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』

【ダイジェスト】

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

目次

本書は SEC BOOKS「つながる世界のセーフティ＆セキュリティ設計入門」から事故事例及びインシデント事例等をベースにセーフティ設計、セキュリティ設計及びその見える化の重要性を訴求するために、一部を抜粋したダイジェストです。

セーフティ設計、セキュリティ設計、及びその見える化の手法解説については、SEC BOOKS「つながる世界のセーフティ＆セキュリティ設計入門」を参照下さい。

はじめに

i)　概要

複数の健康器具を組み合わせたヘルスケアサービスや、スマートフォンで家電を制御するサービスなど、異なる分野の製品やサービスを組み合わせた新たなサービスが始まっており、今後は、さらに様々な製品等による高度なつながるサービスが出現すると見込まれています。このような「つながる世界」においては個々の製品の問題がシステム全体の問題となります。1 つの機器のセキュリティ上の脅威だったものが、つながることによりシステム全体の脅威となり、1 つの機器の安全上のハザードがシステム全体の安全上のハザードになり得ます。また、問題が発生したときは迅速な説明責任が求められるようになってきています。

本書は「つながる世界」において求められる安全や安心といった観点から、セーフティ設計（設計の段階で安全を作りこむこと）とセキュリティ設計（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）、及び設計品質の見える化（エビデンスを使って論理的に第三者に分かるように説明すること）の必要性について分かりやすく解説した SEC BOOKS のダイジェストです。

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

「見える化」による設計品質評価

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。

本書は機器やシステムの安全・安心を実現することを目的として、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。

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。

SEC BOOKS の構成と想定読者

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	○	○			○

注：本ダイジェストは、SEC BOOKS の内容（全 6 章）のうち、1～3 章を抜粋して掲載しています。

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。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。

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

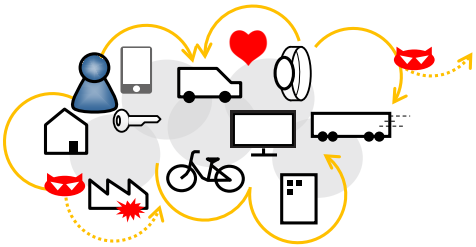


図 1-1　つながる世界のイメージ

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、自動的にデータの収集・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

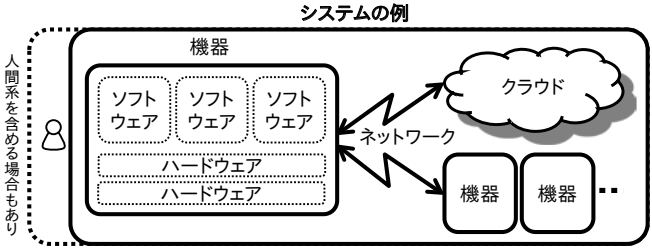


図 1-2　つながる世界のシステムのイメージ

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。

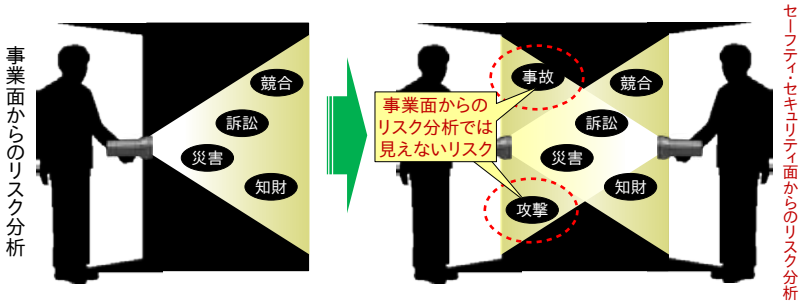


図 1-3 本書が対象とするリスクのイメージ

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[1]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。

---

1 経済産業省，“消費生活用製品安全法”
http://www.meti.go.jp/policy/consumer/seian/shouan/contents/shouan_gaiyo.htm

