SEC BOOKS

IPA Better Life with IT

つながる世界のセーフティ&セキュリティ設計入門

IoT 時代のシステム開発『見える化』

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

はじめに

i)　概要

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(IPA/SEC: Information-technology Promotion Agency, Software Reliability Enhancement Center)の下に組織したワーキンググループ（WG: Working Group）で作成したものです。本書は、機器やシステムの安全・安心を実現するためのセーフティとセキュリティの設計手法、及びソフトウェアの再利用や流通において第三者に論理的に説明できる設計品質の見える化手法などについて分かりやすく解説した入門書です。解説範囲には、設計の前段階で必要となる機器やシステムのリスク評価も含めています。

本書では、具体的な機器やシステムをイメージしやすいように、自動車、スマートフォン、ヘルスケア機器、スマート家電などの生活に欠かせない機器（以下「生活機器」）を例として取り上げています。これらの生活機器を開発する上では、セーフティ設計（設計の段階で安全を作りこむこと）はもちろん、近年、ネットワークにつながるようになっていることからパソコン等の情報機器同様にセキュリティ設計(設計の段階で脆弱性の低減や脅威への対策を考慮に入れること)も必要となります。そこで本書では、上記生活機器を「安全・安心を実現すべき製品例」として選びました。

現状、セーフティとセキュリティの設計は独立したプロセスで実現することが多いと想定されますが、上記の理由から、今後の開発現場においては、ともに関係性を持って推進されることが必要となります。

「見える化」による設計品質評価

ii)　対象となる読者

本書の想定読者と、各読者向けのコンテンツを下表に示します。セーフティとセキュリティの設計はハザードや脅威からユーザーの身体や財産を守る重要なプロセスであることから、本書は経営層から運用・サポート担当まで、製品・システムに関係する全ての方々にお読みいただきたいものとなっています。

本書の想定読者

本書の構成 / 想定読者	1章&3章 セーフティとセキュリティ	2章 事故事例	設計・開発・見える化の手法		
			4章 セーフティ設計	5章 セキュリティ設計	6章 見える化
経営・企画	○	○			
設計・開発	○	○	○	○	○
評価・検証	○	○	○	○	○
運用・サポート	○	○			○

iii)　本書の考え方

IPA/SEC では平成 18 年、身の回りのシステムの安全性向上のための入門書を「組込みシステムの安全性向上の勧め(機能安全編)」として公表しています［1]。しかし、近年、生活機器には盗聴やソフトウェア改ざんなどを防ぐための「セキュリティ設計」も重要となっています。また、生活機器のセキュリティ上の課題は「安全」にも影響を及ぼす可能性があります。そこで本書では、「安全設計」と「セキュリティ設計」の解説を併記するとともに、両者を含めた設計品質の見える化について解説することとしました。

iv)　表記について

表記上のバランスをとるため、「安全」を「セーフティ」と表記しています。ただし、別の単語と組み合わせた用語については、「機能安全」、「安全策」などのようにそのまま使用しています。

また、カタカナの表記については他の規格や資料からの引用はそのまま記載しますが、できるだけ読みに近い「外来語の表記」［2］［3］に沿うよう配慮しました。また、対話に役立つよう、読みがある略語はカタカナで読みを記載しました。

v)　略語一覧

本書で使用している略語と名称を下表に示します。

略語	名称
ASIL	Automotive Safety Integrity Level
CAPEC	Common Attack Pattern Enumeration and Classification
CC	Common Criteria for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
CSIRT	Computer Security Incident Response Team
CVSS	Common Vulnerability Scoring System
EAL	Evaluation Assurance Level
ECC	Error Check and Correction
EDSA	Embedded Device Security Assurance
EVITA	E-safety vehicle intrusion protected applications
FMEA	Failure Mode and Effect Analysis
FTA	Fault Tree Analysis
HAZOP	Hazard and Operability
ISIRT	Information Security Incident Response Team
IEC	International Electrotechnical Commission
IPA	Information-technology Promotion Agency, Japan
IPA/SEC	Information-technology Promotion Agency, Japan Software Reliability Enhancement Center
JIS	Japanese Industrial Standards
IoT	Internet of Things
ISO	International Organization for Standardization
MBD	Model Based Development
MBSE	Model Based Systems Engineering
MoD	Ministry of Defence
OMG	Object Management Group
PKI	Public Key Infrastructure
PL	Performance Level
PP	Protection Profile
SIL	Safety Integrity Level
SQuaRE	Systems and software Quality Requirements and Evaluation
ST	Security Target
STAMP	Systems-Theoretic Accident Model and Processes
STPA	System-Theoretic Process Analysis

目次

第1章
つながるシステムのセーフティとセキュリティ

現代のシステムは、ネットワークを介して様々な機器やクラウドと連携しながら動作しています。こうした「つながるシステム」においては、セキュリティ上の脅威がネットワークを介して波及し、さらにソフトウェアで制御されるセーフティ機能にも影響を与える可能性があります。そこで、的確なリスク対応、セーフティとセキュリティの設計、及び見える化による設計情報の共有が重要となります。

1.1 つながる世界のシステムとリスク

(1) つながる世界のイメージ

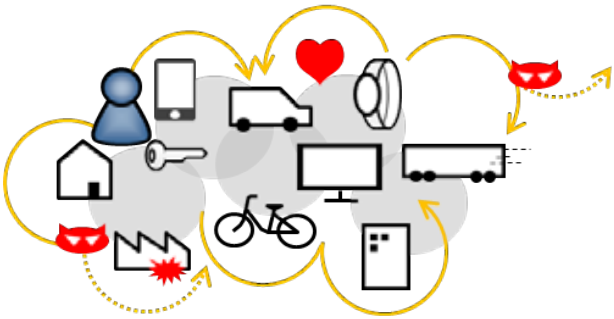


図 1-1 つながる世界のイメージ

従来は個別に動作していた生活機器が、情報通信技術の発展に伴い相互にネットワークでつながるようになり、連携してユーザーにサービスを提供したり、自動的にデータ収集・分析を行って他の生活機器に送信するようになりました。今後も、異なる分野の機器やシステムの連携が拡大すると予想されます。

(2) つながる世界のシステム

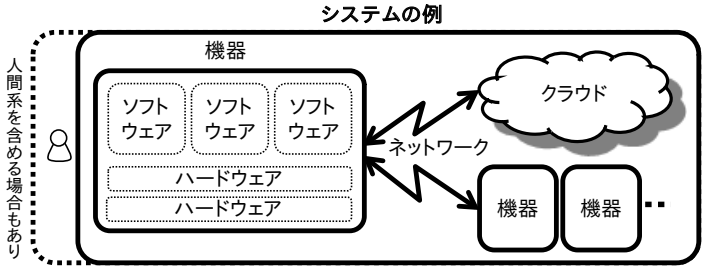


図 1-2 つながる世界のシステムのイメージ

本書では、機器をクラウドや他の機器とネットワークでつなげ、「体系的」に動作するようにしたものを「システム」と呼んでいます。機器の故障や誤動作はネットワークを介して他の機器に影響を与えます。また、クラウドなどの外部接続により、ウイルスなどの攻撃が発生する危険性もあります。つながる世界では、個々の機器だけでなく、システム全体として安全・安心を考える必要があります。

1.2 セーフティとセキュリティによるリスク対応

(1) リスクから見たセーフティとセキュリティ

ビジネスにおいては、競合や災害など様々な事業リスクがあります。しかし、つながる世界の機器やシステムにおいては、事故や攻撃などセーフティとセキュリティ上のリスク対応も必要となります。そこで本書では、これらのリスクに焦点を当て、その分析や低減の必要性について説明しています。

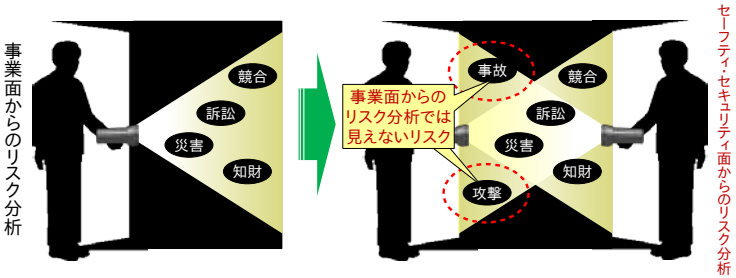


図 1-3 本書が対象とするリスクのイメージ

まず、セーフティとセキュリティ上のリスクについて説明します。事業上取り扱う機器やシステムには、ソフトウェアの欠陥や脆弱性のように誤動作や第三者からの攻撃によりユーザーの身体や財産に危害をもたらす要因が潜在する可能性があります（セーフティに関する要因を「ハザード」、セキュリティに関する要因を「脅威」と呼びます）。実際に危害が発生すれば、損害賠償や機器の回収、消費生活用製品安全法の製品事故情報報告・公表制度［4］への対応などによりビジネスへの影響は多大となります。

セーフティとセキュリティ上のリスクについては、ハザードや脅威の発生しやすさ及び被害の深刻度から評価する方法があります。被害が深刻でも発生する確率がゼロに近ければリスクは小さくなりますし、軽微な被害でもネットワークを介して波及する場合にはリスクは大きくなります。安全性を高める機能（以下「セーフティ機能」）はソフトウェアで制御されるものが多いため、セキュリティ上の脅威がネットワークを通じて他の機器のソフトウェアに影響を与え、広範囲でセーフティ機能が誤動作を起こせば、リスクは測り知れません。

つながる世界においては、ハザードや脅威の被害が広範囲に広がり、企業のビジネスにとって重大なリスクとなりうるため、積極的な対応が必要です。

(2) 守るべき対象から見たセーフティとセキュリティ

セーフティの対象となる「被害」としては、例えば自動車の衝突による怪我、機器の発火による家屋の焼失などが挙げられます。これに対してセキュリティの対象となる「被害」は、例えば機器やシステムの不正利用や停止、ソフトウェアやデータの改ざん、個人情報漏えい、電子決済時の金銭の詐取などが挙げられます。このように対象となる「被害」は多岐にわたるため、セーフティとセキュリティの設計においては、まず守るべき対象を洗い出すことが必要となります。

なおセキュリティ上の脅威がセーフティ機能に影響を与える可能性があるため、図 1-4 のようにセキュリティ設計により守るべき対象がセーフティの範囲まで広がりつつあります。

守るべきものの例	保護対象の例	セーフティ	セキュリティ
人	命		
	身体		
	心		
物	システム		
	機械		
金	金銭		
情報	データ、ソフトウェア		
	品質		

図 1-4 広がるセーフティとセキュリティの守るべき対象範囲

守るべき対象を決定した後、これらに対するリスクを評価し、必要なセーフティとセキュリティの設計でリスクを許容できるレベルまで低減することで、安全・安心なサービスの提供が可能となります。

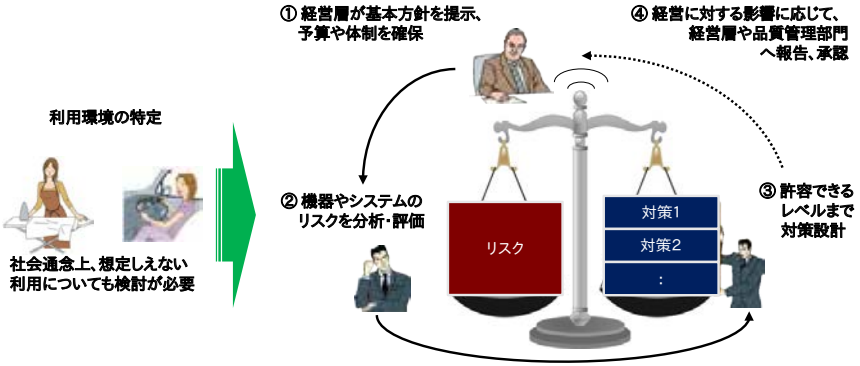


図 1-5 基本方針に基づいたセーフティとセキュリティの対策

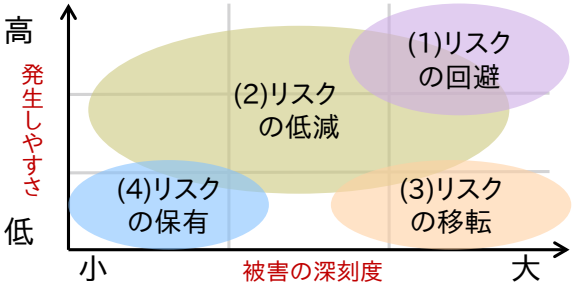
業務システムなどにおける情報セキュリティでは、リスク対応を図 1-6 の 4 つの対応方法で整理しています。機器やシステムにおけるセキュリティ設計においては、セーフティ機能への影響も勘案して対応方法を検討する必要があります。

(1) リスクの回避　リスクのある機能を削除したり全く別の方法に変更したりすることにより、リスクが発生する可能性を取り去る。

(2) リスクの低減　リスクに対して対策を講じることにより、発生しやすさや被害の深刻度を低減する。

(3) リスクの移転　保険加入や、リスクのある部分を他社製品・システムに置き換えることにより、リスクを他社などに移す。

(4) リスクの保有　リスクが小さい場合、特にリスクを低減するための対策を行わず、許容範囲内として受容する。



出典：「情報セキュリティマネジメントと PDCA サイクル」［5］の図を基に作成

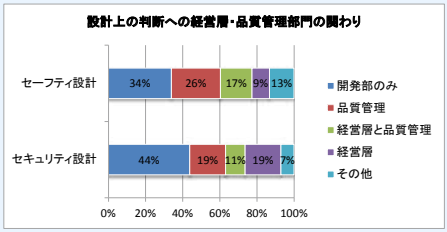
図 1-6　発生しやすさと被害の深刻度から見たリスク対応方法の目安

コラム1 セーフティとセキュリティの設計に関わる重要事項は誰が判断する?

～「セーフティ・セキュリティ設計の見える化推進のためのアンケート」より～

2015 年実施

セーフティとセキュリティに先行して取り組んでいると想定される自動車、スマートフォン、ヘルスケア、スマート家電の 4 分野に対して、セーフティ設計・セキュリティ設計の実施状況の把握のため、アンケートを実施しました。この結果、回答者の大半がセーフティ設計・セキュリティ設計が必要であると回答し、その必要性を認めていることが分かりました(セーフティ設計とセキュリティ設計の両方が必要: 76%、セキュリティ設計のみ必要 : 19%、セーフティ設計のみ必要 : 4%)。しかし、セーフティ設計・セキュリティ設計の必要性は認識されているものの、実際に判断基準の拠り所となるセーフティ設計・セキュリティ設計に関する基本方針はないとの回答がそれぞれ半数を超えています(セーフティ:65%、セキュリティ : 54%)。また「セーフティ設計・セキュリティ設計上の判断に、経営層や品質管理部門責任者が関わるか」と言う設問に対して、セーフティにおいては 34%、セキュリティに関しては 44%が、責任者は判断に関わらず、現場 (開発部門) で判断しているとの回答もあります。



これらから見えてくることは、まだまだ多くの組織において、セーフティ・セキュリティの重要事項 (要件・仕様を含む) を現場で判断するための基本方針がなく、かつ重大な事件・事故につながる可能性のある設計の判断に経営的な関与がなく、現場でなされているのではないかと言うことです。

また経営層や品質管理部門責任者等のステークホルダーとの情報共有としても強力なツールになるアシュアランスケース等を使った見える化の調査も行いましたが、まだ共通的なツール(GSN,CAE 及び D-Case 等, P.74 参照)の導入に関しては未発展段階であることが分かりました (導入実績 : セーフティ : 15%、セキュリティ : 3%)。判断を仰ごうとしても説明ができない、という状況になっていないでしょうか。

アンケート公開 URL : http://www.ipa.go.jp/sec/reports/20150910.html

1.3 セーフティとセキュリティの設計の見える化の必要性

本書でいう「セーフティとセキュリティ設計の見える化」とは、複雑になりがちな安全対策やセキュリティ対応などを、第三者にエビデンスを使って論理的に説明できるようにすることを指します。見える化の目的としては、設計開発支援、第三者認証や国際規格の取得などが挙げられます。

(1) 設計開発支援

設計開発の各段階において、設計内容を共有するために「見える化」を利用します。具体的な効果を図 1-7 に示します。

効果例	概要
1 ソフトウェア設計や再利用時の設計内容の理解	新製品開発やバージョンアップ時のソフトウェア再利用時に、設計内容を理解するために活用
2 ステークホルダーとの設計情報共有	社内の関係者や連携サービス提供者との設計情報共有に活用。セーフティ設計とセキュリティ設計のすり合わせにも活用
3 トレーサビリティ、説明責任	問題が発生したときに設計内容を確認したり、問題と設計との関係を説明したりするために活用

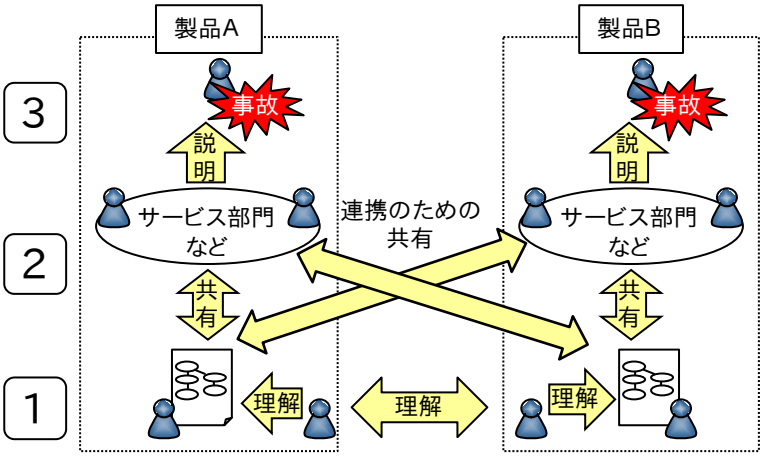


図 1-7 セーフティとセキュリティ設計の見える化の期待効果

(2) 第三者認証、国際規格の取得

セーフティとセキュリティの設計が業界規格や国際規格に準拠していることを説明するために活用することができます。規格によっては、見える化の一手法である「アシュアランスケース」を要求するものもあります（6.2，P.73 参照）。

1.4 つながる世界の品質保証

異なる分野の機器やシステム同士がつながる場合、ある機器で発生した事故や攻撃の影響がネットワークを通じて他の機器に伝搬する可能性があります。そこでつながるシステムにおいては、相手の機器やシステムのセーフティとセキュリティのレベルを基に、情報提供の可否、受領した情報や制御信号の信頼性、サービス範囲などを決定する必要があります。

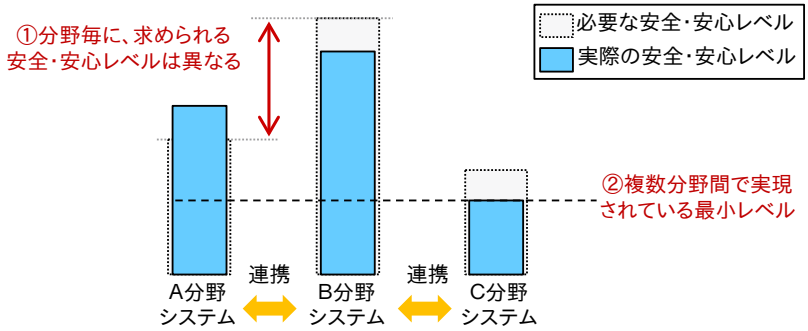


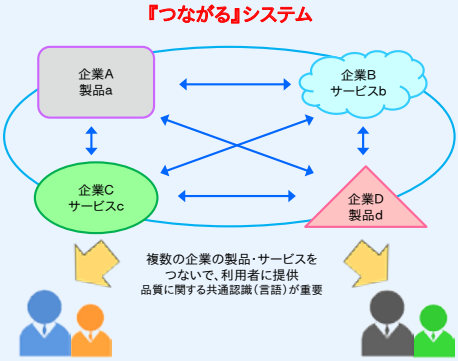
図 1-8 つながる世界の品質の考え方

また、自動車、スマートフォン、ヘルスケア機器、スマート家電など異なる分野ではそれぞれの歴史や背景があるため、セーフティとセキュリティに対する考え方にも違いがあります。

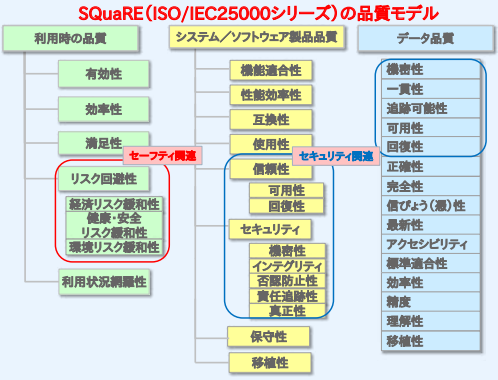
そこで前述のように、各機器やシステムのセーフティとセキュリティの設計品質を見える化し、異なる分野のステークホルダー間で共有することで、相手の分野の考え方の理解、機器やシステムの設計品質の評価、セーフティとセキュリティのレベルに合わせたサービス範囲の決定などを行うことが可能となります。このように設計品質の見える化は、つながる世界の安全・安心の実現には欠かせないものです。

