KR Maritime Cyber Security

News from KOREAN REGISTER

Feb 2019

Vol. 010

한국선급 활동

● 영국 선사 대상 사이버보안 적합성 인증서 수여

한국선급은 지난 2월 12일 영국의 해운선사인 'Songa Shipmanagement'의 회사 사이버보안 인증 심사를 마치고 사이버보안 적합성 인증서를 수여하였다고 밝혔다.

Songa 선사는 탱커선을 주요 선종으로 운항 관리하는 선사로서 금 번 한국선급의 회사 사이버보안 인증 심사를 통과함으로써 정보보안시스템 및 관리 선대의 사이버 공격 대응 체계에 대해 한국선급으로부터 인증 받은 최초의 선사가 되었다.

최근 해사산업계 전반에 걸쳐 최신 정보통신기술이 광범위하게 적용됨에 따라 해상 사이버공격에 대한 위험 또한 전 세계적으로 증가하고 있다. 따라서 개별 선박 뿐 아니라 이들의 운항을 총체적으로 관리하는 선사차원의 사이버보안 대응 및 관리에 대한 중요성이 대두되고 있다. 이에 따라 한국선급은 지난해 ISO 27001, IEC 62443, NIST Framework 등 국제 보안표준과 IMO 및 BIMCO의 해상 사이버보안 가이드라인 등을 준용한 해상 사이버보안 관리 시스템 인증 체계를 최종 구축하였으며, 선사 및 선박에 사이버보안 인증 서비스를 제공하고 있다.

인력관리, 리스크관리, 자산관리, 사고대응 및 복구 등 총 18개 카테고리의 87개 검사항목을 통과한 Songa 선사는 사이버보안에 대한 IMO 및 RIGHTSHIP, TMSA등 화주검사 요구사항을 모두 만족할 뿐 아니라 사이버 공격에 대한 대응 및 보호체계를 갖추었음이 공식적으로 인정되었다. 이후 한국선급은 총 23척의 동사 관리 선박에 대한 사이버보안 인증을 순차적으로 진행할 예정이다.

● e-Navigation Underway International 2019

한국선급 e-Navigation TFT는 지난 2월 덴마크 코펜하겐에서 개최된 e-Navigation Underway 2019에 참석하여 디지털 신기술의 해상적용을 위한 최신 국제 정책 동향 및 기술개발 현황을 모니터링하였다.

컨퍼런스는 총 4개의 세션으로 구성되어 해사업계 전문가들의 활발한 논의가 이루어졌다. 드론, 사이버보안, 블록체인 등 신기술 개발 및 도입 현황에 대한 발표가 있었고 모든 세션에서 사이버보안에 대한 질의 및 중요성이 강조되어 헤사업계의 사이버보안 대응 및 전략 수립이 필요함을 확인할 수 있었다.

특히 [세션 4]에서는 사이버보안을 주제로 BIMCO(발틱해국제해운협회)에서 최근 개정한 '선박 사이버보안 가이드라인(Rev.3)'이 소개되었으며, 해상 사이버보안 및 정보보안에 대한 덴마크의 국가 전략과 이니셔티브가 소개되어 주목을 끌었다.

향후 선박 사이버보안을 위해서는 해사업계의 다양한 이해관계자(항만, 선주, 선급, 조선소, 제조업체, 서비스업체 등)의 책임과 역할이 명확히 식별되어야 하며, 덴마크와 같이 국가 차원에서 해사업계의 전략 수립이 필요할 것으로 예상된다.

