2017

해상 사이버보안 가이드라인

Ver 1.0

한 국 선 급

서문

본 해상 사이버보안 가이드라인은 선박과 회사가 도입해 운영하는 IT 기술과 서비스에 대해 내외부의 사이버 위협으로부터 안전성을 강화하기 위한 제언의 목적으로 제작되었습니다.

이에 따라 본 가이드라인에서 제시하는 권고 및 정보는 전적으로 사용자의 위험 부담 하에 사용하는 것을 전제로 제공되는 것입니다. 이 가이드라인에 명시된 정보, 서비스, 프로세스를 포함하여 문서 내용의 정확성, 완전성, 적합성 또는 유용성에 대해 어떠한 대표성이나 보증은 주어지지 않으며, 어떠한 관리 의무 또는 책임도 한국선급은 지지 않음을 인지하기 바랍니다.

이 가이드라인은 선박과 회사가 취하는 사이버보안에 대한 개별적인 심사 및 검사를 위한 기반을 제공하지 않으며 단순한 사이버 물리 시스템이 탑재된 선박에 충분히 적용이 가능하지만, 복잡한 사이버 물리 시스템을 갖춘 선박은 더 높은 수준의 관리를 필요로 하며 사이버보안 전문가 또는 회사를 통해 추가 지원을 받아야 합니다.

차 례

제 1 장 일반사항 ····· 1

제 1 절 개요 ····· 1

101. 작성배경 ····· 1

102. 목적 ····· 1

103. 적용 및 범위 ····· 1

104. 사이버위협 ····· 1

105. 정의 ····· 2

106. 참고 문헌 ····· 2

제 2 장 리스크 평가 ····· 4

제 1 절 개요 ····· 4

101. 일반사항 ····· 4

제 2 절 사이버보안 리스크 평가 ····· 4

201. 정보자산의 식별과 고려사항 ····· 4

202. 취약성 식별 ····· 5

203. 사이버보안 리스크분석 ····· 6

204. 리스크 감소 방안 식별 ····· 6

205. 리스크 평가 결과와 사이버보안 강화 ····· 7

제 3 장 리스크 관리 ····· 8

제 1 절 개요 ····· 8

101. 일반사항 ····· 8

제 2 절 사이버보안 조직의구성과 운영 ····· 8

201. 조직 구성 및 운영 ····· 8

202. 사이버보안 위원회 ····· 9

제 3 절 사이버보안 인식제고 및 교육 ····· 9

301. 교육 계획 ····· 9

302. 교육 대상 ····· 9

303. 교육 내용 및 방법 ····· 10

304. 교육 시행 및 평가 ····· 10

제 4 절 기술적 보안 활동 ····· 10

401. 접근통제 정책 ····· 10

402. 네트워크 접근통제 ····· 11

403. 접근권한 관리 ····· 11

404. 인증 및 식별 ····· 11

405. 통신 암호화 ····· 12

406. 암호화 관리 ····· 12

407. 보안성 심의 ····· 12

제 5 절 관리적 보안 ····· 13

501. 인적 보안 ····· 13

502. 운영절차 관리 ····· 14
503. 시스템 및 서비스 운영 보안 ····· 14
504. 패스워드 및 권한 관리 ····· 16
505. 이동식 저장매체 관리 ····· 17
506. 악성코드 대응 ····· 18
507. 로그 관리 및 모니터링 ····· 19
508. 지속적인 검토 및 검증 ····· 19
제 6 절 물리적 보안 ····· 19
601. 보호구역 통제 ····· 19
602. 출입 및 물품통제 ····· 20
603. 설비 및 시설관리 ····· 21
604. 환경보안 ····· 22

제 4 장 사이버보안 사고 대응 ····· 23

제 1 절 개요 ····· 23
101. 일반사항 ····· 23
제 2 절 대응 ····· 24
201. 사고 대응 계획 ····· 24
202. 사고의 대응 ····· 24
203. 사이버보안 사고 결과보고 ····· 25
제 3 절 사이버보안 사고 사후관리 ····· 25
301. 사이버보안 사고 분석 및 공유 ····· 25
302. 사이버보안 사고 재발 방지 ····· 26

제 5 장 복구관리 ····· 27

제 1 절 개요 ····· 27
101. 일반사항 ····· 27
제 2 절 복구 ····· 27
201. 복구 계획 ····· 27
202. 복구 절차 ····· 27
203. 개선 ····· 28

부록 1 OT 시스템 매핑

제 1 장 일반사항

제 1 절 개요

101. 배경

1. 정보통신기술(ICT)의 발전이 지속됨에 따라 선내 운영기술(OT)과 정보기술(IT)이 접목되어 업무효율을 극대화시키고 있다. 그러나 선박과 회사의 업무 환경의 변화는 선박 시스템으로의 비인가된 접근 또는 악성코드 감염과 같은 사이버보안 사고 발생 가능성을 높이는 요인이 될 수도 있다.
2. 사이버보안 사고에 대한 예방이나 대응 절차의 부재는 안전, 환경 및 상업적으로 중대한 피해를 야기할 수 있다. 증가하는 사이버 위협에 대응하여 다양한 이해관계자의 지원을 받는 국제 해운조직들은 선박 또는 회사의 사이버보안에 대한 탄력적인 접근법을 개발할 수 있도록 돕기 위해 가이드라인들을 개발하였다.
3. 이 사이버보안 가이드라인은 선박 및 회사에 특화되어 있지만, 적절한 표준 및 관련 규정의 요구사항을 포함하고 있다.
4. 이 가이드라인은 사이버 위협에 대한 식별 및 대응을 위하여 리스크 기반 접근법을 제공한다.

102. 목적

이 문서는 선주, 관리자, 운영자에게 그들의 선박 및 회사 시스템의 사이버보안을 유지하고 강화하기 위해 필요한 절차 및 조치를 만들고 사이버보안 시스템의 운영을 평가하기 위한 실질적인 가이드라인을 제공한다.

103. 적용 및 범위

이 가이드라인은 선박과 운영 회사의 정보기술 및 운영기술 시스템에 적용하기 위해 개발되었다.

104. 사이버 위협(Threat)

1. 이 가이드라인에서 다루는 회사 및 선박의 시스템에 대한 일반적인 사이버보안 공격의 유형은 아래와 같다.
   (1) 악성 코드(Malware) : 트로이 목마, 바이러스 및 웜 또는 랜섬웨어와 같이 정당한 인지 또는 허가 없이 컴퓨터 시스템에 접속하거나 데이터 또는 프로그램 등을 훼손, 변경, 위조하거나 운영 방해 등 악성행위를 위해 고안된 악성 소프트웨어로 구식 또는 패치 되지 않은 소프트웨어의 알려진 결함 또는 문제점을 악용할 수 있다. 또한 악성 코드는 시스템의 취약점, 부적절한 설계, 하드웨어 오작동 및 프로토콜 구현상의 오류 등의 취약점을 통해 원격으로 또는 현장에서 시스템을 작동 시킬 수 있다. 일반적으로 악성 코드는 링크를 통해 사용자가 실행하거나 전자 메일 첨부 파일이나 악성 웹 사이트를 통해 배포된다.
   (2) 소셜 엔지니어링(Social engineering) : 잠재적인 사이버 공격자가 주로 소셜 미디어 등을 통하여 인간 상호작용의 신뢰를 바탕으로 내부 개인을 속여 보안절차를 파기하는데 사용되는 비기술적 침입 수단으로 피싱, 파밍, 스미싱 등이 대표적인 소셜 엔지니어링 기법에 속한다.
   (4) 워터 홀링(Water holing) : 가짜 웹 사이트를 구축하거나 방문자를 부당하게 이용하기 위하여 진짜 웹사이트를 손상시키는 행위를 말한다.
   (5) 스캐닝(Scanning) : 특정 또는 불특정 네트워크나 시스템을 대상으로 사이버 공격을 수행하기 위해 시스템의 특성을 파악하기 위한 행위로 해킹의 사전 단계이다.
   (6) 랜섬웨어(Ransomware) : 컴퓨터 시스템의 소유자의 허가 없이 시스템 내 일부 또는 전체 데이터를 암호화 시켜 정보에 대한 접근을 제한하고 해커가 지정한 계좌로 송금을 하여야 암호를 풀어주는 금품 갈취형 악성 프로그램을 말한다.
   (7) 서비스 거부(DoS) 공격 : 시스템을 악의적으로 공격해 해당 시스템의 자원을 부족하게 하

여 원래 의도된 용도로 사용하지 못하게 하는 공격으로, 수단, 동기 및 표적은 다양할 수 있으나 인터넷 사이트 또는 서비스 기능을 일시적 또는 무기한으로 방해 또는 중단을 초래한다.

(8) 무작위 대입(Brute force) : 비인가된 공격자가 특정 시스템의 접속 목적을 위해 올바른 암호가 발견될 때까지 가능한 모든 암호를 대입하는 공격 방식을 말한다.

(9) IP 스푸핑(Spoofing) : IP 주소를 변조하거나 속여서 접근제어목록(ACL : Acess Control List)를 우회하거나 회피하여 공격하는 방식을 말한다.

(10) 스니핑(Sniffing) : 네트워크 통신과정에서 다른 상대방의 패킷 정보를 도청하는 공격 방식을 말한다.

(11) 홈페이지 변조(Homepage Modulation) : 특정 홈페이지에 접속했을 때 화면을 원래의 것과 다르게 바꿔 놓는 악의적인 공격 행위를 말한다.

2. 위에서 언급된 내용은 최근 등장하고 있는 위협과 공격기법의 일부 예시로 사이버 위협과 공격 유형은 공격자에 의해 다양하게 등장하고 있으며, 공격에 사용되는 기법은 정교해지고 있음을 인지하여야 한다.

105. 정의

1. **사이버보안**이라 함은 정보 및 통신 시스템과 그에 포함된 정보가 손상, 무단 사용 또는 수정되지 않도록 보호하는 활동 또는 프로세스, 역량 등을 말한다.
2. **사이버 물리 시스템**이라 함은 센서와 액추에이터를 갖는 물리시스템과 이를 제어하는 컴퓨팅 요소가 결합된 네트워크 기반 분산제어 시스템을 말한다.
3. **정보기술**이라 함은 컴퓨터, 네트워킹 장치, 프로세스 등 데이터를 생성, 검색, 처리, 저장 및 전송에 사용되는 자동화 시스템을 말한다.
4. **운영기술**이라 함은 밸브, 펌프 등과 같이 물리적 장치와 프로세스 등을 직접적으로 모니터링 및/또는 제어하는 자동화 시스템을 말한다.
5. **악성코드**라 함은 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 프로그램을 말한다.
6. **사이버보안 사고**라 함은 외부 또는 내부의 악의적인 사용자에 의한 비인가된 시스템 사용, 사용자 계정 도용, 악성코드 유입 및 실행, 사이버보안 시스템 방해 등 회사나 선박 시스템의 서비스를 왜곡 또는 지연시키거나 시스템을 파괴, 데이터를 변조, 삭제하는 등의 행위를 말한다.
7. **취약성**이라 함은 시스템의 기능 명세, 설계 또는 구현 단계의 오류나 시동, 설치 또는 운용상의 문제점으로 인하여 시스템이 지니게 되는 보안상의 약한 부분을 말한다.
8. **기밀성**이라 함은 자산이 인가된 당사자에 의해서만 접근하는 것을 보장하는 것을 말한다.
9. **무결성**이라 함은 자산이 인가된 당사자에 의해서 인가된 방법으로만 변경 가능한 것을 말한다. 이는 자산의 완전성과 정확성을 보장하는 것을 의미한다.
10. **가용성**이라 함은 자산이 적절한 시간에 인가된 당사자에게 접근 가능해야 하는 것을 말한다.
11. **이동식 저장매체**라 함은 디스켓, 외장형 하드디스크, USB 메모리, CD, DVD 등 자료를 저장할 수 있는 일체의 것으로 서버, PC 시스템과 분리할 수 있는 기억장치를 말한다.
12. **외부자**라 함은 회사와 계약에 의해 장비, 용역 및 서비스를 제공하는 외부 전문가, 장비공급업체 및 외부용역업체, 기타 회사의 사이버보안 관련 자산에 접근이 허용된 자 및 업체를 말한다.
13. **책임추적성**이라 함은 시스템 내 각 개인은 유일하게 식별되어야 한다는 정보보호 원칙 하에 정보처리시스템은 누가, 언제, 어떠한 행동을 하였는지 기록하여 필요 시 그 행위자를 추적할 수 있게 하여 정보보호 규칙을 위반한 개인과 그 행위에 대하여 책임을 지도록 한다.

106. 참고 문헌

1. National Institute for Science and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, Feb 2014.
2. BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI The Guidelines on

Cyber Security Onboard Ships, July 2017
3. ISO/IEC 27001:2013 - Information Technology - Security techniques - Information security management systems - Requirements, Sept 2013.
4. International Maritime Organization (IMO) MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management, July 2017.
5. Korea Internet & Security Agency (KISA) Guidelines for Information Security Management System Certificate Application, July 2016.

