IPA

安全関連システムのセキュリティ向上にむけて

制御システム セーフティ・セキュリティ要件検討ガイド

–基本編–

第1版

はじめに

従来、社会インフラで使用される制御システムは、独自システムによる閉じた環境で運用されてきましたが、IoT化などのオープン技術の進展や事務系システムとの相互接続など稼働環境が大きく変化しています。

近年では、サイバー攻撃の増大により、セキュリティ対策が急務となっています。しかしながら現場では、「セーフティとセキュリティ双方に精通した技術者が極めて少ない」、「セキュリティ要件を実現した場合、安全要件に及ぼす影響をどう考えたらよいのかわからない」などの課題に直面しています。

セーフティ関係者の多くはセキュリティリスクへの認識は十分とはいえません。同時に、セキュリティ関係者の多くには、機密漏洩が健康や安全性、環境にとって重大な影響を及ぼすとの認識が不足しています。両者が相互にわかりあい、連携してゆくにはまだ時間を要すると思われます。

一方、安全規格に適合済の既設システムを多数抱え、運用している事業関係者からは、「安全性を確保しながらセキュリティ検討をどのように進めたらよいのか」という差し迫ったニーズが多く寄せられています。

そこで、本書はまず現状すぐに取組みを進める上での基本的な考え方、検討の手順を示しました。セーフティとセキュリティの本格的な連携については、双方関係者の理解、認識がより深まった将来に扱うこととしました。

本書が、セーフティなシステムを手がける企業がこれからサイバーセキュリティの取り組みを進めてゆく上で、参考になれば幸いです。

基本編：目次

1．本ガイドの概要

目的

本書は以下を目的として作成しました。

■既存のセーフティシステム*1に対し、セーフティ*2要件とセキュリティ要件を連携させ、すり合わせるための考え方を示します。

■さまざまな産業分野で汎用的に活用できるよう、基本となるプロセスを、ケーススタディにより例示します。

■本書の構成
本書は、基本編とケーススタディ編の2分冊です。

基本編	基本となる検討プロセスの手順
ケーススタディ編	検討システムによる解説

- 基本編では、セーフティ・セキュリティ検討プロセスの手順を概説しています。
  各産業領域で実際に活用する際の「適用上のポイント」を掲載しました。
- ケーススタディ編では、より理解を深めることができるよう、抽象化されたシステム（以降、検討システムと称する）を用いて詳細に解説しています。

＊1）本書では便宜上「安全」を「セーフティ」、国際機能安全規格に適合した安全関連システムを「セーフティシステム」と表記しています。
またセーフティ・セキュリティをS&Sと表記している箇所もあります。
＊2）セーフティ、セキュリティ等用語定義は付録Aを参照してください。

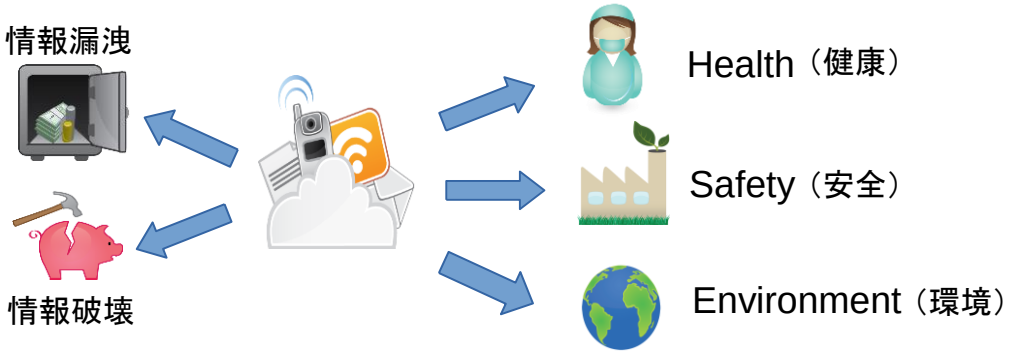
基本的な考え方

【セーフティファースト】

■本書は、セーフティシステムを含む制御システムによって稼働中の工場、プラント等があり、セーフティゴール（安全性の確保）は実現済であるという環境を想定します。

■こうした既存設備に対し、セキュリティ対応を行います。セーフティとセキュリティを同時検討し、新システムを構築する場合は対象外とします。

■情報システムと異なり、制御システム特有のセキュリティ要素を考慮する必要があります（右図）。



【グローバル対応と関連規格】

■事業のグローバル化に伴い、国際規格の認証取得を行う企業が増えています。本書では、汎用性のある下記規格に基づく内容としています。

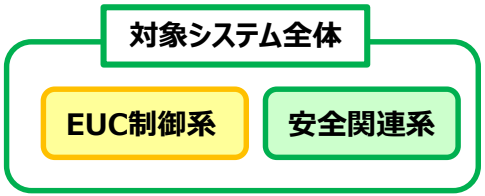
- IEC 61508 series – 電気・電子・プログラマブル電子安全関連系の機能安全
- IEC 62443 series - 産業用通信ネットワーク-ネットワークシステムセキュリティ

■実際のシステム開発においてセキュリティ対応を行う場合、各分野の国際規格（本ガイド付録D参照）への適合が求められます。

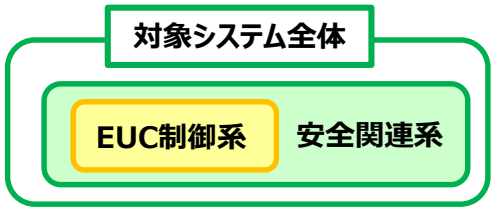
前提事項

【本書で扱う制御システム】

- 電気、石油・ガス、化学、輸送他の重要インフラの内、システム障害発生時に及ぼす人命や環境への影響に関わるシステムは、国や地域の法規制及び国際規格、業界標準等に基づきライフサイクル全般にわたる安全性を重視したものづくりが行われています。
- セーフティシステムは一般的に安全関連系を通常のEUC*1制御系と分離した構成として構築します。
- ケーススタディ編では下図の分離構成に基づくセーフティシステムを前提としています。



安全系と非安全系を分離した構成
（ケーススタディ編の構成）



安全系の中に非安全系が同居した構成*2

*1) EUC(Equipment Under Control) : 被制御機器

*2) IEC 61508では安全関連系が安全機能及び安全以外の機能の両方を実現しなければならない場合、どの非安全関連機能が故障しても、安全関連機能には危険側故障が生じないことを示さない限り、全てのハードウェア及びソフトウェアは、安全関連であるとして取り扱わなければならないと規定する。

前提事項

【想定読者】

■中級レベルのセーフティ開発の経験・スキルを持つインテグレータ
- セーフティシステム開発の経験はあるが、セキュリティについてはまだ十分な経験を持っていない

■セーフティシステムを含む重要インフラを保有する事業者

【その他留意事項】

■工場並びに生産設備システムの構築・運用の関係者として、事業者、システムインテグレータ（以下インテグレータ）、機器メーカを想定します。
- 事業者：工場並びに生産設備システムの保有者
- インテグレータ：システムの安全要求とセキュリティ要求および両者の妥当性確認の遂行者
- 機器メーカ：システムに適用される安全制御機器、セキュリティ機器等の規格適合品の供給者

■実際の検討では、対象設備も広範にわたり多種多様な動作仕様、機器を扱うため、作業ボリュームが膨大になると予想されます。
本書は「検討時の要点・考え方を示すことが主眼」です。そのため、本書の解説は、仮定もしくは状況設定を行い、範囲ならびに深掘りの程度も限定していることにご留意ください。

コラム：情報セキュリティと制御セキュリティの違い

■安全性を求められる制御システムのセキュリティ対応を検討する際は、情報システムとの違いを理解しておく必要があります。

	情報システム	制御システム
対象	・情報	・モノ（設備、製品）、サービス（連続稼働）
技術サポートの期間	・３～５年	・10~20年
システム更新	・随時パッチ対応可能	・停止・再起動は容易ではない
目的・優先順位	・情報漏えいの防止 ・潜在的な脅威から守る ・C(機密性)、I(完全性)、A(可用性)	・サイバーセキュリティ脅威、潜在的な危険に至る脅威から制御システムを守る ・H(健康)、S(安全性)、E(環境)＋A(可用性)、I(完全性)、C(機密性)
分析・対策	・脅威分析	・安全分析と脅威分析
	・サイバーセキュリティを考慮した設計 ・継続監視 ・インシデントレスポンス	・サイバーセキュリティを考慮した設計 ・安全を考慮した設計 ・継続監視 ・インシデントレスポンス
運用管理	・主に情報システム部門	・主に現場の生産・技術部門

