

1. はじめに

1.1. 本書の目的

本書は、自動車のライフサイクルを通じたサイバーセキュリティマネジメントシステム（CSMS）の要求を示した ISO/SAE 21434 Road vehicles - Cybersecurity engineering（以下、ISO/SAE 21434）の解説書である。

ISO/SAE 21434 の要求事項は非常に抽象的に書かれており、各社がその要求事項を適用するには、①要求の策定背景の理解と、②業界動向を踏まえた解釈が必要となる。これらの課題を解決するため、本書では ISO 規格の原文と翻訳文に加え、解説として要求事項の策定背景や解釈などを記載している。そのため、各要求事項の必要性の理解や、その実現手段を導出する際のヒントを得たい場合に、本書を活用することができる。

1.2. 本書の構成

本書では、1 章に “本解説書” の概要” を、2 章に “ISO/SAE 21434 の必要性と全体概要” を記載する。その後、3 章以降には ISO/SAE 21434 の章構成に合わせて具体的な解説内容を記載している。ISO/SAE 21434 と本解説書の対応関係を図 1 に示す。

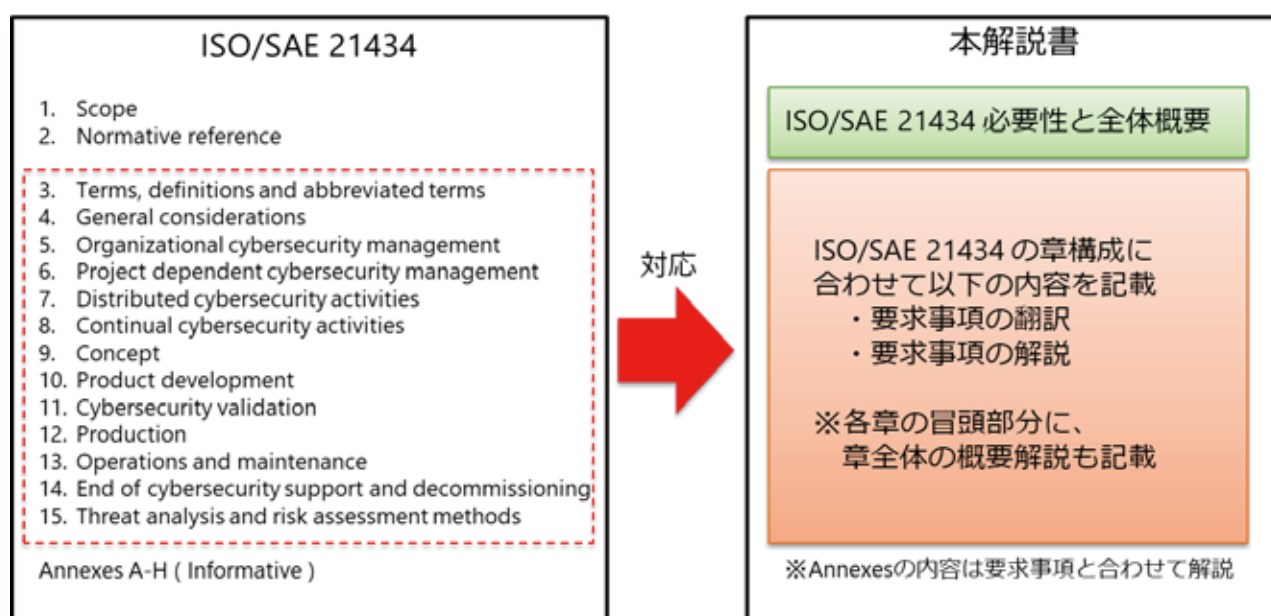


図 1 ISO/SAE 21434 と本解説書の対応関係

なお、本書には規格要求の原文と翻訳文の対比は記載しない。対比については、日本規格協会が販売している文書を参照すること。

5. Organizational cybersecurity management（組織のサイバーセキュリティ管理）

【5章全体の解説】

ISO/SAE 21434 の 5 章 “組織のサイバーセキュリティ管理” では、企業内にサイバーセキュリティガバナンスの構築すること、および、サイバーセキュリティ文化を醸成することが求められている。

