KR Maritime Cyber Security

News from KOREAN REGISTER

Sep 2018

Vol. 005

● 한국 요꼬가와전기와 사이버보안 상호협력 기술교육 수행

지난 8월 7일, 한국선급 사이버보안 대응 TFT에서는 요꼬가와전기 본사에서 LNGC 기술 교육 및 사이버보안 상호협력 기술교육을 수행하였다. 교육은 양일간 진행되었으며 교육 커리큘럼은 다음과 같다.

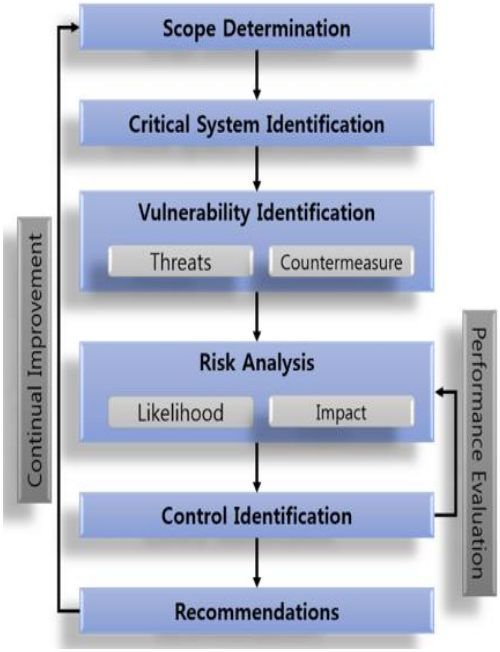
날짜	강의	교육과정	상세내용
8.7(화)	Yokogawa	· LNGC 기술교육 [8H]	· LNG Carrier 프로세스 이해 · LNG Carrier 사이버보안
8.8(수)	한국선급	· 해사사이버보안의 이해[2H] · 해사사이버보안 관리 실무[2H]	· 사이버 자산관리 · 사이버 위협 · 사이버 리스크평가 이해

요꼬가와전기는 자동화 시스템 솔루션 공급업체로서 통합 제어 시스템 분야에 독보적인 기술 및 시장(산업공장, 정유설비 및 LNG Carrier)를 점유하고 있고, 높은 수준의 사이버보안 솔루션을 업계에 제공하고 있다. 지난 7월 한국선급과 사이버보안 MOU를 체결하여 해상 사이버보안 관리시스템 회사 인증, 선박 사이버보안 운영기술(OT : Operating Technology) 시스템 규칙 적용 연구를 공동 수행하고 있다. LNGC는 다수의 사이버 시스템이 탑재되며, 통합제어 시스템의 복잡도 및 중요도가 증가하고 있어 사이버보안 필요성이 대두되고 있다.

본 교육 및 공동 연구수행을 통해 한국선급은 LNGC OT 시스템 사이버보안 기술력을 제고할 것으로 기대한다.

● 티원아이티와 사이버 리스크평가 수행

지난 8월 30일, 한국선급 사이버보안 대응 TFT는 티원아이티와 회사 사이버 리스크평가 워크샵을 수행하였다. 사이버 리스크평가의 목적은 선박 및 회사의 자산을 사이버 위협으로부터 보호하고 사이버보안의 지속적인 향상 및 관리를 위한 기반을 마련하기 위함이며, 선박 및 회사 주요 시스템에 대한 사이버보안 현재 리스크 수준을 확인하고 사이버보안 수준을 향상시킬 수 있도록 관리적, 기술적, 물리적 측면에서의 보안 대책을 워크샵을 통해 확인할 수 있다.



한국선급은 4단계로 구성된 독자적인 사이버 리스크평가 프로세스를 2017년 12월 구축하여 Songa Shipmanagement 社 본사 및 선박 23척에 적용한 바 있다. (7월 뉴스레터 참조)

티원아이티는 선박 전산장비 유지보수, SW 개발 전문 업체로서 현대상선, 에이치라인, 현대글로비스, KTSAT 등 해운, 통신, 조선 분야에서 IT 서비스를 제공하고 있으며, 지난 5월 한국선급과 사이버보안 MOU를 체결하여 회사 인증을 진행하고 있다. 한국선급 사이버보안 인증을 위해 위해서는 사이버 리스크평가 문서를 제출해야 한다. 한국선급에서 제공하는 사이버보안 인증 및 기술서비스 상세사항은 홈페이지를 통해 확인 할 수 있다.