2. 基本プロセス

セーフティ・セキュリティ（S&S）検討プロセスの概要

- 生産設備を所有する事業者の要請により、インテグレータが事業者と共にセーフティシステムに対し、サイバーセキュリティ対応を行うための検討プロセスを示します。

- セーフティシステムはすでに構築済という想定です。
プロセスの冒頭（Step0）で、その経緯を確認する工程を補足的に説明します。

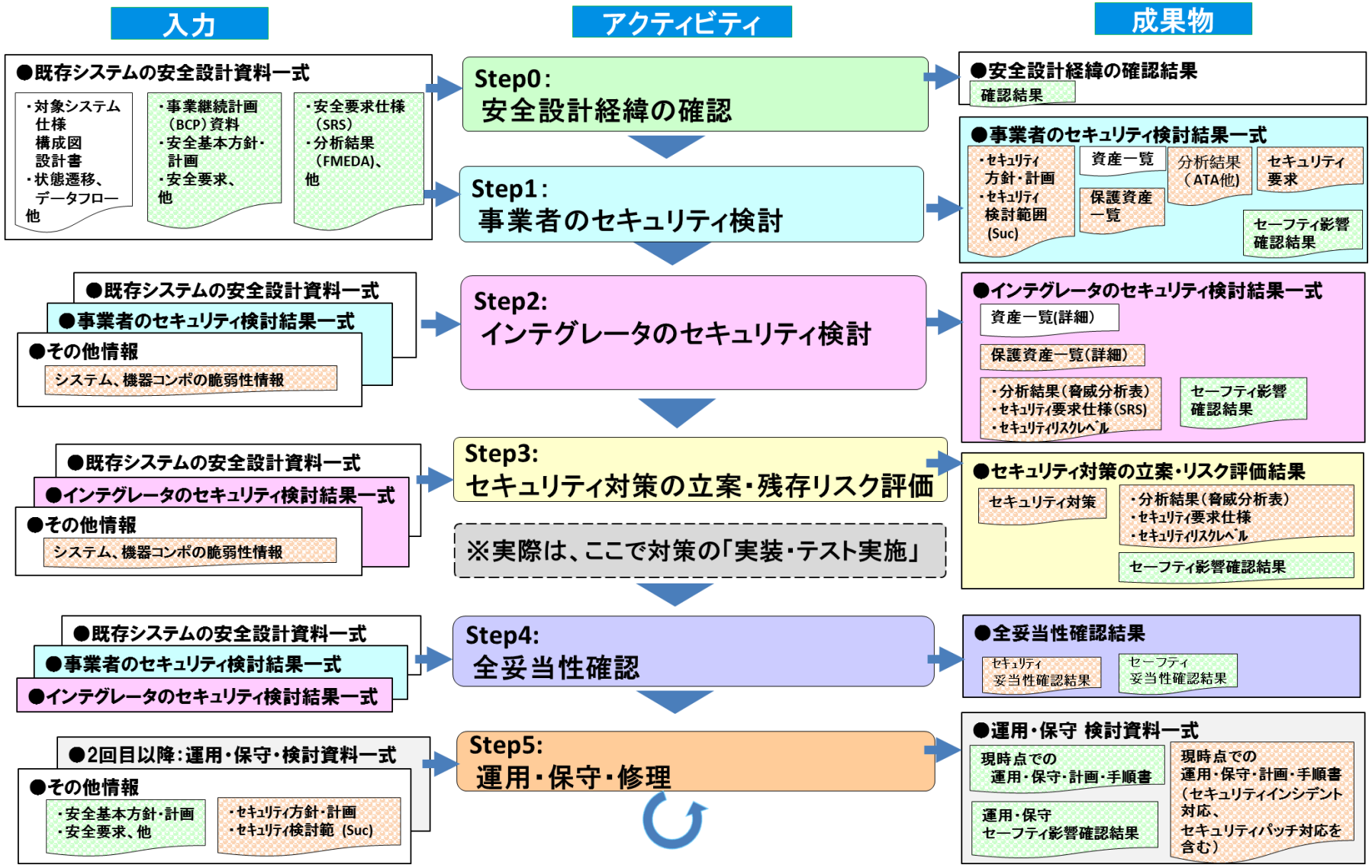
- インテグレータは必要な機器を機器メーカから調達するものとします。

- 以上の想定に基づき本プロセスは、事業者とインテグレータの活動にフォーカスし、機器の開発・実現フェーズは対象外とします。

- 基本編ではプロセスの概要を述べ、詳細はケーススタディ編で解説します。

「既存の制御システム」に対するS&S検討プロセス（全体像）

■下図はステップごとの入出力情報を示したものです。



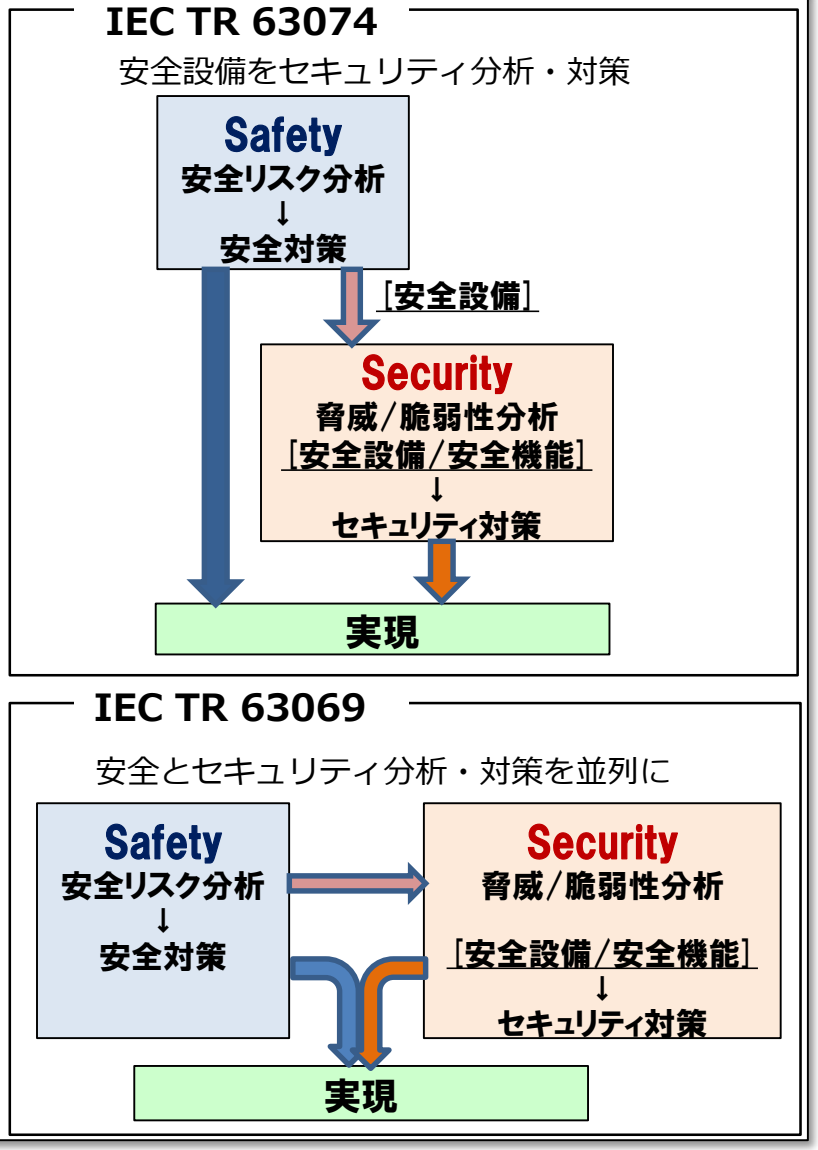
コラム：国際規格における制御システムのS&Sプロセス検討

■産業オートメーションシステムの機能安全とサイバーセキュリティの統合に向けた規格策定が進んでいます。

- IEC TR 63074
  （安全制御系のセキュリティ面／TC44機械安全分野）
- IEC TR 63069
  （機能安全とサイバーセキュリティの連携フレームワーク／TC65産業オートメーション）

■前者は既存の安全制御システムのためのセキュリティ対策であり、本書の方針に類似しています。
一方、後者はより一般的な制御システムにおける安全とセキュリティの分析・対策を目指しています。

■これらの規格を参考に、各分野の安全・セキュリティ規格の開発が進むと思われます。



セーフティ・セキュリティ（S&S）検討プロセスの概要

Step0　安全設計経緯の確認

検討システムの安全設計経緯の理解 （検討システムはIEC 61508準拠システムとして実現済）

Step1　事業者のセキュリティ検討

事業者は、事業者視点で、一連のセキュリティ分析・要求抽出を行い、セキュリティ要求をインテグレータに提示する。

Step2　インテグレータのセキュリティ検討

インテグレータは、インテグレータ視点で、一連のセキュリティ分析・要求抽出を行う。

Step3　セキュリティ対策の立案と残存リスク評価

インテグレータは、機器メーカの協力を得て、セキュリティ対策を立案し、残存リスクを評価し、セキュリティ要求を満足しているか妥当性確認を行う。

Step4　全妥当性確認

事業者とインテグレータは、共同で安全・セキュリティ・仕様要求を満足しているか全妥当性確認を行う

Step5　運用・保守・修理

運用・保守・修理のセーフティ・セキュリティ対応を行う

Step 0　安全設計経緯の確認

Step0　安全設計経緯の確認

入力	アクティビティ	成果物
・事業継続計画（BCP）資料 ・安全基本方針・計画 ・安全要求、他	0-1 検討システムの事業上のリスクを確認 ・事業リスクの確認 ・安全基本方針の確認	
・検討システム仕様・構成図・設計書 ・状態遷移、データフロー他	0-2 検討システムの概要を確認 ・概要 ・関係者 ・ライフサイクル ・安全対策の経緯 ・デフォルトのセキュリティ機能	確認結果
・安全要求仕様（SRS） ・分析結果（FMEDA）、他		

Step1　事業者のセキュリティ検討

＜入力・成果物の区分＞
一般要求事項　セーフティ　セキュリティ

Step 0　安全設計経緯の確認

■セキュリティ検討に先立ち、既存の検討の対象となるシステム（以降、検討システム）の安全設計経緯を確認します。

■検討システムは機能安全規格の認証取得済という前提です。ただし、構築当時から時間が経過し、当時の担当者が不在あるいは当事の設計者であったとしても失念していることも考えられます。そのため、構築当時に考慮された事業リスク、安全設計の方針を再確認します。

■事業者はインテグレータ・機器メーカと共同で作成した
- 安全要求仕様書（SRS*1）等のドキュメント
- FMEDA*2などの安全分析のエビデンス

などを用い、検討システムの危険事象ならびに安全機能を確認します。

*1) SRS（Safety Requirement Specification）：安全要求仕様
*2) FMEDA（Failure Modes Effect and Diagnostics Analysis）:故障モード影響診断解析

Step 1　事業者のセキュリティ検討

Step0　安全設計経緯の確認

Step1　事業者のセキュリティ検討

入力	アクティビティ	成果物
・事業継続計画（BCP）資料 ・安全基本方針・計画 ・安全要求、他	1-1 セキュリティ方針・計画の策定、SuC＊1識別	・セキュリティ方針・計画 ・セキュリティ検討範囲（Suc）
・検討システム仕様・構成図・設計書 ・状態遷移、データフロー他	1-2 セキュリティリスク分析 ・事業者による資産明確化 ・ZC（ゾーン・コンジット）分割 ・保護資産の抽出 ・影響度・発生可能性評価 ・セキュリティ要求の抽出	資産一覧 分析結果（ATA他） 保護資産一覧 セキュリティ要求
	1-3 セーフティへの影響確認	セーフティへの影響確認結果

Step2　インテグレータのセキュリティ検討

＜入力・成果物の区分＞
一般要求事項　セーフティ　セキュリティ

*1) SuC（System under Consideration ）：セキュリティ検討対象システム

Step 1　事業者のセキュリティ検討

- 最初に、事業者の視点でセキュリティ対応方針を明確にします。この対応方針には、インシデントレスポンスのための計画も含まれます。

- 次に、事業者が把握する範囲で保護資産を抽出し、セキュリティリスク 分析を行います。この結果を「セキュリティ要求」としてインテグレータに提示します。

- セキュリティ要求の例を以下に示します。
  - （可用性）故意や過失などによる生産システムの停止を防止し、許可された利用者が必要なときに必要な情報にアクセス可能であることを確実にすること。
  - （完全性）生産システムの情報・データが常に完全であることを保証すること。
  - （完全性）許可されていない利用者によってデータを改ざんまたは破壊されるのを防ぐこと。
  - （機密性）生産に関わる情報には許可された利用者のみアクセス可能とすること。

- 既存のセーフティシステムにセキュリティ要求が与える影響を事業者の視点で確認します。

Step 2　インテグレータのセキュリティ検討

Step1 事業者のセキュリティ検討

Step2　インテグレータのセキュリティ検討

入力

- ・検討システム 仕様・構成図・設計書
- ・状態遷移、データフロー 他
- ・セキュリティ方針・計画
- ・セキュリティ検討範囲（Suc）
- 資産一覧
- ・安全要求仕様（SRS）
- ・分析結果（FMEDA）、他
- 分析結果（ATA他）
- 保護資産一覧
- セキュリティ要求
- システム、機器の脆弱性情報
- セーフティへの影響確認結果

アクティビティ

2-1　事業者からの要求事項の確認
- ・事業者セキュリティ要求事項の確認
- ・システム構成の詳細化

2-2　セキュリティリスク分析
- ・セキュリティリスク分析の手順
- ・インテグレータによる保護資産の抽出
- ・脅威の識別
- ・脆弱性の識別
- ・被害内容の確認

2-3 リスク評価
- ・評価指標
- ・リスクレベルの求め方
- ・リスクレベルの決定

成果物

- 詳細資産一覧
- 保護資産一覧（詳細）
- ・分析結果（脅威分析表）
- ・セキュリティ要求仕様
- ・セキュリティリスクレベル
- セーフティへの影響確認結果