구분	주요내용
[세션 1] 산업계 : 초기 개척자로서의 이점과 장벽	신기술(AI, 드론, 사이버보안) 에 대한 규칙 제정이 필요하며,해사업계 기관의 데이터가 공유될 수 있도록 패러다임 전환 필요
[세션 2] 규정과 표준	규정과 표준은 자율 산업 성장의 장벽과 이익이 될 수 있는 양면성이 있으며 해사업계에 긍정적인 결과를 이끌어 내도록 역할 필요
[세션 3] 항만 및 연안국	e-Navigation 결과물을 항만에 적용한 서비스 및 드론 적용 사례 소개, EMSA는 해상 안전, 보안, 예방 및 선박, 석유 및 가스 설비에 의한 해양 오염에 대한 대응을 위해 신기술 적용 계획 발표, 대한민국은 스마트 해상물류 시스템 구축 전략 발표
[세션 4] 사이버보안 (선박 사이버보안 및 안전관리)	덴마크 해사청은 해사분야 사이버보안 로드맵과 계획을 2019.1.1.일부터 수립하여 실행 예정이며, BIMCO 및 CIRM 등 해사분야 협의체에서 2년간 해사 사이버보안 관련 진행 사항 발표.

Ref. : About e-Navigation Underway 2019

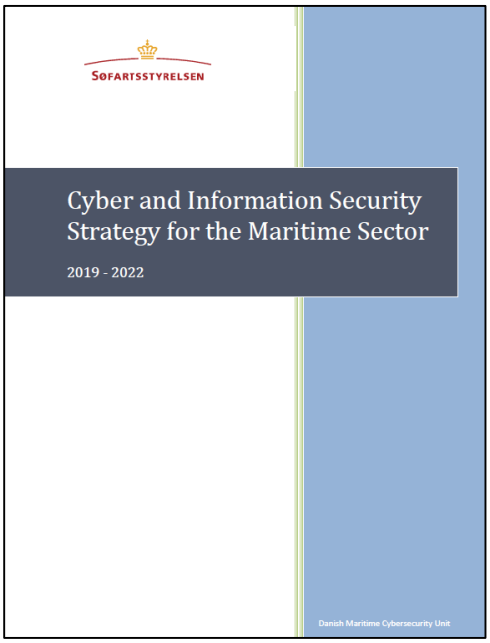
덴마크 정부, 해사 사이버보안 전략 발표(2019-2022)

● 해상 부문의 사이버 및 정보 보안 전략 발표

덴마크 산업 자원부(Department of Industry, Business and Financial Affairs)는 사이버 및 정보보안 전략의 일환으로 해운 업계에 새로운 부문 별 전략을 발표했다. 이 전략에는 IT 보안을 강화하고 해상 부분에서 사이버 위협을 방지 하기 위한 여러가지 계획이 포함되어 있다. 목적은 사이버 공격으로부터 덴마크 해역의 항해 안전과 선박 운항, 추진 및 항해를 위한 시스템 및 소프트웨어를 포함한 덴마크 선박의 안전을 보장하는 것이다. 또한 교통 모니터링, 경고 및 정보 시스템과 같은 서비스뿐만 아니라 선박의 안전 운항과 연결되는 다른 시스템도 포함된다. 덴마크 해사 당국(Danish Maritime Authority)은 덴마크 해사 사이버보안 부서 (Danish Maritime Cybersecurity Unit)를 설립하여 하기 전략을 단계적으로 실행할 예정이다.

<단기 전략(2019)>

- 덴마크 해사 사이버보안 부서 설립
- EU 및 국제법
- 해상 운영자와 사이버보안 센터(CFCS) 간의 단일 연락 지점
- CFCS에 덴마크 해사청 직원의 파견 근무
- 해상 분야에서 협력 및 지식 공유를 통한 인지도 향상



<중기 전략(2020-2021)>

- 해양부문 관계자를 위한 특별한 목적과 사용자 친화적인 권고 사항
- IT 보안 문화 및 인식
- 사이버보안 및 정보보안 관리 및 관련 표준화된 프로세스에 초점
- 해상 부문의 지속적이고 강력한 사이버보안 및 정보보안 준비
- IT 보안 사건 대응을 위한 공동 조기 경고 계획
- 일반 사이버보안 및 정보보안 연습 계획 및 구현

