1. NK のサイバーセキュリティの取り組みについて

1. はじめに

IT（情報技術）の進展に伴いサイバー攻撃が公共機関や企業の活動を麻痺させるリスクが高まっており，海運界においても航行安全の侵害や経済的被害等の様々なリスクが懸念されています。

また, 2021 年から ISM コードに基づく安全管理システムの中へサイバーリスクに対するマネジメントを取り込むことが事実上要求されるとみられており，船舶におけるサイバーセキュリティ対策に関心が高まってきております。

本件に関し，船級協会の立場からこれまで IMO（国際海事機関）や IACS(国際船級協会連合)における取組を紹介し，日本海事協会がこれまでに公表したサイバーセキュリティに関する基本的な考え方やガイドライン，及び今後発行予定のガイドラインや NK サイバーノーテションの取得の方法についても説明いたします。

2. サイバーセキュリティに関する最新動向

2.1 IMO（国際海事機関）

IMO は第 98 回の海上安全委員会にて，“安全管理システムにおける海事サイバーリスクマネジメント”(Res.MSC.428(98))を採択。この決議の内容としては，ISM コードの目的及び機能要件に従って，サイバーリスクマネジメントを安全管理システムにおいて考慮すべきとの要件が盛り込まれ，2021 年 1 月 1 日より後の，最初の DOC 年次審査までに，サイバーリスクが安全管理システムで適切に対処していることを RO 等に確認されることが必要となります。上記決議を強制要件とする旗国は，2020 年 8 月末の情報でマーシャル諸島，ケイマン諸島，キプロス，オーストラリア，英国，リベリア，シンガポール，バヌアツとなっています。

2.2 IACS（国際船級協会連合）

IACS は 2016 年 7 月にサイバーシステムパネルを立ち上げ，2018 年 11 月までに下記 12 の Recommendations (勧告）が公表されました。

・No.153 ソフトウェアの保守手順
・No.154 機器の手動/機側制御
・No.155 緊急時対応計画
・No.156 ネットワーク構造
・No.157 データの保証
・No.158 物理的セキュリティ
・No.159 ネットワークセキュリティ
・No.160 船舶システムデザイン
・No.161 インベントリリスト

・No.162 インテグレーション
・No.163 遠隔アップデート/アクセス
・No.164 通信及びインターフェース

IACS は上記 12 の Recommendation を 1 つに統合する作業を実施し，2020 年 5 月に No.166 Recommendation on Cyber Resilience として統合した Recommendation を発行しております。今後 IACS では，この Recommendation No.166 を UR 化とし強制要件とする作業を行っています。

2.3 MTS-ISAC への加盟

サイバーセキュリティの分野では，各国において業界ごとの情報共有・分析のために，ISAC（Information Shearing Analysis Center）が組織化されています。（日本でも金融 ISAC，電力 ISAC，医療 ISAC 等が存在）この中で米国の非営利団体として，海事分野に特化した MTS-ISAC が設立されたことから，2020 年 7 月 7 日に，船級協会として，また米国外の法人として，初めて NK が加盟いたしました。

これにより海事分野に関する最新のサイバーセキュリティ情報を入手することができ，効果的な NK のサイバーセキュリティ対策を提案することができるものと考えます。

3. NKサイバーセキュリティガイドラインの紹介

3.1 サイバーセキュリティに対する考え方

2019 年 2 月に日本海事協会のサイバーセキュリティに関する基本的な考え方を「ClassNK サイバーセキュリティアプローチ」として公表致しました。

サイバーセキュリティの最重要事項は船舶の安全運航の確保であり，船舶の運航を支える IT（情報技術）及び OT（運用・制御技術）における可用性の確保が最優先となり，セキュリティ・バイ・デザインな設計，就航後のマネジメントシステムの構築が重要となります。これらのサイバーセキュリティ対策を理解するための概念図は図 1 となります。

