

지능형 해상교통정보 연계시스템에서의 개인정보 보안에 관한 연구

송용학* · 김현* · 조득재** · 백종화** · † 김도연

*, † (주)지엠티 기술연구소, **선박해양플랜트연구소

A Study on Privacy Security in Maritime Information Gateway System

Yong-hak Song* · Hyun Kim* · Deuk-Jae Cho** · Jong-Hwa Beak** · † Do-yeon Kim

*, † GMT Co., Ltd., Seongnam-si, 13486, Korea

**Korean Research Institute of Ships & Ocean engineering, Daejeon, 34103, Korea

요 약 : 해양수산부는 지능형 해상교통정보 체계 운영을 통해 해사안전 서비스를 제공 중이며, 제공 중인 서비스의 경쟁력 확보를 위한 신뢰성 및 품질 향상 연구가 지속적으로 필요한 상황이다. 이러한 경쟁력 확보를 위해, 지능형 해상교통정보 체계의 실시간 운영 영향을 최소화하는 대용량 해양정보 연계 시스템에 대한 기본설계를 수행하고, 개인정보 보안 문제와 전체적인 시스템 실현을 위해 가명화/암호화 절차가 적용된 이론적 하드웨어 구조도를 제시한 바 있다. 하지만 제시한 구성도 및 설계는 전체적인 개념만을 포함하며, 실제 사용되고 있는 실시간 해양정보 연계를 위해서는 대한민국의 개인정보 보호법을 만족할 수 있는 상세한 개인정보 보안 방안이 요구된다. 이 연구는 이러한 문제의 해결을 위해 지능형 해상교통정보 연계 시스템에서 연계하는 실시간 해양정보 내에서 개인정보 보호법을 침해할 수 있는 요소(선주, 선사, 선장, 항해사, 어민 등의 개인정보)를 식별하고, 식별한 개인정보를 가명화/암호화하여 타 기관으로 연계할 수 있는 방법을 연구한다.

핵심용어 : 지능형 해상교통정보 체계, 대용량 해양정보, 연계 시스템, 개인정보 보호법, 개인정보 보안

Abstract : The Ministry of Oceans and Fisheries is providing maritime safety services through the operation of the Korean e-Navigation service, and research is continuously needed to improve reliability and quality to secure the competitiveness of the system. In order to secure such competitiveness, we presented the basic design for the big-data maritime information gateway system for minimizes the real-time operation impact of the Korean e-Navigation service, and a theoretical hardware structure diagram including pseudonymization procedures to implement the overall system and solve privacy security issues. However, the proposed structure diagram and design include only the overall concept, to link real-time maritime information, required detailed privacy security method to satisfy the Privacy Act of the Republic of Korea. To solve this problem, this study will identify factors to violate the Privacy Act within the real-time maritime information(privacy of shipowner, shipping company, captain, navigator, fisherman, etc.) linked by the big-data maritime information gateway system, and research the method to link the secured information to other institutions by encrypting identified the factors.

Key words : Korean e-Navigation service, Maritime big-data, Gateway System, Privacy Act, Privacy Security

1. 서 론

해양수산부는 지능형 해상교통정보 체계(해상교통정보시스템, Korean e-Navigation Service) 운영을 통해 해사안전서비스를 제공 중이며, 서비스의 신뢰성 및 품질 향상을 위한 지속적인 연구가 필요하다(한국형 e-Navigation 사업단, 2020).

이러한 신뢰성 및 품질향상을 위한 요구와 타 유관기관의 정보연계에 대한 요구를 만족하기 위해, 지능형 해상교통정보 체계의 실시간 운영 영향을 최소화하는 대용량 해양정보 연계 시스템에 대한 설계와 이론적 구조도를 제시한 바 있다(송용학 외 2인, 2022).

하지만, 실제 사용되고 있는 실시간 해양정보 연계를 위해서는 대한민국의 개인정보 보호법(개인정보 보호법, 2020)을 만

족할 수 있는 상세한 개인정보 보안 방안이 요구된다.

이 연구는 지능형 해상교통정보 연계 시스템에서 연계하는 실시간 해양정보 내에서 개인정보 보호법을 침해할 수 있는 요소(선주, 선사, 선장, 항해사, 어민 등의 개인정보)를 식별하고, 식별한 개인정보를 가명화/암호화하여 타 기관으로 연계할 수 있는 실제 시스템 결과를 보일 예정이다.

2. 대용량 해양정보의 개인정보보호 취약점식별

2.1 지능형 해상교통정보 체계의 개인정보보호 필요필드

지능형 해상교통정보 체계는 AIS, V-Pass, LTE-M 선박정보(위치, 정적) 및 각종 타 기관 연계정보 DB와 Join되어

† 교신저자 : 정희원, dykim@gmtc.kr
* 정희원, (yongdak, kihy)@gmtc.kr
** 정희원, (djcho, jhbeak)@kriso.re.kr

통합선박정보 서비스를 관리하는 통합 DB, 그리고 각각의 해사서비스를 제공하는 서비스DB들로 구성되어있다. 그 중 개인정보 보호법 제2조 1항에 의거하여 개인이 식별될 수 있는 정보로 선박NO, 선박ID, 선박GPS위치정보, 신호포판번호, 선박명(한, 영), 선박원부, IMO번호, CALLSIGN, 선박코드, MMSI, 고유번호, RFID, MRN, MRN_SN, 검사원명 등이 식별된다.

