CHARTING THE FUTURE

ClassNK

船上のシステム及び機器のサイバーレジリエンスに関するガイドライン（第1.0版）

［日本語 / Japanese］

Cyber Resilience of SYSTEMS EQUIPMENT

改訂履歴

No.	日付	区分	改訂内容
1	2023.11.02	新規	新規作成

はじめに

従来の船用システムは、主に物理的な接続や制御に依存しており、外部からの不正アクセスや攻撃などの脅威に対して、それほど深く考慮する必要はありませんでした。しかし、急速な技術進歩により、これらのシステムがコンピュータやインターネットを介してデジタル的に相互接続されるようになりました。これにより、船用システムはサイバー空間にさらされるようになり、サイバー攻撃のリスクが高まっています。サイバー攻撃は、船用システムの安全性や信頼性を損なうだけでなく、海上における人命と財産の安全確保及び海洋環境の汚染防止に対する脅威となり得ます。このようなサイバー攻撃への防衛策として、サイバーセキュリティが注目されることとなりました。

2022 年 4 月、IACS（International Association of Classification Societies：国際船級協会連合）によって、サイバーセキュリティに関する 2 つの UR（Unified Requirement：統一規則）が新規に発行されました。それが、UR E26 及び UR E27 です。これらは、サイバー攻撃によるサイバーインシデントの発生を低減し影響を軽減する機能（以下、サイバーレジリエンス）に関する要件であり、UR E26 では船舶が、UR E27 では船上のシステム及び機器が対象として定められております。これらの目的は、サイバーレジリエンスに関する最低限の要件を船舶、船上のシステム及び機器に適用することで、サイバーセキュリティを最低限確保した船舶を実現することにあります。UR E26/27 の発行を受けて、日本海事協会（以下、本会）では、これらを鋼船規則 X 編（以下、X 編）に取り入れることとしました。

サイバーセキュリティ対策が船級規則に強制要件として取り入れられることは、今回が初めてとなります。そのため、関係者方々から多くの疑問が生じることが予想されます。また、サイバー攻撃は常に変化します。より複雑かつ巧妙に進化する攻撃に対応するためには、サイバーセキュリティに関する情報の更新は不可欠です。このような懸念事項に対して、本会は最高品質の船級サービスを提供する第三者機関として、積極的に情報を発信しております。その情報発信の一環として、本ガイドラインを発行する運びとなりました。

本ガイドラインは、X 編 4 章（UR E27（Rev.1））の解説本となります。主に、システム及び機器の製造者（供給者）を対象としております。具体的には、以下の事項について解説する手引きとなっています。

・適用範囲及び承認プロセス

コンピュータシステムが適用されるかを含め、本会での承認に関する手順を示しております。また、提出書類及び立会検査の要件についても、詳しく解説しております。

・サイバーレジリエンスの要件

システム及び機器に対するサイバーレジリエンスの要件について、解説しております。この要件は、IEC62443 をベースとしてその一部を取り入れたものです。これらの要件について、本会の解釈として詳細を記載しております。

本ガイドラインの構成

1章　適用

X編4章（UR E27）の適用範囲について解説します。ここは、コンピュータシステムに対するX編4章（UR E27）の適用の要否について確認するための章となっております。

2章　承認プロセス

コンピュータシステムに対する具体的な承認プロセスについて解説します。X編4章（UR E27）における本会の承認について、その承認は個品承認と使用承認の2つがあります。ここは、2つの承認プロセスの全体像を把握するための章となっております。

3章　提出資料の解説

コンピュータシステムの提出資料の要件について解説します。X編4章（UR E27）における本会の承認について、はじめに、本会機関部によって書類審査が実施されます。ここは、提出資料の詳細を理解するための章となっております。

4章　立会検査の解説

コンピュータシステムの立会検査の要件について解説します。X編4章（UR E27）における本会の承認について、書類審査完了後、本会検査支部によって立会検査が実施されます。ここは、立会検査の詳細を理解するための章となっております。

5章　システム要件の解説

コンピュータシステムのセキュリティ要件のひとつであるシステム要件について解説します。システム要件とは、コンピュータシステムへの実装が求められるセキュリティ機能に関する要件です。ここは、システム要件の詳細を理解するための章となっております。

6章　セキュア開発ライフサイクルに関する要件の解説

コンピュータシステムのセキュリティ要件のひとつであるセキュア開発ライフサイクルに関する要件について解説します。セキュア開発ライフサイクルとは、セキュアな製品の開発及び保守を目的としたライフサイクルを指します。ここは、セキュア開発ライフサイクルの詳細を理解するための章となっております。

目次

注意事項　本ガイドラインでは、たびたび「鋼船規則 X 編」の規則番号を参照しておりますが、当該規則は現段階ではまだ公表されておりません。当該規則は UR E26 及び UR E27 を取り入れた本会の規則として位置づけられる予定となっており、2024 年 7 月を目途として新規発行を計画しております。皆様のご理解を賜りますようお願い申し上げます。

1 章 適用

この章では、X 編 4 章（UR E27）が適用となるコンピュータシステムについて解説します。X 編 4 章（UR E27）の適用の要否に関するフローチャートを図 1 に示します。

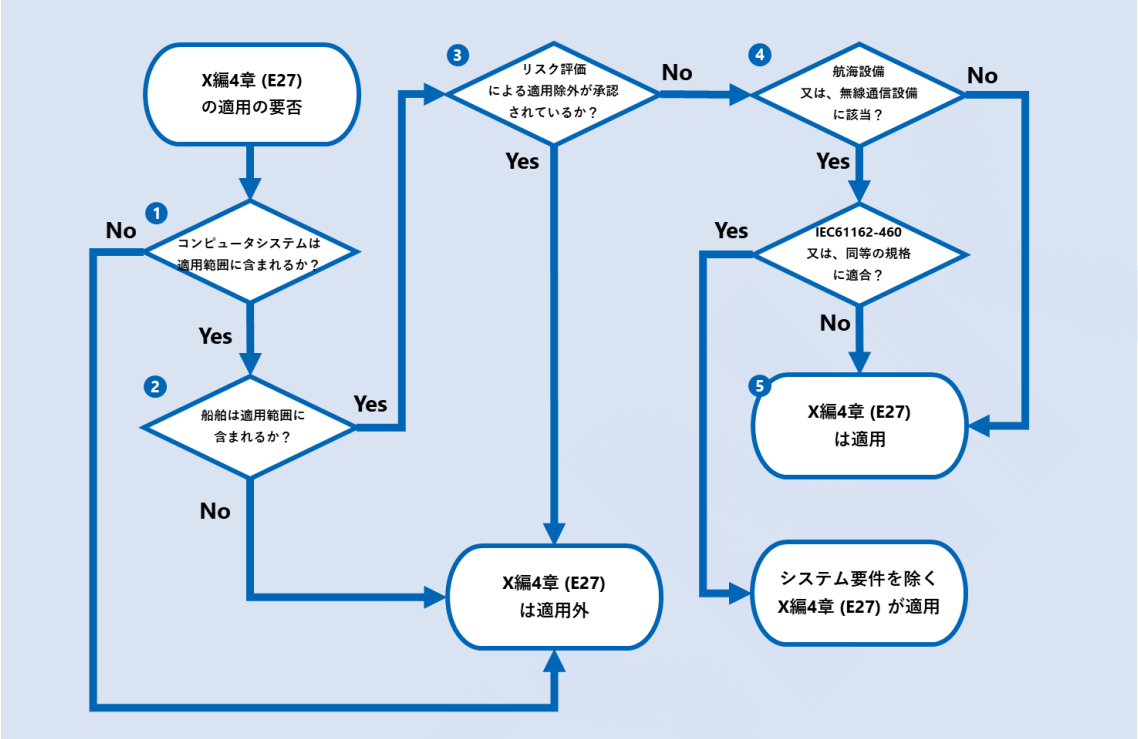


図 1　適用の要否に関するフローチャート

1 適用範囲に含まれるコンピュータシステム

コンピュータシステムとは、情報の収集、処理、維持、使用、共有、発信又は消去のような、1 又は複数の特定の目的を達成するために組織された、1 のプログラム可能なデバイスまたは相互運用できる複数のプログラム可能な電子デバイスであり、プログラマブルロジックコントローラー（PLC）を含みます。このようなシステムについて、サイバーインシデントによって侵害された場合に、人の安全及び船舶の安全にとって危険な状況並びに／又は環境に対する脅威に導きうるものは、X 編 4 章（UR E27）の対象となります。

以下に、適用範囲に含まれると考えられるコンピュータシステムの例を示します。これは、X 編 5 章（UR E26）にて、サイバーレジリエンスを考慮すべき船舶の機能及びシステムとして掲げられているものから、その一例を示したものです。なお、これらは一例にすぎず、例えば、X 編 5 章（UR E26）の適用範囲内のセキュリティゾーンに含まれるコンピュータシステムは、以下の表に関わらず X 編 4 章（UR E27）の適用対象となる場合があります。したがって、以下の一例が X 編 4 章（UR E27）の適用を決定づけるものではございませんので、その点はご留意ください。

推進

機関制御装置	機関遠隔制御装置
主ボイラ制御装置	CPP 制御装置
電気推進制御装置	FGSS 制御装置
機関警報監視装置（データロガー含む）	ウォータジェット推進装置

操舵

操舵システム制御装置	旋回式推進システム制御装置

投錨及び係留

ウインドラス制御装置	ムアリングウインチ制御装置

発電及び分電

発電機制御装置（パワーマネージメントを含む）	電力変換装置（電気推進船等）
バッテリーマネジメントシステム（リチウムイオン電池により構成される総容量 20kW 以上のもの）	

火災探知及び消火システム

火災探知器（火災表示／警報装置等）	固定式泡消火装置
固定式炭酸ガス消火装置	固定式甲板泡消火装置
局所消火装置	水噴霧装置
ドライケミカル粉末消火装置	

ビルジ及びバラストシステム、積付計算機

バラスト水遠隔制御装置	積付計算機

水密性及び浸水装置

水密扉動力開閉装置	浸水警報装置

照明（例えば、非常灯、低位置、航海灯等）

非常灯装置	低位置照明装置
航海灯制御装置	

要求される**安全システム**であって、当該システムの混乱又は機能障害が船舶の運航にリスクをもたらしうるもの（例えば、非常停止システム、荷役安全システム、圧力容器安全システム及びガス検知システム等）

イナートガス装置	荷役監視制御装置
液化ガス緊急遮断装置	可燃性ガス検知装置
液化ガス再液化装置	補助ボイラ制御装置
GCU 制御装置	ガス燃料タンク監視制御装置

条約により要求される**航海設備**

航海用レーダー	船首方位伝達装置（THD）
電子プロッティング装置（EPA）	船舶自動識別装置（AIS）
自動物標追跡装置（ATA）	航海情報記録装置（VDR）
自動衝突予防援助装置（ARPA）	船首方位制御方式自動操舵装置（HCS）
音響測深機	航跡制御方式自動操舵装置（TCS）
衛星航法装置（GPS）	船舶長距離識別追跡装置（LRIT）
音響受信装置	船橋航海当直警報装置（BNWAS）
船速距離計	電子海図情報表示装置（ECDIS）

船級規則又は条約により要求される**船内及び船外通信システム**

一般非常警報装置	船内通信装置
ナブテックス受信機	VHF デジタル選択呼出聴守装置
高機能グループ呼出受信機（EGS 受信機）	デジタル選択呼出装置（DSC）
VHF デジタル選択呼出装置	デジタル選択呼出聴守装置
GMDSS 無線設備	

その他

自動船位保持設備

❷ 適用範囲に含まれる船舶

X 編 4 章（UR E27）は、次に掲げる船舶であって、本会に登録する 2024 年 7 月 1 日以降に建造契約が行われる船舶に搭載されるコンピュータシステムに対して適用となります。

・国際航海に従事する旅客船（高速旅客船を含む）
・国際航海に従事する総トン数 500 トン以上の貨物船
・国際航海に従事する総トン数 500 トン以上の高速船

・総トン数 500 トン以上の海洋構造物
・建造に従事する自航海洋構造物（例えば、風力発電機の設置、保守及び修理等）

上記以外の船舶に搭載されるコンピュータシステムは適用外となりますので、承認は必要ありません。なお、船舶への搭載を予定されていない場合でも、使用承認の取得は可能です。具体的なプロセスについては、「使用承認プロセス」にて詳しく解説しております。

使用承認プロセス P. 14

❸ リスク評価

システムが X 編 5 章（UR E26）で要求されるリスク評価を実施し、本会の承認を受けた場合、X 編 4 章（UR E27）の適用外となります。

❹ 航海設備又は無線通信設備

システムが航海設備又は無線通信設備に該当する場合、IEC61162-460 又は、同等の規格に適合している製品は、X 編 5 章（UR E26）の要件を満たすことを条件に、システム要件（5 章参照）を免除することができます。

❺ 鋼船規則 X 編 4 章が適用となる場合

システムが、X 編 4 章（UR E27）の適用となる場合、同章に定められる要件を満たさなければなりません。したがって、製品の出荷前に書類審査及び立会検査を実施する必要があります。具体的なプロセスについては、「個品承認プロセス」にて詳しく解説しております。

個品承認プロセス P. 5

2 章 承認プロセス

本章では、X 編 4 章（UR E27）及び船用材料・機器等の承認及び認定要領第 7 編 10 章で規定されるコンピュータシステムの承認プロセスを解説します。本章の目的は、X 編 4 章（UR E27）における本会の承認プロセスの全体像を把握することです。

承認プロセスの概要

本章の承認プロセスを進めるにあたって、まずは、製品が本章の適用を受けるかを確認する必要があります。適用については、「1 章 適用」にて詳しく解説しております。

1 章 適用 P.1

X 編 4 章（UR E27）が適用となるコンピュータシステムについて、その承認は個品承認と使用承認の 2 つがあります。それぞれの承認の概要は以下のとおりです。

承認の種類	説明
個品承認	製品に対する承認を指します。X 編 4 章（UR E27）が適用となる船舶に搭載されるコンピュータシステムに対して適用され、製品ごとに承認が必要となります。
使用承認	型式に対する承認を指します。船舶に搭載準備する前に、あらかじめ代表的な型式に対して X 編 4 章（UR E27）に規定される審査及び検査を行うことで、個品承認に必要なプロセスの一部が省略されます。

個品承認プロセス

個品を承認するためのプロセスでは、システムの使用承認の有無及び同型船への承認実績により、複数のプロセスに分かれます。プロセスの概要は以下のとおりです。

個品承認プロセス	概要
システムが使用承認を有していない場合	原則として、すべての書類審査及び立会検査を実施いただく必要があります。
システムが使用承認を有する場合	一部の書類審査を省略することができます。試験結果を提出することで、立会検査も省略することができます。
以前承認された同一のシステムを同型船に搭載する場合	以前承認されたシステムとの差分を比較及び検討した上で、一部又はすべての書類審査及び／又は立会検査を省略します。

個品承認のフローチャートを図 2 に示します。

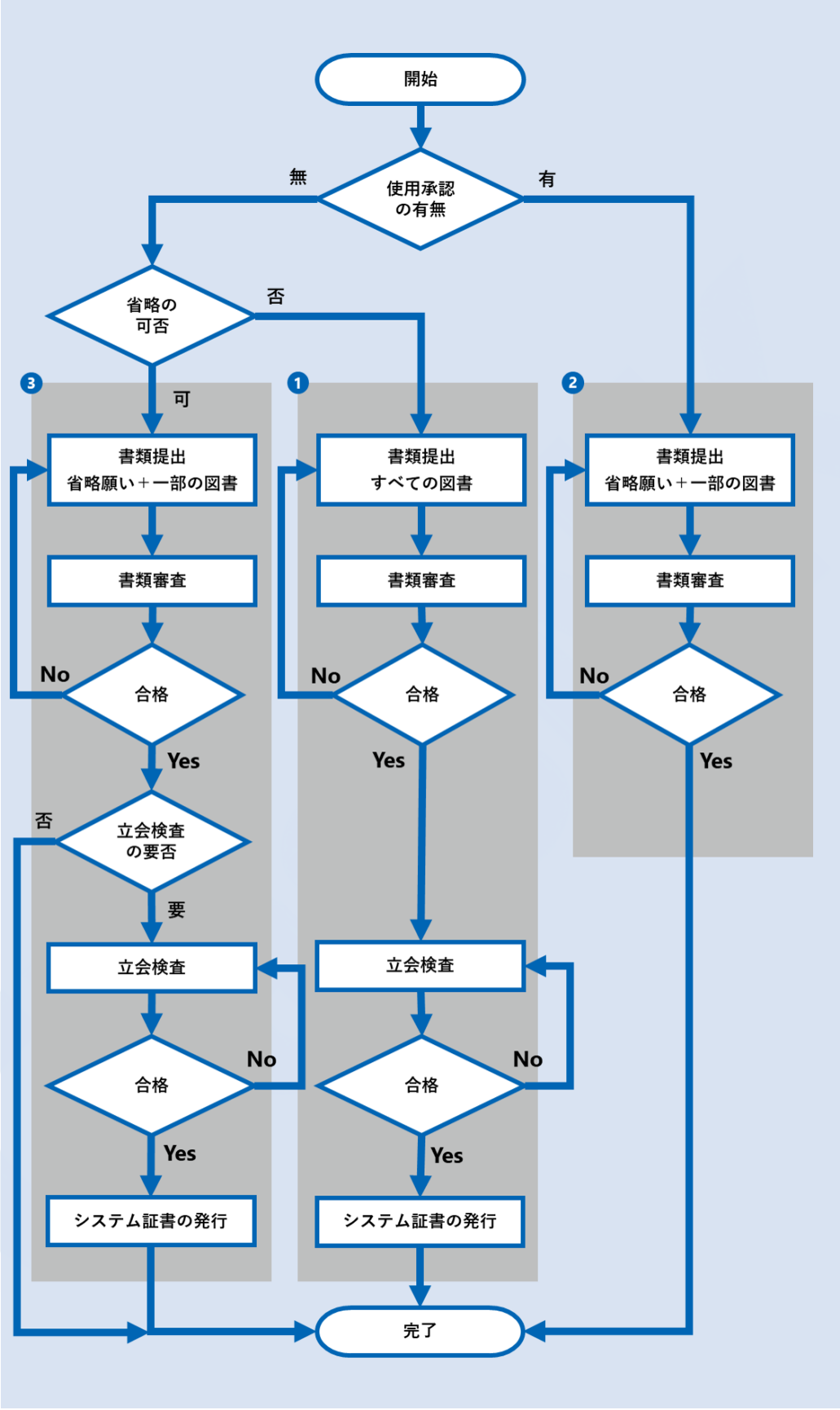


図 2　個品承認のフローチャート

❶ システムが使用承認を有していない場合

システムが使用承認を有していない場合のフローチャートを図 3 に示します。

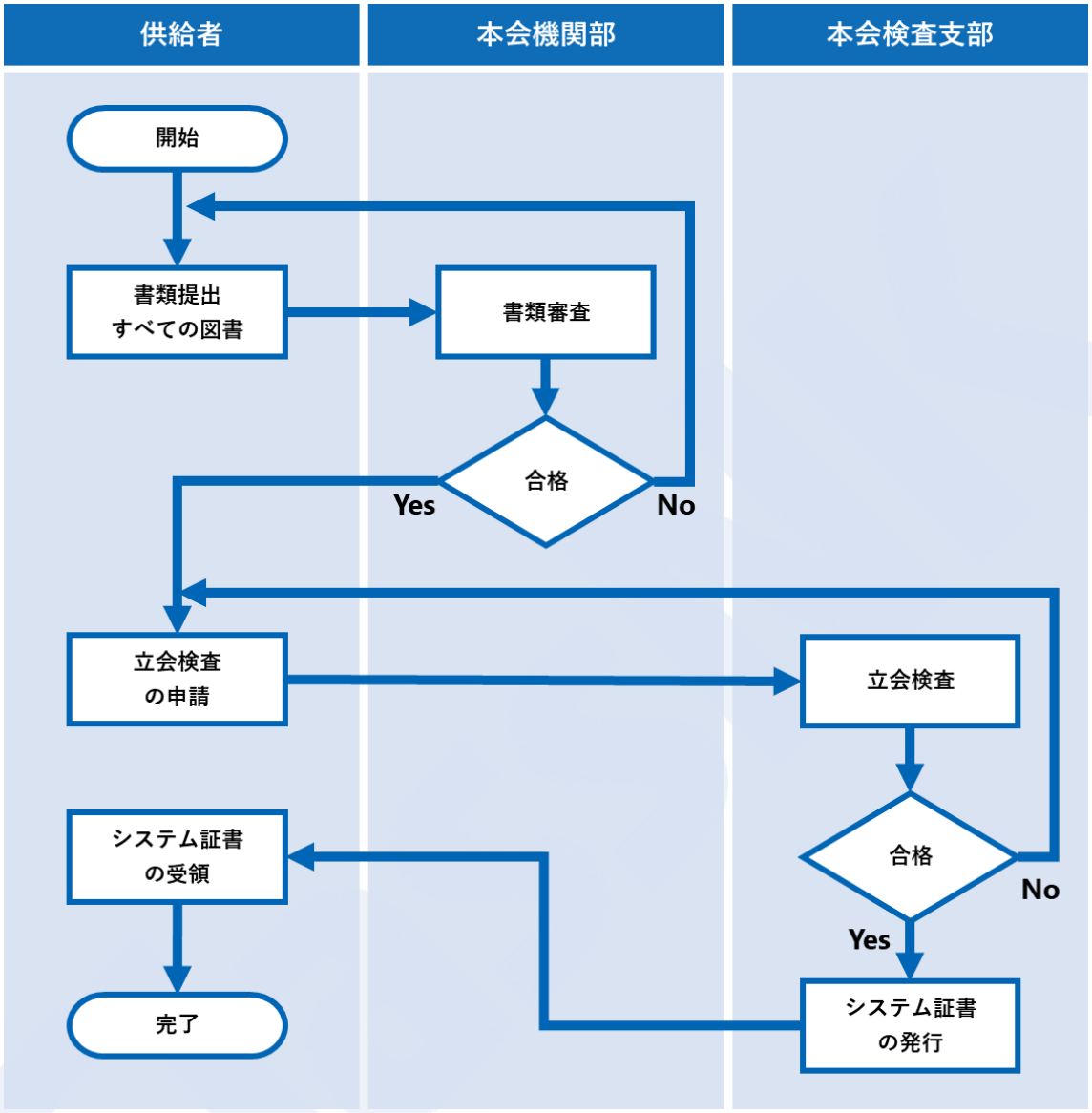


図 3　システムが使用承認を有していない場合のフローチャート

■ 提出書類・書類審査

使用承認を有していないシステムの場合、原則として、すべての資料を個船ごとに提出する必要があります。資料の提出には、本会 NK-PASS をご利用ください。NK-PASS については、以下の URL を参照ください。

https://www.classnk.or.jp/hp/ja/activities/portal/nk-pass.html

また、提出が必要となる資料は、以下のとおりです。

	提出資料
□	コンピュータシステム資産インベントリ
□	トポロジー図
□	セキュリティ機能の説明
□	セキュリティ機能の試験方案
□	セキュリティ構成指針
□	セキュア開発ライフサイクル文書
□	コンピュータシステムの保守及び検証のための計画
□	就航後のインシデント対応とリカバリープランをサポートする情報
□	計画の変更に関する管理

提出資料の詳細については、「3 章 提出書類の解説」をご確認ください。

3 章 提出資料の解説 P. 18

提出資料を受領次第、書類審査を実施します。提出資料に不備がございましたら、本会から連絡しますので、該当資料を追加／修正の上で再提出ください。審査が完了しましたら、提出資料に承認印又は参考印を押印のうえ、返却します。

■ 立会検査

書類審査が完了次第、本会検査員の立会いの下、立会検査を実施します。製造所最寄りの検査支部へ立会検査を申請ください。最寄りの検査支部については、以下の URL から検索することが可能です。

https://www.classnk.or.jp/hp/ja/directory/dir_top.aspx

なお、立会検査では、承認が要求される資料の一部に基づいて実施します。立会検査に必要となる資料は以下のとおりです。

	立会検査に必要となる資料
□	コンピュータシステム資産インベントリ
□	トポロジー図
□	セキュリティ機能の試験方案
□	セキュリティ構成指針
□	セキュア開発ライフサイクル文書

したがって、立会検査を申請いただく際は、事前に本会の図面審査及び現場確認以外のコメントがクリアになっていることを確認ください。確認できましたら、検査支部にそれらの資料を申請書に併せてご提出ください。

使用承認を有していないシステムの場合、原則として、すべての検査を実施することと

なります。要求される検査は、以下のとおりです。

	立会検査
□	一般的な検査項目
□	セキュリティ機能試験
□	セキュリティ機能の正確の設定
□	セキュア開発ライフサイクル

立会検査の詳細については、「4 章 立会検査の解説」をご確認ください。

4 章 立会検査の解説 P. 39

立会検査が完了しましたら、本会検査支部よりシステム証書が発行されます。システム証書を受領しましたら、本会の承認プロセスは完了となります。

❷ システムが使用承認を有する場合

システムが使用承認を有する場合のフローチャートを図 4 に示します。

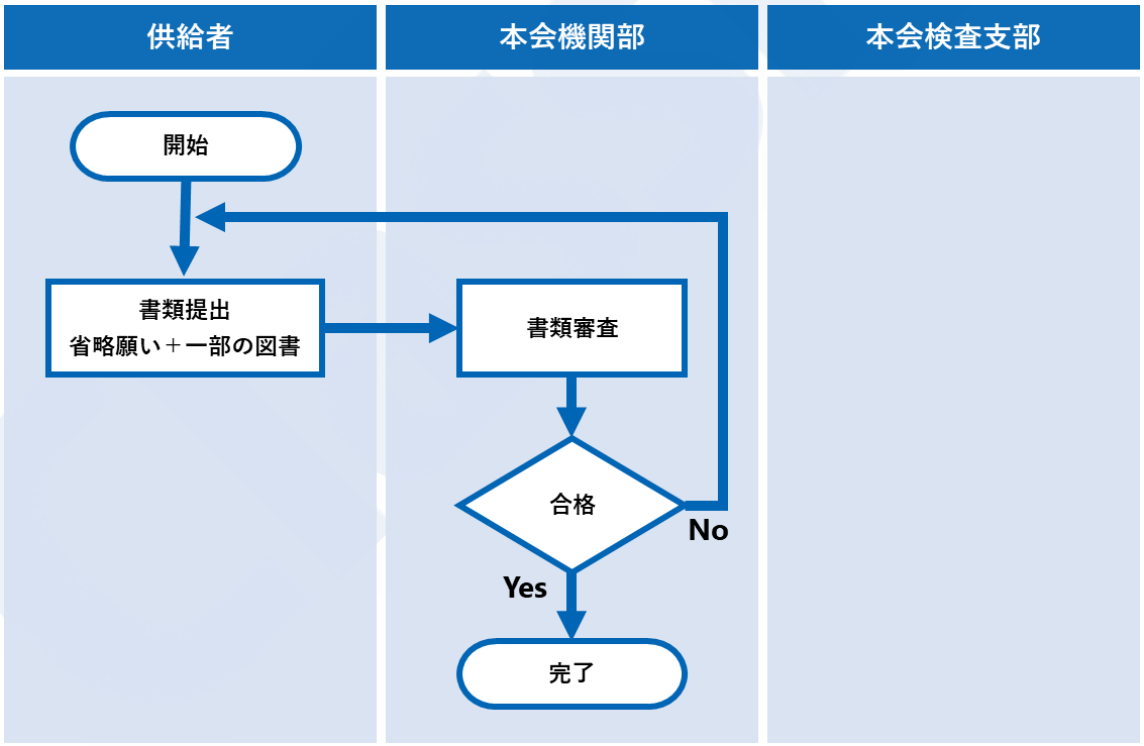


図 4　システムが使用承認を有する場合のフローチャート

■ 提出書類・書類審査

使用承認を有するシステムの場合、要求される資料の提出が省略されます。省略を希望される場合には、以下の事項が記載された図面審査の省略願いを提出ください。

	使用承認による書類審査省略願いの詳細
□	使用承認証書の写し
□	使用承認品とのソフトウェアのバージョン含む差分のリスト

図面の提出にあたっては、本会 NK-PASS をご利用ください。NK-PASS については、以下の URL を参照ください。

https://www.classnk.or.jp/hp/ja/activities/portal/nk-pass.html

また、提出が必要となる資料とは、以下のとおりです。

	提出資料
□	コンピュータシステム資産インベントリ
□	トポロジー図
□	試験結果
□	使用承認による書類審査省略願い

提出資料の詳細については、「3 章 提出書類の解説」をご確認ください。

3 章 提出資料の解説 P. 18

提出資料を受領次第、書類審査を実施します。提出資料に不備がございましたら、本会から連絡しますので、該当資料を追加／修正の上で再提出ください。審査が完了しましたら、提出資料に承認印および参考印を押印のうえ、返却します。

使用承認を有するシステムの場合、立会検査は不要です。したがって、承認された資料を受領しましたら、本会の承認プロセスは完了となります。

❸ 以前に承認された同一のシステムを同型船に搭載する場合

以前に承認された同一のシステムを同型船に搭載する場合のフローチャートを図 5 に示します。

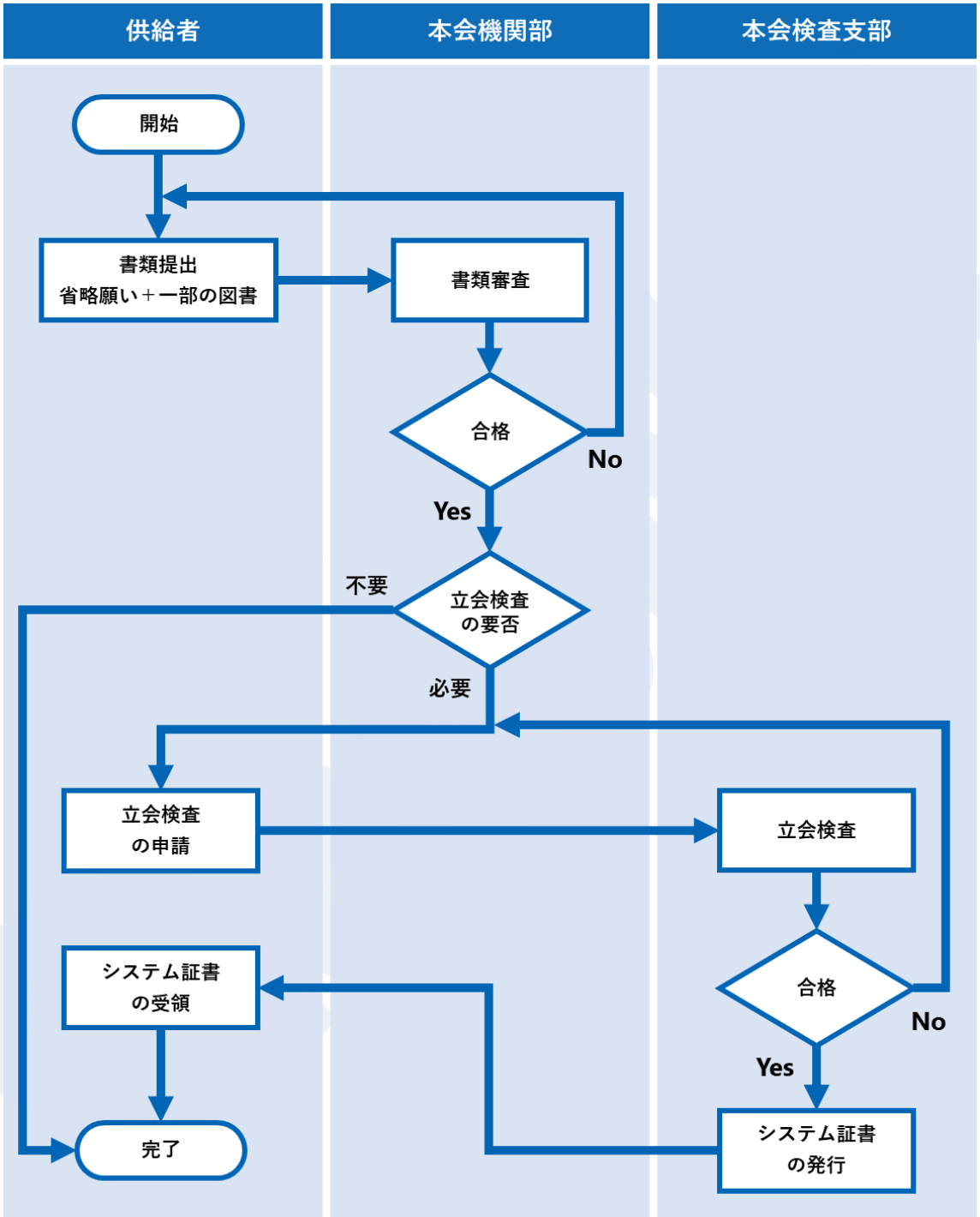


図 5　以前に承認された同一のシステムを同型船に搭載する場合のフローチャート

■ 提出書類・書類審査

同一のシステムが同型船に搭載される場合において、以前に承認された資料から変更が無ければ、第二船以降については、資料提出の省略が可能となります。省略を希望される場合には、以下の事項が記載された図面審査の省略願いを提出いただき、本会が省略を適当と認めることを条件とします。

	同型船による書類審査省略願いの詳細
□	以前に関連資料が承認された船舶（参照船）の情報
□	参照船および対象船のソフトウェアバージョン情報（バージョンアップ履歴を添付ください）
□	参照船と対象船の仕様差リスト（差分を全て記載ください）
□	提出の省略を希望する資料名称

また、立会検査につきましても、システム構成やその機能・制御仕様が以前に本会検査員立会の下で実施された試験と同一、かつ試験結果が同一であることを証明できる資料を試験立会の省略願いに添えて提出いただくことで立会検査の省略を個別に検討します。 この立会検査の省略願いには以下の事項を記載ください。

	同型船による立会検査省略願いの詳細
□	以前に関連資料が承認された船舶（参照船）の情報
□	参照船および対象船のソフトウェアバージョン情報（バージョンアップ履歴を添付ください）
□	参照船と対象船の仕様差リスト（差分を全て記載ください）

上記の場合、提出が必要となる資料は、以下のとおりとなります。

	提出資料
□	コンピュータシステム資産インベントリ
□	トポロジー図
□	試験結果
□	同型船による書類審査省略願い
□	同型船による立会検査省略願い（要求する場合）

