

平成 21 年度

組込みシステムにおける 情報セキュリティ対策および 機能安全に関する調査研究

平成 22 年 3 月

社団法人 組込みシステム技術協会



この事業は、競輪の補助金を受けて
実施したものです。

<http://ringring-keirin.jp>

第 1 部

組込みシステム業界における 情報セキュリティ対策

簡易的な ISMS 制度の調査研究

社団法人 組込みシステム技術協会

安全性向上委員会

製品安全ワーキンググループ

はじめに

昨年度に JASA 会員各社に行ったアンケート調査（平成 20 年度機能安全委員会報告書付録「アンケート調査『情報セキュリティ対策実施状況』の結果報告」）では、どの会社も組織の情報セキュリティ管理に強い関心を持ち、また自社固有の取り組みを行っている姿が浮かび上がりました。JASA 会員は情報セキュリティに日々接する業種に属しますから、「情報セキュリティ対策の必要 100%」という結果は当然ですが、しかしその対策に関しては、自前で行っているような回答の一方で「セキュリティ対策の人材不足」や「対策予算不足」、「実務上の負担が大きい」の回答も 50%や 40%を越え、十分対策をなしていない実態も浮かび上がりました。「投資対効果が見えづらい」ことも経営者を悩ませているようです（回答 43%）。

自社の情報セキュリティ管理がきちんとしていることを証明するには、第三者認証制度を活用すればよいのですが、ISMS(ISO/IEC 27001)の認証取得には数百万円、維持審査に毎年数十万円の費用がかかるといわれています。エンタープライズ系のように取得が入札条件になるというのでもあれば、「投資」の甲斐もあるかもしれませんが、組込み系の企業に対しては、今のところ発注企業からの取得の強制はないようです。

しかしこのことは会員各社が、情報セキュリティ管理から逃れることができている、ということでは毛頭ありません。実状はアンケートのごとく「人材不足、予算不足、実務負担大」のようです。

そこで本年度は、このような会員各社の実状に応えるべく、簡易ながら的確な「JASA 式情報セキュリティ管理評価制度」とでもいうべきものを考案しました。企業規模は資本金 1 億円以下、または従業員 100 人以下を想定し、JASA 会員企業の 150 社程度を対象としています。会員各社の方々にご活用いただければと願っております。

最後に、財団法人 JKA をはじめ本事業へご協力いただいた方々に感謝申し上げます。

J A S A 安全性向上委員会
セキュリティワーキンググループ
委員長兼主査 漆原 憲博

目次

第1章	情報セキュリティマネジメントシステムの規格と評価制度	5
1.1	ISMS とは	5
1.2	ISMS の必要性	5
1.3	簡易型 ISMS の確立	6
第2章	組込みシステム業界における情報セキュリティ対策に関する簡易的な ISMS 制度	8
2.1	提案	8
2.2	評価制度の概要	8
2.3	簡易評価制度の概要	9
2.3.1	情報セキュリティ管理体制の成熟度を評価する仕組み	9
2.3.2	ISO 27001 (ISMS) との比較	10
2.4	情報セキュリティ対策成熟度評価シート	11
2.4.1	設問	11
(1)	-----管理系-----	11
(2)	-----実施系-----	12
2.4.2	評価基準と方法	13
2.5	評価の結果	14
第3章	情報セキュリティ対策成熟度プロトテスト	15
3.1	J 社(プロトテスト実施日：2009. 12. 3～2009. 12. 4)	15
(1)	現状	15
(2)	プロトテストチーム (J 社) 所見	15
(3)	プロトテスト受験者側意見 (J 社の代表取締役社長)	16
3.2	A 社(プロトテスト実施日：2009. 12. 19)	18
(1)	現状	18
(2)	プロトテストチーム (A 社) 所見	19
(3)	プロトテスト受験者側意見 (A 社代表取締役)	19
3.3	今後の改善点(プロトテストチームのまとめ)	21
第4章	会員企業に対する JASA のサービス	22
第5章	セキュリティワーキンググループの今後の課題	24
おわりに		25
附録1	情報セキュリティ管理体制構築に関する規程などのサンプル集	26
①	情報セキュリティ対策基準	27
②	リスク管理規程	55
③	成熟度評価チェックシート	67

附録 2 関係機関、団体などの資料	76
1. 参考資料 1	76
2. 参考資料 2	77
3. セキュリティ関連用語・教育関係	78

第1章 情報セキュリティマネジメントシステムの規格と評価制度

ISO/IEC 27001 (JIS Q27001)

情報セキュリティマネジメントシステム (ISMS) の概要と、組込みシステム業界に ISMS がなぜ採り入れられないかを検証した。

1.1 ISMS とは

情報セキュリティマネジメントシステム (ISMS : Information Security Management System) とは、

- (1) インターネット上のホームページの改ざん
- (2) ハードウェア/ソフトウェアのトラブル
- (3) 関係者による情報の漏えい
- (4) 事業継続への対応

これらの情報セキュリティ上の問題解決と、自らのリスク対策を決め計画を持ち、資源配分をして、マネジメントシステムとして安全に運用することである。

そのためには、企業組織に情報セキュリティの管理体制を構築する必要がある。

企業組織が保護すべき情報資産について、機密性 (Confidentiality)、完全性 (Integrity)、可用性 (Availability) をバランス良く維持し、いわゆる PDCA (後述) を回して常時改善することが、ISMS の基本コンセプトである (ISO/IEC 13335-1:2004 を参考)。

機密性とは、認可されていない個人、エンティティ (団体等) 又はプロセスに対して、情報を使用不可又は非公開にする特性であり、完全性とは、資産の正確さ及び完全さを保護する特性、可用性とは、認可されたエンティティ (団体等) が要求したときに、アクセス及び使用が可能である特性である。

1.2 ISMS の必要性

ISMS の国際標準規格のフルスペックは ISO/IEC 27001 (JIS Q27001) といい、その運用とは当該組織において ISMS を確立 (Plan)、導入・運用 (Do)、監視・見直し (See)、改善・維持 (Action) することで、PDCA の運用サイクルを廻すこととしている。

PDCA とは一般に以下を言う。

- Plan : 情報セキュリティ対策の具体的計画・目標を策定する。
- Do : 計画に基づいて対策の導入・運用を行う。
- Check : 実施した結果の監視・見直しを行う。
- Act : 経営陣による改善・処置を行う。

ISMS の基本方針は、企業組織の情報セキュリティの管理体制がこの PDCA サイクルを継続的に繰り返し、常時情報セキュリティレベルの向上を図ることによって当該組織を健全化し、向上させることにある（図 1.1 参照）。

組込み業界においても、発注企業からの情報の保護などが要求されるので、少なからずとも ISMS への対応は必要である。

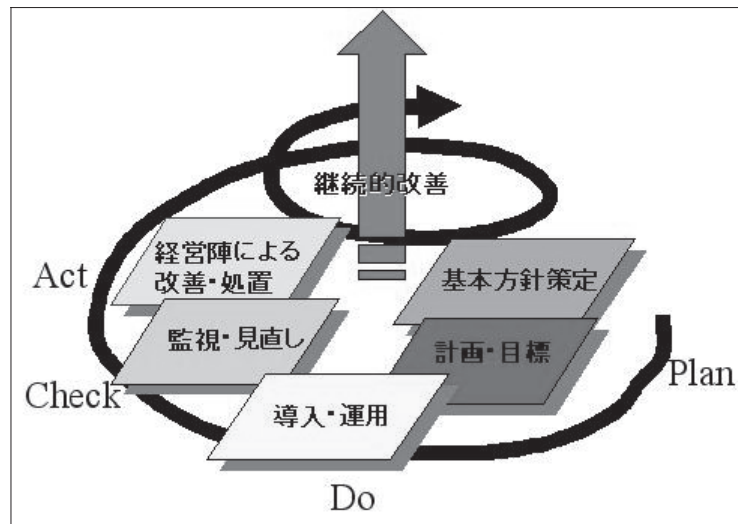


図 1.1 PDCA サイクル（参考：ISMS 適合性評価制度）

1.3 簡易型 ISMS の確立

ISMS（ISO/IEC 27001（JIS Q 27001））の守るべき必須項目のほか要求事項は管理策と呼ばれ、全部で 133 項目ある。管理策のうち対象組織自らの事業活動全般ならびに直面するリスク全体を考慮して選択した項目について、ルール of 文書化を主体に ISMS を確立し、導入、運用、監視、見直し、維持し、かつこれを継続的に改善することである。

しかしながら、これらの事を中小企業で実施するには人・物・金のすべてにわたり負担が大きく、対応が困難な状況にある。

JASA では、2009 年 1 月に「情報セキュリティ対策実施状況」について JASA でアンケート調査を実施した。

対象は JASA 正会員 201 社、有効回答数 76（回収率 37.8%）を得た。情報セキュリティに

対する認識では、「必要性を認める」が 100%に対し、「対策を実施している」が約 80%であった。情報セキュリティ対策を進める上での課題として、「表 1.1 情報セキュリティ対策上の課題」に掲げる。

表 1.1 情報セキュリティ対策上の課題

	課 題	数	%
1	セキュリティ対策推進人材の不足	39	51.3
2	セキュリティ対策予算の不足	33	43.3
3	投資対効果が見えづらい	33	43.3
4	実務上の負担が大きい	32	42.1
5	取引先にコスト負担ができない	22	28.9
6	どこまで対策すべきか不明	21	27.6
7	内部統制、法的対応等への対応が困難	21	27.6
8	教育・訓練が行き届かない	18	23.7
9	従業員の意識が低い	13	17.1
10	取引先の要求への対応が困難	10	13.2
11	最適なツールや相談するところがない	5	6.6
12	経営陣の理解が得られない	2	2.6

これらの点を踏まえて ISO/IEC 27001:2005 (JIS Q 27001:2006) の ISMS 認証取得の実施率を調査した結果、JASA 会員企業 196 社のうち認証取得企業は 17 社 (8.7%) であり、資本金別では、1 億円以下が 4.1% (6 社/146 社)、1 億円以上が 18.3% (11 社/50 社) であった。また、JASA 会員企業 200 社について社員規模別に調べた結果、取得企業は 8.5% (17 社/196 社) で、社員数 100 人以下では 1.5% (2 社/133 社)、100 人以上で 22.4% (15 社/67 社) であった。

しかし、資本金別のうち、資本金 1 億円以下、従業員数 10 人以下の零細企業に限定してみると 10 人以下の企業が 43 社であり、ISMS 認証取得率は 0%という状況であった。このことから、社員数が少なく、情報セキュリティのための専任要員が確保できないことや、予算確保が課題の大きな問題であることが分かる。

そこで、今後、組込み業界の多数を占める小規模企業の情報セキュリティ対策をどうすべきか、また簡易的で安価な評価制度を含めて検討すべきであるとの結論に至った。

まとめ

組込みシステム業界では中小零細企業が多く ISMS 認証取得が難しいので、費用と要員負担が少なく済む制度を検討し、簡易的な ISMS 制度を研究開発する事とした。

第2章 組込みシステム業界における

情報セキュリティ対策に関する簡易的な ISMS 制度

組込みシステム業界向けに簡易的な ISMS 制度を考案し、その制度がどうあるべきかを研究し、その結果を提案するものである。

中小企業が多くを占める JASA 会員企業においては、高額な ISMS 認証取得に代えて、この簡易的な ISMS 制度により体制構築し第三者の評価を受ける事が、今後、各社のビジネス展開に対し有効に働く事を期待している。

※附録 1 について

簡易的な ISMS 制度による、情報セキュリティ体制の構築を検討される企業は、26 頁からの附録 1「情報セキュリティ対策の体制構築用サンプル集」を元に検討されたい。

また、準備が整い次第 JASA の会員ページに、上記サンプル集のファイルを掲示するので必要に応じダウンロードし利用して頂きたい。

サンプル集は、改良のために随時変更することがあるので、適時、内容の確認が必要となる。

2.1 提案

JASA の情報セキュリティワーキンググループでは、簡易的な ISMS 評価制度なるものとして情報セキュリティ対策の成熟度評価制度（以下、成熟度評価または、成熟度評価制度と略す）を創案しここに提案する。

2.2 評価制度の概要

現行のマネジメントシステムの認定・認証制度のスキームは、先ず（財）日本適合性認定協会（JAB）もしくは（財）日本情報処理開発協会（JIPDEC）の 2 つの認定機関のどちらから、ISO/IEC 17021「マネジメントシステムの審査を提供する機関に対する要求事項」によって認定を受けた審査登録機関から認証を受けた組織が、ISMS の認証取得組織となる。

発注企業は、この ISMS 認証取得組織であるかによって、発注先企業を選別するところが多くなっており、組込みシステム業界の企業に対しても波及してきている。

前記したように、この認証を取得するには多大な負担が必要なので、組込みシステム業界としては非常に難しい。

そこで、ISMS 認証取得に代わる制度として、第三者による情報セキュリティ対策の成熟度評価制度を考案し、JASA が主体となり簡易的な ISMS 評価制度を設けたい。

それにともない、会員企業には、教育・指導などのサービス活動も必要となる。

成熟度評価制度の、体制構築から評価証書授与までの概要を図 2.1 に示す。

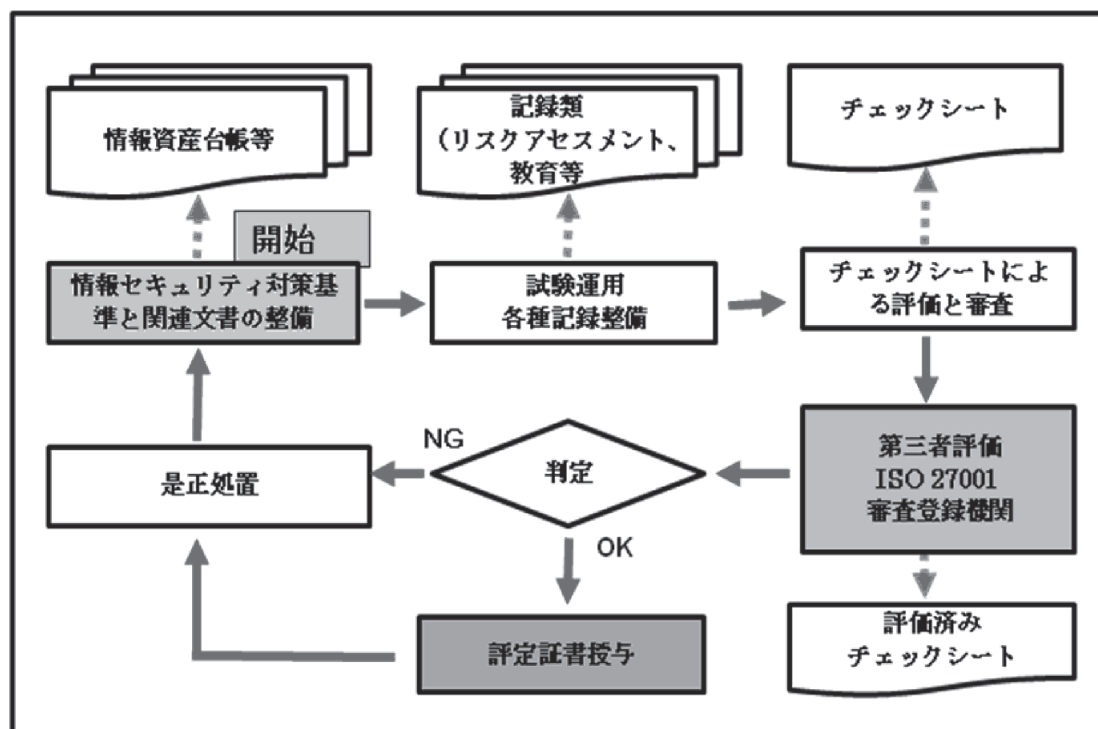


図 2.1 成熟度評価制度の概要

図中、体制構築は「情報セキュリティ対策基準と関連文書の整備」から始まり、破線矢印は作成される帳票類を示す。

2.3 簡易評価制度の概要

本成熟度評価制度は、情報セキュリティ対策成熟度評価シート（以下、評価シートと略す）により、常に自己評価出来ることに特徴がある。

そして、第三者の審査機関が訪問審査し、成熟度を審査し成熟度レベルを評価し、JASA が「評価証書」を発行する。

2.3.1 情報セキュリティ管理体制の成熟度を評価する仕組み

- (1) 組込みシステム開発企業向けの、評価シートを元に企業の成熟度レベルを計る。
- (2) 評価シートによる評価は、**管理系**と**実施系**の 2 分野がある。
- (3) 推進団体は（社）組込みシステム技術協会（JASA）とし、対象組織は概ね資本金 1 億円以下、従業員 100 人以下の企業・組織で、当面原則として JASA 正会員企業（現在約 150 社）とする。
- (4) 評価シートの概要
 - ① IPA のセキュリティ対策ベンチマークをベースに組込み業界向けにアレンジしたものを作成した。
 - 用語、ビジネス形態、開発環境などを考慮し、設問を増減している。

② 概要を 2.4 に示す。

全体を、管理系（問 1～問 2）と実施系（問 3～問 4）の 2 分野とし、全質問数を約 150 とする。

③ 評価ランクの算出方法は、各設問の評価結果の平均値を算出し、小数点以下は切り捨てるものとする（Excel の自動計算による）。

2.3.2 ISO 27001 (ISMS) との比較

（審査費用と企業側の作業負荷の低減策）

- (1) 評価シートにより未達成項目を可視化できるので、それらの項目に対し是正することでマネジメントシステムとして利用が可能。
- (2) 組込みシステム業界に特化したリスク管理による、リスクアセスメントの簡素化
- (3) 内部監査を省略
- (4) 規程類と関連書類のサンプルの利用による社内工数の削減
- (5) 管理策の簡素化 （「表 2.1 ISO 27001 の管理策との比較」を参照）
 - ① 組込みシステム業界向けの管理策に絞込み
 - ② 簡素化による規定類の文書量の削減

表 2.1 ISO 27001 の管理策との比較（△：一部採用）

	ISO 27001 附属書 A 「管理目的と管理策」	簡易的な ISMS
1	セキュリティ基本方針	○
2	情報セキュリティのための組織	○
3	資産の管理	○
4	人的資源のセキュリティ	○
5	物理的及び環境的セキュリティ	○
6	通信及び運用管理	○
7	アクセス制御	○
8	情報システムの取得、開発及び保守	○
9	情報セキュリティインシデントの管理	△
10	事業継続管理	×
11	順守（関係法令などと就業規則）	○

2.4 情報セキュリティ対策成熟度評価シート

本評価シートは、第三者の審査機関が審査し評価する時にも使用する。

また、企業内で自己評価のために使用し、不足な点を改善し成熟度をレベルアップするためにも使用して頂きたい。

※各問の末尾カッコ内数字は、設問数を表わす。

詳細なチェックシートは附録1「情報セキュリティ対策の体制構築用サンプル集」を参照のこと。

2.4.1 設問

(1) -----管理系-----

問1 情報セキュリティに対する組織的な取組状況について（全50問）

問1-1 情報セキュリティポリシーや情報セキュリティ管理に関する規定（12問）

問1-2 経営層を含めた情報セキュリティやコンプライアンス（法令順守）の推進体制の整備（11問）

問1-3 重要な情報資産について、レベルごとの分類、さらにレベルに応じた表示や取扱をするための方法の制定。（6問）

問1-4 重要情報について、入手、作成、利用、保管、交換、提供、消去、破棄等の業務プロセス毎の適切な措置（6問）

問1-5 外部組織に業務や情報システムの運用管理を委託する際の契約書に記載する、セキュリティ上の要件。（3問）

問1-6 従業者（派遣を含む）に対する人事異動時の守秘義務の書面など、セキュリティに関する就業上の義務の明確化。（7問）

問1-7 全従業者（経営層や派遣を含む）に対する、情報セキュリティに関する計画的な教育や指導の実施。（5問）

問2 物理的（環境的）セキュリティ上の施策について（全22問）

問2-1 特にセキュリティを強化したい建物や区画に対しての、セキュリティ対策の実施。（6問）

問2-2 顧客、ベンダー、運送業者、清掃業者など、建物に出入りする外部の人々についての、セキュリティ上のルール制定と実践（4問）

問2-3 重要な情報機器や配線などを、自然災害や人的災害などを配慮した配置、または設置および保守。（5問）

問2-4 重要な書類、モバイルPC、記憶媒体などについてのセキュリティ管理。（7問）

(2) -----実施系-----

問 3 情報システム（以下開発用システムも含む）及び通信ネットワーク及び開発環境などの運用管理状況に関するセキュリティ対策について（全 33 問）

問3-1 情報システムについての、運用環境や運用データに対する適切な保護対策の実施。（6 問）

問3-2 情報システムの運用に際しての必要なセキュリティ対策の実施。（9 問）

問3-3 不正プログラム（ウイルス、ワーム、トロイの木馬、ボット、スパイウェアなど）への対策の実施。（6 問）

問3-4 導入している情報システムに対する、適切な脆弱性対策の実施。（5 問）

問3-5 通信ネットワークを流れるデータや、公開サーバ上のデータに対する、暗号化などの適切な保護策の実施。（3 問）

問3-6 モバイル PC や USB メモリなどの記憶媒体やデータを外部に持ち出す場合、盗難、紛失などを想定した適切なセキュリティ対策の実施。（4 問）

問 4 情報システムのアクセス制御の状況及び情報システムの開発、保守におけるセキュリティ対策の状況について（全 26 問）

問4-1 情報（以下データも含む）や情報システムへのアクセスを制限するための、利用者 ID の管理、利用者の識別と認証の適切な実施。（4 問）

問4-2 情報や情報システム、業務アプリケーション、開発用のシステムなどに対するアクセス権の付与と、アクセス制御の適切な実施。（3 問）

問4-3 ネットワークのアクセス制御の適切な実施。（5 問）

問4-4 業務システム及び組込みシステムの開発において、必要なセキュリティ要件の定義と、その設計や実装への反映。（7 問）

問4-5 ソフトウェアの選定や購入、情報システムの開発や保守に際して、セキュリティ上の観点から、点検のプロセスごとの実施など、適切なプロセス管理の実施。（7 問）

問 5 情報セキュリティ上の事故対応状況について（全 16 問）

問5-1 万が一システムに障害が発生し際、必要最低限のサービスを維持できるようにするため、情報システム（開発用のシステムなども含む）に障害が発生する場合をあらかじめ想定した適切な対策の実施。（7 問）

問5-2 情報セキュリティに関連する事件や事故が発生した際の、必要な行動を適切かつ迅速に実施できるような備え。（4 問）

問5-3 何らかの理由で情報システムが停止した場合でも、必要最小限の業務継続の措置（5 問）

2.4.2 評価基準と方法

評価は、成熟度を1～5の5段階のランク付とする。

具体的には、ランク1から2は評価なし、ランク3～5でISMSの審査機関などの評価を受けることができるものとする。詳細は表2.2に示す。

表 2.2 情報セキュリティ成熟度レベル(案)

ランク	点数	成熟度 (%)	評価内容
1	0	0%～25%未満	評価できず、証明なし。
2	1	25%～50%未満	評価できず、証明なし。
3	2	50%～65%未満	さらに一層の努力が必要、条件付き合格。
4	3	65%～80 未満	努力が必要、条件付き合格
5	4	80%～100%	合格、ISO 27001 認証取得を推奨

※点数は、各設問の評価結果の平均値(小数点以下切り捨て)より算出する。

評価方法は、基本的には評価時点のスナップショットでサンプリング方式とし、初年度以降毎年継続して評価を行う。なお、評価者やJASAは、評価結果や知り得た事実、機密事項として扱う。

評価のメリットは、銀行融資の担保能力強化や、発注企業および社会的要求にこたえることである。

そのため、経済産業省、JIPDEC、IPAなどに働きかけ社会的認知を高めるほか、IT関連の諸団体(社団法人情報サービス産業協会(JISA)やNPO日本ネットワークセキュリティ協会(JNSA)など)にも働きかけて参加企業の拡大をはかる必要がある。

評価手順の概要は以下の図2.2のとおりである。

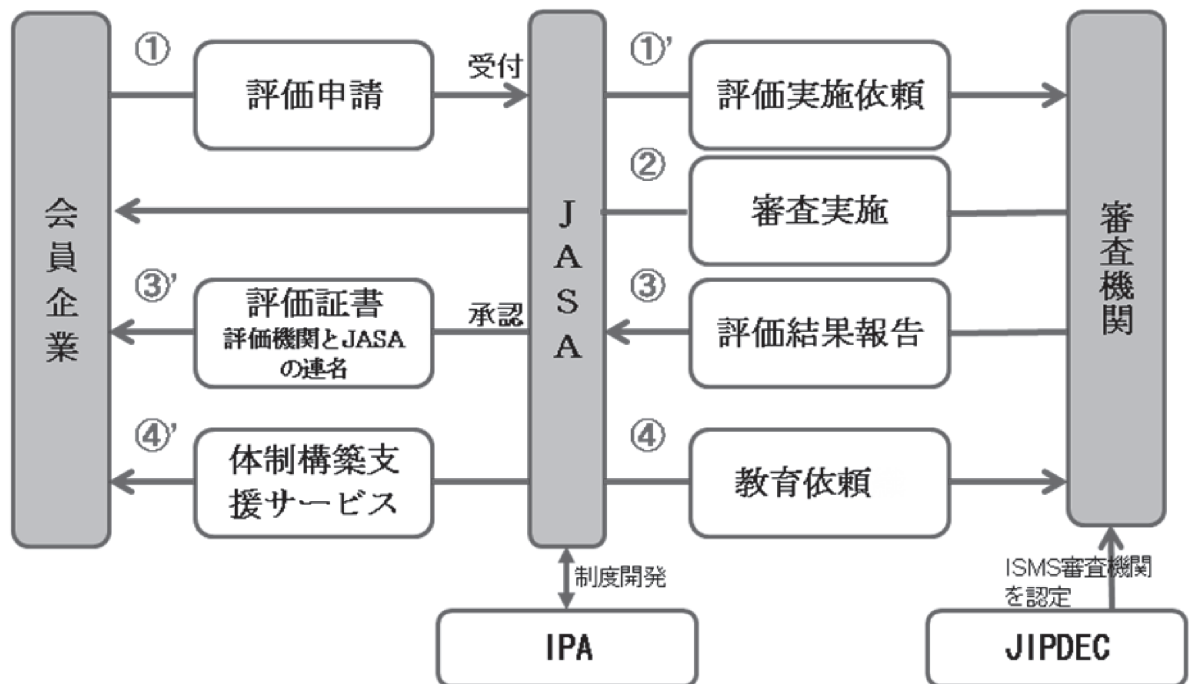


図 2.2 情報セキュリティ簡易評価サービス概念図

2.5 評価の結果

審査機関から JASA に発行される審査結果報告書を受け、JASA がランク付けを評定する。JASA が認めれば審査機関と連名で発行する評価証書を会員企業が取得でき、その有効期間は 1 年間とする。

会員企業には提携する ISMS 審査機関を JASA が紹介する。

まとめ

審査機関による第三者評価を受けることで、情報セキュリティ対策の実施度合いが客観的な評価結果となるので、取引先などへの信頼度が向上する。

第3章 情報セキュリティ対策成熟度プロトテスト

(2 社)の結果報告と改善点

評価制度の完成度を上げるために、J 社及びA社の 2 社にご協力頂きプロトテストを実施し、考察した結果を本評価制度の改善策とした。

実施日はJ 社が 2009 年 12 月 3 日～2009 年 12 月 4 日、A 社が 2009 年 12 月 9 日で、プロトテストチーム構成は、三輪、済賀、大原の 3 名であった。

以下にその概要と結果報告を述べる。

なお、改善点は十分に検討し附録 1「情報セキュリティ対策の体制構築用サンプル集」の各資料に反映してある。

3.1 J 社(プロトテスト実施日：2009. 12. 3～2009. 12. 4)

(1) 現状

経営層はそれなりに情報セキュリティの重要性を認識している。現状でインシデントに相当するものが起きていないので、家族的な経営の中で暗黙知によるセキュリティ対応を評価できる構造をベンチマーキングの中に組み込んでほしいとの意見があった。また基準等は文章の見直しやハイパーリンク・パワーポイントを駆使した分かりやすいものにしてほしいとの意見があった。

従業者層は、管理層から新人まで、また東京支店の管理者など立場上様々であること、共通認識のもととなるルールや指針のドキュメントが現状では整備されていないことなどから、セキュリティ上白紙の状態なのでベンチマーキングの結果にバラツキ（実施者 11 人）が目立った。例えば、不正プログラムのチェックや外部委託開発における使用許諾及び知的所有権の契約の問題などでレベルに 1～5 の範囲で隔たりが出た。しかし一方で、セキュリティ項目の全体的な観点の整理に役立つ、円滑な業務活動ができる、との意見も聴かれた。

(2) プロトテストチーム（J 社）所見

経営層の暗黙知を重視せよとの意見に対し、もともとベースになるのが BS7799 という英国発の基準なので、日本の企業文化に合わないこと、ルールや方針が明文化されていないとセキュリティの個々の項目に対して従事者全体の共通認識が醸成されにくいなどを指摘した。

一橋大学大学院の野中郁次郎教授らが示した SECI モデルも暗黙知と形式知の相互変換を通じて知識を体得するプロセスであり、セキュリティ対策がその知的サイクルのきっかけとなればよいと考える。

家族的経営とは別に、気になるのが近年特に目立つ自社社員や取引先社員による内部からの「情報漏えい」である。アンケート調査では、故意、過失にかかわらず「情報漏えい」の70%以上は内部からというのが常識的になっており、内部から情報漏えいが起る確率が高いことを当然考慮すべきと思われる。

過失による漏えいの中でも、IPAの報告書（「情報漏えいインシデント対応方策に関する調査¹」2007年8月）によると、過失による漏えいが46.4%（紛失・盗難32.0%、誤送信・Webでの誤公開等14.4%）と約半分を占めており、過失による漏えい対策も重要である。

また、基準やベンチマーキングそのものはエンタープライズ系企業を想定したものがベースとなっているので、文章をはじめ更に見直す必要がある。

ベンチマーキング手法は、現状のレベルを可視化すると同時に、ベストなものと自社のギャップを明らかにして現状のギャップをうめるべくセキュリティを改善する経営変革手法の1つであると捉えるのが望ましい。

競争環境の厳しい今日、社内の知識だけでは競争相手に追いつかないが、社外の知識を活用することにより、円滑かつ高速に経営改善に結びつけることが重要である。

そのためJASAやIPAその他の活用を視野に入れた総合的なソリューションの提示が求められる。特にセキュリティレベル分けに権威づけが重要となる。

従事者層では、まずはルールや方針を制定し、セキュリティに対する共通認識となりかつ人によってブレないベースラインを引くことが重要である。

セキュリティインシデントの発生の多くは管理上のミスがほとんどであることから、再発防止のためやセキュリティマネジメントの実施のエビデンス（証拠）確保のために、ルールに則った記録を常時採取して残すことが第三者を納得させるための基本となる。

実行可能なルール作りには、セキュリティ技術だけでなく、人と人との関わり合いや日ごろの業務プロセスを重視する必要がある。

(3) プロテスト受験者側意見（J社の代表取締役社長）

予測していたことではあるが、訪問先での組織のセキュリティチェックにおいては経営層と一般社員層の間にセキュリティ対策に関する意識のずれが大きかった。

IPAの作成したチェックシートを用いてチェックを行ったが、その結果にそれが表れている。

ここでは以下の議論を踏まえ、チェックシートの評点の改善をIPAに対して正式に提案するものである。

経営層は自社のセキュリティ対策を実行されていると高く評価しているにも係わらず、一般社員層では組織的対策がなされていないと手厳しい。中間層はその間にあ

¹情報漏えいインシデント対応方策に関する調査
<http://www.ipa.go.jp/security/awareness/johorouei/index2.html>

る。

チェックシートをつぶさにみると、一般社員層では、問いの中にある「ルールを決めているか」に比重を置いているようであり、その結果得点が低くなる。検査の対象として選択した会社はどれもルールを明確に決めていない。

他方経営層は、ルールは決めていないが、セキュリティが守られている、という事実に関心を置いて回答する。

結果的に経営層による得点は高くなる。

ルールの有無は経営の善し悪し、セキュリティ事故の発生には無関係というのが、小さい企業の主張のようである。

これには根拠がある。企業において基本的なモラルが醸成されているのであれば、ルールは不要ではないか。この手のいわば「社員を犯人に見立てる」ようなルールはむしろ社員を疑いの目で見ることであり、今までの社風に反することではないか。

そのような企業には明文化はされていないが、暗黙知（野中郁次郎）のルールやモラルが存在しているといえるのではなかろうか。これはいわば、家庭の善し悪しを見るのに、いちいちルールの有無を尺度とするのか、という批判に似ている。

確かに、少人数の会社には、家庭や家族になぞらえることも、あながち的外れとはいえない。

また教育の効果に対する信頼というものが、いちいちこの手の社員を疑うようなルールを作ることを妨げているともいえる。

家庭や学校、また企業に入ってから教育などが（日常の交流を含んだ教育、あるいは日本社会の風土）、もし信頼に足るのであれば、この手のルールの作成は不要となるのであろう（性善説）。

他方、そうは言っても、企業の運営がルールと照らし合わせてその是非を検証することは、第三者に対しては説得的な方法ではある。

ルールはないが、日々のその会社の社員の振る舞いを第三者が観察して、事故の発生率を推測することは難しく、鑑識眼の高い第三者でなければ不可である。また暗黙知がその組織にどう働いているか。

これは日本の経営が世界に称揚される際に、かなり説得的な認知の働きであり、今後も研究に値すると思われ、ISO など明文化に頭を悩まされている経営者には待たれる研究と思われるが、セキュリティの（犯人に見立てるのではない）うっかりした事故を日々PDCA で回して防止すべし、という ISO の推奨するセキュリティマネジメントからみると、実際的ではないように思われる。

組織のセキュリティ評価の問題は、以上述べたような問題も問うことは忘れてはならないが、組織の負担を軽くして、実状をはかり、改善するという観点から観ると、いかに現状がセキュリティで守られていると主張したとしても、それを第三者に何をもちて示すか（エビデンス）、という問題に再び戻る。

国内外との企業の交流も当たり前になっている。第三者が理解できるルールが存在、そのルールに対して現実が対応しているか。これは我々の業界で言えば、仕様書に対して実装したプログラムがその通り動いているかというテスト検証のことと同じである。

あるいはより一般的に言えば、経験則の科学的実証・反証の話と同様である。

結局組織のセキュリティ対策とは、その組織の現実を、それに対応するルールと照らしあわせて改善を図るということに他ならない。

このことを是とすると、たとえばチェックシートで、ルールの有無に重きをおいて回答したか、組織の実際に重きをおいて回答したかで、回答にバラツキが出るようなものではなく、両者を個々に回答させ、かつ両者を合算するような方式にすればよいのではないかと思われる。

3.2 A社（プロトテスト実施日：2009.12.19）

(1) 現状

組織全体が3階の1フロアに集中していて管理しやすいが、同じ部屋に他社（協力会社）が共存している。セキュリティの対象は、当面開発部門（プロジェクトルーム兼サーバールーム）に限定し、他から物理鍵で人もエリアも隔離されている。DMZはオープンエリアに用意されているが、サーバ類は置いていない。

また、我々が用意した基準（サンプル）に従って「情報セキュリティ対策基準」「情報セキュリティ管理体制組織図」「オフィスレイアウト図」「オフィスネットワーク図」「IT設備（ハードウェア及びソフトウェア）」「情報資産台帳」「情報セキュリティ管理体制組織図」及びプロジェクトルーム兼サーバールームの「鍵管理簿」と「入退出記録簿」を予め準備していた。

セキュリティの適用範囲は、「ECドライバ開発プロジェクト」という1プロジェクトで、外部とは直接的なネットワーク接続はない。担当は京都本社の1人を割り当て、ベンチマーキングは社長と担当者に東京支店の開発本部の開発者が加わった。

組込み系企業の開発部門では、自前でサーバをたてたり、開発環境は必ずしもWindowsではなくLinux他が多いという特殊性がある。

また、開発環境を客先とそろえておく必要からソフトウェアの更新に制約があり、OSのセキュリティパッチ等が容易に適用できない点も、エンタープライズ系企業とは異なる。

当面東京支店の開発本部という限定されたセキュリティ対策を取りやすい範囲から始めて、近い将来順次全社に拡大する方針である。

組込み系企業の開発部門では、自前でサーバをたてたり、開発環境の特殊性も考慮する必要がある。

(2) プロトテストチーム（A社）所見

対象のプロジェクトルーム兼サーバールームは机のほかに開発環境しかなく、鍵は各自の管理で機密情報は開発リーダーが管理しているのと、ネットワーク上のセグメントは独立しているので、当面セキュリティ上の問題は少ない。

また、開発環境は必ずしも Windows ではなく Linux、Unix、Mac など多種多様のハードおよび OS がある事も組込み業界の特殊性である。

ただ開発プロセス上、セキュアプログラミングの必要性、人件費を考えた場合、CISO (Chief Information Security Officer) などセキュリティマネジメントの専門的な部分のみを外部の専門家に委託すればよいというセキュリティアウトソーシングの考え方もある。現にクラウドコンピューティングのセキュリティでは、クラウド提供業者とエンドユーザの間でセキュリティを専門に扱う業者（シマンテック Hosted Service グループなど）も出現している。この部分、組込み系の中小企業に対して格安で JASA が肩代わりする体制を作る方法もある。その体制を確実なものにするために、収益の一部を使って JASA 側担当者の資格維持費に充てるなど手立ても考えられる。

また、基準やベンチマーキングのチェックシートでは、特殊性を考慮した組込みの開発現場に特化したもの、特に知財を意識した契約的なものも含んだ情報セキュリティの確立が望まれる。

(3) プロトテスト受験者側意見（A社代表取締役）

情報セキュリティ対策基準の重要性と、その運用の必要性は、私(社長)は、理解しており、全社での運用の必要性を感じている。

事務方(管理本部)、営業本部を巻き込むと大げさになりすぎるため、今回のプロト運用では、セキュリティの必要性を理性的に理解できる開発本部のみに閉じた運用とした。

そもそも弊社は、一般的な企業並みの体制を整えているため、建物への入室などの管理は、管理本部主導で、全社統一の規則が作られている。それに加えて、情報セキュリティ対策基準を運用するには、本来は、管理本部の協力無しには、行えない。また、管理業務の分掌からしても、本来は管理本部の領域であろう。

しかし、弊社の管理本部は弊社なりの電子化されたシステムを運用、管理してはいる(例えば、メール・アカウントの管理、金銭台帳の PC サーバでの運用管理)ものの、そもそも、管理本部は、前近代的なセキュリティにしか理解が及ばず、情報セキュリティ対策基準に対応した体制を作るには、理系的な理解力で導入を推進しなければならないだろう。

また、弊社においては、営業本部というものは、なにか新しいことをしようとする、しばしば反対勢力になっている。その反対の理由は、大抵、「新しい事柄を導入

するのが面倒くさい」ということである。

営業本部に対しては、導入を決め、システムや規則の概略が決まった段階で協力を申し出、あとは強制的に従わせるしかない。

今回は、管理本部を巻き込まなかったため、全社の顧客や個人情報や、金銭に関する台帳、証憑は、情報セキュリティ対策基準の運用対象にはならなかった。

さて、今回は、開発本部に閉じた運用を行った。弊社 CTO 開発本部長は、セキュリティ運用について、重要性は認識していたものの、実際の運用に関しては、ほぼ知識がなかった。

今回、CTO 以下社員各位にセキュリティ運用の実際を経験させ、今後の全社に普及させる推進役にさせることを狙った。

今回のプロト運用に関わった人数は、社長を含む 5 名である。情報セキュリティ管理事務局は、社長、CTO、一般社員で構成し、セキュリティ運用に係る問題について考えることを目指した。

プロト運用の対象となる開発のために、開発室とサーバを用意した。

その環境整備のための要員が 1 名 実際の開発業務(運用対象)にあたったのが、1 名である。

しかしながら、弊社 CTO が仕事の処理能力が低く、なかなか今回の情報セキュリティ対策基準の運用に着手しなかった。それにより、すべての事柄の運用がほんのさわりだけとなってしまった。非常に愚かなことである。

社長を長とする、情報セキュリティ管理事務局も組織したが、いまだ、一度も会議を開いていない。また、開発業務を行う担当者ですら、実際には開発作業そのものは着手した程度である。

人数は、5 人と少ないものの、情報セキュリティ対策基準の重要性、必要性和、運用方法については、各人が理解したものと考えている。

今後は、今回、プロト運用に携わった人間を中心に、まず、開発本部で情報セキュリティ対策基準の適用対象プロジェクトを広げたい。

その後、管理本部の情報システムにも本情報セキュリティ対策基準を適用し、最後に営業本部の扱う情報も情報セキュリティ対策基準を適用した運用を行いたい。

セキュアな開発環境の運用は、信頼のできるソフトウェアを作成するのに重要である。自分たちで作成したソフトウェアにセキュリティ・ホールがまったくなく、堅牢であっても、自分たちが意識しないあいだに、他の何者かによって、コードを書き換えられ、バックドアや、脆弱性を植え付けられては何もならない。

したがって、人々から信頼を得られるソフトウェアを開発する者は、開発環境などのセキュリティにも気を配った上で、ソフトウェア開発を行うべきであろう。

3.3 今後の改善点(プロトテストチームのまとめ)

2社を対象にしたプロトテストを実施した結果、今後全般的に改善すべき点として次にあげ、今後継続的に留意していきたい。

- (1) 情報セキュリティ対策成熟度チェックシートに、組込みシステム開発業界向けにアレンジが必要である。
- (2) 用語、業界特有の環境（測定機器を含む開発環境など）、ターゲットの開発進捗との同期など、組込みシステム向けの設問内容を見直し、組込みシステム業界向けの用語・シチュエーションを加味する。例えば、開発環境について、コンパイラ、測定器、ターゲットハードウェア、ICE等を追加する。
- (3) 情報セキュリティ対策成熟度チェックシートによる実施程度を可視化し評価するので、J社の例のような社内で通用しているという「暗黙のルール」については第三者に対する説得力を書くので文書化により明示する必要がある。
- (4) 情報セキュリティ対策基準と情報セキュリティ対策成熟度チェックシートの設問に過不足があるので双方に加筆修正すべきである。（付録1にあるものは修正済み）
- (5) 情報セキュリティ管理ではリスクアセスメントが必須であり、簡略化出来る方法を検討すべきである。（付録1にあるものは簡略化を考慮して作成した）

第4章 会員企業に対する JASA のサービス

JASA 会員向けのサービスとして提案

情報セキュリティ対策の成熟度評価制度全般に渡って会員企業を支援するほか、情報セキュリティに関する啓蒙活動、よろず相談、教育、評価・審査などの種々のサービスは、JASA が一元的な窓口となつて実施することが、会員企業に於ける情報セキュリティ体制構築に寄与できると考え以下の事を JASA の業務とすることを提案する。

- (1) JASA 会員向けのサービスとして提案する。
- (2) 内容は、教育、管理者代行、審査、認証、セキュリティ相談などとする。
- (3) 教育と啓蒙活動の実施および付帯する資料の作成。
- (4) 経営者向け、一般社員向け別々にするか、それとも一緒にするか検討を要するが継続した会員サービスの一環とすべきと考える。
- (5) 評価証書の発行

第三者の審査を受け評価結果として所定の評定レベルであることの証明としてのロゴが必要となる。

JASA には現段階で審査機関としての体制がないので、ISMS (ISO 27001) の審査登録機関による評価を JASA が証明する形式とした。

審査登録機関の審査を受け、審査機関名と JASA の連名にすることで、取引先などに客観的に評価を受けられるようにしたので、ビジネス展開に有利に働くと考えている。

JASA のロゴ名称案としては、次のものが考えられるが、商標権の調査と検討が必要なので、今後の JASA の決定を待ちたい。

- ① コンパクト情報セキュリティ (CIS)
- ② シンプル情報セキュリティマネジメントシステム (SIMS)
- ③ Embedded Information Security by JASA (EIS)
- ④ シンプル情報セキュリティマーク (SISM)
- ⑤ ISMS、Compact Edition - A subset of ISMS for Embedded Software Industry.
- ⑥ ISMS、Simple Edition - A subset of ISMS for Embedded Software Industry.
- ⑦ ISMS、Special Edition - A subset of ISMS for Embedded Software Industry.
- ⑧ ISMSE(Elements) A subset of ISMS for Embedded Software Industry.

- (6) 審査・評価費用

審査・評価費用は審査機関によるが、低コスト化の観点から審査員の移動費用を除き 30 万円以内を目指し調整していきたい。

まとめ

JASA がこれらのサービスを会員企業に実施することで、組込みシステム業界各企業の情報セキュリティ対策の体制構築が促進される事を期待している。

第5章 セキュリティワーキンググループの今後の課題

平成 21 年度のセキュリティワーキンググループとしての活動は、簡易的な ISMS 制度としての「情報セキュリティ対策の成熟度評価制度」の開発が主であったが今後さらに精度を高め充実を図る必要があると考えている。

また、他にも取り組むべき課題は多くあり、そのうち今後の調査研究など取り組むべきいくつかの課題を以下に示しておく。

- (1) 「情報セキュリティ対策に関する組込み業界向けの簡易的 ISMS」の評価制度の実施とセキュリティ相談窓口の検討。
- (2) ISO 自己適合宣言などによる情報セキュリティ対策の体制構築と実用化の取組みの検討。これらの検討に際しては、IPA セキュリティセンターからご助言をいただくことになっている。
- (3) 組込みシステム開発における情報セキュリティ対策の技術的課題に関する検討
 - ・ 組込みシステムのセキュリティへの取組み（これに関しても IPA セキュリティセンターからのご協力、ご指導を得ることになっている）
 - ・ ISO/IEC 15408 関連(Common Criteria)の研究
 - ・ ノキアを中心とした海外メーカーによる SafeCode やマイクロソフトの SDL (Security Development Lifecycle) などの調査研究
 - ・ 情報セキュリティ関係筋からのセミナー開催
- (4) 最近の注目すべき情報セキュリティ上の課題についての研究
 - ・ セキュアなプラットフォームの調査研究
 - ・ クラウドコンピューティングにおけるセキュリティの調査研究
 - ・ セキュリティ要求工学へのアプローチ
 - ・ ETSS²の体系の中で活用できる情報セキュリティに関する教材開発の研究
 - ・ マネージメントと技術に関する教材。他の制度の研究—compTIA³ Security+⁴

² ETSS：組込みスキル標準のこと。IPA が組込みソフトウェアの開発力強化を実現するために策定したもので、わが国の産業競争力強化を目的に、組込みソフトウェア分野の人材育成や人材活用を活性化させるため、保有スキルや求められるスキルを可視化するもの。

³ CompTIA：EDI が様々な規格で利用され情報が飛び交う中、ISO や IEEE に対し標準化を提言するため、各社が集まる場として 1982 年に設立された（日本支局設立は 2001 年 4 月）。IT 業界内で作成された各業務の実務能力基準の認定活動などを行っている IT 業界団体。欧米を中心とし 14 拠点をもち、メンバー企業として 102 カ国 20、000 機関以上（2007 年 4 月現在）の企業が参加している。2000 年に南アフリカ、2001 年に日本・オーストラリアと拠点を増やし、欧米の IT 業界団体から世界の IT 業界団体へと活動を広げるべく、その後も規格標準化の提言を中心に、リサーチ、CompTIA 資格の認定など、IT 業界と中央機関や教育機関との橋渡し役として、活動している。

⁴ セキュリティ技術者の実務能力を評価するワールドワイドの認定資格。詳しくは、http://www.comptia.jp/pdf/Security_plus.pdf を参照のこと。

おわりに

「情報セキュリティ対策には終わりが無い」と言われます。今回考案の制度または書式が、十分に使われたとしても、組織は生きていますから、いわゆるPDCAを回す必要があります。ISMS制度でもそううたっています。

しかしそもそも「十分に使う」ほど書式がよくできているか、あるいは書式がうまくできても組織の実態が伴わないのではなどの、あまり芳しくない状態が浮かんできます。実際認証を取得しようと思えば、数百万円もかかるものをタダでとか、維持審査も無しにということも虫がよすぎるのかもしれない。

しかし数百万円をかけようとも維持審査に数十万円をかけようとも、情報セキュリティ対策を演じるのは個々の社員です。個々の社員の方々が、現場でセキュリティ対策を実行しない限り、成果は得られません。IPAなども、セキュリティセンターでセキュリティのチェックシートを掲示し、診断を行うように促しています。

われわれのセキュリティWGも今後会員各社へ対策の実行を啓発したり、研修をしたりと考えております。また文書だけでは、人に動いていただく管理はなかなかうまく行きません。そこで直接ご指導にうかがうことも計画しております。

そしてまた、IPAなど外部の機関とも協力をしながら、よりよい対策のあり方を研究して行こうと考えております。数年後、JASA会員は少なくとも組織の情報セキュリティ対策は万全であるというお墨付きを得たならば、協会も益々発展し、会員であるわれわれの存在意義も高まろうというものです。

本報告書は大部のISMSの、簡易ながら的確なエッセンスでありたいと念じております。同時に不備を恐れるものではありません。どんどんご意見をいただき、われわれJASA会員のためになるハンドブックに仕立て上げたいと願っております。

最後にこの1年間の精力的なご活動をいただいた本ワーキンググループの委員各位に、またご協力をたまわった専門機関の方々、JASA会員企業の方々に、あらためて感謝申し上げます。

平成22年3月

JASA 安全性向上委員会
セキュリティワーキンググループ
委員長兼主査 漆原 憲博

附録 1

情報セキュリティ管理体制構築に関する 規程などのサンプル集

サンプル集は、JASA の会員企業向けのホームページの準備ができ次第、一連の資料をファイルで掲載するので、情報セキュリティ管理体制構築のために、是非ともご利用頂きたい。（これらのサンプル集は改善のために随時修正するので了承願いたい）

1) 情報セキュリティ対策の体制構築用サンプル集（添付および HP に掲載予定）

1. 情報セキュリティ対策基準.doc
2. リスク管理規程.doc
3. 情報セキュリティ対策成熟度評価シート.doc

2) 関連サンプル集（HP に掲載予定）

- ① 情報セキュリティ基本方針（サンプル 1）.doc
- ② 情報セキュリティ基本方針（サンプル 2）.doc
- ③ 組織図.xls
- ④ 重要情報管理台帳.xls
- ⑤ セキュリティエリア図.xls
- ⑥ 社内ネットワーク図.ppt
- ⑦ ソフト・アカウント管理表.xls
- ⑧ ハードウェア管理票.xls
- ⑨ サーバ室入退出記録簿.xls
- ⑩ 機密保持誓約書(従業者用).doc
- ⑪ 教育実施記録.xls
- ⑫ 利用許可ソフト分類.xls
- ⑬ 業務委託基本契約書.doc
- ⑭ 業務委託個別契約書.doc
- ⑮ 機密保持覚書（協力会社）.doc

情報セキュリティ対策基準(サンプル)

(v0.98 2010.03.01)

株式会社

ご利用上の注意

- * 本基準はサンプルとして作成しております。組織内で規程類を作成する場合に参考にして頂きご利用願います。
- * 本書にある灰色でマークの部分は選択/修正/削除をご検討下さい。
- * 本書にある下線付き斜体の部分は注釈です。完成時には削除願います。
- * 本書では、1項目の場合でも項番を付けております。ご利用時に項番の追加/削除をご検討下さい。

制定日：20____年____月____日

承認	作成

目次

1.	総則.....	1
1.1	目的	1
1.2	適用範囲	1
1.3	用語の定義	1
2.	入退室管理.....	3
2.1	施設への入退出	3
2.2	セキュリティエリア	3
2.3	来訪者.....	4
2.4	施設の施錠管理	4
2.5	不審者への対応	5
3.	重要資産	5
3.1	重要資産	5
3.2	重要資産の分類	5
3.3	重要情報の管理	5
4.	重要情報	6
4.1	重要情報の取扱い	6
4.2	重要情報の保管と廃棄	6
4.3	その他の重要資産の取扱い	7
5.	移送・通信時の取り扱い.....	8
6.	データのバックアップ.....	9
6.1	サーバ内データのバックアップ.....	9
7.	盗難等防止措置	10
7.1	パソコン及び携帯電話の盗難・紛失等防止措置	10
7.2	携帯電話	10
8.	機器・装置の物理的保護.....	11
8.1	施設面に関する考慮事項.....	11
8.2	運用に関する考慮事項	11
9.	アクセス権.....	11
9.1	アクセス権とその管理	11

10.	不正アクセスとアクセス記録.....	13
10.1	不正アクセス対策.....	13
10.2	アクセス記録.....	13
11.	不正ソフトウェア.....	14
11.1	不正ソフトウェアに対する対策.....	14
11.2	社内システムの利用.....	14
12.	開発(受託)契約.....	16
12.1	契約を締結するときの対策.....	16
12.2	オープンソフトを使用するときの対策.....	16
13.	外部委託契約におけるセキュリティ要求事項.....	16
14.	機密保持誓約書（従業員）.....	17
14.1	従業員の義務と責任.....	17
14.2	機密保持誓約書の留意点.....	17
15.	情報セキュリティの事象及び弱点の対策.....	18
15.1	情報セキュリティの事象(障害、不具合、事件事故)及び弱点の報告.....	18
16.	適用法令の順守.....	19
16.1	適用法令及び社内規程の維持管理.....	19
16.2	適用法令の識別.....	19
17.	本基準の見直しと改訂.....	22
17.1	定期見直し.....	22
17.2	適宜見直し.....	22
18.	附則.....	23
	作成者、承認者、制定日.....	23
19.	改訂履歴.....	24

1. 総則

1.1 目的

本基準は、当組織の情報セキュリティ対策に対する具体的な取り組みを示したものであり、考えられるリスク（不正アクセス、情報の漏えい・改ざん・破壊・紛失、コンピュータシステムの事故等）を低減し、個人情報などの重要な情報資産を確実に保護するための施策を規定するものである。

1.2 適用範囲

1.2.1 本基準の適用範囲

株式会社 _____ 本社および横浜支店の開発部に勤務する従業員全員とし、顧客先にて勤務する者は除く。

顧客先にて勤務する者は、顧客先の管理を適用するが、適用範囲の従業員と同様な教育を行うものとする。

1.2.2 対象組織等

【組織】：株式会社 _____ 開発部、横浜支店開発部

【施設】：本社 〒 _____ 東京都 _____ 区 _____

横浜支店 〒 _____ 神奈川県横浜市 _____ 区 _____

【対象者】：社長、役員および、対象組織の下記業務に携わる全社員と全従業員

【業務】：当社の全業務 _____ の開発および _____ の管理業務

【資産】：対象組織の全業務、サービスにかかわる紙と電子情報（データ、業務情報など）、情報システムおよびソフトウェア、開発に必要な環境すべてとする

【ネットワーク】：全社ネットワークおよびクローズド LAN

1.3 用語の定義

1.3.1 本基準で使用する用語の定義

1) 重要資産

別に定めるリスク管理規程により、情報セキュリティ管理責任者及び部門長が重要資産と指定した個人情報を含む全ての情報資産とする。

2) 重要情報

別に定めるリスク管理規程により重要資産の中にある情報とする。

3) 情報セキュリティ管理事務局

本基準を実施するにあたり、情報セキュリティの取り組みを推進する責任部門で、企画・実施・改善について責任を持つ。

4) 情報セキュリティ管理責任者（代表取締役）

本基準を実施するにあたり、全般的な取り組みを主導する責任者及び、当組織の施設と設備に対し主導する責任者。

- 5) 情報セキュリティ管理事務局（管理部長）
情報セキュリティ管理事務局の取り組みを主導する責任者。
- 6) 部門責任者
当組織の組織を編成する部門の責任者で、本基準を部門内で実施するための責任者。
- 7) 情報システム管理責任者
本基準を実施するにあたり、情報システムについて全般的な取り組みを主導する責任者。
- 8) 従業者
役員、社員、派遣スタッフ、協力会社社員（常駐者）、パートおよびアルバイト等、当組織に勤務する全ての者。
- 9) 情報システム利用者
情報セキュリティ管理責任者が情報システムの利用を承認した従業者。
- 10) 情報セキュリティ管理責任者が承認した、税理士、社会保険労務士など社員サービスの為に作業をする者。
- 11) 来訪者
当組織に出入りする従業者以外の者。お客様、取引業者など。
- 12) 情報システム
本基準で意図する情報システム（開発環境を含む）とは以下のものである。
 - ① パソコン（デスクトップおよびノート型）
 - ② サーバ（メールサーバ、ファイルサーバ、プロキシサーバ、共用サーバなど）
 - ③ キーボード、ディスプレイ、マウス、プリンタ、イメージリーダ等の入出力装置
 - ④ HD、FD、MO、CD-R、DVD-R等の外部記憶装置
 - ⑤ OS、ミドルウェア、アプリケーションソフト（ブラウザ、電子メールソフトなど）
 - ⑥ ゲートウェイ、ファイアーウォール、ルータ、ハブ、スイッチ
 - ⑦ ネットワーク設備及び通信回線など
 - ⑧ ホスティングサービス¹などの外部サーバ
 - ⑨ 計測機器（電圧・電流計・ロジアナなど）
 - ⑩ 開発ターゲットの環境 ICE、対象ハード、ブレッドボードなどの擬似対象ハードなど
 - ⑪ その他当組織が事業継続するために運用する情報に関するシステム

¹ **ホスティングサービス** (hosting service) は、インターネットに情報を発信するコンピュータ(サーバ)の容量の一部を賃貸するサービスでレンタルサーバ (rental server) とも言う。通信事業者やインターネットサービスプロバイダが自社設備を用いて提供しているサービスで、専門の業者もある。ほとんどのサービスでは、1台のサーバを複数の顧客で共有する形になっており、使える容量の上限があらかじめ定められている。一般に、上限容量が多ければ多いほど高価になる。レンタルサーバ事業者は、サーバや回線を自前で用意できない顧客から公開したい情報内容(コンテンツ)を預かり、インターネットに接続された自社サーバで公開する。(IT用語事典 e-Words 参照)

13) 付帯文書

本基準に付帯する文書は、以下のものがある。

① 情報資産の棚卸リスト/重要情報管理台帳

情報資産の棚卸リストおよび保管場所別に整理されたリストで、資産名、担当者、責任者、保管場所、保管期間、重要度などの項目を記載したもの。

リスクアセスメントは重要情報管理台帳にある情報に付いて実施する。

② リスクアセスメント管理規程

重要情報管理台帳にある情報資産のリスク管理に関する規程。

③ エリア区分図

利用施設のセキュリティエリア、フリーエリアなどを記載した図。

④ 重要情報の取り扱い手順書（必要時）

⑤ 重要情報の持ち出しリスト

重要情報の名称、持ち出し日付と持ち出し者および許可責任者、返却日/廃棄日付と返却者および返却確認者などを記載したリスト。

⑥ 使用を許可したソフトウェアおよび Web サイトのリスト

・オフィスソフトウェアや開発用ソフトウェアなど許可されたソフトウェアのリスト

・情報収集など業務で閲覧を許可する Web サイトのリスト

⑦ アクセス権設定管理台帳

情報システム利用者のアクセス権、ID、パスワードなどを記載したリスト。

⑧ アクセス記録（ログ）

サーバなどシステムが記録しているもの。

2. 入退室管理

2.1 施設への入退出

2.1.1 施設への入退出の制限

- 1) 施設への出入りは、従業者、当組織従業者が随行する来訪者に限定する。
- 2) 従業者は、施設への入退出の際、必ず所定の通用口から行うものとする。
- 3) 清掃業者、宅急便業者、各種外部保守要員の入退出については、情報セキュリティ管理責任者の責任のもとに行う。
- 4) 入退出にかかる記録の採取を行う。

2.2 セキュリティエリア

2.2.1 セキュリティエリアの設定

- 1) 会社は、施設及び資産のセキュリティを確保するために次の2つのエリアを設定し、

重要情報を取り扱うのはセキュリティエリア内のみとする。

① 来訪者に入室を許可しないエリア（以下、セキュリティエリア）

ネットワークにおいては、ファイアーウォールで守られた社内ネットワーク。
セキュリティエリア内に、宅配便などの荷物の受払場所がある場合は、受払場所を設定する。

② 来訪者に入室を許可するエリア（以下、フリーエリア）

ネットワークにおいては、Web サーバ、メールサーバ等のように外部に公開するサーバなどは非武装地帯(DMZ：Demilitarized Zone)に設置するものとする。

- 2) 情報セキュリティ管理責任者はセキュリティレベルを明示した「エリア区分図」を作成し、管理しなければならない。
- 3) セキュリティエリアには、次の管理策を実施する。
 - ① フリーエリアからは独立させ、施錠の管理を行うこと。
 - ② 鍵の管理は情報セキュリティ管理責任者が責任を持って行う。
 - ③ 情報セキュリティ管理責任者が許可した者のみ入退出ができる。
 - ④ サーバ室やプロジェクト室については、セキュリティエリア内に設け、別途入退出管理を行う。
- ⑤ 入退出許可のない者が、セキュリティエリアに出入りする際には、必ず、入退出許可のある者の帯同のもとに行う。

2.3 来訪者

2.3.1 来訪者への対応

- 1) 来訪者には必ず従業者が帯同し、その従業者が来訪者の行動に対し責任を負うものとする。
- 2) 来訪者への対応は、2.2 で規定した来訪者が入れるフリーエリアで行う。
- 3) 原則としてセキュリティエリアへの入場は禁止するが、必要に応じて同エリアに案内する場合は、必ず情報セキュリティ管理責任者の承認を得るものとする。

2.4 施設の施錠管理

2.4.1 施設の解錠・施錠

- 1) 施設への入館・入室時の解錠および最終退室・退館時の施錠は、従業者が行うものとする。
- 2) 施設の出入り口を施錠する鍵（または ID カード）と、鍵の保管庫の鍵（または ID カード）は、従業者各自が責任を持って管理し使用する。
 出入り口鍵の管理責任者：管理部長
 鍵の保管庫の鍵の管理責任者：管理部長
- 3) 最後に施設を退出するものは、施設を一周し不審者がいないことを確認した上で、出入り口を施錠する。

2.4.2 適用範囲の従業員に変更が出た場合の措置

- 1) 人事異動による職場が変更になった者、および、退職者からは当該日に鍵(またはIDカード)などの貸与物を返却させる。
- 2) 貸与物の返却を受けられなかった場合は紛失したものとし、すぐさま鍵を変更するものとする。

2.4.3 建物への入退出ルール

- 1) 建物への入退出ルールはビル管理者の指示に従う。
(事務所の出入り口を施錠する鍵は、就業時はセキュリティエリア内の所定の場所に保管し、終業後はビル管理者の指定する保管庫に格納する。格納後は扉が自動的にロックされた事を確認する。人事異動等が生じた場合には、パスワード等があればそれを変更する。) ビルによって、管理方法が違うので実情に合わせてください。

2.5 不審者への対応

2.5.1 不審者の識別及び対応

従業員が帯同していない来訪者等の不審者を見つけた場合には、必ず従業員から声をかけ、身元、訪問先、目的等を確認する。

- 1) 確認できた場合、担当従業員に来訪者の帯同をさせる。
- 2) 確認できなかった場合、氏名および連絡先を確認した上で、退出を求める。

3. 重要資産

3.1 重要資産

- 1) 重要資産は、別に定めるリスク管理規程により分類した情報資産管理台帳にあるものの全てとする。
- 2) 重要資産は、情報セキュリティ管理事務局が情報資産管理台帳に登録し管理するものとし、情報セキュリティ管理責任者の承認が必要とする。

3.2 重要資産の分類

- 1) 重要資産には、「重要情報」と「その他の重要資産」(ハードウェア、ソフトウェア、ネットワークなど)がある。
- 2) 重要資産の基本管理は、リスク管理規程に定め、管理方法は、それぞれの資産の特性に合わせた管理をする事とし、リスク発生時には損失が最小限になるような方法で管理しなければならない。

3.3 重要情報の管理

リスク管理規程で定めた重要情報を以下の通りに分類し管理する。

この分類は、紙文書としての情報、サーバに保管している情報、電子媒体にデータとして保存されている電子情報の全てに適用される。

また、紙文書としての情報は、収納したファイルまたはフォルダ等に、ラベル等を貼付

け分類を明示し区別する。

(外部の者が容易に識別できないように、ラベルに具体的な情報名は書かずフォルダ分類記号（または分類名）とするのが良いです。)

3.3.1 情報の分類

1) 極秘情報

社内の特定者のみに開示可能な情報で、外部から預かる個人情報を含む情報。

システム開発プロジェクトなどのように、プロジェクトメンバーにだけ特別に開示を認められたものも含む。

2) 社内秘情報

極秘情報のうち社内開示を認められたもの。

3) 公開情報

当社のものであると他社のものであるものとは問わず、カタログ、パンフレット、ニュースリリース、等により一般に公開されている情報や一般の市販書籍をいう。

3.3.2 情報の例として以下のものがある。

1) 秘密情報(機密性)には極秘情報と社内秘情報の2段階があり、個人情報などの法律で定められた情報は極秘情報とする。

2) 見積書、納品書、請求書などの取引に関する情報および、対象組織内で作成・使用する情報は社内秘とする。

3) 社外（お客様、取引先など）から秘密指定を受け預託又は譲渡されたものは、極秘情報とする

4. 重要情報

4.1 重要情報の取扱い

重要情報の取扱いは、保管場所、アクセス権の設定などを記録し管理するものとする。

1) 極秘情報

アクセス権を特定し持ち出しには、情報セキュリティ管理責任者または、情報を所有している部門責任者の許可を必要とする。また、業務目的以外の複製は不可とする。

2) 社内秘情報

社外への持ち出しには、情報を所有している部門責任者又は、情報システム管理責任者の許可を得るものとする。

3) 公開情報

特に定めない。

4.2 重要情報の保管と廃棄

4.2.1 重要情報の保管

1) 重要情報に指定された、紙文書、電子媒体は、**施錠が可能なキャビネット（キャビ**

ネット名)に保管する。

施錠が可能なキャビネットがない場合は、追加の鍵などで処置をして下さい。

- 2) 重要情報に指定された、電子データとしてパソコン・サーバに保管されている場合には、それぞれの情報に相応するアクセス権を設定する。
- 3) 取り扱い方法に付いて、詳細を記した手順書を別途作成する。

本書で規定できないケース、特別な資料などのケースは別途手順書を作成して下さい。

4.2.2 キャビネットの施錠の管理

- 1) キャビネットの鍵と施錠の管理は、管理部長、及び、部門管理のものは部門責任者が責任を持つものとする。
- 2) 従業員が重要情報の取出し、または保管する場合は、管理部長または部門責任者の許可を得るものとする。