コラム2 つながる世界の品質モデル ～共通言語としての「SQuaRE」～

IT を活用した製品の社会における役割が増えるにつれて、利用者の期待は機能だけに限らず、セーフティとセキュリティ、快適さ、楽しさ、ビジネスへの貢献など多様化し、かつ高い満足度が求められるようになっています。また、スマートフォンを利用したクラウドサービスは、これまで接点がなかった多様な事業者同士が「つながる」システムになっています。しかし、製品・サービスに関与する様々なタイプの利用者、事業者等のステークホルダーが考える品質は、定義や考え方が異なる可能性があるため、異なるステークホルダー間で共通の認識を持つ事が難しい現状があります。



このときに有効なのが国際規格「SQuaRE（スクウェア）：ISO/IEC 25000 シリーズ」で規定された品質モデルです。SQuaRE はこれまで接点がなかったステークホルダー間の共通言語の役割を果たし、多様なニーズを共通の枠組みの中で整理できます。本ガイドブックの対象であるセーフティ・セキュリティも SQuaRE の品質モデルの一部に含まれています。



IPA では、製品・サービスの提供者向けに SQuaRE の基本的な知識と活用を解説したガイドブックを書籍として発行しました。ぜひ「つながる」システムの開発に SQuaRE を有効活用してください。

■ガイドブック

書籍：つながる世界のソフトウェア品質ガイド（平成 27 年発行）

http://www.ipa.go.jp/sec/publish/20150529.html

第2章
事故及びインシデント事例

現代のソフトウェアはあらゆる場面で絶え間なく日常生活と社会を支える、重要な役割を担っています。ソフトウェアを原因としたセーフティ上の事故と、セキュリティ上のインシデントは極力避けるように開発されていますが、技術革新や社会の変化にも対応するよう、検討しなおす必要があります。ここではその参考として事故及びインシデントの事例を紹介します。

2.1 事故及びインシデント発生のメカニズム

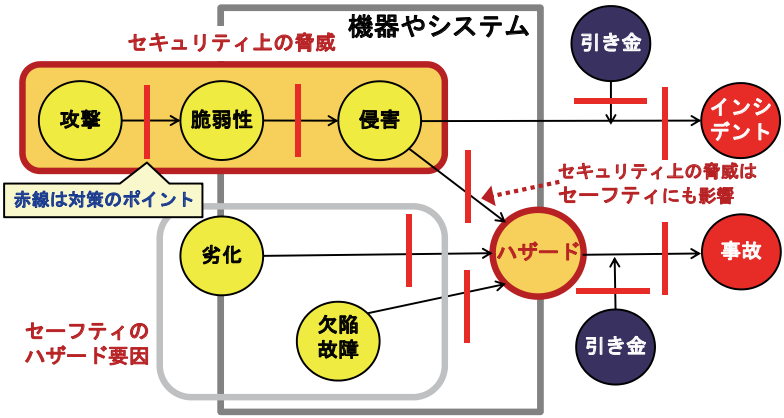
2.2 事故事例

2.3 インシデント事例

2.4 その他の事故事例、インシデント事例一覧

2.1 事故及びインシデント発生のメカニズム

事故やインシデント（セキュリティ上の望ましくない事象）を防ぐためには、発生メカニズムの理解が重要です。図 2-1 は事故とインシデントが発生するプロセスの例です。黄色で示した複数の原因から、オレンジ色のハザード・脅威を経由して赤い事故・インシデントにつながります。途中の赤線は対策可能な部分になります。［6］［7］



出典：英国RSSB「The Yellow Book」及びSESAMOプロジェクト「SECURITY AND SAFETY MODELLING FOR EMBEDDED SYSTEMS」を基に作成

図 2-1　セーフティとセキュリティの被害の発生プロセス

本章では、事故及びインシデントの事例を紹介するとともに、上図のどの時点で止めることが可能であったかを考察します。なお、セーフティとセキュリティに関する国際規格では用語の定義がありますが、聞きなれない言葉も多いため、本書では表 2-1 のように用語を使用しています。

表 2-1　本書におけるセーフティとセキュリティの用語の使い方

概念	本書での用語	
	セーフティ	セキュリティ
1）望ましくない事象	事故	インシデント
2）1 の事象を引き起こす直接的な危険源	ハザード	脅威
3）2 の原因の基となる、機器やシステムの弱点、問題点、危険源	故障、欠陥、劣化	脆弱性、侵害

2.2 事故事例

事例1: 後続列車がホームに進入できなくなる ～動作パターンの洗い出し不足で欠陥を見逃し～

事象

ある鉄道会社で、同一ホームを利用する列車の制御に誤りがあり、後続列車がホームに進入できないトラブルがありました。具体的には、先行する列車が折り返し出発したにも関わらず、先行する列車向けの制御信号が出続けたため、後続の列車への制御信号が出されず、ホームに入ることができませんでした。

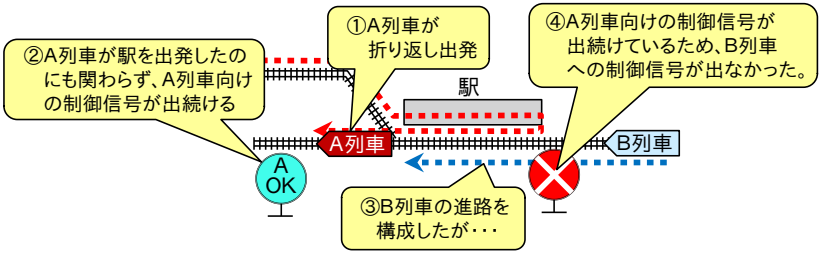


図 2-2 駅での障害発生状況［8］

原因

システムの本稼働前に実列車を用いたテストを行っていましたが、テストシナリオの洗い出しに漏れがあり、上記のケースはテストしていなかったとのことです。また、システムの動作を総合的にテストできる検証環境もなかったとのことです。

対策のヒント

4章で紹介しますが、安全を実現するためには、想定されるあらゆるケースについてハザードの特定及びリスク評価を行う必要があります。今回は人命や設備の危害にはつながりませんでしたが、動作されるケースについてもれなく検証できるよう、パターンの洗い出し及びシミュレーションによる検証環境の整備が必要です。

⇒ハザードの洗い出しについては 4.2.1, P.36 参照

事例2: ブレーキの制動距離が長くなる ～セーフティ機能が誤動作～

事象

2014 年 8 月、ある自動車会社から、以下のリコール情報が出されました。

> ブレーキ倍力装置に負圧を供給するブレーキ負圧電動ポンプを制御する EV ECU の制御プログラムが不適切なため、リレー接点が固着したと誤判定する場合がある。そのため、ブレーキ警告灯が点灯するとともに警告音が鳴り、ブレーキ負圧電動ポンプが停止し、そのままの状態で使用すると制動距離が長くなるおそれがある。

出典：国土交通省「リコール・改善対策の届出」より抜粋

ブレーキ倍力装置は、ブレーキペダルを介して伝えられる運転手の制動力を、負圧によって補助する事でブレーキに制動力を数倍の力で伝えるものです。負圧提供するポンプが停止してもブレーキ自体は動作しますが、より大きな力を必要とするため、制動距離が長くなります。

図 2-3　制御ソフトウェアの誤判定による危険

原因

ECU の制御プログラムの不具合により、故障が発生したとの誤判定がおき、より重大な事故を防ぐためにブレーキ負圧電動ポンプの停止が発生したものと推定されます。

対策のヒント

セーフティ機能は、故障や誤動作が発生した場合でも事故などのリスクを低減するために追加するものであり、セーフティ機能自体が誤動作することのないよう、設計品質の向上が望まれます。

⇒設計品質の向上については、4.2.3, P.45 参照

事例3: ガスメーターの安全機能が動作しなくなる ～セーフティ機能の動作基盤が停止～

事象

2003 年、日本ガス協会と経済産業省から、マイコンガスメーターの一部の機種でコントローラーのソフトウェアに不具合があり、ガス流量監視・遮断機能や感震遮断機能などの安全機能および通信機能が動作しなくなる恐れがあるため、対象機種約 2 万 7 千個を交換するとの発表がありました。なお、ガスの使用量の計測自体には問題はないとのことでした。

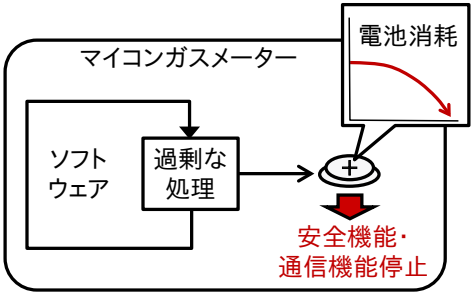


図 2-4　ガスメーターの安全機能が動作しなくなる

原因

ガスメーターの検定の有効期間は 7～10 年であり、マイコンガスメーターの内蔵電池も一般に期間内は持つように設計されますが、ソフトウェアの欠陥により内蔵電池が急激に消耗し、約 1 年半で電池電圧の低下を招き、各種機能が正常に動作しなくなってしまったそうです。

対策のヒント

セーフティ機能自体は品質の高い設計になっていても、機器やシステムの根幹的な機能（この場合は内蔵電池）が使用できなくなることで安全性が確保できなくなる事例として参考になります。近年のガスメーターでは、内蔵電池が消耗するとガスの供給を停止することで安全性を確保する機能が見られますが、セーフティ設計のリスク分析で（電池切れ）ハザードを特定して対処すべきであったと考えられます。

⇒ハザードの想定については、4.2.1(3), P.38 参照

事例4: 心臓ペースメーカーが動作しなくなる ～停止してはいけない製品が故障で停止～

事象

2007 年 2 月、ある医療機販売会社から、一定の条件において心臓ペースメーカーが誤動作を起こすため、システムソフトウェア修正を行うとの発表がありました。心臓ペースメーカーは、心臓の鼓動が途切れたり、一定以上の間隔を超えてしまったりした時、それを感知（センシング）して電気刺激を心臓に送り（ペーシング）、心臓が正常なリズムで鼓動することを助けるサポータです。今回の事象では一定条件下で、本来は電気刺激を送り、正常鼓動にしなくてはならないところを、その電気刺激の抑制（不具合）が発生し、心臓が正常なリズムで鼓動できなくなり、息切れ、疲労感、めまい、失神など埋込み前の症状等が見られる可能性があるとのことです。

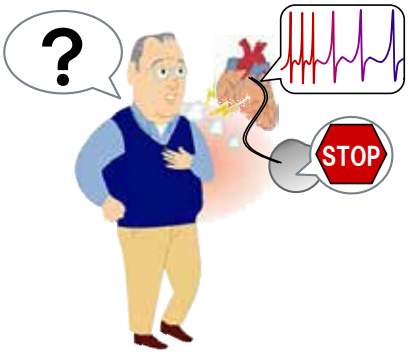


図 2-5　心臓ペースメーカーが動作しなくなる

原因

システムソフトウェアの欠陥が原因で、ある自動処理が実施されることをきっかけとしてペーシングの抑制が発生していました。

対策のヒント

人命に関わる機器やシステムにもソフトウェアの欠陥はありえます。セーフティ対応が必要な機器やシステムの中には、自動車のような故障時は安全に止まることで人命を守れるものだけでなく、健康や生命に関わるために故障時にも止まることが許されないものも存在します。その場合は通常のセーフティよりも強化された二重、三重の対策が求められることもあります。

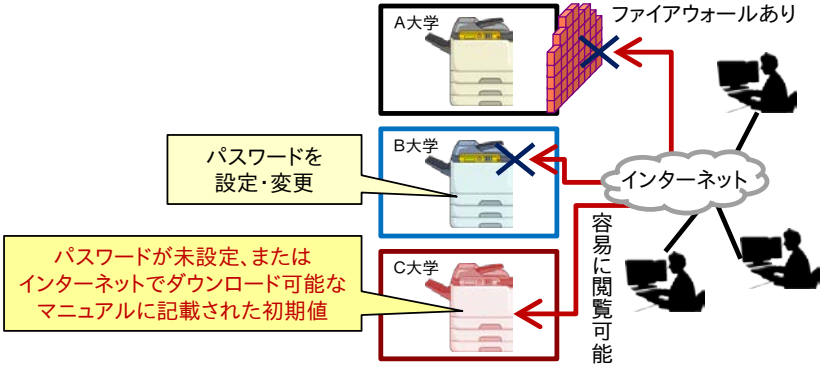
⇒セーフティ対応については 4 章, P.34 参照

2.3 インシデント事例

事例1: 複合機内のデータが外部からアクセスできる状態に ～重要なセキュリティ対応がユーザー任せに～

事象

2013 年、大学などに設置されたコピー・プリンタ複合機が外部からインターネット経由でアクセスできる状態となっていることが新聞で報道されました。複合機用にファイアウォールを設置したり、パスワードを設定・変更したりしている場合は問題ありませんでしたが、一部の大学では複合機に蓄積された住民票、免許証、健康診断の問診票などのデータが公開状態にありました。



出典: 読売新聞サイト記事の図を基に作成

図 2-6 複合機内のデータが外部からアクセスできる状態に

原因

メーカーが出荷時に管理者用のパスワードを設定していなかったり、初期設定パスワード（「123456」など）を記載したマニュアルをインターネット上で公開していたりしたことが問題として挙げられます。また、大学において複合機がファイアウォールなしでインターネット接続されることを想定しておらず、設置時のアドバイスも行っていなかったことも問題でした。

対策のヒント

セキュリティ知識を持たないユーザーやセキュリティ対応が不充分な利用環境を想定し、確実なパスワードの設定・変更、未設定時のアクセス制限、ユーザー説明などを行う必要があったと考えられます。

⇒セキュリティ設計の手法については、5.2.3, P.59 参照

事例2: 無線で心臓ペースメーカーを停止可能に ～セーフティだけでなく、セキュリティにも配慮が必要～

事象

2012 年、米国で研究者が心臓ペースメーカーへの伝送装置を利用して 10m 弱の距離から致死に至る電流を流したり、ペースメーカー内のソフトウェアを書き換えたりする実験を公表しました。同様の研究実証は2008 年にも行われており、当時、米会計検査院（GAO）が米国食品医薬品局（FDA)に検討を促し、FDA が医療機器メーカーに警告を発した経緯もあります。

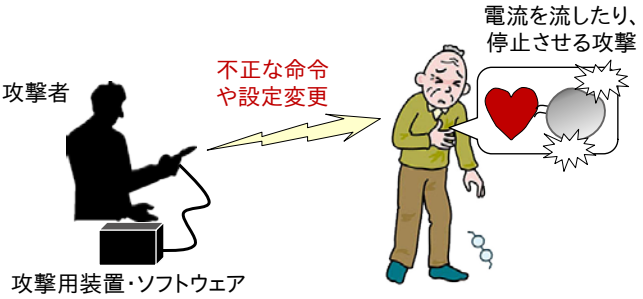


図 2-7　ペースメーカーの脆弱性

原因

医薬品や医療機器に関しては、複数の法律により品質や安全性の確保が進められていますが、セキュリティに関しては世界的に規格や法制度が充分とはいえません。メーカーも意図的な攻撃を考慮していなかったものと想定されます。

対策のヒント

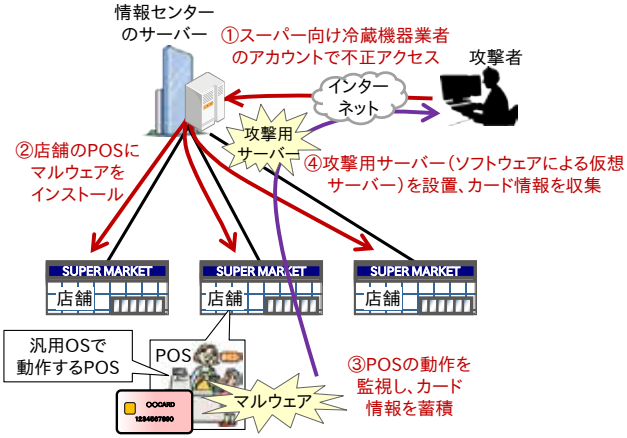
特に無線を利用した攻撃は、攻撃者が対象に隣接する必要がないため、実行の容易性が高まります。特に人命に関わる機器やシステムについては、攻撃者の視点に立って、通常の考え方では想定しえない脅威を見つけ出し、対応することが必要です。

⇒脅威の特定については、5.2.1, P.53 参照

事例3: POS 端末感染による顧客情報の大量流出 ～機器の汎用 OS 上で動作するマルウェア～

事象

2013 年、米国の大手小売チェーンの POS 端末がマルウェア（悪意のあるソフトウェア）に感染し、4000 万人分の顧客のカード情報及び 7000 万人分の個人情報が流出していたことが明らかになりました。手口としては、本チェーンの情報センターに不正アクセスし、管理サーバーから各店舗の POS 端末にマルウェアを埋め込んでカード情報などを収集したと見られています［9］。



出典：一般社団法人重要生活機器連携セキュリティ協議会「生活機器の脅威事例集」を基に作成

図 2-8　POS からの個人情報流出

原因

情報センターのサーバーには、スーパー向け冷蔵機器業者に与えられた遠隔管理用 ID･パスワードをフィッシングメールによって詐取して侵入したそうです。また、店舗の POS 端末に最新のマルウェア対策ツールが使用されていなかったため、攻撃者はマルウェアを埋め込むことが可能でした。POS 端末を攻撃するマルウェアは 2008 年頃から登場し、2014 年に急速に種類が増えています［10］。

対策のヒント

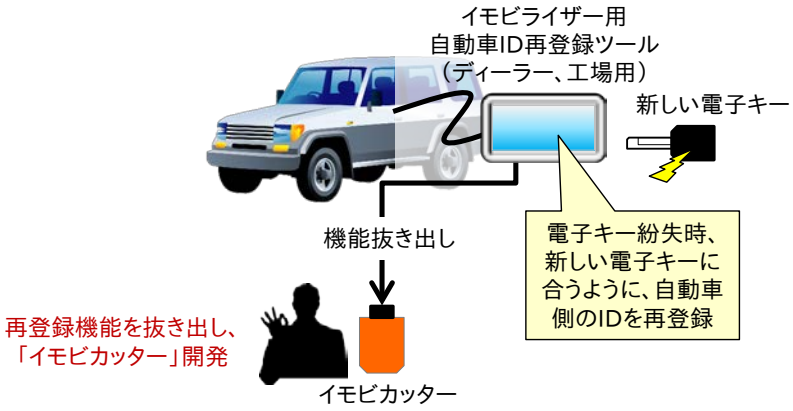
情報センターのサーバーへのアクセス制限の強化、POS 端末に配布されるソフトウェアの認証などが必要です。また、関連業界への攻撃が活性化している時期には、自社システムへの攻撃の有無を確認することが大切です。

⇒脅威情報の収集については 5.2.1(5) P.56 参照

事例4: イモビライザーの無効化による自動車盗難
～ネットで通販されていた最上位のセキュリティ権限～

事象

電子キーと自動車の ID を電子的に照合するイモビライザーは、物理的な鍵と比較して偽造が困難といわれていますが、近年、イモビライザーを無効化するツール（イモビカッター）による自動車の盗難が相次いでいます。イモビカッターは、自動車整備ツールから電子キー紛失時のための ID 再登録機能を抜き出したもので、自動車の整備用端子に接続し、手持ちの電子キーと合う ID を書き込むことで解錠が可能になります［9］。2012 年 11 月にはイモビカッターを使用して自動車を盗んでいたグループが逮捕され、愛知県では 2013 年 7 月から正当な理由なくイモビカッターを所有することを罰する条例が施行されました。



出典：一般社団法人重要生活機器連携セキュリティ協議会「生活機器の脅威事例集」を基に作成

図 2-9　イモビライザーを無効化するイモビカッター

原因

ディーラーで使われている自動車整備ツールの中の、最上位の権限にあたるセキュリティ機能の再設定機能が悪用されたことが原因です。

対策のヒント

このような特権的な操作権限は、ツールとして市販されても不正利用されないような対策が必要です。この場合は機器間の認証が有用です。

⇒セキュリティ設計の手法については 5.2.3, P.59 参照

2.4 その他の事故事例、インシデント事例一覧

(1) 事故事例

表 2-2 事故事例一覧

報道時期	発生機器	内容
2005 年	証券発注システム	発行済み株式数の 42 倍の誤発注に対して取引が成立、ソフトウェアの欠陥で取消ができず
2006 年	電動立ち乗り二輪車	ソフトウェアの不具合により、タイヤが逆回転し運転者が振り落とされる危険性があった
2008 年	二重化システム	稼働系の故障時にリセット通知が出続け、稼働系は自己が処理中と判断、待機系は稼働系の故障を認識できず、切り替えが行われなかった
2008 年	モノレール	インバーターが電源装置の高周波ノイズにより操作を認識しなくなり異常加速、車両がオーバーラン。単線のため衝突の可能性もあった
2014 年	大型トラック	変速機の制御プログラムに不具合があり、ギヤのセレクト位置を検出できないことがあり、誤ったギヤに変速されるおそれがあった

(2) インシデント事例

表 2-3 インシデント事例一覧

報道時期	発生機器	内容
2013 年	胎児モニタ	米国の医療センターで胎児モニタ装置がマルウェアに感染、装置の応答が遅くなった
2014 年	ATM	ATM の内部ユニットにスマートフォンを USB 接続、ウイルスを感染させることで、以後、携帯メールを送信するだけで ATM から現金を引き出せる攻撃手法が登場した
2015 年	輸液ポンプ	患者に自動的に薬液を注入するマイコン制御のポンプに脆弱性があり、薬液の上下限の設定をネットワーク経由で変更可能であった

