을 우크라이나 사태로 확인가능하다. 물론 국가적으로 민감한 사안(예: 국방 계획이나 국가정보 등 국가안보와 관련된 워크로드)에 관한 것이라면 데이터 현지화 규정이 적합할 수 있다. 인공지능 사용을 포함한 위협 인텔리전스의 발전으로 사이버 공격을 보다 효과적으로 탐지가 필요하고, 인터넷 연결 엔드포인트 보안을 통해 클라우드 서비스 및 기타 연결된 컴퓨터 장치에 보안 소프트웨어 코드를 신속하게 배포해 맬웨어를 식별하고 비활성화기 위해서는 데이터의 중요성과 위협을 평가한 후 사례별로 구현해야 한다.

III. 정보보호 및 개인정보보호 관리체계 인증 통제항목

클라우드 이용이 확산됨에 따라 글로벌 클라우드 공급업체들은 정보보호 및 개인정보보호 관리체계 인증(ISMS-P)의 의무 대상은 아니지만, 클라우드를 사용하는

임의 사용자의 편의와 보안적 신뢰성을 보장하기 위해 매년 ISMS-P에 대한 인증심사를 한국인터넷진흥원로부터 수검을 받고 있었다. 또한, 인증심사 대상의 수요 증가와 인증기관의 역할에 전념하고자 한국인터넷진흥원은 한국정보통신진흥협회(KAIT), 한국정보통신기술협회(TTA)등의 심사기관을 추가 지정하여 운영하고 있다[5]. Microsoft는 “클라우드 서비스(Azure) 한국 리전의 인프라 운영”의 심사범위로 2018년부터 IaaS에 대하여 한국인터넷 진흥원으로부터 매년 수검을 받아오고 있다[6]. Azure 운영환경에 대한 절차 확인을 위해 총 35종의 표준운영절차(Standard Operating Procedure)에 대하여 절차대로 운영되고 있는지에 대한 점검을 받고 있다. 또한, 2022부터는 통합된 정보보호 및 개인정보보호 관리체계 인증(ISMS-P)로 최초인증을 획득하였다. 2018년에는 5개, 2019년에는 4개, 2020년에는 6개, 2021년에는 6개, 2023년에는 5개의 결함에 대하여 보완조치를 완료한바 있다. 본 논문에서는 하이퍼스케일 클라우드상 에서의 결함사항을 분석하고, 클라우드 환경의 확산에 따라 2018년 제도통합[5]으로 ISMS-P 통제항목이 수정되었으나 하이퍼스케일 환경과 ISO/IEC 27001 및 SOC 보안 국제 표준과의 정합성을 고려하여 보다 클라우드에 특화된 통제항목 개선방안을 제시한다.

1. 클라우드 관련 ISMS-P 통제항목

클라우드 환경의 확산에 따라 제도통합 시기와 맞물려 클라우드 환경을 고려한 ISMS-P 통제항목이 표 2와 같이 신설, 변경되었다[5].

표 2. ISMS-P 클라우드 관련 보호대책 요구사항
Table 2. Cloud Specific Controls in ISMS-P

분야	항목	상세내용
2.3. 외부자 보안	2.3.1 외부자 현황 관리	업무의 일부(개인정보취급, 정보보호, 정보시스템 운영 또는 개발 등)를 외부에 위탁하거나 외부의 시설 또는 서비스(집적정보통신시설, 클라우드 서비스, 애플리케이션 서비스 등)를 이용하는 경우 그 현황을 식별하고 법적 요구사항 및 외부 조직·서비스로부터 발생되는 위험을 파악하여 적절한 보호대책을 마련하여야 한다.
2.10. 시스템 및 서비스 보안관리	2.10.2 클라우드 보안	클라우드 서비스 이용 시 서비스 유형(SaaS, PaaS, IaaS 등)에 따른 비인가 접근, 설정 오류 등에 따라 중요정보와 개인정보가 유·노출되지 않도록 관리자 접근 및 보안 설정 등에 대한 보호대책을 수립·이행하여야 한다.

2.10. 2의 클라우드 보안에 있어서는 표 3의 기준으로 주요 확인이 이루어진다.