제 2 장 리스크 평가

제 1 절 개요

101. 일반사항

1. 사이버보안 리스크 평가의 목적은 식별된 선박 및 회사의 자산에 대한 사이버보안 수준을 지속적으로 향상시키기 위한 기반을 마련하기 위함이다.
2. 선박 및 회사의 주요 시스템 중 위협에 취약한 부분을 식별하고 사이버 위협에 대한 리스크 감소 방안을 마련하여 사이버보안을 강화하기 위해 구조화되고 체계적인 리스크 평가 방법론을 사용한다.

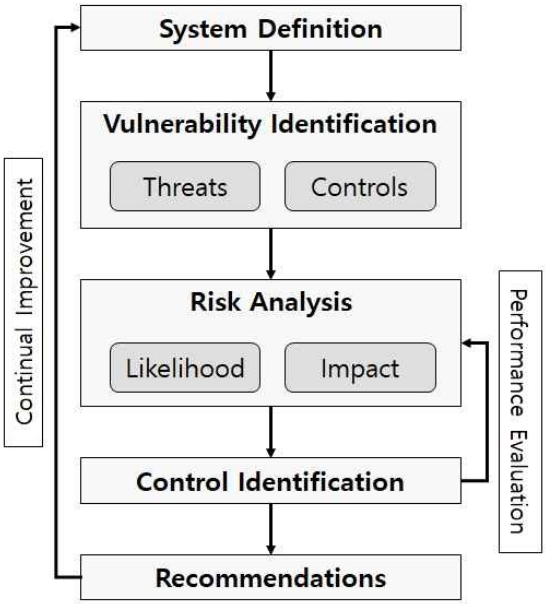

그림 1 사이버보안 리스크 평가 절차

3. 체계적인 사이버보안 리스크 평가를 통하여, 선박 및 회사의 주요 시스템에 대한 사이버보안 리스크 수준을 확인하고, 목표로 하는 리스크 수준과의 차이(Gap)를 분석하여 사이버보안 수준을 향상시킬 수 있도록 전략적 결정을 수행하여야 한다.

제 2 절 사이버보안 리스크 평가

201. 정보자산의 식별과 고려사항

1. 사이버보안 리스크 평가를 위한 첫 번째 단계에서는, 리스크 평가 대상에 대한 명확한 이해를 위하여 필요한 모든 정보를 수집하고 리스크 평가 목적, 범위 및 리스크 허용 수준 등 리스크 평가 작업을 위하여 필요한 모든 사항들을 정의한다.
2. 사이버보안 리스크 평가 작업을 위하여 최소한 다음과 같은 정보들을 준비하여야 한다.
   (1) 네트워크 구성(Network topology) 및 구역 분류(Zone or Node)
   (2) 대상 시스템 정보(소프트웨어/하드웨어 목록, 시스템 인터페이스, 주요 IT/OT 시스템)
   (3) 리스크 허용 기준
3. 네트워크 구성도는 평가대상 시스템을 쉽게 이해할 수 있도록 작성되어야 하며, 구역 분류를 위한 정보를 제공하여 취약성 분석 작업 시 체계적으로 시스템을 검토할 수 있도록 하여야 한다.

4. 일반적으로, 독립형(Stand-alone) 시스템은 직접 인터넷에 연결된 시스템이나 제어되지 않은 네트워크에 연결된 시스템에 비해 상대적으로 사이버 공격에 덜 취약할 수 있다. 하지만 그럼에도 불구하고 네트워크를 통해 선박 시스템이 제어되지 않은 네트워크에 연결될 수 있는 가능성과 특히 인적 요인과 관계된 사항들에 주의를 기울여야 한다.
5. 리스크 평가 시 고려되어야 할 주요 선내 시스템과 잠재적 위협 대상은 다음과 같다.
   (1) 화물 관리 시스템: 위험 화물을 포함한 화물의 관리 및 제어용 디지털 시스템은 육상의 다양한 시스템과 연계된다. 그러한 시스템들은 인터넷을 통하여 화주가 사용 가능한 선적 추적 도구가 포함될 수 있다. 이러한 종류의 인터페이스들은 화물 관리 시스템 및 화물 적하 목록 상의 데이터를 사이버 공격에 노출시킬 수 있다.
   (2) 선교 시스템: 서비스 제공 및 업데이트를 위해 육상 네트워크와 연계된 디지털, 네트워크 네비게이션 시스템 사용의 증가는 사이버 공격의 증가로 이어질 수 있다. 다른 네트워크와 연결되지 않은 선교 시스템들은 제어 또는 제어되지 않은 네트워크로부터 그들 시스템을 업데이트 하는데 사용되는 이동식 저장장치들로 인해 동등하게 취약할 수 있다. 사이버보안 사고는 서비스 거부 혹은 조작 등으로 확대 될 수 있으며, 따라서 ECDIS, GNSS, AIS, VDR 및 Radar/ARPA를 포함한 선박 항해와 연계된 모든 시스템들에게 영향을 미칠 수 있다.
   (3) 추진, 기관 관리, 전력 제어 시스템: 선내 기관, 추진, 조종 모니터링 및 제어를 위한 디지털 시스템의 사용은 사이버 공격에 취약할 수 있는데 특히 시스템들의 취약성은 원격 상태기반 모니터링과 함께 사용되거나 통합 선교 시스템을 사용하는 선박 항해 및 통신장비와 통합될 때 증가할 수 있다.
   (4) 접근 제어 시스템: 감시, 선내 보안 알람, 전자 인사관리 시스템을 포함한 선박의 물리적 보안 및 선박, 화물의 안전을 보장하기 위해 접근 통제를 지원하는 디지털 시스템
   (5) 승객 서비스와 관리 시스템: 재산관리, 탑승 및 접근 통제에 사용되는 디지털 시스템은 승객과 관련된 귀중한 데이터를 가질 수 있다.
   (6) 공용 네트워크에 연결된 승객: 승객의 편의를 위하여 선내 설치된 고정/무선 인터넷 연결 네트워크를 의미한다. 이들 네트워크는 제어되지 않은 시스템으로 간주되어야 하며, 선내에서 어떠한 주요 안전 시스템과도 연결되어서는 아니 된다.
   (7) 관리자 및 선원 복지 시스템: 선박 관리 또는 선원 복지용 선내 컴퓨터 네트워크는 인터넷 접근과 이메일 서비스를 제공할 때 위험에 노출될 수 있다. 이들 시스템이 선내 시스템 및 데이터로의 접근을 얻기 위해 사이버 공격자에 의해 이용 될 수 있다. 이러한 시스템은 제어되지 않은 시스템으로 간주하고 선내 어떠한 주요 안전 시스템과도 연결되어서는 아니 된다.
   (8) 통신 시스템: 위성 또는 다른 무선 통신을 이용한 인터넷 연결의 가용성은 선박의 위험을 증가시킬 수 있다. 서비스 제공자에 의해 구현된 사이버보안 메커니즘은 신중하게 고려되어야 하지만 모든 선상 시스템 및 데이터를 보호하기 위하여 전적으로 의존해서는 아니 된다.
6. 리스크 허용 기준은 사이버보안 목표 수준과 평가 결과 나타난 리스크 수준을 비교하기 위한 척도로, 리스크 허용 기준을 설정함에 있어 주의를 기울여야 한다. 리스크 허용 기준 설정을 위하여 기존 사이버보안 사고 데이터, 산업계에서 통용되는 리스크 허용 기준, 선박산업 동향 및 선박회사의 정책 등 다양한 자료들을 고려하여야 한다.

202. 취약성 식별

1. 취약성 식별 작업은 사이버 위협과 그로 인한 영향 및 사이버 리스크 완화 방안을 식별하는 작업으로, 각 IT & OT 시스템에 대한 사이버 위협의 다양한 시나리오들을 식별할 수 있다.
2. 취약성 식별 작업은 시스템 정의 단계에서 식별된 구역 분류(zone, node)들의 각 시스템별 사이버 위협 위험요소, 그로 인한 영향, 이미 적용된 리스크 감소 방안 및 추가 적용 가능한 방안을 식별하여 발생 가능한 모든 사이버보안 사고 시나리오 목록을 작성한다.
3. 대상 시스템의 취약성을 체계적으로 식별하기 위해 "그림 2 리스크 매트릭스"를 사용할 수 있다.
4. 사이버보안에 대한 리스크 감소 방안 및 통제 관련 사항은 **제 3장** 리스크 관리를 참고한다.

203. 사이버보안 리스크 분석

1. 리스크 분석은 식별된 사이버보안 위협 시나리오들의 리스크를 정성적 또는 정량적으로 표현하기 위한 작업으로, 선박과 회사의 사이버보안 리스크를 확인하고 시스템 내부 사이버 위협에 취약한 부분을 검토할 수 있게 한다.
2. 정성적 리스크 분석 방법으로 빈도 지수(LI: Frequency/Likelihood Index)와 심각도 지수(SI: Severity Index)를 리스크 지수(RI: Risk Index)로 표현하는 리스크 매트릭스(Risk Matrix)를 사용할 수 있다. 또한 충분한 데이터가 준비되어 있을 경우, 널리 통용되는 증명된 리스크 분석 기법을 사용하여 정량적 분석을 수행할 수 있으며, 이외에도 회사가 보유한 고유의 리스크 분석 방법을 적용하여도 무방하다.

			Impact				
		SI	1	2	3	4	5
	LI		Insignificant	Minor	Moderate	Major	Significant
Likelihood	5	Certain	5	10	15	20	25
	4	Likely	4	8	12	16	20
	3	Moderate	3	6	9	12	15
	2	Unlikely	2	4	6	8	10
	1	Rare	1	2	3	4	5

그림 2 리스크 매트릭스 예시

3. 사이버 위협의 발생 빈도(Likelihood)와 사이버 위협으로 인한 영향(Impact)을 결합하면 사이버보안의 리스크가 결정된다.
4. 사이버 위협 발생 빈도 등급 선정(Ranking) 시에는 접근 용이성(Ease of access)을 충분히 고려하는 것이 효과적이다. 예를 들어, 원격 인터넷 연결을 통해 업데이트 또는 제어할 수 있는 시스템은 독립형 시스템보다 쉽게 접근이 가능하다. 접근 용이성 결정을 위해 다음 사항들을 고려한다.
   (1) 원격 연결: 선박이 아닌 곳에서의 시스템 접근. 예를 들어 육상 운영 센터 또는 장비 공급업체의 육상 모니터링 시스템에 대한 원격 연결이 포함된다.
   (2) 물리적 접근 가능성: 선박 내부의 장비에 접근. 예를 들면 잠금 해제 된 캐비닛 도어 및 장비가 위치한 곳에서의 쉬운 조작 가능성.
   (3) 연결 및 통합: 네트워크를 통해 다른 시스템과 연결된 시스템. 일반적으로, 시스템을 통합하거나 인터페이스를 만들기 위해 정보 공유 및 중앙 집중식 관리 방식을 사용한다.
5. 사이버 위협으로 인한 영향은 보안 3요소 즉, 기밀성(C: Confidentiality), 무결성(I: Integrity), 가용성(A: Availability)을 고려하여 등급 매김을 하며, 세 가지 보안 속성 등급(보안 속성 중 가장 높은 등급 고려)과 사이버 위협 발생 빈도가 결합되어 사이버 시스템의 리스크 등급이 결정된다.

204. 리스크 감소 방안 식별

1. 사이버 위협 시나리오가 식별되고 관련 시나리오 별 현재 적용된 리스크 감소 방안들이 식별되면, 추가 리스크 감소 방안의 필요성을 검토하여 새로운 방안을 제안한다.
2. 리스크 감소 방안은 사이버 위협의 발생 빈도를 줄일 수 있는 방안과 사이버 위협으로 인한 영향을 최소화 할 수 있는 방안으로 구분할 수 있다.
3. 식별된 각 시나리오 중 리스크가 리스크 허용 기준을 초과하거나 또는 목표하는 사이버보안 리

스크 수준보다 높게 나타난 시나리오들은 관련 리스크 수준을 낮출 수 있도록 적절한 감소 방안을 마련하여야 한다. 리스크 감소 노력이 필요한 곳을 선별하기 위하여 일반적으로 고려하는 사항은 다음과 같다.

(1) 리스크 수준(Risk levels) : 발생 빈도와 영향을 고려하여 측정 또는 평가된 정도
(2) 발생 가능성(Probability) : 사고로 인한 피해의 심각성과는 별개로, 실제로 발생할 수 있는 가능성의 정도
(3) 사고 심각성(Severity) : 사고의 발생 가능성과는 별개로, 발생 시 피 피해 규모의 정도
(4) 신뢰성(Confidence) : 발생 빈도 또는 사고 영향에 대하여 불확실성이 높은 리스크 모델이 적용된 시나리오에 대한 충분한 검토.

