

전자기록부의 설비 및 보안 등에 관한 기술요건(제20조의2제1항 관련)

1. 하드웨어의 기술요건

- 가. 컴퓨터 및 주변기기 등의 하드웨어는 국제전기기술위원회(IEC)에서 정한 국제 전자·전기 기술 표준(60092 및 60533을 말한다)에 적합해야 한다.
- 나. 전자기록부는 종이문서와 같은 수준의 정보 연속성을 확보하기 위해 무정전 전원장치(UPS) 등 별도의 전원 공급 장치를 갖추야 한다.

2. 소프트웨어의 기술요건

가. 기능요건

- 1) 소프트웨어는 기록된 정보를 저장할 때 관련 항목의 입력이 완료되지 않으면 해당 기록된 정보의 저장 처리를 하지 않아야 한다.
- 2) 소프트웨어는 다음의 기능을 제공해야 한다.

가) 다음의 항목이 포함된 보안 관련 감사 로그를 생성할 수 있는 기능

- (1) 접속 에러
- (2) 요청 에러
- (3) 시스템 이벤트
- (4) 백업 및 복구 이벤트
- (5) 구성 변경
- (6) 감사 로그 이벤트

나) 위 가)(1)부터 (6)까지의 항목에는 다음의 항목이 포함되어야 한다.

- (1) 이벤트 시각
- (2) 소스(발신 장비, 소프트웨어 및 사용자 계정에 관한 정보를 말한다)
- (3) 카테고리
- (4) 형식
- (5) 이벤트 아이디
- (6) 이벤트 결과

다) 국제협약 부록 2 및 국제협약에 부수되는 전자기록부 승인 지침에 따라 전자기록부가 출력되는 기능

라) 전자기록부 작성자(이하 "작성자"라 한다)가 작성한 정보를 처리할 때 작성자의 서명을 요구하는 기능

마) 작성 단위별로 선장의 서명을 요구하는 기능

바) 이전의 작성 일시, 작성자 또는 작성 항목 등을 검색하거나 확인할 수 있는 기능. 이 경우 작성자의 자격이나 신원이 확인된 경우에만 검색하거나 확인할 수 있어야 한다.

사) 최초로 작성된 시간, 변경된 시간 및 작성·변경 이력이 검증된 시간을 확인할 수 있는 기능

아) 작성자가 전자기록부를 작성한 후 현재의 상태를 파악할 수 있는 기능

자) 전자기록부 작성 항목 중 승인되지 않은 항목이 있는 경우 선택이 항목에 입항하기 전에 선장에게 승인을 요청하는 기능

차) 선장이 작성자가 작성한 항목을 승인하지 않으려는 경우 그 사유를 작성하여 첨부할 수 있는 기능

카) 다음의 전자파일을 첨부할 수 있는 기능

(1) 선박평형수의 처리시설에의 배출과 관련된 계약서, 영수증 등의 전자파일

(2) 국제협약에 따라 화물기록부 등에 이서(裏書)가 요구되는 경우 이서된 화물기록부 등을 확인할 수 있는 전자파일

타) 종이문서와 같은 수준의 정보 보존성을 확보하기 위한 다음의 기능

(1) 별도의 오프라인 저장장치에 전자기록부에 기록된 정보를 백업할 수 있는 기능. 이 경우 백업 프로세스는 소프트웨어의 정상적인 작동에 영향을 미치지 않아야 한다.

(2) 별도의 오프라인 저장장치에 백업된 정보의 복원을 시작하기 전에 그 백업된 정보의 무결성(無缺性)을 확인하는 기능

(3) 작성된 항목이 변경될 때마다 별도의 오프라인 저장장치에 백업하는 기능

파) 기록된 정보의 무결성 검사를 수행하거나 지원할 수 있는 기능. 이 경우 검사 결과는 별도로 기록·보관되어야 한다.

하) 기록된 정보의 무결성 검사 시 기록물이 무단으로 변경되거나 기록된 정보의 변경을 시도한 사실이 발견되면 자동으로 선장 또는 작성자 등에게 통지하는 기능

3) 소프트웨어의 그래픽 사용자 인터페이스(GUI)는 별지 제6호서식의 선박평형수관리기록부의 형식으로 구성되어야 한다.

4) 선박평형수를 처리·교환·주입 및 배출(이하 "처리등"이라 한다)한 시간·위치 등 선박평형수의 처리등과 관련된 메타데이터를 소프트웨어가 자동으로 입력하는 기능을 제공하는 경우에는 자동 입력 기능의 고장에 대비하여 수동 입력 기능을 함께 제공해야 한다.