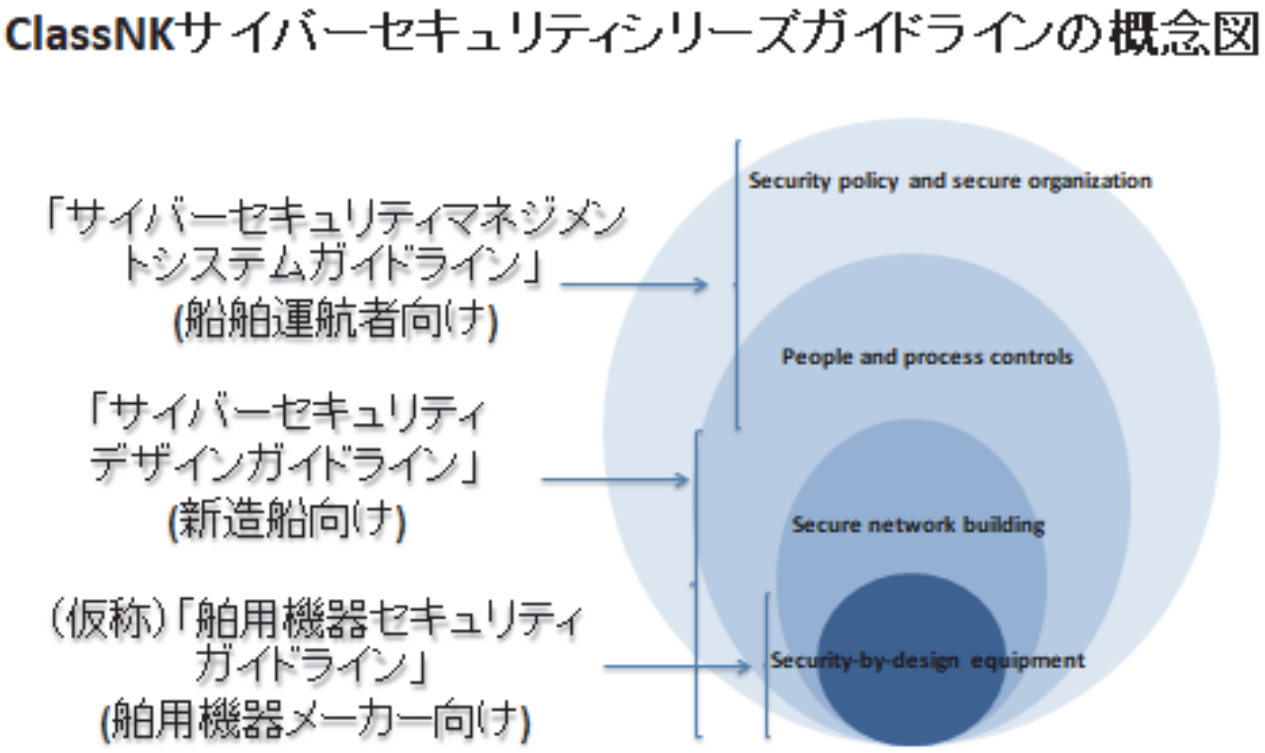


図 1　サイバーセキュリティの階層

図 1 で示す階層ごとに，既存の情報セキュリティの国際規格等から船舶へ適用可能な部分を採用し，「どの関係者が何をすべきか」について明確化にしております。

「ClassNK サイバーセキュリティアプローチ」は，現在公表されているものが最終ではなく，最新のサイバーセキュリティ情報を専門家と共に分析を行い継続的に見直しと最新化が行われる予定です。

3.2　ガイドラインの公表

「ClassNK サイバーセキュリティアプローチ」に基づき日本海事協会は，現在 3 つのガイドラインを公表しております。

3.2.1　「船舶におけるサイバーセキュリティデザインガイドライン」（第 2 版）

図 1 の”Secure network building”と”People and process　control”をカバーするガイドラインであり，主に造船所及び建造船主向けのものとなっています。IEC62443-2-1 及び IEC62443-3-3 の中で船舶建造に適用できるものを抽出，また IACS Rec.No.166 の要件を推奨事項として掲載。

3.2.2　「船舶におけるサイバーセキュリティマネジメントシステム」（第 1 版）

図 1 の”Security policy and secure organization”と”People and process control”をカバーするガイドラインであり，船主及び船舶管理会社向けのものとなっています。

ISO27001 と 27002 の基本構造を参考に，ISM コード体系との親和を図ったマネジメント

システムを運用できることが前提のガイドラインとなっており，日本海事協会では本ガイドラインに沿った認証サービスをすでに開始しています。

3.2.3 「ソフトウェアセキュリティガイドライン」

図 1 の”Secure-by-design equipment”をカバーするガイドラインであり，主に舶用機器メーカー向けに対するものとなります。サイバーセキュリティに関する，ISO/IEC 規格をベースに舶用に必要な要素を抽出したものであり，ソフトウェアの開発プロセスと機能要件を検証するためのガイドラインとなります。本ガイドラインの運用による認証はすでに実施可能な体制にあります。