4. 새로운 리스크 감소 방안을 제안할 경우에는 리스크 감소 방안에 적용되는 비용과 적용함으로써 얻게 되는 효과를 고려하여야 한다.
5. 제안된 모든 리스크 감소 방안들과 관련하여, 적용 시 얻게 되는 사이버보안 효과와 발생 가능한 부작용(Side effect)들이 평가되어야 하고, 적용 이후 잔존하는 리스크의 처리 방안을 검토하여야 한다.

205. 리스크 평가 결과와 사이버보안 강화

1. 사이버보안 리스크 평가 결과는 선박 및 회사의 현재 사이버보안 리스크 수준과 리스크 감소가 필요한 영역, 리스크 감소를 위하여 요구되는 추가 작업들 및 리스크 감소 방안 적용 담당자를 쉽게 찾아볼 수 있도록 적절하게 문서화되어야 한다.
2. 선박 및 회사의 사이버보안 체계는 사이버보안 리스크 평가 결과를 바탕으로 사이버보안 리스크 및 사이버보안 취약 구역을 주기적으로 모니터링할 수 있도록 하는 절차가 포함되어 있어야 하며 이를 통하여 사이버보안 체계의 지속적인 개선이 가능하도록 하여야 한다.

제 3 장 리스크 관리

제 1 절 개요

101. 일반사항

1. 사이버보안은 안전하고 효율적인 선박 운영을 위하여 회사의 고위 경영층으로부터 선박 내 선원에 이르기까지의 회사 및 선박의 모든 수준에서 고려되어야 한다.
2. 사이버보안은 회사의 고위 경영층에서부터 시작되어야 하며, 이에 대한 이유는 다음과 같다.
   (1) 사이버보안 수준 향상을 위해서는 표준 사업 절차 및 운영에 영향을 미쳐 더욱 많은 시간과 비용, 인력 등 자원을 투입하게 한다. 따라서 사이버 위험과 보안 적용에 대한 균형을 평가하고 결정하는 것은 고위 경영층의 전략적 책임이다.
   (2) 사이버보안 수준 향상은 회사가 고객, 공급 업체 및 당국과 상호작용하는 방식을 변경하고 이해관계자 간 협력에 대한 새로운 요구사항을 부과할 수 있다. 때문에 이러한 관계들을 어떻게 이끌어낼지에 대한 방안은 고위 경영층에서 결정해야 한다.
   (3) 일반적으로 회사의 고위 경영층의 전략적 결정 및 위험대비 보상 절충안을 기반으로 사이버 사건 발생 시 관련 비상계획을 수립해야 한다.
   (4) 고위 경영층은 목표와 관련하여 사이버보안 정책을 수립하고, 관련 자원의 제공을 보장하며, 사이버보안의 중요성을 전달하고, 지속적인 개선을 촉진하여야 한다.
   (5) 고위 경영층은 조직 내 중요 정보 및 정보 자산을 취급하는 직무를 정의하고 업무를 수행하는 임직원을 사이버보안 담당자로 지정하고 최종 의사결정을 할 수 있는 자를 '사이버보안 최고 책임자'로 지정하여야 한다.
3. 회사는 사이버보안에 필요한 자원을 식별하고 적절히 제공하여야 한다. 검토 및 검증 시 필요하다고 요구되는 자원에 대해서는 부득이한 사유가 없는 경우 최대한 제공할 수 있어야 한다. 특히 인적 자원이 역량을 개발하고 기록을 유지하도록 보장한다.
4. 회사는 내·외부 비인가자의 침입 탐지 및 차단, 정보유출 방지 등을 위하여 보안 시스템을 도입 및 운영하고 필요한 운영절차를 수립하여야 한다.
   (1) 사이버보안 시스템에 대한 책임과 권한 지정
   (2) 사이버보안 시스템 적용(등록, 변경, 삭제 등) 절차
   (3) 지속적인 운영 검토, 검증 및 평가
   (4) SW/HW 교체, 패치, 최신 정책 등의 최신화 등 유지관리 절차
   (5) 사이버보안 시스템 이벤트 처리절차(정책에 위배되는 이상징후 탐지, 확인, 보고, 비상대응 등)
   (6) 사이버보안 시스템 접근통제 정책
5. ISO 27001, 정보보호 관리체계(ISMS : Information Security Management System) 인증과 같이 공인된 제3자의 인증은 사이버보안의 운영을 향상시키는데 있어서 좋은 방법이 될 수 있으며 회사가 가진 사이버보안의 가치를 높일 수 있다. 특히 외부 감사는 조직이 안전하지 못한 이전의 행동 패턴으로 되돌아가지 않도록 보장해줄 수 있는 좋은 수단이므로 높은 수준으로 권고한다.

제 2 절 사이버보안 조직의 구성과 운영

201. 사이버보안 조직

1. 사이버보안 위협으로부터 대응하고 사이버보안 수준을 유지 및 향상시키기 위하여 회사는 사이버보안 조직을 구성한다.
2. 회사의 고위경영자는 사이버보안 실무를 담당할 조직을 구성하고 사이버보안 책임자가 해당 조직을 운영할 수 있도록 지원하여야 한다.
3. 사이버보안 조직은 회사의 특성에 따라 조직할 수 있는데 일반적으로 보안 조직의 의사결정을

수행하는 사이버보안 최고 책임자를 통해 선박 내 사이버보안 책임자 및 담당자, 기술 분야의 실무 책임자 및 담당자, 관리·물리 분야 실무 책임자 및 담당자 등을 총괄하도록 한다.

4. 사이버보안 조직의 구성, 각 업무 담당자별 책임과 의무 등은 문서화된 형태로 고위 경영층의 검토 및 승인을 획득하여야 한다.

202. 사이버보안 위원회

1. 회사의 고위경영자는 사이버보안 활동을 검토 및 승인하기 위한 사이버보안 위원회를 운영하도록 한다.
2. 업무 관계 부서 내에는 사이버 보안 담당자를 지정하고 비상설 조직인 사이버보안 위원회를 구성하여 회사 내 사이버보안 정책과 지침이 회사 전체에 적용될 수 있도록 하여야 한다.
3. 사이버보안 위원회는 다음과 같이 구성할 수 있다.
   (1) 위원장 : 사이버보안 위원회 소집, 의안 통보 및 직무 총괄
   (2) 참석위원 : 사이버보안 책임자, 사이버보안 관리자, 사이버보안 담당자, 기술 분야 실무 책임자 및 담당자, 관리·물리 분야 실무 책임자 및 담당자
   (3) 사이버보안 위원회는 다음과 같이 운영한다.
      (가) 위원회의 회의주기는 연 1회 이상으로 하고 위원장이 필요하다고 인정할 때는 수시로 개최될 수 있다.
      (나) 위원장의 유고시에는 CEO가 지명한 위원이 그 직무를 대행한다.
      (다) 위원회의 회의는 재적의원 과반수의 출석으로 개최하고, 출석위원 과반수의 찬성으로 의결한다. 위원장은 표결권을 가지지 않으나, 가부동수일 경우에는 결정권을 갖는다.

제 3 절 사이버보안 인식제고 및 교육

301. 교육 계획

1. 평가된 리스크 분석 결과와 대응방안이 선박과 회사 내에 적절하게 적용되기 위해서는 사이버보안 교육이 병행되어야 한다. 이를 위해 회사는 다음의 항목이 포함된 사이버보안 교육 계획을 전년도 말에 수립하여야 한다.
   (1) 교육 시기(예 : 분기별, 반기별 등) 및 기간
   (2) 교육 대상
   (3) 교육 내용
   (4) 교육 방법(예 : 온라인, 집체교육 등)
   (5) 교육 결과 Feedback 방안
2. 예산 배정 및 집행 권한을 보유하고 있는 경영진(최고 경영자)은 연간 사이버보안 교육계획을 검토하고 승인하여 사이버보안 교육이 계획에 따라 이행될 수 있도록 적극 지원하여야 한다.

302. 교육 대상

1. 사이버보안 교육대상에는 사이버보안 관리체계 범위 내 관련 자산에 직간접적으로 접근하는 정규직 임직원, 임시 직원, 외주용역업체 직원 등 모든 인력을 포함하여야 한다.
2. 사이버보안 자산이 위치한 장소에 접근할 수 있는 청소원, 경비원 등에게도 기본적인 사이버보안 인식교육을 수행하여야 한다.
3. 교육대상이 하도급에 의해 파견된 직원인 경우 해당 용역업체 담당자가 사이버보안 교육을 수행할 수 있도록 관련 자료를 제공하고 지원하여야 한다.
4. 사이버보안 교육 대상에 대해서는 직무와 지식수준 등을 고려하여 내용 및 수준을 차별화하여 교육이 이루어질 수 있도록 하여야 한다.

303. 교육 내용 및 방법

1. 기본 사이버보안 교육에는 다음과 같은 내용을 포함하여야 한다.
   (1) 사이버보안의 기본 개요
   (2) 사이버보안 관리체계 구축 절차 및 방법
   (3) 사이버보안 관련 임직원이 준수하여야 할 사이버보안 관련 내부 규정 및 법률
   (4) 사이버보안 사고에 대비한 예방, 탐지 및 대응, 분석, 복구 등의 기술
   (5) 최근 사이버보안 사고 사례 및 사이버보안 관련 국내외 동향
   (6) 사이버보안 규정 위반 시 상벌규정, 법적 책임 등
2. 교육을 효과적으로 시행하기 위하여 집체교육, 이러닝교육, 부서자체교육 등 다양한 교육방법을 정할 수 있다.
3. 교육의 대상, 내용, 기간 등에 따라 효과적으로 교육을 수행할 수 있는 방법(예 : 집체교육, 온라인 교육, 전달 교육 등)을 선택하여야 한다.
4. 사이버보안 인식제고를 위하여 사이버보안의 날 지정, 포스터 또는 뉴스레터를 제작할 수도 있다.
5. IT 담당자(운영, 개발), 사이버보안 담당자는 일반 직원과 별도로 직무별 업무 수행에 필요한 사이버보안 교육을 받아야 한다. 직무별 교육은 다음과 같은 교육과정을 활용할 수 있다.
   (1) 사이버보안 관련 컨퍼런스, 세미나, 워크샵 참가
   (2) 사이버보안 관련 교육 전문기관 내 교육 수료
   (3) 외부 전문가 초빙을 통한 내부 교육 및 세미나

304. 교육 시행 및 평가

1. 경영진(최고 경영진)의 승인을 받은 사이버보안 교육 계획에 따라 정규직 임직원, 임시직원, 외주용역, 외부자 등을 대상으로 연 1회 이상 기본 사이버보안 교육을 시행하여야 한다.
2. IT 및 사이버보안 직무자는 기본 사이버보안 교육 이외에 직무별 사이버보안 교육을 별도로 연 1회 이상 이수하여야 한다.
3. 기본 사이버보안 교육 이외에 다음과 같은 상황이 발생할 경우 추가적인 사이버보안 교육을 수행하여야 한다.
   (1) 사이버보안 관련 협약 및 강제 규정 변경
   (2) 회사 내 사이버보안 관련 정책 및 절차 변경
   (3) 회사 내·외부 사이버보안 사고 발생
   (4) 업무 환경의 중대한 변화 발생(예 : 사이버보안 관리체계 범위 변경)
5. 출장, 휴가 등으로 인해 정기 사이버보안 교육에 불참한 인력에 대해 전달교육, 추가교육, 온라인 교육 등의 방법으로 사이버보안 교육을 시행하여야 한다.
6. 채용으로 인해 신규 인력 발생 시, 업무 투입 전에 사이버보안 교육을 실시하여 조직 내 사이버보안 관련 사전 지식이 없는 데 따른 보안규정 위반, 보안사고 발생의 위험수준을 낮추도록 하여야 한다.
7. 교육 시행 후, 교육 공지, 교육자료, 출석부 등과 같은 기록을 남기고 미리 마련된 평가기준에 따라 설문 또는 테스트 등을 통해 교육 내용의 적절성과 효과성을 평가하여야 한다.
8. 교육평가 결과 내용에서 도출된 문제점에 대해 개선 대책을 마련하고 차기 교육 계획 수립 시 반영하여야 한다.

제 4 절 기술적 보안 활동

401. 접근통제 정책

1. 회사, 선박 내의 네트워크, 서버, 응용 프로그램, DB, 모바일기기 등 자산별 접근통제 정책을

적용하고 보안 요구사항, 데이터 및 서비스 접근 및 분산 네트워크 상 접근권한 관리 등 법적·계약적 요건이 접근통제에 반영되어야 한다.