Step3 セキュリティ対策の立案と残存リスク評価

＜入力・成果物の区分＞
一般要求事項　セーフティ　セキュリティ

Step 2　インテグレータのセキュリティ検討

■インテグレータは事業者作成のセキュリティ検討資料に基づき、セキュリティ要求事項を確認します。

■次に、開発製品や調達品の情報に基づき、システム構成を詳細化し、分析の準備を行います。

・インテグレータは購入製品も含め当該システムを構成する製品の脆弱性を把握できているものとします（コラム  ）。

■以下の手順でセキュリティ分析を実施します。（脅威分析シート（付録C)を活用）

抽出・検討項目		備考	
保護資産の抽出		インテグレータによる保護資産の抽出	
脅威の識別		脅威の分類（通信妨害、不正アクセス、改ざん、脆弱性利用・・）	
脆弱性の識別		事業リスクにつながる事象・事業者セキュリティ要求からの逸脱	
被害内容の確認		脅威事象発生時の被害内容	
リスク評価	影響度	3段階のレベルで分類	高中低
	発生可能性	3段階のレベルで分類	高中低
	リスクレベル	3段階のレベルで分類	高中低

コラム：脆弱性情報はどこから？データベース化のすすめ

■一般的な情報システムの脆弱性、セキュリティ攻撃等に関する情報は、以下の機関、団体などから収集できます。システムに関する脆弱性情報は機器ベンダ含め、データベース化などにより常日頃から共有・蓄積できる仕組みを用意しましょう！

■セキュリティ情報参照先（例）

- JPCERT/CC （一般社団法人JPCERTコーディネーションセンター）
- IPA/ISEC（独立行政法人情報処理推進機構 セキュリティセンター）
- ICS-CERT(The Industrial Control Systems Cyber Emergency Response Team)
  ※米国国土安全保障省（DHS)の組織
- JNSA（特定非営利活動法人日本ネットワークセキュリティ協会）
- NISC（内閣サイバーセキュリティセンター）

Step 2　インテグレータのセキュリティ検討

- 保護資産の抽出時、
  「H（健康）S（安全性）E（環境）＋A（可用性）I（完全性）C（機密性）」
  の観点を考慮します。

- セキュリティ分析には様々なものが知られていますが（付録B参照）、本書では全体を鳥瞰しやすく、各要素同士の関係性を理解しやすいと思われるATA（攻撃木分析）を用いています。

- 発生可能性及び発生時の影響度の面からリスク評価します。これらは、攻撃者のスキルや攻撃の動機などによっても変化します（コラム  ）。

コラム：脅威分析における要素（攻撃の容易性）

■セキュリティリスクはセーフティのように確率的に発生するわけではなく、攻撃者側の動機・攻撃スキルなどの要素にも依存します。
しかし、攻撃者側の動機や攻撃の容易性に関する要素は数値化しにくいのが現状です。例えば、以下の要素別の観点で、最初にスコアリング評価を実施し、最終的には、これらの要素を総合的に評価し、「脅威の発生のしやすさ」を考えて判断してもよいでしょう。

脅威として考える要素	具体的な評価指標
攻撃にどのくらい時間を要するか	攻撃に必要な時間が何日か？何年か？ 事実上不可能な計算量か？
専門知識がどのくらい必要か	ツールがあればできるレベルか？ IT技術者が可能なレベルか？研究者レベルか？
対象のシステムがどのくらい知られているか	仕様の公開がなされているのか？ 一般に入手が難しい仕様か？
攻撃のタイミングがどの程度与えられているか	いつでも攻撃可能か？ 保全を行っているときのみ攻撃可能か？
攻撃する装置の入手の困難性	攻撃ソフトウェアが入手容易か？ 対象ハードウェア、ソフトウェアが入手容易か？

Step 3　セキュリティ対策の立案と残存リスク評価

Step2　インテグレータのセキュリティ検討

Step3 セキュリティ対策の立案と残存リスク評価

入力	アクティビティ	成果物
・検討システム 仕様・構成図・設計書 ・状態遷移、データフロー他 保護資産一覧 システム、機器の脆弱性情報 ・分析結果（脅威分析表） ・セキュリティ要求仕様 ・セキュリティレベル ・安全基本方針・計画 ・安全要求、他 ・安全要求仕様（SRS） ・分析結果（FMEDA）、他	3-1セキュリティ対策の立案 ・対策の立案と残存リスク評価 3-2セーフティへの影響確認 ・確認事項 ・影響有無の確認	セキュリティ対策 ・分析結果（脅威分析表） ・セキュリティ要求仕様 ・セキュリティリスクレベル セーフティへの影響確認結果

Step4　全妥当性確認

＜入力・成果物の区分＞
一般要求事項　セーフティ　セキュリティ

Step 3　セキュリティ対策の立案と残存リスク評価

■特定されたセキュリティ脅威に対する対策を立案します。

※事業者のセキュリティ要求を満たしているか、脅威の度合いが許容範囲までに低減できることを確認します。本ステップは必要に応じ、機器メーカと共同で実施します。

■立案されたセキュリティ対策のセーフティに及ぼす影響を検証します。

- セキュリティ対策がセーフティ機能を毀損しないか
  （効果が同等の代替案があればセーフティに影響しない対策案を選択）
- セーフティ機能がセキュリティ対策をバイパスしたり無効化していないか

■セキュリティ対策の内容によっては、セーフティ機能との両立性を検証するために多くの時間とコストを要する場合もあります。対策の実装がセーフティシステムの改変を伴うのであれば、機能安全再認証が必要になります。そうした場合は事業判断を含めた検討を行うことになります。

■本書では実現フェーズを含めていません。ただし実際の開発では本ステップ以降の実現フェーズを通じ、残存リスクが許容範囲まで低減できることを評価します。

コラム：再利用・購入機器のセキュリティ

- IEC 61508、ISO 26262では、
  - 再利用コンポーネント
  - サプライヤが提供する、COTS＊1、SEooC ＊2コンセプト製品
  - システム開発に使用するツール群

  に対しても評価を行い、安全妥当性の確認を行うことが要求されています。
- IEC 62443では、
  対象機器のセキュリティ機能要求、ソフトウェア開発プロセスに関する要求の記載があります。
- 本書のケーススタディ編で紹介する、「セーフティな既存システムにセキュリティ対策を行う」ケースでも、そのシステムで利用するコンポーネントに、脆弱性が潜んでいないか？セキュアに設計・開発された製品か？確認します。制御システムは、安全機構としてのコンポーネントが存在するため、慎重に評価・導入を決定しなければなりません。（例：EDSA認証＊3製品）

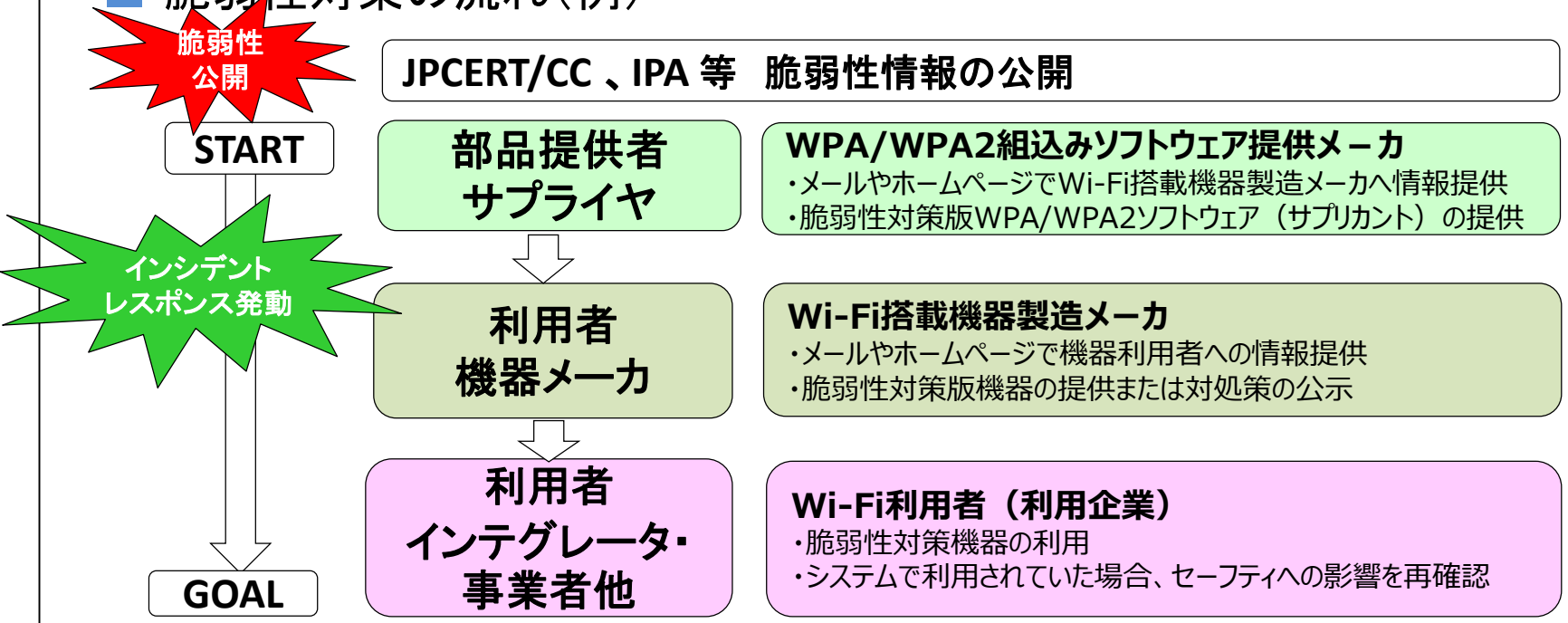
＊1） COTS（commercial off-the-shelf）商用目的の既製ソフトウェア製品やハードウェア製品、ライセンス
＊2） SEooC（Safety Element out of Context） 想定仕様外の安全エレメント
＊3） EDSA認証　制御機器認証プログラム「EDSA」国内認証制度

コラム：機器・部品に脆弱性がみつかったら？

無線LANの脆弱性 （事例）

2017年10月にWPA/WPA2（Wi-Fi認証プロトコル）に関する脆弱性（KRACKs：Key Reinstallation Attacks：鍵再インストール攻撃）がベルギーの研究者により公開されました。
KRACKsは、悪意のある第三者によるリプレイ攻撃により、暗号通信で使用しているセッション鍵(暗号通信用の鍵)が推測され、通信の盗聴や改ざん等が行われるという脆弱性です。
WPA2は、Wi-Fi暗号化通信認証でセキュリティレベルが高いとされていたため、様々な機器に実装されていました。そのため、その脆弱性対策が多くのメーカや利用者で必要となりました。

脆弱性対策の流れ（例）



Step 4　全妥当性確認

Step3 セキュリティ対策の立案と残存リスク評価

Step4　全妥当性確認

入力

- ・安全基本方針・計画
- ・安全要求、他
- ・安全要求仕様（SRS）
- ・分析結果（FMEDA）、他
- セーフティへの影響確認結果
- ・検討システム仕様・構成図・設計書
- ・状態遷移、データフロー他
- セキュリティ対策
- ・分析結果（脅威分析表）
- ・セキュリティ要求仕様
- ・セキュリティレベル

アクティビティ

- ・安全妥当性確認
- ・セキュリティ妥当性確認

成果物

- セーフティ妥当性確認結果
- セキュリティ妥当性確認結果

Step5　運用・保守・修理

＜入力・成果物の区分＞
一般要求事項　セーフティ　セキュリティ

Step 4　全妥当性確認

■事業者はインテグレータと共同で、セキュリティ対策が実装された機器コンポーネント及び、サブシステムより構成される検討システム全体が、元々のセーフティ要求を満たしていることを確認します。

