統合ガイド

安全なデバイス統合への指針

Anybus 組み込みネットワーク・インターフェース

パート 1: 産業オートメーション・デバイスに関するセキュリティ規制と関連規格

パート 2: HMS Networks が考えるサイバーセキュリティ

パート 3: ベストプラクティスとセキュアな統合

はじめに

背景

産業のデジタル化が進展する中で、産業用ネットワークが生産現場外部の機械設備に接続されるようになりました。その結果、こうした設備へのアクセスが増加すると同時に、脅威に遭遇する可能性が高くなっています。

地域産業を保護するサイバーセキュリティへの意識とその重要性を増進する目的で、サイバー・レジリエンス法 (CRA) などの新たな規制も施行されています。

このような状況から、通信の信頼性を担保し、セキュリティ規制への確実な遵守を実現するには、産業用通信インターフェースを統合する際にサイバーセキュリティに配慮することが不可欠になっています。

HMS Networks は長年、サイバーセキュリティ強化に対する需要の増加を綿密に追跡し、企業のプロセス強化と製品の堅牢化でそのような需要に応えてきました。この積極的な取り組みにより、安全な通信インターフェースを容易に実装できるようになっています。

本書の目的

本書は、各種の製造元を対象として、Anybus 組み込みネットワーク・インターフェースを産業向け製品に統合する手順を示すガイドブックです。

本書は次の 3 部構成となっています。

パート 1: サイバーセキュリティを対象とした規則と規格の概要

パート 2: HMS Networks におけるサイバーセキュリティとプロセスに対する考え方、およびそのソリューションに実装されたセキュリティ対策の概要

パート 3: 現在期待されるセキュリティ対策の実現に向け、最善の手法をデバイス製造元向けに示すガイド

パート 1: 産業オートメーション・デバイスに関するセキュリティ規制と関連規格

オートメーション・デバイスの製造元にとって、信頼性に優れた製品を実現し、財務面と企業評価面の損害を最小限に抑えるうえで、サイバーセキュリティに取り組むことが優れた手立てです。一方で、通信機能を備えた製品を対象とする CRA などのサイバーセキュリティ規制と、生産とインフラの設備を対象とする NIS2 などの規制が近年になって導入されたことから、サイバーセキュリティ戦略の実施が努力義務ではなく必須になっています。

こうした規則の大半は、引き続き明確化が必要であり、整合した各種規格の確立には至っていません。その結果、製品の適合対応と法令遵守整備に時間を要するデバイス製造元や機械製造元は不確実性に直面しています。

- このパートでは、通信インターフェースを備えた機器に直接関連する規則と、機器を使用するユーザーを通じて製造元に間接的に関連する規則 (購買要件) を扱います。
- それに続き、既に指針となっている既存のサイバーセキュリティ規格と、産業デバイス製造元が最初に取り組むべきサイバーセキュリティ戦略を扱います。

一方、サイバーセキュリティ上のコンプライアンスに伴うお客様の負荷を軽減すべく、HMS Networks はこうした規制動向をモニターし、すべての必須要件に対処する対策を自社製品に実装することで、お客様がすぐに使用できる認証済みの産業デバイス向けネットワーク・インターフェースを提供しています。これにより、弊社の通信ソリューションは、サイバーセキュリティの実装にお客様が要する労力だけでなく、持続的で詳細な脆弱性監視とセキュリティ保守でお客様が要する労力を大幅に軽減できます。

1. 規制と購買の要件

日常的なサイバーセキュリティへの取り組みの実施そのものが、デバイス製造元にとって優れた実際的な手段です。製品の信頼性を引き上げ、財務面と企業評価の面で発生が考えられる損害を最小限に抑えます。これまで、適切なサイバーセキュリティ水準は、各デバイス製造元が独自に設定していました。CRA や NIS2 などの新たな規則により、サイバーセキュリティは努力義務ではなく必須の取り組みになっています。

本章では、デバイス製造元に直接または間接的に関連する、特に重要なサイバーセキュリティ規制を取り上げます。次の章では、規制への適合を示す目的で利用できる技術規格を分析します。

NIS2: ネットワークと情報システムのサイバーセキュリティ

NIS2 は前身の NIS1 を置き換える EU 指令です。NIS1 は、エネルギー、運輸、ヘルスケア、金融、水管理などのインフラやデジタル・インフラのサイバーセキュリティ要件を扱う規格でした。

NIS2 は、公共電子通信事業者、これまで以上に多くのデジタル・サービス、廃棄物と排水の管理、重要製品の製造、郵便と宅配のサービス、中央と地方の行政を対象とし、さらに宇宙分野にまで及んでいます。

これらの分野の中規模組織と大規模組織には、適切なサイバーセキュリティ・リスク管理対策を講じ、関連する政府機関に重大インシデントを報告することが求められます。

EU 加盟国には 2024 年 10 月 17 日までに NIS2 を国内法制化することが求められていました。しかし、19 の加盟国がこの法制化期限を守れず、欧州委員会による違反処理手続きが始まっています。

いまだに、NIS2 は EU の多数の組織に影響を及ぼしています。CRA や RED のサイバーセキュリティと異なり、NIS2 には規制遵守の証明に使用できる整合規格がありません。それに代わり、各加盟国が詳細な適合要件を決定します。

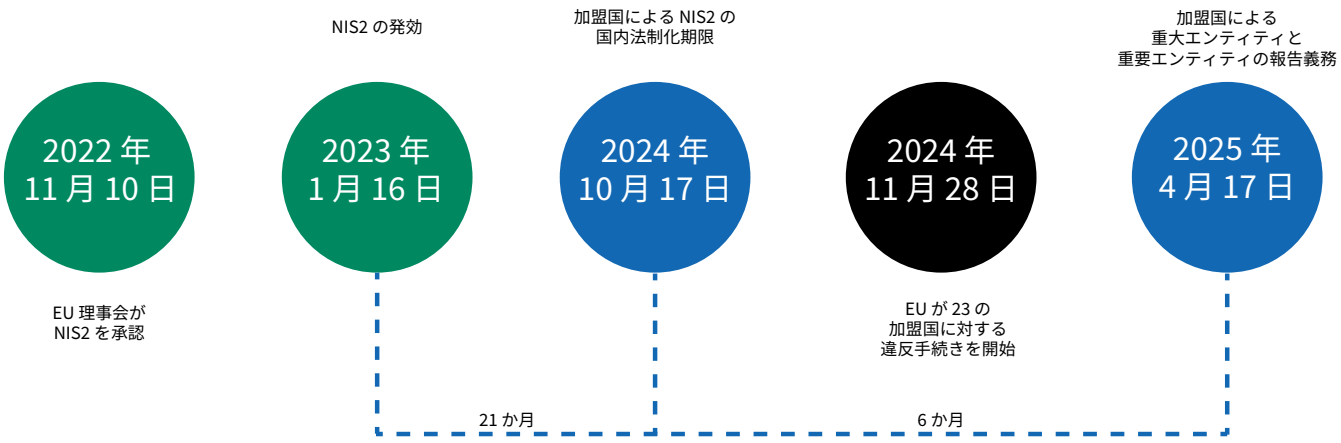

図 1. EU での NIS2 の実施と施行に関する主な管理点

IT サイバーセキュリティで NIS2 適合を証明するために広く使用されている規格は ISO 27001 です。ISO 27001 は、IT システムのセキュリティ、個人のセキュリティ、物理的セキュリティを適切に扱っている規格です。一方で、オペレーショナル・テクノロジーにはそれほど適していません。オペレーショナル・テクノロジーの適合証明では、IEC 62443 シリーズが広く使用されています。

NIS2 がデバイス製造元と機械製造元に直接関連することは多くありません。ただし、NIS2 の対象となる顧客からの要件で間接的に関連することはあります。デバイス製造元と機械製造元に対する要件の多くは、IEC 62443 規格が基本となっています。

サイバー・レジリエンス法 : コネクテッド製品を対象としたサイバーセキュリティの広範な枠組み

EU サイバー・レジリエンス法 (CRA) は、欧州市場で販売される、デジタル要素を備えた全製品を対象として、サイバーセキュリティの必須要件を導入しています。

安全な製品の設計、脆弱性の管理、デバイスのライフサイクルの中で 5 年間以上の更新提供が要求されることから、全世界の製造元に関連します。

2026 年 9 月からは、悪用された脆弱性と重大なインシデントを積極的に報告することが製造元に義務付けられます。さらに、2027 年 12 月 11 日までに、技術文書、適合性評価、ソフトウェア部品表 (SBOM) などに全面的に対応することが義務化されます。

また、CRA では重要度に応じて製品が分類されることから、適合性の評価手段が製品によって異なります。移行期間条項が存在しないことから、この期日前に開発が完了していたとしても、期日以降に製造される各製品も新たな法律に適合している必要があります。

規制の解釈を明確にするため、欧州委員会は整合規格の策定を要請しています。CRA 遵守を証明するには、この整合規格も必要です。欧州委員会の要請では、CRA の整合規格は RED サイバーセキュリティの整合規格に基づくことが求められています。