4.2.3 重要情報の廃棄

- 1) 重要情報に指定された紙文書、電子媒体の廃棄は、物理的に裁断・破壊もしくは溶解することにより読取り不可の状態にして廃棄する。
 - 2) 廃棄業者に依頼する場合は、産業廃棄物処理業者及び特別管理産業廃棄物処理業者としての許可を得ている業者を選抜する。
 - 3) 廃棄業者に依頼した時は、廃棄証明書などを受け取る。
 - 4) 重要情報に指定された電子データがパソコン・サーバに保管されている場合には、指定のソフトウェアを使用して削除するか、白紙データで上書き保存後当該ファイルを削除する。
 - 5) 指定のソフトウェアはシステム管理責任者が別途定める。
- ※ パソコンを廃棄又はリース会社等へ返却する時は、内部ハードディスクを指定のソフトウェアによりシステム管理責任者の監督のもと全て削除、廃棄した上で返却する。

4.3 その他の重要資産の取扱い

- 1) 情報システム管理者は社内のシステムに障害、不具合が発生したときは保守に関する関連企業と連携し原則として、対策方法を決め、システムごとに決められた期間内にシステムの復旧をするとともに、被害状況を含めて情報セキュリティ管理責任者に報告するものとする。
- 2) 情報システム管理者はシステムの利用者に社内のシステムに障害、不具合が発生したときは、代替処理手順を作成しシステムの利用者に通知するものとする。
- 3) 復旧が長期化する場合は代替処理手順を作成するとともに、関係する部門および取引先に連絡をするものとする。
- 4) システムごとの復旧期間は、以下のとおりとする。

① 業務システム 発生後の翌日午前中

② 開発システム 発生日当日中

③ 経理システム 翌日中

④ XXX

社内のシステムごとに記載して下さい。

- 5) 開発環境などの重要資産（開発用サーバ、開発ツール、ターゲット、テスト用機材など）は、特に完全性と可用性が重要なので、月1回の定期的な点検、および新規プロジェクト着手時、テスト時など開発フェーズが変わるごとに点検を実施するものとする。
- 6) 顧客先などから預託された資機材およびソフトウェア、データなどは、極秘情報と同様にアクセス権管理と点検管理をし、特に、機密性(C)と完全性(I)を保証しなければならない。

5. 移送・通信時の取り扱い

個人情報を含む文書・データなどの重要情報を外部と移送・通信などで授受する際には以下の取り扱いとする。

1) 紙文書の場合

簡易書留以上で送達記録の取れるものを使用し、授受を行なうものとする。

2) CDなどの媒体に格納する電子データの場合

暗号化または、パスワード付き zip 形式（または rar 形式など）で圧縮処理をした上で電子媒体に保存し、簡易書留以上で授受を行うものとする。

3) 電子メールに添付する場合

電子メールに添付しての授受は、暗号化ソフトで暗号化または、パスワード付き zip 形式（または rar 形式など）で圧縮処理をした上で²SSL または³PGP などを使用した暗号メールにて行うものとする

3) 電子メールに添付する場合

電子メールに添付しての授受は、暗号化ソフトで暗号化または、パスワード付き zip 形式(または rar 形式など) で圧縮処理をした上でメールに添付するものとする。

下表を参考にして実情に合わせて選択してください。

² SSL (Secure Socket Layer) は、インターネット上で情報を暗号化して送受信するプロトコル。現在インターネットで広く使われているデータを暗号化し、プライバシーに関わる情報やクレジットカード番号、企業秘密などを安全に送受信することができる。また、SSL は公開鍵暗号や秘密鍵暗号、デジタル証明書、ハッシュ関数などのセキュリティ技術を組み合わせ、データの盗聴や改ざん、なりすましを防ぐことができる。(IT 用語事典 e-Words 参考)

³ PGP とは、Philip Zimmermann 氏によって開発された暗号化ソフトウェア。暗号化には RSA と IDEA が使われている。

メール送信時のセキュリティ強度				
	SSL または PGP	暗号化ソフト	zip または rar	セキュリティ強度
メール本文と添付ファイルを暗号化	○			高い
添付ファイルだけを暗号化		○		中高
添付ファイルだけをパスワードロック			○	低い

- 4) ウェブ上のフォームで個人情報などの重要情報を収集する場合は、通信路上での盗聴を防止するために、SSL による暗号化など技術的な対策を構築して収集を行うものとする。

6. データのバックアップ

6.1 サーバ内データのバックアップ

6.1.1 データのバックアップの手順

- 1) バックアップはシステム管理責任者の監督のもとで行う。
- 2) バックアップは毎日行うものとする。
- 3) バックアップデータは、サーバとは別のハードディスクに取得し、3 世代前までのものを管理する。必要に応じ 4 世代以上について管理することを妨げない。
保存世代数は実情に合わせてください。
- 4) バックアップ用ハードディスクは、正常な取得を確認した上で所定の場所に保管する。バックアップ用ハードディスクが常時サーバに接続状態にあるので、接続の切断や誤操作から保護するためにサーバと同一のサーバラックに保管する。

6.1.2 データの復旧

- 1) 障害発生時には迅速に復旧させるために、システム管理責任者の監督の下にデータの復旧を行う。その場合、最新のバックアップデータから復旧を行うものとする。

6.2 バックアップデータの廃棄

- 1) 保管期間を経過したバックアップデータは、常に新しいもので上書きするものとし、それ以前のバックアップデータは廃棄する。

7. 盗難等防止措置

7.1 パソコン及び携帯電話の盗難・紛失等防止措置

7.1.1 ノートパソコン使用者の義務

- 1) 申請等により許可された者以外、社外への持ち出しを禁止する。
- 2) 社外使用時は個人情報及び機密情報は、一切ハードディスクに保管しないものとする。
情報は暗号化もしくはパスワード付き zip 形式（または rar 形式⁴など）で圧縮してから、USB メモリに格納し持ち出す。
- 3) 社外使用時はログインパスワード（BIOS および OS）を設定し、万が一、紛失した際に第三者による起動を困難にする措置を講ずるものとする。
- 4) 社外持ち出しの場合は、不備がないかをチェックするとともに、個人情報・重要情報が無い事を確認するものとする。
- 5) 終業後は、盗難防止のために施錠付のキャビネットにて保管する。またはワイヤーロックをかけ、容易に持ち出しできないようにしておくものとする。

7.1.2 スクリーンセーバー

- 1) パソコン使用者は、離席時には Windows キー+「L」キーなどで画面をロックする。
- 2) 不正使用から防護するために 15 分以内でパスワードロック付きのスクリーンセーバーが起動するように設定するものとする。

7.2 携帯電話

（社用の携帯電話がない場合は、この項は削除して下さい）

携帯電話の使用者は、紛失または盗難などにより、個人情報が漏えいしないように対策を講ずることとする。

- 1) 携帯電話の電話帳には、会社名、担当者名(姓のみ)と電話番号、メールアドレスのみを記録し、その他の情報は記録しないものとする。
- 2) 遠隔ロック機能のある機種は予め遠隔ロックをかけ、万が一紛失した際は、遠隔ロック機能のある機種は遠隔ロックをかけ、遠隔ロック機能のない機種は、直ちに通信キャリアの窓口に電話して当該携帯電話を無効化するものとする。

⁴ RAR（ラー）はデータ圧縮のファイルフォーマットの一つ。元々は MS-DOS ベースのファイル圧縮ソフトウェアの名前及びファイルフォーマットである。ZIP に比べ高圧縮のファイルが作成でき、また他のデータ圧縮フォーマットにはあまり見られない特色としてリカバリレコードという一種のハミング符号を付加することで、圧縮ファイルの破損の修復が可能であることが挙げられる。また、分割が可能で、あるファイルを一定のサイズごとに分割して圧縮することができる。（Wikipedia）

8. 機器・装置の物理的保護

8.1 施設面に関する考慮事項

8.1.1 サーバ設置場所等における物理的安全対策

- 1) 建物及び室内の内装及び照明器具は、地震時に落下及び損傷しないよう措置を講ずる。
- 2) サーバはラック等に収納し、適切に据え付ける事により、転倒・落下・損傷・盗難等を防止する。
- 3) 無停電電源装置等により電力を安定供給する。
- 4) 空気調和設備は、設置位置に応じた移動、転倒及び振動防止の措置を取る。
- 5) ケーブル等は、誤接続・破損の危険を避けるために整理し、バインドした上で保護する。
- 6) サーバルームはセキュリティエリアとは独立に入退出管理を行う。
- 7) 顧客先などから預託された資機材は、特に配慮が必要でプロジェクトルームまたは鍵のかかるラックなどに保管する。

8.2 運用に関する考慮事項

8.2.1 施設利用時の留意事項

- 1) 情報システム管理責任者もしくは情報システム管理責任者が指名したものだけが、サーバを操作する事が出来る
- 2) サーバ等の管理を外部に委託する場合、安全対策に関する事項および守秘義務を盛り込んだ作業契約（秘密保持契約⁵⁾）を締結する。

9. アクセス権

9.1 アクセス権とその管理

9.1.1 アクセス権の設定

- 1) 社内の情報システムに対するアクセス権限の付与、抹消、変更は、部門責任者または情報システム利用者が情報システム管理責任者に申請し、情報システム管理責任者が適切に実施する。
- 2) アクセス権限の利用に対する責任は部門責任者または情報システム利用者が負う。
- 3) 部門責任者または情報システム管理責任者は、部門所属の情報システム利用者に適切なアクセス権が付与されているか常に留意し、抹消、変更が必要と判断した場合は、遅滞なく上記（1）の手続きに則り申請する。

⁵⁾ 「秘密保持契約書」とは、秘密（＝機密）情報を開示するときに締結する契約書。ビジネスの世界ではお馴染みの契約書で、一般的に NDA (Non Disclosure Agreement) と呼ばれ、機密保持契約書、守秘義務契約書などと呼ばれることもある。今日のように企業間競争が激化している時代には、秘密情報の漏えいにはより敏感になる必要があり、自社のノウハウ等が第三者に漏れたりすると、企業の存続にかかわる事態を招きかねない。（「あどみん法務・知財部」参照）

- 4) アクセス権付与、抹消、変更の申し出を受けたシステム管理責任者は、適切にアクセス権の設定を行い、設定したアクセス権限を「アクセス権設定管理台帳」に記録する。
- 5) システム管理責任者は、「アクセス権設定管理台帳」が適切であるかを1ヶ月に一回以上確認するものとする。

9.1.2 情報システム管理責任者によるIDおよびパスワードの管理

IDとパスワードを情報システム部門で管理する場合

- 1) 情報システム管理責任者は、情報システム利用者の管理を行う。
- 2) 情報システム管理責任者は、情報システム利用者にIDとパスワードを付与する。
- 3) 情報システム利用者から自己のIDまたはパスワードの開示等の問い合わせがあった場合、対面した上で必ず本人であることを確認した上で回答する。
- 4) パスワードは容易に類推できないもので6文字以上の英数字とする。
- 5) パスワードは3か月毎に更新するものとし、情報システム管理責任者が期限の1週間前までに情報システム利用者に更新勧告の通知をするものとする。

更新期間は、利便性を損なわない範囲で短期間が望ましいです。

IDだけを情報システム部門で管理する場合

- 1) 情報システム管理責任者は、情報システム利用者の管理を行う。
- 2) 情報システム管理責任者は、情報システム利用者にIDと仮パスワードを付与する。
- 3) 情報システム利用者から自己のIDまたはパスワードの開示等の問い合わせがあった場合は、対面した上で必ず本人であることの確認した上で、IDと仮パスワードを発行する。
- 4) 情報システム利用者は仮パスワードでログインし、ただちに本パスワードを登録するものとする。パスワードは容易に類推できないもので6文字以上の英数字とする。
- 5) 仮パスワードの有効期間は1週間とする。
- 6) 本パスワードの有効期間は3か月とし、情報システム利用者が随時更新できるものとする。

更新期間は、利便性を損なわない範囲で短期間が望ましいです。

9.1.3 情報システム利用者によるIDおよびパスワード管理

- 1) 情報システム利用者は、自己のIDおよびパスワードを他人に口外してはならない。また、メモ用紙などに書き残してはならない。
- 2) システム管理責任者から付与された、IDおよびパスワードにより使用を開始し、以後も情報システム管理責任者が更新したパスワードを使用する。

システム管理責任者から付与された、IDおよび仮パスワードにより本パスワードを登録した後に情報システムの使用を開始し、以後も情報システム利用者本人が更新したパスワードを使用する。

- 3) パスワードは3ヶ月に一度更新する。
- 4) パスワードを入力する際は、他人に盗み見されないように留意する。
- 5) パスワードが他人に漏えいした可能性がある場合は、その旨をシステム管理責任者に報告し、直ちにパスワードの変更を依頼する。

パスワードが他人に漏えいした可能性がある場合は、その旨をシステム管理責任者に報告し、直ちにパスワードを変更する。

更新期間は、利便性を損なわない範囲で短期間が望ましいです。

10. 不正アクセスとアクセス記録

10.1 不正アクセス対策

10.1.1 安全管理策と問題発生時の対応

情報システム管理責任者は、情報システムを不正アクセスから防御するために次の事項の対策を実施するものとする。

- 1) 通信経路は、インターネット回線、インターネットプロバイダを用いる。
- 2) 外部と社内ネットワークの間にはルータ及びファイアーウォールを設置する。
- 3) 外部から社内ネットワークへの無許可のアクセスは認めない。
一般公開用 Web サーバまたはメールサーバ、Proxy サーバ⁶などは非武装地帯(DMZ：Demilitarized Zone)に設置するものとする。
ホスティングサービスを利用しており、外部ネットワークと接続するサーバがない場合は削除して下さい。
- 4) 問題発生時には、システムファイル等に改ざんが行われていないか確認する。また、情報システム管理責任者の判断により必要に応じてこれらの確認を行う。
- 5) ネットワーク上に、特に重要なデータ等がある場合には、フォルダ又はファイル毎にアクセスコントロールを個別に設定する。

10.2 アクセス記録

10.2.1 重要情報に対するアクセス記録

情報システム管理責任者は、個人情報などの重要情報に対するアクセスに対し次の措置を講じる。

- 1) 情報に対するアクセスや操作の成功と失敗の記録（ログ）を随時採取する。
- 2) 定期的に記録（ログ）を分析することで、不正アクセスの早期発見に努める。
- 3) 異常アクセスが認められない場合は、印刷物は直ちに廃棄する。
- 4) 採取した記録（ログ）は漏えい、滅失およびき損から保護する適切な保護策を講じる。

⁶ Firewall の一形態としてプロキシ(Proxy：代理)サーバが存在する。Proxy は自分自身がサーバとして、一見透過なサービスを提供しながら、不正なパケットの通過を拒否する。内部の PC から外部の Web サーバを参照するときの接続形態は、内部 PC→Proxy→Web サーバとなる。PC にとっては Web サーバの代理をして、Web サーバから見れば PC の代理をしている。(Firewall&Forest 参照)

- 5) 採取した記録（ログ）の保存期間は3ヶ月とする。

11. 不正ソフトウェア

11.1 不正ソフトウェアに対する対策

(文中は Windows に付いて記述しておりますので、Mac, Linux, Unix などを使用している場合は、それらの仕組み名で記述してください。)

11.1.1 安全管理策

情報システム管理責任者は、ウイルス等の悪質なソフトウェアから、社内の情報システムを防御するために、次の対策を講ずる。

- 1) 社内で使用するパソコンやサーバには、対策ソフトを導入する。
- 2) 情報システム管理責任者は、対策ソフトの更新情報を随時確認し、バージョンアップがあった際には、サーバから自動的に配信する。
情報システム管理責任者は、対策ソフトの更新情報を随時確認し、バージョンアップがあった際には、情報システム利用者に更新するように通知する。
- 3) 情報システム利用者のパソコンは、毎週自動的にスキャンを実施するように設定する。
職場、業務に応じて頻度を決めて下さい。(1回/週で設定するケースが多いようですが、PCの起動時に自動的にスキャンするケースも多いです。)
- 4) 情報システム利用者は Windows Update の自動更新を「有効」に設定しておき、手動でも随時更新を行う。
- 5) 情報システム管理責任者は、OS のアップデート情報や、不正アクセス、各種攻撃についての情報を常に収集し、必要に応じて社員に対策を指示する。
- 6) 顧客等が外部から持ち込んだパソコン等は、原則として社内ネットワーク及び、コンピュータシステムへの接続を禁止する。ただし、情報システム管理責任者が許可を与えた場合はこの限りではない。

11.1.2 セキュリティパッチの適用

- 1) 情報システム管理者は、情報システムへの適合性を考慮し、OS 等のセキュリティパッチの適用を判断し、情報システム利用者に対し指示を行う。

11.1.3 感染の可能性がある場合

- 1) 情報システム利用者はパソコン等の情報端末やサーバが感染したことにより、システムに悪影響を及ぼしていると考えられる場合、それらを直ちにネットワークから物理的に切断する。
- 2) 情報システム管理責任者に直ちに報告し、その指示に従う。

11.2 社内システムの利用

11.2.1 基本遵守事項

- 1) パソコン等は、利用を許可された者（情報システム利用者）のみが操作可能とし、来

訪者など利用が許可されていない者の使用を禁ずる。

- 2) パソコン等は、原則として会社から貸与されたものを使用し、個人所有のものを社内
に持ち込んで서는ならない。ただし、情報システム管理責任者の許可を得たものは除く。
- 3) 社内のネットワークやコンピュータに外部から接続する事は原則として許可しない
ものとする。ただし、VPN 接続⁷は申請により許可するものとするが、情報システム管
理責任者が構築した方法以外の方法で社外から接続してはならない。
- 4) パソコン等は、許可なく外部に持ち出してはならない。
- 5) 個人情報を含む重要情報は指定のサーバに保管し、パソコン等には作業用の必要最小
限かつ一時的なもの以外は保存してはならない。
パソコン等に保存した重要情報を含むファイルは、作業終了後、直ちに完全削除する。
- 6) パソコン等は、ID とパスワードによるアクセス権の設定を行わなければならない。
- 7) Winny 等のファイル交換ソフトをパソコン等にインストールすることを禁止する。

11.2.2 インターネット利用者の遵守事項

- 1) Web ブラウザは、会社指定のものを利用し、許可なく変更してはならない。
- 2) 業務目的以外のインターネットの利用は禁止する。
- 3) インターネット上の Web サーバを利用した電子メール（フリーメール等）の利用は禁
止する。

ただし、必要に応じて情報システム管理責任者が認めた場合はこの限りではない。

- 4) 許可した Web サイト以外からファイルをダウンロードする場合、情報システム管理責
任者の指示の元に行うものとし、許可なく行ってはならない。ファイルをダウンロー
ドした際には、ウイルスの混入などのチェックを行って安全を確認してから使用する。
- 5) ネットワークを不正アクセスや攻撃等を行う目的で使用してはならない。その際パス
ワードを通知する必要がある場合は、別便にて通知する。

11.2.3 電子メール利用者の遵守事項

- 1) 電子メールソフトは、会社で指定したものを使用し、許可なく変更してはならない。
- 2) 電子メールは業務利用を目的とし、私的利用に関しては原則禁止とする。電子メール
の内容は、必要に応じて会社がチェックできるものとする。
- 3) ファイルを添付して電子メールを送信する際には、添付するファイルに不備、ウイル
スの混入がないかのチェックを行ってから送信する。
- 4) 機密性を要する情報を電子メールで送る際には、送信先メールアドレスには特に注意
する。

⁷ VPN (Virtual Private Network) とは、公衆回線をあたかも専用回線であるかのように利用できるサービス。最近ではもっぱらデータ通信の拠点間接続サービスのことを指し、企業内 LAN を通信キャリアの持つバックボーンネットワークを通じて相互に接続するサービスをいう。専用線と違ってキャリアのバックボーンに「相乗り」する形となり、低コストで拠点間接続が可能となる。バックボーンでは様々な企業のデータが混在して流れることになるが、データは認証や暗号化で厳重に保護・管理されるため、混信や漏えい、盗聴などの危険性は低い。(IT 用語事典 e-Words 参考)

- 5) 添付ファイルを社外に送信する場合、暗号化またはパスワード付き zip 形式（または rar 形式など）で圧縮した上で送信する。
- 6) 送信元が不明な電子メールを受信した場合、添付ファイルまたは電子メール自体を開封せず、情報システム管理責任者に連絡しその指示に従う。
- 7) 複数の取引先など社外の複数の方に同報メールを送る場合は、必ず宛先「to:」を自分のメールアドレスに入力して、送付先全てのメールアドレスを「BCC:」に入力し、メールアドレスがむやみに露出しないようにする。
- 8) その他の障害の場合
情報システム管理責任者に直ちに報告し、その指示に従う。

12. 開発(受託)契約

12.1 契約を締結するときの対策

契約文書に次の事柄を確認し明文化することに留意するものとする。

- 1) 納期、金額
- 2) ハードの開発遅延による追加費用の請求可否
- 3) 納品の場所と、納品物(CD、DVD、USB メモリなど)
- 4) 納品内容 ソース、実行モジュール、仕様書、設計書ほか開発資料、
テスト報告書（テスト計画、テスト環境、テスト項目とテストデータ）
- 5) 権利の所在 委託側、受託側、一部受託側（独自技術）
- 6) オープンソフトを使用するときの定め
- 7) 受注できなかった時の、見積り仕様書の返却義務

12.2 オープンソフトを使用するときの対策

- 1) オープンソフトを使用する場合に委託側の承認を得ること。
- 2) 著作権および権利形態の確認すること。
 - ① 開示が有料/無料か： クレジットの表示
 - ② 開示するものはなにか： ソース、オブジェクト、実行モジュール
 - ③ ソースの改変の可否について
不可、可能、条件付き可能(再配布禁止・改変後登録など)
 - ④ 第3者の権利を侵害していないことの証明を受けること。
権利者発行の使用許諾書の入手などを必要とする。

13. 外部委託契約におけるセキュリティ要求事項

外部委託におけるセキュリティ要求事項は、当事者間での合意された契約書に記載を行い、締結を行う。

- 1) 情報資産に関する業務について、外部委託等を行う場合は、委託を行う組織は事前に脅威を分析し、必要な技術的対策を実施すること。
- 2) 委託等にあたっては、情報システムやネットワークを保護する方法の指定、守秘義務、損害賠償、監督権等のセキュリティ要求事項の遵守について明記した契約を締結すること。
- 3) 委託等を行う組織は外部契約先におけるセキュリティ要求事項の遵守について、定期的に確認すること。
- 4) 外部契約先が契約条件のセキュリティ要件を遵守していないことが明らかになった場合の契約の打ち切りや、すみやかな回復措置の実施について契約条件として契約書に明記すること。

14. 機密保持誓約書（従業員）

14.1 従業員の義務と責任

情報セキュリティについて従業員の義務と責任を明確にするために、従業員は「機密保持誓約書」にある内容について承諾し、署名捺印して会社に提出するものとする。

14.2 機密保持誓約書の留意点

「機密保持誓約書」では次の事柄などを確認するものとする。

- 1) 当社のすべての情報資産は、当社の許可なく持ち出さないこと、ならびに第三者に一切開示または提供しないこと。
- 2) 当社が保有する情報資産を定められた利用目的以外の目的で使用しないこと。
- 3) 情報資産を、偽りその他不正の手段により入手しないこと。
- 4) 情報資産を、改ざんあるいはき損、破壊等に類する行為をしないこと。
- 5) 当社が顧客および取引先などの第三者より入手したすべての情報資産は、その第三者との契約および、当社の諸規程ならびに法令等に従い取り扱うこと。
- 6) 機密情報が含まれるすべての媒体および、それらの複写物等を厳重に管理し、機密情報の漏えい防止に努めること。
- 7) 当社に入社する以前に入手した第三者の機密情報を業務に使用しないこと。
- 8) 雇用契約終了時には、会社の業務に関する機密情報を含む資料および、記憶媒体等を会社に返却または、会社の指示に基づき廃棄すること。
- 9) 在職中に知り得た機密情報については、雇用契約終了後においても就業規則および関係法令に違反する行為を行わないこと。

15. 情報セキュリティの事象及び弱点の対策 (障害、不具合、事件、事故)

15.1 情報セキュリティの事象(障害、不具合、事件事故)及び弱点の報告

関連法に対する違反ならびに、セキュリティ上の要求事項の違反に対しての対策を規定する。

15.1.1 報告

- 1) 従業者は、当社において情報セキュリティ事象・インシデントが発生した場合、または弱点：セキュリティ欠陥、若しくはその脅威や疑い（事故が起こる可能性）を知見した場合は、部門管理者を通じて速やかに情報セキュリティ管理事務局長と情報セキュリティ管理責任者に報告を行うものとする。その場合、独自に判断し解決を図ってはならない。
- 2) 事象と弱点の例
 - ① サービス、装置又は施設の停止
 - ② システムの誤動作又は過負荷
 - ③ 人による誤り
 - ④ 個別方針又は指針の非順守
 - ⑤ 物理的セキュリティの取決めに対する違反
 - ⑥ 管理されていないシステム変更
 - ⑦ ソフトウェア及びハードウェアの誤動作
 - ⑧ アクセス違反など
- 3) 従業者は、ウイルス感染や不正アクセスの被害の恐れがある場合は、速やかに対象システムをネットワークから切り離し、情報セキュリティ管理事務局に報告を行い指示に従うものとする。

15.1.2 対策の立案と実施

- 1) 情報セキュリティ管理事務局は報告に基づき、業務に与える影響と被害規模を算出し対応策を立案実施するものとする。
- 2) 情報セキュリティ管理事務局は対応したすべての結果について、情報セキュリティ管理責任者に報告を行うとともに、再発防止策を策定し必要があれば本基準を
- 3) 対応策等についての指示については、報告指示体制に従い速やかに実施しなければならない。
- 4) 報告指示体制のレベルの分類
 - ① レベル1（深刻度：低）
問題の発生原因・被害の範囲とも一部門に限定される場合。 → 部門
 - ② レベル2（深刻度：中）
セキュリティ侵害により、会社全体が被害者となる場合。 → 会社全体
 - ③ レベル3（深刻度：高）
顧客や取引先等に被害を与えた場合。 → 顧客
情報セキュリティ管理責任者は、必要に応じて監督諸官庁、警察、コンピュータ緊急対応センター（例－IPA：情報処理推進機構）等にも報告を行う。

16. 適用法令の順守

刑法及び民法などの関連法に対する、違反ならびに、セキュリティ上の要求事項の違反をさけるため適用法令を明確にする。

16.1 適用法令及び社内規程の維持管理

- 1) 情報セキュリティ推進事務局は、管理部と連携し維持管理を行う。
- 2) 情報セキュリティ推進事務局は、新たな法律及び変更があった場合は、情報セキュリティ委員長に報告し、本情報セキュリティ対策基準を見直して、必要に応じて改訂する。

16.2 適用法令の識別

順守すべき適用法令について「表 15.1 適用法令」に示す。

表 15.1 適用法令

区分	法令名	概要
通信の秘密	電気通信事業法	第4条（秘密の保護） 電気通信事業者の取扱中に係わる通信の秘密は、侵してはならない。 電気通信事業に従事する者は、在職中電気通信事業者の取扱中に係わる通信に関して知り得た他人の秘密を守らなければならない。その職を退いた後においても、同様とする。
知的財産	著作権法	著作権や意匠権、商標など、知的財産権に係わる問題について、それを侵害した場合には罰則が適用される場合がある。中でもソフトウェアの著作権については、私用許諾条件及び契約などを確実に遵守する必要がある。

不正行為 犯罪行為等	不正アクセス行為の禁止等に関する法律	電気通信回路を経由して他人の識別情報（IDやパスワードなど）を利用して、権限を有していないシステム・ネットワークに侵入することを禁止している。また、情報資産の重要度に関わらず、不正アクセスを助長する行為（他人の認証識別情報を無断で提供する行為）も禁止されている。これらに違反した場合は、罰則が適用される。また、アクセス制御機能を管理する者は、識別情報を適切な管理と有効性の検証、必要に応じた高度化についての努力義務がある。
	不正競争防止法	企業など正当な保有者の有している機密情報が不正使用・開示される場合、「事業者間の不公平な競争」を防止するために、企業など正当な保有者が不正使用の差し止め請求を行える。その保護を受けるための前提条件として、「機密情報を客観的に秘密として管理していること」が必要とされる。 営業秘密管理指針（経産省） 「営業秘密」とは、①秘密として管理されていること、②有用な情報であること、③公然と知られていないことの3つの要件を満たす技術上、営業上の情報である。

不正行為 犯罪行為等	刑法	第 161 条の 2（電磁的記録の不正作出及び共有） 第 234 条の 2（電子計算機損壊等業務妨害） データを損壊し、もしくはコンピュータに虚偽の情報もしくは不正の指令を与えるなどして、人の業務を妨害する行為を禁じている。 第 246 条の 2（電気計算機使用詐欺） コンピュータに虚偽の情報もしくは不正の指令を与えて不実のデータを作り、または虚偽のデータを人の事務処理の用に供して、財産上不法の利益を得、またはこれを得させる行為を禁じている。 第 258 条（公用文書等毀棄）／第 259 条（私用文書等毀棄） 公務所の用に供する電磁的記録／権利または義務に関する電磁的記録の損壊行為を禁じている。
	公益通報者保護法	国民生活の安心や安全を損なうような企業不祥事が相次いで起きており、その多くが内部の関係者からの通報で明らかになっている。こうした法令違反行為を労働者が通報した場合、解雇等の不利益な取扱いから労働者を保護し、事業者の法令遵守（コンプライアンス）を確保しなければならない。

個人情報保護	個人情報保護法	本人の意図しない個人情報の不正な流用や、個人情報を扱う事業者がずさんなデータ管理をしないように、一定数以上の個人情報を取り扱う事業者を対象に義務を課している。本人の了解なくして個人情報の流用や売買、譲渡は規制されることになる。国の定める一定数以上の従業員を持つ企業体や、大量のカルテを有する医療機関など、個人情報をデータベース化（電子情報、紙データを問わない）する事業者は、個人情報を第三者に提供する際に、利用目的を情報主体（本人）に通知し了解を得なくてはならない。また不正流用防止のための管理を行う義務が発生する。
労働者派遣法	労働者派遣法	労働者派遣事業の適正な運営と派遣スタッフの就業条件の整備、雇用の安定、福祉の増進などを守るための義務を課している。

17. 本基準の見直しと改訂

17.1 定期見直し

情報セキュリティ管理責任者は、原則として最低年1回は情報資産の棚卸し及び重要度評価の見直しを行うものとする。（リスク管理規程）

17.2 適宜見直し

次に該当した場合は17.1に関わらず適宜検討の上、本基準を見直し改訂するものとする。

- 1) セキュリティ事件・事故が発生した場合。
- 2) 社内システム・ネットワークに変更等があった場合。
- 3) 社外からの情報により、新たな脅威または脆弱性が見つかり、管理方法の変更が必要な場合。
- 4) 協力会社や顧客等ステークスホルダーから、申し入れがあった場合。

18. 附則

作成者、承認者、制定日

18.1 作成者、承認者

本基準は、情報セキュリティ管理事務局が作成し、情報セキュリティ管理責任者が承認する。

18.2 制定日

本基準は 20__年 __月 __日に制定する。

リスク管理規程(サンプル)

(v0.93 2010.03.01)

株式会社

ご利用上の注意

- * 本基準はサンプルとして作成しております。組織内で規程類を作成する場合に参考にして頂きご利用願います。
- * 本書にある灰色でマークの部分は選択/修正/削除をご検討下さい。
- * 本書にある下線付き斜体の部分は注釈です。完成時には削除願います。
- * 本書では、1項目の場合でも項番を付けております。ご利用時に項番の追加/削除をご検討下さい。

制定日：20__年__月__日

承認	作成

目次

1. 総則	1
1.1 規程の位置付け.....	1
1.2 目的.....	1
1.3 適用範囲.....	1
1.4 対象者.....	1
1.5 用語の定義	1
2. 情報資産の棚卸し.....	2
2.1 情報資産の保護責任.....	2
2.2 情報資産の調査.....	2
2.3 情報資産の調査・記録.....	3
3. 情報資産の重要度評価.....	4
3.1 評価範囲	4
3.2 評価基準	4
3.3 情報資産の区分.....	5
4. 管理レベルの分類.....	6
4.1 管理レベル分類と情報資産管理台帳	6
4.2. 情報資産管理台帳作成フロー	8
5. 情報資産の棚卸しと重要度評価の見直し.....	9
6. 改訂履歴	10

1. 総則

1.1 規程の位置付け

本規程は、情報セキュリティ対策の基本規程である「情報セキュリティ対策基準」に基づき、適用範囲における情報セキュリティ対策を実施及び改善、維持するためのリスク管理のプロセスと手法及び、責任について定めた規程である。

本書では組み込みシステム業界向けに、リスクアセスメントを極力簡便に出るように手順を簡略しております。

本格的なリスクアセスメントを、検討される場合は下記¹JIPDECのホームページを参考にして頂き、自社に合ったリスクアセスメントをご検討願います。

ISMS ユーザーズガイド-JIS Q 27001:2006 (ISO/IEC 27001:2005) 対応-

<http://www.isms.jipdec.jp/doc/JIP-ISMS113-21.pdf>

ISMS ユーザーズガイド-JIS Q 27001:2006 (ISO/IEC 27001:2005) 対応-

-リスクマネジメント編-

【本文】 <http://www.isms.jipdec.jp/doc/JIP-ISMS113-21.pdf>

【付録1】 <http://www.isms.jipdec.jp/doc/JIP-ISMS113-11apl.pdf>

1.2 目的

本規程は、対象組織に様々な形態で存在する情報資産を明確にし、対象となる情報資産の重要度、及び脅威・脆弱性に基づいてセキュリティ管理策を決定し、リスク管理を実施する。また、その手順を明確にすることにより、セキュリティ管理を維持・改善していくことを本規程の目的とする。

1.3 適用範囲

「情報セキュリティ対策基準」に従う。

1.4 対象者

「情報セキュリティ対策基準」で定める適用範囲のすべての従業者とする。

1.5 用語の定義

本規程内で用いる用語の定義は「情報セキュリティ対策基準」に従う。

¹財団法人 日本情報処理開発協会
(Japan Information Processing Development Corporation: JIPDEC)

2. 情報資産の棚卸し

適用範囲の組織が保有する情報資産の棚卸しから、重要資産の抽出までの手順を次の通り定める。

2.1 情報資産の保護責任

すべての情報資産に対して情報セキュリティ管理責任者が責任を持ち。適切な保護を実施するものとし、各情報資産について保有者を明確にする。

2.2 情報資産の調査

1) 情報資産の洗い出し範囲

適用範囲における各従業員が保有するすべての情報資産について、次の分類に従い「情報資産棚卸しシート」に洗い出しを行う。

2) 情報資産の分類

調査に際しては、情報資産を「表 2.1 情報資産の分類表」に従い分類する。

本書にある情報資産の分類を参考にして頂き、企業内での呼称、名称を使用して「表 2.1 情報資産の分類表」に記載して下さい。

表 2.1 情報資産の分類表

情報資産		
No	分類名	情報名
1	顧客/取引先の 営業情報	営業渉外情報 見積り仕様書 見積書 契約書 顧客情報
	技術情報	業務システム・データ 開発システム・データ 開発仕様書・設計書 テスト計画・結果 ソースプログラム
3	社外秘情報	経営計画 稟議・報告書 財務諸表 社内規程集

		通達 連絡文書
4	個人情報	社員名簿、賃金台帳、履歴書 名刺、アドレス帳、
5	通信・メールの情報	本文、添付ファイル 通信文書
6	ソフトウェア	業務システムで使用しているもの 個別で使用しているもの 開発で使用しているもの OS、Office など フリーソフト、シェアソフト
7	ハードウェア	個別パソコン、サーバ 外付け HD、モデム、ルータ、HUB 可搬性媒体（CD、USB メモリ、SSD など） プリンタ、複写機、FAX、携帯電話 エミレータ、測定機器
8	サービス	通信サービス ホスティングサービス 空調、電源など

2.3 情報資産の調査・記録

「情報資産棚卸しシート」を用いて情報資産の保管形態、保管場所、利用者の範囲等(表 2.2 情報資産の属性と説明を参照)について記載する。

表 2.2 情報資産の属性と説明

属性	説明
保管形態	情報資産の保管されている状態 例) 紙媒体、ファイルサーバ、個人用 PC、CD 等 可搬型メディア、録音テープ、ビデオテープ 等

保管場所	情報資産が保管されている場所 例) 鍵付きキャビネット (鍵の有/無) 書棚、個人机の引き出し、保管庫 (鍵の有/無)、 社内物品庫、外部委託倉庫 等
管理責任者	〇〇部長, △△課長等
保管期間	情報資産を保管しておかなければならない期間。 例) 「20XX 年〇月〇日まで」、「〇年間保存」、「永久保存」 等
利用者の範囲	情報資産を配布する社員の範囲、或いはその情報資産に対してアクセス権限を持つ利用者の範囲。 例) 「役職名または個人名のみ」、「部署名」、「社内限り」 等

3. 情報資産の重要度評価

3.1 評価範囲

すべての情報資産の管理レベルを決定するために、その重要度の評価を行う。

3.2 評価基準

評価の際には、情報資産を次の「表 3.1 情報資産の評価項目と評価内容」とおり評価する。

表 3.1 情報資産の評価項目と評価内容

評価項目	評価内容
機密性 (C)	アクセス権のないもの又は、プロセスに対して、情報を使用不可又は非公開にする特性 ※漏えい、盗用の内容に留意が必要なもの
完全性 (I)	情報資産の完全さ及び正確さを保護する特性 ※改ざん、破壊、滅失の留意が必要なもの
可用性 (A)	アクセス権のあるもの又は、プロセスが要求したときに、アクセス及び使用が可能である特性 ※保管庫の鍵の保管、ID・パスワードの管理に留意が必要なもの

評価は次に示す情報資産の区分に基づき評価し、評価結果 (C/I/A のランク値) を、「情報資産洗い出しシート」に記録する。

(4)

3.3 情報資産の区分

情報資産は、機密性(C)、完全性(I)、可用性(A)それぞれについて以下の表に従いランク付けする。

表 3.2 機密性 (C)

ランク	レベル	機密性の分類区分
3	極秘	特定の関係者のみがアクセス可能な情報資産。漏えいした場合、会社又は、部門全体に影響がでるもの。
2	社内	社内一般にアクセス可能な情報資産。(社員及び承認されたスタッフのみが使用できる)。漏えいした場合、自担当のみに影響がでるもの。
1	公開	社外一般にアクセス可能な情報。漏えいした場合に、ほとんど影響がないもの。

表 3.3 完全性 (I)

ランク	レベル	完全性の分類区分
2	高い	情報の内容を変更された場合、会社又は部門全体に影響がでるもの。
1	低い	情報を不正に変更された場合、ほとんど業務の支障はない。

※顧客からの仕様書、契約書などは完全性を2とする。

表 3.4 可用性 (A)

ランク	レベル	可用性の分類区分
2	高い	利用不可能の場合、会社または部門全体に影響がでるもの。
1	低い	一日利用不可能でもほとんど業務に影響がでない。

※開発環境（開発用サーバ、開発ツール、ターゲット、テスト用機材など）は、可用性を2とする。

月1回の点検または、新規プロジェクト着手時、テスト環境構築時に点検を実施する必要がある。

4. 管理レベルの分類

情報資産の重要度評価（C/I/A のランク値）を元に表 4.1 リスク管理レベル分類表により管理レベルを分類し「情報資産洗い出し分類シート」に記録し、管理すべき情報をまとめた「情報資産管理台帳」を作成する。

4.1 管理レベル分類と情報資産管理台帳

情報資産管理台帳で管理する情報資産は、表 4.1 リスク管理レベル分類表に示す「リスク管理レベル」が 2 または 3 のものとする。

表 4.1 リスク管理レベル分類表

リスク管理	リスク管理レベル	機密性 (C)	完全性 (I)	可用性 (A)
管理する	3	3	—	—
	2	2	2	2
管理しない	1	1	1	1

※リスク管理レベル 3 の情報は、機密とし利用者を限定した管理をする。

- 4.1.1 「情報資産洗い出しシート」を元に、表 4.1 リスク管理レベル分類表で「管理する」ものだけを抽出し「情報資産管理台帳」としてまとめ、情報セキュリティ管理責任者が管理方法を承認する。
- 4.1.2 「情報資産管理台帳」に登録した情報資産を「重要資産」とし、その内「表 2.1 情報資産の分類表」に示す「顧客/取引先の営業情報」、「技術情報」、「社外秘情報」、「個人情報」、「通信・メールの情報」を「重要情報」とする。

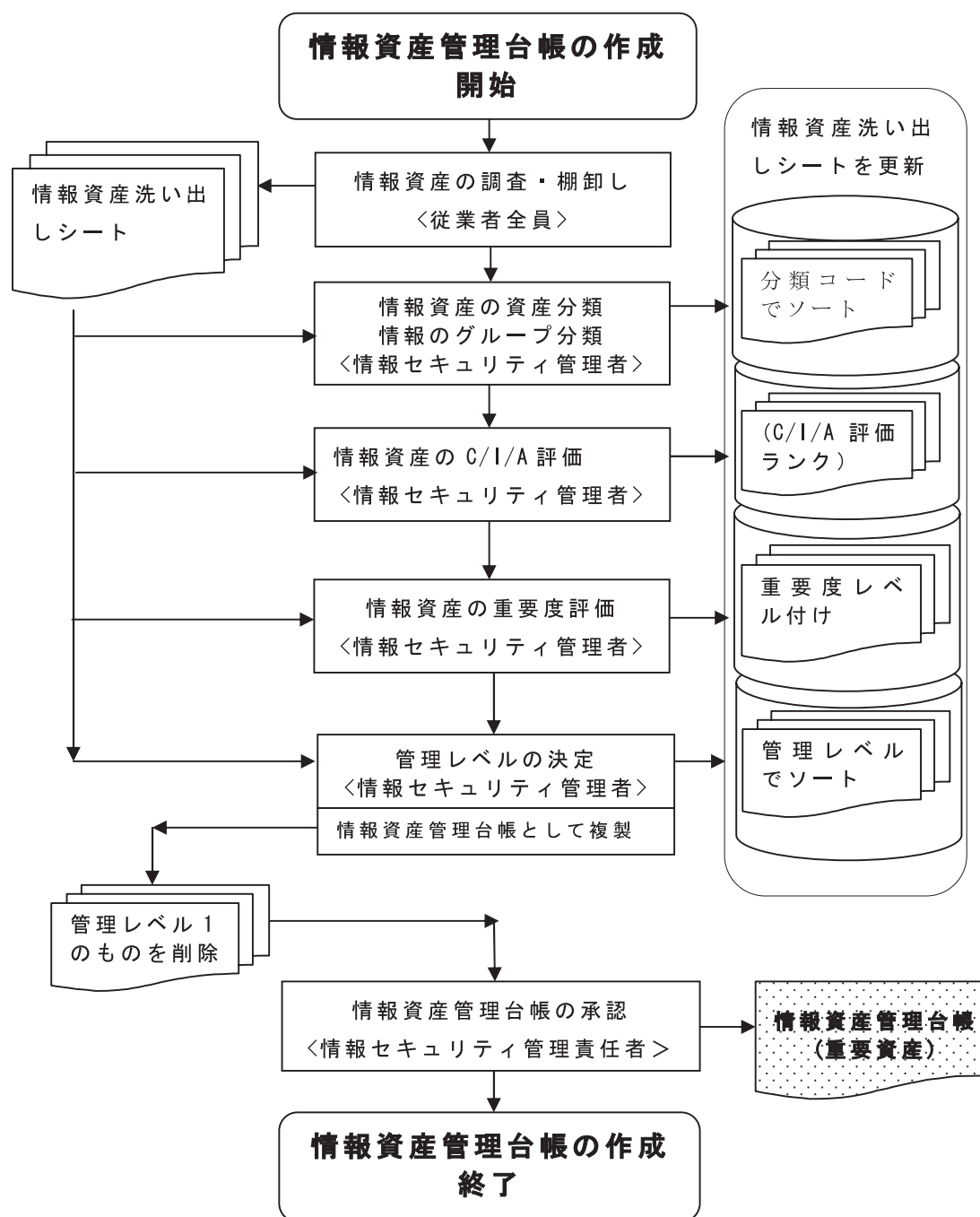
4.2 重要資産の管理

- 4.2.1 重要資産の管理方法は、資産の形態・用途および、それぞれの特性（機密性(C)、完全性(I)、可用性(A)）に合わせた管理をする事とし、次の「表 4.2 想定される脅威・事故事象・損失の例」にある脅威、事故事象に対し、損失が極力最小限になるような方法で、管理しなければならない。

表 4.2 想定される脅威・事象・損失の例

脅威	事象等	損失
1. 災害	ハードウェアの破壊 ソフトウェアの破壊 建物の損壊	コンピュータ機器の買替・修復費用の発生 業務の遅延、停止
2. 故障	ハードウェアの故障 ソフトウェアの故障 通信回線の故障 ライフラインの故障 システム等の故障	コンピュータ機器の修復費用の発生 業務の遅延、停止 企業イメージの低下 機会利益の喪失 賠償責任の発生、信用失墜
3. 過失	オペレーションミス 情報漏えい 回線切断等の事故	業務の遅延や停止 企業イメージの低下 信用失墜
4. 故意 (内部・外部)	コンピュータ関連機器の破壊 ソースプログラムの破壊、改ざん データの破壊、改ざん	コンピュータ機器の修復費用の発生 情報資産の消失
	情報漏えい、ネットワーク侵入 ハードウェアの不正使用	業務の遅延や停止 企業イメージの低下 信用失墜 賠償責任の発生

4.3 情報資産管理台帳作成フロー



※＜＞内は実施者

図 4.1 情報資産台帳作成フロー

5. 情報資産の棚卸しと重要度評価の見直し

情報セキュリティ管理責任者は、原則として最低年 1 回は情報資産の棚卸し及び重要度評価の見直しを行うものとする。

但し、次に該当した場合は、検討の上適宜見直しを実施するものとする。

- (1) セキュリティ事件・事故が発生した場合。
- (2) 社内システム・ネットワークに変更等があった場合。
- (3) 新規に開発環境を構築する場合または、開発環境を変更する場合。
- (4) 社外からの情報により、新たな脅威または脆弱性が見つかり、管理方法の変更が必要な場合。
- (5) 協力会社や顧客等ステークスホルダーから、申し入れがあった場合。
- (6) 会社または事業所が引越しをした場合。

組込みシステム開発企業の情報セキュリティ対策成熟度評価シート(記入用)

v1.0

対象企業名:	総合評価レベル
日付	記入者名:

全ての項目をご記入ください。(第1部 25問、第2部 15問の計40問)
各設問の「レベル入力欄」に各問の選択肢1～5を選択し入力してください。
各問に対して、「利用していない」「禁止している」などで、解答できない場合は「レベル5」として下さい。

※各設問の定義

- 1.「情報システム」とは、業務システム、開発用システムおよび、その環境全般を指します。
- 2.「従業者」とは、経営者や協力会社の常駐社員及び、派遣を含みます。
- 3.「外来者」とは、顧客、ベンダー、運送業者、機器の保守業者、清掃業者などという

管理系について

問1:	情報セキュリティに対する組織的な取組状況について、以下の設問(1)～(7)に、次の選択肢の中から最も当てはまる回答をお選びください。	
設問(1)～(7)の選択肢(各設問の項目ごとに「レベルの入力欄」で1～5の数字を選択してください)		
レベル 1	経営層にそのような意識があるが、方針やルールを定めていない。	
レベル 2	経営層にそのような意識はあり、方針やルールの整備、周知を図りつつあるが、一部しか実現できていない。	
レベル 3	経営層の承認の下に方針やルールを定め、全社的に周知・実施しているが、実施状況の確認はできていない。	
レベル 4	経営層の承認の下に方針やルールを定め、全社的に周知・実施しており、責任者による定期的確認も行っている。	
レベル 5	4.に加え、環境変化をダイナミックに反映し、改善も図っており、他社の模範となるレベルに達している。	

設問1-1	情報セキュリティポリシーや情報セキュリティ管理に関する規程 (ポリシーや規程は、サンプルのコピーではなく、自組織の事業やリスクを鑑みた内容であることが重要です。また、そうしたポリシーや規程を 実践 するためには、定めた規程類を関係者に十分に周知させると共に、規程類の順守状況を 点検 し、必要に応じて 見直す ことが大切です。)	レベル入力欄
1-1-1	情報セキュリティポリシーや管理規程が明文化され、それを実践しているか	
1-1-2	組織内での十分な討議や検討を経て、事業リスクに見合った内容となっているか	
1-1-3	適用範囲は会社全体または、必要な組織全体をカバーしているか	
1-1-4	社長ないし上級役員などの責任者が承認しているか	
1-1-5	全従業者に対して周知しているか	
1-1-6	定期的に見直すための手続を定めているか	
1-1-7	あらかじめ定められた時期や間隔、又は重大な変化が発生した場合に、見直しを実施する内容となっているか	
1-1-8	規程の改訂結果について、社長ないし上級役員などの責任者の承認を得る内容となっているか	
1-1-9	その改訂結果について、組織の長ないし上級役員などの責任者の承認を得て、周知徹底しているか	
1-1-10	従業者に対し就業規則などで、セキュリティに関する就業上の義務を明確にしているか	
1-1-11	組織内の情報セキュリティ対策活動や、情報システムに関する点検しているか	
1-1-12	情報システムが業務以外の目的で利用されることを防止するための、措置を講じる内容となっているか	
1-1-13	情報システムに対し、ネットワークのモニタリングを行うなど、確認する内容となっているか	

組込みシステム開発企業の情報セキュリティ対策成熟度評価シート(記入用)

設問1-2	経営層を含めた情報セキュリティやコンプライアンス(法令順守)の推進体制の整備		レベル入 力欄
	(推進体制を整備するためには、経営層がリーダーシップを発揮すること、各担当者の権限と責任を明文化することなどが重要です。また、法令順守のためには、順守すべき法令を正確かつ網羅的に把握することが必要です。)		
	1-2-1	情報セキュリティ委員会など意思決定をする組織を設置しているか	
	1-2-2	その組織は、ルールを決定したり、各部署の活動を調整したりする組織であるか	
	1-2-3	その組織の責任者は経営層の人間が担当しているか	
	1-2-4	その組織において、情報セキュリティに関する適切な責任や資源配分を検討しているか	
	1-2-5	単独行動による不正行為を牽制するため、職務や権限を適切に分離しているか	
	1-2-6	関係当局や情報セキュリティの専門家などの情報収集体制を構築しているか	
	1-2-7	事業遂行上の関係法令、基準、規制などを収集しポリシーなどの加筆修正する内容となっているか	
	1-2-8	オープンソースソフトウェアなど第三者の知的財産権を保護するための手続を定めているか	
	1-2-9	その手続に発注者の了解を求める内容になっているか	
	1-2-10	個人情報(名刺等も含む)を保護するために必要な対策を定めているか	
	1-2-11	その対策を定め、実施状況を確認しているか	
	1-2-12	不正競争防止法の保護情報要件(営業秘密など)を、経産省の参考文書をポリシーに添付するなどして周知しているか	
	1-2-13	入退室記録、重要情報の持出・返却記録、事故・事件の対策記録などの記録を残す仕組みがあるか	
1-2-14	特に法定の保存文書(開発契約書など)について、施錠管理など厳格な管理を実施しているか		
設問1-3	重要な情報資産について、レベルごとの分類、さらにレベルに応じた表示や取扱をするための方法の整備。		レベル入 力欄
	(情報資産をその重要性に応じて管理するためには、レベル分けし、レベルに応じた表示や取扱方法などを定め、その情報の管理責任者を定める必要があります。)		
	1-3-1	重要な情報資産は、情報システムのハードウェアやサービスを含めてその目録(台帳)を作成しているか	
	1-3-2	情報資産の管理責任者を明確に定めているか	
	1-3-3	情報資産の重要性に応じた分類及び取扱方法を定めているか	
	1-3-4	情報システムから出力した情報についても、重要性のレベルや取扱が明確になっているか	
	1-3-5	上記1-3-3の分類及び取扱方法に従った表示をしているか	
1-3-6	情報資産を利用できる部署や人などを特定しているか		
設問1-4	重要な情報について、入手、作成、利用、保管、交換、提供、消去、破棄等の業務プロセス毎の適切な措置		レベル入 力欄
	(適切な措置とは、業務プロセスごとの作業責任者や作業手順の明確化、取扱者の限定、処理の記録や確認などを指します。また、業務プロセスは、手作業で行うか、情報システムに依存するかを問いません。)		
	1-4-1	各業務プロセスの作業責任者を明確化しているか	
	1-4-2	各業務プロセスの作業責任者は各業務プロセスの作業担当者を限定し、権限付与の状況を確認しているか	
	1-4-3	重要情報のアクセスの記録・保管、権限外作業の有無の確認しているか	
	1-4-4	重要な情報について、漏えいや不正利用を防ぐために、保護対策方法を定めているか	
	1-4-5	その保護対策方法には、重要な情報が消失、変更、誤用されないように、考慮した運用方法を定めているか	
1-4-6	その保護対策方法には、組織内外での情報交換についてのルールと手順を定めているか		
設問1-5	外部組織に業務や情報システムの運用管理を委託(ホスティングサービスなど)する際の、契約書に記載するセキュリティ上の要件。		レベル入 力欄
	(セキュリティ上の要件とは、たとえば情報の漏えいや消失、情報あるいは情報システムの誤用などの防止を指します。)		
	1-5-1	運用管理の委託契約書に、業務内容、サービスレベル、重要情報の安全措置や機密保持などの責任を明確に記載しているか	
	1-5-2	運用管理の委託業務の確実な実施や委託先でのセキュリティ対策実施状況を報告や記録により確認しているか	
1-5-3	運用管理の委託業務内容の変更について把握する仕組みがあり、変更を記録しているか		

組込みシステム開発企業の情報セキュリティ対策成熟度評価シート(記入用)

設問1-6	従業者(派遣を含む)に対する人事異動時の守秘義務の書面など、セキュリティに関する就業上の義務の明確化。 (従業者に情報セキュリティについての要求を順守させるためには、従業者の管理責任者を明確にし、就業規則や服務規律などに明示するなどして、従業者が順守すべきルールなどを明確にし、それらを周知させておく必要があります。さらに、退職や異動に際しては、貸与した資産の返却を確認すること、付与したアクセス権限を削除することも大切です。)	レベル入力欄
	1-1-1	
	1-6-2	
	1-6-3	
	1-6-4	
	1-6-5	
	1-6-6	
	1-6-7	

設問1-7	全従業者(経営層や派遣を含む)に対する、情報セキュリティに関する計画的な教育や指導の実施。 (従業者に対する教育は、情報セキュリティ対策の有効性を向上させるために必要不可欠です。関係者全員に対する教育を適切に実施し、その効果が得られていることを確認することによって、技術的なセキュリティ対策との相乗効果を期待できます。特に、保護すべき情報資産へのアクセス管理を確実なものとするために、パスワードや鍵の管理の徹底はとても大切です。情報セキュリティ教育は、全員に漏れなく定期的に行うことが大切です。セキュリティ対策上の順守事項、禁止事項の徹底とともに、情報セキュリティの脅威と対策についての教育も必要です。)	レベル入力欄
	1-7-1	
	1-7-2	
	1-7-3	
	1-7-4	
	1-7-5	

問2:	物理的(環境的)セキュリティ上の施策について、以下の設問(1)～(4)に、次の選択肢の中から最も当てはまる回答をお選びください。	
設問(1)～(4)の選択肢(各設問の項目ごとに「レベルの入力欄で1～5の数字を選択してください」)		
レベル 1	方針やルールを明文化しておらず、実施もされていない。	
レベル 2	方針やルールの整備、周知を図りつつあるが、一部しか実現できていない。	
レベル 3	方針やルールを定め、全組織に周知・実施しているが、記録等による実施状況の確認はできていない。	
レベル 4	方針やルールを定め、全社的に周知・実施しており、責任者が記録等による実施状況の確認も行っている。	
レベル 5	4.に加え、周囲の環境変化をダイナミックに反映し、常に改善を図っており、他社の模範となるべきレベルに達している。	

設問2-1	特にセキュリティを強化したい建物や区画に対しての、セキュリティ対策の実施。 (重要な情報や関連する設備が数多く存在する場所については、セキュリティ対策として特段の配慮が必要となります。このような場所(建物や区画)については、入室可能な人をできるだけ制限したり、外部からの侵入者に対する防護策を強化したりすることが必要です。対策としては、間仕切りやゲートを設けるなどして、境界を明確にし、入退館や入退室管理を実施する、あるいは警報装置の設置などを行います。また、荷物の受渡し場所や外部者の作業場所の確保、外来者の来訪履歴の	レベル入力欄
	2-1-1	
	2-1-2	
	2-1-3	
	2-1-4	
	2-1-5	
	2-1-6	
	2-1-7	

組込みシステム開発企業の情報セキュリティ対策成熟度評価シート(記入用)

設問2-2	顧客、ベンダー、運送業者、清掃業者など、建物に出入りする外部の人々についての、セキュリティ上のルール制定と実践 (建物や事務所の中には、数多くの情報や関連する設備が所在しているので、これらの情報や設備に触れる機会のある外来者に対しては、それぞれのリスクの状況に応じたルールの制定と、それに従った運用を行う必要があります。自組織の建物や事務所には、思ったよりも多くの外来者が出入りしている事があります。そうした外来者に守って頂くべきルールをあらかじめ定めておくことが重要です。)	レベル入力欄	
2-2-1	外来者の出入りによるリスクに対して適切な対策を定めたか		
2-2-2	外来者が建物内や室内で作業する場合、適切な管理の下で作業を行わせているか		
2-2-3	立ち入りを許した区域内(オープンスペース)で、外来者との対応を実施しているか		
2-2-4	顧客との打合せ場所および、案内時の動線や行動範囲などにおいて、セキュリティエリアを決めているか。		
設問2-3	問1-3 重要な情報機器や配線などを、自然災害や人的災害などを配慮した配置、または設置および保守。 (重要な情報機器や配線については、偶発的な事故による損壊や外部の者による盗み見や損壊を防ぐなど、安全上の配慮が必要です。偶発的な事故に対しては、機器の転倒防止、漏水被害対策、周辺での飲食禁止、踏みつけや引っ張りによる断線の防止など、設備本体や周辺で起こりうる事故を洗い出し、それらに備えた対策を行うことが重要です。また、外部の者による盗み見や損壊に対しては、機器や配線などに、容易に接触できないようにすることが重要です。安全性に配慮した配置または設置とは、たとえば、重要なシステムの安全な場所への設置、盗み見の防止や盗聴防止などに配慮した設置、配線類の地下や床下への埋設、浸水、火災、地震などを考慮した配置などをいいます。)	レベル入力欄	
2-3-1	機密情報を保有している情報システムなどを、許可者のみがアクセスできる安全な場所(施錠可能なサーバーラックなど)に設置しているか		
2-3-2	セキュリティエリアの入口から、情報処理設備などが見えないように配置または設置しているか		
2-3-3	情報システム等のディスプレイモニタは、画面盗視されないように配置を工夫しているか		
2-3-4	損傷や盗聴等に配慮して、電源コード、通信ケーブル、HUB、アクセスポイントなどを適切に配置しているか		
2-3-5	情報システムは、地震による転倒防止、水漏れの予防、停電時の代替電源確保等を実施しているか		
設問2-4	重要な書類、モバイルPC、記憶媒体などについてのセキュリティ管理。 (書類や電子的な記憶媒体などによって情報が漏えいする事故が数多く発生しています。これらを防止するための適切な管理とは、たとえば、保管キャビネットの施錠やプリント出力の放置禁止、記憶媒体の粉碎廃棄などを言います。また、重要な書類には、情報システムに関する文書を含みます。)	レベル入力欄	
2-4-1	重要な書類、モバイルPC、記憶媒体などを適切に管理する事項を定めているか		
2-4-2	重要な書類、記憶媒体などは、物理的に破壊するなどしてから廃棄しているか		
2-4-3	重要な情報やライセンス付きソフトウェア等を格納した装置や記憶媒体を破棄する際は、中のデータを確実に消去しているか		
2-4-4	重要な書類や記憶媒体が紛れ込まないよう、机上、書庫、会議室等の整理整頓を実施しているか		
2-4-5	事務所、机、保管キャビネットなどの施錠管理を実施しているか		
2-4-6	郵便物、FAXの送受信物、印刷物(プリントアウトしたものも含む)などの放置禁止や保護を実施しているか		
2-4-7	情報システムに関する情報も重要書類として取り扱い、施錠管理や適切な廃棄処理などを実施しているか		

組込みシステム開発企業の情報セキュリティ対策成熟度評価シート(記入用)

実施系について

問3:	情報システム(以下開発用システムも含む)及び通信ネットワーク及び開発環境などの運用管理状況に関するセキュリティ対策について、以下の設問(1)～(6)に、次の選択肢の中から最も当てはまる回答をお選びください。	
	設問(1)～(6)の選択肢(各設問の項目ごとに「レベルの入力欄で1～5の数字を選択してください)	
レベル 1	方針やルールを明文化しておらず、実施もされていない。	
レベル 2	方針やルールの整備、周知を図りつつあるが、一部しか実現できていない。	
レベル 3	方針やルールを定め、全組織に周知・実施しているが、記録等による実施状況の確認はできていない。	
レベル 4	方針やルールを定め、全社的に周知・実施しており、責任者が記録等による実施状況の確認も行っている。	
レベル 5	4.に加え、周囲の環境変化をダイナミックに反映し、常に改善を図った結果、他社の模範となるべきレベルに達している。	

設問3-1	情報システムについての、運用環境や運用データに対する適切な保護対策の実施。 (システム開発には、多数の作業者が関与するなど、大きなリスクが潜在しています。そのため、適切な保護には、開発環境、テスト環境と運用環境の分離、運用システムの変更管理手順の策定・実施、個人情報などの重要なデータを含む本番データの使用制限などが含まれます。)	レベル入力欄
3-1-1	自社の業務システムの開発においては情報システムの運用環境を、開発環境やテスト環境から分離しているか	
3-1-2	受託開発 においては開発環境を業務システムの運用環境から分離しているか	
3-1-3	受託開発 においては開発環境とテスト環境を分離しているか	
3-1-4	個人情報などの重要情報をテストに用いる際、廃棄手続きとその確認方法等を定めているか	
3-1-5	開発したシステムの運用環境への移行時や変更時のトラブル回避のため、運用環境の変更や開発ターゲット(システムやハード)の変更に対する規定を定めているか	
3-1-6	運用環境や開発ターゲット(システムやハード)の変更は、変更内容や、変更作業(過程も含む)を記録しているか	
3-1-7	情報システムの利用状況(サーバのログなど)を適宜把握しているか	
3-1-8	その結果、必要な場合は情報システムの性能や容量の増減管理を行っているか	
3-1-9	業務システムの受け入れについて、予め定めた要求事項や基準が満足されているかのテストを行っているか	

設問3-2	情報システムの運用に際しての、必要なセキュリティ対策の実施。 (情報システムや通信ネットワークの運用管理に必要な情報セキュリティ対策には、情報セキュリティの確保に必要な事項を含む各種手順書の作成、ルールに従った運用の実施とその監視、ログの取得と分析などが含まれます。)	レベル入力欄
3-2-1	システム運用におけるアクセス権の設定などを明文化しているか	
3-2-2	情報システムの安定運用やセキュリティの観点から見た運用手順を定めているか	
3-2-4	情報システムの運用管理の責任者は、その運用状況を点検しているか	
3-2-5	セキュリティ事象、障害、利用者の作業などセキュリティ関連のイベントログを取得しているか	
3-2-6	情報システムや通信ネットワークなどの、設備の使用状況を記録しているか	
3-2-7	その記録を適宜点検し、異常の有無を確認しているか	
3-2-8	不正行為の証拠隠蔽等の目的で、システムログや各種記録が、改ざん、消去されないよう配慮しているか	
3-2-9	正確な時刻管理のため、サーバや端末などの機器類について、常に時刻が同期するよう設定しているか	

設問3-3	不正プログラム(ウイルス、ワーム、トロイの木馬、ボット、スパイウェアなど)への対策の実施。 (不正プログラム対策には、ウイルス対策ソフトを導入し、パターンファイルの更新を適時行うことなどが含まれます。また、定期的なウイルス検査を実施し、万が一問題が生じた場合にとるべき処置を周知しておくことも大切です。)	レベル入力欄
3-3-1	組織内のサーバやクライアントPCに対して、ウイルス対策ソフトを適切に配置しているか	
3-3-2	ウイルスなど不正ソフトのパターンファイルの更新を適切に行っているか	
3-3-3	各サーバやクライアントPCについて、自動的にウイルス検査を行っているか	
3-3-4	情報システム利用者に、ウイルス発見やセキュリティ問題発生時の処置について周知しているか	
3-3-5	外部で使用したPCを内部ネットワークに接続する前に、ウイルス駆除などの(検疫)処理を行っているか	
3-3-6	不正プログラムに攻撃されないよう、OSやアプリケーション(開発用のエディタ、コンパイラなども含む)へのパッチ適用など脆弱性解消を行っているか	

組込みシステム開発企業の情報セキュリティ対策成熟度評価シート(記入用)