2. 접근통제 기능 또는 소프트웨어를 포함하여 접근통제 정책 및 절차를 수행할 수 있는 방법이 존재하고 이에 따라 적절히 운영하여야 한다.
3. 접근통제 정책을 적용할 때에는 항시 적용되는 접근통제 규칙과 일정기간 또는 선택적으로 존재하는 접근통제 규칙이 구분되어 적용되어야 한다.
4. 보안상 중요한 접근통제 규칙의 경우 관리자의 승인을 거쳐 설정 또는 변경하도록 한다

402. 네트워크 접근통제

1. 회사, 선박 내의 네트워크를 구성하는 자산들에 대한 목록 및 네트워크 구성도를 작성하여야 하며, 네트워크 구성 변경 이력을 관리하여야 한다.
2. 네트워크 담당자는 네트워크 구축 및 변경 시 시스템, 네트워크 및 라우팅 장비의 물리적 위치, 접속계정, 서비스 포트(Port) 및 IP 주소 정책 및 목록 등에 대하여 정기적으로 현황과 그 적절성을 검토하여야 한다.
3. 회사, 선박 내의 네트워크 담당자는 인가된 사용자에게만 IP 주소를 개인별로 부여하고, 내부 네트워크의 IP 주소를 사설 IP 주소로 구성하여야 하며 이를 기밀사항으로 관리하여야 한다.
4. 네트워크 구축 시에는 라우터, 스위치 또는 가상 랜(VLAN)을 통하여 실제 네트워크 리소스를 공유하는 네트워크를 여러 하위 네트워크로 분리하여 구성하도록 하여야 한다.
5. 공개용 웹서버를 내부 네트워크와 분리하여 구성할 때에는 내부 네트워크와 외부네트워크 사이 DMZ를 설치하고 내부 네트워크로의 진입 접점에는 침입차단 시스템과 같은 접근통제 시스템이 설치 운영되도록 한다.
6. 네트워크 담당자는 중요 시스템을 분류하고 중요 시스템별 관리·운영자, 개발자 및 외부자 등에 대하여 핵심 업무 특성별로 네트워크를 분리하여 관리하며, 특히 선박의 안전에 영향이 높은 제어에 사용되는 네트워크는 다른 네트워크와 별도로 분리하여 안전하게 보호하여야 한다.
7. 내부 네트워크가 아닌 외부 네트워크를 통해 내부 네트워크나 선박 네트워크로의 접근을 차단하여야 하며 불가피하게 접속이 필요한 경우 인가된 접속자를 식별하고 안전한 암호화 통신이 이뤄질 수 있도록 보안성을 강화해야 한다.
8. 선박의 안전에 영향이 높은 제어시스템을 위한 네트워크는 다른 네트워크와 별도로 구분하여 안전하게 보호하여야 한다.

403. 접근권한 관리

1. 접근권한 관리를 통하여 비인가자의 접속 시도 및 정보 획득 차단을 통하여 시스템의 기밀성, 무결성을 향상시킬 수 있다.
2. 사용자별 접근권한에 대한 등록·변경·삭제 시에는 공식적인 신청·승인 절차를 수립하여 관리하도록 한다.
3. 접근권한 부여 시 1인 1계정 원칙을 준수하도록 하며, 업무 담당자의 계정이 타 업무 담당자 또는 외부 업체 담당자와 공유되지 않도록 하여야 한다.
4. 시스템 접근권한 부여 시에는 사용자가 업무를 수행하는데 필요한 최소한의 권한으로 부여되어야 하며 담당자 업무 특성에 따라 차등 부여되어야 한다.
5. 시스템 관리자, 외부자 및 특수 권한 사용자의 접근권한은 명시적으로 식별되어야 한다.
6. 접근권한은 사용자의 인사이동, 퇴직, 휴지 등 변동사항 발생 시 사용자 계정 활성화 또는 비활성화를 통하여 접근권한 현황에 대하여 지속적으로 관리 및 검토하여야 한다.

404. 인증 및 식별

1. 선박 내 시스템에 접속하는 모든 사용자에는 보안 인증을 시행하여야 한다. 일반적으로 계정과 패스워드를 통한 인증을 사용하나 주요 데이터 또는 정보 시스템에 대해서는 강화된 인증을

적용할 수 있다.

2. 패스워드 인증

(1) 패스워드 인증 방식은 가장 단순하고 일반적인 형태의 인증이며 기본적인 취약점을 해결하기 위한 방법이다.

(2) 패스워드 관리 정책이 없을 경우 안전하지 않은 패스워드 사용으로 사람이나 컴퓨터 알고리즘에 의해 쉽게 추측되어 권한이 없는 엑세스를 허용할 수 있으므로 관리 정책을 설정하여 안전한 패스워드를 사용해야 한다. 또한 패스워드 정책에는 다음의 사항에 대하여 접속제한 절차를 포함하여야 한다.

(가) 패스워드 복잡도(문자구성 및 길이)

(나) 유추하기 쉬운 패스워드의 사용 제한

(다) 패스워드 변경 주기

(라) 벤더가 제공한 디폴트 패스워드의 변경 및 사용제한

(마) 연속적인 비밀번호 입력 오류에 대한 접속 제한

(3) 패스워드는 다양한 해킹방법(예 : 네트워크 스니핑, 데이터 베이스 해킹) 등에 의해 유출될 수 있으며 다음의 기술적인 방법으로 보호가 필요하다.

(가) 패스워드 저장 시 단방향 암호화

(나) 패스워드 전송 시 암호화

(4) 패스워드 정책은 시스템 접근 대상 인력의 능력, 운영 중인 시스템에서 지원하는 패스워드 정책을 고려하고 시스템 운영에 지장이 없는 수준에서 결정되어야 한다.

3. 패스워드 이외의 인증

리스크 평가를 통하여 패스워드 사용만으로는 취약성이 해결되지 않는 접속의 경우에는 일회용 비밀번호(OTP : One Time Password), 인증서, 보안토큰, 생체인식 등 강화된 인증 사용을 고려할 수 있다.

4. 식별

(1) 관리자 및 특수권한 사용자 등 시스템에서 사용자를 유일하게 구분할 수 있는 식별자(ID)를 할당하고 추측 가능한 식별자(root, admin, administrator)의 사용을 제한하여야 한다.

(2) 사용자에게 부여된 계정 정보는 공유되지 않도록 하여야 한다.

405. 통신 암호화

1. 사용자나 관리자, 유지보수 작업자는 회사와 선박 시스템 간 통신 시 안전한지 않은 프로토콜을 사용하지 않도록 조치하여야 한다.
2. 통신의 기밀성을 강화하기 위하여 암호화가 적용된 프로토콜(예 : HTTPS, SFTP, SNMP V3, SSH 등)을 사용하도록 한다.

406. 암호화 관리

1. 회사와 선박은 정보자산 식별을 통해 기밀 이상의 보안등급을 갖는 정보자산은 암호화하여 저장 관리되도록 한다.
2. 암호화 적용 시 암호화 기준, 암호화 프로그램 및 키 관리 등을 위하여 회사와 선박 내 기준과 절차를 마련하고 관리하여야 한다.

407. 보안성 심의

1. 네트워크, 시스템, SW 등 회사와 선박 내 중요한 정보자산이 신규 도입, 변경 등이 발생할 경우 회사가 요구하는 사이버보안 기준에 적합한 지 여부를 검토하는 보안성 심의를 적용하여야 한다.
2. 보안성 심의 대상은 회사가 사전에 수립한 정책에 따라 적용하되, 일반적으로는 내부 시스템과 외부 시스템 간 연동되고 중요 정보를 전송하는 경우, 외부로 공개되는 시스템 및 네트워크 장비 설치, 시스템 내 운영체제의 변경 등 IT 개발 및 운영 업무의 변화가 발생하거나 그 변화로

인해 보안상 중대한 영향이 발생할 경우 등으로 이러한 경우에 보안성 심의를 적용하도록 한다.

3. 보안성 심의 절차는 별도로 마련하여 사이버보안 최고 책임자의 승인을 획득하도록 한다.

제 5 절 관리적 보안

501. 인적 보안

1. 주요 직무자 지정

(1) 회사, 선박 내의 중요정보를 취급 또는 중요 시스템을 관리·운영하는 자를 주요 직무자로 지정하여야 한다.

(2) 회사, 선박 내의 중요정보를 취급하는 주요 직무자의 경우 업무 범위 및 목적에 벗어나는 정보 처리 권한을 부여하지 않도록 주요 직무자를 최소한으로 지정하여야 한다.

2. 직무 분리

회사, 선박 내 직무별 권한과 책임을 분산시켜 다음과 같은 직무 분리 기준을 수립하여야 한다.

(가) 개발과 운영 직무 분리

(나) 정보시스템(서버, DB, 네트워크 등)간 운영직무 분리

3. 보안유지 서약서

(1) 신규로 채용되거나 전입된 인력은 회사의 중요 정보 취급 및 사이버보안의 필요성과 책임에 대해 명시된 서약서에 서명하고 회사에 제출하여야 한다.

(2) 임직원의 퇴직 시 및 전출 시에는 직무상 알게 된 조직의 중요 정보에 대한 누출 방지를 위하여 보안유지 서약서를 받고 누출 발생 시 그에 따르는 법적 책임이 있음을 상기시킨다.

(3) 임시직원 혹은 외주 용역 업체 직원에게 정보자산에 대한 접근권한을 부여할 경우, 사이버보안 준수 의무 및 미준수로 인한 사건 발생 시 손해배상 청구 등의 내용이 담긴 보안 서약서에 서명을 받아야 한다. 이러한 보안 서약서 및 보안유지 서약서는 법적 분쟁 발생 시 증거자료로 사용 할 수 있기 때문에 필요 시 용이하게 찾아볼 수 있도록 보관되어야 한다.

(4) 서약서에 개인정보가 포함될 경우 비인가된 제3자에게 누출되지 않도록 물리적으로 안전한 장소에 보관하여야 한다.

4. 퇴직 및 직무변경 관리

(1) 부서 이동, 휴직 및 퇴직 등 인사 변경 발생 시 정보자산 반납, 접근권한의 변경 및 회수 조치가 신속하게 이루어질 수 있도록 인사 부서는 해당 내용을 관련 부서와 공유하여야 하고, 관련 부서는 지체 없이 절차에 따라 시행 하고 사이버보안 담당 부서는 그 결과를 확인하여야 한다.

(2) 퇴직자가 중요 자산에 대한 계정을 공유 사용하고 있었다면 계정의 비밀번호를 즉시 변경하여야 한다.

(3) 사이버보안 책임자의 변경 및 사이버보안 업무 담당자 변경 시 중요 정보의 인계인수 및 이전 담당자의 접근은 즉시 차단되어야 하고, 다른 적절한 방법으로 확인되어야 한다.

5. 상벌규정

임직원이 사이버보안 관련 회사 내부 규정 및 보안유지 서약서에 명시된 책임을 충실히 이행하지 않고 중요 정보 및 정보자산을 훼손, 유출한 경우, 관계법령상의 책임 및 처벌규정을 인사규정에 포함하여야 한다.

6. 외부자 보안

(1) 업무를 외부자에게 위탁하거나 정보자산에 대한 엑세스를 허용할 경우, 중요정보의 유출 및 정보자산의 침해 사고를 방지하기 위하여 다음과 같은 보안요구사항을 식별하고 관련 내용을 계약서 및 협정서 등에 명시하여야 한다.

(가) 보안 서약서 제출

(나) 위탁 업무 수행 직원의 주기적인 사이버보안 교육 수행

(다) 업무수행 관련 취득한 중요정보 유출 방지 대책

(라) 외부자 내부네트워크(업무망) 연결 시 인터넷접속 제한

(마) 외부자의 접근 공간에 대한 물리적 보호조치(장비, 매체 반출입 및 출입통제 등)
(바) 외부자 직원 PC 등 단말 보안(백신 설치, 안전한 패스워드 설정, 화면보호기 설정 등)
(사) 조직 정보자산 접근 허용 시 과도한 권한이 부여되지 않도록 접근권한 부여 및 해지 절차
(아) 무선네트워크 구축 및 사용제한(필요 시 리스크 분석을 통한 대책 마련 후 책임자 승인)
(자) 재위탁 하도급 계약 시 본 계약 수준의 보안요구사항 정의
(차) 보안요구사항 위반 시 처벌, 손해배상 책임
(카) 보안사고 발생에 따른 보고 의무 등

(2) 외부자가 보안요구사항을 준수하고 있는지 주기적으로 점검을 수행하여야 한다. 외주 용역업체가 자체적으로 사이버보안 책임자를 지정하여 보안점검을 수행한 경우, 그 결과를 주기적으로 점검하고 문제점 발생 시 재발방지를 위한 추가적인 보호대책을 수립하고 이행하여야 한다.

(3) 업무 상 외부자가 변경되는 경우 변경 사항은 즉각적으로 보고되어야 하고 정보자산 반납, 기존 정보의 유출 보호(중요정보 파기) 및 접근 통제가 지체 없이 이루어져야 한다. 이는 외부자와의 계약 종료 시에도 동일하게 적용된다.

502. 운영절차 관리

1. 변경 관리

(1) 지속적인 검증 및 검토, 사이버 사건 발생 및 취약성 식별, 사이버 트렌드 변화 등에 의하여 자산 및 시스템의 변경이 요구될 수 있다. 이 경우 회사는 장비운용관리절차(가칭)를 준용하여 회사 사이버보안 책임자의 최종 승인 하에 요청사항을 최대한 지원하여야 한다.