■ 立会検査

立会検査省略願いにより、すべての検査の省略が認められた場合、立会検査は不要となりますので、本会の承認プロセスは完了となります。

立会検査を一部またはすべて実施する場合は、「❶ 使用承認を持たないシステムに対する個品承認プロセス」と同様、製造所最寄りの検査支部へ立会検査をお申込みください。最寄りの検査支部については、以下の URL から検索することが可能です。

https://www.classnk.or.jp/hp/ja/directory/dir_top.aspx

なお、立会検査では、承認が要求される資料の一部が必要となります。立会検査に必要となる資料は以下のとおりです。

	立会検査に必要となる資料
☐	コンピュータシステム資産インベントリ
☐	トポロジー図
☐	セキュリティ機能の試験方案
☐	セキュリティ構成指針
☐	セキュア開発ライフサイクル文書

使用承認を有していないシステムの場合、原則として、すべての検査を実施することとなります。しかし、前述の「立会検査省略願い」により、一部検査の省略が認められる場合があります。その場合、以下の立会検査項目の中から必要となる検査を、本会検査員立会の下で実施ください。

	立会検査
☐	一般的な検査項目
☐	セキュリティ機能試験
☐	セキュリティ機能の正確の設定
☐	セキュア開発ライフサイクル

立会検査の詳細については、「4 章 立会検査の解説」をご確認ください。

4 章 立会検査の解説 P. 39

立会検査が完了しましたら、本会検査支部よりシステム証書が発行されます。システム証書を受領しましたら、本会の承認は完了となります。

使用承認プロセス

使用承認を取得するためのプロセスの概要について解説します。使用承認プロセスのフローチャートを図 6 に示します。

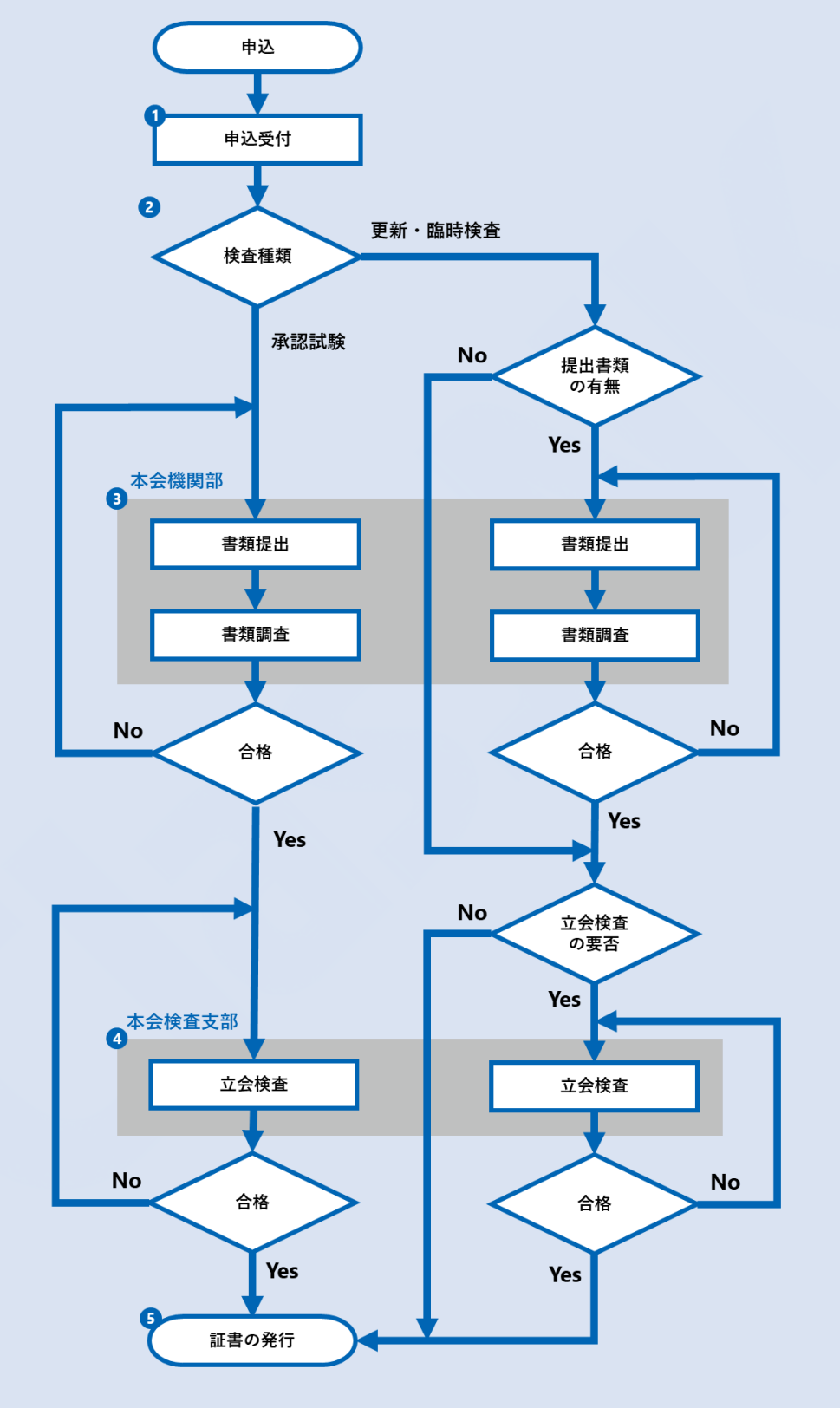


図 6　使用承認のフローチャート

❶ 申込

使用承認を申込む場合は、申請書（Form7-8(J)）を、所要事項を記入の上、本会機関部へNK-PASS 又は電子メール（mcd@classnk.or.jp）等で提出してください。その際は、UR E27に関する使用承認である旨、お伝えください。なお、申込書は下記 URL の NK ホームページ「船級検査（製品の製造事業所）」からダウンロード可能です。

http://www.classnk.or.jp/hp/ja/download/dl_appli.aspx

❷ 審査種類

使用承認では、以下の 3 種類の審査がございます。

検査	説明
承認審査	システムに対して、使用承認を新規取得する場合に実施される審査です。
更新審査	使用承認を有するシステムの有効期限を更新する場合に実施される審査です。使用承認の有効期限は 5 年間であり、有効期限の更新を希望される場合は、この審査を実施する必要があります。
臨時審査	使用承認を有するシステムが変更される場合に実施される審査です。

❸ 提出書類・書類審査

承認審査では、初めに、使用承認を取得するにあたり必要な資料を提出していただきます。提出については、以下いずれかの方法で提出いただくこととなります。

a) NK-PASS
b) 電子メール（mcd@classnk.or.jp）
c) 郵送（この場合は、資料は各 3 部提出される必要があります。）

なお、申込時にあわせて書類を提出いただくことでも差支えございません。本会に提出する資料については、次に掲げる資料となっております。

	提出資料
☐	コンピュータシステム資産インベントリ
☐	トポロジー図
☐	セキュリティ機能の説明
☐	セキュリティ機能の試験方案
☐	セキュリティ構成指針
☐	セキュア開発ライフサイクル文書
☐	コンピュータシステムの保守及び検証のための計画

□	就航後のインシデント対応とリカバリープランをサポートする情報
□	計画の変更に関する管理

提出資料の詳細については、「3 章 提出書類の解説」をご確認ください。

3 章 提出資料の解説 P. 18

提出資料を受領次第、書類審査を実施します。提出資料に不備がございましたら、本会から連絡しますので、該当資料を追加で提出ください。

承認審査では、すべての資料を提出いただく必要があります。
更新審査では、書類審査は必要に応じて実施されます。書類審査が必要となるケースは、使用承認の承認日（あるいは更新日）から、承認品の仕様に変更があった、規則改正により提出書類の一部変更又は追加があった等です。
臨時審査では、変更が発生した資料のみを提出いただくことで差支えございません。その際には、変更箇所が分かるように「変更履歴」を文書化する等により、本会へ通知する必要があります。

❹ 立会検査

書類審査が完了次第、本会検査員の立会いの下、立会検査を実施します。立会検査のお申込みについては、製造所最寄りの検査支部へ申請いただくことになります。最寄りの検査支部については、以下の URL から検索することが可能です。
https://www.classnk.or.jp/hp/ja/directory/dir_top.aspx
なお、立会検査では、承認が要求される資料の一部が必要となります。立会検査に必要となる資料は以下のとおりです。

	立会検査に必要となる資料
□	コンピュータシステム資産インベントリ
□	トポロジー図
□	セキュリティ機能の試験方案
□	セキュリティ構成指針
□	セキュア開発ライフサイクル文書

したがって、立会検査を申請いただく際は、まずは本会の図面審査が完了していることをご確認ください。ご確認後、検査支部にそれらの資料を申請書と併せてご提出ください。

立会検査では、審査ごとに要求される検査が異なります。
承認審査では、すべての検査項目を実施することになります。原則として、すべての検

査を本会検査員の立会いの下、実施いただく必要がございますが、検査員が認めた場合はこの限りではございません。検査日程や内容については、検査支部に相談して下さい。

更新審査では、立会検査は必要に応じて実施されます。立会検査が必要となるケースは、規則改正により立会試験の要件に変更や追加が発生した等です。

臨時審査では、システムに変更があった場合に、立会検査が必要と判断される場合に要求されます。

立会検査の詳細については、「4 章 立会検査の解説」をご確認ください。

4 章 立会検査の解説 P. 39

❺ 証書の発行

立会検査が完了しましたら、本会検査支部より本会機関部へ試験の合否が連絡されます。合格の場合、本会機関部より使用承認証書を発行します。

承認審査の場合、証明書の有効期間は、発行日から起算して 5 年を経過する日となります。

臨時審査では、以前の証明書を一部変更した上で、発行されることとなります。この場合、証明書の有効期間は、原則として以前の証明書から変更されません。

更新試験の場合、証明書の有効期間は、前回の有効期間が満了する日の翌日から起算して 5 年を経過する日となります。

新たな証書を受領しましたら、本会の使用承認プロセスは完了となります。

3 章 提出資料の解説

本章では、X 編 4 章（UR E27）に規定する提出資料に関する詳細を解説します。

提出資料の概要

■ 提出資料の要件

X 編 4 章（UR E27）では、コンピュータシステムのサイバーレジリエンスに関する資料として、計 10 点の提出資料の要件が規定されております。各資料は以下のとおりです。

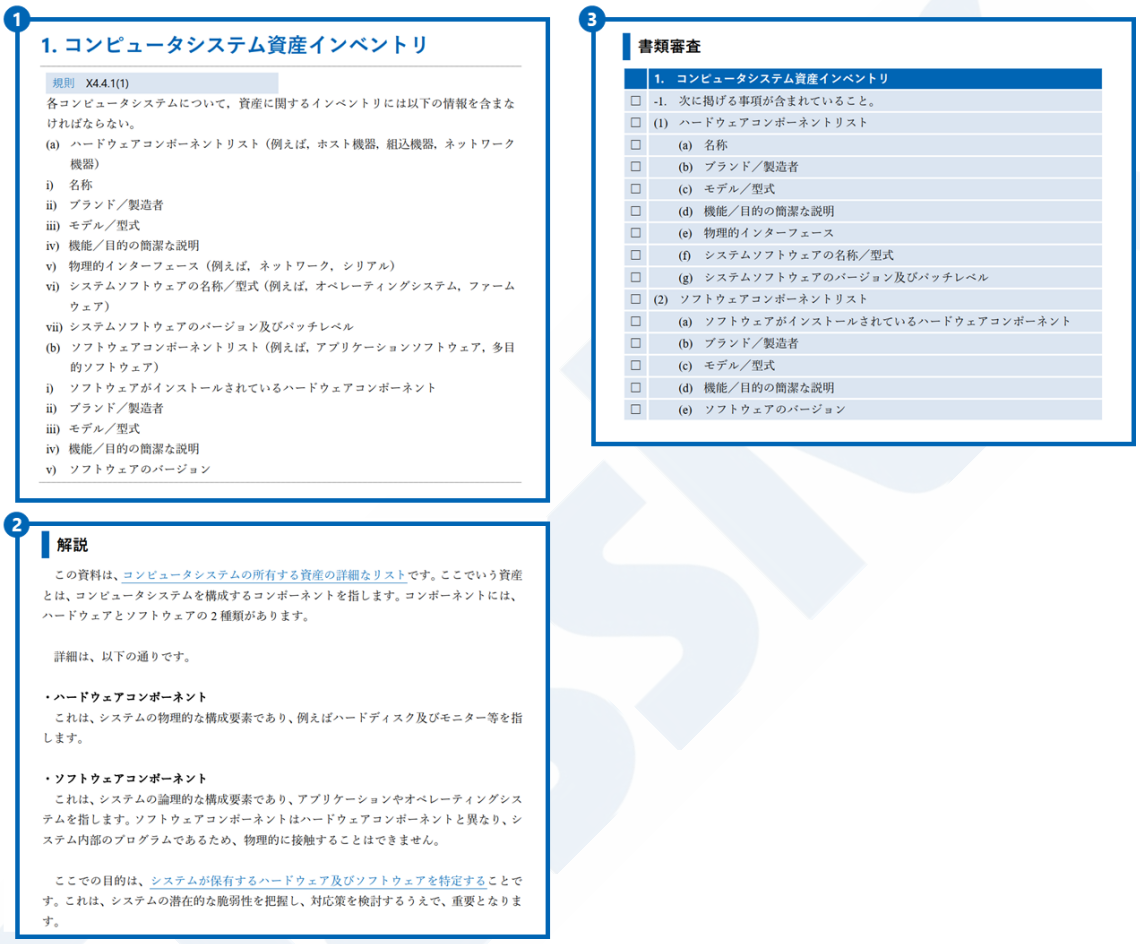
提出書類の要件

■ 要求される資料は承認プロセスごとに異なる

個品承認の場合、使用承認の有無や同型船で承認実績によって提出が要求される資料が異なります。それぞれの承認プロセスにて要求される提出資料については、「2 章 承認プロセス」にて詳しく解説しております。

提出資料の詳細

以降のページの見方



① 要件

提出資料の名称と要件の詳細です。

② 解説

提出資料の解説です。

③ 書類審査

提出資料の要件に関する書類審査のチェックリストです。

1. コンピュータシステム資産インベントリ

規則　X4.4.1(1)

各コンピュータシステムについて，資産に関するインベントリには以下の情報を含まなければならない。

(a) ハードウェアコンポーネントリスト（例えば，ホスト機器，組込機器，ネットワーク機器）

i) 名称

ii) ブランド／製造者

iii) モデル／型式

iv) 機能／目的の簡潔な説明

v) 物理的インターフェース（例えば，ネットワーク，シリアル）

vi) システムソフトウェアの名称／型式（例えば，オペレーティングシステム，ファームウェア）

vii) システムソフトウェアのバージョン及びパッチレベル

viii) 対応している通信プロトコル

(b) ソフトウェアコンポーネントリスト（例えば，アプリケーションソフトウェア，多目的ソフトウェア）

i) ソフトウェアがインストールされているハードウェアコンポーネント

ii) ブランド／製造者

iii) モデル／型式

iv) 機能／目的の簡潔な説明

v) ソフトウェアのバージョン

解説

この資料は、コンピュータシステムの所有する資産の詳細なリストです。ここでいう資産とは、コンピュータシステムを構成するコンポーネントを指します。コンポーネントには、ハードウェアとソフトウェアの 2 種類があります。

詳細は、以下のとおりです。

・ハードウェアコンポーネント

これは、システムの物理的な構成要素であり、ホスト機器、組込機器およびネットワーク機器を指します。

・ソフトウェアコンポーネント

これは、システムの論理的な構成要素であり、アプリケーションやオペレーティングシステムを指します。ソフトウェアコンポーネントはハードウェアコンポーネントと異なり、システム内部のプログラムであるため、物理的に触れることはできません。

ここでの目的は、システムが保有するハードウェア及びソフトウェアを特定することです。これは、システムの潜在的な脆弱性を把握し、対応策を検討する上で、重要となります。

補足　コンピュータシステムがコンピュータシステム資産インベントリに従って正しく構成されていることを、立会検査にて確認します。詳細は、「1. 一般的な検査項目」にて詳しく解説しております。

一般的な検査項目　P. 41

書類審査

	1.　コンピュータシステム資産インベントリ
☐	-1.　次に掲げる事項が含まれていること。
☐	(1)　ハードウェアコンポーネントリスト
☐	(a)　名称
☐	(b)　ブランド／製造者
☐	(c)　モデル／型式
☐	(d)　機能／目的の簡潔な説明
☐	(e)　物理的インターフェース
☐	(f)　システムソフトウェアの名称／型式
☐	(g)　システムソフトウェアのバージョン及びパッチレベル
☐	(h)　対応している通信プロトコル
☐	(2)　ソフトウェアコンポーネントリスト
☐	(a)　ソフトウェアがインストールされているハードウェアコンポーネント
☐	(b)　ブランド／製造者
☐	(c)　モデル／型式
☐	(d)　機能／目的の簡潔な説明
☐	(e)　ソフトウェアのバージョン

2. トポロジー図

規則　X4.4.1(2)

(a)　物理トポロジー図は，システムの物理的な構成を図示しなければならない。当該図は，コンピュータシステム資産インベントリ中のハードウェアコンポーネントを特定できるようにしなければならない。また，当該図は以下を図示しなければならない。

i)　全てのエンドポイント及びネットワーク機器（冗長化されたユニットの識別を含む）

ii)　I/O ユニットとの通信を含む通信ケーブル（ネットワーク，シリアルリンク等）

iii)　その他のネットワーク又は，システムとの通信ケーブル

(b)　論理トポロジー図は，システム内のコンポーネント間のデータフローを図示しなければならない。また，当該図は以下を図示しなければならない。

i)　通信エンドポイント（ワークステーション，コントローラー，サーバー等）

ii)　ネットワーク機器（スイッチ，ルーター，ファイアウォール等）

iii)　物理コンピュータ及び仮想コンピュータ

iv)　物理通信経路と仮想通信経路

v)　通信プロトコル

要求されたすべての情報を明確に示すことができる場合は、物理的及び論理的トポロジー図をまとめても差支えない。

解説

トポロジー図とは、ネットワークの構成が物理的及び論理的に示された図です。これは、物理トポロジー図と論理トポロジー図の 2 種類があります。

詳細は、以下のとおりです。

・物理トポロジー図

物理的なネットワークの構成図です。例えば、システムの配置及び接続ケーブルの経路などの情報が記載されます。

・論理トポロジー図

論理的なネットワークの構成図です。これは、物理的な構成要素に関する通信の流れに加えて、仮想コンピュータや仮想通信経路などの仮想空間内の流れも図示されます。

ここでの目的は、システムの物理的及び論理的な構成を把握することです。これは、システム統合時にネットワークのセキュリティゾーンを決定する、及びセグメント化する際に重要となります。

補足　コンピュータシステムがトポロジー図に従って正しく構成されていることを、立会検査にて確認します。詳細は、「1. 一般的な検査項目」にて詳しく解説しております。

一般的な検査項目　P. 41

書類審査

	2.　トポロジー図
☐	-1.　次に掲げる事項が含まれていること。
☐	(1)　物理トポロジー図
☐	(a)　全てのエンドポイント及びネットワーク機器（冗長化されたユニットの識別を含む）
☐	(b)　I/O ユニットとの通信を含む通信ケーブル（ネットワーク，シリアルリンク等）
☐	(c)　その他のネットワーク又は，システムとの通信ケーブル
☐	(2)　論理トポロジー図
☐	(a)　通信エンドポイント（ワークステーション，コントローラー，サーバー等）
☐	(b)　ネットワーク機器（スイッチ，ルーター，ファイアウォール等）
☐	(c)　物理コンピュータ及び仮想コンピュータ
☐	(d)　物理通信経路と仮想通信経路
☐	(e)　通信プロトコル

3. セキュリティ機能の説明

規則　X4.4.1(3)

(a) 当該図書は，ハードウェア及びソフトウェアコンポーネントを備えたコンピュータシステムが，**要求されるセキュリティ機能**をどのように満足するかに関して記載しなければならない。

(b) X 編 5 章（UR E26）の適用範囲内のコンピュータシステムに対する，あらゆるネットワークインターフェイスを記載しなければならない。これには，通信先のコンピュータシステム，データフロー及び通信プロトコルを含めなければならない。統合者が通信先のコンピュータシステムを他のセキュリティゾーンに割り当てている場合には，**セキュリティゾーン境界の保護を担うコンポーネント**について，当該コンピュータシステムの一部として納入されるかどうかを詳細に記載しなければならない。

(c) X 編 5 章（UR E26）の適用範囲外のシステム又は外部のネットワークに対するあらゆるネットワークインターフェイス（信頼できないネットワーク）を記載しなければならない。これには，**追加で要求されるセキュリティ機能**への準拠を明記し，乗組員への関連する手順又は指示を含めなければならない。**セキュリティゾーン境界の保護を担うコンポーネント**について，当該コンピュータシステムの一部として納入されるかどうかを詳細に記載しなければならない。

(d) 各要求事項については，別の章をそれぞれ指定するものとする。システム内の全てのハードウェア及びソフトウェアコンポーネントは，説明の中で関連するものとして扱われなければならない。

(e) 要求事項に完全に準拠していない場合，その旨を記載し，補完的対策を提案しなければならない。補完的対策は，次のとおりとする。

i) 元々規定されている要件と同じ脅威から保護すること。

ii) 元々規定されている要件と同等の厳しさ，正確さであること。

iii) 本章の他の要求事項により要求されるセキュリティ管理ではないこと。

iv) 新たなセキュリティリスクを発生させないこと。

要求事項への準拠を確認するために必要な補足資料（例えば，OEM 情報[1]）は，説明文中で参照し，提出しなければならない。

解説

セキュリティ機能の説明とは、X4.4.2 及び X4.4.3 で規定されるセキュリティ機能の詳細が説明されている資料となります。

具体的には、以下について記載される必要があります。

・セキュリティ機能及び補完的対策

[1] **OEM**　Original Equipment Manufacturer の略。他社ブランドの製品を製造する企業を指す。

この資料には、システム要件を満足するためのセキュリティ機能について説明されている必要があります。システム要件とは、コンピュータシステムに対してサイバーセキュリティ対策として求められるセキュリティ機能に関する要件です。

また、補完的対策とは、本来のセキュリティ機能に代えて採用された対策です。システムに対して、要求されるセキュリティ機能を実装できない場合、その機能に代替する補完的対策を講じることとなります。

詳細は、「5 章 システム要件の解説」にて、詳しく解説しております。

5 章 システム要件の解説 P. 47

・ネットワークインターフェイス

これは、ネットワークと接続するためのポイント（接点）を指します。例えば、イーサネット NIC[1]及び無線 LAN アダプタ等が該当します。ネットワークインターフェイスは、通信先のコンピュータシステム、データフロー及び通信プロトコル等の情報と併せて、この資料に含める必要があります。ネットワークインターフェイスは、以下のネットワークごとに記載される必要があります。

・X 編 4 章（UR E27）の適用範囲内のネットワーク

これは、X 編 4 章（UR E27）に従って承認されたシステムによって構成されたネットワークを指します。

・信頼できないネットワーク

これは、X 編 4 章（UR E27）の適用範囲外のネットワークを指します。例えば、インターネット等が該当します。また、この場合、セキュリティゾーン境界の保護を担うコンポーネントがシステムの一部として納入されるかどうかについて詳細が記載されている必要があります。

・要求事項への準拠を確認するために必要な補足資料

書類審査

	3. セキュリティ機能の説明
☐	-1. 次に掲げる事項が含まれていること。
☐	(1) セキュリティ機能及び補完的対策
☐	(a) 詳細は、ガイドライン 5 章「システム要件の解説」を確認すること。
☐	(2) ネットワークインターフェイス
☐	(a) X 編 4 章（UR E27）の適用範囲内のネットワーク
☐	(b) 信頼できないネットワーク
☐	セキュリティゾーン境界の保護を担うコンポーネントについて、システムの一部として納入されるかどうかについて詳細が記載されていること。
☐	(3) 要求事項への準拠を確認するために必要な補足資料

[1] **NIC** Network Interface Card（ネットワークインターフェイスカード）の略。例えば、LAN ポート等。

4. セキュリティ機能の試験方案

規則　X4.4.1(4)

(a)　当該図書は，システムが**要求されるセキュリティ機能**及び**追加で要求されるセキュリティ機能**の要求事項に準拠していることを，試験によりどのように実証するかを説明しなければならない（補完的対策を含む）。当該方案には，各要件について章ごとに分けて記載し，以下についても含めなければならない。

i)　必要な試験条件（すなわち，期待される試験結果で繰り返し試験を行うことができることを保証すること。）

ii)　試験機器

iii)　初期条件

iv)　試験手法，詳細な試験手順

v)　期待される試験結果及び合格基準

当該方案は，試験中に試験結果を更新し，所見を記録する手段を含むこと。

解説

セキュリティ機能の試験方案とは、X 編 2.2.3 (2)で規定されるセキュリティ機能試験の立会試験のための試験方案となります。立会試験では、この資料に従って要求されるセキュリティ機能の実証試験を行います。要求されるセキュリティ機能の詳細は、「5 章　システム要件の解説」にて詳しく解説しております。

4 章 立会検査の解説　P. 47

なお、セキュリティ機能の代替として補完的対策を講じる場合、補完的対策の確認を行います。それらの確認方法も、この資料に含める必要があります。

また、この資料には、各要件の実証試験に対する試験条件、試験機器、初期条件、試験手法、期待される試験結果等を含む必要があります。さらに、試験中に試験結果や所見を記録するための記入欄を含める必要があります。

立会試験の詳細は、「2. セキュリティ機能試験」に詳しく解説しております。

セキュリティ機能試験　P. 43

書類審査

	4.　セキュリティ機能の試験方案
□	-1.　次に掲げる事項が含まれていること。
□	(1)　セキュリティ機能の実証試験及び補完的対策の確認
□	各要件の詳細は、ガイドライン 5 章「システム要件の詳細」を確認すること。

☐	(a)　必要な試験条件
☐	(b)　試験機器
☐	(c)　初期条件
☐	(d)　試験手法，詳細な試験手順
☐	(e)　期待される試験結果及び合格基準
☐	(f)　試験結果及び所見の記入欄

5. セキュリティ構成指針

規則　X4.4.1(5)

(a) 当該図書は，セキュリティ機能の推奨設定を説明し，デフォルト値を特定しなければならない。この目的は，**X 編 5 章（UR E26）**及び統合者の顧客による仕様（例えば，ユーザアカウント，権限，パスワードポリシー，機器の安全状態，ファイアウォール規則等）に従って，セキュリティ機能が実装されていることを保証することである。

(b) セキュリティ構成指針は，**システム要件のひとつである「29 ネットワーク及びセキュリティ構成設定」**の検証の根拠となるものである。

解説

セキュリティ構成指針とは、コンピュータシステムに提供されるセキュリティ機能の推奨設定及びデフォルト値を説明する資料となります。この資料は、供給者によって提供される指針にて推奨されるネットワーク及びセキュリティ構成に従って設定するための指針となります。この資料の目的は、統合者の顧客が自身の仕様に従って、システムのセキュリティ機能を適切に設定し、活用できることを確実にすることです。

詳細は、以下のとおりです。

・セキュリティ機能の推奨設定に関する説明

セキュリティ構成指針では、セキュリティ機能の設定方法や使用方法についての詳細な説明が提供されます。これには、例えば、使用者の認証の設定方法、暗号化オプションの選択と設定、ネットワークフィルタリングの設定などが含まれます。

・特定されたデフォルト値

指針では、各セキュリティ設定のデフォルト値も明示されます。デフォルト値は通常、システムのインストール直後の設定を示します。しかし、多くの場合、デフォルト設定は最もセキュアな設定ではないため、統合者はこれらの設定を見直し、所有者のニーズやポリシーに合わせて調整する必要があります。

また、セキュリティ構成の設定は、システム要件のひとつである「29 ネットワーク及びセキュリティ構成設定」によって、セキュリティ機能としてシステムに実装される必要があります。詳細は、「29 ネットワーク及びセキュリティ構成設定」に詳しく解説しております。

ネットワーク及びセキュリティ構成設定　P. 124

書類審査

5.　セキュリティ構成指針

☐	-1. 次に掲げる事項が含まれていること。
☐	(1) セキュリティ機能の推奨設定に関する説明
☐	(2) 特定されたデフォルト値

6. セキュア開発ライフサイクル文書

規則　X4.4.1(6)

当該図書は，要求に応じて本会に提出され，**セキュア開発ライフサイクル**に関する要求事項に従った供給者のプロセス及び管理の記述を含むものでなければならない。また，ソフトウェアの更新及びパッチの適用について記載しなければならない。当該文書は，**本会の検査**のために準備されなければならない。

解説

セキュア開発ライフサイクル文書とは、セキュア開発ライフサイクルの要件に適合するためのプロセス及び管理が記載される資料となります。セキュア開発ライフサイクルとは、セキュアな製品の開発及び保守を目的としたライフサイクルを指します。

詳細は、以下のとおりです。

・セキュリティ面をどのように扱ったかの記録

X 編 4.5.1 によると、システムの開発は、次に掲げる段階において、セキュリティ面をどのように扱ったかを記録した文章を作成する必要があります。

(1) 要件分析段階
(2) 設計段階
(3) 実装段階
(4) 検証段階
(5) リリース段階
(6) 保守段階
(7) 終了段階

・セキュア開発ライフサイクルに関するプロセス及び管理

セキュア開発ライフサイクルに関する要件では、各要件を満たすためのプロセスを明確にする旨を規定しております。したがって、各要件のプロセスをこの資料に含む必要があります。また、各要件のプロセスに従って、システムが設計及び製造されていることを証明する必要もあります。そのため、記録書等の証憑書類の作成についても、同プロセス内にて言及されなければなりません。セキュア開発ライフサイクルに関する各要件の詳細は、「6 章 セキュア開発ライフサイクルに関する要件の解説」にて詳しく解説しております。

6 章 セキュア開発ライフサイクルに関する要件の解説　P. 154

・ソフトウェアの更新及びパッチの適用

ソフトウェアの更新及びパッチの適用に対応しているかどうかを明確にする必要があります。特に、パッチの適用については、パッチを適用しない場合にどのようなリスクがあ

るかを明確にする必要があります。ソフトウェアの更新については、「3. 依存コンポーネント又はオペレーティングシステムのセキュリティアップデート文書」にて詳しく解説しております。また、パッチの適用については、「2. セキュリティアップデートの文書」にて詳しく解説しております。

依存コンポーネント又はオペレーティングシステムのセキュリティアップデート文書 P. 160

セキュリティアップデートの文書 P. 158

書類審査

	6. セキュア開発ライフサイクル文書
☐	-1. 次に掲げる事項が含まれていること。
☐	(1) セキュリティ面をどのように扱ったかの記録
☐	次に掲げる段階において、記録した文章を作成すること。
☐	(a) 要件分析段階
☐	(b) 設計段階
☐	(c) 実装段階
☐	(d) 検証段階
☐	(e) リリース段階
☐	(f) 保守段階
☐	(g) 終了段階
☐	(2) セキュア開発ライフサイクルに関するプロセス及び管理
☐	各要件の詳細は、ガイドライン 6 章「セキュア開発ライフサイクルに関する要件の解説」を確認すること。
☐	(3) ソフトウェアの更新及びパッチの適用

7. コンピュータシステムの保守及び検証のための計画

規則　X4.4.1(7)

当該図書は，要求に応じて本会に提出され，システムのセキュリティ関連の保守及び試験に関する手順を含むものでなければならない。当該文書は，**システム要件のひとつである「19 セキュリティ機能の検証」**で要求する，システムのセキュリティ機能のあるべき動作をユーザーが確認する方法についての指示を含むものでなければならない。

解説

コンピュータシステムの保守及び検証のための計画とは、セキュリティ機能の維持に必要な保守及び試験の手順について説明した文書となります。これは、システム所有者がシステム運用後にセキュリティ機能を保守及び試験するための手段及び指示を示す資料です。供給者がそれらの情報を明確に提供することで、所有者は適切な作業を行うことが可能になります。システム運用後の保守及び試験については、X 編 5 章（UR E26）にて定期的に実施されることが要求されます。

また、システム要件のひとつである「19 セキュリティ機能の検証」では、セキュリティ機能のあるべき動作を検証する機能を実装する旨が規定されています。この機能は、セキュリティ機能の保守及び試験をサポートする機能となります。したがって、この機能の詳細や使用方法が、この資料内に含まれなければなりません。詳細について、「19 セキュリティ機能の検証」にて詳しく解説しております。

セキュリティ機能の検証　P. 101

書類審査

	7. コンピュータシステムの保守及び検証のための計画
□	-1. 次に掲げる事項が含まれていること。
□	(1) セキュリティ機能の推奨設定に関する説明
□	(2) セキュリティ機能のあるべき動作をユーザーが確認する方法
	システム要件「19 セキュリティ機能の検証」によって実装された機能が含まれていること。

8. 就航後のインシデント対応とリカバリープランをサポートする情報

規則　X4.4.1(8)

当該図書は，要求に応じて本会に提出され，ユーザーが以下を達成することを可能にする手順又は指示を含むものでなければならない。

(1) ローカル独立制御
(2) ネットワークの分離
(3) 監査記録によるフォレンジック
(4) あらかじめ決定した出力
(5) バックアップ
(6) 復旧
(7) 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

解説

就航後のインシデント対応とリカバリープランをサポートする情報とは、サイバーインシデントが発生した場合に、システム所有者がその対応及び復旧するための具体的な手順が記載された資料です。

詳細は以下のとおりです。

・ローカル独立制御

ローカル独立制御とは、システムを設置場所又はその近傍で直接行う制御です。これは、遠隔制御される主機又は可変ピッチプロペラの機側制御装置に使用されるコンピュータシステムに対して適用されます。適用されるコンピュータシステムにおいては、ネットワークから独立制御状態に移行するための手順及び独立制御状態での操作手順などが記載される必要があります。

・ネットワークの分離

ネットワークの分離とは、コンピュータシステムをネットワークから分離することです。これは、セキュリティが突破された場合にシステムを分離することで、更なる拡大を防ぐとともに、不可欠な機能をサポートします。ここでは、システムをネットワークから分離するための手順が記載される必要があります。例えば、組み込まれたネットワークデバイスにある物理的な ON/OFF スイッチの操作などが挙げられます。

・監査記録によるフォレンジック

フォレンジックの具体的な対応です。フォレンジックとは、監査記録[1]及び監査ログ[2]を用いて、重要なイベントの原因や経緯を調査・分析する活動を指します。ここでの目的は、システムに対するフォレンジックをサポートすることです。したがって、この資料には、フォレンジックの具体的な手順を含む必要があります。例えば、監査記録及び監査ログの情報収集、原因分析に関する手順等が挙げられます。

なお、この対応は、セキュリティ機能の要件の一つである「13. 監査可能な事象」を達成する機能によりサポートされます。詳細について、「13. 監査可能な事象」にて詳しく解説しております。