● 국가인적자원개발 컨소시엄 교육과정 안내

KR 교육훈련원이 정부(해양수산부, 고용노동부 및 산업통산자원부) 지원 '인적자원개발 전문기관'으로 새로운 지평을 열게 되었다.

교육훈련원은 지난 7월 '국가인적자원 컨소시엄 사업 공동훈련센터'로 선정되었으며, 이를 계기로 어려운 상황에 있는 해사업계 인적자원개발 사업에 능동적으로 기여할 수 있게 되었다. 교육훈련원은 해사업계의 사전수요 조사 및 분석을 통해 2018년도 하반기에 선급 특성화 교육과정 및 인증분야 등 14개 교육과정을 우선 선정하여 운영할 예정이며, 교육 과정은 아래와 같다. 컨소시엄 교육은 한국선급과 컨소시엄 체결 기업의 재직자를 대상으로 무상으로 지원되며 교육 신청접수는 KR Academy 홈페이지를 통해 접수할 수 있다.

※ http://champ.krs.co.kr/main/main.jsp

(한국선급 컨소시엄센터 -> 교육과정 안내 -> "해사 사이버보안의 이해" 또는 "해사 사이버보안 관리 실무")

국가인적자원개발 컨소시엄 교육과정 안내

교육 과정 명	교육시간	교육 일자	교육 장소
SOLAS & MARPOL 협약 이해	2일(16h)	2018.10.15-10.16	한국선급 국제교육 훈련센터
		2018.11.12-11.13	
선체구조 및 강도(Hull Structure and Strength)	1일(8h)	2018.09.20	
선박 기관도면의 이해	2일(16)	2018.09.17-09.18	
Design Course – Oil Tanker & Chemical Tanker (Hull & Equipment Part)	1일(8h)	2018.10.29	
Design Course – Oil Tanker & Chemical Tanker (System & Equipment Part)	1일(8h)	2018.10.30	
Design Course - LNG&LPG Carrier (Hull & Equipment Part)	1일(8h)	2018.11.15	
Design Course - LNG&LPG Carrier (System & Equipment Part)	1일(8h)	2018.11.16	
Fire Fighting System(FSS Code)	1일(8h)	2018.10.15	
Rightship inspection 요구사항 이해 및 실무	2일(16h)	2018.10.11.-10.12	
선박감리 일반	2일(16h)	2018.10.22.-10.23	
해사 사이버보안의 이해	1일(8h)	2018.10.17	
해사 사이버보안 관리 실무	2일(16h)	2018.10.18.-10.19	
해운산업 통합 관리 시스템 구축 및 운영 실무	2일(16h)	2018.09.13.-09.14	
		2018.10.24.-10.25	
방폭(화재폭발방지) 기초	1일(8h)	2018.11.30	

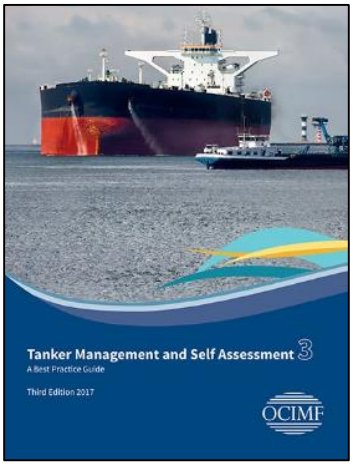
OCIMF TMSA/SIRE VIQ 사이버보안

해운업계에 부는 4차산업 변화에 발맞춰 선박은 급속도로 디지털화가 되고 있다. 하지만 동전의 양면과 같이 최신 정보통신기술에 선박운용 의존성이 커짐에 따라 해커에 의한 선박 사이버위협이 큰 문제로 대두되고 있다. 일례로 세계 최대 해운회사인 AP 뮐러-머스크는 작년 6월 랜섬웨어(NotPetya)에 감염돼 약 3000억원의 피해를 입은바 있다.

날로 커지는 선박사이버위협에 대응하고자 국제해사기구(IMO)는 2021년부터 선박안전관리규칙(ISM Code)에 사이버위협을 포함시켜 관리하기로 의결했으며, 해운업계 역시 화주검사(OCIMF TMSA/SIRE)에 사이버보안 항목을 요구하고 있다.