<장기 전략(2022)>

- 사이버보안 및 정보보안 지식을 해양 당국과 이해 관계자가 쉽게 접근하고 검색 할 수 있는 디지털 허브 및 커뮤니케이션 플랫폼을 개발 필요성 및 가능성 확인

Ref. : New strategy for cyber security in the Danish maritime sector

UK 정부, Maritime 2050 전략 추진

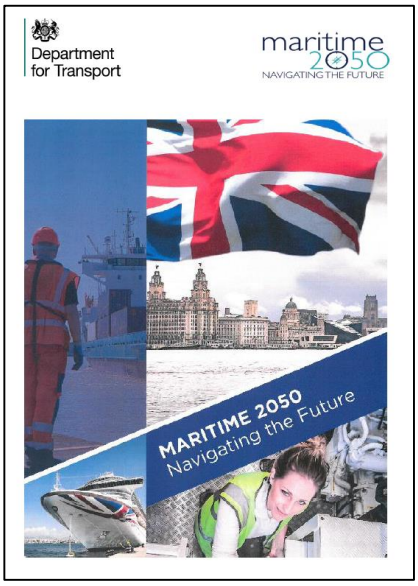
● **Maritime 2050을 위한 단·장기 전략 및 권고사항 발표**

영국 정부는 2030년까지 무명 항구에 '해양 혁신 허브 (Maritime Innovation Hub)'창설을 포함하여 새로 발표된 Maritime 2050 전략의 핵심 요소인 기술 혁신을 착수했다. Maritime 2050은 산업, 기술, 무역, 환경, 인력, 인프라,보안 등 7가지 주제를 중심으로 영국 정부가 해상 성장을 지원하기 위해 업계와 어떻게 협력 할 수 있는지에 대한 로드맵을 설정한 최초의 장기 국가 전략이다.

스마트 포트의 개발은 디지털 및 자동화 프로세스의 이점을 활용하여 원활한 연결로 물품 처리량을 극대화하기 위해 새로운 비즈니스 모델을 창출하는 것을 목표로 한다. 정부는 또한 영국의 영해에서 국제 사업체를 유치해 수행할 수 있도록 자국 내 자율운항선박의 틀을 법제화하겠다고 약속했다. 전송 체인을 통해 종이 기반 프로세스를 대체하는 것은 선원들의 필수 교육 및 인증 검증을 효율화하기 위한 디지털 문서의 도입, 블록체인 등의 신기술의 잠재적 이점 연구와 같은 전략의 또다른 명시적인 푝표이다. 2025년까지 디지털 영국 선박 등록 제도의 창설을 포함하여 2030년까지 영국의 해상 부문에 대한 완전한 종이없는 관리가 예상된다.

영국은 또한 2050 년까지 전 세계적으로 조화된 표준을 기대하면서 IMO에서 국제 표준을 설정하고 시스템의 상호 운용성을 보장하기위한 노력을 주도하여 투명한 데이터 중심의 영국의 해양 공간 디지털화를 규율하고자 한다.

사이버보안은 정부가 해상 산업의 다양한 분야에 걸쳐 개발이 계속됨에 따라 강력한 방어를 유지하는데 있어 중요한 고려사항으로 주목 받고 있다. 공급망 전체에 걸쳐 사이버 위협에 대한 복원력을 확보하고 스스로를 보호하기 위한 책임은 산업계에 있으나 영국 정부가 해상 사이버보안 총체적인 솔루션 제공자로서 국가 사이버보안 센터를 통해 사이버 위협을 평가하고 위협에 대한 정보 및 조언을 제공하기 위해서는 산업계와의 긴밀한 협의가 필요하다.