しかし、2025 年半ばの時点で、整合規格は策定中です。そのため、CRA 期日への対応を今から進めなければならない製造元は不確実性に直面しています。

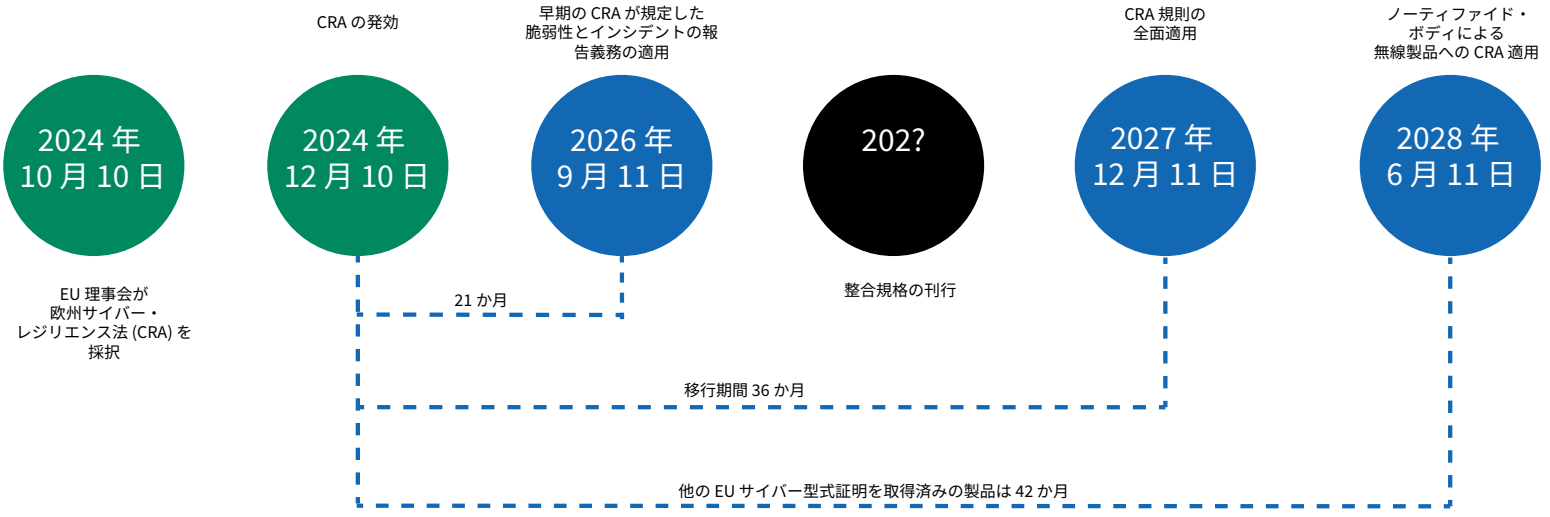

図 2. 時系列で見るサイバー・レジリエンス法 (CRA) の主な管理点

RED 指令 : 無線製品のサイバーセキュリティ強化

無線機器指令 (RED) は、無線通信デバイスなどの無線機器に健康上、安全性、EMC の要件の遵守を義務付ける、既存の EU 規則です。

2021 年の「Delegated Regulation (EU) 2022/30」により、RED 指令の基本的なサイバーセキュリティ要件が発効しました。

この要件は、インターネットに接続可能な無線製品に適用されます。適用開始日は 2025 年 8 月 1 日です。有線接続の産業デバイス自体は RED サイバーセキュリティ要件の対象ではないものの、それらのデバイスに無線接続機能を組み込むとこの要件の対象になります。たとえば、タブレットやスマートフォンを使用して無線を設定する機能を備えた産業デバイスは、その全体が RED サイバーセキュリティ要件の対象となる場合があります。

Wi-Fi、Bluetooth、セルラー接続機能を備えた産業デバイスなどの無線対応製品には、個人データの保護、不正アクセスの防止、ネットワーク・レジリエンスの確保に向けた安全対策を確実に搭載することが、その製造元に求められます。

ファクトリー・オートメーションでは、産業環境で使用するコネクテッド・デバイスに RED 適合のサイバーセキュリティ機能を組み込むことが要求されます。その結果、無線ゲートウェイからエッジ・デバイスまであらゆる要素が影響を受けます。特に、クラウド・システムやユーザー・ネットワークに接続するデバイスで重要です。

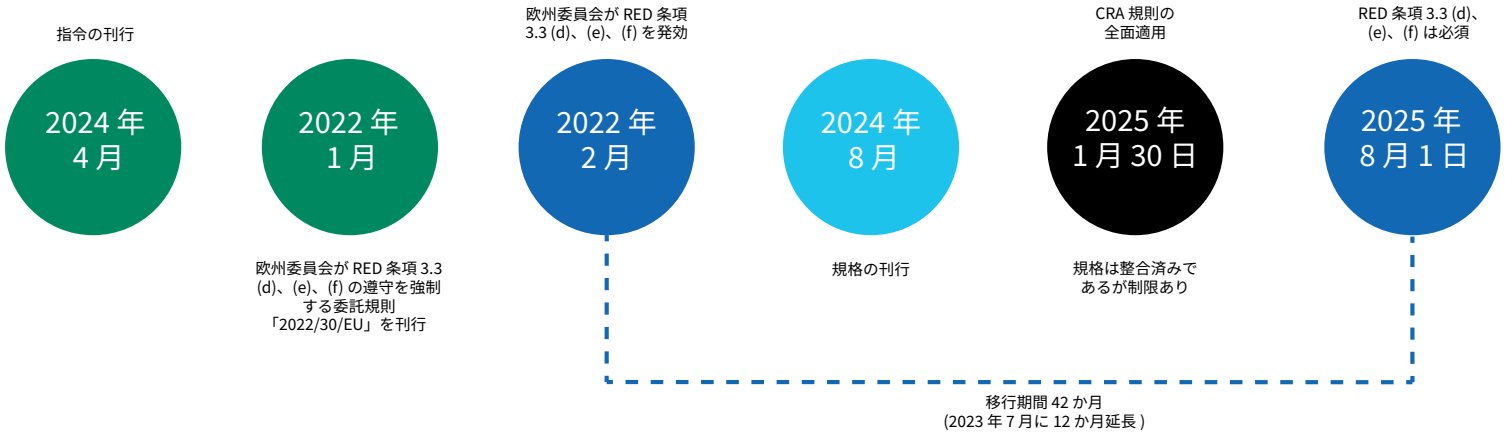

図 3. 無線装置指令 (RED) のサイバーセキュリティ要件の主な管理点

サイバーセキュリティに関する購買要件

大企業や政府機関では、サイバーセキュリティに関する購買要件を確立していることが普通です。

特に米国政府機関からの受注では、多くの場合、国立標準技術研究所 (NIST) が作成した NIST サイバーセキュリティ規格、ガイドライン、ベストプラクティスの遵守が求められます。

NIST の遵守は法的な要件ではありませんが、米国政府のサプライヤーとサブサプライヤーが多数にわたることから広範囲の影響が発生します。

サイバーセキュリティに関する保険要件

サイバーセキュリティが資産の保険に加入する前提条件となる事例が増加しています。たとえば、海運業界では新しい船舶が保険に加入する際に格付け機関の承認が必要です。

「E27 Cyber Resilience of On-board Systems and Equipment」は国際船級協会連合が制定した規格です。この規格は、主に IEC 62443 を基本としていますが、船舶と無関係な要件が除外されています。

船舶のサイバーセキュリティ要件は船主に適用されますが、海運分野に製品を納めるデバイス製造元と機械製造元にも間接的に関連します。

2. 規格

IEC 62443 産業通信ネットワーク - ネットワークとシステムのセキュリティ

IEC 62443 規格シリーズは、オートメーション・システムと制御システムにおけるオペレーショナル・テクノロジー (OT) のセキュリティを扱っています。ISO 27001 規格を補完し、情報セキュリティ管理システム (IT インフラ) に重点を置いています。