■同時に、セキュリティ対策により、検討システム全体のセキュリティ要件を満足できていることを確認します。

■上記の確認は、インテグレータから提出されたドキュメントチェック、実稼働環境において実施すべき動作試験（ペネトレーション試験＊1など）で行われます。

＊1）ペネトレーション試験：　既知の手法を用いて実際に侵入や攻撃を試みる試験

Step 5　運用・保守・修理

Step4　全妥当性確認

Step5　運用・保守・修理

入力

- ・安全基本方針・計画
- ・安全要求、他
- ・セキュリティ方針・計画
- ・セキュリティ検討範囲（Suc）
- ・2回目以降は、現時点での運用・保守計画・手順書

アクティビティ

- ・セキュリティ対応計画の立案と実施
- ・継続的メンテナンスの実施

成果物

- ・現時点での運用・保守計画・手順書
- 運用・保守セーフティへの影響確認結果

＜入力・成果物の区分＞
一般要求事項　セーフティ　セキュリティ

Step 5　運用・保守・修理

■セキュリティ対策として、以下のような、運用・保守で行うべき事項があるか確認します。
- 定期的な脆弱性確認、パッチ適用、侵害時エスカレーション手順、関係者コンピテンシー管理、入退管理、遠隔保守など

■運用・保守で行うべき項目があった場合、既存のセーフティに関わる運用・保守の対応体制、ドキュメントに対し、その項目に対してセキュリティ運用に関連する内容を反映します。

■運用開始前までに、以下の事項等を含む情報を関係者で周知、共有します。
- セキュリティ対策が反映された運用・保守仕様
- セキュリティインシデントレスポンスが含まれた運用・保守手順

■運用開始以降は、各種手順書・計画書を継続してメンテナンスします。

3. 産業分野適用時のポイント

本章について

■本書ではさまざまな産業分野で活用できるものとするため、セーフティは IEC 61508、セキュリティは IEC 62443 に基づいています。

■一方、分野ごとに産業発展の経緯あるいはビジネスモデルが異なります。セーフティ対応は各分野の子規格（付録D参照）への適合を要するなど、実開発に適用する際には各分野の事情、製品の特徴に即した対応が必要です。

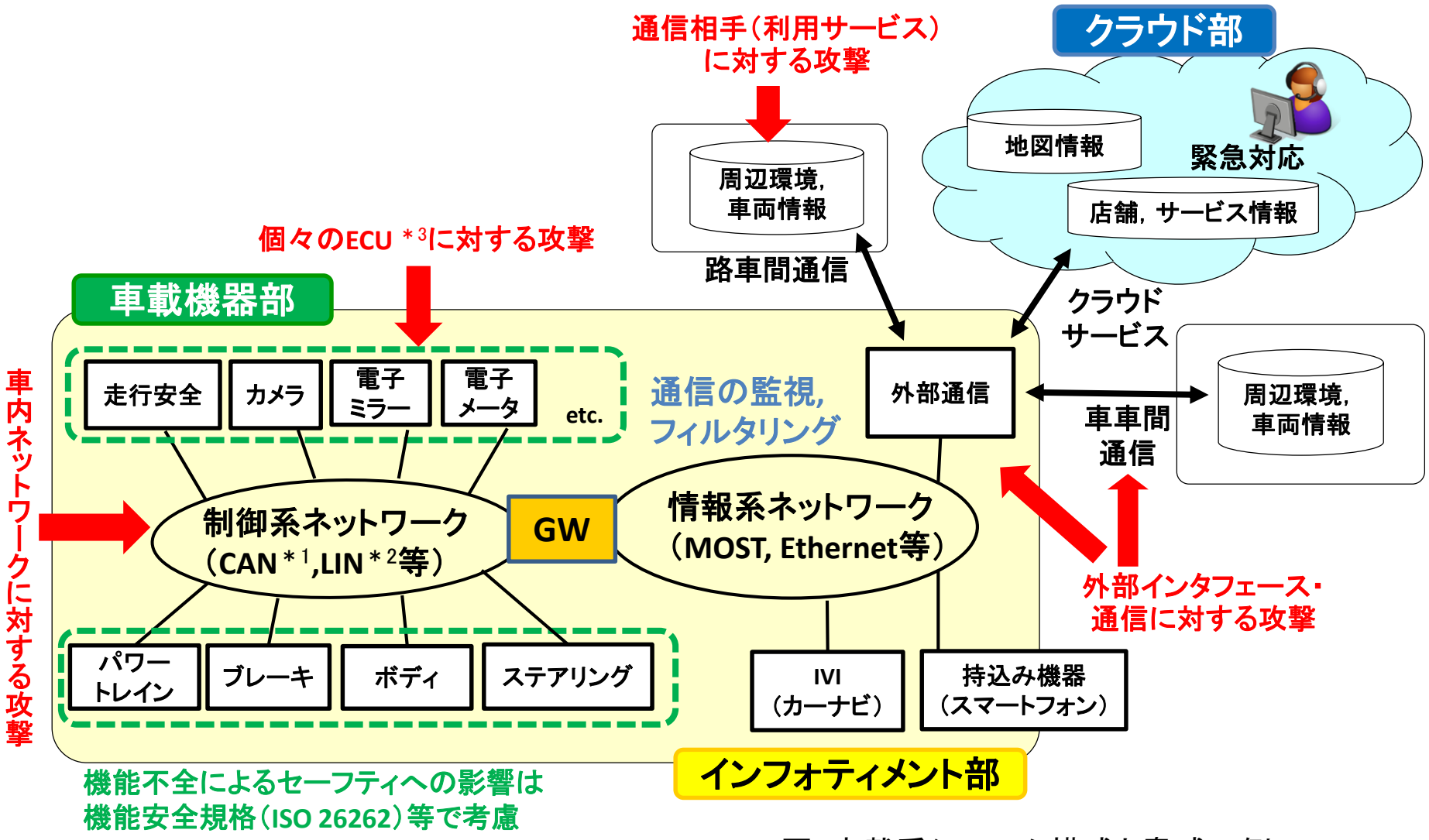
■そこで本章では、各産業分野における事情を以下の観点で整理し、セキュリティ対応を行う上で気を付けるべきポイントをまとめました。

①システム構成
②使用者・関係者
③リスク分析

3-1 車載系システム

自動車を取り巻く環境の現状と変化	●利用形態の変化 ・人間自らが運転➡人間による運転のみを前提としない運転（自律走行） ・車の個人所有➡車の共有・共有利用 （カーシェア、ライドシェア） ●機能の変化 利用形態の変化に伴い、自動車に搭載される機能も変化しています。 ・セーフティを維持・向上させる運転支援技術 ・より快適で便利な移動を支援するインフォテインメント技術 ・利用形態の多様化に伴う自動車管理技術（例：スマートフォンでドアの開閉を実現） ●仕組みの変化 搭載機能の増加や、環境への影響減を目指して自動車の仕組みも変化しています。 ・ガソリンエンジン➡ハイブリッド、EV ・電動化、車車間／路車間／外部ネットワークとの通信、IT技術の導入 これらの変化は、車両の管理方法、セキュリティ対策を考える上での前提、責任の所在にも大きな影響を与えます。セーフティに影響を及ぼす可能性のあるセキュリティ脆弱性を持つ自動車がリコールの対象にもなりました。
関係者	●利用者 （個人、レンタカー／カーシェア・ライドシェアサービス提供会社） ●開発者 （自動車・自動車部品・車載半導体各メーカ、ソフトウェアベンダ） ●保守者、販売者 （ディーラ、修理・中古販売・個人売買支援会社）
分析 ・範囲	●分析者：自動車メーカ、自動車部品メーカ、自動車関連サービス会社 ●分析方法:セーフティの分析結果をベースに、セキュリティの分析を進める。 市場に出ている自動車の種類が多岐に渡ること、利用形態が拡大していることを踏まえて、分析対象や前提を検討します。 ●守るもの：人命、自動車、所有者や利用者の個人情報

3-1 車載系システム



図：車載系システム構成と脅威の例

＊1）CAN（Controller Area Network）　＊ 2）LIN(Local Interconnect Network)　＊3)ECU（Engine Control Unit）

3-1 車載系システム

想定される脅威と対策

●車載機器部：走る、曲がる、止まるなど自動車の本来の機能部
（脅威）・車はインターネット接続を未想定であり、車内LANのCANは暗号化されていません
・CANの接続先のECUに対し、外部から変な信号が入り誤動作する可能性があります
（対策）・車内LANそのものを暗号化するAutosar＊1のSecOC＊2
・HW暗号復号を行うHSM＊3搭載のEVITA＊4（規格化）➡車載機器部のセキュリティ強度（高）
・稼働中の車、コスト面の考慮から、現行CANに対し、不正規なコマンドパターンの検知機能を設け、不正規コマンドを無効化するアプローチCMI-ECU＊5などの対策

●インフォテイメント部：ナビやオーディオなど乗員に走行以外のUIを提供
（脅威）・USBやBluetooth等を通じ他機器と接続。インターネット通信同様のセキュリティリスク
（対策）・PCなどと同様に、外部や内部（車載機器部）との通信部にファイヤウォール設置
・OS・アプリ、権限情報などの改ざん検知

●クラウド部：レストラン、駐車場などの膨大な情報を、自動車に外部から提供
（脅威）・通常のインターネット接続と同様
（対策）・同様のセキュリティ対応が必要（会員サービスシステム接続時：会員認証・アクセス権限対策）

●路車間通信、車車間通信
（脅威）・通信相手（利用サービス）に対する攻撃、外部インタフェース・通信に対する攻撃
（対策）・車両情報の信頼性確保（電子署名、証明書等）と、セキュアな通信制御装置の利用など

●全体として
学会等の場では、以下のような複合的攻撃手順により、悪意の第三者が他人の自動車の運転を邪魔する例が報告されています
・CANコマンドの解析（オフライン実施）
・インフォテイメント部のオンエアアップデート悪用による改ざん
・インターネット部でのユーザなりすまし
そのため、車載セキュリティではアーキテクチャ全体の把握と全体視点での対策が求められます

＊1）Autosar（AUTomotive Open System Architecture）　＊2）SecOC（Secure on Board Communication）
＊3）HSM（Hardware SecurityModule）　＊4）EVITA（E-safety Vehicle Intrusion proTected Applications）　＊5）CMI-ECU（Centralized Monitoring and Interceptor ECU）

3-1 車載系システム

・国際規格
・業界標準
・ガイドライン等

●セーフティ規格：ISO 26262
●セキュリティ規格：ISO/SAE 21434（策定中）

●ガイドライン
JASO TP-15002：情報セキュリティ分析
IPA自動車の情報セキュリティへの取組み：取組み指針
SAE 3061：車載セキュリティのポイント、機能安全プロセスとセキュリティプロセスとの対応関係

●業界の取組み
AUTOSAR：車載システムのソフトウェアプラットフォーム規格の策定
EVITA：欧州の自動車セキュリティ研究プロジェクト。脅威分析や対策技術を検討。
Jaspar：日本国内での業界団体。制御ネットワークにおけるメッセージ認証のガイドラインを策定。
FASTR：ソフトウェア更新のガイドライン策定
Auto-ISAC：自動車の脆弱性報告、管理