표 3. 클라우드 보안의 세부점검 항목
Table 3. Cloud Security Checklist

항목	세부점검항목
2.10.2 클라우드 보안	클라우드 서비스 제공자와 정보보호 및 개인정보보호에 대한 책임과 역할을 명확히 정의하고 이를 계약서(SLA 등)에 반영하고 있는가?
	클라우드 서비스 이용 시 서비스 유형에 따른 보안위험을 평가하여 비인가 접근, 설정오류 등을 방지할 수 있도록 보안 구성 및 설정 기준, 보안설정 변경 및 승인 절차, 안전한 접속방법, 권한 체계 등 보안 통제 정책을 수립·이행하고 있는가?
	클라우드 서비스 관리자 권한은 역할에 따라 최소화하여 부여하고 관리자 권한에 대한 비인가된 접근, 권한 오남용 등을 방지할 수 있도록 강화된 인증, 암호화, 접근통제, 감사기록 등 보호대책을 적용하고 있는가?
	클라우드 서비스의 보안 설정 변경, 운영 현황 등을 모니터링하고 그 적절성을 정기적으로 검토하고 있는가?

또한, 시스템 유형별 인증범위 고려사항 중 신청기관이 클라우드서비스를 이용하여 정보통신서비스를 제공하는 경우, 신청기관이 관리 가능한 운영체제, DB, 응용프로그램 등은 인증범위에 포함하고 있다[5]. 단 클라우드서비스 형태에 따라 심사범위가 달라질 수 있으므로 관리범위, 지배권 소유 여부, 책임 소재 등에 따라 심사범위를 판단해야 한다고 정의하고 있다. 또한, 정부에서는 클라우드서비스 이용 시 안전성 및 신뢰성이 검증된 클라우드서비스 제공자를 이용할 것을 권고하고 있다. 국내 및 해외 클라우드서비스 모두 해당 범위에 포함하고 있는데, 하이퍼스케일의 특성상 자원의 빠른 배포(Scale-out)와 줄임(Scale-in)의 성능 및 제로트러스트 기반(Zero-Trust)의 기술적 관리적 성능 및 보안성의 기술적 차이는 상당하다고 볼 수 있다. 이에, 기술적 우위를 차지하고 있는 해외 클라우드 서비스에 있어서 ISMS-P 통제항목의 세부점검 항목으로 만으로는 검토하기 어려운 범위가 있는 것이 현실이다. 또한, 국제표준이나 해외 감독(Audit)과 국내 인증심사원의 견해(View) 차이가 있는 것이 현실이다. 이러한 기술적 격차와 국내 현실에 맞는 통제항목의 개선을 위해서는 하이퍼스케일 클라우드의 결함사항을 분석함으로써 한국 특화된 ISMS-P 통제항목 개발이 가능하다고 할 수 있다.

표 4. Microsoft Azure 운영 범위의 ISMS-P 결함내역
Table 4. ISMS-P Findings of Microsoft Azure's Operation

