2019년 한국항해항만학회 추계학술대회
2019년 11월 20일(수)~21(목) 부산항국제전시컨벤션센터

VTS 및 소형선박 항해장비의 항적추출을 통한 디지털 포렌식 절차 및 모델서비스

† 이병길 · 최병철*

*,† 한국전자통신연구원

A Digital Forensic Procedure and Service of Ship with VTS and Navigation Device

† *Byung-Gil Lee · Byeong-Chel Choi**

**,† ETRI, 161 Gajeong-dong, Yuseong-ku, Daejeon 305-345, Korea*

요 약 : VTS 관제시스템에서 선박 사고로서 재난 수준으로 발생되는 경우, 사고의 수사과정에서 선박의 사고 상황에 대한 철저한 분석이 이루어져야 한다. 하지만 VTS 시스템에서 레이더 관제 범위내에 있는 경우와 선박의 AIS 신호가 정상적으로 잘 수신되는 경우는 위치정보를 추출하여 선박의 사고원인 파악이 가능하다. 하지만 그 이외의 경우로서 선박에서 송신하는 정보가 정상적으로 수신되지 못하는 경우 또는 관제 범위를 벗어나는 경우는 수사과정은 어려움에 봉착한다. 이러한 상황에서는 선박의 항해 장비를 이용한 선박의 항적 조사가 매우 중요하다. 즉, VTS 에서 항적 수집이 되는 경우에도 선박 자체의 항적 정보가 추출이 되는 경우 더욱 정확한 사고분석이 가능하기 때문이다. 본 논문에서는 항적 추출이 가능성이 있는 선박의 항해장비의 종류와 특징 그리고 포렌식을 적용하는 절차에 대하여 조사하였다. 이러한 정보는 향후 국내 발생되는 국가적 재난 수준의 해양사고에 대하여 수사와 분석에 도움을 주며, 해외에서 발생되는 국내 선박과 연관된 사고나 국내 여행객이 탑승한 해외의 대형 해양 사고의 조사, 분석에 전문가로서 파견 활동하는데 도움을 줄 수 있다.

핵심용어 : VTS, e-Navigation, PortCall 도선, ETA

Abstract : *In the VTS, the predictions of vessel mobility and situation awareness of maritime environment are basic function. In recent years, pilotage information is an essential aware element of VTS personnel for vessel traffic management. So, we designed the structure of pilotage information service with VTS and tested in real environment. In the future, similar pilotage information can be used as a useful VTS service.*

Key words : *Digital Forensic, VTS, Voyage*

1. 서 론

국내 발생된 대형 선박 사고는 70년 남영호 침몰사고, 93년 서해 훼리호 침몰사고, 07년 허베이 스피리트호 기름 유출 사고, 14년 세월호 침몰사고, 17년 스텔라데이지호 사고, 19년 현대글로비스 골든 레이호 사고 등 이 존재한다. 특히 국내 5년간 해양사고 발생 추이를 보면 매년 지속적으로 증가 추세이며 인적 물적 사회적 비용이 수반되어지므로 피해는 커지는 추세이다. 선박 등록 척수 기준으로 18년 3.8%에 해당되며, 소형선박(어선 등)이 전체 사고의 80% 정도 수준(재결분기준)이다. 이러한 선박의 사고형태를 보면 충돌사고가 가장 많은 비중이며, 접촉, 좌초, 전복, 침몰 등 이며, 원인은 운항과실이 주된 원인이 된다. 운항과실의 종류는 아래와 같은 원인이 주된 세부 원인이다.

