IACS統一規則（UR）E26及びE27の概要

- UR E26「船舶のサイバーレジリエンス」

- UR E27「船上のシステム及び機器のサイバーレジリエンス」

UR E26の概要

タイトル : Cyber resilience of ships
船舶のサイバーレジリエンス

主な内容 : 新造時におけるネットワーク構築に向けた設計や、それを踏まえた船舶の建造、就航後における書類の維持管理等に関する要件

関係者 : 主に、造船所／システム統合者
（供給者／機器製造者や船主との相互協力も必要）

UR E26の目次 （主に造船所／システム統合者向け、ただし、供給者や船主の協力も必要）

- IACS Rec 166
- BIMCOガイドライン
- NIST SP 800-53
- IEC 62443

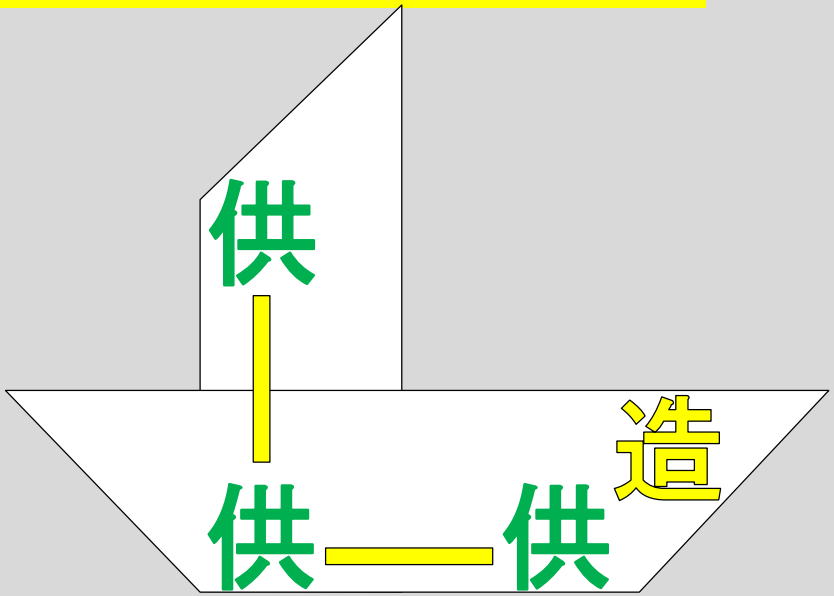
等を参考に規定

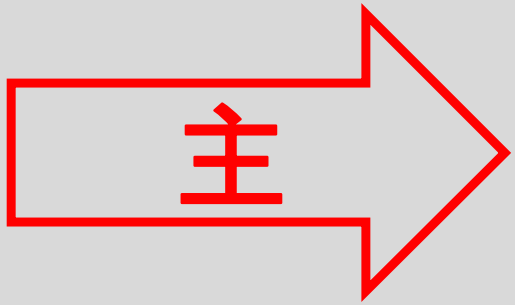
1. 導入 ・・（3ページ）
   - サイバーレジリエントといえる船舶を提供するための統一的な最低要件を制定
   - 適用対象は（UR E27でもこれと同じ）
     - OTシステム（航海設備や無線通信設備を含む）
       → IEC 61162-460によることができる
     - 当該OTシステムとInternet Protocolベースの通信ができる他のシステムとのインターフェースまで
   - ゴールベースアプローチ

2. 定義 ・・（3ページ）

3. ゴール及び要件の構成 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・（1ページ）
   - ゴール：サイバーレジリエントな、安全で保護された海運をサポート
   - サブゴール：識別、防御、検知、対応、復旧
   - 各要件に根拠も明示（UR E27よりも情報量が多い）
   - 設計、建造、就航後の各段階でなされるべきことも（Appendixに）記載

＜直後3枚のスライドの補足＞





供給者
供給者
供給者
→ 造船所/システム統合者 → 船主/会社

（Supplier） （Shipyard/System Integrator） （Shipowner/Company）

次ページ以降、要件への関係の深さのイメージを供／造／主で示す。
ただし、それは厳密なものではなく、その記載にかかわらず、相互の協力が不可欠なものも多いことに注意が必要。詳しくはUR本文参照。

4. 要件

4.1 識別／Identify ・・（1項目、1ページ半）

供造主 - ハードウェア、ソフトウェア、ネットワーク関するインベントリを作成し、船舶の一生にわたって更新すること。

4.2 防御／Protect ・・（7項目、7ページ）

造主 - セキュリティゾーンを超える通信は、明示的に許可されたものに限定すること。

造 - ファイアウォール等で防御し、過度のデータフローも防ぎ、不要な機能は制限すること。

供 造 主 - ウィルス対策ソフト等で防御すること。（手順や物理的保護、製造者の推奨によっても可。）

供造主 - アクセス制御として、鍵を掛け、部外者によるアクセスは監視下に限り、取外し可能なメディアの使用も管理し、アクセス権も管理し、最小権限の原則を適用する等を行うこと。