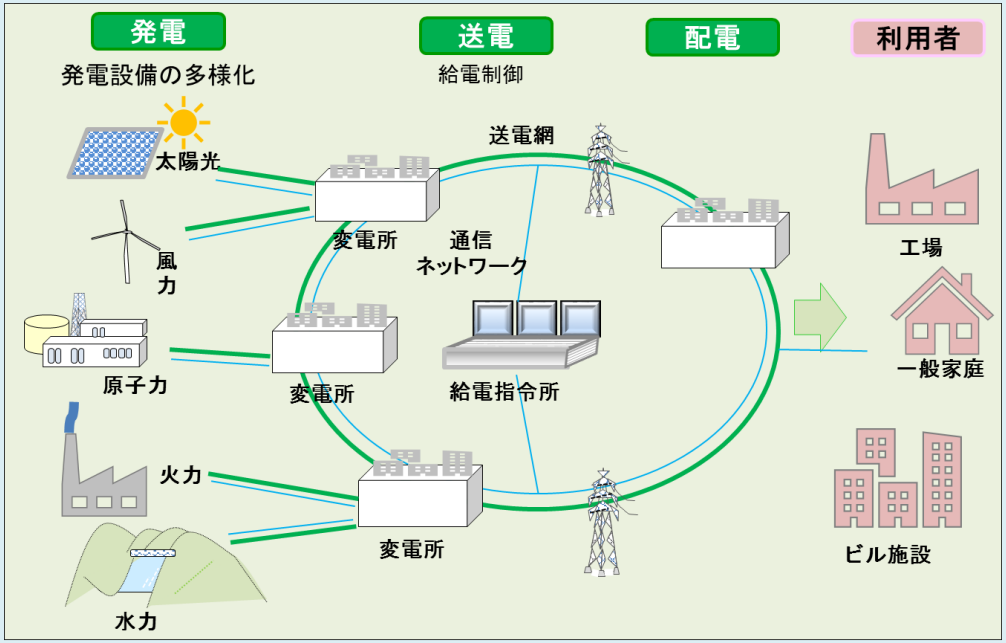
●本ガイド活用について
・セーフティは、自動車メーカの方針やISO 26262をベースに考えられており、すでに自動車メーカやサプライヤでは、セーフティ確保のプロセスが構築されています。
このことから、IEC 61508とISO 26262という規格の違いはあるものの、本ガイドの適用前提に近いといえます。
・セキュリティは、ISO 26262第2版、J3061、ISO/SAE 21434等で現在検討が進んでいます。今後この規格が公開され、適用に至るまでに、セキュリティ上のリスク評価方法の検討や、社内教育を行う際に本ガイドを利用してもよいでしょう。

3-2 電力系システム

電力系システムをとりまく環境

●東日本大震災以降、電力系システムをとりまく環境は大きく変化しています。
・再生可能エネルギーの導入・活用
・電力の供給側・需要側の双方が連携した省エネルギー化
・新規参入の発電事業者や小売事業者との送電・配電網接続

●従来、電気事業者が管理してきた電力系システムは、上記の環境変化に伴い送電網や通信ネットワークに多くの事業者との接点が増加しつつあり、セキュリティ対策もシステム構成に合わせて対応する必要があります。



関係者

●電気事業者
発電事業者、送電事業者、一般送配電事業者、特定送配電事業者、小売電気事業者
●システムインテグレータ、メーカ
●利用者

3-2 電力系システム

分析範囲	●分析者：電気事業者、インテグレータ、メーカ他 ●分析方法:セーフティ・セキュリティの分析については、他システムと、基本は同じですが、電力の安定供給、電気工作物の保安確保を妨害するような目的等、社会情勢の背景を意識したサイバー攻撃を脅威として想定し、運用面でのセキュリティレスポンスを検討するための分析計画も見直す必要があります。
・ガイドライン等	●電力制御システムセキュリティガイドライン 日本電気技術企画委員会（JESC）では、 「電力制御システムセキュリティガイドライン」を2016年に発行しました。 このガイドラインは、電力制御システム等のサイバーセキュリティ対策の的確な実施を目的として、電気事業者が実施すべき電力制御システム等のセキュリティ対策の要求事項が以下のように規定されています。 ・プロセス：セキュリティ管理組織の設置及びマネジメントシステムの構築、教育の実施 ・システム・設備：ネットワーク分離やデータ保護、アクセス制御 ・運用・管理：データ管理や権限割当、パッチ管理 今後、電気事業法下の技術基準及び保安規程に組み込まれることが経済産業省により計画されています。 ●電力制御システムにかかわる各事業者が、このガイドラインの要求事項を実現する際に、本ガイドを、セキュリティ分析の入門書、教育教材として活用できるでしょう。

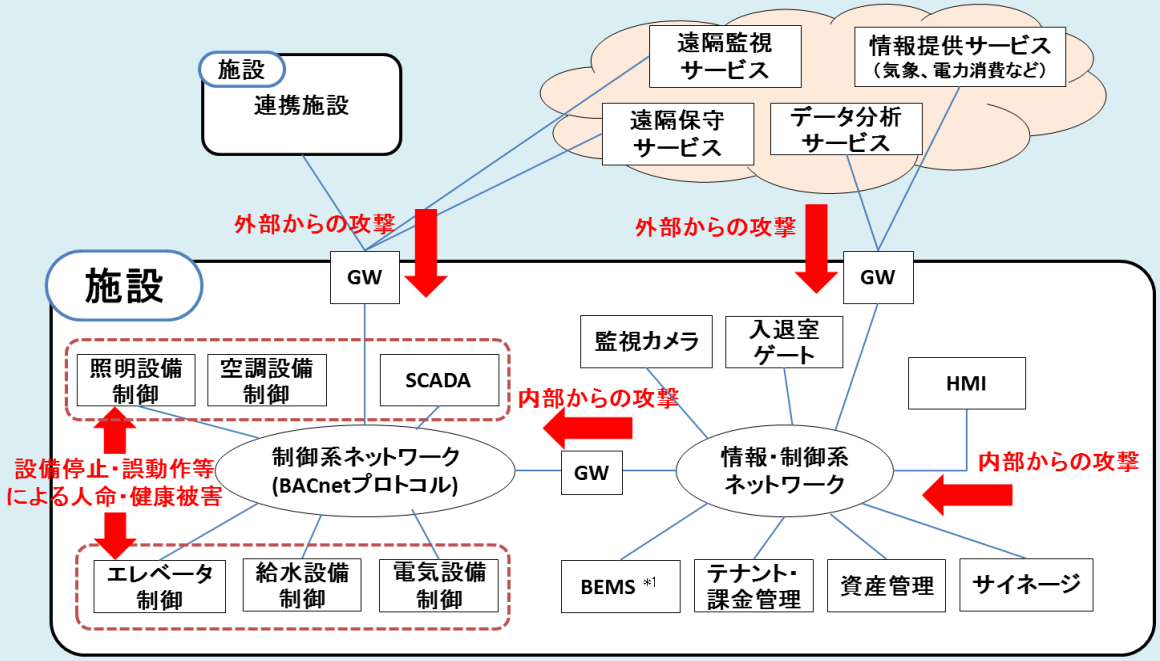
3-3 施設監視制御システム

安全要求事項

システム構成の特徴

●安全性に関する要求事項は、「人命」がほとんどのウェイトを占めます。施設の用途によっては、空調設備、防災設備、防犯設備などの停止や誤動作により健康被害や人命に影響を及ぼす恐れがあります。

●施設監視制御システムは、空調設備、照明設備、エレベータ設備、電気設備、給水設備などの複数の設備や各種センサーがネットワークに繋がるIoT化が進んでいます。構成上の特徴として、情報取得や保守サービスのために外部と接続され、さらに異なるインテグレータによる連携施設の施設監視制御システムが相互に接続されることがあげられます。また複数のメーカかつセキュリティ対策レベルが異なる機器が接続されることもあります。



*1) BEMS: Building Energy Management System

3-3 施設監視制御システム

使用者・関係者	●施設管理者：システム運用者、警備員、清掃業者など ●施設使用者：テナント契約者、テナント従業員、顧客など ●システム供給者：インテグレータ、機器メーカ、保守サービス事業者など
分析レベル ・範囲	●施設監視制御システムのセキュリティ事故関連としては、リモート保守回線を介して保守拠点からマルウェアが感染し施設の操業停止などの被害をもたらした事例や通信プロトコルBACnet実装の脆弱性が報告されています。 例えば、以下のようなセキュリティへの影響が、二次的にセーフティに影響を与える恐れがあるといえます。 ・外部ネットワークからの攻撃によるサービス停止（可用性の喪失） ・施設内部からの攻撃（内部犯、USBメモリ、マルウェア）による制御情報や制御プログラムの改ざん（完全性の喪失） ・施設で扱う図面等の重要情報の漏えい（機密性の喪失） 施設監視制御システムでは、複数のメーカのセキュリティ対策レベルが異なる機器が接続され、またリモート保守や施設間連携のため外部と接続されるケースがあることから、インテグレータは事業者が実施した分析結果における責任範囲を明確化し、分析を進める必要があります。また当該施設の使用目的(オフィス、商業施設、工場、病院、介護、空港、港湾など)によって同種のリスクであってもインパクトが異なることも考慮しなければなりません。特に重要な施設においては、リモートアクセス、USBメモリなどの外部記憶媒体、内部犯に関するリスクを考慮します。施設監視制御システムにおいて保護すべき項目は、人命、個人情報(特にプライバシーに関わるもの)、制御情報(センサーデータ、制御コマンド)を少なくとも含む必要があります。

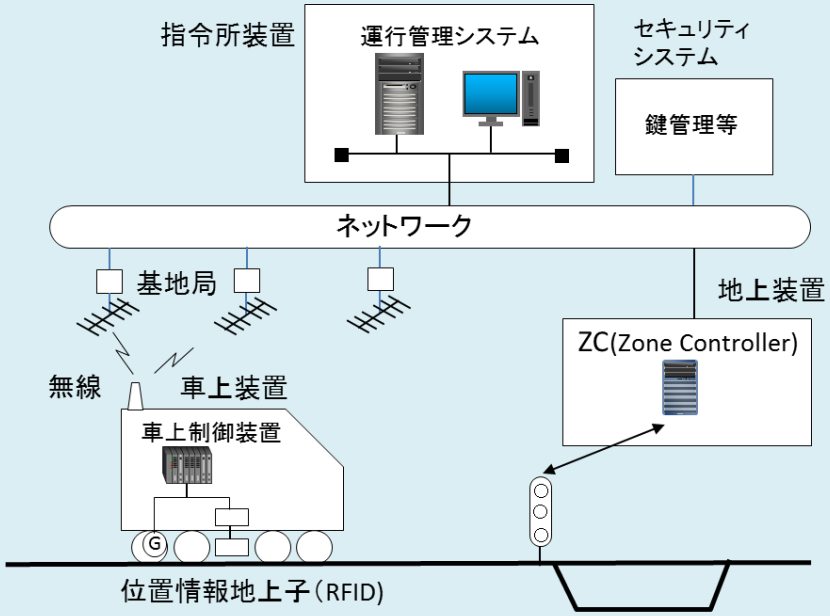
3-3 施設監視制御システム

対策技術	●ネットワーク分離、異常ふるまい検知（人、機器、ネットワーク）、 第三者認証機器使用、セキュリティマネジメントシステム導入、 定期的なセキュリティ診断、CSIRT設置、人員への情報セキュリティ教育など
・業界標準 ・ガイドライン等	●第三者セキュリティ認証： EDSA (CSSC)、CSMS(JIPDEC) ●ガイドライン： IoTセキュリティ総合対策 – 総務省　サイバーセキュリティタスクフォース
・本ガイドの利用ついて	●2020年オリンピック・パラリンピックの国内開催に向け、多数の収容が見込まれる施設や重要設備を収容する設備など大会運営に影響する施設を中心に内部犯を含むサイバー攻撃への警戒が重要視されています。 インテグレータは、本ガイドで説明するセキュリティリスク分析手法により、セーフティに影響する資産（情報資産、機能資産、物理的資産、人的資産）を明確にした上で、想定されるセキュリティの脅威を抽出し、定量評価に基づき、セーフティを考慮した対策の優先度付けを行うことで効果的な対策が可能となります。 また内部犯対策としては、IT的な対策だけでなく、物理対策（IDカードや入退室ゲートの導入など）、人材教育（セキュリティマインドを醸成させる）のような「人的対策」を融合させることが、重要な取り組みとなります。