第3章
セーフティとセキュリティのための開発プロセス

本章では、開発プロセスにおけるセーフティとセキュリティの必要性や具体的なプロセスについて説明します。また、セーフティとセキュリティの設計が加わることによる課題と対応例について示します。その上で、セーフティとセキュリティの違いを把握しつつ、両者を連携して進めることで効率化を図る考え方を示します。

3.1 開発プロセスにおけるセーフティとセキュリティの対応

(1) セーフティとセキュリティ対応の必要性

2章の事例のような事故やインシデントはどのような対応を行っていれば防げたのでしょうか。事故の事例に関しては、

・テストシナリオが網羅的ではなく、不具合を発見できなかった

・安全関連系の機能でありながら、一つの不具合で動作に支障をきたした

などの課題が挙げられます。また、インシデントの事例に関しては、

・ユーザーの環境や運用に対する想定が楽観的であった

・脅威の想定が不充分であった

などの課題が挙げられます。これらについては、過去の知見や事例などを収集・分析し、事故やインシデントを引き起こすハザードや脅威を想定、セーフティとセキュリティの対応を行うことで予防できた可能性があります。

しかしながら今後の「つながる世界」においては、過去の知見や事例からは想像もできないハザードや脅威も懸念されます。例えば、故障や攻撃がネットワークを通じて他の機器やシステムに影響を与え、現状では予想できない事態を引き起こすかもしれません。このため、セーフティとセキュリティの対応を開発プロセスの上流から組み入れ、要求仕様の段階から将来のハザードや脅威に備えていくことが必要です。

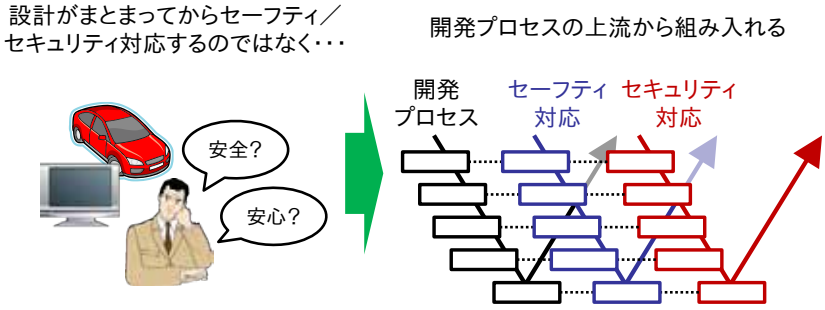


図 3-1 開発プロセスの上流からセーフティとセキュリティの対応を組み入れる

(2) セーフティとセキュリティの設計への経営層の関与

機器やシステムのセーフティとセキュリティの対応は、企画から設計開発、販売・サポート、廃棄まで、ライフサイクル全体において必要となります。また、事故やインシデントが発生すると、損害賠償や企業の信用失墜など、ビジネスに取り返しのつかない影響を与える場合がありますので、セーフティとセキュリティの対応には、開発部門の責任者だけでなく、経営層や品質管理部門責任者も関与することが必要です。

具体的には、経営層は企業としてセーフティとセキュリティを実現するための基本方針（ポリシー）を策定し、それを開発現場に徹底することが必要です。実現のための予算確保や体制整備も欠かせません。また、機器やシステムの設計においては、要件レベル、システムレベル及びハードウェア／ソフトウェアレベルの各段階においてセーフティとセキュリティに関わる「要求・分析」、「設計・開発」及び「テスト・評価」のサイクルを回すとともに、経営に大きな影響を及ぼすものについては、見える化されたドキュメント等を使って経営層や品質管理部門責任者に報告、承認を得ることが必要です（「見える化」については 6.1, P.69 参照）。

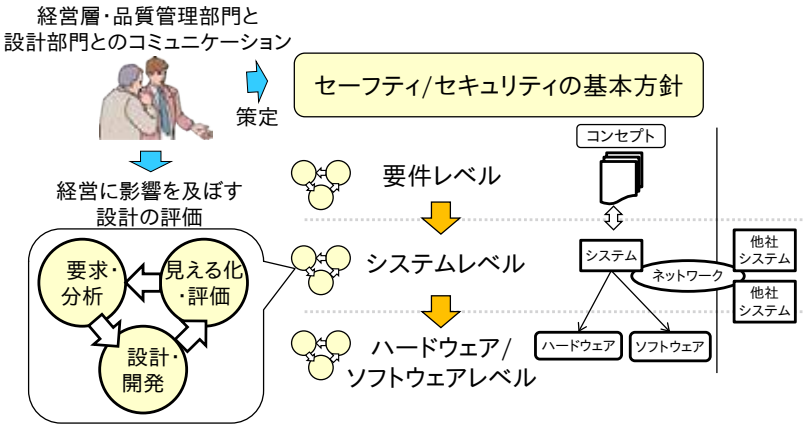


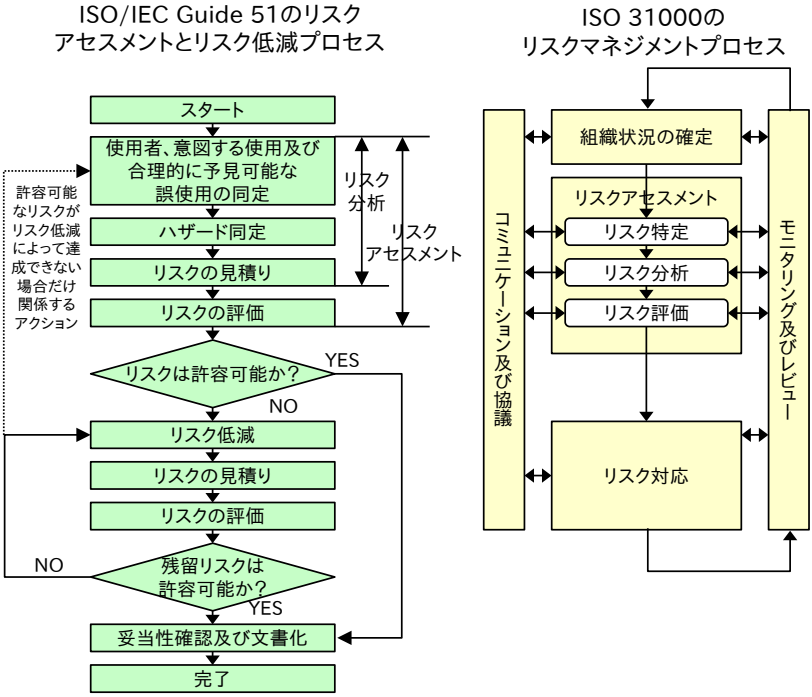
図 3-2 セーフティとセキュリティの設計への経営層の関与

これにより、開発現場に対して企業としての安全・安心に対する考え方を周知できる上、万一、事故やインシデントが発生した場合に、経営層が迅速に対応を行うことが可能となります。

3.2　セーフティとセキュリティの対応のプロセス

(1)　リスク対応全体のプロセス

セーフティの基本概念を明確化した国際規格である ISO/IEC Guide 51 及びセキュリティ関連規格で参照されているリスクマネジメントの国際規格 ISO 31000 では、図 3-3 のようにリスク対応のプロセスが示されています。



出典：ISO/IEC GUIDE 51:2014 及び ISO 31000:2009 を基に作成

図 3-3　ISO/IEC Guide 51 と ISO 31000 におけるリスク対応のプロセス

セーフティとセキュリティのリスク対応プロセスは、表現は異なるものの、リスクの特定、リスク分析、リスク評価、リスク対応というプロセスを繰り返すという基本的な流れは同様です。セーフティではリスクの原因としてハザードを特定（同定）、セキュリティでは脅威を特定することとなります。

(2) リスク低減のプロセス

前述の ISO/IEC Guide 51 では、設計段階におけるリスク低減プロセスとして、以下の「3 ステップメソッド」が示されています。

表 3-1 ISO/IEC Guide 51 のリスク低減策「3 ステップメソッド」

3 ステップメソッド	概要
STEP1：本質的安全設計	可能な限りリスクを除去するか軽減すること（ハザードの排除・無力化・隔離）
STEP2：ガード及び保護装置	除去できないリスクに対しては、必要な保護手段を採用すること
STEP3：使用上の情報提供	STEP2 の低減策後にも残るリスクをユーザーに知らせ、特別なトレーニングを必要としたり、身体保護具を必要とするか等を明記すること

出典：経済産業省「リスクアセスメント・ハンドブック実務編」［11］を基に作成

STEP1 の本質的安全設計とは、ハザードとなる部品や機能自体を除去したり、耐久性が高い部品を使用して発生確率を減らしたりする対策です。STEP2 は必要な保護手段による対策であり、特にセーフティ機能によるものを機能安全と呼びます。STEP3 はユーザーへのリスク情報の提供による対策です。セキュリティにおいても同様に、脅威の原因となる情報や機能の除去によるリスクの回避、セキュリティ機能の追加や強化による対策などによりリスクの低減を図ります。

以上のようにセーフティとセキュリティのリスク低減においても類似したプロセスがあるため、連携して実施することにより効率化が図られると期待されます。

(3) セーフティ機能とセキュリティ機能の高信頼化の重要性

前述のリスク低減プロセスにおいて、STEP1 の本質的安全設計やリスク回避後、STEP2 でセーフティ機能とセキュリティ機能によりリスク対応する場合、その機能自体が故障したり、誤動作したりするようではリスクを低減できません。そのため、セーフティ機能とセキュリティ機能に対しては、より品質の高い設計が必要となります。

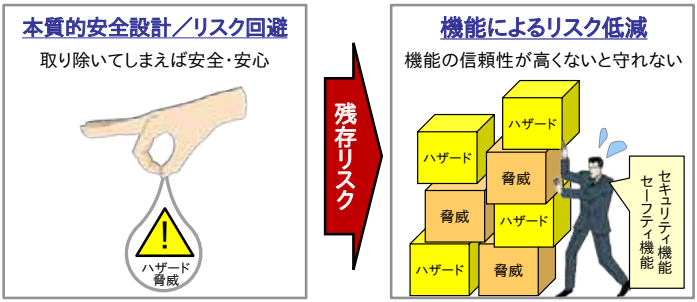


図 3-4　セーフティ機能とセキュリティ機能の重要性

3.3　セーフティとセキュリティの開発プロセスの課題と対応

図 3-5 にV字開発モデル［12］とセーフティとセキュリティ設計のプロセスの関係を例示します。機器やシステムを構成する組込みシステム（機器に組み込まれたコンピューターシステム）に対して、図のようなプロセスでリスクを低減するためのセーフティとセキュリティ機能を組み込む設計を行います。

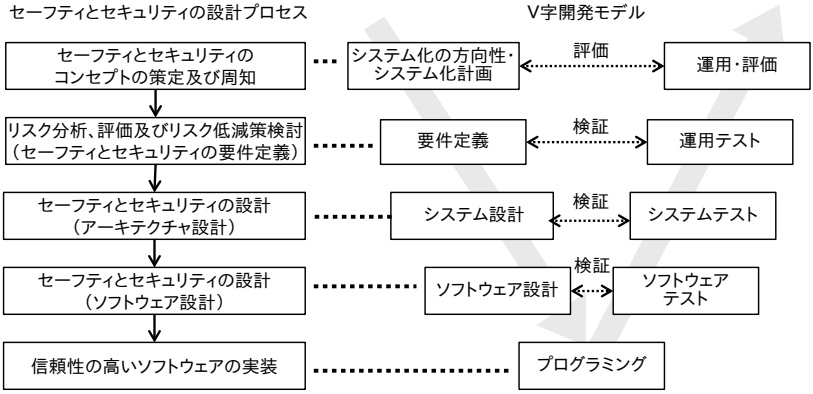


図 3-5　V字開発モデルとセーフティとセキュリティ設計のプロセス

しかし生活機器の組込みシステムの CPU やメモリ、通信速度は性能が低いものが多く、新たにセーフティ機能やセキュリティ機能を追加する場合は、処理に遅延が生じる可能性があります。また、セキュリティ機能が外部からの攻撃を防ぐためにメモリ上のデータ配置を複雑化することで、他の機能の処理に影響が生じることもあります。

このため、機器やシステム上でセーフティとセキュリティ機能を実現するためには、必要十分なリソースと、要件定義とシステム設計のすり合わせ（検討の繰り返し）が必要となります。これについては、下の図 3-6 のように Twin Peaks モデル［13］などの手法を利用し、「要件」→「セーフティ／セキュリティ分析」→「アーキテクチャー」のサイクルを繰り返しながら詳細化を図っていくことが挙げられます。

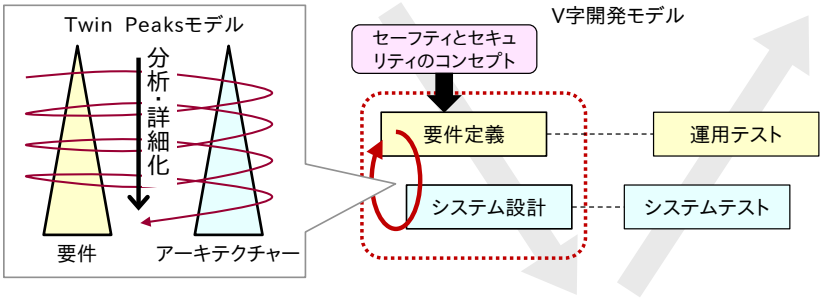


図 3-6　Twin Peaks モデルによる要件とアーキテクチャーの分析･詳細化

3.4　セーフティとセキュリティの特徴の比較

本章では、セーフティとセキュリティの対応のプロセスが類似しているため、併せて検討することで効率化を図る考え方を説明しました。しかしセーフティとセキュリティとでは性質の違いも多く、用語も異なります。そこで、参考として表 3-2 に両者の相違点を示します。

表 3-2　セーフティとセキュリティの相違点

相違点	セーフティ	セキュリティ
保護対象の違い	人命、財産（家屋等）など	情報の機密性、完全性、可用性など
原因の違い	合理的に予見可能な誤使用、機器の機能不全	意図した攻撃
被害検知の違い	事故として表れるため、検知しやすい	盗聴や侵入など、検知しにくい被害も多い
発生頻度	発生確率として扱うことができる	人の意図した攻撃のため確率的には扱えない
対策タイミング	設計時のリスク分析・対策で対応	時間経過により新たな攻撃手法が開発されるので、継続的な分析・対策が必要

上記のとおり、セーフティとセキュリティでは、保護対象や原因などの点で大きな違いがあり、必要とされる技術や知識も異なるため、対応する技術者が異なるケースが多いのが現状です。しかしながら、つながる世界では、セキュリティ上の脅威がネットワークを通じて伝搬し、機器やシステムのセーフティに影響を与える可能性もあり、両分野は互いに影響しあっています。そのため、安全・安心な機器やシステムを実現するためには、両分野の技術者が相違点を理解した上で、協力して対応する必要があります。

第4章
ソフトウェア技術者のための セーフティ設計

機器やシステムの故障やユーザーの誤操作による事故は、人命や財産に危害を及ぼし、企業のビジネスにも多大な影響を与える可能性があります。できるだけ早期にハザードを取り除くことが必要です。本章では、セーフティ対応のプロセスにおけるハザードの特定、リスク評価及びセーフティ設計を中心に解説します。

4.1　セーフティ対応の開発プロセス

システムのセーフティ（安全性）とは、機器やシステムが危害や損害をもたらすことのない期待度合いを指します。以下に JIS(日本工業規格)における定義を示します。

> 安全性：システムが、規定された条件のもとで、人の生命、健康、財産又はその環境を危険にさらす状態に移行しない期待度合い
> (JIS X 0134：1999 システム及びソフトウェアに課せられたリスク抑制の完全性水準)

実際に事故が発生すると損害賠償や信頼の失墜などビジネス上の損失は多大であり、特に人命は取り返しがつかないことから、設計段階での的確なセーフティ対応が求められます。

セーフティ対応のプロセスとしては、まず、機器やシステムに潜在する危険(ハザード）を特定し、その発生しやすさと被害の深刻度からリスクを評価します。この結果、リスクに応じてセーフティ設計を進めます。

本章では図 4-1 の流れで、各プロセスについて手法を中心に説明します。また、セーフティに関連する国際規格（評価・認証制度）についても説明します。

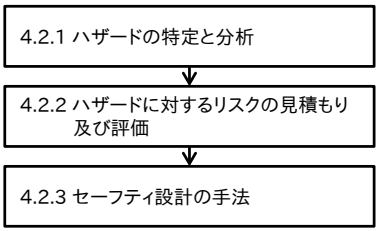


図 4-1　セーフティ対応の開発プロセス

4.2　セーフティ設計

4.2.1　ハザードの特定と分析

ハザードとは、機器やシステムが不動作・誤動作などにより危害や損害をもたらす潜在的な要因を意味します。新たな機器やシステムを開発する場合には、従来の製品や他の事故事例を収集・分析し、ハザードを特定（「同定」とも呼ばれます）する必要があります。以下に、その手法の例として FTA、FMEA、HAZOP 及び STAMP/STPA の概要を説明します（各手法は独立しており、任意に選択して適用することが可能です）。

(1)　FTA（Fault Tree Analysis）

FTA は事故などの事象について、トップダウンで原因を分析し、ハザードを特定する手法で、表記方法が IEC 61025:2006（JIS C 5750-4-4:2011）で規定されています。図 4-2 に一例を示します。何らかの事故などを対象とし、その事象（「頂上事象」）が発生するための「中間事象」をツリー上に展開します。以下の表記例では、同時発生が条件の場合に「AND ゲート」、いずれかの発生が条件の場合に「OR ゲート」で分岐させます。なお「基本事象」とはこれ以上展開できない事象であり、図 4-2 の例では基本事象①は中間事象①のハザードの一つとなります。また「非展開事象」とは、展開は可能であるが省略していることを示します。

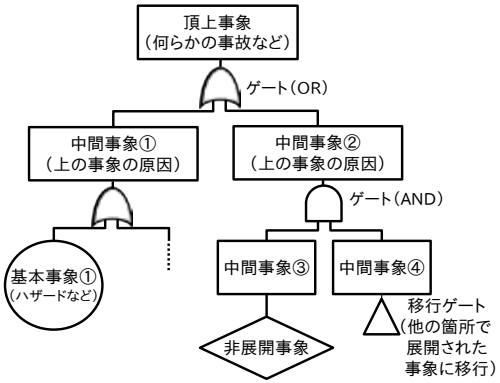


図 4-2　FTA の表記例

FTA は、手順自体はシンプルで分かりやすい手法ですが、多数の機器やシステムが相互に連携する場合にはツリー構造が大規模になり、扱いづらくなります。

(2) FMEA（Failure Mode and Effects Analysis）

FMEA は、システムや装置などの故障要因の抽出手法として、システムを構成する機器や部品にある故障が発生したとき、その故障がシステムにどのような影響を及ぼすかを解析し、大きな影響を及ぼす機器や部品をみつけるための手法です。具体的には、国際規格の IEC 60812 の FMEA 規格 2 の標準ワークシートなどを参考に、対象となる機器やシステムに適した評価項目や、故障モードの発生頻度、致命度などの評価方法を設定し、ワークシートを作成します。

表 4-1　エアコン設計用 FMEA の例

部品、機構	故障モード	原因	影響	重要度	設計対応	確認、効果
温水弁	弁閉まらず 電極破損	弁磨耗 絶縁不良	暖停止不能 火災	A A	弁漏れ小構造 メンテナンス 保護カバー採用	加速耐久性確認 破損時問題なし
ドレンポンプ	回らず	過熱（軸受） 過熱（巻線）	排水不能 運転不能	A A	モーター部冷却強化 玉軸受採用、保護回路	(20 年以上)確認

出典：経済産業省「消費生活用製品向けリスクアセスメントのハンドブック」［14］を基に作成

その上で、機器やシステムの「故障モード」(機器あるいは部品の故障の状態、故障現象)を抽出し、ワークシートで分析を行います。

FTA が事故などの事象からその要因となるハザードを分析していくトップダウン方式であることに対して、FMEA は故障モードから事故などの影響を想定していくボトムアップ方式といえます。このため、事故が発生する前に故障などを想定して予防を行える点がメリットです。ただし、実際に事故が起こる前に誤使用などのヒューマンエラーや環境条件までを考慮して故障モードや原因を想定することは容易ではない点、複合的な故障は検討に適さない点などが課題です。

(3) HAZOP（Hazard and Operability）

HAZOP（ハゾップ、IEC 61882:2001）では設計で想定するプロセスと実際のプロセスの「ずれ（異常）」に着目し、「ずれ」を解消するか、「ずれ」により危険な状態や事故に移行することを防ぎます。HAZOP では表 4-2 のような「ガイドワード」を設定し、システム・機器に応じた適切なパラメータ（変数）と組み合せ、表 4-3 のように該当する「ずれ（異常）」を整理します。

表 4-2　HAZOP の基本的なガイドワード

HAZOP ガイドワード	意味
No or not	ない，設計意図の完全な否定
More	量的な増加
Less	量的な減少
As well as	余分など質的な調整／増加
Part of	部分，不充分など質的な調整／減少
Reverse	逆，反対など設計意図とは論理的に反する
Other than	別もの，完全な置換

出典：JIS C 5750-3-1 を基に作成

FTA が事故などを起点としているのに対し、HAZOP では設計と実際の「ずれ」を起点とすることで予期せぬ事象を洗い出せる点がメリットといえます。ただし、事故につながらない事象も含まれ、検討項目が増えるため、整理が必要です。