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。

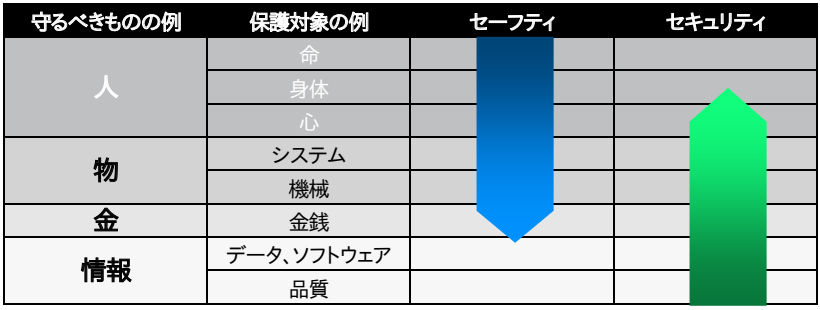


図 1-4 広がるセーフティとセキュリティの守るべき対象範囲

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。

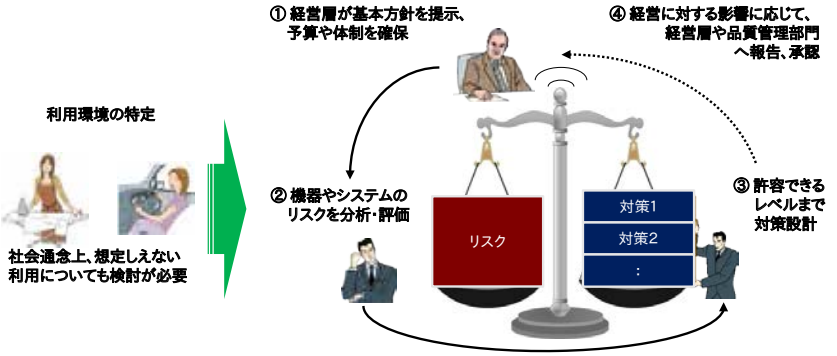


図 1-5　基本方針に基づいたセーフティとセキュリティの対策

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。

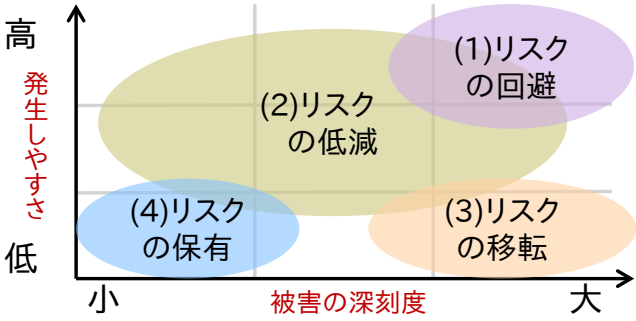


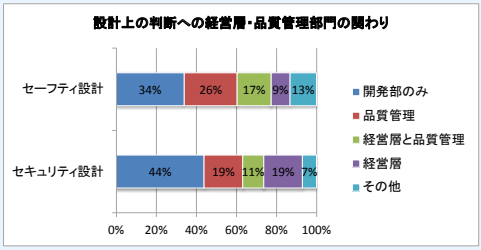
図 1-6　発生しやすさと被害の深刻度から見たリスク対応方法の目安

＜コラム＞ 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)の導入に関しては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