3-4 鉄道信号システム

システム構成の特徴

●以下は一般的な無線式列車制御システムの概要を示したものです。



安全要求事項

●安全性に関する要求事項は、「人命」がほとんどのウェイトを占めます。
列車の運行における安全状態は明確であり、多くの場合、列車を停止させることが安全な状態遷移であり、想定されない制御となった場合、信号システムは列車を停止させる制御を行います。

使用者・関係者

●開発・製造者/サプライヤ：信号メーカ、装置メーカ
インテグレータ(信号システム)：事業者もしくは信号メーカ
オペレータ/メンテナンス：事業者、信号メーカ
カスタマー：乗客、利用者

3-4 鉄道信号システム

■前記の「無線式列車制御システム」に基づき、事業者・インテグレータが行うセキュリティ検討の手順を示しました。無線等相互接続による新たな脅威への対処を行う上で、本ガイドのStepとの対応も示しています。

本ガイドの
Step1に相当

本ガイドの
Step2に相当

○セキュリティを含めた要求仕様の策定
- ・守るべき資産の明確化
- ・セキュリティ対策と機能への影響検討
- ・安全性とセキュリティ対策の相互影響検討
- ・投資可能金額との関係性検討

○セキュリティ対策継続性
- ・お客様の死亡、怪我、係員の死亡、怪我
- ・セキュリティ対策の見直しルール
- ・CSIRTとの関係性
- ・セキュリティメンテナンスなどの保守契約の検討

○発注仕様、メンテナンス契約仕様の策定

○列車運行に当たっての大きな方針の確認
- ・安全性に関する事項
- ・運行の品質に関する事項
- ・投入する人的・資金的なリソースの確認

○方針と矛盾する好ましからざる事項の抽出
- ・列車の脱線、衝突、追突
- ・運行不能、遅延
- ・セキュリティアップデートのための人員、費用　など

:運用の観点
主として事業者が担当

:システム構築の観点
主としてインテグレータが担当

:両者による協働作業

次頁に続く

3-4 鉄道信号システム

本ガイドの
Step1に相当

本ガイドの
Step2に相当

本ガイドの
Step3以降に
相当

本ガイドの
Step5に
相当

前頁より

○上記事象の重篤性の見積もり
・お客様の死亡、怪我、係員の死亡、怪我
・攻撃によるシステム維持不能によるサービス中断、
レベル低下等

○上記事象が起こる可能性のある攻撃と対応
・有線ネットワーク、無線ネットワーク
・ソフトウェア、データ　などへの攻撃と対処法、費用を検討

○システムのセキュリティポリシーの策定
・システムでの対応と人的対応の切り分け

○インタフェースの分析
・攻撃経路の想定
・保守インタフェースの運用分析

○セキュリティ対策手段の選定

○事業者へのフィードバック

○対策手段実装・テスト

○運用におけるセキュリティ対応の継続

3-5 ヘルスケア系

ヘルスケア（健康・病院・介護）現場の状況 脅威と対策へのアプローチ	●地域医療連携や医療介護連携等の推進を背景に、病院や介護施設の中だけではなく、診断・治療・介護の外部連携がはじまっています。 「個人宅と病院」「病院と病院」「病院と介護施設」等、インターネットを利用した個人データのやり取りは日常になっています。健康診断も定点観察的な健康診断ではなく、生体センサーを利用した継続的な生体データ収集での健康診断に変わっていくかも知れません。 ●従来、病院では、医療機器を中心としてセーフティ対策が重視されてきました。セキュリティ対策は、主に病院の患者個人情報、医療情報システムが対象でしたが、今後は介護施設・自治体などの連携先、つまり「つながった世界」でのセーフティ＆セキュリティ対策の検討が、ヘルスケア分野でも必須となるでしょう。 本ガイドは、システム全体でのリスク分析と必要な対策を考える際の手順として、参考にできるプロセスを紹介しています。
・法規 ・業界標準 ・ガイドライン等	●医薬品医療機器・システムの取扱い ・法規制対象のものは、医薬品医療機器等法（薬機法）が適用されます。 『医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律』 ・法規制対象外は、GHS（Good Health Software）ガイドラインに従うことが推奨されます。 ・医療情報システム＊1でセキュアなシステム構築するには、3省4ガイドライン＊2に従う。 ＊1）医療情報システム・・・電子カルテ、オーダリングシステム、医事会計システムなど ＊2）3省4ガイドライン 厚労省：『医療情報システムの安全管理に関するガイドライン』 総務省：『ASP・SaaS における情報セキュリティ対策ガイドライン』 『ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン』 経産省：『医療情報を受託管理する情報処理事業者における安全管理ガイドライン』

コラム：医療ソフトウェア（ヘルスソフトウェア）のセーフティ＆セキュリティ

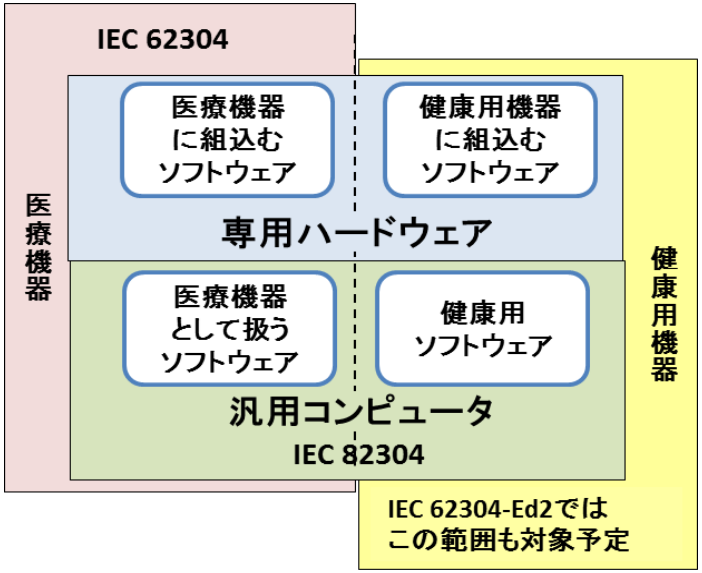
■平成26年の薬事法改正により医療機器の定義に「プログラム及びこれを記録した記録媒体」を加えることになりました（薬機法）。医療機器は、下表のようにリスクの程度により4つのクラスに分類され、クラスにより適切な品質管理が求められます。ヘルスソフトウェアも同様ですが、ソフトウェアの動作プラットフォーム別に、下図のように分類されます。

■リスクマネジメント規格は、JIS T 14971（医療機器–リスクマネジメントの医療機器への適用）があります。また、サイバーリスクのある医療機器プログラムは、「医療機器におけるサイバーセキュリティの確保について」（平成27年4月28日薬食安発0428第1号通知）などを参考に、必要な措置を行う必要があります。

表：医療機器のカテゴリー

国際分類	リスクの程度	改正薬事法分類	医療機器製品の例
クラスⅠ	不具合が生じた場合でも、人体へのリスクはきわめて低い	一般医療機器	Ｘ線フィルム、鋼製小物、体外診断用機器、歯科技工用用品
クラスⅡ	不具合が生じた場合でも、人体へのリスクは比較的低い	管理医療機器	Ｘ線撮影装置、ＣＴ装置、ＭＲＩ装置、電子内視鏡、超音波診断装置、歯科用合金、消化器用カテーテル
クラスⅢ	不具合が生じた場合、人体へのリスクが比較的高い	高度管理医療機器	透析器、人口骨、人工呼吸器、血管用カテーテル
クラスⅣ	患者への侵襲性が高く、不具合が生じた場合、生命の危険に直結する恐れがある		心臓ペースメーカー、人工心臓弁、ステント

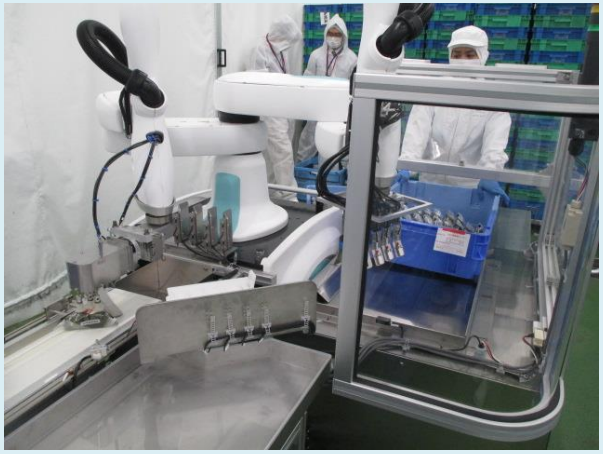
図：ヘルスソフトウェアの分類



IEC 62304：医療機器ソフトウェアーソフトウェアライフサイクルプロセス
IEC 82304：ヘルスソフトウェアー第1部：製品安全の一般要求事項

3-6 産業ロボット

産業ロボットをとりまく環境	●ロボットは安全柵で囲むことで作業者に危害を与えないように構築することが一般的でした。いま、ロボットの作業内容を拡大するため、人・ロボットの協同作業が注目されています。この場合、ロボットは柵で囲まれないため、人が接近したときの安全対策が重要となります。 ●また、Industry4.0により工場の生産設備やロボットシステムが、工場の内外を問わずネットワークアクセスできるようになり、生産性や品質向上を追求しています。これは、セキュリティリスクが高まったことを意味します。 ●ロボットや機械が故障しても、人のヒューマンエラーであっても、セキュリティ脅威があっても、機械は事故や事件を起こしてはいけません。このため、制御システムの機能安全とサイバーセキュリティの技術が注目されています。 ●機械学会や工業会は、機能安全の啓発に注力してきましたが、セキュリティの技術調査・標準化にも乗り出しました。
関係者	●事業者(工場オーナ) ●ロボットシステムインテグレータ、ロボット/機器メーカ ●工程作業者、保守作業者



協働作業ロボットの例
(経産省METI Journal 2017.11.16)

3-6 産業ロボット

分析範囲	●分析者：事業者、インテグレータ ●分析方法:工場や事業所のセキュリティ対策は別途実施されているものとして、製造設備、生産ライン、ロボットシステムなどを分析単位とします。 安全対策(ISO 12100やISO 13849-1に基づく)を実施し、さらに安全対策で追加した(安全)制御機器についてセキュリティ対策（IEC 62443に基づく)を実施します。 安全対策とセキュリティ対策の矛盾・競合についても、分析及び解消します。
ガイドライン等	●IEC TR 63069(策定中) 産業プロセス計測・制御・自動化-機能安全とセキュリティのフレームワーク ●IEC TR 63074 (策定中) 安全制御システムの機能安全におけるセキュリティ面 - 安全制御系の機能安全とセキュリティを両立する製品開発に向けた、各種要求事項や技術要求を明確化します。IEC TR 63069がプロセスオートメーションを含む汎用産業分野を範囲とするのに対し、IEC TR 63074はFA機械設備を対象とします。 ●制御システム セーフティ・セキュリティ要件検討-ケーススタディ編(IPA/SEC) - 本書の続編。産業ロボットシステムを例題に、安全かつセキュアなロボットシステム構築の手順を示します。 ●つながる世界の開発指針(IPA/SEC) - IoT製品開発者が開発時に考慮すべきリスクや対策を明確化した指針