3.3 今後のガイドライン検討の方向性

日本海事協会では，”Secure-by –design equipment”「ソフトウェアセキュリティガイドライン」にかわるガイドラインとして，（仮称）舶用機器ガイドラインの発行を予定しています。その内容としてはセキュリティ・バイ・デザインな舶用機器を設計及び審査するためのガイドラインを予定しており，コンピュータシステムのハード及びソフトに対してサイバーセキュリティに関する Type Approval を与えるガイドラインを予定しております。

本件に係る技術要件としては，制御システムセキュリティに関する基準である IEC62443 を適用することを予定していますが，IEC62443 の要件をすべて適用するのではなく，舶用製品に重要とされるものを抽出することを考えております。発行については 2021 年 4 月を予定とし作業を行っております。

4. NK サイバーノーテーション取得の手順

「船舶におけるサイバーセキュリティデザインんガイドライン」（第 2 版）を適用することにより，新造船に対して NK サイバーノーテーション**“CybR-G”**を付与することが可能となりました。NK サイバーノーテションに関する取得の手順は ，下記 4.1 項～4.8 項の流れで実施するものと考えていますが，船舶の仕様，工程等により適宜変更することは可能とです。

4.1 基本設計書（Design Philosophy Document）の作成

IACS Rec.166 によると，機能を簡単説明したコンピュータベースシステムの目的及び制御可能な各種システムを明確に特定したシステムブロック図を作成することとなっています。これは自動運航船等の船内に複雑なネットワークシステムを有する船舶について，その概要を把握するために必要な資料と考えられます。しかしながら従来の船舶のようにコンピュータネットワークが船内の一部に限定され複雑なネットワークシステムを有することのない船舶については，特段基本設計書を作成する必要は無いものと考えられます。

NK デザインガイドラインにおいて，基本設計書の作成及び提出は要求されるものではありませんが，上記の通り複雑なネットワークシステムを有する船舶については関係書の認識を共通とするためにも基本設計書の作成を推奨いたします。

4.2　インベントリリストの作成

本船上に装備されるすべてのコンピュータシステムを記載したインベントリリストを作成する必要があります。インベントリリストの目的としてはサイバー攻撃から守るべき機器の識別が主な目的と考えられます。

インベントリリスト作成の第一段階としては船内のすべてのコンピュータシステムのリストアップを行うこととなります，リストアップされたコンピュータシステムの中から本船の運航 ，安全等への影響度をレベル分けし，サイバー攻撃から守るべき重要なコンピュータシステムの判別を行うこととなります。

重要度が判別された後は, 各コンピュータシステムがネットワークに接続されるか否か，機器本体に有している通信ポート，USB ポート及び無線通信機能の有無及びそれらの使用状態を明確にしインベントリリストに記載する。

4.3　単純なネットワーク図の策定

インベントリリストにより判別されたネットワークに接続されている重要用途の機器について，各機器がどのように接続されるかの調査をおこない，船内ネットワークシステムを把握する。この段階で策定するネットワーク図は詳細な情報が記載されている必要は無く，次項で要求されるリスクアセスメントに対応できるものであれば問題ありません。

具体的には，TCP/IP 通信がどのようなシステム間で行われているかを明示されていれば問題ないものと考えます。一般的なシリアル通信についてはサイバー攻撃の直接的な対象と考えられないので，参考として記載されていることを推奨いたします。

4.4　リスクアセスメントの実施

リスクアセスメントについては，基本的に 2 段階で実施されることを推奨いたします。

第 1 段階としては，各機器製造者による自社製のコンピュータシステムに対するリスクアセスメントとなります。第 1 段階のリスクアセスメントが必要な機器は，インベントリリスト作成時に重要用途と判断された機器が対象と考えます，リスクアセスメントは主としてネットワーク経由のサイバー攻撃を考慮する必要があると考えられますが，ネットワークに接続されていない機器にあっても，悪意のある第 3 者による機器への直接接続によるサイバー攻撃の可能性が否定できないので，スタンドアロンの機器であってもリスクアセスメントは必要と考えます。

第 2 段階は統合者によるリスクアセスメントが必要と考えます。統合者はインベントリリスト，単純なネットワーク図及び製造者によるリスクアセスメントの結果を考慮し，本船のネットワークシステム全体についてリスクアセスメントを実施する必要があります。

リスクアセスメントはネットワーク構成のみならず，本船の物理的な配置についても考慮して行う必要があるものと考えます。

4.5　詳細なネットワーク図の策定

統合者はリスクアセスメントの結果を考慮して，詳細なネットワーク図を策定することとなります。リスクアセスメントにより許容できないリスクが顕在化することとなりますが，これらのリスクを低減するために各種のセキュリティ対策を検討し，その対策を盛り込んで詳細なネットワーク図を策定していただきます。