表 4-3　HAZOP における「ずれ（異常）」の整理例

No.	パラメータ	ガイドワード	ずれの内容	ずれの原因	システムへの影響	安全対策
1	回転速度	Less	回転速度小	・回転機構への異物の噛込み	・過電流による電子機器の発熱 ・機器の過大振動	・電流リミッター ・変異センサーによる電源遮断
2	温度	More	冷却水温度高	・ソフトウェアエラーによる熱交換器流量制御バルブの誤閉止	・温度上昇による電子制御系の誤作動 ・機器の劣化	・温度モニタ ・流量モニタ

出典:「川原卓也：潜在危険分析とリスク分析、(株)日本機能安全、機能安全エキスパート・セミナー」を基に作成

(4) STAMP/STPA

STAMP（スタンプ、Systems-Theoretic Accident Model and Processes）はシステム理論に基づく事故モデル、STPA（System-Theoretic Process Analysis）は STAMP に基づくハザード分析手法です。FTA や HAZOP は主に機器単体のハザード分析を対象としていますが、つながる世界ではシステムが複雑に連携するため、STAMP/STPA ではシステム間の制御構造（コントロールストラクチャ）に着目し、「コンポーネント間の相互作用」を分析します。以下に手順の概要を説明します。

Step.0 準備

避けるべき事故とハザードを想定し、システムの制御構造を図にします。

Step.1 非安全な制御の識別によるハザードシナリオの分析

以下の 4 つのガイドワードを基に、機器間の制御において事故をもたらすと懸念されるハザードを洗い出します。

1. “Not Provided”
   安全のためのコントロールアクションが設置されていない
2. “Incorrectly Provided”
   ハザードにつながる、安全ではないコントロールアクションが設置されている
3. “Provided Too Early, Too Late, or Out of Sequence”
   安全のためのコントロールアクションが設置されているが、タイミングが遅すぎる、早すぎる、または定められた順序に設置されていない
4. “Stopped Too Soon”
   安全のためのコントロールアクションが設置されているが、すぐに止まる、もしくは適用が長すぎる

Step.2 制御ループの作成による潜在要因の分析

ハザード毎に制御主体と制御対象プロセスの制御ループ図を作成し、原因となる不適切な制御や矛盾の可能性を洗い出します。制御主体は制御対象プロセスに対して制御を行います。制御の結果、制御対象プロセスは制御主体に対して、応答などのフィードバックを返すことがあります。制御主体は制御対象プロセスの状態を「モデル」として持ち、制御が必要かどうか判断します。

Step.3 潜在要因に対する対策

洗い出された不適切な制御や矛盾などに対し、それらが発生しないような安全制約（安全対策や安全制御）が整備されているかを確認します。

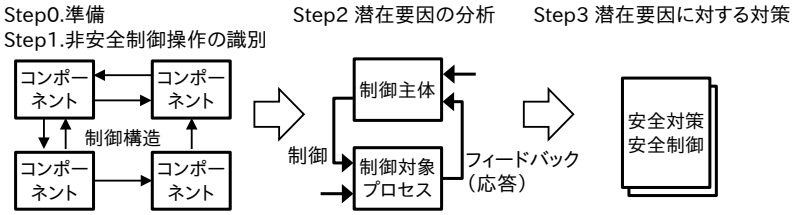


図 4-3　STAMP/STPA のイメージ

STAMP/STPA は、宇宙、航空、自動車やエネルギーなど複数の分野でハザード分析に利用されています［15］［16］［17］。

(5)　ハザードの例

本項で説明してきた手法で特定されるハザードにはどのようなものがあるのでしょうか。ここでは自動車分野及びスマート家電分野を例に、具体的なハザードを列記します。

表 4-4　自動車分野のハザードの例

No	ハザードのタイプ	ハザードの例
1	アクチュエータ故障	ブレーキ故障、操舵機故障など
2	センサー故障	車輪速度値異常、ドア開閉値異常など
3	誤動作	電磁波による、電圧変動による誤動作など
4	挟み込み	自動ドア、電動ウインドウなど
5	回転部への巻き込み	車輪、ファン、ベルトなど
6	静かな接近	動いていることに気づかれにくいなど
7	燃料による火災	ガソリン、ガス、大容量電池など
8	感電	EV 充電時、事故による充電池露出など
9	化学物質の爆発	エアバッグが不意に爆発
10	人・物に衝突	死角の人・物、スリップ、車線変更、出会い頭など
11	操作間違い	壁に急発進、ブレーキとアクセル同時踏み込みなど
12	注意低下	居眠り、わき見など
13	意識喪失	病変、事故で重体、救助要請できないなど

表 4-5　スマート家電分野のハザードの例

No	ハザードのタイプ	ハザードの例
1	巻き込み、はさみこみ	洗濯槽、自動ドアなど
2	長時間の熱	充電池による低温やけど、電気カーペットなど
3	高温・過熱	ポットの熱湯あふれ、機器の過熱など
4	部品故障	モーター・パワーコンディショナ・充電池の火災、エレベーター誤動作など
5	感電	ぬれ手、短絡、地絡など
6	過電流	電池の過充電、配線・プラグの炎上など
7	電池切れ	携帯型治療器の停止、ドローン墜落など
8	電波の混信	エアコン、ドローンのリモコン誤動作・停止など
9	水没	電子機器破損、人の死亡など
10	ほこり	電気回路の短絡、過熱など
11	誤飲	幼児とボタン型電池、小型機器など
12	転倒	ひっかけ、振動による電気製品の転倒など
13	復電	地震による停電復旧後の通電火災など

4.2.2　ハザードに対するリスクの見積もり及び評価

ハザードが特定されたら、そのハザードによって被害に至る状況を分析し、発生しやすさや被害の深刻度を明らかにすることで、生じるリスクを見積もります。例えば、部品の劣化などにより発生する故障とユーザーの操作や環境条件の組み合わせにより必ず発生する故障では発生しやすさが異なります。また、起動しなくなる故障と人命に係る誤動作では、想定される被害の深刻度が異なります。そこで、発生しやすさと被害の深刻度を組み合せてリスクを導出します。次に、見積もったリスクを評価し、許容できるレベルかを判定します。

表 4-6 に手法の例を示します。なお、※印の手法は 4.2.1 でハザードの特定と分析の手法として紹介したものですが、同時にリスクの見積もりを行うことも可能です。

表 4-6　リスク見積もり及び評価手法の例

手法	手法の概要
リスクマトリックス	危害の発生頻度と危害の重大性から 2 軸の表形式でリスクの程度を分類する(4.2.2(1), P.42 参照)
リスクグラフ	頻度、過酷度、止めやすさなど複数要素の有無を順に判断して、リスクのレベルを分類する(4.2.2(2), P.43 参照)
FTA※	事故など望ましくない事象を起点に、その発生原因を体系的に整理する(4.2.1(1), P.36 参照)
FMEA※	部品の故障を起点に、システムへの影響を体系的に検討する(4.2.1(2), P.37 参照)
HAZOP※	ガイドワードとパラメータ（変数）を組み合せ、システマティックに設計想定からの「ずれ」を仮定し、システムのハザードを想定する（4.2.1(3), P.38 参照）
STAMP/STPA※	システム間の制御ごとにガイドワードを適用して、複雑なシステムでの相互作用のハザードを特定する（4.2.1(4), P.39 参照）

（注）※の手法は、ハザード特定にも使われる手法（4.2.1, P.36 参照）

出典：「米国における STAMP（システム理論に基づく事故モデル）研究に関する取り組みの現状」［15］、JEMIMA「機能安全規格の技術解説」［18］を基に作成

例として、リスクマトリックス及びリスクグラフの概要を説明します。

(1)　リスクマトリックス

危害の発生頻度と危害の重大性のランクをそれぞれ縦軸、横軸とするマトリックスを作成し、その各マス目に対応するリスクの大きさのクラス番号を記入します。リスクマトリックスの縦軸と横軸の分類については製品の特性に合わせて設定するか、公表されているものから選択します。手順としては、まず特定されたハザードについて、発生頻度と危害の程度を見積もります。次に、リスクマトリックスを用いてリスクのクラスを判定します。

図 4-4 に、独立行政法人製品評価技術基盤機構(NITE)製品安全センターで採用しているリスクマトリックスの一種である R-Map を示します［19］。リスクのクラスが A1～A3（許容できないレベル）にマッピングされたハザードについては、許容可能なレベルに移行するまで、発生頻度や危害の程度を低減する対策を行います。

発生頻度							
5	(件/台･年) 10^{-4}超	頻発する	C	B3	A1	A2	A3
4	10^{-4}以下 10^{-5}超	しばしば発生する	C	B2	B3	A1	A2
3	10^{-5}以下 10^{-6}超	時々発生する	C	B1	B2	B3	A1
2	10^{-6}以下 10^{-7}超	起こりそうにない	C	C	B1	B2	B3
1	10^{-7}以下 10^{-8}超	まず起こり得ない	C	C	C	B1	B2
0	10^{-8}以下	考えられない	C	C	C	C	C
			無傷	軽微	中程度	重大	致命的
			なし	軽傷	通院加療	重症、入院治療	死亡
			なし	製品発煙	製品発火 製品焼損	火災	火災(建物焼損)
			0	I	II	III	IV

危害の程度(危害の重大性)

A1～3：対策必須
（対策しなければ製品の出荷は不可）

B1～3：要対策
対策の検討を行うことが必要

C：許容可能

出典：(財)日本科学技術連盟「製品安全,リスクアセスメントのための R-Map 入門(第 1 版)」［19］を基に作成

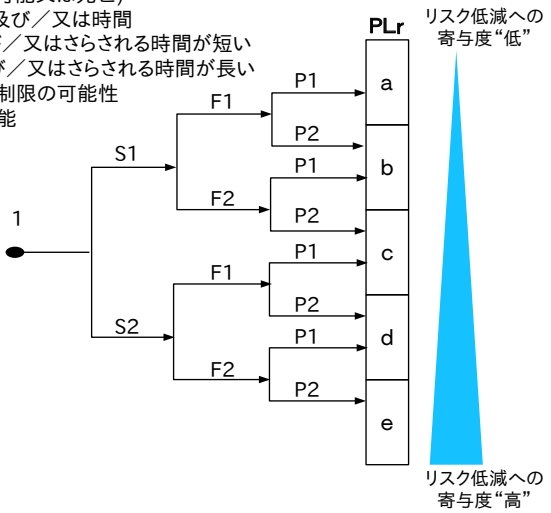
図 4-4　R-Map の例

NITE では、消費者向け製品の事故事例に対して R-Map でリスクの見積もり及び評価を行った結果を Web サイトで公開しています［20］。

(2)　リスクグラフ

国際規格のひとつ「ISO 13849-1:2006(JIS B 9705-1:2011)」（機械類の安全性-制御システムの安全関連部：設計のための一般原則）では単位時間当たりの危険側故障発生確率から規定した「PL（パフォーマンスレベル）」を定義しています。機械の安全機能を実行する部分を「制御システムの安全関連部」と呼び、近年、安全関連部を構成する機器には半導体部品が多く使われ、制御もハードワイヤー制御からソフトウェア制御に移って来ています。予見可能な条件下で、安全機能を実行するための制御システムの安全関連部の能力を規定するために用いられる区分レベルを PL と呼びます。この安全関連制御システムの PL は「要求パフォーマンスレベル(PLr)」と同等かそれ以上であることが求められます。図 4-5 に、この PLr を決定するために使われるリスクグラフを示します。

記号の説明
1:リスク低減に安全機能の寄与度を評価するため開始点
S:傷害のひどさ
S1:軽症(通常、回復可能な傷害)
S2:重傷(通常、回復不可能又は死亡)
F:危険源への暴露の頻度及び／又は時間
F1:まれ～低頻度、及び／又はさらされる時間が短い
F2:高頻度～連続、及び／又はさらされる時間が長い
P:危険源回避又は危害の制限の可能性
P1:特定の条件下で可能
P2:ほとんど不可能



出典：JIS B 9705-1:2011 を基に作成

図 4-5　リスクグラフ

リスクグラフは、3 つのリスクの要素（リスクパラメータ「S」「F」「P」）について、2 つの選択肢で振り分けることでリスク評価を行います。リスクの 3 要素は「傷害のひどさ(S)」、「危険源への暴露の頻度、及び／又は時間(F)」及び「危険源回避又は危害の制限の可能性(P)」となります。

PL は、対象とする制御システムの安全関連部がハザードを回避する能力であり、単位時間当たりの危険側故障発生確率（安全でなくなる故障の発生確率）により a～e にランク分けされます。

表 4-7　パフォーマンスレベル

パフォーマンスレベル(PL)	単位時間当たりの危険側故障発生の平均確率
a	10^{-5}以上 10^{-4}未満　(0.001%～0.01%)
b	3×10^{-6}以上 10^{-5}未満　(0.0003%～0.001%)
c	10^{-6}以上 3×10^{-6}未満　(0.0001%～0.0003%)
d	10^{-7}以上 10^{-6}未満　(0.00001%～0.0001%)
e	10^{-8}以上 10^{-7}未満　(0.000001%～0.00001%)

出典：JIS B 9705-1:2011 を基に作成

危険側故障発生確率は「カテゴリ(安全関連部の構造)」、「平均危険側故障時間」、「平均診断範囲」及び「共通原因故障」といった要素により決定されます(決定方法は「ISO 13849-1:2006(JIS B 9705-1:2011)」をご参照ください)。この PL が許容できないレベルである場合には、セーフティ機能を追加・増強するなどの対応を行い、再度、PL を導出します。なお、PL を含めたセーフティとセキュリティの尺度については、6 章の表 6-1, P.72 を参照ください。

4.2.3 セーフティ設計の手法

(1) セーフティ対策の考え方

特定されたリスクが許容できないレベルの場合には、3.2 で説明したように、本質的安全設計によりリスクの除去や軽減を図り、それでも許容できないリスクが残る場合には安全防護策及び保護装置(セーフティ機能など)により対応します。表 4-8 に、リスク低減に関する考え方を例示します。

表 4-8 リスク低減に対する考え方の例

考え方	内容	本質的安全の例	機能安全の例
フールプルーフ	知識や経験が不足していても事故に至らない仕組み	・バッテリーが正しい向きにしか入らない構造のデジタルカメラ	・洗濯機の回転を検知して停止するまでフタを開かないようにする機能
アフォーダンス	自然に想定された利用方法を選択したくなる仕組み	・形を使う(構造で実現) ・色を使う(〃) ・場所を使う(〃)	・形を使う(機能で実現) ・色を使う(〃) ・場所を使う(〃)
フェールセーフ	環境の状況や、部品の故障による被害を最小限にとどめる仕組み	・バッテリーが上がっても機械的に解錠できる自動車のドアロック	・揺れを検知してヒーターを停止する機能
フォルトトレランス	システムの一部に問題が生じても機能停止させない仕組み	・パンクしても短距離であれば安全に走行し続けられるタイヤ	・ネットワーク制御機器が通信障害時に自律的に動作を維持する機能
多層防御	一つの仕組みで守れなくても別の仕組みがあること	・本質的安全の組み合わせにより、リスクを低減	・あるセーフティ機能が故障しても、別のセーフティ機能でリスクを低減

出典:IPA 「組込みシステムの安全性向上の勧め」[1]を基に作成

(2) セーフティに有効な設計手法

セーフティ機能は機器に組み込まれたコンピューターシステムで実現されるものが多く、センサーや外部ネットワークからの情報を基に柔軟に処理を行うことが可能となっています。しかし、ソフトウェアの欠陥やハードウェア故障により、セーフティ機能自体が動作しなくなる可能性もないとはいえません。そこで、セーフティ機能を実現する組込みシステムでは、設計品質を高める手法が使用されています。

組込みシステムのソフトウェアの規模は年々増大しており、そのソースコードの行数は、数百万行から一千万行といわれています［21］。このような大規模な組込みソフトウェアの設計・検証を容易とし、設計品質を高める手法を表 4-9 に例示します。

表 4-9　設計品質を高める手法の例

設計手法	内容	効果
モデルベース開発(MBD)	制御などの処理を数式として表現した「モデル」を用いて、機器やシステムの挙動をシミュレーションしながら仕様検討及び設計を行う手法	挙動を検証しながら設計可能、開発サイクルも高速化
モデルベースシステムズエンジニアリング(MBSE)	「製品やサービスなどのシステムの開発を成功に導く」ことを目的として、システム開発の全体最適を図るための技法、そのためのプロセスを定義している	大規模で複雑なシステムもモデルの集合として表現しやすい
形式手法	数理論理学に基づく仕様記述言語を用いて設計対象を表現することで、あいまいさを除去するとともにツールによる設計検証の支援を可能とする手法	あいまいさの除去により、論理的な厳密性が高まる

「モデルベース設計」や「形式手法」では、設計情報からコードを自動生成するツールもあり、開発品質やコストの改善にも寄与することが期待されます。

また、二重化などにより機器やシステムの安全性を高める仕組みの例を表 4-10 に示します。

表 4-10　機器やシステムの安全性を高める仕組みの例

仕組み	内容
領域分割	マイコン(コア)、仮想マシン、メモリの領域、ネットワークなどを機能や安全度ごとに分割して、被害の影響範囲を限定的とする。故障やソフトウェアの欠陥の影響範囲を最小限にするためのインヒビット設計［22]など。
自己診断	製品・システム内の異常を定期的に監視して復帰または停止させる。ウォッチドッグ、FDIR(故障検知-分離-修復)［23］等
人間中心設計(ISO 9241-210)	人間工学やユーザービリティの知識と技術を適用することにより使いやすく、操作誤りの少ないインタフェースを構築する
二重化(多重化)	ソフトウェア／ハードウェアを二重化（多重化）し、異常時に処理を切り替えたり（デュプレックス方式)、並列実行して動作を比較したりして異常を検出する（デュアル方式）

組込みシステムにおいては、前述の手法や仕組みを各々の特徴を活かしながら柔軟に組合せて利用することが可能です。

(3)　使用上の情報の提供によるリスクの低減

リスクに対する本質的安全及び機能安全の設計後、残存するリスクに対して、利用者への情報提供による低減を検討します。表 4-11 に、ISO/IEC Guide51:2014 におけるリスク低減手順（ステップ３）に示された項目を示します。

表 4-11　ISO/IEC Guide 51:2014　設計で取られるリスク低減策(抜粋)

使用上の情報を提供する
- ・製品上 又は梱包上への方策
  - － 警告標識・表示、警告信号
  - － 警告装置
- ・使用のための指示
  （必要な場合）
  取扱説明書に使用情報又は
  訓練情報

上記の警告機能や取扱説明書での情報提供によるリスク低減効果を評価･検証し、設計時点の最終的な残存リスクを明らかにします。なお、製品での警告標識・表示、警告信号や警告装置もセーフティ機能に含まれますので、品質が高い設計が必要となります。

4.3　セーフティ設計の評価・認証

1998 年に制定された国際規格である IEC 61508 は「電気・電子・プログラマブル電子安全関連系の機能安全」に関して構想段階から設計・開発を含め保守・廃棄に至るまでを 16 のフェーズに分け、それぞれのフェーズ毎に要求事項を定めたものです。本基準は、ハードウェア／ソフトウェアに対する要求事項のほか、参考としてリスクと安全度の概念や安全度水準（SIL: Safety Integrity Level）の決定方法なども記載しています。機能安全に関連した規格は、現在まで表 4-12 のように各分野で制定されています。

表 4-12　機能安全に関連した主な規格の制定状況

制定された年	分野	規格番号
1998 年	全般	IEC 61508-1,3,4,5
2000 年	全般	IEC 61508-2,6,7
2001 年	原子力	IEC 61513
2002 年	鉄道システム	IEC 62278
2003 年	プロセス産業	IEC 61511-1
	鉄道	IEC 62279
	電動モーター	IEC 61800
2004 年	プロセス産業	IEC 61511-2,3
	家庭用電気機器	IEC 60335
2005 年	機械類	IEC 62061
2006 年	医療機器ソフトウェア	IEC 62304
2010 年	全般（改訂）	IEC 61508
2011 年	自動車	ISO 26262
2014 年	パーソナルケアロボット	ISO 13482

認証機関による機能安全認証には、機器やシステムが上記規格に準拠していることを認証する「製品認証」と、企業等の開発プロセスが機能安全規格に準拠していることを認証する「プロセス認証」などがあります。製品認証を取得することにより、一定の安全度水準を満たす機器やシステムであることを顧客に説明する際の根拠となります。またプロセス認証を取得することにより、新たな機器やシステムの認証を取得する場合にソフトウェア開発のプロセスに関する評価の一部を省略することが可能となります。

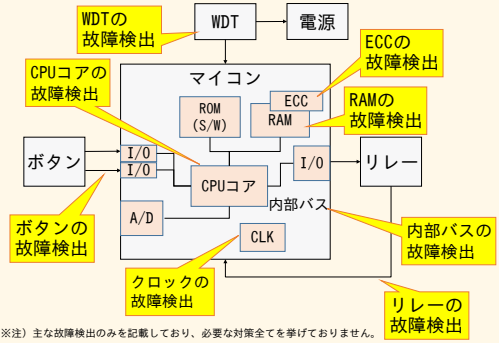
コラム3 機能安全設計、どこまで考えれば完成！？

株式会社ヴィッツ
森川 聡久さん

IEC 61508, ISO 26262 などの機能安全規格では、様々な構成要素の「故障による危険」をも防げる設計が必要ですが、「どこまで対処すれば充分に安全か」を説明するのは非常に苦労します。