監査可能な事象 P. 86

・あらかじめ決定した出力

攻撃により通常の動作を維持できなくなった場合に、出力をあらかじめ指定した状態に設定する対応です。この対応は、セキュリティ機能の要件の一つである「20. あらかじめ決定した出力」を達成する機能によりサポートされます。詳細について、「20. あらかじめ決定した出力」にて詳しく解説しております。

あらかじめ決定した出力 P. 104

・バックアップ

重要なファイルをバックアップするための対応です。この対応は、セキュリティ機能の要件の一つである「26. システムのバックアップ」を達成する機能として実装されます。詳細について、「26. システムのバックアップ」にて詳しく解説しております。

システムのバックアップ P. 117

・復旧

システムが混乱又は故障の後、既知の復旧及び再構成するための対応です。既知の保護された状態とは、以下の状態を指します。

・システムパラメータがデフォルト[3]又は安全な値であること
・セキュリティに関する重要なパッチ[4]が再インストールされること
・セキュリティに関する設定が再確認、再設定されていること
・システム文書及び操作手順が使用可能であること
・アプリケーション及びシステムソフトウェアが安全な設定で再インストールされること

---

[1] **監査記録**　セキュリティに関わる重要な事象の単一の記録
[2] **監査ログ**　監査記録を時系列に収集したもの
[3] **デフォルト**　システムが出荷時に設定されている標準値、状態、動作条件。
[4] **パッチ**　システムの脆弱性やセキュリティ上の欠陥を修正するためのプログラム。

・バックアップデータから情報が復元されていること

ここでの目的は、システムが混乱又は故障の後、既知の保護された状態に復旧及び再構成することとなります。したがって、この資料には、既知の保護された状態に復旧及び再構成する手順及び指示を含める必要があります。

なお、ここでの要求事項の一部は、セキュリティ機能の要件の一つである「27. システムの復旧及び再構成」を達成する機能として実装されている場合があります。詳細について、「27. システムの復旧及び再構成」にて詳しく解説しております。

システムの復旧及び再構成 P. 119

・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

ここでは、制御されたシャットダウン、リセット、ロールバック及び再起動の手順について記載される必要があります。

制御されたシャットダウンとは，ソフトウェアの機能により，コンピュータシステム又はネットワークの電源を切る際に，接続された他のシステムが実行中の処理を実施／中止又は，終了して，接続を切ることにより，安全で既知の状態にすることです。強制的なシャットダウンでは、データ又はプログラム及びオペレーティングシステムファイルの破損などにより、不可欠な機能の喪失につながる可能性があるため、この手順が求められます。

リセットとは、システムのメモリを消去し、初期状態へ戻すことです。

ロールバックとは、システムを以前の安全な状態へ戻すことです。

再起動とは、システムを停止させ、すぐに再度起動することです。

書類審査

	8. 就航後のインシデント対応とリカバリープランをサポートする情報
☐	-1. 次に掲げる手順又は指示が含まれていること。
☐	(1) ローカル独立制御
☐	(2) ネットワークの分離
☐	(3) 監査記録によるフォレンジック
☐	(4) あらかじめ決定した出力
☐	(5) バックアップ
☐	(6) 復旧
☐	(7) 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

9. 計画の変更に関する管理

規則　X4.4.1(9)

当該図書は，要求に応じて本会に提出されなければばらない。当該計画書は，サイバーセキュリティに特化したものではなく，**X 編 3 章（UR E22）**でも要求されているものであることが期待される。

解説

計画の変更に関する管理とは、サイバーセキュリティの変更に関する管理手順書です。サイバーセキュリティの変更とは、例えばセキュリティパッチの適用などが該当します。

この資料は、X 編 3 章（UR E22）で要求されるハードウェア及びソフトウェアの両方を対象とした変更管理手順と統合したものとして作成されることが推奨されます。X 編 3 章（UR E22）で要求される変更管理については、X 編 3.6 に規定されております。

書類審査

	9. 計画の変更に関する管理
□	-1. サイバーセキュリティに関する変更管理手順が含まれていること。ただし、X 編 3 章（UR E22）で要求される変更管理手順書が提出されている場合はこの限りではない。

10. 試験結果

規則　X4.4.1(10)

X 編 4 章（UR E27）のセキュリティ機能を満たす，使用承認証書を有するコンピュータシステムは，本会による検査を免除することができる。ただし，供給者が署名した試験結果は，供給者が設計，製造，試験，設定及び強化が完了していることを実証するものとし，本会は検査において当該図書の確認を行う。

解説

試験結果とは、供給者が製品に対して設計，製造，試験，設定及び強化が完了していることを実証する資料です。使用承認証書を有するコンピュータシステムは、この資料を本会へ提出することで、本会の提出資料の一部及び立会検査を省略できます。使用承認証書を有する場合の個品承認のプロセスは、「2 章 承認プロセス」をご確認ください。

2 章 承認プロセス　P. 5

詳細は、以下のとおりです。

❶

試験	日付	結果	添付資料
(1) 一般的な検査項目			
(2) セキュリティ機能試験			
(3) セキュリティ機能の正確な設定			
(4) セキュア製品開発ライフサイクル			
(5) インストール時におけるハードニング			

❷

日付	
社名	
部署名	
氏名	
署名	

❶ 試験記録欄

(1)から(4)は、X 編 2.2.3（ガイドライン 4 章）で要求される立会検査の試験項目となります。(5)は、インストール時におけるハードニングとなります。ここでは、セキュリティ強化指針で規定される指針に基づいて、ハードニングが実施される必要があります。セキュリティ強化指針の詳細は、以下に詳しく解説しております。

セキュリティ強化指針　P. 168

(1)から(5)までの検査は、試験日及び結果について記録されます。また、検査結果を実証する資料を関連資料としてご提出ください。（例：セキュリティ機能の試験方案、ハードニング実施記録書など）

❷ 署名欄

試験結果には、供給者により署名される必要があります。すべての検査が完了しましたら、日付、社名、部署名及び氏名を記載のうえ、ご署名ください。

書類審査

	10.　試験結果
☐	-1.　次に掲げる検査項目が含まれていること。
☐	(1) 一般的な検査項目
☐	(2) セキュリティ機能試験
☐	(3) セキュリティ機能の正確な設定
☐	(4) セキュア開発ライフサイクル
☐	(5) インストール時におけるハードニング
☐	-2.　供給者による署名が含まれていること。

4 章 立会検査の解説

本章では、X 編 4 章（UR E27）で要求される立会検査の詳細を解説します。

立会検査の概要

■ 立会検査の要件

X 編 4 章（UR E27）では、コンピュータシステムのサイバーセキュリティに関する立会検査として、計 4 点の検査項目の要件が規定されております。各項目は以下のとおりです。

立会検査に要求される検査項目

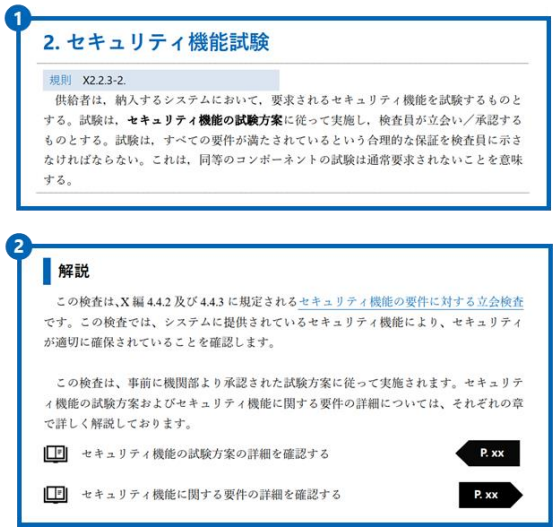
■ 事前に準備される資料

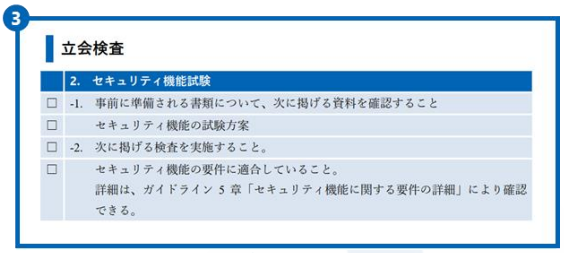
立会検査では、承認が要求される資料の一部が必要となります。したがって、立会試験での申請に併せて、以下の資料をご提出ください。

	立会検査に必要となる資料
☐	コンピュータシステム資産インベントリ
☐	トポロジー図
☐	セキュリティ機能の試験方案
☐	セキュリティ構成指針
☐	セキュア開発ライフサイクル文書

立会検査の詳細

以降のページの見方





1 要件

立会検査の名称と要件の詳細です。

2 解説

立会検査の解説です。

3 書類審査

立会検査のチェックリストです。

1. 一般的な検査項目

規則　X2.2.3-1.

供給者は，設計，製造及び内部での試験が完了したことを証明しなければならない。また，納入されるシステムが，承認された文書によって正確に示されていることを証明するものとする。これは，システムを検査し，コンポーネント及び配置／構成を資産に関する**インベントリ**及び**トポロジー図**と比較することによって実施しなければならない。

解説

この検査は、システムが適切に製造されたかどうかを確認する検査です。この検査では、システムがプロセスどおりに完成されていることを実証するために、書類確認および外観検査を実施します。

この検査の詳細は以下のとおりとなります。

・書類確認

設計，製造及び内部での試験が完了したことを示す記録を確認します。

・外観検査

システムのコンポーネント及び配置／構成をコンピュータシステム資産インベントリおよびトポロジー図により確認します。

コンピュータシステム資産インベントリおよびトポロジー図の詳細については、「3 章　提出資料の要件に関する詳細」で詳しく解説しております。

コンピュータシステム資産インベントリ　P. 20

トポロジー図　P. 22

立会検査

	1.　一般的な検査項目
☐	-1.　事前に準備される書類について、次に掲げる資料を確認すること。
☐	(1)　コンピュータシステム資産インベントリ
☐	(2)　トポロジー図
☐	-2.　次に掲げる検査を実施すること。
☐	(1)　書類確認
☐	(a)　設計が完了したことを示す記録
☐	(b)　製造が完了したことを示す記録

☐	(c) 社内試験が完了したことを示す記録
☐	(2) 外観検査
☐	(a) システムの構成
☐	コンピュータシステム資産インベントリ及びトポロジー図と比較すること

2. セキュリティ機能試験

規則　X2.2.3-2.

供給者は，納入するシステムにおいて，要求されるセキュリティ機能を試験するものとする。試験は，**セキュリティ機能の試験方案**に従って実施し，検査員が立会い／承認するものとする。試験は，すべての要件が満たされているという合理的な保証を検査員に示さなければならない。これは，同等のコンポーネントの試験は通常要求されないことを意味する。

解説

この検査は、X 編 4.4.2 及び 4.4.3 に規定予定のセキュリティ機能の要件に対する立会検査です。この検査では、システム要件で要求されるセキュリティ機能により、セキュリティが適切に確保されていることを確認します。

この検査は、事前に機関部より承認された試験方案に従って実施されます。「セキュリティ機能の試験方案」および「システム要件」に関する要件の詳細については、それぞれの章で詳しく解説しております。

セキュリティ機能の試験方案　P. 26

5 章　システム要件の解説　P. 47

立会検査

	2.　セキュリティ機能試験
☐	-1.　事前に準備される書類について、次に掲げる資料を確認すること。
☐	セキュリティ機能の試験方案
☐	-2.　次に掲げる検査を実施すること。
☐	システム要件に適合していること。 詳細は、ガイドライン 5 章「システム要件の解説」を確認すること。

3. セキュリティ機能の正確な設定

規則　X2.2.3-3.

供給者は，検査員に対して，システムのコンポーネントにおけるセキュリティ設定が**セキュリティ構成指針**に従って構成されていることを試験／実証しなければならない。当該実証は，セキュリティ機能の試験と同時に実施することができる。セキュリティの設定は，報告書に文書化されなければならない。(構成指針の船舶特有の事例等)

解説

この検査は、システムのコンポーネントがセキュリティ構成指針に従って構成されていることを確認する検査です。セキュリティ構成指針とは、コンピュータシステムに提供されるセキュリティ機能の推奨設定を説明した資料となります。詳しくは、「セキュリティ構成指針」にて詳しく解説しております。

セキュリティ構成指針　P. 28

この検査の詳細は、以下のとおりです。

・供給者による試験／実証

供給者は、システムのコンポーネントが定められたセキュリティ構成指針に従って設定されていることを示す必要があります。具体的には、セキュリティ機能の推奨設定が設定されていることを確認します。

・セキュリティ機能の試験との同時実施

このセキュリティ構成の検証は、「セキュリティ機能試験」にて実施される「ネットワーク及びセキュリティ構成設定」の機能の実証試験として実施されます。試験の方法について、「ネットワーク及びセキュリティ構成設定」にて詳しく解説しております。

ネットワーク及びセキュリティ構成設定　P. 124

・報告書への文書化

セキュリティ設定とその検証結果は、報告書として文書化される必要があります。これは、設定が指針に準拠していることを明示的に示し、後で検証できるようにするためです。また、この報告書は試験終了後速やかに担当検査支部へ提出する必要があります。

立会検査

	3.　セキュリティ機能の正確な設定
□	-1.　事前に準備される書類について、次に掲げる資料を確認すること。
□	セキュリティ構成指針
□	-2.　次に掲げる検査を実施すること。

□	ネットワーク及びセキュリティ構成設定の要件に適合すること。 詳細は、ガイドライン 5 章「システム要件の詳細」中「ネットワーク及びセキュリティ構成設定」により確認できる。

4. セキュア開発ライフサイクル

規則　X2.2.3-4.

供給者は，**セキュア開発ライフサイクル文書**を参考に，**セキュア開発ライフサイクル**の要件に適合していることを実証しなければならない。

解説

この検査は、X 編 4.5 に規定予定のセキュア開発ライフサイクルの要件に対する立会検査です。この検査では、セキュア開発ライフサイクルに従って、セキュアな製品が製造されていることを確認します。

この検査では、セキュア開発ライフサイクルの要件に規定する管理されたプロセスに従って、製品が製造されていることを確認します。具体的には、マネジメントシステム文書により文書化された各要件の取り扱いが、そのとおりに実施されていることを確認します。各要件は、マネジメントシステム文書により、どのように要件を満足したかを示す記録が作成されなければなりません。したがって、本試験では、その記録の確認を行います。

本検査では、各要件の詳細を把握するために、機関部より承認されたセキュア開発ライフサイクル文書を参考とします。なお、セキュア開発ライフサイクル文書およびセキュア開発ライフサイクルに関する要件については、それぞれの章で詳しく解説しております。

セキュア開発ライフサイクル文書　P. 30

6 章 セキュア開発ライフサイクルに関する要件の解説　P. 154

立会検査

	4. セキュア開発ライフサイクル
☐	-1. 事前に準備される書類について、次に掲げる資料を確認すること。
☐	セキュア開発ライフサイクル文書
☐	-2. 次に掲げる検査を実施すること。
☐	セキュア開発ライフサイクルの要件に適合していること。 詳細は、ガイドライン 6 章「セキュア開発ライフサイクルに関する要件の詳細」を確認すること。

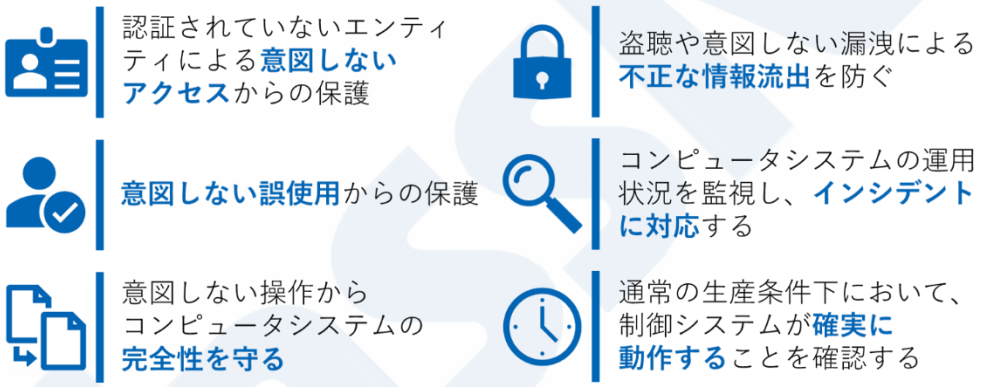
5 章 システム要件の解説

本章では、X 編 4.4.2 および 4.4.3 で要求されるシステム要件の詳細を解説します。システム要件とは、コンピュータシステムに求められるセキュリティ機能に関する要件です。セキュリティ機能は、コンピュータシステムに対する脅威や攻撃から保護するための具体的な手段となります。最低限のセキュリティレベルの要求事項を満たすセキュリティ機能をコンピュータシステムに実装することにより、船舶をサイバー攻撃からのリスクを低減します。

システム要件の概要

■ 要求されるセキュリティ機能とは

システム要件は、システムに対する技術的セキュリティ要求事項として、6 つの基礎的要求事項を設定しています。



基礎的要求事項のもと、それぞれの目的を満たすためのシステム要件が定められます。各システム要件では、その要件で要求されるセキュリティ機能を実装することとなります。要求されるセキュリティ機能は、原則としてすべてのコンピュータシステムに適用されます。要求されるセキュリティ機能は以下のとおりとなります。

認証されていないエンティティによる意図しないアクセスからの保護

1. 使用者（人）の識別及び認証 P. 53

2. アカウントの管理 P. 56

3. 識別子の管理 P. 59

意図しない誤使用からの保護

意図しない操作からコンピュータシステムの完全性を守る

盗聴や意図しない漏洩による不正な情報流出を防ぐ

コンピュータシステムの運用状況を監視し、インシデントに対応する

通常の生産条件下において、制御システムが確実に動作することを確認する

■ 信頼できないネットワークには追加のセキュリティ機能が必要

X 編 4 章（UR E27）の適用の対象とならないコンピュータシステムが含まれるネットワークは、信頼できないネットワークと呼ばれます。これは、最低限のセキュリティ対策が講じられていないネットワークを指します。信頼できないネットワークとのネットワーク通信を行う場合、セキュリティをより強化しなければなりません。そのため、追加で要求されるセキュリティ機能の要件が適用となります。

追加で要求されるセキュリティ機能は以下のとおりとなります。

追加で要求されるセキュリティ機能

■ 一部のセキュリティ機能を設けられない場合は

何らかの理由により、要求されるセキュリティ機能を設けることができない場合、そのセキュリティ機能に代替する手段が講じられる必要があります。これは、補完的対策と呼ばれ、以下の条件を満たすことで、代替する手段として認められる場合がございます。

i) 元々規定されている要件と同じ脅威から保護すること。
ii) 元々規定されている要件と同等の厳しさ，正確さであること。
iii) 本章の他の要求事項により要求されるセキュリティ管理ではないこと。
vi) 新たなセキュリティリスクを発生させないこと。

補完的対策については、各要件の詳細にて、その一例を示している場合があります。例えば、以下のとおりです。

例　アカウント機能が実装できない

この場合、使用者を識別することができないため、攻撃者により、容易にアクセスされるリスクがあります。補完的対策としては、鍵付きのボックスに入れる等が挙げられます。鍵を施錠することにより、鍵を所有する人のみアクセスが可能となるため、代替手段として認められます。

なお、セキュリティ機能を補完的対策とする場合、以下の提出資料に対して、その対策又は試験方法を記載する必要があります。

・セキュリティ機能の説明

各々のセキュリティ機能の要件に対して、どのような機能が実装されているかを説明する資料です。セキュリティ機能を補完的対策とする場合、この対策の詳細を記載することとなります。詳細は、「セキュリティ機能の説明」に詳しく解説しております。

セキュリティ機能の説明　P.24

・セキュリティ機能試験

各々のセキュリティ機能に要求される実証試験の試験方案です。セキュリティ機能を補完的対策とする場合、この対策が講じられることによりセキュリティ機能の要件を満足することを立会検査にて確認する必要があります。詳細は、「セキュリティ機能試験」に詳しく解説しております。

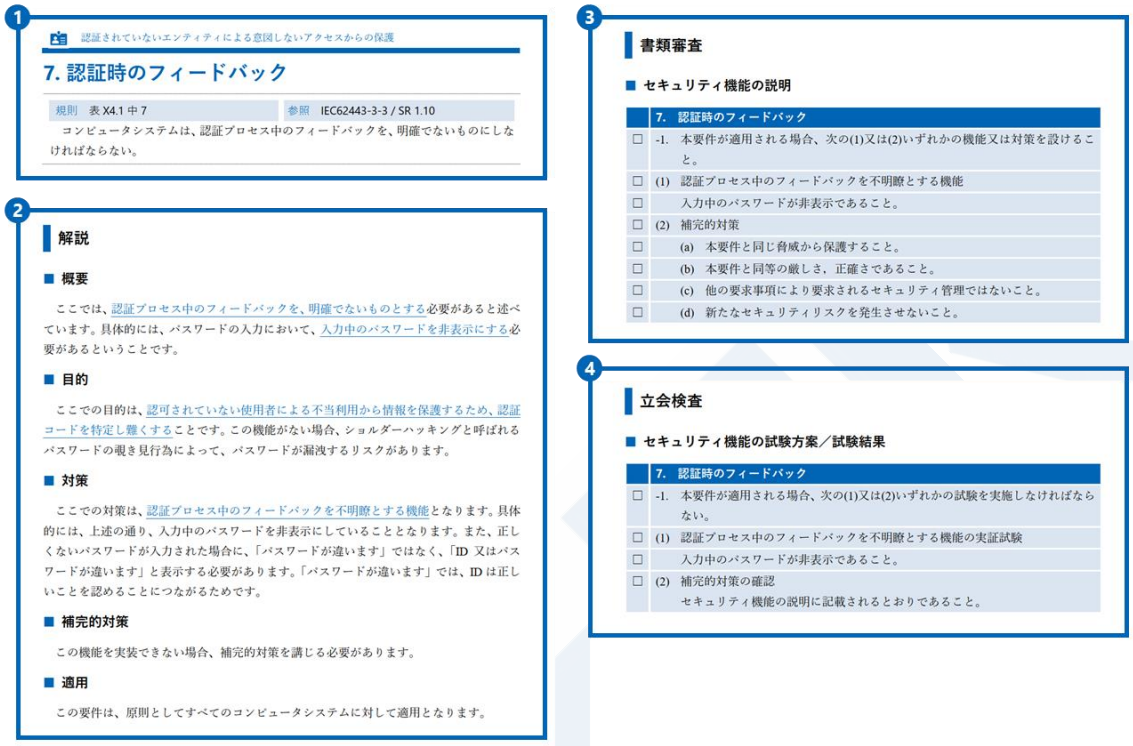
セキュリティ機能試験　P. 43

■ 一部のセキュリティ機能が適用されない場合がある

一部のシステム要件は、一部のコンピュータシステムに適用されない場合があります。例えば、「5. 無線アクセスの管理」の要件は、無線通信を行うシステムに対して要求されるセキュリティ機能ですので、無線通信をしないシステムは適用外となります。適用の要否についても、各要件の詳細にて、その一例を示しております。なお、システム要件を適用外とする場合、こちらもセキュリティ機能の説明内に、その詳細を記載する必要があります。

システム要件の詳細

以降のページの見方



① 要件

システム要件の名称と詳細です。名称の上段には、その要件における基礎的要求事項を記載しております。

② 解説

システム要件の解説です。以下で構成されています。

・概要：要件の概要
・目的：要件の主な目的
・対策：要件の具体的な対策
・補完的対策：要件を満たすために、本来のセキュリティ機能に代えて採用された対策
・適用：要件が適用される場合、またはされない場合

③ 書類審査

システム要件に関する書類審査のチェックリストです。

・セキュリティ機能の説明：X 編 4.4.1(3)で要求される提出資料。

④ 立会検査

システム要件に関する立会検査のチェックリストです。

・セキュリティ機能試験：X 編 2.2.3-2.で要求される立会検査。

1. 使用者（人）の識別及び認証

規則	参照
表 X4.1 中 1	IEC62443-3-3 / SR 1.1

コンピュータシステムは、直接又はインターフェース[1]を介してシステムにアクセス可能なすべての使用者（人）を識別及び認証するものでなければならない。

解説

■ 概要

ここでは、システムにアクセス可能なすべての人を識別及び認証することが必要だと述べています。識別と認証については、以下のとおりです。

用語	説明
識別	使用者それぞれを区別することです。これは、自身が誰であるかを示す識別子を用いて行います。人の識別の場合、識別子はユーザ名が一般的に使用されます。
認証	使用者が本人であることを証明することです。これは、識別子に加えて認証コードと呼ばれる使用者自身の身元を証明するための情報を用いて行います。認証コードは、パスワードが一般的に使用されます。

つまり、システムにログインするために、識別子と認証コードを使用する必要があるということです。

■ 目的

ここでの目的は、システムの利用を認められていない人に使用されるリスクを低減することです。システムが識別及び認証をしない場合、攻撃者により不正にアクセスされる可能性があります。これにより、船舶の運航に影響を及ぼす可能性があります。

■ 対策

ここでの対策は、すべての使用者（人）を識別及び認証する機能となります。具体的には、以下のとおりです。

・アカウントの機能

[1] **インターフェース**　使用者（人）とコンピュータシステムとの間で情報のやり取りを可能にする媒介または接点。例えば、Windows 等の汎用 OS によるソフトウェアへのアクセスは、デスクトップインターフェースを介して行われる。

識別子および認証コードを組み合わせたものはアカウントと呼ばれ、使用者を識別および認証するために利用されます。システムの利用者は、この機能によりシステムへログインできる必要があります。なお、識別子、認証コードおよびアカウントについては、それぞれの要件にて、詳しく解説しております。

アカウントの管理 P. 56

識別子の管理 P. 59

認証コードの管理 P. 62

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。以下に補完的対策の一例を示します。

・物理的なセキュリティ対策

識別及び認証を機能として実装する代わりに、物理的なアクセスに制限を加えることで、この機能を補完できます。例えば、あらかじめ決められた人員が管理する鍵がなければ、システムを操作できない構造とすることです。この場合、個々人の識別及び認証は不要であること、使用者それぞれの権限について検討されていること等が重要です。権限については、「8. 権限付与の実施」に詳しく解説しております。

権限付与の実施 P. 73

■ 適用

この要件は、原則としてすべてのコンピュータシステムに対して適用となります。

書類審査

■ セキュリティ機能の説明

	1. 使用者（人）の識別と認証
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 使用者（人）を識別及び認証する機能
☐	(a) 識別子によって識別すること。
☐	(b) 識別子および認証コードによって認証すること。
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。

☐	(d)　新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	1.　使用者（人）の識別と認証
☐	-1.　本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1)　使用者（人）を識別及び認証する機能の実証試験
☐	(a)　正規の識別子及び認証コードでログインできること。
☐	(b)　非正規の識別子及び／又は認証コードでログインできないこと。
☐	(2)　補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

2. アカウントの管理

規則　表 X4.1 中 2	参照　IEC62443-3-3 / SR 1.3

コンピュータシステムは、権限を有する使用者によるすべてのアカウントの管理（アカウントの追加、有効化、変更、無効化及び削除を含む）をサポートする機能を提供するものでなければならない。

解説

■ 概要

ここでは、すべてのアカウントを管理する必要があると述べています。アカウントとは、使用者の識別及び認証に使用されるものであり、識別子[1]および認証コード[2]で構成されます。識別及び認証については、「1. 使用者（人）の識別及び認証」に詳しく解説しております。

使用者（人）の識別及び認証　P. 53

また、この要件の対象となる使用者は、基本的には「人」のみとなります。しかし、以下の条件を満たす場合は、「人」に加えて、「ソフトウェアプロセス」及び「デバイス」も対象となります。

・無線通信を行う場合
・信頼できないネットワークとのネットワーク通信を行う場合

なお、無線通信については「5 .無線アクセスの管理」に、信頼できないネットワークとのネットワーク通信については、「32. 使用者（ソフトウェアプロセスとデバイス）の識別及び認証」に詳しく解説しております。

無線アクセスの管理　P. 65

ソフトウェアプロセス及びデバイスの識別及び認証　P. 132

■ 目的

ここでの目的は、システムの使用者を適切に管理することです。この管理が不適切であると、使用の権限を持たない人によって不正アクセスされる可能性があります。

[1] **識別子**　自身が誰であるかを示すもの。ユーザ ID 等。
[2] **認証コード**　使用者自身の身元を証明するための情報。パスワード等。

■ 対策

ここでの対策は、権限を有する使用者によるすべてのアカウントの管理（アカウントの追加、有効化、変更、無効化及び削除を含む）をサポートする機能となります。この機能は、管理権限が設定された人（管理者）のみ使用できるように制限することが必要です。

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。アカウントの有効化及び無効化が実装されていない場合は、追加および削除にて補完する旨などを記載する必要があります。

■ 適用

以下の場合、この要件は適用となりません。

・「1. 使用者（人）の識別及び認証」の機能を補完的対策とする場合、又は同要件が適用外の場合

使用者の識別及び認証する機能を実装していない場合、アカウントの機能がありません。この場合、この要件は適用外となります。

書類審査

■ セキュリティ機能の説明

	2. アカウントの管理
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) アカウントを管理する機能
☐	(a) 次に掲げる機能を実装していること。
☐	i) アカウントの追加、変更及び削除
☐	ii) アカウントの有効化及び無効化（補完的対策をとる場合は、その理由）
☐	(b) 権限を有する使用者のみが、アカウントを管理できること。
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	2. アカウントの管理
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) アカウントを管理する機能の実証試験
☐	(a) 次に掲げる機能が動作すること。
☐	i) アカウントの追加、変更及び削除
☐	ii) アカウントの有効化及び無効化
☐	(b) アカウントの管理権限について、次のとおりであること。
☐	i) 権限を有する使用者のみが、アカウントを管理できること。
☐	ii) 権限を有していない使用者が、アカウントを管理できないこと。
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

3. 識別子の管理

規則　表 X4.1 中 3　　参照　IEC62443-3-3 / SR 1.4

コンピュータシステムは、使用者、グループ及び役割による識別子の管理をサポートする機能を提供するものでなければならない。

解説

■ 概要

ここでは、使用者、グループ及び役割による識別子の管理が必要と述べています。識別子とは、自分自身が誰であるかを示すものです。人の識別では、一般的にユーザ名等が該当します。

また、この要件の対象となる使用者は、基本的には「人」のみとなります。しかし、以下の条件を満たす場合は、「人」に加えて、「ソフトウェアプロセス」及び「デバイス」も対象となります。

・無線通信を行う場合
・信頼できないネットワークとのネットワーク通信を行う場合

なお、無線通信については「5 .無線アクセスの管理」に、信頼できないネットワークとのネットワーク通信については、「32. 使用者（ソフトウェアプロセスとデバイス）の識別及び認証」に詳しく解説しております。

無線アクセスの管理　P. 65

ソフトウェアプロセス及びデバイスの識別及び認証　P. 132

■ 目的

ここでの目的は、要件のとおり、使用者、グループ及び役割による識別子を管理することです。

■ 対策

ここでの対策は、使用者、グループ及び役割による識別子の管理をサポートする機能です。具体的には、以下のとおりとなります。

・グループアカウントを作成する機能

グループアカウントとは、グループや役割によりまとめられた集団のアカウントです。アカウントについては、例えば以下の一例が考えられます。

・航海士と機関士
・システムの利用者と保守整備者
・システムの管理者と利用者

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。

■ 適用

以下の場合、この要件は適用となりません。

・「1. 使用者（人）の識別及び認証」の機能を補完的対策とする場合、又は同要件が適用外の場合

使用者の識別及び認証する機能を実装されていない場合、識別子はありません。この場合、この要件は適用外となります。

使用者（人）の識別及び認証 P. 53

書類審査

■ セキュリティ機能の説明

	3. 識別子の管理
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 使用者、グループ及び役割による識別子の管理をサポートする機能
☐	識別子を追加、変更及び削除すること。
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	3. 識別子の管理

☐	-1.	本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1)	使用者、グループ及び役割による識別子の管理をサポートする機能の実証試験
☐		識別子を追加、変更及び削除すること。
☐	(2)	補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

4. 認証コードの管理

規則　表 X4.1 中 4	参照　IEC62443-3-3 / SR 1.5

コンピュータシステムは、次に掲げる機能を提供するものでなければならない。

・認証コードの内容の初期化
・制御システムのインストールに際しての、すべてのデフォルト認証コードの変更
・すべての認証コードの変更／更新
・保存及び伝送されるすべての認証コードの、不正開示及び変更からの保護

解説

■ 概要

ここでは、認証コードを管理する必要があると述べています。**認証コード**とは、使用者が自身の身元を証明するための情報です。認証コードは、主にパスワード、PIN[1]、セキュリティトークン[2]、公開鍵認証方式[3]で利用する秘密鍵、物理鍵[4]、指紋認証及び顔認証などがあります。

また、この要件の対象となる使用者は、基本的には「人」のみとなります。しかし、以下の条件を満たす場合は、「人」に加えて、「ソフトウェアプロセス」及び「デバイス」も対象となります。

・無線通信を行う場合
・信頼できないネットワークとのネットワーク通信を行う場合

なお、無線通信については「5 .無線アクセスの管理」に、信頼できないネットワークとのネットワーク通信については、「32. 使用者（ソフトウェアプロセスとデバイス）の識別及び認証」に詳しく解説しております。

無線アクセスの管理　P. 65

ソフトウェアプロセス及びデバイスの識別及び認証　P. 132

[1] **PIN**　Personal Identification Number の略。認証コードのひとつ。通常、4～6 桁の数字で構成される。
[2] **セキュリティトークン**　システムにアクセスするための一時的なコードである「ワンタイムパスワード（OTP）」を発行する機器。
[3] **公開鍵認証方式**　認証コードのひとつ。公開鍵と秘密鍵のペアを用いて認証を行う方式。
[4] **物理鍵**　認証コードのひとつ。物理的なロック（金庫、システムなど）を解錠するための鍵。

■ 目的

ここでの目的は、認証コードの機密性を確保することです。認証コードが漏洩することで、攻撃者に不正使用される可能性があります。これによって、船舶の運航に影響を及ぼす可能性があります。