最上位のポリシーと末端の構成要素にまで至る各種手順のすべてを網羅し、産業用制御システムの整合性と可用性を重視しています。

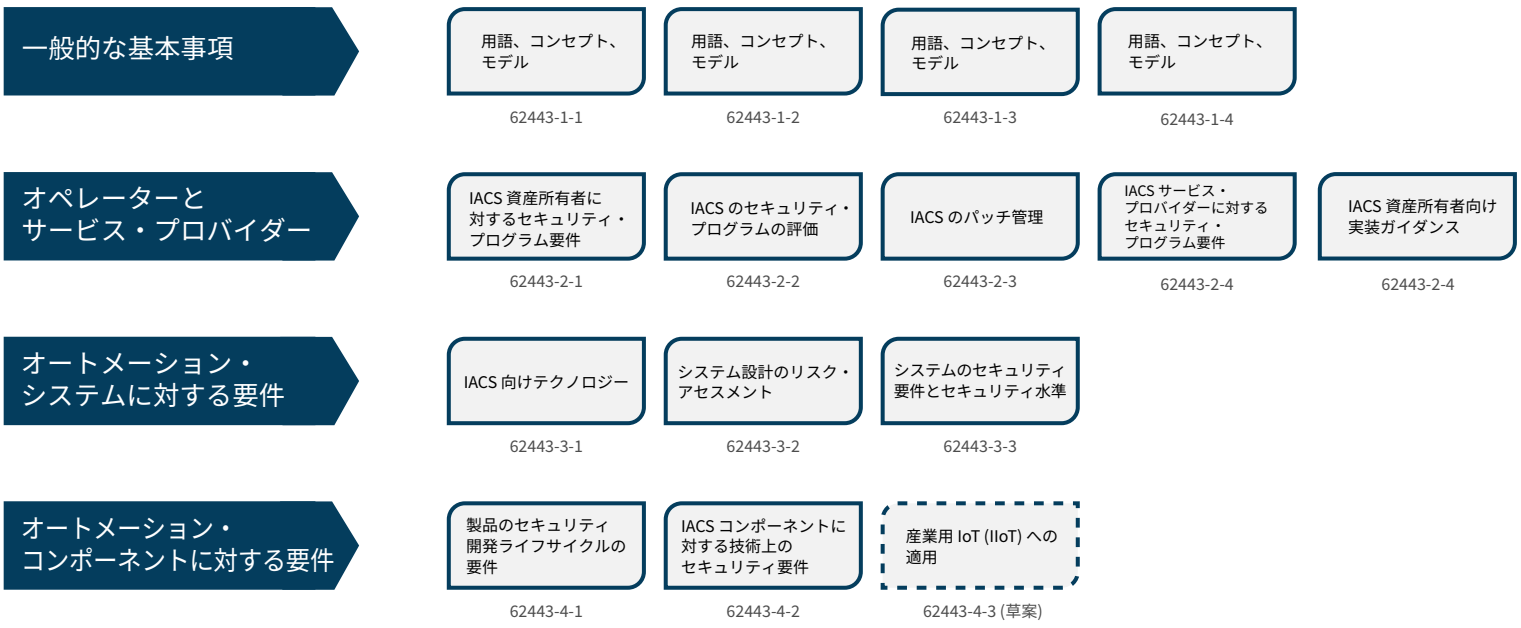

図 4. 産業サイバーセキュリティを対象とした IEC 62443 規格シリーズの構成。

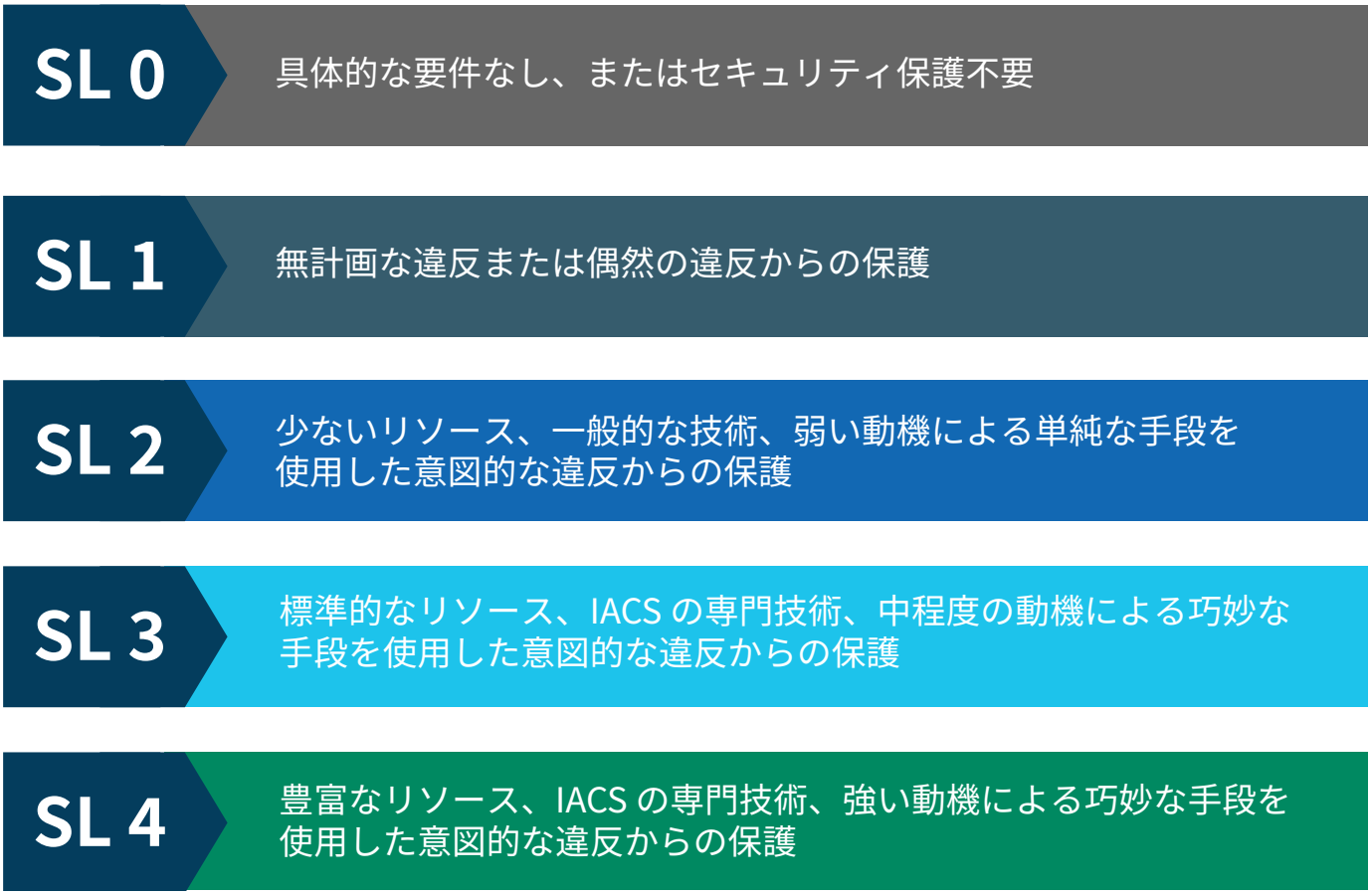

図 5. IEC 62443 が規定するセキュリティ・レベル SL 0 ～ SL 4。

この規格はレベル 0 ～ 4 の 5 段階のセキュリティ・レベルを規定しています。セキュリティ・レベル 0 に対しては、どのような要件もありません。

設備所有者がこの規格を利用することで、適切な水準のサイバーセキュリティを実現できるほか、外部に対して以下を証明する文書化機能も確立できます。

- NIS2 などの規制要件を遵守していることを証明する。
- セキュリティが適切な水準にあることを保険会社に証明する。
- サイバーセキュリティが適切な水準にあることを顧客や株主に証明する。

設備の指針となる原則は、OT ネットワークをセグメント化することと、重要な機械と生産ラインの組織内産業通信を監視および制御する通信経路の実装により、オートメーション・デバイスの外部露見を最小限に抑えることです。

設備に求められるセキュリティ水準を達成するには、システムとその構成要素もサイバーセキュリティ要件に適合する必要があります。このような要件に応えようとするデバイス製造元は、IEC 62443-4-x 規格をよりどころとして要件に関する体系的で詳細な指針を手に入れ、オートメーションの各構成要素でサイバーセキュリティの文書化と実装に対処できます。

CRA の観点から見て、IEC 62443 は重要な規格です。CRA と整合できるように規格の拡張が進められているからです。

この作業として、IEC 62443-4-1 と IEC 62443-4-2 の欧州向け拡張規格の制定のほか、「プロファイル規格」と呼ばれる IEC 62443-5-x 規格と、詳しい評価手法を規定する IEC 62443-6-x 規格の新規制定があります。

無線機器に対する EN 18031 の一般的なセキュリティ要件

EN 18031 規格シリーズは、欧州無線機器指令 (RED) への整合規格です。この規格を基に無線機器を試験することで、RED 指令のサイバーセキュリティ要件に適合していることが推定できます。

欧州委員会は、RED サイバーセキュリティ規格を基に CRA の整合規格を制定することを標準化団体に要請しています。この点で、CRA の観点からこれは重要な規格です。したがって、EN 18031 は CRA 遵守に向けた適切な出発点です。

また、RED に整合する最初のサイバーセキュリティ規格でもあります。整合を目指す規格に対する要件の 1 つとして、規格に基づく試験による法的安定性の提供が挙げられます。

つまり、規格に基づく試験の合否が試験担当者に左右されないことが求められます。この点が、リスクに基づく試験の手法をとる IEC 62443 と EN 18031 との違いです。

NIST の FIPS と SPECIAL PUBLICATION (SP)

米国商務省に属する国立標準技術研究所 (NIST) は、連邦情報処理標準 (FIPS) のほか、サイバーセキュリティに関する Special Publication (SP) を多数公開しています。

FIPS はサイバーセキュリティの重要な側面を標準化した規格です。その例を以下に挙げます。

- Advanced Encryption Standard (AES): 元々の Rijndael の名前でも知られる暗号方式です。ほぼすべての Web サーバーと、他の暗号通信の大部分で利用されています。
- Secure Hash Algorithms (SHA): 暗号学的ハッシュ関数群です。
- 暗号学的強度が高い乱数発生器。現代のマイクロコントローラーのほとんどは、FIPS の承認を受けたハードウェア方式の乱数発生器を備えています。

Special Publication (SP) は、多くの場合、サイバーセキュリティに関するガイドラインを記述した資料です。たとえば、「NIST Special Publication 800-63B」はパスワードに関する勧告を記述しています。

FIPS と SP はほとんどの米国連邦政府機関で必須の購入物件であるほか、政府機関以外の組織でも広く利用されています。IEC 62443 と EN18031 はどちらも、サイバーセキュリティのベストプラクティスに関して NIST を参照しています。

UL 2900 規格 : ネットワーク接続可能な製品のソフトウェア・サイバーセキュリティ

UL 2900 は、ネットワーク接続可能な製品のサイバーセキュリティに関する規格群です。UL 規格の中には、ANSI でも規格化されているものがあります。
ANSI/UL 2900-1 は製品に対する一般的な要件を扱い、主に安全な開発とテストの要件を規定しています。