設問3-4	導入している情報システムに対する、適切な脆弱性対策の実施。 (適切なぜい弱性対策には、ぜい弱性情報や脅威情報の定期的な入手、不要なサービスの停止といったセキュリティを考慮した設定や、パッチ(修正プログラム)の適用、バージョン管理や構成管理、変更管理などが含まれます。)	レベル入力欄
3-4-1	最新のぜい弱性情報や脅威情報を適宜収集しているか	
3-4-2	脆弱性の拡大や脅威の増大があった場合にはパッチ適用について評価し、パッチ適用などの必要な措置を実施しているか	
3-4-3	パッチの入手は、信頼のおけるソフトウェア開発元に限られているか	
3-4-4	入手したパッチは、評価とテストをして適切に適用されているか	
3-4-5	情報システム導入に際して、情報システムの管理責任者によるセキュリティを考慮した運用設定を実施しているか	
3-4-6	Web サイトの公開にあたっては、不正アクセスや改ざんなどを受けないよう、脆弱性の解消を行っているか	
3-4-7	Web サイトの公開にあたっては、Webページの不正アクセスや改ざんなどについて定期的に検査を実施しているか	
設問3-5	通信ネットワークを流れるデータや、公開サーバ上のデータに対する、暗号化などの適切な保護策の実施。 (適切な保護策には、VPNの使用や重要な情報のSSLなどによる暗号化があります。また、重要な情報を電子メールでやりとりする場合には、情報を暗号化しておくことも効果的です。)	レベル入力欄
3-5-1	外部ネットワークから内部ネットワークや社内情報システムへアクセスする場合、VPN 等安全な通信路を使用しているか (外部ネットワークからの接続を禁止している場合はレベルを5として下さい)	
3-5-2	社内外を問わず、Webブラウザなどで重要な情報にアクセスする際、SSL など暗号化プロトコルを用いてサーバ〜クライアント間の通信データを暗号化しているか	
3-5-3	重要な情報を電子メールでやり取りする場合に、添付ファイルやメッセージそのものの暗号化などで保護しているか	
設問3-6	モバイルPCやUSBメモリなどの記憶媒体やデータを外部に持ち出す場合、盗難、紛失などを想定した適切なセキュリティ対策の実施。 (モバイルPCやUSBメモリなどの記憶媒体の使用場所には、外部のパブリックスペースやリモートオフィス、自宅などを含みます。社外では、社内での利用に比べて盗難や紛失のリスクが高いことを考慮し、外部持ち出しに関する規程を定めたり、強固な認証や暗号化などの対策が必要になります。)	レベル入力欄
3-6-1	モバイルPC やUSB メモリ、CD、SSD(以下可搬記憶媒体)などの使用や外部持ち出しについて、規程を定めているか	
3-6-2	外部に可搬記憶媒体を持ち出す場合、申請制や利用者認証機構、情報の暗号化などで紛失や盗難対策を講じているか	
3-6-3	モバイルPC にログオンする際に、利用者ID とパスワードなどによる認証を実施しているか	
3-6-4	モバイルPC などに保存されているデータを、その重要度に応じて暗号化しているか	
設問3-7	組込みシステムの開発環境を整備しシステムの安全性とセキュリティと品質を向上するための適切な対策の実施 組込みシステムの開発は、多くの場合ターゲットがハードでありハードの開発進捗と並行して開発することになります。そのため変更管理や環境整備の不備などから、セキュリティ事故が発生する頻度が高くなります。また、納期遅延や仕様不備などの手戻りを防止するために、常に整備することが必要となります。	レベル入力欄
3-6-1	コンパイラやリンクモジュール、エミレータなどを開発ターゲットにあわせて整備しているか	
3-6-2	開発環境の利用者を制限したり、開発環境へのアクセスを制限をしているか	
3-6-3	開発環境のネットワークは、外部接続と切り離されているか。	
3-6-4	開発に必要なエミレータやブレッドボードなどのターゲットとの整合性確認をしているか	
3-6-5	開発に必要な、測定機器類のキャリブレーションおよび、メンテナンスを実施しているか	
問4:	情報システムのアクセス制御の状況及び情報システムの開発、保守におけるセキュリティ対策の状況について、以下の設問(1)～(5)に、次の選択肢の中から最も当てはまる回答をお選びください。	
設問(1)～(5)の選択肢(各設問の項目ごとに「レベルの入力欄で1～5の数字を選択してください)		
レベル 1	方針やルールを定めておらず、実施されていない。	
レベル 2	方針やルールの整備、周知を図りつつあるが、一部しか実現できていない。	
レベル 3	方針やルールを定め、全社的に周知・実施しているが、実施状況の確認はできていない。	
レベル 4	経営層の指示と承認の下に方針やルールを定め、全社的に周知・実施しており、かつ責任者による状況の定期的確認も行っている	
レベル 5	4.に加え、周囲の環境変化をダイナミックに反映し、常に改善を図った結果、他社の模範となるべきレベルに達している。	

組込みシステム開発企業の情報セキュリティ対策成熟度評価シート(記入用)

設問4-1	情報(以下データも含む)や情報システムへのアクセスを制限するための、利用者IDの管理、利用者の識別と認証の適切な実施。 (適切な利用者IDの管理には、利用者IDに関する規程の整備、利用者IDの定期的な見直しによる不要なIDの削除や共用IDの利用制限、本来必要ではない特権を設定したIDの発見と見直し、見破られやすい単純なパスワードの設定禁止などが	レベル入力欄
4-1-1	適正な利用者管理のため、利用者IDの登録や削除に関する規程を整備しているか	
4-1-2	その規程にそって、利用者IDを定期的に見直しているか	
4-1-3	利用者の異動や退職により、不要になった利用者IDの無効設定漏れ、IDの不正利用などを定期的に点検しているか	
4-1-4	利用者IDの不正利用を防ぐため、空白のパスワードや単純な文字列のパスワードを設定しないよう、利用者に求めているか	
4-1-5	利用者が情報システムにアクセスするごとに、そのIDとパスワードによる識別と認証を確実に実施しているか	
設問4-2	情報や情報システム、業務アプリケーション、開発用のシステムなどに対するアクセス権の付与と、アクセス制御の適切な実施。 (適切なアクセス権の管理には、あらかじめ方針を定めておき、その方針に基づいてアクセスできる情報システムを利用者ごとに限定すること、利用できる機能を制限すること、利用者のアクセス権をレビューすることなどがあります。)	レベル入力欄
4-2-1	利用者ごとに情報、情報システム、アプリケーション、開発用のシステム等のアクセス権限を適切に設定しているか	
4-2-2	適切な権限付与が行われているか、必要以上の権限付与がないかなど、利用者アクセス権の定期的な確認をしているか	
4-2-3	特に重要情報を格納した情報システムや開発用のシステムについては、一度のアクセスでの利用時間制限等アクセス条件による制御を行っているか(開発用システムでは利用時間制限を解除する機能が必要な場合もある)	
設問4-3	ネットワークのアクセス制御の適切な実施。 (ネットワークへの接続に伴って、接続したネットワーク経由で侵入されるといったリスクが増大します。そのようなリスクを低減するためには、ネットワークへの適切なアクセス制御が不可欠です。ネットワークの適切なアクセス制御には、たとえばネットワークの分割や外部からの接続時の認証などがあります。)	レベル入力欄
4-3-1	外部のネットワークから内部のシステムへアクセスする際(モバイルPCを使用する場合を含む)に、利用者認証を実施しているか(外部ネットワークからの接続を禁止している場合はレベルを5として下さい)	
4-3-2	情報システムや開発用システムへのアクセス制限のために、ネットワークの論理的切り離しや接続制限をしているか	
4-3-3	許可されていないワイヤレスアクセスポイントの設置を禁止しているか(ワイヤレスの接続を禁止している場合はレベルを5として下さい)	
4-3-4	無線LANを利用してネットワークにアクセスする場合に、WPA等の暗号化などセキュリティ対策を実施しているか(ワイヤレスの接続を禁止している場合はレベルを5として下さい)	
4-3-5	内部のネットワークに接続する端末機器を限定するため、ネットワーク接続時に端末認証しているか	
設問4-4	業務システム及び組み込みシステムの開発において、必要なセキュリティ要件の定義と、その設計や実装への反映。 (開発したシステムは、完成した後に改変を加えることは困難で、コストも膨らみます。企画、設計などの初期の段階から情報セキュリティについて配慮することが必要です。そのためには、自組織での開発、外部委託による開発を問わず、開発の際に必要なセキュリティ対策としては、仕様書にセキュリティ上の要求事項を盛り込むこと、設計や開発に際してぜい弱性を作りこまないように配慮すること、ぜい弱性を残さないための適切なシステムテストを実施することなどがあります。)	
4-4-1	利用者の種別と権限の区分、業務フローの交差(複数の役割を持つ人の存在)など、セキュリティ上の要求事項を仕様書に盛り込んでいるか	
4-4-2	条件に合わないデータの入力ができない仕組みなど、入力データに対するチェック機能を適切に実装しているか	
4-4-3	必要な機能の動作確認、誤動作分析、脆弱性分析などにより、業務処理プロセス及び回路制御を適切に実装しているか	
4-4-4	利用する形態に応じて部署単位や職務形態単位などで、情報の保護機能を適切に実装しているか	
4-4-5	出力データの妥当性や表示メッセージの正しさなどに関するチェックを適切に行っているか	
4-4-6	脆弱性をチェックするサービスやソフトウェアなどを利用して、潜在的な脆弱性を取り除いているか	
4-4-7	脆弱性を作り込まないためにセキュアコーディング手法を用いるなど、プログラミング上の配慮がなされているか	
設問4-5	ソフトウェアの選定や購入、情報システムの開発や保守に際して、セキュリティ上の観点から、点検のプロセスごとの実施など、適切なプロセス管理の実施。 (ソフトウェアにセキュリティ上の問題を混入させないための管理が重要。たとえば、選定や購入、開発や保守を外部委託している場合は、ソフトウェアの開発元を確認すること、開発や保守に際しては、ソースコードへのアクセス管理といったセキュリティ対策の実施状況の記録やレビューの記録など、セキュリティ上の観点からの点検が可能かどうかを回答してください。)	レベル入力欄
4-5-1	運用に供する情報システムについて、ソフトウェアの更新、パッチ適用などリスク低減のためのソフトウェア導入や変更に関する手順を整備しているか	
4-5-2	権限のない関係者以外にはソースコードへのアクセスを制限しているか	
4-5-3	ソフトウェアのバージョンや構成の変更に関する手順を整備し、厳重に管理しているか	
4-5-4	ソフトウェアにトロイの木馬などの不正プログラムが組み込まれていないかどうかをチェックしているか	
4-5-5	外部委託によるソフトウェア開発を行う場合、使用許諾、知的所有権などについて取り決めてしているか	
4-5-6	外部委託によるソフトウェア開発で、品質や作業範囲、セキュリティ条件など記載した標準契約書や合意書を用意しているか	
4-5-7	開発や保守を外部委託する場合に、委託先のセキュリティ管理の実施状況を把握できるように取り決めてしているか	

組込みシステム開発企業の情報セキュリティ対策成熟度評価シート(記入用)

問5:	情報セキュリティ上の事故対応状況について、以下の設問(1)～(3)に、次の選択肢の中から最も当てはまる回答をお選びください。	
	設問(1)～(3)の選択肢(各設問の項目ごとに「レベルの入力欄で1～5の数字を選択してください」)	
レベル1	方針やルールを定めておらず、実施されていない。	
レベル2	方針やルールの整備、周知を図りつつあるが、一部しか実現できていない。	
レベル3	方針やルールを定め、全社的に周知・実施しているが、実施状況の確認はできていない。	
レベル4	経営層の指示と承認の下に方針やルールを定め、全社的に周知・実施しており、かつ責任者による状況の定期的確認も行っている	
レベル5	4.に加え、周囲の環境変化をダイナミックに反映し、常に改善を図った結果、他社の模範となるべきレベルに達している。	

設問5-1	万が一システムに障害が発生し、必要最低限のサービスを維持できるようにするため、情報システム(開発用のシステムなども含む)に障害が発生する場合をあらかじめ想定した適切な対策の実施。 (情報セキュリティの重要な要素の一つである可用性に影響を与える事象のうち、影響の度合いが最も大きいのは、情報システム関連機器の障害であると言っても過言ではありません。情報システムに求められる可用性の条件を満たすためには、可用性に関する要求に対応した適切な障害対策機能の情報システムへの組み込みが欠かせません。適切な対策には、たとえばシステムの二重化、バックアップと運用記録の取得、障害対応手順の明確化、外部委託先とのサービスレベルの合意(※可用性とは、情報システムを使う権限のある人がいつでも使えるようにすることをいいます)	レベル入力欄
5-1-1	情報システムの可用性に関する要求(最低限運用しなければならない時間帯や許容停止時間等)は明確で妥当なものか(※可用性とは、情報システムを使う権限のある人がいつでも使えるようにすることをいいます)	
5-1-2	障害対策の実行に必要なバックアップ情報の取得や、運用記録などの確保を適切に行っているか	
5-1-3	事故への即応処理として、障害部分の切り離し、縮退運転、情報の回復や情報システムの復旧など、障害発生時に必要となる機能を情報システムに組み込んでいるか (※縮退運転とは、提供する機能やサービスの対象者の絞り込みなどにより、障害時でも、必要最低限のサービスを提供できるようにすることを言います)	
5-1-4	その組み込んだ機能が、適切に機能することを定期的に確認しているか	
5-1-5	障害発生時の対応手順や、障害対策処理の実施要領(実施責任者の設置、システム復旧処理手順など)を策定しているか	
5-1-6	関係者への障害対応要領の周知や、障害対応のスキルに関する教育や訓練を実施しているか	
5-1-7	情報システムの運用を外部に委託している場合(ホスティングサービスなど)、障害発生時にも所定のサービスレベルが維持されることを、委託先との間で契約書等で相互に確認しているか	
5-1-8	障害の検出や原因分析、対処策の検討などに必要なデータとして、システムの各種ログを取得できているか	

設問5-2	情報セキュリティに関連する事件や事故が発生した際の、必要な行動を適切かつ迅速に実施できるような備え。 (情報セキュリティに関連する事件や事故が発生した場合に、被害の拡大を防ぎ局所化するためには、事件や事故に必要な対応を組織全体で適切かつ迅速に実施できなければなりません。そのためには、事件や事故を想定し、実施すべき作業やその実施要領を確立するとともに、現場の要員がいざというときに対応作業を円滑に実行できるように備えておくことが必要となります。事件や事故への備えには、そうした万が一の場合にとるべき行動をあらかじめ検討しておくこと、検討した結果を文書にまとめて関係者に周知しておくこと、緊急の連絡網を整備すると共に、必要な要員や資機材を揃えられるようにあらかじめ手配しておくことなどがあります。また、個人情報などの漏えいが発生した場合に、影響を受ける可能性のある本人への連絡、主務大臣などへの報告、事実関係や再発防止策の公表などを円滑に進めるため、手順などを整備しておくことも重要セキュリティにかかわる出来事、事件や事故の発生時の対応について、報告手順や実行手順、被害状況の確認、復旧・再開手順など実施要領を定めているか	レベル入力欄
5-2-1	セキュリティにかかわる出来事、事件や事故の発生時の対応について、報告手順や実行手順、被害状況の確認、復旧・再開手順など実施要領を定めているか	
5-2-2	セキュリティにかかわる出来事、事件や事故に関する対応要領を関係者に周知・徹底しているか	
5-2-3	セキュリティにかかわる出来事、事件や事故の発生時の緊急連絡網を含む対応体制を構築しているか	
5-2-4	セキュリティにかかわる出来事、事件や事故への対応に必要なリソースやツールを適切に(正常に移働することを定期的にチェックするなど)準備しているか(※ここでのリソースやツールとは、障害対応要員、障害を記録するためのディスク領域、障害報告機能や分析機能などを指します)	

設問5-3	何らかの理由で情報システムが停止した場合でも、必要最小限の業務継続の措置。 (地震、台風、水害などの自然災害による施設、システム機器、業務アプリケーション、業務データの損壊や、開発環境の破壊、そのほか情報システムに生じた重大事故によって、情報システムが停止し短時間で復旧の目処がたたなくなるような事態の発生が考えられます。万が一、情報システムが停止してしまった場合に備えて、普段は情報システムで行っている業務をたとえば手作業で代替できるように、業務の手順書や様式類をあらかじめ用意しておくこと、またそうした手作業を実施できる場所や資機材を確保しておくこと、さらに手作業で代替できるように要員を訓練しておくことなどが重要です。)	レベル入力欄
5-3-1	情報システムが停止した場合に、自組織の業務に及ぼす影響について検討した事があるか	
5-3-2	各業務の重要度や、業務システムのトラブルがそうした業務に及ぼす影響の大きさについて把握しているか(※BIA:ビジネスインパクトアナリシスの有無)	
5-3-3	情報システムの停止が長期になる場合に備え、業務を継続するための方針やシナリオ(事業継続計画)を策定しているか	
5-3-4	情報システムの長期停止時に必要となる、バックアップシステム/データへの切り替えや業務の手作業への切り替えなどは、何時でも実施できるよう、手順の策定や関係者への周知と訓練を実施しているか	
5-3-5	外部連絡など、情報システムが長期停止の場合に必要なその他の措置についても検討し、実施要領を策定しているか	

附録 2

関係機関、団体などの資料

セキュリティ関係 URL

1. 参考資料 1

- ① 経済産業省「中小企業セキュリティ対策促進事業とは？」
<http://www.jnsa.org/jkusei/sokusin.html>
- ② IPA 「5分でできるセキュリティ診断」
<http://www.ipa.go.jp/security/fy20/reports/sme-guide/documents/sme-shindan-s.pdf>
- ③ IPA「中小企業の情報セキュリティ対策ガイドライン」
<http://www.ipa.go.jp/security/fy20/reports/sme-guide/press.html>
- ④ IPA 組込みセキュリティワークショップ
<http://www.ipa.go.jp/security/event/2007/wses-workshop/>
- ⑤ IPA の組込みセキュリティ関係記事
<http://itpro.nikkeibp.co.jp/article/NEWS/20060518/238408/>
- ⑥ IPA2009 情報セキュリティ白書 3 節「社会や生活の基盤としての組込みシステムセキュリティの現状と課題～自動車、情報家電、制御システムのセキュリティ～」
<http://www.ipa.go.jp/security/publications/hakusyo/2009/hakusho2009.html>
- ⑦ IPA2008 情報セキュリティ白書「ますます進む『見えない化』第 10 位組込み製品の増加」
<http://www.ipa.go.jp/security/vuln/documents/10threats2008.pdf>
- ⑧ 情報セキュリティ Q&A
<http://j-net21.smrj.go.jp/well/security/index.html#q1>
- ⑨ IPA セキュア・プログラミング講座
<http://www.ipa.go.jp/security/awareness/vendor/programmingv2/index.html>
- ⑩ 自動車における組込みセキュリティについて
http://www.ipa.go.jp/security/vuln/documents/200912_SEMI.pdf

2. 参考資料 2

2009 情報セキュリティ白書（IPA 発行）の資料・ツール類

- ① 2008 年のコンピューティングウイルス届出状況
<http://www.ipa.go.jp/security/txt/2009/documents/2008all-vir.pdf>
- ② 2008 年のコンピュー不正アクセス届出状況
<http://www.ipa.go.jp/security/txt/2009/documents/2008all-cra.pdf>
- ③ ソフトウェア等の脆弱性関連情報に関する届出情報
<http://www.ipa.go.jp/security/vuln/report/press.html>
- ④ 2008 年度第 2 回情報セキュリティに関する脅威に対する意識調査
<http://www.ipa.go.jp/security/fy20/reports/ishiki02/index.html>
- ⑤ 組織の情報セキュリティ対策自己診断テスト
<http://www.ipa.go.jp/security/benchmark/index.html>
- ⑥ セキュリティ要件検討支援ツール
<http://www.ipa.go.jp/security/fyl8/development/localgov/>
- ⑦ ウィルス情報データベース「ウィルス情報 iPedia」の公開について
<http://www.ipa.go.jp/security/isg/zha.html>
- ⑧ 脆弱性対策情報データベース（JVN iPedia）
<http://jvndb.jvn.jp/>
- ⑨ SQL インジェクション検出ツール iLogScanner V2.0
<http://www.ipa.go.jp/security/vuln/iLogScanner/index.html>
- ⑩ セキュリティ情報 RSS ポータルシステムの公開
<http://www.ipa.go.jp/security/fyl9/development/rss/index.html>
- ⑪ TCP/IP-に係る既知の脆弱性検証ツール
http://www.ipa.go.jp/security/vuln/vuln_TCPIP_Check.html
- ⑫ LSI 回路解析ツール（開発中：2009 年度公開予定）
<http://www.ipa.go.jp/about/toolcatalog/security/security-08.html>

3. セキュリティ関連用語・教育関係

- ① IPA/SEC サポート情報：用語集
<http://www.ipa.go.jp/security/glossary/glossary.html>
- ② Goo 情報セキュリティ用語辞書
<http://dictionary.goo.ne.jp/infsec/>
- ③ Security&Trust セキュリティ用語事典
<http://www.atmarkit.co.jp/fsecurity/dictionary/indexpage/securityindex.html>
- ④ 情報セキュリティの教育資料
<http://www.jnsa.org/ikusei/>
- ⑤ e-ラーニング
<http://www.jnsa.org/ikusei/learning/Jukou/top.php>
- ⑥ IPA 5分でできるセキュリティポイント学習
http://www.ipa.go.jp/security/vuln/5mins_point/105_themes.html

J A S A 安全性向上委員会

情報セキュリティワーキンググループ委員

漆原	憲博	株式会社ジェーエフピー
三輪	一義	I SMS コンサルタント
済賀	宣昭	東海ソフト株式会社
竹岡	尚三	株式会社アックス
中村	憲一	アップウィンドテクノロジー・インコーポレイテッド
大原	衛	地方独立行政法人 東京都立産業技術研究センター
金田	光範	東芝システムテクノロジー株式会社
岸本	輝昭	岩手県立大学
田向	忠夫	株式会社ジェーエフピー
門田	浩	「IPA・SEC」／日本電気株式会社
前澤	敏昭	(社)組込みシステム技術協会
待山	絵理	(社)組込みシステム技術協会

第 2 部

組込みシステムにおける 機能安全に関する調査研究

機能安全に関する事例研究

社団法人 組込みシステム技術協会

安全性向上委員会

製品安全ワーキンググループ

はじめに

本報告書は、昨年度に引き続き、組込み系の安全に高い関心を持つ JASA メンバーが集まり、編集したものです。

昨年度は、組込み系の安全設計に必要と思われる基本知識や関連規定を調査しましたが、今年度は、各分野の安全施策について、広く事例を集めました。また、安全に関する用語の意味が誤って使われていたり、複数の訳語が存在しているなど、足並みが揃っていない現実も見えてきたので、用語集作成にも挑戦いたしました。

第 1 章は、機能安全の認証概要と自動車、鉄道、原子力、宇宙など分野ごとの安全設計思想と、安全認証（SIL3）を取得した製品の概要について、調査結果をまとめています。分野毎にいろいろ特殊事情もありますが、多くの事例を眺めると、安全設計の基本的なアプローチ方法やキーワードがよく理解できると思います。

第 2 章は、2009 年 11 月から 12 月にかけて、東京開催の展示会とネットを使った調査を行い、安全認証を取得している製品や機能安全関連のツールをリストアップしました。システムの安全設計をゼロから始めるのはたいへんですが、これらの製品を活用するとシステム設計は格段に容易になると思われます。ただ、すべての安全関連製品を集めきったとは言えません。我々の検索・調査から漏れた優秀な製品もあると思います。

第 3 章は、安全設計が非常に普遍的なテーマであるにも関わらず、情報が散在している事情に鑑み、JASA にて集めた安全設計に関する情報の公開を検討するものです。どのような公開方法が有効化さらに議論していきたいと思っています。

第 4 章は、用語集です。安全は業界や技術分野横断的な共通課題であるにも関わらず、用語が統一されていません。信頼性に関する用語については、JIS Z 8115 「ディペンダビリティ(信頼性)用語」があります。しかし、我々組込み産業からみると、IT 系だけでは物足りない部分もあります。それは明治大学の向殿先生も認識されているところでありました。そこで、向殿先生から頂いた用語集も参考にしながら、昨年度報告書や今年度活動の中から用語を拾い出し、編集を試みました。この用語集もまだ発展途上です。来年度もさらに整備していく必要があると思います。

本報告書が、組込み系の開発、特にソフトウェア開発に従事する方々にとって、多少なりとも役に立てば幸いです。

J A S A 安全性向上委員会
製品安全ワーキンググループ
主査 金田 光範

目次

第 1 章 安全性向上に関する活動の事例調査	85
1.1 機能安全認証の概要	86
1.2 制御システムの安全	92
1.3 安全 PLC	105
1.4 自動車の安全	123
1.5 原子力分野の安全性・信頼性対策の概要	134
1.6 ソフトウェアの安全	151
1.7 鉄道の安全	160
1.8 安全規格認証製品	179
第 2 章 安全に関わる製品調査	188
第 3 章 機能安全の Web. その事例と期待効果	210
第 4 章 機能安全に関する用語	215

第 1 章 安全性向上に関する活動の事例調査

近年、多くの製品にコンピュータが組み込まれ、その故障や不具合によって、思いもかけない危険が人に迫ってきている。製品を設計するときは、人間に危害を及ぼすような危険源とならない製品とすることを最初に考える必要があり、これを「本質安全」という。しかし、全ての製品に対して本質安全を設計することは不可能で、制御系をベースとする安全系等によって、一定の安全を確保することが必要となる。この設計思想を「機能安全」という。

1998 年の IEC 61508 制定によって、マイコンやソフトウェアを使って機能安全を実現することが可能になり、組込みシステムでの安全性が議論されることが増えてきた。

そこで第 1 章では、認証動向や認証取得のプロセス、制御系をベースとする安全システム事例や SIL3 認証製品事例などをはじめ、機械、自動車、原子力、鉄道といった各分野の機能安全事例について紹介する。また、機能安全規格の紹介、詳細な資料に基づき、実際の現場での機能安全の進め方や、運用・評価の方法、具体的な認証取得の概要や実際に取得する上でのポイントなどについても紹介する。

1.1 では、製品安全に関する認証動向や認証取得のプロセスについてテュフズードジャパン(株)の事例を基に紹介する。

1.2 では、制御系をベースとする製品安全システム事例やパフォーマンスレベル (PL) の考え方について IDEC(株)の製品事例を基に紹介する。

1.3 では、IEC61508 認証製品についてジェイテクト(株)の製品事例を基に紹介する。

1.4 では、自動車の機能安全の最新動向と対応について日産自動車(株)の事例を基に紹介する。

1.5 では、原子力プラントの制御室設計を通じた信頼性向上についてテクノバ(株)の事例を基に紹介する。

1.6 では、組込ソフトウェア製品の信頼性・安全性の定量的評価法についてビジネスキューブ・アンド・パートナーズ(株)の事例を基に紹介する。

1.7 では、機能安全における鉄道の安全について日本大学中村教授のご見解を基に紹介する。

1.8 では、制御機器の安全について IDEC(株)の製品事例を基に紹介する。

1.1 機能安全認証の概要

本節はテュフズードジャパン株式会社の御協力を得て、2009 年 7 月 17 日に開催された JASA/ET セミナーの竹市正彦氏の講演をベースに他の調査も含めて当委員会がレポートをまとめたものである。

1.1.1 テュフズードジャパンの活動概要

テュフズード (TÜV SÜD) はテュフラインランド (TÜV Rheinland) を上回る世界最大級の第三者試験・認証機関 (民間) である。本社はいずれもドイツにある。TÜV は「Technischer Überwachungs Verein」の略で「技術検査協会」を意味する。

ちなみに TÜV という 1 つのグループがあるわけではなく、テュフズードとテュフラインランドはそれぞれ独立の別会社である。ドイツ国内では地域わりで分担している業界があるが、国際的には完全な競争状態となっている。

テュフズードの沿革は 19 世紀半ば (1866 年)、バイエルン地域の蒸気ボイラー技術検査協会設立に始まる。当時、最新技術の代表であった蒸気ボイラーの爆発事故が多発し、建物の崩壊や多数の死傷者が発生するという惨事が相次いだ。人々から安全性と品質の確保への要求が高まり、蒸気ボイラーの試験・検査を行う組織を立ち上げるようになった。

20 世紀に入り、検査対象の範囲が拡がり、電気機器、機械装置、パイプライン、タンク等広範囲にわたってきた。1926 年には、自動車の情報・検査センターが設立されている。第二次世界大戦後は、製油所、原子力、プラスチック技術の試験・検査も加わり、その後家電、娯楽用品、オフィス用品の型式試験も開始し、個人生活の安全性確保も対象となった。1970 年代には、コンピュータ、マイクロプロセッサ、データの保護等もテュフズードのサービスに追加され、その後、省エネや環境保護に関する研究やアドバイスも行うようになった。1971 年以来、スポーツ用品、手工芸用品、おもちゃ、家電等の検査機関として公式に認定されている。GS マーク (安全性試験)、DIN テストマーク、世界山岳連盟 (UIAA) のテストマークを発行している。

現在は世界に 600 以上の拠点を備え、高度な技術力を持つ 13,000 を超える専門家を抱えている。テュフズードジャパンは 1983 年に設立され、アジアでは 25 年以上の経験を有している。

連絡先：本社 東京都新宿区西新宿 4-33-4 住友不動産西新宿ビル 4 号館 8F

関西本部 大阪府大阪市淀川区宮原 3-5-24 新大阪第一生命ビルディング 10F

Tel : 06-6396-0368

Mail : masahiko.takeichi@tuv-sud.jp

東京試験場 神奈川県川崎市麻生区栗木 2-8-20

URL ; <http://www.tuv-sud.jp/>

(注) 機能安全については主に関西本部が担当している。

1.1.2 機能安全認証サービス

電子システムによって安全関連機能を制御している機器の場合、その信頼性と安全性は、危険の程度に見合ったレベルであることが証明されている必要がある。テュフズードグループは、電子システムに対する信頼性／安全性、すなわち SIL (Safety Integrity Level) の認証書を発行することができる。尚、ISO13849-1 で要求される PL (Performance level) も評価可能である。

テュフズードが安全認証の対象としている主な規格は下記の通りである。

• IEC 61508	電子システムの機能安全
• IEC 62061	機械類の機能安全規格
• ISO 13849-1	機械の安全性—制御装置の安全性関連部品
• IEC 61511	プロセス用アプリケーションの安全規格
• IEC 61131	プログラマブルコントローラ—プログラミング言語

対象製品の主なものとしては下記がある

- PLC
- 産業用ロボット
- ロボット制御機器
- プレス機器
- ガス関連機器
- 車載用電子システム
- 鉄道用 車両・信号システム・コンポーネント
- FA 機器
- 安全計装
- ASIC、FPGA
- センサ、アクチュエータ
- ソフトウェア、ソフトウェアツール、OS 等
- 化学プラント

etc

なお、テュフズードは認証だけでなく、対象製品の試験や評価レポートの発行も提供している。

1.1.3 機能安全規格の要求事項

要求は大きく 4 つに分かれる

- ① FSM (Functional Safety Management)
- ② System Requirement (システム要求仕様)
- ③ Hardware Requirement (ハードウェア要求仕様)
- ④ Software Requirement (ソフトウェア要求仕様)

(1) FSM

FSM は非プロジェクト要件（全社的なマネジメントシステム）と特定のプロジェクト要件の 2 つに分かれる。

非プロジェクト要件としては、以下を要求している。

規格の有効性・利用性

Availability of the valid standards

監査手順

Audit of processes

市場で発見された不良（クレーム等）の分析と監視

Observation and analysis of filed detected faults

実際の故障率と計算上の故障率の比較

Comparison of calculated and effective failure rates

関する人員の IEC61508 に関する教育計画の策定

Training plan of personal (IEC61508)

文書テンプレートの現実化

Actualization of document templates

特定プロジェクトに関わる要件としては以下を要求している。

- ・ 安全ライフサイクル間における全活動の計画・管理

Planning and control of all activities during the safety lifecycle

該当するチームメンバーの責任の定義づけ

Definition of the responsibilities of the team members

文書テンプレートの利用

Usage of document templates

各階段における全活動の文章化及び計画

Planning and documentation of all activities for each phase

安全に関わる確認作業と妥当性検証の文書化及び計画

Planning and documentation of the safety verification and validation activities

安全評価活動の文書化及び計画

Planning and documentation of the safety assessment activities

- ・ 要求事項のトラッキング

Requirements tracking

- ・ 書類審査

Review of documents

(2) システム要求仕様

- ・ 定義、略語

Definitions, Abbreviations

- ・ システムアーキテクチャに対する要求事項

Requirements to the system architecture

- ・ 故障の検出及び制御に対する要求事項

Requirements to the detection and control of failures

- ・ 系統的障害の制御と回避

Avoidance and Control of systematic Faults

- ・ システムレベルでの機能安全性の証明

＝System Block Diagram を使った System-FMEA による証明

Proof of functional safety on system level

(3) ハードウェア要求仕様

- ・ 定義・略語

Definitions, abbreviations

- ・ 危険側故障の制限値に対する要求事項

Requirements to the limits of dangerous failures

- ・ ハードウェアレベルでの機能安全性の証明

Proof of function safety on hardware level

- ・ 回路図レベルでの故障の影響に関する分析

Analysis on the influence of failures on circuit diagram level

- ・ 機能安全上の各部品、及び影響の即知の故障モードによる分析

Analysis of the known failure models of each component and the influence safety

- ・ 達成し得る診断率（DC）と安全側故障比（SFF）の証明

Proof of the achievable DC (Diagnostic Coverage) and

Safe Failure Fraction (SFF)

- ・ 危険側故障の確率計算
Calculation of the probability of dangerous failures
- ・ “故障挿入” 試験 (F. I. T.) による検証
Determination of the according “Fault insertion” tests

(4) ソフトウェア要求仕様

- ・ ソフトウェア安全ライフサイクルの構築
Specific of a software safety lifecycle
- ・ ソフトウェアの品質及び安全性を保証する手法
Measures for the guarantee of quality and safety of software
- ・ 個々の作業におけるライフサイクルの各ステップのセグメント化
Partitioning of each phase of the lifecycle in elementary actions
- ・ 確実な技術と手法の定義 (see Annex A and B of IEC 61508-3)
Definition of adequate techniques and measures
- ・ 活動の文書化
Documentation of the activities
- ・ 職責の明確化
Establishment of responsibilities
- ・ 全ての SRS からの派生と一貫性
Derivation and consistence to the overall Safety
Requirement Specification (SRS)
- ・ ソフトウェア要求機能の説明
Description of the required Software Functions
安全状態を達成するための機能
Functions for achieving the safe state
ハード・ソフトウェアの故障を、発見、表示、対処するための機能
Functions for detection, indication and handling of failures
in hard -and software
オンライン・オフラインの機能
Function for online-and offline-testing
- ・ 非安全関連機能とのインターフェース
Interfaces to non safety relevant functions
- ・ リアクション・パフォーマンスと時間
Performance and time of reaction
- ・ それぞれの安全関連ソフトウェア機能への SIL に基づく割当

SIL allocation to each safety relevant software function

⇒Details see IEC61508-3, table A.1

1.1.4 認証取得の概要

最初に機能安全の認証に関する教育を行った後、大きく七つのフェーズに分けて認証取得作業が進行する。

第 0 フェーズは教育。セミナー、ワークショップ、テクニカル・ミーティングを通じて機能安全プロジェクトの準備を行う。

第 1 フェーズは、安全に関する基本計画や安全要求仕様の確認、FSM の監査 (Audit) などを行う。概ね 2 週間ほどかかる。このフェーズである程度のレベル (100 点満点の 60 点以上) にないと、次のフェーズには進めない。

第 2 フェーズは、ハードウェア、ソフトウェアの各ドキュメントのレビュー、FMEA のレビュー、FIT、安全ライフサイクルの監査などを行う。概ね 5 週間ほどかかる。

第 3 フェーズでは、危険側故障や安全機能の失敗確率の計算や故障モードの解析などをテュフが自ら行う。概ね 2 週間ほどを要する。

第 4 フェーズは、電磁波ノイズテスト、電氣的安全性テスト、環境テストなどを行う。概ね 4 週間を超える作業となる。

第 5、第 6 フェーズは、ユーザー側のドキュメント体系、工場の検査を必要により実施する。作業期間は合せて概ね 1 週間である。

第 7 フェーズは、テストレポートの作成や認証作業を一ヶ月ほどかけて行う。

以上で、最短でも半年ほど必要となるが、一般的には 1 年から 2 年以上かかる場合もあるらしい。

テュフズードジャパンは、製品開発後の認証取得は、ドキュメントの整備や試験のやり直し、設計変更の可能性が高いので、開発開始時から同時に認証の手続きを行う方がはるかに効率が良いと言っている。相談にはいつでも応じるとのことである。

また、認証作業の対象となるドキュメントは、基本的なコンセプトを説明するものは、原則英文での提出が必須となる。図面や試験結果、フィールドデータなど、証拠図書などは、日本語でよいものもあるが、詳しくは、テュフズードジャパンに問合せた方がよい。

<参考資料>

1. 第 14 回 JASA/ET セミナー 2009 年 7 月 17 日

「機能安全シリーズ 第 1 回 製品安全の確保と認証」

http://www.jasa.or.jp/top/activity/jevent/38th_detail.html

2. テュフズードジャパン株式会社ホームページ

<http://www.tuv-sud.jp/>

1.2 制御システムの安全

本節は IDEC 株式会社規格安全ソリューションセンター規格安全推進グループに所属されている前田育男推進リーダーの御協力を得て、レポートをまとめたものである。

1.2.1 IDEC(株)の活動概要

IDEC 社は創業以来 60 年以上、制御を主体としたものづくり技術の研究開発を行っている。ヒューマンマシンインタフェースとしてのスイッチや安全技術、LED やレーザを応用するフォトリソ技術、ものづくりにおいてロボットをフル活用したセル生産技術など、豊富な実績と蓄積されたノウハウで新しい分野を切り拓き、世界各国（欧州、中国、アメリカ等）で信頼のブランドとして高い評価を得ている。

- ①ものづくり次世代生産技術
- ②安全・防爆・規格インテリジェンス
- ③テクノロジーイノベーション・制御技術の進化
- ④トレーサビリティ；新事業・制御との融合

の 4 つのテーマを掲げ、これまでに蓄積された保有技術やソリューション力を資産として、研究開発を推進している。

連絡先：

本社 大阪市淀川区西宮原 1-7-31

Tel : 06-6398-2500

東京本社 東京都港区港南 4-1-8 リバージュ品川 12F

Tel : 03-5782-7690

技術研究センター 大阪市淀川区西宮原 1-7-31

URL ; <http://www.idec.com/>

1.2.2 規格改定について

1.2.2 では、制御システムの安全に関する考え方について最初に紹介する。制御システムの安全に関わる ISO 13849 をベースとした欧州規格 EN954-1（≒ISO 13849-1:1999）が 2009 年 12 月 28 日に新しい規格に移行する（その後の欧州委員会の審議で 2011 年 12 月 31 日に延期）ので、特に大きく変更されるパフォーマンスレベル（PL）の考え方について紹介する。もう少し具体的に説明すると現状の ISO 13849-1:1999 は機械安全の重要な規格の一つである、機械類の安全性-制御システムの安全関連部- 第 1 部：「設計のための一般原則」であり、2009 年でその適用期間を終え、ISO 13849-1:2006 に完全移行することになる。これにより、機械の制御システムの安全レベルは、従来の「カテゴリ」の考え方を残しつつ「信頼性」、「チェック機能」そして「共通原因故障」などが追加されたパフォーマンスレベルという指標で表すように変更されることになる。この、パフォーマ

ンスレベルという指標で表すようにしたところが、今回の規格改定における最大の変更点である。

システムの安全ということでは、例えばドアの開閉時のインターロック装置があるが、こうした安全のための機能は、ロボットを使用した生産システム（図 1.2.1）や半導体製造装置（図 1.2.2）であっても同様である。

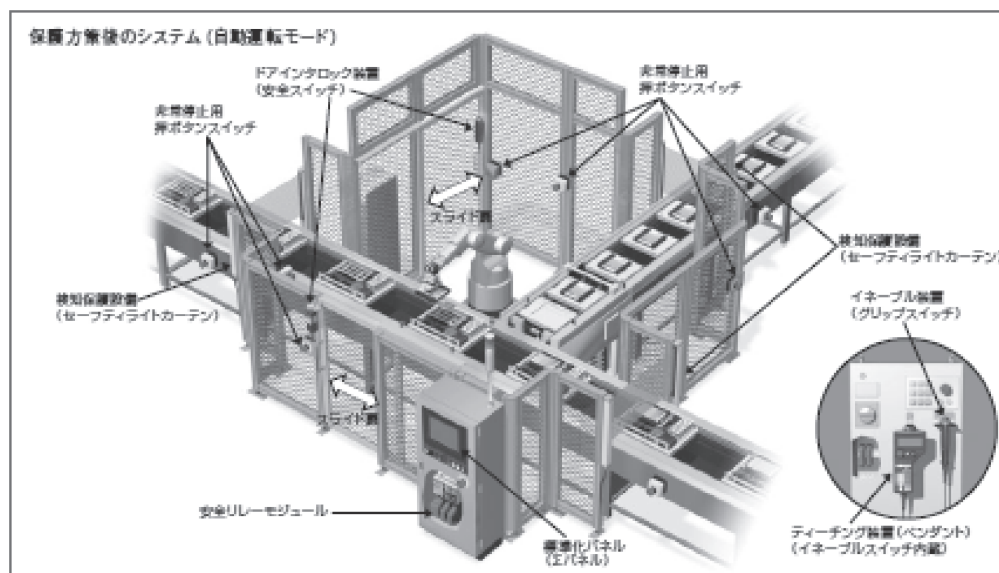


図 1.2.1 安全に配慮したロボットを使用した生産システムの例（出典：IDEC 社資料）

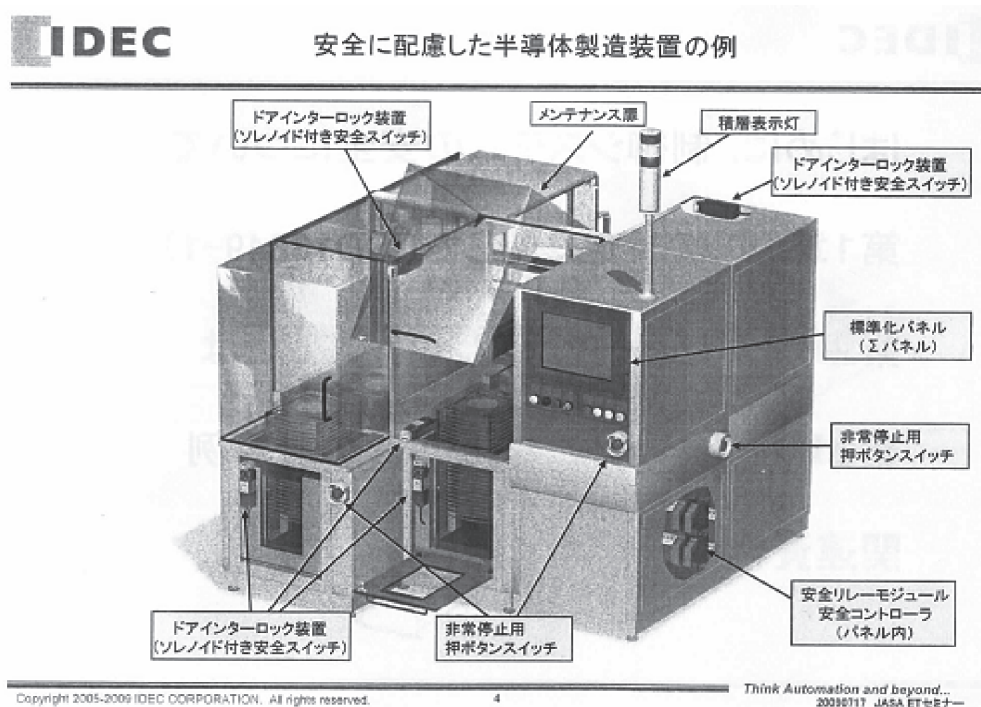


図 1.2.2 安全に配慮した半導体製造装置の例（出典：IDEC 社資料）

機能安全のベースとなる考え方にリスクアセスメントがある。リスクアセスメントは、①機械類の制限の決定、②危険源の同定、③リスクの見積もり、④リスクの評価といった手順（図 1.2.3）で実施する。

リスクアセスメントを実施した結果、リスクの低減が必要となった危険源に対して、リスク低減方策を検討し実施することになる。安全制御装置等はこうしたリスクを減らすために用いられるものである。

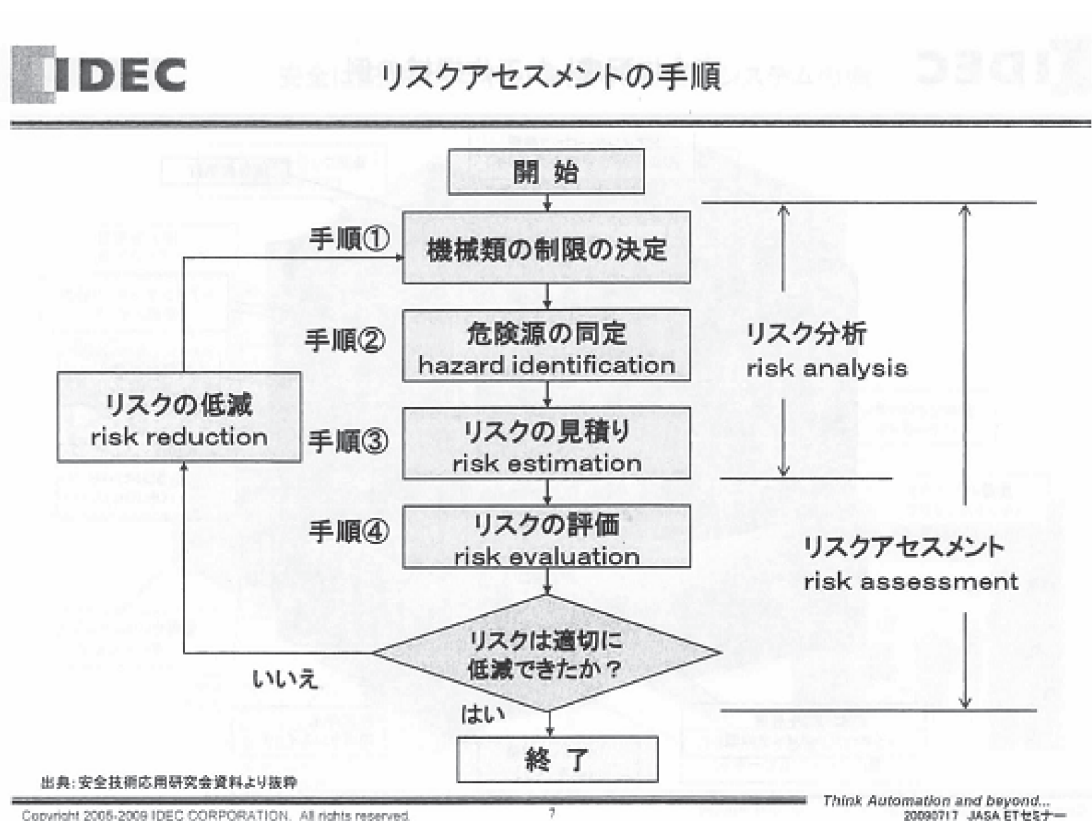


図 1.2.3 リスクアセスメントの手順（出典：IEEC 社資料）

リスクを低減するための手法（図 1.2.4）として、3 ステップメソッドと呼ばれる手法がある。この方法論に関しては、ISO 12100/JIS B 9700 に記載されている。

3 ステップメソッドは、設計の段階で事故が起きないように危険を排除する設計を行うための「本質的安全設計方策」、それでも十分低減できないリスクから人を保護するために、安全防護物や非常停止手段等によって保護を行うための「安全防護及び付加保護方策」、以上 2 つの方策を行ってもまだ残ってしまう残留リスクに関して、その情報を使用者に伝え、さらにリスクを低減させる方策としての「使用上の情報」の 3 つから成る。

また方策実施にあたっては優先順位があり、「本質的安全設計方策」をステップ 1、「安全防護及び付加保護方策」をステップ 2、「使用上の情報」をステップ 3 とすると、

ステップ 1>ステップ 2>ステップ 3 の順となる。こうした安全設計のためのステップや考え方は、組込みシステムを設計する上でも重要である。

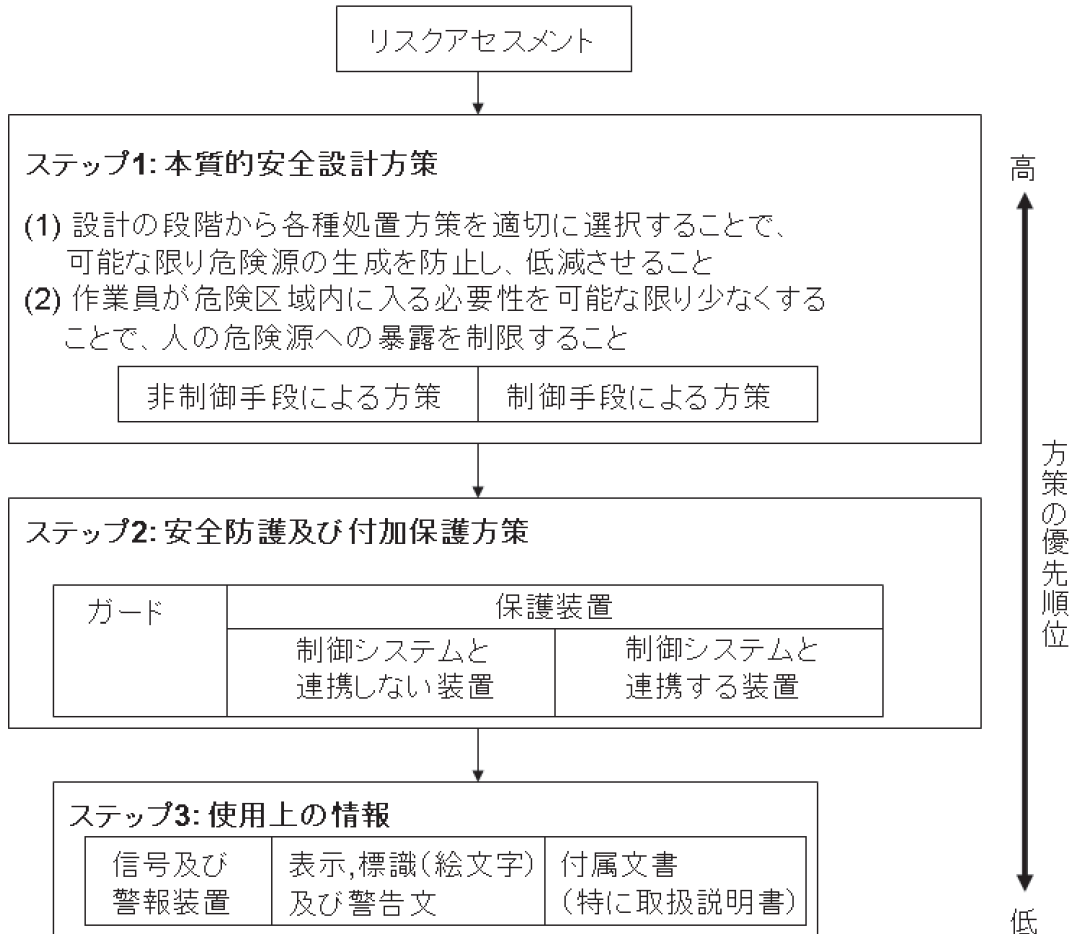


図 1.2.4 ISO 12100-2 で規定されるリスク低減方策(出典：安全の国際規格第二巻機械安全)

リスク低減の方策としては、本質安全設計方策が最も重要である。機械構造、防爆構造、機械結合に対する確実な安全設計を実施するための方策と人に分かりやすい機構にする、明るいところで作業するといった人間工学の原則としての方策も含まれる。

制御に使われるアクチュエータに対する機械的な本質安全設計のための安全条件は確実に停止することである。そのために、危険源が装置内にあれば異常時に装置のドアを開かなくするといったことや、人が侵入してはいけないエリアにライトカーテン（図 1.2.5）を設置し、人を検知したら装置を停止させるといった安全防護が必要となる。

イネーブルスイッチ（図 1.2.6）は、握っているときのみ作動するスイッチである。ドアの開閉を一例とすると、インターロックスイッチによるドアロックの方式としては、通電を停止してロックをかける方式と通電することでロックをかける方式がある。非常停止

用押しボタンスイッチなどによる非常停止装置は、安全性を保つための最終手段となる。こうした装置は、安全性を確実に保つ側を考慮し、設計しなければならない。

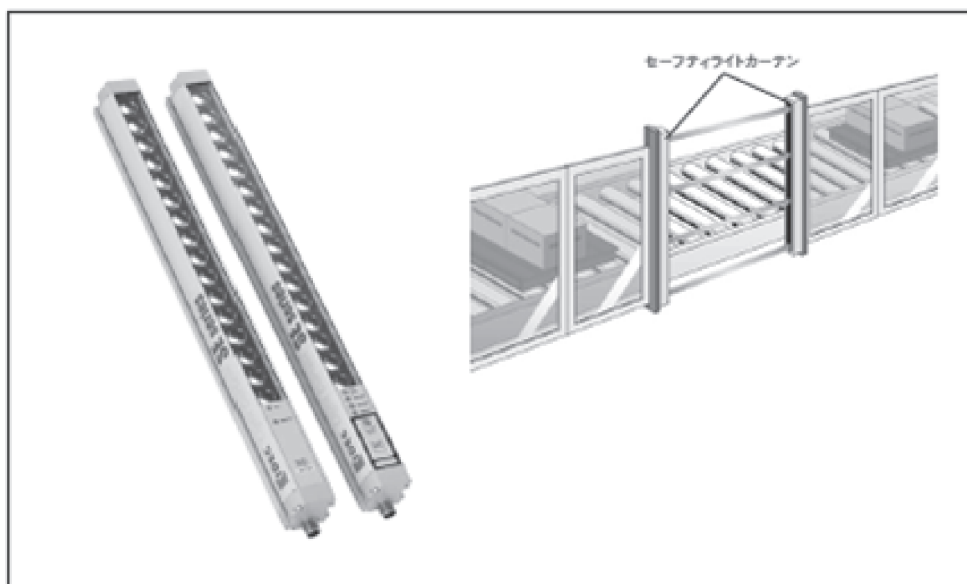


図 1.2.5 ライト(光)カーテン例 (出典：IDEC 社資料)

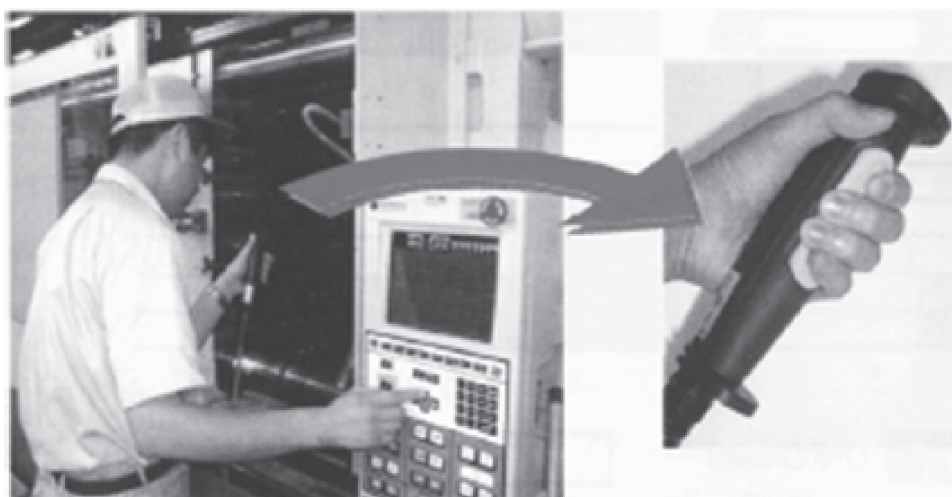


図 1.2.6 イネーブル装置例 (出典：IDEC 社資料)

機能安全としての安全回路の要件は ISO 13849 に記載されている。IEC 62061 との違いとしては、機械特有のものも含んでいるところにある。安全回路は、安全コントローラ、シーケンサを基に構築することが多い。

国際安全規格では、下記項目の通りはじめから機械は故障するということを認めて安全を確保する考え方が盛り込まれている。

- ・品質を上げて故障しないようにする
- ・定期的に故障の有無をチェックする
- ・故障しても安全機能を維持させる
- ・故障を検出したら運転させない

国際安全規格の「カテゴリ」は電気系の安全指標「SIL」と同様、機械系の安全指標で用いられてきた。カテゴリは制御システムが故障した場合の安全機能の維持能力を現しており、B、1、2、3、4と5つに分類され、維持能力はBが最も低く4が最も高くなっている（表 1.2.1）。カテゴリBの安全機能の維持管理能力は、「欠陥発生時、安全機能を損なう場合が十分起こりえる」で、カテゴリ内で最も低い。この分類を基に、制御システムが故障した場合のリスクの大きさによって、適切なカテゴリを選択することになる。

表 1.2.1 カテゴリと安全機能の維持管理能力（出典：IDEC 社資料）

分類 (カテゴリ)	要件の要約	安全機能の維持能力（抵抗性）
B	・機械制御システム安全関連部の目的機能を実現すること。	・欠陥発生時安全機能を損なう場合が十分起こりえる。
1	・カテゴリBの要件を満たすこと。 ・十分吟味された高信頼性のコンポーネントを使用し、安全の確保は安全原則に従うこと。	・カテゴリBと同様であるが、安全関連部の安全確保機能の信頼性は高い。
2	・カテゴリBの要件を満たすこと。 ・安全の確保は安全原則に従うこと。 ・安全機能が適当な間隔でチェックされること。	・安全機能の消失はチェックによって検出されるが、チェック間隔時間の間では安全機能は損なう。
3	・カテゴリBの要件を満たすこと。 ・安全の確保は安全原則に従うこと。 ・設計要件：単一欠陥で安全機能を損なわないこと。単一欠陥はできる限り検出されること。	・単一欠陥で安全機能は損なわれない。 ・すべてではないが、欠陥の検出ができる。未検出欠陥の蓄積によって安全機能を損なう場合がある。
4	・カテゴリBの要件を満たすこと。 ・安全の確保は安全原則に従うこと。 ・設計要件：単一欠陥は安全機能実行時、もしくはその前に検出されること。これが実施できないときは、欠陥の蓄積で安全機能を損なわないこと。	・欠陥が生じた場合、常に安全機能は損なわれない。 ・欠陥は安全機能実施の前の段階で安全機能実施が必ず間に合うように、予防設置として検出される。

ISO 13849-1:2006 は確定的であった安全回路の考え方に確率的要素を加えたところに新しさがある。また IEC 62061 は、IEC 61508 の機械セクター規格である。（図 1.2.7）

図 1.2.7 で示している規定の適用領域としては、IEC 61508 は太線で囲んでいる領域全体の内部、IEC 62061 は太い点線で囲んでいる内部、ISO 13849-1:2006 は細い点線で囲んでいる内部、ISO 13849-1:1999 は細い実線で囲んでいる内部となっている。

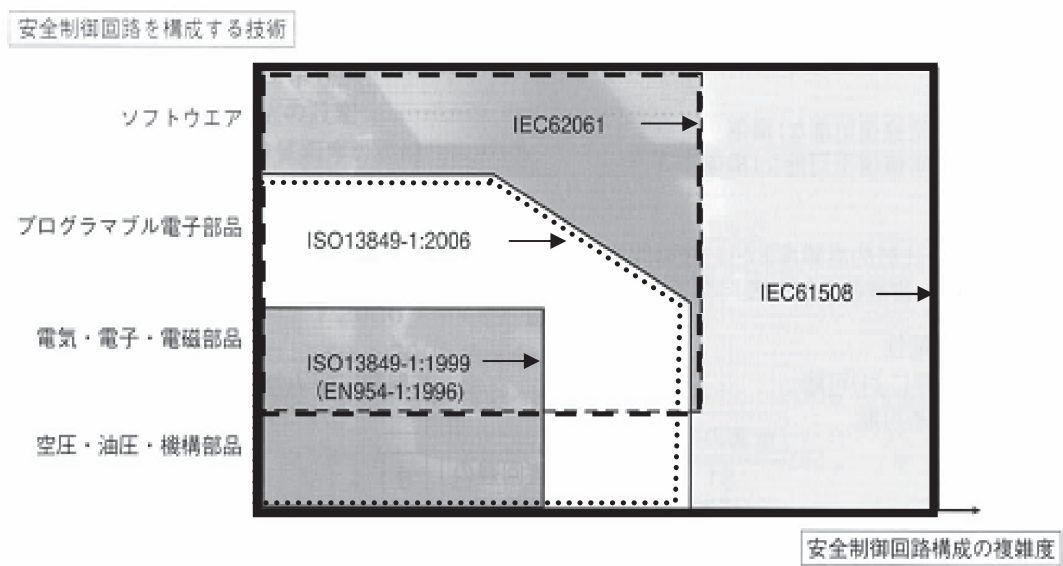


図 1.2.7 規定改定の適用範囲イメージ例（出典：IDEC 社資料）

図 1.2.7 の規定改定の適用範囲イメージ例の基となる考え方を表 1.2.2 に示す。表 1.2.2 は IEC 62061 と ISO 13849-1:2006 の適用法の推奨案をまとめたものである。

表 1.2.2 IEC 62061 と ISO 13849-1:2006 の適用法の推奨案（出典：IDEC 社資料）

	安全関連性能を実現する技術	ISO13849-1:1999	ISO13849-1:2006	IEC62061
A	非電氣的，例えば液圧式	○	○	対象外
B	電氣機械的，例えばリレー，複雑でない電子部品	○	PL= e までの指定のアーキテクチャのみ (備考 1 参照)	SIL3までのすべてのアーキテクチャ
C	高複雑度電子システム，例えばプログラム式	○	PL= d までの指定のアーキテクチャのみ (備考 1 参照)	同上
D	AとBの複合	○	PL= e までの指定のアーキテクチャのみ (備考 1 参照)	○ 備考3参照
E	CとBの複合	○	PL= d までの指定のアーキテクチャのみ (備考 1 参照)	SIL3までのすべてのアーキテクチャ
F	CとA，又はCとA及びBの複合	○	○備考 2 参照	○ 備考 3 参照
○は，当該アイテムがその規格で扱われていることを示す。 備考1 指定のアーキテクチャは，13849-1:2006の附属書Aに示され，パフォーマンスレベルの定量化に関する簡単化したアプローチが与えられている。 備考2 高複雑度電子システムには，13849-1:2006のPL= d までの指定のアーキテクチャ又はIEC62061のすべてのアーキテクチャを用いることができる。 備考3 非電氣的な制御システムには，サブシステムとして13849-1:2006に適合する部品を用いること。				

1.2.3 規格改定に伴うパフォーマンスレベル（PL）の考え方について

パフォーマンスレベルとは、今までのカテゴリの考え方に MTTFd（Mean Time to Dangerous Failure）（平均危険側故障時間）、DC（Diagnostic Coverage）（診断範囲）、CCF（Common Cause Failure）（共通原因故障）といったものを加えたものである。（図 1.2.8）

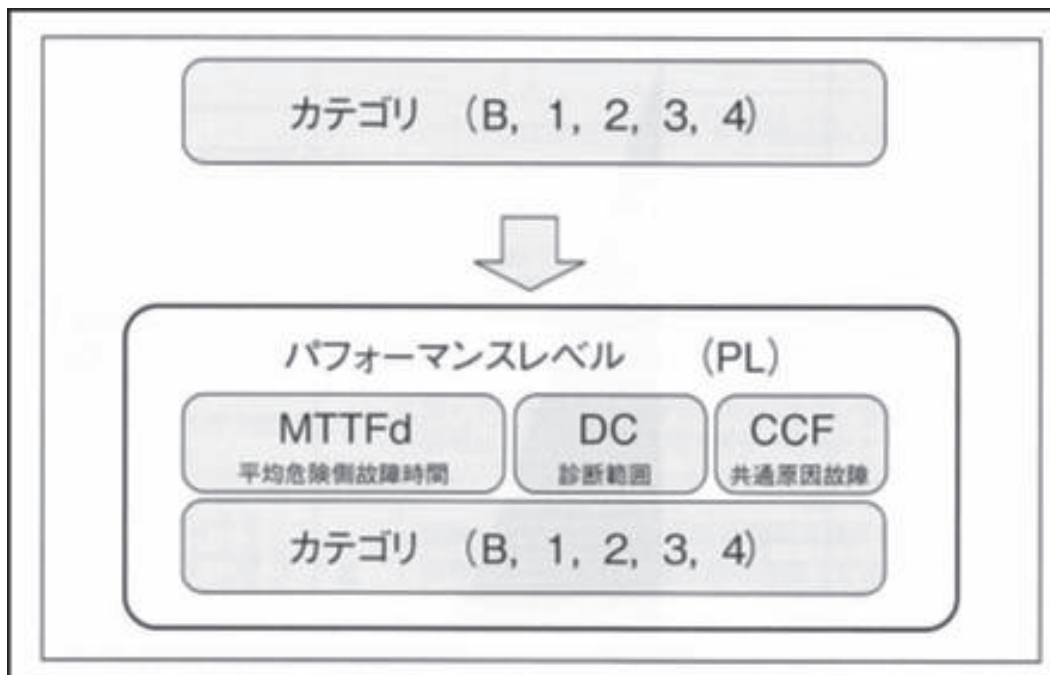


図 1.2.8 カテゴリからパフォーマンスレベルへ（出典：IDEC 社資料）

MTTFd とは、危険側故障を生じるまでの平均時間のことである。（図 1.2.9）

3. カテゴリ、MTTFd、DCの概略

3-2. MTTFdとは

P.8

MTTFdとは？
危険側故障を生じるまでの平均時間

- ・各チャンネルのMTTFdは、100年を限度とする
- ・MTTFdは、3年未満を規定していない

図2-11. DC(診断範囲)の区分

表示	範囲
low	$3\text{年} \leq \text{MTTFd} < 10\text{年}$
medium	$10\text{年} \leq \text{MTTFd} < 30\text{年}$
high	$30\text{年} \leq \text{MTTFd} < 100\text{年}$

Copyright 2005-2009 IDEC CORPORATION. All rights reserved.