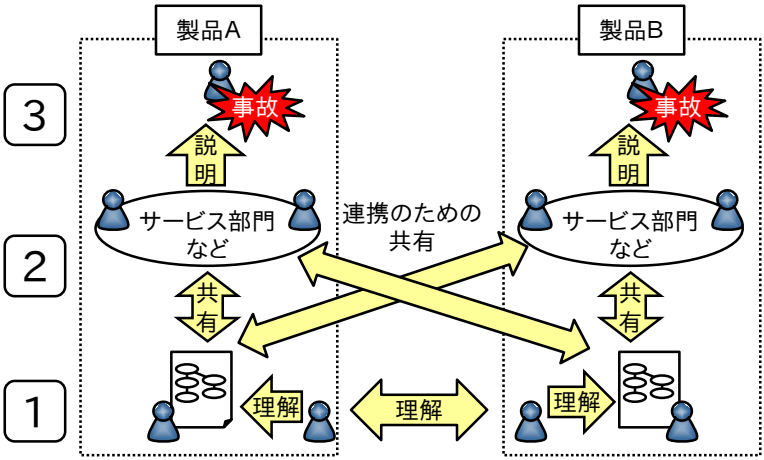


図 1-7 セーフティとセキュリティ設計の見える化の期待効果

(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。

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。

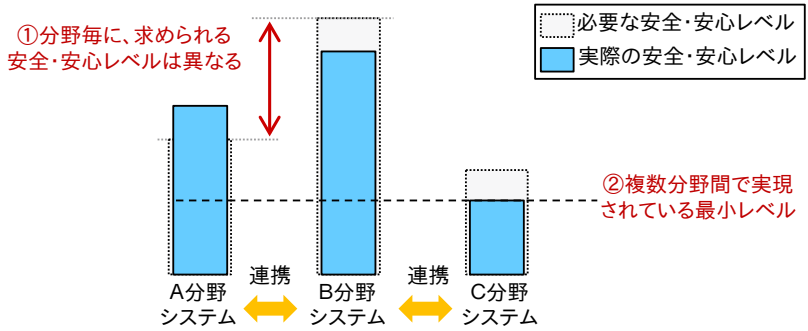


図 1-8　つながる世界の品質の考え方

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。

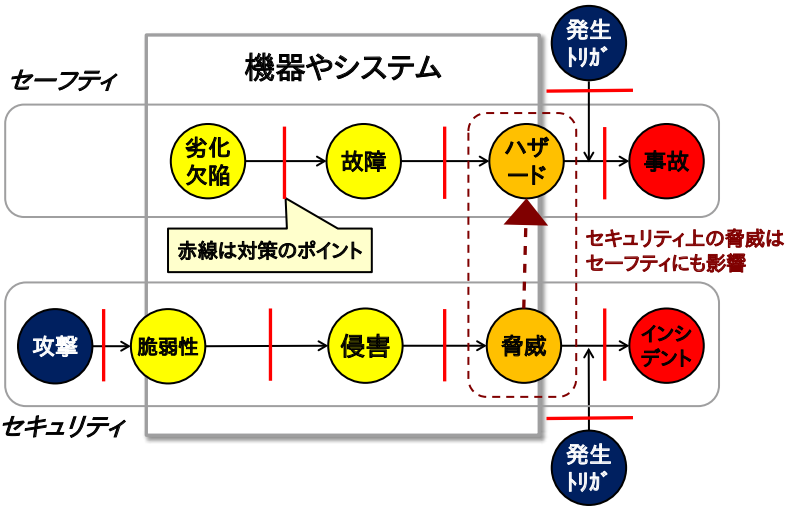
そこで前述のように、各機器やシステムのセーフティとセキュリティの設計品質を見える化し、異なる分野のステークホルダー間で共有することで、相手の分野の考え方の理解、機器やシステムの設計品質の評価、セーフティとセキュリティのレベルに合わせたサービス範囲の決定などを行うことが可能となります。このように設計品質の見える化は、つながる世界の安全・安心の実現には欠かせないものです。