故障は恒久故障と一時故障に大別できますが、一般的に「一時故障」の方が対策は難しいです。例えば RAM の場合、ノイズや宇宙線によって、ある変数の 1 ビットが化けた場合を想定する必要があります。もし、この一瞬の故障が重大な危険を引き起こす可能性があれば、常に監視が必要です。ECC 付きの RAM は簡単な対策としてよく採用されています。しかし、RAM とマイコンをつなぐ内部バスの故障は検出できないためこれだけでは不充分です。一方、ソフトウェアで変数を二重化し比較する方法で、内部バス故障を検出できます。

では、ECC＋内部バス故障対策があれば充分でしょうか？実はまだ充分ではありません。何故なら、ECC が本当に正常に動作するかが保証されていないためです。筆者の過去の対策例では、「ECC 自身の故障検出回路」を搭載した ECC を用いて、常に監視する方法があります。



※注）主な故障検出のみを記載しており、必要な対策全てを挙げておりません。

それでは、ECC 自身の故障検出回路に対する監視は？と考えていくと、終わりがありませんよね･･･。どこまで深く検討すべきかは、規格の定める安全度水準（SIL,ASIL,PL など。6.1(5), P.71 参照）によって異なります。鉄道規格では、3 重故障まで考慮するべき場合もあります。

一方、ソフトウェア設計においても、「バグを検出するチェック機構」の搭載が要求されています。データの範囲チェック、実行順序の監視、ソフトウェアを 2 種類のアルゴリズムで実装して結果を比較する方法など、様々です。

最後に、本コラムでは機能安全設計に焦点を当てましたが、それだけでは「安全を担保する構成要素の信頼性」を保証することはできません。高い開発品質・管理品質を伴ってこそ、安全を実現できることを忘れてはなりません。

第5章
ソフトウェア技術者のための セキュリティ設計

セキュリティ対応のコストは、運用段階になると設計段階の 100 倍必要という説もあり、できるだけ早期に対応することが必要です。本章では、セキュリティ対応のプロセスの前段となる脅威の特定、リスク評価及びセキュリティ設計を中心に解説します。

5.1　セキュリティ対応の開発プロセス

機器やシステムに対する脅威としては、盗聴や不正アクセスによる情報漏えいやプライバシー侵害、データやソフトウェア改ざんによる誤動作や予期せぬ停止など、様々なものが想定されます。また脅威によってはセーフティを実現する機能にも影響を与え、事故の発生や顧客の信頼失墜、機器交換・システム改修コストなど、多大な損害も懸念されます。そのため、確実なセキュリティ対応が求められます。

セキュリティ対応のプロセスとしては、まず、守るべき対象や目標を設定します。例えば、重要な情報が漏えいしないこと、ソフトウェアが改ざんされないこと、システムが停止させられないことなどが挙げられます。次に、これらに対する脅威を特定し、その発生しやすさと被害の深刻度からリスクを評価します。この結果、リスクの規模に応じてセキュリティ設計を進めます。

本章では、図 5-1 の流れで、脅威の特定からセキュリティ設計までのプロセスについて、手法を中心に説明します。また、セキュリティに関連する国際規格（評価・認証制度）についても説明します。

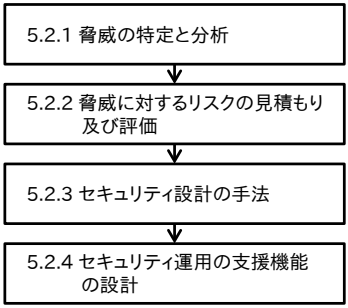


図 5-1　セキュリティ対応の開発プロセス

なお、図 5-2 のように、市場で運用されている段階で脆弱性が発見された場合には機器の交換やシステムの改修などが必要となるため、設計・開発・テスト段階と比較して膨大なコストや手間が必要となります。そのため、できるだけ早期にセキュリティ対応を行うことが必要です［24］。

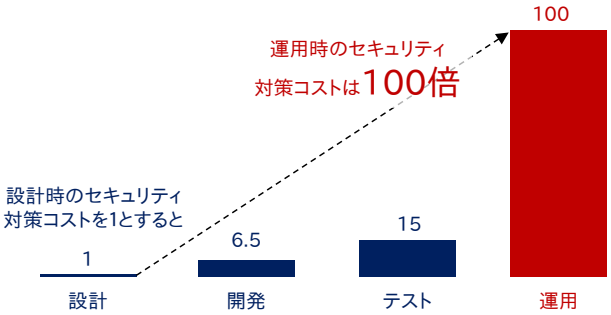


図 5-2　開発工程別のセキュリティ対策コスト

セキュリティ設計に関連する規格としては、工場・プラントなど大規模な制御システム分野では IEC 62443 や、汎用的なコモンクライテリア（CC、ISO/IEC 15408）があり、評価認証制度も実施されておりますが、本書で対象とする自動車や家電などの生活機器分野については検討の途上にあります。そこで本書では、幅広い分野で規格化が進んでいるセーフティ設計の手法の利用も含めて、セキュリティ設計の手法を紹介します。

5.2　セキュリティ設計

5.2.1　脅威の特定と分析

セキュリティ上の「脅威」はセーフティにおける「ハザード」に相当し、事故またはインシデントのような「あってはならない状態」に至る潜在的な要因を指します。脅威の例としては、権限のない者が他のユーザーのパスワードを盗んで機器やシステムを不正利用したり、システムの脆弱性を突いてサービスを停止させたりする攻撃が挙げられます。

攻撃者は、機器やシステムの設計者やユーザーの予想を覆す方法で攻撃してくるため、脅威の特定は容易ではありません。脅威の特定には、ソフトウェアやシステムの構成、攻撃の入口（ネットワーク、ユーザー、他の機器やシステム等）、守るべき情報やサービス（「資産」と呼びます）を明確化することが不可欠となります。それに基づいて、どのような脅威が発生し、どのような事象が引き起こされるのかを想定し、列挙していくことになります。

以下に、脅威の特定と分析に有効な手法を紹介します。(1)と(2)は機器やシステムに対する直接の脅威を想定、それが引き起こす被害の深刻度を追っていく手法、(3)は回避したい深刻な被害を引き起こす脅威を想定して攻撃手段をブレークダウンする手法となります。重要な機器やシステムに対しては、一つの手法だけでなく、手法の組み合わせにより脅威の特定の網羅性を高めることが可能となります。

また、(4)は攻撃者の視点で脅威を特定する手法であり、機器やシステムの特性や利用環境を基に手法を選択します。(5)は脅威に関する情報収集であり、共通的に必要です。

(1)　STRIDE 脅威モデル

脅威は多種多様である上、日々新しい攻撃手法が開発されているため網羅的な整理は困難です。そこでここでは、主要な脅威を整理した STRIDE（ストライド）脅威モデルを説明します。STRIDE は主要な脅威の頭文字を並べたもので、機器やシステムに対してこれらの脅威が存在するかを確認することで、脅威の特定の手掛かりとします。

表 5-1　STRIDE 脅威モデル

項目	英称	概要
なりすまし	Spoofing	コンピューターに対し、他のユーザーを装うこと
データの改ざん	Tampering with Data	権限なしでデータを改ざんし、データの完全性を失わせること
否認	Repudiation	ユーザーがあるアクションを行ったことを否認し、相手はこのアクションを証明する方法がないこと
情報の暴露	Information Disclosure	アクセス権限を持たない個人に情報が公開されること
サービス不能	Denial of Service	正規のユーザーがサーバーやサービスにアクセスできないこと
権限の昇格	Elevation of Privilege	権限のないユーザーがアクセス権限を得ること

出典：Microsoft 社「セキュリティ上の脅威の評価」［25］及び

「Security Planning Through Threat Analysis」［26］を基に作成

(2)　共通攻撃パターン一覧

共通攻撃パターン一覧「CAPEC（ケイペック、Common Attack Pattern Enumeration and Classification）」［27］では、機器やシステムに対する攻撃だけでなく、人の操作を誤らせたり、情報を聞き出したりする手口も含めた攻撃手法が階層的に整理されています。表 5-2 にある最上位カテゴリの攻撃手法と対象から順に当てはめて検討することで、脅威の特定が容易になります。

表 5-2　共通攻撃パターン一覧(CAPEC)の最上位カテゴリ

攻撃手法	攻撃対象
情報収集、資源消耗、注入、なりすまし相互作用、状態遷移操作、機能の悪用、確率的な手法、認証の攻略、権限承認の攻略、データ構造の操作、資源の操作、対象の分析、物理アクセスの獲得、不正コード実行、一部システムの置換、システムのユーザーを操作	ソーシャルエンジニアリング（人） 供給関係 通信 ソフトウェア 物理セキュリティ ハードウェア

出典：CAPEC Web サイト［27］を基に作成

(3)　アタックツリーによる脅威分析

「アタックツリー（Attack Tree）分析」は攻撃者のゴールを設定し、ゴールに至る攻撃手順をツリー状に展開することで脅威の分析を行います。図 5-3 にイメージを示します。

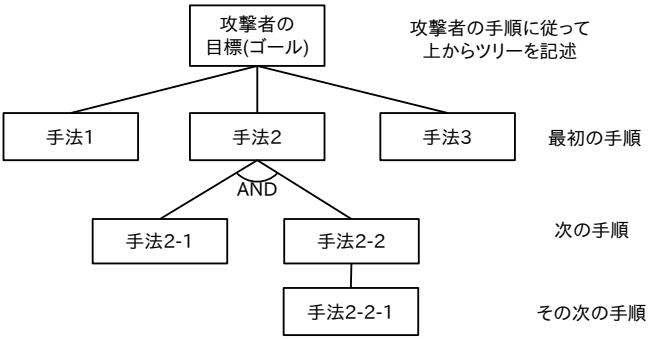
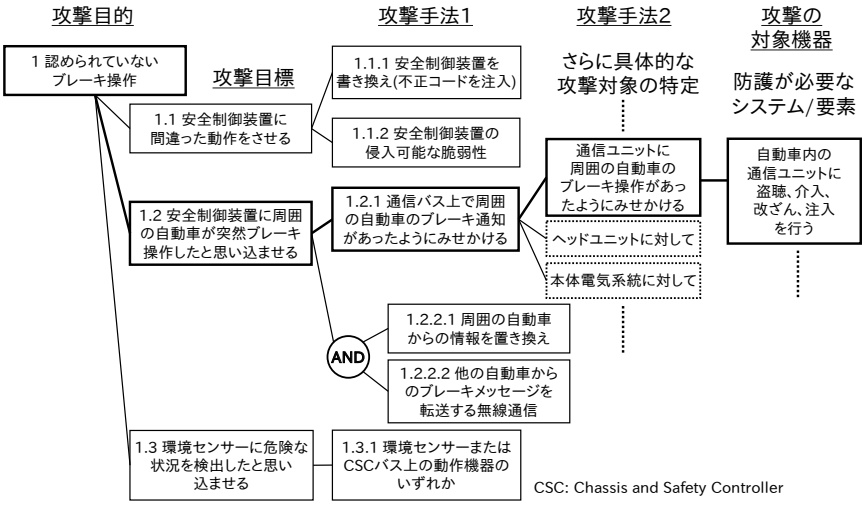


図 5-3　アタックツリーのイメージ

アタックツリー分析では、攻撃者の動機から推定される攻撃目的に対して、目的達成のステップを詳細化していくとともに、想定される手段をすべて記述することで、下方に向かってツリー状に展開していきます。

図 5-4 に、欧州の自動車セキュリティ関連プロジェクト「EVITA」［28］で作成されたアタックツリーの例を示します。図左上”1”にある頂上事象に対して、その脅威・攻撃手法をツリー状に展開しています。図 5-3 のアタックツリーとは構成が異なり、枝葉の末端は、4 章で紹介した FTA と同様に、最初に攻撃対象となる機器を指します。



出典：IPA「自動車の情報セキュリティへの取組みガイド」［29］を基に作成

図 5-4　EVITA における自動車セキュリティのアタックツリーの例(FTA 型)

(4) ミスユースケースによる脅威の特定

攻撃者は設計者が想定していない方法で機器やシステムを攻撃してきます。そこで「ユースケース図（ユーザー視点で利用シーンを想定した図）」に「攻撃者」を追加した「ミスユースケース図」を作成し、攻撃者が対象の機器やシステムに対して攻撃する目的や得ようとする利益を想定することで、脅威を特定します[30]。本手法は、攻撃者の属性を個人や組織に設定したり、金銭や社会的影響などの結果を想定したりすることで、攻撃者の動機を想定しやすくします。

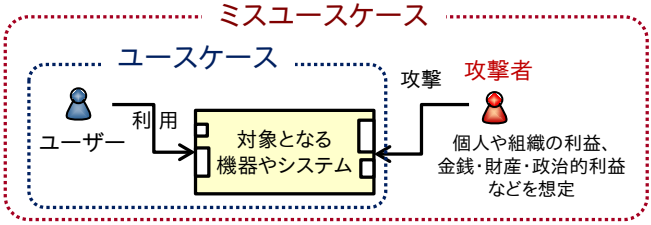


図 5-5　攻撃者からの視点を含めた分析(ミスユースケース図)

(5) 最新の脅威情報の収集と共有

多様化するサイバー攻撃に対応するために、国内外の各分野において情報共有分析センター（ISAC：Information Sharing and Analysis Center)が設立されており[31][32]、最新の脅威情報の収集と共有が行われています。また、米国国土安全保障省（DHS: United States Department of Homeland Security）が運営する脅威対応機関 ICS-CERT（The Industrial Control Systems Cyber Emergency Response Team）や IPA が公表する統計資料やレポート（情報セキュリティ 10 大脅威など）、BlackHat などの国際会議での論文などでも、最新の脅威情報の収集が可能です。今後は生活機器の脅威に関しても、国内外での情報提供が行われることが期待されます。それらの情報を活用することで、機器やシステムに対する最新の脅威の特定が容易になると想定されます。

(6) 脅威の例

本項で説明してきた手法で特定される脅威にはどのようなものがあるのでしょうか。ここでは自動車分野及びスマート家電分野を例に、具体的な脅威を列記します。

表 5-3　自動車分野の脅威の例

No	脅威のタイプ	脅威の例
1	安易な設定	カーナビなどへの容易に推測できるパスワードの設定など
2	ウイルス感染	USB 経由によるカーナビへのウイルス感染、異常動作など
3	不正利用	遠隔車両管理システムの悪用による自動車の使用停止など
4	不正設定	整備ツールによる車両設定の不正変更など
5	情報漏えい	カーナビ上の個人情報の漏えいなど
6	盗聴	車載機とサービスセンター間の通信の盗聴など
7	サービス停止	無線妨害によるスマートキーの施錠不能など
8	偽メッセージ	交通システムの乗っ取りによる偽の交通情報提供など
9	ログ喪失	ドライブレコーダー上のデータ消去など
10	不正中継	スマートキーの無線通信の不正中継による解錠など
11	否認	ユーザーによる車両設定の変更及びその行為の否認など
12	権限の昇格	権限がない者による保守用イベントデータレコーダー（操作や車両動作の履歴記録装置）のデータ取り出しなど

表 5-4　スマート家電分野の脅威の例

No	脅威のタイプ	脅威の例
1	安易な設定	エアコンなどへの容易に推測できるパスワードの設定など
2	ウイルス感染	宅内ルーターのウイルス感染及び不正な通信の中継など
3	不正利用	宅内カメラへの不正アクセスによるのぞき見など
4	不正設定	遠隔からの録画設定の不正変更
5	情報漏えい	スマートメーターの電力データ漏えいによる生活パターンの把握など
6	盗聴	ヘルスケアデバイスの無線通信の盗聴による健康データの詐取など
7	サービス停止	ガスメーターの不正操作繰り返しによる電池消耗及びメータ停止など
8	偽メッセージ	家庭向け情報サービスのデータ改ざんによる偽メッセージの表示など
9	ログ喪失	家電への不正アクセス後のログ消去による痕跡喪失など
10	不正中継	家に近づくとエアコンを ON にするウェラブルデバイスの無線の不正中継による家電不正操作など
11	否認	家電への従量制課金サービスの利用の否認など
12	権限の昇格	子供によるペアレンタル設定の解除、親から禁止された操作の実行など

5.2.2　脅威に対するリスクの見積もり及び評価

脅威が特定されたら、その脅威によって被害に至る状況を分析し、発生しやすさと被害の深刻度を明らかにします。例えば、駐車場や宅内に立ち入って、機器に結線して行うような攻撃は、インターネット経由の攻撃と比較して目撃される可能性が高いため、攻撃者にとって行いにくい（発生しにくい）といえます。また、機器やシステムのセーフティ機能に誤動作を起こさせる攻撃と、温度や湿度などの計測データを盗聴する攻撃では、被害の深刻度が異なります。

つぎに、発生しやすさ（現実の発生頻度、難易度、攻撃者の利益などから判定）と被害の深刻度からリスクを見積もり、許容可能なレベルかを評価します。以下で、具体的なリスク評価手法を説明します。

(1)　ハザード分析手法を利用したリスク評価

リスク評価には、4章で紹介したFTA、FMEA、HAZOPなどのセーフティの手法を利用することが可能です。例えばFTAでは故障や事故などの「事象」が発生する原因をツリー構造で分析しますが、「事象」を「脅威」に置き換え、ツリーの過程にある事象に「発生確率（年間に発生する頻度など）」を割り当てて計算することで、脅威の発生しやすさを求めることができます［33］。この値と被害の深刻度からリスクの見積もりが可能となります。

(2)　CVSSによる脆弱性のリスク評価

CVSS(Common Vulnerability Scoring System）は、情報システムの脅威の原因となる「脆弱性」の「被害の深さ」や「攻撃のしやすさ」などから「被害の深刻度」を同一の基準の下で定量化する手法です［34］。発生のしやすさと定量化された深刻度から、リスクの見積もりが可能となります。CVSSは専用の計算式を使用することで単一の指標を導き出せるという簡潔さが利点です。CVSSの計算式は既存の脆弱性情報の蓄積を基に重み付けされており、CVSS v2（バージョン2）では、CVSS基本値4未満が深刻度「注意」、4以上7未満が深刻度「警告」、7以上が深刻度「危険」と区分しています。CVSSはITU X.1521で国際標準化され、世界中で30以上の脆弱性情報提供サイトにおいて脆弱性を示す指標として採用されています［35］。

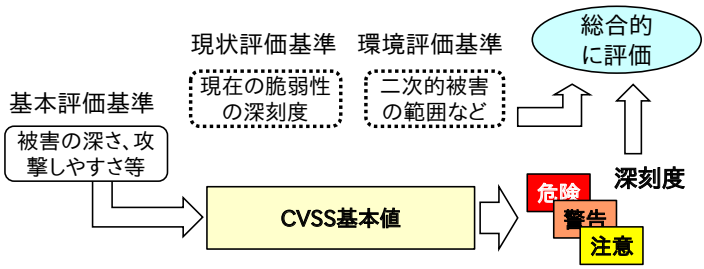


図 5-6　CVSS における脆弱性の深刻度評価のイメージ

(3)　脅威に対するその他のリスク評価手法

その他にも、MASG(Advanced Misuse Case Analysis Model with Assets and Security Goals) [36], ゴール指向要求分析法(KAOS 手法など) [37]、i*(アイスター)フレームワーク [30] [38]、Secure Tropos(セキュアトロポス) [30] [38] などの手法が研究されています。

なお、2015 年 3 月には公益社団法人自動車技術会が「自動車の情報セキュリティ分析ガイド」を公表しています。本項で紹介した CVSS を応用した分析方法などを紹介しており、他分野においてもリスク分析手順として参考となります。

5.2.3　セキュリティ設計の手法

(1)　セキュリティ対策の考え方

1 章の図 1-6(P.10)でも示したとおり、リスク評価の結果に基づいて、

・リスクが非常に大きい場合は、開発取りやめを含めた「リスクの回避」
・リスクが充分に小さい場合は、対応しないことによる「リスクの保有」
・被害は深刻であるが発生可能性が低い場合は、保険や外部委託による「リスクの移転」

といった対応を行い、上記以外の場合にはセキュリティ設計などにより「リスクの低減」を図ります。ただし利便性とセキュリティはトレードオフの関係にあり、例えば機器やシステムのユーザー認証機能を強化すればユーザーの手間が増えるという課題があるため、配慮も必要です。

セキュリティ上の脅威がセーフティ機能に影響を与える可能性を考慮すれば、経営層が関与して、前述の判断の基となる基本方針を定めておくことが必要です。

また、セーフティとセキュリティの対策が重複したり、矛盾したりすることのないよう、両者の要求仕様のすり合わせを行う仕組みも必要となります。

4章の表 4-8(P.45)に示したフールプルーフやフォルトトレランス、多層防御などの考え方もセキュリティ対策に有効です。具体的には、ユーザーに生活機器のセキュアな管理は行えないという前提で機器内の情報やユーザー権限を最小限に抑えたり、膨大な不正なアクセスが集中しても機器やシステムの機能を最低限、維持したり、複数のセキュリティ機能を施すことで攻撃を成功させないといった考え方で対策を行います。