● **OCIMF TMSA (3판) 개정**

OCIMF TMSA(3판) 개정으로 2018.1.1부터 탱커선(O/C, Oil, Shuttle, Gas)을 보유하고 있는 선사는 사이버보안 관리능력이 요구되며 사이버보안 정책서·절차서 이행, 리스크평가 수행, 임직원 인식제고 교육 등을 포함한 17개 항목을 점검한다.

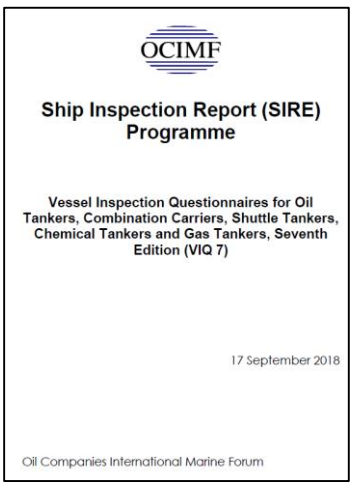


● **OCIMF SIRE VIQ(7판) 개정**

OCIMF SIRE VIQ(7판)은 2018.9.17부터 선박에 적용되며 사이버보안 대응계획을 포함한 정책서·절차서 이행, 선박 IT/OT 시스템 물리적 접근 통제, 개인 휴대용 장비 통제, 선원 인식제고 교육 등의 4개항목을 점검한다.

대응 방안 및 시사점

선사는 체계적인 사이버 보안 관리 시스템 구축이 필요하며, 사이버보안 정책의 수립 및 적용, 사이버 리스크평가를 통한 개선, 선사 임직원 및 선원 인력에 대한 지속적인 인식제고 및 전문화된 교육이 요구된다.



Ref. Oil Companies International Marine Forum

선박 바이러스 감염 및 오작동 사례

국내 선박 사이버보안 현황을 조사한 결과 선박 업무용 PC, PMS/통신 서버가 랜섬웨어 바이러스, AutoRun 바이러스, FBI 바이러스 등에 감염된 것으로 확인되었다. 이러한 바이러스 감염의 경로는 다음과 같다.

- E-MAIL을 통한 첨부파일 클릭 시 감염
- V-SAT을 통한 인터넷 사용으로 감염
- 외부 작업자들의 USB를 선내 PC에 연결
- 내국 및 외국 선원들의 개인 USB를 통한 감염
- 선원들의 복지용 외장형 HDD를 통한 감염

사이버사고 예방을 위해서는 윈도우 최신 패치 설치, 백신 최신 패치 업데이트가 팔요하며 무분별한 USB 사용을 방지하기 위한 선박 사이버보안 정책 수립 및 이행, 선원 인식제고 및 3rd Party 관리 조치가 필요하다.

감염사례	감염위치	감염 경로	조치 사항
랜섬웨어 바이러스	· PMS & 통신 서버 · 클라우드 서버 PC	· E-MAIL을 통한 첨부파일 클릭 시 감염 · VSAT을 통한 인터넷 사용으로 감염	· 윈도우 패치 적용 · 윈도우 재설치
AutoRun 바이러스	· 통신용 서버 · 클라이언트 PC	· 외부 작업자들의 USB를 선내 PC에 연결 · 내국 및 외국 선원들의 개인 USB를 통한 감염 · 선원들의 복지용 외장형 HDD를 통한 감염	· 백신 업데이트 후 치료 · 백신 설치 후 치료 · 윈도우 재설치
FBI 바이러스	· PMS & 통신용 서버	· 인터넷을 통한 감염	· 백신 업데이트 후 치료 · 윈도우 재설치

대응 방안 및 시사점

해상 분야에서 발생한 사이버보안 사고는 각 선사 뿐만 아니라, 각 국가별 항만 분야에서도 사이버보안 요구사항을 강화하는 계기가 되고 있다. 항만에 접안하는 모든 선박에도 유효하게 적용될 가능성이 높아 각 기업별 지속적이고 단계적 접근이 필요하다.

사이버 위협의 이해

● 사이버 위협 이해하기

사이버 위협이란, 조직 운영, 조직 자산, 개인, 기타 조직 또는 국가에 대해 사이버 시스템을 통한 무단 액세스, 파괴, 공개, 정보 수정 또는 서비스 거부와 같은 잠재적으로 악영향을 미칠 수 있는 상황이나 사건을 의미한다. (출처 : NIST SP : 800-128)

사이버위협은 ICT 기술이 발전함에 따라 자산에 미치는 영향이 변화하므로 자산의 취약점을 파악하기 위해 주기적으로 목록화 할 필요가 있다.