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

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。



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

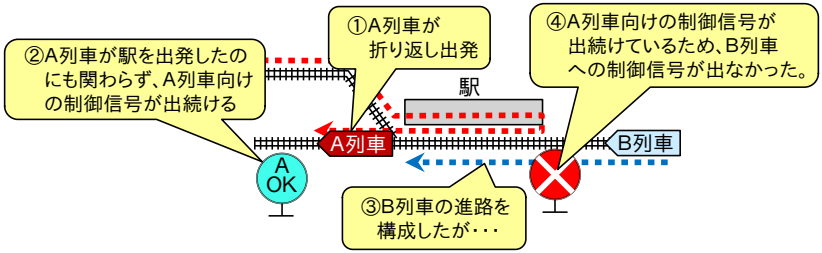
図 2-1　セーフティとセキュリティの被害の発生プロセス

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。



出典：IPA「情報処理システム高信頼化教訓集」の図を基に作成

図 2-2 駅での障害発生状況

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

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。

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。

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。

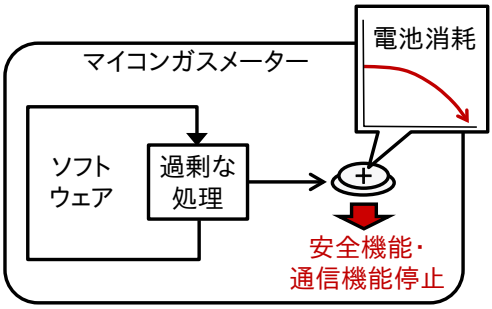


図 2-4　ガスメーターの安全機能が動作しなくなる

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。

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。

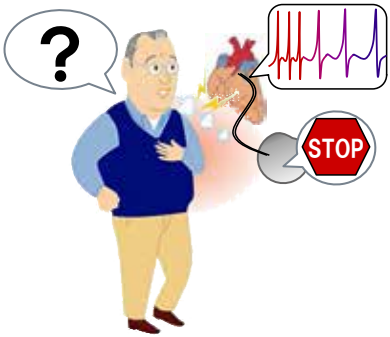


図 2-5　心臓ペースメーカーが動作しなくなる

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

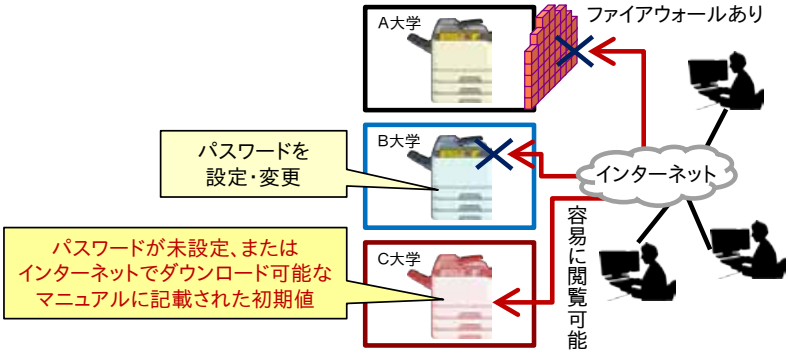
人命に関わる機器やシステムにもソフトウェアの欠陥はありえます。セーフティ対応が必要な機器やシステムの中には、自動車のような故障時は安全に止まることで人命を守れるものだけでなく、健康や生命に関わるために故障時にも止まることが許されないものも存在します。その場合は通常のセーフティよりも強化された二重、三重の対策が求められることもあります。

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。

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。

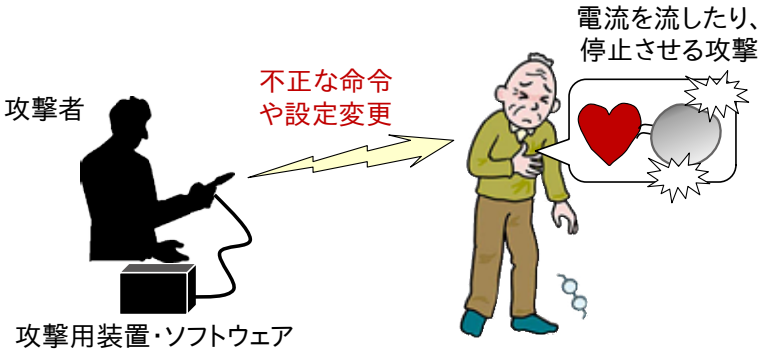


図 2-7　ペースメーカーの脆弱性

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。

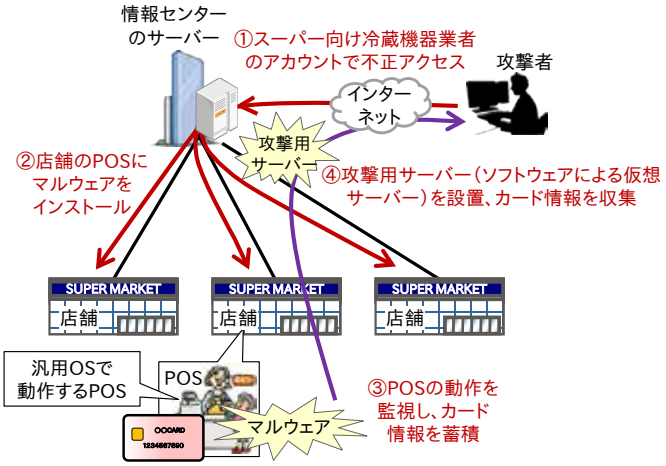
対策のヒント

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。

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。



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。

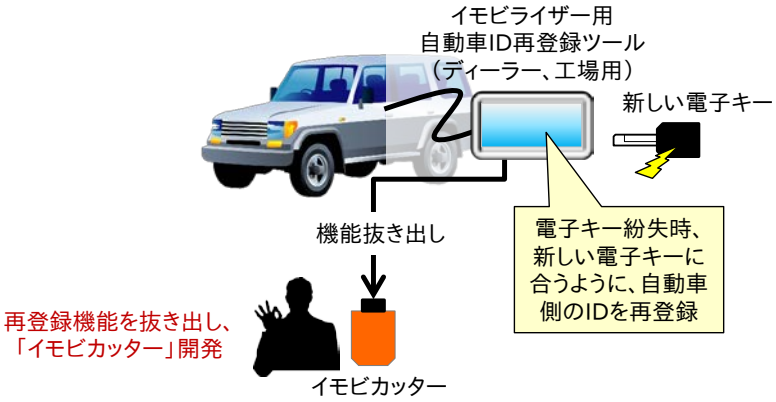
対策のヒント

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。

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。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。