	통제 분야	결함내역
'18	4.1.1 정보자산 식별	일부 보안장비 및 네트워크 장비에 대한 자산식별 미흡
	5.1 법적요구사항 준수검토	개인정보 수집, 처리방침 관련 법규 준수 검토가 일부 미흡
	10.2.3 접근권한 검토	일부 정보시스템에 대한 접근권한 검토 미흡
	11.2.9 백업관리	네트워크 장비의 환경설정(Configuration) 백업 확인 불가
	11.6.2 로그기록 및 보존	일부 정보시스템에 대한 권한 부여, 로그기록 확인이 어려움
'19	1.2.1 상위 정책과의 연계성	위험 관리 절차와 전사 위험관리 프레임워크 간 일관성 확보가 미흡함
	3.2.1 외부자 보안 이행 관리	네트워크센터 물리보안 위탁업체의 운영에 대한 관리가 미흡함
	5.3 내부감사	내부감사시 정보통신망법 및 개인정보의 기술적, 관리적 보호조치 법적 요구사항에 대한 점검이 수행되지 않음
	10.4.1 네트워크 접근	일부 네트워크 장비로의 접근통제 설정 미흡
'20	3.3 정보보호대책 선정 및 이행계획 수립	전년도 K-ISMS 결함내용에 대한 이행이 미흡함
	5.1 법적요구사항 준수검토	일부 시스템의 개인정보 국외이전, Azure Portal DB탈퇴 시 파기, 개인정보 처리방침의 일부 필수항목 누락 등 법적 요구사항 준수 검토 필요
	7.1.4 출입통제	데이터센터 방문자 출입통제 미흡
	9.1.1 암호 정책 수립	대부분의 네트워크 장비에서는 Password8/9을 적용하고 있으나, 일부 장비에서 Password7 사용으로 비밀번호 암호화 기준 적용 미흡
	10.4.1 네트워크 접근	일부 정보시스템 연결시간 제한 정책 미준수
	11.6.1 시각 동기화	일부 정보시스템의 시각 동기화되고 있지 않음
'21	1.2.1 정보자산 식별	일부 정보자산에 대하여 식별이 미흡한 문제점이 발견됨
	1.2.2 현황 및 흐름분석	주요 직무자의 현황 및 흐름분석 현행화 미흡
	1.4.1 법적 요구사항 준수 검토	홈페이지에 게시된 개인정보처리방침 및 이용자 개인정보 처리 시의 법적 요구사항 준수 여부를 확인한 결과 문제점이 발견됨
	2.3.3 외부자 보안 이행 관리	외부자 보안 이행 관리에 대해 문제점이 발견됨
	2.9.6 시간 동기화	CCTV의 시간 동기화에 대한 검토가 미수행됨
'23	1.2.1 정보자산 식별	일부 정보자산 식별이 미흡한 문제점이 발견됨
	1.2.2 현황 및 흐름분석	정보서비스 흐름도 검토 결과 문제점이 발견됨
	1.4.1 법적 요구사항 준수 검토	일부 정보자산 식별에 대해 문제점이 발견됨
	2.5.6 접근권한 검토	정보시스템 접근권한 점검 결과 문제점이 발견됨
	2.6.1 네트워크 접근	네트워크 시스템 접근 및 정책 관리가 미흡한 문제점이 발견됨

21년 결함사항 중 1.2.1. 정보자산 식별 관련해서는 클라우드 운영환경을 관리하기 위한 시스템 중 일부 정보자산에 대하여 식별이 미흡한 문제점이 발견되었다. 모든 관리 운영이 자동화 되어 운영되는 하이퍼스케일 클라우드 환경에서는 많은 운영 툴(Tool)이 존재하고, 툴간의 통합이나 신규로 개발되어 도입되는 툴들이 존재한다. 이러한 운영 툴 중 정보자산 리스트에 기입되지 않았던 툴에 대한 식별 요청이 있었다. 또한, 1.2..2 현황 및 흐름분석에 있어서는 주요 직무자의 현황 및 흐름분석 현행화 미흡이 지적되었다. 프로덕션(Production) 환경에 툴 접속을 위한 접근통제 흐름을 식별하고, 프로덕션 환경에 접속하는 단말에 대한 접근통제 흐름에 대한 식별 요청이 있었다. 1.4.1 법적 요구사항 준수 검토에 있어서는 홈페이지에 게시된 개인정보처리방침 및 이용자 개인정보 처리 시의 법적 요구사항 준수 여부를 확인한 결과 개인정보 수집·이용 시 법적고지사항 표기 오류와 개인정보처리방침 현행화 미흡이 지적되어, 인증범위 대상 홈페이지에 게시된 개인정보처리방침을 현행화 하고, 개인정보 처리 관리 등의 절차를 재확인하여 이용자 개인정보 관리를 강화를 위한 조치를 수행하였다.. 2.3.3. 외부자 보안 이행 관리에 있어서는 수탁사 일부 보유기간 경과한 개인정보 파기 미흡이 지적되었다. 임대한 데이터센터의 출입관리시스템에서 출입자 정보를 3년간 보관함을 고지하고 있으나, "출입카드 대여이력 조회" 결과 3년이 경과된 개인정보가 파기되지 않은 사례가 발견되어 개인정보 파기 여부, 업무환경 보안 준수 여부 등 외부자의 보안 이행이 조치되었다. 2.9.6. 시간 동기화에 대해서는 CCTV의 시간 동기화에 대한 검토가 미 수행 사항이 결함으로 지적되었다. 임대한 데이터 센터의 CCTV 모니터링시스템에 설정된 촬영시간 정보가 표준시간으로 동기화되어 있지 않았고, 보완 조치 시 CCTV 모니터링시스템의 촬영시간 정보를 표준시간으로 동기화를 수행하였다.