(2) 신규 시스템 도입, 유지보수업체 변경 등 사이버보안 시스템 관련 환경 변화가 있을 경우 운영절차 내용을 검토하여 변경 사항을 반영하여야 한다. 또한 운영절차(매뉴얼)의 작성일자, 변경일자, 검토 및 승인자 등에 대한 이력도 함께 관리하여야 한다.

(3) 운영체제 업그레이드, 상용 소프트웨어 설치, 운영 중인 응용프로그램 기능 개선, 네트워크 구성 변경, CPU/메모리/저장장치 증설 등 정보자산 변경이 필요한 경우 변경요청, 책임자의 검토 및 승인, 변경확인, 변경이력관리 등의 공식적인 절차를 수립하고 이행하여야 한다.

(4) 정보자산 변경이 필요한 경우 변경에 따른 보안, 성능, 업무 등에 미치는 영향을 분석하여 변경에 따른 영향을 최소화 할 수 있도록 변경을 이행하고 변경 실패에 따른 복구방안을 사전에 고려하여야 한다. 변경의 규모를 고려하여 영향 분석 대상 기준은 자체적으로 정할 수 있다.

2. 대외비 취급

운영절차(또는 매뉴얼)는 사이버보안 시스템 운영과 관련된 중요 자료이므로 회사의 민감한 정보(IP 등 시스템 정보)가 포함된 경우 대외비 문서로 지정하여 해당 업무 관련자만 접근할 수 있도록 통제하여야 한다.

3. 외부 위탁업체의 운영절차 관리

(1) 사이버보안 시스템 운영을 외부 위탁하는 경우 외부 아웃소싱 업체가 운영절차(매뉴얼)를 수립하고 있는지 확인하고 절차에 따라 시스템 운영을 보장하도록 계약서에 관련 내용을 명시하여야 한다. 운영 점검항목 등을 통해 외부 아웃소싱 업체가 절차를 준수하고 있는 지 주기적으로 확인하여야 한다.

(2) 운영절차(매뉴얼)는 외부 아웃소싱 업체가 자체 수립하거나 위탁사의 절차를 준용하여 수립할 수 있다.

503. 시스템 및 서비스 운영 보안

1. 시스템 인수

(1) 새로운 시스템의 도입, 업그레이드 시의 승인 기준이 확립되고 구매 계약서 등에 반영되어야 한다.

(2) 인수 이전에 보안성 심의 등 시스템 승인 테스트가 수행되어야 하고 기준에 적합할 경우 인수되어야 한다.

2. 성능 및 용량 관리
(1) 부족한 성능 및 용량으로 인한 실패를 회피하기 위해서 계획을 수립하여야 한다.
(2) 현재 장비의 성능 및 용량이 요구되는 사용자의 수준을 만족시켜야 한다.
(3) 성능 및 용량의 현황과 요구사항은 지속적으로 모니터링 되고 기록되며, 분석되어 향후 계획 수립에 반영하며 개선이 필요할 경우 이에 따라 조정하여야 한다.

3. 장애 관리
(1) 장애 관리를 위해 장애사항을 인지하고 대응하기 위한 절차를 수립하고 이에 대한 이력을 기록하고 보관하여야 한다.
(2) 중대한 장애기록 및 보고는 회사 또는 선박의 관리자가 확인하여야 한다.

4. 원격작업 관리
(1) 인터넷과 같은 외부네트워크를 통한 선박 시스템의 원격접속은 원칙적으로 금지하며, 부득이한 경우 다음과 같은 보안대책을 마련하여야 하여야 한다.
(가) 원격운영에 대한 사이버보안 최고책임자 승인절차
(나) 접속 단말 및 사용자 인증절차: ID/PW 이외의 강화된 인증방식 적용
(다) 한시적 접근권한 부여: VPN 계정, 시스템 접근권한 등
(라) 데이터의 암호화 통신
(마) 접속 단말 보안(예: 백신 설치, 보안패치 적용 등)
(바) 원격운영 현황(원격운영 인가자, VPN 계정 발급 현황 등) 지속적인 모니터링
(사) 원격 접속 기록 로깅 및 주기적 분석
(아) 원격운영 관련 보안인식교육 시행 등

5. 무선 네트워크 관리
(1) 선박의 시스템에 연결이 가능한 무선네트워크 환경 구축 시에는 내부 승인절차를 마련하여 비인가된(사설)무선네트워크 장비(Rogue AP: Access Point)를 운영하지 않도록 하여야 하며 사전 보안성 검토를 수행하여 다음과 같은 보호대책을 적용하여야 한다.
(가) 무선네트워크 장비 접속 단말기 인증 및 보안
(나) 무선네트워크 장비(예: AP, Access Point) 보안 및 허용 장비 리스트
(다) 무선 네트워크를 통하여 접근 할 수 있는 시스템 범위 정의
(라) 무선네트워크 사용권한 신청/변경/삭제 절차
(마) 사용자 식별 및 인증
(바) 정보송수신 시 무선망 암호화 기준(예: WPA2)
(사) SSID(Service Set IDentification) 브로드캐스팅 중지 및 추측 어려운 SSID 사용 등
(2) 시스템 네트워크에 무선네트워크 환경을 구축하는 것은 업무의 편리성을 증대할 수는 있으나 충분한 보호대책 마련 없이 적용할 경우 선박의 안전에 심각한 상황을 초래할 수 있으므로 반드시 필요한 경우를 제외하고는 매우 신중하게 접근하여야 한다.

6. 백업 관리
(1) 사이버 시스템 장애, 데이터 파손 등으로 인한 피해를 최소화하고, 조속한 복구를 위하여 시스템 가동 및 복구에 필요한 데이터의 백업계획을 수립하여 운영하여야 한다.
(2) 각 시스템 관리자는 백업계획에 따라 정기 또는 필요시에 백업을 실시하여야 한다.
(3) 백업대상은 중요정보(개인정보, 기밀정보 등), 문서, 각종 로그(이벤트 로그 등), 환경설정 파일 등 대상 정보 및 시스템의 중요도를 고려하여 선정하여야 하며 정해진 절차에 따라 백업관리를 수행하여야 한다.

7. 취약점 점검
(1) 시스템 취약점 점검 정책과 절차를 다음과 같은 내용을 포함하여 수립하여야 한다.
(가) 취약점 점검 대상 (예 : 서버, 네트워크 장비 등)
(나) 취약점 점검 주기
(다) 취약점 점검 담당자 및 책임자 지정

(라) 취약점 점검 절차 및 방법 등

(2) 시스템 중요도에 따라 주기적으로 다음과 같은 내용을 포함하여 취약점 점검을 실시하여야 한다.

(가) 라우터, 스위치 등 네트워크 장비 구성, 설정 취약점

(나) 서버 OS, 보안 설정 취약점

(다) 방화벽 등 정보보호시스템 취약점

(라) 어플리케이션, 소프트웨어 취약점

(3) 취약점 점검 시 회사의 규모 및 보유하고 있는 정보의 중요도에 따라 모의침투테스트를 수행하는 것을 고려하여야 한다.

(4) 취약점 점검 시 이력관리가 될 수 있도록 '점검일시', '점검대상', '점검방법', '점검내용 및 결과', '발견사항', '조치사항' 등이 포함된 기록을 작성하여 사이버보안 책임자에게 보고한다.

504. 패스워드 및 권한 관리

1. 패스워드 관리

(1) 중요시스템에 대한 사용자의 안전한 패스워드 사용 및 관리절차(작성규칙 등)를 다음과 같이 수립하고 이행하여야 한다.

(가) 사전공격(Dictionary attack)에 취약하지 않도록 가능한 문자(영문 대소문자), 숫자, 특수문자 등을 일정 자리수 이상으로 조합하도록 패스워드 작성규칙을 수립하고 주기적으로 변경(반기 1회 이상 권고)

(나) 연속 숫자, 생일, 전화번호, 아이디 등 추측하기 쉬운 개인 신상정보를 활용한 취약 패스워드사용 제한

(다) 시스템 도입 시 초기/임시 패스워드 로그인 시 지체 없이 변경

(라) 패스워드 처리(입력, 변경) 시 마스킹 처리

(마) 종이, 파일, 포켓용 소형기기 등에 패스워드 기록 및 저장을 제한하고 부득이하게 기록 및 저장해야 하는 경우 암호화 등의 보호대책 적용

(바) 사이버보안 사고가 발생 또는 패스워드의 노출 징후가 의심될 경우 지체 없이 패스워드 변경

(사) 패스워드 자동 저장 금지

(2) 패스워드가 기록되는 저장장치는 비밀등급에 준하여 취급하고 잠금장치로 비인가자의 접근을 통제할 수 있는 안전한 곳에 보관하여야 한다.

2. 권한 관리

(1) 시스템 영역별(네트워크장비, 중요 시스템 등)로 사용자 계정 등록, 비활성화 및 접근권한 등록, 변경·삭제에 관한 공식적인 검토, 승인절차를 수립하여 이행하여야 한다.

(2) 시스템에 등록된 사용자 계정 및 접근권한 부여 현황은 문서 또는 시스템적으로 기록·관리되어야 한다.

(3) 불가피하게 외부 업체에 접근 권한을 주는 경우 내부 조직 책임자의 승인을 득하여 필요시에만 부여하도록 하며 외부인의 사용이 종료된 경우 즉시 비활성화 하도록 한다. 또한 장기 미사용자, 직무변경자, 퇴직자 및 업무시간 외 사용(필요 시) 등에 경우에도 접근을 제한할 수 있도록 한다.

(4) 선박 시스템의 하드웨어 및 소프트웨어의 경우, 선박 사이버보안 책임자의 승인 하에 상위 직급의 담당자만이 접근하여 설정 등을 변경할 수 있도록 관리하여야 한다.

3. 접근을 통제할 수 없을 경우

선박의 Drydocking, 신조선 또는 현존선 인수 등과 같이 접근통제의 적용 시 어려운 경우에는 중요한 데이터나 시스템은 완전 잠금 조치를 취하거나 선박 외부의 안전한 곳에 보관 하였다가 재설치 하도록 한다. 다만 정보자산의 재가동 시 악의적 프로그램의 설치 여부를 확인하기 위하여 보안점검을 실시한 후 사용할 수 있도록 한다. OT 시스템의 경우 사용 전 기능들이 정상적으로 작동하는지 테스트 한 후 사용할 수 있도록 한다.

505. 이동식 저장매채 관리

1. 이동식 저장매체 관리

(2) 이동식 저장매체는 모든 네트워크상의 기술적 장벽을 우회하여 시스템에 접근할 수 있는 수단이므로 외부 환경에서 사용된 이동식 저장매체가 내부 정보자산에 접속되지 않도록 하여야 한다.

(3) 업무용으로 개인 이동식 저장매체를 사용하는 것은 원칙적으로 금지하여야 하며 업무 목적상 외장하드, USB 메모리, CD 등의 저장매체를 사용하여야 하는 경우 허가된 저장매체만 사용할 수 있도록 다음과 같은 정책 및 절차를 수립하고 이행하여야 한다.

(가) 휴대용 저장매체 취급(사용)범위 : 통제구역, 제한구역 등 보호구역별 저장매체 사용 정책 및 절차 수립

(나) 휴대용 저장매체 사용허가 및 등록절차

(다) 휴대용 저장매체 반출, 반입 절차

(라) 휴대용 저장매체 폐기, 재사용에 대한 절차

(마) 휴대용 저장매체 보호대책 등

(4) 휴대용 저장매체를 통해 바이러스, 악성코드가 유포되지 않도록 휴대용 저장매체가 연결되는 단말기에 다음과 같은 대책을 적용하고 주기적으로 점검하여야 한다.

(가) 휴대용 저장매체 자동실행 기능 해지

(나) 휴대용 저장매체 이용 시, 독립된 시스템을 통해 바이러스 및 악성코드 사전 검사

(다) 휴대용 저장매체 내 숨김파일 및 폴더 등이 표시되도록 PC 등 단말기 옵션 변경 등

(라) 중요 장비의 경우 특정한 또는 지정된 저장매체만 사용 가능하도록 기술적으로 보호

(5) 외부자의 노트북과 같이 시스템에 연결 전 사전 점검(scanning)이 어려운 휴대용 저장매체의 경우, 충분히 바이러스 등으로부터 안전함을 검증 하였다는 문서를 외부자로부터 확보하여야 한다.

(6) 업무목적으로 사용이 허용된 휴대용 저장매체의 경우 식별번호, 유형, 사용목적, 관리자, 책임자 등이 명시된 보유목록을 작성하고 주기적인 자산실사를 통해 목록을 현행화하여야 한다.

2. 저장매체의 처리(폐기, 재사용) 절차

(1) 사용 연한 경과, 고장 등의 사유로 시스템을 폐기 또는 재사용(양도, 내부판매, 재활용 등)할 경우 저장매체 처리에 관한 절차를 수립하여 저장매체에 저장된 중요정보 유출을 방지하여야 한다.