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。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。

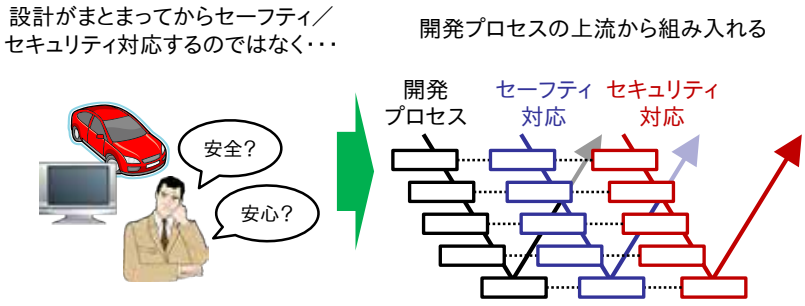


図 3-1　開発プロセスの上流からセーフティとセキュリティの対応を組み入れる

(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。

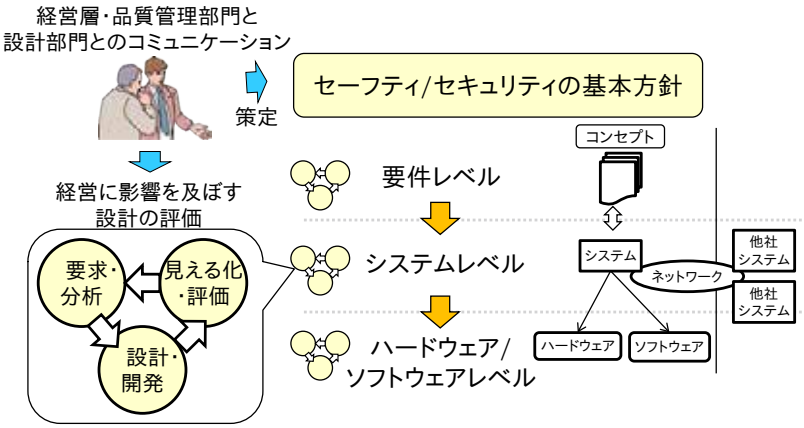


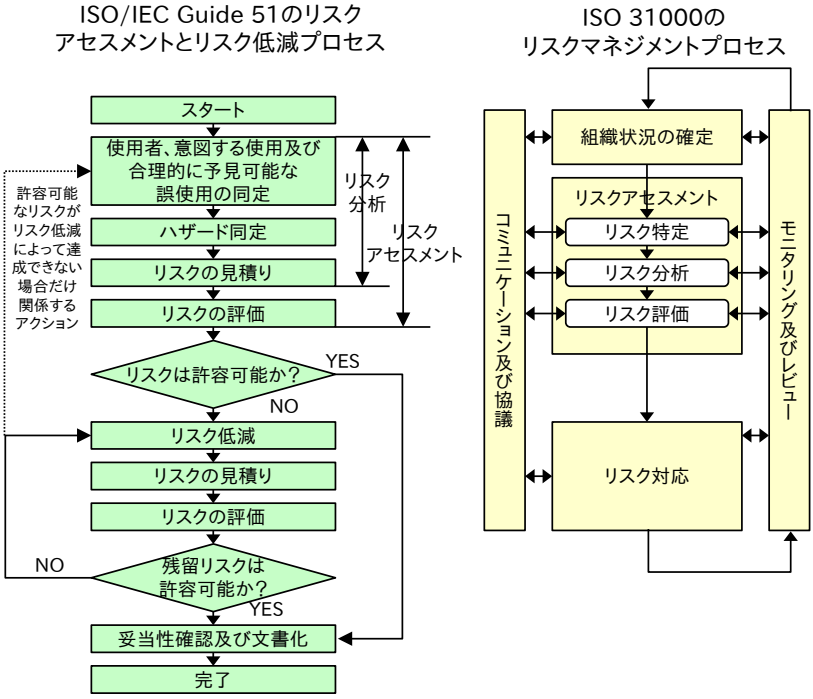
図 3-2 セーフティとセキュリティの設計への経営層の関与

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」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。