造 - 無線通信は、許可された人／プロセス／デバイスに限定し、暗号化等も活用すること。

供 造 主 - 遠隔アクセスは明示的な許可を要し、ログを残す等して、保守時もロールバックや多要素認証等を求め、アクセス失敗後一定時間は再試行不可、多数失敗でブロック等を行うこと。

造主 - 携帯用及び可搬式デバイスの接続は、船舶の運航や保守に必要ないものはブロックすること。

4.3 検知／Detect・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・（2項目、1ページ半）

造主 - ネットワークを監視し、過大なトラフィックや不正な接続等の異常時に警報を発すること。

4.4 対応／Respond・・・・・・・・・・・・・・・・・・・・・・・・・・・・・（4項目、3ページ）

供 造 主 - インシデント対応計画書を、設計の情報も集めて、初回年次検査までに作り、船の一生にわたり更新し、紙で保持すること。

供造 - バックアップの機側制御は、主制御システムから独立し、監視も制御も自己完結していること。

造 - ネットワークの分離は、手動又は自動で物理的に実行でき、データ依存性も明示しておくこと。

供造 - 機能不全時にミニマルリスクコンディション（状況に応じた低リスクの停止状態等）に至ること。

4.5 復旧／Recover・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・（3項目、3ページ）

供 造主- 復旧計画書を、設計の情報（復旧やバックアップの手順、ネットワークの構成図等）も集めて、初回年次検査時までに作り、船の一生にわたり更新し、船上及び陸上に紙で保持すること。

造主- バックアップ計画書を作成し、バックアップ及びリストアが、適時に完全に安全に行えること。

造 - 制御されたシャットダウン、リセット、ロールバック、再起動を、文書に従って行えること。

5. 機能の評価と試験のための試験方案 ・・・・・・・・・・・・・・（2ページ）

供 - 設計及び建造段階で、機器に関する試験方案及び試験結果報告書を作成及び更新。

造 - ネットワーク全体に関しても、試験方案及び試験結果報告書を作成及び更新。

造主 - 変更を管理しつつ更新した試験方案の最新版が、現実と合っていることを検証。

主 - 就航後も試験方案を更新、運用手順も定め、定期的訓練や操練も実施して管理。

6. 要件の適用対象から除外する際に用いるリスク評価・・（2ページ）

造主 - 適用しない要件の一覧表を船上に保管すること。

造 - 設計及び建造段階では、造船所がリスク評価を実施及び更新すること。

主 - 就航後は船社が更新して船級に提出すること。船級は受入れ又は拒否できる。
受入れ可否の判断基準が12点示されているが、これらと異なる説明も可。

Appendix 行動及び提出図書の要旨 ・・・・・・・・・・・・・・・・・（5ページ）

供造主 - 各文書につき、要求されるのはどの段階（設計、建造、試運転、運航、検査）で、作成、更新、提供するのは誰（供給者、造船所／統合者、船社）で、それを船級はどうするのか（承認、確認等）等を一覧表にまとめたもの。

UR E27の概要

タイトル : Cyber resilience of on-board systems and equipment
船上のシステム及び機器のサイバーレジリエンス

主な内容 : **機器の設計及び製造時に組み込むサイバー関連機能、並びに、設計開発の各段階におけるセキュリティ面の取扱いに関する要件**

関係者 : **主に、供給者／機器製造者**

UR E27の目次　（主に供給者向け）

1. 一般　・・・・・・・・・・・・・・・・・・・・・・・　（1ページ半＋定義2ページ）
2. セキュリティの考え方　・・・・・・・・・・・・・・・・・・・・・・・（1ページ）
3. 承認用に船級協会宛てに提出いただく図書　・・・（1ページ半）
4. システムに関する要件
   - 4.1　要求されるセキュリティ機能　・・・・・・・・・・（3ページ）
   - 4.2　追加のセキュリティ機能　・・・・・・・・・・・・・・・・（1ページ）
5. 製品の設計及び開発に関する要件　・・・・・・・・・・・（2ページ）