● 한국선급 해상사이버보안 관리시스템 인증 검사항목(CSMS1)

204.1 위험관리 : 내부 정보기술 및 운영기술 환경에 의한 영향을 미치는 외부 환경 요인을 위협으로 식별하고 목록화하여야 한다.

● BSI 10대 위협

ICS에 대한 위협은 기존의 취약성으로 인해 ICS 및 관련 기업에 잠재적으로 손상을 줄 수 있는 공격 또는 이벤트로 인한 것이다. 다음 표는 독일 연방정보 보안국에서 발표한 ICS에 대한 가장 중대한 위협 목록이다. 지난 7월 뉴스레터에 이어 BSI 10대 사이버 위협 중 '**사회공학과 피싱 공격**'에 대해서 분석하고자 한다.

No. (old No.)	Top 10 2016	Top 10 2014
1 (3)	Social Engineering and Phishing†	Malware Infection via Internet and Intranet
2 (2)	Infiltration of Malware via Removable Media and External Hardware	Infiltration of Malware via Removable Media and External Hardware
3 (1)	Malware Infection via Internet and Intranet	Social Engineering
4 (5)	Intrusion via Remote Access	Human Error and Sabotage
5 (4)	Human Error and Sabotage	Intrusion via Remote Access
6 (6)	Control Components Connected to the Internet	Control Components Connected to the Internet
7 (7)	Technical Malfunctions and Force Majeure	Technical Malfunctions and Force Majeure
8 (9)	Compromising of Extranet and Cloud Components	Compromising of Smartphones in the Production Environment
9 (10)	(D)DoS Attacks	Compromising of Extranet and Cloud Components
10 (8)	Compromising of Smartphones in the Production Environment	(D)DoS Attacks

Ref. : Industrial Control System Security – Top 10 Threats and Countermeasures 2016

● **BSI 10대 위협 : 사회 공학과 피싱 공격**

사회 공학은 일반적으로 비 기술적인 방법으로 정보 또는 IT 시스템에 대한 무단 액세스를 얻는 방법이다. 사회 공학은 호기심, 도움, 신념, 공포 또는 권위 존중과 같은 인간의 특성을 이용한다. 이러한 특성은 위협원이 직원을 의도적으로 또는 부주의하게 행동하도록 유도하는 전환 전략으로 자주 사용된다. 일반적인 예는 사기성 전자 메일 (피싱 메일)이다.이러한 종류의 전자 메일은 직원들이 맬웨어가 포함 된 첨부 파일을 열거나 악성 웹 사이트로 유도한다

<가능 시나리오>

▣ 위협 행위자가 피해자의 로그인 자격 증명을 얻거나 사기성 메시지를 통해 멀웨어를 배포한다.

▣ 열었을 때 트로이 목마 또는 랜섬웨어와 같은 맬웨어를 설치하는 겉보기에 해가 되지 않는 링크나 첨부파일이 있는 전자 메일

▣ 스피어 피싱은 대상자에게 정확하게 맞춘 전자 메일을 사용하여 대개 적은 수의 공격 대상을 공격하는 데 사용된다. 다른 소스 중에서도 회사 웹 사이트 또는 소셜 네트워크에서 가져온 공개 정보가이드 용도로 사용된다.

▣ 위협 에이전트는 서비스 기술자처럼 자신감 있고 친절한 태도로 또는 허위 정보를 제공함으로써 건물이나 사이트에 대한 무단 액세스를 얻을 수 있다.

<대책>

- 대상 고객 특정 보안 인식 교육 실시
- 조직 예방 조치 : 보안 정책의 수립 및 시행
  - 기업의 주요 자산의 식별 및 분류
  - 데이터 백업 정책 수립
  - 사내 직원뿐만 아니라 파트너 및 서비스 제공 업체에 대한 기밀 유지
  - 종이에 인쇄된 정보 파쇄 정책
  - 디지털 저장 매체의 안전한 폐기
  - 모바일 장비 처리 규정 (개인 정보 보호 필름, 보안 저장 장치)
- 사이버 사건 및 의심스러운 행동에 대한 알람 채널 도입
- 적용되는 규정을 시행하고 부정 행위 또는 공격 (예 : 장치 또는 액세스 제어)을 자동으로 탐지하기위한 기술 보안 메커니즘의 사용
- 사고 발생시 데이터 및 응용 프로그램을 복원하기위한 정기적인 백업