Ref. : UK launches Maritime 2050 strategy

사이버 위협의 이해(OWASP Top 10)

● 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 해상 사이버보안 시스템 인증 검사항목(CS1)

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

● OWASP Top 10

OWASP(Open Web Application Security Project)는 오픈소스 웹 어플리케이션 보안 프로젝트이다. 주로 웹에 관한 정보노출, 악성 파일 및 스크립트, 보안 취약점 등을 연구하며 웹 어플리케이션 취약점 중에서 빈도가 많이 발생하고, 보안상 영향을 크게 줄 수 있는 10대 항목(OWASP Top 10)을 2004년, 2007년, 2010년, 2013년, 2017년 기준으로 발표하였다. 지난 1월 뉴스레터에 이어 **'A1 : 2017 - 인젝션'** 을 분석하고자 한다.

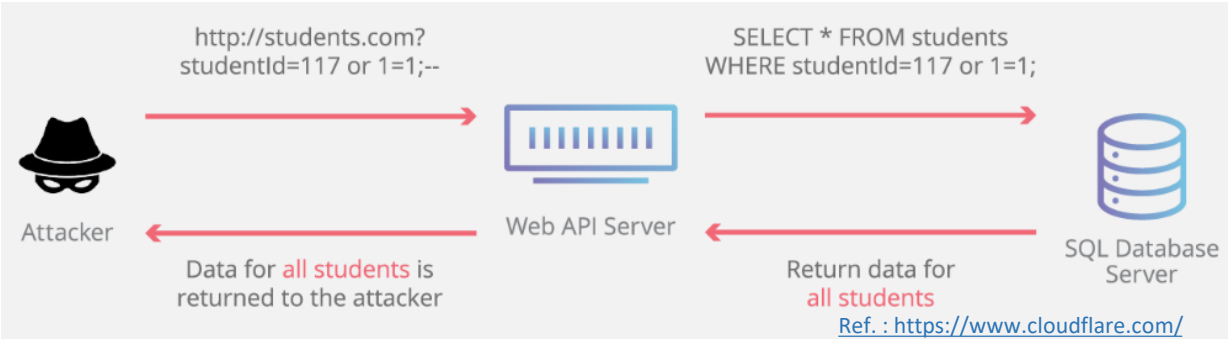
OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – 인젝션	→	A1:2017 – 인젝션
A2 – 취약한 인증과 세션 관리	→	A2:2017 – 취약한 인증
A3 – 크로스 사이트 스크립팅 (XSS)	↘	A3:2017 – 민감한 데이터 노출
A4 – 안전하지 않은 직접 객체 참조 [A7 항목과 병합됨]	∪	A4:2017 – XML 외부 개체 (XXE) [신규]
A5 – 잘못된 보안 구성	↘	A5:2017 – 취약한 접근 통제 [합침]
A6 – 민감한 데이터 노출	↗	A6:2017 – 잘못된 보안 구성
A7 – 기능 수준의 접근 통제 누락 [A4 항목과 병합됨]	∪	A7:2017 – 크로스 사이트 스크립팅 (XSS)
A8 – 크로스 사이트 요청 변조 (CSRF)	☒	A8:2017 – 안전하지 않은 역직렬화 [신규, 커뮤니티]
A9 – 알려진 취약점이 있는 구성요소 사용	→	A9:2017 – 알려진 취약점이 있는 구성요소 사용
A10 – 검증되지 않은 리다이렉트 및 포워드	☒	A10:2017 – 불충분한 로깅 및 모니터링 [신규, 커뮤니티]

Ref. : OWASP Top 10 Project

● **OWASP 10대 위협 'A1 : 2017 - 인젝션'**

인젝션은 공격자가 악의적으로 주입한 데이터를 웹 애플리케이션에서 데이터베이스의 정상적인 쿼리 일부로 인식하고 실행할 때 발생하는 취약점으로, 데이터를 입력받거나 데이터베이스 정보를 요청하는 곳에는 인젝션 공격이 가능하다. 공격방법이나 사용언어에 따라 인젝션의 종류가 달라지는데, SQL 인젝션, HTML 인젝션, OS command 인젝션, LDAP 인젝션 등이 있다.