4.6　ネットワークシステムの有効性確認

統合者は，適用された各種のセキュリティ対策について，その有効性の評価を実施しリスクが十分低減されることを確認されなければならない。また有効性評価の結果については文書化し保管される必要があります。

4.7　現場審査及び試験

有効性が確認されたネットワークシステムについて，詳細なネットワーク図と現場のネットワークが同一であることについて，NK 審査員の確認が必要となります。また審査員立ち合いのもとセキュリティ試験を実施していただくこととなります。

4.8　完成図面の作成及び船上への保管

統合者は本船の完工までに,「船舶におけるサイバーセキュリティデザインガイドライン」（第 2 版）3 章 3.3.3 に規定された図面等を完成図面として準備していただき，本船に保管していただくこととなります。

5.　まとめ

2021 年以降は ISM コードにおいて, サイバーリスクを扱うことが要求されることとなることから，船舶管理者は配下の既存船に対して，サイバー対策を行うことが必要となります。具体的な対策として ISM コードに基づく安全管理システムと別にサイバーセキュリティマネジメントシステム（CSMS）を構築し運用するスキームが主流となることが予想されます。また，新造船にあっては，IACS が公表した Recommendation No.166 が，将来的に統一規則化(UR 化)されることから，造船所，機器メーカーにあっては，近い将来 IACS 統一規則(UR)に適合した船舶を設計することが要求されるものと考えられます。

このような状況の中で，日本海事協会としては，常に新しい情報を収集し，ガイドラインを適切に改訂することで，関係各者へ有益なサービスを提供してまいります。

NKのサイバーセキュリティに関する取り組み

1. サイバーセキュリティに関する最新動向
2. NKサイバーセキュリティガイドラインの紹介
3. NKサイバーノーテーション取得の手順

1. サイバーセキュリティに関する最新動向

IMO Resolution MSC.428(98)（16 June 2017）

MSC決議

Maritime Cyber Risk Management in Safety Management Systems

安全管理システムにおける海事サイバーリスクマネジメント

- サイバーリスクの脅威と脆弱性に対する意識を高めることが緊急に必要
- ISMコードの目的及び機能要件に従って，サイバーリスクマネジメントを安全管理システムにおいて考慮されるべき
- 2021年1月1日より後，最初のDOC年次審査までに，サイバーリスクが安全管理システム（SMS）で適切に対処されていること

➡ サイバーリスクに対するリスクマネジメントの構築

1. サイバーセキュリティに関する最新動向

ClassNK

MSC.428(98)に関するサーキュラーを発出し強制化を表明した旗国 (2020年10月16日現在)

オーストラリア，バハマ，ケイマン諸島，キプロス，リベリア，マーシャル諸島，ミャンマー，ノルウェー，シンガポール，英国，バヌアツ

1. サイバーセキュリティに関する最新動向

ClassNK

国際船級協会連合（IACS）はサイバーセキュリティに関する推奨事項を公表

- **サイバーシステムパネル (2016年7月～)**

  2018年11月　12本の推奨事項を公表

  2020年　5月　12本をまとめて1本化した推奨事項 Rec.166を公表

“Based on the experience gained from the practical implementation of this Recommendation IACS will assess the suitability of using it as the basis for a Unified Requirement on Cyber Resilience.”

Unified Requirement : IACS 統一規則 (IACSホームページより)