■ 対策

ここでの対策は、認証コードを管理する機能となります。パスワードを例に、具体的には以下のとおりです。

・認証コードの初期化

例えば、パスワードの初期化です。認証コードを失った場合に、新しい認証コードを設定することができます。

・システムのインストール時にデフォルトの認証コードの強制変更

例えば、初期パスワードからの変更です。初期状態の認証コードが予測しやすい、あるいは広く公開されている場合に潜在的なセキュリティリスクを軽減することができます。

・すべての認証コードの変更や更新認証

例えば、パスワードの変更です。コードをいつでも変更することができます。

・保存や伝送されるすべての認証コードについて、不正開示および変更からの保護

例えば、パスワードの暗号化です。認証コードの機密性を保護することができます。

補足　認証コードにパスワードを利用している場合は、その強度に関する要件が「6. パスワードによる認証の強度」に定められております。

パスワードによる認証の強度　P. 68

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。

■ 適用

以下の場合、この要件は適用となりません。

・「1. 使用者（人）の識別及び認証」の機能を補完的対策とする場合、又は同要件が適用外の場合

使用者の識別及び認証する機能を実装していない場合、認証コードはありません。この場合、この要件は適用外となります

使用者（人）の識別及び認証　P. 53

書類審査

■ セキュリティ機能の説明

	4. 認証コードの管理
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
□	(1) 認証コードを管理する機能
□	次に掲げる機能を実装していること。
□	(a) 認証コードの初期化（例：パスワードの初期化）
□	(b) システムのインストール時にデフォルトの認証コードの強制変更（例：初期パスワードからの変更）
□	(c) すべての認証コードの変更や更新（例：パスワードの変更）
□	(d) 保存や伝送されるすべての認証コードについて、不正開示および変更からの保護（例：パスワードの暗号化）
□	(2) 補完的対策
□	(a) 本要件と同じ脅威から保護すること。
□	(b) 本要件と同等の厳しさ，正確さであること。
□	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
□	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	4. 認証コードの管理
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
□	(1) 認証コードを管理する機能の実証試験
□	次に掲げる機能の動作を確認すること。
□	(a) 認証コードの初期化（例：パスワードの初期化）
□	(b) システムのインストール時にデフォルトの認証コードの強制変更（例：初期パスワードからの変更）
□	(c) すべての認証コードの変更や更新（例：パスワードの変更）
□	(d) 保存や伝送されるすべての認証コードについて、不正開示および変更からの保護（例：パスワードの暗号化）
□	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

5. 無線アクセスの管理

規則　表 X4.1 中 5	参照　IEC62443-3-3 / SR 1.6

コンピュータシステムは、無線通信をするすべての使用者（人、ソフトウェアプロセス又はデバイス）を識別及び認証する機能を提供するものでなければならない。

解説

■ 概要

ここでは、無線通信をする使用者を識別および認証する必要があると述べています。無線通信の場合、使用者の識別および認証は人だけではなく、ソフトウェアプロセスとデバイスも対象となります。ソフトウェアプロセスおよびデバイスについては、以下のとおりです。

用語	説明
ソフトウェアプロセス	システムが利用するプログラムやアプリケーションを指します。
デバイス	システムを利用する物理的なハードウェアや機器を指します。

■ 目的

ここでの目的は、サイバー攻撃のリスクがある無線通信下でのセキュリティを強化することです。無線通信と有線通信の大きな違いは、電波の届く範囲であればリモートから攻撃者が容易にネットワークにアクセスできてしまう点です。有線の場合は、ポートを閉じる、入退室管理などの物理的対策も有効となります。しかし、それらの対策は無線通信には有効でありません。したがって、無線接続下で利用可能な識別及び認証機能を設け、正規の使用者のみアクセス可能な状態にすることが、対策として必要となります。

■ 対策

ここでの対策は、無線通信をする人、ソフトウェアプロセス又はデバイスを識別及び認証する機能です。例えば、以下が挙げられます。

・IEEE802.1X

これはネットワーク端末を認証するための規格です。RADIUS 等の認証サーバによって使用者の識別及び認証を行うことにより、無線接続のセキュリティを強固にします。

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。

■ 適用

以下の場合、この要件は適用となりません。

・コンピュータシステムが無線通信しない場合

コンピュータシステムが無線通信しない場合は、この要件は適用されません。

書類審査

■ セキュリティ機能の説明

	5. 無線アクセスの管理
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 無線通信を行うすべての使用者を識別、認証する機能
☐	(a) 人の識別と認証
☐	i) 識別子によって識別すること。
☐	ii) 識別子および認証コードによって認証すること。
☐	(b) ソフトウェアプロセスの識別と認証
☐	i) 識別子によって識別すること。
☐	ii) 識別子および認証コードによって認証すること。
☐	(c) デバイスの識別と認証
☐	i) 識別子によって識別すること。
☐	ii) 識別子および認証コードによって認証すること。
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	5. 無線アクセスの管理
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) 無線通信を行うすべての使用者を識別、認証する機能の実証試験
☐	(a) 人の識別と認証

☐	i) 正規の識別子および認証コードによってログインできること。
☐	ii) 非正規の識別子および認証コードによってログインできないこと。
☐	(b) ソフトウェアプロセスの識別と認証
☐	i) 正規の識別子および認証コードによってログインできること。
☐	ii) 非正規の識別子および認証コードによってログインできないこと。
☐	(c) デバイスの識別と認証
☐	i) 正規の識別子および認証コードによってログインできること。
☐	ii) 非正規の識別子および認証コードによってログインできないこと。
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

6. パスワードによる認証の強度

規則	参照
表 X4.1 中 6	IEC62443-3-3 / SR 1.7

コンピュータシステムは、パスワードの設定を、最短の長さ及び文字の種類の多様性に基づいて、強化する機能を提供するものでなければならない。

解説

■ 概要

ここでは、パスワードの設定を、最短の長さ及び文字の種類の多様性に基づいて、強化する必要があると述べています。つまり、パスワードは短すぎず、多様な文字によって設定できる必要があるということです。

■ 目的

ここでの目的は、攻撃者によるパスワードの推測を難しくすることです。例えば、パスワードが 4 桁の数字だけで構成されている場合、その強度は低く、簡単に推測される可能性が高くなります。

■ 対策

ここでの対策は、パスワードの設定を強化する機能となります。具体的には、パスワードの最低限の長さ及び文字の種類について、システムに適したものとするように強化する必要があります。参考となる指針は、以下のとおりです。

・NIST[1] SP800-63
長さ：少なくとも 8 文字（ユーザが作成するパスワードの場合）
種類：ASCII(REF 20)文字。スペース。Unicode(ISO/OSC10646)文字等

・(NISC[2])インターネットの安全
種類：英大小文字＋数字＋記号 26 種で合計 88 種

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。以下に補完的対策の一例を示します。

[1] **NIST** 米国国立標準技術研究所。National Institute of Standards and Technology の略。
[2] **NISC** 内閣サイバーセキュリティセンター。National Center of Incident Readiness and Strategy for Cybersecurity の略。

・多要素認証

認証方法を 2 要素以上とすることで、認証の強度が上がるため、この要件の機能を補完することができます。多要素認証については、「31. 使用者（人）の多要素認証」に詳しく解説しております。

使用者（人）の多要素認証 P. 129

■ 適用

以下の場合、この要件は適用となりません。

・認証コードにパスワードを使用しない場合

認証コードにパスワードを使用しない場合は、この要件は適用されません。

書類審査

■ セキュリティ機能の説明

	6. パスワードによる認証の強度
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) パスワードの設定を強化する機能
☐	(a) 最短の長さ
☐	対策に掲げた指針等に基づいて決定されたものであること
☐	(b) 文字の種類の多様性
☐	対策に掲げた指針等に基づいて決定されたものであること
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	6. パスワードによる認証の強度
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) パスワードの設定を強化する機能の実証試験
☐	(a) 最短の長さ

☐	次に掲げる項目に適合すること。
☐	i) 決定された最短の長さ以上で、パスワードが設定できること。
☐	ii) 決定された最短の長さ未満で、パスワードが設定できないこと。
☐	(b) 文字の種類の多様性
☐	決定された文字の種類で、パスワードが設定できること。
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

7. 認証時のフィードバック

規則	参照
表 X4.1 中 7	IEC62443-3-3 / SR 1.10

コンピュータシステムは、認証プロセス中のフィードバックを、明確でないものにしなければならない。

解説

■ 概要

ここでは、認証プロセス中のフィードバックを、明確でないものとする必要があると述べています。具体的には、パスワードの入力において、入力中のパスワードを非表示にする必要があるということです。

■ 目的

ここでの目的は、認可されていない使用者による不当利用から情報を保護するため、認証コードを特定し難くすることです。この機能がない場合、ショルダーハッキングと呼ばれるパスワードの覗き見行為によって、パスワードが漏洩する可能性があります。

■ 対策

ここでの対策は、認証プロセス中のフィードバックを不明瞭とする機能となります。具体的には、上述のとおり、入力中のパスワードを非表示にしていることとなります。また、正しくないパスワードが入力された場合に、「パスワードが違います」ではなく、「ID 又はパスワードが違います」と表示する必要があります。「パスワードが違います」では、ID は正しいことを認めてしまっているからです。

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。

■ 適用

この要件は、原則としてすべてのコンピュータシステムに対して適用となります。

書類審査

■ セキュリティ機能の説明

	7. 認証時のフィードバック
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。

☐	(1)　認証プロセス中のフィードバックを不明瞭とする機能
☐	入力中のパスワードが非表示であること。
☐	(2)　補完的対策
☐	(a)　本要件と同じ脅威から保護すること。
☐	(b)　本要件と同等の厳しさ，正確さであること。
☐	(c)　他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d)　新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	7.　認証時のフィードバック
☐	-1.　本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1)　認証プロセス中のフィードバックを不明瞭とする機能の実証試験
☐	入力中のパスワードが非表示であること。
☐	(2)　補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

8. 権限付与の実施

規則	参照
表 X4.1 中 8	IEC62443-3-3 / SR 2.1

すべてのインターフェースにおいて，使用者（人）に，職務分離及び最小特権の原則に従って権限を割り当てられるものでなければならない。

解説

■ 概要

ここでは、使用者（人）は「職務分離」と「最小特権」という 2 つの重要な原則に従って、権限を割り当てられる必要があると述べています。職務分離と最小特権については、以下のとおりです。

用語	説明
職務分離	一つの重要なタスクを二人以上に分けて、**一人が全ての権限を持つことを防ぐ原則**です。これは、個人だけでなく、役割やグループによる分離も可能です。具体的には、作業の担当者と承認者を分離するなどです。
最小特権	使用者（人）がその職務を遂行するのに**必要最小限の権限だけを持つという原則**です。具体的には、管理者はシステムの設定やユーザの追加などの操作が可能ですが、一般の使用者はシステムの操作のみが許可されます。

したがって、使用者（人）又は使用者（人）の役割を明確に定義し、適切な権限を割り当てた上で、使用者（人）が許可された操作のみ可能となるように制限することが必要ということです。

■ 目的

ここでの目的は、使用者に対して権限を適切に割り当てることです。

■ 対策

ここでの対策は、職務分離及び最小特権の原則に従って権限を割り当てることをサポートする機能となります。具体的には以下のとおりです。

・アクセス制御リストによって権限を管理する

アクセス制御リストとは、システムのリソース（ファイルやデータベース等）へのアクセスを制御するためのリストです。アクセス制御リストは以下の要素等によって構成されています。

要素	説明
主体 **Subject**	アクセスを許可された使用者（人）です。これは、グループベースを含むすべての使用者（人）が該当します。
対象 **Object**	アクセスを許可されたリソースです。例えば、ファイル、データベース、ネットワークリソースなどが該当します。
権限 **Permission**	アクセスを許可された操作です。例えば、読み取り、書き込み、実行などが該当します。

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。以下に補完的対策の一例を示します。

・物理的なセキュリティ

「1. 使用者（人）の識別及び認証」の機能について補完的対策をとる場合、システムにこの機能を実装できません。その場合は、物理的なセキュリティ等により、この機能を補完する必要があります。例えば、システムの利用者と保守整備者の権限付与の場合、保守整備者のみが保有する鍵などによりメンテナンスが可能となる等です。

使用者（人）の識別及び認証 P. 53

■ 適用

この要件は、原則としてすべてのコンピュータシステムに対して適用となります。

書類審査

■ セキュリティ機能の説明

	8. 権限付与の実施
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 職務分離及び最小特権の原則に従って権限を割り当てることをサポートする機能
☐	アクセス制御リスト等により、次に掲げる要素が管理されていること
☐	(a) 主体 (Subject)（例：グループベースを含むすべての使用者）
☐	(b) 対象 (Object)（例：ファイル、データベース、ネットワークリソース）
☐	(c) 権限 (Permission)（例：読み取り、書き込み、実行）
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。

☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	8. 権限付与の実施
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) 職務分離及び最小特権の原則に従って権限を割り当てることをサポートする機能
☐	アクセス制御リスト等により、次に掲げる要素が職務分離及び最小特権の原則に従って管理されていること
☐	(a) 主体（Subject）（例：グループベースを含むすべての使用者）
☐	(b) 対象（Object）（例：ファイル、データベース、ネットワークリソース）
☐	(c) 権限（Permission）（例：読み取り、書き込み、実行）
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

9. 無線の使用の管理

規則　表 X4.1 中 9	参照　IEC62443-3-3 / SR 2.2

コンピュータシステムは、一般に受け入れられるセキュリティに関する業界の慣行に従って、システムへの無線接続の認可、監視及び使用制限を実施する機能を提供するものでなければならない。

解説

■ 概要

ここでは、一般に受け入れられるセキュリティに関する業界の慣行に従って、システムへの無線接続の認可、監視及び使用制限を実施する必要があると述べています。一般に受け入れられるセキュリティに関する業界の慣行とは、一般的に使用される無線通信技術を指します。例えば、Wi-Fi や Bluetooth が該当します。また、無線接続の認可、監視及び使用制限については、以下のとおりです。

機能	説明
認可	特定のリソースや機能へのアクセスを許可又は拒否するプロセスのことです。これは通常、認証の後に行われ、使用者がアクセスまたは実行できる操作を制御します。
監視	無線接続された機器を監視することです。
使用制限	無線接続できる機器に対する使用を制限することです。

■ 目的

ここでの目的は、サイバー攻撃のリスクが高い無線通信下での使用に関するセキュリティをより強化することです。適切なセキュリティ対策が講じられていない場合、攻撃者が該当するアクセスポイントに接続し攻撃される可能性があります。

■ 対策

ここでの対策として、システムへの無線接続の認可、監視及び使用制限を実施する機能となります。WPA2-PSK 認証[1]の場合を例に説明します。

・認可

使用者毎に特定のリソースへのアクセスを許可または拒否する機能です。SSID（Service

[1] **WPA2-PSK 認証**　事前共有キーを使用して無線通信下のアクセスをセキュアにする認証方式

Set Identifier）及び暗号キーによって認証することで、ネットワークへのアクセスを制御します。

・監視

無線接続された機器を監視する機能です。Windows PC の画面等によって、接続された機器の一覧を確認することができます。なお、接続された機器は MAC アドレスによって識別されています。MAC アドレスとは、機器が固有に持つ物理的なアドレスです。

・使用制限

無線接続できる機器に対する使用を制限する機能です。MAC アドレスフィルタリングと呼ばれる機能により、特定の MAC アドレスを持つ機器のネットワークへのアクセスを制限します。

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。

■ 適用

以下の場合、この要件は適用となりません。

・無線通信をしない場合

コンピュータシステムが無線通信技術を有しておらず、アクセスポイントとならない場合は、本要件は適用されません。

書類審査

■ セキュリティ機能の説明

	9. 無線の使用の管理
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) システムへの無線接続の認可、監視及び使用制限を実施する機能
☐	(a) 一般的に受け入れられるセキュリティに関する業界の慣行に従って、次に掲げる機能が実装されること
☐	i) 認可
☐	ii) 監視
☐	iii) 使用制限
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	9. 無線の使用の管理
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) システムへの無線接続の認可、監視及び使用制限を実施する機能の実証試験
☐	次に掲げる項目に適合すること。
☐	(a) 設定画面等により、SSID 及び暗号キーの設定を確認できること
☐	(b) 試験用の SSID 及び暗号キーを設定できること
☐	(c) 接続した Windows PC の画面等により、接続された機器の一覧が確認できること
☐	最低でも、MAC アドレスが確認できること
☐	(d) 使用制限（MAC アドレス等）機能がある場合、許可された機器だけが接続できること
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

10. 可搬式及び携帯用デバイスの使用の管理

規則	参照
表 X4.1 中 10	IEC62443-3-3 / SR 2.3

可搬式及び携帯用デバイスの使用に対応したコンピュータシステムは、次に掲げる機能を含むものでなければならない。

a) 可搬式及び携帯用デバイスの使用は、設計上許可されたものだけに制限すること。

b) 可搬式及び携帯用デバイスへ／からのコード及びデータの転送を、制限すること。

注：ポートの制限／ブロッカー（及びシリコン）は、特定のシステムでは受け入れられうる。

解説

■ 概要

ここでは、システムが可搬式又は携帯用デバイスと接続する場合、デバイスを管理する必要があると述べています。可搬式及び携帯用デバイスとは、持ち運び可能な装置のことです。例えば、USB メモリ、スマートフォン、タブレット、ラップトップなどが該当します。

■ 目的

ここでの目的は、可搬式又は携帯用デバイス経由でマルウェアに感染するリスクを低減することです。デバイスからのマルウェア感染は、デバイス本体だけではなく、システムのセキュリティ機能として保護される必要があります。

■ 対策

ここでの対策として、可搬式及び携帯用デバイスの使用制限及び転送制限の機能となります。具体的には以下のとおりです。

・使用制限

許可されたデバイスのみを接続できるように制限します。

・転送制限

システムとデバイス間のコード及びデータの転送を制限します。

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。以下に補完的対策の一例を示します。

・ポートをブロッカーによりブロックする

ブロッカーとは、コンピュータの USB ポートや LAN 端子等に差し込むことで、そのポ

ートを物理的にブロックする物理的なセキュリティツールです。ブロッカーによりポートをブロックすることにより、可搬式及び携帯用デバイスの使用を防止するため、この機能を補完することができます。

・可搬式及び携帯用デバイスのクリーンアップ

可搬式及び携帯用デバイスを使用する前に、専用のハードウェア等によりマルウェアのスキャン及びクリーンアップすることで、この機能を補完することができます。

■ 適用

以下の場合、この要件は適用となりません。

・可搬式及び携帯用デバイスの使用に対応していない場合

可搬式及び携帯用デバイスの使用に対応していない場合は、本要件は適用されません。

書類審査

■ セキュリティ機能の説明

	10. 可搬式及び携帯用デバイスの使用の管理
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 可搬式及び携帯用デバイスの使用制限及び転送制限の機能
☐	(a) 可搬式及び携帯用デバイスの使用制限
☐	許可されたデバイスが使用できること
☐	(b) 可搬式及び携帯用デバイスの転送制限
☐	デバイスのコード及びデータの転送が制限されていること
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	10. 可搬式及び携帯用デバイスの使用の管理
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) 可搬式及び携帯用デバイスの使用制限及び転送制限の機能の実証試験
☐	(a) 可搬式及び携帯用デバイスの使用制限

☐	次に掲げる項目に適合すること。
☐	i) 許可されたデバイスが使用できること。
☐	ii) 許可されないデバイスが使用できないこと。
☐	(b) 可搬式及び携帯用デバイスの転送制限
☐	デバイスのコード及びデータの転送が制限されていること
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

11. モバイルコード

規則　表 X4.1 中 11	参照　IEC62443-3-3 / SR 2.4

コンピュータシステムは、Java スクリプト、ActiveX 及び PDF のようなモバイルコードの使用を制御するものでなければならない。

解説

■ 概要

ここでは、モバイルコードの使用を制御する必要があると述べています。モバイルコードとは、使用者が明示的にダウンロードやインストールなどの操作を行わなくても、ネットワークを介して他のコンピュータシステムからダウンロードされ自動的に実行されるプログラムのことです。

■ 目的

ここでの目的は、モバイルコードの自動実行によるセキュリティリスクを防止することです。マルウェアの中には、モバイルコードの仕組みを悪用して、コンピュータへの感染、不正な操作、改ざんなどに応用するものがあります。それらを防止するため、モバイルコードを制限する必要があります。

■ 対策

ここでの対策は、モバイルコードの使用を制御する機能となります。具体例として、ブラウザを削除する、ポリシーの設定でモバイルコードの動作を禁止することが挙げられます。

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。

■ 適用

以下の場合、この要件は適用となりません。

・Web アクセス（クライアント）機能がない場合

Windows 等の汎用的なオペレーティングシステム[1]（汎用 OS）を使用しない場合、Web アクセス（クライアント）機能が無い場合が殆どです。Web にアクセスされなければ、モバイルコードが自動的にダウンロードされることはありません。このような場合は、本要

[1] **オペレーティングシステム**　コンピュータシステムを動かす基盤となるソフトウェア。略して、OS。Windows 等一般的に普及している OS を汎用 OS という。

件は適用されません。

書類審査

■ セキュリティ機能の説明

	11. モバイルコード
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
□	(1) モバイルコードの使用を制御する機能
□	(a) モバイルコードの使用を制御できること（例：ブラウザを削除する、ポリシーの設定でモバイルコードの動作を禁止する）
□	(2) 補完的対策
□	(a) 本要件と同じ脅威から保護すること。
□	(b) 本要件と同等の厳しさ，正確さであること。
□	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
□	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	11. モバイルコード
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
□	(1) モバイルコードの使用を制御する機能
□	(a) モバイルコードの使用を制御できること（例：ブラウザを削除する、ポリシーの設定でモバイルコードの動作を禁止する）
□	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

12. セッションロック

規則	参照
表 X4.1 中 12	IEC62443-3-3 / SR 2.5

コンピュータシステムは、設定可能な無操作時間の経過後又は手動によるセッションロックの有効化後に、更なるアクセスを防止することが可能なものでなければならない。

解説

■ 概要

ここでは、自動または手動いずれかの方法によりセッションをロックできる必要があると述べています。**セッション**とは、使用者がシステムにログインしてからログアウトするまでの一連の操作を指します。また、システムを一定時間操作しない場合に、セッションをロックすることを**セッションロック**と言います。

■ 目的

ここでの目的は、無操作時間中にセッションが悪用されるリスクを低減することになります。セッションがロックできない場合、攻撃者にセッションを乗っ取られる可能性があります。この結果、システムが不正に操作されることにより、システムの可用性を損なう可能性があります。

■ 対策

ここでの対策は、自動または手動いずれかのセッションロックの機能となります。

・自動によるセッションロック

無操作時間が設定できることが求められます。なお、船舶の運航に直接影響を及ぼすシステムは、この機能により可用性を損なう可能性があるため、推奨されません。

・手動によるセッションロック

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。

■ 適用

以下の場合、この要件は適用となりません。

・HMI を介したセッションを使用しない場合

例えば、ブラウザ等 HMI を介したセッションを使用しない場合、この要件は適用されま

せん。

書類審査

■ セキュリティ機能の説明

	12. セッションロック
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 自動または手動いずれかのセッションロックの機能
☐	(a) 自動によるセッションロックについては、以下を確認すること：
☐	i) 無操作時間の経過後にセッションがロックされること
☐	ii) 無操作時間が設定できること
☐	(b) 手動によるセッションロックについては、以下を確認すること：
☐	i) 手動によりセッションがロックされること
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	12. セッションロック
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) 自動または手動いずれかのセッションロックの機能の実証試験
☐	(a) 自動によるセッションロックについては、以下を確認すること：
☐	i) 無操作時間の経過後にセッションがロックされること
☐	ii) 無操作時間が設定できること
☐	(b) 手動によるセッションロックについては、以下を確認すること：
☐	i) 手動によりセッションがロックされること
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

13. 監査可能な事象

規則	参照
表 X4.1 中 13	IEC62443-3-3 / SR 2.8

コンピュータシステムは、少なくとも次に掲げる事象について、セキュリティに関連する監査記録を作成するものでなければならない：アクセス制御、オペレーティングシステム[1]の事象、バックアップ及び復元の事象、設定の変更、通信の喪失

解説

■ 概要

ここでは、セキュリティに関する重要な事象の監査記録を作成する必要があると述べています。監査記録とは、セキュリティに関わる重要な事象の記録です。

■ 目的

ここでの目的は、監査する必要がある重要な事象の発生を記録することになります。重要な事象の発生が記録されなければ、監査が適切に実行されず、事象の原因分析が難しくなります。

■ 対策

ここでの対策は、重要な事象の監査記録を作成する機能となります。具体的には、以下の事象について、監査記録を作成する必要があります。

・アクセス制御

コンピュータやネットワークにアクセスできる使用者を制限する機能を指します。ログイン試行の成功及び失敗、アクセス権限の変更などが該当します。これらを記録することにより不正アクセスや権限の乱用を追跡できます。

・オペレーティングシステムの事象

システムの起動及び停止、システムエラー、ソフトウェアの更新及びインストール等 OS に関連する全てのアクティビティを指します。

・バックアップ及び復元の事象

データのバックアップ及び復元に関するアクティビティを記録します。バックアップ及び復元、バックアップの成功及び失敗、バックアップデータの改ざんの試行などが含まれます。

・設定の変更

システムの設定がいつ、どのように、誰によって変更されたかを記録します。これには、

[1] **オペレーティングシステム**　コンピュータシステムを動かす基盤となるソフトウェア。略して、OS。Windows 等一般的に普及している OS を汎用 OS という。

セキュリティ設定、ネットワーク設定及び使用者の権限設定などが含まれます。

・通信の喪失

ネットワーク接続の中断及び喪失、サービス間の通信の中断、システムがネットワークに接続できない事象などを記録します。これにより、ネットワーク攻撃及び接続問題を特定することができます。

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。以下に補完的対策の一例を示します。

・外部の監視システムにより、監査記録を作成する

外部の監視システムが事象の発生を記録することにより、この機能を補完できます。外部の監視システムとは、例えば、機関制御盤（ECC）などが該当します。

■ 適用

この要件は、原則としてすべてのコンピュータシステムに対して適用となります。

書類審査

■ セキュリティ機能の説明

	13. 監査可能な事象
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 重要な事象の監査記録を作成する機能の機能
☐	(a) 次に掲げる事象の監査記録が作成できること。
☐	i) アクセス制御
☐	ii) オペレーティングシステムのイベント
☐	iii) バックアップと復元
☐	iv) 設定変更
☐	v) 通信の喪失
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	13. 監査可能な事象
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) 重要な事象の監査記録を作成する機能の実証試験
☐	(a) 次に掲げる事象の監査記録が作成できることを確認すること。
☐	i) 次に掲げる事象の監査記録が作成できること。
☐	ii) アクセス制御
☐	iii) オペレーティングシステムのイベント
☐	iv) バックアップと復元
☐	v) 設定変更
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

14. 監査用の記憶容量

規則	参照
表 X4.1 中 14	IEC62443-3-3 / SR 2.9

コンピュータシステムは、監査記録[1]の記憶容量を、ログ管理に関する一般に認識された推奨に従って割り当てる機能を提供できるものでなければならない。監査の仕組みは、当該容量を超過する可能性を下げるように実装されなければならない。

解説

■ 概要

ここでは、監査記録の記憶容量をログ管理に関する一般的に認識された推奨に従って割り当てる必要があると述べています。ログ管理に関する一般に認識された推奨とは、例えば NIST[2] SP800-92 があります。

また、監査の仕組みは、当該容量を超過する可能性を下げるように実装する必要があるとも述べています。これは、必要な期間にわたって監査記録を補完できる容量を確保することを指しています。

■ 目的

ここでの目的では、監査に必要な量の監査記録を保管することです。必要なログが十分に確保されていない場合は、セキュリティインシデントの脅威を調査および分析をすることが困難となります。

■ 対策

ここでの対策は、監査記録の記憶容量をログ管理に関する一般的に認識された推奨に従って割り当てる機能及び容量を超過する可能性を下げるような監査の仕組みとなります。具体的には、以下のとおりとなります。

・ログ管理の一般的な推奨事項に基づいて、監査記録の保管容量を確保する

NIST SP800-92 などの一般的な推奨事項が記載された指針や保持ポリシーを考慮に入れ、適切な保管容量を確保する必要があります。

・必要な期間に亘ってログを適切に保管できる容量を確保する

保管容量の計算では、一定期間で生成されるログの量と、その容量をどの程度の期間保管できるかを正確に検討することが重要です。

■ 補完的対策

---

[1] **監査記録**　セキュリティに関わる重要な事象の単一の記録

[2] **NIST**　米国国立標準技術研究所。National Institute of Standards and Technology の略。

この機能を実装できない場合、補完的対策を講じる必要があります。以下に補完的対策の一例を示します。

・リムーバブルメディア等の外部記憶媒体への書き出し機能

十分な保管容量を確保できない場合、保管容量が超過する前に、監査記録をリムーバブルメディアなどの外部記憶媒体へ書き出すことにより、この機能を補完します。この場合、一定期間での書き出しが必要など、書き出し機能の仕様を明記する必要があります。

■ 適用

以下の場合、この要件は適用となりません。

・「13. 監査可能な事象」の機能を補完的対策とする場合、又は同要件が適用外の場合

監査記録を作成する機能を実装していない場合、この要件は適用外となります。詳細について、「13. 監査可能な事象」に詳しく解説しております。

監査可能な事象 P. 86

書類審査

■ セキュリティ機能の説明

	14. 監査用の記憶容量
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 監査記録の記憶容量をログ管理に関する一般的に認識された推奨に従って割り当てる機能
☐	(a) ログ管理の一般的な推奨事項に基づいていること（例：NIST SP800-92）。
☐	(b) 容量を超過する可能性を下げるような監査の仕組みであること。
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	14. 監査用の記憶容量

☐	-1.	本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1)	監査記録の記憶容量をログ管理に関する一般的に認識された推奨に従って割り当てる機能の実証試験
☐		(a) ログ管理の一般的な推奨事項に基づいていること（例：NIST SP800-92）。
☐		(b) 容量を超過する可能性を下げるような監査の仕組みであること。
☐	(2)	補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

15. 監査プロセスの不具合への対応

規則	参照
表 X4.1 中 15	IEC62443-3-3 / SR 2.10

コンピュータシステムは、監査プロセスの不具合発生時に、不可欠なサービス及び機能の喪失を防ぐ機能を提供するものでなければならない。

解説

■ 概要

ここでは、監査プロセスの不具合発生時に、不可欠なサービス及び機能の喪失を防ぐ必要があると述べています。監査プロセスとは、監査記録[1]に関わる処理です。具体的には、監査記録を作成する機能などです。想定される不具合としては、システムのソフトウェアやハードウェアのエラー、監査処理メカニズムの障害、保存容量の超過などが考えられます。また、不可欠なサービス及び機能とは、船舶の運航に重大な影響を及ぼすような機能を指します。つまり、監査記録に関わる処理によりエラーが発生した場合に重要な機能が損なわれない必要があるということです。

■ 目的

ここでの目的は、監査プロセスにより、不可欠なサービス及び機能の喪失するリスクを防止することです。監査プロセスと不可欠なサービス及び機能が一連のプロセスとなっている場合、監査記録に関わる機能の損失により、不可欠な機能の停止を引き起こす可能性があります。

■ 対策

ここでの対策は、監査プロセスの不具合発生時に、不可欠なサービス及び機能の喪失を防ぐ機能となります。例えば、監査に関わる機能と不可欠な機能を分離するなどです。

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。

■ 適用

以下の場合、この要件は適用となりません。

- **「13. 監査可能な事象」の機能を補完的対策とする場合、又は同要件が適用外の場合**
  監査記録を作成する機能を実装していない場合、この要件は適用外となります。詳細に

[1] **監査記録**　セキュリティに関わる重要な事象の記録

ついて、「13. 監査可能な事象」に詳しく解説しております。

監査可能な事象 P. 86

書類審査

■ セキュリティ機能の説明

	15. 監査プロセスへの不具合の対応
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 監査プロセスの不具合発生時に、不可欠なサービス及び機能の喪失を防ぐ機能
☐	(a) 監査プロセスの不具合発生時に、不可欠なサービス及び機能が喪失しないこと（例：監査に関わる機能と不可欠な機能を分離する）
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	15. 監査プロセスへの不具合の対応
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) 監査プロセスの不具合発生時に、不可欠なサービス及び機能の喪失を防ぐ機能の実証試験
☐	(a) 監査プロセスの不具合発生時に、不可欠なサービス及び機能が喪失しないこと（例：監査に関わる機能と不可欠な機能を分離する）
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

16. 日時の記録

規則	参照
表 X4.1 中 16	IEC62443-3-3 / SR 2.11

コンピュータシステムは、監査記録[1]に日時を記録するものでなければならない。

解説

■ 概要

ここでは、監査記録に日時を記録する必要があると述べています。

■ 目的

ここでの目的は、監査が必要となる事象がいつ発生したか等、タイムラインを作成することです。タイムラインが把握できない場合、事象の原因分析が困難になります。

■ 対策

ここでの対策は、日時を記録する機能となります。具体的には、タイムスタンプとなります。タイムスタンプとは、特定のイベントがログとして生成された日時のことです。

タイムスタンプを生成する際には、信頼性を確保するために、時計専用のハードウェア（リアルタイムクロック IC[2]等）やシステム内部のクロック（システムクロック[3]）を利用することが推奨されます。システムクロックを利用する場合、起動後の動作時間をカウントした値を日時に読み替えることで、日時記録とすることが可能ということになります。

なお、タイムスタンプは、他のシステムと同期する必要がありません。

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。

■ 適用

以下の場合、この要件は適用となりません。

・「13. 監査可能な事象」の機能を補完的対策とする場合、又は同要件が適用外の場合

監査記録を作成する機能を実装していない場合、この要件は適用外となります。詳細について、「13. 監査可能な事象」に詳しく解説しております。

---

[1] **監査記録**　セキュリティに関わる重要な事象の単一の記録

[2] **リアルタイムクロック IC**　現在の日付や時刻を保持するための集積回路。バッテリーによってバックアップされており、システムの電源が切断されても時刻を維持する。

[3] **システムクロック**　システムに内蔵されている時計。システムのハードウェアの中で一定の周期で動作するもの（例えば、演算装置）が行った動作回数を基準としている。

書類審査

■ セキュリティ機能の説明

	16. 日時の記録
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 監査記録に日時を記録する機能
☐	(a) 監査記録にタイムスタンプが付与されること（例：リアルタイムクロック IC、システムクロック等）
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	16. 日時の記録
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) 監査記録に日時を記録する機能の実証試験
☐	(a) 監査記録にタイムスタンプが付与されること（例：リアルタイムクロック IC、システムクロック等）
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

17. 通信の完全性

規則	参照
表 X4.1 中 17	IEC62443-3-3 / SR 3.1

コンピュータシステムは、伝送される情報の完全性を保護するものでなければならない。
注）無線ネットワークには、暗号化の仕組みが採用されなければならない。

解説

■ 概要

ここでは、伝送される情報の完全性を保護する必要があると述べています。**完全性**とは、情報が正確で完全であるようにすることです。つまり、情報が改ざんされることなく、元の状態を保持したまま、送信される仕組みが必要ということです。