SQL(Structured Query Language) 인젝션은 SQL 데이터베이스에서 데이터를 수정하거나 검색하는 데 사용되는 코드 삽입 기술이다. 공격자가 특정 SQL 명령을 실행하면 권한이 없는 사용자가 기존 데이터를 변경하고 트랜잭션 및 균형을 수정하고 모든 서버 데이터를 검색 및 / 또는 파기 할 수 있다. 가장 심각한 형태의 SQL 인젝션은 공격자가 기계에 대한 루트 액세스 권한을 얻고 완벽한 제어 권한을 부여하는 것이다.



<정상 SQL 쿼리> : 학생 ID에 '117'을 입력하면, 특정 학생 기록만을 반환한다.

<SQL 인젝션 쿼리> : 학생 ID에 '117 or 1=1'을 입력하면, or 이하의 '1=1'이 항상 참이므로 데이터베이스는 학생 테이블의 모든 데이터를 공격자에게 반환한다.

취약점 확인 방법

애플리케이션은 아래와 같은 경우 공격에 취약합니다.

- 사용자 제공 데이터가 유효하지 않거나, 필터링 되어지지 않거나, 애플리케이션에 의해 정제되지 않습니다.
- 상황 인식 기반 필터링 없이 동적 쿼리나 매개 변수화 되지 않은 호출이 인터프리터에서 직접 사용됩니다.
- 악의적인 데이터가 객체 관계형 매핑(ORM) 검색 매개 변수 내에서 사용되어 추가로 민감한 정보를 추출합니다.
- 악의적인 데이터가 직접적으로 동적 쿼리 안에 포함된 구조적 데이터와 악의적 데이터를 포함한 명령어, 일반 명령어, SQL, 저장 프로시저에 사용되거나 연결됩니다.

보다 일반적으로 SQL, NoSQL, 운영체제 명령어, ORM(Object Relational Mapping), LDAP, EL(Expression Languages), OGNL(Object Graph Navigation Library) 인젝션이 있습니다. 이 개념은 모든 인터프리터 간에 동일합니다. 애플리케이션이 인젝션에 취약한지 판별하기 위해선 소스코드를 리뷰하는 것과 더불어 모든 파라미터, 헤더, URL, 쿠키, JSON, SOAP, XML 데이터 입력에 대한 철저한 자동화 테스트가 가장 좋은 방법입니다. 기관은 정적 애플리케이션 보안 테스트(SAST)와 동적 애플리케이션 테스트(DAST) 툴을 CI/CD 파이프라인에 포함시켜 새로운 인젝션 결함을 운영 시스템 배포 전에 발견할 수 있습니다.

보안 대책

인젝션을 예방하기 위해서는 데이터를 지속적으로 명령어와 쿼리로부터 분리시켜야 합니다.

- 기본 옵션은 인터프리터 사용을 피하거나 매개변수화된 인터페이스를 제공하는 안전한 API를 사용하거나 ORMs 툴을 사용하도록 마이그레이션 하는 것입니다.
  주의 : 매개변수화 된 경우에도 PL/SQL이나 T-SQL과 데이터/쿼리가 연결되거나 악의적인 데이터가 EXECUTE IMMEDIATE 또는 exec()와 함께 실행된다면 저장 프로시저는 여전히 SQL 인젝션을 실행할 수 있습니다.
- 서버측 "화이트리스트"나 적극적인 입력값 유효성 검증을 하십시오. 하지만 많은 애플리케이션이 모바일 애플리케이션을 위한 텍스트 영역이나 API와 같은 특수 문자를 필요로 하기에 완벽한 방어책은 아닙니다.
- 남은 동적 쿼리들을 위하여 특정 필터링 구문을 사용하여 인터프리터에 대한 특수 문자를 필터링 처리하십시오.
  주의 : 테이블, 컬럼 이름 등과 같은 SQL 구조는 필터링 처리를 할 수가 없기 때문에 사용자가 제공한 구조 이름은 안전하지 않습니다. 이는 보고서 작성 소프트웨어의 일반적인 문제입니다.
- LIMIT과 다른 SQL 컨트롤 쿼리를 사용하여 SQL 인젝션으로 인한 대량 노출을 예방하십시오.