(가) 저장매체 확인 및 승인: 시스템 폐기 또는 재사용 시 저장매체 확인하고 폐기 또는 재사용 여부 결정

(나) 저장매체 폐기, 재사용에 따른 처리방법 정의(예: 폐기 → 물리적 폐기 또는 디가우징 등, 재사용 → 3회 이상의 완전 포맷)

(다) 저장매체 처리 확인 및 기록

(2) 저장매체의 폐기 시 물리적, 전자적으로 완전파괴하고 재사용 시에는 완전포맷 방식으로 정보를 삭제하여야 한다.

(3) 회사 및 선박에서 자체적으로 저장매체 폐기할 경우 폐기이력에 대한 감사증적을 확보할 수 있도록 다음 항목이 포함된 관리대장을 작성하고 관련 책임자가 확인하여야 한다.

(가) 폐기일자

(나) 폐기 담당자, 확인자명

(다) 폐기방법

(라) 폐기확인(사진 등) 등

(4) 시스템, PC 등의 유지보수, 수리과정에서 저장매체 교체, 복구 등의 상황 발생 시 저장매체 내 중요정보를 보호하기 위하여 유지보수 신청 전 데이터 이관 및 파기, 암호화, 계약 시 비밀유지서약 등과 같은 보호대책을 마련하여야 한다.

506. 악성코드 대응

1. 악성코드 통제

(1) 바이러스, 웜, 트로이목마 등의 악성코드로부터 시스템을 보호하기 위하여 다음 항목을 포함한 지침 및 절차를 수립하여야 한다.

(가) 사용자 PC 사용지침 (불분명한 이메일 및 파일 열람 금지, 허가받지 않은 프로그램 다운로드 및 설치 금지 등)

(나) 이메일 등 첨부파일에 대한 악성코드 감염 여부 검사

(다) 실시간 악성코드 감시 및 치료

(라) 백신프로그램을 통한 주기적인 악성코드 감염여부 모니터링 정책

(마) 백신엔진 최신 버전 유지 및 주기적 업데이트

(바) 사용자 교육 및 정보제공

(2) 백신 프로그램을 설치할 수 없는 경우, 데이터 이동 경로에서 사전 점검이 될 수 있는 추가적인 조치를 적용한다.

(3) 악성코드 감염 발견 시 추가적인 확산과 피해 최소화를 위하여 다음과 같은 항목이 포함된 대책을 마련하여야 한다.

(가) 악성코드 감염 발견 시 대처 절차 (예 : 네트워크케이블 분리 등)

(나) 비상연락망 (예: 회사 담당자, 백신업체 담당자, 관련 기관 연락처 등)

(다) 대응보고서양식 (발견일시, 대응절차 및 방법, 대응자, 방지대책 포함) 등

2. 패치 관리

(1) 운영체제(서버, 네트워크, PC 등) 및 (상용) 소프트웨어(오피스 프로그램, 백신, DBMS 등)의 경우 지속적으로 취약점이 발견되고 있으며, 해당 소프트웨어 배포사의 경우 취약점에 대응하는 패치(patch)파일을 지속적으로 공개하고 있다. 따라서 서버, 네트워크 장비, PC 등에 설치되어 있는 운영체제, 소프트웨어 패치적용을 위한 정책 및 절차를 수립하여 이행하여야 한다.

(가) 서버, 네트워크 장비, 보안시스템, PC 등 대상별 패치정책 및 절차 : 패치정보 입수 및 적용방법 설정

(나) 패치 담당자 및 책임자 지정

(다) 패치 관련 업체(제조사) 연락처 등

(라) 선박의 경우, 적절한 패치 시기 및 방법 (특히 백신)

(마) 하드웨어 업체 또는 소프트웨어 업체가 더 이상 업데이트를 제공하지 않을 경우의 대책

(2) 주요 서버, 네트워크 장비, 보안시스템 등에 설치된 운영체제, 소프트웨어 버전 정보, 패치일 등을 확인할 수 있도록 목록으로 관리하고 최신 보안패치 여부를 주기적으로 확인하여야 한다.

(3) 주요 서버, 네트워크 장비의 경우 공개 인터넷 접속을 통한 패치는 원칙적으로 금지한다. 다만 불가피한 경우 사전 리스크 분석을 통해 보호대책을 마련한 후 책임자 승인 후 적용한다.

(4) 운영시스템에 패치를 적용하는 경우, 시스템 가용성에 영향을 미칠 수 있으므로 패치 적용은 리스크 분석 등을 통하여 충분하게 영향을 분석한 후 책임자가 승인하여 적용하여야 한다.

(5) 패치를 적용하기 전 가능한 무결성 점검을 시행한 후 적용하여야 한다.

507. 로그 관리 및 모니터링

1. 로그관리

주요 정보자산 및 사이버 시스템 사용자 접속기록은 사용자 실수 또는 의도적 공격의 원인에 대한 책임 추적성을 확보할 수 있다. 주요 정보자산의 접속기록은 주기적으로 검토하여 오남용 등의 이상 징후를 확인하여야 한다. 다음 사항이 포함된 검토(모니터링)절차를 수립하고 절차에 따라 이행하여야 한다.

(가) 검토대상 : 사용자 접속기록을 검토할 중요정보 및 주요 시스템 선정

(나) 검토주기 : 월 1회 이상(권고)

(다) 검토기준 및 방법 : 업무목적 이외의 중요정보 과다처리(조회, 변경, 삭제 등), 업무시간 외 접속, 비정상적인 접속(미승인 계정 접속 등)등의 기준 및 확인 방법 수립
(라) 검토 담당자 및 책임자 지정
(마) 이상 징후 대응절차 등(사이버보안 책임자에게 보고, 경위 확인, 벌칙조항 적용 등)

2. 외부로부터의 침해시도의 인지

외부로부터의 침해시도가 의심되는 이상 징후를 신속하게 인지할 수 있도록 다음과 같은 항목이 포함된 모니터링 절차를 수립하여 이행하여야 한다. 회사의 규모 및 시스템 중요도가 높은 경우 24시간 침해시도 실시간 모니터링 수행을 고려하여야 한다.

(가) 모니터링 대상범위 : 침해시도 탐지 및 차단하기 위한 각종 시스템 이벤트 로그 등
(나) 모니터링 방법 : 외부 전문업체를 통한 모니터링, 자체 모니터링 체계 구축 등
(다) 담당자 및 책임자 지정
(라) 모니터링 결과 보고체계
(마) 침해시도 발견 시 대응절차 등

508. 지속적인 검토 및 검증

1. 적절한 주기로 장비 및 시스템의 검사, 보안 시스템 이행 상황을 검토한다. 그 점검방법 및 빈도는 시스템의 중요도에 따라 달리 정해진다. 점검의 수행은 선박 또는 회사의 사이버보안 담당자가 자체적으로 할 수 있으며, 불가능한 경우 외부 IT 서비스 공급 업체에 의해 수행할 수 있다. 추가적인 장비 및 시스템 업데이트, 설치, 보수가 요구된다면 별도의 관리절차(가칭)의 마련하여 처리하고, 모든 기록은 유지한다.
2. 회사는 절차들이 준수되고 효과적으로 운용되고 있는지를 검증하기 위하여 연 1회 내부심사 및 경영 검토를 시행한다. 이는 품질 내부감사 및 경영검토와 동시에 시행할 수 있으며, 절차 역시 준용하나 계획, 내용 및 결과는 사이버보안 책임자에 의하여 검토되어야 한다. 감사를 시행하는 직원은 충분한 자격이 있어야 하고, 피감 부서와는 독립되어 있어야 한다.
3. 적절한 주기로 평가된 사이버 리스크 및 운영 절차에 대해서 유효성을 검토하여야 한다. 보안 사건 및 보안 장애 등 추가적으로 식별된 취약성 등은 검토 주기와는 관계없이 이벤트의 발생 시 사이버 리스크 평가에 추가적으로 반영되어야 한다. 그리고 운영 절차의 유효성을 검토 할 시 다음과 같은 사항들을 반영한다.

(1) 산업계(예 : IMO, 한국선급, IACS 등)에서 배포하는 사이버 관련 지침
(2) 사이버보안 트렌드
(3) 내부심사, 경영검토, Master's Review 등에서 식별한 절차상의 개선점

제 6 절 물리적 보안

601. 보호구역 통제

1. 보호구역 지정

(1) 전산실, 시스템 운영실 및 통신장비실 등 업무의 중요도 및 정보자산의 위치에 따라 물리적 보호 구역을 다음과 같이 구분하고 구역별 보호대책을 수립하고 이행하여야 한다.
(가) 제한구역 : 비인가된 접근을 방지하기 위하여 별도의 출입통제 장치 및 감시시스템이 설치된 장소로 출입 시 출입증이 필요한 장소(예 : 사이버보안 담당 부서 사무실, 선박 화물구역의 갑판 등)
(나) 통제구역 : 제한구역의 통제항목을 모두 포함하고 출입자격이 최소인원으로 유지되며 출입을 위하여 추가적인 절차가 필요한 곳(예 : 전산실, 통신장비실, 선교, 기관실 등)
(2) 통제구역은 회사 내부에서도 출입 인가자를 최소한으로 제한하고 있으므로 통제구역임을 표시하고 필요시 출입을 전자식 또는 자물쇠 등으로 잠금 조치하여 접근 시도 자체를 원천적으로

차단하여야 한다.

2. 보호구역 내 작업

(1) 정기점검, 유지보수 등 주요 설비 및 시스템이 위치한 보호구역 내에서 임직원 및 외부인이 작업을 수행할 경우 다음 사항을 고려하여 작업 신청 및 승인, 작업 기록 작성, 모바일 기기 반출입 통제 등의 절차를 마련하여야 한다.

(가) 작업신청 시 관련자(예: 회사 사이버보안 책임자, 선박보안 책임자) 검토 및 승인 필요

(나) 작업기록에는 작업일자, 작업시간, 작업목적, 작업내용, 작업업체 및 담당자명, 검토자 승인자 등 포함

(다) 작업 수행을 위한 보호구역 출입 절차 마련 및 출입기록의 주기적 검토

(라) 작업 수행을 위한 모바일기기 반출입 및 모바일 기기 안전성 확보 절차(백신 설치 등) 마련

(2) 작업의 원활한 수행을 위하여 불가피하게 모바일기기를 사용해야 하는 경우 모바일 기기 반출입 통제에 따라 사전 승인 및 모바일 기기의 내부파일 확인, 카메라에 스티커 부착 등 보안 조치를 수행한 후 사용하여야 한다.

602. 출입 및 물품통제

1. 출입통제

(1) 각 보호구역 별로 출입가능한 부서, 직무, 업무를 정의하고 출입 권한이 부여된 임직원을 식별하여 그 현황을 관리하여야 한다. 출입내역은 기록되어야 하고 정기적으로 검토되어야 한다. 통제구역의 경우 업무 목적에 따라 최소한의 인원만 출입할 수 있어야 한다. 특히 보호구역에 외부인 출입이 필요한 경우 방문객 출입증 발급 및 패용, 방문 장소만으로의 출입권한 제한, 담당자 동행 및 출입대장 작성 등의 별도의 절차를 마련하여야 한다.

(2) 출입통제에 대한 기록이 시스템적으로 로그를 남기지 않는 경우 출입대장을 작성한다. 출입대장은 다음과 같은 기준으로 주기적으로 검토되어야 한다.

(가) 업무 목적에 적합한 출입권한 부여: 업무 목적에 비해 과도한 출입권한 부여 시 권한 조정, 장기간 미출입 시 권한 회수 등 조치

(나) 절차에 따른 출입권한 부여: 보호구역 출입절차에 따른 권한 부여 여부 확인 (임의적 출입권한 생성 확인)

(다) 퇴직자 또는 직무변경자 출입권한 삭제·조정 및 출입증 회수: 퇴직자 출입증 회수 및 출입권한을 삭제, 직무변경에 따른 출입권한 조정

(라) 업무시간 외 출입: 일상 업무시간 이외 출입 시 출입사유 확인

(마) 비인가자의 출입 시도: 중요한 보호구역인 통제구역의 비인가자 출입시도를 확인하여 그 사유를 확인하고 조치

(바) 외부자 출입기록: 유지보수, 비상 시 외부자 출입 적정성 검토

(3) 보호구역 내 다음 항목에 대한 반출입 통제 정책 및 절차를 수립하고 이행하여야 한다.

(가) 장비(예: 서버, 네트워크 장비, 항온항습기 등)

(나) 문서(예: 업무관련 대외비 이상의 문서)

(다) 저장매체(예: CD, 테이프 등)

(4) 반출입관리대장을 별도로 마련하여 일시, 품명 및 수량, 반출입 담당자, 반출입장소, 반출입 사유, 관리부서 확인 및 서명 등과 내용이 포함되어 이력관리를 하고 책임자가 주기적으로 관리대장 내용의 적정성을 확인하여야 한다.

2. 물품통제

(1) 보호구역별로 아래의 물품에 대한 반출입 통제절차를 수립하여야 한다.