Ref. : Industrial Control System Security – Top 10 Threats and Countermeasures 2016

사이버 사고 대응 및 복구 체계 수립 가이드

● 사이버 사고 대응 및 복구 체계 수립의 필요성

회사는 회사 내부와 선박의 사이버 자산에 발생 가능한 사이버보안 사고에 대비하여야 한다. 사이버보안 사고에 대비하기 위해서는 사이버보안 사고 대응 계획을 수립하고 운영하여야 한다. 사고 대응 계획에서는 보안사고의 정의 및 범위, 긴급 연락체계 구축, 보안사고 발생 시 보고 및 대응절차, 사고 복구조직의 구성, 교육 계획등이 포함되며 절차상으로 사이버보안 사고에 대한 대응, 복구, 보고로 구성 될 수 있다.

● 한국선급 해상사이버보안 관리시스템 인증 검사항목(CSMS1)

사고대응 및 복구(208.1) : 회사는 사고 발생 시 사고 유형과 그에 따른 대응방법 및 절차 등을 포함한 사고대응 및 복구 정책을 수립하여야 한다.

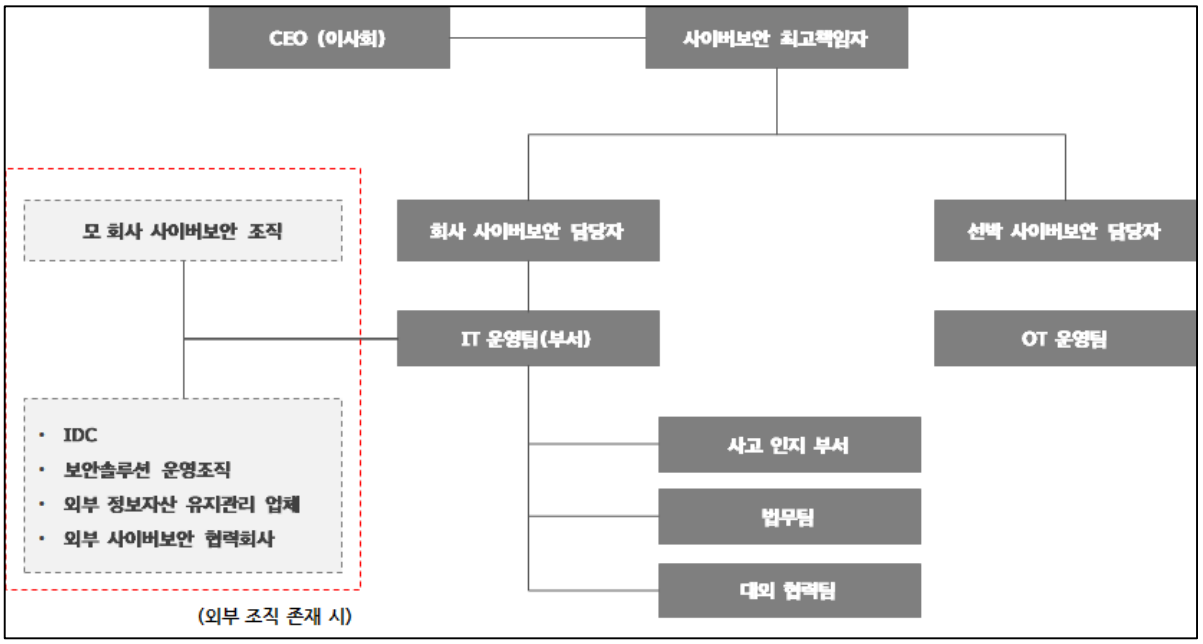
사고대응 및 복구(208.2) 회사는 시스템 운영 및 보안이슈에 즉각적으로 대응 및 복구 업무를 수행할 조직 또는 담당자를 구성하여 역할 및 책임을 정의하여야 한다. 또한 내외부 관련자들과 신속한 연락이 가능하도록 비상연락망 체계를 구축하고 비상 연락망을 최신화하여 관리하여야 한다.