コラム：ネットワークセキュリティの世界動向

■サイバーセキュリティ政策は、影響力の大きい米国、欧州を中心にそれぞれの事情に即し独自に進んでいますが、脅威情報の共有等相互に協調する取り組みが行われています。

■セキュリティ技術の標準化は経路制御や電子メールなど通信インフラに関するもの、接続端末側での認証等、各団体(ITU-T＊1, 3GPP＊2, GSMA＊3等)ごとに策定が進められています。

【米国の政策】
・2014年にNISTがサイバーセキュリティフレームワークを公開し、2015年にはサイバーセキュリティ法が通過、またDHSからは「IoTセキュリティの戦略的原則」がリリースされました。
・2017年5月にNISTサイバーセキュリティフレームワークを連邦政府機関に義務付けるなど、米国サイバーセキュリティ強化に取り組んでいます。

【欧州の政策】
・2015年12月に、ネットワーク・情報セキュリティ指令(NIS Directive)が可決され、2016年7月から施行されました。エネルギー、輸送、医療、金融などの重要インフラを保有する大手企業に対し、十分なセキュリティ対策とインシデント報告が義務付けられました。

【標準化の動向（例）】
・DNSSEC（DNS Security Extensions）
特定ドメインの問い合わせ応答を偽造する攻撃に対し、DNSサーバの完全性を確認。

・電子メール DKIM（DomainKeys Identified Mail）
メールサーバにおいて、送信メールに秘密鍵で署名を付加。

・脅威情報共有のための仕様
侵入の兆候を知り対策に活用するための標準フォーマットSTIX（Structured Threat Information eXpression）、STIXで記述された情報を配送するプロトコルTAXII（Trusted Automated eXchange of Indicator Information）などがあります。

＊1）ITU-T（Telecommunication standardization sector）　＊2）3GPP（3rd Generation Partnership Project）
＊3）GSMA（Global System for Mobile communication Association）

コラム：安全(Safety)とセキュリティ(Security)の融合をめざして

1946年にENIACというコンピュータが生まれた。情報化社会の始まりである。そして、1971年に発表されたインテルの4004を始まりとするシリコン上で動作するコンピュータであるマイコンの登場は情報化と物を結びつけた。2000年代には組み込みシステムという言葉が生まれた。これは物にマイコンを搭載することである。今や、電話、眼鏡、時計、指輪など、あらゆるものにマイコンが埋め込まれている。身に着けるものだけでなく、家電、自動車、そして電力、ガス、交通、医療などの重要インフラも例外ではない。このような組込化に対応して機能安全という概念が生まれ、各種の分野で国際標準化が進んでいる。

しかし、時代は歯車を一つ進めつつある。IoT、CPS、AIという言葉が頻繁に聞こえてくる。そこには、組込システムのネットワーク化がベースにある。ネットワーク化ではサイバーセキュリティを意識せざるをえない。つまり、機能安全からの飛躍を意味する。End of Life、Software Update、 Security Operation Centerなど機能安全の世界では馴染みのない概念を入れていく必要がある。同様に、サイバーセキュリティの専門家は安全系の言葉に馴染みがない。両者の融合には、まだ時間がかかりそうである。
まずは、安全(Safety)とセキュリティ(Security)とを同じ土俵にあげることから始めたい。

電気通信大学
新　誠一

付録

A. 用語定義

出典：

一般財団法人　日本規格協会

IEC/TS 62443-1-1 Ed. 1.0:2009（英和対訳版）
産業用通信ネットワーク ― ネットワーク及びシステムセキュリティ ― 第1-1部：用語，概念及びモデル
Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models

IEC 62443-2-1 Ed. 1.0:2010（英和対訳版）
産業用通信ネットワーク ― ネットワーク及びシステムセキュリティ ― 第2-1部：産業用オートメーション及び制御システムセキュリティプログラムの確立
Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program

IEC 61508-4 Ed. 2.0:2010（英和対訳版）
電気・電子・プログラマブル電子安全関連系の機能安全－第4部：用語の定義及び略語
Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations

B. セーフティ・セキュリティ脅威分析手法
（一覧, ATA, STAMP/STPA）

C. 脅威分析シート

D. 参考情報：国際規格・業界標準・ガイドライン等

用語定義

用語	定義	出典
セーフティ safety	許容できないリスクから免れている状態 freedom from unacceptable risk	IEC 61508-4 Ed2
セキュリティ security	a) システムを保護するためにとられる対策 measures taken to protect a system b) システムを保護するための対策が確立され、維持管理されていることから生じる、システムの状態 condition of a system that results from the establishment and maintenance of measures to protect the system c) 認可されていないアクセスが行われず、無認可の又は偶発的な変更、破壊及び喪失が行われないというシステム資源の状態 condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss d) 認可されていない人及びシステムがソフトウェアおよびそのデータを変更することも、システム機能へのアクセスを取得することもできないという十分な信頼を提供し、なおかつ、認可されている人及びシステムがこの行為を拒否されないことを確実にする、コンピュータに基づくシステムの能力 capability of a computer-based system to provide adequate confidence that unauthorized persons and systems can neither modify the software and its data nor gain access to the system functions, and yet to ensure that this is not denied to authorized persons and systems e)産業用オートメーション及び制御システムの適切かつ意図された運用に対する違法の又は望まれない侵入又は干渉の防止 prevention of illegal or unwanted penetration of, or interference with the proper and intended operation of an industrial automation and control system	IEC 62443-1-1 Ed1

用語定義

用語	定義	出典
リスク risk	危害の発生頻度及び過酷度の組み合わせ combination of the probability occurrence of harm and the severity of the harm	IEC 61508-4 Ed2
	特定の脅威が特定の脆弱性を利用し、特定の結果が生じる確率として表現される損失の予想 expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence	IEC 62443-1-1 Ed1
フォールト fault	機能ユニットに要求される機能遂行能力の低下又は喪失を引き起こす可能性がある異常状態 abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function	IEC 61508-4 Ed2
故障（機能失敗） failure	ある機能ユニットの要求機能の遂行能力の終結、又は要求された以外の機能の誤運用 termination of the ability of a functional unit to provide a required function or operation of a functional unit in any way other than as required	IEC 61508-4 Ed2
潜在危険 hazard	危害の潜在的な源 potential source of harm	IEC 61508-4 Ed2
危険状態 hazardous situation	人、財産又は環境が、一つ又は複数の潜在危険にばく（曝）露されている状態 circumstance in which people, property or the environment are exposed to one or more hazards	IEC 61508-4 Ed2
危険事象 hazardous event	結果として危害が生じることがある事象 event that may result in harm	IEC 61508-4 Ed2

用語定義

用語	定義	出典
危害 harm	身体への傷害、人の健康逸失、所有物の毀損又は環境破壊 physical injury or damage to the health of people or damage to property or the environment	IEC 61508-4 Ed2
インシデント incident	システムによって提供されるサービスの品質の中断又は低下を招くか又は招く可能性のある、システム又はサービスの期待される運用の一部ではない事象 event that is not part of the expected operation of a system or service that causes or may cause, an interruption to, or a reduction in, the quality of the service provided by the system	IEC 62443-2-1 Ed1
脅威 threat	セキュリティを侵害して損害を引き起こす可能性がある事象、能力、アクション又は事象が存在する場合に生じる、セキュリティ違反の可能性 potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm	IEC 62443-1-1 Ed1
脆弱性 vulnerability	システムの完全性又はセキュリティポリシーを侵害するために利用される可能性がある、システムの設計、導入、又は運用とマネジメントにおける欠陥又は弱点 flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's integrity or security policy	IEC 62443-1-1 Ed1
セキュリティ機能 security function	ゾーン内又はコンジット内の装置及びシステムの正常な動作に直接作用するか間接的に影響を及ぼす可能性がある、認可されていない電子的な介入を防ぐゾーン又はコンジットの機能 function of a zone or conduit to prevent unauthorized electronic intervention that can impact or influence the normal functioning of devices and systems within the zone or conduit	IEC 62443-1-1 Ed1

用語定義

用語	定義	出典
安全機能 safety function	E/E/PE安全関連系又は他リスク軽減措置によって遂行される機能. この機能は，特定の危険事象に関して，EUC に関わる安全な状態を達成又は保持する function to be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event	IEC 61508-4 Ed2
安全関連系 safety-related system	次の両方を満足するシステム。 – EUC を安全な状態に移行させるため、又は EUC の安全な状態を維持するために必要な、要求された安全機能を行う。 – それ自体で，又はその他の E/E/PE 安全関連系及び他リスク軽減措置によって、要求される安全機能に対して必要な安全度を達成する designated system that both – implements the required safety functions necessary to achieve or maintain a safe state for the EUC; and – is intended to achieve, on its own or with other E/E/PE safety-related systems and other risk reduction measures, the necessary safety integrity for the required safety functions	IEC 61508-4 Ed2
被制御機器 （管理対象の機器） EUC(Equipment Under Control)	製造、プロセス、運輸、医療、その他の業務に供される機器、機械類、装置、プラントなど equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities	IEC 61508-4 Ed2 IEC 62443-1-1 Ed1
産業用オートメーション及び制御システム IACS(Industrial automation and control systems)	産業プロセスの安全で、セキュアで信頼できる運用に直接作用するか間接的に影響を及ぼす可能性がある要員、ハードウェア及びソフトウェアの集合 collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process	IEC 62443-1-1 Ed1

セーフティ・セキュリティ脅威分析手法

考え方	特徴	セーフティ	セキュリティ
ボトムアップ分析	システムの構成要素の故障モード、故障率が明確な場合に有効	FMEA （IEC 60812）	FMVEA
トップダウン分析	避けたい事象/達成すべき攻撃ゴールに対して、その達成方法をツリー状に分析 過去のハザード/攻撃情報がある場合に有効多重故障/攻撃の考慮も可能	FTA （IEC 61052）	ATA
逸脱分析	正常動作からの逸脱（中間事象）をガイドワードを使って列挙	HAZOP （IEC 61882） SHARD	STRIDE/Microsoft SDL SHARD SASTD
ゴール指向分析	達成すべきゴールに対して、その達成方法を分析	―	KAOS
ミスユースケース	ユースケース図を対象に関係者（アクター）の不正な振る舞いを分析	―	―
システム理論的プロセス分析	システムを制御システムと捉え、制御＆フィードバックの逸脱を分析	STAMP/STPA	STAMP/STPA-Sec

FMEA（Failure Mode and Effect Analysis）
FTA（Fault Tree Analysis）
HAZOP（HAZard and OPerability studies）
SHARD（Software Hazard Analysis and Resolution in Design）
STAMP/STPA（System Theoretic Accident Model and Processes/ System Theoretic Process. Analysis）

FMVEA（Failure Modes, Vulnerabilities and Effects Analysis）
ATA（Attack Tree Analysis）
STRIDE（Spoofing identity・Tampering・Repudiation・Information Disclosure・Denial of Service・Elevation of Privilege）
SASTD（Safety Analysis method based on State Transition Diagram）
KAOS（Knowledge Acquisition in autOmated Specification）