2.2 가명화/암호화 알고리즘 적용

가명화/암호화 알고리즘은 단방향 알고리즘과 양방향 알고리즘으로 구분되지만, 지능형 해상교통정보 연계시스템의 경우 개인정보 보호법 28조2의 ①에 의거하여 가명정보의 처리에 관한 특례를 적용받는 사항이므로 동조 ②에 의거하여 가명정보를 제3자(타 기관)에게 제공할 경우 특정 개인이 식별될 수 없어야 한다. 이에 따라 복호화가 가능한 양방향 알고리즘은 적용이 불가능하므로 단방향 알고리즘인 MD5, 혹은 SHA 알고리즘을 사용하여야 한다.

또한, MD5 알고리즘과 SHA0, SHA1은 현재 보안관련 용도로 사용이 권장되지 않으므로 Fig. 1에서 보이는 SHA2-256을 적용하여 가명화/암호화를 진행한다.

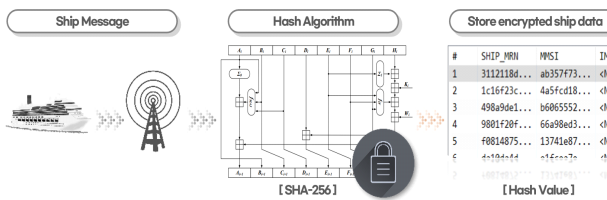


Fig. 1 The SHA2-256 Algorithm for the B-mIGS

3. 보안 처리된 지능형 해상교통정보 연계 시스템

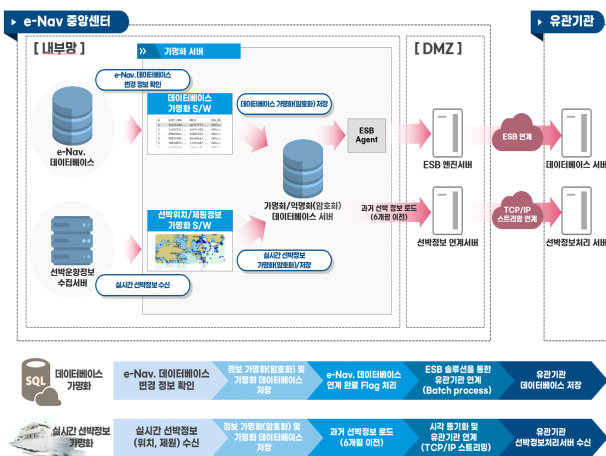


Fig. 2 The security-processed flow for the B-mIGS

보안 처리된 지능형 해상교통정보 연계 시스템은 해양수

산부에 존재하는 원본 데이터에서 보안처리 대상과 아닌 나머지 데이터를 구분하고, 가명화 SW를 통해 보안처리 된 별도 DB로 데이터 이관을 수행한다. Fig. 2에서 보인 이러한 보안 과정을 통해 유관기관은 가명화 된 DB로만 접근이 가능하며, 유관기관으로의 데이터 연계결과는 Fig. 3에서 보인다.

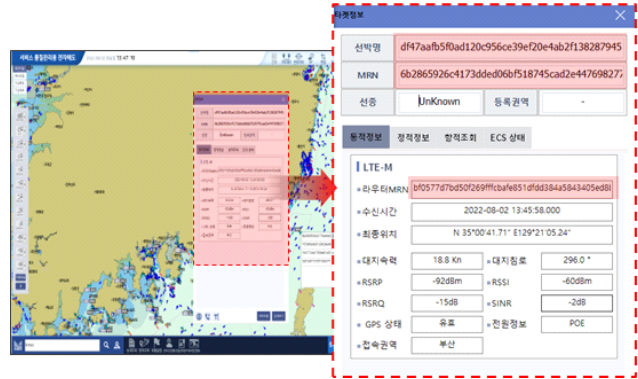


Fig. 3 The result after data encryption

4. 결 론

이 연구는 지능형 해상교통정보 체계의 DB데이터 중에서 개인정보 보호법을 침해할 수 있는 정보를 식별하였으며, 개인정보 보안을 위한 알고리즘 선택과 그 알고리즘의 순서도 및 가명화/암호화 적용 결과를 보였다.

해사 개인정보 보호 및 암호화 알고리즘 적용 결과는 바다 국민의 개인정보를 보호함으로써 자유와 권리를 보장하며, 연구원들의 연구윤리 확립으로 건강한 생태계를 확보할 수 있다.

본 연구는 개인정보의 가명화/암호화를 수행한 데이터 연계 결과를 보였으나 유관기관에서 해당 데이터를 통한 연구개발 시 분석대상 선박의 추적성 관리 등에 어려움이 있기 때문에 이러한 문제 해결이 추후 연구과제로 남는다.

감 사 의 글

* 본 논문은 해양수산부와 해양수산과학기술진흥원의 지원을 받아 수행하는 '지능형 해상교통정보 서비스 기반의 해상 디지털 정보활용 기술개발'에 의해 수행되었습니다.

참 고 문 헌

[1] 한국형 e-Navigation 사업단(2020), 해사안전 스마트화를 위한 해사디지털 기술개발전략 기획보고서

[2] 송용학, 김현, 김도연(2022), "유관기관 정보 공유를 위한 지능형 해상교통정보 체계의 대용량 해양 정보 연계 시스템 기본 설계에 대한 연구", 한국해양학학회 학술대회논문집 2022.6, pp. 308-309.

[3] 개인정보 보호법(2020), 대한민국 법률 제16930호, 2020.2.4.