2016. 6. 9.

주요국 클라우드 보안 규정 동향

강송희
(dellabee@spri.kr)

SPRi 소프트웨어정책연구소

1. 주요국 공공부문 데이터 분류 기준

□ 미국 데이터 분류 기준

o 공공부문 데이터 분류 및 통제 기준이 '08년보다 간소화

- FedRAMP[1] 2.0·NIST[2] SP800-53 R3('14.6), DoD DISA CC SRG[3] ('15.1) 등에서 공공부문 데이터 통제 기준 갱신

* 기본적인 분류 및 통제 기준은 RA-2 Security Categorization, AC-4 Information Flow Enforcement를 따르며, 데이터 분류 기준은 FIPS 199분류에 준함

<미국 NIST 공공 부문 데이터 분류 기준>

보안 목표	잠재적 영향도		
	낮음(Low)	보통(Moderate)	높음(High)
기밀성	비인가된 정보 유출이 조직 및 국민에게 미미한(limited) 악영향을 미침	비인가된 정보 유출이 조직 및 국민에게 중대한(serious) 악영향을 미침	비인가된 정보 유출이 조직 및 국민에게 심각한(severe or catastrophic) 악영향을 미침
무결성	비인가된 정보의 수정 또는 파기가 조직 및 국민에게 미미한 악영향을 미침	비인가된 정보의 수정 또는 파기가 조직 및 국민에게 중대한 악영향을 미침	비인가된 정보의 수정 또는 파기가 조직 및 국민에게 심각한 악영향을 미침
가용성	정보의 사용이나 정보 시스템에 대한 접근이 제한될 때 조직 및 국민에게 미미한 악영향을 미침	정보의 사용이나 정보 시스템에 대한 접근이 제한될 때 조직 및 국민에게 중대한 악영향을 미침	정보의 사용이나 정보 시스템에 대한 접근이 제한될 때 조직 및 국민에게 심각한 악영향을 미침

(자료: NIST SP 800-60 Volume 1 Revision 1: Guide for Mapping Types of Information and Systems, '08.8)

1) Federal Risk and Authorization Management Program
2) National Institute of Standards and Technology
3) Department of Defence Defence Inforamtion System Agency Cloud Computing Security Requirement Guide

<미국 DoD DISA 클라우드 정보 분류 체계>

현재	기존	상세 내용	예시
2등급	1등급	공개 승인된 미분류 정보	
	2등급	통제되지 않는 미분류 정보	
4등급	3등급	통제되는 미분류 정보	
	4등급	통제되는 미분류 정보	수출 통제(무기, 라이선스, 핵기술 정보) 개인정보(식별 정보 포함), 민감한 의료 정보, 핵심 인프라 정보, 민감한 보안 정보, 법적 통제 정보 등
5등급	5등급	통제되는 미분류 정보	국가 보안 시스템(NSS, National Security Systems)
6등급	6등급	기밀로 분류된 정보	

(자료: 美 DISA DoD(2015.1), Cloud Computing Security Requirements Guide)

□ 영국 데이터 분류 기준

o 영국 정부는 클라우드 시대에 맞는 신규 데이터 분류 기준을 발표('14.4)하였으며, 90%이상이 OFFICIAL기준에 해당하여 클라우드로 이관 가능(Diginomica, '14)

<영국 공공 부문 데이터 분류 기준>

구분	데이터 분류		
	OFFICIAL	SECRET	TOP SECRET
정의	일반적인 공공부문 사업, 서비스 관련 정보로서 유출 및 훼손, 파기시 미미한 악영향	민감한 정보로서 유출 및 훼손, 파기시 군 역량에 중대한 악영향	가장 민감한 정보로서 유출 및 훼손, 파기시 안보, 경제에 심각한 악영향을 미치고 인명 손실을 일으킬 수 있음
베이스라인 보안 목표	조직원 각각이 보안 책임	합리적 보안 장치 및 절차 구비	견고한 보안 장치 및 절차 구비
표시	명시적인 표시 의무 없음	명시적인 표시 의무	명시적인 표시 의무

(자료: UK Cabinet Office: Government Security Classifications, '14.4)

2. 주요국 공공부문 클라우드 보안 요구사항

□ 미국 공공부문 클라우드 보안 요구사항

o 미국 국방부(DoD, Department of Defence) 클라우드 요구사항에 따르면 최상위 등급인 5·6급 정보는 타 고객과 물리적 분리 필수

- 하위 등급인 2·4급 정보는 논리적 분리가 필수
- 모든 정보는 미국 법적관할 내에서 보관해야 함

□ 영국 공공부문 클라우드 보안 요구사항

o 영국 중앙 정부, 영국 지자체, 대학 및 자선 단체 등 공공부문에서 사용하는 클라우드는 논리적 분리가 최소 보안요구사항임

- 영국 중앙 정부의 경우 영국 공공부문의 네트워크인 PSN(Public Services Network)을 통해 접속
- 영국 지자체, 대학 및 자선 단체에서 사용하는 클라우드는 유럽 내에 위치해야 하며 SSL/VPN으로 접속 가능

<英·美 공공 부문 클라우드 최소 보안 요구사항 비교>

요구사항	美5·6등급	英 중앙부처	美2·4등급, 英지방정부 ·공공기관
SaaS 99.9% 가용성 보장	○	○	○
SSL/VPN 사용	○	○	○
재해 복구(이중화, 백업, 재해복구센터)	○	○	○
전담 보안팀 구성	○	○	○
탄력성, 온디맨드 확장성	○	○	○
고객 포털 - 과금 포함 운영 투명성	○	○	○
전용(Dedicated) 서버군	○	○	○
직원 보안 통제사항	○	○	○
정보자원의 논리적 분리	○	○	○
정보자원 물리적 분리	○		
중앙행정기관 전용 네트워크 연결		○	

(자료: 오라클 백서, DISA, NIST 자료 재가공, '14.9)

3. 시사점: 정보 분류·최소 요구사항에 따른 다수준 보안

□ 정보 분류와 보안 최소 요구수준에 따른 합리적인 다수준 보안 체계 필요

o 일괄 보안은 보안위협의 원천봉쇄와 관리정책의 단순화가 장점이나 성능 및 편의성의 저하와 비용 증가 등을 감수해야 함

o 다수준 보안은 지능형·적응형 관리 정책이 필요하나 민감한 정보와 시스템에 대한 선택과 집중을 통해 성능·편의성 향상과 비용 절감

<클라우드 내 다수준 보안 시스템 예시>

정보자원 분류		1계층		2계층	3계층
민감도		높음		중간	낮음
보안수준		높음		중간	기본
접근제어 (운영·인증)	읽기	3요소 인증 (예: 암호, 보안토큰, 생체인식보안)		2요소 인증 (예: 암호, 보안토큰)	1요소 인증 (예: 암호 또는 개인식별번호)
	쓰기	3요소인증+서명+OTP		2요소인증+서명	1요소인증+서명
암호화	구분	일반	민감	전부	전부
	알고리즘	단순 암호화 (대칭 치환)	산업표준 (AES, RC4)	산업표준 (blowfish)	단순암호화 (대칭치환)

자료: Dorairaj and Kaliannan('15)

OPEN 공공누리 공공저작물 자유이용허락 출처표시 상업용금지 변경금지

이 저작물은 "공공누리" 출처표시-상업적이용금지-변경금지 조건에 따라 이용할 수 있습니다.