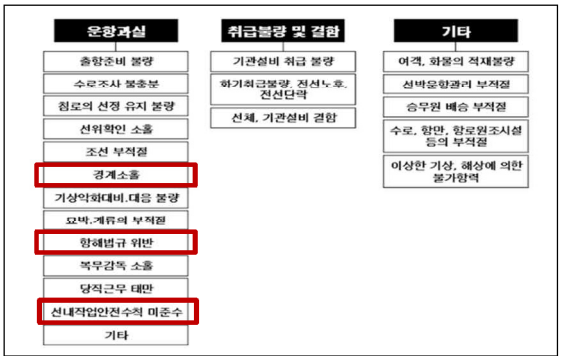

Fig. 1 운항과실의 종류

† 정회원, bglee@etri.re.kr

현재까지 해양사고에 대한 수집 및 분석 체계에 대하여는 해양경찰청, 해양수산부, 해양안전심판원 등에서 사고관련 자료를 각자 별도로 정리하고 있으며, 공유 체계 또한 없다.

그리고 표준화된 사고 분석 데이터베이스로 되어 있지 않으며, 개별수집유지에 따라 통합관리가 되지 못하며, 단순한 통계 현황은 파악할 수 있으나, 사고 원인분석을 체계적으로 하기 어려운 수준이다. 또한 사고 현장에서도 포렌식에 대한 체계가 없어 사고후 VTS 장비에 의존하여 육상 수집된 자료위주로 해결하고 있다. 이러한 체계로 사고 후 고의 자료 삭제, 침수, 전원 Off로 인해 증거자료 제거되어 사건 해결이 어려운 사건도 많이 발생되어 사고에 대한 효과적인 절차와 체계를 파악하고자 한다.

2. VTS 관제시스템을 이용한 사고 분석 및 디지털 포렌식

현재까지 해양사고의 분석은 관제시스템에서 항적 데이터 추출을 통하여 선박정보와 환경정보 등을 적용한 시험분석보다는 관제시스템의 재생화면에서 동영상 저장(또는 화면저장) 수준으로 이루어진 단순 저장화면의 분석만이 진행되어 왔다.

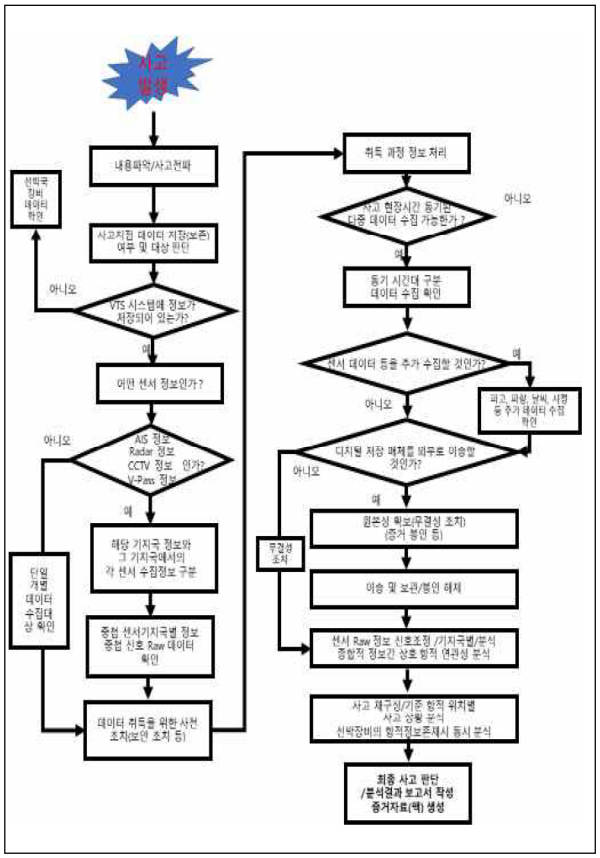

Fig. 2 VTS 관제시스템을 통한 해양사고 디지털포렌식 절차

즉, 사고 현장에서 선박이 송신한 VTS에서 수신된 AIS 정보와 레이더 위치 정보, 융합된 데이터 항적 정보의 세부적인 항적 정보를 통하여 종합적 분석 검증과정은 쉽지 않다. 이는 VTS 장비 자체가 필요한 정보를 추출하기 쉬운 형태가 아닌 외산 메이커 장비이며, 음성교신정보, 위치정보, 선박 COG, SOG 등 다양한 정보로 재구성할 수 있는 형태의 세부적 데이터가 주어지지 않기 때문이기도 하다.