■ 目的

ここでの目的は、伝送される情報が不当に変更、削除および破壊されるリスクを防止することです。伝送される情報が改ざんされてしまうと、情報の信頼が失われることとなり、運航の安全が脅かされる可能性があります。

■ 対策

ここでの対策は、情報の受信側が情報の改ざんを検証する機能です。具体的には、以下の機能となります。

・受信データと送信データに相違がある場合、送信元にデータの再送を要求する機能
・受信データと送信データとの相違が続いた場合、警報を発する機能

また、無線通信を使用する場合は、強度の高い暗号技術アルゴリズムを採用する必要があります。この理由は、無線通信下ではコンピュータシステムの外部から容易に伝送中の信号を傍受できるためです。暗号化については、「22. 暗号の使用」に詳しく解説しております。

暗号の使用 P. 108

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。

■ 適用

以下の場合、この要件は適用となりません。

・ネットワークや他のコンピュータシステムに接続しない場合

ネットワークや他のコンピュータシステムに接続しない場合、本要件は適用されません。

書類審査

■ セキュリティ機能の説明

	17. 通信の完全性
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 伝送される情報の完全性を保護する機能
☐	(a) 次に掲げる機能が実装されていること
☐	i) 受信データと送信データに相違がある場合、送信元にデータの再送を要求する機能
☐	ii) 受信データと送信データの相違が続いた場合、警報を発する機能
☐	(b) 無線通信を行う場合、伝送される情報に暗号技術の仕組みが使われていること
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	17. 通信の完全性
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) 伝送される情報の完全性を保護する機能の実証試験
☐	(a) 次に掲げる機能があること
☐	i) 受信データと送信データに相違がある場合、送信元にデータの再送を要求する機能
☐	ii) 受信データと送信データの相違が続いた場合、警報を発する機能
☐	(b) 無線通信を行う場合、伝送される情報に暗号技術の仕組みが使われていること
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

18. 悪意のあるコードからの保護

規則	参照
表 X4.1 中 18	IEC62443-3-3 / SR 3.2

コンピュータシステムは、悪意のあるコードや不正なソフトウェアによる影響を防止、検知及び低減するための適切な保護手段を実行する機能を提供できるものでなければならない。また、保護の仕組みを更新する機能を有するものでなければならない。

解説

■ 概要

ここでは、悪意のあるコードや不正なソフトウェアによる影響を防止、検知及び低減するための適切な保護手段を実行する必要があると述べています。悪意のあるコードや不正なソフトウェアとは、システムを意図的に不正かつ有害に動作させることを目的として作られたプログラムまたはソフトウェアであり、通称**マルウェア**と呼ばれます。

■ 目的

ここでの目的は、マルウェアによるリスクを最小化することです。

■ 対策

ここでの対策は、マルウェアによる影響を防止、検知及び低減するための適切な保護手段を実行する機能となります。具体的には、以下のとおりです。

・マルウェアによる影響を防止するための機能

マルウェアがシステムへ侵入することを防ぐ手段です。具体的には、アプリケーションのホワイトリスト制限、リムーバブルメディアの実行制限、サンドボックス機能等が該当します。

・マルウェアによる影響を検知するための機能

マルウェアがシステム内に侵入し感染したかどうかをチェックする手段です。具体的には、侵入検知システム(IDS)、マルウェアスキャンやマルウェア対策ソフト、エンドポイントセキュリティソフトによる検知等が該当します。

・マルウェアによる影響を低減するための機能

マルウェアが発生した場合にその影響を最小限に抑制する手段です。具体的にはファイルの削除、感染端末の隔離等が該当します。

また、これらの対策は、導入している仕組みが有効に機能するように、定期的に更新される必要があります

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。以下に補完的対策の一例を示します。

・外部のセキュリティデバイス

ファイアウォール等の外部のセキュリティデバイスにより、マルウェアを防止・検知及び低減することで、この機能を補完できます。

■ 適用

以下の場合、この要件は適用となりません。

・汎用 OS[1] を使用しない場合

マルウェアは、通常 Windows などの汎用 OS を対象に作られています。したがって、汎用 OS を使用しない独自の OS が搭載されたコンピュータシステムは、マルウェアが存在しない可能性が高く、本要件は適用されません。

書類審査

■ セキュリティ機能の説明

	18. 悪意のあるコードからの保護
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
□	(1) 悪意のあるコードや不正なソフトウェアによる影響を防止、検知及び低減するための適切な保護手段を実行する機能
□	(a) 次に掲げる機能が実装されていること
□	i) マルウェアによる影響を防止するための機能（例：アプリケーションのホワイトリスト制限、リムーバブルメディアの実行制限、サンドボックス機能）
□	ii) マルウェアによる影響を検知するための機能があること（例：侵入検知システム(IDS)、マルウェアスキャンやマルウェア対策ソフト、エンドポイントセキュリティソフトによる検知）
□	iii) マルウェアによる影響を低減するための機能があること（例：ファイルの削除、感染端末の隔離）
□	(2) 補完的対策
□	(a) 本要件と同じ脅威から保護すること。
□	(b) 本要件と同等の厳しさ，正確さであること。
□	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
□	(d) 新たなセキュリティリスクを発生させないこと。

[1] **汎用 OS** 汎用的なオペレーティングシステム。例えば、Windows 等。

立会検査

■ セキュリティ機能試験

	18. 悪意のあるコードからの保護
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
□	(1) 伝送される情報の完全性を保護する機能の実証試験
□	(a) 次に掲げる機能が実装されていること
□	i) マルウェアによる影響を防止するための機能（例：アプリケーションのホワイトリスト制限、リムーバブルメディアの実行制限、サンドボックス機能）
□	ii) マルウェアによる影響を検知するための機能があること（例：侵入検知システム(IDS)、マルウェアスキャンやマルウェア対策ソフト、エンドポイントセキュリティソフトによる検知）
□	iii) マルウェアによる影響を低減するための機能があること（例：ファイルの削除、感染端末の隔離）
□	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

19. セキュリティ機能の検証

規則	参照
表 X4.1 中 19	IEC62443-3-3 / SR 3.3

コンピュータシステムは、セキュリティ機能のあるべき動作の検証をサポートし、また、保守中に発生した異常を報告する機能を提供するものでなければならない。

解説

■ 概要

ここでは、セキュリティ機能のあるべき動作の検証をサポートすることが必要と述べています。ここでいうセキュリティ機能とは、X 編 4 章で要求されるセキュリティ機能のなかで、実装されているものすべてです。つまり、実装されているセキュリティ機能の動作が正常に実行していることを確認できるようにすることが必要ということです。

また、保守中に発生した異常を報告する必要もあります。

■ 目的

ここでの目的は、X 編 4 章（UR E27）で要求されるセキュリティ機能をシステムに実装し、その機能が要求を満たすための動作が正常に実行していることを確認することです。適切な試験が行われない場合、必要な時にセキュリティ機能が機能しない可能性があります。さらに、保守中に異常が発生した場合でも、それが報告されることにより、保守への信頼性が向上します。

■ 対策

ここでの対策は、セキュリティ機能のあるべき動作の検証をサポートする機能、および保守中に発生した異常を報告する機能となります。具体的には、以下のとおりです。

・セキュリティ機能の動作検証を行う機能

実装されたセキュリティ機能の動作を検証する機能です。例えば、人を認証する機能では、不正なアカウントによりログインが試行された場合、そのログインが拒否される等が該当します。

・保守中に異常を報告する機能

メンテナンス中に起こる可能性のある問題を通知する機能です。例えば、ウイルス対策ソフトを導入している場合、ウイルスやマルウェアの識別コードやパターンの更新に失敗した時にメッセージが出力される等が該当します。

補足　これらの機能は、所有者[1]がシステムを保守する際に利用されます。その利用をサポートするため、供給者は「コンピュータシステムの保守及び検証のための計画」に、これらの機能を確認する方法についての指示を含める必要があります

コンピュータシステムの保守及び検証のための計画　P. 32

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。

■ 適用

この要件は、原則としてすべてのコンピュータシステムに対して適用となります。

書類審査

■ セキュリティ機能の説明

	19.　セキュリティ機能の検証
☐	-1.　本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1)　セキュリティ機能のあるべき動作の検証をサポートし、また、保守中に発生した異常を報告する機能
☐	(a)　セキュリティ機能の動作検証を行う機能
☐	実装されたセキュリティ機能の動作が検証できること
☐	(b)　保守中に発生した異常を報告する機能
☐	保守中に検知した異常が報告されること（例：ウイルス対策ソフトを導入している場合、ウイルスやマルウェアの識別コードやパターンの更新に失敗した時にメッセージが出力される等）
☐	(2)　補完的対策
☐	(a)　本要件と同じ脅威から保護すること。
☐	(b)　本要件と同等の厳しさ，正確さであること。
☐	(c)　他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d)　新たなセキュリティリスクを発生させないこと。

立会検査

[1] **所有者**　建造段階においては、船舶を発注する組織又は個人であり、就航後においては、船舶を所有、又は管理する組織のことをいう。一般的に、建造中は造船所、建造後は船主となる。

■ セキュリティ機能試験

	19. セキュリティ機能の検証
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) セキュリティ機能のあるべき動作の検証をサポートし、また、保守中に発生した異常を報告する機能
☐	(a) セキュリティ機能の動作検証を行う機能
☐	i) 実装されたセキュリティ機能の動作が検証できること
☐	(b) 保守中に発生した異常を報告する機能
☐	i) 保守中に検知した異常が報告されること（例：ウイルス対策ソフトを導入している場合、ウイルスやマルウェアの識別コードやパターンの更新に失敗した時にメッセージが出力される等）
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

20. あらかじめ決定した出力

規則	参照
表 X4.1 中 20	IEC62443-3-3 / SR 3.6

コンピュータシステムは、攻撃により通常の動作を維持できなくなった場合に、出力をあらかじめ指定した状態に設定する機能を提供するものでなければならない。あらかじめ指定した状態とは、次に掲げるものとすることができる。

・非使用時の状態
・最後の既知の値、または
・固定値

解説

■ 概要

ここでは、攻撃により通常の動作を維持できなくなった場合に、出力をあらかじめ指定した状態に設定する必要があると述べています。あらかじめ指定した状態とは、以下のとおりです。

指定した状態	説明
非使用時の状態	システムの電源が切れている状態です。
最後の正常値	システムが攻撃される直前に出力していた値です。
固定値	システムがあらかじめ設定しておいた特定の値です。 この値は所有者[1]等によって決められる値となります。

■ 目的

この機能の目的は、システムが攻撃によって機能不全に陥ったとしても、特定の状態を保持することで、システム全体の安全性を高め、かつ問題の解決を容易にすることです。例として、船用プラントを制御するシステムが攻撃された場合を想定します。もしシステムが攻撃により予期せぬ出力が発生した場合、それが機器の誤作動を引き起こし、正常な運航ができなくなる可能性があります。このような場合、システムを停止させたり、安全な動作範囲に戻したりするなどの、事前に定められた状態へ移行することで、安全の確保が可能となります。

■ 対策

[1] **所有者**　建造段階においては、船舶を発注する組織又は個人であり、就航後においては、船舶を所有、又は管理する組織のことをいう。一般的に、建造中は造船所、建造後は船主となる。

ここでの対策は、出力をあらかじめ指定した状態に設定する機能となります。この機能により、上述された指定した状態に変更できる必要があります。

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。

■ 適用

この要件は、原則としてすべてのコンピュータシステムに対して適用となります。

書類審査

■ セキュリティ機能の説明

c	20. あらかじめ決定した出力
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 出力をあらかじめ指定した状態に設定する機能
☐	出力について、少なくとも次に掲げるいずれかの状態へ変更できること
☐	(a) 非使用時の状態
☐	(b) 最後の正常値、または固定値
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	20. あらかじめ決定した出力
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) 出力をあらかじめ指定した状態に設定する機能の詳細
☐	出力について、少なくとも次に掲げるいずれかの状態へ変更できること
☐	(a) 非使用時の状態
☐	(b) 最後の正常値、または固定値
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

21. 情報の機密性

規則	参照
表 X4.1 中 21	IEC62443-3-3 / SR 4.1

コンピュータシステムは、読取りに関して明示的な承認が求められる情報について、保管時であるか伝送中であるかにかかわらず、機密性を保護する機能を提供するものでなければならない。

注：無線ネットワークの場合、伝送中のすべての情報の機密性を保護するために、暗号化の仕組みが採用されなければならない。

解説

■ 概要

ここでは、読取りに関して明示的な承認が求められる情報について、保管時であるか伝送中であるかにかかわらず、機密性を保護する必要があると述べています。

読取りとは、データベースやファイルから情報を取得することです。例えば、インターネットでウェブページを閲覧する時、ブラウザがウェブサーバからデータを読み取ることでページを表示しています。

また、明示的な承認が求められる情報とは、許可された人のみアクセスが可能となる情報です。つまり、取得に許可が必要な情報は、機密性を確保する必要があるということです。

■ 目的

ここでの目的は、許可された人のみアクセスが可能となる情報の機密性を確保することです。情報の機密性が損なわれると、情報漏えいや情報の不正利用等につながる可能性があります。

■ 対策

ここでの対策は、読取りに関して明示的な承認が求められる情報の機密性を保護する機能となります。具体的には、以下のとおりです。

・保管時に情報の機密性を保護する機能

使用者の認証及び認可などのアクセス権に関わる機能や情報を暗号化する機能などを指します。

・伝送中に情報の機密性を保護する機能

通信を暗号化する機能などを指します。また、一対一での有線接続は、伝送中の機密性の確保につながります。

また、無線通信を使用する場合は、伝送中のデータにアクセスされる可能性があること

から、暗号化の仕組みを採用する必要があります。暗号化については、「22. 暗号の使用」に詳しく解説しております。

暗号の使用 P. 108

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。

■ 適用

この要件は、原則としてすべてのコンピュータシステムに対して適用となります。なお、情報が伝送されない場合は、伝送中における情報の機密性は適用外となります。

書類審査

■ セキュリティ機能の説明

	21. 情報の機密性
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 読取りに関して明示的な承認が求められる情報について、保管時であるか伝送中であるかにかかわらず、機密性を保護する機能
☐	(a) 次に掲げる機能を確認すること
☐	i) 保管時に情報の機密性を保護する機能
☐	ii) 伝送中に情報の機密性を保護する機能
☐	(b) 無線通信を使用する場合、のすべての情報の機密性を保護するために、暗号化の仕組みが採用されていること。
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

この要件は、書類審査にて確認しますので、立会検査は不要となります。

22. 暗号の使用

規則	参照
表 X4.1 中 22	IEC62443-3-3 / SR 4.3

暗号を使用する場合、コンピュータシステムは一般に受け入れられるセキュリティに関する業界の慣行及び推奨に従って、暗号アルゴリズム、鍵の長さ及び仕組みを使用するものでなければならない。

解説

■ 概要

ここでは、推奨された暗号アルゴリズム、鍵の長さ及び仕組みを使用する必要があると述べています。暗号アルゴリズム、鍵の長さ及び仕組みについては、以下のとおりです。

用語	説明
暗号アルゴリズム	データを暗号化および復号化（元に戻す）したり、ハッシュ化したりする手順や規則を指します。
鍵の長さ	鍵を構成するビット数のことです。ビット数が多いほど、鍵の組み合わせが増えて、暗号の強度が高くなります。
鍵の仕組み	鍵がどのように生成され、管理されるかです。管理とは、例えば、定期的な鍵の変更、鍵の破壊、鍵の配布及び暗号鍵のバックアップなどがあります。

■ 目的

ここでの目的は、暗号技術を活用し情報の完全性及び機密性を確保することです。

■ 対策

ここでの対策は、一般に受け入れられるセキュリティに関する業界の慣行及び推奨に従った暗号技術を採用することとなります。「一般に受け入れられるセキュリティに関する業界の慣行及び推奨」は、例えば以下のとおりです。

- **ISO/IEC 19790**
- **NIST**[1] **SP800-57**
- **NIST FIPS14**
- **「電子政府における調達のために参照すべき暗号のリスト」**

[1] **NIST** 米国国立標準技術研究所。National Institute of Standards and Technology の略。

https://www.cryptrec.go.jp/list.html

・「暗号鍵管理システム設計指針（基本編）」

https://www.ipa.go.jp/security/crypto/guideline/ckms.html

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。

■ 適用

以下の場合、この要件は適用となりません。

・暗号技術を使用してしない場合

暗号技術を使用していない場合は、この要件の適用外となります。

書類審査

■ セキュリティ機能の説明

	22. 暗号の使用
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの仕組み又は対策を設けること。
☐	(1) 一般に受け入れられるセキュリティに関する業界の慣行及び推奨に従って、暗号アルゴリズム、鍵の長さ及び仕組み
☐	次に掲げるものが、一般に受け入れられるセキュリティに関する業界の慣行及び推奨に従っていること。
☐	(a) 暗号アルゴリズム
☐	(b) 鍵の長さ
☐	(c) 鍵の仕組み
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

この要件は、書類審査にて確認しますので、立会検査は不要となります。

23. 監査ログへのアクセス

規則	参照
表 X4.1 中 23	IEC62443-3-3 / SR 6.1

コンピュータシステムは、権限を有する人及び／又はツールによる読取り専用での監査ログへのアクセスの機能を提供するものでなければならない。

解説

■ 概要

ここでは、権限を有する人及び／又はツールが監査ログへ読取り専用でアクセスできる必要があると述べています。権限を有する人とは、監査ログの閲覧を認可された人であり、例えばセキュリティ監視者を指します。一方、権限を有するツールとは、この機能の使用を認可されたプログラムです。例えば、SIEM[1]と呼ばれるセキュリティ関連のイベントや警告を監視および分析するためのソフトウェアが該当します。また、監査ログとは、監査記録[2]を時系列に収集したものです。これは、複数の監査記録をまとめたものとして捉えることができます。

■ 目的

ここでの目的は、監査ログが改ざんされるリスクを低減することです。

■ 対策

ここでの対策は、閲覧権限を有する人及び／又はツールが監査ログに読取り専用でアクセスする機能となります。

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。

■ 適用

・「13. 監査可能な事象」の機能を補完的対策とする場合、又は同要件が適用外の場合

監査記録を作成する機能を実装していない場合、この要件は適用外となります。詳細について、「13. 監査可能な事象」に詳しく解説しております。

監査可能な事象 P. 86

書類審査

[1] **SIEM** セキュリティ情報イベント管理。Security Information and Event Management の略。

[2] **監査記録** セキュリティに関わる重要な事象の記録

■ セキュリティ機能の説明

	23. 監査ログへのアクセス
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
□	(1) 閲覧権限を有する人及び／又はツールによる読取り専用での監査ログへのアクセスの機能
□	(a) 閲覧権限を有する人及び／又はツールが監査ログへアクセスできること
□	(b) 閲覧権限を有する人がログの内容を変更できないこと。
□	(2) 補完的対策
□	(a) 本要件と同じ脅威から保護すること。
□	(b) 本要件と同等の厳しさ，正確さであること。
□	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
□	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	23. 監査ログへのアクセス
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
□	(1) 出力をあらかじめ指定した状態に設定する機能
□	(a) 次に掲げる項目に適合すること。
□	i) 権限を有する人及び／又はツールが監査ログへアクセスできること。
□	ii) 権限を有しない人及び／又はツールが監査ログへアクセスできないこと。
□	(b) 閲覧権限を有する人がログの内容を変更できないこと。
□	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

24. サービス拒否攻撃からの保護

規則	参照
表 X4.1 中 24	IEC62443-3-3 / SR 7.1

コンピュータシステムは、DoS[1]事象発生中にも、不可欠な機能を維持するための最小限の機能を提供するものでなければならない。

注：DoS 事象時にコンピュータシステムが縮退モードで動作することは許容されるが、危険な状況を引き起こす可能性のある方法で故障してはならない。例えば、ネットワークの容量が過剰に使用される及びコンピュータのリソースが過剰に消費される等、過負荷に基づく DoS 事象を考慮すべきである。

解説

■ 概要

ここでは、DoS 事象発生中にも、不可欠な機能を維持する必要があると述べています。DoS とは、Denial of Service の略であり、サーバ等に対して大量の情報を送信することで、システムが正常に動作しなくなる攻撃手法です。

■ 目的

ここでの目的は、DoS 攻撃によって不可欠な機能が停止されるリスクを防止することです。この攻撃により、システムの停止など可用性が損なわれる可能性があります。そのため、必要不可欠な機能を維持するための対策が求められます。

■ 対策

ここでの対策は、DoS 事象発生中にも、不可欠な機能を維持するための最小限の機能を提供することとなります。具体的には以下のとおりです。

・通信処理プロセスの優先順位を低くする
・アクセス可能な IP アドレスに制限をかける

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。以下に補完的対策の一例を示します。

[1] **DoS 攻撃**　Denial of Service（サービス妨害）の略。中でも、DDoS（分散型サービス妨害）攻撃は、複数のコンピュータやデバイスを利用し、ウェブサイトやサーバに大量のトラフィックを送ることで、システムをより大規模に妨害する。

・外部のセキュリティ機器により、アクセス可能な IP アドレスに制限をかける

外部の境界保護デバイス（ファイアウォール等）により、アクセス可能な IP アドレスに制限をかけることで、この機能を補完することができます。

■ 適用

この要件は、原則としてすべてのコンピュータシステムに対して適用となります。

書類審査

■ セキュリティ機能の説明

	24. サービス拒否攻撃からの保護
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの仕組み又は対策を設けること。
□	(1) DoS 事象発生中にも、不可欠な機能を維持するための最小限の機能
□	DoS 事象中に、不可欠な機能が維持されていること（例：通信処理プロセスの優先順位を低くする等）
□	(2) 補完的対策
□	(a) 本要件と同じ脅威から保護すること。
□	(b) 本要件と同等の厳しさ，正確さであること。
□	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
□	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	24. サービス拒否攻撃からの保護
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
□	(1) DoS 事象発生中にも、不可欠な機能を維持するための最小限の機能
□	DoS 事象中に、不可欠な機能が維持されていること（例：DoS 攻撃のシミュレーション試験の結果確認）
□	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

25. リソースの管理

規則	参照
表 X4.1 中 25	IEC62443-3-3 / SR 7.2

コンピュータシステムは、リソースを使い果たさないように、セキュリティ機能によるリソースの利用を制限する機能を提供するものでなければならない。

解説

■ 概要

ここでは、セキュリティ機能によるリソースの利用を制限する必要があると述べています。リソースとは、システムが利用できる物理的または論理的な資源を指します。具体的には、CPU 処理時間、プロセス使用メモリ、ストレージ使用容量およびネットワーク帯域などが挙げられます。

■ 目的

ここでの目的は、セキュリティ機能によるリソースの不足を防ぐことです。リソースの不足について、原因となるセキュリティ機能および想定される事象の一例は、以下のとおりです。

原因となるセキュリティ機能	想定される事象
ウイルス対策ソフトのウイルススキャン	CPU の処理速度が低下する
	メモリの空き容量が不足する
セキュリティログの長期保存	ハードディスクの容量が不足する

■ 対策

ここでの対策は、セキュリティ機能によるリソースの利用を制限する機能です。リソース不足の原因となるセキュリティ機能又は想定される事象に対して、リソースを不足させないための機能を実装する必要があります。例えば、以下のような対策が考えられます。

原因となるセキュリティ機能、又は想定される事象	対策
ウイルス対策ソフトのウイルススキャン	システムの稼働時間外でスキャンする。
	リソースの空き容量が一定の値を下回った場合に、スキャンを停止する。
セキュリティログの長期保存	ログを書き出す際に残存容量を確認し、不足し

	そうな場合は警報を発する。
	リングバッファ方式[1]に変更する。
ネットワーク帯域の圧迫	帯域制御などにより、通信量を制御する。

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。以下に補完的対策の一例を示します。

・十分なリソースを確保する

セキュリティ機能によるリソースの不足が生じないように、十分なリソースを確保することで、この機能を補完できます。この場合、十分なリソースである根拠を示す必要があります。

■ 適用

この要件は、原則としてすべてのコンピュータシステムに対して適用となります。

書類審査

■ セキュリティ機能の説明

	25. リソースの管理
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) リソースを使い果たさないように、セキュリティ機能によるリソースの利用を制限する機能
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	25. リソースの管理

[1] **リングバッファ方式** 一時的にデータを保存するバッファ領域において，循環的に利用されるデータ保存方式。古いデータから順に上書きされる。

☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) リソースを使い果たさないように、セキュリティ機能によるリソースの利用を制限する機能の実証試験
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

26. システムのバックアップ

規則	参照
表 X4.1 中 26	IEC62443-3-3 / SR 7.3

コンピュータシステムは、通常の運用に影響することなく、重要なファイルの識別及び場所特定並びに使用者レベル及びシステムレベルでの情報（システム状態に関する情報を含む）のバックアップ[1]実施をサポートするものでなければならない。

解説

■ 概要

ここでは、システムのバックアップについて、以下 2 点が必要であると述べています。

・重要なファイルをバックアップする
・バックアップは通常の運用に影響しない

■ 目的

ここでの目的は、復旧すべき重要なファイルを確実にバックアップすることです。

■ 対策

ここでの対策は、復旧すべき重要なファイルをバックアップする機能となります。復旧すべき重要なファイルについては、システムによって決定されるべきです。それらは、通常の運用に影響しないようにバックアップされる必要があります。

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。以下に補完的対策の一例を示します。

・予備品と交換する

予備品へ交換することで、この機能を補完できます。この場合、予備品は元のシステムと同じ設定を持っていることが重要です。予備品には、システムそのものの他、CD や DVD などのインストールディスクが該当します。

■ 適用

以下の場合、この要件は適用となりません。

・バックアップをとる必要がない場合

[1] **バックアップ**　システムに何らかの障害が発生した場合に備えて、データを別の場所にコピーすること。

バックアップの目的は、攻撃者によってプログラムやデータのファイルが書き換えられることにより、システムがダウンした場合に、復旧することです。したがって、プログラムを書き換えできない場合は、バックアップは不要となります。プログラムを書き換えできないとは、ハードウェアにプログラムが直接書き込まれている場合のことであり、例えばハードウェアにプログラムが直接書かれていて、専用の治具を物理的にハードウェアに接続しない限りプログラムを書き換えられない場合などが該当します。

書類審査

■ セキュリティ機能の説明

	26. システムのバックアップ
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
□	(1) 復旧すべき重要なファイルをバックアップする機能
□	(a) システムの復旧に必要となるデータがバックアップされること
□	(b) 通常の運用に影響しないこと
□	(2) 補完的対策
□	(a) 本要件と同じ脅威から保護すること。
□	(b) 本要件と同等の厳しさ，正確さであること。
□	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
□	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

c	26. システムのバックアップ
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
□	(1) 復旧すべき重要なファイルをバックアップする機能の実証試験 システムの復旧に必要となるデータがバックアップされること
□	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

27. システムの復旧及び再構成

規則	参照
表 X4.1 中 27	IEC62443-3-3 / SR 7.4

コンピュータシステムは、混乱又は故障の後、既知の保護された状態に復旧及び再構成される機能を提供するものでなければならない。

解説

■ 概要

ここでは、サイバーインシデントによる混乱又は故障の後、既知の保護された状態に復旧及び再構成される必要があると述べています。サイバーインシデントとは、サイバー攻撃によって、コンピュータシステム等に悪影響を及ぼす事象です。これには、不正アクセス、情報の悪用や改ざん、破壊、不適切な開示が含まれます。

■ 目的

ここでの目的は、サイバーインシデントが発生した後、以前の状態へ素早く復旧及び再構成することです。

■ 対策

ここでの対策は、サイバーインシデントによる混乱又は故障の後、既知の保護された状態に復旧及び再構成される機能となります。具体的には、以下のとおりです。

・リカバリ機能

リカバリ機能とは、システムやアプリケーションが故障や障害から復旧するプロセス全般を指します。リカバリ機能の考慮すべき要素は以下のとおりです。

・システムパラメータがデフォルト[1]又は安全な値であること
・セキュリティに関する重要なパッチ[2]が再インストールされること
・セキュリティに関する設定が再確認、再設定されていること
・システム文書及び操作手順が使用可能な状態であること
・アプリケーション及びシステムソフトウェアが安全な設定で再インストールされること
・バックアップデータから情報が復元されていること

[1] **デフォルト**　システムが出荷時に設定されている標準値、状態、動作条件。
[2] **パッチ**　システムの脆弱性やセキュリティ上の欠陥を修正するためのプログラム。

補足　既知の保護された状態への復旧及び再構成について、パッチやアプリケーションの再インストールやセキュリティ設定の再設定等、セキュリティ機能のみにより達成することは難しいものもあります。その場合は、既知の保護された状態へ戻すための手順書にその対応方法を明記いただくことになります。この手順書は、「就航後のインシデント対応とリカバリープランをサポートする情報」として、本会への提出が求められる参考資料となります。立会検査では、この資料に明示された方法に従って、システムが既知の保護された状態に復旧及び再構成できることを確認します。この資料の詳細は、「就航後のインシデント対応とリカバリープランをサポートする情報」に詳しく解説しております。

就航後のインシデント対応とリカバリープランをサポートする情報　P. 33

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。以下に補完的対策の一例を示します。

・予備品と交換することにより、インシデント発生後即座に既知の保護された状態に回復・再設定する

予め用意した予備品へ交換することで、この機能を補完できます。この場合は、先に述べた「就航後のインシデント対応とリカバリープランをサポートする情報」に予備品への交換手順を含める必要があります。

■ 適用

この要件は、原則としてすべてのコンピュータシステムに対して適用となります。

書類審査

■ セキュリティ機能の説明

	27.　システムの復旧及び再構成
☐	-1.　本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1)　混乱又は故障の後、既知の保護された状態に復旧及び再構成される機能 次に掲げる事象を達成する機能であること。なお、この機能によって、すべて事象を達成する必要はない。
☐	(a)　システムパラメータがデフォルト又は安全な値であること
☐	(b)　セキュリティに関する重要なパッチが再インストールされること
☐	(c)　セキュリティに関する設定が再確認、再設定されていること
☐	(d)　システム文書及び操作手順が使用可能な状態であること

☐	(e) アプリケーション及びシステムソフトウェアが安全な設定で再インストールされること
☐	(f) バックアップデータから情報が復元されていること
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	27. システムの復旧及び再構成
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) 復旧すべき重要なファイルをバックアップする機能の実証試験 「就航後のインシデント対応とリカバリープランをサポートする情報」に明示された方法に従って、システムが既知の保護された状態に復旧及び再構成できること。
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

28. 代替電源

規則	参照
表 X4.1 中 28	IEC62443-3-3 / SR 7.5

既存のセキュリティ状態又は文書化された縮退モードに影響することなく、代替電源へ及び代替電源から切り替える機能を提供するものでなければならない。

解説

■ 概要

ここでは、代替電源について、以下 2 点が必要であることを述べています。

- 代替電源へ切り替える、および代替電源から切り戻す
- 既存のセキュリティ状態や文書化された縮退モードに影響しない

縮退モードとは、システムに異常が発生した際、性能や機能を制限する、又は異常箇所を切り離すなどによって、不完全ながらもシステム本来の機能を継続させるモードです。

■ 目的

ここでの目的は、一時的に電源が喪失された場合においても、システムのセキュリティを確保することです。代替電源へ及び代替電源から切り替わる際、一定時間電源の喪失が発生します。この際、電源喪失による影響が、システムのセキュリティ状態や機能等に及ばない必要があります。

■ 対策

ここでの対策は、既存のセキュリティ状態又は文書化された縮退モードに影響することなく、代替電源へ及び代替電源から切り替える機能となります。具体的には、電源喪失時にセキュリティ機能が喪失することを防ぐように、内蔵のバッテリーや蓄電池などにより、給電が途切れない仕様とすることが挙げられます。

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。以下に補完的対策の一例を示します。

・コンピュータシステムを二重化した上で、一方を代替電源から供給する

コンピュータシステムを二重化することで、この機能を補完することができます。

■ 適用

この要件は、原則としてすべてのコンピュータシステムに対して適用となります。

書類審査

■ セキュリティ機能の説明

	28. 代替電源
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 既存のセキュリティ状態又は文書化された縮退モードに影響することなく、代替電源へ及び代替電源から切り替える機能
☐	次に掲げる状態に影響することなく、代替電源へ及び代替電源から切り替えること
☐	(a) 既存のセキュリティ状態
☐	(b) 文書化された縮退モード
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	28. 代替電源
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) 既存のセキュリティ状態又は文書化された縮退モードに影響することなく、代替電源へ及び代替電源から切り替える機能の実証試験
☐	次に掲げる状態に影響することなく、代替電源へ及び代替電源から切り替えること
☐	(a) 既存のセキュリティ状態
☐	(b) 文書化された縮退モード
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

29. ネットワーク及びセキュリティ構成設定

規則	参照
表 X4.1 中 29	IEC62443-3-3 / SR 7.6

コンピュータシステムのトラフィック[1]は、供給者によって提供される指針にて推奨されるネットワーク及びセキュリティ構成に従って設定される機能を提供するものでなければならない。コンピュータシステムは、現在用いられているネットワーク及びセキュリティ構成の設定へのインターフェースを提供するものでなければならない。

解説

■ 概要

ここでは、コンピュータシステムのトラフィックは供給者によって提供される指針にて推奨されるネットワーク及びセキュリティ構成に従って設定される機能を実装する必要があると述べています。供給者によって提供される指針とは、提出資料のひとつである「セキュリティ構成指針」を指します。

■ 目的

ここでの目的は、供給者が推奨するネットワークやセキュリティ構成に設定することです。設定ミスや DoS 攻撃などによってシステムの可用性が阻害される場合があります。この場合に、供給者が意図するネットワーク及びセキュリティ構成に修正される必要があります。

■ 対策

ここでの対策は、供給者によって提供される指針にて推奨されるネットワーク及びセキュリティ構成に従って設定できる機能（パラメータの設定等）となります。具体的には、以下のとおりです。

・ネットワーク構成を設定する機能

IP アドレス[2]、サブネットマスク[3]を設定する機能となります。

・セキュリティ構成を設定する機能

セキュリティ構成とは、コンピュータシステムに実装されるセキュリティ機能などに関するパラメータ設定機能などが該当します。

---

[1] **トラフィック**　ネットワークを流れる情報及びその量。

[2] **IP アドレス**　ネットワーク上の住所。十進数 4 つ（例「198.51.100.10」）で表し、ネットワーク上で通信する相手を識別するために用いる値。

[3] **サブネットマスク**　IP アドレスのうち、どの値がネットワーク部、ホスト部を指すかを示す値。ネットワークを細分化（サブネット化）する時などに変更する。