17

Think Automation and beyond...
20080717 JASA ET037-7

図 1.2.9 MTTFd（平均危険側故障時間）とは（出典：IDEC 社資料）

DC とは、診断効果の尺度であり、検出される危険側故障率に対する全危険側故障率の故障比率で決定することができる。（図 1.2.10）

3. カテゴリ、MTTFd、DCの概略

3-3. DCavgとは

P.8

DCとは？
 診断効果の尺度であり、検出される危険側故障率に対する
 全危険側故障率の故障率比で決定することが出来る

$$DC = \frac{\sum \lambda_{DD} \text{ (検出される危険側故障率)}}{\sum \lambda_{total} \text{ (全体の危険側故障率)}}$$

図2-10. 各チャンネルのMTTFd(平均危険側故障時間)の区分

表示	範囲
None	$DC < 60\%$
Low	$60\% \leq DC < 90\%$
Medium	$90\% \leq DC < 99\%$
High	$99\% \leq DC$

Copyright 2005-2009 IDEC CORPORATION. All rights reserved.
Think Automation and beyond.
20090717 JASA STSナニ

図 1.2.10 DC（診断範囲）とは（出典：IDEC 社資料）

パフォーマンスレベル（PL）とは、安全に関わる制御システムの1時間あたりの危険側に障害が発生する平均確率を a～e の5段階に分類したものである。（図 1.2.11）

パフォーマンスレベル (PL)	時間当たりの危険側障害発生 の平均確率
a	10^{-5} 以上、 10^{-4} 未満
b	3×10^{-6} 以上、 10^{-5} 未満
c	10^{-6} 以上、 3×10^{-6} 未満
d	10^{-7} 以上、 10^{-6} 未満
e	10^{-8} 以上、 10^{-7} 未満

図 1.2.11 パフォーマンスレベル（PL）とは（出典：IDEC 社資料）

これに対し、リスクパラメータを基に要求されるパフォーマンスレベル（PLr）を選択する。（図 1.2.12）

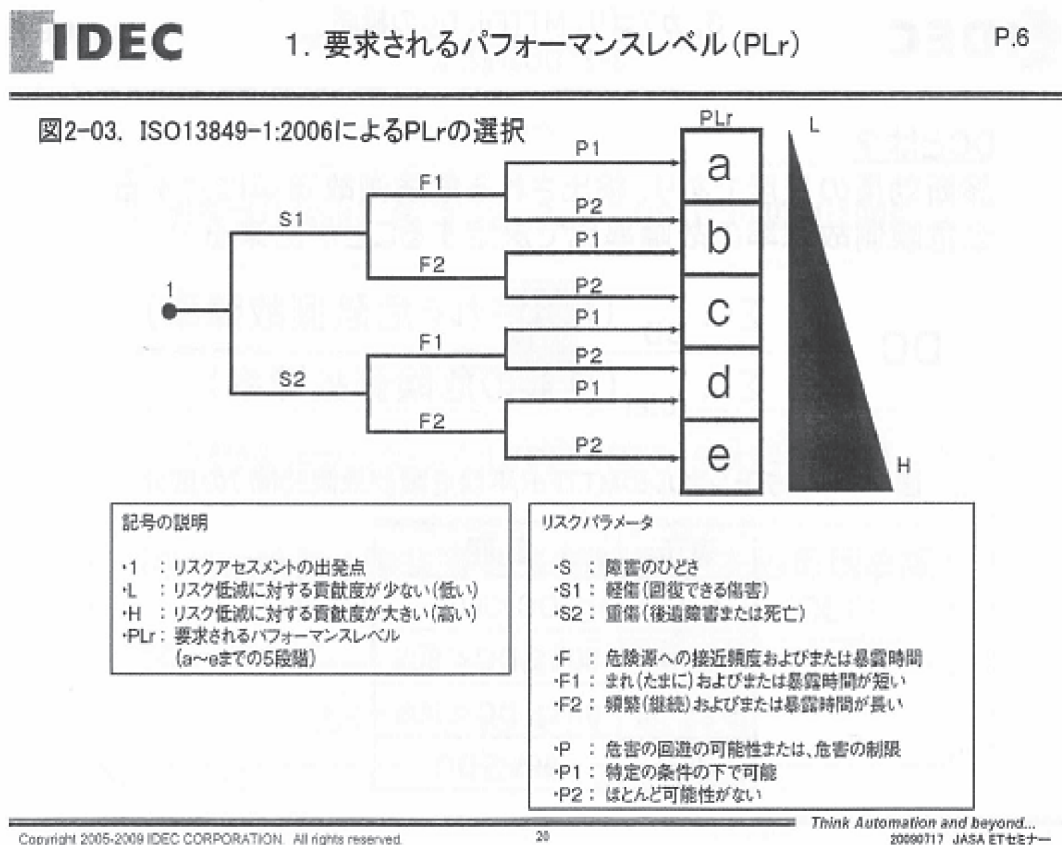


図 1.2.12 要求されるパフォーマンスレベル（PLr）の選択（出典：IDEC 社資料）

リスクグラフ法によるリスク評価によって決定した PLr（a～e）が、安全に関わる制御システムに最低限必要とされる達成レベルが、パフォーマンスレベル(PL)となる。パフォーマンスレベルを構築するにあたっては、カテゴリーの他に、MTTFd（平均危険側故障時間）、DC（診断範囲）、CCF（共通原因故障）といったものを考慮して設計する必要がある（図 1.2.13）。

また、構築した安全関連制御システムのパフォーマンスレベル(PL)は、安全機能維持レベルの目標値である（PLr）と同等以上とならなければならない。

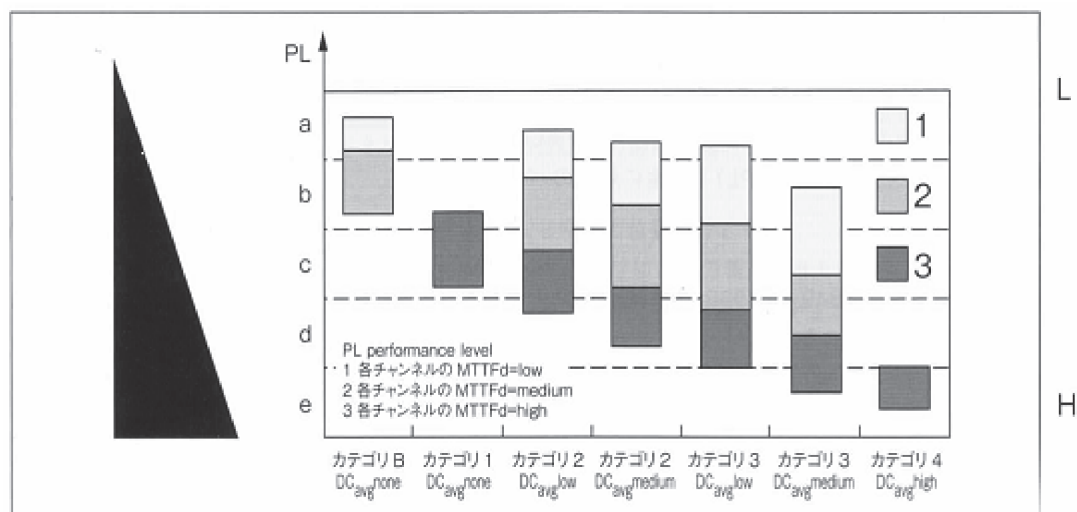


図 1.2.13 パフォーマンスレベル(PL)とカテゴリ、MTTFd（平均危険側故障時間）、DC（診断範囲）の関係図（出典：IDEC 社資料）

リスクアセスメントを実施した結果、リスクの低減が必要となった危険源に対して、リスク低減方策を検討し実施することになる。リスクアセスメントとリスク低減方策の流れは、図 1.2.14 に、保護方策として制御システムを用いる場合の設計プロセスを図 1.2.15 に示す。

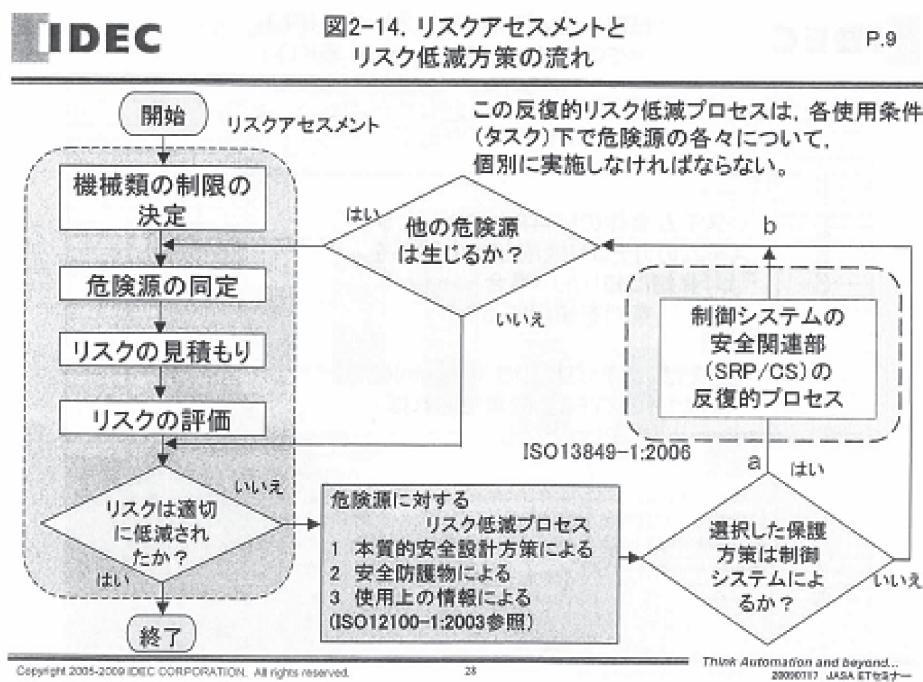


図 1.2.14 リスクアセスメントとリスク低減方策の流れ（出典：IDEC 社資料）

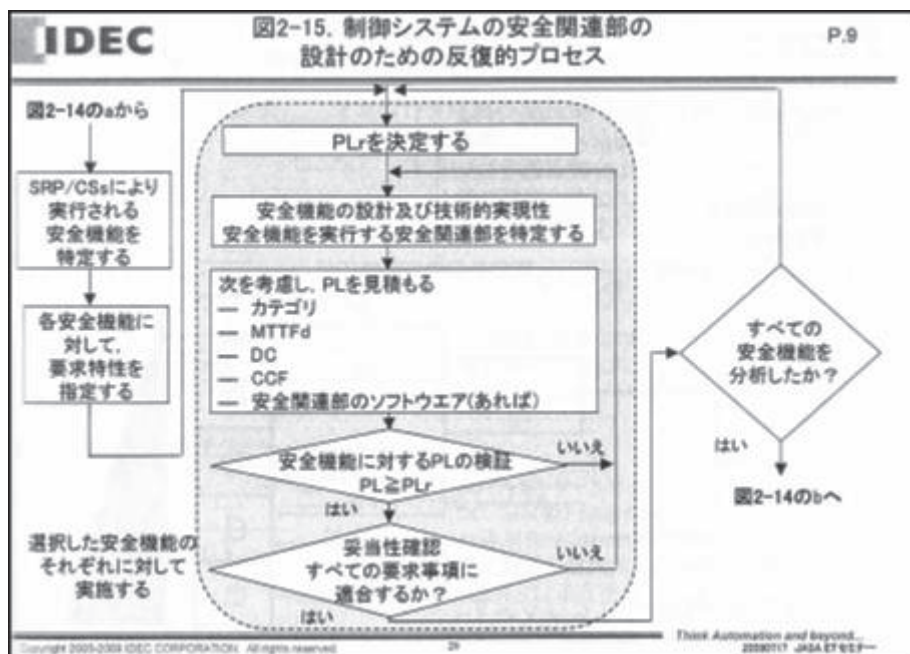


図 1. 2. 15 保護方策として制御システムを用いる場合の設計プロセス（出典：IEEC 社資料）

こうした流れを受けて、実際のパフォーマンスレベル(PL)の計算を行う。この PL を決定するための各要素の詳細、具体的な計算例に関しては、IEEC 社資料：安全コンセプトブック 別冊「機械安全—コントロールシステムの安全関連部—設計原則」編を参照願う。

1.3 安全 PLC

本節は株式会社ジェイテクトメカトロ制御技術部制御開発室の宮脇マネージャーの御協力を得て、レポートをまとめたものである。

1.3.1 株式会社ジェイテクトの活動概要

ジェイテクト社はトヨタグループに属する機会・自動車製品の製造をする会社である。企業姿勢としては、

- ・ 新たな価値を創造し、広く社会に「喜びと感動」を提供する。
- ・ グローバルで革新的な経営により、社会との調和ある成長を目指す
- ・ 人間尊重を基本に、明るく活力ある企業風土をつくる
- ・ 安全で豊かなくらしの実現に取り組む

であり、事業領域としては先端技術開発、システム化、技術深耕の 3 つの軸とステアリング、ベアリング、ドライブライン、工作機械メカトロの 4 つの商品群をメインに活動をしている。特にメカトロニクス分野の PLC（プログラマブル・コントローラ）においては、安全 PLC として国際安全規格の IEC 61508 における安全度水準である SIL3 を取得している。

連絡先：

大阪本社 大阪府中央区南船場 3-5-8

Tel : 06-6271-8451

名古屋本社 名古屋市中村区名駅 4-7-1 ミッドランドスクエア 15F

Tel : 052-527-1900

URL ; <http://www.jtekt.co.jp/>

1.3.2 安全 PLC の種類

安全 PLC には次の 2 種類がある。

(1). Fail tolerable 型 安全 PLC

- ・ 用途：主としてプロセス工業用
- ・ 特徴： ①設備保護目的
②故障が発生しても、運転は続行
③電源を入れたまま故障部品の交換が可能

(2). Fail safe 型 安全 PLC

- ・用途：主として機械工業用
- ・特徴： ①作業者保護目的
②故障が発生すれば安全状態に移行
③電源を切って故障部品の交換

1.3.3 安全制御の基本

安全制御の基本とは、ユネイトな情報伝達要素による情報伝達の形態として、システムに安全情報が入力されない限り誤って運転許可信号を発生することがないという制御形態を言う。

機能安全では、故障を 2 種類に分類している。それは、安全側故障 (safe failure fraction) と危険側故障 (dangerous fraction) である。

安全側故障は、安全関連システムを危険状態または機能喪失状態にするような、潜存在を有しない故障 (IEC 61508-4 3,6,8) を表し、危険側故障は、安全関連システムを危険状態または機能喪失状態にするような、潜存在を有する故障 (IEC 61508-4 3,6,7) を表している。

規格上、普通の PLC の危険側故障モードと安全側故障モード比率はオーソライズされたデータがない限り 50 対 50 である。安全 PLC は SIL 安全認証 SIL3 レベルになると例えば数千年に 1 回に危険側故障になる。

安全 PLC とは非常事態が起きた時、確実に止めることが要求される、さらに危険側故障発生頻度が安全故障に比較して小さいことを非対象故障モードという。

1.3.4 設備における安全 PLC の導入

安全 PLC と汎用 PLC

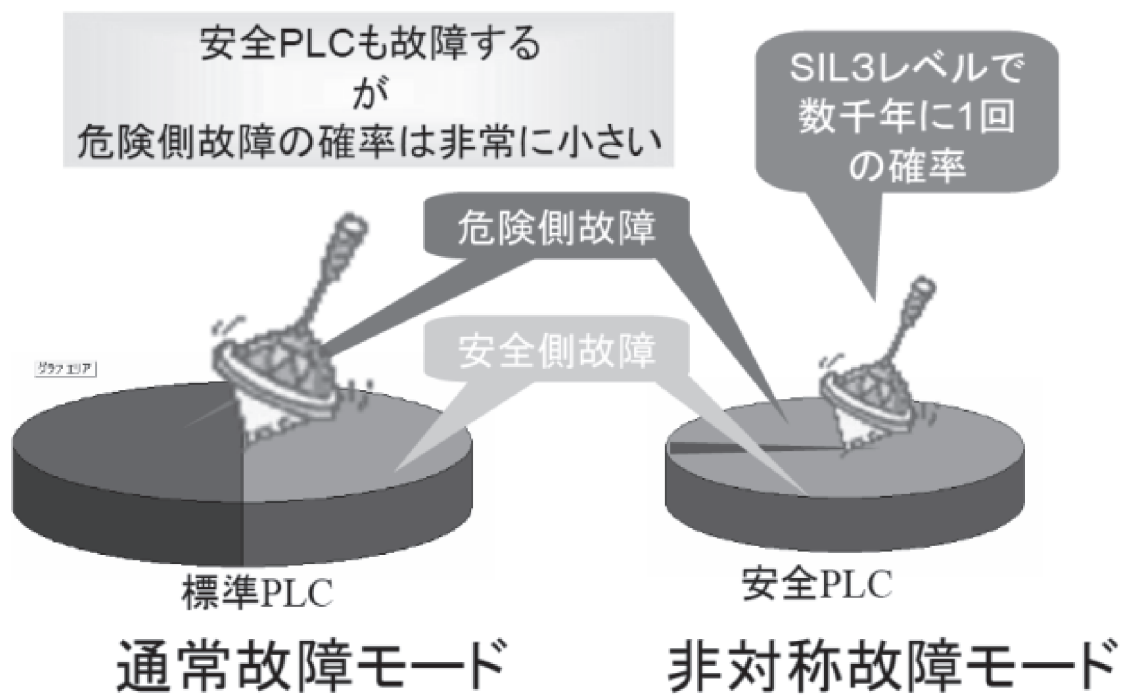


図 1.3.1

引用：(株)ジェイテクト JASA 機能安全セミナー資料より

1.3.5 機械設備における安全 PLC との導入

機械設備のリスク低減方策としては、まず本質的安全設計（Inherent safety）方策→安全防護による保護方策→付加の保護方策→使用者への情報順序で保護方策を取り、許容可能なリスク低減することを義務付けている。ISO12100 の規格体系を図 1.3.2 で示す。

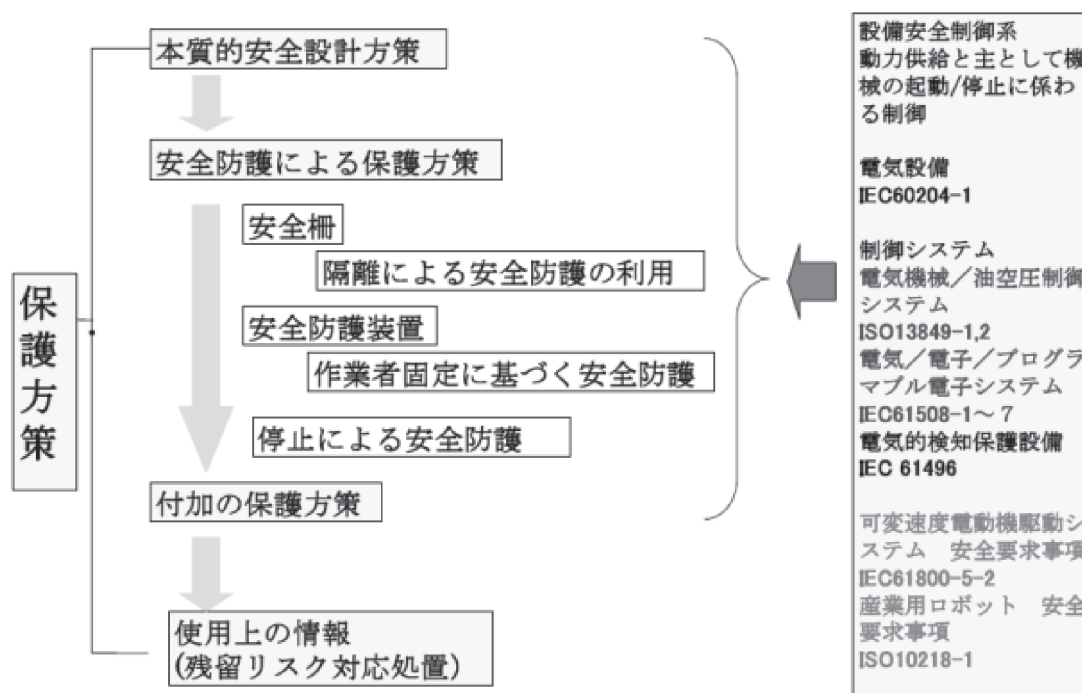


図 1.3.2 設備のリスク低減手順（ISO12100）

引用：(株)ジェイテクト JASA 機能安全セミナー資料より

またこれらの安全設計を可能にするためには、安全制御システムが不可欠であり、主として動力の供給/遮断と起動/停止の制御を実施する。制御装置としては安全リレー、安全 PLC が採用されるが、最近では電気/電子/プログラマブル電子システム（IEC61508-1～7）規格¹⁾に認証された安全 PLC が、安全制御において重要な位置付けとなっている。

¹⁾ ISO12100-1～2 2003: Safety of machinery, Basic concepts, general principles for design.

① 実際のリスク低減

具体的なリスク低減の手順をイメージした図を図 1.3.3 に示す。

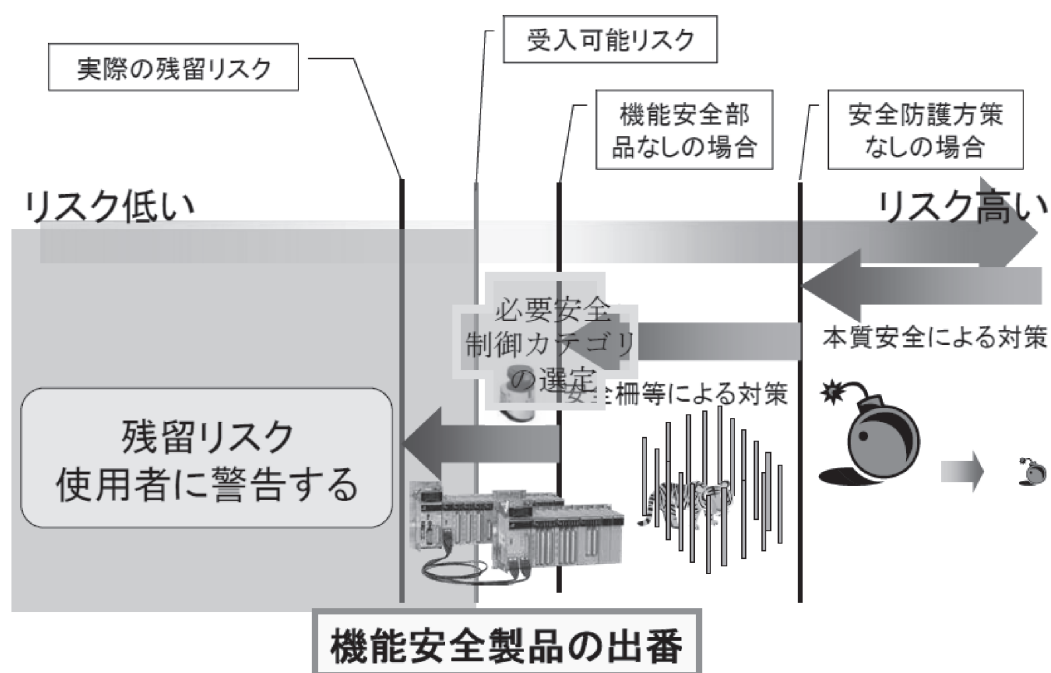


図 1.3.3

引用：(株)ジェイテクト JASA 機能安全セミナー資料より

機械分野においては、2006 年に従来の制御システムの安全設計ガイド規格であった EN954-1（旧 ISO13849-1）が改定され、従来の定性的な安全カテゴリ評価と IEC61508 の定量的安全評価を取り入れた新しい ISO13849-1²⁾（2006 年制定）が発効された。

²⁾ ISO13849-1 2006 Safety of machinery-Safety-related parts of control system-Part 1 general principle for design.

② 安全 PLC 適用範囲

製品の適応可能な停止カテゴリについては EN60204-1 条項 9.2.2 に基づいて次の三つのカテゴリに分類されており表 1.3.1 の内容で対応可能である。

安全PLCのEN60204-1における適用可能停止カテゴリ

停止種類	条項 9.2.2 停止カ テゴリ	説明	安全PLC適応範 囲
非制御停止	0	機械のアクチュエータ電源を即断する。	適応可能
制御停止	1	機械のアクチュエータが停止するまで電源を供給し停止後、電源を遮断する。	適応可能
制御停止	2	機械アクチュエータに電源を供給した状態での停止。 安全PLCだけでは実現できない。ISO14118 (EN 1037)意図しない起動からの保護に対応した付加的な手段、装置が必要。	安全PLCだけでは適 応不可能 例) 再起動防止/機械的 分離/ 静止監視装置 (IEC61800-5-2) (ISO10218-1)

表 1.3.1 安全 PLC 適用範囲

引用：(株)ジェイテクト JASA 機能安全セミナー資料より

実際の安全制御システムは IEC61508-6 におけるセンサー部、ロジックソルバー部、アクチュエータ部より構成されており（図 1.3.4）そのプログラミング、各部とのつなぎ配線／回路を含めてシステム全体でフェールセーフ構造を達成する必要がある。

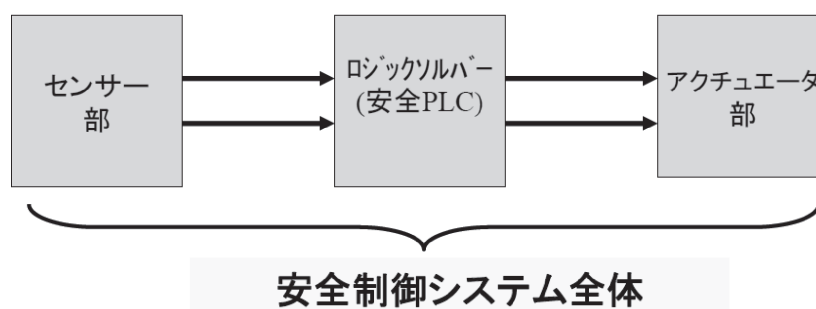


図 1.3.4

引用：(株)ジェイテクト JASA 機能安全セミナー資料より

1.3.6 従事の制御装置安全評価

カテゴリ	必要条件	安全機能
B	・機械制御システム安全関連部の目的機能を実現すること。	・故障発生時、安全機能を損なう場合が十分起こりえる
1	・カテゴリBの要件を、満たすこと ・十分吟味された高信頼のコンポーネントを使用し、安全の確保は安全原則に従うこと。	・カテゴリBと同様であるが、安全関連部の安全確保機能の信頼性が高い
2	・カテゴリBの要件を、満たすこと ・安全の確保は安全原則に従うこと。 ・安全機能は、適当な間隔でチェックされること。	・安全機能の消失はチェックによって検出されるが、チェック間隔時間の間では、安全機能は損なう
3	・カテゴリBの要件を、満たすこと ・安全の確保は安全原則に従うこと。 ・設計要件：単一故障で安全機能を損なわないこと単一故障は、できる限り検出されること	・単一故障で安全機能は損なわれない 全てではないが、故障の検出ができる。 未検出故障の蓄積によって、安全機能を損なう場合がある
4 開発目標	・カテゴリBの要件を、満たすこと ・安全の確保は安全原則に従うこと。 ・設計要件：単一故障は安全機能実行時、もしくはその前に、検出されること。これが実施できないときは、故障の蓄積で安全機能を損なわないこと。	・故障が生じた場合、常に安全機能は損なわれない 単一故障は全て検出ができる。 故障は、安全機能実施の前の段階で安全機能実施が必ず間に合うように予防措置として検出される。

図 1.3.5 安全カテゴリーとは？（EN954-1）

引用：(株)ジェイテクト JASA 機能安全セミナー資料より

従来の FA 分野での制御システムの安全設計ガイド規格であった EN954-1 による定性的な制御カテゴリーの層別基準を示す。

FA 分野においては通常はカテゴリ 2, 3, 4 が通常の適用範囲となる。（図 1.3.6）

安全カテゴリ-2, 3, 4 について（EN954-1）

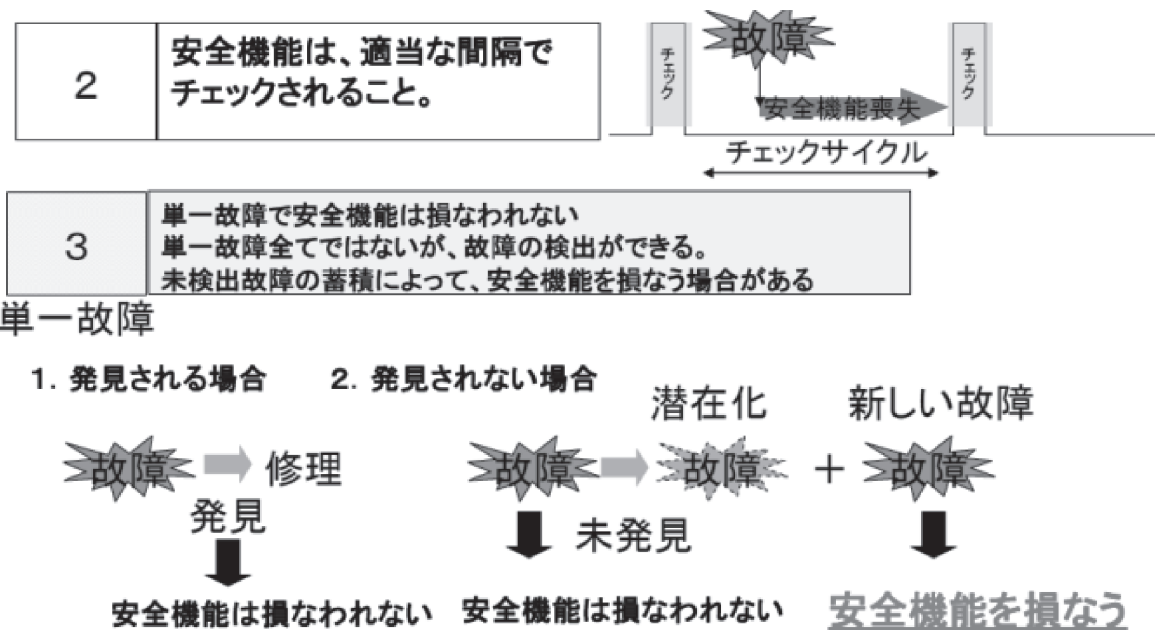


図 1.3.6

引用：(株)ジェイテクト JASA 機能安全セミナー資料より

カテゴリ 2：1 チャンネル構造で、定期的に自動診断を実施し、チェック間隔の時間に故障した場合、次のチェックまでの安全機能の喪失が考えられる。

カテゴリ 3：2 チャンネル構造で、単一故障では安全機能を喪失しない。ただし、全ての単一故障を発見できないため、未検出故障の蓄積による安全機能の喪失が考えられる。

カテゴリ 4:2 チャンネル構造ですべての単一故障を発見できる。複合故障の場合の故障蓄積でも安全機能を喪失しない。(図 1.3.7)

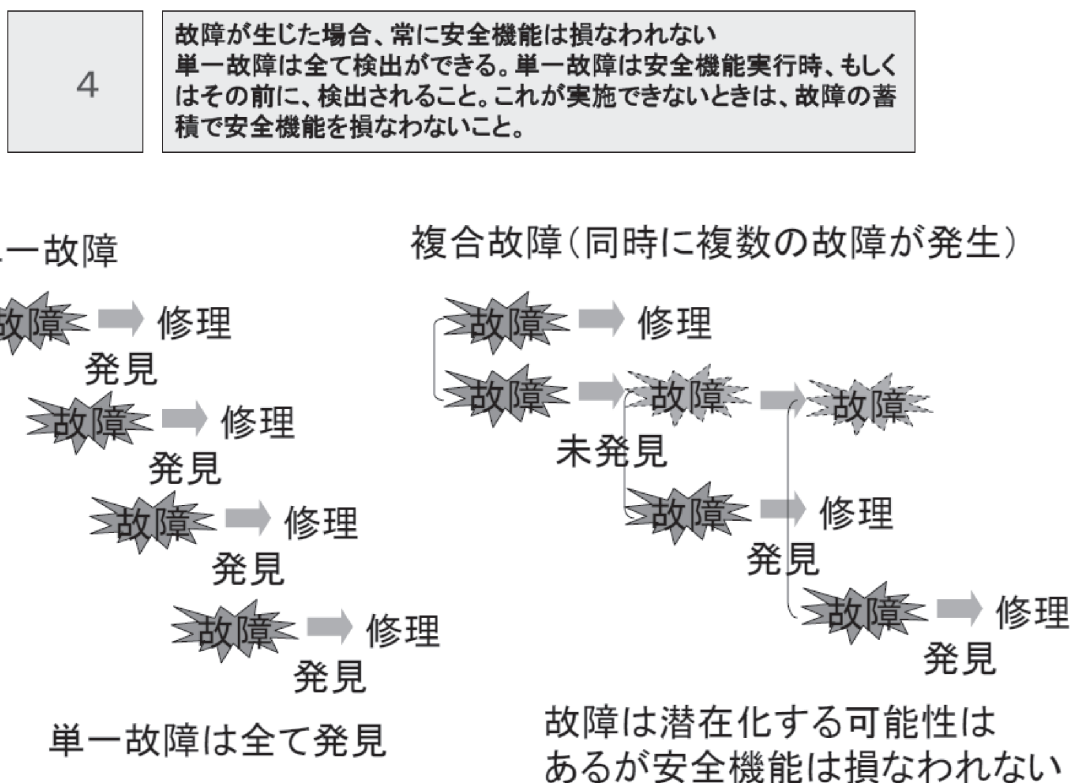


図 1.3.7

引用：(株)ジェイテクト JASA 機能安全セミナー資料より

EN954 規格の特長は、上記の安全カテゴリの判断は容易に理解し決定できる点である。しかし、EN954-1 においては、システムが、正しく設計されていることが前提であり、急速に発展した新技術 (state of the art technology) により複雑化している制御装置にたいして適合しておらず、またそこに組み込まれているソフトウェアの評価にも全く対応していなかった。

IEC61508 と EN954 との相違点として、主として以下の項目が挙げられる。

- (1) 安全システムの定量的なリスク管理と評価
- (2) 設計から廃棄までのライフサイクル管理
- (3) ソフトウェアのライフサイクル管理

1.3.7 安定の定量化について

IEC 61508 の場合 安全カテゴリーは安全完全性レベルSILで定量化

- 低需要モード(プラント関係に適用)
- 高需要/連続モード(機械関係に適用)

高需要/連続モードの場合

SILはPFHファクターにより指定されます(1時間あたりの平均的な危険故障率)

SIL	1時間当たりの危険故障確率	
1	$10^{-6} \leq X < 10^{-5}$	
2	$10^{-7} \leq X < 10^{-6}$	
3	$10^{-8} \leq X < 10^{-7}$	開発目標
4	$10^{-9} \leq X < 10^{-8}$	

SIL4は原子力発電所レベルに適応、通常の設備は最高でSIL3

図 1.3.8 安全水準 SIL とは？ (IEC61508)

引用：(株)ジェイテクト JASA 機能安全セミナー資料より

IEC61508 はパート 1 から 7 まである膨大な規格であるが、主な記述は以下の三つの内容区分に分けられる。また製品の認証を取得するためには、以下の各項目の要求項目を開発製品の SIL 目標にあわせ、これらを満足させる事が必要である。

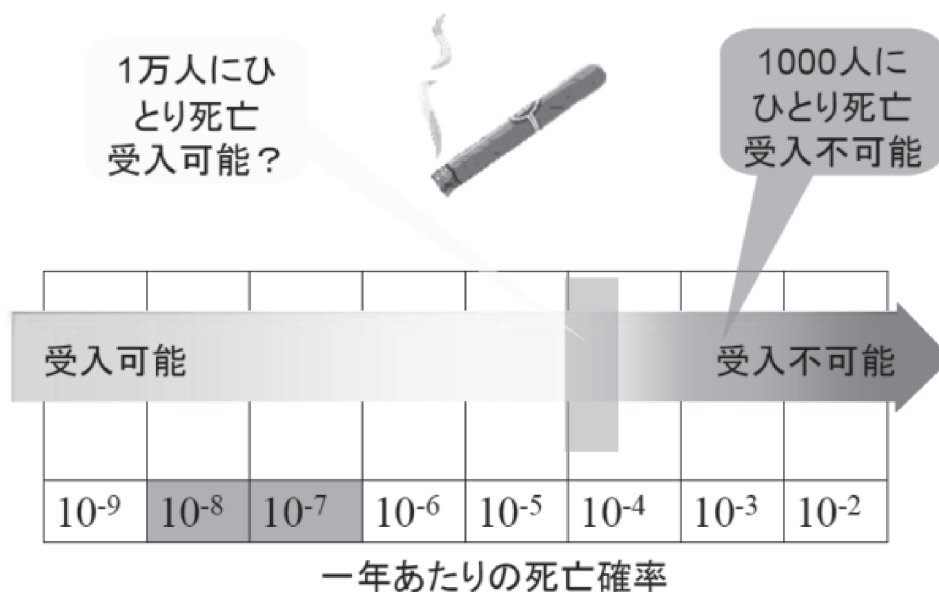


図 1.3.9 (参考) 受入可能なリスク 1

引用：(株)ジェイテクト JASA 機能安全セミナー資料より

自然災害による死亡



1.3.8 IEC61508 について

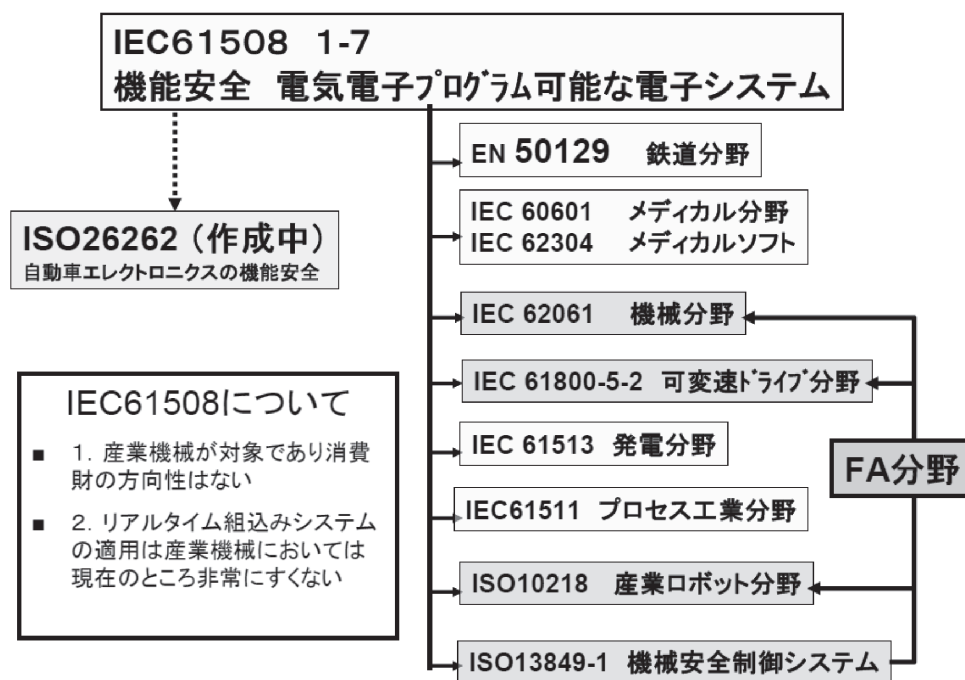


図 1.3.12

引用：(株)ジェイテクト JASA 機能安全セミナー資料より

機能安全とは、その入力に応じて正確に作動するシステム・機器に依存する全体の安全システムの一部である。安全機能が実行され、各安全機能に要求されるパフォーマンスのレベルに対応する場合、機能安全が達成される。どんな高温にも耐えられるような材質で設計されたモータはむしろ本質的な安全に分類される。本規格は現在においては、最新技術を安全目的に使用するために、各産業分野で適用されている。現在の各分野の国際安全規格の相互関連を図 1.3.12 に示す。

IEC61508 はパート 1 から 7 までの膨大な規格

主な記述としては以下の 3 つの内容があると考えられる。

製品の認証をとるためには、各項目の要求事項を開発製品の目標とする安全水準 (SIL) にあわせて適応する。

- (1). FSM (機能安全マネジメントシステム)
- (2). ハードウェア
- (3). ソフトウェア

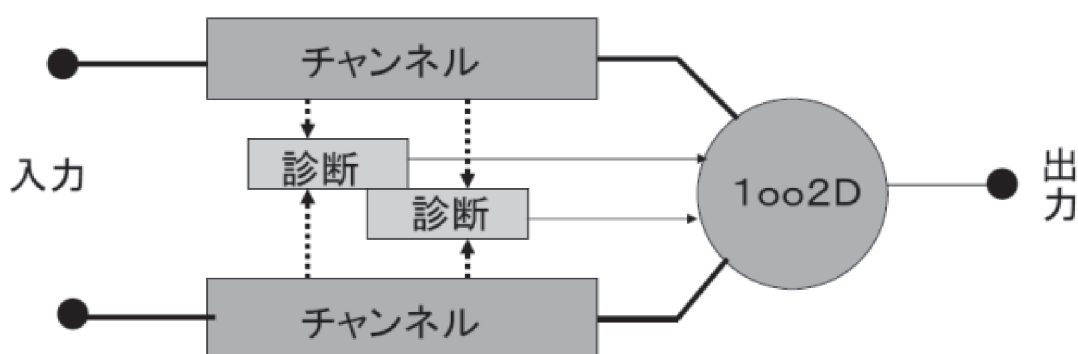
① FSM 機能安全マネジメントシステム

- ・ 会社組織レベル

- ・ 責任範囲の定義
- ・ スタッフのトレーニングと資格
- ・ 組織内ガイドラインと参照標準類
- ・ 独立したアセスメント部門と審査
- ・ 各標準の維持改善活動
- ・ 市場で発見された不具合、クレームの分析と監視

FMS の内容は、上記内容より ISO9000 シリーズの QM(品質マネジメントシステム)に非常に似ており、まさに品質を安全に置き換えた活動が必要になる。注目すべきことは、対象製品の SIL 目標にあわせて、独立したアセスメント部門が個人→部署→組織と層別されていることである。

IEC61508-6: 1oo2D (1 out of 2 diagnostic)



並列に接続された2本のチャンネルから構成

TOYOPUC-PCSの場合

- ・いずれかのチャンネルの診断試験で障害が検出された場合 安全状態(非常-OFF)
- ・両方のチャンネルに障害が検出された場合も 安全状態(非常-OFF)

図 1.3.13 アーキテクチャ決定

引用：(株)ジェイテクト JASA 機能安全セミナー資料より

通常の SIL2 あるいはカテゴリ 3 以上のプログラマブル電子システムにおいては 1oo2 (one out of 2) 以上のアーキテクチャで構成されたフェールセーフを実現している。図 1.3.13 に(株)ジェイテクト製安全 PLC TOYOPUC-PCS のアーキテクチャを示す。

TOYOPUC-PCS のアーキテクチャは並行接続された二つのチャンネルから構成されており、いずれかのチャンネルの診断試験で障害が検出された場合、あるいは出力状態が一致しない場合、システムは安全状態（通常は出力 OFF 状態）に速やかに移行する。

クリティカルティ分析

主としてソフトの検査に適用各部のクリティカルティを判断して低い部分については審査を1レベル低くする

安全の重大なソフトウェア(C3)

ソフトウェアの指定された機能からの単一の乖離は危険な状態をもたらすかもしれません。

例) 生命に直結する医療機器の制御ソフトウェア

安全関連するソフトウェア(C2)

ソフトウェアの指定された機能からの単一の乖離だけでは危険な状態をもたらさない、しかし別のソフトウェア・エラーまたは安全関連のハードウェア故障と結合して危険な状態になる。

例) CPU、メモリの自己診断ソフトウェア

フィードバックがないソフト(C1)(モニターソフト)

ソフトウェアは安全の制御機能、あるいは保護または検知機能はもっていないが、そのようなソフトウェア部分とのインターフェース機能を持っています。結果として、ソフトウェア・エラーは安全に影響があるかもしれません。

例) モニターI/Fソフトウェア

図 1.3.14

引用：(株)ジェイテクト JASA 機能安全セミナー資料より

クリティカルティ別要求 SI

表 1.3.2

引用：(株)ジェイテクト JASA 機能安全セミナー資料より

システムとしての要求 SIL値	エレメントのクリティカルティ		
	C1	C2	C3
SIL1	安全機能に関係ないことの証明	SIL1必要	SIL1必要
SIL2	安全機能に関係ないことの証明	SIL1必要	SIL2必要
SIL3	安全機能に関係ないことの証明	SIL2必要	SIL3必要
SIL4	安全機能に関係ないことの証明	SIL3必要	SIL4必要

故障の考え方

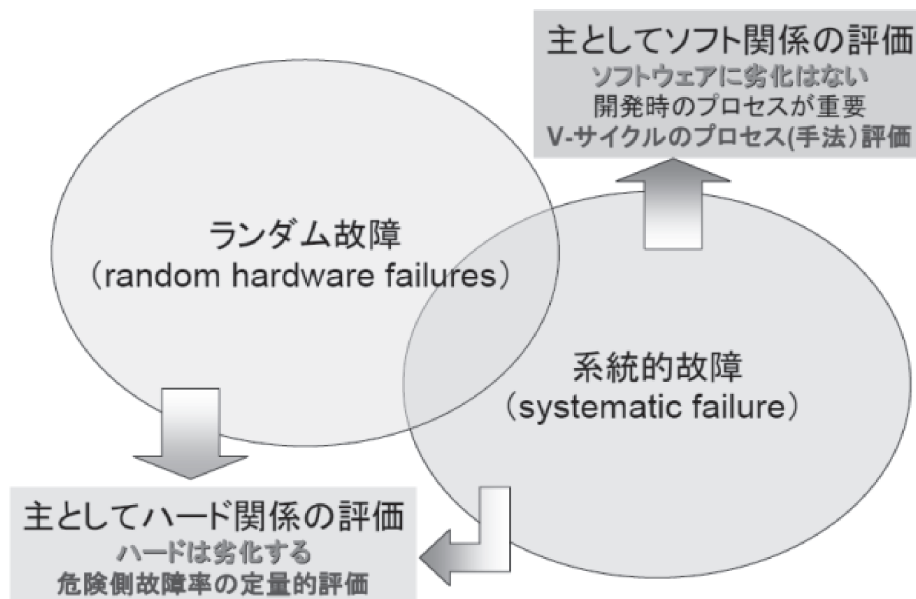


図 1.3.15

引用：(株)ジェイテクト JASA 機能安全セミナー資料より

② ハードウェア

ハードウェアについては危険側故障率の定量的評価が必要になり、下記データより SIL を算定する。規格上は PFD と PFH の二種類であるが、FA 分野では PFH (1 時間当たりの危険側故障確率) が採用される

ランダムハードウェア (random hardware failures)

故障評価

FMEA

部品の故障率

安全故障率 (SFF)

診断範囲 (DC)

共通原因未検出故障率 (β)

プルーフテスト間隔 (T)

SIL PFH、PFH の計算

③ ソフトウェア

ソフトウェアに関しては、安全通信ソフト以外では定量的評価が困難なため、系統的故障 (systematic faults) の回避に重点が置かれている。そのためにライフサイクル (ソフトの場合、V サイクル図 1.3.16 参照) が審査の対象となる。ステップごとに目標の

SIL 別に採用手法が推奨されており、これを採用した開発・試験が必要である。また推奨手法を採用しない場合、採用しない理由の説明が必要とされている。

ソフトウェア V サイクル

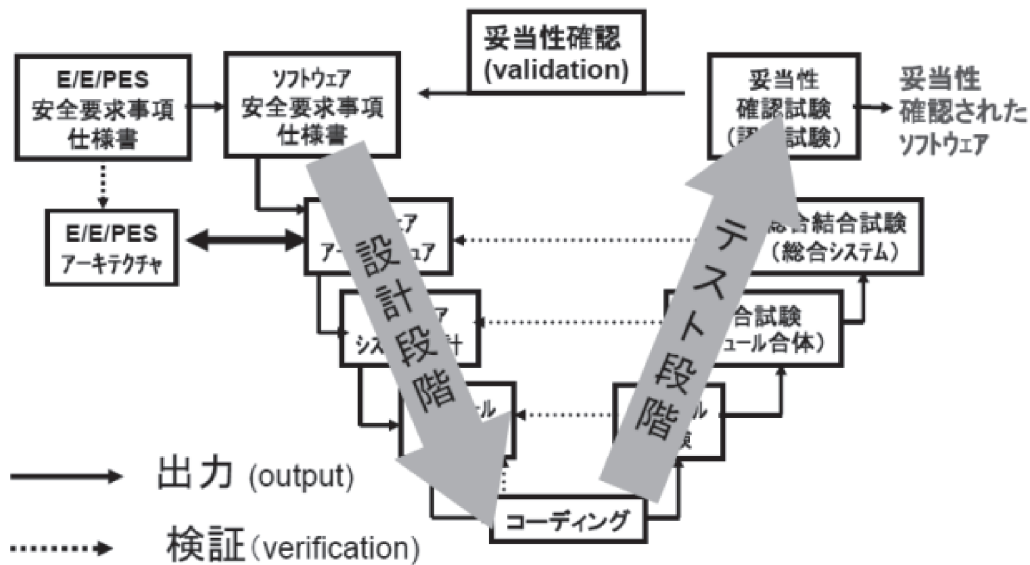


図 1.3.16

引用：(株)ジェイテクト JASA 機能安全セミナー資料より

妥当性確認については認証製品の場合、第三者機関の認証試験が必要となり、そのテスト方法の選択についても目標 SIL による。

1.3.9 FA 分野における国際安全規格動向

機能安全製品の開発

通常の開発業務のほか第三者機関の認証に労力と費用、時間が必要。

認証を取得する事により、いままで安全上許可されていなかった事がかのうとなりつつある。

安全 PLC といえば、安全リレーでしか許可されていなかった安全制御を PLC できるようになり、フィールドバスにおいても従来は安全に関わる信号を通信で伝送することは許されなかったが、認証された安全フィールドバスでは通信で可能となった。

いろいろな分野で機能安全が採用されるようになってきた。

1.4 自動車の安全

本節は日産自動車電子技術開発本部山下修平氏が 2009 年 9 月 18 日開催された JASA/ET セミナーにおいて行った、ISO 26262 最新状況とその解釈、と題する講演をベースにまとめたものである。

同氏の連絡先は以下の通り。

日産自動車電子技術開発本部 電子信頼性技術開発部

電子信頼性評価グループ

山下修平様

〒243-0192 神奈川県厚木市岡津古久 560-2

電話：046-270-1211

FAX：046-270-1543

E-mail：shuhei@mail.nissan.co.jp

1.4.1 ISO26262 導入のモチベーション

古くはオートクルーズの不具合によるといわれた車の暴走問題があり、近年では自動車の機能性能向上に伴う車載用電子機器の大規模化や協調性の複雑化、さらに最近では EV, HEV の登場による総合制御の必要性が高まってきており、また、安全設計に関しては従来からの社会的受容レベルへの適切な対処に匹敵するだけの配慮が必要であることがそのモチベーションである。

1.4.2 経緯

ISO 26262 は IEC 61508 の自動車版ともいえるもので、古くは 2000 年に IEC 61508 が成立した頃から、ヨーロッパの自動車メーカーを中心に、その自動車版の策定が必要であるという議論がされて来た。2003 年その制定化に向けてヨーロッパ特にドイツ・フランスのメーカーを中心にその制定化の検討が具体的に活発化した。日本は当初よりウオッチはしていたが、この頃より積極的に参加を検討しはじめ、その後日本からは(社)自動車技術会が窓口になり、大手自動車メーカーと多くの部品メーカーがこれに参加している。第一回の検討会議が日本も参加して 2005 年にドイツで開催された。その後は ISO TC22 SC3 WG16 として 2011 年の ISO 化を目指して活動しており、2009 年 7 月—12 月の DIS 投票期間を経て 2011 年年央には ISO 規格として成立の見込み。講演者はそこの分科会長である。

1.4.3 規格の位置づけ

自動車は移動する機械(ISO)でありながら部品は電気系(IEC)が多用されている。つまり機械系でありながら電機系という両面性を持つ。このような特殊性をカバーする規格である。具体的には ISO/IEC ピラミッド左最下段に、すなわち機械系安全規格群の C 規格、個別機械安全規格に位置づけられる。参考までに図 1.4.1 に示す。

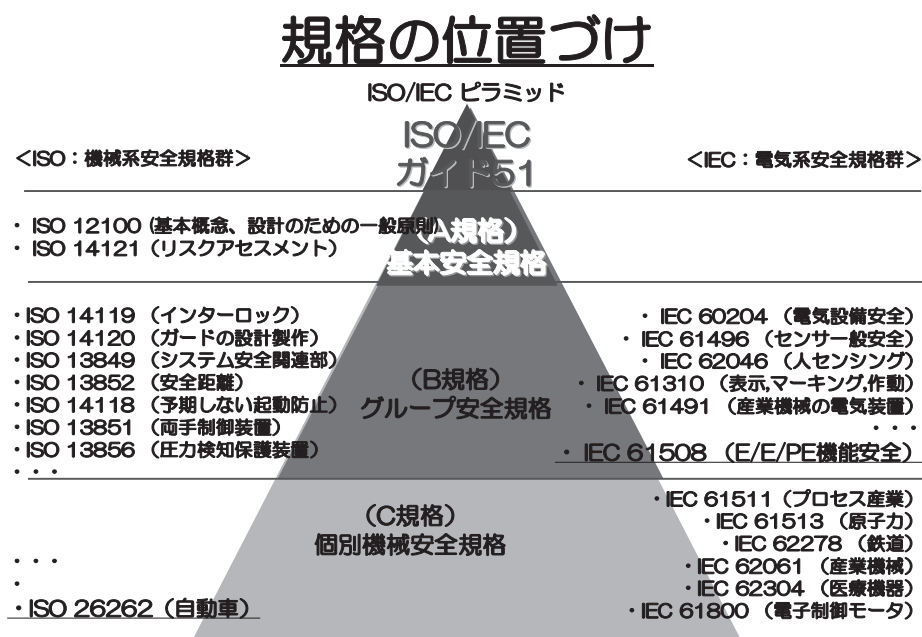


図 1.4.1 (出典：日産自動車資料)

1.4.4 規格の成り立ち

基本的には IEC 61508 を踏襲しながら、過去の遺産、即ち、車載用組み込み電子機器技術や、実績のある安全設計を加味し、自動車分野におけるコモンプラクティスである信頼性工学や品質プロセスの成果を取り入れている。特筆すべき特徴として一般機械の SIL に相当する ASIL(Automotive Safety Integrity Level)の導入である。この特徴は自動車に特化した追加のルールや手法を取り入れたところにある。図 1.4.2 に簡単に示す。

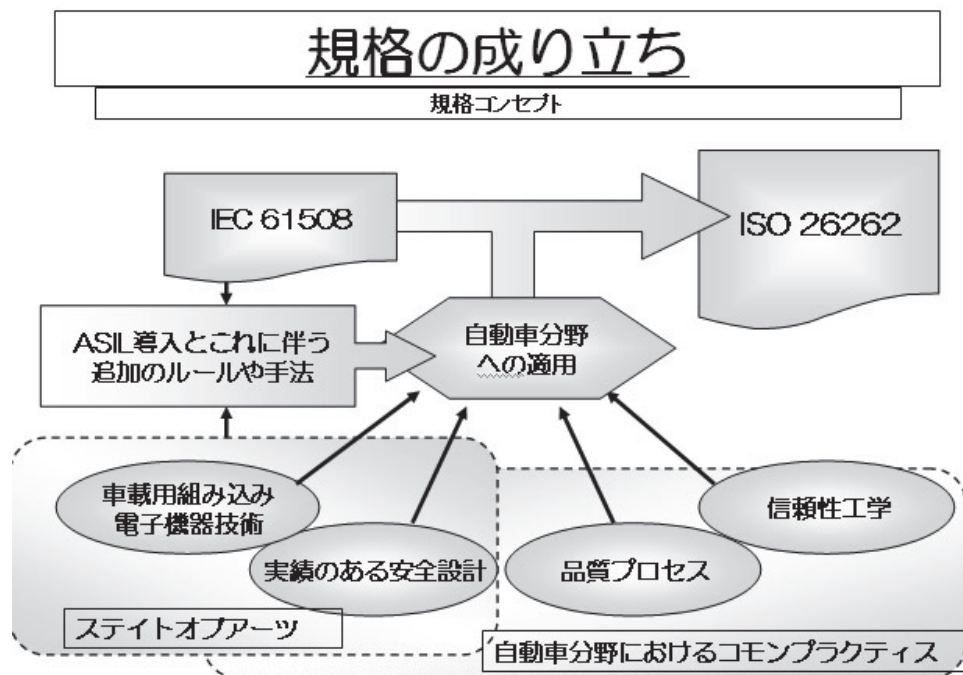


図 1.4.2 (出典：日産自動車資料)

1.4.5 規格のスコープ

ISO 26262 とは、自動車向け機能安全規格であることは既述の通りである。自動車専用の機能安全規格が作られることになった最大の理由として、従来の機能安全規格、IEC 61508 がおもにプラント系の限られた環境で使われるシステムを想定して作られた規格であるため、不特定多数の大衆が顧客であり、固定されない動的機械であるところの自動車への適用に無理があったことがあげられる。

近年の自動車は電気自動車やハイブリッド自動車などに見られるように電子部品が占める割合が増加し、さらに、相互にネットワークで接続されているため、部品の異常がどこに影響を与えるかが非常にわかりづらいシステムになっている。そのため、個別の機能の安全だけを考えるのでは足りず、機能間をまたがった安全コンセプト・基準の確立が必要とされて来た。

ISO 26262 の対象となるのは安全に関連する電気・電子システムであり、リスクアセスメント手法、プロセス要件、プロダクトが満たすべき要件の3つを規定することにより機能安全を標準化している。ASIL は電子システムの部品ごとに車両メーカーが設定することになっている。本件は後述する。

ISO 26262 の構造は以下のようになっている。

- 第1部 用語
- 第2部 機能安全の管理
- 第3部 コンセプトフェーズ

- 第4部 製品開発（システム）
- 第5部 製品開発（ハードウェア）
- 第6部 製品開発（ソフトウェア）
- 第7部 生産・運用
- 第8部 支援プロセス
- 第9部 ASIL 志向・安全志向の分析
- 第10部 ISO 26262 のガイドライン

1.4.6 IEC 61508 との対比

第一の違いは IEC 61508 の安全要求水準は目標故障確率的属性を持つ SIL であるのに対して、ISO 26262 の ASIL はその属性を持たず、あくまで安全要求水準であり、また、前者は据付型設備を指向しているのに対し、後者は、車載組み込みシステムには機能系と監視系が同居しており、その扱いに独特の注意が必要であること、また、固有の開発 V Model や分担開発の手法がすでに相当程度に確立しておることがあげられる。また対象が交通に参加する不特定多数者であり日常のメンテナンスはあまり期待できないという大量生産の工業製品であり、固有のライフサイクルを持つ動的機械であるところの自動車に特化したものでもある。

ISO 26262 と IEC 61508 の主な違いを表 1.4.1 にまとめた。

表 1.4.1 (講演内容から作成)

IEC 61508 対比

親規格との共通点と差異

IEC 61508	ISO 26262
SIL: 目標故障確率的属性	ASIL: 安全要求水準
据付型設備指向	車載組み込みシステム, 主機能系と監視系の同居
	固有の開発Vモデル,分担開発, 積み上げ型開発
	消費者向け大量生産工業製品, 固有ライフサイクル
	不特定多数の交通参加者, 専用E/C/Sクラス

1.4.7 規格の構成

規格の全体構成の概要は文末に載せた規格全体構成図を参照のこと。

1.4.8 セーフティーライフサイクル（抜萃）

まず 1) concept phase 2) product development 3) after SOP の主要 3 フェーズに分割ができ、1)のフェーズでは item definition→Initiation of the safety lifecycle→Hazard analysis and risk assessment→Functional safety concept と続き、その後 2) を経て 3) に進む。この部分は IEC 61508 と原則的に同じである。その概要を図 1.4.3 に示す。

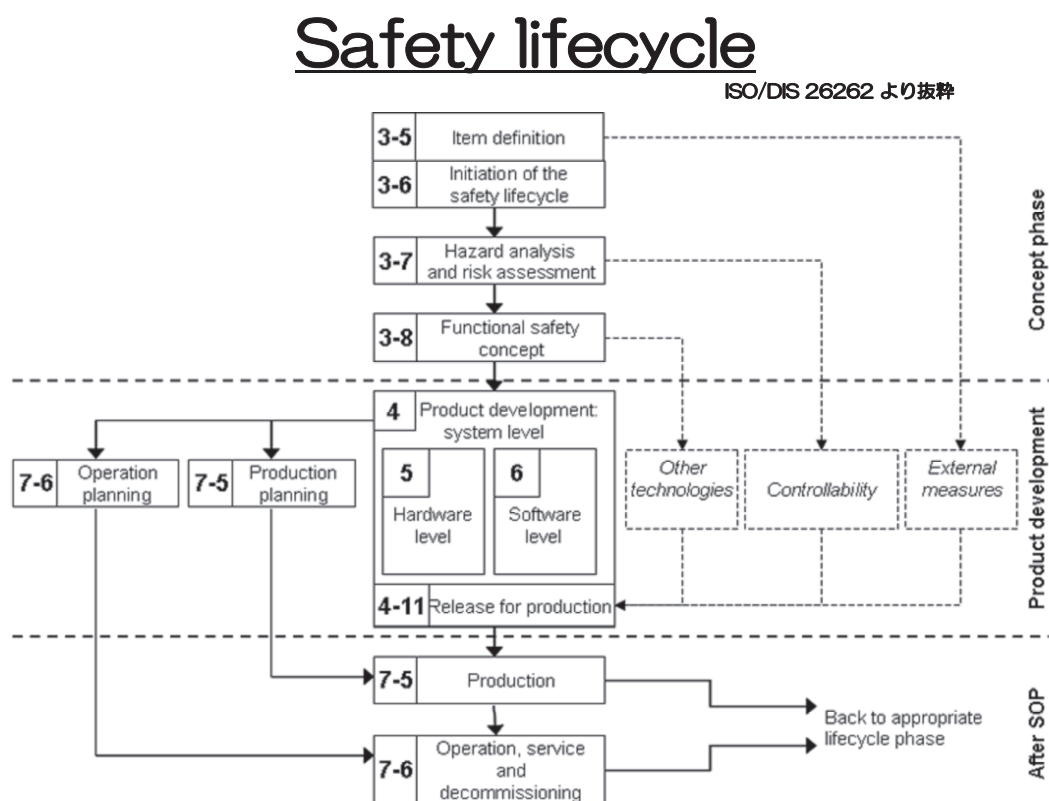


図 1.4.3（出典：日産自動車資料）

1.4.9 本質安全と機能安全

鉄道の踏切事故を例にとれば、前者が立体交差化でリスクを排除するのに対して、後者は遮断機、警報機、運用規則などの方策を組み合わせることでリスクを許容レベルまで低減するところにある。鉄道といえども場所によっては後者を適用せざるを得ず、新幹線の場合も日本国内は前者であるが、台湾においては後者であった。

自動車の場合は、そのおかれた状況から、本質安全ではなく、機能安全が適用される。

1.4.10 ASIL と H&R (Hazard & Risk) その概念

IEC 61508 においても ISO 26262 においても、リスクの重大性に対して起き得る可能性を様々な手法で低減し、最終的に許容可能なリスク (tolerable risk) まで低減することにより、対象システムの安全性を確保しようとする考え方であることは基本的にかわらない。リスク低減後に残った残余のリスクは残留リスクと呼ばれ、このリスクは許容可能なリスク以下で無ければならない。この概念を図 1.4.4 に示す。

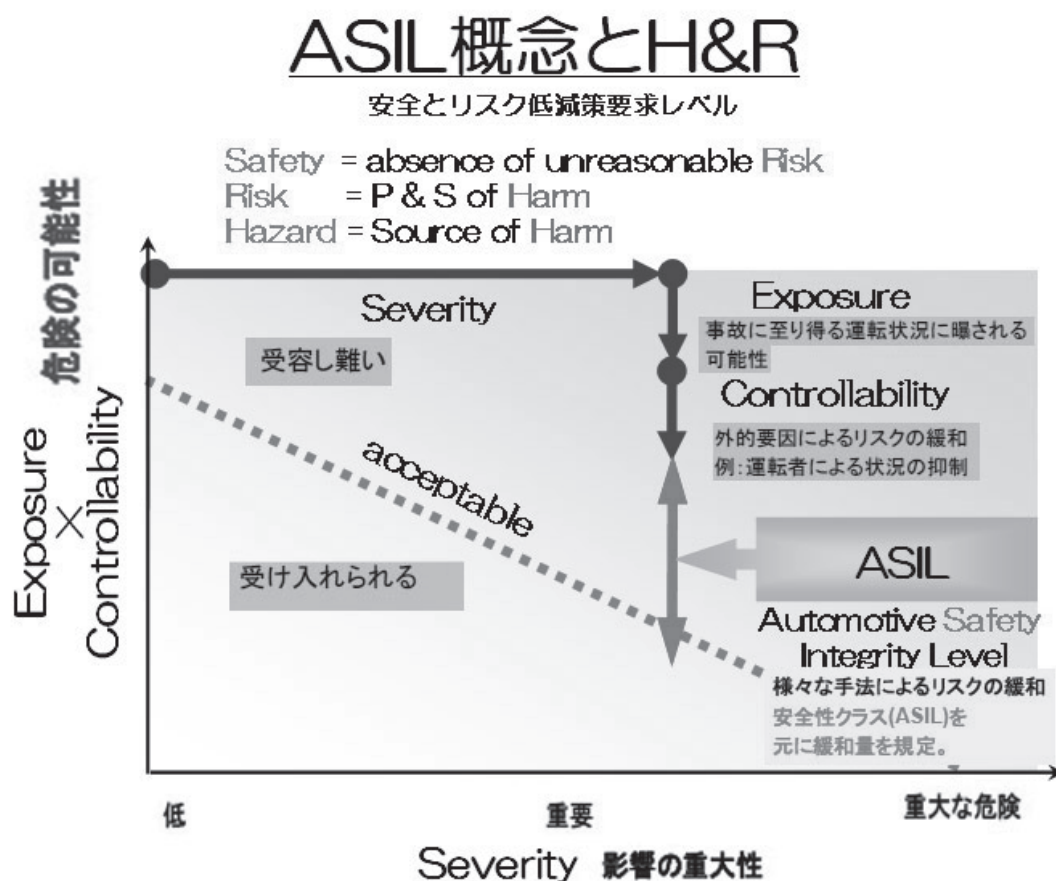


図 1.4.4 (出典：日産自動車資料)

1.4.11 ASIL determination

ASIL のレベルには A から D までの 4 段階に分かれることは前述の通りであるが、その具体的な区分けは、以下のように決められる。

Exposure を 0 から 4 までの 5 段階に分け、Controllability を同じく 0 から 3 までの 4 段階に分け、それぞれの掛け合わせの結果を、A から D までの 4 段階で表示する。具体例を図 1.4.5 に示す。