サイバーセキュリティガバナンスの構築

サイバーセキュリティガバナンスを構築するためには、まず企業のサイバーセキュリティポリシーを定め、ポリシーに沿ったルール&プロセスを策定し、それを実行するための組織体制を構築する必要がある。サイバーセキュリティガバナンスの全体像を図 7 に示す。

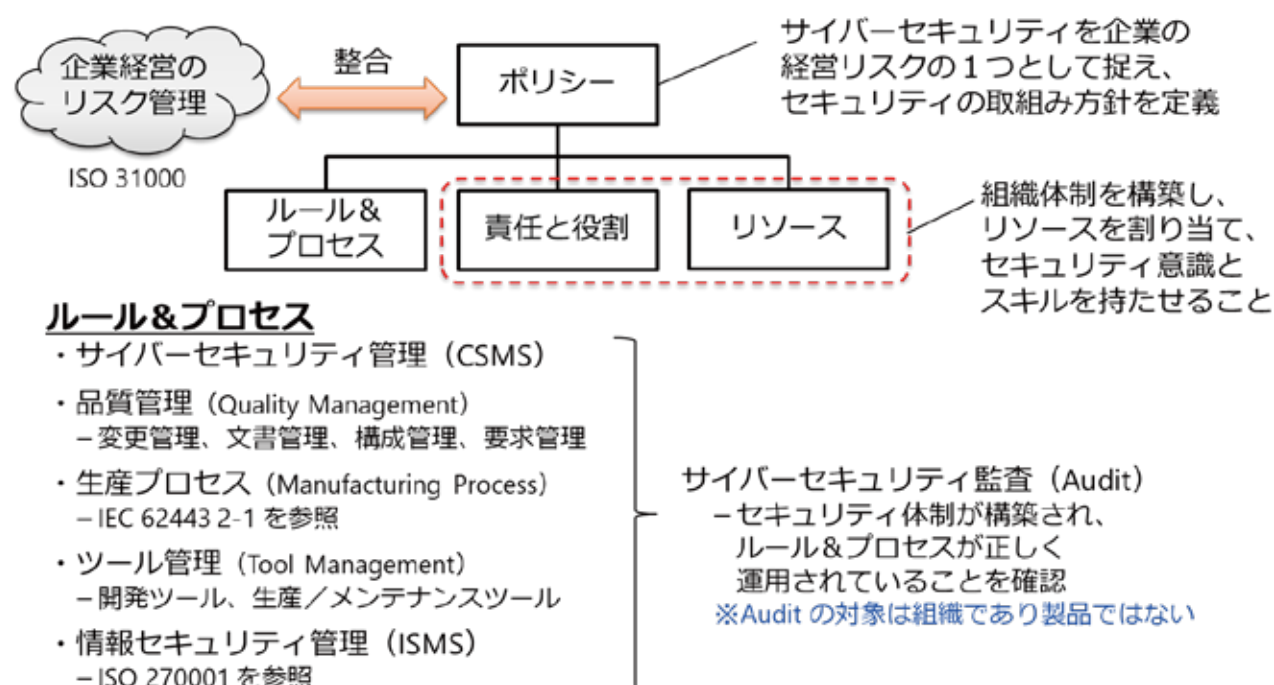


図 7 サイバーセキュリティガバナンスの全体像

サイバーセキュリティ文化の醸成

サイバーセキュリティ文化を醸成するには、組織に対するサイバーセキュリティ教育を実施する必要がある。定期的なサイバーセキュリティ教育の実施によって、組織で以下 2 つを管理する。

➤ サイバーセキュリティ意識の管理

例. セキュリティの必要性の理解や、セキュリティに配慮した行動への変容など

➤ サイバーセキュリティ開発能力の管理

例. 脅威分析／脆弱性分析を行うエキスパートや、設計／評価などを行う実務者の認定など

5.1. General (全般)

サイバーセキュリティエンジニアリングを可能にするため、組織はサイバーセキュリティガバナンスと、サイバーセキュリティ文化（サイバーセキュリティ意識管理、能力管理、継続的改善を含む）を確立し、維持する。これには、策定した組織のルールとプロセスが、本規格の目的に反していないかを、独立に監査することが含まれる。