Ⅳ. 클라우드에 특화된 통제항목 개선방안

1. 클라우드 데이터센터 계약운영 주체별 관리적 세부 통제마련

대부분의 글로벌 클라우드공급업체는 국내 IDC 사업자의 데이터 센터를 임대하여 운영하고 있다. 글로벌 C 클라우드공급업체가 데이터를 센터를 직접 지어서 운영하는 경우에는 글로벌 표준에 입각하여 운영되고 책임을

지기 때문에 결함으로 지적될 사항이 상대적으로 적다. 그러나, 임대하는 IDC의 CCTV나 데이터센터에 대한 출입자를 관리하는 주체가 IDC 사업자에게 위임된 경우가 결함으로 지적되는 사례가 있었다. 표 5의 외부자 현황 관리의 통제항목에 대하여 데이터센터의 운영과 임대 현황을 분석하여 운영 구획별 운영주체에 대한 책임/관리 범위에 대하여 명시 및 관리하는 방향으로 통제 항목 개선이 필요하다.

표 5. ISMS-P 외부자 보안 통제
Table 5. ISMS-P Security Control for the external identity

통제분야	상세내용
2.3. 외부자 보안	업무의 일부(개인정보취급, 정보보호, 정보시스템 운영 또는 개발 등)를 외부에 위탁하거나 외부의 시설 또는 서비스(집적정보통신시설, 클라우드 서비스, 애플리케이션 서비스 등)를 이용하는 경우 그 현황을 식별하고 법적 요구사항 및 외부 조직·서비스로부터 발생되는 위험을 파악하여 적절한 보호대책을 마련하여야 한다.
2.3.1 외부자 현황 관리	

2. 정보자산에 대한 식별 현황의 현행화 방안 도출

온-프레미스(on premises) 방식의 정보자산 식별에 상대적으로 익숙한 인증 심사원들은 하이퍼스케일 클라우드 환경에서 자산의 변화가 빈번하고, 많은 운영 툴의 도입환경에 대한 환경에 대한 변화에 익숙하지 않다은 경향이 있다. 이로인해, 목록으로 제출된 리스트에표기가 누락된 자산에 대하여 결함으로 지적하는 사례가 다수 발견된다. 하이퍼 스케일 클라우드 환경은 전체의 모든 자원 및 흐름을 한눈에 파악하기에 용이하지 않다. 반면에, 글로벌 클라우드공급업체에서는 자동화된 자산의 식별을 위해 쿼리(Query)로 파악하여 케이스 별 문제점을 개선하는 것에 익숙하다. 모든 환경이 자동화 되어있고 자산의 변화가 지속적인 환경이 그 이유이다. 그러나, 현행 ISMS-P 제도에서는 데이터의 흐름이나 네트워크 접근 방법에 있어서도 흐름도를 가시적으로 제시하도록 한다. 자동화 된 환경에서 각 레이어(Layer) 별 데이터 흐름도를 빠짐 없이 문서로 제시하도록 하는 것에 대한 개선이 필요하다.

표 6. ISMS-P 위험관리 통제
Table 6. ISMS-P Risk Management Control

통제분야	상세내용
1.2. 위험관리	관리체계 전 영역에 대한 정보서비스 및 개인정보 처리 현황을 분석하고 업무 절차와 흐름을 파악하여 문서화하며, 이를 주기적으로 검토하여 최신성을 유지하여야 한다.
1.2..2 현황 및 흐름분석	

3. 법적 요구사항 준수를 유도하기 위한 현실화 방안 마련

개인정보처리방침에 대하여 고객의 개인정보에 대한 가시성을 확보해 주기위한 취지로 개인정보 처리 방침에 대한 표기 방식에 대한 지적이 인증심사 시 매년 발생한다. 그러나 글로벌 클라우드공급 업체의 책임공유모델(Sheard-Responsible Model)[7]에 따라 클라우드공급업체 자체는 고객의 데이터에 접근을 하거나 취급하는 일이 극히 제한적이다.