즉, 정확한 사고분석을 위하여는 단순 재생화일이 아닌 추가적 처리된 정보가 요구된다.

레이더 정보인 경우를 예로 들면, 기존 관제사가 보는 정보에서 좀 더 신호처리가 덜 가미된 로우 데이터 정도를 다양한 형태로 변경하고, 분석하는 기법과 중첩된 레이더중에 레이더의 각도에 따라 선박이동 형태가 더 정확하게 볼수 있는 특정 레이더 사이트 정보를 가미하여 보는 것이 필요하다.

본 논문에서는 관제시스템을 통하여 사고 분석하는 포렌식 모델과 절차를 그림 2와 같이 설계하였다.

3. 선박 탑재한 항해 장비를 이용한 사고 분석 및 디지털 포렌식

VTS 시스템에서 데이터 수집이 용이 하지 않은 경우가 존재할 수 있다. VTS 시스템에서 레이더 관제 범위 내에 있는 경우와 선박의 AIS 신호가 정상적으로 잘 수신되는 경우는 위치정보를 추출하여 선박의 사고원인 파악이 가능하다.

하지만 그 이외의 경우로서 선박에서 송신하는 정보가 정상적으로 수신되지 못하는 경우 또는 관제 범위를 벗어나는 경우는 수사과정은 어려움에 봉착한다. 이러한 상황에서는 선박의 항해 장비를 이용한 선박의 항적 조사가 매우 중요하다. 즉, VTS 에서 항적 수집이 되는 경우에도 선박 자체의 항적 정보가 추출이 되는 경우 더욱 정확한 사고분석이 가능하기 때문이다.

따라서 선박의 항해장비에 대한 파악과 해당 장비의 데이터 수집 과정이 요구된다. 선박의 항해장비는 선박의 규모에 따라 달라지며, 정확성 또한 달라지는 다양한 제조회사로부터 판매되는 장비가 존재하여 데이터 분석과정은 매우 어려워진다.

항해장비의 데이터수집이 되어지는 경우, 디지털 포렌식이 되는 수집절차는 다음 그림 3과 같다.

항해장비는 아래와 같은 장비 등이 존재하며, 각 제조회사별로 독특한 구조의 파일 생성이 이루어지므로 관련 정보를 지원받아 기술개발이 이루어져야 가능하다.

- AIS 송수신 장비 (대부분 위치정보가 저장되지 않음)
- GPS 플로터 장비
- V-PASS 장비
- ECDIS 장비
- VDR(Voyage Data Recorder) 장비

이러한 항해장비는 제조회사별로 수집된 데이터로부터 항적이 수집되어지는 경우, 법적 증거물로 사용되기 위하여는 관리연속성(Chain of Custody)이 유지되어져야하며, 이는 디지털 증거의 수집, 이송 및 분석 과정에서 증거무르이 보관 주체들 간의 연속적인 승계내역(담당자, 전달과정, 처리내용, 보관방법, 해시값 등)을 기록함으로써 디지털 증거가 최초 수집된 상태 그대로 어떠한 변경없이 관리되었음을 입증하는 절차이다.