(2) セキュリティに有効な設計手法

4章の表 4-9、表 4-10(P.46)に示した設計品質を高める手法や機器やシステムの安全性を高める仕組みはセキュリティ設計にも有効です。具体的には、形式手法によりあいまいさを除去した設計を行ったり、領域分割により機器がウイルス感染しても被害を最小限にとどめたり、多重化により機器やシステムの可用性(必要なときに利用できること)を高めることが可能です。

また、通常の使用では事故に至ることのないソフトウェア上の欠陥が、意図的な攻撃者の糸口になることもありますので、セキュリティ設計においては攻撃を防ぐ観点での設計が必要となります。表 5-5 にセキュリティ設計に有効な設計手法の例を示します。

表 5-5 セキュリティ設計に有効な設計手法の例

手法	概要
ソフトウェア品質向上設計	脆弱性を低減するために、セキュアプログラミング、セキュアコーディング、コードの静的解析、脆弱性評価などを開発工程に組み入れる［39］
セキュリティフレームワークの活用	効率的にセキュリティ機能を実現するため、あらかじめセキュリティ対策手法や機能が組み込まれた開発ツールやパーツの採用を検討する
プログラミング言語	厳密な型検査や副作用の排除、宣言的で簡潔な技術を強制するような、脆弱性が生じにくいプログラミング言語を検討する
形式手法	特に高いセキュリティを必要とする場合には、設計内容が要件を満たすことを論理的に検証できる形式手法を検討する

(3) セキュリティレベルの指標

セキュリティにおける指標の例としては、コモンクライテリアの評価保証レベル EAL(Evaluation Assurance Level)が挙げられます（表 5-6)。例えば、パスポートに内蔵するスマートカード(IC カード)には「EAL4」に脆弱性試験を追加した「EAL4+」という高度な評価保証レベルが要求されます［40]。一方、オフィスや一般家庭、コンビニエンスストアなどで利用されるコピー・プリンタ複合機の場合は、不特定な利用者が利用できる環境を想定した「EAL3」が要求されます［41]。このようなセキュリティにおける指標を設定することで、製品の調達者と納入者でセキュリティレベルの合意が容易になります。

表 5-6　コモンクライテリアにおけるセキュリティ機能の評価保証レベル(EAL)

EAL	保証要求内容	想定されるセキュリティ保証レベル
EAL1	機能テスト	クローズドな環境での運用を前提に安全な利用や運用が保証された場合に用いられる製品の保証レベル
EAL2	構造化テスト	利用者や開発者が限定されており、安全な運用を脅かす重大な脅威が存在しない場合に用いられる保証レベル
EAL3	方式的テスト、及びチェック	不特定な利用者が利用できる環境、不正対策が要求される場合に用いられる製品の保証レベル
EAL4	方式的設計、テスト、及びレビュー	商用機器やシステムにおいて高度なセキュリティ確保を実現するために、セキュリティを考慮した開発と生産ラインを導入して生産される製品の保証レベル
EAL5	準形式的設計、及びテスト	特定の分野の商用製品・システムにおいて、最大限のセキュリティ確保をするためにセキュリティの専門家の支援により開発、生産された製品の保証レベル
EAL6	準形式的検証済み設計、及びテスト	重大なリスクに対抗して高い価値のある資産を保護するために、開発環境にセキュリティ工学技術を適用して開発された特別性の製品の保証レベル
EAL7	形式的検証済み設計、及びテスト	非常にリスクが大きい環境や高い開発費用に見合う資産を保護するために開発された製品の保証レベル。

出典：IPA ISO/IEC 15408 IT セキュリティ評価及び認証制度パンフレット(2014 年 4 月版)を基に作成

(4) セキュリティ対応の要素技術

攻撃者は、様々な情報、技術、ツールを駆使して攻撃してきますので、セキュリティ対応も、様々なセキュリティ要素技術を組み合わせて対応することが必要

となります。具体的には、耐タンパー性や暗号化のように攻撃から対象を守る技術、認証や電子署名のように真正性を確認する技術、ログ・監視や侵入検知のように攻撃を発見する技術などを組み合わせ、セキュリティを確保します。表 5-7 に要素技術の例を示します。

表 5-7　セキュリティ要素技術の例

技術名	概要	対応する脅威例
耐タンパー性	機器に格納されたソフトウェアや暗号鍵データを解析されないように、こじ開けられると自動的にメモリを消去したり、漏えい電磁波や電力消費量の測定による解析を防ぐ特殊な回路を追加したりすることで、攻撃への耐性を高める	機器に格納されたソフトウェアを読みだされ、コピー製品を作られることを防ぐ
暗号化	機器に格納したデータや機器間で送受信するデータを暗号化し、不正に読みだされたり盗聴されたりした場合でも情報漏えいを防ぐ	生活機器で測定した個人のデータが送信中に盗聴され、プライバシーが侵害されることを防ぐ
認証	正規のユーザー、サーバー、機器などの真正性を確認することで、なりすましによる不正利用や機器・部品の不正な入れ替えを防ぐ	所有者でない者が勝手に機器を利用することを防ぐ
アクセス制御	認証されたユーザーの権限の範囲で、機器やシステムの利用を認可する	子供が親の許可なしで有料サービスを利用しないよう、ペアレンタル機能で制限する
電子署名	ソフトウェア更新用ファイルなど重要なデータに電子的な署名を付与することで、ファイルの真正性や完全性（改ざんされていないこと）を確保する	偽のソフトウェア更新ファイルの送りつけによるウイルス感染を防ぐ
侵入検知	機器やシステムへの不正な侵入、実行中のメモリまたはソフトウェアの改ざんなどをリアルタイムで検知する	ネットワーク経由で機器に不正アクセスされた場合、即時に検知して遮断する
ログ・監視	機器やシステムへのアクセス記録を蓄積・分析し、攻撃回数の統計などを作成することで、万一侵入された場合の被害や攻撃元を明らかにする	不正アクセスのログを分析し、攻撃元や攻撃が成功した原因を特定し、対策する

なお、組込みシステムのセキュリティ対策に関しては、「組込みシステムのセキュリティへの取組みガイド（2010 年度改訂版）」［42］、「自動車の情報セキュリティへの取組みガイド」［29］などが参考となります。

5.2.4　セキュリティ運用の支援機能の設計

(1)　セキュリティ更新機能の必要性

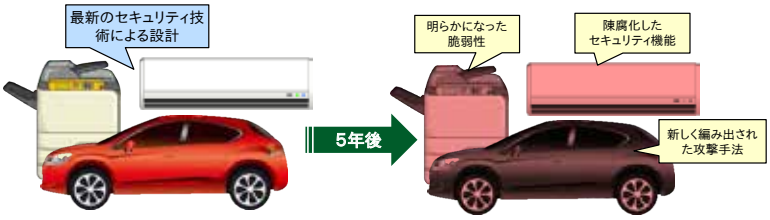


図 5-7　セキュリティ設計の陳腐化

生活に関わる機器やシステムは5～10 年利用するものも珍しくありません。開発時には最新技術を用いてセキュリティ設計を行ったとしても、製品化後に月日が経過するほど、新たな脆弱性の発見、攻撃者による新たな手法の開発、技術進歩に伴う搭載されたセキュリティ技術の陳腐化などにより、急速に脆弱化していくことが想定されます。また攻撃者は、脆弱性が明らかになると一斉に攻撃してきます。このため、今後のセキュリティ設計においては、経年による脆弱化に対して迅速に対応できるセキュリティ設計が重要です。

(2)　セキュリティ更新機能の設計

経年による脆弱化に対して、機器を交換したり、サービスセンターで預かったりしてセキュリティ機能を更新するのでは、コストも手間も要します。これに対しては、パソコンのようにセキュリティ更新用のソフトウェアやデータをネットワーク経由で配布し、機器やシステム側で自動更新する方法が有用です。カーナビなど一部の機器では、USB メモリや SD カードを挿入経由や、無線ネットワーク経由でソフトウェア機能や地図データの更新が行われていますので、セキュリティ更新用ソフトウェアについても同様に更新可能であると想定されます。

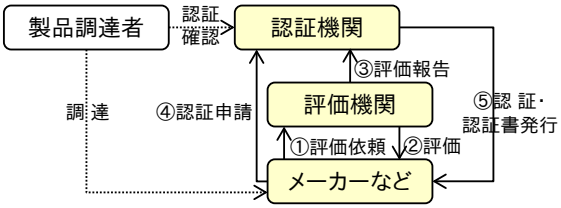
ただしこの場合、ソフトウェアの更新作業を悪用した攻撃、例えば、機器をネットワークに接続した際のウイルス感染、なりすましたサーバーからの偽の更新データのダウンロード、更新用データの改ざん・送り付けなどへの対応が必要となります。また、攻撃を防げずに不正な更新が行われた場合でも、ソフトウェアの異常な動作を検知したり、更新をバックデートしたりする仕組みの組込みも必要です。

5.3　セキュリティ設計の評価・認証

セキュリティ対応が適切に行われていることを客観的に評価する仕組みとしては、企業や組織の情報セキュリティ管理体制などのマネジメントを対象とする認証制度と、機器やシステムの設計や実装を対象とする認証制度があります。後者には、製品や機器のセキュリティ機能を対象としたコモンクライテリア認証、暗号モジュールを対象とした CMVP(Cryptographic Module Validation Program)認証、制御機器を対象とした EDSA(Embedded Device Security Assurance)認証などがあり、規格に基づいたセキュリティ機能の設計や実装を保証しています。

(1)　コモンクライテリアによる第三者認証制度

コモンクライテリアは、情報セキュリティの観点から、情報技術に関連した機器やシステムが適切に設計され、その設計が正しく実装されていることを評価するための国際規格です［43］。調達側が分野別にセキュリティ要件をとりまとめたプロテクションプロファイル（PP）または開発側が機器やシステムのセキュリティ要件をとりまとめたセキュリティターゲット（ST）に適合しているかを評価機関が評価し、認証機関が認証します。調達者は認証機関の Web サイトで認証された機器を確認することができます。（メーカー等が公開を希望する場合）



出典：IPA「IT セキュリティ評価及び認証制度」［43］を基に作成

図 5-8　コモンクライテリア認証のスキーム

本認証制度で、評価・認証された機器やシステムは国際協定に基づき加盟国においても有効と認められます(CCRA: 国際承認アレンジメント［44］)。認証機関の Web ページにはコピー・プリンタ複合機分野で認証を取得している製品が多数掲載されています。なお、2014 年に新たな協定が発表され、加盟各国の政府調達における本制度活用促進のため、USB などの暗号化ストレージやモバイルデバ

イスなど、製品タイプごとの cPP（Collaborative Protection Profile）[45]が順次、作成されています [46]。

(2) 脆弱性評価

セキュリティに対応したソフトウェア開発においては、セキュリティ設計が正しく実装されているかを確認するだけでなく、図 5-9 のような方法で脆弱性を評価することが重要です。

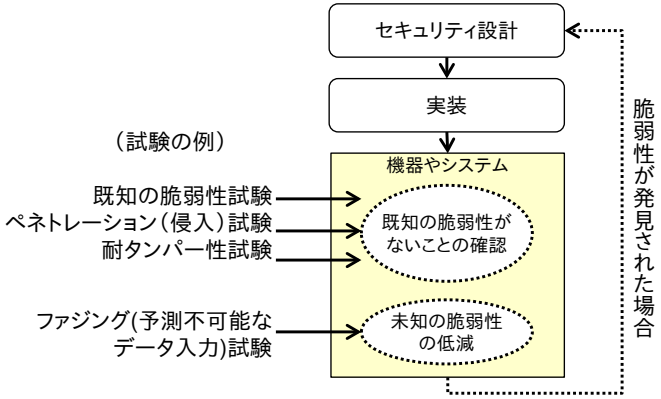


図 5-9　脆弱性評価のイメージ

セキュリティに対応したソフトウェア開発の評価段階では、特定の脆弱性が取り除かれているかを確認します。具体的には、「SQL インジェクション」や「ログイン機能の脆弱性」など、基本的かつ重要な既知の脆弱性 [47]がないことを確認します。製品の用途に応じて、特定の侵入攻撃手法を再現するペネトレーション試験や耐タンパー性試験も行います。

また、製品に不具合を起こしそうなデータの入力を繰り返すブラックボックス的な試験として「ファジング試験」があります。本試験は多数の試験データを自動的に生成するツールにより行います [48]。EDSA など一部の認証規格では通信ロバストネス（堅牢性）の試験が要求されており [49]、その試験として、ファジング試験が行われます。

なお重要なシステムについては、製品出荷後においても新たな脅威や攻撃手法が登場するたびにリスク評価を行い、必要に応じてリスクの回避方法を周知したり、製品を改良したりするなどの対応が必要です。

コラム4 コモンクライテリアと形式手法

セーフティでは電子機器の機能安全に関する国際規格 IEC 61508 に基づく認証取得が広まっています。1 時間あたりの故障発生率に基づき 1 から 4（数値が高い方が信頼性が高い）の SIL が定義されており、SIL2 以上においては、形式手法の採用が推奨されています。セキュリティにおいても ISO/IEC 15408 に基づくセキュリティ機能が実現されていることを確認する評価保証レベルとして 1 から 7 の EAL が定義されており、コモンクライテリアとして知られています。EAL5 以上においては、形式手法の使用が保証要件として規定されています。形式手法は、数学を基盤としたソフトウェア工学におけるソフトウェア及びハードウェアシステムの仕様記述、開発、検証の技術です。セキュリティ要件は命題(不変条件)として書くことができ、形式手法は命題を証明するために有効な手法です。形式手法の手法、記法、ツールは、適応対象が広がるにつれ多くのものが開発され、目的にあわせて使われてきています。

IPA では、これから形式手法を導入される方のために、以下のような入門者用、導入者用の資料を公開しています。

- 形式手法導入課題を解決する「形式手法活用ガイドならびに参考資料」
- 実務家のための形式手法 教材「厳密な仕様記述を志すための形式手法入門」
- 「厳密な仕様記述における形式手法成功事例調査報告書」

またソフトウェアの信頼性を高めるための取り組み事例集である「先進的な設計・検証技術の適用事例報告書」にも下記のような文献を掲載しています。

表題	事例提供元	記述言語
形式手法を用いたセキュリティ検証	アーク・システム・ソリューションズ(株)	Event-B
宇宙システムにおける上流工程仕様の妥当性確認技術	宇宙航空研究開発機構(JAXA)	SpecTRM, SPIN
モデル検査の適用による上流工程での設計の誤り	(株)東芝	Promela, SPIN
モデル検査とテストによる車載オペレーティングシステムの検証	北陸先端科学技術大学院大学	Promela, SPIN
通信制御ソフトウェア開発における状態遷移設計の品質向上への取り組み	富士通(株)	Promela, SPIN
仕様記述言語 VDM++ を用いたシステムの仕様の記述	フェリカネットワークス(株)	VDM++
形式仕様記述手法を用いた高信頼性を達成するテスト手法とその実践	フェリカネットワークス(株)	VDM++

コラム5 インシデント対応の勘所

富士通株式会社
奥原 雅之さん

事業運営に影響を与えたり、情報セキュリティを脅かしたりする事件や事故のことを一般に「セキュリティインシデント」と呼びます。例えば情報システムに対する外部からの攻撃の発生、コンピューターウイルスへの感染、情報システムや製品におけるセキュリティホールの発見などはいずれもセキュリティインシデントとなりえます。セキュリティインシデントが発生したときは、それによる被害を最小限に留めるために、事態を適切に、かつ迅速にコントロールする必要があります。

インシデント発生時にまず実施しなければならないのが被害拡大の防止です。限られた時間の中で必要な情報を収集し、的確な被害拡大防止の対策を取ります。状況によってはシステムの停止、製品の回収など、多くのコストを掛ける決断をしなければなりません。このような決断を素早く行うことができるように、事前に関係者による緊急対応方針を決めておくことが非常に重要です。

続いて行うのがインシデント状況からの回復です。インシデントの原因となった脅威や問題点を根本的に除去します。このための原因調査にある程度の時間が必要になります。インシデントの脅威が去ったら、インシデントの詳細な分析と関係者への報告を行います。そして、その結果を知識として整理し、次のインシデント防止に役立てます。

このようなセキュリティインシデント対応の中心になるのがセキュリティインシデント対応チーム CSIRT(シーサート)または ISIRT(アイサート)です。普段からこのようなチームを組織内で準備しておくことで、インシデント対応をより的確かつ素早く行うことができます。

以下にインシデント対応のためのガイドライン、及びセキュリティインシデント対応チーム設立に関する参考情報を例示します。

ISO/IEC 27035:2011	Information technology -- Security techniques -- Information security incident management
ISO/IEC 29147:2014	Information technology -- Security techniques -- Vulnerability disclosure
ISO/IEC 30111:2013	Information technology -- Security techniques -- Vulnerability handling processes
JPCERT コーディネーションセンター	https://www.jpcert.or.jp/

第6章
ロジカルな設計品質の説明

対象となる機器やシステムについて、なぜその設計で目標が達成されるかを、事実（証拠）に基づき、論理的かつ第三者でも容易に理解できる表記で説明する手法を「設計品質の見える化」と呼びます。これはセーフティとセキュリティの設計においても有用です。

見える化の一手法である「アシュアランスケース」は、一部の業界規格や国際規格の認証において要求されるほか、設計開発の現場でも複雑な設計情報を共有する手段として活用され始めています。

6.1　ソフトウェアの設計品質の見える化

ソフトウェアの設計内容について社内や発注先のレビューを受けたり、新製品開発のためにソフトウェア資産を再利用したりするときには、設計に関するドキュメントが必須です。このドキュメントは、第三者でも分かりやすい表記であるだけでなく、その設計によって目標（ゴール）が達成されることが、事実（証拠）に基づき、論理的（ロジカル）に説明されていることが必要です。これにより、第三者への「設計品質」の説明・共有や過去の設計の理解が容易になります。

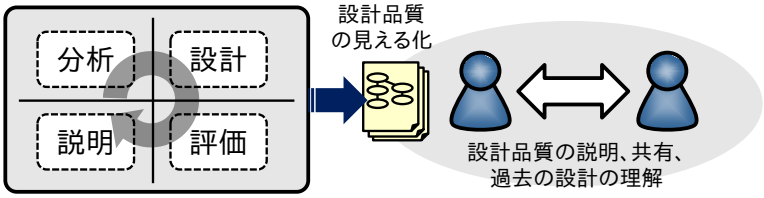


図 6-1　ソフトウェアの設計品質の見える化

このようなソフトウェアの「設計品質の見える化」により、次に示すような効果が期待されます。

(1)　ソフトウェアの再利用時の設計内容確認

製品の新規開発やバージョンアップにおいて既存製品のソフトウェアや汎用のライブラリなどを利用する場合、設計内容を確認するために「見える化」されたドキュメントの活用が有用です。特にセーフティとセキュリティの設計においては、再利用するソフトウェアのセーフティとセキュリティの設計の前提、過程、根拠などを確認し、利用可能な部分を流用することで効率化を図ることができます。

(2)　ステークホルダーとの設計品質の合意

機器やシステムの設計を行う際には、その設計によって目標が達成されるか、設計における検討プロセスは適切であるかなどについて、必要に応じてステークホルダー（関係する開発部門、品質管理部門、受発注企業など）に説明する必要があります。その際に設計情報を共有する手段が必要となります。

特にセーフティとセキュリティの設計においては、重大なリスクへの対応について経営層に説明し、理解及び納得いただくことが必要です。そのため、第三者でも分かりやすく、事実（証拠）に基づいて論理的に設計品質を説明できる「見える化」されたドキュメントが有用です。

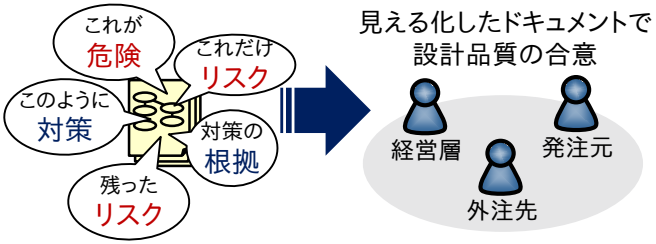


図 6-2　経営層、発注元、外注先との設計品質の合意

(3) トレーサビリティ、説明責任

機器やシステムに問題が発生した場合、ドキュメントなどを基に設計の履歴や検討経緯などを追跡し（トレーサビリティ）、早急に原因を究明する必要があります。また、設計上の欠陥の有無を明確にし、ユーザーや関係者に説明する責任も生じます（説明責任）。この際に「設計品質の見える化」のドキュメントが有用となります。事故が発生してから慌てて設計書を参考にドキュメントを作成するのでは、緊急対応には間に合いませんし、設計品質のエビデンスとしても不充分です。機器やシステムの設計時に見える化を行うことが重要です。

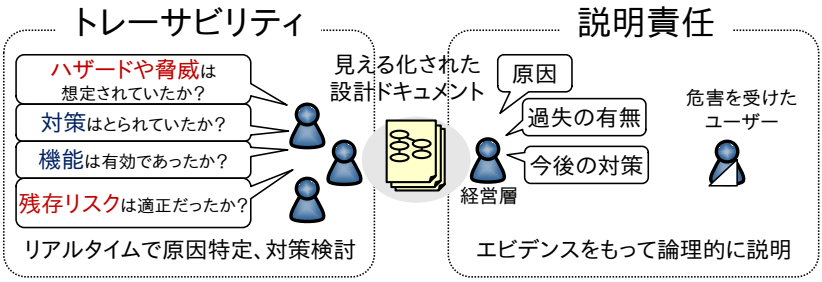


図 6-3　問題発生時の設計品質の説明、共有

(4)　第三者認証、国際規格の取得

業界規格や国際規格に基づいて特定分野の製品を認証するスキームがあります。製品が規格に準拠していることを評価機関が評価したり、規格の要求事項に適合している製品として認証機関が認証・登録したりします。ユーザーである政府や企業は、認証の有無を参考としたり、調達条件としたりすることで、自らが評価することなく信頼できる製品の調達が可能となります。「設計品質の見える化」は、評価機関に製品が規格に準拠した設計であることを説明する際に有用です。