Annex I　関連するUR及び参考文献　・・・・・・・・・・・（半ページ）

IEC 62443-3-3ベース

IEC 62443-4-1ベース

1. 一般 ・・・・・・・・・・・・・・・・・・・・・・・・ （1ページ半＋定義2ページ）

- 機器及びシステムの設計及び製造段階におけるセキュリティ機能の組込みを要するような、継続的に発展する一連の管理策が必要
- サイバーレジリエントといえるシステム及び機器を提供するための統一的な最低要件を制定
- システムのハードウェアの耐環境性能 ⇒ UR E10による
- ソフトウェアの機能に関する機器の安全性 ⇒ UR E22による
- 適用対象は、UR E26と同じ
  - OTシステム（航海設備や無線通信設備を含む）
    → IEC 61162-460によることができる
  - 当該OTシステムとInternet Protocolベースの通信ができる他のシステムとのインターフェースまで

2. セキュリティの考え方 ・・・・・・・・・・・・・・・・・・・・・・・・ （1ページ）

- 「機器」とは、ネットワークデバイス、セキュリティデバイス、コンピュータ、自動化デバイス、クラウド上の仮想マシン等

- 要件を満たすため、本来のセキュリティ機能に代えて又は加えて、補完的対策（同等以上の別の対策）を採用することもできる

- 型式承認に際しては、システム内で補完的対策が実行されるべき、すなわち、船上の設備や操作手順によるバリアに頼らないべき

- 不可欠なシステムについてのセキュリティ対策は、当該システムの可用性に悪影響を及ぼすものであてはならない

3. 承認用に船級協会宛てに提出いただく図書 ・・・（1ページ半）

- インベントリ（システムに含まれる機器の詳細な一覧）
- 各機器に関連するハードウェアの詳細
- ソフトウェアの一覧
- ネットワーク又はシリアルのフロー
- ネットワークセキュリティ機器
- セキュア開発ライフサイクル文書（セクション5参照）
- システムの保守計画書
- 復旧計画書
- システムの試験方案
- システムが要件をどのように満たすかの記述
  （取扱説明書又は使用者マニュアル等）
- 変更管理計画書

＜直後4枚のスライドの補足＞

- 参照先として、IEC規格の該当箇所が明記されている。

  IEC 62443-3-3・・・産業用通信ネットワーク – ネットワーク及びシステムセキュリティ –
  第3-3部：システムセキュリティ要求事項及びセキュリティレベル

  IEC 62443-4-1・・・産業用オートメーション及び制御システムのセキュリティ –
  第4-1部：安全な製品開発ライフサイクル要求事項

- IEC規格の該当箇所には、次に示す情報がある。
  - 「Requirement」
  - 「Rationale and supplemental guidance」← 内容理解に有用

4. システムに関する要件

4.1 要求されるセキュリティ機能 ・・・・・・・・・・・・（3ページ）

① 使用者（人）の識別及び認証（IEC 62443-3-3中、5.3.1一部変更）
② アカウントの管理（同5.5.1）
③ 識別子の管理（同5.6.1一部変更）
④ 認証コードの管理（同5.7.1）
⑤ 無線アクセスの管理（同5.8.1）
⑥ パスワードによる認証の強度（同5.9.1一部変更）
⑦ 認証時のフィードバック（同5.12.1一部変更）
⑧ 権限付与の実施（同6.3.1一部変更）
⑨ 無線の使用の管理（同6.4.1）
⑩ 可搬式及び携帯用デバイスの使用の管理（同6.5.1一部変更）
⑪ モバイルコード（同6.6一部変更）
⑫ セッションロック（同6.7.1一部変更）
⑬ 監査可能な事象（同6.10.1一部変更）
⑭ 監査用の記憶容量（同6.11.1一部変更）

(2) UR E27の概要（船上のシステム及び機器のサイバーレジリエンス）

⑮	監査プロセスの不具合への対応	（同6.12.1一部変更）
⑯	日時の記録	（同6.13.1一部変更）
⑰	通信の完全性	（同7.3.1一部変更）
⑱	悪意のあるコードからの保護	（同7.4.1一部変更）
⑲	セキュリティ機能の検証	（同7.5.1一部変更）
⑳	入力の検証	（同7.7.1一部変更）
㉑	あらかじめ決定した出力	（同7.8一部変更）
㉒	情報の機密性	（同8.3.1）
㉓	暗号の使用	（同8.5.1一部変更）
㉔	監査ログへのアクセス	（同10.3.1）
㉕	サービス拒否攻撃からの保護	（同11.3.1一部変更）
㉖	リソースの管理	（同11.4.1）
㉗	システムのバックアップ	（同11.5.1）
㉘	システムの復旧及び再構成	（同11.6.1）
㉙	非常用電源	（同11.7.1）
㉚	ネットワーク及びセキュリティ構成設定	（同11.8.1）
㉛	最小限の機能性	（同11.9大きく変更）