● 시스템 복구 목표 설정 (예시)

구분	영향도	긴급도	RTO*
복구 1순위	○ 전체 조직과 관련된 중요한 업무 프로세스에 심각한 영향 ○ 선박 운항 및 화물 운송에 중요한 업무 프로세스에 심각한 영향	즉각적 해결	최대 12시간 이내
복구 2순위	○ 중요한 업무 프로세스의 부분적으로 심각한 영향 ○ 선박 운항 및 화물 운송 업무의 부분적으로 심각한 영향	가능한 신속한 해결	최대 3일 이내
복구 3순위	○ 전체 조직 운영에 미미한 영향 ○ 선박 운항과 무관한 영향	어느 정도 대응시간을 가지고 해결	최대 30일 이내

※RTO(Recovery Time Objective)에 필요한 시간은 회사가 결정

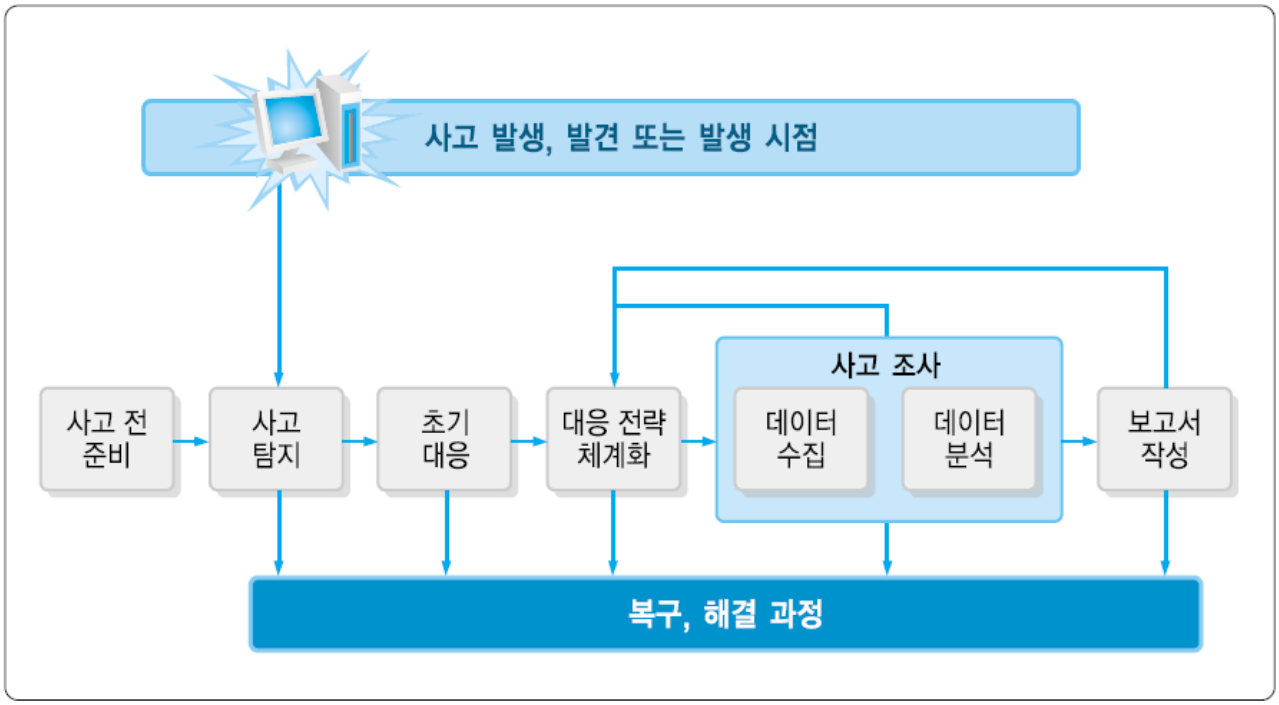
● 사이버 사고 대응 조직(예시)



● 사이버 사고 대응팀 주요역할(예시)