소프트웨어 개발 및 테스트 가이드

● 소프트웨어 개발보안의 필요성

소프트웨어 개발보안은 사이버공격의 원인인 보안약점(개발자의 실수, 논리적 오류 등)을 SW개발단계에서 사전에 제거하고 SW 개발 생명주기(SDLC) 의 각 단계별로 수행하는 일련의 보안활동을 통하여 안전한 SW를 개발·운영하기 위한 보안활동이다. 안전한 소프트웨어를 개발 및 도입하기 위해서는 프로젝트에 참여하는 각 구성원들의 역할과 책임이 명확하게 정의되어야 하며, 소프트웨어 개발 생명주기의 각 단계에 보안활동이 수행되어야 하며, 개발보안을 위한 표준이 확립되어야 한다. 2016년 12월에 개정·고시된 '행정기관 및 공공기관 정보시스템 구축·운영 지침(행정자치부고시 제 2016-48호)'은 개발보안과 관련하여 행정기관 및 공공기관이 정보화사업을 추진할 경우 준수해야 할 SW개발보안 기준 및 절차 등이 정의되어 있다. [출처 : 행정자치부, SW 개발 보안 가이드라인]

● 한국선급 해상 사이버보안 인증 검사항목(CS1)

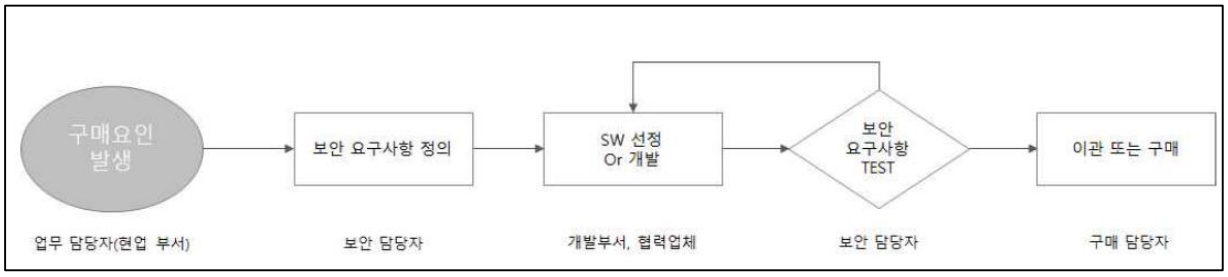
개발 및 테스트 절차 수립(212.1) : 소프트웨어 및 응용프로그램의 도입 전 보안 테스트를 실시하기 위한 절차를 수립하여야 한다.

테스트 수행(212.2) : 소프트웨어 테스트를 통해 결함을 확인하고 테스트를 통과하지 못한 경우 실제 운영시스템에 적용을 금지하여야 한다.

테스트 수행(212.3) 테스트 수행을 위한 테스트환경을 구축하고 절차에 따라 테스트를 실시한다.

운영환경 이관(212.4) : 테스트를 통과한 소프트웨어는 적용 전 책임자의 승인 획득 후 운영시스템에 적용하여야 한다.