4.2 追加のセキュリティ機能 ・・・・・・・・・・・・・・・（1ページ）

信頼できないネットワークと通信を行うシステムに、追加で適用

||

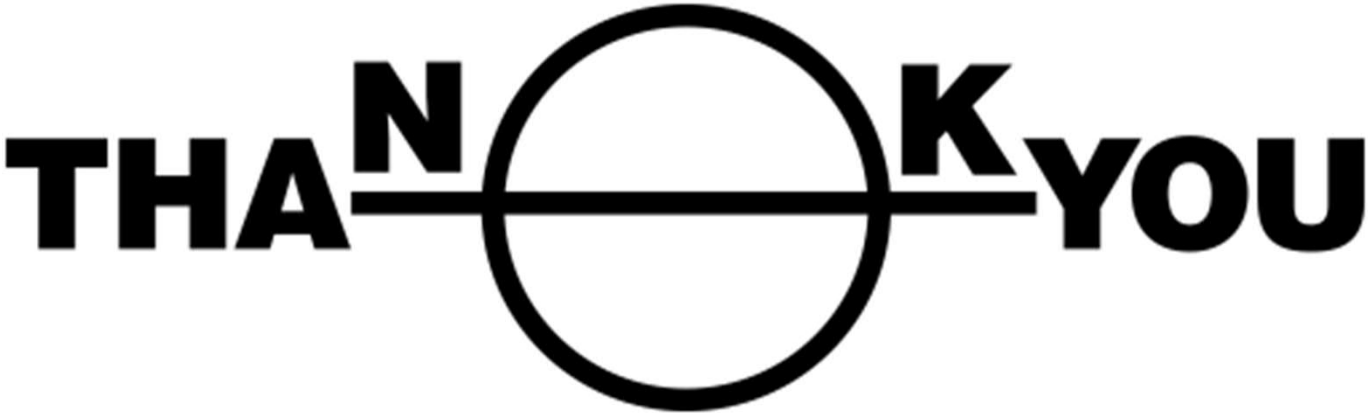
OTシステムと他のシステムとのインターフェース

㉜	使用者（人）の多要素認証（IEC 62443-3-3中、5.3.3.2一部変更）	
㉝	ソフトウェアプロセス及びデバイスの識別及び認証	（同5.4.1一部変更）
㉞	失敗したログイン試行	（同5.13.1一部変更）
㉟	システム使用通知	（同5.14.1）
㊱	信頼できないネットワーク経由のアクセス	（同5.15.1一部変更）
㊲	アクセス要求の明示的な承認	（同5.15.3.1一部変更）
㊳	リモートセッションの終了	（同6.8.1）
㊴	暗号化による完全性の保護	（同7.3.3.1一部変更）
㊵	セッションの完全性	（同7.10.1一部変更）
㊶	セッション終了後のセッションIDの無効化	（同7.10.3.1一部変更）

5. 製品の設計及び開発に関する要件 ・・・・・・・・・・（2ページ）

（IEC 62443-4-1：産業用オートメーション及び制御システムのセキュリティー
第4-1部：安全な製品開発ライフサイクル要求事項）

- セキュア開発ライフサイクル（SDLC／Secure Development Lifecycle）文書に、各段階（要件分析、設計、実装、検証、リリース、保守、終了）でセキュリティ面をどう扱ったかを記録し、承認用に船級協会宛てに提出いただく。
- コード署名に使用する秘密鍵を不正アクセス又は改ざんから保護する管理策を保有する。(IEC 62443-4-1/SM-8)（SM：セキュリティマネジメント）
- 製品のセキュリティ更新に関する文書を、使用者に入手可能にする。（IEC 62443-4-1/SUM-2）（SUM：セキュリティアップデートマネジメント）
- 製品が，依存するコンポーネントに又はOSのセキュリティ更新に対応しているかどうかを記載した文書を、使用者に入手可能にする。(IEC 62443-4-1/SUM-3)
- セキュリティ更新が，セキュリティパッチが本物であることを検証できる方法で，製品使用者に入手可能にする。(IEC 62443-4-1/SUM-4)
- 製品に関する文書であって，セキュリティに関する多層防御の戦略を記述したものを作成する。（IEC 62443-4-1/SG-1）（SG：セキュリティガイドライン）
- 製品使用者に関する文書であって，外部の環境から提供されることが期待されるセキュリティ上の多層防御の手段を記述したものを作成する。(IEC 62443-4-1/SG-2)
- 製品使用者に関する文書であって，製品のインストール時及び保守時における製品のハードニングの指針を含むものを作成する。(IEC 62443-4-1/SG-3)



for your kind attention