ASIL determination

E/C/S⇒ASILの概要

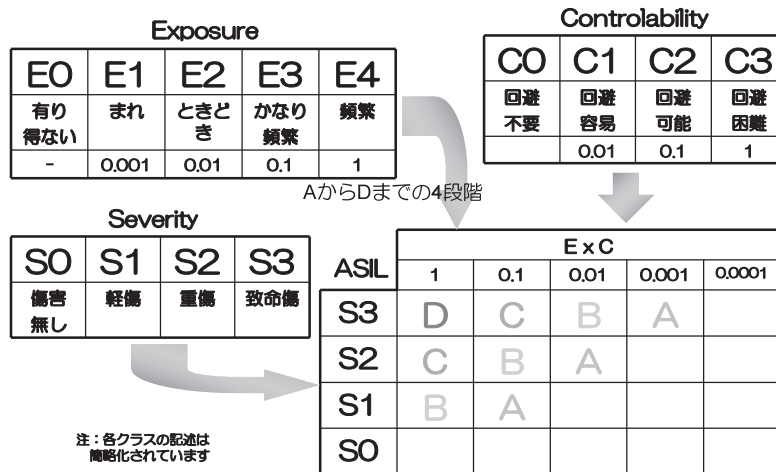


図 1.4.5 (出典：日産自動車資料)

1.4.12 運転時の ASIL 具体感

システムごとに固有の ASIL はきめられない。が、ハザード毎の ASIL 相場感というべきものは共有できるようになってきている。ただしこれはあくまで一定のシステム定義を仮定した仮値であることに注意。概要を図 1.4.6 にまとめた。

ASIL 相場感

システム毎に固有ASILは決められない

		QM	A	B	C	D
走る	急発進					
	急加速					
	駆動力喪失					
	急減速					
止まる	1 輪最大制動					
	4 輪最大制動					
	制動機能喪失					
曲がる	セルフステア					
	ステアリングのロック					
	アシスト喪失					
見える	視界喪失					

注：事象の記述は正確ではない。'走行中の'、'意図しない'等の表現が省略されている

図 1.4.6 (出典：日産自動車資料)

1.4.13 規格導入の基本手順

安全設計の基本的フローは図 1.4.7 のごとく従来からなんら変わらない、まず要求機能のデザインから始まり FMEA などによる解析を経て、十分なレベルの診断やフェイルセーフを加える、不十分と判断されれば再度設計の見直しなどを行う。規格はこの安全処置の十分・不十分の明確な判断基準を与えるものである。

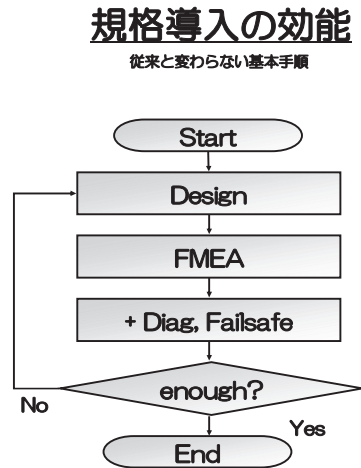


図 1.4.7 (出典：日産自動車資料)

1.4.14 安全処置の解釈の例

ASIL を横軸にとりプロダクト要件とプロセス要件に大別した具体的安全処置を縦軸にとったものを図 1.4.8 に示した。但し、これはあくまで任意に選んだ一例である。

安全処置の手厚さ解釈の例

任意に選んだ一例

安全処置の例		A	B	C	D
プロダクト要件	1st SMの装備	M	M	M	M
	2nd SMの装備		W	M	M
	1st SMの対RHF有効性（総合診断率目標）		90%	97%	99%
	2nd SMの対RHF有効性（総合診断率目標）		60%	80%	90%
	SMの対RHF有効性（総合残存故障率目標）		100fit	100fit	10fit
	ソフトエラー検知と処置	基本手法のみ ←→ 各種手法の組み合わせ			
プロセス要件	新規性・開発計画レビュー	担当設計部署内で実施		関連部署合同で実施	部門レベルでの実施
	サプライアプロセス監査				
	システム設計検証ツール	FMEA MUST		FMEA/FTA setでMUST	
	シミュレーションまたはプロトタイピングによるシステム検証	WANT		MUST	
	仕様記述手法	自然言語MUST		図式表現の併用MUST	

図 1.4.8 (出典：日産自動車資料)

プロセス要件のシステム設計検証ツールについて言えば、A,B ランクであれば FMEA だけで十分であるが、C,D ランクでは FMEA だけでなく FTA もセットで必要であり、より厳格な検証が必要であることを、この図は表している。

1.4.15 ASIL 付与のルール

基本的ルール は Inheritance, Assignment, Decomposition および Limitation である。関連する重要な概念としては、Item/Element, 要求工学、SR 割り当て、ASIL 付与がその主たるものである。Decomposition とは主機能に対して監視系を設けるなどの広義の冗長構成をとることにより、安全要件の ASIL の減免を計るものである。図 1.4.9 はその概念図である。

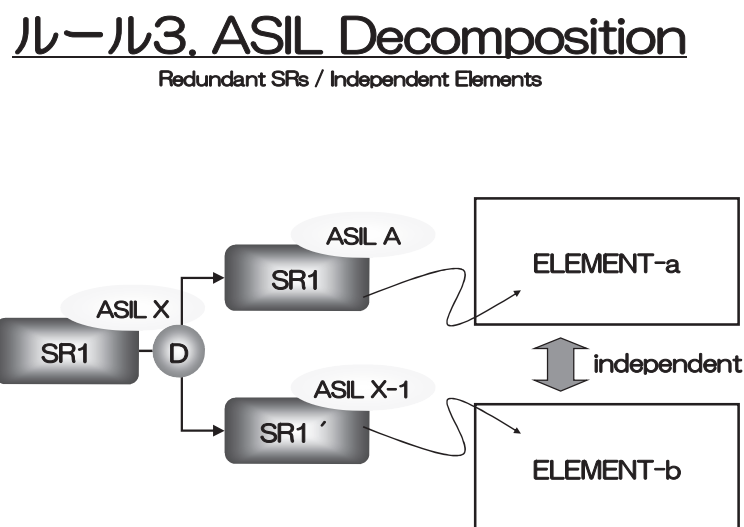
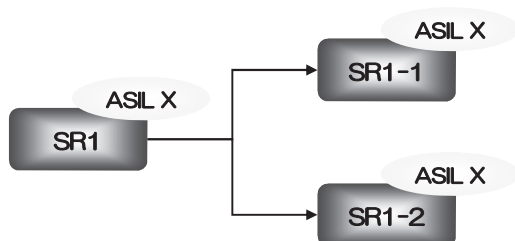


図 1.4.9 (出典：日産自動車資料)

また、導入部に於いては要求工学的アプローチの方法が推奨される。その他 Inheritance, Assignment および Limitation の各概念については以下の図 1.4.10 を参考にされたい。

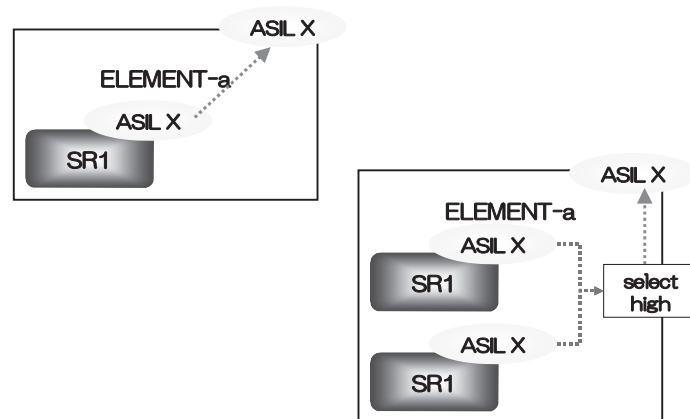
ルール1. Inheritance

ASIL on SR



ルール2. ASIL assignment

ASIL on Element



ルール4. Limitation

Limitation by interference free

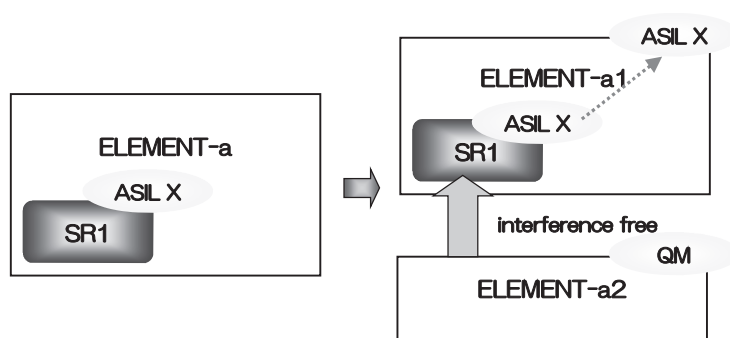


図 1.4.10 (出典：日産自動車資料)

規格全体構成

ISO/DIS 26262 より抜粋

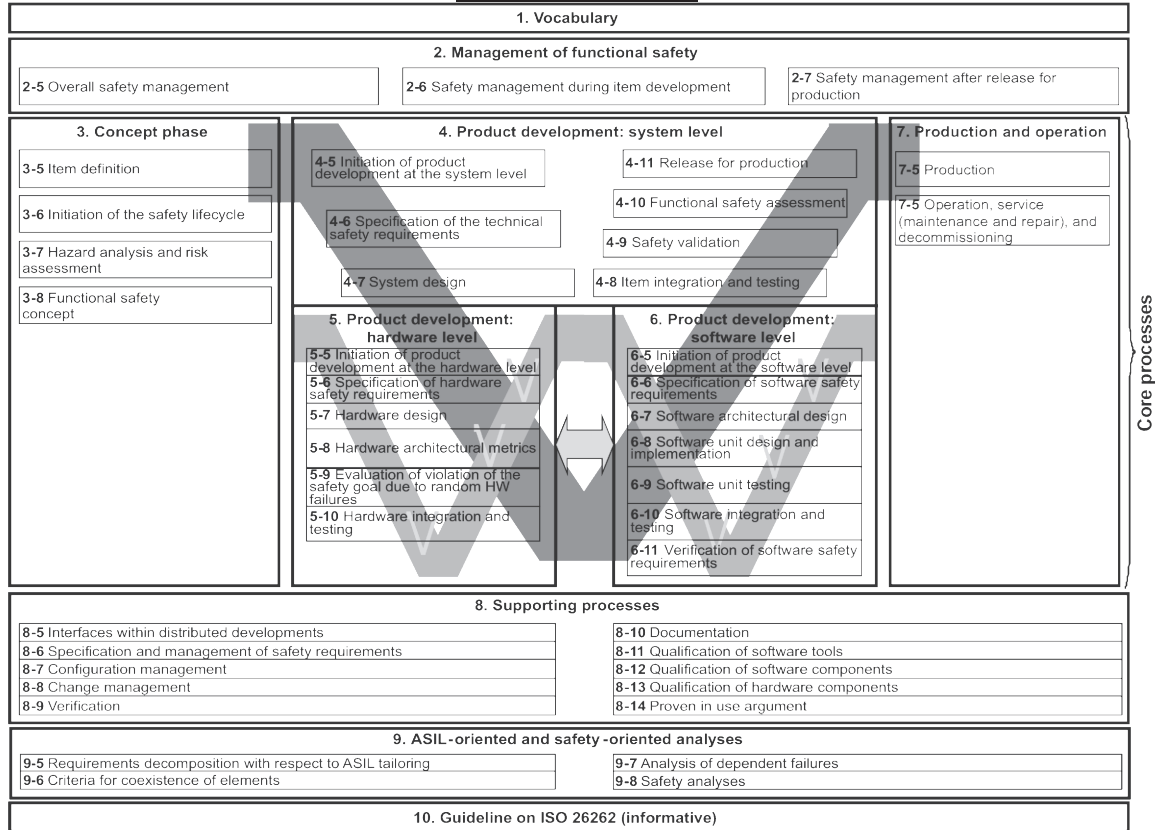


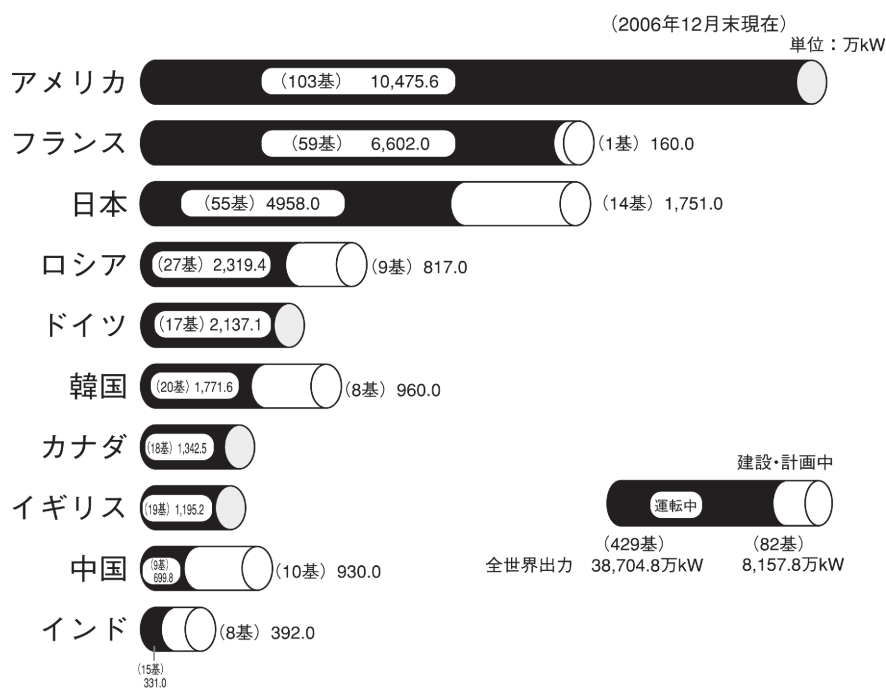
図 1.4.11 (出典：日産自動車資料)

1.5 原子力分野の安全性・信頼性対策の概要

本節は株式会社テクノバ藤田常務の御協力を得て、レポートをまとめたものである。

1.5.1 原子力発電所の概要

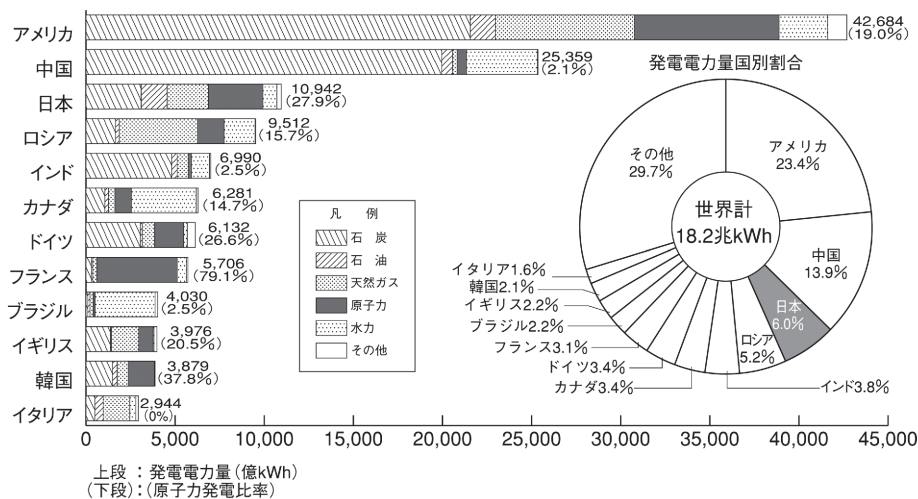
世界の原子力発電設備の状況を、図 1.5.1、図 1.5.2 に示す。また日本の原子力発電設備の分布状況を図 1.5.3 に示す。発電量では、米国が世界最大であり、仏、日が続く。日本は世界第3位の原子力大国である。ただ、最新の情報も加味すると、10～数十年のうちに中国が最大の原子力発電大国になる可能性がある。



出典：日本原子力産業協会「世界の原子力発電開発の動向2006年次報告」

図 1. 5. 1 主要国の原子力発電設備

(2005年)



出典：ENERGY BALANCES OF OECD COUNTRIES 2004-2005
ENERGY BALANCES OF NON-OECD COUNTRIES 2004-2005

図1. 5. 2 主要国の発電電力量と割合

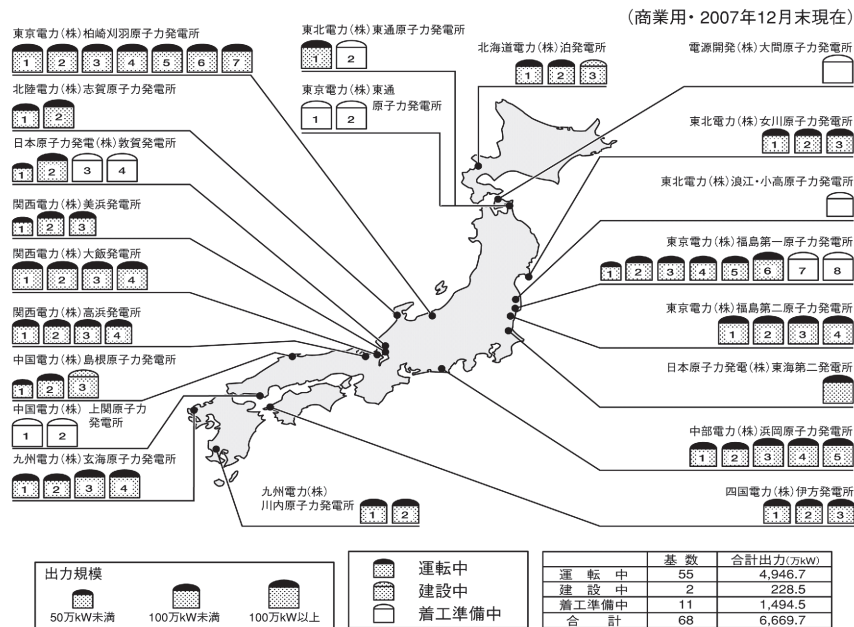


図1. 5. 3 日本の原子力発電所

日本で稼働中の商用原子力発電所は、軽水減速軽水冷却のタイプであるが、さらに加圧水型炉（PWR）と沸騰水型炉（BWR）とに分かれる。それぞれのプラント概略を図 1.5.4、図 1.5.5 に示す。

CO₂ をほとんど出さない原子力発電所は、地球温暖化対策への有効な手段であり、多くの国、特に潜在成長力の大きい国において建設計画が大きく動き出している。しかし一方で、原子力への不安は、多くの人が感じている。特に日本は、世界唯一の被爆国であり、拒否反応は大きい。原子力プラントのトラブルがどの程度周辺的安全性へ影響を及ぼすのか、わかりにくいことも不安を大きくさせる。そこで、国際原子力機関（IAEA）が国際評価尺度（INES：図 1.5.6）を定めており、日本でも原子力プラントのトラブルの都度、この尺度を利用して公表している。

1.5.2 原子力発電所の燃料

原子力発電所（原発）のエネルギー源は、ウラン燃料であるが、ウランの核分裂反応により生成されるプルトニウムもエネルギー源となる。

燃料の成分構成を図 1.5.7 に示す。天然ウランは、U238 がほとんどで核反応を発生しやすい（燃えやすい）U235 は、わずか 0.7% である。原発では、U235 を 3～5% まで比率を増やした濃縮ウランを使う。なお核兵器に使われるウランは、90% 以上の高濃縮ウランである。

1.5.3 放射能と放射線

放射能と放射線が混同しがちなので、先に定義を確認しておく。

- ① 放射能：放射線を出す能力、または放射線を出す納涼区のある物質。放射性物質。
- ② 放射線：一般的には高いエネルギーを持った電磁波や粒子線を言う。紫外線や赤外線も高いエネルギーを持つ電磁波であるが、放射線には含めていない。原子力発電所で、問題になる放射線は、アルファ線（ヘリウム原子核）、ベータ線（電子）、ガンマ線である。

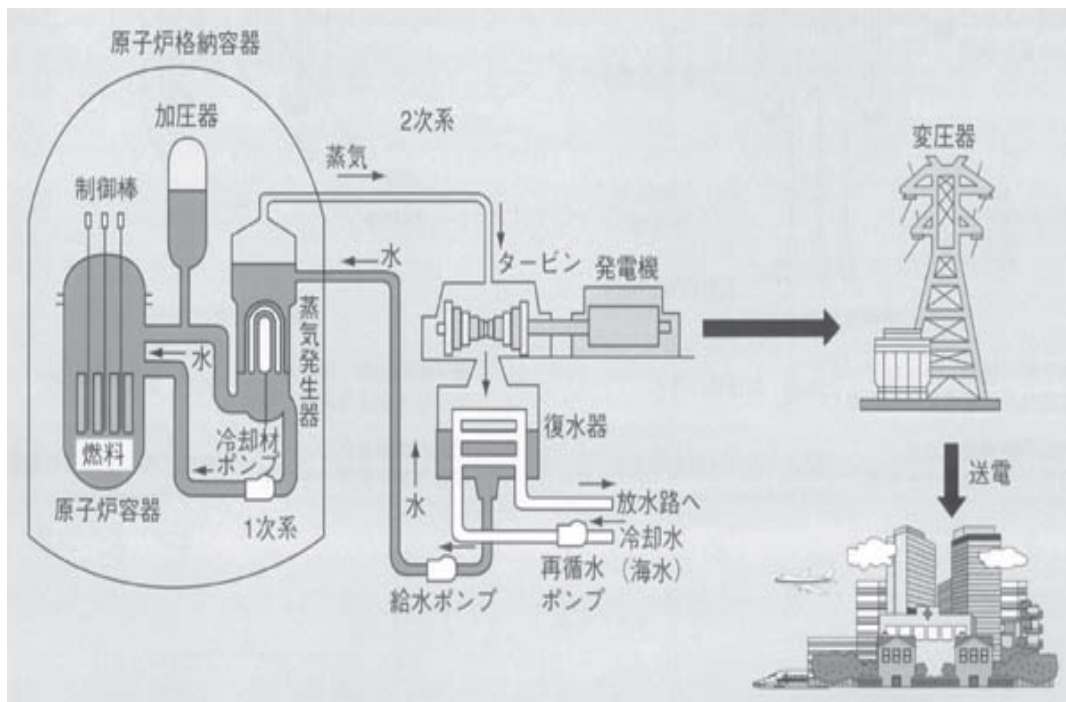


図1. 5. 4 プラント概要 (PWR)

JNES (独) 原子力安全基盤機構

防災対象原子力施設 原子力発電所の概要

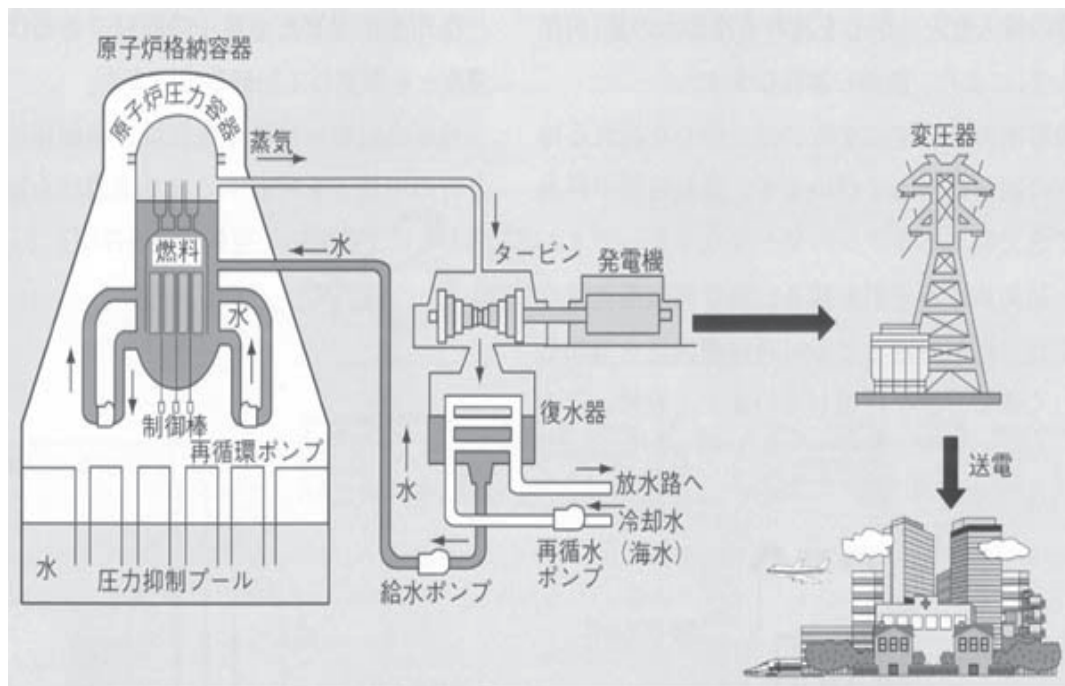
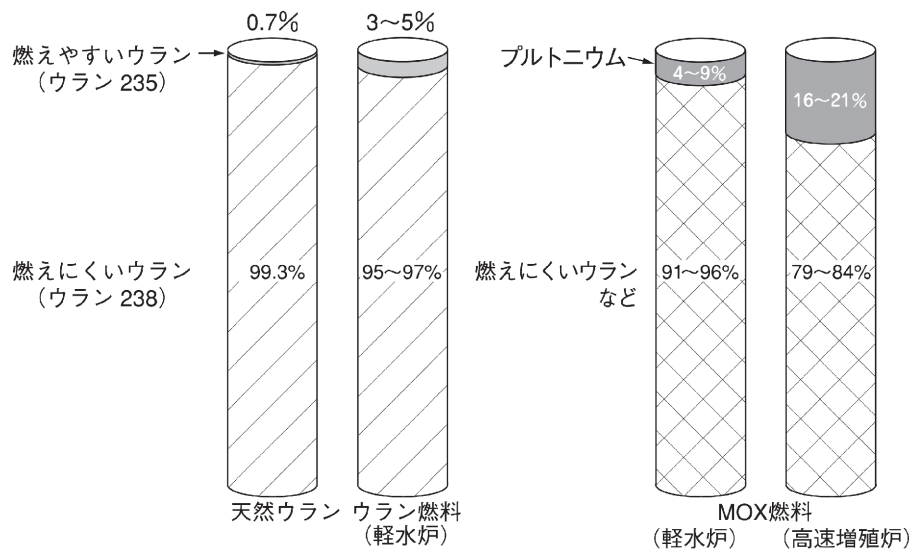


図1. 5. 5 プラント概要 (BWR)

	レベル	基準（最も高いレベルが当該事象の評価結果となる）			参考事例 (INESの公式評価でない ものが含まれている)
		基準1：所外への影響	基準2：所内への影響	基準3：深層防護の劣化	
事故	⑦ (深刻な事故)	放射性物質の重大な外部放出 {ヨウ素131等価で数万テラベクレル 相当以上の放射性物質の外部放出}			チェルノブイリ 事 故 (1986年)
	⑥ (大 事 故)	放射性物質のかなりの外部放出 {ヨウ素131等価で数千から数万テラベ クレル相当の放射性物質の外部放出}			
	⑤ (所外へのリスク を伴う事故)	放射性物質の限られた外部放出 {ヨウ素131等価で数百から数千テラベ クレル相当の放射性物質の外部放出}	原子炉の炉心の重大な損傷		スリーマイル アイランド事故 (1979年)
	④ (所外への大きな リスクを伴わない 事故)	放射性物質の少量の外部放出 {公衆の個人の数ミリシーベルト程 度の被ばく}	原子炉の炉心のかなりの損傷/ 従業員の致死量被ばく		J C O 臨 界 事 故 (1999年)
異常な 事 象	③ (重 大 な 異 常 事 象)	放射性物質の極めて少量の外部放出 {公衆の個人の十分の数ミリシー ベルト程度の被ばく}	所内の重大な放射性物質による 汚染／急性の放射線障害を生じ る従業員の被ばく	深層防護の喪失	
	② (異常事象)		所内のかなりの放射性物質に よる汚染／法定の年間線量限 度を超える従業員の被ばく	深層防護のかなりの劣化	美浜発電所2号機 蒸気発生器 伝熱管損傷 (1991年)
	① (逸 脱)			運転制限範囲からの逸脱	もんじゅ ナトリウム漏えい (1995年)
	① (逸 脱)				
尺度以下	① (尺度以下)	安全上重要ではない事象			
評価対象外		安全に関係しない事象			

シーベルト(Sv)は、放射線が人体に与える影響を表わす単位。(ミリは1,000分の1)
ベクレル(Bq)は、放射性物質の量を表わす単位。(テラは10¹²=1兆)

図 1. 5. 6 国際原子力事象評価尺度



MOX(Mixed Oxide)燃料：プルトニウムとウランを混ぜ合わせて作った燃料(ウラン・プルトニウム混合酸化燃料)で、軽水炉のプルサーマル計画や高速増殖炉などで使用される。

図 1. 5. 7 原子力発電所の燃料構成

自然界には、多くの放射性物質があり、人は常に放射線を浴びている。日光浴が度を過ぎると有害のように放射線も大量に浴びると有害である。日常浴びる放射線の量について図 1.5.8 に示す。また、原子力発電所など放射線作業従事者が年間浴びている放射線量について図 1.5.9 に示す。原子力発電所が運転中に外部へ放出する放射線は自然界の放出量に較べてわずか数%にすぎず、作業員が浴びる放射線は、医療検診で浴びる量に較べて 2 桁以上低い。

放射能がもし外部へ放出されると、その放射能が放射線を出し続けるので、非常に問題となる。なお、一般的には、気体性の物質（原子番号の小さい物質）は半減期が短く、固体物質は半減期が長期になる。

原子力発電所では、放射能を閉じ込めること、特に半減期の長い物質を閉じ込める事が、安全性確保の最重要課題である。

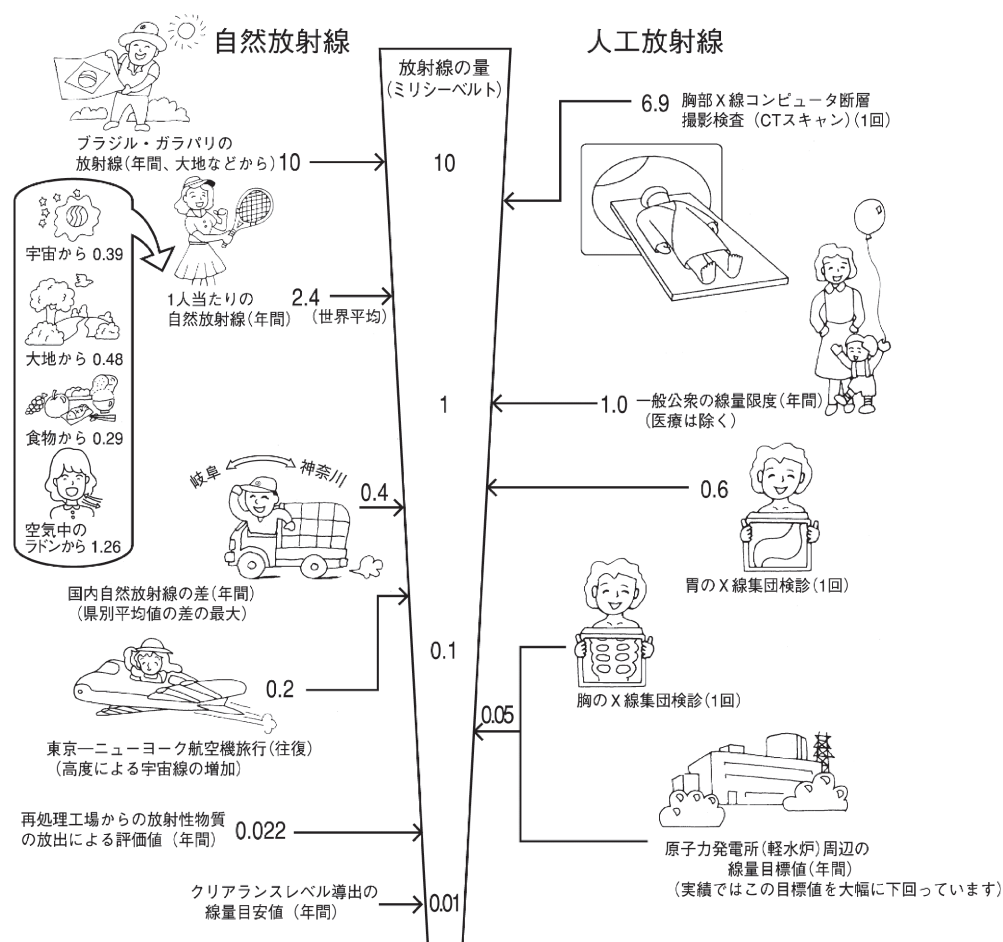
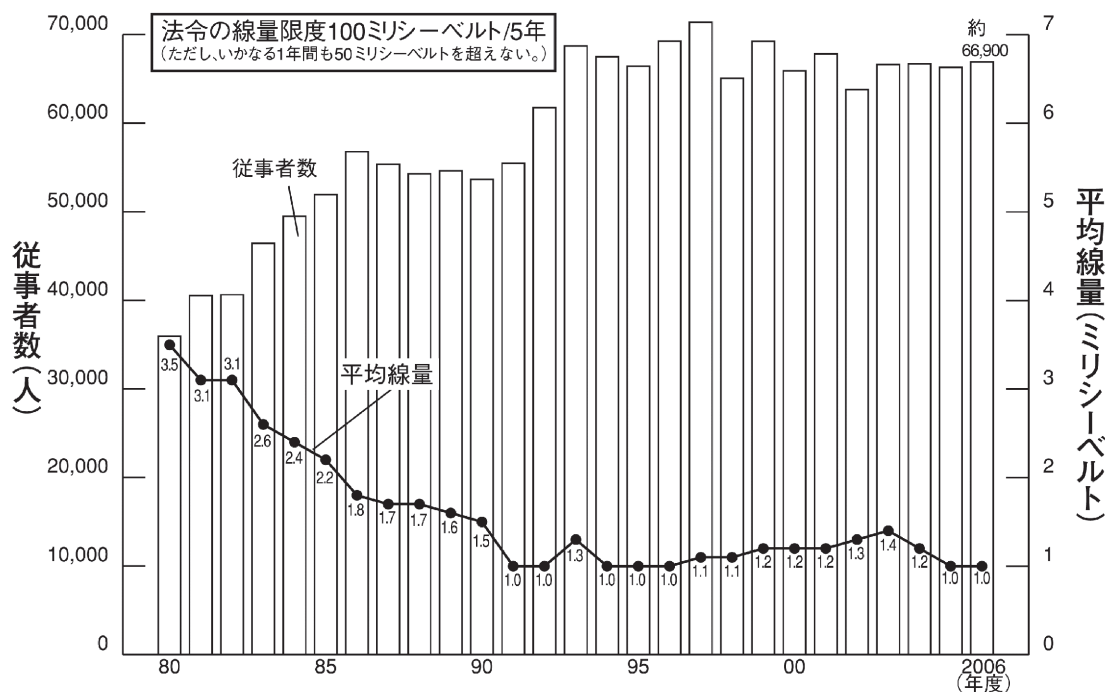


図 1. 5. 8 日常生活と放射線量



出典：原子力施設運転管理年報（平成19年版）

図 1. 5. 9 作業者の放射線量

1.5.4 原子炉の安全設計

原子力発電所の安全確保については、一般産業と異なり、強い放射性物質を扱っていることから、格段に厳しい規制が制定されており特徴ある設計思想がとられている。

(1) 安全確保の基本的考え方

原子力発電所の安全確保のうえで、基本的な思想は、深層防護といわれる思想である。多重防護、多層防護（注：最近では深層防護と多重防護を使い分ける専門家も増えている→コラム参照）と呼ぶこともある。これは、第一に異常の「発生防止」、第二に発生した場合の「拡大抑制」、第三に発生後の影響を最小限に食い止める「影響緩和」という考え方である。資源エネルギー庁が示している安全確保の全体像について、図 1.5.10 に示す。

① 異常発生防止

事故発生を未然に防止するために、事故に至る恐れのある事象や要因をできるだけ取り除いた信頼性の高い設計を行う。重要な系統については、性能、経年劣化等に対して充分余裕の持った設計を行う。運転についても制限範囲に対し余裕を待たせること、等が該当する。

② 異常拡大抑制

深層防護の第一段階である異常の「発生防止」が計画されたとおりに機能したとし

ても、予期せぬ天変地異や想定外の事態が全く発生しないとは言えない。そのため、万一異常が発生しても、これを大事に至る前に検出して、原子炉を安全な停止状態に移行させる仕組みを設けることである。

③ 異常影響緩和

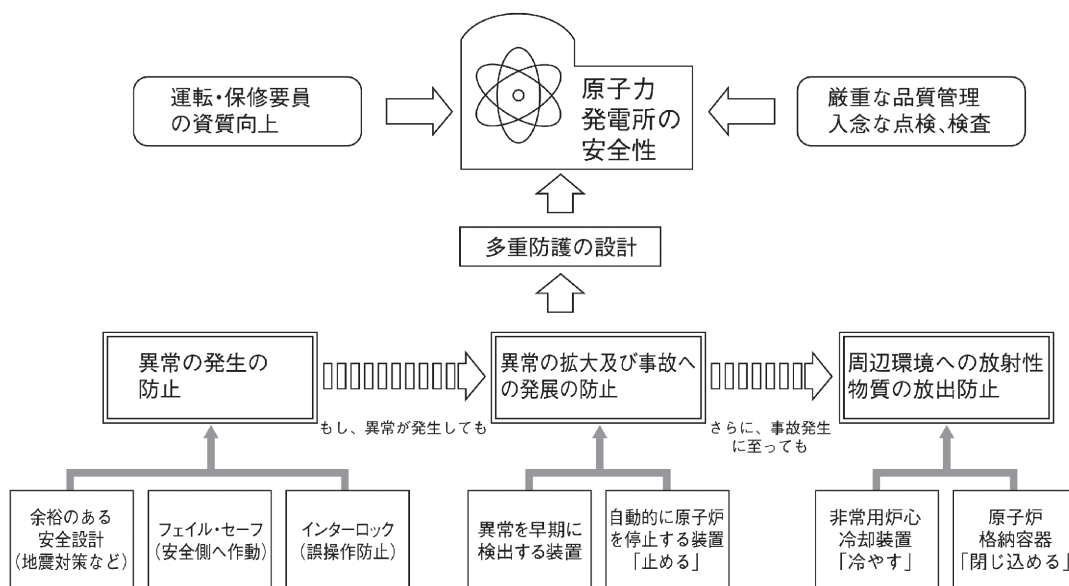
深層防護の第一段階、第二段階の備えにも係らず、異常が事故へと拡大した場合に備え、放射能を閉じ込めることである。換言すると周辺環境への放射能放出を防止する仕掛けを設けることである。軽水炉では、冷却水（軽水）の確保が、放射能閉じ込めの基本となる。

④ アクシデントマネジメント

前述までの「発生防止」、「拡大抑制」、「影響緩和」の深層防護の考え方により安全は十分に確保されると考えられるが、それでもなお、機器の故障が複数同時に発生し、さらに複数の操作ミスやその他の事象が幾つも重なることにより、想定外の重大事態（シビアアクシデント）が発生するかもしれないと考えて、シビアアクシデントの発生防止、影響緩和等の対策を検討・整備し、さらに発生時の対処手順なども整備している。

⑤ 防災

以上の諸々の対策にも係らず放射性物質が放出され、周辺市民へ危害を及ぼす事態を想定して、周辺住民の避難や保護対策などの整備と訓練も進められている。



出典：資源エネルギー庁「原子力2007」

図 1. 5. 10 安全確保の全体像

コラム 深層防護、多重防護、多様性

深層防護も多重防護もほぼ同義語として扱っているケースが多いが、最近の研究では、以下のように使い分けるケースもあるようである。

多重防護は、同等の安全系を複数設置することで安全系の故障による被害を防ぐ。一方、深層防護は、ひとつの安全系で防ぎ切れなかった事象を、異なる方法によって次の段階で事象の影響を抑制し、被害を最小限にとどめる考え方である。

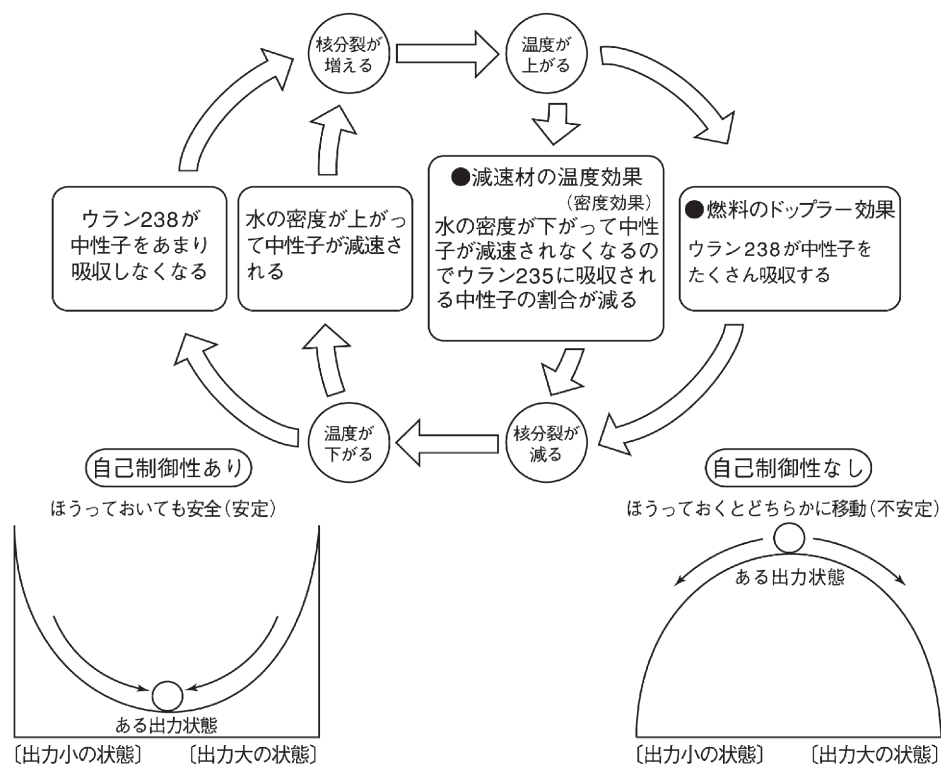
多様性は、異なる考え方の安全系を用いる。Defense in Depth+Diversity で D3 と呼ばれることが多いが、これは、深層防護+多様化のことで原子力分野でよく使われる。原子力では、デジタル系による自動停止システムと、運転員による監視とハードウェアによる手動停止の組み合わせを、多様化と呼んでいる。

S. K

(2) 安全設計の特徴

①原子炉固有の安全性（自己制御性）

日本の商用原子力発電所は、軽水冷却軽水減速のタイプであるが、この炉は、核分裂が増えて出力が増大（温度上昇）すると、核物理的特性により、核分裂が抑制される仕組みになっている（図 1.5.11 参照）。発電所の出力を上げるためには、制御棒を引き抜くなど、核分裂に有効な中性子束密度を増やす必要があるが、中性子束密度を上昇させても、すぐ負のフィードバックが効くので、穏やかに安定的に出力変化させることができる。



出典：資源エネルギー庁「原子力2007」他

図 1. 5. 11 原子炉固有の安全性

③ 止める、冷やす、閉じ込める機能

原子力発電所の特徴的な安全設備として、前述の「拡大抑制」と「影響緩和」に相当する「止める」。「冷やす」。「閉じ込める」機能が用意されている。止める機能は、放射線量の増加や地震の振動大等のような様々な異常兆候を、4重化された多様な検出器で捉えて、すべての制御棒を原子炉へ急速挿入させて核反応を停止（原子炉停止：スクラム）させる。

また、原子炉の冷却水が減って燃料の冷却効率が低下すると燃料が高温損傷する可能性があり放射能の放出につながる恐れがあるため、通常の給水系以外に非常用炉心冷却系（ECCS）を用意して炉内に注水するようになっている。これが冷やす機能である。

さらに、万一燃料の損傷によって、放射能が放出されても格納容器内に閉じ込めて外部への漏れを充分低くするような多くの設備で構成されている。

④ 5重の壁

閉じ込める機能を確実に確保するための設計として、5重の壁が用意されている。

図 1. 5. 12 にそれを示す。第一の壁は、燃料ペレットである。燃料ペレットは、酸化ウランの粉末を焼き固めたセラミックであり、核反応によって生成される核分裂性物質を

保持している。第二の壁は、燃料被覆管（燃料棒）である。燃料ペレットは、長尺円筒形の燃料棒の中に封入されている。ペレットから放出される核分裂生成物は、燃料棒内に保持される。第三の壁は、原子炉压力容器と周辺の配管及び隔離弁（原子炉冷却材圧力バウンダリー）である。万一燃料棒が破損して核分裂生成物が冷却水中に放出されても、このバウンダリー内に閉じ込める。第四の壁は、原子炉格納容器である。万一バウンダリーの外へ冷却水が流出する事故が発生しても、機密性の高い原子炉格納容器内に放射性物質を閉じ込める。第五の壁は原子炉建屋である。原子炉格納容器から漏れ出てくる放射性物質を保持し、気体性廃棄物などは、外部環境へ放出する前にフィルター処理し、安全なレベルまで線量を減少させる。

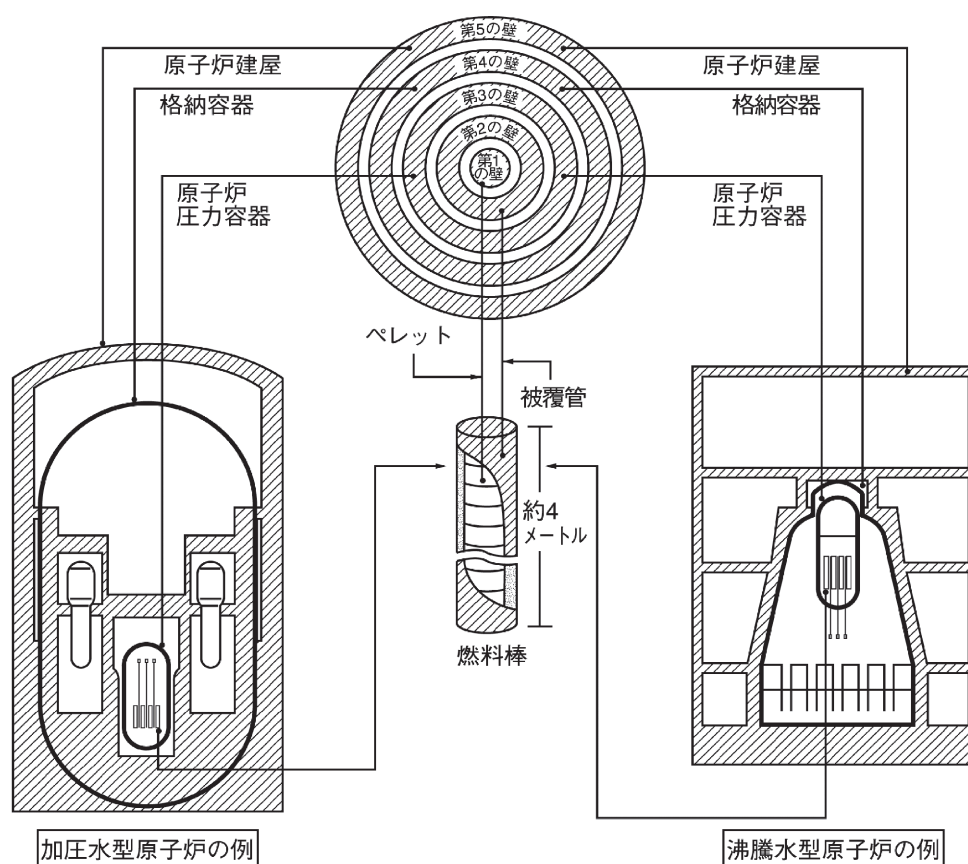
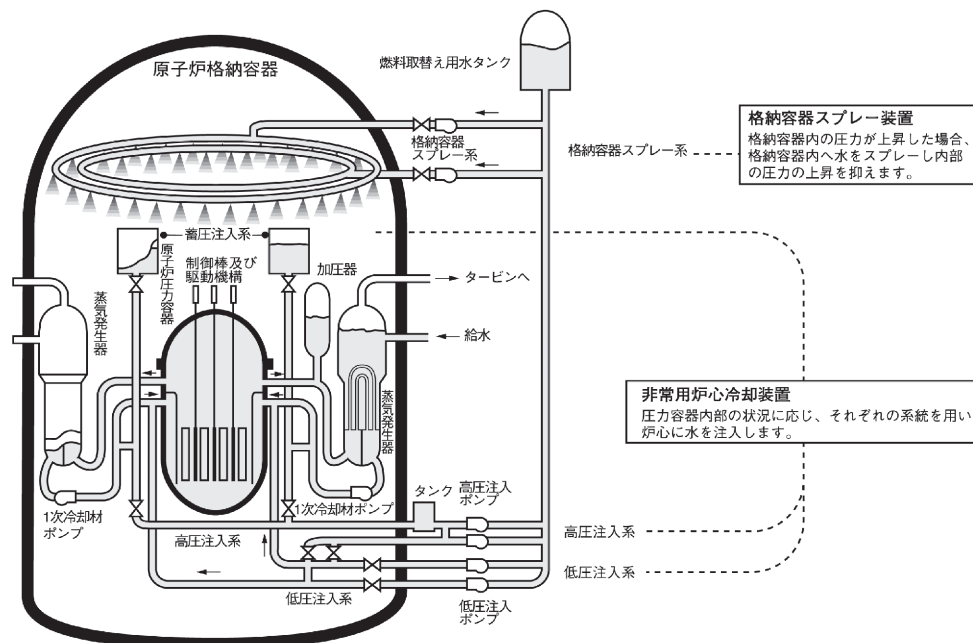


図 1.5.12 五重の壁

⑤ 工学的安全施設

万一、設備の故障や破損が生じても放射性物質の拡散が防止・抑制されるように、工学的安全施設と呼ぶ設備が用意されている。工学的安全施設には、事故時に炉心に冷却水を注入する非常用炉心冷却系（ECCS : Emergency Core Cooling System）や放射性物質の大気放出を抑制する非常用ガス処理系、放射性物質を閉じ込める原子炉格納容器などがある。

ECCSには、図1.5.13に示すように原子炉内圧力が高圧時に注水できる高圧注入系と、原子炉内圧力が低圧時に大量注水する低圧注入系がある。設備の重要性を考慮して設備の多重化、多様化が図られている。またディーゼル発電機も備えられ外部電源がなくても機能できる。



出典：資源エネルギー庁「原子力2007」

図 1. 5. 13 非常用炉心冷却系

⑥ 耐震対策

原子炉建屋は、堅固な地盤（岩盤）上に設置される。さらに過去の推定される最大地震に尤度を持たせた想定最大地震に堪えるような耐震設計がなされている。

⑦ 高信頼設計

前述のように、原子力発電所は、さまざまな安全対策がとられているが、実際に必要な時に必要な機能を発揮するためには、個々の機器や部品と、その構成が十分な信頼性を確保していなければならない。また、様々な環境条件や保守性、操作性も考慮して、機器の故障や運転員の誤操作、誤不操作があっても安全性が損なわれないような工夫がなされている。信頼性確保の主な方式を列記する。

- フェイルセーフ ： 機器故障、電源喪失、誤操作などが生じてても機器や系統（システム）が安全側に動作するように設計すること。

- インターロック : 所定の条件が満足されない限り次の操作または運転続行が許容されないようにすること。一定の条件が整わない限り操作や運転ができないようにして、誤操作や故障波及を防止する。
- 冗長化・多重化 : 単一故障が発生しても機能が維持するよう、同一機能を有する機器や系統を多重に設置すること。
- 多様性の確保 : 共通要因によって多重化している機器や系統が同時に故障することを避けるために、同一機能であっても設計概念や動作メカニズムの異なる機器や系統を設けること。
- 独立性 : 多重性、多様性を有する機器や系統が、共通要因によって機能喪失することのないように機器や系統を相互に分離配置すること。
- HE 回避 : 運転や保守に関する誤操作（HE : Human Error）を回避するために、表示器や操作スイッチは一定の設計ルールによって形状や色などを統一している。さらに運転シミュレーションを行って、ご操作の発生しやすいデザインの検出・改良を行っている。

(3) 安全評価

前節で述べた安全設計の思想について、意図した通りの安全性を有しているかどうかを解析・評価するのが安全評価である。原子力発電所で発生しうる多くの異常事象を原子炉への影響や予想発生頻度から類型化して、それぞれの種類のなかで代表的な異常事象を選定し、発電所の応答解析を行い主要パラメーターが基準を満足していることを確認する。通常考えられる最も厳しい単一故障の発生を想定し、最も厳しいシナリオで、他の条件も保守的に想定してもなお安全性が確保されることを示す。

上記の類型化した異常事象のうち放射性物質放出の可能性のある事象を重大事故として取り上げ、さらにより多くの放射性物質放出量を想定した仮想事故を仮定して、非居住区域の範囲の妥当性や人口密集地からの距離の確保等を確認する「立地評価」も行われる。

(4) リスク評価とアクシデントマネジメント

前述の安全評価に加えて、スリーマイルアイランド原子力発電所 2 号機（TMI-2）の事故以降、確率論的な安全評価（PSA : Probabilistic Safety Assessment）手法が評価されるようになってきた。

PSA を行うことによって炉心損傷確率（シビアアクシデントの発生確率）が定量的に求められる。日本の原子力発電所におけるシビアアクシデントの発生確率は、工学的には現実に起こらないと言えるぐらい極めて小さいと言われている。しかし、なお残存するリスクを可能な限り小さくするよう活動しているが、この活動をアクシデントマネジ

メント（AM）と言っている。1994年にAM整備方針がまとめられ、設備、手順書、組織などの見直しが行われ、2002年に完了し、AM実施後のPSA評価によってさらに大きく安全性が向上したと言われている。

(5) 原子力防災

確率論的には放射性物質の周辺への放出はほとんど考えられないが、そうした実態と切り離して、原子力発電所等のある地域は原子力災害に対して地域防災計画を策定している。防災計画の中でも原子力防災は、放射性物質が目に見えないだけに専門機関の役割が重要になっている。一方で、通報連絡、住民の避難処置、飲食物の摂取制限など、一般の防災対策と共通していることも多いので、地域防災計画（原子力災害対策編）は、災害対策基本法と原子力災害対策特別措置法とに基づいて策定されている。

1.5.5 制御室の国際規格

原子力発電所に関する国際規格や法令は数多いので、本書では制御室や計測制御系に係るものを取り上げる。

(1) 規格の審議体制

原子力発電所の制御室や計測御系については、IEC／TC45（International Electrotechnical Commissions:国際電気標準会議／Technical Committee:専門委員会）にて、原子力計測（Nuclear Instrumentation）を審議している。TC45の下にSC45A（原子力施設の計測・制御）と、SC45B（放射線防護計測）という2つの分科委員会（SC: Sub Committee）が設置されている。さらに具体的なテーマ毎に作業グループ（WG）が組織され規格の審議を進めている。制御室については、WGA8が担当している。

(2) 制御室の国際規格

代表的な規格は、IEC60964 Ed2 Nuclear Power Plants – Control Rooms – Design で、2009年2月に第2版が発行されている（初版は1989年3月発行）。プロジェクトリーダーは、日本の藤田祐志氏が担当している。IEC60964は、TMI事故後の制御室設計のあり方をまとめたものである。特徴は、

- a. 「Control Room System」の概念を明確化し網羅的で一貫性のある制御室設計の推進に規格の面からアプローチしたものであること。
- b. 機能設計から詳細設計にわたり一貫性あるスパイラル設計を求めている。人間中心設計を標榜するプロセス規格の先駆となるものである。

（注：スパイラル設計とは、トップダウン設計とボトムアップ設計を組合せ、）

V&Vを繰り返して設計を煮詰める設計プロセスのこと）

IEC60964 では、制御室が「Human-Machine Interface」、「Operating Procedures」、「Control Room Staff」、「Training Program」の4つから構成されていると考え、スパイラル設計を進めるべきとする。この概念を図 1.5.14、図 1.5.15 に示す。

また、IEC60964 の関連規格を図 1.5.16 に示す。

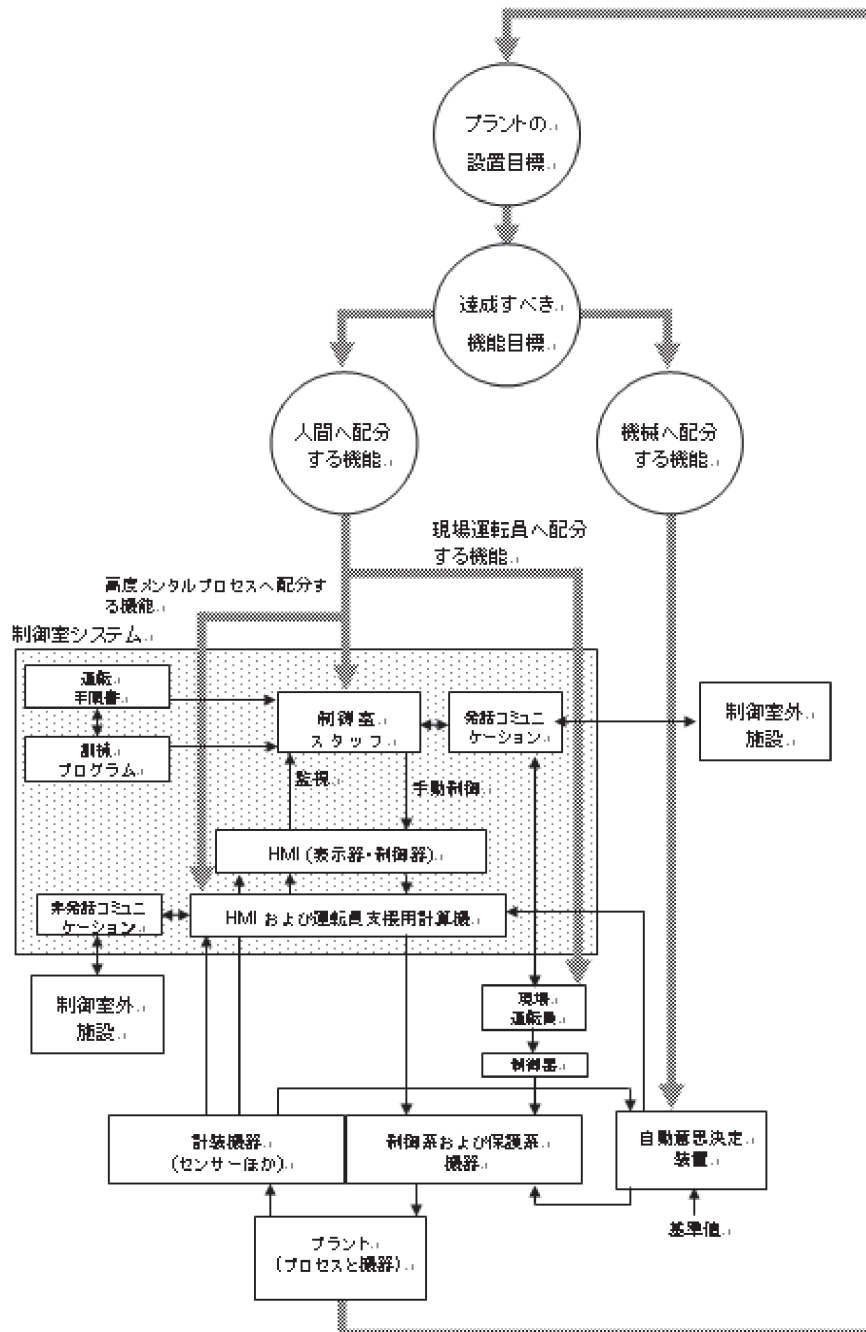


図 1. 5. 14 制御室システムの概要

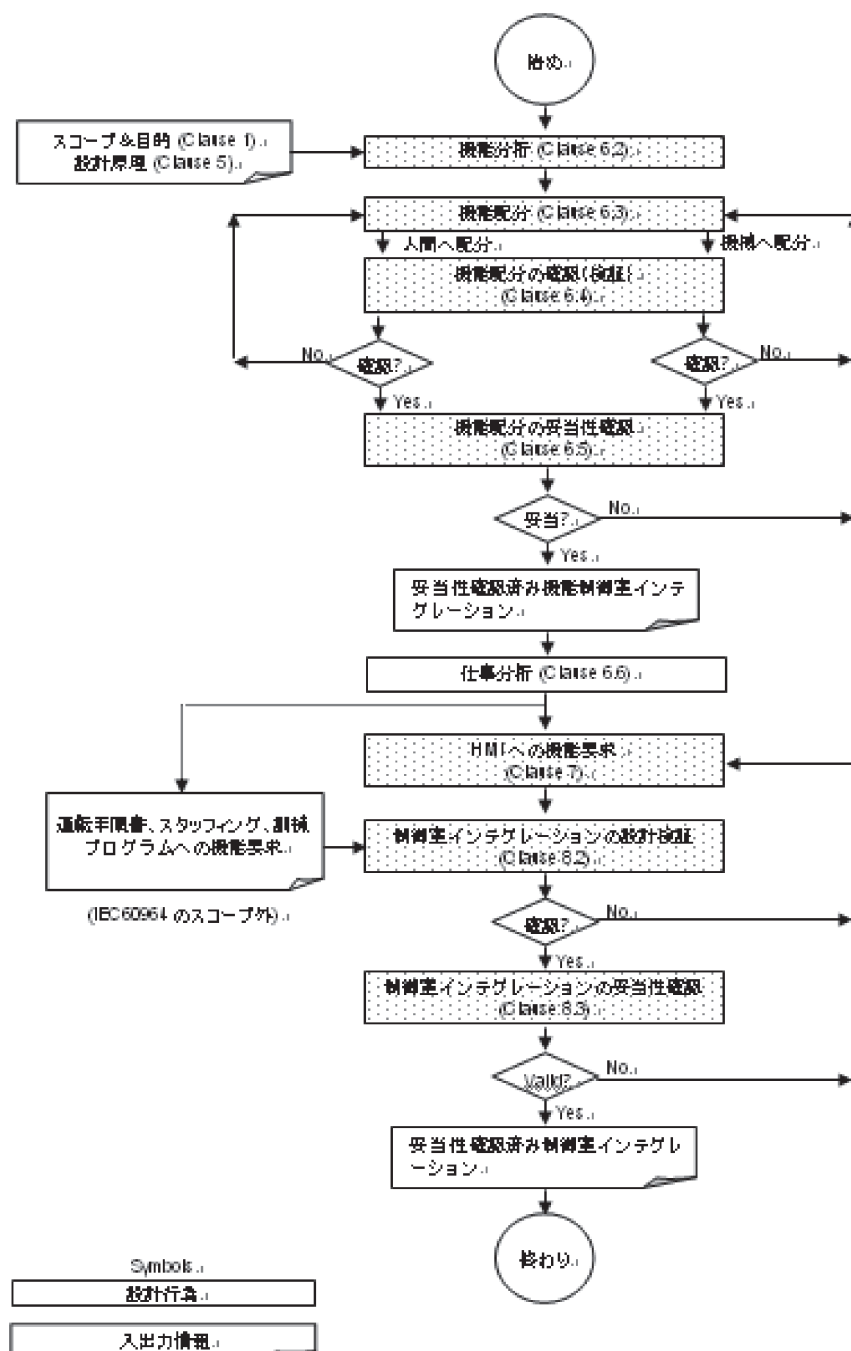


図 1. 5. 15 制御室設計のプロセスと標準

規格番号: 名称	内容
IEC60960: Functional design criteria for a safety parameter display system for nuclear power stations	SPDS (安全パラメータ表示システム) の機能設計標準を定める。
IEC60965: Supplementary control points for reactor shutdown without access to the main control room	中央制御室外緊急停止盤の機能設計標準を定める。
IEC60964: Design for control rooms of nuclear power plants	中央制御室設計の設計手順および関連する標準を定める。WGA8所掌の規格群の最上位に位置する所謂「親規格」
IEC61227: Nuclear power plants – Control rooms – Operator controls	中央制御室の制御器(スイッチ等)の機能設計標準を定める。
IEC61771: Nuclear power plants – Main control-room – Verification and validation of design	中央制御室設計のV&Vに関する標準を定める。
IEC61772: Nuclear power plants – Main control room – Application of visual display units (VDU)	中央制御室の表示器(表示計等)の機能設計標準を定める。
IEC61839: Nuclear power plants – Design of control rooms – Functional analysis and assignment	中央制御室設計における人間と機械の機能分担に関する標準を定める。
IEC/TR61963: Nuclear power plants - Main control room - Comparison of IEC 60964 to similar standards on control room design	IEC60964と、同規格に類似した規格との比較をまとめた技術報告書
IEC 62241: Nuclear power plants - Main control room - Alarm functions and presentation	中央制御室の警報の機能設計標準を定める。
IEC/TR 62247: Nuclear power plants - Main control room design - A review of the application of IEC 60964 (1989)	IEC60964の適用状況をまとめた技術報告書
IEC/IEEE 62646 Ed. 1.0 publication, Nuclear Power Plants - Control Rooms – Computer based procedures	計算機化手順書に関する標準を定める。IEC-IEEE Dual Logo 候補

図 1. 5. 16 IEC60964 関連規格

参考文献

1. 第 16 回 JASA/ET セミナー 2009 年 10 月 16 日 組込みシステム技術協会
http://www.jasa.or.jp/top/activity/jevent/40th_result.html
2. 発変電工学総論 電気学会大学講座 2007年11月20日 電気学会 (発売元オーム社)
3. 日本工業標準調査会 国際標準について
<http://www.jisc.go.jp/international/iec-tc.html>
4. 日本電気計測器工業会 (JEMIMA) IEC/TC45 (原子力計測)
<http://www.jemima.or.jp/press/pdf/news090911.pdf>
5. 電気事業連合会ホームページ
<http://www.fepc.or.jp/present/safety/index.html>
6. 原子力安全基盤機構
<http://www.jnes.go.jp/>
7. 日本電気協会 原子力規格委員会
<http://www.denki.or.jp/committee/nuc/index.html>

1.6 ソフトウェアの安全

本節はビジネスキューブ・アンド・パートナーズ株式会社の御協力を得て、レポートをまとめたものである。

1.6.1 ビジネスキューブ・アンド・パートナーズ株式会社の活動概要

ビジネスキューブ・アンド・パートナーズ株式会社は 2000 年 7 月に創業し、ハイテク製造業向けコンサルティングや新規事業プロデュース、プロフェッショナルコミュニティ運営などを手掛けている。近年では、ISO/IEC 15504 (Automotive SPICE 含む) や CMMI などのプロセスモデルや IEC 61508/ISO DIS 26262 の機能安全規格に基づいたコンサルティングサービスを実施され、高い評価を得ている。特に、フォードグループからアジア地域では唯一のソフトウェア品質パートナーに認定されている。また、上記のコンサルティングサービスに関連したトレーニングに加えて、各種ソフトウェア開発手法や定量的な信頼性/安全性評価法も多数提供している。

連絡先：

本社 東京都渋谷区恵比寿 1-20-18 三富ビル新館 10F

Tel : 03-5791-2121

URL <http://biz3.co.jp/>

1.6.2 ソフトウェア製品の問題事例について

近年、ソフトウェア製品は市場ニーズに応じて、開発期間は短縮される中、多種・多様な機能を実装するために大規模化・複雑化の一途を辿っている。この様な状況下において、ソフトウェア製品の信頼性・安全性の低さが問題視されるようになってきた。つまり、運用段階において、ソフトウェア内に潜在する論理的な欠陥や誤り、いわゆるソフトウェア・フォールト（以下、フォールトと略す）により引き起こされるソフトウェア故障が表面化すると、ユーザに多大な影響を及ぼし、さらには人命に関わる重大な事故を引き起こす場合も考えられる。その一例として、エンタープライズ系システムでは、2005 年 12 月 8 日にみずほ証券株式会社によるジェイコム株式会社株の誤発注を取り消せない問題が発生し、これによりみずほ証券株式会社は 200 億以上の損害を被った事例を紹介し、組込系システムでは、車載ソフトウェアの問題事例の推移を日経 Automotive Technology2007 年 9 月号に掲載されたデータを用いて紹介している（図 1.6.1 参照）。

ECU不具合の増加と、受入検証の限界 ⇒ ソフトウェアに起因した問題増加

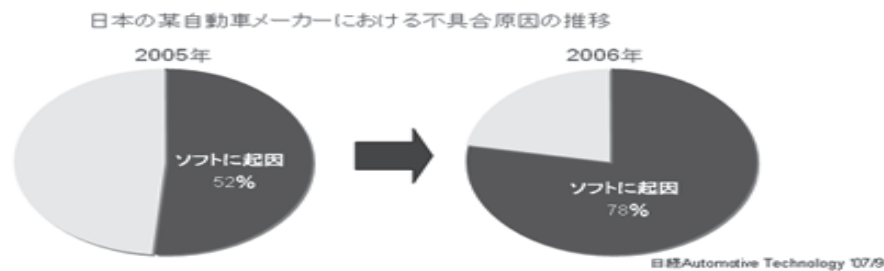


図 1.6.1 車載ソフトウェアの問題事例.