パート 1 は、あらゆる製品に適用できる水平的規格と捉えることができます。

パート 2 は、次のような特定の製品範囲を扱う垂直的規格群です。

- ANSI/UL 2900-2-1: ネットワーク接続可能なヘルスケア製品に対する要件。
- UL 2900-2-2: 産業用制御システム向け規格 (現時点では ANSI 未採用)
- UL 2900-2-3: 保安と生命安全の警告システム向け規格 (現時点では ANSI 未採用)

米国食品医薬品局 (FDA) は政府規制への適合を示す手段として、ANSI/UL 2900-1 と ANSI/UL 2900-2-1 を承認しています。

ISO/IEC 27000: 情報セキュリティ・マネジメント・システム (ISMS)

ISO/IEC 27000 は、情報セキュリティ・マネジメント・システムの要件を扱う規格群です。情報セキュリティの関連要素を扱い、組織的管理策、人的管理策、物理的管理策、技術的管理策を規定しています。

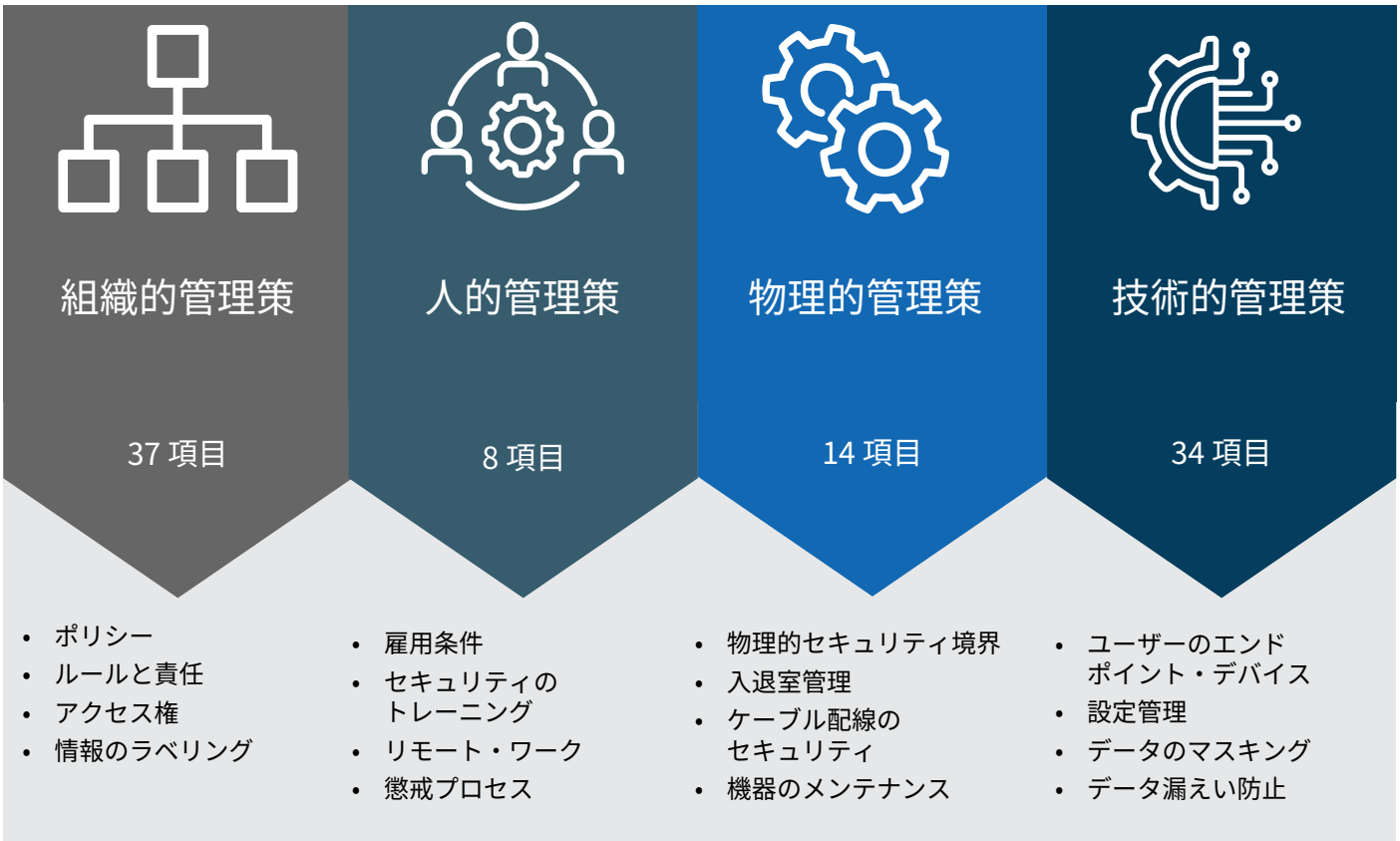

図 6. ISO/IEC 27000 が規定する情報セキュリティ・マネジメント・システムの管理カテゴリー。

図 7. 20 以上の規格で構成する ISO/IEC 27000 規格群。多彩な水準の抽象概念と分野固有の要素を扱います。

3. デバイス製造元と機械製造元に対するサイバーセキュリティ要件

デバイス製造元と機械製造元に対するサイバーセキュリティ要件の主な発生源は次の 2 点です。

- 直接の政府規制
- 顧客の購買要件

財務損失の防止と高い企業評価の維持に効果的で強固なサイバーセキュリティの確保は、製造元自身の利益にもなります。

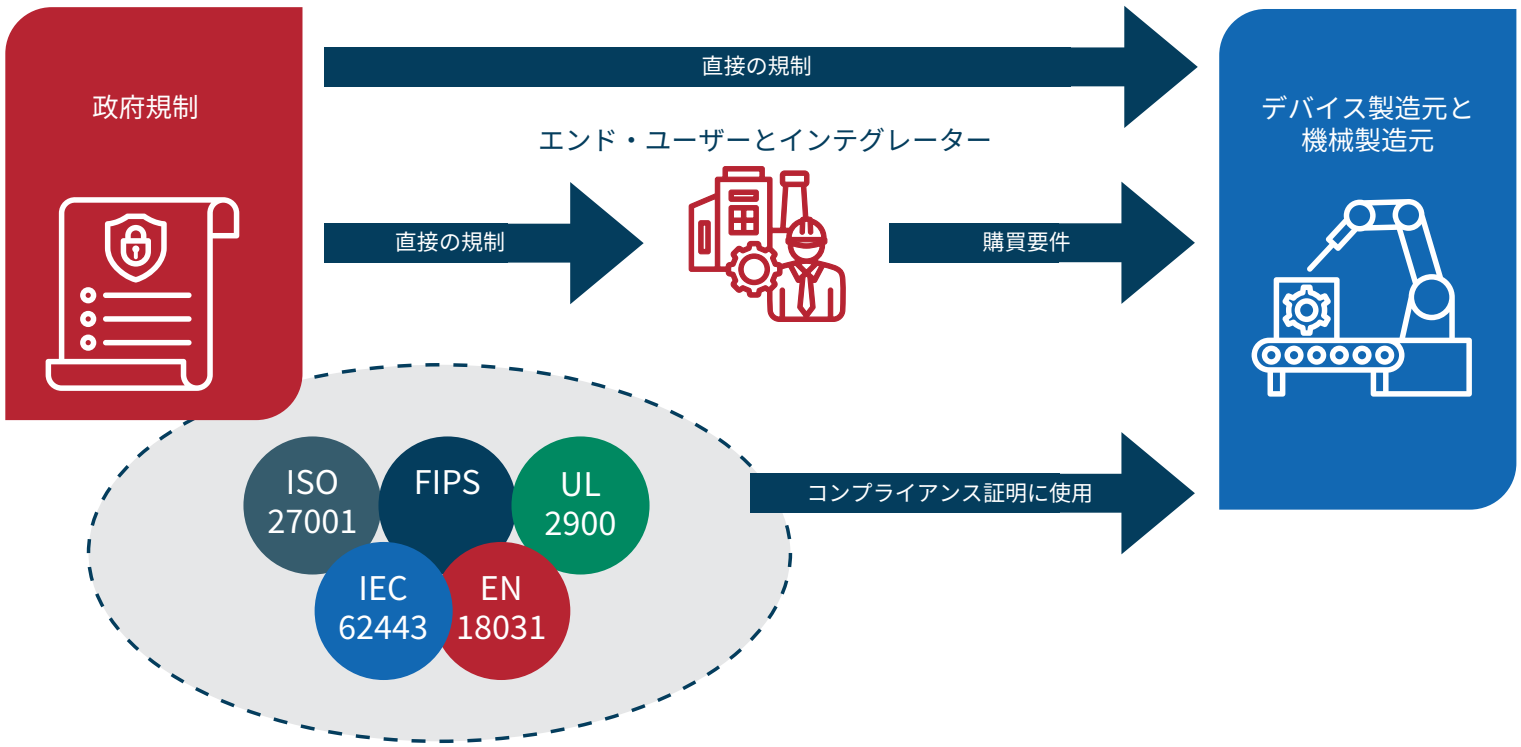

図 8. デバイス製造元と機械製造元に対するサイバーセキュリティ要件の発生源。

デバイス製造元と機械製造元が直接の政府規制と購買要件の両方に対応するには、最低限のサイバーセキュリティ機能を製品に実装し、安全な開発実務を文書化する必要があります。