부서	주요 역할	비고
사이버보안팀	O 회사 또는 선박 사고대응 업무 총괄 O 사고 원인, 경과, 후속조치 현황 등에 대한 보고 O 외부 유관 업체 긴급 연락망 가동 및 업무 지시 O 조직 내 사고 확산 방지를 위한 대응방안 발표 O 사고 원인 분석 및 대응책 마련 O 조직 내부 Help-Desk 운영	외부 조직이 해당 업무를 수행할 수 있음
IT(OT) 운영팀	O 사고 발생 시스템 원인 분석 또는 근거 자료 보존 O 비상 시스템 가동 또는 시스템 긴급 복구 O 데이터 복구 및 가동 O 사이버보안 솔루션 재점검 및 후속조치 적용	외부 조직이 해당 업무를 수행할 수 있음
사고 인지 부서 (현업 부서, 선박 운항부서 등)	O 사고 인지 및 내부 신고 또는 보고 O 신고 시 보안사고 경위에 대하여 상세 내용 작성	-
법무팀 & 대외 협력팀	O 사고로 인한 관련 감독기관 등에 대한 업무 협의 O 침해사고 또는 비상사태 관련 신고 O 법적 이슈 최소화를 위한 사이버 보안팀과 협의	-
외부 유관 분야 전문업체	O IDC, 보안 솔루션 운영업체, 시스템 유지보수 업체 등 유관 시스템 긴급 복구 및 재가동	-

● 사이버 보안사고 대응 절차(예시)



단계	절차별 주요 내용
사고 전 준비과정	사고가 발생하기 전 사고대응팀과 조직적인 대응 준비 및 사고 대응 위한 문서 점검
사고 탐지	정보보호 및 네트워크 장비에 의한 이상 징후 탐지. 관리자에 의한 침해 사고의 식별
초기대응	초기 조사 수행, 사고 정황에 대한 기본적인 세부사항 기록, 사고대응팀 신고 및 소집, 침해사고 관련 부서에 통지
대응 전략 체계화	최적의 전략을 결정하고 관리자 승인을 획득. 초기 조사결과를 참고해 사고 조사과정 시 수사기관 공조 여부를 판단
사고조사	데이터 수집 및 분석을 통하여 수행. 언제, 누가, 어떻게 사고가 일어났는지, 피해 확산 및 사고 재발을 어떻게 방지할 것인지 결정
보고서 작성	의사 결정자가 쉽게 이해할 수 있는 형태로 사고에 대한 정확한 보고서 작성
복구 및 해결	차기 유사 공격을 식별 및 예방하기 위한 보안 정책의 수립, 절차 변경, 사건의 기록, 장기 보안 정책 수립, 기술 수정 계획수립 등 결정

Ref. : KISA 침해사고 분석절차 안내서(2010-8호)

용어 설명

- **OCIMF :** OCIMF(Oil Companies International Marine Forum)는 Torrey Canyon 해양사고(1967)이후 해양오염에 대한 관심 및 우려가 증가되는 상황에서 Oil 관련 회사(Shell, BP, Exxon Mobile, Total, Chevron 등)가 모여 1970년 4월 9일 런던에서 조직된 포럼으로, Tanker 선과 Oil Terminal로부터 발생 가능한 해양오염 예방 및 안전 확보에 기여하고 있다.
- **SIRE :** SIRE(Ship Inspection Report) 프로그램은 유조선(액화가스선, 화학제품운반선 포함)의 안전성을 평가하는 수단들 중 하나로 과거 여러 Oil Major에서 동일한 선박에 시행함으로써 야기된 검사 인력 낭비 / 선원의 업무 로드 등을 덜어 주기 위해 OCIMF에서 1993년에 도입한 프로그램이다. OCIMF Member에게 OCIMF 웹사이트를 통하여 12개월간 SIRE 공유되며, 각 Oil Major사는 검사를 실시하지 않고 SIRE report를 통하여 선박을 평가 가능하다.
- **TMSA :** TMSA(Tanker Management and Self Assessment)는 근본 RISK의 원인이 되는 운항선사 안전관리에 대한 일원화된 평가 기준이 없어, Sub-Standard 운항선사의 식별 및 퇴출을 위해 2004년 OCIMF에서 개발하였다. TMSA 자체 평가를 통해 운항선사는 미흡한 안전관리 수준을 식별하고 지속적 개선을 위해 활용될 수 있으며, Oil 회사는 TMSA Audit 결과에 따라 장/단기 비즈니스의 가능 여부를 결정할 수 있다.
- **V-SAT :** V-SAT(Very Small Aperture Terminal)은 직경 2.4m 이하의 크기를 갖는 소형 안테나를 사용하는 초소형 지구국을 의미한다. 정지위성인 C대역 외에 Ku대역도 이용하게 되면서 지구국 안테나의 소형화가 가능하게 되었다. C/Ku/Ka 주파수 대역은 항공기, 육상, 해상에서 모두 사용할 수 있으며, L 주파수대역은 해상에서 음성통화에 사용한다.