ここで、”Fault” と”Failure” が規格においても混同されているケースがあるので、図 1.6.2 に示すように”Fault” と”Failure” を定義し、図 1.6.3 で IEC61508 や MISRA-SA での考え方を紹介している：

故障 (Failure)
● システムの指定性能からの逸脱 ● 故障はシステムの障害または誤り (Error) の結果である
障害 (Fault)
● システムの誤りに至る異常状態 ● 障害は偶発的または系統的である
エラー (Error)
● システム内に障害を作り込む原因となった人的作業

図 1.6.2 語句の定義.

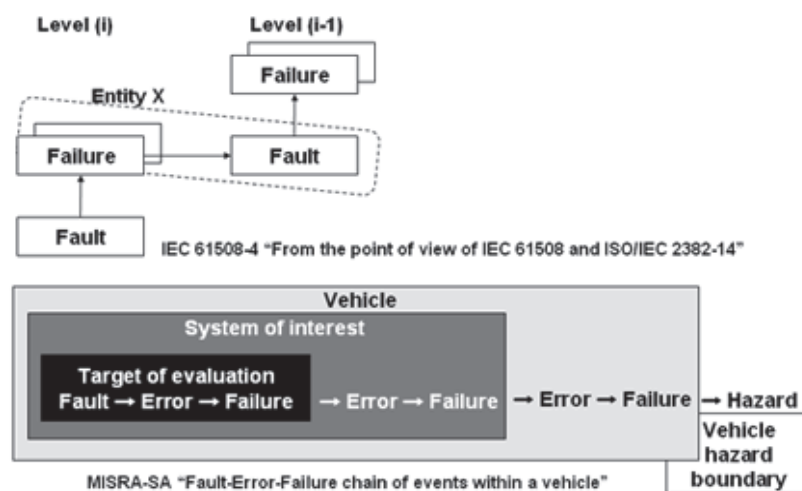


図 1.6.3 IEC 61508-4 及び MISRA-SA での”Fault” と”Failure” の考え方.

1.6.3 ソフトウェア製品の問題事例解決に向けて

ここでは、車載ソフトウェア開発における取組について紹介する。

車載ソフトウェア開発における問題事例を解消するために、欧州の完成車メーカーは、先ずソフトウェア品質特性(図 1.6.4)のうち、プロセス品質を改善するために、IEC 15504 に基づく Automotive SPICE を構築し、各サプライヤーでの適用を義務付けた。これは、各サプライヤーにおける開発プロセスの統一を図り、開発プロセスに対して任意レベル以上の習熟性の保持を義務付けた。つまり、完成車メーカーは、ブラックボックス化していた開発作業をホワイトボックス化することで、開発作業の進捗度やソフトウェア製品の品質を制御しやすくし、上述した車載ソフトウェア製品の問題事例の解消を目指した。

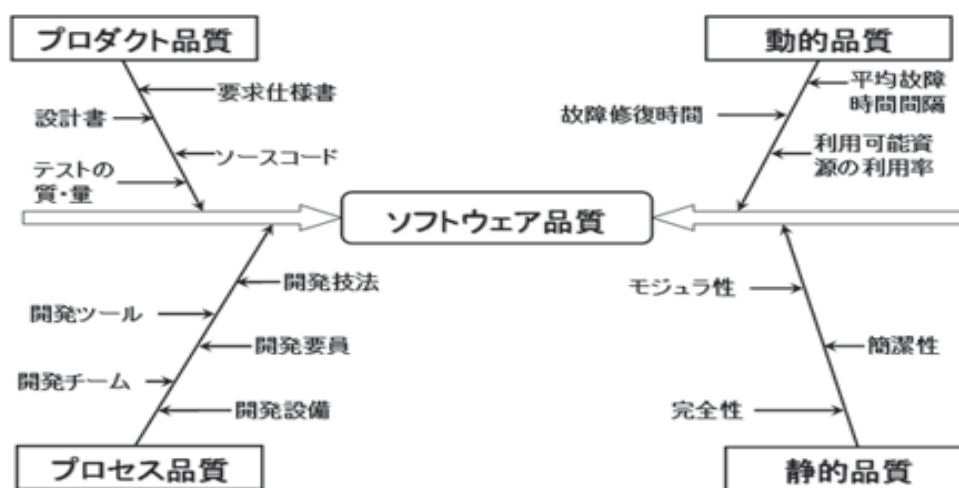
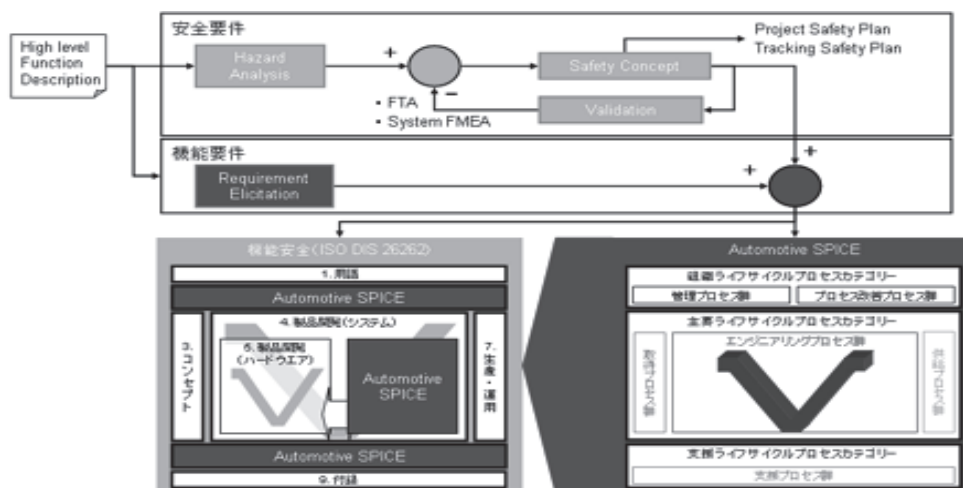


図 1.6.4 ソフトウェアの品質特性.

しかしながら、Automotive SPICE のみでは安全性を担保することが困難であることが判明した。つまり、ソフトウェア開発における要求機能に安全性に関わる項目が欠落している場合、安全性が確保されたソフトウェアが構築されているとは言えない。つまり、ソフトウェア品質の構成要素である安全性と信頼性の関係は図 1.6.5 で表すことができる。また、2008 年開催の SPICE Days において、ドイツ自動車工業会から Automotive SPICE と ISO/CD 26262 との統合アセスメントの構想が発表され、2009 年 7 月にリリースされた ISO/DIS 26262 では「資格を持った SPICE アセッサーは、開発プロセスにおいて、安全監査および開発プロセスのアセスメントを同時に実施できる」という文言が追加され、ISO/DIS 26262 が提唱する管理・支援プロセスおよびソフトウェアに関する開発プロセスと、Automotive SPICE が提唱するプロセスを同等と見なすことができる、という判断に基づいており(図 1.6.6)、今後、各サプライヤーは、Automotive SPICE のみならず、ISO/DIS 26262 を含めた開発プロセスの構築が要求されることになるだろう。



1.6.4 定量的なソフトウェア製品の安全性評価のアプローチ

今日の機能安全規格（IEC 61508、ISO/DIS 26262 など）では、ハードウェア開発において推奨される開発手法や定量的な分析手法が定義されているのに対して、ソフトウェア開発では推奨される開発手法のみが定義され、実際の開発作業に幾つの開発手法を用いたかのみに、安全度レベル（Safety Integrity Level、以降 SIL と略す）が決定されている。これは、様々な危険因子が含まれているため、安全性を評価するための手法としては適切ではない。例えば、採用された開発手法によって開発作業を実施する開発者のスキルにバラツキがあり、この様な状況で開発されたソフトウェア製品の品質にもバラツキが生じるために、規格内で定義されているソフトウェアに対する SIL 定義は改めるべきであると考えている。

そこで、ソフトウェアの安全性の定量的な評価、つまり SIL 算出はどの様にすれば可能なのか、という問題を解決するために、エンタープライズ系システム開発において従来から適用されている、ソフトウェア信頼度成長モデル (Software Reliability Growth Model、以降 SRGM と略す) を用いた信頼性評価手法を用いて、定量的な安全性評価に応用することを提案している。ここで、ソフトウェア信頼度成長モデルに関連する参考文献として文献①～文献③を参照のこと。また、SRGM による分析・定量化手法は、1978 年に AT&T 研究所の Goel 博士と Okumoto 博士の論文 (文献④参照) によって提案された手法である。

次に、SRGM を用いて定量分析が可能な信頼性評価尺度を以下に示し、描画可能なグラフを図 1.6.7 に示し、信頼性評価尺度の関係図を図 1.6.8 に示す：

- **信頼度成長曲線**：テスト進捗と共に発見された累積フォールト数の時間的傾向及び変化を示す。
- **期待残存フォールト数**：分析時点において、ソフトウェア内に残存するフォールト数の時間的傾向及び変化を示す。本尺度は、出荷後、顧客先でソフトウェア故障として指摘され得る可能性がある件数の目安として使用する。
- **瞬間フォールト発見率**：分析時点において、現在のテスト環境下でテストした場合、任意のテスト期間中に発見されるフォールト数の予測値を示す。
- **瞬間テスト空間拡大率**：分析時点において、テストによって、任意のテスト期間中に発見可能となるフォールトの増加数の予測値を示す。
- **ソフトウェア信頼度**：分析時点において、現在のテスト環境下でテストした場合、任意の期間中にフォールトが発生する事無く、期待通りにソフトウェアが動作する確率を示す。
- **瞬間 MTBF**：分析時点において、フォールトが発生する事無く、期待通りにソフトウェアが動作する任意のテスト期間の予測値を表す。特に本尺度は、集計単位当りに発見されたフォールト数を基に計算した平均故障時間間隔の推定値を示し、直近のテスト状況を忠実に反映する尺度である。
- **累積 MTBF**：瞬間 MTBF と同一であるが、特に本尺度は、テスト開始～現在迄に発見された累積フォールト数を基に計算した平均故障時間間隔の推定値を示し、テスト開始～現在迄のテスト状況を忠実に反映する尺度である。
- **擬似テストパス網羅率**：分析時点において、フォールトの検出状況を基に C0 カバレッジを擬似的に予測した値で、現在迄のテストパスのカバー率を表す。
- **新規フォールト生成率**：分析時点において、ソフトウェア内に潜在する総フォールト数の増加率の予測値を表す。これは、テスト開始当初に潜在する総フォールト数に対して、分析時点における総フォールト数が増加しているか否かを表す尺度で、デバッグ時の修正作業の確実度を示す。
- **テスト進捗度管理図**：テスト作業が安定（順調に信頼性が成長）して進捗しているか否かを QC7 つ道具の 1 つである管理図を用いて見える化した尺度である。

- **最適リリース日**：4 種類のコストパラメータを設定することにより、ソフトウェアのライフサイクル中に必要となるコストを見える化した尺度である。本尺度で描画するグラフの最小値を示すポイントが、テスト終了（顧客へのリリース可能日）ポイントであるとして、テスト終了時の判断材料の 1 つとして使用する。

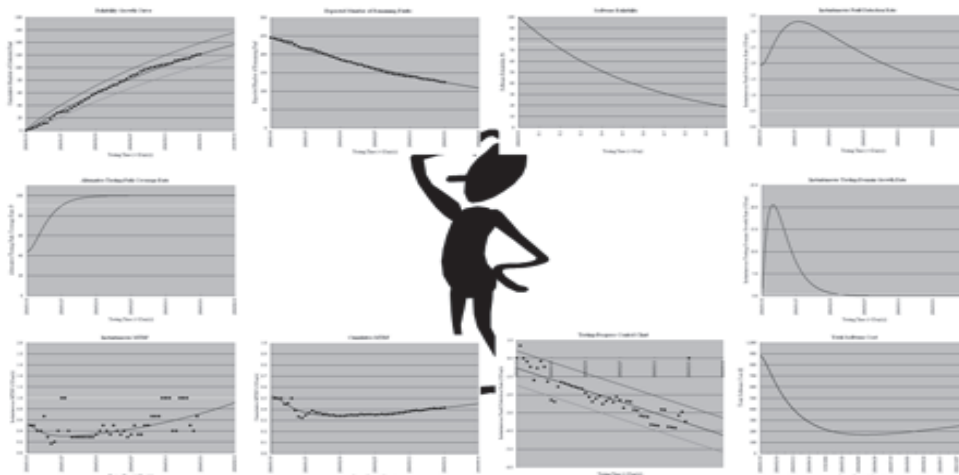


図 1.6.7 信頼性評価尺度の描画例.

これら 11 種類の信頼性評価尺度のうち、フォールト発生頻度、つまり安定稼動状態が表現可能な瞬間 MTBF／累積 MTBF を用いることにより、テスト対象であるソフトウェアに対する SIL を算出することが可能である。本評価手法を適用した SIL 算出は、図 1.6.8 に示す高頻度作動要求もしくは連続モード運用にのみ適用可能である。これらのモードにおける SIL は故障率を表しているため、故障率と平均故障時間間隔（MTBF）との関係は次式で与えられる：

$$\text{故障率} = \frac{1}{\text{MTBF}}. \quad (1)$$

ここで、瞬間 MTBF／累積 MTBF は次式にて与えられる：

$$\text{瞬間MTBF} = \frac{1}{h(t)}, \quad (2)$$

$$\text{累積MTBF} = \frac{t}{H(t)}, \quad (3)$$

$$H(t) = \int_0^t h(x) dx. \quad (4)$$

式(4)の $H(t)$ は非同次ポアソン過程の平均値関数と呼ばれ、時刻 t までに検出される累積

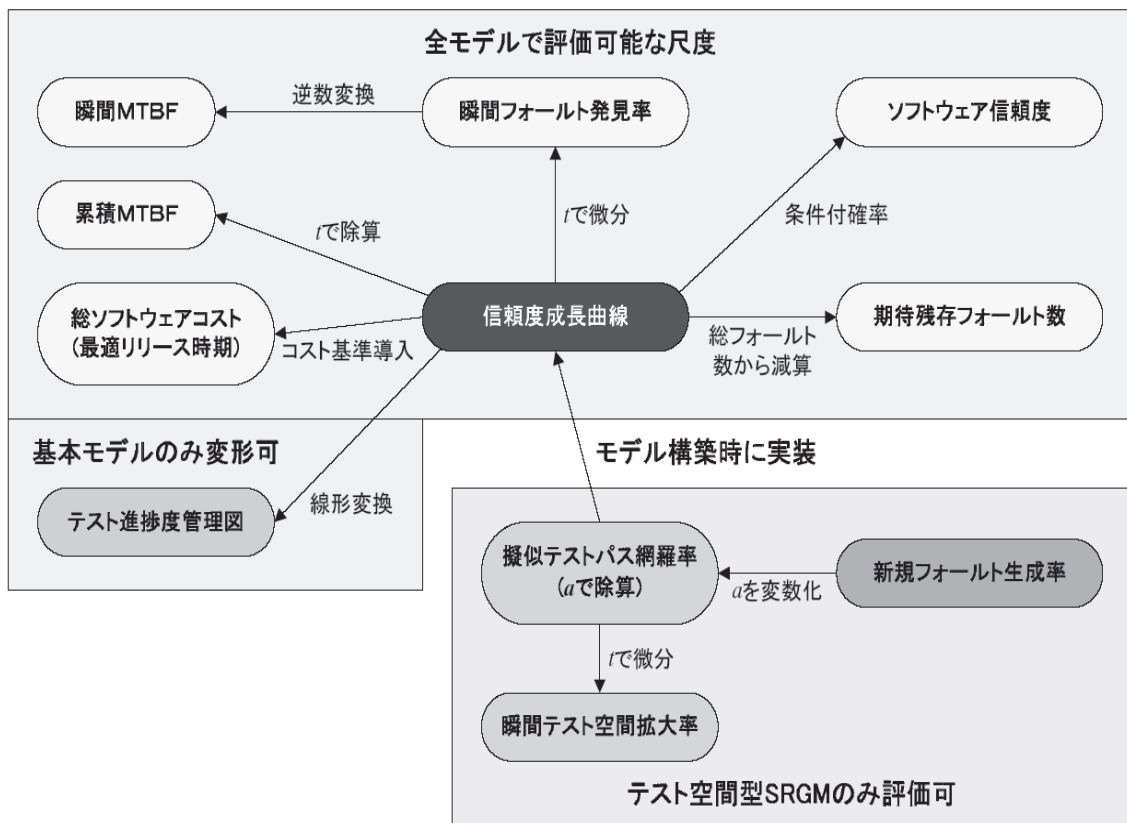


図 1.6.7 ソフトウェアの信頼性評価尺度関係図。

	低頻度作動 要求モード運用 ^{*1}	高頻度作動要求または 連続モード運用 ^{*2}
SIL4	10 ⁻⁵ 以上 10 ⁻⁴ 未満	10 ⁻⁹ 以上 10 ⁻⁸ 未満
SIL3	10 ⁻⁴ 以上 10 ⁻³ 未満	10 ⁻⁸ 以上 10 ⁻⁷ 未満
SIL2	10 ⁻³ 以上 10 ⁻² 未満	10 ⁻⁷ 以上 10 ⁻⁶ 未満
SIL1	10 ⁻² 以上 10 ⁻¹ 未満	10 ⁻⁶ 以上 10 ⁻⁵ 未満

*1: 作動要求当りの機能失敗平均確率

*2: 単位時間当りの機能失敗平均確率 (1/時間) 10⁵時間 = 11.4年

図 1.6.8 IEC 61508 におけるソフトウェア安全度レベル。

フォールト数の期待値を表し、 $h(t)$ は非同次ポアソン過程の強度関数と呼ばれ、単位時間当りに検出されるフォールト数、つまり瞬間フォールト発見率を表す。現在までに、様々なテスト環境や運用環境を反映した平均値関数 $H(t)$ が提案されているが、 $H(t)$ によって表現可能な確率分布が重要であるため、代表的な $H(t)$ とその確率分布を以下に示す：

平均値関数 $H(t)$	確率分布
ゴンペルツ曲線	極致分布
ロジスティック曲線	ロジスティック分布
指数形 SRGM	指数分布
指数形 SRGM(一般系)	ワイブル分布
遅延S字形 SRGM	2 次アーラン分布
遅延 S 字形 SRGM(一般系)	n 次アーラン分布
習熟S字形 SRGM	不完全ロジスティック分布
テスト空間型 SRGM(スキル)	位相分布
対数ロジスティックモデル	対数ロジスティック分布
対数正規モデル	対数正規分布
修正 Duane モデル	パレート分布

さらに、分析に用いるフォールトは、安全側及び危険側の両フォールトを用いて分析するために、危険側フォールトにフォーカスする必要がある。つまり、検出されたフォールト内容を分析することによって、危険側フォールトあるいは安全側フォールトに区分する必要がある。しかし、フォールトによっては区分が困難なケースも発生し得るために、以下に示す 3 区分によって、危険側フォールト率 (dangerous fault ratio、以降 DFR と略す) を算出する：

- フォールト内容が危険側／安全側に明確に区分可能な場合
 $DFR = \text{危険側フォールト数} \div \text{全フォールト数}$
例：検出フォールト数 100 件中、危険側フォールト数 1 件 $\Rightarrow DFR = 0.01$
- フォールト内容が危険側／安全側に明確に区分できない場合
 $DFR = \text{不明フォールト数} \div (\text{全フォールト数} + \text{不明フォールト数})$
例：検出フォールト数 100 件中、不明フォールト数 1 件 $\Rightarrow DFR = 0.0099$
- 上記ケースが混在する場合
 $DFR = (\text{危険側フォールト数} + \text{不明フォールト数}) \div (\text{全フォールト数} + \text{不明フォールト数})$
例：検出フォールト数 100 件中、危険側フォールト数 1 件、不明フォールト数 1 件
 $\Rightarrow DFR = 0.0198$

上記のように計算された DFR を瞬間 MTBF／累積 MTBF の分析結果に乗じることによって、危険側故障率を計算することができ、計算結果に応じた SIL を分析時点での安全性の実力値であると判断することができる。以下に一例を示す：

例：ソフトウェア信頼性評価尺度による分析結果として 18 ヶ月間バグ無く動作可能で

あり、検出フォールトの内容から $DFR=0.0099$ である場合

$$\text{故障率} = 1 \div (1.5 \times 365 \times 24) \times DFR = 7.54 \times 10^{-7}$$

∴ 現在のレベルは SIL2 となる

ゆえに、ソフトウェア製品に対して定義された目標 SIL と、分析時点で得られた SIL に乖離（予実差）がある場合、早期に目標 SIL が達成できるように、ソフトウェアの信頼性評価によって得られた分析結果をテスト作業に反映する必要がある。

SRGM を活用したソフトウェア信頼性評価尺度による定量的な分析手法や分析結果をテスト作業に反映する方法について、詳しくは、ビジネスキューブ・アンド・パートナーズ株式会社に問い合わせた方がよい。

参考文献

1. 山田茂：「ソフトウェア信頼性モデルー基礎と応用ー」、日科技連出版社、1994.
2. H. Pham：「Software Reliability」、Springer-Verlag、Singapore、2000.
3. 山田茂、藤原隆次：「ソフトウェア信頼性：モデル、ツール、マネジメント」、プロジェクトマネジメント学会、2004.
4. A. L. Goel and K. Okumoto：「A time dependent error detection rate model for a large scale software system」、Proc. 3rd USA-Japan Computer Conference、pp. 35-40、1978.

1.7 鉄道の安全

本節は日本大学理工学部 中村教授のご講演をもとに、まとめたものである。

1.7.1 鉄道の安全の概要

鉄道の安全は、機能安全という考えが普及する以前からフェールセーフという概念を核に展開されてきた。そのフェールセーフ技術も多様で、安全性向上を意図しその時代時代の技術を取り入れる努力がなされ、今日のシステムに到達している。そして現在は、コンピュータを用いた保安制御システムが普及しており、そこには機能安全と深い関係がある。

1.7.2 実際の事例 1

そのようにして構築されてきた鉄道の制御システムではあるが、実際には多くの問題を経験しており、その中から教訓をくみ出す努力がなされてきた。機能安全の関係からその事例を見てみる。

(1) 新幹線の ATC

1964 年 4 月オリンピック開催を目前に実用を開始した新幹線は、安全の粋を極めたシステムとして評価され、利用客も順調に伸び、山陽新幹線開業、全国新幹線網構想と順調に推移していた。しかし、安全性の要とされた ATC にその信頼を根底から覆すような事故が発生した。

1974 年に新大阪駅での事例

1973 年 2 月鳥飼基地で発生した ATC 異常現示事故は、列車のオーバーランとして処理されたが 1974 年 9 月品川基地で発生した ATC 異常現示事故は、電磁誘導という雑音によって引き起こされた事が判明し、ATC の意外な弱点が浮き彫りにされ、技術的な対策がなされた。しかし、その 2 ヶ月後に新大阪駅で発生した ATC 異常現示事故は、深刻な問題を投げかけることになった。

新大阪駅での事故の原因は、ATC の電源に挿入された自動電圧調整器 (AVR) で発生した振幅のわずかな揺れ、すなわち乱調に原因があったことが突き止められた。900Hz の搬送波を得るため 60Hz の 15 次高調波を用いていたが、乱調で生成された成分も 15 倍され、900Hz に加算されて、最高速度を許容する 210 信号に化けたのであった。

実は鉄道信号の世界では、産業界で用いられるフィードバック形の AVR が乱調を起こすことは知られており、「ATC にはフィードバック形の AVR は使わない」というノウハウが伝承されていたはずであった。しかし、新大阪では、まさに禁止されていた回路で実現した最新の AVR が使われていたのである。

この事実は、当時の国鉄の技術陣には深刻な問題として捉えられた。列車制御における

フェールセーフは、様々な技術を駆使して実現されているのであるが、その技術や本質を正しく汲み取って設計するという物作りが、今後も維持されるであろうかという懸念を抱いたのである。とくに、技術発展のスピードは益々増大する。この中で、安全性技術が漏れなく組込まれるようなシステム作りを目指した取組みの必要性が痛感された。

1.7.3 安全性確保思想の見直し

(1) 安全性確保思想の見直し

新幹線の事例から得られた教訓は、これまで徒弟制的に安全性技術を伝承してきた物作りの仕組みの限界であった。過去に得られた重要な安全設計の知識や情報が漏れなく活かされるような仕組みの構築が求められた。

委員会を組織して行なわれた活動の中で、まず、伝承すべき安全性技術のサーベイがなされた。そして、当時、安全性を工学的に織込もうとしていた「MIL STD 882」のシステム安全性工学の手法を雛形として、鉄道独自の「信号設備安全性管理の手引き(1979)」がまとめられた。

そこでは、

- ・ 安全性フィロソフィの明確化
- ・ 安全性データ蓄積手法の確立
- ・ 安全性設計手法の体系化
- ・ 安全性解析手法の確立
- ・ 安全性管理手法の確立

などを柱とし、システムのライフサイクルを通じた安全性活動が提唱された。この一連の活動は、「システム安全性工学の現状と鉄道信号への導入：鉄道研究報告(1981)」として報告されている。

(2) 鉄道信号のフェールセーフ技術

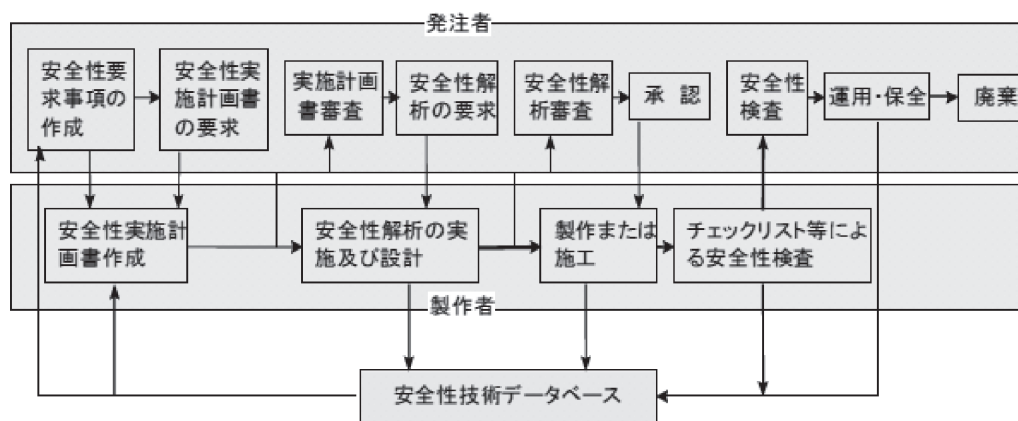
信号設備安全性管理の手引きは、フェールセーフを基本とするという思想が貫徹されている。しかし、安全性技術のデータベース化活動の中でその実態がより明確になった。その概要を説明する。

まず、列車制御はフェールセーフでなければならないとして、「信号設備施設基準規定(国鉄)」の総則には、フェールセーフの原則というものが明示されている。しかし、その実態は様々な技術手法から成り立っていることが明らかとなった。その結果、単に安全性技術を組込むだけではなく、新たな技術開発時にもこれまでの思想が貫徹される必要があり、その方法論として「ライフサイクルに着目した安全性管理」が重要になると認識された。「信号設備安全性管理の手引き」の狙いもまさにそこにあった。

(3) ライフサイクルにおける安全性管理

ライフサイクルにおける安全性管理を図示すると下図のようになる。そして、安全性をライフサイクル全般にわたって管理 するということは、今日の機能安全が拠り所としている思想に通じる。

ライフサイクルにおける安全性管理



「システム安全性工学の現状と鉄道信号への導入：鉄道研究報告(1981)」

ライフサイクルにおける安全管理では、まず、発注側が提示する安全性要求事項に対して、製造側は、安全性実施計画書を作成する。ここには、コアとなる部分に対して過去の安全性技術との対応や、新規に開発する部分での安全性解析や安全性試験の有無等を記載する。発注側はその内容の妥当性を審査し、安全性解析事項の決定と設計を許可する。その結果実施された安全性解析については、要求レベルを満たしているかのチェックを経て、設計製作に移行する。なお、これらの作業を通じて産み出された新たな安全性技術は、データベースに登録される。作成後は、チェックリストなどによる安全性検査及び受け入れ側の安全性検査を経て、運用・保全そして廃棄というフェーズに移行する。

当然のことながら、システムが出来上がってからも、設計、施工、検査の各フェーズにおいて産み出された安全性技術は、データベースという知識のバンクにフィードバックされる。

このように、安全性実施計画書は、安全性技術データベースを参照して作成されるが、システムを作り上げるまでの間だけ参照するのではなく、システムが出来上がってからも、安全性技術データベースを参照して維持、更新される。すなわち、設計、施工、検査の各フェーズからのフィードバックを受け安全性実施計画書も更新される。そして、システムの維持にそれが反映される。

現在の、機能安全には、「過去に産み出された安全性技術やノウハウの有効利用やそれに依拠した安全性水準の折り込み」という発想が欠けている。ひるがえって、日本の鉄道

が 1980 年代初頭に作ったライフサイクルにおける安全性管理は、安全性技術データベースに集積した過去の技術を活かすという大きな長所がある。

1985 年に、国鉄の保安システムにはじめてコンピュータが利用されるが、従来の安全性技術に置換される新たな技術の開発や審査にこの安全性管理の思想が有効に利用され、成果を挙げた。

次に、鉄道におけるこのような活動を一般産業との対比で評価する。

1.7.4 産業界共通の安全技術

(1) 産業界共通の安全技術

安全に関わる産業領域では、いずれもフェールセーフを重要な技術要素として位置付けている。その実態や方法論について共通認識を図り、その原則や共通技術を確立しようとして 1980 年頃に、学会で議論が繰り広げられた。しかし、産業界ごとに安全性技術は多様であり、フェールセーフという考え方すらも共通認識がなしえず、産業界を横断する共通の原則、原理は構築されなかった。

例えば、障害発生時の対応においても、鉄道では、安全側に落とし込む。列車を停止させる方向の動作させることをフェールセーフと呼んでいた。これは「狭義のフェールセーフ」である。それに対して、交通管制では、障害発生時には機能を縮退していく、「フェールソフト」的な技術をフェールセーフと称している。また、航空機では、障害が発生しても飛行を続けることをフェールセーフと呼んでいる。これは通常、多重化により実現されるものであり「多重安全機構」によって実現される。

このように、フェールセーフそのものの定義が業界ごとに多様で、安全を共通に語ることができない状態であった。このような状況を背景に、文献やマスコミにおけるフェールセーフの定義も次の図のように、多様になっている。

フェールセーフの定義

朝日現代用語 ：知恵蔵 1994	構造の部材の一つに疲労亀裂などが生じても、直ちに全体の致命的破壊に進まないようにする設計の考え方。実際には、多くの部材に加重を分担させたり、二重構造を用いる。いずれも適切な点検で欠陥を発見・修理するのが前提
電子通信ハンドブック (電子通信学会)	素子に故障が生じても誤動作したり危険な出力を生じない
電子用語辞典 (日刊工業新聞社)	何か故障が起きたとき、大事故にならないよう電気回路あるいはシーケンス回路またはシステムを配慮してあること
JIS (W 0108-1976)	一部の部材が壊れても構造全体は安全で、その設計荷重の特定の比率の荷重を一定期間は受けもつことができる構造
JIS (Z 8115-1981)	アイテムに故障が生じても安全性が保持されるように配慮してある設計
朝日新聞社説 (1987. 6. 20)	一つの機能に故障や不具合があっても、他の装置が作動し全体の安全が保てる仕組み
読売新聞社説 (1985. 9. 15)	多重安全構造

(2) ソフトウェアの安全性

このような状況は、産業領域でコンピュータ利用が進むにつれて状況が変化した。制御論理がソフトウェアによって実現されるようになるに伴ない、センサとアクチュエータを慎重に使用すれば、多くの安全関連のシステムが同様な手法で実現できるようになった。すなわち、制御論理に計算機ソフトウェアを使用するようになって、各業界で独自に発展した安全技術が、共通のプラットフォーム上に展開されるようになった。このような時代には、ソフトウェアの安全性の保障をいかに実現するかが、鍵として共通に認識されるようになった。ここに、機能安全という新たな共通カテゴリーができあがったともいえる。

ソフトウェアの安全性については、基本的に2つの考えがある。バグ(誤り)が完全にないプログラムの作成が可能とする考えと、プログラムにバグはつきものであるから、プログラム作成時にはバグを極力残存させないように配慮し、運用時にはバグに起因して発生する不具合が危険側に遷移しないようにシステムを構成する、という考えである。この両者は、産業領域に関わらず共通のものである。バグのないプログラムを作成するために、形式手法(VDM、Z)などを用いることがよく行われている。プログラムにバグがあることを前提にしている場合は、ソフトウェア作成時にはV&Vモデルによって管理されたソフトウェア製造プロセスを運用したり、デザイン・ダイバシティ診断機構を組み込んだりすることが行われている。

その結果、産業界共通のフレームというものができ得る状況になった。それは、産業領域にかかわらず、コンピュータで実現するという共通の土壌出現により、安全を共通の言葉で語り合える状況ができたのである。産業界ごとに異なっていた方法論は、単なるソフトウェアのアルゴリズムの差というものだけになった。

そういう状況に伴って、機能安全について規定した国際規格 IEC61508 も、共通規格として受け入れられ、その規格に沿った領域の規格が数多く生み出されることとなった。IEC61508 は安全性を RISK という尺度で評価するものである。

安全性をシステムの挙動や状態などを中心に議論すると、適用領域ごとに多様であり、統一した定義は得られない。RISK という評価値で抽象化することにより、その後の対策は共通に議論が可能になった。それまで、業界により差異がみられた安全性に関する捉え方は、今日では RISK を中心にした考え方に収束した。

結局、過去には産業界ごとに独自の安全要件があり、個別の安全性技術が展開された。しかし、計算機利用技術の進展により、共通の方法論を展開することができるようになり、方法論が規格化できた。個別の方法論は、アルゴリズムの中で行われるようになった。このように、保安制御装置のコンピュータ化は新たな世界を創造したが、鉄道における保安装置のコンピュータ化について紹介する。

(3) 鉄道信号の安全指針

信号システムが電磁機器、電子技術によって実現されていた時代には、鉄道の安全性技術は、非対称誤り論理素子である信号用リレーを用いてフェールセーフな装置を構成するとともに、多様なフェールセーフ技術を駆使して、鉄道独自の安全性技術を産み出していた。

しかし信号システムがコンピュータ式信号システムになると、コンピュータに相応しい安全性手法が模索され、

- ・確率論的安全性確保
- ・安全性確保の核を限定
- ・SLCP の工程内作業の厳格化

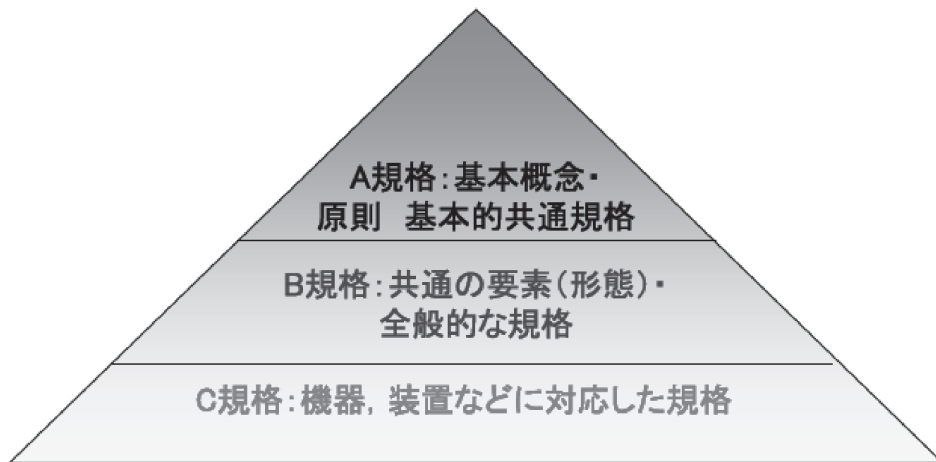
など、産業界共通の安全性技術のフレームの採用へ移っていった。すなわち、コンピュータ制御を意図した鉄道信号の安全確保には、個別各論的な安全性技術を当てはめるだけでは不十分であり、システムティックな方法論が必要との見解に至った。そのため、「信号保安装置へのマイクロエレクトロニクス導入指針」(文献 1.7-3)が 1983 年にまとめられ、電子連動装置開発時の安全性立証のバイブルとされた。

さらに、国際的には機能安全を意図した企画案審議がなされていることに鑑み、鉄道総研は電子連動装置実用化の経験を踏まえた新たな共通ガイドラインを制定するとして、委員会を組織し、1995 年の委員会の報告として、「列車制御システムの安全性技術指針」(文献 1.7-3)が上梓された。これは、電子連動装置のみならず各種コンピュータ化信号装置開発を経て、技術を集約した指針である。IEC61508 の流れを先取りし、ライフサイクルが取り入れられていた。その後の信号保安装置開発時のマニュアルとして位置づけであった。また、鉄道信号分野に RISK という概念を明示したのもこの技術指針である。鉄道の保安制御システムに関わる規格類の整理は次のようになされた。

(4) 安全性規格

国際規格は、下図に示すように階層構造を取っており、機能安全の規格はB規格に位置する。さらに、鉄道部門を対象としたC規格は、このB規格を下に制定されている。

規格化時代の安全性確保大系 システムや機器・装置に関する安全関連規格の構成



IEC61508 の規格に流れる安全性に対する基本的思想は、ISO12100 に見ることができる。すなわち、下記のようなステップを遵守することにより、目標とする安全性が達成されるというものである。

ステップ1 設計段階に前提条件を定め、その下で考えられる RISK を評価

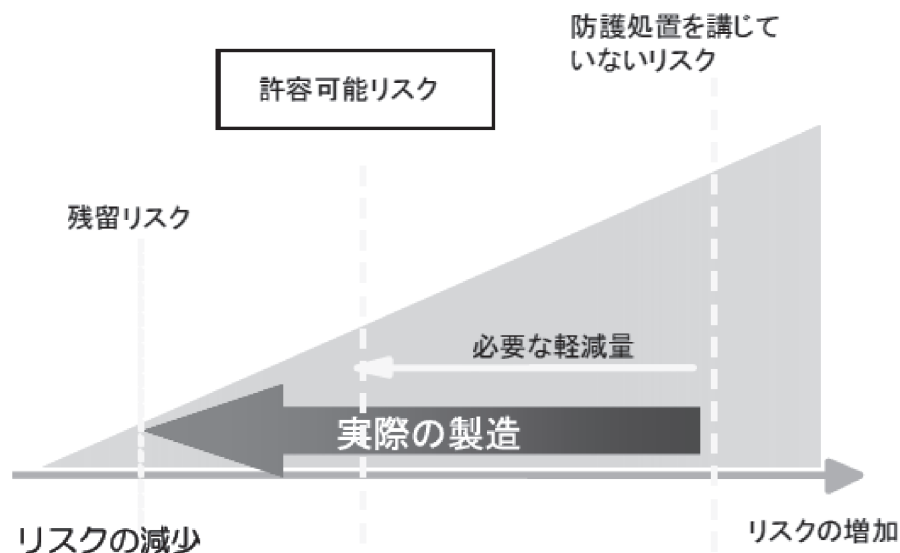
ステップ2 受入れ RISK 水準との乖離の度合いからカテゴリ水準の策定

ステップ3 カテゴリ水準に対応した設計・製造・検査・運用・・・

ステップ4 その妥当性を第三者が審査

また、RISK 軽減の概念は、下図のようなものである。なお、ガイド 51 は A 規格に位置する。

RISK軽減の概念(ガイド51)



C規格に位置する鉄道用の規格の1つにIEC62278がある。この規格はRAMS (Reliability, Availability, Maintainability and Safety)の規格である。

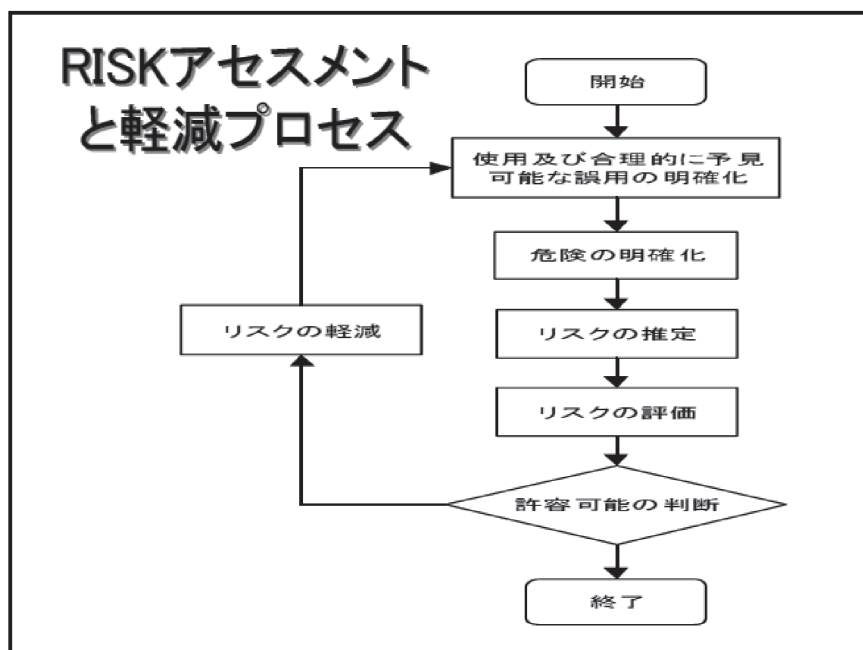
RISKの値は、下表に示すようにIEC62278にて例示されている。ここで、THRとはTolerable Hazard Rateで許容できるハザードの率である。なお、 $10^{-9} \leq \text{THR} < 10^{-8}$ のSIL 4というのは、大体一万年に一回の確率で発生するというものである。

RISKの値(IEC62278)

THR(h ⁻¹ /機能)	SIL
$10^{-9} \leq \text{THR} < 10^{-8}$	4
$10^{-8} \leq \text{THR} < 10^{-7}$	3
$10^{-7} \leq \text{THR} < 10^{-6}$	2
$10^{-6} \leq \text{THR} < 10^{-5}$	1

THR: Tolerable Hazard Rate

RISK アセスメントと軽減プロセスは下図のようなフローで表現され、許容可能水準以下になるまで、リスク低減を繰り返す。



(5) 機能安全規格 IEC61508

次に、機能安全に規格に対し、鉄道の列車制御部門での実践事例と見解をまとめる。

機能安全規格 IEC61508 の背景には、ソフトウェアの問題がある。それは、次のように整理される。

1. 計算機に頼る時代になり、コンピュータが次第に安全機能を遂行するようになった
2. 安全の考え方に関する手引書が必須になった
3. 電気・電子・プログラマブル電子系は全安全ライフサイクルにわたって何をなすべきか包括的な扱い方を規定すべきと考えられた
4. 全ての電氣的な安全関連系に対し、合理的、かつ、整合性がある技術指針が展開可能な規格が必要とされた

これらを受けて、機能安全規格 IEC61508 規格が制定されたが、その体系はご存知のように次のようになっている。

第1部: 一般要求事項

第2部: 電気・電子・プログラマブル電子安全関連系に対する要求事項

第3部: ソフトウェア要求事項

第4部: 用語の定義及び略語

第5部: 安全度水準決定方法の事例

第6部: 第2部及び第3部の適用指針

第7部: 技術及び手法の概観

1996 年に新しい技術指針の検討を開始した当時、鉄道信号の技術者や事業者から、IEC61508 等のコンセプトに対するネガティブな意見が多かった。その代表的な見解は以下のようなものであった。

- ・従来の作業に加えて、新たに、審査、文書整備と認証というものは、新たな負荷を強いることになる
- ・一般化は独自技術の構築や、差別化を阻害する
- ・コスト増につながる

一方で、時代の趨勢を先読みし、新規に開発を行なうシステムに、規格のプロセスを実際に適用し評価してみようではないか、という建設的な意見もあった。その代表が、理想的な電子連動装置を目指した PRIME の開発であった。規格案(当時)の定めるプロセスを設計、製造、そして検査のフェーズに適用したところ、バグ件数の削減や収束の速さに結びついたという思いがけない効果が確認された。結局、厳格なプロセスの実行であったが、総合的には、生産性の向上が見られた。

上記の電子連動装置 PRIME は、1985 年の電子連動装置実用化後の課題を集約し、10 年後時点での理想的な電子連動装置の開発を行おうというもので、鉄道信号メーカ 3 社による共同プロジェクトであった。機能安全を先駆的にソフトウェア開発に適用した事例ともいえよう。

PRIME の品質は下図に示す通り、障害発生率、運転阻害率の両方において優れていた。

SMILE は鉄道総研が核となり鉄道信号メーカ 3 社が参加して開発したものであった。一方、PRIME は企業が独自にプロジェクトを作り開発したもので、鉄道総研は第 3 者機関として設計審査や検査部署として関わった。PRIME での生産性向上は、ソフトウェア開発の手戻りがまったく無かったことによってもたらされたといえる。

機能安全規格に準じたソフトの品質評価

System	総運用時間 (H)	障害発生率 (1/H)	運転阻害率 (1/H)
SMILE (FSM)	9.81×10^6	2.04×10^{-6}	0.92×10^{-6}
PRIME (ILP)	2.63×10^4	0	0

宗方;安全関連の国際規格に準拠して開発した電子連動装置とソフトウェアの実践評価」信頼性、Vol.23、No.7、2001.11

1.7.5 機能安全規格適用における課題

(1) 整備される鉄道用規格

鉄道用規格(C規格)として、IEC61508に準拠したドメイン規格の整備が行われた。その代表的なものとしては、

- ・ EN50126: Railway Applications: The specification and demonstration of dependability, reliability, availability maintainability and safety (RAMS) = IEC62278

- ・ EN50128: Railway Applications: Software for railway control and protection systems = IEC62279

- ・ EN50129: Railway Applications: Safety related electronic systems for signaling. (safety case)

などがある。

RAMSの規格ともいわれるIEC62278は、IEC61508の思想にのっとり鉄道用に制定された規格である。これら規格を下に実践の経験が蓄積されて行くにつれ、担当者の間では、いわゆるRISK至上主義に対する疑問の声も聞かれるようになった。

そもそも

- － 鉄道信号はフェールセーフが第一である
- － 致命的事象にフェールセーフを基本とした対策を漏れなく実施する

この、設計思想は今日においても堅持されている。ただ、その結果として残留する危険側故障率評価をすることはあるが、はじめに故障率を算出しRISK等級を定めることにはなじまないとする見解である。さらに、頻度計算を行うためには、データが必要となるが、そのデータすらも自信を持って使えるものを持ち合わせてはいない。そもそも、RISKを算出するのは、安全性水準SIL(Safety Integrity Level)を得るためである。とするなら、RISK等級は直感で十分であり、RISKの厳密な算出はさして意味を持たないという見解には一定の説得力がある。

規格が期待するRIISKの役割は、適切なSILの算出である。しかし、SILは実質、高々4レベルの分類でしかない。下図の最右欄のとおり、意味的には4レベルに集約される。全く新規な複雑系の開発の場合には、RISK評価を行ないSILを定めるというプロセスは意味がある。しかし、鉄道のシステムのように、枠割りが明確に理解でき、安全性上の水準もブレなく定まるような場合には別のアプローチがあって良い。

規格が期待するRISKの役割

- 適切なSILの算出
- SILは高々4レベル

極めて重要	6	5	4
高い水準が要求される	5	4	3
配慮が必要	4	3	} 2
望ましい	3	2	
あまり関係ない	2	1	} 1
配慮する必要ない	1		

鉄道のATCは、SIL4レベルが要求されている。そして、致命的な事象には対策を実施し高い安全性を確保してきた。同様な機能をするシステムの開発において、故障率を厳密に計算せねばSILが求められないとする根拠は薄い。たとえ、故障率を厳密に計算することによって、仮にSIL等級が多少下がったとしても、結局、誰もそれを価値とみなさず、本来の安全性確保に邁進されるに相違ない。

(2) 安全性手法からみたRISK解析の有効性

本来、安全性手法を考えるのに、確率論的な考え方と、決定論的な考え方があり、システムに対して適切な安全性手法を採用しなければならない。決定論的安全性手法は、システム挙動が明確で豊富な経験があるものに対して用いるべきもので、現実には鉄道や産業機械などでは採用されている。確率論的安全性手法は、原子炉や宇宙開発のように、複雑かつ一品料理的に製造されるもので、システムのすべての振る舞いを把握することが困難な場合に採用されるものである。

確率論的安全性手法では、あらゆる事象をRISKで評価し、RISKが妥当な水準まで低減するようにする。確率論的手法は、網羅性と徹底性に優れる。重要なことは、RISK評価をレベル付けに矮小化してレベルを満たしたことに満足するのではなく、RISKを妥当な水準まで下げるプロセスに意味がある。

(3) 組込みシステムの開発に必要な活動

安全性手法の導入は、組込みシステムの開発に必要な活動である。安全性手法の選択は、SILに集約することができる。そして、SILであれば先に述べたようにRISKのすべてを計算しなくとも困らない。SILは直感的に判断してもさほどブレはないという、素晴らしい利点がある。

RISK を算出して SIL を決めることにきゅうきゅうしても余り意味がない。例えば、最近では、FPGA を使用しているシステムが増加しているが、部品としての FPGA の故障率がそもそも不明である。その FPGA を使用したシステムの故障率を算出しても誰がそれを保障し得ようか。数値そのものにはあまり意味がない。

逆に、システムの機能や使命に着目し、SIL を定めて、システム全体で直感的に安全性を考えたほうが合理的である。もちろん、構成要素への SIL の割り当ても行わねばならない。そして SIL に従った Safety Life-Cycle Process の厳密な適用と、その妥当性の第三者認証も非常に重要な意味を持っている。

そのための、認証組織と体制の整備が急務であるが、この点での我が国の遅れを認識しなければならない。組込みシステムの中にも、国際規格時代の今日では機能安全への認証が求められるものがある。ここでの認証者の役割は、SLCP のプロセスが厳格に実施されていることはもとより、組込まれた安全性技術の妥当性、充足性の吟味も重要である。

例えば、日本が受注した台湾高速鉄道では、日本で使われていて実績ある信号システムを用いると言っても、それが国際規格に則ったものであるのか、どんな基準をクリアしているのかと言うことが問われた。我が国には認証機関がないため、厄介な注文ではあったが、具体的な装置の設計やソフトウェア開発に対しては、鉄道総研などの実力を備えた機関が独自に審査を行い、設計上は安全性に問題ないことを評価し、認定をクリアするという手順が踏まれた。

(4) 組込みシステムの安全性技術

組込みシステムの安全性技術は、多様な技術の総体として安全性が確保されることが普通で、個々の安全性技術が重層的に作用していることが多い。したがって、安全性技術の効果は、多様な側面で働く。

この重層的であり、多様な側面をもつ組込みシステムの安全技術をどのように評価するかは、設計者、評価者の双方にとって重要な課題である。受注者や製造者は、コストパフォーマンスに基づいた最適設計を行わねばならない。コストパフォーマンスを追求した受注者の作成したものが、機能安全の要件を満たしているか否かを評価することは重要である。

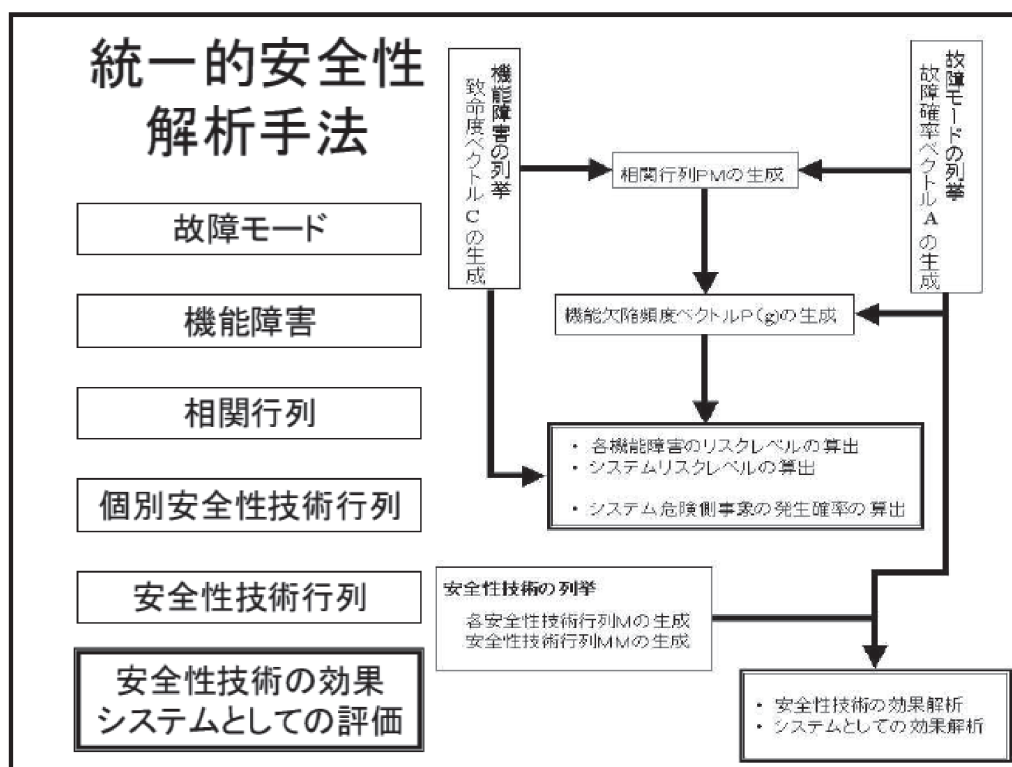
よって、個々の安全性技術に対する合理的な評価が重要になる。

安全性の評価方法として一般的な手法のほかに、講演者と鉄道総研が開発した統一的な安全性解析手法がある。一般的な安全性評価手法には、マルコフモデルや FMEA、FTA という方法がある。マルコフモデルによる評価では、システム状態モデルを使用するが、それはマクロ的評価手法となる。マクロ的評価手法では、内部に組込まれた多くの安全技術の一つ一つの評価や吟味が容易ではない。FMEA、FTA でも、多くの安全技術が重層的に作用するような場合に、その効果を個別的に評価することは難しい。

また、評価には安全性技術を組込まなかった場合の危険性や信頼性、さらに安全性技術

を組込んだときの個々の技術の評価と、その結果としてシステムが有する安全性の評価が求められる。このように、実際には多くの視点からの評価が求められ、これまではそれぞれ相応しい手法や考え方に依拠して個別に評価を行ってきた。

このような状況の打破を意図して、開発した手法が「統一的安全性解析手法」である。統一的安全性手法は下図の通り、各要素を総合的にとらえ、また、統一的な評価を行う。これによって、重層的で多様な安全性技術の総合的な効果を測ることができ、システムとしての評価を行える。



統一的信頼性・安全性解析手法では、まず、信頼性は、故障の発生確率によって定まるとする。このため各要素の故障モードに応じた故障確率を要素とする故障確率ベクトルを導入する。故障確率ベクトルは、システムを構成する要素が採り得る故障モードに対応する発生確率を列ベクトルとして表現する(それを故障確率ベクトル A とする)。

各故障とシステムに期待される機能との関係(有=1/無=0 とする)を相関行列で表現する(それを相関行列 PM とする)。

すると、次のような機能欠陥頻度ベクトル G が算出できる。

$$\text{機能欠陥頻度ベクトル } G = PM \times A$$

安全性はすなわち、機能障害の中で危険側のものの総和を 1 から減じればよい。従って、機能欠陥頻度ベクトル G を吟味することで、安全性を論じることができる。

一方、安全性技術の作用は、個々の故障モードがシステムの障害に結びつかないように抑止するところにある。安全性技術によって要素の故障モードがどのくらい抑止されるか

を(1~0)の数字を割り当てることで、1つのベクトルができる。このベクトルを対角行列に展開し故障確率ベクトルAに乘じたものに、PM行列を掛けることにより安全性技術の効果が算出できる。また、複数の安全性技術の場合には、それぞれのベクトルから安全性技術行列を作り、その対応する列要素の積からベクトルを作ることによって相互の効果を加味した評価ができる。

この手法はリスクの計算や信頼性、安全性、安全性技術の効果等がシステマティックに算出できるが、残念ながら、手法の提案とケーススタディのみに終わっている。

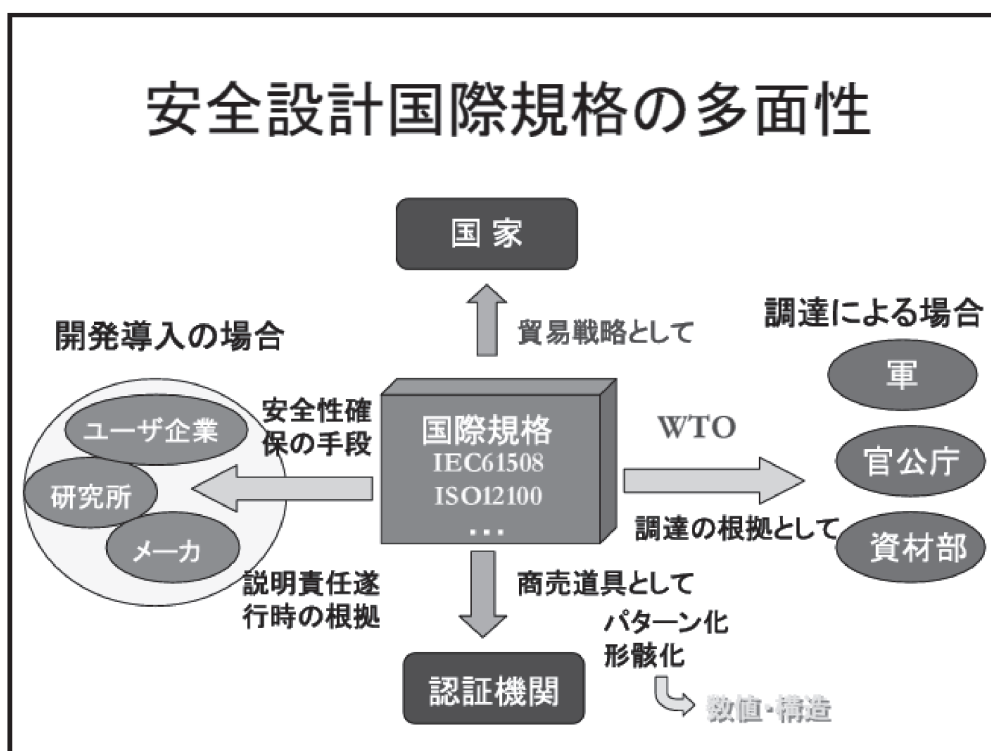
(5) 規格の流れに見る方向性

コンピュータ利用システムの安全性確保と評価は、既に方向性が定まったといえる。

これからは、安全度水準SILの策定とSILに対応したSLCPの実施と、第三者による認証の仕組みを整えるべきであることを繰り返し述べてきた。

今後の多くの組込みシステムには、国際規格の思想に則った対応が否応なしに要求される。安全性技術の考え方に対する正当な理解とその上での実践、そして、認証体制の整備が急務である。

ところで、単に規格を遵守するばかりでなく、規格の持つ意味にも着目する必要がある。というのは安全設計の国際規格は、下図のように多面性があるからである。



安全性技術のプロセスに則って開発を行うのは、大変であるが、国際規格のプロセスに則っていれば、国際的に調達されることが可能になる。調達側も規格に則って作られたこ

とが確認されれば、安心して調達の対象にできる。

一方、認証機関が認証作業の容易化のために、認証基準をパターン化しようとする動きが見られる。本来、説明責任を果たせれば技術的内容に自由度が認められていたものが、ある範疇以外は認められないということになると、本来の目的が形骸化する恐れがある。とくに、有力な認証機関を多く抱える国がそのような方向での議論を積極的に推進していることも気付きではある。

また、国際規格が貿易戦略の中に位置づけられて使われかねないという側面にも目を向ける必要がある。とくに、国際化の流れの中に進んでいこうとすると、規格がある意味では、我が国の進出に対する障壁ともなるし、ある意味では相手側が我が国に進出してくる際の武器として使われることもある。台湾高速鉄道での教訓を忘れてはならない。

1.7.6 機能安全の形骸化

機能安全の概念は、ソフトウェアという厄介なものを使いこなし、安全性が要求される分野にまで拡大しようとしたときには有効な方法論を提示している。しかし、それは SLCP の各プロセスが厳格かつ正当に実施されている話であり、そのうちの 1 つにでもほころびがあると、きわめて危険な事態を引き起こす。モノレールの事故で露呈した問題点を紹介する。

(1) 事例：湘南モノレール

平成 20 年 2 月 24 日の日曜日、湘南モノレールでとんでもない事故が発生した。湘南江ノ島駅方に向かっていていた列車が、異常な加速が見られた後、運転士の操縦に反して減速ができなくなり、運転士が非常ブレーキを扱っても駅に停車できず、出発側の分岐器に衝突して停止したという事故である。

その事故の原因は、車両の電源回りで発生した雑音によって VVVF インバータ (PWM 制御) が制御不能になったという故障であった。もちろん、車両の良好とはいえない電磁環境を想定した電源引き回しが行なわれてしかるべきであるが、全く配慮がなされていなかったために、雑音が不正な通信電文として処理され、異常処理の不具合と相まって、乗務員のマスコン操作を受け付けなくなってしまったのである。この種の不具合は、単一事象では起こらない事が多い。今回は、誤った電源引き回し、信号線のノイズ対策不良、そして不正割込みに対するソフトウェアの誤った処理が主要因である。

VVVF インバータは、モータの電源を制御する装置であり、加減速などを司る機能はマイコン制御である。VVVF インバータには、動作状況を運転席に通知するモニタ接続用の信号線が実装できるようになっていた。しかし、当該の湘南モノレールでは、モニタを設けていなかったために接続口の端子は開放になっていたが、プルアップもプルダウンもさ

れていなかったために、極めてノイズを受けやすい状況になっていた。

ノイズなどによって、不適切な信号がマイコンに入力されると、その信号は、VVVF 内のマイコンでは、不正割り込みとして処理された。その不正割り込み処理ルーチンによってタイマ割り込みを含めた全ての割り込みが禁止され、運転士の操作入力すらも読めなくなったというものであった。

ブレーキと関わりのある VVVF は ATC などの保安装置にとっても最後の砦である。ATC 等の保安装置は、機能安全の思想により入念にチェックされたはずである。しかし、部品として実装した VVVF にこのような落とし穴があるとは設計段階で気がつかなかったのであろう。VVVF の処理そのものはソフトウェアとはいえきわめて単純な構造である。しかし、なぜ、不正割り込み時に他の割り込みまでマスクしたのか、そしてそのようなソフトウェアの不具合に対してウォッチドッグタイマ WDT も無力であった。設計時の盲点ともいえよう。

この事例に待つまでもなく、実はコンピュータ制御において、割り込みをどのように扱うかはきわめて重要な意味を持つ。

(2) 鉄道信号におけるソフトウェアの安全技法

鉄道信号におけるソフトウェアの安全技法は、シングル・スレッド方式としてタスクを起動し、マルチタスクは使わないことにしている。それにより、クリティカルなタイミングでのタスクのプリエンプション(切替え)がもつ RISK を回避する。また、スレッド実行時は割り込み処理を行なわせない。スレッドの最後のタスクが終わって、先頭タスクに戻る際に、割り込みに対応した処理を行なわせる（下図）。このシングル・スレッドの処理は周期的に行う。これは、各処理に確実に CPU 資源を与えることができるし、複雑さを回避している分、検査も容易になる。

シングル・スレッド方式としてマルチタスクは使わない



さらに、タスク間の通信はデータの非対称な受け入れ検査を行う。入力の変化にも非対称診断を行なう。また、入力変化の合理性診断を行い、ありえない入力の変化は、異常として扱うようにする。

今日現在は、シングル・スレッドで処理を行うのが基本であるが、CPU の高性能化が進んだ現在、高機能化への要求は高い。しかし、安定稼働しているシステムに、新たなソフトウェアを組込むと言うことは、せっかく確保してきた品質を再度ゼロから検証を行なわせることと等価である。このような事情を背景に、独立したスレッドとして、独立性を維持しつつ機能拡張を図る方法も検討されつつある。

(3) 機能安全から見た湘南モノレールの問題点

機能安全から湘南モノレールの問題を見ると、

- ・ VVVF のプログラム作成時に SIL はどのように考えられたか？
- ・ ATC の SIL に応じた物作りが厳格になされていたのであろうか？
- ・ モニタのコネクタが接続されないときの挙動まで予測できたか？
- ・ ATC 設計者は VVVF を PES の一つと認識していたか？プログラマブル部品と意識したか？
- ・ VVVF を使う ATC では部品調達時に何を要求したか？