표 7의 법적 요구사항 준수여부를 연 1회 이상 정기적으로 검토하고 있는가에 대한 세부점검항목에 대하여 국내 법적 요구사항을 준수하는지에 대한 현 이슈 별 검토가 필요하지 단순 개인정보처리방침의 폰트나 원하는 배치에 대하여 지속적으로 결함으로 지적되는 것은 올바르지 않다.

표 7. ISMS-P 관리체계 점검 및 개선 통제
Table 7. ISMS-P Management System Review and Improvement

통제분야	상세내용
1.4 관리체계 점검 및 개선	조직이 준수하여야 할 정보보호 및 개인정보보호 관련 법적 요구사항을 주기적으로 파악하여 규정에 반영하고, 준수 여부를 지속적으로 검토하여야 한다.
1.4.1 법적 요구사항 준수 검토	

현재 ISMS의 법적 검토에 있어서 정보통신망법, 개인정보보호법, 클라우드 컴퓨팅법등이 주요 검토 대상이 된다. 글로벌 비즈니스에 있어서 전 세계 모든 나라에 특화된 법령을 모두 충족하기 위한 검토는 쉽지 않다. 현재 Microsoft는 표 8의 세부 법령에 대하여 매년 91개 이상의 자체 점검을 실시하고 있다. 법령에 대한 정합성을 고려하여 선택과 집중을 통해 감사시기에 주로 이슈가 되는 법령을 집중적으로 검토하여 한국법 준수 요구사항을 명확히 함으로써 세부 점검이 필요하다. 예를 들어, OpenAI의 등장으로 고위험 AI 시스템에 대한 법안이 등장하고, 편향이 개인의 건강, 안전에 영향을 미치거나 차별로 이루어질 수 있는 사항에서 클라우드 환경에

서 개발된 SaaS서비스에 대한 범용 AI와 고위험군에 대한 개인정보 및 각종 규제가 논의되고 있는 시기이다. 이러한 현안에 대하여 클라우드공급업체 측면에서 점검해야 하는 사항과 SME(Small and medium-sized enterprises) 를 위한 별도 통제 항목 마련이 시급하다. 또한, 해당되는 이슈의 인증시기라면 관련 법에 해당년에 집중적으로 점검하는 것이 필요하다. 많은 법을 점검의 범위로 두는 것 보다는 선택적으로 깊이 있는 인증 심사가 이루어지기 위해서는 법적 요구사항에 대한 보다 상세한 검토가 이루어지도록 통제항목 개선이 필요하다.

표 8. 클라우드 사업자의 주요 요구사항 점검 법령
Table 8. Legislation key requirements for cloud providers

법령명	개정일자
정보통신망법	[시행 2021. 12. 9.] [법률 제18201호, 2021. 6. 8., 일부개정]
(개인정보보호위원회) 개인정보의 기술적·관리적 보호조치 기준	[시행 2021. 9. 15.] [개인정보보호위원회고시 제2021-3호, 2021. 9. 15., 일부개정]
개인정보 보호법	[시행 2020. 8. 5.] [법률 제16930호, 2020. 2. 4., 일부개정]
개인정보 보호법 시행령	[시행 2022. 10. 20.] [대통령령 제32813호, 2022. 7. 19., 일부개정]
(개인정보보호위원회) 개인정보의 안전성 확보조치 기준	[시행 2021. 9. 15.] [개인정보보호위원회고시 제2021-2호, 2021. 9. 15., 일부개정]
(개인정보보호위원회) 표준 개인정보 보호지침	[시행 2020. 8. 11.] [개인정보보호위원회고시 제2020-1호, 2020. 8. 11., 제정]
클라우드컴퓨팅법	[시행 2020. 12. 10.] [법률 제17344호, 2020. 6. 9., 타법개정]
클라우드컴퓨팅법 시행령	[시행 2020. 12. 10.] [대통령령 제31221호, 2020. 12. 8., 타법개정]