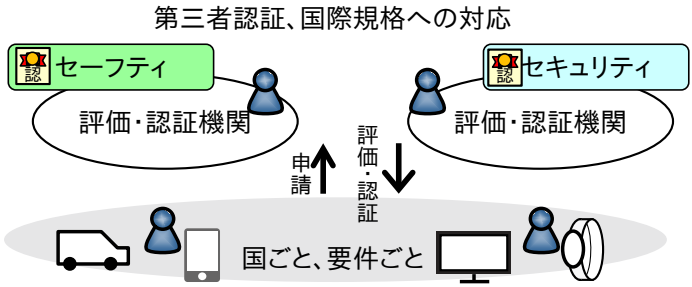


図 6-4　第三者認証、国際規格への対応

自動車やヘルスケア分野にはセーフティに関する国際規格があり、現在、セキュリティの追加も検討が進んでいます。なお、国際規格の一部は日本国内で認証を受ければ協定を締結した国でも有効となる認証スキームがありますが、国や地域ごとに評価・認証が必要となる規格も多いため、国際的に通用する手法で設計の見える化を行うことが有用です。

(5)　国際規格におけるセーフティとセキュリティの様々な尺度

表 6-1 に、国際規格で使用されているセーフティとセキュリティの対応レベルを表す尺度を示します。業界毎に異なる尺度や、同じ尺度でも定義が異なるものを使用していることが分かります。現在、IEC 62061(SIL) と ISO 13849-1(PL) など、一部の規格ではセーフティの尺度の一本化に向けた動きも見られます。来るべき“つながる世界”に向けて、異なる分野の機器間においてもセーフティとセキュリティの尺度を適用できるよう、検討が進むことが期待されます。

表 6-1　国際規格で用いられる尺度の例

規格／規格群	適用先の例	尺度	備考
セーフティ			
ISO 10218-1	産業用ロボットとデバイス	PL／SIL	尺度としては、PL(ISO 13849-1)と、SIL（IEC 62061）を参照
ISO 13482	生活支援ロボットとデバイス	PL／SIL	尺度としては、PL(ISO 13849-1)と、SIL（IEC 62061）を参照
ISO 13849-1	機械装置向けの安全関連の電子制御システム	PL	IEC 62061 の SIL との相互関係が定義されている
ISO 25119	農業用トラクタと機械	AgPL	予見できる状況でのセーフティ関連部品の性能を示す5段階のレベル
ISO 26262	車載向けの安全関連の電子制御システム	ASIL	ASIL は、ISO 26262 固有の尺度
IEC 61496	機械装置向け安全関連の電気的検知保護設備	タイプ	タイプ別に SIL／PL を対応させている
IEC 61508	産業分野全般の安全関連の電子制御システム	SIL	IEC 61508 は、機能安全に関する基本規格の位置づけ
IEC 61511	プロセス産業向けの安全計装システム	SIL	IEC 61508 の SIL と同様
IEC 62061	機械装置向けの安全関連の電子制御システム	SIL	IEC 61508 の SIL と類似だが厳密には定義が異なる
IEC 62304	医療機器ソフトウェアのライフサイクルプロセス	クラス	ソフトウェアシステムが誘発するハザードの重大さに基づく尺度
セキュリティ			
ISO/IEC15408	IT 製品や情報システム	EAL	製品や設計文書の評価項目の数と種類に応じた尺度。現在規格の改訂に向け議論中の模様
IEC 62443	産業用オートメーションシステム及び制御システム	SL	制御システムの、運用管理、システム、装置の全般をカバーし、一部完成、一部開発中

PL：Performance Level, SIL：Safety Integrity Level, AgPL: Agricultural Performance Level, ASIL: Automotive Safety Integrity Level, EAL：Evaluation Assurance Level, SL：Security Level（表内登場順）

本項で説明した設計品質の見える化の手法として「アシュアランスケース」があります。次項では、具体的な表記法も含めて紹介します。

6.2 アシュアランスケースについて

(1) アシュアランスケースとは

1988 年に北海油田「Piper Alpha」で火災が発生し、167 名が死亡する事故がありました［50］。本油田では運用に関する規範は定められていたものの、安全を確保する仕組みが不充分であったり、現場での情報伝達がうまくいかなかったりしたため、最悪の結果を招いてしまったとされています。この反省として、機器やシステムの安全性について規範や手順を定めるだけでなく、それらにより安全性を確保できることを、分かりやすく、論理的かつ事実に基づいたエビデンスで説明する「セーフティケース（Safety Case）」が英国 HSE(Health and Safety Executive)で導入されました［51］。同様のアプローチは、セキュリティやその他の分野にも導入されており、セキュリティの確保の場合はセキュリティケース、ディペンダビリティの確保の場合は「ディペンダビリティケース(Dependability Case)」と呼び、それらを総称して「アシュアランスケース(Assurance Case)」と呼んでいます。現在では、表 6-2 にあるように、複数の規格やガイドラインにおいてアシュアランスケースが要求されるようになりました。

表 6-2　アシュアランスケースを求める規格やガイドラインの例

分野	アシュアランスケースを要求する規格やガイドラインの例	概要
航空	Safety Case Development Manual（EUROCONTROL：The European Organization for the Safety of Air Navigation）［52］	航空管制の安全管理に関するセーフティケース作成のガイドライン
鉄道	The Yellow Book（英国 Rail Safety and Standards Board Ltd.）［7］	英国における鉄道信号システムの安全性の保証
軍事	Defence Standard 00-56（MoD：英国国防省）［53］	英国国防省の、防衛システムの安全管理システムに関する規格
自動車	ISO 26262（ISO：国際標準化機構）［54］	自動車の機能安全の規格
医療機器	Infusion Pumps Total Product Life Cycle / Guidance for Industry and FDA Staff（FDA：米国 Food and Drug Administration / Infusion Pump Improvement Initiative）［55］	医療機器の輸液ポンプに関するガイドライン

(2) アシュアランスケースの表記法

「アシュアランスケース」の基本的な記述に関しては ISO/IEC 15026-2 に規定があり、表記は人が日常的に使用する自然言語で記述します。また表 6-3 に示すようなグラフィカルなアシュアランスケースの表記法の利用が広がっており、これらを使うことにより主張する内容や根拠、その関係を図形や矢印を使ってわかりやすく表現できます。

表 6-3　グラフィカルなアシュアランスケースの表記法一覧

表記法 / 特徴	CAE	GSN	D-Case
正式名称	Claim, Argument, Evidence	Goal Structuring Notation	Dependability Case
登場時期	1998 年	2011 年	2012 年
構成要素	3 種類 （主張、議論、証拠）	6 種類 （次頁表 6-4 参照）	GSN を拡張（モニタ、パラメータ、アクション、外部接続、説明責任）
開発組織	英 Adelard 社、ロンドン大学	英ヨーク大学	日 DEOS プロジェクト

CAE は主張(Claims)、議論(Arguments)及び証拠(Evidence)の 3 要素で表現することにより簡潔化及び効率化を図った表記法です [56]。GSN は ISO 26262 などの規格において根拠資料となるアシュアランスケースに使用されている表記法です [57]。D-Case は GSN をベースにディペンダビリティを保証するための記述を行うために拡張された表記法です。D-Case を開発した一般社団法人ディペンダビリティ技術推進協会(DEOS 協会)D-Case 部会は、GSN も表記できる D-Case エディターを公開しています [58]。また、アシュアランスケース表記法のメタモデルとして SACM(Structured Assurance Case Metamodel)が OMG で標準化されており [59]、CAE, GSN 等で表現したアシュアランスケースを、SACM 形式の属性表記を経由して変換することが可能です。

表記法の例として、表 6-4 に GSN の構成要素を示します。

表 6-4　GSN の構成要素

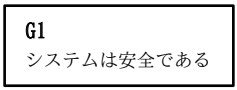
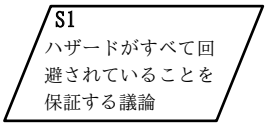
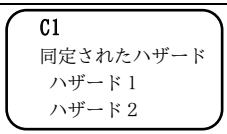
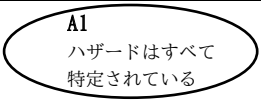
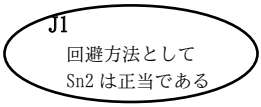
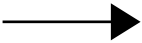
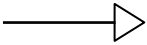
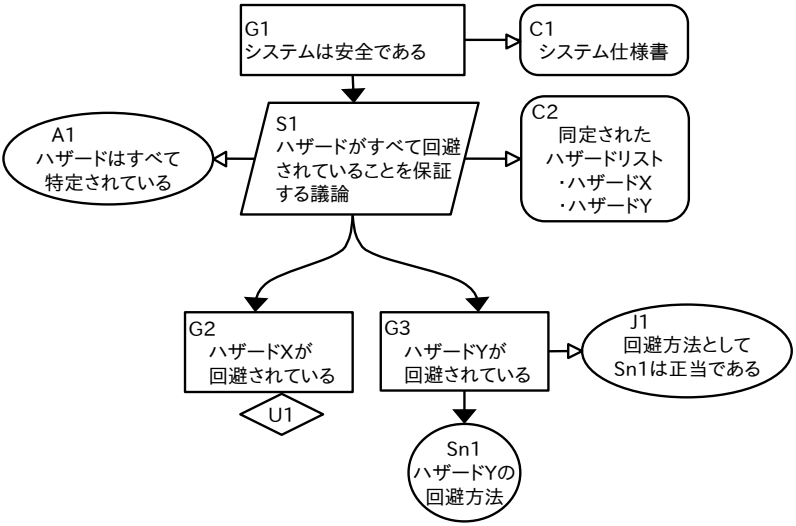
構成要素	説明	表記例
ゴール (Goal)	保証したいこと（議論の主張）、ゴールはさらに詳細なゴール（サブゴール）に分解される	
ストラテジ (Strategy)	ゴールとそれをサポートするサブゴールの間に存在する推論、サブゴールに分割する時の考え方	
コンテキスト (Context)	前提となる事実、情報や発言なども表せる	
ソリューション (Solution)	ゴールが成り立つことを最終的に保証するもの、具体的な証拠	
アサンプション (Assumption)	特定の主張か戦略が基づく有効な前提	
ジャスティフィケーション (Justification)	特定の主張か戦略を適用した理由か、その正当性	
アンデベロップド (undeveloped)	議論の流れでまだ展開されていない要素を表す。ゴール、ストラテジにつけることができる	
サポートリンク (SupportedBy)	黒矢印で表し、ゴールからゴール、ゴールからストラテジ、ゴールからソリューション、ストラテジからゴールで利用可能	
コンテキストリンク (InContextBy)	白矢印で表し、ゴールからコンテキスト、ゴールからアサンプション、ゴールからジャスティフィケーション、ストラテジからコンテキスト、ストラテジからアサンプション、ストラテジからジャスティフィケーションで利用可能	

図 6-5 に GSN の表記例を示します。図のように要素毎に枠の形状が決まっており、内部に自然言語で記述し、流れに沿って線で結合することで、設計における議論や論証を第三者でも分かりやすい形で表記することができます。



出典：(独) 産業技術総合研究所 セーフティとセキュリティ規格の同時認証方法論について [57]、及び Origin Consulting 社(GSN Working Group)「GSN COMMUNITY STANDARD VERSION 1」 [60]を基に作成

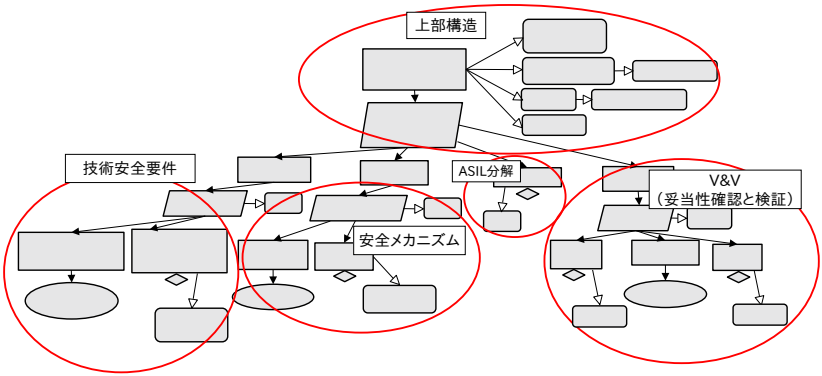
図 6-5　GSN での表記例

6.3　アシュアランスケースの具体例

(1)　セーフティに関する具体例

自動車分野では、機能安全規格として ISO 26262 が制定されています。本規格における「機能安全」とは、「電気電子(E/E)システムの機能不全のふるまいにより引き起こされるハザードが原因となる、不合理なリスクの不在」と定義されており、自動車の電気電子システムが対象となります。IPA は 2012 年度、前述の GSN を用いて ISO 26262 に適合するように実験的に自動車のセーフティケースを作成しました［61］。

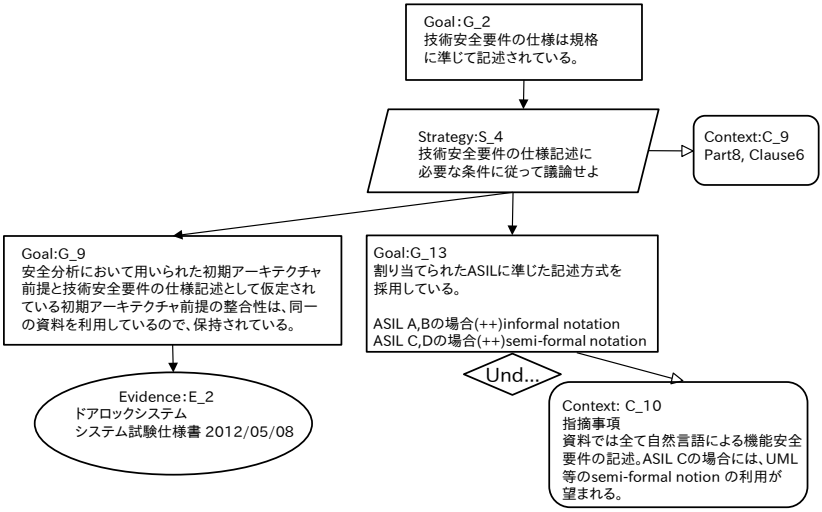
ISO 26262 は 10 の Part に分かれており、Part4 ではシステムレベルの製品開発について規定しています。図 6-6 は、その中の第 6 節「技術安全要件仕様」を GSN で表記したもので、議論の構造を決める「上部構造」、「技術安全要件（Technical safety requirements）」の仕様記述に関する部分、「安全メカニズム」、「ASIL 分解」、機能安全要件に関する「V＆V（妥当性確認と検証）」から構成されています。



出典：「既製システムを ISO 26262 に適合させる場合のセーフティケースの利用とその評価」［61］を基に作成

図 6-6　IPA/SEC が実験的に作成した ISO 26262(Part4-6)の GSN 図

図 6-7 は、図 6-6 の中の技術安全要件を抜き出したものです。Strategy：S_4 では ISO 26262 の Part8-6 節の「安全要件の仕様と管理」を Context：C_9 として位置づけています。



出典:「既製システムを ISO 26262 に適合させる場合のセーフティケースの利用とその評価」[61]を基に作成

図 6-7　ISO 26262(Part4-6)の「技術安全案件の仕様」部分の GSN 図

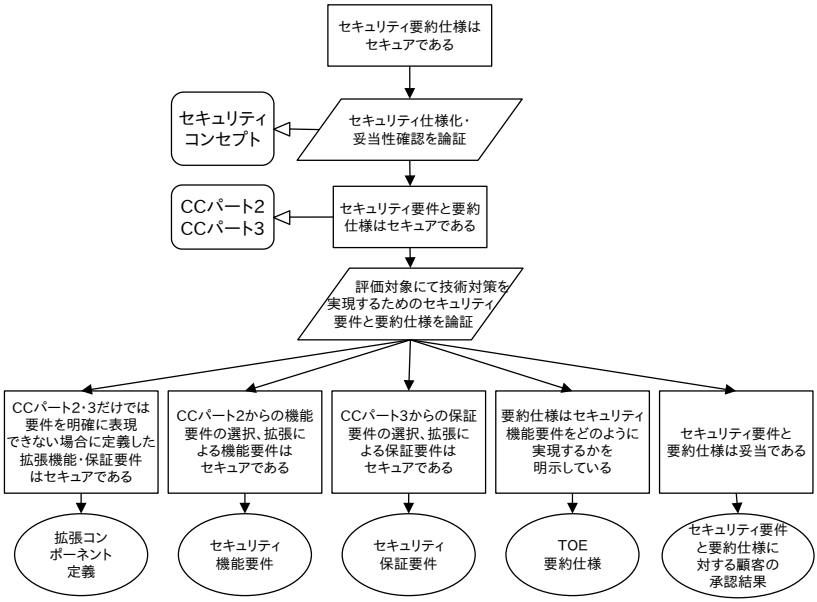
このように、セーフティ設計のゴール、議論、リスク対応と根拠などがGSNで記述され、全体の関係が図示されることで、品質管理部門や発注者によるレビューが容易になると期待されます。

また医療分野では、米国において、既に普及しているモバイル型の輸液ポンプ(定期的に身体に薬品を注入する機器)の安全性についてアシュアランスケースで妥当性を検証するレポートが公表されています[62]。いずれも研究実証ではありますが、内容としては実用化が可能なレベルであり、今後の普及が期待されます。

(2)　セキュリティに関する具体例

コモンクライテリア認証(5.3(1), P.64 参照)取得時において、アシュアランスケースを用いてセキュリティ仕様を決定する手法として「CC-Case」が提案されています[63]。コモンクライテリア認証においては、対象となる製品のセキュリティ設計仕様書であるセキュリティターゲット(ST)が必要となります。CC-Caseでは、コモンクライテリア認証の規格をモデル化し、コンテキストとして位置づけながらST作成(設定と妥当性検証)プロセスを記述します。これによって、コモンクライテリア認証の規格に適合したSTの作成、評価機関による妥当性の

確認などが容易となります。図 6-8 に CC-Case におけるセキュリティ機能要件を実システム上で実装する方法を示したセキュリティ要約仕様化段階のアシュアランスケースの例を示します。



出典：情報セキュリティ大学院大学他「CC-Case～コモンクライテリア準拠のアシュアランスケースによるセキュリティ要求分析・保証の統合手法」［63］を基に作成

図 6-8　CC-Case のセキュリティ要約仕様化段階のアシュアランスケース

また、米国国土安全保障省では、システム開発がセキュアであることを、ソフトウェア開発ライフサイクルを通じて検証するセキュリティアシュアランスケースを例示しています。両者とも具体的なアシュアランスケースが示されており、事例として有用です。

(3)　設計検証における見える化の例

開発したソフトウェアに対して顧客の評価を受ける際、「テスト記録」や「バグ曲線」だけでなく、開発過程の内部レビュー記録を「見える化」し、提示することによりソフトウェアの内部構造や実装方法も含めた「開発内容」を説明することが可能となります。また、顧客の要求項目を詳細化する際の「開発側の想定」や試験仕様を作成する際の「テスト項目の選択過程」を「見える化」し、提示す