サイバーセキュリティへのコンプライアンスの負荷軽減策として、認証済みネットワーク・インターフェースを利用できます。

こうしたインターフェースは、必要なサイバー防御の大部分を実装済みであり、関連するセキュリティ規格の認証を取得しています。

EU サイバー・レジリエンス法 (CRA) が 2024 年末に承認されたものの、現時点では必要な CRA 整合規格が制定されていません。その結果、全製品の新規格適合に時間を必要とするデバイス製造元と機械製造元は不確実性に直面しています。

購買要件では、不確実性がさらに大きくなります。現時点では、NIS2 などの規制の影響をエンド・ユーザーとインテグレーターが全面的には見通せないためです。また、両者は最上位のセキュリティ要件を購買要件に反映する必要もあります。

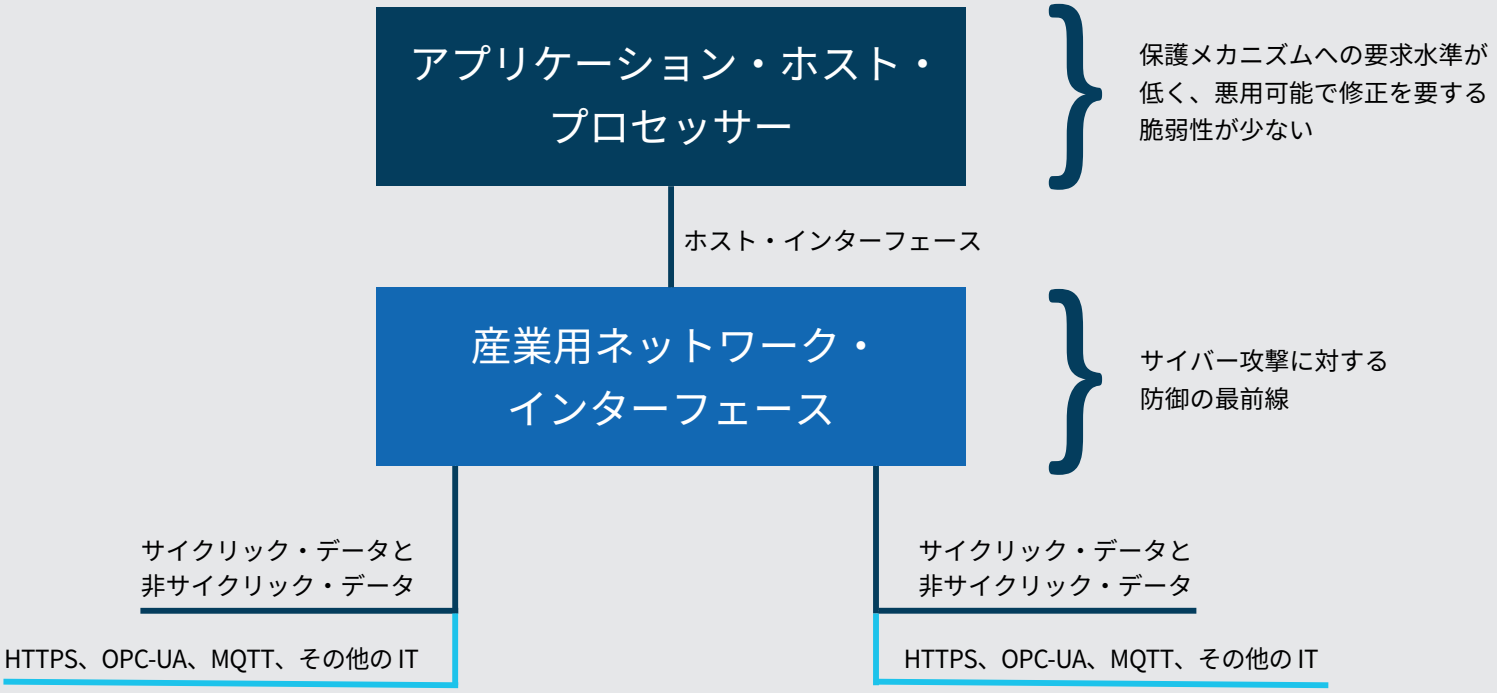

図 9. 認証済みネットワーク・インターフェースがサイバー防御の最前線として機能。

たとえば、2027 年 12 月以降に欧州市場で製品を合法的に販売するために対応を必要とする多数の要件リストが CRA に記述されています。

以下に示すとおり、認証済みネットワーク・インターフェースを利用すると、必要な CRA タスクの多くを遂行できます。

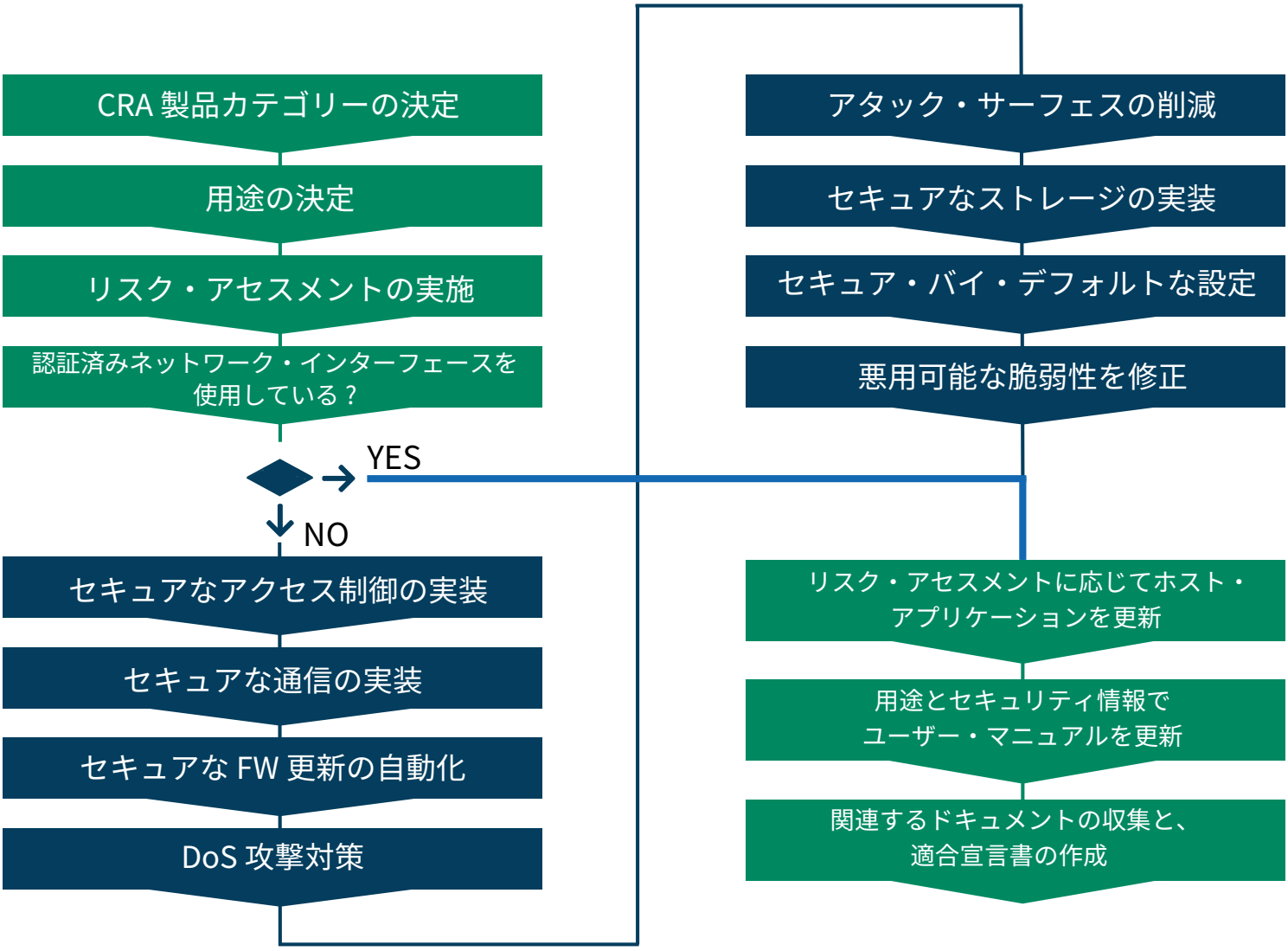

図 10. CRA 規制適合のためのワークフローとタスク。認証済みネットワーク・インターフェースを使用することによる利点を示しています。

パート 2: HMS Networks が考えるサイバーセキュリティ

HMS Networks は産業用情報通信技術 (ICT) 分野のマーケット・リーダーであり、35 年以上の経験を有します。

世界中で数千社の企業が 1,000 万台を超える HMS Networks 製品を統合し、効果的な通信と情報共有が可能な産業用機械とデバイスを実現しています。

HMS Networks は、お客様から信頼される安全な通信製品の提供とメンテナンスに力を注いでいる企業です。財務状態が健全で経験豊富な安定した企業である弊社は、サイバーセキュリティの長期的な課題に取り組み、対処できます。

業界でのリーダーシップ、豊富な経験、技術的な専門性、製品のメンテナンス保証を兼ね備えた HMS Networks の製品は、デバイスや機械への統合を目指す製造業のお客様にとって安全な製品購入先です。

HMS Networks では、産業用組み込み通信インターフェースは産業用ネットワーク・テクノロジー (INT) 部門の扱いとなっており、Anybus ブランドで提供されています。

「INT ではリアルタイム通信、産業用制御、サイバーセキュリティに重点を置いています。これらを産業用オートメーションの 3 本柱と位置付けています」
- HMS Networks、産業用ネットワーク・テクノロジー部門、シニア・バイス・プレジデント、Bartek S. Candell。