サイバーセキュリティエンジニアリングをサポートするために、組織はツールの管理や、品質管理システムの適用など、サイバーセキュリティのマネジメントシステムを実装する。

5.2. Objectives (目的)

本章の目的は以下の通り。

- a) サイバーセキュリティのポリシーと、サイバーセキュリティに関する組織のルール、およびプロセスを定義する
- b) サイバーセキュリティ活動を実行するために必要な責任と対応する権限を割り当てる
- c) サイバーセキュリティの遂行をサポートする（サイバーセキュリティプロセスと関連プロセス間の相互作用の管理とリソースの提供を含む）
- d) サイバーセキュリティリスクを管理する
- e) 能力管理、意識管理、継続的な改善を含むサイバーセキュリティ文化を確立し、維持する
- f) サイバーセキュリティ情報の共有を管理・支援する
- g) サイバーセキュリティのメンテナンスを支援するための管理システムを確立し、維持する
- h) 使用するツールがサイバーセキュリティに悪影響をおよぼさないというエビデンスを提供する
- i) 組織のサイバーセキュリティ監査を実施する

5.3. Inputs (入力)

5.3.1. Prerequisites (前提条件)

無し。

5.3.2. Further supporting information (さらなるサポート情報)

以下の情報を考慮することができる。

- 品質管理をサポートする標準に準拠した既存のエビデンス

例. ISO 9001 [8] と組み合わせた IATF 16949 [7]、ISO 10007[9]、Automotive SPICE®1、ISO/IEC 330xx ファミリの規格 [10]、ISO/IEC/IEEE 15228 [11] および ISO/IEC/IEEE 12207 [12]

5.4. Requirements and recommendations (要求と推奨事項)

5.4.1. Cybersecurity governance (サイバーセキュリティガバナンス)

[RQ-05-01] 組織は、以下を含むサイバーセキュリティポリシーを定義すること。

- a) 路上走行車両のサイバーセキュリティリスクの認知
- b) 対応するサイバーセキュリティリスクを管理する経営幹部のコミットメント

注1：サイバーセキュリティポリシーには、組織の目的や他のポリシーへのリンクを含めることができる

注2：サイバーセキュリティポリシーには、組織の外部または内部のコンテキストを考慮して、製品またはサービスポートフォリオに関する一般的な脅威シナリオのリスクへの対処に関するステートメントを含めることができる。

【RQ-05-01 の解説】

組織は、サイバーセキュリティに対するトップマネジメントを行うために、サイバーセキュリティポリシーを定めなければならない。サイバーセキュリティポリシーは「サイバーセキュリティを企業の経営リスクの1つ」として捉え、企業の取組み方針を定義する必要がある。なお、企業の経営リスクの管理方法は、ISO/IEC 31000 を参考にすることができる。

RQ-05-01 の a) の要求に記されている車両のサイバーセキュリティリスクでは、ロードユーザへの悪影響を考慮する必要がある。悪影響の事例は、Annex.F を参照とする。また、b) の要求については、組織として以下を明確にしておく必要がある。

- サイバーセキュリティリスクに備えるための費用や体制
- 組織として保持するリスク／保持できないリスクの判断基準
- セキュリティインシデントが発生した際の経営陣の対応 など

[RQ-05-02] 組織は、以下のルールとプロセスを確立および維持すること。

- a) 本規格の要求を実行できるようにすること
- b) 対応するアクティビティの実行を支援すること

例 1：プロセス定義、技術ルール、ガイドライン、手法、および、テンプレート

注 3：サイバーセキュリティのリスク管理には、活動の労力と利益の考慮事項を含めることができる

注 4：コンセプト、製品開発、製造、運用、保守、廃棄のルールとプロセスには、TARA の手法、情報共有、サイバーセキュリティモニタリング、サイバーセキュリティインシデント対応やトリガーなどが含まれる

注 5：脆弱性の開示に関するルールとプロセスは、例えば ISO 29147 [14] の情報共有のパートに従って定義することができる

注 6：包括的なサイバーセキュリティポリシー（[RQ-05-01] を参照）と、組織固有のサイバーセキュリティルールおよびプロセス（[RQ-05-02] を参照）、責任（[RQ-05-03] を参照）とリソース（[RQ-05-04] を参照）の関係を図 8 に示す。

