KISTI 마이데이터 플랫폼 내 개인정보처리시스템의 보안 진단 방안에 관한 연구

강남규, 이만희*

한국과학기술정보연구원, *한남대학교

ngkang@kisti.re.kr, *manheelee@hnu.kr

A Study on Security Assessment Measure for Personal Data Processing Systems in the KISTI MyData Platform

Kang Nam Gyu, Lee Man Hee*

Korea Institute of Science & Technology Information, *Hannam University

요 약

KISTI는 데이터 기반의 지역사회 현안 해결을 위해 활용하는 데이터의 범위를 과학기술데이터에서 마이데이터로 확대하고 있으며, 이를 위해 마이데이터 플랫폼을 구축하여 운영하고 있다. 이 플랫폼을 통해 다양한 마이데이터 실증서비스를 추진하고 있으며, 대전시 임산부 이동지원서비스 '무브메이트'처럼 실증 이후에 지자체의 정식 서비스로 확장된 성과도 나타나고 있다. 마이데이터플랫폼 내에 개인정보가 축적되면서 개인정보 보호 및 개인정보처리시스템에 대한 보안 중요성이 점점 더 부각되고 있으며, 이에 대한 보안 진단과 개선 방향 도출이 핵심 과제로 떠오르고 있다. 본 연구에서는 KISTI 마이데이터 플랫폼 내에서의 개인정보처리시스템에 대한 보안 진단 방법과 절차를 제시하고, 이를 통해 보안 수준을 체계적으로 점검·강화하기 위한 방안을 제안한다.

Ⅰ. 서 론

KISTI는 데이터 기반의 지역 현안 해결을 위해 활용하는 데이터의 범위를 과학기술데이터에서 마이데이터로 확대하고 있으며, 마이데이터 플랫폼의 구축 및 운영은 물론, 현안 해결을 위한 다양한 실증서비스를 개발하고 있다. 예를 들어, 대전시 임산부 이동지원 실증서비스인 '무브메이트'의 경우, 대전 거주 임산부의 개인정보와 택시 결제 정보 등의 마이데이터를 활용하여 대전시의 정책적 고민을 해결하였으며, 현재는 시의 정식 서비스로 운영되고 있다. 무브메이트의 월간 이용률은 기존의 '사랑나눔콜' 서비스와 유사한 수준을 기록하고 있어, 대전시의 임산부 이동지원 체계가 이원화된 구조로 안정적으로 정착된 것으로 평가할 수 있다.

무브메이트를 통해 수집된 개인데이터는 KISTI 마이데이터 플랫폼에 저장되어 처리되고 있다. 플랫폼 내에서 개인데이터가 지속적으로 축적됨에 따라 개인정보 보호 및 개인정보처리시스템에 대한 보안의 중요성이 점점 더 부각되고 있다. 또한 정부의 개인정보보호법과 개인정보의 안전성 확보 조치 기준 등의 관련된 법령 및 현행 규칙에 따라 안전한 개인정보 처리가 요구되고 있으며 암호화 등의 기술적 보호 조치 이행이 의무화되고 있다. 더불어 개인정보 유출과 도난 방지 등을 위해 취약점 점검을 포함하여 내부 관리 계획을 수립하고 시행하는 것이 법적으로 요구되고 있다.

이에 따라, 개인정보를 다루는 KISTI 마이데이터 플랫폼의 보안 수준을 체계적으로 점검하고, 개인정보 보호를 위한 관리 계획 수립과 기술적·관리적 조치를 수립할 필요가 있다. 본 연구에서는 플랫폼 내에서의 개인정보처리시스템에 대한 보안 진단 방법과 절차를 제시하고, 이를 통해 보안 수준을 체계적으로 평가·강화하기 위한 방안을 제안하고자 한다.

Ⅱ. 보안 진단 절차

1. 보안 진단 개요

KISTI 마이데이터 플랫폼에서는 개인정보를 주로 처리하므로 이를 안전하게 보호하는 것이 중요하다. 이를 위해 전송 구간 암호화나 데이터베이스 암호화를 통해 개인정보를 안전하게 저장하고 전송할 수 있는 등의 방안은 이미 적용되어 있지만, 플랫폼과 실증서비스 구축과 운영 환경에서의 보안과 정보보호가 더 요구된다. 또한 최근 급증하는 공급망 공격에 대응하기 위해 상용 SW를 비롯하여 오픈소스 SW까지 공급망 보안에 대한 점검도 필요하다.