という疑問が出る。これらが欠けていると、機能安全が満たされないシステムになってしまう。機能安全を考える際には反芻すべき教訓と考えている。

(4) IEC61508 規格における今日の問題

このほか、IEC61508 規格における今日の問題として次のようなものが考えられる。

- ・ 認証機関の要求が力を得てきつつある
- ・ 数量評価が重視される傾向にある
- ・ アーキテクチャの画一的解釈がなされるようになってきた
- ・ 要件の単なる網羅で本質的な内容が軽視されがちである
- ・ 安全性立証という本来の思想が形骸化する懸念がある

上記は、主に規格の主旨が次第に形骸化されつつあることを物語っている。

また、安全性技術を独自に長く磨いてきた組織の立場からすると、

- ・ 過去の経験や技術に触れない弱点がある
- ・ 技術の総合的・有機的な関係に無配慮

ということも、大きな問題である。安全性技術は奥が深い。これらに対し実績を積んだ部署と、全く経験がない部署が、機能安全の規格の前では全く同じ物作りをして市場に出される。経験を一切考慮しないという規格が、何をもたらすか、過去の安全性技術やノウハウに依拠することを要しない方向性には問題があろう。

機能安全は、「安全性立証」ができなければ、「安全性立証」が万人を納得させられねば、世の中に出すべきではないという基本があった。本来の思想が再確認されねばならない。

参考文献

文献 1.7-1 「信号における安全性技術調査書(1978)」

文献 1.7-2 「信号設備安全管理の手引き(1979)」

文献 1.7-3 「信号保安装置へのマイクロエレクトロニクス導入指針」、鉄研速報、No. A-83-147、1983

文献 1.7-4 「列車制御システムの安全性技術指針」、鉄道総研報告、1996.3

文献 1.7-5 安全関連の国際規格に準拠して開発した電子連動装置とソフトウェアの実践評価」、宗方、信頼性、Vol.23. No.7、2001.11

1.8 安全規格認証製品

本節は IDEC 株式会社 伊佐泰夫氏が 2009 年 11 月 27 日開催された JASA/ET セミナーにおいて行った、セーフティコントローラにおける機能安全について；制御機器の機能安全と事例、と題する講演をベースにまとめたものである。

同氏の連絡先は以下の通り。

IDEC 株式会社マーケティング戦略本部 伊佐泰夫様

〒532-8550 大阪市淀川区西宮原 1-7-31

電話：06-6398-2504

FAX：06-6398-2547

E-mail：yisa@idec.co.jp

1.8.1 開発初期における確認の重要性

今回セーフティコントローラを開発し販売したわけだが、もしそれ以前の開発の経験が無く開発していたら、大変なことになっていた。

一番苦労した点は、セーフティコントローラに繋がる安全入力機器や安全出力機器の特性をよく理解して開発しなければ、あとでとんでもないことになるということである。

我々の場合、開発はハード、ソフトおよび全体の 3 つのユニットに分かれて行った。役割分担でやってみて、最初は全くわからなかったのだけれど途中からからわかってきたことは、全体を考える設計者がソフト設計者に正しい情報を与えていなかったということであった。作動する機器を開発すること自体はソフトとハードを結びつければいいわけだが、それで正しいのかという評価をすることが非常に難しい。特に最近の機器の部品というのは電子化されているので初めから安全についてわかった上で開発をしないと、後々、様々な問題が出てくることに注意しなければならない。

特に開発の当初は、開発の範囲は相当幅広く考えることができるので、メンバーがお互いに自分の考えで進めていくという傾向があり、この時点でも他のメンバーと意見調整をよくしておかないと、あとで調整に苦しむことになる。

トータルシステムを考える開発者と、ハード・ソフトを考える開発者がお互いに中身をはっきり把握しておかないと問題が起きるということである。

仕様がグレーのエリアについてはお互いに必ず確認することが重要である。

1.8.2 IDEC 社の製品紹介

まず IDEC における安全機器にはどういうものがあるか概念の説明があり、その後具体的な製品紹介が行われた。

製造ラインに人間が全く入る必要がなければ安全機器というのは必要ないが、メンテナ

ンスその他で中に入る必要がどうしても生まれる。またコンベアで運ぶ部分については囲いきれない場合もある。基本的に囲いの中にある機械（ロボット）を囲いの中に入ってティーチングペンダント操作するなどのメンテナンス作業者を、各種の安全スイッチでまもるという形態になる。

以上が一般的な製造ラインにおける概念であるが、注意しなければならないのは、半導体製造装置の安全というのは他の製造装置とは大きく異なる部分がある。それは急に止めると熱暴走などの危険があるということである。この点に留意して安全回路を構築する必要がある。

また、食品包装機械の場合は、衛生面から洗浄することが頻繁にあるため洗浄に適したような安全スイッチを考えないといけない。IDEC は様々な用途に適した、IEC/ISO 規格に適合している多くの種類のセーフティコンポーネントを製造販売している。また、安全関連部に使われる安全リレーモジュール・セーフティコントローラや各種安全関連商品も製造販売している。

1.8.3 様々な安全スイッチが生まれた経緯

昔、リミットスイッチが、安全上の問題を頻発したことから、ヨーロッパから強制乖離機能を持ったセーフティリミットスイッチが開発され販売されるようになった。それにあわせて非常停止用押しボタンスイッチなども強制乖離機能付に変わっていった。

非常停止用機器のポイントは、停止した際に不具合が起きないように直接開路動作機能付き（以前は、強制乖離機能という名称）であること。操作部は、押された位置で接点が開いた状態でラッチングしなければならない。他に操作部は、手のひらで押す形のきのこ形で即座に操作でき、スイッチ本体は赤、背景は黄色に彩色されなければならないという規格上の制約がある。

直接開路動作機能の要点は、接点溶着が発生してもアクチュエータ（操作部）の押し込む直接の力によって、溶着した接点を引きはがす機構のことである。そもそもは EN 規格から出てきたもので、強制乖離機構と翻訳されていた。

強制乖離機構というのは EN の Positive Opening Action の訳語であるがその後アメリカからクレームがあり、Positive は絶対という概念を包含することから、Direct という表現に変えられ、その訳として直接開路動作機構という用語が出来、新 JIS 上で使用されている。

現在新 JIS に採用されている用語は IEC/ISO の直訳が多く、一見しただけでは意味のわからぬことがあり、その場合は、原文である英文を見ることにした方がよい。

直接開路動作の規定により作られるスイッチは、非弾性体（例えばスプリングに頼らない）を経由して開閉操作部に結合された接点を有する機器で、操作力が直接接点に伝達され、接点が完全に開路する構造のものであり、規格上、開路力が規定されている。

規格上はこういうものを使って安全を確保するという形になっている。その後、機能

安全という考え方が確立されていく中で、電子化されたコントローラを使って、安全が確保されていくようになった。

1.8.4 安全スイッチ・コントローラの基本

機械は故障し、作業者はミスを犯すことをまず認めた上で、仮にこれらが起きても作業者に危害をおよぼさないという安全対策の考えにのっとったものである。例えば、危険区域を監視し、作業者が危険区域に近づいた危険情報を、機械に与えて停止させる「危険検出型」のシステムと、作業者が危険区域に存在しない安全情報を機械に与えて運転を許可する「安全確認型」のシステムを比較した場合、前者は危険情報の伝達が故障したときに機械に「安全」という判断をさせてしまうことに対し、後者は安全情報の伝達が故障したときにも機械に「危険」という判断をさせることができる。つまり、後者は Failure to Safety のシステムである。

安全確認型システムの定型的な例は、非常停止スイッチによる緊急時の機械の停止や、ドアインタロック装置、許可を与えるスイッチなどで構成され、その概念を図 1.8.1 に示す。

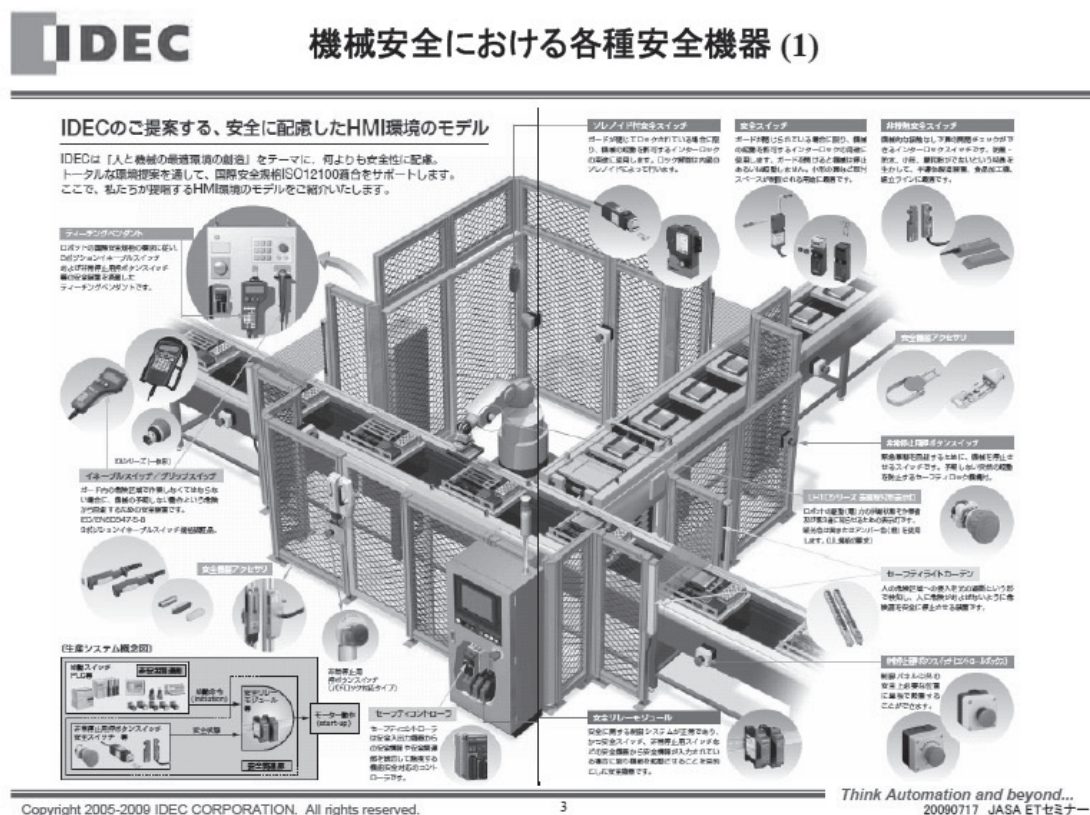


図 1.8.1 (出典 IDEC 社資料)

ドアインタロック装置とは、一般的にガードなどに取り付けるインタロック装置のことである。「インタロック」とは、安全情報（安全装置により安全が確認されているときに限り生成される情報）にもとづき、機械の可動部の動作を許可したり、禁止したりする仕組みをいう。許可を与えるスイッチとは、例えば、突然の危険に遭遇した作業者が咄嗟的にスイッチから手を離す場合もあれば、逆に身体の硬直などによりスイッチを握りこんでしまう場合もあり、ON からさらに押し込むと OFF する 3 ポジション（OFF-ON-OFF）動作を行うものである。

現在はNC接点ノーマリー・クローズ型が使われる。ここが一般的な制御機器と逆の考え方になっていることに注意してほしい。

このような形になっている理由は、非常停止の安全ロック機構について、「操作部が押された場合は、全て非常停止命令が発せられたものとして、回路が遮断され、その状態で保持させなければならない」という EN（European Norm）規格がある為である。非常停止用ボタンは、異常発生時に確実かつ瞬時に作動させられる形状が重要視される。その一方で誤動作時には、作動しない安全性も必要である。これを満たすものとして、人や物がボタンにあたった場合でも、操作部が完全にロックされるまで接点が開離しない機構を採用している。機械安全の考え方では配線が切断されたということまで考えないといけない。

1.8.5 強制ガイド式リレー

EN 規格により、危険度の高いシステムや機械には、少なくとも 1a+1b の接点構成を持った安全リレーを搭載しなければならない。又、その a 接点、b 接点は決して同時に閉じることはない。仮に接点が溶着した場合でも、接点間隔を少なくとも 0.5mm 以上確保しなければならない。これは EN 規格で規定されている。兎に角、同時に接点がオフあるいはオンにならない構造にしなければならない。

1.8.6 安全リレーモジュール

非常停止用スイッチや安全スイッチなどは、安全な状態が確認されている情報を作り出す部分として位置づけられているが、安全リレーモジュールは、それらの安全情報の入力によってフェールセーフに機械の起動を許可し、安全情報が無くなった場合に、フェールセーフに機械の運転をやめさせるという役割を持ったモジュールである。安全確認の情報を作り出す部分と安全リレーモジュールのようにシステムをフェールセーフ化する部分をあわせて、国際安全規格では制御システムの安全関連部分と呼んでいる。

1.8.7 安全スイッチ

作業者の安全が確保されない状態になったときに作動し、自動的にラインを停止させるスイッチのことで、具体的にはガードの可動側に取り付けられた安全スイッチ専用のアクチュエータが、ガードを閉じてスイッチ本体に情報伝達することによってのみ操作可能

になる。IDEC は多種多様の安全スイッチを製造販売している。

1.8.8 ロック付安全スイッチ

ロック付安全スイッチは、機械が稼動中に作業者が誤って扉の中に入ることを防止するために、ロック機構を備えた安全スイッチである。

1.8.9 セーフティーコントローラ

安全リレーモジュールより汎用性がほしいが安全に関するソフトを自らは組みたくない、あるいは、メカニカル入力と電子入力機器でユニットを分けたくないなどの、顧客の様々な要望を満たす形で開発することにした。

IDEC のものは、下記のように多くの特徴を持っている。

すなわち、(1) 安全回路の主要パターンをあらかじめ内蔵しており、ロジック選択するだけで容易にシステム構成が可能のように工夫されている。(2) プログラムレスでロジックの選択のみで、部分停止や全体停止が可能となっている。(3) ひとつのユニットで非常停止用押ボタンスイッチからライトカーテンまで様々な入力の対応が可能となっている。(4) 安全入出力の状態や Safety One(複数の安全入力を 1 つのユニットで簡単に設定できるプログラムレス・ツールレスのセーフティーコントローラ)のエラー情報をモニタ出力できる。(5) Safety One にソレノイド駆動出力を完備している。(6) PLC 側の出力数削減。(7) IEC 61508 シリーズの安全性インテグリティレベル 3、ISO 13849-1 のパフォーマンスレベル e、EU954-1 の安全カテゴリ 4 までの安全性能をそれぞれ満足させる等の特徴を持つ。(8) チャタリング除去等はあらかじめ考慮して作られており、顧客の方で考える必要がないなどである。これらの特徴を備えた代表的な製品に FS1A がある。

FS1A は 8 つのロジックを内蔵しているがそのうちロジック 1 (汎用ロジック) と接点間の同期時間が設定できない機器に対応したロジック 5 の概念は図 1.8.2 と 1.8.3 の通りである。

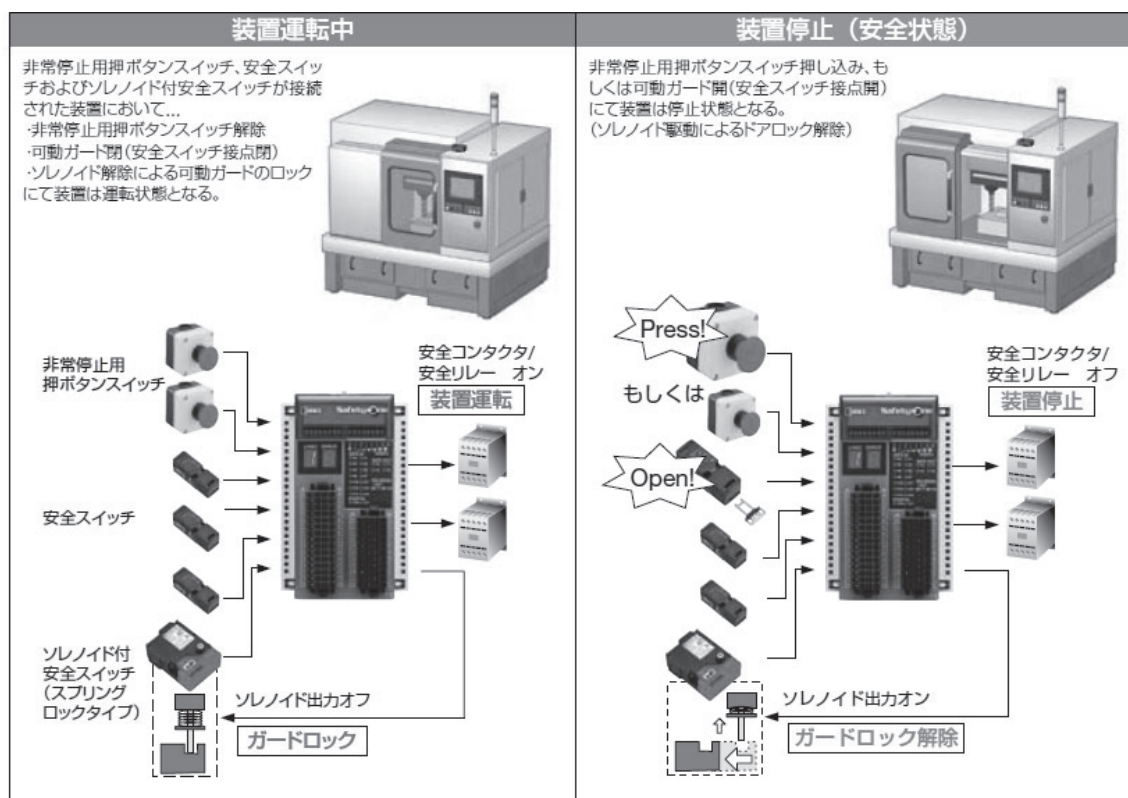


図 1.8.2 ロジック 1（出典 IDEC 社資料）

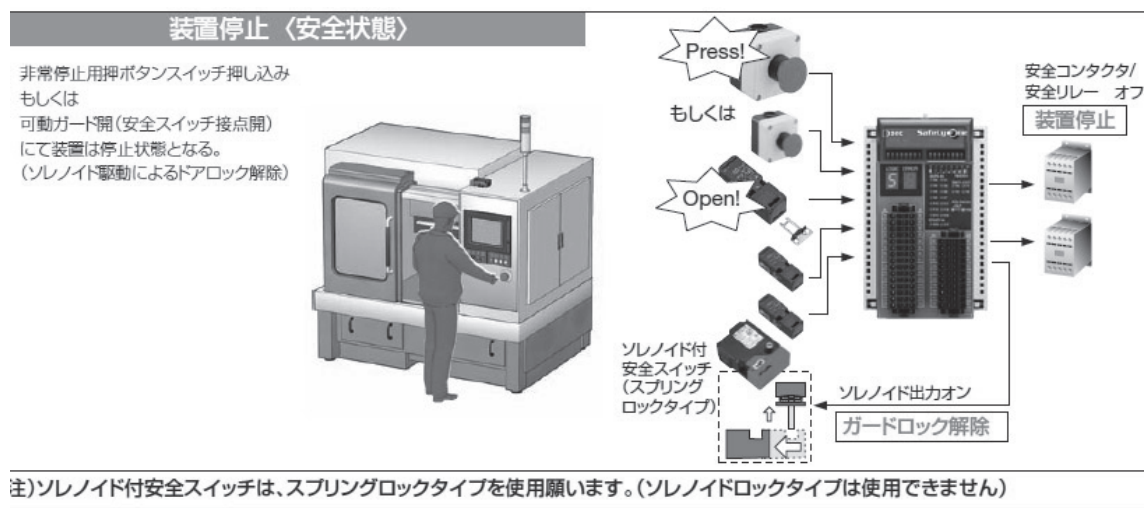


図 1.8.3 ロジック 5（出典 IDEC 社資料）

1.8.10 まとめ

ロボットを使った製造ラインを例としてリスクアセスメントの実施手順は以下の通りである。

1. 安全防護策は何もない
2. 安全柵で囲う。このままでは扉が開いて人が入っても装置は止まらない。
3. 安全スイッチを設置し扉が開いたら、ロボットが止るようにする。
4. 安全スイッチその2（回転物）回転物は止めに行ってもすぐには止らない。止るまでイムラグがある。ロックをかけて安全が確認されるまで人間が入れないようにする。この種のスイッチをロック装置付き安全スイッチと呼ぶ。
5. 安全コントローラ 論理部に一般PLCを接続している場合、異常状態を感知できず、扉が開いていることをシステム側が理解できない。この場合安全コントローラ・安全リレーモジュールを使って安全を確保する。
6. ティーチングにも大きな危険が潜んでいる。イネーブルスイッチ、3ポジションスイッチが安全確保に活躍する。二人同時に入ったばあい、一人が何も持っていないのは、いざという場合危険きわまりないので、最低限グリップスイッチを持ち、どちらの一方もイネーブルスイッチで機械を止めにいけるようにする必要がある。
7. ティーチングペンダントを操作するときはロボットのスピードを落とすようにする。さらに安全に配慮して非常停止ボタンをつける。
8. より多人数向けのパドロックハスプに南京錠をかける方式
人が入っているにもかかわらず、扉が閉まりロックされるとロボットが動き出す仕組みになっていることが多々ある。このような危険をなくすために扉にパドロックハスプを付け、中に入る作業者が南京錠をかける方式を採用する。自動車の製造ラインなどでは何人もの作業者が柵内に入る場合が考えられる。全ての人が南京錠を取らない限り扉は閉められないようにして安全を確保する。パドロックハスプに南京錠をかけることにより、アクチュエータ挿入口がふさがれ、不用意な機械の再起動を防止できる。作業者全員がそれぞれの南京錠でパドロックハスプに施錠し、その後全ての南京錠を開錠して初めて再起動出来るようなシステムにすれば、危険区域内に取り残される事故を防止できる訳である。
9. 半導体製造装置のようにすぐに止めては危険が想定される場合は、EMO(緊急遮断装置)と組み合わせて使う。

1.8.11 開発裏話・・・これから開発する人への助言も含めて

1. 安全スイッチ

安全スイッチの場合メカニカルな動作をするので、特に電子系安全機器に接続する場合は、動きを十分に把握した上で設計する必要がある。

2. PNP と NPN

安全の面では基本的に PNP でなければ駄目という制約がある。規格上は書いていないが、ヨーロッパは PNP が常識であるため、あえて規格上で制限されていない。NPN の場合、認証機関が認証しない可能性が高く、この点十分な注意が必要である。

3. 安全規格

安全規格はヨーロッパの企業が始めたヨーロッパ的考え方であるが、国際競争上積極的に関わっていかないと日本にとって不利な規格が出来てくる。そういう観点から IDEC は規格策定から積極的に参加している。規格にあっていないと世界中のどこにも売れないのが現実である。IDEC 製品は日本企業で初めて IEC スタンドアードに採用された実績がある。

また、規格の変化に迅速に対応する必要がある。一例として「カテゴリ」と「PL(パフォーマンスレベル)」がある。従来は「カテゴリ」で安全制御システムを評価してきたが、ISO 13849-1 : 2006 からは、「PL(パフォーマンスレベル)」によって評価するようになった。これらの変更迅速に対応しないと、大金を投じて製造した商品が規格にあわないというだけで、どこにも売れないという事態も起きうる。

認証について

- A. 開発当初のステージで開発コンセプトを明確にしておく必要がある。これはコンセプト認証というのがあり、コンセプトが明確になっていないと認証作業に入ってくれないからである。
- B. 認証機関以上に開発者は該当規格に精通している必要がある。規格は膨大であり、一方認証機関は比較的少人数から成り立っており、場合によっては認証機関が該当規格をよく知らないこともあり得る。
- C. IEC の認証が万全と考えてはいけなない。場合によっては別途 UL 規格（アメリカ）の認証も取っておく必要があることがある。
- D. とにかく認証取得には膨大な資金と時間が掛かる。このことを開発コンセプトに牢記しておかないと、とんだコスト倒れになることがある。汎用品であればある程度製品コストに転嫁できるが、少数品の場合は特に注意が必要である。

第 2 章 安全に関わる製品調査

昨年度の報告書「組込み系技術者のための安全設計入門」の「SIL3 取得関連製品の現状」に引き続き規格認証機関から SIL3 認証を得ている製品および機能安全への取組みを行っている製品などを調査した。

調査期間は、2009 年 4 月から 2010 年 2 月、調査対象は、C E A T E C 2009、E T 2009、計測展 2009、およびインターネット検索である。

調査した製品は表 2.1 に示す。尚、昨年度の調査結果に新しい調査結果を加える形としたので、本報告書で全ての調査結果がわかるようになっている。

関連製品一覧

表2.1 SIL3取得関連製品一覧

備考： 記載順は、製品区分順

開発元／販売元	製品名	製品区分
Rockwell Automation／ ロックウェルオートメーションジャパン	Guard PLC システム	PLC
ジェイテクト/光洋電気工業	KOSTAC Safety AZ-C1	PLC
シュナイダーエレクトリック／ 富士電機機器制御	Preventa XPS MC シリーズ	PLC
ジェイテック (JTEKT)	TOYOPUC-PCS	PLC
三菱電機	安全シーケンスMELSEC safety	PLC
キーエンス	セーフティネットワークコントローラ SC シリーズ	PLC
オムロン	セーフティネットワークコントローラ NE1A- SCPU シリーズ	PLC
オムロン	フレキシブルセーフティーユニットG9SX	PLC
TRICONEX社製TRINCON/ 株山武	安全計装システム	PLC
HIMA(独)/株日立ハイテクトレー ディング	日立安全計装システム/EX-8000シリ ーズ	PLC
富士電気システムズ(株)	安全計装システム	PLC
ABB in Japan	AC800M HI	PLC
株東芝 セミコンダクター社	モーター制御向け32Bit マイコン TMPM370FYFG/FYDFG	PLC
IDEC(株)	FS1A形 セーフティコントローラ Safety ONE	PLC
IDEC(株)	非常停止用押釦スイッチφ16XA、 φ22Wシリーズ、FBシリーズ	器具

開発元／販売元	製品名	製品区分
Green Hills Software／ アドバンスドデータ コントロールズ	INTEGRITY	RTOS
Wind River/ウィンドリバー	VxWork	RTOS
利芝システムテクノロジー	安診太郎	安全性 評価
サンクス	小型ビームセンサ ST4	光センサ
ETAS/イータス	ASCET	コード 生成
Esterel Technologies/ シディ・アダプコ・ジャパン	SCADE Suite	コード 生成
As-International Association/ 日本 AS-i協会会員会社	AS-Interface Safety at Work	ネットワー ク
キーエンス	セーフティライトカーテンSL-V シリーズ	ライトカー テン

PLC

GuardPLCシステム

システムコンポーネント

SIL3適合

《主要機能》

- ◆ コントローラ、I/O、プログラミング・構成ツールから構成されている。
- ◆ プログラミング・構成ツールはWindows上で動く。

《開発元》 Rockwell Automation (米国)

<http://www.automation.rockwell.com/>

《販売元》 ロックウェルオートメーションジャパン

<http://www.automation.rockwell.co.jp/>

《製品情報》

<http://www.automation.rockwell.co.jp/applications/gs/ap/gsjp.nsf/pages/GuardPLC>

KOSTAC Safety AZ-C1

システムコンポーネント

SIL3適合

《主要機能》

- ◆ プログラミングとして、ファンクションブロック機能とラダー機能を用意している。
- ◆ 安全及び非安全の制御を1台で実行できる。
- ◆ S/N インターフェイス機能(各種オープンネットワーク接続用 I/F 別途ゲートウェイモジュールが必要)
- ◆ 安全ラダー回路チェック機能

《開発元》 ジェイテクト <http://www.jtekt.co.jp/index.html>

ステアリング装置(自動車用)と駆動部品、各種ベアリング、各種工作機械、制御機器を製造、販売。

《販売元》 光洋電子工業 <http://www.koyoele.co.jp/>

《製品情報》 光洋電子工業株式会社 東京都小平市天神町1-171

サポートセンタ Tel:042-349-7700 Fax: 042-345-7994Mail
info@koyoele.co.jp

Preventa XPS MC システム

システムコンポーネント

SIL3適合

《主要機能》

- ◆ それぞれ独立した安全機能を制御できる。その選択と構成はPC上のソフトウェアを使って設定できる。
- ◆ 安全入力は16ないし32点、出力は独立した8点までの安全出力が可能。
- ◆ 安全マットのモニタ等、安全機能は30種類用意され、すべて認証済み。
- ◆ 通信として、CANopen, Profibus, Modbus1に対応できる。

《開発元》 シュナイダーエレクトリック（フランス）

<http://www.schneider-electric.co.jp/>

《販売元》 富士電機機器制御

<http://www.fesys.co.jp>

《製品情報》

http://www.fujielectric.co.jp/fcs/jpn/f/f_SE_h02-PreventaXPSM_Series.html

TOYOPUC-PCS

システムコンポーネント

SIL3適合

《主要機能》

- ◆ プログラミングとして、ファンクションブロック機能とラダー機能を用意している。
- ◆ 安全フィールドバス機能
- ◆ S/N インターフェイス機能（各種オープンネットワーク接続機能用 I/F 別途ゲートウェイモジュールが必要）
- ◆ 安全ラダー回路チェック機能

《開発元》 ジェイテクト <http://www.jtekt.co.jp/index.html>

ステアリング装置（自動車用）と駆動部品、各種ベアリング、各種工作機械、制御機器を製造、販売。

《販売元》 ジェイテクト

《製品情報》

<http://www.jtekt.co.jp/products/toyopuc/toyopuc-pcs/index.htm>

安全シーケンスMELSEC safety

システムコンポーネント

SIL3適合

《主要機能》

- ◆ 従来のシーケンサMELSECをもとにして、規格に適合させた。
- ◆ 安全規格が要求する診断機能や安全機能を備えたMELSEC-QSと、安全フィールドネットワークCC-Link Safetyを含む。システム構成概念図は、図8. 6を参照。
- ◆ 非常停止スイッチ、ライトカーテンなどを接続して、非常停止などの安全制御を実行する。
- ◆ 自己診断機能を持ち、故障検出時に安全出力を強制的にOFFにできる。
- ◆ 最大入力8点、出力4点のリモート局を最大64局接続可能。
- ◆ プログラミングツールはMELSECと同様で、PC上のGX Developerにてパラメータ設定、プログラミングする。

《開発&販売元》三菱電機

<http://www.mitsubishielectric.co.jp/corporate/tech/index.html>

《製品情報》

<http://www2.mitsubishielectric.co.jp/plcq/safety/index.j.htm>

セーフティコントローラSCシリーズ

システムコンポーネント

SIL3適合

《主要機能》

- ◆ ユニット増設によってフレキシブルに安全I/Oを増設可能。
- ◆ 部分停止/全停止やロボットティーチング制御にも対応可能。

《開発元》 キーエンス <http://www.keyence.co.jp/index.jsp>

《販売元》 キーエンス

《製品情報》

<http://www.keyence.co.jp/switch/safety/sc>

セーフティネットワークコントローラ NE1A-SCPUシリーズ

システムコンポーネント

SIL3適合

《主要機能》

- ◆ 従来、リレーを組み合わせていた安全制御回路のプログラマブル化を実現。用意されているファンクションロックを選択、組み合わせてプログラムを作成できる。
- ◆ マルチベンダネットワーク DeviceNetに接続でき、DeviceNet Safetyシステムを構成できる。システム構成図は図8.3を参照。
- ◆ 1台のコントローラは、12ないし16入力可能。ネットワークに16ないし8台までのコントローラを接続可能。
- ◆ I/Oターミナルは、最大16点の入出力可能で、32台までネットワークに接続可能。
- ◆ 標準コントローラからも安全システムのモニタリングが可能。

《開発元》 オムロン http://www.omron.co.jp/r_d/index.html

《販売元》 オムロン <http://www.fa.omron.co.jp/index.html>

《製品情報》 http://www.fa.omron.co.jp/product/family/1625/index_p.html
http://www.fa.omron.co.jp/product/family/1626/index_p.html

フレキシブル セーフティユニット G9SX

システムコンポーネント

SIL3適合

《主要機能》

- ◆ 従来のリレーに比べて、多入力、多出力の複雑な安全制御回路を柔軟に構成できる。
- ◆ 論理接続機能によって拡張が容易。

《開発元》 オムロン http://www.omron.co.jp/r_d/index.html

《販売元》 オムロン <http://www.fa.omron.co.jp/index.html>

《製品情報》 http://www.fa.omron.co.jp/product/family/1524/index_p.html

安全計装システム

システムコンポーネント

SIL3適合

《主要機能》

- ◆ 構成ハードウェアに対し、3重化と2-out-of-3(2oo3)の多数決論理による冗長化機能。
- ◆ 理論値MTTF100年以上の高稼働率の実現
- ◆ オンラインメンテナンスとして故障発生時、稼働中の2回路で2重化運転を継続、異常発生表示とヒューマンエラー防止を十分考慮した部品交換方式
- ◆ システム動作中に潜在する故障を検出するため力端トランジスタのスタックや出力端スイッチの動作確認を定期的、自動的に実施している。

《開発元》 TRICONEX社製TRICON (SIL3)

《販売元》 株式会社 山武

《製品情報》 <http://jp.yamatake.com/product/iap/ks/sis/index.html>

日立安全計装システム EX-8000シリーズ

システムコンポーネント

SIL3適合

《主要機能》

- ◆ 安全性を要求されるプラントの緊急遮断システムの構築
- ◆ 安全PLCの動作状況監視等の安全確保システムの構築

《開発元》 HIMA (独)

《販売元》 (株)日立ハイテクトレーディング

《製品情報》

<http://www.hitachi-hitec.com/group/hcs/products/jyohouseigyo/anzen.html>

安全計装システム

システムコンポーネント

SIL3適合

《主要機能》

- ◆ TUVで認証された50種類のFBによる安全制御プログラムのエンジニアリングが可能
- ◆ S/W「Safety Matrix」による安全回路の自動生成
- ◆ 障害発生時、瞬時に異常事象（故障要因、動作機器）の把握
- ◆ exSILentaia社のexSILentia PFD, SIL計算結果をエンジニアリングデータとしてインポートが可能

《開発元》

《販売元》 富士電機システムズ株式会社

《製品情報》 <http://www.fesys.co.jp/sougou/seihin/micrex-nx/>

AC 800M HI

システムコンポーネント

《主要機能》

- ◆ 安全度レベルを下げることなく、1台のコントローラで安全計装とプロセス制御を結合が可能
- ◆ 安全ラブラリとして、監視ライブラリ、監視基本ライブラリ、火災ガスライブラリ、通信ラブラリを保持各ライブラリはSIL2またはSIL3認証アプリケーションで使用することが可能。
- ◆ プログラミング言語として各SILをallowedファンクション・ブロック・ダイアグラム(SIL1-3), ST(SIL1-3), SFC(SIL1~2)

《開発元》

《販売元》 ABB in Japan

《製品情報》

<http://www.abb.com/product/seitp334/86e458470ba0572f4825762b002f0682.aspx>

**モーター制御向け32Bitマイコン
TMPM370FYFG/FYDFG**

システムコンポーネント

SIL3適合

《主要機能》

- ◆ 最小命令実行時間は12.5ns (@80MHz)
- ◆ 高速でモータ制御とシステム全体制御を同時に可能
- ◆ モータ制御回路は2回路内臓
- ◆ ベクトル制御に必要な高速12bitAD変換器は三相PWM生成回路に同期したサンプリングが可能

《開発元》 (株)東芝 セミコンダクター社

《販売元》 _____

《製品情報》 <http://www.semicon.toshiba.co.jp>

FS1A形
セーフティコントローラ
SafetyONE

システムコンポーネント

SIL3適合

《主要機能》

- ◆ 安全回路のパターンを8個用意。
- ◆ プログラムレス、パターン選択のみで部分停止、全体停止可能
- ◆ ひとつのユニットで非常停止用押ボタンスイッチからライトカーテンまで様々な入力の対応が可能
- ◆ 安全入力の状態、セーフティコントローラのエラー出力を実現
- ◆ セーフティコントローラにソレノイド駆動出力を完備。PLC側の出力数削減可能

《開発元》 IDEC株式会社

《販売元》 _____

《製品情報》

http://www.idec.com/usen/products/Catalogs/AS-i_Safety/E-stops/overview.html

器具

非常停止用押釦スイッチ

φ 16XA、φ 22XWシリーズ、FBシリーズ

器具

SIL3適合

《主要機能》

- ◆セーフティスレーブ機能を内蔵し、AS-interface Safety at Workに対応
- ◆ φ 16、φ 22は、「セーフブレークアクション」、セーフティロック機構、直接回路動作機能を採用および安全機器の省配線化、省スペース化を実現
- ◆保護構造はIP65

《開発元》 IDEC株式会社

《販売元》 _____

《製品情報》

<http://www.idec.com/jpia/products/Catalogs/Safety Products/emergencystop.html>

RTOS

INTEGRITY

ソフトウェアコンポーネント

SIL3適合

《主要機能》

- ◆ 仮想アドレス空間を使ってカーネルとタスクのメモリ空間を分離し、かつタスク間のメモリ空間の分離。
- ◆ タスクごとにメモリとプロセッサ時間の割当のを保証。
- ◆ 高速な割り込み処理によって極小の割込遅延時間(約200ns)を達成。
- ◆ POSIX, VxWorks, μ ITRON向けのAPIを提供。
- ◆ 静的解析ツール等を有する統合開発環境MULTIを備え、最新モデルベース開発ツールとの協調連携が可能。

《開発元》 米国 Green Hills Software <http://www.ghs.com/>

《販売元》 アドバンスドデータコントロールズ <http://www.adac.co.jp/>

《製品情報》 <http://www.adac.co.jp/products/integrity/index.html>

VxWorks

ソフトウェアコンポーネント

SIL3適合

《主要機能》

- ◆ 航空宇宙、船舶等の分野に適用できる高い応答性を有している。
- ◆ 認証取得のための開発プロセスを規定。
- ◆ 認証が取れるAPIサブセットVxWorks/Certを規定。
- ◆ 取得に必要な膨大なドキュメントを提供する。

《開発元》 Wind River (米国) <http://www.windriver.com/>

《販売元》 <http://www.windriver.com/japan/>

《製品情報》 <http://www.windriver.com/japan/products/vxworks/index.html>

安全性評価

安診太郎

ツール

《主要機能》

- ◆ IEC61508に基づいてソフトウェアの機構安全性を総合的に評価する。
- ◆ 開発プロセスに照らして、各フェーズごとに安全度の達成度をグラフ、表を用いてわかりやすく表示する適用事例として図8.4を参照。

《開発&販売元》 東芝システムテクノロジー <http://www3.toshiba.co.jp/tst/>

《製品情報》 <http://www3.toshiba.co.jp/tst/product/anshintaro.htm>

光センサ

小型ビームセンサ ST4

システムコンポーネント

SIL3適合

《主要機能》

- ◆ LEDビームを用いて、1センサヘッドあたり最長15mの範囲を感知できる。
- ◆ 1コントローラの最大6センサヘッドを取り付け可能。
- ◆ 最大3コントローラまで無干渉で構成できる。

《開発元》 サンクス <http://sunx.jp/japanese/company/profile/technology.html>
センシング技術とレーザ技術をコア技術として、FA化に貢献している。

《販売元》 サンクス <http://sunx.jp/index.html>

《製品情報》 <http://sunx.jp/japanese/products/safety/st4/index.html>

コード生成

ASCET

ツール

SIL3適合

《主要機能》

- ◆ ASCETは自動車用ECUソフトウェア開発を支援するツールセット。モデリング、プロトタイピング、コード生成等を支援する。
- ◆ ASCET-SEはモデルから各種マイクロプロセッサをターゲットとする量産用 ECUコードを自動生成するツール。
- ◆ AUTOSAR準拠の開発を支援できる。
- ◆ MATLAB/Simulink モデル及び UML表記からの変換が可能。
- ◆ XML形式でデータを保存し、要件管理、構成管理等のツールとの連携が可能。
- ◆ 対応するマイクロプロセッサは、日立、NEC、Motorola、Infineon、TI等。
- ◆ 生成されたコードは、MISRA-Cに準拠し、SIL3に適合する。

《開発元》 ETAS (ドイツ) http://www.etas.com/ja/about_etas.php

車載ECU用ソフトウェア開発ツールの専門メーカーであり、2004年からAUTOSARのプレミアムメンバになっている。

《販売元》 イースタ <http://www.etas.com/ja/index.php>

《製品情報》 http://www.etas.com/ja/products/ascet_software_products.php

《主要機能》

- ◆ 要件管理機能によるトレーサビリティ管理
- ◆ システム設計ツールとのインターフェース(SysML/UML,アルゴリズム設計ツール)
- ◆ SCADE言語によるモデリング(データフロー/制御フローの自由な構造)
- ◆ モデルレベルでの検証支援(セマンティックチェック、モデルシミュレーション、モデルカバレッジ、形成検証、ワーストケース実行時間見積り、コンパイラ検証キット)
- ◆ 認証可能なCコードの自由生成
- ◆ 設計モデルに対するレポートの自動生成

《開発元》 Esterel Technologies (フランス)

<http://www.esterel-technologies.com/>

《販売元》 シーディーアダプコ・ジャパン <http://www.cdaj.co.jp/>**《製品情報》** <http://www.cdaj.co.jp/product/070000scade/index.html>

ネットワーク

**AS-Interface
Safety at Work**

システムコンポーネント

SIL3適合

《主要機能》

- ◆ 標準 AS-i システムに非常停止スイッチ等のセーフティ機器を接続することが可能とする。
- ◆ セーフティ信号伝送のために、標準AS-i システムにセーフティモニタとセーフティスレーブを追加する。スレーブからモニターへの最大応答時間は、40ms。
- ◆ AS-i システムとは、制御システムにセンター、アクチュエータを接続するネットワークである。システム構成概念図は図8.5を参照。

《開発元》 AS-International Association <http://www.as-interface.net>

AS-Interfaceを普及、促進すること及び、IEC62026-2(AS-Interfaceを規定)の改定・技術サポートをする団体。日本AS-i 協会は、各国にある協会の一つで、日本国内への普及拡大と各種要望をとりまとめて提出する団体。

《販売元》 日本AS-i 協会会員会社。(シーメンス/ピーアンドエフ/IDEC/富士電機機器制御等) <http://www.as-i.jp/>

《製品情報》 http://www.as-i.jp/prd_sms1.html

ライトカーテン

セーフティ ライトカーテン
SL-Vシリーズ

システムコンポーネント

SIL3適合

《主要機能》

- ◆ 機器の存在が見れる表示灯内臓。
- ◆ スリムタイプだけでなく、堅牢・防水タイプもラインアップ。

《開発元》 キーセンス <http://www.keyence.co.jp/index.jsp>

《販売元》 キーセンス

《製品情報》 http://keyence.co.jp/switch/safety/sl_v/index.jsp

第3章 機能安全の Web. その事例と期待効果

本委員会は、「製品安全 Web ページ」を作成し、JASA の Web サーバにて運用している。製品安全 Web ページは、製品安全に関する情報を集積し、情報のポータルサイトとなることを目指して運用している。

以下では Web ページとしての目標を議論する。

3.1 ポータルサイトが具備すべきことから

ポータルサイトが具備すべきことからとして、次のような事柄が考えられる。

- 1) 最新情報
- 2) 情報公開
- 3) 通常の情報へのポインタ (アンカ)
- 4) 情報交換 掲示板
- 5) ダウンロード・ページ
- 6) 最近の情報の解説
- 7) 最近の動向
- 8) 実力判定クイズ
- 9) アンケートのページ
- 10) 意見を投稿するページ

以下では、上記の各項目について詳しく述べる。

3.1.1 最新情報

最新情報とは、製品安全に関する最新の情報への参照であり、新しい情報へのポインタ (アンカ) を簡単に掲載する。

基本的に、題名と、記事本体へのアンカを掲載する。それに加えて、抄訳があればなお良い。が、抄訳を作成する手間やコストが必要となる。

3.1.2 情報公開

報告書を Web ブラウザで読めるようにする。

報告書を HTML 形式に直し、Web ブラウザで直接に読めるようにする。

「最近の情報の解説(後述)」を、アーカイブ(蓄積)していき、それを公開していけば、それによっても公開情報は増える。

b)用語辞典(機能安全用語辞典)

2008 年度、2009 年度に、吟味して、定めた用語を、用語辞典として公開する。

製品安全の分野の用語は、まだ共通のものとして固まっていないものがあるので、どの用語を使うかの指針を委員会で持たなければならない。

3.1.3 通常の情報へのポインタ(アンカ)

製品安全に対応した各製品などの情報を集積し、公開する。

JASA メンバー以外の情報も、網羅的に取り上げるべきである。

製品安全 Web ページは JASA の費用で運用されているため、JASA メンバー企業は、優先的に有利な位置に表示されるような配慮などが必要である。

3.1.4 情報交換

掲示板が考えうる。掲示板は、モデレータが居れば、不適切発言を削除でき、また、議論の方向性を決められる。また、最初から、運用のポリシーを明確にして、はっきり打ち出しておけば問題が出ることがない。

ただし、モデレータが不在の掲示板は、いわゆる「荒れた」状態になるので、モデレータを担当する人的資源やコストが無い場合は、掲示板は運用すべきではない。

3.1.5 ダウンロード・ページ

報告書などをファイルとしてダウンロードできるようにする。報告書は JASA に権利があり、報告書のすべてを、会員以外に無制限に配布することは難しい。したがって、PDF 形式による配布は行えないだろう。

3.1.6 最近の情報の解説

製品安全に関する最近の情報の解説を行う。抄訳や解説記事を掲載すれば、魅力的なサイトとなり、訪れる人が増え、ポータルサイトとしての価値が高まるだろう。しかし、ながら記事を書く労力が必要となり、完全な無償のボランティアにより実施し続けることは難しいと思われる。委員会の希望としては、26262 の解説などを手始めに手がけてみたい。

3.1.7 最近の動向

製品安全に関する最近の情報の解説を行う。製品安全はこれからの分野であるから、最近の動向を解説した記事を掲載すれば、非常に価値が高く魅力的である。これについても、記事執筆の労力が必要であり、無償ボランティアによるものでは、すぐに限界が来ることが予測される。

3.1.8 実力判定クイズ

試験を作成する。Web ページで問題を出題し、回答者はブラウザ上で回答を行う。数問から数十問を一通り回答した後、機械が採点し点数などを表示する。回答者は誤ったところを、自己学習できるようにする。

評判が良ければ、ETEC のような有償による試験を実施する事業化も可能だろう。

問題作成の労力が必要である。また、システムの立ち上げ時には、出題、採点のシステムを作成するコストが必要である。

3.1.9 アンケートのページ

委員会の必要に応じて、適宜、アンケートを実施できるようにする。

製品安全についての一般的なアンケートや、本委員会に関するアンケートを適宜実施できるページを用意する。

アンケートのシステムも、作成のコストが必要である。

3.1.10 意見を投稿するページ

意見収集用の掲示板か、メール送付用のアンカが、あれば、それでことは足りる。

掲示板は前述のように、モデレータが必要なので、低コスト運用の場合は、委員会へのメール送付用のアンカを用意するのが良いだろう。

3.2 製品安全 Web ページの目標

3.1 節では、ポータルサイトとして考えうる項目を列挙した。

ここでは、本委員会での、製品安全 Web ページの初期の立ち上げ時に実現すべき機能を考える。

これまでの委員会活動により、製品安全の用語集、製品情報や報告書などは充実しており、公開して広く活用されるべき価値を持っている。

したがって、本委員会では、製品安全 Web の立ち上げ時には、製品安全の用語集、製品情報、ダウンロード・ページを作成し用意する。

アンケートなどは、本当に必要とされ、作成のための資源があるときに、作成するとし、Web ページの立ち上げ時には用意せず、作成もしない。

モデレータを立てる資源がないため、当面、掲示板は採用しないこととする。

3.3 実現技術

製品安全 Web ページを実現する技術について述べる。

Web サーバは、JASA の Web サーバを利用する。JASA の Web サーバに Wiki システムを導入し、Wiki システムを用いて、製品安全 Web ページを運用する。

Wiki システムは HTML 言語など知らなくとも、Web ブラウザを用いたユーザ・インターフェースで、Web ページの新規作成、編集、更新が可能である。委員会のメンバーが直接に編集を行えるので、便利である。

アンケートと実力判定クイズなどは、CGI として実現する。CGI 記述言語は、perl、Ruby、PHP などを考えており、本委員会としては、特段、言語をひとつに決定する必要はないと考えている。ただし、先述のとおり、アンケートなどは、初期には作成しない。

3.4 現状

現在は、JASA のサーバ上の Wiki システムにて運用中である。

用語集、製品情報、報告書などのダウンロード・ページ(ダウンロード対象のコンテンツは作成中)が稼働している。

近々には、コストの目処がつけば、アンケートのページを作成したい。

また、実力判定クイズは、興味深いので、今後、作成者、コストの目処などがつけば、実現したい。

3.5 期待される効果

製品安全の用語集、集積された製品情報は、他に比類が無く、魅力的である。

最初に適切な広報がなされれば、早期に多くのページビューを実現できるであろう。

コンテンツが比類なく魅力的なので、早期の立ち上がりが多少悪くとも悲観せずに、情報提供を続けることが重要であろう。長い期間に情報を検索され、ページを見られるうちに、認知度が上がり、それにつれページビューもあがることと思われる。

それに伴ない、本委員会の成果も認知され、また JASA の価値も再認識されるであろう。

第 4 章 機能安全に関する用語

本報告書に出てきたキーワードを中心に機能安全に関する用語集をまとめた。

主な引用先や参考文献として、向殿政男教授のご好意により、規格化予定の ①同氏監修 JIS B 9701:0000「機械類の安全性—基本用語」で作られた用語集の素案を提供いただいた。これに加えて、JIS 規格の ②JIS B 9700-1:2004 (ISO 12100-1:2003)「機械類の安全性—設計のための基本概念、一般原則—第 1 部：基本用語、方法論」、③JIS C 0508-4:1999「電気・電子・プログラマブル電子安全関連系の機能安全—第 4 部：用語の定義及び略語」、④JIS Z 8115:2000「ディペンダビリティ（信頼性）用語」を参照した。その他、製品安全ワーキンググループ調査研究で使用した向殿政男教授監修の 3 部作、第 1 巻「安全設計の基本概念」、第 2 巻「機械安全」、第 3 巻「制御システムの安全」も参考にした。

本用語集の編集に当たり、以下の点に留意した。

- (1) 定義の厳密性から JIS 規格の定義を最優先した。
- (2) 規格間でも用語の定義や表記が異なる場合がある。その場合は、③→④→①／②の順で優先度をつけて、本用語集の説明として採用した。
- (3) 規格で定義されていない用語や、IT 一般用語など、機能安全に直結しない一般的な用語も含むが、これらは本書の記載に従ったり、Web 上の情報や他の文献を参考に説明を加えた。

本用語集は、機能安全に係る用語集として初めての試みであるが、2010 年には国際規格 IEC 61508 の第 2 版が発行されるなど進歩・発展中の分野であり、また、近年多方面から注目を浴びている分野でもあるので、用語集としては、表記の適切化や網羅性の拡充など、今後の改善も必要とされる。今後 JASA のホームページを通じて Web 等で公開すると同時に随時ブラッシュアップを図るため、読者のご支援をお願いしたい。

以上読者諸氏の機能安全の理解上の一助になれば著者一同望外の喜びでもある。最後にご協力頂いた明治大学理工学部情報科学科の向殿政男教授に深謝申し上げる。

見出	用 語	英文 (略号)	解 説	出 典
	A A、B、C規格	A、B、C Standard	国際安全規格はA、B、Cの三層構造の体系となっており、Aは基本安全規格、Bはグループ安全規格、Cは個別機械安全規格をいう。このような体系により原則上、あらゆる分野にもれなく適用可能となっている。	JIS B 9700-1:2004 Ⅲ) の図1.1)
	ALARP	As low as reasonably practicable	許容域のリスクと非許容域のリスクとの間に、トレードオフ領域があり、多少のリスクがあっても得られる便益の方が大きいと判断できるケースでは、適切に実行可能な範囲でできるだけリスクを低くしなければいけないとする考え方。	
	ALE	Annual Loss Exposure	米国標準技術研究所 (NIST: National Institute of Standards and Technology) が推奨する定量的リスクアセスメントの手法であり、次式で求められる年間の予想損失額をいう。	
	C CASSスキーム	Conformity Assessment of Safety related System Scheme	2001 年より開始されている IEC 61508 に適合していることを証明する認証制度のスキーム。英国で石油化学プロセス産業が中心となって創設された。CASSスキームは、部品供給者からエンドユーザに至る製品/プロセスの認証体系を形成し、5つのタイプの認証形式が考えられている。	
	Category	Category	ここでは安全カテゴリのこと。カテゴリに同じ。	JIS B 9705-1、3.2
	COTS	Commercial Off-The-Shelf	ソフトウェアやハードウェアの製品に利用される、一般にライセンス提供される既製品やパッケージなどの商用製品を指し、防衛産業から始まった。COTS により市販のサブシステムを組み込むことによって、開発の速度を上げ、コストも抑えられる反面、仕様や設計についての情報が不足から安全性能に問題があるケースがある。	
	CRAMM	CCTA Risk Analysis and Management Methodology	英国大蔵省 (CCTA: Central Computer and Telecommunications Agency) と英国規格協会 (BSI: British Standard Institute) が共同開発した資産の識別、資産評価を質的技法と量的技法を併用し、脅威、脆弱性を分析する手法。	
	D DISC PD3000方式	Delivering Information Solution to Customer (DISC) PD3000 method	GMITS (The Guidelines for the management of IT Security: ITセキュリティマネジメントのためのガイド) の情報資産の範囲をITから一般の情報資産にまで拡大したアプローチを取る。管理基準をチェックリストとし、基準からの差異 (GAP) に基づき脆弱性を分析する。以下の算出式により、リスクを定量的に示す手法。 リスク=資産価値×脅威×脆弱性 DISCは、英国規格協会の事業の一つで、文書管理、情報通信技術に関する標準規格の普及を目的にガイドブックや実践書を出版している。この事業の一環としてBS7799の認証取得に関して実践的な解説を行う文書としてPD3000シリーズが出版されている。	
	DSL	Domain Specific Language	ある特定の製品や特定の分野に特化したドメイン固有言語のこと。ドメイン特化言語あるいはドメイン固有プログラミング言語とも言われる。CやJavaのような汎用プログラミング言語やUML (Unified Modeling Language) のような汎用モデリング言語とは	
	E E/E/PES	Electrical/Electronic/Programmable Electronic System	電気/電子/プログラマブル電子系の略号。制御、保護又は監視を行う1個以上のE/E/PE機器を含むシステム。入力装置 (センサーなど) /データハイウェイ及び他の通信経路/出力装置/最終装置 (アクチュエータなど) を含む。例えば、輸送機器、化学プラント、医療機器などにおけるE/E/PEがこれに相当する。なお、IEC 61508では、機械だけで構成する装置は含まない。	JIS C 0508-4:1999 3.3.3
	ECC	Error Correcting Code	符号化の段階で、情報ビットに加えて、検査ビットと呼ばれる冗長ビットをもたせておき、それを利用して誤りを自動的に訂正できるようにした符号。代表的なものに「ハミング符号」がある。	
	ETA	Event Tree Analysis	イベントツリー解析 / 事象の本解析のことで、安全性解析やリスクアセスメントで用いられる手法の1つ。ある初期事象からスタートして、いろいろな経路をとることにより結果がどうなるかを明らかにする手法である。	情報マネジメント用語事典
	EUC	Equipment Under Control	被制御装置又は被制御系のこと。製造、輸送、医療、その他の活動に用いられる機器、機械、装置やプラントなどのこと。 備考 EUC制御系はEUCから分離区別される。	JIS C 0508-4:1999 3.2.3
	EUCリスク	EUC risk	EUCまたはこれとEUC制御系との相互作用によって生じるリスク。 備考1 リスクは、各々の危険事象に対応している。個々の危険事象に対して、E/E/PE安全関連系、他技術安全関連系及び外的リス軽減施設を用いて、必要とされるリスク (すなわち機能安全にかかわる当該リスク) の軽減が行わなければならない。 備考2 EUCリスクの決定の主目的は、E/E/PE安全関連系、更に他技術安全関連系及び外的リス軽減施設を考慮しない場合でのリスクに対する論点と決定することにある。	JIS C 0508-4:1999 3.2.4
	EUC制御系	EUC Control System	プロセス及び/又はオペレータからの信号に応答して、EUCを望ましい方法で運転するための出力信号を生成するシステム。EUC制御系は、入力装置及び最終要素を含む。	Ⅱ) 表4.6
	F FMEA	Failure Mode and Effects Analysis	日本語では「故障モードとその影響解析」という。JIS Z 8115では、「設計の不完全さや潜在的な欠点を見出すために、構成要素の故障モード (形態) とその上位アイテム (システム) への影響を解析する技法」とされ、潜在的な故障・不具合の防止を目的としたボトムアップの体系的な分析手法である。設計段階で事故・故障を設計段階で予測・摘出する「設計FMEA」、製造工程中での各故障モードの管理信頼性を評価する「工程FMEA」がある。	JIS Z 8115:2000 情報マネジメント用語事典
	FMECA	Failure Mode and Effect Analysis Failure Mode、Effects and Criticality Analysis	故障モードとその影響解析手法であるFMEAに故障モードの発生確率を加えて“致命度” (Criticality) を算定し、対策の優先順位を合理的に決定する手法をいう。FMEAでは故障がシステムに対して致命的影響を及ぼすのか、軽微なのかを重要度として表わすが、FMECAはこれに故障モードが発生する頻度を加味して故障リスクの大きさを算出し、システムの安全性を定量的に評価する。致命度の尺度としては、危険度 (影響の厳しさX発生率)、危険優先度 (厳しさX発生率確率X検知可能性)、致命度指数などがある。	

見出	用 語	英文 (略号)	解 説	出 典
	FMEDA	Failure Modes、Effects and Diagnostic Analysis	「故障モード影響診断解析」に同じ。	
	FTA	Fault Tree Analysis	安全性及び信頼性の両面から見て、発生してほしくない事象に関し、論理記号を用いて、その発生の経過を遡って枝分かれの形で表した図（樹形図）に展開した上で、発生経路及び発生原因、発生確率を解析する技法。	
	G GMITS	Guidelines for the Management for IT Security	ISO/IEC TR13335が紹介しているセキュリティリスクを分析するガイドライン。以下の算出式により、リスクを定量的に示す。 『リスク（金額／年）』＝『予想損失額（金額）』×『発生頻度（回数／年）』	
	H HAZOP	Hazard and Operability Study	リスクシナリオ分析手法の一つで、化学プロセスにおける複数の独立した事象が複雑に絡む故障を取り扱うために開発された手法。特に設計仕様（例えば、温度、圧力、PH、攪拌、反応）から逸脱した運転を行なった際、設計の目標値からのズレの発生個所及びそこで発生するハザードとその原因を解析し、それぞれの原因から危険事象への進展を阻止する防護機能と改善対策を調査する手法として用いられる。目標値からのズレを想定するために、「ガイドワード」を用いるのが一般的である。	
	HTA	Hierarchical Task Analysis	階層的課題分析という手法。複数の作業工程からなる職務や分岐を含む作業、複数人の協働による作業等について分析する際に用いられる人間工学的なアプローチをとる階層的課題分析技法。インタフェース設計・評価や機能の割当て、エラー予測、作業負荷評価などに適用される。	
	I IEV	International Electrotechnical Vocabulary	国際電気標準用語集のこと。IEC（International Electrotechnical Commission：国際電気標準会議）規格で使用する用語の定義と、用語そのものの多国語表記、多国語索引を分野別に分冊としたIEC 60050シリーズ規格として発行されている。	IEC 60050
	ISO 13849	ISO 13849	機械類の安全制御システムに要求される一般原則や性能を規定する規格。国際規格の3段階の階層構造でいうB1に属する。従来のISO 13849-1：1999は、「カテゴリ」で安全制御システムを評価してきたが、ISO 13849-1：2006からは、「PL（パフォーマンスレベル）」によって評価するようになった。	
	ISO/IEC Guide 51	ISO/IEC Guide 51：1999（Safety Aspects - Guidelines for their Inclusion in Standards）	安全側面に関する事項を規格に盛り込む場合の指針について規定した国際基準。各種安全規格の最上位に位置付けられる。	Ⅲ）3.1 ISO 13849-1とは（P.99）
	J JRMS	JIPDEC Risk Analysis Method 2002	JIS Q 2001「リスクマネジメントシステム構築のための指針」に基づいて、日本情報処理開発協会（JIPDEC）が開発した定性的リスク分析方法論であるJRAM（JIPDEC Risk Analysis Method）からぜい弱性分析方法を適用して開発されたリスク・マネジメントの仕組み。脆弱性分析をベースとし、ネットワークを前提とした情報環境を認識し、さらに情報リスクが経営の根幹を握るという局面も考慮した視点も手法に取り入れられている。組織の脆弱性を認識するには、関係者のリスク認識度合いについてJRMSの質問項目を通して把握し、それにより現状を促える。	セキュリティ用語辞典
	M MISRA	MISRA	MISRAはThe Motor Industry Software Reliability Associationの略で、欧州の自動車業界団体の名前。MISRAでつくられた標準のうちC言語のためのコーディングガイドラインMISRA-Cが有名。	
	MOP	Maintenance and Operability Study	プラントの保守や操作に関して、ハードウェア上の危険源を識別する手法の1つ。	J. Gould, M. Glossop, A. Ioannides, REVIEW OF HAZARD IDENTIFICATION. TECHNIQUES, HSL/2005/58
	MTTR	Mean Time To Restoration	平均修復時間。修復時間の期待値。	JIS Z 8115
	P PFD	Probability of Dangerous Failure on Demand	EUCまたはEUC制御系から作動要求があったときに、E/E/PE安全関連系が規定の安全機能を実行できない確率。	
	PFH	Frequency of a Dangerous Failure per Hour	E/E/PE安全関連系における単位時間あたりの危険側故障の確率。	
	PHA	Preliminary Hazard Analysis	これまでのハザードまたは故障の経験、知識によって、危害やハザードを招くおそれのある事象の特定を行い、さらに現時点で与えられている生産活動、施設、製品、システムの条件下でそれらが発生する可能性を特定する手法。開発プロジェクトの初期段階で、設計の詳細や操作手順について情報がほとんどない場合に一般的に用いられる。	Think IT
	R Risk Graph	Risk Graph	リスクグラフに同じ。	
	Risk Matrix	Risk Matrix	リスクマトリックスに同じ。	
	R-Map	Risk-Map	リスクマップに同じ。	
	S SIL	Safety Integrity	安全度水準に同じ。	JIS C 0508-4:1999
	SRP/CS	Safety-Related Parts of Control Systems	制御システムの安全関連部と同じ。	Ⅲ）第3章 コラム（P.107）
	SRS	Safety Related System	安全関連系と同じ。	JIS C 0508-4:1999 3.4.1
	T TBQ	Taxonomy-Based risk identification Questionnaire	リスクの同種側面の集まりを「クラス」、それを構成するものを「要素」、要素に属する性質を「属性」といい、リスクをこの三つの属性に分類し、この属性に関するチェックリスト作成する手法。元々はソフトウェア開発のリスクを特定するために開	