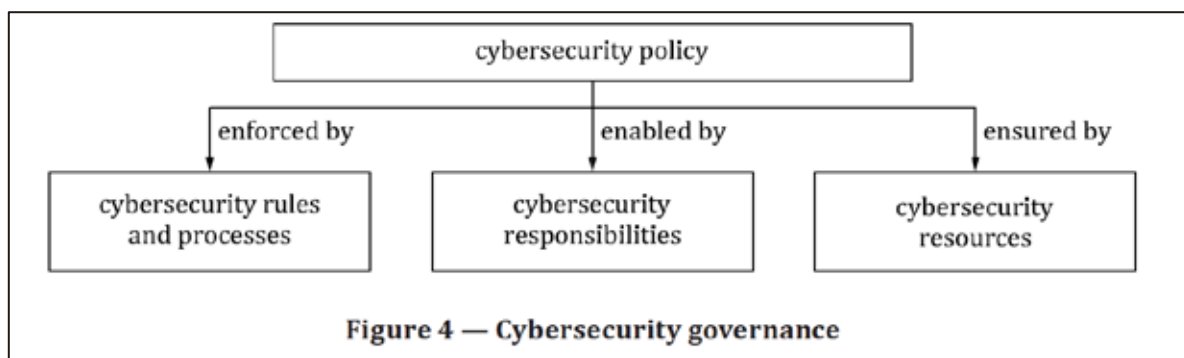


図 8 サイバーセキュリティのガバナンス

【RQ-05-02 の解説】

ISO/SAE 21434 では、ポリシーの下にルール&プロセスと記載されているが、ルールとプロセスの違いを理解するには、ISO/IEC 27000 の ISMS（情報セキュリティマネジメントシステム）における情報セキュリティポリシーが参考となる。ISMS の情報セキュリティポリシーの構成を図 9、および、表 1 に示す。

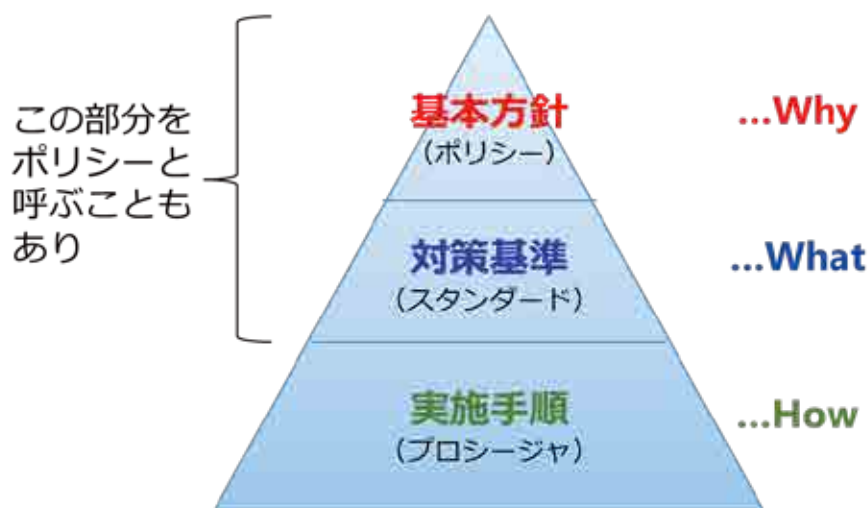


図 9 ISMS の情報セキュリティポリシー

表 1 ISMS の情報セキュリティポリシー

文書名	概要
基本方針 (ポリシー)	組織の経営者が情報セキュリティに取り組む姿勢を示し、組織が取る行動を社内外へ宣言するもの。
対策基準 (スタンダード)	基本方針に従い「何をしなければならないか」を記述するもの。 組織として情報セキュリティに取り組むためのルール（規程）に相当。
実施手順 (プロシージャ)	基準を満たすため、誰が、何を、どのように 実施するかを定めたプロセスに相当するもの。