본 연구에서는 개인정보 암호화에 대한 점검 방안, 시스템 취약점 점검과 조치 등의 시스템 보안 강화 방안, 마이데이터 플랫폼에 설치된 SW에 대한 공급망 보안 위협 요소를 분석하여 보안을 강화하는 방안에 대해서 살펴보고자 한다.

2. 개인정보 암호화

개인정보에 대한 암호화를 위해서는 암호화 대상을 식별하고 식별된 대상을 어느 수준으로 암호화할 것인가를 결정하는 것이 중요하다. 이를 위해 개인정보의 안정성 확보조치 기준, 암호 알고리즘 및 키 길이 이용 안내서 등 개인정보보호위원회나 한국인터넷진흥원의 법령이나 행정규칙 등의 관련 자료 분석이 선행되어야 한다. 또한 개인정보처리시스템에 적합한 암호 알고리즘에 대한 조사도 필요하다.

개인정보보호위원회의 개인정보의 안전성 확보조치 기준 안내서(2024.10)에 따르면 그림 1과 같이 인증정보에 대한 저장/송·수신시 암호화, 개인정보의 저장/송·수신시 암호화 등에 대한 내용을 각각 구분하여 안내하고 있다. 관련 안내서를 참고하여 플랫폼 내에서 개인정보 대상 암호화 항목을 파악하고, 항목별 암호 알고리즘 선정도 선정한다. 암호화 알

고리즘은 국가정보원의 검증대상 암호 알고리즘 및 검증필 암호 모듈 사용을 해야하며, 관련 알고리즘의 안전성 유지기간은 표 1과 같다.

구분		「개인정보 보호법」에 따른 암호화 대상 개인정보	
		이용자가 아닌 정보주체	이용자
정보통신망을 통한 송·수신 시	인터넷망	개인정보	
	정보통신망	인증정보(비밀번호, 생체인식정보 등)	
저장 시	저장 위치 무관	주민등록번호	
		인증정보(비밀번호, 생체인식정보 등) ※ 단, 비밀번호는 일방향암호화	
		-	여권번호, 운전면허번호, 외국인등록번호, 신용카드번호, 계좌번호, 생체인식정보
	인터넷망 구간, DMZ	고유식별정보	-
	내부망	고유식별정보 ※ 단, 주민등록번호 외의 고유식별정보를 저장하는 경우에는 영향평가 또는 위험도 분석을 통해 암호화 적용여부 및 범위를 정할 수 있음	
개인정보취급자 컴퓨터, 모바일기기, 보조저장매체 등에 저장 시		고유식별정보, 생체인식정보	개인정보

(그림 1) 개인정보 암호화 적용 기준 요약

(표 1) 암호화 알고리즘 안전성 유지기간

보안 강도	대칭키암호 알고리즘 (보안강도)	해시함수 (보안강도)	공개키 암호 알고리즘				암호 알고리즘 안전성 유지기간 (년도)
			인수분해 (비트)	이산대수		타원곡선 암호 (비트)	
				공개키 (비트)	개인키 (비트)		
112 비트	112	112	2048	2048	224	224	2011~ 2030년
128 비트	128	128	3072	3072	256	256	2030년 이후
192 비트	192	192	7680	7680	384	384	
256 비트	256	256	15360	15360	512	512	

3. 시스템 보안 강화

마이데이터 플랫폼 내 보안 취약점 점검 및 조치를 위해 진단 도구를 활용하여 시스템내 소프트웨어의 취약점을 점검하고 침투 테스트 도구를 활용하여 외부 공격 가능성까지도 점검할 필요가 있다. 개인정보의 안전성 확보조치 기준 등의 관련 문서 분석을 통해 접근 권한 및 접근 통제 기준을 파악하고, 인증 및 권한 관리 방안과 절차를 제시해야 한다. 또한 접근 시 기록되는 로그와 이를 모니터링할 수 있는 체계까지도 구축되었는지 확인과 점검이 필요하다. 취약점 점검과 조치에 관련된 기술문서들은 다음과 같다.

- 개인정보의 안전성 확보조치 기준(개인정보보호위원회)
- 공개SW를 활용한 소프트웨어 개발보안 점검 가이드(행정안전부)
- 소프트웨어 보안약점 진단가이드(행전안전부)
- 소프트웨어 개발보안 가이드(행정안전부)
- 주요정보통신기반시설 기술적 취약점 분석, 평가 방법 상세가이드(과학기술정보통신부)

또한 취약점 점검은 웹 취약점과 시스템 취약점을 분리하여 각각에 적합한 취약점 진단도구를 활용해야 한다. 취약점 진단과 Nmap, Sqlmap, ZAP, Cooxie, Wireshark 등을 활용할 수 있으며 침투 테스트를 위해서 Havij, Burp Suite, Recon-ng 등을 활용할 수도 있다.