● 소프트웨어 보안성 검토 절차 (예시)



● 소프트웨어 도입 시 보안성 점검 체크리스트 (예시)

SW 애플리케이션 도입 시 보안성 검토사항	점검결과	비고
접근제어		
특정 호스트/네트워크만 접속 제한을 할 수 있는가?		
접속 유지시간을 설정할 수 있는가?		
원격접속은 암호화할 수 있는 기능이 있는가?		
사용자 인증		
패스워드의 최소문자를 제한할 수 있는 기능이 있는가?		
잘못된 로그인 시도 시 해당 계정 잠금 기능이 있는가?		
패스워드는 특수문자를 포함하도록 설정하는 기능이 있는가?		
패스워드는 주기적으로 변경하도록 설정하는 기능이 있는가?		
보안기능		
익명접속을 제한하는 기능이 있는가?		
로그인 시간 제한기능이 있는가?		
백업 및 복구 기능이 있는가?		
가용성		
무결성을 점검하는 기능이 있는가?		
애플리케이션외 불필요 서비스를 제한할 수 있는가?		
시간동기화 기능이 있는가?		
소프트웨어 업데이트 기능이 있는가?		
관리 및 모니터링		
로그인 실패 및 성공로그를 설정할 수 있는가?		
프로세스 추적기능을 설정할 수 있는가?		
권한사용 감사를 설정할 수 있는가?		

● 소프트웨어 취약점 진단 절차 (예시)

단계	예시
대상선정	SW 코드 중 필수 모듈 XX개
체크리스트 작성	체크리스트 개발 시 OS, 버전 등 고려
진단 수행	필수 진단 모듈 및 Common 모듈 대상 점검
진단결과 분석	진단 결과 작성 및 분석
대응 방안 도출	진단결과에 대한 대응 방안 마련
이행점검	취약한 소스에 대한 조치 여부 확인
보고서 작성	진단 결과 보고서 작성

용어 설명

- **NIST Cybersecurity Framework** : 미국의 표준기술연구소(NIST)에서는 2014년 사이버보안향상법(Cybersecurity Enhancement Act)에 따라 보안 프레임워크를 만들냈으며, 2018년 4월 버전 1.1을 발표했다. 프레임워크는 사이버보안이 물리적 사이버 및 인적 차원에 미치는 영향을 포함하여 사이버보안을 해결할 수 있는 유연한 방법을 제공한다. 이 프레임워크는 정보기술(IT), 산업 제어 시스템(ICS), 사이버 물리 시스템(CPS), 사물인터넷(IoT) 기술에 의존하는 조직에 적용가능하다.
- **e-Navigation** : 기존의 선박운항 관리 기술에 첨단 정보통신기술을 융복합하여 선박에서는 실시간 해양안전정보를 자유롭게 활용하여 안전운항을 도모하고, 육상에서는 첨단화된 선박 모니터링 기술을 통해 선박의 안전운항을 원격지원하기 위한 차세대 해양안전종합관리체계를 의미한다.
- **블록체인(Blockchain)** : 블록체인은 거래 내역이 담긴 장부를 거래에 참여한 모든 구성원에게 분산하여 저장하는 기술이다. 거래 내역을 한 곳에 모아 저장하는 방식이 아닌, 그 블록체인의 이용자들 모두에게 분산 저장하므로 위변조 위험이 적고 데이터 보호 비용도 줄일 수 있다. 블록은 일정 시간 동안의 거래 내역 뿐 아니라, 이전에 생성된 블록을 암호화한 결과도 함께 저장한다. 이전 블록과 현재 블록, 그리고 미래 블록이 사슬(Chain)로 연결되어 있으므로, 블록이 길어질수록 보안성이 강화되는 특징이 있다.
- **SDLC(Software Development Life Cycle)** : 소프트웨어 개발 수명 주기란, 시스템 엔지니어링, 정보 시스템, 소프트웨어 공학 분야에서 정보 시스템의 계획 및 개발, 테스트, 유지보수, 폐기와 같은 일련의 과정 혹은 주기를 나타낸다. 소프트웨어 개발 보안 또는 시큐어 코팅이란 안전한 소프트웨어 개발을 위해 소스 코드 등에 존재할 수 있는 잠재적인 보안 취약점을 제거하고, 보안을 고려하여 기능을 설계 및 구현하는 등 소프트웨어 개발 과정에서 지켜야할 일련의 보안 활동을 말한다.