補足　この機能は、システムの保守時において、セキュリティを強化する際にも利用されます。その際、セキュア開発ライフサイクルによって作成された「セキュリティ強化指針」が、セキュリティの強化をサポートします。「セキュリティ強化指針」は、以下にて詳しく解説しております。

セキュリティ強化指針　P. 168

また、セキュリティ構成を設定する機能について、セキュリティ機能が推奨設定であること、デフォルト値であることを立会試験により確認します。推奨設定及びデフォルト値は「セキュリティ構成指針」に含まれる必要があります。「セキュリティ構成指針」については、以下にて詳しく解説しております。

セキュリティ構成指針　P. 26

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。

■ 適用

この要件は、原則としてすべてのコンピュータシステムに対して適用となります。

書類審査

■ セキュリティ機能の説明

	29.　ネットワーク及びセキュリティ構成設定
☐	-1.　本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1)　供給者によって提供される指針にて推奨されるネットワーク及びセキュリティ構成に従って設定される機能
☐	次に掲げるものを設定できること
☐	(a)　ネットワーク構成
☐	(b)　セキュリティ構成
☐	(2)　補完的対策
☐	(a)　本要件と同じ脅威から保護すること。
☐	(b)　本要件と同等の厳しさ，正確さであること。
☐	(c)　他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d)　新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	29. ネットワーク及びセキュリティ構成設定
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) 供給者によって提供される指針にて推奨されるネットワーク及びセキュリティ構成に従って設定される機能
☐	次に掲げるものを設定できること
☐	(a) ネットワーク構成
☐	(b) セキュリティ構成
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

30. 最小限の機能性

規則	参照
表 X4.1 中 30	IEC62443-3-3 / SR 7.7

次に掲げるもののインストール、可用性及びアクセス権は、システムが提供する機能の厳格な要求に限られなければならない。

- オペレーティングシステム[1]ソフトウェアのコンポーネント[2]、プロセス及びサービス
- ネットワークサービス、ポート[3]、プロトコル[4]、ルート[5]及びホスト[6]へのアクセス並びにすべてのソフトウェア

解説

■ 概要

ここでは、システムの機能に不可欠でないものは、インストールしない、利用可能な状態としないおよびアクセス可能な状態としない必要があると述べています。

■ 目的

ここでの目的は、不要な機能を無効化し、システムの機能を最小限にすることで、セキュリティホールの発生を抑制することです。システムに実装される機能は、多ければ多いほど、セキュリティホールが生じやすく、サイバー攻撃を受ける可能性があります。

■ 対策

ここでの対策は、システムの機能、設定情報を最小限にすることです。具体的には、以下のサービスや機能に対して、必要最低限とする必要があります。

・オペレーティングシステムソフトウェアのコンポーネント、プロセス及びサービス

・ネットワークサービス、ポート、プロトコル、ルート及びホストへのアクセス並びにすべてのソフトウェア

■ 補完的対策

---

1 **オペレーティングシステム**　コンピュータシステムを動かす基盤となるソフトウェア。略して、OS。Windows 等一般的に普及している OS を汎用 OS という。

2 **コンポーネント**　機器、システム、ソフトウェア等の一部分を指す。

3 **ポート**　機器、システム、ソフトウェア等が外部の別の主体と接続や通信を行うための末端部分を指す。USB ポート、LAN ポート等の物理的な通信ポートも含まれる。

4 **プロトコル**　複数のシステムが滞りなく通信できるように定められた約束事や手順を指す。対応していないプロトコルを用いて通信することはできない。

5 **ルート**　データが通過する経路。

6 **ホスト**　処理装置や記憶装置などを内蔵した、他の機器に何らかの機能を提供するコンピュータ本体を指す。

この機能を実装できない場合、補完的対策を講じる必要があります

■ 適用

この要件は、原則としてすべてのコンピュータシステムに対して適用となります。

書類審査

■ セキュリティ機能の説明

	30. 最小限の機能性
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの事項又は対策を設けること。
☐	(1) 最小限の機能性
☐	次に掲げるものの「インストール、可用性及びアクセス権」の機能を必要最小限とすること
☐	(a) オペレーティングシステムソフトウェアのコンポーネント、プロセス及びサービス
☐	(b) ネットワークサービス、ポート、プロトコル、ルート及びホストへのアクセス並びにすべてのソフトウェア
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	30. 最小限の機能性
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) 最小限の機能性
☐	不要な機能及びサービスが実装されている場合、それらが無効化されていること。
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

31. 使用者（人）の多要素認証

規則　表 X4.1 中 31　　参照　IEC62443-3-3 / SR 1.1, RE 2

信頼できないネットワークから又は当該ネットワークを経由してコンピュータシステムにアクセスする場合、使用者（人）には多要素認証が要求される。

解説

■ 概要

ここでは、信頼できないネットワークを経由してアクセスする場合、使用者（人）の認証プロセスを多要素認証とする必要があると述べています。多要素認証とは、異なる 2 つ以上の要素を組み合わせて、システムが人を認証することを指します。NIST-SP 800-63[1]によると、認証要素は次に掲げる 3 種類に分類されます。

用語	例
知識要素 **Something you know**	本人だけが知っているものです。例えば、パスワード、PIN[2]などが該当します。
所持要素 **Something you have**	本人だけが持っているものです。例えば、セキュリティトークン[3]、公開鍵認証方式[4]で利用する秘密鍵、物理鍵[5]などが該当します。
生体要素 **Something you are**	本人の体の一部などです。たとえば、指紋、顔などが該当します。

■ 目的

ここでの目的は、人を認証する機能を強化することです。信頼できないネットワークは、セキュリティ面で信頼性が低いネットワークであるため、認証プロセスを強化することで、セキュリティを向上させる必要があります。人を認証する機能については、「1. 使用者（人）の識別及び認証」をご参照ください。

---

[1] **NIST**　米国国立標準技術研究所。National Institute of Standards and Technology の略。

[2] **PIN**　Personal Identification Number の略。通常 4～6 桁の数字で構成され、個人を識別するための秘密の数値コード。

[3] **セキュリティトークン**　システムにアクセスするための一時的なコードである「ワンタイムパスワード（OTP）」を発行する機器。

[4] **公開鍵認証方式**　公開鍵と秘密鍵のペアを用いて認証を行う方式。

[5] **物理鍵**　物理的なロック（金庫、システムなど）を解錠するための鍵。

■ 対策

ここでの対策は、使用者（人）を認証する場合の多要素認証の機能となります。この機能により、使用者（人）は異なる 2 つ以上の要素によって認証される必要があります。

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。

■ 適用

以下の場合、この要件は適用となりません。

・信頼できないネットワークとネットワーク通信を行わない場合

追加で要求されるセキュリティ機能は適用されないので、この要件の適用外となります。

書類審査

■ セキュリティ機能の説明

	31. 使用者（人）の多要素認証
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの事項又は対策を設けること。
☐	(1) 使用者（人）に対する多要素認証の機能
☐	(a) 異なる 2 つ以上の要素により認証されること
☐	(b) 正規の認証コードを使用した場合、ログインが可能であること
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	31. 使用者（人）の多要素認証
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) 使用者（人）に対する多要素認証の機能
☐	(a) 正規の認証コードでログインできること。

□	(b) 非正規の認証コードでログインできないこと。
□	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

32. ソフトウェアプロセス及びデバイスの識別及び認証

規則	参照
表 X4.1 中 5	IEC62443-3-3 / SR 1.2

コンピュータシステムは、ソフトウェアプロセス及びデバイスを識別及び認証するものでなければならない。

解説

■ 概要

ここでは、システムに使用されるソフトウェアプロセスやデバイスに対して、識別及び認証する必要があると述べています。ソフトウェアプロセスおよびデバイスについては、以下のとおりです。

用語	説明
ソフトウェアプロセス	システムが利用するプログラムやアプリケーションを指します。
デバイス	システムを利用する物理的なハードウェアや機器を指します。

■ 目的

ここでの目的は、システムが信頼されていないネットワークと通信する場合、システムがソフトウェアプロセスやデバイスを認証することによって、不正アクセス等のリスクを低減することです。信頼できないネットワーク下では、不正アクセスの可能性が高まります。そのため、識別と認証は人間だけでなく、ソフトウェアプロセスとデバイスに対しても行うことで、通信のセキュリティをより強化します。

■ 対策

ここでの対策は、システムに使用されるソフトウェアプロセスやデバイスに対する識別と認証の機能となります。これらは、人の場合と同様、識別子及び認証コードにより識別及び認証される必要があります。

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。

■ 適用

以下の場合、この要件は適用となりません。

・信頼できないネットワークとネットワーク通信を行わない場合

追加で要求されるセキュリティ機能は適用されないので、この要件の適用外となります。

書類審査

■ セキュリティ機能の説明

	32. ソフトウェアプロセス及びデバイスの識別及び認証
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) ソフトウェアプロセス及びデバイスを識別及び認証する機能
☐	(a) ソフトウェアプロセスの識別と認証
☐	i) 識別子によって識別すること。
☐	ii) 識別子および認証コードによって認証すること。
☐	(b) デバイスの識別と認証
☐	i) 識別子によって識別すること。
☐	ii) 識別子および認証コードによって認証すること
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	32. ソフトウェアプロセス及びデバイスの識別及び認証
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) ソフトウェアプロセス及びデバイスを識別及び認証する機能の実証試験
☐	(a) ソフトウェアプロセスの識別と認証
☐	i) 正規の識別子および認証コードによってログインできること。
☐	ii) 非正規の識別子および認証コードによってログインできないこと。
☐	(b) デバイスの識別と認証
☐	i) 正規の識別子および認証コードによってログインできること。
☐	ii) 非正規の識別子および認証コードによってログインできないこと。
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

33. 失敗したログイン試行

規則	参照
表 X4.1 中 33	IEC62443-3-3 / SR 1.11

コンピュータシステムは、一定時間内における信頼できないネットワークからの連続した無効なログイン試行の制限を実施するものでなければならない。

解説

■ 概要

ここでは、信頼できないネットワーク経由でのログインについて、一定期間に間違ったパスワードで繰り返しログインすることを防止する必要があると述べています。

■ 目的

ここでの目的は、ブルートフォースアタック[1]やDoS攻撃[2]等の連続したサイバー攻撃を防御することです。攻撃を防御できない場合、パスワードが漏洩したり、ネットワークやシステムの機能が停止したりします。

■ 対策

ここでの対策は、一定時間内における連続した無効なログイン試行を制限する機能となります。この機能により、設定された試行回数を超えた場合、そのアクセスは拒否される必要があります。また、拒否されたアクセスは、指定された期間または管理者によってロック解除されるまで継続されるものでなければいけません。

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。

■ 適用

以下の場合、この要件は適用となりません。

・「1. 使用者（人）の識別及び認証」の機能を補完的対策とする場合、又は同要件が適用外の場合

使用者の識別及び認証する機能を実装されていない場合、識別子はありません。この場

[1] **ブルートフォースアタック（総当たり攻撃）** パスワードを解読するために、可能性のあるすべての組み合わせを試すサイバー攻撃の手法。自動化ツールを使用することで、何千回ものログインを試行する。

[2] **DoS 攻撃** Denial of Service（サービス妨害）の略。中でも、DDoS（分散型サービス妨害）攻撃は、複数のコンピュータやデバイスを利用し、ウェブサイトやサーバに大量のトラフィックを送ることで、システムをより大規模に妨害する。

合、この要件は適用外となります。

1. 使用者（人）の識別と認証 P. 53

・信頼できないネットワークとネットワーク通信を行わない場合

追加で要求されるセキュリティ機能は適用されないので、この要件の適用外となります。

書類審査

■ セキュリティ機能の説明

	33. 失敗したログイン試行
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 連続した無効なログイン試行を制限する機能
	次に掲げる項目に適合すること。
☐	(a) 連続した無効なログイン試行が設定された試行回数を超えた場合、アクセスを拒否すること
☐	(b) 拒否されたアクセスは、指定された期間または管理者によってロック解除されるまで続くこと
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	33. 失敗したログイン試行
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) ソフトウェアプロセス及びデバイスを識別及び認証する機能の実証試験
☐	次に掲げる項目に適合すること。
☐	(a) 連続した無効なログイン試行が設定された試行回数を超えた場合、アクセスを拒否すること
☐	(b) 拒否されたアクセスは、指定された期間または管理者によってロック解除されるまで続くこと
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

34. システム使用通知

規則	参照
表 X4.1 中 34	IEC62443-3-3 / SR 1.12

コンピュータシステムは、認証前にシステム使用通知メッセージを表示する機能を提供するものでなければならない。システム使用通知メッセージは、権限を有する人員により設定可能でなければならない。

解説

■ 概要

ここでは、システム使用通知メッセージを表示する必要があると述べています。システム使用通知メッセージとは、人がシステムにログインする前に表示されるメッセージのことを指します。

■ 目的

ここでの目的は、システムを使用する前に、システムの利用規約やセキュリティポリシー等、システムの利用条件への同意を求めることです。このような同意は、使用者に対してシステムの使用に関する責任を明確します。

■ 対策

ここでの対策は、システム使用通知メッセージを表示する機能となります。これは、使用者（人）を認証する前にメッセージが表示される必要があります。また、メッセージを編集する機能も必要となります。その理由は、システムの利用規約やセキュリティポリシーが変更された場合に、適切に反映させることができるようにするためです。編集機能は、適切なメッセージが表示されるように、管理者など権限を有する人のみにより編集できる必要があります。

補足　システム使用通知メッセージに一般的に含まれる内容の例を以下に示します。これらは参考であり、必ずしもこれらに限定されるわけではありません。

・個人が特定のコンピュータシステムにアクセスしている。
・システムの使用が監視、記録及び監査の対象になる場合がある。
・システムの無認可での使用は禁止されている。
・システムの使用は監視及び記録の同意を示す。

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります

■ 適用

以下の場合、この要件は適用となりません。

・信頼できないネットワークとネットワーク通信を行わない場合

追加で要求されるセキュリティ機能は適用されないので、この要件の適用外となります。

・HMI が実装されていない場合

システム使用通知メッセージを表示するためのモニターなどの HMI を持っていない場合は、この要件の適用外となります。

書類審査

■ セキュリティ機能の説明

	34. システム使用通知
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) システム使用通知メッセージを表示及び編集する機能
☐	次に掲げる機能を実装していること。
☐	(a) システム使用通知メッセージを表示する機能
☐	認証前にシステム使用通知メッセージが表示されること。
☐	(b) システム使用通知メッセージを編集する機能
☐	権限を有する人員によって編集できること。
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	34. システム使用通知
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) システム使用通知メッセージを表示及び編集する機能
☐	次に掲げる機能を実装していること。
☐	(a) システム使用通知メッセージを表示する機能

☐	認証前にシステム使用通知メッセージが表示されること。
☐	(b) システム使用通知メッセージを編集する機能
☐	次に掲げる項目に適合すること。
☐	i) 権限を有する人員によって編集できること。
☐	ii) 権限を有さない人員によって編集できないこと。
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

35. 信頼できないネットワーク経由のアクセス

規則	参照
表 X4.1 中 35	IEC62443-3-3 / SR 1.13

信頼できないネットワークから又は当該ネットワークを経由してのコンピュータシステムへのすべてのアクセスは、監視及び制御されなければならない。

解説

■ 概要

ここでは、信頼できないネットワークを経由するアクセスを監視および制御する必要があると述べています。

■ 目的

ここでの目的は、信頼できないネットワークからのアクセスを監視し、必要に応じて特定のアクセスを制限または遮断することです。これにより、攻撃者による不正アクセスを防止します。

■ 対策

ここでの対策は、アクセスを監視および制御できる機能となります。例えば、侵入検知システム（IDS）を組み込む等です。

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。以下に補完的対策の一例を示します。

・外部のセキュリティ機器により、アクセスを監視及び制御する

システムがこの機能を持たない場合、この要件を満たすための外部のセキュリティ機器により、この機能を補完することとなります。

■ 適用

以下の場合、この要件は適用となりません。

・信頼できないネットワークとネットワーク通信を行わない場合

追加で要求されるセキュリティ機能は適用されないので、この要件の適用外となります。

書類審査

■ セキュリティ機能の説明

	35. 信頼できないネットワーク経由のアクセス
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 信頼できないネットワークを経由するアクセスを監視及び制御する機能
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	35. 信頼できないネットワーク経由のアクセス
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) 信頼できないネットワークを経由するアクセスを監視及び制御する機能
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

36. アクセス要求の明示的な承認

規則	参照
表 X4.1 中 36	IEC62443-3-3 / SR 1.13, RE 1

コンピュータシステムは、船上にいる権限を有する人員により明示的に承認された場合を除き、信頼できないネットワークから又は当該ネットワークを経由したアクセスを拒否するものでなければならない。

解説

■ 概要

ここでは、承認権限を有する使用者（人）により明示的に承認された場合を除き、信頼できないネットワークから又は当該ネットワークを経由したアクセスを拒否する必要があると述べています。

■ 目的

ここでの目的は、信頼できないネットワークからの不正なアクセス要求を拒否することです。これにより、攻撃者による不正アクセスを防止します。

■ 対策

ここでの対策は、承認権限を有する使用者（人）により明示的に承認された場合を除き、信頼できないネットワークから又は当該ネットワークを経由したアクセスを拒否する機能となります。具体的には、以下 2 点の機能が該当します。

・使用者（人）に対して、アクセスの承認権限を割り当てる機能
・承認されていないアクセスを拒否する機能

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。

■ 適用

以下の場合、この要件は適用となりません。

・信頼できないネットワークとネットワーク通信を行わない場合
追加で要求されるセキュリティ機能は適用されないので、この要件の適用外となります。

書類審査

■ セキュリティ機能の説明

	36. アクセス要求の明示的な承認
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
□	(1) 承認権限を有する使用者（人）により明示的に承認された場合を除き、信頼できないネットワークから又は当該ネットワークを経由したアクセスを拒否する機能
□	(a) 使用者（人）に対して、アクセスの承認権限を割り当てる機能
□	(b) 承認されていないアクセスを拒否する機能
□	(2) 補完的対策
□	(a) 本要件と同じ脅威から保護すること。
□	(b) 本要件と同等の厳しさ，正確さであること。
□	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
□	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	36. アクセス要求の明示的な承認
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
□	(1) 承認権限を有する使用者（人）により明示的に承認された場合を除き、信頼できないネットワークから又は当該ネットワークを経由したアクセスを拒否する機能
□	(a) 使用者（人）に対して、アクセスの承認権限を割り当てる機能
□	(b) 承認されていないアクセスを拒否する機能
□	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

37. リモートセッションの終了

規則	参照
表 X4.1 中 37	IEC62443-3-3 / SR 2.6

コンピュータシステムは，設定可能な無操作時間の経過後に自動で又はセッションを開始した使用者が手動で，リモートセッションを終了する機能を提供するものでなければならない。

解説

■ 概要

ここでは、手動または自動によりリモートセッションを終了する必要があると述べています。リモートアクセスとは、インターネット等を経由して、遠隔地からコンピュータシステムへアクセスすることです。例えば、陸上の施設からのモニタリングなどが該当します。

■ 目的

ここでの目的は、必要なリモートセッションが終了した時点でセッションを終了できることです。これにより、セッションが不必要に接続されたままになることを防ぎ、不正アクセスを防ぐことが可能となります。

■ 対策

ここでの対策としては、リモートアクセスのセッションを終了する機能となります。具体的には、自動又は手動いずれかによるリモートセッションのログアウト機能となります。

対策	説明
自動での終了	無操作の状態が設定した時間継続した場合に、自動的にログアウトする機能です。
手動での終了	リモートアクセスを受ける側（ローカル側）及びリモートアクセスする側（リモート側）に機能を設け、セッションを開始した使用者の操作によってログアウトすることができる必要があります。ローカル側の機能は、管理者画面等で強制ログアウトする機能などです。

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。

■ 適用

以下の場合、この要件は適用となりません。

・信頼できないネットワークとネットワーク通信を行わない場合

追加で要求されるセキュリティ機能は適用されないので、この要件の適用外となります。

・リモートアクセス機能がない場合

ローカルでのネットワーク通信のみ行う場合は、この要件の適用外となります。

書類審査

■ セキュリティ機能の説明

	37. リモートセッションの終了
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
□	(1) リモートセッションを終了する機能
□	次に掲げる機能のいずれかを実装していること。
□	(a) 自動でリモートセッションを終了する機能
□	次に掲げる項目に適合していること。
□	i) セッションが終了する無操作時間を設定すること。
□	ii) 設定可能な無操作時間の経過後にセッションが終了すること。
□	(b) 手動でリモートセッションを終了する機能
□	使用者の操作によってセッションが終了すること。
□	(2) 補完的対策
□	(a) 本要件と同じ脅威から保護すること。
□	(b) 本要件と同等の厳しさ，正確さであること。
□	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
□	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	37. リモートセッションの終了
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
□	(1) リモートセッションを終了する機能の実証試験
□	次に掲げる機能のいずれかを実装していること
□	(a) 自動でリモートセッションを終了する機能
□	次に掲げる項目に適合していること

☐	i)　セッションが終了する無操作時間を設定すること
☐	ii)　無操作時間の経過後にセッションが終了すること
☐	(b)　手動でリモートセッションを終了する機能
☐	使用者の操作によってセッションが終了すること
☐	(2)　補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

38. 暗号化による完全性の保護

規則　表 X4.1 中 38　　参照　IEC62443-3-3 / SR 3.1, RE 1

コンピュータシステムは、信頼できないネットワークとの又は当該ネットワークを経由した通信中における情報の変更を認識するために、暗号化の仕組みを採用するものでなければならない。

解説

■ 概要

ここでは、暗号技術を使用し、通信中の情報の変更を認識する必要があると述べています。ここでいう暗号技術とは、情報が送信元から目的地までの間に変更されていないことを確認するための技術を指します。

■ 目的

ここでの目的は、通信中の情報の変更を認識することです。情報の不正な変更を認識できなければ、システムに間違った情報が伝達されてしまい、システムの運用に影響を及ぼす可能性があります。

■ 対策

ここでの対策は、通信中の情報の変更を認識するための暗号化の仕組みとなります。例えば、電子署名（デジタル署名）[1]等です。暗号化については、「22. 暗号の使用」に詳しく解説しております。

暗号の使用　P. 108

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。

■ 適用

以下の場合、この要件は適用となりません。

・信頼できないネットワークとネットワーク通信を行わない場合

追加で要求されるセキュリティ機能は適用されないので、この要件の適用外となります。

[1] **電子署名（デシタル署名）**　メッセージの送信者がそのメッセージの作成者であることを証明し、メッセージが送信後に改ざんされていないことを保証するための技術。

書類審査

■ セキュリティ機能の説明

	38. 暗号化による完全性の保護
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの仕組み又は対策を設けること。
☐	(1) 信頼できないネットワークとの又は当該ネットワークを経由した通信中における情報の変更を認識するための暗号化の仕組み
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

この要件は、書類審査にて確認しますので、立会検査は不要となります。

39. 入力の検証

規則	参照
表 X4.1 中 39	IEC62443-3-3 / SR 3.5

コンピュータシステムは、プロセス制御の入力として使用される又はコンピュータシステムの動作に直接影響する、信頼できないネットワーク経由のすべての入力データにつき、構文、長さ及び内容を検証するものでなければならない。

解説

■ 概要

ここでは、信頼できないネットワークからの入力データを検証する必要があると述べています。

■ 目的

信頼できないネットワークでは、攻撃者から不正なデータを入力される可能性が高まります。入力データの検証を行い、不正なデータの受取りを防ぐことで、セキュリティを向上させる必要があります。

■ 対策

ここでの対策として、入力データの構文、長さ、内容を検証する必要があります。

対策	説明
構文の検証	入力データが**決められた形式やルールに従っているか**どうかをチェックします。例えば、数値や日付などのデータ型やフォーマット、文字コードやエンコーディングなどが正しいかどうかを確認します。
長さの検証	入力データが**決められた長さや範囲に収まっているか**どうかをチェックします。例えば、文字数や桁数、最大値や最小値などが適切かどうかを確認します。
内容の検証	入力データが**決められた条件や基準に合致しているか**どうかをチェックします。例えば、存在しない値や禁止された値、矛盾した値などが含まれていないかどうかを確認します。

なお、ここでいう検証とは、検証結果の処理までを含めた一連のプロセスを指します。つまり、無効なデータと判断した場合、データの受取りを拒否する等、どのように対応するかを明確にする必要があります。

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。

■ 適用

以下の場合、この要件は適用となりません。

・信頼できないネットワークとネットワーク通信を行わない場合

追加で要求されるセキュリティ機能は適用されないので、この要件の適用外となります。

書類審査

■ セキュリティ機能の説明

	39. 入力の検証
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 入力データを検証する機能
☐	(a) 次に掲げる入力データの要素を検証すること。
☐	i) 構文
☐	ii) 長さ
☐	iii) 内容
☐	(b) 無効なデータと判断した場合、適切に対応すること。(例：入力データの受取りを拒否する等)
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	39. 入力の検証
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) 入力データを検証する機能の実証試験。
☐	無効なデータと判断した場合、適切に対応すること。(例：入力データの受取りを拒否する等)
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

40. セッションの完全性

規則	参照
表 X4.1 中 40	IEC62443-3-3 / SR 3.8

コンピュータシステムは，セッション[1]の完全性を保護するものでなければならない。無効なセッション ID は，拒否されなければならない。

解説

■ 概要

ここでは、セッションの完全性を保護し、無効なセッション ID の使用を拒否する必要があると述べています。セッションの完全性の保護とは、セッションが許可された使用者と関連付けられ、この関連性を維持することであり、セッション ID が使用されます。セッション ID とは、セッションを識別するための識別子（ID)を指します。

■ 目的

ここでの目的は、セッション ID の不正利用を防止することです。セッション ID の完全性が保護されていない場合、セッションハイジャック[2]やセッション固定攻撃[3]等により、セッション ID が悪用される可能性があります。

■ 対策

ここでの対策は、以下 2 点の機能となります。

・セッションの完全性を保護する機能
・無効なセッション ID の使用を拒否する機能

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。

■ 適用

以下の場合、この要件は適用となりません。

・信頼できないネットワークとネットワーク通信を行わない場合

追加で要求されるセキュリティ機能は適用されないので、この要件は適用されません。

・HMI を介したセッションを使用しない場合

例えば、ブラウザ等 HMI を介したセッションを使用しない場合、この要件は適用されま

---

[1] **セッション**　使用者がシステムにログインしてからログアウトするまでの一連の操作。

[2] **セッションハイジャック**　既存のセッションを不正に乗っ取る攻撃手法。

[3] **セッション固定攻撃**　攻撃者が事前に決めたセッション ID を被害者に強制的に使わせ、被害者になりすます手法。

せん。

書類審査

■ セキュリティ機能の説明

	40. セッションの完全性
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) セッションの完全性を保護し、無効なセッション ID の使用を拒否する機能
☐	次に掲げる項目に適合すること
☐	(a) セッションの完全性を保護すること
☐	(b) 無効なセッション ID の使用を拒否すること
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	40. セッションの完全性
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) セッションの完全性を保護し、無効なセッション ID の使用を拒否する機能の実証試験
☐	次に掲げる項目に適合すること
☐	(a) セッションの完全性を保護すること
☐	(b) 無効なセッション ID の使用を拒否すること
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

補足 セッションに関して、他にも要求される機能があります。以下のページを参照ください。

セッションロック P. 84

セッション終了後のセッション ID の無効化 P. 152

41. セッション終了後のセッション ID の無効化

規則	参照
表 X4.1 中 41	IEC62443-3-3 / SR 3.8, RE 1

コンピュータシステムは、使用者のログアウト又はその他のセッション終了（ブラウザセッションを含む）に伴い、セッション ID[1]を無効化するものでなければならない。

解説

■ 概要

ここでは、使用者のログアウト又はブラウザセッションを含むセッション終了後、セッション ID を無効化する必要があると述べています。

■ 目的

ここでの目的は、セッション ID を速やかに無効化することで、セッションが悪用されるリスクを防止することです。セッションが終了された後もセッション ID が有効のままであると、セッションハイジャック[2]やセッション固定攻撃[3]等により、セッション ID が悪用される可能性があります。

■ 対策

ここでの対策は、使用者のログアウト又はブラウザセッションを含むセッション終了時にセッション ID を無効化する機能となります。

■ 補完的対策

この機能を実装できない場合、補完的対策を講じる必要があります。

■ 適用

以下の場合、この要件は適用となりません。

・信頼できないネットワークとネットワーク通信を行わない場合

追加で要求されるセキュリティ機能は適用されないので、この要件は適用されません。

・HMI を介したセッションを使用しない場合

---

[1] **セッション**　使用者がシステムにログインしてからログアウトするまでの一連の操作。**セッション ID** とは、使用者が使用するセッションを識別するための一意の識別子(ID)。

[2] **セッションハイジャック**　既存のセッションを不正に乗っ取る攻撃手法。

[3] **セッション固定攻撃**　攻撃者が事前に決めたセッション ID を被害者に強制的に使わせ、被害者になりすます手法。

例えば、ブラウザ等 HMI を介したセッションを使用しない場合、この要件は適用されません。

書類審査

■ セキュリティ機能の説明

	41. セッション終了後のセッション ID の無効化
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 使用者のログアウト又はブラウザセッションを含むセッション終了後、セッション ID を無効化する機能
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

立会検査

■ セキュリティ機能試験

	41. セッション終了後のセッション ID の無効化
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) 使用者のログアウト又はブラウザセッションを含むセッション終了後、セッション ID を無効化する機能の実証試験
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

補足 セッションに関して、他にも要求される機能があります。以下のページを参照ください。

セッションロック P. 84

セッションの完全性 P. 150

6章 セキュア開発ライフサイクルに関する要件の解説

本章では、X編4章（UR E27）で要求されるセキュア開発ライフサイクルに関する要件の詳細を解説します。セキュア開発ライフサイクルとは、セキュアな製品の開発及び保守を目的としたライフサイクルを指します。これは、例えば納入後のセキュリティアップデートの配信や、セキュリティに関する多層防御の戦略等が挙げられます。このライフサイクルは、IEC62443-4-1という規格の要求事項の一部を、X編4章（UR E27）に取り入れたものとなります。

セキュア開発ライフサイクルの概要

■ セキュア開発ライフサイクルに関する要件とは

X編4章（UR E27）では、IEC62443-4-1から7つのセキュア開発ライフサイクルの要求事項が取り入れられております。各要件は以下のとおりです。

セキュア開発ライフサイクルに関する要件

■ セキュア開発ライフサイクルに従ったプロセス又は管理が必要

製造者は、設計、製造及び保守などの各段階において、製品がセキュアな状態を維持するために、セキュア開発ライフサイクルに従ったプロセス又は管理を導入する必要があります。

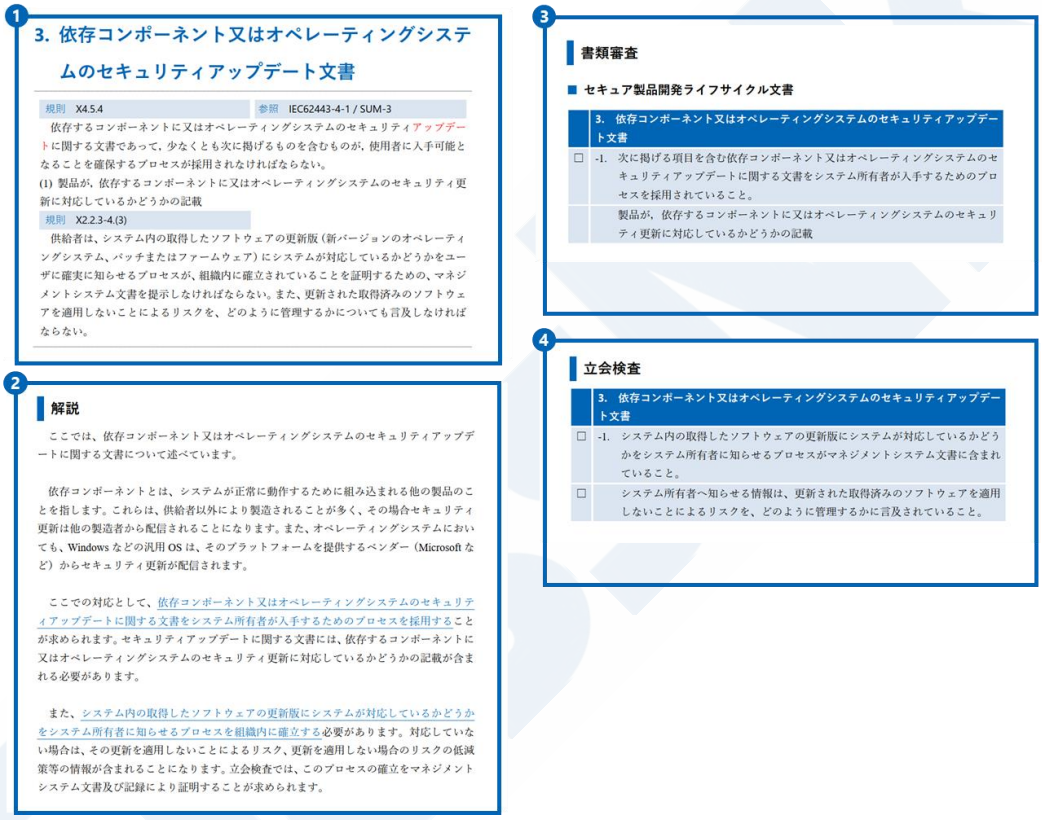
このプロセス及び管理とは、セキュアな製品を維持するために、製造者が順守すべき手順

又は指示です。これは、例えばセキュリティアップデートの提供手順を作成するプロセスであったり、セキュリティの多層防御策を作成するプロセスであったりが挙げられます。

このプロセス又は管理は、製造者が定めるマネジメントシステムの一環として取り組まれるものです。したがって、これらは、品質管理マニュアル又はそれに紐づく手順書のようなマネジメントシステム文書により文書化される必要があります。

セキュア開発ライフサイクルの詳細

以降のページの見方



1 要件

セキュア開発ライフサイクルに関する要件の名称と詳細です。X 編 4 章（UR E27）では、各要件に対して規則が 2 つずつ規定されています。

2 解説

セキュア開発ライフサイクルに関する要件の解説です。

3 書類審査

セキュリティ機能に関する要件に関する書類審査のチェックリストです。

・セキュア開発ライフサイクル文書：X 編 4.4.1(6)で要求される提出資料

4 立会検査

セキュリティ機能の要件に関する立会検査のチェックリストです。

・セキュア開発ライフサイクル：X 編 2.2.3-4.で要求される立会検査

1. 秘密鍵の管理

規則　X4.5.2　　参照　IEC62443-4-1 / SM-8

製造者は、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ための手順上及び技術上の管理策を保有しなければならない。