HMS Networks の詳細は Web サイトをご覧ください。
www.hms-networks.com/about

4. HMS Networks のセキュリティ標準とセキュリティ・プロセス

情報セキュリティ・マネジメント・システムと
セキュリティ関連認証

最高レベルの品質とセキュリティを確保するため、HMS Networks では情報セキュリティ・マネジメント・システム (ISMS) を運用しています。ISMS プロセスの一環として以下の認証規格に従っています。

- ISO 9001: ISO 9001 規格に適合した開発プロセスを通じ、最高の品質と信頼性を確保します。
- ISO27001: リスクを管理し、取り扱うデータと情報の機密性、完全性、可用性を保護するためのシステムです。
- IEC62443-4-1 ML3: Anybus 製品の開発プロセスは、成熟度レベル 3 の要件に適合し、開発プロセスと製品ライフサイクル全体を通して堅固なセキュリティ管理を提供できます。 認証証明書はこちらをご覧ください。

HMS Networks は EU 一般データ保護規則 (GDPR) が規定する規則に従っています。Anybus 組み込みネットワーク・インターフェースは、その動作に個人ユーザー情報を必要とせず、転送もしません。詳細は、HMS Networks のプライバシー・ポリシー (www.hms-networks.com/privacy-policy) をご覧ください。

ISMS 運用のためのセキュリティ対策

HMS Networks では、Anybus 組み込みネットワーク・インターフェースのライフサイクルを通じて機密性と完全性を確保するため、表 1 に示すセキュリティ対策を同製品に実装しています。

要件	HMS Networks による運用
データの機密性	5 章に挙げたセキュリティ関連認証に従い、ISMS による管理を全面的に運用。
安全な開発と製造の環境	• 承認を受けた人物にのみ、制限付きの物理的アクセス権と論理的アクセス権を付与 • 扉を施錠し、勤務時間外では警報装置を稼働。 • すべてのアクセスと変更を詳しく記録した全面的な監査証跡を HMS Networks で維持。 • 訪問者には HMS Networks の従業員が同行。 • 社内での写真撮影などの記録を禁止。
サプライチェーン全体での完全性の保証	ソフトウェアでは、ファームウェア用の証明書と、PC ベースの設定ソフトウェアとドライバー用の証明書を利用。ハードウェアでは、名の通った産業用 EMS サプライヤーを利用し、すべてのサプライヤーを HMS Networks 側で監査。製品の完全性を担保するため、社内で製品の完全性検査を実施。

表 1. セキュリティ対策。

セキュリティ・バイ・デザイン

Anybus の開発プロセスとして要件収集、設計、コーディング、テスト、デプロイ、文書化などがありますが、どの段階でもセキュリティは不可欠な要素です。

従業員のセキュリティ教育

サイバーセキュリティ意識向上トレーニングを全従業員が受講しています。また、開発者はセキュア・コーディングの訓練を受け、ソース・コードのレビューを実施します。

セキュリティ製品のテストと検証

セキュリティ・バイ・デザインの取り組みとして、脆弱性になる可能性がある部分の特定を重視した包括的なテストがあります。

この作業では、悪用される可能性がある、意図しない製品機能や設定の発見を目的として、セキュリティ重視のテスト・ケースを実行します。

Anybus CompactCom 40 に使用しているコードを対象として HMS Networks が実施しているレビューとテストを表 2 に示します。HMS Networks では、製品の要件に応じて試験項目とレビュー項目を選択しています。

製品の発売後も定期的に製品のインターフェースをテストして、新たな脅威に対するレジリエンスを確保しています。

レビューや試験の種類	コンプライアンス
コード・レビュー	チェックイン前にすべてのコードをレビュー。
侵入テスト	製品要件に基づき、製品の各部をテスト
静的コード解析	Synopsis Coverity ツール
ファジング・テスト / 堅牢性テスト	PROFINET バージョンでは Netload。 その他すべてのバージョンでは Achilles。
脆弱性スキャナー	Achilles

表 2. Anybus CompactCom のテスト。

5. 製品ドキュメントと提供情報

製品ドキュメント、設計ガイド、適合宣言書

製品とネットワークの専用ユーザー・マニュアルには、製品の機能と能力のほか、オートメーション・デバイスに製品を実装して設定する手順が詳しく記述されています。

このセキュリティ設計ガイドは既存の製品ユーザー・マニュアルを補完する資料です。Anybus 組み込みネットワーク・インターフェースの設計とライフサイクル管理のための、製品セキュリティに関するコンテンツとガイダンスを収録しています。

製品特有の詳細なセキュリティ情報と使用手順が、追加の製品セキュリティ・データシートに記載されています。

適合宣言書は、関連するネットワーク・テクノロジー規格や、EU や英国などの地域規格を遵守するために発行される資料です。

これらのドキュメントの入手先は以下のとおりです。

- HMS Networks のテクニカル・サポート Web ページ - 製品参照ページ www.hms-networks.com/technical-support からサポートとダウンロードのセクションを選択してください。
- Anybus CompactCom の HMS Networks 開発者ポータル : www.hms-networks.com/embedded-network-interfaces/developer-portal/overview

ライフサイクル管理

HMS Networks は、製品のライフサイクルを管理するプロセスを確立済みです。機能とセキュリティのメンテナンスは製品の成熟度段階に従って実施されます。製品のセキュリティ・データシートに製品固有の詳細情報が記述されていることがあります。

詳細は Web サイト www.hms-networks.com/product-life-cycle をご覧ください。

最新版ファームウェアへの更新

製品に適用可能な最新版ファームウェアの入手については、HMS Networks のテクニカル・サポート・チームにお問い合わせください。

HMS Customer and Distributor Information System (CDIS) にご登録いただくと、新規ファームウェアのリリースに関する通知を受け取ることができます。サポートページ www.hms-networks.com/technical-support の [Product and security alerts] セクションで [Subscribe to Alerts] ボタンを選択してください。

Anybus 組み込みネットワーク・インターフェースの更新に利用できるソリューションがいくつかあります。その更新プロセスでは、専用のメカニズムによってファームウェアの妥当性が検証されます。具体的な情報については、本書のベストプラクティスに関するセクションと製品のセキュリティ・データシートをご覧ください。

オープンソースの利用

HMS Networks は、Anybus 組み込みネットワーク・インターフェースにオープンソース・ソフトウェアを組み込むことがあります。このようなソフトウェアは、HMS Networks が検証し、セキュリティ上の脆弱性に対する対策を確実に実施したうえで製品ファームウェアに統合されます。

このように利用されるオープンソース・ソフトウェアの詳細と、付随するライセンス情報については、関連するネットワーク・ガイドをご覧ください。HMS Networks のテクニカル・サポート Web ページ www.hms-networks.com/technical-support で公開されています。

SBOM

HMS Networks は、お客様の要求に応じて、関連するファームウェアのソフトウェア部品表 (SBOM) を提供できます。

脆弱性の管理と情報提供

セキュリティ上の脆弱性に関する情報が Web サイト www.hms-networks.com/cyber-security で公開されています。この Web サイトから RSS フィードを直接サブスクライブすることで、最新コンテンツに関する通知を受け取ることができます。

HMS Networks では、製品の脆弱性と思われる状況を誰でも報告できるプログラムとして HMS Responsible Disclosure Program を用意しています。詳細は Web サイト www.hms-networks.com/cyber-security/responsible-disclosure-program をご覧ください。

バックドア不在宣言

Anybus 組み込みネットワーク・インターフェースには、外部インターフェースとのバックドアや隠しアカウントが文書化されずに存在していることはありません。

また、リモート・アクセス機能は搭載されておらず、クラウドベース・サービスとの固有な外部通信を確立することもありません。

6. Anybus 組み込みネットワーク・インターフェースの接続機能の概要

Anybus 組み込みネットワーク・インターフェースは、デバイス製造元による統合によって産業ネットワークを介したデータ共有を実現することを目的としています。

以下の機能に対応するために、複数の通信インターフェースを備えています。

- オートメーション・コントローラーとの間でプロセス・データを送受信するための産業用 Ethernet ネットワーク
- 必要に応じた設定と診断のための Web ベース機能
- IT アプリケーションとの情報の送受信に使用する IIoT プロトコル
- ホスト・アプリケーションとの統合をサポートする API