本推奨事項を強制要件化すべくIACSにて議論を開始

1. サイバーセキュリティに関する最新動向

ClassNK

NKは海事分野に特化したサイバーセキュリティの情報共有・分析のため，“MTS-ISAC”（米国）に加盟しました

Maritime Transportation System ISAC
https://www.mtsisac.org/

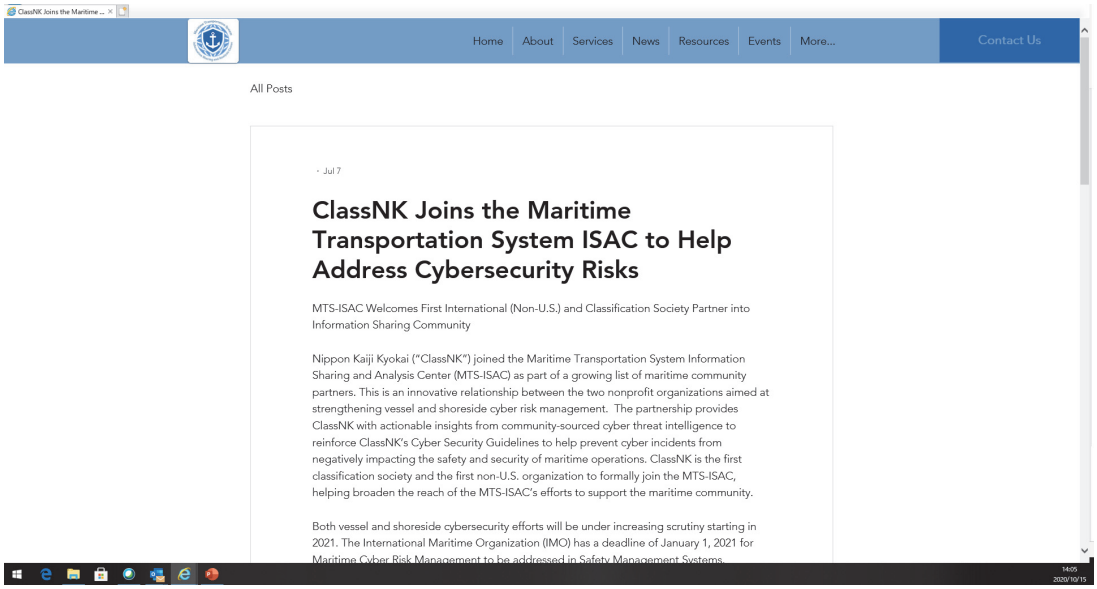
- サイバーセキュリティの分野では，各国において業界ごとの情報共有・分析のために，ISAC（Information Shearing Analysis Center）が組織化されている（日本でも金融ISAC，電力ISAC，医療ISAC等が存在）
- 米国の非営利団体として，海事分野に特化したMTS-ISACが設立された。
- 2020年7月7日，船級協会として，米国外の法人として，初めてNKが加盟

最新の情報分析に基づくサイバーセキュリティ対策要件を提案

1. サイバーセキュリティに関する最新動向

ClassNK

MTS-ISACのHPに掲載された，NKがMTS-ISACに加盟したことを知らせるニュース（MTS-ISAC HPより）



2. NKサイバーセキュリティガイドラインの紹介

2. NKサイバーセキュリティガイドライン

日本海事協会としての基本的な考え方を「ClassNK サイバーセキュリティアプローチ」として公表（2019年2月）

1. 最重要事項は安全運航の確保

- 船舶の運航を支えるIT及びOTにおける可用性の確保を優先
- セキュリティ・バイ・デザインな設計，就航中のマネジメントシステムの構築

2. サイバーセキュリティ対策の階層を設定

- サイバーセキュリティ対策をいくつかの階層で整理
- 階層ごとに，既存の情報及び制御セキュリティの国際規格等から船舶へ適用可能な部分を採用し，「どの関係者が何をすべきか」について明確化

3. 継続的な見直しと最新化

- 最新のサイバーセキュリティ情報を専門家と共に分析
- 船舶におけるサイバーセキュリティ対策について，その時点におけるベストプラクティスを提案

現在発行済みのNKサイバーセキュリティガイドライン

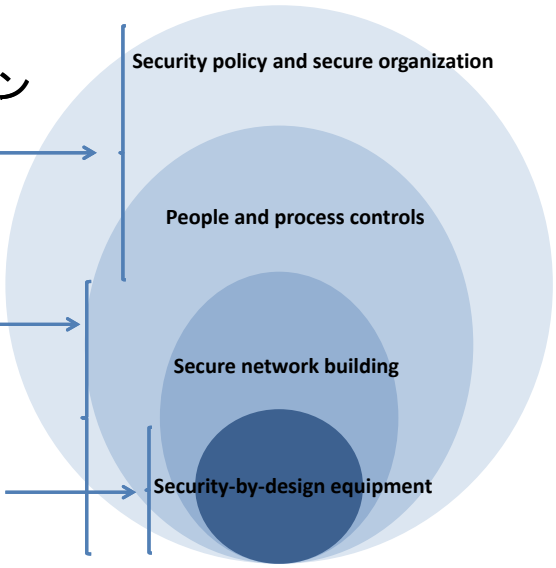
名称	対象	参照規格
船舶におけるサイバーセキュリティマネジメントシステム（第1版）	就航船及び船舶管理会社	ISO27001, ISO27002
船舶におけるサイバーセキュリティデザインガイドライン（第2版）	新造船	IEC62443-2-1, IEC62443-3-3 IACS Rec.No.166
ソフトウェアセキュリティガイドライン（第1版）	ソフトウェア開発者	ISO/IEC27001, ISO27002 ISO/IEC27005, ISO/IEC27034-1等