ISO 29147 に従った脆弱性情報の公開ルール／プロセスとは？

RQ-05-02 の注 5 では、ISO 29147 を参考にして、脆弱性開示のルール／プロセスを作成することを要求している。なお、日本では IPA が発行している“情報セキュリティ早期警戒パートナーシップガイドライン”を参考とすることができる。詳細は以下を参照とする。

IPA：情報セキュリティ早期警戒パートナーシップガイドライン

URL：https://www.ipa.go.jp/security/ciadr/partnership_guide.html

ISO 29147 では、脆弱性公開ポリシーを策定し、脆弱性情報の受付と公開を行うための仕組みを作することを求めている。ISO 29149 に従った脆弱性情報を取り扱う流れを図 10 に示す。

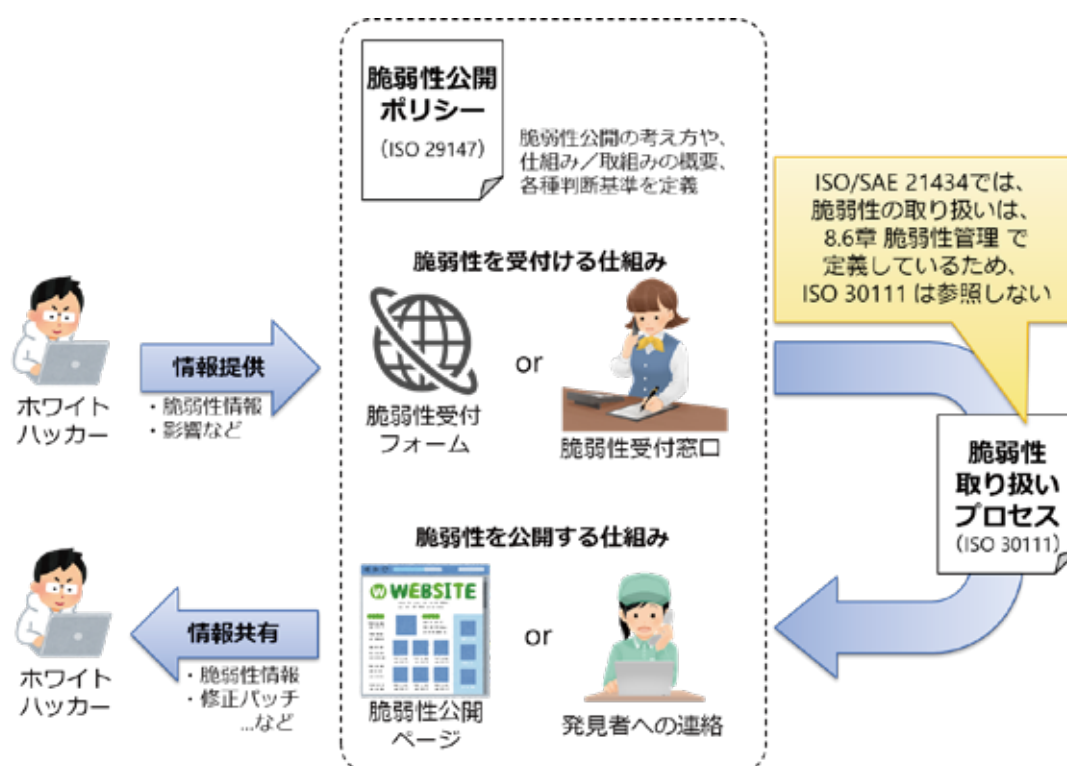


図 10 ISO 29147 に従った脆弱性情報を取り扱う流れ

脆弱性情報の受付では、例えば自社製品に関連する脆弱性情報を報告してもらうための Web サイトや、受付用の電話窓口などを設置する。もし、バグバウンティ（脆弱性報奨金制度）などを導入する場合は、受け付けた情報に対して報奨金を支払う仕組みへの考慮も必要となる。

脆弱性情報の公開では、報告された脆弱性への対処を行った後、脆弱性を塞ぐための修正パッチなどを Web サイトなどから公開する。ただし、現在の車載 ECU で脆弱性が見つかった場合、ディーラなどでプログラムの修正を行うことが一般である。そのため、対象となる車両をディーラまで持ち込んでもらうための案内を、ユーザに郵送するなどの仕組みで対応するケースも考えられる。