ることにより、「開発プロセス」の説明も可能となります。これらにより、顧客に対して新たな価値を提示することができます。

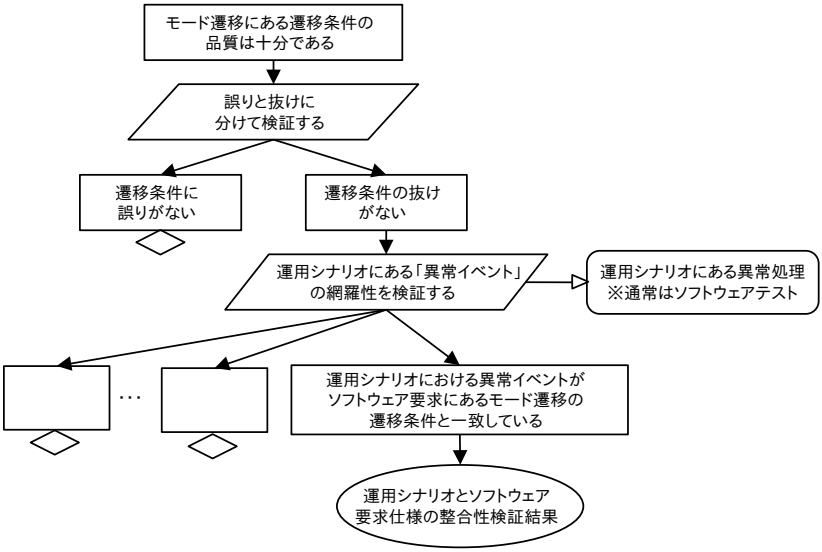


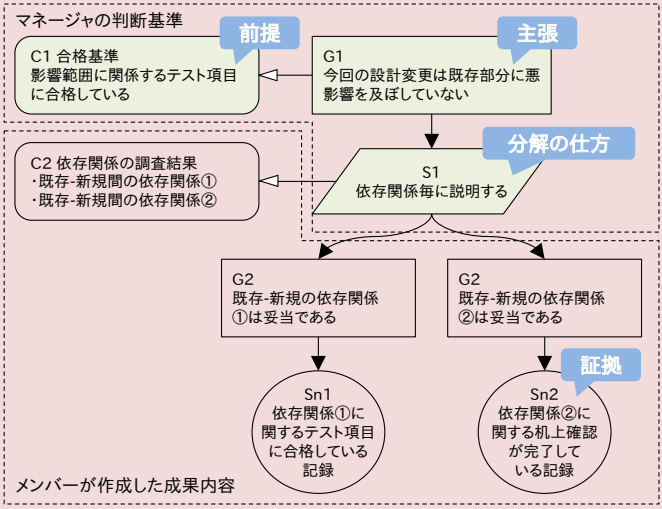
図 6-9　設計検証における見える化の例

また現状では、ソフトウェア設計の品質評価は熟練者によるレビューが中心となっていますが、このレビューが「見える化」されることによって熟練者の知見に基づく「評価プロセス」も若手の開発者に共有されます。「見える化」されたドキュメントを中心に開発者間の議論が活性化することで設計品質が向上し、後工程での手戻りを減らすことにもつながります。アシュアランスケースは、「コンテキスト（暗黙的な要求を含む前提）」と「ストラテジ（レビュー視点による戦略）」、そして「ゴール（検証項目）」の論理的な関係性を「見える化」することが可能な手法であり、前述のソフトウェアの「開発内容」、「開発プロセス」、「評価プロセス」の「見える化」に有効です。本手法により、顧客がソフトウェアの品質を新たな側面から評価できるようになるとともに、熟練者の知見・技術の共有、設計品質のさらなる向上など、様々な効果が期待されます。

コラム6　多忙なマネージャでも設計内容に踏み込んでレビューできる方法

株式会社デンソークリエイト
小林　展英 さん

ここ数年、システムの大規模化に加えて、セーフティ、セキュリティへの関心の高まりもあり、開発の最前線を担うマネージャには、システム全体を俯瞰できる幅広い知識と、メンバーが作成した設計成果の妥当性を適切に判断できる深い知識が益々求められています。しかしながら、多忙なマネージャがメンバー以上に深い知識を持つことは難しく、プロセスの履行状況のみを妥当性の判断基準とする場面もあるようです。



成果内容を見える化した事例

上図は、こうした状況を解消し、マネージャが設計内容に踏み込んで妥当性を判断できるようになるために、マネージャの判断基準にメンバーが作成した設計成果を紐付けた結果になります。設計内容を把握するメンバーが調査結果(C2)に基づいて適切な粒度に分解して説明することで、マネージャは自分の考える合格基準(C1)を満足していない成果(Sn2)の存在に気づくことができます。本事例のように、GSNを介して顧客が期待する成果のあるべき姿を語れるマネージャと、成果内容を熟知したメンバーがお互いの弱点を補い合うことで、多忙なマネージャであっても成果内容に踏み込んだレビューができるようになります。

6.4 セーフティとセキュリティの同時認証に対応する SafSec

セーフティ、セキュリティの規格は、個々の認証取得だけでも相当の手間やコストを要するので、両者を同時に取得することは極めて困難です。SafSec はアシュアランスケースを活用して、両者の認証取得の効率化を図る枠組みです。

SafSec は、英国国防省（MOD）の支援により Praxis High Integrity Systems 社（現 Altran Praxis 社）が作成したもので、英国の安全規格 Def-Stan 00-56 及び国際セキュリティ規格 ISO/IEC 15408（コモンクライテリア）などを対象としています。SafSec では、信頼できるサービスを提供できる能力を「ディペンダビリティ」、ハザードや脅威のような望ましくない状況を導く要因を「ロス」と表現し、アシュアランスケース(ディペンダビリティケース)を作成します。SafSec における概念は、セーフティとセキュリティの概念を統合し、かつ重複した部分を除外したものであるため、セーフティとセキュリティの認証取得に共通的に使用できるドキュメントを作成することができます。

表 6-5　SafSec における概念の関係

SafSec における概念	安全領域における概念	セキュリティ領域における概念
アシュアランス要件	SIL	EAL
原因分析	FTA,FMEA	脅威/脆弱性分析
ディペンダビリティケース	セーフティケース	ST （セキュリティターゲット）
ディペンダビリティ要件	安全要件	セキュリティ・ オブジェクティブ
ロス	ハザード	脆弱性
リスク	頻度と深刻度	頻度と深刻度

出典：（独）産業技術総合研究所 セーフティとセキュリティ規格の同時認証方法論について［57］を基に作成

SafSec には、現状では様々な課題があります。例えば、ハザード分析と脅威分析では手法が異なるため、一つのディペンダビリティケースでは表現できません。このため、まずディペンダビリティケースを作成し、さらにセーフティとセキュリティの規格認証に向けてそれぞれのアシュアランスケースに変更する必要があるため、従来よりも手間やコストを要してしまう場合があります。

6.5 ディペンダビリティアシュアランスケースのフレームワーク

2015 年 3 月、IPA/SEC が策定した消費者向け機器のアシュアランスケースのフレームワーク「DAF for SSCD(Dependability Assurance Framework for Safety-Sensitive Consumer Devices)」が国際標準化団体 OMG(Object Management Group)に標準規格として認定されました [64]。本フレームワークは、自動車やロボット、スマートハウスなどの消費者向け機器に対して高い安全性や信頼性、可用性を確保する開発方法論で、構成は表 6-6 の通りです。

表 6-6　DAF for SSCD の構成

略語	名称	概要
DCM	Dependability Conceptual Model	ディペンダビリティ概念モデルの定義
DPM	Dependability Process Model	ディペンダビリティプロセスの定義
DAC	Dependability Assurance Case	ディペンダビリティケースによる保証の構造

出典：IPA「コンシューマデバイス機能安全規格が正式に OMG 標準規格へ」 [65]を基に作成

DCM は、既存の機能安全規格の構造を概念モデルとして見える化することで理解しやすく表現するもので、ISO 26262（Part1～Part3）を参考に作成されています。DPM は、ディペンダビリティを保証するための開発プロセスを規定するもので、繰り返し確認するプロセスを加えた点が特徴です。DAC は「保証ケース（ディペンダブルにするための観点、実現手段、実現された証拠等からなる文書等）」作成のためのテンプレートであり、検討が先行する自動車のエンジンストールの保証ケース案を提供しています。

本フレームワークは、日本流のすり合わせ開発との融和性が高いものであり、消費者向け機器の安全性や信頼性の向上の参考となります。

おわりに

「つながる世界」においては、身の回りの機器やシステム同士がネットワークで連携することで生活空間上に新しいサービスや価値を生み出しています。しかしながら「つながる世界」では、ネットワークを介して脅威が波及するなど新たな問題も生じています。そこで機器やシステムの開発においては、今まで以上にセーフティとセキュリティへの対応が必要とされています。

本書では「つながる世界」におけるセーフティとセキュリティのリスク分析及び設計手法の説明を行うとともに、それらの設計品質を見える化することで関係者が設計を理解・共有する手法（アシュアランスケース）を紹介しています。現状及び将来のハザードや脅威に対して、効果的にセーフティとセキュリティ対応を行う上で、本書が一助となることを期待します。

付録 参考文献

[1] IPA/SEC, “組込みシステムの安全性向上の勧め（機能安全編）,” [オンライン]. Available: http://www.ipa.go.jp/sec/publish/tn05-011.html.

[2] 文部科学省, “外来語の表記,” 1991. [オンライン]. Available: http://www.mext.go.jp/b_menu/hakusho/nc/k19910628002/k19910628002.html.

[3] テクニカルコミュニケーター協会, “外来語（カタカナ）表記ガイドライン 第 2 版,” 2008. [オンライン]. Available: http://www.jtca.org/ai_collaboration/katakana_wg/katakana_guide.pdf.

[4] 経済産業省, “消費生活用製品安全法,” [オンライン]. Available: http://www.meti.go.jp/policy/consumer/seian/shouan/contents/shouan_gaiyo.htm.

[5] IPA, “情報セキュリティマネジメントと PDCA サイクル - リスクアセスメント,” 2015. [オンライン]. Available: https://www.ipa.go.jp/security/manager/protect/pdca/risk_ass.html.

[6] SESAMO Project, “SECURITY AND SAFETY MODELLING FOR EMBEDDED SYSTEMS, ISSE Workshop, 2014,” 2014. [オンライン]. Available: http://sesamo-project.eu/sites/default/files/downloads/publications/02-isse14-sesamo.pdf.

[7] Railtrack, “Engineering Safety Management Issue 3, Yellow Book 3, Volume 1 and 3, Fundamentals and Guidance,” 2000.

[8] IPA, “「情報処理システム高信頼化教訓集（IT サービス編）」2014 年度版,” [オンライン]. Available: http://www.ipa.go.jp/sec/reports/20150327_1.html.

[9] 一般社団法人重要生活機器連携セキュリティ協議会, “生活機器の脅威事例集,” [オンライン]. Available: https://www.ccds.or.jp/public_document.html.

[10] トレンドマイクロ, “急増する POS システムへの攻撃と POS マルウェアファミリ,” [オンライン]. Available: http://blog.trendmicro.co.jp/archives/9902.

[11] 経済産業省,“リスクアセスメント･ハンドブック実務編,”[オンライン]. Available: http://www.meti.go.jp/product_safety/recall/risk_assessment.html.

[12] IPA, “共通フレーム２０１３の概説,” [オンライン]. Available: https://www.ipa.go.jp/files/000027415.pdf.

[13] B. Nuseibeh, “Twin Peaks,” [オンライン]. Available: http://www.ics.uci.edu/~andre/ics223w2006/nuseibeh.pdf.

[14] 経済産業省, “消費生活用製品向けリスクアセスメントのハンドブック第一版,” [オンライン]. Available: http://www.meti.go.jp/product_safety/recall/risk_assessment.html.

[15] IPA, “米国における STAMP（システム理論に基づく事故モデル）研究に関する取り組みの現状（前篇）,” [オンライン]. Available: https://www.ipa.go.jp/files/000038950.pdf.

[16] IPA, “米国における STAMP（システム理論に基づく事故モデル）研究に関する取り組みの現状（後編）,” [オンライン]. Available: https://www.ipa.go.jp/files/000039623.pdf.

[17] IPA セミナー（有人宇宙システム株式会社）, “安全解析手法 STAMP／STPA の概要と事例紹介,” [オンライン]. Available:

http://sec.ipa.go.jp/seminar/20140121.html.

[18] JEMIMA, “機能安全規格の技術解説,” 2013. [オンライン]. Available: http://tech.jemima.or.jp/doc/func_safety_201311.pdf.

[19] 財)日本科学技術連盟・R-Map 実践研究会編著, “製品安全, リスクアセスメントのための R-Map 入門(第 1 版),” 10 5 2011. [オンライン]. Available: https://www.juse.or.jp/reliability/introduction/03.html.

[20] NITE, 製品安全センター, , “100 の事例から製品事故リスクを低減する、NITE の「製品事故 100 選」,” 2014. [オンライン]. Available: http://www.nite.go.jp/data/000055687.pdf.

[21] 経済産業省,“組込みシステム産業の課題と政策展開,”16 11 2011. [オンライン]. Available: http://www.jasa.or.jp/et/ET2011/visitor/images/pdf/S1_web_data111116.pdf.

[22] 財団法人機械振興協会, “機械の安全・信頼性に関するかんどころ,” 2011. [オンライン]. Available: http://www.jspmi.or.jp/system/file/3/839/document.pdf.

[23] 白坂成功, “アーキテクト～アーキテクトは何ができるのか～,” 2012. [オンライン]. Available: http://home.jeita.or.jp/page_file/20121205162200_Vrq3c4OemA.pdf.

[24] Kevin Soo Hoo, “Tangible ROI through Secure Software Engineering, .Security Business Quarterly,. Vol.1, No.2, Fourth Quarter, 2001”.

[25] Microsoft, “セキュリティ上の脅威の評価,” [オンライン]. Available: https://msdn.microsoft.com/ja-jp/library/ms172104%28v=vs.80%29.aspx.

[26] Microsoft, “Security Planning Through Threat Analysis,” 12 2007. [オンライン]. Available: https://msdn.microsoft.com/ja-jp/library/cc756184%28v=ws.10%29.aspx.

[27] MITRE, “CAPEC (Common Attack Pattern Enumeration and Classification),” [オンライン]. Available: http://capec.mitre.org/.

[28] EVITA Project, “Deliverable D2.3: Security requirements for automotive on-board networks based on dark-side scenarios,”2009. [オンライン]. Available: http://www.evita-project.org/Deliverables/EVITAD2.3.pdf.

[29] IPA, “自動車の情報セキュリティへの取組みガイド,” 2013. [オンライン]. Available: http://www.ipa.go.jp/security/fy24/reports/emb_car/.

[30] 国立情報学研究所　吉岡信和, “セキュリティ要求工学技術とその実効性,” [オンライン]. Available: http://www.fuka.info.waseda.ac.jp/rewg-sub/workshop/201305/IPSJ-REWS-SSE-intro.pdf.

[31] Telecom-ISAC Japan, “セキュリティ情報提供,” [オンライン]. Available: https://www.telecom-isac.jp/public/security.html.

[32] 株式会社三菱総合研究所, “米国のセキュリティ情報共有組織（ISAC)の状況と運用実態に関する調査,” 3 2010. [オンライン]. Available: http://www.nisc.go.jp/inquiry/pdf/fy21-isac.pdf.

[33] 株式会社日立製作所　永井康彦,“情報システムに対するセキュリティ国際標準化の動向と日立製作所の対応,” [オンライン]. Available: http://www.hitachihyoron.com/jp/pdf/1999/06/1999_06_10.pdf.

[34] IPA,“共通脆弱性評価システム CVSS 概説,”20 3 2014. [オンライン]. Available: http://www.ipa.go.jp/security/vuln/CVSS.html.

[35] IPA, “脆弱性の深刻度評価の新バージョン CVSS v2 への移行について,” 30 11 2009. [オンライン]. Available: http://www.ipa.go.jp/security/vuln/SeverityLevel2.html.

[36] 情報セキュリティ大学院大学 大久保隆夫, “MASG,” [オンライン]. Available: https://www.jstage.jst.go.jp/article/ipsjjip/22/3/22_536/_pdf.

[37] 電気通信大学 田原康之ら, “KAOS によるセキュリティ要件の獲得・分析,” *情報処理 Vol.50 No.3*, p. 203, 2009.

[38] 国立情報学研究所, “安全要求分析,” 2014. [オンライン]. Available: http://www.topse.jp/syllabus/09/html/sre_12014.htm.

[39] IPA, “セキュアプログラミング講座,” [オンライン]. Available: http://www.ipa.go.jp/security/awareness/vendor/programmingv2/clanguage.html.

[40] JBMIA, 外務省領事局旅券課, “旅券冊子用 IC のためのプロテクションプロファイル -能動認証対応-,” 15 2 2010. [オンライン]. Available: http://www.ipa.go.jp/security/jisec/certified_pps/c0247/c0247_pp.pdf.

[41] IPA, “IEEE 2600.1™-2009:運用環境 A におけるプロテクションプロファイルの IEEE 標準規格(日本語訳),” 18 1 2012. [オンライン]. Available: http://www.ipa.go.jp/security/publications/ieee/index.html.

[42] IPA, “組込みシステムのセキュリティへの取組みガイド（2010 年度改訂版）,” 2010. [オンライン]. Available: http://www.ipa.go.jp/security/fy22/reports/emb_app2010/.

[43] IPA, “IT セキュリティ評価及び認証制度,” [オンライン]. Available: https://www.ipa.go.jp/security/jisec/index.html.

[44] IPA, “国際承認アレンジメント（CCRA）,” 2015. [オンライン]. Available: http://www.ipa.go.jp/security/jisec/ccra/.

[45] IPA, “CCRA/ICCC 2014 報告, P.11, cPP とは,” 2014. [オンライン]. Available: https://www.ipa.go.jp/security/jisec/seminar/documents/CCRAReport_20141022.pdf#page=11.

[46] IPA,“海外のプロテクションプロファイルの翻訳,”2014. [オンライン]. Available: http://www.ipa.go.jp/security/publications/pp-jp/index.html.

[47] 財団法人地方自治情報センター(LASDEC), “地方公共団体における情報システムセキュリティ要求仕様モデルプラン（Web アプリケーション）,” 2012. [オンライン]. Available: https://www.j-lis.go.jp/lasdec-archive/cms/12,28369,84.html.

[48] IPA, “脆弱性対策：ファジング,” [オンライン]. Available: http://www.ipa.go.jp/security/vuln/fuzzing.html.

[49] CSSC 認証ラボラトリー,“ISASecure® EDSA 認証とは,”[オンライン]. Available: http://www.cssc-cl.org/jp/about_edsa/index.html.

[50] Oil&GasUK, “Piper Alpha: Lessons Learnt, 2008,” [オンライン]. Available: http://www.oilandgasuk.co.uk/cmsfiles/modules/publications/pdfs/HS048.pdf.

[51] 日本船舶海洋工学会,“大規模海上浮体施設の構造信頼性および設計基準研究委員会報告書,” [オンライン]. Available: http://www.jasnaoe.or.jp/research/dl/report_p-8.pdf.

[52] European Air Traffic Management, Safety Case Development Manual, European, 2006.

[53] 英国国防省 Ministry of Defence, Defence Standard 00-56, Issue 4, 2007.

[54] ISO, ISO 26262, Road Vehicles – Functional Safety, 2011.

[55] FDA, “Infusion Pumps Total Product Life Cycle Guidance for Industry and FDA Staff,” 2 11 2014. [オンライン]. Available: http://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm209337.pdf.

[56] Adelard 社,“Claims, Arguments and Evidence (CAE),”[オンライン]. Available: http://www.adelard.com/asce/choosing-asce/cae.html.

[57] （独）産業技術総合研究所 田口研治, “セーフティとセキュリティ規格の同時認証方法論について,” [オンライン]. Available: http://www.ipa.go.jp/files/000044156.pdf.

[58] D-Case, “D-Case チーム,” [オンライン]. Available: http://www.dcase.jp/.

[59] OMG, “Structured Assurance Case Metamodel (SACM), Version 1.0,” [オンライン]. Available: http://www.omg.org/spec/SACM/1.0/.

[60] G. W. Group, “GSN Standard,” [オンライン]. Available: http://www.goalstructuringnotation.info/.

[61] IPA/SEC, “既製システムを ISO26262 に適合させる場合のセーフティケースの利用とその評価,” 2013. [オンライン]. Available: http://www.ipa.go.jp/files/000026856.pdf.

[62] Software Engineering Institute, “Towards an Assurance Case Practice for Medical Devices,” http://www.sei.cmu.edu/reports/09tn018.pdf.

[63] 情報セキュリティ大学院大学、名古屋大学, “CC-Case～コモンクライテリア準拠のアシュアランスケースによるセキュリティ要求分析・保証の統合手法,” [オンライン]. Available: http://lab.iisec.ac.jp/~tanaka_lab/images/pdf/kennkyukai/kennkyukai-2013-09.pdf.

[64] OMG, “Dependability Assurance Framework For Safety-Sensitive Consumer Devices (DAF) 1.0,” [オンライン]. Available: http://www.omg.org/spec/DAF/.

[65] IPA, “コンシューマデバイス機能安全規格が正式に OMG 標準規格へ,” *SEC journal 41*, p. 37, 2015.

索引

本ガイドブックは、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) サプライチェーンにおける品質の見える化 WG において作成しました。

編集者（敬称略）

主　査	後藤　厚宏	情報セキュリティ大学院大学
委　員	麻薙　年男	東芝情報システム株式会社
	梅田　浩貴	国立研究開発法人 宇宙航空研究開発機構（JAXA）
	奥原　雅之	富士通株式会社
	金田　光範	地方独立行政法人 東京都立産業技術研究センター
	櫛引　豪	一般財団法人 日本品質保証機構（JQA）
	小林　展英	株式会社デンソークリエイト
	田口　研治	国立研究開発法人 産業技術総合研究所
	森川　聡久	株式会社ヴィッツ
	林　彦博	パナソニック株式会社
事務局	鈴木　基史	IPA／SEC(パナソニック アドバンストテクノロジー(株))
	中野　学	IPA／セキュリティセンター
	西尾　桂子	IPA／SEC
	宮原　真次	IPA／SEC

作成支援　株式会社 ユビテック

SEC BOOKS

つながる世界のセーフティ＆セキュリティ設計入門

IoT 時代のシステム開発『見える化』

平成 27 年 10 月 7 日　　1 版 1 刷発行
平成 28 年 3 月31日　　2 版 1 刷発行

監　修　者　　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)
発　行　人　　松本 隆明
発　行　所　　独立行政法人情報処理推進機構(IPA)
　　〒113-6591
　　東京都文京区本駒込 2-28-8
　　文京グリーンコート　センターオフィス 16 階
　　URL https://www.ipa.go.jp/sec

ISBN 978-4-905318-35-4 Printed in Japan

ISBN978-4-905318-35-4
C3055 ¥556E

9784905318354

定価：本体 556 円＋税

1923055005563

IPA 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-TN15-001