ClassNKサイバーセキュリティガイドラインの概念図

「サイバーセキュリティマネジメントシステムガイドライン」
(船舶運航者向け)

「サイバーセキュリティデザインガイドライン」
(新造船向け)

「ソフトウェアセキュリティガイドライン」
(舶用機器メーカー向け)



船舶におけるサイバーセキュリティマネジメントシステム

（要求事項及び管理策）2019年2月 第1版

対象：**船舶管理会社**及び**船舶**に**証書**を

ISMコードと同じサイクルで発給

ISO27001及び27002の基本構造を参考にISMコード体系との親和を図ったマネジメントシステム

認証取得のポイント

・ネットワーク構成図に基づくリスクアセスメントの実施

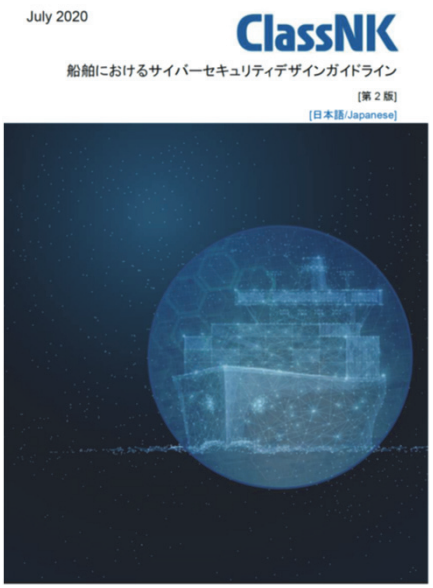
・リスクアセスメントに基づく管理策の実施

船舶におけるサイバーセキュリティデザインガイドライン

2019年2月　第1版（適用船無し）

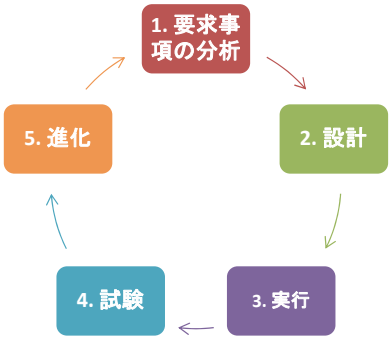
2020年7月　第2版

- 対象：新造船
- サイバーノーテーション(CybR-G)
- IACSの最新の推奨事項を適用
- 将来的なIACSの強制要件化へ向けたトライアルを開始
- すでに第2版に基づくノーテーションを受注



ソフトウェアセキュリティガイドライン　2019年5月　第1版

- 対象：舶用機器メーカー
- ISO/IECの関係規格をベースに舶用に必要な要素を抽出したガイドラインに基づき、その開発プロセスと機能要件を検証する



（仮称）舶用機器セキュリティガイドライン

2021年4月　発行予定

- 対象：舶用機器メーカー
- 内容：コンピュータを使用した舶用機器（ハード及びソフト）に対してサイバーセキュリティのType Approvalを与えるためのガイドライン

IEC62443-4-1，4-2の規定を取り込むことを予定しており，製品に対する技術要件の承認及び開発プロセスに対する承認を適用することを検討中。
現在発行済みのソフトウェアガイドラインの要件を考慮。

3. NKサイバーノーテーション取得の手順

NKサイバーノーテーション：CybR-G

取得のプロセス

設計

- インベントリリスト
- ネットワーク図
- リスクアセスメント

建造

- ネットワークの実装
- 現場審査及び試験

船級取得

- 証書発行
- （船級証書へCybR-Gの記載）

建造段階における本船のサイバー対策を審査しノーテーションを付与

3. NKサイバーノーテーション取得の手順

ClassNK

新造船，サイバーノーテーション適用船に対する設計及び審査の流れ

1. 基本設計書の作成 (DPD)
2. インベントリリストの作成
3. 単純なネットワーク図の策定
4. 船内ネットワーク全体のリスクアセスメント
5. 詳細なネットワーク図の策定
6. ネットワークシステムの有効性評価
7. 現場審査及び試験
8. 完成図面の作成及び船上に保管

3. NKサイバーノーテーション取得の手順

ClassNK

1.基本設計書（DPD)の作成

IACS Rec.166
7.1.2　システムドキュメント
7.1.2.1 カテゴリI，II，IIIシステム，及び上記と連動するその他のコンピュータベースのシステムの設計/プロジェクトコンセプトフェーズでは，以下の文書を作成する必要がある。