見出	用 語	英文 (略号)	解 説	出 典
	TOE	Target Of Evaluation	評価の対象となるソフトウェアやハードウェアなどの製品をいう。これらは、それに関連する管理者及び使用者の手引書(利用者マニュアル、ガイダンス、インストール手順書など)を含むことがある。	
V	Vモデル (V字モデル)	V model (V Character Model)	ソフトウェア開発の中で行うべき活動とその成果物を規定して、ソフトウェア開発のライフサイクルをグラフィカルに表現したもの。自動化されたシステム検証フレームワークとの関連でなされるステップを要約している。ドイツ政府関連のソフトウェア開発工程を規定するために開発された。	
W	What-if	What-if	非体系なブレインストーミング手法であり、手順として、悪い事態を仮定し、それによって起きる事故とその安全防御を考察する。例えば、評価チームのメンバそれぞれの気付きにより、「ポンプが故障で停まったら」、「バルブが閉まったら」、「不純物が混入したら」といった異常の引き金事象を想定し、それが発生した際のプロセスへの影響の検討、安全策の妥当性を評価する。	
あ	アーキテクチャ	Architecture	システムでのハードウェア及びソフトウェア要素の構成法。	JIS C 0508-4:1999 3. 3. 5
	アーキテクチャ制約	Architecture constraints	サブシステムの「タイプ」、「安全側故障割合」、および、「ハードウェアフォールトトレランス」によって、システムが主張できる安全度の上限を定めるもの。	
	アイテム	Item	ディペンダビリティの対象となる、部品、構成品、デバイス、装置、機能ユニット、機器、サブシステム、システムなどの総称、又はいずれか。	JIS Z 8115
	アクチュエータ	Actuator	制御機器の、外部に対して作動力が働く部分 (IEV 441-15-22)。	*) JIS B 9960-1、 3. 1
	圧力 (検知) マット	Pressure (sensitive) mat	圧力を検出するセンサ、制御装置及び一つもしくはそれ以上の出力信号開閉装置を含み、上に立っている人、又は上を歩く人を検出する保護装置。 ISO12100-1の3. 23. 5参照。 備考 圧力検知マットの有効検知領域は部分的に変形してセンサが作動する。	*) ISO 13856-1、 3. 1
	安全	Safety	受容できないリスクから免れている状態。言い換えれば、残存リスクが許容リスク以下であることが安全の必要条件である。	JIS C 0508-4:1999 3. 1. 8
	安全側故障	Safe failure	安全関連系を潜在的に危険な方向、すなわち、機能失敗の状態にする可能性がない故障。 備考1 安全性向上のための多チャンネルをもつシステムでは、安全側ハードウェア故障が誤ったシャットダウンへと導くことはより少ない。 備考2 安全側故障率を λS 、危険側故障率を λD と表記すると、安全関連系全体の故障率 λ は、 $\lambda = \lambda S + \lambda D$ となる。	JIS C 0508-4:1999 3. 6. 8
	安全関連系	Safety-Related System (SRS)	EUCを安全な状態に移行させるため、又はEUCの安全な状態を維持するために必要な安全機能を行い、かつ、それ自体で、若しくは、その他のE/E/PE安全関連系、他技術安全関連系、又は、外的リスク軽減施設と協調して、要求される安全機能に対して必要な安全度水準 (SIL) を達成するようなシステムをいう。E/E/PES以外の技術に基づく安全関連系を他技術関連系という。	JIS C 0508-4:1999 3. 4. 1
	安全関連ソフトウェア	Safety-related software	ある安全関連系の安全機能を実施するために用いるソフトウェア。	JIS C 0508-4:1999 3. 5. 11
	安全規格の階層構造	Hierarchical Structure of Safety Standard	機械安全に関する規格の制定をするための基準としてIEC及びISOが共同で作成したIEC/ISOガイド51には、国際規格を階層別に分類することを規定しており、その安全規格の全体的な体系をいう。最新の技術で製造される機械にも適用できるような規格構造としている。	
	安全機能	Functional safety Safety Function	E/E/PE安全関連系、他技術安全関連系又は外的リスク軽減施設によって遂行される機能。この機能は、特定の危険現象に対してEUCにかかわる安全な状態を達成又は保持する。	JIS C 0508-4:1999 3. 5. 1
	安全機能要求仕様	Safety functions requirements specification	安全関連系が実行する安全機能にかかわる要求事項が含まれる仕様。 備考1 この仕様は安全要求仕様の一部 (安全機能の部分) であり、安全関連系によって実施されなければならない安全機能にかかわる要求事項を包括する。 安全要求仕様参照。 備考2 仕様は、安全機能が明確に理解できるという条件を満たせば、テキスト、流れ図、マトリックスなどの形式で記述してもよい。	JIS C 0508-4:1999 3. 5. 9
	安全故障率故障割合	Safe Failure Fraction (SFF)	サブシステムの全体の故障率に占める安全側故障率の割合。 $(\lambda S + \lambda DD) / (\lambda S + \lambda D) < \lambda S$:安全側故障率、 λD :危険側故障率、 λDD :自己診断テストによって検出可能な危険側故障率」という式で定義される。	
	安全度	Safety integrity	ある安全関連系が、定められた期間、すべての定められた条件で、要求される安全機能を果たす確からしさ。 備考1 安全関連系の安全度の水準が高いほど要求される安全機能に失敗する確率が低くなる。 備考2 安全度の決定には、不完全な状態へと導く機能失敗の全原因 (ランダムハードウェア故障及び決定論的原因故障) が含まなければならない。 備考3 安全度には、ハードウェア安全度及び決定論的原因安全度が含まれる。	JIS C 0508-4:1999 3. 5. 2
	安全度水準	Safety Integrity Level (SIL)	安全関連系 (SRS) に割り当てられる安全機能の安全度要求事項を特定するための4種類の可能な離散的水準。安全度水準4は最高の安全度水準であり、1は最低である。	JIS C 0508-4:1999 3. 5. 6
	安全度要求仕様	Safety integrity requirements specification	安全関連系が実行する安全機能にかかわる安全度の要求事項を含む仕様。安全要求仕様参照。 備考 この仕様は安全要求仕様の一部 (安全度の部分) である (安全要求仕様参照)。	JIS C 0508-4:1999 3. 5. 10
	安全な状態	Safe state	安全が達成されているEUCの状態。 備考 EUCは、潜在的に危険な状態から最終的に安全な状態に移行する間、幾つかの中間的な状態を遷移する場合がある。幾つかの状況では、安全な状態は、EUCが制御し続ける場合だけ存在する。そのような連続制御は、短時間又は無期限にわたることもある。	JIS C 0508-4:1999 3. 1. 10

見出	用 語	英文 (略号)	解 説	出 典
	安全文化	Safety culture	安全に関して組織・個人における姿勢・特性 (ありよう) を集約したもの、すなわち組織と個人の双方を含めて、安全問題について適切に対処すること。安全文化の基本概念は、1986年に発生したチェルノブイリ事故の原因の調査・分析の結果をきっかけとして生まれた。そのとき国際原子力機関IAEA国際原子力安全諮問グループ (INSAG : International Nuclear Safety Advisory Group) が行なった報告「チェルノブイリ事故の検討会議の概要報告」の中で安全文化の必要性が提唱された。	
	安全防護	Safeguarding	安全を防護すること又はそのための保護装置。本質的安全設計方針によって合理的に除去できない危険源、又は十分に低減できないリスクから人を保護するための安全防護物の使用による保護方針。 備考 JIS B 9700-2:2004の5は安全防護を扱う。	*) JIS B 9700-1、3.20
	安全要求仕様	Safety requirements specification	安全関連系が実行する安全機能にかかわるすべての要求事項を含む仕様。 備考 この仕様は、つぎのように分類できる。①安全機能要求仕様、②安全度要求仕様	JIS C 0508-4:1999 3.5.8
	安全ライフサイクル	Safety lifecycle	安全関連系の遂行上に必要な業務。プロジェクトの概念フェーズから出発してすべてのE/E/PE安全関連系、他技術安全関連系及び外的リスク軽減施設の必要性が終了するまでの期間に生じる。全安全ライフサイクルを参照。	JIS C 0508-4:1999 3.7.1
い	イネーブル装置	Enabling device	連続的に操作するとき、機械が機能することを許可する起動制御に連携して用いる補足的な手動操作装置。 備考 イネーブル装置の規定については、JIS B 9960-1:1999の9.2.5.8を参照。	*) JIS B 9700-1、 3.26.2
	インターロック	Interlock	特定の条件 (一般的にはガードが閉じていない場合) のもとで危険な機械機能の運転を防ぐことを目的とした機械装置、電気装置又はその他の装置。 備考 インターロック装置 (Interlocking device) ともいう。	*) JIS B 9700-1、 3.26.1
う	運用モード	Mode of operation	安全関連系への作動要求頻度の観点から区分する安全関連系の使用法。これは、低頻度作動要求モードか、高頻度作動要求モード又は連続モードのどれかとしてよい。	JIS C 0508-4:1999 3.5.12
え	影響解析	Impact analysis	あるシステムの機能や要素の変化によって生じる、当該システムのその他の機能や要素又はその他のシステムへの影響を特定する業務。	JIS C 0508-4:1999 3.7.4
	エミッション値	Emission value	機械から生じるエミッション (例えば、騒音、振動、危険物質、放射) を数量化した数値。 備考1 エミッション値は機械の特性についての情報の一部であり、リスクアセスメントのデータ等として使用される。 備考2 用語“エミッション値”は、機械使用中の人のエミッションへの暴露を数量化した“暴露値”と混同すべきでない。暴露値はエミッション値を使用して推定することができる。 備考3 標準化された方法により、例えば、同種の機械間で比較できるように、エミッション値を適切に測定しそれらが関係する不確かさを決定する。	*) JIS B 9700-1、3.38
	エラー	Error	計算、観察又は測定された値もしくは状態と、真の特定された又は理論的に正しい値もしくは状態との不一致。	JIS C 0508-4:1999 3.6.11
お	オペレータ	Operator	機械の据付、運転、調整、保全、清掃、修理、運搬を業務とする単独の人又は複数の人。	*) TR B 0008、3.21
か	ガード	Guard	保護するために機械の一部として設計された物理的なバリア。 備考1 ガードは、次のように機能する。 ー 単独の場合：可動式ガードでは“閉じた状態”のときだけ有効であり、固定式ガードでは“確実に取り付けられている状態”のときだけ有効である。 ー ガード施錠式又は施錠なしのインターロック装置と組み合わせる場合：ガードの位置によらず、保護が確実にされる。 備考2 ガードはその設計によって、例えば、ケーシング、シールド、カバー、スクリーン、ドア、囲いガードと呼ばれる場合がある。 備考3 ガードの種類及びその要求事項は、JIS B 9700-2:2004の5.3.2及びISO 14120を参照。	*) JIS B 9700-1、3.25
	外的リスク軽減施設	External risk reduction facility	E/E/PE安全関連系及び他技術安全関連系から分離、区分され、かつ、それらを用いない、リスクを軽減又は緩和する手段。例えば、排出装置、防火壁、堤防など。	JIS C 0508-4:1999 3.4.3
	ガイドワード	Guideword	HAZOPにおいて、ハザードを確認し、その操作上の問題点を分析し、目標値からのずれを想定するための言語をいう。ガイドワードとしては、「no」、「more」、「less」、「as well as」、「part of」、「reverse」、「other than」、「sooner」、「later」、「where else」、「higher」、「lower」、「service failure」、「corrosion、erosion」、「spare equipment」、「safety」などが用いられる。	
	回復	Recovery	修復に同じ。	
	外部電源喪失	Black Out:BO	外部電源から電力供給を受けている場合、故障などの理由によりその電力を失うこと。電力喪失は、機能喪失となりうるので、安全設計では重要な事象である。	
	カテゴリ	Category	不具合 (障害) に対する抵抗性 (フォールト・レジスタンス)、及び不具合 (障害) 条件下の挙動に関する制御システムの安全関連部の分類 (B、1、2、3、4の5種類) であって、安全関連部の構造的配置及び／又は安全関連部の信頼性によって達成される。	*) JIS B 9705-1、3.2
	可用性	Availability (Performance)	要求された外部資源が用意されたときと仮定したときアイテムが与えられた条件で、与えられた時点、又は期間中、要求機能を実行できる状態にある能力。	JIS Z 8115
	監査	Audit	実際の業務やその成果物が、法令や各種規制、規程及びその他の通達など予め定められたルールや規範に則っているかどうかを、客観的な第三者が適切な手法を用いて検証し、是正すべき点があればそれを指摘する業務のこと。	

見出	用 語	英文 (略号)	解 説	出 典
	感度分析	Sensitivity analysis	どのリスクがプロジェクトに最も影響を与える可能性があるかを明らかにすること。他の全ての不確実な要素をベースライン値（基準値）に固定した状態で、プロジェクトの個々の不確定要素が、検討対象となっている目標に与える影響の度合いを調べる。	
き	危害	Harm	人の受ける身体的障害若しくは健康障害、又は財産若しくは環境の受ける害。	JIS B 9700-1 3.5
	機械安全規格	Safety standard of machinery	機械類の安全性についての国際規格群で、A基本安全規格、Bグループ安全規格、C個別機器安全規格の3階層体系となっている。A、B、C規格参照。	
	危険側故障	Dangerous failure	安全関連系（SRS）を危険な方向すなわち機能喪失の状態にする可能性を持つ障害。 備考 その可能性が現実化するかどうかは、システムのチャネル構成法に依存するであろう。安全性向上のための多チャネルを持つシステムでは、危険側ハードウェア故障がシステム全体を危険、すなわち、機能喪失の状態へと導くことはより少ない。	JIS C 0508-4:1999 3.6.7 JIS B 9700-1 3.30
	危険側故障率	Frequency of a Dangerous Failure per Hour	時間当たりの危険側故障の率を危険側故障率という。安全関連系（SRS）のリスク軽減に関して故障は、安全側故障と危険側故障とに分類されるが、危険側故障の算出式は危険側故障＝検出可能危険側故障＋検出不可能危険側故障であらわされる。	
	危険側優先度	Risk priority number	FMEA等でリスクを評価する尺度で、きびしさ×発生頻度×検出難易度により求められる。	
	危険区域	Danger zone Hazard zone	人が危険源に暴露されるような機械類の内部及び／又は機械類周辺の空間。	*) JIS B 9700-1、3.10
	危険源	Hazard	危害を引き起こす潜在的根源。 備考1 “危険源”という用語は、その発生源（例えば、機械的危険源、電氣的危険源）を明確にし、又は潜在的な危害（例えば、感電の危険源、切断の危険源、毒性による危険源、火災による危険源）の性質を明確にするために適切である。 備考2 この定義において、危険源は、次を想定している。 — 機械の“意図する使用”の期間中、恒久的に存在するもの（例えば、危険な動きをする要素の運動、溶接工程中の電弧、不健康な姿勢、騒音放射、高温）又は — 予期せずに現れ得るもの（例えば、爆発、意図しない及び予期しない起動の結果としての押しつぶしの危険源、破損の結果としての放出、加速度又は減速度の結果としての落下） 注）JIS C 0508では、“Hazard”は、潜在危険と訳している。	*) JIS B 9700-1、3.6
	危険源の組合せ	Hazard combination	機械的危険源、電氣的危険源、熱的危険源、放射線の危険源、人間工学無視による危険源など複数の各種危険源の組み合わせ。個々には些細とみられる危険源であっても、これらが互いに組み合わせられて重要な危険源と同等になる場合がある。	
	危険事象	Harmful event	危険状態から結果として危害に至る出来事。	*) JIS Z 8051、3.4
	危険状態	Hazardous situation	人が少なくとも一つの危険源に暴露される状況。暴露されることが、直ちに又は長期間にわたり危害を引き起こす可能性がある。 すなわち、人、財産又は環境が、一つ又は複数のハザードにさらされる状態。	*) JIS B 9700-1、3.9
	機能安全	Functional safety	EUCとEUC制御系の全体に関する安全のうち、E/E/PEの安全関連系、他技術安全関連系及び外部リスク軽減施設に依存する部分。つまり、システムにはそれぞれの危険源は存在するが、安全装置の機能によるリスク低減によって許容できるレベルにまで達成された安全のこと。	JIS C 0508-4:1999 3.1.9 ISO 1200-1 3.28
	機能安全監査	Functional safety audit	計画された定めに基づく機能安全要求事項に定められた手順が効果的に実施されているか、更に定められた目的の達成に適切であるかを決定する系統的、かつ独立した審査。	JIS C 0508-4:1999 3.8.4
	機能安全評価	Functional safety assessment	根拠に基づいて、一基以上のE/E/PE安全関連系、他技術安全関連系又は外的リスク軽減施設によって機能安全が達成されることを判定するための調査。	JIS C 0508-4:1999 3.8.3
	機能相関図	Function flow diagram	システムを構成するサブシステムや要素の機能の相互関係を情報や制御の流れとともに図示したもの。	
	機能ユニット	Functional unit	特定の目的を遂行することのできるハードウェア、ソフトウェア又はその両者からなる製品。 IEV191-01-01では、機能ユニットではなく、より一般的な用語”アイテム”（item）が使用されている。アイテムには、時に人も含まれる。	JIS C 0508-4:1999 3.2.1
	基本安全規格	Basic safety standard	あらゆる機械に適用できる基本概念や設計の原則などを規定した規格。A規格	
	共通原因故障	Common Cause Failures (CCF)	1つ以上の事象を原因とする故障で、それが冗長系の二つ以上の分離したチャネルそれぞれに故障を同時に引き起こし、システムの故障を生じさせるもの。 すなわち、単一の事象から生じる異なったアイテムの故障であって、これらの故障が互いの結果でないもの。 備考 共通原因故障は、共通モード故障と混同しないようにする必要がある。（IEC 60050のIEV-191-04-23参考）	JIS C 0508-4:1999 3.6.10 JIS Z 8115 JIS B 9700-1、3.33
	許容リスク	Tolerable risk	現在の社会的価値観から受容されるリスク（ISO/IEC Guide 51 第2版：1997ドラフト）。	JIS C 0508-4:1999 3.1.6
く	偶発故障期 偶発故障期間	Constant (Random) failure intensity period Random failure period Change failure period Constant failure rate period	修理系アイテムの運用期間中、故障強度がほぼ一定である期間、又は非修理系アイテムの運用期間中、故障率がほぼ一定である期間。 備考1. 修理系アイテムの場合は”一定故障強度期間”（Constant failure intensity period）、非修理系アイテムの場合は”一定故障率期間”（Constant failure rate period）ともいう。 備考2. 初期故障期間を過ぎ、磨耗故障期間に至る以前の時期に偶発的に故障が発生する期間。	JIS Z 8115：2000

見出	用 語	英文 (略号)	解 説	出 典
	組込システム	Embedded system	家電製品や産業機器などに搭載され、それを制御することで特定の機能を実現するコンピュータシステムの総称。組込みシステムが対象としているものは、炊飯器やエアコンなどの家電から、人工衛星やミサイルなどの宇宙/軍事に至るまで多岐にわたる。また、汎用的なPCと異なり目的が様々であることから、専用のソフトウェア（組込みOSやアプリケーションソフトウェア等）とハードウェアは多種多様である。	
	グループ安全規格	Group safety standard	ある程度広範囲な機械群に対して適用できる安全性を規定した規格。B規格。	
	クロスセッション法	Cross session method	先行している他の事例から将来像を予測する方法。時間と空間を超え、似たような状況を探し、先行した指標を読み、対象を切断、輪切りにした状態で判断する。	
け	形式手法	Formal method	論理学、集合論、代数学などの数学を基礎としたシステムの仕様記述手法、検証手法などの総称。要求、仕様、設計などを自然言語ではなく、形式的言語で記述することにより、あいまいさを排除し、上流工程での検証を可能とする。半形式手法では、全ての記述を形式化しないので、形式的手法よりも導入しやすく、仕様や設計は他の(半)形式的手法に置き換えることもできる。IEC 61508において規定されている手法で、Data flow diagramsやDecision tablesなどの記法のほか、truth tablesなどの手	
	形式証明	Formal proof	仕様もしくはプログラムの正しさを、数学的・論理的に証明すること。STL 4の安全度水準が要求されるシステムにおいては、形式証明 (formal proof) の実施が強く推奨 (HR: highly recommended) されている。	
	決定論的原因安全度	Systematic safety integrity	安全関連系の安全度のうち、危険側の機能失敗に導く決定論的原因故障にかかわる部分。 備考 決定論的原因安全度は、常に定量化が不可能である（通常可能なハードウェア安全度と区別される）。	JIS C 0508-4:1999 3. 5. 4
	決定論的原因故障	Systematic failure	ある種の原因に決定論的に関連する故障。この原因は、設計変更、製造過程、運転手順、文書化又はその他の関係する要因の修正によってだけ除かれる。システムティック故障に同じ。	JIS C 0508-4:1999 3. 6. 6
	公式手法	Formal method	形式手法を参照。	
	公式証明	Formal proof	形式証明を参照。	
こ	構成管理	Configuration management	ライフサイクルを通じて、進展するシステム要素の変化を管理し、連続性と追跡性を保持するために、そのような要素を同定する業務。	JIS C 0508-4:1999 3. 7. 3
	高頻度作動要求モード	High frequency operation request mode	安全関連系への作動要求頻度が、年1回より大きいか、または、ブルーテスト頻度の2倍よりも大きい運用モード。逆の運用モードを低頻度作動要求モード (Low frequency operation request mode) という。	JIS C 0508-4:1999 3. 5. 12
	合理的に予見可能な誤使用	Reasonably foreseeable misuse	供給者によって意図されない状態又は目的による製品、プロセス又はサービスの使用法。ただし、それらの使用法は、通常考えられる人の挙動と関連し、又はその挙動の結果から誘発され得るものである (ISO/IEC Guide 51:1997)。	JIS C 0508-4:1999 3. 1. 11
	コートニ理論	Courtney Theory	1992年英国のリチャード・コートニにより提唱されたリスク分析手法である。以下の算出式により、リスクを定量的に示す。 リスク＝脅威の発生頻度 X 被害の大きさ	
	故障	Failure	要求される機能を遂行する能力がアイテムになくすること、すなわち、ある機能ユニットの要求される機能遂行能力の終結。機能失敗とも言う。故障は、（ハードウェアでの）ランダムハードウェア故障と（ハードウェア又はソフトウェアでの）決定論的原因故障（システムティック故障）とに分類される。 備考1 故障後に、アイテムは不具合（障害）になる。 備考2 故障は事象であって、状態を意味する不具合（障害）とは区別される。 備考3 ここに定義される概念はソフトウェアだけで構成されるアイテムには適用しない。[IEC 60050のIEV-191-04-01参考]	JIS Z 8115 JIS C 0508-4:1999 3. 6. 4 JIS B 9700-1、3. 32
	故障モード	Failure mode	故障状態の形式による分類で、例えば、断線、短絡、折損、磨耗、特性の劣化などの物理・化学的な変化（システムの破壊）をいう。	JIS Z 8115 : 1981
	故障モード影響診断解析	Failure Modes、Effects and Diagnostic Analysis (FMEDA)	FMEDAをベースに自己診断テストの能力評価ができる拡張した分析手法。通常のFMEAによる分析に加えて、安全側故障か危険側故障かの区別、故障率、故障診断方法、診断による故障検出率等についても考慮し、システム全体での診断率を算出する手法。	
	故障率曲線	Bathtub curve	機械や装置の時間経過に伴う故障率の変化を表示した曲線のこと。その形からバスタブ曲線と呼ばれて、時間の経過により初期故障期、偶発故障期、摩耗故障期の3つに分けられる。	
	固定式ガード	Fixed guard	工具の使用によって、又は取付け手段を破壊することによってのみ、開いたり又は取り外すことができるような方法（例えば、ねじ、ナット、溶接により）で取り付けられたガード。 工具を使用せずに開くことができるガードは、可動式ガードという。	*) JIS B 9700-1、 3. 25. 1
	個別機械安全規格	Specific safety standard	特定の機械又は機械群に対する詳細な安全性要求事項を規定する規格に関連する国際規格体系のうち、最下層のC規格のこと。C規格が存在する機械はC規格に従って設計することになるが、C規格が存在しない機械の場合はA規格及びB規格に従って設計することになる。	JIS B 9700-1:2004解説 図1
	固有安全	Inherent safety、Intrinsic safety	安全のために自己を制御する性質。本質安全のこと。例えば、水を冷却・減速材としている原子炉（軽水炉）には、核分裂の増加を抑制する性質があり、これを特に原子炉の固有の安全性と呼んでいる。	

見出し	用語	英文(略号)	解説	出典
さ	サブシステム	Subsystem	システムとは、設計上の意図に従って相互作用を行う要素の集合であり、システムの要素は、サブシステムといわれる別のシステムになり、制御するシステム又は制御されるシステムとなることもある。システムは、ハードウェア、ソフトウェア更に人的な相互作用を含むこともある。 備考 人は、システムの一部になりうる。	JIS C 0508-4
	残留リスク 残存リスク	Residual risk	安全措置が取られた後に、なお残存するリスク(ISO/IEC Guide 51第2版：1997ドラフト) 備考 この規格は次のように区別する。 ― 設計者が保護方を講じた後の残留リスク ― 全ての保護方を実施した後の残留リスク	JIS C 0508-4:1999 3.1.7) JIS Z 8051 JIS B 9700-1、3.12、図1参照
し	自己診断率	Diagnostic coverage	自動的な診断テストによって実現される危険側ハードウェア故障の低減率。	JIS C 0508-4:1999
	システムティック安全度	Systematic safety integrity	決定論的原因安全度参照。	
	システムティック故障	Systematic failure	決定論的原因故障参照。	
	システム故障	System failure	系全体の機能の喪失または、規定された機能水準を下回る、系の一時的機能低下、すなわち系のサービス中断として用いる言葉。	JIS Z 8115
	時相論理	Temporal logic formulary	時相論理とは、時間を状態変化として問題を理解し表現するための規則と表記法の体系で、システムのハードウェアやソフトウェアの要求仕様を記述する方法である。形式証明で利用される。大きく分岐時間を扱うものと線形時間を扱うものの二種類がある。時相論理式とは、時間に関する様相を論理式で示したもので、記号論理学に必然性演算子と可能性演算子を付加したものの。	
	シナリオライティング法	Scenario-writing method	仮説に従い将来の定性的な情景を時間や分野を区別して予測を記述し、複数の代替案を作成する。組織の外部環境に生じる様々な出来事を論理的に積み上げ、現在の状況から将来どのような状況が生まれるかを予測する手法。社会調査の手法としてアンケートやヒアリング情報と組み合わせる。	Think IT
	シミュレーション法	Simulation method	モデルを作り、コンピュータプログラムを使って予測する方法。例えば気象予測の例では、ハリケーンの被害予測を、風速の増幅に大きな影響を与える火山地形図や地域独特の建設習慣などをデータ化し、ハリケーンの中心気圧や暴風圏、進路の変化による規模の変動、地域に与える影響などをシミュレーションする例がある。	
	従属故障	Dependent failure	故障によるフォールトとの存在確率が、故障を引き起こす各々の原因の無条件存在確率の単純な掛け算として表現できない故障。	JIS C 0508-4:1999 3.6.9
	修復	Restoration	フォールト状態の後、アイテムが要求機能を遂行する能力を取り戻すこと。回復(Recovery)ともいう。	JIS Z 8115
	修理系	Repairable item Repairable system	運用開始後、保全によって故障の修理が可能な系。	JIS Z 8115
	障害(不具合)	Fault	予防保全若しくは計画的行動又は外部資源の不足によって機能を実行できない状態を除き、要求される機能を実行できないアイテムの状態。本書では不具合、不適合も同義語として扱う。 備考1 障害(不具合)は、しばしばアイテム自体の故障の結果であるが、事前の故障がなくても存在することがある。[IEC 60050のIEV 191-05-01参考] 備考2 不具合(障害)及び故障という語は、しばしば同義語として使用される。	JIS B 9700-1、3.31 III)表3.7 JIS Z 8115 (フォールトと表現している。)
	使用者	User	機械及びそれに関連する電気装置を使用する者。	*) JIS B 9960-1、3.57
	使用上の情報	Information for use	使用者に情報を伝えるための伝達手段(例えば、文章、語句、標識、信号、記号、図形)を個別に、又は組み合わせて使用する保護方策。 注記 使用上の情報は、次のように分類される。 ― 機器の状態変化や異常状態を知らせるための信号及び警報装置 ― 機器を正しく使用するために必要な表示、標識(絵文字)及び警告文 ― 機器の運転や保全等に必要とされる附属文書 備考 JIS B 9700-2:2004の6.は使用上の情報を扱う。	*) JIS B 9700-1、3.21
	状態遷移図	State transition diagram	ある条件が成立したときに、ある状態から別の状態に移ることを図式化した図のこと。時間の経過や状況の変化に基づいて、そのときの動作を記述する。状態を円で、状態の変化を矢印で図示し、タスクの状態変化を図式化する場合に用いられる。	
	冗長	Redundancy	アイテム中に要求機能を遂行するための二つ以上の手段が存在する状態。 備考1 冗長で手段の一部が故障してもアイテムは故障とならない性質を特に冗長性という。 備考2 冗長なシステムを冗長系という。 備考3 JIS C 0508では、ある機能ユニットに要求される機能を実行するための又はデータが情報を表すための十分な手段に、更に追加された手段と表現されている。	JIS Z 8115 JIS C 0508-4:1999 3.3.10
	冗長設計	Redundant design	システムの構成要素や機能の実現手段を複数用意した冗長性によって、一部に故障が発生しても上位系の障害に至らないよう配慮した設計。	
	初期故障期 初期故障期間	Early failure period	アイテムの運用初期において、与えられた時点での修理系アイテムの瞬間故障強度、又は非修理系アイテムの瞬間故障率が後に続く期間の値よりも著しく高い期間。	JIS Z 8115
	深層防護	Defense in depth	原子力施設の安全性確保の基本的考え方の1つ。原子力施設の安全対策を多段的に構成しており、次の3段階からなる。1)異常発生防止のための設計、2)万一異常が発生しても事故への拡大を防止するための設計、3)万一事故が発生しても放射性物質の異常な放出を防止するための設計。多重防護ともいう。	原子力防災用語集
	診断テスト間隔	Diagnostic test interval	安全関連系のフォールトを発見するために定められた診断範囲をもつオンラインテストを実施する時間間隔。	JIS C 0508-4:1999 3.8.7

見出	用 語	英文 (略号)	解 説	出 典
	信頼性	reliability	アイテムが与えられた条件の下で、与えられた期間、要求機能を遂行できる能力。 備考1 一般に、信頼性性能は適切な尺度で数量化され、これを信頼度という。 備考2 ソフトウェアアイテムの場合、信頼性は系の運用経過時間中に発生する故障要因の修正と変更で改善が進み、一般に信頼度は経過時間とともに向上していく。 (IEC 60300-3-6、MT15参照)。	JIS Z 8115
	信頼性ブロック図	Reliability Block Diagram	一つ以上の機能モードをもつ複雑なアイテムにおいて、複数のブロックで表わされる下位アイテム又はその組合せのフォールトが、アイテムのフォールトを発生する仕組みを示したブロック図。	JIS Z 8115
サ セ	スリーステップメソッド	3-step Method	設計者により、次の手順で講じられる保護方策。 — ステップ1: 本質的安全設計方策 — ステップ2: 安全防護及び付加保護方策 — ステップ3: 使用上の情報 (例: 取扱説明書、信号と警報装置、表示、標識、警告文など)	*) JIS B 9700-1、5.4及びJIS B 9700-1、図2参考
	制御機器	Control device	制御回路の中にあつて機械の運転制御に使用される機器 (例えば、位置センサ、手動操作スイッチ、リレー、電磁弁)。	*) JIS B 9960-1、3.9
	制御システム	Control system	手動制御装置 (手動制御器/アクチュエータ)、データ記憶・論理処理、センサ、保護装置、信号、表示、警告装置から構成される。	*) JIS B 9700-1、附属書A参考
	制御システムの安全関連部	Safety-related parts of control systems (SRP/CS)	入力信号に応答し、かつ安全関連出力信号を生成する制御システムの部分又は附属部分。SRP/CSといい、これを構成する製品には次のものがある。例: リレー、ソレノイドスイッチ、PLC、モータ制御ユニット、両手操作スイッチ、圧力検知装置。	*) ISO 13849-1 3.1 III) 第3章 コラム (P. 107)
	制御装置	Controlgear	開閉機器並びに、これらに付随する制御、計測、保護及び調整装置との組み合わせ。また、相互接続、付属品、エンクロージャ及び支持構造を持ったこれらの機器及び装置の組み合わせに対する一般用語。 通常、これは、電気を使用する装置を制御することを目的としている。	*) JIS B 9960-1、3.10
	制御停止	Controlled stop	制御装置が停止信号を認識すると、例えば指令電気信号をゼロにするが、停止するまでは、機械アクチュエータへの電気/電力を残しておく機械の停止方法。	*) JIS B 9960-1、3.11
	制御用計算機	Process computer	プロセスの制御や計測等機器をコントロールするための計算機で、コントロールコンピュータ、制御コンピュータ、プロセスコンピュータなどとも呼ばれる。通称プロコン。	
	製造物責任法	Products Liability Act	製品の欠陥により、消費者・利用者などの第三者が生命・身体または財物に関して生じた損害について、当該欠陥製品の製造・流通等に関与した者が負う損害賠償責任を規定した法律 (通称PL法という) をいう。	
	静的解析ツール	Static analysis tool	ソフトウェア・プログラムを実行することなく、ソースコードの品質を測定/評価し、ソースコードに内在する問題を改善するためのツール。プログラムに対して、ツールにより機械的にチェックを行うことにより、文法スタイルの誤りやパターン化されたバグ (バッファオーバーフローの脆弱性、メモリ競合状態やメモリリークなど) を検出する。	
	性能レベル	Performance Level (PL)	リスク低減実施後の安全制御システムの性能レベル。また予見可能な条件下で、制御システムの安全関連部による安全機能実行能力を指定するために使用されるレベル。	ISO 13849-1:2006
	セーフティケース	Safety case	システムが想定される使用環境において、十分安全であると信じられるのはなぜかという議論 (Augment) を与えるものであり、そのための記法や議論の枠組みとして、要求事項 (Claim) - 議論・推論 (Augment) - 証拠 (Evidence) という3層構造の論理体系が提案されている。	T. P. Kelly, Arguing Safety - A Systematic Approach to Managing Safety Cases, PhD Thesis, University of York, 1998
	セーフティコンポーネント	Safety Component	部品のこと。安全の原理・原則を採り入れた設計で、かつ第三者機関による安全性を立証された部品をセーフティコンポーネントと称する。	JIS B 9960-1、3.22
	セキュリティ	Security	一般的には、情報セキュリティのことで、情報の機密性、完全性及び可用性を維持すること。さらに、真正性、責任追及性、否認防止及び信頼性のような特性を維持することを含めても良い。組込製品の規格では、ISO/IEC 15408がセキュリティ評価基準などに関する国際標準になっており、セキュリティの一般モデル、機能要件、保証要件などが定められている。	JIS Q 27002:2006
	ゼロメカニカルステート設計	zero mechanical state design	製品が保有している種々のエネルギーがすべてゼロになった時、安全性が最も高くなるという考え方を基本とした設計。	
	全安全ライフサイクル	Overall safety lifecycle	IEC 61508における安全獲得のための16のフェーズ全体をさす。単に「安全ライフサイクル」と呼ぶ場合も多い。16のフェーズは概念の設定に始まり、リスク分析を行い、最終的には廃棄のフェーズに至る。 9番目のフェーズには、「E/E/EPs安全ライフサイクル (the E/E/PES safety lifecycle) 」、「ソフトウェア安全ライフサイクル (the software safety lifecycle) 」、「システムやソフトウェアに関係するフェーズが存在する。	IEC 61508-1 p. 33
	潜在危険	Hazard	危害に到る根源的な原因要素で、潜在しているだけでは危害には到らないが、ミスや故障などによって顕在化した場合、危害 (Harm) となって現れる。	JIS C 0508-4:1999 3.1.2
	潜在バグ	Potential bug	まだ顕在化していないが、プログラムの中に存在する可能性のあるバグ。	
	潜在リスク	Potential risk	目に見えないリスク。リスクマネジメント上では、業務への悪影響を潜在的に有していると考えられる状態を意味する。 (注) JIS C 0508-4:1999 には、リスク、許容リスク、残存リスクの用語定義はあるが、潜在リスクの定義はない。ただし、潜在危険 (Hazard) が定義されている。	ITマネジメント「続企業価値創造に向けた攻めのITマネジメント」第11回

見出し	用語	英文(略号)	解説	出典
そ	相対危険度評価法	Relative ranking techniques	プロセスの持つ危険性について、指標値を用いて各種のプロセスプラントを相対的に比較評価する定量的評価技法の総称。米国化学技術者協会AIChE (American Institute of Chemical Engineers)では、Relative Ranking Techniquesと呼んでいる。この手法の代表的なものが、米国のダウケミカル社で考案されたDow方式、英国ICI社のMond方式、日本の労働省通達「化学プラントのセーフティ・アセスメントに係る指針」がある。	
	ソフトウェア	Software	データ処理機構の運用に関係があるプログラム、手順、データ、ルールおよび任意の付随する文書化を含む知的創造物。 備考 ソフトウェアは、それが記録される媒体から区別される。	JIS C 0508-4:1999 3.2.2
	ソフトウェアライフサイクル	Software lifecycle	ソフトウェアが着想されてから、それがもはや使用に供されなくなるまでの間に生じる業務。 備考1 ソフトウェアライフサイクルは、典型的に、要求事項フェーズ、開発フェーズ、テストフェーズ、統合フェーズ、設置フェーズそして部分改修フェーズを包含す	JIS C 0508-4:1999 3.7.2
	ソフトウェア安全度	Software safety integrity	プログラマブル電子系のソフトウェアが定められた期間、すべての定められた条件でその安全機能を達成する確からしさを示す尺度。	JIS C 0508-4:1999 3.5.3
	ソフトウェア安全度水準	Software safety integrity level	ある安全関連系のソフトウェアの安全度を特定するための4種類の可能な離散的水準の一つ(安全度水準及びソフトウェア安全度参照)。安全度水準4は最高の安全度水準であり、1は最低である。	JIS C 0508-4:1999 3.5.7
	ソフトウェア安全要求仕様	Software safety requirements specification	安全関連系の実現において必要なソフトウェアへの要求仕様をまとめたもの。安全機能要求仕様と安全度要求仕様の両方を含まなければならない。安全機能のロジックを実現するための機能と、安全機能の度を確保するための機能がある。ハードウェアの診断機能は、ソフトウェアによって実現されるものが多い。	JIS C 0508-4:1999 3.5.11参考
た	ダイバーシティ(多様性)	Diversity	要求される機能を実行する異なる手段。 例 多様性は、異なる物理的原理又は異なる設計方法で達成されるであろう。	JIS C 0508-4:1999 3.3.9 Ⅲ) 図3.17
	他技術安全関連系	Other technology safety-related system	電気・電子・プログラマブル電子以外の技術に基づく安全関連系。例えば解放弁(リリーフバルブ)は他技術安全関連系である。	JIS C 0508-4:1999 3.4.2
	多重防護	Multiple Protection	深層防護参照。	
	妥当性確認	Validation	最終製品とその支援機能が、全体として使用者の用途に適合しているかいないかを確認する行為。 備考1 妥当性確認は、通常、最終製品について規定の運用条件の下で実施される。 備考2 ソフトウェアアイテムの場合、要求仕様事項を満たしているかをどうかを決定するために、開発プロセスの最終段階で、システム及びその構成部品を評価し、実証するプロセス。	JIS Z 8115 JIS C 0508-4 3.8.2
ち つ て	チャンネル	Channel	ある機能を独立して実行する要素又は要素群。例えば、2チャンネル構成とは、同一の機能を独立して実行する2チャンネルを持つ構成である。 備考 この用語は、完全なシステムを表すことも、システムの部分(例えば、センサ、最終要素)を表現することもある。	JIS C 0508-4:1999 3.3.8
	ツートハンドコントロール	Two-hand control device	両手で同時に操作をしなければ、装置が動作しないように配慮した設計。安易な操作をさける。両手操作制御装置に同じ。	*) JIS B 9960-1、 3.26.4
	定性的リスク分析	Qualitative risk analysis	認識したリスクに対するリスクの発生確率を考慮した優先順位付けを行う分析手法。リスク発生時のプロジェクト目標に及ぼす影響だけでなく、コスト、スケジュール、スコープ、品質などのプロジェクトの制約条件に対するリスク許容度などの要因を査定する。	
	低複雑度E/E/PE安全関連系	Low complexity E/E/PE safety-related system	E/E/PE安全関連系のうち、次の条件が同時に成り立つもの。 一 各々の部品のフォールトモードが明確に定義される。 一 フォールトモードでのシステムの挙動が完全に決定できる。 備考 フォールトモードでのシステムの挙動は、解析及び/又は試験方法によって決定されてよい。	JIS C 0508-4:1999 3.4.4
	ディペンダビリティ	Dependability	アベイラビリティ性能及びこれに影響を与える要因、すなわち信頼性性能、保全性性能及び保全支援能力を記述するために用いられる包括的な用語。	JIS Z 8115
	ディレーティング	Derating	アイテムのストレス比の低減。信頼性を改善するために計画的にストレスを定格値から軽減する行為。 部品に加わるストレスを軽減するために、定格値を下回る値で使用する。部品の故障はストレスの累積によって引き起こされるとすれば、ストレスを軽減すれば寿命を長くできる(故障率を下げられる)。このストレスの軽減がディレーティングと呼ばれるもので、例えば、電子部品に対する主要なストレスは、温度、電圧、電流、及び電力である。	JIS Z 8115 JISC日本工業標準調査会 HPより
	データフロー図	Data Flow Diagram (DFD)	システム間のデータの発生・吸収・処理・蓄積など流れを矢印で繋いで図示したもの。データの発生から出力まで視覚化することによって、データの流れを明確にし、ネックや効率化しやすいポイントを発見し易くする。	
	適合確認	Verification	規定された要求事項が満たされていることを、客観的証拠としての調査及び提示によって確認する行為。又は製品がライフサイクルの中の与えられた段階(又はその部分段階)に対して定義されるディペンダビリティ(信頼性)仕様に適合しているかいないかを判定する行為。 備考1 設計及び開発において、検証(又は適合確認)は、対象となる活動の結果を調査・吟味し、その活動に関して明記された要求事項に適合しているかいないかを判定することに係わるものである。 備考2 ソフトウェアアイテムの場合は、ある開発段階の製品がその段階の初めに課せられていた条件を満たしているかどうかを決定するため、システム又は部品を評価するプロセス。この評価は一般に要求事項を反映した製品機能の仕様に基づく評価基準によって行われる。 適合確認参照。	JIS Z 8115 JIS C 0508-4:1999 3.8.1

見出	用 語	英文 (略号)	解 説	出 典
	デジジョン・ツリー分析	Decision tree analysis	想定シナリオの発生確率とコストにより、どのアクションを講じるかの意思決定をする際に使用する決定木(decision tree)による分析手法。「どのような意思決定が発生するか」、「意思決定項目の間に不確実要素はないか」など選択・分類・分岐を樹形図にして整理し、将来発生するシナリオの全体像を理解する。	
	テストカバレッジ	Test coverage	システム開発のテストにおいて、内部のロジック（命令、分岐、条件など）をどのくらい網羅したテストなのかを示す指標。「テスト網羅率」などとも訳される。これにより、検証が行なわれていないソースコードを管理し、テスト漏れ防止をはかる。	
	テストハーネス	Test harness	開発段階にあるソフトウェアにテストケースを適用して応答を記録することによって、当該開発段階のソフトウェア又はハードウェアの運用環境を（何らかの有用な程度で）模擬することを可能とする施設。 備考 テストハーネスには、テストケース発生器とテストの結果を（正しいと認められた値と自動的に比較することによって、又は人手による解析を実施することによ	JIS C 0508-4:1999 3. 8. 15
	デルファイ法	Delphi method	多くの専門家がそれぞれ独自に意見を出し合い、それを相互に参照し再び意見を出し合う、という作業を繰り返す行うことで、意見を収斂させ、未知の問題に対し確度の高い見通しを得るための手法。米国の研究機関ランドコーポレーションが開発した。	
	電磁耐性	Electromagnetic Immunity	安全関連システムが、付近にある電気機器などから放射される電磁波によって、自身の動作が阻害されないような電磁感受性(EMS:Electro Magnetic Susceptibility)を持つ特性。電磁耐性試験機により、電源線や信号線に混入する電磁波に対する耐性を測定できる。	
と	動的試験	Dynamic testing	必要な挙動ができ、かつ、望まない挙動を行わないことを立証するための統御された系統的な方法によるソフトウェアの実行及び/又はハードウェアの運用。 備考 動的試験は、静的分析に対比される。静的分析はソフトウェア質実行されることを必要としない。	JIS C 0508-4:1999 3. 8. 14
に	人間工学原則	Ergonomic principle	機械の設計（ハードウェアとソフトウェア）に際して、使用時だけでなく、取付け、調整、保守、清掃、修理、移動、運搬などを最適に行うため、作業者の身体的・心理的特性、即ち感覚・知覚の能力、形態学的条件、運動能力や筋力、使用特性、使用環境が人間の能力に及ぼす影響やその限界に配慮して機械の使用に関係する感覚・知覚や身体的・機械的視点から最適化するための諸原則である。	*) JIS Z 8528-1:2001及びJIS Z 8530:2000参考
は	ハードウェア安全度	Hardware safety integrity	安全関連系の安全度のうち、危険側機能失敗に導くランダムハードウェア故障にかかわる部分。 備考 この用語は、安全関連系の安全度を損なう危険側故障に関連している。ここで関係する2個のパラメータは、安全関連系全体の危険側故障率及び作動要求時の機能失敗確率である。前者の失敗パラメータは、安全を維持するために連続した制御を行うことが必要な場合に用い、後者のパラメータは安全関連系に対して使用する。	JIS C 0508-4:1999 3. 5. 5
	ハインリッヒの法則	Heinrich's Law	1件の重大事故の背景に、29件の軽傷の事故と300件の「ヒヤリ」「ハット」する体験があるという労災事故に関する「1:29:300の法則」。1930年代に米国の保険会社に勤務していた安全技師のハーバード・ウィリアム・ハインリッヒ氏が論文の中で発表した。	IT Pro ITレポート
	ハザード	Hazard	危険源と同じ。	
	パターン分類方式	System of pattern classification	経営者や顧客への影響、脅威の大きさを分類する方式。脆弱性対策のガイドラインを定め、管理策が必要な脅威や弱点を分析する。	
	半形式手法	Semi-formal method	準形式手法ともいう。形式手法を参照。	
	半公式手法	Semi-formal method	半形式手法を参照。	
ひ	光カーテン	Light curtain	一つ又はそれ以上の発光器及び受光器の組合せからなり、検出区域、検出能力ともに供給者（機械に関連する設備又は役務を提供する者）が指定する能動的光電保護装置。	*) JIS B 9704-2、 3. 6
	非常停止	Emergency stop	インターロック系の動作または手動により、運転時の機能が未完了であっても人間の安全を損なわない状態で、緊急に運転を止める機能で、次のことを意図する機能。 — 人に対する危険源を又は機械類若しくは工程中のワークへの損害を避けるか又は低減する。 — 人間の単一の動作によって停止指令を出す。 備考 詳細はJIS B 9703を参照。	JIS B 9700-1 3. 37
	非常停止装置	Emergency stop device	非常停止機能を始動するために使用される手動操作の制御機器。 備考 「非常停止機器」ともいう。IEC 60947-5-5:1997参照。	JIS B 9703、3. 2
	被制御機器	Controlled device	制御される装置。EUCのこと。	
	被制御系	Equipment under control (EUC)	製造、プロセス、運輸、医療、その他の業務に供される機器、機械類、装置、プラントなど。備考 EUC制御系はEUCから分離区別される。	JIS C 0508-4:1999 3. 2. 3
	非制御停止	Uncontrolled stop	機械アクチュエータへの電力を切ることによる機械動作の停止であり、ブレーキその他の機械的停止装置はすべて動作させるもの。 非常停止と同じ分類になると設計上はわかりやすいが、システムによっては、非常停止とは別扱いになる場合がある。	*) JIS B 9960-1、 3. 56
	非対称誤り特性	Asymmetrical failure characteristics	安全側の故障モードになる確率が危険側の故障モードになる確率よりも著しく高い特性。	
人	Person	Person	すべての個人をいい、使用者又はその代理者によって、当該機械の使用及び保全を仕事として割り当てられ、教育された人を含む。	*) JIS B 9960-1、1 備考2
	ヒューマンエラー	Human error、Mistake	意図しない結果を生み出す人の行為又は不行為。人的過誤ともいう。 ”又は不行為”を付加することによって、IEV 191-05-25に準拠する。	JIS C 0508-4:1999 3. 6. 12 IEC 61508-4 32. 6. 12 *) JIS B 9700-4、 4. 9

見出	用 語	英文 (略号)	解 説	出 典
ふ	フールプルーフ	Fool-proof	人為的に不適切な行為または過失などが起こっても、アイテムの信頼性および安全性を保持する性質。	JIS Z 8115
	フェールセーフ	Fail safe	アイテムが故障したとき、あらかじめ定められた一つの安全な状態をとるような設計上の性質。	JIS Z 8115
	フォールトアボイダンス	Fault avoidance	安全関連系の安全ライフサイクルの任意のフェーズで、フォールトを導き入れないようにするための技法と手続きの使用。 システムまたはそれを構成する要素の信頼性を高め、可能な限り故障の発生を回避しようとする考え方や、それに基づく設計・製造のアプローチのことをいう。例えば、高信頼素子の採用や高信頼化設計、徹底的なテスト・検証、品質管理体制の整備などがフォールトアボイダンスの典型的な要素である。フォールトアボイダンスと対峙する概念にフォールトトレランスがある。	JIS C 0508-4:1999 3.6.2 JIS Z 8115 Weblio 辞書
	フォールトトレランス	Fault tolerance	フォールト又はエラーの存在下で、要求される機能を遂行し続ける機能ユニットの能力。 つまり、システムに障害が発生したときに、正常な動作を保ち続ける能力で、障害発生時の被害を最小限度に抑える能力のこと。「耐障害性」「故障許容力」などと訳され、「故障が起こった際にどれだけ耐えられるか」という意味が強い。例えば、複数のエンジンを搭載した大型航空機は、いずれかが故障しても残りのエンジンである程度は飛び続けられるよう設計されている。コンピュータシステムでは、電源を多重化したり、定期的にデータのバックアップを取ること、電源に無停電電源装置を用いることなどがフォールトトレランスに当たる。	JIS C 0508-4:1999 3.6.3 JIS Z 8115 IT用語辞典e-Words
	フォールトレジスタンス	Fault resistance	不具合（障害）に対する抵抗性を言い、たとえ不具合（障害）が生じても安全機能に限っては安全を維持する能力のこと。	JIS B 9705
	付加保護方策	Complimentary protective measure	本質的安全設計でなく、安全防護策（ガード又は保護装置の実施）でもなく、使用上の情報でもない保護方策。 注記 付加保護策には、例えば、非常停止、遮断及びエネルギーの消散などの方策がある。	*) JIS B 9700-2、5.5参考 JIS B 9700-1、5.4
	不具合	Fault	「障害」に同じ。	*) JIS B 9700-1、3.31
	複雑度	Complexity	米国のThomas McCabeが開発したソフトウェア測定法の一つで、「循環的複雑度（サイクロマチック複雑度）」と呼ばれている。プログラムの複雑さを測るのにつかわれる指標の1つ。プログラムの複雑さは制御構造の複雑さで定まるとし、この複雑さを経路数（パス）の数で数えるとした。プログラムのソースコードから、線形的に独立し	
	不適合	Nonconformity	アイテムが製造業者の意図した設計又は仕様から逸脱している状態。本書では「障害」「不具合」に同じ。	JIS Z 8115
	ブルーフトテスト	Proof Test	安全関連系の故障状態を見つけるために実施される定期テスト。必要に応じて、システムを”新品”又は実際にこれに近い状態に修復するために、このテストを行う。 備考 ブルーフトテストの効果は、システムがどの程度新品に近い状態に修復されているかに依存している。ブルーフトテストが十分に効果を上げるためには、危険側故障状態を100%発見することが必要であろう。実際上は、低複雑度E/E/PE安全関連系を除いて100%達成は容易ではないので、努力目標と考えるべきである。最小限実施されるすべての安全機能がE/E/PE安全要求事項仕様に従ってチェックされる。分離したチャネルが用いられている場合、それらのテストは、各々のチャネルごとに独立して実行される。なお、ブルーフトテストを実施する時間間隔をブルーフトテスト間隔という。	JIS C 0508-4:1999 3.8.5
	ブルーブン・イン・ユース	Proven in use	安全関連系を構成するある要素において、危険側システムティック故障が起こる可能性が十分低いことを運用経験にもとづいて示すこと。	
	ブレインストーミング法	Brain storming	複数のメンバーが自由にアイデアを出し合い、互いの発想の異質さを利用して、連想を行うことによりさらに多数のアイデアを生み出そうという集団思考法・発想法。 1940年前後にアメリカの広告業界で創案されたが、その狙いは“つまらないアイデアでも、他の出席者には別の素晴らしいアイデアでも、ほかの出席者にはべつ素晴らしいアイデアをひらめかせるかもしれない”というもの。提唱者と言われるA.F. オズボーンは「討論参加者の一人がアイデアを出すと、彼はほとんど自動的に別のアイデアに対する創造力をかき立てる。それと同時に彼のアイデアは他の参加者全員の連想の電源を刺激する」と述べている。	
へ	平均危険側故障時間	Mean Time To dangerous Failure (MTTFd)	MTTFdとは、安全関連部が危険側故障に至るまでの平均時間。作動要求当たりあるいは、単位時間当たりの危険側故障確率である危険側故障は、ある部品が故障したとき、その故障が原因で安全機能を喪失するような故障を指す。MTTFdを求めるには、安全関連部をI：入力、L：論理、O：出力に分けてそれぞれの危険側故障までの時間を求め、それを平均化する。（ISO13849-1:2006の付属書CおよびDより引用）	OMURON Safety Information 38号 (2008.2.26)
ほ	防御的プログラミング	Defensive programming	不正な入力があっても、あるいは、実行環境に異常があっても、極力被害を被らないようにしたプログラム作成法。仕様を満たさない入力があることを予め想定したり、種々のあり得ないと思われることに対処できるように対処したコーディングのこと。	上克郎ほか「ICSE'96報告」（コンピュータソフトウェアVol.14、No.1、1997）
	保護方策	Protective measure	リスク低減を達成することを意図した方策。次により実行される。 — 設計者による方策（本質的安全設計方策、安全防護及び付加保護方策、使用上の情報）及び — 使用者による方策〔組織（安全作業手順、監督、作業許可システム）、追加安全防護物の準備及び使用、保護具の使用、訓練〕 いずれも、リスクを低減するための手段で、リスク低減方策ともいう。 備考 保護法策には、本質的な安全設計、保護装置、保護具、使用上及び据付けの上の情報並びに訓練によるリスクの低減策を含む	*) JIS B 9700-1、3.18
	本質安全	Inherent safety	固有安全とも言い、システムの基本設計や運転特性向けられた概念である。根源からリスクをなくして達成される安全のこと。機能安全に対比される。	

見出	用 語	英文 (略号)	解 説	出 典
	本質的安全設計方針	Inherently safe design measure	ガード又は保護装置を使用しないで、機械の設計又は運転特性を変更することにより、危険源を除去する又は危険源に関連するリスクを低減する保護方針。 注記 本質的安全設計方針には、例えば次のような方針がある。 — 幾何学的要因及び物理的側面を考慮した方針 — 機械設計上の一般的技術知識を考慮した方針 — 適切な技術選択による方針 — 構成品間のポジティブな機械的作用原理を適用した方針 — 機械の安定性に関する方針 — 機械の保全性に関する方針 — 人間工学原則を考慮した方針 — 電氣的危険源防止方針 — 空圧／液圧設備の危険源防止方針 — 制御システムへの本質的安全設計方針の適用 — 安全機能故障の確率の最小化 — 設備の信頼性による危険源への暴露機会の制限 — 搬入（供給）又は搬出（取出し）作業の機械化及び自動化による危険源への暴露機会の制限 — 設定（段取り等）及び保全の作業位置を危険区域外とすることによる危険源への暴露機会の制限 備考 JIS B 9700-2:2004の4. は本質的安全設計方針によるリスクの低減を扱う。	*) JIS B 9700-1、3.19 JIS B 9700-1、4参考
ま	摩耗故障期 摩耗故障期間	Wear-out Failure period	アイテムの運用後期で、修理系アイテムの瞬間故障強度、又は非修理系アイテムの瞬間故障率が、直前の期間の値よりも著しく高い期間。	JIS Z 8115
	マルコフモデル	Markov Model	現在の状態が過去のある時点までの状態に依存して確率的に決定されるような確率過程をマルコフ過程というが、その確率モデルをマルコフモデルという。これを用いることにより自然界や機械の振舞いを数式で記述し、その性質を解析することができる。例えば、センサやアクチュエータで構成される安全関連システムに、状態遷移確率が時間に依存するマルコフモデルを適用して故障診断等に使われる。	
も	目的機能失敗尺度	Target failure measure	安全度要求事項に関して達成される予定された危険側機能失敗確率で、次のどれかによって定められる。 — （低頻度作動要求モード運用では）作動要求当たり設計機能の実行に失敗する平均確率。 — （高頻度作動要求/連続モード運用では）時間当たりの危険側機能失敗確率（1/時間）。	JIS C 0508-4:1999 3. 5. 13
	モジュール	Module	ルーチン、個々の要素又はカプセル化されたルーチン又は相互に所属する個々の要素からなる機能単位。	JIS C 0508-4:1999 3. 3. 6
	モデル検査	Model Checking	システムの設計や仕様からモデルを作成し、モデルが検査項目を満たすかどうかをシステムが取り得る全ての状態に対して検査を実施することによって不具合を発見する技術。検査はモデル検査器に「モデル」と「検査項目」を入力し、モデルが検査項目を満たさない場合、どのような状況で満たされないかという反例（不具合に至るまでのトレース）を出力する。 モデル検査は「モデル作成」、「検査項目作成」、「モデル検査の実施」、「モデル検査結果からの不具合解析」の順で行っていく。	
ら	ライトカーテン	Light curtain	光カーテンに同じ。	
	ランダムハードウェア故障	Random hardware failure	時間に関して無秩序に発生し、ハードウェアの多様な劣化メカニズムから生じる故障。 備考1. 異なる部品ごとに異なる率で生じる多くの劣化メカニズムが存在し、製造上の許容誤差がそれらのメカニズムによって運転中の部品の故障を異なる時刻に引き起こす。従って、多くの部品からなる装置全体の故障は、予測可能な率で生じるが、予測不可能（ランダム）な時刻で発生する。 備考2. ランダムハードウェア故障とシステムティック故障を区別する主な性質は、ランダムハードウェア故障から生じるシステムの機能失敗率（又は適当な他の尺度）が、合理的な精度で予測可能であるのに対して、決定論的原因故障（による機能失敗）が、その性質上正確には予測できない点にある。すなわち、ランダムハードウェア故障によるシステムの故障（機能失敗）率が合理的な精度をもって定量化できるのに対し、システムティック故障によるものは、故障へと導く事象が容易に予測できないので、正確な統計量として把握できない。	JIS C 0508-4:1999 3. 6. 5
り	リスク	Risk	危害の発生率と危害のひどさの組み合わせ	*) JIS B 9700-1、3. 11 (ISO 12100-1:2003) JIS C 0508-4:1999 3. 1. 5
	リスクアセスメント	Risk assessment	リスク分析及びリスクの査定のプロセス。リスク評価に同じ（JIS Z 8115）。	*) JIS B 9700-1、3. 13 JIS Z 8115
	リスクグラフ	Risk graph	想定される「危害のひどさ」「暴露頻度」「危害回避の可能性」の順番で二者択一していき、要求されるパフォーマンスレベルを2分法の図で表現したもの。	
	リスクの見積り	Risk estimation	起こり得る危害のひどさ及びその発生確率を明確にすること。	JIS B 9700-1:2004、 3. 15 (ISO 12100-1:2003)
	リスクパラメータ	Risk parameter (Risk element)	危害のひどさと危害の発生確率で構成され、さらに危害の発生確率は次の要素からなる。 — 危険源へ人が暴露される頻度及び時間 — 危険事象の発生確率 — 危害の回避又は制限するための技術的、かつ人的可能性（例えば、速度の低減、非常停止設備、イネーブル装置、リスクの認知など） 「リスク要素」ともいう。	*) JIS B 9702、7.2参考

見出	用 語	英文 (略号)	解 説	出 典
	リスクマップ	Risk-map	R-Mapともいう。ルービックキューブの一面に似た縦横30の小間に、プロットした各々危害情報の安全度を表示する手法。それにより対象商品を客観的な視点、使用者の視点からデザインして見せる製品安全のツールである。(財)日本科学技術連盟が推進している。	
	リスクマトリックス	Risk matrix	リスクに関して横軸(列)に影響度(強度)、縦軸(行)に発生確率(頻度)を6段階または4段階に分けて作成したマトリックスのこと。そして、それぞれのリスクに影響度と発生確率によってマッピングしていき、高リスク(例えば赤色)、中リスク(例えば黄色)、低リスク(例えば緑色)に色分けしていくことで、プロジェクトのリスクの状況を一瞥できるマトリックス。	
	リスクマネージメント	Risk management	リスクに関して組織を指揮し管理する調整された活動。リスク因子を特定するためやリスクを算出するため一連の情報をシステムの的に使用する。ここで、リスクとはある事象の発生確率とその事象の結果の組合せを意味する。	TR Q 008:20003
	リスクレベル	Risk level (RL)	リスクアセスメントの結果、リスクが受容できるか、対応が必要であるかを判断するための基準。	
	リスク解析(分析)	Risk analysis	潜在的に危険な事象を同定し、当該リスクを推定するための有用な情報の使用。	JIS Z 8115 JIS B 9700-1:2004、 3.14 (ISO 12100-
	リスク査定	Risk evaluation	リスク解析に基づき、社会的、経済的及び環境上の要素を考慮して、当該リスクの受容性について判断がなされる過程。	JIS Z 8115 JIS B 9700-1:2004、 3.16 (ISO 12100- 1:2003)
	リスク低減プロセス	Risk reduction process	「リスク低減方策」に同じ。	
	リスク低減方策	Risk reduction measure	リスクを「受け入れ可能なリスク」まで低減するプロセス。	
	リスク評価	Risk estimation	リスクの評価に同じ。ハザード分析の結果を踏まえて、システムの持つリスクが許容範囲内であるか否かを判断する作業。ハザード分析を十分に実施するためには、ソフトウェアもその対象に含める必要がある。ハザード分析を行うための手法として、比較的早くから使用されているものに、ソフトウェアFTA、ソフトウェアFMEA、ソフトウェアHAZOPがある。	
	リスク評価	Risk evaluation	リスク分析に基づき、リスクの低減目標を達成したかどうかを判断すること。リスク低減の目標を達成している場合や、リスク比較の結果で良い結論が出たならば、機械が安全であるとの確信が得られる。リスクの評価の判定基準は、①リスク低減目標の達成、②類似機械類のリスクとの比較をもってなされる。最後に実行した手順及びその結果を論証するために文書化も要求される。 JIS Z 8115 では、リスク評価は、リスク解析とリスク査定の過程として、Risk assessment と同じとしている。	JIS Z 8115 (*) JIS B 9700-1、3.16
	リスク分析	Risk analysis	リスク因子を特定するための、及びリスクを算定するための情報の系統的な使用。 リスク解析と同じ。	TR Q 0008:2003
	両手操作制御装置	Two-hand control device	その装置を操作する人のためだけの保護手段となるものであり、危険な機械機能の起動開始指令を出し、かつ維持するために、両手による同時操作を少なくとも必要とする制御装置。 備考 詳細はISO 13851:2002を参照。	(*) JIS B 9700-1、 3.26.4
ろ	論理系(ロジック系)	Logic system	論理機能を行うシステムのうちセンサ及び最終要素(アクチュエータ等)を除いた部分。	JIS C 0508-4 3.4.5
よ	予期しない起動	Unexpected start-up、 Unintended start-up	その起動が予期できない性質であるため、危険を発生させる起動。これは、例えば次によって引き起こされる。 ― 制御システム内の故障による、又は制御システムに対する外部からの影響によって生じる起動指令 ― 起動制御における、又は、例えば、センサ若しくは動力制御要素のような機械の他の部分における、不適切な作用によって生じる起動指令 ― 中断後の動力供給の復帰 ― 機械の部分への外部及び内部影響(例えば、重力、風、内燃機関における自己点火等) 備考 自動サイクルの正常なシーケンス中の機械の起動は“意図しない起動”には含まれないが、オペレータの立場からは“予期しない起動”として考えられる。この場合における災害の回避には安全防護方策の使用がある(JIS B 9700-2:2004の箇条5参照)。 備考 「意図しない起動(Unintended start-up)」ともいう。	(*) JIS B 9700-1、3.29

[参考文献]

出典欄の*): JIS B 9701:0000「機械類の安全性—基本用語(案)」(向殿政男監修)より。

出典欄 I): 向殿政男監修第1巻「安全設計の基本概念」、II): 同第2巻「機械安全」、III): 同第3巻「制御システムの安全」より。

JIS C 0508-4:1999: 電気・電子・プログラマブル電子安全関連系の機能安全—第4部: 用語の定義及び略語。

JIS Z 8115:2000: ディペンダビリティ(信頼性)用語。

JIS B 9700-1:2004 (ISO 12100-1:2003) 機械類の安全性—設計のための基本概念、一般原則—第1部: 基本用語、方法論。

おわりに

本報告書は、昨年度に引続き、製品安全WGの活動内容をベースにまとめたものです。

昨年は、安全設計の基本をゼミ形式で勉強し、機能安全関連規格の調査を行うなど、基本技術、基礎的知識の収集を行いました。今年度は、各業界の安全施策や安全製品の応用事例を広く集めることにしました。自動車、鉄道、原子力、宇宙などです。ただ他にも安全に関して高いノウハウを持っている業界は多々あります。来年度は、各業界事例をもう少し集めておきたいと思っております。

また、安全関連製品の調査は、昨年始めて実施しましたが、今年度も再度調査を行いました。ただすべてを網羅しているとは言えません。さらに調査方法を工夫し、さらに広く、深く分析して、安全設計のガイドブックになるような改善が必要と感じております。

安全関連用語が業界や技術分野毎には定義されていますが、横断的な用語定義がなく全く同じ英文用語でありながら和訳が異なっているものもあり、組込み系用の用語集作成に今年度から挑戦することにしました。向殿先生から頂いた安全用語集も参考にさせていただきました。この場を借りて御礼を申し上げます。

この3年間の活動でいろいろな情報が集まってきたので、JASAのホームページに掲載し多くの方々が利用できるような企画もしました。来年度以降、具体化したいと思っております。

2010年は、IEC61508の第2版発行があり、ISO26262も全貌が明らかになりつつあります。

安全・安心な社会が政治・政策の場でもよく話題になっていますが、製品の安全実現については、機能安全の実現でもあります。今後も我々JASAの製品安全WGは微力ながら機能安全の技術向上を目指し、ひいては社会の安全性向上に貢献していきたいと考えております。

平成22年3月

J A S A 安全性向上委員会
製品安全ワーキンググループ
主査 金田 光範

*** 報告書の執筆者一覧 ***

第1章	入月 康晴
1.1 機能安全認証の概要	金田 光範
1.2 制御システムの安全	入月 康晴
1.3 安全 PLC	大塚 悦生
1.4 自動車の安全	漆原 憲博
1.5 原子力分野の安全性・信頼性対策の概要	金田 光範
1.6 ソフトウェアの安全	藤原 隆次
1.7 鉄道の安全	竹岡 尚三
1.8 安全規格認証製品	那須 誠
第2章	大塚 悦生
第3章	竹岡 尚三
第4章	済賀 宣昭

J A S A 安全性向上委員会

製品安全ワーキンググループ委員

漆原 憲博	(委員長)	株式会社ジェーエフピー
金田 光範	(WG主査)	東芝システムテクノロジー株式会社
大塚 悦生	(委員)	東芝システムテクノロジー株式会社
入月 康晴	(委員)	地方独立行政法人 東京都立産業技術研究センター
済賀 宣昭	(委員)	東海ソフト株式会社
那須 誠	(委員)	株式会社ジェーエフピー
中村 憲一	(委員)	アップウインドテクノロジー・インコーポレイテッド
竹岡 尚三	(委員)	株式会社アックス
藤原 隆次	(委員)	ビジネスキューブ・アント・パートナーズ株式会社
小柴 健生	(委員)	アヴァシス株式会社
六反田 喬	(委員)	ガイオ・テクノロジー株式会社
中村 洋	(委員)	株式会社レンタコーチ
前澤 敏昭	(事務局)	社団法人組込みシステム技術協会 (JASA)
兼本 茂	(アドバイザー)	会津大学 コンピュータ理工学部 教授
水口 大知	(アドバイザー)	独立行政法人 産業技術総合研究所
門田 浩	(アドバイザー)	IPA-SEC/日本電気株式会社

禁無断転載

平成 21 年度

**組込みシステムにおける情報セキュリティ対策および
機能安全に関する調査研究**

平成 22 年 3 月

社団法人 組込みシステム技術協会

〒103-0007 東京都中央区日本橋浜町 1-8-12

電話 03-5821-7973

FAX 03-5821-0444

<http://www.jasa.or.jp>