規則　X2.2.3-4.(1)

秘密鍵の管理は、ユーザがその真正性を確認できるようにすることを目的として、電子署名されたソフトウェアをシステムが含む場合に適用される。

供給者は、コード署名に使用される秘密鍵の生成、保管及び使用を不正アクセスから保護することを目的として、方針、手順及び技術的管理が行われていることを立証するマネジメントシステム文書を提示しなければならない。方針及び手順にあっては、役割、責任及び作業プロセスを扱わなければならない。

技術的管理にあっては、物理的なアクセス制限、秘密鍵の保管のための暗号化ハードウェア（ハードウェアセキュリティモジュール[1]等）が含まれなければならない。

解説

ここでは、コード署名に使用する秘密鍵の管理について述べています。この要件は、電子署名されたソフトウェアをシステムが含む場合に適用されます。

コード署名とは、開発者が作成したソフトウェアに対して電子署名[2]を行うことで、そのソフトウェアが改ざんされていないことを保証し、かつ、そのソフトウェアが特定の開発者によって作成されたことを証明する技術のひとつです。この署名を行う際に使用される秘密鍵は、開発者の身元を証明する重要な要素となります。

ここでの対応として、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ための手順上及び技術上の管理策を保有することが求められます。

手順上の管理策としては、例えば以下のようなものがあります。

・秘密鍵の取扱いについて、役割や責任を定めること
・秘密鍵を生成する際には、アクセスが制限されたセキュアな環境で行うこと
・秘密鍵を保管する際には、暗号化やパスワード保護などの措置を施すこと
・秘密鍵を使用する際には、承認や記録などの作業プロセスを設けること

[1] **ハードウェアモジュール（HSM）**　秘密鍵を安全に生成、保管する専用のハードウェア装置。機密情報を安全に保管し、不正アクセスや改ざんから保護する。

[2] **電子署名**　電子的な方法で文書やメッセージの送信者や内容が正しいことを証明する仕組み。電子署名には、公開鍵暗号やデジタル証明書などの技術がある。

技術上の管理策としては、例えば以下のようなものがあります。

・秘密鍵の物理的なアクセス制限として、USB メモリや SD カードなどの外部記憶媒体に保存し、金庫やロッカーなどの施錠可能な場所に保管する。
・秘密鍵の暗号化ハードウェアとして、ハードウェアセキュリティモジュールなどの専用デバイスに保存する。

また、秘密鍵の管理方針を含む上述の管理を組織内に確立する必要があります。立会検査では、この管理の確立をマネジメントシステム文書及び記録により証明することが求められます。管理方針には、役割及び責任などを記載されることとなります。

書類審査

■ セキュア開発ライフサイクル文書

	1. 秘密鍵の管理
□	-1. 電子署名されたソフトウェアがシステムに含まれている場合、次に掲げる管理策が保有されていること。
□	(1) 秘密鍵の手順上の管理策（例：生成、保管及び使用の手順等）
□	(2) 秘密鍵の技術上の管理策（例：物理的なアクセス制限や暗号化ハードウェア等）

立会検査

■ セキュア開発ライフサイクル

	1. 秘密鍵の管理
□	-1. 電子署名されたソフトウェアがシステムに含まれている場合、次に掲げる管理策等がマネジメントシステム文書に含まれていること。また、それらについて、役割、責任及び作業プロセスを扱っていること。
□	(1) 秘密鍵の管理方針
□	(2) 秘密鍵の手順上の管理策（例：生成、保管及び使用の手順等）
□	(3) 秘密鍵の技術上の管理策（例：物理的なアクセス制限や暗号化ハードウェア等）

2. セキュリティアップデートの文書

規則　X4.5.3　　参照　IEC62443-4-1 / SUM-2

製品のセキュリティアップデートに関する文書であって、少なくとも次に掲げる内容を含むものが、（サイバーセキュリティ連絡窓口の設置又は使用者がアクセス可能な定期的発行物等を通じて）使用者に入手可能となることを確保するプロセスが採用されなければならない。

(1) セキュリティパッチ[1]が適用される製品のバージョン番号
(2) 承認されたパッチの手動及び自動プロセス経由による適用方法に関する説明
(3) 製品にパッチを適用することで発生する可能性のある影響（再起動を含む）の記述
(4) 承認されたパッチが適用されたことの確認方法に関する説明
(5) パッチを適用しないこと並びに資産所有者が承認又は導入しないパッチに使用できるメディエーション[2]に関するリスク

規則　X2.2.3-4.(2)

供給者[3]は、セキュリティアップデートを確実にユーザに知らせるためのプロセスが、組織内に確立されていることを証明するための、マネジメントシステム文書を提示しなければならない。ユーザへの情報提供は、**上記 5 項目**を含まなければならない。

解説

ここでは、セキュリティアップデートの文書について述べています。

ここでの対応として、セキュリティアップデートに関する文書をシステム所有者が入手するためのプロセスを採用することが求められます。セキュリティアップデートに関する文書には、以下の内容が含まれる必要があります。

・セキュリティパッチが適用される製品のバージョン番号

セキュリティパッチとは、現行のソフトウェアに含まれている問題を解決するために配布される追加のプログラムです。これは、製品のバージョンに適したセキュリティパッチであることを明確にします。

・承認されたパッチの手動及び自動プロセス経由による適用方法に関する説明
・製品にパッチを適用することで発生する可能性のある影響（再起動を含む）の記述
・承認されたパッチが適用されたことの確認方法に関する説明

---

[1] **（セキュリティ）パッチ**　セキュリティ上の脆弱性及びバグに対処するため又はオペレーティングシステム若しくはアプリケーションを改善するために、インストールされたソフトウェアやデータを更新するよう設計されたソフトウェア

[2] **メディエーション**　承認されていないパッチを利用した場合に代替するリスク低減策のこと。

[3] **供給者**　システムの製造者又は提供者をいう。供給者は、システムを、システム統合者又はシステム所有者に提供することに責任を有する。

・パッチを適用しないこと並びに資産所有者が承認又は導入しないパッチに使用できるメディエーションに関するリスク

メディエーションとは、承認されていないパッチを利用した場合に代替するリスク低減策を指します。これは、パッチの非適用やメディエーションのリスクを明確にし、それに基づいて意思決定を行うために必要となります。

また、セキュリティアップデートをシステム所有者に知らせるためのプロセスを組織内に確立する必要があります。立会検査では、このプロセスの確立をマネジメントシステム文書及び記録により証明することが求められます。

書類審査

■ セキュア開発ライフサイクル文書

	2. セキュリティアップデートの文書
□	-1. 次に掲げる項目を含むセキュリティアップデートの文書が使用者に入手可能となることを確保するプロセスが採用されていること。
□	(1) セキュリティパッチが適用される製品のバージョン番号
□	(2) 承認されたパッチの手動及び自動プロセス経由による適用方法に関する説明
□	(3) 製品にパッチを適用することで発生する可能性のある影響（再起動を含む）の記述
□	(4) 承認されたパッチが適用されたことの確認方法に関する説明
□	(5) パッチを適用しないこと並びに資産所有者が承認又は導入しないパッチに使用できるメディエーションに関するリスク

立会検査

■ セキュア開発ライフサイクル

	2. セキュリティアップデートの文書
□	-1. セキュリティアップデートをシステム所有者に知らせるためのプロセスがマネジメントシステム文書に含まれていること。
□	システム所有者へ知らせる情報は、次に掲げる項目が含まれていること。
□	(1) セキュリティパッチが適用される製品のバージョン番号
□	(2) 承認されたパッチの手動及び自動プロセス経由による適用方法に関する説明
□	(3) 製品にパッチを適用することで発生する可能性のある影響（再起動を含む）の記述
□	(4) 承認されたパッチが適用されたことの確認方法に関する説明
□	(5) パッチを適用しないこと並びに資産所有者が承認又は導入しないパッチに使用できるメディエーションに関するリスク

3. 依存コンポーネント又はオペレーティングシステムのセキュリティアップデート文書

規則　X4.5.4　　参照　IEC62443-4-1 / SUM-3

依存するコンポーネントに又はオペレーティングシステムのセキュリティアップデートに関する文書であって，少なくとも次に掲げるものを含むものが，使用者に入手可能となることを確保するプロセスが採用されなければならない。

(1) 製品が，依存するコンポーネントに又はオペレーティングシステムのセキュリティアップデートに対応しているかどうかの記載

規則　X2.2.3-4.(3)

供給者は、システム内の取得したソフトウェアの更新版（オペレーティングシステム又はファームウェアの新バージョン又はパッチ）にシステムが対応しているかどうかをユーザに確実に知らせるプロセスが、組織内に確立されていることを証明するための、マネジメントシステム文書を提示しなければならない。また、更新された取得済みのソフトウェアを適用しないことによるリスクを、どのように管理するかについても言及しなければならない。

解説

ここでは、依存コンポーネント又はオペレーティングシステムのセキュリティアップデートに関する文書について述べています。

依存コンポーネントとは、システムが正常に動作するために組み込まれる他の製品のことを指します。これらは、供給者以外により製造されることが多く、その場合セキュリティアップデートは他の製造者から配信されることになります。また、オペレーティングシステムにおいても、Windows などの汎用 OS は、そのプラットフォームを提供するベンダー（Microsoft など）からセキュリティアップデートが配信されます。

ここでの対応として、依存コンポーネント又はオペレーティングシステムのセキュリティアップデートに関する文書をシステム所有者が入手するためのプロセスを採用することが求められます。セキュリティアップデートに関する文書には、依存するコンポーネントに又はオペレーティングシステムのセキュリティアップデートに対応しているかどうかの記載が含まれる必要があります。

また、システム内の取得したソフトウェアの更新版にシステムが対応しているかどうかをシステム所有者に知らせるプロセスを組織内に確立する必要があります。対応していない場合は、その更新を適用しないことによるリスクが含まれることになります。立会検査では、このプロセスの確立をマネジメントシステム文書及び記録により証明することが求められます。

書類審査

■ セキュア開発ライフサイクル文書

	3. 依存コンポーネント又はオペレーティングシステムのセキュリティアップデート文書
□	-1. 次に掲げる項目を含む依存コンポーネント又はオペレーティングシステムのセキュリティアップデートに関する文書をシステム所有者が入手するためのプロセスを採用されていること。
□	製品が，依存するコンポーネントに又はオペレーティングシステムのセキュリティアップデートに対応しているかどうかの記載

立会検査

■ セキュア開発ライフサイクル

	3. 依存コンポーネント又はオペレーティングシステムのセキュリティアップデート文書
□	-1. システム内の取得したソフトウェアの更新版にシステムが対応しているかどうかをシステム所有者に知らせるプロセスがマネジメントシステム文書に含まれていること。
□	システム所有者へ知らせる情報は、更新された取得済みのソフトウェアを適用しないことによるリスクを、どのように管理するかに言及されていること。

4. セキュリティアップデートの配信

規則　X4.5.5　　参照　IEC62443-4-1 / SUM-4

サポート対象であるすべての製品及び製品バージョンに対するセキュリティアップデートが，セキュリティパッチ[1]が真正であることを検証できる方法で，製品使用者に入手可能となることを確保するプロセスが採用されなければならない。（IACS[2] の補足：製造者は，リリース前に更新を試験するための QA プロセス[3]を有さなければならない。）

規則　X2.2.3-4.(4)

供給者は，システムセキュリティの更新がユーザに提供されることを保証するプロセスが，組織内に確立されていることを証明するための，マネジメントシステム文書を提示し，ユーザが更新されたソフトウェアの真正性を確認する方法を説明しなければならない。

解説

ここでは、セキュリティアップデートの配信について述べています。

ここでの対応として、セキュリティパッチが真正であることを確認できる方法によって、システム所有者がセキュリティアップデートを入手するためのプロセスを採用することが求められます。セキュリティアップデートをリリースする前の試験について、QA プロセスに定める必要があります。

また、セキュリティアップデートがシステム所有者に提供されることを保証するプロセスを組織内に確立する必要があります。ここで提供されるセキュリティパッチは、上述のとおり、本物であることを検証できなければなりません。立会検査では、このプロセスの確立をマネジメントシステム文書及び記録により証明することが求められます。

書類審査

■ セキュア開発ライフサイクル文書

	4.　セキュリティアップデートの配信
□	-1.　セキュリティパッチが真正であることを確認できる方法によって、システム所有

[1] **（セキュリティ）パッチ**　現行のソフトウェアに含まれている問題を解決するために配布される、追加のプログラム。X 編では、「セキュリティ上の脆弱性及びバグに対処するため又はオペレーティングシステム若しくはアプリケーションを改善するために，インストールされたソフトウェアやデータを更新するよう設計されたソフトウェア」と定義される。

[2] **IACS**　International Association Classification Societies（国際船級協会連合）の略。

[3] **QA プロセス**　品質保証（Quality Assurance）プロセス。製品やサービスが特定の要件、基準、または指標を満たすことを確実にするための一連の活動の流れ。

		者がセキュリティアップデートを入手するためのプロセスが採用されていること。
	-2.	セキュリティアップデートのリリース前に更新を試験するための QA プロセスが採用されていること。

立会検査

■ セキュア開発ライフサイクル

	4. セキュリティアップデートの配信	
□	-1.	セキュリティアップデートがシステム所有者に提供されることを保証するプロセスがマネジメントシステム文書に含まれていること。
□		システム所有者へ知らせる情報は、更新されたソフトウェアの真正性を確認する方法が含まれていること。

5. 製品の多層防御

規則　X4.5.6　　参照　IEC62443-4-1 / SG-1

製品に関する文書であって、製品のインストール、運用及び保守をサポートするために、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プロセスが存在しなければならない。当該文書は、次に掲げる内容を含むものでなければならない。

(1) 製品が実装するセキュリティ機能、また、多層防御の戦略におけるその役割

(2) 多層防御の戦略によって対処される脅威

(3) レガシーコード[1]に関連するリスクを含む、製品に関連する既知のセキュリティリスクへの製品使用者の緩和策

規則　X2.2.3-4.(4)

供給者は、多層防御対策の戦略を文書化するプロセスが、組織内に確立されていることを証明するための、マネジメントシステム文書を提示しなければならない。多層防御対策は、インストール、保守及び運用中に、コンピュータシステム内のソフトウェアに対するセキュリティ上の脅威の軽減を目的としている。脅威の例としては、認証されていないソフトウェアのインストール、パッチ適用プロセスの弱点、船舶の運用段階でのソフトウェアの改ざん等が考えられる。

解説

ここでは、製品の多層防御について述べています。

多層防御とは、一つのセキュリティ対策に依存するのではなく、複数のセキュリティ対策を組み合わせることで、セキュリティリスクを軽減する戦略です。

ここでの対応として、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プロセスを採用することが求められます。製品に関する文書には、以下の内容が含まれる必要があります。

・製品が実装するセキュリティ機能、また、多層防御の戦略におけるその役割

製品が提供する具体的なセキュリティ機能を明示し、それぞれが多層防御戦略においてどのように機能するかを説明します。

・多層防御の戦略によって対処される脅威

多層防御の戦略が対処する具体的な脅威を特定し、それぞれが製品のセキュリティ層にどのように影響を与えるかを説明します。驚異の例としては、要件で述べられているとおりです。

[1] **レガシーコード**　古い技術や手法を使用して作成されたプログラムのこと。これは、新しいセキュリティスタンダードに準拠していない、セキュリティパッチが適用できない等セキュリティ上のリスクを含む可能性がある。

・製品に関連する既知のセキュリティリスクを考慮した、製品使用者の低減策

既知のセキュリティリスクを軽減又は排除するための対策を説明します。特に、レガシーコードと呼ばれる古いソースコードを流用しているシステムでは、新しいセキュリティスタンダードに準拠していない、セキュリティパッチが適用できない等セキュリティ上のリスクを含む可能性があります。

また、上述のプロセスを組織内に確立する必要があります。立会検査では、このプロセスの確立をマネジメントシステム文書及び記録により証明することが求められます。

書類審査

■ セキュア開発ライフサイクル文書

	5. 製品の多層防御
□	-1. 次に掲げる項目を含む製品に関する文書を含む、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プロセスが採用されていること。
□	(1) 製品が実装するセキュリティ機能、また、多層防御の戦略におけるその役割
□	(2) 多層防御の戦略によって対処される脅威
□	(3) レガシーコードに関連するリスクを含む、製品に関連する既知のセキュリティリスクを考慮した、製品使用者の低減策

立会検査

■ セキュア開発ライフサイクル

	5. 製品の多層防御
□	-1. 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プロセスがマネジメントシステム文書に含まれていること。

6. 環境において期待される多層防御策

規則　X4.5.7　　参照　IEC62443-4-1 / SG-2

製品使用者に関する文書であって、製品が使用される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に関する多層防御の手段を記述したものを作成するプロセスが採用されなければならない。

規則　X2.2.3-4.(6)

供給者は、物理的配置、方針、手順のような、外部環境から提供されると期待される多層防御策を文書化するプロセスが、組織内に確立されていることを証明するための、マネジメントシステム文書を提示しなければならない。

解説

ここでは、外部の環境によって期待される多層防御策について述べています。ここでいう外部環境から提供されると思われる多層防御策とは、例えば以下のようなものが考えられます。

防御策	防御策の一例
物理的配置	施錠された扉やセキュリティボックスなど
方針	暗号化の使用、データの保存と破棄方法など
手順	重要なデータのバックアップ、データ喪失からのリカバリー手順など

ここでの対応として、製品が使用される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に関する多層防御の手段を記述したものを作成するプロセスを採用することが求められます。これは、製品によるセキュリティ対策以外に、外部のセキュリティ対策との組み合わせによる多層防御を構築する場合に重要となります。

また、上述のプロセスを組織内に確立する必要があります。立会検査では、このプロセスの確立をマネジメントシステム文書及び記録により証明することが求められます。

書類審査

■ セキュア開発ライフサイクル文書

	6.　環境において期待される多層防御策
□	-1.　製品使用者に関する文書であって、製品が使用される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に関する多層防御の手段を記述したものを作成するプロセスが採用されていること。

立会検査

■ セキュア開発ライフサイクル

	6. 環境において期待される多層防御策
□	-1. 製品使用者に関する文書であって、製品が使用される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に関する多層防御の手段を記述したものを作成するプロセスがマネジメントシステム文書に含まれていること。

7. セキュリティ強化指針

規則　X4.5.8　　参照　IEC62443-4-1 / SG-3

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[1]の指針を含むものを作成するプロセスが採用されなければならない。当該指針は、少なくとも、次に掲げるものに関する指示、根拠及び推奨事項を含むものでなければならない。

(1) 第三者のコンポーネントを含む製品とセキュリティコンテキストとの統合
(2) 製品のアプリケーションプログラミングインターフェース[2]／プロトコル[3]と、ユーザーアプリケーション[4]との統合
(3) 製品の多層防御[5]の戦略の適用及び維持
(4) ローカルセキュリティポリシーをサポートするセキュリティオプション／機能の設定及び使用、また、それぞれのセキュリティオプション／機能に関する次に掲げる事項
    (a) 製品の多層防御の戦略への貢献
    (b) 設定可能な値及びデフォルト値の記述であって、実用上の観点からそれぞれのもつ潜在的な影響によってセキュリティにどのような影響を及ぼすかを含むもの
    (c) 値の設定、変更及び削除
(5) セキュリティ関連のすべてのツール及びユーティリティの使用に関する指示及び推奨事項であって、製品のセキュリティの管理、監視、インシデント処理及び評価をサポートするもの
(6) 定期的なセキュリティ保守活動のための指示及び推奨事項
(7) 製品に関するセキュリティインシデントを供給者へ報告することについての指示
(8) 製品の保守及び管理に関するセキュリティ上のベストプラクティス[6]についての記述

規則　X2.2.3-4.(7)

供給者は、システムの強化指針が作成されることを保証するプロセスが、組織内に確立されていることを証明するため、マネジメントシステム文書を提示しなければならない。当該指針にあっては、不要なソフトウェア、アカウント、サービス等を削除／禁止又は無効化することにより、システムの脆弱性を低減する方法を明記しなければならない。

---

[1] **ハードニング**　攻撃対象領域を減らすことにより、システムの脆弱性を軽減する行為。

[2] **アプリケーションプログラミングインターフェース（API）**　ソフトウェアやアプリケーション間の情報交換を可能にする規則やプロトコル。

[3] **プロトコル**　ネットワーク上のコンピュータが通信するために使用する共通のルール及び信号の組合せ。例えば、HTTP や FTP、SMTP などが該当する。

[4] **ユーザーアプリケーション**　コンピュータにインストールされている、利用者の業務や目的に応じて作成されたプログラム。

[5] **多層防御**　一つのセキュリティ対策に依存するのではなく、複数のセキュリティ対策を組み合わせることで、セキュリティリスクを軽減する戦略。X 編では、「組織の役割及び複数の層にまたがる可変的な防壁を確立するための，人，技術及び運用機能を統合した情報セキュリティ戦略」と定義される。

[6] **ベストプラクティス**　セキュリティおよび産業界の慣習により一般的に推奨されると供給者が決定した、製品のセキュアな設計、開発、試験、保守に関する指針

解説

ここでは、製品のセキュリティハードニング指針について述べています。ハードニングとは、攻撃対象領域を減らすことにより、システムの脆弱性を軽減する行為を指します。例えば、不要なソフトウェア、アカウント、サービス等を削除するなどが該当します。

ここでの対応として、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プロセスを採用することが求められます。この指針には、以下の内容が含まれる必要があります。

・第三者のコンポーネントを含む製品とセキュリティコンテキストとの統合

セキュリティコンテキストは、システムやアプリケーションが実行されるセキュリティ環境を指します。具体的には、製品が物理的セキュリティや外部のファイアウォールの保護を必要とするかどうか、などです。外部のセキュリティ機能を含め環境を設計することで、その環境に適した多層防御戦略を策定することが可能になります。ここでの目的は、製品がセキュリティコンテキストに適合し，かつ，セキュリティコンテキストが製品に対して適切な保護を提供することです。ここで求められるプロセスとは、例えば、物理的セキュリティによりシステムへのアクセスを制限することや、外部のファイアウォールにより適切に通信を制限することなどが該当します。また，第三者のコンポーネントを含む場合は，そのコンポーネントが製品のセキュリティコンテキストに適合し，製品全体のセキュリティレベルを低下させてはいけません。

・製品のアプリケーションプログラミングインターフェース（API）／プロトコルと，ユーザーアプリケーションとの統合

製品の API やプロトコルは，製品の機能やデータをユーザーアプリケーションと共有するための仕組みです。API やプロトコルがユーザーアプリケーションと十分に統合されていない場合，認証や暗号化が不十分であることによって，攻撃者によってアクセスキーが盗まれたり，通信内容が傍受されたりするリスクがあります。そのため、製品が API やプロトコルを利用する場合、「ユーザーアプリケーションを API に安全に統合するための指示、根拠、および推奨事項」が含まれている必要があります。

・製品の多層防御の戦略の適用及び維持

多層防御は，適宜見直しや更新を行うことで，新たな脅威や脆弱性に対応できるように維持する必要があります。そのため、「多層防御に関する安全な運用と保守の指示」が含まれている必要があります。また、それらの指示は、多層防御の戦略を運用および維持する所有者の責任を説明しなければなりません。

・ローカルセキュリティポリシーをサポートするセキュリティオプション／機能の設定及び使用，また，それぞれのセキュリティオプション／機能に関する次に掲げる事項

ローカルセキュリティポリシーとは，製品が動作する利用者環境におけるセキュリティ要件や基準のことです。ここでの目的は、ローカルセキュリティポリシーをサポートするセキュリティオプションや機能により，ローカル環境に適合させることです。そのため、「セキュリティ設定オプション関する説明」が含まれている必要があります。具体的には以下のとおりです。

・製品の多層防御の戦略への貢献

それぞれのセキュリティオプションや機能は，製品の多層防御の戦略においてどのレイヤーでどのような役割を果たすかを明確にする必要があります。

・設定可能な値及びそのデフォルト値の記述

これは，セキュリティと可用性のバランスを考慮して選択し、その影響及び理由を説明する必要があります。

・値の設定、変更及び削除

値の設定、変更，削除等については、適切な権限や手順を遵守して行う必要があります。なお、セキュリティ構成の設定は、システム要件のひとつである「29 ネットワーク及びセキュリティ構成設定」によって、セキュリティ機能としてシステムに実装される必要があります。詳細は、「29 ネットワーク及びセキュリティ構成設定」に詳しく解説しております。

ネットワーク及びセキュリティ構成設定 P. 124

・セキュリティ関連のすべてのツール及びユーティリティに関する指示及び推奨事項であって、製品のセキュリティの管理、監視、インシデント処理及び評価をサポートするもの

セキュリティ関連のツールやユーティリティとは、製品のセキュリティを強化したり，問題を解決したりするために使用するソフトウェアや機器のことです。例えば、暗号化ツール、ログ分析ツール、バックアップツール、アンチウイルスソフトウェアなどがあります。これらのツールやユーティリティは、製品のセキュリティを効果的に管理し、監視し、インシデントに対応し，評価するために必要です。そのため、セキュリティツールやユーティリティが使用される場合、「これらのツールやユーティリティの使用方法の説明」が含まれている必要があります。

・定期的なセキュリティ保守活動のための指示及び推奨事項

定期的なセキュリティ保守活動とは、製品のセキュリティを維持するために行う作業のことです。例えば、パッチ及びアップデートの適用，ログ及びバックアップファイルの確認及び削除、パスワード及び証明書の更新などがあります。定期的なセキュリティ保守活動は、製品に対する新たな脅威や脆弱性に対応し、製品のセキュリティを向上させるために必要です。そのため、「定期的なセキュリティ保守活動の方法の説明、推奨事項」が含まれている必要があります。

・製品に関するセキュリティインシデントを供給者へ報告することについての指示

製品に関するセキュリティインシデントは、製品の可用性に影響を与える可能性があります。供給者へ報告することで、インシデントの原因や影響範囲を調査し、適切な対策や改善策を実施することができます。そのために、「セキュリティインシデントの供給者への報告する手順」が含まれている必要があります。

・製品の保守及び管理に関するセキュリティ上のベストプラクティスについての記述

製品の保守及び管理に関するセキュリティ上のベストプラクティスとは、製品の安全な運用と維持を支援するための推奨される手順や方針です。例えば、アップデートやパッチ適用などが挙げられます。ここでの目的は、これらのベストプラクティスを遵守することで、製品のセキュリティ状態を維持し、脆弱性や攻撃から保護することです。そのため、「製品を安全に管理するためのベストプラクティスの説明」が含まれている必要があります。

また、上述のプロセスを組織内に確立する必要があります。立会検査では、このプロセスの確立をマネジメントシステム文書及び記録により証明することが求められます。

書類審査

■ セキュア開発ライフサイクル文書

	7. セキュリティ強化指針
☐	-1. 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プロセスが採用されていること。
☐	また、次に掲げるものに関する指示、根拠及び推奨事項が含まれていること。
☐	(1) 第三者のコンポーネントを含む製品とセキュリティコンテキストとの統合
☐	(2) 製品のアプリケーションプログラミングインターフェース／プロトコルと、ユーザーアプリケーションとの統合
☐	(3) 製品の多層防御の戦略の適用及び維持
☐	(4) ローカルセキュリティポリシーをサポートするセキュリティオプション／機能の設定及び使用、また、それぞれのセキュリティオプション／機能に関する次に掲げる事項
☐	(a) 製品の多層防御の戦略への貢献
☐	(b) 設定可能な値及びそのデフォルト値の記述であって、それぞれがセキュリティにどのように作用して、実用上どのような影響を及ぼし得るかを含むもの
☐	(c) 値の設定、変更及び削除
☐	(5) セキュリティ関連のすべてのツール及びユーティリティの使用に関する指示及び推奨事項であって、製品のセキュリティの管理、監視、インシデント処理及び評価をサポートするもの
☐	(6) 定期的なセキュリティ保守活動のための指示及び推奨事項
☐	(7) 製品に関するセキュリティインシデントを供給者へ報告することについての指示

□	(8) 製品の保守及び管理に関するセキュリティ上のベストプラクティスについての記述

立会検査

■ セキュア開発ライフサイクル

	7. セキュリティ強化指針
□	-1. 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プロセスがマネジメントシステム文書に含まれていること。

参考文献

(1) IACS Unified Requirements, E26 (April 2022) Cyber resilience of ships

(2) IACS Unified Requirements, E27 (Rev.1) (September 2023) Cyber resilience of on-board systems and equipment

(3) IEC TS 62443-1-1: 2009 Terminology, concepts and models

(4) IEC 62443-3-3: 2013 System security requirements and security levels

(5) IEC 62443-4-1: 2018 Secure product development lifecycle requirements

付録 1 書類審査チェックリスト

製造者　　：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

型式　　：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

製造No.　　：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

提出資料

	1. コンピュータシステム資産インベントリ
☐	-1. 次に掲げる事項が含まれていること。
☐	(1) ハードウェアコンポーネントリスト
☐	(a) 名称
☐	(b) ブランド／製造者
☐	(c) モデル／型式
☐	(d) 機能／目的の簡潔な説明
☐	(e) 物理的インターフェース
☐	(f) システムソフトウェアの名称／型式
☐	(g) システムソフトウェアのバージョン及びパッチレベル
☐	(2) ソフトウェアコンポーネントリスト
☐	(a) ソフトウェアがインストールされているハードウェアコンポーネント
☐	(b) ブランド／製造者
☐	(c) モデル／型式
☐	(d) 機能／目的の簡潔な説明
☐	(e) ソフトウェアのバージョン
☐	(f) 対応している通信プロトコル

	2. トポロジー図
☐	-1. 次に掲げる事項が含まれていること。
☐	(1) 物理トポロジー図
☐	(a) 全てのエンドポイントおよびネットワーク機器（冗長化されたユニットの識別を含む）
☐	(b) I/O ユニットとの通信を含む通信ケーブル（ネットワーク，シリアルリンク等）
☐	(c) その他のネットワーク，又は，システムとの通信ケーブル

☐	(2) 論理トポロジー図
☐	(a) 通信エンドポイント（ワークステーション，コントローラー，サーバー等）
☐	(b) ネットワーク機器（スイッチ，ルーター，ファイアウォール等）
☐	(c) 物理コンピュータ及び仮想コンピュータ
☐	(d) 物理通信経路と仮想通信経路
☐	(e) 通信プロトコル

	3. セキュリティ機能の説明
☐	-1. 次に掲げる事項が含まれていること。
☐	(1) セキュリティ機能及び補完的対策
☐	(a) 詳細は、ガイドライン 5 章「システム要件の詳細」を確認すること。
☐	(2) ネットワークインターフェイス
☐	(a) X 編 4 章（UR E27）の適用範囲内のネットワーク
☐	(b) 信頼できないネットワーク
☐	セキュリティゾーン境界の保護を担うコンポーネントについて、システムの一部として納入されるかどうかについて詳細が記載されていること。
☐	(3) 要求事項への準拠を確認するために必要な補足資料

	4. セキュリティ機能の試験方案
☐	-1. 次に掲げる事項が含まれていること。
☐	(1) セキュリティ機能の実証試験及び補完的対策の確認
☐	各要件の詳細は、ガイドライン 5 章「システム要件の詳細」を確認すること。
☐	(a) 必要な試験条件
☐	(b) 試験機器
☐	(c) 初期条件
☐	(d) 試験手法，詳細な試験手順
☐	(e) 期待される試験結果及び合格基準
☐	(f) 試験結果及び所見の記入欄

	5. セキュリティ構成指針
☐	-1. 次に掲げる事項が含まれていること。
☐	(1) セキュリティ機能の推奨設定に関する説明
☐	(2) 特定されたデフォルト値

	6. セキュア開発ライフサイクル文書
☐	-1. 次に掲げる事項が含まれていること。
☐	(1) セキュリティ面をどのように扱ったかの記録

☐	次に掲げる段階において、記録した文章を作成すること。
☐	(a)　要件分析段階
☐	(b)　設計段階
☐	(c)　実装段階
☐	(d)　検証段階
☐	(e)　リリース段階
☐	(f)　保守段階
☐	(g)　終了段階
☐	(2)　セキュア開発ライフサイクルに関するプロセス及び管理
☐	詳細は、「ガイドライン 6 章　セキュア開発ライフサイクルに関する要件の詳細」を確認すること。
☐	(3)　ソフトウェアの更新及びパッチの適用

	7.　コンピュータシステムの保守及び検証のための計画
☐	-1.　次に掲げる事項が含まれていること。
☐	(1)　セキュリティ機能の推奨設定に関する説明
☐	(2)　セキュリティ機能のあるべき動作をユーザーが確認する方法
	システム要件「19 セキュリティ機能の検証」によって実装された機能が含まれていること。

	8.　就航後のインシデント対応とリカバリープランをサポートする情報
☐	-1.　次に掲げる手順又は指示が含まれていること。
☐	(1) ローカル独立制御
☐	(2) ネットワークの分離
☐	(3) 監査記録によるフォレンジック
☐	(4) あらかじめ決定した出力
☐	(5) バックアップ
☐	(6) 復旧
☐	(7) 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

	9.　計画の変更に関する管理
☐	-1.　サイバーセキュリティに関する変更管理手順が含まれていること。ただし、X 編 3 章で要求される変更管理手順書が提出されている場合はこの限りではない。

	10.　試験結果
☐	-1.　次に掲げる検査項目が含まれていること。
☐	(1) 一般的な検査項目

☐	(2) セキュリティ機能試験
☐	(3) セキュリティ機能の正確な設定
☐	(4) セキュア開発ライフサイクル
☐	(5) インストール時におけるハードニング
☐	-2. 供給者による署名が含まれていること。

システム要件

■ セキュリティ機能の説明

	1. 使用者（人）の識別と認証
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 使用者（人）を識別及び認証する機能
☐	(a) 識別子によって識別すること。
☐	(b) 識別子および認証コードによって認証すること。
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	2. アカウントの管理
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) アカウントを管理する機能
☐	(a) 次に掲げる機能を実装していること。
☐	i) アカウントの追加、変更及び削除
☐	ii) アカウントの有効化及び無効化（補完的対策をとる場合は、その理由）
☐	(b) 権限を有する使用者のみが、アカウントを管理できること。
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	3. 識別子の管理
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 使用者、グループ及び役割による識別子の管理をサポートする機能