ATA（Attack Tree Analysis）:攻撃木分析

ATA

初期のATAは、Bruce Schneierの論文に見ることができる。
ATAは木構造を用いたトップダウン分析手法で、攻撃者および防御側それぞれの視点から以下のような分析作業に有用である。

- 攻撃者の視点：
  標的への攻撃を成功させる為に最も効率が良いルート（費用対効果が最大）を探す。
  - 発動条件が最も緩い「タイミング、人の関与」
  - 攻撃側のリソース（経済力、組織力、専門知識、etc）が少なくて済む
- 防御側（事業者、SI）からの視点：
  見つけたルートの防御力を強化する。
  対策する箇所（ノード）に対策と費用を書くと、攻撃ルート上の対策費用の合計が分かる。
- 表記（図）についてはいくつかのバリエーションが存在し、確立したものはない。
  また安全分析手法であるFTAと統合した記法も存在する。
- システム設計が進捗した段階で、想定した最悪の攻撃シナリオが回避されているかをATAで確認し、詳細なセキュリティリスクは別手法で行うなど、複数の手法を組み合わせると効果的である。

STAMP(Systems-Theoretic Accident Model and Processes)/ STPA(System-Theoretic Process Analysis)

STAMP/STPA*1

（システム理論に基づく事故モデル*2 /システム理論に基づく安全解析手法）

- **特徴**

FTA/FMEAは、コンポーネントの機能不全（故障等）を洗い出し・対策するという従来の信頼性工学によるハザード分析の手法である
STAMP/STPAは、対象システムの機能を「抽象化・階層化」したトップダウンの安全解析手法であり、コンポーネント間の相互作用によるハザード要因をどのように抑制・制御するか考察する

- **利点**

システム機能を「抽象化」することで、ドメインの専門家でない技術者でも解析が可能

- **活用対象**

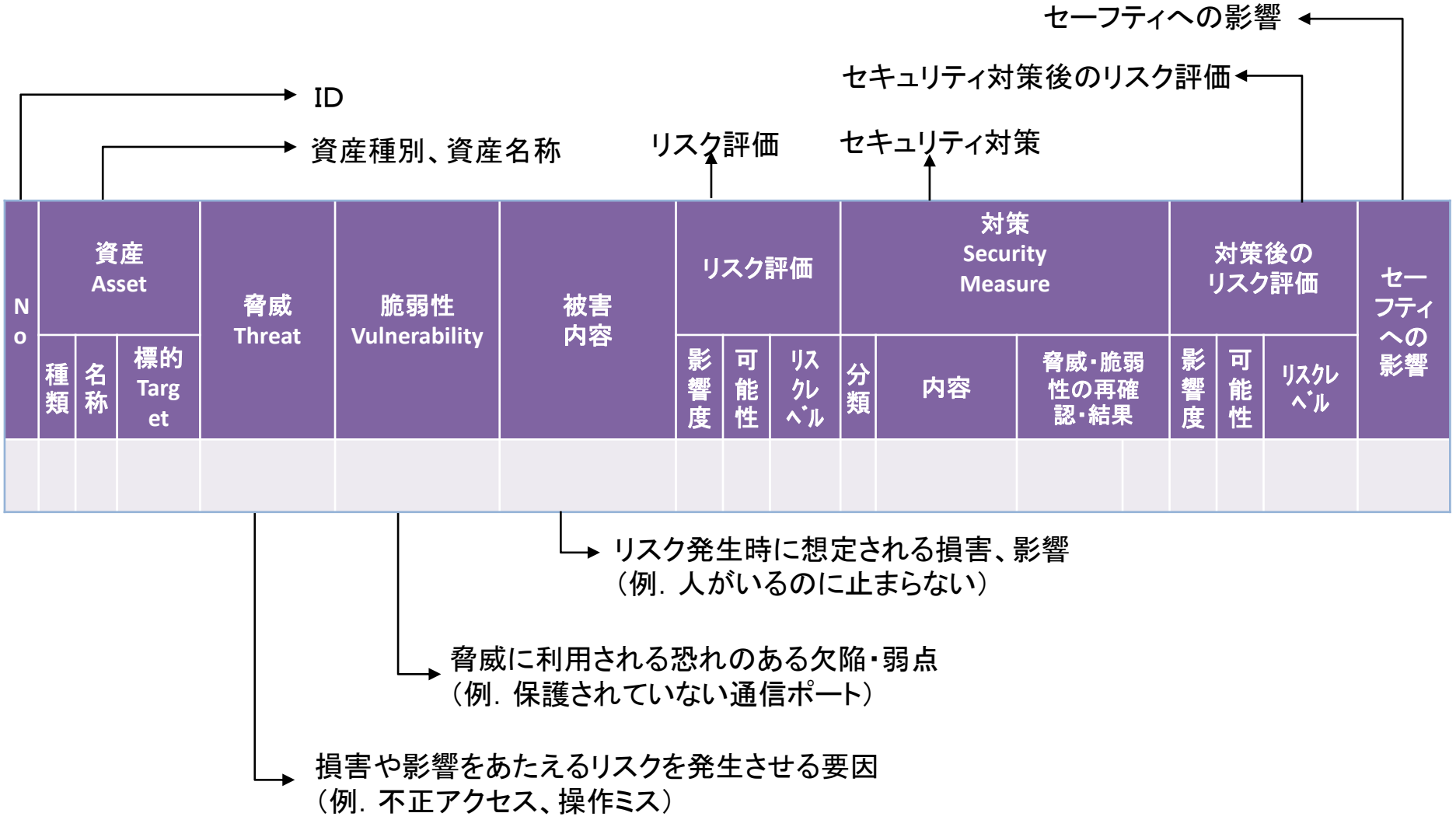
人間と機械の協調による安全制御（例：自動運転）、インターネット接続や大規模なソフトウェアが搭載された複雑なシステムの安全制御など、近年の高度なシステムに利用することが期待できる　また、ハザード分析だけではなく、事故モデルとして、過去の事故や不具合評価に活用でき、拡張システムの検証にも利用可能

・STPA 実施手順の例

＊1）マサチューセッツ工科大学（MIT）のNancy Leveson教授が提唱
＊2）システムの安全制御要素（コントローラ）と、制御される要素（被コントローラ）の相互作用が働かないことによっておきるアクシデントモデル

脅威分析シート

■本書の脅威分析に用いる分析シートを示します。



脅威分析シート

■脅威発生時のシステムに及ぼす影響度、発生可能性はIEC 62443に基づいています。

No	資産 Asset			脅威 Threat	脆弱性 Vulnerability	被害内容	リスク評価			対策 Security Measure			対策後のリスク評価			セーフティへの影響
	種類	名称	標的 Target				影響度	可能性	リスクレベル	分類	内容	脅威・脆弱性の再確認・結果	影響度	可能性	リスクレベル	

脅威発生時の影響度を評価する

影響度	説明	
	工場内	工場外
高	死亡	死亡or重大な地域ｲﾝｼﾃﾞﾝﾄ
中	休職or重傷	苦情or地域社会へ影響
低	応急手当	苦情なし

リスクレベル	発生可能性		
	高	中	低
影響度 高	高	高	中
影響度 中	高	中	低
影響度 低	中	低	低

脅威発生可能性を評価する

発生可能性	説明
高	今後1年以内に発生する可能性が高い脅威、脆弱性
中	今後10年以内に発生する可能性が高い脅威、脆弱性
低	これまで発生したことがなく今後も発生する可能性がほとんどないと考えられる脅威、脆弱性

参考情報：国際規格、業界標準、ガイドライン等

	ドメイン	安全規格	セキュリティ規格	参考資料 （ガイドライン等）
0	--	IEC 61508	IEC 62443 ISO/IEC 27001(ISMS) ISO/IEC 15408(CC)	経済産業省　セキュリティ関連コンテンツ一覧 http://www.meti.go.jp/policy/netsecurity/secdoc/secdoc_list.html 国土交通省　重要インフラにおける情報セキュリティ確保に係るガイドライン http://www.mlit.go.jp/sogoseisaku/jouhouka/sosei_jouhouka9999.html IPA　制御システムのセキュリティリスク分析ガイド https://www.ipa.go.jp/security/controlsystem/riskanalysis.html つながる世界の開発指針（第2版） https://www.ipa.go.jp/sec/reports/20170630.html
1	自動車	ISO 26262	SAE J3061 ISO/SAE　21434＊ 策定中	CCDS製品分野別セキュリティガイドライン 車載器編 https://www.ccds.or.jp/public_document/index.html
2	電力	電気事業法		電力制御システムセキュリティガイドライン https://www.denki.or.jp/wp-content/uploads/2016/07/d20160707.pdf 監視制御用計算機システムにおけるセキュリティ対策のガイドライン（追補1） https://www.jema-net.or.jp/cgi-bin/user/summary.cgi?jem=1158
3	施設監視制御	ISO 16484 (BACS)		IoTセキュリティ総合対策 – 総務省　サイバーセキュリティタスクフォース http://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/index.html http://www.soumu.go.jp/main_content/000510701.pdf
4	鉄道	IEC 62278（RAMS）	IEC 62280	鉄道分野における情報セキュリティ確保に係る安全ガイドライン 第3版 http://www.mlit.go.jp/sogoseisaku/jouhouka/sosei_jouhouka9999.html
5	医療・ ヘルスケア	IEC 60601 IEC 62304 IEC 82304 ISO 14971	IEC 62304　AnnexC IEC 80001 IEC 27002 ISO/IEC 27799	医療機器における情報セキュリティに関する調査 https://www.ipa.go.jp/security/fy25/reports/medi_sec/ 医療情報システムの安全管理に関するガイドライン第5版 http://www.mhlw.go.jp/stf/shingi2/0000166275.html ヘルスソフトウェア開発ガイドライン https://www.good-hs.jp/guidelines.html
6	産業機械	IEC 62061 ISO 12100 ISO 13849-1	IEC 62443 IEC TR 63069＊ 策定中 IEC TR 63074＊ 策定中	制御システムセキュリティ運用ガイドライン http://www.neca.or.jp/wpcontent/uploads/control_system_security_guideline.pdf

編著者：制御システムセーフティ・セキュリティ検討WG

本書は、独立行政法人情報処理推進機構 技術本部　ソフトウェア高信頼化センター（SEC）
「制御システムセーフティ・セキュリティ検討WG」において作成しました。

編著者（敬称略）

主査	宇野　新太郎	学校法人電波学園愛知工科大学
委員	麻薙　年男	東芝情報システム株式会社
	飯島　三朗	株式会社日立産業制御ソリューションズ
	石井　泉	日本信号株式会社
	小田原　育也	東芝デジタルソリューションズ株式会社
	梶本　一夫	パナソニック株式会社
	神余　浩夫	三菱電機株式会社
	菊地　丞	日本信号株式会社
	辻　宏隆	横河電機株式会社
	花田　滋	株式会社日立産業制御ソリューションズ
	松原　豊	国立大学法人名古屋大学
	森　崇	西日本旅客鉄道株式会社
編集者	石田　茂	独立行政法人情報処理推進機構
	細目　紀子	独立行政法人情報処理推進機構
	中谷　博司	独立行政法人情報処理推進機構

制御システム セーフティ・セキュリティ要件検討ガイド
－ 基本編 －

2018年3月　第1版発行

独立行政法人情報処理推進機構(IPA) 技術本部 ソフトウェア高信頼化センター（SEC）
〒113-6591
東京都文京区本駒込2丁目28番8号　文京グリーンコートセンターオフィス16階
https://www.ipa.go.jp/sec/index.html