これらの通信ポート、インターフェース、プロトコルに関する製品固有の詳細については、製品セキュリティ・データシートをご覧ください。

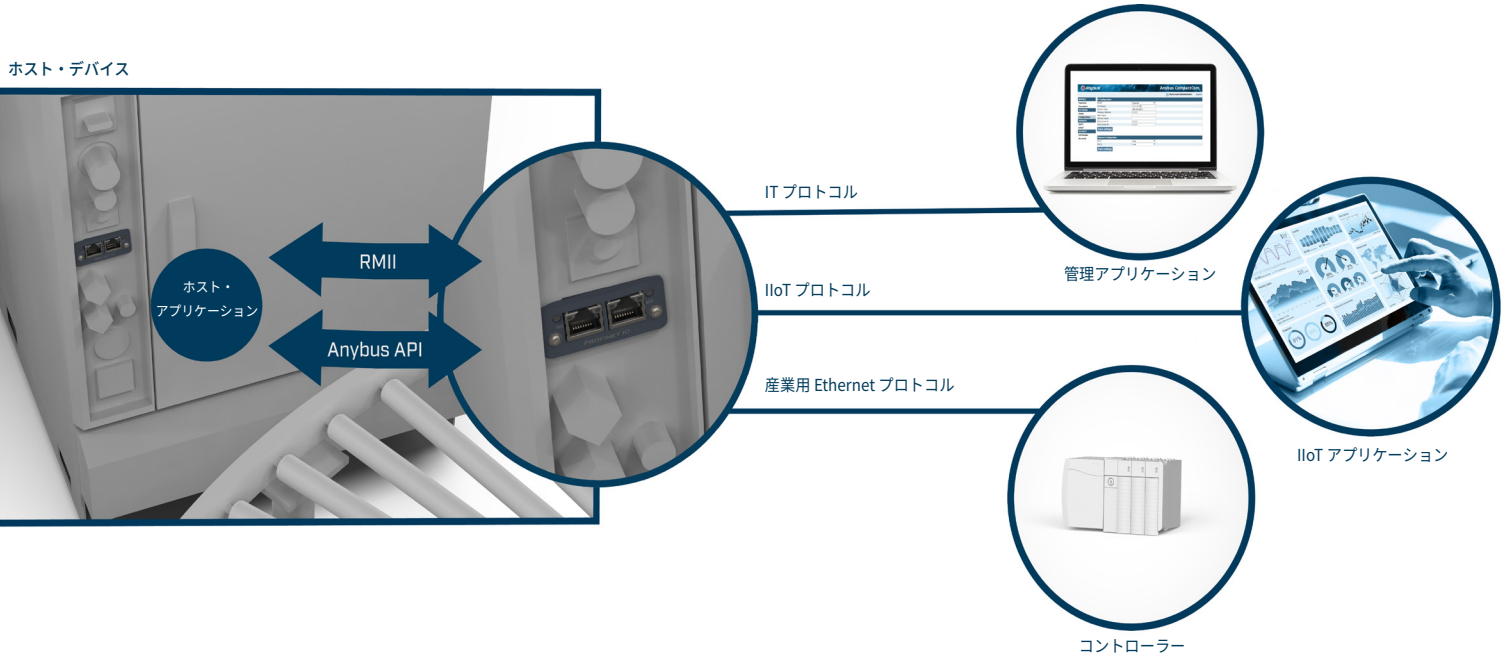

図 11. Anybus CompactCom 40

ANYBUS COMPACTCOM 40: 標準モデルと IIOT SECURE モデルとの比較

Anybus CompactCom 40 組み込みネットワーク・インターフェースには、標準モデルと IIoT Secure モデルが用意されています。

標準モデルは、シリアルまたは Ethernet を使用したプロトコルによる産業用通信機能に重点を置き、IT に特化した管理プロトコルをわずかに用意しています。

IIoT Secure モデルは、Ethernet ベースのプロトコル (PROFINET または Ethernet/IP)、追加の IIoT プロトコル (OPC UA、MQTT)、IT 管理用通信の併用に重点を置いています。また、追加のセキュリティ機能も提供します。

それぞれの詳細については、関連する製品セキュリティ・データシートをご覧ください。

産業用 ETHERNET プロトコルとそのセキュリティ拡張におけるセキュリティ面の検討事項

サイバーセキュリティ要件の進展に対応すべく、産業用通信の業界団体が新しいプロトコル拡張の開発を進めています。このプロトコル拡張では、通信とアプリケーションの両方を保護する先進的なセキュリティ・メカニズムが導入されます。

現時点では、PROFINET、Ethernet/IP、Modbus TCP、BACnet の各プロトコルがこの拡張の対象となっています。これらの拡張の実装状況は、適用可能な初期段階から検討が進行中の段階までさまざまです。POWERLINK と EtherCAT については、セキュリティ拡張をサポートする規格が今のところ存在しません。

Anybus CompactCom 40 IIoT Secure は、サイバーセキュリティでのベストプラクティスに対応できるように設計されています。

現在のところ、セキュアな産業用 Ethernet は市場でそれほど受け入れられていませんが、ハードウェアの観点では暗号化 OT プロトコルに対応可能な製品です。また、以下に挙げた他ベンダーのセキュア OT プロトコルもテスト済みです。

- modbus.org のフレームワークの範囲で、Modbus Security の相互運用性をテスト済み。
- ODVA に参加している他ベンダーの製品と CIP Security を統合し、世界各地の展示会で実演。

産業用シリアル・ネットワークのセキュリティにおける検討事項

シリアル方式のネットワークは論理的に分離された通信ネットワークであることがほとんどで、そこへのサイバー攻撃には大きな労力が必要です。したがって、脆弱性が現れるリスクは低くなります。

そのため、本書ではシリアル方式の産業用通信プロトコルを使用する Anybus CompactCom 製品は取り上げていません。

パート 3: ベストプラクティスとセキュアな統合

このセクションでは、Anybus 組み込みネットワーク・インターフェースの統合に取り組むデバイス製造元向けのベストプラクティスを紹介します。このベストプラクティスを通じて、デバイスや機械のセキュリティを強化し、今後のセキュリティ規制に備えることができます。

本セクションで重点的に取り上げている Anybus Compact Com 40 製品ファミリーは、入手可能な最新のインターフェース・ファミリーです。製品ライフサイクルの実用段階にあり、今後の CRA 要件への対応を HMS Networks が保証しています。

注意 : このベストプラクティスのリストはすべてを網羅しているわけではなく、ここにあるベストプラクティスだけではあらゆる規制への確実な遵守は望めません。必要なセキュリティ水準に応じたリスク・アセスメントと適切な対策を規定するには、該当のプロジェクトやアプリケーションそれぞれを個別に検討してください。

本セクションで取り上げている各機能の詳細とその統合手順については、関連する製品ユーザー・マニュアルをご覧ください。

7. 用途 - 適切な Anybus CompactCom の選択方法

セキュアな統合

Anybus CompactCom は、最終製品に組み込んで使用する製品です。また、その最終製品では、ホスト・インターフェースや内部部品が不正アクセスを受けないようにする必要があります。

アクセスが認められていない人物がホスト・インターフェースへのアクセスに成功すると、通信傍受や設定変更につながる可能性があります。

Anybus CompactCom IIoT Secure は セキュアな通信をサポートします。秘密暗号鍵はセキュリティ・チップに記録されているので、ハードウェアに物理的にアクセスされた場合でも秘密暗号鍵にアクセスされることはありません。

セキュア・ネットワーク

Anybus CompactCom の接続先は信頼できるネットワークに限定する必要があります。セキュリティが考慮されていない産業用 Ethernet プロトコルを使用することから、このような制限が必須です。

Anybus CompactCom IIoT Secure は、産業用 Ethernet 以外のプロトコルでセキュアな通信をサポートします。

こうしたプロトコルは信頼できないネットワークでも利用できますが、そのようなネットワークから産業用 Ethernet 通信にアクセスできないように対策を施す必要があります。そのための手段として、ファイアウォールやデータ・ダイオードなどがあります。

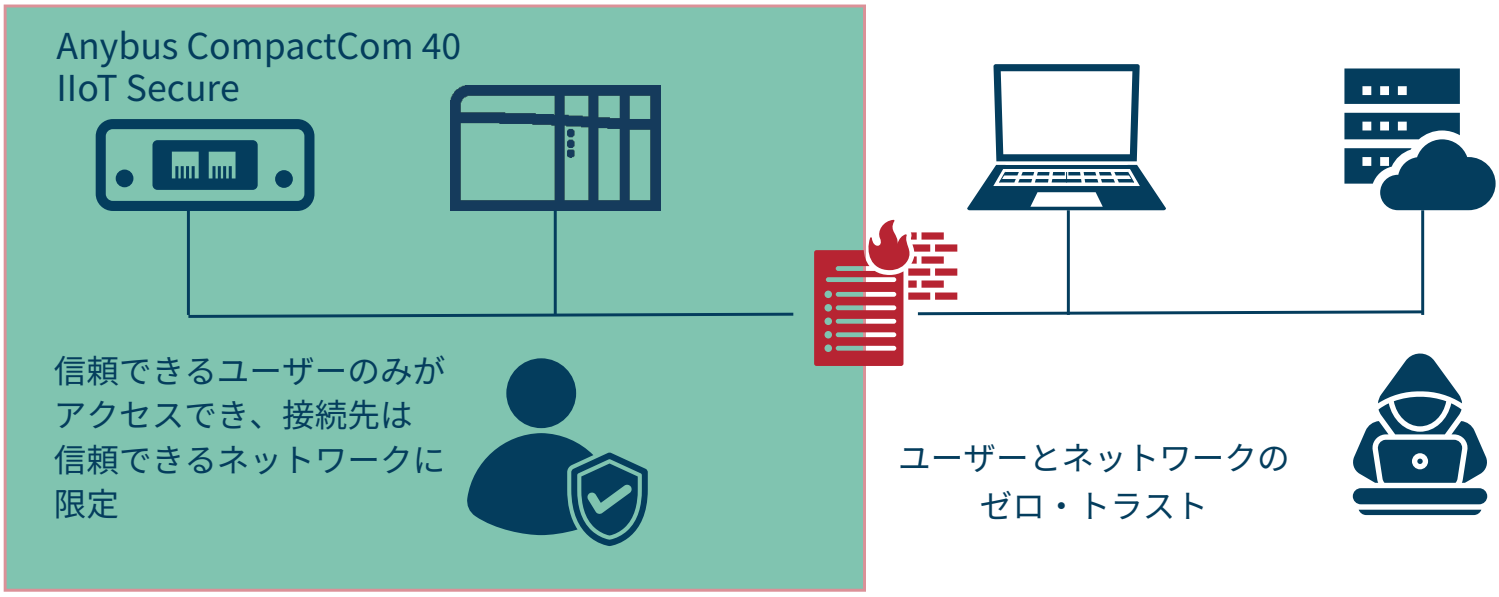

図 12. Anybus CompactCom 40 IIoT Secure の用途

適切な ANYBUS COMPACTCOM の選択方法

標準モデルである Anybus CompactCom 40 Industrial Ethernet は、信頼できる環境と信頼できるネットワークでの産業用途に適しています (CRA に関するセクションを参照)。