☐	識別子を追加、変更及び削除すること。
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	4. 認証コードの管理
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 認証コードを管理する機能
☐	次に掲げる機能を実装していること。
☐	(a) 認証コードの初期化（例：パスワードの初期化）
☐	(b) システムのインストール時にデフォルトの認証コードの強制変更（例：初期パスワードからの変更）
☐	(c) すべての認証コードの変更や更新（例：パスワードの変更）
☐	(d) 保存や伝送されるすべての認証コードについて、不正開示および変更からの保護（例：パスワードの暗号化）
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	5. 無線アクセスの管理
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 無線通信を行うすべての使用者を識別、認証する機能
☐	(a) 人の識別と認証
☐	i) 識別子によって識別すること。
☐	ii) 識別子および認証コードによって認証すること。
☐	(b) ソフトウェアプロセスの識別と認証
☐	i) 識別子によって識別すること。
☐	ii) 識別子および認証コードによって認証すること。
☐	(c) デバイスの識別と認証
☐	i) 識別子によって識別すること。
☐	ii) 識別子および認証コードによって認証すること。
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。

☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	6. パスワードによる認証の強度
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) パスワードの設定を強化する機能
☐	(a) 最短の長さ
☐	対策に掲げた指針等に基づいて決定されたものであること
☐	(b) 文字の種類の多様性
☐	対策に掲げた指針等に基づいて決定されたものであること
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	7. 認証時のフィードバック
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 認証プロセス中のフィードバックを不明瞭とする機能
☐	入力中のパスワードが非表示であること。
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	8. 権限付与の実施
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 職務分離及び最小特権の原則に従って権限を割り当てることをサポートする機能
☐	アクセス制御リスト等により、次に掲げる要素が管理されていること
☐	(a) 主体 (Subject)（例：グループベースを含むすべての使用者）
☐	(b) 対象 (Object)（例：ファイル、データベース、ネットワークリソース）
☐	(c) 権限 (Permission)（例：読み取り、書き込み、実行）
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。

☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	9. 無線の使用の管理
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) システムへの無線接続の認可、監視及び使用制限を実施する機能
☐	(a) 一般的に受け入れられるセキュリティに関する業界の慣行に従って、次に掲げる機能が実装されること
☐	i) 認可
☐	ii) 監視
☐	iii) 使用制限
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	10. 可搬式及び携帯用デバイスの使用の管理
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 可搬式及び携帯用デバイスの使用制限及び転送制限の機能
☐	(a) 可搬式及び携帯用デバイスの使用制限
☐	許可されたデバイスが使用できること
☐	(b) 可搬式及び携帯用デバイスの転送制限
☐	デバイスのコード及びデータの転送が制限されていること
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	11. モバイルコード
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) モバイルコードの使用を制御する機能
☐	(a) モバイルコードの使用を制御できること（例：ブラウザを削除する、ポリシーの設定でモバイルコードの動作を禁止する）
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。

☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	12. セッションロック
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 自動または手動いずれかのセッションロックの機能
☐	(a) 自動によるセッションロックについては、以下を確認すること：
☐	i) 無操作時間の経過後にセッションがロックされること
☐	ii) 無操作時間が設定できること
☐	(b) 手動によるセッションロックについては、以下を確認すること：
☐	i) 手動によりセッションがロックされること
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	13. 監査可能な事象
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 重要な事象の監査記録を作成する機能の機能
☐	(a) 次に掲げる事象の監査記録が作成できること。
☐	i) アクセス制御
☐	ii) オペレーティングシステムのイベント
☐	iii) バックアップと復元
☐	iv) 設定変更
☐	v) 通信の喪失
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	14. 監査用の記憶容量
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 監査記録の記憶容量をログ管理に関する一般的に認識された推奨に従って割り当てる機能

☐	(a) ログ管理の一般的な推奨事項に基づいていること（例：NIST SP800-92）。
☐	(b) 容量を超過する可能性を下げるような監査の仕組みであること。
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	15. 監査プロセスへの不具合の対応
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 監査プロセスの不具合発生時に、不可欠なサービス及び機能の喪失を防ぐ機能
☐	(a) 監査プロセスの不具合発生時に、不可欠なサービス及び機能が喪失しないこと（例：監査に関わる機能と不可欠な機能を分離する）
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	16. 日時の記録
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 監査記録に日時を記録する機能
☐	(a) 監査記録にタイムスタンプが付与されること（例：リアルタイムクロック IC、システムクロック等）
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	17. 通信の完全性
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 伝送される情報の完全性を保護する機能
☐	(a) 次に掲げる機能が実装されていること
☐	i) 受信データと送信データに相違がある場合、送信元にデータの再送を要求する機能
☐	ii) 受信データと送信データの相違が続いた場合、警報を発する機能

☐	(b) 無線通信を行う場合、伝送される情報の暗号化の仕組みとなっていること
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	18. 悪意のあるコードからの保護
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 悪意のあるコードや不正なソフトウェアによる影響を防止、検知及び低減するための適切な保護手段を実行する機能
☐	(a) 次に掲げる機能が実装されていること
☐	i) マルウェアによる影響を防止するための機能（例：アプリケーションのホワイトリスト制限、リムーバブルメディアの実行制限、サンドボックス機能）
☐	ii) マルウェアによる影響を検知するための機能があること（例：侵入検知システム(IDS)、アンチマルウェアスキャン）
☐	iii) マルウェアによる影響を低減するための機能があること（例：ファイルの削除、感染端末の隔離）
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	19. セキュリティ機能の検証
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) セキュリティ機能のあるべき動作の検証をサポートし、また、保守中に発生した異常を報告する機能
☐	(a) セキュリティ機能の動作検証を行う機能
☐	実装されたセキュリティ機能の動作が検証できること
☐	(b) 保守中に発生した異常を報告する機能
☐	保守中に検知した異常が報告されること（例：ウイルス対策ソフトを導入している場合、ウイルスやマルウェアの識別コードやパターンの更新に失敗した時にメッセージが出力される等）
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。

☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	20. あらかじめ決定した出力
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) 出力をあらかじめ指定した状態に設定する機能の詳細
☐	出力について、少なくとも次に掲げるいずれかの状態へ変更できること
☐	(a) 非使用時の状態
☐	(b) 最後の正常値、または固定値
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	21. 情報の機密性
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 読取りに関して明示的な承認が求められる情報について、保管時であるか伝送中であるかにかかわらず、機密性を保護する機能
☐	(a) 次に掲げる機能を確認すること
☐	i) 保管時に情報の機密性を保護する機能
☐	ii) 伝送中に情報の機密性を保護する機能
☐	(b) 無線通信を使用する場合、のすべての情報の機密性を保護するために、暗号化の仕組みが採用されていること。
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	22. 暗号の使用
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの仕組み又は対策を設けること。
☐	(1) 一般に受け入れられるセキュリティに関する業界の慣行及び推奨に従って、暗号アルゴリズム、鍵の長さ及び仕組み
☐	次に掲げるものが、一般に受け入れられるセキュリティに関する業界の慣行及び推奨に従っていること。
☐	(a) 暗号アルゴリズム
☐	(b) 鍵の長さ
☐	(c) 鍵の仕組み

☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	23. 監査ログへのアクセス
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 権限を有する人及び／又はツールによる読取り専用での監査ログへのアクセスの機能
☐	(a) 権限を有する人及び／又はツールが監査ログへアクセスできること
☐	(b) 監査ログへのアクセスは読み取り専用であること。
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	24. サービス拒否攻撃からの保護
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの仕組み又は対策を設けること。
☐	(1) DoS 事象発生中にも、不可欠な機能を維持するための最小限の機能
☐	DoS 事象中に、不可欠な機能が維持されていること（例：通信処理プロセスの優先順位を低くする等）
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	25. リソースの管理
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) リソースを使い果たさないように、セキュリティ機能によるリソースの利用を制限する機能
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。

☐	(d) 新たなセキュリティリスクを発生させないこと。

	26. システムのバックアップ
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 復旧すべき重要なファイルをバックアップする機能
☐	(a) システムの復旧に必要となるデータがバックアップされること
☐	(b) 通常の運用に影響しないこと
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	27. システムの復旧及び再構成
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 混乱又は故障の後、既知の保護された状態に復旧及び再構成される機能 次に掲げる事象を達成する機能であること。なお、この機能によって、すべて事象を達成する必要はない。
☐	(a) システムパラメータがデフォルト又は安全な値であること
☐	(b) セキュリティに関する重要なパッチが再インストールされること
☐	(c) セキュリティに関する設定が再確認、再設定されていること
☐	(d) システム文書及び操作手順が使用可能な状態であること
☐	(e) アプリケーション及びシステムソフトウェアが安全な設定で再インストールされること
☐	(f) バックアップデータから情報が復元されていること
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	28. 代替電源
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 既存のセキュリティ状態又は文書化された縮退モードに影響することなく、代替電源へ及び代替電源から切り替える機能
☐	次に掲げる状態に影響することなく、代替電源へ及び代替電源から切り替えること
☐	(a) 既存のセキュリティ状態

☐	(b) 文書化された縮退モード
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	29. ネットワーク及びセキュリティ構成設定
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 供給者によって提供される指針にて推奨されるネットワーク及びセキュリティ構成に従って設定される機能
☐	次に掲げるものを設定できること
☐	(a) ネットワーク構成
☐	(b) セキュリティ構成
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	30. 最小限の機能性
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの事項又は対策を設けること。
☐	(1) 最小限の機能性
☐	次に掲げるものの「インストール、可用性及びアクセス権」の機能を必要最小限とすること
☐	(a) オペレーティングシステムソフトウェアのコンポーネント、プロセス及びサービス
☐	(b) ネットワークサービス、ポート、プロトコル、ルート及びホストへのアクセス並びにすべてのソフトウェア
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	31. 使用者（人）の多要素認証
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの事項又は対策を設けること。
☐	(1) 使用者（人）に対する多要素認証の機能

☐	(a) 異なる 2 つ以上の要素により認証されること
☐	(b) 正規の認証コードを使用した場合、ログインが可能であること
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	32. ソフトウェアプロセス及びデバイスの識別及び認証
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) ソフトウェアプロセス及びデバイスを識別及び認証する機能
☐	(a) ソフトウェアプロセスの識別と認証
☐	i) 識別子によって識別すること。
☐	ii) 識別子および認証コードによって認証すること。
☐	(b) デバイスの識別と認証
☐	i) 識別子によって識別すること。
☐	ii) 識別子および認証コードによって認証すること
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	33. 失敗したログイン試行
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 連続した無効なログイン試行を制限する機能
	次に掲げる項目に適合すること。
☐	(a) 連続した無効なログイン試行が設定された試行回数を超えた場合、アクセスを拒否すること
☐	(b) 拒否されたアクセスは、指定された期間または管理者によってロック解除されるまで続くこと
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	34. システム使用通知
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) システム使用通知メッセージを表示及び編集する機能
☐	次に掲げる機能を実装していること。
☐	(a) システム使用通知メッセージを表示する機能
☐	認証前にシステム使用通知メッセージが表示されること。
☐	(b) システム使用通知メッセージを編集する機能
☐	権限を有する人員によって編集できること。
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	35. 信頼できないネットワーク経由のアクセス
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 信頼できないネットワークを経由するアクセスを監視及び制御する機能
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	36. アクセス要求の明示的な承認
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 承認権限を有する使用者（人）により明示的に承認された場合を除き、信頼できないネットワークから又は当該ネットワークを経由したアクセスを拒否する機能
☐	(a) 使用者（人）に対して、アクセスの承認権限を割り当てる機能
☐	(b) 承認されていないアクセスを拒否する機能
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	37. リモートセッションの終了
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。

☐	(1) リモートセッションを終了する機能
☐	次に掲げる機能のいずれかを実装していること。
☐	(a) 自動でリモートセッションを終了する機能
☐	次に掲げる項目に適合していること。
☐	i) セッションが終了する無操作時間を設定すること。
☐	ii) 設定可能な無操作時間の経過後にセッションが終了すること。
☐	(b) 手動でリモートセッションを終了する機能
☐	使用者の操作によってセッションが終了すること。
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	38. 暗号化による完全性の保護
☐	-1. 本要件が適用される場合､次の(1)又は(2)いずれかの仕組み又は対策を設けること。
☐	(1) 信頼できないネットワークとの又は当該ネットワークを経由した通信中における情報の変更を認識するための暗号化の仕組み
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	39. 入力の検証
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 入力データを検証する機能
☐	(a) 次に掲げる入力データの要素を検証すること。
☐	i) 構文
☐	ii) 長さ
☐	iii) 内容
☐	(b) 無効なデータと判断した場合、適切に対応すること。(例：入力データの受取りを拒否する等)
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。

☐	(d) 新たなセキュリティリスクを発生させないこと。

	40. セッションの完全性
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) セッションの完全性を保護し、無効なセッション ID の使用を拒否する機能
☐	次に掲げる項目に適合すること
☐	(a) セッションの完全性を保護すること
☐	(b) 無効なセッション ID の使用を拒否すること
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	41. セッション終了後のセッション ID の無効化
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 使用者のログアウト又はブラウザセッションを含むセッション終了後、セッション ID を無効化する機能
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

セキュア開発ライフサイクルに関する要件

■ セキュア開発ライフサイクル文書

	1. 秘密鍵の管理
☐	-1. 電子署名されたソフトウェアがシステムに含まれている場合、次に掲げる管理策が保有されていること。
☐	(1) 秘密鍵の手順上の管理策（例：生成、保管及び使用の手順等）
☐	(2) 秘密鍵の技術上の管理策（例：物理的なアクセス制限や暗号化ハードウェア等）

	2. セキュリティアップデートの文書
☐	-1. 次に掲げる項目を含むセキュリティアップデートの文書が使用者に入手可能となることを確保するプロセスが採用されていること。

☐	(1)	セキュリティパッチが適用される製品のバージョン番号
☐	(2)	承認されたパッチの手動及び自動プロセス経由による適用方法に関する説明
☐	(3)	製品にパッチを適用することで発生する可能性のある影響（再起動を含む）の記述
☐	(4)	承認されたパッチが適用されたことの確認方法に関する説明
☐	(5)	パッチを適用しないこと並びに資産所有者が承認又は導入しないパッチに使用できるメディエーションに関するリスク

	3.	**依存コンポーネント又はオペレーティングシステムのセキュリティアップデート文書**
☐	-1.	次に掲げる項目を含む依存コンポーネント又はオペレーティングシステムのセキュリティアップデートに関する文書をシステム所有者が入手するためのプロセスを採用されていること。
☐		製品が，依存するコンポーネントに又はオペレーティングシステムのセキュリティアップデートに対応しているかどうかの記載

	4.	**セキュリティアップデートの配信**
☐	-1.	セキュリティパッチが真正であることを確認できる方法によって、システム所有者がセキュリティアップデートを入手するためのプロセスが採用されていること。
	-2.	セキュリティアップデートのリリース前に更新を試験するための QA プロセスが採用されていること。

	5.	**製品の多層防御**
☐	-1.	次に掲げる項目を含む製品に関する文書を含む、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プロセスが採用されていること。
☐	(1)	製品が実装するセキュリティ機能、また、多層防御の戦略におけるその役割
☐	(2)	多層防御の戦略によって対処される脅威
☐	(3)	レガシーコードに関連するリスクを含む、製品に関連する既知のセキュリティリスクを考慮した、製品使用者の低減策

	6.	**環境において期待される多層防御策**
☐	-1.	製品使用者に関する文書であって、製品が使用される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に関する多層防御の手段を記述したものを作成するプロセスが採用されていること。

	7.	**セキュリティ強化指針**
☐	-1.	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

		を作成するプロセスが採用されていること。
□		また、次に掲げるものに関する指示、根拠及び推奨事項が含まれていること。
□	(1)	第三者のコンポーネントを含む製品とセキュリティコンテキストとの統合
□	(2)	製品のアプリケーションプログラミングインターフェース／プロトコルと、ユーザーアプリケーションとの統合
□	(3)	製品の多層防御の戦略の適用及び維持
□	(4)	ローカルセキュリティポリシーをサポートするセキュリティオプション／機能の設定及び使用、また、それぞれのセキュリティオプション／機能に関する次に掲げる事項
□		(a) 製品の多層防御の戦略への貢献
□		(b) 設定可能な値及びそのデフォルト値の記述であって、それぞれがセキュリティにどのように作用して、実用上どのような影響を及ぼし得るかを含むもの
□		(c) 値の設定、変更及び削除
□	(5)	セキュリティ関連のすべてのツール及びユーティリティに関する指示及び推奨事項であって、製品のセキュリティの管理、監視、インシデント処理及び評価をサポートするもの
□	(6)	定期的なセキュリティ保守活動のための指示及び推奨事項
□	(7)	製品に関するセキュリティインシデントを供給者へ報告することについての指示
□	(8)	製品の保守及び管理に関するセキュリティ上のベストプラクティスについての記述

付録 2 立会検査チェックリスト

製造者　　：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

型式　　：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

製造No.　　：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

立会検査

	1. 一般的な検査項目
□	-1. 事前に準備される書類について、次に掲げる資料を確認すること。
□	(1) コンピュータシステム資産インベントリ
□	(2) トポロジー図
□	-2. 次に掲げる検査を実施すること。
□	(1) 書類確認
□	(a) 設計が完了したことを示す記録
□	(b) 製造が完了したことを示す記録
□	(c) 社内試験が完了したことを示す記録
□	(2) 外観検査
□	(a) システムの構成
□	コンピュータシステム資産インベントリ及びトポロジー図と比較すること

	2. セキュリティ機能試験
□	-1. 事前に準備される書類について、次に掲げる資料を確認すること。
□	セキュリティ機能の試験方案
□	-2. 次に掲げる検査を実施すること。
□	システム要件に適合していること。 詳細は、ガイドライン 5 章「システム要件の解説」を確認すること。

	3. セキュリティ機能の正確な設定
□	-1. 事前に準備される書類について、次に掲げる資料を確認すること
□	セキュリティ構成指針
□	-2. 次に掲げる検査を実施すること。
□	ネットワーク及びセキュリティ構成設定の要件に適合すること。 詳細は、ガイドライン 5 章「システム要件の詳細」中「ネットワーク及びセキュ

	リティ構成設定」により確認できる。

	4. セキュア開発ライフサイクル
□	-1. 事前に準備される書類について、次に掲げる資料を確認すること
□	セキュア開発ライフサイクル文書
□	-2. 次に掲げる検査を実施すること。
□	セキュア開発ライフサイクルの要件に適合していること。 詳細は、ガイドライン 6 章「セキュア開発ライフサイクルに関する要件の詳細」により確認できる。

システム要件

■ セキュリティ機能試験

	1. 使用者（人）の識別と認証
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
□	(1) 使用者（人）を識別及び認証する機能の実証試験
□	(c) 正規の識別子及び認証コードでログインできること。
□	(d) 非正規の識別子及び／又は認証コードでログインできないこと。
□	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	2. アカウントの管理
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
□	(1) アカウントを管理する機能の実証試験
□	(a) 次に掲げる機能が動作すること。
□	i) アカウントの追加、変更及び削除
□	ii) アカウントの有効化及び無効化
□	(b) アカウントの管理権限について、次のとおりであること。
□	i) 権限を有する使用者のみが、アカウントを管理できること。
□	ii) 権限を有していない使用者が、アカウントを管理できないこと。
□	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	3. 識別子の管理
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
□	(1) 使用者、グループ及び役割による識別子の管理をサポートする機能の実証試験
□	識別子を追加、変更及び削除すること。
□	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	4. 認証コードの管理
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
□	(1) 認証コードを管理する機能の実証試験
□	次に掲げる機能の動作を確認すること。
□	(a) 認証コードの初期化（例：パスワードの初期化）
□	(b) システムのインストール時にデフォルトの認証コードの強制変更（例：初期パスワードからの変更）
□	(c) すべての認証コードの変更や更新（例：パスワードの変更）
□	(d) 保存や伝送されるすべての認証コードについて、不正開示および変更からの保護（例：パスワードの暗号化）
□	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	5. 無線アクセスの管理
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
□	(1) 無線通信を行うすべての使用者を識別、認証する機能の実証試験
□	(a) 人の識別と認証
□	i) 正規の識別子および認証コードによってログインできること。
□	ii) 非正規の識別子および認証コードによってログインできないこと。
□	(b) ソフトウェアプロセスの識別と認証
□	i) 正規の識別子および認証コードによってログインできること。
□	ii) 非正規の識別子および認証コードによってログインできないこと。
□	(c) デバイスの識別と認証
□	i) 正規の識別子および認証コードによってログインできること。
□	ii) 非正規の識別子および認証コードによってログインできないこと。
□	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	6. パスワードによる認証の強度
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
□	(1) パスワードの設定を強化する機能の実証試験
□	(a) 最短の長さ
□	次に掲げる項目に適合すること。
□	i) 決定された最短の長さ以上で、パスワードが設定できること。
□	ii) 決定された最短の長さ未満で、パスワードが設定できないこと。
□	(b) 文字の種類の多様性
□	決定された文字の種類で、パスワードが設定できること。
□	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	7. 認証時のフィードバック
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
□	(1) 認証プロセス中のフィードバックを不明瞭とする機能の実証試験
□	入力中のパスワードが非表示であること。
□	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	8. 権限付与の実施
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
□	(1) 職務分離及び最小特権の原則に従って権限を割り当てることをサポートする機能
□	アクセス制御リスト等により、次に掲げる要素が職務分離及び最小特権の原則に従って管理されていること
□	(a) 主体（Subject）（例：グループベースを含むすべての使用者）
□	(b) 対象（Object）（例：ファイル、データベース、ネットワークリソース）
□	(c) 権限（Permission）（例：読み取り、書き込み、実行）
□	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	9. 無線の使用の管理
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
□	(1) システムへの無線接続の認可、監視及び使用制限を実施する機能
□	(a) 一般的に受け入れられるセキュリティに関する業界の慣行に従って、次に掲

	げる機能が実装されること
□	i) 認可
□	ii) 監視
□	iii) 使用制限
□	(2) 補完的対策
□	(a) 本要件と同じ脅威から保護すること。
□	(b) 本要件と同等の厳しさ，正確さであること。
□	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
□	(d) 新たなセキュリティリスクを発生させないこと。

	10. 可搬式及び携帯用デバイスの使用の管理
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
□	(1) 可搬式及び携帯用デバイスの使用制限及び転送制限の機能の実証試験
□	(a) 可搬式及び携帯用デバイスの使用制限
□	次に掲げる項目に適合すること。
□	i) 許可されたデバイスが使用できること。
□	ii) 許可されないデバイスが使用できないこと。
□	(b) 許可されないデバイスが使用できないこと
□	デバイスのコード及びデータの転送が制限されていること
□	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	11. モバイルコード
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
□	(1) モバイルコードの使用を制御する機能
□	(a) モバイルコードの使用を制御できること（例：ブラウザを削除する、ポリシーの設定でモバイルコードの動作を禁止する）
□	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	12. セッションロック
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
□	(1) 自動または手動いずれかのセッションロックの機能の実証試験
□	(a) 自動によるセッションロックについては、以下を確認すること：
□	i) 無操作時間の経過後にセッションがロックされること
□	ii) 無操作時間が設定できること

☐	(b) 手動によるセッションロックについては、以下を確認すること：
☐	i) 手動によりセッションがロックされること
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	13. 監査可能な事象
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) 重要な事象の監査記録を作成する機能の実証試験
☐	(a) 次に掲げる事象の監査記録が作成できることを確認すること。
☐	i) 次に掲げる事象の監査記録が作成できること。
☐	ii) アクセス制御
☐	iii) オペレーティングシステムのイベント
☐	iv) バックアップと復元
☐	v) 設定変更
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	14. 監査用の記憶容量
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) 監査記録の記憶容量をログ管理に関する一般的に認識された推奨に従って割り当てる機能の実証試験
☐	(a) ログ管理の一般的な推奨事項に基づいていること（例：NIST SP800-92）。
☐	(b) 容量を超過する可能性を下げるような監査の仕組みであること。
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	15. 監査プロセスへの不具合の対応
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) 監査プロセスの不具合発生時に、不可欠なサービス及び機能の喪失を防ぐ機能の実証試験
☐	(a) 監査プロセスの不具合発生時に、不可欠なサービス及び機能が喪失しないこと（例：監査に関わる機能と不可欠な機能を分離する）
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	16. 日時の記録
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
□	(1) 監査記録に日時を記録する機能の実証試験
□	(a) 監査記録にタイムスタンプが付与されること（例：リアルタイムクロック IC、システムクロック等）
□	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	17. 通信の完全性
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
□	(1) 伝送される情報の完全性を保護する機能の実証試験
□	(a) 次に掲げる機能があること
□	i) 受信データと送信データに相違がある場合、送信元にデータの再送を要求する機能
□	ii) 受信データと送信データの相違が続いた場合、警報を発する機能
□	(b) 無線通信を行う場合、伝送される情報の暗号化の仕組みとなっていること
□	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	18. 悪意のあるコードからの保護
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
□	(1) 伝送される情報の完全性を保護する機能の実証試験
□	(a) 次に掲げる機能が実装されていること
□	i) マルウェアによる影響を防止するための機能（例：アプリケーションのホワイトリスト制限、リムーバブルメディアの実行制限、サンドボックス機能）
□	ii) マルウェアによる影響を検知するための機能があること（例：侵入検知システム(IDS)、アンチマルウェアスキャン）
□	iii) マルウェアによる影響を低減するための機能があること（例：ファイルの削除、感染端末の隔離）
□	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	19. セキュリティ機能の検証
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならな

	い。
☐	(1) セキュリティ機能のあるべき動作の検証をサポートし、また、保守中に発生した異常を報告する機能
☐	(a) セキュリティ機能の動作検証を行う機能
☐	i) 実装されたセキュリティ機能の動作が検証できること
☐	(b) 保守中に発生した異常を報告する機能
☐	i) 保守中に検知した異常が報告されること（例：ウイルス対策ソフトを導入している場合、ウイルスやマルウェアの識別コードやパターンの更新に失敗した時にメッセージが出力される等）
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	20. あらかじめ決定した出力
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) 出力をあらかじめ指定した状態に設定する機能の詳細
☐	出力について、少なくとも次に掲げるいずれかの状態へ変更できること
☐	(a) 非使用時の状態
☐	(b) 最後の正常値、または固定値
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	21. 情報の機密性
	立会試験は不要

	22. 暗号の使用
	立会試験は不要

	23. 監査ログへのアクセス
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) 出力をあらかじめ指定した状態に設定する機能
☐	(a) 次に掲げる項目に適合すること。
☐	i) 権限を有する人及び／又はツールが監査ログへアクセスできること。
☐	ii) 権限を有しない人及び／又はツールが監査ログへアクセスできないこと。
☐	(b) 監査ログへのアクセスは読み取り専用であること。
☐	(2) 補完的対策の確認

	セキュリティ機能の説明に記載されるとおりであること。

	24. サービス拒否攻撃からの保護
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) DoS 事象発生中にも、不可欠な機能を維持するための最小限の機能
☐	DoS 事象中に、不可欠な機能が維持されていること（例：DoS 攻撃のシミュレーション試験の結果確認）
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	25. リソースの管理
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) リソースを使い果たさないように、セキュリティ機能によるリソースの利用を制限する機能の実証試験
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	26. システムのバックアップ
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの機能又は対策を設けること。
☐	(1) 復旧すべき重要なファイルをバックアップする機能
☐	(a) システムの復旧に必要となるデータがバックアップされること
☐	(b) 通常の運用に影響しないこと
☐	(2) 補完的対策
☐	(a) 本要件と同じ脅威から保護すること。
☐	(b) 本要件と同等の厳しさ，正確さであること。
☐	(c) 他の要求事項により要求されるセキュリティ管理ではないこと。
☐	(d) 新たなセキュリティリスクを発生させないこと。

	27. システムの復旧及び再構成
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) 復旧すべき重要なファイルをバックアップする機能の実証試験 「就航後のインシデント対応とリカバリープランをサポートする情報」に明示された方法に従って、システムが既知の保護された状態に復旧及び再構成できること。
☐	(2) 補完的対策の確認

	セキュリティ機能の説明に記載されるとおりであること。

	28. 代替電源
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) 既存のセキュリティ状態又は文書化された縮退モードに影響することなく、代替電源へ及び代替電源から切り替える機能の実証試験
☐	次に掲げる状態に影響することなく、代替電源へ及び代替電源から切り替えること
☐	(a) 既存のセキュリティ状態
☐	(b) 文書化された縮退モード
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	29. ネットワーク及びセキュリティ構成設定
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) 供給者によって提供される指針にて推奨されるネットワーク及びセキュリティ構成に従って設定される機能
☐	次に掲げるものを設定できること
☐	(a) ネットワーク構成
☐	(b) セキュリティ構成
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	30. 最小限の機能性
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) 最小限の機能性
☐	不要な機能及びサービスが実装されている場合、それらが無効化されていること。
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	32. ソフトウェアプロセス及びデバイスの識別及び認証
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) ソフトウェアプロセス及びデバイスを識別及び認証する機能の実証試験
☐	(a) ソフトウェアプロセスの識別と認証

☐	i) 正規の識別子および認証コードによってログインできること。
☐	ii) 非正規の識別子および認証コードによってログインできないこと。
☐	(b) デバイスの識別と認証
☐	i) 正規の識別子および認証コードによってログインできること。
☐	ii) 非正規の識別子および認証コードによってログインできないこと。
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	33. 失敗したログイン試行
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) ソフトウェアプロセス及びデバイスを識別及び認証する機能の実証試験
☐	次に掲げる項目に適合すること。
☐	(a) 連続した無効なログイン試行が設定された試行回数を超えた場合、アクセスを拒否すること
☐	(b) 拒否されたアクセスは、指定された期間または管理者によってロック解除されるまで続くこと
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	34. システム使用通知
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) システム使用通知メッセージを表示及び編集する機能
☐	次に掲げる機能を実装していること。
☐	(a) システム使用通知メッセージを表示する機能
☐	認証前にシステム使用通知メッセージが表示されること。
☐	(b) システム使用通知メッセージを編集する機能
☐	次に掲げる項目に適合すること。
☐	i) 権限を有する人員によって編集できること。
☐	ii) 権限を有さない人員によって編集できないこと。
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	35. 信頼できないネットワーク経由のアクセス
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) 信頼できないネットワークを経由するアクセスを監視及び制御する機能

☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	36. アクセス要求の明示的な承認
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) 承認権限を有する使用者（人）により明示的に承認された場合を除き、信頼できないネットワークから又は当該ネットワークを経由したアクセスを拒否する機能
☐	(a) 使用者（人）に対して、アクセスの承認権限を割り当てる機能
☐	(b) 承認されていないアクセスを拒否する機能
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	37. リモートセッションの終了
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) リモートセッションを終了する機能の実証試験
☐	次に掲げる機能のいずれかを実装していること
☐	(a) 自動でリモートセッションを終了する機能
☐	次に掲げる項目に適合していること
☐	i) セッションが終了する無操作時間を設定すること
☐	ii) 無操作時間の経過後にセッションが終了すること
☐	(b) 手動でリモートセッションを終了する機能
☐	使用者の操作によってセッションが終了すること
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	38. 暗号化による完全性の保護
	立会試験は不要

	39. 入力の検証
☐	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
☐	(1) 入力データを検証する機能の実証試験。
☐	無効なデータと判断した場合、適切に対応すること。（例：入力データの受取りを拒否する等）
☐	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	40. セッションの完全性
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
□	(1) セッションの完全性を保護し、無効なセッション ID の使用を拒否する機能の実証試験
□	次に掲げる項目に適合すること
□	(a) セッションの完全性を保護すること
□	(b) 無効なセッション ID の使用を拒否すること
□	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

	41. セッション終了後のセッション ID の無効化
□	-1. 本要件が適用される場合、次の(1)又は(2)いずれかの試験を実施しなければならない。
□	(1) 使用者のログアウト又はブラウザセッションを含むセッション終了後、セッション ID を無効化する機能の実証試験
□	(2) 補完的対策の確認 セキュリティ機能の説明に記載されるとおりであること。

セキュア開発ライフサイクルに関する要件

■ セキュア開発ライフサイクル

	1. 秘密鍵の管理
□	-1. 電子署名されたソフトウェアがシステムに含まれている場合、次に掲げる管理策等がマネジメントシステム文書に含まれていること。また、それらについて、役割、責任及び作業プロセスを扱っていること。
□	(1) 秘密鍵の管理方針
□	(2) 秘密鍵の手順上の管理策（例：生成、保管及び使用の手順等）
□	(3) 秘密鍵の技術上の管理策（例：物理的なアクセス制限や暗号化ハードウェア等）

	2. セキュリティアップデートの文書
□	-1. セキュリティアップデートをシステム所有者に知らせるためのプロセスがマネジメントシステム文書に含まれていること。
□	システム所有者へ知らせる情報は、次に掲げる項目が含まれていること。
□	(1) セキュリティパッチが適用される製品のバージョン番号

☐	(2)	承認されたパッチの手動及び自動プロセス経由による適用方法に関する説明
☐	(3)	製品にパッチを適用することで発生する可能性のある影響（再起動を含む）の記述
☐	(4)	承認されたパッチが適用されたことの確認方法に関する説明
☐	(5)	パッチを適用しないこと並びに資産所有者が承認又は導入しないパッチに使用できるメディエーションに関するリスク

	3.	**依存コンポーネント又はオペレーティングシステムのセキュリティアップデート文書**
☐	-1.	システム内の取得したソフトウェアの更新版にシステムが対応しているかどうかをシステム所有者に知らせるプロセスがマネジメントシステム文書に含まれていること。
☐		システム所有者へ知らせる情報は、更新された取得済みのソフトウェアを適用しないことによるリスクを、どのように管理するかに言及されていること。

	4.	**セキュリティアップデートの配信**
☐	-1.	セキュリティアップデートがシステム所有者に提供されることを保証するプロセスがマネジメントシステム文書に含まれていること。
☐		システム所有者へ知らせる情報は、更新されたソフトウェアの真正性を確認する方法が含まれていること。

	5.	**製品の多層防御**
☐	-1.	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プロセスがマネジメントシステム文書に含まれていること。

	6.	**環境において期待される多層防御策**
☐	-1.	製品使用者に関する文書であって、製品が使用される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に関する多層防御の手段を記述したものを作成するプロセスがマネジメントシステム文書に含まれていること。

	7.	**セキュリティ強化指針**
☐	-1.	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プロセスがマネジメントシステム文書に含まれていること。

船上のシステム及び機器の
サイバーレジリエンスに関するガイドライン（第 1.0 版）
［日本語 / Japanese］

一般財団法人 日本海事協会

事業開発本部　海技部

〒102-8567　東京都千代田区紀尾井町 4 番 7 号
Tel ：　03-5226-2177
E-mail : met@classnk.or.jp

技術本部　機関部

〒102-0094　東京都千代田区紀尾井町 3 番 3 号
Tel ：　03-5226-2022
E-mail : mcd@classnk.or.jp

www.classnk.or.jp

November 2023