V. 결 론

데이터를 클라우드 환경으로 이전하면 모든 자원에 대한 가시성 제공이 가능하기 때문에 데이터 거버넌스가 강화되고, 비즈니스 핵심으로서의 보안성 담보가 가능하다. 또한, 복원력 및 복구 가능성 기반의 설계가 가능하기 때문에 하이퍼스케일 클라우드로 주요 국가 기반시설이 지정 운영되고 있다. 국내는 정보보호 및 개인정보보호 관리체계 인증제도가 융합화, 고도화되고 있는 침해위협을 효과적으로 대응[5]할 수 있도록 기업의 정보보호 및 개인정보보호 수준 제고를 위해 기반시설 지정 운영에 사회 전반에 적용되고 있다.

본 논문에서는 하이퍼스케일 클라우드상 에서의 결함사항을 분석하고, 하이퍼스케일 환경과 ISO/IEC 27001 및 SOC 보안 국제 표준과의 정합성을 고려하여 보다 클라우드에 특화된 통제항목 개선방안을 제시하였다.

기술적 격차와 국내 현실에 맞는 통제항목의 개선을 위해서는 하이퍼스케일 클라우드의 결함사항을 분석함으로써 첫째, 클라우드 데이터센터 계약운영 주체별 관리적 세부 통제를 마련하였다. 둘째, 정보자산에 대한 식별 현황의 현행화 방안 도출하였다. 셋째, 법적 요구사항 준수를 유도하기 위한 현실화 방안 마련을 통해 하이퍼 스케일 클라우드 특화된 ISMS-P 통제항목 개선 방안을 수립하였다.

본 연구를 통해 현 ISMS-P 통제항목의 세부점검 항목으로 만으로는 검토하기 어려운 범위를 해소하고 국내 인증심사원의 인식제고에 기여 할 수 있다.

향후에는 본 연구에서 수립된 ISMS-P 통제항목 개선 방안을 기반으로 공공영역의 클라우드 보안인증제를 위한 통제항목을 연구하고자 한다.

References

[1] Miicrosoft, “Defending Ukraine: Early Lessons From the Cyber War” pp. 2, June 2022.

[2] John D. Moteff, “Critical Infrastructures: Background, Policy, and Implementation,” Congressional Research Service, June 2015.

[3] American Presidential directive PDD-63, which set up a national program of "CIP," https://fas.org/irp/offdocs/pdd/pdd-63.htm. May 1998.

[4] Samantha Lee, “The cloud-computing market is set to double to $116 billion by 2021 – these 3 charts show why that’s probably good news only for Amazon, Google, Microsoft, and Alibaba,” Business Insider, Nov 2018.

[5] Personal Information & Information Security Management System(ISMS-P) Guideline, Korea Internet & Security Agency, July 2107.

[6] Korea K-ISMS, Microsoft. https://learn.microsoft.com/en-us/azure/compliance/offerings/offering-korea-k-isms

[7] Could Shared Responsibility, Microsoft.

https://learn.microsoft.com/ko-kr/azure/security/fundamentals/shared-responsibility

[8] Moving forward: use of modern technologies in the judiciary, March 2023
https://rm.coe.int/0900001680aa97fe

[9] Dong Hyun Kim, Younho Lee, "A Study on the ISMS-P Accreditation Effect Using the Seven Threats of Security - Focused on Enterprise Size and Career", Journal of KIIT, Vol. 18, No. 4, pp. 109-119, Apr. 30, 2020.
DOI : 10.14801/jkiit.2020.18.4.10

저 자 소 개

신 용 녀(정회원)

- 1999년 : 숭실대학교 컴퓨터학사.
- 2001년 : 고려대학교 전산학 석사.
- 2008년 : 고려대학교 전산학 박사.
- 2002년 ~ 2009년 : 한국인터넷진흥원 연구원.
- 2010년 ~ 2014년 : 한양사이버대학교 컴퓨터학과 교수.
- 2015년 ~ 2018년 : 아마존 웹 서비스 기술이사.
- 2018년 ~ 현재 : 마이크로소프트 최고기술임원.