(가) PC 및 모바일 기기(노트북, 태블릿 PC 등)

(나) 중요정보 및 자산의 데이터가 포함된 문서 또는 저장매체

(다) 기타 사이버보안 책임자가 통제대상 물품으로 추가 지정한 물품

(라) 반출입내역의 주기적 점검 등

(2) 보호구역 내 모바일기기 반출·입 시 '물품 반출·입 대장'에 관리 이력을 기록하여야 하며 출입통제 담당자는 그 이력을 주기적으로 확인하여야 한다.
(3) 반출·입 통제대상 물품은 업무시간 중에 반출입하여야 한다. 단, 사전에 출입통제 담당자의 승인을 받은 경우에는 예외로 한다.
(4) 장비 유지보수를 위한 반출·입 시에도 중요정보 및 자산정보를 삭제하거나 암호화하여 이를 통한 정보유출이 발생하지 않도록 하여야 한다.

603. 설비 및 시설관리

1. 보호설비

(1) 보호구역의 중요도와 특성에 따라 화재, 전력이상, 비인가된 외부침입 등을 방지하기 위하여 보호구역별 필요한 다음과 같은 설비를 갖추고 운영절차를 마련하여야 한다.
(가) 온습도 조절기(항온항습기 또는 에어컨)
(나) 화재감지 및 소화설비
(다) 누수감지기
(라) UPS, 비상발전기, 전압유지기
(마) CCTV, 외부침입감지 및 경보, 출입통제시스템(예 : 지문인식, 출입카드시스템 등)
(바) 전력선 이중화
(사) 파손방지(예: 시스템기기 하부의 rack 설치, 적절한 Lashing 등)
(2) 사이버보안 시스템을 외부에 위탁 운영하는 경우 화재, 침수, 전력이상, 도난 등의 위협으로부터 보호되도록 보안요구사항을 계약서에 반영하고 운영 상태를 주기적으로 점검하여야 한다.

2. 케이블 보안

(1) 전력 및 통신케이블 등이 외부의 영향 없이 안정적으로 전력 및 데이터 전송이 이루어질 수 있도록 다음과 같은 보호조치를 취하여야 한다.
(가) 전력 및 통신케이블은 물리적으로 구분하여 배선
(나) 전력 및 통신케이블에 대한 식별(어느 시스템에 연결되어 있는지 확인 필요)
(다) 전력 및 통신케이블 사이의 상호간섭을 방지하기 위한 거리유지
(라) 케이블을 지지하고 보호할 수 있는 설비 설치(예: 케이블 트레이)
(마) 도청이나 손상이 일어나지 않도록 케이블을 보이지 않게 매설할 것
(바) 배전반 등에 대한 접근통제

604.환경보안

1. 개인업무 환경보안

일상업무를 수행하는 사무 환경에 대해 다음과 같은 보호대책이 명시된 정책을 수립하고 이행하여야 한다. 임직원으로 하여금 개인업무 환경에서의 사이버보안 준수여부를 자가진단하게 하고 주기적으로 관리부서에서 준수여부를 점검하여야 한다.
(가) 일정시간 자리 이석, 퇴근, 휴가 시 책상 위에 중요문서, 저장매체방치 금지
(나) 중요 문서가 보관된 서랍장, 캐비넷 잠금장치 사용
(다) 일정시간 컴퓨터 미사용 시 화면보호기를 설정, 재시작 시 로그인 설정, 장기간 자리 이석 시 컴퓨터 로그오프
(라) 안전한 로그인 비밀번호 사용 및 주기적 변경
(마) 개인용컴퓨터 백신설치, 최신 패치, 공유폴더 설정 제한
(바) 개인용컴퓨터 및 업무시스템 안전한 로그인 비밀번호 사용 및 주기적 변경, 로그인정보(ID, 비밀번호) 노출 금지(포스트잇 기록 부착 등)
(사) 중요 정보가 포함된 문서 폐기 시 세절기를 이용한 파쇄 등

2. 공용 업무 환경보안

공용으로 사용하는 사무기기, PC, 파일서버, 문서고 등에 대해 다음과 같은 보호대책을 수립하고 이행하여야 한다. 사이버보안 책임자는 각 사무기기, 파일서버, 문서고 등에 적용해야 할 보호대

책 준수 여부를 주기적으로 점검하여 미준수 사항 발견 시 관련 내용을 임직원들에게 공고 또는 교육을 수행하여 주의를 환기시켜야 한다.

(가) 공용사무기기: 팩스, 복사기, 프린트 등의 공용사무기기 주변에 중요정보문서 방치 금지

(나) 공용PC: 일정기간 미사용 시 화면보호기를 설정, 재시작 시 로그인 암호설정, 공용패스워드 사용 시 주기적으로 패스워드 변경, 중요정보 저장 제한

(다) 파일서버: 파일서버 접근권한을 부서별, 업무별 등으로 부여하여 불필요한 정보공개 최소화, 사용자 별도 접근계정 발급, 공용 PC 보안대책 적용

(라) 문서고: 문서고에 대한 접근권한을 부서별 혹은 업무별로 부여하여 출입가능인원을 최소화하고 CCTV 혹은 출입통제시스템을 설치하여 출입이력 관리

(마) 공용 사무실: 회의실, 프로젝트룸, 화상회의실 등 공용사무실 내 중요정보 문서 방치 금지

(바) 기타 공용 업무 환경에 대한 보안대책 수립

제 4 장 사이버보안 사고 대응

제 1 절 개요

101. 일반사항

1. 회사는 회사 내부와 선박의 정보자산에 발생 가능한 사이버 보안 사고에 대비하여야 한다.
2. 일반적으로 사이버보안 사고는 다음과 같은 유형으로 구분되며, 회사와 선박의 상황에 따라 사이버보안 사고의 등급을 적용하여 관리하여야 한다.
   (1) 정보시스템의 가동 및 서비스 중단
   (2) 악성코드 유포
   (3) 서비스 거부 공격
   (4) 불완전하고 부정확한 정보로 인한 오류
   (5) 기밀성 및 무결성 위반
   (6) 정보시스템의 오용
   (7) 내부 임직원 또는 승객의 개인정보 유출
3. 사이버보안 사고에 대비하기 위해 별도의 비상계획 또는 사이버보안 사고 대응계획을 수립하여 운영하여야 한다.
4. 비상계획 내 회사는 보안사고의 정의 및 범위, 긴급연락체계 구축, 보안사고 발생 시 보고 및 대응절차, 사고 복구조직의 구성, 교육계획 등이 포함되며 절차 상으로는 사이버보안 사고에 대한 대응, 복구, 보고로 구성하는 것이 일반적이다.
5. 비상계획에 포함될 대상은 비즈니스와 자산, 운영의 중요도와 리스크 평가의 결과에 따라 중요 자산으로 식별된 시스템들을 주 대상으로 하며, 다음을 최소한 포함하여야 한다.
   (1) IT 시스템
      (가) 리스크 평가 결과 리스크가 높은 것으로 식별된 시스템
      (나) 지속적인 시스템의 운영 중단 시 비즈니스와 자산 또는 회사에 상당한 재정적 손상을 초래할 수 있는 시스템
   (2) OT 시스템
      (가) 리스크 평가 결과 리스크가 높은 것으로 식별된 시스템
      (나) 시스템의 사고로 인해 인명 또는 선박의 안전, 환경에 대하여 위험한 상황을 초래할 수 있는 시스템
6. IT 및 OT 시스템이 탑재된 선박을 위한 비상계획을 개발할 때에는 IT 및 OT 시스템에 대한 사이버보안 사고의 차이점을 이해하고 대응 조치의 우선순위를 정하는 것이 중요하다.
7. 일부 IT 시스템의 사이버보안 사고는 회사의 비즈니스 연속성에 영향을 줄 수 있지만, 선박의 안전 운항에는 영향을 주지 않으므로 해당 IT 시스템의 사이버보안 사고에 대해서는 그 영향성을 고려하여 심각하지 않다고 판단될 경우 대응계획에 포함되지 않을 수 있다.
8. OT 시스템에 대한 사이버보안 사고로 인한 시스템의 오작동 또는 중단은 선박의 안전한 운항에 중요하고 즉각적인 영향을 미칠 수 있으므로 안전에 중요한 시스템들에 대해서는 대응계획 및 사고 후의 복구계획이 포함되어야 한다.
9. 안전관리시스템에는 이미 사고 또는 위험 상황을 보고하고 의사결정을 위한 의사소통 및 권한 수준을 정의하는 절차가 포함되어야 한다. 그러므로 관련 절차에 사이버 사건 발생 시 의사소통 및 권한을 반영하도록 수정되어야 한다.

제 2 절 대응

201. 사고 대응 계획

1. 사고 대응 계획은 사이버보안 사고에 대한 탐지, 사고의 대상과 원인에 대한 식별, 그리고 사고에 대한 적시적이고 효과적인 대응을 지원하기 위해 직원이 쉽게 이해가능하고 즉시 이용 가능한 형태로 문서화한 것이다.
2. 사고 대응계획은 사고에 대해 적시적 대응을 하지 않을 경우 선박의 안전에 직접적으로 영향을 주는 OT 시스템과 단시간 중단에도 비즈니스에 큰 영향을 주는 IT 시스템들에 대한 구체적인 조치 절차를 포함하여야 하며 최소한 다음을 포함하여야 한다.
   (1) 역할과 책임
   (2) 적용되는 IT 시스템과 OT 시스템 또는 자산 목록
   (3) 시스템 또는 자산 별 사이버보안 사고 현상과 사고원인
   (4) 사고원인에 대한 대응 계획 및 절차
   (5) 주기적 훈련 및 교육 요건
   (6) 주기적 검토 및 개선 절차
3. 다음은 대응계획에서 고려될 수 있는 선박 내 사이버보안 사고의 예시이다.
   (1) 전자 항법 장비의 가용성 손실 또는 항법 관련 데이터의 무결성 손실
   (2) 글로법 위성항법시스템을 포함하되 이에 국한되지 않는 외부 데이터 소스의 가용성 또는 무결성 손실
   (3) 추진력, 보조 시스템 및 기타 중요한 시스템을 포함한 산업 제어 시스템의 가용성 손실, 데이터 관리 및 제어의 무결성 손실
   (4) 디도스 공격에 의한 회사와의 통신 두절

202. 사고의 대응

1. 사이버보안 사고의 대응 절차에는 사고의 탐지와 원인 분석, 대응 및 복구가 포함된다.
2. 사이버보안 사고로 인한 증상이 감지될 경우 사고 대응 옵션을 판단하기 위해서 신속한 사고의 원인 식별이 이루어져야 한다.
3. 사고의 증상은 다음 중 하나를 포함할 수 있다.
   (1) 비정상적으로 많은 네트워크 트래픽
   (2) 디스크 공간 부족 또는 사용 가능한 디스크 공간의 현저한 감소
   (3) 비정상적으로 높은 CPU 사용
   (4) 새 사용자 계정 생성
   (5) 관리자 수준 계정의 사용 또는 실제 사용
   (6) 잠긴 계정
   (7) 사용자가 직장에 없을 때 사용 중인 계정
   (8) 삭제된 로그 파일
   (9) 비정상적으로 많은 수의 이벤트가 있는 전체 로그 파일
   (10) 바이러스 백신 또는 IDS 알림
   (11) 사용할 수 없는 바이러스 백신 소프트웨어 및 기타 보안 컨트롤
   (12) 예기치 않은 패치 변경
   (13) 외부 IP 주소에 연결하는 시스템
   (14) 시스템에 대한 정보 요청 (사회 공학 시도)
   (15) 의도치 않은 설정 변경
   (16) 예상하지 못한 시스템 종료
   (16) 인가된 이용자에 대한 데이터 접근 차단
5. 사고의 증상을 바탕으로 사고의 원인을 식별하는 것이 효과적인 사고 대응으로 이어지므로 사

고 대응 계획에는 실질적으로 운영자의 사고의 원인 식별과 적절한 사고 대응 절차에 대한 내용이 사고대응계획에 포함되어야 한다.

6. OT 시스템의 경우 보호하기 위해 취해진 조치와 관계없이, 사고로 인해 시스템이 손상될 가능성이 항상 있으며, 정확한 사고 원인을 식별하기 어려운 경우가 발생할 수 있다. 그러므로 문제가 발생한 시스템의 사용을 중지하고 제어 능력을 회복할 수 있는 대안적인 운영 방법의 가용성 여부를 사고 대응 계획에서 확인할 수 있어야 한다. 예를 들어, 이중화된 시스템 또는 수동/지역 제어 옵션의 유무를 식별할 수 있어야 하며, 관련된 신속한 대안적인 제어 능력의 복구를 위한 절차가 계획서 상에서 확인될 수 있어야 한다.