4. SW 공급망 보안 관리

소프트웨어의 설계, 개발, 배포, 유지보수의 전과정에서 사용되는 부속 소프트웨어 및 관리 체계를 통칭하여 SW 공급망이라고 정의하며, 상용 또는 오픈소스 SW가 공급되면서 공급과정에서 발생하는 해킹, 침투, 변조, 악성코드 삽입 등과 같은 각종 보안 위협을 공급망 위협이라고 한다. 마이데이터 플랫폼의 정보보호를 위해 사용중인 여러 SW에 대한 공급망 보안 위협 요소를 분석하고, SBOM(Software Bill of Materials) 등의 관리 체계가 필요하다. 플랫폼과 연계된 제3자(외부서비스, 공개SW, 협력업체 등)로부터 발생할 수 있는 공급망 보안 위협을 식별하고 평가하여 이를 예방하기 위한 제도적, 기술적 방안을 수립하기 위해서 표 2와 같이 4단계 관리 체계를 제안한다.

(표 2) 공급망 보안 위협을 예방하기 위한 제도·기술적 관리 체계

단계	내용
(1단계) 서드파티 위험 평가 체계 구축	- 서드파티 범위 정의(외부서비스, 공개 SW, 협력업체 등) - 서드파티 위험 평가 항목 및 기준 정의 (보안 취약점, 법규 준수 등) - 위험 평가 절차 및 방법론 도출
(2단계) 서드파티 공급망 보안 위험 평가	- 외부 연계 서비스/시스템에 대한 공급망 위험 분석 - 외부 업체와 체결된 계약/SLA 내 보안 요구 사항 준수 여부 검토 - 서드파티 및 공급망 위험에 대한 종합적 위험 대응 전략 수립
(3단계) SW 공급망 보안 SLA 기준 도출	- SW 개발, 운영, 유지보수 단계별 보안 SLA 항목 정의 - SLA 측정 및 평가 방법 제시 - SLA 미준수 시 제재 방안 및 계약 해지 조건 명시 등
(4단계) 공급망 보안 모니터링 및 감사 체계 설계	- 서드파티 보안 취약점 정보, 보안 업데이트 현황 등 지속적인 모니터링 체계 구축 - 주기적인 공급망 감사 계획 수립 - 감사 결과 기반 재선 조치 및 재평가 프로세스 정의

플랫폼 내의 관리 대상 시스템과 SW를 효과적으로 관리하기 위해 SBOM을 도입할 필요가 있다. SBOM은 소프트웨어 구축에 사용되는 다양한 구성요소의 세부 정보와 공급망 관계를 목록화한 문서로써, 플랫폼 내의 관리 대상 자산을 정의하고 이를 토대로 SBOM으로 관리할 수있다. SBOM에는 버전 업데이트와 패치 적용 현황을 추적하고 취약점 정보를 공유할 수 있는 체계가 정의된다. 또한 변경 이력 관리 프로세스와 취약점 위험도 평가 방식도 정의되어 공급망 내 보안 사고시 원인 분석과 복구를 위한 협업 구조까지도 구성할 수 있다. 결과적으로 SBOM을 통해 관리 대상 시스템에 적용된 SW와 구성요소의 취약점을 실시간으로 식별하고 대응까지 가능하다.

Ⅲ. 결론

최근 국내 대형 통신사에 대한 해킹 공격으로 개인정보가 유출되는 사고가 있었다. 개인정보보호에 대한 중요성이 더욱 커져가는 상황에서, KISTI 마이데이터 플랫폼 내에서 개인정보처리시스템에 대한 보안 진단 방법과 절차가 정의되고, 보안 수준을 체계적으로 점검하기 위한 방안 마련과 실행이 반드시 필요하다.

ACKNOWLEDGMENT

이 논문은 2025년도 한국과학기술정보연구원(KISTI)의 자체연구사업으로 수행한 연구입니다. ((KISTI) J25JR001-25, KISTI 마이데이터 플랫폼 구축, 운영 및 실증 확대)

참 고 문 헌

[1] KISTI 마이데이터 플랫폼, https://mydata.kisti.re.kr

[2] 개인정보보호위원회 개인정보의 안전성 확보조치 기준 안내서, https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS217&mCode=D010030000&nttId=10719

[3] 김광준, “소프트웨어 공급망 관리를 위한 글로벌 솔루션 동향”, 정보보호학회지, v32 no.5, pp.27-34, 2022