標準モデルはすべての産業用プロトコル (シリアル方式と Ethernet ベース) で利用できます。

Anybus CompactCom 40 IIoT Secure モデルは、産業用 Ethernet 通信と、IIoT 接続や Web サーバー接続の両方を必要とする用途に最適です。 追加のセキュリティ機能を備えていることから、顧客による外部のセキュリティ対策を必要とすることが少なく、信頼できるネットワークの外部での通信を保護できます。

また、Anybus CompactCom 40 IIoT Secure は、長期的なセキュリティ要件と暗号化 OT 通信の拡張機能に対応できるので、将来にわたって運用できるソリューションです。このような進化は、主にファームウェアの更新によって実現します。

現在利用している Anybus CompactCom 40 が標準モデルであっても、モデル共通の Anybus Host API によって最小限の労力で IIoT Secure モデルに更新できます。

セキュア・バイ・デフォルト - 通信インターフェース

デバイスのアプリケーションに不要な Anybus CompactCom の論理インターフェースと物理インターフェースはすべて、デバイスの製造元で閉じるか無効化する必要があります。

- 2 番目の Ethernet ポートなど、使用していない物理通信ポートを無効化します。使用していない Ethernet ポートの有効化と無効化を設定する機能をエンド・ユーザーに提供する方法もあります。
- デバイスに意図した動作に不要な通信機能 (Web サーバー、FTP、SNMP など) を無効化します。
- プロトコル (MQTT、OPC UA など) の暗号化機能を可能な限り有効化します。

設定、バックアップ、回復

本章では、Anybus CompactCom 40 インターフェースを設定する方法、デバイス設定を優れた信頼性でバックアップし、また回復する方法として、推奨できる手順を紹介します。その目的は、デバイス設定の簡素化、セキュリティの強化、ライフサイクルを通じて予測可能なデバイス挙動の維持にあります。

一般的な推奨事項

Anybus CompactCom 40 インターフェースの設定では、以下の点に留意することをおすすめします。

- 設定箇所の制限 : デバイスの挙動と設定の定義先とするインターフェースを、1 つのみまたはできるだけ少数に限定します。
- 安全な設定チャネル : 安全な通信インターフェースを優先的に利用します。可能であれば、アクセス権限を定義し、設定の権限をユーザー・ロールに割り当てます (たとえば、統合 Web サーバーを介して IIoT Secure モデルを使用します)。
- バックアップと回復の計画 : 設定のバックアップと復元に対応した設定手法を可能な限り利用します。そのような機能が標準で用意されていない場合は、それをデバイス・アプリケーション上で実装します。

固定的な機能と挙動をホスト・アプリケーションで指定

静的な挙動や固定的な通信機能を備えたデバイス・アプリケーションでは、これらをホスト・アプリケーションのファームウェアに直接実装することを優先します。

- これにより、バックアップ手順や回復手順を別途必要とすることなく、一貫性のある予測可能な挙動をデバイスに維持できます。
- ファームウェアに定義した挙動は、標準的なファームウェア更新の過程で更新できるので、デバイスのバージョンが変わっても意図した動作を維持できます。

主な利点 : メンテナンスを簡素化でき、固定的な機能の設定を外部で管理する必要がありません。

ネットワーク記述ファイルを利用してユーザー・デバイスを設定

変数データ・マッピングやオプション挙動などのユーザー定義オプションをサポートしているデバイスでは、GSD や EDS などのネットワーク記述ファイルによる産業用プロトコルの初期化メカニズムを利用します。このようなファイルを使用することで以下の効果が得られます。

- PLC 環境でユーザーが設定パラメーターを定義できます。

- 初期化のたびにパラメーターが自動的にデバイスへ転送されます。

- コントローラーのプロジェクト・ファイルに設定が保存されるので、持続性と一貫性を確保できます。

主な利点 : デバイス自体を手動で操作することなく、ユーザー固有の柔軟な設定が可能です。

専用のソフトウェア・ツールによるデバイス設定

専用ソフトウェア・ツールを使用してデバイスを設定する必要がある場合は以下の点に留意します。

- ホスト・アプリケーションは、そのツールから設定データや設定ファイルを受け取る必要があります。

- それに続き、Anybus CompactCom 40 ホスト API を介して設定を保管し、また適用する必要があります。

この構成では、専用ツールとホスト・アプリケーションで以下の処理に対応する必要があります :

- 設定データのバックアップと復元。

- 機密設定パラメーターの認証とそれらに対するアクセス制御。

主な利点 : セキュリティと復元性を確保しつつ、設定データを一元管理 (ホスト・アプリケーションと通信インターフェース) できます。

ANYBUS の WEB サーバーによる設定

Anybus CompactCom 40 の統合 Web サーバーを使用し、デバイス固有の設定に合わせてネットワークを設定し、カスタムの Web ページをホストできます。ただし、以下の重要な注意点があります。

- 組み込みの Web サーバーは、設定パラメーターのバックアップも復元もサポートしません。

- 設定インターフェースを保護するために、アクセス保護とユーザー認証をデバイス製造元が実装する必要があります。

- IIoT Secure モデルに対しては、Web サーバーが以下の機能をサポートします。

    - 暗号化通信

    - ユーザーとロールに基づくアクセス制御

ただし、これらのモデルでもバックアップ機能と復元機能は用意されていません。
主な利点 : 設定で使用できるインターフェースが得られ、リモート・セットアップが必要なデバイスに最適です。ただし、バックアップ方針をユーザー側で検討する必要があります。

アクセス保護とユーザー管理

FTP や Web サーバーなどの IT 管理機能を使用する場合は、固有のアプリケーション要件に応じてユーザー構造を構築します。

このユーザー構造に、それぞれ異なるアクセス権限レベルを設定したさまざまなユーザー・ロールを定義します。ユーザー名とパスワードによる認証をインターフェースで有効化します。インターフェースへの不正アクセスを防止するために、複雑なパスワードを使用します。

識別とバージョン管理

HMS Networks の API が提供する Anybus Identification オブジェクトを、デバイスのバージョン、ステータス、診断の情報に使用します。Anybus CompactCom 40 では、専用の識別要素または各プロトコル仕様に基づくメカニズムを使用して、この資産管理情報をアプリケーション・コントローラーやネットワーク管理ツールと標準化された手法で共有します。

関連する情報要素やメカニズムについては、Anybus CompactCom ネットワーク・ガイドをご覧ください。

ドキュメントの提供

Anybus CompactCom 40 の機能実装に基づくグローバルなデバイス・インターフェース機能を記述した包括的なデバイス・ドキュメントとセキュリティ情報を提供します。提供された Anybus CompactCom 40 のセキュリティ・データシートを利用して、デバイスのセキュリティ記述を作成します。

システム全体で効果的にバージョンを管理するために、Anybus CompactCom 40 に関するバージョン管理を統合します。この管理では、ホスト・アプリケーションとファームウェアの具体的なコンポーネントを対象とします。このバージョン管理を、Anybus CompactCom のインターフェースに反映できます。

デバイス製造元は、Anybus CompactCom 40 に使用されているオープンソースのソフトウェアやハードウェアに関する HMS Networks の声明を自社のドキュメントに記述し、それを実装内容に応じて補完できます。また、そのようにする必要があります。オープンソースに関する弊社の声明は、関連するネットワーク・ガイドに掲載されています。

ネットワーク通信のコンプライアンス確保

デバイス実装全体が、関連する産業用ネットワークのパフォーマンス・テストと適合性テストに合格し、ネットワーク認証を取得できるようにします。HMS Networks では、そのハードウェアとファームウェアの各リリースが、関連するプロトコル・テクノロジーに適合し、認証を取得した状態にしています。これにより、デバイス製造元では、インターフェースを統合したデバイスのコンプライアンスを容易に実現できます。

ネットワーク組織ごとに異なるポリシーに従い、デバイスのライフサイクル全体を通して、このネットワーク適合性を最新の状態に維持します。

デバイスを最新状態に維持

一貫性のある高水準のセキュリティを維持するために、Anybus CompactCom のモジュールを最新の状態に維持します。

Anybus CompactCom の製品ニュース、ファームウェア更新、セキュリティ上の助言に関する情報を入手するとともに、HMS Networks のプロアクティブなコミュニケーション・チャネルにご登録ください (詳細は関連する章を参照)。

デバイス製造元は、HMS Networks が公開する製品の変更通知とセキュリティ上の助言が自社デバイスとどのように関連しているか、また自社デバイスにどのように影響するかを、そのデバイスのアプリケーションとの関連から評価する必要があります。

現場に設置したデバイスの正確なトレーサビリティを確保するために、バージョン情報を忘れずに更新してください。

運用の終了

Anybus CompactCom の運用を終了する場合は、デバイスを工場出荷状態にリセットし、Anybus CompactCom 上に保存されたユーザー・アカウントと固有のモジュール設定情報を削除します。

HMS Networks
産業用 ICT
(情報通信テクノロジー) で
最善の選択肢。

www.hms-networks.com