1) 基本設計書
以下の情報から構成される基本設計書を作成すべきである。
a. 機能を簡単に説明したコンピュータベースのシステムの目的
b. 制御可能な各種システムを明確に特定したシステムブロック図又は計画を作成し，以下の情報を示す。
i.制御，監視および管理機能のための外部ネットワークとの通信のモデル
ii.関連システム

NKデザインガイドラインではDPDの作成は要求していないが，複雑な船内ネットワークシステムを構築する場合は，DPDの作成を推奨する。

2. コンピュータシステムのインベントリリストの作成

「船舶におけるサイバーデザインガイドライン」

3.3.1　図面及び資料

-1.　4.1.1に規定されるコンピュータ機器リスト

船内に設置されるコンピュータシステムの一覧を作成し，コンピュータシステムの識別及び評価を実施する。

インベントリリストへ記載すべき情報（IACS Rec.166, 7.1.2.2インベントリ―リスト）

名称，製造者，型式，組み込みファームウェアのバージョン，物理特性，設置場所，接続されているスイッチのリスト等

インベントリリストの例

Equipment list for Computer Based System

						Documents No:	Date:
						Shipyard :	Hull No. :

1.Navigation Equipment

Sheet No.	Equipments	Manufacture (Supplier)	Type	Serial No.	Physical Location	Risk Assessment Report No.	Type approval certificate No.
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							

2. Radio Equipment

Sheet No.	Equipments	Manufacture (Supplier)	Type	Serial No.	Physical Location	Risk Assessment Report No.	Type approval certificate No.
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							

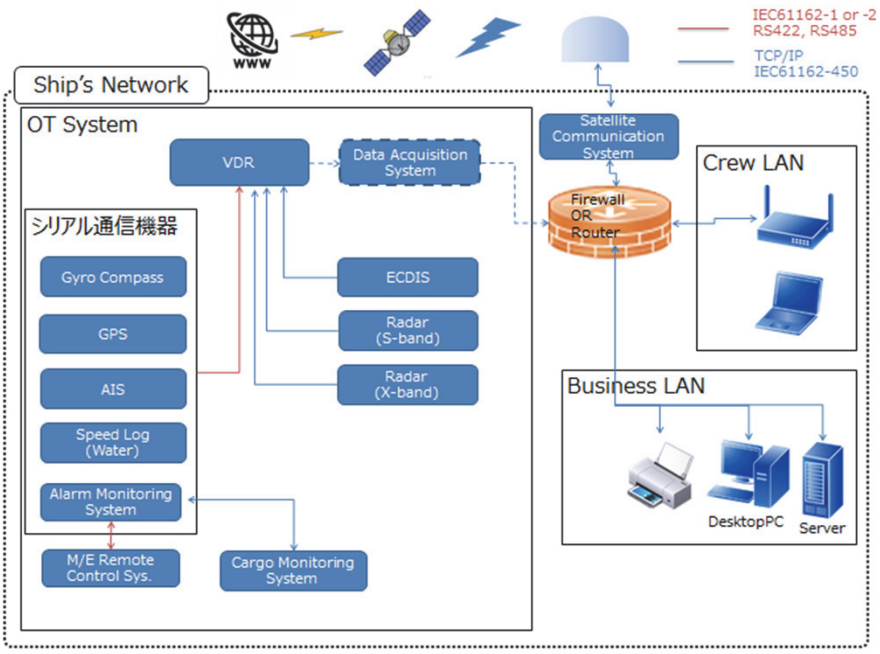
3. 単純なネットワーク図の策定

「船舶におけるサイバーデザインガイドライン」

4.1.3　ネットワーク図の策定
統合者は，セキュリティリスクへの影響を把握するために，ネットワークの種類及び一般的な設置場所と，論理グループ化したコンピュータ機器のネットワークとの接続を示す，単純なネットワーク図を策定しなければならない。

リスクセスメントに必要な情報を記載した単純な船内ネットワーク図を作成する。使用される衛星通信機器，TCP/IP通信の接続状況（参考としてシリアル通信も記載）ネットワークゾーンの分離状況等について明記

単純なネットワーク図の例



4. 船内ネットワーク全体のリスクアセスメント

「船舶におけるサイバーデザインガイドライン」
4.1.4 リスクアセスメント
統合者はリスクアセスメントを実施し，その結果を文書化しなければならない。
（リスクアセスメントは下記の2段階で実施することが標準）