203. 사이버보안 사고 결과보고

1. 사이버보안 사고 발생 시 사이버보안 사고 보고서가 작성되어야 하고 보고서에는 다음과 같은 사항이 포함되어야 한다.
   (1) 사이버보안 사고 발생 일시
   (2) 보고자와 보고 일시
   (3) 사고 내용(발견사항, 피해내용 등)
   (4) 사고 대응 경과 내용
   (5) 사고 대응까지의 소요 시간 등
2. 회사의 유·무형 자산에 심각한 영향을 끼칠 수 있는 사이버보안 사고가 발견되거나 발생할 경우 최고 경영층가지 보고하여야 한다.
3. 선박의 운항 중 발생한 사이버보안 사고의 경우 사전에 마련된 보고절차와 대상(ex : 기국 관련 정부부처 항만기관, 화주 등)에게 보고하여야 한다.

제 3 절 사이버보안 사고 사후관리

301. 사이버보안 사고 분석 및 공유

1. 사이버보안 사고 분석은 적절한 대응을 보장하고 복구활동을 지원하기 위하여 수행되어야 한다.
2. 사이버보안 사고가 처리되고 종결된 후 이에 대한 분석이 수행되어야 하며 그 결과가 보고되어야 한다.
3. 사이버보안 사고 분석 및 평가에 의해 얻어진 정보는 관련 조직 간에 공유하며 분석된 결과에 따라 필요한 경우 정책, 절차, 조직 등의 사고대응체계에 대해 변경을 수행하여야 한다.
4. 사이버보안 사고에 대한 취급 및 처리는 다음과 같다.
   (1) 자동사고 처리 프로세스 : 회사는 자동처리 매커니즘을 사용하여 사건 처리 프로세스를 지원한다. 사건 처리 프로세스를 지원하는 자동화된 매커니즘에는 온라인 사고 관리 시스템이 포함된다.
   (2) 동적 재구성 : 회사는 사고 대응 능력의 일부로 동적 재구성을 포함한다. 예를 들면, 라우터 규칙, 액세스 제어목록, 침입 탐지/방지 시스템 매개변수 및 방화벽과 게이트웨이에 대한 필터 규칙의 변경이 포함된다.
   (3) 운영의 연속성 : 회사는 회사의 임무와 비즈니스 기능의 지속성을 보장한다. 사건의 분류는 설계/구현 오류 및 생략, 악의적인 공격, 타깃이 불분명한 악의적인 공격 등을 포함한다.
   (4) 정보의 상호연계 : 회사는 사고 정보 및 개별 사건 대응을 상호 연관시켜 사고 인식 및 대응에 대한 전사적 관점을 달성한다. 적대적인 사이버 공격은 회사에서 설정한 다양한 보고서 및 보고 절차를 비롯한 여러 출처의 정보를 모아야만 관찰할 수 있다.
   (5) 정보시스템의 자동 작동 불능 : 회사는 회사가 정의한 보안 위반이 탐지되면 정보 시스템을 자동으로 비활성화 할 수 있는 기능을 구현한다.
   (6) 내부자의 위협(구체적인 기능) : 회사는 내부자 위협에 대한 사고 처리 능력을 구현한다.
   (7) 내부자의 위협(내부 조직 협조) : 회사는 회사의 구성요소 전반에 걸쳐 내부자 위협에 대한

사건 처리 기능을 조정한다. 내부자 위협 사건(준비, 탐지 및 분석, 봉쇄, 박멸 및 복구 포함)에 대한 사건 처리에 효과적이기 위해 다양한 회사 구성요소 또는 요소 간의 긴밀한 조정이 필요함. 이러한 구성 요소는 미션/비지니스 소유자, 정보시스템 소유자, 인적 자원 사무소, 구매 사무소, 인적/물적 보안 사무소, 운영 인력, 리스크 관리 기능이 포함된다.

(8) 외부 조직과의 상관관계 : 회사는 외부 조직과 협력하여 사건 정보를 상호 연관시키고 공유함으로써 사건 인식 및 효과적인 사건 대응에 대한 회사의 목표를 달성한다. 사건 처리와 관련하여 회사와 외부 조직 간 조정은 중요한 리스크 관리 역량을 제공할 수 있다.

(9) 직접적/역동적인 응답 역량 : 회사는 회사에서 정의한 역동적인 응답 기능을 사용하여 보안 사고에 효과적으로 대응한다. 이 통제 강화는 보안사고(예: 적대적인 사이버 공격 중 적의 행동)에 대한 대응으로 적시에 교체 또는 새로운 기능 배치를 처리한다.

(10) 공급 체인 협조 : 회사는 공급망 사건과 관련된 사건 처리 활동을 공급망에 관련된 다른 업체과 조정한다. 공급망 활동과 관련된 업체에는 시스템/제품 개발자, 통합 업체, 제조업체, 포장 업체, 조립 업체, 유통 업체, 공급 업체 및 재판매 업체가 포함된다.

302. 사이버보안 사고 재발 방지

1. 회사는 정기적으로 사고 대응계획에 포함된 내용과 사고 시나리오를 바탕으로 주기적인 훈련과 친숙화를 위한 교육을 실시하여야 하며, 이행 결과를 기록으로 남겨야 한다.
2. 회사는 매년 정기적으로 이전 사이버보안 사고 및 관련 대응에서 얻은 교훈을 바탕으로 사고 대응 계획을 개선하여 업데이트하여야 한다.

제 5 장 복구 관리

제 1 절 개요

101. 일반사항

1. 재해, 사고, 장애 등으로 인한 재해, 사고, 장애 등으로 인해 발생 가능한 피해를 최소화하고 회사, 선박 내 업무의 업무 연속성을 유지관리하기 위한 적절한 조직구성과 업무 연속성계획 및 복구체계를 수립하여야 한다.
2. 복구 관리 계획 수립 시 복구 조직, 비상연락체계, 복구절차 등을 포함하여 다음 단계와 같은 과정과 산출물 등을 수립하여야 한다.

(1) 개시단계 : 업무 연속성관리에 대한 정책 수립 및 범위설정, 자원분배
(2) 전략수립단계 : 업무 연속성검토 및 업무영향분석
(3) 구현단계 : 기술적 대책, 조직 구성 및 체계의 문서화 등
(4) 운영관리단계 : 시험, 교육·훈련, 검토 및 갱신 활동 등을 포함

제 2 절 복구

201. 복구 계획

1. 사이버보안 사건의 영향을 받는 시스템이나 자산을 적시에 복구할 수 있도록 복구 프로세스와 절차가 실행 및 유지되어야 한다.
2. 데이터 복구기능은 다음과 같이 구현되어야 한다.

(1) 각 시스템이 최소한 매주 자동으로 백업되고 민감한 정보가 저장된 시스템은 보다 자주 백업되어야 한다. 시스템을 백업에서 신속하게 복구할 수 있도록 운영 체제, 응용 프로그램 소프트웨어 및 시스템의 데이터가 전체 백업 절차에 각각 포함되어야 한다. 모든 백업 정책은 규제 또는 공식 요구사항을 준수해야 한다.
(2) 백업이 올바르게 작동하는지 확인하기 위해 데이터 복구 프로세스를 수행하여 백업 미디어의 데이터를 정기적으로 테스트해야 한다.
(3) 백업이 물리적 보안이나 암호화를 통해 저장 될 경우와 네트워크를 통해 이동되는 경우에 백업이 적절하게 보호되는지 확인해야 한다. 여기에는 원격백업이나 클라우드 서비스도 포함된다.

202. 복구 절차

1. 사이버사고 또는 재해 유형을 식별하고 재난재해시나리오에 따라 업무영향분석을 수행하여 유형별 예상 피해규모 및 영향을 분석할 수 있는 체계를 구축하여야 한다.
2. IT 및 OT 시스템 복구 목표시간, 복구시점을 정의하고 적절한 복구 전략 및 대책을 수립하여야 한다.
3. IT 및 OT 시스템 복구전략 및 대책에 따라 효과적인 복구가 가능한 지 시나리오, 일정, 방법, 수행절차 등을 포함한 시험 계획을 수립하여야 한다.
4. 시험결과, IT 및 OT 환경변화, 법규 등에 따른 변화를 반영하여 복구 전략 및 대책을 보완하여야 한다.
5. 복구 활동은 조정 센터, 인터넷 서비스 제공업체, 공격 시스템 소유자, 희생자, 기타 CSRT 및 공급 업체와 같은 내외부 담당자와 조정되어야 한다.

(1) 홍보 활동이 관리되어야 한다.
(2) 사건 후 평판이 복구되어야 한다.
(3) 복구 활동은 내부 이해관계자와 경영진에게 전달되어야 한다.

203. 개선

1. 학습 계획과 프로세스는 학습된 교훈을 향후 활동에 통합함으로써 향상되어야 한다.
2. 복구 계획은 교훈이 포함되어야 한다.
3. 복구 전략이 업데이트되어야 한다.
4. 복구 절차 및 도구는 다음과 같다.

(1) 분기마다 또는 새로운 백업 장비 구입 시 마다 테스트 팀은 테스트 베드 환경에서 시스템 백업을 복구하여 시스템 백업의 무작위 샘플을 평가해야 한다.

(2) 복구된 시스템은 백업의 운영체제, 응용프로그램 및 데이터가 모두 손상되지 않았는지 확인되어야 한다.

(3) 악성 소프트웨어에 감염된 경우 복구 절차는 실제 감염 이전 시점의 백업버전을 사용하도록 수립되어야 한다.

4. 유효성 테스트

(1) 평가팀은 시스템을 식별하고 최신 백업을 사용하여 테스트 시스템(실제 또는 가상)을 복구해야 한다.

(2) 복구 결과를 원래 시스템과 비교하여 시스템이 올바르게 복구되었는지 확인해야 한다.

아래 테이블은 이해를 돕기 위하여 선박의 기능 및 서비스를 OT 시스템과 매핑한 것이다. 이 시스템 목록은 완전한 것이 아니며, 나열된 OT 시스템의 관련성은 기술적 배치와 선박의 유형에 따라 다르다. 또한 다른 OT 시스템이 목록에 추가될 수도 있다. 이 목록의 순서는 중요도와 관계가 없다.

표 1 선박 기능과 관련된 OT 시스템 예시

선박 기능/서비스	OT 시스템
추진	• 추진시스템(드라이버, 샤프트, 기어, 프로펠러 등) 및 추진 보조 기관을 위한 로컬 및 원격 제어, 모니터링 및 경보 시스템 • 추진 안전 시스템
발전 및 배전	• 엔진, 터빈, 발전기, 배터리, 다른 전력원 및 보조 기관을 위한 로컬 및 원격 제어, 모니터링 및 경보 시스템 • 전력 관리 시스템 • 전력원(power source) 안전 시스템 • 전기 회로 보호 시스템
조타	• 조타 장치 (방향타, 추진기, 워터젯 등) 및 조타 보조 장치를 위한 로컬 및 원격 제어, 모니터링 및 경보 시스템
항해	• 레이더 • 전자해도표시시스템(ECDIS) • 자동항해시스템 • 자동식별시스템(AIS) • 위치참조시스템(GPS, 등) • 선박항해기록장치(VDR) • 선교항해당직경보시스템(BNWAS) • CCTV • 항해등 시스템 • 기상 항로 지원 시스템 • 경사 및 자이로시스템(Heading/gyro system)
통신	• 외부 통신시스템(GMDSS, 위성, 무선(radio) 등) • 내부 통신시스템(PA, GA, 유선, 무선(radio) 등)
평형수	• 평형수 펌프, 밸브 및 센서를 위한 로컬 및 원격 제어, 모니터링 및 경보 시스템 • 로컬 계산(calculation) 시스템
앵커링	• 앵커링(anchoring) 및 윈치(winch) 제어 및 모니터링 시스템 • 자세 계류(mooring) 제어 시스템
화물 운영	• 화물 펌프, 밸브를 위한 로컬 및 원격 제어, 모니터링 및 경보 시스템 • 화물 높이(level), 압력 및 온도 모니터링 및 경보 시스템 • 화물 탱크 및 다른 화물 관련 안전 시스템 • 불활성 가스 제어 및 모니터링 시스템 • 선적(loading) 및 하역(offloading) 제어 및 모니터링 시스템 • 크레인 제어 및 모니터링 시스템 • 화물 조절(conditioning), 온도, 환기 시스템

화재 및 가스	• 화재 감지 시스템 • 가스 감지 시스템(가스 연료) • 방화문 제어 및 모니터링 시스템 • 화재 펌프 제어 및 모니터링 • 소화 시스템
점화원 제어	• 가스 탐지 시스템 • 비상 정지 시스템
거주 및 승객	• 환기 및 공조(climate control) 시스템 • 비상 안전/대응 시스템 • 홍수(flooding) 감지 시스템
배수(drainage) 및 빌지(bilge) 펌프	• 빌지 펌프, 밸브, 센서를 위한 로컬 및 원격 제어, 모니터링 및 경보 시스템 • 물 진입(ingress) 모니터링 및 경보 시스템
기타 시스템	• 보조(auxiliary) 보일러 제어 및 모니터링 시스템 • 보조 안전 시스템 • 소각기 제어 및 모니터링 시스템 • 주 경보 시스템 • 통합 제어, 모니터링, 경보 및 안전 시스템 • 재킹(jacking) 제어 및 모니터링 시스템 • 오염 예방 시스템