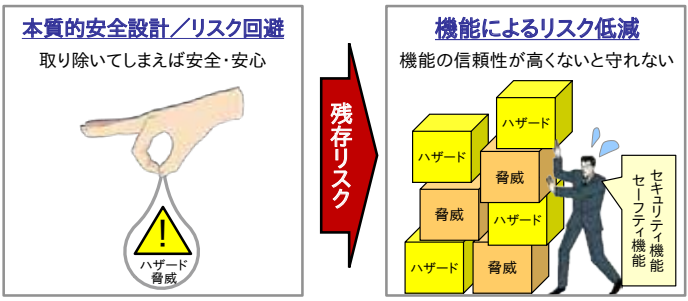


図 3-4　セーフティ機能とセキュリティ機能の重要性

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。

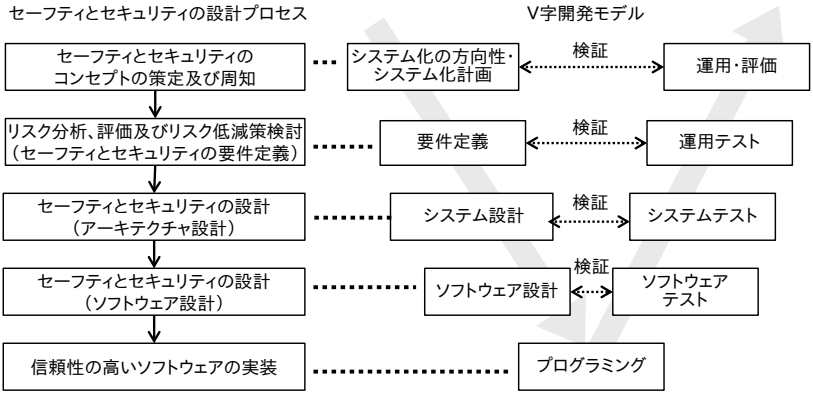


図 3-5　V字開発モデルとセーフティとセキュリティ設計のプロセス

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。

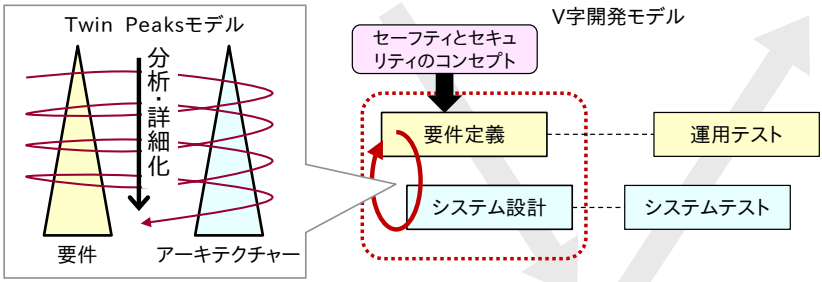


図 3-6　Twin Peaks モデルによる要件とアーキテクチャーの分析･詳細化

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（図 3-7）

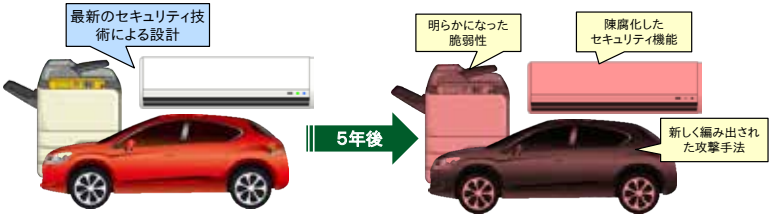


図 3-7　セキュリティ設計の陳腐化

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。

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リスク低減の重要性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・共有することの必要性を紹介しています。現状及び将来のハザードや脅威に対して、効果的なセーフティとセキュリティ対応の重要性を理解するために、本書が一助となることを期待します。

また実際に製品、サービスのセーフティ設計・セキュリティ設計をこれから行う設計者の方は、是非、SEC BOOKS「つながる世界のセーフティ＆セキュリティ設計入門」をご活用下さい。

本書は、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	

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』【ダイジェスト】

平成 27 年 10 月　第 1 刷発行

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 2-28-8

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