1）コンピュータシステムの製造者による各機器単体のリスクアセスメント

製造者が対応できないリスクを統合者が考慮する。

インベントリリスト及び単純なネットワーク図

検討のための資料

2）統合者による船内ネットワークシステム全体のリスクアセスメント

5. 詳細なネットワーク図の策定

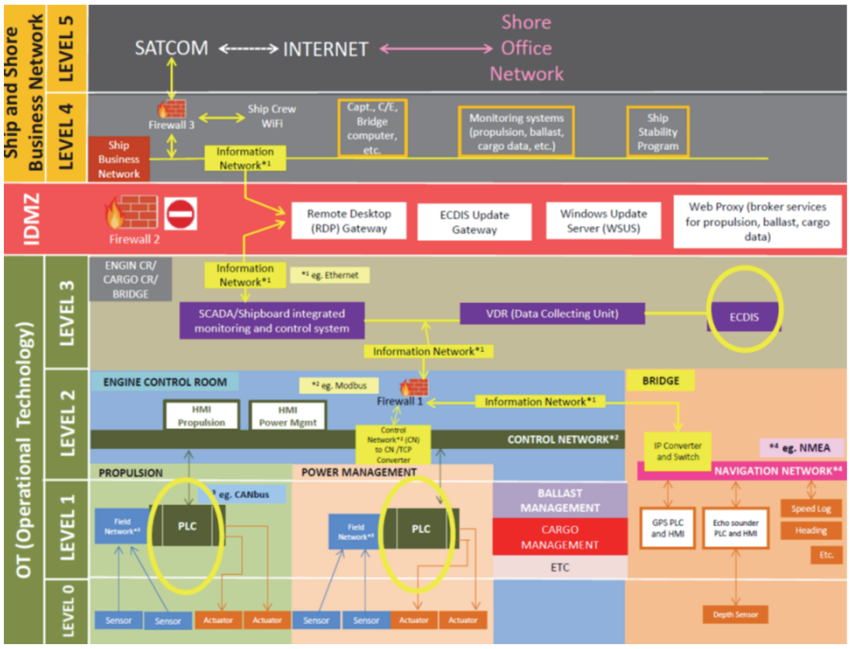
「船舶におけるサイバーデザインガイドライン」
3.3.1 図面及び資料
-5. ネットワーク論理構成図

「IACS Rec.166 7.1.2.1 2)ネットワーク構成図」
システム間，サブシステム間及びサブシステムの各種構成要素間の通信手段を規定したネットワーク構成図を作成する。

詳細なネットワーク構成図にはリスクアセスメントの結果により必要とされたセキュリティ対策を盛り込む必要がある。

3. NKサイバーノーテーション取得の手順

詳細なネットワーク図の例



3. NKサイバーノーテーション取得の手順

6. ネットワークシステムの有効性評価

「船舶におけるサイバーデザインガイドライン」

4.2.2　有効性評価

統合者は，次の事項を決定し，実装したセキュリティ対策の有効性を評価して，その結果を文書化しなければならない。

-1.　評価の実施時期，実施者及び方法

-2.　評価結果のレビュー時期及び対象者

リスクアセスメントで明らかになった受容できない脅威が，セキュリティ対策により，脅威レベルを受容できるレベルまで低下することができているかを確認する。

セキュリティ対策の例：ファイアーウォールの設置，
ネットワークの分離

7. 現場審査及び試験

「船舶におけるサイバーデザインガイドライン」

3.3.2　造船所における試験
-1.　審査員は統合者から提出されたセキュリティリスク対応が確実に行われていることを本船上において確認を行う。
-2.　審査員立ち合いのもと5.5.3に規定されるセキュリティ試験を行わなければならない。審査員の立ち合いが困難な場合には，十分な試験実績を有する試験業者の発行する試験成績書を提出することに換えることができる。

策定された詳細なネットワーク図と船上で構築されたネットワークが整合していることの確認する，船上試験方法については，個船毎にネットワーク構成が異なるためケースバイケースで対応の予定。

8. 完成図面の作成及び船上への保管

NKデザインガイドライン
3.3.3船上に保持すべき図面等
-1.　完工後の船舶には下記の資料が保管され，適切に管理されなければならない。
(1)　5.4.1に定めるネットワーク及びセキュリティの構成設定に関する手順
(2)　5.4.2の規定に適合したコンピュータ機器リスト
(3)　5.4.3に定める公衆ネットワークサービスのセキュリティに関する文書
(4)　セキュリティ試験方案（更新審査時に要求されるもの）

本船就航までに，船上に上記図面等が搭載されていることを審査員が確認