#### 나. 보안요건

1) 소프트웨어는 보안과 관련하여 다음의 기능을 제공해야 한다.

가) 사용자, 시스템 및 기록된 정보 등을 보호하기 위해 시스템 수준의 백업을 수행할 수 있는 기능. 이 경우 백업 프로세스는 소프트웨어의 정상적인 작동에 영향을 미치지 않아야 한다.

나) 접근 권한의 할당이 가능한 공식적인 사용자 등록 및 등록 해지 기능  
다) 모든 사용자 유형에 대한 접근 권한을 할당하거나 폐지하기 위한 공식적인 사용자 접근 권한 설정 기능

라) 특수 접근 권한에 대한 할당과 사용을 제한하고 통제할 수 있는 기능

마) 전자기록부의 사용을 인증받은 사람을 관리하는 다음의 기능

(1) 할당된 비밀 인증정보를 사용하는 경우 비밀번호를 구성하는 항목의 최소 개수 및 다양한 문자 유형으로 구성 가능한 비밀번호의 안정성을 조정할 수 있는 기능

(2) 공개 키(Public key) 기반 인증을 사용하는 경우 공개 키 기반 구조의 영역 범위에서 상호작용하고 작동할 수 있는 기능

(3) 대칭 키(Symmetric key) 기반 인증을 사용하는 경우 다음의 사항이 포함된 기능

(가) 대칭 키를 사용하는 상호 신뢰 확립 기능

(나) 공유 암호의 안전한 저장 기능

(다) 공유된 비밀에 대한 접속 차단 기능

(라) 인증에 사용되는 알고리즘, 국제적으로 인정되거나 권장되는 보안 관행에 따른 암호화 보안 매커니즘

(마) 그 밖에 국제적으로 인정된 자격 증명 매커니즘

바) 사용 권한 없는 사람의 접근을 차단하기 위한 변조 방지 기능 또는 무단 접근 감지 기능

사) 인가되지 않은 물리적 접근이 시도된 경우 선장에게 자동으로 통지하는 기능

아) 기록된 정보의 변경 내역이 선장에게 통지되고, 그 통지 내역이 보안 관련 감사 로그에 저장되는 기능

2) 소프트웨어에 적용되는 전자서명에는 다음의 인증 방식 중 하나 이상의 방식이 적용되어야 한다.

가) 사용자명과 비밀번호 입력을 통한 로그인 2단계 인증

나) 생체 인식 펜을 사용하는 서명패드 사용

다) 지문 인식 스캐너 사용

라) 그 밖에 해양수산부장관이 인정하는 인증 방식

다. 데이터요건

1) 전자기록부는 선박 내 다른 전자적 기록장치와 연계하여 정보를 입력하거나 출력할 수 있도록 데이터 형식을 구성해야 한다.

2) 기록된 정보는 마지막으로 기록된 날부터 5년 간 훼손, 위조, 비인가 접근 또는 비인가 공개 시도로부터 보호되어야 한다.

3) 기록된 정보가 변경된 경우에는 다음의 기능을 제공해야 한다.

가) 사용자 계정 및 선장의 승인 여부 등을 포함한 데이터 변경 이력 관리 기능

나) 데이터 출력 시 데이터 변경 여부 표시 기능

다) 선장이 변경된 데이터를 보완하거나 재검증한 결과를 시스템 담당자 등에게 통지하는 기능

4) 별도의 저장장치(이하 "별도저장장치"라 한다)에 저장되는 데이터는 다음의 형식으로 저장되어야 한다.

가) 암호화되어 정보에 대한 무단 접속이 불가능하고 데이터가 저장되면 기록의 수정이 불가능한 읽기 전용 형식

나) 데이터를 다른 저장소로 복사할 수 있는 형식

다) 데이터의 출력이 가능한 형식

5) 별도저장장치에 저장되는 정보는 다음의 형식으로 저장해야 한다. 이 경우 선장의 디지털 서명(이름 및 서명시각)을 포함하여 저장해야 한다.

가) 휴대전자문서(PDF) 포맷 형식

나) 휴대전자문서(PDF) 포맷 형식이 아닌 경우 주변의 전산 환경을 고려하지 않고 출력이 가능한 형식

6) 별도저장장치는 무결하고 지속적으로 보관 가능한 상태로 유지되어야 한다.

라. 유지보수요건

1) 국제협약이 개정된 경우 국제협약의 개정 내용을 반영하여 소프트웨어가 업데이트되어야 한다.

2) 업데이트는 개정된 국제협약이 발효되기 전까지 완료되어야 한다.