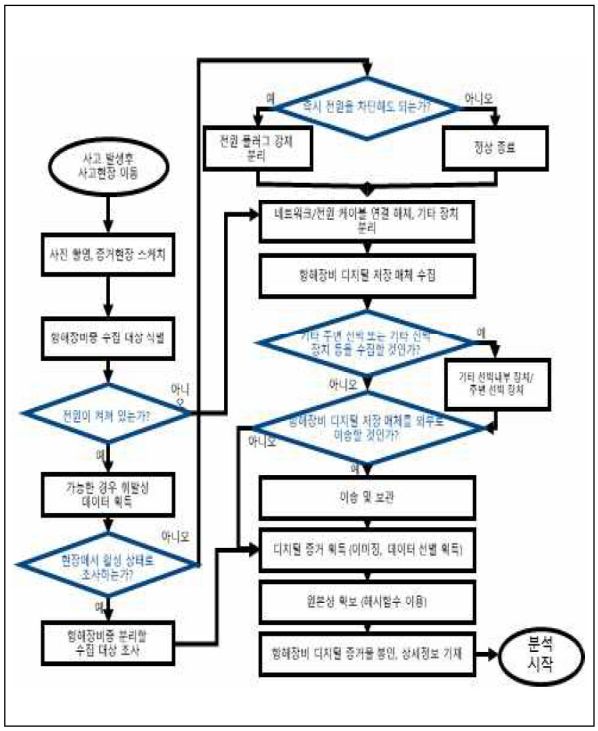

Fig. 3 선박 탑재한 항해장비를 이용한 해양사고 디지털포렌식 절차

사고 데이터와 사고분석결과는 아래와 같이 항해장비 정규화 DB 시스템을 통하여 통합적 관리하는 것이 요구된다.

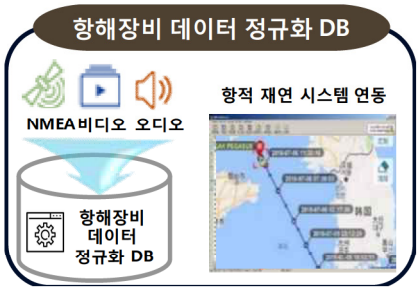

Fig. 4 항해장비의 포렌식 데이터의 정규화 DB

이것은 사고 후 유사 사고시 사고에 대한 분석과정에 재활용될 수 있으며, 사고 분석 대상 장비가 동일한 장비인 경우, 더욱 빠르게 분석할 수 있다.

3. 결 론

본 논문에서는 재난 수준의 해양사고가 발생되는 경우, 선박의 사고에 대한 상황을 정확히 파악하는 것이 요구되어 왔다. 즉, 선박간의 피해규모, 과실 유무를 판단하기 위하여 해양경찰의 수사 진행 절차가 수반된다. 이러한 수사과정에서는 육상의 VTS 시스템에서의 항적 분석과정과 육상 시스템에서 데이터 수집이 용이하지 않은 경우, 또는 명확한 분석이 어려운 경우 등에 대하여 선박 탑재한 항해장비의 항적 등 사고 상황에 대한 분석이 요구되는데, 해당 처리 절차에 대하여 분석하였다.

향후 이러한 사고에 대비하여 사고 절차에 따라 필요한 시스템 개발을 수행함으로써 사고에 대한 판단 뿐만 아니라 나아가 동일 사고 예방까지 가능하게 된다.

또한 사고조사 정보를 데이터베이스화 하여 세부적으로 요구되는 시스템 장비, 분석 가능한 프로그램이 개발된다면, 신속하게 사고 분석과 조치가 가능하게 될 것이다.

이러한 해양사고에 대한 분석 기술개발은 최근 국민의 의식수준의 향상과 더불어 사고 발생시 정확한 판단과 신속한 조치를 할 수 있도록 하는 체계로서 선진 해양국가로서 반드시 요구되는 기술이라 할 수 있다.

참 고 문 헌

[1] IALA 홈페이지, VTS Committee/e-Navigation

[2] “분쟁소지가 있는 공해상에서 Digital Forensic을 이용한 해결방안”, Vol. 12 2007 한국 컴퓨터정보학회 논문지

후 기

본 연구는 2019년 해양경찰청 재원으로 해양수산과학기술진흥원의 지원을 받아 수행된 연구임 (해양사고 현장 디지털 증거물 무결성 및 증거능력 확보를 위한 항해 장비 디지털 포렌식 기법 개발)